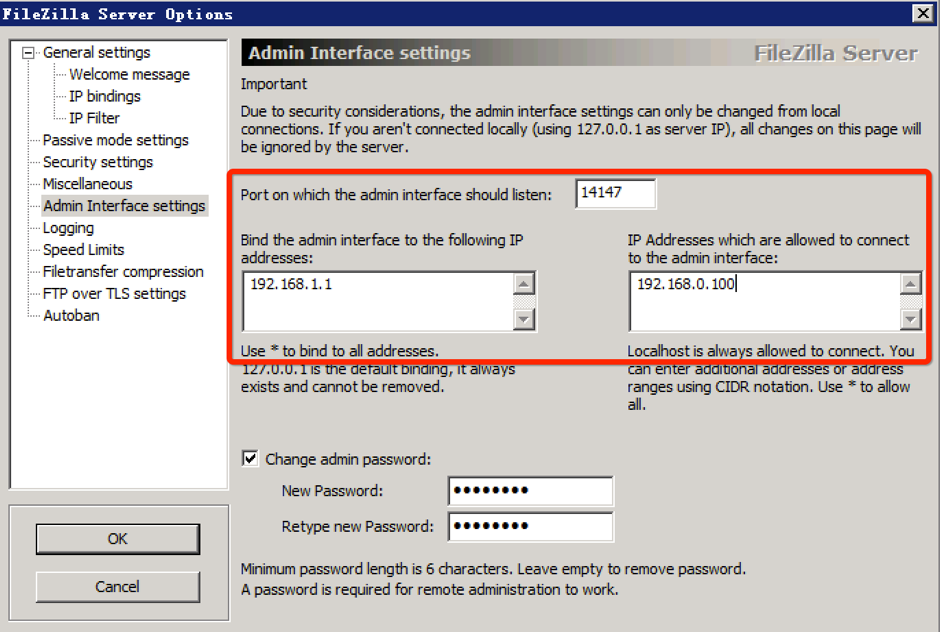
# FileZilla FTP Server 安全加固

本加固文档以 FileZilla Server 0.9.60 版本为依据编写，以下大部分配置都是通过 FileZilla 服务器的“Edit”->“Settings”菜单打开的“FileZilla Server Options”来完成。

# 1.设置管理密码

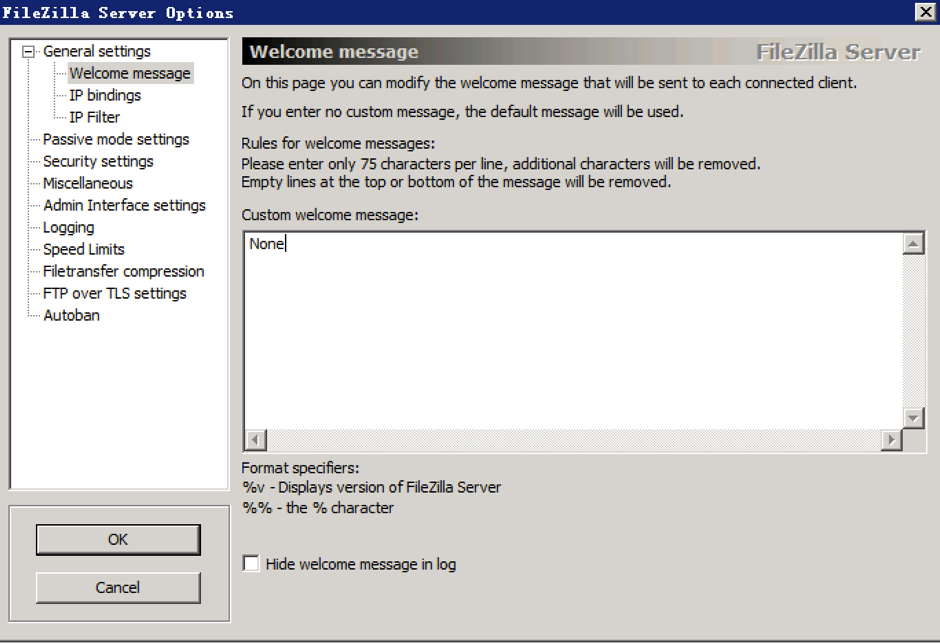
服务器默认管理密码为空，建议设置一个较复杂的密码（至少包含大小写字母、数字、特殊符号中的任意两种）。



