EFTP3

Product Documentation and User Guide

Who's watching your data?

Documentation for EFTP3 Version 3.1.0
Updated Thursday, 15 May 2003

Table of Contents

INTRODUCTION 4

HISTORY 4

HOW DOES IT WORK 4

THE COMPONENTS 6

FTP Client 7
- Site Manager 7
  - Creating sites - a step-by-step instruction 8
  - Buttons Explained 8
- Quick Connect 9
- Connect/Disconnect 9
- Preferences 9
  - Operational Settings 10
  - Visual Settings 12
  - Security Settings 13
  - Connection Type 14
- Transfer Queue 15
- Connection Information 16
- Log Window 16
- Client Reset 16
- FTP State 16
- Up One Dir 16
- Refresh 16
- Home Dir 16
- Local View 17
- Remote View 17
- CLI (Command Line Interface) 17
- Queue 17
- Status Indicator 18

FTP Server 18
- Activity 19
- Preferences 19
  - Main Settings 20
  - Messages 22
  - Permanent Links 24
  - Virtual File System 25
  - Security Settings 26
  - IP Allow/Deny List 27
  - Web Based Admin 28
- User Administration 29
  - Creating users - a step-by-step instruction 29
  - User Administration explained 29
- Group Administration 33
  - Creating groups - a step-by-step instruction 33
  - Group Administration explained 33
- Access Rights 35
  - The Seven Rights 35

SUPPORT OPTIONS 36

Introduction

EFTP stands for Encrypted File Transfer Protocol (FTP). This application is a revolutionary new way of transferring files between two internet hosts so that any unscrupulous attempts to view your transfers or gain confidential information are thwarted. I'm not suggesting that your ISP or any of the main carriers would do such an act, but it's better to be safe than sorry. FTP has been around for ages and is a very quick and stable method of doing file transfers, however it does not provide the advanced security required for transferring confidential data.

With the availability of Network analysis tools like "Sniffer Pro" and "Ethereal", it is possible to capture network traffic between two hosts, provided you are on a network segment between the two hosts. Additionally, it is also possible to configure routers to capture traffic, or even to bridge two network ports so that a single computer can be set up to monitor network traffic for a large portion of the network. Now although you may trust your IT staff as I do mine, it is not impossible for a hacker or disgruntled employee to use this technology to steal corporate secrets, and therefore this product exists.

History

EFTP was originally written by Khamil Landross, who has unfortunately not been able to continue with the project due to insufficient free time. We approached Mr Landross and acquired his source code and product on condition that we keep it free for personal use, which we happily agreed to.

EFTP 1 was a never-released product. It was proprietary, wasn't based on any internet standards, and had limited functionality. With the availability of the ICS (Internet Component Suite), Khamil rewrote it and based the program on the FTP standard (RFC 959). EFTP2 is still today being used by many businesses and individuals alike.

How does it work

EFTP functions exactly the same as any other FTP Client and Server. The only difference is that before the standard USER and PASS authentication handshake, the client sends to the server its public key, and the server answers it with its own public key, after encrypting it with the client's public key. Another difference is that the client and server set up another Key to use for file transfers.

Example:

1. 30/04/2003 19:16:42 Attempting to connect to Localhost (127.0.0.1:21) using a Direct connection.
2. 30/04/2003 19:16:42 RECV <- 220 awaiting input
3. 30/04/2003 19:16:42 Session Established to Localhost (127.0.0.1:21)
4. 30/04/2003 19:16:42 SEND -> PUBK ++11KE:lM34IIsBUeyIUD8eCUfpaQY2oPGktvbWJHeVHgCx5lStCz9OKXRbWaSQGMNmkEaebjaVPMay+1yB60Q+g-GNAE1280512
5. 30/04/2003 19:16:42 RECV <- 666 ++11JE:WeTw4EcJYj2qzR2g7TLMZrLDDGwY3FBKzIhb91Tp-59Opl25QavH3uFVlooAdQv6x5YB0zRPV-fK96AlkGMoGU0640512
6. 30/04/2003 19:16:42 Two way RSA Control port encryption ESTABLISHED
7. 30/04/2003 19:16:42 SEND -> TC
8. 30/04/2003 19:16:42 RECV <- 909 No Terms and Conditions exist
9. 30/04/2003 19:16:42 SEND -> USER lester
10. 30/04/2003 19:16:43 RECV <- 331 Password required for lester.

11. 30/04/2003 19:16:43 SEND -> (It's a secret!)
12. 30/04/2003 19:16:43 RECV <- 230 User lester logged in.
13. 30/04/2003 19:16:43 SEND -> GETK
14. 30/04/2003 19:16:43 RECV <- 777 a×2JÛQ§¢ü^&òÎÊ'æ÷ËPì²™aÃ£ªË˜L"ž°ijöWhmÎ^>šÌ¬F´□%¿K·fôY„O
15. 30/04/2003 19:16:43 SEND -> SYST
16. 30/04/2003 19:16:43 RECV <- 215 UNIX Type: L8 - EFTP3 Server v3.0.8.53
17. 30/04/2003 19:16:43 SEND -> TYPE I
18. 30/04/2003 19:16:43 RECV <- 200 Type set to I.
19. 30/04/2003 19:16:43 SEND -> PORT 127,0,0,1,6,9
20. 30/04/2003 19:16:43 RECV <- 200 Port command successful.
21. 30/04/2003 19:16:43 SEND -> RETR *encryption.key*
22. 30/04/2003 19:16:43 RECV <- 150 Opening data connection for *encryption.key*.
23. 30/04/2003 19:16:43 RECV <- 226 File sent ok
24. 30/04/2003 19:16:43 Verification of Blowfish encryption Keys SUCCEEDED
25. 30/04/2003 19:16:43 SEND -> SYST
26. 30/04/2003 19:16:44 RECV <- 215 UNIX Type: L8 - EFTP3 Server v3.0.8.53 - Encryption ENABLED
27. 30/04/2003 19:16:44 SEND -> PWD
28. 30/04/2003 19:16:44 RECV <- 257 "/D:/" is current directory.
29. 30/04/2003 19:16:44 SEND -> PORT 127,0,0,1,6,10
30. 30/04/2003 19:16:44 RECV <- 200 Port command successful.
31. 30/04/2003 19:16:44 SEND -> LIST
32. 30/04/2003 19:16:44 RECV <- 150 Opening data connection for directory list.
33. 30/04/2003 19:16:44 RECV <- 226 File sent ok

In our FTP activity log above, we can see the client sending its public key in line 4. The 064 at the end is the key length, and the 0512 is the number of bits in the key. This is so that the server knows what length key to expect and set for the client. The server responds with a 666 response, and adding its own public key in line 5. However line 5 above is NOT what went across the wire, because the server actually sent that information AFTER encrypting it with the client's public key. What you are seeing in the log is what the client understands after it has unencrypted the line with its own private key. Line 6 verifies that control port encryption has been established.

When connecting to non-EFTP servers, you will get a message similar to

30/04/2003 19:22:19 Error encountered - 500 'PUBK ++11KE:lM34IlsBUeyIUD8eCUfpaQY2oPGktvbWJHeVHgCx5lStCz9OKXRbWaSQGMNmkEaebjaVPMay+1yB60Q+g-GNAE1280512': command not understood.
30/04/2003 19:22:19 Two way RSA Control port encryption FAILED

Or

30/04/2003 19:23:09 Error encountered - 500 Syntax error, command unrecognized.
30/04/2003 19:23:09 Two way RSA Control port encryption FAILED

This is not in fact an error, it's just informational. It does however mean that your session is unencrypted and therefore unsafe.

If the server you are connecting to is in fact an EFTP server, but it does not have a public/private keypair, then you will see an error message similar to the following:

30/04/2003 19:25:02 Error encountered - 503 RSA Encryption not available on this server
30/04/2003 19:25:02 Two way RSA Control port encryption FAILED

The communication in lines 9-12 has all been sent and received encrypted, and therefore any people sniffing the wire are not able to identify the username and password, which would normally be sent in plain text in a standard FTP environment.

But hold the phone! Commands like USER, PASS, CWD, GET etc are not the only things to be sent in plain text. All your directory structures returned from a DIR and LIST command are also sent in plain text and can also be sniffed. While this in itself is not harmful, it could give hackers an idea of the files that are stored on the server, and therefore could identify it as a potential gold mine, and end up concentrating all their efforts on obtaining access to that server.

Fortunately, EFTP incorporates an additional form of encryption that will make all file transfers both ASCII and BINARY totally illegible for any persons who are attempting to obtain such data. In our example above, the client requests a Key from the server (line 13). The server responds with a randomly generated key that is only valid for the current session (each client gets their own key). The client does some additional checks to verify the key authenticity, starting off with a SYST command (line 15). It then requests a file called *encryption.key*, to which the server sends a 4 Kb randomly generated file that has been generated (lines 17-24). The client receives this file, and confirms the key authenticity before deleting the file. If the validation is successful, you get a message

```
Verification of Blowfish encryption Keys SUCCEEDED
```

The client then continues to log in, get the remote path (usually home directory).

So, not only are all the commands sent to and from the server encrypted with PGP level security (RSA Encryption up to 2048 bits), but the files and directory structures are also encrypted using Blowfish, which is presently only vulnerable to a "brute force" method of cracking. Vulnerable isn't really an accurate word to use though. A brute force method of cracking basically means you try every password possible. As our Client and Server use randomly generated passwords for the blowfish encryption (which is negotiated and communicated using RSA encryption), it would take an average of 2.079650567184059146058666043 0318e+114 attempts to crack the encryption using that method.

Once you have established the connection using an EFTP client and EFTP server, you can rest assured that any attempts to monitor your transfers over the wire would be completely and utterly futile.

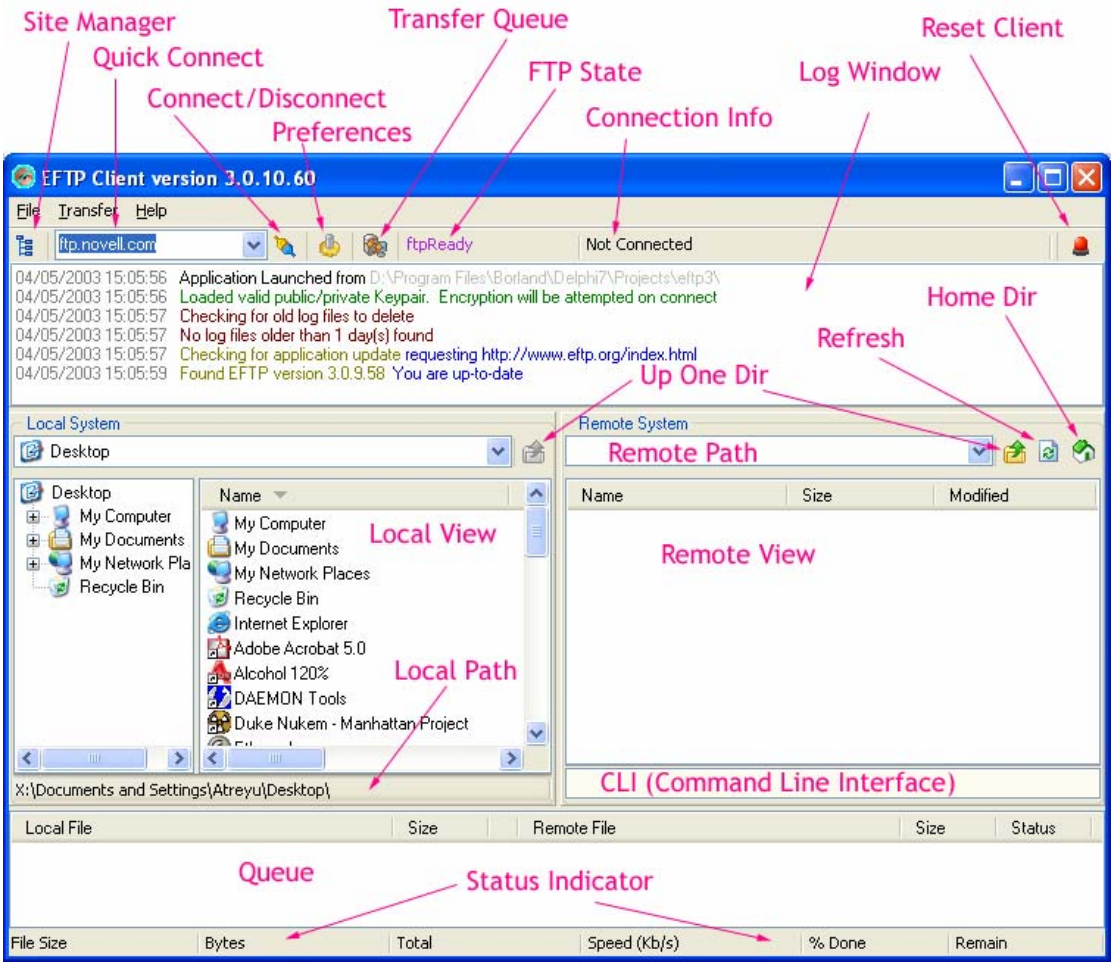
If your client is speaking to a server that does not understand this encryption, then the client will continue in non-encrypted mode.

The Components

In the previous version of EFTP, there was one application that had a combined client and server. While this might have been a good idea, the feedback that Khamil received was more towards making it two applications, for additional flexibility. We've gone for this approach, so that it is clear and easy to understand. Please remember, in order to have encryption, you need both the Server and Client to be EFTP, otherwise the encryption will not work.

