Symantec™ Validation and ID Protection Service (VIP)

Integration Guide for Pluggable Authentication Modules (PAM)

Symantec

Symantec VIP Integration Guide for Pluggable Authentication Modules (PAM)

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated May 27, 2014

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/index.html

Contents

Chapter 1

Introduction

VIP Integration Guide for Pluggable Authentication Modules (PAM) describes how to integrate the VIP integration module for PAM with VIP Enterprise Gateway to allow the User Name – Security Code authentication method. In this authentication method, the first factor is validated by VIP Enterprise Gateway, and the second factor is validated by Linux/Solaris/HP-UX/AIX PAM.

Partner Information

Table 1-1 Partner Information

Partner Name	Red Hat®/Oracle®/ HP®/IBM®
Product Name	Pluggable Authentication Modules (PAM)

Integration Overview

Table 1-2 Integration Overview

Authentication Methods Supported	User Name – Security Code
Client Integration	VIP Enterprise Gateway (EG) 8.x and higher
Supported Operating System	■ Red Hat Enterprise Linux 5.3 (32 Bit/64 Bit) ■ Red Hat Enterprise Linux 6.2/6.3 (64 Bit) ■ Solaris 10 (Sparc/x86)/HP-UX/AIX (32 Bit)
Supported Protocols	■ Telnet 0.17-39 (Linux) ■ Telnet 11.10.0 (Solaris Sparc/x86) ■ FTP 2.0.5-12 (Linux) ■ FTP 2.6.2 (Solaris Sparc/x86) ■ OpenSSH 4.3p2-29 (Linux) ■ OpenSSH 6.2p2 (Solaris Sparc/x86) ■ SunSSH 1.1.6 (Solaris Sparc/x86) ■ SFTP (HP-UX/AIX)

Software Requirement

SUNWlibC patch 119964-24 or higher (for Solaris x86)

Remote Access Integration Architecture

Authentication Method: User Name – Security Code

The following flow diagram illustrates the User Name – Security Code authentication method for PAM using the VIP Authentication Service:

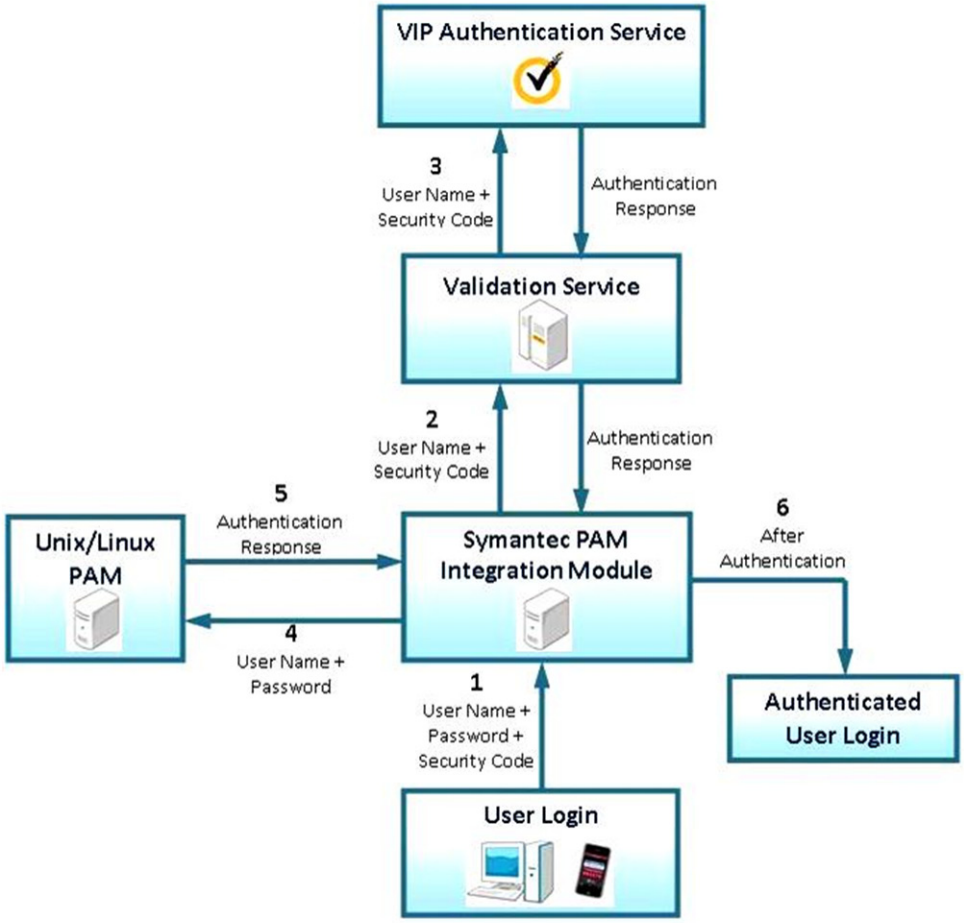

Figure 1-1 Authentication Process for User Name + Security Code Authentication Method

1. The user enters a user name, password, and security code.
2. As the first part of the two-factor authentication process, the VIP integration module for PAM sends the user name and the security code to the Validation Service.
3. The Validation Service authenticates the user name and the security code with the VIP Authentication Service.
4. As the second part of the two-factor authentication process, the VIP integration module for PAM authenticates the user name and the password with the Linux/Solaris/HP-UX/AIX PAM.
5. If Linux/Solaris/HP-UX/AIX PAM authenticates the user name and the password, the Linux/Solaris/HP-UX/AIX PAM returns group permission details to the VIP integration module for PAM along with the authentication response.
6. Based on this response, the user is allowed to log in.

