CryptoKey
User Guide

Trademarks
DualShield Unified Authentication, CryptoKey, MobileID, QuickID, PocketID, SafeID, GridID, FlashID, SmartID, TypeSense, VoiceSense, DevicePass, RemotePass and Site Stamp are trademarks of Deepnet Security Limited. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights
Under the international copyright law, neither the Deepnet Security software or documentation may be copied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Deepnet Security.

Licence Conditions
Please read your licence agreement with Deepnet carefully and make sure you understand the exact terms of usage. In particular, for which projects, on which platforms and at which sites, you are allowed to use the product. You are not allowed to make any modifications to the product. If you feel the need for any modifications, please contact Deepnet Security.

Disclaimer
This document is provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Deepnet Security may make improvements of and/or changes to the product described in this document at any time.

Contact
If you wish to obtain further information on this product or any other Deepnet Security products, you are always welcome to contact us.

Deepnet Security Limited
Northway House
1379 High Road
London N20 9LP
United Kingdom

Tel: +44(0)20 8343 9663
Fax: +44(0)20 8446 3182
Web: www.deepnetsecurity.com
Email: support@deepnetsecurity.com

Contents

Introduction

CryptoKey is a secure USB flash drive with hardware encryption. Every bit of data saved into the drive is encrypted in real time by an on-board AES 256-bits encryption module. In addition, data saved into the drive is also scanned for virus and malware by a built-in Antivirus and Antimalware engine.

Using CryptoKey is as simple as using an ordinary USB flash drive. The only difference is that CryptoKey needs to be unlocked with your password before it is can be used.

