RSA Authentication Agent 7.0 for PAM—Installation and Configuration Guide for Solaris

The RSA SecurID solution provides two-factor authentication to protect access to data and applications. This access can be through remote dial-in connections, local access, domain and terminal services access, Internet and VPN connections, intranet and extranet applications.

The SecurID solution consists of an Authentication Manager server, an authentication agent that communicates with the server, and authenticators that generate the tokencode. The authentication agent initiates a SecurID authentication session when a user attempts to access a protected resource. It verifies data provided by the user against the data stored in the Authentication Manager server. Based on the result, the user is either allowed or denied access.

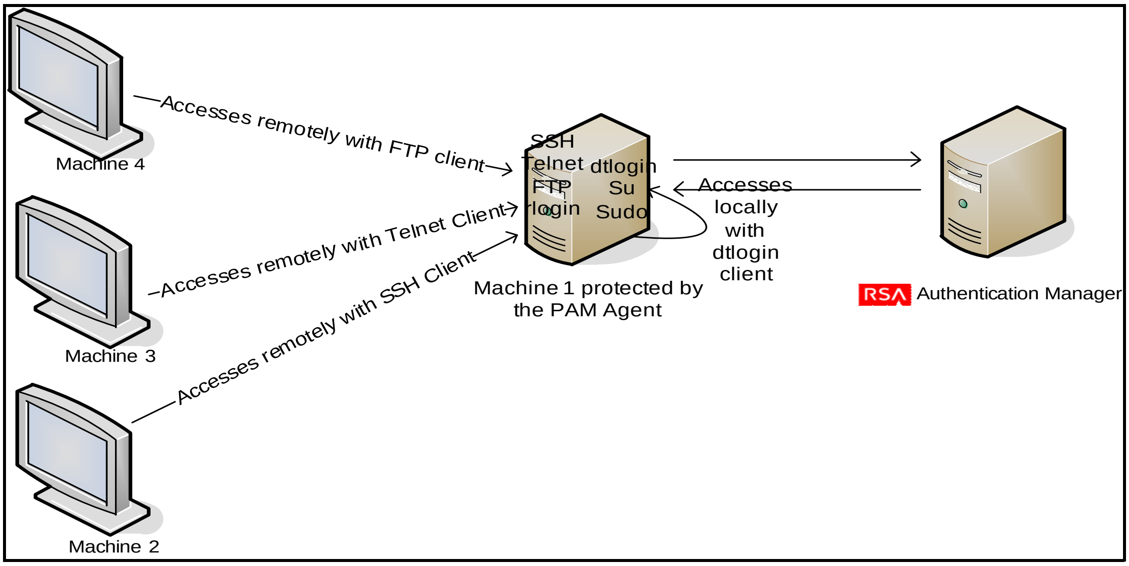
Overview of the RSA Authentication Agent 7.0 for PAM

The RSA Authentication Agent 7.0 for PAM (pluggable authentication module) enables RSA SecurID authentication on UNIX systems, using either standard or OpenSSH connection tools.

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

Agent Workflow

A machine protected by the PAM agent can be accessed either locally or remotely.


Machine 4
Accesses remotely with FTP client
SSH
Telnet
FTP
rlogin
dtlogin
Su
Sudo
Accesses locally with dtlogin client
Machine 3
Accesses remotely with Telnet Client
Accesses remotely with SSH Client
Machine 1 protected by the PAM Agent
RSA Authentication Manager
Machine 2

This section describes the working of the agent for PAM.

1. A user attempts to access a machine protected by the PAM agent, either locally or remotely:
    - If accessed locally, local logon tools supported such as login are used.
    - If accessed remotely, remote logon tools supported such as rlogin, telnet, ssh, and ftp are used.
2. The PAM infrastructure intercepts all logon requests, and using PAM configuration files, arrives at the RSA module:
    - If the user requesting access is not to be challenged by RSA SecurID, the RSA PAM module allows the request to proceed.
    - If the user requesting access is to be challenged by RSA SecurID, the agent continues the authentication process.
3. The agent prompts the user for the user name.
4. The agent requests the user for the passcode.
5. The agent sends the user name and passcode to Authentication Manager in a secure manner:
    - If Authentication Manager approves the request, the agent grants access to the user.
    - If Authentication Manager does not approve the request, the agent denies access and takes appropriate action.

