# RSA SecurID Software Token 3.0
## *for Windows® Workstations*
## User's Guide

**Contact Information**

See our Web sites for regional Customer Support telephone and fax numbers.


RSA Security Inc.
**www.rsasecurity.com**

RSA Security Ireland Limited
**www.rsasecurity.ie**


## Trademarks



## License agreement



## 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 exporting this product.

## Distribution

Limit distribution of this document to trusted personnel.



First printing: June 2002

# Contents

# About RSA SecurID Software Token

You have been given the RSA SecurID Software Token 3.0 for Windows Workstations application to use to access a network or standalone resource protected by an RSA ACE/Server. This application provides a software-based security token that resides on your hard drive or smart card. With the token, you can use the application to gain access to protected company resources.

To access a protected resource, you must "authenticate" to the RSA ACE/Server. Authentication is the process by which you prove your identity to the system. To authenticate, you select a software token and enter a PIN, a personal identification number known only to you. The application uses the PIN and the current 8-digit random number (called the tokencode) generated by the Software Token application to calculate a PASSCODE that it sends to the RSA ACE/Server. When the Server verifies that the PASSCODE is valid, you are granted access to the protected resource. During these transactions, your PIN is never exposed. The combination of PIN and tokencode provides secure user authentication and access control.

## Software Tokens

A software token is an encrypted file that your administrator assigns to you. This file can reside on your hard drive or your smart card. RSA SecurID Software Token uses the token to generate a tokencode that the RSA ACE/Server can recognize. The Software Token application operates with multiple tokens. This makes it possible for more than one organization to assign you a token.

You need a software token to authenticate so that you can access a protected resource. When logging in to an organization, you select the appropriate token from the Software Token application and use it to log in.

## Preparing to Use the Application

Before you can use the RSA SecurID Software Token application to authenticate, you need to perform a few setup tasks.

| | |
|---|---|
| • Install the software | "Installation Procedure" on page 6 |
| • Install a software token | "Installing Software Tokens Manually" on page 7 |
| • (For smart card users) Set up smart card access | "Setting Up Smart Card Communication" on page 24 |
| • (For smart card users) Transfer the software token to your smart card | "To transfer a software token to a smart card:" on page 27 |
| • (Optional) Set a passphrase for the software token or the smart card | "To set or change a token passphrase:" on page 20 |
| • Create or obtain a PIN | "Obtaining a PIN" on page 21 |

# Installing the Software

Your RSA ACE/Server administrator has created an installation package for installing the Software Token application and software tokens. The types of installations are as follows:

- The administrator can install the application and software tokens on your computer remotely. All you have to do is reboot your system when the installation is complete.
- The administrator can install the application on your computer remotely and supply you with a separate software token distribution file. You will then install the software tokens manually. See "Installing Software Tokens Manually" on page 7.
- The administrator can provide an installation setup file in a network directory, on a Web site, or in an e-mail attachment. You will then use the steps in "Installation Procedure" on page 6.

## Upgrades

If RSA SecurID Software Token 2.5 or 2.5.1 is currently installed on your computer, the installation program will automatically upgrade your system to Software Token 3.0. If you have a version of the application earlier than 2.5, contact your administrator for assistance in upgrading to 3.0.

When you upgrade from Software Token 2.5 or 2.5.1, smart card information entered in the Smart Card Reader Selection utility for 2.5 or 2.5.1 is not carried over to Software Token 3.0. You will need to re-define your smart card communication selections. See "Setting Up Smart Card Communication" on page 24.

## Installation Procedure

**Note:** You must have administrative privileges on your computer before you can install the application.

**To install the RSA SecurID Software Token application:**

1. Navigate to the location where the RSA SecurID Software Token **setup.exe** program resides.
2. Double-click **setup.exe**.
3. Follow the instructions on the installation screen.
   The RSA SecurID Software Token program is installed, and "RSA SecurID Software Token" appears in the Start menu.

## Installing Software Tokens Manually

The RSA SecurID Software Token application allows any number of software tokens on your hard drive, up to 5 on an RSA SecurID 3100 Smart Card, and up to 10 on other supported smart cards. If you need multiple tokens, your administrator will supply them. Software tokens are contained in a distribution file with the extension **.sdtid**.

The administrator can set a distribution password for each token in the distribution file to ensure that only the intended user can install the tokens. If the tokens have distribution passwords, you must enter the correct password for each token before you can install that token. Be sure to memorize the passwords. If you forget the distribution passwords, the administrator will have to re-issue the token distribution file.

**Note:** You need write permission to the directory into which the Software Token application is installed before you can install software tokens. Your administrator can either grant write permission or install the tokens for you.

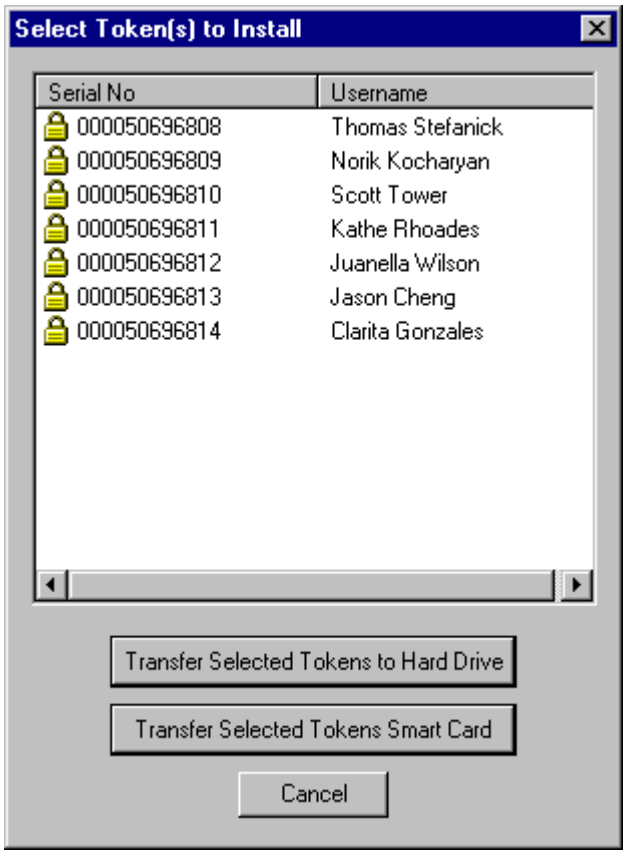
**Before you begin:**

- Be sure the administrator has given you the distribution passwords, if any, assigned to the tokens in the distribution file.
- If you are using a smart card, make sure your smart card reader is installed and working and that you have inserted your smart card into the reader.

