Acknowledgements

We would like to thank the following people, without whom this project would not have been possible.

Bruce Schreiner, Counterpane Systems - For the design of Blowfish and Twofish
http://www.counterpane.com
Francois Peitte : For providing freeware code for FTP and internet components. (Your postcard is on it's way) http://www.rtfm.be/fpiette/indexuk.htm
David Barton : For providing freeware code for several Encryption techniques.
http://www.scramdisk.clara.net/d_crypto.html

I would like to also thank the following people (names used with permission).

Phil Viton - helping track down bugs and excellent improvement suggestions.
Peter Babik - for help with testing and fixing major bugs. Also, for excellent suggestions.
Siddy - for his installer splash screen and help with testing.
Matt Kahn - for his great help at testing and excellent suggestions.

And all those currently anonymous people.

Configuration

All of the settings on the

To access the configuration page, select the Setings / User Administration Tab, then click either the Client Settings, Server Settings or Global Options tabs. There are many options available, and they will all be explained below :

Global Settings

Miscellaneous Settings

Launch EFTP with Windows as a service.

This will put in the registry key (for Windows NT and 98) so that EFTP will launch before any users have logged in. NOTE : EFTP will launch, but the server won't necessarily start. To make the server start, choose the option in the Server Settings.

Check for Update on Startup.

This option will make the application automatically download a .html file (using the HTTP protocol) on startup, which will tell it what version is available on the internet. If the version number is newer, it will inform you that there is a new version available and ask if you would like to download it. Generally it is a good idea to continuously update this application, because it is always being improved. If you choose to retrieve the udpate, then the application will use your default browser to download the file http://www.eftp.org/eftp2setup.exe. You will need to manualy launch the setup once the file has been completely downloaded. This was so designed so that your client would not be tied up downloading this file via it's own FTP.

Start Maximized & Start Minimized.

By default, this application will start as a normal window on your desktop. It is possible to start this application maximized by checking the Start Maximized checkbox - I would guess that most people would want this option to be on. It is also to start the application minimized by checking the Start Minimized button checkbox. To start this application in normal window again, ensure that both of these checkboxes are unchecked. Needless to say, you cannot have both of these buttons checked at the same time.

Minimize to Tray and Hide from Taskbar

These two options work together. You can make it so that the application when mimized will appear on the system tray (near the clock). You can also hide it from the taskbar (which would be in most cases your preferred choice) by selecting the option Hide From Taskbar.

Mask Passwords

If you want to see all the passwords on screen and in log files, you can switch this OFF

Don't Warn When Quitting

This will disable the warnings that you are connected to somebody and also the warnings if anybody is connected to you when you try to close the application.

Delete temporary files on exit (*.key and *.tmp files in EFTP directory)

When changing directories and checking encryption keys, EFTP saves temporary files in it's folder. By selecting this option, you can remove these files when the application terminates. If you need to send these files as part of bug reporting, don't have this checkbox checked, or be sure to send the files before the application closes. It is not necessary to keep these files, and won't do any harm to have them deleted. The .key files are used for encryption negotiation, and the .tmp files are used for receiving directory structures from the remote host.

Logging Settings

Show Client Log Window / Show Server Log Window

In case you are not interested with seeing the logs, you can turn them off by checking either of these boxes. The change is immediate.

Timestamp Events

This will timestamp each logged event in both the client and server so that you can see when an event occurred.

Verbose Logging (screen)

In case you want to see every message sent to and from the client/server, you can set this option on/off. For troubleshooting purposes, we would consider you turn this option on. NOTE : This shows all commands in unencrypted format, but you can see by the status on the top of the client screen whether or not command channel encryption is being used. It should say ENABLED if it is being used.

Timestamp Events

This will timestamp each event the moment it happened.

Log IP's with events.

In case you have a busy server, it is nice to see which IP did what and when.

Include Directory Logs

This will include the directory listings from the sites, useful for debugging. If there is a site which does not display properly, then please turn on this option, connect to a site, wait for it to fail, and then send us the log file.

Log To File

If you wish to log the events to a file, select this box. Remember to specify log file names.

Timestamp Logs

This will create a new log for each time the application is started. The time and date of when the session began will be appended to the filename specified.

Append Logs

Only available if you do not timestamp logs. This option will not overwrite an existing log, but rather add to the log. If you don't have this checked, and you don't have Timestamp Logs checked, then the existing log will be overwritten and a new one created.

