客户端实用工具

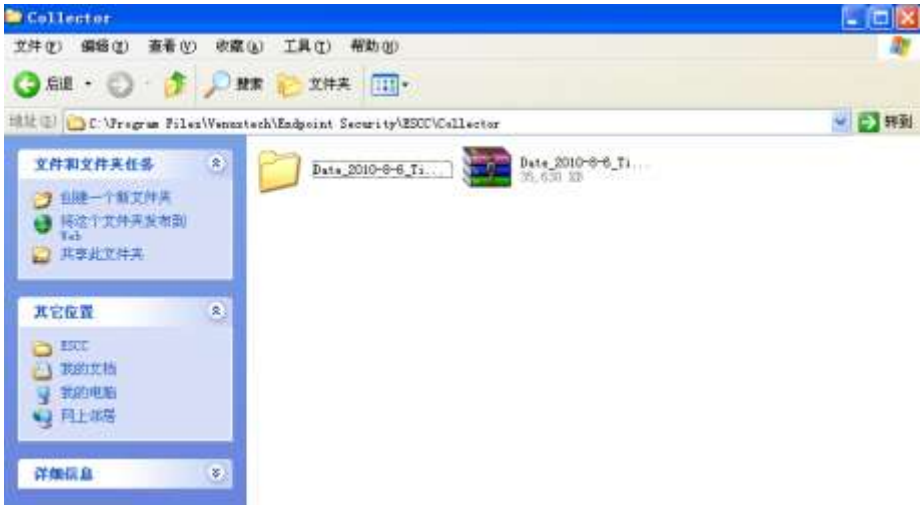
天珣自带有部分供服务器和客户端使用的工具，包括服务器诊断工具、客户端诊断工具离线补丁工具等，这些工具放在安装光盘的 tools 目录中。

天珣客户端诊断工具

天珣客户端诊断工具是当客户端发生异常，例如线程、句柄数过多，CPU、内存占用率过高，CC 无法停止服务等，收集客户端软硬件信息以及 dmp 文件以便分析的一个实用诊断工具。

