



## RSA SecurID Ready Implementation Guide

Last Modified: March 12, 2008

### Partner Information

---

Product Information	
Partner Name	SanDisk
Web Site	<a href="http://www.sandisk.com">www.sandisk.com</a>
Product Name	Cruzer Enterprise / SanDisk CMC
Version & Platform	2.0.5.20 /
Product Description	<p>Cruzer® Enterprise is a USB drive specifically designed to meet the unique security, compliance, and manageability needs of enterprise-size businesses. With hardware based encryption and mandatory access control, Cruzer Enterprise helps IT managers more effectively protect information on company issued portable storage devices. Cruzer Enterprise drives can also function as RSA SecurID Authenticators for secure remote access to corporate resources.</p> <p>SanDisk Central Management and Control (CMC) software is an innovative software solution that allows corporate IT departments to centrally manage company issued Cruzer Enterprise USB devices both inside and outside the corporate environment. SanDisk CMC can remotely manage and provision RSA SecurID credentials to Cruzer Enterprise USB drives.</p>
Product Category	RSA SecurID Ready Authenticator

# SanDisk®



## Solution Summary

---

Based on the partnership between RSA and SanDisk, two-factor authentication and secure storage are now available on a single, company-issued USB flash drive – ideal for employees who want to travel light yet be fully connected, ideal for IT departments concerned with data security and regulatory compliance challenges. The RSA SecurID Software Authenticator is integrated with the SanDisk® Cruzer® Enterprise USB flash drive, allowing access to applications protected by RSA SecurID, while offering users the native security and high performance of the SanDisk Cruzer Enterprise. What's more, this drive is managed and controlled by IT departments with SanDisk Central Management and Control (CMC) Software to provide continuous enforcement of company policy, tracking and monitoring activity beyond the corporate network.

Functional Description	
Authenticator provides its own GUI to present tokencode	Yes
Authenticator can securely store token seed record	Yes
Authenticator supports copy/paste of tokencode	Yes
Authenticator supports multiple seed records	Yes (Number)
Authenticator supports passphrase protection of application	Yes (drive unlock)
Authenticator provides RSA Software Token Automation (user enters only PIN to authenticate)	N/A
Partner product provisions Authenticator (creates account, assigns token, delivers seed to device)	Yes
Authenticator supports CT-KIP provisioning protocol	N/A





# Product Configuration for Interoperability

---

## Introduction

SanDisk Cruiser® Enterprise USB drives are specifically designed to meet the unique security, compliance, and manageability needs of enterprise-size businesses. It does not rely upon users to decide which files to secure. Instead it requires **mandatory access control** for all files, storing them in an encrypted, password-protected partition. This provides security and protects stored data in the event of device loss or theft.

Cruzer Enterprise features ultra fast transfer speeds, a simple interface, and the ability to plug-and-play. It's intuitive and practical enough for users to start using immediately. With hardware based encryption and mandatory access control, Cruzer Enterprise helps IT managers more effectively protect information on company issued portable storage devices.

Cruzer Enterprise is managed by SanDisk's CMC (Central Management & Control) server software, making it easy for IT managers to provision and monitor flash drives throughout their lifecycle. At the same time, Cruzer Enterprise flash drives with RSA SecurID software tokens provide two-factor authentication for network access – requiring something users have (the one-time password generated on the drive) and something users know (their SecurID PIN).

This “two-for-one” solution gives users a single device for secure data storage and strong authentication – a true alternative to carrying both a flash drive and a separate RSA SecurID hardware authenticator.

---

 **Note:** As part of this solution, the SanDisk CMC server is required to provision RSA SecurID Software Authenticators to the Cruzer Enterprise Drive.

---

## Before You Begin

This section provides instructions for using the partners' product as an RSA SecurID Authenticator and to provision an RSA Authentication Manager Server. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding. Before installing the CMC RSA Connector, ensure that your Cruzer Enterprise drives are being successfully managed by the SanDisk CMC Server and that users can login securely to unlock their drives.

---

 **Note:** Version 2.0 Software Tokens are not supported for use with SanDisk Cruiser Enterprise/CMC. Only version 3.0 (AES) Software Token seed records are supported.


