Symantec VIP Integration Guide for Pluggable Authentication Modules
Table of Contents

About integrating Pluggable Authentication Modules with Symantec VIP ........................................ 4
  System requirements....................................................................................................................................... 4
  VIP supported features.................................................................................................................................... 5
  Supported protocols....................................................................................................................................... 6
  Authentication method................................................................................................................................. 6
  Integration overview...................................................................................................................................... 8

Configuring the VIP integration module for second-factor authentication...................................... 9
  Prerequisites.................................................................................................................................................. 9
  Adding a Validation server............................................................................................................................ 9

Preparing to integration PAM with VIP.............................................................................................. 10
  Configuring RADIUS configuration file....................................................................................................... 10
  Advanced configuration of PAM Files............................................................................................................. 12

Configuring PAM for use with Linux, CentOS, and Ubuntu............................................................... 13
  Prerequisites................................................................................................................................................. 13
  Client-Server Communications Protocol (Telnet)......................................................................................... 14
  Client-Server Communications Protocol (FTP).......................................................................................... 15
  Secure Shell Connections (OpenSSH/SFTP)............................................................................................... 16
  Testing the integration for Linux, CentOS, and Ubuntu.............................................................................. 17
    Client-Server Communications Protocol (Telnet)...................................................................................... 17
    Client-Server Communications Protocol (FTP)........................................................................................ 18
    Secure Shell Connections (OpenSSH)...................................................................................................... 18
    Secure FTP (SFTP)..................................................................................................................................... 18

Configuring PAM for use with Solaris............................................................................................ 19
  Prerequisites................................................................................................................................................. 19
  Client-Server Communications Protocol (Telnet)......................................................................................... 20
  Client-Server Communications Protocol (FTP).......................................................................................... 20
  Secure Shell Connections (OpenSSH)........................................................................................................ 21
  Secure Shell Connections (SunSSH)........................................................................................................... 22
  Testing the integration for Solaris................................................................................................................ 23
    Client-Server Communications Protocol (Telnet) on Solaris 10.............................................................. 24
    Client-Server Communications Protocol (FTP) on Solaris 10................................................................. 24
    Secure Shell Connections (OpenSSH) on Solaris 10.............................................................................. 24
    Secure Shell Connections (SunSSH) on Solaris 10................................................................................ 24

Configuring PAM for use with HP-UX (32-bit)................................................................................. 25
  Prerequisites................................................................................................................................................. 25
  Configuring Secure Shell Connections (OpenSSH).................................................................................... 25
Configuring Client-Server Communications Protocol (SFTP) ................................................................. 26
Testing the integration for HP-UX ................................................................................................................... 27
  Secure Shell Connections (OpenSSH) (on HP-UX) .................................................................................. 27
  Client-Server Communications Protocol (SFTP) (on HP-UX 11.31) ......................................................... 27
  Configuring PAM for use with HP-UX (64-bit) .......................................................................................... 28
    Installing HP-UX for PAM .............................................................................................................. 28
  Testing the integration for HP-UX using the Client-Server Communications Protocol (FTP) protocol ......... 29
    User ID–LDAP Password–Security Code authentication method .............................................................. 29
Configuring PAM for use with AIX .............................................................................................................. 32
  Prerequisites .............................................................................................................................................. 32
  Secure Shell Connections (OpenSSH) .......................................................................................................... 32
    Task 1: Configure the SSH Daemon to use PAM on AIX Platforms .......................................................... 33
    Task 2: Configure the VIP integration module for PAM to support OpenSSH connections on AIX Platforms ......................................................................................................................... 33
  Client-Server Communications Protocol (SFTP) ........................................................................................ 34
  Testing the integration for AIX .................................................................................................................... 34
    Secure Shell Connections (OpenSSH) (on AIX) ..................................................................................... 34
    Client-Server Communications Protocol (SFTP) (on AIX) ..................................................................... 34
Copyright Statement .................................................................................................................................. 35
About integrating Pluggable Authentication Modules with Symantec VIP

The traditional user name and password authentication are no longer enough to meet today's evolving security threats and regulatory requirements. However, users demand an easy-to-use authentication solution. What is needed today is stronger and smarter authentication to secure corporate data and applications, while offering greater ease of use.

Symantec VIP is a cloud-based authentication service that enables enterprises to securely access online transactions, meet compliance standards, and reduce fraud risk. VIP provides an additional layer of protection beyond the standard user name and password through a wide variety of additional authentication capabilities including:

- **Two-factor authentication** – dynamic, one-time-use security codes generated by a user's VIP credential in the form of mobile apps, desktop software, security tokens, and security cards.
- **Out-of-band authentication** – dynamic, one-time-use security codes delivered by phone call, by SMS text message or email, or by push notifications sent to a registered mobile device.

VIP is based on OATH open standards, an industry-wide consortium working with other groups to promote widespread strong authentication. Because Symantec hosts the service, enterprises engage one solution to support multiple enterprise, partner, and customer-facing applications that require strong authentication. Intended for administrators, this guide helps you prepare for VIP integration by providing a comprehensive outline for planning, decision making, and task prioritization for a successful deployment.

Users generate a security code on a VIP credential that they register with Symantec's VIP Service. They use that security code, along with their user name and password, to gain access to the resources that are protected by Pluggable Authentication Modules (PAM).

