RSA SecurID® Software Token 2.2 for Android Administrator's Guide

Contact Information

RSA Link at **https://community.rsa.com** contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

Dell, RSA, the RSA Logo, EMC and other trademarks, are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. For a list of RSA trademarks, go to **www.emc.com/legal/emc-corporation-trademarks.htm#rsa**.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell Inc. or its subsidiaries, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by Dell Inc.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

Dell Inc. believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

August 2017

Contents

Preface

About This Guide

This guide is intended for RSA Authentication Manager administrators and IT personnel who will provision and deploy software tokens. Do not make this guide available to the general user population, with the exception of Appendix A, which an administrator might choose to distribute.

This guide provides the following information:

- A description of the supported token types
- An overview of the methods for provisioning and deploying software tokens
- Information on security features provided for the software token app
- A troubleshooting section with workarounds for common issues, and a list the error and informational messages provided by the app.
- Procedures for installing and using the software token app that an administrator can distribute to users

Product Documentation

For more information about RSA SecurID Software Token for Android, see the following documentation:

Release Notes. Provides information about what is new and changed in this release, as well as other pertinent information.

Quick Start. Helps users install the app and import software tokens. Also describes how to use a token for RSA SecurID authentication. The *Quick Start* is located in the **android220_doc.zip** archive and is available in all supported languages. RSA recommends distributing the *Quick Start* to users.

Help. Describes the app screens and associated procedures. You access the Help from the app on the device.

Related Documentation

RSA Authentication Manager 8.x Administrator's Guide. Provides an overview of Authentication Manager and its features. Describes how to configure the system and perform a wide range of administration tasks, including managing users and security policies and provisioning RSA SecurID tokens.

For RSA Authentication Manager documentation on RSA Link, go to: **https://community.rsa.com/community/products/securid**.

Security Console Help. Describes day-to-day administration tasks performed in the Security Console interface used with RSA Authentication Manager. To view Help, click the **Help** tab in the Security Console.

RSA SecurID Authentication Engine 2.8.1 for Java Developer's Guide. Describes APIs that allow you to integrate RSA SecurID strong authentication directly into your homegrown apps.

To access the RSA SecurID Authentication Engine 2.8.1 (SAE) documentation, go to: **https://community.rsa.com/community/products/securid**.

RSA SecurID Software Token Converter 3.1 Administrator's Guide. The Token Converter 3.1 is a command line utility for converting individual RSA SecurID software token files into alternative delivery formats, including custom compressed token format (CTF) URLs and QR Codes. QR Codes can be scanned into the Token app. To download the Token Converter, go to **https://www.rsa.com/en-us/products-services/identity-access-management/securid/software-tokens/software-token-converter**

RSA SecurID Software Token Security Best Practices Guide. Describes best practices designed to ensure secure operation of RSASecurID software token apps.

To access the *Best Practices Guide*, go to **https://community.rsa.com/docs/DOC-35128**.

Support and Service

RSA Link – RSA SecurID Space	**https://community.rsa.com/community/products/securid**
Customer Support	**https://community.rsa.com/community/rsa-customer-support**
RSA Ready Partner Program	**www.rsaready.com**

RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

Before You Call Customer Support

Make sure you have access to the device running RSA SecurID Software Token for Android.

Please have the following information available when you call:

- ❑ Your RSA Customer/License ID.
- ❑ Product software version number.
- ❑ The model of the Android device on which the problem occurs.
- ❑ The Internet connection(s) available on the Android device (3G/4G and Wi-Fi, or Wi-Fi only).
- ❑ The Android OS version under which the problem occurs.

1 Overview

About RSA SecurID Software Token for Android

RSA SecurID Software Token for Android is authentication software that transforms an Android device into a network authentication device. The software consists of a mobile app and separately installed software tokens. With a token installed, the app generates 6-digit or 8-digit pseudorandom numbers, called tokencodes (one-time passwords), at regular intervals. Authorized users with Android devices can use tokencodes, in combination with an RSA SecurID PIN, for two-factor authentication when they access resources protected by SecurID, such as Virtual Private Networks (VPNs) and web applications.

Before provisioning and deploying software tokens, an administrator must do the following:

- Determine how users will authenticate. For more information, see "Supported Token Types" on page 10.
- Decide whether to generate SDTID files, CTF URL links, or CT-KIP URL links. For more information, see "Provisioning and Distribution Methods" on page 12.
- Decide whether to bind each token to a specific Android device or leave the default binding (device class GUID.) For more information, see "Device Binding" on page 16.

