RSA ACE/Agent 5.0 for PAM
Installation and Configuration Guide

Contact Information

See our Web sites for regional Customer Support telephone and fax numbers.

RSA Security Inc.	RSA Security Ireland Limited
www.rsasecurity.com	www.rsasecurity.ie

Trademarks

License agreement

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 exporting this product.

Distribution

Limit distribution of this document to trusted personnel.

First printing: April 2003

Contents

Overview

RSA ACE/Agent 5.0 for PAM (Pluggable Authentication Module) enables RSA SecurID authentication using either the following standard or OpenSSH connection tools.

Standard tools:

- login
- rlogin
- telnet
- rsh
- su
- ftp

OpenSSH tools:

- sftp
- ssh
- scp

This Agent uses shared libraries that have been customized by RSA Security. The PAM Agent supports all forms of RSA SecurID authenticators for access to UNIX servers and workstations.

Platform Support

RSA ACE/Agent 5.0 for PAM is supported on Linux 7.3 and on Solaris 8 and 9. Note the conditions for using standard connection tools and OpenSSH on these operating systems.

Operating System	OpenSSH Tools	Standard Tools
Solaris 8, 9	Recommended	Supported
Linux 7.3	Required	Not supported

Specific configuration settings are necessary for several standard connection tools. For more information, see “Known Configuration Issues” on page 10.

The use of OpenSSH requires that you download additional software necessary for compiling source code. For more information, see “OpenSSH” on page 6.

OpenSSH

RSA ACE/Agent 5.0 for PAM can be used 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. OpenSSH is included with Red Hat Linux 7.3 and Solaris 9 operating systems. You can download this software free of charge from the OpenSSH web site at **www.OpenSSH.org**. This web site also contains important information about using open source software, such as required compiling tools and other prerequisites.

The following OpenSSH tools are supported with the RSA ACE/Agent 5.0 for PAM. You can use

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

Installation and Configuration

Installing the PAM Agent

RSA ACE/Agent 5.0 for PAM is a downloadable **.tar** file on the RSA Security web site. This installation procedure assumes that you have successfully downloaded the **.tar** file. Before you perform the installation, verify that:

- You have root permissions on the Host.
- You have the most up-to-date version of **sdconf.rec**, and have placed it in an accessible directory (for example, /**var/ace**). The root administrator on the Host must have write permission to **sdconf.rec**. Set an environment variable called VAR_ACE that points to the location of **sdconf.rec**.

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

To install the RSA ACE/Agent 5.0 for PAM:

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

   ```
   tar -xvf pam_agent.tar
   ```

2. Run the install script. Type

   ```
   ./install_pam.sh
   ```

3. If you obtained this product from somewhere other than the countries listed, type **n** to display an alternate license agreement; otherwise press ENTER to continue.
4. After carefully reviewing the license text, type **A** to accept the License Terms and Conditions that are displayed and continue installing the software. If you do not accept, the installation aborts.
5. Press ENTER to accept the directory path to **sdconf.rec**. If the path is incorrect, verify that it is correctly defined in the VAR_ACE environment variable.
6. For each of the remaining installation prompts, press ENTER to accept the default value, or type in a different path.

Configuring the PAM Agent

You must edit one or more configuration files to enable the RSA ACE/Agent 5.0 for PAM and to ensure that it functions properly with your connection tools. If you plan to use OpenSSH, or to implement reserve passwords for root administrators, additional configuration steps are required. See "Configuring OpenSSH" on page 9 and "Configuring Reserve Passwords" on page 9 for information and instructions.

Note: Save backup copies of configuration files before you make any edits. The configuration changes take effect immediately after you save the file. You do not need to restart the Host.

On Linux, multiple configuration files are located in the **/etc/pam.d** directory. Each file uses the name of the connection tool. On Solaris, a single configuration file named **pam.conf** is located in the **/etc** directory. The following examples show how to protect **sshd** and **rlogin** with RSA SecurID on Linux 7.3 and on Solaris 8.

To configure sshd with the PAM Agent on Linux 7.3:

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

```
auth       required   /lib/security/pam_nologin.so
auth       required   /lib/security/pam_securetty.so
auth       required   /lib/security/pam_env.so
auth       sufficient /lib/security/pam_rhosts_auth.so
auth       required   /lib/security/pam_stack.so service=system-auth
account    required   /lib/security/pam_stack.so service=system-auth
password   required   /lib/security/pam_stack.so service=system-auth
session    required   /lib/security/pam_stack.so service=system-auth
```

3. Comment out the following line

```
auth       required   /lib/security/pam_stack.so service=system-auth
```

4. Enable **sshd** to point to the PAM Agent module. Type

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

To configure rlogin with the PAM Agent on Solaris 8:

1. Change to the **/etc** directory. Open the file **pam.conf** and scroll to the Authentication Management section. This section is displayed as follows.

```
# Authentication management
#
login   auth required /lib/security/pam_unix.so.1
login   auth required /lib/security/pam_dial_auth.so.1
#
rlogin  auth sufficient /lib/security/pam_rhosts_auth.so.1
rlogin  auth required /lib/security/pam_unix.so.1
#
dtlogin auth required /lib/security/pam_unix.so.1
#
rsh     auth required /lib/security/pam_rhosts_auth.so.1
other   auth required /lib/security/pam_unix.so.1
```

2. Comment out this line.
   ```
   #rlogin    auth required    /lib/security/pam_unix.so.1
   ```
3. Enable **rlogin** to point to the PAM Agent module. Type
   ```
   rlogin auth required    /lib/security/pam_securid.so
   ```

Note: Edit only the "Authentication Management" section of this file. Do not make changes to any other section.