Chapter 2

Installation and Configuration

Integration Summary

The following procedures describes how to configure the VIP integration module for PAM to use two-factor authentication through VIP Enterprise Gateway:

- **Task 1**: "Install and Configure VIP Enterprise Gateway" on page 3
- **Task 2**: "Configure the VIP Integration Module for PAM" on page 3

"Test an End User" on page 17

Task 1. Install and Configure VIP Enterprise Gateway

You must do the following:

- Install and Configure VIP Enterprise Gateway.
- Add the Validation Server in the User Name - Security Code authentication mode.
- To test the Validation Server, download and run the vsradiusclient_test utility (available in the tools.zip file from the VIP Manager Web site) on the PAM client host in verbose mode. The following is a sample command:

  ```
  # tools/<platform>/vsradiusclient_test --server-host <your_server_ip> --
  server-port <your_server_port> --secret <your_server_password> --client-ip
  <your_client_ip> --user-name <username> --password <security_code> --verbose
  ```

  where, <platform> is linux, linux_x86-64, solaris_sparc, solaris_x86, hpux, or aix.

For more information, refer to *VIP Enterprise Gateway Installation and Configuration Guide*.

Task 2. Configure the VIP Integration Module for PAM

You must complete the procedures that are described in this section to configure the VIP integration module for PAM.

You must configure the VIP integration module for PAM to communicate with the Validation Service using the RADIUS protocol. For more information, See "Configuration for RADIUS Communication" on page 4. After you complete this configuration, you can proceed with one of the following configurations as required:

- **Client-Server Communications Protocols (Telnet)**

  The VIP integration module for PAM can be used to support interactive communication protocol. For more information on configuring the VIP integration module for PAM to support interactive communication (Telnet), See "Client-Server Communications Protocol (Telnet)" on page 7.

- **Client-Server Communications Protocols (FTP)**

  The VIP integration module for PAM can be used to support non-interactive communications protocol. For more information on configuring the VIP integration module for PAM to support FTP (non-interactive communication), See "Client-Server Communications Protocol (FTP)" on page 9.

- **Secure Shell Connections (OpenSSH)**

  The use of security code-based two-factor authentication is also supported through OpenSSH servers. You must enable client platforms (where users enter their user names, passwords, and security code values)

with the OpenSSH client. For more information on configuring OpenSSH client configuration, See "Secure Shell Connections (OpenSSH)" on page 10.

- **Secure Shell Connections (SunSSH)**

  The use of security code-based two-factor authentication is also supported through SunSSH servers. You must enable client platforms (where users enter their user names, passwords, and security code values) with the SunSSH client. For more information on configuring SunSSH client, See "Secure Shell Connections (SunSSH)" on page 15.

- **Client-Server Communications Protocol (SFTP)**

  For more information on configuring the VIP integration module for PAM on the HP-UX/AIX platform to support SFTP, See "Client-Server Communications Protocol (SFTP)" on page 16.

You can use PAM flags to change the default configuration. For more information on PAM flags, See "Advanced Configuration of PAM Files" on page 16.

Configuration for RADIUS Communication

Complete the following steps to configure the VIP integration module for PAM to communicate with the Validation Service using the RADIUS protocol:

1 Log in as root to the server on the PAM client host machine.

2 Run the `camouflage` utility (available in the `tools.zip` file from the VIP Manager Web site), specifying your RADIUS shared secret on the command line.

Usage:

```
camouflage <password>
```

Example:

```
# tools/<platform>/camouflage password
RNq6gi75hp0erLCbB7idaQ==
```

where, `<platform>` is linux, linux_x86-64, solaris_sparc, solaris_x86, hpux, or aix.

Note: Do not use the 32-bit `camouflage` utility on 64-bit Linux.

---

3 Modify the entries in the `RADIUS configuration` file at `/etc/raddb/vrsn_otp` (you must create it, if it does not exist). Enter the correct RADIUS host IP, port number, encrypted shared secret, and (optionally) the timeout and retry values used by the local machine. For example, a line in the configuration file reads as follows:

For linux, linux_x86-64, solaris_sparc, and solaris_x86:

```
vipeg_server_ip:port <camouflaged_password> 5 3
```

For HP-UX and AIX:

```
vipeg_server_ip:port <camouflaged_password> 5 3  local_ip
```

`vipeg_server_ip:port` is the IP address and the port number of the validation service (RADIUS server) to which the VIP integration module for PAM connects.

