

天翼云 · 网页防篡改 用户使用指南

目 录

1	概述	5
1.1	产品定义	5
1.2	术语解释	5
1.3	产品功能	5
	文件篡改防护.....	5
	网站攻击行为防护.....	5
	网站文件发布与备份.....	6
	日志与告警.....	6
	系统管理和防护功能.....	7
1.4	功能特点	8
1.5	应用场景	8
2	购买指南	9
2.1	规格.....	9
2.2	购买.....	9
2.3	升级.....	10
2.4	续订.....	11
2.5	退订.....	12
3	快速入门	12
3.1	安装网页防篡改集中管理中心.....	12

3.2	登录.....	12
3.3	获取机器码.....	13
3.4	授权文件导入.....	13
3.5	配置客户端及站点.....	14
3.5.1	安装监控代理.....	14
3.5.2	添加服务器.....	14
3.5.3	添加站点.....	15
3.5.4	测试及发布.....	16
3.6	端口开放情况.....	17
4	操作指南.....	17
4.1	网页防篡改 SERVER 端安装.....	17
4.2	客户端安装.....	19
4.2.1	Windows (支持 Winserver2008、2012、2016 版本).....	19
4.2.2	客户端 Linux 版本安装.....	24
4.3	登录.....	26
4.3.1	系统访问.....	26
4.3.2	登录.....	26
4.3.3	密码找回.....	28
4.4	首页.....	28
4.4.1	页面顶部.....	28
4.4.2	管理服务器.....	30

4.5	篡改防护	33
4.5.1	篡改告警	33
4.5.2	篡改告警分析	34
4.6	安全防护	35
4.6.1	安全防护告警	35
4.6.2	安全防护告警分析	36
4.7	系统	36
4.7.1	系统告警	36
4.7.2	告警通知记录	37
4.7.3	用户管理	38
4.7.4	授权管理	39
4.7.5	系统配置	40
4.7.6	系统日志	42
4.8	端口开放情况	43
4.9	网页防篡改卸载	43
4.9.1	Client 端卸载	43
5	常见问题	44
5.1	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？	44
5.2	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？	45
5.3	上传网页文件时，出现无法更新的情况该如何处理？	45
5.4	保护站点的有些目录不需要监控，如何设置？	45

5.5	网页防篡改的整体架构是什么?	45
5.6	如何修改网页防篡改 WEB 管理界面使用的端口?	45

1 概述

1.1 产品定义

网页防篡改（GT-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 术语解释

监控代理：安装在 web 站点服务器上，主要用于监控站点状态，执行管理中心所配置的策略，本地生效。

集中管理中心：主要用于用户管理，策略下发，日志监控，以及管理各安装监控代理的服务器；

1.3 产品功能

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；

异地（非网站目录）保留篡改后的页面篡改后快照，包括页面修改，和新增

支持忽略保护策略；正则表达式；忽略篡改保护；

支持 Https 的网站篡改检测，HTTPS 网站防篡改，理论上嵌入应该直接支持；

保护防篡改内嵌模块和守护进程自己；

网站攻击行为防护

能够防止 SQL 数据库注入式攻击；

能够防止跨站脚本漏洞；

能够防止网站盗链；

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；可按照条件（按时间戳前，后，区间；按子文件夹；按 WEB 服务器）；

支持双机热备功能；

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；

告警的通知包括手机短信通知、邮件通知、管理界面警示框；

图形报表的综合统计和分析；

SQL 注入告警：

记录网站 SQL 注入攻击的行为；

告警查询，导出成 excel，自动清除，全部清除功能；

告警的通知包括手机短信通知、邮件通知、管理界面警示框；

图形报表的综合统计和分析；

盗链告警：

记录网站盗链行为；

告警查询，导出成 excel，自动清除，全部清除功能；

告警的通知包括手机短信通知、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；

授权方式：最小授权单位为一台 web 服务器硬件主机；

授权类型：按时间，按服务器硬件主机数量按系统类型；

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 功能特点

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；

1.5 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 购买指南

2.1 规格


网页防篡改根据 web 服务器的数量收费，如：有两个网站，放置于同一个 web 服务器上，购买一个 license 即可，如存在于两个服务器上，需购买两个 license。

产品名称	规格	产品计价
网页防篡改	Web 服务器台数	980 元/台/ 月

（享受一年 85 折扣、两年 7 折、三年 5 折）

2.2 购买

用户需要先安装网页防篡改集中管理中心，确保已获取了产品机器码，并且开放了 1443 端口然后购买网页防篡改的授权。安装和获取机器码参考 3.1 章。

在天翼云官网找到网页防篡改介绍页面，点击“立即开通”或者在控制中心找到网页防篡改产品点击“”，填写订购需求，支付完成后，3 个工作日内会有电话通知授权开通，用户可以到网页防篡改产品控制台去下载授权文件。

购买须知:

- 1、本订购页购买的是网页防篡改的授权，授权按web服务器台数和产品使用周期收费。以授权文件交付，可在控制台下载。
- 2、须单独一台云主机部署网页防篡改镜像，请确保已完成网页防篡改的安装，并开放1443端口再订购授权。

订购数量: 订购数量指需要监管的web服务器台数

实例名称:

机器码:
安装完网页防篡改控制端，登录控制端获取机器码，具体操作查看 [《网页防篡改用户使用指南》](#)

IP地址:
授权需要，请提供装有网页防篡改的云主机的弹性IP地址。

购买时长: 1个月 2个月 3个月 4个月 5个月 6个月 7个月 8个月 9个月 10个月 11个月 1年 2年 3年
85折 7折 5折

费用总计 **980.00** 元 **立即订购**

我已阅读，理解并接受 [《天翼云网页防篡改服务协议》](#)

2.3 升级

用户可以通过升级操作购买更多 web 服务器监管权限。升级操作在网页防篡改实例列表页面进行操作。



实例名称	web服务器个数	开通时间	截止时间	授权文件	操作
ctwt-fn7z	1	2019-07-19 14:54:09	2019-08-19 14:54:09 已过期	bssupload 下载	升级 续订
ctwt-n3wu	1	2019-07-19 15:01:49	2019-08-19 15:01:49 已过期	bssupload 下载	升级 续订

共 2 条 [<](#) [1](#) [>](#) [前往](#) 页

点击“升级”弹出升级弹窗，填写需要新增的 web 服务器台数，确认升级信息完成支付。3 个工作日内会有电话通知授权配置完成，用户可以到网页防篡改产品控制台去下载授权文件。

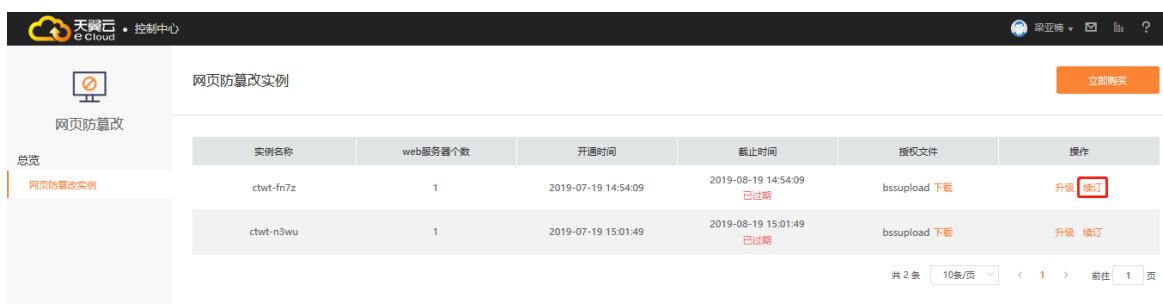
注：承载的 web 服务器台数增多涉及云主机的配置也需要对应升级。



2.4续订

用户可以通过续订延长产品使用时限, 续订前需要保证承载网页防篡改的弹性云主机已续订。

在控制台找到网页防篡改产品, 点击进入实例页面。点击“续订”, 弹出续订页面。



选择续订时间, 确认续订信息并完成支付。3个工作日内会有电话通知授权配置完成, 用户可以到网页防篡改产品控制台去下载授权文件。



2.5 退订

无特殊情况本产品不支持退订。

3 快速入门

3.1 安装网页防篡改集中管理中心

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。用户可以以镜像的形式获取集中管理中心安装包也可以通过帮助中心链接：

<https://www.ctyun.cn/help/qslist/2386> 自行下载安装。

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
10-20 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。

3.2 登录

默认访问方式为：<https://服务器ip:1443>，即可访问管理服务端。

默认账号密码如下：super（超级管理员）admin（系统管理员）operator（操作员），viewer（审查员），默认密码统一为 Admin%100

3.3 获取机器码

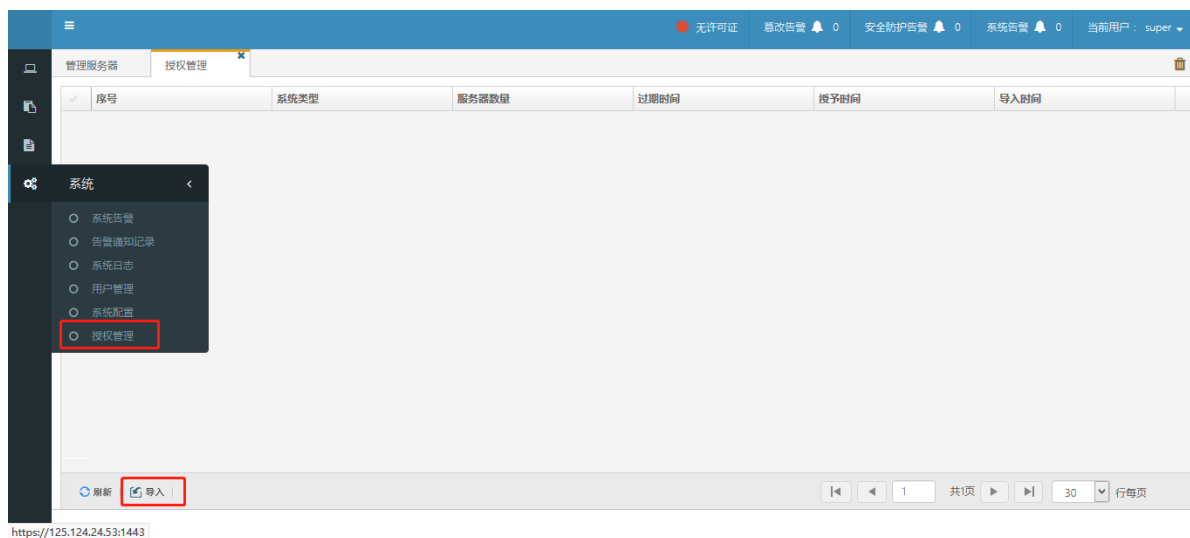
网页防篡改页面登录后，首页即可获取机器码，如下图，



获取到机器码后到天翼云官网购买网页防篡改授权。完成购买后在自己的邮箱查看授权文件。

3.4 授权文件导入

系统->授权管理，点击“导入”，导入授权文件。




3.5 配置客户端及站点


3.5.1 安装监控代理

待管理的 web 服务器需要安装对应的监控代理。

以镜像的形式安装网页防篡改集中管理中心，只需要到 C:\tamper_server\client_package 路径下查找监控代理。以软件形式获取安装包可通过链接 <https://www.ctyun.cn/help/qslist/2386> 找到所需的监控代理。安装步骤详见 4.2


