AxCrypt File Encryption Software for Windows

Quick Installation Guide

Version 1.6

November 2004

This guide describes how to install and quickly get started using AxCrypt to encrypt, decrypt, edit, store and send documents privately and securely.

The following topics are covered:

1. Additional information
2. Requirements and limitations
3. Installation procedure
4. How to use
5. Information on security

1. Additional information

This quick guide only contains the basic information necessary to get started with AxCrypt.

Please refer to the following resources for further information:

Where	What
http://axcrypt.sf.net	• Full Documentation • Privacy Policy • FAQ • Command Line Usage
http://www.axantum.com	• Introduction to encryption • White Paper 'About AES' • White Paper 'Public Key Based Licensing' • Information about other encryption software • About the maker of AxCrypt
http://sf.net/projects/axcrypt	• Source code • Beta versions • Forums • Mailing list

2. Requirements and Limitations

AxCrypt requires very little and is compatible with all current versions of Windows.

Resource	Value
Memory (RAM)	About 5 Mega bytes of virtual memory when active.
Hard disk space	2 Mega byte
Temporary disk space	Up to about 1.5 x the size of a file being encrypted.
Processor	Pentium
Operating System	Windows 98, ME, NT 4 sp 4, 2000, XP Home, XP Professional, 2003
User permissions	Any user can run AxCrypt
Installation permissions	Administrator in NT, 2000, XP and 2003.
Maximum file size	About 500 – 700 Mega byte on Windows 98 and ME. Only limited by disk space on NTFS.
Maximum number of encrypted files	Only limited by disk space.
Development environment	To recompile AxCrypt from downloaded source code you need Visual Studio 2002 or later.

3. Installation Procedure

This section will explain how to install AxCrypt, step by step.

> *Important! You must be logged in as a system Administrator to install AxCrypt on Windows NT 4, 2000, XP or 2003.*

Get the latest version

☞ To install AxCrypt you need the installation program, please find and download the most recent release on http://axcypt.sf.net before continuing.

When you download, you may chose to either store the file on your computer, and run it later or you may run it directly from the download site. If you run it directly, skip directly to 'Verify Digital Signature' below.

Run the installer

The installer is typically named `AxCrypt-Setup.exe`, but it may also be named after the version, for example `AxCrypt-1.6.exe`.

Double-click the program to run it.

Verify Digital Signature (Windows XP Service Pack 2 or later)

Windows XP Service Pack 2 or later supports automatic verification of digital signatures of executables downloaded from the Internet such as the AxCrypt installer.

The digital signature gives you some assurance, if properly verified, that the software is not infected with a virus or contains other hostile code.

AxCrypt is digitally signed by Axantum Software AB so you can ensure its authenticity.

You should see a dialog similar to the following:

☞ If you do not see a dialog at all this is not a problem – only if you see a dialog like above, but which cannot be verified or contains unexpected names should you be wary.

