RSA SecurID® Software Token 5.0.2 for Windows Administrator's Guide

Revision 2

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, the RSA Logo 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 RSA trademarks, go to **www.emc.com/legal/emc-corporation-trademarks.htm#rsa**.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

EMC 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." EMC CORPORATION 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 2015
Revised: March 2017

Contents

Revision History 5

Preface 7
- About This Guide 7
- RSA SecurID Software Token 5.0.2 for Windows Documentation 7
- Related Documentation 7
- Support and Service 8
  - Before You Call Customer Support 8

Chapter 1: Overview and Requirements 9
- About RSA SecurID Software Token 5.0.2 for Windows 9
- Standard Desktop Application 9
- RSA SecurID Software Token with Automation 10
- Internet Explorer Plug-In 10
- Connected RSA SecurID 800 Authenticator 11
- Customization Policies 12
- Secure Sites 13
- System Requirements 13
- Token Storage Devices 14
- Support for Visually Impaired Users 14
- Virtual Machines 14
- Clock Settings 15

Chapter 2: Installing the Application 17
- Before You Begin 17
- Token Storage Database Options for VPN Client Applications 18
- Token Database Copy Protection 19
- Installing RSA SecurID Software Token for Windows 19
  - Enterprise-Wide Installations 20
  - Windows Installation Package 20
  - Install the Application Using the InstallShield Program 21
  - Command Line Installation 22
  - Command Line Examples 26
  - Modify an Installation 28
  - Repair an Installation 31
- Upgrading RSA SecurID Software Token for Windows 32
  - Upgrade Procedures 32
- Uninstalling RSA SecurID Software Token for Windows 33
  - Uninstall the Application Using the Program List 33
  - Uninstall the Application Using the Command Line 33

Chapter 3: User Options for Managing Tokens and Devices 35
Importing Tokens 35
Import a Token Automatically Using CT-KIP 36
Import a Token from the Web Using the Desktop Application 36
Import a Token from an Email Attachment 37
Import a Token Automatically from a Default Directory 38
Import a Token from a Non-Default Directory 39
Change a Token Name 40
Select a Token 40
Device Passwords 41
Set a Device Password 41
Change a Device Password 42
Remove a Device Password 42
Reset the Device (Local Hard Drive) 43
Device Passwords for Third-Party Plug-Ins 44
View Token Information 45
View Token Storage Device Information 46
Delete a Token 47
Obtaining the Next Code 48
Enter the Next Code 48
Disable Next Code Mode 48

Chapter 4: Troubleshooting 49

Appendix A: Customizing the Application 51
Customization Policies 51
Policies for RSA SecurID Software Token for Windows 51
Policy Details 52
ActivationCode 52
CtkipUrl 53
DisableDeleteToken 53
DisableSetDevicePassword 54
OnlyOneToken 54
TokenExpirationNotification 54
TokenRenewalURL 54
ValidDevices 54
Customizing RSA SecurID Software Token for Windows 56
Add the RSA Administrative Template 56
Configure Group Policy Settings 56
Updating the Token Storage Device Serial Number 57

Appendix B: Logging 59
Setting the Logging Level 59
Location of Log Output Files 59
Log Message Format 60
Sample Log Messages 61

Revision History

Revision Number	Date	Revision
1	January 2017	Updated for RSA SecurID Software Token 5.0.1 for Windows: • Removed the "What's New in This Release" and "What's Changed in this Release" sections. The *Release Notes* contain information on the updates and changes in version 5.0.1. • Updated Chapter 2, "Installing the Application" with the new filenames and upgrade instructions. RSA SecurID Software Token 5.0.1 supports upgrading from version 5.0. • Added Windows 10 support to the "System Requirements" section. • Added descriptions of the Device Name and Device Serial Number registry entries to Appendix A, "Customizing the Application."
2	March 2017	Updated for RSA SecurID Software Token 5.0.2 for Windows: • Updated Chapter 2, "Installing the Application" with the new filenames and upgrade instructions. RSA SecurID Software Token 5.0.2 supports upgrading from version 5.0 and version 5.0.1. • Added statements that the command line installation must be run as an administrator. • Updated the location for the Device Name and Device Serial Number registry entries in Appendix A, "Customizing the Application."

Preface

About This Guide

This guide describes how to prepare for and deploy RSA SecurID® Software Token 5.0.2 for Windows (the SecurID desktop application). This guide is intended for RSA Authentication Manager administrators and other personnel who are responsible for deploying and administering the SecurID desktop application. It assumes that these personnel have experience using RSA Authentication Manager. Do not make this guide available to the general user population.

RSA SecurID Software Token 5.0.2 for Windows Documentation

For more information about the SecurID desktop application, see the following documentation:

Administrator's Guide. (This guide.) Provides information for security administrators on deploying and managing the SecurID desktop application.

Provisioning Guide. Describes the tasks required to configure and distribute software tokens using RSA Authentication Manager 8.*x*. Also covers user Self-Service options.

Release Notes. Provides information about what is new and changed in this release and workarounds for known issues. The latest version of the *Release Notes* is available on RSA Link at **https://community.rsa.com**.

RSA SecurID Software Token Help. Explains how to import tokens, set an RSA SecurID PIN, authenticate with SecurID, and manage tokens. You access Help topics from the SecurID desktop application.

Related Documentation

For more information related to the SecurID desktop application or software tokens, see the following:

RSA Authentication Manager 8.x Administrator's Guide. Provides an overview of Authentication Manager and its features. Describes how to configure the system and perform a wide range of administration tasks.

RSA Authentication Manager Help. Instructions for performing daily administration tasks in the Security Console and configuration and setup tasks in the Operations Console (RSA Authentication Manager user interfaces). Includes instructions for the most common tasks for Help Desk Administrators. To view Help, click the **Help** tab in the Security Console or the Operations Console.

RSA SecurID Authentication Engine 2.8.1 for Java Developer's Guide. Provides a detailed description of the Authentication Engine API for Java.

RSA SecurID Software Token Security Best Practices Guide. Identifies best practices designed to ensure secure operation of RSA SecurID software token applications. To download this guide from RSA Link, go to: **https://community.rsa.com/docs/DOC-35128**.

RSA SecurID Software Token Deployment Planning Guide. Provides information on planning an enterprise-wide software token deployment, including transitioning from hardware tokens to software tokens, and examples of software token provisioning and delivery on desktop and mobile platforms. To download the *RSA SecurID Software Token Deployment Planning Guide*, go to **https://community.rsa.com/docs/DOC-35127**.

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.

Before You Call Customer Support

Make sure that you have direct access to the computer running the RSA SecurID Software Token 5.0.2 for Windows software.

Please have the following information available when you call:

- ❑ Your RSA Customer/License ID.
- ❑ RSA SecurID Software Token software version number.
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system under which the problem occurs.

1 Overview and Requirements

This chapter introduces RSA SecurID Software Token 5.0.2 for Windows (the SecurID desktop application) and provides system requirements and other general information.

About RSA SecurID Software Token 5.0.2 for Windows

RSA SecurID Software Token 5.0.2 for Windows is authentication software that runs on 32-bit and 64-bit Windows operating systems and allows users to verify their identity to resources protected by RSA SecurID. The application must be installed on desktops and laptops, along with separately installed software-based security tokens. SecurID software tokens generate one-time passwords (OTPs) at regular intervals. With the SecurID desktop application, users can enter the current OTP, along with other security information, to gain access to Virtual Private Networks (VPNs) and web applications. The software provides strong two-factor authentication and eliminates the need for the user to carry a separate hardware token.

Standard Desktop Application

The RSA SecurID Standard desktop application provides an installation package for customers who do not require the software token automation API features of the product. This package does not contain the dynamically linked STAUTO32 API (**stauto32.dll**). This security enhancement is intended to help prevent potential misuse of the API.

Install the Standard desktop application if users will authenticate manually to a VPN client or web resource that does not have integrated SecurID functionality. As shown in the following figure, the user is prompted for a username and RSA SecurID passcode (PIN and tokencode).

RSA SecurID Software Token with Automation

The RSA SecurID Software Token with Automation provides an installation package to support backwards compatibility for using the software token automation API. The software token automation API enables integration with leading VPN and remote access applications so that users are only required to enter a user name and RSA SecurID PIN for authentication.

Install the RSA SecurID Software Token with Automation if users will authenticate to a VPN client or web resource that has integrated RSA SecurID functionality. As shown in the following figure, the user is prompted only for a username and RSA SecurID PIN.

Internet Explorer Plug-In

RSA SecurID Software Token 5.0.2 for Windows provides an optional Internet Explorer plug-in that allows users to authenticate to selected web pages without manually entering a one-time password (OTP). The Internet Explorer plug-in is a custom feature of the desktop application. To install the plug-in, select **Custom** in the InstallShield installation program or specify the InternetExplorerPlugin feature on the Windows Installer command line. For instructions, see "Installing RSA SecurID Software Token for Windows" on page 19.

The Internet Explorer plug-in is accessible by web sites protected by RSA Authentication Agent for Web for IIS. You must use the updated HTML template pages included in **RSAWebAgentTemplates.zip** to replace the existing HTML template pages used by Authentication Agent for Web. The HTML template pages contain JavaScript defining the RSA SecurID authentication prompts to be displayed when a user attempts to access a protected site. For the most recent RSA Authentication Agent for Web for IIS template files, see **https://www.rsa.com/en-us/products/identity-and-access-management/securid-authentication-agents**.

To invoke the plug-in, users open Internet Explorer and navigate to a protected web site. An authentication page prompts users to select a software token from their list of tokens and enter their username and PIN. After users enter their PIN, the passcode (OTP) generated by the SecurID desktop application is passed automatically to RSA Authentication Manager. Users do not need to open the SecurID desktop application to get an OTP.

Note: RSA SecurID Software Token 5.0.2 for Windows does not support running multiple instances of the Internet Explorer plug-in within the same browser process. As a result, users cannot use the Internet Explorer plug-in to authenticate simultaneously to multiple sites that are protected by SecurID.

Connected RSA SecurID 800 Authenticator

You can use an RSA SecurID 800 Authenticator (SecurID 800) connected to a USB port with RSA SecurID Software Token for Windows for automatic tokencode retrieval by a VPN client application. You can also use a connected SecurID 800 with the optional Internet Explorer plug-in for automatic tokencode retrieval by web resources protected by RSA SecurID. Users only need to enter their SecurID PINs to be authenticated.

To use connected SecurID 800 Authenticators, you must install RSA Smart Card Middleware 3.6. A plug-in that is installed automatically with the SecurID desktop application allows the Smart Card Middleware and the desktop application to communicate with the SecurID 800.