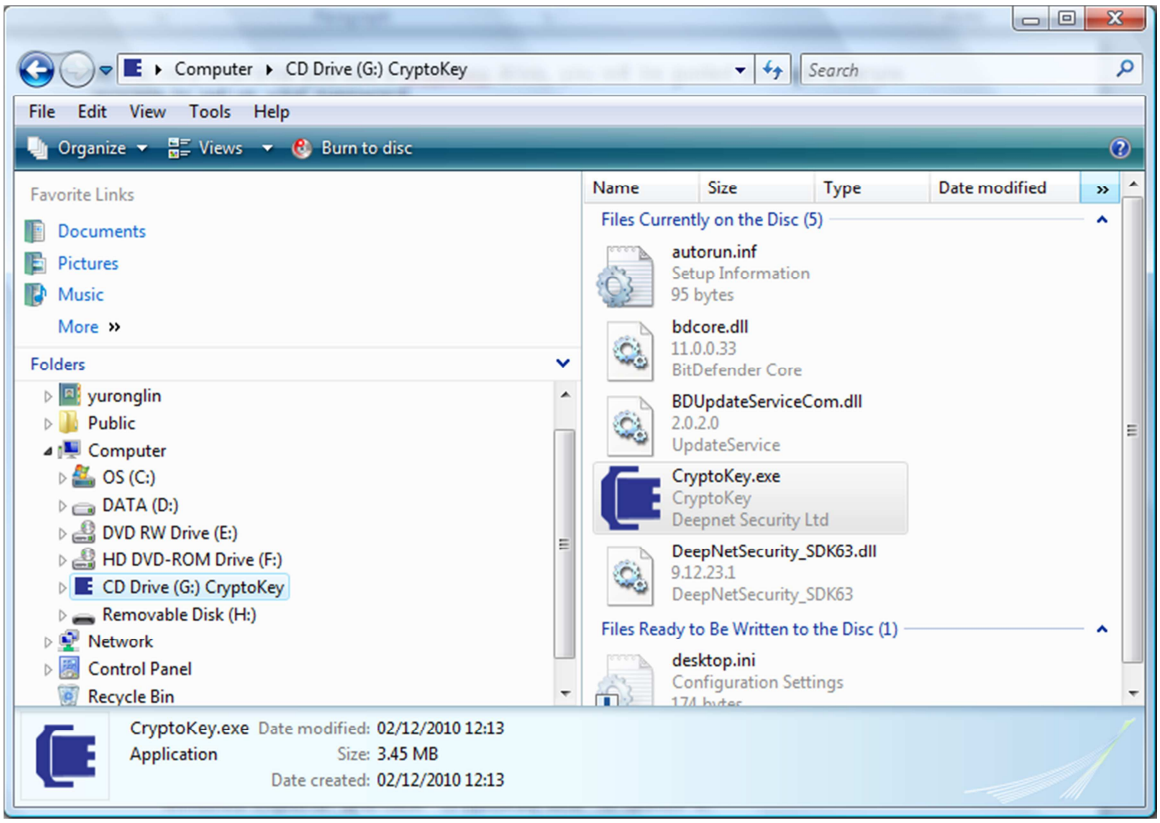
First-time Use

At the very first time you use a CryptKey drive, you will be guided through a simple process to set up your password.

Step 1. Insert your CryptoKey drive into a USB port in your PC or laptop

If the Autoplay feature is enabled on your PC/Laptop, then in a few seconds you will see the screen below:

If the Autoplay feature is disabled, then you have to locate the drive in the Windows Explorer and click "CryptoKey.exe" to launch it.



Step 2. Set Password

As it is a brand new drive, you need to first set up your own password. Click the "Set Password" button.

Your password must be compliant to the password policy that is set by the IT administrator of your organisation or vendor. To check the password policy, move your mouse cursor over the "Password Policy" link.

Enter your password and confirm it. Depending on your password policy, you might be allowed to enter a password hint.

Finally, click "Go" to set up your password.

Unlock a Drive

Insert your CryptoKey drive into a USB port in your PC or laptop

If the Autoplay feature is enabled on your PC/Laptop, then in a few seconds you will see the screen below:

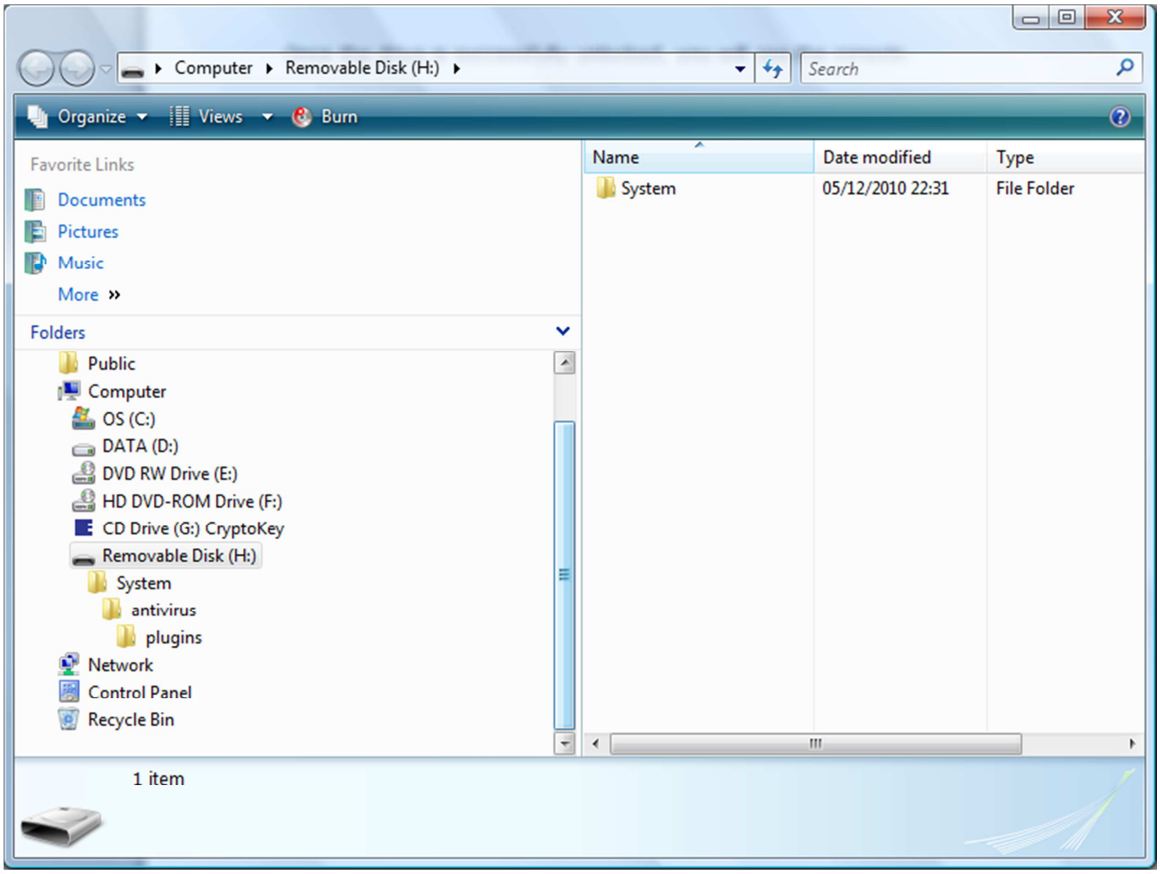
If the Autoplay feature is disabled, then you have to locate the drive in the Windows Explorer and click "CryptoKey.exe" to launch it.