3.5.2 添加服务器

点击管理服务器下的 ，在弹出的 web 服务器界面，填入客户端名字（自定义），IP（客户端的 IP），描述（自定义），同步文件端口和通知端口（默认填写即可）。



Web服务器

名称	<input type="text"/>
IP	<input type="text"/> IPV6 <input type="checkbox"/>
描述	<input type="text"/>
同步文件端口	<input type="text" value="8011"/>
通知端口	<input type="text" value="8020"/>

填写完成后，客户端会显示在线，正常在线为绿色表示。如显示为灰色 ，则需要检查客户端配置及两端的服务启动情况。

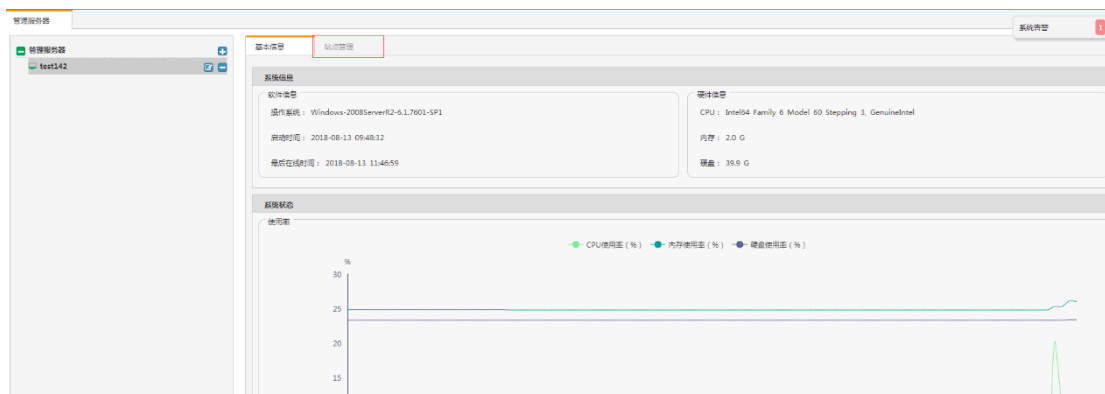


客户端正常连接之后，需要配置保护站点，先确定保护站点路径，及将站点目录完成备份至服务端操作系统的 C:\ftp 目录下（默认 windows 服务端的发布目录为 C:\ftp 下，Linux 服务端的发布目录为 /var/www/ftp 下）。如需更改发布目录，windows 修改方式：修改 C:\tamper_server\etc\publish_server.conf 文件中的 publish_root_path = c:/ftp 属性，填写将要修改的目录即可。Linux 修改方式：修改 /opt/tamper_server/etc/publish_server.conf 文件中的 publish_root_path = /var/www/ftp

以下我们 C:\www 为保护目录为例，在服务端 C:\ftp 目录下建立发布目录 beifen-ceshi，将 C:\www 目录下的内容全部备份至 C:\ftp\beifen-ceshi，

3.5.3 添加站点

选中添加的 web 服务器，点击右侧的站点管理



点击添加按钮，在弹出的配置信息中填入信息，如下图所示

站点名称（组名）是在服务端的 ftp 目录下建立的目录的名称，

服务器类型自定义填写，描述内容自定义

站点目录为需要保护的目录的路径(C:\www 为例)，

自动同步，需勾选

忽略文件，可以以文件、目录形式忽略

开启保护，需勾选

配置信息
✕

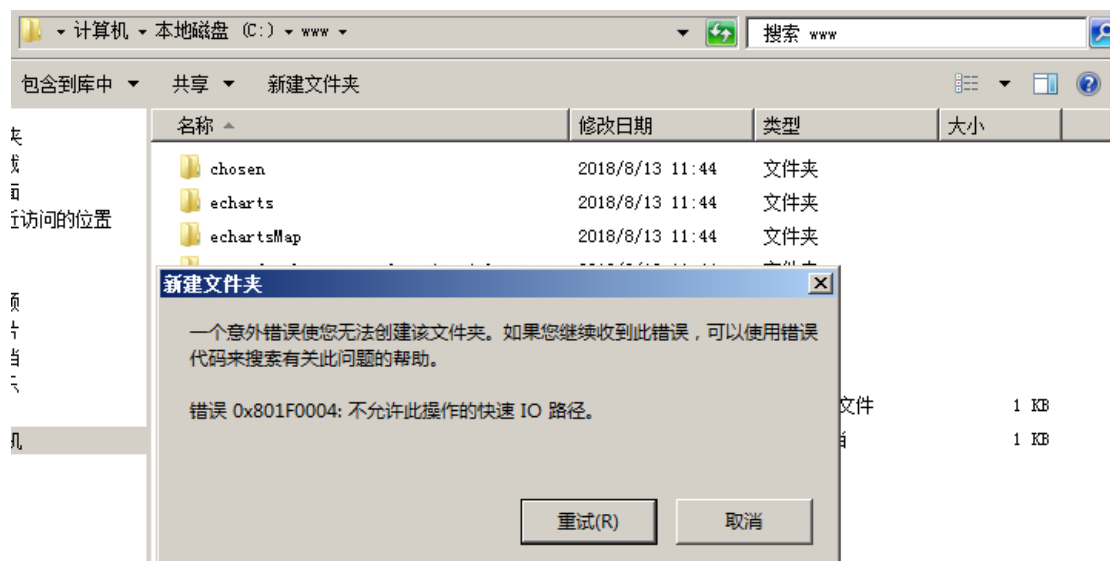
站点名称(组名)	<input type="text" value="beifen-ceshi"/>
服务器类型	<input type="text" value="apache2.2"/>
描述	<input type="text"/>
站点路径	<input type="text" value="C:\www"/>
自动同步	<input checked="" type="checkbox"/>
忽略文件/目录	<input type="text"/> +
开启保护	<input checked="" type="checkbox"/>

确定
关闭

3.5.4 测试及发布

默认 windows 服务端的发布目录为 C:\ftp 下，Linux 服务端的发布目录为/var/www/ftp 下），如更改按照更改后的目录为准，

1. 在发布目录下新增文件，看是否同步至网站目录
2. 测试防篡改：C:\www 保护生效，



测试同步：在服务端的服务器 C:\ftp\beifen-ceshi，新建文件测试看同步是否生效

3.6 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 8010、8011、60001—600010 端口 → 对服务端开放

4 操作指南

4.1 网页防篡改 Server 端安装

以镜像方式安装可忽略一下步骤，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：

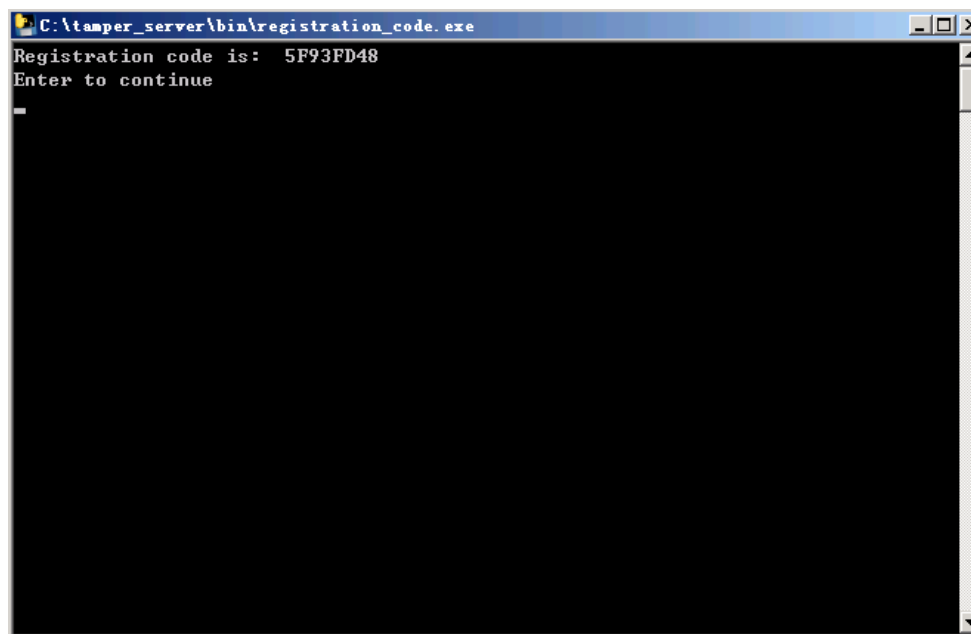
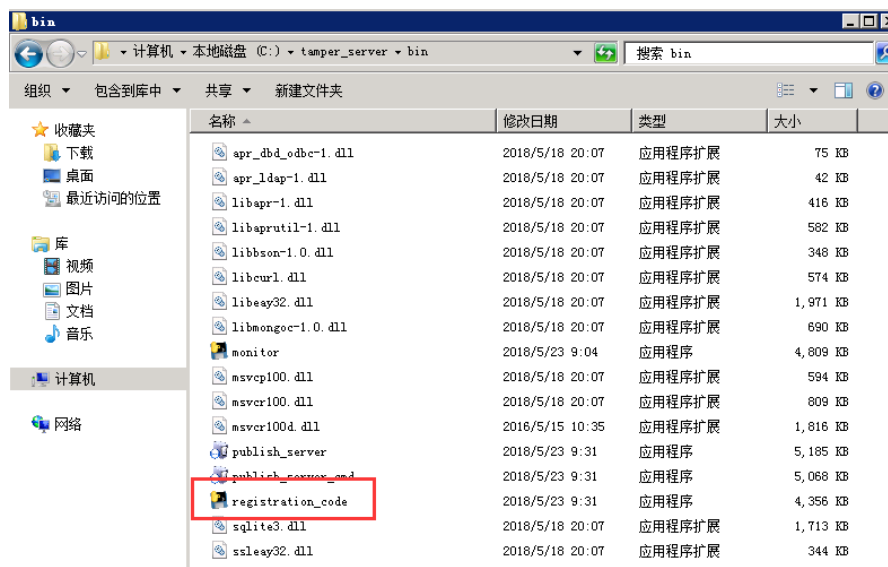
2. 执行安装

f) 检查服务启动情况：

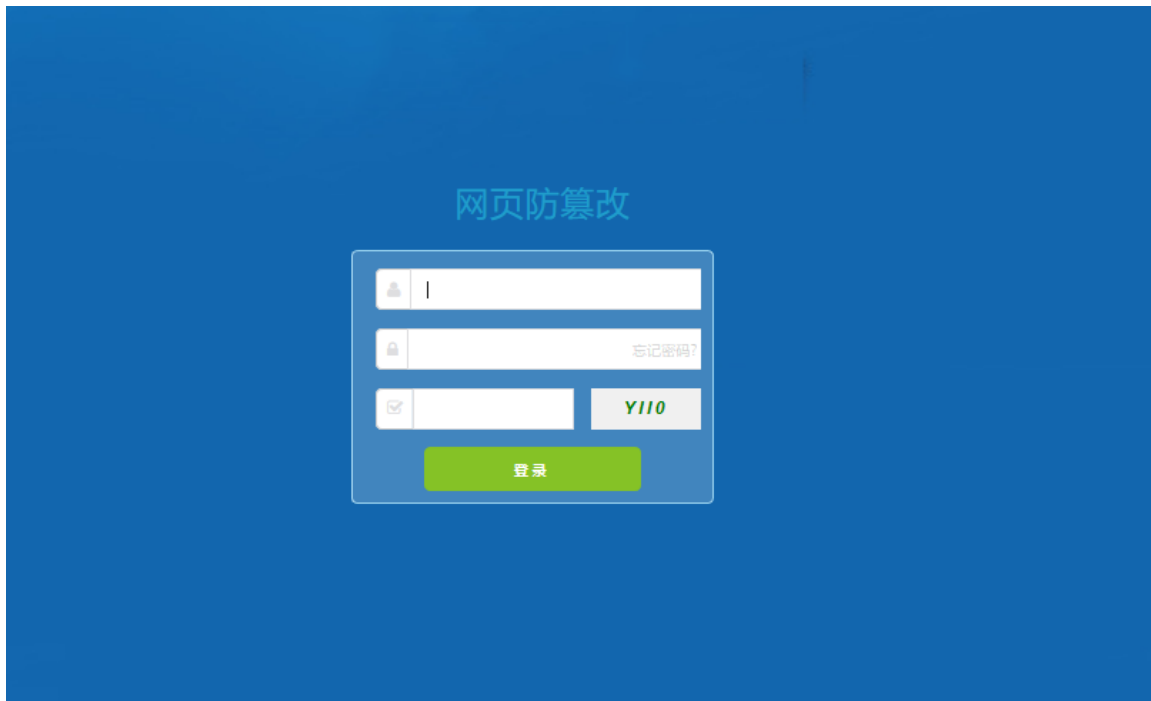
安装完成后，检查系统服务是否已启动：Apache2.2、MongoDB（数据库服务），及 AntitamperPublishService（安装之后不会启动，只有导入授权才能启动）。

