RSA SecurID Software Token 2.0 For Palm Handhelds User's Guide

This guide explains how to install and use your RSA SecurID Software Token 2.0 for Palm Handhelds application. This guide assumes that you know how to

- Use Palm Desktop and HotSync Manager to load new applications onto your Palm handheld.
- Navigate the Palm user interface and run applications.

The RSA SecurID for Palm Handhelds application features online tips to help you use and configure the program. To view the tips, tap the **i** icon on any of the RSA SecurID application screens.

Quick Start

This section contains all the steps necessary to install the RSA SecurID application and token, and to use your token to authenticate for the first time.

Step 1: Verify Installation Requirements

To install RSA SecurID Software Token 2.0 for Palm Handhelds application and a software token, you must have

- A handheld device running Palm OS 4.0 or higher connected to a PC.
- Palm Desktop v 4.0 or higher software installed on a PC running one of the following versions of Windows:
  - Windows 98 SE
  - Windows NT SP6a
  - Windows 2000 Professional SP4
  - Windows XP Professional

  The operating system should be running the latest hot fixes and service packs.

Step 2: Verify Application and Token Files

Your administrator will send you the following files that you will need to install and use RSA SecurID Software Token 2.0 for Palm Handhelds:

- The RSA SecurID Software Token application files: **SecurID.prc** and **SecIDLib.prc**
- An RSA SecurID software token file in the **.sdtid** format.
- The token conversion utility (**MakePDB.exe**), which converts the **.sdtid** file to a Palm OS-formatted **.pdb** file.
- This guide, the *RSA SecurID Software Token 2.0 For Palm Handhelds User's Guide* (**securid_palm_users.pdf**).

Step 3: Set the Correct Date and Time

Correct clock settings are crucial to the proper functioning of the RSA SecurID application. Before installing, check to make sure the clock settings on your handheld device are correct. To change the clock settings, see your handheld device documentation.

Step 4: Identify Your Palm Handheld Serial Number

Each Palm handheld device has a serial number assigned to it by Palm Inc. To ensure that no one else can use the token assigned to you, your RSA ACE/Server administrator may associate your token with your handheld device serial number.

Note: This step is optional and is required only when your administrator issues a token file that is associated with your handheld device. If your handheld device does not display a serial number, it does not support use of a token record that is associated with a specific device.

To find the serial number:

1. Turn on your Palm handheld device.
2. In the Applications Launcher, tap **App** > **Info**.
3. Tap **Version**.

   The serial number displays in the **ID** field.

Step 5: Install the RSA SecurID Application

Your administrator has provided you with two application files containing the RSA SecurID application and library.

Before you begin, your handheld device must be in its cradle, and connected to your PC.

Note: RSA SecurID Software Token 2.0 for Palm Handhelds is not compatible with any previous version of RSA SecurID Software Token. You must remove any previous version of the application and tokens from the handheld before installing version 2.0.

To install the application:

Use the Palm Desktop Install Tool to install the files **SecurID.prc** and **SecIDLib.prc**. See your handheld device documentation for information about using the Palm Desktop software.

When the installation is complete, the RSA SecurID icon appears in the handheld device Application Launcher.

Step 6: Start the RSA SecurID Application

To start the RSA SecurID application:

1. In the Application Launcher, tap the RSA SecurID icon.
2. Read the terms of the license, and tap **I accept**. The application does not start until you accept the license.

   The first time that you start the application, a message displays to remind you to set the time correctly.
3. If valid token distribution files (**.sdtid** files) are present on your handheld device, the token install procedure starts automatically. Click **OK** to install the token.

Demo Mode

Demo mode runs a demo token that allows you to explore some of the features of the RSA SecurID application, but you cannot use the demo token to authenticate and access protected resources. After you install a valid token, the demo token no longer appears.

Demo mode runs under the following conditions:

- There are no tokens installed.
- You restart the application, the active token is passphrase protected, and the passphrase that you enter is incorrect.
- You delete all of the tokens from your handheld device.

