Readme

This *Readme* contains important information not included in the standard RSA ACE/Server 5.2 documentation set. RSA Security strongly recommends that you read this document before installing RSA ACE/Server. Also read the *Getting Started* booklet as a guide to installing, deploying, and using RSA ACE/Server and RSA SecurID two-factor user authentication.

If You Downloaded RSA ACE/Server 5.2

If you downloaded RSA ACE/Server 5.2, the full documentation set is provided in your download file in a folder named **aceservdoc**. When reading the documentation, where appropriate, substitute the term *online distribution file* for *software CD*. In procedures, you may need to adjust the details of some steps. For example, you might navigate to a directory on your hard drive rather than on the CD.

You should have already received the Welcome Kit and license diskettes with your original RSA ACE/Server package.

Installation and Upgrade Information

- Refer to the *RSA ACE/Server 5.2 Installation Guide* for your platform to view system requirements, including patch levels for your operating system.
- You cannot install RSA ACE/Server software in a directory whose name contains a space (for example, “Program Files”).
- If you are upgrading to RSA ACE/Server 5.2 for Windows from an earlier version, you must first close all RSA ACE/Server applications, shut down the RSA ACE/Server brokers and disable automatic startup, and restart your system. Then you can begin the upgrade installation.
- When you upgrade to RSA ACE/Server 5.2 for Windows, the setup program asks you to specify a folder outside of the RSA ACE/Server directory structure to hold backup copies of critical program and database files from your current installation. This is a precaution in case problems are encountered during the upgrade, and you need to restore your current system. Note that you will need your current system’s original installation CD to restore it.

High Availability

With this release, customers with an RSA ACE/Server Advanced license can run their Primary server on the Veritas Cluster Server high availability system in Sun Solaris 9, with full support from RSA Customer Support.

RSA ACE/Server 5.2 does not support HP Service Guard or IBM HACMP high availability systems.

Performance Testing

The RSA ACE/Server 5.2 documentation set includes the *RSA ACE/Server 5.1 Scalability and Performance Guide*. RSA ACE/Server 5.2 meets or exceeds the performance measurements published in that book.

Troubleshooting and Technical Notes

Web Express 1.2

Hot Fix for Web Express 1.2

If you are using Web Express 1.2, RSA Security strongly recommends that you install an available hot fix. The hot fix corrects an issue where users' PINs are displayed as plain text in the **default-out.log** file.

Contact RSA Security Customer Support for information about this hot fix.

Web Express and Quick Admin

If you are using Web Express 1.2, and you want to run Quick Admin on the same web server, make sure to install Web Express first, then install Quick Admin over it. (This is contrary to the procedure documented in the *RSA SecurID Web Express 1.2 Installation and Configuration Guide*, which is in error.)

Databases Supported by Web Express

Web Express works with third-party databases. However, they must be JDBC-compliant databases that support nested SQL statements (for example, Microsoft Access). Web Express does not work with MySQL and other databases that do not support nested SQL statements.

Database Administration

Using Double-Byte Output from Custom Queries with Crystal Reports

As described in the "Reports" chapter of the *RSA ACE/Server 5.2 Administrator's Guide*, the Custom Queries feature enables you to query the database and send the output to a CSV, HTML, or XML file. When your RSA ACE/Server database contains data with Japanese, Chinese, or Korean (double-byte) characters, Crystal Decision's Crystal Reports application cannot directly import the data from these output files.

Workaround: Install Microsoft Excel. Install Crystal Decisions, including the Microsoft Office plug-in. Specify output of your query data to a CSV file, then open the file with Microsoft Excel. Save the file as an Excel (**.xls**) file. Open the Excel file with Crystal Reports.

Using the ATK to Run Custom Queries Automatically

The Custom Queries feature in the Database Administration application does not provide a capability to run database queries automatically at scheduled times.

Workaround: To run queries in the background using an OS scheduler, use the administration toolkit to write a program using the **Sd_DynamicSelect** function. For information, see the *RSA ACE/Server 5.2 Administration Toolkit Reference Guide* (**ace_admin_toolkit.pdf**).

Issuing Software Tokens

When you run the **Issue Software Tokens** command in Database Administration, and select **Multiple Tokens Per File** and **Limit File Size To 1.44MB**, there are two defects:

- The first file that RSA ACE/Server 5.2 creates contains the fixed number of 100 tokens (as designed). This file is typically 51KB in size. However, after that, only one token per file is issued. Depending on the number of tokens that you issue, you can end up with many hundreds of files, only the first one actually containing more than one token.
- If you are issuing tokens directly to a floppy disk, and you issue enough software tokens to fill the disk, no warning is given, and potentially a number of token files of 0 bytes can be created.

