SecurID Authenticator App Administrator's Guide

SecurID

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

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

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.

Copyright © June 2020 World Wide Web Consortium, (MIT, ERCIM, Keio, Beihang). http://www.w3.org/Consortium/Legal/2015/doc-license (for https://w3c.github.io/webauthn/)

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 RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA 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." RSA 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.

February 2022

Contents

Preface

About This Guide

This guide is for administrators who manage SecurID Authentication Manager and the Cloud Authentication Service, and who deploy the SecurID Authenticator app to their users. Do not make this guide available to the general user population.

For a complete list of SecurID documentation, see SecurID Link.

SecurID Support and Service

You can access community and support information on SecurID Link at https://community.securid.com. SecurID Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Support for SecurID Authentication Manager

Before you call Customer Support for help with the SecurID Authentication Manager appliance, have the following information available:

- Access to the SecurID Authentication Manager appliance.
- Your license serial number. To find this number, do one of the following:
  - Look at the order confirmation e-mail that you received when your ordered the product. This e-mail contains the license serial number.
  - Log on to the Security Console, and click **License Status**. Click **View Installed License**.
- The appliance software version. This information is located in the top, right corner of the Quick Setup, or you can log on to the Security Console and click **Software Version Information**.

Support for the Cloud Authentication Service and Identity Routers

If your company has deployed identity routers and uses the Cloud Authentication Service, SecurID provides you with a unique identifier called the Customer Support ID. This is required when you register with SecurID Customer Support. To see your Customer Support ID, sign in to the Cloud Administration Console and click **My Account > Company Settings**.

RSA Ready Partner Program

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

Chapter 1: Overview

This chapter introduces SecurID Authenticator for macOS and provides general information.

About SecurID Authenticator for macOS

SecurID Authenticator for macOS is authentication software that runs on 64-bit macOS computers and allows users to verify their identity to resources protected by SecurID. SecurID Authenticator 5.0 for macOS app supports both SecurID Software Token and cloud-based multifactor authentication to manage all your authentication needs. Be it on-prem, cloud, or hybrid infrastructure, you will now have one single app to manage effectively. By adding support for cloud MFA for macOS users, the new authenticator helps move your authentication to the cloud with continued support for software tokens. With the SecurID Authenticator, users can enter the SecurID Software Token (OTP) or cloud-based multifactor authentication, along with other security information, to gain access to Virtual Private Networks (VPNs) and web applications. The application provides strong two-factor authentication and eliminates the need for the user to carry a separate hardware token or mobile device.

.

Software Token Management Features

The SecurID Authenticator app supports the following features for managing software tokens:

- **Multiple Token Support.** Users can import up to 10 software tokens per device. An Authentication Manager server can provision three software tokens to an individual user. 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. Nicknames must be unique, are case sensitive, and cannot consist entirely of spaces.

  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 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. Users who delete all of their tokens must contact an administrator to request replacement tokens, or use Self-Service if available.
- **Token Expiration Warning.** Software tokens expire on the first second of the token expiration date (00:00:00 GMT). To ensure that the user always has a working software token installed, the app displays a warning indicating how many days remain before the token expires, starting 30 days before the expiration date. The user can contact the administrator or use a Self-Service (if available) to request a

replacement token.

You will be able to easily extend the lifetime of expired tokens in a way that is transparent to users. You use the Security Console to extend a token’s availability. Users will not see token expiration dates in the app.

Users will be able to replace tokens with the same serial number without deleting the token first.

Cloud based Multi Factor Token Management Features

- **Multiple Token Support.** Users can import up to 10 authenticate tokens per device. SecurID authenticate tokens can be provisioned to the same device by different companies.
- **Rename a Token Card**. Users can rename an account card so that they can instantly recognize it in the SecurID Authenticator app.
- **Delete the Account**. Users can delete any account, including the Active ones.
- **PIN Management**. If the CAS Server is configured to require PIN to view Authenticate Tokencodes, then the Users can perform the below operations:
    - Users can set PIN during their first time Viewing of Authenticate Tokencode.
    - Users can Reset their PIN.
    - Users can use Forgot PIN option to reset their PIN if they forgot their existing PIN.

App Security Features

SecurID Authenticator app includes the following security features.

Token Security on the Device

After the macOS computer is registered to CAS or a token is imported to the SecurID Authenticator app, it is protected with unique application data that cannot be migrated to another device. 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 and the macOS computer needs to be re-registered to CAS.

Next Code Retrieval for Software Token

RSA Authentication Manager or RSA SecurID Authentication Engine can detect when a user provides multiple incorrect tokencodes or passcodes in succession. In this situation, the user is prompted to enter the next tokencode or passcode to authenticate. This requirement helps ensure that the code is being generated by a token in the possession of the authorized owner.

