

---

**久安世纪统一安全运维平台**  
**LS-SOP V1.0 管理员快速操作手册**

---

北京久安世纪科技有限公司

2019 年 01 月

## 目录

<b>1. 功能介绍</b> .....	<b>1</b>
<b>2. 环境要求</b> .....	<b>1</b>
<b>3. 初始设置</b> .....	<b>1</b>
3.1 登录设备 .....	1
3.2 IP 地址修改 .....	2
<b>4. 目录添加</b> .....	<b>3</b>
<b>5. 用户添加</b> .....	<b>4</b>
<b>6. 设备添加及授权</b> .....	<b>5</b>
6.1 设备添加 .....	5
6.2 设备账户添加 .....	6
6.3 批量设备授权 .....	7
<b>7. 应用添加及授权</b> .....	<b>9</b>
7.1 应用添加 .....	9
7.2 批量应用授权 .....	10
<b>8. 审计信息查看</b> .....	<b>11</b>
8.1 相关控件安装 .....	11
8.2 TELNET/SSH 录像审计 .....	12
8.3 RDP 图形录像审计 .....	14
<b>9. 注意事项</b> .....	<b>14</b>
<b>10. 应急办法</b> .....	<b>15</b>

## 1. 功能介绍

久安世纪统一安全运维平台（以下简称“LS-SOP”或“堡垒机”）是用于对内部或者第三方运维管理员的运维操作行为进行集中管控审计的系统。可以帮助客户规范运维操作行为、控制并降低安全风险、满足等级保护级其他法规对IT 内控合规性的要求。

## 2. 环境要求

堡垒机登录运维方式提供 Web 页面登录方式，其中 Web 页面支持运维终端采用 Windows/ IE、Google、火狐以及 Mac OS 常用的 Safari 的浏览器登录（指纹认证暂支持 Windows IE 浏览器）。不改变登录运维习惯。

## 3. 初始设置

### 3.1 登录设备

1、首先通过 Web 页面登录：[https://堡垒机\\_IP](https://堡垒机_IP)

（出厂默认 EHT0, IP 为 192.168.1.100），输入用户名密码登录：

默认管理员账户为 admin、密码管理员 password、审计管理员 audit。

默认密码：与厂商联系。



登录首页右侧为堡垒机本机 CPU、硬盘、内存、SWAP 分区的利用率百分比，中间部分则是系统当前的信息，包括系统状态和当前协议并发量信息



### 服务状态查询，查询堡垒机各项服务是否正常运行

The screenshot shows the '服务状态' (Service Status) page. It contains a table with the following data:

服务名称	服务描述	状态	操作
vpn	系统SSL VPN服务	正常	重启 停止
ftp	系统ftp 审计服务	正常	重启 停止
ssh	系统ssh 审计服务	正常	重启 停止
rdp	系统rdp 审计服务	正常	重启 停止
authd	系统认证授权服务	正常	重启 停止
radius	系统radius 服务	正常	重启 停止
play	系统回放服务	正常	重启 停止
ha	双机服务	失败	启动

## 3.2 IP 地址修改

系统配置-网络配置，根据实际使用的网口，来修改对应的网口地址，如下图（以 eth0 为例）：

The screenshot shows the '网络配置' (Network Configuration) page. It contains a table with the following data:

网卡名称	启用	网卡IP	掩码	网关	状态	操作
ETH0	启用	192.168.10.131	255.255.255.0	192.168.10.2	●	修改
ETH1	启用	172.16.210.11	255.255.255.252		●	修改
BR0	禁用	1.1.1.1	255.255.255.255		●	修改

点击修改，输入需要修改后正确的 IP 地址：

网络配置 静态路由 PING TRACE

启动:	启用 ▾
IPv4地址:	192.168.10.131
IPv4掩码:	255.255.255.0
IPv4网关:	192.168.10.2
IPv6启用:	关闭 ▾
IPv6地址:	
IPv6网关:	
DNS服务器一:	
DNS服务器二:	

保存修改

点击保存修改，会提示如下选项，确定修改，和重启网卡服务，根据提示选择即可。

确定要修改吗?

禁止此页再显示对话框。

确定 取消

修改成功,网络将重新启动,确定重启吗?

