CipherShare

User's Guide

Proven Security Solutions Incorporated

www.provensecuritysolutions.com

Copyright © 2006

Copyright Notice

Table of Contents

1. Introduction

*CipherShare 3.0 is a secure and powerful **business application** that combines the best of advanced encryption technology, collaboration and information management. It offers a broad range of **sophisticated security, collaboration and document management services**, all packaged in an easy to use environment.*

*CipherShare is a true **roaming secure workspace** with real-time synchronization and maximum security. All you need is the CipherShare software and an Internet connection.*
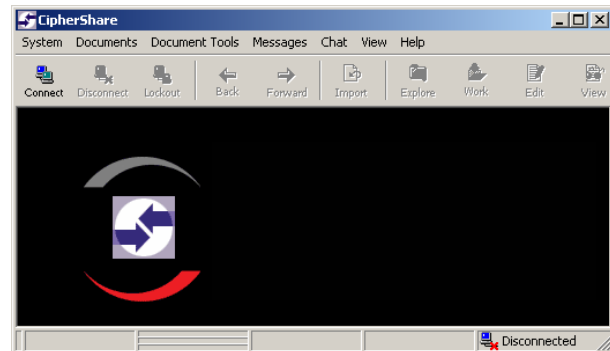
This guide is designed for anyone who intends to use CipherShare. The sequence of topics covered should correspond with the order of how you will use CipherShare, from your first installation to customizing your options.

Once you have installed CipherShare you should start by briefly reviewing **The CipherShare Screen** to familiarize yourself with available CipherShare features.

The section, **Sharing Your CipherShare Documents Securely**, guides you through the required steps to perform the most basic functions of creating a new document within CipherShare or of importing an existing document into CipherShare and sharing it.

Document Controls and Characteristics discusses all the options available when sharing your documents. These properties are customized for each individual document.

Managing Your CipherShare Documents is also a very important section to follow as you begin to receive, edit and manage your CipherShare documents. The remaining sections can be looked at once you begin to expand your usage of CipherShare.

Online Help is also provided within the program.

2. Hardware & Software Requirements

These are the minimum specified requirements.

	CipherShare^{TM} Server	CipherShare^{TM} Client
Operating System	Windows 2000	Windows 98/ME Windows NT 4.0 SP6 Windows 2000 Windows XP Home/Professional
CPU Type & Speed	500MHz Pentium III Processor	350 MHz Pentium III Processor
Hard Drive Space	1.5 MB for the application with additional space required for stored data.	5 MB for application and more for your cached data.
Memory	512 MB RAM	128 MB RAM
Internet Connection	Any speed with TCP/IP connection.	Any speed with TCP/IP connection.

3. Getting started

3.1 Setting up your New Account

Step 1: Obtain Your Account Information

To use CipherShare, you must have already obtained the following from a CipherShare Security Officer:

- **Username**
- **Temporary Password**
- **Office Name**
- **Network Connection Address & Port Number**

If you have not already received this information from a CipherShare Security Officer you will not be able to use the application.

Note: In some cases, CipherShare may be pre-configured with the correct Office Name, Network Connection Address and Port Number. Please check with your system administrator to determine if this is the case.

Step 2: Install CipherShare

CipherShare is distributed as a single installation setup file. Double-clicking this file will result in CipherShare being installed on your PC. Your system administration personnel should provide you with information as to where to find the installation setup file. As an alternative, you can download CipherShare released setup files from ***Proven Security Solutions***.

Step 3: Launch CipherShare

To launch CipherShare:

- Click on the "**Start**" menu
- Select "**Programs**"
- Select "**CipherShare**"
- Click on "**CipherShare Version 3**"

Step 4: Login to CipherShare

The login screen consists of the following:

1. **Profile**: A profile is simply a label that helps to organize your login information. Using profiles makes it much easier to use CipherShare with multiple workgroups (typically referred to as "Offices") since selecting a profile automatically fills in the username and office associated with that profile.

   When you use CipherShare for the first time, only one profile exists: "**My Profile**". You may continue to use that profile name or change it to something more meaningful to you by clicking in the **Profile** field and typing in a new profile name (see the section entitled "**Adding a New Profile**" below).

2. **Username**: Type your username **exactly** as the CipherShare Security Officer provided it to you.

3. **Password**: Type your temporary password **exactly** as the CipherShare Security Officer provided it to you.

4. **Office Name**: Type your office name **exactly** as the CipherShare Security Officer provided it to you.

   NOTE: You may be required to change the network connection and port number using the **Settings** button as shown below. **Do so ONLY if instructed by your system administrator. See Section 10.2 for more details on how to change your connection settings.**
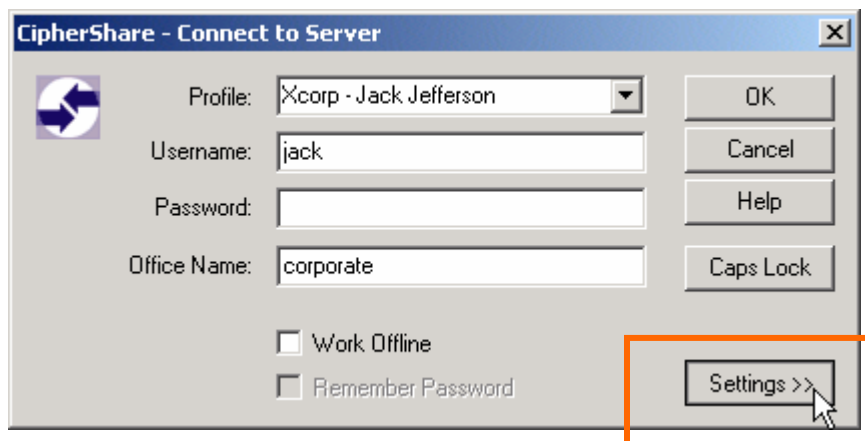
<u>Adding a Profile</u>

Each time you change a Profile, you add that profile to the list of profiles available to you.

To add a new profile:

1) **Click in the Profile** field

2) **Type a new profile name** (e.g. a meaningful descriptive phrase about the connection)

3) **Enter your account information** as described above

Your account information will now be saved under the new profile name.
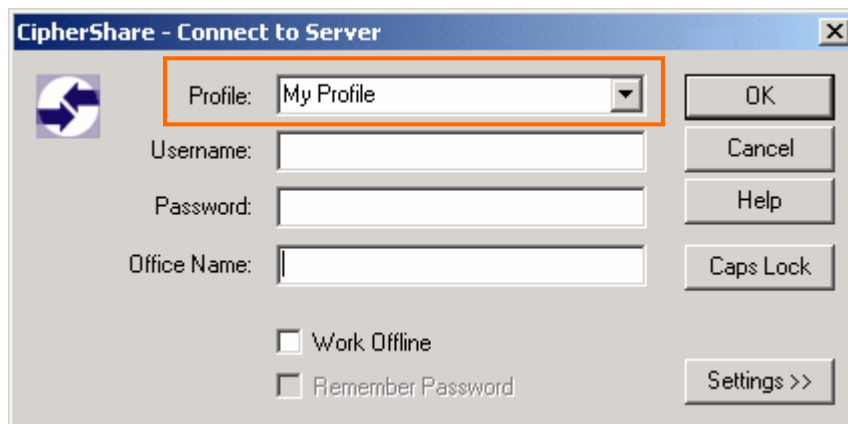
Selecting a Profile: To select a profile, click the down arrow beside the profile box and select a profile from the list of those you have created. Remember that you will always have to enter your password to login to CipherShare (unless you have selected the *Remember Password* option).

Login Successful

If you have entered the correct login information, CipherShare will log you in to the specified office and help you through the process of creating a new account as described in Section 3.2.

Login Unsuccessful

If you have not entered the correct login information, CipherShare will return the following message:

Simply click "**OK**" to return to the main CipherShare Screen, click the "Connect" button and try the login process again. **NOTE**: CipherShare will allow up to 5 unsuccessful attempts before

disabling an account. A CipherShare Security Officer can re-enable the account, but the user will have one chance to enter a valid password or the account will become disabled again.

3.2 Logging in for the First Time – Initializing your CipherShare Account

Once you have successfully logged in to CipherShare for the first time, you will use the "New Account Wizard".

The New Account Wizard will display several screens to help you through this process as shown below.

Step 1:   Click "Next"

Simply click "Next" to begin the account creation process.
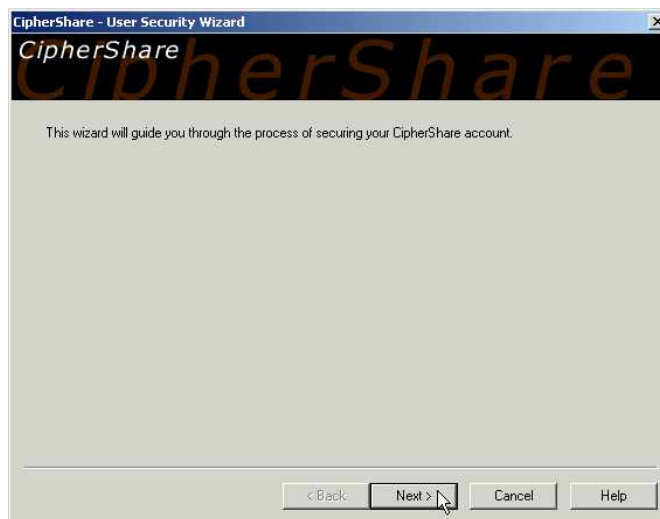
Step 2:   Click "Read Me…" to Read Password Warning

You must click on the **Read Me** button to read the important information on how to make a good password and click *OK before you can proceed with setting your own password.*
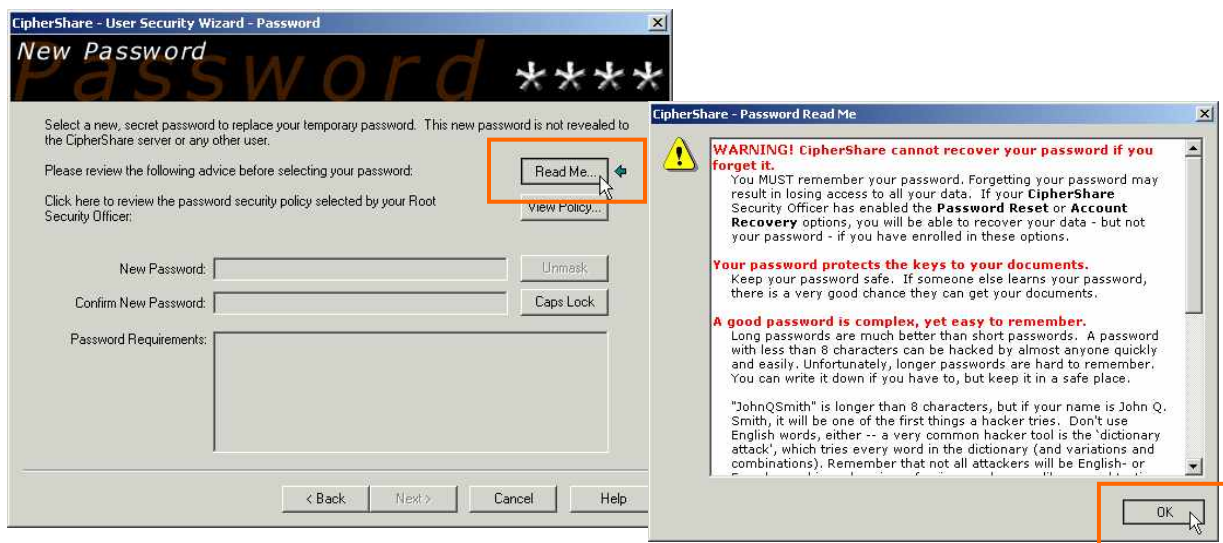
Step 3:   Create Your New Password

You will be prompted to enter your **New Password** and confirm it to replace the temporary password you were given. Once you have successfully entered a password and confirmed it, click **Next** to continue.

Note: You will have to meet the **Password Requirements** as determined by your CipherShare Security Officer. The Password Requirements display will show you interactively what requirements have not yet been met. As requirements are met, they disappear from the display. Click on **View Policy…** to review all security parameters.

This new password will be used to authenticate your identity in the CipherShare office and register your encryption keys. **DO NOT FORGET YOUR PASSWORD!**

View Policy: Allows you to see the CipherShare Security Policy as set by the Root Security Officer.

Unmask: Allows you to see your password in clear text.

NOT RECOMMENDED

Caps Lock: Shows you if Caps Lock is currently on and allows you to turn it on or off.

Password Requirements: Interactive display shows you if you have met the password requirements.

WARNING: *You **MUST** see the above New Password screen in the setup wizard **the first time** you login to CipherShare. If you do not see the New Password screen, or you see the **Warning message below**, someone may have already accessed your account and generated keys at a different workstation. You should contact your CipherShare Security Officer if you see this message the first time you log in. This warning message should be expected when you roam to a different workstation.*

11 of 77
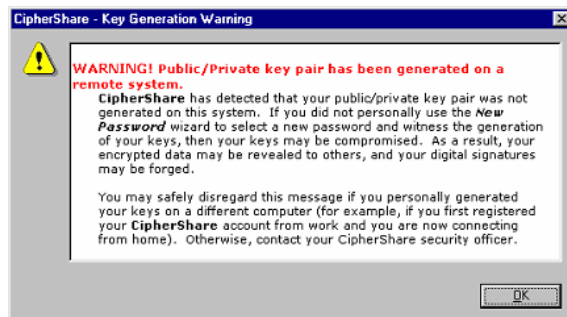
Step 3(a):   Enroll in Password Reset (if enabled by the Security Officer)

CipherShare supports password reset in cases of a forgotten password, but **ONLY** if your CipherShare Security Officer has enabled this feature. **If this feature has NOT been enabled, you will go directly to the next Step.**

If Password Reset has been enabled, you must provide the answers to 5 questions. Your CipherShare Security Officer will have prepared a number of questions that you can choose from; however, it is perfectly acceptable for you to create your own questions. If you forget your password and require it to be reset to a new value, you will be expected to provide the answers to the questions you selected on the Password Reset Coordination screen of a CipherShare Security Officer's session. By having a policy requiring that the questions be answered by you in the physical presence of a CipherShare Security Officer, the potential for a social engineering attack is eliminated.

Password Reset Enrollment

This may occur the first time you login to CipherShare, or after a subsequent login if the feature was not initially enabled by a Security Officer. You may also manually initiate enrollment if you wish to change the questions you use or the answers to some of the questions. When this feature is enabled, you will be asked to follow these steps:

1. You will be notified that the Password Reset feature has been enabled by the following message:
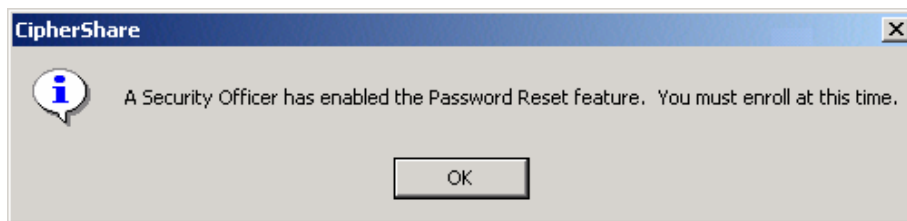
   Click "**OK**" to continue

2. You will then be presented with the "**Password Reset**" dialogue. Click "**Read Me**" to continue.
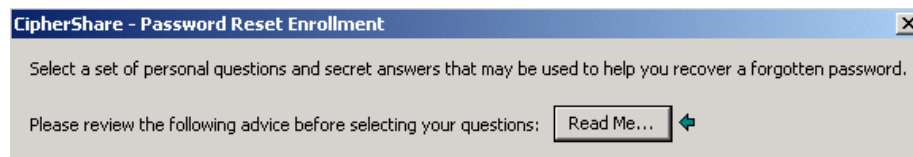
3. You will then be presented with the "**Password Reset Readme**" dialogue. Click "**OK**" to continue.
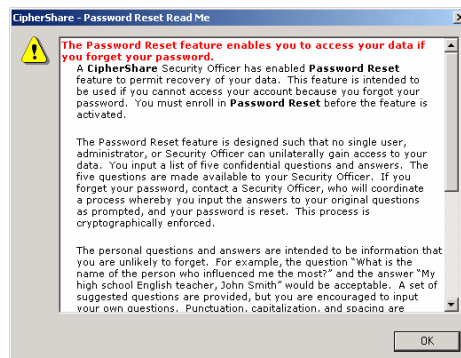
4. You will then be presented with the "**Password Reset**" dialogue with the question and answer fields available for input.

    Questions are presented in the left-hand column, answers on the right.

    You must provide questions and answers for all 5 entries.

    You may either provide your own question by **clicking in one of the question fields** on the left and **typing your customized question**, or you may **click on the drop down arrow** to the right of the question field and **select one of the existing questions** as shown below.

    You must then provide an answer to each question in the corresponding answer area to the right of the question.

    NOTE: For extra security, you may click the "Mask" button to hide your answers.

    Once you have chosen your questions and answers, click "**OK**" to continue. Your questions will be stored for future reference. A hashed digest of your questions and answers is used to secure a recovery copy of your private key material.

    Do NOT forget your answers, <u>exactly</u> as typed. They will be critical to resetting your password should you forget it.

Step 3(b): Enroll in Account Recovery (if enabled by the Security Officer)

CipherShare supports account recovery in cases an individual has permanently left an organization without purging their documents, but **ONLY** if the CipherShare Security Officer has enabled this feature. **If this feature has NOT been enabled, you will go directly to the next Step.**

See Enrolling in Account Recovery in Section 10.7 for details on this procedure.

Step 4: Finish Creating Your Account

To finish creating your account, click **Finish** as shown below.

You may view the security policy for the office by clicking "**View Policy**".

You may also click **Back** to return to the previous screen.

