Software License Agreement

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE LOADING THE SOFTWARE. BY CLICKING "I ACCEPT" BELOW, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE, YOU ARE SIGNING THIS AGREEMENT, THEREBY BECOMING BOUND BY ITS TERMS. IF YOU DO NOT AGREE WITH THIS AGREEMENT, THEN CLICK "I DO NOT ACCEPT" BELOW AND RETURN ALL COPIES OF THE SOFTWARE AND DOCUMENTATION TO SECURE COMPUTING CORPORATION ("SECURE COMPUTING") OR THE RESELLER FROM WHOM YOU OBTAINED THE SOFTWARE.

If this Software is being installed by a third party (for example, a value-added reseller, consultant, employee, or agent), such third party represents that it has the authority to bind the person or entity for whom the Software is being installed, and that its acceptance of this Agreement in the manner set forth above does bind such person or entity.

1. Grant of License. Secure Computing grants to you, and you accept, a non-exclusive, and non-transferable license (without right to sub-license) to use the Software Products as defined herein.

2. Software Products. "Software Product(s)" means (i) the machine-readable object-code versions of software contained in the media (the "Software"), (ii) the published user manuals and documentation that are made available for the Software (the "Documentation"), and (iii) any updates or revisions of the Software or Documentation that you may receive (the "Update"). Under no circumstances will you receive any source code of the Software. Software Products provided for use as "backup" in the event of failure of a primary unit may be used only to replace the primary unit after a failure in fact occurs. They may not be used to provide any capability in addition to the functioning primary system that they backup.

3. Limitation of Use. You may not: 1) copy, except to make one copy of the Software solely for back-up or archival purposes; 2) transfer, distribute, rent, lease or sublicense all or any portion of the Software Product to any third party; 3) translate, modify, adapt, decompile, disassemble, or reverse engineer any Software Product in whole or in part; or 4) modify or prepare derivative works of the Software Products. You agree to keep confidential and use your best efforts to prevent and protect the contents of the Software Product from unauthorized disclosure or use. Secure Computing reserves all rights that are not expressly granted to you.

4. Limited Warranty and Remedies. Secure Computing warrants that the medium/media on which its Software is recorded is/are free from defects in material and workmanship under normal use and service for a period of ninety (90) days from the date of shipment to you. Secure Computing does not warrant that the functions contained in the Software will meet your requirements or that operation of the program will be uninterrupted or error-free. The Software is furnished "AS IS" and without warranty as to the performance or results you may obtain by using the Software. The entire risk as to the results and performance of the Software is assumed by you. If you do not receive media which is free from defects in materials and workmanship during the 90-day warranty period, you will receive a refund for the amount paid for the Software Product returned.

5. Limitation Of Warranty And Remedies. THE WARRANTIES STATED HEREIN ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES AND COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS WHICH VARY BY STATE OR COUNTRY.
SECURE COMPUTING’S AND ITS LICENSORS ENTIRE LIABILITY UNDER, FOR BREACH OF, OR ARISING OUT OF THIS AGREEMENT, IS LIMITED TO A REFUND OF THE PURCHASE PRICE OF THE PRODUCT OR SERVICE THAT GAVE RISE TO THE CLAIM. IN NO EVENT SHALL SECURE COMPUTING OR ITS LICENSORS BE LIABLE FOR YOUR COST OF PROCURING SUBSTITUTE GOODS. IN NO EVENT WILL SECURE COMPUTING OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR OTHER DAMAGES WHETHER OR NOT SECURE COMPUTING HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

6. **Term and Termination.** This license is effective until terminated. You may terminate it at any time by destroying the Software Product, including all computer programs and documentation, and erasing any copies residing on computer equipment. This Agreement also will automatically terminate if you do not comply with any terms or conditions of this Agreement. Upon such termination you agree to destroy the Software Product and erase all copies residing on computer equipment.

7. **Ownership.** This Software is licensed (not sold) to you. All intellectual property rights including trademarks, service marks, patents, copyrights, trade secrets, and other proprietary rights in or related to the Software Products are and will remain the property of Secure Computing or its licensors, whether or not specifically recognized or protected under local law. You will not remove any product identification, copyright notices, or other legends set forth on the Software Product.