# 2.Banner 信息

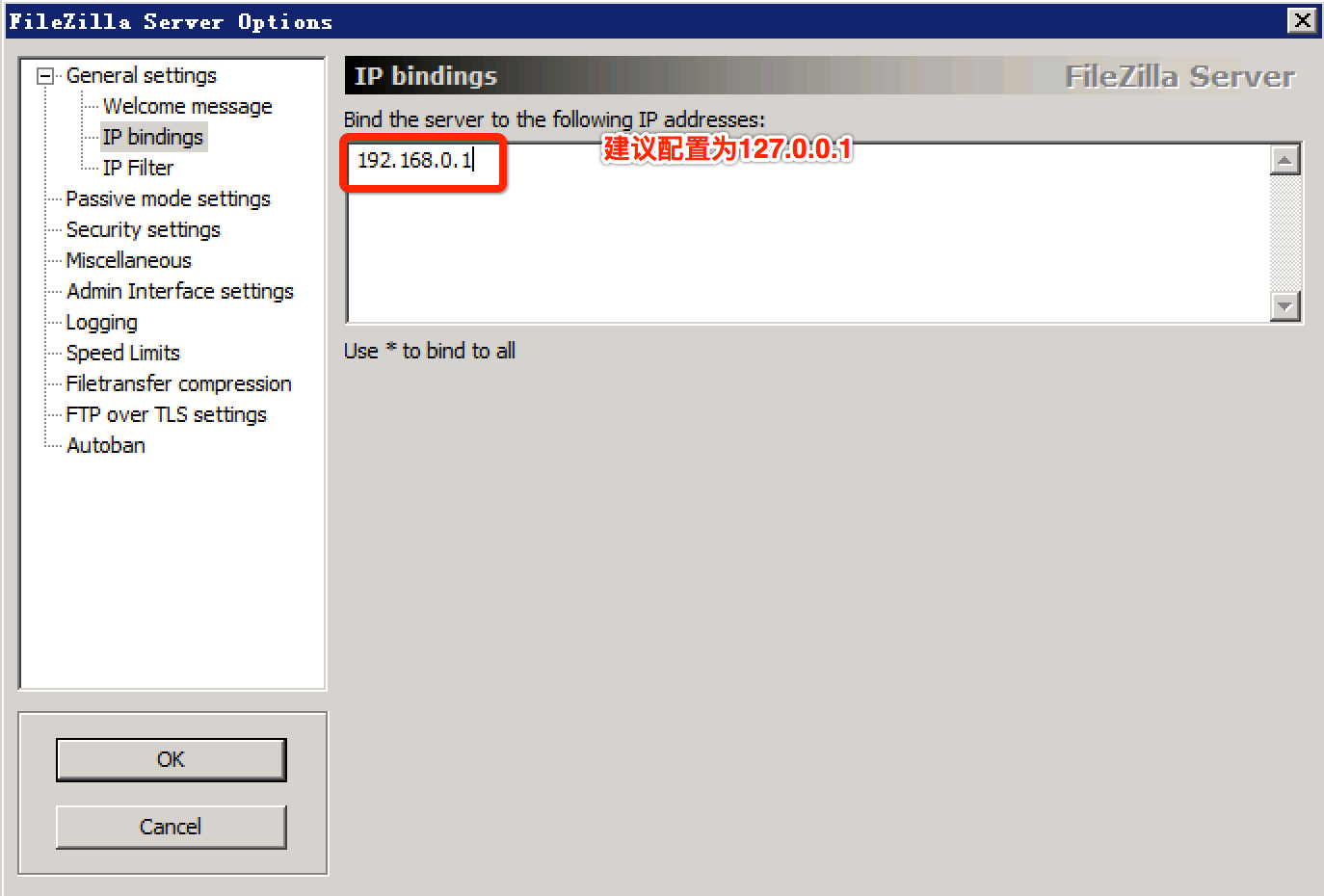
默认情况下，访问 FTP 服务器的时候，将会显示服务器的版本信息，通过屏蔽服务器的版本信息显示，可以加大攻击者的时间成本。