You install the Middleware from the RSA Authentication Client 3.6 product kit at **https://community.rsa.com/community/products/securid/authentication-client-36/downloads**. Install the Middleware as documented in the *RSA Authentication Client 3.6 Installation and Administration Guide* at **https://community.rsa.com/community/products/securid/authentication-client-36**.

If the SecurID 800 is the only token used with the desktop application, it is automatically the active token (the token from which OTPs are retrieved). If the user has imported software tokens to the desktop application, however, the user must open the application and select the SecurID 800 serial number (or nickname) from the list of tokens. For details, see the RSA SecurID Software Token Help.

Note: You cannot import software tokens to a SecurID 800. Only the built-in token can be used to generate OTPs.

Customization Policies

You can set policies to customize the behavior of RSA SecurID Software Token 5.0.2 for Windows.

The following table summarizes the customization policies. For details and instructions, see Appendix A, "Customizing the Application."

Important: RSA recommends that you set customization policies before you install the application.

Policy	Description
ActivationCode	Specifies that the Windows user security identifier (user SID) should be used as the activation code for a token provisioned using dynamic seed provisioning (CT-KIP). To allow a token to be imported automatically the first time that the user launches the application, you must set both ActivationCode and CtkipUrl.
CtkipUrl	Prefills the **Enter URL** field in the application so that the user does not have to enter the URL when importing a token provisioned using CT-KIP.
DisableChangeTokenName	Specifies whether or not users can change the nicknames assigned to their tokens.
DisableDeleteToken	Specifies whether or not users can delete their tokens.
DisableSetDevicePassword	Specifies whether or not users are permitted to set a device password. Applies only to the Local Hard Drive (RSA) plug-in.
OnlyOneToken	Specifies that users can have only one token installed.
TokenExpirationNotification	Changes the number of days before the application displays a notification informing the user that a token is nearing its expiration date. If you do not set this policy, the notification is displayed 30 days before the token expires. If used with TokenRenewalURL, this policy adds a link in the token expiration notification to a URL where the user can request a replacement token.
TokenRenewalURL	Used with the TokenExpirationNotification policy. Specifies a URL link to display in the token expiration notification. For example, the link could be the URL of the RSA Self-Service portal where the user can request a replacement token.
ValidDevices	Specifies a whitelist of storage devices to which tokens can be imported.

Secure Sites

You can assign each user up to three tokens, and for each token, you can designate up to three secure web sites for that token to protect. For example, if a user has three tokens, you can protect up to nine web sites. The separate sitelist template that was provided with the RSA SecurID Toolbar 1.4.2 product is not supported. If secure web sites are not designated, then the user can attempt to authenticate with the token at any web site that is protected by your RSA Authentication Manager deployment.

When configuring a token, you can specify secure sites by adding the TOOLBAR_SITEURL1, TOOLBAR_SITEURL2, and TOOLBAR_SITEURL3 attributes to the token record. The attribute value must be the web URL of the secure site. IP addresses are not supported as secure sites.

You can use an asterisk as a wildcard to represent any characters. This can provide access to all of the sites in a specific domain. For example, an administrator can enter https://*.xyz.com to allow access to all of the sites that end with .xyz.com.

In RSA Authentication Manager 8.*x*, you can add up to three secure web sites to the software token profile, which specifies software token configuration and distribution options. When you configure a token that uses this software token profile, you can add, remove, or update the secure sites as needed.

For instructions on how to use this feature, see the *RSA SecurID Software Token 5.0 for Windows Provisioning Guide*.

System Requirements

The following table lists the system requirements for RSA SecurID Software Token 5.0.2 for Windows.

Description	Requirement
Operating System	RSA SecurID Software Token 5.0.2 for Windows supports the following: • Windows 10 32-bit and 64-bit • Windows 8.1 32-bit and 64-bit • 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

Description	Requirement
Internet Explorer support for Internet Explorer Plug-In	RSA SecurID Software Token 5.0.2 for Windows supports the following: • Internet Explorer 11 on Windows 10, Windows 8.1, and Windows 7 • Internet Explorer 10 on Windows 8.1 and Windows 7 • Internet Explorer 9 on Windows 7 and Windows Vista • Internet Explorer 8 on Windows 7 and Windows Vista **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.

Token Storage Devices

A token storage "device" is a logical storage container for tokens. The SecurID desktop application can store tokens on the user's hard drive, a Trusted Platform Module (TPM), a biometric device, a flash drive, or another supported device. By default, the application stores tokens on the user's local hard drive. For more information, see the *RSA SecurID Software Token 5.0 for Windows Provisioning Guide*.

Support for Visually Impaired Users

RSA SecurID Software Token 5.0.2 for Windows supports the use of screen readers for visually impaired users. RSA has tested the application with the JAWS for Windows Screen Reading Software. You can download JAWS from the Freedom Scientific web site. Once you install JAWS, no additional configuration is required to use the software with the SecurID desktop application.

Virtual Machines

The SecurID desktop application has not been fully tested and qualified on virtual machines. RSA Customer Support will initially assist you with issues that occur on a virtual machine, 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 desktop application and RSA Authentication Manager 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 desktop application. Users crossing time zones with their computer need to change only the time zone in order to reflect the correct local time.

2 Installing the Application

This chapter describes installing RSA SecurID Software Token 5.0.2 for Windows (the SecurID desktop application), upgrading from a previous version, repairing the application, and uninstalling the application.

Important: 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.

Before You Begin

Before you install the SecurID desktop application, decide whether to:

- Install the optional Internet Explorer browser plug-in. This feature allows users to authenticate to selected web pages without manually entering a one-time password (OTP).

  The Internet Explorer plug-in is accessible by web sites protected by RSA Authentication Agent for Web for IIS. You must use the updated HTML template pages included in **RSAWebAgentTemplates.zip** to replace the existing HTML template pages used by Authentication Agent for Web. For the most recent RSA Authentication Agent for Web for IIS template files, see **https://www.rsa.com/en-us/products/identity-and-access-management/securid-authentication-agents**.

  For more information, see "Internet Explorer Plug-In" on page 10.

- Customize the behavior of the application using policy settings. For example, install the database that will contain the user's software tokens (token database) to a location other than the default directory. For more information, see Appendix A, "Customizing the Application."
- Change the database that contains tokens stored on the local hard drive from the default per-user database to a single database. For more information, see "Token Storage Database Options for VPN Client Applications" on page 18.
- Disable the default copy protection on the token database. For more information, see "Token Database Copy Protection" on page 19.

Note: After you install the SecurID desktop application, you will need to issue and provision software tokens. For more information, see the *RSA SecurID Software Token 5.0 for Windows Provisioning Guide*.

Token Storage Database Options for VPN Client Applications

The first time a user runs RSA SecurID Software Token 5.0.2, a token storage database is created on the user's computer. This database is a container for the tokens imported to the local hard drive. When a user performs an RSA SecurID authentication, the application retrieves the tokencode from the token in the database.

The default token storage database is a per-user database, meaning that it contains only those tokens that belong to a specific user of the computer. The per-user database is intended to be used by VPN client applications that are running in the user context. (To run in the user context, the user must start the VPN client application.)

If your users log on to the VPN client before logging on to Windows (referred to as "prelogon" or "start before logon") or you run your VPN client as a service, you cannot use the default per-user database. You must instead configure your installation to create a single database that contains all of the tokens stored on the hard drive.

This is required for the following reasons:

- When a user logs on to the VPN client before logging on to Windows, the user context is not known (the user cannot be identified), because the user has not yet logged on to Windows. Therefore, the SecurID desktop application cannot locate the user's token.
- When a VPN client is running as a service, a specific user cannot be identified and that user's token cannot be located because the VPN client is running as System instead of as a user.

Important: Due to the user context issues, the RSA SecurID Software Token 5.0.2 for Windows supports prelogon VPN authentication and running the VPN client as a service for only one user who has been issued only one software token. However, the application supports a single user with multiple tokens if the VPN client application provides the option of selecting a token from a list.

To create a single database, you must install the desktop application from the **msiexec** command line, using the SETSINGLEDATABASE property. This property creates a single database in the **All Users** directory. When the user starts prelogon to the VPN client, for example, the VPN client retrieves a token from **All Users**.

If necessary, you can create the single database in a location other than the default location. For more information, see "Command Line Properties" on page 23.

Important: Use the SETSINGLEDATABASE property only on single-user machines. Do not use this property if multiple users share a computer, because doing so gives all users access to all tokens stored in the single database.

Token Database Copy Protection

RSA SecurID Software Token 5.0.2 for Windows uses the following data protection mechanisms to tie the token database to a specific computer:

- Binding the database to the computer's primary hard disk drive
- Implementing the Windows Data Protection API (DPAPI)

These mechanisms ensure that an unauthorized user cannot move the token database to another computer and access the tokens.

If you replace a hard disk drive on a computer, the token database installed on that computer cannot be recovered, and you must issue new tokens to users of that computer. If you back up users' hard disk drives on a daily basis, and you are concerned about possibly having to replace hard disk drives, you can preserve users' software tokens by disabling copy protection when you install the RSA SecurID Software Token. To do so, you must install the application from the command line and set the SETCOPYPROTECTION property to FALSE. This disables binding the database to the hard disk drive on all computers on which you install the application. For a command example, see "Command Line Examples" on page 26.

Even if you disable copy protection, the database is still protected by DPAPI. You can further protect the database by having the user set a device password, as described in "Set a Device Password" on page 41.

Installing RSA SecurID Software Token for Windows

RSA SecurID Software Token 5.0.2 for Windows provides two separate Windows Installer MSI files (available in 32-bit and 64-bit versions):

RSASecurIDToken502.msi (32-bit) and **RSASecurIDToken502x64.msi** (64-bit). Install the RSA SecurID Standard desktop application 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).

RSASecurIDTokenAuto502.msi(32-bit) and **RSASecurIDTokenAuto502x64.msi** (64-bit). Install the RSA SecurID Software Token with Automation 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.

For more information, see "Standard Desktop Application" on page 9 and "RSA SecurID Software Token with Automation" on page 10.

Both Windows Installer MSI files contains a database of information on the elements of the installation, uninstallation, and upgrades for the application and its components. If you do not want to customize the product, you can double-click the MSI file to start an interactive installation. To customize the product, you must invoke the MSI file from the command line, specifying the features and properties that you want to install.

Note: RSA recommends that you set any customization policies before you install the application. For more information, see "Customizing the Application" on page 51.