Workaround: Use the **One Token Per File** option, and issue the files to a location on your hard drive. Alternatively, to create one file, you can use **Multiple Tokens Per File** without limiting the file size to 1.44MB. For example, one file with 2000 tokens is about 1MB in size. Then you can manually copy the file(s) to a floppy diskette.

Synchronizing Specific Groups from LDAP Directory Servers

As described in the *RSA ACE/Server 5.2 Administrator's Guide*, the LDAP synchronization capability enables you to capture LDAP user data, including the LDAP group(s) to which they belong. For example, with an organizational unit containing two groups, all users and the groups to which they belong are synchronized into the RSA ACE/Server database.

However, suppose you want to synchronize only one group within an organization unit into RSA ACE/Server. You could do this by using LDAP controls in Database Administration, as described in this section.

Note: This capability only works for Microsoft's Active Directory and Novell's eDirectory. It does not work for Sun Microsystem's Sun ONE Directory Server.

To access the filtering and querying controls for an existing synchronization job, select **User** > **LDAP Users > Edit Synchronization**. (Alternatively, you can select **Add Synchronization** to create a new job.)

For Active Directory:

In the Edit (or Add) Synchronization dialog box, the default filter is:

```
samaccountname=*
```

where * is a wildcard meaning all names. You could change the filter to have leading or trailing letters (for example, **A*** would get all names that begin with **A**).

1. To filter for users who belong to a specific group, use a filter similar to:

   ```
   (&(samaccountname=*)(memberOf=cn=groupname,cn=orgunitname,
   dc=ldapservname,dc=com))
   ```

   Note: The value of the **memberOf=** string must be a complete domain name. No wildcards are allowed.

2. Next, in the Edit (or Add) Synchronization dialog box, click **Options**.
3. In the LDAP User and Group Synchronization Options dialog box, check **Synchronize users with their LDAP Groups**.
4. In the **Base DN** field, specify the full domain name, for example:

   ```
   cn=groupname,cn=orgunitname,dc=ldapservname,dc=com
   ```

5. Close the dialog boxes.

   When the synchronization job is run, only the users in the specified group are synchronized into the RSA ACE/Server database.

For Novell eDirectory:

In the Edit (or Add) Synchronization dialog box, the default filter is:

```
uid=*
```

where * is a wildcard meaning all names. Note that you could also have leading or trailing letters (for example, **A*** would get all names that begin with **A**).

1. To filter for users who belong to a specific group, use a filter similar to:

   ```
   (&(uid=*)(groupMembership=cn=groupname,ou=orgunitname,
   o=ldapservname))
   ```

   Note: The value of the **groupMembership=** string must be a complete domain name. No wildcards are allowed.

2. Next, in the Edit (or Add) Synchronization dialog box, click **Options**.
3. In the LDAP User and Group Synchronization Options dialog box, check **Synchronize users with their LDAP Groups**.
4. In the **Base DN** field, specify the full domain name, for example:

   ```
   cn=groupname,ou=orgunitname,o=ldapservname
   ```

5. Close the dialog boxes.

   When the synchronization job is run, only the users in the specified group are synchronized into the RSA ACE/Server database.

Miscellaneous

- If you perform a task that affects any of the lists that appear in the following dialog boxes, the changes are not immediately reflected in the list:
  - Associated Groups and Associated Sites (both accessed from the Edit Site dialog box)
  - Agent Host Activations and Members (accessed from the Edit Group dialog box)
  - Group Activations (accessed from the Edit Agent Host dialog box)
  - Group Memberships (accessed from the Edit User dialog box)

  You may see this behavior when you activate a group on an Agent Host, change the name of an Agent Host associated with a site, associate a group with a site, or add users to a group.

  Workaround: To refresh the list, close the dialog box and reopen it.

RSA ACE/Agent

In some cases, when the administrator changes the Primary Server's IP address (for example, when replacing the old Primary's machine), an RSA ACE/Agent can fail to connect to the new Primary Server.

To make sure that an RSA ACE/Agent can connect to the new Primary, it must be able to connect to another Server (a Replica) in the realm. If the Agent's Server list only contained the old Primary, there would be no way for the Agent to get a new Server list. (If you encounter such a situation, contact RSA Security Customer Support for assistance.)

Assuming that the Agent can connect to another active Server, it should get a new Server list and be able to connect to the new Primary. The old Primary remains in the Agent's extended Server list. An Agent can also fail to connect to the new Primary because the first Server in this extended list is used when all the Servers are temporarily unavailable because of high authentication loads.

