Release Notes
RSA SecurID® Software Token 5.0.3 for Windows

July 2021

Introduction

RSA SecurID® Software Token 5.0.3 for Windows provides strong authentication from Windows desktops and laptops to Virtual Private Networks (VPNs) and other resources protected by RSA SecurID.

This document lists what's new in RSA SecurID Software Token 5.0.3 for Windows and contains other information you need before installing the application. It also describes workarounds for known issues. This document contains the following sections:

These *Release Notes* may be updated. The most current version can be found on RSA Link at **https://community.rsa.com**.

What's New in This Release

RSA SecurID Software Token 5.0.3 for Windows is a cumulative release that resolves customer-reported issues. For more information, see Fixed Issues.

Note: You must have administrator privileges to install or uninstall the application. In Windows 10, you must right-click the Windows Installer MSI file, and select **Run as administrator** to install the application, and you must select **Run as administrator** to launch the application. In all versions of windows, the command line installation must be run as an administrator.

When you install RSA SecurID Software Token 5.0.3 for Windows, or version 5.0.1 or version 5.0.2, the installer generates a unique device serial number for the location where tokens are stored. If the application is installed in the default location on the local hard drive, then launching the SecurID desktop application for the first time creates registry entries for the token storage device name and the device serial number.

RSA SecurID Software Token 5.0.3 for Windows, or version 5.0.2, changes the Device Name and Device Serial Number registry entries to the following location:

HKEY_CURRENT_USER\SOFTWARE\RSA\Software Token\Desktop\DeviceInformation

In version 5.0.1, the registry entries were in the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\RSA\Software Token\Library\ Plugins\DeviceInformation

Name	Type	Default Values	Description
Device Name	REG_SZ	Local Hard Drive (RSA)	This registry entry is only generated if the tokens are stored on the local hard drive. If the tokens are stored on a supported biometric device, a supported Trusted Platform Module (TPM), or another supported device plug-in, then a registry entry is not created. You can use the SecurID desktop application to see where a token is stored. Click **Options > Manage Token**, and select **Token Storage Devices**.
Device Serial Number	REG_SZ	Dynamically generated Serial number	The unique serial number of the local hard drive where the tokens are stored. If the tokens are not stored on the local hard drive, then a unique device serial number is generated for the device, but the corresponding Device Serial Number registry entry is not created.

Note: Do not edit these registry entries.

A device serial number uniquely identifies a specific device. Every instance of the installed SecurID desktop application contains a hard drive plug-in that has a unique device serial number. You can use the device serial number to bind a token to a specific device. If the same user installs the application on a different computer, the user cannot import software tokens into the application because the hard drive plug-in on the second computer has a different device serial number from the one to which the user's tokens are bound.

The SecurID desktop application allows you to bind a token to a specific device type, a device serial number, or a Windows user security identifier (user SID). The device type and device serial number are displayed in the Token Information window and the Token Storage Devices window. You can obtain a Windows user SID through a third-party utility.

For more information on device binding, see the *RSA SecurID Software Token 5.0 for Windows Provisioning Guide*.

RSA SecurID 800 Authenticator

To use connected RSA SecurID 800 authenticators with RSA SecurID Software Token 5.0.3 for Windows, you must install RSA Smart Card Middleware 3.6 on desktops and laptops. You can install the Middleware from the RSA Authentication Client 3.6 product kit. To download the kit, go to the **myRSA** website. Follow the installation instructions in the **RSA Authentication Client 3.6 Installation and Administration Guide** on RSA Link.

Operating System Requirements

The following table lists the system requirements for RSA SecurID Software Token 5.0.3 for Windows.

Description	Requirement
Operating system	RSA SecurID Software Token 5.0.3 for Windows supports the following: • Windows 10 32-bit and 64-bit • Windows 8.1 32-bit and 64-bit
Internet Explorer support for Internet Explorer Plug-In	RSA SecurID Software Token 5.0.3 for Windows supports the following: • Internet Explorer 11 on Windows 10 and Windows 8.1 • Internet Explorer 10 on Windows 8.1 **Note:** The Internet Explorer Plug-In does not support the Microsoft Edge browser. On Windows 10, the Internet Explorer Plug-In supports Internet Explorer 11 only.
Disk space	1 KB available space for each software token installed

Supported Provisioning Servers

You can provision software tokens for use with the SecurID desktop application with the following RSA products.

RSA Product	Description
RSA Authentication Manager	RSA Authentication Manager 8.*x*, including RSA Self-Service. With RSA Self-Service, users can request software tokens and manage their SecurID PINs, thereby reducing administrative overhead. For more information, see the *RSA SecurID Software Token 5.0 for Windows Provisioning Guide*.
RSA SecurID Authentication Engine (SAE)	RSA SecurID Authentication Engine 2.8.1 for Java (SAE for Java) SAE is an Application Programming Interface (API) that provides the backend authentication functions of RSA SecurID. You can integrate SAE into your existing infrastructure to authenticate SecurID desktop users. SAE supports exporting software token files (SDTID files). It does not provide out-of-the-box support for dynamic seed provisioning (CT-KIP). For more information, see the **RSA SecurID Authentication Engine documentation page** on RSA Link.

Product Packages

Installation Package

The RSA SecurID Software Token 5.0.3 for Windows installation package, **RSASecurIDToken503.zip**, contains the following files.

Note: The MSI filenames are different in the 32-bit and 64-bit versions of **RSASecurIDToken503.zip**.

