F-Secure Desktop 2.0 Help

Contents

What's New

Changes in the User Interface

Web Club

Quick Start

Using F-Secure Desktop

Security

Practical Advice

Notification and Error Messages

Technical Support

Changes in the User Interface

F-Secure Desktop 2.0 is fully compatible with F-Secure Desktop 1.0 and recognizes encrypted files, security profiles, and encryption keys created by F-Secure Desktop 1.0.

What's new in F-Secure Desktop 2.0?

The new features include:

- F-Secure Desktop 2.0 is available not only for Windows 3.x and Windows 95, but also for Windows NT 4.0.
- With F-Secure Desktop 2.0, you can now choose which of the two ciphers, Blowfish or 3DES, will be used for encrypting your data.
- F-Secure Desktop 2.0 can now compress files while encrypting them. This saves disk space and improves security.
- F-Secure Desktop 2.0 can now pack files into compressed encrypted self-extracting packages. The packages can be transferred freely as electronic mail attachments, or through FTP. Files can be extracted from such package under any MS Windows operating system, without the requirement to have F-Secure Desktop 2.0 installed.
- With F-Secure Desktop 2.0, you can now maintain not only the list of Secret files, which are encrypted and decrypted automatically, but also the list of TopSecret files, which are only encrypted, but never decrypted automatically.
- F-Secure Desktop 2.0 has a user interface which is much easier to use. You can control the Secret, TopSecret, and Excluded lists of files through the dialog box of F-Secure Desktop Explorer.

Web Club

One of the most convenient ways you can reach Data Fellows is through the World Wide Web. You can easily reach the Data Fellows Web Club, which provides support to F-Secure Desktop customers, directly from F-Secure Desktop.

To connect to the Web Club, double-click the F-Secure Desktop icon in the Control Panel, then click the **Web Club** button. Alternatively, choose **Web Club** from the File Manager **F-Secure** menu. In Windows 95 and Windows NT 4.0, select a file or folder with the right mouse button and then choose **Properties** from the displayed menu. Click the **Encryption** tab, and then click the **Web Club** button. Refer to Configuring your World Wide Web Browser for information on how to configure your WWW browser for accessing the Web Club nearest to you.

To connect to the Web Club directly from your Web browser, open this location:

- http://www.us.datafellows.com/f-secure/desktop/webclub/.

Creating a New Security Profile

F-Secure Desktop Wizard

The F-Secure Desktop Wizard helps you create a new security profile for F-Secure Desktop, securing the files on your computer that contain sensitive information. If you are upgrading from a previous version of F-Secure Desktop, the wizard will help you upgrade your existing security profile so that you can take advantage of the new opportunities offered by the latest version of F-Secure Desktop.

The wizard uses a number of “pages” to guide you through the security profile configuration process. You can move to the next page by clicking the **Next** button.

If any changes in the security profile are required in the future, click the F-Secure Desktop icon in the Windows Control Panel, or select the Options command from the File Manager F-Secure menu.

Selecting Mode

If you are upgrading from a previous version of F-Secure Desktop, the next page will offer the two options: choose either **Create new security profile** or **Upgrade existing security profile**. Select the first option to create an entirely new user security profile if you are installing F-Secure Desktop for the first time. Select the second option if you are upgrading from a previous version of F-Secure Desktop, so that you can take advantage of the additional opportunities presented by the latest version of the program.

If you are upgrading from a previous version of F-Secure Desktop, you will see not all pages of the wizard, but only those which are new in this version of F-Secure Desktop. If you would like to modify other parameters of your user profile, for example, change your password, refer to Updating Your Security Profile for more information.

Selecting a User Name and Passphrase

Enter your user name in the provided **User Name** field. The user name you specify must be in accordance with the appropriate file naming conventions, because your user name also becomes the name of the file in which your encryption key is stored.

For example, in Windows 3.1 the user name should be no longer than 8 characters, should begin with a letter or a number, and can contain any keyboard characters, except the following: comma (,), colon (:), semicolon (;), equal sign (=), quotation mark (“), slash (/), backslash (\), vertical bar (|), brackets ([ ]), period (.), and spaces. There is no difference between the uppercase and the lowercase letters. The filename extension is reserved for F-Secure Desktop’s use.

In Windows 95 and Windows NT 4.0, the user name may be up to 255 characters and include spaces, but cannot contain the following characters: / \ : * ? “ < > |.

If the user name you entered already exists in the system, the F-Secure Desktop Setup Wizard will ask your permission to overwrite the existing security profile, with the option to choose another user name.

After you have specified your user name, enter the passphrase of your choice in the **Passphrase** and **Confirm Passphrase** fields. The passphrase can be from 6 to 80 characters long and can contain white spaces and any typographical characters. The passphrase is case sensitive, so it differentiates between uppercase and lowercase letters. If you wish to change your passphrase later, you can do that at any time by choosing **Options** from the File Manager **F-Secure** menu or by clicking the F-Secure Desktop icon in the Windows Control Panel, and then selecting the **User** tab and clicking the **Passphrase** button.

Please note that selecting a good passphrase is vital for ensuring the security of your data. The difference between a normal password and a passphrase is that a passphrase is usually much longer, and not a single word, but a phrase which is easy for you to remember, but impossible for others to guess. More information about selecting a good passphrase is available in Some Easy Ways of Making Your Information More Secure.

Click **Next** after you have entered your user name and passphrase, and the next page will be displayed.

Selecting the Secure Delete Process

When a confidential document is encrypted, it is in effect saved on the disk as a new document whose contents are modified so that they cannot be accessed without knowing the passphrase. The original, unencrypted document is deleted from the disk, making it inaccessible to normal users and programs. However, because there are ways to recover some or all of the original deleted information, the space on the disk which contained the information must be overwritten in a secure fashion.

Please specify the number of times the original files will be overwritten, from the following three options:

- Overwriting the file once with random data.
- Overwriting the file first with a pattern, then with its complement, and once with random data.
- Overwriting the file first with a pattern, then with its complement, and finally five times with random data.

You can modify your Secure Delete settings at any time by choosing **Options** from the File Manager **F-Secure** menu or by clicking the F-Secure Desktop icon in the Windows Control Panel and then selecting the **Security** tab.

Selecting a Personal or Shared Encryption Key

Next you will be asked to select your master encryption key. The master key can be one of two kinds: personal if you will only use it to secure your own information, or shared if the key will be used to secure information shared by a workgroup.

F-Secure Desktop encrypts each file with a random encryption key. Then the random encryption key is encrypted with your personal encryption key or your shared encryption key and stored in the header of the encrypted file. Thus, your personal or shared encryption key is really the master key to all the encrypted files.