In the app, click **Next Code icon (Right arrow which is present beside the token displayed)** , this will eliminate the need for the user to wait until the next interval.

Virtualized Environments

TheSecurID Authenticator for macOS has not been fully tested and qualified in virtualized environments. RSA Customer Support will initially assist you with issues that occur on virtualized machines, but may eventually request that you reproduce the issue on a supported physical machine before they proceed further with the case.

Clock Settings

The SecurID Authenticator app and SecurID Authentication Servers rely on Coordinated Universal Time (UTC). The time, date, and time zone settings on the local computer and on the computer running Authentication Manager must always be correct in relation to UTC. If the time settings on a user's computer change significantly, they will no longer be synchronized with the time settings on the Authentication Manager host, and the user may not be able to authenticate. If this happens, the user must contact the server administrator to have the token resynchronized.

Instruct users to verify that the time, time zone, and Daylight Saving Time (DST) settings on their computer are correct before they use the SecurID Authenticator app. Users crossing time zones with their computer need to change only the time zone in order to reflect the correct local time.

Chapter 2: Installing and Using the SecurID Authenticator App

System Requirements

You can install SecurID Authenticator 5.0 on macOS computers running the following operating systems:

- macOS Monterey (12.0 or later)
- macOS BigSur (11.0 or later)

Intel and Apple M1 ARM based processors are supported.

Installation Package

SecurID Authenticator installation package, **SecurID Authenticator 5.0 for macOS.dmg**, contains the following:

- SecurID Authenticator.app (application file)
- Device Definition File (containing macOS-5.0-swtd.xml - Upload to AM if macOS 5.0 device type is not available for software token distribution)
- Alias to Application (can be used to drag and drop the Application to /Applications)
- Alias to UninstallSecurIDAuthenticator.command (can be used to uninstall the SecurID Authenticator for macOS app)

.

Install and Manage the SecurID Authenticator for macOS App

The SecurID Authenticator app can be installed directly onto a device from the App Store or from MDM. The new app has a new icon in the App Store.

Install from DMG

1. Ensure your account is having administrator privileges.
2. Download the zip file containing the DMG of SecurID Authenticator 5.0 for macOS from SecurID link.
3. Extract the zip file and double click to open it and mounts it to your macOS computer..
4. Drag and drop the **SecurID Authenticator** app to the **Applications** folder.
5. Click on the launchpad and verify that you see **SecurID Authenticator** app.

Note: SecurID Authenticator 5.0 for macOS can co-exist with SecurID Software Token 4.2.3

Authentication Procedures

Authentication Procedures with Software Token

Authentication Procedures with Multifactor Authentication

Uninstall the SecurID Authenticator for macOS App

Please follow the below steps to Uninstall SecurID Authenticator for macOS:

1. Open terminal.
2. sudo "/Applications/SecurID\ Authenticator.app/Contents/SharedSupport**/UninstallSecurIDAuthenticator.command**"

   Or double click the

   "**UninstallSecurIDAuthenticator.command**" present in /Applications/SecurID\.app/Contents/SharedSupport/

Chapter 3: Software Token Overview

Managing Software Token

The SecurID Authenticator 5.0 for macOS app supports SecurID software tokens. With a software token installed on the user's macOS computer, the app generates 6-digit or 8-digit pseudorandom numbers, called tokencodes (one-time passwords), at regular intervals. Users can use a tokencode, in combination with a PIN, to access resources protected by SecurID, such as Virtual Private Networks (VPNs) and web applications.

Before provisioning and deploying software tokens, you must decide:

- How users will authenticate. See Supported Token Types.
- Whether to generate SDTID files, CTF URL links, or CT-KIP URL links. See Provisioning and Distribution Methods.
- Whether to bind each token to a specific macOS computer or leave the default binding (device class GUID.) See Device Binding.

Supported Software Token Types

SecurID supports the following software token types for user authentication:

- **PIN integrated with tokencode (PINPad-style).** The user enters a SecurID PIN in the Enter PIN text field on the macOS computer to produce a passcode (one-time password). The user authenticates by entering the passcode in the protected resource.
- **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 a hardware fob that displays tokencodes.
- **Tokencode only.** The user authenticates by entering the current tokencode displayed on the device (no PIN required).

Note: Because tokencode-only authentication does not use two-factor authentication, SecurID strongly recommend 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*.

Provisioning Software Tokens

To provision software tokens and authenticate macOS computer users, you need a supported version of Authentication Manager.

Authentication Manager supports two methods for deploying SecurID software tokens:

- **Security Console.** You initiate the process of assigning and distributing the user's token using the Security Console, a web-based administrative console.
- **Self-Service Console.** You configure Self-Service provisioning and allow 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.

See RSA Authentication Manager documentation on SecurID Link.