---



## Installing the SanDisk CMC RSA Connector

The SanDisk CMC RSA Connector uses RSA Authentication Manager Administrative APIs (and thus the Authentication Manager **apidemon** service) to automatically provision and manage RSA Software Authenticators. When working with a version 6.1 RSA Authentication Manager Server, create a system environment variable `APIDEMON_ALT_PATH` that is set equal to the prog directory of your RSA Authentication Manager installation. By default, the value of this path is `C:\Program Files\RSA Security\RSA Authentication Manager\prog`. Reboot the machine after adding this environment variable.




---

 **Note:** Consult RSA SecureCare Online Solution a29520 for more information on enabling the apidemon on a version 6.1 Authentication Manager Server.

---

Proceed with the instructions in the section entitled Installing the CMC Connector for RSA SecurID Authentication in the Cruiser Enterprise CMC Setup and Deployment Guide. Double-click `Setup.exe` in the CMC RSA Connector folder to begin the CMC connector installation. Follow the setup prompts as outlined in the document above to complete the installation.


After restarting the machine, you can start the SanDisk CMC RSA Connector service (Token Server Support) from Administrative Tools \Services:

 Terminal Services	Allows user...	Started	Manual	Local System
 Terminal Services S...	Enables a ...	Disabled	Disabled	Local System
 Themes	Provides u...	Disabled	Disabled	Local System
 Token Server Support		Started	Automatic	.\Administrator
 Uninterruptible Pow...	Manages a...		Manual	Local Service

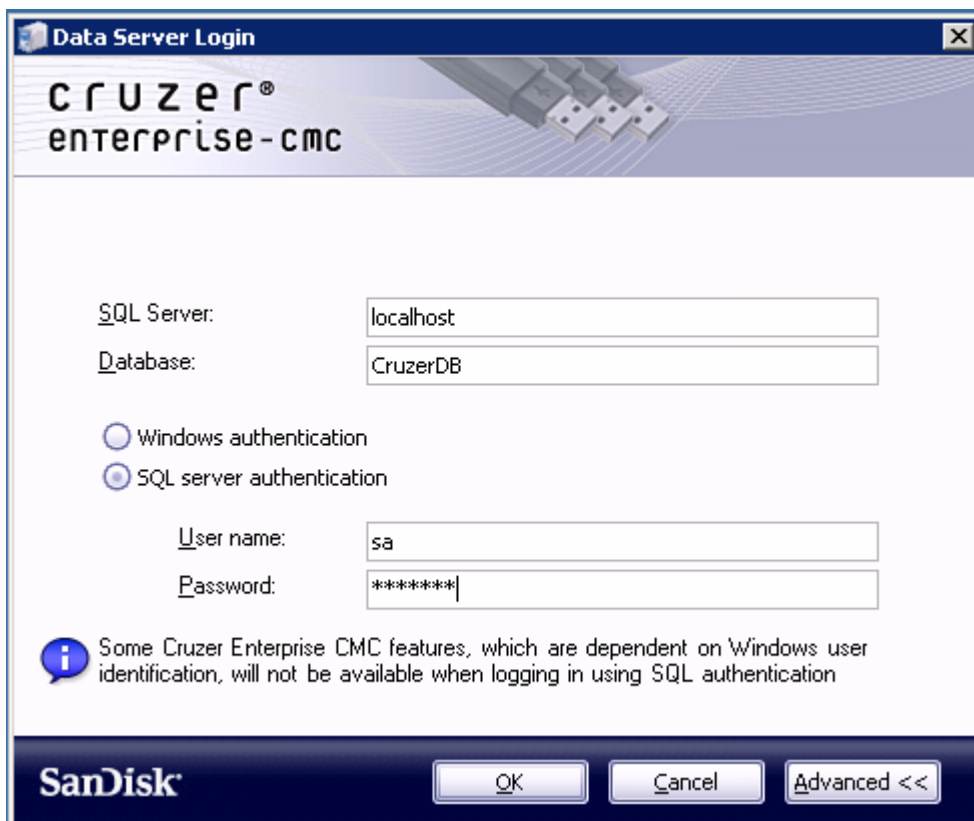
Once you have verified that the SanDisk CMC RSA Connector is starting properly, you will be able to assign RSA SecurID Software Authenticators and provision them to users directly from the SanDisk CMC Administrative Console.



