



# FileZilla FTP Server

...

Hello again

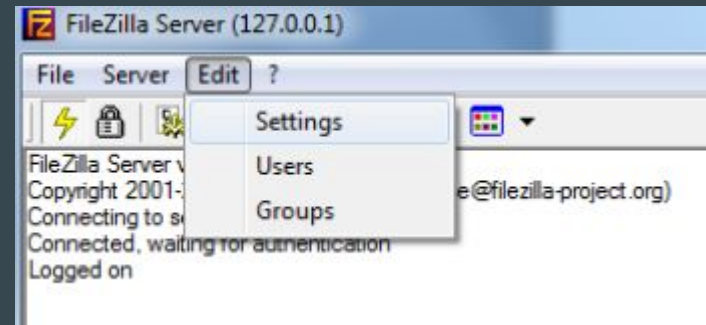
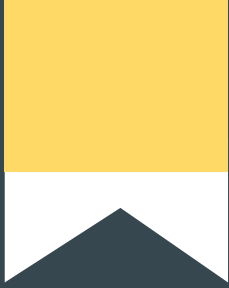
# Basics



# What is it?

---

- Free software, cross-platform FTP application, consisting of FileZilla Client and FileZilla Server.



# Where are the Settings?

- Settings are at Edit > Settings > FileZilla Server Options in FileZilla Server.

# Change Stuff

# Admin Password

- Default- the server admin password is empty, so change it

FileZilla Server Options

Admin Interface settings

Important

Due to security considerations, the admin interface settings can only be changed from local connections. If you aren't connected locally (using 127.0.0.1 as server IP), all changes will be ignored by the server.

Port on which the admin interface should listen: 14147

Bind the admin interface to the following IP addresses:

192.168.1.1

IP Addresses which are allowed to connect to the admin interface:

192.168.0.100|

Use \* to bind to all addresses.  
127.0.0.1 is the default binding, it always exists and cannot be removed.

Localhost is always allowed to connect.  
You can enter additional addresses and ranges using CIDR notation.

☒ Change admin password:

New Password: .....

Retype new Password: .....

Minimum password length is 6 characters. Leave empty to remove password.  
A password is required for remote administration to work.

OK

Cancel

# Welcome Message

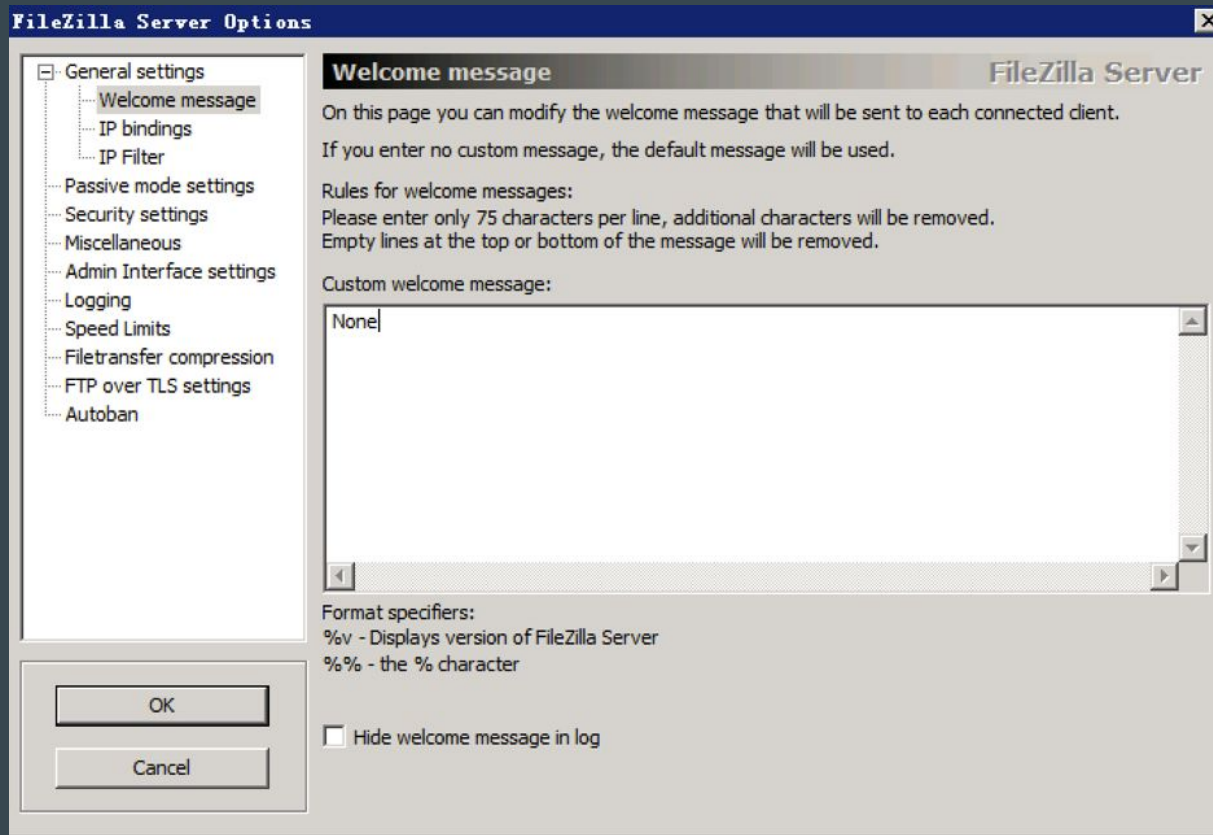
- Default- server version information is displayed in the welcome message when a client accesses an FTP server
  - It is better to hide it

