Release Notes
RSA ACE/Agent v 4.4 for Windows NT

June 2000

If you have questions that the documentation does not address and have a service contract, RSA SecurCare® Online may have your answers. If you need to place a technical support call, our technical support numbers can be reached from our Support page on the RSA Security web site, http://www.rsasecurity.com. If you are a SecurCare Developer Support Customer, call +1.781.687.7700 between the hours of 9 a.m.-6 p.m., U.S. Eastern Standard Time.

Introduction

This document summarizes the new and changed features of the RSA ACE/Agent v 4.4 for Microsoft® Windows NT® product. It also contains information about limitations and known problems found in the software. Read this document before installing the Agent software.

This document includes information about:

- Hardware Requirements
- Software Requirements
- New Features
- Changed Functionality
- Limitations
- Known Problems
- Additional Information

Hardware Requirements

The RSA ACE/Agent v 4.4 for Windows NT software is supported only on Intel x86 processors. The product is **not** supported on MIPS, PowerPC, or Alpha processors.

Software Requirements

Other requirements for the RSA ACE/Agent v 4.4 for Windows NT product include:

- RSA ACE/Server® v 3.3.1 or later
- Microsoft Internet Information Server (IIS) 4.0

- Microsoft Windows NT 4.0 Service Pack 5 or later

  Note: RSA Security recommends using Service Pack 6a with the Web Access Authentication feature set of the Agent.

- Microsoft Internet Explorer 4.0 and higher or Netscape® Communicator 4 and higher

Refer to the *RSA ACE/Agent v 4.4 for Windows NT Installation Guide* for more information about requirements specific to each authentication feature set.

New Features

The following features have been added to version 4.4 of the Agent:

- Local access authentication support for pcAnywhere 9.0, Windows Terminal Server 4.0, and Citrix MetaFrame 1.8 on the Intel platform. These platforms are **not** supported while using the Network access authentication feature set.
- Support for the following Microsoft BackOffice® 4.5 products: Outlook® Web Access server, Exchange Server 5.5, Internet Information Server (IIS) 4.0, Site Server 3.0, and Site Server Commerce Edition 3.0.
- Online product registration that lets you use your Web browser to register the Agent.
- Support for multiple virtual Web servers running on an IIS 4.0 server.
- Support for multi-homed servers.
- Multiple domain name and domain cookie support across multiple servers in the same or different Web domains.
- New Web access authentication (formerly "WebID® ") cookie API: your application can add information to the cookie and extract it at a later time.
- Ability to customize the Web access authentication prompt pages for each virtual Web server.
- Ability to customize the text messages in Web access authentication prompt pages. For example, you can display "PASSCODE incorrect" messages in a language other than English, or change the wording of the message to "Your PASSCODE is incorrect! Please enter the correct PASSCODE."
- New Microsoft Management Console (MMC) snap-in extensions for the Internet Service Manager (ISM). One extension lets you extend the Web Server property sheet in the ISM with the RSA SecurID Web access authentication feature set for each configured virtual Web server. The second and third extensions put a checkbox for enabling and disabling RSA SecurID Web access protection on the Virtual Directory, Directory, and File property sheets.

  The MMC snap-in extensions allow you to remotely administer the Web access authentication settings of any server on which you have installed Web access authentication.

- New Advanced properties sheet in the RSA ACE/Agent Control Panel that allows you to clear the node secret, set an IP address override for multi-homed servers, filter event messages out of the Windows NT Event Viewer log, set diagnostic tracing levels and specify where to record trace output, and set timeout values on remote access prompts.

Changed Functionality

Web Access Authentication Settings

The Web access authentication (formerly "WebID") configuration settings have been moved from the Web properties sheet in the RSA ACE/Agent Control Panel to the Internet Service Manager (ISM) snap-in of the Microsoft Management Console (MMC). You can start the ISM either from the Web properties sheet or through the MMC. Refer to the *RSA ACE/Agent v 4.4 for Windows NT Administrator's Guide* for more information.

