Release Notes
RSA SecurID Software Token 4.1

November 13, 2009

Introduction

RSA SecurID Software Token 4.1 (the SecurID desktop application) allows users to import software-based security tokens that they can use to verify their identity to Virtual Private Networks (VPNs) and other resources protected by RSA SecurID.

This document lists what's new and changed in RSA SecurID Software Token 4.1. It includes workarounds for known issues. Read this document before installing the software. 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**.

What's New in This Release

This section describes the major changes introduced in this release. For detailed information on each change, see the *Administrator's Guide*.

Additional operating system support. This release supports the following operating systems:

- Windows 7 Enterprise 32-bit and 64-bit
- Windows 7 Professional 32-bit and 64-bit
- Windows Vista Business SP1 and SP2 32-bit and 64-bit
- Windows Vista Enterprise SP1 and SP2 32-bit and 64-bit
- Windows XP Professional SP3
- Mac OS X 10.5.x and 10.6.x

SecurID integration with additional VPN client applications. This release adds support for SecurID integration with Juniper Networks Odyssey Access Client, Juniper Networks Secure Access SSL, and Check Point VPN-1 SecureClient. SecurID integration allows VPN clients to automatically retrieve the current tokencode.

Support for additional logon methods with VPN client applications. This release supports logging on to supported VPN clients before logging on to Windows (known as "prelogon" or "start before logon") and running supported VPN clients as a service. The following VPN clients support SecurID authentication for prelogon, running as a service, or logging on to the VPN client after logging on to Windows:

- Juniper Odyssey
- Check Point VPN-1
- Cisco VPN Client
- Nortel VPN Client

Device binding enhancements. This release of the Windows version of the application supports binding a software token to a Windows user security identifier (user SID). This allows the user to import a token to a supported token storage device on any computer in the domain. No interaction with the SecurID desktop application is required to obtain the binding information.

Support for customization policies with the Mac OS X implementation. With this release, you can set customization policies to change default behaviors of the Max OS X version of the SecurID desktop application. For details, see the appendix "Customizing the Application" in the *Administrator's Guide*.

Additional customization policies. This release supports additional customization policies, which allow you to change the default application behavior. For example, you can set a policy to prevent users from changing the nickname assigned to their token. For a complete description of customization policies, see the appendix “Customizing the Application” in the *Administrator’s Guide*.

Additional web browser plug-in support. This release of the Windows version of the application supports an optional web browser plug-in for Mozilla Firefox. The web browser plug-in, with the RSA Authentication Agent for Web, allows users to authenticate to web pages protected by SecurID without manually entering a tokencode.

New logging support. This release provides a logger that is configured to output a rolling file. You can control the amount of information that is logged by setting a registry key (Windows) or creating a plist (Mac OS X). For example, you can choose to log messages that are useful for debugging or log only application errors. For more information, see the appendix “Logging” in the *Administrator’s Guide*.

Improved support for screen readers. In this release, screen readers do not read the PIN out loud as the user types it. Users can tab through all of the screens, and the screen readers can read all of the text on the screen.

Token provisioning enhancements. This release provides enhancements that simplify token provisioning. For example, on Windows, you can set a custom policy specifying that the user SID should be used as the CT-KIP activation code. This allows the user to automatically import a token or automatically replace a token using Dynamic Seed Provisioning. Another policy, supported on Windows and Mac OS X, causes the application to display a URL link when a user’s token is about to expire or has expired. The link redirects the user to a web portal (for example, the URL of the RSA Credential Manager) where the user can request a replacement token. For more information, see the chapter “Customizing the Application” in the *Administrator’s Guide*.

New installation options. On Windows and Mac OS X, you can now install the database containing the user’s software tokens (token database) to a location other than the default directory. The Windows version provides additional options. For example, you can set a single database for those cases where you need to support pre-logon authentication (logging on to a VPN client application before logging on to Windows). Additional command line properties are described in the chapter “Installing the Application” in the *Administrator’s Guide*.

Support for RSA SecurID 800 authenticator with RSA Smart Card Middleware. This release integrates the RSA Hardware Authenticator Plug-In 4.1, which allows separately installed RSA Smart Card Middleware and the SecurID desktop application to communicate with a connected SecurID 800. For more information, see the section “Using an RSA SecurID 800 Authenticator with the Application (Windows Only)” in the *Administrator’s Guide*.

Resolution of issues with RSA SecurID 800 authenticator. This release resolves issues related to the use of a connected SecurID 800 with the SecurID desktop application. (BZ69224, BZ110757, BZ116692, BZ121937, BZ121939, BZ122558)

Options for RSA Secured Partners

This release provides the following new options for RSA Secured Partners. To obtain the associated software developer’s kits and documentation, contact RSA Partner Engineering.

