RSA SecurID Software Token 1.3 for iPhone and iPad
Administrator’s Guide
Contact Information
See the RSA corporate web site for regional Customer Support telephone and fax numbers: www.rsa.com

Trademarks
RSA, the RSA Logo, SecurID, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For the most up-to-date listing of RSA trademarks, go to www.rsa.com/legal/trademarks_list.pdf.

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.

Note on encryption technologies
This product may contain encryption technology. Many countries prohibit or restrict the use, install, or export of encryption technologies, and current use, install, and export regulations should be followed when using, installing 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.
## Contents

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

### Chapter 1: Planning for Deployment
- About RSA SecurID Software Token: 9
- System Requirements: 9
- Supported Authentication Servers: 10
  - Automated Token Provisioning Solutions: 10
- System Clock Settings: 11
  - Synchronize Date, Time, and Time Zone Settings: 11
- Supported Software Token Configurations: 11
- Token Provisioning Mechanisms: 13
  - File-Based Provisioning: 13
  - Dynamic Seed Provisioning: 13
- Token Security During Provisioning: 14
  - Device Binding: 14
  - Password Protection of File-Based Tokens: 15
- Token Security on the Device: 16
- Next Code Feature: 16
- Token Delivery Options: 17
- RSA SecurID Authentication: 18
  - Supported Token Types: 18
  - Authentication with a PINPad-Style Software Token: 19
  - Authentication with a Fob-Style Software Token: 20
  - Authentication with a PINless Software Token: 21

### Chapter 2: Installing the Application
- Performing Pre-Deployment Tasks: 23
- Installation Overview: 23
  - Install the Application Directly to a Device: 24
  - Install the Application by Syncing It Through iTunes: 25
- Distribute the Quick Start Document: 25
- Updating to Application Version 1.3: 25
  - Update from the Apple App Store: 26
  - Update from the Device: 26
- Uninstalling the Application: 27
  - Uninstall the Application from the Device: 27
  - Uninstall the Application from iTunes: 27
Chapter 3: Provisioning Tokens Using RSA Authentication Manager 7.1

Preparing to Provision Tokens ................................................................. 29
Provisioning Tokens Using Dynamic Seed Provisioning .......................... 31
Before You Begin .................................................................................. 32
Install the Device Definition File ............................................................ 33
Configure the Token Record in RSA Authentication Manager 7.1 .......... 33
Specify the Token Distribution Method .................................................. 38
Provisioning File-Based Tokens ............................................................. 38
Before You Begin .................................................................................. 39
Configure the Token Record and Set a Token File Password ................. 40

Chapter 4: Using RSA Credential Manager Self-Service Provisioning

Preparing to Use Self-Service Provisioning ........................................... 41
Review Supported Token Configurations .............................................. 42
Install the iPhone 1.3 Device Definition File ........................................ 42
(Recommended) Require Device Binding ................................................. 42
Issuing Software Tokens Using RSA Credential Manager ................. 43
Step 1: Configure RSA Credential Manager Token Management Settings ... 44
Step 2: Replace the Request Approval Notification E-Mail Template .... 46
Step 3: Allow Users to Create a Self-Service Account ........................... 46
Step 4: Provide Instructions for Requesting a Software Token .......... 46
Step 5: Approve Software Token Requests ........................................... 48
Step 6: Instruct Users on How to Install the Token ......................... 49

Chapter 5: Provisioning Tokens Using RSA Authentication Manager 6.1

Preparing to Provision Tokens ................................................................. 51
Provisioning File-Based Tokens ............................................................. 53
Before You Begin .................................................................................. 53
Configure the Token Record in RSA Authentication Manager 6.1 .......... 53
Bind the Token Using Token Extension Data ........................................ 56

Chapter 6: Delivering Software Tokens

Token Delivery Mechanisms ................................................................. 59
Delivering Dynamically Provisioned Tokens Using a Hyperlink ........... 60
Step 1: Issue a Dynamically Provisioned Token ................................... 60
Step 2: Construct a URL Link ............................................................... 61
Step 3: Compose and Send an E-mail Message ................................. 62
Step 4: Instruct Users on How to Install the Token ......................... 63
Step 5: Verify Successful Execution of the CT-KIP Protocol ............. 63
Delivering File-Based Tokens as E-mail Attachments ....................... 64
Before You Begin .................................................................................. 64
E-mail a Token File Attachment .......................................................... 64
Instruct Users on How To Install the Token ...................................... 64
Delivering File-Based Tokens Using a Hyperlink ......................................................... 65
  Step 1: Issue the Software Token as an SDTID File ............................................. 66
  Step 2: Convert the Token File .............................................................................. 67
  Step 3: Compose and Send an E-mail Message ..................................................... 68
  Step 4: Instruct Users on How to Install the Token .............................................. 68

Chapter 7: Troubleshooting ...................................................................................... 69
  Customer Support Information ............................................................................... 69
  Application Installation Problems .......................................................................... 69
  Token Installation Problems .................................................................................. 70
    Application Is Not Installed .................................................................................. 70
    Errors Issuing the Token in RSA Authentication Manager .................................. 70
    Invalid Token ....................................................................................................... 70
    File Password Errors ......................................................................................... 70
    Token Converter Errors ...................................................................................... 71
    CT-KIP URL Format Errors .................................................................................. 71
    E-mail Message Format Errors .......................................................................... 71
    Network Communication Errors .......................................................................... 71
  Authentication Problems ....................................................................................... 72
    User Error ............................................................................................................. 72
    Error Exporting Tokens ....................................................................................... 72
    Time Synchronization Problem .......................................................................... 72
    Expired Token ...................................................................................................... 72
  Error Messages ....................................................................................................... 73

Index ......................................................................................................................... 75
Preface

About This Guide

This guide describes how to install RSA SecurID Software Token 1.3 for iPhone and iPad (the RSA SecurID application) and provision software tokens to the application in an enterprise environment. It is intended for RSA Authentication Manager administrators and IT personnel who are responsible for deploying and administering the 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 Documentation

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

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

Quick Start. Helps users install the application and install a software token. Also describes how to use a token to access resources protected by RSA SecurID.

Help. Describes procedures associated with the application screens. Users can open the Help file by tapping the Help (?) icon in the application.

Release Notes. Provides workarounds for known issues and includes other information about the application. It is intended for administrators.

Related Documentation

RSA SecurID Authentication Engine 2.6 for Java Developer's Guide. Provides a detailed description of the Authentication Engine API as well as information for properly using the API to detect and protect against common security vulnerabilities.

RSA SecurID Authentication Engine 2.6 for Java Javadoc. Documents the Authentication Engine Java classes. The Javadoc is located in the \doc\javadoc folder of the RSA SecurID Authentication Engine Developer's Kit.

RSA SecurID Software Token Converter 2.6 Readme. Describes how to convert a token exported as an SDTID file to a compressed format that can be delivered to an iPhone or iPad device.

RSA Authentication Manager 7.1 Administrator's Guide. Provides information about how to administer users and security policy in RSA Authentication Manager 7.1.

RSA Security Console Help. Describes day-to-day administration tasks performed in the RSA Security Console used with RSA Authentication Manager 7.1.
RSA Authentication Manager 6.1 Administrator's Guide. Provides information about how to administer users and security policy in RSA Authentication Manager 6.1.


You must have an account on RSA SecurCare Online to access the Best Practices Guides. For the guides, go to:

Best Practices for RSA SecurID Authenticators and RSA Authentication Manager

Support and Service

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

RSA SecurCare Online offers a knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, installant technical news and software downloads.

Before You Call Customer Support

Make sure that you have direct access to the device that is running the application.

Please have the following information available when you call:

- Your RSA Customer/License ID.
- RSA SecurID application version number.
- The model of the device on which the problem occurs.
- The device operating system version under which the problem occurs.
1

Planning for Deployment

This chapter introduces RSA SecurID® Software Token 1.3 for iPhone and iPad (the RSA SecurID application) and lists the system requirements and supported software token configurations.

About RSA SecurID Software Token

RSA SecurID Software Token is authentication software that transforms an iPhone, iPad, or iPod touch device into a SecurID authentication device. The software consists of an application and a separately installed software-based security token.

A software token generates a 6-digit or 8-digit pseudorandom number, or tokencode, at regular intervals. When the tokencode is combined with a PIN, it is called a passcode. The tokencode or passcode serves as a one-time password (OTP). Authorized device users can use OTP values, along with other security information, to verify their identity when they attempt to access resources protected by SecurID, such as Virtual Private Networks (VPNs) and web applications. Users enter a new OTP every time they authenticate to a protected resource.

System Requirements

Make sure that you meet the following system requirements for installing and provisioning the application.

- One of the following:
  - iPhone 3G/3GS running iOS 3.0 or later
  - iPhone 4 running iOS 4.0 or later
  - iPad running iOS 3.2 or later
  - iPad 2 running iOS 4.3.3 or later
  - iPod touch running iOS 4.0 or later
  - Any iPhone, iPad, or iPod touch device running iOS 5.0.
- For the latest supported versions, go to [http://www.rsa.com/iphone](http://www.rsa.com/iphone).
- (Optional) A Windows or Mac computer running iTunes 9.2 or later.
- Access to a network protected by RSA Authentication Manager 6.1, RSA Authentication Manager 7.1 SP3, or RSA SecurID Authentication Engine 2.6.
- 3.2 MB available space on the device.
Supported Authentication Servers

To issue software tokens for use with the application, you need one of the following authentication servers:

- RSA Authentication Manager 7.1 SP3. You may need to setup a proxy server for RSA Authentication Manager 7.1 if:
  - You are deploying software tokens using CT-KIP (Cryptographic Token Key Generation Protocol). You must configure a proxy server to connect to mobile devices through Secure Sockets Layer (SSL).
  - You want to restrict users from directly accessing RSA Authentication Manager for self-service token provisioning. You can configure a proxy server to accept RSA Self-Service Console requests and proxy to the Self-Service Console. For more information, go to http://www.rsa.com/node.aspx?id=2535, and click the “Configuring a Self Service Proxy Server Technical Publication” link.

- RSA SecurID Appliance 3.0

  **Note:** References to RSA Authentication Manager 7.1 also apply to the Appliance.

- RSA Authentication Manager 6.1

- RSA SecurID Authentication Engine 2.6 for Java

Automated Token Provisioning Solutions

If you have a large number of users, RSA recommends automating the administrative work involved in issuing tokens. RSA provides the following web-based solutions for automating the issuance process:

- **RSA Credential Manager.** Credential Manager enhances the capabilities of RSA Authentication Manager 7.1 by providing self-service software token provisioning. A configurable self-service console allows end users to request software tokens to use with specific mobile devices. Credential Manager is included in RSA Authentication Manager 7.1 Enterprise Edition.