File	Description
RSASecurIDToken503.msi (32-bit) or **RSASecurIDToken503x64.msi** (64-bit)	Application installer file for the RSA SecurID Standard desktop application.The 32-bit and 64-bit versions have different filenames. Install this variant if users will authenticate manually to a VPN client or web resource that does not have integrated SecurID functionality. The user is prompted for a username and RSA SecurID passcode (PIN and tokencode).
RSASecurIDTokenAuto503.msi (32-bit) or **RSASecurIDTokenAuto503x64.msi** (64-bit)	Application installer file for the RSA SecurID Software Token with Automation. The 32-bit and 64-bit versions have different filenames. Install this variant if users will authenticate to a VPN client or web resource that has integrated RSA SecurID functionality. The user is prompted only for a username and RSA SecurID PIN.
def\Desktop-Windows-5.x-swtd.xml **def\Desktop-Windows-5.x-Auto-swtd.xml**	Device definition files required for provisioning tokens to the Windows platform with RSA Authentication Manager. You must import the device definition file into Authentication Manager. Use **Desktop-Windows-5.x-swtd.xml** for the RSA SecurID Standard desktop application, or use **Desktop-Windows-5.x-Auto-swtd.xml** for the RSA SecurID Software Token with Automation.
template\RSASecurIDToken.adm	Administrative template for customizing the application using Windows Group Policy. For more information, see the *Administrator's Guide*.

Documentation

For the most recent documentation, see the **RSA SecurID Software Token for Microsoft Windows documentation page** on RSA Link.

Upgrades

RSA SecurID Software Token 5.0.3 for Windows supports upgrading from version 5.0, version 5.0.1, and version 5.0.2. Upgrading overwrites the existing version and copies the existing token database to the 5.0.3 token database.

You can upgrade to the same variant of the application and the same token storage database option. For example, you can upgrade from version 5.0 of the RSA SecurID Software Token with Automation and a per-user database to version 5.0.3 of the RSA SecurID Software Token with Automation and a per-user database.

You can upgrade 5.0, 5.0.1, or 5.0.2 to either the 32-bit or 64-bit version of 5.0.3. For instructions, see the *Administrator's Guide*.

Fixed Issues

SWTDT-2039. After closing the SecurID desktop application on a second monitor and disconnecting the monitor, the SecurID desktop application would not display on the main monitor if the application was restarted. This issue is resolved.

SWTDT-1813. Resolved a version 5.0.2 upgrade issue that overwrote an environment variable.

SWTDT-1732. Resolved an issue in which the SecurID desktop application did not display correctly on devices that use the Windows 10 text scaling feature, such as Microsoft Surface Pro 4 tablets. RSA supports text scaling values of 200% or less.

Known Issues

This section explains issues that remain unresolved in this release and solutions or workarounds.

The registry contains two Device Serial Number entries after upgrading the RSA SecurID desktop application from version 5.0.1 to version 5.0.2

Tracking Number: SWTDT-1763
Problem: After successfully upgrading the RSA SecurID desktop application from version 5.0.1 to version 5.0.2, the Device Serial Number registry entry is located in **HKEY_LOCAL_MACHINE\SOFTWARE\RSA\Software Token\Library\Plugins\DeviceInformation** and **HKEY_CURRENT_USER\SOFTWARE\RSA\Software Token\Desktop\DeviceInformation**.
Workaround: Manually remove the **HKEY_LOCAL_MACHINE\SOFTWARE\RSA\Software Token\Library\Plugins\DeviceInformation** registry key after upgrading.

Uninstalling the SecurID desktop application deletes the user registry and token database only for the user who performs the uninstallation

Tracking Number: SWTDT-1429
Problem: The RSA SecurID desktop application uninstaller program removes the user registry and the token database only for the user who uninstalls the application. For example, on a shared computer, the registry entries and token database are removed for the person who uninstalled the application, but are not removed for other users of the computer.
Workaround: Manually remove the **HKEY_CURRENT_USER\Software\RSA\Software Token** registry key and the database directory for all users of a machine. The database directory location on Windows 7, Windows 8, Windows 10, and Windows Vista is:

```
C:\Users\userid\AppData\Local\RSA\RSA SecurID Software Token Library
```

The countdown display in the SecurID desktop application does not match the countdown display on the connected RSA SecurID 800 authenticator

Tracking Number: SWTDT-986
Problem: The RSA SecurID desktop application has a countdown display that shows the number of seconds remaining before the tokencode changes. When you use a connected SecurID 800 authenticator with the application, the countdown display in the application does not match the countdown display on the front of the SecurID 800. The display on the SecurID 800 is the true countdown time.
Workaround: Even though the remaining time displayed in the application may be different, the user can still authenticate successfully with the SecurID 800.

Removing the Local Hard Drive (RSA) plug-in from the application does not remove the token database

Tracking Number: SWTDT-1358
Problem: If you uninstall the Local Hard Drive (RSA) plug-in (HDDPlugin), but you do not uninstall the entire application, the token database is not removed from the computer.
Workaround: To remove the token database, uninstall the entire application. This removes the token database for the user who performs the uninstallation. On a shared computer, use the workaround described in Tracking Number 1429 to remove the token database for all users of the computer.

Using certain customization policies together is not supported

Tracking Number: SWTDT-1364
Problem: Using the ActivationCode customization policy in conjunction with the OnlyOneToken policy causes issues. RSA does not support using the two policies together.
Workaround: If you want to autoimport a single token, use the ActivationCode policy with the CtkipUrL policy, but do not use the OnlyOneToken policy.

Restarting the SecurID desktop application is required after changing the token storage device password

Tracking Number: SWTDT-1707
Problem: If a user changes a token storage device password, the SecurID desktop application does not prompt the user to enter the new password when importing a token.
Workaround: After changing the device password, restart the SecurID desktop application. The user is prompted to enter the new password.

Support and Service

You can access community and support information on RSA Link at **https://community.rsa.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 at **www.rsaready.com** 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.

July 2021

Intellectual Property Notice

Open Source License