在客户端发生异常而无法定位时，管理员将天珣客户端诊断工具拷贝到客户端任何一个目录里，运行：

运行后显示“正在收集信息中，请稍候。。”此时工具将收集必要的信息，完成后将自动打开已收集信息的文件目录：

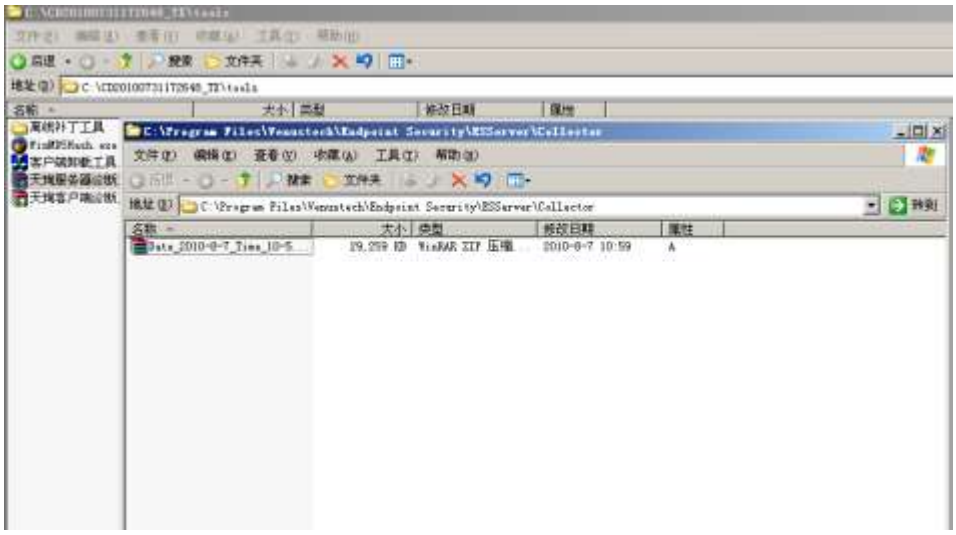


默认文件保存在客户端安装目录的 collector 目录下，只有在运行过客户端诊断工具之后才会自动产生此目录。

将此诊断文件进行分析，可以深层次的分析出客户端目前的运行状态，从而有针对性的发现问题和解决问题。

天珣服务器诊断工具

天珣服务器诊断工具与客户端诊断工具类似，在服务器出现异常时，可以用此工具收集一些必要的信息和 dmp 文件：



运行完成后在服务器安装目录的 collector 目录下生成诊断文件，并由这个诊断文件来分析服务器出现的问题。

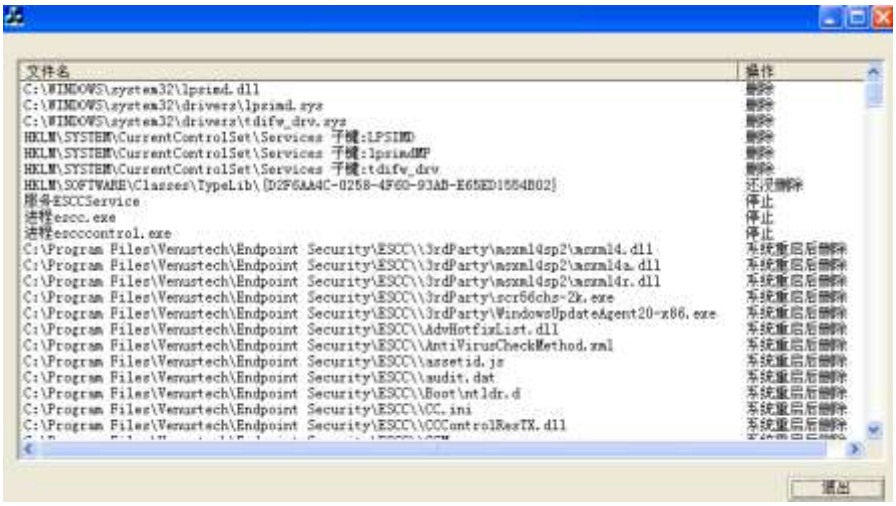
客户端卸载工具

虽然天珣提供自动卸载客户端的策略配置，但是有时由于某些未知原因，天珣客户端无法卸载或者卸载不完全，此时可以使用此客户端卸载工具将客户端完全卸载掉。

在客户端上运行此卸载工具：

点击“是”进行卸载，完成后提示：

点击“确定”后将会显示卸载过程和删除与未删除的文件信息：

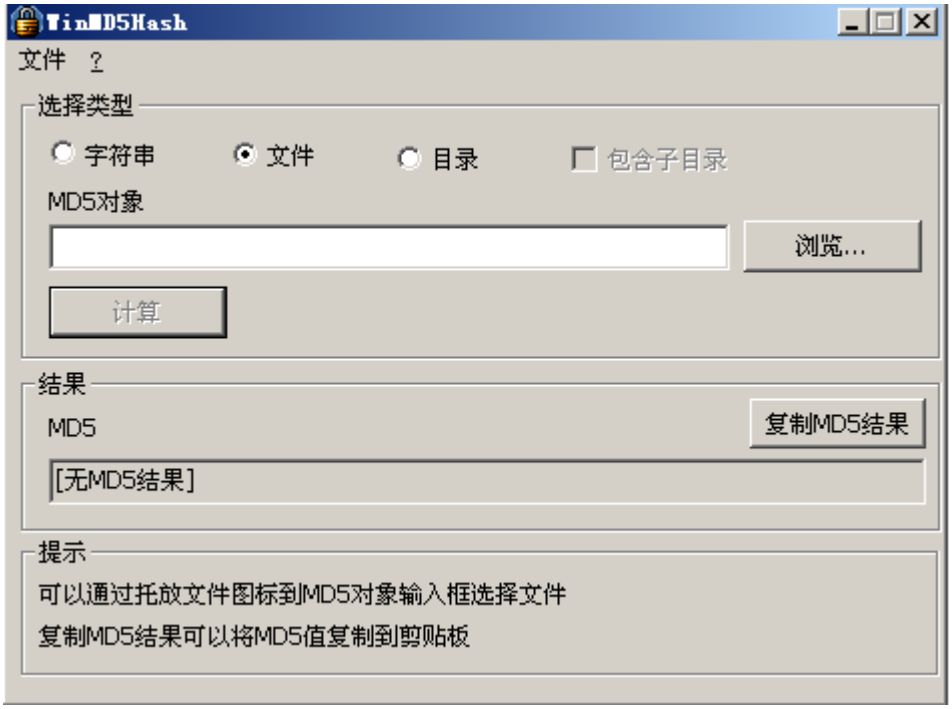


系统重启后客户端就已完全卸载。

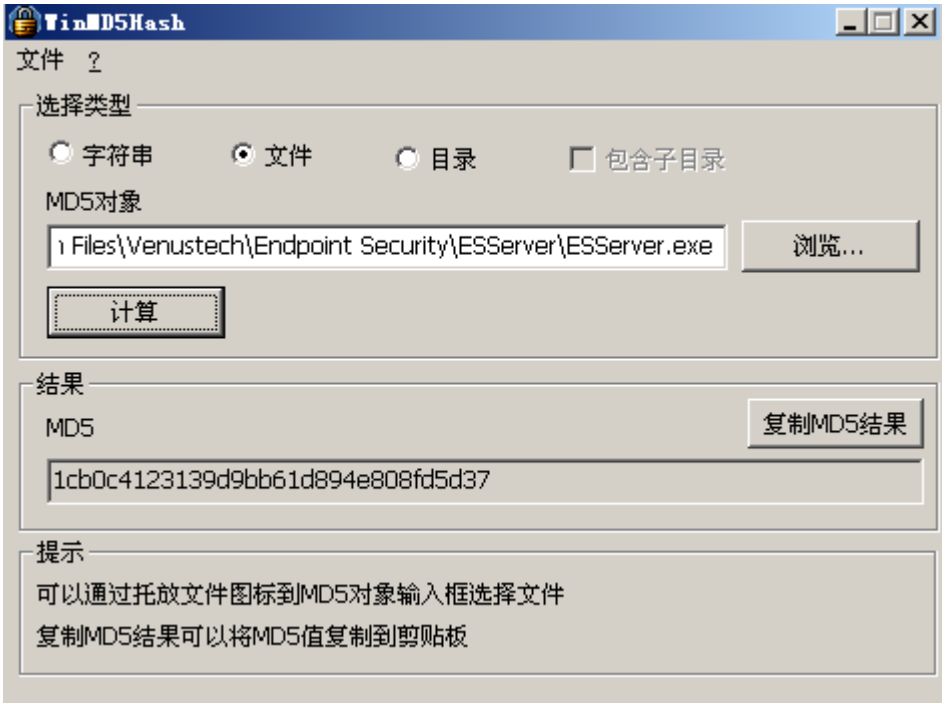
Winmd5Hash.exe

此工具是用来对某些进程或文件生成 md5 码的，在配置进程红名单时，可能担心客户端通过修改文件名等方式伪造红名单进程，那么可以通过对此进程或软件进行 md5 码校验来避免。