默认发布目录为 C:\ftp

g) 安装完成后，需要生成机器码提交给授权制作人员。进入 C:\tamper_server\bin 目录下，双击 registration_code.exe 程序，会自动生成机器码，如下图：



a) 浏览器访问 UI: [https://\[server端服务器IP\]](https://[server端服务器IP])



- b) 用超级管理员账户（super/Admin%100），登录系统后，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。

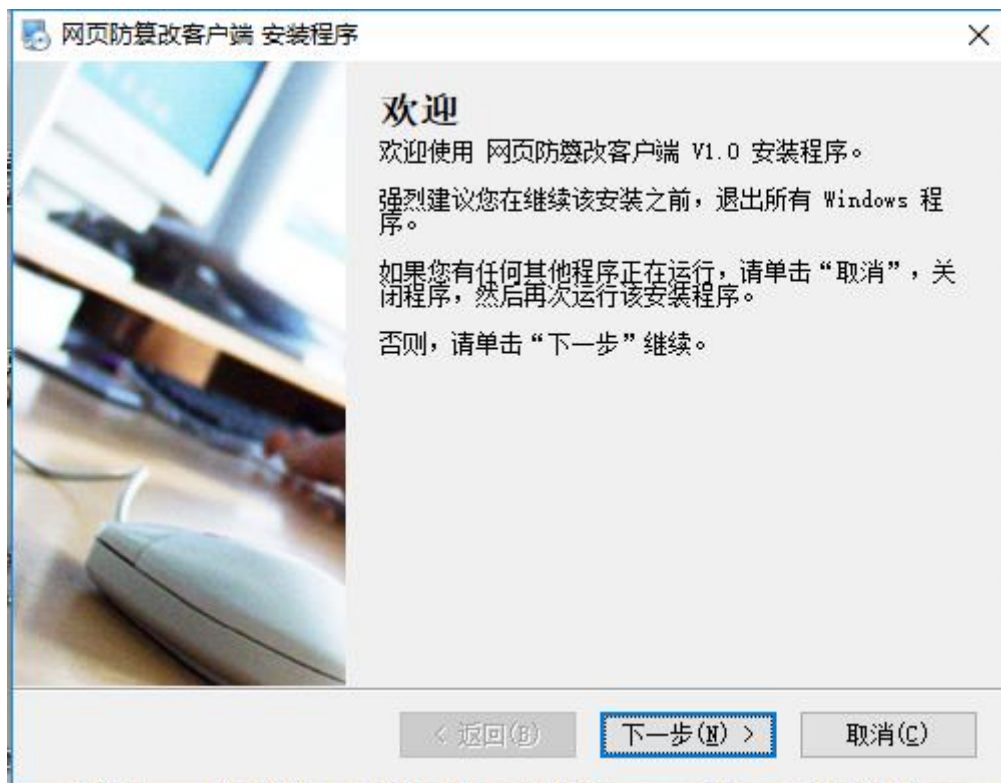
AntitamperClientService - Client S...			自动	本地系统
AntitamperPublishService - Publish...		已启动	自动	本地系统
Apache2.2	Apa...	已启动	自动	本地系统
Application Experience	存		手动	本地系统

4.2 客户端安装

4.2.1 Windows（支持 Winserver2008、2012、2016 版本）

1. 安装包，在光盘中 windows 目录下的 install_client
2. 执行安装

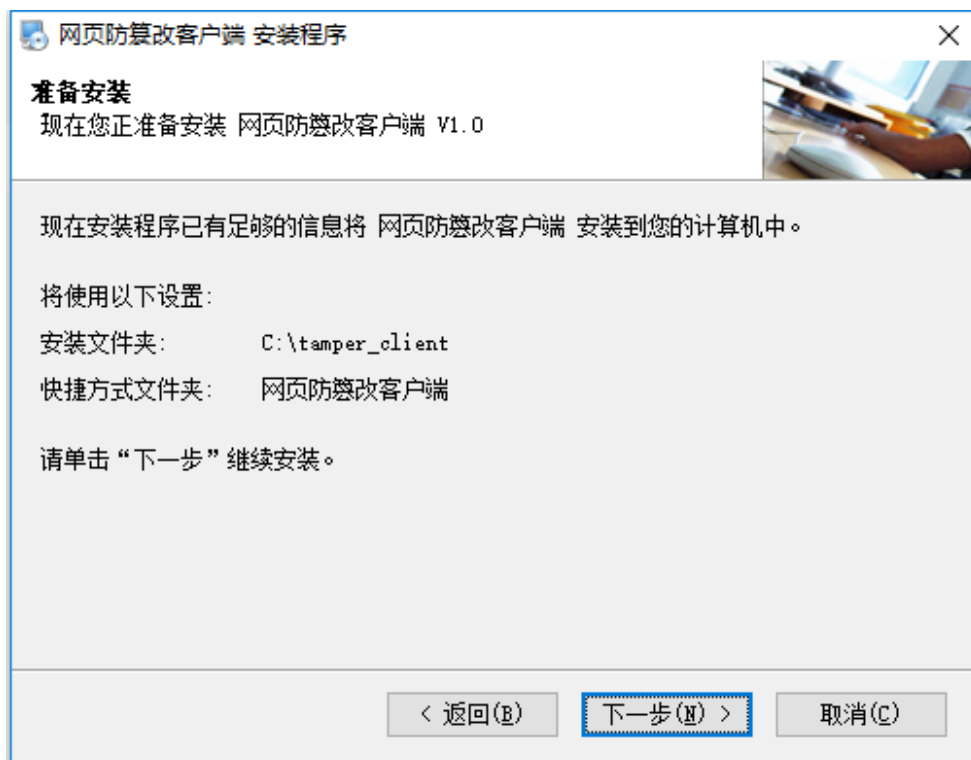
- a) 双击 .exe 程序文件进入安装步骤，如下图所示



b) 点击下一步，输入 server 端 IP 地址。



c) 服务端默认且必须安装在 C:\tamper_server,

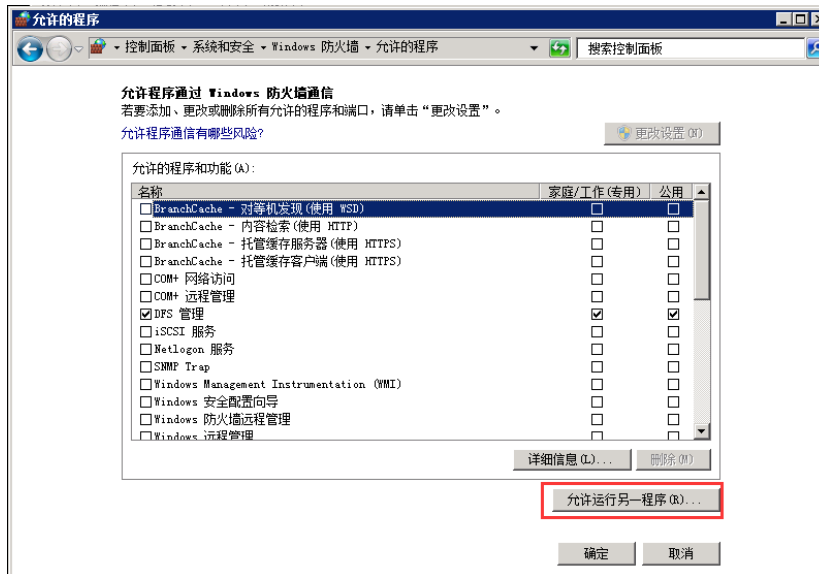


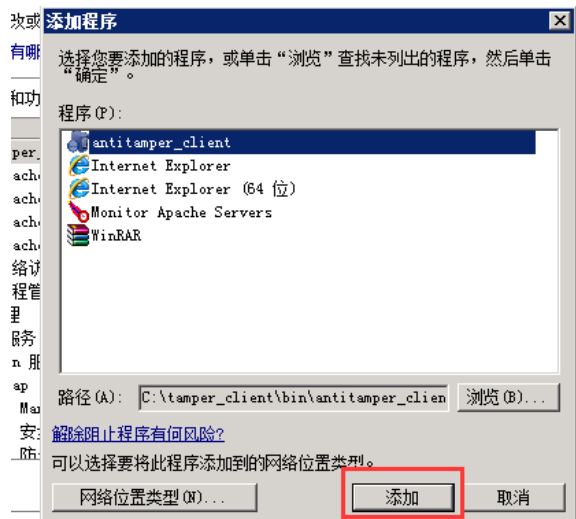
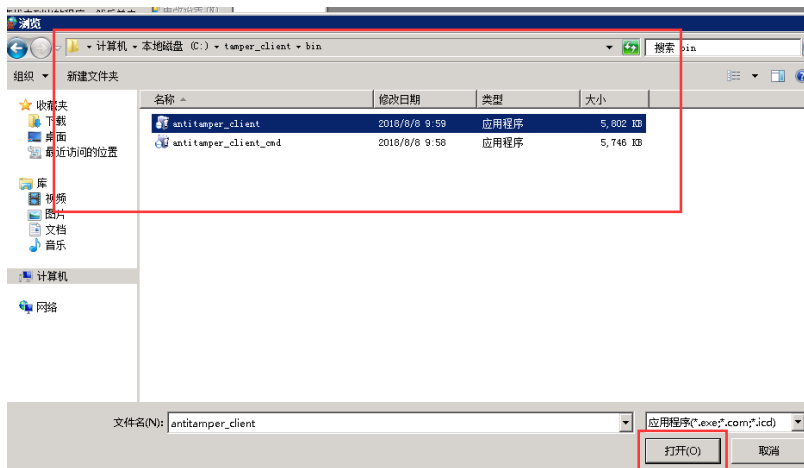
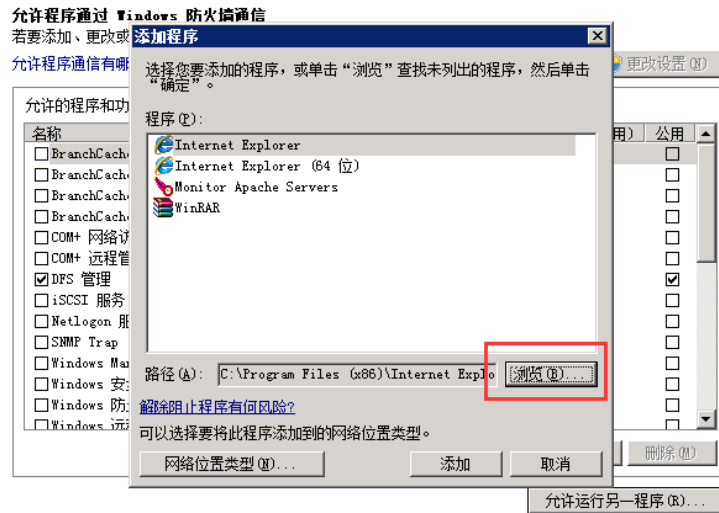
d) 点击下一步即开始安装，安装完成界面如下，