**System requirements**

The integration environment used in this document is based on the following software:

**Table 1: System requirements**

<table>
<thead>
<tr>
<th>Product/Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Partner Name</strong></td>
<td>• Red Hat</td>
</tr>
<tr>
<td></td>
<td>• Oracle</td>
</tr>
<tr>
<td></td>
<td>• Hewlett-Packard</td>
</tr>
<tr>
<td></td>
<td>• IBM</td>
</tr>
<tr>
<td></td>
<td>• Ubuntu</td>
</tr>
<tr>
<td><strong>Authentication Methods Supported</strong></td>
<td>• User ID - Security Code</td>
</tr>
<tr>
<td></td>
<td>• User ID - Password - Security Code (supported only for HP-UX 64-bit)</td>
</tr>
<tr>
<td>Product/Platform</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Supported Operating System</td>
<td>• Red Hat Enterprise Linux 5.3 (32/64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Red Hat Enterprise Linux 6.2/6.3 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Solaris 10 (Sparc/x86) (32-bit)</td>
</tr>
<tr>
<td></td>
<td>• HP-UX (32-bit)</td>
</tr>
<tr>
<td></td>
<td>• HP-UX (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• AIX 5.x POWER5 (32-bit)</td>
</tr>
<tr>
<td></td>
<td>• AIX 7.1 POWER5 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• CentOS 7.x (32-bit)</td>
</tr>
<tr>
<td></td>
<td>• CentOS 7.2/7.3 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Ubuntu Server 16.04 (32/64-bit)</td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>• Telnet 0.17-39 (Linux)</td>
</tr>
<tr>
<td></td>
<td>• Telnet 11.10.0 (Solaris Sparc/x86)</td>
</tr>
<tr>
<td></td>
<td>• FTP 2.0.5-12 (Linux)</td>
</tr>
<tr>
<td></td>
<td>• FTP 2.6.2 (Solaris Sparc/x86)</td>
</tr>
<tr>
<td></td>
<td>• OpenSSH 4.3p2-29 (Linux)</td>
</tr>
<tr>
<td></td>
<td>• OpenSSH 6.2p2 (Solaris Sparc/x86)</td>
</tr>
<tr>
<td></td>
<td>• OpenSSH 7.2p2 (Ubuntu)</td>
</tr>
<tr>
<td></td>
<td>• SunSSH 1.1.6 (Solaris Sparc/x86)</td>
</tr>
<tr>
<td></td>
<td>• SFTP (HP-UX)</td>
</tr>
<tr>
<td></td>
<td>• SFTP (AIX)</td>
</tr>
<tr>
<td></td>
<td>• SFTP (Ubuntu)</td>
</tr>
</tbody>
</table>

**NOTE**

You must run SUNWlibC patch 119964-24 or higher (for Solaris x86).

**VIP supported features**

VIP supported features lists the VIP Enterprise Gateway features that are supported with Pluggable Authentication Modules.

### Table 2: VIP supported features

<table>
<thead>
<tr>
<th>VIP feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First-factor authentication</strong></td>
<td></td>
</tr>
<tr>
<td>AD/LDAP password using VIP Enterprise Gateway</td>
<td>Yes (HP-UX 64-bit only)</td>
</tr>
<tr>
<td>VIP PIN</td>
<td>No</td>
</tr>
<tr>
<td><strong>Second-factor authentication</strong></td>
<td></td>
</tr>
<tr>
<td>VIP Push</td>
<td>No</td>
</tr>
<tr>
<td>SMS</td>
<td>No</td>
</tr>
<tr>
<td>Voice</td>
<td>No</td>
</tr>
<tr>
<td><strong>Selective strong authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Target resource based</td>
<td>No</td>
</tr>
<tr>
<td>End user-based</td>
<td>Yes</td>
</tr>
<tr>
<td>Risk-based</td>
<td>No</td>
</tr>
<tr>
<td><strong>General authentication</strong></td>
<td></td>
</tr>
<tr>
<td>VIP feature</td>
<td>Support</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Multi-domain</td>
<td>No</td>
</tr>
<tr>
<td>Anonymous user name</td>
<td>Yes</td>
</tr>
<tr>
<td>Legacy authentication provider integration (delegation)</td>
<td>No</td>
</tr>
<tr>
<td>AD password reset</td>
<td>No</td>
</tr>
<tr>
<td><strong>Integration method</strong></td>
<td></td>
</tr>
<tr>
<td>VIP JavaScript</td>
<td>No</td>
</tr>
<tr>
<td>VIP Login</td>
<td>No</td>
</tr>
<tr>
<td>SOAP Web Service APIs</td>
<td>No</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Supported protocols

The following are the supported protocols for different platforms:

#### Table 3: Supported protocols

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux/CentOS</td>
<td>Telnet, FTP, OpenSSH</td>
</tr>
<tr>
<td>Solaris</td>
<td>Telnet, FTP, OpenSSH, SunSSH</td>
</tr>
<tr>
<td>HP-UX</td>
<td>OpenSSH, SFTP</td>
</tr>
<tr>
<td>AIX</td>
<td>OpenSSH, SFTP</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>OpenSSH, SFTP</td>
</tr>
</tbody>
</table>

### Authentication method

The following flow diagram illustrates the User ID–Security Code authentication method for PAM using the VIP Authentication Service.
Table 4: Workflow description for PAM using the VIP Authentication Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The user enters a user name, password, and security code on the PAM client host.</td>
</tr>
<tr>
<td>2</td>
<td>The VIP integration module for PAM sends the user name and the security code to VIP Enterprise Gateway for authentication.</td>
</tr>
<tr>
<td>3</td>
<td>As the first part of the two-factor authentication process, the VIP Enterprise Gateway validation server authenticates the user name and the security code with VIP Service. The VIP Service then returns an authentication response to VIP Enterprise Gateway.</td>
</tr>
</tbody>
</table>
Step | Description
--- | ---
4 | VIP Enterprise Gateway returns an Access-Accept Authentication response to the VIP integration module for PAM.
5 | As the second part of the two-factor authentication process, the VIP integration module for PAM sends the user name and the password to a UNIX host. If a UNIX host authenticates the user name and the password, the UNIX host returns group permission details to the VIP integration module for PAM along with the authentication response.
6 | Based on the response from UNIX host, the VIP integration module for PAM allows the user access to the protected resources.