**To install software tokens manually:**

1. Do one of the following:
   - In the Software Token application, click **File > Import Tokens**, and navigate to the location of the SDTID file.

- In Windows Explorer, locate and double-click the SDTID file.




**Note:** Transfer Selected Tokens to Smart Card is displayed only if you have set up smart card access and a card is in the reader. See "Setting Up Smart Card Communication" on page 24.

2. In the Select Token(s) to Install screen, highlight the serial numbers of the software tokens you want to install.
3. Click the appropriate **Transfer Selected Tokens** option (either to the hard drive or to your smart card).
4. If the tokens have distribution passwords, enter each password when prompted, clicking **OK** after each one.
5. Click **File > Select Token** to view the tokens that have been installed.

**Note:** The title bar of the dialog box always displays the serial number of the currently selected token.

# Using Add-on Programs

The RSA SecurID Software Token product comes with add-on programs: the RSA ACE/Agent Browser Plug-In and the Login Automation program. The RSA ACE/Server administrator will let you know whether to use one of these programs for authentication.

## RSA ACE/Agent Browser Plug-In

The RSA ACE/Agent Browser Plug-In lets you use your software token to access a protected Web site. You must have a Web browser installed. The RSA ACE/Agent Browser Plug-In has been qualified with

- Internet Explorer 5.5 or 6.0
- Netscape Communicator 4.79

**Note:** The Browser Plug-In does not work with Internet Explorer 6.0 on Windows NT.

### Authenticating with the RSA ACE/Agent Browser Plug-In

During your first authentication session, you are prompted for your username and PIN. Thereafter, the Browser Plug-In "remembers" your username, and you are prompted only for a PIN. Once you enter the PIN, a PASSCODE is generated and passed to the RSA ACE/Server. You do not need to run the Software Token application to generate a PASSCODE.

**To authenticate with the Browser Plug-In:**

1. Bring up your Web browser and attempt to access a protected Web site.

In the Choose Token box, select **RSA SecurID Software Token**.


2. Select a software token from the drop-down menu.
3. Enter your username and PIN.

**Note:** If you are using the selected software token for the first time, enter **0000** in the Enter PIN box to signal the login application that your token is in New PIN mode. Enter a new PIN when prompted. Be sure to memorize the PIN. If you forget it, contact your administrator.

## Login Automation

The Login Automation program allows you to dial in to a remote server and authenticate by selecting a software token and typing a PIN. You do not need to run the RSA SecurID Software Token application to generate a PASSCODE.

Before you can use the Login Automation program to authenticate, you must

- Create a Windows Dial-Up Networking (DUN) phone book entry. To set up Dial-Up Networking, see the Help for your Windows operating system or talk with your RSA ACE/Server administrator.
- Set up a connection profile, using the Login Automation program. See "Setting Up a Connection Profile" on page 11.

## How the Login Automation Program Works

The Login Automation program uses script files to send authentication information, notably the RSA SecurID PASSCODE, from the user's computer to a remote RSA ACE/Server host. The program comes with a default script, **rasall.scp**, which is located in the same folder as the RSA SecurID Software Token application. The RSA ACE/Server administrator can edit the default script or create a new script, if necessary.

When you log in with Login Automation, the Login Automation program performs these steps:

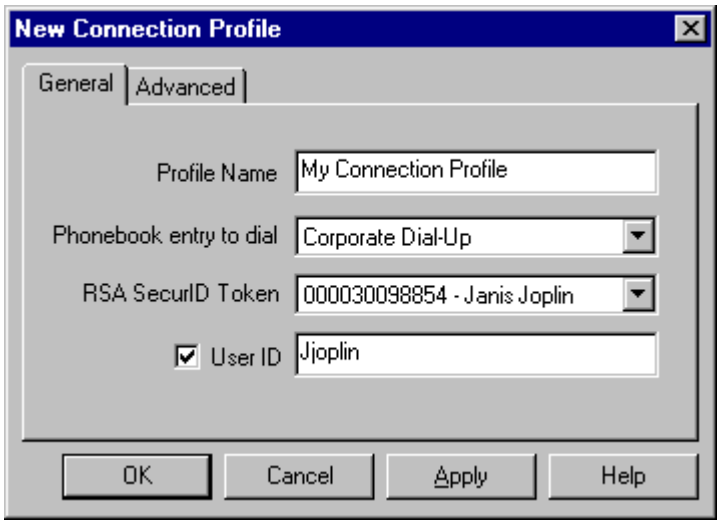
- Saves the original script in a backup file.
- Modifies the original script by adding the current PASSCODE.
- Uses the Windows Remote Access Service API to dial the entry specified in the Login Automation profile. (The script is passed to the API as a parameter.)
- Copies the backup script back into the original script file.

For example, the Login Automation program saves the **rasall.scp** file to **rasall.bak**, executes **rasall.scp**, and copies **rasall.bak** to **rasall.scp**. The changes made during execution are lost.

## Setting Up a Connection Profile

**To set up a connection profile:**

1. Open the Login Automation program.
2. Click **Profile >>> > New**.




3. Click the **General** tab, and enter the following information:
   - **Profile Name**. Any name you want to use.
   - **Phonebook entry to dial**. Contains the DUN entry. The administrator will have given you the name of this entry.

- **RSA SecurID Token**. The software token to be used for login. Select the token you want to use from the drop-down menu.
- **User ID**. Your login username.

4. Click **OK**.

## Editing, Deleting, or Testing a Connection Profile

You can change or delete an existing connection profile. You can also test a connection profile to be sure that the PASSCODE has been added successfully to the script.

**To edit an existing connection profile:**

1. Start the Login Automation program.
2. On the RSA SecurID Login screen, select the connection profile you want to edit.
3. Click **Profile >>> > Edit**.
4. On the Editing Profile screen, make the changes in the connection profile.
5. Click **OK**.

**To delete a connection profile:**

1. Start the Login Automation program.
2. On the RSA SecurID Login screen, select the connection profile you want to delete.
3. Click **Profile >>> > Delete**.
   The message **Are you sure you want to delete profile <*profile_name*>** appears.
4. Click **Yes** to delete the selected connection profile.