Supported Token Types

RSA SecurID Software Token for Android supports the following token types for user authentication:

- **PIN integrated with tokencode (PINPad-style).** The user enters an RSA SecurID PIN in the Enter PIN screen on the Android device to produce a passcode (one-time password). The user authenticates by entering the passcode in the protected resource. The user experience is similar to authenticating with an RSA hardware device that contains a key pad for PIN entry.
- **PIN followed by tokencode (fob-style).** The user authenticates by entering a SecurID PIN in the protected resource, followed by the current tokencode displayed on the device. The user experience is similar to authenticating with an RSA hardware fob that displays tokencodes.
- **Tokencode only.** The user authenticates by entering the current tokencode displayed on the device (no PIN required).

Important: Because tokencode-only authentication does not use two-factor authentication, RSA strongly recommends that you require the standard logon password in addition to the tokencode. For more information about the proper use of tokens that do not require a PIN, see the *RSA SecurID Software Token Security Best Practices Guide* on RSA Link at **https://community.rsa.com/docs/DOC-35128**.

Software Token Management Features

RSA SecurID Software Token for Android supports the following features for managing tokens:

- **Multiple Token Support.** Users can import up to 10 software tokens per device. An RSA Authentication Manager server can provision three software tokens to an individual user. RSA SecurID software tokens can be provisioned to the same device by different companies.
- **Token Nicknames.** Users can set token names to identify their tokens. Token names are called "nicknames" in the authentication servers. Nicknames can contain up to 32 alphanumeric characters, must be unique, must be alphabetic or alphanumeric, and are not case sensitive.

  As the administrator, you can optionally set a nickname when configuring a token record. If you do not set a nickname, tokens are imported to the app with default names based on installation order: Token 1, Token 2, and so on. The user can rename tokens after importing them to the app.

  If you use Self-Service provisioning with RSA Authentication Manager 8.1 or later, you can allow users to set a nickname when they request a token. The token is imported into the app with the user-supplied nickname.

- **Delete Token option.** Users can delete any token, including the Active token. Users who delete all of their tokens must contact an administrator to request replacement tokens, or use Self-Service if it has been deployed.
- **Token Expiration Warning.** Software tokens used with the Android app expire at 00:00:00 GMT of the token's expiration date. To ensure that the user always has a working software token installed, the OTP screen (Tokencode or Passcode) displays a notification starting 30 days before the expiration date. For example, if a token will expire on July 31, a notification is displayed on July 1 and thereafter. If the user allows the token to expire, the Expired Token screen is displayed with information about the expired token. The user can contact the administrator or use Self-Service (if allowed) to request a replacement token.

Provisioning Software Tokens

To provision software tokens and authenticate Android device users, you need a supported version of RSA Authentication Manager, as described in the *Release Notes*, or RSA SecurID Authentication Engine 2.8.1 for Java.

RSA Authentication Manager supports two methods for deploying RSA SecurID software tokens:

- **Security Console.** The administrator initiates the process of assigning and distributing the user's token using the Security Console, a web-based administrative console.
- **Self-Service Console.** The administrator configures Self-Service provisioning and allows the user to create an account. The user then enrolls to use Self-Service and requests a software token, using a web-based Self-Service Console.

  Self-Service provisioning is included with the Authentication Manager Enterprise Server license.

For RSA Authentication Manager documentation on RSA Link, go to: **https://community.rsa.com/community/products/securid**.

RSA SecurID Authentication Engine (SAE) is an Application Programming Interface (API) that provides the back-end authentication functions of RSA SecurID. After the API is successfully integrated into your environment, RSA SecurID users can be authenticated without needing an RSA Authentication Manager server. For more information, go to **https://community.rsa.com/community/products/securid**.

Provisioning and Distribution Methods

This section provides an overview of the methods available for distributing software tokens to Android devices.

QR Codes

RSA SecurID Software Token for Android supports scanning a CTF URL or CT-KIP URL encoded in a QR Code. The user points the device camera at the QR Code to automatically scan the token into the Token app.

