Imation
IronKey Enterprise

RSA Ready Implementation Guide for RSA SecurID

Last Modified: June 18th, 2015

Partner Information

Product Information	
Partner Name	Imation
Web Site	www.ironkey.com
Product Name	IronKey Enterprise
Version & Platform	3.4.x for Windows
Product Description	IronKey Enterprise devices are quickly deployed and centrally managed USB flash drives with always-on, hardware-based encryption. IronKey Enterprise delivers managed and auditable data protection to prevent a data breach and achieve safe harbor. Organizations can consolidate portable storage and two-factor authentication with a single device using an on-board RSA SecurID software authenticator. The IronKey Enterprise Management Service allows organization to easily manage thousands of devices and enforce device-specific policies, including password strength, password retry limits and on-board portable applications. IronKey Enterprise logs device use for reporting and compliance.

Solution Summary

To enable organizations to achieve compliance and protect data, IronKey Enterprise safeguards user data everywhere it goes, with strong encryption certified to the highest standards. All user data on IronKey Enterprise USB flash drives is encrypted in hardware with high-speed, AES 256-bit CBC-mode encryption.

IronKey Enterprise allows organizations to consolidate portable storage and strong authentication with a single device. IronKey Enterprise includes an on-board RSA SecurID software authenticator, including support for web-based CT-KIP provisioning to accelerate deployment. To provide greater security compared to disk storage, the token seed is stored a private storage area on IronKey Enterprise devices. The token seed is only accessible to the RSA SecurID software authenticator. This provides further protection against malware that might attempt to steal token seeds.

IronKey Enterprise is deployed quickly using the cloud-based IronKey Enterprise Management Service. The IronKey Enterprise Management Service allows organizations to easily manage thousands of IronKey Enterprise devices and enforce device-specific policies, including password strength, password retry limits and onboard portable applications. Administrators are in full control of deployed devices and if needed can remotely disable devices and wipe data. IronKey Enterprise logs device use for reporting and compliance.

Functional Description	
Authenticator provides its own GUI to present tokencode	Yes (RSA GUI)
Authenticator can securely store token seed record	Yes
Authenticator supports copy/paste of tokencode	Yes
Authenticator supports multiple seed records	Yes (100)
Authenticator supports passphrase protection of application	Yes
Authenticator provides RSA Software Token Automation (user enters only PIN to authenticate)	No
Partner product provisions Authenticator (creates account, assigns token, delivers seed to device)	No
Authenticator supports CT-KIP provisioning protocol	Yes

Partner Product Configuration

Introduction

IronKey Enterprise secures data with always-on hardware encryption to meet compliance and data protection requirements. All user data on an IronKey Enterprise drive is encrypted with high-speed, AES CBC-mode encryption. IronKey Enterprise is deployed quickly using the cloud-based IronKey Enterprise Management Service. Administrators are in full control of deployed devices and if needed can remotely disable devices and wipe data. IronKey Enterprise logs device use for reporting and compliance. Integrated, on-board RSA SecurID provides users with a single strong authentication device.