You cannot install both variants of the 5.0.2 application on the same computer. For example, if you install the Standard desktop application and then attempt to install the RSA SecurID Software Token with Automation, an error message occurs and the installer exits.

If you attempt to install the same variant on the same computer with the InstallShield program, the installation program displays the Program Maintenance window. This window allows you to modify, repair, or remove the application.

For information on removing the application, see "Uninstalling RSA SecurID Software Token for Windows" on page 33.

Enterprise-Wide Installations

You can install RSA SecurID Software Token 5.0.2 for Windows on a large number of computers using a third-party deployment tool, such as Microsoft System Center Configuration Manager. If you specify a silent installation, the application is installed on all computers without requiring users to interact with the installation program. A silent installation is ideal for organizations that do not allow non-administrators to install software.

With Configuration Manager or another third-party deployment tool, you can include token files (SDTID files) in your deployment package. Configure the distribution package so that tokens will be installed to **Desktop** or to **My Documents**. This ensures that tokens will be imported automatically when a user starts the application.

When you create the distribution package, you must use a specific script so that each user receives a unique token. For example, use a script that contains logic such as the following to ensure that only the target user receives the token.

> "if systemresource.name=LAPTOP-LAP, copy *username*.sdtid c:\Users\username\Desktop"

Windows Installation Package

The RSA SecurID Software Token 5.0.2 for Windows installation kit, **RSASecurIDSoftwareToken502.zip**, contains the following (depending upon whether you have the 32-bit or 64-bit version):

- An installation package for the Standard desktop application, **RSASecurIDToken502.msi** (32-bit) or **RSASecurIDToken502x64.msi** (64-bit).
- An installation package for the desktop token with Software Token Automation installation, **RSASecurIDTokenAuto502.msi** (32-bit) or **RSASecurIDTokenAuto502x64.msi** (64-bit).
- A device definition file for the Standard desktop application, **def\Desktop-Windows-5.x-swtd.xml**. This file specifies the supported capabilities and attributes of tokens used with the desktop application. For more information, see the *RSA SecurID Software Token 5.0 for Windows Provisioning Guide*.

- A device definition file for the RSA SecurID Software Token with Automation, **def\Desktop-Windows-5.x-Auto-swtd.xml**. This file specifies the supported capabilities and attributes of tokens used with the desktop application. For more information, see the *RSA SecurID Software Token 5.0 for Windows Provisioning Guide*.
- An administrative template, **template\RSASecurIDToken.adm**. For more information, see "Customizing the Application" on page 51.

Install the Application Using the InstallShield Program

This section describes how to install RSA SecurID Software Token 5.0.2 for Windows using the InstallShield installation program.

Before You Begin

- You must have administrator privileges to install RSA SecurID Software Token 5.0.2 for Windows.
- The Internet Explorer plug-in requires Internet Explorer 8, 9, 10, or 11. Before installing this plug-in, make sure users have the correct version installed on a supported Windows operating system. For more information, see "System Requirements" on page 13.

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.

Procedure

1. Open the installation kit.
2. In the root directory, double-click the **msi** file:

   Note: In Windows 10, you must right-click the Windows Installer MSI file, and select **Run as administrator** to install the application.

   - To install the Standard desktop application, click **RSASecurIDToken502.msi** (32-bit) or **RSASecurIDToken502x64.msi** (64-bit).
   - To install the RSA SecurID Software Token with Automation, click **RSASecurIDTokenAuto502.msi** (32-bit) or **RSASecurIDTokenAuto502x64.msi** (64-bit).
3. On the Welcome screen, click **Next**.
4. On the License Agreement screen, read the terms of the license agreement, and then select **I accept the terms in the license agreement**. You must accept the terms in the license agreement to continue the installation. To print the license agreement, click **Print**. Click **Next**.

   The Setup Type screen is displayed.

5. Do one of the following.
   - To install the application to the default location without installing the Internet Explorer plug-in, select **Typical**, click **Next**, and click **Install**. When the installation is complete, select the option to launch the application or click **Finish**.

     You do not need to restart your computer.
   - To install the Internet Explorer plug-in, or to install the application to a location other than the default, select **Custom**.

     The Custom Setup screen is displayed. The RSA SecurID Token Library is installed by default. You cannot remove this feature.
6. Do one of the following:
   - To install the application to a directory other than the default, click **Change**. Change the destination directory, and click **OK**.
   - To install the Internet Explorer plug-in, click the plus sign to display the plug-in option, select the plug-in, and select **This feature will be installed on local hard drive**.
7. Click **Next**.
8. On the Ready to Install the Program screen, click **Install**.

   When the installation is complete, you are prompted to launch the application.
9. Do one of the following:
   - To start the application, select **Launch RSA SecurID Token**, and click **Finish**.
   - If you do not want to start the application, click **Finish**.

     You do not need to restart your computer.

Command Line Installation

A Windows Installer command line installation allows you to install product features to meet your specific requirements. For example, if you use the software token library with a supported third-party plug-in that has its own user interface, you can exclude the desktop application executable ("DesktopClient") from the installation. The installation package also provides command line properties that allow you to change the location where specific components are installed on the user's system.

Note: You must run the command line installation as an administrator.

Features That Can Be Installed or Uninstalled from the Command Line

The following table describes the product features that you can install or uninstall from the command line.

Feature Name	Description	Installed by Default?
DesktopClient	The client components of the application, including the application user interface.	Yes
InternetExplorerPlugin	Internet Explorer plug-in	No
HDDPlugin	Local Hard Drive (RSA) plug-in. This is the default storage device plug-in.	Yes
HWAuthenticatorPlugin	RSA Hardware Authenticator Plug-In 5.0.2, which supports using a connected SecurID 800 authenticator with the desktop application. For more information, see "Connected RSA SecurID 800 Authenticator" on page 11. **Note:** You can leave this plug-in installed even if you do not use connected SecurID 800 devices.	Yes

Command Line Properties

The following table describes the properties that you can set using the command line. Once you set a command property, you cannot change it unless you first uninstall the application.

Property	Description	Values
COPYTOSYSTEM32	Installs a copy of the software token library, **stauto32.dll**, and its dependent DLLs (**QtCore4.dll** and **QtGui4.dll**) into the **system32** directory. Does not add the application path to the system PATH environment variable, because the application will find **stauto32.dll** in the **system32** directory. You may want to use this option if adding the application path to the System path causes the System path to exceed the Windows length limit.	TRUE or FALSE. If set to TRUE, the installation program does not modify the system PATH environment variable, and copies DLLs to the system32 directory. Default is FALSE.

Property	Description	Values
SETCOPYPROTECTION	Sets copy protection on the token database by binding the token database to the primary hard disk drive on the computer. For more information, see "Token Storage Database Options for VPN Client Applications" on page 18.	TRUE or FALSE. If set to TRUE, copy protection is enabled. If set to FALSE, copy protection is disabled. Default is TRUE.
SETDATABASEDIR	Installs the database containing the user's software tokens (token database) to a location other than the default directory. Allows enterprises that do not allow Write access to the default installation directory, or that have other drives that are set up for encryption, to configure the location of the token database directory during a silent installation. The total length of the database name combined with the database directory cannot exceed the maximum pathname length for the platform. **Important:** You must give nonadministrative users Read, Write, and Modify privileges to the database directory. Otherwise, they might not be able to use the application. The database should not be installed in protected directories such as **Program Files** and the **C:** root directory.	Set the database directory path as follows. **For a Per-User Database:** The path must begin with ~/ or ~\, making it relative to the user directory and applicable to multiple users. The user directory on Windows 7, Windows 8, Windows 10, and Windows Vista is **C:\Users*username***. **For a Single Database:** You can either specify an absolute path or use the %HOMEDRIVE% Windows environment variable. An absolute path begins with the drive letter and a backslash: *drive*:\. The %HOMEDRIVE% variable specifies a drive letter that is set in Active Directory. The database will be owned by the first user to use the application. The default directory on Windows 7, Windows 8, Windows 10, and Windows Vista is **~\AppData\Local\RSA\ RSASecurID Software Token Library**. Directory path elements are created if they do not exist. The /../ characters are not allowed.
SETSINGLEDATABASE	Creates a single token database. Set this property to TRUE to allow prelogon to a VPN client application. Because the VPN client cannot identify the user prior to Windows logon, the user's tokens must be stored in a single database that is not associated with the specific user. This property is intended for users who do not share a computer. This property is not supported if multiple SecurID users share a computer.	TRUE or FALSE. If set to TRUE, changes the default database location from the specific user location to **C:\ProgramData\RSA\…** on Windows 7, Windows 8, Windows 10, and Windows Vista. Default is FALSE.

Command Line Syntax

To install RSA SecurID Software Token for Windows from the command line, use the Windows Installer command, **msiexec**, with appropriate options.

Note: You must run the command line installation as an administrator.

Follow these guidelines for a command line installation:

- All properties entered on the command line are interpreted as uppercase, but the value retains case sensitivity. For example, you can enter the SETSINGLEDATABASE property in uppercase or lowercase, but you must enter the value (TRUE or FALSE) in uppercase.
- By default, the application is installed to the **Program Files** directory. To change the location of the destination directory, use the Windows Installer INSTALLDIR property.
- To install specific features, and exclude others, you must use the **msiexec** command with the ADDLOCAL property. You must specify each feature that you want to install. The ADDLOCAL property takes the form ADDLOCAL=*PropertyValue*. Separate each value with a comma. See "Command Line Examples" on page 26.
- To add or remove a feature after performing an installation, you must reinstall the software. To remove a feature, use the REMOVE property. To add a feature that you did not initially install, use the ADDLOCAL property. See "Modify an Installation Using the Command Line" on page 29.
- If pathnames or properties contain spaces, enclose the entire path in quotation marks.
- Enter command line options (for example, /i) in either lowercase or uppercase. Windows Installer command line options are case insensitive.
- To review the results of the installation, use the /lv option (verbose logging). Store the log file, for example, install.log, in a known location, such as %USERPROFILE%.

Note: For more information on Windows Installer command line options, open a command line, and type **msiexec**. This displays **msiexec** command options. For additional details, access the Microsoft Developer Network Library (MSDN Library) and search on "Windows Installer Command Line Options."

Command Line Examples

The following sections contain examples of installations performed using the Windows Installer **msiexec** command line. The /i option, with the MSI filename, installs the application. The examples use the /qn option, which specifies a silent, or quiet installation (no user prompts), and the /lv option, which creates a verbose installation log.

