Release Notes
RSA SecurID® Software Token with Automation 4.1.2 for Windows and Mac OS

January 2017

Introduction

RSA SecurID® Software Token with Automation 4.1.2 (the SecurID desktop application) provides strong authentication from Windows and Mac OS desktops and laptops to Virtual Private Networks (VPNs) and other resources protected by RSA SecurID.

This document describes what's new in RSA SecurID Software Token with Automation 4.1.2 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 SecurCare Online at **https://knowledge.rsasecurity.com**.

Release Notes Revision History

Revision 3 (No version update)	January 2017	• RSA has qualified RSA SecurID Software Token with Automation 4.1.2 to run on Mac OS 10.12 Sierra.
Revision 2 (No version update)	August 2016	• RSA has qualified RSA SecurID Software Token with Automation 4.1.2 to run on Mac OS X El Capitan. • Four known issues have been added.
Revision 1 Windows Build 40	June 2014	• RSA has qualified RSA SecurID Software Token with Automation 4.1.2 to run on Windows 8.1 64-bit systems. • One issue has been fixed. Please see SWTDT-1634 in "What's Fixed in This Release" on page 2. • Upgrade functionality for hotfix releases has been implemented. Please see "Upgrades" on page 6. • Two known issues were modified. Please see SWTDT-624 and SWTDT-1580 in "Known Issues on Mac OS Systems" on page 7.

What's New in This Release

RSA SecurID Software Token 4.1.2 with Automation provides support for 64-bit Windows and Mac OS operating systems. (For OS support, see Operating System Requirements on page 2.) This release allows 64-bit VPN applications to integrate with the 64-bit SecurID application. With RSA SecurID integration, VPN client applications can obtain tokencodes automatically so that users can authenticate to their VPN client without having to manually copy and paste tokencodes. The user only needs to enter his or her username and RSA SecurID PIN.

Important: Version 4.1.2 runs only on 64-bit operating systems. Customers with existing deployments on 32-bit operating systems should continue to use Version 4.1.1.

This release provides upgrade functionality for “hotfix” releases, allowing upgrade installation to be performed when a previous installation of RSA SecurID® Software Token for Windows 4.1.2 exists on the system.

What’s Changed in This Release

- The Standard version of the application (without Automation) is not supported.
- The RSA SecurID Trusted Platform Module/Smart Card Plug-In 1.0 is no longer supported.
- The following custom features are no longer supported:
  - VpnMode custom policy. This policy was associated only with Windows XP systems. For information about customizing the SecurID desktop application, see the *Administrator’s Guide*.
  - FirefoxPlugin (web browser plug-in for Firefox). The option is no longer provided either through the command line or in the interactive installation program.
  - STOPVISTABROWSER command line property. This policy was associated only with Windows Vista systems.
- To use connected RSA SecurID 800 authenticators with RSA SecurID Software Token with Automation 4.1.2 (Windows only), 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 **https://knowledge.rsasecurity.com/scolcms/set.aspx?id=9588**. Follow the installation instructions in the *RSA Authentication Client 3.6 Installation and Administration Guide*.

What’s Fixed in This Release

SWTDT-1634 - Changing the system date while the Software Token application was open did not trigger the application to update the One-Time Password for the new date configuration. The application now displays the correct One-Time Password if the system date is changed.

Operating System Requirements

RSA SecurID Software Token with Automation 4.1.2 for Windows requires one of the following:

- Windows 8.1 (64-bit)
- Windows 2008 Server (64-bit)
- Windows 2008 Server R2 (64-bit)
- Windows 7 (64-bit)

RSA SecurID Software Token with Automation 4.1.2 for Mac OS requires one of the following:

- Mac OS Sierra (version 10.12, 64-bit)
- Mac OS X El Capitan (version 10.11, 64-bit)

- Mac OS X Mountain Lion (version 10.8, 64-bit)
- Mac OS X Lion (version 10.7, 64-bit)