进入“General settings”下的“Welcome message”，从右侧的“Custom welcome message”输入框中删除“%v”变量，或者直接将全部文本替换为自己的文字；另外，建议勾选下面的“Hide welcome message in log”，可以减少日志中的垃圾信息。



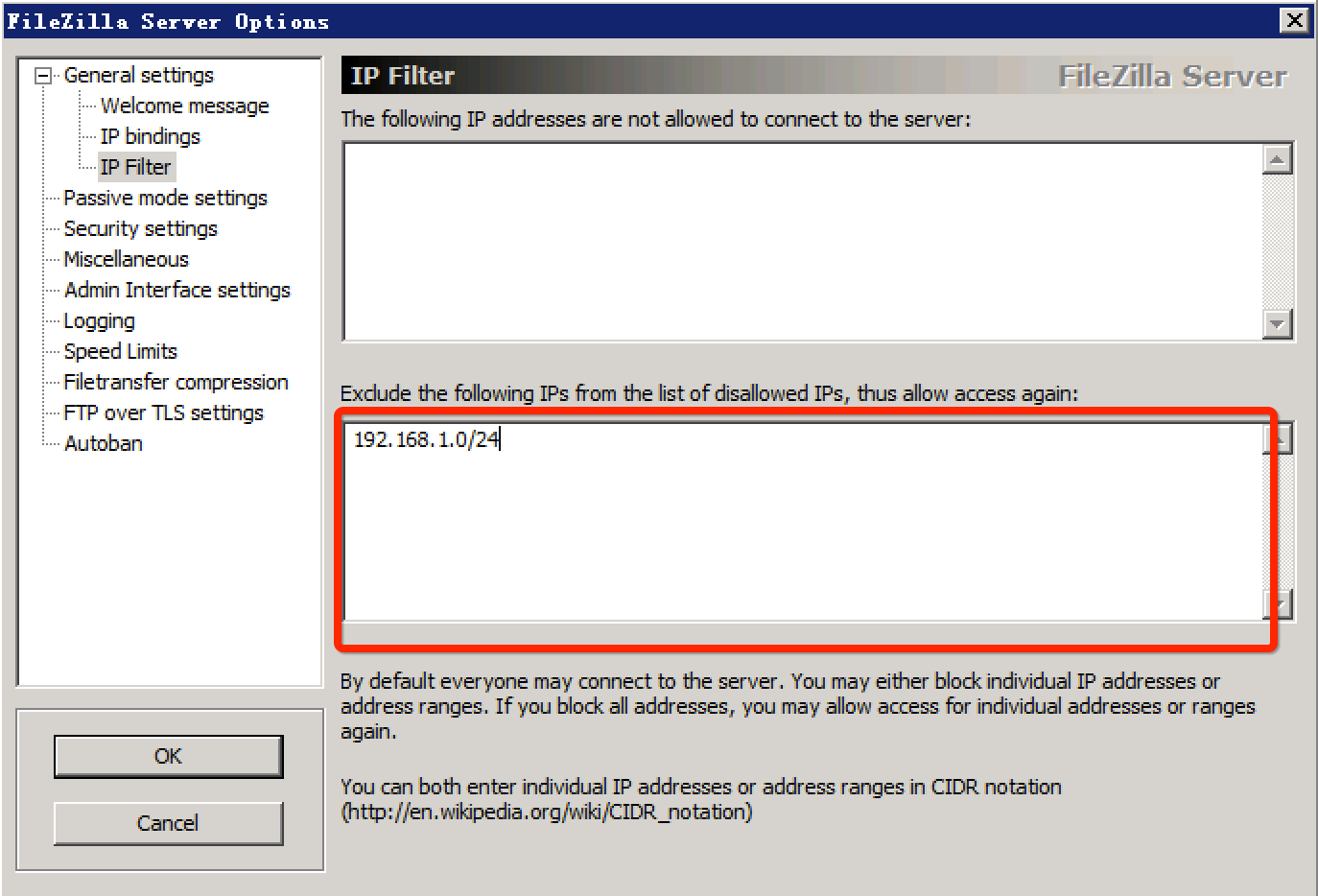
# 3.监听地址和端口

建议只在其中的一个地址上启用 FTP 服务（例如：当我们只需要在内网使用FTP服务时，就不需要再服务器绑定的公网地址上开启 FTP 服务），进入“General settings”下的“IP Bindings”，在右侧窗口中将默认的 \* 号修改为指定的地址