You have two options for the personal or shared encryption key.

- You can create a new personal or shared encryption key to be used to protect your data.
- You can select an already existing personal or shared encryption key. It can be: a backup key, a key left on your system after a previous F-Secure Desktop installation, or a key created by someone to share encrypted information among a workgroup.

To create a new key, click **Create new key** button and the **Random Number Generator** dialog box will be displayed.

Move your mouse randomly (scribble) in the dialog box to generate random mouse movements, which can be then be used to create a random seed for the cryptographically strong random number generator that F-Secure Desktop uses. The random number generator then creates the encryption key. You can view the progress on the screen. When enough randomness has been generated, the **Random Number Generator** dialog box will close.

To choose an existing encryption key, click the **Select existing key** button, browse for the key and select it, then, when prompted, type in the passphrase associated with that key. If the passphrase is incorrect, the existing key will be inaccessible, and you will need to create a new encryption key or try to access the key with a different passphrase.

The encryption key you have selected will be stored on your hard disk in the F-Secure Desktop installation directory as a file with your user name as the file’s name and .key as the file’s extension.

It is highly recommended that you create a backup of your encryption key on a floppy disk, according to the instructions provided in the next Help Topic. Should your encryption key be accidentally or purposefully deleted from your computer, you would only need to retrieve the floppy disk with your backup key, copy the backup key into your F-Secure Desktop directory, and you would be able to access your encrypted F-Secure files again!

Backing up Your Encryption Key

The next step is to create a backup of your encryption key, preferably on a floppy disk. This step is necessary, because without a backup key you will not be able to access your encrypted files if your F-Secure Desktop encryption key becomes corrupted or if you forget your F-Secure Desktop passphrase. Refer to Restoring Your Backup Key for information on restoring your encryption key by using the backup.

Enter a passphrase, which will be specifically used to protect the encryption key backup, into the Passphrase and Passphrase Confirmation fields. The passphrase length must be at least 6 characters. It may contain any printing characters, including spaces. The passphrase is case-sensitive, so it will differentiate between uppercase and lowercase letters. This passphrase will serve the sole purpose of protecting your backup key.

After your passphrase is accepted, the **Browse** button is activated. Click the **Browse** button to select the drive and directory where you would like to store your backup, and click **Save** to create the backup of your encryption key.

We recommend that you back up your encryption key to a floppy disk, write the backup passphrase on a piece of paper, seal the floppy disk and the note into an envelope, and store the envelope in a safe or other secure location. This is the only way to ensure that you would be able to restore your data in case you forget your encryption passphrase.

Now the **Next** button is activated, click it and the **Secret** page will be displayed.

Selecting Secret Files

The next dialog box displays the list of your Secret files, which should be empty if you have just installed F-Secure Desktop. The Secret files are encrypted and decrypted automatically. Automatic encryption of all Secret files takes place when you end your Windows session or execute the **Start Auto Encryption** command. Automatic decryption of all Secret files is performed when you begin your Windows session or execute the **Start Auto Decryption** command. Each time when F-Secure Desktop is about to perform automatic encryption or decryption, it prompts you for your passphrase. This ensures that nobody else, but the owner, is able to access the Secret files.

The Secret file list can contain individual files and entire folders of files. Since you have just installed F-Secure Desktop, the Secret list is empty. You can add files to the Secret list now or at a later time. Click the **Change** button to add files to the Secret file list now. Refer to Managing File Lists for information on how to edit your Secret list after you have created your security profile.

After you have clicked the **Change** button, the **F-Secure Desktop Explorer** dialog box is displayed.

In the upper half of the dialog box, the files and folders are shown. The lower half of the dialog box contains the Secret list. You can add to the Secret list individual files, groups of files, or whole file folders. In the latter case, if you put a folder on the Secret list, all the files from this folder will become Secret. Although it is possible to select an entire drive for automatic protection, it is not recommended to encrypt whole drives. If you choose to add an entire drive to the Secret list, confirmation will be requested.

In the upper half of the dialog box, browse for the file or folder you would like added to the Secret list. Select the file or folder with the right mouse button and choose **Secret** from the displayed menu. Alternatively, select the file or folder with your left mouse button and choose **Secret** from the **File** menu. You can also add files and folders to the Secret list by dragging them while pressing the left mouse button and dropping them on the list.

When you add a file or folder to the Secret list, they appear on the Secret list, and their icons are changed to the following icons:
. If you add a folder to the Secret list, its icon is changed to
and all the files it contains also become Secret files and their icons are changed respectively to
.
To remove an item from the list, select it with the right mouse button and choose the **Remove From List** command from the displayed menu. Alternatively, select the file with the left mouse button and choose the **Remove From List** command from the **File** menu.

After you have added files to the Secret list, click **OK** to save your changes, or **Cancel** to cancel the changes. Then click **Next** to move to the next dialog box.

Selecting TopSecret Files

The TopSecret files are even more secret than the Secret files. They are encrypted automatically at the end of Windows session or by **Start Auto Encryption** command, just like Secret files, but can be decrypted only manually. After you decrypt a TopSecret file manually and work with it, it is automatically encrypted again at the end of Windows session or by executing the command and remains that way until you need to decrypt it again. Since you have just installed F-Secure Desktop, your TopSecret list is empty.

To add files to the TopSecret list, click **Change**. The **F-Secure Desktop Explorer** dialog box is displayed with the TopSecret list in its lower half. You will be able to access this dialog box at any other time to modify your TopSecret list. Refer to Managing File Lists for more information on **F-Secure Desktop Explorer**.

To add files or folders to the TopSecret list, select them with your right mouse button and click **TopSecret**. You can also select them with your left mouse button and choose **TopSecret** from the **File** menu, or drag-and-drop files and folders into the TopSecret list. The file or folder will appear on the list, and its icon in the F-Secure Desktop Explorer dialog box will change to one of the following icons: .

Just like with Secret list, if you add a folder to the TopSecret list, all the files it includes also become TopSecret, and their icons are respectively changed to the following: . Although it is possible to select an entire drive for automatic protection, it is not recommended to encrypt whole drives. If you choose to add an entire drive to the TopSecret list, confirmation will be requested.
Incidentally, a file you would like added to the TopSecret list may already be on the Secret list. In this case, two options are possible. First, the file can be on the Secret list as a part of its parent folder. In this case, when you add this file to the TopSecret list, it also remains on the Secret list. Because the TopSecret list has a higher priority than Secret list, however, any file which is simultaneously on both lists is essentially a TopSecret file, and has the corresponding icon.