RSA SecurID Authentication Engine (SAE) is an Application Programming Interface (API) that provides the back-end authentication functions of SecurID. After the API is successfully integrated into your environment, SecurID users can be authenticated without needing an Authentication Manager server. For more information, see RSA SecurID Authentication Engine Documentation on SecurID Link.

Provisioning and Distribution Methods

This section provides an overview of the methods available for distributing software tokens to macOS computer.

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: SecurID recommends using dynamic seed provisioning because the CT-KIP process helps prevent the potential interception of the token's seed. Only use SDTID or CTF if your company policy dictates that the SecurID Authenticator apps cannot connect to the Internet or that a CT-KIP server cannot be set up.

You deliver a dynamically provisioned token to the SecurID Authenticator app by sending an email message containing a custom CT-KIP URL hyperlink to the email client on the user's device. The user clicks the URL link in the email or enters the link in the app to import the token.

To support dynamic seed provisioning (CT-KIP) on SecurID Authenticator device, you must make sure that the Authentication Manager server meets the App Transport Security (ATS) requirements. For more information, see App Transport Security Requirements for Dynamic Seed Provisioning on the facing page.

File-Based Provisioning (SDTID Files)

Authentication Manager and RSA SecurID Authentication Engine (SAE) for Java can generate software token (SDTID) files. SecurID 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 user's device.

If you password-protect the file, SecurID 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 macOS computer.

Authentication Manager 8.1 and later generates CTF strings in a legacy numeric format, as described in the Authentication Manager Help. 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: SecurID strongly recommends protecting CTF strings with a password. Set the password on the SDTID file when provisioning the token in Authentication Manager. 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 clicks the URL or enters the link in the app to import the token, and enters the password to complete the import.

To download the Token Converter and documentation, go to SecurID Software Token Converter

App Transport Security Requirements for Dynamic Seed Provisioning

ATS operates by default for apps linked against the iOS 9.0 or macOS 10.11 SDKs or later. This network encryption and security feature requires a server that supports Transport Layer Security (TLS) protocol version 1.2 or later with forward secrecy ciphers and certificates that are signed using a SHA-256 or later signature algorithm.

RSA Authentication Manager 8.1 Service Pack 1 (SP1) Patch 13 or later with the TLS 1.2 Mode update applied supports the required TLS encryption version, but you must ensure that the SSL console certificate used by Authentication Manager meets the ATS requirements.

If the SSL certificate that you use to secure your CT-KIP connections does not use SHA-256 or later, then you must replace it. The default RSA Authentication Manager SSL console certificates do not meet the ATS requirement. For instructions on replacing the Authentication Manager SSL console certificate, see the RSA Authentication Manager Administrator's Guide.

Also ensure that your entire Authentication Manager CT-KIP provisioning infrastructure is ATS compliant. Non-compliant network appliances, such as proxy servers, firewalls, and load balancers, might prevent CT-KIP provisioning requests from reaching the Authentication Manager CT-KIP server. These noncompliant appliances may require a simple SSL certificate replacement or more complicated firmware upgrades to achieve compliance. Contact your appliance vendor for further assistance in ensuring that your appliances are ATS compliant.

If you meet these requirements, then apps that are built with the RSA SecurID SDK 2.4 on Xcode 7.3.1 or later can perform CT-KIP provisioning with RSA Authentication Manager 8.1 Service Pack 1 (SP1) Patch 13 or later with the TLS 1.2 Mode update applied. Users who have SecurID Authenticator for macOS installed are not required to download additional updates to ensure compatibility.

For more information on ATS, go to

https://developer.apple.com/documentation/security/preventing_insecure_network_connections.

Provisioning Software Tokens Using the Security Console

Authentication Manager includes the web-based Security Console that allows you to provision and distribute software tokens. An Authentication Manager Super Admin must create a software token profile. The profile specifies 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, use macOS 5.0 device type (The macOS-5.0-swtd.xml device definition file which is included in the Installation Package) for SecurID Authenticator for macOS app.

For more information, see the RSA Authentication Manager Administrator's Guide on the *RSA Authentication Manager Documentation page* on SecurID Link.

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 SecurID tokens, including software tokens.

For more information, see the Help topic "RSA Self-Service Overview" on the *RSA Authentication Manager Documentation page* on SecurID Link.

Security Features for Software Token

The SecurID Authenticator app includes the security features described in this section.

Token Security on the Device

After a token is imported to an macOS computer, it is protected with unique application data that cannot be migrated to another device.

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 Tokencode Retrieval

RSA Authentication Manager and RSA SecurID Authentication Engine can detect when a user provides multiple incorrect one-time passwords (OTPs) in succession. By default, users are allowed to enter three invalid OTPs. 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.

When a user's token is in Next Tokencode mode, the user can click an arrow on the token card in the SecurID Authenticator app to immediately retrieve the next code without waiting for the next interval.