# 4.访问控制

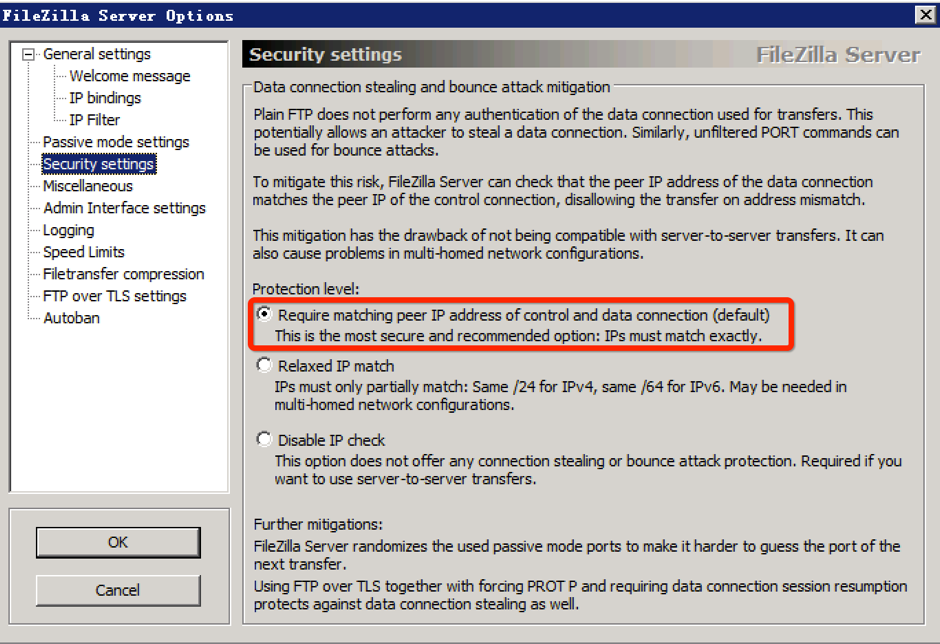
进入“General settings”下的“IP Filters”，在右侧上部的窗口中填入要阻止的 IP 范围，在下面的窗口中填写允许的 IP 范围。通常采用默认阻止所有IP（\*号），然后仅允许部分 IP 的方式来进行有效的限制。例如，下图中仅允许 192.168.1.0/24 网段访问 FTP 服务。



另外，FileZilla 服务器也支持用户级和用户组级的 IP 过滤器，从“Edit”->“Users/Groups”菜单即可打开对应的设置页，在设置页中找到“IP Filters”，然后选择需要设置的用户，设置允许和拒绝的IP即可。设置方法与全局 IP 过滤器相同。