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：





4.2.2 客户端 Linux 版本安装

4.2.2.1 Centos/RHEL 系列

1. 通过上传工具将 antitamper_client_v4.3.20_centos_redhat.tar.gz 上传至 Linux 服务器，
执行解压命令 `tar -zxvf antitamper_client_v4.3.20_centos_redhat.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_v4.3.20_centos_redhat`，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_v4.3.20_centos_redhat_20180808]# ./install.sh
start install client
Input IP:192.168.198.143

InFace List:
lo
eno16777736

net iface 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_v4.3.20_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_v4.3.20_centos_redhat_20180808]# ps aux |grep antitamper_client
root 7549 0.3 0.5 409572 22608 ? S1 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_v4.3.20_centos_redhat_20180808]#
```

Client 端启停命令:

`./antitamper_client start` --启动

`./antitamper_client restart` --重启

`./antitamper_client stop` --停止

特别注意：在防火墙启动的情况下，访问 ftp 需要开发以下端口：

```

# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8011 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8010 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60000 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60001 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60002 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60003 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60004 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60005 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60006 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60007 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60008 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60009 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 60010 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
    
```

4.2.2.2 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_v4.3.20_debian_ubuntu.tar.gz` 上传至 debian 或 Ubuntu 服务器，将 `antitamper_client_v4.3.20_suse.tar.gz` 上传至 Suse 服务器。

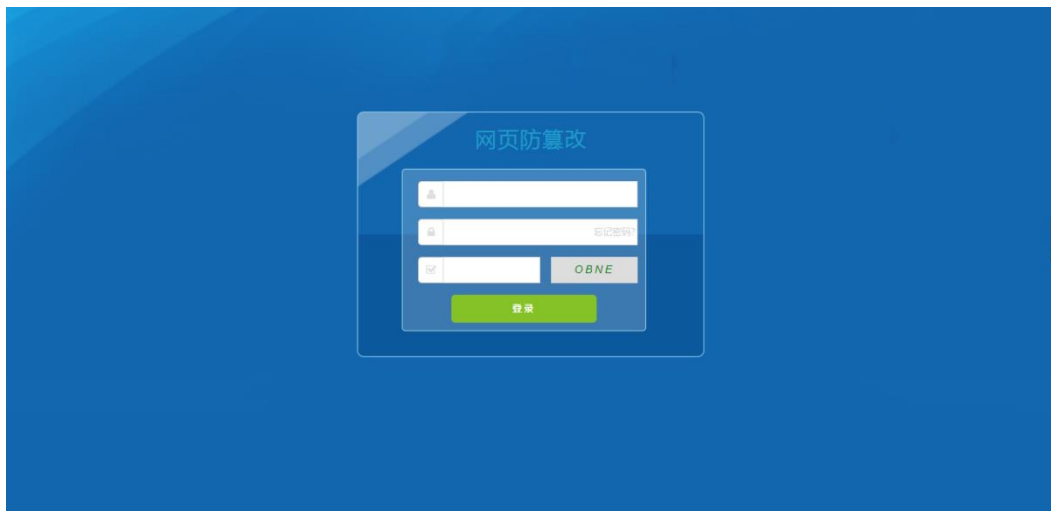
执行解压命令将 `antitamper_client_v4.3.20_debian_ubuntu.tar.gz` 或 `antitamper_client_v4.x_suse.tar.gz` 安装包解压。

2. 具体配置和安装步骤与上一章节“4.2.2.1Centos/RHEL 系列”一致。

4.3 登录

4.3.1 系统访问

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。



4.3.2 登录

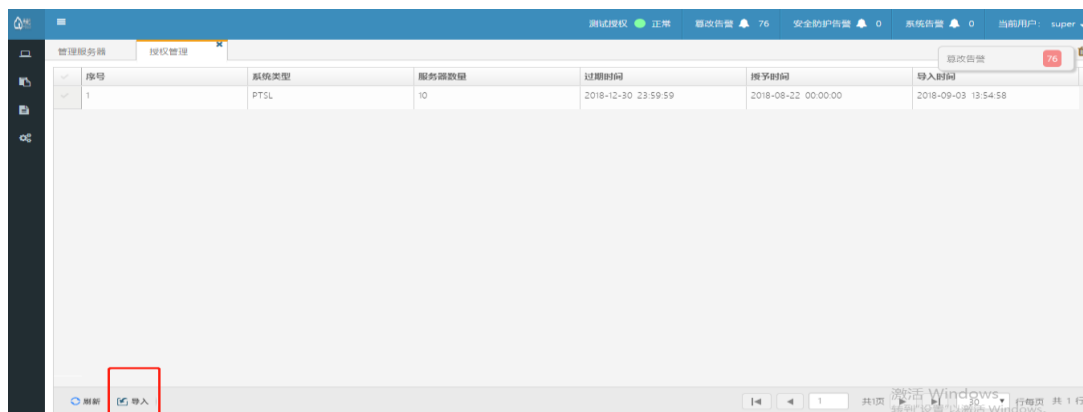
默认账号密码如下：super（超级管理员）admin（系统管理员）

operator（操作员），viewer（审查员），默认密码统一为 Admin%100

默认账户权限分配表如下：

权限 \ 角色	系统管理员 (Admin)	普通管理员 (Operator)	审计用户 (Viewer)	超级用户 (Super)
服务器基本信息	✓	✓	✓	✓
手动同步	✓	✓		✓
服务器编辑/删除	✓	✓		✓
导出、查看篡改告警	✓	✓	✓	✓
删除、清除篡改告警	✓	✓		✓
篡改告警分析	✓	✓	✓	✓
查看安全防护告警	✓	✓	✓	✓
删除、清除安全防护告警	✓	✓		✓
安全防护告警分析	✓	✓	✓	✓
导出、查看告警通知记录	✓	✓	✓	✓
删除、清除告警通知记录	✓	✓		✓
导出、查看系统日志	✓	✓	✓	✓
删除、清除系统日志	✓	✓		✓
查看用户信息	✓			✓
用户管理	✓			✓
授权历史				✓
系统配置	✓			✓
导入授权				✓

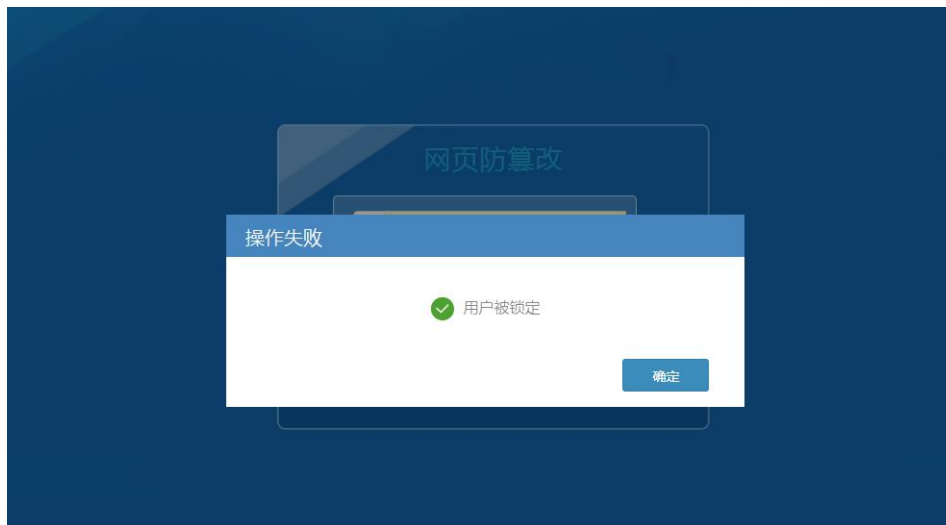
1. 登录页面，输入正确的登录名和密码，点击【登录】按钮，进入系统首页，首次登录需使用 super 登录，导入许可证，防护功能才能正常使用，如下图，点击左侧系统-系统配置-许可证-更新，将可用的许可证文件上传。



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。



4.3.3 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。



4.4 首页

4.4.1 页面顶部

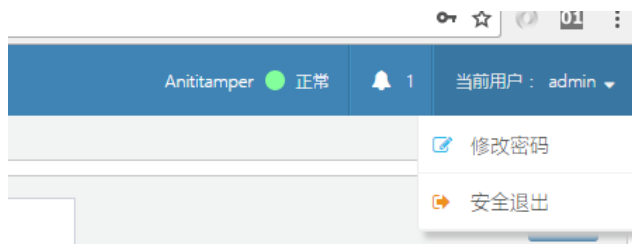
页面顶部右上角显示“许可证状态”、“篡改告警”、“安全防护告警”、“系统告警通知”、“当前登录账户”和按钮。




3. 许可证状态有四种：无许可证、正常、剩余 x 天、过期 x 天。
4. 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）。
5. 安全防护告警，提示当前的所有安全防护告警数量，点击【安全防护告警】，打开安全防护告警列表（列表内容详见 3.3 章节）。
6. 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。

系统告警						
Web服务器	全部	Web服务器IP	时间范围	开始时间	至	结束时间
✓	1	aaa	192.168.1.7	连接客户端aaa模块失败	2018-03-12 13:49:02	否
✓	2	aaa	192.168.1.7	连接客户端aaa失败	2018-03-12 13:48:50	否
✓	3	Test1	192.168.1.115	连接客户端Test1失败	2018-03-12 05:16:10	是
✓	4	Test	192.168.1.107	连接客户端Test失败	2018-03-11 18:05:58	是
✓	5	Test1	192.168.1.115	连接客户端Test1模块失败	2018-03-11 17:47:09	是
✓	6	Test	192.168.1.107	连接客户端Test模块失败	2018-03-11 17:36:16	是
✓	7	Test1	192.168.1.115	连接客户端Test1失败	2018-03-11 05:16:06	是
✓	8	Test	192.168.1.107	连接客户端Test失败	2018-03-10 18:05:55	是
✓	9	Test1	192.168.1.115	连接客户端Test1模块失败	2018-03-10 17:47:02	是
✓	10	Test	192.168.1.107	连接客户端Test模块失败	2018-03-10 17:36:10	是
✓	11	Test1	192.168.1.115	连接客户端Test1失败	2018-03-10 05:16:01	是
✓	12	Test	192.168.1.107	连接客户端Test失败	2018-03-09 18:05:53	是
✓	13	Test1	192.168.1.115	连接客户端Test1模块失败	2018-03-09 17:46:58	是
✓	14	Test	192.168.1.107	连接客户端Test模块失败	2018-03-09 17:36:07	是

- 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。
7. 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”。

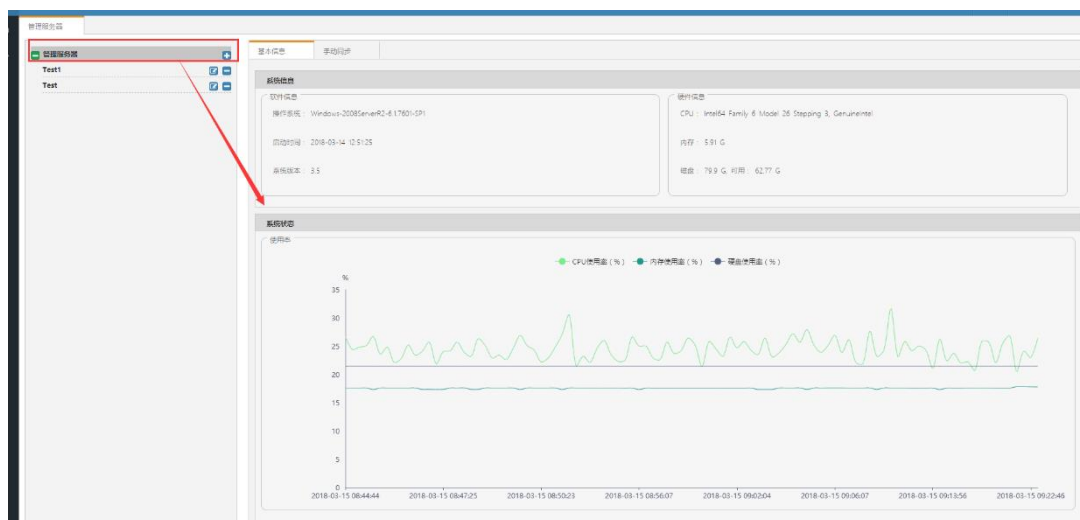


- a) 点击【修改密码】，可修改当前登录账户的密码。

- b) 点击【安全退出】，系统退出到登录页面。
8. 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。

4.4.2 管理服务器

管理服务器默认展示当前发布服务器的基本信息。左侧以树形显示所有“管理服务器”，点击根节点右侧显示发布服务器的“基本信息”和“手动同步”页卡。



4.4.2.1 基本信息

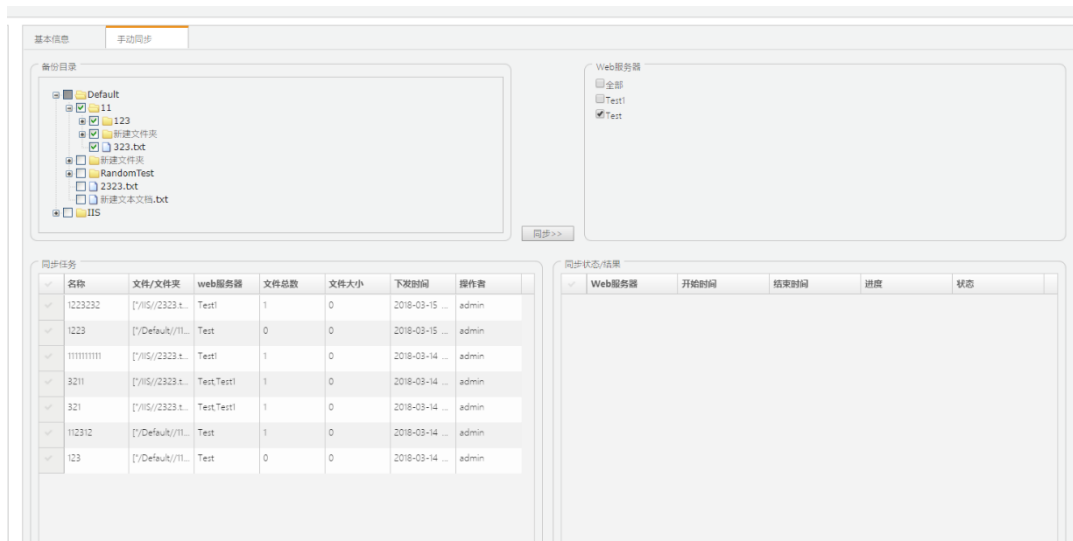
基本信息页面，显示所选中的服务器的“系统信息”和“系统状态”，系统状态为实时的 CPU、内存和磁盘使用率曲线。基本信息能够实时采集到数据的前提是：所采集的服务器上 Monitor 服务已开启（windows）。

名称	描述	状态
 AntitamperMonitorService - Monitor Service...		已启动

4.4.2.2 手动同步

手动同步和自动同步不可同时使用，默认开启自动同步功能。

当发布服务器配置文件未设置自动同步时（即配置文件 `publish_server.conf` 中“`auto_sync=false`”），可以通过 UI 中手动同步功能，将备份目录的文件同步到被保护的服务器中。



1. 在“备份目录”中选择需要同步的目录，并在右侧勾选“web 服务器”后，点击【同步】按钮后，输入同步任务名称并确认后，就开始执行同步任务。

2. “同步任务”表格中显示同步的历史任务，勾选一条历史同步任务右侧“同步状态/结果”中展示该任务的进度和结果。

同步状态/结果：完成、未知

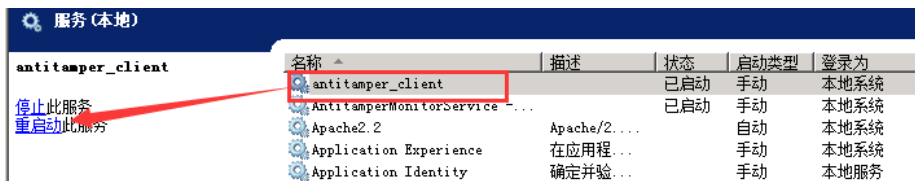
1. 自动识别客户端

当客户端启动并正确配置了 `etc/antitamper_client_windows (linux).conf`，可以在管理服务器模块下看到相应的客户端。

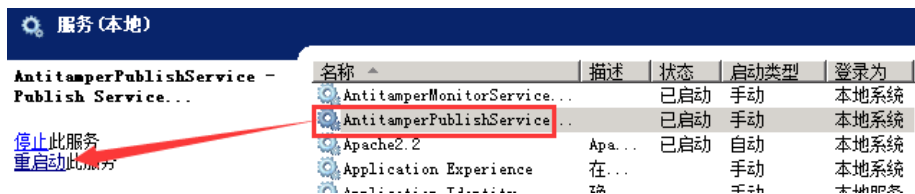
```