Client Log File

You must use the browse feature to the right of this entry box to specify where you wish to create the file. If you don't specify a file extention, then none will be added for you, except if you have timestamp logs specified. If you dont' specify a filename, then no client log will be created, even if you have Log To File checked.

Server Log File

You must use the browse feature to the right of this entry box to specify where you wish to create the file. If you don't specify a file extention, then none will be added for you, except if you have timestamp logs specified. If you dont' specify a filename, then no server log will be created, even if you have Log To File checked.

Command Channel Encryption Settings (Currently Disabled)

EFTP has become even more secure now with up to 2048 bit Command Channel encryption for sending and receiving commands. To find out how this works, check "How the Authentication Works"

To enable this feature, you have to generate a keypair on the machine you are using, and the clients that want to connect to you, or the server you wish to connect to. This keypair is unique to the application, and it is not required to manually give the host or server your public key - this is done automatically for you.

You can set the key strength by changing the key bits and key length. WARNING - Generating a new key can take up to 5 minutes using the highest settings, and your application may look like it has stopped responding. This is in fact not the case, and your application will resume normal operation once the new keypair has been created.

Server Settings

Start Server component on Application Startup

By selecting this option, the server will automatically attempt to go live when the application starts. If you wish, you can select this option and place a shortcut to EFTP in your startup folder, this way your FTP server will start whenever windows starts.

Server Port

This setting is mandatory for the server to function properly. By default, FTP servers sit on port 21, but if you want to avoid detection of having a service on port 21, you can use an alternative port. The higher the port, the less chance that the service will be detected, as people normally don't have the patience to scan every possible port. Port values range from 0 to 65535, although unix will treat the ports as 0 to 32767 and -1 to -32768.

Maximum Concurrent Users

This will set the maximum amount of users that can connect to your server at one time. Minimum 1, maximum 10000.

Default home directory

This is good to set so that users who don't get assigned a home directory from either any of their group memberships or from their own settings, will get this home directory. Usually you would make this home directory maybe a directory which does not have subdirectories, or which has links to other areas. Remember that if a user does not have a home directory, he will be denied access.

Encryption Settings.

You can only have one of the two options selected here. Encrypted and Normal Clients. This option will allow clients which don't support encryption and EFTP clients to work. This is the default setting, but will allow clients to connect and transfer files unencrypted. The more secure setting would be allow Encrypted Only Clients, in which case encryption MUST be successfully negotiated before the user can download any files or change directories.

Show Superuser Warnings

This option will alert you when a user logs in with superuser access. The alert will be a red message in the client and server logs. By turning this option off, you can also surpress the confirmation when you make a user a superuser when editing user details (check User Administration)

Connect Message / Login Message / Logout Message

With EFTP you can specify a text file to display when the users connect (before they attempt login), as well as a message to display after they have logged in, and even a message to display when they have logged out. Use the Folder icon next to the appropriate box to locate and select a text file of your choice. Use the notepad icon to either a) create a document (if none exists, it will propt to create), or b) edit the document selected.

IP Address Allow/Deny

A great new feature is to add IP address denies/allows. Unfortunately, only IP addresses can be used for the moment, there is no support for hostnames - yet.

Allow

Use this radio button to specify the list is an ALLOW list. Only users who's IP addresses match IP addresses/ranges specified in the list will be allowed in. If you don't have any IP addresses specified, then no checking will occur. The list is automatically saved when you exit the application.

Deny

Use this radio button to specify the list of disallowed IP Addresses. Users who's IP Addresses match IP addresses/ranges specified in the list will be denied access. If you don't have any IP addresses specified, then no checking will occur. The list is automatically saved when you exit the application.

Add

Use the Add button to add an IP Address/Range to the list.

Delete

Use the delete button to delete IP Address(es)/Range(s) from the list.

Clear

Use this button to clear the list completely. This is not a reversable process.

How to add IP Addresses/Ranges.

EFTP will do a compare of the IP Address/range specified with the first part of the connecting IP Address. For example : If you have specified 10.14.15 in the list, it will match the IP Address 10.14.15.31. Don't use wildcards if you can. If you use the * wildcad, then it will ignore it, and only match the numbers and dots before the asterisk

Virtual Directories

Virtual directories are basically replacing real directories with other names. This is useful if you wish to hide your directory structure, or if you want to structure your server in such a way as to make things understandable. You would probably want to use Virtual Directories along with Permanent Links or normal links.

The server basically remembers the real directory where the user is located, and returns the virtual name for that directory when the client does a PWD or XPWD.