8. **Export Restrictions.** You agree to comply with all applicable United States export control laws and regulations, including without limitation, the laws and regulations administered by the United States Department of Commerce and the United States Department of State.

9. **U.S. Government Rights.** Software Products furnished to the U.S. Government are provided on these commercial terms and conditions as set forth in DFARS 227.7202-1(a).

10. **Entire Agreement.** This Agreement is our offer to license the Software Product to you exclusively on the terms set forth in this Agreement, and is subject to the condition that you accept these terms in their entirety. If you have submitted (or hereafter submit) different, additional, or other alternative terms to Secure Computing or any reseller or authorized dealer, whether through a purchase order or otherwise, we object to and reject those terms. Without limiting the generality of the foregoing, to the extent that you have submitted a purchase order for the Software Product, any shipment to you of the Software Product is not an acceptance of your purchase order, but rather is a counteroffer subject to your acceptance of this Agreement without any objections or modifications by you. To the extent that we are deemed to have formed a contract with you related to the Software Product prior to your acceptance of this Agreement, this Agreement shall govern and shall be deemed to be a modification of any prior terms in their entirety.

11. **General.** Any waiver of or modification to the terms of this Agreement will not be effective unless executed in writing and signed by Secure Computing. If any provision of this Agreement is held to be unenforceable, in whole or in part, such holding shall not affect the validity of the other provisions of this Agreement. You may not assign this License or any associated transactions without the written consent of Secure Computing. This License shall be governed by and construed in accordance with the laws of California, without regard to its conflicts of laws provisions.
Technical Support information

Secure Computing works closely with our Channel Partners to offer worldwide Technical Support services. If you purchased this product through a Secure Computing Channel Partner, please contact your reseller directly for support needs.

To contact Secure Computing Technical Support directly, telephone +1.800.700.8328 or +1.651.628.1500. If you prefer, send an e-mail to support@securecomputing.com. To inquire about obtaining a support contract, refer to our "Contact Secure" Web page for the latest information at www.securecomputing.com.

Customer Advocate information

To suggest enhancements in a product or service, or to request assistance in resolving a problem, please contact a Customer Advocate at +1.877.851.9080. If you prefer, send an e-mail to customer_advocate@securecomputing.com.

If you have comments or suggestions you would like to make regarding this document or any other Secure Computing document, please send an e-mail to techpubs@securecomputing.com.

Printing history

<table>
<thead>
<tr>
<th>Date</th>
<th>Part number</th>
<th>Software Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 2000</td>
<td>86-0933999-A</td>
<td>Pluggable Authentication Module (PAM), Version 1.0</td>
</tr>
<tr>
<td>June 2000</td>
<td>86-0933999-B</td>
<td>Pluggable Authentication Module (PAM), Version 1.0</td>
</tr>
<tr>
<td>February 2001</td>
<td>86-0933999-C</td>
<td>Pluggable Authentication Module (PAM), Version 1.0</td>
</tr>
<tr>
<td>September 2001</td>
<td>86-0933999-D</td>
<td>Pluggable Authentication Module (PAM), Version 1.0</td>
</tr>
<tr>
<td>May 2002</td>
<td>86-0933999-E</td>
<td>Pluggable Authentication Module (PAM), Version 1.1</td>
</tr>
<tr>
<td>September 2004</td>
<td>86-0933999-F</td>
<td>Pluggable Authentication Module (PAM), Version 1.3</td>
</tr>
<tr>
<td>August 2005</td>
<td>86-0933999-G</td>
<td>Pluggable Authentication Module (PAM), Version 1.3</td>
</tr>
</tbody>
</table>
SafeWord PremierAccess Support for PAM

About this document

This document describes the Pluggable Authentication Module (PAM) authenticating agent for Solaris and Linux integration with SafeWord PremierAccess. It is intended for use by the person responsible for administering their organization’s network and its users.