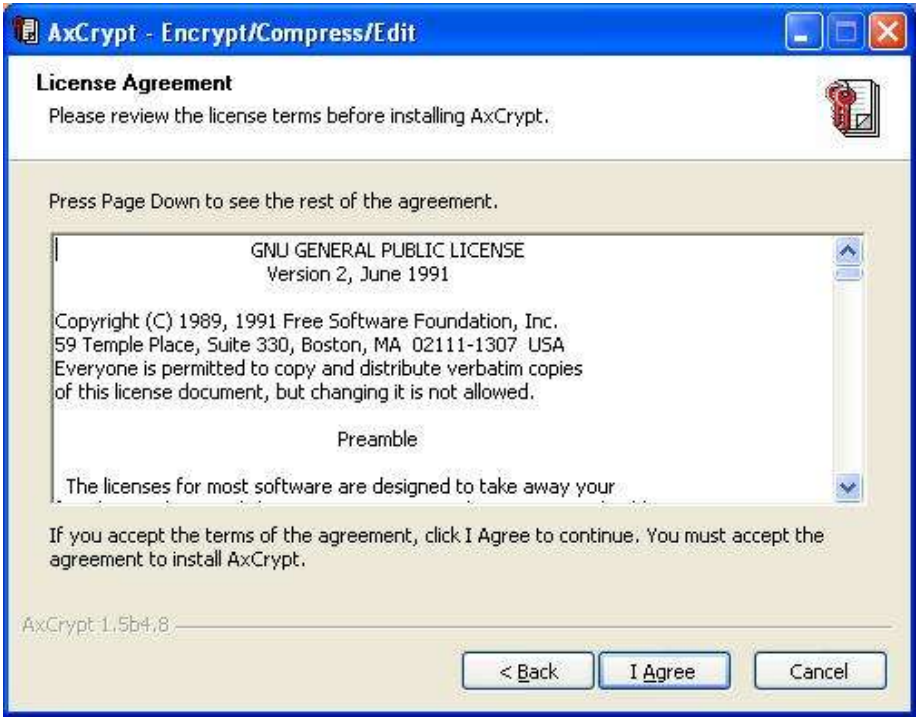
Chose Language

AxCrypt supports a number of languages for it's dialogs and commands. Please select a language when prompted:

☞ Click 'OK' when you have selected a language. The rest of the installation will proceed using that language, as will AxCrypt menus and dialogs.

Accept the license agreement

AxCrypt is licensed under the GNU General Public License. This is an open source license which essentially gives you the right to free use and distribution of AxCrypt as long as you do not charge money for the software, and that you make any changes available in source code form as well.



Click 'I Agree'.

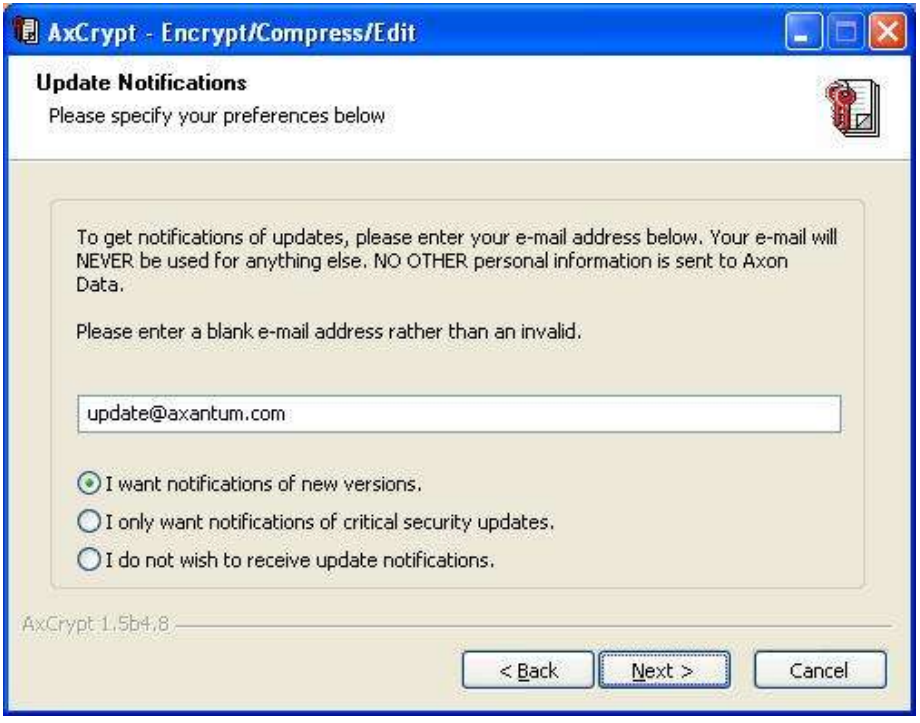
Sign up for notifications of updates

As a user of AxCrypt you may sign up for free notifications of updates. There are three levels available:

- Notifications are sent for every new version.

- Only send notifications of critical security fixes.
- Do not send any notifications (not recommended).

☞ Please do not supply an invalid e-mail address! If you do not wish to supply one, just leave the field blank.