  For instructions on configuring Credential Manager to issue software tokens for iPhone and iPad devices, see “Using RSA Credential Manager Self-Service Provisioning” on page 41. For more information, go to http://www.rsa.com/node.aspx?id=1180. Also see the RSA Authentication Manager 7.1 Administrator’s Guide.

- **RSA Authentication Deployment Manager.** Formerly RSA SecurID Web Express, RSA Authentication Deployment Manager 1.3 offers end users a self-service platform for requesting tokens. Deployment Manager is available for use with RSA Authentication Manager 6.1. If you have a valid maintenance contract, go to https://www.rsasecurity.com/go/form_ins.asp or contact your Account Manager. If you do not have a maintenance contract, contact your local RSA sales representative or reseller.
System Clock Settings

The SecurID algorithm uses Coordinated Universal Time (UTC) settings to calculate the current one-time password (OTP). Software tokens rely on the host device (the iPhone or iPad device) to determine the correct UTC time value. For this reason, the local time, the time zone, and Daylight Saving Time must all be set correctly so that users can perform RSA SecurID authentication from their devices. Users who cross time zones with their devices need only to change the time zone to reflect the correct local time.

Synchronize Date, Time, and Time Zone Settings

To ensure that users are able to use their software token, instruct them to verify the clock settings on their devices before you provision software tokens.

Supported Software Token Configurations

The RSA SecurID application supports provisioning one software token per device. The token configurations available with the RSA SecurID application depend on which version of Authentication Manager you use. In the following table, the configurations with a blue check mark are supported by the specified server. The configurations with a red X are not supported.

Note: You must issue 128-bit (AES) tokens. The RSA SecurID application does not support 64-bit (SID) tokens.

<table>
<thead>
<tr>
<th>Token Attributes</th>
<th>RSA Authentication Manager 7.1</th>
<th>RSA Authentication Manager 6.1</th>
<th>RSA Credential Manager</th>
<th>RSA SecurID Authentication Engine 2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>128-bit AES</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Time-based</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8-digit tokencode</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>6-digit tokencode</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>60-second tokencode duration</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>30-second tokencode duration</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>PINPad style tokens</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

1: Planning for Deployment 11
<table>
<thead>
<tr>
<th>Token Attributes</th>
<th>RSA Authentication Manager 7.1</th>
<th>RSA Authentication Manager 6.1</th>
<th>RSA Credential Manager</th>
<th>RSA SecurID Authentication Engine 2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fob-style tokens (PIN entry in the protected resource)</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>PINless tokens</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Token file password</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Options for binding the token to the iPhone device GUID</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Options for binding the token to a Device ID or UDID</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
Token Provisioning Mechanisms

RSA SecurID supports the following token provisioning mechanisms:

- File-based provisioning, available in RSA Authentication Manager 6.1, RSA Authentication Manager 7.1, including RSA SecurID Appliance 3.0 and RSA Credential Manager 1.0, and RSA SecurID Authentication Engine 2.6 for Java.
- Dynamic Seed Provisioning, available in RSA Authentication Manager 7.1, including RSA SecurID Appliance 3.0 and RSA Credential Manager 1.0

File-Based Provisioning

With file-based provisioning, an XML-format software token file (also called an SDTID file) is generated by Authentication Manager or the Authentication Engine token export utility when you issue a software token to a user. This file contains the shared secret ("seed") used by the SecurID algorithm, along with other metadata associated with the token (expiration date, serial number, number of digits in the tokencode, and so on).

To protect the seed against attack, the seed is encrypted using the AES encryption algorithm and an optional password. The seed is a string of random binary data, which when decrypted gives no hint that it is a valid secret. To gain access to the seed, an attacker would have to test each attempted decryption against the target Authentication Manager, which would cause the server to rapidly disable the software token that is under attack.

Dynamic Seed Provisioning

Dynamic Seed Provisioning is a client-server protocol that enables secure, rapid setup of software tokens. A feature of RSA Authentication Manager 7.1, Dynamic Seed Provisioning uses the industry-standard Cryptographic Token Key Initialization Protocol (CT-KIP).

Dynamic Seed Provisioning eliminates the need for a token distribution file. Instead, the software token application running on the device (the client) and Authentication Manager (the server) use a four-pass CT-KIP protocol to exchange information that is used to dynamically generate a unique seed on the client and the server. In this way, the CT-KIP protocol protects against potential interception of the seed.

When you issue a CT-KIP token in Authentication Manager, a unique one-time token activation code is generated. To allow a user to install a CT-KIP token, you must communicate the activation code and the URL (service address) of the CT-KIP server.
Token Security During Provisioning

You can strengthen token security when provisioning tokens in RSA Authentication Manager using:

- **Device binding.** Associates a token with a specific user’s device or with any supported iPhone or iPad device. The administrator configures device binding when issuing a token in RSA Authentication Manager. For more information, see the following section, “Device Binding.”

- **Password protection of file-based tokens (SDTID files).** The administrator creates a token file password when issuing a token in Authentication Manager. For more information, see “Password Protection of File-Based Tokens” on page 15.

**Note:** Password protection is not used on tokens issued using Dynamic Seed Provisioning.

Device Binding

When configuring a software token record in Authentication Manager, you can bind the token by configuring a token extension attribute (DeviceSerialNumber). Binding the token ensures that it is installed only on a specific device or class of devices. RSA strongly recommends binding file-based software tokens.

With Dynamic Seed Provisioning, use of the one-time activation code helps alleviate some of the security issues associated with file-based tokens. For more security assurance, however, it is good practice to bind CT-KIP tokens.

Device Class Binding

You can bind software tokens intended for iPhone or iPad devices to one of the “iPhone 1.3” device type GUID (globally unique identifier). This default option allows the user to install the token to any iPhone or iPad device that is supported by the RSA SecurID application. It prevents the token from being installed on other types of mobile devices or on computers running an RSA SecurID software token application. The iPhone and iPad GUID is 556f1985-33dd-442c-9155-3a0e994f21b1.

Device ID and Device UDID Binding

A Device ID or unique device identifier (UDID) is a unique sequence of letters and numbers that identifies a specific device. A token bound to a Device ID or UDID cannot be installed on another device. For devices running iOS 3.x, the Device ID is the device’s UDID. It is a forty-character, alphanumeric string. For devices running iOS 4.x or later, the RSA SecurID application provides a Device ID. It is a 24-character, alphanumeric string.

**Note:** Apple is deprecating unique device identifier (UDID) access for iOS applications. This version of the RSA SecurID application adds its own unique identifier, a Device ID, for binding tokens to specific devices. You can bind tokens to a Device ID or UDID. However, the RSA SecurID application does not provide a mechanism for retrieving the UDID on devices running iOS 4.x or later.
You bind tokens when issuing them in your authentication server (for example, RSA Authentication Manager). Before you can bind a token to a specific device, the user must provide the Device ID. Users can view their Device ID or UDID from the Info screen on their device. The application also provides an option for users to e-mail their Device ID to their system administrator. For more information, see “Step 4: (Recommended) Obtain the Device ID for Binding the Token” on page 35.

**Determine Your Device Binding Mechanism**

Use the information in the following table to help you decide which binding mechanism best suits your requirements.

<table>
<thead>
<tr>
<th>Binding Mechanism</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 1.3 Device</td>
<td>Provides less protection for file-based tokens than binding to a Device ID because the token file can be installed on iPhone or iPad devices other than the user’s device.</td>
</tr>
<tr>
<td>Type GUID (default</td>
<td>Prevents installing the token on a computer or on a mobile device other than an iPhone or iPad.</td>
</tr>
<tr>
<td>mechanism)</td>
<td>Easy to implement because the Authentication Manager administrator can bind all tokens to the same device type.</td>
</tr>
<tr>
<td></td>
<td>Because the device type GUID is the default binding entry in Authentication Manager 7.1, the administrator does not need to configure a token extension attribute.</td>
</tr>
<tr>
<td>Device ID or UDID</td>
<td>Provides a high level of protection because the token will only install on the device with the specified Device ID or UDID.</td>
</tr>
<tr>
<td></td>
<td>Requires the administrator to obtain the Device ID or UDID from the user before configuring the token record.</td>
</tr>
</tbody>
</table>

**Password Protection of File-Based Tokens**

File-based software tokens should be protected during transit with a password that is sent to the user separately from the token. The user must enter the password in the RSA SecurID application on the device to complete the token installation.

Assigning a token password is intended to help protect against malicious users gaining access to the SDTID file and attempting to install the token on a different device. However, if the software token does not use device binding, the password mechanism does not prevent a user who has access to both the SDTID file and the password from installing the token on multiple devices. For this reason, RSA strongly recommends using both device binding and password protection with file-based tokens.
Token Security on the Device

After a token has been installed on a device, it is stored in a token database and protected with a set of system attributes. When the application needs to open the token database, it queries the system for the set of attributes used and checks them for validity. If a user or malware attempts to copy the token database to another device, the user cannot obtain tokencodes, and the application appears as not having a token.

For stronger security, RSA recommends that users enable the data protection feature on their devices. Data protection provides additional security for e-mail messages and attachments by protecting the device with a user-configured passcode. The feature is available on iPhones running iOS 4.x and later and on all iPad models. For more information, see the article on data protection at [http://support.apple.com/kb/HT4175](http://support.apple.com/kb/HT4175).

Next Code Feature

RSA Authentication Manager and RSA SecurID Authentication Engine can detect when a user provides multiple incorrect one-time passwords (OTPs), in succession. This situation may be caused by user error, time drift on the device running the application, or it may indicate that an attacker has gained access to the token and is attempting to gain unauthorized access. When this occurs, the authentication server places the token in Next Tokencode mode. In Next Tokencode mode the user must enter the next successive code to authenticate. Requiring the user to provide the next code helps ensure the code is being generated by a token in the possession of the proper owner.

This version of the RSA SecurID application provides a Next Code button that allows a user whose token is in Next Tokencode mode to immediately retrieve the next code. The user does not need to wait for the device to display the next code.
**Token Delivery Options**

RSA provides several options for delivering tokens to supported devices. Use the information in the following table to help you decide which option best suits your requirements.

