深圳市惠尔顿文档系列

军工保密资格
互联网接入
设置指南

深圳市惠尔顿信息技术有限公司
Shenzhen Wholeton Information Technology Co., Ltd.

深圳市惠尔顿技术部/编

目录

前言

为帮助做军工保密相关项目的用户了解网络安全审计设备相关的设置，我们编写了《深圳市惠尔顿军工保密资格互联网接入设置指南》。

本指南分为十个部分：

第一部分为快速连接设备，主要介绍了连接设备要做的一些事情；

第二部分为设备激活，主要介绍了设备如何激活；

第三部分为网络配置设置，主要介绍了设备最常用到的一种接入模式的配置的方法以及连接到网络中连线方式；

第四部分为认证设置，主要介绍了建立互联网接入终端审批和登记制度的一些设置方法和功能以及要做的认证策略等；

第五部分为策略管理，主要介绍了应用层策略中最常用的两种管控，网页管控和邮件管控的设置策略情况；

第六部分为系统管理，主要介绍系统三员管理的设置以及重启设备和恢复默认设置的情况；

第七部分为数据中心，主要介绍的是数据的导出和历史台账记录情况。

第八部分为网络培训，主要介绍的是惠尔顿提供的网络培训事项。

第九部分为保密检查注意事项，主要介绍的是保密检查等相关注意事项。

第十部分为售后服务，主要介绍的是产品售后维修事项。

本指南与国家的军工保密资质认证过证密切相关，希望各位用户认真阅读，祝各位用户企业发展更好更快。

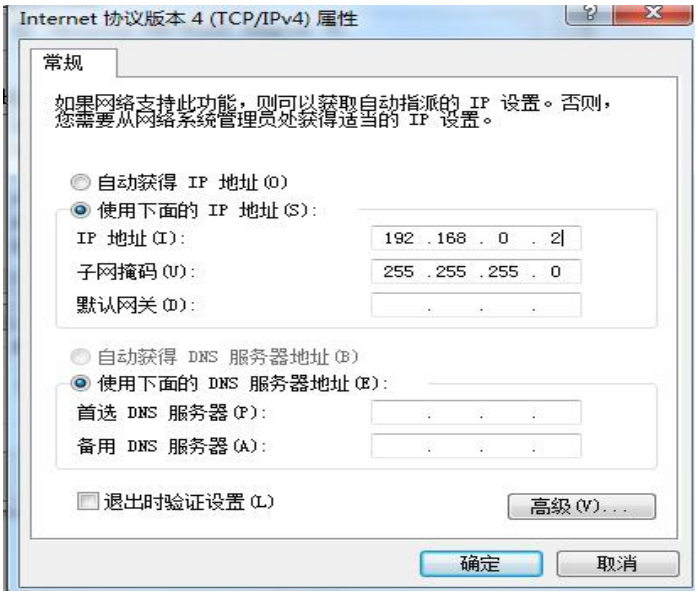
备注说明：军工保密资质认证互联网接入评定，1 未建立互联网接入终端审批和登记制度，或者未设置管理员的，1 分；2 单位在一地的互联网接入口多于 2 个，或者对接入口未采取符合规定的防护监管技术措施的，2 分；3 未采取管理和技术措施对互联网上网行为进行监控审计的，2 分。

深圳市惠尔顿信息技术有限公司

2024 年 10 月

一 快速连接设备

设备界面登陆方式：http://192.168.0.254（将电脑网线连接设备 eth1 口，电脑 IP 设置成 192.168.0.0/24 网段 IP，例如 192.168.0.2）



