天翼云·网页防篡改

用户使用指南

天翼云科技有限公司

目录

1. 产品简介

1.1 产品定义

网页防篡改（CT-WT WebpageTampering）是针对网站篡改攻击的一款防护产品，通过文件底层驱动技术对 Web 站点目录提供全方位的保护，为防止黑客、病毒等对目录中的网页、电子文档、图片、数据库等任何类型的文件进行非法篡改和破坏提供解决方案。

1.2 产品优势

B/S 架构

基于 B/S 架构的远程管理，管理员无需安装客户端仅通过浏览器即可登陆管理系统进行管理，无需关心操作系统类型，更加方便快捷；

三权分立

支持多用户，多角色管理，依照管理员、审计员、配置管理员等进行用户权限管理，不同用户权限明确，满足管理需要；

驱动级技术

采用操作系统驱动层文件防护技术 应用防护逻辑采用嵌入式脚本开发，更加灵活方便帮助用户扩展应用层防护功能； 支持管理端集群式部署并且支持分布式文件系统存储，相比传统的双机热备部署方式提高了系统的可靠性；

安全性高

对备份文件进行加密存储和访问权限控制，避免未授权用户登录系统对文件进行修改，产品各个模块间采用 SSL 通讯，保障产品自身通讯安全性；产品的自身防护功能，可防止自身进程被停止，程序文件被删除；

支持 IPv6 类型的 IP 地址

服务端可以通过 ipv6 的地址访问。客户端识别并支持 Ipv6 类型的 IP 地址添加。

1.3 功能特性

- **文件篡改防护**

  同时对多台网站服务器文件进行防止篡改，包括文件被修改，被添加，被删除；

  同时对同一台服务器内的多个 web server 进行防篡改；

  同时对同一 web server 内的多个 virtual host 进行防篡改；

  保护防篡改内嵌模块和守护进程自己；

- **网站文件发布与备份**

  支持内容发布；

  支持实时同步；

支持手动同步；
实体间通信采用 SSL 加密；

- **日志与告警**

  系统日志：
  记录用户登录，退出；添加，删除 Web server；添加，修改，删除用户；
  查询，导出成 excel,自动清除和全部清除；
  文件传输日志：
  记录文件同步，文件删除，文件恢复；
  日志查询，导出成 excel；
  篡改告警：
  记录文件删除，修改，添加，恢复等篡改和保护行为；
  告警查询，导出成 excel，自动清除，全部清除功能；
  告警的通知包括、邮件通知、管理界面警示框；
  图形报表的综合统计和分析；
  告警查询，导出成 excel，自动清除，全部清除功能；
  告警的通知包括邮件通知、管理界面警示框；
  图形报表的综合统计和分析；

- **系统管理和防护功能**

  用户管理功能：
  添加，删除，修改用户功能；
  提供权限控制功能；管理员可以修改所有用户；普通用户可以修改自己；
  锁定、解锁用户功能，可以手动锁定用户一定时间；密码错误次数满后自动锁定用户；
  创建密码复杂度验证功能；
  设定用户登录 IP 列表；
  提供邮件形式密码找回功能；
  授权管理功能：
  基于 License 文件的授权；
  历史授权记录：第二授权时，显示历史授权记录；
  授权提醒和邮件通知：包括过期，无授权，授权快过期
  服务器管理功能：
  添加删除和修改 Web 服务器的管理功能；
  监控管理服务器的 CPU,内存，硬盘等使用情况，获取管理服务器的基本信
  系统配置功能：
  密码复杂度配置；
  通知邮件配置；
  授权过期提醒配置；
  自动清除告警和日志配置
  重试登录配置；

授权导入和当前授权信息显示。

1.4 应用场景

- **电子政务网站和企业门户网站**
  在我国举办重大活动期间，各行各业的网站遭受不法份子的破坏以及国外黑客攻击的几率大大增加。
- **金融银行、证券机构**
  各类金融银行、证券机构积极开展网上金融业务，如遭受篡改，不仅仅是形象受损信誉度降低，还会带来巨大的经济损失。
- **中小型企业**
  中小型企业往往防护薄弱，常常被黑客挂马篡改，对访问者造成困扰，也影响企业声誉。

2. 计费模式

2.1 购买

用户可以自行选择组合订购和证书订购。

- 组合订购指同步订购授权和云主机；
- 证书订购指订购授权、不订购云主机。

2.1.1 组合订购

1) 订购方式：选择组合订购
2) 防护数量：选择被防护的 web 服务器数量
3) 数据盘：选择被防护的 web 服务器中 web 目录大小总和。
4) 部署主机：选择可用区、vpc、子网，默认选择网页防篡改的镜像（
防篡改镜像分为 windows 和 linux：

如果用户只有 windows 就买 win 主机， 只有 Linux 就买 Linux 主机，两者都有买 linux 主机)

支持系统情况列表，服务端同时支持 Windows、Linux，请按客户实际情况进行部署

组件	支持的操作系统
Windows 服务端	支持 2008R2sp1/2012sp1/2016
Windows 客户端	支持 2003(x86/x64)/2008(x86/x64)/2012/2016
Linux 服务端	支持 CentOS/RHEL/中标麒麟 7.x
Linux 客户端	支持 CentOS/RHEL(6.x/7.x)/Ubuntu/Suse/Debian

主机规格根据防护的 web 服务器数量来定，系统盘 50G、数据盘客户自行确认。

Web 服务器数量	配置
1-5 个	CPU·两核·4G 内存·数据盘大小要求是网站目录大小而定
6-10 个	CPU·四核·4G 内存·数据盘大小要求是网站目录大小而定
11-20 个	CPU·四核·8G 内存·数据盘大小要求是网站目录大小而定

备注：Web 服务器数量最大 50，20-50 所需云主机配置为 CPU4 核，8G 内存，输盘视网站目录大小而定。

5) 安全组：选择安全组，网页放篡改保所选安全组已放通 20813 端口（Linux SSH 登录），20813 端口（Windows 远程登录）和 ICMP 协议（Ping），1443（用于登录访问）、 UDP/8020（用于授权）；

6) 购买时长 1 个月到 3 年

7) 订购确认页面同“云堡垒机”