Another problem can occur if the **sdopts.rec** file marks the old Primary as the only Server to be used. In this case, because the old Primary's IP address is offline, the Agent will fail. For more information, see "Creating an sdopts.rec File (for RSA ACE/Agent Administrators)" in the *RSA ACE/Server 5.2 Administrator's Guide*.

Typically, however, an Agent works because of the **sdstatus.12** record, which is written when the Agent first successfully starts up and authenticates. If the Agent administrator decides to use the **sdopts.rec** (by creating a new one or modifying an old one) on the Agent Host, the **sdstatus.12** record will be deleted. In this case, the Agent reverts to using the most recent **sdconf.rec** file on its host system. This can cause failures, especially if only the old Primary is in the **sdconf.rec** file.

Windows Platform Issues

RSA ACE/Server and Sun ONE Directory Server Incompatibilities

If you attempt to install RSA ACE/Server and the Sun ONE (iPlanet) Directory Server (version 5.1) on the same machine, a dynamic link library (DLL) conflict causes the Sun ONE server to crash when it attempts to start its services. This is because RSA ACE/Server uses a later version of the **nssl.dll** than the one used by Sun ONE, and the later version is not backward-compatible.

Workaround: In general, RSA Security strongly advises the use of dedicated machines for your RSA ACE/Server Primary and Replicas. If you want to run Sun ONE Directory Server, run it on another machine on your network.

UNIX Platform Issues

Installing Replica Server Software

There is an error in the *RSA ACE/Server 5.2 for UNIX Installation Guide* (**ace_install_unix.pdf**). In the section entitled “Command Line Arguments,” the **-R** command line option to specify the pathname of the Replica package does not work.

Workaround: Do not use the **-R** option. Instead, run the command without it, and you will be prompted to specify the pathname of the Replica package.

Starting and Stopping Processes

- Use the **aceserver stop** command to stop the **aceserver** process. Do not use a **kill** command.
- Use the **kill *PID*** command to stop an **sdlogmon** process. Do not use the **kill -9 *PID*** command.
- Running a program with an argument (for example, **/bin/ksh -n** …) from the default shell field does not work.

TACACS+

- Under certain circumstances, such as a high amount of network traffic, cross-realm authentication may not be successful on a NAS machine running both the RSA ACE/Server and the RSA ACE/Agent for UNIX software with TACACS+ enabled.

  During these situations, the RSA ACE/Server successfully completes a cross-realm authentication, but the success status is not immediately returned to the client, and a user is denied access.

  You can eliminate this problem by designating the RSA ACE/Server installed on the NAS machine to handle all cross-realm authentications, and by making certain configuration adjustments on the Server, as follows.

  1. In the **VAR_ACE** directory on the Server with TACACS+ enabled, create an **sdopts.rec** file. Specify the following:

     – A priority of 10 for the RSA ACE/Server on the ACE/Server performing TACACS+ authentications

     – That all alias Server IP addresses be ignored

     See “Creating an sdopts.rec File” in the chapter, “Agents and Activation on Agent Hosts,” in the *RSA ACE/Server 5.2 Administrator's Guide*.

2. Set the server time-out on the NAS machine between 15 and 30 seconds.

> **Note:** If the NAS machine you are using does not allow the server time-out setting to be adjusted, cross-realm authentication will not function when TACACS+ is enabled on the machine.

- Cisco IOS 11.1 (6) has a bug that prevents the RSA Security TACACS Server from operating in New PIN mode with TACACS+. Upgrading to IOS 11.1 (7) or later fixes the problem.
- PPP connections to the TACACS+ daemon must be invoked using a post-login window, in which the **Username** and **Passcode** prompts appear to the user. Without this window, the user will be unable to complete authentications when they are in New PIN or Next Tokencode mode. Use the if-needed authentication qualifier for PPP authentication.
- Next Tokencode mode with TACACS+ restricts users to a 30-second inactivity time-out, which causes a problem when a user needs to wait for the next tokencode on a token. The 30-second inactivity time-out is hard-coded in older revisions of the Cisco router/communications server firmware. Set the inactivity timeout to 120 seconds using the command **tacacs-server login-timeout 120**.

```
Multihomed host detected; Primary IP assumed is: 255.255.255.255
```

To solve this problem, make sure that your Server's machine name resolves to exactly the same name that appears in your Replica table.