Node Secret Storage

In versions prior to version 4.4 of the RSA ACE/Agent for Windows NT, the node secret that is shared between the Agent and the RSA ACE/Server was stored in the **securid** file on the Agent host. During startup of version 4.4, the Agent finds the node secret file, stores the node secret in the Registry, and then deletes the node secret file found on the Agent host.

To remove the node secret from the Registry, click **Clear Node Secret** on the new Advanced properties sheet of the Agent control panel. If you clear the node secret, make sure that the RSA ACE/Server administrator deselects the **Sent Node Secret** setting for the Agent host in the Server database. Afterwards, run the **sdtest** utility to re-authenticate to the Server, so that the Server will send a new node secret to the Agent. Make certain that you reboot afterwards for the new node secret to take effect. Refer to the *RSA ACE/Agentv 4.4 for Windows NT Administrator's Guide* for more information.

Use of the Agent with RSA ACE/Server in a RADIUS Environment

In a RADIUS environment, the Agent and the RSA ACE/Server are installed on one Windows NT machine. Before you upgrade the Agent to version 4.4, make certain that you rename the **aceclnt.dll** file in the Server executable files directory (either in the default directory, **C:\ace\prog**, or wherever you have installed the Server executable files). When you install version 4.4 of the Agent, the new **aceclnt.dll** file will find the node secret file (**securid**) and store the node secret in the Registry.

Limitations

Network Access Authentication and DHCP

Do **not** use Network access authentication in an environment where IP addresses are dynamically assigned using the Dynamic Host Configuration Protocol (DHCP).

Web Access Authentication and Java Script Support

As RSA SecurID users browse a protected Web site that uses HTML frames, the PASSCODE prompt can be displayed in a very small frame on the page and so be too small to read clearly. To avoid this problem, RSA SecurID users should enable Java script support in their Web browsers. When Java script support is enabled, the Agent will put the PASSCODE prompt in a window that displays on top of the Web browser window. Users can easily re-authenticate before returning to browsing a Web site.

Users of the RSA SecurID Software Token v 2.0 product will not encounter this problem if they enable Java script support.

If users re-authenticate in a single WWW domain, they must click the close box of the PASSCODE prompt window to dismiss the window. Users who re-authenticate in multiple domains can click **OK** in the window after the authentication messages for the multiple domains are displayed there.

If you are upgrading to version 4.4 of the Agent, refer to the topic entitled, "Installation Guide Addendum," in the section named "Additional Information" in these Release Notes.

Web Access Authentication PASSCODE Prompt Pages and POST Operations

POST operations can be interrupted by PASSCODE prompt pages if users' Web access authentication cookies expire while their data is being POSTed. In all environments, set the Web access authentication cookie option **Cookies Expire If Not Used Within the Specified Time** on your virtual Web servers to avoid having cookies expire while data is being POSTed. In a COM/ASP environment, you can use ASP Session variables in your pages instead of passing values through the use of POSTed FORM data.

Known Problems

Effect of Uninstalling pcAnywhere on Local Access Authentication

If you uninstall Symantec's pcAnywhere product from the Windows NT machine on which you have installed the Agent, the uninstall process unloads from the Registry an important dynamic link library (DLL) file named **sdgina.dll** that supports the Agent's Local access authentication feature set. To recover from this situation, make certain that you perform the following procedure:

1. Uninstall pcAnywhere.
2. When prompted, immediately reboot the Windows NT machine.
3. Open the RSA ACE/Agent Control Panel and enable Local access authentication.
4. When prompted, immediately reboot the machine again.

Performing these tasks will reload the required **sdgina.dll** file and prevent the machine from hanging with a blue screen.

Effect of Installation or Upgrade on Web Access Authentication

When you upgrade to Microsoft IIS 4.0 to use the Agent, you must reapply the Windows NT Service Pack you were using prior to the upgrade.

If you install the Agent on a Windows NT server with a Service Pack older than Service Pack 6a, the MMC can hang the first time that you enable RSA SecurID Web access authentication on a virtual Web server (referred to in the MMC as a "Web Site"). As a workaround, stop the virtual Web server, enable Web access authentication, and then restart the virtual Web server.