Supported Provisioning Servers

You can provision software tokens for use with RSA SecurID Software Token with Automation 4.1.2 using:

- 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 document *Provisioning RSA SecurID Software Tokens with RSA Authentication Manager 8.x*.
- RSA Authentication Manager 7.1, including RSA Credential Manager, the self-service and provisioning component. With RSA Credential Manager, users can request software tokens and manage their SecurID PINs, thereby reducing administrative overhead.
- RSA SecurID Appliance 3.0
- RSA Authentication Manager 6.1
- RSA SecurID Authentication Engine 2.8.1 for Java (SAE for Java)
- RSA SecurID Authentication Engine 2.3 for C (SAE for C)

  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 go to **http://www.emc.com/security/rsa-securid/rsa-securid-authentication-engine.htm**.

Windows Product Packages

Windows Installation Package

The RSA SecurID Software Token with Automation 4.1.2 for Windows installation package, **RSASecurIDToken412.zip**, contains the following files.

File	Description
RSASecurIDTokenAuto412x64.msi	Application installer file
def\Desktop-Windows-4.x-Auto-swtd.xml	Device definition file required for provisioning tokens to the Windows platform with RSA Authentication Manager 7.1. For first-time installations of the SecurID desktop application, you must import the device definition file into Authentication Manager. For upgrades, use the device definition file you imported previously. **Note:** If you are using RSA Authentication Manager 8.x, you do not need to import the device definition file. Authentication Manager 8.x contains the device definition files for the SecurID desktop application.
template\RSASecurIDToken.adm	Administrative template for customizing the application using Windows Group Policy. For more information, see the *Administrator's Guide*.

Windows Documentation Package

The RSA SecurID Software Token with Automation 4.1.2 for Windows documentation package, **RSASecurIDTokenDocs412.zip**, contains the following files.

File	Description
SecurIDToken412_admin.pdf	Administrator's Guide
SecurIDToken412_quickstart.pdf	*Quick Start* guide for end users
SecurIDToken412_release_notes.pdf	These *Release Notes*
SoftwareTokenProvisioningAM8_admin.pdf	*Administrator's Guide* for provisioning software tokens with RSA Authentication Manager 8.x

Windows Token Library SDK and Utility Packages

The following token library SDK and utility packages are available for the Windows implementation.

File	Description
RSASecurIDSDK412.zip	Token Library SDK for Windows. Allows developers to use the Software Token Automation APIs to integrate the RSA SecurID Software Token 64-bit framework into their applications. To download the SDK, go to **https://knowledge.rsasecurity.com/scolcms/set.aspx?id=8554**.
RSASecurIDUtils412.zip	RSA SecurID Token Import utility (Token Importer). Command line utility for importing software tokens into token storage devices supported by the SecurID desktop application. You can import tokens from token files (SDTID files) or from a CT-KIP server URL without interacting with the desktop application's user interface (unless importing to a password-protected device). To download this package and associated documentation, go to **http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators/ms-windows.htm**. **Note:** No changes were made to the Token Importer for this release. If you have used version 4.1.1 of the Token Importer, you can continue to use it with version 4.1.2 of the SecurID desktop application.

Mac OS Product Packages

Mac OS Installation Package

The RSA SecurID Software Token with Automation 4.1.2 for Mac OS installation package, **RSASecurIDMac412.dmg**, contains the following files.

File	Description
RSASecurIDTokenAutoMac412x64.pkg	Application installer file.

File	Description
def\Desktop-Mac-4.x-Auto-swtd.xml	Device definition file required for provisioning tokens to the Mac OS platform with RSA Authentication Manager 7.1. For first-time installations of the SecurID desktop application, you must import the device definition file into Authentication Manager. For upgrades, use the device definition file you imported previously. **Note:** If you are using RSA Authentication Manager 8.x, you do not need to import the device definition file. Authentication Manager 8.x contains the device definition files for the SecurID desktop application.
template\com.rsa.SoftwareToken.Policies.plist	Administrative template file for customizing the application using a plist file. For more information, see the *Administrator's Guide*.