Install the Application Silently

The following command installs the 32-bit version of the application, the default storage device plug-in (hard drive plug-in), and the RSA Hardware Authenticator Plug-In. To install the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

For the Standard desktop application, type:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
```

For the RSA SecurID Software Token with Automation, type:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log
```

Install the Application, Internet Explorer Plug-In, and Hard Drive Plug-In

The following command uses the ADDLOCAL property to silently install the 32-bit version of the application, the Internet Explorer plug-in, and the default storage device plug-in (HDDPlugin). To install the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

For the Standard desktop application, type:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
ADDLOCAL=DesktopClient,InternetExplorerPlugin,
HDDPlugin
```

For the RSA SecurID Software Token with Automation, type:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log ADDLOCAL=DesktopClient,InternetExplorerPlugin,
HDDPlugin
```

Install a Copy of the Software Token API to the system32 Directory

The following command uses the COPYTOSYSTEM32 property to install a copy of the software token API into the **system32** directory. Use a command similar to this one if adding the application path to the System path will cause the System path to exceed the Windows length limit.

To run these examples for the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

For the Standard desktop application, type:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
COPYTOSYSTEM32=TRUE
```

For the RSA SecurID Software Token with Automation, type:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log COPYTOSYSTEM32=TRUE
```

Set Copy Protection

The following command uses the SETCOPYPROTECTION property to remove token binding from the local hard drive. Use a command similar to this one to avoid having to reissue new tokens if you replace users' hard disk drives. This command does not affect copy protection provided by the DPAPI implementation.

To run these examples for the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

For the Standard desktop application, type:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
SETCOPYPROTECTION=FALSE
```

For the RSA SecurID Software Token with Automation, type:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log SETCOPYPROTECTION=FALSE
```

Install the Token Database to a Non-Default Location

The following command silently installs the 32-bit version of the application and installs the token storage database to a non-default location. Use a command similar to this one to install the token database in a custom directory if your company does not allow Write access to the default installation directory or if you have other drives that are set up for encryption.

To install the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

For the Standard desktop application, type:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
SETDATABASEDIR=~\rsatokens
```

For the RSA SecurID Software Token with Automation, type:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log SETDATABASEDIR=~\rsatokens
```

Install a Single Token Database to the Default Location

The following command silently installs the 32-bit version of the application and creates a single token storage database that is not associated with a specific user. The database resides in the **All Users** directory. Use a command similar to this one if you are using an application that has integrated SecurID functionality.

To install the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

For the Standard desktop application, type:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
SETSINGLEDATABASE=TRUE
```

For the RSA SecurID Software Token with Automation, type:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log SETSINGLEDATABASE=TRUE
```

Install a Single Token Database to a Non-Default Location

The following command silently installs the 32-bit version of the application and creates a single token storage database that is not associated with a specific user. To install the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

Using an absolute path with the SETDATABASEDIR property creates a single database instance that is owned by the first user to use the application.

The first example specifies an absolute path that begins with the drive letter and a backslash: *drive*:\. The second example uses the %HOMEDRIVE% Windows environment variable to specify the drive letter that is set in Active Directory.

For the Standard desktop application, type:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
SETSINGLEDATABASE=TRUE SETDATABASEDIR=c:\LocalDir
```

For the RSA SecurID Software Token with Automation, type:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log SETSINGLEDATABASE=TRUE
SETDATABASEDIR=%HOMEDRIVE%\LocalDir
```

Modify an Installation

You can modify an existing installation to add or remove installable features.

Modify a Single Installation Using the Program List

You can add or remove the Internet Explorer plug-in from a single installation using the Windows program list.

Note: You cannot use the program list to install or remove the hard drive plug-in (HDDPlugin) or the RSA Hardware Authenticator Plug-In (HWAuthenticatorPlugin). You must use the **msiexec** command line.

Procedure

1. In the Control Panel, click **Programs > Programs and Features**, and then select **RSA SecurID Software Token** or **RSA SecurID Software Token with Automation**.
2. Click **Change** to launch the **RSA SecurID Software Token Setup Wizard**. Click **Next**.
3. Select **Modify** and click **Next**.
4. Do one of the following:
   - To install the Internet Explorer-plug-in, select **This feature will be installed on local hard drive**.
   - To remove the Internet Explorer plug-in, select **This feature will not be available**.
5. Click **Next**, and click **Install**.
6. Click **Finish**.

Modify an Installation Using the Command Line

You can modify an installation on multiple computers using the **msiexec** command. You can use the **msiexec** command to add or remove the Internet Explorer plug-in or to remove the local hard drive plug-in or the Hardware Authenticator Plug-In.

Add the Internet Explorer Plug-in Using the Command Line

Use the **msiexec** command with the ADDLOCAL property, and specify the value of the Internet Explorer plug-in.

These examples silently install the 32-bit version of the application and default device plug-in, add the Internet Explorer plug-in, and log the results to a file. To silently install the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

Standard desktop application example:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
ADDLOCAL=DesktopClient,HDDPlugin,
InternetExplorerPlugin
```

RSA SecurID Software Token with Automation example:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv c:\install.log
ADDLOCAL=DesktopClient,HDDPlugin,
InternetExplorerPlugin
```

Remove the Internet Explorer Plug-in Using the Command Line

Use the **msiexec** command with the REMOVE property, and specify the value of the Internet Explorer plug-in.

These examples silently remove the Internet Explorer plug-in and log the results to a file. To run these examples for the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

Standard desktop application example:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
REMOVE=InternetExplorerPlugin
```

RSA SecurID Software Token with Automation example:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log REMOVE=InternetExplorerPlugin
```

Remove the Local Hard Drive Plug-in Using the Command Line

Use the **msiexec** command with the REMOVE property, and specify the value of the local hard drive plug-in.

These examples silently remove the local hard drive plug-in and log the results to a file. To run these examples for the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

Standard desktop application example:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
REMOVE=HDDPlugin
```

RSA SecurID Software Token with Automation example:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log REMOVE=HDDPlugin
```

Remove the RSA Hardware Authenticator Plug-In Using the Command Line

Use the **msiexec** command with the REMOVE property, and specify the value of the Hardware Authenticator Plug-In.

These examples silently remove the Hardware Authenticator Plug-In and log the results to a file. To run these examples for the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

Standard desktop application example:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
REMOVE=HWAuthenticatorPlugin
```

Desktop application with Software Token with Automation example:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log REMOVE=HWAuthenticatorPlugin
```

Repair an Installation

You can repair errors in the existing installation. The repair process rewrites required registry entries, reinstalls missing files, replaces old files, and reinstalls shortcuts. Repairing the installation does not affect tokens that you have imported unless the token database has become corrupted. In that case, you must import new tokens.

Repair a Single Installation Using the Program List

You can repair a single installation using the program list.

Procedure

1. In the Control Panel, click **Programs and Features**, and then select **RSA SecurID Software Token** or **RSA SecurID Software Token with Automation**.
2. Click **Change** to launch the **RSA SecurID Software Token Setup Wizard**. Click **Next**.
3. Select **Repair**, and click **Next**.
4. On the Ready to Repair the Program screen, click **Install**.
5. When the repair is complete, click **Finish**.
6. When prompted, click **Yes** to restart the computer, or **No** to manually restart later.

Repair an Installation on Multiple Computers Using the Command Line

You can repair an installation on multiple computers using the **msiexec** command line.

Procedure

Use the **msiexec** command with the /f option. The following examples silently repair an installation and logs the results to a file. To repair the 64-bit version of the application, change the installer filename to **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

For the Standard desktop application, type:

```
msiexec /qn /f pathname\RSASecurIDToken502.msi /lv c:\install.log
```

For the RSA SecurID Software Token with Automation, type:

```
msiexec /qn /f pathname\RSASecurIDTokenAuto502.msi /lv
c:\install.log
```

Upgrading RSA SecurID Software Token for Windows

RSA SecurID Software Token 5.0.2 for Windows supports upgrading from version 5.0 and version 5.0.1. Upgrading overwrites the existing version and copies the existing token database to the 5.0.2 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 5.0.2 of the RSA SecurID Software Token with Automation and a per-user database. If you want to change the variant of the application or the database option, then you must uninstall the existing application. For more information, see "Uninstalling RSA SecurID Software Token for Windows" on page 33.

You can upgrade 5.0 and 5.0.1 to either the 32-bit or 64-bit version of 5.0.2.

If the optional Firefox browser plug-in is installed, upgrading to 5.0.2 removes it. To install the Internet Explorer plug-in that is supported by this release, select **Custom** in the InstallShield installation program or specify the InternetExplorerPlugin feature on the Windows Installer command line.

Note: If you installed a previous version to a directory other than the default, and you want to install version 5.0.2 to that directory, you must select a Custom setup and change the destination directory to match your previous installation.

Upgrade Procedures

You can upgrade using the MSI file or the msiexec command line.

Upgrade Using the MSI File

For the Standard desktop application, run the RSA SecurID Software Token 5.0.2 MSI file **RSASecurIDToken502.msi** (32-bit) or **RSASecurIDToken502x64.msi** (64-bit).

For the RSA SecurID Software Token with Automation, run the RSA SecurID Software Token 5.0.2 MSI file **RSASecurIDTokenAuto502.msi** (32-bit) or **RSASecurIDToken502x64.msi** (64-bit).

Note: In Windows 10, you must right-click the Windows Installer MSI file, and select **Run as administer** to upgrade the application.

Upgrade Using the Command Line

Enter the **msiexec** installation command with your preferred options. If you installed the Internet Explorer plug-in, and you want to use it with version 5.0.2, specify ADDLOCAL=InternetExplorerPlugin.

Note: You must run the command line installation as an administrator.

For example, the following command silently upgrades to RSA SecurID Software Token 5.0.2 for Windows (32-bit), installs the default per-user token database, reinstalls the default features, and adds the Internet Explorer plug-in and Local Hard Drive Plug-In. To silently upgrade the 64-bit version of the application, substitute **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

For the Standard desktop application, type:

```
msiexec /qn /i pathname\RSASecurIDToken502.msi /lv c:\install.log
ADDLOCAL=DesktopClient,HDDPlugin,InternetExplorerPlugin
```

For the RSA SecurID Software Token with Automation, type:

```
msiexec /qn /i pathname\RSASecurIDTokenAuto502.msi /lv c:\install.log
ADDLOCAL=DesktopClient,HDDPlugin,InternetExplorerPlugin
```

Uninstalling RSA SecurID Software Token for Windows

You can uninstall RSA SecurID Software Token for Windows using the program list or from the command line. Uninstalling the application also removes the software token database of the user performing the uninstall. It does not remove the token databases of other users who share the same system.

Note: You must have administrator privileges to uninstall the application.

Uninstall the Application Using the Program List

Use the following procedure to uninstall the application using the program list.