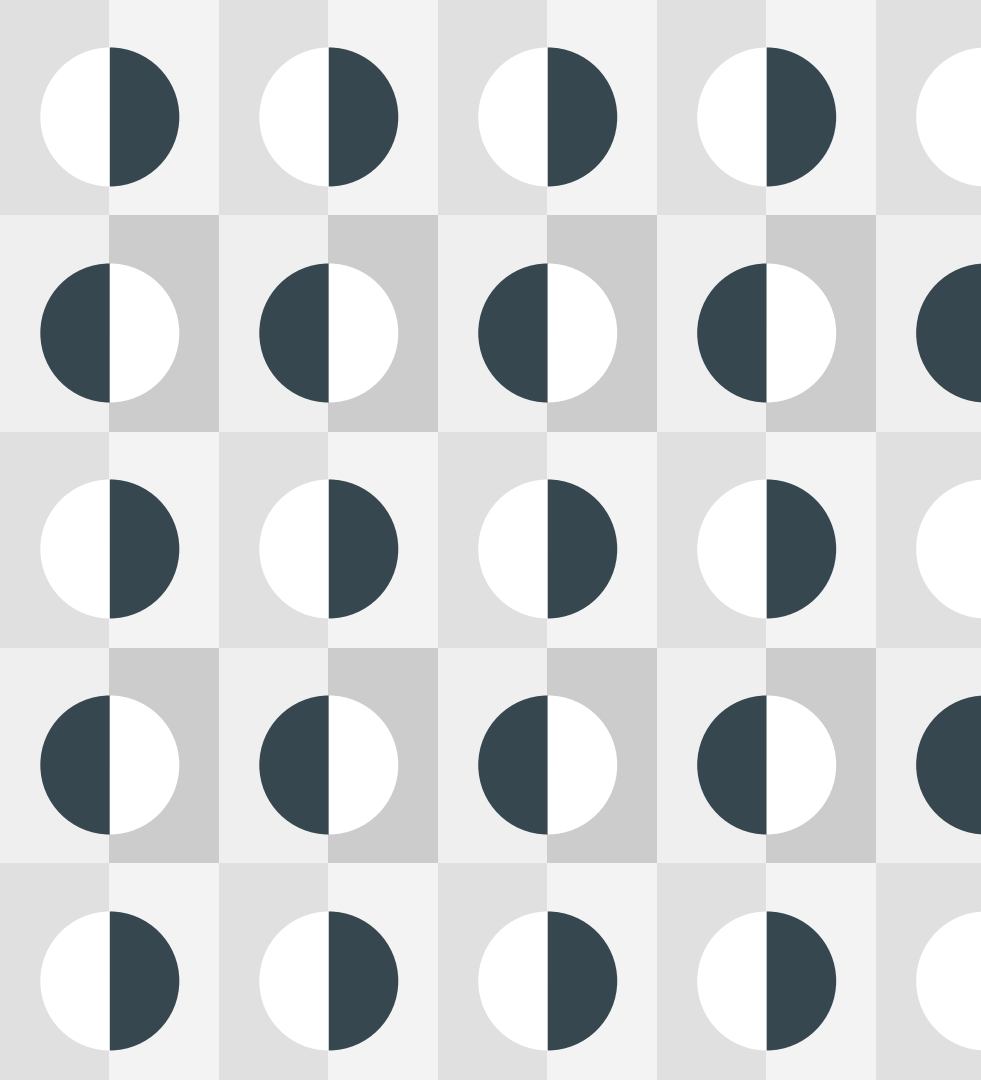
# How to Hide it?

