

FTP:

FTP 的默认端口为

FTP control 20

FTP data 21

所以默认状态下可以 list. 如果要提高 FTP 服务器的安全性, 我觉得改变端口开始治标不治本。建议使用 FTPS(FTP over SSL), 应用 SSL 方式将传送的密码和数据加密, 相对安全。此方式的默认端口是 989,990.

简介:

Filezilla是一个非常流行的开源的免费的FTP客户端、服务器端的项目, Filezilla的主要优势在于: 高安全、高性能。Filezilla的安全性是来自于其开放源代码的。Filezilla的高性能来自于其代码的开发平台是C/C++, 自身基础就好于其他VB/Dephi平台开发的应用程序, 因此Filezilla具有可媲美IIS的性能。在千兆网络带宽上, 可轻松满足数百用户同时高速下载。目前Filezilla也存在一些不足, 主要缺点就是不支持配额, 即本身不提供上传、下载总文件大小配额的功能。

FileZilla Server 伺服器的程式看成兩部份, 第一部份是 FTP 的 Service 服務, 他是提供其他電腦透過 FTP 通訊協定連線進來存取檔案用的網路服務, 這部份的功能可以讓他隨著電腦自動開機啟動。而伺服器啟動後我們並不會看到什麼視窗或圖示, 它會在 Windows 系統的背景執行, 只有在檢視「工作管理員」時, 才可以看得到。

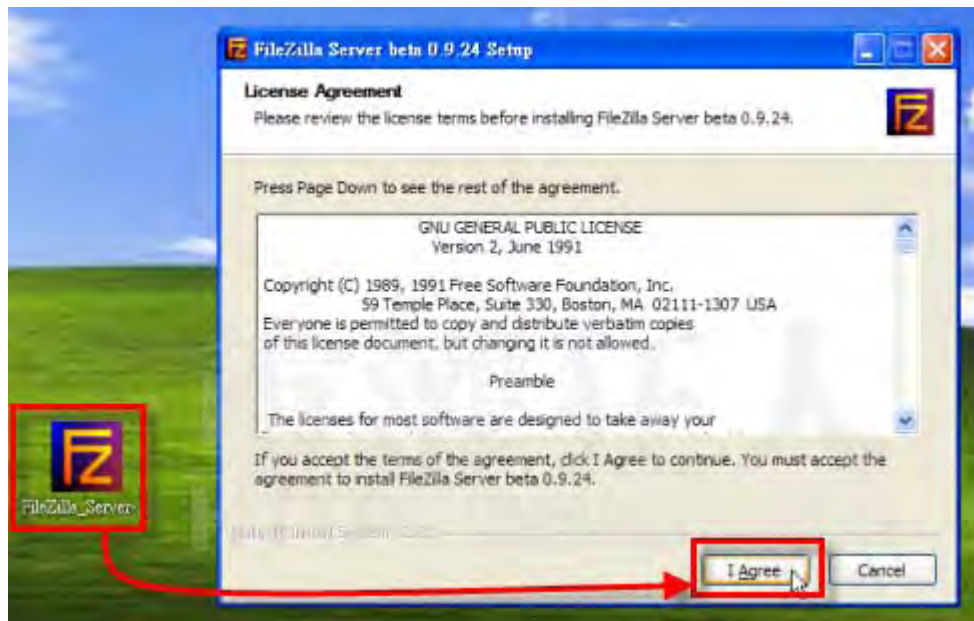
另外一步部份是「FileZilla Server Interface」伺服器管理介面, 這個管理介面是管理FTP伺服器、新增或移除FTP帳戶時才會用到。只要安裝時設定好FileZilla Server 的 Service 與組態、帳戶之後, 其他時候可以不用開啟伺服器管理介面, FTP 也可以正常運作。(因為 FTP 伺服器會在安裝好之後, 開機自動執行)。

大概知道有這兩個東西之後, 下面的安裝過程就會比較清楚一點。後面會有個步驟問我們是否要開機自動啟動 FTP Service 或是否要開機自動啟動 Server Interface, 講的就是這兩個東西。

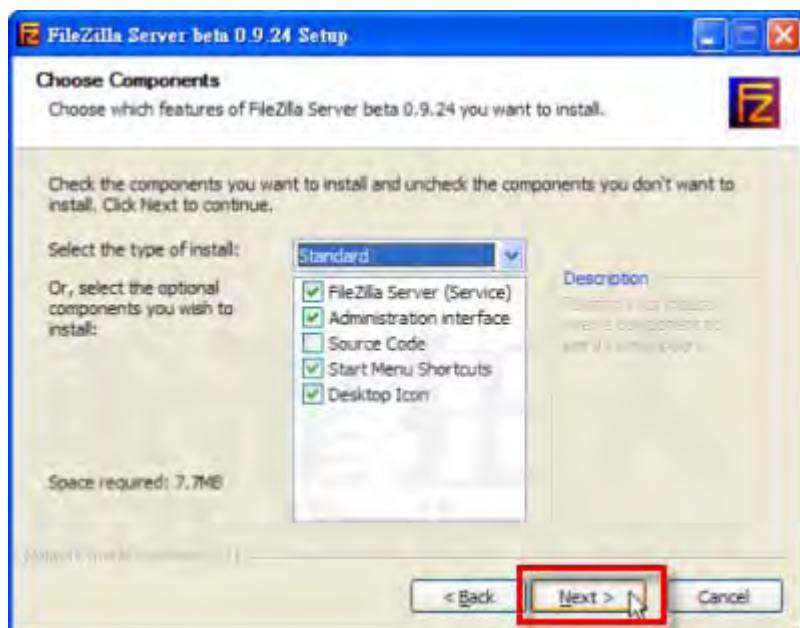
安裝:

第 1 步 选用最新版本的filezilla_server。 <http://filezilla-project.org/>

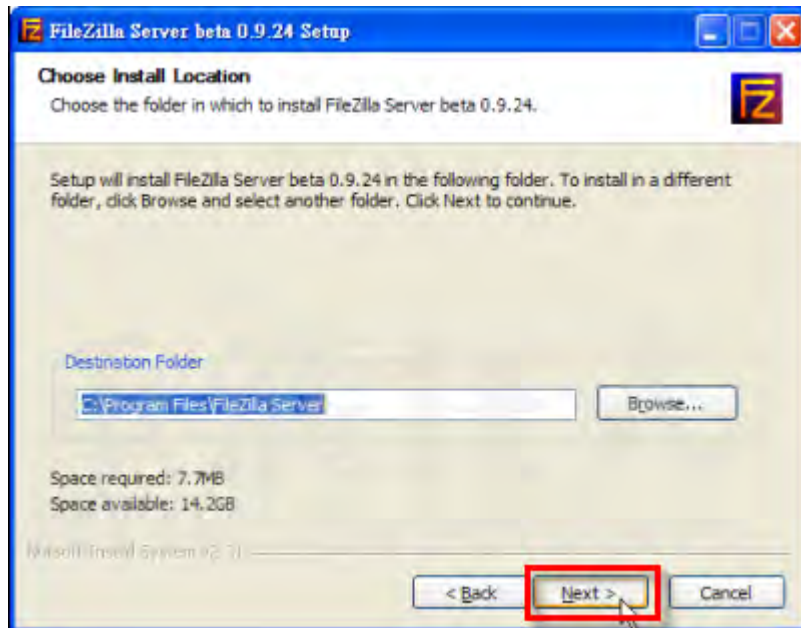
然後在「FileZilla_Server-0_9_24.exe」安裝檔上按兩下滑鼠左鍵, 執行安裝程序, 接著再按一下〔I Agree〕按鈕, 開始安裝。



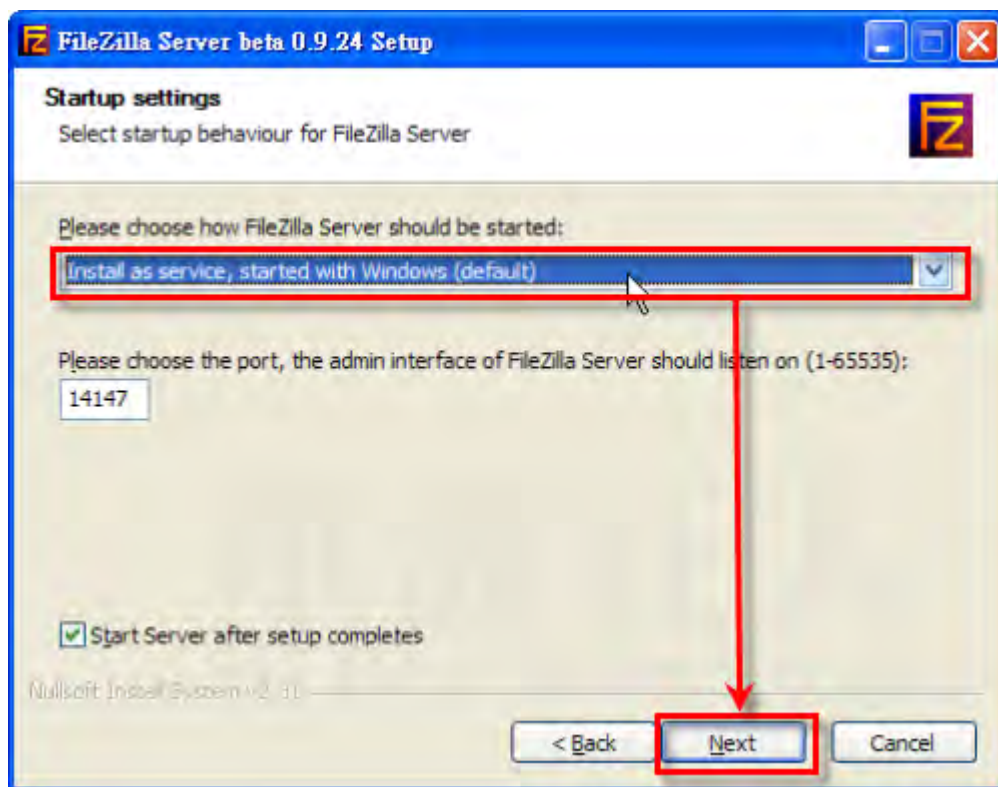
第 2 步 接著他會問你要安裝哪些元件，安裝方式：默认的标准，按一下（Next）繼續下一步。



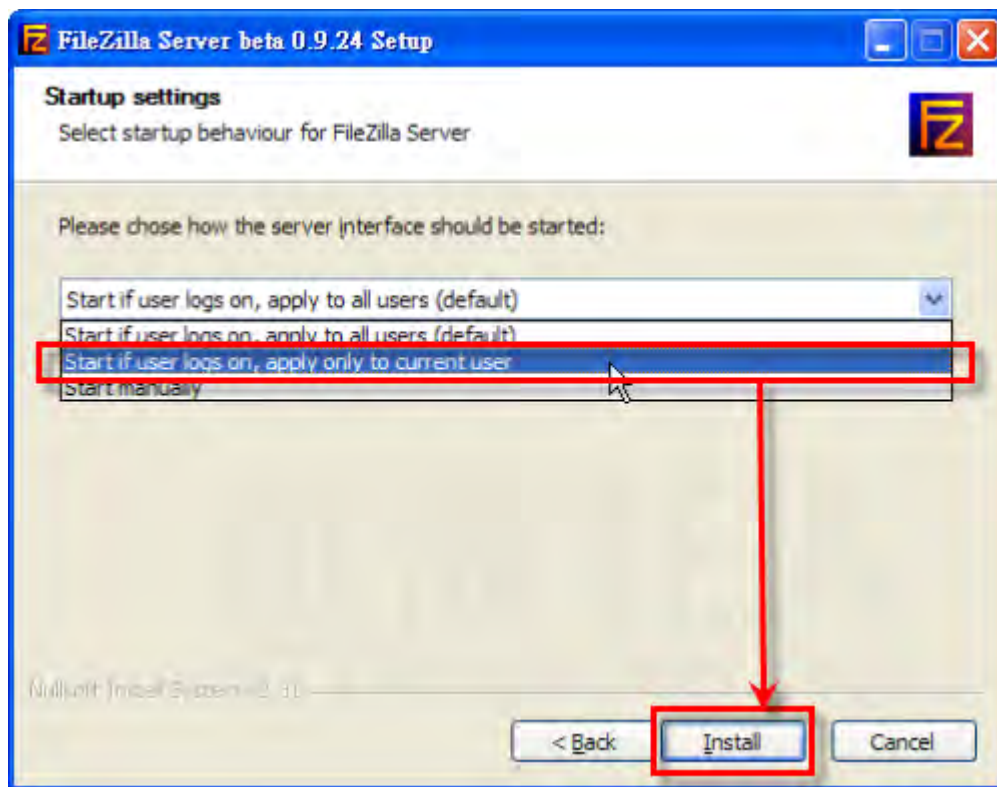
第 3 步 接著他會問你要將FTP伺服器程式安裝到哪個資料夾去，**強烈推薦安裝到非默认路径，以增加安全系数**。請按一下（Next）按鈕，繼續下一步。



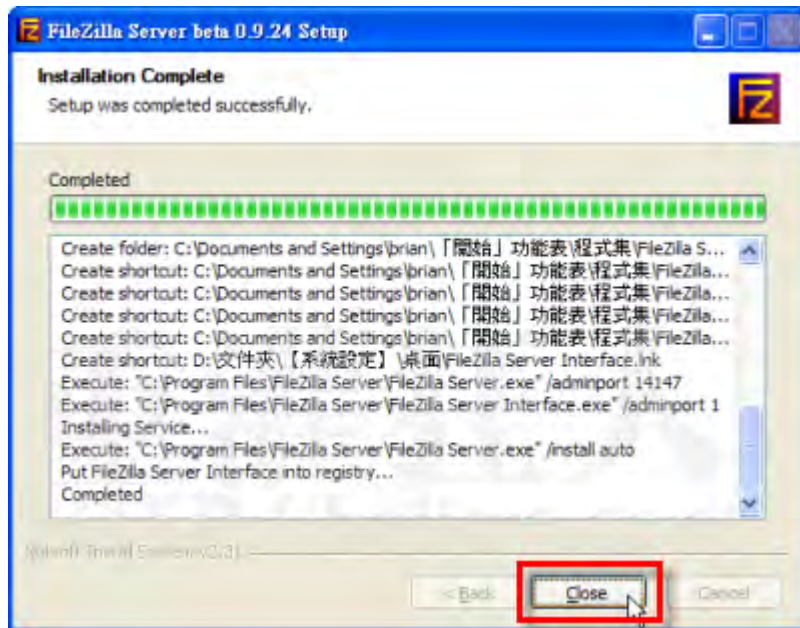
第 4 步 此步驟是詢問我們是否要讓FTP伺服器在電腦開機時自動啟動，請點選【Install as service, started with Windows (default)】，再按一下（Next）。這樣FTP伺服器便會自動被安裝成系統的Service，每次開機後便會自動再背景中啟動並執行FTP伺服器的功能。設置管理端口“14147”，強烈推薦修改此端口，例如：改成 38121 端口。（注意不要和常見服務如 80 端口衝突）



第 5 步 接著我們可以設定是否在開機時自動啟動「FileZilla Server Interface」伺服器管理介面，如果你常常需要管理你的FTP伺服器，可以選【Start if user logs on, apply only to current user】。一般來說都是選最下面的【Start manually】，要用時再手動開啟即可。