Example : Say you have the following virtual directory mappings

Directory	
M:\Hidden Documents	\Temp
N:\Financial Statements	\Finance
D:\Temp	\

Then whenever a user is in M:\Hidden Documents, they will see the directory as \Temp. If D:\Temp is their home directory, then you would probably want to create a link to M:\Hidden Documents in D:\Temp, so that the user does not see M:\Hidden Documents - the link will show it as \Temp.

Permanent Links

Very useful with Virtual Directories (above). Basically, the permanent link will display links regardless of which directory you are in. A link to a directory will NOT show if you are in the directory. Here is a basic example of how it would be used.

Directory	Link Name
D:\Home	Home Directory
M:\Movies	Movies
N:\Naughty Pics	Pics
O:\Organic Recipies	Recipies
P:\Pandora's Box	Hacking

So when the user logs in, and their home directory is D:\Home, then included in the directory listing for D:\Home, they will see links to Movies, Pics, Recipies and Hacking. If they are in a directory not shown above, then they will see links to all 5 directories.

Client Settings

Socks Server

This is the default socks server that will be used when no socks server is specified in the individual site information. If you want a specific site to use no socks server at all, you can ovverride this default socks server in the client site details.

Socks Port

The port to use with the socks server. By default this is 1080, but you HAVE to type a number in, whether it is the default number or not.

Socks Username

This is only required if your socks server requires you to authenticate

Socks Password

This is only required if your socks server requires you to authenticate

Default Passive Mode

This switch will turn Passive Mode ON or OFF by default. This cannot be overridden in the client settings, but it will not be a problem if Passive mode is on for every session. Passive mode gets around some implementations of NATs and Firewalls.

Automatically Skip files which already exist complete

This will automatically skip files that are already downloaded (presuming you are downloading into the same place).

Automatically Resume files which partially exist

This will automatically resume files that have already been partially downloading (presuming that you are downloading to the same place).

Becoming a Server

Becoming a server is quite easy - you require the following :

A Port number

This is usually port 21, but can be any port number, including port 0. Valid values are -32768 up to 32767. To set the port number, it is on the Setup Screen.

A user

Without at least one user, nobody can log in. Technically, this is also a requirement, even though the server will go up without any users in the database. If you add users when the server is already online, you do not have to restart the server. On the same note, if you change a users rights, the user will need to log out and back in for those changes to become in effect, as the rights are all read when the user logs in.

Working the server

Starting a Server

To start the server, you can press F11, or click Server -> Start Server.

Stopping a Server

To stop the server, you can press F12, or click Server -> Stop Server. If you stop the server when users are connected, they will be automatically disconnected.

Kick all Users

To kick all users immediately, select Server -> Kick all Users. This function is actually pointless, because normally you would not really want to do this.

Beta Testing / Bug Reporting

As with any application, it is bound to have one or two bugs. Even though this application is free, I will fix bugs and provide limited support. Before e-mailing me a bug, please check the bug tracking page at http://www.eftp.org. To submit a bug, please e-mail eftp2@eftp.org Please give details of the version number you have, and explain how to reproduce the "bug".

Your feedback will remain confidential, and your e-mail address will not be given out to any parties for any reason.

Connecting to a Server

To connect to a server, the data must be entered into the Connection Manager. Once you have selected a site in Connection manager, then clicking the connect or reconnect button will take you to that site.

It is not necessary to read the following, but it is here for your edification and delight.

The process of connecting to the server is as follows :

- You connect to the selected port of the server, the server acknowledges your connection, and asks to send username.
- You send the username, the server will respond by asking for your password.
- You send your password, the server will at this time either successfully authenticate you or reject your authentication request.
- You request a SYST command to the server, the server should respond.
- If the SYST response contains the word "EFTP", and you have set the client to use an encryption key, then the client sends a request for the file *encryption.key*, otherwise the client will attempt to work in non-encrypted mode, and continue at the part when the client does a PWD request.
- If the client receives a file *encryption.key* (saved as sitename.key in the PATH of the EFTP executable), then the client will check the encryption key, and then turn on encryption if the checking is successful. If the encryption key check is not successful, then the client continues with the PWD, unless it is set to force encryption in which case it will just disconnect.
- Once the encryption key has been checked and was successful, then the client sends another SYST command, to indicate to the server that the encryption negotiation was successful. The server then turns it's encryption on, and then replies with the confirmation that encryption was successful. The client now continues as follows :
- The Client sends a PWD - The server responds with a home directory.
- The Client sends a DIR command - The server responds with a directory listing of the home directory. NOTE - the server will ALWAYS allow the listing of the home directory, whether or not you give the LIST rights to it.