4. The CipherShare Screen

The CipherShare main screen consists of the following:

Main Menu Bar

Icon Toolbar

Document Tree

Document List

Status Window

Status Bar
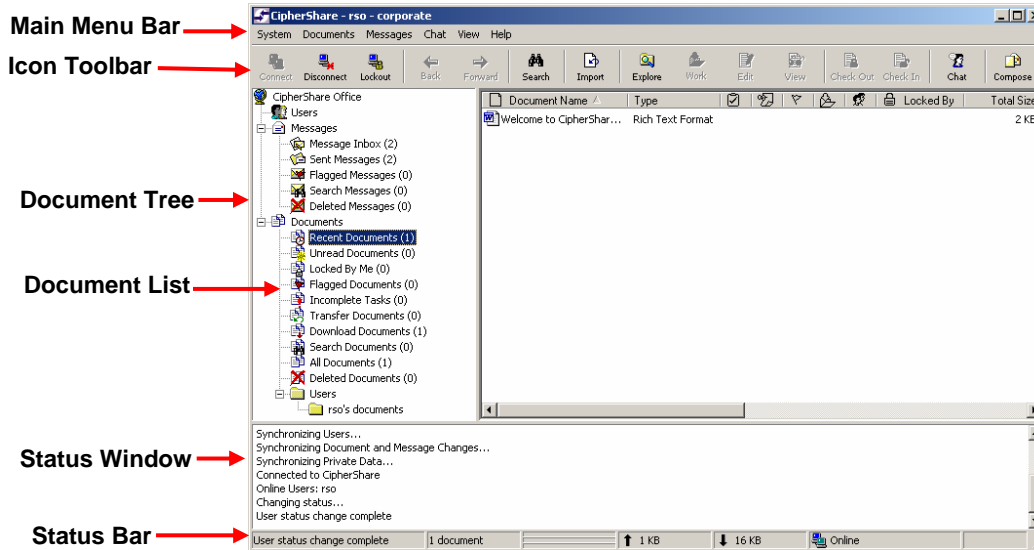
4.1 Main Menu Options

The main menu consists of six main categories with several functions listed under each.

- **System** offers the options to: connect, disconnect, lockout, change your online status, edit your details, change your password, manage key settings, sign a key, enroll in password reset or account recovery, set advanced options and exit the application.

- **Documents** lists different groups of functions dealing with the management of your files. You have the option to: create a new CipherShare document, work with multiple documents, edit a document, view a document, delete a document, import documents edit your document properties, check in/check out a document, view locked document information, detect/clear work files, export a file or directory, create an encrypted self-extracting archive of documents, mark documents as read or synchronize documents.

- **Messages** lists different functions that you can perform on CipherShare messages. You have the option to: view an existing message, compose a new message, reply to or forward a message, or delete a message. All CipherShare messages are encrypted before transmission and are only decrypted by the recipients.

- **Chat** allows you to initiate a new chat session. You must select the users with whom you wish to chat. All CipherShare chat sessions are encrypted.

- **View** provides the option to display the **toolbar**, the **status bar** or the **status window**. You can reorder CipherShare column headings in the Users List, Documents List or Messages List by dragging and dropping.

- **Help** provides the option to display **help information**, display an **error log** and information about CipherShare.

15 of 77

4.2 The Toolbar

The toolbar provides a shortcut method to select specific functions. You may use these once you are familiar with how the CipherShare application works.

Invokes the connection dialogue window to make a connection to the server.

Disconnects from the server.

Lockout immediately disables your CipherShare window.

Go back to a previous selection.

Return to a selection after having used Back.

Allows you to search for documents you have access to.

Import a document into CipherShare from your PC.

Opens a window to allow you to find a file on your PC.

Work makes a file accessible to an application by putting a decrypted copy of the file in the "My CipherShare Files for *username – officename*" folder on your desktop.

Open the selected document for editing. You must have at least Author privilege to edit a document.

Open the selected document for viewing. You cannot save changes to a document opened for viewing, even if you have Author privilege.

Check out the selected document. This marks the document as Locked. A document must be Checked Out before it can be modified. Edit automatically does a Check Out.

Check In the selected document. This creates a new version by determining the difference between this and the previous version in the office. The document is then unlocked.

Initiate a secure Chat session with selected Users.

Compose a secure message to selected Users.

Reply securely to the sender of a selected message.

Reply securely to all recipients of a selected message.

Access online help.

.

4.3 Document Tree

The Document tree is contained in the left section of the main screen. It functions mainly as a filter, providing different options to view and sort your document list.
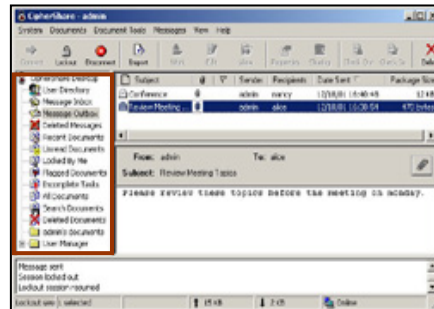
User Directory

Click on **Users** at the top of the document tree to view the user directory.

The User Directory displays a list of all user information including; online/offline status, key trust level and workgroup.

By **selecting and right-clicking on a user**, you can choose to establish a Chat session, compose a CipherShare message, sign a user's key or verify a user's fingerprint.
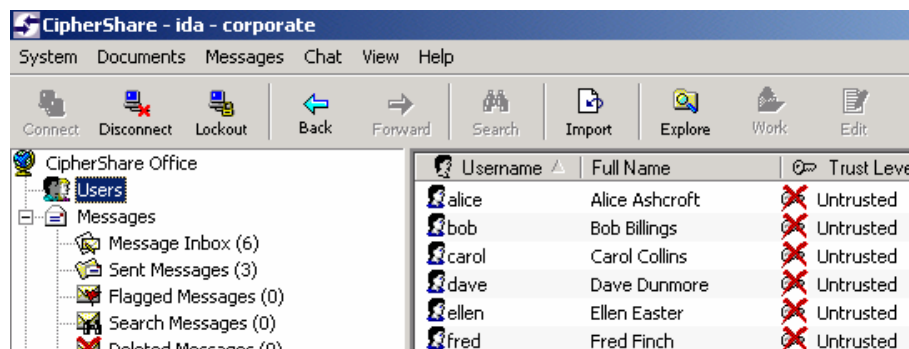
Messages

- *Message Inbox* displays all the messages sent to you.
- *Sent Messages* displays all the messages that you have sent.
- *Flagged Messages* displays messages flagged by you for specific actions.
- *Search Messages* opens up the search window and allows you to search for specific messages by entering search criteria in the fields provided.
- *Deleted Messages* displays all messages marked for deletion.

Documents

- *Recent Documents* **lists the 10 (default) documents most recently accessed by you.**
- ***Unread Documents*** displays all documents that have been recently changed and not been opened by you. These will appear bolded.
- ***Locked By Me*** lists all files that you have locked for editing.
- ***Flagged Documents*** displays all documents flagged by you for specific actions.
- ***Incomplete Tasks*** lists all the files with assigned tasks that are overdue or due.
- ***Transfer Documents*** displays all documents that are currently being uploaded or downloaded.
- ***Download Documents*** displays all documents in the office that are not cached on your PC.
- ***Search Documents*** opens up the search window and allows you to search for specific documents by entering search criteria in the fields provided.
- ***All Documents*** lists all the files that you can access in the CipherShare database.
- ***Deleted Documents*** display all documents marked for deletion. If you are not a Manager of the document, then emptying this type of document from this list removes you from the share list for the document.
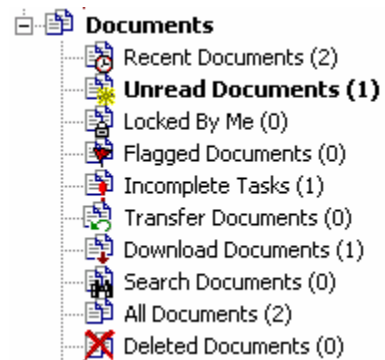
Document Folders

Every user has a private folder under the **Users** folder labeled **< username's > documents**. Chat logs that you choose to save are stored in a subfolder in this folder. Other folders that you create, or are created by others and shared with you, are displayed in this area as well. Double clicking on a folder will expand the tree and display any folders or files grouped under it. You may also collapse these folders.

To ***Create a Folder***, right click on the folder you'd like to create the new folder in and click **New Folder**. You may then enter the name of the new folder.

To Delete a Folder, right click on the folder and select **Delete**. You will be asked if you want to delete a specific file in the folder or all files. ***NOTE***: *When all files are deleted from a folder, the folder is also deleted.*
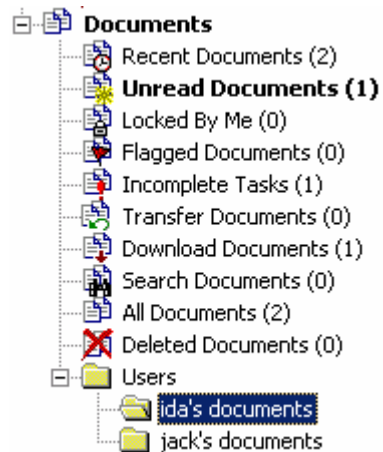
4.4 Column Headings

The center of your CipherShare window displays a listing of your CipherShare files. Information about these files is categorized under the different column headings.

Document Name and *Type* specifies the name of the document and its type.

- *Folder* contains the document's assigned Folder Name.

- *Last Modified* and *Modified By* contain the date and time of the last document modification and who it was modified by.

- *Access Level* contains the access permission you have for the document (Reader, Author or Manager).

- *Status* contains the status information assigned to the document.

- *Locked By* displays a lock icon to indicate that the document is currently locked for editing. When a document is locked, the user who locked it is indicated.

- *Total Size* displays the total number of bytes in the compressed, encrypted file.

- *Download Size* displays the number of bytes that will be downloaded from the office when you download this file. The Download Size decrements during a document download transaction.

- *Upload* displays a progress bar and an indication or percent complete during a document upload transaction.

- *Download* displays a progress bar and an indication of percent complete during a document download transaction.

- *Notes* indicates that there is a note attached to the document.

- *Tasks* indicates that a task is assigned to the document. If the check mark is red, the task assigned is overdue.

- *Flag* will indicate if a document is specifically marked for any reason that you specify.

- *Working File on Disk* indicates that the document has been decrypted into the CipherShare Desktop Work Folder in preparation for viewing/editing using a related document specific application.
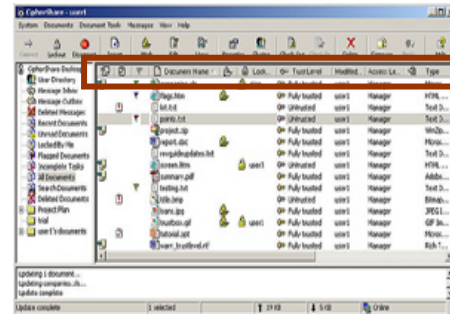
TIP! *These columns can be sorted in **ascending/descending** order by clicking on the **column-heading bar**. Resizing can be done by clicking and dragging the column with the mouse. You can also drag and drop the column headings in the order you would like to arrange them.*

4.5 Message Column Headings

- *Subject* contains the specified message subject.

- *Flag* displays a flag if a message is specifically marked for any reason that you specify.

- *Sender* contains the name of the sender.

- *Recipients* contains the name(s) of the recipient(s).

- *Date Sent* indicates the date and time the message was sent.

- *Total Size* indicates the compressed CipherShare file size.
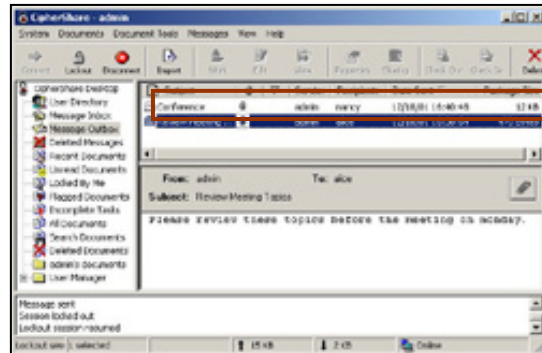
4.6 Status Bar

The status bar is located along the bottom of the CipherShare window. It indicates your current status.
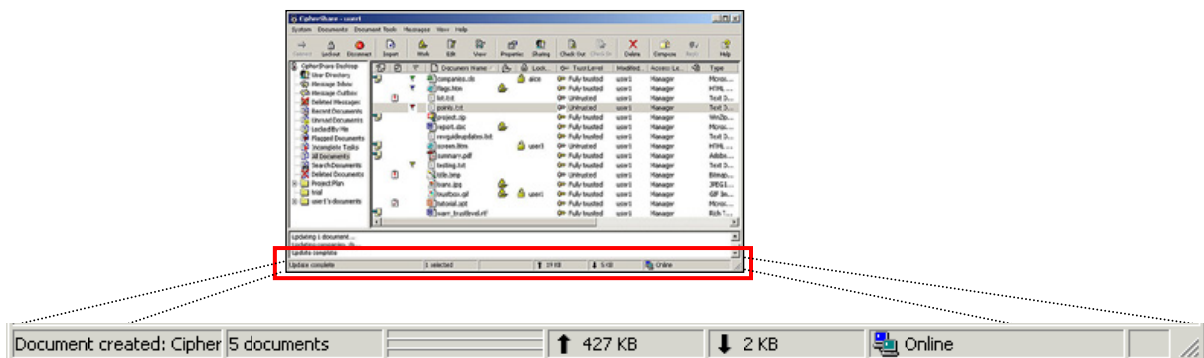
- The first section of the status bar indicates any events that are currently running. A list of these actions can be viewed in the Status Window (*View menu*)

- The second section indicates the total number of documents selected/contained in the current folder (but not its sub-folders).

- The third section indicates **network activity**. The meter will progress repeatedly from left to right until the process is complete.

- The fourth and fifth sections indicate how many **bytes** have been uploaded and downloaded since the beginning of your session.

- The sixth section will indicate whether you are **online/offline**, **disconnected** or in the process of **connecting** to the system. If you are online and selected a specific online status

(refer to System / Change My Status), it will be reflected here. Right clicking on this field also allows you to change your online status.

4.7 Status Window

The status window, if you choose to view it, will appear before the status bar, towards the bottom of the CipherShare window. The Status Window displays a running list of occurring CipherShare events.

The presentation of this window is controlled by selecting Status Window (*View menu*).
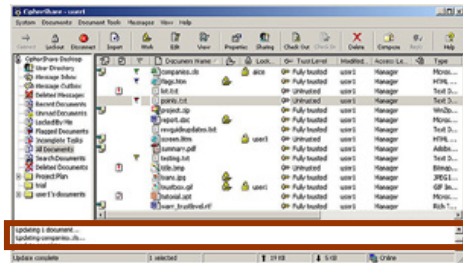
5. Sharing Documents Securely

5.1 Creating a New CipherShare Document

1. To create a new document within CipherShare, choose **New** from the **Documents** menu.
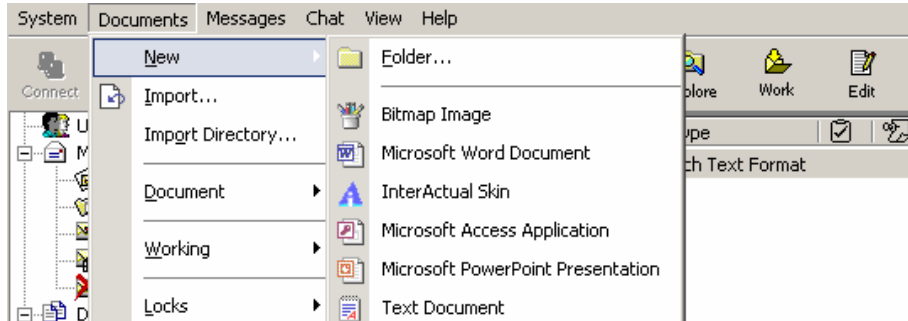
2. Choose which file type you wish to create from the slide-out menu. The file types on this menu are detected as being supported by your computer. If the type you wish to create is not available on the list, click on **Other…** and enter a filename and extension.

3. The **New Document Wizard** will launch. You may **rename** the new document in the prompted field. A **file name and its proper extension** is mandatory.

4. You **must** assign a **Folder Name** to the file. You may assign a **Status** and **Description** to the file as well.

5. Press **Next >** to continue.
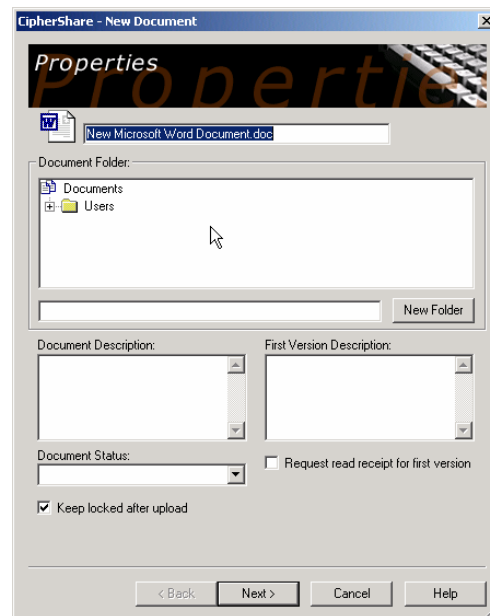
6. Set your **Share List** by clicking on the users you wish to share with or by adding users from a previously defined share group.

7. Click *Finish*.

5.2 Working With Documents

Editing a Document or File

To Edit a document or file, simply double-click on the document or file name. CipherShare will prompt you for which double-click behavior you would like. Click **Edit** to **lock and edit** the file. To preserve this behavior, check the **Use this as my default option check** box and then click **Edit** as follows.
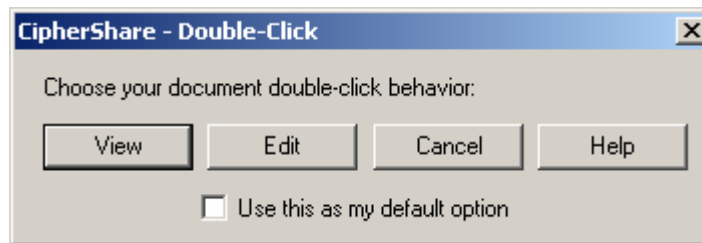
CipherShare will lock your document to prevent others from editing it at the same time and open the document in the associated application (e.g. Word). You may now work with the document as you would normally.

Saving Your Edits and Changes

To save your changes:

1. Use the file **Save** option in the application you are using to save your edited document (e.g. save your edits to a Word document by using **Save**).

2. **Close** your application after you have saved the document. Your file should now appear in the main CipherShare window with a **lock** and a **work icon** as follows:

This indicates that the file is currently locked by you, and editing changes have been made.

3. **Right-click** on the file and choose **Check In** from the menu as follows.
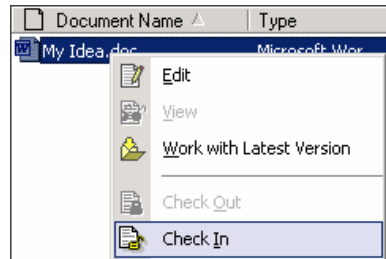
This will upload the difference between the original file and your newly changed file to the **CipherShare Server**. (You may choose to **Undo Checkout** if you do not wish to retain your changes.)

Your file is now saved with its new changes and shared with the chosen users. It should appear unlocked in your document list. Your work icon may remain. Choose **Clear Work Files** (Documents/Working menu) to erase the decrypted working copy of the file.
(Note: Work Files are automatically erased when you disconnect from the CipherShare office.)