Use one of the following methods to create the QR Code:

- **Generate a QR Code in RSA Authentication Manager 8.1 Service Pack 1 or later.** RSA Authentication Manager 8.1 Service Pack 1 (SP1) or later can generate QR Codes that each contain a CT-KIP URL. To use this feature, the Self-Service Console is required. An administrator must create a software token profile that uses the Android 2.x device type, dynamic seed provisioning (CT-KIP), and QR Codes.

  For more information, see the *RSA Authentication Manager Administrator's Guide* on RSA Link. Go to: **https://community.rsa.com/community/products/securid**.

- **Convert a CT-KIP URL to a QR Code with a Third-Party Conversion Tool.** RSA Authentication Manager 8.1 or later generates custom URLs containing CT-KIP data. The scheme portion of the custom CT-KIP URL is com.rsa.securid. This scheme is required when using custom CT-KIP URLs to provision software tokens to the Token app. After generating a custom CT-KIP URL, use a third-party QR Code conversion tool to embed the custom CT-KIP URL in a QR Code.

- **Convert a CTF URL or an SDTID file to a QR Code.** You can generate a legacy-format custom CTF URL containing token data using RSA Authentication Manager 8.1 or later, but you must use a third-party QR Code conversion tool to convert the custom CTF URL to a QR Code.

  If you use Authentication Manager to generate software token files (SDTID files), you can use the RSA SecurID Software Token Converter 3.1 (Token Converter 3.1) utility to convert an individual token file to a QR Code that contains a custom CTF URL.

  RSA SecurID Authentication Engine (SAE) for Java does not natively generate QR Codes. You must use the Token Converter 3.1 utility to convert an SDTID file to a CTF URL embedded in a QR Code.

  When Token Converter 3.1 converts an SDTID file to a QR Code, the output is a JPEG file containing the QR Code image. The Token app can scan the QR Code to import the token. If you password-protect the SDTID input file, the app prompts for the password to complete the QR Code import.

  Download RSA SecurID Software Token Converter 3.1 from **https://www.rsa.com/en-us/products-services/identity-access-management/securid/software-tokens/software-token-converter** and follow the instructions in the *RSA SecurID Software Token Converter 3.1 Administrator's Guide.*

Dynamic Seed Provisioning

Dynamic seed provisioning uses the Cryptographic Token Key Initialization Protocol (CT-KIP) to eliminate the need for a token distribution file (SDTID file).

Note: RSA recommends using the RSA Authentication Manager dynamic seed provisioning feature because the CT-KIP process is engineered to prevent the potential interception of the token's seed. Only use SDTID or CTF if your company policy dictates that the Token apps cannot connect to the Internet or that a CT-KIP server cannot be set up.

You deliver a dynamically provisioned token to the Token app with a QR code or by sending an email message containing a custom CT-KIP URL hyperlink to the email client on the Android device. The user scans the QR code or taps the URL link in the email to import the token.

File-based Provisioning (SDTID Files)

RSA Authentication Manager and RSA SecurID Authentication Engine (SAE) for Java are designed to generate software token files (SDTID files). RSA strongly recommends protecting SDTID files with a token file password as part of the provisioning process.

To deliver a token, you send an email with an SDTID file attachment to the email client on the Android device. If you password-protect the file, RSA recommends sending the password separately, using a secure channel and best practices for communicating sensitive data.

Compressed Token Format (CTF Strings)

Compressed token format (CTF) is an alphanumeric or numeric format for delivering software tokens to mobile devices.

RSA Authentication Manager 8.1 and later generates CTF strings in a legacy numeric format, as described in the *RSA Authentication Manager Administrator's Guide*. If you require alphanumeric CTF strings, use Authentication Manager to provision password-protected SDTID files and then convert them using the RSA SecurID Software Token Converter 3.1 (Token Converter) command line utility.

RSA SecurID Authentication Engine (SAE) for Java administrators obtain CTF strings by exporting the token to an SDTID file. Convert the password-protected SDTID file using the Token Converter 3.1.

Note: RSA strongly recommends protecting CTF strings with a strong password. Set the password on the SDTID file when provisioning the token in Authentication Manager or when exporting the token to an SDTID file using SAE for Java. Use the -password option on the Token Converter command line.

By default, Token Converter 3.1 generates alphanumeric CTF strings appended to a URL. To deliver the CTF string, you send an email containing the URL to the user's device. The user taps the URL to import the token, and enters the password to complete the import.