This document contains the following topics:

- “Introducing the SafeWord Agent for PAM” on page 2
- “Operating system requirements” on page 2
- “Installing PAM” on page 2
- “Editing the SafeWord PAM configuration file” on page 7
- “Editing the PAM configuration file” on page 11
- “Excluding users from SafeWord authentication” on page 17
- “Updating your software” on page 17
- “Uninstalling PAM” on page 19

Note: The term “SafeWord” is used as a blanket term that refers to SafeWord PremierAccess throughout this document.
Introducing the SafeWord Agent for PAM

The PAM framework allows applications in need of authentication and other security services to access those services in a generic way. Using PAM, authentication services can be updated without the rewriting of applications to make use of improvements or new technologies.

Operating system requirements

The Agent for PAM is supported on the following operating systems:

- Solaris 9 and 10
- Linux Redhat Enterprise 3.0

Installing PAM

The PAM Agent software is available on the SafeWord PremierAccess Deployment CD which is included in your product box. Before installing the software, you should review the Read Me First, the Known Issues, and the Release Notes included with it.

PAM can be installed on Solaris or Linux platforms in GUI (graphic user interface) mode or in console (text) mode. If you are installing in console (text) mode, refer to "Installing PAM in console (text) mode" on page 5. To install in GUI mode, continue to the next section.

Installing PAM in GUI mode

To install PAM in GUI mode:

1. Insert the PremierAccess Deployment CD in your computer’s disc drive.

2. Change to the CDROM /UNIX/solaris/PAM directory or the CDROM /UNIX/linux/PAM directory depending on the operating system you are using.

3. Run the following command:
   On Solaris: ./setupPAMsolarisSparc.bin
   On Linux: ./setupPAMLinux.bin

   The Install Wizard extracts the files for installation. When complete, the Welcome window appears.

   **Important:** If the installation fails to start and a message displays saying that there is not enough space to extract temporary files, restart the installer and specify the path to a temporary directory. For example: ./setupPAMsolarisSparc.bin -is:tempdir /full/path/to/tempdir where /full/path/to/tempdir is the full path to a directory that already exists. After installation you can remove any temporary directories created by the installer. These will have the name ismp* or istemp*.
4. Click **Next**. The License Agreement window appears.

5. After reviewing the license agreement carefully, click **I Accept the terms of the License Agreement**. You must accept the license agreement to continue with the installation. After making your selection, click **Next**. The Choose Directory window appears.

6. The default destination is `/opt/PremierAccess/pam`. Choose the default, browse to a new installation destination, or enter one in the **Directory Name** field, then click **Next**. The Authentication Server Configuration window appears.
7. Enter the PremierAccess AAA Server host IP address in the Host IP field and enter the port on which it listens in the Port number field, then click Next. The PAM installation summary information appears.

8. Confirm that the summary information is correct, then click Install. When the installation is done, a successful installation message appears.

9. Click Finish to exit the installer.
Installing PAM in console (text) mode

This section provides instructions to install and configure PAM in console (text) mode. If you prefer to install the software in GUI mode, refer to "Installing PAM in GUI mode" on page 2. To install in console (text) mode:

1. Insert the Deployment CD into your computer’s disc drive.

2. Change to the CDROM/UNIX/solaris/PAM directory or the CDROM/UNIX/linux/PAM directory (based on the operating system you are using.

3. Run the following:
   - For Solaris: ./setupPAMSolarisSparc.bin-console
   - For Linux: ./setupPAMLinux.bin-console

4. The Installation Wizard for PAM launches and extracts the installation files. When the extraction is complete, the Welcome window appears.

   **Important:** If the installation fails to start and a message displays saying that there is not enough space to extract temporary files, restart the installer and specify the path to a temporary directory. For example: ./setupPAMSolarisSparc.bin -is:tempdir /full/path/to/tempdir -console

   Where /full/path/to/tempdir is the full path to a directory that already exists. After installation, you can remove any temporary directories created by the installer. These will have the name ismp* or istemp*.

   Since you are installing the agent in console (text) mode, you will be using your keyboard’s numeric keys in place of GUI buttons to proceed through the installation. Table 1 summarizes the numeric keys to use in order to install the agent in console mode.
Table 1. Console (text) mode keyboard commands

<table>
<thead>
<tr>
<th>Press:</th>
<th>To do the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘1’ on your keyboard</td>
<td>to continue to the Next window</td>
</tr>
<tr>
<td>‘2’ on your keyboard</td>
<td>to return to the Previous window</td>
</tr>
<tr>
<td>‘3’ on your keyboard</td>
<td>to Cancel an action</td>
</tr>
<tr>
<td>‘5’ on your keyboard</td>
<td>to Redisplay the current window with the default values populated</td>
</tr>
</tbody>
</table>

**Note:** When you change the values on any fields, those changes become the defaults when you choose the Redisplay option.