Mac OS Documentation Package

The RSA SecurID Software Token with Automation 4.1.2 for Mac OS documentation package, **RSASecurIDMacDocs412.dmg**, contains the following files.

File	Description
SecurIDToken412_admin.pdf	Administrator's Guide
SecurIDToken412_quickstart.pdf	*Quick Start* guide for end users
SecurIDToken412_release_notes.pdf	These *Release Notes*
SoftwareTokenProvisioningAM8_admin.pdf	*Administrator's Guide* for provisioning software tokens with RSA Authentication Manager 8.x

Mac OS Token Library SDK and Utility Packages

The following token library SDK and utility packages are available for the Mac OS implementation.

File	Description
RSASecurIDMacSDK412.dmg	Token Library SDK for Mac OS. Allows developers to use the Software Token Automation APIs to integrate the RSA SecurID Software Token 64-bit framework into their applications. To download the SDK, go to **https://knowledge.rsasecurity.com/scolcms/set.aspx?id=8555**.
RSASecurIDMacUtils412.dmg	RSA SecurID Token Import utility (Token Importer). Command line utility for importing software tokens into token storage devices supported by the SecurID desktop application. You can import tokens from token files (SDTID files) or from a CT-KIP server URL without interacting with the desktop application's user interface (unless importing to a password-protected device). To download this package and associated documentation, go to **http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators/mac-os.htm**. **Note:** No changes were made to the Token Importer for this release. If you have used version 4.1.1 of the Token Importer, you can continue to use it with version 4.1.2 of the SecurID desktop application.

Upgrades

RSA SecurID Software Token with Automation 4.1.2 for Windows supports upgrading from versions 4.1 and 4.1.1 with Software Token Automation only.

RSA SecurID Software Token with Automation 4.1.2 for Mac OS supports upgrading from version 4.1.1 with Software Token Automation. Upgrades are not supported from Mac OS X Mountain Lion.

To upgrade, run the version 4.1.2 installation program for your platform. Version 4.1.2 overwrites the previous version and copies the token database from the previous version to the version 4.1.2 token database.

Hotfixes for Windows

Hotfix releases for Windows, from version 4.1.2 Build 40 onward, can be installed as upgrades if a previous installation of version 4.1.2 already exists on the machine.

To install a Windows hotfix as an upgrade, navigate to the directory containing the hotfix installation package, and issue the following command from the command line:

```
msiexec /i <installer filename.msi> REINSTALL=ALL REINSTALLMODE=vamus
REBOOT=ReallySuppress
```

where `<installer filename.msi>` is the name of the hotfix installation package.

Note: After installing a hotfix upgrade using the method above, do not attempt to repair the installation using the Repair feature from the Programs and Features menu in the Windows Control Panel. To repair an installation, use the Change feature instead.

Hotfixes for Mac

To install a Mac hotfix as an upgrade, simply run the installation package.

Known Issues on Windows and Mac OS Systems

This section explains issues that remain unresolved in both the Windows and Mac OS versions of this release and solutions or workarounds.

Import token from URL fails when using Dynamic Seed Provisioning (CT-KIP) as the delivery method and device serial number as the activation code

Tracking Number: SWTDT-1727
Problem: When the software token delivery method is set to Dynamic Seed Provisioning (CT-KIP) in RSA Authentication Manager, and the device serial number is used as the activation code, importing tokens from URL fails if the device serial number contains more than 25 characters. The activation code field automatically truncates input to 25 characters.

Workaround: Import the token using SecurID Token Import Utility 5.0, which enables you to specify device serial numbers longer than 25 characters on the command line.

