

FileZilla Server

使用手册

目 录

| | |
|-----------------------------|----|
| FileZilla Server 使用手册 | 1 |
| 一、 简介..... | 3 |
| 二、 安装..... | 4 |
| 三、 配置..... | 8 |
| 1. 基本设置..... | 8 |
| 2. 匿名FTP配置..... | 12 |
| 3. 标准FTP用户配置..... | 15 |
| 4. 虚拟目录配置..... | 19 |
| 5. 加固Filezilla安全 | 23 |

一、 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，目前其客户端软件 Filezilla Client 3.0 有着非常广泛的市场。

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。开源为何能保证安全？每一款软件产品诞生后，都有很多人试图发现其漏洞进行攻击，以获取权限和其他利益。如果是开源软件，攻击者就会下载这个软件的源代码，从源头上分析其内部漏洞在那里，并且进行攻击。开源的规模越大，下载阅读其源代码的人也多，这个软件也就越普及。随着其逐渐改进，漏洞就越来越少，最后成为了公认极其安全的软件，这和互联网中数万程序员的贡献是分不开的。这类软件的代表就是 Linux 平台下的 Apache、PHP、MySQL、Bind、Vsftpd 等大量高可靠性软件。而不开放源代码的闭源软件，人们无法对其进行研究，因此，只能将他当作“黑盒”来研究，研究的过程中没有源代码，很难找到其错误。即便找到了一些错误，还有更多的漏洞隐藏在代码中，但是因为代码不公开，因此人们短期内无从发现，后期使用会暴露出很多问题。一些闭源软件甚至保留有“后门”，以方便远程遥控，比如 Windows，比如 Serv-U。而开源软件代码是开放的，如果开发者在里边植入“后门”等危险代码，就会被互联网上广大的程序员揪出来，因此，这里也可以看出，开源，是对安全的最好保证。

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。

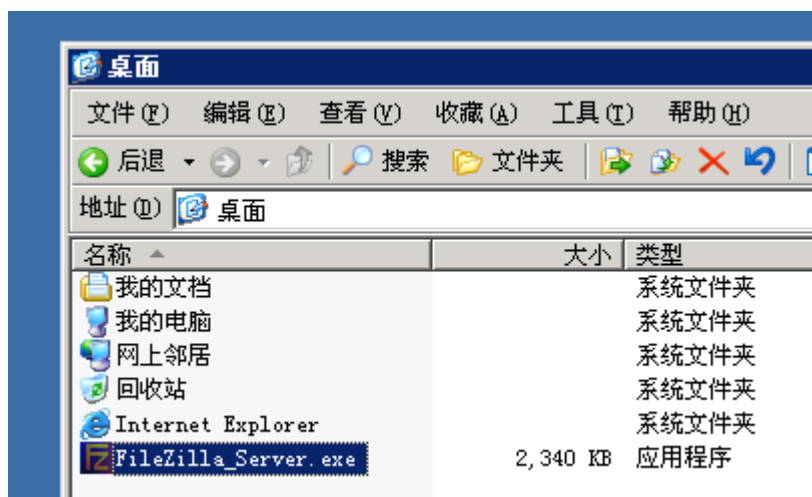
目前 Filezilla 也存在一些不足，主要缺点就是不支持配额，即本身不提供上传、下载总文件大小配额的功能。即便如此，免费的 Filezilla 正越来越多的占领原来 Serv-U 等软件的市场，变得更加贴近用户了。

二、 安装

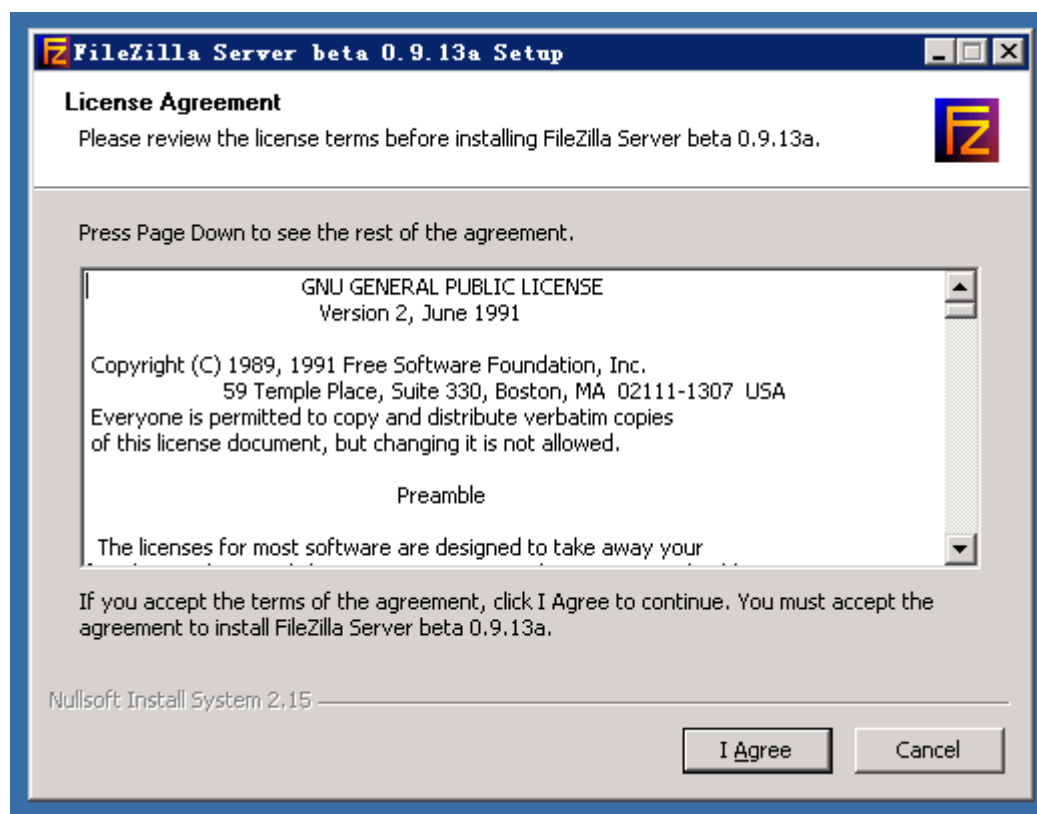
安装过程非常简单，首先下载 Filezilla Server 安装文件，如果觉得去国外英文官方网站下载速度慢，也可以从这里下载：