## Provisioning RSA SecurID Software Authenticators to SanDisk Cruiser Enterprise Users

 **Note:** This section assumes that users have already activated and can log in to their Cruiser Enterprise device. For information on registering users and managing devices, please consult the Cruiser Enterprise CMC Setup and Deployment Guide.

1. To begin, log in to the SanDisk CMC Administrative Console:



2. Highlight the configuration set you wish to manage and select the Configuration tab:



3. On the Configuration tab, select **RSA SecurID** from the selection list:



General Info

Backup Component

Content Auditing

**RSA SecurID**

Display a custom logo on Cruiser Enterprise login screens

**Support**

URL:

4. Select Enable RSA SecurID Authentication Plug-In and enter the RSA Connector URL:

**RSA SecurID Settings**

Enable RSA SecurID Authentication Plug-in

**RSA SecurID Ready**

**RSA Authentication Manager Server**

RSA Connector URL:

After entering this information, click the  button to save your changes. Now that the connector information has been stored, you can proceed to assigning an RSA Software Authenticator to an end user.

Highlight the user you wish to provision and select the **Configuration** tab:

RSA

- Administrator
- Harvey Jones
- Gavin J. Carlson
- Sheila G. Carlson**



5. Choose **RSA SecurID** from the selection list as before, and select the **Add** button in the **Tokens** dialog:

**RSA SecurID Settings** i

Enable RSA SecurID Authentication Plug-in **RSA SecurID<sup>®</sup> Ready**

**RSA Authentication Manager Server**

RSA Connector URL:

**Tokens**

i All token assignments and allocations occur immediately. The Save button only affects the Enable/Disable Application check box.

Token seria...	Token user	Issue date	Device serial	Device owner
000039403873	scarlson	3/5/2008	0f112570a061...	Sheila G. Carlson
000039403874	scarlson	3/6/2008	0f112570a061...	Sheila G. Carlson

6. The **Add Tokens** dialog box will then be displayed. Enter relevant information for the end user, such as the user's RSA SecurID login and First Name/Last Name, and click the **Add** button.

If using variables as in the example below, this information will be come from the user's Active Directory/SanDisk CMC User account. Also, if a user with the given login does not exist in the RSA Authentication Manager Server, then an account will be created:



**Add Tokens** [X]

Login: [%AccountName%] [...]

First name: [%GivenName%] [...]

Last name: [%SN%] [...]

[Empty text box]

[Add] [Cancel]

7. The CMC Administrator will then be prompted for the administrative credentials established during installation of the connector:

**RSA Authentication Manager** [X]

 Please enter your RSA Authentication Manager administrative credentials in order to perform administrative actions.

User name: Administrator

Password: [Redacted]

Domain: PE

[OK] [Cancel]

Enter the appropriate information and select **OK**.



8. The **Add Tokens** window should then show the status of the Add Token operation:

**Add Tokens**

Login: %AccountName%

First name: %GivenName%

Last name: %SN%

Summary:

Tokens requested: 1  
Tokens allocated: 1  
Tokens failed: 0

Add Close

9. If the operation was successful, you should see this token now listed as assigned to the given user:

RSA SecurID Settings

Enable RSA SecurID Authentication Plug-in

**RSA SecurID Ready**

**RSA Authentication Manager Server**

RSA Connector URL:  
<https://vm3075.pe.rsa.net/CmcRsaTokenServer/>

**Tokens**

*All token assignments and allocations occur immediately. The Save button only affects the Enable/Disable Application check box.*

Token seria...	Token user	Issue date	Device serial	Device owner
000039403873	scarlson	3/5/2008	0f112570a061...	Sheila G. Carlson
000039403874	scarlson	3/6/2008	0f112570a061...	Sheila G. Carlson
000039403875	scarlson	3/13/2008	0f112570a061...	Sheila G. Carlson

