

RSA SecurID Token 2.3 for the Java ME Platform User Help

RSA SecurID Token 2.3 for the Java ME Platform is authentication software that transforms a Java-enabled device into an RSA SecurID token that you can use to access resources protected by RSA SecurID software, such as a VPN client or a web site.

Use this document to learn how to use the device as an RSA SecurID token. The document includes the following sections:

[Installing the RSA SecurID Token Application](#)

[Importing a Token](#)

[Setting a PIN if the Device Displays a PIN Prompt](#)

[Setting a PIN if the Device Displays a Tokencode](#)

[Using the RSA SecurID Token to Access a Protected Resource](#)

[Changing the Token Password](#)

[Viewing the Token Serial Number, Device ID, and Application Information](#)

[Viewing GMT and Local Time](#)

[Stopping the RSA SecurID Token Application](#)

[Removing the RSA SecurID Token Application](#)

[Troubleshooting](#)

Installing the RSA SecurID Token Application

RSA SecurID Token 2.3 for the Java ME Platform must be installed on a device running Java Platform Micro Edition (J2ME) and Mobile Information Device Profile (MIDP) 2.0. If you are not sure whether the device meets these requirements, ask an administrator.

Note: RSA SecurID Token 2.3 for the Java ME Platform does not upgrade the previous version of this application, RSA SecurID Token 2.2 for the Java ME Platform. If the previous version is already installed on the device, follow the instructions provided by an administrator.

Local time, the time zone, and the Daylight Savings Time setting must be set correctly so that you can use the token to access resources protected by RSA SecurID software. Before installing the RSA SecurID Token application on the device, verify that these settings are correct.

To install the RSA SecurID Token application:

1. Do one of the following:
 - Download the application using the browser on the device. Use the URL provided by an administrator, or go to the RSA web site: <http://rsa.com/jme/>. When prompted, press **Yes** to download the application, and follow the prompts to install the application on the device. If you are prompted to choose whether you want to install the application on the device or a memory card, select the device.
 - Install the application on the device using a file transfer or device management utility that is compatible with the device, for example, Nokia PC Suite or Sony Ericsson PC Suite.
The application file is **SecurID.jar**, but if the application is customized in any way, an administrator will also provide **SecurID.jad** and instruct you to install the application using this file. For more information, see the documentation on the utility.
2. Start the RSA SecurID Token application. The License Agreement screen is displayed.
3. Read the text of the license agreement, and press **Accept**. (You must accept the license agreement before you can use the application.)
4. Do one of the following:
 - If a token is not included with the application, the Import New Token screen is displayed. You must import a token before you can use the application. See the following section, [“Importing a Token.”](#)
 - If a token is included with the application, continue to the next step.
5. If the application was installed with a password-protected token, enter the password provided by your administrator, and press **OK**.
6. Do one of the following:
 - If the token requires a PIN and the device displays a PIN prompt, you must create a PIN. See [“Setting a PIN if the Device Displays a PIN Prompt”](#) on page 4.
 - If the token requires a PIN and the device displays a tokencode, you must create a PIN. See [“Setting a PIN if the Device Displays a Tokencode”](#) on page 5.
 - If the token does not require a PIN, a tokencode is displayed immediately and you can begin using the token. See [“Using the RSA SecurID Token to Access a Protected Resource”](#) on page 6.

Importing a Token

If the RSA SecurID Token application was not installed with a token, you must install a token before you can use the application.

A device running RSA SecurID Token 2.3 for the Java ME Platform supports only one token. If a token was already imported to the device, a new token overwrites it.

Use the appropriate procedure to import a token:

- To use the Web Download method, see the following section, [“Importing a Token Using the Web Download Method.”](#)
- To use the Numeric Input method, see [“Importing a Token Using the Numeric Input Method”](#) on page 4.

Importing a Token Using the Web Download Method

Before you begin, make sure that you have the token activation code. An administrator may also provide a URL if the application is not configured to download the token automatically from a specific URL.

To import a token using the Web Download method:

1. On the Import New Token screen, select **Web Download**. (If the Import New Token screen is not displayed on the device, select **Menu > Import New Token**, and select **Web Download**.)
2. Enter the Activation Code, and if the URL field is displayed, enter the URL provided by an administrator.
3. If prompted to use airtime, select **Yes**, and wait for the download to complete.
4. Do one of the following:
 - If the token requires a PIN and the device displays a PIN prompt, you must create a PIN. See [“Setting a PIN if the Device Displays a PIN Prompt”](#) on page 4.
 - If the token requires a PIN and the device displays a tokencode, you must create a PIN. See [“Setting a PIN if the Device Displays a Tokencode”](#) on page 5.
 - If the token does not require a PIN, a tokencode is displayed immediately and you can begin using the token. See [“Using the RSA SecurID Token to Access a Protected Resource”](#) on page 6.