The other possibility is that the file has been added to the Secret list “personally.” In this case, when you add such file to the TopSecret list, it is automatically removed from the Secret list.

To remove a file or folder from the TopSecret list, select it with the right mouse button and choose the **Remove From List** command. Alternatively, select the file or folder with your left mouse button and choose **Remove From List** from the **File** menu. Refer to Managing File Lists for more information about editing F-Secure Desktop file lists.

After you have selected TopSecret files, click **OK** to save your changes, or **Cancel** to cancel the changes. Then click **Next** to move to the next dialog box.

Selecting Files to Be Excluded from Automatic Protection

F-Secure Desktop maintains a list of Excluded files, which are not subject to automatic encryption even though they may also be on the Secret and TopSecret lists. However, if necessary, the files from the Excluded list may be encrypted manually.

After you have installed F-Secure Desktop, the Excluded file list already contains the following files that are not recommended for encryption: all the files with the .exe, .dll, .bat and .key extensions, and files in certain system directories

Click the **Change** button if you would like to modify your Excluded list. The **F-Secure Desktop Explorer** dialog box is displayed with the Excluded list in its lower half. You will also be able to access this dialog box at any other time. Refer to Managing File Lists for more information on **F-Secure Desktop Explorer**.

To add files or folders to the Excluded list, select them with your right mouse button and click **Excluded**. You can also select them with your left mouse button and choose **Excluded** from the **File** menu, or drag and drop files and folders into the list. The file or folder will appear on the list, and its icon in the F-Secure Desktop Explorer dialog box will be changed to one of the following: . If you add a folder to the Excluded list, all the files it contains are also added to the list and their icons are changed respectively to the following: . Drives can also be added to the Excluded list, without any restrictions. In this case, all files and folders on the Excluded drive also become Excluded.

In addition to the above methods, it is possible to add new entries with wildcards to the Excluded list, for the example: *.exe, which will make Excluded all the files with the .exe extension. To add such an entry, choose **New Excluded Entry** from either the **File** menu or from the right-clicking menu and the new entry without a name will appear on the Excluded list. Type in the name of the entry, for example: *.exe, or C:\Windows\*.exe.

To edit the name of an entry, select it on the list and either click the entry's name with the left mouse button, press F2, or choose **Edit Excluded Entry** from the **File** menu. Alternatively, select the entry on the list with the right mouse button and choose **Edit Excluded Entry** from the displayed menu. Then edit the name of the entry.

Please notice, that the Excluded list has the highest priority of all the three lists. Hence, if one file is simultaneously on the Excluded list and on one (or both) of the TopSecret and Secret lists, the file in question is essentially an Excluded file.

To remove an item from the Excluded list, select it with the right mouse button and choose **Remove From List** or select it with the left mouse button and choose **Remove From List** from the **File** menu. Refer to Managing File Lists for more information about editing F-Secure Desktop file lists.

After you have added files to the Excluded list, click **OK** to save your changes, or **Cancel** to cancel the changes. Then click **Next** to move to the next dialog box.

Selecting the Compression Option

F-Secure Desktop offers an option of compressing your files during encryption. Select the check box if you would like to save space on the disk and enhance security.

Do not select the check box if speed of encryption is your main consideration, since compression slows down both the encryption and decryption processes.

Selecting the Encryption Algorithm

There are two options for the encryption algorithm that will be used to encrypt your data. Both algorithms are regarded as very reliable and unbreakable. Select either the 3DES (three key triple-DES), which is a modification of the very well-respected and mature DES (Data Encryption Standard) cipher, or Blowfish, which is a fairly young, compact, and very fast cipher. Refer to F-Secure Desktop's Encryption Technology, for more information on the Blowfish cipher.

Finishing the Security Profile Setup

When the Setup is completed, F-Secure Desktop Wizard will confirm that. Click **Finish** to exit Setup and to save your security profile, or **Back** if you would like to return to a previous page for revision.

After you click **Finish**, a dialog box is displayed asking whether you would like to have your computer restarted. Select **Yes**, to have Windows restarted immediately, and select **No** if you would like to restart your computer at a later time.

You can change your passphrase, or edit your Secret, TopSecret, and Excluded lists of files at any time by using the **Options** command from the File Manager **F-Secure** menu, or by clicking the F-Secure icon in the Windows Control Panel.

Upgrading Security Profile

F-Secure Desktop 2.0 is fully compatible with F-Secure Desktop 1.0 and understands encrypted files, security profiles and keys created with the previous version. If you have been using F-Secure Desktop 1.0, your user profile is preserved during installation. When F-Secure Desktop Wizard starts after the program installation, its second dialog box offers you to upgrade the existing security profile to take advantage of the additional opportunities now available.

Select the **Upgrade existing security profile** option, click **Next**, and in the next dialog box select your user name from the list.

After selecting your user name, click **Next** and the wizard will present you with dialog boxes offering the additional options newly available in the latest F-Secure Desktop version. Refer to Creating a New Security Profile for more information about selecting the appropriate options. See the Help Topics: Selecting TopSecret Files, Selecting the Compression Option, and Selecting the Encryption Algorithm.

Overview

Using F-Secure Desktop is very easy. You can encrypt and decrypt data manually or automatically. Automatic encryption and decryption can be performed at the end and beginning of the Windows session, or by executing the **Start Auto Encryption** and **Start Auto Decryption** commands.

Three file lists, maintained by the F-Secure Desktop, define which of the above methods is used for a particular file. The Secret file list contains files which are encrypted or decrypted automatically, the TopSecret list contains files which are only encrypted, but not decrypted, automatically, and the Excluded list contains files which are never encrypted automatically.

Customize your F-Secure Desktop environment to suit your particular security needs by actively managing the Secret, TopSecret, and Excluded files lists through F-Secure Desktop Explorer. Refer to Managing File Lists for more information.

F-Secure Desktop will not encrypt files having the attributes of read-only, hidden, or system files, because encrypting such files could cause your system to malfunction.

Securing Files with Automatic Protection

Automatic Decryption at the Beginning of Windows Session

Every time you start your Windows session, you are prompted by F-Secure Desktop to type in your passphrase, so that your Secret files can be automatically decrypted.

Enter your passphrase to perform decryption or choose **Cancel** if you would like to leave the files encrypted. You can decrypt them later either manually, or automatically by executing the **Start Auto Decryption** command or by clicking the Auto Decrypt Files icon in the Program Manager F-Secure Desktop program group.

Automatic Encryption at the End of Windows Session

When you end your Windows session, you are prompted to enter your passphrase again, so that Secret and TopSecret files can be encrypted automatically.

Enter your passphrase to encrypt the Secret and TopSecret files.

