

EDR杀毒软件安装操作指南

一、EDR杀毒软件下载：

1. 可以登录OA系统，在“工具下载”处，下载安装包。如下图示：



2. 在浏览器地址栏输入：<https://192.168.10.161/ui/login.php> 可直接在登录控制台界面下载，如下图示：（建议使用谷歌浏览器, 或IE11以上版本浏览器）



3. 在浏览器地址栏输入：https://192.168.10.161/ui/web_install.php 可直接在登录控制台界面
下载。（建议使用谷歌浏览器,或IE11以上版本浏览器）

二、EDU杀毒软件安装方法

1. Windows平台客户端安装方法

（注意：windos系统，特别是XP系统,安装前先关闭其它杀毒软件）

前提环境确认：检测终端主机与终端检测响应平台网络是否正常通信。安装Agent的telnet命令检测管理平台(192.168.10.161)的443、8083、54120端口是否可以正常通信(端口不通的话，关闭电脑防火墙，再试), 如下图示：



```
ca. 管理员: 命令提示符
Microsoft Windows [版本 10.0.16299.15]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>telnet 192.168.10
正在连接 192.168.10... 无法打开到主机的连接。 在端口 23: 连接失败

C:\Users\Administrator>telnet 192.168.10.161 443
```

点击Windows『下载安装包』按钮，下载安装软件。



双击进行安装

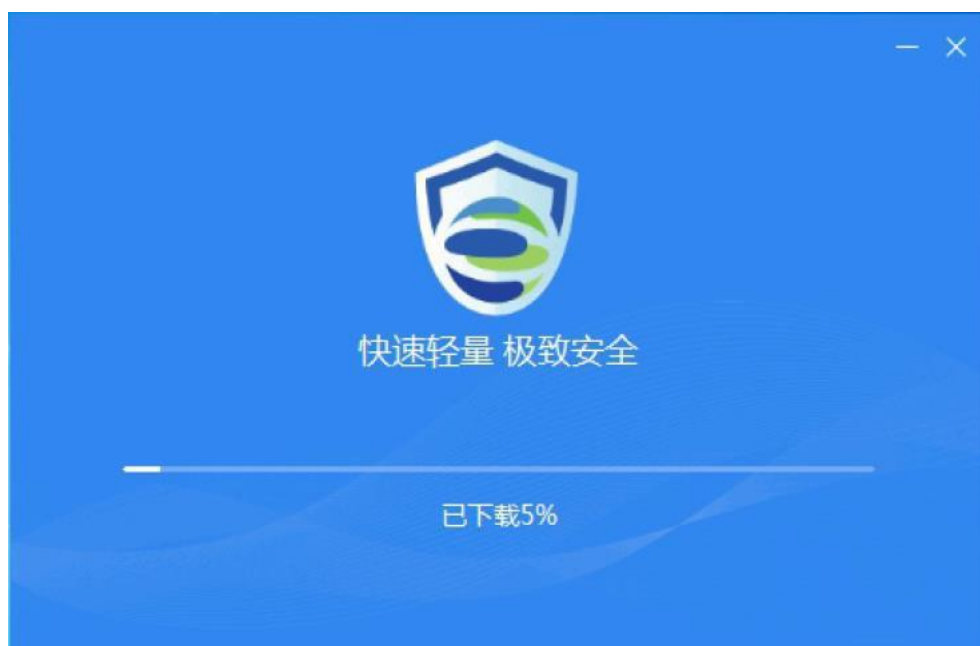


选择安装目录，默认为C:\ProgramFiles\Sangfor\EDR\agent
若终端上已经存在其它的杀毒软件会提示以下信息，如下图：



选择兼容模式可继续安装，将会关闭文件实时监控功能。建议安装前卸载其它杀毒软件
再进行安装。

进行安装



完成安装



完成安装后点击桌面的图标：进行资产配置。填写[归属信息]。

EDR终端防护中心

安装成功！请完善和确认您的资产信息

基本信息

计算机名称： HBZ-PC
IP地址： 192.200.244.45
MAC地址： FE-FC-FE-B0-96-61
操作系统： Windows 7 x64

归属信息

资产名称： sangfor
资产责任人： hbz
工号： xxxx
联系方式： 18926349301
邮箱： xxx@xxxx.com
资产位置： xxxx

开启防护

开启防护。



安装完成。



2. Linux平台Agent安装方法

前提环境确认：检测终端与终端检测响应平台网络是否正常通信。使用nc检测管理平

台的443、8083、54120端口是否可以正常联通。

如：nc -v -w 10 EDR_IP地址端口8083进行端口测试。

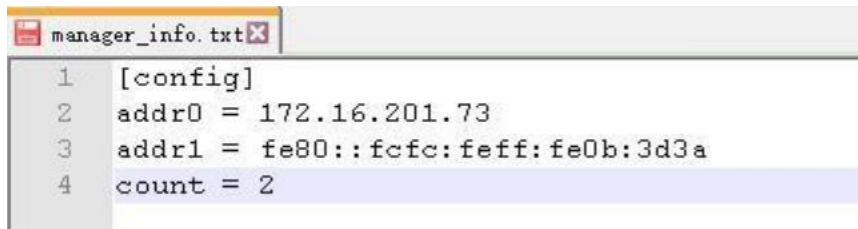
```
nc-v-w10192.168.10.1618083
```

方法一：

下载安装软件



将文件拷贝到linux终端中，以一台64位操作系统终端为例，解压文件，使用无参安装执行./agent_installer.sh，-管理平台地址通过manager_info.txt进行修改



```
manager_info.txt X
1 [config]
2 addr0 = 172.16.201.73
3 addr1 = fe80::fcfc:feff:fe0b:3d3a
4 count = 2
```

使用自定义安装(安装路径可选)./agent_installer.sh-h<managerip>-p
<managerhttpsport>-d<installdir>-f，指定安装目录、managerIP和端口完
成安装。

(tips:每个命令之间有空格)


```
[root@redhat64-x64 ~]# ls
anaconda-ks.cfg EPS_1.0_Build_20161201.tar.gz install.log install.log.syslog
[root@redhat64-x64 ~]# tar -zxvf EPS_1.0_Build_20161201.tar.gz
agent_installer.sh
manager_info.txt
[root@redhat64-x64 ~]# ./agent_installer.sh /home/eps/agent 200.200.128.60
start download eps module
download eps module success
/home/eps/agent install success
eps start success
[root@redhat64-x64 ~]#
```

```
[root@localhost zzp]# ./agent_installer.sh -h 10.62.7.15 -p 443 -d /home/ -f
edr agent is installing on x86_64 machines
systemd model
start download edr module
curr install path: /home/sangfor/edr/agent url:https://10.62.7.15:443
agent size is 103.9MB
===== ] [11.77%]
```

方法二:

命令行方式下载agent工作到运行wget的当前目录。

wget--no-check-certificatehttps://%MGRIP%/html/linux_edr_installer.tar.gz

后续安装步骤与方式一解压压缩包后一致。

安装完成。

也可参照下图提示进行安装:



Linux操作系统

- 1、点击下载安装文件，或执行下载命令 `wget --no-check-certificate https://192.168.10.161/download/linux_edr_installer.tar.gz` 进行下载
- 2、将安装包拷贝至终端
- 3、在终端解压安装包 `tar -zxvf linux_edr_installer.tar.gz`
- 4、执行命令 `./agent_installer.sh`
- 5、执行完成，终端的agent程序将自动连接EDR管理中心

(为了提升终端性能，开启微隔离功能的linux终端，建议安装ipset)