1. Go to General settings > Welcome message
2. Remove the %v variable from the Custom welcome message input box on the right, or replace all the text with your own text
3. Check the 'Hide welcome message in log' option



# Visual Representation



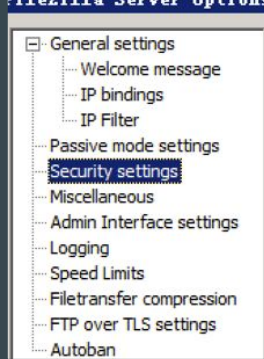


**YAY! Enable  
Stuff**

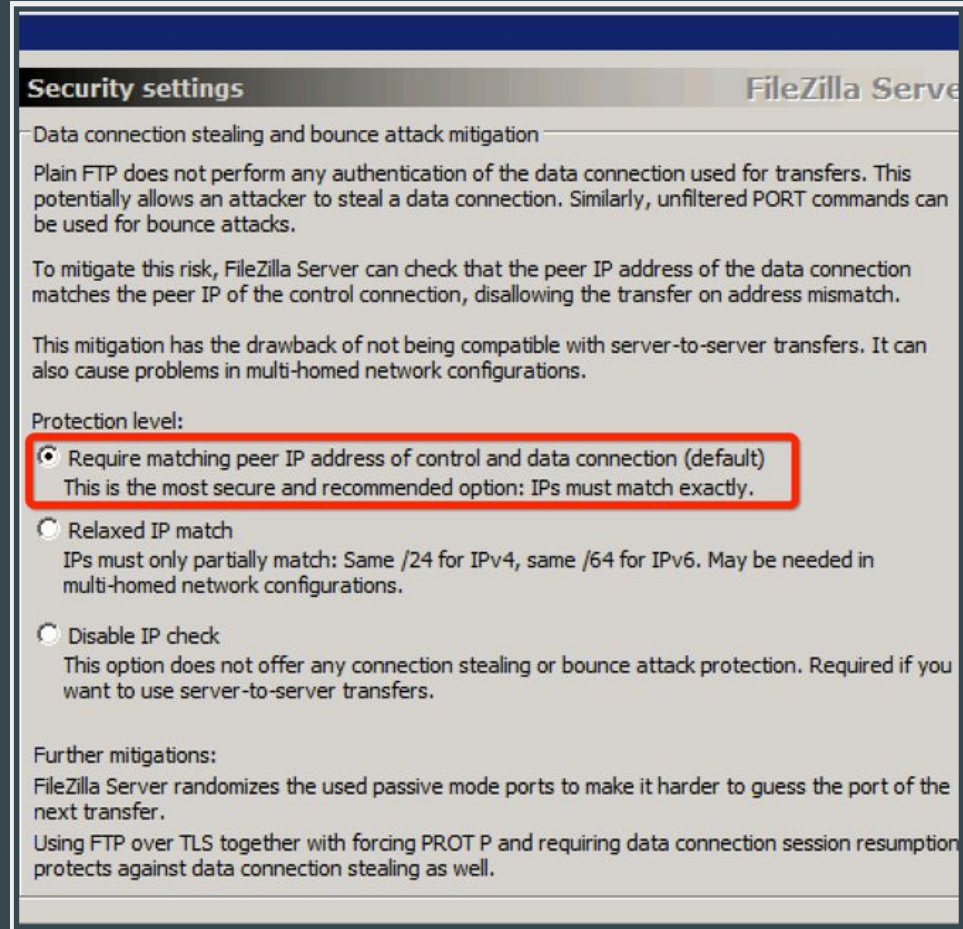
# Bounce Attack Protection

- FTP Bounce attack is an attack that uses the FXP feature.  
Unfiltered PORT commands can be used for bounce attacks.
- Enable the bounce attack mitigation option
  - FileZilla Server checks if peer IP address of the data connection = peer IP of the control connection
- tl;dr basically prevents middle man attacks

