Introduction
The RSA SecurID Software Token app transforms your Android smartphone into an RSA SecurID authentication device.

The app, when provided with a software token, allows you to verify your identity, or “authenticate,” to your VPN client application and other sensitive network resources with one-time passwords (OTPs) generated on your device.

How to Obtain Your OTP—PIN-Enabled Token
Normally, you are issued a token that requires a PIN, and you create your PIN during your first RSA SecurID authentication. If you have not yet created a PIN, see “Setting a PIN” before you attempt to authenticate. When you start the RSA SecurID app, it detects that your token requires a PIN and displays the screen associated with the type of PIN-enabled token that you were issued.

Enter PIN screen. If the Enter PIN screen is displayed, you enter your PIN and touch the Enter button. The app displays a passcode, which is your PIN combined with the current tokencode. The passcode is your OTP.

Tokencode screen. If the Tokencode screen is displayed, you do not enter anything in the RSA SecurID app. Instead you enter your PIN in the protected application. Next to your PIN, you type the current tokencode. This combination is your OTP.

How to Obtain Your OTP—PINless Token
Your IT or Help Desk administrator may issue you a token that does not require a PIN. When you start the RSA SecurID app, it displays the Tokencode screen. The current tokencode is your OTP.

Installing the RSA SecurID App

Important: You must install the RSA SecurID app from Android Market. The app is available at no cost.

To install the RSA SecurID app:
1. Verify that you have an Internet connection.
2. In your list of apps, touch the Market icon.
3. Do one of the following:
   • Touch Apps, and touch the Communication category. Scroll to RSA SecurID.
   • Touch Search, enter the keywords RSA SecurID, and touch the Search icon.
4. Touch RSA SecurID Software Token.
5. Touch Install.
   The device displays a list of functions to which the application will require access.
6. Touch OK to start the download.
   The status icon displays the progress of the download. When the download is complete, a notification icon appears in the status bar. Additionally, the app is listed in the Notifications window.

Provide the Device ID (if Required)
Before issuing you a software token, your IT or Help Desk administrator may ask you to provide the device ID that identifies your device to your service provider. The administrator uses the ID to associate your token with your specific device. This prevents the token from being imported to another device.

Your device ID is either an IMEI (International Mobile Equipment Identity) or an MEID (Mobile Equipment Identity). Use the following instructions to locate the IMEI/MEID.

To locate the IMEI or MEID:
1. Touch the RSA SecurID icon to open the app.

2. Touch Menu > About.
3. Locate the IMEI/MEID number.
4. Touch Menu > Copy IMEI/MEID.
5. Open your device e-mail client, and paste the IMEI/MEID into an e-mail message. Send the e-mail to your IT or Help Desk administrator.
Importing a Software Token

After you have installed the app and, optionally, provided your device ID to your IT or Help Desk administrator, you are ready to import a software token. Your token will be delivered to your device in an e-mail message. You can import a token in the following ways:

- From a link within an e-mail
- From the Import Token screen in the app

Before You Begin:
Verify that your device has an Internet connection.

Important: To complete your token import, you may need to enter a one-time token activation code or a token password provided by your administrator. Make sure that you have the activation code or password available before starting the token import.

Import a Token—E-mail Link

Your administrator sends an e-mail to your device. A link within the message contains your software token data.

To import a token from a link in an e-mail:

1. In your device e-mail, open the message, and touch the link.
2. When prompted to select which application to open (Complete action using), touch RSA SecurID.
3. If your administrator provided you with a token activation code or token password, enter this information, and touch OK.

Important: If a progress indicator is displayed, wait for the import to finish. Do not cancel the import.

4. After you have imported the token, delete the e-mail containing the link.

Import a Token—Import Token Screen

If you cannot import your token by touching a link in an e-mail that your administrator sent to your device, you must use the Import Token screen in the RSA SecurID app to import your token.