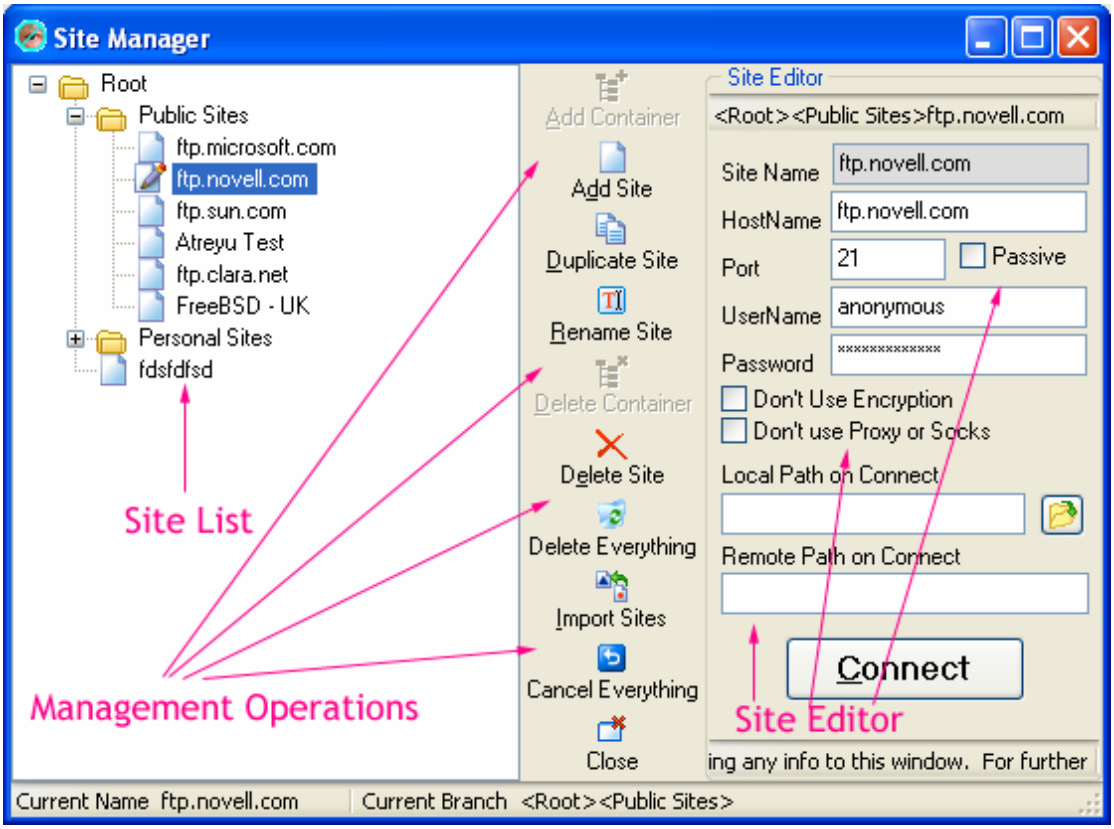
FTP Client

The Client does most of the work strangely enough. The server just obeys its commands but the client is the real brains in the operation. This is what the client looks like:



Site Manager

The Site Manager is always the first port of call. It is where you define which servers you would like to connect to, and gives you additional options for those sites.



Once in the Site Manager, you can use the Management Operation buttons to manage your site list. Whatever you do here is automatically saved when you either perform a new operation (Add Site, Rename Site, etc), Connect to a site or Close this window. If you made a mistake, you can always click the Cancel Everything button, which will revert all the data to what it was when you opened the Site Manager. Once you close the Site Manager, all changes you have made in that editing session will become permanent.

Creating sites - a step-by-step instruction

Using this step by step guide, we will create a new site.

1. If you don't already have the Site Manager open, Click the Site Manager Icon.
2. Select the **Root** Container.
3. Click **Add Site.**
4. Give the new site a name.
5. Select the newly created site under **Root**. (You may need to expand root first).
6. Next to **HostName**, enter either the host name or IP address of the server.
7. For **Port**, enter 21 (default FTP port) or the port number you were given.
8. If you are behind a firewall or NAT, check the **Passive** checkbox.
9. Enter your User Name next to **UserName.**
10. Enter your password next to **Password.**
11. All done! Now you can click **Connect** or set the other options if required.

Buttons Explained

Most of the buttons here are self explanatory, but for your convenience I'll describe what each one does.

- **Add Container** – use this button to create a new container or sub-section. The folder "Public Sites" is such a container.
- **Add Site** – this will add a new site under the current container. In the example above, the current container is Public Sites, which is located under Root.
- **Duplicate Site** – if you wish to duplicate site information, you can use this button. This is useful if you are given a new password for the same site, but wish to retain the old password information just in case.
- **Rename Site** – most people won't need to use this button, but the feature is there anyway.
- **Delete Container** – use this to delete a container and all of its children. I would think this button would get used even more rarely than the Rename Site button.
- **Delete Site** – if you wish to delete a site from the list, use this button.
- **Delete Everything** – if you really must get rid of all site information, click this button.
- **Import Sites** – useful if you wish to keep a backup of your site information (this file is called sitedata.ini), and have to restore it at a later stage. Just import it in, and you get all your entries back. Also useful if you wish to share site lists with other people.
- **Cancel Everything** – clicking the Cancel Everything button will revert all the data to what it was when you opened the Site Manager.
- **Close** – use this button to close down the Site Manager without changing your connection status.

The **Site Editor** is where you enter all the information for the selected site. NOTE – you must select a site you wish to edit before filling in any of the information.

The **Connect** button will make the currently selected site your chosen site for any further connections and disconnections. When you click this button, the Site Manager will close, and the **Connect** button on the Client main form will be pressed for you automatically.

Quick Connect

A simplified list of the sites you can connect to. To use, click the drop down box and choose a site which corresponds to the site you wish to connect to. This list will always show in the order that sites were created.

Connect/Disconnect

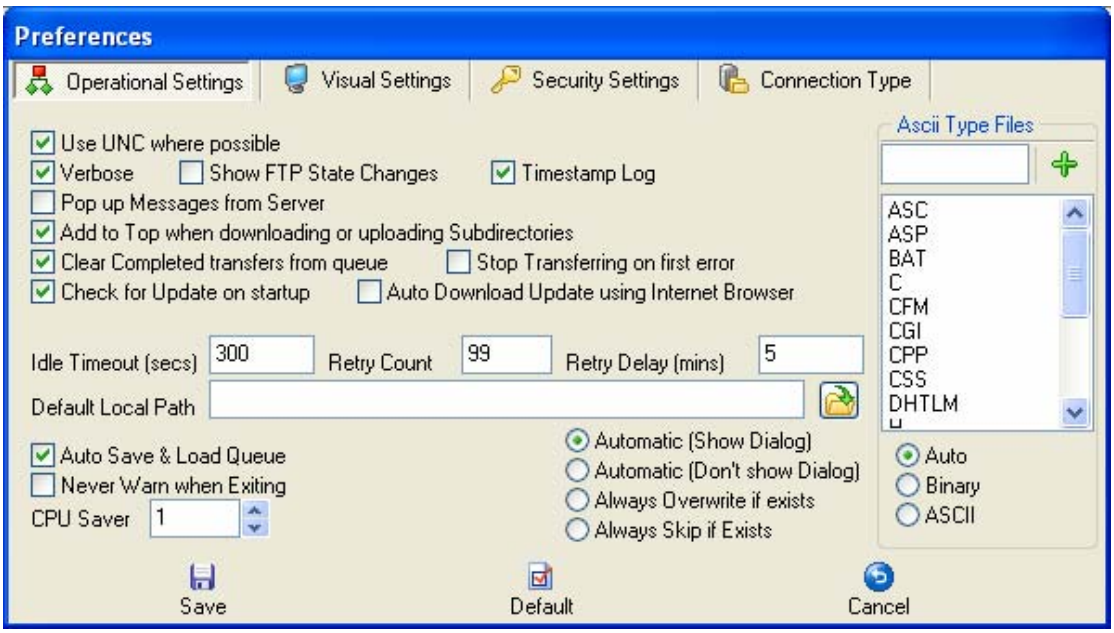
Most of the time you would use this button to disconnect from your current site, as the Site Manager would press it for you to connect in the first place. If you need to re-connect to the same site, you can do this by clicking this button. NOTE: You may only connect and disconnect if the client is in *ftpReady* mode. If you are busy transferring files, or waiting for a response from the server, you need to either abort the transfers or wait for the server reply.

Preferences

The options are split into 4 different categories; Operational, Visual, Security, and Connection Type. All these settings are stored in a single file, named EFTP3Client.ini. The buttons at the bottom of the Options screen will do the following:

- **Save** – this will save the changes you've made (if any), and then close this window.
- **Default** – this will reset all options to their default values
- **Cancel** – this will revert all changes you have made back to what they were when you opened this window

Operational Settings



There are several operational settings that you can have.

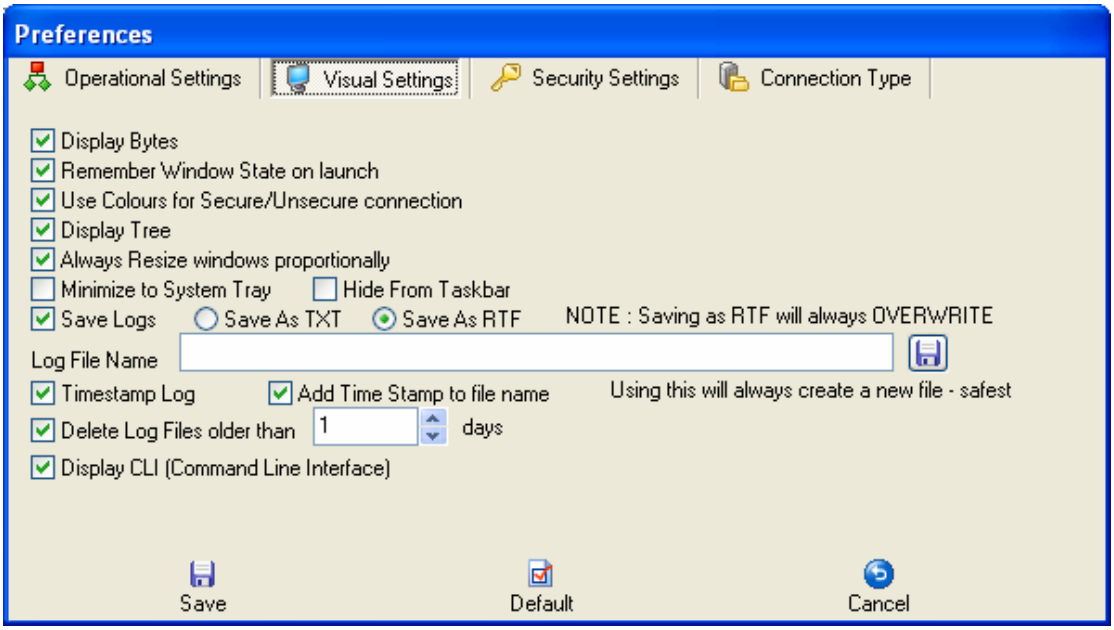
- **Use UNC where possible -** this application is UNC aware, so if you browse to a mapped drive in your Local View, this option will convert the mapped drive to a UNC pathname, and use UNC pathnames when you add files to the queue. NOTE: Using this option you may see a slight delay when browsing or adding files to the queue. This is because Windows Explorer is verifying the UNC pathname, as it is a different entity from the mapped drive letter.
- **Verbose** - I call this the techno-geek option. Use this to see all communications between the client and server. This option will be required if you are reporting a problem.
- **Show FTP State Changes** - use only if requested by us for support reasons. This will show the clients state changes in the log, but this information would be useless otherwise.
- **Pop up Messages from Server** - the server from time to time sends you greetings and messages. Most of these messages go by in the log window without being noticed, but having this option on will bring a pop-up window to your attention with the whole message on. NOTE: When this pop-up happens, the pop-up window will have control and will STOP your client from operating.
- **Add to Top when downloading or uploading Subdirectories** - when you upload and download subdirectories, the application traverses into those subdirectories and then adds the files to the queue to be processed. By adding them to the top of the queue, you process each subdirectory immediately, rather than at the end. Deleting directories on the remote side will always add them to the top of the queue, as it has to process the directories in that fashion.
- **Clear Completed transfers from queue** - by default, any items processed successfully from the queue are removed from the queue. If you wish to keep a record of the files you have downloaded, you can set this option, and the queue will never reduce in size.
- **Stop Transferring on first error** – When errors occur, i.e. permission denied and so forth, then having this checked will make the client stop processing the queue at that point. With this unchecked, the client will move on to the next file and so on.
- **Check for Update on Startup** – Having this option checked will make EFTP get the file http://www.eftp.org/index.html, which contains information about the latest

version of EFTP. It will then display on the log view, whether or not you have the latest version or if there is a new one to download