Procedure

1. In the Windows Control Panel, click the program list (for example, **Programs**).
2. Click **RSA SecurID Software Token** or **RSA SecurID Software Token with Automation**, and click **Uninstall**.
3. When prompted to verify that you want to remove the program, click the appropriate removal option.

Uninstall the Application Using the Command Line

Use the following procedure to uninstall the application using the command line.

Procedure

Use the **msiexec** command with the /x (uninstall) option. The following examples uninstall the 32-bit version of the application silently and log the results to a file. To uninstall the 64-bit version of the application, substitute **RSASecurIDToken502x64.msi** or **RSASecurIDTokenAuto502x64.msi**.

Standard desktop application example:

```
msiexec /qn /x pathname\RSASecurIDToken502.msi /lv c:\install.log
```

RSA SecurID Software Token with Automation example:

```
msiexec /qn /x pathname\RSASecurIDTokenAuto501.msi /lv
c:\install.log
```

3 User Options for Managing Tokens and Devices

This chapter provides an overview of how users can manage tokens stored on their hard drive or on another supported device plug-in. Use the information in this chapter to familiarize yourself with the RSA SecurID Software Token 5.0.2 for Windows (the SecurID desktop application) user interface.

From the application user interface, users can:

- Import tokens
- Change a token name
- Select a token if multiple tokens have been imported
- Set a password to protect tokens stored on the local hard drive
- Set a password or enter other credentials to protect tokens stored on a supported third-party device
- View information about a token
- View information about installed token storage devices
- Delete a token
- Obtain the next code

Note: Before users can import tokens, an administrator must issue and provision software tokens. For more information, see the *RSA SecurID Software Token 5.0 for Windows Provisioning Guide*.

Importing Tokens

RSA provides the following mechanisms for importing tokens to the application:

- Import a token automatically using CT-KIP. (The administrator must have set the ActivationCode policy to 1 and the CtkipUrl policy to the URL of the CT-KIP server.)
- Import a token from the web (CT-KIP) using the SecurID desktop application.
- Import a token from an email attachment.
- Import a token automatically from a default directory.
- Import a token from a non-default directory.

When importing a token, the user is prompted to select the device that will store the token if more than one supported device plug-in is installed (for example, a biometric device and the local hard drive) and you did not bind the token to a device.

Import a Token Automatically Using CT-KIP

If you provision tokens using Dynamic Seed Provisioning (CT-KIP), you can customize RSA SecurID Software Token 5.0.2 for Windows to automatically import a token the first time the user starts the application, as long as either of the following conditions is met:

- The user does not already have a token.
- All of the tokens in the user's token database have expired.

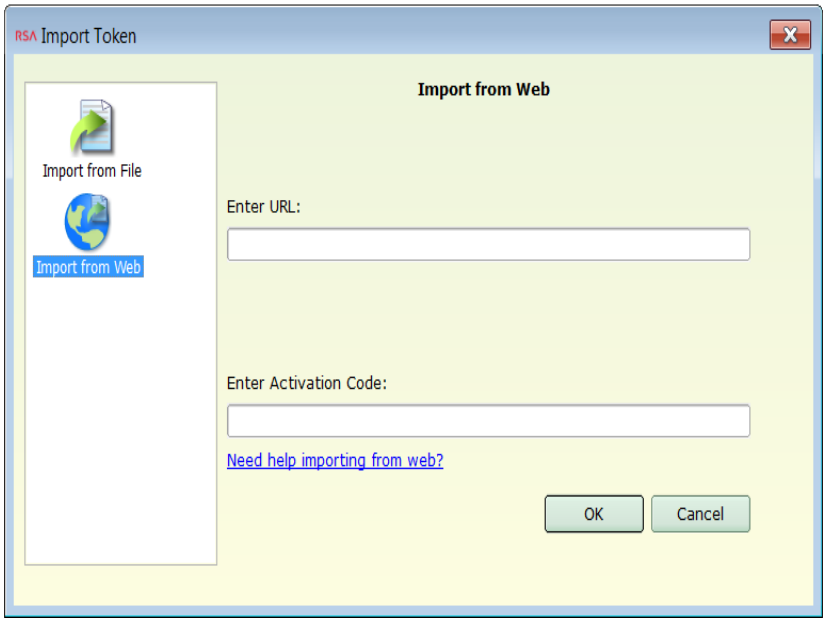
Auto-import requires setting the ActivationCode and CtkipUrl policies. For more information, see "Customizing the Application" on page 51.

Import a Token from the Web Using the Desktop Application

If you provisioned a token using CT-KIP, the user must import it using the SecurID desktop application if you did not set policies to auto-import the token or if the user already has a token.

Procedure

1. Start the SecurID desktop application.
   The Import Token screen is displayed.
2. Click **Import from Web**.
   The Import from Web screen is displayed.



3. In the **Enter URL** field, enter the CT-KIP URL.

   Note: If you configured the CtkipUrl policy, the **Enter URL** field is prefilled.

4. In the **Enter Activation Code** field, enter the activation code. Click **OK**.

5. If prompted to select a device, click the name of the device where the token will be stored, for example, "Local hard drive (RSA)."
6. Click **OK**.

   A success message is displayed.
7. If prompted to rename your token, do one of the following:
   - To change the token name, click **Change Name**. Enter a name of 1 to 24 characters (for example, "VPN Token"). Click **OK**.
   - If you do not want to change the name, click **OK** to close the screen.

Import a Token from an Email Attachment

If you distribute a token as an SDTID file, a user can import the token from an email attachment. After the token has been imported, the application deletes the SDTID file.

Procedure

1. Double-click the file attachment, for example, "token1.sdtid."
2. When prompted to open or save the attachment, click **Open**.

   The SecurID desktop application detects the token file and starts up.

Note: On some Windows machines, you may be prompted to select the application that you want to use to open the file. In that case, you must manually select the SecurID desktop application.

3. If prompted, enter the file password, and click **OK**.
4. If prompted to select a device, click the name of the device where the token will be stored, for example, "Local hard drive (RSA)."
5. Click **OK**.

   A success message is displayed.
6. If prompted to rename your token, do one of the following:
   - To change the token name, click **Change Name**. Enter a name of 1 to 24 characters (for example, "My VPN Token"). Click **OK**.
   - If you do not want to change the name, click **OK** to close the screen.

Import a Token Automatically from a Default Directory

If you distribute a token as an SDTID file, a user can save it to a default directory where the application can automatically locate it. You can optionally use a deployment tool to push the file to a default directory. If you provision multiple tokens to a single user, the application imports the files one at a time. The application then deletes each token file, as long as the file is not marked read-only or otherwise protected.

The default directories are **Desktop** or **My Documents**.

Procedure

1. Save the SDTID file attachment to one of the default directories.
2. Start the application.

   The application automatically detects the token file and imports the token.

   If you, as administrator, use a deployment tool to push the file to one of the default directories, the token is imported automatically the next time the user starts the application.
3. If prompted, enter the file password, and click **OK**.
4. If prompted to select a device, click the name of the device where the token will be stored, for example, "Local hard drive (RSA)."
5. Click **OK**.

   A success message is displayed.
6. If prompted to rename your token, do one of the following:
   - To change the token name, click **Change Name**. Enter a name of 1 to 24 characters (for example, "My VPN Token"). Click **OK**.
   - If you do not want to change the name, click **OK** to close the screen.

Import a Token from a Non-Default Directory

If a user saves a token file to a directory other than one of the default directories, the user can import the token using either of the following methods:

- Navigate to the token file and double-click the file.
- Import the token using the desktop application.

After the token has been imported, the application deletes the SDTID file.

Procedure

1. Start the SecurID desktop application.
   The Import Token screen is displayed.
2. Click **Import from File**.
3. Browse to the folder that contains the SDTID file, and double-click the file.
4. If prompted, enter the token file password, and click **OK**.
5. If prompted to select a device, click the name of the device where the token will be stored, for example, "Local hard drive (RSA)."
6. Click **OK**.
   A success message is displayed.
7. If prompted to rename your token, do one of the following:
   - To change the token name, click **Change Name**. Enter a name of 1 to 24 characters (for example, "My VPN Token"). Click **OK**.
   - If you do not want to change the name, click **OK** to close the screen.

Change a Token Name

If you assign a nickname to a token in RSA Authentication Manager, the token is imported with that nickname. Otherwise, the application displays the token serial number, for example, 000027874079. When a user imports a token, the application prompts the user to change the token name.

The user can change the token name immediately, dismiss the dialog box and retain the existing name, or change the name later.

Note: If you do not want users to change the nickname that you assigned, you can set the DisableChangeTokenName policy. For more information, see Appendix A, "Customizing the Application."

Procedure

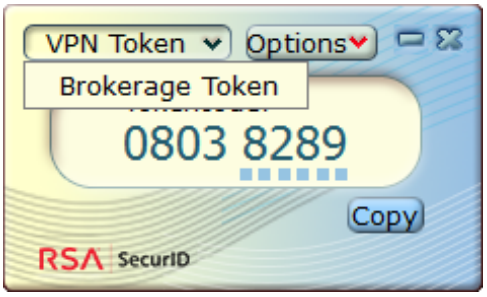
1. Click **Options > Manage Token**, and select **Change Token Name** from the list.
2. In the **Change Name** field, type the new name.
   The token name can contain from 1 to 24 characters and must be unique.
3. Click **OK**.
4. If prompted, enter the device password.
5. Click **OK**.

Select a Token

The application displays the name of the active token, which is either the token that a user is currently using to obtain tokencodes or the last token imported to the application. A user who has more than one token can select a different token, if required.

Procedure

Click the down arrow to the right of the active token name and select a different token. The selected token becomes the active token.



Device Passwords

Users can set a device password to protect all tokens stored on the local hard drive. The device password can contain from 1 to 20 characters. Setting a device password helps ensure that only the user for whom the tokens are intended can access the tokens. The following figure shows the Change Device Password screen.

Once a device password is set, the application prompts for the device password the first time that a user performs a protected operation with a token. For example, the user must enter the device password after entering a PIN, renaming a token, or when attempting to delete a token. The user is prompted for the device password only once per session.

Set a Device Password

Use the following instructions to set a device password for the first time.

Procedure

1. Click **Options > Token Storage Devices**, and click **Change Device Password**.
2. In the **New Password** field, enter a password.
3. In the **Confirm Password** field, reenter the password, and click **OK**.

Change a Device Password

Use the following instructions to change an existing device password.