Enter your password and Click "Go" to unlock your CryptoKey drive

Unlocking the drive might take a few seconds.

Once the drive is successfully unlocked, you will see the console.

And in your Windows Explorer, you will see a new Removable Disk:



You can now save and copy data to/from the drive as if it was an ordinary USB drive.

Lock a Drive

There are 3 ways you can lock a CryptoKey drive.

1. If you want to lock the drive but not to shut down its console, then select "Tools | Lock"

2. If you want to lock the drive also to shut down its console, then select "Tools | Exit"

3. You simply unplug the drive from the USB port. As soon as a CryptKey drive is unplugged from a PC/Laptop, it is automatically locked.

Register a Drive

If you are a business user, then you might be required by your organisation to register your CryptoKey drive. By registering your drive with your organisation's central management server, you will be able to recover your password in the case you have forgotten password, or to wipe out your drive in the case you have lost your drive. Furthermore, you will be able to use your CryptoKey drive as a two-factor authentication token.

To register your drive, select "Settings | Register Device"

You need to enter the server address which should have been provided by your administrator.

Enter your user name and password. Please note this password is not the password that you have set up for the CryptoKey drive itself, it is your account password in your organisation's database which is normally an Active Directory.

Depending on your organisation's policy, you might be asked to enter an activation code to activate your registration. You will normally receive your activation code in an SMS text message to your mobile phone or in an email message in your email box. Otherwise, you can get your activation code from your IT administrator.

If your username/password and activation code are correct, your drive will have been successfully registered.

Password Recovery

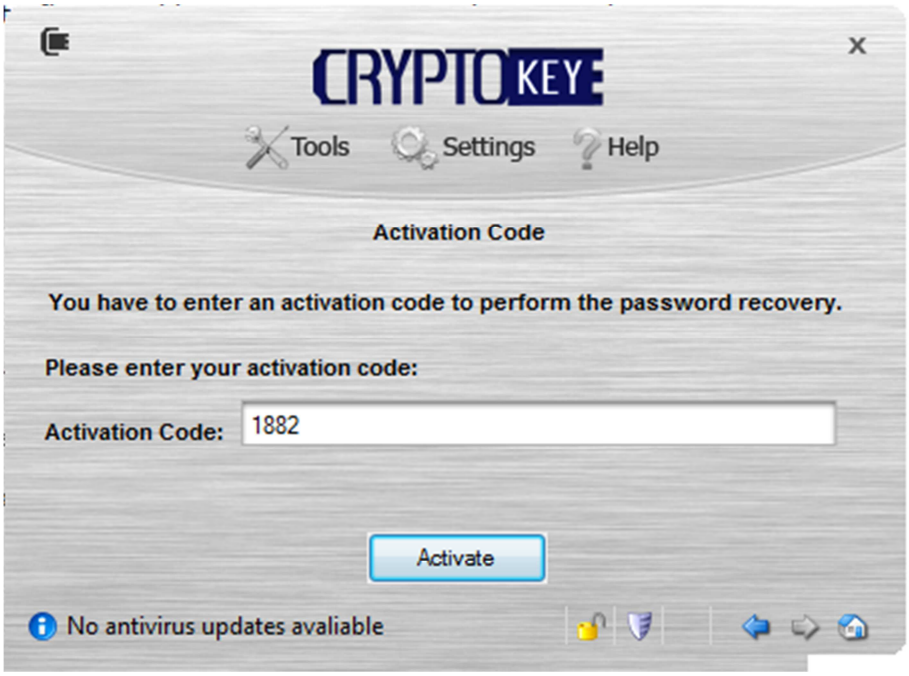
If you have forgotten your password, you can automatically recover it from your central management server (Automatic Recovery) or you can manually recover it with the help of your IT administrator or help desk.