To continue from this section, you should go to the Navigation and Queue sections.

Frequently Asked Questions

For an updated list of Frequently asked questions, you should check the FAQ page on http://www.eftp.org This help file might not contain the more recent asked questions.

Is this product available for Linux?

I will be happy to port this product to Linux, but I can't afford the $999 for "Kylix" which is the development package we would need. If anybody got this for christmas and does not need it, we would never say no to a gift...

Will this program remain proprietory?

It's not really proprietory, I'm using a standard FTP implementation, and just modifying it a bit so that the data chunks are encrypted rather than sent in normal binary (or ASCII) mode. Once you've read how the encryption is done, you could probably write your own client/server.

Is the source code available?

As much as I would like to make all the source code available, I am afraid I cannot. I will make part of the source code available, including the parts which make up the encryption, but my application also uses commercial code which I am not licensed to supply. The source code I will supply will only help those in understanding how the program works, but they will need to program the rest (like the shell explorer windows) on their own.

Is there any back doors to this program?

No there is not. I challenge anybody to try to find one. If there is a weakness in this application, let me know and I will announce it personally. I didn't intend this application to provide high encryption when it can be circumvented. There are NO back doors, and the source code which handles authentication will be available so that you can see for yourselves.

How can I REALLY see if the data is being encrypted?

There are two ways to ensure the data is being encrypted. First of all, on the client side, when you connect, it should give you the message about encryption being enabled, and what the strength is. If you would like conclusive proof, use a program like Sniffer, transfer a simple .TXT file (or another file which you can easy see in traces), and then see if you can see the file in the traces. This is what I am using to ensure that the encryption is being done.

Why is this program free?

It's too much hastle, and I think the taxman has enough of my already hard earned money, why give them more?

If I wanted to send you a donation, where would I send it to?

Amazon vouchers are cool, send them to us via e-mail.

Group Administration

The purpose of groups is so that you can give a large amount of users the same rights, by making them members of the groups. For example, if you wanted 30 users to have access to D:\MP3's and E:\MP3's, then create a group called MP3's and then make those 30 users members of that group, instead of having to give the individual rights to the users.

To start editing the groups, select Settings / Server Admin -> Groups. When editing groups, the server and client portions will continue to work in the background.

You have 6 main options.

NEW : Use this to create a new group. When you create a new group, you cannot use the name of a group which has already been used, but you can have the same word if you use different cases. Example, you can add a group called "Warez" if a group called "warez" already exists.

CLONE : Use this option to create a new group, but to copy the access rights of an already existing group and place into the new group. The new group will have the same home directory too, but the new group will not be by default enabled.

DELETE : You can delete groups using this button. NOTE : If you delete this group, no checks are done to remove the group from users. This won't have a negative effect, but if you create a new group with the same name, then the users who were previously members of the group will now have the same rights as the new group with the same name.

RENAME : Change the name of a group. Note that you will have the same problem if you had deleted the group. The users who were members of the old group will NOT be members of the new group, but of the old group name which does not exist any more.

SAVE : It is not necessary to use the save option, it is automatically saved when you exit the application, but it won't be saved if the application crashes. NOTE : Any changes you make are immediately in affect (except for already logged in users), the SAVE will just commit it to disk.

DISCARD : If you stuff up, and you accidentally delete a group which you didn't want to do, then you can use the DISCARD button. This will reload the group database from the last saved copy.

Administration

Editing a group is easy - select the group from the left pane, and then it's details will be shown on the right of the pane.

Current Group : This shows you the group name that you are currently editing. This is here so that you can see which group it is you are editing.

Home Directory : This is to set a group's home directory. This users's home directory will always override any group home directories. A user needs a home directory from either his user account or any of his group memberships, otherwise they will be denied access.

Group Enabled : You have to enable a group before the rights will be used for users who are members of the group. If you disable a group, then users who are members of the group will no longer receive those rights. Note : Users who are already logged in will not be affected.

Access Rights : These are the rights which are given to the users who are members of the group. For more infromation about these rights, read the Access Rights page.