If you choose Cancel, your Secret and TopSecret files will remain unencrypted and unprotected until your next Windows session.

Automatic Decryption with Start Auto Decryption Command

If you need to have all your Secret files decrypted after the beginning of Windows session, open the File Manager and choose **Start Auto Decryption** from the **F-Secure** menu. Under Windows 95 and Windows NT 4.0 you can also select the My Computer icon with the right mouse button and click **Encrypt**. From the displayed submenu, choose **Start Auto Decryption**. Alternatively, double-click the Auto Decrypt Files icon in the F-Secure Desktop program folder.

You will need to enter your passphrase before the files are decrypted.

Automatic Encryption Using Start Auto Encryption Command

If you need to have your Secret and TopSecret files encrypted before you actually leave Windows, open the File Manager and choose **Start Auto Encryption** from the **F-Secure** menu. Under Windows 95 and Windows NT 4.0 you can also select the My Computer icon with the right mouse button and choose the **Encrypt** command. From the displayed submenu, choose **Start Auto Encryption**. Alternatively, double-click the Auto Encrypt Files icon in the F-Secure Desktop program folder.

You will need to enter your passphrase before the files are encrypted.

F-Secure Desktop Windows 95 and Windows NT 4.0 Shell Extension

F-Secure Desktop users running Windows 95 or Windows NT 4.0 can enjoy a state-of-the-art F-Secure Desktop shell extension. Any file, folder, or drive, when selected with the right mouse button, displays two new menu entries: **Encrypt**, and **Secure Delete**.

More:

Quick In-Place Encryption and Decryption

Encryption Property Page

Quick In-Place Encryption and Decryption

Select any file on the Windows 95 or Windows NT 4.0 desktop or in the Windows Explorer with the right-hand button of your mouse, and then choose **Encrypt**. The displayed submenu contains the following commands: **Decrypt**, **Encrypt**, and **Create Encrypted Package**.

Note that, if the file is not encrypted, out of the two possible **Decrypt** and **Encrypt** commands, only one option is available- to **Encrypt** the file. F-Secure Desktop recognizes that this file is not encrypted, and hence does not offer to decrypt it. To encrypt this file, just click the command, and enter your passphrase in the displayed dialog box. Even Excluded files can be encrypted in this way.

Correspondingly, if you select an encrypted file, the submenu includes only the **Decrypt…** command. To decrypt the file, just click the command, and enter your passphrase in the displayed dialog box.

If you select two or more files which are currently in both encrypted and decrypted form, right-click them, and then choose **Encrypt**; the following menu will be displayed:

Now both commands, **Encrypt Selected** and **Decrypt Selected**, are available. To perform the desired operation, click the command of your choice, and enter your passphrase in the displayed dialog box. If the selection contains hidden, system, or read-only files, such files will be left unencrypted.

It is not recommended to encrypt an entire drive, because this can cause your system to malfunction. If you choose to perform encryption on an entire drive, F-Secure Desktop will ask for confirmation before it proceeds encrypting all the files on the selected drive.

Encryption Property Page

Under Windows 95 and Windows NT 4.0, there is an additional **Encryption** property page. To access this property page, select a file or folder with the right mouse button, choose **Properties** from the displayed menu, and then click the **Encryption** tab.

The **Encryption** property page contains the following four options: **None**, **Secret**, **TopSecret**, and **Excluded**. These options indicate the F-Secure Desktop file list on which the selected file or folder is included explicitly. If a file or folder is on a file list due to its extension, or because its parent folder is on that list, the file list options in the **F-Secure Desktop Properties** dialog box are unavailable. If a file or folder is not on any file list, **None** is selected.

You can change the status of the file or folder by selecting another option. Select **None** to remove the file or folder off all file lists; select either of **Secret**, **TopSecret**, or **Excluded** to add or move the file of folder to that list. Refer to Managing File Lists for more information on F-Secure Desktop file lists.

The **Encryption** property page also contains two buttons: **Web Club**, for connecting to the Data Fellows Web Club, and **Options**, for opening the **F-Secure Desktop Properties** dialog box.

Click the **Web Club** button to connect to the Data Fellows Web Club, which offers assistance to all F-Secure Desktop customers. Click the **Options** button if you need to update your security profile: change your passphrase, set up your Web browser, select another encryption algorithm or Secure Delete process, update your F-Secure Desktop file lists. You will be able to do that by using the **F-Secure Desktop Properties** dialog box. Refer to Updating Your Security Profile for more information about the **F-Secure Desktop Properties** dialog box.

Accessing F-Secure Desktop from the Windows File Manager

Encrypting Files Manually

Decrypting Files Manually

Encrypting Files Manually

Even Excluded files can be encrypted manually. In order to encrypt a file manually, start the Windows File Manager. You will see the **F-Secure** menu in the menu bar.

In the File Manager, select the file to be encrypted.

Then, choose **Encrypt** from the **F-Secure** menu, or click the **Encrypt** shortcut button on the File Manager toolbar. You will be prompted to enter your passphrase.

Enter your passphrase into the passphrase field of the dialog box and select **OK**. This starts the encryption of the file, and the progress of encryption is displayed on the screen. You should be able to monitor this progress, unless the encrypted file is too small.

The resulting encrypted file will have the same name as the original file, but its extension will be changed to .fff. If two or more files will have the same name, but different extensions, after encryption they will receive extensions .ff1, .ff2, and so on, depending on the number of the files with the same name.

If the typed passphrase differs from your passphrase as it is stored by F-Secure Desktop, the program will notify you. In this case, enter the correct passphrase, or click **Cancel** to cancel Encryption.

Decrypting Files Manually

In order to decrypt a file manually, start the Windows File Manager. You will see the **F-Secure** menu in the menu bar.

In the File Manager, select the file to be decrypted. Then, choose **Decrypt** from the **F-Secure** menu in the File Manager menu bar, or click the **Decrypt** shortcut button in the File Manager toolbar. Alternatively, just double-click the file in the File Manager window.

Enter your passphrase, into the passphrase field of the displayed dialog box and click **OK**. This will start decryption of the file, and the progress of decryption will be displayed on the screen. You should be able to monitor this progress, unless the file being decrypted is too small. The resulting decrypted file will have its original extension.

If the typed passphrase differs from the your passphrase as it is stored by your copy of the F-Secure Desktop, the program will notify you. In this case, enter the correct passphrase, or click **Cancel** to cancel decryption.