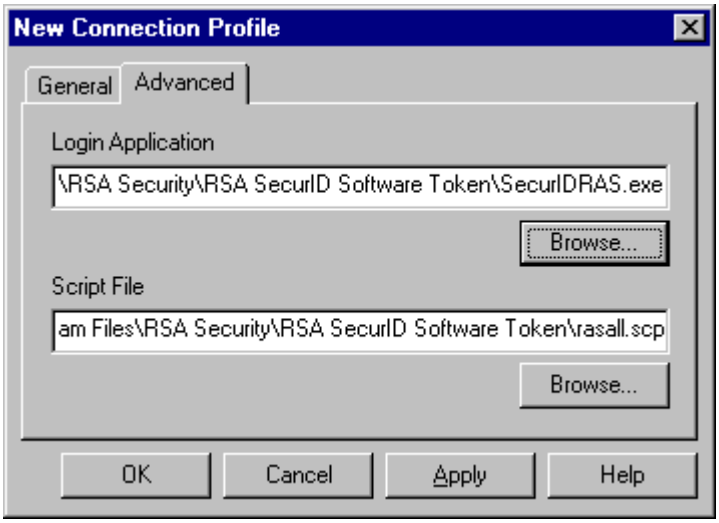
**To test a script:**

1. Start the Login Automation program.
2. On the RSA SecurID Login screen, select the connection profile you want to test.
3. Enter your PIN.
4. Click **Profile >>> > Test**.
   The application adds the PASSCODE to the script and launches the script in Notepad so that you can view it. If changes are required, contact your administrator.

## Selecting an Alternative Script File

If your RSA ACE/Server administrator edited the Login Automation script file or created a new script, you can use the **Advanced** tab on the New Profile screen to apply the new script to your connection profile. The administrator will tell you the location of the new script.

**Note:** Do not alter the Advanced settings unless instructed by your administrator.




**To apply a non-default script:**

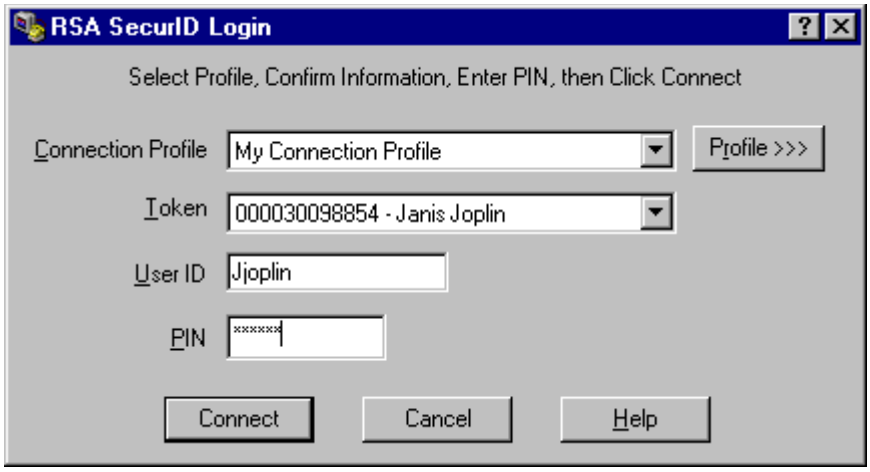
1. Open the Login Automation program and click **Profile >>> > Edit**.
2. Click the **Advanced** tab.
3. Click **Browse** to locate the script file.
4. Click **Apply**.

## Authenticating With Login Automation

**To authenticate with login automation:**

**Note:** RSA Security strongly advises that you use your Dial-Up Networking program with the Software Token application before you try to authenticate with Login Automation. This will ensure that your dial-up connection is configured and working properly. You should also dial in manually if you are having a problem with Login Automation. See "Authenticating with Manual Dial-Up Networking"on page 30.

1. Open the Login Automation tool.



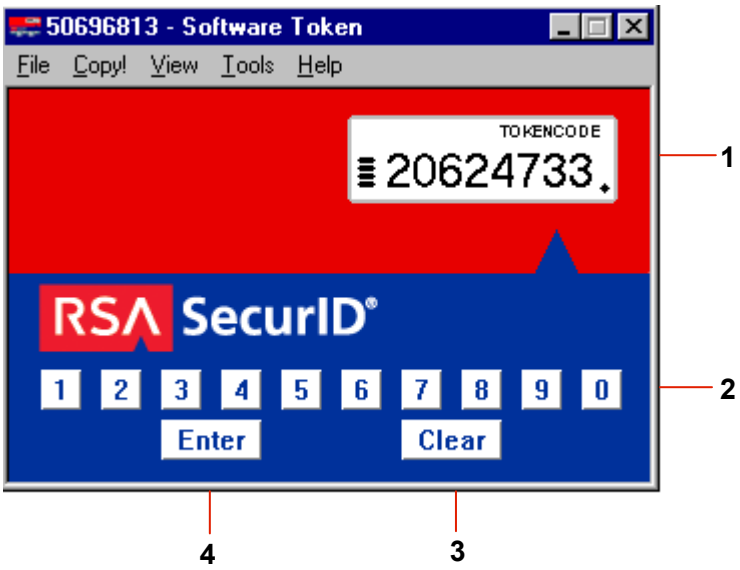

2. Enter a PIN to use for Login Automation. Be sure to memorize the PIN. You will need to enter the PIN every time you use Login Automation.
3. Click **Connect**.
   A confirmation message such as **PASSCODE ACCEPTED**, appears.

# Understanding the Application User Interface

The graphical user interface for the RSA SecurID Software Token for Windows Workstations application is designed to emulate the look of the RSA SecurID hardware tokens (physical tokens) sold by RSA Security. The user interface has two views, Token View and Advanced View. Click the **View** menu to select the view you want. The view you select is a matter of preference. The menu bar is the same for each view, and operations within the application can be done from either view. When you select a view, it becomes the default.