备注：设备 ip 忘记了，可用 192.168.192.254 这个 ip 登陆（电脑连接设备 eth1 口，电脑 IP 设置成 192.168.192.2）。

登陆设备管理界面时：建议使用**谷歌浏览器**。

二 设备激活

设备激活采用微信扫码方式，产品使用之前一定要先激活。

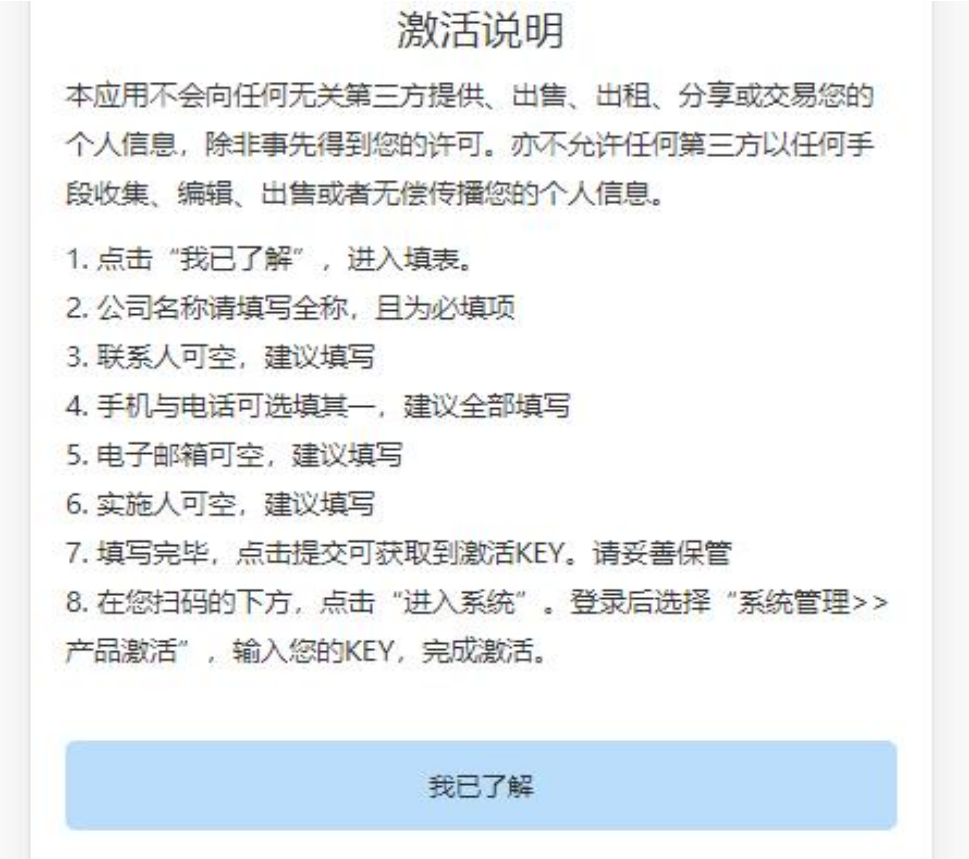
设备激活步骤：

1 激活检测

登陆系统时，系统自动检测是否激活，如未激活会跳转到激活界面，如下图：

2 微信扫码

使用手机微信扫码进入到信息填写页（按照提示操作），如下图：



3 获取激活 key

获取激活 key，如下图：

4 产品激活

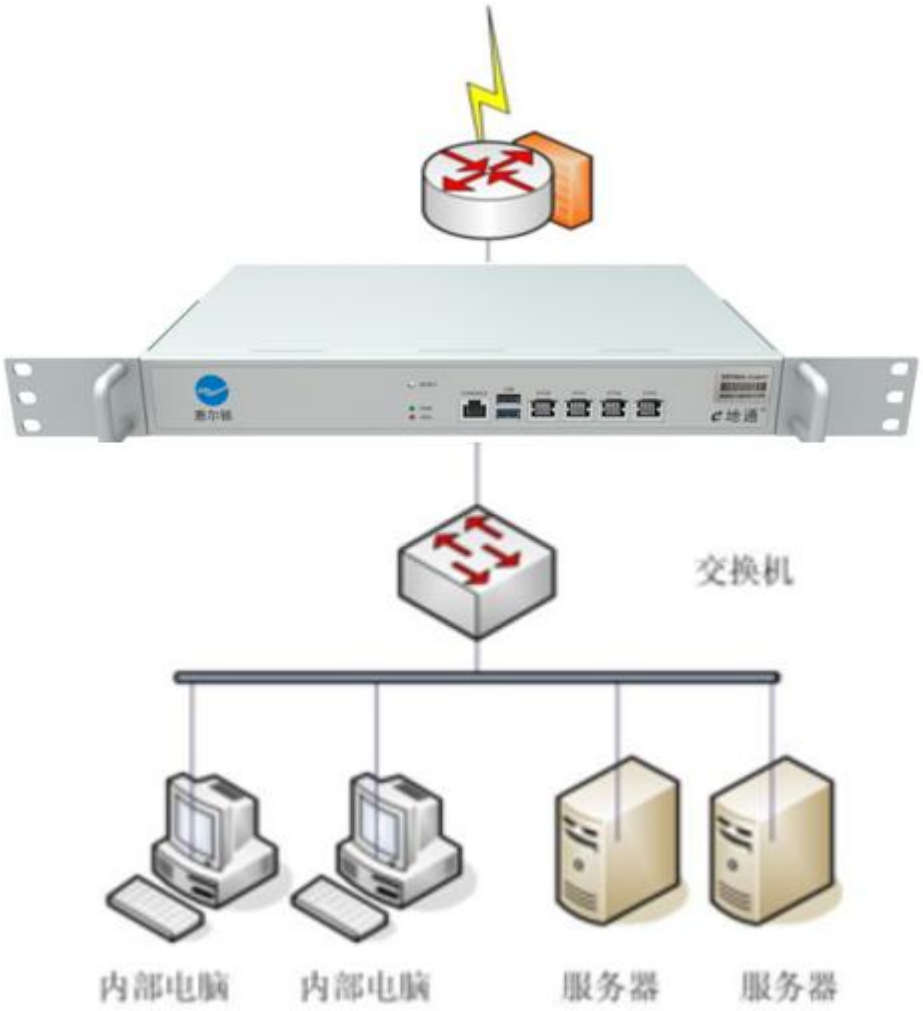
获取到激活 KEY 后，在二维码的下方，点击【进入系统】；默认登陆用户名和密码都是 admin。
导航到【系统管理/产品激活】，在产品密钥那里填上获取的 KEY，如果设备已联网，可以点获取密钥。如下图：

三 网络配置

1 网桥模式

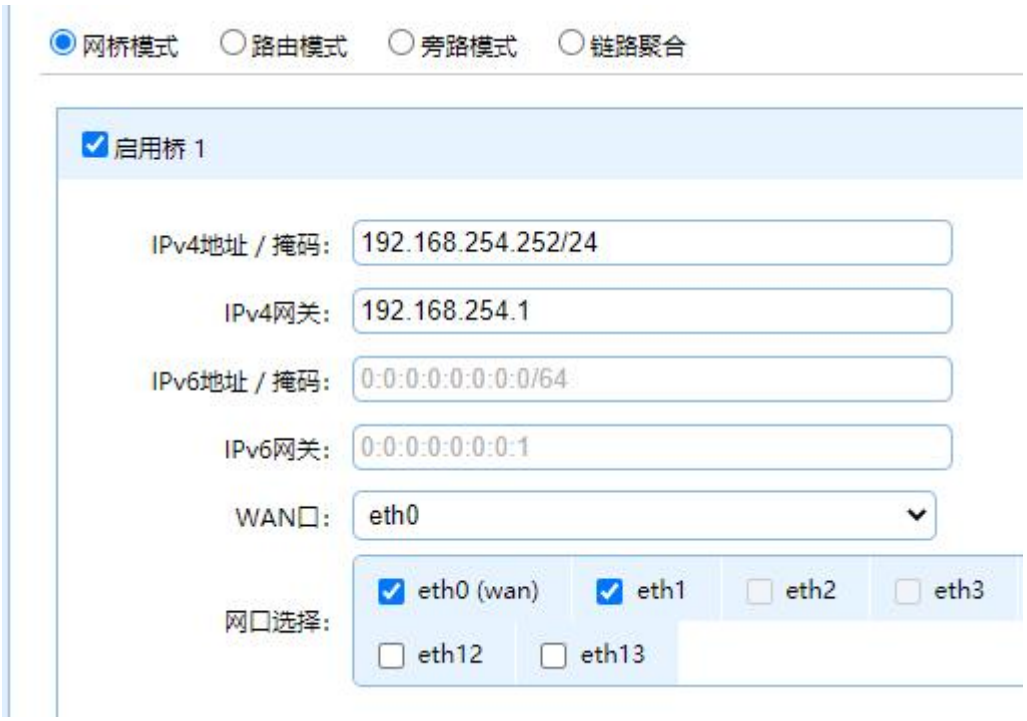
网桥模式是把网络安全审计设备桥接在路由器和交换机之间，以桥模式部署时对网络没有改动，不支持路由转发 、NAT、 DHCP 等功能。

网桥模式的接线顺序：网络安全审计设备的 eth0 口连接路由器的 LAN 口；网络安全审计设备的 eth1 口连接局域网的交换机。部署拓扑模式（如下图）：



配置方法：

导航到【网络配置/接入模式】，如下图：



1、接入模式选择“网桥模式”（eth0 口和 eth1 口为桥 1，eth2 和 eth3 为桥 2）；

2、桥一模式的接线顺序：eth0 口连接路由器的 LAN 口，eth1 口连接局域网的交换机；

3、IP 地址设置和路由器在同一个网段的，并未使用的 IP 地址；

4、默认网关指的是路由器的 IP 地址；

5、单击“保存”，立即生效。

6、 wan 口可选择，桥 1wan 口默认 eth0。

聚合设置如下图：

1、接入模式选择“聚合模式”（eth0 口和 eth1 口为上行口，eth2 和 eth3 为下行口，可调整）；

2、聚合模式的接线顺序：eth0 和 eth1 口连接路由器的聚合口，eth2 和 eth3 口连接交换机的聚合口；

3、聚合口 IP 地址设置和路由器在同一个网段的，并未使用的 IP 地址；

4、默认网关指的是路由器的 IP 地址；

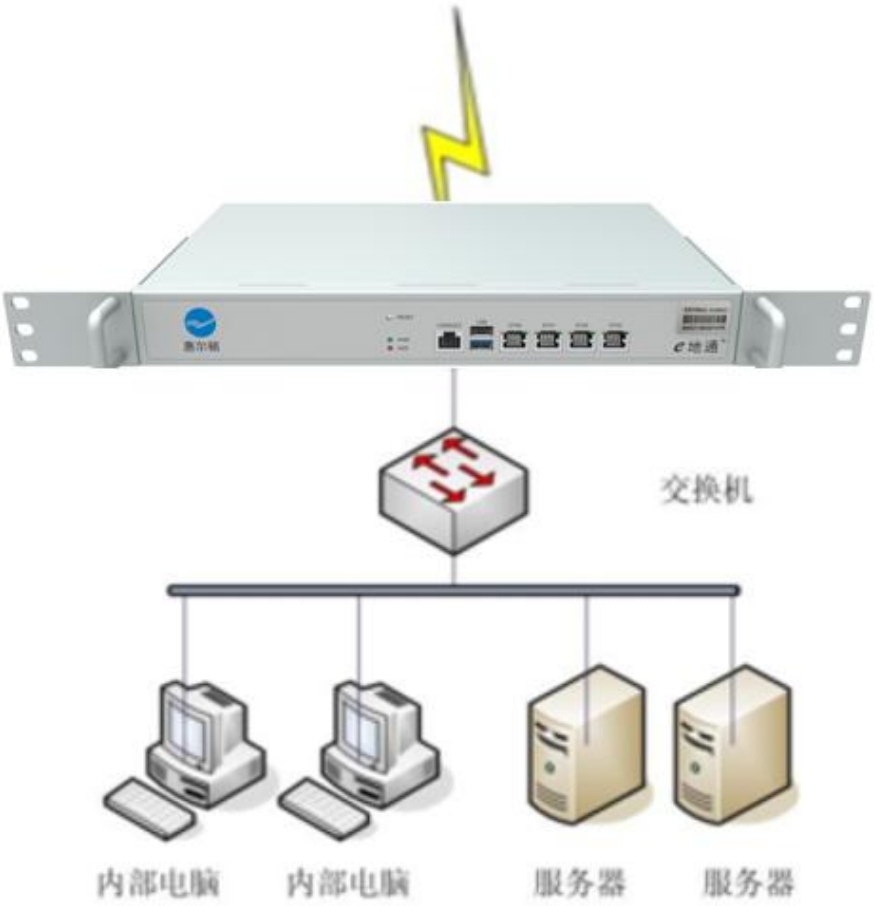
5、单击“保存”，立即生效。

备注：4 网口以上型号设备有管理口设置，路由器和交换机之间是聚合链路需要启用“聚合链路”，模式默认是动态聚合；不是聚合链路，不要启用“聚合链路”，聚合接口可选择调整，默认 eth0 和 eth1 连接上行路由器，eth2 和 eth3 连接下行交换机。