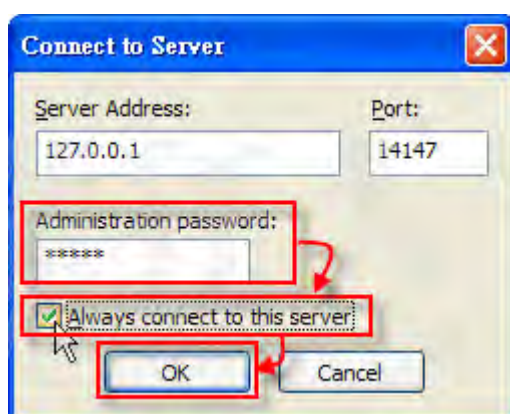


第 6 步 安裝好之後，請按一下（Close）按鈕，結束安裝程序。



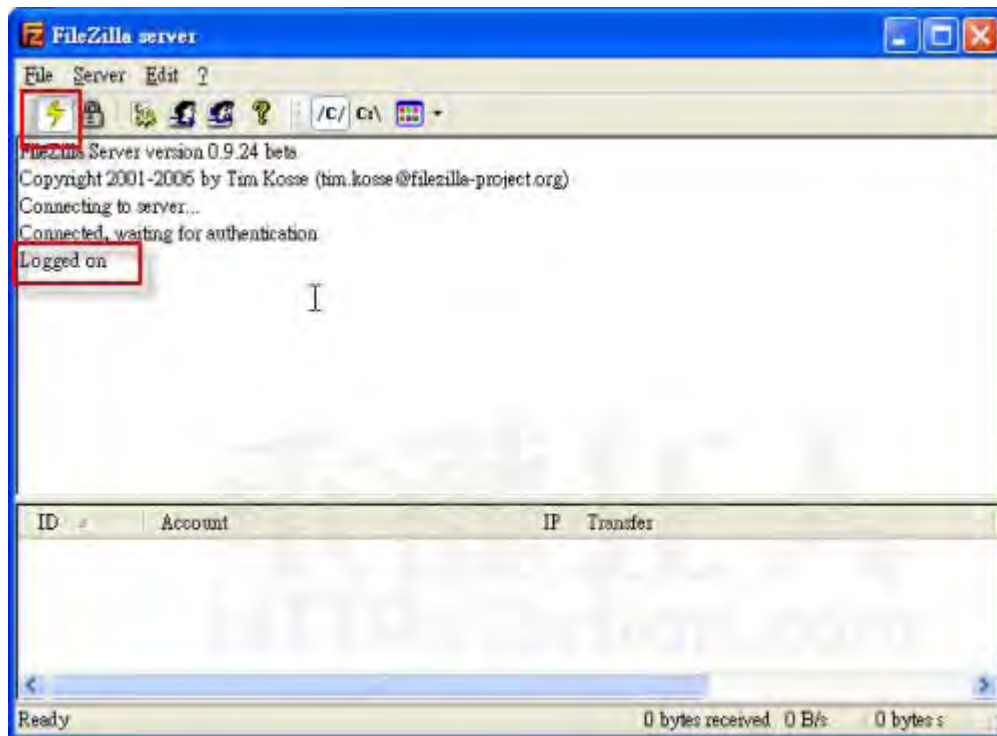
第 7 步 安裝好軟體後，啟動FileZilla伺服器時，會出現一個「Connect to Server」視窗，我們可以在「Administrator password:」欄位中输入本服务器Filezilla服务的密码，输入管理端口号（管理端口到底是多少，请参考前文安装过程中填写的具体数字是多少。），然後勾選「Always connect to this server」再按下（OK）。建议选中“总是连接到本服务器”的选项，即表示每次启动管理控制台，都是管理本机的Filezilla服务。

注意：修改端口和密码非常重要，这是确保Filezilla安全的重点，必须修改端口，必须设置密码！密码建议足够复杂！可以在管理界面中进行修改。



第 8 步 如圖，出現FileZilla伺服器管理介面後，我們可以在視窗上半部看到目前的FTP伺服器的運作狀況，如果有出現「Logged on」或「Server online」

的字樣，表示已經順利上線。我們可以隨時點按上方的閃電圖示切換上線、離線，即可手動開啟或關閉FTP站。



服务器设置：

第1步 进行服务器全局参数设置：点“Edit”菜单，选“Settings”

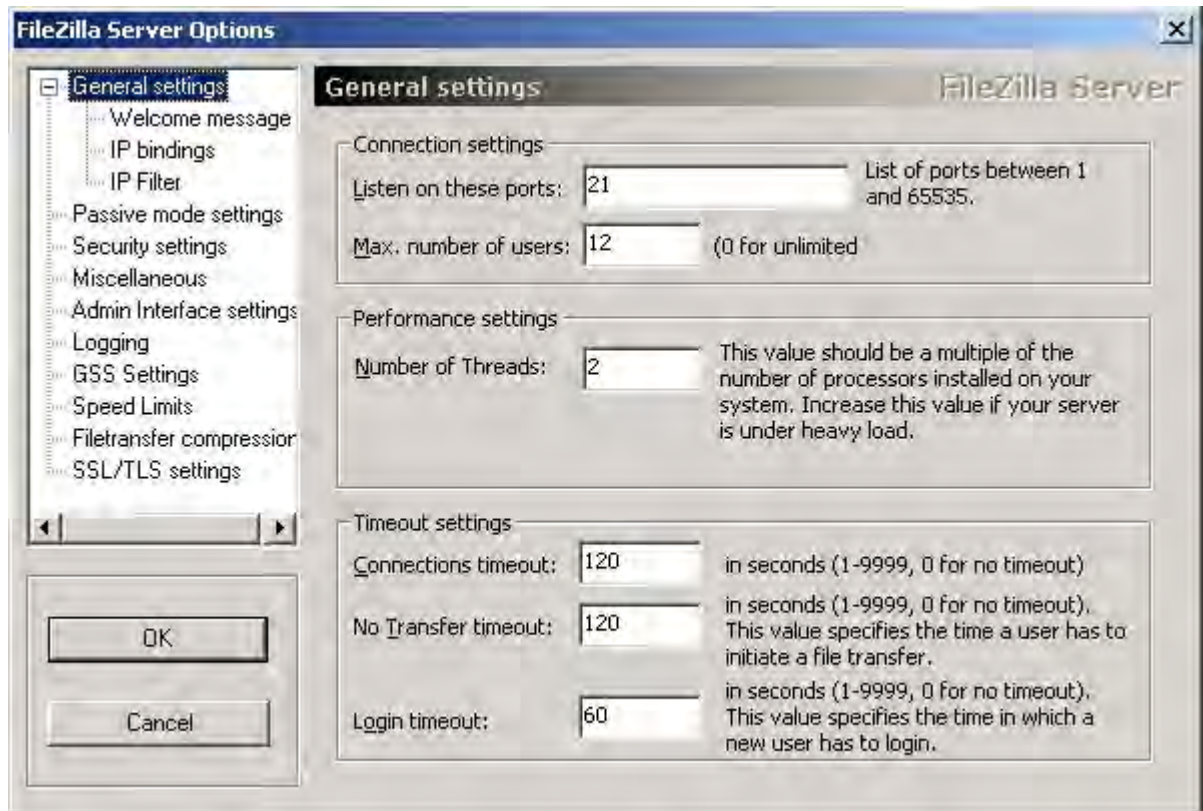
General settings（常规设置）：

Listen on Port：监听端口，其实就是FTP服务器的连接端口。

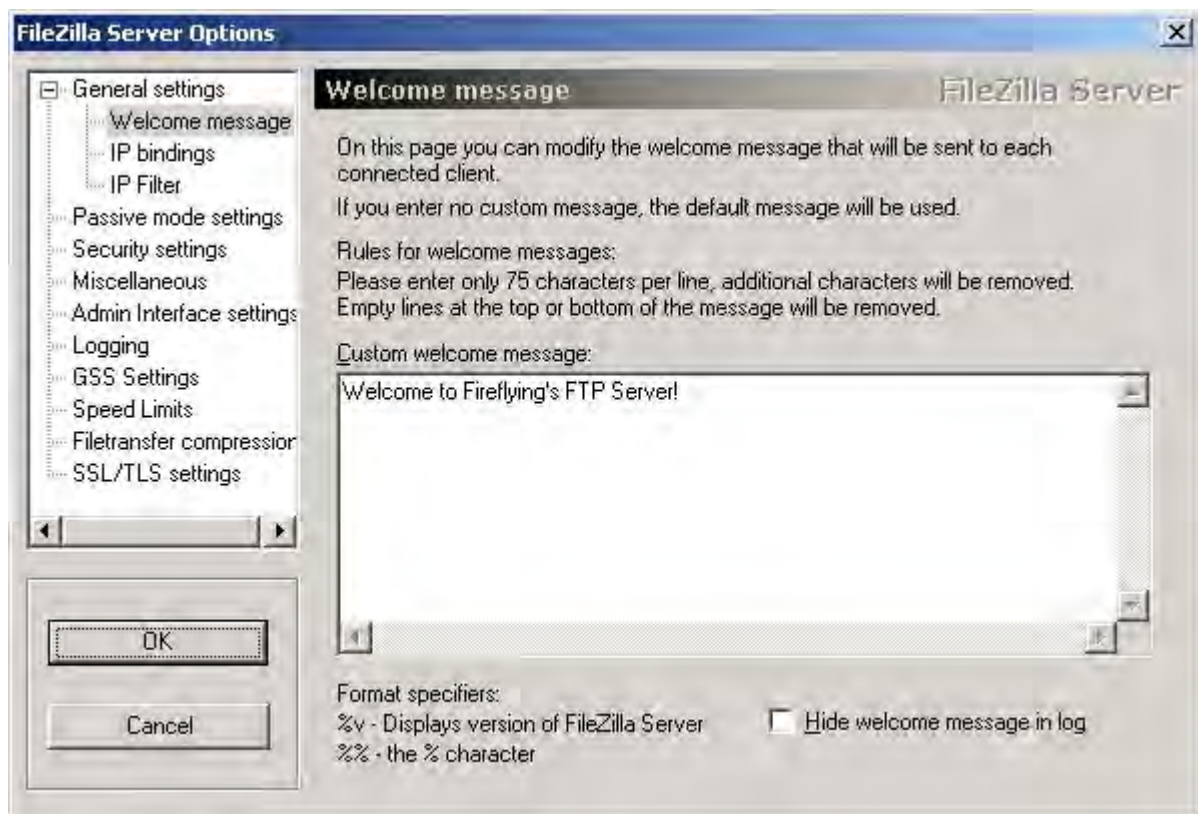
Max.Number of users：允许最大并发连接客户端的数量。

Number of Threads：处理线程。也就是CPU优先级别。数值调得越大优先级越高，一般默认即可。

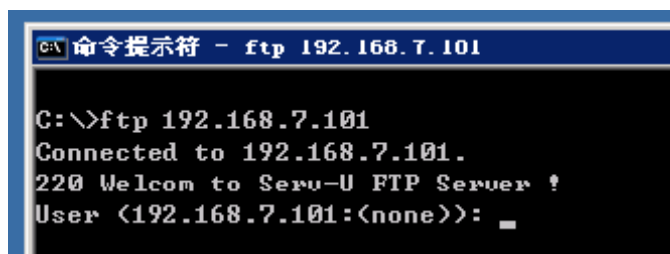
timeout setting：超时设置，自上至下分别为：连接超时、传输空闲超时、登入超时。单位为秒。



Welcome message页面设置：客户端登录成功以后显示的Welcome信息。建议不要用软件默认的，因为任何软件都不能保证没有什么漏洞，如果在这里暴露软件名称的话，一旦这个FTP Server软件有什么安全漏洞，别有用心的人知道了服务器软件的名称就可能针对性地发起攻击。所以建议这里设置的信息不要包含任何服务器资料。**强烈建议修改默认的欢迎信息为“Welcom to Serv-U FTP Server”，这样Filezilla在欢迎消息中就会Serv-U字样，以达到欺骗攻击者的目的。注意：本步骤非常重要！**

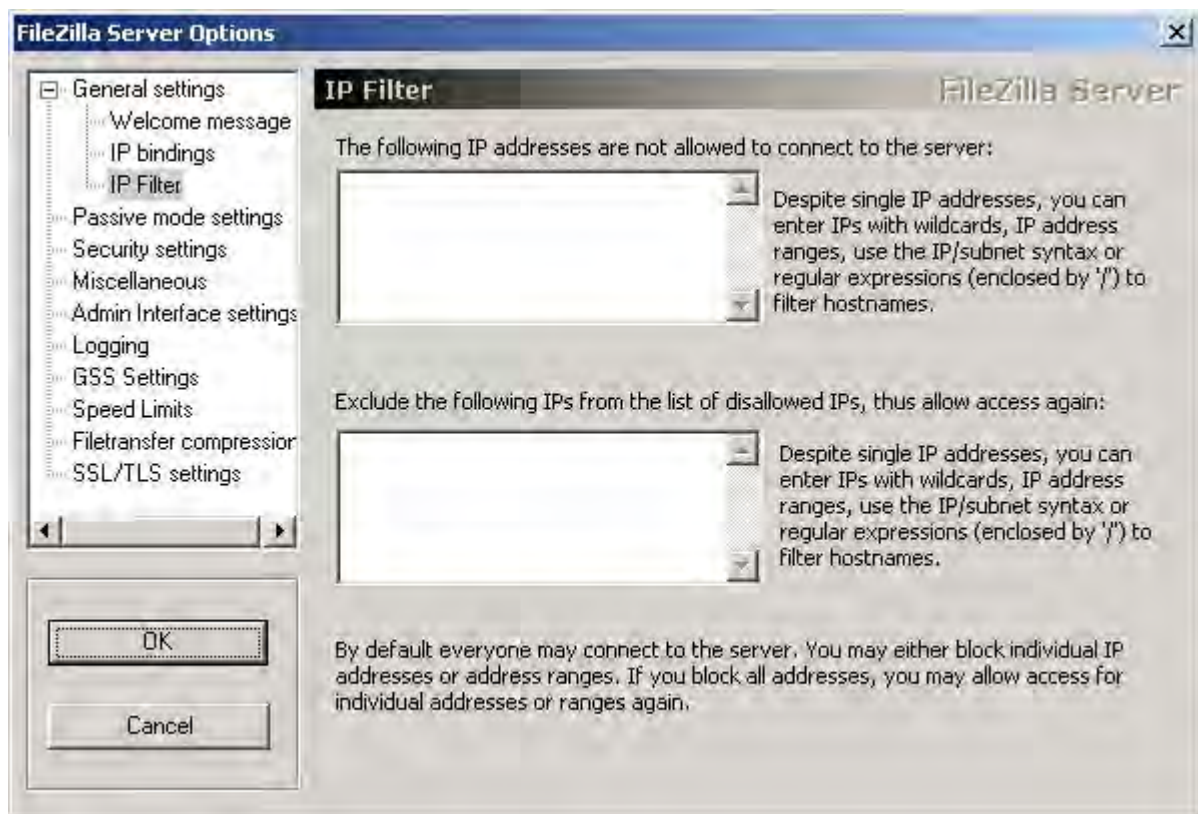


现在我们用telnet去连接一下FTP的21端口，即可看到修改过的“假”的提示信息，这样服务器的安全性可以得到比较明显的提高。



IP bindings（IP 绑定）页面：把服务器与 IP 地址绑定，使用*以绑定到所有地址。

IP Filter（IP 过滤器）页面：设置 IP 过滤规则，在上面栏目中的 IP 是被禁止与 FTP 服务器连接的，下面的是允许的。格式：可以是单个 IP 地址、IP 地址段，可以使用通配符、使用 IP/subnet 语法或正则表达式（以“/”结尾）来过滤主机名。



