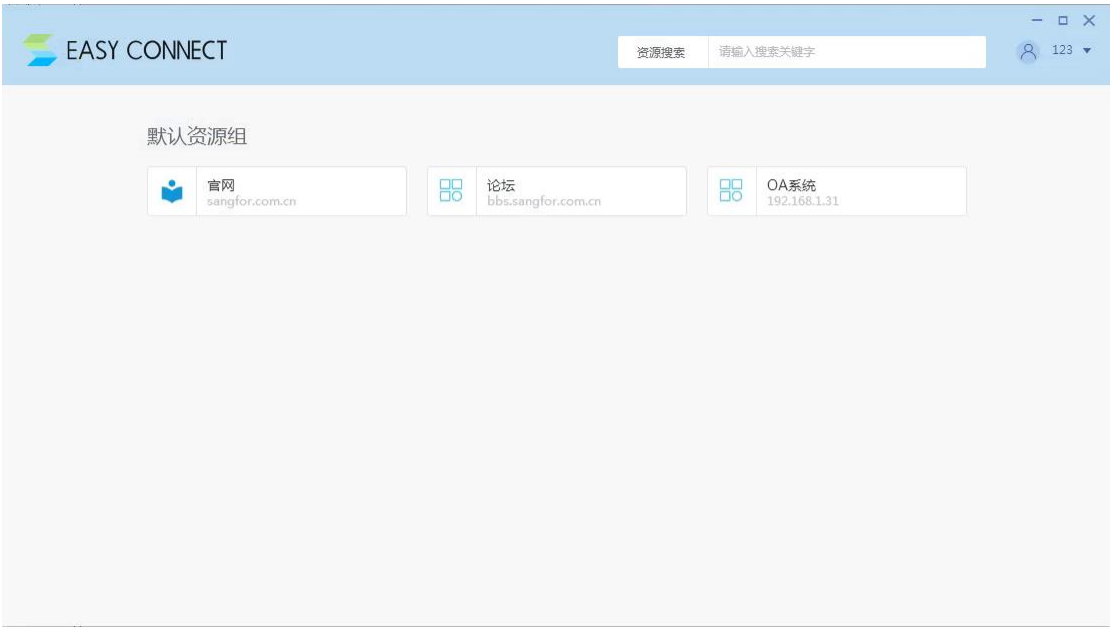
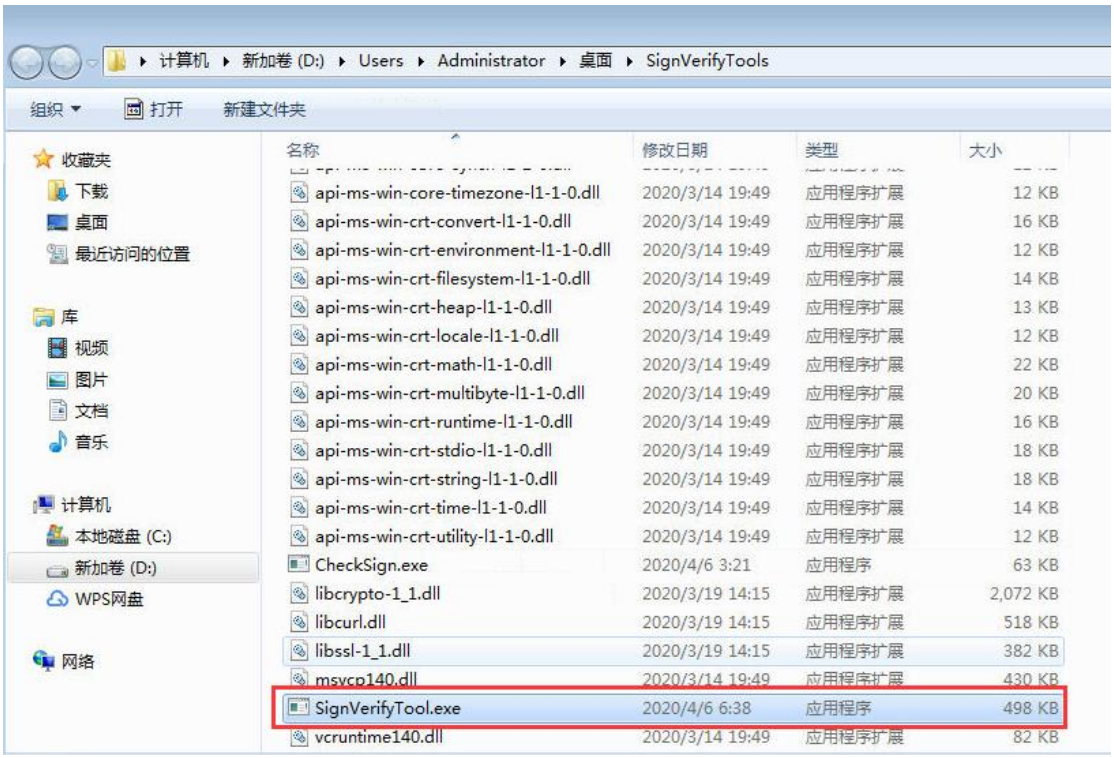
设备控件签名自检工具使用说明