此工具就是用来从外部生成 md5 码的，双击打开工具：



选择“文件”、“字符串”或“目录”，以“文件”为例，点击浏览选择想要生成 md5 码的文件或进程名：



点击计算即可生成 md5 码值，再点击“复制 md5 结果”，将其复制到剪贴板，然后在配置策略时将此 md5 码粘贴过去即可。

经过 md5 码校验的红名单进程或软件，如果客户端伪造一个同名称的进程，将会被检

测到与 md5 码不匹配导致客户端不符合安全基线要求。

离线同步工具

在一些军工或政府部门，一般内网中是不允许上互联网的，但是用户可能又需要使用在线补丁和更新病毒码的功能。由于无法上网中心服务器无法连接到互联网上的外网服务器，那么只有通过离线同步工具来间接导入外网服务器上的补丁和病毒码。

“离线同步工具”位于 tools 文件夹中。当中心服务器不能连接外网时，就可以使用“离线同步工具”去同步外网上的补丁。 “离线同步工具”需要有一个有效的 license 授权才能去同步外网上的补丁，将离线同步工具和有效的 license 一起拷贝到能连接外网的计算机上，便可下载外网上的补丁，并且会在离线同步工具目录下生成一个名为 OfflineHotfix 的文件夹，所有从外网下载回来的补丁都放在该文件夹下。当同步完外网补丁之后，将离线同步工具文件夹整个的拷贝到装有中心服务器的计算机上，“补丁导入本地”便可将 OfflineHotfix 文件夹里面的补丁文件全部导入到中心服务器 Venustech\Endpoint Security\ESServer\Download\AutoUpdate 目录下。