Custom time source support. This release provides RSA Time Provider Interface 1.0, a software developer’s kit that specifies the interface that must be implemented to provide a custom time source for use within token provider plug-ins when they are generating tokencodes. This interface is intended for organizations in which users’ system times may be out of sync with the RSA Authentication Manager server, which would result in authentication failures.

USB device support. This release provides a distribution kit (**RSA SecurIDUSBSDK410.zip)** that contains a version of the SecurID desktop application that can be run from a USB device. For the application to import tokens or generate tokencodes, you must create a token storage plug-in. Use the **RSASecurIDPluginSDK410.zip** distribution kit to obtain sample plug-in code and documentation describing how to create a token storage plug-in. Once you have developed the token storage plug-in, install it on the USB device along with the files from the **RSASecurIDUSBSDK410** distribution kit.

Release Packages

This section describes the release packages for the Microsoft Windows and Mac OS X versions of the SecurID desktop application. For more information, see the *Administrator's Guide*.

Windows Installation Package

The RSA SecurID Software Token 4.1 for Windows Desktops installation kit, **RSASecurIDToken410.zip**, contains the following files:

- An installation package, **RSASecurIDToken410.msi**.
- Documentation, as described in "Product Documentation" on page 4.
- A device definition file, **Desktop-Windows-4.x-swtd.xml**. This file is used with RSA Authentication Manager 7.1 and specifies the capabilities and attributes of software tokens used with the desktop application for Windows.
- An administrative template, **RSASecurIDToken.adm**, for use in customizing the application with Windows Group Policy.

This release also provides the following additional items for Windows implementations:

- A utilities package, **RSASecurIDUtils410.zip**, containing the RSA SecurID Token Import utility, a command line executable that allows users or system administrators to install tokens without interacting with the application user interface. You can download this package and associated documentation from **https://www.rsa.com/node.aspx?id=1162**.
- A developer's kit, **RSASecurIDSDK410.zip**, containing the components and documentation needed to integrate with the RSA SecurID Token framework. VPN application developers can use the RSA SecurID Token framework to obtain tokencodes directly, so that users can authenticate to their VPN client without having to manually copy and paste tokencodes. You can obtain the developer's kit from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

Mac OS X Installation Package

The RSA SecurID Software Token 4.1 for Mac OS X installation package, **RSASecurIDToken410.dmg**, contains the following files:

- An installer file, **RSASecurIDSoftwareToken410.mpkg**.
- Documentation, as described in "Product Documentation" on page 4.
- A device definition file, **def/Desktop-Mac-4.x-swtd.xml**, that specifies the capabilities and attributes of software tokens used with the desktop application for Mac OS X.

This release also provides the following additional items for Mac OS X implementations:

- A utilities package, **RSASecurIDMacUtils410.dmg**, containing the RSA SecurID Token Import utility, a command line executable that allows users or system administrators to install tokens without interacting with the application user interface. You can download this package and associated documentation from **http://www.rsa.com/swtokenmac**.
- A developer's kit, **RSASecurIDMacSDK410.dmg**, containing the components and documentation needed to integrate with the RSA SecurID Token framework. VPN application developers can use the RSA SecurID Token framework to obtain tokencodes directly, so that users can authenticate to their VPN client without having to manually copy and paste tokencodes. You can obtain the developer's kit from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

Product Documentation

The following documentation is provided with the product kit.

Title	Filename
Administrator's Guide	**SecurIDToken_admin.pdf**
Quick Start	**SecurIDToken_quickstart.pdf**
Help (accessible from the application)	
Release Notes (this document)	**SecurIDToken_release_notes.pdf**

Machine Requirements

The Windows version of the application can be run on virtualization software. However, it is possible for the time to be incorrect in the virtual image and cause the tokencodes to be incorrect. For this reason, RSA does not recommend running the Windows version of the application on virtualization software.

The Mac version of the application must be installed on a physical machine running a supported version of Mac OS X.

Known Issues

This section explains issues that remain unresolved in this release. Wherever a workaround or fix is available, it has been noted or referenced in detail.

Issues Affecting the Application on Windows and Mac OS X

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

Tracking Number: TOK-2616
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 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 if they are re-imported. However, tokens that are transferred from version 4.0 to version 4.1 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.

Issues Affecting the Application on Windows Only

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

Tracking Number: 100327
Problem: When you install the web browser plug-in for Internet Explorer with the 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. To enable the browser plug-in for other users, the language setting must be added manually.
Workaround: Provide users with instructions for adding the language setting. Users who uninstall the product 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 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.