Application displays token nickname incorrectly for token files issued with non-ASCII characters

Tracking Number: SWTDT-1328
Problem: If you issue a token file and assign a nickname (token name) containing non-ASCII characters (for example, ISO-Latin or Asian characters) using RSA Authentication Manager 6.1, the token name is not displayed properly in the RSA SecurID desktop application, although the token still works properly. Tokens issued using RSA Authentication Manager 6.1 and imported into version 4.0 of the application may display the token name incorrectly in version 4.1.x if they are re-imported. However, tokens that are transferred from version 4.0 to version 4.1.x display the token name correctly. If you issue tokens using RSA Authentication Manager 7.1, and you need to use non-ASCII characters, you must configure Authentication Manager to use the UTF-8 character set. Otherwise, the token might not be imported, or the application will not display the token name correctly.

Workaround: Use one of the following workarounds:

- **RSA Authentication Manager 6.1.** Use only ASCII characters when issuing the token file, or instruct the user to rename the token in the application.
- **RSA Authentication Manager 7.1.** Configure Authentication Manager to use the UTF-8 character set. For instructions, contact RSA Customer Support.

Known Issues on Mac OS Systems

This section explains issues that remain unresolved in the Mac OS version of this release and solutions or workarounds.

Logging feature does not work on Mac OS X 10.8 or later

Tracking Number: SWTDT-1616
Problem: On Mac OS X 10.8 or later, the RSA SecurID Software Token logging feature does not work. The application logs only the error message “Software token library -47 General Error”. Attempts to modify the default logging level do not succeed.

Workaround: None.

On some Mac OS X 10.11 hosts, RSA SecurID Software Token application stops responding when the host is idle for extended periods

Tracking Number: SWTDT-1726
Problem: On some Mac OS X 10.11 hosts, when the host is idle for extended periods of time (usually three to four hours), the RSA SecurID Software Token application stops responding.

Workaround: Use Force Quit to close RSA SecurID Software Token, then restart the application.

Import token from URL fails on Mac OS X 10.10 when TLS 1.2 Mode and Dynamic Seed Provisioning (CT-KIP) are enabled in RSA Authentication Manager

Tracking Number: SWTDT-1724
Problem: On Mac OS X 10.10, when TLS1.2 Mode is enabled and the software token delivery method is set to Dynamic Seed Provisioning (CT-KIP) in RSA Authentication Manager, importing tokens from URL using RSA SecurID Software Token fails, displaying an error message.

Workaround: If TLS 1.2 Mode must remain enabled, use SDTID or CTF provisioning for Mac Desktop Token.

Known Issues on Windows Systems

This section explains issues that remain unresolved in the Windows version of this release and solutions or workarounds.

Internet Explorer plug-in does not work on Windows 8.1 64-bit systems running Internet Explorer 11

Tracking Number: SWTDT-1635
Problem: The Internet Explorer plug-in does not work on Windows 8.1 64-bit systems running Internet Explorer 11.
Workaround: You can use the Internet Explorer plug-in on Windows 8.1 32-bit with RSA SecurID Software Token 4.1.1. RSA intends to resolve this issue in a future release of RSA SecurID Software Token for Windows.

The Help file for the application does not work on Windows systems running Internet Explorer 11

Tracking Number: SWTDT-1608
Problem: You cannot access the application’s Help file on systems running Internet Explorer 11.
Workaround: Instruct users to use the Firefox browser to view the Help.

Web plugin does not work correctly when Internet Explorer security zone level is set to High

Tracking Number: SWTDT-1580
Problem: If Internet Explorer's security zone level is set to **High**, ActiveX controls cannot be executed, which prevents the RSA SecurID Software Token web plugin from working properly.
Workaround: Ensure that Internet Explorer's security zone level is set to **Medium-high** or lower, or configure a custom security level to permit ActiveX controls.

To set Internet Explorer's security zone level to Medium-high:

1. Open Internet Explorer.
2. Click the **Tools** menu, and then click **Internet Options**.
3. On the **Security** tab, select the security zone you want to modify.
4. Move the **Security level for this zone** slider to **Medium-high**, or a lower security level of your choice.
5. Click **Apply**.
6. Click **OK** to close the window.

