RSA ACE/Agent 5.2 for UNIX
Installation and Configuration Guide

Contact Information

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

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
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.

RSA Security Notice

First printing: October 2003

RSA ACE/Agent 5.2 for UNIX

This guide provides instructions for

- Performing pre-installation tasks
- Installing RSA ACE/Agent 5.2 for UNIX
- Performing post-installation tasks

Supported Platforms and Hardware

RSA ACE/Agent 5.2 for UNIX is supported on

- ❑ HP-UX 11i running on PA-RISC 2.x processors
- ❑ IBM AIX 5L v 5.1 or 5.2 on PowerPC and RISC/6000 processors
- ❑ Solaris 8 and Solaris 9 on UltraSPARC processors

Pre-Installation Tasks

Before you install this Agent, perform all steps in this section to prepare each workstation.

Note: You must have root permissions on the workstation.

To prepare a UNIX workstation:

1. Log in to the workstation as **root**.
2. Create a temporary directory. Type

   ```
   mkdir /agent_tmp
   ```

3. Specify an installation directory. This can be an existing directory or a new one that you create.

   Important: Your installation directory should have at least 5MB of disk space available.

4. Verify that the hostname of the workstation can be resolved from the RSA ACE/Server. If you do not know the hostname of the workstation, issue the **hostname** command.
5. Use the **ping** or **telnet** command to verify that the hostnames of the RSA ACE/Server can be resolved from the workstation.
6. On the RSA ACE/Server, check the name and port number of the authentication service by running **sdinfo** or by opening the **/etc/services** file.

   If you are *not* using NIS, the authentication service name and port number must also be the **/etc/services** file on the workstation.

7. Change to the temporary directory. Type
   ```
   cd /agent_tmp
   ```
8. Copy the RSA ACE/Server configuration file (**sdconf.rec**) from the Primary Server to the temporary directory. If you use **ftp**, perform the transfer in binary mode.

Installing RSA ACE/Agent 5.2 for UNIX

This installation procedure assumes that you have

- Successfully downloaded the RSA ACE/Agent 5.2 for UNIX from the RSA Security website
- Untarred the appropriate file to the temporary directory that you created in step 2 of the previous section.

Note: RSA Security recommends that you do not install RSA ACE/Agent 5.2 for UNIX on a machine that already has the RSA ACE/Server installed.

To install RSA ACE/Agent 5.2 for UNIX:

1. Change to your temporary directory. Type
   ```
   cd /agent_tmp
   ```
2. Start the installation program. Type
   ```
   aceagent/platform/sdsetup -agent [-o yes] [-p path]
   ```
   where *platform* is the operating system on which you are installing.
   The following table explains the parameters.

-o yes | no	This parameter allows you to reinstall without first having to remove existing files. When you specify **yes**, the installation program moves all existing files to **ace_tmp**, overwriting the current contents of **ace_tmp**. When you specify **no**, the installation program terminates, allowing you to move all existing files to another location. Once files are move to **ace_tmp**, you can delete them or move them to another location. If you do not move or back up the files in **ace_tmp** before you reinstall the Agent, the contents of **ace_tmp** are permanently lost. **Important:** When you complete the installation, be sure to copy **sdstatus.12** and **sdopts.rec** from **ace_tmp/data** to your installation directory. You need these files to perform test authentications and to configure load balancing. For information on load balancing, see the section "Load Balancing by Agent Hosts" in the chapter "Agents and Activation on Agent Hosts" in the *RSA ACE/Server 5.2 Administrator's Guide*. For information on performing test authentications, see the section "Performing a Test Authentication" in the chapter "Installing the RSA ACE/Server" in the *RSA ACE/Server 5.2 for UNIX Installation Guide*. If you are upgrading and you have already configured a shell script for AIX 5L in your current version, be sure to copy the script from **ace_tmp/prog** to your installation directory. For more information, see "Configuring RSA ACE/Agent 5.2 for UNIX on AIX 5L" on page 6.
-p *path*	This parameter specifies the pathname of the top-level directory where you want all RSA ACE/Agent subdirectories and files to be located.

Post-Installation Tasks

When the installation program **sdsetup -agent** is complete, configuration information is displayed. Review this information, taking special note of the host IP address and encryption values. If the error messages **unable to resolve** and **Error: gethostbyname failed** appear in the CLIENT ADDRESS field, verify:

- The correct name of the host in the **/etc/hosts** file.
- That your name resolution service is functioning properly.

To add this Agent Host to the RSA ACE/Server database, follow the instructions in the chapter "Agents and Activation on Agent Hosts" in the *RSA ACE/Server 5.2 Administrator's Guide*.

Preparing for RSA SecurID Authentication

You should develop an implementation plan for introducing RSA SecurID to end users. For more information, see the section "Planning Token Deployment" in the *RSA ACE/Server 5.2 Deployment Guide.*

Configuring RSA ACE/Agent 5.2 for UNIX on Solaris and HP

You can configure a user's login procedure to use RSA SecurID by specifying **sdshell** as the user's default shell. Ensure that the user's UNIX system default shell is specified in the default shell field of the user record in the RSA ACE/Server database. To modify a user's record, see the topic "Edit User" in the RSA ACE/Server Help.