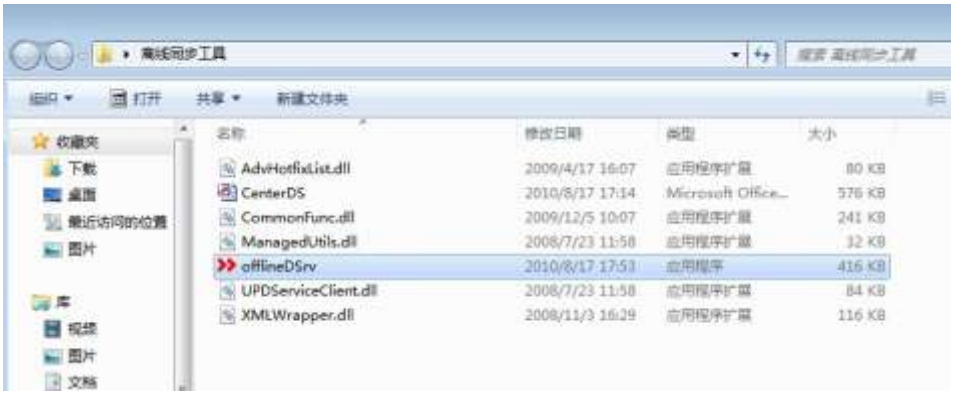
注意 1：运行离线同步工具的计算机必须安装 framework。
注意 2：有效 license 授权是指没有过期的并且是天珣研发中心正式授予的 license，不受 IP 地址绑定的限制
注意 3：离线同步工具不支持断点续传，即如果在同步外网补丁中途断网的话，只能重新运行该工具。
注意 4：离线同步工具只能将补丁导入中心服务器，不能导入到本地服务器，本地服务器上的补丁必须从中心服务器上同步。
注意 5：离线同步工具同步外网服务器上的补丁文件时，该工具所在的目录盘的可用空间必须大于 2G

离线同步工具使用流程是这样的：

首先将离线同步工具拷贝到一台可以上互联网的普通 PC 上，通过这台能上互联网的 PC 将外网服务器的补丁和病毒码同步下来，然后再将这些补丁、病毒码和一些相关配置文件拷贝到内网的中心服务器上进行导入即可。