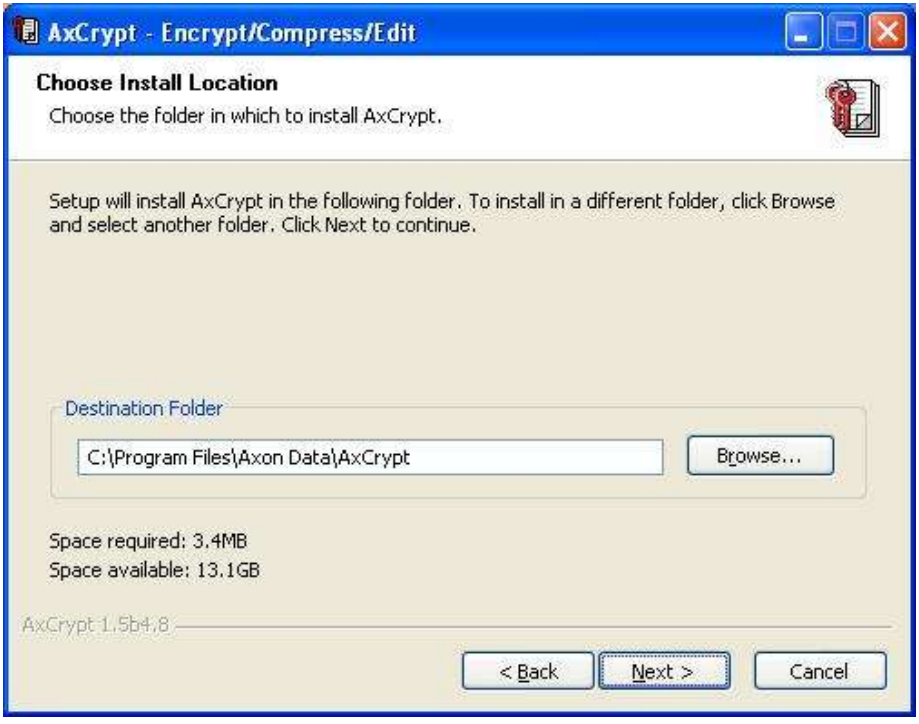


✍ Enter you valid e-mail, or blank the field
✍ Select your notification level
✍ Click 'Next'

Chose Where to Install (Advanced Users Only)

You have the option to change the location where AxCrypt is installed.

There is no normally no need to change this, just leave this as it is unless you know why you want to change it.

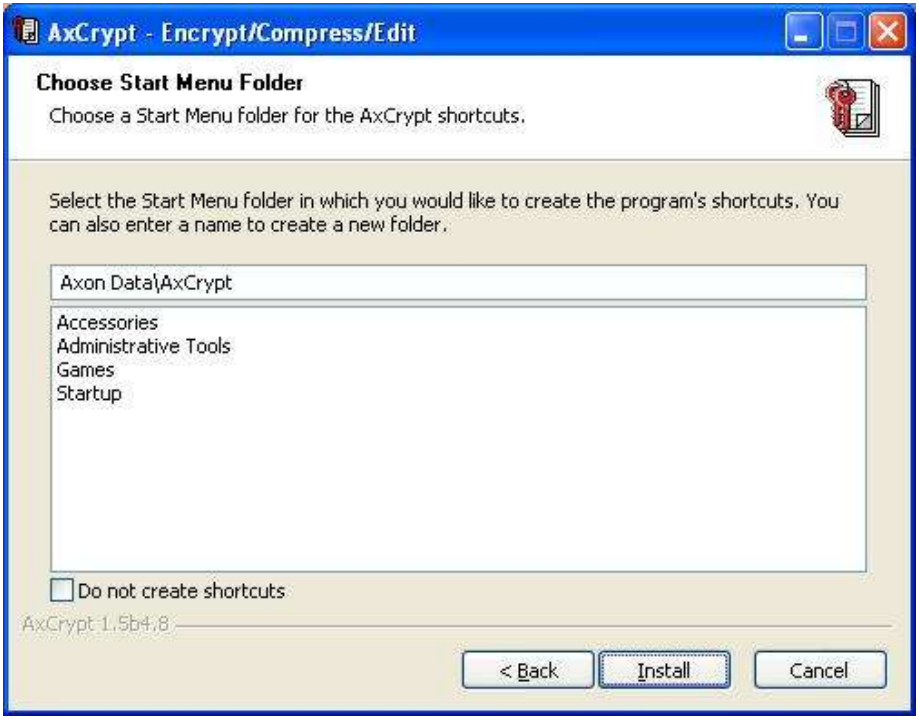


- Click ‘Next’

Choose a Start Menu folder (Advanced Users Only)

You now have the option to change the default location of the Start Menu items.