To download the Token Converter and documentation, go to **https://www.rsa.com/en-us/products-services/identity-access-management/securid/software-tokens/software-token-converter**

Provisioning Software Tokens Using the Security Console

RSA Authentication Manager includes the web-based Security Console that allows an administrator to provision and distribute software tokens. An RSA Authentication Manager Super Admin must create a software token profile. Software token profiles specify software token configuration and distribution options.

If you plan to use several provisioning methods (for example, CT-KIP and CTF), create separate software token profiles for each method so that you do not have to edit the profile to change the distribution method.

When you add a software token profile, you must create a software token profile for Android that uses the Android 2.x device definition file.

For more information, see the *RSA Authentication Manager Administrator's Guide* on RSA Link. Go to: **https://community.rsa.com/community/products/securid**.

Provisioning Software Tokens Using the Self-Service Console

RSA Authentication Manager 8.1 or later includes RSA Self-Service. The Self-Service Console provisioning component allows users to request RSA SecurID tokens, including software tokens.

Self-Service provisioning requires the following tasks:

1. **Setting up the Self-Service Console.** You must set up the Self-Service Console before users can request software tokens. To access the set-up options, in the RSA Security Console, click **Setup > Self-Service Settings**.

   In the **Provisioning** section, you need to work with the following:

   - **Workflow Policies.** Use workflow policies to define the number of approval or distribution steps and customize email notifications to be sent to users who request software tokens.

     Note: RSA recommends reviewing the email notification template to determine if you need to customize the notification.

   - **Manage Authenticators.** Use this option to select the software token profiles to use for provisioning and the settings you can configure for Self-Service.

     After you select an Android software token profile, do the following:

     – You can replace the default display name and description.

     – In the **Application Installation Download URL** field, enter the Google Play URL. The URL will be displayed in the request approval email sent to the user.

     – (Optional) The Token app has embedded Help. The product kit contains a *Quick Start* document (PDF) for users. In the **Device Help Document URL**, enter the URL where you are hosting the software token *Quick Start*. The URL will be displayed in the request approval email sent to the user.

2. **Provide information for users to request software tokens.** For information that you can distribute to users, see "Requesting Software Tokens in the Self-Service Console" on page 31.
3. **Approve software token requests.**

For more information, see the *RSA Authentication Manager Administrator's Guide* on RSA Link. Go to: **https://community.rsa.com/community/products/securid**.

Software Token App Security Features

RSA SecurID Software Token for Android includes the security features described in this section.

Token Security on the Device

After a token is imported to an Android device, it is protected with a set of system attributes. When the app needs to open the token database, it queries the system for the set of attributes and checks them for validity. If an unauthorized user or malware attempts to copy the token database to another machine or device, the user cannot obtain tokencodes or the app appears as not having a token. If the user obtains a new device, the software token must be reissued.

Next Code Retrieval

RSA Authentication Manager and RSA SecurID Authentication Engine can detect when a user provides multiple incorrect one-time passwords (OTPs) in succession. (The default of invalid OTP entries is three.) This situation may be caused by user error, time drift on the device running the app, or it may indicate that an unauthorized user has gained access to the token and is attempting to use it. When this occurs, the authentication server places the token into Next Tokencode mode. The user must enter the next successive code (tokencode or passcode) to authenticate. Requiring the user to provide the next code helps ensure that the code is being generated by a token in the possession of the authorized owner.

The Token app provides a Next Code option that allows a user whose token is in Next Tokencode mode to immediately retrieve the next code, eliminating the need for the user to wait until the next interval.

Software Token Configuration

RSA strongly recommends using device binding and token passwords for software tokens.

Device Binding

When provisioning a software token record in Authentication Manager, you can bind the token by configuring a token extension attribute (DeviceSerialNumber). Binding is engineered to allow installation only on a specific device or class of devices. RSA strongly recommends binding both file-based and CT-KIP tokens.

You can bind software tokens intended for Android devices to one of the following:

Android device class GUID (globally unique identifier)

By default, software tokens provisioned for Android devices in RSA Authentication Manager 8.x are bound to the Android 2.x device class GUID (globally unique identifier).

The Android device class GUID allows the user to import the token to any Android device that is supported by the Token app. It prevents the token from being imported to other types of mobile devices or to desktops or laptops running an RSA SecurID software token app.

The Android device class GUID is:

a01c4380-fc01-4df0-b113-7fb98ec74694

Device ID

A device ID is a unique sequence of 24 letters and numbers assigned to a specific Android device by the Token app. A token bound to a device ID cannot be used on any other device.