`<camouflaged_password>` is the encrypted version of the RADIUS shared secret obtained in the previous step.

5 is the timeout (in seconds). The timeout is how long the module waits until deciding that the server has failed to respond.

3 is the number of retries. A retry value is the number of times the module attempts to connect to the server (in conjunction with timeout) until deciding that the server has failed to respond. This parameter is a Symantec-unique addition to the standard RADIUS configuration.

(Optional) `local_ip` is the IP address of the local machine from which the RADIUS server is reachable, in case there are multiple NIC on the machine.

4 Optionally, to support fail over to multiple RADIUS servers, add an additional line for the failover RADIUS server.

For example:

For Linux, Linux_x86-64, Solaris_Sparc, and Solaris_x86:

```
vipeg_server_ip_other:port <camouflaged_password> 5 3
```

For HP-UX and AIX:

```
vipeg_server_ip_other:port <camouflaged_password> 5 3 local_ip
```

Note: If two RADIUS servers are configured and both servers are up, the validation requests are load-balanced in round-robin sequence within a 20-second period. When one server is up, requests are sent to the active server.

5 Optionally, to disable the two-factor authentication for certain groups, add the following line with the list of group names separated by colons. For example:

```
no2fa groupname1:groupname2:groupname3
```

The users belonging to these LDAP and local groups (`groupname1`, `groupname2`, and `groupname3`) do not have to provide a security code, because strong authentication is disabled for them.

Note: The feature to disable two-factor authentication for selective groups (`no2fa`) is also supported for the LDAP groups on Solaris_Sparc and Solaris_x86 platforms that are configured with Microsoft AD or Oracle LDAP.

6 For proper security this file should have permissions (0600), which are readable by root.

Sample RADIUS Configuration File

The following is an example of the RADIUS configuration file (/etc/raddb/vrsn_otp). The same configurations apply to servers on Linux/Solaris platforms.

```
# vrsn_otp configuration file. Copy to: /etc/raddb/vrsn_otp
#
# For proper security, this file SHOULD have permissions 0600,
# that are readable by root, and NO ONE else. If anyone other than
# root can read this file, then they can spoof responses from
# the server!
#
# There are 4 fields per line in this file. There may be multiple
# lines. Blank lines or lines beginning with '#' are treated as
# comments, and are ignored. The fields are:
#
# server:port camouflagedSecret [timeout] [retries]
#
# If multiple RADIUS server lines exist, they are tried in order.
# The first server to return success or failure causes the module
# to return success or failure. Only if a server fails to respond
# is it skipped, and the next server in turn is used.
#
# RADIUS server and port are required.
# RADIUS sever secret should be the radius server shared secret
```

```
# encrypted with Symantec camouflage tool.
#
# The timeout field controls how many seconds the module waits
# before deciding that the server has failed to respond. This field
# is optional. Default value is 5.
#
# The retries field controls how many times the module tries before
# deciding that the server has failed to respond. This field is
# optional. Default value is 3.
#
# server:port camouflagedSecret [timeout(s)] [retries]
vipeg_server_ip_1:port <camouflaged_password> 5 3
vipeg_server_ip_2:port <camouflaged_password> 5 3
```

The following is an example of the RADIUS configuration file (typically, `/etc/raddb/vrsn_otp`) for HP-UX/AIX:

```
# vrsn_otp configuration file. Copy to: /etc/raddb/vrsn_otp
#
# For proper security, this file SHOULD have permissions 0600,
# that are readable by root, and NO ONE else. If anyone other than
# root can read this file, then they can spoof responses from
# the server!
#
# There are 5 fields per line in this file. The fifth field is optional.
# There may be multiple
# lines. Blank lines or lines beginning with '#' are treated as
# comments, and are ignored. The fields are:
#
# server:port camouflagedSecret [timeout] [retries] [local_ip]
#
# If multiple RADIUS server lines exist, they are tried in order.
# The first server to return success or failure causes the module
# to return success or failure. Only if a server fails to respond
# is it skipped, and the next server in turn is used.
#
# RADIUS server and port are required.
# RADIUS sever secret should be the radius server shared secret
# encrypted with Symantec camouflage tool.
#
# The timeout field controls how many seconds the module waits
# before deciding that the server has failed to respond. This field
# is optional. Default value is 5.
#
# The retries field controls how many times the module tries before
# deciding that the server has failed to respond. This field is
# optional. Default value is 3.
#
# The local_ip field is the IP of local machine from which radius server could be
# reached. This field is optional. If not specified it will pick up Default IP of
# server:port camouflagedSecret [timeout(s)] [retries] [local_ip]

vipeg_server_ip_1:port <camouflaged_password> 5 3 local_ip
```

```
vipeg_server_ip_2:port <camouflaged_password> 5 3 local_ip
```

Client-Server Communications Protocol (Telnet)

On Linux:

Complete the following steps to configure the VIP integration module for PAM to support Telnet log-in service on Linux platforms:

1. Log in as root to the server on the PAM client host machine.
2. Copy the VIP integration module for PAM to /lib/security (on 64-bit Linux, copy to /lib64/security):

   ```
   # cp PAM/linux/pam_vrsn_otp.so /lib/security/
   ```

   You must ensure that the module has executable permission.
3. Copy the files `libvsradiusclientimpl.so` and `libvsauthotpclient.so` (which are included in the PAM package) to a directory in the system path, such as `/lib or /usr/lib`. On 64-bit Linux, copy to a directory in the system path such as `/lib64 or /usr/lib64`).