5.3 Importing and Sharing Existing Documents and Files

To import a file that already exists on your computer, simply follow these steps:

Step 1: Choose an Import method

a. Choose *Import* (Documents menu). Navigate to the directory that contains the files you want to import, select and open them.
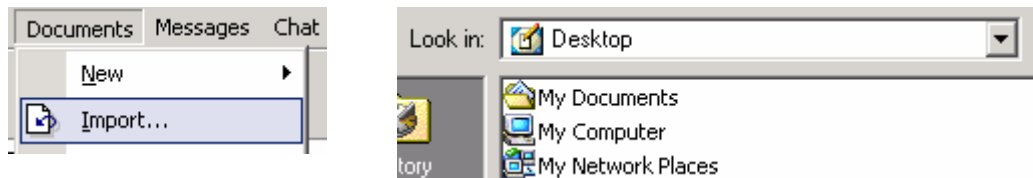
b. Click on the *Import* icon in the tool bar. Navigate to the directory that contains the files you want to import, select and open them.

c. *Drag and Drop* your files from Windows Explorer to the main CipherShare window.

A warning will appear regarding **Importing** and the **Secure Delete** feature. Press **OK**.
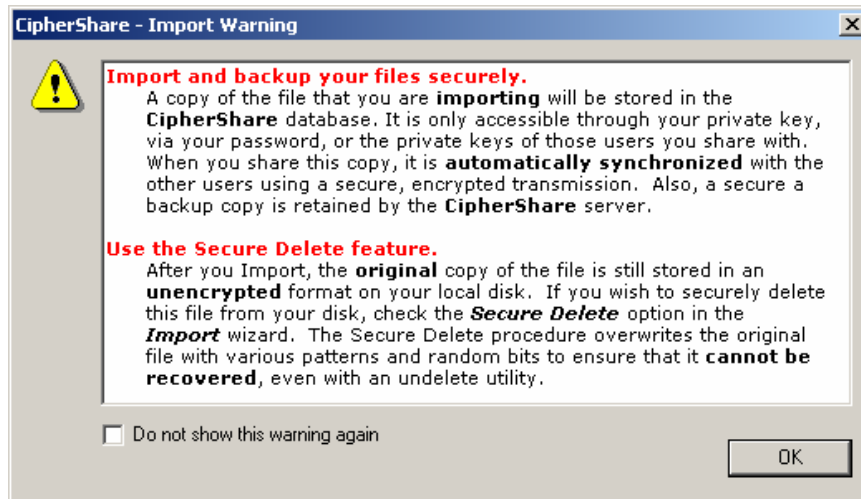
> **TIP!** *Multiple files can be selected by holding down the control key, or you can use the shift key to select a range.*

Step 2: Keep or change the name of your file(s).

When you have selected the files you wish to import, the **Import Wizard** will launch, allowing you to choose the name and folder for the imported file(s).

The name of the file will be the name of the file you are importing. If you wish to change the name of the file, **type a new name in the name field**.
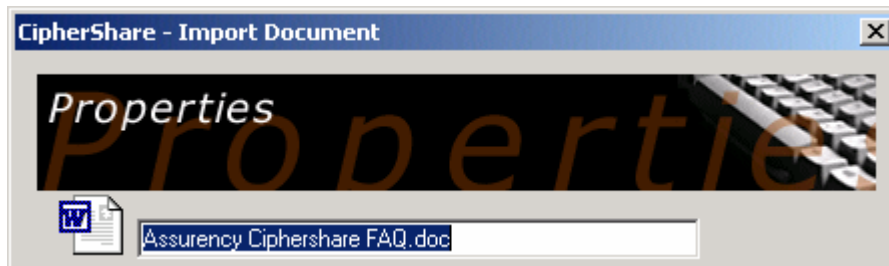
NOTE: If you are importing more than one file, the file name will say *multiple files selected*.

Step 3: Choose a folder for your file(s).

You **must** *assign files to a Folder*. To select a folder into which the imported file will be placed, simply click on the folder.

To create a new folder, click on an existing folder, click **New Folder** and type in a folder name. The new folder will be created as a sub-folder of the folder you have selected.
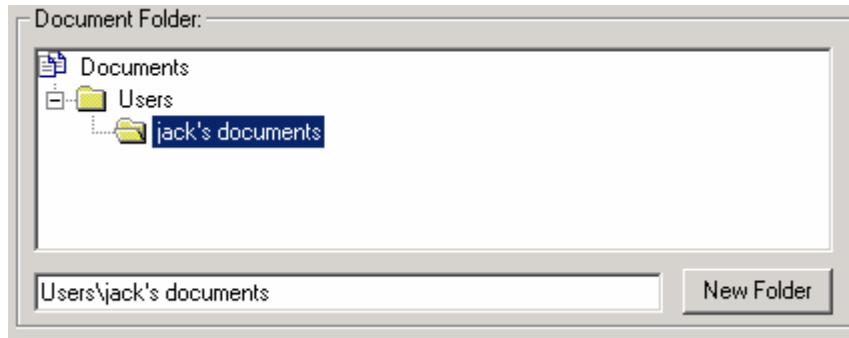
Step 4: Add a document description, first version description, status, and read receipt.

To add a document description, first version description and status, simply click in the desired field and type your description.

If you wish to be notified when someone with whom you have shared the document has actually opened the document, check the **Request read receipt for first version** checkbox.

If you wish to keep the file locked after upload, check the **Keep locked after upload** check box.

If you wish to delete the original file from your computer after import (so that it is only stored in CipherShare), check the **Securely delete original file(s)** check box. Note that if you have selected this option, **the file will only be available through CipherShare**.

To delete every file you import, select the **Securely Delete imported file by default** check box (System / Options / Documents tab).

Press **Next** to continue.

Step 5: Share your document

To share your document with other members of your office, simply **check the name of the person** you wish to share the document with. Sharing is NOT required.
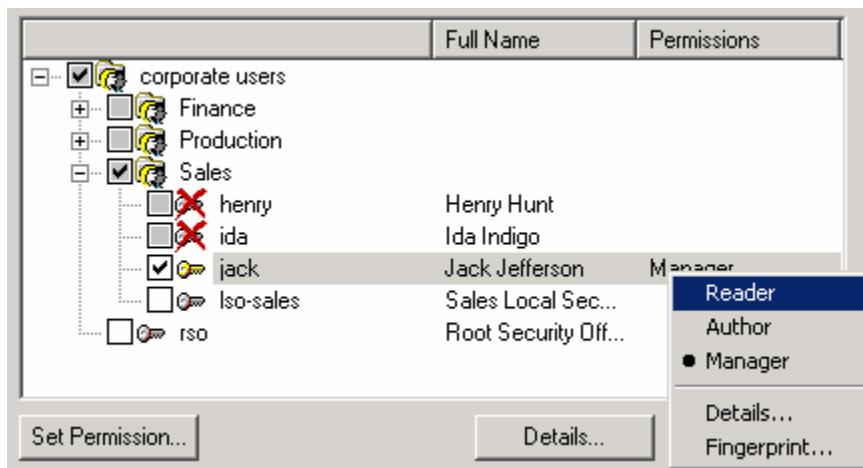
By default, the share permission is "Reader". To change their permission to "Author" or "Manager", **right click on the name** and select the appropriate permission.

The permission levels in CipherShare are as follows:

1) **Reader** – Read only access. Cannot modify or change with whom the document is shared with. Deleting the document only removes the Reader from the share list.
2) **Author** – May read and modify but not change with whom the document is shared. Deleting the document only removes the Author from the share list.
3) **Manager** – All privileges including read, modify, delete, move, change versions.

To confirm the identity of a user, you may view their details and digital fingerprint by **right-clicking on their name** and selecting **Details** or **Fingerprint**.

Click **Finish**. You should see the file you have just imported in your main file list.
The file will also be shared at this point, with the users on the document's Share List.

Untrusted Users

If this window appears, (or a key trust warning appears) it means you are attempting to share a document with **Untrusted Users** (i.e. someone with an unsigned key). This notification will appear every time you share a new document or renew its properties, or send a secure message to an untrusted user.

- In the Untrusted Users List, you can choose to sign the user's key by selecting it and clicking **Sign Key.** *It is recommended that you **verify** the user's key by verifying its **fingerprint** phrase or code before signing the key. (Typically this will be done by a Security Office.)*
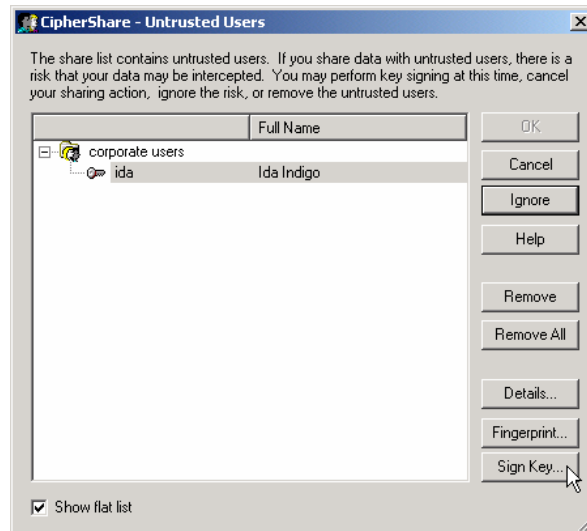
- The user's key information will be displayed. (Refer to the section on **Key Signing**)

You will be asked to confirm signing the user's key. Once you have signed a user's key they will be removed from the untrusted users list and their key will be gold.

If it is desired to continue sharing without an untrusted user you can click on **Ignore.** The document will not be shared with that user**.**

5.4 Import a Directory

Step 1: Choose an Directory Import method

If you would like to import an entire directory, do one of the following:

- Choose **Import Directory** (Documents menu).
- *Drag and drop* your directory into the CipherShare window.

TIP! *You can only import one directory at a time, but it may have multiple subdirectories under it.*
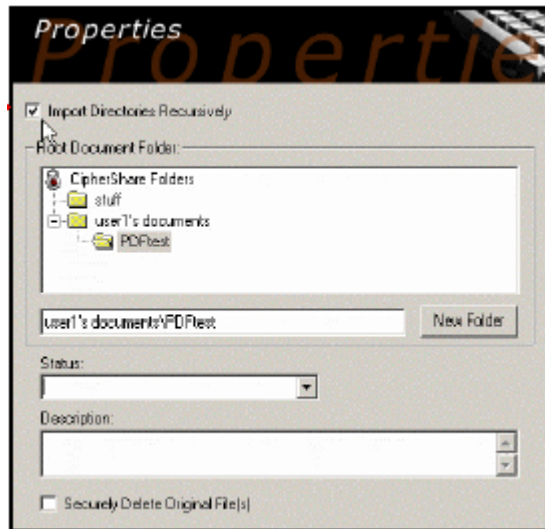
NOTE: All directories and files contained within the directory will be imported, keeping its original structure.

Step 2: Choose a folder

You **must** specify a **folder** for the imported directory under which it will be stored. Select a folder by clicking on it. To create a new folder click **New Folder**.

Step 3: Share your directory (if desired)

Assign a **Share List** and set **Access Permission** as explained previously in **Section 5.1**. Sharing is NOT required.

5.5 Email Notification

This allows you to send a notification regarding a document or message to the public email address of users on your **Share List**.

1. Select **Send Email Notification** from the *Documents / Tools* or *Messages* menu.

2. The dialog box will open, listing everyone on your share list and their email address. If you wish to edit a user's email address, select it and click on **Edit Email Address**.
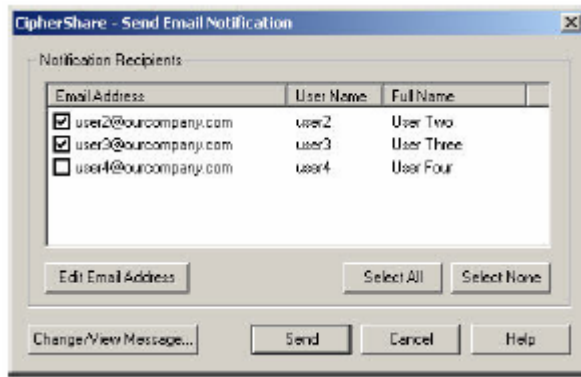
3. Select the users to whom you wish to send the email. You may use **Select All** users or **Select None** to facilitate this activity.

4. If you wish to change the default notification message, select **Change/View Message**. Enter your Email **Subject** and **Body**. When you are finished choose **Send**.

Note: Your email client may generate an alert to advise you that CipherShare is attempting to send an email using the email client.

5.6 Sharing Files With Non-CipherShare Users Through Archives

To share documents securely with others who do not have CipherShare access, you can use a **CipherShare Archive.**

A **CipherShare Archive** is a self-extracting, encrypted file that contains one or more documents. It can be opened and decrypted by anyone who knows the password.

Once an Archive has been created, it can be safely shared through public Internet channels such as email or FTP.

NOTE: The Archive file will remain encrypted and password protected *wherever it resides.*

Saving an Archive to Your Local Disk

1. Highlight the CipherShare file(s) you wish to send as an archive to your local disk.

2. Select **Archive...** from the **Documents / Export** menu.

3. A wizard will launch, prompting you to name the file and specify a saving location.
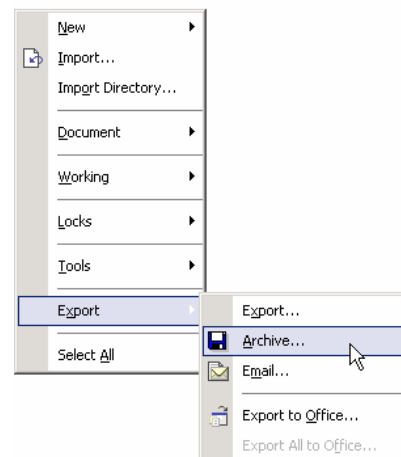
4. Click on **Save**. A CipherShare Archive dialog box will launch, with the selected directory and archive file name at the top. You should also see your document(s) listed. Press **Next**.

5. You must enter and confirm a **Secret Phrase**. You can choose to display this secret phrase for your own purposes by clicking on the **Unmask** button.

6. Press **Next** to send the archive to your local disk. You will see the archive meter move. Once the meter reaches the endpoint, the process is completed. Click on the Close button. You should see the archive in the directory you chose, identified by the CipherShare icon.
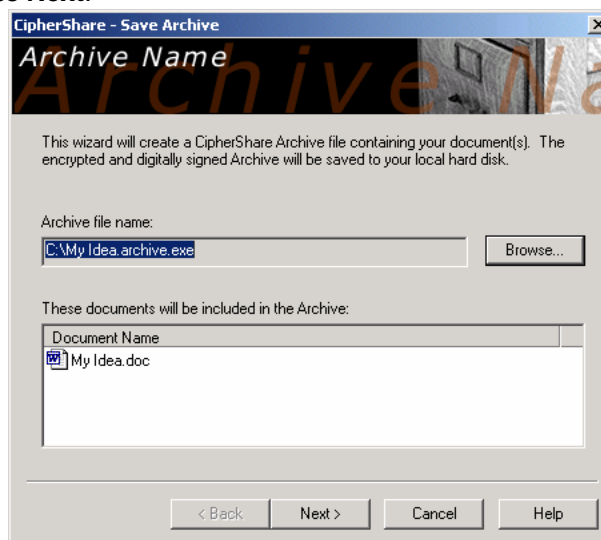
To Open the Archive

1. Double-click on the archive file (.exe). A CipherShare dialog box should appear.

2. Enter the **Secret Phrase** that was created for the archive.

3. Click the **OK** button. The archive information should be displayed, as well as a list of the files contained.

4. Select a file and click on **Extract**. *You can only extract one file at a time.*

5. Select a location where the file is to be saved and press **Save**. Press **Quit** to close the archive window.

To Email the Archive

The archive file is an executable program. Many email virus checkers do not accept emails with executable attachments. Thus, before sending an archive as an email attachment, you should change the filename from xxxxx.archive.exe to xxxxx.archive. This will allow it to pass through email virus filters. The recipient will need to rename the attachment back to xxxxx.archive.exe and then double click it in order to extract the archived files.

6. Document Controls and Characteristics

Controls and characteristics associated with documents can be customized using the functions listed in the bottom section of the Documents menu.

6.1 Document Properties

1. **Select a document**, right-click and choose **Properties...** (or select it from the Documents / Document menu). The Properties Dialog Box will open. You may rename the file in the first field and the Folder Name in the second field. All documents must have a **name** and an assigned **folder**.

   You may only rename files for which you have **Manager** privileges (e.g. those documents you have created or to which you have been granted Manager access).

2. Choose the **Status** type of your file (i.e. Draft, Finalized, Proposed, etc.). The **Description** field is optional.

3. Press **OK** to make your changes.

6.2 Share List

The share list displays those users that have access to a document and their privilege level. Select a document, right-click and choose **Sharing...** (or select it from the **Documents / Document** menu).

Creating a Share List

You may only create or modify the share list of a document for which you have Manager privilege.

1. Navigate by expanding the share tree OR select **Show all users** to view all office members in one alphabetical list.

2. **Check the box** beside the user(s) with whom you wish to share the document. This creates your **Share List**.

   ☑ All members under this group are selected.
   ☑ Some members under this group are selected.
   ☐ No members under this group are selected.
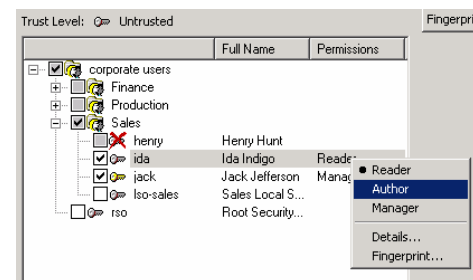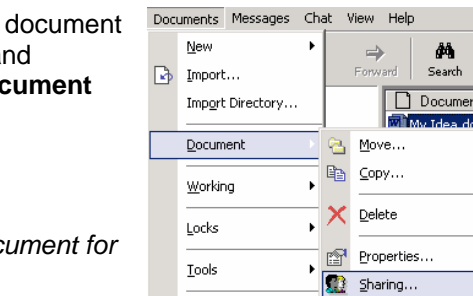
   Alternatively you can select a Share Group from the pull down list and click on **Confirm and Add.** Use the **Confirm Share Group** dialog box to confirm the users of your Share Group. Choose **OK** if this is correct, or edit by unselecting any
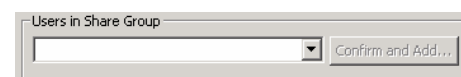
users. Share Groups allow you to quickly share a document with a predetermined group of people with pre-assigned privilege levels.