# How?



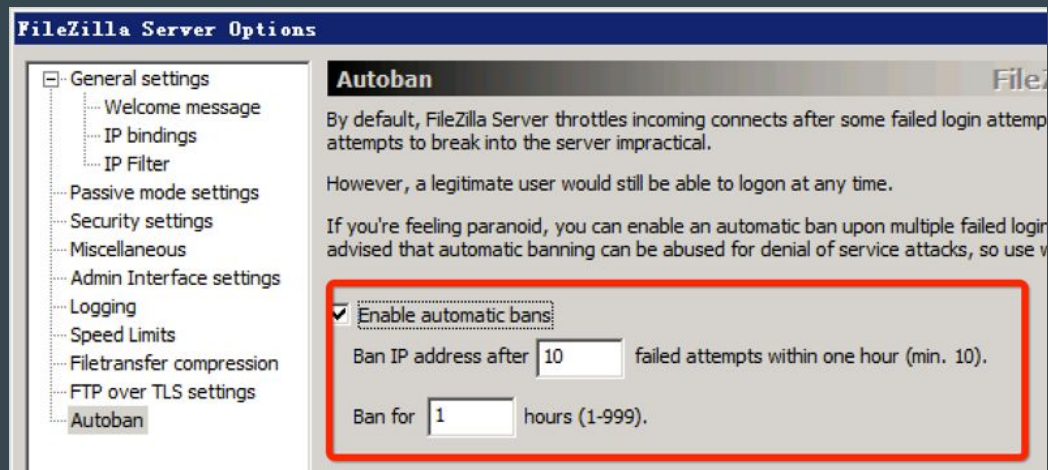
1. Go to General settings > Security settings.
2. For Protection level, check **Require matching peer address of control and data connection**



# Automatic Bans

- Block a client IP address that has multiple failed login attempts
- Hinders brute-force attacks

## 1. Go to Autoban



The screenshot shows the 'FileZilla Server Options' dialog box with the 'Autoban' tab selected. The 'Autoban' section is highlighted with a red rectangle. The 'Enable automatic bans' checkbox is checked. The 'Ban IP address after' field is set to 10, and the 'Ban for' field is set to 1 hour.

**FileZilla Server Options**

**Autoban**

By default, FileZilla Server throttles incoming connects after some failed login attempts to break into the server impractical.

However, a legitimate user would still be able to logon at any time.

If you're feeling paranoid, you can enable an automatic ban upon multiple failed login attempts. However, automatic banning can be abused for denial of service attacks, so use with caution.

☒ **Enable automatic bans**

Ban IP address after  failed attempts within one hour (min. 10).

Ban for  hours (1-999).

It's like discord autoban bot, or secpol account lockout settings

# Logging

## FileZilla Server Options

### ☐ General settings

.... Welcome message

.... IP bindings

.... IP Filter

.... Passive mode settings

.... Security settings

.... Miscellaneous

.... Admin Interface settings

.... **Logging**

### Logging

☒ Enable logging to file

☐ Limit log file size to  KB

Logfile type:

☐ Log all to 'FileZilla Server.log'

☒ Use a different logfile each day (example)

☐ Delete old logfiles after

# TLS Encryption Authentication

- FileZilla Server supports TLS encryption
  - Encrypts data using cool algorithms
- If you do not have a certificate, you can use the built-in certificate creation feature to create one.
  - Don't worry about providing real information in the certificate, it just needs all boxes to be filled with something
    - In practical scenarios, don't put random stuff though



## FileZilla Server Options



- General settings
  - Welcome message
  - IP bindings
  - IP Filter
- Passive mode settings
- Security settings
- Miscellaneous
- Admin Interface settings
- Logging
- Speed Limits
- Filetransfer compression
- FTP over TLS settings**
- Autoban

### FTP over TLS settings

☐ Enable FTP over TLS support (FTPS)

☐ Disallow plain unencrypted FTP

#### X.509 Certificate

Private key file:

Certificate file:

Key password:  Password will be stored in plaintext.