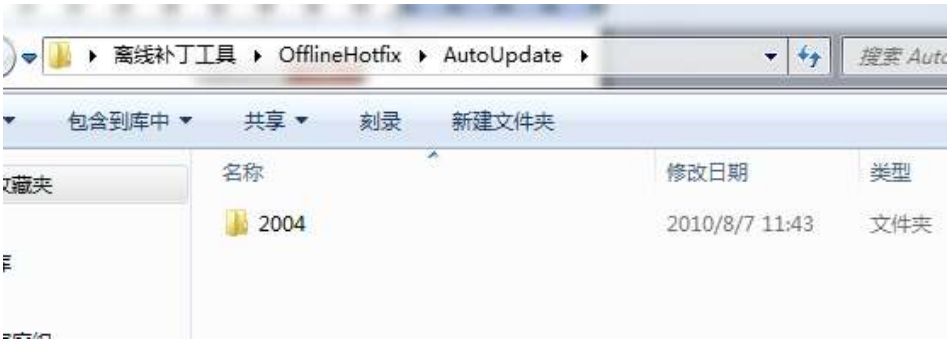
离线同步工具导入外网补丁

将 license 放在离线同步工具目录下，并拷贝到可上互联网的机器上，点击运行 offlineDSrv，并点击“外网补丁下载”：



当目录中没有 license 文件或 license 文件有问题时，将会显示加载 license 失败！

在同步过程中，我们可以看到在离线同步工具的目录下会自动生成 OfflineHotfix 目录，在此目录下自动同步外网服务器上的补丁：



同步完成后，将离线同步工具目录拷贝到内网中心服务器任何目录下，并运行，点击“补丁导入到本地”：

发布成功后，打开中心服务器安装目录的 download\AutoUpdate 目录，可以看到已经将补丁同步过来：

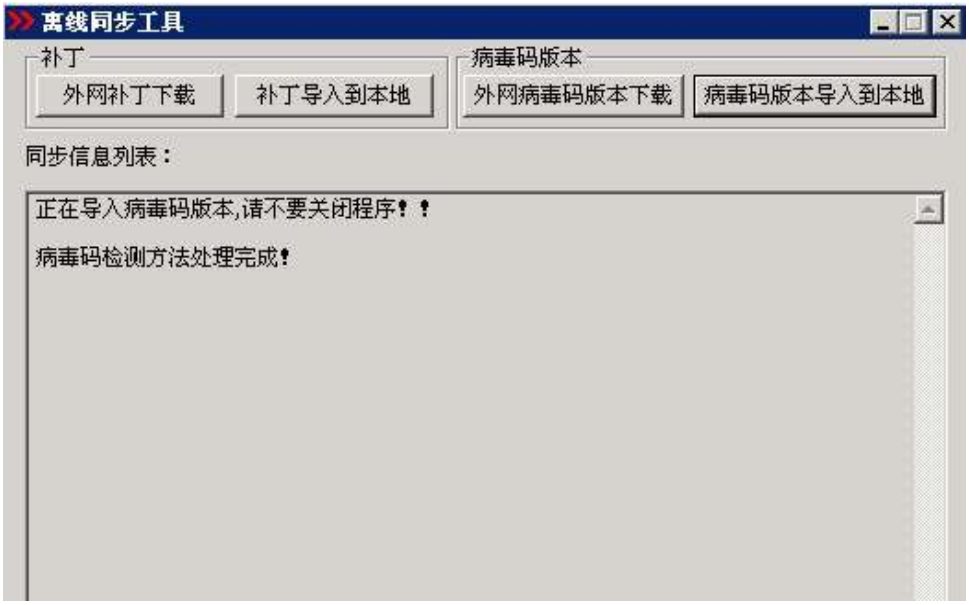
然后打开服务器 web 管理界面，在在线补丁源页面中可以看到已经同步的补丁列表，在补丁分发中可以将其分发到客户端：

离线同步工具导入外网病毒码

将 license 放在离线同步工具目录下，并拷贝到可上互联网的机器上，点击运行

offlineDSrv，并点击“外网病毒码版本下载”：

同步完成后，将离线同步工具目录拷贝到内网中心服务器任何目录下，并运行，点击“补病毒码版本导入到本地”：



发布成功后，打开 web8833 页面上的安全基线—》防病毒软件策略，然选一个防病毒软件，进入该策略的编辑页面，点击“选择病毒码版本”

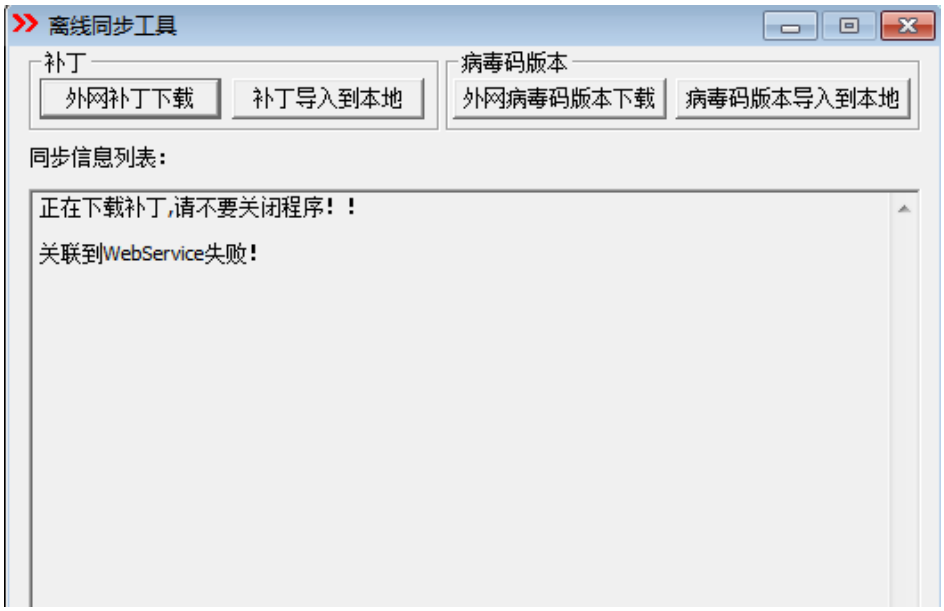
此时会弹出一个提窗口，如果在外网服务器上该防病毒软件有新增的病毒码版本，同步完成后该窗口就会出现相应的新的病毒码：