<table>
<thead>
<tr>
<th>Delivery Mechanism</th>
<th>Administrative Tasks</th>
<th>End User Actions</th>
<th>Supported Devices and Provisioning Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail attachment</td>
<td>1. Issue a file-based token using standard Authentication Manager processes.</td>
<td>Select the token file attachment, and enter the token password, if required.</td>
<td>Device:</td>
</tr>
<tr>
<td></td>
<td>2. Send an e-mail message with a token file attachment to the user’s device.</td>
<td></td>
<td>• iPhone or iPod touch running iOS 4.0 or later</td>
</tr>
<tr>
<td></td>
<td>3. Securely communicate the token password to the user, if required.</td>
<td></td>
<td>• iPad running iOS 3.2 or later</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provisioning servers:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• RSA Authentication Manager 7.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• RSA Authentication Manager 6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• RSA SecurID Authentication Engine 2.6 for Java</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reference: “Delivering File-Based Tokens as E-mail Attachments” on page 64</td>
</tr>
<tr>
<td>E-mail hyperlink</td>
<td>1. Issue a file-based token using standard Authentication Manager processes.</td>
<td>1. Open the e-mail message in the device e-mail, and touch the embedded hyperlink.</td>
<td>Device:</td>
</tr>
<tr>
<td>(file-based tokens)</td>
<td>2. Convert the token to Compressed Token Format.</td>
<td>2. Enter the token file password, if prompted.</td>
<td>• iPhone running iOS 3.0 or later</td>
</tr>
<tr>
<td></td>
<td>3. Send an e-mail message with a hyperlink that contains converted token data to the user’s device.</td>
<td></td>
<td>• iPad running iOS 3.2 or later</td>
</tr>
<tr>
<td></td>
<td>4. Securely transmit the token password, if required, to the user.</td>
<td></td>
<td>• iPod touch running iOS 4.0 or later</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provisioning servers:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• RSA Authentication Manager 7.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• RSA Authentication Manager 6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reference: “Delivering File-Based Tokens Using a Hyperlink” on page 65</td>
</tr>
<tr>
<td>E-mail hyperlink</td>
<td>1. Dynamically provision a token using standard Authentication Manager processes.</td>
<td>1. Open the e-mail message in the device e-mail, and touch the embedded hyperlink.</td>
<td>Device:</td>
</tr>
<tr>
<td>(dynamically provisioned tokens)</td>
<td>2. Send an e-mail message with a hyperlink that contains token data to the user’s device.</td>
<td>2. Enter the token activation code, if prompted.</td>
<td>• iPhone running iOS 3.0 or later</td>
</tr>
<tr>
<td></td>
<td>3. Securely transmit the token activation code to the user, if not included in the hyperlink.</td>
<td></td>
<td>• iPad running iOS 3.2 or later</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• iPod touch running iOS 4.0 or later</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Provisioning server:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RSA Authentication Manager 7.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reference: “Delivering Dynamically Provisioned Tokens Using a Hyperlink” on page 60</td>
</tr>
</tbody>
</table>
RSA SecurID Authentication

RSA SecurID uses two-factor authentication, a protocol in which two different factors are used in conjunction to verify a user’s identity. Two-factor authentication typically is a sign-on process where a user proves his or her identity with “something you know” and “something you have.” Using two factors delivers a higher level of authentication assurance than using one factor (for example, a password).

With RSA SecurID, something you have is a software token, and something you know is a PIN. The combination of the PIN and the current tokencode generated by the software token forms a passcode. The passcode is the one-time password (OTP) used for authentication. For every authentication, the user obtains a new OTP, which must be entered along with other security information, such as a user name.

The specific SecurID authentication procedure depends on the type of software token that you issue: PINPad-style, fob-style, or tokens that do not require a PIN (PINless).

Supported Token Types

- **PIN-Enabled Tokens.** RSA Authentication Manager 7.1, RSA SecurID Authentication Engine 2.6, and RSA SecurID Appliance 3.0 support two types of PIN-enabled software tokens: PINPad-style and fob-style. Each type offers strong two-factor authentication assurance. The RSA SecurID application recognizes the token type that is installed on the device and displays customized screens accordingly. RSA Authentication Manager 6.1 supports PINPad-style tokens, but does not support fob-style tokens.

- **PINless Tokens.** All supported versions of RSA Authentication Manager can issue software tokens that do not require entering a PIN. If you issue PINless tokens, the user authenticates with the currently displayed tokencode (something you have). You should not issue PINless tokens unless you plan to require a second authentication factor, such as a Windows password. For information about the proper use of PINless tokens, see the RSA SecurID Best Software Token Best Practices Guide.
Authentication with a PINPad-Style Software Token

Note: RSA Authentication Manager 7.1, RSA SecurID Appliance 3.0, RSA SecurID Authentication Engine 2.6, and RSA Authentication Manager 6.1 support issuance of PINPad-style software tokens.

With PINPad-style software tokens, the user enters his or her SecurID PIN on the Enter PIN screen on the device. This action generates the OTP (passcode). To complete the authentication, the user enters the OTP, along with other security information, into the protected resource. For example, with a VPN client application, the user typically enters a user name and the OTP.

This authentication experience is similar to using an RSA SecurID PINPad-style hardware token, such as the SD520, where the user enters the PIN on the token’s numeric keypad, and then enters the displayed OTP in the protected resource.

PINPad-style software tokens require a 4–8 digit numeric PIN.

The following figure shows user authentication to a VPN client application with a PINPad-style software token.
Authentication with a Fob-Style Software Token

**Note:** RSA Authentication Manager 7.1, RSA SecurID Authentication Engine 2.6, and RSA SecurID Appliance 3.0 support issuance of fob-style software tokens. RSA Authentication Manager 6.1 does not support issuance of fob-style software tokens.

Fob-style software tokens do not require you to enter the SecurID PIN on the device. Instead of displaying an Enter PIN screen, the device displays tokencodes. To authenticate to a VPN client application, for example, the user enters security information (typically, a user name) in the VPN client. The user then enters the PIN, followed by the current tokencode displayed on the device. The combination of the PIN and tokencode forms the OTP (passcode).

Fob-style software tokens used with the SecurID application require a 4–8 digit PIN. To require alphanumeric PINs, the administrator must configure the token policy in the RSA Security Console (`Authentication > Policies > Token Policies`).

The following figure shows user authentication to a VPN client application with a fob-style software token.

1. Enter PIN in VPN client.
2. Obtain tokencode from SecurID application.
3. Enter tokencode after PIN in VPN client.
Authentication with a PINless Software Token

**Note:** RSA Authentication Manager 7.1, RSA SecurID Appliance 3.0, RSA SecurID Authentication Engine 2.6, and RSA Authentication Manager 6.1 support issuance of PINless software tokens.

If you issue tokens that do not require a PIN, the user authenticates with the tokencode (OTP). For example, to authenticate to a VPN client application, the user obtains the current OTP from the Tokencode screen on the device. The user enters the OTP and other security information, such as a user name, in the protected resource.

The following figure shows user authentication to a VPN client application with a PINless software token.

1. Obtain tokencode from SecurID application.

2. Enter tokencode in VPN client.
2

Installing the Application

This chapter describes how to install RSA SecurID Software Token 1.3 for iPhone and iPad devices, upgrade from a previous version, and uninstall the application.

Performing Pre-Deployment Tasks

To prepare for deployment of the application in your enterprise, complete the tasks in the following table.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Download the application from the Apple App Store.</td>
<td>“Installation Overview” on page 23</td>
</tr>
</tbody>
</table>
| 2. Provision software tokens. | • “Provisioning Tokens Using RSA Authentication Manager 7.1” on page 29  
• “Provisioning Tokens Using RSA Authentication Manager 6.1” on page 51 |
| 3. Distribute the end-user Quick Start document. | “Distribute the Quick Start Document” on page 25 |

Installation Overview

The RSA SecurID application is available at no cost from the Apple App Store. The RSA web site provides the following web link, which you can use to direct users to the application: http://www.rsa.com/iphone. You can copy the link into an e-mail message and send it to users’ device e-mail programs or to their computers. That way users do not have to search for the application in the App Store. After the users have installed the application, you must provision their devices with a software token. For more information, see one of the following:

- Chapter 3, “Provisioning Tokens Using RSA Authentication Manager 7.1”
- Chapter 4, “Using RSA Credential Manager Self-Service Provisioning”
- Chapter 5, “Provisioning Tokens Using RSA Authentication Manager 6.1”
Users can install the application directly onto their device from the App Store. Or, they can launch the App Store in iTunes, download the application to their computer, and then sync it to the device. The following figure shows these two options.

Install the Application Directly to a Device

Use the following procedure to install the application directly onto your device from the App Store.

**To install the application directly to a device:**

1. Tap the App Store icon on your device.
2. Browse the Business category, and select RSA SecurID Token.
3. Enter your Apple ID or iTunes account credentials.
   The device exits to the Home screen to display the download progress. When the download is complete, the application is available on the device.
Install the Application by Syncing It Through iTunes

Use the following procedure to download the application to your computer and install it onto your device through a sync.

To install the application through a sync:

1. Connect your device to a USB port on your computer.
2. Launch the App Store in iTunes.
3. Browse the Business category, and select RSA SecurID Token.
4. Download the application to your computer.
5. If prompted, authenticate with your Apple ID or iTunes account credentials.
6. Instruct iTunes to sync the application onto your device, and apply the changes.

Distribute the Quick Start Document

RSA provides a Quick Start document in PDF format to help users install and use the application. The Quick Start contains instructions for:

- Downloading and installing the application
- Installing a software token
- Setting a PIN (if required) during the user’s first RSA SecurID authentication
- Using the application to log on to resources protected by RSA SecurID

The product documentation is located on the RSA web site at http://www.rsa.com/iPhone. RSA recommends that you download the documentation and e-mail the Quick Start to users.

After launching the application, users can access the Help file for the application by tapping the Help (?) icon.

Updating to Application Version 1.3

Users who have installed previous versions of the RSA SecurID application will automatically receive a notification of an update to the application on the App Store icon on their device or if they access the Apple App Store. You do not need to issue new tokens, as existing tokens remain in the token database and work with version 1.3 of the application.

There are two ways to upgrade:

- From the Apple App Store, as described in the following section, “Update from the Apple App Store.”
- From the device, as described in “Update from the Device” on page 26.
Update from the Apple App Store

Use the following procedure to update the application from the Apple App Store.

**To update from the Apple App Store:**

1. At the bottom of the screen, tap **Updates**.
2. Tap the application to see more information about the update.
3. Tap **Update**.
4. Enter your Apple ID and password to complete the update.

Update from the Device

Use the following procedure to update the application from the device.

**To update from the device:**

1. Tap the **App Store** icon.
2. Tap the **Update** icon represented by the red alert bubble located on the lower navigation bar.
3. Select the **RSA SecurID** icon to open the update page.
4. On the update page, tap the gray **FREE** icon. This icon changes to a green **INSTALL** icon.
5. Tap the **INSTALL** icon.
6. Enter your Apple ID and password to complete the update.
Uninstalling the Application

You can uninstall the RSA SecurID application from your iPhone or iPad device and from iTunes. Uninstalling the application from your device does not remove it from your iTunes library. If you uninstall the application from iTunes but not from the device, and then you sync, the application will still be available on the device. This section describes how to permanently uninstall the application from both your device and iTunes.

Uninstall the Application from the Device

Use the following instructions to uninstall the application from the device.

To uninstall the application from the device:
1. Touch and hold any application icon on the Home screen until the icons start to wiggle.
2. Tap the “x” in the corner of the RSA SecurID application.
3. Tap **Delete**, and press the **Home** button.