Note: This problem does not occur on Windows NT servers with Service Pack 6a installed. RSA Security recommends that you install Service Pack 6a if you plan to use the Web access authentication feature set.

If you are upgrading to version 4.4 of the Agent, you must perform the following steps before Web access authentication becomes fully functional:

1. After performing the upgrade, follow the instructions in the *RSA ACE/Agent v 4.4 for Windows NT Installation Guide* for installing the MMC snap-ins.

2. Disable Web access authentication on each virtual Web server, and click **Apply**.
3. Enable Web access authentication on each virtual server as needed, and then click **Apply** to make sure the new settings are applied.

Note: After an upgrade to version 4.4, the values of some existing Web access authentication settings revert to their default settings. Some values that are affected include the Web access authentication cookie **Expiration Time** setting, the options **Cookies Always Expire After the Specified Time** and **Cookies Expire If Not Used Within the Specified Time**, and many advanced settings. After you upgrade the Agent, review your Web access authentication settings and adjust them as necessary to suit your site.

Additional Information

Installation Guide Addendum

When Java script support is enabled, the Agent will put the PASSCODE prompt in a window that displays on top of the Web browser window, where users can easily re-authenticate before returning to browsing a Web site. The following material pertains to support of the PASSCODE prompt window, and is an addendum to the "Upgrading and Web Access Authentication HTML Forms" section in Chapter 2 of the *RSA ACE/Agent v 4.4 for Windows NT Installation Guide*.

In the files named **newpin.htm**, **newpin2.htm**, **nextprn.htm**, **passcdro.htm**, and **passcode.htm** that are installed with version 4.4 of the Agent into the ***%SYSTEMROOT%*\system32\aceclnt** directory, make certain that you find and copy the Java script that begins with

```
<script language=JavaScript>
```

and ends with

```
</script>
```

You must copy the ***entire*** block of Java script, including the </script> tags at the end of the respective pages that appear before the </body> tags. Paste the Java script just *before* the </body> tag in your customized versions of these files. In addition, make certain that your RSA SecurID users enable support of Java scripts in their Web browsers.

For more information about these HTML forms, refer to the *RSA ACE/Agent v 4.4 for Windows NT Administrator's Guide*. For more information about upgrading to version 4.4 of the Agent, refer to the *RSA ACE/Agent v 4.4 for Windows NT Installation Guide*.

New Log Out URL Feature for Web Access Authentication

In version 4.4 of the Agent, you can now include a URL that immediately invalidates users' Web access authentication cookies. If users click a link containing the URL, such as at the end of a browsing session, their cookies become invalid and they are prompted for their RSA SecurID PASSCODEs. Add the following relative URL to a link on your Web pages:

```
/webid/sdiis.dll?logoff?referrer=/goodbye.html
```

where **goodbye.html** is an example of a page which informs users that their cookies have expired and prompts them to re-authenticate. The users' Web browsers will add the Web server name as needed.

For example, the link could look like this:

```
<a href="/webid/sdiis.dll?logoff?referrer=/goodbye.html">Logoff</a>
```

If you do not provide an argument to **referrer=**, users are sent to the root directory on the virtual Web server. The ASP sample pages, located on the Agent CD-ROM in the **\acesupp\nt_clnt\sdk\samples\web\ASP** directory, contain a reference to this URL.

Clarification for the RSA ACE/Agent Authentication API Guide

You can find the *RSA ACE/Agent Authentication API Guide* as a .PDF file named **AuthAPI.pdf** on the Agent distribution CD-ROM. On page 8, the text should read as follows:

Data Encapsulation

You cannot access data directly in the entire **SD_CLIENT** data structure, but you can now obtain a handle to this data area. Use the handle in other API calls that provide the requested data, which include the **AceGetAlphanumeric**, **AceGetAuthenticationStatus**, **AceGetMaxPinLen**, **AceGetMinPinLen**, **AceGetShell**, **AceGetSystemPin**, **AceGetTime**, **AceGetUserData**, and **AceGetUserSelectable** calls.