**Integration overview**

Complete the following general tasks to integrate the VIP integration module with PAM. The topics listed provide detailed procedures for each task.

**Table 5: Tasks for configuring the VIP integration module for second-factor authentication**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure the VIP integration module for second-factor authentication.</td>
<td>Prerequisites</td>
</tr>
<tr>
<td>2</td>
<td>Add a Validation server.</td>
<td>Adding a Validation server</td>
</tr>
<tr>
<td>3</td>
<td>Prepare to integrate PAM with the VIP integration module.</td>
<td>Overview of integration preparation</td>
</tr>
</tbody>
</table>
| 4    | Configure PAM for use. | See the appropriate overview topic, based on your operating system:  
  - Overview of configuring PAM for use with Linux, CentOS, and Ubuntu  
  - Overview of configuring PAM for use with Solaris  
  - Overview of configuring PAM for use with HP-UX (32-bit)  
  - Overview of configuring PAM for use with HP-UX (64-bit)  
  - Overview of configuring PAM for use with AIX |
Configuring the VIP integration module for second-factor authentication

Complete the following general tasks to configure the VIP integration module for second-factor authentication.

Table 6: Tasks for configuring the VIP integration module for second-factor authentication

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Complete the prerequisites.</td>
<td>Prerequisites</td>
</tr>
<tr>
<td>2</td>
<td>Add a Validation server.</td>
<td>Adding a Validation server</td>
</tr>
</tbody>
</table>

Prerequisites

- Before you integrate your PAM with Symantec VIP for second-factor authentication, you must make sure that your first-factor authentication is working. You must ensure that the PAM application is configured with local user or LDAP and a user is able to log into the application with a user name and a password.
- Install and configure VIP Enterprise Gateway. For configuration procedures, refer to the VIP Enterprise Gateway Installation and Configuration Guide.

Adding a Validation server

You must complete the following steps to create a Validation server:

1. Log in to VIP Enterprise Gateway and click the Validation tab.
2. Click Add Server. The Add RADIUS Validation server dialog box is displayed.
3. Configure the RADIUS validation parameters:

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td>Select Unix/Linux from the drop-down list.</td>
</tr>
<tr>
<td>Application Name</td>
<td>Select the vendor’s application that you use, Pluggable Authentication Module (PAM).</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>Select the mode that you want to use for first and second-factor authentication: UserID – Security code: In this authentication mode, your User Store such as AD/LDAP validates the first-factor (user name and password). VIP Enterprise Gateway validates the second-factor (user name and security code) with VIP Service. Ensure that your first-factor validation works before selecting this authentication mode.</td>
</tr>
</tbody>
</table>

4. Click Continue. This completes the addition of the Validation server.

   For information on configuring the Validation server details, refer to VIP Enterprise Gateway Installation and Configuration Guide.

   NOTE

   If you are using Enterprise Gateway version 9.7 or earlier, then create the Validation Server in the User Name - Security Code mode.
Preparing to integration PAM with VIP

Complete the following general tasks to prepare to integrate PAM with VIP.

Table 7: Tasks for preparing to integrate PAM with VIP

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure the RADIUS configuration file.</td>
<td>Configuring RADIUS configuration file</td>
</tr>
<tr>
<td>2</td>
<td>(Optional) Configure advanced settings.</td>
<td>Advanced configuration of PAM Files</td>
</tr>
</tbody>
</table>

Configuring RADIUS configuration file

Task 1. Edit the configuration file

1. Create a `vrsn_otp` file under `/etc/raddb` and copy the appropriate sample contents to this file.

   • On Linux, CentOS, Solaris, and Ubuntu:
     
     ```
     # Configure the server, port, password, timeout and retries.
     Radius_server:port camouflagedSecret [timeout] [retries]
     
     # For example,
     #Server1:1812 9aBGbl21xquFeIu1TDLPsrVZ4GmkpNZJqJl7Tmg?GuUg= 5 3
     #Server2:1813 9aBGbl21xquFeIu1TDLPsrVZ4GmkpNZJqJl7Tmg?GuUg= 5 3
     
     # configure no2fa group, user who are all part of this group will be
     # excluded from 2 factor authentication
     #no2fa
     
     # For example
     #no2fa groupname1:groupname2:groupname3
     
     # 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. Remove the bracket.
     
     # 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. Remove the bracket.
     
     # On AIX and HP-UX:
     
     # Configure the server, port, password, timeout, and retries.
     ```
Radius_server:port camouflagedSecret [timeout] [retries] [local_ip]

For example,
#Server1:1812 9aBGbL21xguFeIU1TDLPSrVZ4GmkpNZJqJ1TMg7GuUg= 5 3 local_ip1
#Server2:1813 9aBGbL21xguFeIU1TDLPSrVZ4GmkpNZJqJ1TMg7GuUg= 5 3 local_ip2

#configure no2fa group, user who are all part of this group will be
#excluded from 2 factor authentication

#no2fa

#For example, no2fa groupname1:groupname2:groupname3

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. Remove the bracket.