Automatic Recovery

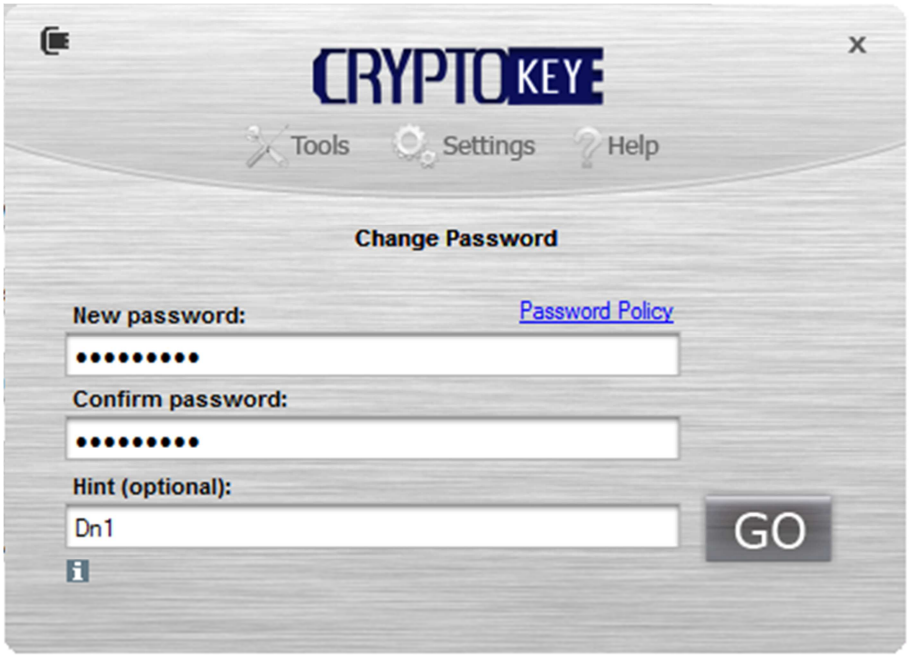
Select "Tools | Security | Recover Password | Automatic Recovery"

You will be asked to first provide your user name and password:

Depending on your organisation's policy, you might be asked to enter an activation code to activate your password recovery. You will normally receive your activation code in an SMS text message to your mobile phone or in an email message in your email box. Otherwise, you can get your activation code from your IT administrator.



If your username/password and activation code are correct, you will then be able set a new password:



Once your new password has been successfully set, you will be able to unlock your drive with the new password

Manual Recovery

Select "Tools | Security | Recover Password | Manual Recovery"