These users will be selected in addition to those define in your current Share List.

Often you want to apply the same permissions to a new document that are assigned to all the other documents in the folder. To do this use the **Users in Document Folder** to have CipherShare analyze the permissions associated with all the existing documents in the folder and present a suggested sharelist for you to use. Click on **Confirm and Add** in this area to view this list.
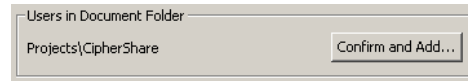
User Types

You may only share a document with **active users** (those with keys).

Gold key: directly trusted user.

Combination key: indirectly trusted user through a Security Officer.

Silver key: untrusted user, i.e. key material has not been verified.

Inactive key: user has not generated keys by making an initial connection to the office.

Access Permission

You may also assign each user an **Access Permission** for the document by right-clicking on their name and selecting **Reader** (default), **Author** or **Manager**.

- **Reader:** has read-only access to the document. (default privilege)
- **Author:** has permission to edit the file, edit notes and tasks but cannot delete the file.
- **Manager:** has all permissions, including permanently deleting a file.

TIP: *If you are sharing with all users in a section, you can assign group permission by selecting the section, right-clicking and choosing an access permission.*

CipherShare will initially assign permissions to a new document in a folder based on the permissions already assigned to all other documents in the folder. This is intended to facilitate permission assignment to a community of interest.

Sharing Multiple Documents – Common Share Lists

Multiple documents can be shared by either:

- Selecting multiple documents, right-clicking and choosing **Sharing…**
- Selecting a folder from the CipherShare document tree, right-clicking and choosing **Sharing…**

Since each document has its own specified share list, the share lists may be combined or overlap when sharing multiple documents. This results in a Common Share List and the interpretation is as follows:

☑   user is on all share lists for all documents

☑   user is on at least one of the share lists for at least one of the documents.

If you click on a user with a grey checked box, it will become a white checked box. This means that the user has common settings on all share lists for all documents.

The **Access Permission Level** for each user on a common share list will reflect the **minimum** permission level granted on any of the share lists.

6.3 Document Versions

Normally, when you work with a document in CipherShare, you are working with the latest version of the document.

Each time a document is modified and saved, however, CipherShare creates a new version of the document that is digitally signed by the user responsible for the modifications. Each version contains those modifications only.

This feature allows you to view the entire version and modification history for a document and determine who is responsible for a specific set of modifications.

To view document versions, **select a document**, **right-click** and choose **Versions...** (or select it from the Documents menu). This will display all versions of the document in a list format.
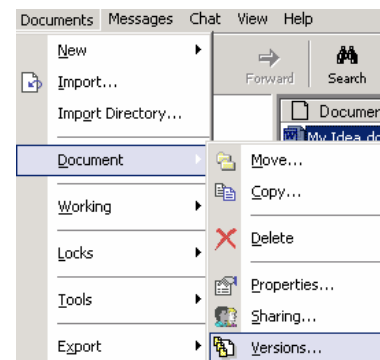
Note that the each version has a number of data elements associated with it including date and time stamp, the name of the version creator, and so on.

ID	Create Time	Creator	Version Size
1	2/13/2004 7:54:59 PM	jack	1 KB
2	2/14/2004 1:20:17 PM	jack	1 KB
3	2/14/2004 1:20:40 PM	jack	464 bytes

To work with a specific version of the document, select a version and choose one of the buttons on the right-hand side of the versions dialogue box. These include:

- **Details:** This will list specific information about the current file such as: date created, last modified, last accessed and file size. Use this control to add a description for a version**.**
- **View:** The selected version launches its native application in **read-only** mode.
- **Export**: Decrypts the selected version and copies it onto your local disk.
- **Archive:** The selected version can be sent as an Archive to your local disk.
- **Compare:** If you select two different versions and click **Compare**, the native application will be launched highlighting the differences between the selected versions.
    NOTE: this feature works for Word documents only.
- **Rollback:** This removes the selected version making the previous one the most current.

TIP   *The last entry on your versions list will be saved as the most recent copy of that document. Only work with different versions of the same document. Do not import any foreign files.*

6.4 Access Audit

Select a document, right-click and choose **Audit...** (or select it from the Documents / Document menu). This displays a log of all user modifications to the document.

Note that each modification is digitally signed by a specific CipherShare user. This ensures that each action taken against a document is accurately recorded, and therefore that the integrity of the document can always be audited and maintained.

Select an entry in the Digital Signatures list and click **Verify** to display information about this specific entry.
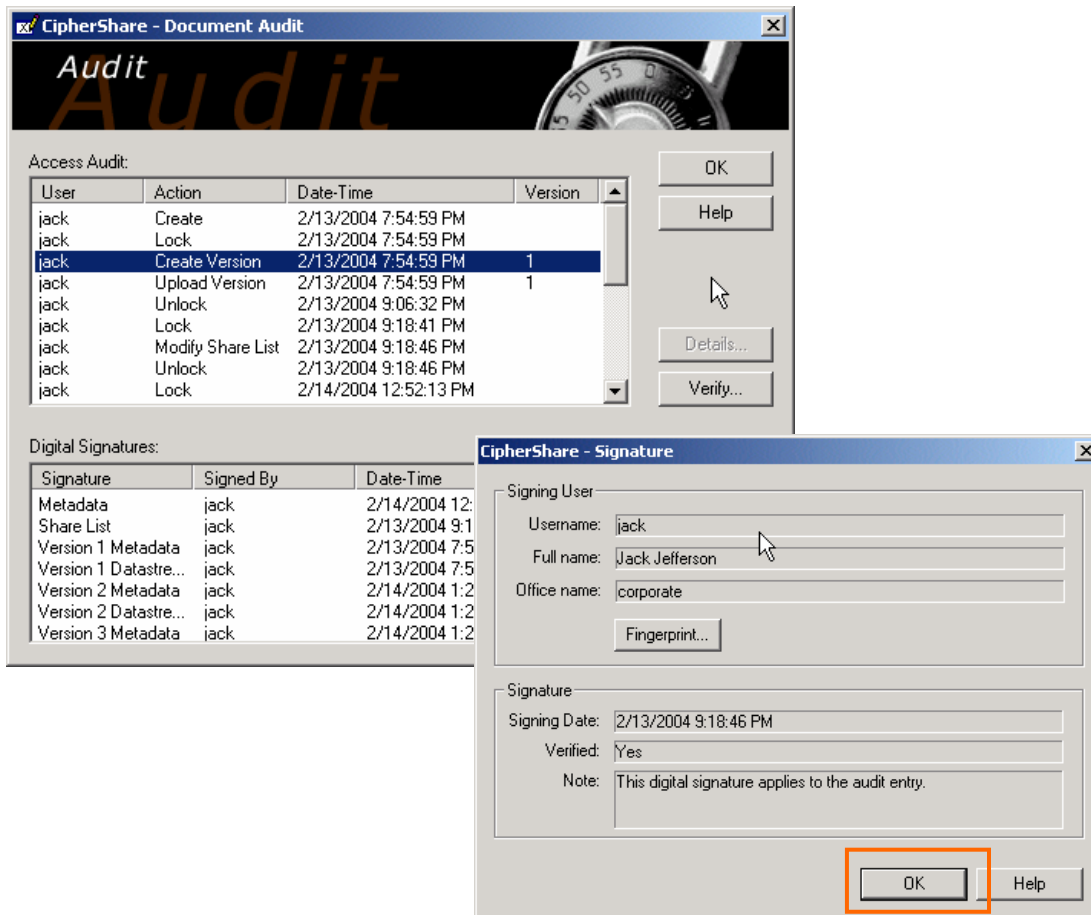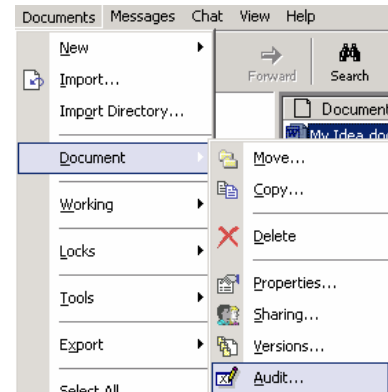
Click on **OK** when you are finished viewing the information.

6.5 Document Notes

Document Notes can be used as a form of electronic "post-it" note attached to a document. This allows users working on a document together to discuss an issue around the document without affecting the document itself.

Creating a Note

To create a note for a document, select a document, right-click and choose **Notes...** (or select it from the Documents / Document menu). This displays the *Document Notes* dialog window.

TIP! *To quickly access a note attached to a document, double click on the document's* ***note icon***.
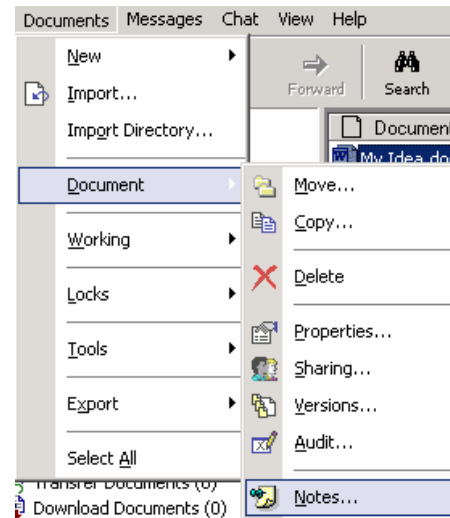
Attaching a Note to the Current Document

1. Click *New* from the menu presented in the Document Notes window. The notes properties dialog box will display.
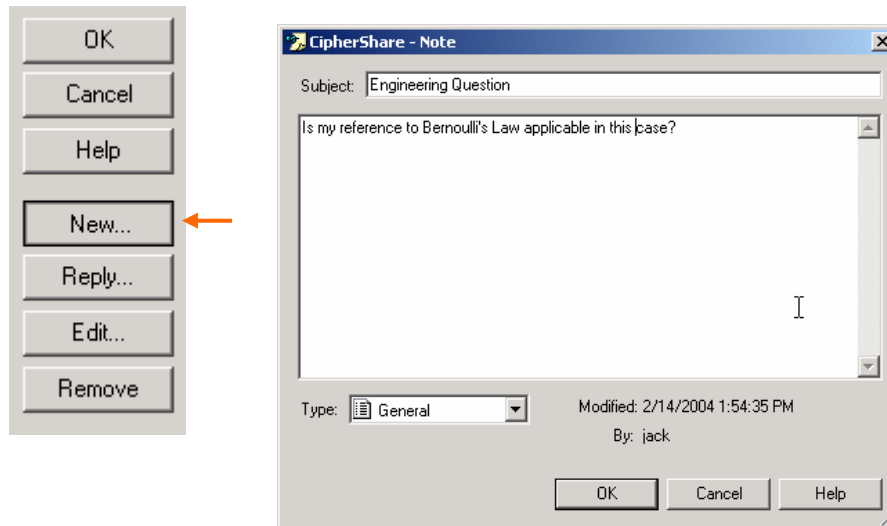
2. Fill in the **Subject** field (mandatory).
3. Enter your **Note** (mandatory). The note will be available to everyone on the share list for the specified document.
4. You may select a **Type** (i.e. general, alert, info, question, or problem).
5. Click the **OK** button to save your changes. You will return to the **Notes main page** and your note information is displayed. Press *OK* to complete the attachment of your note.

A colored indicator will appear beside the list of notes depending on the Type you've chosen (General, Alert, Info, Question, Problem).

Editing Notes:

You can only edit the notes that you have created.

1. Select the note you wish to edit and click on the **Edit** button. This will allow you to edit any of the note fields.

2. Click the **OK** button to save your changes. You will return to the **Notes main page** and your note information is displayed. Press **OK** to complete the updating of your note.

Replying to a Note:

1. Select the note you wish to reply to and click **Reply**.

2. Fill in the **Subject** field (mandatory).

3. Enter your **Notes** (mandatory). The note will be available to everyone on the **share list** for the specified document.

4. You may assign a **Type** (i.e. general, alert, info, question, or problem).

5. Click **OK** to close the reply window. You will return to the **Notes main page** and your reply is displayed. Press **OK** to complete your reply note.

6.6 Document Tasks

Tasks can be used to assign action items to yourself or others in relation to a particular document.
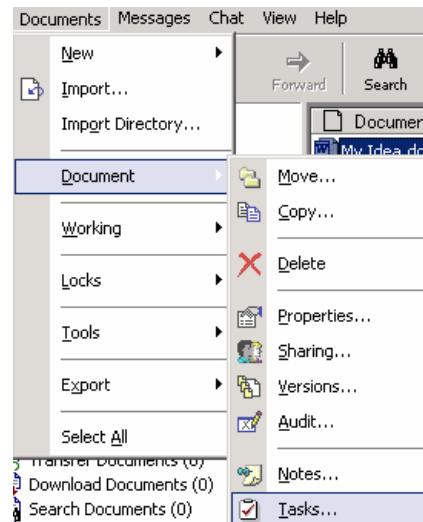
Select a document, right-click and choose **Tasks...** (or select it from the Documents / Document menu).

TIP *To quickly access a task assigned to a document, double click on the document's **task icon**.*

This displays the **Document Tasks** dialog window.

There are three viewing modes available for the list of tasks:

- **All Tasks:** This will list all tasks assigned for the currently selected document. You
may assign a new task by clicking **New**. You
may view details of a selected task by
clicking **View** or by double-clicking on the
selected task entry (read-only).

- **Tasks Assigned by you:** This will list all
tasks assigned by you, for the currently
selected document. You may assign a new
task by clicking **New**. You may edit or view
details of a selected task by clicking **Edit**.
You may delete a task by clicking **Remove**.

- **Tasks Assigned for you:** This will list all
tasks assigned to you, for the currently selected file. You may assign a new task by
clicking **New**. You may view details of a selected task by clicking **View** or by double
clicking on the selected file (read-only).
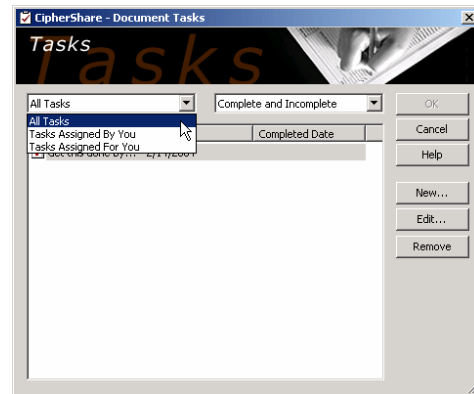
Assigning a Task to the Current Document:

1. Click *New.* The tasks properties dialog box will display.

2. Under the **Details Tab** fill in the Description field (mandatory) and text field (optional).

3. Under the **Recipients Tab** check the box beside the names of those you wish to assign
the task to. The list of names is taken from the current share list.

4. Under the **Time Tab** choose a due date by modifying the date field or by clicking on the
pull down arrow to select a date from a calendar. If you want to further qualify the due
date by time of day, check the box by the time and select the desired time of day.

5. Click the OK button to save your settings. You will return to the Tasks main page and
your task information is displayed. Press *OK* to complete the activation of your task.

NOTE: A red exclamation mark in the document list indicates that a task is overdue.

Indicating Completed Tasks

1. If the task is completed, under the **Time Tab** click the check box next to *Completed*.
This will activate the field.

2. Set the **completion date** by modifying the date field or by clicking on the pull down arrow
to select a date from a calendar. If you want to further qualify the completion date by time
of day, check the box by the time and select the desired time of day.

3. The *Completed by*: field will automatically be filled with your user name.

Click the *OK* button to save your changes. You will return to the Tasks main page and your
task information should be displayed. Press *OK* to complete the activation of your task
changes.

Editing/Deleting Tasks

Only the tasks that you have created can be edited or deleted.

1. Select **Tasks Assigned by You**. This displays all the tasks you have created.

2. To edit or delete a task:

   - Select the task you wish to edit and click on the *Edit* button. This will allow you to edit any of the task fields.
   - Select the task you wish to delete and click on the *Remove* button.

3. Click the *OK* button to save your changes. You will return to the Tasks main page and your task information is displayed. Press *OK* to complete the activation of your task changes.

6.7 Document Flags

Flags can be used to organize the documents that are most important to you. All of your flagged documents are shown in your **Flagged Documents** list.

Select a document, right-click and choose **Flag...** (or select it from the Documents / Document menu).

*To quickly access a flag assigned to a document, double click on the document's **flag icon**.*
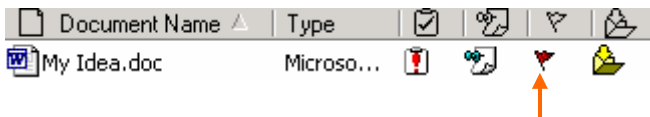
This displays the **Private Document Flag** dialog window.
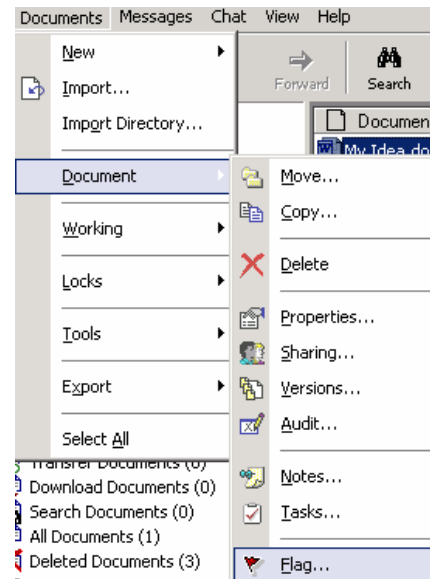
Creating A New Flag

1. Using the Flag pull down arrow, select a flag colour (Red, Blue, White, Green, or Yellow).

2. Optionally add any notes about the Flag to use as a personal reminder.

3. Click **Set Flag** to attach the Flag to your document.

4. Click **Clear Flag** to remove a flag from your document.
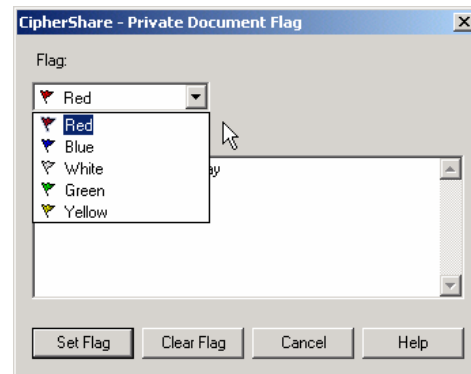
Flags are a personal tool to help your organize your documents. The flags you create are only visible to you. The interpretation of the flag colours is a personal preference.

7. Managing CipherShare Documents

7.1 Accessing Documents

Document Locked Symbol

🔒 **Locked**: When a document is currently being edited, either by you or by another user, it is indicated in the **Locked By** column with a lock icon and the name of the user editing it.