2 路由模式（NAT）

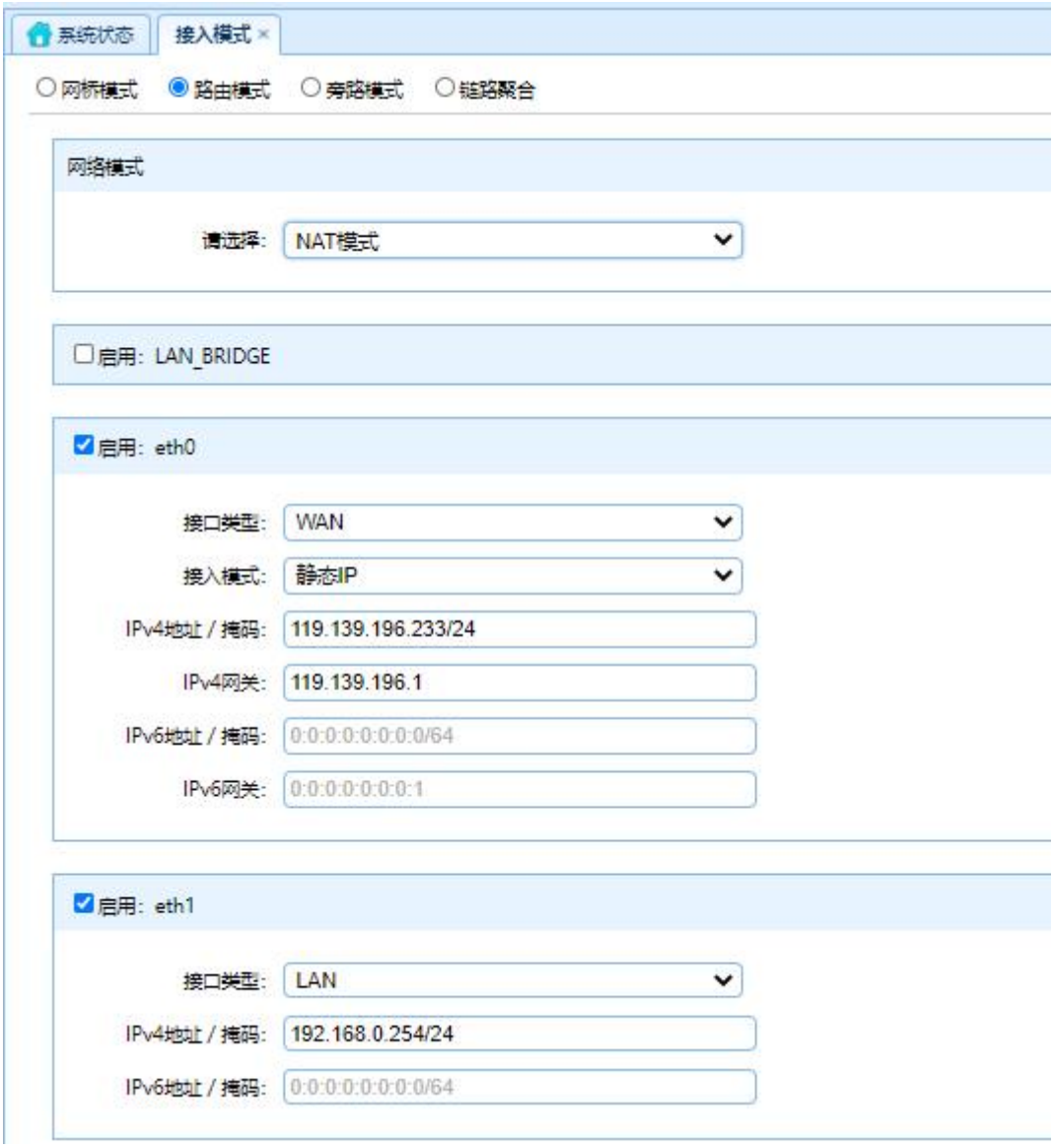
路由模式（NAT）是把网络安全审计设备作为网关使用，放在网关出口，直接连接互联网；

路由模式的接线顺序：网络安全审计设备的 eth0 口连接 modem 或者光纤入口，网络安全审计设备的 eth1 口连接局域网的交换机。部署拓扑模式如下图；



配置方法：

导航到【网络配置/接入模式】，如下图：



1、在接入模式里选择【接入模式】为[路由模式]，【网络模式】里选择[NAT]；

2、【启用接口】里勾选对应要使用的接口，使用 eth0 口接入互联网，eth1 口接局域网；

3、在【接入类型】中根据网络接入方式选择不同的类型[静态 IP]、[PPPOE（ADSL）]或者[自动获取]；

静态 IP：使用运营商分配的 ip 手动设置 IP 地址和默认网关；

PPPOE（ADSL）：使用运营商分配的上网账号和上网密码，拨号上网；

自动获取：从 DHCP 服务器上自动获取 IP 地址；

4、选择完【接入类型】并设置好相应网络参数；

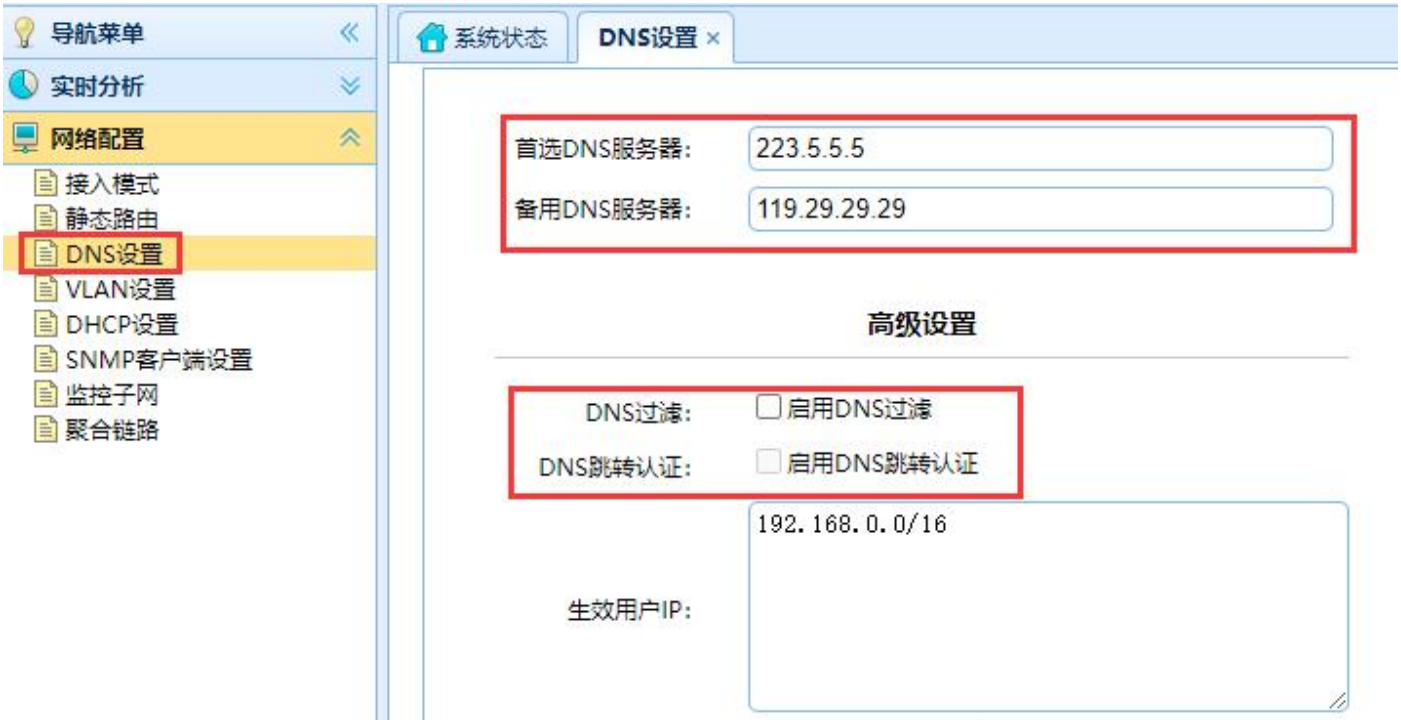
5、单击“保存”，立即生效。

3 DNS 设置

DNS 是指域名服务器（Domain Name Server）。为了能正确的采用域名去访问网页，需要设置正确的 DNS 服务器，为设备和局域网内的计算机能正确的解析域名；可使用系统默认的 DNS 或者按照当地网络运营商 DNS 填写。

