

RSA PAM Authentication Agent Installation on RedHat Linux

Contact JPL Service Desk to have the system added as a TFA authentication agent.

Prepare PAM Authentication Agent Environment

Download Authentication Agent configuration file from

```
https://dir.jpl.nasa.gov/tfa/sdconf/sdconf.rec
```

Copy sdconf.rec into /var/ace

```
# mkdir /var/ace
# cp sdconf.rec /var/ace
# chown root:root /var/ace/sdconf.rec
# VAR_ACE="/var/ace/"
# echo $VAR_ACE
/var/ace/
```

Edit or create the client configuration file:

```
# vi /var/ace/sdopts.rec
CLIENT_IP=<host_IP_address>
```

Save file and exit (:wq)

Perform PAM Authentication Agent installation

Download PAM-Agent_v7.0.0.29 from [https://dir.jpl.nasa.gov/tfa/PAM-](https://dir.jpl.nasa.gov/tfa/PAM-Agent_v7.0.1.29.02_25_11_04_30_33.tar)

```
Agent_v7.0.1.29.02_25_11_04_30_33.tar
```

Untar file

```
# tar xvf PAM-Agent_v7.0.0.29.02_25_11_04_30_33.tar.gz
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/sparc/
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/sparc/sd_pam_agent.tar
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/aix/
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/aix/sd_pam_agent.tar
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/hp_itanium/
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/hp_itanium/sd_pam_agent.tar
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/lnx/
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/lnx/sd_pam_agent.tar
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/sol_x86/
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/sol_x86/sd_pam_agent.tar
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/install_pam.sh
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/uninstall_pam.sh
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/license.txt
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/Release_Notes/
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/Release_Notes/Images/
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/Release_Notes/Images/small_logo.gif
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/Release_Notes/release_notesPAMAgent70P1.html
PAM-Agent_v7.0.0.29.02_25_11_04_30_33/Release_Notes/styles/
```

```

PAM-Agent_v7.0.0.29.02_25_11_04_30_33/Release_Notes/styles/rel_notes_style.css
# cd PAM-Agent_v7.0.0.29.02_25_11_04_30_33

# ./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
*** IMPORTANT ***
PLEASE READ CAREFULLY BEFORE CONTINUING WITH THIS INSTALLATION. AT THE END
OF THE LICENSE TERMS AND CONDITIONS STATED BELOW, CUSTOMER WILL BE ASKED TO
ACCEPT OR REJECT SUCH TERMS. BY INDICATING ITS ACCEPTANCE, CUSTOMER AGREES
TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT.
<skipped>
*****
Do you accept the License Terms and Conditions stated above? (Accept/Decline)
[D] Accept
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.
pam/ pam/doc/ pam/lib/ pam/lib/pam_securid.so pam/bin/ pam/bin/acestatus
pam/bin/acetest
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 6.0 for PAM
*****

```

RSA 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/64bit
# ./acetest
Enter USERNAME: <username>
Enter PASSCODE: <PIN + token>

```

"Authentication successful" should appear if the user credential is correct. Otherwise, contact JPL Service Desk for assistance.

Configuration PAM to support SSH Server with SecurID Credentials

Edit both sshd and sudo files

For RHEL4:

```
# vi /etc/pam.d/sshd
```

(Comment the line [insert a hash symbol before the line]:)

```
#auth required pam_stack.so service=system-auth
```

(Insert the following line below the newly commented line:)

```
auth required pam_secured.so
```

Save file and exit.

```
# vi /etc/pam.d/sudo
```

(Comment the line [insert a hash symbol before the line]:)

```
#auth required pam_stack.so service=system-auth
```

(Insert the following line below the newly commented line:)

```
auth required pam_secured.so
```

Save file and exit (:wq).

For RHEL5

```
# vi /etc/pam.d/sshd
```

(Comment the line [insert a hash symbol before the line]:)

```
#auth include system-auth
```

(Insert the following line below the newly commented line:)

```
auth required pam_secured.so
```

Save file and exit (:wq).

```
# vi /etc/pam.d/sudo
```

(Comment the line [insert a hash symbol before the line]:)

```
#auth include system-auth
```

(Insert the following line below the newly commented line:)

```
auth required pam_secured.so
```

Save file and exit (:wq).

For RHEL6

```
# vi /etc/pam.d/sshd
```

(Comment the line [insert a hash symbol before the line]:)

```
#auth include password-auth
```

(Insert the following line below the newly commented line:)

```
auth required pam_secured.so
```

Save file and exit (:wq).

```
# vi /etc/pam.d/sudo
```

(Comment the line [insert a hash symbol before the line]:)

```
#auth include system-auth
```

(Insert the following line below the newly commented line:)

```
auth required pam_secured.so
```

Save file and exit (:wq).

For RHEL7

```
# vi /etc/pam.d/sshd
```

(Comment the line [insert a hash symbol before the line]:)

```
#auth include password-auth
```

(Insert the following line below the newly commented line:)

```
auth substack secured-auth
```

Save file and exit (:wq).

```
# vi /etc/pam.d/secured-auth
```

(Insert the following below the "auth required pam_env.so" line:)

```
auth sufficient pam_secured.so
```

Save file and exit (:wq).

```
# vi /etc/pam.d/sudo
```

(Comment the line [insert a hash symbol before the line]:)

```
#auth          include          system-auth
```

(Insert the following line below the newly commented line:)

```
auth include securid-auth
```

Save file and exit (:wq).

Configuration SSH Server with SecurID Credentials

```
# vi /etc/ssh/sshd_config
```

(Modify the lines as given below.)

```
PermitRootLogin no  
PasswordAuthentication no  
ChallengeResponseAuthentication yes  
UsePrivilegeSeparation no
```

Save file and exit (:wq). #

```
/etc/init.d/sshd restart
```

SSH Client Verification Test

WARNING: 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 the Authentication Agent was installed and PAM module is configured. The login should prompt for PASSCODE after username is entered.