- **Auto Download Update using Internet Browser** – Having this checked will use your Internet browser to download the latest version of EFTP, should the check find you or not on the latest version. You will most likely have to intervene at this point to tell your browser where you want the file saved. If you launch the file without saving, then you should close your Client (and Server if applicable) before allowing the installation to continue.
- **Idle Timeout (secs)** – If for any reason your client is no longer receiving data from the server, or the client is no longer in use, this idle timeout will kick in, and do one of the following:
    - If Client is not busy transferring – Client will start transferring
    - If Client is not busy transferring and it has no files in queue – Client will disconnect
    - If Client was busy transferring – Client will disconnect, save queue into a temporary queue, and then attempt to reconnect.
- **Retry Count** – this is the amount of times the client will try to reconnect in the case where the server is not contactable due to communication problems.
- **Retry Delay** – This is the delay time before attempting reconnects. With a retry count of 99 times and a retry delay of 5 minutes, the client will try to reconnect to the server for 8¼ hours.
- **Default Local path** – Some users have a special place to download all their files to. By setting this to be that path, the client will automatically change the local view to be this path upon successful connection to any site. This option is overridden by any site specific local paths (if applicable). Use the Open Folder button to locate the folder, or type it in manually.
- **Auto Save & Load Queue** – Usually when you disconnect from sites, the queue is cleared. Having this option checked will make your client save the queue when you disconnect, and load the queue when you reconnect to the same site.
- **Never Warn when Exiting** – If this is checked, then when you try to exit if you are connected, the client will pop up a warning to say you are connected. By not having this option checked, the Client will just disconnect and close without warning.
- **CPU Saver** – This is only really useful if your client has an incredibly fast connection (10 Mbit/sec or more). The higher this option, the less frequent the client updates the statistics at the bottom of the screen, and therefore the less CPU it takes.
- **Automatic (Show Dialog)** – When uploading or downloading files that already exist, using this setting will automatically choose the best action for you (overwrite, or skip), but will still show you the dialog to confirm.
- **Automatic (Don't show Dialog)** - When uploading or downloading files that already exist, using this setting will automatically choose the best action for you (overwrite, or skip).
- **Always Overwrite if exists** – If you are trying to upload or download a file which already exists, this option will make the client ignore the fact the file exists, and just overwrite what's already there.
- **Always Skip if Exists** - If you are trying to upload or download a file which already exists, this option will make the client skip this file regardless of what the file sizes are.
- **Ascii Type Files** – This list is used to tell the client which types of files should be sent in ASCII mode. Text files with line feeds are usually sent in ASCII mode, otherwise they might not be recognised on the remote side. All other files including pictures, applications, archives, audio and video should be sent in binary mode. It is ONLY necessary to list files which are definitely text files. To add more ASCII file types here, type in the extension and click the + button. To remove ASCII file types, just highlight the one you want to remove and press the DEL key.
- **Auto** – Make the client automatically choose whether the file to download/upload should be transferred in binary or ASCII mode. In auto mode it will use the list above for ASCII files, and Binary mode for everything else.

- **Binary** – Make the client transfer all files in Binary mode, regardless of what their file extension is. You may experience corruption by using this option.
- **ASCII** – Make the client transfer all files in ASCII mode, regardless of what their file extension is. You will most likely experience corruption by using this option.

Visual Settings

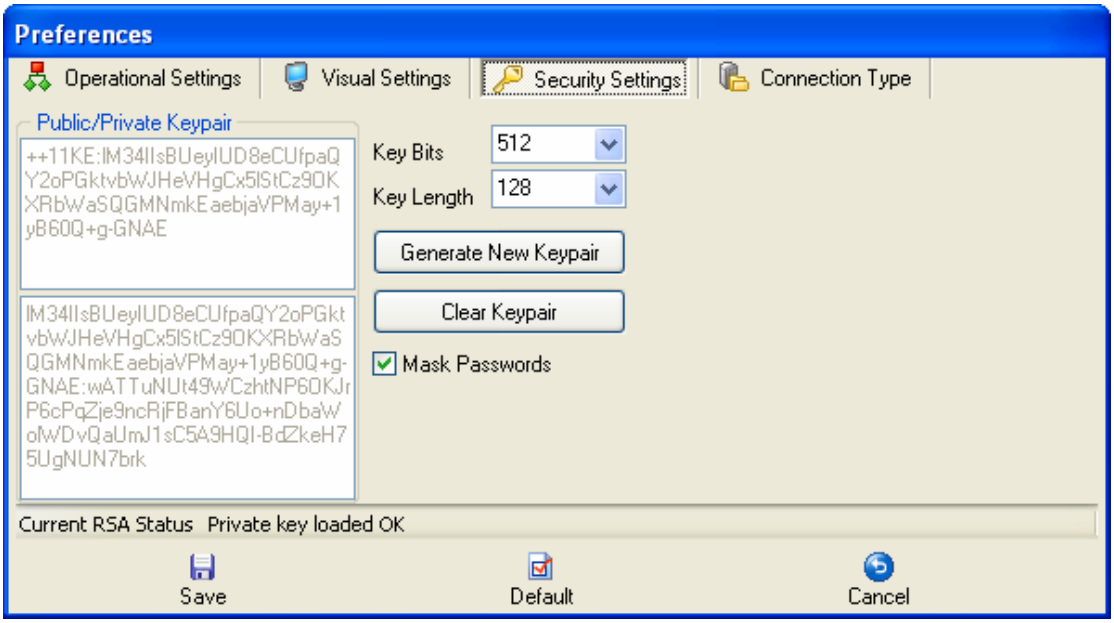


There are presently the following visual settings available.

- **Display Bytes** – since the remote view shows all files as bytes, I thought it would be nice to do the same for the explorer view too. Setting this option will display the number of bytes of a file, instead of the default Kb, Mb or Gb that Explorer shows. How nice it would be to have this option in the real Windows Explorer.
- **Remember Window State on launch** this will make the program remember the window size, location and state (normal or maximized) so that when you start it again, it will be where it was last time.
- **Use Colours for Secure/Unsecure connection** - for those people who would like to see whether or not their connection is secure or not, this option will make the remote view window change colour depending on the connection type. A light red background means that it is an UNSECURE connection, whereas a green background means it is a SECURE (encrypted) connection. A white background means that the site is set for unencrypted mode. (Using a proxy server will automatically set the site to be unencrypted)
- **Display Tree** - if you don't want the tree view on the Local View, you can turn it off here. Most FTP applications don't use this anyway, but some people prefer to navigate using the tree view instead of the list view.
- **Always Resize windows proportionally** – Whenever you resize the client window, this option (if checked) will resize the local view, remove view, log and queue proportionally for better viewing pleasure.
- **Minimize to System Tray** – This will create an icon in the System tray when you minimize the application.
- **Hide from Taskbar** – This must be used in conjunction with the Minimize to System Tray. When checked, this will also remove the application from the main taskbar, so it is only accessible from the system tray.
- **Save Logs** – This setting will save the log every 10 minutes, as well as closing the application down.

- **Save As TXT** – this will save the log as a plain text file, viewable in NOTEPAD or similar program. If the log file already exists, the log will be appended to the existing file.
- **Save As RTF** – this will save the log as a RTF (Rich Text Format). The file is viewable in applications such as Microsoft Word. NOTE: Using this option will overwrite any files that exist. To avoid this, use the **Add Time Stamp to file Name** option.
- **Log File Name** – With this you can specify the name of the log file. If this is blank, the logs will be saved in the same directory as the Client is running from (unless you have specified a different directory using the /c switch)
- **Timestamp Log** - this will add the timestamp to the log view and log files.
- **Add Time Stamp to file Name** – This will add a timestamp to the log file name. The timestamp will be that of the date and time of when the log was started – i.e. when the application started. Using this option is the safest way to ensure you have kept log files from previous sessions
- **Delete Log Files Older than** – Of course, log files can get plentiful, depending on how many times you run the client. The application can be set to delete log files that are older than a specified number of days using this option. NOTE: If you change the location of your log files, or naming convention thereof, then older log files that do not match the new naming convention will not be deleted.
- **Display CLI (Command Line Interface)** – The CLI is where users can type in commands to send directly to the server. This is usually only used in conjunction with Scripting support (described later). Not all FTP commands are presently supported. If there is a command that you wish to have included here, please post an enhancement request on the forum.

Security Settings



When you install EFTP3 for the first time, you will not have a public/private keypair. One of the first tasks you should do is CREATE a keypair. This is required in order to establish both types of encryption, because the 2nd type of encryption will only get negotiated if the first type of encryption is working. The default of 512 Bits and length of 64 is sufficient. The larger your Key length and the more bits you ask for, the longer it will take to decrypt the commands and replies from client to server.

It is never necessary to tell anybody what this keypair is. The client will automatically tell the server what its public key is, and the private key is never revealed. It's only really displayed here because it makes it look cool, and also you can see the keys change when you re-generate new keys. When generating new keys, the application will seem like it has hung, but if you watch the Current RSA Status panel, you will see it change as the lengthy process of generating a new keypair progresses.

You are not able to generate a new keypair if you are connected to a server in encrypted mode, and you are also not

Key Generation:

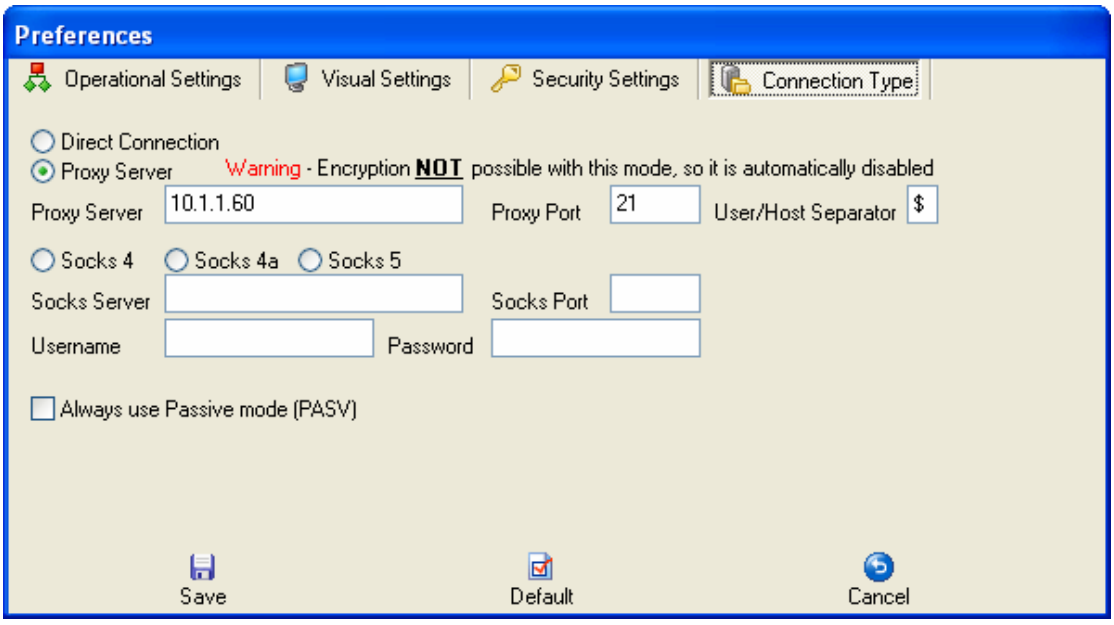
- **Key Bits** – Defines the number of bits to be used in the RSA calculation.
- **Key Length** - Defines the length of the encryption of the Symmetric Key
- **Generate New Keypair** - Creates a public/private key pair of the length defined by the Key Length.
- **Clear Keypair** – destroy the keypair displayed on the left. It is not necessary to clear the keypair to generate a new one. It is not advised to ever clear the keypair.

NOTE: Keys on Client and Sever **DO NOT** have to be the same, and it is advised never to give out your private key.

Other options:

- **Mask Passwords** - the log file and Site Manager will always show the password in clear text. If you wish, you can mask the password so that the password is not visible.

Connection Type



In most organizations, it is customary to have a firewall and a proxy server, and outgoing traffic is usually blocked for security reasons. Fortunately, EFTP is able to utilize two of the most common access gateways for such scenarios.

- **Direct Connection** – The Client will attempt to connect direct to the IP Address specified in the site manager. This is the preferred method of connection. With

this method, you are able to utilize all of the features of the client, including encryption.

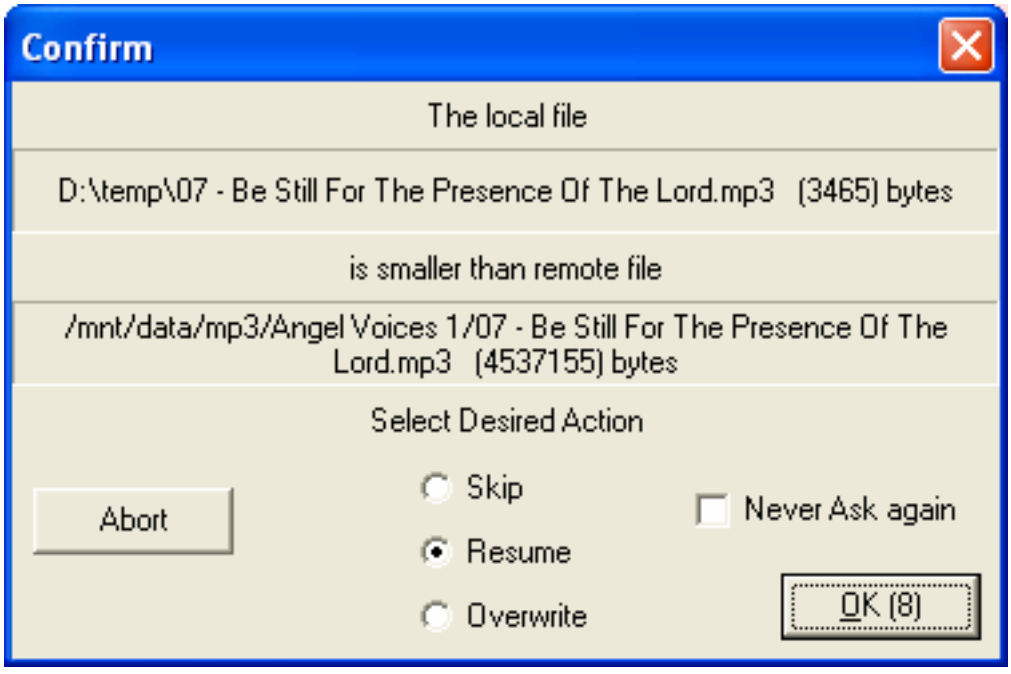
- **Proxy Server** – The client will attempt to connect to the Proxy server specified in the Proxy Server settings, and then via this proxy will attempt to connect to the external site. With this setting, the client will act slightly differently. When it receives a ready prompt, it will then specify the user as username@hostname. Some proxy servers (like BorderManager) require a $ to separate the user & hostname, whereas others use an @ sign. *NOTE:* Because Proxy servers basically act on your behalf, they do not support encryption and therefore your client cannot support encryption. Any connections made using this method will automatically make your client not attempt to use encryption, and also will use Passive mode.
- **Socks Server** - With this set, the client will connect to the socks server, and then from there make a direct connection to the remote server. Using this option will allow your client to use encryption.
- **Always Use Passive Mode (PASV)** - If you are behind a NAT connection, then you will always need to use Passive mode to connect to a server. Instead of having to remember to set Passive mode on each site when you manage your sites, you can set a permanent Passive mode connection here.