#### Explicit and implicit FTP over TLS

☒ Allow explicit FTP over TLS (default: yes)

Note: Explicit FTP over TLS shares the normal FTP port configured on the General settings page.

Listen for implicit FTP over TLS connections on the following ports (default: 990):

#### File transfer security

These settings need to be enabled for file transfers to be secure.

☒ Force PROT P to encrypt file transfers when using FTP over TLS

☒ Require TLS session resumption on data connection when using PROT P

OK

Cancel

### FileZilla Server



This dialog will help you to create a new private key and a self-signed certificate, needed by FileZilla Server to accept TLS connections.

Please fill out the required information. Wrong or missing information may confuse clients.

Key size: ☐ 1280 bit ☒ 2048 bit ☐ 4096 bit

2-Digit country code:

Full state or province:

Locality (City):

Organization:

Organization unit:

Contact E-Mail:

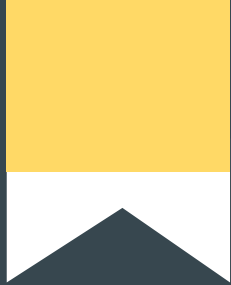
Common name  
(Server address):

Save key and certificate to this file:

Generating the certificate may take some time depending on the key size.



# User Stuff



# Use complex user passwords

Self Explanatory    Hope you have  
a brain

# Users and Groups

Edit > Users

Edit > Groups

# Modifying users

- Similar to `lusrmgr.msc`, you can add/remove users and groups that can access FTP shares
- Each user can have different username-password combinations for different access permissions on different files
- There are no default users or groups; you make your own
  - We can make “beans” an administrative group, and any user in “beans” may have full control access to the “SecretRecipe” share
  - We can create an anonymous user of any name and give it only read-permissions to the “Program Installation” folder