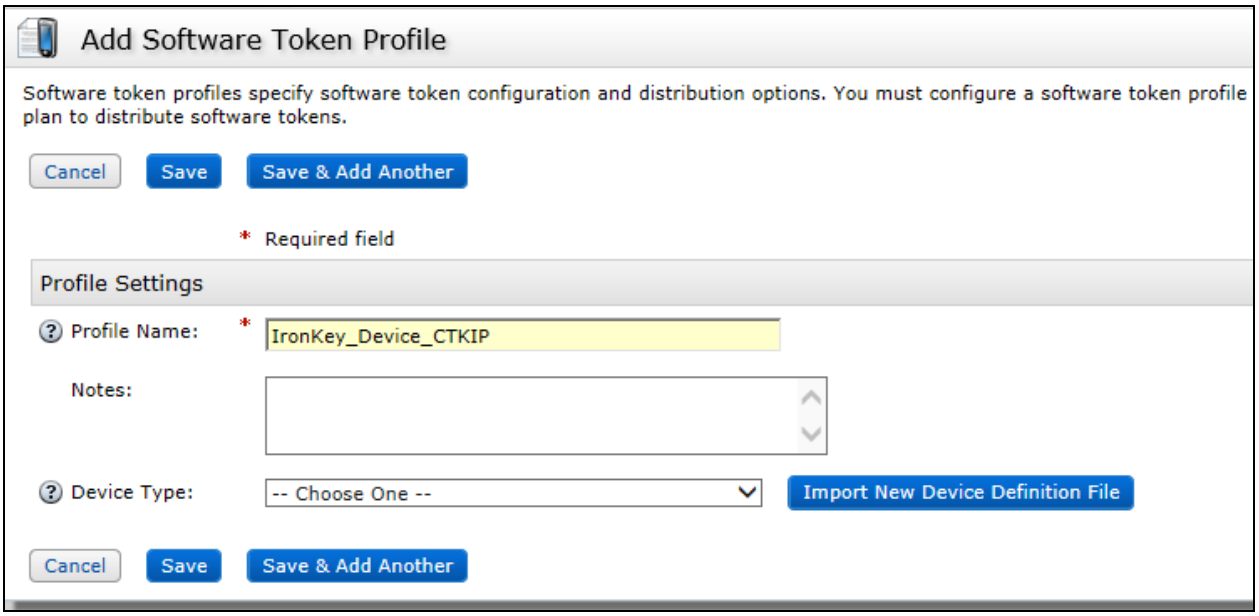
Uploading the IronKey Device Definition File

Before provisioning an RSA SecurID Software Token to IronKey Enterprise, it is first necessary to upload the IronKey **Device Definition File** to the RSA Authentication Manager Server. Download the device definition file for the IronKey Device here:

https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=202081534&arg12=downloaddirect&transaction=signon&quiet=true

To add the device definition file **IronKey-Device-3.4.x-swtd** to Authentication Manager 8.1, perform the following steps:

1. Save the device definition file to a folder on your computer.
2. In the RSA Security Console, click **Authentication… Software Token Profiles…Add New**:



3. Click the **Import New Device Definition File button**.
4. Browse to the location of the IronKey device definition file. Click **Submit**.
5. Configure the software token profile to use **IronKey Device 3.4.x** as the Device Type.

Note: 6-digit tokens are not supported for use with the IronKey Enterprise Device. This is reflected in the IronKey Device Definition file.

Provisioning the IronKey RSA SecurID Authenticator

RSA SecurID Token Import via File Based Provisioning

Note: For more information on provisioning the IronKey RSA SecurID Authenticator, consult the *IronKey Enterprise User Guide*

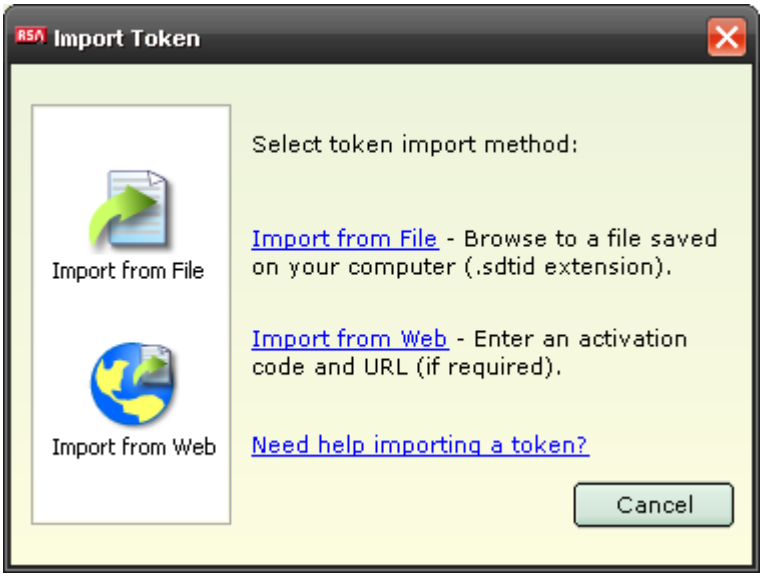
IronKey devices can be provisioned via the standard RSA SecurID Software Token file-based or CT-KIP provisioning methods -- there is no additional configuration required to interoperate with your existing RSA SecurID infrastructure.