antitamper_client_windows.conf
1 Daemon false
2 OS "Windows 2008R2"
3 IP 192.168.1.122
4 ClientName Test 对应UI中"Web服务器名称"
5 PID "c:\\tamper_client\\tmp\\antitamper_client.pid"
6 KeepAliveInterval 60
7
8 Log.Level Notice
9 Log.Dir "c:\\tamper_client\\log"
10 Log.Count 5
11
12 MongoDB.Host 192.168.1.115
13 MongoDB.Port 27017
14 MongoDB.Database tamper
15 MongoDB.Username admin
16 MongoDB.Password 123456
17 MongoDB.Max 4
18 MongoDB.Keep 2
19 MongoDB.SSL false
20 MongoDB.Timeout 15
21 MongoDB.MD5MaxSize 10485760 Web站点信息
22
23 Web.Name "Default"
24 Web.DocRoot "C:/www"
25 Web.TmpFile "c:\\tamper_client\\tmp\\antitamper.tmp"
26 Web.SoftwareVersion "httpd 2.2.25"
27 Web.DBMType sqlite3
28 Web.DBMFile c:\\tamper_client\\etc\\finger_print.db
29 Web.Ignore *.log
30
31 FTP.Url 192.168.1.115
32 FTP.Port 2021
33 FTP.Url2 localhost
34 FTP.Port2 2022
    