   ```
   # cp PAM/linux/libvsradiusclientimpl.so /usr/lib/
   # cp PAM/linux/libvsauthotpclient.so /usr/lib/
   ```
4. Verify that the files you copied in the previous step have the same file permissions. You must ensure that the module has executable permission.
5. Create a backup of the appropriate configuration file. For Telnet, back up the configuration file for the service (`/etc/pam.d/remote`).
6. Edit the configuration file to include the VIP integration module for PAM at the top of the PAM stack. For example, modify the entries as follows for Telnet service (on 64-bit Linux, specify `/lib64/security/pam_vrsn_otp.so`):

   ```
   auth       required     /lib/security/pam_vrsn_otp.so prompt=SecurityCode:
   auth       required     pam_securetty.so
   auth       include      system-auth
   account    required     pam_nologin.so
   account    include      system-auth
   password   include      system-auth

   # pam_selinux.so close should be the first session rule

   session    required     pam_selinux.so close
   session    include      system-auth
   session    required     pam_loginuid.so
   session    optional     pam_console.so

   # pam_selinux.so open should only be followed by sessions to be executed in the user
   context

   session    required     pam_selinux.so open
   session    optional     pam_keyinit.so force revoke
   ```

On Solaris:

1. Log in as root to the server on the PAM client host machine.
2. Copy the VIP integration module for PAM to `/usr/lib/security`:

   ```
   # cp PAM/solaris/pam_vrsn_otp.so /usr/lib/security/
   ```

   You must ensure that the module has executable permission.
3. Copy the files `libvsradiusclientimpl.so` and `libvsauthotpclient.so` (which are included in the PAM package) to a directory in the system path, such as `/lib or /usr/lib`.

   ```
   # cp PAM/solaris/libvsradiusclientimpl.so /usr/lib/
   # cp PAM/solaris/libvsauthotpclient.so /usr/lib/
   ```
4. Verify that the files you copied in the previous step have the same file permissions. You must ensure that the module has executable permission.
5. Create a backup of the common PAM configuration file (`/etc/pam.conf`).
6. Edit the configuration file to include the VIP integration module for PAM at the top of the PAM stack. For example, modify the entries as follows for Telnet service.

   ```
   telnet  auth       requisite  pam_vrsn_otp.so split_password
   telnet  auth       required   pam_authtok_get.so.1
   telnet  auth       required   pam_unix_cred.so.1
   telnet  auth       required   pam_unix_auth.so.1 try_first_pass
   telnet  account    required   pam_unix_account.so.1
   telnet  password   required   pam_passwd_auth.so.1
   telnet  session    required   pam_unix_session.so.1
   ```

   Sample PAM stack for LDAP user (Assumption: LDAP server is running on Microsoft AD):

   ```
   telnet   auth      requisite  pam_vrsn_otp.so split_password
   telnet   auth      required   pam_authtok_get.so.1
   telnet   auth      required   pam_unix_cred.so.1
   telnet   auth      sufficient pam_krb5.so.1
   telnet   auth      required   pam_unix_auth.so.1 try_first_pass
   telnet   account   required   pam_unix_account.so.1
   telnet   password  required   pam_passwd_auth.so.1
   telnet   session   required   pam_unix_session.so.1
   ```

   Sample PAM stack for LDAP user (Assumption: LDAP server is running on Oracle LDAP):

   ```
   telnet    auth     requisite   pam_vrsn_otp.so split_password
   telnet    auth     required    pam_authtok_get.so.1
   telnet    auth     required    pam_unix_cred.so.1
   telnet    auth     sufficient  pam_unix_auth.so.1 try_first_pass
   telnet    auth     required    pam_ldap.so.1
   ```

```
telnet    account    required    pam_unix_account.so.1

telnet    password   required    pam_passwd_auth.so.1

telnet    session    required    pam_unix_session.so.1
```

Note: The first line in this example configures VIP Integration module for PAM. The remaining lines may vary depending on the user system's configuration.

If there are no entries for telnet in `/etc/pam.conf`, you can add VIP integration module to other stack as follows:

```
other    auth      requisite    pam_vrsn_otp.so
```

However, this will authenticate telnet along with services not listed in the `pam.conf` file (sshd, ftp, etc).

It is recommended to configure separate stack for each service.

Client-Server Communications Protocol (FTP)

On Linux:

Complete the following steps to configure the VIP integration module for PAM to support FTP service on Linux platforms.