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. Remove the bracket.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius_server_ip:port</td>
<td>The IP address and the port number of the validation service (RADIUS server) to which the VIP integration module for PAM connects.</td>
</tr>
<tr>
<td>camouflagedSecret</td>
<td>The encrypted version of the RADIUS shared secret obtained in the previous step. Task 2. Run the Camouflage utility</td>
</tr>
<tr>
<td>timeout</td>
<td>The default timeout is 5 (in seconds). The timeout is how long the module waits until deciding that the server has failed to respond.</td>
</tr>
<tr>
<td>retries</td>
<td>The default retry value is 3. 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</td>
</tr>
<tr>
<td>local_ip</td>
<td>The IP address of the local machine from which the RADIUS server is reachable, in case there are multiple NIC on the machine. This field is supported only on HP-UX and AIX.</td>
</tr>
</tbody>
</table>

**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.

2. Optionally, to disable the two-factor authentication for certain local groups, add group name to no2fa. For example,

   no2fa groupname1:groupname2:groupname3
The users belonging to these local groups (groupname1, groupname2, and groupname3) do not have to provide a security code, because strong authentication is disabled for them.

3. Set file permission as 0600 to the vsdn_otp file.

   **Task 2. Run the Camouflage utility**

4. Log in to the PAM server as a root user.

5. Run the camouflage utility (available in the tools.zip file from the VIP Manager Web site).

   **Usage:** camouflage <password>

   For example, # tools/<platform>/camouflage password

   RNq6gi75hp0erLCbB7idaQ==

   Do not enter the following characters in the password: & = " as this will lead to authentication failure.

   Where <platform> is linux, linux_x86-64, solaris, solaris_x86, hpux, or aix.

   **NOTE**

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

6. Copy the encrypted shared secret and paste it in vsrn_otp.

### Advanced configuration of PAM Files

You can use the PAM flags to change the default configuration.

**Table 8: PAM flags**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>split_password</td>
<td>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. <strong>Note:</strong> This flag is not supported on the HP-UX and the AIX platforms.</td>
</tr>
<tr>
<td>debug</td>
<td>If specified, the VIP integration module for PAM writes more information into the syslog file.</td>
</tr>
<tr>
<td>conf=&lt;filename&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>prompt=&lt;prompt_string&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**NOTE**

The VIP integration module for PAM returns PAM_IGNORE for the user root. VIP does not protect the root user.
Configuring PAM for use with Linux, CentOS, and Ubuntu

Complete the following general tasks to configure PAM for use with HP-UX (32-bit).

Table 9: Tasks for configuring PAM for use with Linux, CentOS, and Ubuntu

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Complete the prerequisites.</td>
<td>Prerequisites</td>
</tr>
</tbody>
</table>
| 2    | Configure the protocol. | See the appropriate topic, based on the integration you implement:  
• Client-Server Communications Protocol (Telnet)  
• Client-Server Communications Protocol (FTP)  
• Secure Shell Connections (OpenSSH)  
• Secure FTP (SFTP) |
| 3    | Test the integration | See the appropriate topic, based on the integration you implement:  
• Client-Server Communications Protocol (Telnet)  
• Client-Server Communications Protocol (SFTP) (on HP-UX 11.31) |

Prerequisites

1. Log in to the PAM server as a root user.
2. Copy the following Linux VIP integration modules from linux folder on 32-bit or linux_x86-64 folder on 64-bit downloaded from VIP Manager:
   - pam_vrsn_otp.so
   - libvsradiusclientimpl.so
   - libvsauthotpclient.so
3. Set permission for the files as 755.
4. Move the VIP integration files downloaded in step 2 to the following PAM system path:

<table>
<thead>
<tr>
<th>File type</th>
<th>File location</th>
</tr>
</thead>
</table>
| 32-bit (Linux/CentOS) | # cp pam_vrsn_otp.so /lib/security/  
                         | # cp libvsradiusclientimpl.so /usr/lib/  
                         | # cp libvsauthotpclient.so /usr/lib/   |
| 64-bit (Linux/CentOS) | # cp pam_vrsn_otp.so /lib64/security/  
                         | # cp libvsradiusclientimpl.so /usr/lib64/  
                         | # cp libvsauthotpclient.so /usr/lib64/   |
| 32-bit (Ubuntu)    | # cp pam_vrsn_otp.so /lib/i386-linux-gnu/security  
                         | # cp libvsradiusclientimpl.so /usr/lib/i386-linux-gnu  
                         | # cp libvsauthotpclient.so /usr/lib/i386-linux-gnu  |
Next

Continue with configuring the protocol. See the appropriate topic, based on the protocol you implement:

- Client-Server Communications Protocol (Telnet)
- Client-Server Communications Protocol (FTP)
- Secure Shell Connections (OpenSSH)
- Secure FTP (SFTP)

Client-Server Communications Protocol (Telnet)

1. Complete the prerequisites.

Prerequisites

2. Create a backup of the appropriate configuration file service (/etc/pam.d/remote).

3. Add the following entries to the configuration file:

   On 32-bit,
   
   auth required /lib/security/pam_vrsn_otp.so prompt=SecurityCode:

   On 64-bit,
   
   auth required /lib64/security/pam_vrsn_otp.so prompt=SecurityCode:

   For example, see the sample configuration file.
4. Restart the Telnet service.

**Next**

Continue with testing the integration. See the appropriate topic, based on the protocol you implement:

**Testing the integration for Linux, CentOS, and Ubuntu**

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

1. Complete the prerequisites.

   **Prerequisites**

2. Create a backup of the appropriate configuration file service (/etc/pam.d/vsftpd).

3. Add the following entries to the configuration file:

   On 32-bit,
   ```plaintext
   auth required /lib/security/pam_vrsn_otp.so split_password
   ``

   On 64-bit,
   ```plaintext
   auth required /lib64/security/pam_vrsn_otp.so split_password
   ``

   For example, see the sample configuration file.