下载地址：http://www.swsoft.com.cn/temp/FileZilla_Server.exe

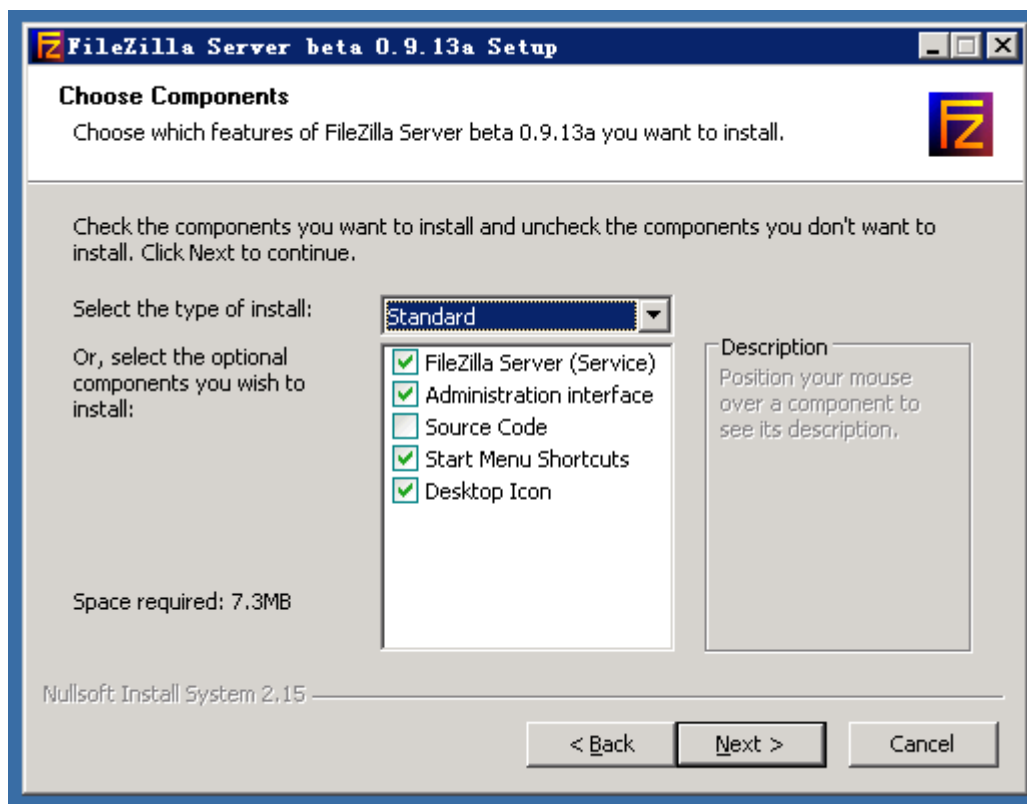
将安装包下载到桌面，准备安装。



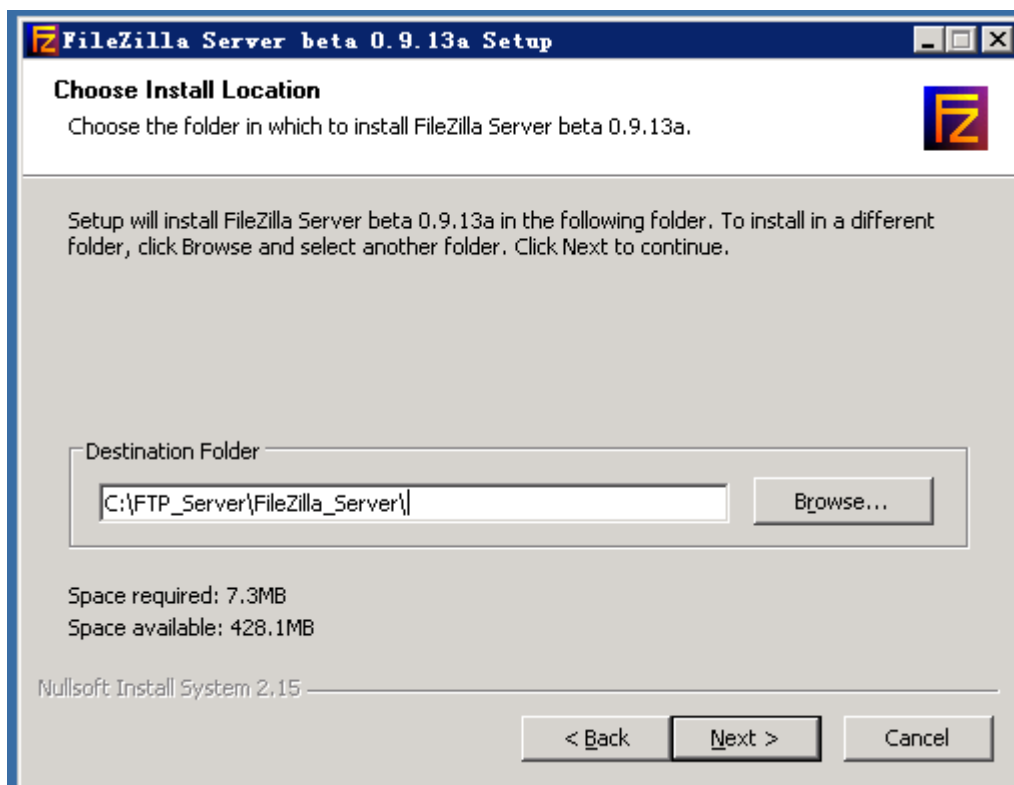
双击安装程序开始安装。点击“I Agree”继续。



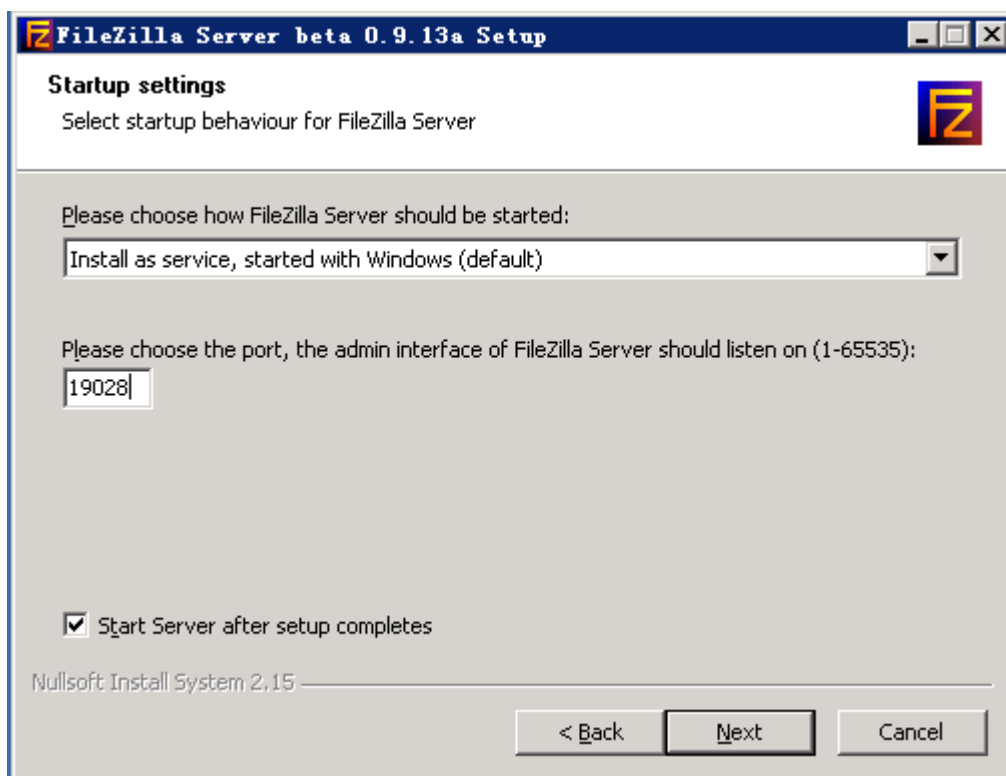
选择安装方式，默认的标准即可。其中“Source Code”源代码一般不用安装，除非是想研究 FileZilla 的代码。



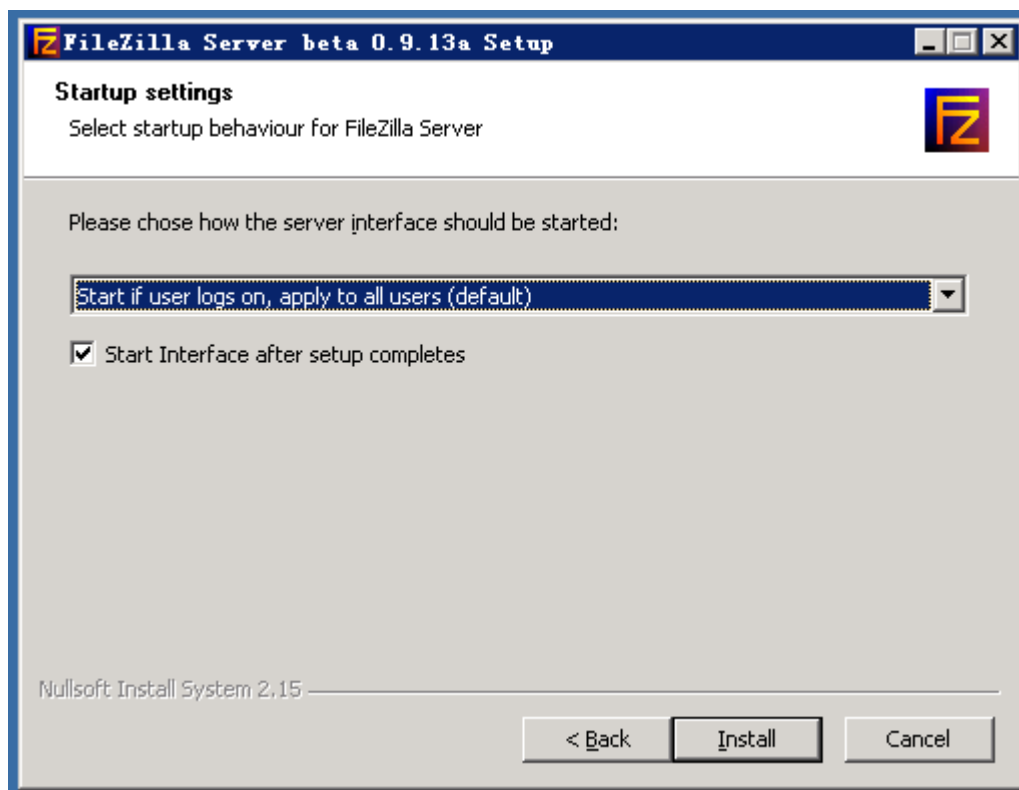
选择安装路径，强烈推荐安装到非默认路径，以增加安全系数。例如如下路径：



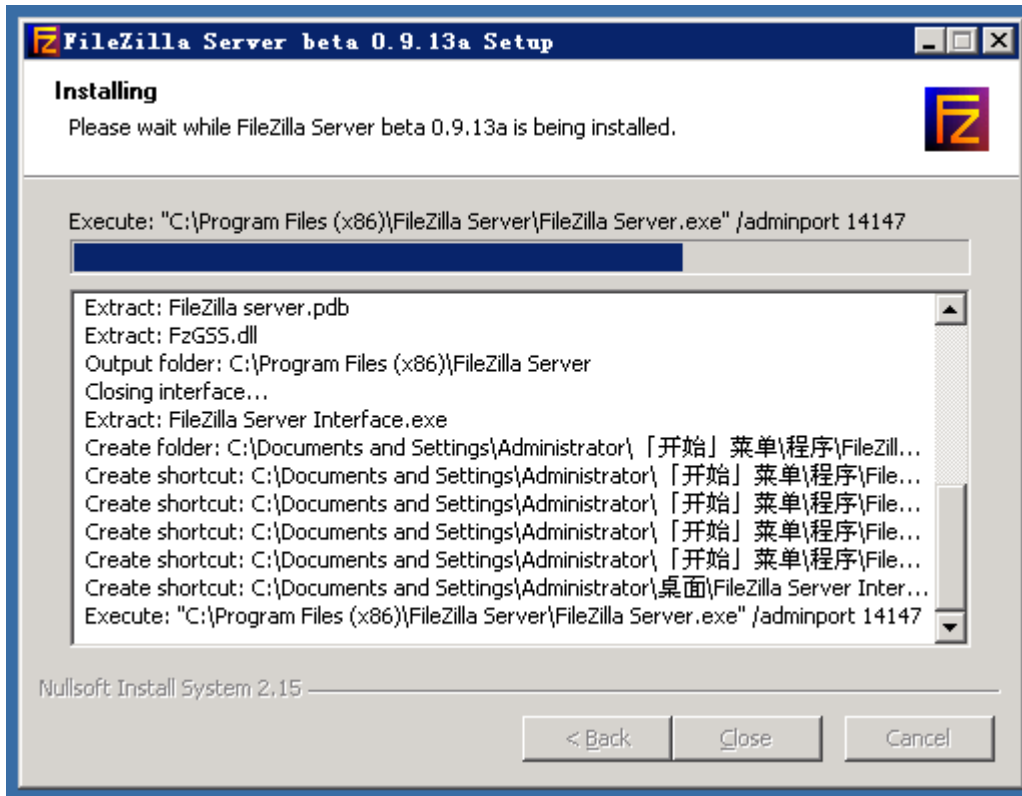
选择“安装为服务，并随机自动启动”的选项。下边的 14147 是管理端口，强烈推荐修改此端口，例如改成 38121 端口。（注意不要和常见服务如 80 端口冲突）。



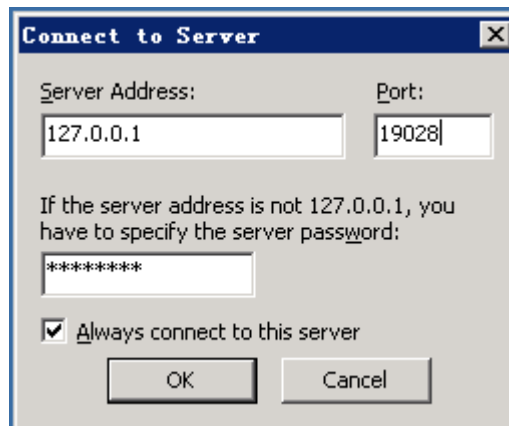
选择“当管理员登录时候，启动管理界面”的选项。



安装进行中。

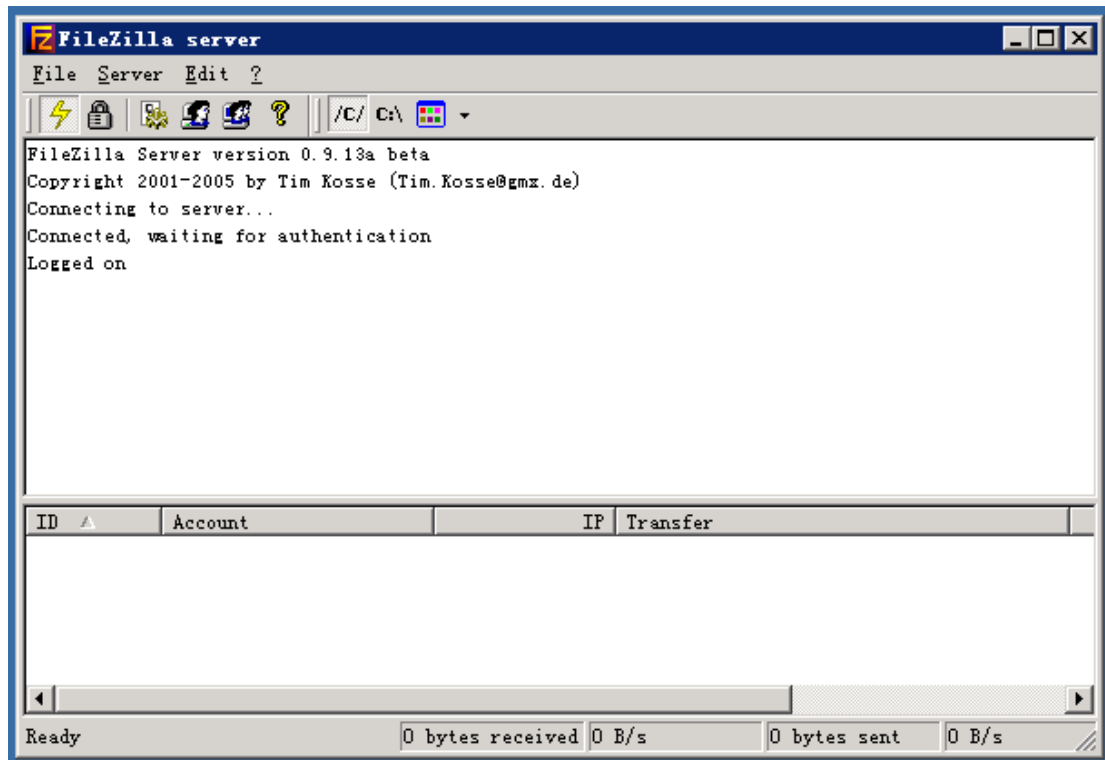


至此安装完成，安装程序自动启动管理控制台，默认是连接到本机的管理端口。管理端口到底是多少，请参考前文安装过程中填写的具体数字是多少。建议选中“总是连接到本服务器”的选项，即表示每次启动管理控制台，都是管理本机的 Filezilla 服务。下边有一个输入密码的对话框，在里边输入本服务器 Filezilla 服务的密码。




