RSA® SecurID® Software Token 2.2 for Android Quick Start

Introduction

Welcome to RSA SecurID Software Token 2.2 for Android, authentication software that transforms your Android smartphone or tablet into an RSA SecurID authentication device.

To use the app, you must import a software token. The app generates a new tokencode every 60 or 30 seconds. You use the current tokencode to access resources protected by SecurID, for example, your corporate VPN. If your software token requires a SecurID PIN, you use a PIN combined with the tokencode, which is a passcode. The tokencode or passcode is your one-time password (OTP).

This document describes how to install the Token app and how to import and use a software token. You can import up to 10 software tokens to your device. You must import each token separately.

Install the Token App

Install the free app from Google Play (Play Store).

To install the app:

1. Make sure your device has an Internet connection.
2. In your list of apps, tap the **Google Play** or **Play Store** icon.
3. Tap **Search**, and enter the keywords **RSA SecurID**.
4. Select **RSA SecurID Software Token**.
5. Tap **Install**.

   The device displays a list of functions to which the application will require access.
6. Tap **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. The app is also listed in the Notifications window.

Start the Token App

To start the app:

1. In your app list, tap the Token icon.
2. Read the license agreement and select **I have read and accept the terms of the agreement**. Tap **Continue**.

Next Step

After you accept the license agreement, you are ready to import a software token.

- If your administrator asked for your device ID, go to the following section, "Email Your Device ID."
- If your administrator sent you a software token without asking for your device ID, go to the section "Import a Software Token."

Email Your Device ID

Your administrator may ask for your device ID before sending you a token. The device ID will be used to bind the software token to your device to ensure that the software token cannot be used on another device. Make sure an email account is set up on your device. Make sure you have your administrator's email address.

To email your device ID:

1. On the Welcome screen, tap **Device ID**.
2. Do one of the following:
   - Tap **Email Device ID** to open an email message containing the device ID.
   - Tap **Copy Device ID** to copy the device ID.
3. If you select the email option, enter your administrator's email address in the **To:** field, and send the email.
4. Go to "Import a Software Token."

Email Your Device ID for Additional Tokens

If you need additional software tokens, and your administrator wants to bind them, you must provide your device ID with each request. Your device ID is displayed in the Information screen.

To email your device ID for additional tokens:

1. Tap **Info**.
2. Do one of the following:
   - Tap **Device ID** > **Email Device ID** to open an email message containing the device ID.
   - Tap **Device ID** > **Copy Device ID** to copy the device ID.
3. If you select the email option, enter your administrator's email address in the **To:** field and send the email.
4. Go to "Import a Software Token."

Import a Software Token

You will receive your software token in an email message as a file attachment or URL link, or your administrator may have you scan a QR Code®. You may also need to enter one of the following when prompted:

- A password
- A one-time activation code

Make sure you have the password or activation code on hand before starting to import your token.

Use one of the following import procedures, depending on the email instructions you received.

Email Attachment

To import a software token from an email attachment:

1. Open the email on your device and locate the message with the file attachment (.sdtid file extension).
2. Tap the file attachment.
3. If prompted, enter the password. Tap **OK**.
4. For security reasons, delete the email.

RSA® SecurID® Software Token 2.2 for Android Quick Start

URL Link

To import a software token from a URL link in email:

1. Open your device email and locate the message with the URL link.
2. Tap the URL link.
3. When prompted to "Complete action using," tap **Token**.
4. If prompted, enter the activation code or password. Tap **OK**.
5. If prompted to accept a server certificate, tap **Accept**.
6. For security reasons, delete the email.

Import URL Option

Use the following manual procedure if you cannot import a token by tapping a URL link.

To import a software token using the Import URL option:

1. Open your device email and locate the message with the URL link.
2. The URL link starts with **http://127.0.0.1/securid**. Tap and hold the link and select the Copy option.
3. Navigate to the Token app. On the Welcome screen, tap **Import Token > Import URL**.
4. In the text field, tap and hold, then tap **Paste**.
5. If prompted, enter the activation code or password and tap the Enter button.
6. If prompted to accept a server certificate, tap **Accept**.
7. For security reasons, delete the email.

Note: To import additional tokens manually, tap **Token List**, and then tap **Import URL**.

Scan QR Code

Follow your administrator's instructions to access the QR Code containing your token data, then use the following instructions to capture the QR Code.

To import a software token by scanning a QR Code:

1. Navigate to the Token app. On the Welcome screen, tap **Import Token > Scan QR Code**.
2. Make sure the QR Code is entirely and clearly visible. Point the camera towards the QR Code to capture it.
3. If prompted, enter the activation code or password and tap **OK**.

Note: To import additional tokens by scanning a QR Code, tap **Token List**, and then tap **Scan QR Code**.

Set a PIN

Note: If your token does not require a PIN, go to "Authenticate to a Protected Resource."

Before You Begin

Depending on the token imported, when you start the Token app, you see the Enter PIN screen or the Tokencode screen.