How the Authentication Works

RSA Command Channel Encryption

Just after the client has connected to the server, the client will send a PUBK command to the server, and include it's public Key. The server will respond (encrypting it with the client's public key) with it's public key, and once this has been done, all subsequent commands, including USER, PASS, RETR, QUIT, etc are encrypted using the client and server's public keys. Unfortunately, RSA is slow, and all commands will generate high utilization during the encryption and decryption moments. In order to enable this feature, you have to generate keypairs on both the client and the server.

Blowfish Data Channel Encryption

During the login process, the client will request a file called *encryption.key* from the server.

If the server has an ecyryption key for the client, then it will create a block of data 1020 bytes large, containing completely random data. It will then calculate a 32 bit (4 byte)checksum on those 1020 bytes of data and append it to the end, making a 1024 byte block of totally incomprehendable data. It will then encrypt that block of data using the encryption key that it has for that user, and then send it to the user.

The client receives this data (saving it as sitename.key in the eftp program folder), and then basically does a reverse operation. It decrypts the 1024 byte block using the encryption key that it has, and then does a CRC check on the first 1020 bytes of data. If the checksum matches the last 4 bytes of data, then the encryption key is assumed to be the same, and then the client sends a SYST command to the server, to indicate it is happy and tells the server to turn the encryption on. All file transfres from this point (including directory listings) will now be encrypted. For infromation on how the encryption works, see the How the Encryption Works topic.

If the encryption key on the client and server are incorrect, then the CRC check will fail, and encryption will not be turned on. The client will continue in non-encrypted mode, depending on what optoins you have set. The encryption key is never sent from the client to the server or vice-versa. I might change this model later, but for now this is how it is.

How the Encryption Works

Once the encryption keys have been checked and verified (check How the Authentication Works), encryption will be used for all files (including directory listings). Directory listings is basically a temporary text file sent from the server to the client, and saved as ip address + connection handle + .tmp in the EFTP directory, and then read and displayed.

One improtant thing to note, is that the file is never encrypted at source, and decrypted at destination. The file is read as normal data, and then encrypted before being sent. Also another thing to note is that the algorythm used is Blowfish, but I am considering using Twofish, as it is a more powerful and faster encryption technique.

When uploading a file, the Client reads 1514 bytes of data, encrypts that block of data using it's encryption key, sends it to the server. The server receives the data, stores it in a buffer, and then decypts the data 1514 bytes at a time. The server has to store it in a buffer before decrypting, because it is not guaranteed how much data the server will receive at one time - this is not controlled by the winsock layers and lower levels.

When downloading a file, the Server reads 2048 bytes of data, encrypts that block of data using the encryption key, and then sends it to the client. The client receives the data, stores it in a buffer, and then decypts the data 2048 bytes at a time. The client has to store it in a buffer before decrypting, because it is not guaranteed how much data the client will receive at one time - this is not controlled by the winsock layers and lower levels.

As you can see, encryption is not requiring to encrypt the file first before sending. This also thankfully means that file resumes can happily commence regardless of whether encryption was used or is being used etc. For example, if you upload 20 Mb in unencrypted mode, and then switch to encrypted mode, and continue the same (resume upload) file, then the file will still be correct in the final result.

The encryption and decryption is done so fast (on the fly), that you can quite easily upload/download a file at 500 Kbyte/sec.

Navigation

The local side (Left)

This is slightly different to most of the ftp clients that you are used to. The left hand side, is a pure exlorer window. When you double-click it, it will do what explorer would normally do. Example - if you double-click a .mpg file, then it will play it. If you double-click a .jbc file then it will try to mount/dismount the bestcrypt container. Drag and drop must use a RIGHT mouse button, not the usual left mouse button. To upload a file, drag and drop the file (using the right mouse button) to the queue, or you can drop the selection on the remote side, which will then add it to the queue.

Left double click to change directories and to execute files

The remote side (right)

The remote side uses either the left mouse button or the right mouse button to drag and drop to the queue. You can also of course drag and drop it to the left hand side to add it to the queue. You can only use this side if you are connected to a remote host. Left double-click to change directories (iconized by a folder icon), or to download a file (iconized by a white page). You can also change directory into links, iconized by a little bookmark type symboll.

Other Navigation

Other parts of the application can be accessed by clicking on the appropriate tab. The Client portion of this application can be accessed by selecting the Client Session tab (under the toolbar). The Server portion can be accessed by clicking the Server Session tab. By clicking the Settings / User Admin, you can get access to three more tab screens immediately below.