Importing a Token Using the Numeric Input Method

To import a token using the Numeric Input method, you need to enter the numeric string provided by an administrator. Before you begin, make sure that you have this number available.

To import a token using the Numeric Input method:

1. On the Import New Token screen, select **Numeric Input**. (If the Import New Token screen is not displayed on the device, select **Menu > Import New Token**, and select **Numeric Input**.)
2. Enter the numeric string.
Enter the first 5 numbers into field **1 of 17**, the next 5 numbers into field **2 of 17**, and so on. When there is only 1 number left, enter it in the last field.
3. Press **OK**.
4. If the token is password protected, enter the password provided by an administrator, and press **OK**.
5. Do one of the following:
 - If the token requires a PIN and the device displays a PIN prompt, you must create a PIN. See the following section, [“Setting a PIN if the Device Displays a PIN Prompt.”](#)
 - If the token requires a PIN and the device displays a tokencode, you must create a PIN. See [“Setting a PIN if the Device Displays a Tokencode”](#) on page 5.
 - If the token does not require a PIN, a tokencode is displayed immediately and you can begin using the token. See [“Using the RSA SecurID Token to Access a Protected Resource”](#) on page 6.

Setting a PIN if the Device Displays a PIN Prompt

If you are issued a token that requires a PIN, you must create a PIN the first time you use the token for authentication. The application you use to set your PIN may reside on your computer, or you may be able to access it from the device. In the following procedure, the application resides on the computer.

To set a PIN if the device displays a PIN prompt:

1. On your computer, open the protected application, for example, your VPN client.
2. Enter your user ID. You are prompted for a passcode.
3. On the device, enter your token password, if prompted.
4. On the Enter PIN screen, enter four zeros, and press **OK**. A passcode is displayed.
5. On your computer, when prompted, enter the passcode from the device in the **Passcode** field.

6. On your computer, when prompted, enter and confirm your new PIN. Your PIN must contain four to eight digits, and it cannot begin with a zero.
You are prompted for a new passcode.
7. From the RSA SecurID Token application menu on the device, select **Menu > Re-enter PIN**, and enter the PIN you created. A new passcode is displayed. Enter it in the **Passcode** field on your computer.

Note: The code changes every 60 seconds. A timer counts down the time remaining before the code changes. If the code changes before you can enter it on your computer, enter the new code to complete your authentication.

Setting a PIN if the Device Displays a Tokencode

If you are issued a token that requires a PIN, you must create a PIN the first time you use the token for authentication. The application you use to set your PIN may reside on your computer, or you may be able to access it from the device. In the following procedure, the application resides on the computer.

To set a PIN if the device displays a tokencode:

1. On your computer, open the protected application, for example, your VPN client.
2. Enter your user ID. You are prompted for a passcode.
3. On the device, enter your token password, if prompted. A tokencode is displayed.
4. On your computer, when prompted, enter the tokencode from the device in the **Passcode** field. You are prompted to create a PIN. Your PIN must contain four to eight digits, and it cannot begin with a zero.
5. On your computer, when prompted, enter and confirm your new PIN. You are prompted for a new passcode.
6. In the RSA SecurID Token application on the device, wait for the tokencode to change.
7. After the tokencode changes, return to the protected application on your computer. In the **Passcode** field, enter your PIN. Enter the tokencode displayed on the device directly to the right of the PIN.

Note: The code changes every 60 seconds. A timer counts down the time remaining before the code changes. If the code changes before you can enter it on your computer, enter the new code to complete your authentication.

Using the RSA SecurID Token to Access a Protected Resource

This procedure describes how to access a protected resource using the RSA SecurID token on the device.

To access a protected resource:

1. On your computer, open the protected application, for example, your VPN client.
2. Enter your user ID. You are prompted for a passcode.
3. On the device, start the RSA SecurID Token application, and enter your token password, if required.
4. If your token requires a PIN, do one of the following:
 - If the RSA SecurID Token application displays a PIN prompt, enter your PIN, and press **OK**. The device displays a passcode. Enter the code in the application on your computer.
 - If the RSA SecurID Token application displays a tokencode instead of a PIN prompt, enter your PIN in the application on your computer, and enter the tokencode to the right of your PIN.
5. If your token does not require a PIN, enter the tokencode displayed on the device in the application on your computer.