配置方法：

导航到【网络配置/DNS 设置】，如下图：



DNS 跳转认证：开启后，打开网页自动跳转到上网认证界面，需要先启用“DNS 过滤”，再启用“DNS 跳转认证”，另外生效用户 ip 填电脑 ip 或者网段。

4 DHCP 设置

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）通常被应用在大型的局域网络环境中，主要作用是集中的管理、分配 IP 地址，使网络环境中的主机动态的获得 IP 地址、Gateway 地址、DNS 服务器地址等信息，并能够提升地址的使用率。

在 NAT 模式和路由模式下可以启用，如果选择了启动 DHCP 服务，那么用户在网络设置时可以选择自动获取 IP 和 DNS。

配置方法：

导航到【网络配置/DHCP 设置】，在【DHCP 设置】界面上点击<DHCP 服务器配置>，如下图：

四 认证配置

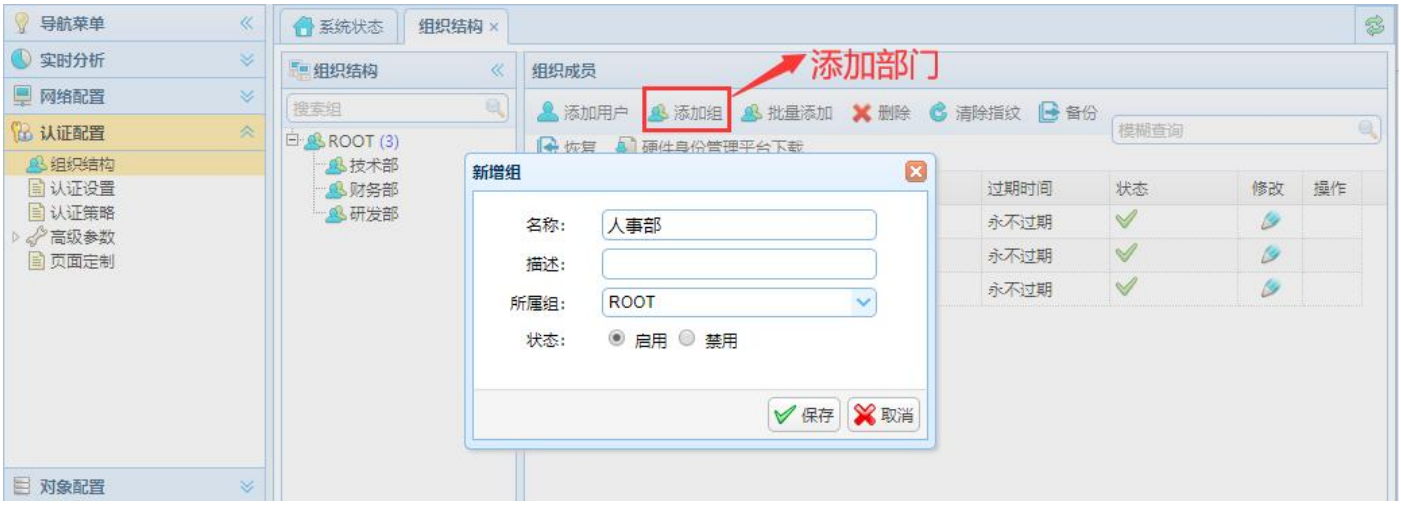
1 组织结构

组织结构将一个企业的上网人员以树状的结构在设备中展示出来，按照部门方式创建，管理员可以灵活构建或者修改组织结构以适应企业的组织结构变化和上网管理的要求。组织结构如下图：