**Note:** The next time you sync your iPhone device, if the application reappears on your device, it is probably because you set your synchronization setting to **All Applications**. To ensure that the application does not reappear on your device, change this setting to **Selected Applications**.

Uninstall the Application from iTunes

Use the following procedure uninstall the application from iTunes.

To uninstall the application from iTunes:
1. In iTunes, select the **Applications** content area, and right-click the RSA SecurID Token application.
2. Click **Delete**.
3. When asked if you are sure you want to remove the application from your library, click **Remove**.
4. When asked whether you want to move the application to the trash or keep it in the **Mobile Applications** folder, click **Move to Trash**. The application is removed from your iTunes library.
5. Connect your iPhone or iPad device to your computer. If you have not manually deleted the application from your device, you are asked if you want to transfer the item from your device back to your iTunes library. Click **Don’t Transfer**.
Provisioning Tokens Using RSA Authentication Manager 7.1

This chapter describes how to provision software tokens using RSA Authentication Manager 7.1 or RSA SecurID Appliance 3.0.

Preparing to Provision Tokens

Before you begin the token provisioning process, keep the following in mind:

• You can use either Dynamic Seed Provisioning or file-based provisioning to issue tokens using RSA Authentication Manager 7.1.

• You must issue 128-bit (AES) tokens. The application does not support 64-bit (SID) tokens.

You must also do the following:

• Review the software token configurations supported with RSA Authentication Manager 7.1. For more information, see “Supported Software Token Configurations” on page 11.

• (Recommended) Determine the mechanism that you will use to bind tokens. For more information, see “Device Binding” on page 14.

• Determine the type of token that you want to issue: PINPad, fob-style, or PINless. For more information, see “RSA SecurID Authentication” on page 18.
Use the information in the following table to become familiar with provisioning methods and iOS requirements, and then click the reference link to see more information on the provisioning method that you plan to use.

<table>
<thead>
<tr>
<th>Provisioning Method</th>
<th>iOS Requirements</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Dynamic Seed Provisioning (CT-KIP)                     | • iPhone running iOS 3.0 or later  
• iPad running iOS 3.2 or later  
• iPod touch running iOS 4.0 or later | • “Provisioning Tokens Using Dynamic Seed Provisioning” on page 31  
• “Delivering Dynamically Provisioned Tokens Using a Hyperlink” on page 60 |
| File-based provisioning with the token delivered as e-mail attachment | • iPhone or iPod touch running iOS 4 or later  
• iPad running iOS 3.2 or later | • “Provisioning File-Based Tokens” on page 38  
• “Delivering File-Based Tokens as E-mail Attachments” on page 64 |
| File-based provisioning with compressed token data delivered in an embedded hyperlink in e-mail | • iPhone running iOS 3.0 or later  
• iPad running iOS 3.2 or later  
• iPod touch running iOS 4.0 or later | • “Provisioning File-Based Tokens” on page 38  
• “Delivering File-Based Tokens Using a Hyperlink” on page 65 |
Provisioning Tokens Using Dynamic Seed Provisioning

To use Dynamic Seed Provisioning, you configure and issue a token in RSA Authentication Manager 7.1 or RSA SecurID Appliance 3.0, selecting CT-KIP as the distribution method. To deliver the token, you must construct a URL link that contains the CT-KIP URL and activation code, and send an e-mail message containing the URL link to the user’s device. In the device Mail application, the user taps the URL link to install the token.

Dynamic Seed Provisioning requires an activation code generated in Authentication Manager to complete the token installation. If you include the token activation code as part of the URL link, the user can install the token with one tap. If you deliver the activation code separately, for example, through internal corporate e-mail, the user is prompted to enter the activation code to complete the token installation.

The following figure provides an overview of Dynamic Seed Provisioning, and the sections that follow describe the provisioning steps in detail.
The following table lists the CT-KIP provisioning tasks, and the sections that follow describe each step.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install the iPhone 1.3 device definition file to the Authentication Manager server or use the iPhone 1.0 device definition file.</td>
<td>“Install the Device Definition File” on page 33</td>
</tr>
<tr>
<td>2. Configure the software token record.</td>
<td>“Configure the Token Record in RSA Authentication Manager 7.1” on page 33</td>
</tr>
<tr>
<td>3. Distribute the token.</td>
<td>“Specify the Token Distribution Method” on page 38</td>
</tr>
<tr>
<td>4. Deliver the token to the user’s device.</td>
<td>“Delivering Dynamically Provisioned Tokens Using a Hyperlink” on page 60</td>
</tr>
</tbody>
</table>

**Before You Begin**

Before you can issue tokens using CT-KIP in RSA Authentication Manager 7.1, you must complete the following tasks in the RSA Security Console:

1. Install tokens (**Authentication > SecurID Tokens > Install Tokens Job > Add New.**)
2. Add users (**Identity > Users > Add New.**)
3. Assign software tokens to users (**Identity > Users > Manage Existing.**)

For procedures, see the RSA Security Console Help.
Install the Device Definition File

Software tokens issued using RSA Authentication Manager 7.1 or RSA SecurID Appliance 3.0 must be associated with a device definition file. This is an XML file that specifies the supported capabilities and attributes of tokens used with the application. The device definition file specifies the supported tokencode characteristics, the token type (PINPad-style, fob-style, or PINless), whether the token is CT-KIP capable, and the supported binding attributes. The iPhone 1.3 device definition file is included with the product documentation zip file at http://www.rsa.com/iphone.

Before you issue software tokens to use with the RSA SecurID application, you may need to install the device definition file on your RSA Authentication Manager 7.1 server. The iPhone 1.3 device definition file supports binding a token to the iPhone device class GUID. If you have upgraded from a previous version of the application, and you want to use the iPhone device class GUID as your device binding attribute, you must install the iPhone 1.3 device definition file.

To install the device definition file:

1. Download the zip file containing the device definition file from http://www.rsa.com/iphone, and save it to a folder on your computer.

2. In the RSA Security Console, click Authentication > Software Token Device Types > Install Token Device Type.

3. Click Browse to locate the iPhone 1.3 device definition file.

4. Select the file, and click Submit.

Configure the Token Record in RSA Authentication Manager 7.1

This guide assumes that you have installed software token records into Authentication Manager, assigned tokens to users, and are ready to configure them in the Security Console. The following sections describe key steps for configuring token records for use with the RSA SecurID application. For more information on configuring token records, see the Security Console Help.

Step 1: Access the Edit Token page

To access the Edit Token page:

1. Log on to the Security Console.

2. Click Authentication > SecurID Tokens > Manage Existing.

3. Locate the token that you want to edit, click the drop-down arrow next to its serial number, and select Edit.
Step 2: Select the User Authentication Requirement

In the SecurID PIN Management section, do one of the following:

- Select **Require PIN during authentication** if you want the user to authenticate with a passcode (PIN plus tokencode).
- Select **Do not require PIN (only tokencode)** if you want the user to authenticate with a tokencode only (no PIN).

![SecurID PIN Management](image)

Step 3: Select the Software Token Device Type

From the Software Token Device Type drop-down list, select **iPhone 1.3** if you installed the iPhone 1.3 device definition file. Otherwise, select the option that you used with your previous version of the RSA SecurID application.

![Software Token Device Type](image)

Selecting the device type displays the **Device Specific Attributes** section, which lists the attributes that you can assign to tokens used with iPhone devices.
Step 4: (Recommended) Obtain the Device ID for Binding the Token

By default, tokens issued for iPhone devices in RSA Authentication Manager 7.1 are bound to the iPhone device type GUID. This allows the token to be installed on any supported iPhone, iPad, or iTouch, but not on another type of mobile device. The device type GUID is the default entry in the DeviceSerialNumber field.

If you want to restrict the delivery of the token to a specific device, you can bind the token to the Device ID of a user’s device. For devices running iOS 3.x, the Device ID is the device’s UDID, which is a device-specific sequence of 40 letters and numbers. For devices running iOS 4.x and later, the Device ID is a unique sequence of 24 letters and numbers.

Before you can bind a token to a specific device, you must obtain the device’s Device ID. To obtain the Device ID, the device must have the RSA SecurID application installed. The RSA SecurID Application displays the Device ID on the Info screen.

Obtain the Device ID from the Application

Provide users with the instructions below to send the administrator their Device ID.

Note: The device must have an e-mail account configured to perform this procedure.

To obtain the Device ID from the installed RSA SecurID application:

1. Install RSA SecurID Software token 1.3 for iPhone and iPad on the device.
2. From the device, start the RSA SecurID application.
3. Tap the Information (i) icon
4. Tap Email.
5. Enter the SecurID administrator’s e-mail address, and send the message.
Step 5: (Optional) Bind the Token

In the Software Token Device Type section, in the DeviceSerialNumber field, do one of the following:

- To bind the token to the iPhone device type GUID, leave the default entry.
- To bind the token to the Device ID, delete the default entry, and replace it with the Device ID. An example is shown in the following figure.

![Software Token Device Type](image)

**Note:** Leave the Nickname field blank. The application does not currently support assigning the token a user-friendly name.
Step 6: Select the Software Token Settings

In the Software Token Settings section, select the software token settings. The following figure shows the settings available for the RSA SecurID application, and the table explains each setting.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displayed Value</td>
<td>Displayed Value options are available if you selected Require PIN during authentication as the user authentication requirement.</td>
</tr>
<tr>
<td></td>
<td>• Select Passcode (PIN incorporated into tokencode) to issue a PINPad-style software token.</td>
</tr>
<tr>
<td></td>
<td>• Select Tokencode (PIN entered followed by tokencode during authentication) to issue a fob-style software token.</td>
</tr>
<tr>
<td></td>
<td>If you selected Do not require PIN (only tokencode) as the user authentication requirement, the default displayed value is always set to “Tokencode.” The displayed value options do not affect the behavior of PINless tokens.</td>
</tr>
<tr>
<td>Tokencode Length</td>
<td>Select either 6-Digits or 8-Digits.</td>
</tr>
<tr>
<td>Tokencode Type</td>
<td>Time Based is automatically selected, indicating that the tokencode changes at a regular interval. Event-Based tokens are not supported.</td>
</tr>
<tr>
<td>Tokencode Duration</td>
<td>Select either Display next tokencode every 30 seconds or Display next tokencode every 60 seconds.</td>
</tr>
</tbody>
</table>
Specify the Token Distribution Method

After you configure the user’s software token record, you must specify the token distribution method and select an attribute to use for the token activation code. The activation code can contain a maximum of 40 characters. If you bound the token to the Device ID, you can use the Device ID as the activation code. Otherwise, select a system-generated activation code.

To distribute the token:

1. In the Basics section, next to Distribution Method, select Generate CT-KIP Credentials for Web Download.

2. Under Options, do one of the following:
   - If you bound the token to the Device ID, and you want to use the Device ID as the token activation code, select DeviceSerialNumber.
   - If you did not bind the token to the Device ID, select System Generated Code.