第 2 步 Passive mode settings (被动传输模式设置): 这个页面要重点关注。

如果服务器本身直接拥有公网 IP, 可以选软件默认的 “Default”。

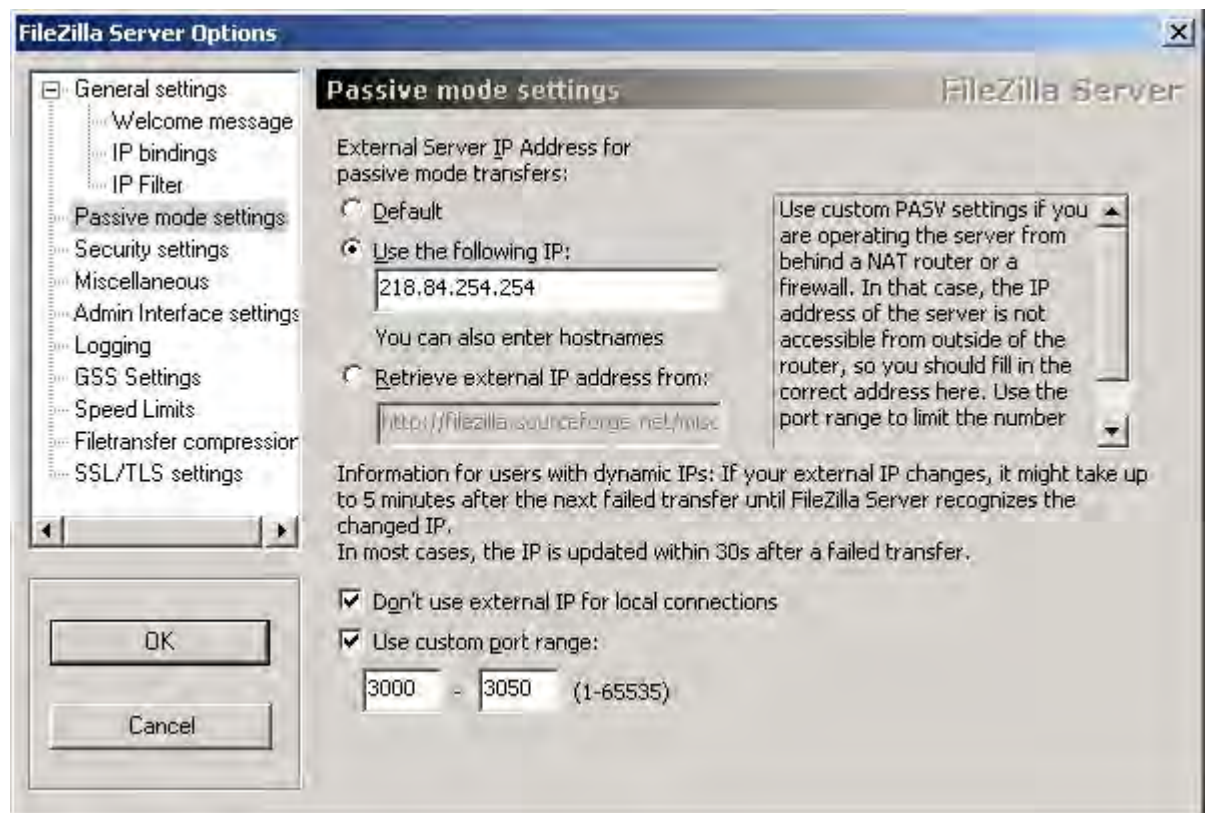
如果服务器是在局域网里面, 在一个网关后面, 那么就要选择第二项 “Use the follwoing IP”, 并且在下面的输入栏填写公网的 IP 地址; 否则, 客户端用 PASV 被动模式可能无法连接 FTP 服务器。因为服务器是在内网中, 在客户端使用 PASV 模式连接服务器的时候, 服务器收到连接请求之后需要把自身的 IP 地址告诉客户端, 由于服务器在内网中, 它侦测到的 IP 地址是内网的 (如 192.168.0.5), 它把这个 IP 地址交给客户端, 客户端自然无法连接。在这里设置了指定的 IP 地址后, 服务器就会把这个公网合法的 IP 地址提交给客户端, 这样才能正常建立连接。

如果服务器是动态 IP 的, 那么可以选择下面的 “Retrieve external IP address from”, 利用 FileZilla 官方网站免费提供的 IP 查询页面获取当时的公网合法 IP, 然后服务器把这个公网合法 IP 地址提交给客户端。当然静态 IP 也可以用这个, 只不过没有必要。

这个设置页面对服务器位于内网的情况非常重要。有些 FTP 服务器端没有这个设置项目, 客户端就只能用 Port 主动模式连接。当然有些客户端软件针对这个问题有专门的设置, 如 FlashFXP 的站点设置中只要选中 “被动模式使用站点 IP” 就可以了。

对于在局域网中的服务器, 如果服务器没有置于 DMZ 区, 那么强烈建议选中下面的 “Use custom port range” 定义 PASV 端口范围。由于 PASV 模式中, 是服务器随机打开端口, 然后把打开的端口号告诉客户端, 让客户端连接打开的端口。但是因为服务器处于网关后面, 如果网关那里没有做对应的端口映射, 客户端从外网就无法连接服务器打开的端口, 导致 PASV 模式连接失败。在这里限定

服务器打开的端口范围，然后到连接外网的网关那里，对服务器的这些端口做端口映射（虚拟服务）。这需要服务器和 Internet 网关设备配合设置，这样外网的客户端才能用 PASV 模式连接进来。



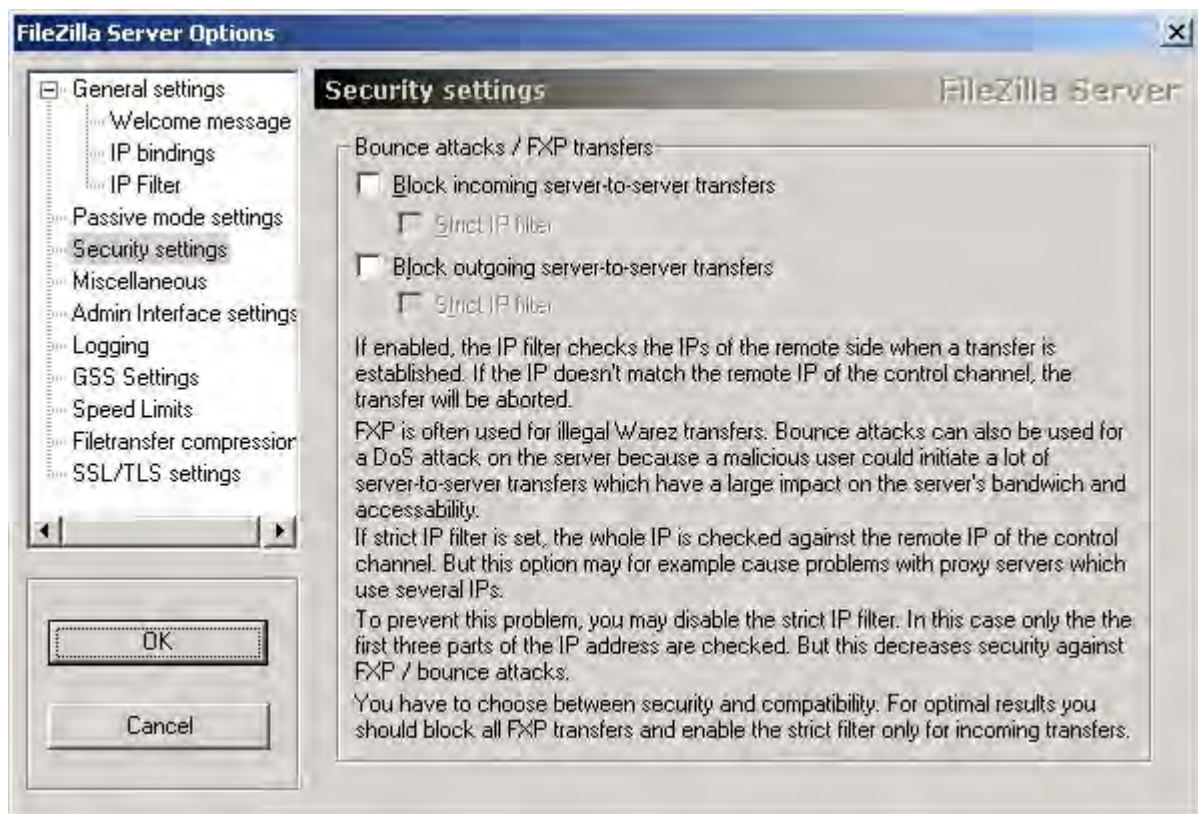
第 3 步 Security settings（安全设置）：这里的两个选项关系到能否 FXP。软件默认状态“Block incoming server-to-server transfers”和“Block outgoing server-to-server transfers”两项都是选中的，前面那项是禁止连入的服务器对传，后面是禁止传出的服务器对传。也就是说默认状态不允许 FXP，如果需要使用 FXP，那么就把这两个项目取消选择。注意 FXP 传输除了跟这个页面的设置有关，还跟 IP 过滤器有关。

说明：如果启用，IP 过滤器在传输开始时检查远端 IP，如果 IP 不符合控制通道中的远端 IP，传输将被取消。

FXP 经常被用来传输非法盗版软件，反弹攻击亦可被用来发起对服务器的 Dos 攻击，因为恶意用户可以发起多个服务器到服务器传输，这将对服务器的带宽和可用性造成很大影响。

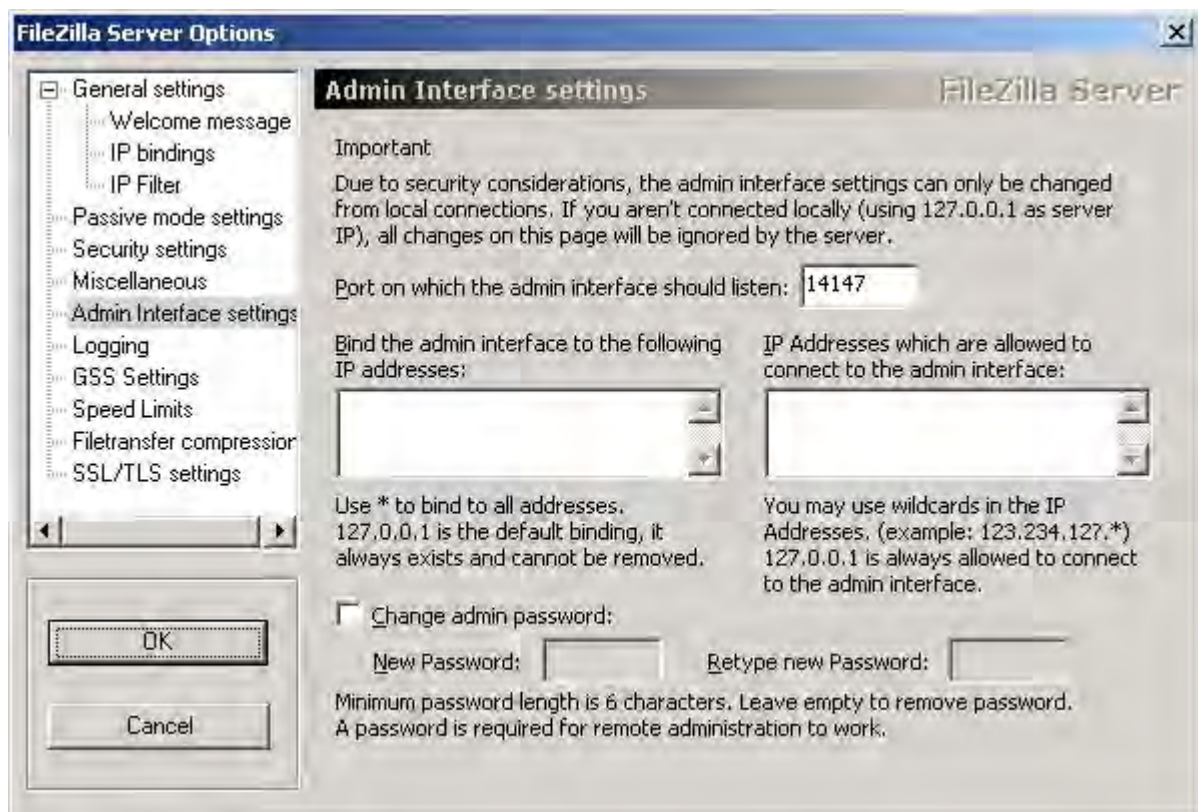
如果设置了严格过滤 IP，整个 IP 将与控制通道中的 IP 进行比较，但此选项可能会对使用了多个 IP 的代理服务器引发问题。

为了避免此问题，可以禁用严格 IP 过滤，这样只检查 IP 地址的前三部分，但这会使对 FXP/反弹攻击的安全都降低。因此，你需要在安全和兼容性之间做选择，要想达到最佳效果，你可以阻止所有的 FXP 传输并且仅对传入的传输启用严格过滤。

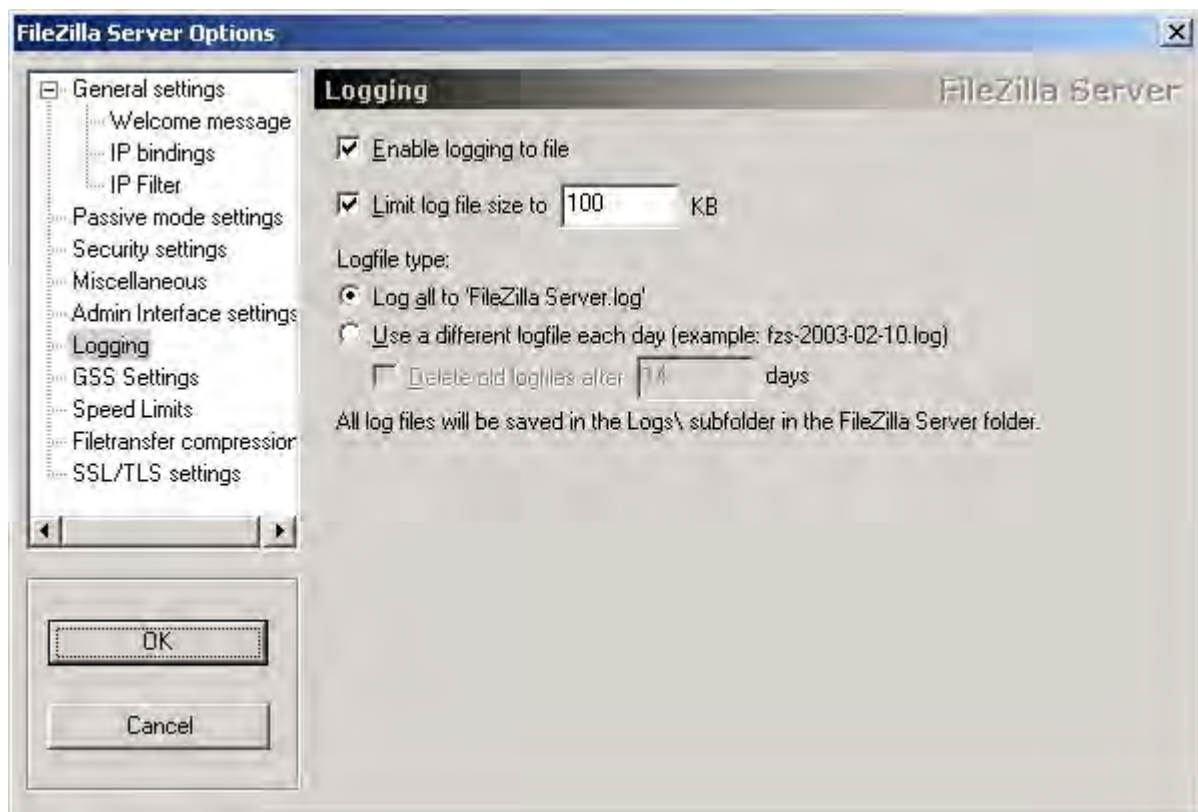


第 4 步 Admin Interface setting (管理员界面设定): 这个就是登录配置服务器界面的一些参数。端口号的设置在安装的时候也出现过。下面两栏可以定义允许远程登录配置的网络界面和 IP 地址, 第一个空白可以设置把管理界面绑定到 IP 地址, 使用*以绑定所有 IP 地址, 127.0.0.1 是默认绑定, 它一直存在且不可被移除; 第二个空白设置允许连接到管理界面的 IP 地址, 可以使用通配符 (例如: 123.234.12?.*), 127.0.0.1 总是被允许连接到管理界面的。在最下面更改管理员口令。