1. Complete the steps 1 through 4 as described for Linux in the Client-Server Communications Protocol (Telnet) section.
2. Create a backup of the appropriate configuration file. For FTP, back up the configuration file for the service (`/etc/pam.d/vsftpd`).
3. Edit the configuration file to include the VIP integration module for PAM at the top of the PAM stack. For example, modify the entries as follows to specify split password for FTP service (on 64-bit Linux, specify the path as `/lib64/security/pam_vrsn_otp.so`):

```
auth        required     /lib/security/pam_vrsn_otp.so split_password
session     optional     pam_keyinit.soforce revoke
auth        required     pam_listfile.so item=user sense=deny
                         file=/etc/vsftpd/ftpusers onerr=succeed
auth        required     pam_shells.so
auth        include      system-auth
account     include      system-auth
session     include      system-auth
session     required     pam_loginuid.so
```

On Solaris:

Complete the following steps to configure the VIP integration module for PAM to support FTP service on Solaris platforms:

1. Complete the steps 1 through 5 as described for Solaris in Client-Server Communications Protocol (Telnet).
2. Edit the configuration file to include the VIP integration module for PAM at the top of the PAM stack. For example, modify the entries as follows to specify split password for the FTP service:

```
ftp     auth      requisite   pam_vrsn_otp.so split_password
ftp     auth      required    pam_authtok_get.so.1
```

```
ftp     auth      required    pam_unix_auth.so.1 try_first_pass
ftp     account   required    pam_unix_account.so.1
ftp     password  required    pam_passwd_auth.so.1
ftp     session   required    pam_unix_session.so.1
```

Sample PAM stack for LDAP user (Assumption: LDAP server is running on a Microsoft AD):

```
ftp      auth      requisite   pam_vrsn_otp.so split_password
ftp      auth      required    pam_authtok_get.so.1
ftp      auth      sufficient  pam_krb5.so.1
ftp      auth      required    pam_unix_auth.so.1 try_first_pass
ftp      account   required    pam_unix_account.so.1
ftp      password  required    pam_passwd_auth.so.1
ftp      session   required    pam_unix_session.so.1
```

Sample PAM stack for LDAP user (Assumption: LDAP server is running on Oracle LDAP):

```
ftp      auth      requisite    pam_vrsn_otp.so split_password
ftp      auth      required     pam_authtok_get.so.1
ftp      auth      required     pam_dhkeys.so.1
ftp      auth      required     pam_unix_cred.so.1
ftp      auth      sufficient   pam_unix_auth.so.1 try_first_pass
ftp      auth      required     pam_ldap.so.1
```

Note: The first line in this example configures VIP Integration module for PAM. The remaining lines may vary depending on the user's system configuration.

If there are no entries for ftp in `/etc/pam.conf`, you can add VIP integration module to other stack as follows:

```
other    auth      requisite    pam_vrsn_otp.so
```

However, this will authenticate ftp along with services not listed in the pam.conf file (telnet, sshd, etc).

It is recommended that you configure a separate stack for each service.

Secure Shell Connections (OpenSSH)

On Linux:

Complete the following steps to configure the VIP integration module for PAM to support OpenSSH connections on Linux platforms:

1. Complete steps 1 through 4 as described for Linux Client-Server Communications Protocol (Telnet).
2. Create a backup of the appropriate configuration file. For OpenSSH, back up the configuration file for the service (`/etc/pam.d/sshd`).
3. Edit the configuration file to include the VIP integration module for PAM at the top of the PAM stack. For example, modify the entries as follows to specify split password for OpenSSH (on 64-bit Linux, specify the path as `/lib64/security/pam_vrsn_otp.so`):

```
auth        required     /lib/security/pam_vrsn_otp.so split_password
auth        include      system-auth
account     required     pam_nologin.so
account     include      system-auth
password    include      system-auth
session     optional     pam_keyinit.so force revoke
session     include      system-auth
session     required     pam_loginuid.so
```

4 Create a backup of the OpenSSH configuration file `/etc/ssh/sshd_config`. Edit the configuration file to make the following changes:

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
UsePAM yes
UsePrivilegeSeparation yes
```

5 Restart the SSH daemon after you make the changes.

On Solaris:

Note: If you want to download the source files from the OpenSSH website to install OpenSSH, you must use the `--with-pam` option with the `./configure` command.

Usage:

```
# ./configure --with-pam
```

Complete the following steps to configure the VIP integration module for PAM to support OpenSSH connections on Solaris platforms.

1 Complete steps 1 through 5 as described for Solaris in Client-Server Communications Protocol (Telnet).

2 Edit the configuration file to include the VIP integration module for PAM at the top of the PAM stack. For example, modify the entries as follows to specify split password for OpenSSH:

```
sshd    auth      requisite   pam_vrsn_otp.so split_password
sshd    auth      required    pam_authtok_get.so.1
sshd    auth      required    pam_unix_auth.so.1 try_first_pass
sshd    account   required    pam_unix_account.so.1
sshd    password  required    pam_passwd_auth.so.1
sshd    session   required    pam_unix_session.so.1
```

Sample PAM stack for LDAP user (Assumption: LDAP server is running on Microsoft AD):