5. Press ‘1’ on your keyboard to continue. The PAM License Agreement appears.

6. Review the license agreement, then press “1” on your keyboard to accept the agreement.

   By default, this option is set to not accept the license. If you do not want to accept the agreement, press “0” to finish the procedure. You must accept the license agreement to continue the installation.

7. After accepting the agreement, press “1” to continue. The Choose Directory screen appears.

8. Specify a directory or press the Enter key to accept the default. When your destination is set, press “1” to continue. The Authentication Server Configuration screen appears.

9. Enter the PremierAccess Authentication (AAA) Server host name in the Host Name field, and the port number on which it listens in the Port Number field.

10. After making your choice, press “1” to continue. The Summary Information screen appears.

11. Confirm your settings, then press “1” to continue. The Wizard installs the agent on your computer.

12. When the installation is complete, the Wizard displays a successful installation screen. Press “3” to Finish and exit the Wizard.
SafeWord PAM support allows you to make use of PremierAccess authentication in PAM-compliant applications supplied by Sun and others, such as login and telnet.

**IMPORTANT:** Challenge-response is not supported with the SafeWord Agent for PAM protecting ftp due to limitations of PAM and ftp. The service has no facility for displaying any extra messages, such as a challenge.

`pam_safeword.cfg` is the configuration file for SafeWord support for PAM and contains information that allows the SafeWord client in the module to find the SafeWord daemon, and to set various other authentication parameters. As mentioned earlier in this document, the `pam_safeword.cfg` file must be stored in the `/etc` directory.

The `pam_safeword.cfg` file consists of numbered lines of text; each line of text specifies one parameter. Figure 7 shows the key parameters and settings in a sample `pam_safeword.cfg` file.

**Figure 7. Sample pam_safeword.cfg settings**

<table>
<thead>
<tr>
<th>Parameter Descriptors—A two character ID followed by a space and documentary text</th>
<th>Value/Setting—Controls the behavior of PAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>02 Authen. Server (host weight connects port):</td>
<td>192.168.1.1 0 0 5031</td>
</tr>
<tr>
<td>09 User ID Source (USER/SYSTEM):</td>
<td>SYSTEM</td>
</tr>
<tr>
<td>10 Server’s System Name:</td>
<td>STANDARD</td>
</tr>
<tr>
<td>13 Data file’s dir:</td>
<td>/usr/lib/security</td>
</tr>
<tr>
<td>15 Send Status Messages to User:</td>
<td>ERROR</td>
</tr>
<tr>
<td>16 Send Status Messages to Console:</td>
<td>NONE</td>
</tr>
<tr>
<td>17 Send Status Messages to Log File:</td>
<td>ALL</td>
</tr>
<tr>
<td>18 Status Message Log Filename:</td>
<td>/var/log/pam_safeword.log</td>
</tr>
<tr>
<td>23 Status Message Label:</td>
<td>PAM_Safeword</td>
</tr>
<tr>
<td>27 Client Type:</td>
<td>PAM</td>
</tr>
<tr>
<td>55 Eassp Version:</td>
<td>201</td>
</tr>
<tr>
<td>59 Socket timeout:</td>
<td>25</td>
</tr>
<tr>
<td>1000 Check Pass Action Value (ON/OFF):</td>
<td>OFF</td>
</tr>
</tbody>
</table>
The following list describes the entries in the `pam_safeword.cfg` file.