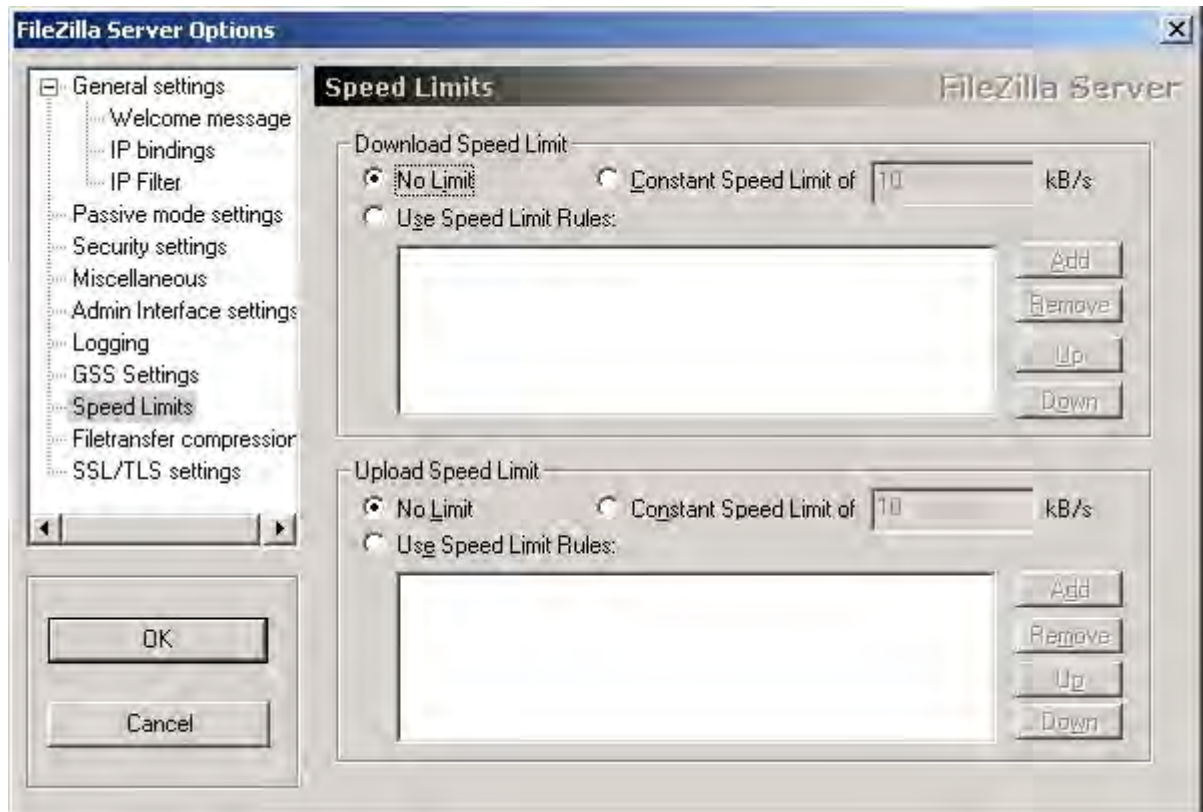
注意: 修改端口和密码非常重要, 这是确保 Filezilla 安全的重点, 必须修改端口, 必须设置密码! 密码建议足够复杂!

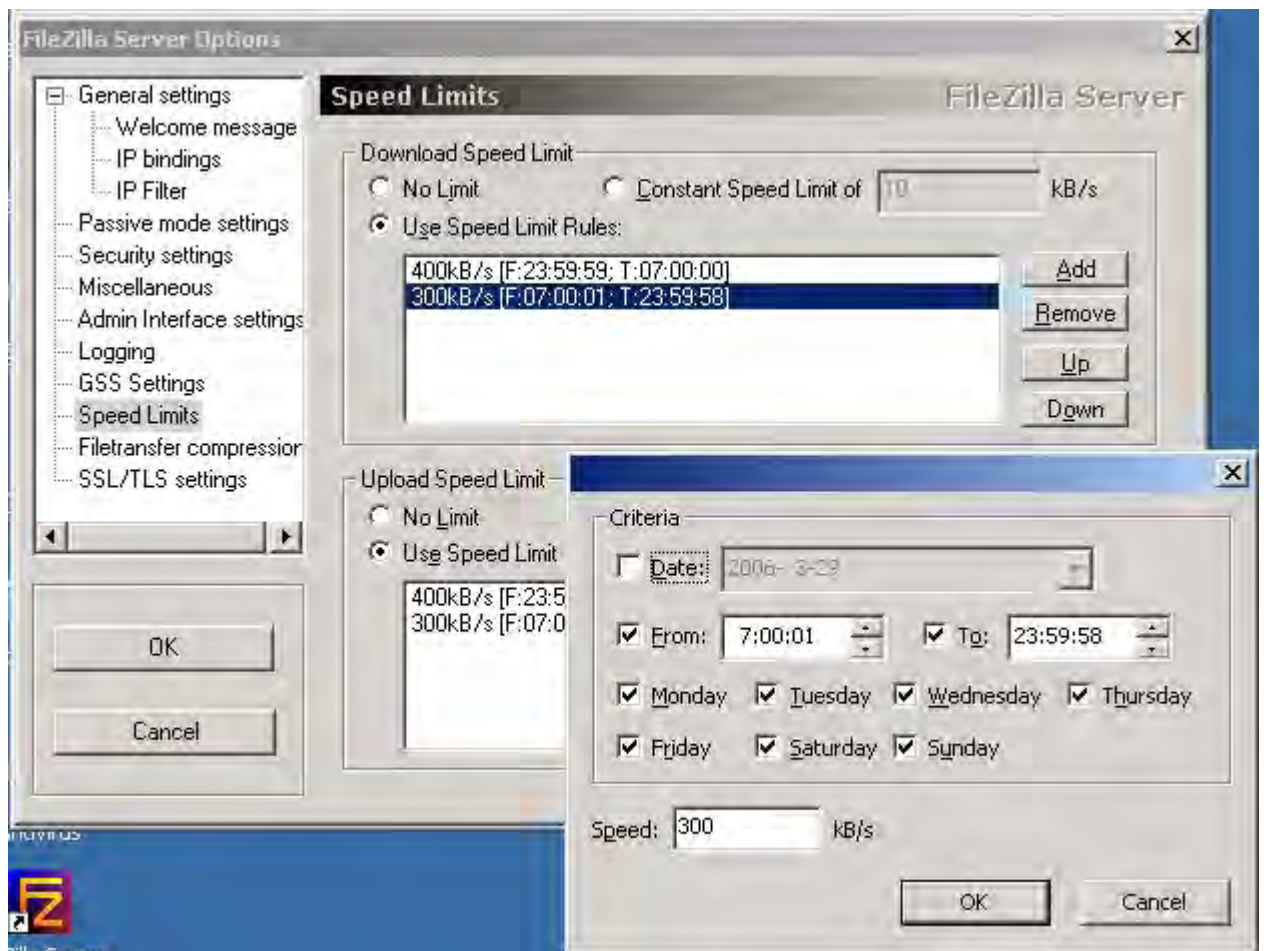


第 5 步 Logging (日志): 设定是否启用日志记录功能以及日志文件大小和文件名。



第 6 步 Speed Limits (速度限制): 这个是全局参数, 默认状态不限速。可以选中 “Constant Speed Limit of” 并填写限速数值来实现速度限制, 下载 (传出) 和上传 (传入) 可以分别设置。还可以根据时段自定义限速规则—— “Use Speed Limit Rules”, 比如这台服务器或者网络连接除了做 FTP 服务器之外还有别的用途, 需要根据时间调度, 不能让 FTP 传输挤占所有网络带宽影响其它的网络服务; 就可以通过这里设置。

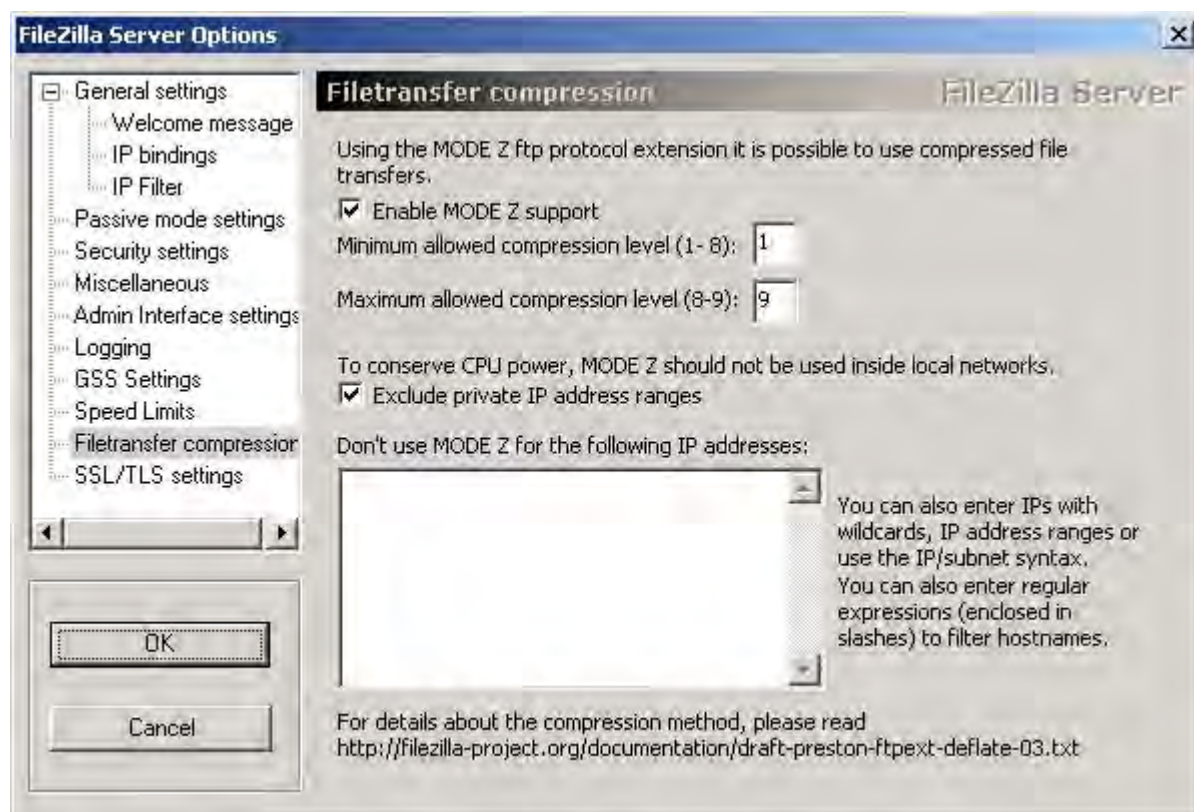




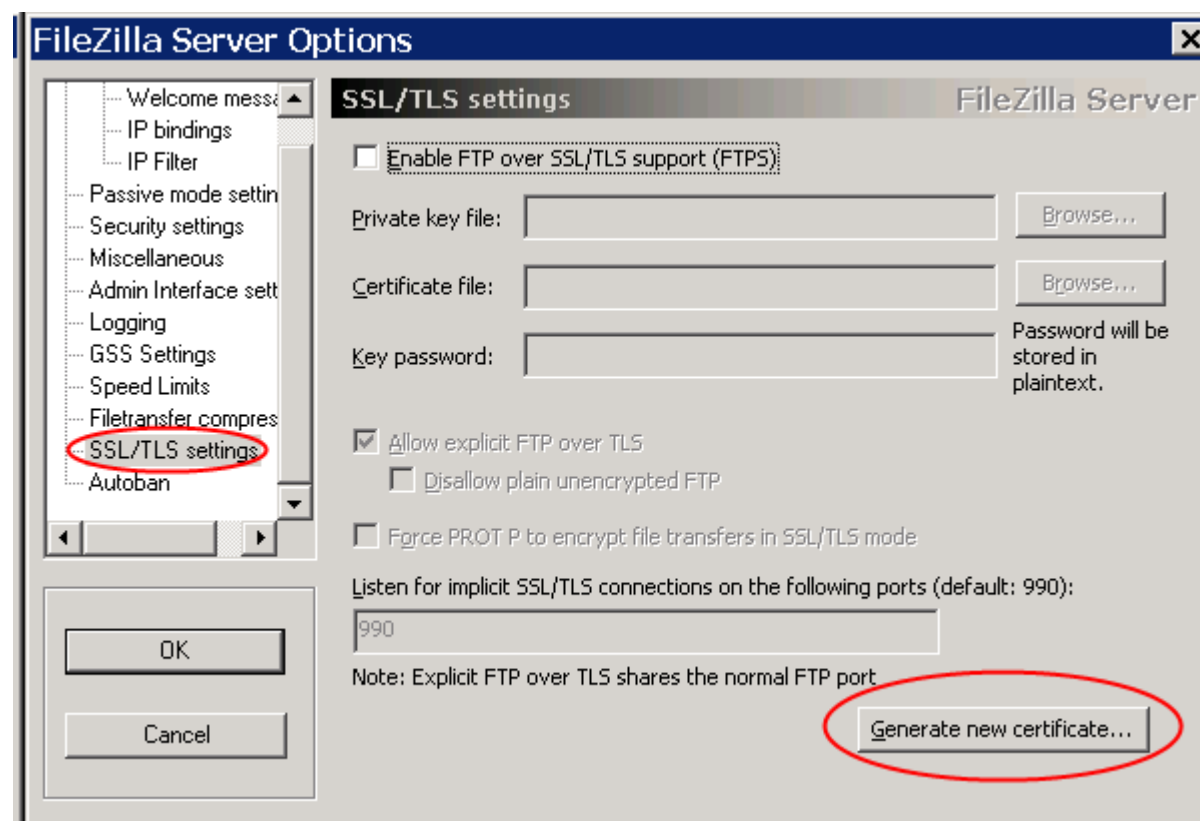
第 7 步 Filetransfer compression (文件传输压缩设置): MODE Z FTP 协议是一种实时压缩的传输协议。在这种模式下,发送方的数据在发出之前先进行压缩,再送到网络链路中传输,接收方将收到数据实时解包,在本地还原重组成原文件。这种模式可以大幅度减少网络中的数据流量,提升传输效率(速度)。当然对于已经压缩过的文件,就几乎没有效果了。要使用这种传输模式,需要服务器端和客户端都支持 MODE Z 协议。

勾选“Enable MODE Z support”就可以启用本服务器的 MODE Z 支持功能,这样,只要客户端也支持 MODE Z 就可以获得它带来的性能提升。“Minimum allowed compression level”和“Maximum allowed compression level”分别设置最小压缩率和最大压缩率。最下面可以输入不启用 MODE Z 功能的目标 IP。

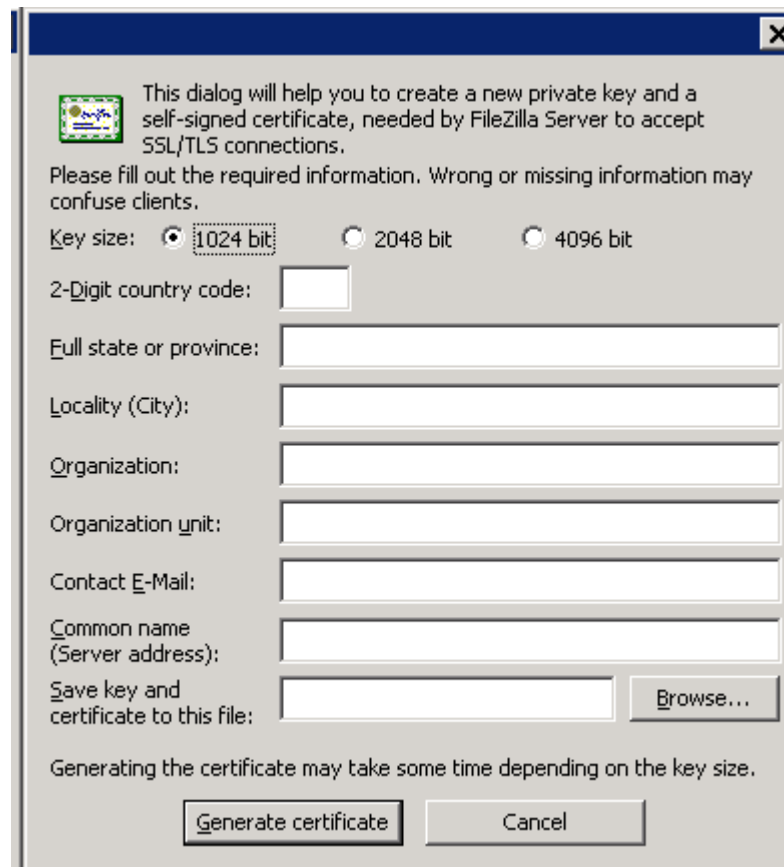
完成这些设置以后,点击“OK”按钮保存设置并退出服务器全局设置页面返回主界面。



第 8 步 设置“SSL/TLS settings”，



在弹出对话框中，输入国家代码、省、市、组织、联系邮件地址等，单击“Generate certificate”。



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

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

Key size: ☒ 1024 bit ☐ 2048 bit ☐ 4096 bit

2-Digit country code:

Full state or province:

Locality (City):

Organization:

Organization unit:

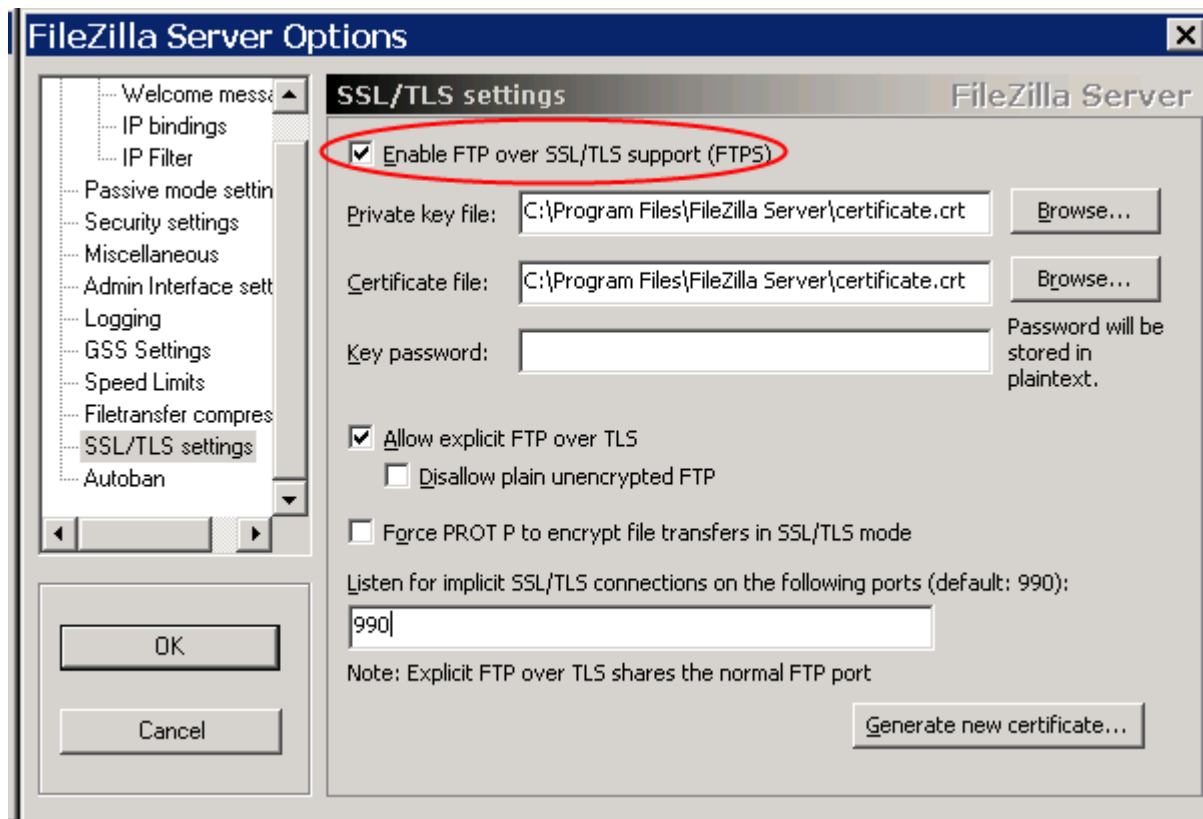
Contact E-Mail:

Common name (Server address):

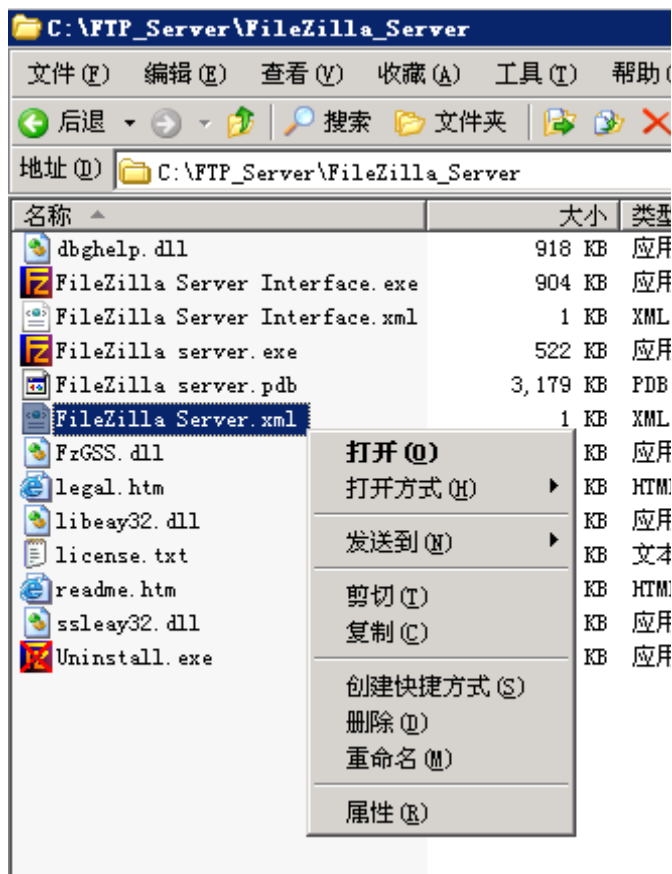
Save key and certificate to this file:

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

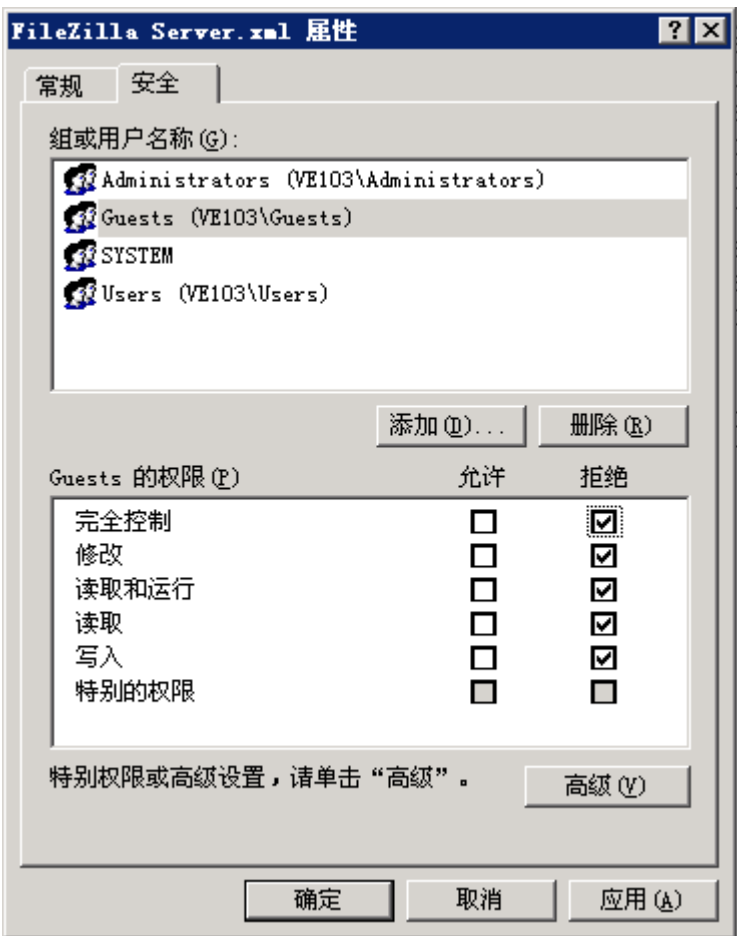
选中“Enable FTP over SSL/TLS support(FTPS)”



第9步 加固权限，找到Filezilla的配置文件，格式是xml格式，鼠标右键点击之，并选择属性。




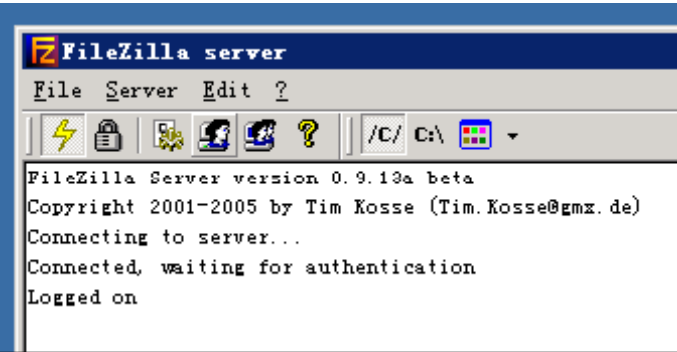
加入Guest组禁止读写的权限，设置为拒绝。



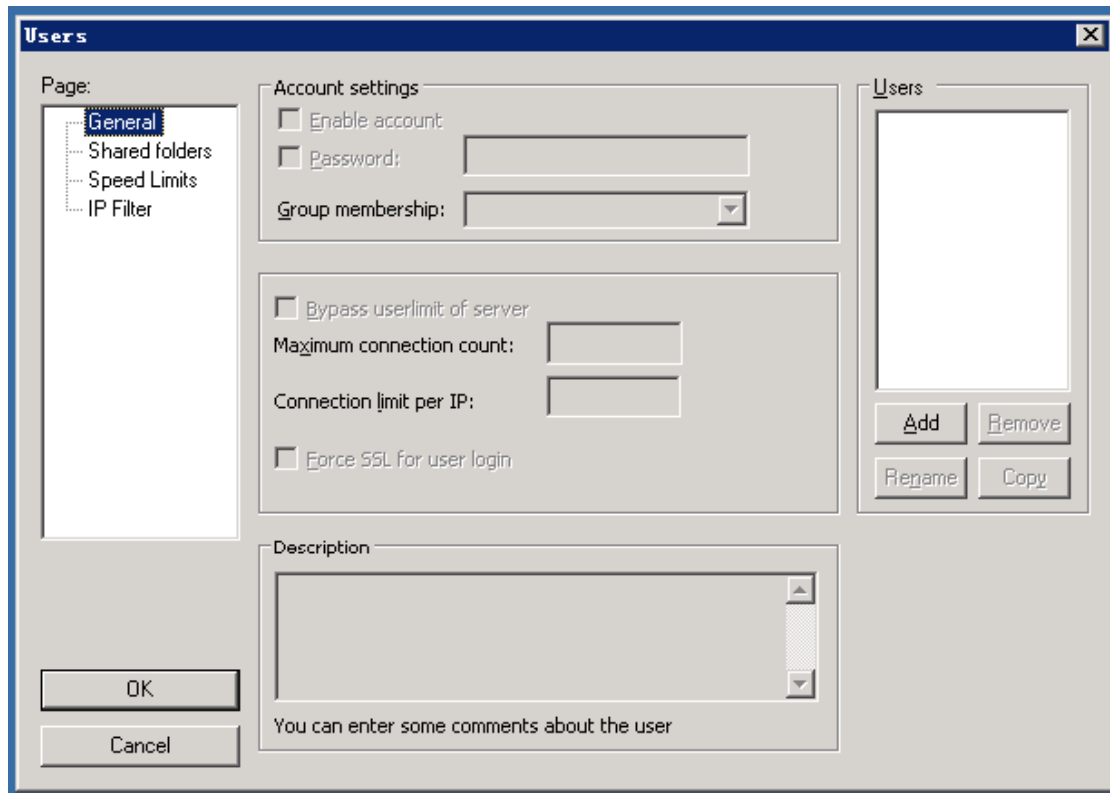
点击确定后，系统会弹出提示，询问拒绝权限优先级高于允许权限，是否要继续，点击是通过即可。