## Token View

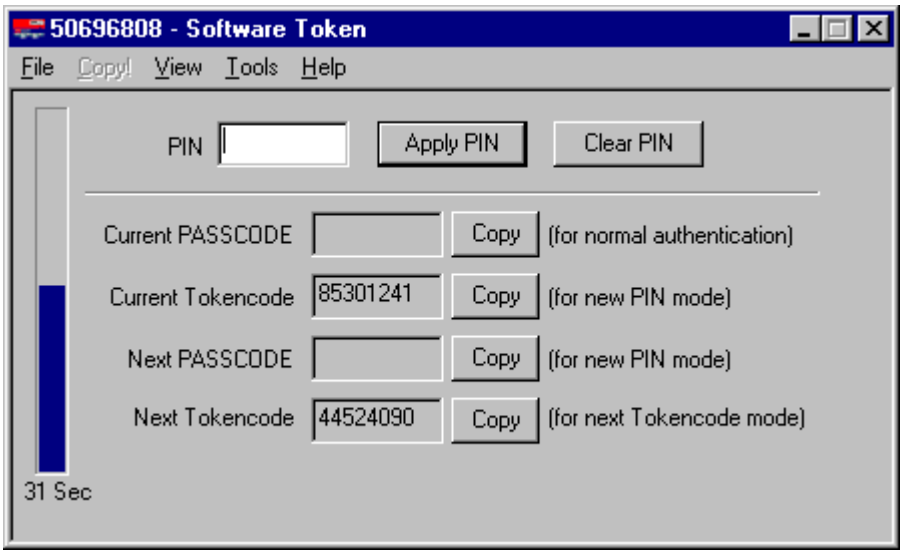
The Token View is shown in the illustration and described in the table that follows.




| | |
|---|---|
| **1** | Display window. Displays current eight-digit tokencode for 60 seconds. Countdown bars on left indicate elapsed time. Each bar = 10 seconds. |
| **2** | Number pad. Used for typing a PIN. |
| **3** | Clear button. Deletes the last digit typed. If you delete all digits, the display is cleared. Press **Clear** once more to return to displaying tokencodes. |
| **4** | Enter button. Confirms PIN entry. As a security measure, the PIN and resulting PASSCODE remain active for a maximum of two minutes. The word PASSCODE appears above the code, indicating that a PASSCODE has been generated. |

## Advanced View

The Advanced View is shown in the illustration and described in the table that follows.




| | |
|---|---|
| **Countdown Bar** | Indicates elapsed time before the next tokencode is displayed. The number of seconds remaining is displayed at the bottom of the bar. |
| **PIN** | Type your PIN and click **Apply PIN** to obtain the current PASSCODE or the next PASSCODE. |
| **Apply PIN** | Confirms PIN entry. The Current PASSCODE and Next PASSCODE are displayed. As a security measure, the PIN and PASSCODEs remain active for a maximum of two minutes. |
| **Clear PIN** | Clears the entire PIN from the PIN box. |
| **Current PASSCODE (Copy)** | Displays the current PASSCODE after you type and apply a PIN. The **Copy** button copies the PASSCODE so that you can paste it into the login application window during normal authentication. |
| **Current Tokencode (Copy)** | Always displays the current tokencode. The **Copy** button copies the tokencode so that you can paste it into the login application window when prompted during authentication in New PIN mode. |

| | |
|---|---|
| **Next PASSCODE (Copy)** | Displays the next PASSCODE when you type and apply a PIN. The **Copy** button copies the PASSCODE so that you can paste it into the login application window when prompted during authentication in New PIN mode. |
| **Next Tokencode (Copy)** | Always displays the next tokencode. The Copy button copies the next tokencode so that you can paste it into the login application window when prompted during authentication in Next Tokencode mode. |

## User Interface Menus

The Token View and the Advanced View have the same menu bar. The menu items are used to select a token, copy the tokencode so that you can paste it into the login window of your application, obtain the next tokencode, set or change a passphrase for your token, manage your smart card, and view the help file

| | |
|---|---|
| **File** | **Select Token** selects the software token you want to use for authenticating.<br>**Show Token Information** provides the serial number of the selected token, the token identifier, and the location of the token (hard drive or smart card).<br>**Import Tokens** allows you to import multiple software tokens in the form of SDTID files into the application.<br>**Show Database Information** displays the location of the software token database on your computer and gives database copy protection status.<br>**Exit** closes the application. You can also exit by clicking the X at the top right of the application. |
| **Copy!**<br>(available only in Token View) | Highlights and copies the tokencode or the PASSCODE. You can also right-click the tokencode or PASSCODE, click **Select All** (to highlight the number), and click **Copy**. Ctrl + C also performs a copy. |
| **View** | Lets you select either the Token View or the Advanced View.<br>**View Next Code** produces the next tokencode. Select this option if you are trying to authenticate and are prompted for the next tokencode. If you have entered a PIN, View Next Code displays the next PASSCODE.<br>**Always on Top** keeps the Software Token user interface on top of other applications that are open on your computer. |

| | |
|---|---|
| **Tools** | **Set Token Passphrase** lets you set a new passphrase for your token or change the current passphrase for the token.<br>**Set Smart Card Passphrase** lets you set a new passphrase for your smart card or change the current passphrase for the smart card.<br>**Transfer Token to Smart Card** transfers the currently displayed software token from your hard drive onto your smart card.<br>**Smart Card Options** lets the Software Token application know whether you are using a smart card, what type of smart card you are using, and how to access it. The default selection is **Not using smart cards**. |
| **Help** | Brings up help on specific screens or the entire help file. |

# Setting Up the Software

This section is for users who will be using the Software Token application to authenticate.

Before you can use the application to authenticate, you need to perform a few setup tasks:

- Verify time settings
- Set a passphrase for your token (recommended)
- Obtain a PIN

## Verifying Time Settings

RSA SecurID Software Token and the RSA ACE/Server rely on Greenwich Mean Time (GMT). The time, date, and time zone settings on your local computer and on the computer running the RSA ACE/Server must always be correct in relation to GMT. If the time settings on your computer drift, they will no longer be synchronized with the time settings on the RSA ACE/Server host, and authentication cannot take place. You are responsible for maintaining these settings on your local computer.

If you travel with your computer and you cross time zones, you do not need to change any time settings. However, if you want these settings to reflect the local time, you must follow the requirements of your operating system when changing them.

### Operating System Requirements

| Operating System | Required Changes |
|---|---|
| Windows 98 | Change the date, time, and time zone settings on your computer all at the same time. |
| Windows NT v 4.0<br>Windows 2000<br>Windows XP | Change only the time zone setting. Time and date settings are then updated automatically. |

**Important:** Failure to observe these guidelines can cause authentication to fail.

To verify or change the date, time, and time zone settings on your local computer, click the time in the lower right part of the Windows desktop.

## Setting or Changing a Token Passphrase

To prevent unauthorized persons from using the RSA SecurID Software Token application on your computer, you have the option of creating a passphrase for the token after you install it. A passphrase is similar to a password except that spaces are permitted in a passphrase. For example, "my secret phrase" is a valid passphrase. A passphrase can contain up to 32 characters.