Settings is where you would do most of your application settings and configuration. It is not necessary to save these settings, they are automatically saved when you exit the application. These settings are better explained in the Configuration Page. You can also Edit Users (See User Administration for more info) and Groups (See Group Administration for more info).

Access Rights

You can assign access rights to users and groups.   You can have up to 32 access rights per user/group, and combined 128 access rights for a user who is a member of several groups.   If a user is a member of too many groups, and the combined access rights for all those groups is greater than 128, then the last access rights will not be given to the user.

Types of Access Rights

The following types of access rights are available.

Read

This right is required in order to read a file.   This is not the same as reading a directory - this is the List right as described below.   This right will allow people to download a file.

Write

In order to upload or append a file, you will require this right.

Create

Create is different to Write, because it is specifically to allow the user to create a directory. Usually you would give this right as well as Write rights to a specific directory.

List

This is usually required for every directory the user has access to, without this right, the user will not be able to change into this directory.

Delete

This will allow users to delete files and/or directories.

Rename

To allow the user to rename a file or directory (sometimes useful), grant this right.

Inherit

This will let the right be available for that directory specified, and all subsequent subdirectories.   You would usually grant this except to maybe an upload directory where you don't allow creating of directories.

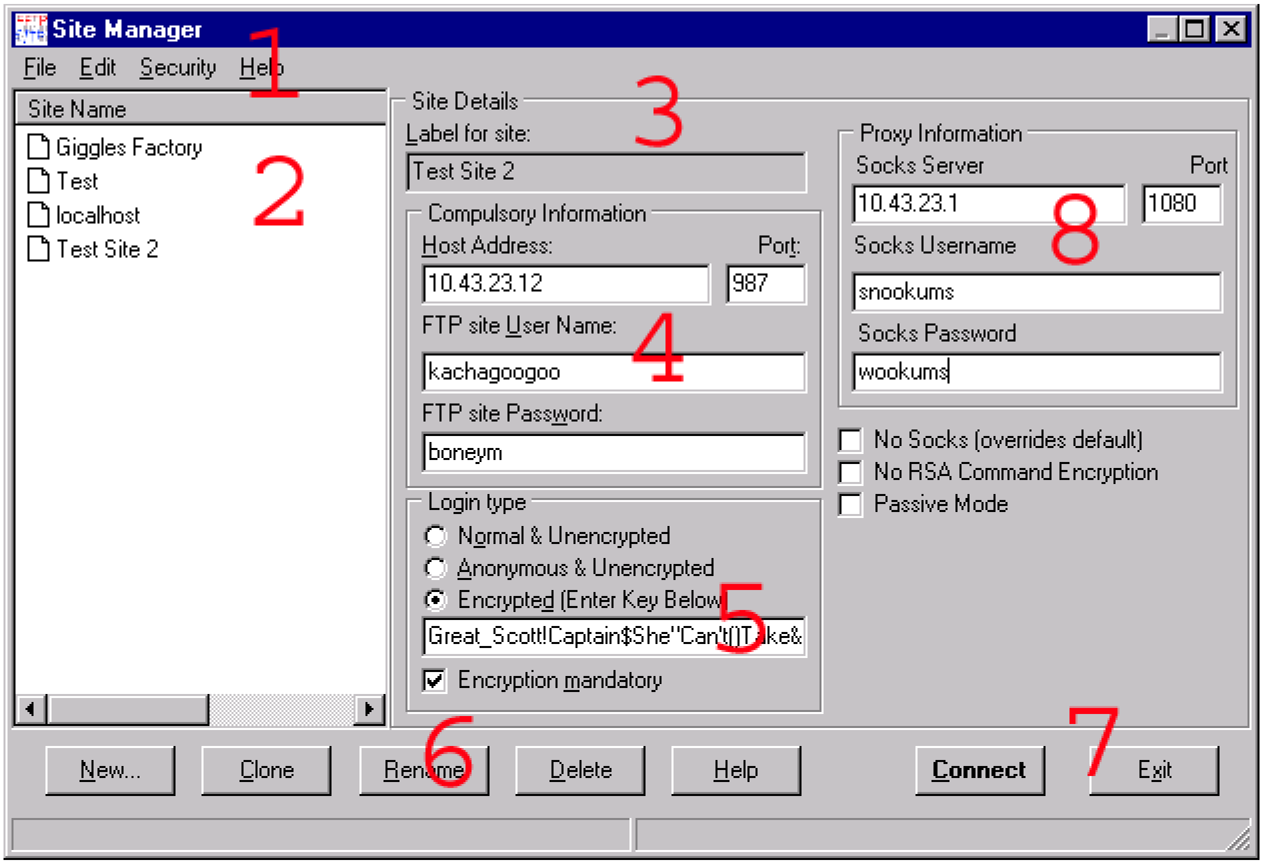
Superuser Right

A User (not a group) can be given the superuser flag, which means that the user will have all rights to all directories that you have access to (including UNC paths, other computers, etc), regardless of what the operation is.   Give this only to users who you can trust enough.   Usually you would only give this right to your own user account so you can access your files from another location.