**02 Authen. Server: 192.168.1.1 0 0 5031**

This entry contains either the name of the server's host or its IP address in text form, and the port socket number for the service. There are four pieces of information needed to specify a server:

- Host name or IP address where the SafeWord authentication server is located (required). A maximum of 4 servers can be specified (using a separate 02 entry for each server).
- Priority value used for load balancing (required). The default value is set to 0 for PAM. This value determines which server will be used. There are two schemes for selecting SafeWord servers:
  - **Prioritized scheme**—This scheme specifies a primary server that is always used, if possible. If it goes down, then the next server on the list is used as a backup. To specify this scheme, set all the weights to 0. The priority is the order in which they servers are entered in the file, the first entry has the highest priority.
  - **Load balancing**—This scheme provides a way to distribute the client load across multiple servers. As each session requires a server, a server is selected in round-robin fashion. For an equal balancing of all servers, enter a 1 for all servers. For unequal loading, simply increase the weight of one or more of the servers, thereby increasing that server's load.

Example:

02 Server: serverA 1  
02 Server: serverB 2  
02 Server: serverC 3  

After 6 sessions, serverA will have been used once, serverB twice and serverC three times.

- The maximum number of connections allowed for this server (required). This may be adjusted according to resource availability and performance needs. If this value is not used, it must be set to 0.
- Service port or socket number. Specify the port number of the SafeWord authentication server.

*Note:* Specify port 5031 for EASSP2 (default in PremierAccess) or 5030 for EASSP1.
• **09 User ID Source (USER/SYSTEM): SYSTEM**
  Specifies the source of the user ID, that is, whether the user ID for authenticating with PremierAccess is picked up from the `/etc/passwd` file, or specified by the user.

• **10 Server's System Name: STANDARD**
  Specifies which SafeWord system environment will be used. The default system name is STANDARD.

• **13 Data file's dir:**
  (For Solaris) `/usr/lib/security/pam_safeword.so.1`
  (For Linux) `/lib/security/pam_safeword.so.1`
  Data Files Directory refers to the location where the `pam_safeword.so.1` file is written and stored.

• **15 Send Status Messages to User: ERROR**
  This entry determines what type of status messages PAM can send to users. Valid parameters are:
  — NONE: No messages are sent.
  — ERROR: Error messages are sent.
  — INFO: Routine informational messages are sent.
  — DEBUG: Debugging messages are sent.
  — ALL: All messages are sent.

  *Note: More than one parameter can be specified.*

• **16 Send Status Messages to Console: NONE**
  This entry determines what types of status messages PAM sends to the unix syslog. This value is usually set to ERROR. Valid parameters are:
  — NONE: No messages are sent.
  — ERROR: Error messages are sent.
  — INFO: Routine informational messages are sent.
  — DEBUG: Debugging messages are sent.
  — ALL: All messages are sent.

  *Note: More than one parameter can be specified.*
**17 Send Status Messages to Log File: ALL**

Determines which status messages PAM sends to the log file. A log file is a plain ASCII file that can be edited or manipulated with any ASCII text editor or utility.

Valid parameters are:
- NONE: No messages are sent.
- ERROR: Error messages are sent.
- INFO: Routine informational messages are sent.
- DEBUG: Debugging messages are sent.
- ALL: All messages are sent.

*Note: More than one parameter can be specified.*

**18 Status Message Log Filename: /var/log/pam_safeword.log**

If you specify status messages to be written to a status file (specified in line 17), this entry specifies the name of the file where those messages will be written.

**23 Status Message Label: PAM_Safeword**

Specifies the label that will prefix messages generated by PAM.

**27 Client Type: PAM**

This line mentions the name of the agent authenticating with SafeWord. This information is used while registering the PAM Agent with the SafeWord server.

**55 Eassp Version: 201**

Specifies the EASSP protocol version used by the PAM module for communicating with SafeWord PremierAccess. A setting of 201 specifies EASSP2, a setting of 101 specifies EASSP1.

**59 Socket Timeout: 25**

Specifies the time in seconds for which the PAM module waits before disconnecting from the SafeWord PremierAccess server.

**1000 Check Pass Action Value (ON/OFF): OFF**

PAM can interpret the user's pass actions as authorization values to restrict the PAM user to selected machines or access points. When set to ON, a pass action of 0 signifies denial of authorization, while a non-zero value grants it. When set to OFF, all successfully authenticated users will be granted access by the PAM module.
Editing the PAM configuration file

On your system, you must edit the appropriate PAM configuration file as supplied by the operating system and add the module to the appropriate services.