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！

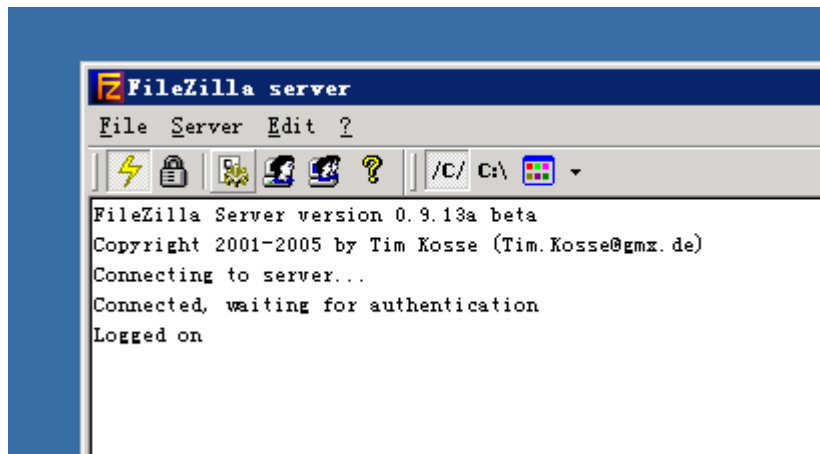
点击 OK 后，即可启动初始化之后的管理控制台，配置完成。



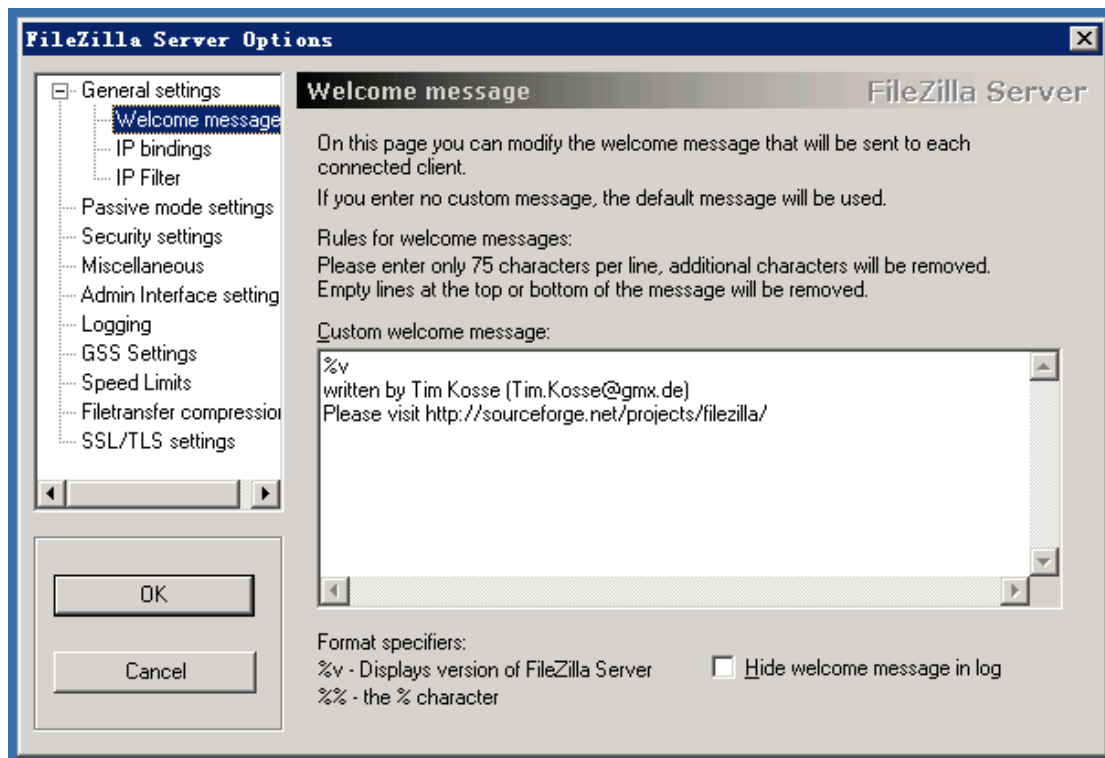
三、 配置

1. 基本设置

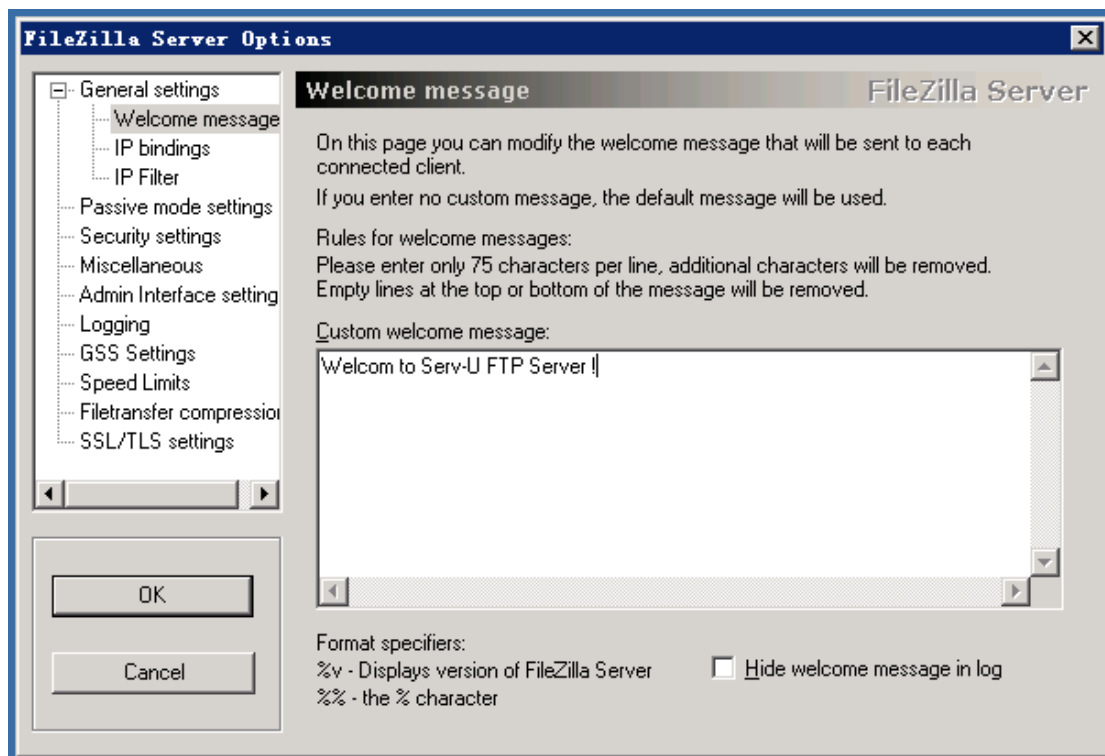
Filezilla 默认的模式是 Port 模式，不是 Passive 被动模式。为了解决防火墙后的客户端连接问题，最好是启用 Passive 模式。要启动被动模式，首先打开管理控制台，点击左起第三个图标  进入系统设置。



点击左侧“Welcome message”菜单，即 FTP 登录后的欢迎信息。



为了安全起见，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！**

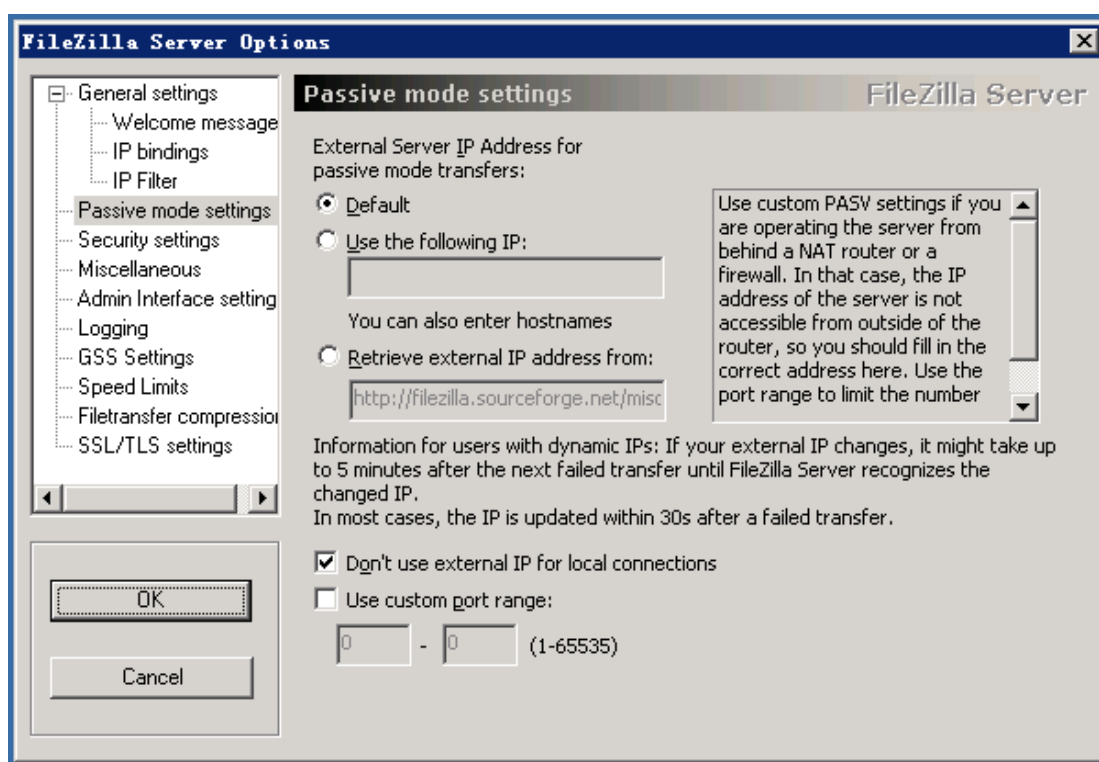


现在我们用 telnet 去连接一下 FTP 的 21 端口，即可看到修改过的“假”的提示信息，这样服务器的安全性可以得到比较明显的提高。

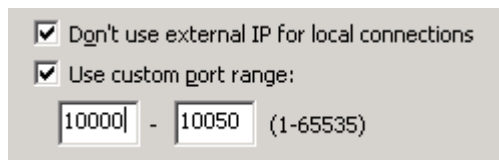
```
CA 命令提示符 - ftp 192.168.7.101

C:\>ftp 192.168.7.101
Connected to 192.168.7.101.
220 Welcom to Serv-U FTP Server !
User <192.168.7.101:(none)>: _
```