This ensures that only one person can make changes to a document at a time. In order to lock a document or multiple documents at a time, select them, right-click and choose Check Out (or select it from the Documents / Locks menu). In order to edit a document right away, right-click and choose Edit (or select it from the Documents / Working menu). This will lock the document automatically and open it in its native application.

TIP! *To quickly view all the files that are locked by you, click on the **Locked By Me** folder in the **Document Tree**.*
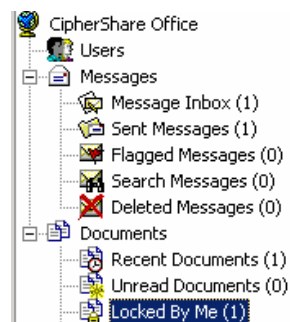
Check In

📄 **Check In**: After you have **edited and saved** your document, you must use **Check In** to save your changes to CipherShare. If you do not check your document in, your changes will not be available to others on the share list.

This will upload the saved document to the CipherShare database, and unlock the document so that it can be viewed or updated by other users. Check In All can be used to upload and unlock all documents that are currently locked by you.
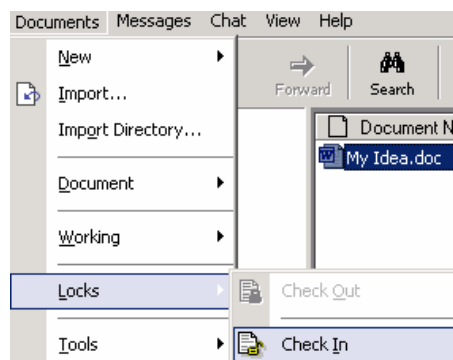
Lock Information: When a document is locked, you can read its Lock Information by choosing **Lock Information** from the Documents / Locks menu. This displays who locked it and the time and date it was locked. After you have finished reading the information, click **OK**.

Work

 Work: Before a CipherShare encrypted
document can be accessed by an application, an
unencrypted working copy must be created. This
normally occurs automatically. However, in some
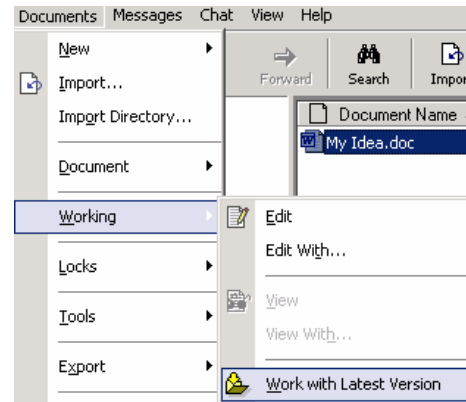cases documents contain links to other documents
(a linked spreadsheet for example).

If you need to access multiple documents
simultaneously you can manually request working
copies before launching the application.

To work with a number of documents, **Select the
documents**, **right-click** and choose **Work with
Latest Version**.

*If you frequently work with linked documents, refer to section 7.5 Auto-Work
to see how CipherShare can automate this process.*

Work files are stored in a folder pointed to by the **My CipherShare
Files** shortcut **on your desktop**. A shortcut is created when you
connect to a CipherShare office. When you disconnect from the
CipherShare office, the work files are securely erased and the
desktop shortcut is removed.

If your computer uses Windows 2000 Professional or Windows XP
Professional, the work area can be protected using Microsoft
Encrypted File System (System / View Security Policy) if enabled by
the Security Officer.
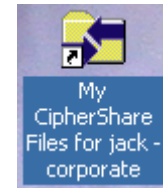
Safe Extentions

Safe Extensions: The safe extensions list controls which file types CipherShare can
automatically launch. This safety feature is designed to force an extra step when sharing a
potentially unsafe file type such as a .bat or .exe file. CipherShare can support any file
type, just add to or remove it from your safe extensions list. You can also disable this
feature. To make changes refer to the System / Options / Extensions tab.

7.2 New and Updated Documents

While connected to a CipherShare office, you will be notified of
new or updated documents by any of the following:

1. A **Notification Bubble** will temporarily slide up near your
    system tray, indicating the user who has created a new
    document or updated an existing document. By single-clicking
    the bubble, you can bring up the CipherShare window and view
    the document. You may turn this off by changing the *balloon
    notifications* selection on the System / Options / Documents
    tab.
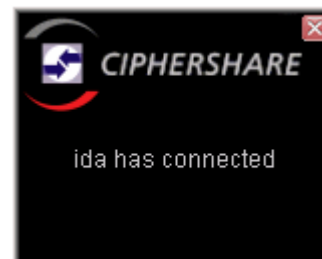
2. A new or updated document automatically appears in the **Unread Documents** folder in the CipherShare documents tree.

3. A new or updated document's name appears **Bolded** within its permanent folder in the document list. Once you have opened the document, it will become **unbolded**. To mark a document as read without opening it, choose **Mark as Read** or **Mark All as Read** (Documents / Document menu).
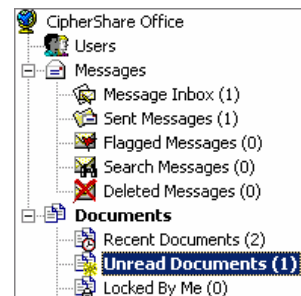
4. A **Sound** will play each time CipherShare detects that a new or updated document has been shared with you. You may turn this off or apply your own sound indicator by going to the **System / Options / Local tab**.

Content Out-of-Sync: If this icon appears along with a size value in the Download Size column of a document, it means that the full document has not been downloaded yet or it may still be in the process of downloading if it is a large file. You can choose to download a document to completion by choosing **Download** (Documents / Working menu).

TIP! *You may add notes, tasks, or a flag or send email notification with an incomplete (out-of-sync) document, but a full document is required to view, edit or move a version.*

7.3 Viewing Documents

The View command allows you to look at a document in **Read Only** mode. You will **not be allowed to make any changes** to the document. (Use the Edit command if you with to make changes – see section below.)

1. Select the document you wish to view.

2. Right-click on the document and choose **View** (or select it from the Documents / Work menu). This will create an unencrypted working copy of the document and launch the document's default application for viewing.
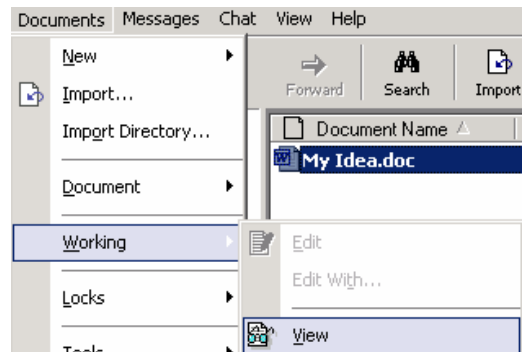
View with: You may specify a different application to use for viewing a document by choosing **View With...** under the Documents / Work menu.

7.4 Editing Documents

This **allows you to make changes** to a document provided that you have at least **Author** permissions for the selected document.
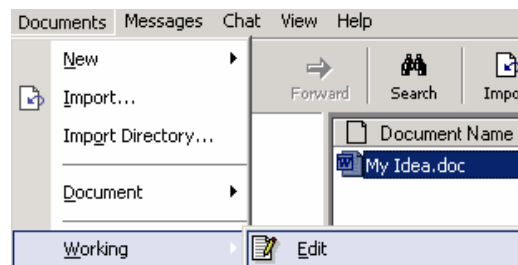
You will **not be allowed to make any changes** to a document for which you only have **Reader** permissions.

1. Select the document you wish to edit. (You can only edit a document if it is **not currently locked** by another user.)

2. **Right-click** on the document and choose **Edit** (or select it from the Documents / Work menu). You will receive a warning about how to properly save a CipherShare document.

    Once you have read the warning and clicked **OK.** A lock will also appear beside the document indicating that it is locked by you for editing purposes.

    Saving your Editing Changes

    Remember that in order to save your changes to an edited document, you must follow this two step process:

1. **Save** the document in the Windows application you are using to edit it

2. **Check In** the document into CipherShare

    NOTE: *You may specify the application you wish to edit the document with by choosing* **Edit With...** *under the Documents / Work menu.*

7.5 Auto-Work

CipherShare allows you to work with individual documents, but there are cases in which individual documents are linked or associated with other documents in CipherShare. An example of this would be several Excel spreadsheets that are linked together.

To work with linked documents, you must ensure that the latest version of all linked documents have been decrypted in your desktop work folder. CipherShare allows you to download and decrypt the entire content for a specific folder (and sub-folders as well) automatically, rather than manually doing each document separately. Keep in mind, however, that this process may take some time if there are lots of files within the folder.

The auto-work feature can be turned off or customized in the **Working with Documents** section on the Documents tab of the System / Options menu.
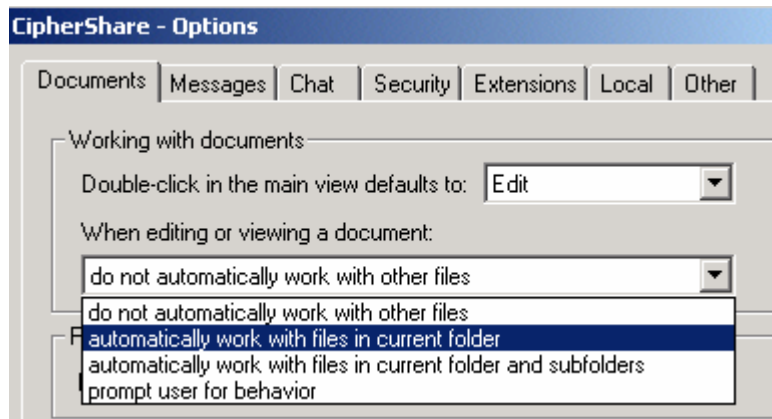
Manually Selecting Linked (Work) Files

You can manually choose to link **Work** documents by selecting the documents and pressing the **Work** icon on the toolbar or selecting **Work** from the **Documents / Work** menu.

A Work icon will appear beside all the documents in the same directory, meaning that they all have been downloade and decrypted into the work folder.

You can remove the decrypted version of a document in the work folder by selecting the document) and choosing **Clear (All) Work Files** (Documents / Work menu).

7.6 My CipherShare Files

Each time you make a CipherShare connection, a folder shortcut entitled **My CipherShare Files** (specifying the user and office name) will appear on your desktop.

This folder contains all CipherShare documents that you have chosen to "work" with and allows you to quickly access and edit your work documents.
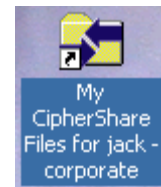
You may also **import new documents** into CipherShare by dragging and dropping them into the **My CipherShare Files** folder.

New documents will not be uploaded to the CipherShare database until you select **Detect New Work Files** (Documents / Work menu).

New work files will also be detected before you disconnect your CipherShare session.

7.7 Saving Documents

1. The recommended method for saving a CipherShare document properly is by choosing **Save** when saving the document in its native application (Refer to the <u>Save As</u> Section below). Make sure to **Close** the native application afterwards.
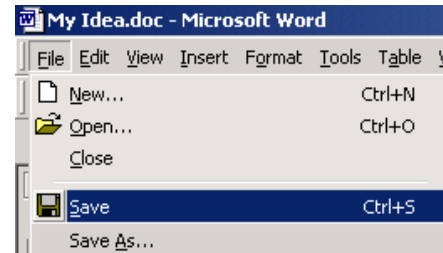
2. Your document should appear **Locked** in the main CipherShare window. You must **right-click** on the file and choose **Check In** (or select it from the **Documents / Locks** menu).

    This will upload your changed document to the **CipherShare Server Database**, unlock it and make it available to those on the Share List.

    The document should no longer appear locked in your document list.
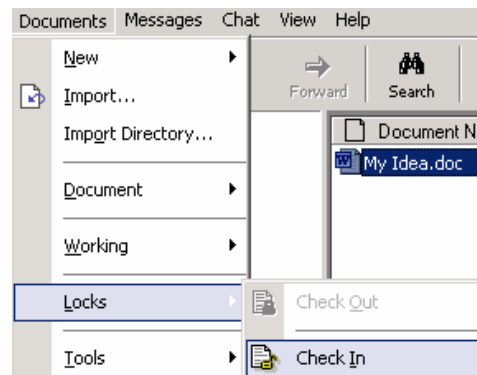
    If you would like to make the current version of a document available to other users during your editing process, you can choose to *keep the document locked* at the time you check it in.

    When a file is locked, you can read its Lock Information by choosing **Lock Information** from the *Documents / Locks* menu. This will display who locked it and the time and date it was locked. After you have finished reading the information, click on **OK.**

7.8 Save As

If you need to use **Save As** to save a document under a different name, you may use it but your new file will not appear in the document list until you choose to **Import** it. By default, documents created using **Save As** are stored in the same work folder as the original document.

Choose **Detect New Work Files** (Documents / Work menu) to see a list of such newly created documents and select those that you need to **Import**. You must import them in order to properly save and upload them to the CipherShare Server database.

When you exit CipherShare, it will detect any new Work Files that you have not imported. Choose **Import** to properly save and upload them to the CipherShare Server database.

You should not use **Save As** to save a document to an area of your computer that is outside the work folder area. Doing so would leave the document in an insecure area of your PC.

7.9 Deleting Documents

You may only delete a document permanently from CipherShare if you have **Manager** privilege for the document.

If you delete a document for which you have **Reader** or **Author** privilege, it is equivalent to requesting that you be removed from the share list for that document. The original document will NOT be deleted. You will simply no longer have access to it.
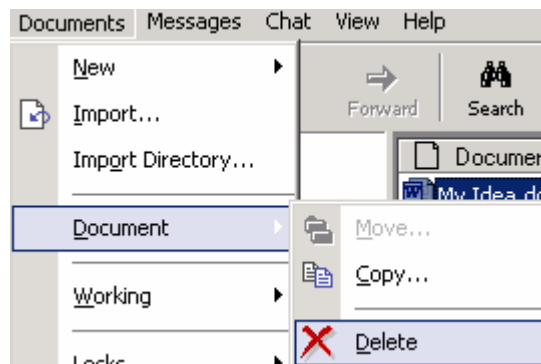
1. Select the document you wish to delete.

2. Right click and choose **Delete** (or select it from the Documents / Document menu).

3. You will be asked to confirm the deletion. Click on **Yes**. The document will be moved to the **Deleted Documents** folder.
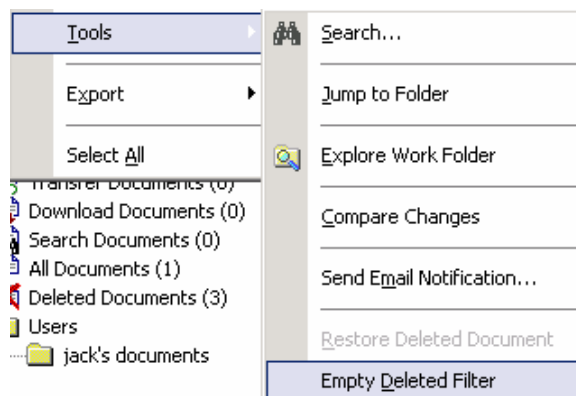
This works similar to a *"Trash Can"*, where documents are retrievable by clicking on **Restore Deleted Item** (Documents / Tools menu) or they can be permanently deleted by clicking on **Empty Deleted Folder** (Documents / Tools menu).

*Note: If you have Manager Privilege for a deleted document, **Empty Deleted Folder** will delete it from your CipherShare database and from those with whom you have shared the document.*

7.10   Exporting Documents

Exporting a document allows you to save a CipherShare document in a local directory on your PC. The document is decrypted and a copy is then stored on your local drive. *This document copy is no longer secure.*

1. Select the document(s) you wish to export.

2. Choose **Export...** from the *Documents / Export* menu. You will be issued a security warning.

3. A **Save As** dialog box will appear. Navigate to where you would like to save the file and click on **Save**. The unencrypted file appears
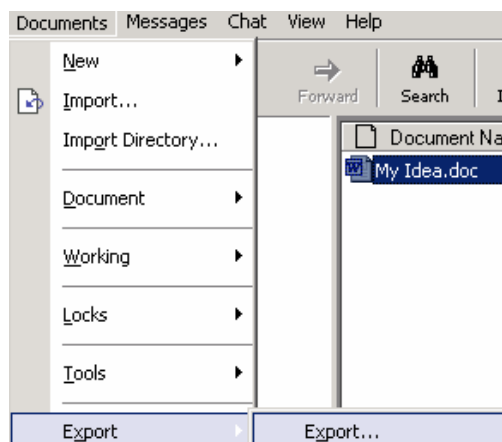
in the specified local computer directory.

8. Secure Messaging

8.1 Composing a New Message

Secure Messaging works like email but is sent in **Real Time**. All messages are encrypted and digitally signed, just like your CipherShare documents.

1. To compose a message you can do either of the following:
   - Click on the **Compose** icon on the toolbar.
   - Choose **New** under the Message menu.

2. Enter the username of each **User** to whom you wish to send a message (must be within the **same office**). By clicking on the **To:** button you can select users from the office list.
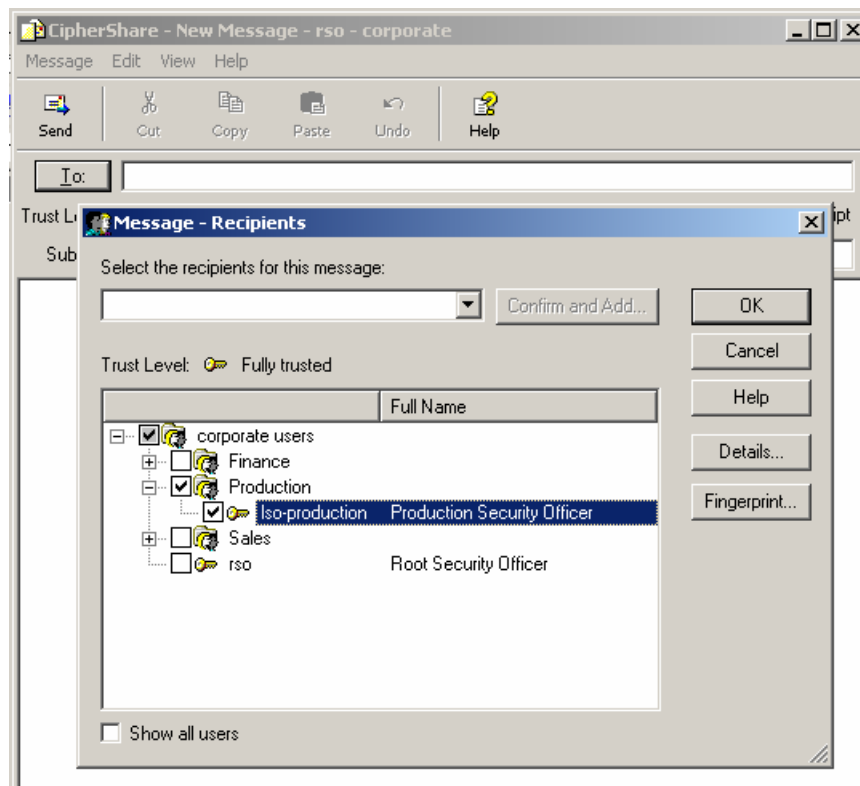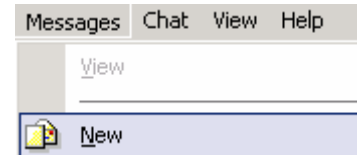

3. A **Subject** is mandatory

4. After completing your message, click on the **Send** button.

8.2 Receiving a Message

While running the CipherShare application, you will be
notified of new incoming messages by any of the following:

- **Message Inbox** on the CipherShare tree will be
  bolded. You must click on **Message Inbox** to display
  your message list.