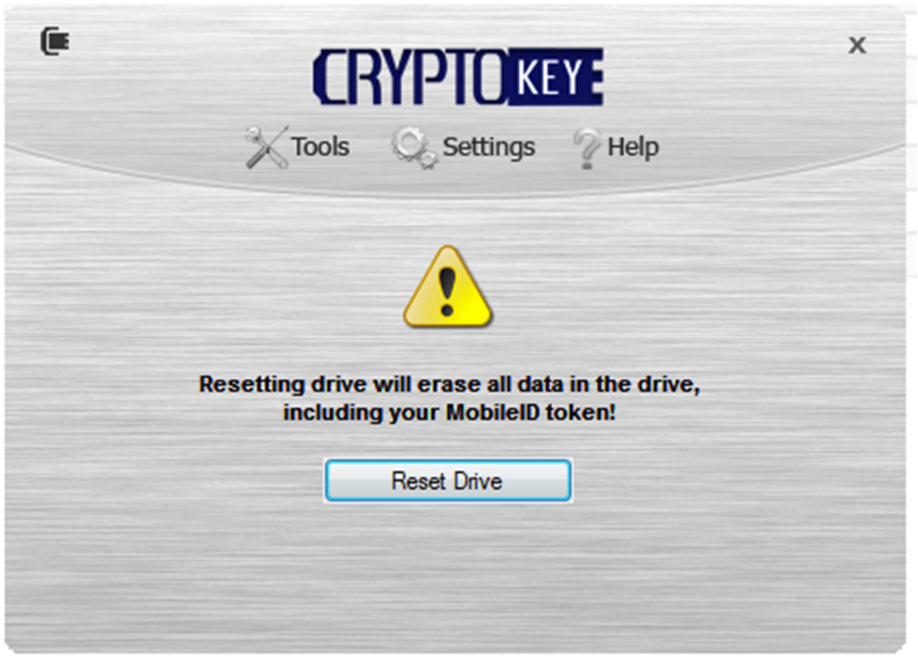
In the manual recovery process, you need to contact your IT administrator or Help Desk and provide the serial number of your drive and a so-called Recovery ID code:

Your IT administrator or Help Desk will then provide you with a Recovery Key that will enable to reset your password.

After you have entered a correct Recovery Key, the rest of the process is the same as the automatic recovery.

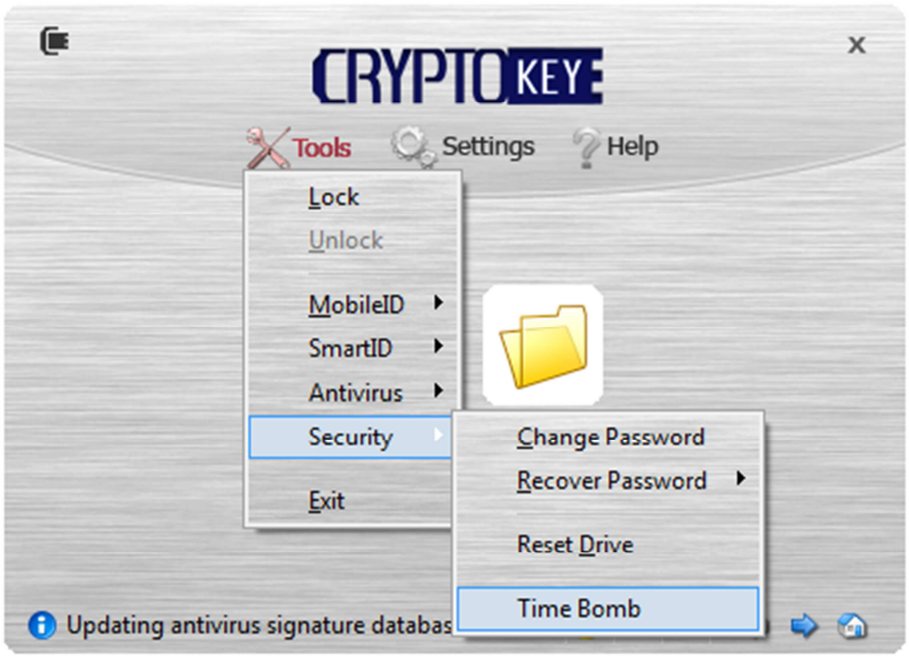
Reset Drive

If you have forgotten your password and do not wish to recover the data in the drive, you can reset your drive with a new password by yourself. Resetting a driving will wipe out all data in the drive.

