

# **RSA Authentication Agent 6.0 for PAM Installation and Configuration Guide**



**The Security Division of EMC**

## **Contact Information**

See the RSA corporate web site for regional Customer Support telephone and fax numbers: [www.rsa.com](http://www.rsa.com)

## **Trademarks**

RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, see [www.rsasecurity.com/legal/trademarks\\_list.pdf](http://www.rsasecurity.com/legal/trademarks_list.pdf). EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.

## **License agreement**

This software and the associated documentation are proprietary and confidential to RSA, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

## **Note on encryption technologies**

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

## **Distribution**

Limit distribution of this document to trusted personnel.

## **RSA notice**

The RC5™ Block Encryption Algorithm With Data-Dependent Rotations is protected by U.S. Patent #5,724,428 and #5,835,600.

# Contents

- Chapter 1: Overview** ..... 5
  - Platform Support ..... 5
  - OpenSSH Support ..... 5
  - Standard Tool Support ..... 6
  - RSA Authentication Manager Support ..... 7
- Chapter 2: Installation and Configuration** ..... 9
  - Installing the PAM Agent ..... 9
    - Setting Up Your Environment ..... 9
    - Enabling the PAM Agent for AIX ..... 9
    - Running the PAM Agent Installation Script ..... 10
  - Upgrading to RSA Authentication Agent 6.0 for PAM ..... 10
  - Performing a Test Authentication ..... 10
  - Configuring the PAM Agent ..... 11
    - Configuration File Names and Locations ..... 11
    - Configuration Examples ..... 11
    - Configuring OpenSSH ..... 13
    - Configuring the PAM Agent for OpenSSH on AIX ..... 14
    - Configuring Stackable Modules ..... 14
    - Enabling Debug Output ..... 18
    - Configuring Reserve Passwords ..... 18
    - Configuring UNIX Group Support ..... 19
    - Known Configuration Issues ..... 20
  - Uninstalling the PAM Agent ..... 22
- Chapter 3: Troubleshooting** ..... 23
  - Authentication Utilities ..... 23
  - System Log Messaging ..... 24
    - Configuring the System Log ..... 24
    - PAM Agent Authentication Messages ..... 24
  - Getting Support and Service ..... 25
    - Before You Call for Customer Support ..... 25
- Index** ..... 27



# 1

## Overview

RSA Authentication Agent 6.0 for PAM (Pluggable Authentication Module) enables RSA SecurID authentication using either standard or OpenSSH connection tools.

The PAM Agent uses shared libraries that RSA has customized and supports several forms of RSA SecurID authenticators for access to UNIX servers and workstations.

---

### Platform Support

- AIX 5L v5.3 with TL5 (SP6) on 64-bit PowerPC processors
- HP-UX 11.0 and 11i on RISC 32-bit processors
- HP-UX 11i v2 on Itanium 64-bit processors
- Red Hat Enterprise Linux AS, ES, and WS 4.0 on Intel Xeon and AMD Opteron 64-bit processors
- Solaris 10 on SPARC 64-bit processors
- Solaris 10 x64 on Intel Xeon and AMD Opteron 64-bit processors
- Solaris 10 x86 on Intel 32-bit processors
- SUSE Linux Enterprise Server 9 (SP3) and 10 on Intel Xeon and AMD Opteron 64-bit processors

---

### OpenSSH Support

The PAM Agent is compatible with the OpenSSH suite of software tools. This software enhances operational security by encrypting data that is sent from client machines to the PAM Agent Host.

---

**Note:** RSA recommends that you use OpenSSH tools.

---

To use OpenSSH, you must download additional software necessary for compiling source code. The software is available at [www.OpenSSH.org](http://www.OpenSSH.org). This web site contains important information about using open source software, such as required compiling tools and other prerequisites.

The following OpenSSH tools are supported with the PAM Agent. You can use:

- ssh in place of telnet or rlogin
- sftp in place of ftp
- scp in place of rsh/remsh

For information about configuring OpenSSH, see “[Configuring OpenSSH](#)” on page 13.