In addition to providing basic access checks during standard authentication, agents also handle several security-related housekeeping tasks, such as those related to the Next Tokencode mode and the New PIN mode.

In the Next Tokencode mode, Authentication Manager requests for the next tokencode displayed on the user's token. If the next tokencode is not sent to Authentication Manager, the authentication fails.

The Authentication Manager administrator determines if the user associated with a particular token requires a new PIN, and also the characteristics of the PIN. In the New PIN mode, the agent prompts the user for a new PIN, and sends the information to Authentication Manager.

System Requirements

This section describes the minimum software requirements for installing the agent.

Requirement	Support
Operating System	Solaris version 10 (update 8) with Zones UltraSparc: 64-bit. Intel Xeon: 32-bit and 64-bit. AMD Opteron: 32-bit and 64-bit

Requirement	Support
RSA Authentication Manager	Versions 6.1.2, 7.1 SP2, and 7.1 SP3
Tools	• telnet • login • rlogin • su • ssh (ssh, sftp and scp) • sudo 1.7.3 • ftp (limited to a single transaction) • dtlogin
OpenSSH (Optional)	5.5 P1
OpenSSH tools (Optional)	• ssh • sftp • scp

Note: On Intel and AMD, on the 64-bit operating system, only 32-bit PAM agent binaries are available. Therefore, only 32-bit tools are supported.

Prerequisites

You must ensure that you have the following, to be able to install the agent.

- ✔ 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 latest version of the **sdconf.rec** file from RSA Authentication Manager stored in an accessible directory, such as **/var/ace**, on the agent host.
- ✔ The root administrator on the host has write permission to the directory in which the **sdconf.rec** file is stored.
- ✔ You have created an agent host record for the PAM agent in the Authentication Manager database. For more information, see the RSA Authentication Manager documentation.
- ✔ If you require sudo, you must have the supported version installed. You can download the supported sudo version from **www.sudo.ws**.

✓ If you are using OpenSSH, you must have the additional software required for compiling source code. This software is available at **www.OpenSSH.org**. This web site contains important information about using open source software, such as the required compiling tools and other prerequisites.

Installing the RSA Athentication Agent 7.0 for PAM

Installing the PAM agent involves setting up your environment and running the installation script. This section describes these tasks.

To install the agent, complete the tasks in the following table.

Task	Reference
Configure OpenSSH (Optional)	"Configure OpenSSH" on page 4
Install the agent	"Install the PAM Agent" on page 4
Perform a test authentication	"Perform a Test Authentication" on page 4

Configure OpenSSH

The PAM agent is compatible with OpenSSH. To display passcode authentication messages to users, the **sshd_config** file must be edited. To do this, you must have successfully downloaded and installed the OpenSSH software, and configured the PAM modules to work with OpenSSH. Refer to the OpenSSH documentation for any installation information.

To display passcode authentication messages to users:

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

   This 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 UsePrivilegeSeparation parameter to no.
5. Set the ChallengeResponseAuthentication parameter to yes.

Install the PAM Agent

To install the PAM agent:

1. Change to the PAM agent installer directory.
2. Untar the file by typing:

   tar -xvf <**filename.tar**>

3. Run the install script by typing:
   ./<filename>/install_pam.sh
4. Follow the prompts until you are prompted for the **sdconf.rec** directory:
   - If the path is correct, press ENTER.
   - If the path is incorrect, enter the correct path.
5. For each of the subsequent installation prompts, press ENTER to accept the default value, or enter the appropriate value.

Note: After installation, check that VAR_ACE in the **/etc/sd_pam.conf** file points to the correct location of the **sdconf.rec** file. This is the path to the configuration files. The whole path must have -rw------- root root permission.

Perform a Test Authentication

You must perform a test authentication to ensure that the PAM agent is functioning properly. For information on how to perform a test authentication, see "acetest" on page 15.

Upgrading to the PAM 7.0 Agent

You can upgrade only from version 6.0. Back up the configuration files before overwriting to save the configuration settings, if required.

To upgrade to version 7.0 of the agent, complete the tasks in the following table.

Task	Description
1. Install the agent.	For more information, see "Install the PAM Agent" on page 4.
2. Overwrite the existing installation files.	When the installer prompts asking if you want to overwrite your current installation, type y.
3. Run the conversion utility.	For more information, see "Conversion Utility" on page 17.