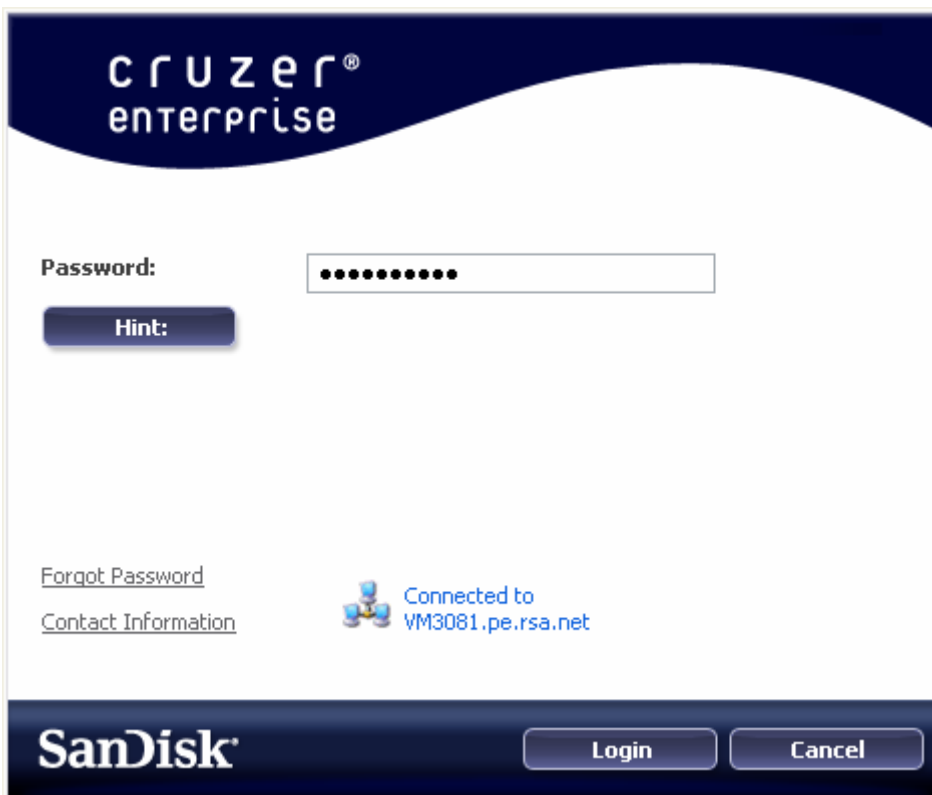


The next time the user logs into his or her Cruiser Enterprise drive, the token with this serial number will be available to generate RSA SecurID Passcodes.

## Using the SanDisk Cruiser Enterprise RSA SecurID Authenticator

Once users have been successfully provisioned, they will see the RSA SecurID application available from their drive. The steps to use this application are as follows:

1. The user logs into the Cruiser Enterprise drive:



2. Since the drive is managed by the SanDisk CMC Server, the user will see a green icon in the system tray if he or she is connected to the CMC Server:

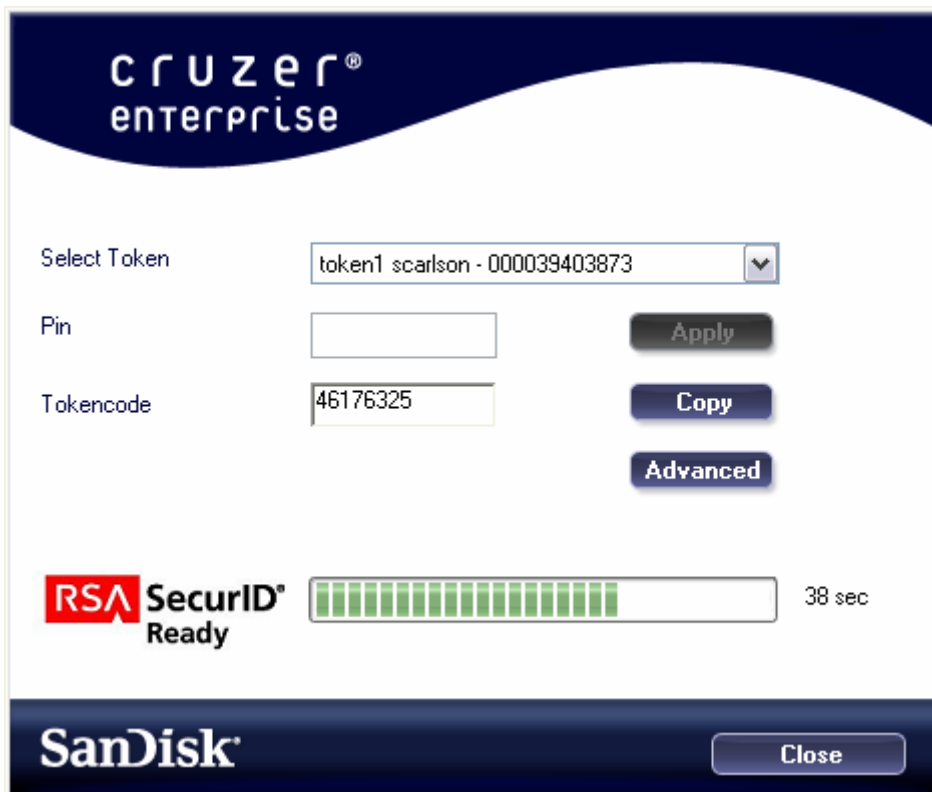




3. Clicking on this icon and selecting **RSA SecurID Software Token... Launch** will start the application:



4. The user will then see a list of Software Tokens that have been provisioned from the Select Token drop-down box.






5. The user can then enter his or her SecurID Pin and click the **Apply** button to generate a SecurID Passcode:

**cruzer<sup>®</sup>**  
**enterprise**

Select Token: token1 scarlson - 000039403873

Pin: •••• **Apply**

PASSCODE: 79993054 **Copy**  
**Advanced**

**RSA SecurID<sup>®</sup>** Ready  44 sec

**SanDisk** **Close**

6. The user can then either type this Passcode manually into an authenticating system, or use the **Copy** button to copy/paste it into an application. By clicking **Advanced** the user can also get the next Tokencode or Passcode, which can be useful for New PIN or Next Tokencode mode authentications.

# Certification Checklist for 3rd Party Applications

Date Tested: March 6th, 2008

Product	Operating System	Tested Version
<b>RSA Authentication Manager</b>	Windows 2003 Server	6.1.3
<b>SanDisk CMC Server</b>	Windows 2003 Server	2.0.5.12
<b>SanDisk Cruzer Enterprise</b>	Windows XP	2.0.5.20
<b>RSA SecurID Ready Authenticator Criteria</b>		
<b>RSA Software Token Import</b>		
v3.0 (AES) software token seed	✓	v3.0 copy & password-protected seed
v3.0 (AES) password-protected seed	✓	v3.0 (AES) multi-token seed file
v3.0 (AES) copy-protected seed	✓	v3.0 (AES) pinless token
<b>RSA Software Token SDK or Embedded RSA OTP Algorithm</b>		
Strong encryption of seed database		✓
Copy protection of seed database		✓
Proper display of current tokencode		✓
Interface to enter PIN		✓
Proper display of current PASSCODE		✓
Proper display of lifetime of current code		✓
Successful removal of installed token(s)		✓
Successful re-provisioning of installed token(s)		✓
Proper display of token serial number		✓
Successful addition of token alias/nickname		✓
Successful rename/removal of token alias/nickname		✓
Passphrase protection of application or token		✓
Proper setting of default token		✓
Ability to copy/paste PASSCODE		✓
Successful authentication using partner device		✓
Partner product displays RSA SecurID Ready logo		✓
<b>RSA Software Token Automation (SoftID API)</b>		
SoftID API-enabled application can automatically extract PASSCODE from Partner product		N/A
Successful authentication using partner device and SoftID API-enabled application		N/A
<b>RSA Software Token Provisioning (CT-KIP)</b>		
Partner product can be successfully seeded via CT-KIP protocol		N/A
<b>RSA Software Token Provisioning (RSA Authentication Manager Administrative API)</b>		
Partner product provisions Authentication Manager username		N/A
Partner product provisions RSA Software Token assignment		N/A
Partner product provides delivery mechanism for Software Token (.SDTID)		N/A

JEC

✓ = Pass ✗ = Fail N/A = Non-Available Function