**Note:** Do not confuse the token passphrase, which protects a token, with the PIN you enter during authentication. Be sure to memorize the passphrase. If you forget it, you will not be able to use that token and will have to contact your RSA ACE/Server administrator.

**To set or change a token passphrase:**

1. Start the Software Token application.
2. Click **File > Select Token**, and select the token for which you want to set a passphrase.
3. Click **Tools > Set Token Passphrase**.


4. Type a new passphrase in the **New Passphrase** box.
5. Re-type the new passphrase in the **Confirm** box, and click **OK**.

**Note:** You can remove a token passphrase by entering your current passphrase and then leaving the **New Passphrase** and **Confirm** boxes blank.

Once you set a token passphrase, you will be prompted to enter it whenever you

- Start the Software Token application (if the last token used was passphrase protected).
- Select a passphrase-protected token and use it for authentication.
- Insert a passphrase-protected smart card into the card reader.

## Obtaining a PIN

A PIN is your secret, memorized personal identification number. Your PIN is used with the current code (tokencode) to generate a numeric code called a PASSCODE. The PASSCODE is read by the RSA ACE/Server, which must authenticate the PASSCODE before you can access the protected resource.

Your RSA ACE/Server administrator may give you a default PIN with the software token, allow you to create your own PIN, or have you obtain a system-generated PIN. If you receive a default PIN and want to change it, ask the administrator to put your software token into New PIN mode. See "Replacing a PIN in New PIN Mode" on page 22.

**Note:** You can create a PIN during your first authentication session.

The requirements for a PIN are

- The PIN must contain between 4 and 8 numerals. The RSA ACE/Server administrator will inform you of any other restrictions.
- The first numeral cannot be a zero (0).

### Creating a PIN for a New Software Token

**To create a PIN for a new software token:**

1. Start the Software Token application in either Token View or Advanced View.
2. Start a login session to access your remote RSA ACE/Agent-protected host.
3. After responding to the login prompt, you are prompted to enter a PASSCODE. Do one of the following:
   - In Token View, click **Copy!** to copy the current tokencode, and paste the tokencode into your login application at the Enter PASSCODE prompt.
   - In Advanced View, click **Copy** next to the Current Tokencode box, and paste the tokencode into your login application at the Enter PASSCODE prompt.

   **Note:** If you are prompted for a PIN rather than a PASSCODE, enter 0000 in the Enter PIN box to signal the host that your token is in New PIN mode.
4. When prompted, type your new PIN in the login application window and press ENTER.

5. When prompted, retype your new PIN in the login application window and press ENTER.
6. Continue the authentication process. For instructions, see the appropriate topic in "Accessing Protected Resources" on page 29.

## Obtaining a System-Generated PIN

**To obtain a system-generated PIN:**

1. Start the Software Token application in either Token View or Advanced View.
2. Start a login session to access your remote RSA ACE/Server-protected host.
3. After responding to the login prompt, you are prompted for a PASSCODE. Do one of the following:
   - In Token View, click **Copy!** to copy the current tokencode, and then paste the tokencode into your login application at the Enter PASSCODE prompt.
   - In Advanced View, click **Copy** next to Current Tokencode, and paste the tokencode into your login application at the Enter PASSCODE prompt.
4. When asked if you are prepared for the system to generate and display a PIN, make sure that no one can see your screen, and type **yes**. A system-generated PIN appears on your screen for 10 seconds.
5. Memorize your new PIN. Do not write it down.
6. Continue the authentication process. For instructions, see the appropriate topic in "Accessing Protected Resources" on page 29.

## Replacing a PIN in New PIN Mode

When you attempt to authenticate, you will be put into "New PIN mode" in the following circumstances:

- If you have never created a PIN or been assigned a PIN by your RSA ACE/Server administrator. In that case, see "Creating a PIN for a New Software Token" on page 21.
- If you have forgotten your PIN or your PIN has been compromised (for example, an unauthorized person has learned it). In that case, follow the instructions in this section.

You can replace a PIN in New PIN mode using either Token View or Advanced View. The new PIN is created during the authentication procedure.

**To replace a PIN for a software token that is in New PIN mode, using Token View:**

1. Start a login session to access the login window of your application.

   You are prompted to enter your PIN.
2. Start the Software Token application in Token View.

3. On the number pad, type your current PIN, and click **Enter**.
   The generated PASSCODE appears.
4. Click **Copy!** to copy the PASSCODE, and paste it into your login application.
   You will be prompted for a PIN.
5. On the number pad, type your new PIN, and click **Enter**.
   The new PASSCODE appears.
6. On the Software Token application menu bar, click **View > Next Code**.
7. Click **Copy!** to copy the next PASSCODE, and paste it into your login application.

**To replace a PIN for a software token that is in New PIN mode, using Advanced View:**

1. Start a login session to access the login window of your application.
2. Start the Software Token application in Advanced View.
3. Type your PIN, and click **Apply PIN**.
4. Click **Copy** next to the Current PASSCODE box, and paste the PASSCODE into your login application.
   You will be prompted for a PIN.
5. In the Software Token Advanced View, enter a new PIN, and click **Apply PIN**.
6. Click **Copy** next to the Next PASSCODE box, and paste the PASSCODE into your login application.

# Using a Smart Card with the Application

If you will be using a smart card with the RSA SecurID Software Token application, the software driver for your card reader must be installed and the card reader must be connected to your computer. Your RSA ACE/Server administrator may do the installation or have you do it. Whenever you log in to a protected resource, first insert your smart card into the reader.

Before you can use your smart card for authentication, you must

- Set up smart card communication.
- Transfer a software token to your smart card.
- (Optional) Set a smart card passphrase.