Obtain the Agent Version Number

To obtain the version number of the installed agent for PAM:

1. Change to the **<PAM Agent Install Directory>\lib\<bit version>** directory.
2. Type the following line:
   strings pam_securid.so | grep "Agent"
   This returns the version number of the installed agent.

Configuring Tools

This section describes how to configure supported tools to work with the PAM agent.

- Configure su
- Configure telnet
- Configure login
- Configure ssh and Related Tools
- Configure rlogin
- Configure ftp
- Configure sudo
- Configure dtlogin

Configure su

To configure su to work with the PAM agent:

1. Change to **/etc** directory.
2. Open the **pam.conf** file, and scroll to the Authentication Management section.
3. Comment the following lines, if they exist:
   su auth requisite pam_authtok_get.so.1
   su auth required pam_dhkeys.so.1
   su auth required pam_unix_cred.so.1
   su auth required pam_unix_auth.so.1
4. Add the line:
   su auth required pam_securid.so

Configure telnet

To configure telnet to work with the PAM agent:

1. Change to the **/etc** directory
2. Open the **pam.conf** file, and scroll to the Authentication Management section.

3. Comment the following lines, if they exist:
   telnet auth requisite pam_authtok_get.so.1
   telnet auth required pam_dhkeys.so.1
   telnet auth required pam_unix_cred.so.1
   telnet auth required pam_unix_auth.so.1
4. Add the line:
   telnet auth required pam_securid.so

Configure login

To configure login to work with the PAM agent:

1. Change to the **/etc** directory.
2. Open the **pam.conf** file, and scroll to the Authentication Management section.
3. Comment the following lines, if they exist:
   login auth requisite pam_authtok_get.so.1
   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
4. Add the line:
   login auth required pam_securid.so

Configure ssh and Related Tools

To configure ssh and related tools such as scp and sftp to work with the PAM agent:

1. Change to the **/etc** directory.
2. Open the **pam.conf** file, and scroll to the Authentication Management section.
3. Comment the following lines, if they exist:
   sshd-kbdint auth requisite pam_authtok_get.so.1
   sshd-kbdint auth required pam_dhkeys.so.1
   sshd-kbdint auth required pam_unix_cred.so.1
   sshd-kbdint auth required pam_unix_auth.so.1
4. Add the line:
   sshd-kbdint auth required pam_securid.so

Configure rlogin

To configure rlogin to work with the PAM agent:

1. Change to the **/etc** directory.
2. Open the **pam.conf** file, and scroll to the Authentication Management section.

3. Comment the following lines, if they exist:
   ```
   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
   ```
4. Add the line:
   ```
   rlogin auth required pam_securid.so
   ```

Configure ftp

To configure ftp to work with the PAM agent:

1. Change to the **/etc** directory.
2. Open the **pam.conf** file, and scroll to the Authentication Management section.
3. Comment the following lines, if they exist:
   ```
   ftp auth requisite pam_authtok_get.so.1
   ftp auth required pam_dhkeys.so.1
   ftp auth required pam_unix_cred.so.1
   ftp auth required pam_unix_auth.so.1
   ```
4. Add the line:
   ```
   ftp auth required pam_securid.so
   ```

Configure sudo

To configure sudo to work with the PAM agent:

1. Change to the **/etc directory**.
2. Open the **pam.conf** file, and scroll to the Authentication Management section.
3. Comment the following lines, if they exist:
   ```
   sudo auth requisite pam_authtok_get.so.1
   sudo auth required pam_dhkeys.so.1
   sudo auth required pam_unix_cred.so.1
   sudo auth required pam_unix_auth.so.1
   ```
4. Add the line:
   ```
   sudo auth required pam_securid.so
   ```

Configure dtlogin

To configure dtlogin to work with the PAM agent:

1. Change to the **/etc directory**.
2. Open the **pam.conf** file, and scroll to the Authentication Management section.

3. Comment the following lines, if they exist:
   dtlogin auth requisite pam_authtok_get.so.1
   dtlogin auth required pam_dhkeys.so.1
   dtlogin auth required pam_unix_cred.so.1
   dtlogin auth required pam_unix_auth.so.1
4. Add the line:
   dtlogin auth required pam_securid.so

Configuring the Agent

You can customize the PAM agent configuration to use the agent features, and the UNIX features supported by the agent. Before you make any configuration changes, make backup copies of the original configuration files.