2.1.2 证书订购

1) 订购方式：

■ 选择证书订购；证书订购需要传客户已订购的弹性云主机的 uuid

2) 防护数量：选择被防护的 web 服务器数量

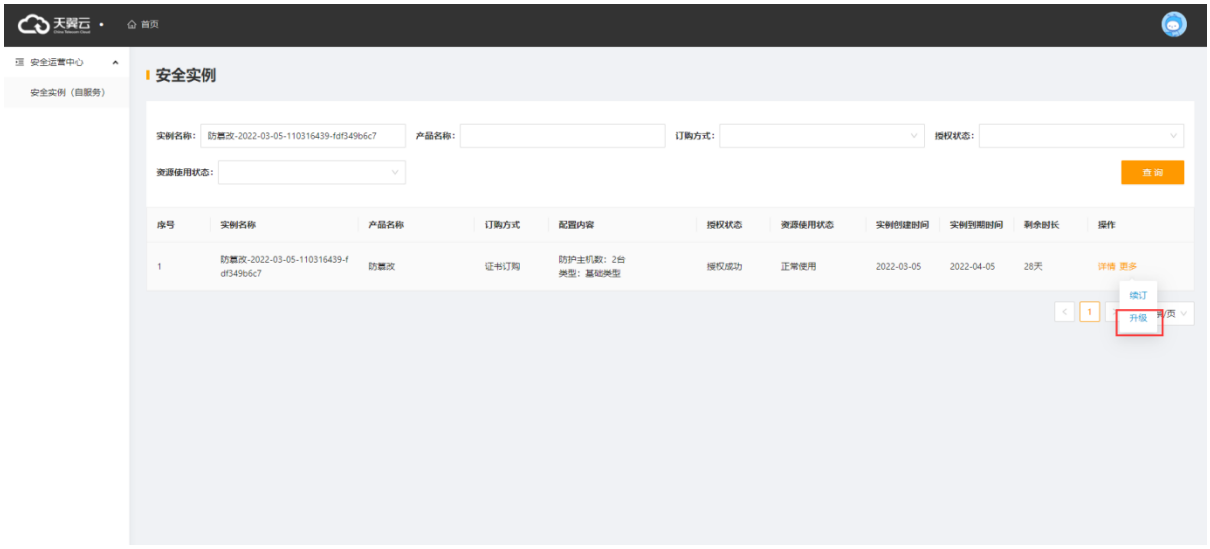
3) 填写防篡改镜像云主机的服务器的主机标识 UUID

4) 选择订购时长

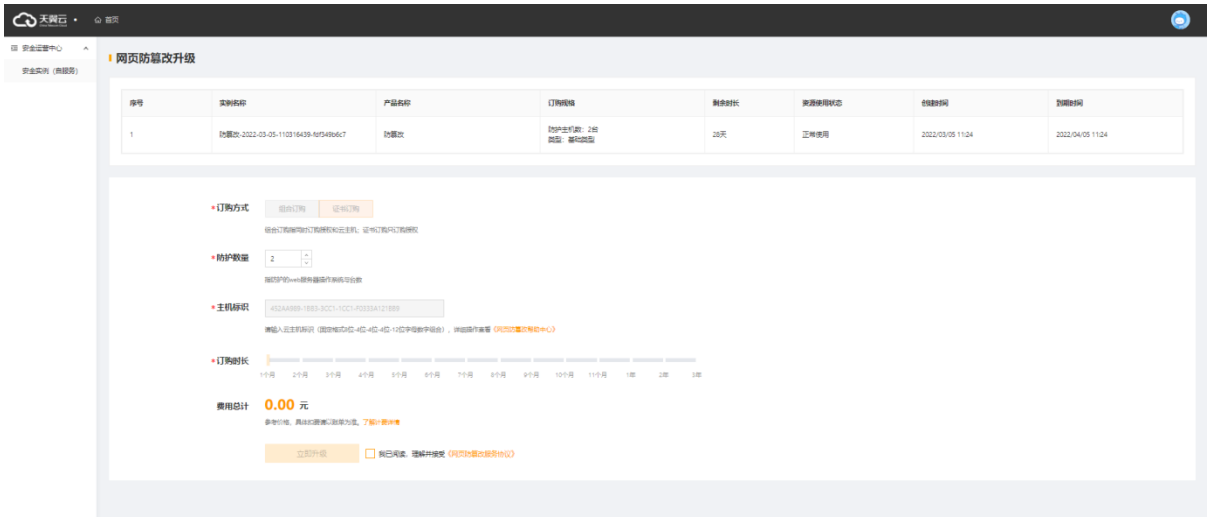
5) 提交订购

2.2 升级

用户可以通过升级操作使用更高级版本。

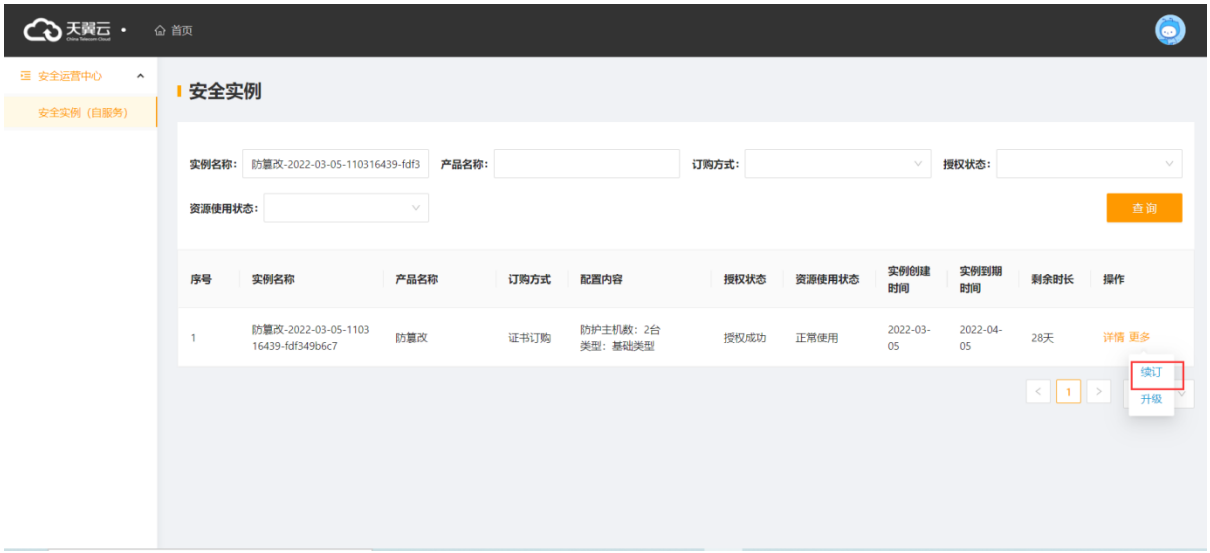


点击【升级】弹出升级弹窗。显示当前防篡改订购实例名称，选择升级的防护数量，费用总计，网页防篡改服务协议。



2.3 续订

用户可以通过续订延长产品使用时限，续订操作在控制中心列表页面进行操作。



点击【续订】弹出续订弹窗。显示当前防篡改订购实例名称，选择续订的时间，当前服务截止的日期，费用总计，网页防篡改服务协议。

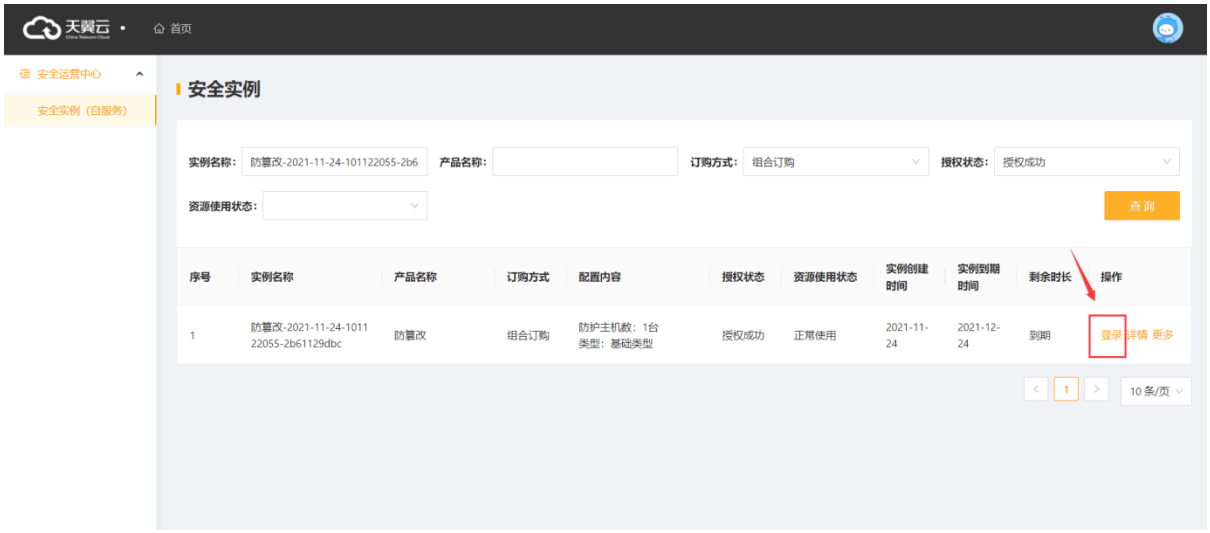
2.4 退订

本产品一经订购立即生效，除不可抗力因素之外，不支持退订。

3. 快速入门

3.1 单点登录

点击登陆安全产品，直接单点登录产品的管理平台。

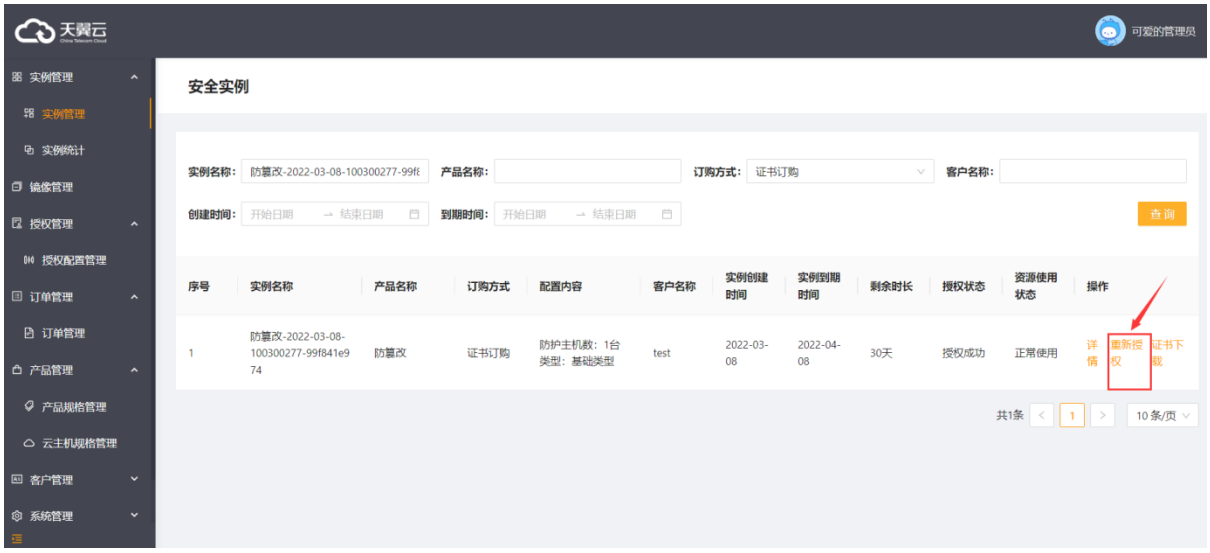


3.2 重新授权

重新授权需依据订购类型：

(1) 组合订购的实例，点击“重新授权”即授权到云主机。

(2) 证书订购的实例，点击“重新授权”弹出页面如下，填写 uuid，会重新生成 licence 文件，覆盖原有 licence 文件。



3.3 安装集中管理中心

网页防篡改控制端可以通过镜像安装，镜像通过 400 电话或者天翼云工单系统提出申请，由客服共享到天翼云账号对应节点。用户需要接收镜像，然后起一台云主机来承载业务，然后再进行授权的订购。

安装集中管理中心所需云主机的系统类型为 windows 2008 规格要求对照下表：

Web 服务器数量	配置

1-5 个	CPU·两核·4G 内存·数据盘大小要求是网站目录大小而定
6-10 个	CPU·四核·4G 内存·数据盘大小要求是网站目录大小而定
11-20 个	CPU·四核·8G 内存·数据盘大小要求是网站目录大小而定

网页防篡改控制端与各 web 端服务器网络可达即可，为了授权方便和产品初始化的配置，须分配一个弹性 IP 地址。完成安装后即可用浏览器访问控制端管理页面进行登录。

3.4 登录

默认访问方式为：https://服务器 ip:1443，即可访问管理服务端（默认账号密码请咨询厂商）。
备注：请务必修改默认密码，使用默认密码存在安全风险。

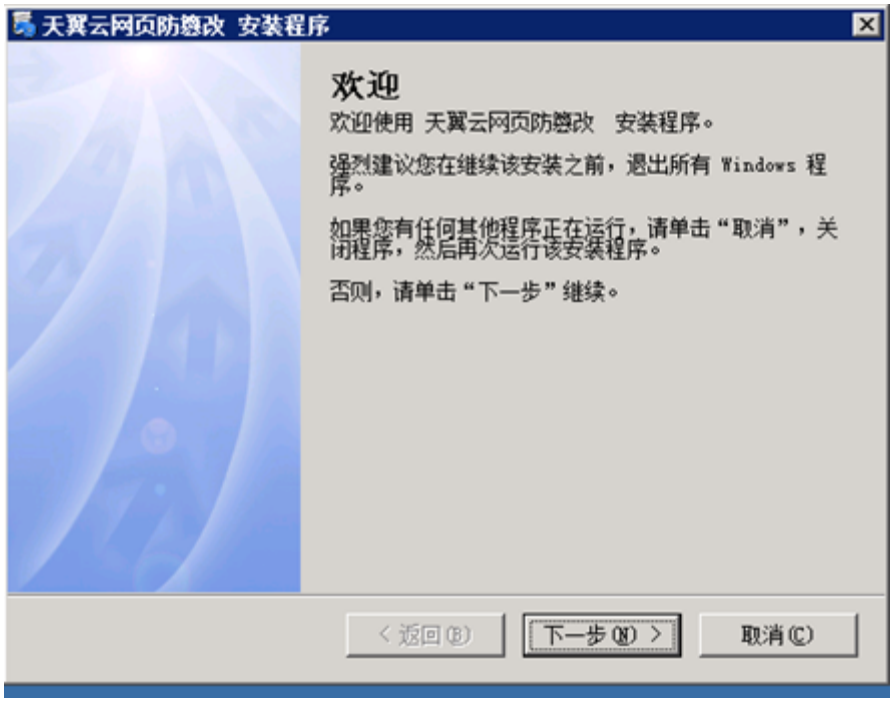
3.5 端口开放情况

服务端需要开放 tcp1443 端口：用于 web 管理登录□对管理人员开放
Udp 8020 端口：用于告警通知□对客户端 ip 放行
客户端需开放 tcp 8011 端口□对服务端开放

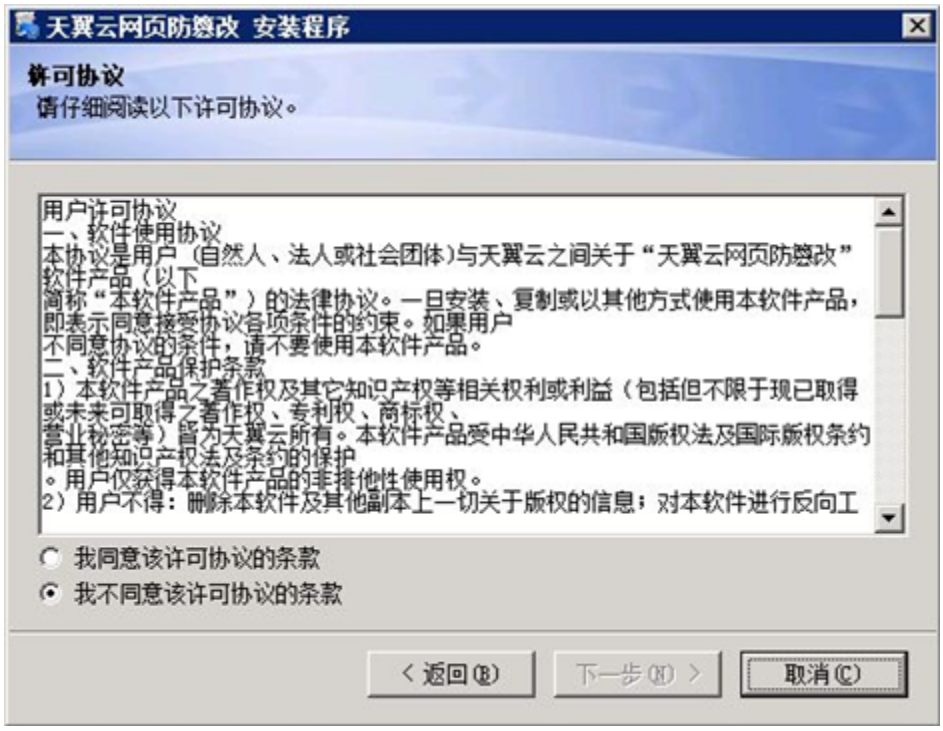
4. 用户指南

4. 1 安装集中管理中心

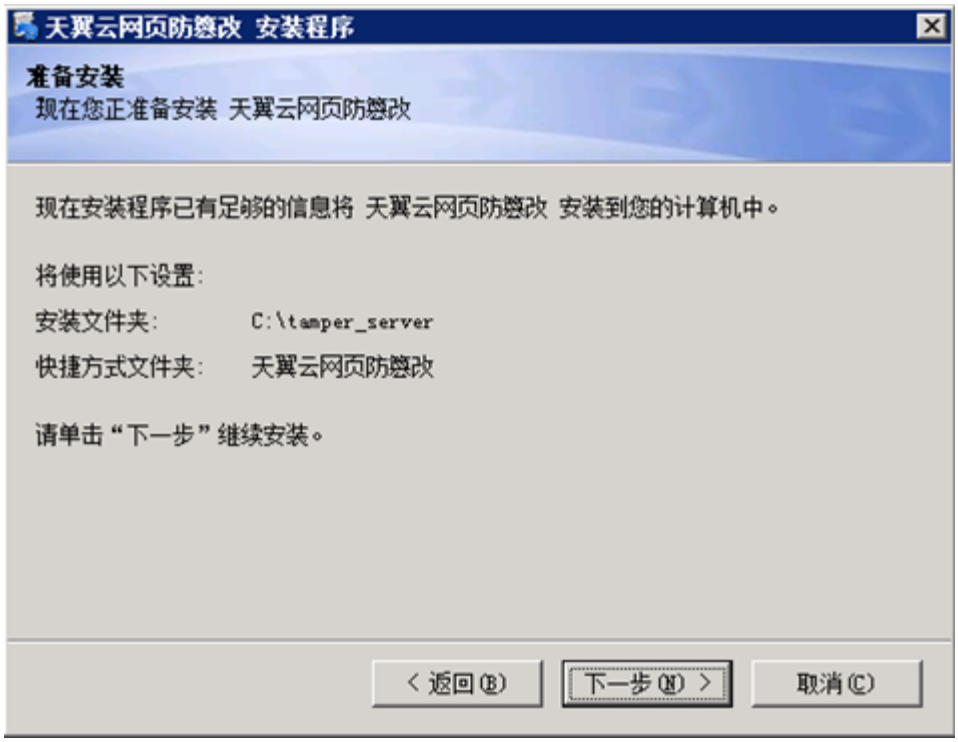
以镜像方式安装集中管理中心可忽略以下步骤，自行获取软件安装步骤如下：
1. 安装包
打开安装文件，进入 Windows 目录，server_install.exe 程序：
2. 执行安装
a)双击“server_install4.3.8-天翼云”进入安装步骤，如下图所示