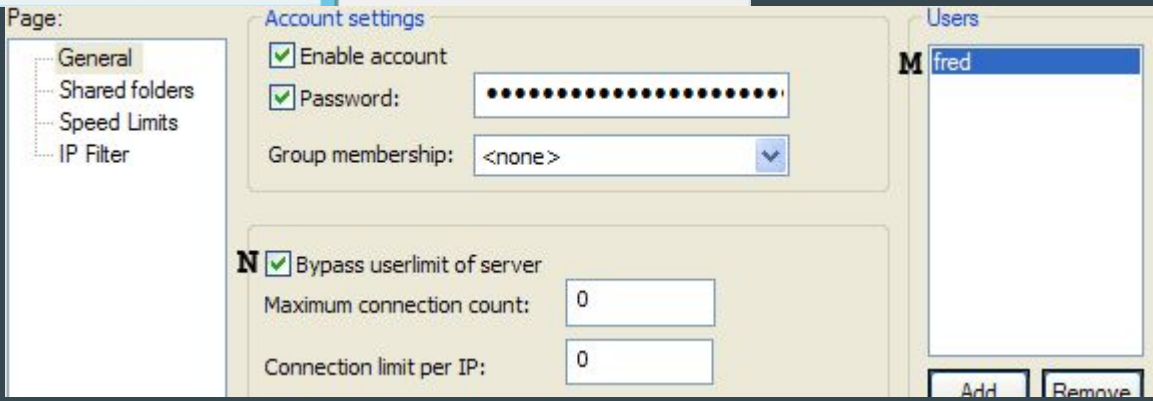
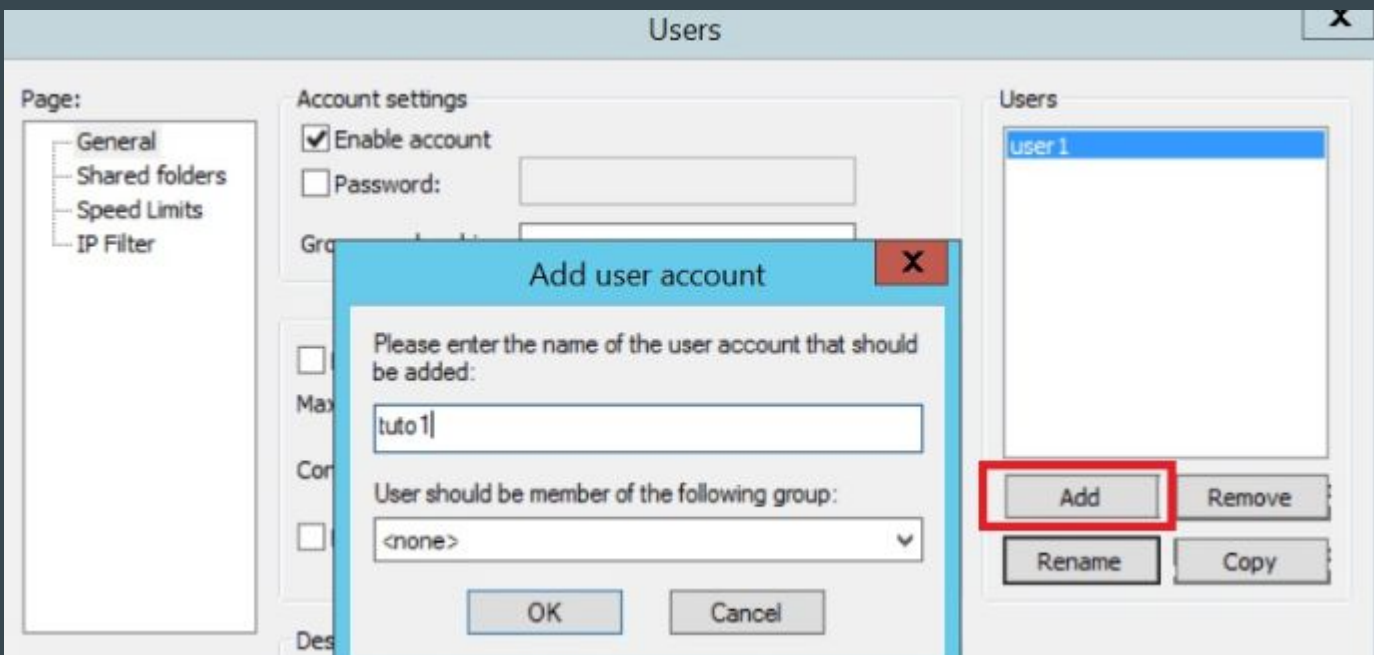
# Where to go to modify?

