

A KASPERSKY LAB'S COMPANY



INFOWATCH

InfoWatch CryptoStorage

Quick Start Guide

INFOWATCH CRYPTOSTORAGE

Quick Start Guide

© InfoWatch

<http://www.infowatch.com>

Last edited: September 2009

Table of Contents

CHAPTER 1. INTRODUCTION	4
1.1. Hardware and Software Requirements	5
1.2. General Conventions.....	6
1.3. Technical Support.....	6
CHAPTER 2. INSTALLING INFOWATCH CRYPTOSTORAGE	7
2.1. Installation.....	7
2.2. Managing Licenses	9
2.3. Getting and Installing Licenses using an Activation Code	10
2.4. Updating the Product.....	11
CHAPTER 3. GETTING STARTED	12
3.1. What is a Protected Object	12
3.2. Accessing Protected Objects	13
3.3. System Interface.....	14
3.4. Encrypting Existing Objects	15
3.5. Protected Containers.....	16
3.6. Managing Access to Protected Objects	17
CHAPTER 4. CONCLUSION	18

CHAPTER 1. INTRODUCTION

InfoWatch CryptoStorage (hereafter InfoWatch CryptoStorage or the System) – is a system intended to protect confidential information stored on a PC against unauthorized access using cryptographic means.

While protecting data, the System uses **transparent encryption**, when data is encrypted during protection and stored encrypted inside a protected object. The protected data is decrypted in RAM when requested and the uploaded data is encrypted.

Data is encrypted with the 128-bit AES algorithm. This algorithm is approved by the international cryptography community and represents a cryptographic standard. AES is approved by the U.S. National Institute of Standards and Technology (Standards and Technology (NIST) Federal Information Processing Standards (FIPS) PUB 197 26.11.2001).

The main functions of the System are listed below.

Data protection

With the System, you can:

- protect all data on disk volumes (including the system and the boot volumes), on Flash drives, and other USB Mass Storage devices.
- protect the contents of individual files and folders within the NTFS file system;
- create protected virtual disks (the protected containers) to store confidential data;
- protect RAM contents which are saved to hard disk when the system hibernates, crash dump data which is saved to hard disk when a fatal error occurs and data from temporary files and swap files against unauthorized access.

Handling protected data

With the System, you can:

- delimit access to protected information using password authorization;
- set up multi-user access to protected data;
- store protected objects inside other protected objects with any nesting depth;

- prevent accidental or intended deletion of protected objects by limiting access to these objects;
- use protected containers, folders and files located both on the user's workstation and on local network resources;
- move protected objects together with the physical carrier to another computer where the System is installed and use the objects on this computer;
- wipe files and folders (both protected and unprotected).

This guide explains how to start using InfoWatch CryptoStorage, describes the architecture of the System and its features.

1.1. Hardware and Software Requirements

Your computer must meet the following hardware and software requirements to run InfoWatch CryptoStorage.

Hardware requirements:

- processor Intel Celeron 1 GHz or higher;
- RAM 256 MB;
- 5 MB free disk space to install the application.

Software requirements:

- Any of the listed operating systems:
 - Microsoft Windows 2000 Server Service Pack 4;
 - Microsoft Windows 2003 Server;
 - Microsoft Windows 2000 Professional Service Pack 4;
 - Microsoft Windows XP Service Pack 3;
 - Microsoft Windows Vista Service Pack 2;
 - Microsoft Windows 7.

System supports operating systems on both x86 and x64 platforms.

1.2. General Conventions

This document contains different types and styles to bring your attention to specific information. Table 1 contains style description.

Table 1. Style description

Style	Description
Bold	Indicates programs (if they are mentioned for the first time in the document), GUI elements. Bold typeface also indicates terms and definitions.
<i>Italics</i>	Indicates document names, table of contents at the beginning of chapters and sub-chapters. Italics also indicates attribute names and values in a table. Some other text elements (if no special styles are provided for them) are also marked in italics.
Font Courier New	Indicates file names, program code examples. When describing configuration files, the style denotes parameter values, examples of settings.

1.3. Technical Support

You can download new versions of the InfoWatch CryptoStorage software product and documentation from our website <http://www.infowatch.com> at <http://www.infowatch.com/downloads>.

If you cannot resolve issues which arise when using the licensed versions of the System, you can contact our technical support service either at <http://www.infowatch.com/support/cryptostorage> or by e-mail support@infowatch.com.

CHAPTER 2. INSTALLING INFOWATCH CRYPTOSTORAGE

2.1. Installation

Attention!

