RELIABLE NETWORK
SAFE WORLD
TOPSEC

天融信终端威胁防御系统
服务器版本安装手册

天融信
TOPSEC

1 安装 windows 客户端

天融信终端威胁防御系统的客户端程序安装在用户的桌面系统上，并执行企业管理中心管理员配置的安全策略，对桌面系统进行监管维护。

安装客户端软件，需要通过已经部署完成的企业管理中心进行下载安装。

注意：安装此终端威胁防御客户端前卸载 360 杀毒、电脑管家等其他杀毒软件

1.1 下载客户端

下载客户端程序的步骤如下：

1）通过浏览器登录客户端下载界面，访问：**http://172.16.204.217**，进入下载页面，如下图所示。

2）点击“本地下载”按钮，将安装包保存到本地。也可选择点击“离线包下载”按钮，将离线包保存到本地。

1.2 安装客户端

安装客户端程序的具体步骤如下：

1） 下载完成后，程序名称格式如 installer_1.0.15.0(https#172.16.204.217_8090)_32_chs.exe。双击下载的程序，弹出安装窗口，如下图所示。

如果企业管理中心和客户端主机之间的网络不正常等原因，可能弹出如下安装窗口。

输入企业管理中心的地址和提供安装升级服务的端口，在此文本框中输入：http://172.16.204.217:8090。此时，要保证企业管理中心和客户端主机之间的网络连接始终正常。

2）输入完成后，点击“确定”按钮，如下图所示。

输入客户端的责任人，选择客户端所属的部门（务必选中自己所在的部门）、所在的物理位置以及终端类型。

3）输入完成后，点击“确定”按钮，如下图所示。

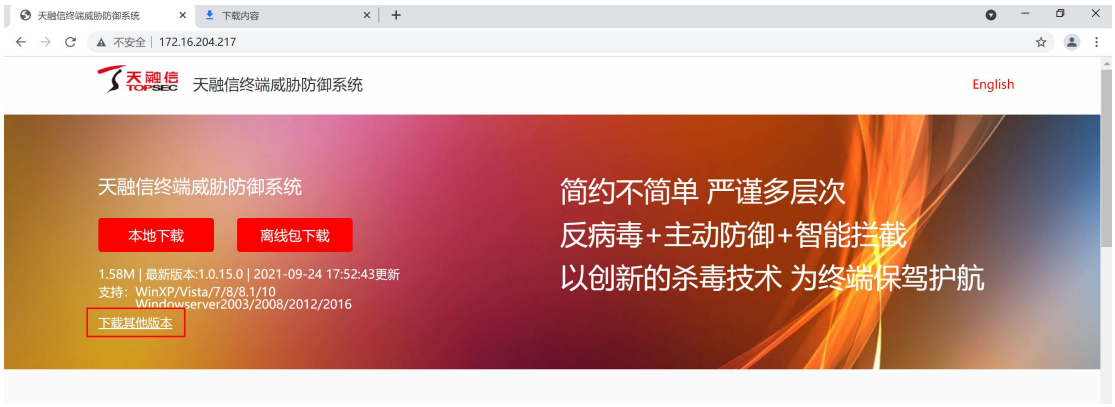
4）安装完成后，直接进入客户端首页，如下图所示。

安装后，可在企业管理中心的终端中心中对该终端进行管理，关于管理终端的操作具体请参见《天融信终端威胁防御系统用户手册》。

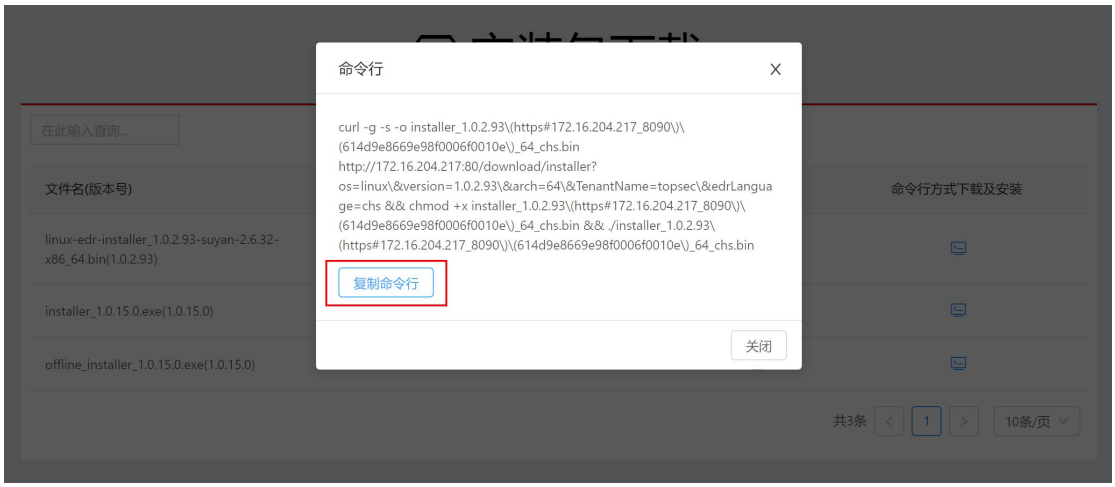
2 安装 linux 客户端

2.1 命令行下载方式及安装

1）通过浏览器登录客户端下载界面，访问：**http://172.16.204.217**，进入下载页面，如下图所示，点击**下载其他版本，**进入安装包下载页面