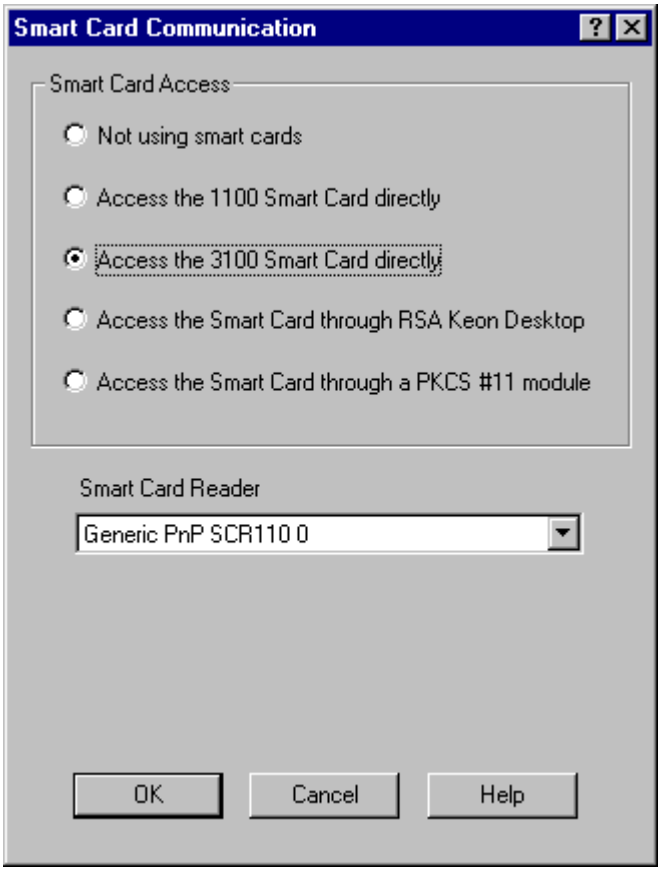
## Setting Up Smart Card Communication

Before you can use a smart card with the Software Token application, the application must be set up to communicate with your smart card.

**Note:** The RSA ACE/Server administrator may elect to set up smart card communication for you. The administrator will also tell you which smart card communication method to use.

## Smart Card Communication Methods

The Software Token application can communicate with a smart card directly through a smart card reader attached to your computer, through the RSA Keon Desktop, or through a PKCS #11 module.




### Direct Access

The application software can access your RSA SecurID 3100 Smart Card directly from a card reader attached to your computer. Your RSA ACE/Server administrator will supply you with the reader and the software driver for the reader. When you select direct access for your RSA Smart Card, you will be prompted for the associated reader.

RSA SecurID 3100 Smart Cards come with a temporary password that you must enter when you insert the card into the reader. A "Change Password" button allows you to change the temporary password. This password is a security feature of the RSA SecurID 3100 Smart Card and cannot be removed from the card.

**Note:** If you have been using an RSA SecurID 1100 Smart Card with a previous version of the Software Token application, it should also work with Software Token 3.0.

### Through the RSA Keon Desktop

You can use the Software Token application with the RSA Keon Desktop 5.6. Before using the application with the Desktop, make sure that you are logged in to the Desktop.

### Through a PKCS #11 Module

If you select the PKCS #11 module as the smart card access method, a box labeled "PKCS11 Module" is displayed. To use this access method, you need to have the associated .**dll** file installed on your computer, and you need to know the name and location of the file. Contact your RSA ACE/Server administrator if you need help.

**To set up smart card communication:**

1. Start the Software Token application.
2. On the menu bar, click **Tools > Smart Card Options**.
3. In the Smart Card Communication dialog box, click next to the method by which the software will access your smart card. If you are unsure which selection to make, ask your RSA ACE/Server administrator.
4. In the Smart Card Reader box, accept the default selection if it is the reader you will use, or use the drop-down menu to make a selection. You will not be prompted for a smart card reader if you choose the RSA Keon Desktop access method.
5. Click **OK**.

**Note:** If you change your smart card access method, you will be prompted to select a software token.

## Transferring a Software Token to a Smart Card

If you have been issued a smart card that does not already contain a software token, you need to transfer at least one software token from your hard drive to your smart card. You can store a maximum of 5 software tokens on an RSA SecurID 3100 Smart Card, or 10 software tokens on another supported smart card. Tokens must be transferred to your smart card one at a time. Before you begin, verify that a software token is installed on your hard drive.

**Note:** You need write permission to the directory into which the Software Token application is installed before you can transfer software tokens to your smart card. Your administrator can either grant write permission or transfer the tokens for you.

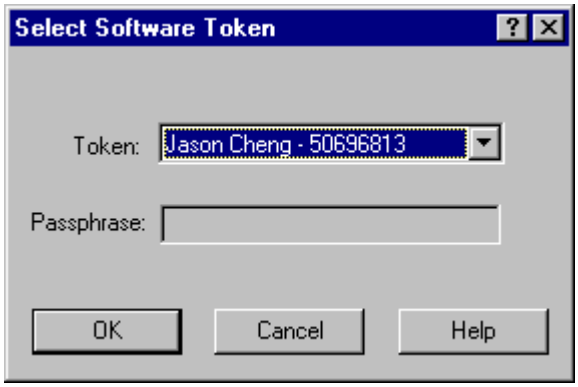
Administrative operations involving software tokens on smart cards (such as changing or resetting token passphrases, or deleting tokens from cards) can be performed only by the RSA ACE/Server administrator.

**To verify that a software token is installed on your hard drive:**

1. Start the Software Token application.
   The serial number of the currently selected token appears in the title bar.
2. On the menu bar, click **File > Select Token**.
3. In the Token box, use the drop-down menu to display the list of installed software tokens.

**To transfer a software token to a smart card:**

1. Insert the smart card into the card reader.
2. Start the Software Token application.
3. On the menu bar, click **File > Select Token**.
4. In the Select Software Token dialog box, select the listed token or use the drop-down menu to select a different token.




**Note:** If you do not select a software token, the program will transfer the current token.

5. On the Software Token application menu bar, click **Tools > Transfer Token to Smart Card**. When prompted to confirm the transfer, click **Yes**.

**To confirm the transfer:**

On the Software Token application menu bar, click **File > Select Token**. The software token is now identified as **Smart Card - *serial_number***.

## Setting a Smart Card Passphrase

You can set a passphrase for your smart card to protect the tokens on the smart card from unauthorized access.

**To set a smart card passphrase:**

1. Start the Software Token application and insert the smart card into the card reader.
2. In either the Token View or the Advanced View, click **Tools > Set Smart Card Passphrase**.
3. Type a passphrase in the New Passphrase box.
4. Re-type the passphrase in the Confirm box, and click **OK**.
   An **Operation Successful!** message confirms the passphrase.

# Accessing Protected Resources

This section covers procedures for local and network authentication; authenticating with manual dial-up networking; and authenticating to a protected Web site. It also explains what to do if your software token is put into Next Tokencode mode.

**Note:** To authenticate with the RSA ACE/Agent Browser Plug-In, see "Authenticating with the RSA ACE/Agent Browser Plug-In" on page 9. To authenticate with the Login Automation program, see "Authenticating With Login Automation" on page 14.