The following table lists OpenSSH version support for your operating system.

| <b>Operating System</b>                              | <b>OpenSSH Tools Supported Versions</b> |
|--|---|
| AIX 5L 5.3 with TL5 (SP6) on (64 bit)                | 4.5 p1                                  |
| HP-UX 11.0 and 11i (32 bit)                          | 4.3 p2                                  |
| HP-UX 11i v2 on Itanium (64 bit)                     | 4.5 p1                                  |
| Red Hat Enterprise Linux AS, ES, WS 4.0 (64 bit)     | 4.3 p2                                  |
| Solaris 10 (32 bit)                                  | 4.3 p2                                  |
| Solaris 10 SPARC (64 bit)                            | 4.5 p1                                  |
| SUSE Linux Enterprise Server 9 (SP3) and 10 (64 bit) | 4.5 p1                                  |

## Standard Tool Support

The following table lists supported standard tools by platform.

| <b>Platform</b>  | <b>Standard Tools</b>   |
|--|---|
| <b>All</b>   | <ul style="list-style-type: none"> <li>• telnet</li> <li>• login</li> <li>• rlogin</li> <li>• su</li> <li>• ftp (limited to single transaction)</li> </ul>                          |
| <b>HP-UX 11.0</b><br><b>HP-UX 11i</b>  | dtlogin (limited to single transaction)   |
| <b>Red Hat Enterprise Linux AS, ES, and WS 4.0</b>                                 | GDM with the following desktop themes: <ul style="list-style-type: none"> <li>• Circles</li> <li>• Happy GNOME</li> <li>• Happy GNOME with Browser</li> <li>• Blue Curve</li> </ul> |
| <b>Solaris 10 SPARC (64 bit)</b><br><b>Solaris 10 x64</b><br><b>Solaris 10 x86</b> | dtlogin   |

---

| <b>Platform</b>   | <b>Standard Tools</b>   |
|---|---|
| <b>SUSE Linux Enterprise Server 9 (SP3) and 10 (64 bit)</b> | GDM with the following desktop themes: <ul style="list-style-type: none"><li>• Circles</li><li>• Happy GNOME</li><li>• Happy GNOME with Browser</li><li>• SuSe</li></ul> kdm (limited to single transaction)<br>xdm (limited to single transaction) |

---

---

## **RSA Authentication Manager Support**

The PAM Agent supports RSA ACE/Server 6.0 and RSA Authentication Manager 6.1. You must install the latest available patches for either of these versions.





# 2

## Installation and Configuration

---

### Installing the PAM Agent

Installing the PAM Agent involves setting up your environment; enabling the PAM Agent, if you are using the AIX platform; and running the installation script. This section describes these tasks.

### Setting Up Your Environment

Before you perform the installation, verify that:

- You have root permissions on the Agent Host.
- You have created an installation directory on the machine on which you are installing the PAM Agent.
- You have the most up-to-date version of the **sdconf.rec** from the RSA Authentication Manager stored in an accessible directory, such as **/var/ace**, on the Agent Host.

---

**Note:** The root administrator on the Host must have write permission to the directory in which the **sdconf.rec** is stored.

---

- You have created an Agent Host record for the PAM Agent in the RSA Authentication Manager database. For more information, see the RSA Authentication Manager documentation.
- You have set an environment variable called **VAR\_ACE** that points to the location of **sdconf.rec**.

---

**Note:** The Host must be physically secure in a locked room. Allow only administrative access to this location.

---

### Enabling the PAM Agent for AIX

Complete this procedure if you are running the PAM Agent on the AIX operating system. It is not required by the HP-UX, Linux, SUSE, or Solaris operating systems.

#### To enable the PAM Agent on AIX 5L v5.3 with TL5 SP6 (64 bit):

1. Change to the **/etc/security** directory, and open **login.cfg**.
2. Comment the line as follows:  

```
#auth_type = STD_AUTH
```
3. Enable the PAM Agent. Type:

```
auth_type = PAM_AUTH
```

## Running the PAM Agent Installation Script

### To install the PAM Agent:

1. Change to the directory you created when you downloaded the software, and untar the file. Type:
 

```
tar -xvf filename.tar
```
2. Run the install script. Type:
 

```
./install_pam.sh
```
3. Follow the prompts until you are prompted for the **sdconf.rec** directory. If the path is correct, press ENTER. If the path is incorrect, verify that it is correctly defined in the VAR\_ANCE environment variable.
4. For each of the remaining installation prompts, press ENTER to accept the default value, or type in a different path.

---

## Upgrading to RSA Authentication Agent 6.0 for PAM

To upgrade to RSA Authentication Agent 6.0 for PAM, follow the instructions in the preceding section, “[Installing the PAM Agent](#).” When the installer asks if you want to overwrite your current installation, type **y**. Your previous configuration settings are migrated during the upgrade.

---

**Note:** You can upgrade to RSA Authentication Agent 6.0 for PAM only on the HP-UX 11.0 and 11i operating systems. You cannot upgrade on the Solaris, Linux, SUSE, or AIX operating systems.