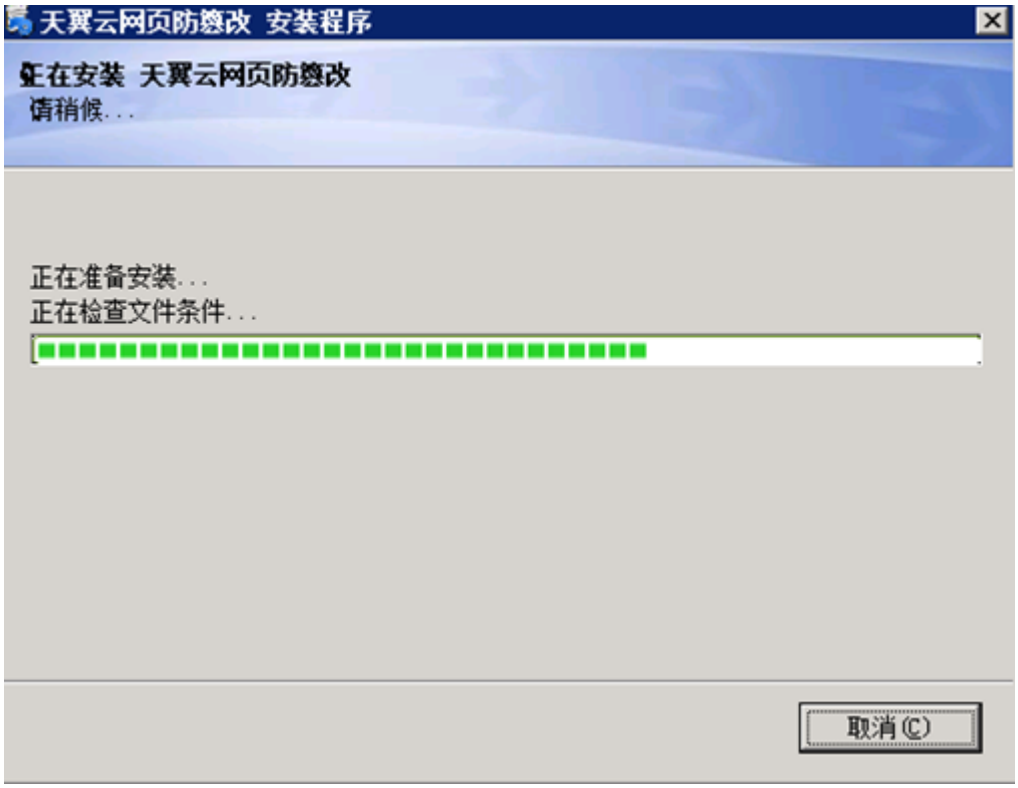
b)点击下一步，点击同意许可协议方可进行下一步操作，如下图所示



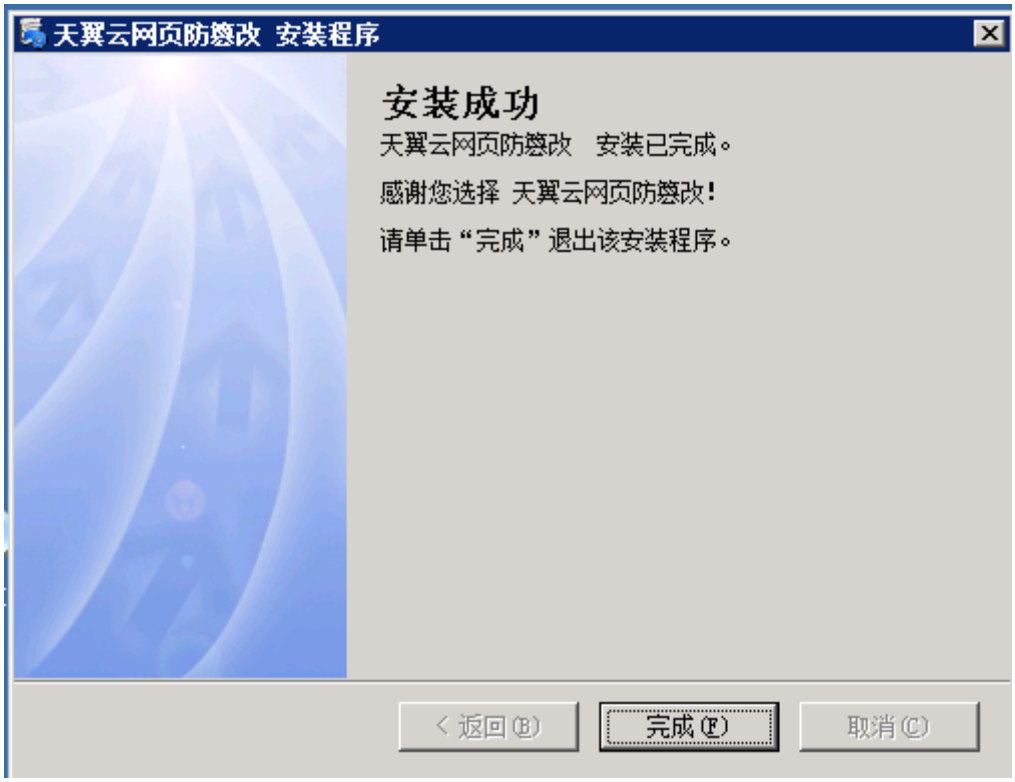
c）服务端默认且必须安装在 C:\tamper_server，



d)点击下一步即进入安装过程，如下图所示，



e)等待至安装完成，如下图所示



f)检查服务启动情况：

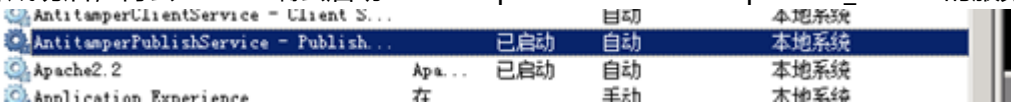
安装完成后，检查系统服务是否已启动：AntitamperApache2.4 、AntitamperMongoDB（数据库服务），及 AntitamperPublishService。

默认发布目录为 C:\ftp

g)安装完成后，登录首页查看软硬件信息机器码提交给授权制作人员。

a) 浏览器访问 UI：https://[server 端服务器 IP]

a) 用超级管理员账户登录系统后（默认账号密码请咨询厂商），进入授权管理页面，导入授权文件成功后，再去 server 端去启动 AutitamperPublishService-publish_server 的服务。

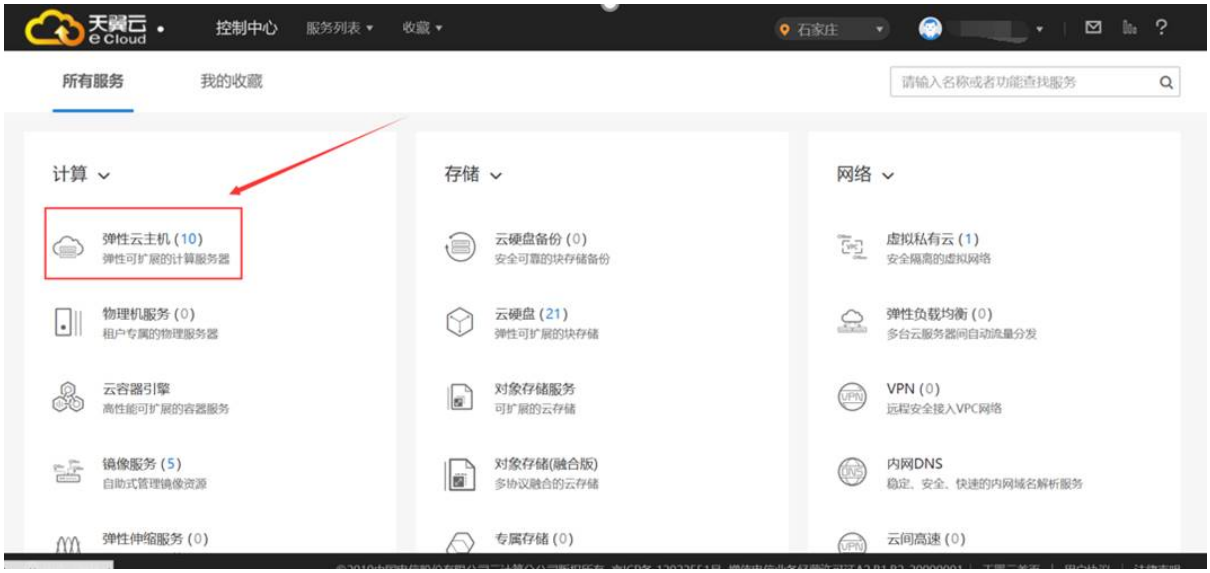


4. 2 Server 端安装

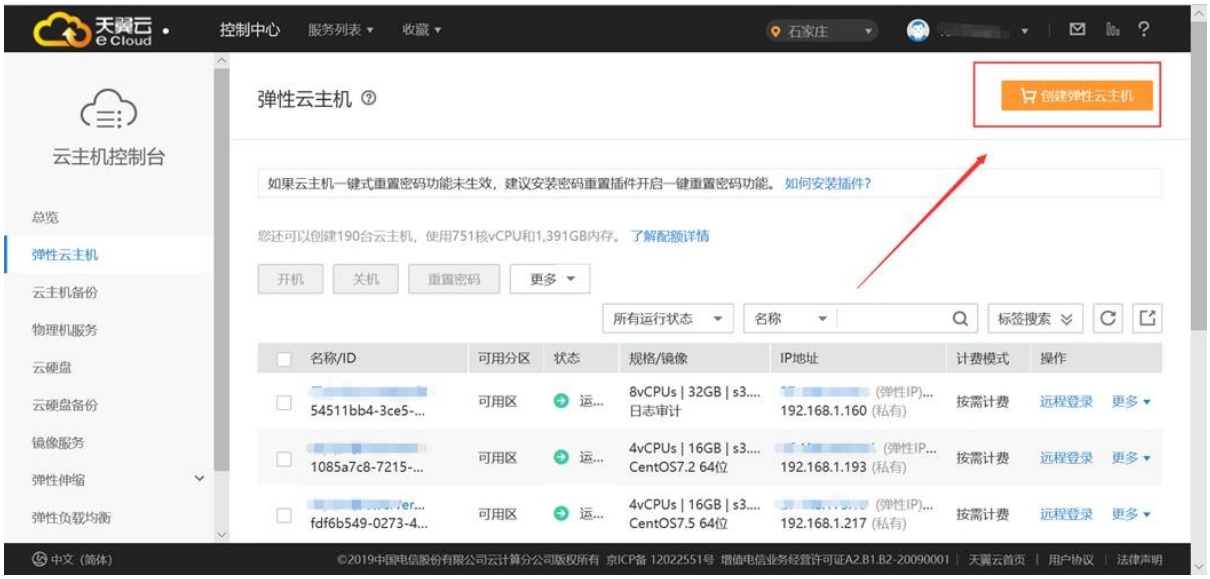
通过天翼云网页防篡改公共镜像新开一台云主机承载网页防篡改业务，操作步骤如下，

1、登陆天翼云官网（https://www.ctyun.cn/home/）-账号-控制中心

2、选择弹性云主机

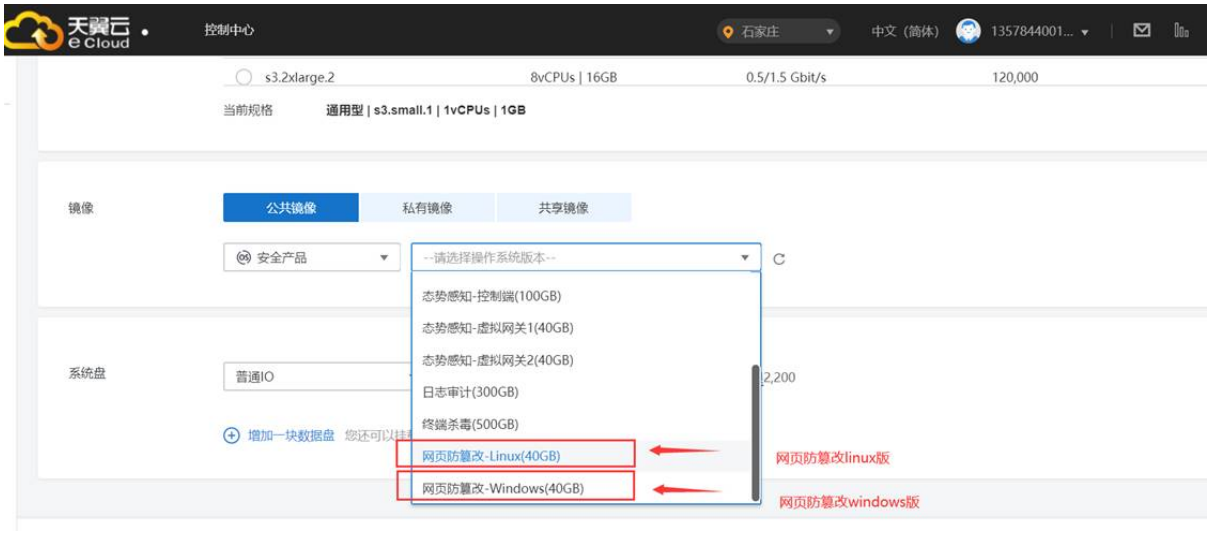


3、创建弹性云主机

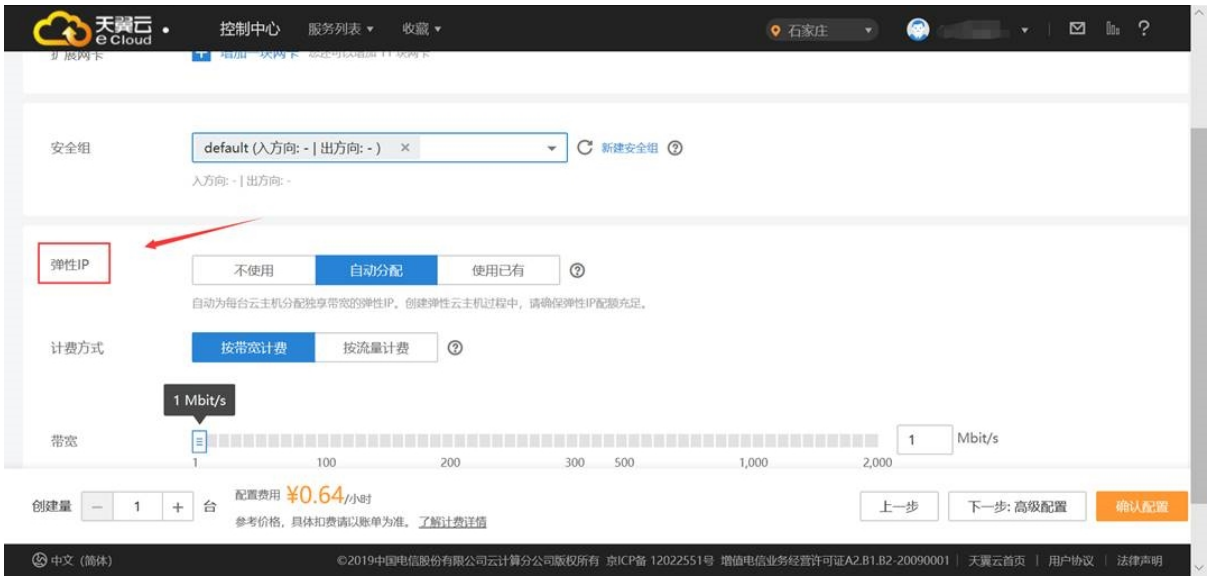


4、选择镜像

在公有镜像中选择安全产品-网页防篡改-Linux（40GB）或者 网页防篡改-Windows（40GB），建议根据防护主机类型选择对应系统版本，其它项根据产品要求和客户要求选择。