Updating Your Security Profile

You can change your F-Secure Desktop configuration by changing settings in the **F-Secure Desktop Properties** dialog box. This dialog box can be opened either from the Windows Control Panel by clicking the F-Secure Desktop icon, or from the Windows File Manager by selecting **Options** from the **F-Secure** menu. In Windows 95 and Windows NT 4.0 you can also select a file or a folder with the right mouse button, choose **Properties** from the displayed menu, then click **Encryption** tab and choose the **Options** button.

Once the **F-Secure Desktop Properties** dialog box is opened, click the **General** tab to view information about F-Secure Desktop and to connect to the Data Fellows Web Club. Click the **User** tab if you need to change your passphrase. Click the **Security** tab page to choose another encryption algorithm, change your Secure Delete settings and edit your F-Secure Desktop file lists. Click the **Web Club** tab to select and test your World Wide Web browser

More:

Changing Passphrase

Selecting Encryption Algorithm and Other Process Options

Managing File Lists

Changing Passphrase

To change your passphrase, click the **Change Passphrase** button in the **User** page of the **F-Secure Desktop Properties** dialog box.

Type in your current passphrase in the **Current Passphrase** field, and type the new passphrase into the **New Passphrase** and **Confirm New Passphrase** fields. Your new passphrase may contain any typographical characters including spaces, and should be at least 6 characters long.

Selecting Encryption Algorithm and Other Process Options

Click the **Security** tab to choose another encryption algorithm, compression option, and to change your settings of the Secure Delete process.

There are two options for the encryption algorithm that will be used to encrypt your data. Both algorithms are regarded as very reliable and unbreakable. Select either the 3DES (three key triple-DES), which is a modification of the very well-respected and mature DES (Data Encryption Standard) cipher, or Blowfish, which is a fairly young, compact, and very fast cipher. Refer to F-Secure Desktop's Encryption Technology for more information on the Blowfish cipher.

F-Secure Desktop also offers an option of compressing your files during encryption. Select the check box if you would like to save space on the disk and to enhance security. Do not select the check box if speed of encryption is your main consideration, since compression slows down both the encryption and decryption processes.

The Secure Delete process effectively erases the originals of your encrypted files.

There are three options for this process:

- overwriting the file to be erased with random data.
- overwriting the file first with a pattern, then with its complement, and once with random data.
- overwriting the file first with a pattern, then with its complement, and finally five times with random data.

Select the desired options and click **OK**. Click **View Files** to open the F-Secure Desktop Explorer dialog box.

Managing File Lists

The **F-Secure Desktop Explorer** dialog box is a convenient tool for managing the three F-Secure Desktop file lists: Secret, TopSecret, and Excluded. The **F-Secure Desktop Explorer** dialog box can be opened by clicking the Desktop Explorer icon in the F-Secure Desktop program folder, or by choosing the **Desktop Explorer** command from the **F-Secure** menu in the File Manager. Alternatively, it can be accessed from the **F-Secure Desktop Properties** dialog box, by first clicking the **Security** tab, and then choosing the **View Files** button.

In its upper half, the F-Secure Desktop Explorer dialog box displays the hierarchy of files and folders on your computer. The files and folders which belong to a file list are distinguished by special icons. Each file list is denoted by an icon of its own.

The lower half of the dialog box presents the three F-Secure Desktop file lists, only one of which is visible at a time. To go to a particular file list, click its corresponding tab.

Each file can be “personally” only on one F-Secure Desktop file list, but it can also be on a second file list as a part of its parent folder, and it can be on the Excluded list as a file with a particular, for example .exe, extension. Thus, a file can be on two, or even three file lists simultaneously.

The Excluded file list has the highest priority of the three file lists, and is followed in priority by the TopSecret list. This means, that any file, which is on the Excluded list and on another file list simultaneously, is essentially an Excluded file, and will have the following Excluded file icon: . Similarly, if a file is simultaneously on the TopSecret and Secret file lists, it is essentially a TopSecret file, which is also reflected by its icon:
.

To add a file or folder to a file list, select it with the right mouse button and choose from the displayed menu the command which corresponds to this list. You can also choose the same command from the **File** menu, or use the corresponding shortcut button on the toolbar, after having selecting the file of folder with the left mouse button.

Alternatively, click on the tab of the file list you want to edit, then drag a file or folder from the upper half of the dialog box and drop it into the file list. You can also grab a file or folder from one file list, drag it, and then drop it on the tab of a different file list. This will move the item from one file list to another.

You can also add new entries to the Excluded file list by choosing the **New Excluded Entry** from the **File** menu, or from the right-clicking menu. After the new entry appears on the Excluded list, type in its name, for example: *.exe. This will add all the files with the .exe extension to the Excluded list. To edit an Excluded list entry, select it on the list with the right mouse button and choose **Edit Excluded Entry** from the displayed menu. Alternatively, select the entry on the list with the left mouse button and then either press F2, or click on the entry's name with the left mouse button, or choose **Edit Excluded Entry** from the **File** menu. Then, edit the name of the entry.

To remove a file or folder from a list, select it with the right mouse button and choose the **Remove From List** command from the displayed menu. You can choose the same command from the **File** menu, after having selected the file of folder with the left mouse button.

Using F-Secure Desktop Wizard

F-Secure Desktop Wizard is started automatically after you have installed F-Secure Desktop, and helps you create a new security profile, or upgrade a security profile created with the previous version of F-Secure Desktop.

When launched as an independent program, F-Secure Desktop Wizard serves for creating additional and editing existing security profiles. To start F-Secure Desktop Wizard, use the F-Secure Desktop icon in the F-Secure Desktop program folder.

Once you have started the wizard, read information on the first page, and then click **Next** to move to the second page. Use the **Back** and **Next** buttons to navigate. You can exit the wizard at any time by clicking **Cancel**.

More:

Selecting Mode

Updating Existing Security Profile

Selecting Mode

In the second dialog box of the wizard, you can choose between creating a new security profile or editing (upgrading) an existing security profile.

If you are creating a new security profile, select the **Create New Security Profile** option. See Creating a New Security Profile for information on how to select options for your new security profile.

If you wish to update an existing security profile, including the one created by the previous version of F-Secure Desktop, select the other option. The other option will be either to **Edit Existing Security Profile**, or to **Upgrade Existing Security Profile**, depending on whether the wizard was started independently or after F-Secure Desktop installation. Then click **Next**.

Updating Existing Security Profile

In the displayed dialog box, select your user name from the list and click **Next**. F-Secure Desktop will ask you to enter your passphrase. Type in the passphrase and click **OK**.

If you wish to upgrade a security profile created by the previous version of F-Secure Desktop, see Upgrading Security Profile for more information.