Procedure

1. Click **Options > Token Storage Devices**, and click **Change Device Password**.
2. In the **Current Password** field, enter the existing password.
3. In the **New Password** field, enter a new password.
4. In the **Confirm Password** field, reenter the new password, and click **OK**.

Remove a Device Password

Use the following instructions to remove a device password. Keep in mind that this removes the additional protection from the tokens stored on the local hard drive.

Procedure

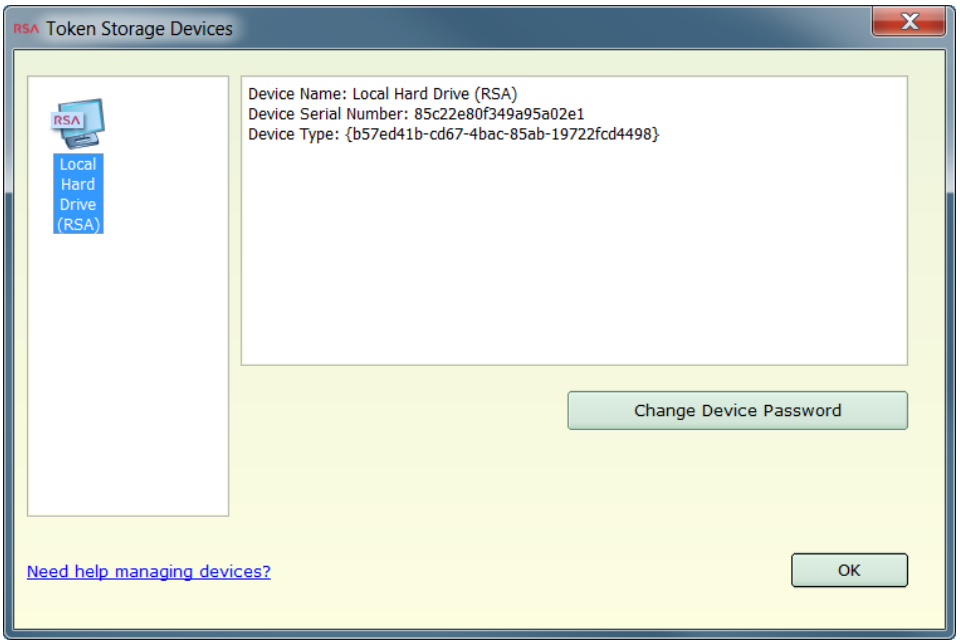
1. Click **Options > Token Storage Devices**, and then **Change Device Password**.
2. In the **Current Password** field, enter your existing password.
3. Leave the **New Password** and **Confirm Password** fields empty, and click **OK**.

Reset the Device (Local Hard Drive)

If a user forgets the device password, the user must reset the device. Resetting the device causes the existing tokens to be deleted. After resetting the device, the user must request new tokens.

Procedure:

1. Click **Options > Token Storage Devices**.
2. In the left pane of the Token Storage Devices screen, click **Local Hard Drive (RSA)**.



3. Click **Change Device Password**.

4. In the **Forgot your password?** section, click **Reset Device**.

The following warning is displayed:

```
Warning: By proceeding, all tokens on the selected device
will be deleted and the device password will be reset.
```

5. Click **OK**.

   The following message is displayed:

```
Successfully deleted tokens and removed password.
```

6. Click **OK**.

Device Passwords for Third-Party Plug-Ins

Depending on your implementation, users can import tokens to a supported third-party device, for example, a TPM or biometric device. If the device supports passwords, the user can set a device password or enter other credentials.

Procedure:

1. Click **Options > Token Storage Devices**.
2. Select the device on which your tokens are stored.

   If the device supports passwords, the **Change Device Password** button is displayed.
3. Click **Change Device Password**, and follow the instructions in the third-party plug-in.

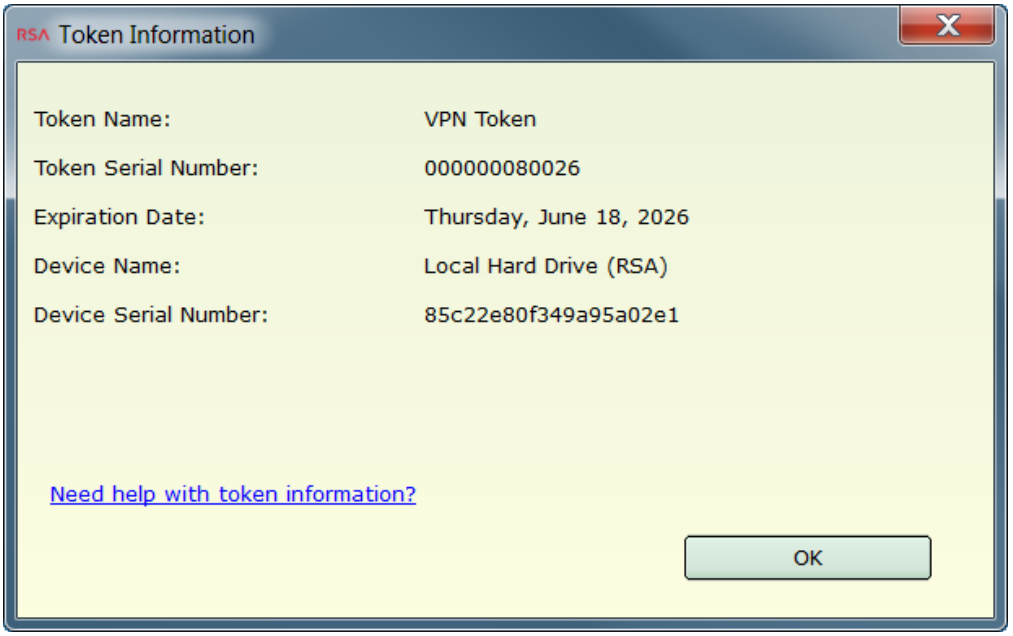
View Token Information

Users can view information about the active token.

Procedure:

Click **Options > Manage Token**, and select **Token Information**.

The Token Information dialog box opens.



The following table lists the token information that is displayed.

Field	Description
Token Name	The user-friendly name of the token, if one has been assigned. For example, "VPN Token."
Token Serial Number	The serial number that identifies the token to Authentication Manager.
Expiration Date	The date when the installed token will expire. Software tokens expire on the expiration date at 00:00:01 GMT.
Device Name	The device on which the token is stored. This can be the local hard drive, a supported biometric device, a supported TPM, or another supported device plug-in. The default device is the local hard drive of the computer, which is labeled Local Hard Drive (RSA).
Device Serial Number	The serial number of the device on which the token is stored.

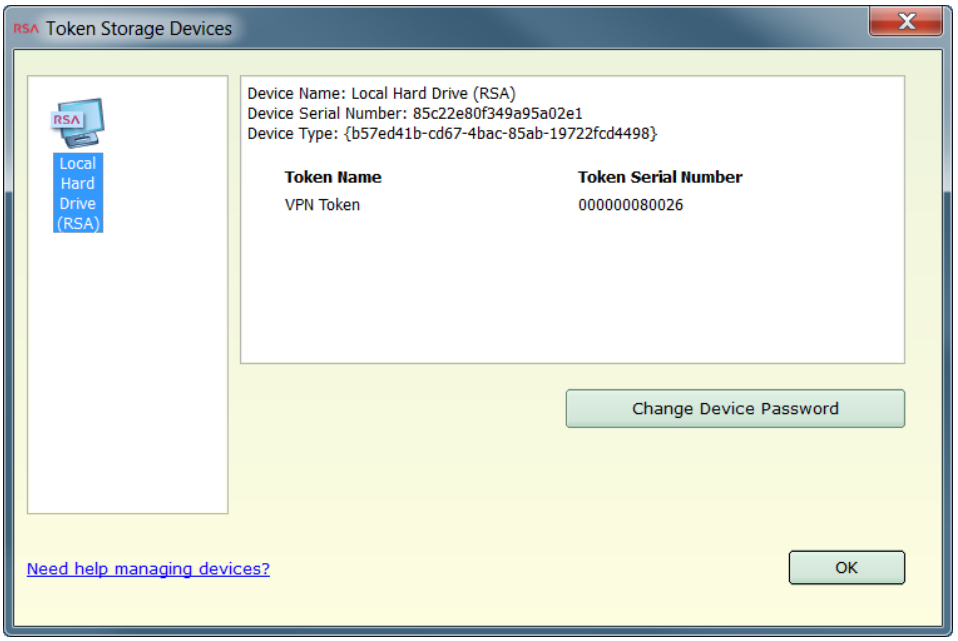
View Token Storage Device Information

Users can view information about the device on which they have stored their tokens.

Procedure

Click **Options > Manage Token**, and select **Token Storage Devices**.

The Token Storage Devices dialog box opens.



The following table lists the storage device information that is displayed.

Field	Description
Device Name	The name of the storage device on which the token is stored. This can be the local hard drive, a supported biometric device, a supported Trusted Platform Module (TPM), or another supported device plug-in. The default device is the local hard drive of the computer, which is labeled Local Hard Drive (RSA).
Device Serial Number	The serial number of the token storage device.
Device Type	A globally unique identifier (GUID) that identifies the specific type of device. Each type of storage device has a unique GUID.
Token Name	The user-friendly name of the token, if it exists. Otherwise, the column displays the token's serial number.
Token Serial Number	The serial number of the token.

Delete a Token

A user does not need to delete a token unless it has expired or the user is instructed to do so by the administrator. If a user deletes the last remaining token, the application prompts the user to import a new token.

When deleting tokens from a password-protected database, the user is prompted for the password if the user has not entered it previously during the session. If the user has forgotten the password, the user must delete all of the tokens and contact the administrator to request replacement tokens. For more information, see "Reset the Device (Local Hard Drive)" on page 43.

Note: You can set the DisableDeleteToken policy to prevent users from deleting tokens. For more information, see Appendix A, "Customizing the Application."

Procedure

1. Click **Options > Manage Token**, and select **Delete Token** from the drop-down list.

   You are prompted to confirm that you want to delete the token.

2. Click **Yes**.

   If prompted, enter the device password.

3. Click **OK**.

Obtaining the Next Code

Under some conditions, an application that is protected by RSA SecurID may prompt the user to enter a code to provide additional verification. The user can obtain the code from the SecurID desktop application.

The next passcode is required if the user has a PINPad-style software token. A PINPad-style software token requires the user to enter his or her SecurID PIN into the SecurID desktop application to generate a one-time password (OTP), or passcode.