# 5.FTP Bounce配置

FTP Bounce 攻击是一种利用 FXP 功能的攻击形式，默认情况下服务器未关闭相关的功能，建议将相关功能设置为阻止，如果服务器仍然需要在与某个特定IP的服务器之间使用该功能，建议勾选下面的 “Strict IP Filter” 选项，然后通过 “IP Filters” 来进行限制。相关设置参见“访问限制”章节的内容。

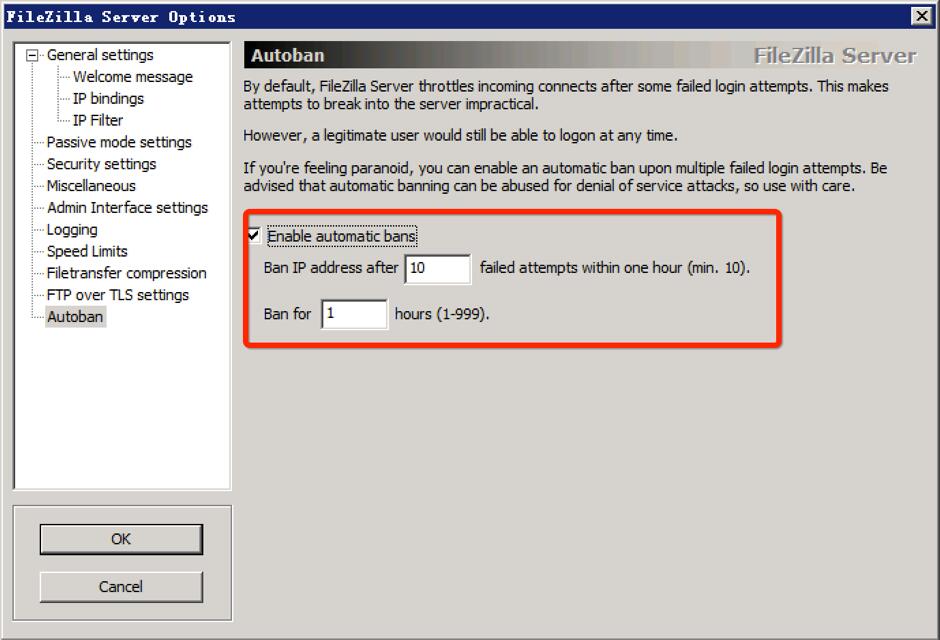


默认选项已经启用了需要精确匹配连接地址，建议用户不要修改。

# 6.用户认证策略

默认情况下，当出现多次用户认证失败后，服务器会断开与客户端的链接，但并没有严格的限制策略，通过下面的设置，可以对连续多次尝试登录失败的客户端 IP 进行阻止，干扰其连续暴力尝试行为。