---



---

## Performing a Test Authentication

RSA recommends that you perform a simple test authentication to ensure that the PAM Agent is functioning properly. You must use a token with a PIN that is already registered in the Authentication Manager database. Follow the New PIN procedure for proper registration. For additional information, contact your Authentication Manager administrator.

### To perform a test authentication:

1. Change to the **/opt/pam/bin** directory. Type:
 

```
./acetest
```
2. Enter your user name and passcode.

If you are repeatedly denied access, contact your Authentication Manager administrator.

---

## Configuring the PAM Agent

Before you make any configuration changes, make backup copies of the original configuration files. If you plan to use OpenSSH or to implement reserve passwords for root administrators, you must perform additional configuration steps. For instructions, see “[Configuring OpenSSH](#)” on page 13 and “[Configuring Reserve Passwords](#)” on page 18.

### Configuration File Names and Locations

On Linux, multiple configuration files are located in the `/etc/pam.d` directory. Each file uses the name of the connection tool. On AIX 5.3, Solaris 10, and HP-UX 11.0, 11i, and 11i v2, a single configuration file named `pam.conf` is located in the `/etc` directory.

### Configuration Examples

The following examples show how to protect several of the most commonly used connection tools with RSA SecurID on each supported operating system.

---

**Important:** For AIX, HP-UX, and Solaris, edit only the “Authentication Management” section of the configuration file. Changes to any other section are not necessary for configuring SecurID authentication. In addition, RSA recommends that you enable only the PAM Agent for each connection tool in the configuration file. Comment out all other rules in the “Authentication Management” section for each connection tool.

---

#### **su on AIX 5L v5.3 with TL5 SP6 (64 bit):**

1. Change to the `/etc` directory. Open the `pam.conf` file, and scroll to the Authentication Management section.
2. Locate the `su` section, and comment the lines as follows:  

```
#su auth sufficient /usr/lib/security/pam_allowroot  
#su auth required /usr/lib/security/pam_aix
```
3. Enable `su` to point to the PAM Agent module. Type:  

```
su auth required /usr/lib/security/pam_securid.so
```

#### **telnet on AIX 5L v5.3 with TL5 SP6 (64 bit):**

1. Change to the `/etc` directory. Open the `pam.conf` file, and scroll to the Authentication Management section.
2. Locate the `telnet` section, and comment the line as follows:  

```
#telnet auth required /usr/lib/security/pam_aix
```
3. Enable `telnet` to point to the PAM Agent module. Type:  

```
telnet auth required /usr/lib/security/pam_securid.so
```

**login on HP-UX 11.0, HP-UX 11i (32 bit), and HP-UX 11i v2 (64 bit):**

1. Change to the `/etc` directory. Open the `pam.conf` file, and scroll to the Authentication Management section.
2. Locate the **login** section, and comment the line as follows:  

```
#login auth required /usr/lib/security/libpam_unix.1
```
3. Enable **login** to point to the PAM Agent module. Type:  

```
login auth required /usr/lib/security/pam_securid.1
```

**su on HP-UX 11.0, HP-UX 11i (32 bit), and HP-UX 11i v2 (64 bit):**

1. Change to the `/etc` directory. Open the `pam.conf` file, and scroll to the Authentication Management section.
2. Locate the **su** section, and comment the line as follows:  

```
#su required /usr/lib/security/libpam_unix.so.1
```
3. Enable **su** to point to the PAM Agent module. Type:  

```
su auth required pam_securid.1
```

**sshd on Red Hat Linux (64 bit):**

1. Change to the `/etc/pam.d` directory.
2. Open the `sshd` file. The following text is displayed:  

```
auth      required      pam_stack.so service=system-auth
auth      required      pam_nologin.so
account   required      pam_stack.so service=system-auth
password  required      pam_stack.so service=system-auth
session   required      pam_stack.so service=system-auth
session   required      pam_limits.so
session   optional     pam_console.so
```
3. Comment out the following line:  

```
auth      required      pam_stack.so service=system-auth
```
4. Enable **sshd** to point to the PAM Agent module. Type:  

```
auth      required      pam_securid.so
```

**rlogin on Solaris 10 x86 (32 bit), Solaris 10 x64, and Solaris 10 SPARC (64 bit):**

1. Change to the `/etc` directory. Open the `pam.conf` file, and scroll to the Authentication Management section.
2. Locate the **rlogin** section, and comment the lines as follows:  

```
#rlogin auth sufficient      pam_rhosts_auth.so.1
#rlogin auth requisite       pam_authtok_get.so.1
#rlogin auth required        pam_dhkeys.so.1
#rlogin auth required        pam_unix_cred.so.1
#rlogin auth required        pam_unix_auth.so.1
```
3. Enable **rlogin** to point to the PAM Agent module. Type:  

```
rlogin auth required      pam_securid.so
```