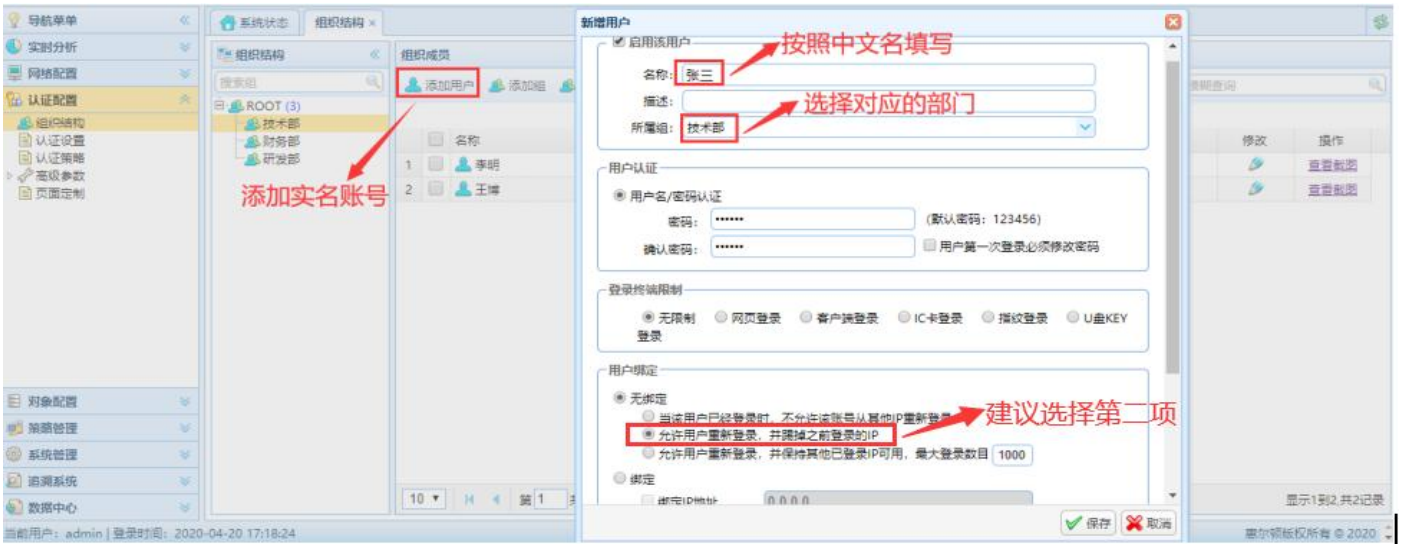
2 添加组和上网用户

配置方法：

导航到【认证配置/组织结构】，如下图：



导航到【认证配置/组织结构】，如下图：



3 配置实名认证上网参数

配置方法：

导航到【认证配置/认证设置】，如下图：

4 配置上网认证策略

配置方法：

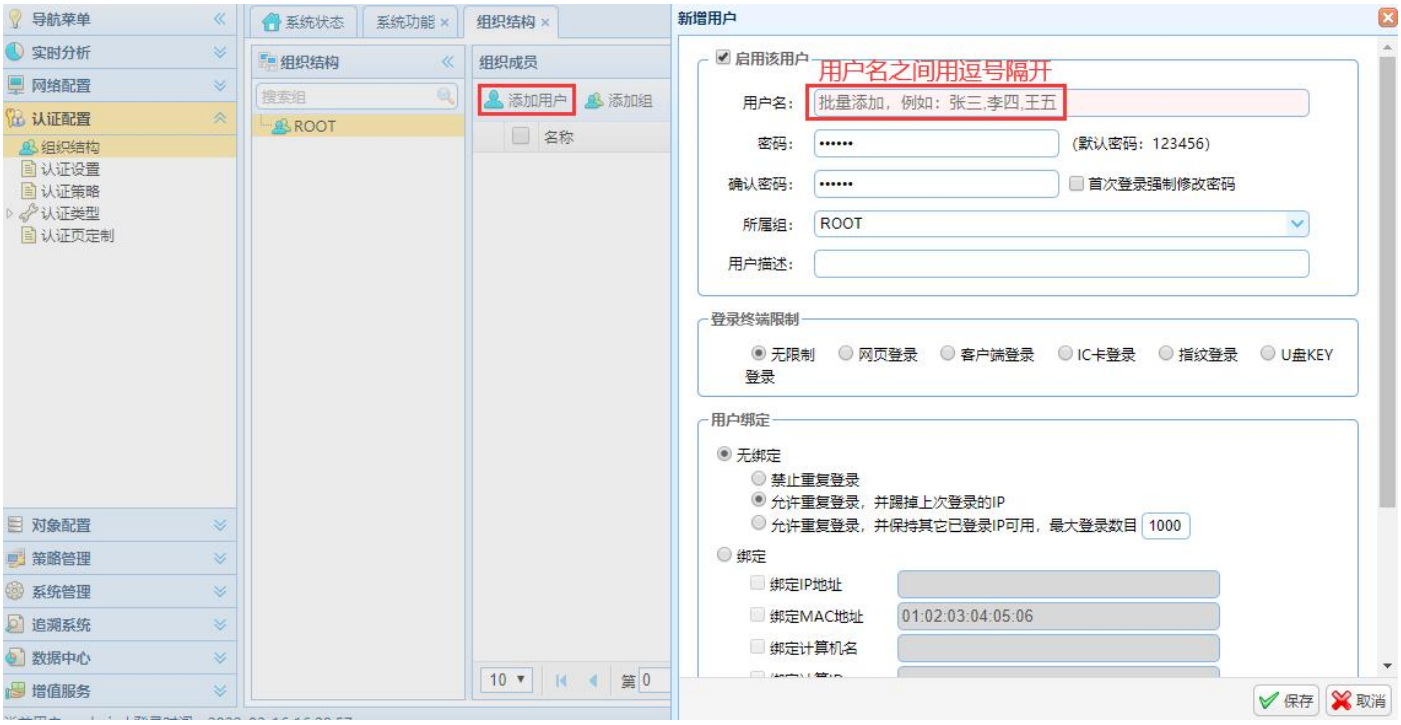
导航到【认证配置/认证策略】，如下图：

5 批量添加

功能：添加大批量用户。

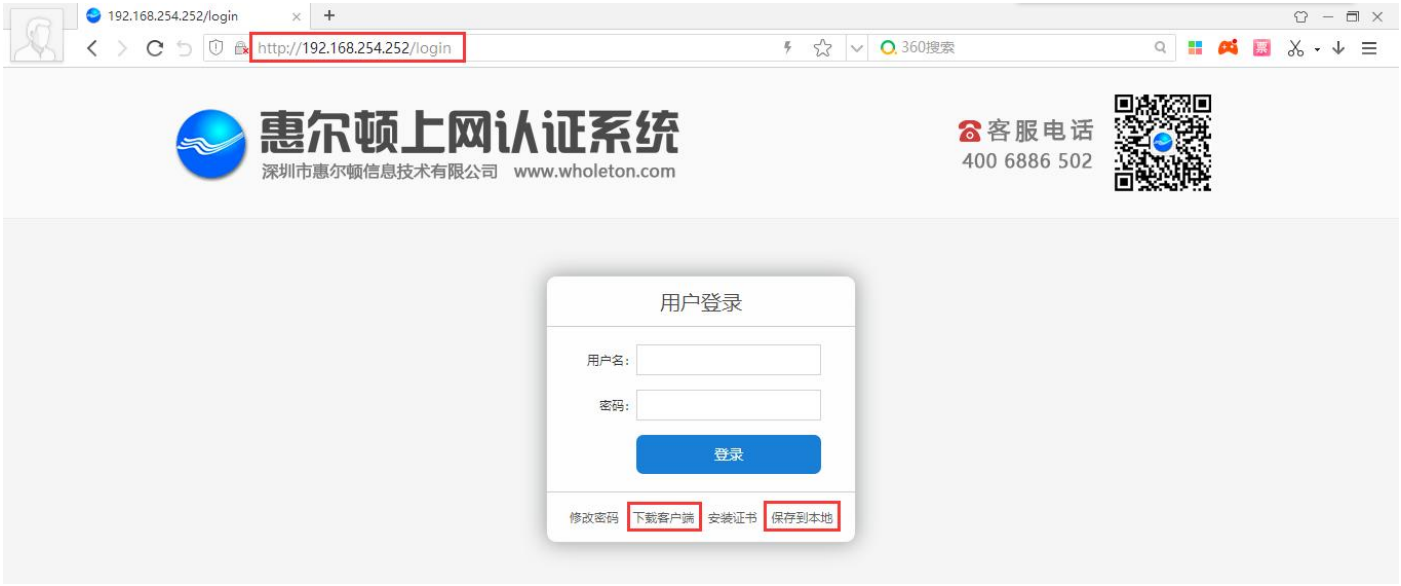
配置方法：

导航到【认证配置/组织结构】，如下图：



6 网页认证

认证地址：http://审计设备 ip/login　如下图：



备注：建议收藏上网认证页面，或者点击右下角“保存到本地”，可保存到桌面，上网时直接打开。

认证注销页：如下图：

备注：上网时认证注销页不要关和刷新，认证下线时不要直接关浏览器或者关机，要点右下角注销按钮。