```



以上客户端或服务端配置文件修改之后，重启对应服务后，已配置的 Web 服务器“Test”就会添加到“管理服务器”中，UI 中可见。

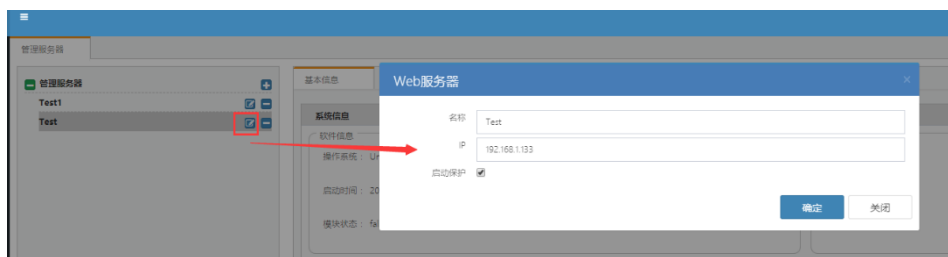


客户端服务




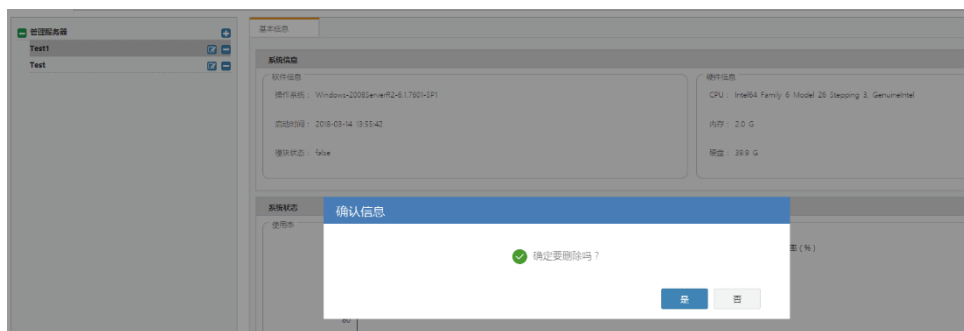
2. 编辑服务器信息

Web 服务器名称后，点击  按钮，可对该 Web 服务器信息进行编辑，自动添加的 Web 服务器需要打开编辑界面手动添加“IP”。



3. 删除服务器

Web 服务器名称后，点击  按钮，可对该 Web 服务器信息进行删除。



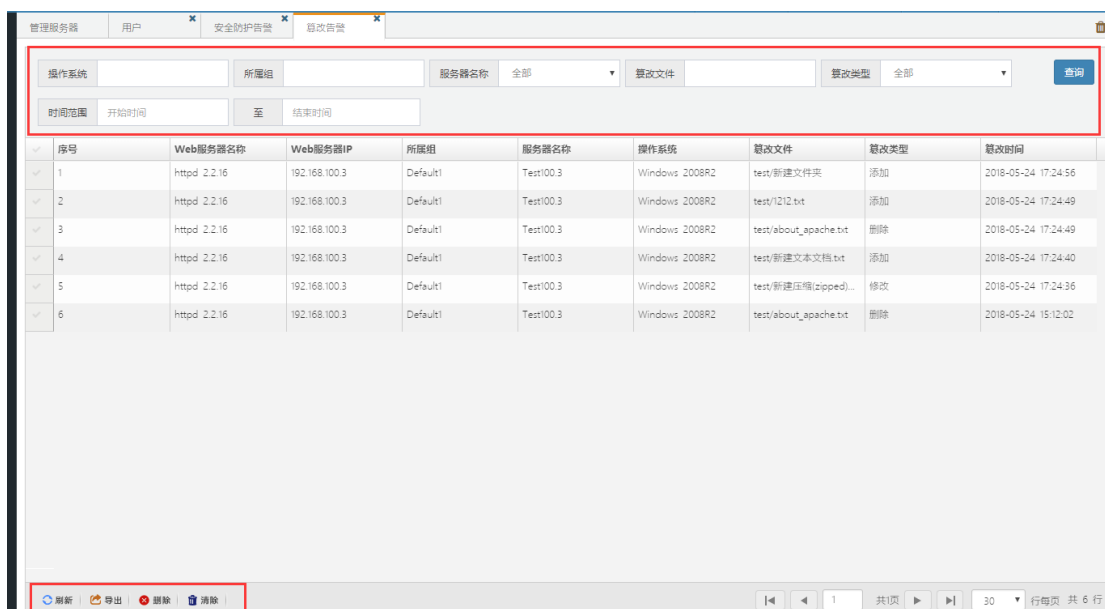
4.5 篡改防护

4.5.1 篡改告警

路径：“篡改防护->篡改告警”。

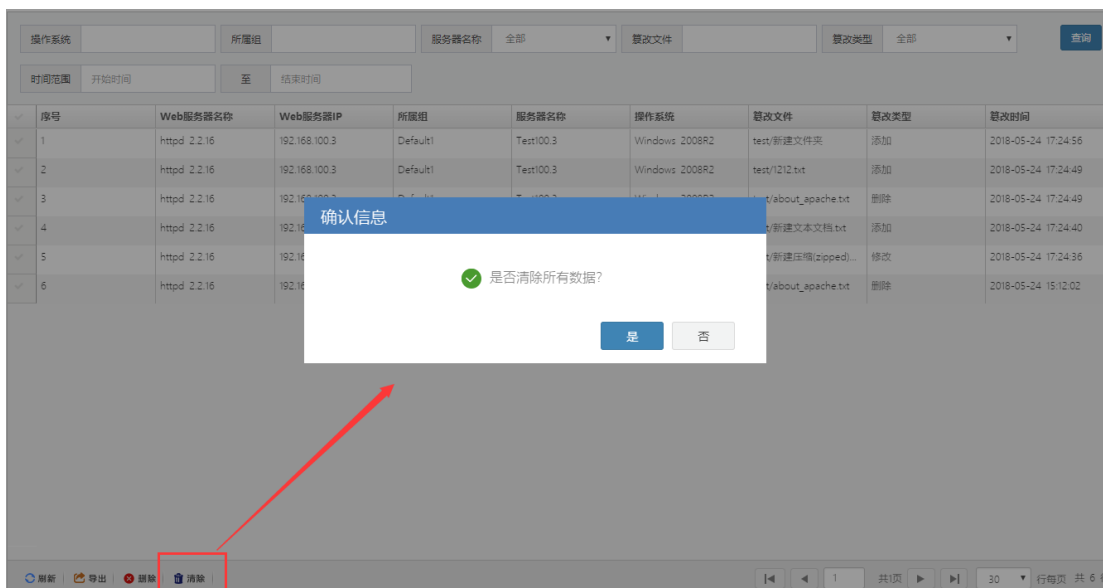


当被保护的 Web 站点的文件或目录被修改后，系统会发出告警信息，并将篡改的文件或目录进行自动恢复。如下图所示，篡改类型包括添加、修改和删。



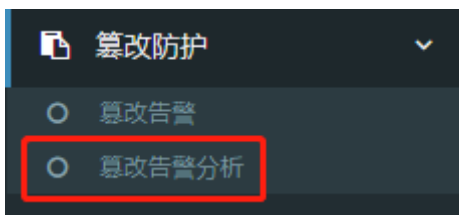
序号	Web服务器名称	Web服务器IP	所属组	服务器名称	操作系统	篡改文件	篡改类型	篡改时间
1	httpd 2.2.16	192.168.100.3	Default1	Test100.3	Windows 2008R2	test/新建文件夹	添加	2018-05-24 17:24:56
2	httpd 2.2.16	192.168.100.3	Default1	Test100.3	Windows 2008R2	test/1212.txt	添加	2018-05-24 17:24:49
3	httpd 2.2.16	192.168.100.3	Default1	Test100.3	Windows 2008R2	test/about_apache.txt	删除	2018-05-24 17:24:49
4	httpd 2.2.16	192.168.100.3	Default1	Test100.3	Windows 2008R2	test/新建文本文档.txt	添加	2018-05-24 17:24:40
5	httpd 2.2.16	192.168.100.3	Default1	Test100.3	Windows 2008R2	test/新建压缩(zippe)...	修改	2018-05-24 17:24:36
6	httpd 2.2.16	192.168.100.3	Default1	Test100.3	Windows 2008R2	test/about_apache.txt	删除	2018-05-24 15:12:02

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。

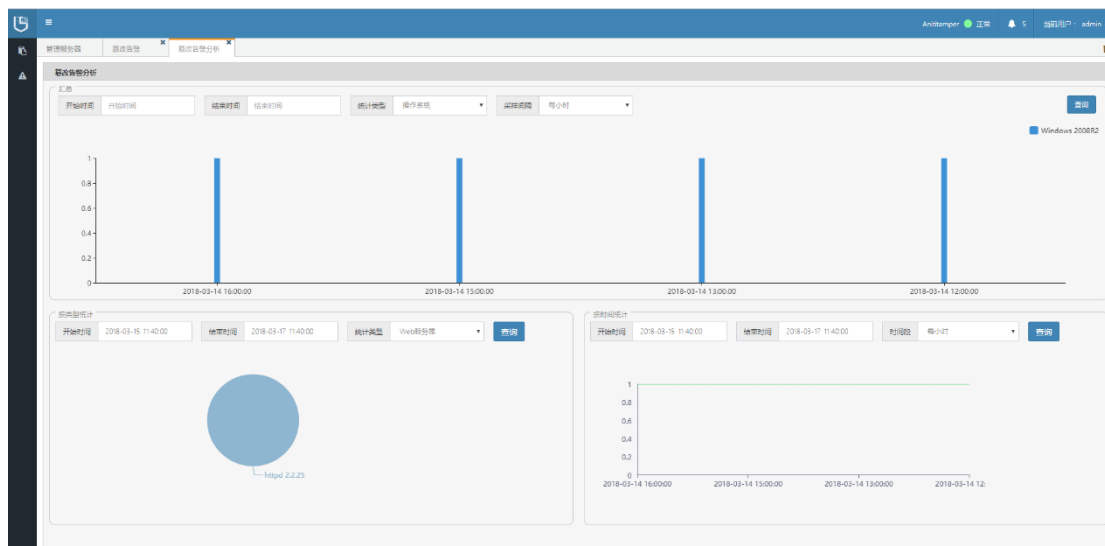


4.5.2 篡改告警分析

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。



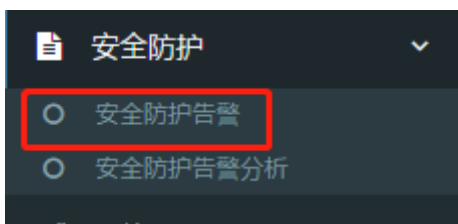
1. “汇总”统计为柱形图，可根据时间范围、统计类型（操作系统、Web 服务器、服务器）和采集时间间隔（每小时、每天、每周、每月）进行筛选统计。

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。

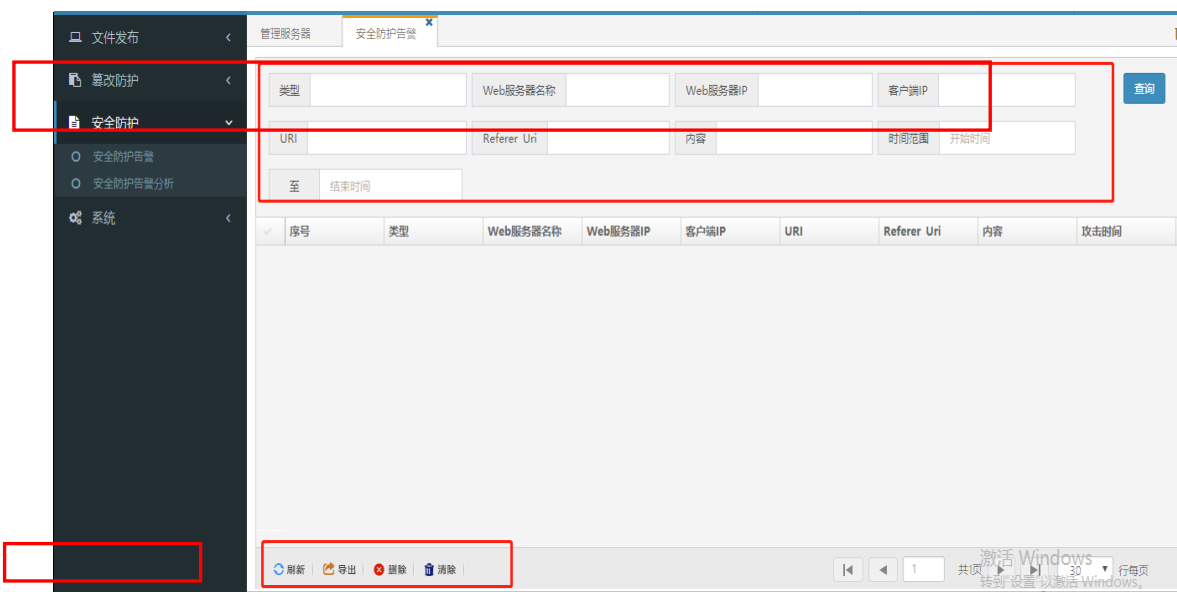
4.6 安全防护

4.6.1 安全防护告警

路径：“安全防护->安全防护告警”。



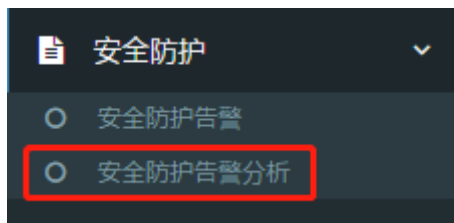
安全防护告警包含 SQL 注入告警、XSS 跨站攻击、盗链告警及 D0S 攻击的告警。启用安全防护功能需要在被保护站点 web 服务器中配置 modsecurity 模块。



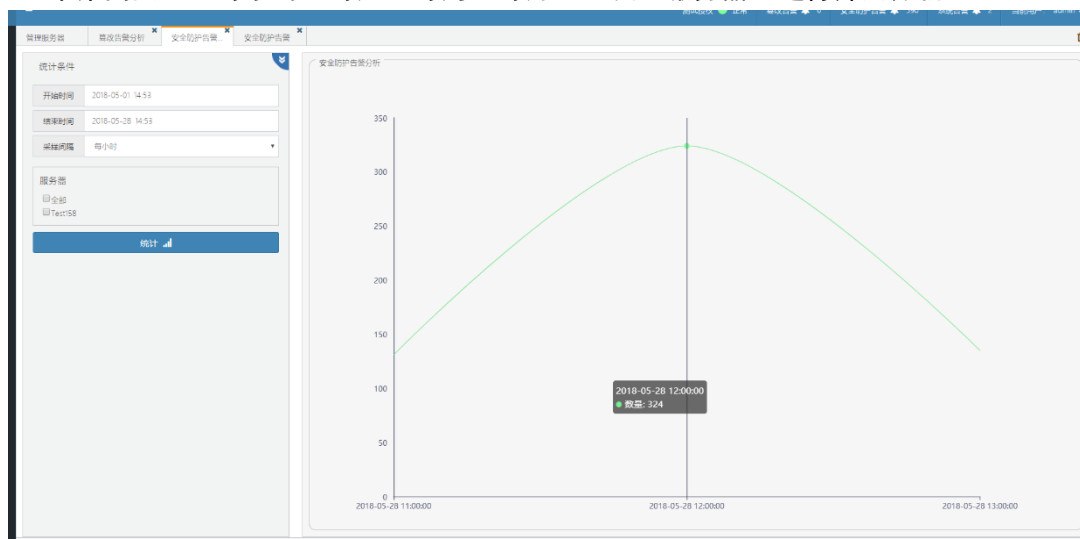
1. 如图所示，列表有查询功能，可通过“类型”、“Web 服务器名称”、“Web 服务器 IP”、“客户端 IP”、“URI”、“Referer Uri”、“内容”、“时间范围”等筛选条件对“安全防护告警记录”进行查询。
2. 通过【导出】按钮可将当前列表中显示“安全防护告警记录”导出到 csv 格式文件。通过【删除】按钮可勾选数据进行删除；通过【清除】按钮，可将“安全防护告警记录”全部清除。

4.6.2 安全防护告警分析

路径：“安全防护->安全防护告警分析”。



安全防护告警分析，对安全告警历史的分析，并以图表形式展示。如下图所示，可根据“开始、结束时间”、“采集间隔”（每小时、每天、每周、每月）、及“服务器”进行筛选分析。

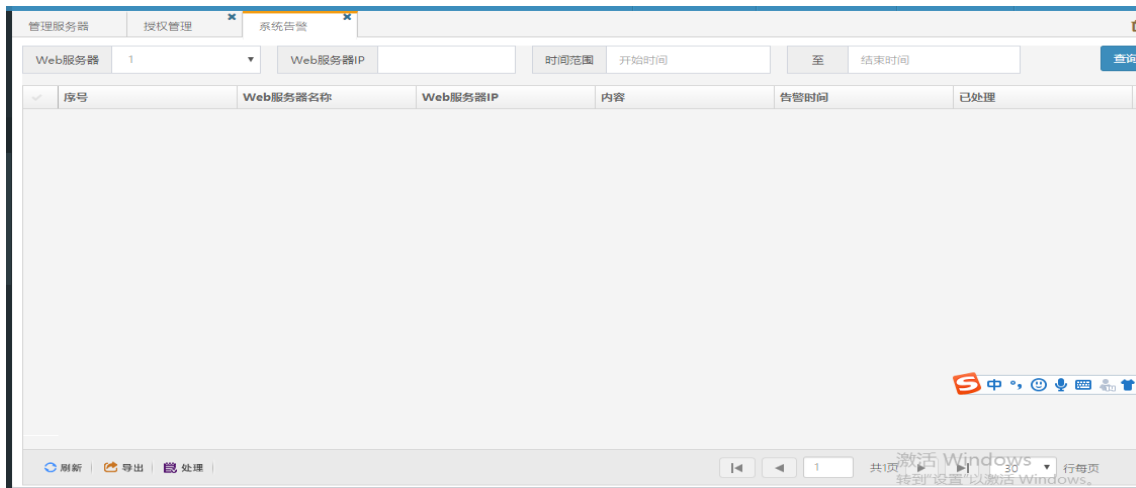


4.7 系统

4.7.1 系统告警