- Bolded message(s) will appear in your message list.
  Click on the message(s) to display the text in the
  message window. The message line will be unbolded
  once you have read the message.
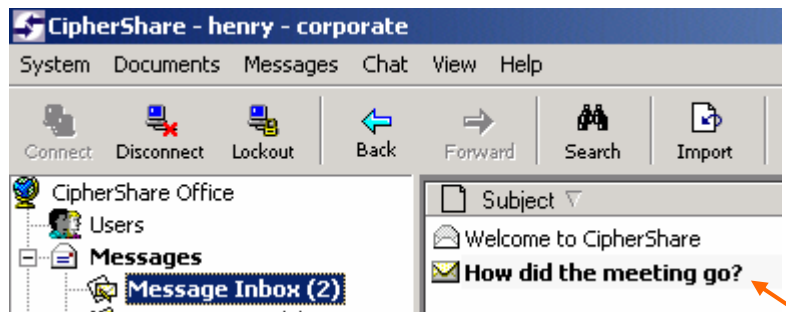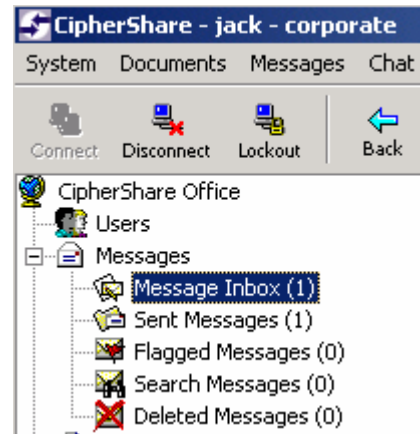
- **New Message Sound** will play every time CipherShare
  detects that you've received a new message. You may
  turn this off or apply your own sound indicator by going to
  the Sound area on the System / Options / Local tab.

- A **Notification Bubble** will temporarily slide up
  near the system tray, indicating the user who has
  sent you a message. By single-clicking the bubble,
  you can bring up the CipherShare window and
  access your Message Inbox. You may turn this off
  by going to the *Systray notification balloons for new
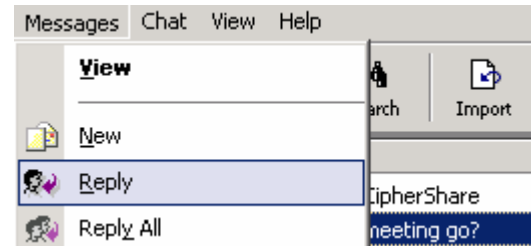 messages* area on the System / Options /
  Messages tab.

Select the new message in *Message Inbox* to view it.

8.3 Replying to a Message

To reply to a message:

1. Select the message to which you wish to reply, right-click and choose **Reply**, or select **Reply** from the Messages menu or choose **Reply** from the icon toolbar.

   The **Reply To:** Message box will open.

2. The name of the originating **User** will appear in the To list. You can type in additional users or click on the **To:** button to select them from the office list.
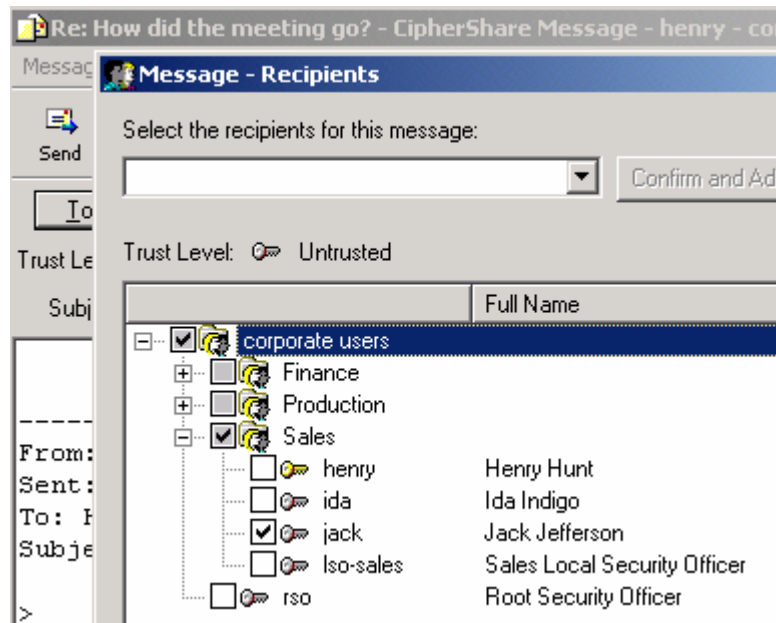

3. The original subject is pre-pended with **Re:**.

4. After entering your response, click on the **Send** button.

8.4 Forwarding a Message

To forward a message:

1. Select the message you wish to forward, right-click and choose **Forward** or select **Forward** from the Messages menu. The **Fwd:** Message box will open.

2. Enter the username of each **User** to whom you wish to forward the message (must be within the **same office**). By clicking on the **To:** button you can select users from the office list.

3. The original subject is pre-pended with **Fwd:**.

4. After entering your comments about the forwarded message, click on the **Send** button.
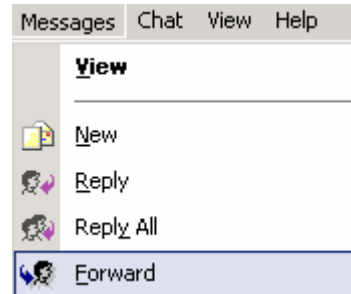
8.5 Deleting a Message

1. Select the message you wish to delete. Right-click and choose **Delete** (or select it from the Messages menu).

2. You will be asked to confirm the deletion. Click on **Yes**. The document will be moved to the **Deleted Messages** folder.

This works in a manner similar to a *"Trash Can"*.

Deleted messages are retrievable by clicking on **Restore Deleted Item** (Messages menu) or they can be permanently deleted by clicking on **Empty Deleted Folder** (Messages menu).
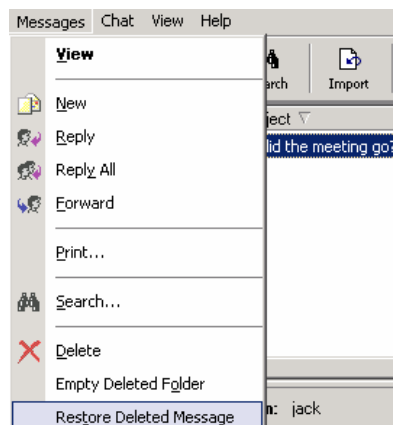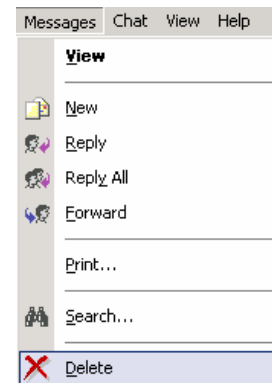
Note: *Unlike other messaging systems, if you delete a message from your **Sent Messages** folder and empty it from the **Deleted Messages** folder, then it will be removed from all recipients' **Message Inbox** folder.*

8.6 Other Message Controls

Mark as read: Messages will become unbolded to appear as if you have read them.

Flags: You may mark any selected message with a coloured flag and specify your own comment for it. *This feature is only visible by you.* Right-click on the message and choose Flag (or select it from the Messages menu).

Adding a Flag

- Choose a colored flag from the pull-down list.
- Enter a note or reminder for yourself.
- Choose Set Flag when you are finished. You should see a colored flag indicator beside the message.

Removing a Flag

- Choose the message you wish to remove the flag from.
- Right-click on it and choose Flag.
- Choose Clear Flag to delete it.

Send Email Notification: This allows you to send an external email notification regarding a CipherShare message.

Archive: This command takes all selected messages and bundles them together into a single file in .rtf format. The archive is then stored under the *<user's name> documents* folder.
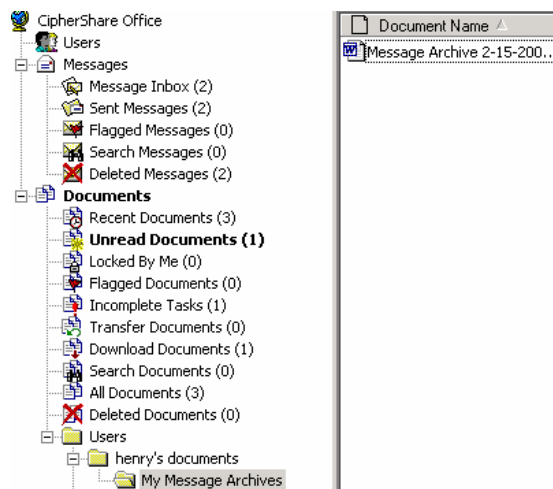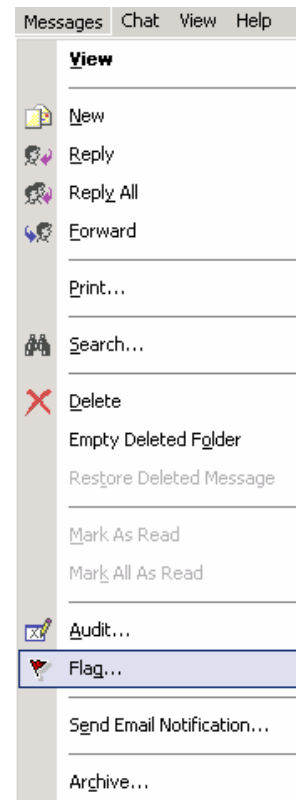
9. Searching for Documents

The **Search Documents** command is located in the **Document tree**, and on the **Toolbar**.

When you select this folder the document search window appears along the top of the CipherShare window.

You can search for specific documents by entering search criteria in the fields provided. The *Advanced* button provides additional search criteria including:

- **User**: You may search for documents based on: Shared with, Is Reader, Is Author, Is Manager, Creator, Last Modifier and Locked by.

- **Status:** The contents of the document Status

- **Date:** The date the document was Created or Last Modified.

- **Size:** Documents whose size of At Least or At Most a specified amount.
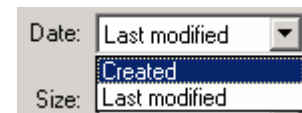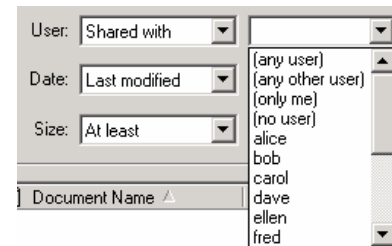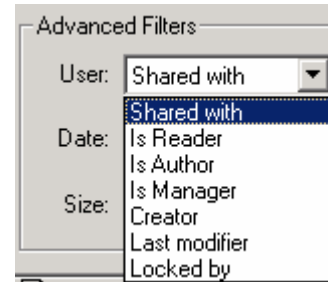
Click on the *Search* button to execute the search. Your search results will be displayed in the search results window.

Click on the *Reset* button to clear the search fields and begin a new search.

To *Exit* the search and return menu and return to the main document list, click on any other folder in the Document Tree.
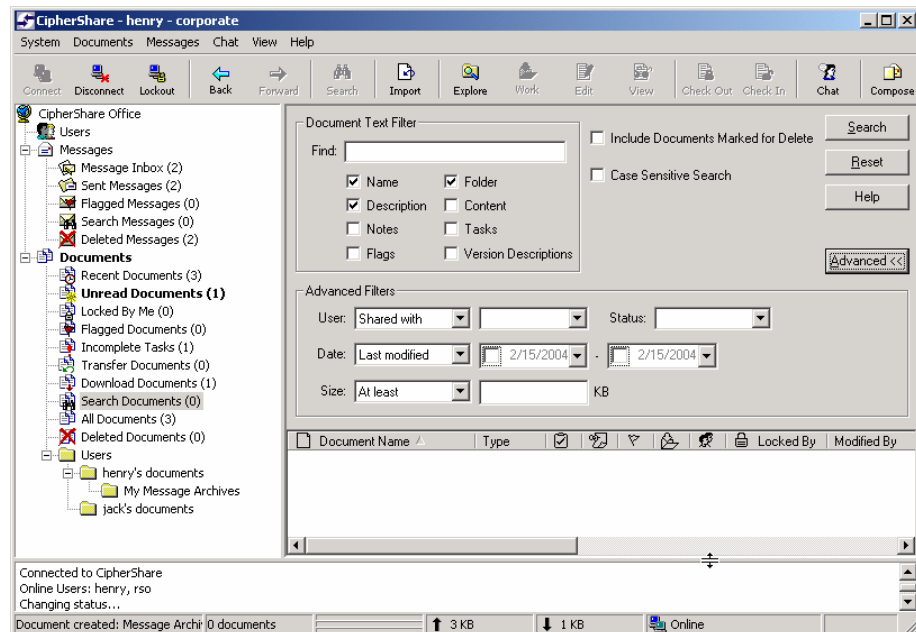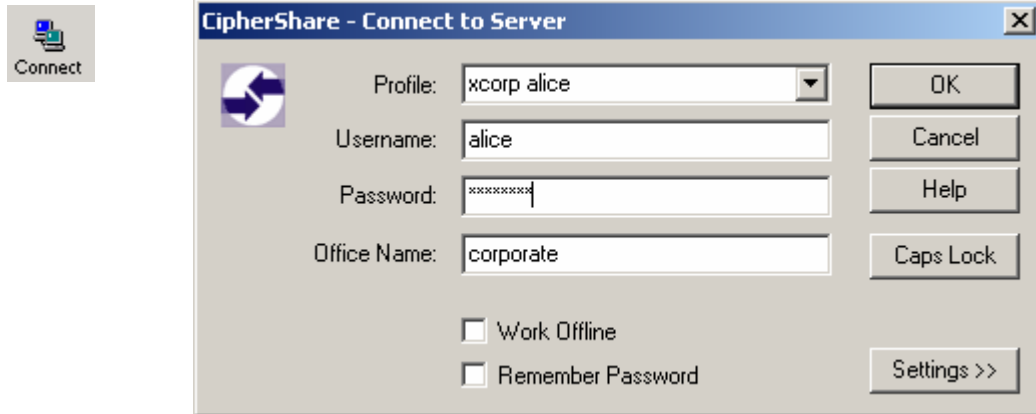
10. CipherShare Advanced Features

10.1   Connecting to the CipherShare Server

You may reconnect to the server at any time by doing the following:

1. Click the "Connect" button or choose "**Connect**" from the "*System"* menu). The "*Connect to Server"* dialog box will open.

2. Select the desired **Profile** (if you have created one) and enter your **Username** and **Password**.

    *Caps Lock***:** Allows you to toggle your Caps Lock button on or off.

3. If the office name field is blank, enter your given *Office Name.*

4. Select *Work Offline* if you are not connected to a network and you wish to access the encrypted documents cached on your computer.

5. Click on the *Settings* button to view more settings such as: database path, server hosts, port number and proxy server. These settings should already have default values that you set on your first connection as indicated by your CipherShare systems administrator.

10.2   Connection Options

The following settings should only be changed by **Advanced Users or as a result of instructions from your CipherShare Systems Administrator**. You may override the default connection settings by entering the proper data in the following fields:

- **Database Path:**
  Click on the **Browse** button and navigate to the desired path that will contain your local CipherShare Database. It should be placed in a directory to which you have **write access**. If you select a folder that is on a shared network drive, you will see a warning message with details indicating how to protect your information in this situation.

- **Reset Local Database:**
  Only select this option if you need to rebuild your local database from scratch.

- **Internet Server Host:**
  External CipherShare Server IP address or domain name.

- **Intranet Server Host:**
  Internal CipherShare Server IP address or domain name.

  Note: An * next to Internet Server Host or Intranet Server Host indicates which connection information CipherShare will use when attempting to establish a connection to the CipherShare Office. The position of the * will change depending on the IP address assigned to your PC and the selections selected in Internet Settings.

- **Server Port:**
  The port on which the CipherShare Server is configured to listen.

- **Keep Alive Timeout:**
  If CipherShare does not receive a Keep Alive message from the server for the specified period of time, then it will assume there is a problem with the connection to the CipherShare server. Recommended default value is 30. This parameter may need to be increased for very busy servers or in situations where the network connection is very slow or prone to errors.

- **Proxy:**
  Select the type of proxy (if required). SOCKS4 and HTTP are supported.

- **Proxy Server Host:**
 Specify the proxy server's IP address or domain name.

- **SOCKS4 Proxy Server Port:**
  Specify the proxy server's port if different from the default values determined for the proxy type.

- **Proxy Username:**
  Specify the username required by an HTTP proxy server.

- **Proxy Password:**
  Specify the password required by an HTTP proxy server.

- By choosing *Intranet Settings…* you can specify which IP address ranges reserved for private network use should be considered as Intranet (checked) or Internet (not checked) addresses when determining which connection to use.
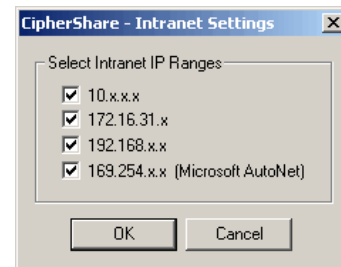
Click *OK*. The user authentication and connection process will begin. The status icon on the bottom right of the screen should show that the connection is in progress.

The status bar at the bottom of the window should look similar to this:
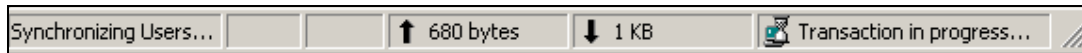
If you have connected successfully to the server, the status will show that you are
Online and the CipherShare window should be activated.

10.3   Disconnecting from the CipherShare Server

To disconnect from the CipherShare server you can do either of the following:

- Choose *Disconnect* (*System* menu).
- Click on the Disconnect button on the toolbar.