3. Click Next to save the configuration and view the token delivery details.

Provisioning File-Based Tokens

RSA Authentication Manager 7.1, RSA SecurID Authentication Engine 2.6, and RSA SecurID Appliance 3.0 support file-based provisioning. With file-based provisioning, you configure a token record in the same way as for dynamically provisioned tokens. However, you select Issue Token File (SDTID) as the token distribution method. This generates a software token distribution file (SDTID file) containing token data.
Before You Begin

Before you can issue SDTID files in RSA Authentication Manager 7.1, you must do the following:

1. Install tokens (Authentication > SecurID Tokens > Install Tokens Job > Add New).
2. Add users (Identity > Users > Add New).
3. Assign software tokens to users (Identity > Users > Manage Existing).

Note: Procedures for the tasks listed above are provided in the RSA Security Console Help.

After completing the prerequisites, you must:

• Configure the token record
• Deliver the token
Configure the Token Record and Set a Token File Password

When configuring the software token record for a file-based token, RSA recommends that you set a token file password to protect the token file in transit. The token file password can contain a maximum of 24 characters. It is case sensitive and can contain numbers, letters, spaces, punctuation, and symbols. The application prompts the user for the password during the token installation. The password is not used again after the token has been installed.

To configure the token record and set a token file password:

1. Follow steps 1 through 4 in “Configure the Token Record in RSA Authentication Manager 7.1” on page 33.
2. In the Basics section, select Issue Token File (SDTID) as the distribution method.
3. In the Token File Options section, from the Password Protect options, select Password or another option for protecting the token distribution file. For information on password options, click Help on this page at the top of the screen.

<table>
<thead>
<tr>
<th>Token File Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Protection:</td>
</tr>
<tr>
<td>Password Protect:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Confirm Password:</td>
</tr>
<tr>
<td>Regenerate Token:</td>
</tr>
</tbody>
</table>

Note: The Enable copy protection field is automatically selected.

4. Enter and confirm a token file password, and click Next to issue the token file.
Using RSA Credential Manager Self-Service Provisioning

This chapter describes how to use RSA Credential Manager for Dynamic Seed Provisioning or file-based provisioning. RSA Credential Manager is the self-service and provisioning component of RSA Authentication Manager 7.1 Enterprise Edition. Users access the Self-Service Console to request a new software token or a replacement token.

Preparing to Use Self-Service Provisioning

You can use Credential Manager for self-service provisioning of file-based tokens (SDTID files) and dynamically provisioned tokens. The following device and iOS support is required.

<table>
<thead>
<tr>
<th>File-Based Token (SDTID)</th>
<th>CT-KIP token</th>
</tr>
</thead>
<tbody>
<tr>
<td>• iPhone or iPod touch running iOS 4 or later</td>
<td>• iPhone running iOS 3.0 or later</td>
</tr>
<tr>
<td>• iPad running iOS 3.2 or later</td>
<td>• iPad running iOS 3.2 or later</td>
</tr>
<tr>
<td></td>
<td>• iPod touch running iOS 4.0 or later</td>
</tr>
</tbody>
</table>

**Note:** To provision SDTID files to devices running an earlier iOS version, you must use the RSA Security Console. For more information, see “Delivering File-Based Tokens Using a Hyperlink” on page 65.

Before you use Credential Manager:

- Review the token configurations that are supported by Credential Manager
- Install the iPhone 1.3 device definition file
- (Recommended) Require device binding
Review Supported Token Configurations

Credential Manager supports standard token configurations. If you want to issue tokens with alternative configurations (fob-style tokens, 6-digit tokencode, or 30-second tokencode duration), you must use the RSA Security Console.

To review the supported token configurations:
See “Supported Software Token Configurations” on page 11.

Install the iPhone 1.3 Device Definition File

Software tokens provisioned using RSA Credential Manager must be associated with a device definition file. This is an XML file that defines the capabilities and attributes of tokens that can be used with the RSA SecurID application. If you have never issued tokens for iPhone devices, you must install the device definition file into Authentication Manager.

If you have upgraded from a previous version of the iPhone application, and you want to use the iPhone device class GUID as the device binding attribute, you must install the iPhone 1.3 device definition file. Otherwise, select the iPhone 1.0 device definition file.

To install the device definition file:
See “Install the Device Definition File” on page 33.

(Recommended) Require Device Binding

You can configure Credential Manager to require users to enter a token binding attribute when requesting a software token for their iPhone device. You can require users to bind the token to their specific device or to the iPhone device type GUID.

To require device binding:

1. Configure Credential Manager to allow users to provide token attribute details, as described in “Step 1: Configure RSA Credential Manager Token Management Settings” on page 44.

2. If you require users to bind their token to their Device ID, instruct them to have the Device ID available before they request a token using the Self-Service Console. For information on obtaining the Device ID, see “Step 4: (Recommended) Obtain the Device ID for Binding the Token” on page 35.

3. If you require users to bind their token to the iPhone device type GUID, instruct them to leave the default binding option provided by Credential Manager.
Issuing Software Tokens Using RSA Credential Manager

To set up Credential Manager for self-service token provisioning, you must perform the tasks listed in the following table.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure Credential Manager token management settings.</td>
<td>“Step 1: Configure RSA Credential Manager Token Management Settings” on page 44</td>
</tr>
<tr>
<td>2. Replace the request approval notification e-mail template</td>
<td>“Step 2: Replace the Request Approval Notification E-Mail Template” on page 46</td>
</tr>
<tr>
<td>3. Allow users to create a self-service account.</td>
<td>“Step 3: Allow Users to Create a Self-Service Account” on page 46</td>
</tr>
<tr>
<td>4. Provide instructions for requesting a software token.</td>
<td>“Step 4: Provide Instructions for Requesting a Software Token” on page 46</td>
</tr>
<tr>
<td>5. Approve software token requests.</td>
<td>“Step 5: Approve Software Token Requests” on page 48</td>
</tr>
<tr>
<td>6. Instruct users on how to install the token.</td>
<td>“Step 6: Instruct Users on How to Install the Token” on page 49</td>
</tr>
</tbody>
</table>
Step 1: Configure RSA Credential Manager Token Management Settings

The following figure shows sample console configuration settings for the RSA SecurID application. Use the following procedure to configure the software token management settings that you want.

To configure Credential Manager to allow users to request a token:

1. From the RSA Security Console, click Setup > Component Configuration > Credential Manager.
2. From the Credential Manager Configuration Home page, under Token Provisioning, click Manage Tokens.
3. On the Manage Tokens page, under Software Token Types Available for Request, do one of the following:
   - Scroll to iPhone 1.3, and click Allow users to request iPhone 1.3 software tokens. This option supports binding tokens to the iPhone device class GUID.
   - Scroll to iPhone 1.0, and click Allow users to request iPhone 1.0 software tokens. This option is available if you provisioned software tokens to a previous version of the iPhone application. This option does not support binding tokens to the iPhone device class GUID.

The Display Name, Image location, and Description fields are automatically populated with the app name, device image, and app description that will be displayed in the Self-Service Console.
4. In the **Require User to Authenticate With** field, select the authentication requirement:
   - Select **Passcode** to provision a PINPad-style token.
   - Select **Tokencode** to provision a token that does not require a PIN.

5. In the **Supported Token Distribution Methods** field, do one of the following:
   - To dynamically provision tokens, click **Generate CT-KIP Credentials for Web Download**.
   - To distribute tokens using SDTID files, click **Issue Token File (SDTID)**. Go to step 7.

6. Leave the **Client Application URL** field blank.

7. (Optional) To make iPhone the default token type for all token requests, select **Make this token type the default option for all token requests**.

8. (Optional) In the **Make Default** field, click **Make this token type the default option for token requests**.

9. (Optional) Use the **Device Help Document URL** field to point to a URL where users can download the **Quick Start** document. Otherwise, leave the field blank.

10. (Optional) In the **Attribute Details** field, select **Allow users to edit token attribute details**.
    Selecting this option allows the user to enter a token binding attribute when requesting a token through the Self-Service Console.

11. (Optional) If you selected **Issue Token File (SDTID)** as the token distribution method, in the **Token File Password** field, select **The user needs to provide the password, to protect the token file**.

    | Token File Password Settings |
    |-----------------------------|
    | Token File Password:        | The user needs to provide the password, to protect the token file. |
    | File Format of Software Token: | ZIP | SDTID |

This option requires the user to create a password to protect the token file. The user must enter this password to install the token. Once the token has been successfully installed, the password is not used again.

12. If you selected **Issue Token File (SDTID)** as the token distribution method, in the **File Format of Software Token** field, select **SDTID**.

13. At the bottom of the screen, click **Save**.
Step 2: Replace the Request Approval Notification E-Mail Template

When you approve a request for a software token, Credential Manager generates an e-mail with instructions for importing the token. The default e-mail template provided by Credential Manager contains some supplementary information that is not needed to import the token.

To ensure an optimal user experience, RSA recommends that you replace the default Request Approval Notification e-mail template with a simplified e-mail template, credmgr_email_template.txt. You can find this file in the \util folder of the RSA SecurID product kit. The replacement template allows the user to automatically import a dynamically provisioned token by tapping a URL link in the e-mail notification. The link contains all of the required token data, including the one-time activation code.

To define e-mail settings:
1. From the RSA Security Console, click Setup > Component Configuration > Credential Manager.
2. On the Credential Manager Configuration Home page, under Token Provisioning, click Define e-mail settings.
3. In the Email Notification Templates section, select Request Approval Notification SW Tokens.
4. In the Body field, delete the existing code and replace it with the code in the replacement template, credmgr_email_template.txt.
5. Click Save.

Step 3: Allow Users to Create a Self-Service Account

To allow users to create a self-service account:
1. Provide a URL link to the Self-Service Console.
2. Instruct users to request an account.
3. Approve the account requests.

Step 4: Provide Instructions for Requesting a Software Token

The following procedure describes the steps for requesting a software token for an iPhone or iPad device using the RSA Self-Service Console. Use this information to guide first-time users through the process.

To request a software token using the RSA Self-Service Console:
1. Log on to the Self-Service Console URL.
2. In the My SecurID Tokens section, click Request a Token.
3. In the Request a Token drop-down box, select I need a specific software token. The Token Type section is displayed.
4. Scroll to and select **iPhone_1.3** or **iPhone 1.0**, as instructed by your administrator.
5. Under **Provide Your Token Details**, in the **DeviceSerialNumber** field, do one of the following, as instructed by your administrator:
   - Leave the default value.
   - Delete the default value, and enter your Device ID, as shown in the following figure.

   ![Provide Your Token Details](image)

   Leave the **Nickname** field blank. This field is provided for applications that support assigning the token a user-friendly nickname. RSA SecurID Software Token 1.3 for iPhone and iPad does not currently support token nicknames.