下图中的设置会对一小时内连续10次登录失败的IP进行阻止，阻止时长为1个小时。

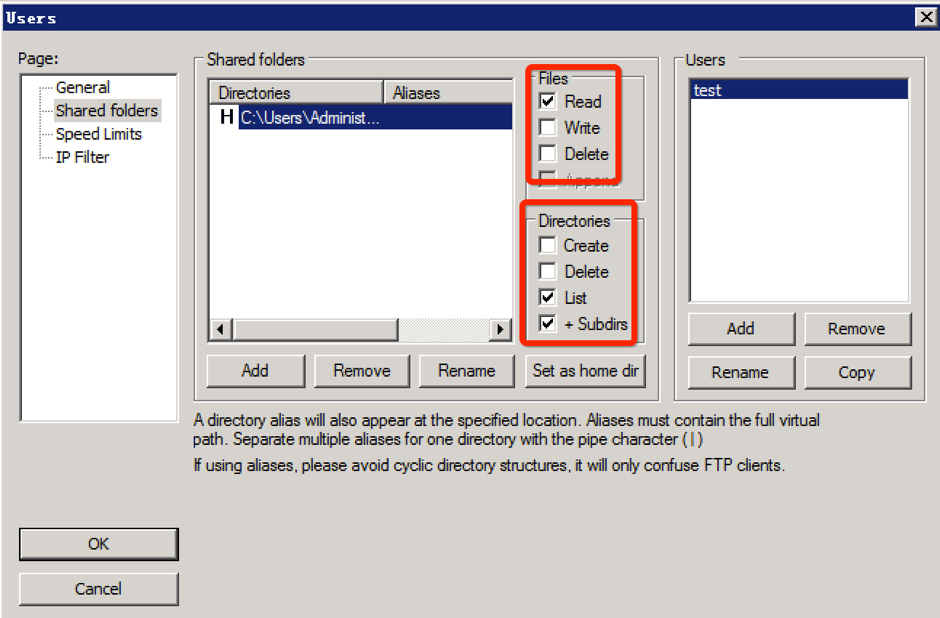


# 7.密码复杂度

FileZilla 服务器未提供密码复杂度相关的设置项，并且服务器的用户是由管理员通过管理接口来添加的，用户也无法通过 FTP 命令来修改密码，因此建议管理员在添加用户时使用复杂的密码。

# 8.访问权限

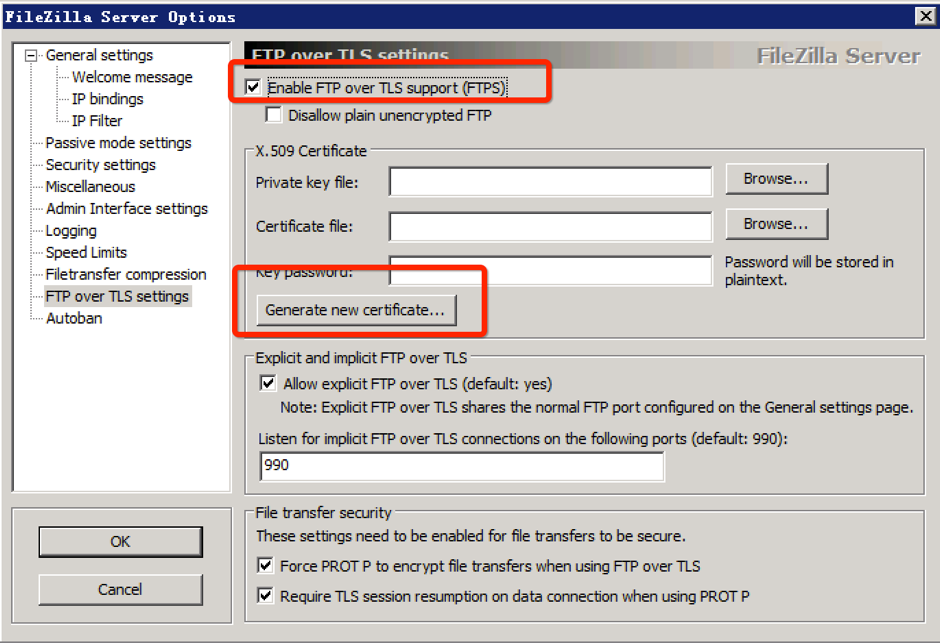
FileZilla 支持目录级别的访问权限设置，可对某个目录设置文件读 、写、删除、添加、目录创建、删除、列举等权限。建议根据实际应用需要，结合用户权限最小化原则来进行文件夹的权限分配。