Transfer Queue

Unfortunately, it is not possible to browse the server while files are transferring (unless you cache the whole site first which is not yet supported), so what we do is put all the file transfers into a queue, and then download/upload the lot at the end. This button needs to be pressed in order for the transfer to commence.

During the transfer, you can press this button again to abort the current transfer, in case you need to make any changes to the queue.

Depending on the type of transfer you are about to do, the client will either perform the transfer, or prompt you to ask what you would like to have done, by presenting a screen similar to this



Basically, this will automatically choose the best option for you, and when the counter on the OK button reaches 0, it will choose the best option. For a download, if the local file smaller, then it will presume to **Resume**. If the local file is the same size as the remote

file, then it will choose **Skip**. If the local file is larger than the remote file, then it will also **Skip**. For an upload, if the local file is larger than the remote file, then it will select **Resume**. If the local file is smaller or the same size as the remote, it will choose **Skip**. Manual intervention is required if you wish to **Overwrite**.

If you wish to abort the current transfer, click the **Abort** button. This will return the file to an *On Queue* state, and stop processing the queue. This is here just in case you need to review the queue.

Additionally, you can make this box never appear again by selecting **Never Ask again**. With this box checked, the client will always use the automatic choice it made. To get this dialog box to come back, you can use the option **Automatic (Show Dialog)** in the Operational Preferences.

Connection Information

The connection information only shows you that you are connected. It shows you the site name, the host address and the port number. It doesn't really do anything else.

Log Window

Based on your preferences, this log file could get quite big or remain small. This is where messages from servers will appear, and also confirmations of uploads and downloads.

Client Reset

If your client is not operating correctly, you can click this button, and the client will reset itself. You can also use this button to cancel an operation, for example, if you are attempting to connect to a server and you realise you typed the name in wrong, then you can use this button to cancel instead of waiting for Winsock to timeout.

FTP State

It shows the FTP Client's current state. It's there for debugging purposes only.

Up One Dir

Use this button to go up one directory either on the remote view or local view.

Refresh

To refresh the remote view (perhaps a new file has been put there), press this button.

Home Dir

Use this button to return to your home directory, or the directory you have specified as your remote directory on connect.

Local View

The local view acts and behaves just like the Windows Explorer does. This also means that all commands you would be able to do in Explorer (right click context menus, etc), are applicable. You are not able to use the tree view to drag and drop directories to the queue or to the remote view. Use the list view to select the files you wish to upload, and drag and drop to the queue or remote view.

Remote View

The remote view is basically the information from the remote server. Directories will have a folder icon, and files will have a file icon. Double-click folders to change into those directories (assuming you have permission). If you wish to download anything, you can select the directories/files and then drag and drop your selection onto either the queue or the listview portion of the local view. When you drag and drop these files, the local directory will be the one displayed at the bottom of the local listview window (in our figure above, it is X:\Documents and Settings\Atreyu\Desktop).

Additionally, if you wish to upload files, select them using the listview on the local view, and drag and drop them on the queue or the remote view.

You can also delete files and subdirectories by highlighting them and pressing the DELETE button, which will add the deletions to the queue.

Use the Up one directory icon to send a CDUP to the server. If you wish to change directories manually (like perhaps to another drive or location), double-click the current directory above the list view and providing the client is ready, you will be prompted for a new location. The FTP Client also keeps a record of where you've been, so that you can easily change back to a directory at a higher level instead of doing many CDUP's. The directory locator is a drop down box, so you can use this drop down box to navigate back up to root if you want to. This information is not written anywhere, so when you log off, it will disappear.

CLI (Command Line Interface)

This will be rarely used. If you however wish to type in a command directly to send to the server, use this. The CLI will primarily be used for scripting support.

Queue

The queue holds a list of files that are waiting to be uploaded, downloaded or deleted. The status can be one of the following

- *On Queue* – the file or directory is waiting to be processed
- *Transferring* – the file is presently being transferred
- *Processing* – the directory or its contents is being processed
- *Failed* – the file or directory has failed to process. Check the log for details.
- *Completed* – the file has completed uploading/downloading
- *Processed* – the directory has been completely processed
- *Deleted* – the file/directory has been successfully deleted.

You are also able to move around items in the queue, to select which files are done first. You cannot move the item that is being processed.

To delete queue items, select the items you wish to delete, and then hit the Del key. This window also has a pop-up menu when you click the right mouse button.

Status Indicator

When transferring files, this indicator will show you statistical information on the current operation.

FTP Server

The FTP server is presently fixed at a maximum of 100 users. Although most FTP servers should be able to handle more, this has been fixed so that not too much load can be put on the machine that will be running the server. The RSA encryption adds a considerable amount of processes, and it would not be ideal to have more than 100 all doing encrypted commands. Fortunately, the blowfish encryption for the data requires hardly any processor power.

The FTP Server is broken up into 4 main sections, each one to be covered in their own section. To switch from section to section, use the appropriate tab below the toolbar.

The toolbar itself contains 2 buttons, a section to select the listening IP, a section for modifying the server port and a section for modifying the maximum connected users.

The left most button is the server stop/start button. Use this to turn your server on or off. IMPORTANT NOTE: Stopping your server just stops people from logging in. Currently connected people will **NOT** be kicked off. If you need to kick all users, use the Kick button instead.

The Sad face icon is really the Kick button. Use this to kick everybody off your server.

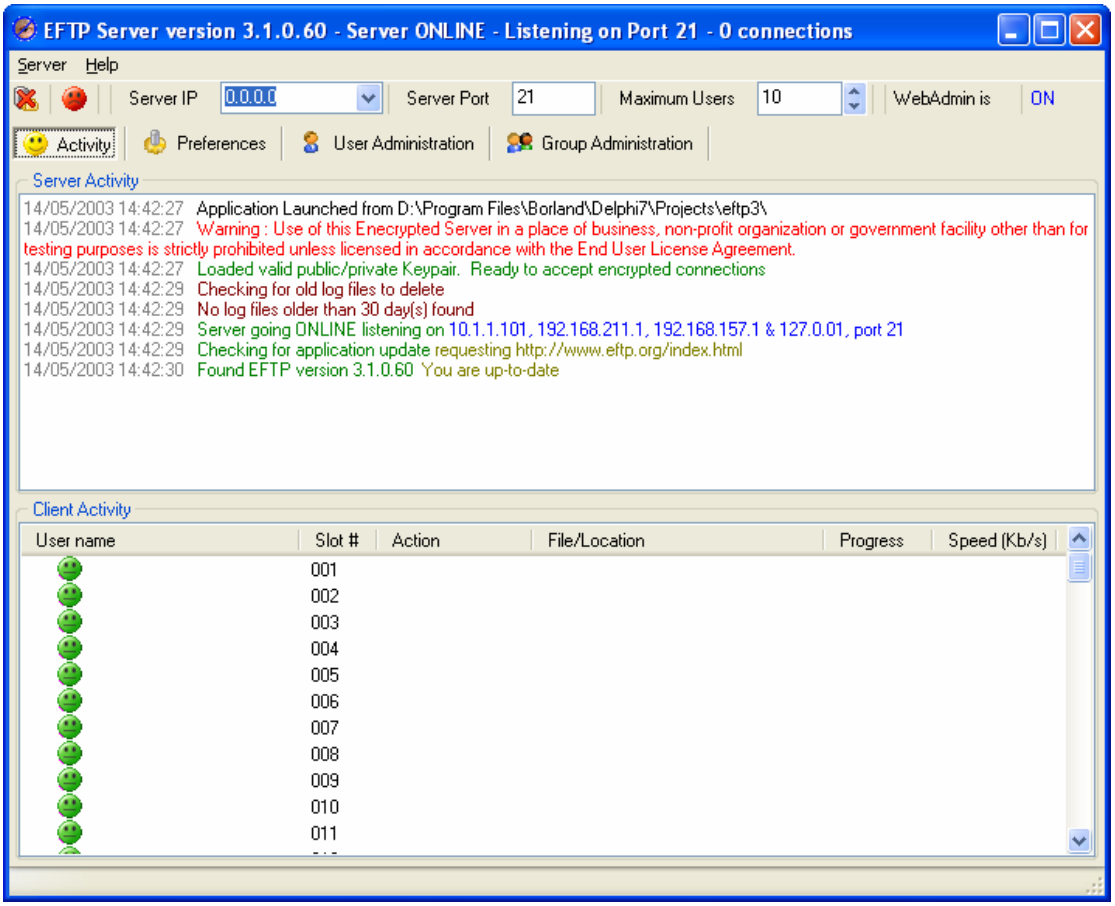
The Server IP list will all the available IP's on your system, as well as 0.0.0.0 (which means to listen on all). For multi-homed servers, this can be a useful option so that only one interface is used for FTP.

The port number you can change anytime, but will only be effective if you restart or start the server. The right-most button is the kick button.

To limit the users to less than 100, change the value to the right of **Maximum Users**.

WebAdmin status – this will show as ON if the WebAdmin portion is listening, or OFF if the WebAdmin portion is not listening. To make WebAdmin start, you can use the Menu, or press F12.

Activity

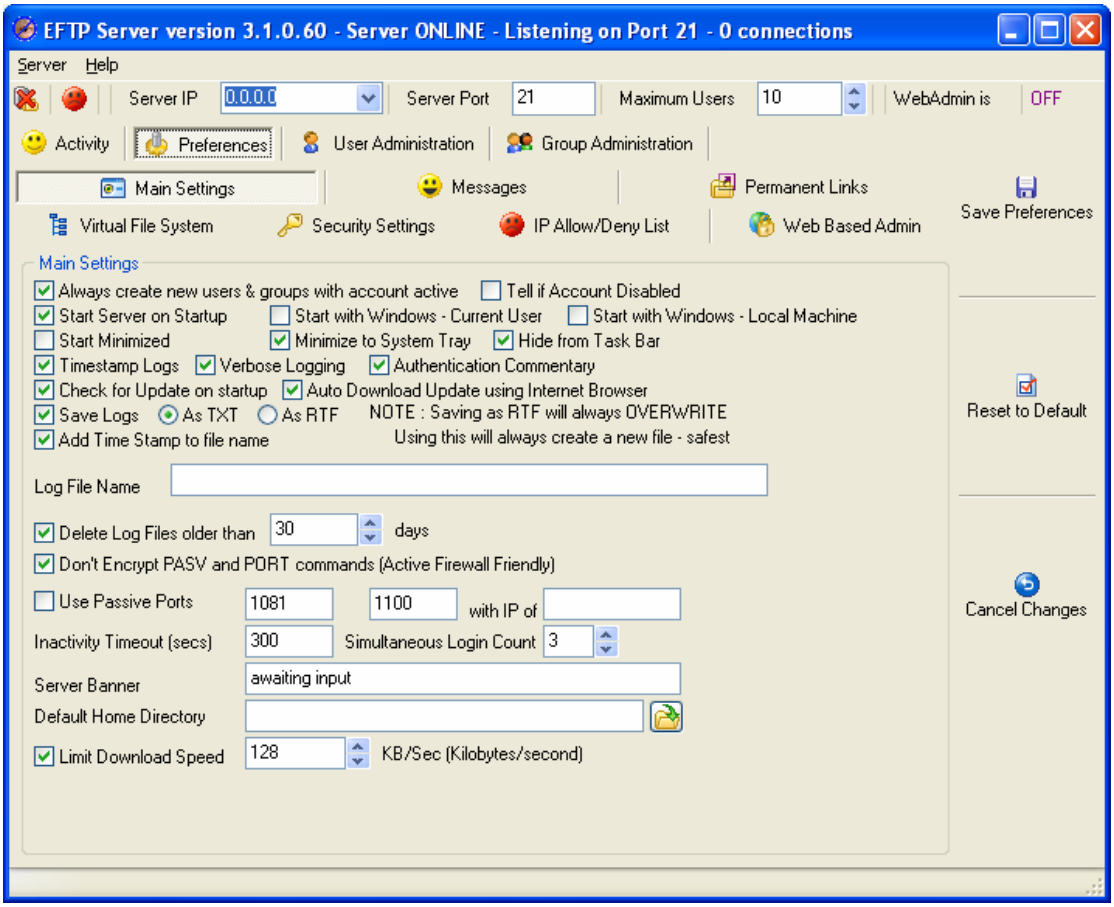


The activity screen basically shows all activity from clients to your server. The top window is the log which is real-time activity, and the bottom screen shows individual user activity. All 100 slots are shown, and slots get filled from the top down, so it is easier to manage. The user name indicates the name of the user that is connected. A padlock icon will appear next to the face. The locked (green) padlock means the user is in secure mode (encryption OK), and the unlocked (red) padlock means the user is connected in unsecure mode (no encryption). The Action shows the last or current action taken by the user. The File/Location shows the file the user is currently uploading or downloading, or the directory that the user is in. Progress will show the speed or success/failure of a command. The speed will calculate the speed where appropriate. NOTE – Speed is always shown as an aggregate of an entire session, and not current speed.