- Edit > Users
- Edit > Groups

# Configure Stuff

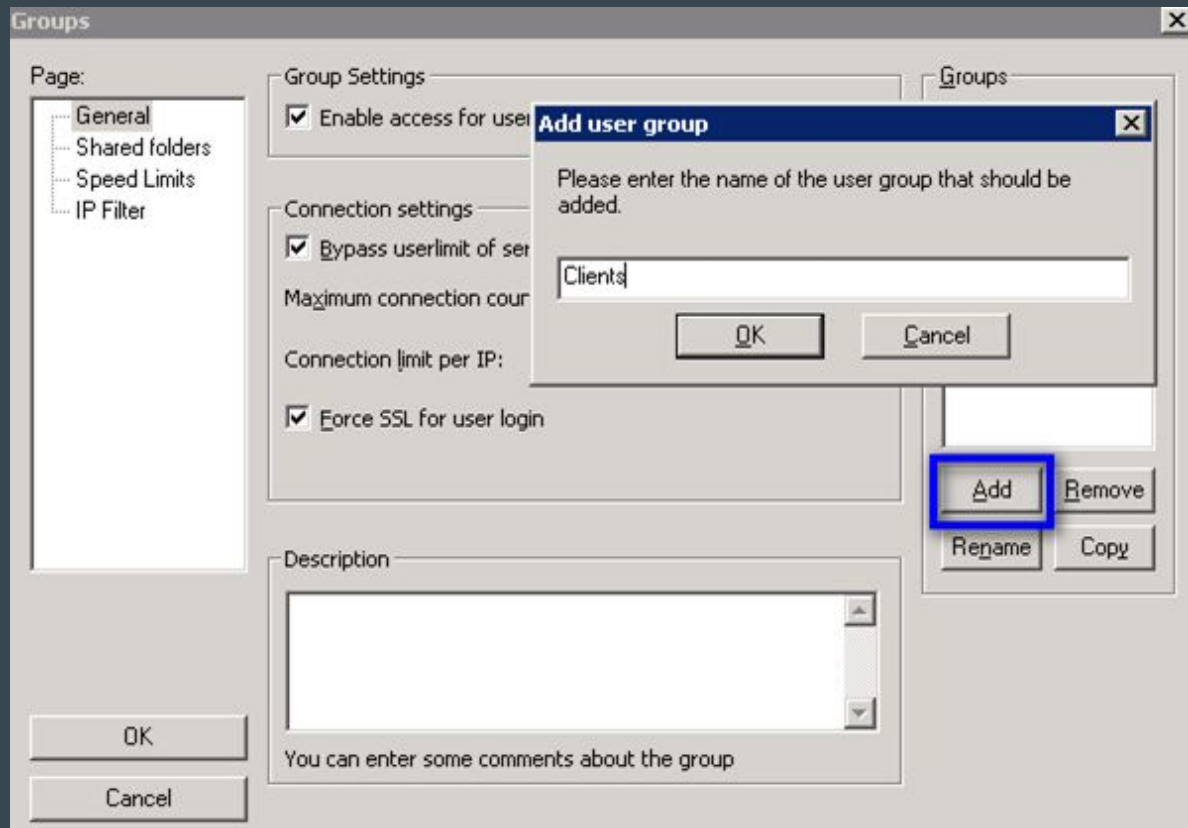
# Least Privilege

- FileZilla supports directory-level access permission settings
- You can grant users the following permissions for a directory:
  - (Files) Read, Write, Delete, and Add Files, and (Directories) Create, Delete, List, and Add Subdirectories.
- Adhering to the principle of least privilege (POLP), limit access to the minimal level that allows normal functioning.

