Readme
RSA Authentication Agent 6.0 for PAM

June 16, 2008

Introduction

This document lists what's new and changed in RSA Authentication Agent 6.0 for PAM (Pluggable Authentication Module). It includes additional installation information, as well as workarounds for known issues. Read this document before installing the software. This document contains the following sections:

This *Readme* may be updated. The most current version can be found on RSA SecurCare Online **https://knowledge.rsasecurity.com**.

Readme Revision History

Revision 1	10/06	Support information and known issues for Red Hat Linux AS, ES, and WS 4.0 (64-bit).
Revision 2	11/06	Support information and known issues for Solaris 10 x86 (32-bit) and HP-UX 11.0 and 11i (32-bit).
Revision 3	01/07	Additional known issues for Red Hat Linux AS 4.0 (64-bit).
Revision 4	02/07	Support information for Solaris 10 x64, Solaris 10 SPARC (64-bit), and HP-UX 11i v2 on Itanium.
Revision 5	06/07	Support information and known issues for AIX 5L v5.3 with TL5 (SP6) on 64-bit PowerPC processors, and SUSE Linux Enterprise Server 9 (SP3) and 10 on Intel Xeon and AMD Opteron 64-bit processors.
Revision 6	06/08	Support information for Red Hat Enterprise Linux AS, ES, and WS 4.6 (32-bit) and Red Hat Enterprise Linux 5.1 (Enterprise Server, Advanced Platform, and Desktop) 32-bit and 64-bit.

Platform Support

The PAM Agent is supported on the following operating systems:

- AIX 5L v5.3 with TL5 (SP6) on 64-bit PowerPC processors
- HP-UX 11.0 and 11i on RISC 32-bit processors
- HP-UX 11i v2 on Itanium 64-bit processors
- Red Hat Enterprise Linux AS, ES, and WS 4.0 on Intel Xeon and AMD Opteron 64-bit processors
- Red Hat Enterprise Linux AS, ES, and WS 4.6 on 32-bit processors
- Red Hat Enterprise Linux 5.1 (Enterprise Server, Advanced Platform, and Desktop) on 32-bit processors
- Red Hat Enterprise Linux 5.1 (Enterprise Server, Advanced Platform, and Desktop) on Intel Xeon and AMD Opteron 64-bit processors
- Solaris 10 on SPARC 64-bit processors
- Solaris 10 x64 on Intel Xeon and AMD Opteron 64-bit processors
- Solaris 10 x86 on Intel 32-bit processors
- SUSE Linux Enterprise Server 9 (SP3) and 10 on Intel Xeon and AMD Opteron 64-bit processors

For OpenSSH support, see the *Installation and Configuration Guide*.

What's New in This Release

This section describes the major changes introduced in this release. For detailed information, see the *Installation and Configuration Guide*.

Support for stackable modules. This feature allows you to prioritize the order of authentication challenges using RSA Authentication Agent 6.0 for PAM with other PAM modules on your network.

Note: FTP is not supported in a stackable environment with the PAM Agent.

Known Issues

This section explains issues that remain unresolved in this release. Wherever a workaround or fix is available, it has been noted or referenced in detail.

Note: For information on properly configuring the PAM Agent, and tips for assisting end users when they authenticate using RSA SecurID, see “Known Configuration Issues” in Chapter 2 of the *Installation and Configuration Guide*.

Additional Configuration to Support telnet and rlogin

Tracking Number: 108824
Problem: In a Red Hat Linux 5.1 environment, the telnet and rlogin tools do not work with the default **/etc/hosts** (loopback address) configuration.
Workaround: Configure the **/etc/hosts** file with the correct hostname and IP address, or appropriately configure the Domain Name System (DNS).

Test Authentication Fails But Supported Tools Can Authenticate

Tracking Number: 108319
Problem: In a Red Hat Linux environment, the acetest utility does not recognize the CLIENT_IP flag in **sdopts.rec** and the test authentication fails. Supported tools, such as telnet and rlogin, are able to authenticate.
Workaround: Add the hostname and IP address to the **/etc/hosts** file, or appropriately configure the Domain Name System (DNS).

Server Information Not Updated When a Replica Is Added or Removed

Tracking Number: 56419
Problem: When you add or remove a Replica Authentication Manager, the PAM Agent does not update its server information to recognize the change.
Workaround: Remove the **sdstatus.1** file from the **/var/ace** directory, and use the acetest utility to perform at least three authentications. You can then use the acestatus utility to verify that the server information has been updated.

FTP Support

Tracking Number: 43586
RSA Authentication Agent 6.0 for PAM does not support the use of FTP on HP-UX 11.0.

Use of Alias IP Addresses

Tracking Number: 44187
Problem: On UNIX operating systems, the PAM Agent does not support the use of alias IP addresses for Agent Host communication through firewalls.
Workaround: Make sure that the **sdconf.rec** file in the **/var/ace** directory contains the valid IP address of the RSA Authentication Manager on which you register the PAM Agent.

FTP Requires vsftpd Package

Tracking Number: 41883
Problem: On Red Hat Enterprise Linux WS 4.0 (64-bit) and WS 4.6 (32-bit), the vsftpd package is required when using FTP with the PAM Agent.
Workaround: The package is available on Red Hat Enterprise Linux AS/ES 4.0 and 4.6.

Kerberos Telnet

Tracking Number: 40927
Problem: The kerberos version of telnet installed with Red Hat 4.0 does not work with the PAM Agent.
Workaround: You must install a legacy version of telnet (RPM) available on Red Hat Enterprise Linux AS, ES, and WS 4.0. To enable the legacy version, type:

```
/sbin/chckconfig krb5-telnet off
/sbin/chckconfig telnet on
```

Note: If you need to make configuration changes for telnet, you must edit the remote file in **/etc/pam.d**.

Red Hat Enterprise Linux Desktop Theme

Tracking Number: 24532
Problem: This issue applies to SUSE Linux Enterprise Server 9 and 10, and Red Hat Enterprise Linux AS, ES, and WS 4.0, 4.6, and 5.1. For the desktop theme Red Hat Enterprise Linux, the logon screens for New PIN mode and Next Tokencode mode appear with the **Passcode** field overlapping the screen messages. In New PIN mode, after you enter your user name and passcode, the next screen should read “You must select a new PIN. Do you want the system to generate your new PIN? Y/N” For Next Tokencode mode, after you enter your user name and passcode, the next screen should read “Wait for the tokencode to change, then enter the new tokencode.”
Workaround: In New PIN mode, after you enter your user name and passcode on the initial logon screen, when the **Passcode** field appears on subsequent screens, press ENTER until the screen reads “your new PIN? Y/N.” Then select either **Y** or **N** to indicate whether you want the system to create your new PIN. In Next Tokencode mode, after you enter your user name and passcode on the initial logon screen, when the **Passcode** field appears on subsequent screens, press ENTER until the screen reads “change, then enter the new tokencode,” and then enter the next tokencode that is displayed on your RSA SecurID token.

Technical Notes

To obtain the version number of the PAM Agent:

1. Change to the **/opt/pam/lib** directory.
2. Type the appropriate command for your operating system.
   On Linux, SUSE, Solaris, and AIX, type:
   ```
   strings pam_securid.so | grep "Agent"
   ```
   On HP-UX 11i and 11i v2, type:
   ```
   strings pam_securid.1 | grep "Agent"
   ```

Getting 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**

Trademarks