6. Under **Create Your PIN**, create and confirm a 4–8 digit PIN.

   **Important:** Memorize your PIN. If you forget your PIN, you will need to access the Self-Service Console to reset it before you can continue using your token.

7. In the **Reason for Token Request** box, enter the reason for your request. For example: “To access the corporate VPN client.”

8. Click **Submit Request**.
   A page opens with a request confirmation number.

9. Print the confirmation page for your records, and then click **OK** to return to the **My SecurID Tokens page**.
   The **My Requests** section lists your pending request. When your administrator approves the request, you will receive an e-mail notification.

### Step 5: Approve Software Token Requests

To complete the provisioning process, you must approve users’ software token requests.

**To approve the request:**
1. In the RSA Security Console, click **Administration > Provisioning**.
2. (Required) In the **Comment to User** field, enter any comments that you want included in the notification e-mail sent to the user.
3. Click **Approve Requests**.

### Software Token Request Approval E-mail

When you approve the user’s request for a software token, an e-mail is sent automatically to the user’s device e-mail address that is associated with the user’s Credential Manager account. RSA recommends that the same e-mail account be configured on the device to expedite the token provisioning process for the user.
The contents of the e-mail depend on whether you selected the CT-KIP delivery option or the SDTID delivery option when configuring Credential Manager.

**E-mail for CT-KIP Delivery**

If you configured Credential Manager to issue CT-KIP tokens, the user receives an e-mail similar to the following from Credential Manager.

```
Your new or additional software token request has been approved with the following comments from your administrator: admin: QE

Please ensure that the RSA SecurID application is installed on your device before attempting to import your software token.

**How to Import Your Software Token:**
1. Please view this e-mail on your mobile device.
2. Tap the link below.

This request was initiated by: smith [smith]
Confirmation #: 8b0fbfa771833640a033e29b14b675916
Approval Date: 1/2/2012 11:15:22 AM EDT

If you did not initiate this request, please contact your administrator with the information in this e-mail.
```

**E-Mail for Token File Delivery**

If you configured Credential Manager to issue SDTID files, the e-mail from Credential Manager contains a token file attachment, for example, “SampleToken.sdtid.”

**Step 6: Instruct Users on How to Install the Token**

The method for installing self-service software tokens depends on the distribution method that you selected, either CT-KIP or SDTID.

- The user installs a dynamically provisioned token by tapping the CT-KIP URL hyperlink displayed in the e-mail notification.
- The user installs a file-based token (SDTID file) from the e-mail attachment to the e-mail notification.

The following token installation procedures are provided for reference.
Install a CT-KIP Token—E-mail Link

Use this procedure to install a CT-KIP token from a hyperlink in the e-mail notification.

To install a CT-KIP token from a hyperlink embedded in an e-mail:

1. On your device, open the e-mail sent from Credential Manager.
2. Tap the hyperlink in the e-mail notification.
3. If prompted, enter the token activation code communicated to you by your administrator, and tap OK.
   Your token is installed, and the application starts.
4. After you have installed the token, delete the e-mail.

Install a File-Based Token—E-mail Attachment

Use this procedure to install a file-based token (SDTID file) from the token file attachment to the e-mail notification.

To install a file-based token from an e-mail attachment:

1. On your device, open the e-mail sent from Credential Manager.
2. Do one of the following:
   - Press and hold the e-mail attachment until a menu is displayed. On the menu, tap Open in RSA SecurID. Go to step 4.
   - Tap the e-mail attachment that contains your token.
      The contents of the token file are displayed.
3. At the top right of the screen, tap Open in RSA SecurID.
4. If prompted, use the device keyboard to enter the token file password into the Enter Password field, and tap OK.
   Your token is installed, and the application starts.
5. After you have installed the token, delete the e-mail.
Provisioning Tokens Using RSA Authentication Manager 6.1

This chapter describes how to provision file-based software tokens using RSA Authentication Manager 6.1. The chapter also describes the supported methods for delivering the tokens to iPhone or iPad devices.

Preparing to Provision Tokens

Before you begin the provisioning tokens using RSA Authentication Manager 6.1, keep the following in mind:

- RSA Authentication Manager 6.1 supports file-based provisioning. To use Dynamic Seed Provisioning (CT-KIP), you must be running RSA Authentication Manager 7.1.
- You must issue 128-bit (AES) tokens. The application does not support 64-bit (SID) tokens.
- Review the software token configurations supported with RSA Authentication Manager 6.1. For more information, see “Supported Software Token Configurations” on page 11.
- Determine the type of token that you want to issue: PINPad or PINless. For more information, see “RSA SecurID Authentication” on page 18.
- Determine the mechanism you will use to bind tokens. For more information, see “Device Binding” on page 14.
Use the information in the following table to become familiar with file-based provisioning, authentication server requirements, and iOS requirements. Click the links to see more information on the provisioning method that you plan to use.

<table>
<thead>
<tr>
<th>Provisioning Method</th>
<th>iOS Requirements</th>
<th>Reference</th>
</tr>
</thead>
</table>
| Issue SDTID file for delivery as e-mail attachment | • iPhone or iPod touch running iOS 4.0 or later  
• iPad running iOS 3.2 or later | • “Provisioning File-Based Tokens” on page 53  
• “Delivering File-Based Tokens as E-mail Attachments” on page 64 |
| Issue SDTID file for delivery using a URL link | • iPhone running iOS 3.0 or later  
• iPad running iOS 3.2 or later  
• iPod touch running iOS 4.0 or later | • “Provisioning File-Based Tokens” on page 53  
• “Delivering File-Based Tokens Using a Hyperlink” on page 65 |
Provisioning File-Based Tokens

With file-based provisioning, you configure a token record using the RSA Authentication Manager 6.1 Database Administration application. To maintain the security of the token file in transit, RSA recommends that you bind and password protect the token.

The following table lists the steps required for file-based provisioning, and the following sections describe each step.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure the software token record</td>
<td>“Configure the Token Record in RSA Authentication Manager 6.1” on page 53</td>
</tr>
<tr>
<td>2. Bind the token using token extension data (recommended)</td>
<td>“Bind the Token Using Token Extension Data” on page 56</td>
</tr>
<tr>
<td>3. Deliver the token to the user’s device</td>
<td>“Delivering File-Based Tokens as E-mail Attachments” on page 64</td>
</tr>
<tr>
<td></td>
<td>“Delivering File-Based Tokens Using a Hyperlink” on page 65</td>
</tr>
</tbody>
</table>

Before You Begin

Before you can issue SDTID files in RSA Authentication Manager 6.1, you must do the following:

- Add token records to the database
- Add users and assign tokens
- Add an Agent Host
- Activate the user on an Agent Host

Note: Instructions for the tasks listed above are provided in the Database Administration application Help.

Configure the Token Record in RSA Authentication Manager 6.1

This section describes key steps in using RSA Authentication Manager 6.1 to configure token records for use with the RSA SecurID application. For more information, see the Database Administration application Help.
To configure a token record in RSA Authentication Manager 6.1:

1. Open the Database Administration application, and select **Tokens > Issue Software Tokens**.

2. Accept the default algorithm (AES SDTID 3.0).

3. Under **Options**, leave **Enable Copy Protection** selected, and select **Edit Extension Data**.

4. If you want to protect the token file with a password, select **Password Protect**, and then enter and confirm a static password of up to 24 case-sensitive characters, or select another password protection option. For information on other password protection options, click the **Help** button at the bottom right of the screen.

5. Under **Output**, in the **Target Directory** field, browse to the directory on your system to which you want the token file to be exported.

6. Under **Output**, select **One Token Per File**.
7. Click Next, and select One user.

8. Click Next, and select the user for whom you want to issue the token. Click OK, and click Next.

9. Do one of the following:
   - To require passcode authentication, leave Do not change selected or select User authenticates with passcode.
   - To issue a token that does not require a PIN, select User authenticates with tokencode only.

10. Click Next, and click Yes.
    The Edit Token Extension Data screen opens. Use the instructions in the following section to bind the token to the user’s device.
Bind the Token Using Token Extension Data

To bind a software token in RSA Authentication Manager 6.1, you must edit token extension data. RSA recommends binding iPhone or iPad software tokens to the Device ID or the iPhone device type GUID. To determine which option to use, see “Determine Your Device Binding Mechanism” on page 15.

Bind the Token to a Device ID

Before you can bind a token to a Device ID, you must obtain the ID information from the user. For more information, see “Step 4: (Recommended) Obtain the Device ID for Binding the Token” on page 35. This section uses binding to a Device ID as an example.

To bind a token to a Device ID:

1. On the Edit Token Extension Data page, in the **Key** field, enter **DeviceSerialNumber**.
2. In the **Data** field, enter the Device ID.
3. Click **Save**, and click **Exit**.
   The result should look similar to the following figure.

Edit Token Extension Data

<table>
<thead>
<tr>
<th>Key</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DeviceSerialNumber</strong></td>
<td><strong>2b6f0cc904d1376e2e1730235f56</strong></td>
</tr>
</tbody>
</table>

Token Serial #: 000000500008
Bind the Token to the Device Type GUID

To bind a token to the device type GUID, you must edit token extension data, using the device type GUID as the data value.

To bind a token to the device type GUID:
1. On the Edit Token Extension Data page, in the **Key** field, enter **DeviceSerialNumber**.
2. In the **Data** field, enter the following device type GUID:
   556f1985-33dd-442c-9155-3a0e994f21b1
3. Click **Save**, and click **Exit**.
   The result should look similar to the following figure.

![Edit Token Extension Data](image)
# Delivering Software Tokens

This chapter describes how to deliver software tokens issued in RSA Authentication Manager to iPhone and iPad devices.

## Token Delivery Mechanisms

RSA provides the mechanisms listed in the following table to deliver software tokens to iPhone and iPad devices.

<table>
<thead>
<tr>
<th>Delivery Mechanism</th>
<th>Provisioning Mechanism</th>
<th>Supported Devices</th>
<th>Reference</th>
</tr>
</thead>
</table>
| E-mail hyperlink (CT-KIP)   | Dynamic Seed Provisioning    | • iPhone with iOS 3.0 or later  
• iPad with iOS 3.2 or later  
• iPod with iOS 4.0 or later | "Delivering Dynamically Provisioned Tokens Using a Hyperlink" on page 60      |
| E-mail attachment as a hyperlink | Compressed Token Format     | • iPhone with iOS 3.0 or later  
• iPad with iOS 3.2 or later  
• iPod touch with iOS 4.0 or later | "Delivering File-Based Tokens Using a Hyperlink" on page 65                 |
| E-mail attachment SDTID file |                              | • iPhone with iOS 4.0 or later  
• iPad with iOS 3.2 or later  
• iPod touch with iOS 4.0 or later | "Delivering File-Based Tokens as E-mail Attachments" on page 64             |
Delivering Dynamically Provisioned Tokens Using a Hyperlink

To deliver dynamically provisioned tokens to users’ devices using CT-KIP, you must create an e-mail message with a hyperlink containing the CT-KIP token data, and send it to the user’s device. The user installs the token by tapping the hyperlink.