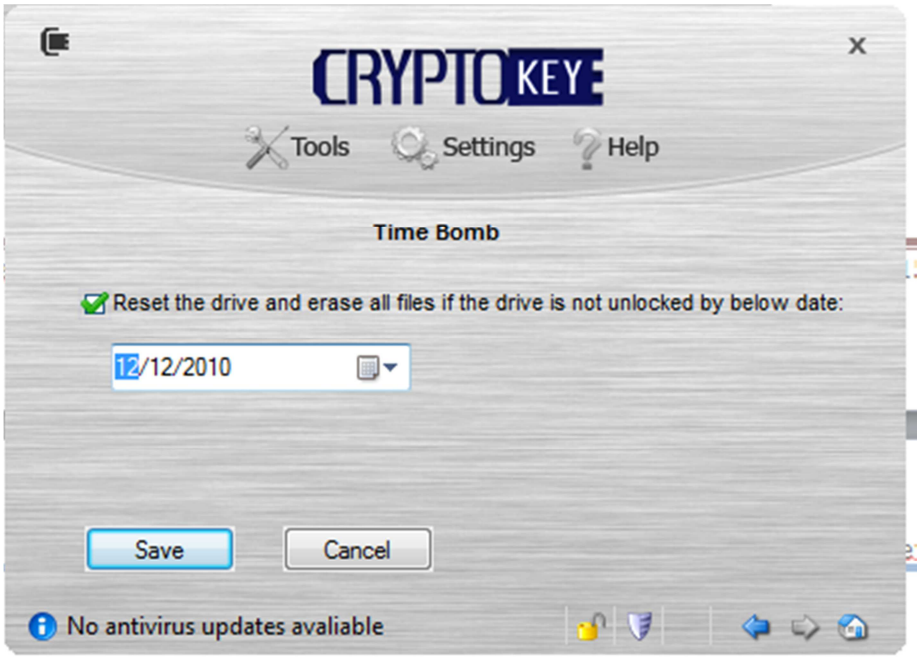


Time Bomb

CryptoKey has a unique feature that enables you to set a time bomb.



If you set a time bomb on your CryptoKey drive, the drive will automatically reset itself and wipe out all data in the drive if the time bomb is not defused before its set-off date.



The time bomb will be automatically defused when you unlock the drive before its set-off date.

Remote Kill

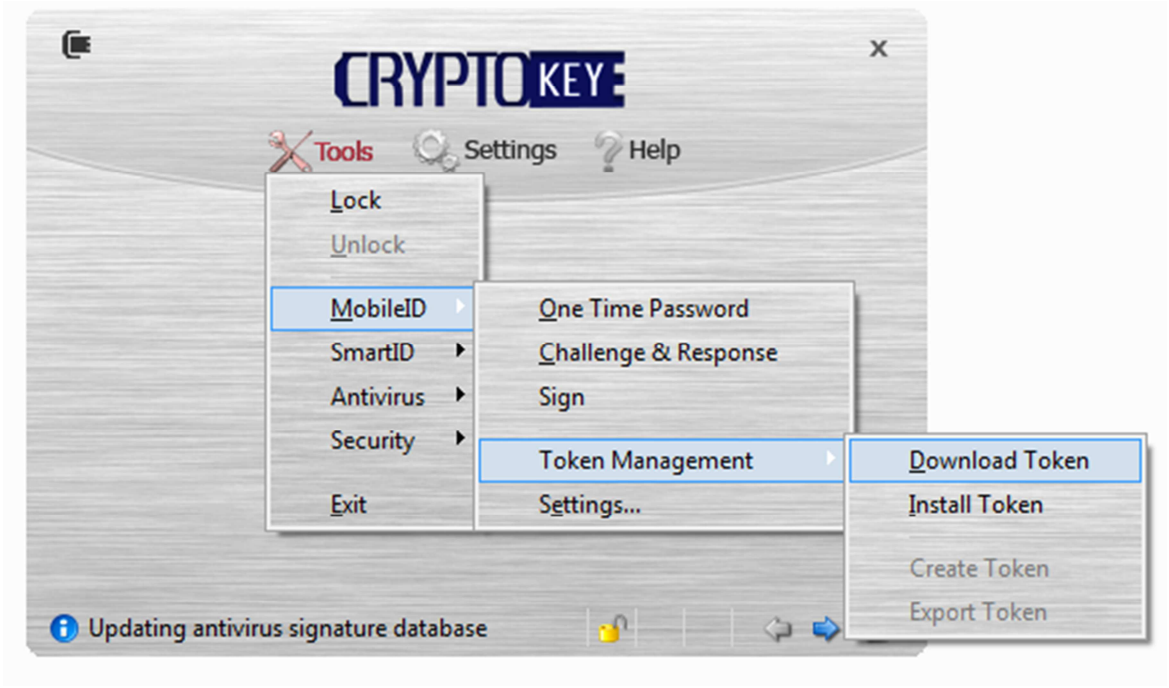
If you have lost your CryptoKey drive, you should report to your IT administrator or Help Desk as soon as possible, and request your drive to be remote killed. Next time your drive is inserted into a PC by someone, it will be killed automatically.