Note that all these rights are not propriatory, which means that they will apply regardless of what the FTP client is.   Remember that this application is 100% compatable with all FTP clients and servers.   If there is a client/server which does not work with this application, please let me know. (Help -> About in EFTP).

The Connection Manager

Below is a representation of the Site Manager, which can be accessed at any time by pressing F4, or selecting it from the main menu (File -> Site Manager)



Site Name
Giggles Factory
Test
localhost
Test Site 2

Site Details
Label for site: Test Site 2

Compulsory Information
Host Address: 10.43.23.12 Port: 987
FTP site User Name: kachagoogoo
FTP site Password: boneym

Login type
○ Normal & Unencrypted
○ Anonymous & Unencrypted
● Encrypted (Enter Key Below)
Great_Scott!Captain$She"Can't()Take&
☑ Encryption mandatory

Proxy Information
Socks Server: 10.43.23.1 Port: 1080
Socks Username: snookums
Socks Password: wookums

□ No Socks (overrides default)
□ No RSA Command Encryption
□ Passive Mode

Index to Numbers

1. The good old trusty menu.

2. This is the list of sites that you have added. By selecting one of them, it will show the details on the right hand side, which is explained below. Once you have selected one, it will automatically be chosen as your quick connect, so therefore you can press the Connect Icon on the main screen (second from the left), and it will connect you to that site. The quick connect is only really useful if you were connected, and you have to reconnect. You can then connect without having to run the Site Manager again.

3. This shows the site you are currently editing. It is possible that the focus is taken off the list, so you can't see by looking at the list which one has actually been selected.

4. More information is stored here on the IP address (or hostname), port number, username and password.

5. This is where you can define whether or not you want to use encryption. You can only use encryption with a EFTP 2 server, so setting this here will not work if you connect to a unix type ftp server. You should read the **[{Link to topic How the Authentication Works:How the Authentication Works}]** and **[{Link to topic How the Encryption Works:How the Encryption Works}]** if this interests you more.

6. Click on the NEW button to add a new site. Click DELETE to remove the highlighted site. You can also rename a site if you wish, by clicking the RENAME button, and you can also Clone a site by clicking the CLONE button.

7. Clicking on HELP will bring up this topic. If you want to connect immediately, press CONNECT, otherwise you can just close the window if you wish. NOTE - there is no SAVE button - everything on this screen is automatically saved for you.

8. Socks information. This will override any socks servers set in default in the settings pages. Leave this blank if you do not wish to use a Socks Server.

Editing Information

When adding a site, you must provide at least 4 pieces of information before you can successfully connect. These are highlighted in red.

Label for Site : This will show you which site is currently being modified.

Host Address : This is either the IP address or DNS name of the host you want to connect to. You can even use localhost if you wish to test from your own machine to your own machine.

Port : If you are not using the default port of 21, you should type in an alternate port number. If you leave this blank, the application will use the default of 21.

Passive Mode : Use this if you need to connect through certain firewalls, or if the site you connect to requires it. If your FTP does not work when you do a LIST or GET, then try to turn this on.

FTP Site User Name : You obviously need a user name to authenticate

FTP Site Password : You also need a passord to authenticate

Login Type :

Normal & Unencrypted : Use this option to opt out of encryption, even if the host supports it.
Anonymous & Unencrypted : Use this option to log in anonymously, but also with no encryption.
Encrypted (Enter Key Below) : Select this option to use encryption on the client side, if it is supported on the server. The key is the one told to you by the person who is hosting the site.

Encryption Mandatory : Select this if you want the client to disconnect if no encryption is available. This will ensure that you cannot accidentally do transfers if encryption was not successfully negotiated.

The Queue

All transfers and deletions are always done by the queue.   If you download or upload a directory, then the files contiained within will be added to the bottom of the queue.   You can now move items up and down the queue, depending on how you wish to download them. You can also save the queue and then re-load the queue.   Best to save before you start downloading.