Preferences

Due to the multitude of options available, the preferences are split into different sections, all available on different pages. You also have 3 buttons in the right hand section. Save Options will save the options immediately, although the options would save automatically when you close the application anyway. Cancel Changes will revert back to the last saved changes state (if any), or the options when the application started. Reset to Default would reset all the options to default (all except the public/private keypair).

Main Settings

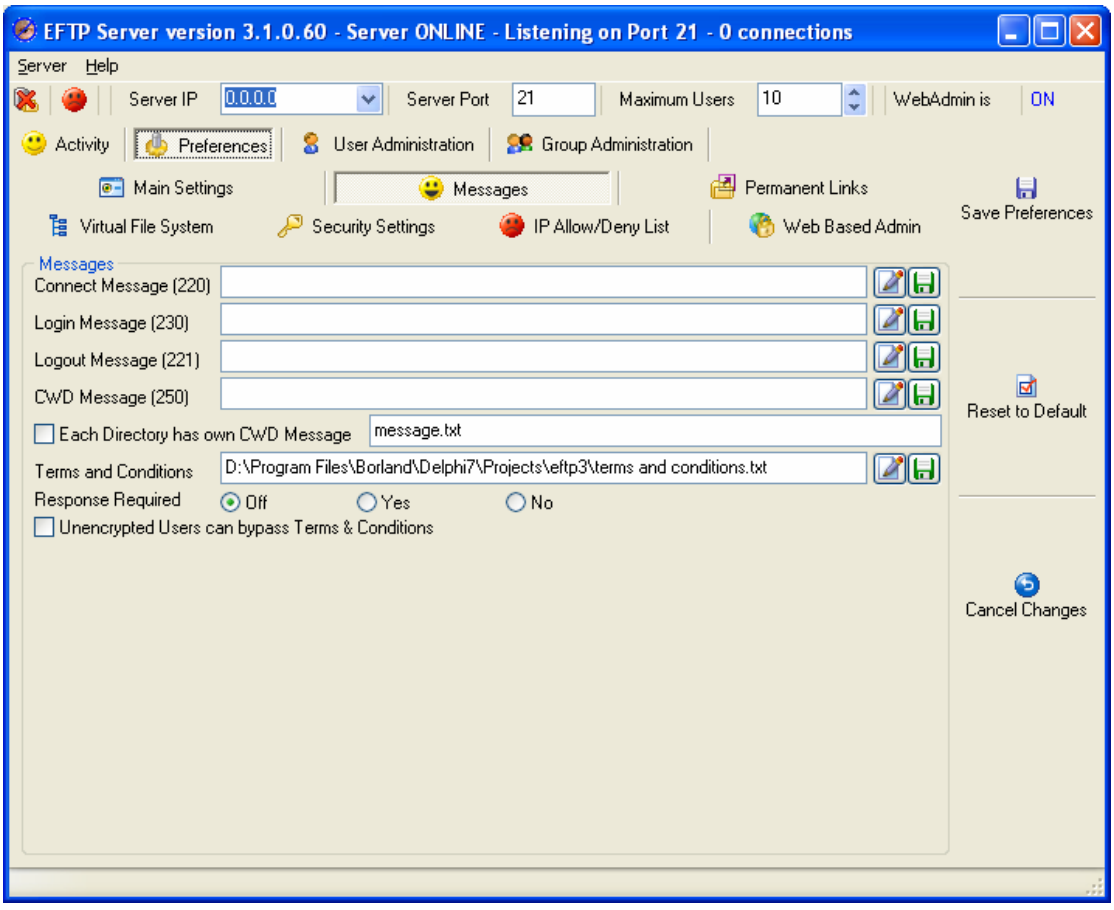


- **Always create new users & groups with account active** - when you create new users and groups, their status of being "active" will depend on whether or not this button has been checked. By default it is off, but some people like their new users and groups to work immediately.
- **Tell if Account Disabled** - usually when people connect and their account is disabled, they are never actually told this. I find that they just end up trying again and trying again, assuming that your server is full. With this option, the server will blatantly tell the client that their account is disabled, and they might stop trying to get in.
- **Start Server on Startup** - standard option really. When you start the program, the server portion will start automatically. NOTE: If you already have a server running, you will get an error message on the screen even before the server window shows. Just OK this error message. You cannot have more than 1 server listening on the same port.
- **Start with Windows - Current User** – will add an entry to the registry of the current user that will make EFTP3 Server run as soon as the user logs in. This will only be effective for the current user that is logged in.
- **Start with Windows - Local Machine** - will add an entry to the registry of the computer that will make EFTP3 Server run as soon as the user logs in. This will affect all users that does a local log in to the computer.
- **Start minimized** – will minimize the application one second after it has completed launching
- **Minimize to System Tray** – used in conjunction with the Start minimized option, will create an icon in the bottom right window next to your clock and other tray icons. This icon will change colour depending on whether the server is active, inactive or has users connected.

- **Hide from Taskbar** – also used in conjunction with the Start minimized option and Minimize to system tray icon, will remove the icon from the main taskbar when minimizing to system tray. This is the default behaviour of most applications, but with EFTP you get the extended choice.
- **Timestamp logs** - checking this box will timestamp all the events that happen on the server. This can be useful in keeping records of all transactions that took place, and when they took place.
- **Verbose Logging** – this will add every single communication the client makes to the server. This is useful in trying to determine problems (should there be any). Verbose logging could also mean that your log files get fairly large.
- **Authentication Commentary** – when users fail to log in, administrators do not always necessarily know why it failed. Having the authentication commentary on will give more detailed information as to the authentication process the client is going through, and will advise the reason for failure.
- **Check for Update on Startup** – Having this option checked will make EFTP get the file http://www.eftp.org/index.html, which contains information about the latest version of EFTP. It will then display on the log view, whether or not you have the latest version or if there is a new one to download
- **Auto Download Update using Internet Browser** – Having this checked will use your Internet browser to download the latest version of EFTP, should the check find you or not on the latest version. You will most likely have to intervene at this point to tell your browser where you want the file saved. If you launch the file without saving, then you should close your Client (and Server if applicable) before allowing the installation to continue.
- **Save Logs** – checking this option will make the server save logs every 10 minutes.
- **Save As TXT** – this will save the log as a plain text file, viewable in NOTEPAD or similar program. If the log file already exists, the log will be appended to the existing file.
- **Save As RTF** – this will save the log as a RTF (Rich Text Format). The file is viewable in applications such as Microsoft Word. NOTE: Using this option will overwrite any files that exist. To avoid this, use the **Add Time Stamp to file Name** option.
- **Add Time Stamp to file Name** – This will add a timestamp to the log file name. The timestamp will be that of the date and time of when the log was started – i.e. when the application started. Using this option is the safest way to ensure you have kept log files from previous sessions
- **Log File Name** – With this you can specify the name of the log file. If this is blank, the logs will be saved in the same directory as the Server is running from.
- **Delete Log Files older than xx days** – having this set will make the server delete log files that are older than a specified number of days. NOTE: If you change the location of your log files, or naming convention thereof, then older log files that do not match the new naming convention will not be deleted.
- **Don't Encrypt PASV and PORT commands** – when using an active firewall to do NAT (Network Address Translation), the firewall needs to know which ports to open for the data connections. It monitors FTP traffic and opens ports according to the PASV and PORT replies the server sends to the client. As these commands are usually encrypted, the active firewall will not understand and as a result it will not open the necessary ports. By switching this option on, the server will not encrypt those replies, making the active firewall function properly. There is no security risk with having this option on.
- **Use Passive Ports** – In some circumstances it is required to do manual port forwarding in a NAT environment. This could be because either you don't have an active Firewall with NAT solution or you are using a different port other than 21 for your server (in which case the Active server does not monitor communications). Instead of forwarding all the ports from 1023 >, you can specify which ports you wish to forward. Using this option will allow you to do that. You need to specify the start port and end port (and external IP address as required) BEFORE you click the box to use passive ports.

- **Inactivity Timeout** – Some users will have clients that stay connected after a download completes. To ensure that you do not waste valuable connections, you can have the server kick users off if they have been inactive for a certain amount of time by setting it here.
- **Simultaneous Login Count** – This will allow users to log in with the same account a certain number of times. Usually you would set this to one to ensure that users cannot take advantage of your good bandwidth. This value can be overridden on a user basis. Simultaneous Login Count works only at user level, not IP level. The reason for this is, if several different users are behind the same NAT network, the client IP will appear to be the same on all of them.
- **Server banner** – The default message when users connect to the server – The banner is preceded by 220, so there is no need to add it. You can have anything you want here
- **Default Home Directory** - sometimes you want a specific directory to always be the home directory for all your users. Set this here, and then you don't have to set each individual user's home directories. This will override any group home directories, but the user's home directories will always take precedence.
- **Limit Download Speed** – This is the system-wide speed limit. The server will divide this speed by the amount of users connected and give each user a portion of the speed for their downloading purposes. Eg: If 128 is used and there are 6 users connected, each user will get no more than 21.3 Kb/sec (give or take a few bytes).

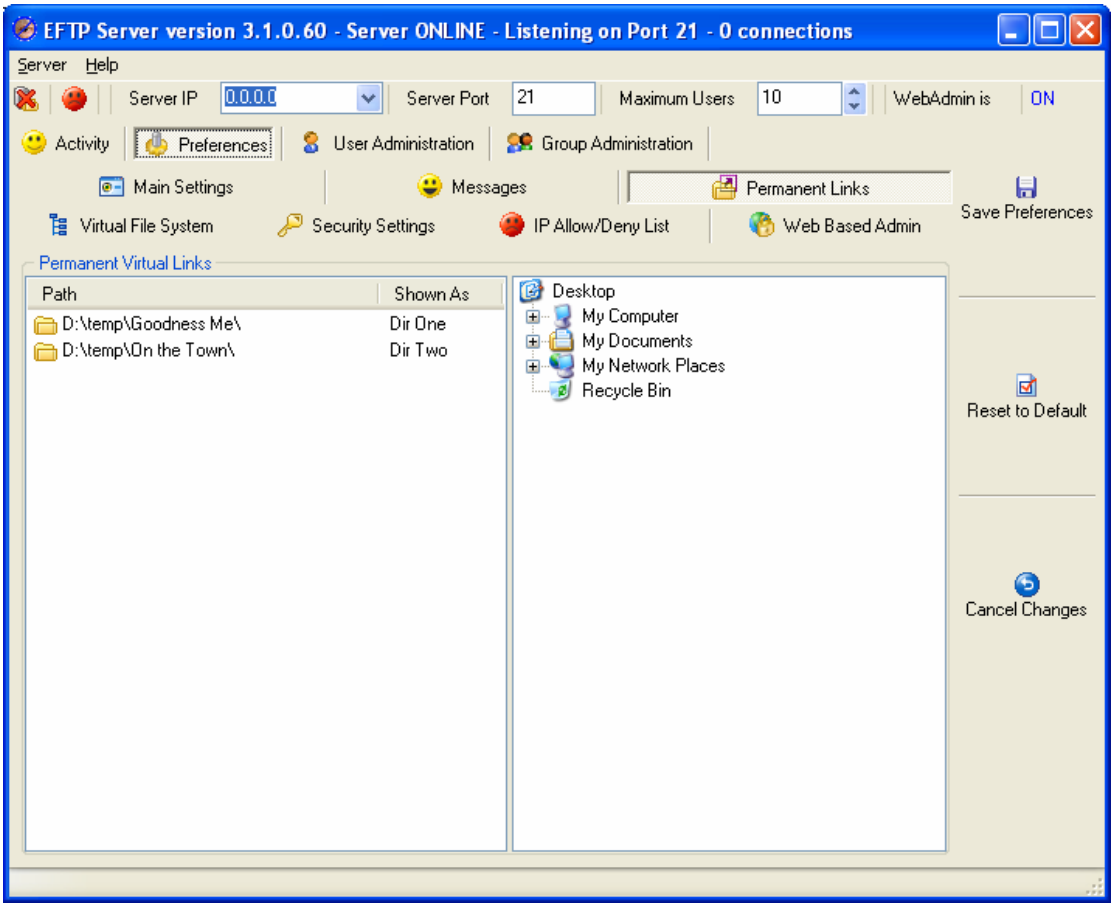
Messages



The server has abilities to send messages during certain operations. Using this page here, you can set these messages for all users that connect.

- **Connect**, **Login**, **Logout & CWD Messages** – these lines here are to define or set text files that contain the login message – they are not to be used for the message themselves. Use the Save icon to locate or define a text file. Use the edit button to edit the text file (using Notepad).
- **Each directory has own CWD Message** - using this option will enable you to define a single filename as a CWD message. If the file exists in the current directory that the user CWD'd to, then it will be displayed instead of the defined CWD message in the field above.
- **Terms and Conditions** – a feature not supported by any other FTP server is a terms and conditions feature. In many countries, it is recognised by law that any electronic agreement is a binding contract between a company and users that connect to its services. By adding a Terms and Conditions feature, you can bind the users by law to conform to the conditions set out as defined in the text file specified. Use the Save icon to locate or define a text file. Use the edit button to edit the text file (using Notepad). Remember to set the appropriate response required. Terms and Conditions will only be negotiated if the clients manage to establish a secure encrypted connection.
- **Response Required**
    - **Off** – the clients do not have to request terms & conditions, and if they do, then the servers tells them that no terms and conditions exist
    - **Yes** – the clients have to request TC's (supported by EFTP client only). The server will allow them to continue authenticating if they answered "Yes" to the terms & conditions.
    - **No** – the clients have to request TC's (supported by EFTP client only). The server will allow them to continue authenticating if they answered "No" to the terms & conditions.
- **Unencrypted Users can bypass Terms & Conditions** – with non-EFTP clients that do not support encryption and this terms & conditions feature, having this checked will make the server ignore the fact that they have not agreed to any terms and conditions.