You must have administrator rights to the computer to install InfoWatch CryptoStorage.

The installation starts with the installation wizard. Each window contains a set of buttons to control the installation process. The buttons provide the following operations:

- **Next** – accept the action and go to the next step of the installation procedure.
- **Back** – return to the previous step.
- **Cancel** – cancel the installation.

See below the step-by-step description of the System installation procedure.

Step 1. Start the Installation

Insert the InfoWatch CryptoStorage setup disk into the CD-ROM drive and run the installation file `CryptoStorage_EN_1_0_VVVV_x86.msi` or `CryptoStorage_EN_1_0_VVVV_x64.msi`.

The `vvvv` letters in the name of the installation file stand for the version of the Product. `x86` or `x64` are the platform of the operating system running on your computer.

Note:

You can download a new version of the InfoWatch CryptoStorage software product at <http://www.infowatch.com/downloads>.

The Welcome to the **InfoWatch CryptoStorage** Setup Wizard screen opens.

Click **Next** to proceed to the next step. Or click **Cancel** to cancel the installation.

Step 2. Accept License Agreement

You must accept the terms of the license agreement to continue the installation and click **Next**.

Step 3. Select the Installation Directory

The default path to the directory where InfoWatch CryptoStorage will be installed is specified in the input field of the **Destination Folder** screen.

You can change the installation directory. Click **Change...** and select a directory in the standard window for selecting the directory, or type the path to the directory in the appropriate input field.

Click **Next** to proceed to the next step.

Step 4. Complete the Installation

After proceeding to the **Ready to install InfoWatch Cryptostorage** screen, click **Install**, to install InfoWatch CryptoStorage.

Follow the installation wizard instructions to complete the installation of InfoWatch CryptoStorage.

When the installation is complete, you will be asked to activate the product. You can select one of the following options:

- **Activate 30-day trial version.**
- **Activate full version.**

To activate the full version, you must get and install a license using an activation code. See information on the procedure for getting and using a license key in Item 2.3 on Page 10. After the type of activation is selected, click **Next**.

Restart the computer to complete the installation. The corresponding notification is displayed.

Attention!

It is strongly advised not to turn off computer's power supply when restarting (when Microsoft Windows is shutting down). It may cause an error while the operating system is starting up.

If the power supply fails, keep hitting the **F8** key when restarting. In the Windows Advanced Options Menu, select the **Last Known Good Configuration** option. After that, reinstall InfoWatch CryptoStorage.

2.2. Managing Licenses

You must get and register a commercial license to make InfoWatch CryptoStorage fully functional.

Note:

With the activated trial license, you can use the full-featured InfoWatch CryptoStorage for 30 days. The password length is limited by 1 character.

When any type of license expires, you can decrypt your data. But you cannot create new protected objects, change access lists or re-encrypt the objects.

You can manage licenses using CryptoStorage Configurator.

To run CryptoStorage Configurator,

from the **Start** menu, select **Programs ► InfoWatch CryptoStorage ► CryptoStorage Configuration**.

In the opened window, click **Licenses....** The Licenses dialog window will be displayed (Figure 1).

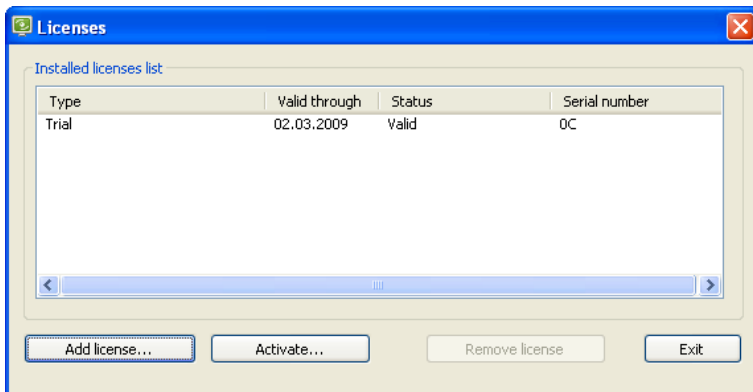


Figure 1. Licenses

This window contains a list of installed licenses and detailed information on each license: type, serial number, current status and validity period.

To add a license to the list, click **Add license....** In the opened dialog window, specify the path to a license file and click **Open**.

Note:

The added license must be given to the same user who owns all other licenses in the list. Otherwise you cannot add a license.

To remove a license from the list, select the license and click **Remove license**.