For Solaris — /etc/pam.conf

For Linux— /etc/pam.d/login

Use the following as a template for modifying the PAM configuration file on your own system. For example, edit as follows to enable SafeWord authentication to telnet access:

**For Solaris:**

To enable SafeWord authentication via telnet, add the following line in /etc/pam.conf:

```
telnet auth required /usr/lib/security/pam_safeword.so.1
```

**For Linux:**

To enable SafeWord authentication via telnet add the following line in /etc/pam.d/login:

```
auth required /lib/security/pam_safeword.so.1
```

The remainder of this section provides additional information about these PAM configuration files on your system.

If implementing PAM on Solaris, see "Editing the pam.conf file for Solaris implementations" on page 12.

If implementing PAM on Linux, see "Editing the /etc/pam.d/login file for Linux implementations" on page 16.
**Editing the pam.conf file for Solaris implementations**

For Solaris implementations, the *pam.conf* file can be edited to select authentication mechanisms for each system-entry application. The file consists of entries following this syntax:

```
service_name module_type control_flag module_path
  module_options
```

- **service_name**—Indicates the name of the service
- **module_type**—Denotes the module type for the service
- **control_flag**—Selects the continuation and failure semantics for the module
- **module_path**—Specifies the pathname to a library object which implements the service functionality
- **module_options**—Specific options that can be passed to the service modules

**Note:** The *module_options* entry is optional. All other values must be defined. Comments can be added to the file by starting the line with a #. Any white space can be used to delimit the fields.

An entry in this file is ignored if one of the following conditions exist:

- The line has less than four fields
- An invalid value is given for module_type or control_flag
- The named module is not found

SafeWord PremierAccess support for PAM only supports the authentication module type. Table 2 lists some of the valid service names that use authentication module types and that can be used with the SafeWord Agent for PAM.
One of three control flags must be selected for each entry to
determine continuation or failure behavior from the module. These
flags determine what the ultimate result (success or failure) will be.
The values are defined below:

- **Required**—This module must return success in order to have the
  overall result be successful.

- **Optional**—If this module fails, the overall result can be successful if
  another module in this stack returns success.

- **Sufficient**—If this module is successful, skip the remaining modules
  in the stack, even if they are labeled as required.

If all of the modules are labeled as required, then authentication
through all modules must succeed in order for the user to be
authenticated. If some of the modules fail, an error value from the first
failed module is reported. If a failure occurs for a required module, all
modules in the stack are still tried, but access is denied.

---

### Table 2. Service names

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Daemon or Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>dtlogin</td>
<td>/usr/dt/bin/dtlogin</td>
</tr>
<tr>
<td>ftp</td>
<td>/usr/sbin/in.ftpd</td>
</tr>
<tr>
<td>login</td>
<td>/usr/bin/login</td>
</tr>
<tr>
<td>rexd</td>
<td>/usr/sbin/rpc.rexd</td>
</tr>
<tr>
<td>rlogin</td>
<td>/usr/sbin/in.rlogind</td>
</tr>
<tr>
<td>rsh</td>
<td>/usr/sbin/in.rshd</td>
</tr>
<tr>
<td>su</td>
<td>/usr/bin/su</td>
</tr>
<tr>
<td>telnet</td>
<td>/usr/sbin/in.telnetd</td>
</tr>
<tr>
<td>uucp</td>
<td>/usr/sbin/in.uucpd</td>
</tr>
</tbody>
</table>
If none of the modules are labeled as required, then at least one of the entries for that service must succeed for the user to be authenticated. The optional flag should be used when one success in the stack is enough. This flag should only be used if it is not important for this mechanism to succeed. For instance, if your users need to have permission associated with a specific mechanism to get their work done, then it should not be labeled as optional.

The sufficient flag allows for one successful authentication to be enough for the user to get in. More information about these flags is given in the next section, which presents the default /etc/pam.conf file.

The following is a sample pam.conf file for Solaris.