You must perform the tasks in the following table, in order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Issue a token using CT-KIP as the distribution method.</td>
<td>“Configure the Token Record in RSA Authentication Manager 7.1” on page 33 “Specify the Token Distribution Method” on page 38</td>
</tr>
<tr>
<td>2. Construct a URL link.</td>
<td>“Step 2: Construct a URL Link” on page 61</td>
</tr>
<tr>
<td>3. Compose an e-mail message with a hyperlink containing the token data, and send it to the user’s device.</td>
<td>“Step 3: Compose and Send an E-mail Message” on page 62</td>
</tr>
<tr>
<td>4. Instruct the user on how to install the token.</td>
<td>“Step 4: Instruct Users on How to Install the Token” on page 63</td>
</tr>
<tr>
<td>5. Verify successful execution of the CT-KIP protocol.</td>
<td>“Step 5: Verify Successful Execution of the CT-KIP Protocol” on page 63</td>
</tr>
</tbody>
</table>

**Step 1: Issue a Dynamically Provisioned Token**

Configure the token record and issue a dynamically provisioned token, if you have not already done so.

**To configure a token record and issue a dynamically provisioned token:**

See the following sections:

- “Configure the Token Record in RSA Authentication Manager 7.1” on page 33
- “Specify the Token Distribution Method” on page 38
Step 2: Construct a URL Link

When you issue a dynamically provisioned token in Authentication Manager, the Distribute Software Token page displays the CT-KIP server URL link in the Service Address field, and the token activation code in the Activation Code field, as shown in the following figure.

To allow the device to install the CT-KIP token, you must construct a larger URL link consisting of prefixed text combined with your CT-KIP server URL and the token activation code.

To construct the URL link:

Construct the URL link as follows:

```plaintext
```

The link must start with

```plaintext
com.rsa.securid://ctkip?url=
```

Note: Earlier versions of the RSA SecurID application required the URL to start with "com.rsa.securid.iphone". To preserve legacy scripts, you can use the earlier URL with application version 1.3.

- `https://customer_ctkip_server_url` represents your CT-KIP server-side URL. The CT-KIP URL must precede the activation code in the URL link. Use the same CT-KIP URL for each new token. Note that the CT-KIP URL is labeled Service Address in RSA Authentication Manager 7.1.

- `&activationCode=activation_code` represents the one-time activation code associated with the token. Append the activation code string to the URL link. You must use a different activation code for each new token. Including the activation code in the URL link is recommended.
  - If you include the activation code string in the URL link, the user does not enter the activation code when installing the token.
– If you do not include the activation code string in the URL link, you must securely transmit the activation code to the user separately. The user must enter the activation code to complete the token installation.

The following example shows a properly constructed CT-KIP URL link with an activation code:

```
&activationCode=00108310
```

The following example shows a properly constructed URL link without an activation code:

```
```

The following example shows a properly constructed URL link with an activation code, using the legacy “com.rsa.securid.iphone” string:

```
&activationCode=00108310
```

**Step 3: Compose and Send an E-mail Message**

Using Microsoft Outlook with Microsoft Exchange Client, create an e-mail message that contains the URL that you constructed as a hyperlink.

**Before You Begin**

- The RSA SecurID application must be installed on the user’s device. If the application has not been installed, the token cannot be installed.
- The device must have network connectivity.
- Securely transmit the activation code to the user if you did not include it in the URL link that you constructed.
- If you use a self-signed certificate in your Authentication Manager CT-KIP deployment, the application displays a warning that the certificate is not trusted and prompts the user to accept or reject the certificate. Instruct the user to accept the certificate.
- Instruct the user to delete the e-mail message containing CT-KIP data as soon as the token has been installed. This measure helps prevent an unauthorized user who might have access to the device from wrongfully obtaining the token.
To compose and send an e-mail with a hyperlink:

1. To ensure that you can create a working hyperlink, set the e-mail message format as follows.
   - For Microsoft Outlook 2007, set the message format to HTML.
   - For Microsoft Outlook 2003, make sure that Microsoft Word is not selected as your default e-mail editor, and set the message format to HTML.

2. Compose a message, using text similar to the following in the message body:
   Tap this link to install your token. When done, delete this message.

3. Select the text to use as the hyperlink, for example, “this link,” and create a hyperlink that contains the URL that you constructed.

4. Send the e-mail to the user’s device.

Step 4: Instruct Users on How to Install the Token

Provide the end-user Quick Start document, or instruct users to follow the instructions in the application Help.

Step 5: Verify Successful Execution of the CT-KIP Protocol

To verify successful communication between the CT-KIP server and the CT-KIP client:

Access the Administration Activity Monitor in the RSA Security Console (Reporting > Realtime Activity Monitors > Administration Activity Monitor).

The following example shows that a CT-KIP key for the token was delivered to the device and that the activation code was deleted from the security domain.

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity Key</th>
<th>Description</th>
<th>Result</th>
<th>Administrator User ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-05-07</td>
<td>Generate CTKIP Key</td>
<td>Administrator &quot;SYSTEM&quot; attempted to generate CTKIP key for CTKIP data &quot;Token&quot; stored in identity source &quot;SYSTEM&quot; managed in security domain &quot;SystemDomain”</td>
<td>Success</td>
<td>SYSTEM</td>
</tr>
<tr>
<td>2010-05-07</td>
<td>Delete CTKIP Authcode</td>
<td>Administrator &quot;SYSTEM&quot; attempted to delete CTKIP authcode &quot;Token&quot; managed in security domain &quot;SystemDomain”</td>
<td>Success</td>
<td>SYSTEM</td>
</tr>
</tbody>
</table>

These results typically indicate that the token was successfully imported to the application. However, in some cases the Activity Monitor might report successful execution of the CT-KIP protocol, but other factors might prevent a successful import. For example, the token would not be imported if the iPhone or iPad device has network connectivity problems.

If the Activity Monitor does not display any activity, the problem is probably a connectivity issue involving the device and the CT-KIP service.
Delivering File-Based Tokens as E-mail Attachments

You can deliver file-based tokens (SDTID files) by sending an e-mail with a token file attachment to the user’s device e-mail address. This delivery mechanism requires the following device and iOS versions:

• iPhone or iPod touch devices running iOS 4.0 or later
• iPad devices running iOS 3.2 or later

Note: To deliver SDTID files to devices running an earlier iOS version, see “Delivering File-Based Tokens Using a Hyperlink” on page 65.

Before You Begin

Before you deliver a file-based token (SDTID file):

• The RSA SecurID application must be installed on the user’s device. If the application has not been installed, the token cannot be installed.
• If you protected the token with a password, securely communicate the token file password to the user.
• Do not encrypt the e-mail using S/MIME, as this will cause an error when the user attempts to install the token.
• Instruct the user to delete the e-mail after the token has been installed to the device. This measure helps prevent an unauthorized user who might have access to the device from obtaining the token.

E-mail a Token File Attachment

Send an e-mail containing the token file attachment to the e-mail address associated with the user's device.

Instruct Users on How To Install the Token

Provide the end-user Quick Start document or instruct users to follow the instructions in the application Help.
Delivering File-Based Tokens Using a Hyperlink

**Important:** You must use the method described in this section to deliver file-based tokens to devices running iOS 3.0.x or iOS 3.1.x.

To deliver file-based tokens with a hyperlink, you must use the RSA SecurID Software Token Converter command line utility to convert the SDTID file to a Compressed Token Format (an 81-digit numeric string containing the token data). The command output is a text file containing the token data appended to a URL. You create an e-mail with a hyperlink containing the URL, and send it to the user. The user taps the hyperlink to install the token.

If you password protect the token in Authentication Manager, the user must enter the token password to complete the token installation. After the user correctly enters the password, the password is not used again.

The following figure shows the provisioning process for converted SDTID files.
Provisioning tokens converted to Compressed Token Format involves the following steps, which are described in the following associated sections.

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Issue the software token as an SDTID file.</td>
<td>“Configure the Token Record in RSA Authentication Manager 6.1” on page 53</td>
</tr>
<tr>
<td>2. Convert the token file to Compressed Token Format.</td>
<td>“Step 2: Convert the Token File” on page 67</td>
</tr>
<tr>
<td>3. Compose an e-mail message with a hyperlink containing token data, and send it to the user’s device.</td>
<td>“Step 3: Compose and Send an E-mail Message” on page 68</td>
</tr>
<tr>
<td>4. Instruct users on how to install the token.</td>
<td>“Step 4: Instruct Users on How to Install the Token” on page 68</td>
</tr>
</tbody>
</table>

**Step 1: Issue the Software Token as an SDTID File**

Issue the software token as an SDTID file, if you have not already done so.

**To issue the software token as an SDTID file:**

See “Configure the Token Record in RSA Authentication Manager 6.1” on page 53.
Step 2: Convert the Token File

After issuing the token file (SDTID file), you must use the RSA SecurID Software Token Converter to convert it to a format that can be installed to an iPhone or iPad device. The Token Converter is a free command line utility that converts a software token record that has been issued as an SDTID file to a Compressed Token Format consisting of an 81-digit string.

To convert a token file:

2. Follow the instructions in the Token Converter Readme. Observe the following requirements:
   - Convert only one token at a time and only one token per token file.
   - Use either the -mobile or -iphone option to specify that the output of the Token Converter will be a text string appended to a specific URL that can be installed to a supported iPhone device.

   Note: The -mobile option is recommended for first-time software token provisioning to the RSA SecurID application. The -iphone option supports legacy scripts that were written against previous versions of the Token Converter.
   - Use the -o filename option to output the string containing the converted token data to a text file that you can send to the user. If you do not use the -o option, the output is written to the screen.
   - Use the -p password option if you password-protected the token file in Authentication Manager.
   - Do not use the -f or the -v option. The -iphone and -mobile options ignore the -f and -v options.
   - If you bound the token in Authentication Manager, the binding information will be transmitted as part of the token data.

Token Converter Output

When you convert a token using the -mobile (or -iphone) and -o filename options, the output is a text file that contains token data appended to a specific URL.

The following example shows sample output using the -mobile option:

```
com.rsa.securid://ctf?ctfData=00206816463136011170432774461076631720647716463
2456201026172002115044627167126500
```

The following example shows sample output using the -iphone option:

```
com.rsa.securid.iphone://ctf?ctfData=00206816463136011170432774461076631720647716463
164632456201026172002115044627167126500
```
Step 3: Compose and Send an E-mail Message

Using Microsoft Outlook with Microsoft Exchange Client, compose an e-mail message containing a hyperlink to the URL with the token data.