Note: The code changes every 60 seconds. A timer counts down the time remaining before the code changes. If the code changes before you can enter it on your computer, enter the new code to complete your authentication.

Changing the Token Password

When a token is password protected, the RSA SecurID Token application prompts you to enter the password before the code is displayed. A password increases the security of your token.

If the token on the device is password protected, you can use the RSA SecurID Token application to create, change, or remove the password. The password can contain up to 30 characters and is case sensitive.

Note: Removing the token password makes the token less secure and is not recommended.

To change the password:

1. On the Tokencode or Passcode screen, select **Menu > Change Password**.
2. Do one of the following:
 - To change the existing password: Enter the current password in the **Current Password** field, and enter the new password in the **New Password** and **Confirm Password** fields.

- To create a password: Enter the new password in the **New Password** and **Confirm Password** fields.
- To remove the password: Enter the current password in the **Current Password** field, and leave the **New Password** and **Confirm Password** fields empty.

Viewing the Token Serial Number, Device ID, and Application Information

The About RSA SecurID option in the application menu launches a screen that shows the following:

- **Token Serial Number.** You may need the token serial number to activate the token, or an administrator may ask you for the token serial number to verify that you were issued the correct token.
- **Device ID.** An administrator may ask you to provide your Device ID number so that the token can be issued with a special security measure that makes the token usable only on the device.

In some cases, the application cannot access the Device ID number. In this case, the Device ID is displayed as “Not available”.

- **Name and version of the RSA SecurID Token application and its resource library.** An administrator may ask you to verify the version of the software installed on the device.

To view the Token Serial Number, Device ID, and application information:

Select **Menu > About RSA SecurID**. The information is displayed.



Viewing GMT and Local Time

The time, date, and time zone settings on the device must be correct in relation to Coordinated Universal Time (also called Greenwich Mean Time, or GMT). Otherwise, your authentication attempts may fail. To assist in troubleshooting, an administrator may ask for the GMT setting displayed in the RSA SecurID Token application.

To view GMT and local time:

On the Tokencode or Passcode screen, select **Menu > View Time**. GMT and local time are displayed.



Stopping the RSA SecurID Token Application

After using the RSA SecurID Token application to access a protected resource, you may stop the application so that you can use the device to perform other functions, such as making a call or using a different application.

To stop the application:

Select **Menu > Exit**.

Removing the RSA SecurID Token Application

To remove the RSA SecurID Token application, stop the application and use the proper method for removing MIDP applications from the device. For more information, see the documentation for the device.

Troubleshooting

The following table provides troubleshooting information. If the information in this table does not resolve your issue, contact an administrator.

Problem	Reason
The RSA SecurID Token application installation fails.	<p>The following conditions can cause an installation to fail:</p> <ul style="list-style-type: none"> • The device is not MIDP 2.0 compliant. • The operating system on the device does not support the application. (Compatible devices include Nokia and Sony Ericsson.) • The download web site is unavailable. • The device cannot download the application because it is not web enabled. • The device does not have enough available memory to install the application.
Application errors occur on the device.	<p>The following conditions can cause application errors on the device:</p> <ul style="list-style-type: none"> • There is no token on the device, and you did not import a token. • The device cannot run unsigned applications.
You cannot import a token, or the token import fails.	<p>General issues that prevent a token import include:</p> <ul style="list-style-type: none"> • The token is invalid, or the application configuration prevents you from importing a token. • The token file is password protected, and you entered an invalid password. • The token was issued for a device with a different Device ID number. • The token type is not supported. <p>Web download issues that prevent a token import include:</p> <ul style="list-style-type: none"> • The device is not web enabled. • No token activation code was specified, or the token activation code is invalid. • No URL was specified, or the URL is invalid or too long. The URL must start with http:// or https://, and also be less than 200 characters. • The web site hosting the download is unavailable. • A general packet failure occurred. • The server is untrusted. <p>Numeric input issue that prevents a token import: mistyping or omitting numbers in the numeric string.</p>



Problem	Reason
You cannot access a protected resource, or you are denied access.	<p>The following conditions can prevent a user from accessing a protected resource:</p> <ul style="list-style-type: none">• The token requires a PIN, and you entered an invalid PIN.• You entered an invalid user name or used the wrong token to access the resource.• The time on the device is not synchronized with the time on the RSA SecurID authentication server.

© 2008 RSA Security Inc. All rights reserved.

Trademarks

RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, go to www.rsa.com/legal/trademarks_list.pdf. EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.