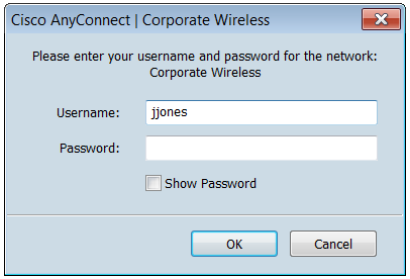
Do one of the following:

- If you see the Enter PIN screen, go to the next section, "Set a PIN (Enter PIN Screen)."
- If you see the Tokencode screen, go to "Set a PIN (Tokencode Screen)"

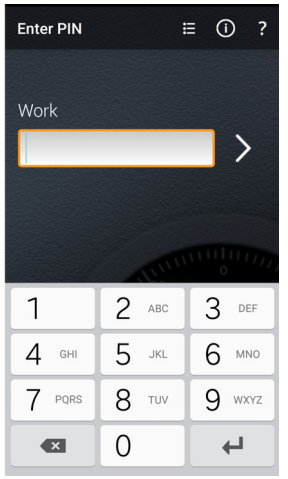
Set a PIN (Enter PIN Screen)

To set a PIN from the Enter PIN screen (VPN Example):

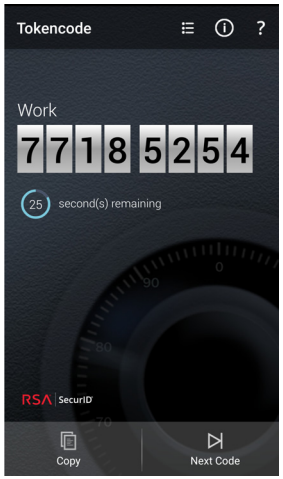
1. From your PC (or your device, if applicable), connect to your corporate VPN.
2. Enter your user name, and leave the logon screen open.



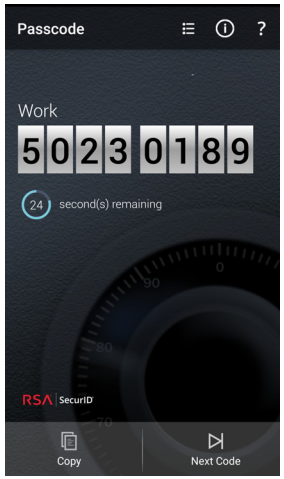
3. On your device, start the Token app.
4. In the Enter PIN screen, tap the **Enter** key or swipe left.



Your device displays a tokencode.



5. In the VPN logon screen, enter the tokencode in the **Passcode or Password** field. You are prompted to create a PIN. Your PIN must contain 4 to 8 digits and cannot begin with a zero.
6. Enter and confirm your new PIN. The VPN prompts for a passcode.
7. On your device, tap the **Back** button or swipe right to return to the Enter PIN screen.
8. Enter your PIN, and tap the **Enter** key or swipe left to display a passcode.



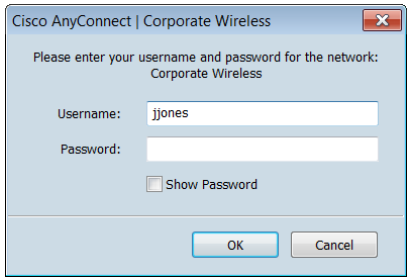
9. In the VPN logon screen, enter the passcode and click **OK**.

Note: If you access your VPN client on your device, you can tap **Copy** on the app menu to copy the passcode, then paste the passcode into the VPN logon screen.

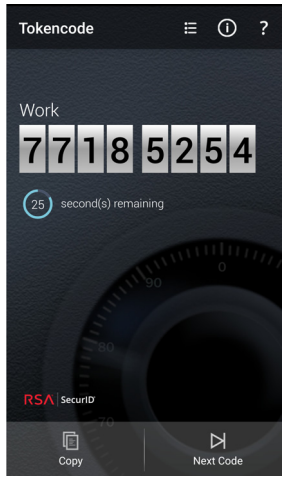
Set a PIN (Tokencode Screen)

To set a PIN from the Tokencode screen (VPN Example):

1. From your PC (or your device, if applicable), connect to your corporate VPN.
2. Enter your user name, and leave the logon screen open.



3. On your device, start the Token app, and view the tokencode.



4. In the VPN logon screen, enter the tokencode in the **Passcode or Password** field. You are prompted to create a PIN. Your PIN must contain 4 to 8 characters and cannot begin with a zero.
5. Enter and confirm your new PIN. The VPN prompts for a passcode.

6. On your device, tap **Next Code**.
7. Return to the VPN logon screen. In the **Passcode or Password** field, enter your PIN. (In this example, the PIN is 18395862.) Enter the tokencode to the right of the PIN. Click **OK**.

Authenticate to a Protected Resource

Use the following instructions to authenticate to a protected resource on your computer or your device. In the following example, the resource resides on a computer.

Select a Token (If Needed)

If you have several software tokens and you need to use a token other than the active token, select the token before you start the authentication process.

To select a different token:

1. On your device, start the Token app.
2. Select **Token List**.
3. Tap the name of the token you need. This activates the token.

Authenticate

To authenticate (VPN Example):

1. Connect to your corporate VPN.
2. Enter your user name and leave the logon screen open.
3. On your device, start the Token app.
4. Do one of the following:
   - If you see the Enter PIN screen, enter your PIN, and tap **Enter**. The device displays a passcode. Enter it in the **Passcode** (or **Password**) field of your VPN.
   - If your token requires a PIN, and the Token app displays the Tokencode screen, enter your PIN in the **Passcode** (or **Password**) field of your VPN, then enter the tokencode to the right of your PIN.
   - If your token does not require a PIN, enter the tokencode in the **Passcode** (or **Password**) field of your VPN.

Authenticate with the Next Code

Sometimes, after you enter your one-time password, you may be prompted to enter the next code (tokencode or passcode) to complete your authentication. This can occur for different reasons, such as entering too many incorrect one-time passwords in succession. Requiring the next code helps ensure that the code is being generated by a token in the possession of the authorized owner.

To authenticate with the next code:

1. When prompted for the next code, return to the Token app on your device.
2. Tap **Next Code**.
3. In the protected resource, enter the code.

Revised: November 2016
Published in the USA.