Note:

You cannot remove the Trial license from the license list.

Attention!

It is strongly not advised to remove the valid commercial license from the list. Otherwise the functionality of the Product will be limited in a way similar to the expired license.

To get and install a license using an activation code, click **Activate**.... Activating a license using an activation code is covered in Item 2.3 on Page 10.

When you finish editing the list of installed licenses, click **Exit** to close the window.

2.3. Getting and Installing Licenses using an Activation Code

You can use an activation code to get and install a license while installing the Product or after the Product is installed, when managing licenses (see Item 2.2 on Page 9).

Attention!

When using an activation code, your computer must be connected to the Internet to download a license from the InfoWatch license service.

To get a license, type a product code consisting of five parts. Each part of the code contains five characters (Figure 2). The code contains digits (except zero) and upper-case Latin letters.

The screenshot shows a 'Product activation' dialog box. It has a blue title bar with a close button. The dialog is divided into two main sections. The first section, 'Enter activation code', contains a text input field with a placeholder 'xxxxx-xxxxx-xxxxx-xxxxx-xxxxx' and two buttons: 'OK' and 'Cancel'. The second section, 'Customer information', contains three fields: 'Country' (a dropdown menu showing 'Russian Federation'), 'Name' (a text input field with 'xxx'), and 'E-mail' (a text input field with 'xx@xxx.ru').

Figure 2. Activating the Product

Then, in the customer information pane, specify your country. You can also specify your name and e-mail address as additional information. Click **OK**.

After that the license is acquired and installed automatically.

Attention!

Only one license is given for each activation code. Keep your product activation code secret.

Copy the license file to another hard disk or removable device. This copy will be needed to restore the System after a failure.

2.4. Updating the Product

You can download a new version of the InfoWatch CryptoStorage software product at <http://www.infowatch.com/downloads>.

To update the Product to a newer version, run the setup program of the new version.

Note:

You cannot update an older version to an earlier version. To install an earlier version, you must first uninstall the existing version of the Product.

CHAPTER 3. GETTING STARTED

InfoWatch CryptoStorage consists of:

- The **CryptoStorage** component, which is intended to encrypt data and handle the data.
- **CryptoStorage configurator**, which is intended to configure subsystems.

The **CryptoStorage** component includes three subsystems to encrypt objects of specific types:

- The **Protected volumes** subsystem protects disk volumes and removable disks.
- The **Protected containers** subsystem enables the use of protected containers.
- The **Protected file system** subsystem encrypts and manages files and folders.

3.1. What is a Protected Object

Any object encrypted by InfoWatch CryptoStorage is called a **protected object** in this document.

There are two groups of **protected objects**:

- **the objects**, created when files within the operating system are converted to a protected form (files, folders, disk volumes, the system and the boot volumes), Flash drives, USB storage devices and other devices of the Mass Storage type);
- the objects, created by InfoWatch CryptoStorage – **the protected containers**.

Attention!

All data placed into a protected object is automatically protected. When you copy data from the protected object into an unprotected area, the data is placed in the open (unprotected) form.

3.2. Accessing Protected Objects

The System allows several users to use the same protected object. InfoWatch CryptoStorage supports two roles for this kind of work: **the owner** and **the user**.

The owner of a protected object is a user who has the right to perform any operations on the object. The protected object owner is assigned when encrypting the object (or when creating a protected object). Each protected object can have only one owner.

A user of a protected object is a user added by the object owner into the object access list. Unlike the object owner, the user's rights to use a protected object are limited.

Table 2 lists user's and owner's rights for various operations on protected objects (the "+" and "-" characters signify whether a right for a specified type of operation is given).

Table 2. Rights of object owners and users

Operation on a protected object	Protected object owner	Protected object user
Attaching/detaching objects	+	+
Using objects (reading, copying, archiving, removal, etc)	+	+
Wiping files or folders Note: Any user can wipe unprotected files and folders on a computer where the System is installed.	+	+
Viewing information on a protected object	+	-
Changing the access list (adding/removing users of a protected object)	+	-
Re-encrypting/decrypting objects	+	-
Creating a protected container using InfoWatch CryptoStorage	+	-

Operation on a protected object	Protected object owner	Protected object user
Changing personal authorization parameters	+	+

3.3. System Interface

You can access functions of the System using Windows Explorer context menu.

To open the CryptoStorage menu:

1. Select the necessary object (a file, a folder, a container, a volume or a removable disk) and right-click it.

The context menu of the selected object will be opened.