Before You Begin

• The RSA SecurID application must be installed on the user’s device. If the application has not been installed, the token cannot be installed.

• The device must have an Internet connection.

• If you protected the token with a password, securely communicate the token file password to the user.

• Instruct the user to delete the e-mail containing the token data as soon as the token has been installed. This measure helps prevent an unauthorized user who might have access to the device from wrongfully obtaining the token.

To compose and send an e-mail with a hyperlink:

1. To ensure that you can create a working hyperlink, set the e-mail message format as follows.
   • For Microsoft Outlook 2007, set the message format to HTML.
   • For Microsoft Outlook 2003, make sure that Microsoft Word is not selected as your default e-mail editor, and set the message format to HTML.

2. Compose a message, using text similar to the following in the message body:
   Tap this link to install your token. When done, delete this message.

3. Select the text to use as the hyperlink, for example, “this link,” and create a hyperlink to the URL with the token data.

4. Send the e-mail to the user’s device.

Step 4: Instruct Users on How to Install the Token

Provide the end-user Quick Start document or instruct users to follow the instructions in the application Help.
Troubleshooting

This chapter describes issues that might occur with RSA SecurID Software Token 1.3 for iPhone and iPad, the RSA SecurID application, and their corresponding solutions.

Customer Support Information

If you need to contact RSA Customer Support in order to resolve an issue, have the following information available:

- Date and time set on the device
- The information presented on the Info screen
- Device name
- Cellular network or wireless provider
- Operating system version
- Device model number

Include a detailed description of the problem that can be used to form the basis for steps to reproduce the issue.

Application Installation Problems

This section describes problems users might encounter when installing the application, and provides workarounds.

- The user has an unsupported device. For a list of hardware requirements, see “System Requirements” on page 9.
- The device does not have enough space to install the application. The user must free up some space on the device. See “System Requirements” on page 9.
- A network failure occurred when the user attempted to download the application from the Apple App Store. Instruct the user to retry the download.
Token Installation Problems

This section describes problems users might encounter when they attempt to install a software token, and provides workarounds.

Application Is Not Installed

The user cannot install a token because the RSA SecurID application has not been installed on the device. Instruct the user to install the application from the Apple App Store before attempting to install a token.

Errors Issuing the Token in RSA Authentication Manager

Token installation problems can result from errors in issuing the token in Authentication Manager, for example:

• The token is not intended for an iPhone device. If you issue tokens in RSA Authentication Manager 7.1, verify that you installed the iPhone 1.3 device definition file or that you previously installed the iPhone 1.0 device definition file. Also verify that you selected “iPhone 1.3” or “iPhone 1.0” as the device type when issuing tokens.

• The token device binding is incorrect. For example, you may have entered an incorrect Device ID when binding the token to a device. Correct the token device binding and reissue the token.

• The token type is not supported (64-bit, SID). Issue a 128-bit (AES) token.

• The death date of the token lifetime configured in Authentication Manager has passed.

Invalid Token

The user received an “Invalid Token” message. This can happen if the administrator makes an error when issuing the token in Authentication Manager.

File Password Errors

The user may not be able to complete the token installation due to errors in entering the token file password, for example:

• The user forgot the token file password. The user must contact the administrator for the token file password.

• The user received an “incorrect password” message. The user must enter the correct password.
Token Converter Errors

Errors in using the Token Converter may prevent a token from being converted properly. For example:

- The token was not converted properly with the Token Converter utility. For example, you did not specify the `-p password` option when converting a password-protected token file or you did not specify the required `-iphone` or `-mobile` option.
- The SDTID file could not be converted properly with the Token Converter utility because the file contained double-byte characters in the `UserFirstName`, `UserLastName`, or `UserLogin` fields. For more information, see “Known Issues” in the RSA SecurID Software Token Converter Readme.

CT-KIP URL Format Errors

The CT-KIP URL link containing the token information is not formatted correctly. To format the link correctly, see “Step 2: Construct a URL Link” on page 61.

E-mail Message Format Errors

An incorrect message format was used to create the hyperlink with the token data. You must embed the CT-KIP URL address into a hyperlink, and use one of the following formats:

- For Microsoft Outlook 2007, set the message format to HTML.
- For Microsoft Outlook 2003, make sure that Microsoft Word is not selected as your default e-mail editor, and set the message format to HTML.

Network Communication Errors

The e-mail message containing the hyperlink with the token data did not reach the user’s device. This can happen in rare cases because of a network communication failure. Instruct the user to refresh the mailbox. If necessary, resend the e-mail.
Authentication Problems

The following sections describe the most common reasons that a user is unable to authenticate with a SecurID token.

User Error

The user may have made one of the following errors:

- The token was disabled due to excessive failed logon attempts. Check the Authentication Manager logs. If the token is not disabled (or expired), ask the user to read you the current tokencode and the subsequent tokencode displayed on the device. After you obtain the pair of tokencodes, resynchronize the token with the Authentication Manager server.
- The user has been issued a token that requires a PIN, and the user attempted to authenticate before creating the PIN. Instruct the user to follow the instructions in the end-user Quick Start or application Help to set a PIN.
- The user entered an incorrect PIN or entered the PIN in the wrong location. For example, the user may have entered the tokencode, followed by the PIN instead of entering the PIN, followed by the tokencode.

Error Exporting Tokens

When issuing a token in RSA Authentication Manager, you chose to have multiple tokens exported in a single SDTID file. When you ran the Token Converter, it properly converted the first token in the file, but that token was intended for a different user, so the user’s attempt to authenticate failed. You must reissue the token, making sure that each SDTID file contains only one token.

Time Synchronization Problem

The time on the device may be out of synchronization with the clock settings in Authentication Manager. Instruct the user to access the Info screen in the RSA SecurID application and to read you the time shown in the GMT field.

Expired Token

The user’s token may have expired. If this occurs, the application displays a “Token Expired” message. The user must contact the administrator to request a replacement token.
Error Messages

If the device displays any of the following error messages, the user must contact the administrator to request a replacement token:

- Invalid URL.
- Token install failed.
- Error communicating with server. Token install failed.
- Token not intended for this device. Token install failed.
- Token expired. Request a replacement token.
- Invalid token.
## Index

### A
- activation code, 13
  - generating, 38
  - system-generated, 38
- Administration Activity Monitor, 63
- application
  - installing, 24
- approving a self-service token request, 48
- authentication issues, troubleshooting, 72
- authentication requirement
  - setting in RSA Authentication Manager 6.1, 55
  - setting in RSA Authentication Manager 7.1, 34
- authentication servers, 10
- automated token provisioning products, 10

### B
- binding a token, 35
  - in RSA Credential Manager, 45
  - options for, 15
- binding mechanism
  - iPhone device type, 15

### C
- Compressed Token Format, 65
  - defined, 67
  - illustrated, 65
- configurations, software token, 11
- configuring
  - file-based token in RSA Authentication Manager 7.1, 40
  - token record in RSA Authentication Manager 6.1, 54
  - token record in RSA Authentication Manager 7.1, 33
- converted token
  - delivering, 67
  - required link format, 67
- Cryptographic Token Key Initialization Protocol (CT-KIP), 13
- CT-KIP, 13
- CT-KIP protocol, verifying in
  - RSA Authentication Manager 7.1, 63
- CT-KIP URL link format, 61
- Customer Support, contacting, 8

### D
- Database Administration application, 54
- database encryption key, 16
- delivering token
  - using Dynamic Seed Provisioning, 31, 60
- device binding
  - overview, 14
  - device binding mechanisms, comparing, 15
  - device definition file, 33
  - Device ID, 14, 35
  - device identifier, 35
  - device type, 14, 34
  - device type GUID, 14
  - DeviceSerialNumber field, 36
  - device-specific attributes, 34
  - Displayed Value field, 37
  - documentation list, 7
  - Dynamic Seed Provisioning, 13, 31
  - illustrated, 31

### E
- editing token extension data, 56
- error messages, 73
- exporting token file, 54

### F
- file-based provisioning, 13
- fob-style software token, 20
- format of converted token URL hyperlink, 67

### G
- generating activation code, 38
- getting support, 8

### H
- helping users get started, 25

### I
- installation
  - options, 24
  - troubleshooting, 69
- installation application
  - illustrated, 24
installing application, 23
   directly, 24
   through sync, 24
iPhone device definition file, 33
iPhone device type, 14

N
Nickname field, 36

P
passcode, 34, 45
password protection, 15
PIN requirement, 34
PINless token, 21
PINPad-style software token, 19, 37
pre-deployment tasks, 23
provisioning prerequisites, 29, 51, 59
provisioning token
   using Compressed Token Format, 65
   using Dynamic Seed Provisioning, 31

R
request approval notification template, 46
requesting a token through RSA Self-Service
   Console, 46
requesting a token using RSA Self-Service
   Console, 46
RSA Authentication Deployment
   Manager, 10
RSA Authentication Manager
   user authentication requirement, 34
RSA Credential Manager, 10
   editing the request approval notification
   template, 46
   sample settings, 44
RSA SecurID authentication overview, 18
RSA Self-Service Console, 46

S
SDTID file format, 54
SDTID files, 13
   issuing in RSA Authentication Manager
      7.1, 40
   password protecting, 15
selecting user authentication requirement
   in RSA Authentication Manager 6.1, 55
   in RSA Authentication Manager 7.1, 34
self-service token, approving request for, 48
software token
   binding to device in RSA Authentication
      Manager 7.1, 35
   device type, 34
   fob style, 20
   PINless, 21
   PINPad style, 19, 37
   supported configurations, 11
software token attributes
   supported in RSA Authentication
      Manager 6.1, 53
   supported in RSA Authentication
      Manager 7.1, 37
   supported in RSA Credential
      Manager, 42
support and service, 8
synchronizing clock settings, 11
system requirements, 9
system-generated activation code, 38

T
token attributes
   supported in RSA Authentication
      Manager 7.1, 37
   supported in RSA Credential
      Manager, 42
token configurations
   supported with RSA Credential
      Manager, 42
token database, 16
token extension data, editing, 56
token file, 13
   exporting, 54
token file password
   allowing user to set in RSA Credential
      Manager, 45
   assigning in RSA Authentication
      Manager 7.1, 40
   setting in RSA Credential Manager, 45
token installation, troubleshooting, 70
token provisioning
   Dynamic Seed Provisioning, 13
   file-based, 13
   mechanisms, 13
token record
   configuring in RSA Authentication
      Manager 6.1, 54
   configuring in RSA Authentication
      Manager 7.1, 33
token security
during provisioning, 14
on the device, 16
tokencode, 45
requirement, 34
tokencode setting in RSA Authentication Manager 6.1, 55
tokens
security during provisioning, 14
troubleshooting, 69

U
UDID, 14
updating to application version 1.2, 25
URL link format, 61
user authentication requirement
    in RSA Authentication Manager 7.1, 34