接下来点击“Passive Mode Settings”选项，进入被动模式设置。



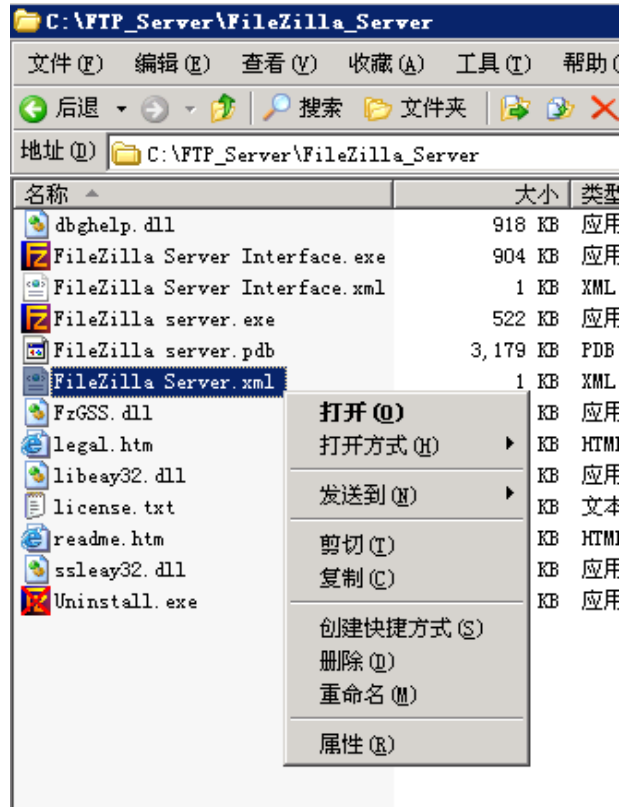
选中启动被动模式端口范围的选项，输入 10000~10050 端口范围，表示被动模式将要使用这个范围的端口。



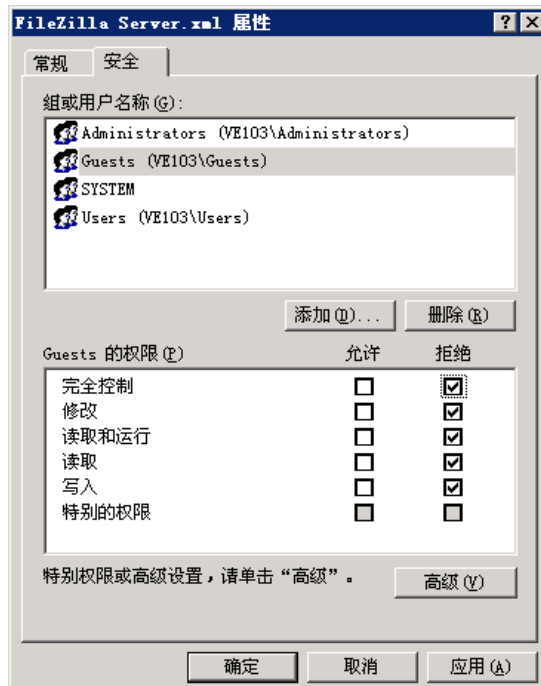
点击确定保存即可。接下来在防火墙上允许 10000~10050 端口范围进出，或者

直接允许 Filezilla server.exe 主程序的互联网访问。

安装的最后一步是加固权限，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。

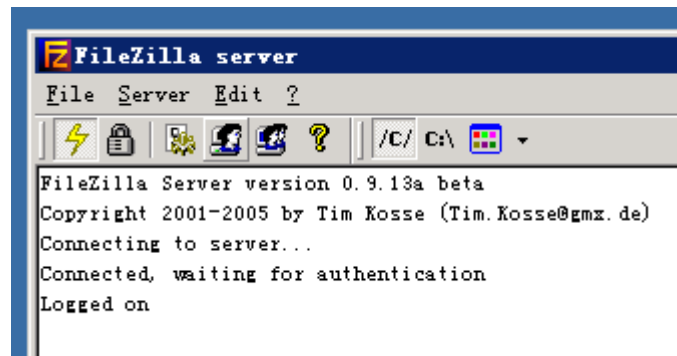


点击确定后，系统会弹出提示，询问拒绝权限优先级高于允许权限，是否要继续，点击是通过即可。

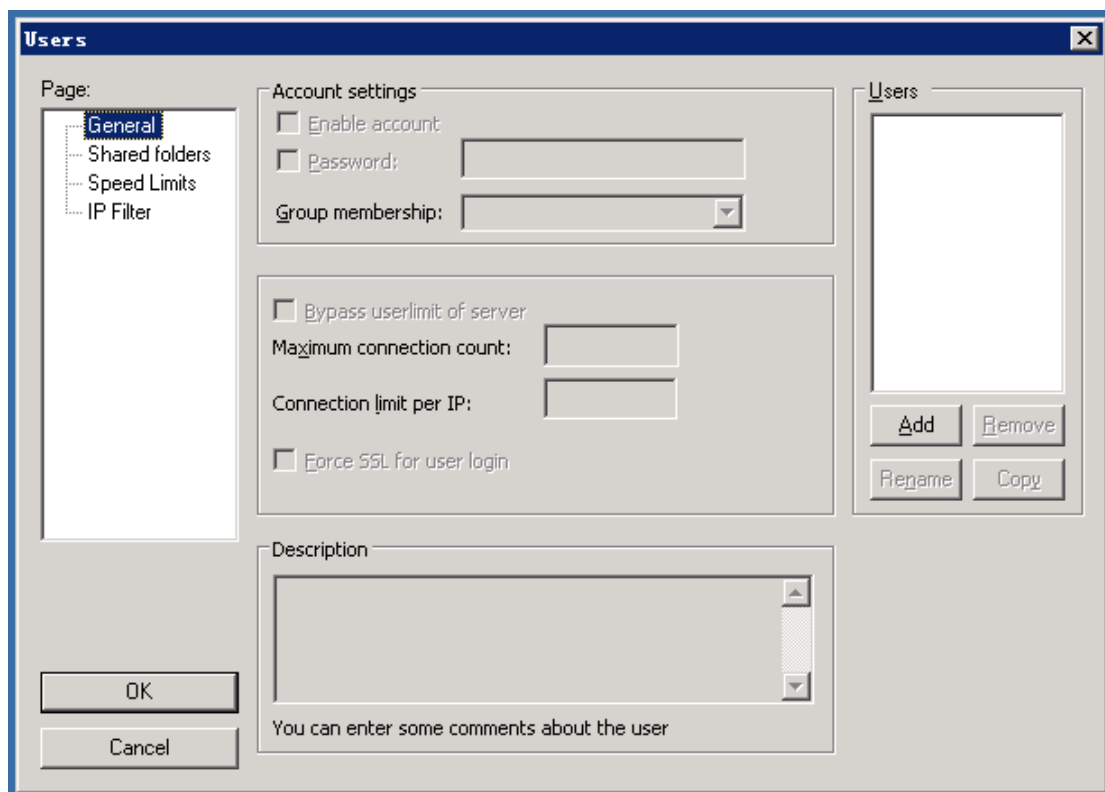
至此初始化基本配置完成。

2. 匿名FTP配置

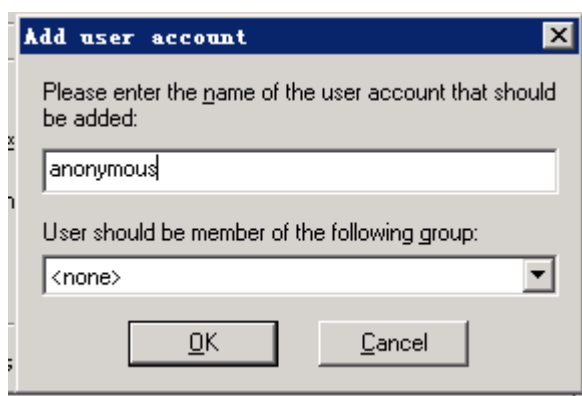
首先打开管理控制台，点击左起第四个图标  进入系统设置。



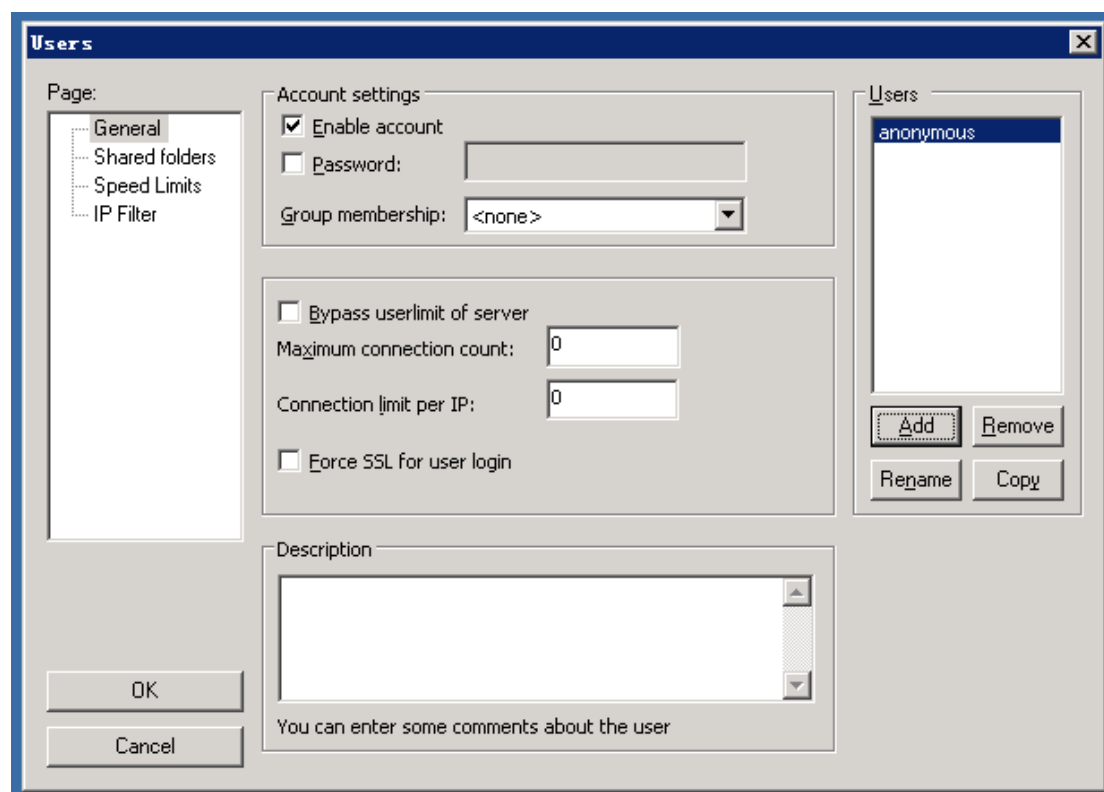
打开 ftp 用户管理界面，点击右侧的  按钮，添加新用户。



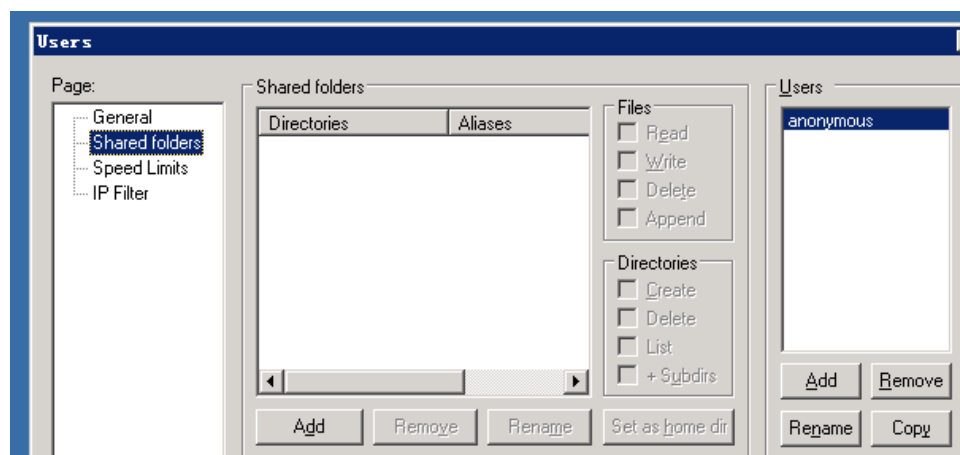
在新增用户的对话框中，输入“anonymous”这个名字，即 FTP 的匿名用户。