<table>
<thead>
<tr>
<th>File type</th>
<th>Configuration file</th>
</tr>
</thead>
</table>
| 32-bit    | auth required /lib/security/pam_vrsn_otp.so  
            | split_password    |
|           | session optional  
            | pam_keyinit.soforce revoke |
|           | auth required pam_listfile.so item-user sense=denyfile=/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 |

| 64-bit    | auth required /lib64/security/pam_vrsn_otp.so  
            | split_password    |
|           | session optional  
            | pam_keyinit.soforce revoke |
|           | auth required pam_listfile.so item-user sense=denyfile=/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 |

4. Restart the FTP service.

**Next**
Continue with testing the integration. See the appropriate topic, based on the protocol you implement:

**Testing the integration for Linux, CentOS, and Ubuntu**

### Secure Shell Connections (OpenSSH/SFTP)

1. Complete the prerequisites.

   **Prerequisites**

2. Create a backup of the appropriate configuration file service (`/etc/pam.d/sshd`).

3. Add the following entries to the configuration file:

   On 32-bit (Linux/CentOS),
   ```
   auth required /lib/security/pam_vrsn_otp.so split_password
   ```

   On 64-bit (Linux/CentOS),
   ```
   auth required /lib64/security/pam_vrsn_otp.so split_password
   ```

   On 32/64-bit (Ubuntu),
   ```
   auth required pam_vrsn_otp.so
   ```

   For example, see the sample configuration file.

---

<table>
<thead>
<tr>
<th>File type</th>
<th>Configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>32-bit (Linux/ CentOS)</strong></td>
<td></td>
</tr>
<tr>
<td>auth required</td>
<td>/lib/security/pam_vrsn_otp.so</td>
</tr>
<tr>
<td>split_password</td>
<td></td>
</tr>
<tr>
<td>auth include</td>
<td>system-auth</td>
</tr>
<tr>
<td>account required</td>
<td>pam_nologin.so</td>
</tr>
<tr>
<td>account include</td>
<td>system-auth</td>
</tr>
<tr>
<td>password include</td>
<td>system-auth</td>
</tr>
<tr>
<td>session optional</td>
<td>pam_keyinit.so force revoke</td>
</tr>
<tr>
<td>session include</td>
<td>system-auth</td>
</tr>
<tr>
<td>session required</td>
<td>pam_loginuid.so</td>
</tr>
<tr>
<td><strong>64-bit (Linux/ CentOS)</strong></td>
<td></td>
</tr>
<tr>
<td>auth required</td>
<td>/lib64/security/pam_vrsn_otp.so</td>
</tr>
<tr>
<td>split_password</td>
<td></td>
</tr>
<tr>
<td>auth include</td>
<td>system-auth</td>
</tr>
<tr>
<td>account required</td>
<td>pam_nologin.so</td>
</tr>
<tr>
<td>account include</td>
<td>system-auth</td>
</tr>
<tr>
<td>password include</td>
<td>system-auth</td>
</tr>
<tr>
<td>session optional</td>
<td>pam_keyinit.so force revoke</td>
</tr>
<tr>
<td>session include</td>
<td>system-auth</td>
</tr>
<tr>
<td>session required</td>
<td>pam_loginuid.so</td>
</tr>
</tbody>
</table>
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 service.

Next

Continue with testing the integration. See the appropriate topic, based on the protocol you implement:

Testing the integration for Linux, CentOS, and Ubuntu

**Testing the integration for Linux, CentOS, and Ubuntu**

See the appropriate procedures to test the integration for Linux, CentOS, and Ubuntu, based on the protocol used:

- Client-Server Communications Protocol (Telnet)
- Client-Server Communications Protocol (FTP)
- Secure Shell Connections (OpenSSH)
- Secure FTP (SFTP)

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

Go to a client host and start a Telnet connection 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 ~]$ logout
```

Connection closed by foreign host.
Client-Server Communications Protocol (FTP)

Go to a client host and 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)

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

For Linux and CentOS:

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

For Ubuntu:

```
root@VM-100498519:/etc/pam.d# ssh -l test_user 192.168.2.100
SecurityCode: 
Password: 
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-28-generic x86_64)
$
```

Secure FTP (SFTP)

For Ubuntu:

```
root@VM-100498519:/etc/pam.d# sftp test_user@192.168.2.100
SecurityCode: 
Password: 
Connected to 192.168.2.100.
sftp> exit
```
Configuring PAM for use with Solaris

Complete the following general tasks to configure PAM for use with Solaris.

Table 10: Tasks for configuring PAM for use with Solaris

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Complete the prerequisites.</td>
<td>Prerequisites</td>
</tr>
</tbody>
</table>
| 2    | Configure the protocol. | See the appropriate topic, based on the integration you implement:  
  - Client-Server Communications Protocol (Telnet)  
  - Client-Server Communications Protocol (FTP)  
  - Secure Shell Connections (OpenSSH)  
  - Secure Shell Connections (SunSSH) |
| 3    | Test the integration | See the appropriate topic, based on the integration you implement:  
  - Client-Server Communications Protocol (Telnet) on Solaris 10  
  - Client-Server Communications Protocol (FTP) on Solaris 10  
  - Secure Shell Connections (OpenSSH) on Solaris 10  
  - Secure Shell Connections (SunSSH) on Solaris 10 |

Prerequisites

1. Log in to the PAM server as a root user.
2. Copy the following Solaris VIP integration modules for **x86** or **SPARC** downloaded from VIP Manager:
   - pam_vrsn_otp.so
   - libvsradiusclientimpl.so
   - libvsauthotpclient.so
3. Set permission for the files as **755**.
4. Move the VIP integration files downloaded from VIP Manager to the following PAM system path:

<table>
<thead>
<tr>
<th>File type</th>
<th>File location</th>
</tr>
</thead>
</table>
| 32-bit    | # cp pam_vrsn_otp.so /usr/lib/security/  
# cp libvsradiusclientimpl.so /usr/lib/  
# cp libvsauthotpclient.so /usr/lib/ |

Next

Continue with configuring the protocol. See the appropriate topic, based on the protocol you implement:

- Client-Server Communications Protocol (Telnet)
- Client-Server Communications Protocol (FTP)
- Secure Shell Connections (OpenSSH)
- Secure Shell Connections (SunSSH)
Client-Server Communications Protocol (Telnet)

1. Complete the prerequisites.

   **Prerequisites**

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

3. Add the following entries to the configuration file:
   
   telnet auth requisite pam_vrsn_otp.so **split_password**

   For example, see the sample configuration file.

<table>
<thead>
<tr>
<th>File type</th>
<th>Configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit</td>
<td>telnet auth requisite pam_vrsn_otp.so</td>
</tr>
<tr>
<td></td>
<td>split_password</td>
</tr>
<tr>
<td></td>
<td>telnet auth required pam_authtok_get.so.1</td>
</tr>
<tr>
<td></td>
<td>telnet auth required pam_unix_cred.so.1</td>
</tr>
<tr>
<td></td>
<td>telnet auth required pam_unix_auth.so.1</td>
</tr>
<tr>
<td></td>
<td>try_first_pass</td>
</tr>
<tr>
<td></td>
<td>telnet account required pam_unix_account.so.1</td>
</tr>
<tr>
<td></td>
<td>telnet password required pam_passwd_auth.so.1</td>
</tr>
<tr>
<td></td>
<td>telnet session required pam_unix_session.so.1</td>
</tr>
</tbody>
</table>

   **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 (such as sshd and ftp). It is recommended to configure separate stack for each service.

4. Restart the Telnet service.

Next

Continue with testing the integration.

Testing the integration for Solaris

Client-Server Communications Protocol (FTP)

1. Complete the prerequisites.

   **Prerequisites**

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

3. Add the following entries to the configuration file:
   
   ftp auth requisite pam_vrsn_otp.so **split_password**
For example, see the sample configuration file.

<table>
<thead>
<tr>
<th>File type</th>
<th>Configuration file</th>
</tr>
</thead>
</table>
| 32-bit    | 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 |

**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.

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

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

However, this will authenticate ftp along with services not listed in the pam.conf file (such as telnet and sshd). It is recommended that you configure a separate stack for each service.

5. Restart the FTP service.

**Next**

Continue with testing the integration.

**Testing the integration for Solaris**

**Secure Shell Connections (OpenSSH)**

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:

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

1. Complete the prerequisites.

   **Prerequisites**

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

3. Add the following entries to the configuration file:

   ```
   sshd auth requisite pam_vrsn_otp.so split_password
   ```
For example, see the sample configuration file.

<table>
<thead>
<tr>
<th>File type</th>
<th>Configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit</td>
<td>sshd auth requisite pam_vrsn_otp.so</td>
</tr>
<tr>
<td></td>
<td>split_password</td>
</tr>
<tr>
<td></td>
<td>sshd auth required pam_authtok_get.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd auth required pam_unix_auth.so.1</td>
</tr>
<tr>
<td></td>
<td>try_first_pass</td>
</tr>
<tr>
<td></td>
<td>sshd account required pam_unix_account.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd password required pam_passwd_auth.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd session required pam_unix_session.so.1</td>
</tr>
</tbody>
</table>

**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 (such as telnet and ftp). It is recommended that you configure a separate stack for each service.

4. 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
```

5. Restart the OpenSSH service.

Next

Continue with testing the integration.

**Testing the integration for Solaris**

**Secure Shell Connections (SunSSH)**

1. Complete the prerequisites.

   **Prerequisites**

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

3. Add the following entries to the configuration file:

   ```
   sshd-kbdint auth requisite pam_vrsn_otp.so split_password
   ```
For example, see the sample configuration file.

### PAM stack

<table>
<thead>
<tr>
<th>Configuration file</th>
</tr>
</thead>
</table>
| 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 a Sun Solaris platform) | 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  
| | server_policy  
| | 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 (such as telnet and ftp). It is recommended that you configure a separate stack for each service.

4. 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

5. Restart the SunSSH service.

### Testing the integration for Solaris

See the appropriate procedures to test the integration for Solaris, based on the protocol used:

- Client-Server Communications Protocol (Telnet) on Solaris 10
- Client-Server Communications Protocol (FTP) on Solaris 10
- Secure Shell Connections (OpenSSH) on Solaris 10
- Secure Shell Connections (SunSSH) on Solaris 10
**Client-Server Communications Protocol (Telnet) on Solaris 10**

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

```bash
bash-3.00$ telnet -l pamtestuser pam_client_host
Trying pam_client_host...
Connected to pam_client_host.
Escape character is '^]'.
Password+SecurityCode:
Sun Microsystems Inc.SunOS 5.10Generic 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
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
bash-3.00$ ssh pamtestuser@pam_client_host
Password+SecurityCode:
Sun Microsystems Inc.SunOS 5.10Generic 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
bash-3.00$ ssh pamtestuser@pam_client_host
Password+SecurityCode:
Sun Microsystems Inc.SunOS 5.10Generic January 2005
$ $ $ Connection to pam_client_host closed.
```
Configuring PAM for use with HP-UX (32-bit)

Complete the following general tasks to configure PAM for use with HP-UX (32-bit).