Configuring OpenSSH

This section assumes that you have successfully downloaded and installed the OpenSSH software. For more information on installation and other requirements, visit the OpenSSH Web site at **www.OpenSSH.org**.

You must edit the **sshd_config** file so that passcode authentication messages can be displayed to end users.

To display passcode authentication messages:

1. Set the "PAMAuthenticationViaKbdInt" parameter to "Yes."
2. Set the "UserPrivilegeSeparation" parameter to "No."

Configuring Reserve Passwords

The RSA ACE/Agent 5.0 for PAM 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 RSA ACE/Server. 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**, edit the appropriate file by adding the "reserve" flag as shown in the examples below. On Linux change to **/etc/pam.d** and edit the appropriate file. On Solaris, a single configuration file named **pam.conf** is located in the **/etc/** directory.

On Solaris, type

```
sshd auth required /lib/security/pam_securid.so reserve
```

On Linux, type

```
auth required /lib/security/pam_securid.so reserve
```

Known Configuration Issues

This information is provided to help you properly configure the RSA ACE/Agent 5.0 for PAM, 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, refer to the *RSA ACE/Agent 5.0 for PAM Readme.*

Operating System	Connection Tool	Known Issues
ALL	**sshd**	By default, regular operating system password prompts are displayed after three unsuccessful RSA SecurID authentication attempts that are made in the same session. During a fourth attempt, if a user enters the correct RSA SecurID passcode when prompted for a system password, the authentication is successful. It is not successful, however, if a user's token is in Next Tokencode mode, or New PIN mode.
Solaris 8, 9	**ftp**	When you use RSA SecurID to protect **ftp**, RSA SecurID authentication prompts and error messages are not displayed to end users; only standard OS prompts and error messages are displayed. Note the following: • Users enter their username at the OS username prompt, and their RSA SecurID passcode at the OS password prompt. • 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 him or her to authenticate with another connection tool such as **rlogin** to verify that the PIN or tokencode is still valid. Static passwords do not function when **ftp** is configured to require RSA SecurID authentication.
Solaris 8, 9	**rlogin**	In NFS environments, the **.rhosts** file in a user's home directory can be configured for remote access to other machines and resources within your network. In this environment, users are required to authenticate using RSA SecurID for local access to their own workstation. However, a user is *not* required to use RSA SecurID if he or she uses **telnet** or **rlogin** for network access to other resources after they have gained local access. RSA Security recommends that you restrict users as necessary in this environment.

Uninstalling the PAM Agent

Note: Before you uninstall the RSA ACE/Agent 5.0 for PAM, you should 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.

To uninstall the PAM Agent:

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

```
./uninstall_pam.sh
```

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 ACE/Server.
- Perform a test authentication.

acestatus

This utility checks the status of each RSA ACE/Server 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 RSA ACE/Server administrator.

Configuration Version. The version of the **sdconf.rec** file that is in use. For RSA ACE/Server 5.0 or later, this number is 12.

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 RSA ACE/Server before a time-out occurs.

Client Timeout. The amount of time (in seconds) that the PAM Agent waits before resending authentication data to the RSA ACE/Server.

Server Release. The version number of the RSA ACE/Server.

Communication. The protocol version used by the RSA ACE/Server and the PAM Agent.

The "RSA ACE/Server List" 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 also 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.

acetest

RSA Security recommends that you test authentication using a token with a PIN that is already registered in the RSA ACE/Server database. A test authentication with a token in New PIN mode requires that you follow the New PIN procedure for proper registration. There are specific instructions for each token type that are provided as part of the RSA ACE/Server CD. Contact your RSA ACE/Server administrator to obtain a copy of the appropriate instructions for each of your token types, and be sure to read them before you perform this test.

To perform a test authentication:

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

   ```
   ./acetest
   ```

2. Enter your username and passcode.
   If you are repeatedly denied access, contact your RSA ACE/Server administrator.

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.

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**. You should verify that you have the latest copy of **sdconf.rec** from your RSA ACE/Server administrator, and that the VAR_ACE environment variable is set properly.

Cannot communicate with RSA ACE/Server

Either the RSA ACE/Server brokers are not started, or there has been a network failure. Contact your RSA ACE/Server administrator or your network administrator.

Reserve password exceeds character limit

The 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 RSA ACE/Server is unable to process authentication requests.

Username exceeds character limit

The character limit for usernames 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	**www.rsasecurity.com/support/securcare**
Technical Support Information	**www.rsasecurity.com/support**

Note: Technical support is not provided during the warranty period unless a valid Software Service Contract is in force.

Make sure that you have direct access to the computer running the RSA ACE/Agent 5.0 for PAM software.

Please have the following information available when you call:

- ❑ RSA ACE/Server 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.