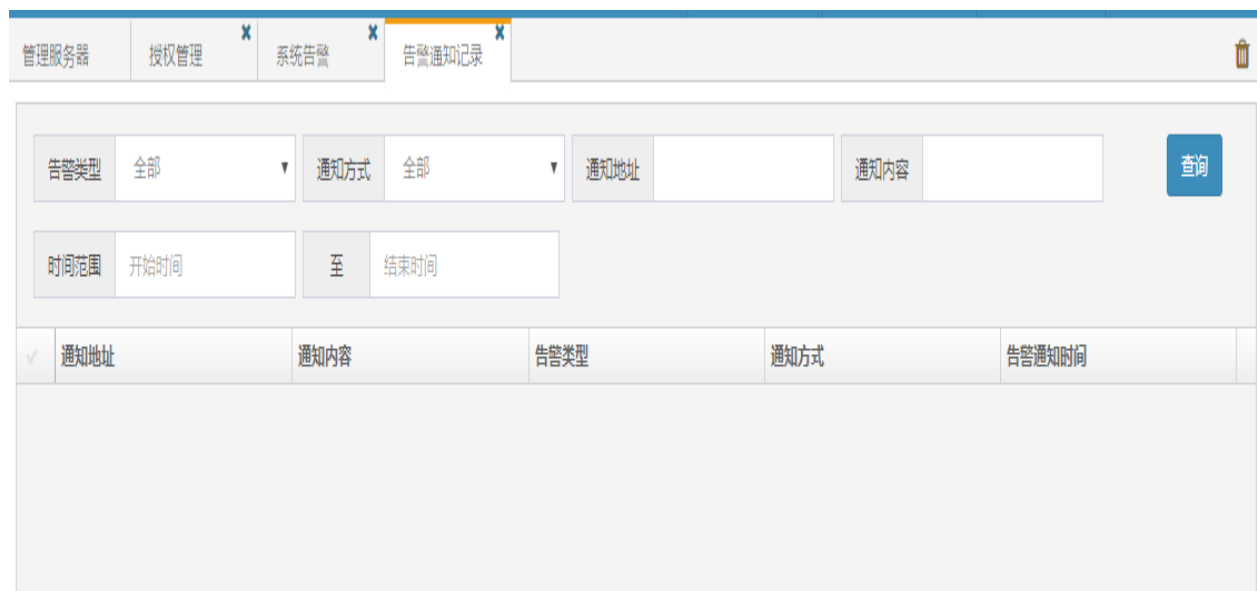
路径：“系统->系统告警”





4.7.2 告警通知记录

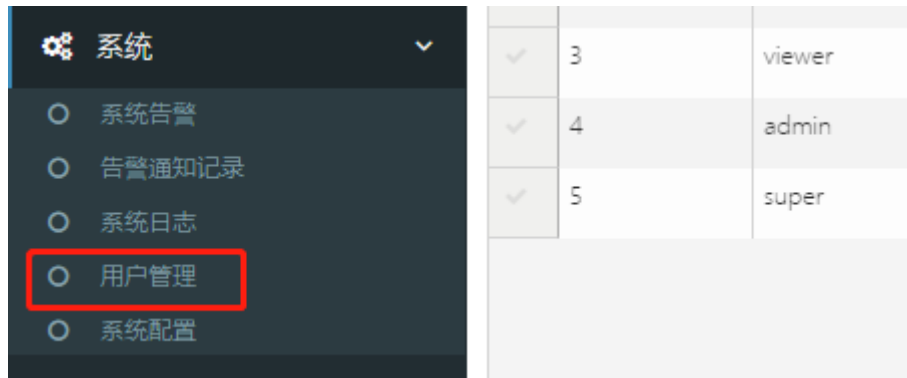
路径：“系统->系统告警”



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。

4.7.3 用户管理

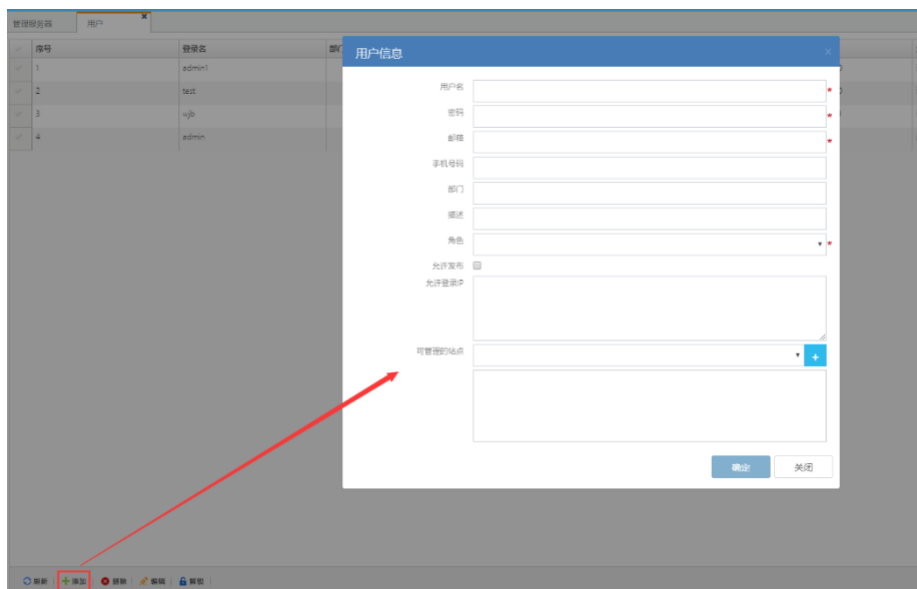
路径：“系统->用户管理”。



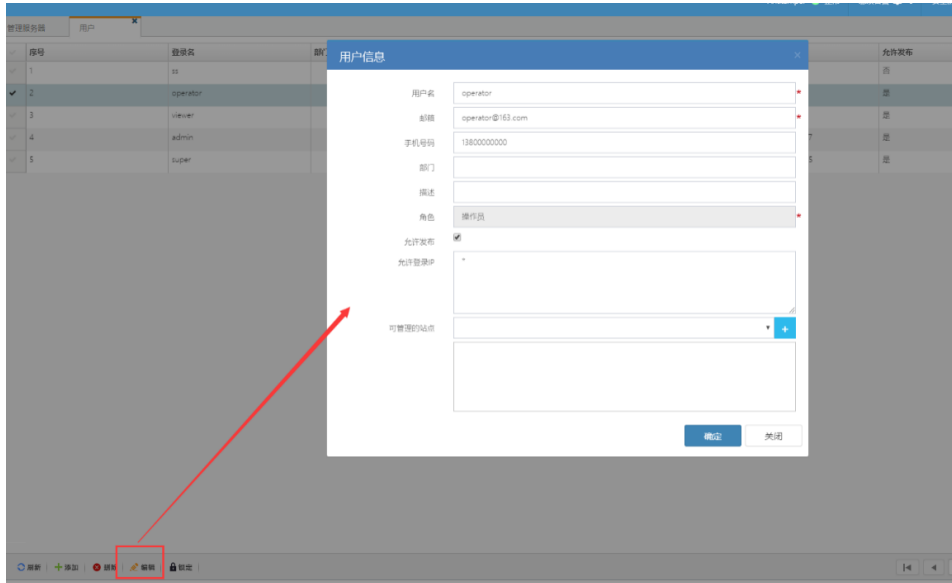
1. 管理员用户 admin 登录，可见所有用户信息，并可以进行添加、修改、删除、解锁等操作。

✓	序号	登录名	部门	Email	角色	上次登录时间	用户有效期	密码有效期	允许发布	是否锁定	操作
✓	1	adm		1357844001@...	管理员	2018-09-03 1...			否	未	
✓	2	operator		operator@163...	操作员				是	未	
✓	3	viewer		viewer@163.c...	审查员				是	未	
✓	4	admin		antitamper@1...	管理员	2018-09-04 1...			是	未	
✓	5	super		super@163.cn	超级管理员	2018-09-04 1			是	未	

- 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】。

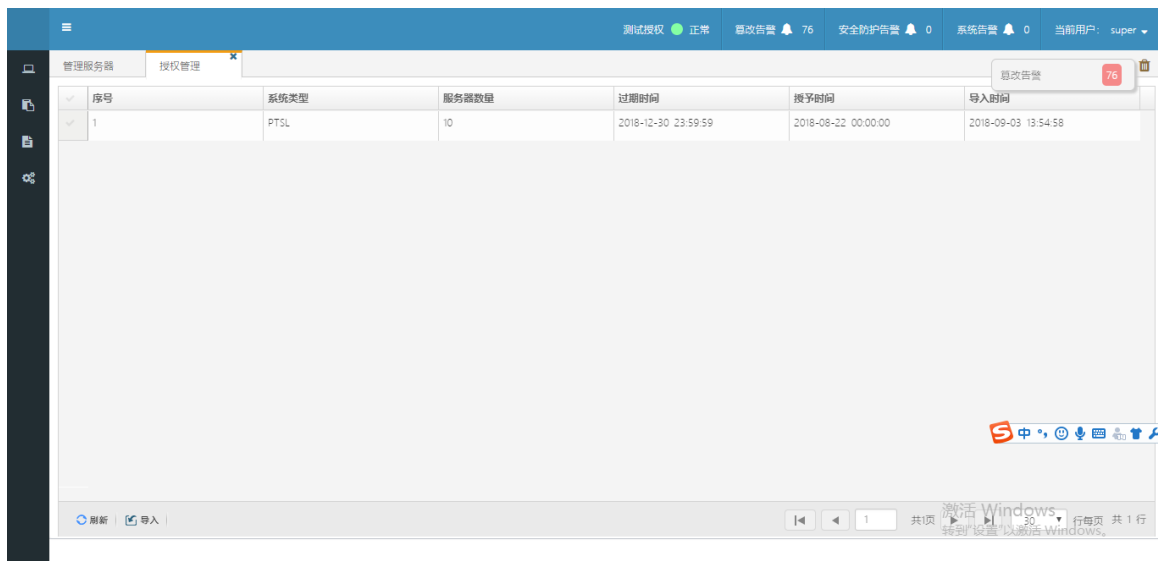
序号	登录名	部门	Email	角色	上次登录时间	允许发布	是否锁定
1	admin1		1213@12.com	Viewer	1970-01-02 00:00:00	否	否
2	test		yujinghuan@sina.cn	Operator	1970-01-02 00:00:00	否	否
3	wjb		12321@126.com	Operator	2018-03-16 17:04:49	否	是
4	admin		ambtamper@163.com	Administrator	2018-03-16 17:13:20	是	否

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。

4.7.4 授权管理

路径：“系统->授权管理”。

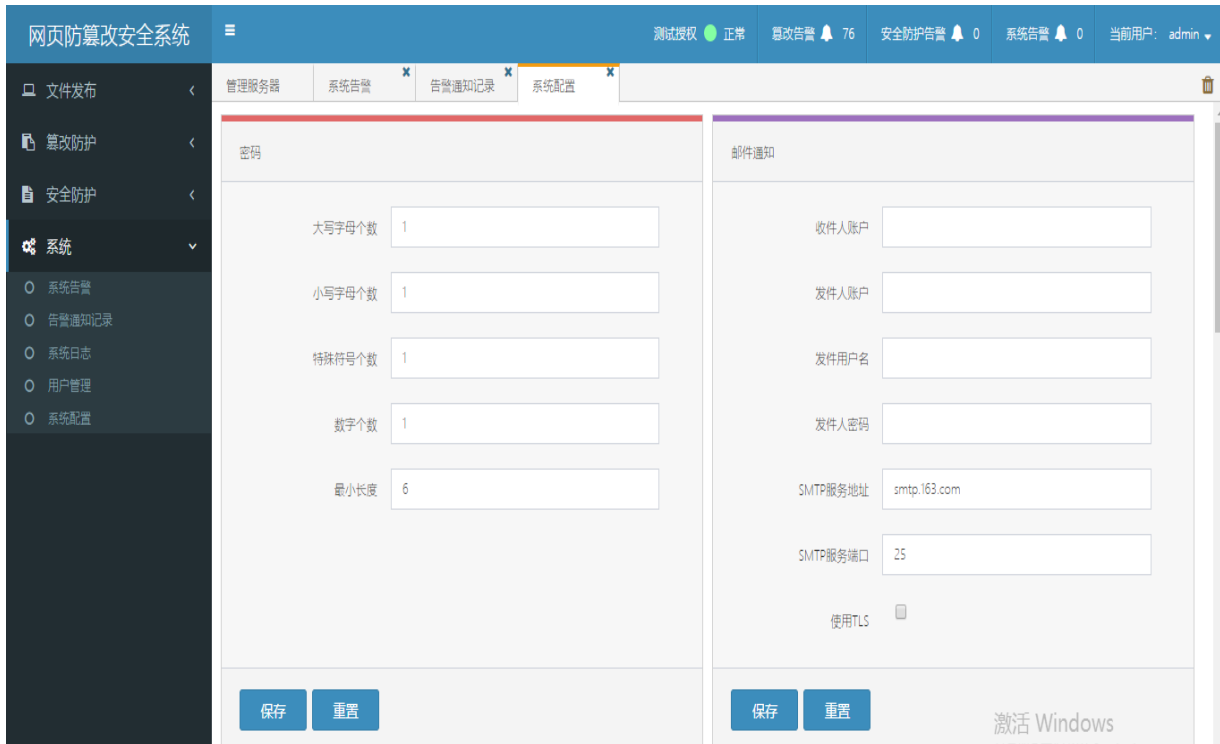
“授权管理”以列表形式展示系统许可证更新的历史记录，授权历史信息为只读不可编辑或删除。



4.7.5 系统配置

路径：“系统->系统配置”，仅管理员账户 super/admin 可见。

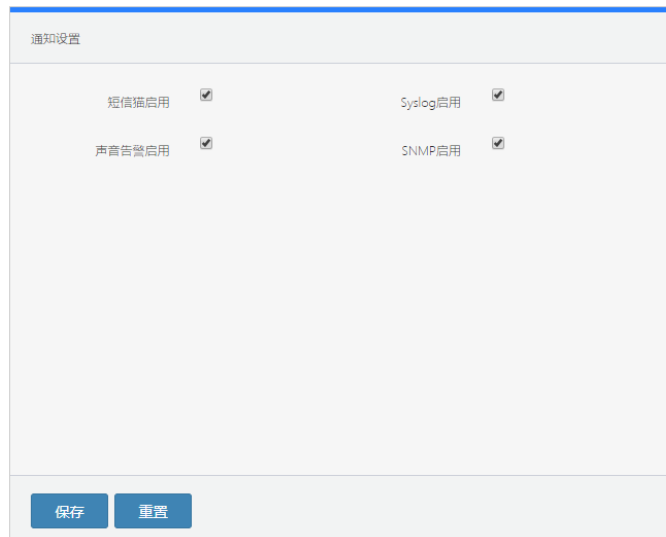
系统配置包括四个部分：系统登录“密码”格式的配置、“邮件通知”的配置、系统“许可证”更新、还有“其他配置”和“通知设置”，如下图所示，图中系统配置为初始化状态。



The screenshot shows the 'System Configuration' page with two main sections:

- 密码 (Password):**
 - 大写字母个数: 1
 - 小写字母个数: 1
 - 特殊符号个数: 1
 - 数字个数: 1
 - 最小长度: 6
- 邮件通知 (Email Notification):**
 - 收件人账户: [Empty]
 - 发件人账户: [Empty]
 - 发件用户名: [Empty]
 - 发件人密码: [Empty]
 - SMTP服务地址: smtp.163.com
 - SMTP服务端口: 25
 - 使用TLS:

Buttons for '保存' (Save) and '重置' (Reset) are present at the bottom of each section.



The screenshot shows the 'Notification Settings' page with the following options:

- 短信猫启用:
- Syslog启用:
- 声音告警启用:
- SNMP启用:

Buttons for '保存' (Save) and '重置' (Reset) are at the bottom.

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“短信猫启用”、“Syslog 启用”、“声音告警启用”和“SNMP 启用”，其中“短信猫启用”的配置细节如下图：~~



~~“Syslog 配置”如下图：~~



Svslog配置

类型: 远程日志

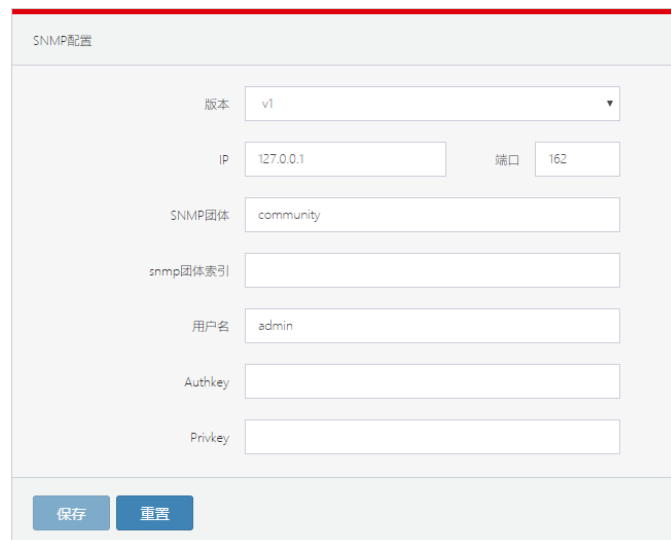
加密方式: MD5

主日志服务器IP: 127.0.0.1

备份日志服务器IP: 127.0.0.1

保存 重置