禁止此页再显示对话框。

确定 取消

## 4. 目录添加

- 1、选择资源管理----资产管理---目录管理

组名	搜索	资源组名称	ID	属性	服务器数	用户数	描述	操作
		test_all	4	全部	0	2		<a href="#">编辑</a>   <a href="#">删除</a>
		分布式资源	5	全部	8	0		<a href="#">编辑</a>   <a href="#">删除</a>
		默认管理员	1	全部	0	3		<a href="#">编辑</a>   <a href="#">删除</a>
		设备组	2	全部	32	0		<a href="#">编辑</a>   <a href="#">删除</a>
		用户组	3	全部	0	1		<a href="#">编辑</a>   <a href="#">删除</a>

[添加新节点](#) [批量添加](#)

2、点击添加新节点（就是目录组的称呼），输入节点名称，其它无需输入，然后点击确认即可（注意：用户组及设备组都在此目录管理下，所以初始设备必须添加节点，便于后续添加用户及设备）。

资源组名称	ID	属性	服务器数	用户数	描述	操作
test_all	4	全部	0	2		<a href="#">编辑</a>   <a href="#">删除</a>
分布式资源	5	全部	8	0		<a href="#">编辑</a>   <a href="#">删除</a>
默认管理员	1	全部	0	3		<a href="#">编辑</a>   <a href="#">删除</a>
设备组	2	全部	32	0		<a href="#">编辑</a>   <a href="#">删除</a>
用户组	3	全部	0	1		<a href="#">编辑</a>   <a href="#">删除</a>

[添加新节点](#) [批量添加](#)

## 5. 用户添加

### 1、选择资产管理---资产管理---用户管理

2017年12月14日 星期四	用户管理	设备管理	目录管理	用户属性	系统类型	SSH公私钥	RADIUS用户	密码密钥	在线用户
	用户名	搜索	<input type="checkbox"/> 显示空目录	<input checked="" type="checkbox"/> 目录截取					
	用户名	真实姓名	运维组	工作单位	令牌状态	生效时间	结束时间	角色	操作链接
	admin	超级管理员	默认管理员		未绑定	2000-01-01 00:00:00	永不过期	管理员	<a href="#">禁用</a> <a href="#">编辑</a> <a href="#">明细</a>
	audit	audit	默认管理员		未绑定	2001-02-10 00:00:00	永不过期	审计员	<a href="#">禁用</a> <a href="#">编辑</a> <a href="#">明细</a>
	password	password	默认管理员		未绑定	2001-02-10 00:00:00	永不过期	密码管理员	<a href="#">禁用</a> <a href="#">编辑</a> <a href="#">明细</a>
	<input type="checkbox"/> test_ceshi	testadmin	test_all		未绑定	2017-11-14 17:11:50	永不过期	运维用户	<a href="#">禁用</a> <a href="#">编辑</a> <a href="#">明细</a> <a href="#">删除</a>
	<input type="checkbox"/> test_ceshi1	test_ceshi1	test_all		未绑定	2017-12-14 22:41:53	永不过期	配置管理员	<a href="#">禁用</a> <a href="#">编辑</a> <a href="#">明细</a> <a href="#">删除</a>
	<input type="checkbox"/> test_zhang	zhang	用户组		未绑定	2017-12-10 22:41:51	永不过期	部门管理员	<a href="#">禁用</a> <a href="#">编辑</a> <a href="#">明细</a> <a href="#">删除</a>

[添加用户](#) [删除用户](#) [编辑选中](#) [批量添加](#) [批量编辑](#) [锁定](#) [AD编辑](#) [导入](#) [导出](#)

页次: 1/1页 20条日志/页 共6条 转到第  页 [首页](#) [上一页](#) [下一页](#) [末页](#)

2、点击添加用户，进行编辑用户信息。此时如添加普通运维账户，只需填写用户名、真实姓名、密码、确认密码和运维组即可，其它选项为可选项，一般无需填写。

用户管理 设备管理 目录管理 用户属性 系统类型 SSH公私钥 RADIUS用户 密码密钥 在线用户

**基本信息**

\*用户名:  \*真实姓名:

\*密码:   随机密码 弱 中 强 \*确认密码:   强制修改密码

电子邮件:  手机号码:

工作单位:  工作部门:

\*运维组: 资源组  证书CN:

生效时间:  过期时间:   永不过期

启用:  限制工具登录:  来源IPv4: 无 来源IPv6: 无 周组策略: 无

同步外部密码: 关闭 LDAP/AD DN:

认证方式:  本地  RADIUS  LDAP  AD  短信  邮件  指纹  本地+指纹 单一认证

优先登录方式: 本地登录 透明登录: RADIUS

WEBportal认证:  Webportal超时时间:

4、输入完成后，点击最下方：保存修改按钮即可。

## 6. 设备添加及授权

### 6.1 设备添加

1、登录设备，选择资源管理---资产管理---设备管理

2017年12月14日 星期四 用户管理 **设备管理** 目录管理 用户属性 系统类型 SSH公私钥 RADIUS用户 密码密钥 在线用户

运维审计 + 报表统计 + 资源管理 - 资产管理 应用发布 策略设置 授权权限 系统配置 + VPN + 其他 +

IP	主机名	系统	设备组	操作
10.43.32.176	总局堡垒机 (主机)	堡垒机平台	分布式堡垒机资源	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
10.43.32.177	总局堡垒机 (备机)	堡垒机平台	分布式堡垒机资源	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
10.43.32.178	一分局堡垒机	堡垒机平台	分布式堡垒机资源	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
10.43.32.179	二分局堡垒机	堡垒机平台	分布式堡垒机资源	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
10.43.32.180	三分局堡垒机	堡垒机平台	分布式堡垒机资源	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
10.43.32.181	边防总队堡垒机	堡垒机平台	分布式堡垒机资源	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
10.43.32.182	消防总队堡垒机	堡垒机平台	分布式堡垒机资源	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
10.43.32.183	铁侦总队堡垒机	堡垒机平台	分布式堡垒机资源	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
47.94.229.159	Linux测试机-159	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
47.94.229.160	Linux测试机-160	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
47.94.229.161	Linux测试机-161	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
47.94.229.162	Linux测试机-162	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除

2、点击添加，进行编辑设备资产信息。一般只需填写主机名、系统类型、IPv4 地和和运维组即可，其它选项为可选项，根据实际情况，一般无需填写。

用户管理 **设备管理** 目录管理 用户属性 系统类型 SSH公私钥 RADIUS用户 密码密钥 在线用户

### 基本信息

\*主机名:  \*系统类型: AIX

\*IPV4地址:  IPV6地址:

\*设备组: 资源组

超级管理员口令:  再输一次口令:

修改方式:  按月  每周  自定义 频率:

\*\*频率说明: 如果修改方式选择每周, 这里填写周记 (1-7), 如果按月, 填写几号 (1-7), 如果是自定义, 这里是几日更新一次 (大雨0的整数)

SSH默认端口:  TELNET默认端口:

FTP默认端口:  RDP默认端口:

VNC默认端口:  X11默认端口:

### 扩展信息

固定资产名称:  规格型号:

部门名称:  存放地点:

4、输入完成后，点击最下方：保存修改按钮即可。

## 6.2 设备账户添加

1、查看已添加好的设备，选择右侧用户进行设备账户添加：

用户管理 **设备管理** 目录管理 用户属性 系统类型 SSH公私钥 RADIUS用户 密码密钥 在线用户

IP  主机名  搜索  显示空目录  目录截取

服务器地址	主机名	系统	设备组	操作
<input type="checkbox"/> 47.94.229.159	Linux测试机-159	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
<input type="checkbox"/> 47.94.229.160	Linux测试机-160	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
<input type="checkbox"/> 47.94.229.161	Linux测试机-161	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
<input type="checkbox"/> 47.94.229.162	Linux测试机-162	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
<input type="checkbox"/> 47.94.229.163	Linux测试机-163	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
<input type="checkbox"/> 47.94.229.164	Linux测试机-164	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
<input type="checkbox"/> 47.94.229.165	Linux测试机-165	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
<input type="checkbox"/> 47.94.229.166	Linux测试机-166	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
<input type="checkbox"/> 47.94.229.167	Linux测试机-167	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除
<input type="checkbox"/> 47.94.229.168	Linux测试机-168	Linux	设备组	<input checked="" type="checkbox"/> 修改 <input type="checkbox"/> 用户(1) <input type="checkbox"/> 应用(0) <input type="checkbox"/> 删除