匿名FTP配置：

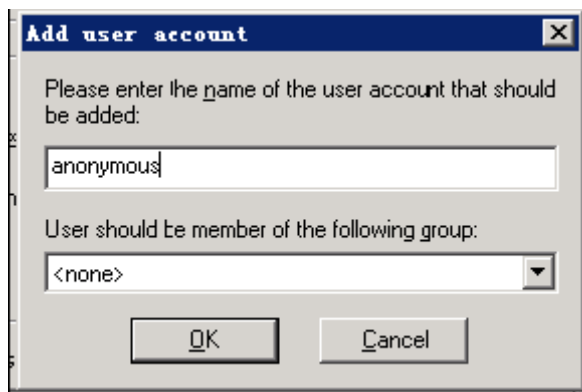
首先打开管理控制台，点击左起第四个图标  进入系统设置。



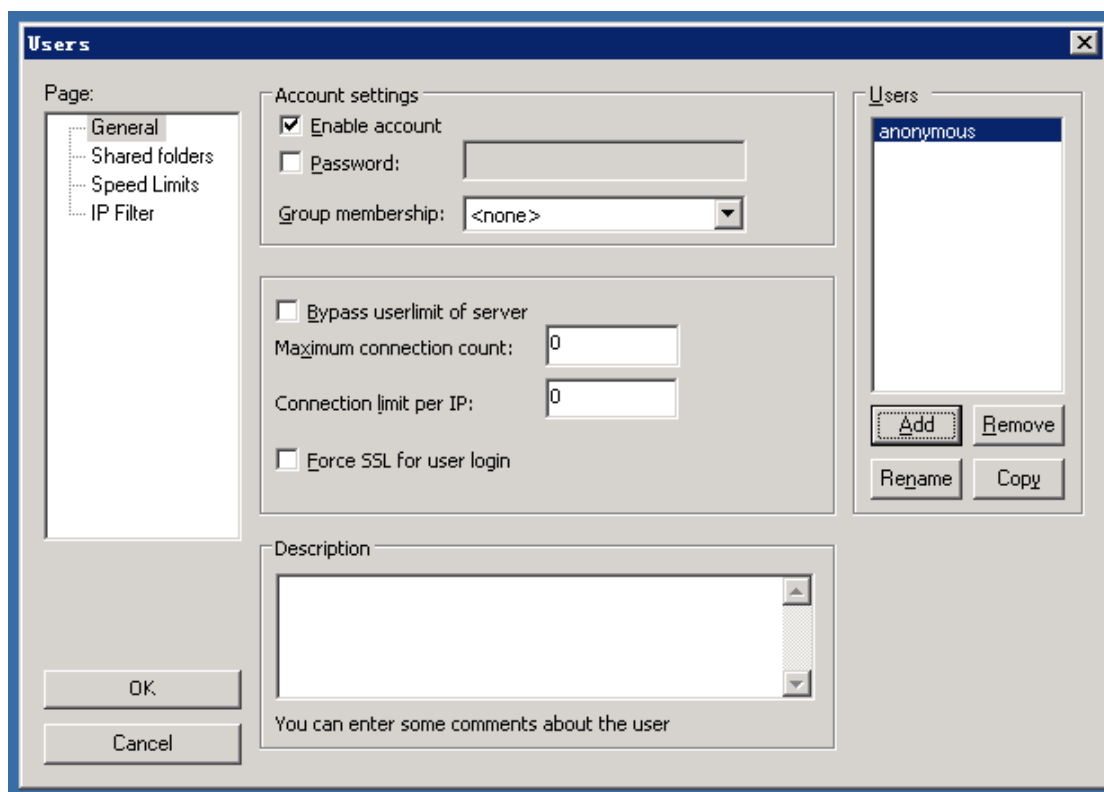
打开ftp用户管理界面，点击右侧的  按钮，添加新用户。



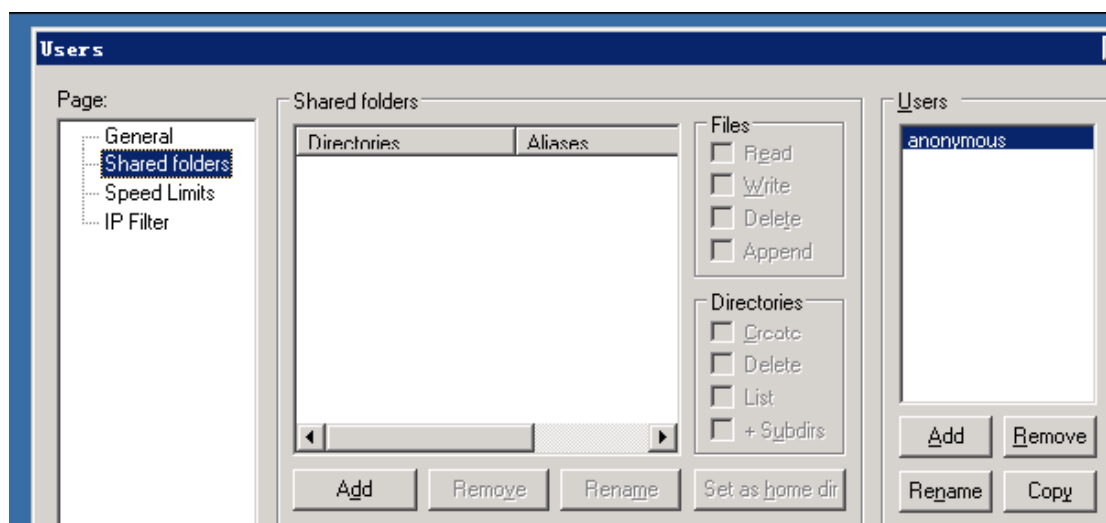
在新增用户的对话框中，输入“anonymous”这个名字，即FTP的匿名用户。



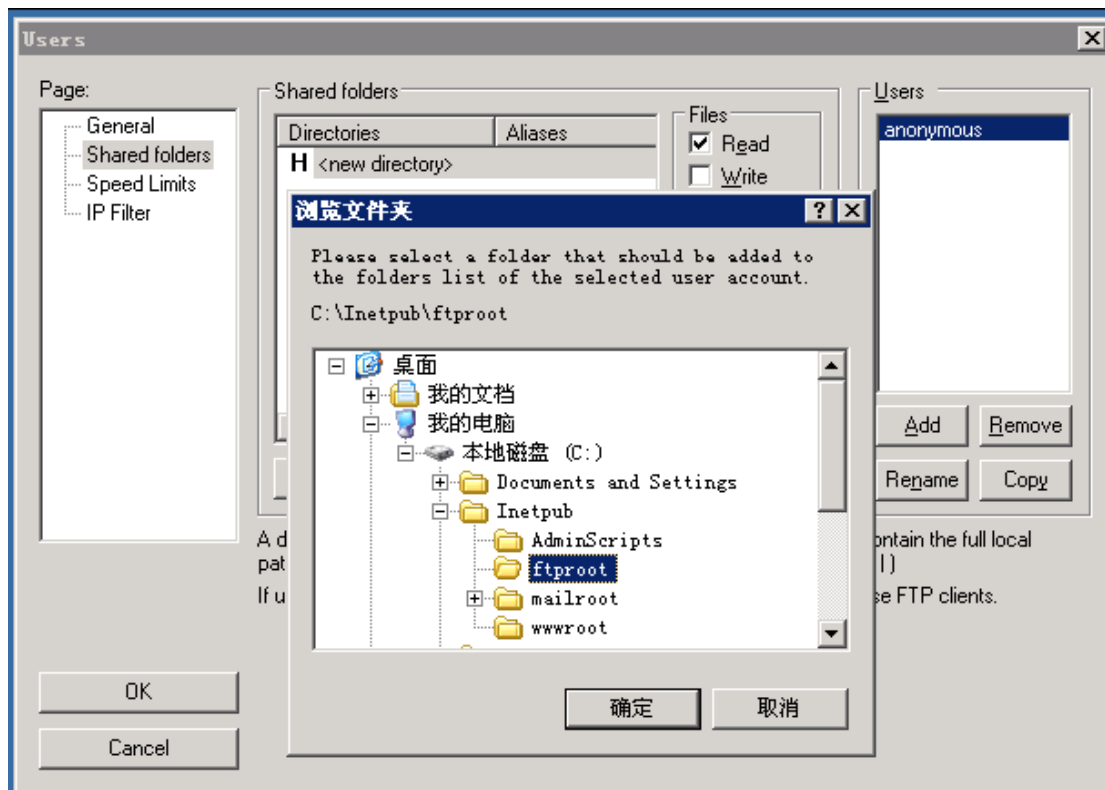
点击确认，添加用户完成，返回用户管理界面。



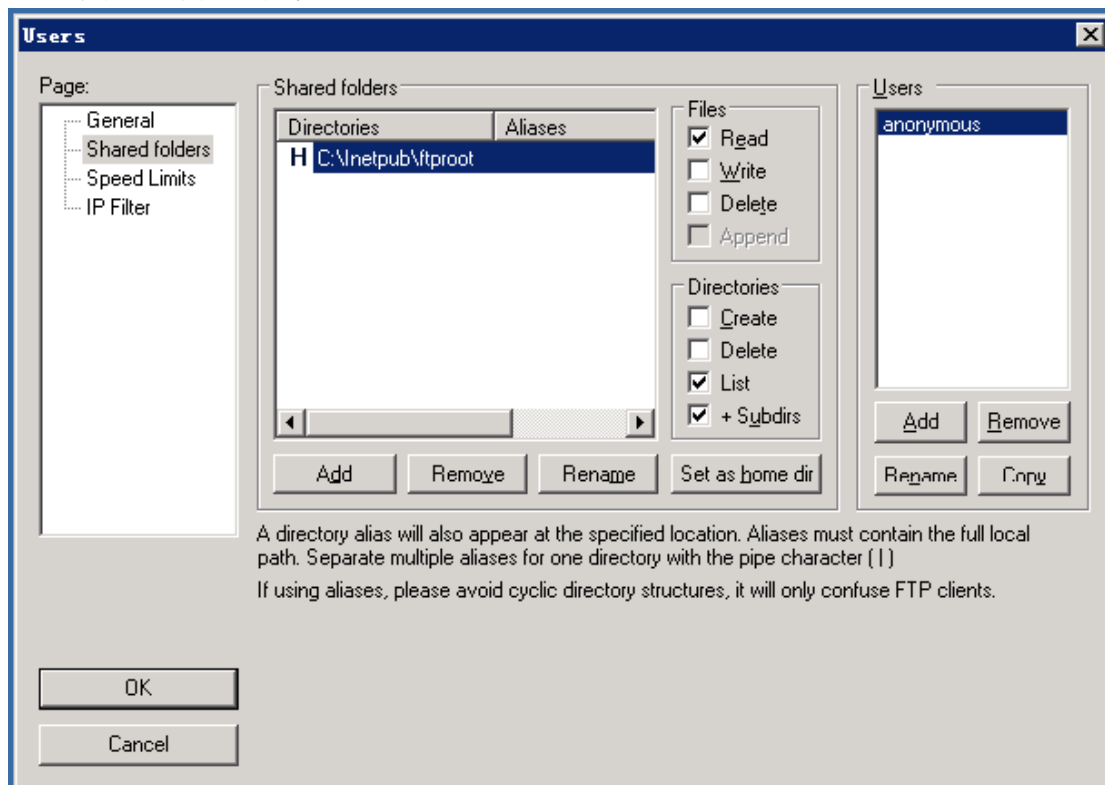
点击左侧的“Shared folders”菜单。点击Add按钮，添加一个目录。



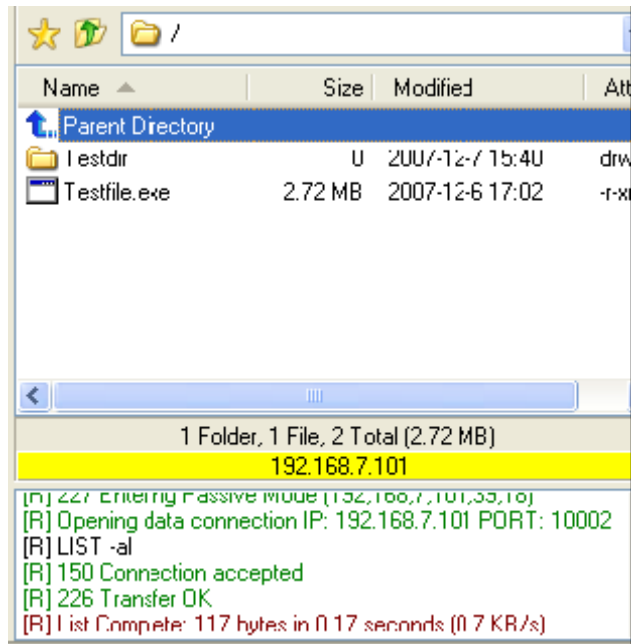
打开浏览文件夹的选项，选择要设置FTP的目录。



点击确定，添加用户完成。



现在用户FTP客户端连接到FileZilla Server上，可以看到匿名FTP已经配置完成。

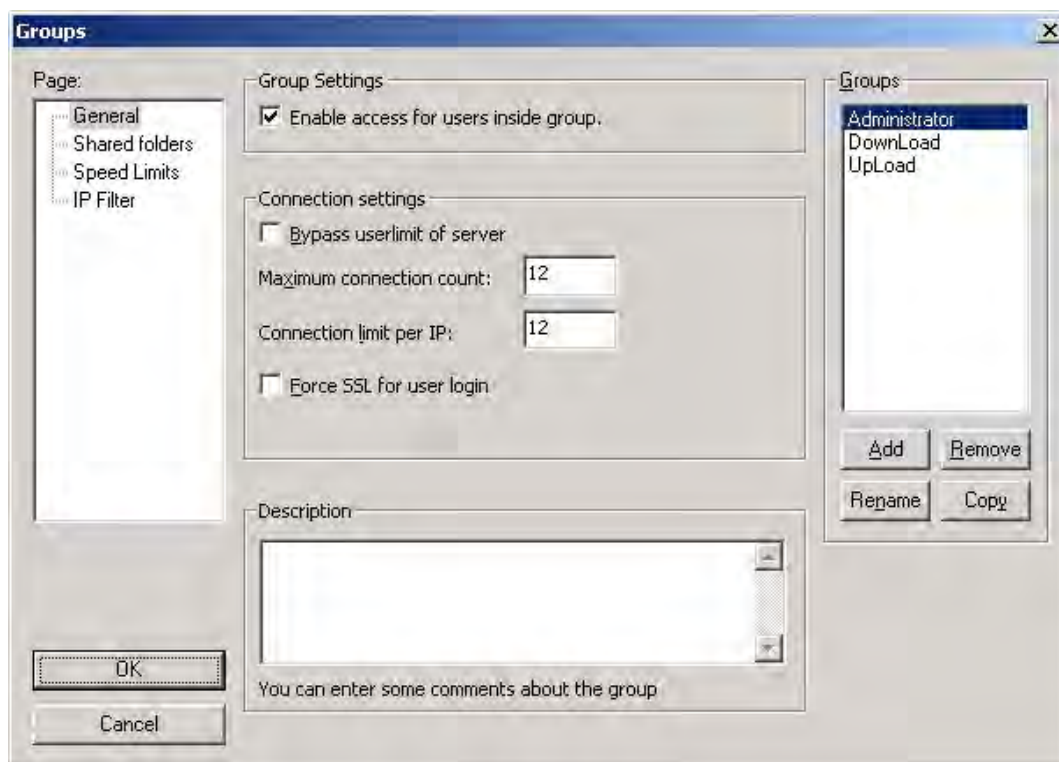


标准 FTP 用户配置：

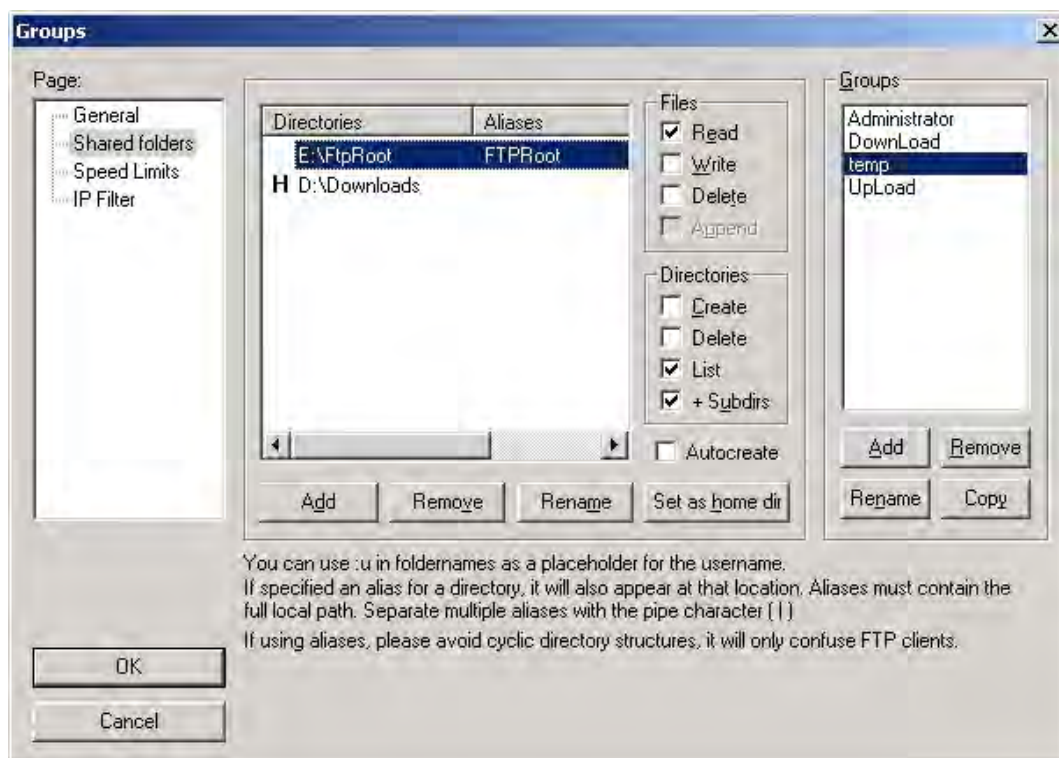
設定流程：開新帳戶→ 設定密碼→ 選定資料夾→ 設定完成。

第1步 进行的是用户组（Group Settings）设置。在主界面点击第五个按钮或者由“Edit”——“Groups”菜单进入。

组设置是为了便于用户归类管理，相同权限的用户归属到同一个组里面，这样就不用重复多次设置每个用户的权限等参数，简化配置和管理工作。点击右边的“Add”按钮创建新组。



组创建完成以后，点“Shared folders”进入目录权限设置页面。点击中间区域的“Add”按钮添加目录。默认状态添加的第一个目录即为该组用户登录之后看到的主目录（Home Directory），主目录前面有个粗体的“H”标识。目录列表右侧分别是对该目录的操作权限设置，上面是文件权限设置，下面是目录权限设置。如果要改变主目录，只要在列表中选中需要设置为主目录的那个，然后点击“Set as home dir”按钮即可。



设置好主目录之后，再点击“Add”按钮把其余的目录依次设置进来就可以了。不过这里得注意，如果仅仅把别的目录添加进去，那么你用客户端连接之后，会发现除了主目录和它的子目录之外，别的目录都看不见。这是怎么回事？这里要说明一个概念——虚拟路径。所谓虚拟路径，就是在客户端看到的目录结构。由于一个用户只能有一个主目录，别的目录如果不映射成虚拟目录的话，客户端将看不到它。所以只有把除了主目录之外的其它目录，虚拟成主目录的子目录，这样在客户端才能看到。