“SNMP 配置” 如下图:



SNMP配置

版本: v1

IP: 127.0.0.1 端口: 162

SNMP团体: community

snmp团体索引:

用户名: admin

Authkey:

Privkey:

保存 重置

4.7.6 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。

级别	全部	时间范围	开始时间	至	结束时间	查询
名称	描述	用户名	IP	级别	操作时间	
✓ 用户登录	用户 admin 登录	admin	106.39.10.162	Info	2018-09-04 13:24:07	
✓ 用户被锁定	用户 adm 尝试登录失败	"System"	106.39.10.162	Warning	2018-09-04 13:23:10	
✓ 用户退出	用户 super退出	super	106.39.10.162	Info	2018-09-04 13:21:43	
✓ 用户登录	用户 super 登录	super	106.39.10.162	Info	2018-09-04 13:16:45	
✓ 新增站点	服务器 1 下新增站点	adm	36.111.88.33	Info	2018-09-03 17:19:23	
✓ 添加服务器	添加服务器 1	adm	36.111.88.33	Info	2018-09-03 17:13:39	
✓ 删除站点	服务器 centos7.0 下删除站点	adm	36.111.88.33	Info	2018-09-03 17:13:16	
✓ 用户登录	用户 adm 登录	adm	36.111.88.33	Info	2018-09-03 17:11:22	
✓ 用户退出	用户 super退出	super	36.111.88.33	Info	2018-09-03 17:11:00	
✓ 添加用户	添加用户 adm Administrator	super	36.111.88.33	Info	2018-09-03 17:10:53	
✓ 用户登录	用户 super 登录	super	36.111.88.33	Info	2018-09-03 17:08:41	

4.8 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 8010、8011、60001—600010 端口→对服务端开放

4.9 网页防篡改卸载

4.9.1 Client 端卸载

4.9.1.1 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。



4.9.1.2 Linux 版本

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

执行安装目录下面的 `uninstall.sh` 脚本：

```
[root@localhost antitamper_client_v4.3.2_centos_redhat_20180808]# cd /opt/tamper_client/  
[root@localhost tamper_client]# ./uninstall.sh  
start uninstall client  
end uninstall client  
[root@localhost tamper_client]#
```

5 常见问题

5.1 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？

答：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 8010、8011、60001—600010 端口→对服务端开放

5.2 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？

答：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；

5.3 上传网页文件时，出现无法更新的情况该如何处理？

答：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。

5.4 保护站点的有些目录不需要监控，如何设置？

答：可在服务端的管理页面设置忽略文件/目录

忽略文件/目录



注：忽略目录以 /* 结尾 (例: tmp/*)，忽略扩展名以 *. 结尾 (例: *.exe)

5.5 网页防篡改的整体架构是什么？

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。

5.6 如何修改网页防篡改 web 管理界面使用的端口？

1、使用记事本修改 httpd-ssl.conf 文件中监听的端口，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
```

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