To import a token using the Import Token screen:

1. In your device e-mail, open the message containing the token data.
2. Open your device’s Copy function (for example, by using a long press), and touch Copy.
3. Select the data that starts with the string “http://127.0.0.1/securid". Do not omit characters or include extra spaces or characters.
4. Touch the RSA SecurID icon to open the app.
5. Touch the Menu > Import Token.
6. On the Import Token screen, touch Menu > Paste to paste the token data into the Enter Token Data field.
7. Touch Import.
8. If your administrator provided you with a token activation code or token password, enter this information, and touch OK.

Important: If a progress indicator is displayed, wait for the import to finish. Do not cancel the import.

9. After you have imported the token, delete the e-mail containing the token data.

Note: If you used the RSA Self-Service Console to create a PIN or you were issued a token that does not require a PIN, see “Authenticate.”

You can set a PIN starting from one of the following screens in the RSA SecurID app:
- Enter PIN screen
- Tokencode screen

Before You Begin
1. Start the RSA SecurID app, and leave it open.
2. Do one of the following:
   - If the Enter PIN screen is displayed, see the following topic, “Set a PIN—Enter PIN Screen.”
   - If the Tokencode screen is displayed, see “Set a PIN—Tokencode Screen.”

The following procedures use a VPN client as an example of the resource that requires identity verification before granting you access.

Set a PIN—Enter PIN Screen

To set a PIN using the Enter PIN screen:
1. On your computer, connect to your VPN client.
2. Enter the user name that your administrator assigned you, and leave the logon screen open.
3. On your device, in the Enter PIN screen, enter four zeros (0000), and touch the Enter button, or swipe left.

4. Read the tokencode from your device.

5. On your computer, enter the tokencode, without spaces, in the Passcode field, and click OK. In this example, you would enter 69278520.

6. On your computer, enter and confirm your new PIN. Memorize your PIN.

7. On your device, wait for the tokencode to change.

8. On your device, swipe right or press the Back button to return to the Enter PIN screen.

9. Enter the PIN that you created, and touch the Enter button, or swipe left.

A passcode is displayed.

Note: The Passcode screen displays the seconds remaining before the passcode changes. If the passcode changes before you can submit it, in the next step, enter the next passcode.

10. On your computer, enter the passcode in the Passcode field, and click OK.

Set a PIN—Tokencode Screen

To set a PIN using the Tokencode screen:

1. On your computer, connect to your VPN client.
2. Enter the user name that your administrator assigned you, and leave the logon screen open.

3. Read the tokencode from your device.

4. On your computer, enter the tokencode, without spaces, in the Passcode field, and click OK. In this example, you would enter 07019425.

You are prompted to create a PIN. Your PIN must contain 4 to 8 digits, or your administrator may instruct you to use a combination of 4 to 8 digits and letters.

5. On your computer, enter and confirm your new PIN. Memorize your PIN.

You are prompted for a passcode.

6. On your device, wait for the tokencode to change.

Note: The Tokencode screen displays the seconds remaining before the tokencode changes. If the tokencode changes before you can submit it, in the next step, enter the next tokencode.
7. Return to your VPN client. In the Passcode field, enter your PIN, followed by the tokencode displayed on your device. Click OK.

### Authenticate

Use the following instructions to authenticate with your software token. The example used in the following procedure is a VPN client application that resides on your computer.

**To authenticate:**

1. On your computer, connect to your VPN client.
2. Enter the username that your administrator assigned you, and leave the logon screen open.
3. On your device, touch the RSA SecurID icon to start the app.
4. Do one of the following:
   - If Enter PIN screen is displayed, enter your PIN, and touch the Enter button, or swipe left. The device displays a passcode. Enter the passcode, without spaces, in the Passcode field on your computer.
   - If the Tokencode screen is displayed, and you have a PIN-enabled token, enter your PIN in the Passcode field on your computer, and then enter the tokencode displayed on your device, without spaces, to the right of your PIN.
   - If you have a PINless token, enter the tokencode displayed on your device, without spaces, in the Passcode field on your computer.

**Note:** The Passcode or Tokencode screen displays the seconds remaining before the code changes. If the code changes before you can submit it, enter the next code.

5. Click OK.