离线同步工具相关异常页面：

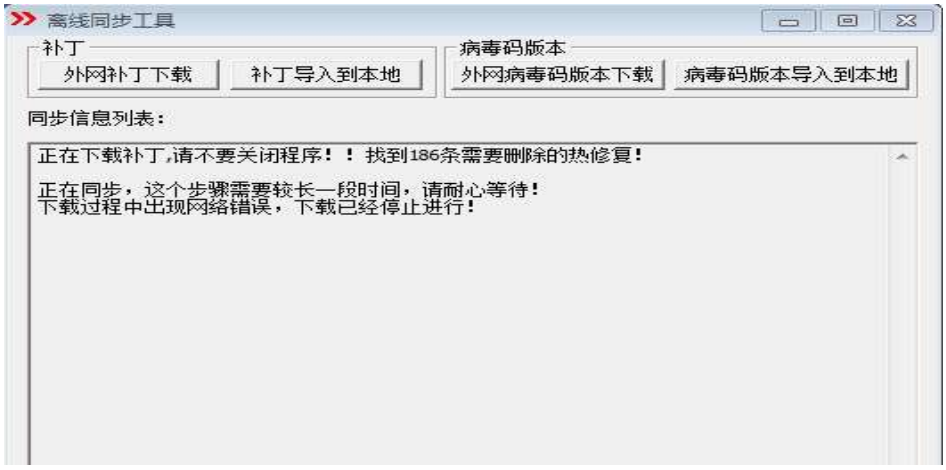
（1）当运行离线补丁工具的计算机没有安装 framework 时，提示如下：

（2）当离线补丁工具目录中没有放入 license 授权，运行该工具，提示如下：

（3）当离线补丁工具运行的计算机没有同外网连接时，提示如下：



（4）在下载外网补丁的过程中，网络中断，提示如下：

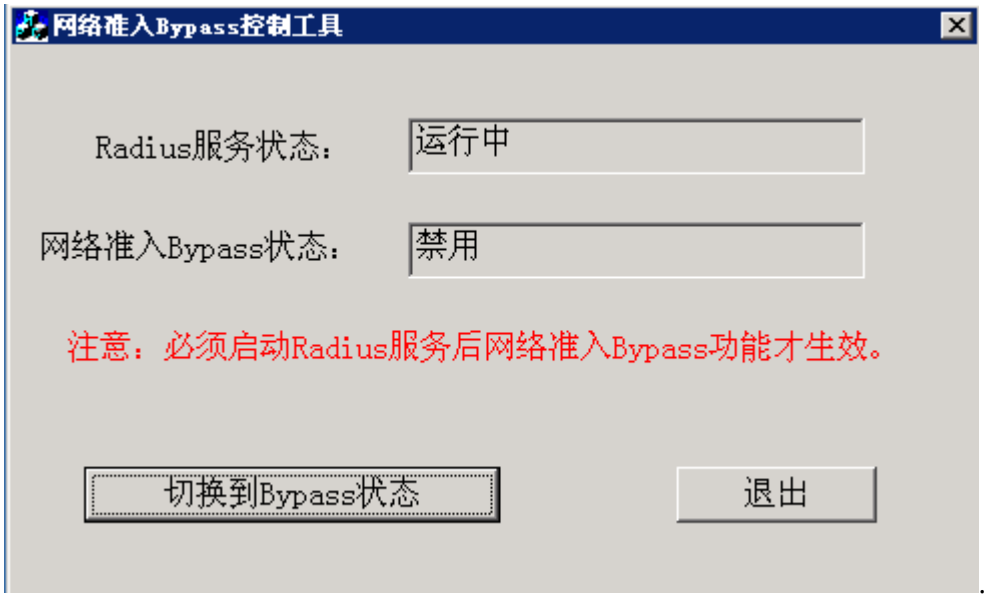


（5）补丁导入本地时，如果导入的计算机没有安装中心服务器时，提示如下：

Radius By Pass 工具

RadiusBypass 适用与网络准入跟 AD 域结合使用的网络准入认证方案.当 AD 域出现故障时,开启 RadiusBypass 工具,可及时将准入认证方案切换成只认证客户端,终端网络准入认证不需要输入 AD 域的用户名密码，就可以通过网络准入认证。

该工具需要运行在安装有 Radius 服务器的机器上。



Radius 故障告警工具

工具适用于用户名密码登录的网络准入认证方式的告警.将告警日志存放到 FTP 服务器上.

工具需配置 RADIUS,域的参数,及 FTP 服务器的地址.

用户名:填写域中的用户名,

密码:用户的密码。

目录名:名称与天珣配置页-基本配置-用户组-目录服务中的目录服务名称对应,不是域的名字。

Radius IP 地址:可以填写多个，每个 ip 以 ，隔开


RadiusAuthTest
radius检测配置
用户名:
adusetest
密码:
****
目录名:
testwork
radius IP地
172.18.20.23
*多个服务器以 , 隔开
日志上报配置
ftp地址:
172.18.20.3
ftp端口:
21
ftp用户名:
user
ftp用户密码:
123456
开始测试
关闭程序