Step 7: Install a Token

Your administrator will send you one or more token distribution files with the **.sdtid** extension that you will download to your PC and convert to a **.pdb** file that you can install on your handheld device. The administrator might have encrypted the file and assigned passphrases to the tokens. Check with the administrator to be sure he or she has given you any necessary passphrases.

To install an RSA SecurID token:

1. Make sure your handheld device is in its cradle and connected to your PC.
2. Run the seed conversion utility (**MakePDB.exe**) and specify the location of the **.sdtid** file.

   If you click **Browse** to specify the location, the file is converted automatically. If you type the location of the file, click **Convert** to convert the file.
3. In the Palm Desktop Install Tool application, add the converted token file (**.pdb**), and then Hot Sync your handheld device with your desktop.

   Note: You can install only one token at a time. If you have more than one token, you must add a single token **.pdb** file, and then Hot Sync your handheld device to install the token before adding the next token **.pdb** file.

   If your handheld device contains an MMC storage card, specify the card as the destination of the token. For more information on using RSA SecurID with an MMC storage card, see "Storing Your Token on an MMC Card" on page 8.

4. On your handheld device, start the RSA SecurID application.

   The token installation procedure starts automatically.

5. If your administrator assigned a passphrase to your token, enter it when you are prompted.

   If a token fails to load, an error message appears. For more information on error messages, see "Troubleshooting" on page 10.

   After the token is installed successfully, it becomes the active token.

6. If you installed your token on an MMC card, close the RSA SecurID application to complete the installation.

Important: As a security measure, synchronizing your handheld device with the Palm Desktop software backs up the RSA SecurID Software Token application only, not your installed tokens. If you need to restore all data to your handheld device, your administrator must resend the token distribution files to you, and then you must reinstall the tokens.

Step 8: Create an RSA SecurID PIN for Your Token

When you create a PIN for your token, do not pick a number that can be easily guessed (such as 1234), and do not write down your PIN. Your PIN cannot begin with a zero.

If your administrator informed you that you do not need a PIN to authenticate, you do not need to create a PIN. Go to "Step 9: Authenticate."

To create a PIN:

1. Start the RSA SecurID application on your handheld device, and enter your token passphrase, if required.

2. Initiate a login session at your PC. After you enter your User ID, the system prompts you to enter a passcode.

3. If you have not previously created a PIN, or your administrator has not assigned you a PIN, enter the tokencode from the RSA SecurID application running on your handheld device.

   If you are authenticating at your PC, the New PIN dialog box opens.

4. Do one of the following:

   - To have the system generate a PIN, select **ACE/Server will generate PIN**, and click **OK**. Your PIN displays for 10 seconds.
   - To create your own PIN, select **I will create PIN**, enter and confirm your PIN, and click **OK**. The PIN must be from 4 to 8 digits long.

5. If any of the following messages appear, try again to create a PIN:

   - PIN and confirmation do not match.
   - PIN must be 4-8 digits.
   - New PIN rejected.

   If you are still denied access, contact your administrator.

6. Once your PIN is accepted, wait for the tokencode to change on your RSA SecurID screen.
7. Continue authenticating by following the instructions in the next section.

Step 9: Authenticate

To authenticate:

1. Initiate a login session.
2. Enter your User ID.
3. Start the RSA SecurID application and enter your token passphrase, if required.
4. If the token that you want to use is not the active token, select the token from the list of available installed tokens.
5. Enter your PIN and tap **Get Passcode**.

   If your administrator informed you that you do not need a PIN to authenticate, tap **Get Passcode**.

   The RSA SecurID application displays a passcode, and a set of bars that indicate how long the passcode is valid.
6. Enter the passcode in the appropriate window on the login screen.

Reference

This section contains procedures for tasks that you may need to perform when using your RSA SecurID Software Token and solutions to common problems that you may encounter.

Authenticating with an RSA SecurID Software Token

Before you authenticate with your RSA SecurID Software Token, be sure that the clock settings on your handheld device are correct.

To authenticate with your RSA SecurID Software Token:

1. Initiate a login session.
2. Enter your User ID.
3. Start the RSA SecurID application, and enter your token passphrase, if required.
4. If you have a PIN for your token, enter your PIN and tap **Get Passcode**.