```
sshd    auth      requisite   pam_vrsn_otp.so split_password
sshd    auth      required    pam_authtok_get.so.1
sshd    auth      sufficient  pam_krb5.so.1
```

```
sshd    auth      required    pam_unix_auth.so.1 try_first_pass
sshd    account   required    pam_unix_account.so.1
sshd    password  required    pam_passwd_auth.so.1
sshd    session   required    pam_unix_session.so.1
```

Sample PAM stack for LDAP user (Assumption: LDAP server is running on Oracle LDAP):

```
sshd    auth      requisite   pam_vrsn_otp.so split_password
sshd    auth      required    pam_authtok_get.so.1
sshd    auth      sufficient  pam_unix_auth.so.1 try_first_pass
sshd    auth      required    pam_ldap.so.1
sshd    account   required    pam_unix_account.so.1
sshd    password  required    pam_passwd_auth.so.1
sshd    session   required    pam_unix_session.so.1
```

Note: The first line in this example configures the VIP Integration module for PAM. The remaining lines may vary depending on the user's system configuration.

If there are no entries for sshd in `/etc/pam.conf`, you can add VIP integration module to the other stack as follows:

```
other    auth      requisite    pam_vrsn_otp.so
```

However, this will authenticate sshd along with services not listed in the `pam.conf` file (telnet, ftp, etc).

It is recommended that you configure a separate stack for each service.

3 Create a backup of the OpenSSH configuration file `sshd_config` available at `/etc/ssh` or at your defined install location. Edit the configuration file to make the following changes:

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
UsePAM yes
UsePrivilegeSeparation yes
```

Additionally, add the following line to disable authentication using Public Key:

```
PubKeyAuthentication no
```

4 Restart the OpenSSH daemon after you make the changes.

On HP-UX:

Complete the following steps to configure the VIP integration module for PAM to support OpenSSH connections on HP-UX platforms.

1 Log in as root to the server on the PAM client host machine.

2 Copy the VIP integration module for PAM to /usr/lib/security:

```
# cp PAM/hpux/libpam_vrsn_otp.sl /usr/lib/security/
```

You must ensure that the module has executable permission.

3 Copy the files libvsradiusclientimpl.sl and libvsauthotpclient.sl (which are included in the PAM package) to a directory in the system path, such as `/usr/lib`.

```
# cp PAM/hpux/libvsradiusclientimpl.sl /usr/lib/
# cp PAM/hpux/libvsauthotpclient.sl /usr/lib/
```

4 Verify that the files you copied in the previous step have the same file permissions (that is, executable permissions) as the rest of the files in that location.

5 Create a backup of the common PAM configuration file (`/etc/pam.conf`).

6 Edit the configuration file to include the VIP integration module for PAM at the top of the PAM stack. For example, modify the entries as follows for OpenSSH:

```
sshd    auth      requisite   libpam_hpsec.so.1
sshd    auth      required    libpam_unix.so.1
sshd    auth      requisite   /usr/lib/security/libpam_vrsn_otp.sl
sshd    account   required    libpam_hpsec.so.1
sshd    account   required    libpam_unix.so.1
sshd    password  required    libpam_hpsec.so.1
sshd    password  required    libpam_unix.so.1
sshd    session   required    libpam_hpsec.so.1
sshd    session   required    libpam_unix.so.1
```

7 Create a backup of the OpenSSH configuration file `/etc/ssh/sshd_config`. Edit the configuration file to make the following changes:

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
UsePAM yes
UsePrivilegeSeparation yes
```

8 Stop the SSH daemon.

9 Enable shared library dynamic path search for SSH daemon.

```
#chatr +s enable /usr/bin/sshd
```

10 Ensure SHLIB_PATH includes `/usr/lib/security/ and /usr/lib`

```
#export SHLIB_PATH=$SHLIB_PATH:/usr/lib/security/:/usr/lib
```

11 Start the SSH daemon after you make the changes.

On AIX:

Before you configure the VIP integration module for PAM to support OpenSSH connections on AIX platforms, you must configure the SSH daemon to use PAM on AIX platforms.

Note: If the SSH daemon is already configured to use PAM, you can ignore Part 1: Configure the SSH Daemon to Use PAM on AIX Platforms in the following procedure.

Part 1: Configure the SSH Daemon to Use PAM on AIX Platforms

Complete the following steps to configure the SSH daemon to use PAM on AIX platforms:

1 Edit the PAM configuration file (`/etc/pam.conf`) to add the SSH PAM authentication. For example, modify the entries as follows:

```
sshd    auth      required    pam_aix
sshd    account   required    pam_aix
sshd    password  required    pam_aix
sshd    session   required    pam_aix
```

2 Edit the `/lib/security/methods.cfg` file by adding the following lines:

```
PAM:
    program = /usr/lib/security/PAM
PAMfiles:
    options = auth=PAM,db=BUILTIN
```

3 Edit the `/etc/security/login.cfg` file to configure the authentication type to PAM.