7 客户端认证

认证设置：

地址：审计设备 ip（注意不是电脑 ip）；

端口：默认 9000，不用改；

用户和密码：认证账号和密码。

配置如下图：

备注：客户端和设备系统具有匹配性，建议在设备网页认证界面下载客户端。

五 策略管理

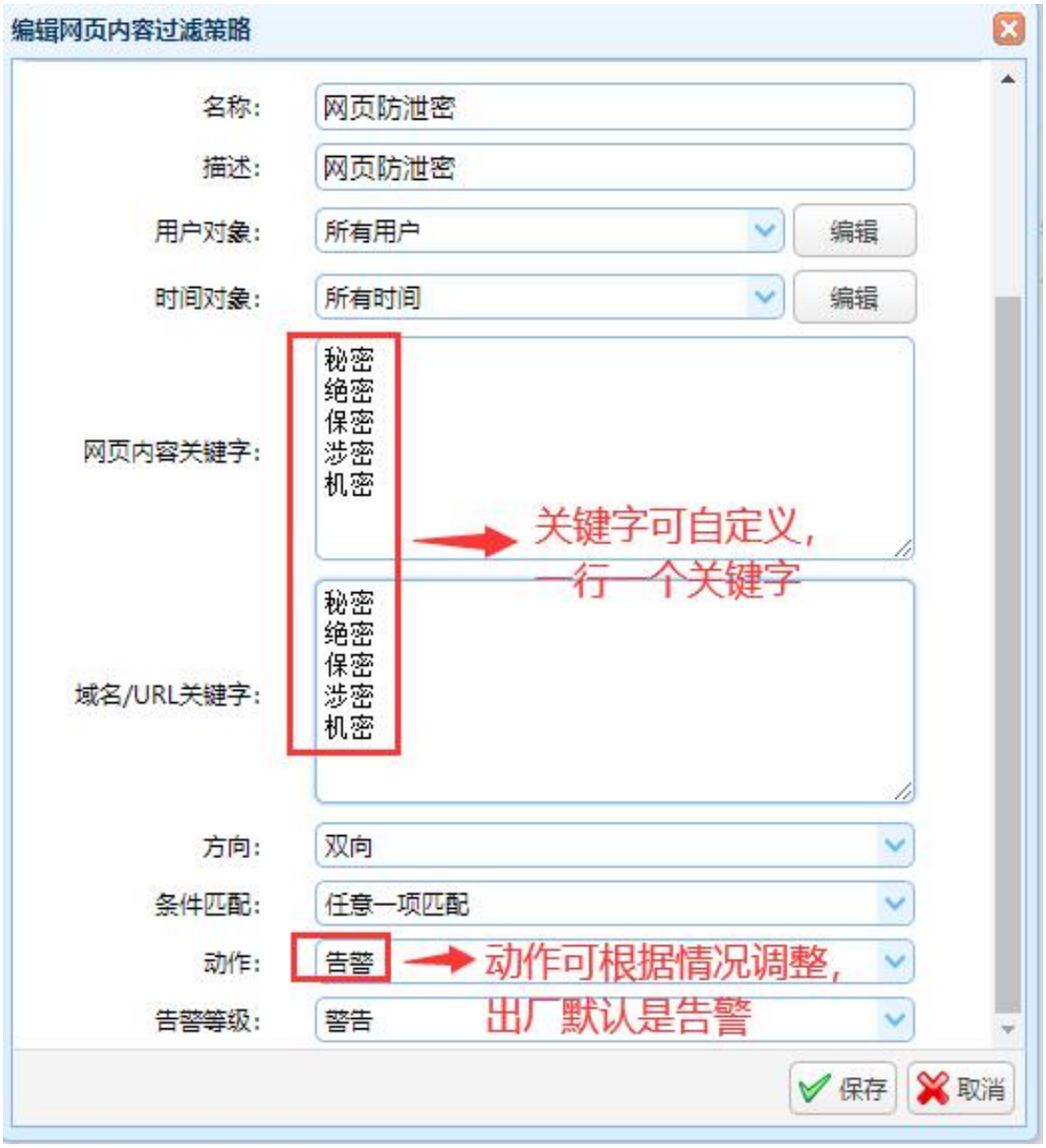
1 网页管控

网页管控包括网页标题的审计、告警、过滤以及网页内容的审计、告警与过滤，用户可以指定网页标题与内容的审计、告警与过滤策略。

配置方法：

导航到【策略管理/应用层策略/网页管控/网页管控】，如下图：

网页关键字过滤设置，可参照下图设置：



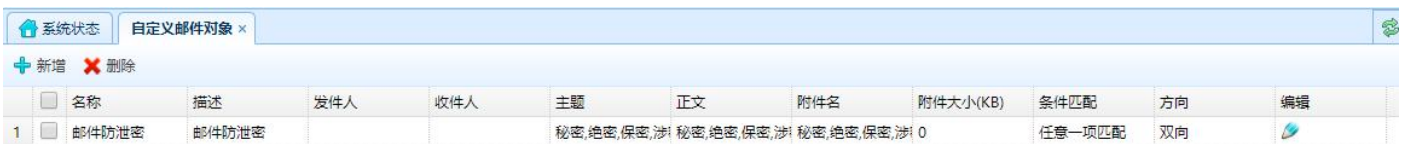
2 邮件管控

邮件过滤可以针对收件人、发件人、正文以及附件名关键字进行过滤，还可以对邮件进行延迟发送，经管理员审核后方可继续发送，能防止一些敏感邮件的传送，保障企业内部信息安全，防止信息泄密。

