中间件在 HTTPS 网站中

配置 WSS 连接说明书

在 Chrome 等新版浏览器中， HTTPS 的网站在连接 Web Socket 服务时，默认强制要求必须使用 WSS 协议，而 WSS 协议中是不能使用 localhost 或 IP 地址的，只能用域名，同时必须配置对应域名的 SSL 证书来使用。所以如果需要在您的 HTTPS 的网站里连接中间件提供的 Web Socket 服务端，请在主域名下面，申请一个**其它地方都不会用到**的二级域名，然后用这个二级域名申请扩展验证（EV SSL）类型的 SSL 证书，并下载 Apache 服务器使用的证书包提供给我们制作授权文件方可使用，连接格式举例：wss://wrl.zorrosoft.com:453?sid=622768&flag=1，其中 wrl.zorrosoft.com 为二级域名，需要替换为自己的，453 是默认的 WSS 侦听端口，可在中间件配置文件中修改，sid 及 flag 等参数含义，请参考中间件的开发者手册。WSS 具体的侦听端口，请搜索中间件的日志文件输出内容，是否有类似这样的一条记录：“127.0.0.1:453 WSS security listening successfully established”，其中 453 就是端口，日志文件在中间件主程序(单机版是 WrlService.exe，网络版是 ZbaService.exe)的 data 子目录下的同名 txt 文件，如果不知道中间件安装位置，可以启动任务管理器，切换到详细信息标签，找到对应的 exe 文件，右键菜单找“打开文件所在的位置”点击，就会自动定位到中间件的程序运行路径。

中间件用 SSL 证书来是做终端电脑的本机 WSS 连接代理，所以不能用已经在其它地方使用的二级域名来做证书，也尽量避免使用主站通配符的 SSL 证书，因为可能存在安全隐患。当使用了 SSL 证书的 WSS 地址连接不上时，在确保连接地址参数及格式正确的前提下，先尝试重启电脑看是否恢复正常，如何还是连接不上，检查操作系统中的 Hosts 文件，默认路径是 C:\Windows\System32\drivers\etc\Hosts，文件中是否有类似“127.0.0.1 wrl.zorrosoft.com”这样的一条，如果没有，很可能是中间件安装时，修改这个配置文件时被拒绝了，确保电脑中杀毒或安全等软件没有拦截修改操作。也可以手工自己修改 Hosts 配置文件添加这样一条，然后以管理员权限启动命令行(cmd.exe)窗口，运行 ipconfig.exe /flushdns 指令，提示配置已更新后再尝试连接。如果还是无法连接，可能是提供的 SSL 证书有问题，注意不能使用自签名的证书，浏览器是不认可的。另外前端可以在发起 WSS 连接失败时，查询返回的具体错误编码，并在网络上根据错误编码找对应的解决方法，请参考

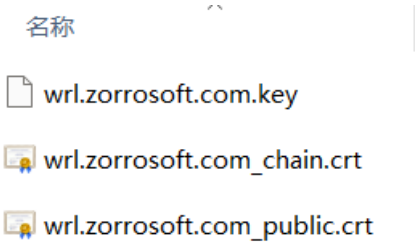
内容：https://www.wbolt.com/ssl-connection-error.html。如果实在无法连接使用，网络版或没有绑定域名授权的单机版情况下，需要修改前端连接的技术方案，B/S 网站需要设置支持跨域请求，就是允许 HTTPS 网站可以发起 WS 连接请求，具体实现请自行解决。

由于 SSL 证书是有期限的，所以请您一定要牢记证书的有效期，**务必在有效期之前几天或更长时间申请到新的证书**，然后提交给我们重新制作授权文件，然后让所有终端电脑更新到最新的授权文件，否则一旦证书的有效期到了，前端也无法再连接中间件获得正常服务了。在测试证书有效性时可以先申请免费证书使用，阿里云等服务商可以提供免费的 SSL 证书，不过目前只有 3 个月的有效期了，系统上线商用的话，务必选择购买尽可能长时间的证书，减少因证书过期引发的系统无法使用问题的机会。申请到新的证书文件包后，可以自行在中间件的测试网页里完成授权文件里的证书信息更新，这一步只能在原来的证书未过期之前进行。

关于如何自行更新授权文件里的证书信息的方法，网络版请在授权服务器的浏览器中打开测试网页 http://local.zorrosoft.com，修改连接按钮上方地址的端口为 800(授权服务器的 WS 默认侦听端口，如果自己修改过，请对应修改到自己的端口号)，点击连接成功后，在发送按钮上方的输入框中复制粘贴以下内容后点击发送：

```
{"req":"Wrl_UpdateSslCert","rid":3,"para":{"Path" : "G:/SSL"}}
```

其中 Path 路径里请务必提前准备好您的 SSL 证书文件，类似这样的：



一个 key 文件，一个_public.crt 文件，一个_chain.crt 文件。发送更新证书请求后，授权服务器授权文件的证书信息就更新成功了。

关于让终端电脑更新授权文件，如果是网络版的话，授权服务器的授权文件更新到新的 SSL 证书后，只需要保证终端电脑可以正常访问授权服务器即可，中间件会定期更新，如果需要强制马上生效的话，前端可以在连接到中间件服务端口后，请求以下指令：
{"req":"Wrl_UpdateAuth","rid":2,"para":{}}。如果是单机版的话，前端可以调用指令 Wrl_UpdateAuth，前提也是在原来的 SSL 证书未到期之前进行，下面是单机版更新授权文件的指令说明：

{"req":"Wrl_UpdateAuth","rid":2,"para":{"Url" : "http://local.zorrosoft.com/Files/Update/WrlAuth.wdb","MD5":"8BBCD7EAD95EFC034B724C4D8A961C03","Size":262144,"Cookie" : "","Auth" : ""}}
先把授权文件放到 B/S 的服务器上，支持 HTTP 协议的下载操作，并设置下载具体路径和文件大小及文件 MD5 编码。

终端电脑使用的中间件软件包，请务必用更新过证书的授权文件(网络版：ZbaAuth.wdb，单机版：WrlAuth.wdb)替换下对应的同名文件。否则新安装的电脑还是无法使用的。如还有问题问题，请加客服微信沟通：ZorroSoft