If you wish to edit a security profile created by the current version of F-Secure Desktop, launch the wizard by clicking F-Secure Desktop Wizard icon in the F-Secure Desktop program folder. Refer to Creating a New Security Profile for information on selecting new options for your security profile.

Restoring Your Backup Key

You may use your backup key to restore your security profile if your key file in the F-Secure Desktop installation directory becomes corrupted or if you forget your passphrase.

If your key file becomes corrupted, insert the disk with the backup key into the floppy drive and copy your backup key into F-Secure Desktop installation directory giving it the name and extension of the corrupted key file. Now you will be able to use your key again, although not with the original passphrase, but with the passphrase you had created for the backup. Click the **Change Passphrase** button on the **User** page of the **Options** dialog box to change the passphrase to your original one.

In case you forgot your user passphrase, set up a new user, and when prompted to select a key, select the Backup.key. After the new security profile has been created, you will be able to decrypt your encrypted files with the newly selected key.

Creating Encrypted Packages

With F-Secure Desktop you can pack files into a self-extracting compressed Encrypted Package, which can then be added to an electronic message and sent over e-mail. Because the package is self-extracting, the person who receives it will not have to run F-Secure Desktop in order to open it. The only thing needed to extract the files is the passphrase, which can be shared between the correspondents in advance. The recipient will only need to run the file, and enter the passphrase in order to open the package.

The self-extracting Encrypted Package can contain several files, folders or groups of files and folders. Please note, that the Encrypted Package does not preserve the original directory structure, and only contains the files themselves and their original names. The original files and folders remain intact. If you need to delete them in a secure fashion, use the command **Secure Delete** from the File Manager **F-Secure** menu or the Windows 95 and Windows NT 4.0 right-clicking menu.

To create a self-extracting Encrypted Package, open the File Manager and select the file, folder or a group of those, located in one folder. Then choose **Create Encrypted Package** from the **F-Secure** menu or click the **Create Encrypted Package** shortcut button on the toolbar.

In Windows 95 or Windows NT 4.0, start the Windows Explorer and select the file, folder or a group of those, located in one folder, with the right mouse button. Choose **Create Encrypted Package** from the displayed menu.

Then enter a passphrase into the presented dialog box. The passphrase can be from 6 to 80 characters, and can include any typographical characters.

The most difficult part would be to make this passphrase available to the package recipient. But then, the two of you can choose a passphrase beforehand, or agree on using some passphrase you already share without naming it explicitly.

After you have entered your passphrase, another dialog box appears, where you can enter the package’s name, and its location on your computer’s hard drive. Browse for the directory where the created package will be stored. In the box below enter the name of the package. You can choose the default, or type in a name of your own. If the package is being created under Windows 95 or Windows NT 4.0, a long name can be entered. In this case, when the package is received under Windows 95 or Windows NT, it will have its long name preserved. If the package is opened under Windows 3.1, the recipient will have an opportunity to choose an 8-character name, including the default one.

After the package has been created, you can attach it to your e-mail message.

Secure Delete

Use the **Secure Delete** command to securely delete your files which contain sensitive information, for example the ones you have sent as Encrypted Packages. To perform secure deletion, first select the files or folders to be deleted in the File Manager or Windows Explorer. Then choose the **Secure Delete** command from either the File Manager **F-Secure** menu or from Windows 95 and Windows NT 4.0 right-clicking menu. You will be prompted for confirmation before the data is actually deleted.

Refer to Selecting Encryption Algorithm and Other Process Options for information about changing the settings of your Secure Delete process.

Configuring your World Wide Web Browser

You can configure and test your World Wide Web browser for accessing the Data Fellows Web Club by clicking the **Web Club** button on the General page of the **F-Secure Desktop Properties** dialog box. You can either choose the browser yourself by clicking **Change Browser** or accept the default one, the path to which is shown in the **Browser** field. From the **Area** list of locations choose the location which is the closest to you. Click **Test** to test your selected browser. See Updating Your Security Profile for information on accessing the **F-Secure Desktop Properties** dialog box.

Maintaining a Resolute Information Security Policy

There are two fundamental requirements for maintaining a resolute information security policy:

- Every document must have a designated owner.
- All documents have a level of confidentiality, which must be specified.

The owner is the person ultimately responsible for the document. This includes the storage, processing, and distribution of the information. The specification of confidentiality makes it possible to create directives guiding these operations. The directives should hold regardless of the medium on which such information is stored, whether it be in a database, individual files, or on paper.

One effective method of creating an information security policy is to use the following four simple specifications of confidentiality for all the documents:

- Public information is available to everyone. No special directions are given regarding storing or processing. An example of public information is the list of organization's direct phone numbers.
- Corporate information is not meant to be viewed by outsiders. Documents containing corporate information should not be left on the screen when leaving the computer and visitors are passing by, for example. Printouts containing corporate information should not be left on the desk overnight. An example of corporate information may be a list of the company's clients.
- Confidential information is to be viewed by a selected group of people only. Printouts containing confidential information should be stored in an archive or other location secure and away from any accidental visitor. The document should display "Confidential" in its header. An example of confidential information is the coming year's detailed marketing budget.
- Classified information is essential for the operations of each organization. It includes business secrets and other data that could harm the organization if leaked to outsiders. Printouts containing classified information should be stored in locked archives. The document should display "Classified" in its header. If a classified document is not needed anymore, it should be run through a paper shredder. Some examples of classified information are business plans and Research & Development documents.

If the owner of a document cannot decide its correct level, the owner's superior should determine the specification.

To maintain a policy of this kind most effectively, you can place all confidential and classified information under the protection of F-Secure Desktop with complete confidence.

F-Secure Desktop's Encryption Technology

F-Secure Desktop is designed with two objectives in mind: ease of use and top security. The ease of use comes from the fact that the files to be kept confidential are transparently encrypted/decrypted when starting and closing your Windows session. You know that your information is safe whenever you have logged out in a normal fashion.

Top security is provided with state-of-the-art encryption technology. F-Secure Desktop uses a fast well-known public block-cipher encryption algorithm called Blowfish. Blowfish was designed specifically for 32-bit computers by Bruce Schneier, a well known cryptography author. The Blowfish encryption algorithm has lasted several years of public cryptanalysis and reviews in numerous cryptography conferences.

F-Secure Desktop uses Blowfish with 256-bit encryption keys generated using a cryptographically strong random number generator.

During installation a master key is generated for access to all encrypted files. This master key is used to encrypt a random encryption key, generated for each file at the beginning of the encryption process.

Each encrypted file contains two sets of encrypted information; the random encryption key encrypted with the master key and the original file contents encrypted using the random encryption key.