一、单台设备检测

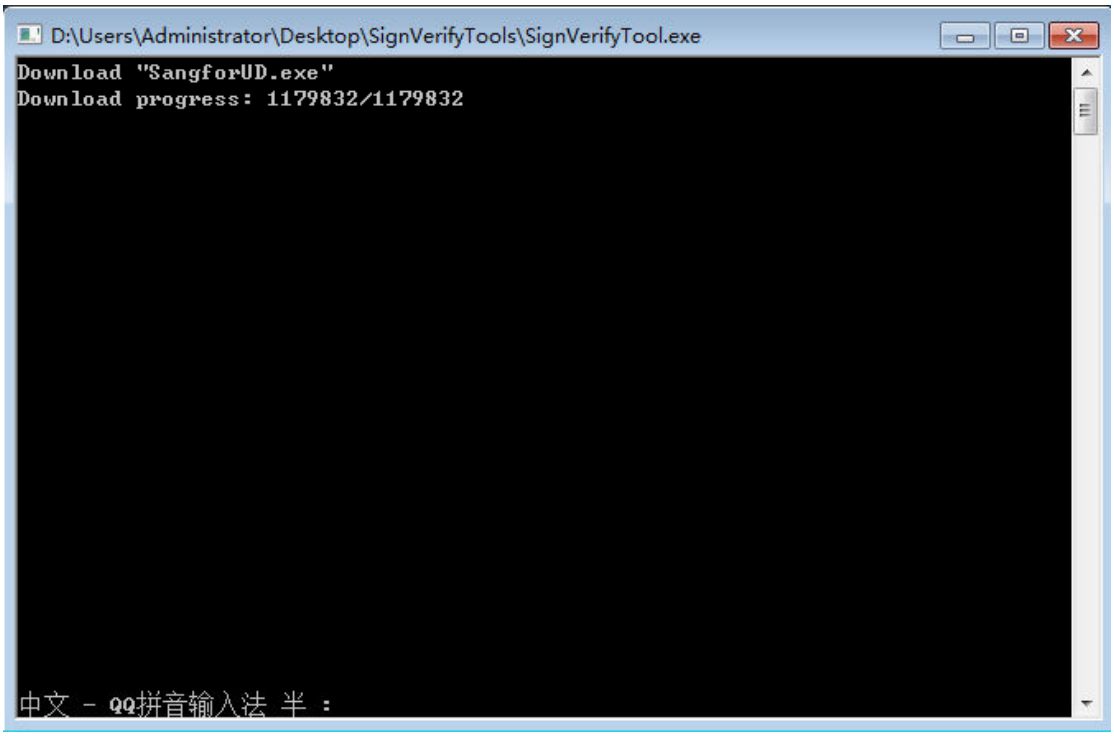
1. 在 Windows 电脑上使用 EasyConnect 登录 SSL VPN 设备。