**sshd on SUSE Linux Enterprise Server 9 (SP3) and 10 (64 bit):**

1. Change to the `/etc/pam.d` directory.
2. Open the `sshd` file. The following text is displayed.

```
auth    include      common-auth
auth    required     pam_nologin.so
account include     common-account
password include    common-password
session include     common-session
# Enable the following line to get resmgr support for
# ssh sessions (see/usr/share/doc/packages/resmgr/README)
#session optional   pam_resmgr.so fake_ttyname
```
3. Comment out the following lines:

```
auth    include      common-auth
auth    required     pam_nologin.so
```
4. Enable `sshd` to point to the PAM Agent module. Type:

```
auth    required     pam_securid.so
```

## Configuring OpenSSH

This section assumes that you have successfully downloaded and installed the OpenSSH software, and that you have configured your PAM modules to work with OpenSSH. For more information on installation and other requirements, go to the OpenSSH web site at [www.OpenSSH.org](http://www.OpenSSH.org).

All of the supported platforms (AIX, HP-UX, Linux, SUSE, and Solaris) require you to edit the `sshd_config` file so that passcode authentication messages can be displayed to end users. The AIX platform also requires you to add `sshd` entries to the `pam.conf` file, as described in [“Configuring the PAM Agent for OpenSSH on AIX”](#) on page 14.

**To display passcode authentication messages:**

1. Open the `sshd_config` file.
2. Set the `UsePAM` parameter to **yes**.
3. Set the `PasswordAuthentication` parameter to **no**.

---

**Note:** Setting the `PasswordAuthentication` parameter to **no** disables the OpenSSH password prompt so that the PAM Agent is used instead. As a result, the user is prompted for an RSA SecurID passcode only.

---

4. Set the `PrivilegeSeparation` parameter to **no**.

## Configuring the PAM Agent for OpenSSH on AIX

If you are running the PAM Agent on the AIX platform, you must edit the `sshd_config` file, as described in [“Configuring OpenSSH”](#) on page 13, and also add `sshd` entries to the `pam.conf` file, as described in the procedure below.

### To configure the PAM Agent for OpenSSH on AIX 5L v5.3 with TL5 SP6 (64 bit):

1. Change to the `/etc` directory, and open `pam.conf`.
2. In the “Authentication” section, type:
 

```
sshd auth required /usr/lib/security/pam_securid.so
```
3. In the “Account Management” section, type:
 

```
sshd account required /usr/lib/security/pam_aix
```
4. In the “Password Management” section, type:
 

```
sshd password required /usr/lib/security/pam_aix
```
5. In the “Session Management” section, type:
 

```
sshd session required /usr/lib/security/pam_aix
```

## Configuring Stackable Modules

You can use RSA Authentication Agent 6.0 for PAM to integrate RSA SecurID with other PAM authentication modules in your environment such as LDAP. You can configure the priority of authentication challenges by editing the appropriate configuration file for your operating system. The following examples show how to configure the login connection tool in a stackable environment with LDAP on each supported operating system.

---

**Note:** RSA Authentication Agent 6.0 for PAM cannot be integrated in a stackable environment on HP-UX 11.0 (32 bit).

---

### AIX 5L v5.3 with TL5 (SP6) on 64 bit:

1. Change to `/etc` and open the `pam.conf` file. The following text is displayed:
 

```
# Authentication management
#
rlogin auth sufficient /usr/lib/security/pam_rhosts_auth
rlogin auth required /usr/lib/security/pam_aix
```
2. Add the following line:
 

```
rlogin auth required /usr/lib/security/pam_securid.so
```

**HP-UX 11i (32 bit):**

1. Change to `/etc` and open the `pam.conf` file.

The following text is displayed:

```
# Authentication management
#
login auth required /usr/lib/security/libpam_unix.1
su auth required /usr/lib/security/libpam_unix.1
#
# Account management
#
login account required /usr/lib/security/libpam_unix.1
su account required /usr/lib/security/libpam_unix.1
dtlogin account required /usr/lib/security/libpam_unix.1
dtaction account required /usr/lib/security/libpam_unix.1
ftp account required /usr/lib/security/libpam_unix.1
#
OTHER account required /usr/lib/security/libpam_unix.1
#
# Session management
#
login session required /usr/lib/security/libpam_unix.1
dtlogin session required /usr/lib/security/libpam_unix.1
dtaction session required /usr/lib/security/libpam_unix.1
OTHER session required /usr/lib/security/libpam_unix.1
#
# Password management
#
login password required /usr/lib/security/libpam_unix.1
passwd password required /usr/lib/security/libpam_unix.1
dtlogin password required /usr/lib/security/libpam_unix.1
dtaction password required /usr/lib/security/libpam_unix.1
OTHER password required /usr/lib/security/libpam_unix.1
```