Sample pam.conf file

```bash
#ident  "@(#)pam.conf 1.19     95/11/30 SMI"
#
# Sample PAM configuration
#
# Authentication management
#
# Uncomment one or more of the following lines to activate
# SafeWord PAM authentication for the selected service(s).
#
#login  auth required /usr/lib/security/pam_safeword.so.1
#telnet auth required /usr/lib/security/pam_safeword.so.1
#ftp    auth required /usr/lib/security/pam_safeword.so.1
#rsh    auth required /usr/lib/security/pam_safeword.so.1
#uucp   auth required /usr/lib/security/pam_safeword.so.1
#su     auth required /usr/lib/security/pam_safeword.so.1
#
# We recommended that you study the information at
# http://www.sun.com/software/solaris/pam before attempting
# to modify your /etc/pam.conf file. Incorrect configuration
# can result in your system denying access to all users,
# including the administrator.
#
loginauth required /usr/lib/security/pam_unix.so.1
loginauth required /usr/lib/security/pam_dial_auth.so.1
#
#loginauth sufficient /usr/lib/security/pam_rhosts_auth.so.1
#loginauth required /usr/lib/security/pam_unix.so.1
#
dtloginauth required /usr/lib/security/pam_unix.so.1
#
rshauth required/usr/lib/security/pam_rhosts_auth.so.1
otherauth required/usr/lib/security/pam_unix.so.1
#
```
About the sample pam.conf file

The sample `pam.conf` file specifies that when running `login`, authentication must succeed for the `pam_unix` and the `pam_dial_auth` module. For `rlogin`, authentication through the `pam_unix` module must succeed, if it fails through `pam_rhost_auth`. The sufficient control flag indicates that for `rlogin` the successful authentication provided by the `pam_rhost_auth` module is sufficient and the next entry will be ignored.

Most other commands requiring authentication require successful authentication through the `pam_unix` module. Authentication for `rsh` must succeed through the `pam_rhost_auth` module.

Selecting OTHER for the service name allows a default to be set for any other commands that need authentication that are not included in the file. The OTHER option makes it easier to administer the file, since many commands that are using the same module can be covered by only one entry. Also, the OTHER option, when used as a “catch-all,” can ensure that each access is covered by one module. By convention the OTHER entry is included at the bottom of the section for each module type. The service_name field is case-insensitive; the capitalization is included to improve readability.

Normally the entry for the module_path is “root-relative.” If the entry for module_path does not begin with a slash, “/”, the path `/usr/lib/security/` is prepended to the filename. Paths to modules located in other directories must start from root.

The values for the module_options can be found in the man pages for the module (for example, `pam_unix(5)` and `pam_dce(5)`).

Making additional changes to the `/etc/pam.conf` file

If the `pam.conf` file is misconfigured or gets corrupted, it is possible that even the root user will not be able to login. Since `sulogin` does
not use PAM, the root user would then be required to boot the machine into single user and fix it. This is especially true in the case of \texttt{pam\_safeword}, where you are dealing not only with the module itself, but also the SafeWord server, as well as the network connection between the two.

Also, to ensure that the root user can still login if the PremierAccess server is unavailable, you can stack the SafeWord and UNIX PAM modules for login. To do so, the corresponding entries in \texttt{/etc/pam.conf} file should be as follows:

\begin{verbatim}
login auth sufficient /usr/lib/security/pam_safeword.so.1
login auth required /usr/lib/security/pam_unix.so.1
\end{verbatim}

However, for the above to work consistently with synchronous or asynchronous tokens, you must disable the echoing of passwords to the screen. Do this by turning off password echo in the authenticator preferences of the corresponding Platinum or Silver token.

### Editing the /etc/pam.d/login file for Linux implementations

For Linux implementations, the following is a sample configuration contained in \texttt{/etc/pam.d/login} for using the SafeWord PAM module with telnet and login:

\begin{verbatim}
#%PAM-1.0
auth required /lib/security/pam_securetty.so
auth required /lib/security/pam_pwdb.so shadow nullok
auth required /lib/security/pam_safeword.so.1
auth required /lib/security/pam_nologin.so
account required /lib/security/pam_pwdb.so
password required /lib/security/pam_cracklib.so
password required /lib/security/pam_pwdb.so nullok use_authtok
md5 shadow
session required /lib/security/pam_pwdb.so
session optional /lib/security/pam_console.so
\end{verbatim}

On Linux, care must be exercised to ensure that the root user can login at the console, if the \texttt{/etc/pam.d/login} file is configured for SafeWord authentication. A simple solution is to add the root user to SafeWord PremierAccess. Another solution is to stack SafeWord and UNIX authentication with the SafeWord authentication tagged as sufficient. This way, the root user can login with UNIX authentication even if the SafeWord authentication is unsuccessful.
Excluding users from SafeWord authentication

SafeWord’s Agent for PAM includes a feature that allows you to exclude specific users from SafeWord authentication by editing the PAM configuration files. To set up the feature you append the parameter `xusers=[path/filename]` to the SafeWord module.