Two-Factor Authentication

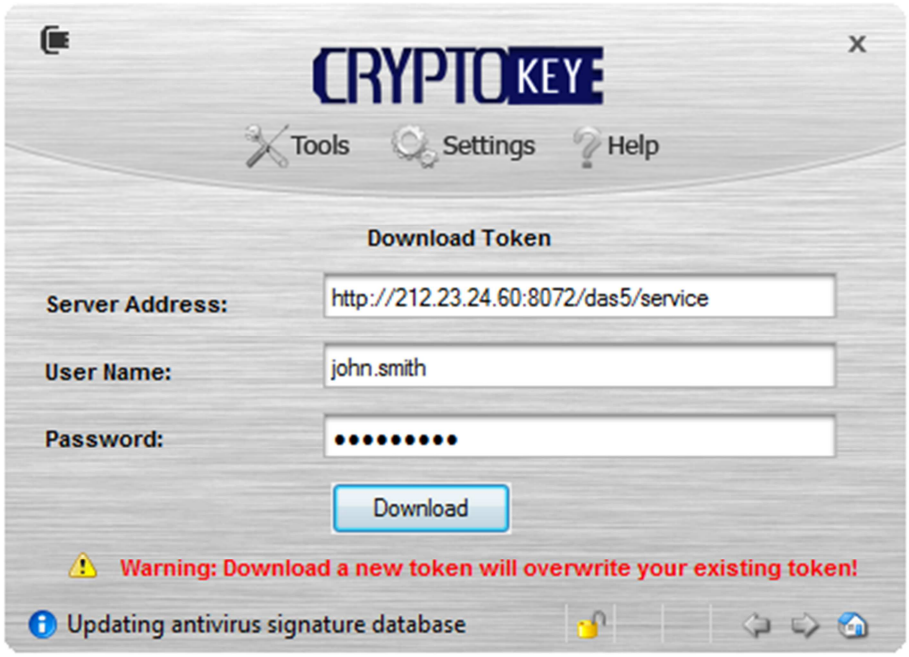
CryptoKey can also be used as a two-factor authentication token. The Deepnet MobileID client is already built into the CrptoKey's console. To use MobileID, all you need is a MobileID token. You can download your MobileID token from the management server automatically or you can install your token manually with the help of your IT administrator or help desk.

Download MobileID Token

To download your MobileID token, select "Tools | MobileID | Token Management | Download Token"