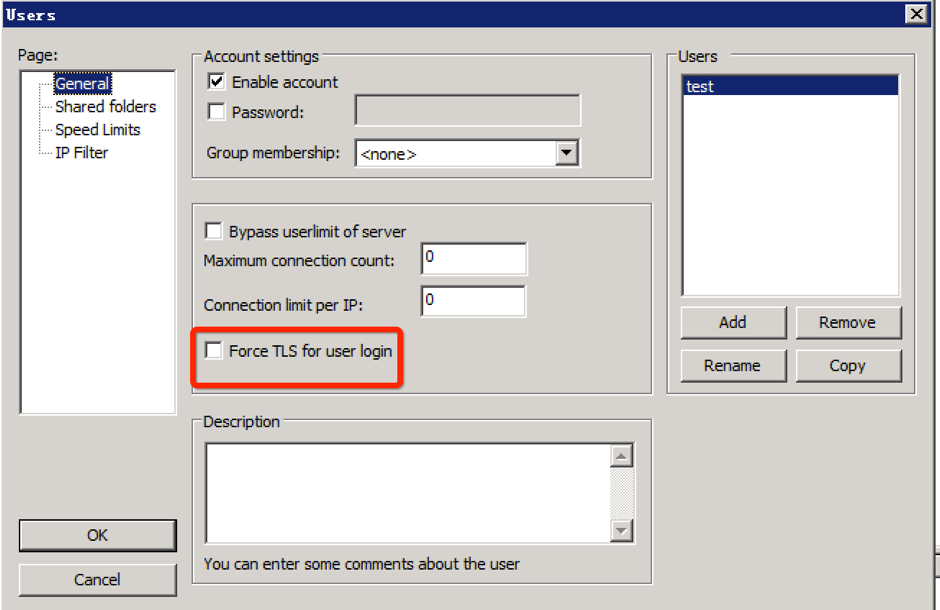
该操作需要提前添加账号和组后才能配置。

# 9.启用TLS加密认证功能

FileZilla server支持TLS加密功能，用户如果没有证书可以使用自带功能创建。



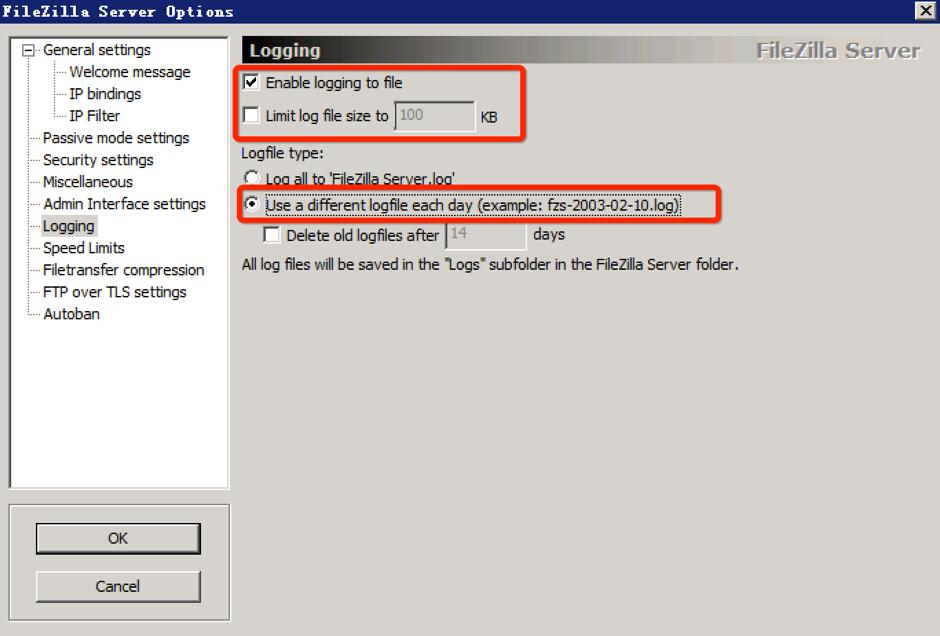
可以针对单个用户强制启用TLS加密访问：



# 10.日志记录

* **开启日志记录**

FileZilla 服务器默认未开启日志记录，为了方便对各种事件的追查，建议开启日志记录功能，并将日志设置为每天一个日志文件，避免单文件过大的问题。



* **日志不记录密码**

默认情况下，日志已经设置不记录用户密码，但在加固的时候应检查此选项是否启用。建议启用此项，避免密码泄露。