To decrypt the file, first the random encryption key is recovered using the master key. The random encryption key can then be used to restore the original file in an unencrypted format.

The master key is never stored unprotected on your hard disk. It is encrypted using a 256-bit key generated from the user’s passphrase. Blowfish is again used to encrypt the master key.

Some Easy Ways of Making Your Information More Secure

Creating and maintaining security of the highest possible level is usually not feasible. Instead, you should target a level of security which is high enough for your organization’s needs, but which is still possible to achieve with reasonable effort and investment.

More:

Create Guidelines for Selecting Passphrases

Create Guidelines for Selecting Passphrases

Create simple guidelines for selecting passphrases. Remember that a good passphrase should be:

- Hard to guess
- Easy to remember without writing it down
- A short sentence you can easily remember or a traditional password made of random letters, numbers, and punctuation
- Longer than 6 characters
- Not in any dictionary

A bad passphrase can be:

- Guessed by trying the user’s name, spouse’s name, dog’s name, different phone numbers, the number in the user’s car’s license plate, or any other related information
- Found by looking for a post-it note under the keyboard or even stuck onto the monitor
- Made of letters of the alphabet only
- Shorter than 6 characters
- Found in a dictionary

As you can see, many of the requirements for a proper passphrase are contradictory. The passphrase should be impossible to guess, yet easy to remember; it should be long and made of random characters; and it should not be written down.

To help your users select proper passphrases, you should recommend them a method for doing so. Some easy methods include:

- Use a mnemonic sentence or just take the first, last, or middle letters from each word: I have 2 Salvador Dali paintings on the wall : “Ih2SDpotw”, “Ie2risnel”, or “Iv2altnhl”
- Make “mistakes” when typing a normal word on the keyboard. For example, Hit each letter one step too high and to the left: turbine : “574g8h3”, moon-unit : “j99h;7h85”
- Combine two unlikely words with punctuation, and replace letters with numbers or punctuation that look like them, such as O, 0; I, 1; Z, 2; E, 3; h, 4; S, 5; C, (; S, $; B, &,; etc.: xmas&modem, “xma$&m0d3m”; bad/herring, “&ad/43rr1ng”.

You should change your passphrase periodically to improve security. A change period of 30 to 90 days is recommended.

Frequently Asked Questions

Question	Answer
How can I create a memorable and secure passphrase?	Refer to Create Guidelines for Selecting Passphrases for tips on choosing the best possible passphrases.
Question	**Answer**
What characters can be included in my user name and passphrase?	Your passphrase may contain upper or lower case alphabetic characters and should be at least six characters long. Your user name may only contain the characters which are allowed in a standard file name. In Windows 3.1 it may not contain the following characters: comma (,), colon(:), semicolon (;), equal sign (=), quotation marks(“), slash (/), backslash(\), vertical bar (|), brackets ([ ]), period (.). In addition a user name may not be longer than eight characters or contain spaces. In Windows 95 and Windows NT 4.0 a user name may be up to 255 characters long and contain spaces, but may not include the following characters: / \ : * ? < > |.

Troubleshooting

Installation

Starting Up

Performance

Security

Installation

Problem

I am not able to install the F-Secure Desktop although I carefully follow all the instructions.

Proposed Solution

F-Secure Desktop requires about 2.5 MB of disk space. Make sure that this space is available and repeat installation.

Starting Up

Problem

When setting up the security profile, the system does not accept the username I choose.

Proposed Solution

Make sure that your chosen username contains only allowed characters.

Performance

Problem

F-Secure Desktop is running slow, what can I do to speed it up?

Proposed Solution

Close all the other applications during encryption or decryption.

Security

Problem

When I type in my passphrase I get the “Passphrase incorrect” message.

Proposed Solution

Check whether the CapsLock key is on. Type in the characters in the same case as they are in your passphrase.

Problem

What should I do if I forget my passphrase and cannot decrypt my encrypted files?

Proposed Solution

Your backup key will allow you to decrypt the files, but you will have to set up a new user profile.

Insert the disk with the backup key into the floppy disk drive. Activate the F-Secure Setup Wizard. Choose a new username, and when prompted to select a key, select a:\backup.key. Type in the passphrase associated with the backup key, and then enter your new passphrase. After your new user profile has been set up, you will be able to decrypt your files.

Problem

I have uninstalled my F-Secure Desktop, but overlooked some files which remained encrypted. How can I decrypt those files?

Proposed Solution

When you ran Uninstall F-Secure Desktop, your key file was not deleted, so it remained in the F-Secure Desktop directory.

	Reinstall F-Secure Desktop and when setting up your user profile, select the existing key left after your previous installation. Select the backup key if the key in F-Secure directory was manually deleted or you don’t remember the passphrase associated with it.
Problem	**Proposed Solution**
At Windows logon instead of entering my passphrase I can press Esc and still start my Windows session.	If you press Esc or click Cancel at Windows logon or logout, your will still be able to start or end your Windows session, but your Secret files will not be automatically decrypted or encrypted. To perform any decrypting or encrypting operations, you must use your passphrase.

F-Secure Desktop Message Box

F-Secure Desktop will display an error message to tell you if there is a problem. Notification and error messages are displayed immediately following the operations that caused them.

The first part of a message presents description of the error, for example: The A:\ disk is full. All the possible error messages are listed below.

The second part of a message describes the interrupted operation, for example:

- Problem occurred during initialization.
  (This may happen while the computer is reading current user information from a disk.)
- Problem occurred during encryption.
- Problem occurred during decryption.
- Problem occurred during passphrase validation.
- Problem occurred when changing passphrase.
- Problem occurred during random seed recalculation.
- Problem occurred during user configuration processing.
  (This may happen while the computer is processing USER.CFG file.)
- Problem occurred during file status verification.
  (If a file corrupted, this error may appear while F-Secure Desktop is determining whether the file in question is encrypted or not.)
- Problem occurred during user key creation.
- Problem occurred during unspecified internal action.
- Problem occurred during file deletion.

Warnings

"There is not enough memory to perform this operation."

Close some or all other active applications and repeat the last operation that caused this message to appear.

"Operation was canceled."

The last operation was canceled by user. This is not a error.

"The passphrase you typed is incorrect."

Retype your passphrase; you may have made a typing error.

"The new passphrase you typed is incorrect."

Retype your new passphrase; you may have made a typing error.

"A passphrase must be at least 6 characters."

To ensure safe protection, the passphrase must be at least 6 characters long.

"No user is available. Would you like to create a new user profile?

This message appears every time you are trying to encrypt or decrypt files if the installation of F-Secure Desktop was interrupted before a user profile was created.

"Error while reading user *.cfg file."