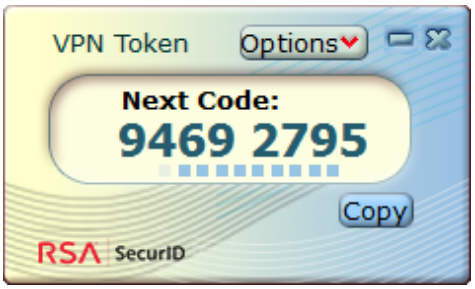
The next tokencode is required if the user has a fob-style software token. The fob-style software token is similar to an RSA SecurID hardware fob, such as the SID700. The software token displays a tokencode.

Enter the Next Code

Use the following procedure to obtain and enter the next passcode or tokencode.

Procedure

1. Click **Options**, and click **Next Code**.
   The next code is displayed.



2. Click the **Copy** button beneath the code display.
3. Paste the code into the required field in the requesting application.

Disable Next Code Mode

After a user submits the next code, the desktop application remains in Next Code mode until the user closes the application, selects a different token, or disables Next Code mode.

Procedure

Click **Options**, and click **Next Code**.

4 Troubleshooting

The following tables describes possible issues that might occur with RSA SecurID Software Token 5.0.2 for Windows (the SecurID desktop application), their possible causes, and corresponding solutions.

Issue	Description
Token import failed.	The cause is likely to be one of the following. In most cases the user receives an error message indicating the reason for the failure and the action to take. **Failure when importing a token from a file** • The user specified the wrong file path and clicked OK, or did not specify a file path and clicked OK. • If the user is attempting to import a token to the RSA token database on the local hard drive, verify that the user has Write permission to the directory where the SecurID desktop application is installed. If not, grant Write permission to the directory. **Failure when downloading a token from the web** • The user typed the URL incorrectly or did not enter the URL. • The user entered a URL that does not start with http:// or https://. • The user entered a blank or invalid activation code. For example, the user omitted or mistyped characters. • The web service cannot access the Internet resource. **Other Possible Causes** • The user provided an incorrect device serial number for binding the token, or the administrator bound the token to an incorrect value. • The user tried to import a token that had already been imported. • The user already imported the maximum number of tokens that the enterprise allows. • The user entered an incorrect token file password. If the user forgot the password, communicate the password again. • The token is not intended to be used on the selected device. • The token is invalid.
User cannot be authenticated by RSA Authentication Manager.	• Verify that the time, date, and time zone settings on the user's computer are accurate. • Check the Authentication Manager logs to determine whether the user's token has been disabled because of failed logon attempts. If the token is not disabled (or expired), ask the user for the tokencode being displayed and resynchronize the token. • The user may have entered an incorrect PIN. Instruct the user to enter the PIN again and retry the authentication.

Issue	Description
User cannot authenticate at a web site, even after allowing an ActiveX control	Verify that the user should have access to the web site. An administrator can configure a token to list up to three secure web sites that a user can access. If this restriction is not configured, then a user can attempt to authenticate with the token at any web site that is protected by your RSA Authentication Manager deployment. A user who attempts to access a restricted site receives an authentication denied message. The authentication request does not reach RSA Authentication Manager for the restricted site. If a user should have access, you can do the following: • Verify that the token record specifies the correct URL. • Check the Windows hosts file on the user's machine, for example, **C:\Windows\System32\drivers\etc**, and verify that it specifies the correct IP address and host name for the web site.
Windows Vista user receives a critical error after installing and trying to open the SecurID desktop application	The wrong root certificate can prevent the application from running. Windows Vista automatically distributes the correct root certificates to users who have Internet access. For information on how to help Windows Vista users who can not connect to Microsoft Update, see **http://support.microsoft.com/kb/931125**.

A Customizing the Application

Use the information in this appendix to customize RSA SecurID Software Token 5.0.2 for Windows (the RSA SecurID Software Token 5.0.2 for Windows).

Customization Policies

You can set customization policies to change default behaviors of the application. RSA recommends that you set any customization policies before you deploy the application to users.

Policies for RSA SecurID Software Token for Windows

Note the following when setting policies for RSA SecurID Software Token 5.0.2 for Windows:

- The value for TokenRenewalURL must be a complete URL that contains the protocol identifier "http" or "https."
- For Boolean policies, 0 (zero) is interpreted as "false," and 1 (one) or any other nonzero value is interpreted as "true."

Registry Location: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RSA\Software Token

Name	Type	Values	Description
ActivationCode	DWORD	0x00000000 (default) 0x00000001	Specifies that the user SID should be used as the CT-KIP activation code. To auto-import a token, you must set ActivationCode to 1, and you must also set a URL link for CtkipUrl.
CtkipUrl	REG_SZ	URL link Empty by default.	Prefills the **Enter URL** field in the application so that the user does not have to enter the URL when manually importing a token provisioned using dynamic seed provisioning (CT-KIP). To auto-import a token, you must set both CtkipUrl and ActivationCode.
DisableChangeTokenName	DWORD	0x00000000 (default) 0x00000001	Prevents users from changing a token nickname assigned in Authentication Manager.
DisableDeleteToken	DWORD	0x00000000 (default) 0x00000001	Prevents users from deleting their tokens. Removes the Delete Token option from the Options menu.

Registry Location: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RSA\Software Token

Name	Type	Values	Description
DisableSetDevicePassword	DWORD	0x00000000 (default) 0x00000001	Prevents users from setting a device password on tokens stored on the local hard drive. Removes the Change Device Password option from the Token Storage Devices screen.
OnlyOneToken	DWORD	0x00000000 (default) 0x00000001	Prevents users from having more than one token.
TokenExpirationNotification	DWORD	0x0000001e (default) Maximum of 0x0000003c (60) or 0x000000000	Changes the number of days before the application displays a notification informing the user that a token is nearing its expiration date. If you do not set this policy, the notification is displayed 30 days before the token expires. If used with TokenRenewalURL, adds a link in the notification to a URL where the user can request a replacement token.
TokenRenewalURL	REG_SZ	URL link. Default is empty string.	Used with TokenExpirationNotification. Displays a URL link in the Token Expiration Notification dialog box. For example, this could be the URL of the RSA Credential Manager portal where the user can request a replacement token.
ValidDevices	REG_MULTI_SZ	Comma-separated string list of valid device GUIDs. Default is empty string.	Specifies a whitelist of devices to which tokens can be imported.

Policy Details

The following sections provide additional details about the customization policies.

ActivationCode

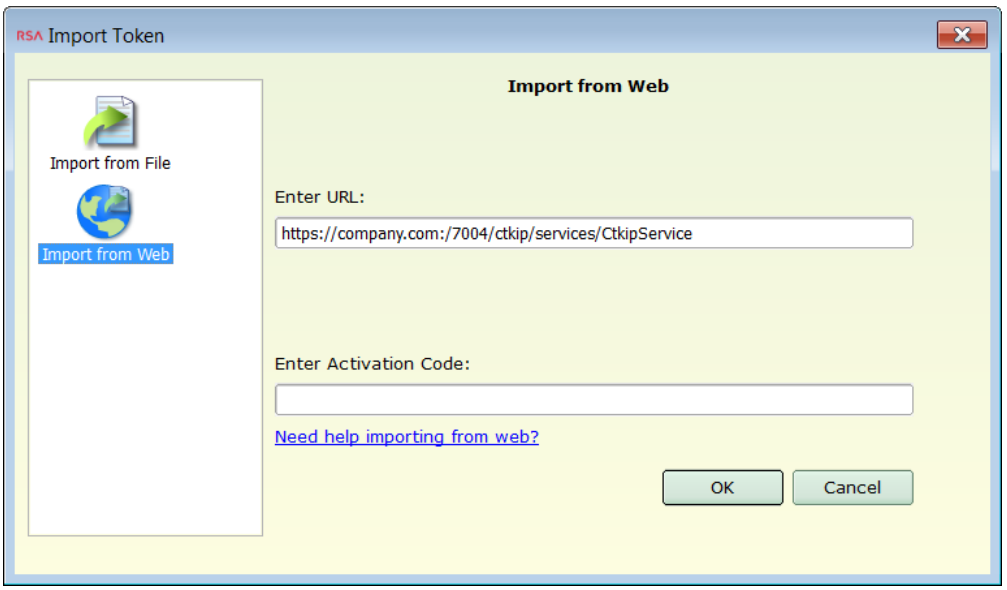
The ActivationCode policy allows you to import or replace tokens using dynamic seed provisioning (CT-KIP) without requiring the user to manually enter an activation code. Before setting this policy, you must bind the user's token to the user SID in RSA Authentication Manager 8.*x*, as described in the *RSA SecurID Software Token 5.0 for Windows Provisioning Guide*.

You can automate the provisioning of one token to a user using CT-KIP by setting both the ActivationCode and the CtkipUrl policies. Set ActivationCode to 1, and set CtkipUrl to the URL of your CT-KIP server. The first time that the user starts the desktop application, the token is automatically imported, as long as one of the following conditions is met:

- The user does not already have a token.
- All of the tokens in the user's token database have expired.

CtkipUrl

By default, when importing a token using CT-KIP, the user must enter the URL of the CT-KIP server and must enter the activation code on the Import from Web screen. If you do not want the user to have to enter the URL, set the CtkipUrl policy. This prefills the **Enter URL** field, and the user then needs to enter only the activation code.



On Windows desktops, you can automate the provisioning of one token to a user by setting both the CtkipUrl policy and the ActivationCode policy, as described in the previous section.

DisableChangeTokenName

By default, users can change the nicknames of their tokens. If you set nicknames on users' tokens when you issue them in Authentication Manager, and you do not want users to change the nicknames, set the DisableChangeTokenName policy. This removes the Change Name option from application user interface.

DisableDeleteToken

By default, all users can delete their tokens. However, users normally do not need to delete a token unless the token has expired or you instruct them to delete a token. If you do not want users to be able to delete tokens, set the DisableDeleteToken policy. This removes the Delete Token option from the application user interface.

DisableSetDevicePassword

By default, users can set a device password to protect all tokens stored in the token database on the local hard drive. This provides added protection for the tokens. If a user forgets the device password, the user must reset the device, which deletes all of the tokens in the database. The user must then request replacement tokens, which can increase administrative overhead. If you want to prevent users from setting a device password, set the DisableSetDevicePassword policy. This removes the Change Device Password option from the Token Storage Devices screen.

OnlyOneToken

By default, users can have multiple tokens. If your implementation does not require users to have multiple tokens, you can use the OnlyOneToken policy to allow each user to import only one token. If you set this policy and a user attempts to import a second token, the application informs the user that only one taken can be installed. If the user chooses to import the new token, the application overwrites the existing token. If the user has stored more than one token when you enable the policy, importing a new token overwrites all of the user's tokens.