If you have a transaction in progress, you will receive a warning and the option to log off.
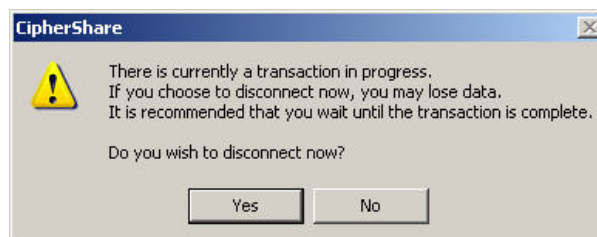
Your document list will disappear, and the CipherShare window will be disabled.
The status bar should show that you are *Disconnected*.

10.4   Exiting the Application

To shut down the CipherShare application window do either of the following:

- **Choose** Exit **(*System* menu).**
- **Click on the exit button of the window.**   ×

10.5   Changing your Password

You may change your password at any time. To change your password:

1. Select ***Change Password…*** from the **System** menu. The **Password Check** dialog box will appear.
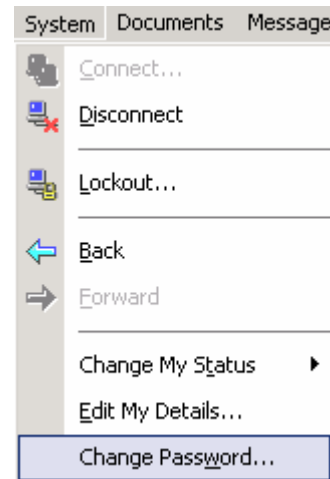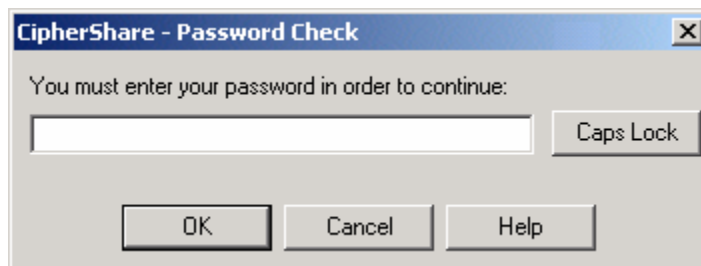
2. **Enter your existing password**. The **Change Password** dialogue will appear.
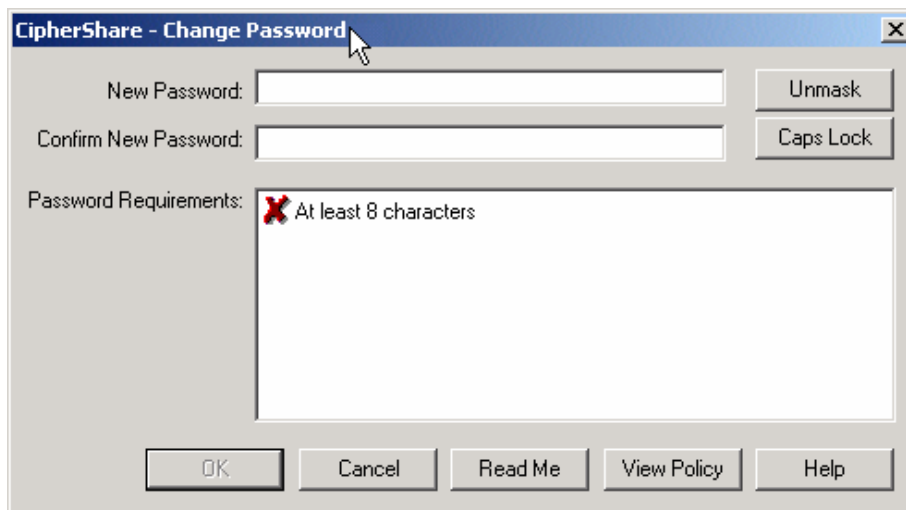
3. You must enter your old password then your new password and confirm it. You will have to meet the **Password Requirements** as determined by your CipherShare Security Officer. The Password Requirements display will show you interactively what requirements have not yet been met. As requirements are met, they disappear from the display. (Click [Read Me] to read about creating a password.)

4. **Enter and confirm your new password**. Do not forget it. You may use **Unmask** to show your new password in clear text, but this is NOT recommended for security reasons.

> *NOTE: The **Password Requirements** panel will interactively show you if you are meeting the password requirements defined by your CipherShare Security Officer.*

10.6   Resetting Your Password (Lost or Forgotten Passwords)

If the Password Reset feature has been enabled by your CipherShare Security Officer, and you have already gone through the password enrollment process (as described in Section 5.2 – Step 3(a)) you will be able to reset your password if it has been lost or forgotten, follow these steps:

1. Ask your CipherShare Security Officer to **co-ordinate a password reset**.

2. Your CipherShare Security Officer will ask you to work with him/her to answer the questions you provided during the Password Reset enrollment.

3. Answer each question exactly as you answered them during the enrollment process.

If you have answered your questions correctly, your CipherShare Security Officer will be able to generate a new temporary password for you. You may then use this password to login to the system exactly as if you were logging in for the first time. You will NOT lose access to any documents or files.

When an Password is Reset, a message is sent to all other users of the office advising them that this has occurred. A second message is sent to all users when you access your account with the temporary password. This causes new keys to be generated for your account. You must have these new keys signed in accordance with your companies key signing policies.

10.7   Enrolling in Account Recovery

If your CipherShare Security Officer has enabled Account Recovery, you will be able to enroll in the account recovery process. Account Recovery allows a CipherShare Security Officer and the Account Recovery agents you designate to recover your account in cases where it is needed (e.g. a sudden accident or death).

Enrollment in account recovery is only possible if it has been enabled. To enroll:

1. Select **Enroll in Account Recovery** from the **System / Key Recovery** menu
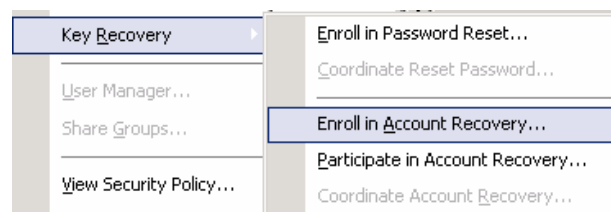
2. Select your **Account Recovery Agents** from those available
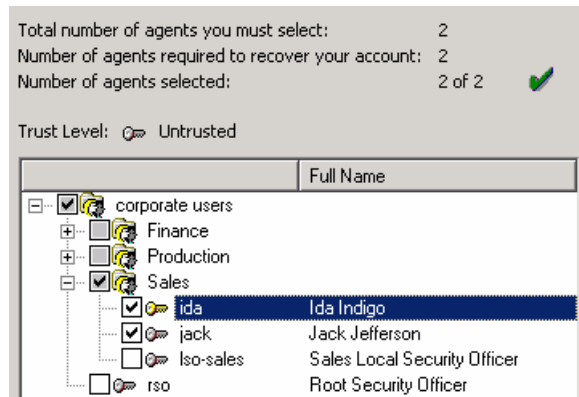
3. You must select individuals until the total number selected matches the number designated by the CipherShare Security Officer.

4. The selected recovery agents equaling "*Number of Agents Required to Recover Your Account*" must collaborate with a Security Officer to gain access to your.

5. Click **OK**

10.8   Participating in Account Recovery

If you have been selected by a user as an Account Recovery Agent, you may be requested to participate in an account recovery process.

To participate in an account recovery process:

1. Select **Participate in Account Recovery** from the **System / Key Recovery** menu.
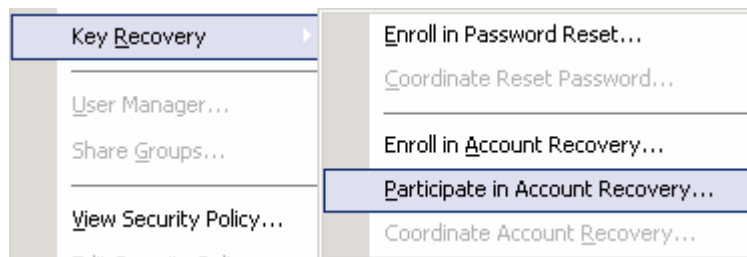
2. Enter your password in the **Password Check** dialogue.
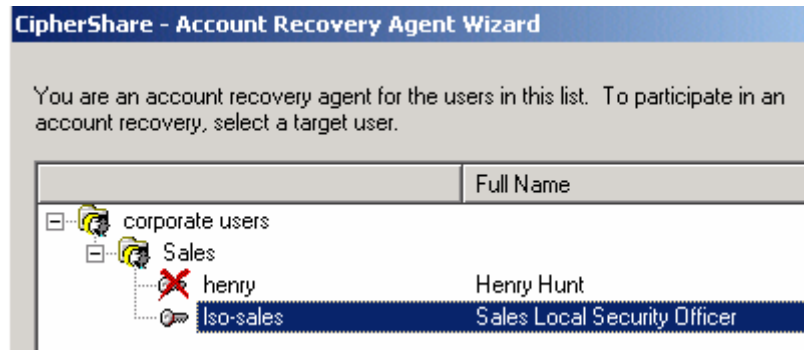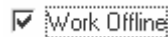
3. Select the user for which you will participate in an account recovery process. Click **Next** to continue.

4. Select the CipherShare Security Officer you will endorse as a Recovery Coordinator. Click **Finish** to complete your participation in the account recovery process.

10.9   Working Offline

If the Work Offline check box option is selected within the login dialog box, you will not connect to the CipherShare server. You can locally access your CipherShare database with all your downloaded documents in **read only** mode. This means that you cannot download any files not in your local database, *create any new CipherShare files or edit your existing CipherShare files, unless previously locked by you when you were working online.*

The status bar shows that you are:

10.10 Inactivity Time Out

A system lockout will automatically be triggered after a specified period of idle time. This is to prevent others from accessing your CipherShare files should you leave your PCunattended.

1. Change this setting by choosing *Options* (*Systems* menu).

2. Click on the *Security* tab and go to the **Inactivity** section.

3. You can **disable** this option by unchecking the checkbox or you can change the **idle time period** to a desired value.

☑ Inactivity Timeout [15] minutes.

Note: The Inactivity Timeout may be grayed out if the Security Officer set the policy to force the use of an Inactivity Timeout.

If you are locked out due to inactivity, CipherShare will prompt you to re-enter your password in order to continue using CipherShare. During an inactivity lockout, your online status will be reported to other users as **Away**.

10.11 Lockout

If you wish to **immediately** have your CipherShare window disabled, you can click on the *Lockout* button on the toolbar. You are required to enter your password to resume your session. Your online status will be reported to other users as **Away**.

10.12 Crash Recovery

CipherShare can automatically detect if you are abruptly disconnected from the CipherShare Server (i.e. due to a power outage or system crash). When reconnecting to the CipherShare server after such an occurrence, you will receive a prompt requesting permission to resume an interrupted transaction.

10.13 Manage Keys

CipherShare allows you to view and manage your security keys by selecting **Manage Keys** on the **System** menu. You will be required to input your password prior to gaining access to this feature.

Your key types consist of the following:

1. **Public Signing Keys:** used to confirm your digital signature when signing documents.

2. **Public Encryption Keys:** used when sharing encrypted documents on the CipherShare server.

3. **Secret Keys:** used for hard drive or local database encryption.
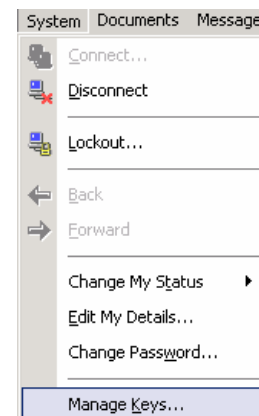
The **Manage Keys** feature allows you to view your existing keys and their creation and expiry dates. You can also view the status of your signing, encryption and secret keys.

To view the digital fingerprint associated with a key, select a key from the displayed list and click "**Fingerprint**".

To generate new keys (recommended once per

CipherShare - Manage Keys

Cryptographic security level: AES-128, ECC-NISTK283, HMAC-SHA256

Key Number	Creation Date	Expiry Date
1	2/14/2004	2/14/2006
2	2/15/2004	2/15/2006

year), click the "**Generate New Keys**" button.

Whenever you generate a new Public Signing Key, you must undertake a key signing process as per your organization's policy so that documents can be shared with you using your newly created key.

10.14 Key Signing

In a typical key signing transaction, two users will co-sign each other's key after first verifying their public key fingerprints. The fingerprints must be verified outside of the CipherShare system, commonly over the phone.

This ensures that the digital identity of the person – as identified by their keys and digital fingerprint – is matched to their real identity. Without formally verifying keys through a key signing process, there is a chance that someone who should not be on the system is masquerading as a legitimate user. Once key signing has taken place, however, the user's identity is established and the key is "**trusted**".

There are two methods by which "**trust**" with another user can be established:

1) Each user could formally verify the identity, and sign the key, of another user. This is the most secure, but also the most labour intensive method by which user's identities are established.

2) The principle of "**transitive trust**" allows people to trust each other through one user – a CipherShare Security Officer – who is responsible for verifying each user's identity. For security reasons, transitive trust can only be granted to a CipherShare Security Officer.

The method used by your CipherShare group will be established by a security policy.
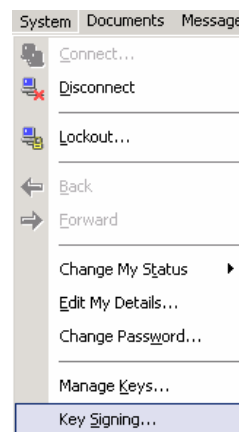
There are three levels of trust in CipherShare:

1) A "**Trusted User**" is someone who's key you've signed directly (you are assured that your connection with them is not being intercepted). This will be indicated by the **gold key** beside their username in the User List.

2) An "**Indirectly Trusted User**" means that you are trusting another user based on their verification with a CipherShare Security Officer (e.g. if User A trusts Security Officer B and Security Officer B trusts User C, then User A can indirectly trust User C). This is indicated by a **combination** key (gold & silver).

3) An "**Untrusted User**" is someone whose key has not been signed by anyone. This is indicated by a **silver key**.

Signing a User's Key Directly

To directly sign the key of another user you should call the person on the phone and then, while the user is on the phone, follow these steps. Make sure the user is logged into the same CipherShare office as you are.

1) Select "**Key Signing**" from the "**System Menu**". You will be presented with the Key Signing screen.

2) Select the user whose key you wish to verify and click the "**Sign Key**" button. You will be presented with the "**Sign Key**" screen as shown below.
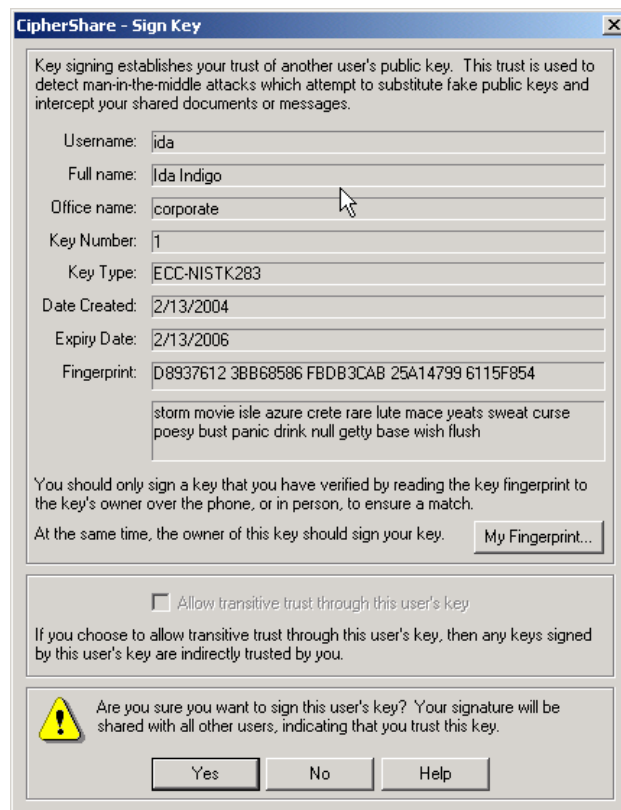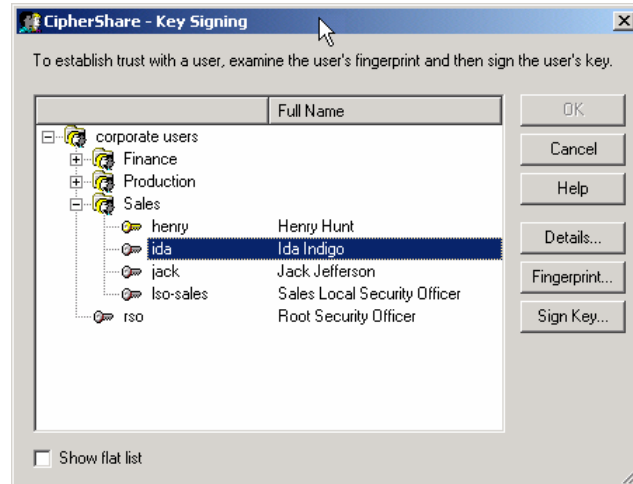
3. Have the user whose key you are verifying veiw their own digital signature by:

   a. Selecting "**Key Signing**" from the **System** menu
   b. Selecting their name
   c. Clicking "Fingerprint"

Ask the user to read out the first four digits of their fingerprint, or the first four words of the fingerprint text as shown below.

Then read out the next four yourself. Repeat alternating reading until the digital fingerprint is completely read through and check to ensure that there is a perfect correspondence between their version of their own digital fingerprint, and the fingerprint you are associating with them.

If these do NOT match perfectly, then the identity of the user within CipherShare does not match the person's real identity. **Your CipherShare Security Officer should be alerted immediately if this is the case**.

If you are satisfied that the two digital fingerprints match, then you are in a position to trust that user. Do so by clicking the "**Sign Key**" button. Their status will change from "**Untrusted**" or "**Indirectly Trusted**" to "**Fully Trusted**".

Repeat the process in reverse (i.e. you read your own digital fingerprint while they read yours) and have them sign your key to establish a mutually trusted relationship.

10.15 Advanced Option Settings

Choose *Options…* from the *System* menu. A tab menu will appear giving you the option to configure the following:

Documents

- **Working with Documents:** allows you to choose the default double-click action on a document – Prompt (default), View or Edit.

- **Recent Documents:** allows you to define how many documents will be displayed when you click on Recent Documents in the Document tree.

- **Automatic folder selection for newly imported documents:** allows you to choose the default naming convention for the folder names of your newly imported documents. This allows you to retain the names of a document's directory folder in Windows Explorer.