To configure a custom security level to permit ActiveX controls:

1. Open Internet Explorer.
2. Click the **Tools** menu, and then click **Internet Options**.
3. On the **Security** tab, click the **Custom level** button.
4. Scroll down the **Security Settings** list until you see **ActiveX controls and plug-ins**.
5. Scroll down to **Run ActiveX controls and plug-ins** and click **Enable**.
6. Scroll down to **Script ActiveX controls marked safe for scripting** and click **Enable**.
7. Click **OK**, then click **OK** again.

Path to token database is not set correctly in the Windows registry if the SecurID desktop application is installed as SYSTEM

Tracking Number: SWTDT-1509
Problem: If you install RSA SecurID Software Token 4.1.2 for Windows as SYSTEM, for example, by silently installing the application using Microsoft Systems Management Server (SMS), the DatabasePath registry entry may be created incorrectly. When the user launches the application, the Import Token screen is displayed because the application cannot find the token database.
Workaround: If you install the application as SYSTEM, using SMS or another third-party installer, always set the database directory using the SETDATABASEDIR command line property. For example, on a Windows 7 system, use a command similar to the following, where *pathname* is the path to the directory that contains the MSI file:

```
msiexec /qn /i pathname\RSASecurIDToken412.msi /lv c:\install.log
SETDATABASEDIR="~/Local Settings/Application Data/RSA/RSA SecurID Software Token
Library"
```

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 and Windows Server 2008 is:

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

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.

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.

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.

The installation program adds the language setting required by the web browser plug-in for Internet Explorer only for the local user who installs the application, and the language setting is not automatically moved to the top of the Languages list in Internet Options

Tracking Number: SWTDT-624
Problem: When you install the web browser plug-in for Internet Explorer with the RSA SecurID desktop application, the **en-securid** language setting, which allows the browser to recognize web pages protected by RSA SecurID, is added only for the local user who installs the application, and is not automatically moved to the top of the Languages list in Internet Options. To enable proper browser plug-in functionality, the language setting must be configured manually.
Workaround: Provide users with instructions for configuring the language setting. Users who uninstall the application should verify that the **en-securid** setting has been removed and if it has not, they should manually remove it in order to restore the browser's original language settings.

To add the en-securid language setting:

1. Open Internet Explorer.
2. Click **Tools > Internet Options**.
3. On the **General** tab, click **Languages**, and then click **Add**.
4. In the **User Defined** field, type **en-securid**.
5. Click **Move up** to move the **User-defined [en-securid]** setting to the top of the list.
6. Click **OK** to exit from each dialog box.

To move the en-securid language setting to the top of the Languages list:

1. Open Internet Explorer.
2. Click **Tools > Internet Options**.
3. On the **General** tab, click **Languages**.
4. Select **User-defined [en-securid]** from the Language list, and click **Move up** to move it to the top of the list.
5. Click **OK** to exit from each dialog box.

To remove the en-securid language setting:

1. Open Internet Explorer.
2. Click **Tools > Internet Options**.
3. On the **General** tab, click **Languages.**
4. In the **Language** section, select **User-defined [en-securid]**, and select **Remove**.
5. Click **OK** to exit from each dialog box.

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.

Copyright © 2009-2017 EMC Corporation. All Rights Reserved. Published in the USA.

Trademarks

RSA, the RSA Logo, SecurID, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to **www.emc.com/legal/emc-corporation-trademarks.htm#rsa**.

Intellectual Property Notice

This software contains the intellectual property of EMC Corporation or is licensed to EMC Corporation from third parties. Use of this software and the intellectual property contained therein is expressly limited to the terms and conditions of the License Agreement under which it is provided by or on behalf of EMC.

Open Source License

This product may be distributed with open source code, licensed to you in accordance with the applicable open source license. If you would like a copy of any such source code, EMC will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. EMC may charge reasonable shipping and handling charges for such distribution. Please direct requests in writing to EMC Legal, 176 South St., Hopkinton, MA 01748, ATTN: Open Source Program Office.