To begin the provisioning process, perform the following steps:

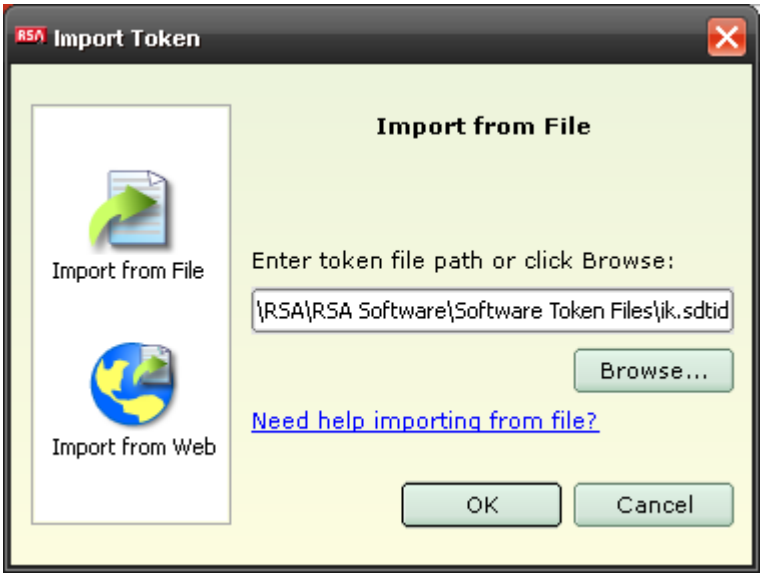
1. Start the IronKey Control Panel, and select **RSA SecurID**:
2. The RSA SecurID Token application will start. Click the **Options** down arrow and select **Import Token:**

Note: If you have never installed a token, the Import Token screen is displayed automatically.

3. Click **Import from File:**



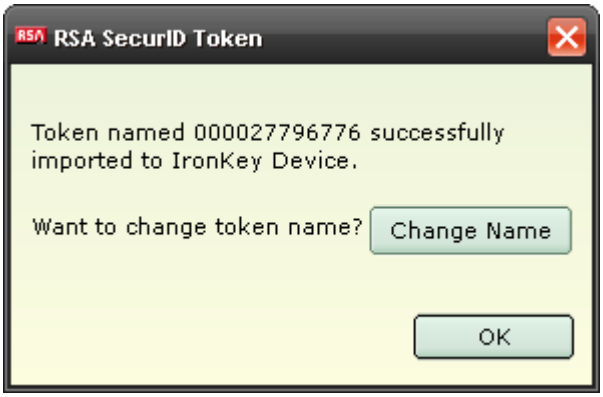
4. Browse to the software token file to import it and select **OK**:



5. If a password is required, the user will be prompted for it at this point:

Click **OK** to continue.

6. Upon successful import, the user will see the following dialog:



The IronKey Device is now ready to use RSA SecurID authentication.

RSA SecurID Token Import via Web (CT-KIP)

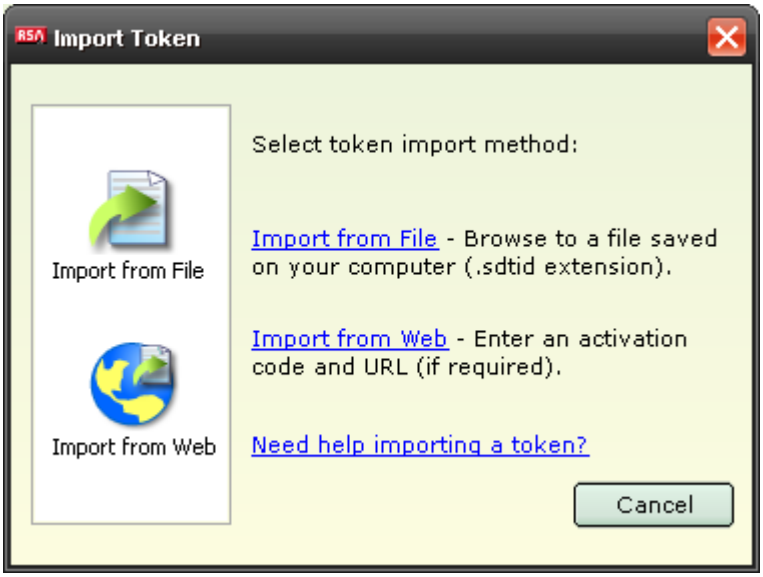
Another option for provisioning SecurID Tokens is to import via the Web. Importing via the Web is an option available as of RSA Authentication Manager 7.1, and uses the CT-KIP dynamic provisioning protocol.