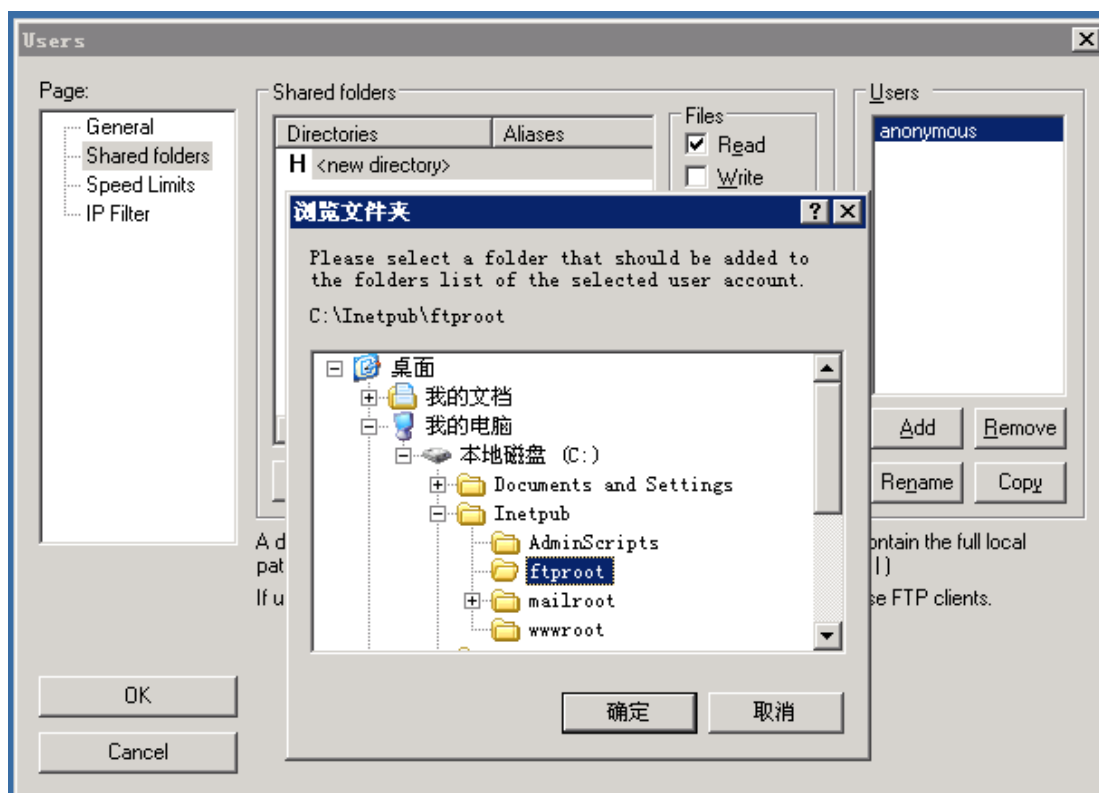
点击确认，添加用户完成，返回用户管理界面。



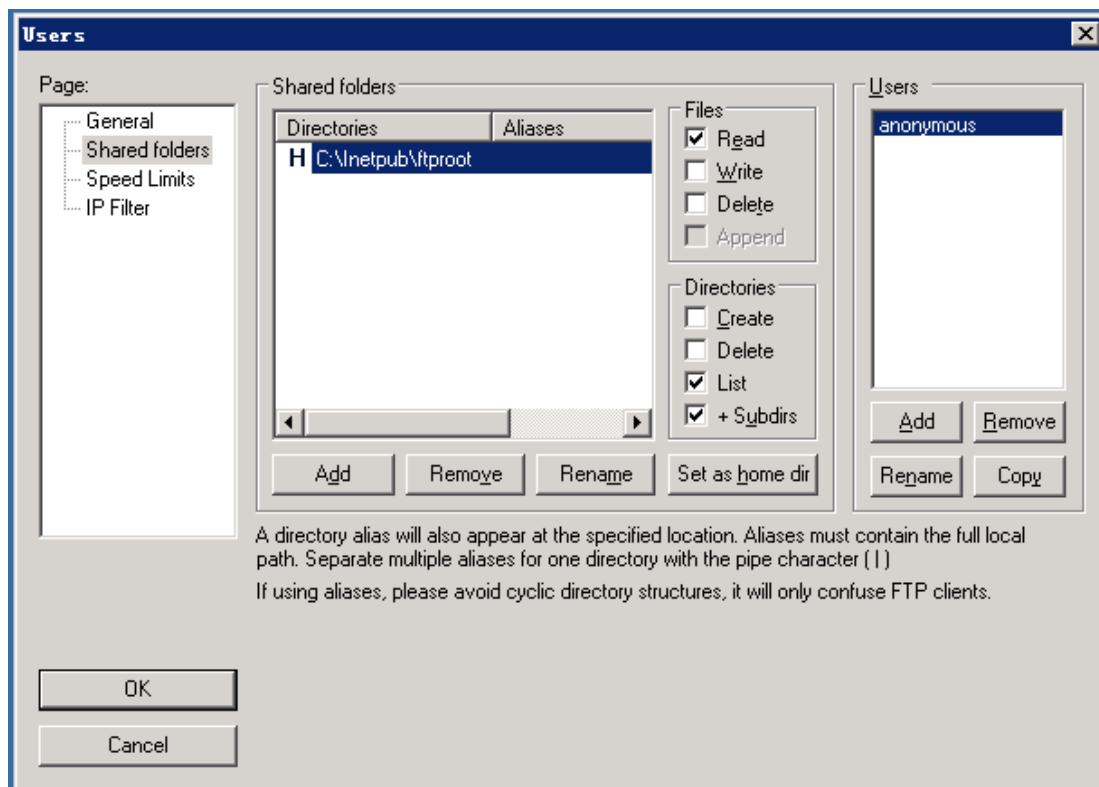
点击左侧的“Shared folders”菜单。点击 Add 按钮，添加一个目录。