Clarification for the RSA ACE/Agent Web Authentication API Guide

You can find the *RSA ACE/Agent Web Authentication API Guide* as a .PDF file named **WebAuthAPI.pdf** on the Agent distribution CD-ROM. The following information should be included in the guide:

In the C environment, the **RSASetTagField** and **RSADeleteTagField** calls can both accept the result of a previous call to them in their **Cookie** arguments, if more than one field is to be set or deleted, respectively.

In the COM/ASP environment, use the request object to set the value of the cookie directly before attempting a second call to the COM API.

In the Perl environment, use **setenv** to set the HTTP_COOKIE variable to the return value of **rsacookie.exe**.

Dialing In to a Protected Network from a Windows 2000 Machine

The following procedure describes how remote RSA SecurID users can dial in from a Windows 2000 machine to a Windows NT 4.0 DNS domain to get access to protected network resources. This procedure is an addendum to the "Using Network Access Authentication with RAS" section of Chapter 5 in the *RSA ACE/Agent v 4.4 for Windows NT Administration Guide*. Following the instructions in that section, make certain that you

- give each remote RSA SecurID user an additional username and password pair to be used just for dialing in to the RAS server. For example, if a user has a network account with the network username **jdoe**, give the user an additional RAS username of **jdoe_ras**, and a RAS password that is distinct from their network password.
- use the Windows NT User Manager on the PDC to add the remote users to a group with permission to dial in to the network (for example, a group named "RSA SecurID Dial-in").

  Make certain that you add the remote users' RAS usernames (for example, **jdoe_ras**) to the group, not their network usernames.
- on the **Network** tab of the RSA ACE/Agent control panel, specify the group with the **Challenge All Users Except** setting, so that the group you created for remote users will not be challenged for their RSA SecurID PASSCODEs. For example, specify **Challenge All Users Except RSA SecurID Dial-**

in.

- add each remote dial-in Windows 2000 computer to your DNS domain, and assign a static IP address to each computer.
- give the following instructions to your remote RSA SecurID users who are dialing in from Windows 2000 machines. The instructions assume that your remote users know how to set up features of their dial-in connection to your network that do not pertain directly to RSA SecurID.

To create and use a dial in connection to a protected network from a Windows 2000 machine:

1. Install the Network access authentication client software on the remote computer.

   For more information, see the *RSA ACE/Agent v 4.4 for Windows NT Installation Guide*.

2. On the Start menu, point to **Settings**, then to **Network and Dial-up Connections**, and click **Make New Connection**.

   The Network Connection Wizard window opens.

3. On the **Network Connection Type** list, click **Dial-up to private network**, and then click **Next**.
4. In the **Phone Number** box, type the phone number for the RAS connection. Click **Next**.
5. On the **Connection Availability** list, click **For all users**, and then click **Next**.
6. In the **Type the name you want to use for this connection** box, enter a name for this dial-up connection, and click **Finish**.

   The Network Connection Wizard window closes and the Network and Dial-up Connections window becomes the focus.

7. In the displayed list of connections, double-click the connection that you just created.

   The window for the connection opens.

8. Click the **Properties** button.

   The Properties window for the connection opens.

9. Click the **Networking** tab. Under **Components checked are used by this connection**, select **Internet Protocol (TCP/IP)**, and click **Properties**.
10. In the **Internet Protocol (TCP/IP) Properties** window, make sure that you have the correct static IP address specified for your machine on the network to which you are going to dial in, and then click **OK**.

    The focus returns to the Properties window for the connection.

11. Click **OK**.

    The focus returns to the connection's window.

12. In the **Username** box of the connection's window, enter the RAS username given to you by your administrator. Enter the RAS password given to you by your administrator in the **Password** box.

    The correct phone number for the RAS connection should also be visible in the **Dial** box.

13. Click the **Dial** button to start the dial-up connection.

14. After your RAS connection is established, you are prompted for your username and password for the network. Enter your network username and password.
15. When the **Enter PASSCODE** prompt appears, enter your RSA SecurID PASSCODE from your RSA SecurID token, and click **OK**.

The system displays a message that you have been successfully authenticated. If the system displays an **Access denied** message, try again to authenticate. If you still cannot authenticate, contact your administrator.

First printing: June 2000

Trademarks