Permanent Links

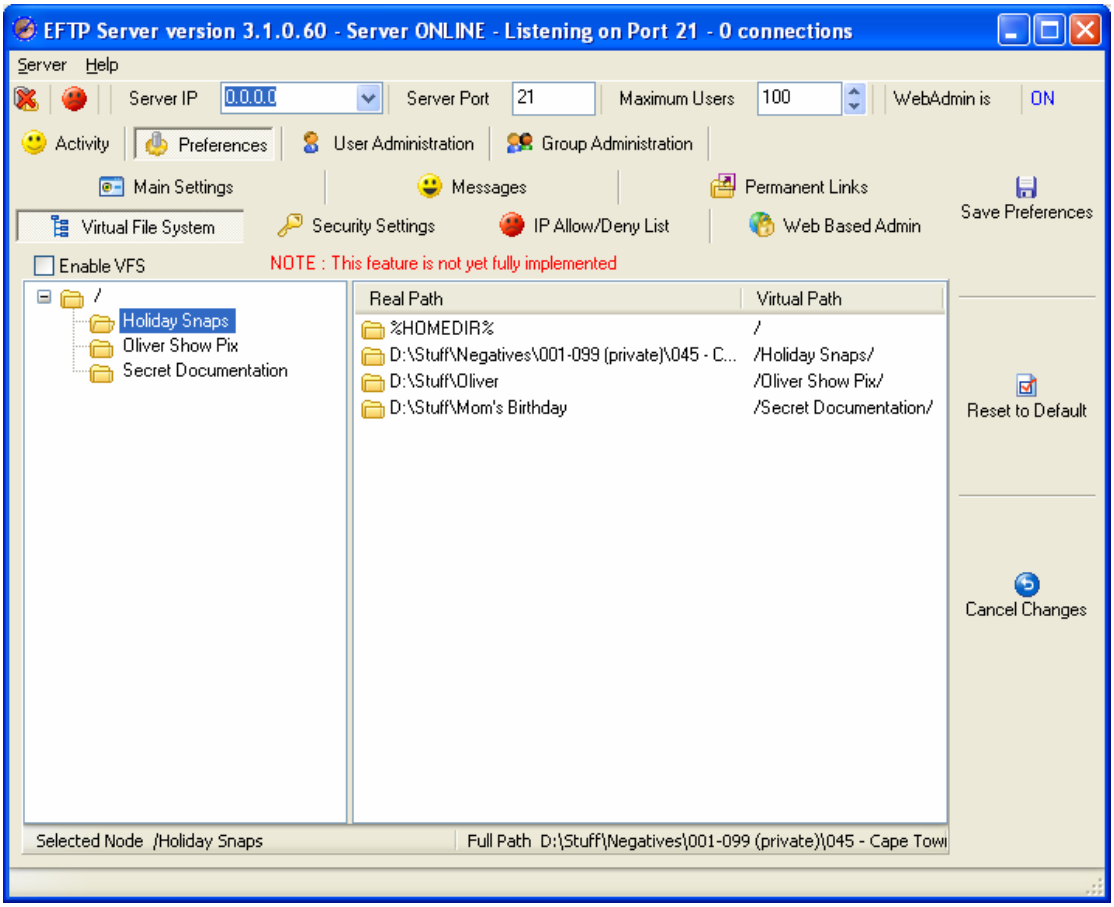


If you have different resources scattered across several mapped or hard drives, it can be quite a nightmare to present everything to your users in a easy manner – hence the purpose of permalinks. Permalinks will appear for users who have LIST access to the destination directory, and will appear in every directory listing they perform. So, regardless of where they brows to, they will always be presented with a link of your choice.

To create a permalink, locate the destination directory on the right, and drag and drop it to the left. You will then be prompted to give it a name. The name that you give it will be the link that is displayed in all directory listings.

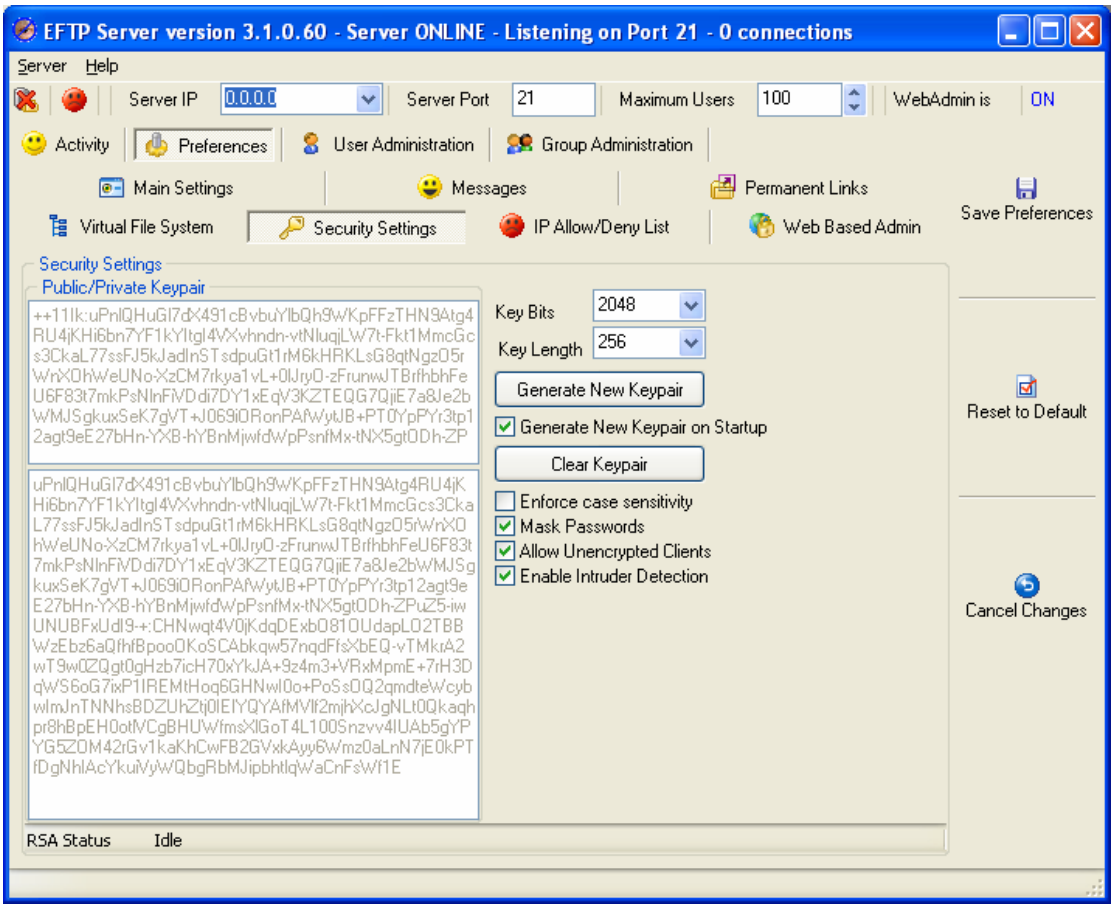
NOTE: Popular web browsers do NOT support symbolic links.

Virtual File System



Work in progress – not a feature that exists yet.

Security Settings



The server requires a public/private keypair for functioning with encryption. One of the first tasks you should do is Generate a new public and private keypair. The default of 512 Bits and length of 64 is sufficient. The larger your Key length and the more bits you ask for, the longer it will take to decrypt those messages. For a highly used server (between 50-100 users), you should keep the key length and key bits low.

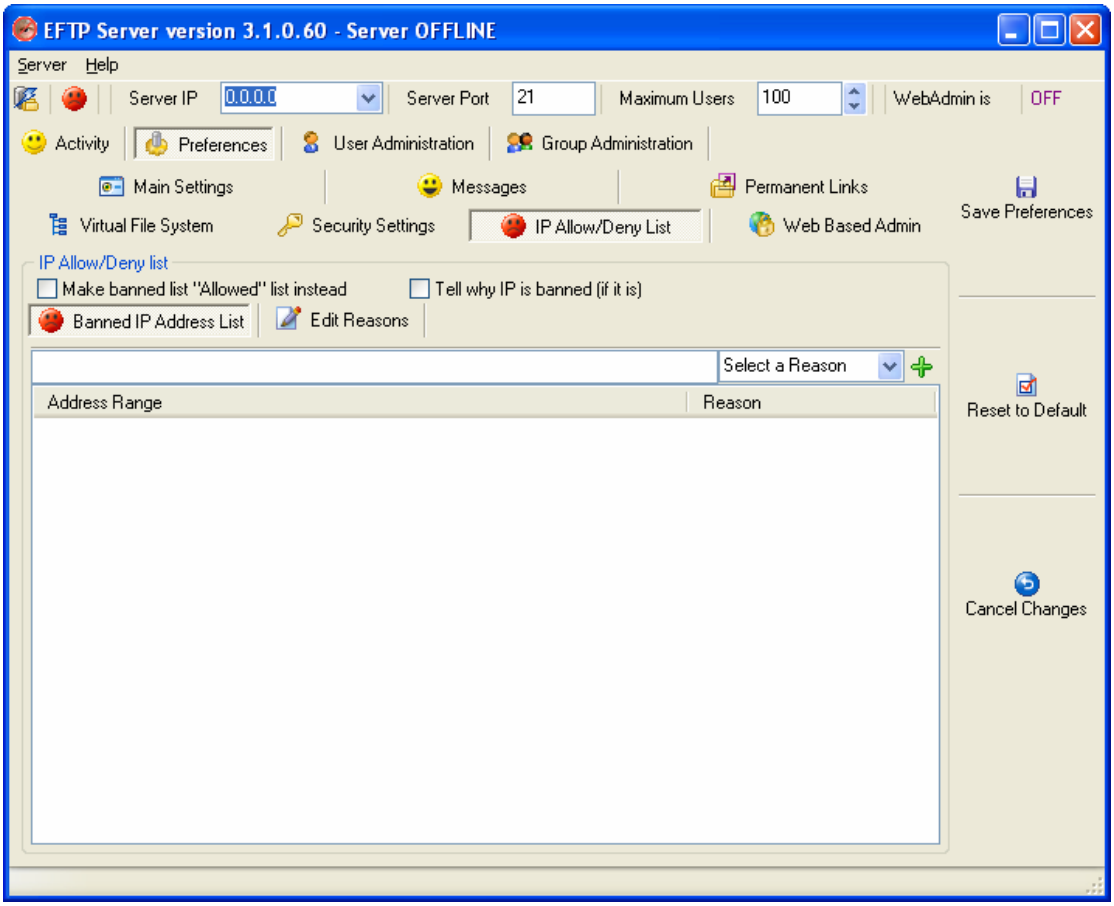
It is never necessary to tell anybody what this keypair is. The server will automatically tell the client what its public key is (after the client has told the server first), and the private key is never revealed. When generating new keys, the application will seem like it has hung, but if you watch the Current RSA Status panel, you will see it change as the lengthy process of generating a new keypair progresses.

You are not able to generate a new keypair if you have any clients connected.

- **Key Bits** – Defines the number of bits to be used in the RSA calculation
- **Key Length** - Defines the length of the encryption of the Symmetric Key
- **Generate New Keypair** – This will make the server generate a keypair based on the Key bits and Key length defined.
- **Generate New Keypair on Startup** - Will make the server generate a new keypair when it starts. It is highly advised to have this set on.
- **Enforce Case Sensitivity** - use this if you wish people's username and passwords to be case sensitive. I personally can't see any benefit for this option, but technically speaking, they should be case sensitive anyway.
- **Mask Passwords** - all passwords in the logs and on user administration is displayed in clear text. Setting this option will mask the passwords with the default masking that Windows assigns.

- **Allow Unencrypted Clients** - this will allow people to connect to your server in unencrypted mode. If you prefer to have only encrypted clients use your server, then uncheck this option.
- **Enable Intruder Detection** – The server will count how many times a certain host has a failed authentication. When this count reaches 3, having this option set will add the hosts IP Address to the ban list. The IP Allow/Deny must be set in Deny mode for this to work.

IP Allow/Deny List



This features doubles as a Banned IP List or Allowed IP List. You cannot have both a banned IP list and allowed IP list (as it contradicts each other).