2. Comment out the following line:  
`su auth required /usr/lib/security/libpam_unix.1`
3. Replace it with the following lines:  
`su auth required /usr/lib/security/libpam_ldap.1`  
`su auth required pam_secuid.1`

**HP-UX 11i v2 (64 bit):**

1. Change to `/etc` and open the `pam.conf` file.

The following text is displayed:

```
# Authentication management
login auth required libpam_hpsec.so.1
login auth sufficient libpam_unix.so.1
su auth required libpam_hpsec.so.1
su auth sufficient libpam_unix.so.1
dtlogin auth required libpam_hpsec.so.1
dtlogin auth sufficient libpam_unix.so.1
```

```

dtaction auth required libpam_hpsec.so.1
dtaction auth sufficient libpam_unix.so.1
ftp auth required libpam_hpsec.so.1
ftp auth sufficient libpam_unix.so.1
rcomds auth required libpam_hpsec.so.1
rcomds auth sufficient libpam_unix.so.1
sshd auth required libpam_hpsec.so.1
sshd auth sufficient libpam_unix.so.1
OTHER auth sufficient libpam_unix.so.1
    
```

2. Comment out the following lines:

```

su auth required libpam_hpsec.so.1
su auth sufficient libpam_unix.so.1
    
```

3. Add the following lines:

```

su auth required libpam_ldap.so.1 try_first_pass
su auth required pam_secured.1
    
```

#### **Red Hat Linux AS, ES, and WS 4.0 (64 bit):**

1. Change to **/etc/pam.d** and open the login file.

The following text is displayed:

```

#%PAM-1.0
auth required pam_securetty.so
auth required pam_stack.so service=system-auth
auth required pam_nologin.so
account required pam_stack.so service=system-auth
password required pam_stack.so service=system-auth
# pam_selinux.so close should be the first session rule
session required pam_selinux.so close
session required pam_stack.so service=system-auth
session required pam_loginuid.so
session optional pam_console.so
# pam_selinux.so open should be the last session rule
session required pam_selinux.so open
    
```

2. Comment out the following lines:

```

auth required pam_securetty.so
auth required pam_stack.so service=system-auth
auth required pam_nologin.so
    
```

3. Replace them with the following lines:

```

auth required pam_secured.so
auth required pam_ldap.so
    
```



**SUSE Linux Enterprise Server 9 (SP3) and 10 (64 bit):**

1. Change to `/etc/pam.d/` and open the `login` file.

```

auth      required      pam_securetty.so
auth      include       common-auth
auth      required      pam_nologin.so
account   include       common-account
password  include       common-password
session   include       common-session
session   required      pam_lastlog.so nowtmp
session   required      pam_resmgr.so
session   optional      pam_mail.so standard
session   required      pam_limits.so # added by orarun

```
2. Comment out the following lines:

```

auth      required      pam_securetty.so
auth      include       common-auth
auth      required      pam_nologin.so

```
3. Replace them with the following lines:

```

auth required pam_secured.so
auth required pam_ldap.so

```

**Solaris 10 x86 (32 bit), Solaris 10 x64, Solaris 10 SPARC (64 bit):**

1. Change to `/etc` and open the `pam.conf` file.  
The following text is displayed:

```

# Authentication management
#
# login service (explicit because of pam_dial_auth
#
login auth requisite pam_authtok_get.so
login auth required pam_dhkeys.so.1
login auth required pam_unix_cred.so.1
login auth required pam_unix_auth.so.1
login auth required pam_dial_auth.so.1
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin auth sufficient pam_rhosts_auth.so.1
rlogin auth requisite pam_authtok_get.so.1
rlogin auth required pam_dhkeys.so.1
rlogin auth required pam_unix_cred.so.1
rlogin auth required pam_unix_auth.so.1

```
2. Add the following line:

```

rlogin auth required pam_secured.so

```

## Enabling Debug Output

To enable debug output for the PAM Agent, edit the appropriate file by adding a debug argument as shown. On Linux, change to **/etc/pam.d** and edit the appropriate file. On all supported versions of AIX, Solaris and HP-UX, a single configuration file named **pam.conf** is located in the **/etc/** directory.