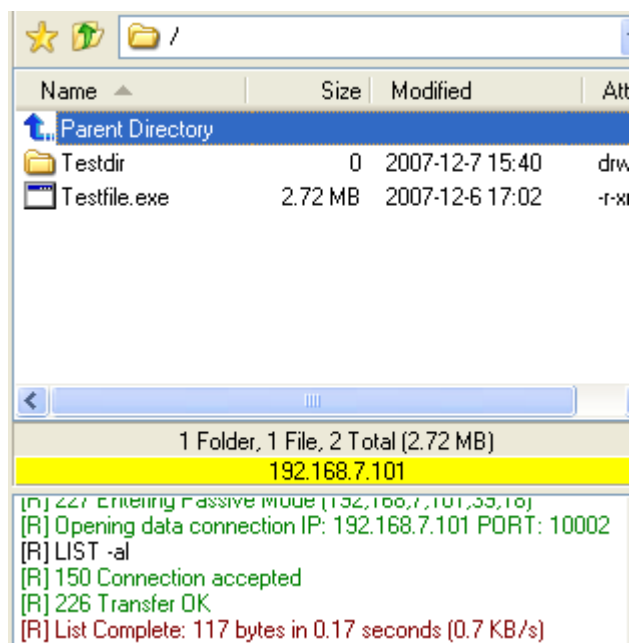
打开浏览文件夹的选项，选择要设置 FTP 的目录。



点击确定，添加用户完成。

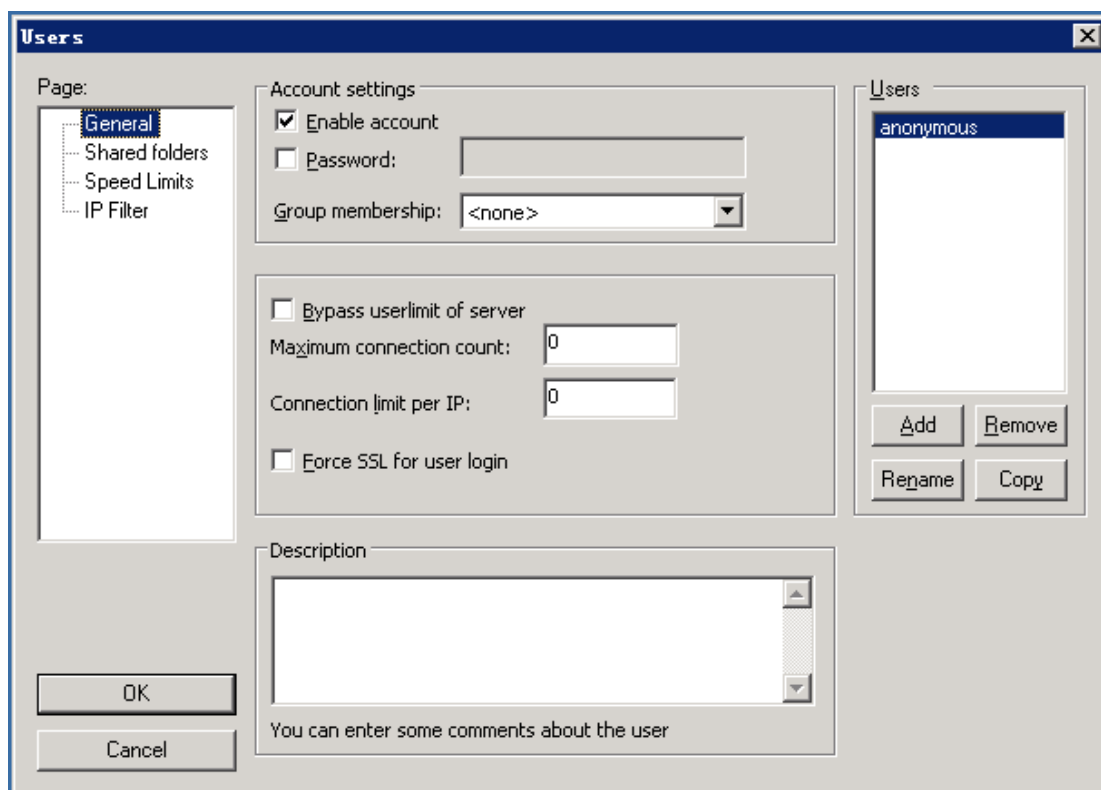


现在用户 FTP 客户端连接到 FileZilla Server 上，可以看到匿名 FTP 已经配置完成。

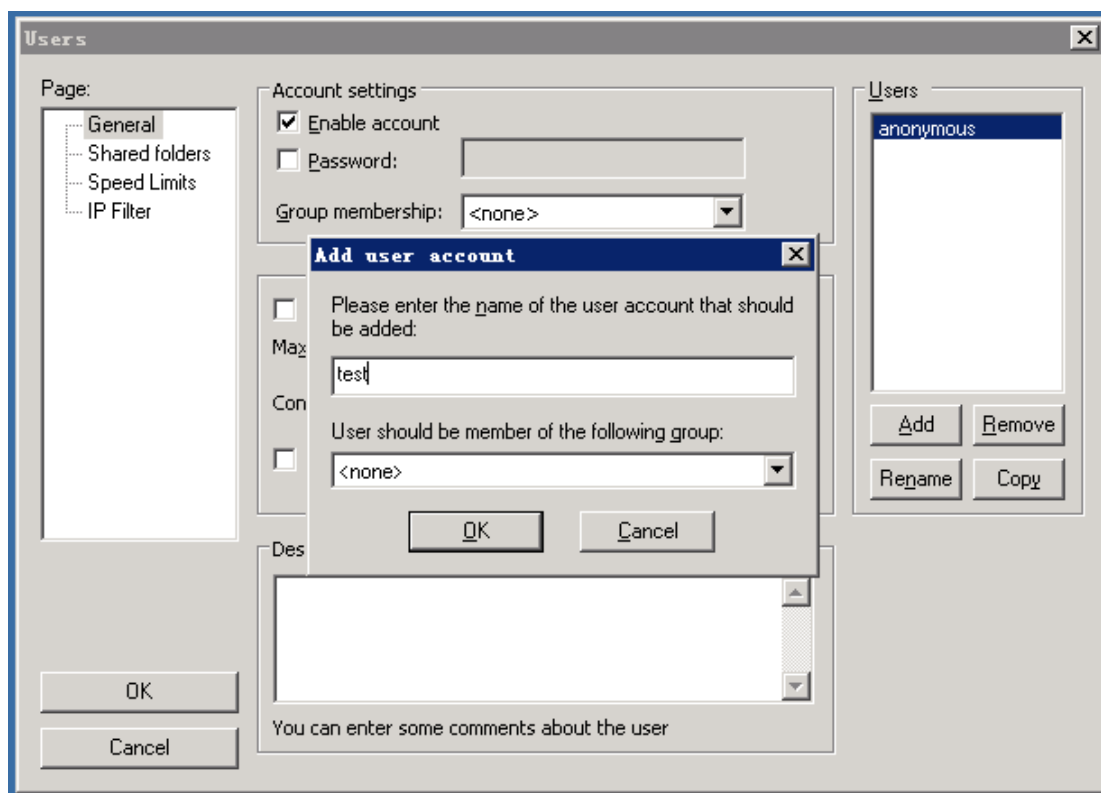


3. 标准FTP用户配置

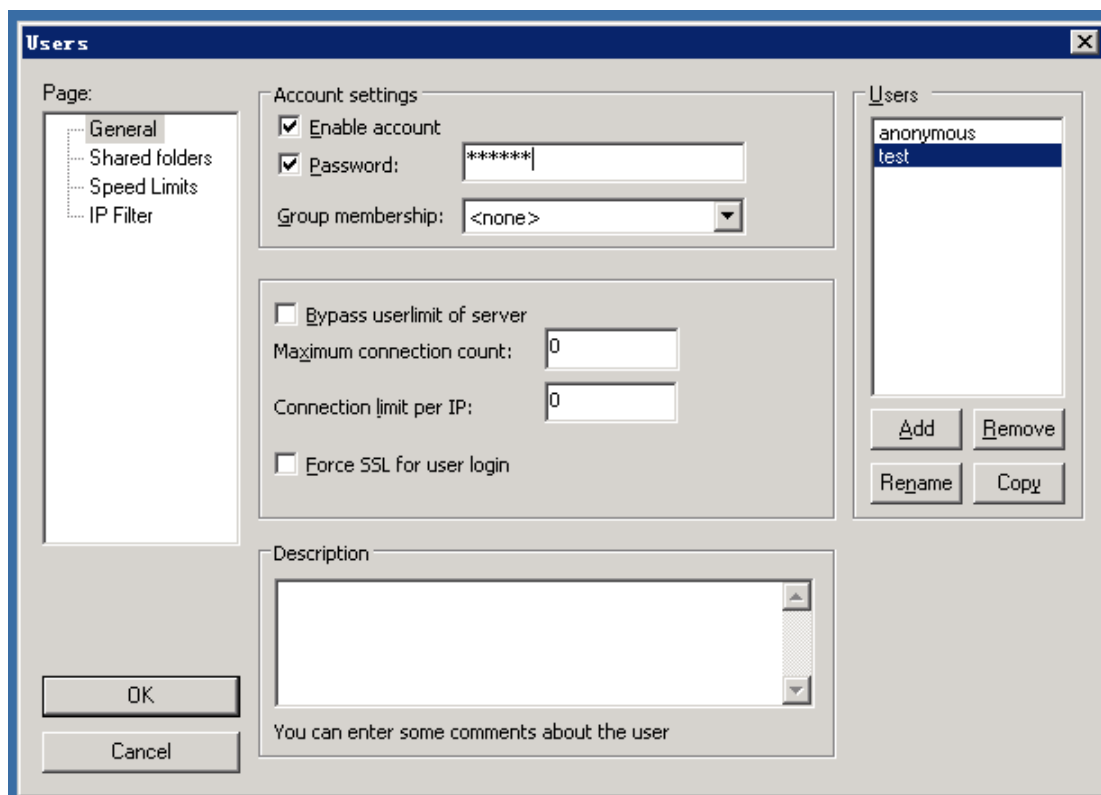
首先进入用户设置界面，点击“Add”按钮添加新的 FTP 用户。



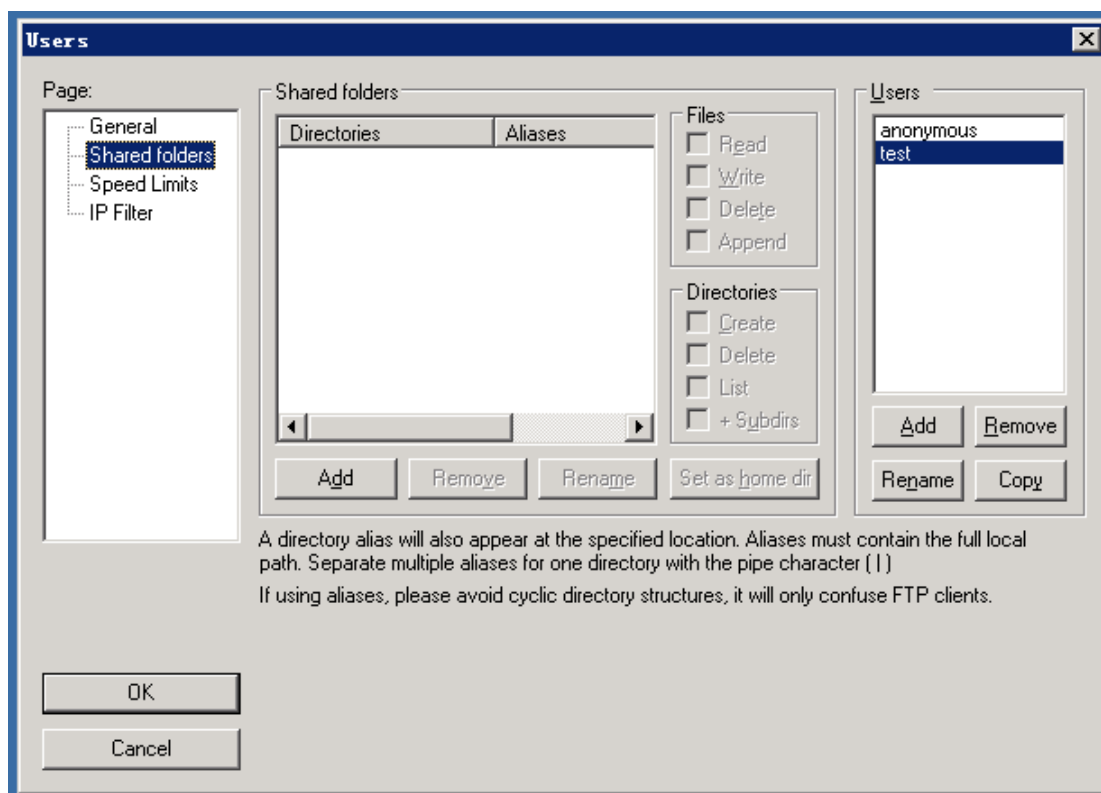
输入用户名 test 。



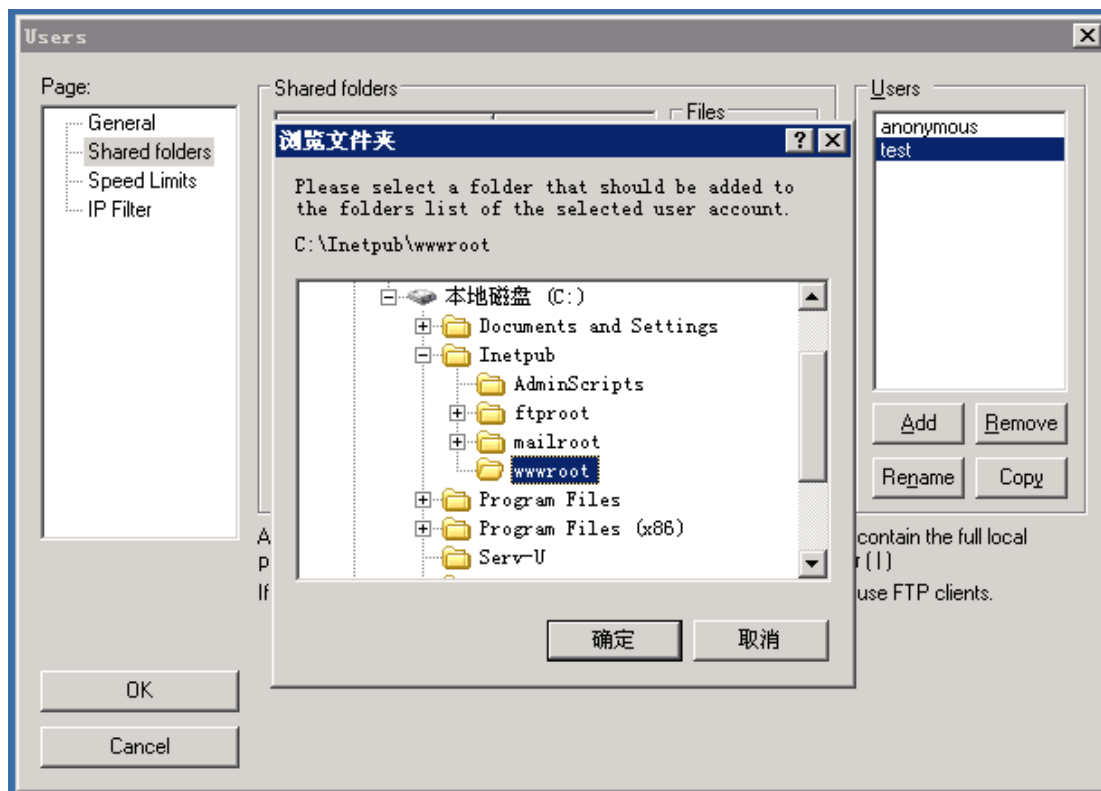
选中 Password 前边的多选框，然后输入密码 123456。



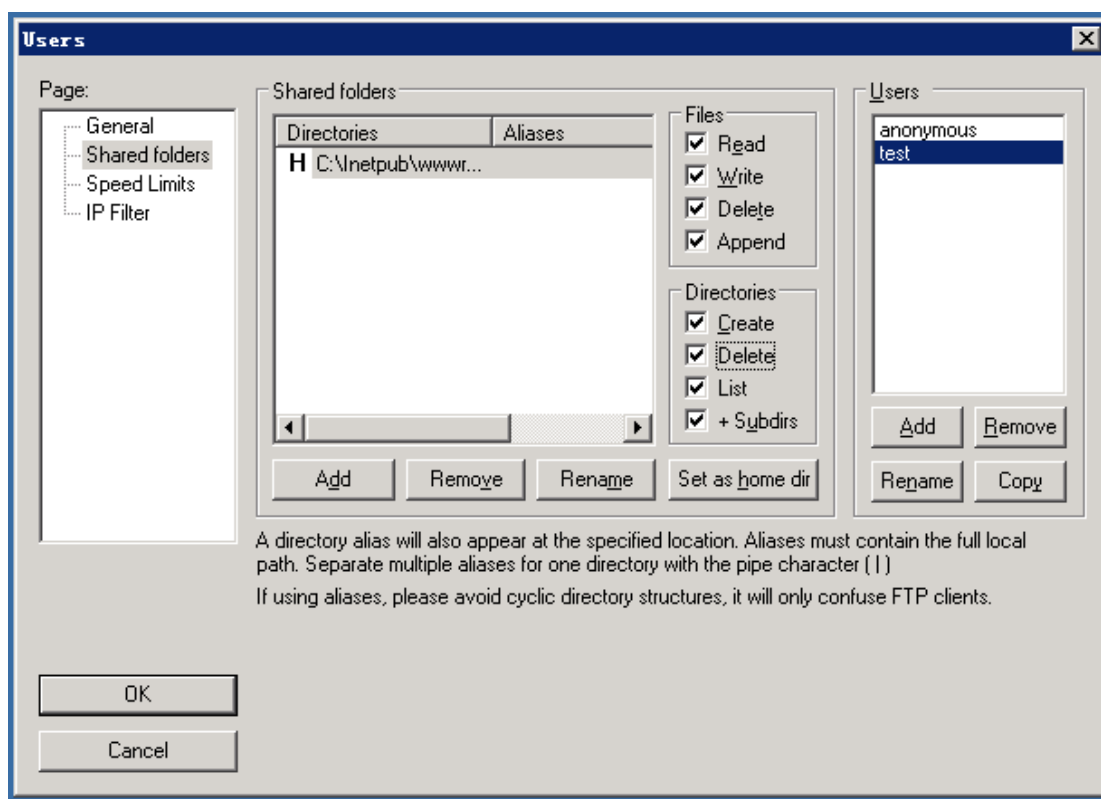
返回到用户管理界面，点击设置文件夹目录，点击 Add 添加目录。



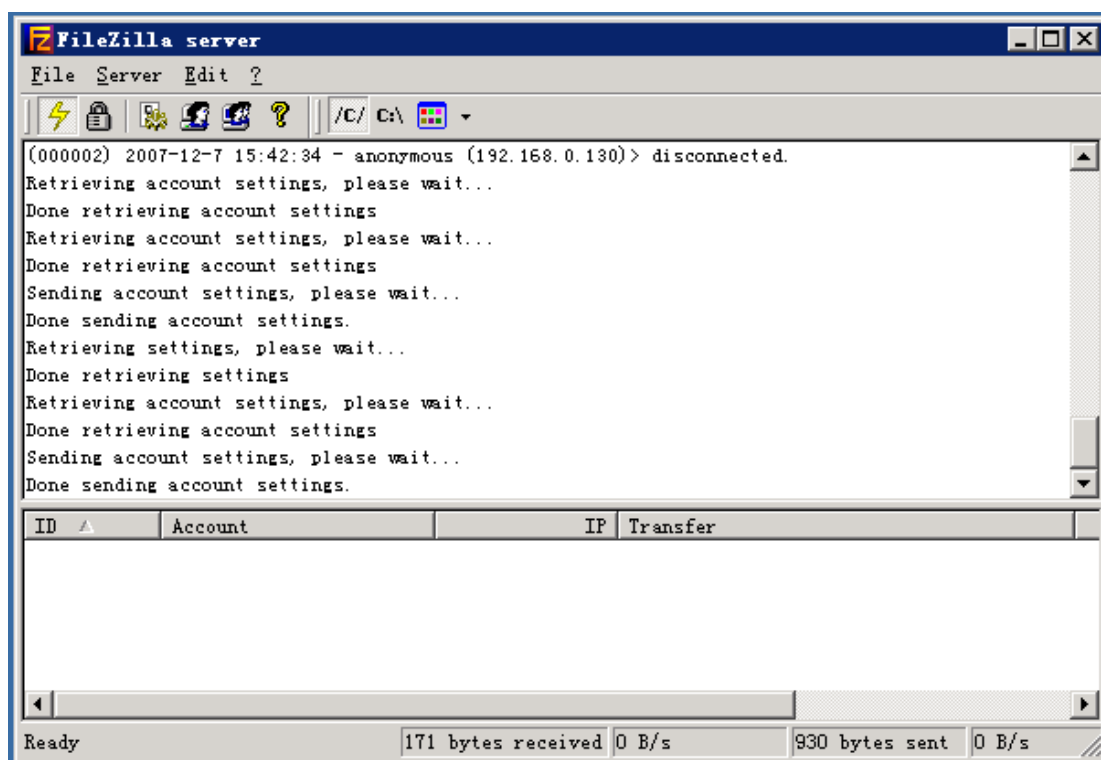