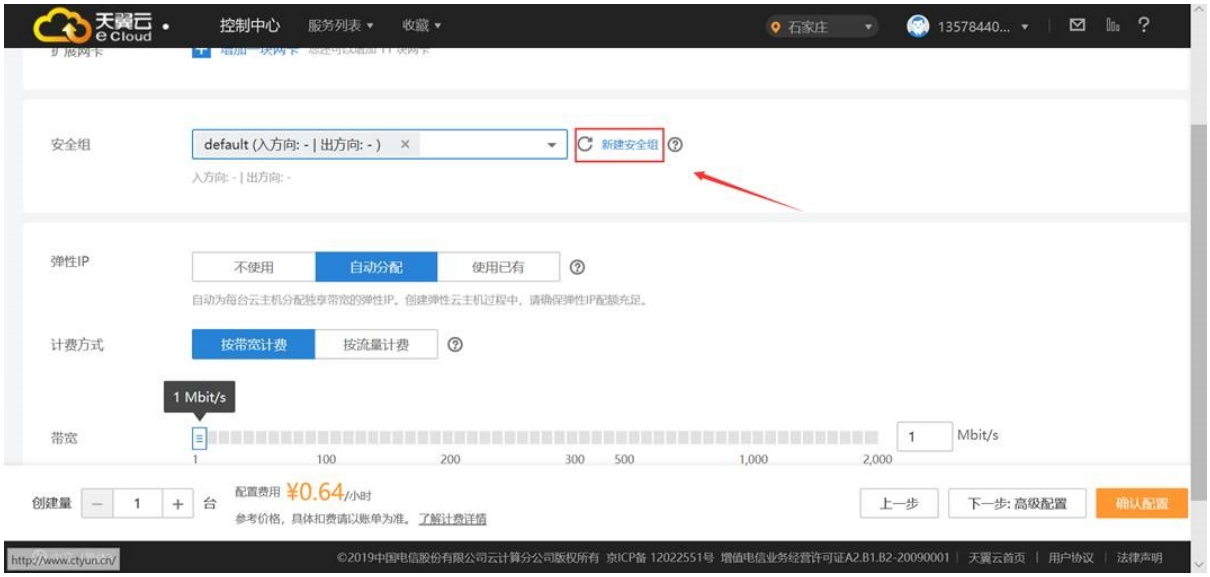


选择开通所需弹性 IP，可以选择自动分配。弹性 IP 用于公网访问管理界面，5M 带宽即可。



5、安全组设置

安全组中，需要加入入方向开通 1443 的规则。



6、命名云主机和填写密码。

7、 提交开通申请，开通完成。

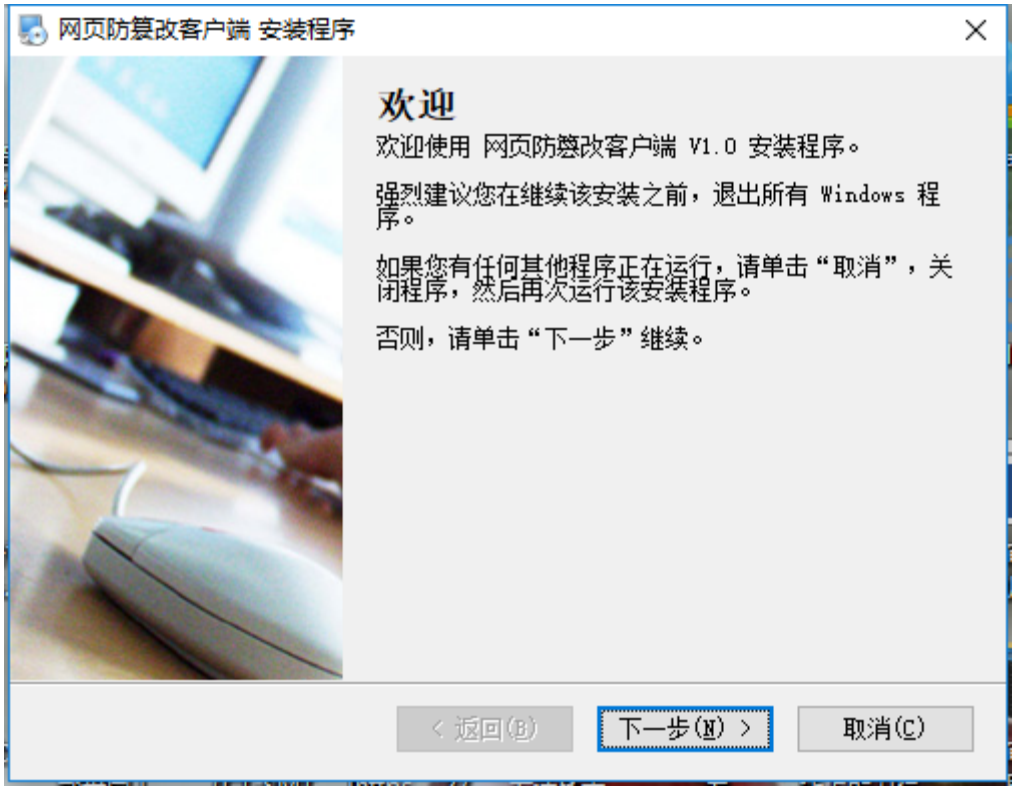
4.3 客户端安装

4.3.1 Windows 版本

1. 安装包，在 windows 目录下的 client_install4.3.8-天翼云

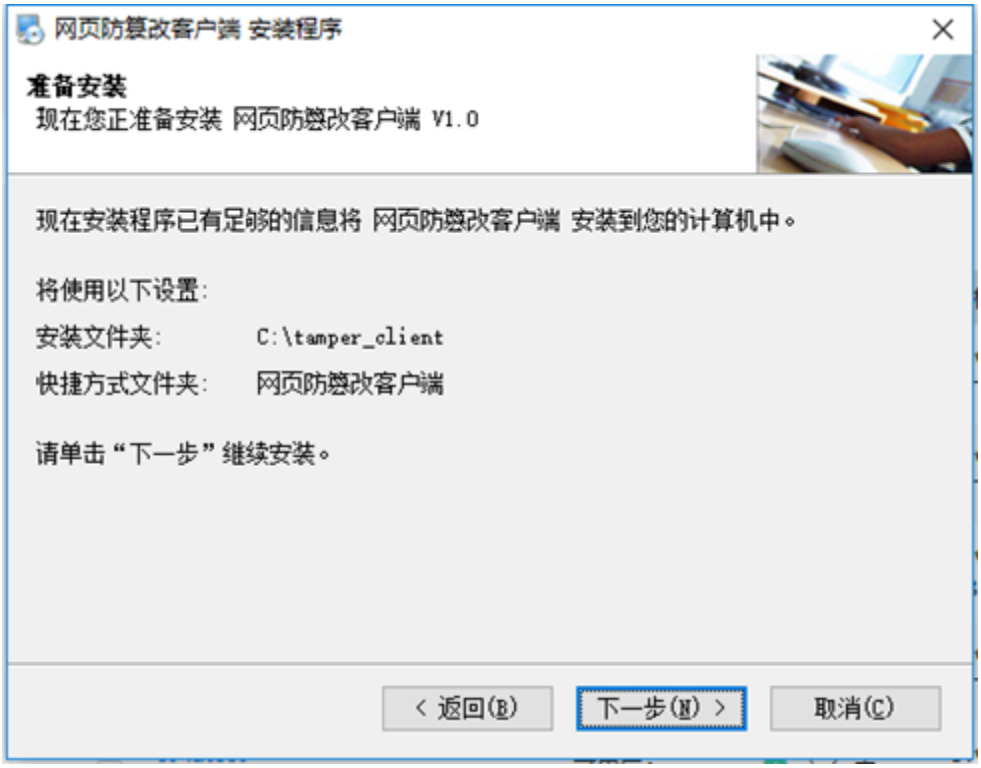
2. 执行安装

a) 双击.exe 文件进入安装步骤，如下图所示



b) 点击下一步，输入 server 端 IP 地址。

c）服务端默认安装在 C:\tamper_server，

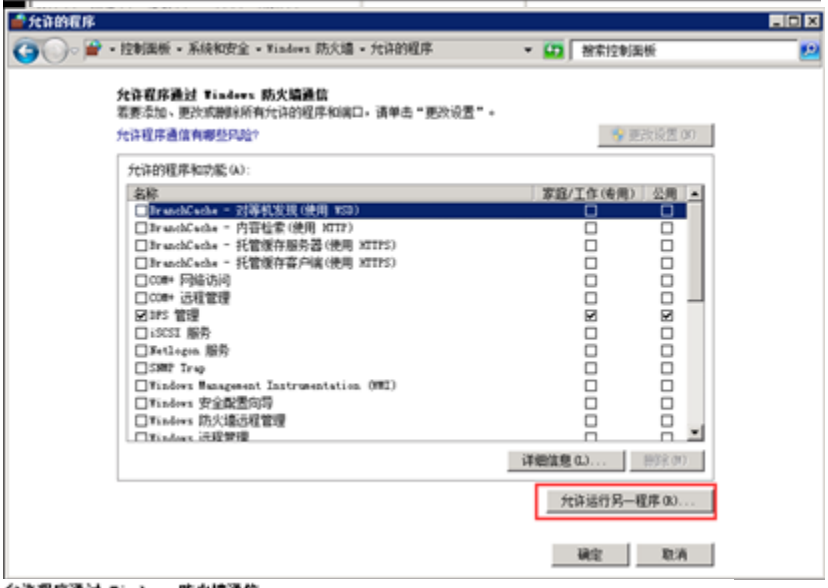


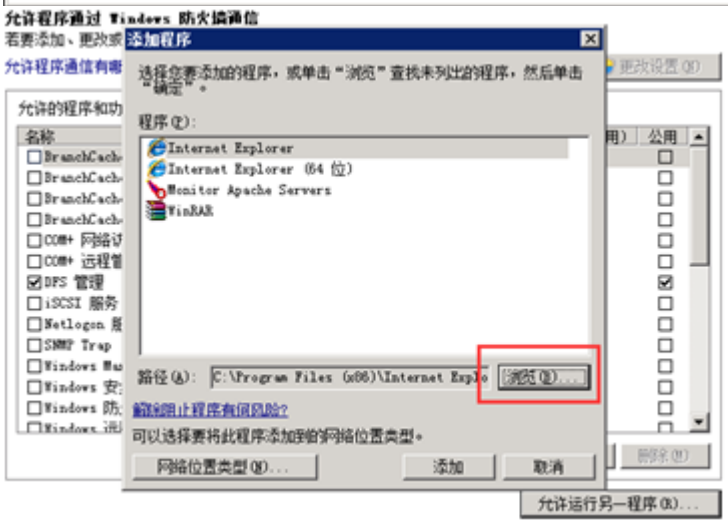
d）点击下一步即开始安装，安装完成界面如下，

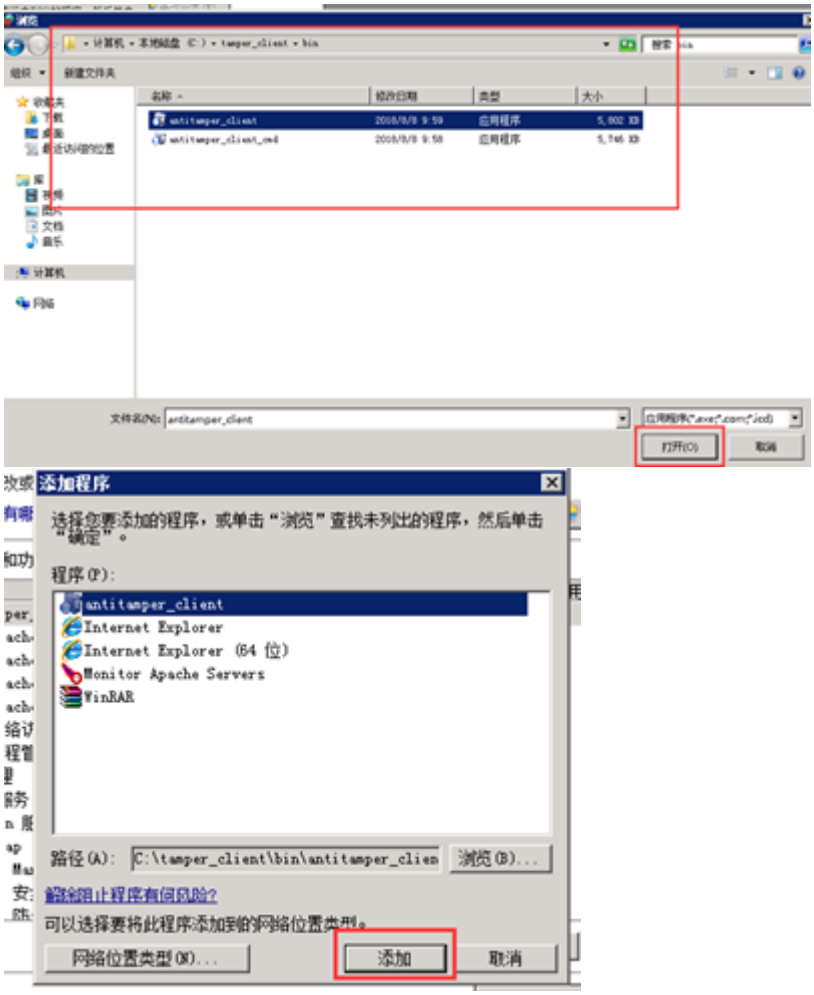
客户端安装完成后，需要重启服务器，重启完成之后，确认 client 端服务 AntitamperClientService 已经启动：