比如本例，主目录是 D:\Downloads，如果不做虚拟路径设置，那么客户端登录进来只能看到主目录里面的内容，还有一个 E:\FTPRoot 目录下面的东西看不到。如何设置虚拟路径？鼠标右键点击列表中的“E:\FTPRoot”目录，在弹出的菜单里面选“Edit aliases”编辑别名；现在要把 E:\FTPRoot 目录作为客户端主目录下的 FTPRoot 目录，那么就在弹出的窗口里面输入“D:\Downloads\FTPRoot”并点击“OK”按钮确定。注意拼写规则，路径的前面部分必须是主目录的绝对路径。这样设置之后，在客户端就可以看到一个“FTPRoot”目录，这个目录其实就是 E:\FTPRoot 目录。

组设置中的“Speed Limits”和“IP Filter”跟全局设置里面的速度限制和 IP 过滤器设置方法是一样的，请参照前面的内容。只不过这个是仅仅针对这个组的用户生效。而全局设置是对所有的用户都生效。设置完毕之后点击“OK”按钮回到主界面。

权限说明：

文件：

Files → Read：可下载档案。

Files → Write：可上传档案。

Files → Delete：可删除档案。

Files → Append：即把文件下载到本地副本并打开编辑，在关闭时再上传到服务器。（问题：不知道是不是在服务器端进行执行编辑。）

目录：

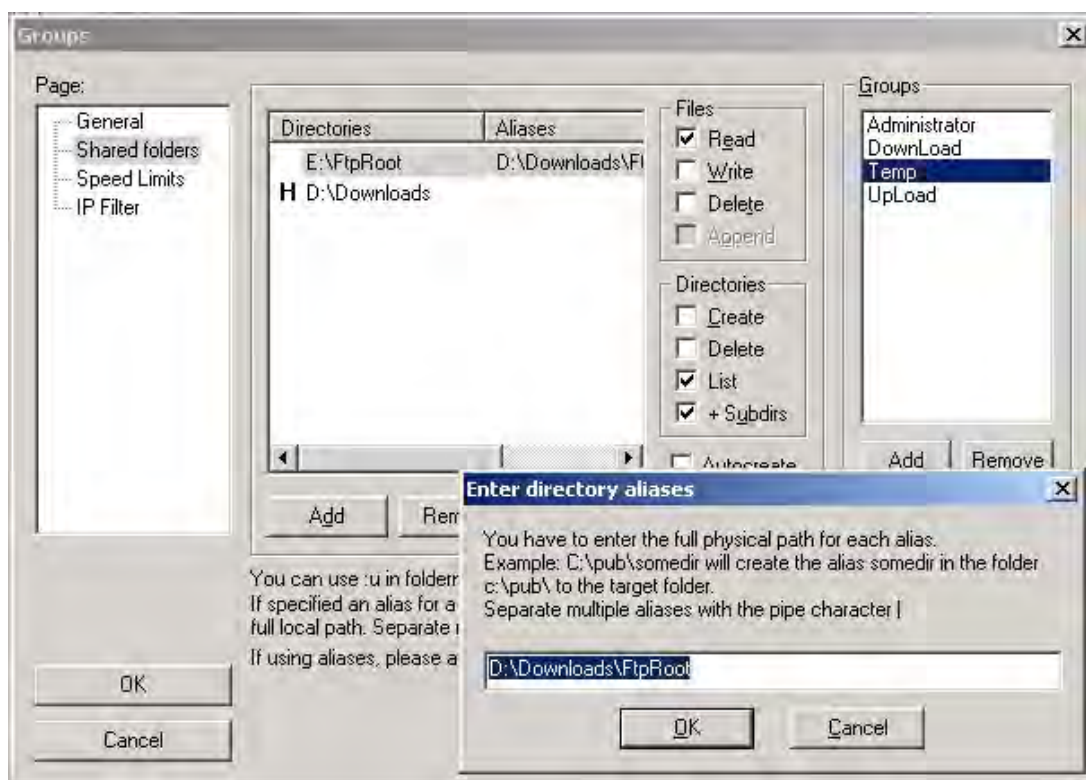
Directories → Creat：可新增子资料夹。

Directories → Delete：可删除子资料夹。

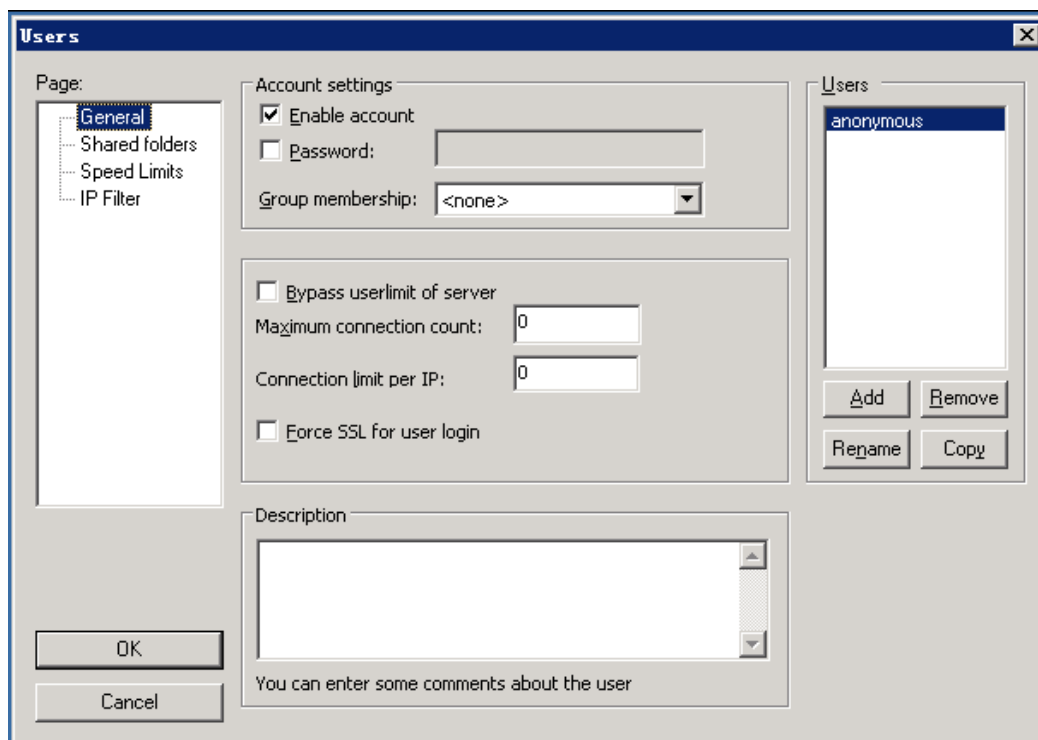
Directories → List：可列出资料夹中的档案。

Directories → +subdirs：列出文件夹中的子文件夹。

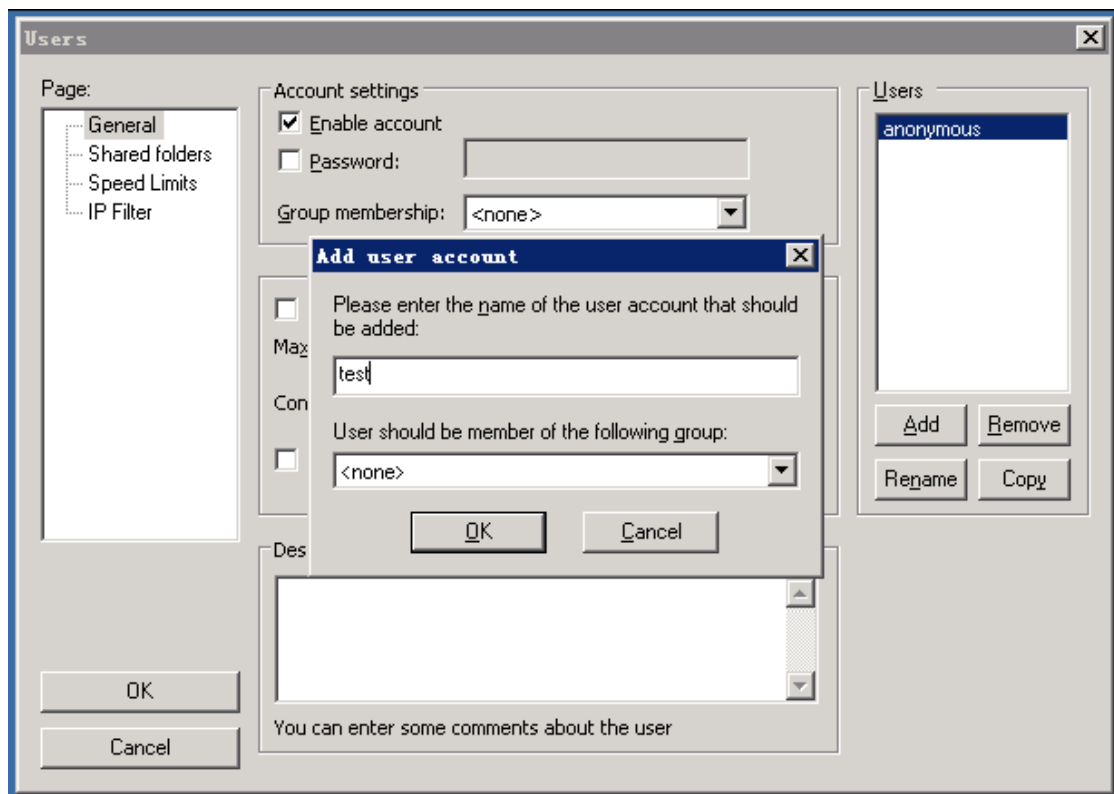
注意：在 FileZilla Server 里设置的对文件、目录的权限，需要依赖 Windows 操作系统中 SYSTEM 帐号对文件、目录的权限设置。



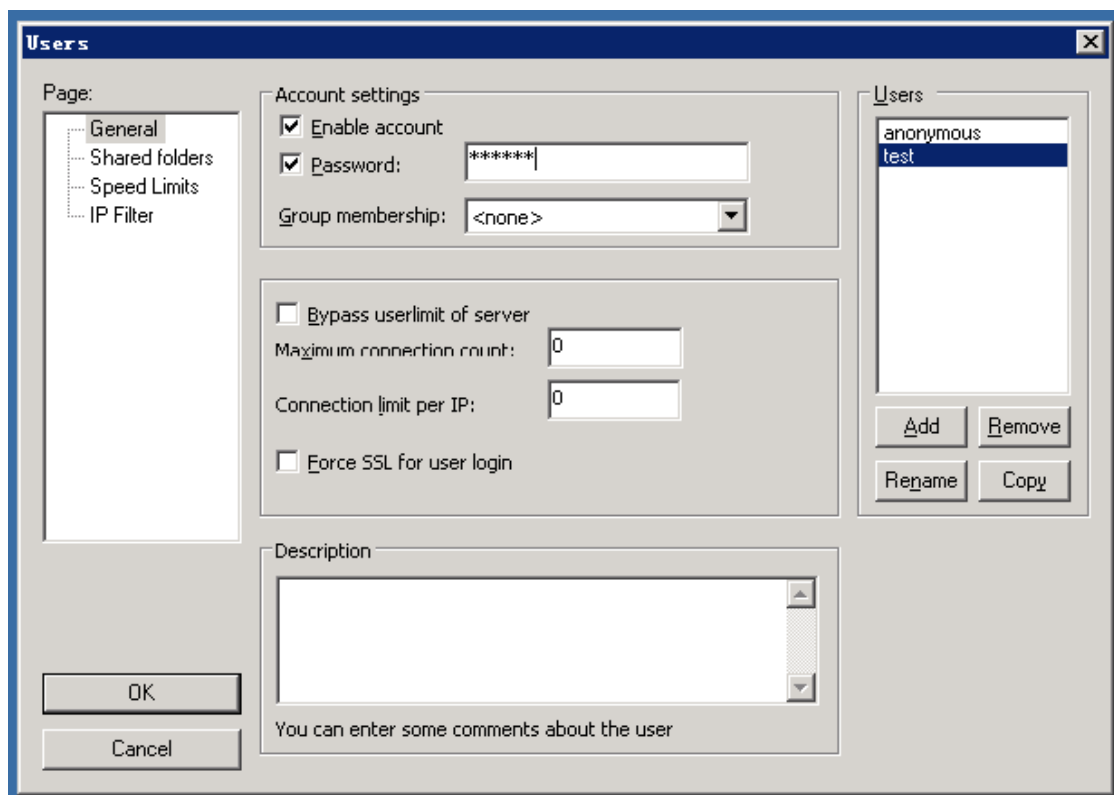
第 2 步 设置用户（Users）。点击主界面第四个按钮或者由“Edit”——“Users”菜单进入。