TokenExpirationNotification

The TokenExpirationNotification policy allows you to change the number of days before the application displays a notification informing the user that a token is nearing its expiration date. By default, the user is notified 30 days before token expiration. You can set the policy to display the notification 1 to 60 days before token expiration.

If the active token has already expired, the notification is not displayed. Instead, the Tokencode or Passcode screen displays "Token Expired."

If you set the TokenRenewalURL policy with the TokenExpirationNotification policy, the notification dialog box displays a link that the user can click to request a replacement token. This opens a web URL, for example, the RSA Credential Manager portal, where the user can request a replacement token.

TokenRenewalURL

The TokenRenewalURL policy is used with the TokenExpirationNotification policy. To set the TokenRenewalURL policy, you enter a URL link that will be displayed in the token expiration notification. The user can click the link to open a URL, such as the RSA Credential Manager portal, where the user can request a replacement token. If you do not set this policy, the token expiration notification does not display a URL link, and the user must contact the administrator to request a replacement token.

ValidDevices

The SecurID desktop application supports storing tokens in the RSA token database on the local hard drive or on a supported TPM, biometric device, or another supported device plug-in.

To control which devices users can access, you can create a device whitelist (a list of supported devices). Using a whitelist ensures that users can import, view, change the name of, and delete only those tokens that are stored in the devices specified in the whitelist. If a user connects a device that is not in the whitelist, the device is not displayed in the Token Storage Devices screen.

If you do not use a device whitelist, the user can import tokens to any device that is recognized by the system and allowed by the token's device binding settings.

Create a Device Whitelist

Use the ValidDevices policy to create a device whitelist. The values must be comma-separated Globally Unique Identifiers (GUIDs), as shown in the following example. Angle brackets are not required.

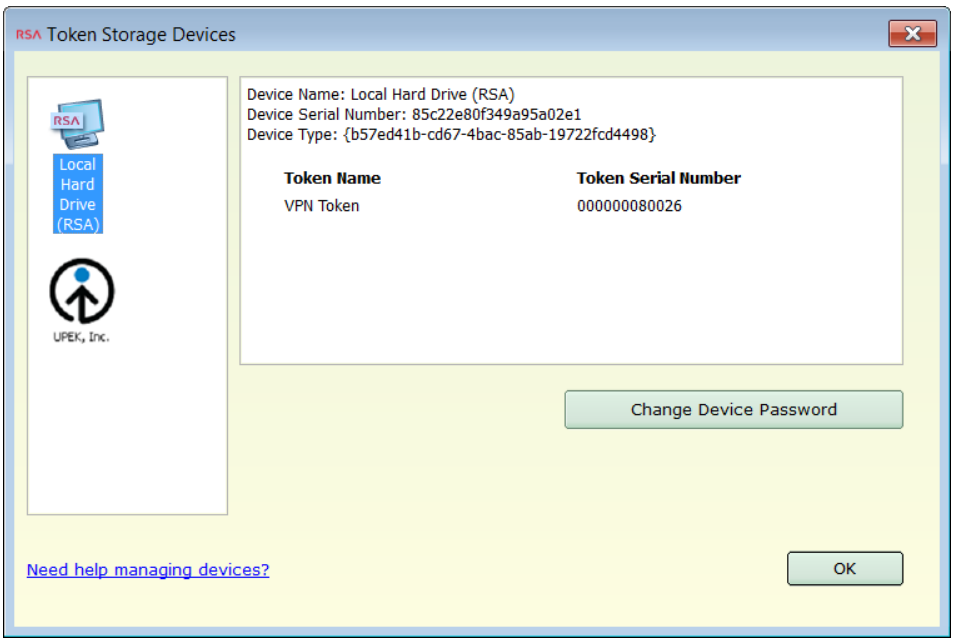
```
8f94b026-d362-4554-ac52-3b01fa33b6f,7484g337...
```

Obtain the device GUIDs from the application.

Procedure

1. Click **Options > Token Storage Devices**.
2. In the left pane, click the device icon for the first device that you want to include in the whitelist.

   For example, the following figure shows two installed devices. The Local Hard Drive (RSA) device is selected, and the associated GUID is displayed in the **Device Type** field.



3. Click the device icon for the next device that you want to add to the whitelist.
4. Click **OK**.

Customizing RSA SecurID Software Token for Windows

You customize RSA SecurID Software Token 5.0.2 for Windows using Windows Group Policy. Setting Group Policy for the SecurID desktop application adds registry keys under **HKEY_LOCAL_MACHINE\Software\Policies\RSA\Software Token**.

RSA provides an administrative template **(RSASecurIDToken.adm)** in the installation kit (**RSASecurIDToken502.zip**). The template describes where the registry-based policy settings are stored in the Windows registry. SecurID desktop application policies are applied on a per computer (per-machine) basis. That is, the policies that you set apply to all users of a particular computer rather than to individual users.

You create Group Policy settings on a domain controller using the Microsoft Management Console (MMC). The groups that you want the policies to affect must exist in Active Directory. For more information, go to **www.microsoft.com** and search on "Group Policy."

Add the RSA Administrative Template

Before you configure Group Policy settings for the desktop application, you must add the RSA administrative template to the Microsoft Management Console (MMC).

Procedure

1. From the Start menu, click **Run**.
2. In the Open dialog box, type **gpedit.msc**, and click **OK** to start the Microsoft Management Console (MMC).
3. Under **Computer Configuration**, click **Administrative Templates**.
4. In the Console menu bar, click **Action > Add/Remove Templates**.
5. Click **Add**, and browse to the location of the **RSASecurIDToken.adm** file.
6. Click the **RSASecurIDToken.adm** file, and click **Open**.
   The template is added to the Add/Remove templates dialog box.
7. Click **Close**.

Configure Group Policy Settings

You can configure Group Policy settings for the desktop application using the RSA administrative template.

Procedure

1. From the Start menu, click **Run**.
2. In the Open dialog box, type **gpedit.msc**, and click **OK** to start the Microsoft Management Console (MMC).
3. Navigate to the RSA administrative template by clicking **Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Software Settings > RSA SecurID Token**.

Updating the Token Storage Device Serial Number

When you install RSA SecurID Software Token 5.0.2 for Windows, 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.

The registry entries are in the following location:

HKEY_CURRENT_USER\SOFTWARE\RSA\Software Token\Desktop \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. For instructions, see "View Token Information" on page 45 and "View Token Storage Device Information" on page 46. 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*.

B Logging

This appendix describes logging in RSA SecurID Software Token 5.0.2 for Windows (the SecurID desktop application), including how to control the amount of information logged, where to find log output files, the log message format, and sample log messages.

Setting the Logging Level

You can control the amount of information logged by the SecurID desktop application by setting a registry key in the following locations:

- For 32-bit and 64-bit machines:

  HKEY_LOCAL_MACHINE\SOFTWARE\RSA\Software Token\Library\LogLevel

- For the 32-bit version of the desktop application installed on 64-bit machines:

  HKEY_LOCAL_MACHINE\Software\Wow6432Node\RSA\Software Token\Library\LogLevel

The following table lists the possible string values.

Note: If you specify any other string value, the logger uses the default value (INFO).

Value	Meaning
DEBUG	Logs messages that are useful for debugging purposes.
INFO	Logs important application information, in addition to errors. (Default)
ERROR	Logs only application errors.
OFF	No information is logged.

Location of Log Output Files

The logger is configured programmatically to output a rolling file named **RSA_Software_Token_Log.txt** in ***Drive:*\ProgramData\RSA**. The maximum size of the log file is set to 1 MB. When this size limit is reached, a backup log file named *filename*.1 (for example, "RSA_Software_token_log.txt.1") is created, and messages are once again logged to the original log file. When the log file again reaches its size limit, the backup log file is replaced.

Log Message Format

The format of the output log file is as follows:

```
[time stamp] [severity level] [thread name] [logging
component] - [message]
```

Format Component	Meaning
Time stamp	The date and time that the message was logged. The date and time are displayed in 24-hour format. The time stamp format is dd mmm yyyy hh::mm::ss, for example, 21 Feb 2017 09:14:21.
Severity level	Indicates whether the message has been logged as an error that occurred in the application (ERROR), as an informational message (INFO), or as a message to aid in debugging (DEBUG).
Thread name	Identifies the thread that was responsible for logging the message.
Logging component	The SecurID desktop application specifies numerous components that have the capability of logging messages. These components are designated by their architectural significance within the application, and include the following: **Desktop Client.** Represents a log message generated from the main application, but not from within the stauto32 library or the Local Hard Drive (RSA) Plug-In. **Software Token Library.** Represents a log message generated from within the stauto32 library. The stauto32 library integrates third-party applications, such as VPN clients, and facilitates seamless integration with RSA SecurID. **Local Hard Drive (RSA) Plug-in.** Represents a log message generated from within the local hard drive plug-in. The user's tokens are stored on the local hard drive (unless you use a third-party plug-in, such as a TPM). **Software Token Migrator.** Represents a log message generated during migration of tokens from a previous version of the application. Migration occurs when users upgrade to a newer version of the application.
Message	The logged message.

Sample Log Messages

This section contains examples and explanations of messages logged by the SecurID desktop application.

05 Sep 2016 10:14:21 ERROR 0x0000c754 RSA Plugin - 217 RSA database corruption detected

Explanation (this is not logged):

Severity Level = ERROR

Thread Name = 0x0000c754

Logging Component = Local Hard Drive Plug-in

Message = 217 RSA database corruption detected

27 Jul 2016 13:23:42 ERROR 0x00005733 Software Token Library - 57 General Error

Explanation:

Severity Level = ERROR

Thread Name = 0x00005733

Logging Component = Software Token Library

Message = 57 General Error

29 May 2016 02:30:54 ERROR 0x0000a537 Software Token Migrator - 217 Old password incorrect

Explanation:

Severity Level = ERROR

Thread Name = 0x0000a537

Logging Component = Software Token Migrator

Message = 217 Error: Old password incorrect

25 Aug 2016 16:16:05 INFO 0x0000161c Software Token Client - Application Settings:

<key>\HKEY_LOCAL_MACHINE\Software\RSA\Software Token\Desktop/InstallDir

<value>C:\p4\dev\sw-authenticators\src\softwaretokenlib\debug

Explanation:

Severity Level = INFO

Thread Name = 0x0000161c

Logging Component = Software Token Client

Message = Application Settings:
<key>\HKEY_LOCAL_MACHINE\Software\RSA\Software Token\Desktop/InstallDir

<value>C:\p4\dev\sw-authenticators\src\softwaretokenlib\debug