2、点击添加，如下图

[用户管理](#)
[设备管理](#)
[目录管理](#)
[用户属性](#)
[系统类型](#)
[SSH公私钥](#)
[RADIUS用户](#)
[密码密钥](#)
[在线用户](#)

选	ID	主机名	IP	系统	系统用户	登录方式	账号信息
---	----	-----	----	----	------	------	------

[添加](#)
[批量添加](#)
[锁定](#)
[导出该主机下的用户](#)

添加用户时，用户名、原始密码、再次输入原始密码栏为必选项（此时的用户名密码为被管理设备的账户密码，如 administrator、root 等），其它根据实际情况来进行选择，如下图：

用户名:	<input type="text"/>	<input type="checkbox"/> 空用户
原始密码:	<input type="password"/>	RADIUS用户认证: <input type="checkbox"/>
再次输入原始密码:	<input type="password"/>	
登录方式:	ssh	是否支持sftp传输: <input type="checkbox"/>
端口:	22	
过期时间:	<input type="text"/>	<input checked="" type="checkbox"/> 点击选择日期或选 永不过期
用户终端:	默认	
命令授权用户:	admin	

2、绑定组或绑定用户，上栏添加好用户名密码，下栏为绑定用户（设备账号单一授权，如批量授权则查看目录 6.3）

绑定组:	<input type="checkbox"/> test3	<input type="checkbox"/> test5	<input type="checkbox"/> test8	<input type="checkbox"/> test_all	<input type="checkbox"/> 用户组
只显示已授权	<input type="checkbox"/> 默认管理员				
只显示未授权	<input type="checkbox"/>				
绑定用户	<input type="checkbox"/> admin(管理员)	<input type="checkbox"/> audit(audit)	<input type="checkbox"/> password(password)	<input type="checkbox"/> test1(测试用户)	<input type="checkbox"/> test_ceshi(testadmin)
只显示已授权	<input type="checkbox"/> test_ceshi1(test_ceshi1)				
只显示未授权	<input type="checkbox"/> test_hanyu(zhanghanyu)				
	<input type="checkbox"/> test_zhang(zhang)				
	<input type="checkbox"/> 批量选择				
	<input type="checkbox"/> 全选				

[确定](#)

## 6.3 批量设备授权

通过系统用户组可以快速地将多个设备的系统账号绑定给平台自然人运维账号。

目录：资产管理---授权权限---系统用户组

系统用户组是指将已经添加的资源的系统账号以列表的形式展现出来，方便分组绑定操作，不用再繁琐的选择资源再选择系统用户然后再进行绑定，简化绑定操作。

点击添加新组就可以添加一个新的系统用户组，界面如下：



点击“添加”进入新组创建页面，如下图所示，首先定义系统用户组名称，如：主机设备组，选中要添加的设备资源（未选设备），点击“添加”按钮，添加到右侧已选设备列表中：



添加完成后，为系统用户组绑定用户或者组时，页面下拉，勾选用户或组，如下图所示。



如选择了一个组，则组下的每个账户都有此系统组的权限。选择后，点击

保存即可。

使用系统用户组来进行绑定可以避免系统账号绑定给自然人账号时的误操作，提供了一个更加清晰高效的绑定界面。

## 7. 应用添加及授权

### 7.1 应用添加

1、选择资源管理-应用发布，点击右侧应用发布



2、点击添加，然后填写应用名称、用户名及密码（应用名称为必填项，用户名、密码为可选），然后选择程序列表（以发布 IE 浏览器为例），选择 IE，然后填写 URL 地址：

3、绑定组或绑定用户，上栏添加好应用信息后，下栏为绑定用户（设备账号单一授权，如批量授权则查看目录 7.2）

是否允许密码自动修改:

激活:

绑定分组  test3  test4  test5  test8  test\_all

只显示已授权   用户组  默认管理员

只显示未授权

绑定用户  admin(管理员)  audit(audit)  password(password)  test1(测试用户)  test\_ceshi(testadmin)

只显示已授权   test\_ceshi1(test\_ceshi1)  test\_hanyu(zhanghanyu)  test\_zhang(zhang)  test\_zhy(测试zhy)