添加一个目录到 test 用户。



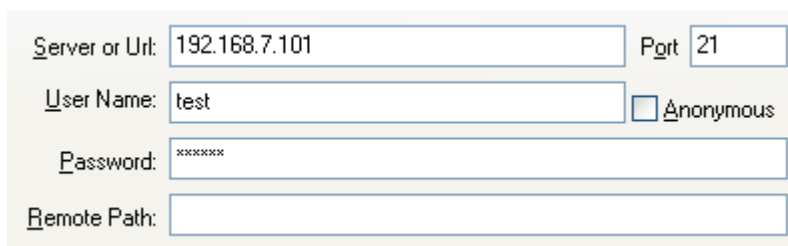
添加完成，再右侧选中 test 用户对这个目录的权限，然后点击左侧的 OK 按钮，配置完成。



配置完成。现在可以使用客户端来测试登录了。

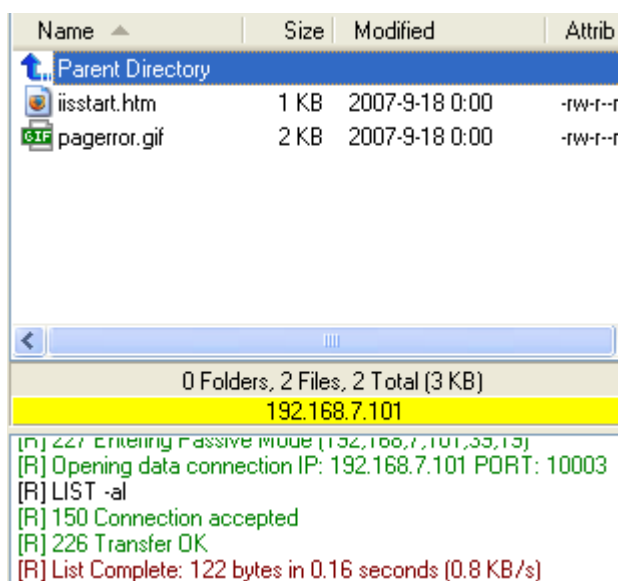


打开 FTP 客户端软件，输入 test 用户名和密码 123456，登录到服务器。



| | | | |
|----------------|---------------|------------------------------------|----|
| Server or Url: | 192.168.7.101 | Port: | 21 |
| User Name: | test | <input type="checkbox"/> Anonymous | |
| Password: | xxxxxx | | |
| Remote Path: | | | |

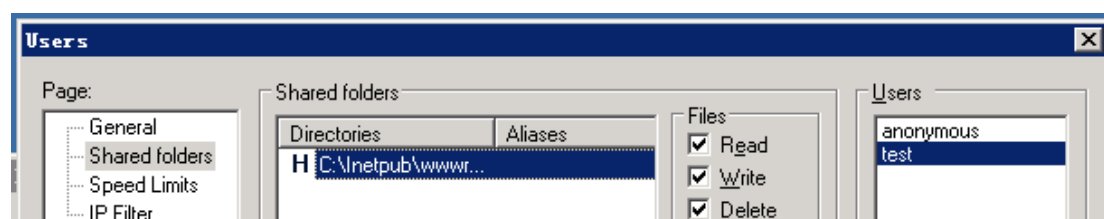
登录成功后，可以看到刚才制定的 FTP 目录下的文件，并具有相应的上传、下载权限。