- **Confirmation Prompts:** allows you to choose whether to display prompts when checking in a document or when deleting a document.

- **Notifications:** allows a notification bubble to slide up near the **system tray** temporarily, indicating the user who has shared with you a new document or a modified document.

- **Importing Documents:** allows you to automatically securely delete the original of an imported document/

Messages

- **Double-click behaviour:** allows you to choose the default double-click action for a message – **View**, **Reply** or **Reply All**.

- **Preview Pane behaviour:** allows you to mark a message as read when displayed in the preview pane.

- **Reply and Forward message formatting:** allows you to choose your reply/forward message prefix and line length.

- **Confirmation prompt** allows you to choose whether to have a warning displayed when choosing to delete a message.

- **Notifications:** allows a notification bubble to temporarily slide up near your **system tray**, indicating the user who has sent you a new message.

- **Spelling:** allows you to specify if you want spell checking to occur while you type a message.

Chat

- **Notifications:** allows a notification bubble to temporarily slide up near your **system tray**, indicating the user who wishes to chat with you.

- **Spelling:** allows you to specify if you want spell checking to occur while you type chat text.

Security

- **Inactivity:** You can disable or enable the Inactivity Timeout feature and set the length of idle time allowed before your CipherShare window is disabled. Your password is required to log back into your session.

- **Warnings:** You have the option to display warnings regarding editing, importing, secure delete, etc.

Extensions

- **Open safe extensions only:** enabling this option allows CipherShare to validate an application's extension before decrypting the file and requesting Windows to launch its associated application.

- **Add safe extension:** allows you to add extensions to the default set of safe extensions pre-configured into CipherShare.

- **Remove:** allows you to remove extensions from the list of safe extension.
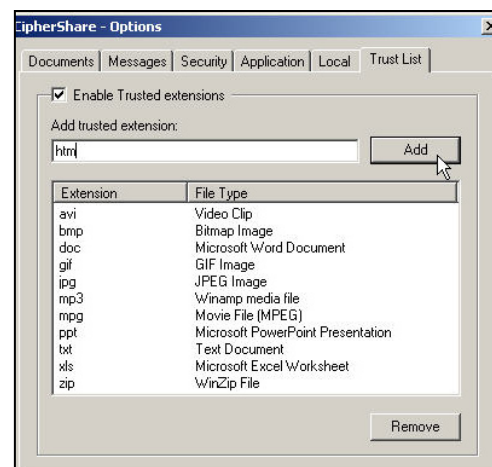
Local

- **Email Settings:** allows you to specify how to send email notifications. Selecting **MAPI** allows CipherShare to use your default mail client for sending email notification. Selecting **SMTP** requires that you enter your own outgoing mail server that can be used to send email notifications on your behalf.

- **Sounds:** allows you to customize and test the WAV file to play in when receiving a new document, message or chat session.

Other

- **Auto-Download):** if selected, allows any file under the threshold size to be **fully downloaded automatically**.

- **Files to display in tree:** allows you the option to choose which filter folders will be displayed in your CipherShare Messages and Documents tree.

- **Notifications:** allows a notification bubble to temporarily slide up near your **system tray**, indicating that a user has just connected or disconnected from CipherShare.

10.16 Online Status Settings

Click on the *System* menu, then hover your mouse over ***Change My Status***. A slide out menu will present you with a number of choices (Online, Busy, Be Right Back, Away, On the Phone, Out to Lunch). Select that status that reflects your current status. This information will be available to others through the Users folder.

You can also change your status by right clicking in the Status area of the Status Bar.

When a lockout timeout occurs or you click on the Lockout icon, your online status automatically changes to Away. When you login again your online status will revert to the setting that existed before the lockout occurred.

11. CipherShare Administration Features

## 11.1 Security Policy Configuration

CipherShare allows the Root Security Officer to configure the security policy specifically for any CipherShare office. The configuration options and how they are implemented are described in the CipherShare 3.0 Server Setup tutorial located on the CipherShare installation disk.   The tutorial can also be accessed through the following link:
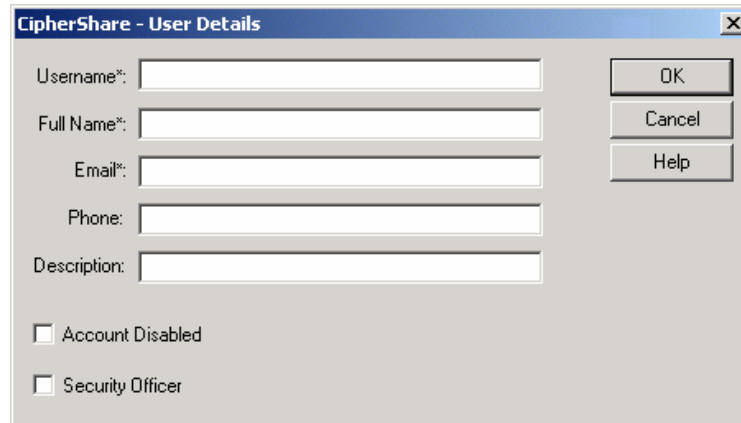
CipherShare 3.0 Setup Tutorial

11.2 User Manager

This feature is used by a **CipherShare** S**ecurity Officer** to initially assign sections, subsections, section Security Officers and user accounts. Only Security Officers can **edit** or **disable** user accounts.

1. Choose **User Manager** from the **System** menu. The user manager dialog box will launch displaying the Office Name, the Root Security Officer, users and sections.
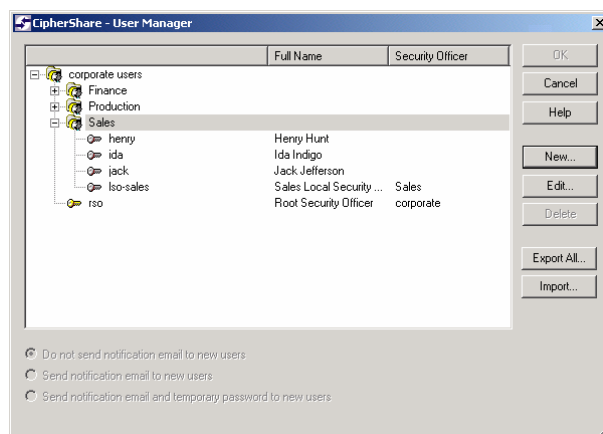
2. Click on *New*. You will have the option to create a new **User** or **Section**.

    a. To create a new section, select Section, enter a Section Name, and click **Ok**

    b. To create a new user, select **User**, **enter the user information** and click **OK**. You may elect to disable the account, and/or make it a **Security Officer** account.

TIP *Once you create a section, you can assign a **Security Officer** to the section, who then has the ability to create user accounts **within that section only**. You may also create Subsections within a Section.*

You may choose to send the new users an **email notification** about their new accounts, with or without their **temporary passwords**.

The message with subject **User Manager Log** will be generated and sent to the security officer responsible for creating the account with each user's temporary password.
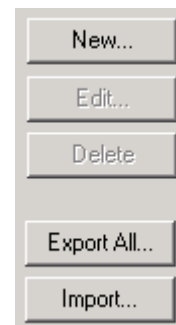
Importing and Exporting User Lists

CipherShare allows the importing and exporting of user lists to streamline the account creation process when creating new offices.

To **export** an existing account list from within the **User Manager**, click **Export All**.

This will generate an "**<office name> users.dat**" file containing all the accounts from the current CipherShare office which can be stored locally on your computer.

To import an account list, click **Import** and select the ".dat" file containing the user list. This will create the accounts in CipherShare and generate temporary passwords.
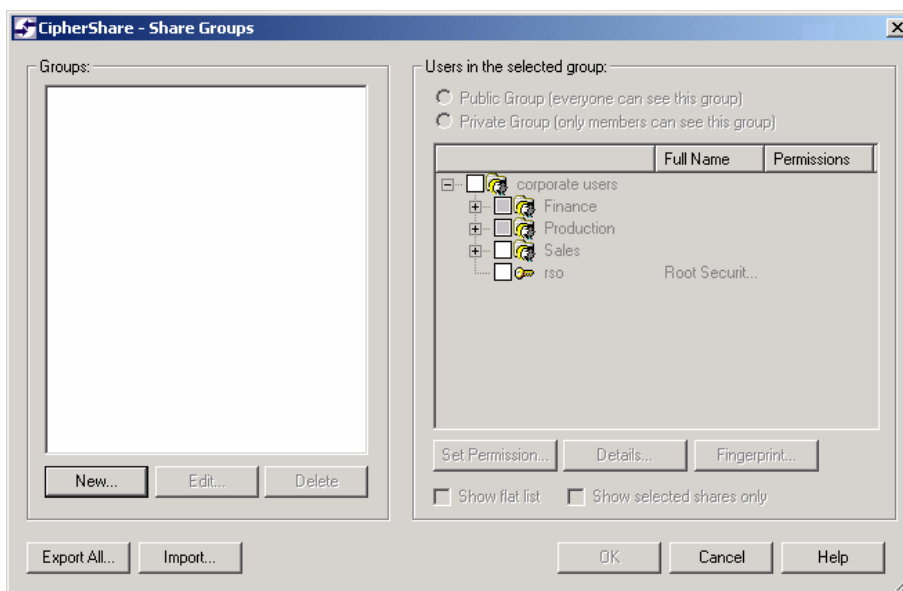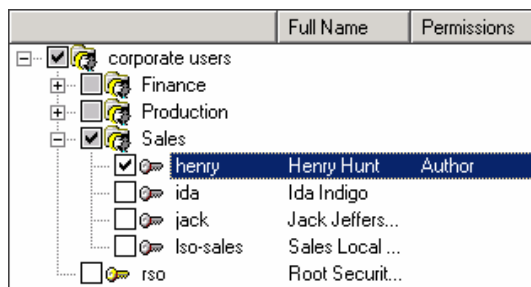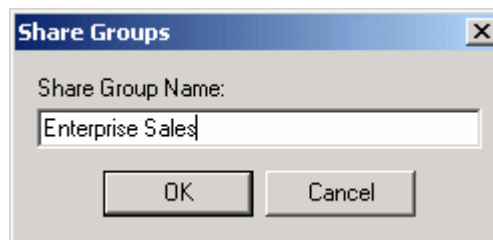
11.3   Share Groups

A Security Officer can define Share Groups to facilitate document sharing through pre-configured lists of users with predetermined privileges.

A user will be able to access these groups in the *Document Sharing* dialog box.

1. Choose **Share Groups…** from the *System* menu.

2. Click on the **New** button and enter a name for the share group.

3. Select the users in the group by checking the box beside their name(s).

4. Assign each user an **Access Permission** by right clicking on the username and selecting **Reader** (default), **Author** or **Manager**. If you would like to set the same permission for an entire section, right-click on the section name and choose an access permission from the menu. All the properties that you set here will be passed on, if you choose to add this share group to a document Share List. The final permission settings chosen in the share list will override any access permissions from the Share Group.

5. Choose whether the share group will be **Public Group** (viewable by everyone) or a **Private Group** (viewable by members only).

6. Once you are finished click on **OK**.

11.4   Password Reset (Lost or Forgotten Passwords)

If you have enabled password reset, you may recover a user's password by coordinating a Password Reset session.

To coordinate a Password Reset session, ask the user for whom the password is to be reset to be available in person or by phone and follow the steps below:

1. Select **Coordinate Reset Password** from the **System / Key Recovery** menu

2. **Enter your password** in the **Password Check** dialogue and click **OK**

3. Select the user for whom the password will be recovered.
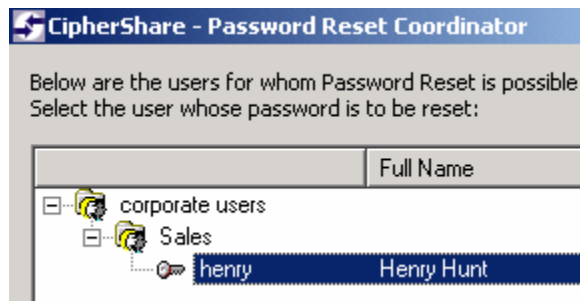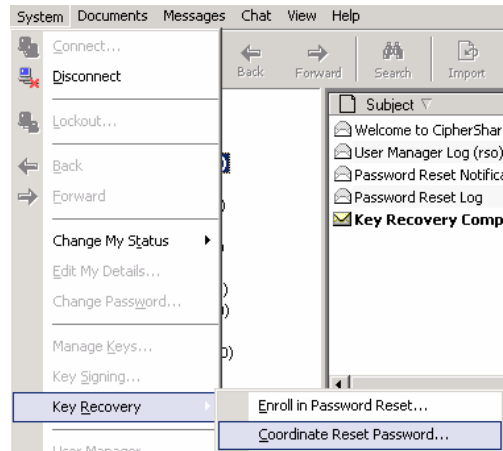
4. Have the user answer their password reset questions and type them into the associated answer areas. When finished, click **Next**.

5. Ensure that the new temporary password for the user is captured and click **Finish**. The user will be able to login to their account with the new temporary password.

11.5   Account Recovery

In cases where access to an account must be enabled in the absence of the account owner (e.g. in the case of a suddenly deceased user or someone who will not disclose their password on termination), CipherShare allows account recovery.

CipherShare's account recovery process relies on the consensus of a minimum set of account recovery agents designated by the user to work in collaboration with a Security Officer. This "split key" approach prevents a single rogue administrator from recovering an account on his/her own.
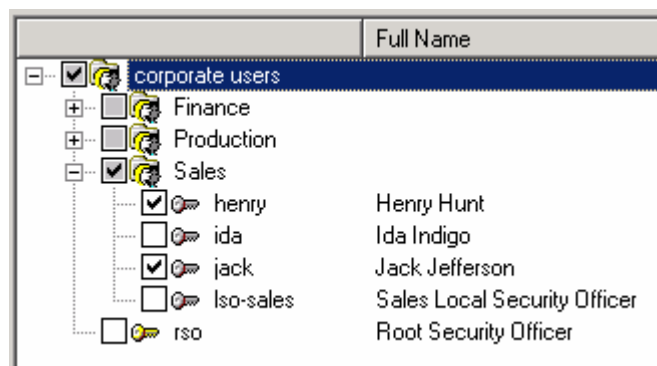
Enabling Account Recovery

To enable account recovery:

1. Select **Edit Security Policy** from the **System** menu

2. Check **Enable Account Recovery**
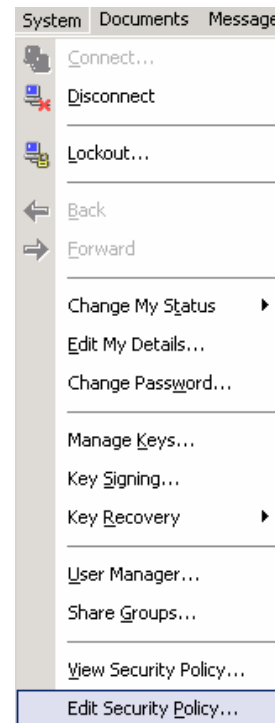
3. Use the up/down arrows to define the total number of **Recovery Agents** (the pool from which account recovery agents can be drawn)

4. Use the up/down arrows to define the threshold number of **Recovery Agents** (the minimum necessary to participate in an account recovery process from that pool)

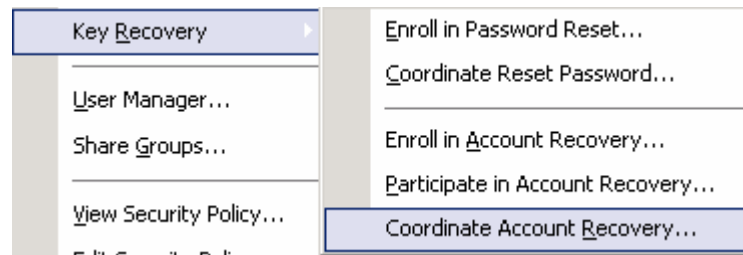5. Click **Add/Remove** to select specific users as recommended Recovery Agents
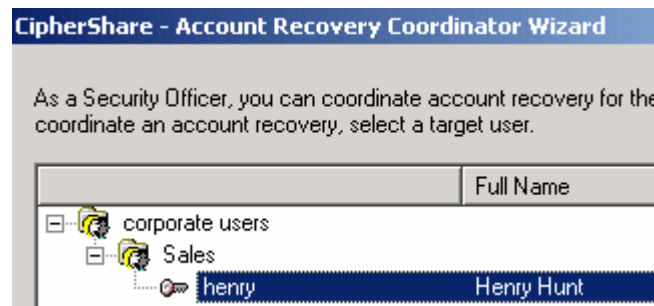
6. Click **OK**

Coordinating Account Recovery
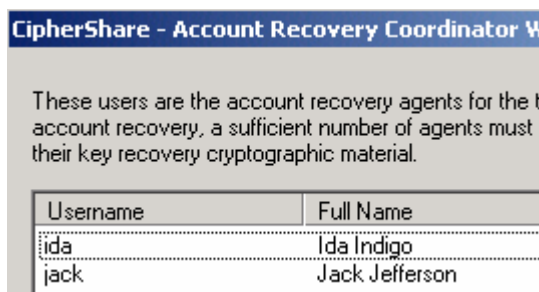
To coordinate an account recovery:

1. Select **Coordinate an Account Recovery** from the **System / Key Recovery** menu.

2. Enter your password in the **Password Check** dialogue.

3. Select a **target user** for the account recovery process.

4. Review the account recovery agents for that account. Click **Next**.

5. Request participation from those agents selected for account recovery. Without their participation, key recovery cannot occur. Click **OK** to send a message to agents not yet participating.

6. Once all key recovery agents have participated, key recovery can occur. Click **Finish** to complete the account recovery process.

75 of 77
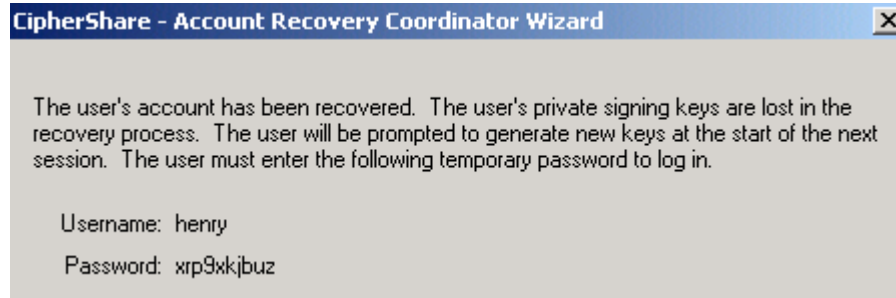
7. Record the new temporary password.

Contact Information
For contact information, please visit: www.provensecuritysolutions.com