点击右边的“Add”按钮创建用户，输入用户名test。



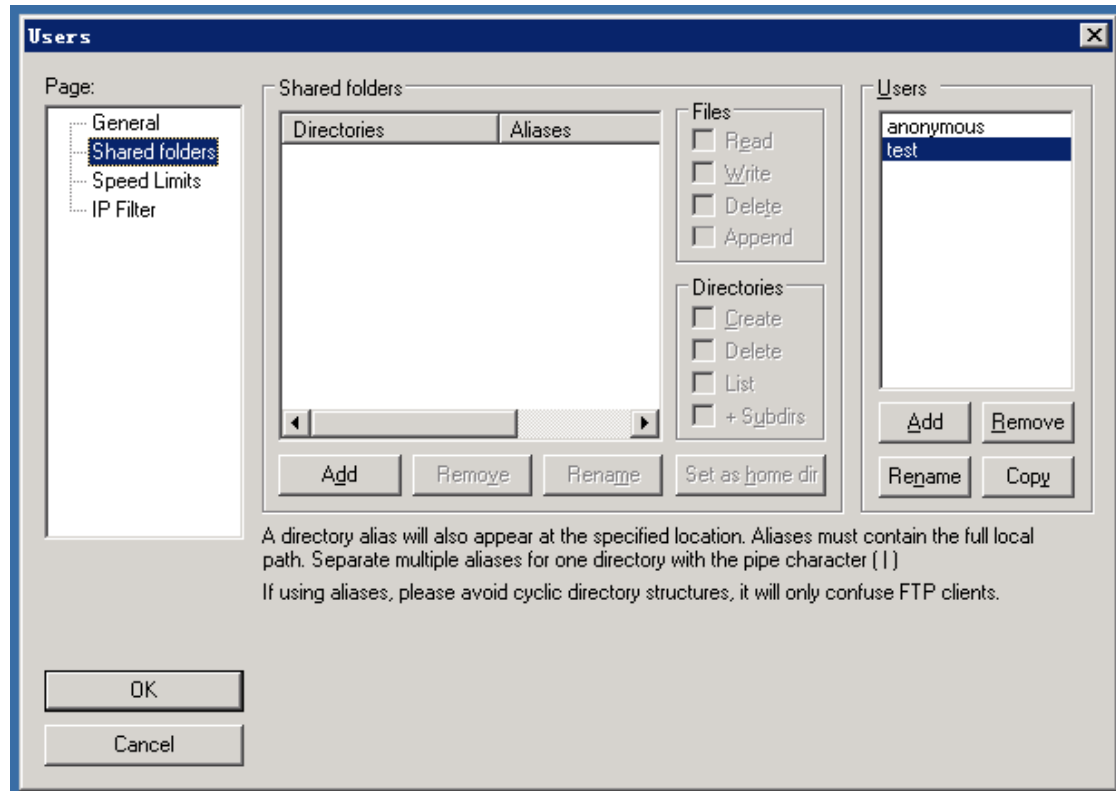
选中Password前边的多选框，然后输入密码123456。



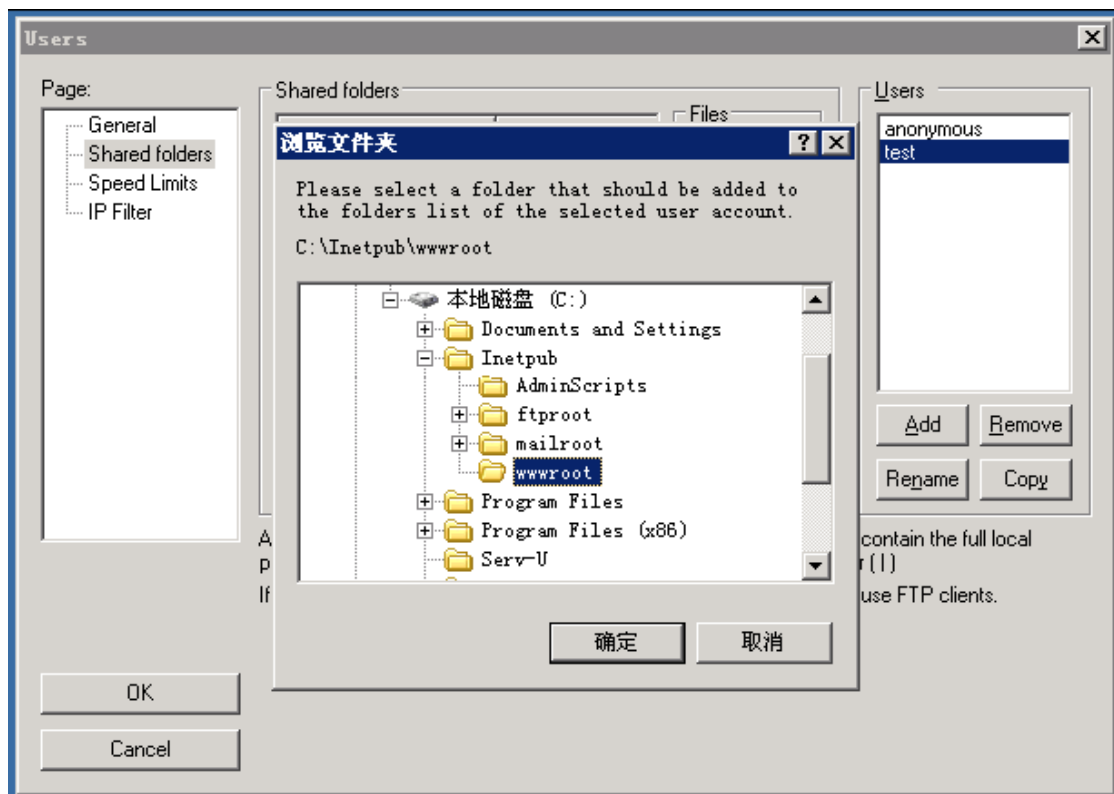
然后从“Group membership”栏选择该用户所属的组（Group），这样该用户将继承该组的所有属性/权限，不用再单独一一设置这些参数了。这也是设置组

体现的方便性，在用户比较多时候使用组来分类会使得管理工作更加方便、高效。当然，也可以设置一个不属于任何组的用户，这样的话，就得单独定制该用户的权限。对于少量特殊用户，可以用这种方式设置。

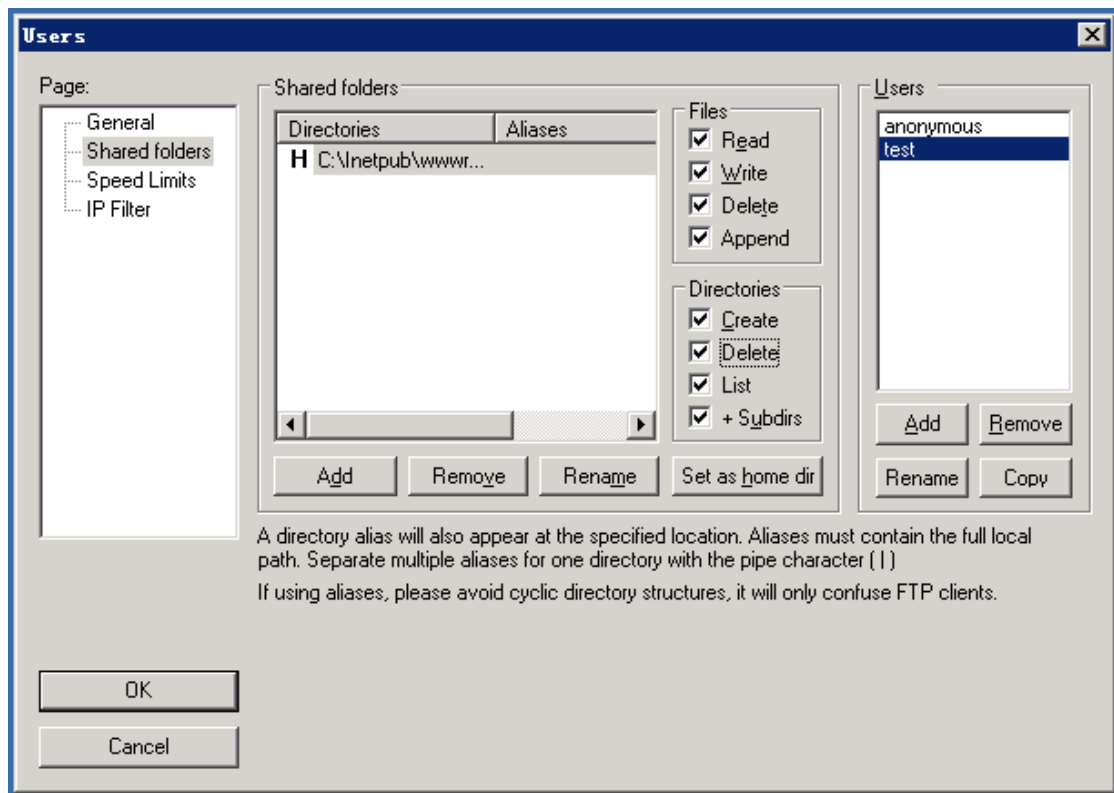
返回到用户管理界面，点击设置文件夹目录，点击Add添加目录。



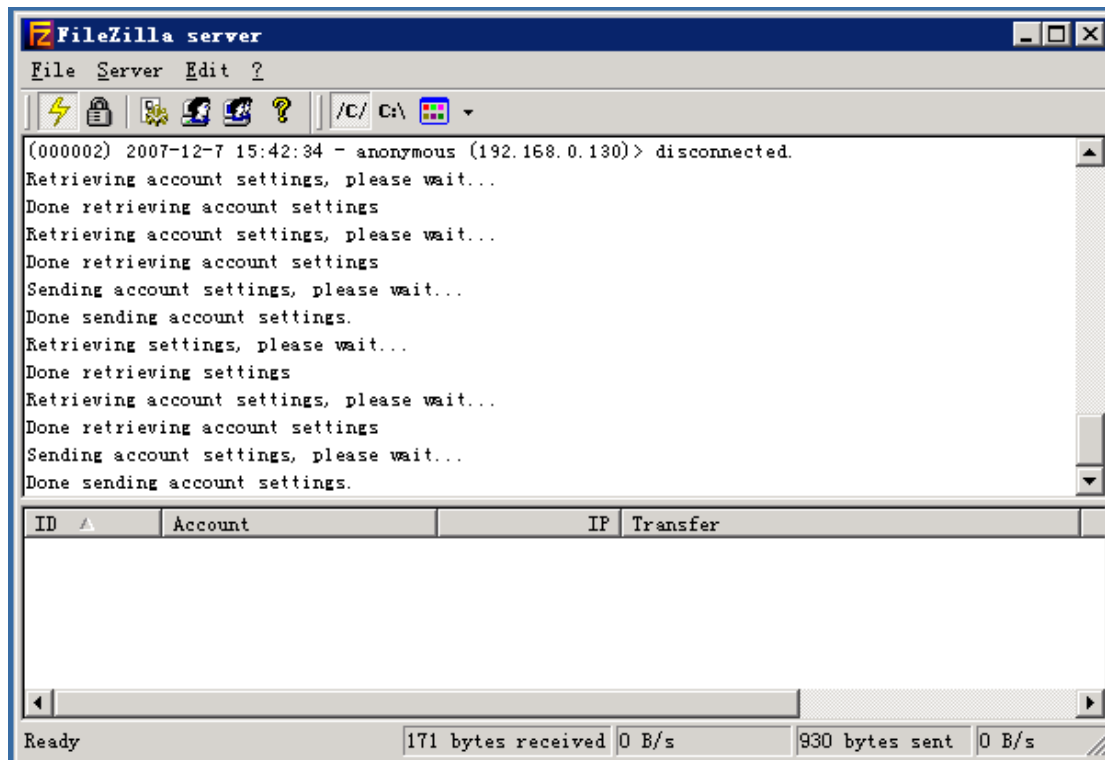
添加一个目录到test用户。



添加完成，再右侧选中test用户对这个目录的权限，然后点击左侧的OK按钮，配置完成。



配置完成。现在可以使用客户端来测试登录了。



打开FTP客户端软件，输入test用户名和密码123456，登录到服务器。

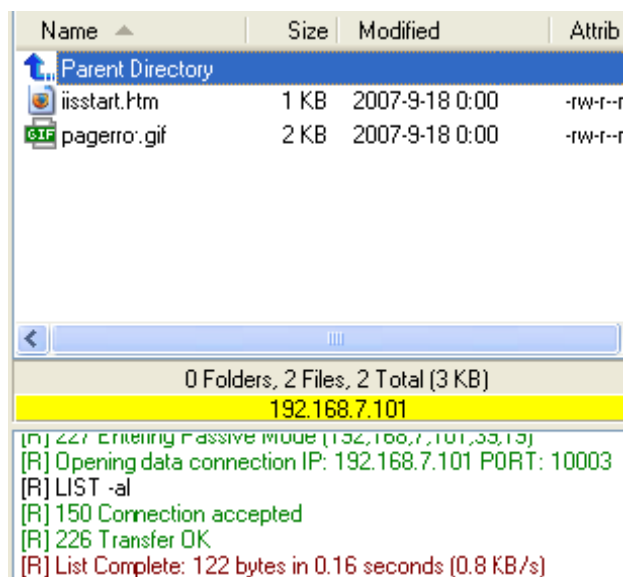
Server or Url: Port:

User Name: ☐ Anonymous

Password:

Remote Path:

登录成功后，可以看到刚才制定的FTP目录下的文件，并具有相应的上传、下载权限。

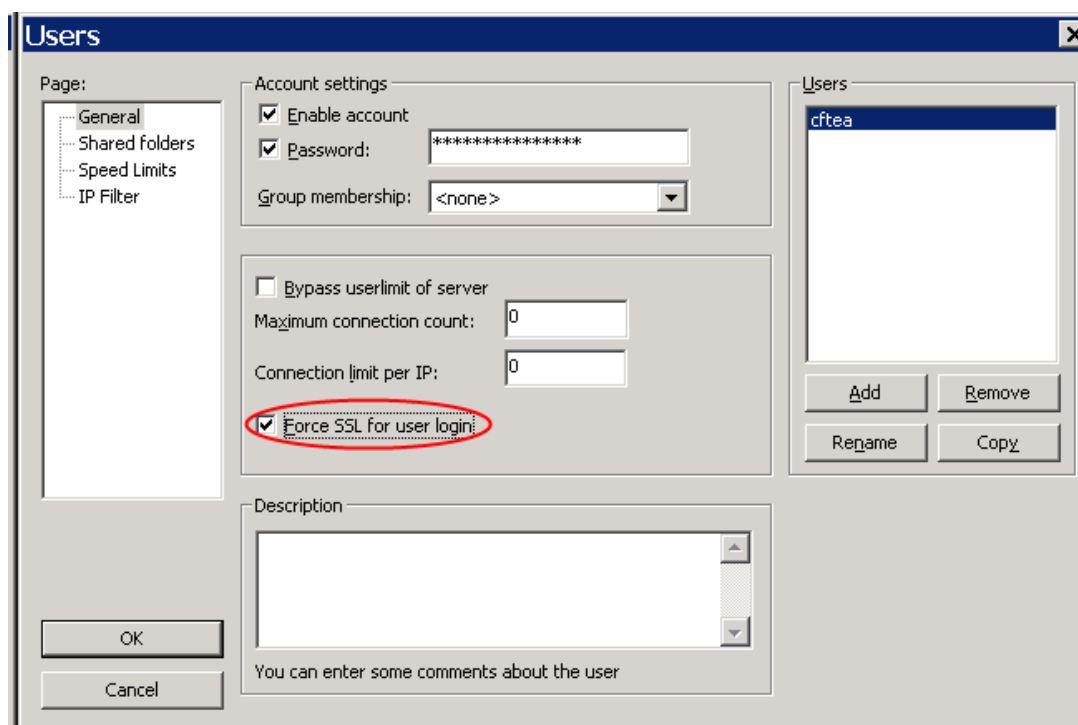


至此，FileZilla Server 的基本设置就完成并可以运行了。

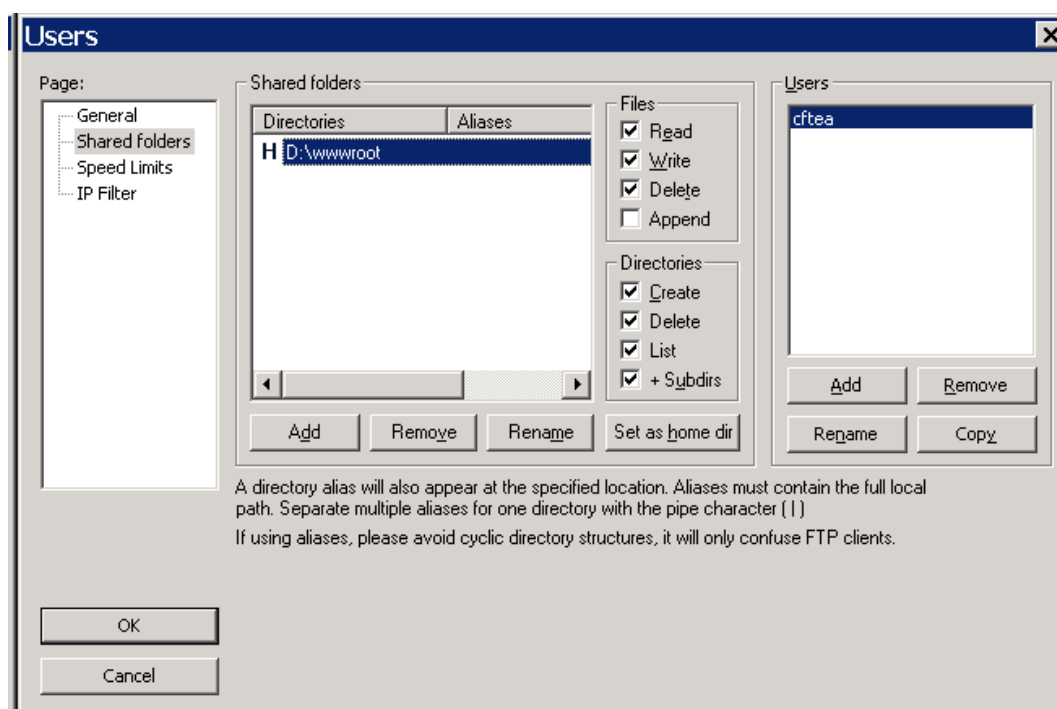


启用 SFTP 设置如下：

打开“Users”对话框：添加用户；输入密码；选中“Force SSL for user login”，目的是强制使用 SSL，当然如果不选的话，要不要使用 SSL，就由客户端自己选择了。



在“Shared folders”中添加 FTP 文件夹，并设置相应权限。



用 FileZilla Client 连接 FTP 服务器。和普通的连接相同，只是注意选择 Servertype，如下图：

The image shows a configuration window for an FTP client with four tabs: General, Advanced, Transfer settings, and Charset. The General tab is active. It contains the following fields:

- Host: 10.50.0.4
- Port: (empty)
- Srvtype: FTPS - FTP over implicit TLS/SSL (This dropdown menu is circled in red)
- Logontype: Normal
- User: cftea
- Password: (masked with asterisks)
- Account: (empty)
- Comments: (empty text area)

对于初次使用 FTP Server 软件的用户，本文也可以作为入门参考。其实所有的 FTP Server 软件安装设置的基本原理都是类似的，掌握了一个之后，别的可以举一反三融会贯通。