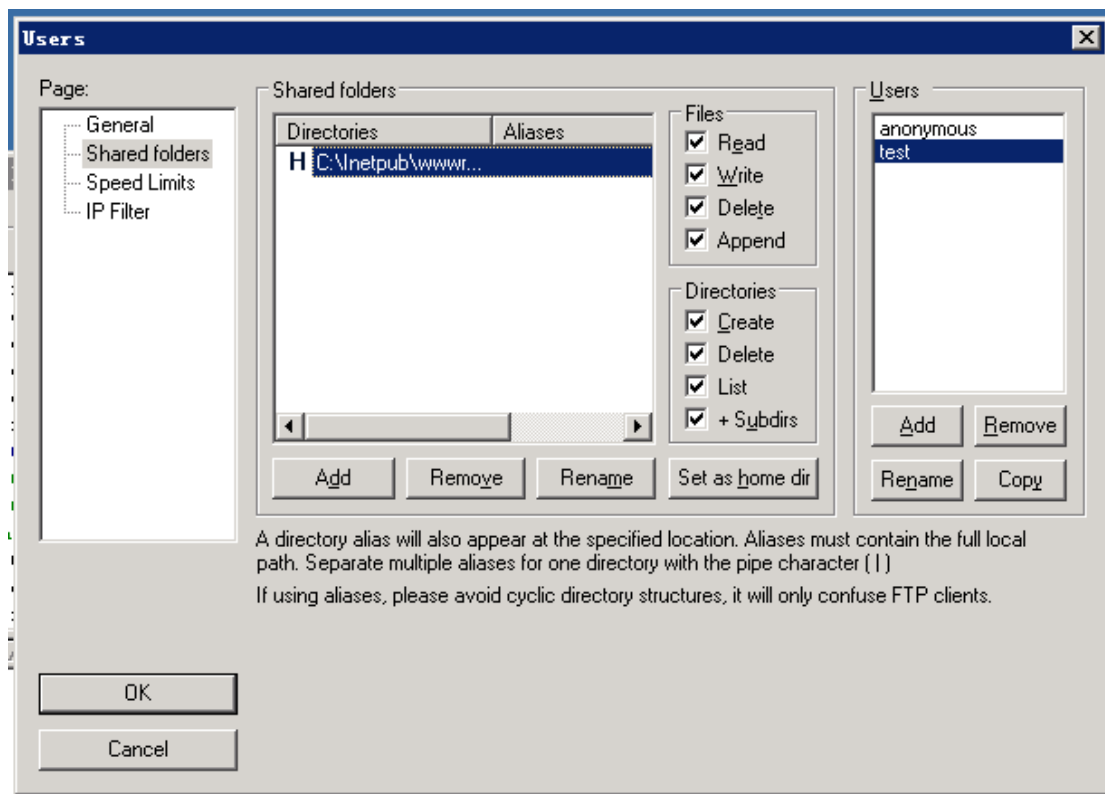
4. 虚拟目录配置

在具有多个目录需要共享的情况下，设置虚拟目录是比较利于管理的选项。通常，一个 FTP 服务器需要有一个“Home”主目录，然后设置若干个虚拟目录。

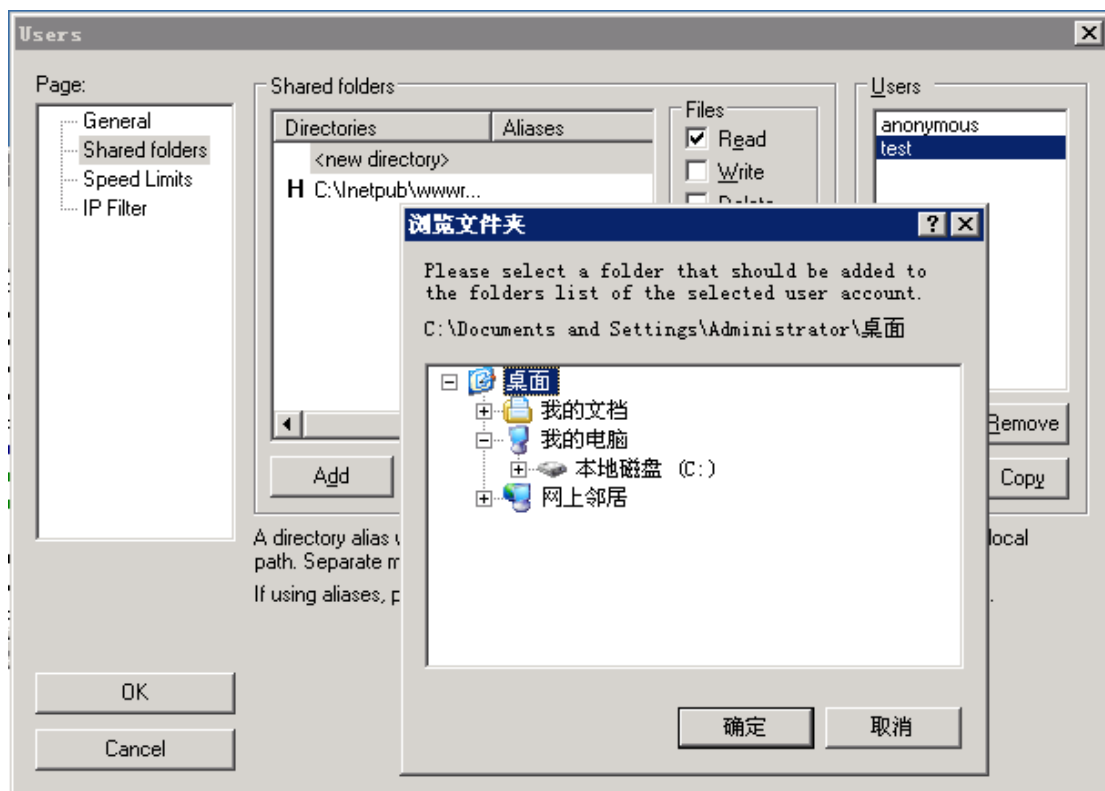
首先进入到用户管理界面，选中 Test 用户，选中当前设置的目录。



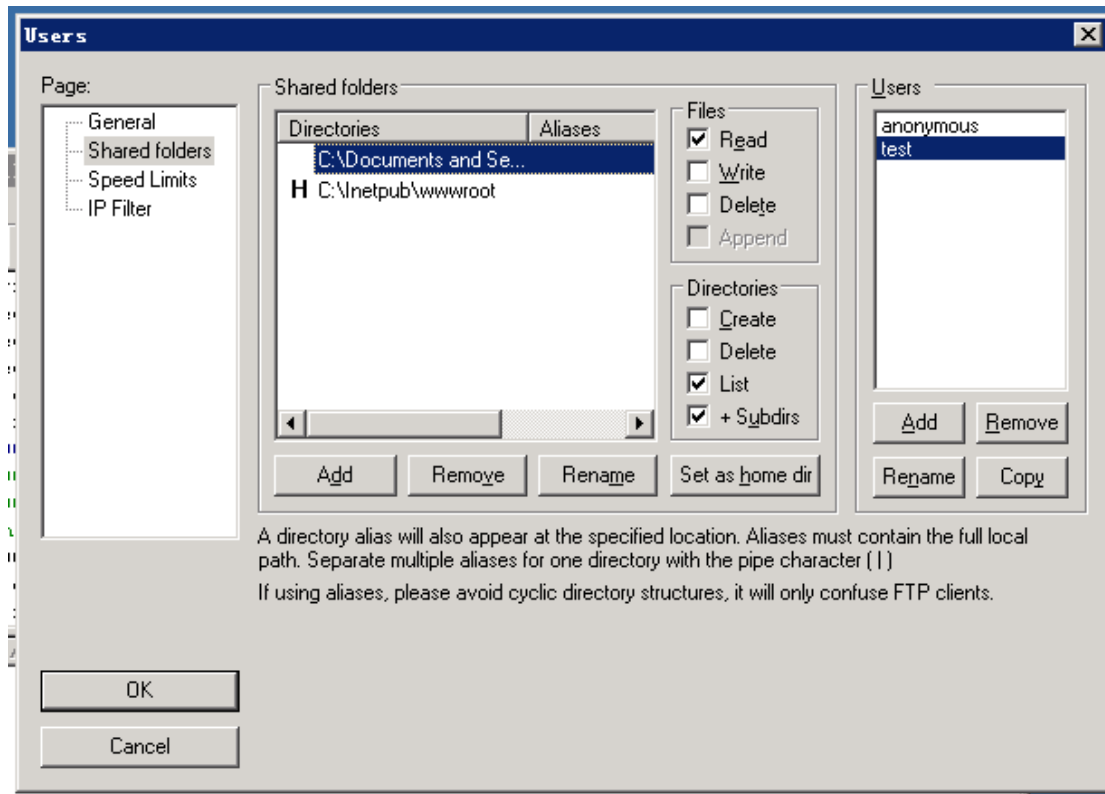
点击“Set as home dir”选项 ，将当前目录设置为“home”主目录。



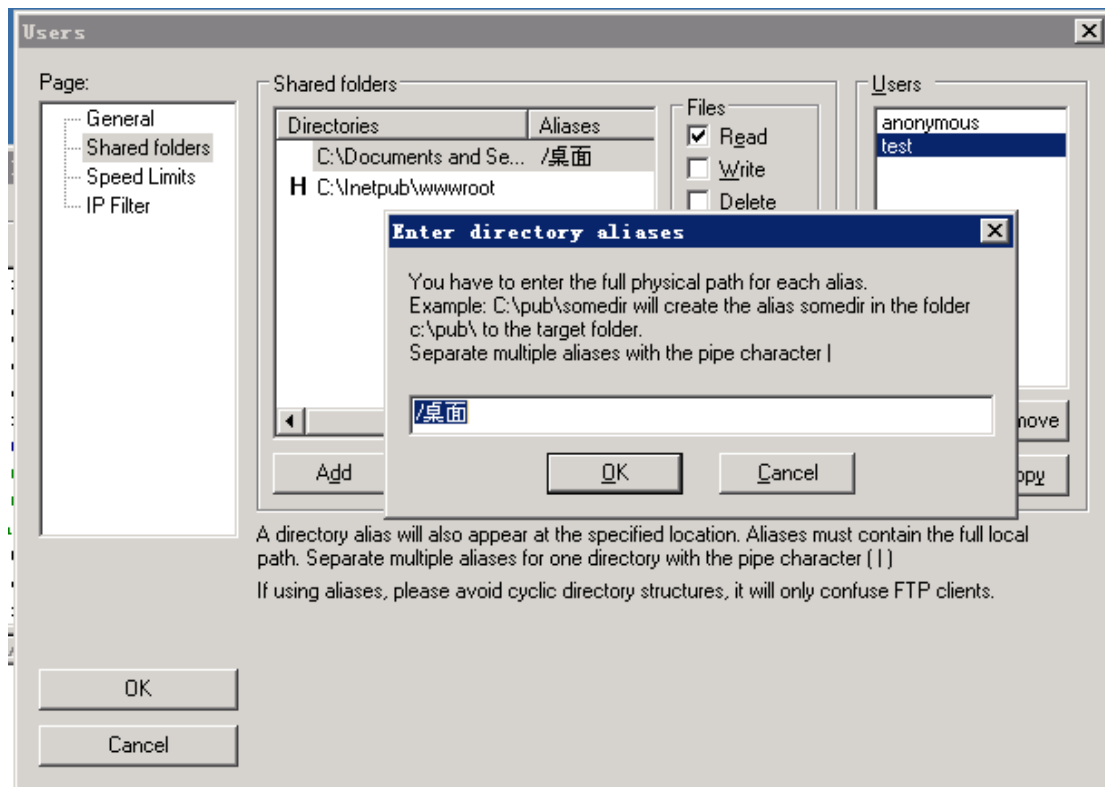
点击 Add 按钮，在原有目录之外，再添加一个别的目录，比如选择桌面目录。



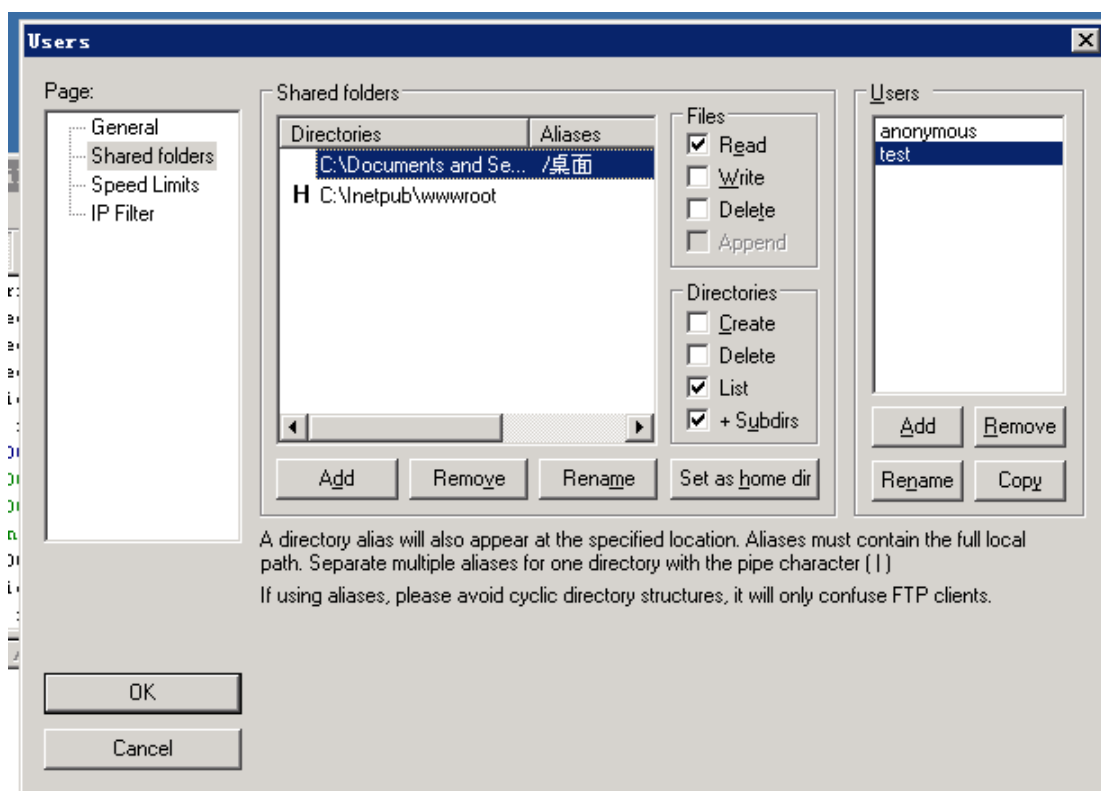
新的目录已经添加到目录清单了。此时添加“别名”，点击“Alias”空白处。



添加 Aliases 别名，注意一定用“/”符号开头，表示是根目录下的虚拟目录。



添加完成。现在可以去登录 FTP，就能看到虚拟目录了。



登录到 FTP 之后，可以看到虚拟目录出现在 test 用户的目录中。

| Name | Size | Modified | Attrib |
|------------------|------|-----------------|----------|
| Parent Directory | | | |
| 桌面 | 0 | 2007-12-7 15:11 | drwxr-- |
| iisstart.htm | 1 KB | 2007-9-18 0:00 | -rw-r--r |
| pagerror.gif | 2 KB | 2007-9-18 0:00 | -rw-r--r |

```
< | | | |
1 Folder, 2 Files, 3 Total, 1 Selected (0 bytes)
192.168.7.101
[!] 227 Entering Passive Mode (192,168,7,101,35,20)
[R] Opening data connection IP: 192.168.7.101 PORT: 10004
[R] LIST -al
[R] 150 Connection accepted
[R] 226 Transfer OK
[R] List Complete: 175 bytes in 0.20 seconds (0.8 KB/s)
```

至此虚拟目录设置完成。

5. 加固Filezilla安全

- 安装 Filezilla 到非标准目录
- 安装过程中设置 Filezilla 的管理端口监听在 127.0.0.1 上的随机端口，例如 38471 等奇怪的没用的端口。
- 安装过程中设置 Filezilla 的管理密码，并设置密码足够复杂
- 在 Filezilla 目录下的 xml 配置文件上，设置 Guests 组禁止读取的权限
- 修改 FTP 登录后的提示信息为 IIS、Serv-U 等信息
- 不要开启 SSL 加密、SFTP 等功能，避免以后出现漏洞

经过如上一些配置，Filezilla 可以做到很高的安全性。