Show or Mask PIN

By default, PIN characters are masked as the user enters them. The user can click on the eye icon to show or hide the masked PIN characters.

Software Token Configuration

SecurID strongly recommends using the following for software tokens:

- Device binding
- Password protection for CTF and SDTID Files

Device Binding

When provisioning a software token record in Authentication Manager, bind the token by configuring a token extension attribute (DeviceSerialNumber). Binding allows installation only on a device or class of devices with a matching device ID.

SecurID strongly recommends binding all tokens to a device class GUID.

macOS Computer Class GUID (globally unique identifier)

Software tokens provisioned for macOS computer in Authentication Manager 8.1 or later are bound to a device class GUID (globally unique identifier). This option allows the user to import the token to any macOS computer that is supported by the SecurID Authenticator app. It prevents the token from being imported to other device platforms or to desktops or laptops running a SecurID Authenticator app.

The macOS computer class GUID is

{ad7a1a8a-91fb-4043-ad1b-c33b32dccc17}

Binding ID

A binding ID (called a device ID in previous versions of the Software Token app) is a unique, 24-character hexadecimal string generated by the SecurID Authenticator app running on a specific macOS computer. A token bound to a binding ID cannot be used by any other app running on the same device or a different device.

You bind a token when configuring it in Authentication Manager. The user must first provide you the binding ID, which is generated when the SecurID Authenticator app is installed. To send the binding ID, the user must have an email account configured on the device.

You must provide users with an email address. Instruct users to treat the binding ID as sensitive information and to use a secure channel to deliver it to you.

To view and email the binding ID, from the Welcome screen or Home screen, the user click **More > About**.

Determine Your Device macOS Binding Option

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

Binding Option	Comments
Binding ID	• The token can only be used by the app running on the device with the specified binding ID. • You must obtain the binding ID from the user before configuring the token record.
macOS computer	• The token can be installed on any macOS computer.

Binding Option	Comments
class GUID	• Helps prevent importing the token to a computer or mobile device other than macOS. • You can bind all tokens to the same device class. • For RSA Authentication Manager 8.1 or later, the macOS computer class GUID 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 your provisioning server. The user must enter the password in the SecurID Authenticator app to import the token.

Assigning a unique token password can help prevent unauthorized access. 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 URL and the password from installing the token on multiple devices. For this reason, SecurID strongly recommends using both device binding and password protection of SDTID files and CTF strings.

Authentication Procedures

Authentication Procedures for Software Token below

Using the SecurID Authenticator App for Cloud-Managed Multifactor Authentication

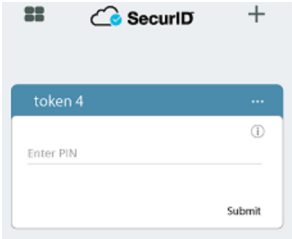
Authentication Procedures for Software Token

This section describes three user authentication options. You can provide the appropriate procedures to your users. Instructions for users are also provided at https://help.access.securid.com/EN_US/Content/Production/ngx_c_what_is_product.html.

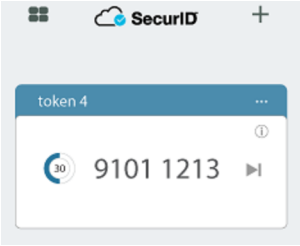
Passcode Authentication (PINPad-Style)

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

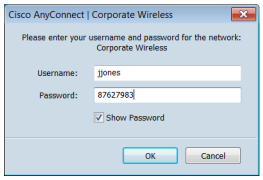
1. Enter the PIN in the SecurID Authenticator app and click **Submit**.



2. View the passcode (PIN integrated with the tokencode).



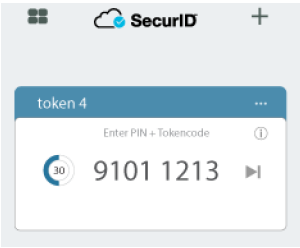
3. Enter the passcode in the protected resource (for example, a VPN).



Passcode Authentication (Fob-Style)

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

1. View the tokencode in the SecurID Authenticator app.



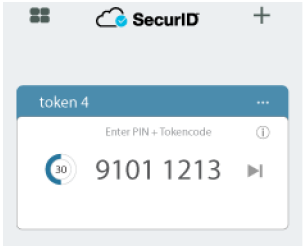
2. Enter the PIN in the protected resource (for example, a VPN). The PIN in this example is 13248675.

3. Enter the tokencode to the right of the PIN in the protected resource (for example, a VPN).

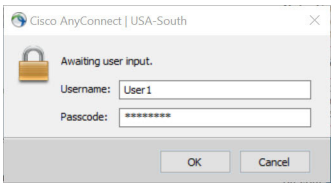
Tokencode-Only Authentication

The following procedure shows how to authenticate to a VPN client with a tokencode only. No PIN is required.