## Before Authenticating

Before authenticating for the first time, make sure

- You have installed a software token or tokens.
- The date and time settings on your computer are accurate.
- If you are using a smart card,
  - A supported smart card reader is installed.
  - You have set the type of smart card access on the Smart Card Communication screen.
  - Your software token has been transferred to the smart card.
  - The smart card is in the card reader.

## Authenticating Locally or Across a Network

Use this procedure to authenticate either locally or across a network or if the RSA ACE/Agent Browser Plug-In is not installed. You can perform this procedure from the Software Token user interface, using either Token View or Advanced View.

If you are using the token for the first time, follow the instructions in "Creating a PIN for a New Software Token" on page 21 before trying to authenticate.

### To authenticate using Token View:

When attempting to access a protected resource, you will be prompted for your username and PASSCODE.

1. Start the Software Token application in Token View.
2. Enter your PIN on the Software Token number pad, and click **Enter**.
   The new code appears with the word "PASSCODE" above it.

3. Click **Copy!** to copy the PASSCODE.
4. Paste the PASSCODE into your login application at the Enter PASSCODE prompt, and press ENTER.
   The confirmation message, **PASSCODE accepted**, appears.

**To authenticate using Advanced View:**

When attempting to access a protected resource, you will be prompted for your username and PASSCODE.

1. Start the Software Token application in Advanced View.
2. In the Software Token PIN box, type your PIN, and click **Apply PIN**.
   The generated PASSCODE appears in the Current PASSCODE box.
3. In the Current PASSCODE box, click **Copy**.
4. Paste the PASSCODE into your login application at the Enter PASSCODE prompt, and press ENTER.
   The confirmation message, **PASSCODE accepted**, appears.

## Authenticating with Manual Dial-Up Networking

Use this procedure to establish a remote dial-up connection to access the protected resource.

**Note:** This is not the same procedure as for Login Automation. If you are using Login Automation, see "Authenticating With Login Automation" on page 14.

You can perform this procedure from the Software Token user interface, using either Token View or Advanced View.

**Before you begin:**

- Make sure your Windows Dial-Up Networking profile is set up. See your administrator if you need help.
- If you are using the token for the first time, follow the instructions in "Creating a PIN for a New Software Token" on page 21 before trying to authenticate.

**To authenticate with manual dial-up networking using Token View:**

1. Start the Software Token application.
2. Double-click the Dial-Up Networking icon on your desktop.
3. Right-click the connections file you want to use for remote access, and click **Properties**.
4. In the connection dialog box, click **Configure**.
5. In the modem properties dialog box, select **Options**.

6. Check **Bring up terminal window after dialing**.
7. Click **OK > OK**.
8. Establish a remote connection.
9. At the Username prompt in the terminal window, type your username, and press ENTER.

   The Enter PASSCODE prompt appears.
10. Using the number pad in the Software Token application, type your PIN, and click **Enter**.

    The new PASSCODE is generated, with the word "PASSCODE" above it.
11. Type the PASSCODE at the Enter PASSCODE prompt in the terminal window, and press ENTER.

    The confirmation message, **PASSCODE accepted**, appears.

**Note:** If you attempt to copy and paste the PASSCODE, the session terminates with the error message "The script has been halted." This is a security feature.

**To authenticate with manual dial-up networking using Advanced View:**

1. Start the Software Token application, and click **View > Advanced View**.
2. Follow steps 2 through 8 above to configure and establish a remote connection.
3. At the Username prompt in the terminal window, type your username, and press ENTER.

   The Enter PASSCODE prompt appears.
4. In Software Token Advanced View, type your PIN in the PIN box, and click **Apply PIN**.

   The Current PASSCODE box displays the generated PASSCODE.
5. Type the PASSCODE at the Enter PASSCODE prompt in the terminal window, and press ENTER.

   The confirmation message, **PASSCODE accepted**, appears.

**Note:** If you attempt to copy and paste the PASSCODE, the session terminates with the error message "The script has been halted." This is a security feature.

# Authenticating to a Protected Web Site

RSA SecurID Software Token 3.0 allows you to use your software token to access protected Web sites to which your company has given you access privileges.

## Requirements for Web Authentication

Use one of the following Web browsers:

- Netscape Communicator v 4.79
- Microsoft Internet Explorer v 5.5 SP2 or 6.0

## Microsoft Internet Explorer Requirement

If you are using Microsoft Internet Explorer, you must change one of the default settings to eliminate a security risk. See the following procedure, "To prevent unauthorized Web access without authentication:" on page 32. Otherwise, if you use your software token to gain access to a protected Web page, then close the browser and leave the machine unattended, an unauthorized person can open Internet Explorer and access the protected page without being required to supply a PASSCODE.

**To prevent unauthorized Web access without authentication:**

1. Open Internet Explorer.
2. On the Tools menu, click **Internet Options**.
3. Under Temporary Internet Files, on the **General** tab, click **Settings**.
4. Under the prompt "Check for newer versions of stored pages," click **Every visit to the page**, and click **OK**.
5. In the Internet Options dialog box, click **OK**.

   This setting ensures that a successful authentication is required every time you or any other user requests access to a protected Web page.

## Web Authentication Procedure

**Note:** If you are using the token for the first time, follow the instructions in "Creating a PIN for a New Software Token" on page 21 before trying to authenticate.

**To authenticate to a protected Web site:**

1. Open your Web browser and try to access the protected Web site.


2. Enter your username.
3. When prompted for a PASSCODE, start the Software Token application in Token View.
4. Type your PIN on the Software Token number pad and click **Enter**.
5. Click **Copy**.
6. Paste the PASSCODE into the PASSCODE box of the Web authentication page.

## Next Tokencode Mode

**Note:** You do not need the following instructions if you are using the RSA ACE/Agent Browser Plug-In or the Login Automation program.

The RSA ACE/Server puts software tokens into Next Tokencode mode when the following events occur:

- The time setting on your computer is incorrect.
- You make several unsuccessful authentication attempts (for example, by entering an incorrect PIN).

If either event occurs and you are authenticating locally or with manual dial-up networking, you will be prompted to enter an additional tokencode.

**To respond to a prompt to enter the next tokencode using Token View:**

1. When prompted for the next tokencode, press **Clear** to clear the PIN.
2. Click **View > Next Code**.
   The next tokencode appears in the numerical box.