Uninstalling SecurID desktop application affects operation of a third-party device plug-in

Tracking Number: 101245
Problem: If the SecurID desktop application and a third-party plug-in containing RSA SecurID software tokens are installed on the same computer, uninstalling the application deletes certain library files that are required for using tokens stored on the device plug-in.
Workaround: After uninstalling the SecurID desktop application, remove and then reinstall the device plug-in. You can then continue to use tokens stored in the device plug-in's token database.

UPEK Protector Suite QL must be installed before SecurID desktop application

Tracking Number: 101980
Problem: If you use UPEK Protector Suite QL 5.8 with the SecurID desktop application, the order in which you install the applications could affect integration with VPN software.
Workaround: To ensure that VPN automation works as intended with Protector Suite QL, install Protector Suite QL before installing the SecurID desktop application. Do not uninstall the SecurID desktop application unless you also uninstall Protector Suite QL.

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

Tracking Number: 103818
Problem: The SecurID desktop application uninstaller program removes the user registry and the token database only for the user who uninstalls the product. For example, on a shared computer, the registry entries and token database are removed for the person who uninstalled the product, 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 is as follows:

On Windows XP:

C:\Documents and Settings\userid\Local Settings\Application Data\RSA\RSA SecurID Software Token Library

On Windows 7 and Windows Vista:

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

You may need to restart the computer if you are using an integrated VPN client configured for prelogon authentication or running as a service

Tracking Number: 125040
Problem: Installing the SecurID desktop application updates the system PATH environment variable. Some VPN client applications that are integrated with RSA SecurID may be configured such that they are not able to recognize the updated system PATH. For example, if the Nortel VPN Client is configured to allow prelogon authentication (logging on to the VPN client application prior to Windows logon) or is running as a service, the Nortel VPN Client will not work correctly, and you will receive an error message indicating that the software token application failed to load. This issue does not occur with VPN clients that are not integrated with RSA SecurID.
Workaround: Restart the computer. This allows the integrated VPN client to recognize the updated system PATH variable and to operate correctly when configured for prelogon or running as a service.

Cannot log on to Check Point VPN-1 SecureClient if a device password is set on the Local Hard Drive (RSA) device

Tracking Number: 127524
Problem: If you set a device password on the default Local Hard Drive (RSA) device, when you attempt to connect to the Check Point VPN-1 SecureClient, the connection fails, and the VPN client application does not open.
Workaround: If you plan to use the Check Point VPN client with the SecurID desktop application, do not set a device password on the Local Hard Drive (RSA) device.

During prelogon authentication to the Check Point VPN-1 Secure Client, you are not prompted to authenticate with a fingerprint if you are using a UPEK device

Tracking Number: 127573
Problem: Prelogon authentication (logging on to the VPN client application prior to Windows logon) to Check Point VPN-1 Secure Client does not work properly on systems using a UPEK device. After you enter your PIN and click **Connect**, the Swipe finger dialog box, which prompts you to authenticate with a fingerprint, does not open.
Workaround: After you enter your PIN and click **Connect**, wait 5 to 10 seconds and then swipe your finger to complete your authentication.

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

Tracking Number: 128493
Problem: The 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 SecurID desktop 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 should still be able to authenticate successfully with the SecurID 800.

The SecurID desktop application and the Check Point VPN-1 SecureClient incorrectly display the serial number of a connected RSA SecurID 800 authenticator

Tracking Number: 128426
Problem: The SecurID desktop application displays only the last eight digits of the SecurID 800 serial number and prepends the letter “x.” For example, if the serial number is 00012345678, the application displays it as x12345678. The Check Point VPN client displays the serial number as -0.
Workaround: No workaround is required. You can still authenticate successfully with the connected SecurID 800. If you need to know the correct serial number, you can obtain it from the back of the authenticator.

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

Tracking Number: 128971
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 103818 to remove the token database for all users of the computer.

Using certain customization policies together is not supported

Tracking Number: 129268
Problem: Using the ActivationCode customization policy in conjunction with the OnlyOneToken policy is known to cause 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.

User must transfer tokens manually from version 4.0 to version 4.1 in one scenario

Tracking Number: TOK-2610
Problem: Tokens used with version 4.0 of the SecurID desktop application are automatically transferred to the version 4.1 token database the first time that you run the version 4.1 application. However, if you start the Token Transfer utility before running the newly installed application (for example, instead of selecting the application from the Start menu, you select the Token Transfer utility), and you then cancel the utility, your tokens are not transferred.
Workaround: To transfer your tokens, reopen the Token Transfer utility, and click **OK**.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Workarounds Directory	**www.rsasecured.com**

Trademarks