Probably something happened to your user .CFG file. Check whether the F-Secure Desktop directory exists and is readable.

"The SAMPLE.DOC file could not be located."

F-Secure Desktop could not locate this file which probably is on an inaccessible disk or does not exist anymore.

"All or part of the ASD:\TEXT?.EXT path is invalid."

Please check your last input.

"The permitted number of open files was exceeded."

If you see this message frequently, increase the FILES setting in your CONFIG.SYS file.

"The SAMPLE.DOC file could not be accessed."

You might have no access to the file in question.

"The A:\ disk is full."

Free up some space on the disk and try again.

"SHARE.EXE was not loaded, or a shared region was locked in the file SAMPLE.DOC."

Probably the file is in use by another application.

"User name cannot contain any of the following characters: *?"<>|.."

The user name serves as a file name for your encryption key, that is why it can only contain characters that may be used in a file name.

"File SAMPLE.FFF is corrupted and cannot be properly decrypted."

Encrypted files should not be modified, otherwise F-Secure Desktop will not be able to perform decryption.

"File integrity error in file SAMPLE.FFF. File cannot be properly decrypted."

Same as the previous message. Encrypted files should not be modified, otherwise F-Secure Desktop will not be able to perform decryption.

"User key file USER.KEY is corrupted."

This might happen, for example, if the file USER.KEY was modified by an application other than F-Secure Desktop.

"Could not decrypt file, decryption key finger print is 1b-2c-34-56-56."

This file was encrypted with F-Secure Desktop, but with a different key, hence you cannot encrypt it with your current key.

Internal Errors

"Internal Error (25). Please contact your F-Secure Desktop distributor."

This may occur if an unexpected error has happened; please send the error code along with the description of the situation to your F-Secure Desktop distributor.

"An unspecified file error (25) in SAMPLE.DOC file. Please contact your F-Secure Desktop distributor."

This may occur if an unexpected file error has happened; please send the error code, a copy of the file that caused the error, and the description of the situation to your F-Secure Desktop distributor.

Contacting F-Secure Technical Support

If you have a question about F-Secure Desktop that the documentation does not address, please feel free to contact your local F-Secure Desktop distributor or Data Fellows directly.

Should you need to call the technical support team, please try to be at your computer to facilitate the call.

Having the following information available will make it easier for your technical support representative to answer your questions:

- Any specific error messages
- F-Secure Desktop version number
- Computer make and model
- Any other information you may think useful in resolving the problem

Data Fellows provides technical support through a variety of electronic services:

Electronic mail:	F-Secure-Desktop-Support@DataFellows.com
World-Wide Web:	http://www.DataFellows.com
	http://www.Europe.DataFellows.com
Anonymous FTP:	ftp.DataFellows.com
	ftp.Europe.DataFellows.com

You can also contact us by mail or phone and ask to speak to our technical support staff:

USA:

Data Fellows Inc.
F-Secure Desktop Sales
4000 Moorpark Avenue, Suite 207
San Jose, CA 95117
USA
tel (408) 244 9090
fax (408) 244 9494

Europe:

Data Fellows Ltd.
F-Secure Desktop Sales
Paivantaite 8
FIN-02210 Espoo
FINLAND
tel +358 9 478 444
fax +358 9 478 445 99

Consult the README file for latest information and instructions.

Disclaimer

All product names referenced herein are trademarks or registered trademarks of their respective companies. Data Fellows Ltd. disclaims proprietary interest in the marks and names of others. Although Data Fellows Ltd. makes every effort to ensure that this information is accurate, Data Fellows Ltd. will not be liable for any errors or omission of facts contained herein. Data Fellows Ltd. reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Data Fellows Ltd.

License Agreement

By exercising your rights to make and use copies of this software you agree to be bound by this agreement. If you do not agree to all of the terms of this agreement, do not copy or use the software.

GRANT. Data Fellows Ltd. grants you a non-exclusive license to use this version of the F-Secure Desktop software (the "Software"). Data Fellows reserves all rights not expressly granted to you. Your license allows you to install and use the software in the number of workstations that you have been invoiced and paid for. The invoice lists the extent of the license. You are also allowed to make a reasonable number of backups of the software. Any user is freely allowed to install the software in his/her home computer, if his use of the software in the office is governed by this license.

MAINTENANCE AND SUPPORT. Separate maintenance and support packages are available. The license itself contains the right for email support for the period of 3 months from purchase.

ENCRYPTION. As the Software contains cryptographic features, you are responsible for ensuring that your use of the Software does not contradict any local legislation or other requirements and rules. In no situation does Data Fellows assume any responsibility for your use of the Software.

DISCLAIMER OF WARRANTY. The software is provided on an "as is" basis, without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose and non-infringement. The entire risk as to the quality and performance of the software is borne by you. Should the software prove defective, you and not data fellows assume the entire cost of any service and repair. This disclaimer of warranty constitutes an essential part of the agreement. Some jurisdictions do not allow exclusions of an implied warranty, so this disclaimer may not apply to you and you may have other legal rights that vary by jurisdiction.

LIMITATIONS. You may not: permit other individuals to use the Software except under the terms listed above; modify, translate, reverse engineer, decompile, disassemble (except to the extent applicable laws specifically allow such restriction), or create derivative works based on the Software; copy the Software other than as specified above; rent, lease, grant a security interest in, or otherwise transfer rights to the Software; or -remove any proprietary notices or labels on the Software.

TITLE. Title, ownership rights, and intellectual property rights in the Software shall remain in Data Fellows, and/or its suppliers. The Software is protected by the copyright laws of the United States and international copyright treaties. This license does not grant you any right to any enhancement or update to the Software.

TERMINATION. The license will terminate automatically if you fail to comply with the limitations described herein. Upon termination of this License, you agree to destroy all copies of the Software.

LIMITATION OF LIABILITY. Under no circumstances and under no legal theory, tort, contract, or otherwise, shall data fellows or its suppliers or resellers be liable to you or any other person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses. In no event will data fellows or its suppliers be liable for any damages, even if data fellows and/or its suppliers shall have been informed of the possibility of such damages, or for any claim by any other party. This limitation of liability shall not apply to liability for death or personal injury to the extent applicable law prohibits such limitation. Furthermore, some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this limitation and exclusion may not apply to you.

HIGH RISK ACTIVITIES. The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Software could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). Data Fellows and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.

MISCELLANEOUS. This Agreement represents the complete agreement concerning this license and may amended only by a writing executed by both parties. This license is personal to you and you agree not to assign your rights in herein, and any attempted assignment by you shall be null and void. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

This Agreement shall be governed by the laws of Finland.