On AIX, type:

```
sshd auth required /usr/lib/security/pam_securid.so debug
```

On HP-UX (all supported versions), type:

```
sshd auth required /usr/lib/security/pam_securid.1 debug
```

On Linux (for both Red Hat and SUSE), edit the appropriate file in **/etc/pam.d** and type:

```
auth required pam_securid.so debug
```

On Solaris (all supported versions), type:

```
sshd auth required pam_securid.so debug
```

## Configuring Reserve Passwords

The PAM Agent allows reserve passwords to be used for root administrators only. Reserve passwords allow administrators access to Hosts during unforeseen circumstances, such as loss of communication between the Agent and the Authentication Manager. In these situations, administrators have the ability to temporarily disable the Agent if users require immediate access to resources on a Host.

To configure reserve passwords for **SSH** on Linux, change to **/etc/pam.d** and edit the appropriate file by adding the “reserve” flag as shown in the following example. On all supported versions of Solaris, HP-UX, and AIX, a single configuration file named **pam.conf** is located in the **/etc/** directory.

On AIX, open the **pam.conf** file and type:

```
sshd auth required pam_securid.so reserve
```

On HP-UX (all supported versions), open the **pam.conf** file and type:

```
sshd auth required pam_securid.1 reserve
```

On Linux (for both Red Hat and SUSE), edit the appropriate file in **/etc/pam.d** and type:

```
auth required pam_securid.so reserve
```

On Solaris (all supported versions), open the **pam.conf** file and type:

```
sshd auth required pam_securid.so reserve
```

## Configuring UNIX Group Support

The PAM Agent supports the UNIX operating system group support feature. You can configure the PAM Agent to always prompt specific groups to authenticate to a protected resource (default), or you can specify groups that the PAM Agent never prompts to authenticate.

### To configure group support:

1. Change to the `/etc` directory, and open `sd_pam.conf`.
2. Set the `ENABLE_GROUP_SUPPORT` parameter to 1.
3. Do one of the following:
  - To always prompt the users in the listed groups to authenticate (“include”), set the `INCL_EXCL_GROUPS` parameter to 1.
  - To never prompt the users in the listed groups to authenticate (“exclude”), set the `INCL_EXCL_GROUPS` parameter to 0.
4. Use the `LIST_OF_GROUPS` parameter to specify the groups you want to include or exclude.

---

**Note:** Do not specify Authentication Manager groups, as this feature is for UNIX groups only.

---

5. Save your changes.

When you enable group support with RSA Authentication Agent 6.0 for PAM, group members can authenticate using RSA SecurID, or with standard UNIX credentials. If you want to have group members authenticate through another PAM module in your stackable environment instead of using UNIX credentials, you must properly configure PAM Ignore Support.

### To configure PAM Ignore Support:

1. Change to the `/etc` directory and open `sd_pam.conf`.
2. Set the `PAM_IGNORE_SUPPORT` parameter to 1.
3. Save your changes.

## Known Configuration Issues

This information is provided to help you properly configure the PAM Agent and to help you assist end users when they authenticate using RSA SecurID. For the most up-to-date information on these and other issues, see the *Readme (PAMreadme.pdf)*.

| Operating System        | Connection Tool | Known Issues  |
|-------------------------|-----------------|---|
| All                     | ftp             | <p>When you use SecurID to protect ftp, SecurID authentication prompts and error messages are not displayed to end users; only standard OS prompts and error messages are displayed. Note the following:</p> <ul style="list-style-type: none"> <li>• Users enter their user name at the OS user name prompt, and their SecurID passcode at the OS password prompt.</li> <li>• If an end user is uncertain as to the status of a token (for example, if the token is in Next Tokencode mode, or New PIN mode), instruct the user to authenticate with another connection tool such as rlogin to verify that the PIN or tokencode is still valid.</li> </ul> <p>Static passwords do not function when ftp is configured to require SecurID authentication.</p> |
| All                     | sshd            | <p>After three unsuccessful SecurID authentication attempts are made in the same session, the connection is closed. You must terminate the session, and start another session.</p>  |
| HP-UX 11.0, 11i, 11i v2 | rlogin, remsh   | <p>Because rlogin and remsh use login to log on to remote hosts, if you enable the PAM Agent for rlogin or remsh, you must also enable the PAM Agent for login. In addition, if you enable the PAM Agent for remsh, you cannot use the command option with remsh.</p>   |
| HP-UX 11.0, 11i         | All             | <p>If you plan to set the requisite flag in <b>/etc/pam.conf</b>, you must install the HP-UX PAM Requisite software package available from the HP software depot at <a href="http://h20293.www2.hp.com">http://h20293.www2.hp.com</a>. In the <b>Search</b> field, enter "HP-UX PAM Requisite software".</p> <p><b>Note:</b> The package is unavailable for HP-UX 11i v2.</p>   |
| HP-UX 11.0, 11i         | dtlogin         | <p>In situations that require a reserve password, this tool does not display any warnings or errors to the administrator who is attempting to authenticate, but instead display the standard prompts.</p>   |