On Solaris 10, a single configuration file named **pam.conf** is located in the **/etc** directory.

The following table lists the various features that can be configured on the agent.

Task	Reference
Enable debug output	"Enable Debug Output" on page 9
Enable SecurID Trace Logging	"Enable SecurID Trace Logging" on page 10
Use stackable modules	"Configure Stackable Modules" on page 10
Use reserve passwords	"Use Reserve Passwords" on page 11
Enable Selected SecurID authentication	"Enable Selected SecurID Authentication" on page 11

Enable Debug Output

To enable debug output for the PAM agent, edit the configuration file by adding a debug argument as described below. For more information, see "System Log Messaging" on page 18.

The configuration file **pam.conf** is located in the **/etc/** directory

To enable debug output for a particular tool, on all supported versions:

1. Change to the **/etc** directory and open the **pam.conf** file.
2. Add debug as an argument for pam_securid.so module:
   <tool name> auth required pam_securid.so debug

Enable SecurID Trace Logging

To enable logging for the PAM agent and for the authentication utilities acetest and acestatus, set the following variables in the **/etc/sd_pam.conf** file.

RSATRACELEVEL=<value>

- This variable enables detailed agent logging and sets the level of logging. The default value is 0.

Value	Description
0	Disables logging
1	Logs regular messages
2	Logs function entry points
4	Logs function exit points
8	All logic flow controls use this (ifs)

Note: For combinations, add the corresponding values. For example, to log regular messages and function entry points, set the value to 3.

- RSATRACEDEST=<filepath>

Specify the file path where the logs must be redirected. By default this is blank. If you do not set this variable in **/etc/sd_pam.conf**, the logs go to standard error for authentication utilities acetest and acestatus, and no logs are generated for authentication tools, even if the RSATRACELEVEL value has been specified.

Note: Default values refer to values when the agent is installed.

Configure Stackable Modules

The PAM agent can be used in a stacked configuration. You can use the agent to integrate the RSA SecurID PAM authentication module with other PAM authentication modules in your environment. You can configure the priority of authentication challenges by editing the appropriate configuration file—**/etc/pam.conf**.

In a stacked configuration, the password or passcode is passed from the previous authentication module. The agent also passes parameters to the next authentication module, and is qualified to work with the arguments—use_first_pass and try_first_pass:

use_first_pass. When this argument is used, the agent uses only the password or passcode passed from the previous module, and denies access if the credentials do not match. The user is not prompted for authentication again.

try_first_pass. When this argument is used, the agent uses the password or passcode passed from the previous module. If the credentials do not match, the user is prompted for authentication.

The following section describes how to configure a connection tool (login tool) in a stacked environment on Solaris 10.

To configure the connection tool (login) to work in a stacked environment:

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
   ```
2. Comment the above lines.
3. Add the following lines:
   ```
   login auth required pam_securid.so
   login auth required pam_ldap.so
   ```

Use Reserve Passwords

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

Note: The UNIX password serves as the reserve password.

To use reserve passwords with a particular tool, on all supported versions:

1. Change to **/etc** and open the **pam.conf** file.
2. Add reserve as an argument to the pam_securid.so module.
   ```
   <tool name> auth required pam_securid.so reserve
   ```

Enable Selected SecurID Authentication

You can configure the agent to selectively always prompt or never prompt users or groups for authentication.

Task	Reference
Enabling selective UNIX group authentication	"Enable Selective SecurID Authentication for UNIX Groups" on page 12

Task	Reference
Enabling selective UNIX user authentication	"Enable Selective SecurID Authentication for UNIX Users" on page 13

When selective group support and selective user support are both enabled, selective user support is considered.

The following table lists the possible values which can be set in the **sd_pam.conf** file.

ENABLE_GROUPS _SUPPORT	ENABLE_USERS _SUPPORT	Result
0	0	Neither feature is enabled.
0	1	Selected User support is enabled.
1	0	Selected Group support is enabled.
1	1	Selected User support is enabled.

Enable Selective SecurID Authentication for UNIX Groups

You can configure the PAM agent to always prompt specific groups to authenticate with SecurID, or to never prompt specific groups to authenticate with SecurID.

Group members excluded from SecurID authentication can be authenticated either with UNIX credentials or through another PAM module in the stack. This can be configured with the PAM_IGNORE_SUPPORT parameter.

Note: Do not specify Authentication Manager groups. This feature is for UNIX groups only.

To enable selective SecurID Authentication for UNIX groups:

1. Change to the **/etc** directory, and open the **sd_pam.conf** file.
2. Set the ENABLE_GROUP_SUPPORT parameter to 1. The default value is 0.
3. Populate the LIST_OF_GROUPS parameter.
4. Set the value for the INCL_EXCL_GROUPS parameter.
   The possible values are:
   - 0—Disable SecurID authentication for the listed groups.
   - 1—Enable SecurID authentication only for the listed groups.

   The default value is 0.
5. (Optional) Set the PAM_IGNORE_SUPPORT parameter.
   The possible values are:
   - 0—Enable UNIX password authentication.

- 1—Disable UNIX password authentication.

The default value is 0.

Note: This parameter is applicable only to groups excluded from SecurID authentication.

6. Save the file.

Note: Default values refer to values when the agent is installed.

Enable Selective SecurID Authentication for UNIX Users

You can configure the PAM agent to always prompt specific users to authenticate with SecurID, or to never prompt specific users to authenticate with SecurID.

Users excluded from SecurID authentication can be authenticated either with UNIX credentials or through another PAM module in the stack. This can be configured with the PAM_IGNORE_SUPPORT_FOR_USERS parameter.

To enable selective SecurID Authentication for UNIX users:

1. Change to the **/etc** directory, and open the **sd_pam.conf** file.
2. Set the ENABLE_USERS_SUPPORT parameter to 1. The default value is 0.
3. Populate the LIST_OF_USERS parameter.
4. Set the value for the INCL_EXCL_USERS parameter.

   The possible values are:

   - 0—Disable SecurID authentication for the listed users.
   - 1—Enable SecurID authentication only for the listed users.

   The default value is 0.
5. (Optional) Set the PAM_IGNORE_SUPPORT_FOR_USERS parameter.

   The possible values are:

   - 0—Enable UNIX password authentication.
   - 1—Disable UNIX password authentication.

   The default value is 0.

   Note: This parameter is applicable only to users excluded from SecurID authentication.
6. Save the file.

Note: Default values refer to values when the agent is installed.

Known Configuration Issues

This section describes known issues with tools on Solaris.

Tool	Known Issue
ftp	When you use SecurID to protect ftp, SecurID authentication prompts and error messages are not displayed to users. Only standard operating system (OS) prompts and error messages are displayed. Note the following: • Users enter their user name at the OS user name prompt, and their SecurID passcode at the OS password prompt. • If a user is uncertain as to the status of a token (for example, if the token is in the Next Tokencode mode, or the 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.
ssh	After three unsuccessful SecurID authentication attempts are made in a single session, the connection is closed. You must terminate the session, and start another session.
rlogin, 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 the 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.
All	In a stacked configuration, with the following configuration (UNIX after SecurID), UNIX authentication is ignored: <toolname> auth sufficient pam_securid.so debug <toolname> auth requisite pam_authtok_get.so.1 <toolname> auth required pam_dhkeys.so.1 <toolname> auth required pam_unix_cred.so.1 <toolname> auth required pam_unix_auth.so.1 If the wrong SecurID password is entered, the user should be prompted for the UNIX password. Instead, the passcode prompt is displayed again.

Uninstall the RSA Authentication Agent 7.0 for PAM

This section provides information on how to uninstall the 7.0 agent for PAM.

Before you Begin

- Configure the RSA SecurID protected tools to use the standard PAM module provided with your operating system.
- Verify that you have root permissions on the host.

To uninstall the PAM agent:

1. Change to the PAM agent home directory.
2. Run the uninstall script. Type:

   ./uninstall_pam.sh

Next Step

Verify that the installation directory has been removed. If the directory still exists, you must remove it manually.

Troubleshooting

This section describes how to troubleshoot using the various utilities of the PAM agent.

Authentication Utilities

The authentication utilities are located in the following directories:

- 32-bit operating system: **<pam agent home>/bin/32bit**
- 64-bit operating system: **<pam agent home>/bin/32bit** and **<pam agent home>/bin/64bit**

Use these utilities to:

- Perform a test authentication. For more information, see "acetest."
- Verify communication between the PAM agent and the Authentication Manager. For more information, see "acestatus."

You can enable logging for these utilities. For more information, see "Enable SecurID Trace Logging" on page 10.

acetest

This utility checks that the agent is functioning properly, by performing a test authentication.

To perform a test authentication:

1. Change to the PAM agent authentication utilities directory.
2. Type:

   ./acetest
3. Enter a valid user name and passcode.

If you are repeatedly denied access, test the Authentication Manager status. For more information, see "acestatus" on page 16, or contact your Authentication Manager administrator.

acestatus

This utility checks the status of each Authentication Manager on which the PAM agent is registered as an agent host.

To check the Authentication Manager status:

1. Change to the PAM agent utilities directory.
2. Type:

   ./acestatus

This gives information on the Authentication Manager server including server name and address.

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

The following table lists the information displayed in the Authentication Manager section.

Returned Information	Description
Configuration Version	The version of the **sdconf.rec** file that is in use. For Authentication Manager 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 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 Authentication Manager.
Server Release	The version number of Authentication Manager.
Communication	The protocol version used by Authentication Manager and the PAM agent.

The following table lists the status information displayed in the Authentication Manager section.

Status Information	Description
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 0.0.0.0 indicates that the agent has not yet received communication from the server.

The following table lists the server status information displayed in the Authentication Manager section.

Server Status	Description
Available for Authentications	This 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.

Conversion Utility

The conversion utility is used when:

- Upgrading to the 7.0 agent.
- The PAM agent co-exists with other SecurID agents.

ns_conv_util

The conversion utility ns_conv_util is located in the following directories:

- 32-bit operating system: **<pam agent home>/bin/32bit**
- 64-bit operating system: **<pam agent home>/bin/32bit** and **<pam agent home>/bin/64bit**

To run the conversion utility:

1. Change to the PAM agent utilities directory.
2. Type **./ns_conv_util**. and give the path to the existing SecurID file location in the machine as first parameter and new destination location of SecurID file as the second parameter.