```
auth_type=PAM_AUTH
```

4 Enable SSH PAM authentication by editing the following parameters in the `/etc/ssh/sshd` configuration file:

```
UsePAM yes
```

5 Restart the SSH daemon.

Part 2: Configure the VIP Integration Module for PAM to Support OpenSSH Connections on AIX Platforms

Complete the following steps to configure VIP integration module for PAM to support OpenSSH connections on AIX platforms:

1 Log in as root to the server on the PAM client host machine.

2 Copy the VIP integration module for PAM to `/usr/lib/security`:

```
# cp PAM/aix/libpam_vrsn_otp.so /usr/lib/security/
```

You must ensure that the module has executable permission.

3 Copy the files libvsradiusclientimpl.so and libvsauthotpclient.so (which are included in the PAM package) to a directory in the system path, such as `/usr/lib`.

```
# cp PAM/aix/libvsradiusclientimpl.so /usr/lib/
# cp PAM/aix/libvsauthotpclient.so /usr/lib/
```

4 Verify that the files you copied in the previous step have the same file permissions (that is, executable permissions) as the rest of the files in that location.

5 Create a backup of the common PAM configuration file (`/etc/pam.conf`).

6 Edit the configuration file to include the VIP integration module for PAM at the top of the PAM stack. For example, modify the entries as follows for OpenSSH:

```
sshd    auth      required   pam_aix
sshd    auth      required   /usr/lib/security/libpam_vrsn_otp.so
sshd    account   required   pam_aix
sshd    password  required   pam_aix
sshd    session   required   pam_aix
```

7 Create a backup of the OpenSSH configuration file `/etc/ssh/sshd_config`. Edit the configuration file to make the following changes:

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
UsePAM yes
UsePrivilegeSeparation yes
```

8 Restart the SSH daemon.

Secure Shell Connections (SunSSH)

On Solaris:

Complete the following steps to configure the VIP integration module for PAM to support SunSSH connections on Solaris platforms.

1 Complete steps 1 through 5 as described for Solaris in Client-Server Communications Protocol (Telnet).

2 Edit the configuration file to include the VIP integration module for PAM at the top of the PAM stack. For example, modify the entries as follows to specify split password for SunSSH:

Sample PAM stack for local user:

```
sshd-kbdint   auth       requisite   pam_vrsn_otp.so split_password
sshd-kbdint   auth       required    pam_authtok_get.so.1
sshd-kbdint   auth       required    pam_dhkeys.so.1
sshd-kbdint   auth       required    pam_unix_cred.so.1
sshd-kbdint   auth       required    pam_unix_auth.so.1
```

Sample PAM stack for LDAP user (Assumption: LDAP server is running on Microsoft AD):

```
sshd-kbdint   auth     requisite    pam_vrsn_otp.so split_password
sshd-kbdint   auth     required     pam_authtok_get.so.1
sshd-kbdint   auth     required     pam_dhkeys.so.1
sshd-kbdint   auth     required     pam_unix_cred.so.1
sshd-kbdint   auth     sufficient   pam_krb5.so.1
sshd-kbdint   auth     required     pam_unix_auth.so.1 try_first_pass
```

Sample PAM stack for LDAP user (Assumption: LDAP server is running on Oracle LDAP):

```
sshd-kbdint   auth     requisite    pam_vrsn_otp.so split_password
sshd-kbdint   auth     required     pam_authtok_get.so.1
sshd-kbdint   auth     required     pam_dhkeys.so.1
sshd-kbdint   auth     required     pam_unix_cred.so.1
sshd-kbdint   auth     sufficient   pam_unix_auth.so.1 try_first_pass
sshd-kbdint   auth     required     pam_ldap.so.1
```

Note: The first line in this example configures VIP Integration module for PAM. The remaining lines may vary depending on the user's system configuration.

If there are no entries for `sshd-kbdint`, you can add VIP integration module to the other stack as follows:

```
other    auth       requisite    pam_vrsn_otp.so
```

However, this will authenticate sshd-kbdint along with services not listed in the `pam.conf` file (telnet, ftp, etc).

It is recommended that you configure a separate stack for each service.

3 In the SunSSH configuration file `/etc/ssh/sshd_config`, make sure that the following option is set:

```
PAMAuthenticationViaKBDInt yes
```

Additionally, add the following line to disable authentication using Public Key:

```
PubKeyAuthentication no
```

4 If there is a change to the configuration file, restart the SSH daemon.

Client-Server Communications Protocol (SFTP)

On HP-UX:

Complete the steps as described for HP-UX in Secure Shell Connections (OpenSSH) to configure the VIP integration module for PAM to support SFTP service on HP-UX platforms.

On AIX:

Complete the steps as described for AIX in Secure Shell Connections (OpenSSH) to configure the VIP integration module for PAM to support SFTP service on AIX platforms.

Advanced Configuration of PAM Files

You can use PAM flags to change the default configuration. Table 1 provides available flags and their descriptions.