1. View the tokencode in the SecurID Authenticator app.



2. Enter the tokencode in the protected resource (for example, a VPN).



Chapter 4: Multifactor Authentication

Using the SecurID Authenticator App for Cloud-Managed Multifactor Authentication

The SecurID Authenticator for macOS supports the following authentication methods to access resources protected by the Cloud Authentication Service:

Authentiction Method	Reference
SecurID Authenticate Tokencode	https://community.securid.com/t5/securid-cloud-authentication/authentication-methods-for-cloud-authentication-service-users/ta-p/623038#Tokenco
Approve (Push Notifications)	https://community.securid.com/t5/securid-cloud-authentication/authentication-methods-for-cloud-authentication-service-users/ta-p/623038#Approve
Device Biometrics	https://community.securid.com/t5/securid-cloud-authentication/authentication-methods-for-cloud-authentication-service-users/ta-p/623038#Device

Users must register their devices before using these authentication methods. SecurID Software Token does not require registration.

Enable Notifications on User Devices

Users must respond to notifications during authentication with Approve or Biometrics. Instruct users to enable notifications on their devices so they can take advantage of these options.

Registering User Devices for Multifactor Authentication

Before using the SecurID Authenticator app to sign in to applications, your users must register their macOS computer. For more information MFA authentication options, see Approve, Authenticate Tokencode, and Biometrics.

Inform the users to refer SecurID Authenticator App Quick Start Guide.

Registration Methods

Users can register an macOS computer using the following methods.

Registration Method	Description
Use SecurID My Page.	My Page is a web portal that helps provide a secure way for users to register macOS computer using multifactor authentication or numeric registration codes. Users sign into My Page on device (for example, a computer), download the SecurID Authenticator app, and complete registration. If an administrator for one account uses the Cloud Administration Console to delete a user's registered device, the SecurID Authenticator app on the user's device continues to work normally for any other account. The activity from one account does not affect the app behavior for other accounts. By default, My Page is disabled. When you enable it, you can also select an access policy that determines which users are allowed to use My Page and which authentication requirements they must satisfy to access the page.
User enters an LDAP password as the Registration Code into the SecurID Authenticator app.	The user downloads SecurID Authenticator app on a device and enters the identity source email address, your Company ID, and the identity source password (as the Registration Code) in the app. You can use the Device Registration Using Password policy to restrict which users are allowed to complete device registration using this method.
User enters a Registration Code generated by the administrator.	You use the Cloud Administration Console to generate a numeric Registration Code and then securely provide it to the user. The user downloads the SecurID Authenticator app on a device and enters the user identity source email address, your Company ID, and the Registration Code in the app.

Account Re-Registration

The following table summarizes how SecurID handles registration with user or changes for macOS computer.

Situation	Resolution
A user completes registration, deletes or uninstalls the SecurID Authenticator app, and then later needs to complete registration again on the same device.	The user installs the SecurID Authenticator app again and re-registers the device without administrative action.
• A user completes registration on one device and then gets a new device. The user needs to complete registration on the new device. • A user performs a factory reset on a registered device and wants to reinstall the app on the same device.	The user can delete the current device in My Page , and then complete registration. Or the administrator must delete the

Situation	Resolution
	user's current device before the user can complete device registration again.
• An existing user who has completed device registration on the device no longer needs the device and gives the device to a new user. • An existing user who has completed device registration on the device no longer needs the device, performs a factory reset, and gives the device to a new user.	If necessary, the existing user deletes the device in My Page or deletes the company in the app. The new user installs the app and completes device registration without administrative action.

Registration with Multiple Accounts

An individual user can use theSecurID Authenticator app on a single registered device to authenticate to resources protected by up to 10 different accounts.

For example, a user who is a contractor for both Company A and Company B can use a single device to perform step-up authentication to access both companies. The user registers the device for one company and uses the My Accounts screen to add additional accounts as needed.

An administrator might use a single device for testing the behavior of the SecurID Authenticator app for a company's testing environment and production environment. If each environment has a unique company ID, the administrator adds an account for each company. Or if each environment uses the same company ID but has a unique user ID, the administrator adds an account for each user ID.

If an administrator for one account uses the Cloud Administration Console to delete a user's registered device, the SecurID Authenticator app on the user's device continues to work normally for any other account. The activity from one account does not affect the app behavior for other accounts.

Chapter 5: Managing Tokens and Accounts

Managing Software Token

Import a SecurID Software Token below

Set a PIN for SecurID Software Token below

Rename a SecurID Software Token Card on page 26

Delete a SecurID Software Token Card on page 26

View Information About My SecurID Software Token Card on page 27

Import a SecurID Software Token

You can import up to 10 software tokens to a macOS computer where the SecurID Authenticator app is installed.