3. Click **Copy!** to copy the tokencode. Paste it into your login application at the Enter Tokencode prompt, and press ENTER.
   The confirmation message, **PASSCODE accepted**, appears.

**To respond to a prompt to enter the next tokencode using Advanced View:**

1. When prompted for the next tokencode, click **Copy** next to the Next Tokencode box.
2. Paste the tokencode into your login application at the Enter Tokencode prompt, and press ENTER.
   The confirmation message, **PASSCODE accepted**, appears.

# Troubleshooting

This section gives suggestions for resolving problems you might encounter.

| Problem | Suggested Actions |
|---|---|
| Cannot install the Software Token application. | You must have administrative privileges on your computer in order to install the application. Contact your administrator. |
| Cannot install or transfer software tokens. | You need write permission to the directory in which the Software Token application is installed. Ask your administrator to give you write permission or to install or transfer the tokens for you. |
| Forgot token passphrase. | You will not be able to authenticate with that token. Contact your administrator. |
| Need to delete a token. | Users cannot delete tokens. Contact the administrator with your request. |
| Need to move tokens from local computer to another computer. | Contact your administrator. |
| Access to the remote host denied. | • Make sure the time, date, and time zone settings on your computer are accurate.<br>• Your token may be disabled because of failed login attempts. Contact your administrator.<br>• Ask your administrator to verify that your RSA SecurID Software Token username is defined in the RSA ACE/Server database and is associated with the same software token.<br>• Make sure your network connection is configured properly, the modem works, and you can hear a dial tone. |
| After several failed authentication attempts, the Next Tokencode prompt appears. | See "Next Tokencode Mode" on page 33. |
| The smart card does not work. | Check that<br>• Your smart card is inserted in the card reader properly.<br>• The card reader is securely attached to the computer.<br>• You have set your smart card access option.<br>• A software token has been transferred to the smart card.<br>• You entered the correct user passphrase for your smart card. If you have forgotten the passphrase, see your administrator. |

| Problem | Suggested Actions |
|---|---|
| Modem does not dial the phone number. | Verify that<br>• Your cables, including the plastic receptacles on the ends of the cables, are in good working order.<br>• A cable extends between the telco jack on the modem and the phone wall jack.<br>• If your modem emits carrier signals but fails to establish a communications link, place the call again.<br>• If you still cannot establish a remote connection, see your modem documentation. |
| Cannot start a remote connection. | • Make sure the Remote Access Server is running.<br>• Make sure Windows Dial-Up Networking (DUN) is configured properly.<br>• Try connecting to the remote site using Windows DUN. If that works, you know that the modem and phone line are working.<br>• Ask your administrator to verify that you are configured as a valid login user on the remote system. |
| Attempts to use Login Automation result in the message "No Windows Dial-Up Networking Phone Book entries were found on the system. You cannot use Login Automation without a valid DUN entry." | Before using Login Automation, you must create a DUN phone book entry. Instructions are provided in the Help for your Windows operating system. If you need assistance, contact your administrator. |
| Attempts to use Login Automation result in the message "There are no valid profiles found. You must create a new profile." | Before using Login Automation, you must create a connection profile to use with your DUN phone book entry. See "To set up a connection profile:"on page 11. |
| Cannot authenticate with Login Automation. | Try to authenticate by dialing in manually. See "Authenticating with Manual Dial-Up Networking" on page 30.<br>If the problem persists, follow this procedure:<br>1. Start the Login Automation program.<br>2. Click **Profile >>> > Edit**.<br>3. Write down the Connection Profile and Profile Settings information. Make sure you include the username and the software token serial number.<br>4. Ask your administrator to call RSA Security Customer Support. |

| Problem | Suggested Actions |
|---|---|
| Login Automation program does not close. | Ask your administrator to check the script files to make sure the backup re-copied itself correctly. You can tell that the copy has succeeded by looking for RSA SecurID keywords in the script file. If you see RSA SecurID data instead of keywords, the re-copy failed. For example, if you see **87779351** instead of **$PASSCODE$**, the recopy operation has failed.<br>To replace the files correctly, make sure the **.bak** file exists and that it is the original script file. Then, delete the current script file (for example, **rasnew.scp**) and rename the backup file to your script file name (for example, rename **rasnew.bak** to **rasnew.scp**). |
| Browser Plug-In page does not appear. | **If you are using Internet Explorer:**<br>1. Open Internet Explorer.<br>2. Click **Tools >Internet Options**.<br>3. Click **Languages** > **Add**.<br>4. In the User Defined box, type **en-securid**.<br>5. Click **OK** to exit from each dialog box.<br>6. Click **Refresh** on your Web browser to display the RSA ACE/Agent Browser Plug-In page.<br>**If you are using Netscape**:<br>1. Open Netscape Communicator.<br>2. Click **Edit > Preferences**.<br>3. Under the Navigator directory, click **Languages** > **Add**.<br>4. In the Others box, type **en-securid**. Click **OK**.<br>5. Click **Reload** on your Web browser to display the RSA ACE/Agent Browser Plug-In page. |
| Cannot select a token on smart card when using Browser Plug-In. | This problem can occur if your computer is running Internet Explorer 6.0 on Windows NT. Use Add/Remove Programs to uninstall the Browser Plug-In, and then follow the procedure in "Authenticating Locally or Across a Network" on page 29. |
| Internet browser hangs. | This problem can occur if your computer is running Internet Explorer 6.0 on Windows NT and you are using a smart card. Use Add/Remove Programs to uninstall the Browser Plug-In, and then follow the procedure in "Authenticating Locally or Across a Network" on page 29. |

| Problem | Suggested Actions |
|---|---|
| With the Browser Plug-In installed, trying to use the Search button in Internet Explorer 5.5 results in a "page not found" message. | Change the Internet Explorer language setting as follows:<br>1. On the Internet Explorer menu bar, click **Tools > Internet Options > General > Languages**. A list of languages appears.<br>2. Do one of the following:<br>• If **English [en-securid]** is the only language listed, click **Add** and click a new language, typically **English (United States) [en-us]**. Click **OK**.<br>• If several languages are listed, but **English [en-securid]** is listed first, go to step 3.<br>3. In the language list, select the new language and click **Move Up** to move the new language to the top of the list.<br>4. Click **OK** on all open panels.<br>5. Close Internet Explorer and restart it. |

# Uninstalling the Application

Use the Windows Add/Remove Programs utility to uninstall the Software Token application. The uninstallation also uninstalls your software tokens. Contact your administrator if you need software tokens for another application.