Note: Uninstalling and reinstalling the Token app generates a new device ID. If a user reinstalls the app, you must obtain the new device ID and update the user's software token record in your authentication server.

You bind tokens to a device ID when configuring the token in Authentication Manager. The user must first provide the device ID. After installing the Token app, the user can select **Device ID** on the Welcome screen and choose one of the following options:

- **Email Device ID.** This option opens an email that is prepopulated with the device ID. The user enters the administrator's e-mail address in the **To:** field. Make sure you provide an email address to users so they can send you the email containing their device ID.
- **Copy Device ID.** This option copies the device ID to the device clipboard. Users who have a Self-Service account on Authentication Manager 8.x or 7.1 can access the Self-Service URL through their device browser and paste the device ID into a device binding field when requesting a software token.

Instruct users to treat the device ID as sensitive information and to use a secure channel to deliver it to the administrator. After the user sends the administrator the device ID, the administrator should use a separate, secure channel to communicate the information needed by the Token app to complete the provisioning process, for example, the CT-KIP URL

Determine Your Device Binding Option

Use the information in the following table to decide which binding option best suits your requirements.

Binding Option	Comments
Android device ID	• The token engineered to allow installation only on the device with the specified device ID. • In a administrator-driven provisioning scenario, requires the administrator to obtain the device ID from the user before configuring the token record. • In a Self-Service provisioning scenario, the user can obtain the device ID from the Token app and enter the device ID when requesting a software token.
Android device class GUID	• The token can be installed on any Android device. • Prevents ability to import the token to a computer or mobile device other than Android. • Allows administrators to bind all tokens to the same device class. • For Authentication Manager 8.x, eliminates the need to configure a token extension attribute since the device class GUID is the default binding entry.

Token Passwords

SDTID files and compressed token format (CTF) strings should be protected during transit by assigning a unique password in RSA Authentication Manager. The user must enter the password in the installed RSA SecurID software token app to complete the token import. The CTF should not be communicated together with the device ID.

Assigning a unique token password can help protect against unauthorized users gaining access to an SDTID file or CTF string and attempting to import the token to a different device. However, if the software token does not use device binding, the password does not prevent a user who has access to both the SDTID file or CTF string and the password from installing the token on multiple devices. For this reason, RSA strongly recommends using both device binding and password protection.

2 Troubleshooting

Problems Installing the App

This section describes problems that users might encounter when installing the app, and provides workarounds.

Problem	Workaround
The app cannot be found on Google Play.	The user has an unsupported device. For hardware requirements, see the *Release Notes*.
The user cannot install the app.	The device does not have network connectivity, or a network failure occurred. Instruct the user to establish a network connection and reattempt to install the app. If this is unsuccessful, instruct the user to attempt to install another app.
The Android device does not have enough space to install the app.	Instruct the user to free up space on the device.

Problems Launching the App

If a user cannot launch the app following installation, provide the following workaround:

1. Open the device Settings.
2. Disable Airplane mode (if enabled).
3. Turn on Wi-Fi.
4. Launch the Token app.

Note: The device does not require a connection to a Wi-Fi network, and Wi-Fi can be turned off immediately after successfully launching the app.

Token Import Problems

The Token app stores information about successful and unsuccessful token imports in a log. The log messages are duplicates of the messages users receive when a token import succeeds or fails. The log stores up to 20 entries. Once the maximum is reached, the oldest log messages are deleted. If a user cannot import a token, ask him or her to access the token import log from the Information screen as follows.

Procedure

1. Tap **Info**.
2. Tap **Import Token Log**.

You can have the user read you the pertinent log messages or ask the user to copy the messages to the device clipboard and paste them into an email.

The following table lists problems users might encounter when attempting to import tokens and suggested workarounds.

Problem	Workaround
User Error	
The user cannot import a token because the app has not been installed on the device.	The user must download and install the app before attempting to import a token.
In a file-based import (SDTID or CTF), the user forgot the token file password or entered an incorrect token file password.	The user must retry with the correct password or contact the administrator for the password.
The user attempted to import a dynamically provisioned token (CT-KIP), but the import failed because the device does not have network connectivity.	The user must establish a network connection. Open the device's browser and try connecting to the URL.
Administrator Error These errors might occur when configuring the token in RSA Authentication Manager.	
The token is not intended for an Android device.	If you issue tokens in Authentication Manager 8.x, verify that you selected the Android 1.x or Android 2.x device type.
The token device binding is incorrect. For example, the administrator may have entered an incorrect device ID when binding the token to a device.	Correct the token device binding and reissue the token.