   If you do not yet have a PIN for your token, the first time you authenticate the application prompts you to create a PIN. For more information, see "Authenticating in New PIN Mode."

   If your administrator informed you that you do not need a PIN, tap **Get Passcode**.

   The RSA SecurID application displays a passcode, and a set of bars that indicate how long the passcode is valid.
5. Enter the passcode in the appropriate window on the login screen.

   If you are prompted to enter the next tokencode, see "Authenticating in Next Tokencode Mode."

Authenticating in New PIN Mode

If the system prompts you to set a PIN, you must either create your own PIN or accept a system-generated PIN. The PIN must be entered into your token when you use it to authenticate.

Authenticating in Next Tokencode Mode

If the system prompts you to enter the next tokencode, wait until the tokencode changes on the RSA SecurID screen, and then enter the next tokencode that displays on your handheld device. If you are not granted access after correctly entering the next tokencode, contact your administrator.

Do not tap **Done** before the next tokencode displays. You do not need to reenter your PIN to authenticate in Next Tokencode mode.

Copying the Passcode

If you want to copy the displayed passcode, tap **Copy**.

Changing the Active Token

Your Palm handheld device can contain up to 10 RSA SecurID tokens. To use a particular token, it must be the "active" token. You must select the token from the set of available tokens on your handheld.

To change the active token:

1. Tap the pick list in the upper right corner of the screen.
2. Tap the name of the token that you want to use to authenticate.
3. Enter the passphrase for the selected token, if required.

Changing a Token Name

The token name has the following restrictions:

- The length must be between 1 and 15 characters.
- The name is case-sensitive.
- The first and last characters in the name cannot be a blank space.

  The RSA SecurID application strips blank spaces from the name when the first or last character is a blank space.
- The name cannot be blank.
- Duplicate names are not allowed.

To change the name of a token:

1. Tap **Token** > **Manage Tokens**.
2. Under **Choose a token**, tap the name of the token.
3. Tap **Manage Tokens** > **Change Name**.
4. Enter a new name for the token, and tap **OK**.
5. If the token is stored on an MMC card, the name change takes affect only after you close the RSA SecurID application, or tap **Device**.

Protecting a Token with a Passphrase

Passphrases prevent unauthorized persons from using the RSA SecurID application on your handheld device. Passphrases are case-sensitive, and can contain numbers, letters, spaces, punctuation, and symbols. RSA Security recommends that passphrases not exceed 20 characters.

Memorize all passphrases that you create. If you forget your passphrase, you are not able to use the token protected by that passphrase. In that case, contact your administrator.

To change or create your token passphrase:

1. Tap **Token** > **Manage Tokens**.
2. Under **Choose a token**, tap the name of the token.
3. Tap **Manage Tokens** > **Change Passphrase**.
4. Enter the old passphrase, if required.
5. Enter and confirm the new passphrase.
6. Tap **OK**.

   You will be prompted to enter the passphrase when you start the application or select a specific token for authentication.

   Note: If you forget the passphrase, a screen opens that allows you to choose and activate another token. If all your tokens are passphrase protected, and you forget the passphrases, contact your administrator.

7. If the token is stored on an MMC card, the passphrase change takes affect only after you close the RSA SecurID application, or tap **Device**.

Removing Passphrase Protection

To remove the passphrase, leave the fields blank in the new passphrase screen, and tap **OK**. The passphrase is removed.

Deleting a Token

1. Tap **Tokens** > **Manage Tokens**.
2. Under **Choose a token**, tap the name of the token.
3. Tap **Manage Tokens** > **Delete**.

   If you see the **Can't Delete Active Token** message, change the active token to another token and try to delete it again. For more information on active tokens, see the section, "Changing the Active Token."
4. Tap **OK**.
5. If the token is stored on an MMC card, the token is deleted only after you close the RSA SecurID application, or tap **Device**.

Note: When you delete the last token, you are returned to demo mode and can no longer use the RSA SecurID application to authenticate to any protected resources. Contact your administrator for a new token.

Identifying the Token Serial Number

Each RSA SecurID software token has a unique identifying serial number. If you have a problem with a token, your administrator will ask you for the serial number.