- Import Token Using URL Link below
- Import Token Using Email File Attachment below

If your macOS computer already has a token and you are adding more, click the plus sign (+) in the upper right corner of the app to get started.

Import Token Using URL Link

Perform following steps.

1. Open the SecurID Authenticator app.
2. Open your email and find an email from your administrator.
3. Open the email and click the hyperlink or copy the URL to a browser or into the app.

   Your software token is now active.

Import Token Using Email File Attachment

Perform following steps:

1. Open the SecurID Authenticator app.
2. Open your email and find the email from your administrator.
3. Open the attached file. Enter the password your administrator provided if required.

   Your software token is now active.

Set a PIN for SecurID Software Token

If you need to set a PIN immediately after importing a software token. These instructions are a general guide. Your IT Help Desk will provide specific information if necessary.

You must reset your PIN if you forget it or it becomes compromised. Use the reset method provided by your IT Help Desk.

1. On your macOS computer, connect to your VPN client or protected application. Enter your username. Leave the dialog box open.
2. Open the SecurID Authenticator app.
3. If your app displays **Enter SecurID PIN**, perform these steps. If you do not see **Enter SecurID PIN**, go to step 4.
    a. Leave the PIN field blank and click **Submit** to view the tokencode.

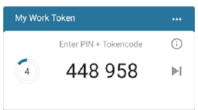
    b. On your macOS computer, in the **Passcode** field, type the tokencode, without spaces, and click **OK**.
    c. When prompted, enter a PIN that contains 4 to 8 numeric digits. It cannot begin with zero. Memorize the PIN.
    d. Confirm the PIN.

    You are prompted for a passcode.
    e. In the app, return to the **Enter SecurID PIN** screen.
    f. Enter the PIN you just created and click **Submit**.

    The passcode appears. This code combines the PIN and tokencode.
    g. Go to the VPN client or application sign-in screen. In the **Passcode** field, type the passcode without spaces. Click **OK**.

    After you set the PIN, you are ready to sign in to applications.
4. Use this method only if you did not perform step 3.
    a. In the VPN client or protected resource screen, enter your user name.
    b. In the **Passcode** field, enter the tokencode that is displayed in the app, without spaces, and click **OK**.

    Tokencode displayed in app:

    c. When prompted, create a PIN that contains 4 to 8 digits. It cannot begin with a zero. Memorize the PIN.
    d. Enter and confirm the PIN.

You are prompted for a passcode.

e. In the app, click **Next Code**.

A tokencode appears.

f. On your macOS computer, in the **Passcode** field, first enter your PIN, then the tokencode in the same field, without spaces. For example:

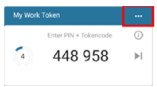
g. Click **OK**.

After you set the PIN, you are ready sign in to applications.

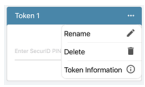
Rename a SecurID Software Token Card

It's a good idea to rename your token so that you can instantly recognize it in the SecurID Authenticator app.

1. Open the SecurID Authenticator app.
2. Click the menu icon (**...**) in the upper right corner of the token card.



3. Click **Rename**.

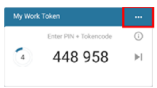


4. Enter the name of your token.
5. Click **Save**.

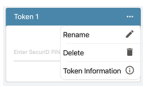
Delete a SecurID Software Token Card

You can delete the SecurID software token from your macOS computer after it expires or if it is no longer needed.

1. Open the SecurID Authenticator app.
2. Click the menu icon (**...**) in the upper right corner of the token card.



3. Click **Delete**.

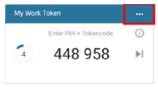


4. When prompted, click **Delete** to confirm.

View Information About My SecurID Software Token Card

You can view the Name, Serial Number, and Device Name associated with your software token.

1. Open the SecurID Authenticator app.
2. Click the **More** menu (**...**) in the upper right corner of the token card.



3. Click **Token Information**.

Managing Cloud Multi Factor Accounts

Add an Account below

Rename a Token Card on the next page

Delete the Account from Your SecurID Authenticator 5.0 App on the next page

Send Email Logs for Troubleshooting on page 29

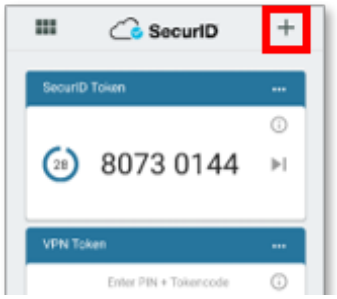
Add an Account

You can add multiple accounts to a single macOS computer for the same company. Each account must use a different username. For example, you can register a macOS computer with Company A, then add accounts using username1@example.com for Account 1 and username2@example.com for Account 2. Or you can add accounts for the same company to different smartphones or macOS computer, using a different username for each account. The accounts can use different apps or the same app.