Problem	Workaround
The token type is not supported, for example, 64-bit SID.	Provision a 128-bit (AES) token.
The death date of the token lifetime configured in Authentication Manager has passed.	Provision a new token.
CT-KIP Errors	
The user cannot import a token because of an error in the CT-KIP URL link. The most likely cause is that the administrator used an older, unsupported link format.	Correct the CT-KIP URL link format, and reissue the token. The URL link must start with the following prefix text: http://127.0.0.1/securid/ctkip?scheme=
The email message containing the URL link did not reach the user's device.	In rare cases, this can occur due to a network communication failure. Instruct the user to refresh the mailbox. If necessary, re-send the email to the user's device.
The device cannot interpret URL links. Nothing happens when the user taps the link.	Instruct the user to copy the link from the email and use the app's Import Token option to manually import the token.
Other	
The user cannot launch the app or import a software token, because the app cannot retrieve device information.	• This problem affects HTC devices on a CDMA network if the device was set to Airplane mode or turned on in an area that did not have a cell signal. Instruct the user to disable Airplane mode, (if enabled), verify that the device has a network connection, and restart the device. • This problem can also occur if the user attempts to launch the app or import a token from a CT-KIP URL link on a Wi-Fi only device without the Wi-Fi connection turned on.

Problem	Workaround
Compressed Token Format Errors	
The user cannot import a token because of an error in the CTF URL link. The most likely cause is that the administrator used an older, unsupported link format.	Correct the CTF URL link format, and reissue the token. The URL link must start with the following prefix text: http://127.0.0.1/securid/ctf?ctfData=
The SDTID file was not converted properly with the Token Converter utility. For example, the -p *password* option was not specified for converting a password-protected token file.	Review the instructions in the *RSA SecurID Software Token Converter 3.1 Administrator's Guide.*
The Token Converter could not convert the SDTID file because the file contained double-byte characters in the **UserFirstName**, **UserLastName**, or **UserLogin** fields.	Double-byte characters are not allowed in these fields.
The user could not import a token from an SDTID file that contained multiple tokens.	Each SDTID file can contain only one token.
Import from Email Errors	
The device cannot interpret URL links. Nothing happens when the user taps the link.	Instruct the user to copy the link from the email and use the app's Import Token option to manually import the token.

Authentication Problems

This section describes problems that users might encounter when attempting to authenticate, and provides workarounds.

Problem	Workaround
User Error	
The token was disabled due to too many failed logon attempts.	Check the Authentication Manager logs. If the token is not disabled (or expired), ask the user to read you the current tokencode and the next tokencode. After you obtain the pair of tokencodes, resynchronize the token in Authentication Manager. **Note:** Instruct users with PIN-enabled tokens to tap the **Enter** button to display the tokencode. No PIN is required.
The user attempted to authenticate before setting a PIN.	Instruct the user to follow the instructions in the user *Quick Start* or app Help to set a PIN.
The user entered an incorrect PIN or entered the PIN in the wrong location. For example, when authenticating when a fob-style token, the user may have entered the tokencode, followed by the PIN, instead of entering the PIN, followed by the tokencode.	Instruct the user on how to authenticate. Provide the user *Quick Start* or remind the user to access the app Help.

Problem	Workaround
Other	
The time on the Android device may be out of synchronization with the clock settings in Authentication Manager.	Instruct the user to access the Information screen in the app and read you the time shown in the **GMT** field. The SecurID algorithm uses Coordinated Universal Time (UTC or GMT) settings to calculate the current one-time password. Software tokens rely on the client device to determine the correct UTC time value. For this reason, the local time, the time zone, and Daylight Saving Time must all be set correctly so that users can perform RSA SecurID authentication from their devices. Users who cross time zones with their devices only need to change the time zone to reflect the correct local time.
One or more tokens have expired.	The user can delete the tokens and contact the administrator to request replacement tokens or use Self-Service, if allowed.

Error Messages

The following table lists error conditions that users might encounter and associated error messages displayed by the Token app.