| Operating System                              | Connection Tool  | Known Issues  |
|---|------------------|---|
| HP-UX 11.0, 11i                               | dtlogin          | <p>When you use SecurID to protect dtlogin, SecurID authentication prompts and error messages are not displayed to end users; only standard OS prompts and error messages are displayed. Note the following:</p> <p>Users enter their user name at the OS user name prompt, and their SecurID passcode at the OS password prompt.</p> <p>If an end user is uncertain as to the status of his or her token (for example, if the token is in Next Tokencode mode, or New PIN mode), instruct the user to authenticate with another connection tool such as rlogin to verify that the PIN or tokencode is still valid.</p> |
| HP-UX 11i                                     | dtlogin          | Not supported in a stackable environment.   |
| HP-UX 11i v2                                  | dtlogin          | Not supported.  |
| Red Hat AS, ES, WS 4.0<br>SUSE 9 (SP3) and 10 | rlogin, rsh      | If the first attempt to process an rlogin or rsh request fails, the session is handed off to the login daemon. Therefore, if you configure Linux to use rlogin or rsh, you must configure the remote file in <b>/etc/pam.d</b> .  |
| Solaris 10 x86, x64, SPARC (64 bit)           | rlogin<br>telnet | In NFS environments, you can configure the .rhosts file in a user's home directory for remote access to other machines and resources within your network. In this environment, users are required to authenticate using SecurID for local access to their own workstations. However, users are not required to use SecurID if they use telnet or rlogin for network access to other resources after having gained local access. RSA recommends that you restrict users as necessary in this environment.  |

---

## Uninstalling the PAM Agent

Before you uninstall the PAM Agent, configure the Host to use the standard PAM module provided with your operating system. In addition, verify that you have root permissions on the Host. When the uninstall completes, verify that the installation directory has been removed. If the directory still exists, you must remove it manually.

### To uninstall the PAM Agent:

1. Change to the `/opt/pam` directory.
2. Run the uninstall script. Type:

```
./uninstall_pam.sh
```

# 3

## Troubleshooting

---

### Authentication Utilities

The authentication utilities are located in the `/opt/pam/bin` directory. Use these utilities to:

- Verify communication between the PAM Agent and the RSA Authentication Manager
- Perform a test authentication

#### **acestatus**

This utility checks the status of each Authentication Manager on which the PAM Agent is registered as an Agent Host. Type:

```
./acestatus
```

If you have questions concerning any of the following information, contact your Authentication Manager administrator.

**Configuration Version.** The version of the `sdconf.rec` file that is in use. For RSA ACE/Server 5.1 or later, this number is 14.

**DES Enabled.** If your configuration environment supports legacy protocols, **YES** is displayed.

**Client Retries.** The number of times the PAM Agent sends authentication data to the Authentication Manager before a time-out occurs.

**Client Timeout.** The amount of time (in seconds) that the PAM Agent waits before resending authentication data to the Authentication Manager.

**Server Release.** The version number of the Authentication Manager.

**Communication.** The protocol version used by the Authentication Manager and the PAM Agent.

The Authentication Manager section displays the following status information:

**Server Active Address.** The IP address that the PAM Agent uses to communicate with the Server. This address could be the actual IP address of the Server you have selected, or it could be an alias IP address assigned to the Server. An IP address of 00.000.00.00 indicates that the Agent has not yet received communication from the Server.

The status of this Server is indicated by one of the following:

**Available for Authentications.** The Server is available to handle authentication requests.

**Unused.** The Server has not yet received an authentication request.

**For Failover only.** The Server is reserved for failover use only.

**Default Server During initial requests.** Only this Server is available to handle requests at this time.

---

## System Log Messaging

By default, several PAM Agent authentication messages are recorded in your system log. For tracing purposes, you can configure your system log to record all PAM Agent authentication messages.

### Configuring the System Log

**To send all authentication messages to the system log:**

1. Change to the `/etc/` directory. Open the `syslog.conf` file.
2. Add `auth.notice` to the line that specifies your system log file.
3. If you are using OpenSSH, remove the `authpriv.none` parameter.