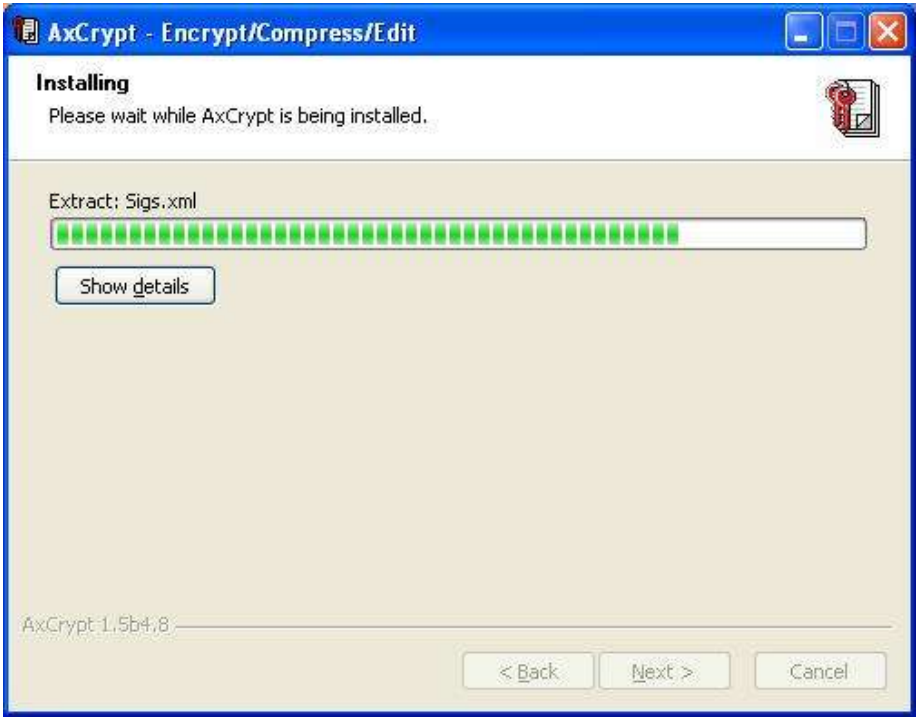
There is usually no need to do this, only do so if you know why you need to.



- Click ‘Install’

The program is installed

AxCrypt will now be installed, and you will see the progress. The installation will typically take between 5 and 20 seconds.



Accept the Internet Connection

If you elected to be notified of updates, AxCrypt will now connect with an Axantum server and send the information.

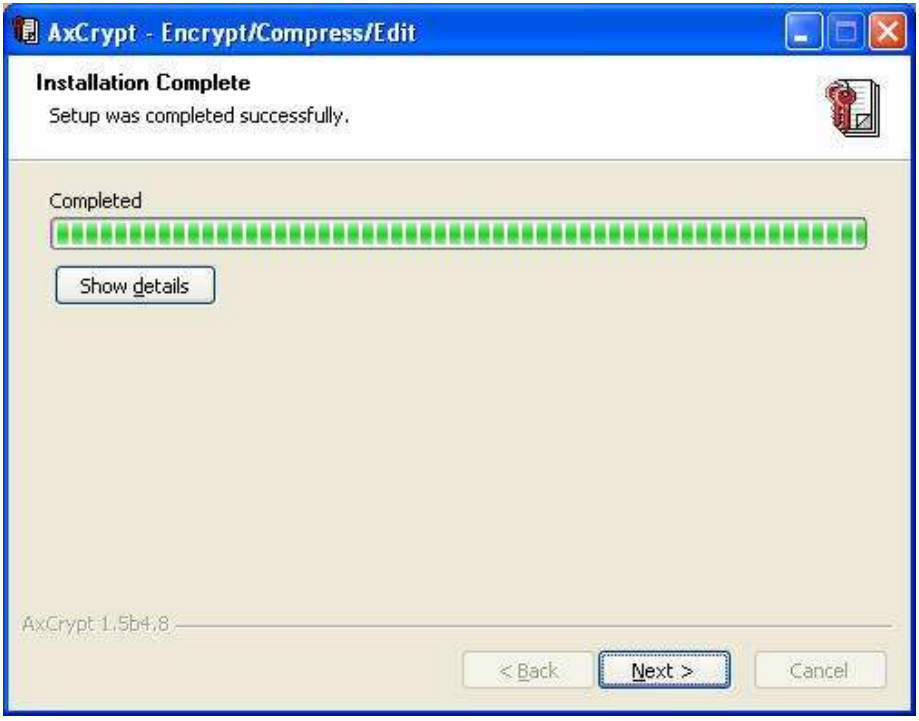
Even if you elected to decline notifications, we'd like to know a few basic facts about the installation – and also just knowing that it's being used is often the only reward we get, so please accept.