Condition	Error Message
The PIN contains fewer than 4 digits or more than 8 digits.	Invalid PIN characters. PIN must contain 4 to 8 digits.
The device does not have a network connection.	Network access is not enabled. Please enable network access.
The user entered an incorrect token file password.	Invalid password. Token import failed. Contact your administrator.
The device cannot establish a network connection, or the CT-KIP server is not operating.	Error communicating with server. Token import failed.
The CT-KIP or CTF URL format is incorrect.	Invalid URL. Token import failed. Contact your administrator.

Condition	Error Message
Format of token data was incorrect.	Token import failed. Invalid token data. Contact your administrator.
An incorrect CT-KIP server URL or activation code was used.	Invalid activation code. Token import failed.
An invalid token was issued, for example, a 64-bit token, 90-second token, or 9-digit token.	Unsupported token. Token import failed. Contact your administrator.
The token sent to the user was bound to a different device.	Invalid device binding. Token import failed. Contact your administrator.
The user attempted to import an expired token.	Token has expired. Please contact your administrator to request a replacement token.
The user attempted to install the token without a network connection.	RSA application data is inaccessible. Please enable 3G/4G or Wi-Fi network. Contact your administrator.
The device was turned on in Airplane mode or in a location that did not have cellular service.	RSA SecurID cannot retrieve device information. Please verify your network connection and restart your device.
The app cannot retrieve the import token log. This could occur in rare cases because the token database is corrupted or the log table is locked by another process.	Unable to retrieve log. Please contact your administrator.
A CTF string created with Token Converter 3.1 has expired.	The URL for importing the token has expired. Please contact your administrator to request a new URL.
A QR Code created with Token Converter 3.1 has expired.	The QR Code for importing the token has expired. Please contact your administrator to request a new QR Code.
An error occurred that caused the app to close. The administrator should contact RSA Customer Support.	The app has encountered an error. Please contact your administrator.

Information Messages

The following messages provide feedback and instructions to the user.

Condition	Information Message
This message may be displayed during a CT-KIP import for a variety of reasons, for example, if your RSA Authentication Manager CT-KIP implementation uses a self-signed certificate.	Accept Server Certificate The certificate for this server was signed by an unknown certifying authority. If you trust this server, tap Accept to continue.
The token was successfully stored in the token database.	Token successfully imported.
The user attempted to import a CT-KIP URL while the import is already in progress.	Token import is already in progress. Please allow the process the finish.
The user selected "Wi-Fi with SIM Card" availability, but has not disabled Airplane mode before attempting to launch the app for the first time.	Disable Airplane mode through your Settings options and restart your device.
The user selected "Wi-Fi Only" availability but has not enabled Wi-Fi before attempting to launch the app for the first time.	Turn on Wi-Fi through your Settings options.
The user selected "Wi-Fi with SIM Card" availability, but has not disabled Airplane mode or enabled Wi-Fi before attempting to launch the app for the first time.	Disable Airplane mode or turn on Wi-Fi through your Settings options. No data will be sent through network.
The user successfully copied the import token log messages.	Log messages copied successfully.

A Installing and Using the Token App

As needed, you can provide the information in this chapter to your users. For example, you can print and distribute the appropriate authentication procedures.

Install the App

The Token app can be downloaded and installed for free from Google Play. Software tokens must be purchased separately from RSA or an RSA Secured Partner.

Upgrades

To upgrade from version 2.0 or later of the app, install version 2.2.4 from Google Play. The software token that the user used with the earlier version of the app will continue to work with the new app.

Before Launching the App

Before launching the app for the first time, the user must do the following:

- Disable Airplane mode (if enabled).
- Turn on Wi-Fi. The device does not need to connect to a Wi-Fi network. As soon as the user launches the app, the user can turn off Wi-Fi.

Note: If the device is Wi-Fi only, the user must leave Wi-Fi on to import a token from a CT-KIP URL.