只显示未授权

全选

## 7.2 批量应用授权

通过应用用户组可以快速地将多个应用资产绑定给平台自然人运维账号。

目录：资产管理——授权权限——应用用户组

应用用户组是指将已经添加的应用资源的信息以列表的形式展现出来，方便分组绑定操作，不用再繁琐的选择资源再选择系统用户然后再进行绑定，简化绑定操作。

点击添加新组就可以添加一个新的应用用户组，界面如下：

2018年01月23日 星期二

系统用户组 **应用用户组** 系统权限 应用权限

组名  用户  用户组

组名	描述	操作
test		<input checked="" type="checkbox"/> 编辑   <input checked="" type="checkbox"/> 删除
test_all		<input checked="" type="checkbox"/> 编辑   <input checked="" type="checkbox"/> 删除

页次：1/1页 20条/页 共2条 转到第  页

点击“添加新组”进入新组创建页面，如下图所示，首先定义应用用户组名称，如：安全设备组，选中要添加的应用资源，点击“添加”按钮，添加到右侧已选应用列表中：



添加完成后，为应用用户组绑定用户或者组时，页面下侧，勾选用户或组，如下图所示。



如选择了一个组，则组下的每个账户都有此应用用户组的权限。选择后，点击保存即可。

使用应用用户组来进行绑定可以避免应用绑定给自然人账号时的误操作，提供了一个更加清晰高效的绑定界面。

## 8. 审计信息查看

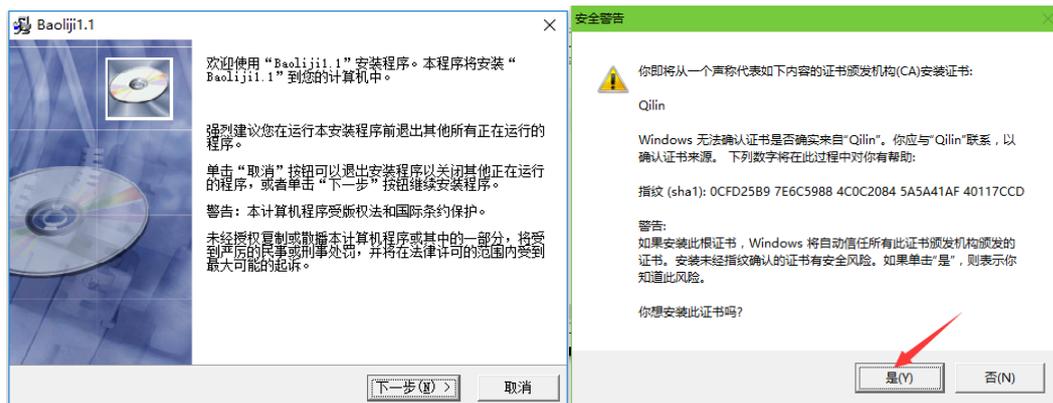
### 8.1 相关控件安装

当管理员需要查看运维人员登录的信息时，此时需要安装堡垒机控件。其它---工具下载，如下图

工具名	操作
2017-02-21-VPN程序.zip	<a href="#">下载</a>   <a href="#">删除</a>
MacOS-TOOLS-2017-727.zip	<a href="#">下载</a>   <a href="#">删除</a>
RDP回放程序.zip	<a href="#">下载</a>   <a href="#">删除</a>
mremote.zip	<a href="#">下载</a>   <a href="#">删除</a>
putty.zip	<a href="#">下载</a>   <a href="#">删除</a>
sshplay.zip	<a href="#">下载</a>   <a href="#">删除</a>
winscp.zip	<a href="#">下载</a>   <a href="#">删除</a>
<b>堡垒机插件2017.zip</b>	<a href="#">下载</a>   <a href="#">删除</a>
应用发布插件-2017-7-6.rar	<a href="#">下载</a>   <a href="#">删除</a>
苹果插件和vpn.rar	<a href="#">下载</a>   <a href="#">删除</a>