Table 11: Tasks for configuring PAM for use with HP-UX (32-bit)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Complete the prerequisites.</td>
<td>Prerequisites</td>
</tr>
</tbody>
</table>
| 2    | Configure the protocol. | See the appropriate topic, based on the integration you implement:  
  • Configuring Secure Shell Connections (OpenSSH)  
  • Configuring Client-Server Communications Protocol (SFTP) |
| 3    | Test the integration | See the appropriate topic, based on the integration you implement:  
  • Secure Shell Connections (OpenSSH) (on HP-UX)  
  • Client-Server Communications Protocol (SFTP) (on HP-UX 11.31) |

Prerequisites

1. Log in to the PAM server as a root user.
2. Copy the following HP-UX VIP integration modules downloaded from VIP Manager:
   - libpam_vrsn_otp.sl
   - libvsradiusclientimpl.sl
   - libvsauthotpclient.sl
3. Set permission for the files as 755.
4. Move the VIP integration files downloaded from VIP Manager to the following PAM system path:

<table>
<thead>
<tr>
<th>File type</th>
<th>File location</th>
</tr>
</thead>
</table>
| 32-bit    | # cp libpam_vrsn_otp.sl /usr/lib/security/  
# cp libvsradiusclientimpl.sl /usr/lib/  
# cp libvsauthotpclient.sl /usr/lib/ |

Next

Continue with configuring the protocol. See the appropriate topic, based on the protocol you implement:

• Configuring Secure Shell Connections (OpenSSH)  
• Configuring Client-Server Communications Protocol (SFTP)

Configuring Secure Shell Connections (OpenSSH)

1. Complete the prerequisites.
   Prerequisites
2. Create a backup of the common PAM configuration file (/etc/pam.conf).
3. Add the following entries to the configuration file:
   sshd auth requisite /usr/lib/security/libpam_vrsn_otp.sl
For example, see the sample configuration file.

<table>
<thead>
<tr>
<th>File type</th>
<th>Configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit</td>
<td>sshd auth requisite libpam_hpsec.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd auth required libpam_unix.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd auth requisite /usr/lib/security/</td>
</tr>
<tr>
<td></td>
<td>libpam_vrsn_otp.sl</td>
</tr>
<tr>
<td></td>
<td>sshd account required libpam_hpsec.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd account required libpam_unix.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd password required libpam_hpsec.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd password required libpam_unix.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd session required libpam_hpsec.so.1</td>
</tr>
<tr>
<td></td>
<td>sshd session required libpam_unix.so.1</td>
</tr>
</tbody>
</table>

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. Stop the SSH service.

6. Enable shared library dynamic path search for SSH daemon.

   # chatr +s enable /usr/bin/sshd


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

8. Restart the SSH service.

   Next

Continue with testing the integration. See the appropriate topic, based on the protocol you implement:

- Secure Shell Connections (OpenSSH) (on HP-UX)
- Client-Server Communications Protocol (SFTP) (on HP-UX 11.31)

### Configuring Client-Server Communications Protocol (SFTP)

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.

#### Configuring Secure Shell Connections (OpenSSH)

Next

Continue with testing the integration. See the appropriate topic, based on the protocol you implement:

- Secure Shell Connections (OpenSSH) (on HP-UX)
- Client-Server Communications Protocol (SFTP) (on HP-UX 11.31)
Testing the integration for HP-UX

Test the integration. See the appropriate topic, based on the protocol you implement:

- Secure Shell Connections (OpenSSH) (on HP-UX)
- Client-Server Communications Protocol (SFTP) (on HP-UX 11.31)

**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.
```
Configuring PAM for use with HP-UX (64-bit)

Complete the following general tasks to configure PAM for use with HP-UX (64-bit).

Table 12: Tasks for configuring PAM for use with HP-UX (64-bit)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install HP-UX for PAM.</td>
<td>Installing HP-UX for PAM</td>
</tr>
<tr>
<td>2</td>
<td>Test the integration</td>
<td>Testing the integration for HP-UX using the Client-Server Communications Protocol (FTP) protocol</td>
</tr>
</tbody>
</table>


Installing HP-UX for PAM

1. Log in as super user.
2. Download the HP-UX PAM RADIUS depot file from the following location: https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HP-UX-PAM-RADIUS
3. Move the depot to the /tmp folder.
4. Verify that the depot is downloaded correctly by entering the following command:
   ```
   swlist -d @ /tmp/<depot_name>
   ```
   The following example indicates the 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 HP-UX PAM RADIUS, enter the following command:
   ```
   swlist -s /tmp/<depot_name>\*
   ```
6. To configure HP-UX PAM RADIUS, edit the /etc/pam.conf and comment the existing ftp lines and add the following line:
   ```
   ftp auth required libpam_radius.so.1
   ```
7. Copy the server.sample file to server in the same location /etc/raddb/server/ and update the following values. For example:
   ```
   server[:port]    shared_secret    timeout (s)
   ```
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Enter a server name.</td>
</tr>
<tr>
<td>Port</td>
<td>The port name or port number. The default port name is &quot;radius&quot; and looked up from /etc/services/</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter a shared secret.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The default timeout value in seconds.</td>
</tr>
</tbody>
</table>

**Next**

Continue with testing the protocol.

**Testing the integration for HP-UX using the Client-Server Communications Protocol (FTP) protocol**

**Testing the integration for HP-UX using the Client-Server Communications Protocol (FTP) protocol**

To test the protocol, go to a client host and start an FTP connection to the PAM client host:

```bash
# ftp pam_client_host
Connected to pam_client_host.
220 HP-UX Test FTP Server
Name (pam_client_host:root): pamtestuser
331 Password required for pamtestuser.
Password: < Enter <password><security_code>
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> bye
221 Goodbye.
```

**User ID–LDAP Password–Security Code authentication method**

The following flow diagram illustrates the User ID–LDAP Password–Security Code authentication method for PAM using the VIP Authentication Service.
Table 13: Workflow description for PAM using the VIP Authentication Service

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The user enters a user name, password, and a security code on the browser or plug-in based login screen.</td>
</tr>
<tr>
<td>2</td>
<td>The VIP integration module for PAM device sends the user name, password, and security code to VIP Enterprise Gateway.</td>
</tr>
<tr>
<td>3</td>
<td>As the first part of the two-factor authentication process, the VIP Enterprise Gateway validation server authenticates the user name and password against your User Store. For example, your User Store can be AD/LDAP. If the User Store authenticates the user name and password, the authentication response includes the group permission details.</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>4</td>
<td>As the second part of the two-factor authentication process, VIP Enterprise Gateway authenticates the user name and security code with VIP Service.</td>
</tr>
<tr>
<td>5</td>
<td>If VIP Service successfully authenticates the user name and security code, then VIP Enterprise Gateway returns an Access-Accept Authentication response to the VIP integration module for PAM device.</td>
</tr>
<tr>
<td>6</td>
<td>Based on the Access-Accept Authentication response, the VIP integration module for PAM device gives the user access to the protected resources.</td>
</tr>
</tbody>
</table>
Configuring PAM for use with AIX

Complete the following general tasks to configure PAM for use with AIX

Table 14: Tasks for configuring PAM for use with AIX

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Complete the prerequisites.</td>
<td>Prerequisites</td>
</tr>
<tr>
<td>2</td>
<td>Configure the protocol.</td>
<td>See the appropriate topic, based on the integration you implement: Secure Shell Connections (OpenSSH) Client-Server Communications Protocol (SFTP)</td>
</tr>
<tr>
<td>3</td>
<td>Test the integration</td>
<td>See the appropriate topic, based on the integration you implement: Secure Shell Connections (OpenSSH) (on AIX) Client-Server Communications Protocol (SFTP) (on AIX)</td>
</tr>
</tbody>
</table>

Prerequisites

1. Log in to the PAM server as a root user.
2. Copy the following AIX VIP integration modules downloaded from VIP Manager:
   - libpam_vrsn_otp.so
   - libvsradiusclientimpl.so
   - libvsauthotpclient.so
3. Set permission for directory as 755.
4. Move the VIP integration files downloaded from VIP Manager to the following PAM system path:
   
   ```
   # cp libpam_vrsn_otp.so /usr/lib/security/
   # cp libvsradiusclientimpl.so /usr/lib/
   # cp libvsauthotpclient.so /usr/lib/
   ```

Secure Shell Connections (OpenSSH)

Complete the following general tasks to configure the VIP integration module for PAM to support OpenSSH connections on AIX.

Table 15: Tasks for configuring the VIP integration module for PAM to support OpenSSH connections on AIX

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure the SSH Daemon to use PAM on AIX</td>
<td>Task 1: Configure the SSH Daemon to use PAM on AIX Platforms</td>
</tr>
<tr>
<td>2</td>
<td>Configure the VIP integration module to support OpenSSH connections</td>
<td>Task 2: Configure the VIP integration module for PAM to support OpenSSH connections on AIX Platforms</td>
</tr>
</tbody>
</table>
Task 1: 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_conf configuration file:

   UsePAM yes

5. Restart the SSH service.

Task 2: Configure the VIP integration module for PAM to support OpenSSH connections on AIX Platforms

1. Complete the prerequisites.

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

3. Add the following entries to the configuration file:

   sshd auth required /usr/lib/security/libpam_vrsn_otp.so

   For example, see the sample configuration file.

<table>
<thead>
<tr>
<th>File type</th>
<th>Configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit</td>
<td>sshd auth required pam_aix</td>
</tr>
<tr>
<td></td>
<td>sshd auth required /usr/lib/security/libpam_vrsn_otp.so</td>
</tr>
<tr>
<td></td>
<td>sshd account required pam_aix</td>
</tr>
<tr>
<td></td>
<td>sshd password required pam_aix</td>
</tr>
<tr>
<td></td>
<td>sshd session required pam_aix</td>
</tr>
</tbody>
</table>

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 service.

Next

Continue with testing the integration. See the appropriate topic, based on the protocol you implement:

- Secure Shell Connections (OpenSSH) (on AIX)
- Client-Server Communications Protocol (SFTP) (on AIX)

Client-Server Communications Protocol (SFTP)

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.

Prerequisites

Next

Continue with testing the integration. See the appropriate topic, based on the protocol you implement:

- Secure Shell Connections (OpenSSH) (on AIX)
- Client-Server Communications Protocol (SFTP) (on AIX)

Testing the integration for AIX

Test the integration. See the appropriate topic, based on the protocol you implement:

- Secure Shell Connections (OpenSSH) (on AIX)
- Client-Server Communications Protocol (SFTP) (on AIX)

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)

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.
```
Copyright Statement

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.

Copyright ©2020 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.