To view the token serial number:

1. On the Palm handheld device, start the RSA SecurID application.
2. Tap **Token** > **Manage Tokens**.
3. Under **Choose a token**, tap the token name.
4. Tap **Manage Tokens** > **Show Serial #**.

Storing Your Token on an MMC Card

If your handheld device contains a slot for an MMC or SMMC storage card, you can choose to store your token on your Palm handheld device's resident RAM, or on the storage card. Keep in mind that if your administrator has associated your token with the serial number of your Palm handheld device, you can use the token on that device only.

When your handheld device has an MMC card inserted in the MMC slot, the main screen of the RSA SecurID Software Token application contains an additional interface component that allows you to access tokens stored in the device memory (**Device**) or on the MMC card (**MMC**).

You can switch between a token stored on the device and a token stored on the MMC card by tapping either **Device** or **MMC**.

Inserting the card while the RSA SecurID application is running

If you insert an MMC card while the application is running, by default the handheld device stops the running application and switches to the Palm Card Information screen. Restart the RSA SecurID application, and choose the storage location of your token.

Removing the card while the RSA SecurID application is running

If you remove the MMC card while the application is running, you will encounter the following:

- Any changes you have made (including installing a token, or changing the name or passphrase of the token) will be lost.

  To save changes to the MMC card, close the RSA SecurID application or tap **Device** before removing the MMC card.

- The **Device** and **MMC** buttons are hidden.

  If you were accessing a token on the card, the application switches to a device-resident token, if one is installed, or to the demo token on the device. You may need to enter a token passphrase, if one is required for the active token. If you were accessing a token on the device, the application continues to function.

Switching between a token on the device and a token on the MMC card

Tapping the **Device** and **MMC** buttons allows you to access tokens stored on the handheld device or MMC card. When you tap the **MMC** button, and you have not installed any tokens on the card, the RSA SecurID application prompts you to create a token database, which will contain only a demo token. If you do not choose to create the token database, the application returns to the handheld device database. When you tap the **Device** button, the application switches to the token database on the device.

Beaming the RSA SecurID Application

To beam the RSA SecurID application to another Palm handheld, you must beam both **SecurID** and **SecIDLib**. As a security precaution to prevent an unauthorized user from copying your unique token record and logging in to the system under your identity, you cannot beam a token. The token is set to operate only on the Palm handheld for which it is created and does not operate on other handheld devices.

When you beam the RSA SecurID application to another handheld device, the application is installed on the receiving handheld device in demo mode. To make the RSA SecurID application fully functional, the user must obtain a valid RSA SecurID software token record file from an administrator and load it onto his or her handheld device.

For more information about beaming applications to another handheld device, see your device documentation.

Uninstalling the Application

Use the menu in the Applications Launcher on your Palm handheld to remove the RSA SecurID application from your handheld device. See your device documentation for information about removing applications.

Troubleshooting

You may encounter the following problems when using RSA SecurID Software Token 2.0 for Palm Handhelds.

The software token failed to load successfully.

The error is one of the following:

- The token distribution file is passphrase-protected. An incorrect passphrase was entered. Reenter your passphrase.
- The token distribution file contains a token that is the same as the token that is already installed on the handheld device. The existing token on the device is not overwritten.
- The token is bound to a handheld device, but the serial number is different than the serial number of your handheld device. Contact your administrator.
- The SecurID database on the handheld device already contains the maximum number of 10 tokens. You can delete one or more of the currently installed tokens and retry loading the token.

You received an "Access Denied" message when you tried to authenticate.

The clock settings on your handheld device are likely incorrect. Adjust the clock settings on your device. For instructions, see the documentation for your device.

Your device crashed and erased the SecurID application files.

Ask your administrator to provide you with the RSA SecurID application file and a token.

You forgot your token passphrase.

You cannot authenticate with that token. Contact your administrator.

You received an invalid passphrase message.

You entered an incorrect passphrase. Reenter your passphrase. If you have forgotten the passphrase, you cannot use the token. Contact your administrator.

You received a "Can't Delete Active Token" message when you tried to delete a token.

Change the active token from the token you want to delete to another token and then try deleting the first token again.

First printing: December 2003