You can use **sdshell** on Agent Hosts that use a name service such as NIS.

RSA SecurID authentication is required on Solaris and HP for *all* access to resources using the login of a designated RSA SecurID user. For system administrators who prefer using the **su** command without having to provide an RSA SecurID passcode, a third authentication shell (**sdshell_adm**), is provided.

Note: Do not use **sdshell_adm** where **sdshell_auth** is required.

Users who are designated to use any of the **sdshell** programs are prompted for an RSA SecurID passcode whenever they attempt to log in. When the user responds to the prompt, the **sdshell** encrypts the input and sends it to the RSA ACE/Server. If the passcode is valid, the Agent Host displays **PASSCODE Accepted** and the user's working shell is executed.

Note: ISDN channel binding is not supported.

To configure Solaris and HP Agent Hosts:

1. Add ***ACEPROG*/sdshell** to the **/etc/shells** file. ***ACEPROG*** represents the full pathname of the RSA ACE/Server program directory.
2. Edit the user's entry in the **/etc/passwd** file (or information service) to specify that this shell is the program **sdshell**. For example, change

   ```
   login:pwd:268:0:username:/disk/homedir/logname: /bin/csh
   ```

   to the following:

   ```
   login:pwd:268:0:username:/disk/homedir/logname:
   ACEPROG/sdshell
   ```

When the user authenticates using RSA SecurID, **sdshell** executes the shell specified in the Agent Host activation record for this login name. For information about specifying a shell for RSA SecurID users, see the topic "Add User" in the RSA ACE/Server 5.2 Help.

Configuring RSA ACE/Agent 5.2 for UNIX on AIX 5L

Note: This Agent does not support the use of NIS (Network Identification Service) on AIX 5L.

On AIX systems, specify **sdshell_auth** as a *primary* authentication method to invoke RSA SecurID passcode prompting.

When you use this method, the user's destination shell (for example, the working shell run after the login procedure is completed) is the shell stored in the user's /etc/password entry. The system disregards any destination shell specified when the user or the user's group was activated on the Agent Host.

To configure AIX 5L Agent Hosts:

1. In the ***ACEPROG*** directory, create a shell script containing the following lines:

   ```
   #!/bin/sh
   installation path/sdshell_auth $*
   exit $?
   ```

   where *installation path* is the full path to the ***ACEPROG*** directory.
2. Set the permissions and ownership of the file to

   ```
   ---s--x--x    root
   ```

3. As **root**, edit **/usr/lib/security/methods.cfg**. Add this line:

   ```
   SECURID:

   program = ACEPROG/<shell script name>
   ```

   where <*shell script name*> is the name of the shell script you created in step 1.
4. If you prefer to perform the configurations using **smit**, go to step 6. Otherwise, go to step 5.

5. As **root**, edit **/etc/security/user**. To require RSA SecurID for all users, make the following changes:

   Under **Default**, change the system and auth1 lines to

   ```
   SYSTEM = "NONE"
   auth1 = SECURID
   ```

   To require RSA SecurID for individual users, under each user's login name, add

   ```
   SYSTEM = "NONE"
   auth1 = SECURID
   ```

6. To perform the configurations using **smit**, do the following:
   - Select **Security and Users**.
   - Select **Users**.
   - Select **Change/Show Characteristics of a user**.
   - Specify the user's name.
   - Change the login authentication grammar line to

     ```
     Login AUTHENTICATION GRAMMAR     NONE
     ```

   - Change the primary authentication method line to

     ```
     PRIMARY authentication method    SECURID
     ```

Configuring X Window Logins

This section explains how to modify X Window files of users designated for RSA SecurID authentication. Without these modifications, X Window logins will not be protected by RSA SecurID.

For X Window logins to be authenticated by RSA SecurID, each of the following conditions must be true:

- The X client login program that controls your X displays must be **xdm** or a vendor equivalent (that is, **vuelogin** for HP).
- The RSA ACE/Server **Xprompt** script must be added to the end of the startup file or files.
- The session file or files must set each user's shell variable as defined in the RSA ACE/Server database.

To configure X Window Logins:

Note: If you are using AIX, perform step 1 through step 5 of this procedure. If you are using Solaris or HP-UX, perform step 2 through step 7 of this procedure.

1. Specify a domain name to serve as an entry point for X Window Login access. Edit the **/usr/dt/config/Xaccess** file by adding a line equivalent to the following:

   ```
   *your_domain_name.com
   ```

2. Edit the display configuration file (**Xconfig** or **xdm-config**) by removing the # at the beginning of the following line:

   ```
   #Dtlogin*authorize: False
   ```

   Important: This parameter must be set to "False".

3. Locate the display manager configuration file for your system.

   The usual path and filename for the display manager configuration file is **/usr/dt/config/Xconfig**. The file on your system may have a different location and name.