### PAM Agent Authentication Messages

#### Cannot locate `sd_pam.conf` file

The configuration file `sd_pam.conf` is not in the `/etc` directory; `/etc` must contain the correct configuration file so that the `VAR_ACE` environment variable can be set properly.

#### AceInitialize failed

`AceInitialize` is an API function call that initializes worker threads, and loads configuration settings from `sdconf.rec`. Verify that you have the latest copy of `sdconf.rec` from your Authentication Manager administrator and that the `VAR_ACE` environment variable is set properly.

#### Cannot communicate with RSA ACE/Server

Either the Authentication Manager brokers are not started, or there has been a network failure. Contact your Authentication Manager administrator or your network administrator.

#### Reserve password exceeds character limit

The maximum character limit for reserve passwords is 256 characters.

#### Invalid reserve password

The reserve password is the same as the system password for the Host. You must know this password if the Authentication Manager is unable to process authentication requests.



### Username exceeds character limit

The maximum character limit for user names is 32 characters.

### Reserve password not allowed. User is not root.

Verify that you have root permissions. Only administrators with root permissions can use the reserve password.

---

## Getting Support and Service

---

|   |   |
|---|---|
| RSA SecurCare Online                    | <a href="https://knowledge.rsasecurity.com">https://knowledge.rsasecurity.com</a> |
| Customer Support Information            | <a href="http://www.rsa.com/support">www.rsa.com/support</a>                      |
| RSA Secured Partner Solutions Directory | <a href="http://www.rsasecured.com">www.rsasecured.com</a>                        |

---

RSA SecurCare Online offers a knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

The RSA Secured Partner Solutions Directory provides information about third-party hardware and software products that have been certified to work with RSA products. The directory includes implementation guides with step-by-step instructions and other information about interoperation of RSA products with these third-party products.

### Before You Call for Customer Support

Make sure you have direct access to the computer running the RSA Authentication Agent for PAM software.

Please have the following information available when you call:

- Your RSA Customer/License ID.
- RSA Authentication Agent for PAM software version number.
- The make and model of the machine on which the problem occurs.
- The name and version of the operating system under which the problem occurs.



# Index

## A

- acestatus utility, 23
- acetest utility, 10, 24
- AIX platform
  - configuring the PAM Agent for OpenSSH, 14
  - debug output, 18
  - enabling the PAM Agent (installation requirement), 9
  - OpenSSH support, 6, 14
  - reserve passwords, 18
  - stackable modules, 14
  - su tool on, 11
  - supported version, 5
  - telnet tool on, 11
- Authentication Manager, supported versions, 7
- authentication utilities, 23

## C

- connection tool examples, 11
  - AIX with su, 11
  - AIX with telnet, 11
  - HP-UX with login, 12
  - HP-UX with su, 12
  - Red Hat with sshd, 12
  - Solaris with rlogin, 12
  - SUSE with sshd, 13

## D

- debug output, 18

## G

- group support, configuring, 19

## H

- HP-UX platform
  - debug output, 18
  - login tool on, 12
  - OpenSSH support, 6
  - reserve passwords, 18
  - stackable modules, 15
  - standard tool support, 6
  - su tool on, 12
  - supported versions, 5

## I

- installation, 9, 10

## K

- known configuration issues, 20

## L

- Linux. *See* Red Hat platform, SUSE platform
- log messages, 24

## O

- OpenSSH, 5
  - configuring, 13
  - configuring the PAM Agent on AIX, 14
  - supported versions, 6

## P

- platform support, 5

## R

- Red Hat platform
  - debug output, 18
  - OpenSSH support, 6
  - reserve passwords, 18
  - sshd tool on, 12
  - stackable modules, 16
  - standard tool support, 6
  - supported versions, 5
- reserve passwords, 18
- RSA Authentication Manager, supported versions, 7

## S

- Solaris platform
  - debug output, 18
  - OpenSSH support, 6
  - reserve passwords, 18
  - rlogin tool on, 12
  - stackable modules, 17
  - standard tool support, 6
  - supported versions, 5

stackable modules, configuring, 14

AIX, 14

HP-UX, 15

Red Hat, 16

Solaris, 17

SUSE, 17

SUSE platform

debug output, 18

OpenSSH support, 6

reserve passwords, 18

sshd tool on, 13

stackable modules, 17

standard tool support, 7

supported versions, 5

system log, 24

## T

test authentication, 10, 23

tools

OpenSSH support, 6

by platform, 6

troubleshooting utilities, 23

## U

uninstalling, 22

UNIX operating system group support, 19

upgrading, 10

utilities

acestatus, 23

acetest, 10, 24

authentication, 23

troubleshooting, 23