No personal information is sent, the section on privacy policy on the AxCrypt web site, http://axcrypt.sf.net details what is sent. The actual string sent is also shown in the dialog.

- Click ‘Yes’ or ‘No’.

Installation is complete

The installation is complete. Please read the next chapter on how to use AxCrypt.



- Click ‘Next’

4. How to use

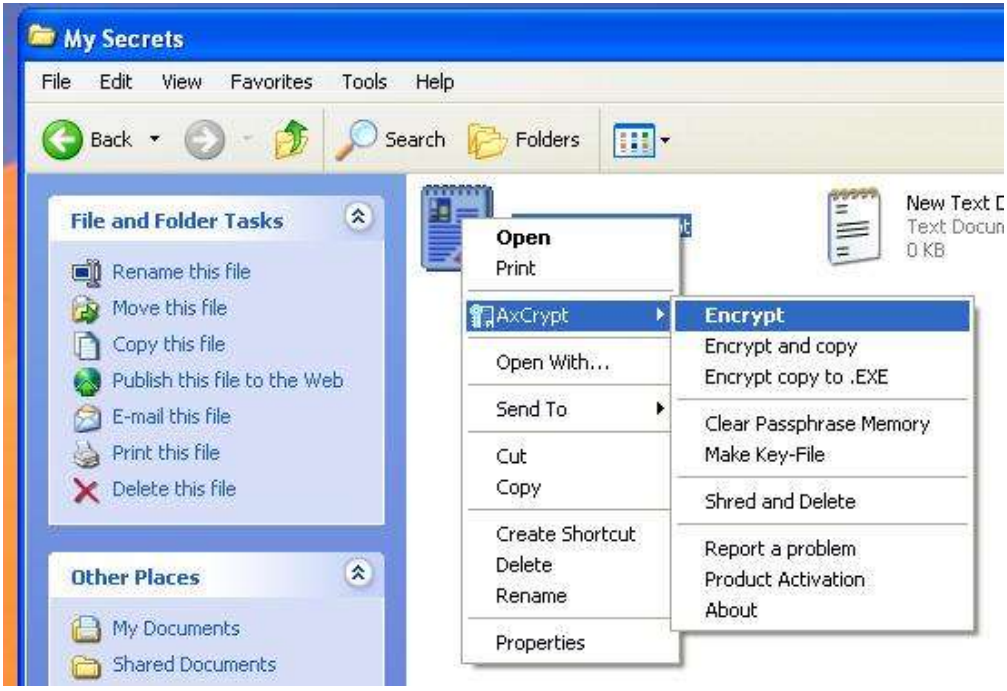
AxCrypt can be used from the command line, from other programs and interactively as a part of Windows Explorer – which is the usage this guide describes. Please see the product home page for details on other usage.

Windows Explorer displays your desktop and is the part of Windows normally used to navigate among all your files and documents, where you *double-click* to open for example.

Context menu

In Windows Explorer you *double-click* to open a document, but you may also *right-click* to see a menu of choices appropriate for the particular document.

This *right-click* menu is called the *context menu*. This is where you'll find most of the functionality of AxCrypt.



Encrypt

To encrypt a file, *right-click* it and select 'Encrypt'. You'll be asked to provide a pass phrase and optionally a key-file.