特别注意：在防火墙启动的情况下，需在防火墙配置中进行如下配置：


Windows 防火墙
控制面板 ▸ 系统和安全 ▸ Windows 防火墙
搜索控制面板
控制面板主页
允许程序或功能通过 Windows 防火墙
更改通知设置
打开或关闭 Windows 防火墙
还原默认设置
高级设置
对网络进行疑难解答
使用 Windows 防火墙来帮助保护您的计算机
Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问您的计算机。
防火墙如何帮助保护计算机?
什么是网络位置?
更新防火墙设置
Windows 防火墙未使用推荐的设置来保护计算机。
使用推荐设置
推荐的设置有哪些?
家庭或工作(专用)网络(O)
未连接
公用网络(P)
已连接
公共场所(例如机场或咖啡店)中的网络
Windows 防火墙状态:
关闭
传入连接:
阻止所有与未在允许程序列表中的程序的连接
活动的公用网络:
网络 2
通知状态:
Windows 防火墙阻止新程序时不要通知我
另请参阅
操作中心
网络和共享中心


允许的程序
控制面板 ▸ 系统和安全 ▸ Windows 防火墙 ▸ 允许的程序
搜索控制面板
允许程序通过 Windows 防火墙通信
若要添加、更改或删除所有允许的程序和端口,请单击"更改设置"。
允许程序通信有哪些风险?
更改设置(N)
允许的程序和功能(A):
名称
家庭/工作(专用)
公用
BranchCache - 对等机发现(使用 WSD)
BranchCache - 内容检索(使用 HTTP)
BranchCache - 托管缓存服务器(使用 HTTPS)
BranchCache - 托管缓存客户端(使用 HTTPS)
COM+ 网络访问
COM+ 远程管理
DFS 管理
iSCSI 服务
Netlogon 服务
SNMP Trap
Windows Management Instrumentation (WMI)
Windows 安全配置向导
Windows 防火墙远程管理
详细信息(L)...
删除(M)
允许运行另一程序(R)...
确定
取消


允许程序通过 Windows 防火墙通信
若要添加、更改或
允许程序通信有哪
更改设置(N)
允许的程序和功
名称
公用
DFS 管理
添加程序
选择您要添加的程序,或单击"浏览"查找未列出的程序,然后单击"确定"。
程序(P):
Internet Explorer
Internet Explorer (64 位)
Monitor Apache Servers
WinRAR
路径(A):
C:\Program Files (x86)\Internet Explo
浏览(R)...
解除阻止程序有何风险?
可以选择要将此程序添加到哪种网络位置类型。
网络位置类型(T)...
添加
取消
删除(D)
允许运行另一程序(R)...



4. 3. 2 Linux 版本

Centos/RHEL 系列

1.通过上传工具将 antitamper_client_v4.3.2_centos_redhat_20180810.tar.gz 上传至 Linux 服务器，

执行解压命令 tar -zxvf antitamper_client_v4.3.2_centos_redhat_20180810.tar.gz 将安装包解压。

2.执行安装，

a)需要用 root 权限进行安装，进入解压后的目录，

cd antitamper_client_v4.3.2_centos_redhat_20180810，目录结构如下：

```
[root@localhost ~]# cd antitamper_server_v4.3.4_Linux_20180810/
[root@localhost antitamper_server_v4.3.4_Linux_20180810]# ls
admin  bin  etc  init.d  install.sh  lib  third_party
[root@localhost antitamper_server_v4.3.4_Linux_20180810]# ll
total 12
drwxr-xr-x 4 root root   28 Aug 10 16:25 admin
drwxr-xr-x 2 root root   76 Aug 10 09:07 bin
drwxr-xr-x 2 root root   32 Aug 10 09:07 etc
drwxr-xr-x 2 root root   68 Aug 10 09:07 init.d
-rwxr-xr-x 1 root root 7009 Aug 10 09:07 install.sh
drwxr-xr-x 2 root root   27 Aug 10 09:07 lib
drwxr-xr-x 6 root root 4096 Aug 10 09:07 third_party
[root@localhost antitamper_server_v4.3.4_Linux_20180810]#
```

b)执行 install 脚本进行安装./install,进入安装过程，如下图所示，输入服务端的 IP 地址，然后输入通信的网卡名称（安装程序会显示最后一个网卡名称，如有多个网卡，请确定通信的网卡，按 N 重新填写）。

```
bin  etc  init.d  install.sh  km  uninstall.sh
[root@localhost antitamper_client_v4.3.2_centos_redhat_20180808]# ./install.sh
start install client
Input IP:192.168.198.143

InFace List:
lo
eno16777736

net inface name is eno16777736?[y|n]y
dstport=8020 dstip=3232286351 ifname=eno16777736 ignore_files=*.log,*.temp protect_root=/var/www/html,/var/www/ftp
end install client
[root@localhost antitamper_client_v4.3.2_centos_redhat_20180808]# ./install.sh
```

c)安装完成后，服务自动启动，查看服务进程：ps aux |grep antitamper_client

```
[root@localhost antitamper_client_v4.3.2_centos_redhat_20180808]# ps aux |grep antitamper_client
root      7549  0.3  0.5 409572 22608 ?        Sl   04:36   0:01 /opt/tamper_client/bin/antitamper_client start
root      7813  0.0  0.0 112644   960 pts/0    R+   04:42   0:00 grep --color=auto antitamper_client
[root@localhost antitamper_client_v4.3.2_centos_redhat_20180808]#
```

Client 端启停命令：

停止　/opt/tamper_client/bin/antitamper_client stop

启动　/opt/tamper_client/bin/antitamper_client start

Debian/Ubuntu/Suse 系列

Debian 系统和 ubuntu 系统的客户端安装包为同一个包，Suse 系统客户端单独一个安装包。

注意：ubuntu 系统不能使用 sudo 安装，须切换到 root 权限下安装。

1.通过上传工具将 antitamper_client_v4.x_debian_ubuntu_20180808.tar.gz 上传至 debian 或 Ubuntu 服务器，将 antitamper_client_v4.x_suse_20180807.tar.gz 上传至 Suse 服务器。

执行解压命令将 antitamper_client_v4.x_debian_ubuntu_20180808.tar.gz 或 antitamper_client_v4.x_suse_20180807.tar.gz 安装包解压。

2.具体配置和安装步骤与上一章节“Centos/RHEL 系列”安装步骤相同。

4.4　登录

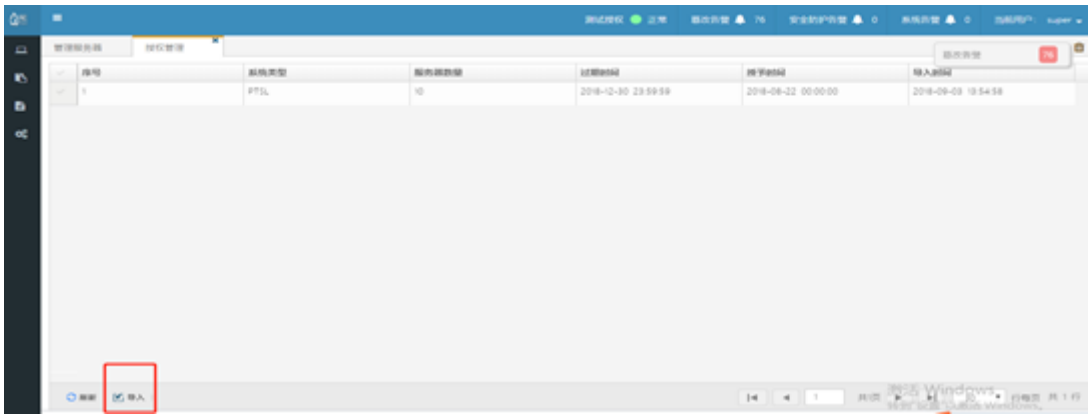
4.4.1　访问

1．天翼云网页防篡改系统采用基于 https 协议的 web 管理平台，支持 Chrome、Firefox 多种版本浏览器。

2．访问 url 为：https://服务端 IP:1443，浏览器访问 url 直接进入登录页面。

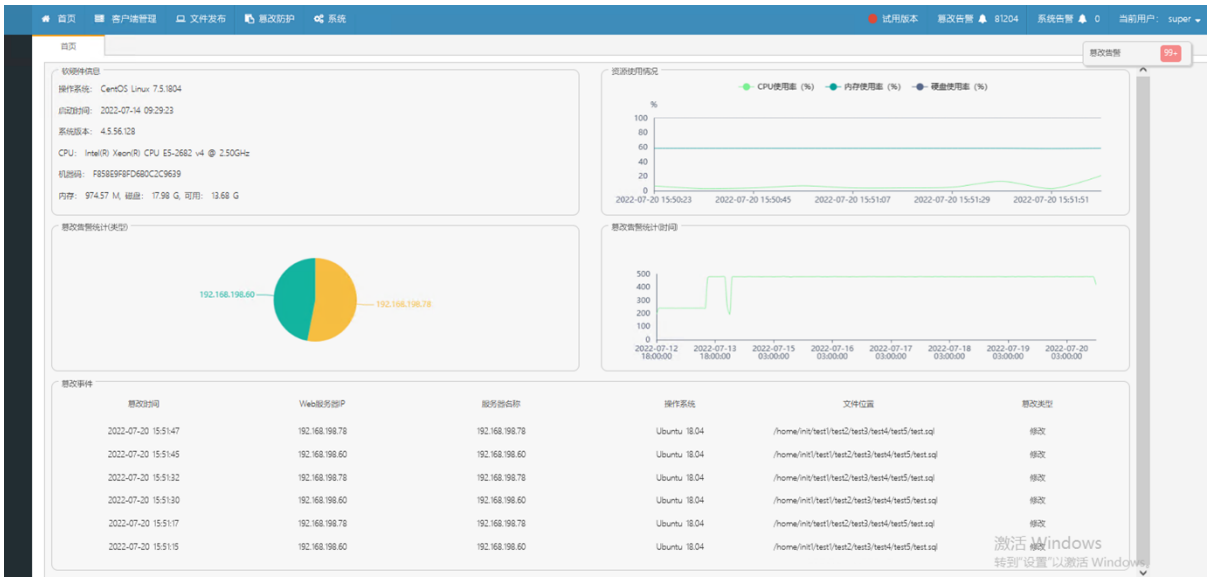
4.4.2 登录

1. 登录页面，输入正确的登录名和密码，点击【登录】按钮，进入系统首页，首次登录需使用super 登录，导入许可证，防护功能才能正常使用，如下图，点击左侧系统-系统配置-许可证-更新，将可用的许可证文件上传。



备注：默认账号以及账号权限分配可咨询厂商。

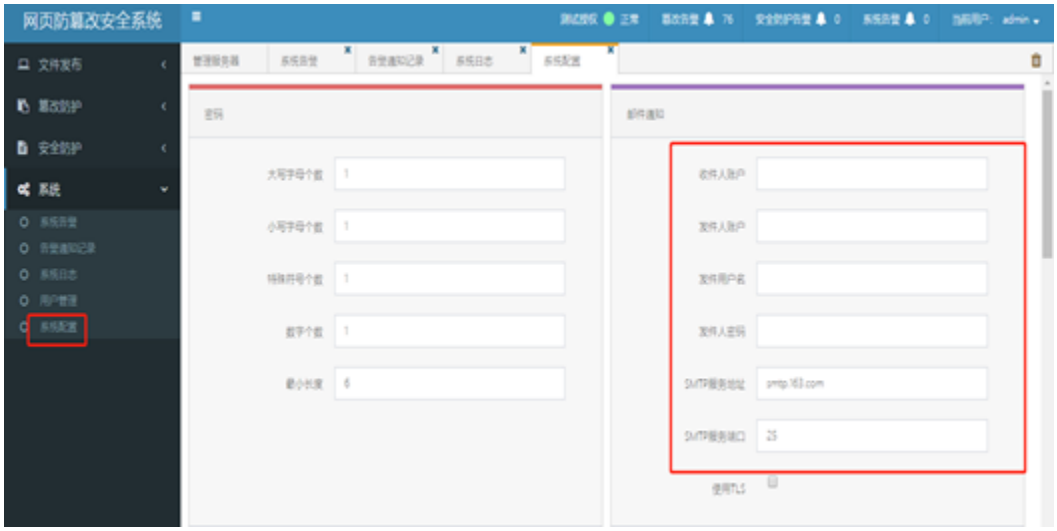
2.登录后的主界面：



3. 如果登录名或密码输入错误时，登录失败，系统会弹出提示。当密码错误的登录失败次数大于5 次（可在系统配置中设置“允许失败次数”）时，该账户会被锁定，管理员用户有解锁权限。