You can add up to twenty accounts (maximum 10 SecurID Software Token and maximum 10 for Authenticate Tokencode) in the SecurID Authenticator app.

Procedure

1. Open the SecurID Authenticator app.
2. Click the plus sign (+) in the upper right corner of the app screen.

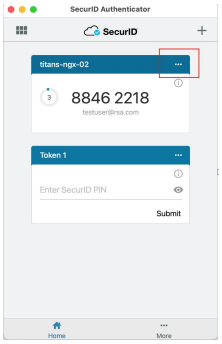


3. Follow the prompts to complete registration.

Rename a Token Card

You can rename an account card so that you can instantly recognize it in the SecurID Authenticator app.

1. Open the SecurID Authenticator app.
2. Click the menu icon (**...**) in the upper right corner of the token card.

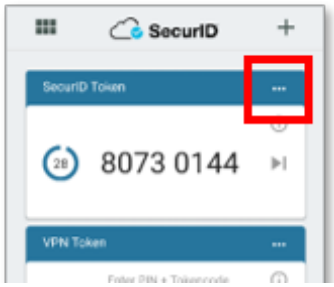


3. Click **Rename**.
4. Enter the name of your token.
5. Click **Save**.

Delete the Account from Your SecurID Authenticator 5.0 App

Procedure

1. Open the app on your macOS computer.
2. On the company account card, click the menu (**...**) in the top right corner.



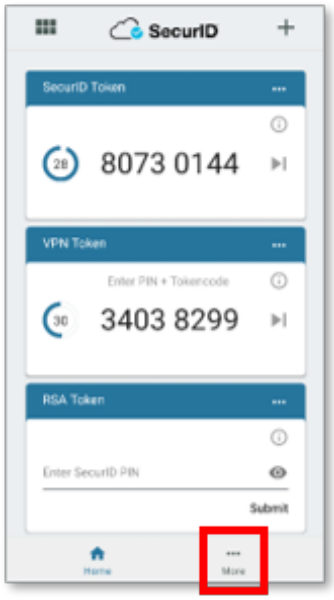
3. Click **Delete**.
4. Confirm the delete when prompted.
5. Continue for every account.

Send Email Logs for Troubleshooting

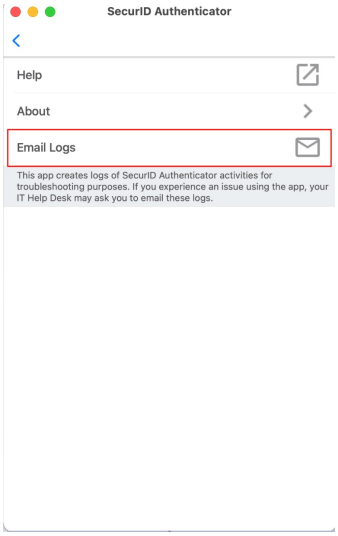
The SecurID Authenticator app automatically creates log files that are used to diagnose problems.

Procedure

1. Open the app.
2. On the home screen, click **More...** in the lower right corner.



3. Click **Email Logs**.



4. When prompted, describe the issue.

Chapter 6: Troubleshooting

This section includes issues for software tokens and MFA (Approve, Authenticate Tokencode, and Biometrics) and the available workarounds for resolving the issues.

Email Logs

The SecurID Authenticator 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 500 lines. After the maximum is reached, the oldest log messages are deleted. If a user cannot import a token, ask the user to send you the log file as follows.

1. From the app Home screen, click **More**.
2. Click **Email Logs**.
3. The user selects the email application. Instruct the users on how to send the logs to you.

Note: SecurID Authenticator uses Apple Mail client to send the logs, If your organization restricts or Apple Mail client is not configured, you can instruct user to fetch the logs from "~/Library/Containers/com.rsa.securid.iphone.SecurID/Data/Documents/SecurIDAuthenticatormacOS Logs.log"

Installation Issues

The following table lists problems that users might encounter while installing the app and provides workarounds.

Problem or Message	Workaround
You need an email account to share the Binding ID and email logs.	Apple mail client has to be configured on the macOS computer.
The SecurID Authenticator for macOS app cannot be found in the Apple App Store.	The user has an unsupported version of macOS. The app supports devices running macOS 11.0 or later.
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 retry. If this is unsuccessful, instruct the user to attempt to reinstall the app again.
Your account cannot be deleted. Contact your IT Help Desk.	Instruct the user to confirm if there is a secure internet connection.

Problem or Message	Workaround
The device does not have enough space to install the app.	Instruct the user to free up space on the device.