2. 解压 SignVerifyTools.7z 文件后。

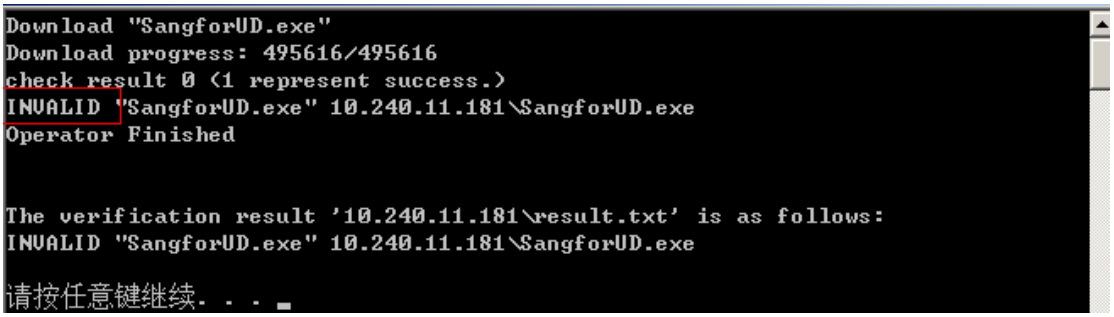


3.双击 SignVerifyTool.exe 运行自检程序，检查结果会在程序控制窗口输出。

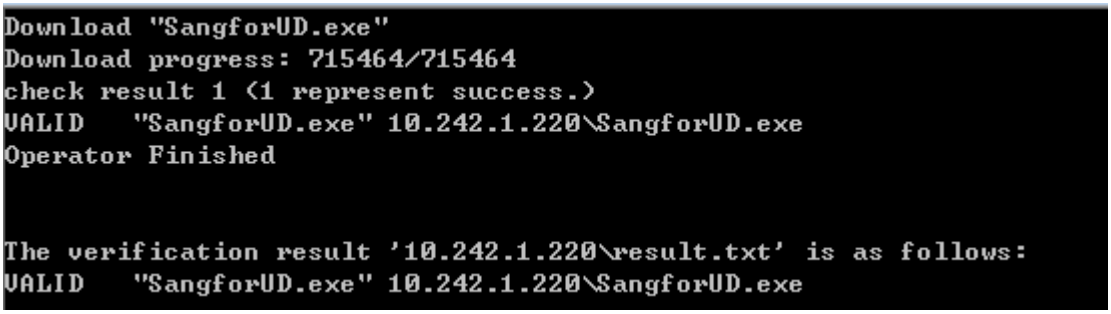


（1）如果当前 PC 上没有正常登录 SSL VPN，运行工具后会提示如下信息：

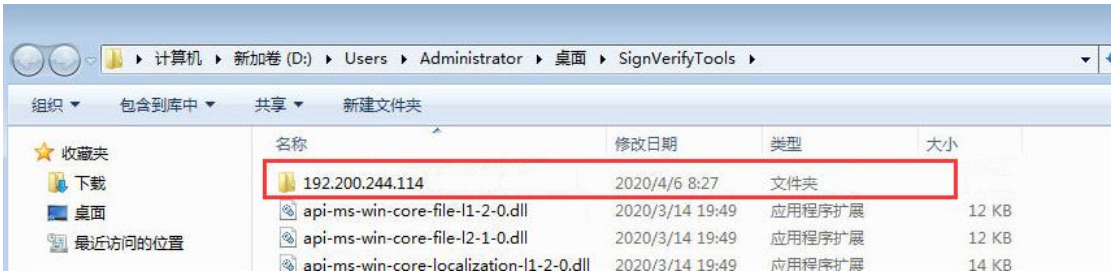
（2）如果设备上的文件被篡改运行后会有“INVALID”的提示

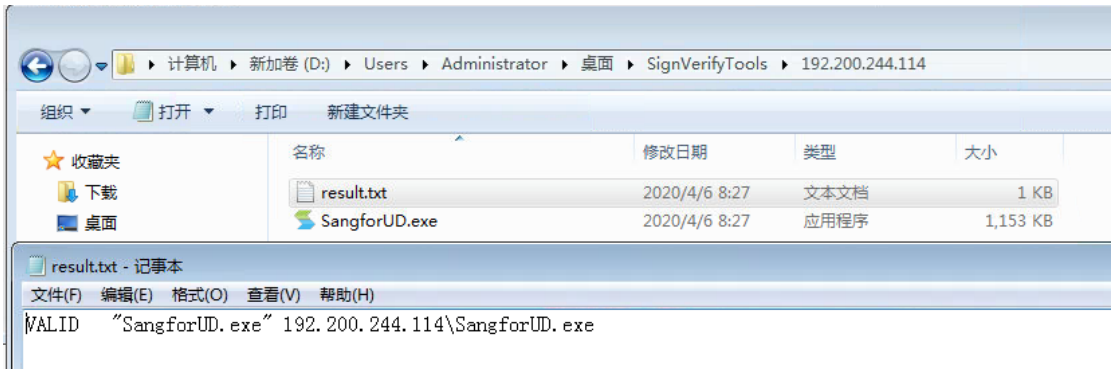


（3）如果设备上的文件未被篡改运行后会有”VALID”的提示



4.最终可以在工具所在目录下生成一个和当前检测设备 IP 相同的目录，下面记录了扫描结果和扫描的控件文件





二、集群环境/分布式集群环境检测

1、 在**内网环境下**分别连接实际节点的 IP，例如 SSL VPN1 的 IP 为 192.168.1.2、SSL VPN2 的 IP 为 192.168.1.3，集群 IP 为 192.168.1.1。
2、 通过 EasyConnect 连接 SSL VPN1 真实的 IP 地址，例如连接 192.168.1.2，登录到对应的 SSL VPN1 设备上。
3、 参考“单台设备检测”方法检测该控件是否被篡改。
4、 通过 EasyConnect 连接 SSL VPN2 真实的 IP 地址，例如连接 192.168.1.3，登录到对应的 SSL VPN4 设备上。
5、 参考“单台设备检测”方法检测该控件是否被篡改。

三、注意事项：

1、 该工具全版本通用。
2、 不支持 Windows XP 和 Windows Server 系列系统使用 SignVerifyTools 工具。
3、 只能检测当前通过 EasyConnect 登录的 SSL VPN 设备。
4、 集群环境下检测无需拆分集群，但是需要每台设备单独检测。
5、 工具支持有 EasyConnect 定制或补丁包的环境下做检测，若检测通过，则说明服务端控件未篡改。
6、 如果发现设备被篡改。请立即联系当地技术服务工程师或拨打 400-630-6430。