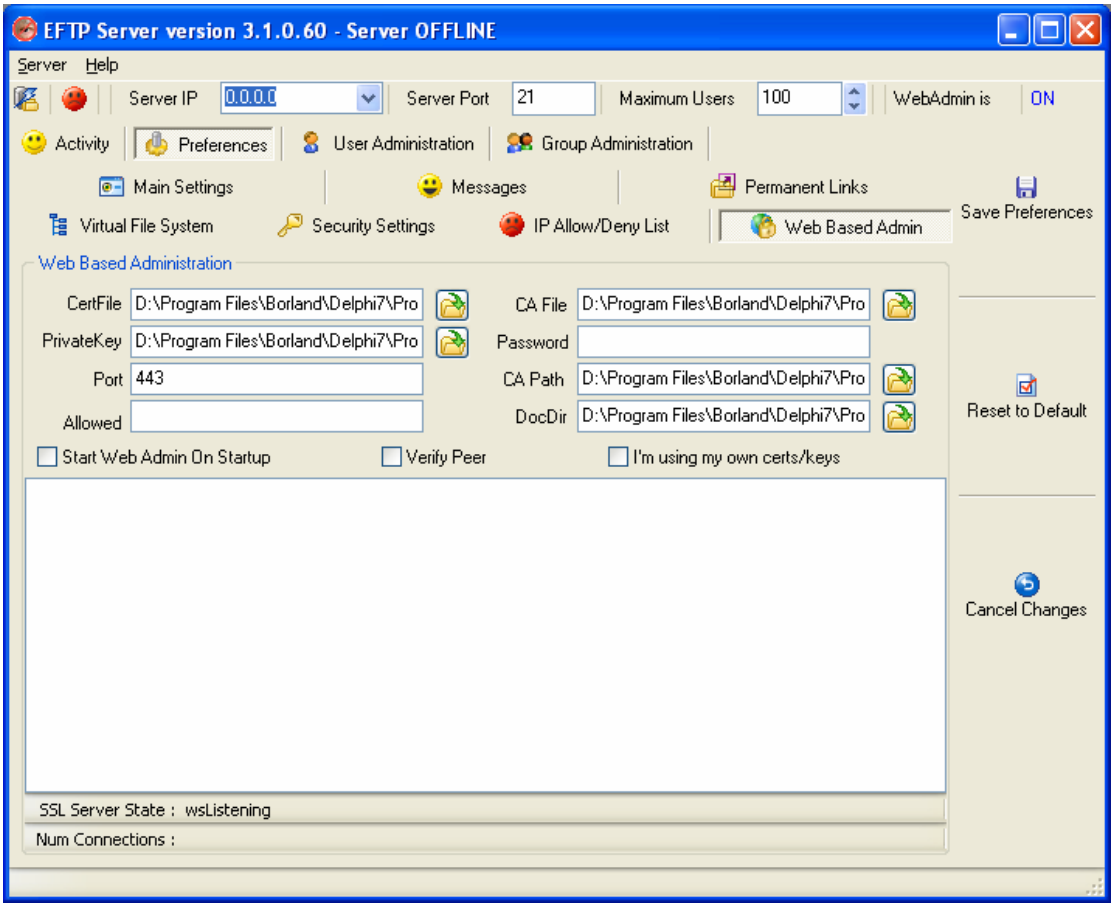
To change the list from Banned to allowed check **Make banned list "Allowed" list instead**.

If you wish to be kind you can even let users know why they are banned by showing them the reason assigned, by checking **Tell why IP is banned (if it is)**.

To add IP Addresses or IP ranges, type in the range in the field at the tip, choose a reason (if you want one) from the drop down list and then click the + button. To remove entries, select them and then press the DEL key.

To edit the reasons list, click on **Edit Reasons** - and you add reasons by entering the reason in the field provided, and then by clicking the + button. The reason is now available to use in the drop down list.

Web Based Admin



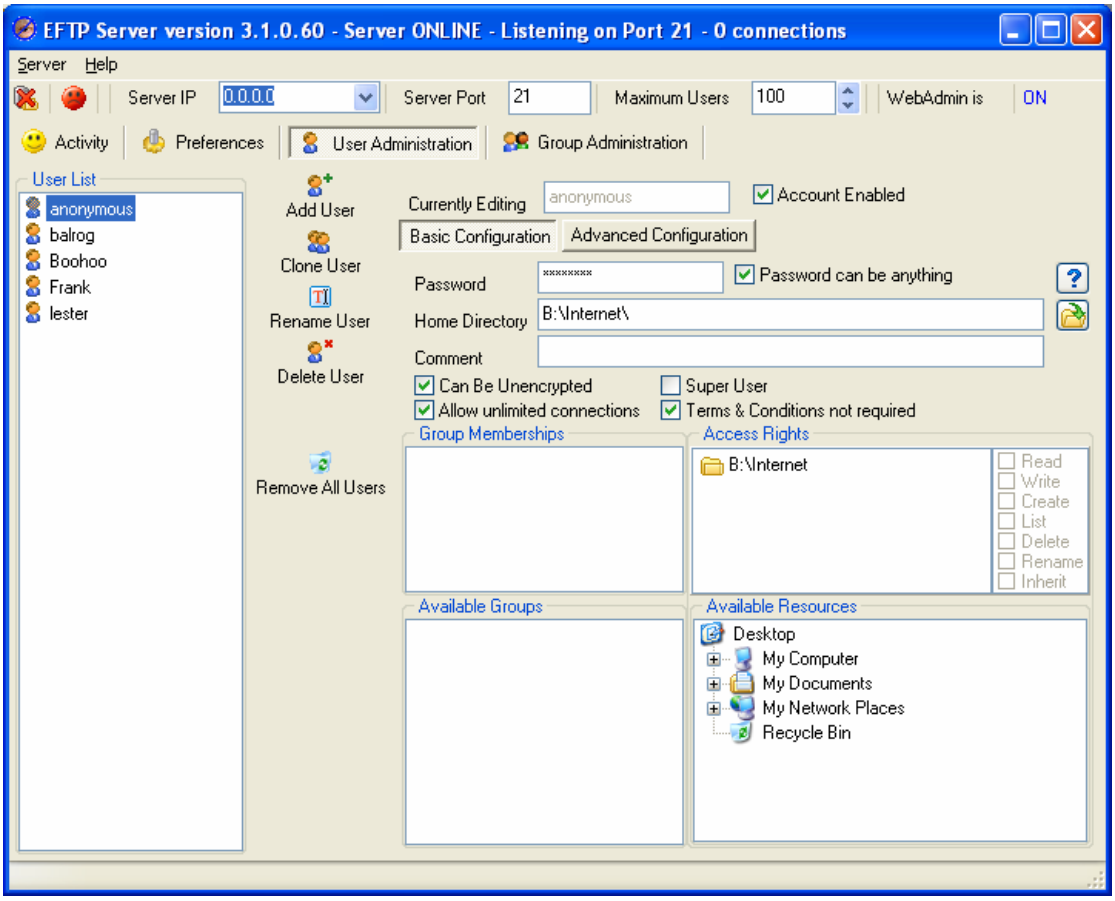
The web administration feature makes use of OpenSSL (http://www.openssl.org). If you are familiar with OpenSSL you are able to assign your own Certificates, Keys and CA File. If your Keys or certificates require a password, enter it in the Password field. If you do not have your own key and cert files, then do no not change any of these fields, apart from the ones listed below. To generate your own key files and cert files, refer to the "Networking Security with OpenSSL", book by O'Reilly pages 59 thru 70: "Setting up a certification authority".

- **Port** - The port for the server admin to listen on. Port 443 is the default SSL port, but you can change this to suit your environment. Remember that many proxy servers have “safe ports” so changing this might make your web admin inaccessible from various locations that use Proxy servers.
- **Allowed** - Add IP addresses or ranges here to specify hosts that are permitted to use this service. If you wish to allow any host, then leave this field blank.
- **Verify Peer** - This will make the server ensure that the client has the correct certificate every time it connects.
- **I’m using my own certs/keys** - Only check this if you have specified your own certificates and keys to use. Until you check this box, the server will always use the standard files supplied with the server for the SSL certificates.

The log window shows in detail the connections made. It is not useful information, but is there for debugging purposes only. The SSL Server State and Num Connections are also informational only.

To connect to the web admin feature, open your browser, and enter the address https://serverip:port/. Where port is the port specified. You can leave out port if you use the default port of 443.

User Administration



Of course, all servers need users. Before I go and explain all the buttons on this page, allow me to assist you in creating a user.

Creating users - a step-by-step instruction

Using our step-by-step guide, we are going to create a user.

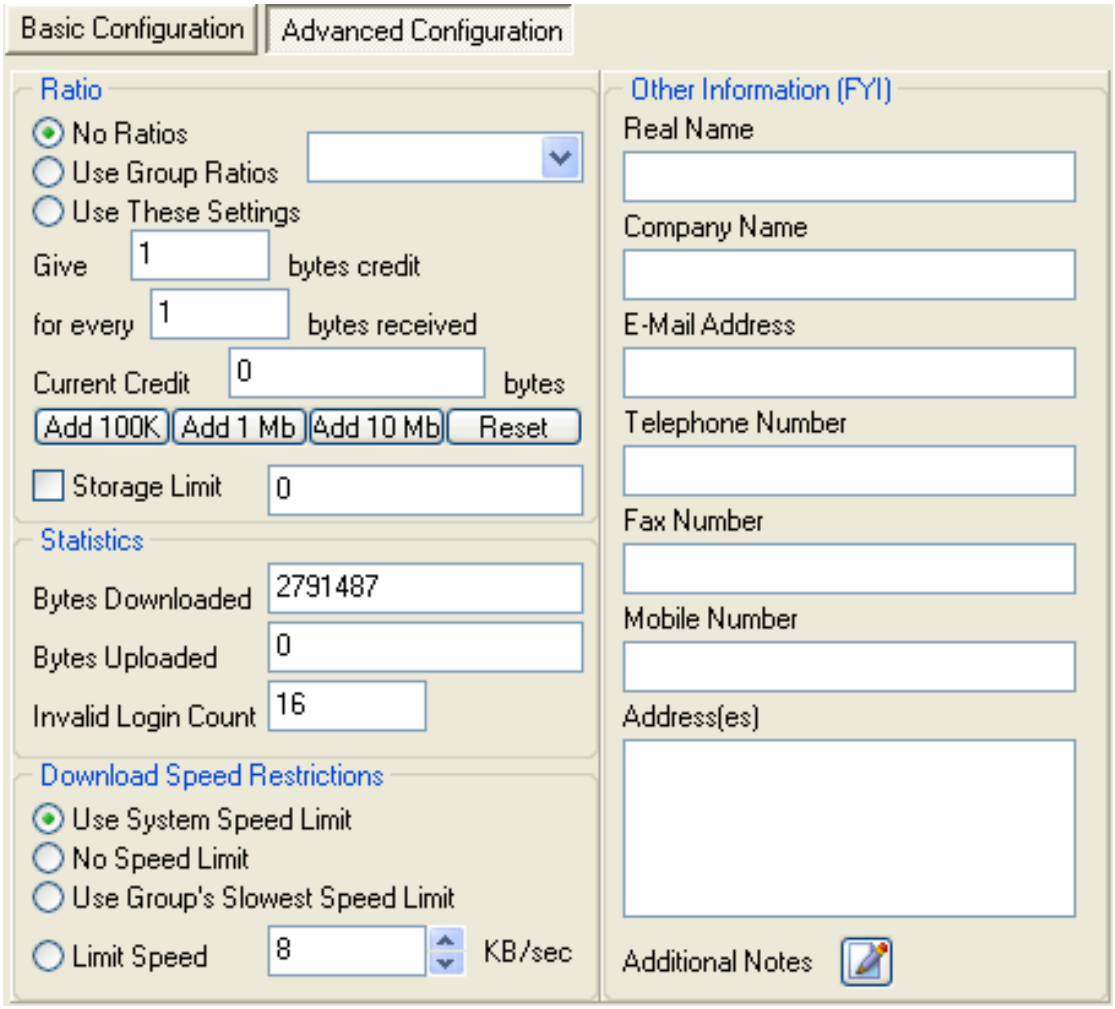
1. Click **Add User**
2. Type in a name. Note: you cannot type in a name that already exists.
3. Your name will appear under the **User List**. Select the name.
4. **Currently Editing** will now show your name.
5. Type in a password in the **Password** field.
6. Drag and drop directories from the **Available Resources** on to **Access Rights**
7. For each item in Access Rights, select the item, and then click the checkboxes **Read**, **List** and **Inherit**
8. Check the **Account Enabled** checkbox.
9. Type in a **Home directory** or alternatively use the open folder dialog to select a home directory.
10. Your user can now log in.

User Administration explained

User information is stored in the file userdata.ini. This is just in case you wish to make a backup of your users.

- **User List** - is a list of all users who are on your system. By clicking any of them on this list, the program will read their information and display it on the right hand pane. Any previous user you were editing is automatically saved.
- **Add user button** – use this to create a new user. You will be prompted for a name. NOTE: you cannot type in a name that already exists. Once you have added the user, you need to select him on the left hand side before you can edit him.
- **Clone user** – if you need to clone a user so that the new user has exactly the same information then use this button. NOTE: You have to have the original user highlighted first.
- **Rename User** – click this if you need to change the login name for the user. Have the user you wish to rename selected first.
- **Delete User** – click to delete the user from your system.
- **Currently Editing** – this shows who you are editing. You cannot rename the user here.
- **Account Enabled** – this button needs to be checked in order for the user to be able to log in.
- **Basic Configuration**
    - **Password** – the password you wish the user to use.
    - **Password can be anything** – regardless of what the users puts in as a password, they will be let in. Suitable only for guest and anonymous logins.
    - **Home Directory** – you can set this to a directory of your choice. If this is blank, then the server will use the default home directory or the first group home directory, and failing that, it will use the first directory in the access list where you have LIST rights to. If all fails, then the user will be denied access.
    - **Comment** – a Single line to be able to make a small comment about the user. This comment is informational only, and does not get shown to the users.
    - **Can be Unencrypted** – If your server is set to only allow encrypted connections (Preferences -> Security -> Allow Unencrypted Clients is Unchecked), then you can allow this account an exception to the rule by checking this option. NOTE: This user specific option will only cancel out the global Security option – it will not enforce encrypted connections, just allow unencrypted connections. To enforce encrypted connections, use the global option instead.
    - **Super User** – if this is checked, then the user has full reign over your entire file system. This option is only really suitable for an administrative login account. This setting is also required if you need to connect to the Web Administration facility.
    - **Allow Unlimited Connections** – This overrides the global setting Preferences -> Main -> Simultaneous Login Count. Most administrators will want users to only be able to log in once. However, this can cause problems for anonymous accounts though, so by having this checked, this user account will be able to log in as many times as the server will permit.
    - **Terms & Conditions not required** – This will effectively set the Terms & Conditions requirement to "Off" for this user account.
    - **Group Memberships** - this is the list of groups that the user is a member of. To add them to a group, just drag and drop the group from the list below to this box.
    - **Available Groups** - a list of all groups on the system.
    - **Access Rights** - this is a list of directories that the user has explicit rights to. To add directories here, use the selector below to drag and drop directories to this window. Each directory has it's own access rights setting. Directories are given the LIST right by default, but you may want to change these rights. See the section below for Access Rights information.