Using a key-file will ensure that the full strength of AxCrypt is applied, but is beyond the scope of this short guide.

Enter a pass phrase, i.e. a sequence of secret strings. This is the secret that will protect your data from viewing by others and undetected tampering.

☞ ***Please note that encryption does not protect you from data loss. Regular backup copying is the only method that will do this.***

Enter your pass phrase a second time for verification. It is vital that you ensure that you actually type what you think you type, and that you remember this pass phrase.

✍ Click 'OK'

☞ ***There are NO BACKDOORS into AxCrypt. If you forget your pass phrase your documents are likely to be irretrievably lost. Write it down, or print it, and keep it in a safe place.***

Open an encrypted document

The encrypted document will have the .axx extension, and be shown with the AxCrypt icon.

To conveniently decrypt the file, just *double-click* it to open it in its own application, and when done have it re-encrypted if modified.

Decrypt an encrypted document

To permanently decrypt a document, *right-click* it, select 'Decrypt' and enter the pass phrase when prompted.

- Click 'OK'

The file will be restored to it's original name and contents.

The pass phrase memory

AxCrypt has the capability to remember any number of pass phrases for decryption, and a default pass phrase for new encryption.

This memory is only as long as your logon session.

☞ If you use the pass phrase memory, you should be using a password protected screen saver, and not leave your system unattended.

To enable this feature, use the provided checkbox options on the pass phrase dialog. The dialogs above show these checkboxes at the bottom.

All options in AxCrypt are 'sticky' – this means that the default is the same as your last choice.

Shredding documents

Did you know that documents that you delete can be very easily recovered by any number of third party tools commonly available on the Internet? One of them is even built into recent versions of Windows – the recycling bin.

With AxCrypt you can elect to delete files and documents in a more permanent way.

Select the files you want to shred, and select the 'Shred' option on the *right-click* menu.

You will always be asked to confirm this, since this operation cannot be undone.

☝ Click 'OK' or 'Cancel' as the case may be.

If you clicked 'OK' your data will now be overwritten with random data before being permanently deleted.

Advanced use

AxCrypt supports a number of a advanced uses which will only be mentioned briefly here:

- You can rename encrypted files to anonymous names – the original names will still be restored on decryption.
- You can create self-decrypting files that you can ship to users who do not have AxCrypt installed.
- There is an install-free decrypt-only 'viewer', AxDecrypt, which you and others can use to decrypt without installing the full program.
- You can create and use key-files which are files with randomly generated strong keys ensuring that your information security is not subject to weaknesses in your chosen pass phrase. These may (and should) be stored on removable media such as USB-drives.

5. Information on security

Encryption alone can never ensure security. It often is a vital tool, but as all tools must be used carefully. A single tool will seldom solve all security needs.

This section tries to point out some additional aspects to consider when using any file encryption product such as AxCrypt for information security – here taken to mean confidentiality and integrity.

Security provided by AxCrypt

The following is true of a file encrypted with AxCrypt:

- If you are using a key-file, your information is protected by the full 128-bit strength of AES – currently considered unfeasible to break.
- If you are using a pass phrase only, AxCrypt will protect your information within the limits of that pass phrase. If it is too short, security suffers. Anything shorter than 10 characters is short. Full 128-bit strength requires a meaningless sequence of at least 22 characters.

☞ If you are interested in more information about the security of the encryption algorithm AES-128 and AxCrypt, please read the white paper 'About AES' available on the AxCrypt web http://www.axantum.com .

Insecurity by other means

AES-128, and thus presumably AxCrypt, is currently viewed as unfeasible to break, and you're using key-files. Are you secure? Not necessarily. As always, the most effective way past a barrier is around it. This applies to encryption as well. A brief list of some ways around AxCrypt follows:

- When you're editing and viewing documents on a computer, applications and the operating systems may leave full or partial copies of the document in temporary locations or the so-called paging file. This is true of Word and Excel for example.
- You computer may have a keystroke logger installed either physically or via software, thus revealing your pass phrase.
- You may be confronted with legal, economic or physical threats to reveal the pass phrase.

These are just some ways around AxCrypt; the remedies to these various situations vary according to the situation.