Troubleshooting Token Issues

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

Problem	Workaround
User Error	
User says the token is missing.	Follow your process to re-import the token. If you suspect a bug, have the user email you the logs. To email logs: 1. In the app, locate and click **More**. 2. Click **Email Logs** and send the log file to the address in your process. If Apple mail client is not configured on the macOS Computer on which SecurID Authenticator is installed, you can instruct user to fetch the logs from "~/Library/Containers/com.rsa.securid.iphone.SecurID/Data/Documents/SecurIDAuthenticatormacOSLogs.log"
Token is missing while screen share	If whole screen is sharing , please stop the screen share.
Your device has reached the maximum token limit.	The user has already reached the maximum limit of 10 software tokens and attempted to import another token. **Note:** Maximum of 20 Token cards (10 Authenticate tokencode and 10 SecurID Software tokens are supported) The user must delete one token before importing another one.
The user cannot import a token because the SecurID Authenticator app is not installed on the device.	The user must download and install the SecurID Authenticator app before importing a token.
The imported token is not intended for this device and has been removed.	Provision a new token for the user.

Problem	Workaround
Contact your IT Help Desk.	
In a file-based import (SDTID or CTF), the user forgot the token file password or entered an incorrect token file password.	Inform the user to retry the password. If it still fails, send the user a new 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 first establish a network connection, then try again to import the token.
Administrator Error The following errors may occur as a result of misconfiguring the token in Authentication Manager.	
The token import failed.	Verify that you selected the macOS 5.0 device type. Correct the token device binding ID and reissue the 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	Correct the CT-KIP URL link, and reissue the token. • The URL link must start with the following prefix text: com.rsa.securid://ctkip?url= ctkipData=

Problem	Workaround
administrator probably used an older, unsupported link format.	
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 user cannot import a token because the wrong email message format was used.	Embed the custom CT-KIP URL within a hyperlink, and set the message format to HTML.
Compressed Token Format Errors	
The user cannot import a token because of an error in the CTF URL link.	The administrator probably 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: com.rsa.securid://ctf?ctfData=
The SDTID file was not converted properly with the Token Converter due to a command line error.	See 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**,	Double-byte characters are not allowed in these fields.

Problem	Workaround
UserLastName, or **UserLogin** fields.	
The user successfully imported the first token from an SDTID file containing multiple tokens, but cannot import the remaining tokens.	The SecurID Authenticator app only imports the first token in a multi-token file and ignores the remaining tokens. Make sure each SDTID file contains only one token.
The user cannot import a token because the wrong email message format was used.	Embed the custom CTF URL within a hyperlink, and set the message format to HTML.
Nothing happens when the user clicks the URL link.	Instruct the user to copy the link from the email and paste it to import the token.

General Token Issues	
Problem	**Workaround**
Enter a unique name for your token. or Token name already exists on this device.	Instruct the user to enter a unique name for each token on a device.
Your token expired on [DATE]. Contact your IT Help Desk. Your token [TOKEN NAME] expires on [DATE]. Contact your IT Help Desk. Multiple Tokens About to Expire.	Provision a new token for the user.

Troubleshooting Registration Issues

The following table lists problems users might encounter during registration.

Problem	Workaround
Registration data expired. Contact your IT Help Desk.	Send the user valid registration information.
Unable to complete registration	In the Cloud Administration Console, click **Users > Management**. Confirm if the user is enabled. If the user is already enabled, tell the user to share the logs for analyzing the errors.
Your device has reached the maximum account limit.	The user has already reached the maximum limit of 10 Authenticate tokencodes and attempted to import another token. **Note:** Maximum of 20 Token cards (10 Authenticate tokencode and 10 SecurID Software tokens are supported) The user must delete one token before importing

Problem	Workaround
	another one.
Activation certificate invalid. Contact your IT Help Desk.	User should try using a separate network. If the issue persists, tell the user to share the logs for analyzing the errors.

Troubleshooting Authentication Issues

This section describes the workarounds to problems that users might encounter when attempting to authenticate.

Problem	Workaround
User Error	
The token was disabled after 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 click **Submit** 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 SecurID Authenticator app Help to set a PIN.
The user entered an incorrect PIN or entered the PIN in the wrong location. For example, when authenticating with 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 with the specific token type. See the app Help home page or in the app, click the (i) icon on the token card.
Other	
The user is unable to authenticate.	The time on the macOS computer may be out of sync with the clock settings in Authentication Manager. The local time, the time zone, and Daylight Saving Time must all be set correctly so that users can authenticate from their devices. Instruct the user to verify that the time zone matches with the local time zone.
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.
The confirmation code in the app does not match with	The user can delete the app, reinstall and re-register

Problem	Workaround
the code that displays on the login screen.	the tokens.

Information_Messages

The following message provide feedback and instructions to the user.

Message	Condition
This server certificate was signed by an unknown certifying authority. If you trust this server, click **Accept** to continue.	This message may be displayed during a CT-KIP import for a variety of reasons, for example, if your Authentication Manager CT-KIP implementation uses a self-signed certificate.