- **Advanced Configuration**



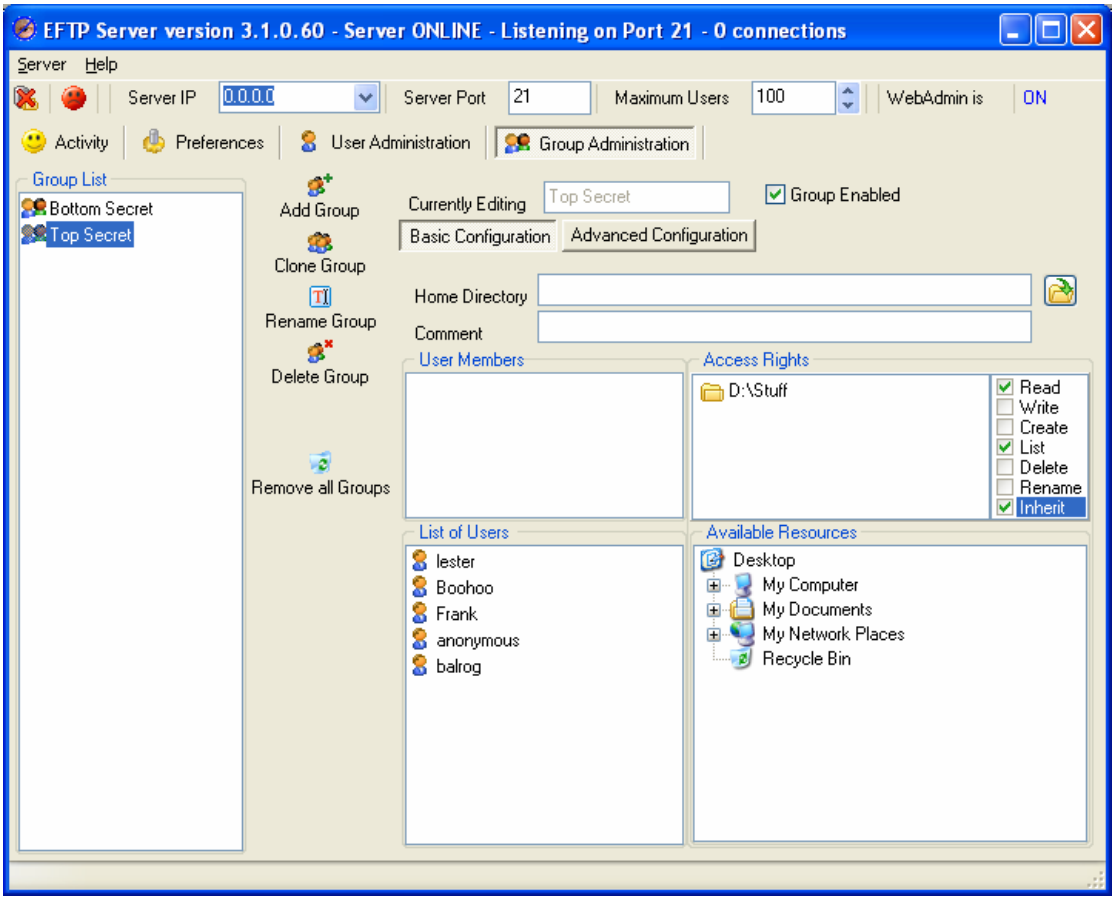
  - **No Ratios** – allow this user to download as much as they want, regardless of how much they upload
  - **Use Group Ratios** – Use the drop down list to choose a group the user is a member of, to give them the ratios assigned to that group.
  - **Use These Settings** – use the settings below
  - **Give _____ bytes credit for every _____ bytes received** - basically, give the users a certain amount of bytes for every amount of bytes they upload. If you wish to make a 2:1 ratio (they give 1 byte you give two back), then specify 2 in the first field and 1 in the second field. For more complicated ratios (like 1.5:1) then do 15 in the first field and 10 in the second.
  - **Current Credit** - this is how much credit the user has built up. You cannot edit this figure, but you can grant him additional credit by clicking the buttons below. Users start with 0 credit when they are first created, but sometimes you wish them to start with a credit so that they are able to sample your wares before uploading similar.
  - **Add 100K** - add 100 Kilobytes of credit for this user.
  - **Add 1 Mb** - adds 1 Megabyte of credit for this user.
  - **Add 10 Mb** - adds 10 Megabytes for this user.
  - **Storage Limit** – specify how much a user can upload. NOTE: Storage space is only checked when users start uploading a file – If the user has more than 0 bytes available to store, then the server will permit the store. However, the user may still upload a single file which is greater than their available storage, as it is not possible to determine how much the user intends to store when they start.

- **Bytes Downloaded** - how much data the user has downloaded on this account.
- **Bytes Uploaded** - how much data the user has uploaded on this account.
- **Invalid Login Count** - how many times an unsuccessful login attempt was attempted with this account.
- **Use System Speed Limit** – Will assign the system speed limit (if any) to this user. The system speed limit is the global speed limit specified in Preferences -> Main Settings -> Limit Download Speed. This is only effective if the global speed limit has been enabled. The speed will be divided by the amount of users connected to the system.
- **No Speed Limit** – Will give the user unlimited download speed (regardless of whether there is a global speed limit or not)
- **Use Group's Slowest Speed Limit** – will limit this user to the lowest speed limit specified in the groups that the user is a member of. For example, Jake is a member of the "Friends" group which has a limit of 32 KB/sec speed. He is also a member of the "Noobs" group which only has a limit of 4 Kb/sec. Jake will effectively get maximum 4 Kb/sec download speed.
- **Limit Speed** – To set your own speed limit, define it here. The Speed is in Kilobytes, not Kilobits. Hint – 256 Kilobits per second = 32 Kilobytes per second.
- **Other Information (FYI)** – This is more for your information only fields where you can add information about the user account. If there is an e-mail address in the e-mail field, you can also right-click that field and select the e-mail option, which will then fire up your default e-mail application.

The user administration is saved every 30 seconds, but is also automatically saved when you either exit the administration, close the application, choose a new user, perform an operation (clone, rename, etc).

NOTE: Any changes made will NOT affect users who are currently logged in – only users who have yet to log in.

Group Administration



To make giving access rights to multiple people easier, we've allowed people to make groups that users can be members of.

Creating groups - a step-by-step instruction

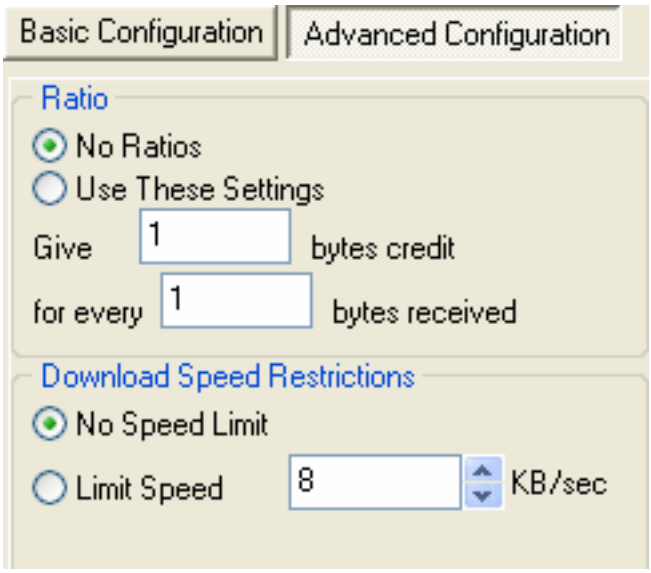
This tutorial will help you create a group using a step-by step approach.
Using our step-by-step guide, we are going to create a user.

1. Click **Add Group**
2. Type in a name. Note: you cannot type in a name that already exists.
3. Your name will appear under the **Group List**. Select the group.
4. **Currently Editing** will now show your group name.
5. Drag and drop directories from the **Available resources** on to **Access Rights**
6. For each item in **Access Rights**, select the item, and then click the checkboxes **Read**, **List** and **Inherit**
7. Check the **Account Enabled** checkbox.
8. Drag and drop the users you wish to be a member of this group from the **List of Users** box into the **User Members**.
9. Those users who are members will now receive all the rights that the group has.

Group Administration explained

Group information is stored in the file groupdata.ini. This is just in case you wish to make a backup of your groups.

- **Group List** - is a list of all groups that are on your system. By clicking any of them on this list, the program will read their information and display it on the right hand pane. Any previous group you were editing is automatically saved.
- **Add Group** – use this to create a new group. You will be prompted for a name. NOTE: you cannot type in a name that already exists. Once you have added the group, you need to select the group on the left hand side before you can edit it.
- **Clone Group** – If you need to clone a group so that the new group has exactly the same information then use this button. NOTE: You have to have the original group highlighted first.
- **Rename Group** – click this if you need to change the group name to a more appropriate name. Have the group you wish to rename selected first.
- **Delete Group** – Click to delete the group from your system.
- **Currently Editing** – this shows the group that you are editing. You cannot rename the group here.
- **Group Enabled** – This button needs to be checked in order for members of this group to receive it's rights.
- **Basic Configuration**
    - **Group Enabled** – You can enable or disable a group membership by easily checking or unchecking this option.
    - **Home Directory** – you can set this to a directory of your choice. User home directories always have preference over this field.
    - **Comment** – You can also add comments for groups.
    - **User Members** - a list of users who are a member of this group
    - **List Of Users** - a list of all users on the system. You can drag and drop users from this list to the list above to make them a member of that group.
    - **Access Rights** - this is a list of directories that the user has explicit rights to. To add directories here, use the selector below to drag and drop directories to this window. Each directory has it's own access rights setting. Directories are given the LIST right by default, but you may want to change these rights. See the section below for Access Rights information.



- **Advanced Configuration**
    - **No Ratios** – no ratios assigned to this group.
    - **Use These Settings** – use the settings below
    - **Give _____ bytes credit for every _____ bytes received** - basically, give the users a certain amount of bytes for every amount of bytes they upload. If you wish to make a 2:1 ratio (they give 1 byte you give two back), then specify 2 in the first field and 1 in the second field. For more complicated ratios (like 1.5:1) then do 15 in the first field and 10 in the second.

- **No Speed Limit** – Assign the group No Speed Limit. NOTE: Users that are a member of this group will always use their own speed limits, and this option effectively has no effect for users.
- **Limit Speed** – Only effective if users use the option "Use Group's Lowest Speed Limit".

The group administration is saved every 30 seconds, but is also automatically saved when you exit the administration, close the application, choose a new group or perform an operation (clone, rename, etc).

NOTE: Any changes made will NOT affect users who are currently logged in – only users who have yet to log in.

Access Rights

There are many access rights that one can assign to directories. They are all listed below with detailed explanations, but first let's learn how this program checks the rights.

When a user logs in, all access rights (up to 128 of them) are stored in a table. The user's access rights are read first, and then the groups in order of the groups they are members of. When you perform an operation where access rights are required (CWD, LIST, DELE, etc), then the application goes through from the top down EVERY access right. If it comes across one which is an explicit right, (i.e. the directory name matches the directory they are in), then it uses those rights and stops checking the rest. If it comes across an inherited right, it will allow access, but continue to check the list for explicit rights. Explicit rights will always override inherited rights. For example, if you had a directory structure like this

- Pictures
  - Celebrities
  - Female Vocalists
  - Male Models
  - Private
  - Sad Faces
  - Teeth

And you wanted to DENY access to the Private subdirectory, then you should create rights to the Pictures directory, and create an explicit right to the Pictures\Private directory with reduced access. Although users should have rights to the Private directory through the inherited parent Pictures, it will use the denied access rights from the explicit right.

The Seven Rights

- **Read** - If you wish users to be able to download files in the directory, then select this on. If users should not be able to download the files in the directory, then leave this unchecked.
- **Write** - this allows users to upload files to the server in the directory selected.
- **Create** - this allows users to create subdirectories in the directory specified.
- **List** - this allows the users the ability to list the directory. This is also required to change into the directory. You would uncheck this right to prohibit directory access like in our example above.
- **Delete** - this will allow users to delete files and subdirectories
- **Rename** - this will allow users to rename files and subdirectories
- **Inherit** - checking this button will make all the rights on this directory flow downwards, and be inherited by all the children. Without this right, users won't be able to change to children directories of the directory you have selected.

Support Options

There are a few support options available to users who have problems.

The point of call should be to check the Forum at http://www.eftp.org/, select the Forum button. Quite often the problem has already been reported, and a fix is available. Always ensure that you are using the latest version of the software before submitting a report.

Any support options where you are required to send personal or confidential information (including log files and INI files), you will be given an e-mail address to send the information to.

For business customers, we endeavour to answer (and fix) your support query within 24 hours. For non business customers (home users), we fix your support query based on a priority system. Security issues have the highest priority, and non-operational annoyances have a lower priority.