4. View the contents of the configuration file (**Xconfig** or **xdm-config**). Although the file may state that it must be located in the standard configuration directory, for the purposes of working with the RSA ACE/Server this is not required.

5. In the configuration file, find the full path and filename of each startup file on your system. For example, on an AIX or Solaris system running the Common Desktop Environment (CDE), you might see

   ```
   Dtlogin*startup:        /usr/dt/bin/Xstartup
   ```

   In this example, which is typical, there is one startup file called **Xstartup** and it is in the same directory as the configuration file. While the startup file could have a different name and be in a different directory, it will be in this form:

   ```
   displaymanagername*startup:[path]
   startupfilename
   ```

   Note: If the full path is not specified, the system looks in default directories to find the specified startup file. RSA Security recommends that you copy your **XConfig** and **Xstartup** files to the **/etc/dt/config** directory and edit them in that directory.

   Add the **Xprompt** script to all startup files referenced in the configuration file. Copy the **Xprompt** file from the Agent Host ***ACEPROG*** directory into each startup file. **Xprompt** scripts must go at the end of the startup file.

6. View the contents of the configuration file (**Xconfig** or **xdm-config**) to find the full path and filename of each session file on your system. For example, on an AIX or Solaris system running CDE, you might see

   ```
   Dtlogin*session:      /usr/dt/bin/Xsession
   ```

   In this example, which is typical, there is one session file called **Xsession**, and it is in the same directory as the configuration file. While the session file could have a different name and be in a different directory, it will be in this form:

   ```
   displaymanagername*session: path/sessionfilename
   ```

   There may be additional Xsession files not referenced in the configuration file. Look in the following locations for Xsession files:

   Solaris

   ```
   /usr/dt/config/Xsession*
   /usr/dt/bin/Xsession*
   ```

   HP

   ```
   /usr/vue/config/Xsession*
   /usr/vue/bin/Xsession*
   ```

   Note: If the /usr/vue/config/Xsession* invokes the /usr/vue/bin/Xsession, then only one of them needs to be modified in step 7.

7. For each session file on the system, perform the following step:

   At the beginning of the file or before execution of any kind of terminal-emulating **X client** program, add the following lines to add a reference to the user's default shell as defined in the RSA ACE/Server database.

   Important: Spacing is critical to proper functioning of the script. Be certain to follow the spacing exactly as shown in the example below. Put a single space where you see gaps between characters. Do not use spaces if the characters shown above are abutting. Specifically, there are exactly nine space characters in this script: there must be a space on both sides of each square bracket, between the **-n** and the open quote, on both sides of each semicolon, and between **export** and **SHELL**.

   ```
   TESTSHELL=‘ACEPROG/sdfindshell‘
   if   [   -n   ”$TESTSHELL”   ]   ;   then
   SHELL=$TESTSHELL   ;   export   SHELL
   fi
   ```

   Perform this step for each session file, whether or not the file is referenced in the configuration file.

   ACEPROG represents the full pathname of **ace/prog**, which holds all Server executables.

   Note: The single quotation marks in the first line of the script are backquotes (probably located on your keyboard with the ~ symbol). If you mistakenly use a forward quote mark (which is on the key with the double quote mark), the script will not work.

X Window Issues

Authentication Window Will Not Accept Input

If you have protected X Window logins and the window that prompts for a passcode does not function properly (cannot be focused on or will not accept input), contact the operating system vendor for patches.

HP VUE User Required to Enter PASSCODE for Each New Window

If an HP VUE user complains of having to enter an RSA SecurID passcode every time the user opens a new window, you could add the following line to the user's **.vueprofile** file:

```
SHELL=destinationshell; export SHELL
```

where *destinationshell* is the shell that opens for the user once authentication is successful. The repeated prompting occurs because the VUE manager inherits the default profile from the user's **/etc/login** file. **sdshell** is defined as the user's shell (required to have **Xstartup** call **sdprompt**), so the user is prompted for an RSA SecurID passcode every time the user opens a new window.

Refer to the HP VUE system administration manual for more details on **.vueprofile**, if necessary.

Login Prompt Continually Redisplays

If an X Window user is returned to the login prompt whenever he or she authenticates, check the accuracy of the shell script added to the **Xsession** file. The script must be entered in the **Xsession** file exactly as it appears on page 9. Verify that the quotation marks are single backquotes and that the spacing is correct.

If you find no errors in the shell script, the user may be experiencing an incompatibility of an X Window security feature and the RSA ACE/Server. Disabling the client authorization mechanism on the X server should resolve the problem.

To disable the X server client authorization mechanism:

1. Check that no one else is on the system.
2. Edit the display configuration file in the **/usr/dt/config** directory (**Xconfig** or **xdm-config**). Change the X Authorization Line from TRUE to FALSE.

   ```
   Dtlogin.terminal.authorize: FALSE
   ```

   where *terminal* is

   - a specific terminal (for example, _0 for the main console)
   - all terminals (specified with an asterisk *)
3. Reboot the system.

Note: If **xdm** is not configured to start up at boot time, start it manually with the **xdm&** command.