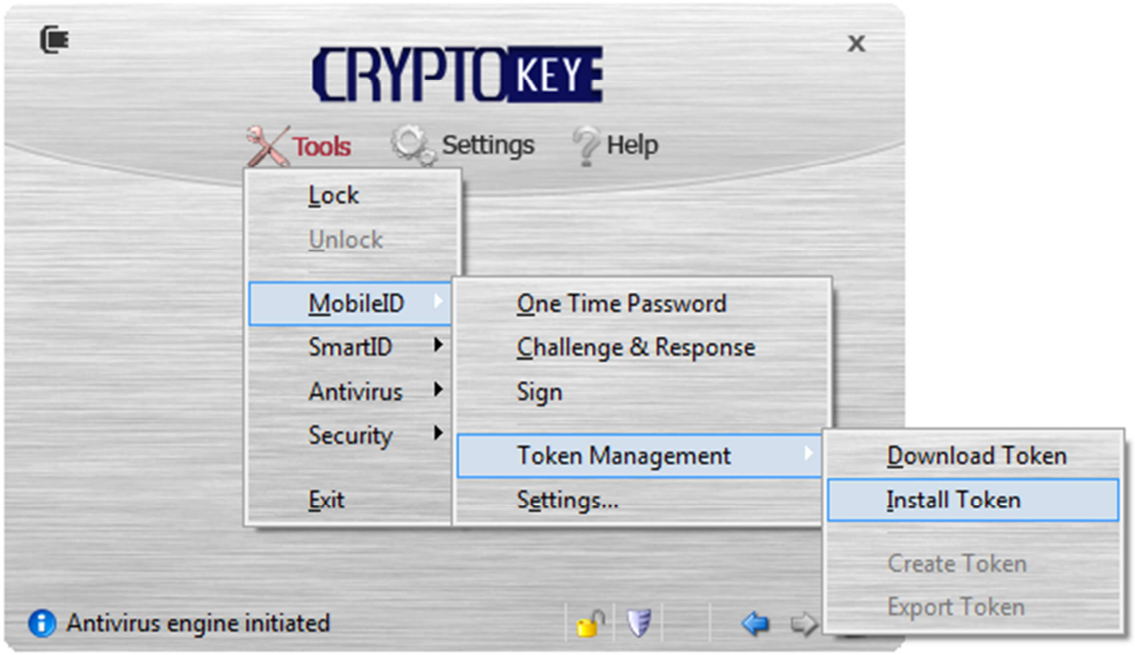
You will be asked to authenticate yourself with the correct user name and password:

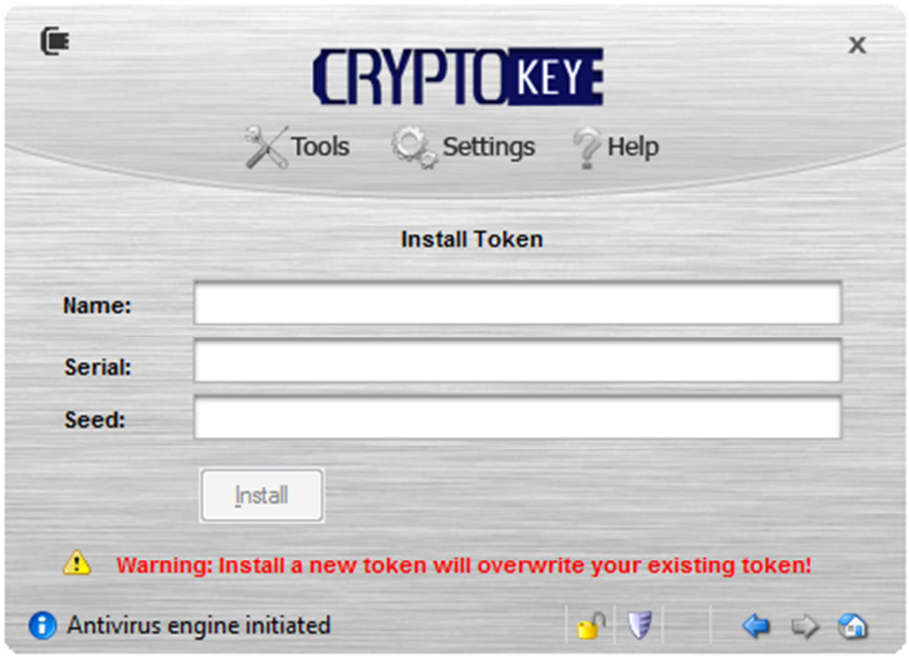


Depending on your organisation's policy, you might be asked to provide an download Authorisation Code which you will normally receive in an SMS text message or email message.

Install MobileID Token

If you are unable to download your MobileID token, you can install it manually.





Contact your IT administrator or help desk for the Serial Number and Seed of your token.

Use Mobile ID

To use your MobileID token, select "Tools | MobileID | One-Time Password"