4.4.3 密码找回

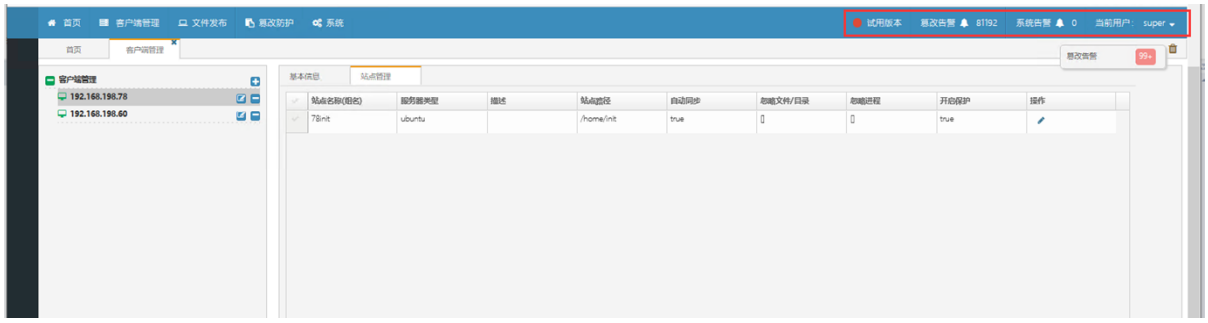
密码找回功能需要 super 或者 admin 用户配置好邮件通知设置，且每个账号需要配置好自己的邮箱，然后在登录页面上输入用户名点击找回密码，会自动发送新密码给用户邮箱。



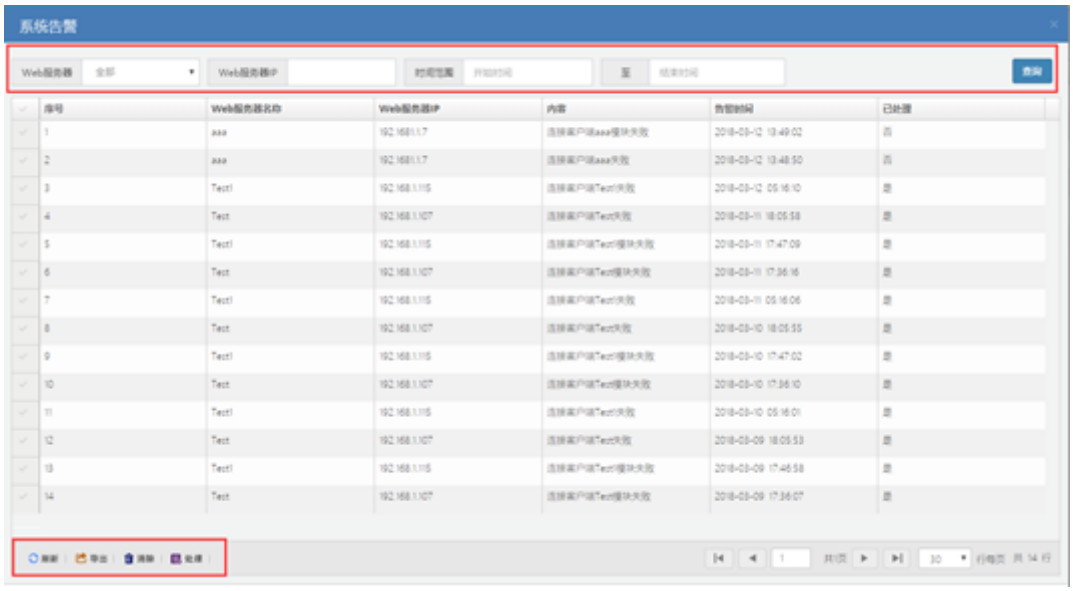
4.5 首页

4.5.1 页面顶部

页面顶部右上角显示“许可证状态”、“篡改告警”、“系统告警通知”、“当前登录账户”和按钮。



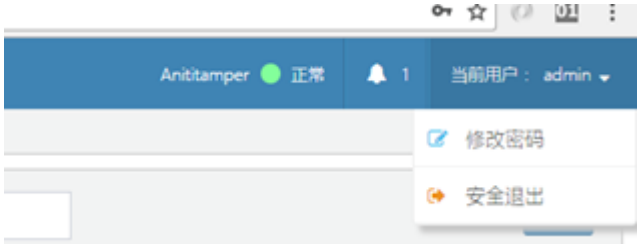
- 许可证状态有四种：无许可证、正常、剩余 x 天、过期 x 天。
- 篡改告警，提示当前的所有篡改告警数量，点击【篡改告警】，打开篡改告警列表（列表内容详见 3.1 章节）。
- 系统告警，提示未处理的告警数量，点击【系统告警】，打开系统告警列表。



a) 上图顶部红框中，通过“Web 服务器”、“Web 服务器 IP”和“时间范围”筛选条件，对系统告警数据进行筛选查询。

b) 上图底部红框中，通过操作【刷新】按钮刷新列表，通过【导出】按钮将列表内容导出并保存为 csv 文件，通过【清除】清空系统告警列表，通过【处理】按钮对单条或多条告警信息进行处理。

- 首页右上角显示“当前登录账户”，点击用户名称后的下拉菜单，下拉出现 “修改密码”和“安全退出”。



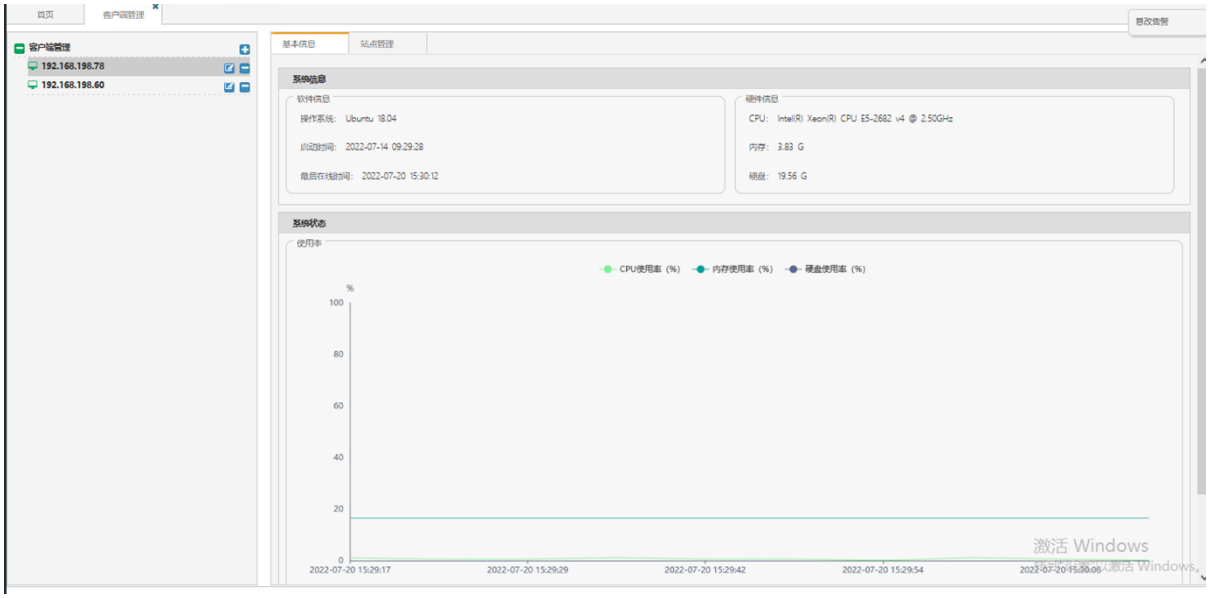
a) 点击【修改密码】，可修改当前登录账户的密码。

b) 点击【安全退出】，系统退出到登录页面。

- 页面右上角登录名称下的 按钮，可关闭当前打开的所有页卡，恢复到系统初始化默认的管理服务器页面。

4.5.2 客户端管理

基本信息：基本信息页面，显示所选中的服务器的“系统信息”和“系统状态”，系统信息为软件信息和硬件信息。软件信息：操作系统、启动时间和最后在线时间，硬件信息：cpu、内存和磁盘。系统状态为实时的 CPU、内存和磁盘使用率曲线。



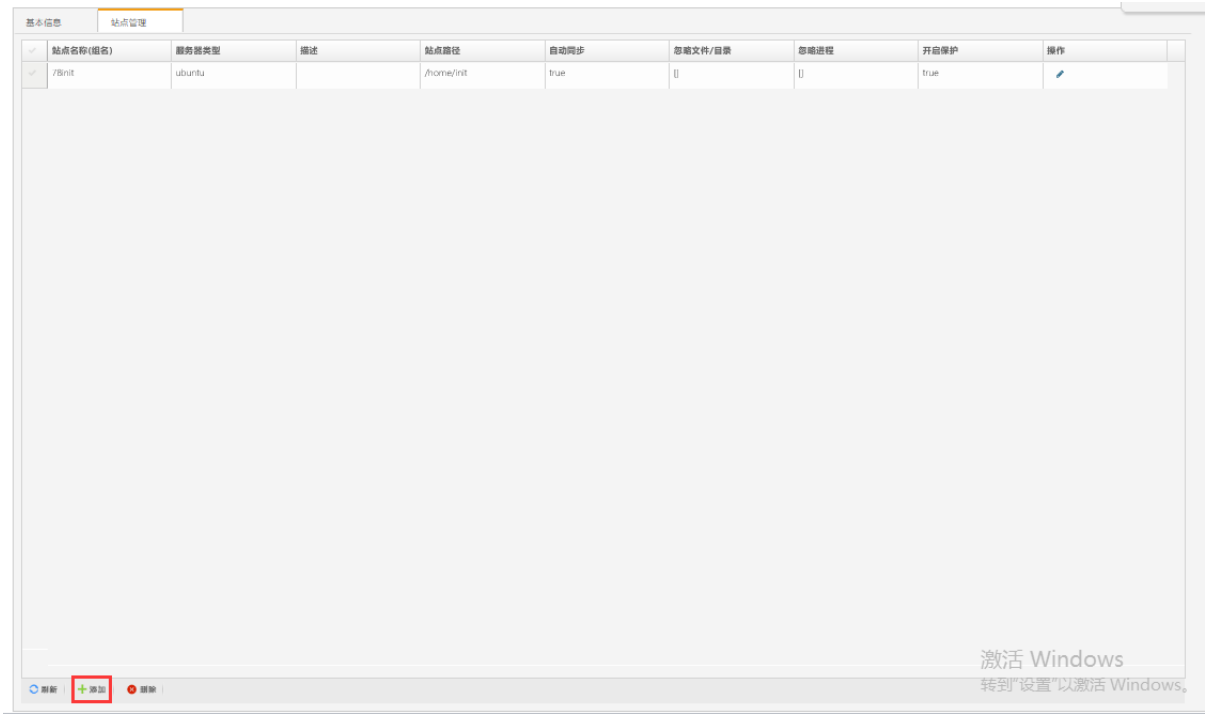
站点管理：可在此处添加站点，点击添加选择站点名称，站点名称为 server 端 ftp 目录下所创建的文件夹名，ftp 目录下创建了几个文件夹这里就会出现几个站点名称可选；服务器类型可自行填写，如 window 某版本或 Linux 的某版本；描述是对该服务器的描述可自行填写，也可不写；站点路径填写的是 server 端的站点同步到 client 端的路径，在 ftp 目录下有

“www_001”和“www_002”两个文件夹，现填写的配置信息表明将 server 端“www_001”目录下的问题同步到 client 端“C:\www”路径下。

是否自动同步可以选择，不选自动同步则需要手动同步；开启保护则是保护 client 端的站点路径，保护开启后，该路径下的文件会被保护起来防止任意篡改；忽略文件/目录，可选择在 client 端站点路径范围以内的某些文件目录或某些文件，对该文件目录或该文件进行忽略，即不保护也不同步，忽略进程，可以将应用的进程添加到防篡改的白名单里，对该进程忽略，这样，该应用可以对保护目录进行修改。

注：添加忽略进程时，要将自动同步取消掉，不然修改的文件也会被同步掉。

选择自动同步，不选择开启保护，则会文件同步，站点路径下的文件或内容可以任意篡改；



4.6 卸载

4.6.1 Windows 版本

进入安装目录 C:\tamper_client，以管理员运行 uninstall.dat 脚本进行卸载，然后将安装目录删除，卸载完成后需要重启服务器才能生效。

4.6.2 Linux 版本

进入客户端安装目录/opt/tamper_client 命令：cd /opt/tamper_client

执行安装目录下面的 uninstall_client.sh 脚本

```
root@ubuntu:~# cd /opt/tamper_client/
root@ubuntu:/opt/tamper_client# ll
total 36
drwxr-xr-x 8 root root 4096 Jul 13 06:48 ./
drwxr-xr-x 3 root root 4096 Jul 13 06:48 ../
drwxr-xr-x 2 root root 4096 Jul 13 06:48 bin/
drwxr-xr-x 7 root root 4096 Jul 13 06:48 dlsync/
drwxr-xr-x 2 root root 4096 Jul 13 06:49 etc/
drwxr-xr-x 2 root root 4096 Jul 13 06:49 km/
drwxr-xr-x 2 root root 4096 Jul 14 01:29 log/
drwxr-xr-x 2 root root 4096 Jul 14 01:29 tmp/
-rwxr-xr-x 1 root root 1145 Jul 13 06:48 uninstall_client.sh*
root@ubuntu:/opt/tamper_client# ./uninstall_client.sh
start uninstall fcg_client
please input password:
```