上传文件

首先安装堡垒机控件，下载后直接打开，选择进行安装即可（如本机有杀毒软件及安全卫士，建议关闭安装，以免控件被误杀）



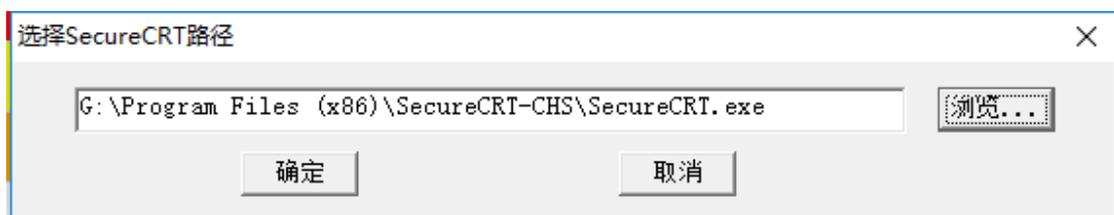
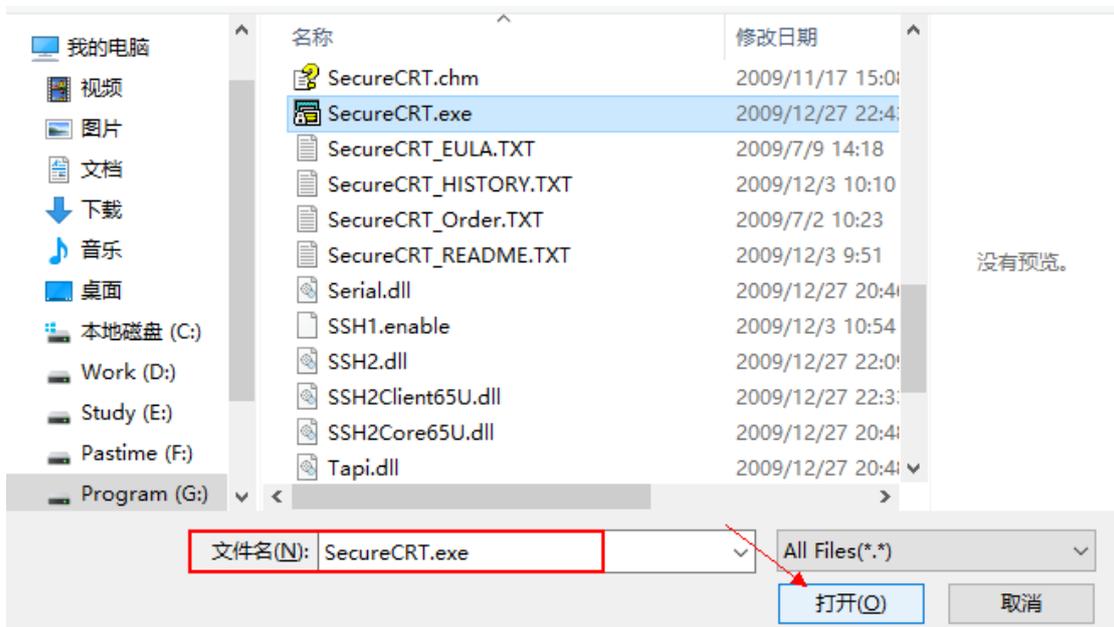
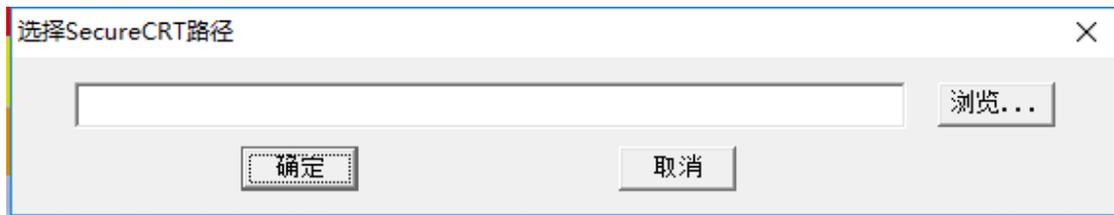
以上如有杀毒软件提示，点击是即可，建议关闭杀毒软件后安装，以免控件被误杀。