2）点击第一个 linux-edr 的命令行方式下载及安装，弹出命令行框，点击复制命令行



curl -g -s -o installer_1.0.2.93\(https#172.16.204.217_8090\)\(614d9e8669e98f0006f0010e\)_64_chs.bin http://172.16.204.217:80/download/installer?os=linux\&version=1.0.2.93\&arch=64\&TenantName=topsec\&edrLanguage=chs && chmod +x installer_1.0.2.93\(https#172.16.204.217_8090\)\(614d9e8669e98f0006f0010e\)_64_chs.bin && ./installer_1.0.2.93\(https#172.16.204.217_8090\)\(614d9e8669e98f0006f0010e\)_64_chs.bin

3）进入 linux 系统的命令行窗口，使用 root 账号复制上面的命令，回车进行安装。

4）输入客户端的责任人，选择客户端所属的部门、所在的物理位置以及终端类型，点击确定，然后提示 setup completed successfully 表示安装成功。

```
[root@localhost /]# curl -g -s -o installer_1.0.2.93\(https#172.16.204.217_8090\)\(614d9e8669e98f0006f0010e\)_64_chs.bin http://172.16.204.217:80/download/installer?os=linux\&version=1.0.2.93\&arch=64\&TenantName=topsec\&edrLanguage=chs && chmod +x installer_1.0.2.93\(https#172.16.204.217_8090\)\(614d9e8669e98f0006f0010e\)_64_chs.bin && ./installer_1.0.2.93\(https#172.16.204.217_8090\)\(614d9e8669e98f0006f0010e\)_64_chs.bin
 *****Welcome to TOPSEC Linux Client*****
[INFO] setting maxmum inotify watches is complete
[INFO] Install topsec virus library
[INFO] start preinstall check
[INFO] Online Installation
614d9e8669e98f0006f0010e
/etc/topav/config_global.conf
{
        "server": {
                "scheme": "https",
                "host": "172.16.204.217",
                "port": 8090
        },
        "install_info": {
                "person": "172.16.204.75",
                "type": "服务器",
                "location": "t1",
                "department": "/All/linux"
        },
        "tenancy_id": "614d9e8669e98f0006f0010e",
        "product_version": "1.0.2.93",
        "outofcontrol": false
}

Stopping Topsec Linux antivirus client:                    [FAILED]
Error:  Service is not installed

Removing Topsec Linux antivirus client:                    [FAILED]
Error:  Service is not installed

20211018-09:36:45.09 Install Topsec Linux antivirus client:                         [  OK  ]

20211018-09:36:45.15 Starting Topsec Linux antivirus client:                        [  OK  ]
 setup completed successfully
[root@localhost /]#
```

2.2 客户端手动使用相关功能

```
[root@localhost /]# topclientctl  foreground

20211018-14:55:16.17 Stopping Topsec Linux antivirus client:                                [  OK  ]

【进程号】 23583
==================欢迎使用天融信客户端==================
【信息】开启时间  2021-10-18 14:55:16
【开启】接收扫描信息和隔离区信息管道协程
【初始化】扫描日志通道配置
【异常账户】 [{polkitd 2 密码失效}]
2021/10/18 14:55:17 Seeked /var/log/secure - &{Offset:0 Whence:2}
【上报异常账户状态】  0 insert data success
2021/10/18 14:55:17 webrce_report.go:38: 设置WebRCE日志
2021/10/18 14:55:17 localextraction_report.go:37: 设置本地提取日志
2021/10/18 14:55:17 syscmdtamper_report.go:37: 设置系统命令篡改日志
2021/10/18 14:55:17 Seeked /var/log/audit/audit.log - &{Offset:0 Whence:2}
2021/10/18 14:55:17 Seeked /var/log/audit/audit.log - &{Offset:0 Whence:2}
2021/10/18 14:55:17 Seeked /var/log/audit/audit.log - &{Offset:0 Whence:2}
xxx,0xxx,02021/10/18 14:55:17 scanlogmonitor.go:56: exit status 6
2021/10/18 14:55:17 scanlogmonitor.go:63: exit status 1
2021/10/18 14:55:17 Seeked /topsec/topav_client/bin/scanlogd/scanlogd.log - &{Offset:0 Whence:2}
【CONNECT STATUS】Connected


##########显示菜单##########
 a  病毒扫描
 c  隔 离 区
 d  升    级
 e  策略信息
 f  本地详情
 g  后门检测
 q  退出程序
选择任务：a
```