User Administration

To start editing the users, select Settings / Server Admin -> Users. When editing users, the server and client portions will continue to work in the background.

You have 6 main options.

NEW : Use this to create a new user. When you create a new user, you cannot use the name of a user which has already been used, but you can have the same word if you use different cases. Example, you can add a user called "Idiot" if a user called "idiot" already exists.

CLONE : Use this option to create a new user, but to copy the access rights of an already existing user and place into the new user. The new user will have the same home directory too, but the new user will not be by default enabled.

DELETE : You can delete users using this button. NOTE : If you delete this user, they will not be immediately logged out, you will need to disconnect them manually.

RENAME : Change the name of a user.

SAVE : It is not necessary to use the save option, it is automatically saved when you exit the application, but it won't be saved if the application crashes. NOTE : Any changes you make are immediately in affect (except for already logged in users), the SAVE will just commit it to disk.

DISCARD : If you stuff up, and you accidentally delete a user which you didn't want to do, then you can use the DISCARD button. This will reload the user database from the last saved copy.

Administration

Editing a user is easy - select the user from the left pane, and then it's details will be shown on the right of the pane.

Current User : This shows you the user name that you are currently editing. This is here so that you can see which user it is you are editing.

Password : This password has nothing to do with the encryption, but it required for users to connect. NOTE that this password CAN be seen on the wire, because the FTP RFC uses clear text passwords. When using SSH (not supported in this application), then the password canot be seen as clear text on the wire. The user anonymous does NOT require a password, because any password will work fine.

Home Directory : This is to set a user's home directory. This users's home directory will always override any group home directories. A user needs a home directory from either his user account or any of his group memberships, otherwise they will be denied access.

Encryption Key : This is a text string of your choice which you have to tell the user when you give them the IP, port, user and pass of your site. The safest way to send this information to them would be in a PGP (or other encrypted) e-mail or encrypted direct client to client chat. Another safe way of doing it is to tell the user that the encryption key is the answer to a question that they would know, example "The encryption key is the same as your favourite song, no spaces and no capitals". The server and client needs to use the same encryption string, otherwise encryption will not be successfully negotiated. The string can contain ANY characters from $00 to $FF (ASCII characters 0 - 255), but Windows is not easily capable of entering these characters.

Account Enabled : You have to enable a user before they will be able to connect. If you disable a user, then the user will no longer be able to log in. Note : Users who are already logged in will not be affected.

User has Superuser Access :   This will give the user unlimited rights accross your entire file system, including file systems you have rights to too.   Example : If you were connected to a NetWare Server, a NT Server and a Unix SMB Share, then the logged in user will be able to access those resources too, if you had mapped drives to those resources.   You would usually only enable this option for your own username so that you can access your entire filesystem without having to give rights to yourself for all your resources.   Only enable this option for users who you really trust.   By default, you will be warned when you enable this option.

Group Membership : Use this to make the user members of groups.

Access Rights : These are the rights which are given to the user.   These rights take precedence over group rights if the same directory location used.   For more infromation about these rights, read the Access Rights page.

EFTP 2

Encrypted File Transfer Protocol Version 2.0
http://www.eftp.org
eftp2@eftp.org

Introduction

EFTP is a combined 32 bit Windows 95/98/2000/ME client/server which incorporates up to 448 bit blowfish encryption and the FTP protocol (RFC 959 implementation) to provide secure file transfers over the Internet. This program works 100% with other FTP Clients/Servers in non-encrypted mode, and provides strong encryption when the remote and local hosts both use EFTP 2. This program is FREE for public domain use.

For more information, please select a topic below.

Copyright Information

This application is free for Public Domain and can be downloaded from the following URL.: `http://www.eftp.org/eftp2setup.exe`. If webmasters or equivalent wish to distrubute this application, please ensure that all links point to the installable executable, so that users can always be assured to get the latest version of the software.

Disclaimer

As with any product, there is always a Disclaimer. I am in no way responsible for any loss of data as a result from either directly using this application, nor can I be held responsible if you choose to use this application for criminal activities, and I especially void myself from any guilt if you choose to use this high encryption illegally in your country. The laws of the use of encryption varies from country to country, so I leave it up to you to decide whether or not you should be using this application.

This product is currently uner Beta Testing, as it is still in development. Although rigorous testing is being done, not every concievable action can be tested, so therefore there is always a possibility something may go wrong. You are encouraged to report all bugs to the us.