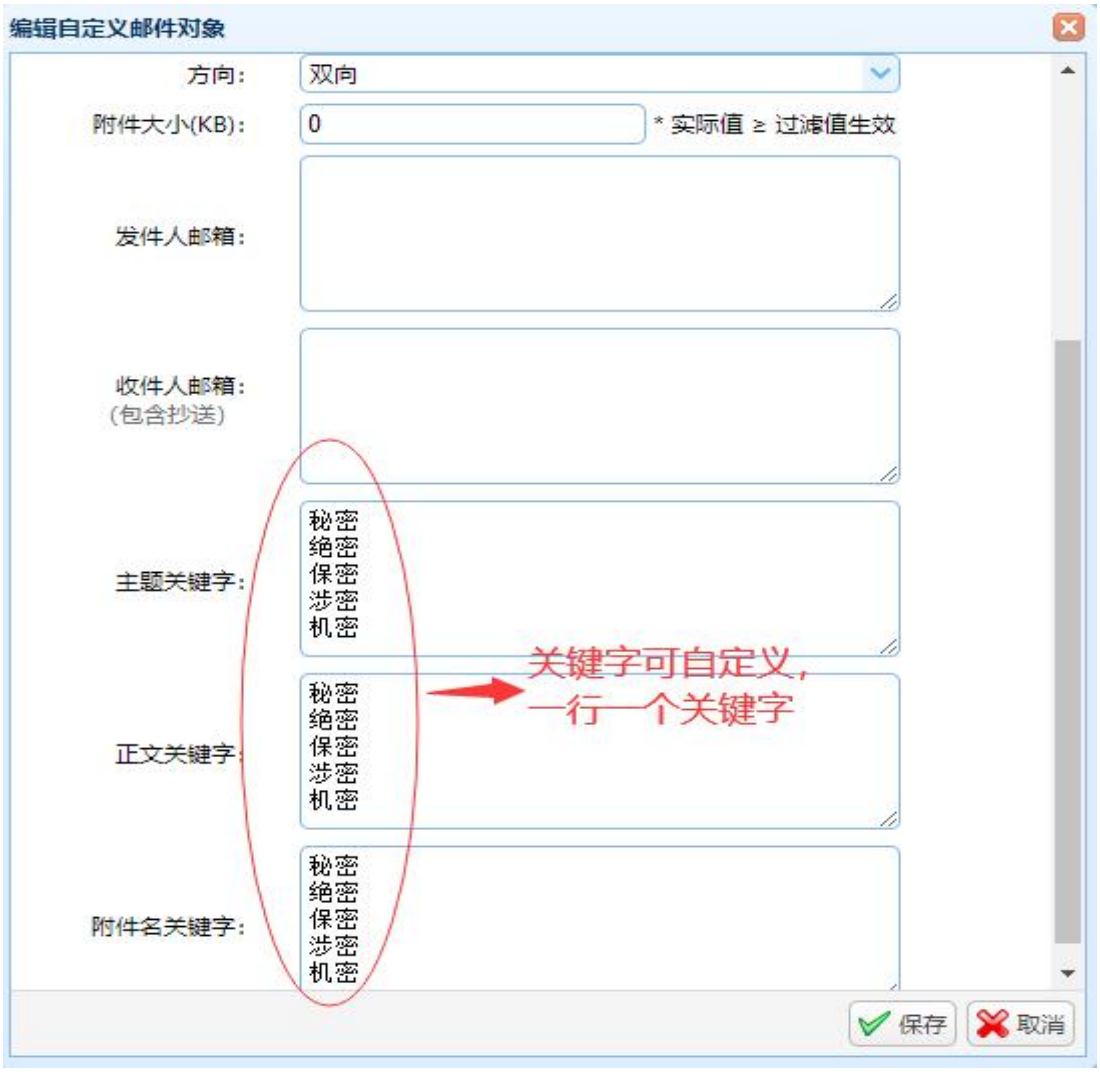
配置方法：

首先自定义邮件对象，邮件对象是制定邮件过滤策略的基础。

导航到【策略管理/应用层策略/邮件管控/自定义邮件对象】，如下图：



邮件的关键字过滤设置，可参照下图设置：



邮件关键字过滤策略

配置方法：

导航到【策略管理/应用层策略/邮件管控/邮件过滤策略】，如下图：

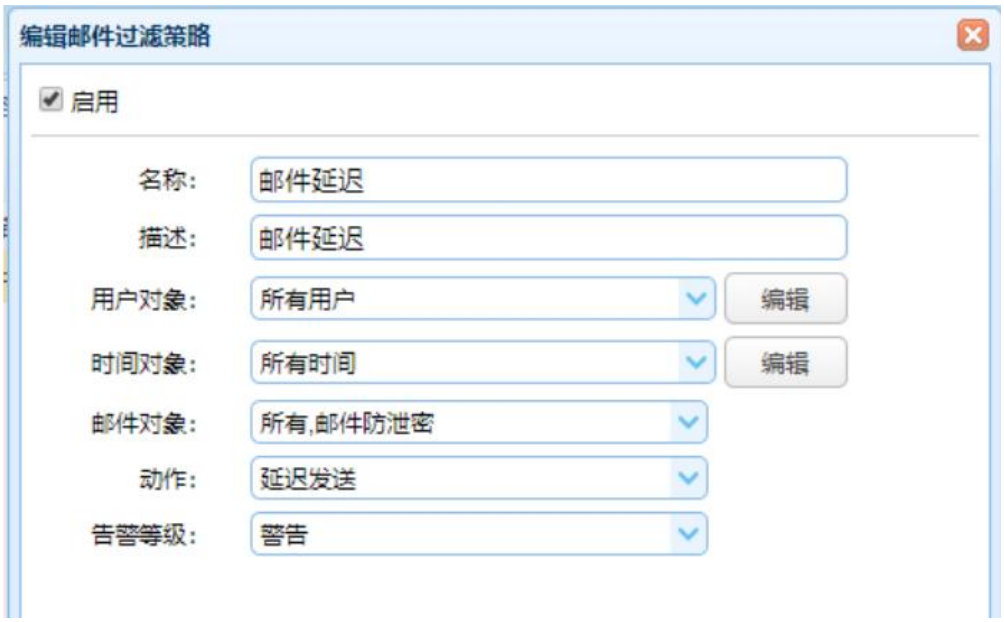
邮件过滤设置，可参照下图设置：

邮件延迟策略

配置方法：

导航到【策略管理/应用层策略/邮件管控/邮件过滤策略】，如下图：

策略设置如下图：



3 热点管控

热点管理可以通过上网行为管理的策略规则对网络里的共享上网行为、终端接入类型进行有效的管控，例如，设备可以识别网络中是否有终端在共享上网，该终端共享的网络接入数量等。也可以根据终端类型进行管控，例如电脑端（Window 版本、iMAC），安卓客户端、iPad、iPhone、Windows phone 等终端类型，并对检测到的终端类型做相应的惩罚行为。

配置方法：

导航到【策略管理/热点管理/共享设置】，在【共享设置】界面可以设置相应的终端控制参数，如下图：

配置说明：

上网共享：勾选“禁止共享上网行为”复选框可以禁止共享上网的行为，例如通过无线路由共享上网，或者使用无线网卡共享上网的共享上网行为，设置最多允许共享上网用户数量可以控制共享上网的数量。

终端类型：勾选“禁止下列选中类型设备接入网络”则启用禁止终端类型功能；勾选电脑、安卓、iPad、iPhone、Windows phone 前面的复选框可以禁止相应的终端设备类型，不勾选表示不禁止。