5. 篡改防护

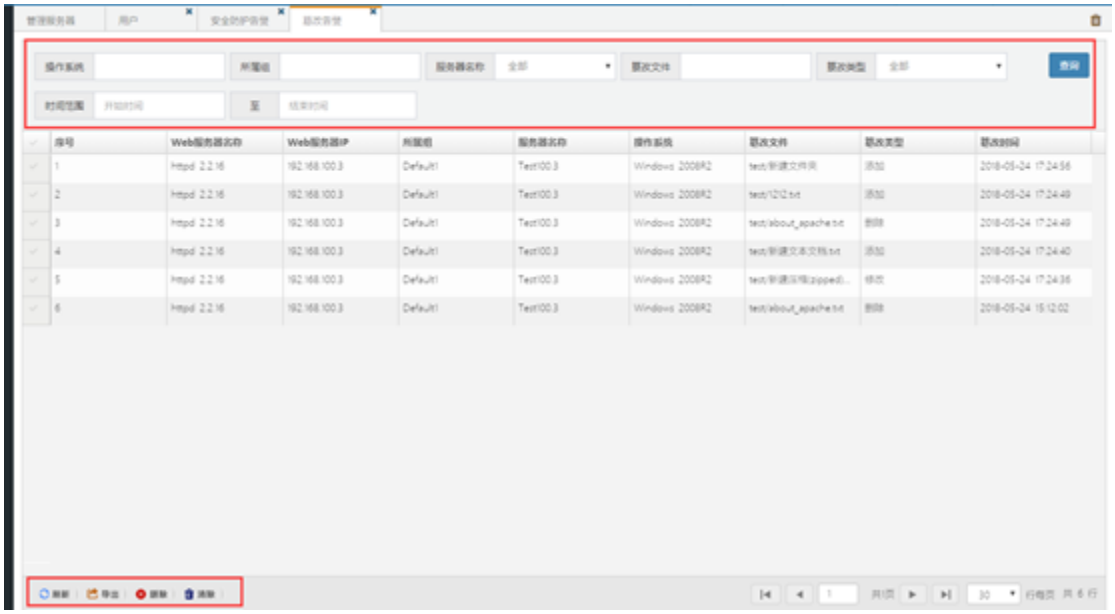
前提条件

请确保您已经安装并登录客户端。具体操作，请参见用户指南。

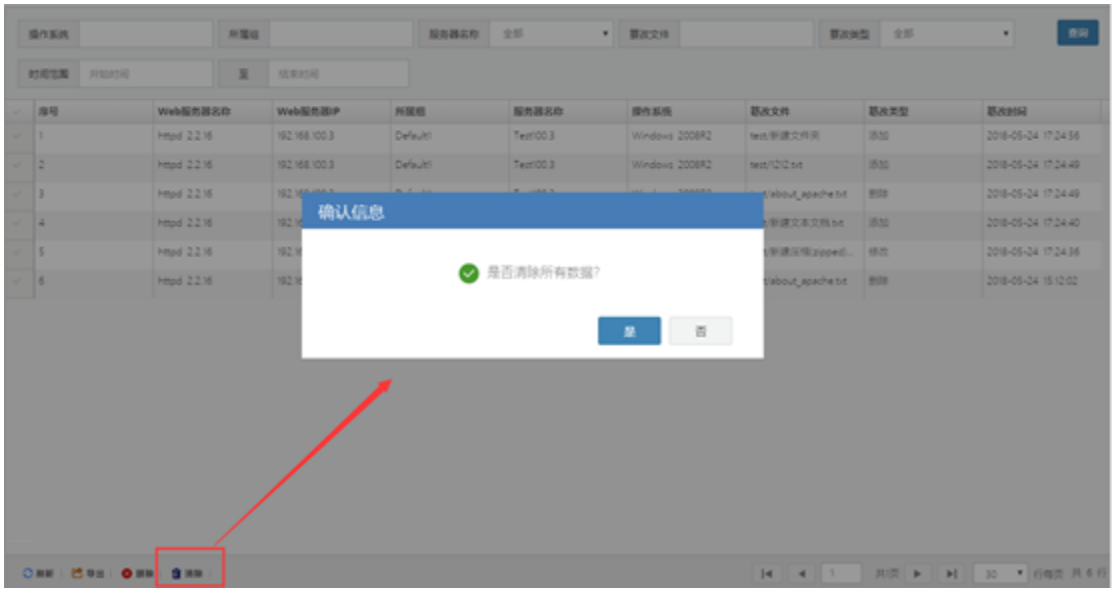
5.1.1 篡改告警

路径：“篡改防护->篡改告警”。

当被保护的 Web 站点的文件或目录被修改后，系统会发出告警信息，并将篡改的文件或目录进行自动恢复。如下图所示，篡改类型包括添加、修改和删除。

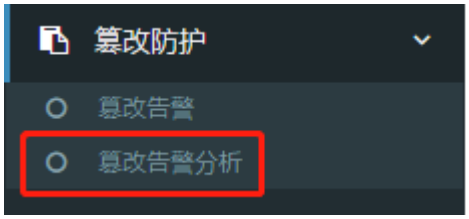


1. 如图所示，列表有查询功能，可通过“操作系统”、“所属组”、“篡改文件”、“篡改类型”、“服务器名称”、“时间范围”等筛选条件对“篡改告警记录”进行查询。
2. 通过【导出】按钮可将当前列表中显示“篡改告警记录”导出到 csv 格式文件。通过【删除】按钮在列表中勾选数据进行删除；通过【清除】按钮，可将“篡改告警记录”全部清除。

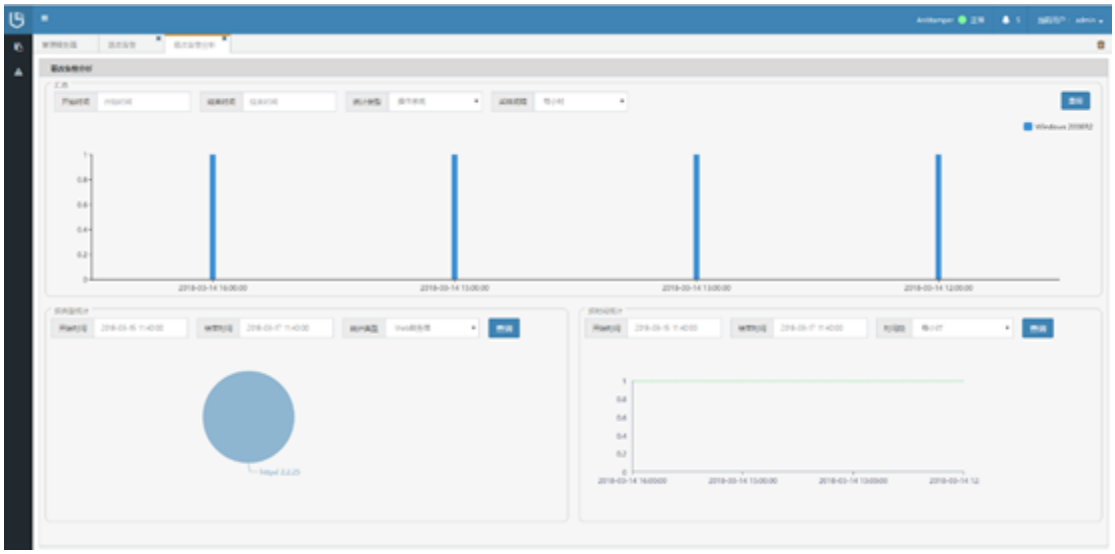


5.1.2 篡改告警分析

路径：“篡改防护->篡改告警分析”。



如下图所示，篡改告警分析包括三部分：汇总、按类型统计、按时间统计。



1. “汇总”统计为柱形图，可根据时间范围、统计类型（操作系统、Web 服务器、服务器）和采集时间间隔（每小时、每天、每周、每月）进行筛选统计。
2. “按类型”统计为饼状图，根据时间范围和统计类型（操作系统、Web 服务器、服务器）进行筛选统计。
3. “按时间”统计为曲线图，根据时间范围和采集时间间隔（每小时、每天、每周、每月）进行筛选统计。

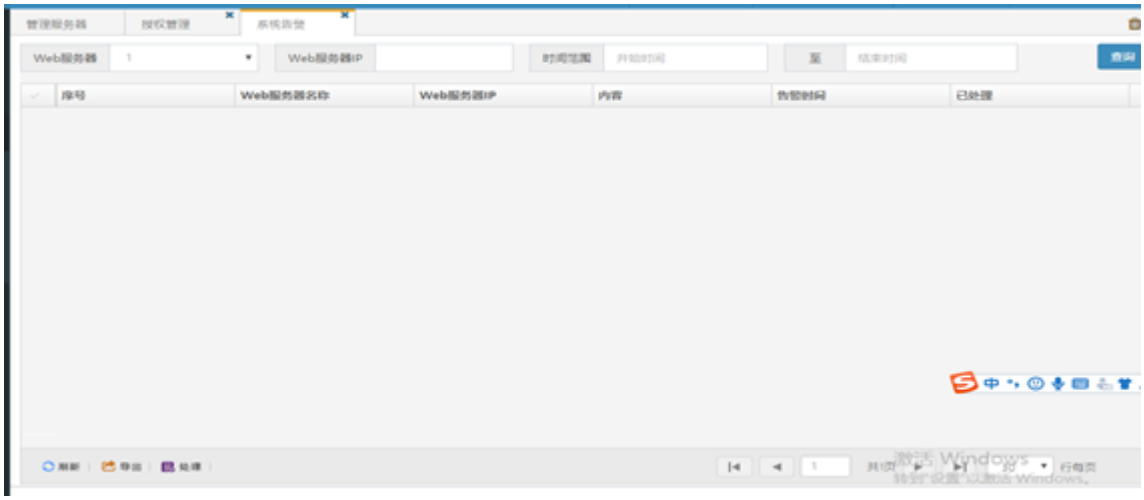
6. 系统

前提条件

请确保您已经安装并登录客户端。具体操作，请参见用户指南。

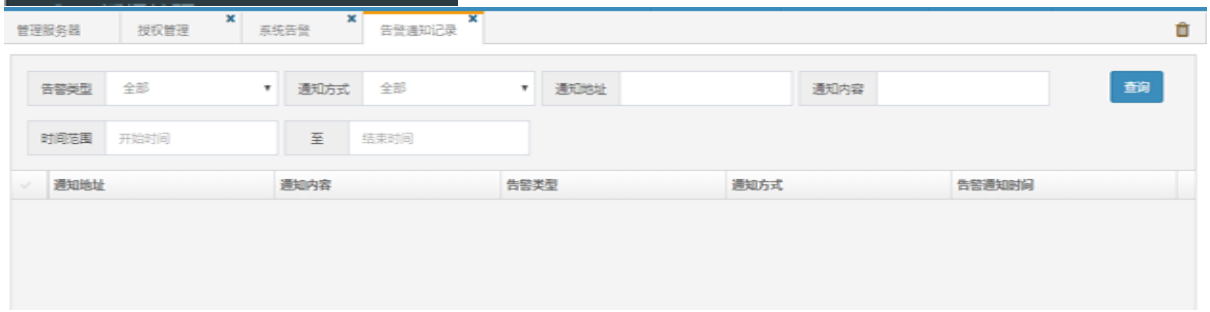
6.1.1 系统告警

路径： “系统->系统告警”



6.1.2 告警通知记录

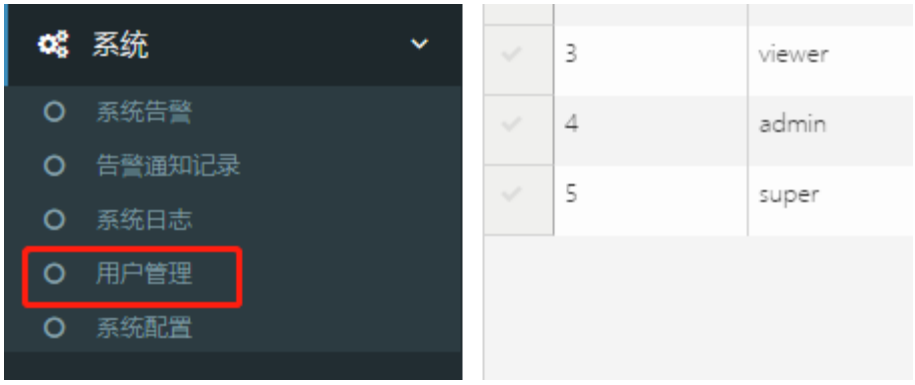
路径：“系统->系统告警”