**Note:** In the parameter, “path” is the desired path to the file, and “filename” is the file where the users to be excluded from SafeWord authentication are listed.

Once the parameter is appended, the SafeWord module will look like the following example:

```
auth required /lib/security/pam_safeword.so.1 [xusers=/etc/pam_safeword_xusers]
auth sufficient pam_stack.so service=system-auth
```

**IMPORTANT:** The second line in this example is for the native Linux authentication module. This line will differ between Solaris and Linux, and between different versions of the operating systems.

Normally you would want to make the SafeWord module required and then set the native module to sufficient. By doing so, the UNIX password is not required unless the user is listed in the file specified by the `xusers` parameter. In this case, the SafeWord module will ignore the user and let the UNIX module perform the authentication.

In the example the file `/etc/pam_safeword_xusers` was used, but any filename can be specified. The contents of the file should look like the following:

```
#
#This file contains a list of users to be excluded from SafeWord authentication. Add users one per line.
#
root
```

**Note:** This file should be owned by root and have permissions set to 644.

Updating your software

Secure Computing updates its agent software regularly and posts those releases as downloads. We recommend you check the Secure Computing Web site at [www.securecomputing.com](http://www.securecomputing.com) on a regular basis to confirm that you are using the most up-to-date version of the software. If you do not have the most up-to-date version of the PAM software, follow the steps below to obtain it.

1. Browse to [www.securecomputing.com](http://www.securecomputing.com).
3. Select **SafeWord PremierAccess Agents**.

4. Select **Download SafeWord Agent for PAM**.

5. A dialog box appears informing you that you are downloading the PAM executable file from **www.securecomputing.com**, and asks if you want to open the file or save it to your computer. Click the **Save** button.

6. When the Save As window appears, use the drop-down menu to choose the location where you want to save the executable file.

7. When you have chosen the location where you want to save the executable file, click the **Save** button.
Uninstalling PAM

You may uninstall PAM in GUI mode or console (text) mode. If you are uninstalling in GUI mode, continue to the next section. If you are uninstalling in console (text) mode, refer to "Uninstalling PAM in console (text) mode" on page 21.

Uninstalling PAM in GUI mode

To uninstall PAM, from the command line enter the following:

```
cd /<YourInstallationPath>/_uninst ./uninstaller.bin
```

The Install Wizard launches. The Wizard uninstalls PAM.

1. Click Next. The Select Features window appears.

2. Ensure that the features you want to uninstall are selected, then click Next. The Summary Information window appears.
3. Review the summary information, then click **Uninstall**. The uninstallation process begins and the Wizard removes PAM from your computer.

4. (Conditional) If modifications have been made to files in the software, you must confirm the removal of those files. Click **Yes** or **Yes to All** to confirm their removal. PAM is removed from your computer. When the process is complete, the Successful Uninstallation window appears.

5. The uninstallation process is complete. Click **Finish** to close the window.
Uninstalling PAM in console (text) mode

To uninstall PAM, from the command line enter the following:

cd /<YourInstallationPath>/_uninst
./uninstaller.bin -console

The Install Wizard launches. The Wizard uninstalls PAM.

1. Press “1” to continue the process.

2. Press “0” to continue uninstalling the agent, and then press “1” to continue to the next screen.
   
   Note: The “0” key is comparable to pressing the Enter button.

3. The Wizard displays a message explaining that the components you have chosen will be uninstalled. It also displays the location from which these components will be removed. Confirm your selections, then press “1” to continue.

4. The uninstallation begins. When it is finished, a message displays explaining that the uninstallation was successful. Press “3” to finish.