

RSA PAM Module Installation on Solaris 10 OS Platform

Preparation

Copy the tar file, PAM-Agent_v7.1.0.1.16.05_06_13_02_04_01.tar, to an installation directory and untar it.

```
# tar xvf PAM-Agent_v7.1.0.1.16.05_06_13_02_04_01.tar

# ls -l
total 18989
-rw-r--r--  1 root      root      9218560 Jun 23 08:35
Agent_v7.1.0.1.16.05_06_13_02_04_01.tar
-rwxrwxrwx  1 root      root      245631 Jun 18  2008 PAMAgent.pdf
-rwxrwxrwx  1 root      root      55629 Jun 18  2008 PAMreadme.pdf
drwxrwxr-x  2 1047      900           3 Jun  3  2008 aix
drwxrwxr-x  2 1047      900           3 Jun  3  2008 hp11
drwxrwxr-x  2 1047      900           3 Jun  3  2008 hpitan
-r-xr-xr-x  1 1047      900      17190 Jun  3  2008 install_pam.sh
-r-xr-xr-x  1 1047      900      20801 Jun  3  2008 license.txt
-r-xr-xr-x  1 1047      900      19757 Jun  3  2008 license2.txt
drwxrwxr-x  2 1047      900           3 Jun  3  2008 lnx32
drwxrwxr-x  2 1047      900           3 Jun  3  2008 lnx64
drwxrwxr-x  3 1047      900           4 Oct 11 15:22 sparc
drwxrwxr-x  2 1047      900           3 Jun  3  2008 sol_x86
-r-xr-xr-x  1 1047      900       9041 Jun  3  2008 uninstall_pam.sh
```

Prepare PAM Module Run Time Environment

```
# mkdir /var/ace
Copy sdconf.rec into /var/ace

# cp sdconf.rec /var/ace
# chown root:root /var/ace/sdconf.rec
```

Installation

```
# cd sparc (for x86, cd sol_x86)
# ./install_pam.sh
```

```
ARE YOU A CUSTOMER ORDERING THIS RSA PRODUCT FROM RSA SECURITY INC., FROM
EITHER NORTH AMERICA, SOUTH AMERICA OR THE PEOPLE'S REPUBLIC OF CHINA
(EXCLUDING HONG KONG): (y/n) [y] <Return>
```

LICENSE AGREEMENT

(License agreement skipped.)

Do you accept the License Terms and Conditions stated above? (Accept/Decline)
[D] **A**

Enter Directory where sdconf.rec is located [/var/ace] **<Return>**

Please enter the root path for the RSA Authentication Agent for PAM directory
[/opt] **<Return>**

The RSA Authentication Agent for PAM will be installed in the /opt directory.

x pam, 0 bytes, 0 tape blocks
x pam/doc, 0 bytes, 0 tape blocks
x pam/lib, 0 bytes, 0 tape blocks
x pam/lib/pam_securid.so, 369420 bytes, 722 tape blocks
x pam/bin, 0 bytes, 0 tape blocks
x pam/bin/acestatus, 185368 bytes, 363 tape blocks
x pam/bin/acetest, 323764 bytes, 633 tape blocks

Checking /etc/sd_pam.conf:

VAR_ACE does not exist - entry will be appended
ENABLE_GROUP_SUPPORT does not exist - entry will be appended
INCL_EXCL_GROUPS does not exist - entry will be appended
LIST_OF_GROUPS does not exist - entry will be appended
PAM_IGNORE_SUPPORT does not exist - entry will be appended
AUTH_CHALLENGE_USERNAME_STR does not exist - entry will be appended
AUTH_CHALLENGE_RESERVE_REQUEST_STR does not exist - entry will be appended
AUTH_CHALLENGE_PASSCODE_STR does not exist - entry will be appended
AUTH_CHALLENGE_PASSWORD_STR does not exist - entry will be appended

* You have successfully installed RSA Authentication Agent 7.1 for PAM

SecurID Verification Test

Note that the test requires a user name and passcode <PIN + token code>.

As a root-privilege user, test PAM module as shown below:

```
# cd /opt/pam/bin/  
# ./acetest  
Enter USERNAME: <user_id>  
Enter PASSCODE: <PIN + tokencode>
```

The result should be successful (as indicated below) if the user credential is correct.

Authentication successful.

Note that in some cases, the RSA SecurID token is in the status of "next tokencode" mode. If that is the case, the test session will look like this:

```
# ./acetest
Enter USERNAME: <user_id>
Enter PASSCODE: <PIN + tokencode1>
Wait for the tokencode to change,
then enter the new tokencode: <tokencode2>
Authentication successful.
```

If authentication testing is not successful, please contact The JPL Service Desk.

SSH Client Verification Test

DO NOT CLOSE THE WINDOW UNTIL YOU'VE CONFIRMED THAT AUTHENTICATION IS WORKING PROPERLY.

With the current root window still open, on a separate SSH client, login to the host on which the Authentication Agent is installed and PAM module is configured. The login should prompt for **PASSCODE** after username is entered.