Quick Admin

- On Windows 2003, Quick Admin has some limitations in its Search capability. Searches that return a high number of values can result in a **Page not found** error in your browser. This issue is being investigated by RSA Security. If you encounter searching problems in Quick Admin running on Windows 2003, contact RSA Customer Support.
- If you intend to run Quick Admin on Windows 2003 with Microsoft's IIS version 6.0 web server, note that there is an error on page 51 of the *RSA ACE/Server 5.2 for Windows Installation Guide* and page 77 of the *RSA ACE/Server 5.2 for UNIX Installation Guide*. In step 1, under the procedure "To configure JRun," the third bulleted item instructs you to select **6.0** as your web server. However, the JRun Wizard does not offer **6.0** as an option, displaying only the **5.0** version.

  Workaround: Select **5.0** and follow the rest of the steps in the JRun Wizard. The Wizard will correctly configure JRun to use IIS version 6.0.
- During Java Runtime Environment installation, the user is sometimes prompted to overwrite the **msvcrt.dll** or other system files.

  Workaround: Click **No** to leave the existing files on the hard disk.
- The Quick Admin software installed on your web server logs all transactions to the **default-out.log** file in the **jrun-install-directory/logs/** directory. This log file can grow large enough to completely fill the disk space on the web server.

  Workaround: Monitor the growth of the **default-out.log** file, and periodically archive the existing file and delete it from the web server.

- If you generate a user report in which you search by Token Ownership with the option **Expiring in x Days**, be aware that the results include tokens that have already expired as well as tokens that will be expiring *within* the designated amount of days.
- When you attempt to generate a user report in which you search by Token Ownership with an option that should not require a search string, you get an error message telling you to enter a search string.

  Workaround: Enter a dummy search string.
- When running Quick Admin software on a Sun ONE web server on Solaris 9, occasionally the browser halts indefinitely (“hangs”). The **default-out.log** file in the **jrun-install-directory/logs/** directory will show a Java Exception error. For example, “An unexpected exception has been detected in native code outside the VM.”

  Workaround: To find out which process is hanging, from the command prompt type

  ```
  ps -ef | grep java
  ```

  Note the process id number, and then type

  ```
  kill -9 process id
  ```

  where *process id* is the process identification number.
- Under certain conditions, it is possible for a site or group administrator to view and change token data of a user who does not fall under his or her scope. When the administrator runs a valid search for users in his or her scope, Quick Admin returns a list of users in that administrator’s scope who meet the search criteria. From that list, the administrator can select a user and go to the Edit User page. However, in the **Default Login/User ID** field, the administrator can then enter the name of a user not in his or her scope, and click **Select Users**. This does display an error message:

  ```
  refreshinfo: Problem processing request: message is "Failed
  to list user info for <name>. ACE Error: Sd_ListUserInfoExt
  Error Invalid user"
  ```

  However, the invalid user’s token(s) still appear in the Assigned Tokens list at the bottom of the page. The administrator is then free to unassign the user’s token.

  Note: This issue will be corrected in RSA ACE/Server 5.2, Patch 1.

RADIUS

- If you have a name resolution conflict on your Primary or Replica, the RADIUS server can crash when starting up. In this case, the RADIUS server generates this message in the Event Log (Windows) or the syslog (UNIX):

  ```
  Multihomed host detected; Primary IP assumed is:
  255.255.255.255
  ```

  To solve this problem, make sure that your RADIUS server’s machine name resolves to exactly the same name that appears in your Replica table.

- The Auth Compatibility Mode on ASCEND MAX servers must be set to **VSA**. RSA ACE/Server 5.2 does not work with ASCEND MAX servers if the Auth Compatibility Mode is set to **Old**.
- Although the RSA RADIUS server can be configured to allow system-generated user PINs, this option is turned off by default and should not be turned on. A system-generated PIN is not encrypted when it is sent back to the user in a RADIUS packet. Because the transmission of unencrypted PINs to users on remote systems involves a clear security risk, RSA Security strongly recommends against allowing system-generated PINs for remote users who are authenticated through a RADIUS server.

  The system parameters of an RSA ACE/Server must be set to allow user-created PINs if the Server is performing authentications in conjunction with an RSA RADIUS server. In addition, each user record created on that RSA ACE/Server must allow for user-generated PINs. Otherwise, users will be unable to establish PINs through a RADIUS server that does not allow system-generated PINs.
- If RADIUS users are denied access, and the error in the RSA ACE/Server log is "Node verification failed," you must change ownership of the node secret file (usually the **securid** file in the ***ACEDATA*** directory) to the owner of the RSA ACE/Server files. To find the owner, run **sdinfo**.

  To avoid this problem, always start the RSA ACE/Server as root or as the RSA ACE/Server file owner.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsasecurity.com/support**

First printing: October 2003 (Rev A)

Trademarks