Readme
RSA ACE/Server 6.0

September 2004

(Version 1.2)

Introduction

This document describes new and updated features, lists known issues, and includes other important information about RSA ACE/Server 6.0.

RSA ACE/Server 6.0 is the authentication, administration, and database management component of RSA SecurID for Microsoft Windows.

RSA ACE/Server 6.0 software is provided in a download kit or on CD. Read this document before installing the software.

This document contains the following sections:

For a roadmap of new features, a description of RSA ACE/Server documentation, and additional information about RSA SecurID for Microsoft Windows, RSA Security recommends that you also read the *RSA ACE/Server 6.0 Getting Started* (**ace_getting_started.pdf**) provided in the Server download package and on the software CD.

Note: To use RSA SecurID for Microsoft Windows, you need to deploy the RSA ACE/Agent 6.0 for Windows, which is included with RSA ACE/Server 6.0. For more information, see the *RSA ACE/Server 6.0 Getting Started* (**ace_getting_started.pdf**).

What's New in This Release

New in this release of RSA ACE/Server are support of the RSA SecurID for Windows solution, offline authentication, Windows password integration, enhanced logging, and additional custom queries. The following subsections summarize these features.

RSA SecurID for Microsoft Windows

The RSA SecurID for Microsoft Windows solution enables you to set up strong, two-factor authentication across your enterprise. With this release, you can use RSA SecurID to protect local computers, domain resources, remote connections, wireless networks, and computers running Microsoft Terminal Services and Citrix Metaframe.

To implement the full RSA SecurID for Microsoft Windows solution in your enterprise, you need to install the RSA ACE/Agent 6.0 for Windows software on the network resources requiring RSA SecurID authentication. For details, see the *RSA ACE/Agent 6.0 for Windows Installation and Administration Guide* and the *RSA SecurID for Microsoft Windows Planning Guide* included with RSA ACE/Agent 6.0 for Windows.

Offline Authentication

When logging on to a Windows 2000 or XP client computer or domain controller, a user typically must enter a password to gain access. With RSA SecurID for Windows, the user must enter a passcode (a PIN combined with the current tokencode).

Normally, a user's name and passcode are authenticated when the RSA ACE/Agent sends them to the RSA ACE/Server. Offline authentication extends the RSA SecurID solution when a user is disconnected from the corporate network or a connection to the RSA ACE/Server is temporarily unavailable. With offline authentication, the RSA ACE/Agent uses strongly encrypted *offline authentication data* on the local machine or domain controller.

If an offline user forgets a PIN, loses a token, or runs out of offline authentication data before reconnecting to the company network, the RSA ACE/Server administrator can give the user an emergency code.

Windows Password Integration

The RSA SecurID for Microsoft Windows solution reduces the cost of password maintenance by enabling Windows password integration.

With password integration enabled, users enter their password only the first time they authenticate with RSA SecurID. The Agent reads and encrypts the password, then sends it to the Server, which stores the password in the database. After that, whenever users authenticate with an RSA SecurID passcode, their Windows password is automatically sent to the Windows authentication engine.

Enhanced Logging

RSA ACE/Server 6.0 logs system activity related to offline authentication. When users are disconnected from the network, offline authentication events are recorded both in the local Windows Event Log, and by the RSA ACE/Agent to a local log file. The next time a user connects to the network and a connection to RSA ACE/Server is available, the log data is transferred to the Server's log database.

In addition, for security purposes, any time an administrator accesses an emergency code for a token or user, RSA ACE/Server logs the event.

Sample Queries

RSA ACE/Server 6.0 includes new sample queries for tracking data related to offline authentication and emergency access codes.

Known Issues

Emergency Passcode Cannot Be Viewed on a Replica

To view an emergency passcode for a user, use **Edit User** in the Database Administration application. In the Edit User dialog box, select **View Emergency Passcode**. This must be done on the Primary. If you attempt to do it on a Replica, the option is unavailable.

Reboot Required After Installing Remote Admin

After installing Remote Admin, you should reboot the computer. Otherwise, the links from the application to the Help are broken.

Token Files Cannot Be Exported in ASCII Format

In the Database Administration application, you can select one or more tokens in the database, and use the **Export Token** command to export the tokens to a file (which you can later reload). In RSA ACE/Server 6.0, the capability to export to ASCII (**.asc**) format is no longer supported. However, note that you will still be able to import token record files in ASCII format.

Offline Authentication Service Port Change Must Be Done Manually

RSA ACE/Server 6.0 includes a new service, the **Offline Authentication Download** service, or **sdoad**. If you enable offline authentication at the system level, the **sdoad** service uses port 5580 by default. If you need to change the port number for this service to avoid conflicts with a third-party service, you can do so through the Configuration Management application in the RSA ACE/Server program group. Note that you must change this port manually on the Primary and all Replicas. Changing it on the Primary, then creating and sending a new Replica package to the Replicas will ***not*** change the port number on the Replicas.

Aliases Not Updated When Upgrading From RSA ACE/Server 5.2 to 6.0

During installation, when you upgrade an existing RSA ACE/Server 5.2 Primary to RSA ACE/Server 6.0, the Primary and Replica aliases are not automatically updated in the Replica table. To work around this, complete the following steps:

1. Upgrade the 5.2 Primary to 6.0 as documented in the *RSA ACE/Server 6.0 for Windows Installation Guide*.
2. On the Primary, launch the Replica Management utility.
3. Select the first Replica in the Server list, click **Details**, and in the Replica Information dialog box, specify up to three aliases for the Replica, then click **OK**.
4. Repeat step 3 for each Replica that has aliases.
5. From the main Replica Management dialog box, select the Primary in the Server list, then click **Generate Replica Package**.
6. A message asks if you want to maintain the **uidxlate.map** file. Click **Yes**.
7. Copy the Replica Package to each Replica machine.
8. Upgrade each Replica machine from RSA ACE/Server 5.2 to 6.0 software, and start each Replica.

The aliases for each Replica will now be listed correctly.

RSA Web Agent 5.2 Requires Hotfix

If you are using the RSA Web Agent 5.2 for Microsoft's Outlook Web Access (OWA) protection, you should download the latest Hotfix, which fixes a crash problem when the Agent experiences heavy usage. You can download the Hotfix from RSA SecurCare Online:

https://knowledge.rsasecurity.com

Documentation Items

UNIX References

In RSA ACE/Server documents, such as the *Administrator's Guide*, there are references to Server support on UNIX platforms. RSA SecurID for Windows, in its initial release, supports only Windows platforms.

However, in follow-on releases, the product will support RSA ACE/Server 6.x running on Sun Solaris 9. References to UNIX, in this case, will apply to the Solaris platform.

Getting Support and Service

RSA SecurCare Online: https://knowledge.rsasecurity.com

Customer Support Information: www.rsasecurity.com/support

Trademarks