当系统配置了邮件或短信形式的告警通知之后，可在告警通知记录中查询，且支持按照告警类型、通知方式、通知地址、通知内容以及时间的筛选查询。

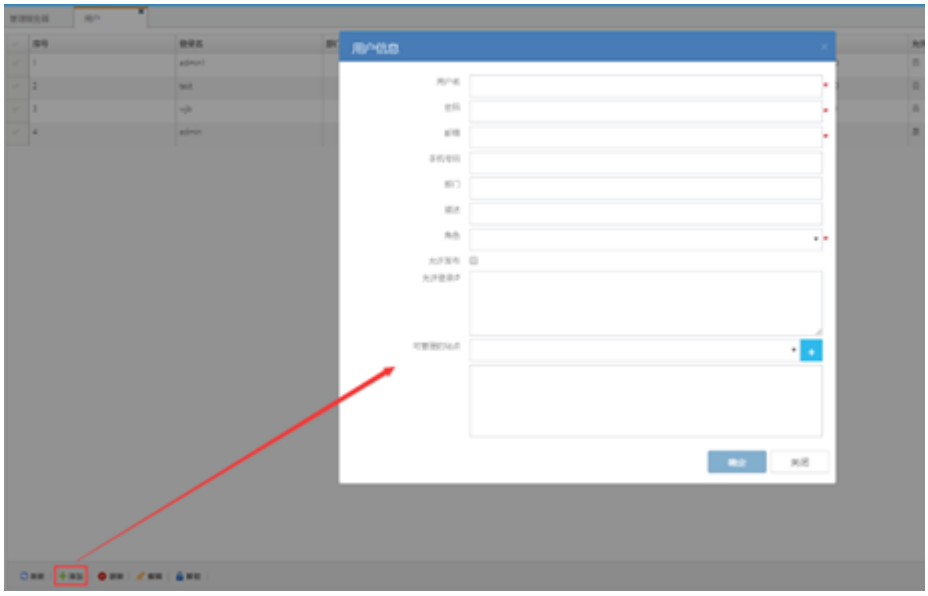
6.1.3 用户管理

路径：“系统->用户管理”。

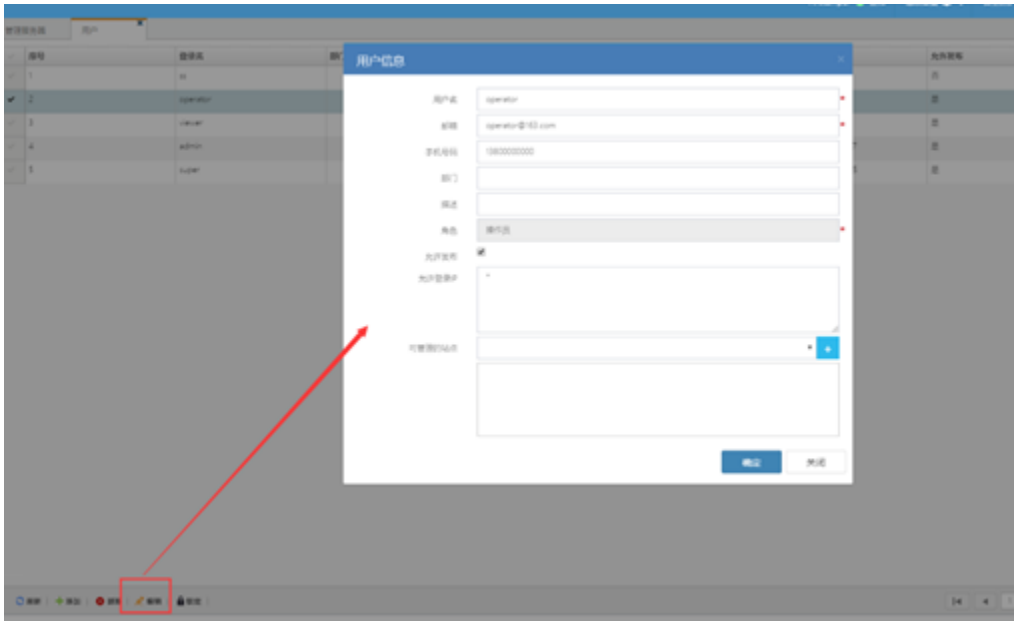


1. 管理员用户 admin 登录，可见所有用户信息，并可以进行添加、修改、删除、解锁等操作。

a) 页面底部【添加】按钮，可打开用户信息编辑页面，添加新用户（如下图，图中带*号的项为必填）

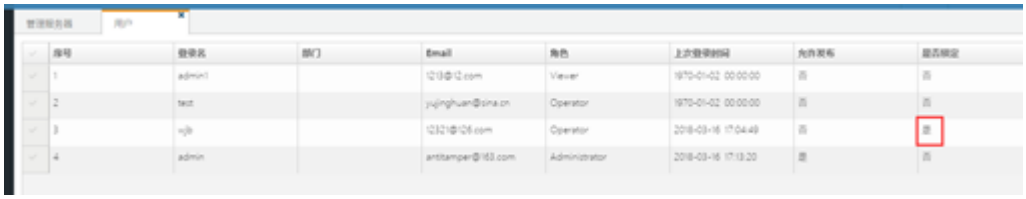


b) 用户列表中，勾选一用户信息，点击页面底部【编辑】按钮，打开用户编辑页面，可修改该用户的信息。



c) 用户列表中，勾选一用户信息，点击页面底部【删除】按钮，可删除该用户的信息。

d) 页面底部【解锁】按钮，解锁用户列表中被锁定用户，勾选该用户点击【解锁】。



2. 普通用户（操作员或审查员）登录，可见所有用户信息，但不可以进行添加、修改、删除、解锁等操作。

6.1.4 授权管理

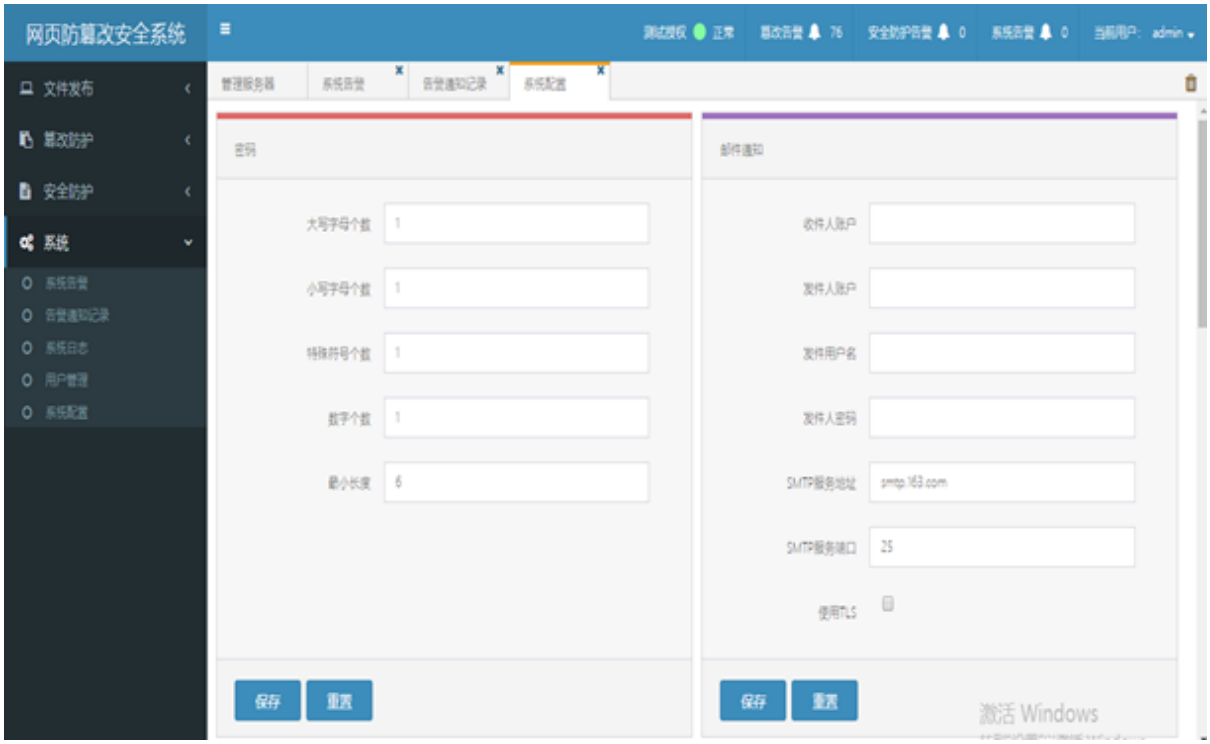
路径：“系统->授权管理”。

“授权管理”以列表形式展示系统许可证更新的历史记录，授权历史信息为只读不可编辑或删除。

6.1.5 系统配置

路径：“系统->系统配置”，仅管理员账户 super/admin 可见。

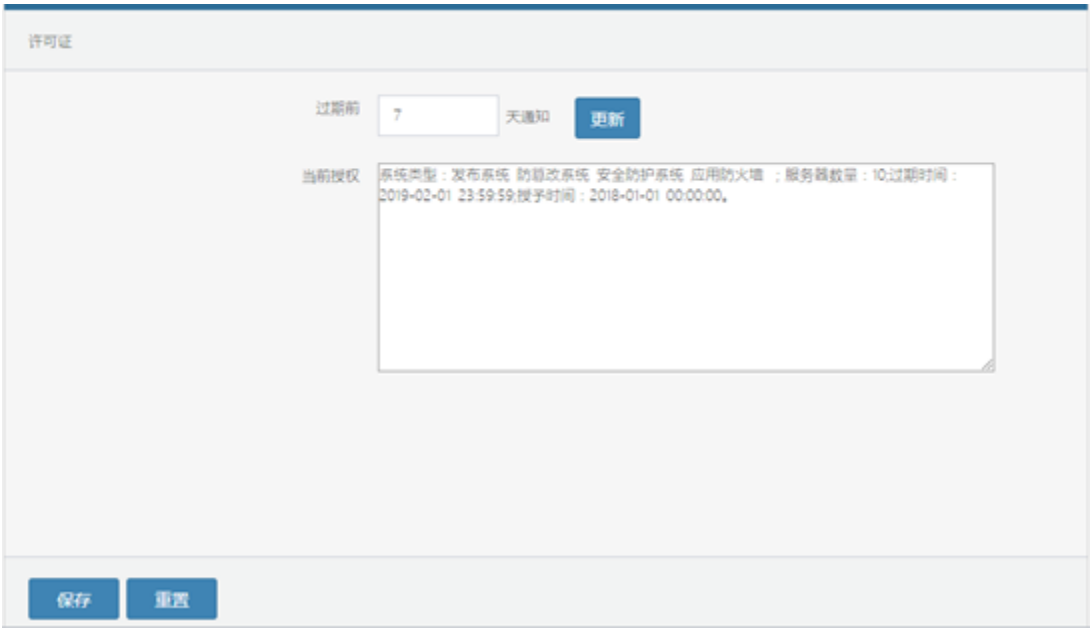
系统配置包括四个部分：系统登录“密码”格式的配置、“邮件通知”的配置、系统“许可证”更新、还有“其他配置”和“通知设置”，如下图所示，图中系统配置为初始化状态。



1. “密码”格式配置包括“大写字母个数”、“小写字母个数”、“特殊符号个数”、“数字个数”和“密码最小长度”（如上图所示），不需要配置的项清空即可。

2.“邮件通知”配置内容如图所示，所有账户及地址和密码、及服务地址和端口都必须配置正确。

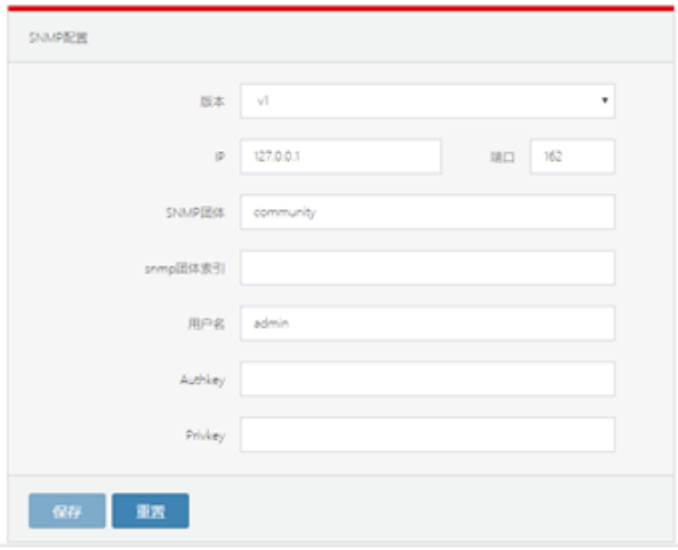
3.系统默认无“许可证”，需要手动添加，并可设置过期前多少天通知，如下图所示，添加“许可证”之后就显示当前授权的信息。



4. “其他配置”为“邮箱通知时间间隔”、“允许登录失败次数”、“保留日志天数”，这些数值都不能设置为 0。

5. “通知设置”包括“Syslog 启用”和“SNMP 启用”，其中“Syslog 配置”如下图：

“SNMP 配置”如下图：



6.1.6 系统日志

路径：“系统->系统日志”。

系统日志功能是对登录账户对系统的操作行为进行记录，如下图所示，可根据“级别”、“时间范围”两个筛选条件进行日志信息查询；可通过列表底部【导出】按钮将日志导出到 csv 文件，也可通过【清除】按钮将日志信息清空。

7. 常见问题

7.1 知识类

Q：网页防篡改的整体架构是什么？

A：网页防篡改分为服务端和客户端，其中服务端包含备份端（发布目录），windows 默认的发布目录为 c:/ftp,linux 发布端默认为/var/www/ftp。在部署完网页防篡改之后网站更新时均在发布目录更新，发布目录会自动同步之网站目录。

7.2 操作类

Q：网页防篡改系统分为两个部分，安装时有什么顺序要求吗？安装过程中应该注意那些问题？

A：网页防篡改系统分为服务端和客户端，一般是先安装服务端，再安装客户端。在安装管理客户端时要注意服务端 ip 的设置及相应的端口开放，端口开放情况为：
服务端需要开放 tcp1443 端口：用于 web 管理登录对管理人员开放 Udp 8020 端口：用于告警通知对客户端 ip 放行
客户端需开放 tcp 8011 端口对服务端开放

Q：安装完成后，查看服务器列表中相应的服务器显示为灰色，Client 端没连上应该如何处理？

A：这可能有几种情况：
查看 Server 端和 Client 端的通信是否正常；
检查 Server 端和 Client 端的端口是否开放，默认端口为 8011、8020；

Q：上传网页文件时，出现无法更新的情况该如何处理？

A：可能会有以下几种可能：
查看网络通讯是否正常，检查服务端和客户端网络是否可达及端口开放情况是否正确。
查看更新目录是否在监控策略目录下，如在监控目录下无法更新，如需更新需在更新监控策略。

Q：保护站点的有些目录不需要监控，如何设置？

A：可在服务端的管理页面设置忽略文件/目录

Q：如何修改网页防篡改 web 管理界面使用的端口?

A：1、使用记事本修改 httpd-ssl.conf 文件中监听的端口两个位置，如下图，默认端口是 1443，修改后保存，文件所在目录为 C:\tamper_server\Apache24\conf\extra\

```
#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
Listen 1443

##
## SSL Virtual Host Context
##

<VirtualHost _default_:1443>

#   General setup for the virtual host
DocumentRoot "${SRVROOT}/htdocs"
```

2、打开资源管理器，重启 AntitamperAapche24 服务，或者直接重新启动服务器。

8. 文档下载

8.1 使用手册

网页防篡改用户使用指南.pdf

8.2 安装包

Windows（支持 Winserver2008、2012、2016 版本）
Linux 版本-Centos/RHEL 系列

9. 相关协议

天翼云网页防篡改服务协议：https://www.ctyun.cn/portal/protocol/10027990