## 8.2 TEINET/SSH 录像审计

点击运维审计---操作审计---Telnet/SSH 目录，点击右侧回放 putty 或者 CRT 工具进行回放

来源地址	设备地址	类型	运维	真实姓名	本地	开始时间	结束时间	文件(O)	详细
123.66.205.116	127.0.0.1	ssh	admin	管理员	root	2017-12-19 18:07:23	2017-12-19 18:07:26	0.1	回放 (putty   CRT   Xshell) 文件 命令(1) 备注 下载
123.66.205.116	127.0.0.1	ssh	admin	管理员	root	2017-12-19 18:06:32	2017-12-19 18:06:44	0.5	回放 (putty   CRT   Xshell) 文件 命令(5) 备注 下载
123.66.205.116	127.0.0.1	ssh	admin	管理员	root	2017-12-19 18:05:14	2017-12-19 18:05:21	0.2	回放 (putty   CRT   Xshell) 文件 命令(2) 备注 下载
36.57.215.181	127.0.0.1	ssh	admin	管理员	root	2017-11-22 19:27:34	2017-11-22 19:27:34	0.0	回放 (putty   CRT   Xshell) 文件 命令(0) 备注 下载
111.132.14.194	127.0.0.1	ssh	admin	管理员	root	2017-11-22 13:18:40	2017-11-22 13:18:40	0.0	回放 (putty   CRT   Xshell) 文件 命令(0) 备注 下载
111.132.14.194	127.0.0.1	ssh	admin	管理员	root	2017-11-22 12:56:47	2017-11-22 12:56:47	0.0	回放 (putty   CRT   Xshell) 文件 命令(0) 备注 下载
111.127.49.35	47.94.229.159	ssh	admin	管理员	root	2017-11-10 07:11:35	2017-11-10 07:11:35	0.0	回放 (putty   CRT   Xshell) 文件 命令(0) 备注 下载
111.127.49.35	127.0.0.1	ssh	hanyu	root	root	2017-11-09 22:54:52	2017-11-09 22:55:09	1.3	回放 (putty   CRT   Xshell) 文件 命令(5) 备注 下载
111.127.49.35	127.0.0.1	ssh	hanyu	root	root	2017-11-09 22:53:12	2017-11-09 22:53:54	14.4	回放 (putty   CRT   Xshell) 文件 命令(9) 备注 下载
36.62.5218	127.0.0.1	ssh	admin	管理员	root	2017-10-09 21:22:35	2017-10-09 21:22:40	0.3	回放 (putty   CRT   Xshell) 文件 命令(4) 备注 下载

首次使用时，需要选择运维工具的目录，以 SecureCRT 为例，选择 SecureCRT（一定要选择到可执行文件），然后点击确定即可。



## 8.3 RDP 图形录像审计

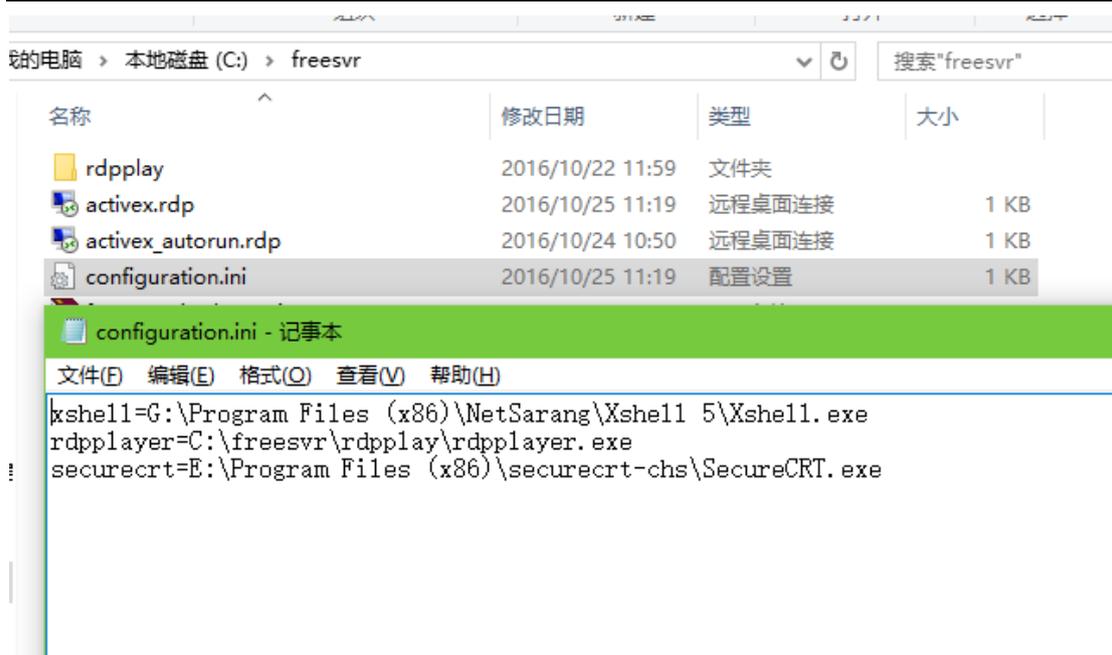
RDP 审计查看：点击运维审计---操作审计页面，选择指定录像条目，点击右侧回放