To provision tokens via the Web, perform the following steps:

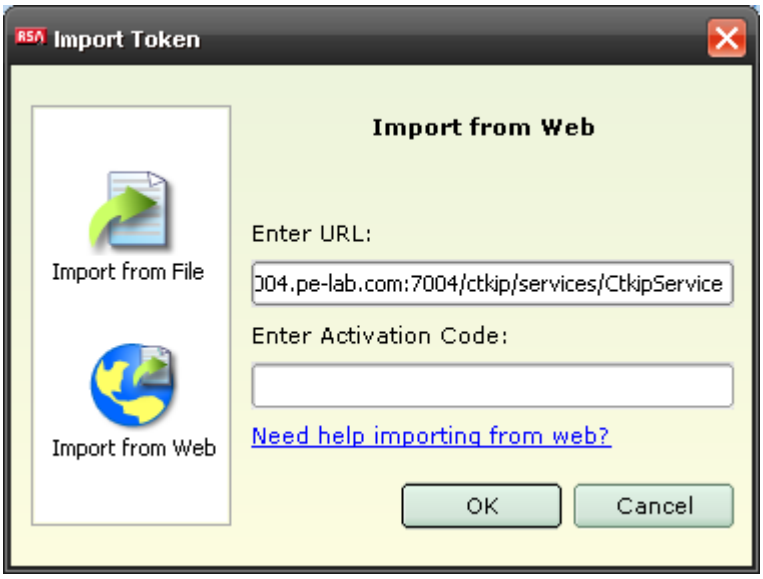
1. Start RSA SecurID Token. Click the **Options** down arrow and select **Import Token:**

Note: If you have never installed a token, the Import Token screen is displayed automatically.

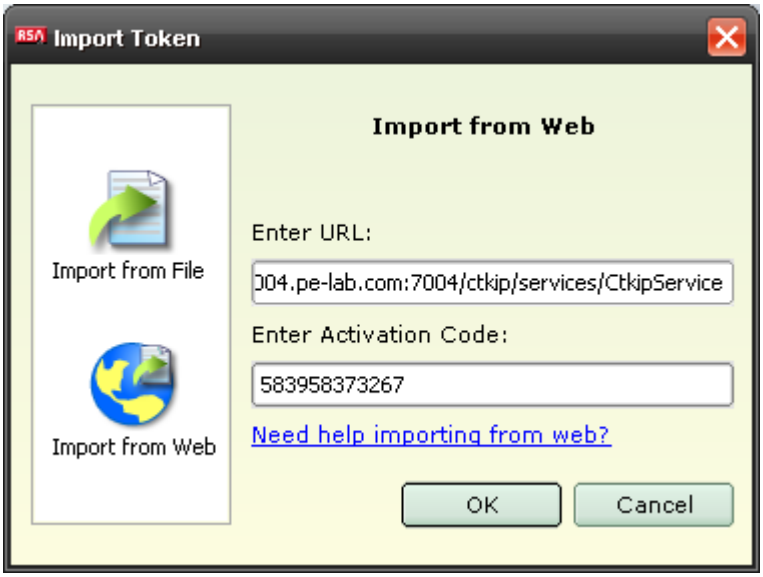
2. Click **Import from Web:**



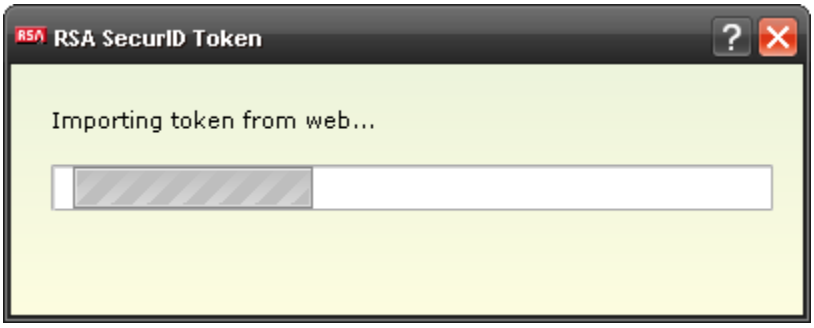
3. The **Install from Web** dialog box opens. In the Enter URL field, enter the URL of the CT-KIP server. If the Enter URL field is prefilled, go to step 5.