2. From the opened context menu, select **InfoWatch CryptoStorage** (see Figure 3).

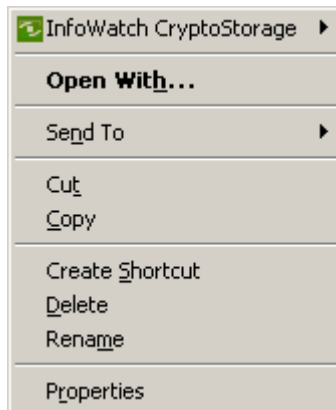


Figure 3. The InfoWatch CryptoStorage menu

This menu item contains a submenu which depends on the type of object and whether the object is protected or not.

3.4. Encrypting Existing Objects

Attention!

You can protect files and folders only within the NTFS file system.

You can protect any file, folder, disk volume or removable disk against unauthorized access.

With the System, an **object owner** can:

- encrypt\ decrypt objects;
- re-encrypt objects using new parameters;
- interrupt the process of encryption\decryption\re-encryption;
- resume encryption\decryption\re-encryption if the process was interrupted. The function is available even if an unexpected situation occurred (for example, when the computer's power supply was turned off);
- cancel encryption\decryption\re-encryption and return to the initial state (this feature is provided to protect disk volumes and removable disks);
- view information on a protected object;

A **user** can:

- move a protected object on a physical carrier to another computer where the System is installed. At the same time the user can continue using the object.
- permanently wipe any file or folder.

You can start using protected objects only upon authorization. You can read, write and delete data only after attachment.

Pay attention to the special features of using protected objects within a file system:

- When you protect a folder, it means that its files and the files inside its subfolders will be protected too.
- Copies and moved files and folders are protected only by the objects which they are placed inside.
- The System does not support the following operations on the protected objects:
 - moving to the Recycle Bin;

- moving files and folders containing files within one volume.
- Unprotected folders containing protected files and subfolders can be moved within a volume to unprotected folders. In this case protected objects do not have to be attached and at the same time their properties remain.
- An unprotected folder containing protected files and subfolders can be moved to the Recycle Bin if all protected objects are attached.

Note:

For more information, see *"InfoWatch CryptoStorage. User Guide"*.

3.5. Protected Containers

With InfoWatch CryptoStorage, you can create special files – the protected containers. These containers are used as virtual disks after they are attached using InfoWatch CryptoStorage. Moreover, container files can be copied, recorded to CD or DVD, emailed and moved to another computer where the System is installed. At the same time the containers can always be attached.

With the System, you can:

- create containers on a hard disk, local network resource or removable disk;
- attach containers as volumes or folders;
- re-encrypt using new data;
- cancel re-encryption and roll back to the previous state;
- detach containers after use;
- view information on a protected container.

To create a container, right-click any place in the opened folder or on the desktop. In the opened context menu select **New ► InfoWatch CryptoStorage Container**.

Note:

For more information, see *"InfoWatch CryptoStorage. User Guide"*.

3.6. Managing Access to Protected Objects

InfoWatch CryptoStorage supports multi-user access to objects. A protected object can be used only by the owner of the object and by users who are added by the object owner to the access list. Each protected object has its own access list.

Each subfolder located inside a protected folder has its defined access list containing a part of the access list of the external (parent) folder. Therefore, the System supports the following access management functions for the **owner** of the folder:

- adding a new user to the access lists of the folder and its subfolders;
- adding an existing user to the access lists of the folder and its subfolders;
- removing a user from the access lists of the folder and its subfolders.

While managing protected files, containers, disk volumes and removable disks, an **owner** can:

- add a new user to an access list;
- remove a user from an access list.

Note:

For more information, see *"InfoWatch CryptoStorage. User Guide"*.

CHAPTER 4. CONCLUSION

InfoWatch CryptoStorage offers you many other functions which are not covered in this document.

This document contains introductory information and describes the main features of the System to help you install and start using CryptoStorage.

Remember that you must take steps in the order described below to safely protect confidential information on your computer:

- Install InfoWatch CryptoStorage and make sure that its subsystems are running.
- Define objects which must be protected.
- Check whether the objects can be encrypted by the System, i.e. whether they meet specific requirements of the encryption process.
- Encrypt the objects.

Once you have completed the steps, you can start using protected data by attaching the protected objects if required.

Detailed information on the encryption process, specific features of using protected objects, recommendations on how to create a strong password and how to manage access to protected objects, see in *"InfoWatch CryptoStorage. User Guide"*.