Font Size Setting

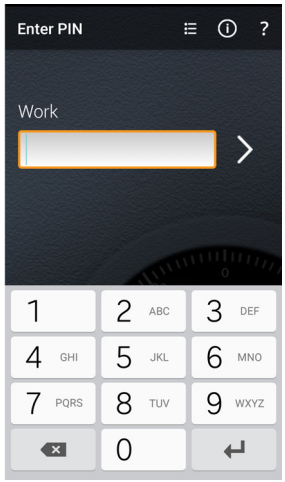
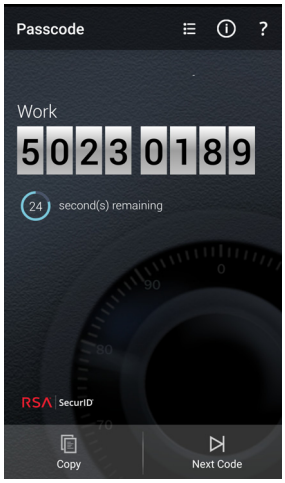
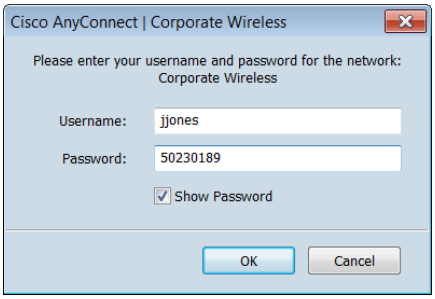
The Token app has been optimized for the Normal font size setting. Using a setting larger than the Normal setting affects the look of certain screens in the app.

Authentication Procedures

This section describes three user authentication options. You can provide the appropriate procedures to your users.

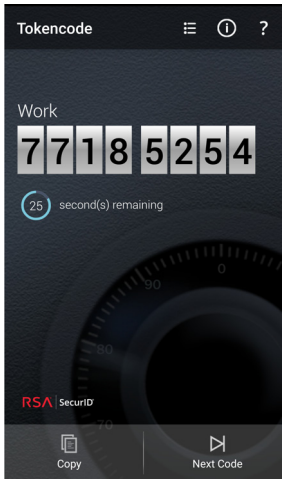
Passcode Authentication (PINPad-Style)

The following table shows how a user authenticates to a VPN client with a PINPad-style software token (PIN integrated with tokencode).

1	Enter the PIN in the Token app on the device.	
2	View the passcode (PIN integrated with the tokencode).	
3	Enter the passcode in the protected resource (for example, a VPN).	

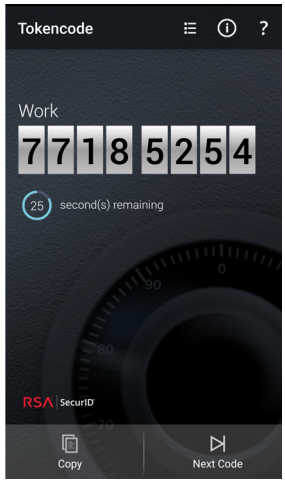
Passcode Authentication (Fob-Style)

The following table shows how a user authenticates to a VPN client with a fob-style software token (PIN entered in protected resource, followed by tokencode).

1	View the tokencode in the Token app on the device.	
2	Enter the PIN in the protected resource (for example, a VPN). The PIN in this example is 18395862.	
3	Enter the tokencode to the right of the PIN in the protected resource (for example, a VPN).	

Tokencode-Only Authentication

The following table shows how a user authenticates to a VPN client with a tokencode. No PIN is required.

1	View the tokencode in the Token app on the device.	
2	Enter the tokencode in the protected resource (for example, a VPN).	

Requesting Software Tokens in the Self-Service Console

The following procedure describes the steps for requesting software tokens for RSA SecurID Software Token for Android. Use this information to assist first-time users.

User Procedure

1. Log on to the Self-Service Console URL.
2. On the My Account page, under **My Authenticators**, click **Request a new token**. The **Select a Token** section shows an Android token selected.
3. Under **Provide Your Token Details**, in the **DeviceSerialNumber** field, do one of the following, as directed by your IT administrator:
   - Leave the default entry.
   - Replace the default entry with your Android device ID.
4. (Optional) In the **Nickname** field, enter a user-friendly name for your token. The nickname can contain up to 32 characters and must be alphabetic or alphanumeric.
5. If required, enter and confirm a token password. Memorize the password. You will be prompted for the password when you import your token to your device.
6. In the **Create Your PIN** section, create and confirm a PIN of 4 to 8 digits. The PIN cannot begin with a zero.

   Important: Memorize your PIN. If you forget your PIN, you will need to access the Self-Service Console to reset the PIN before you can continue using your token.

7. In the **Reason for Token Request** section, enter the reason that you need a software token, for example, "To access the corporate VPN."
8. Click **Submit**.
9. Print the confirmation page, then **OK** to return to your My Account page. The **My Authenticators** section lists your pending request. When your IT administrator approves the request, you will receive an email notification with instructions for importing the token to your device.