Table 2-1 PAM Flags

Field	Description
split_password	If specified, the VIP integration module for PAM retrieves the last six characters of a user's password and sends them to the Validation Service. If the validation is successful, the VIP integration module for PAM removes the last 6 characters from the password and sends the rest of the password field to the next PAM module. In a typical configuration, users enter their password + security code at the password prompt. For FTP, the VIP integration module for PAM requires that the split_password be specified if the VIP integration module for PAM is stacked with other authentication modules. **Note:** This flag is not supported on the HP-UX and the AIX platforms.
debug	If specified, the VIP integration module for PAM writes more information into the syslog file.
conf=<filename>	If this is not specified, the VIP integration module for PAM gets the Validation Service parameters from the default location, `/etc/raddb/vrsn_otp`. If specified, the VIP integration module for PAM reads the Validation Service parameters from the specified configuration file. No spaces are allowed in this flag.
prompt=<prompt_string>	If the prompt_string is not specified, users are prompted with **Password + Security Code** if the split_password is specified and with **Security Code** if the split_password is not specified. You can customize this prompt. No spaces are allowed in this flag. If you integrate the VIP integration module for PAM with FTP, you do not get the customized prompt.

Note: The VIP integration module for PAM returns PAM_IGNORE for the user root.

Test an End User

Client-Server Communications Protocol (Telnet) (on Linux)

Go to a client host and start a telnet to the PAM client host:

```
# telnet pam_client_host
Trying pam_client_host...
Connected to pam_client_host
Escape character is '^]'.
Red Hat Enterprise Linux Server release 5.3 (Tikanga)
Kernel 2.6.18-128.el5 on an i686
login: pamtestuser
SecurityCode:
Password:
[pamtestuser@ pam_client_host ~]$
[pamtestuser@ pam_client_host ~]$ logout
Connection closed by foreign host.
```

Client-Server Communications Protocol (FTP) (on Linux)

Go to a client host and try to start an FTP connection to the PAM client host:

```
# ftp pam_client_host
Connected to pam_client_host.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
Name (pam_client_host:root): pamtestuser
331 Please specify the password.
Password: ← Enter <password><security_code>
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> bye
221 Goodbye.
```

Secure Shell Connections (OpenSSH) (on Linux)

Go to a client host and start the Secure Shell connection to the PAM client host:

```
# ssh -l pamtestuser pam_client_host
Password+SecurityCode:
[pamtestuser@pam_client_host ~]$
[pamtestuser@pam_client_host ~]$ logout
Connection to pam_client_host closed
```

Client-Server Communications Protocol (Telnet) (on Solaris 10)

Go to a client host and start the telnet to the PAM client host:

```
bash-3.00$ telnet -l pamtestuser pam_client_host
Trying pam_client_host...
Connected to pam_client_host.
Escape character is '^]'.
Password+SecurityCode:
Oracle Corporation SunOS 5.10 Generic January 2005
$
$
$ Connection to pam_client_host closed by foreign host.
```

Client-Server Communications Protocol (FTP) (on Solaris 10)

Go to a client host and start an FTP connection to the PAM client host:

```
bash-3.00$ ftp pam_client_host
Connected to pam_client_host.
Name (pam_client_host:user): pamtestuser
331 Password required for pamtestuser.
Password:<- Enter <password><security_code>
230 User pamtestuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp>
ftp> quit
221 Goodbye.
```

Secure Shell Connections (OpenSSH) (on Solaris 10)

Go to a client host and start the Secure Shell connections to the PAM client host:

```
bash-3.00$ ssh pamtestuser@pam_client_host
Password+SecurityCode:
Oracle Corporation SunOS 5.10 Generic January 2005
$
$
$
$ Connection to pam_client_host closed.
```

Secure Shell Connections (SunSSH) (on Solaris 10)

Go to a client host and start the Secure Shell connection to the PAM client host:

```
bash-3.00$ ssh pamtestuser@pam_client_host
Password+SecurityCode:
Oracle Corporation SunOS 5.10 Generic January 2005
$
$
$ Connection to pam_client_host closed.
```

Secure Shell Connections (OpenSSH) (on HP-UX)

Go to a client host and start the Secure Shell connection to the PAM client host:

```
bash-4.2$ ssh pamtestuser@pam_client_host
Password:
SecurityCode:
$
$
$
$ Connection to pam_client_host closed.
```

Client-Server Communications Protocol (SFTP) (on HP-UX 11.31)

Go to a client host and try to start an SFTP connection to the PAM client host:

```
bash-4.2$ sftp pamtestuser@pam_client_host
Password:
SecurityCode:
sftp>
sftp>
sftp> quit
221 Goodbye.
```

Secure Shell Connections (OpenSSH) (on AIX)

Go to a client host and start the Secure Shell connection to the PAM client host:

```
bash-4.2$ ssh pamtestuser@pam_client_host
Password: SecurityCode:
$
$
$
$ Connection to pam_client_host closed.
```

Client-Server Communications Protocol (SFTP) (on AIX 6.1)

Go to a client host and try to start an SFTP connection to the PAM client host:

```
BASH-4.2$ SFTP PAMTESTUSER@PAM_CLIENT_HOST
PASSWORD:
SECURITYCODE:
SFTP>
SFTP>
SFTP> QUIT
221 GOODBYE.
```