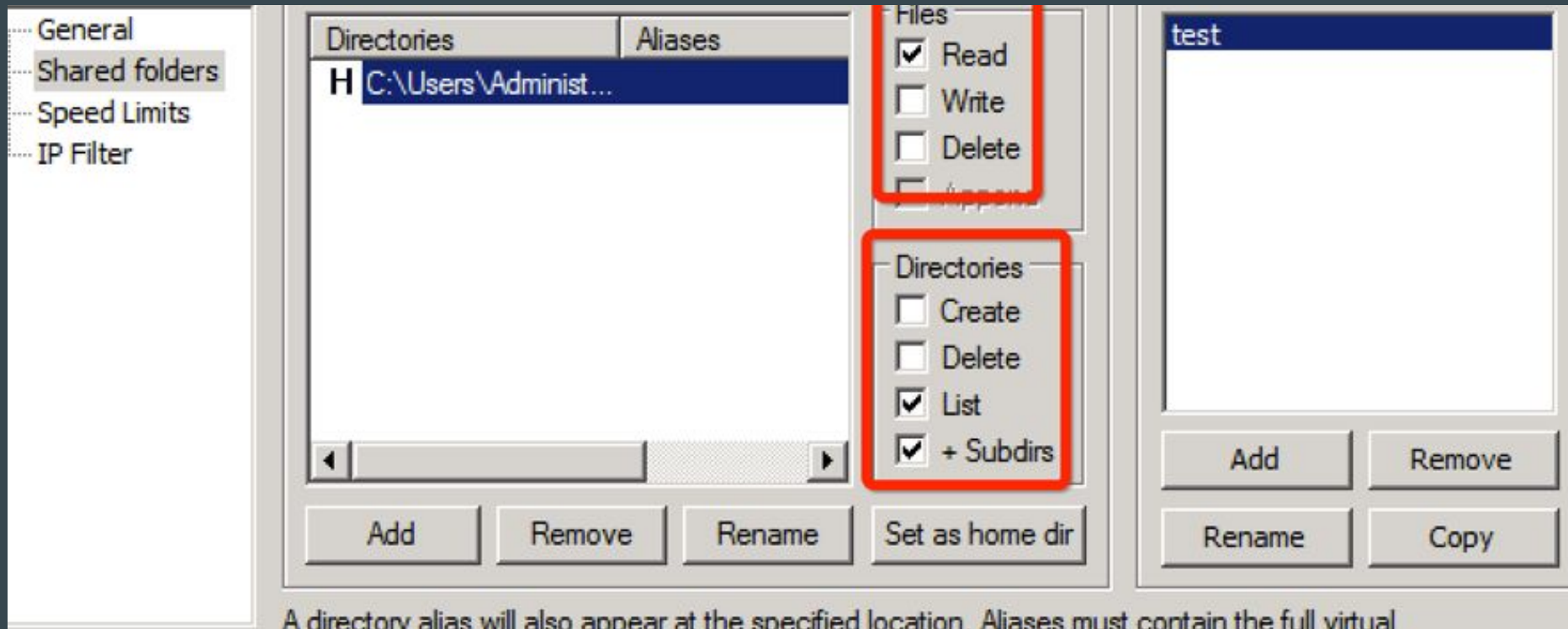


Visuals

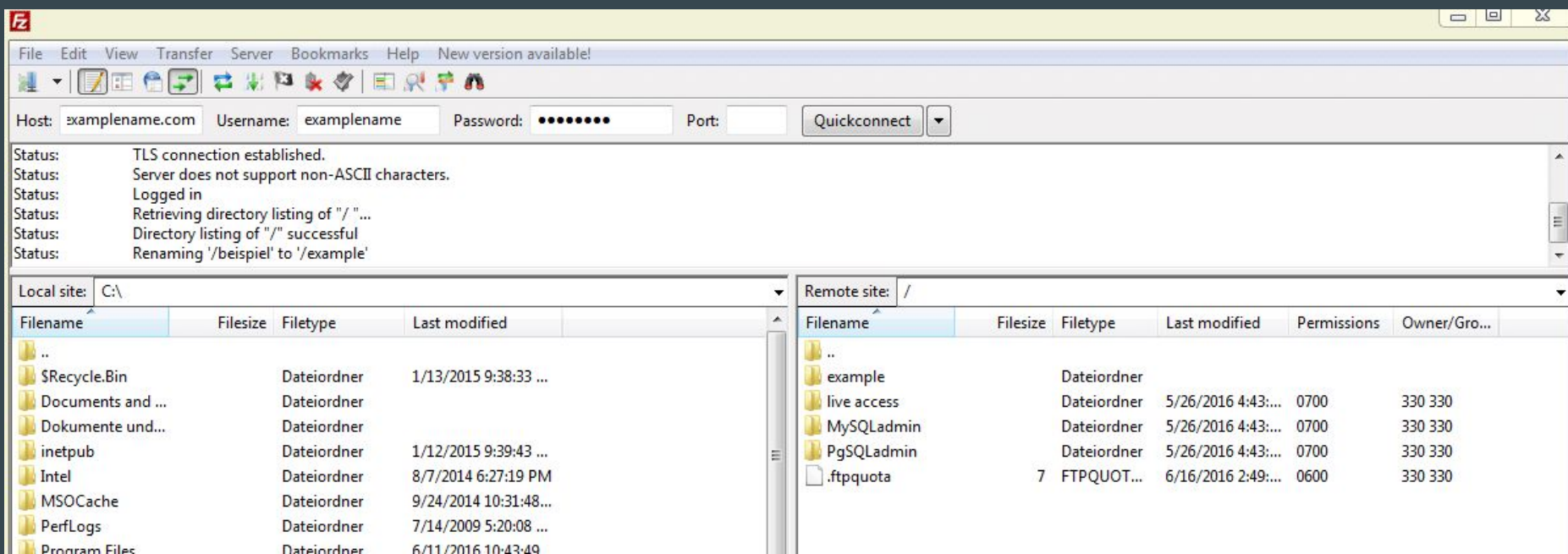




More Visuals



Even More Visuals



What the FileZilla Client looks like



# END

By Troy kids

AKA Asapre and Cchan