The screenshot displays the 'RDP' tab in the '运维审计' (Operation Audit) section. A table lists audit records with columns for source address, device address, user, local address, start time, end time, and file size. The '回放' (Playback) icon for the first record is circled in red. Below the table, a 'Player' window is open, showing a video player interface with a 'File' tab, a table with columns 'Time stamp', 'Type', and 'Event', and playback controls like '暂停', '慢进', and '快进'.

来源地址	设备地址	运维	真实姓名	本地	开始时间	结束时间	文件(K)	详细
111.132.14.194	120.92.17.131	admin	管理员	longer	2017-11-22 12:55:03	2017-11-22 12:55:12	28.109	回放 录屏 鼠标 剪贴板 备注 录像下载
111.132.14.194	120.92.17.131	admin	管理员	longer	2017-11-22 12:53:54	2017-11-22 12:54:09	20.26	回放 录屏 鼠标 剪贴板 备注 录像下载
60.253.213.190	120.92.17.131	admin	管理员	longer	2017-11-18 17:34:41	2017-11-18 17:34:46	78.845	回放 录屏 鼠标 剪贴板 备注 录像下载
121.56.10.231	120.92.17.131	test_ceshi	testadmin	longer	2017-11-14 17:25:20	2017-11-14 17:27:17	236.85	回放 录屏 鼠标 剪贴板 备注 录像下载
111.127.49.35	120.92.17.131	hanyu		longer	2017-11-09 22:54:36	2017-11-09 22:54:47	228.381	回放 录屏 鼠标 剪贴板 备注 录像下载
111.127.49.35	182.48.119.120	hanyu	administrator		2017-11-09 22:54:00	2017-11-09 22:54:32	26.109	回放 录屏 鼠标 剪贴板 备注 录像下载
111.127.49.35	120.92.17.131	hanyu		longer	2017-11-09 22:53:06	2017-11-09 22:54:37	58.244	回放 录屏 鼠标 剪贴板 备注 录像下载
111.127.49.35	182.48.119.120	admin	管理员	administrator	2017-11-09 22:48:39	2017-11-09 22:49:12	71.337	回放 录屏 鼠标 剪贴板 备注 录像下载
111.127.49.35	120.92.17.131	admin	管理员	longer	2017-11-09 22:12:20	2017-11-09 22:12:30	121.08	回放 录屏 鼠标 剪贴板 备注 录像下载
36.62.5.218	120.92.17.131	admin	管理员	longer	2017-10-09 21:20:45	2017-10-09 21:20:55	82.515	回放 录屏 鼠标 剪贴板 备注 录像下载

## 9. 注意事项

如遇到选择路径出错时，会出现点击无响应的情况发生，此时可以到 C:\freesvr 目录下配置文 configuration.ini 进行修改，如下：



此目录是存放运维工具目录的配置文件，如某一工具目录输入错误，可以在这里直接修改正确的可执行文件的目录，或者删除目录指定有问题的一行，保存后，从前台再次登录选择即可。

## 10. 应急办法

如出现意外或需要不通过堡垒机直接进行目标设备访问，首先需要在网络中做放行策略，将原先运维组 IP 地址组对目标设备的访问控制策略（ACL）运维端口做放行配置，然后通过运维审计系统密码管理员进行查看当前目标服务器密码，让运维人员直接访问目的资产信息即可。