```
./ns_conv_util <Existing_Securid_file_path>
```

```
    <New_Securid_dir_path>
```

where:

- Existing_Securid_file_path is the path where the SecurID file exists.
- New_Securid_dir_path is the directory where the newly generated SecurID file should be stored.

For example:

./ns_conv_util /var/ace/securid /var/ace_pam/

If the new destination location is not the same as the location pointed out by VAR_ACE, you must copy the new securid file to this location.

System Log Messaging

By default, several PAM agent authentication messages are recorded in the system log. For tracing purposes, you can configure your system log to record all PAM agent authentication log messages. See "Enable Debug Output" on page 9.

Configure the System Log

To send all authentication messages to the system log:

1. Change to the **/etc/** directory.
2. Open the **syslog.conf** file.
3. Add auth.notice parameter to the line that specifies your system log file.
4. Remove the authpriv.none parameter, if it is specified for the system log file.
5. If you are using telnet or login, add authpriv.notice parameter to the line that specifies the system log file.
6. Save your changes.
7. Restart the syslog daemon.

PAM Agent Authentication Log Messages

The following table lists the authentication log messages.

Message	Description
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 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 is set properly.

Message	Description
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 Authentication Manager is unable to process authentication requests.
User name 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.

Critical File Information

In addition to the binaries (**pam_securid.so**, **acetest**, **acestatus, and ns_conv_util**), the PAM agent maintains the critical files listed in the following table.

File	Description
sdconf.rec	This file is generated by Authentication Manager server, and contains configuration information that controls the behavior of the PAM agent. This file permission should be -rw------- root root.
sdstatus.1	This file is generated by the authentication API to track the last known status of the SecurID Authentication Manager servers. This file permission should be -rw------- root root.
securid	This file contains a shared secret key used to protect the communication between the local machine and Authentication Manager. The name of this file is derived from the local system's configured protocol name for the port over which the agent communicates with Authentication Manager, usually via the "services" file. This file permission should be -r-------- root root. However, it also depends on the OS Umask setting.

File	Description
/etc/sd_pam.conf	Contains configuration settings that control behavior of the PAM agent. This file permission should be -rw-r--r-- root root.

Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Solutions Directory	**www.rsasecured.com**

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 Customer Support

Make sure that 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.

November 2010

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf.**