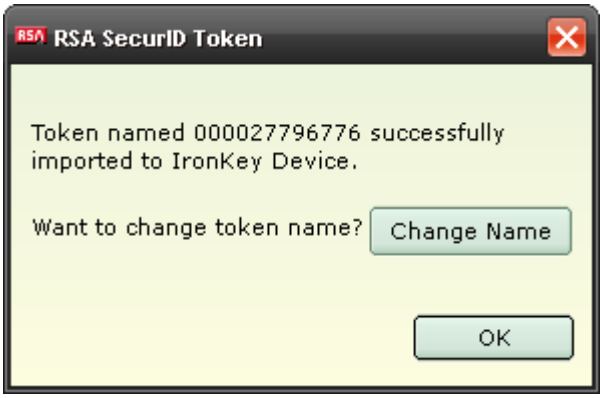
4. In the **Enter Activation Code** field, enter the activation code that your administrator gave you. Click **OK**.



5. The user will see the **Importing Token** dialog:



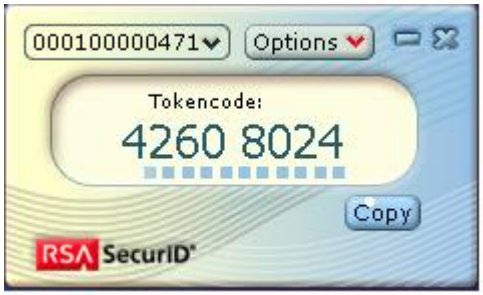
6. Upon successful import, the user will see the following dialog:



The IronKey Device is now ready to be used as an RSA SecurID Authenticator:

Using the IronKey as an RSA SecurID Authenticator

Once users have been provisioned with an RSA SecurID Software Token, they can simply run the RSA Software Token application from the IronKey launcher menu:



The SecurID Passcode can then be used with any websites or applications that perform SecurID authentication.

Additional IronKey Device Configuration

Because the RSA SecurID application is running from a portable environment, the application executable obtains configuration information from INI files. The **SecurID.ini** file is a configuration file that contains the path and the GUID of the token storage plug-in, but can also be configured with customization policies that change the default behavior of the application. This file is found co-located with the SecurID.exe executable on the device filesystem.

For example, the following policy set in the SecurID.ini file will pre-populate the CT-KIP URL when the application is launched:

```
[Plugin]
DLLGUID=aaa11111-2222-333b-b444-555555cccccc
Path=./ikrsaplugin.dll

[Policies]
CtkipUrl=https://somewhere.com:7004/ctkip/services/CtkipService
```

You can also set a policy (ActivationCode=1) to automatically use the user's Windows SID as the activation code for CT-KIP. In order for this to work, you must first pre-populate the **UserSID** software token device type attribute before provisioning the token via CT-KIP.

> **Note: A list of all policy options is available the in Appendix A of the *RSA SecurID Software Token 5.0 Administrator's Guide*.**

Certification Test Checklist for RSA SecurID

Date Tested: June 16th, 2015

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
RSA SecurID Desktop Token	5.0	Windows
IronKey Enterprise	3.4	Windows

RSA Ready Certification Criteria	
RSA Software Token Import	
Provision password-protected token	✓
Provision copy-protected token	✓
Provision PINPad token	✓
Provision FOB-Style token	✓
Provision PINless token	✓
Provision CTKIP token	✓
Provision CTF token	✓
Provision File-based token	✓
RSA Software Token SDK or Embedded RSA OTP Algorithm	
Strong encryption of token database	✓
Copy protection of token database	✓
Proper display of current tokencode	✓
Interface to enter PIN	✓
Proper display of current PASSCODE	✓
Proper display of lifetime of current code (30/60 seconds)	✓
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 Ready logo	N/A

RSA Software Token Automation (Software Token API)	
Software Token API-enabled application can extract PASSCODE from Partner product	N/A
Successful authentication using Software Token API-enabled application	N/A
RSA Software Token Provisioning (RSA Authentication Manager Administrative API)	
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