惩罚时间：惩罚时间是指在设备检测到有违反上面策略的网络行为时，给与的终端的禁止上网的惩罚行为，以分钟为单位，可以自定义设置，最小 1 分钟。

违规惩罚方式：建议选择禁止 ip 方式，禁止数据流可能会出现 https 网页不能禁止问题。

4 SSl 加密审计

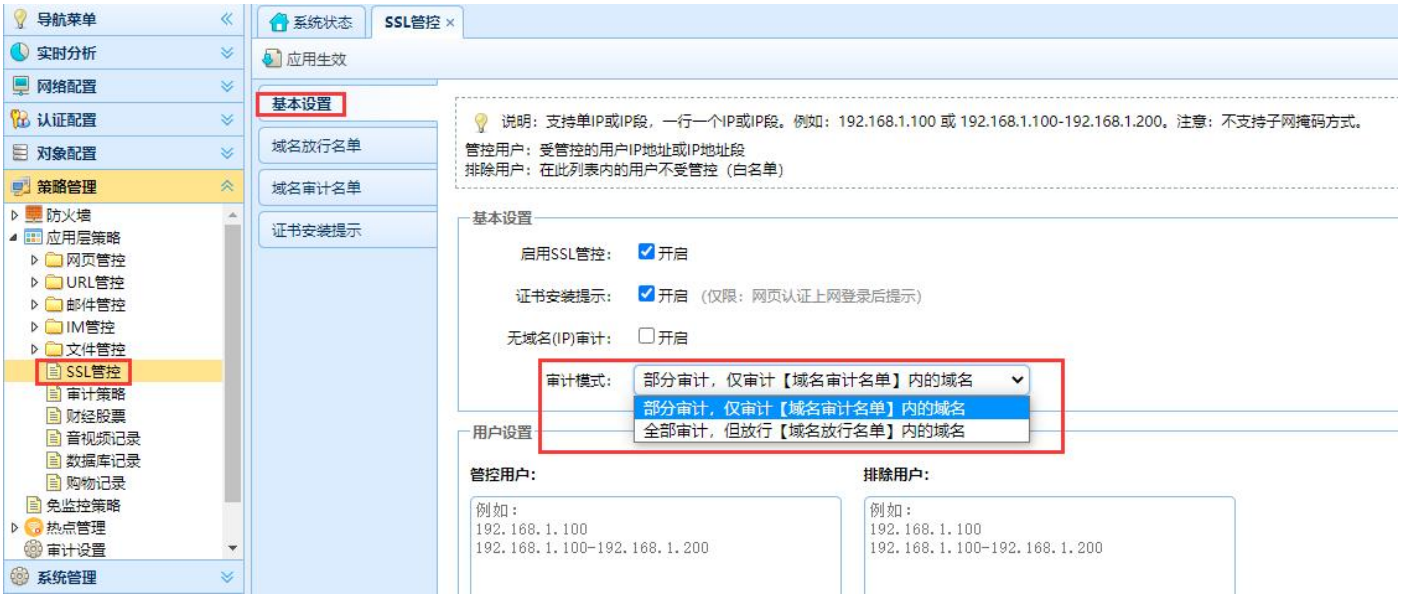
加密审计功能： 审计加密网站和邮件。

服务端：

配置方法：

导航到【策略管理/应用层策略/SSL 管控】，如下图：

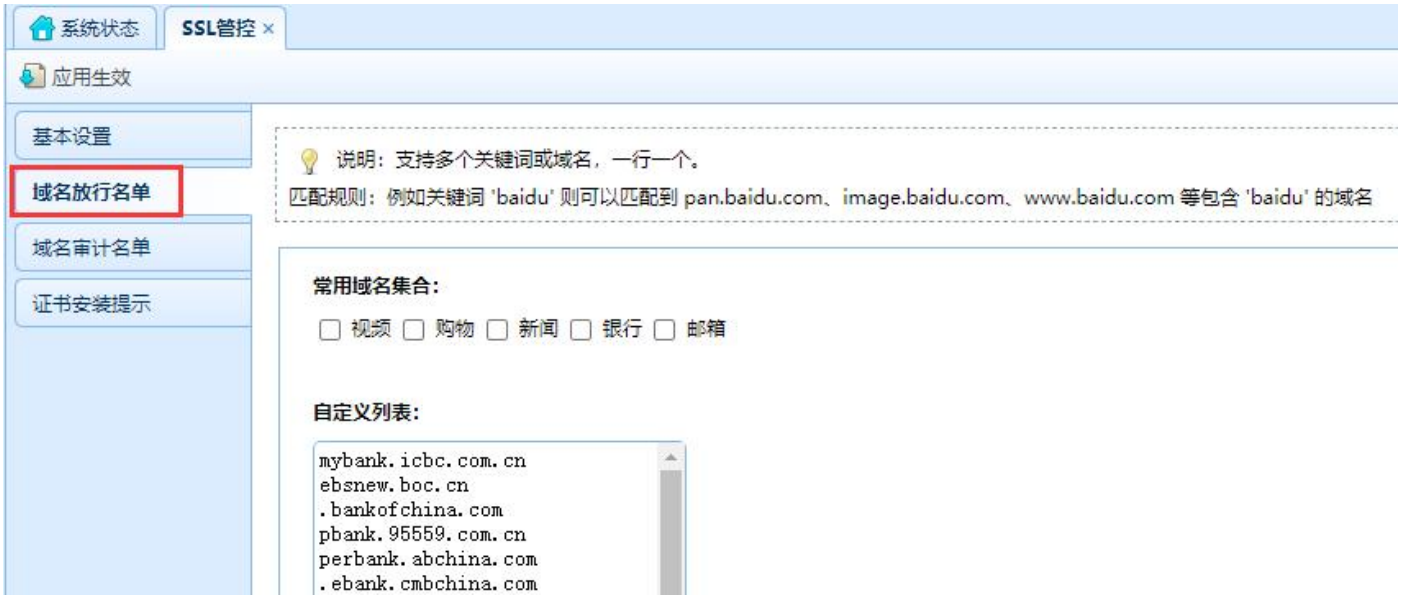
基本设置里面勾选“启用 ssl 管控”和“证书安装提示”。



管控用户里面设置管控用户 IP，可填单个 ip 或者一个范围；最后保存配置，并点击应用生效。

备注：审计模式可选择“全部审计或者部分审计”。全审模式下部分网站如果出现使用异常情况，可以添加到域名白名单里面，例如银行网站。

域名放行名单：默认内置了一些分类，也可以单独把不做 ssl 审计的域名添加进去。



域名审计名单：默认内置了一些分类，也可以单独把需要做 ssl 审计的域名添加进去。

电脑端：

安装 ssl 证书：

可通过设备网页认证界面下载 ssl 证书安装；

可以通过认证客户端安装，安装客户端时会自己安装 ssl 证书。

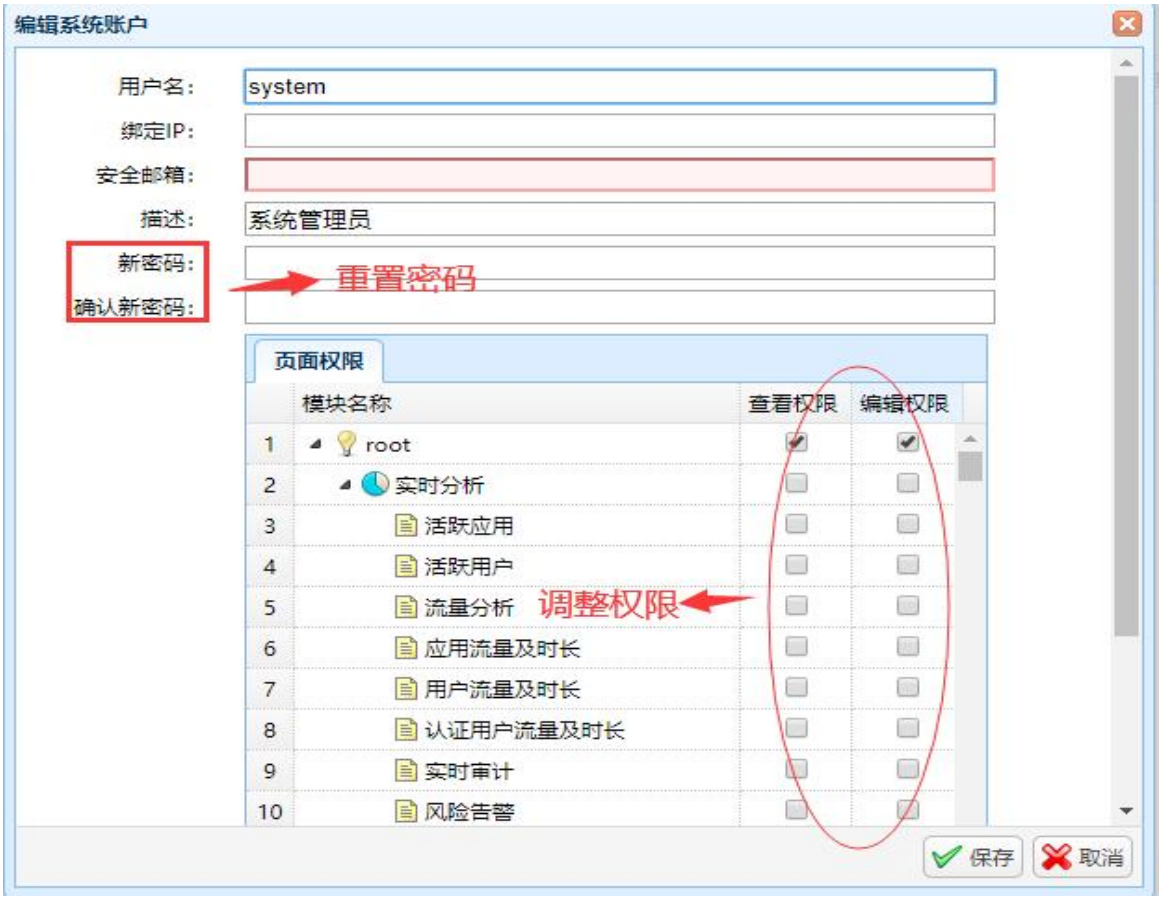
六 系统管理

1 系统账号（三员管理）

导航到【系统管理/系统账户】，如下图：

System（系统管理员）：设置设备网络配置、系统日志、系统时间、系统备份。
Safemanage（安全保密管理员）：设置认证账号、审计策略；查看审计记录。
Auditor（安全审计管理员）： 查看系统操作日志。

三员的密码默认都是 12345678，可以通过 admin 账号进入编辑、重置；三员的权限可以通过 admin 账号调整。
导航到【系统管理/系统账户】，如下图：



2 系统升级

升级方式：系统支持在线升级，每年都有 4 个大版本升级；
升级提醒：设备管理界面有升级提醒；

升级服务期：1 年内免费升级，过期要先续费后才能升级；

具体操作导航到【系统管理/升级管理/在线升级】，如下图：

备注：从上往下升级，升级过程中，设备不要断电和关闭浏览器，另外设备可能会重启，请选择合适时间升级。

3 系统功能

系统功能分为硬件系统和软件服务 2 部分，硬件系统可以做重启、关机、恢复出厂设置操作；软件服务可做重启流控服务、修复数据库、重置数据库、清除缓存、命令行操作。

导航到【系统管理/系统功能】，如下图：

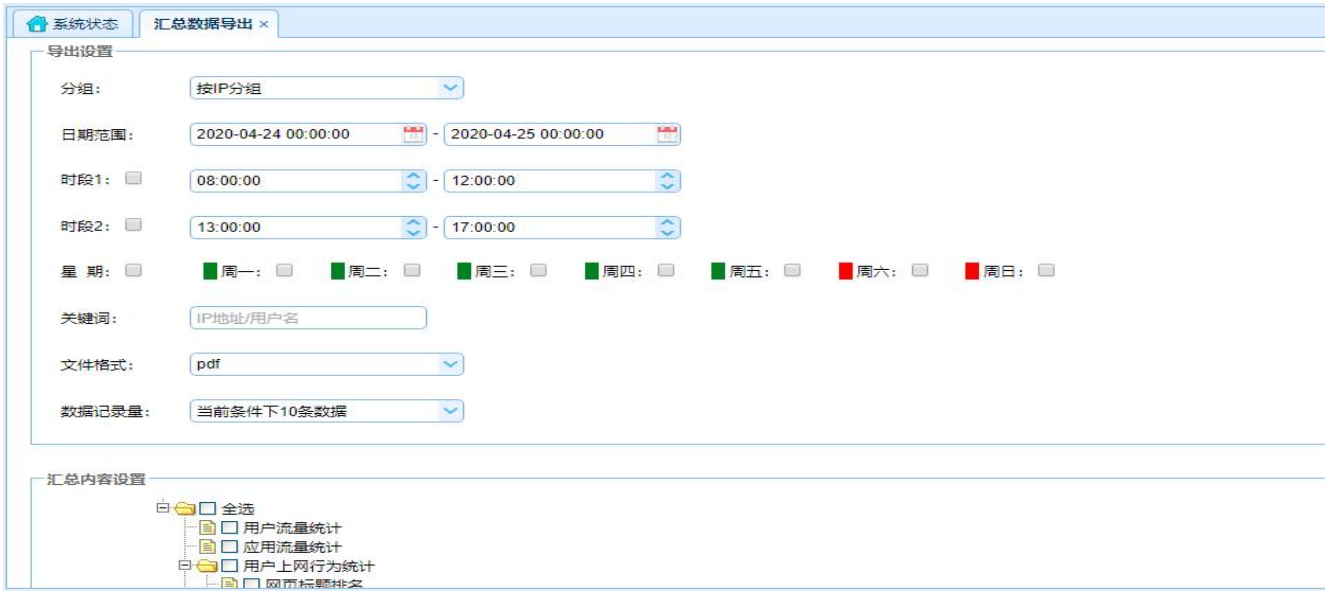
点击“激活信息”查看设备服务和升级是否在保情况。

七 数据中心

1 汇总数据导出

汇总数据导出可以将整个设备的数据以 pdf 或者 excel 格式导出来，形成电子文档，供网络管理员查看。导出时勾选需要导出的表格即可。

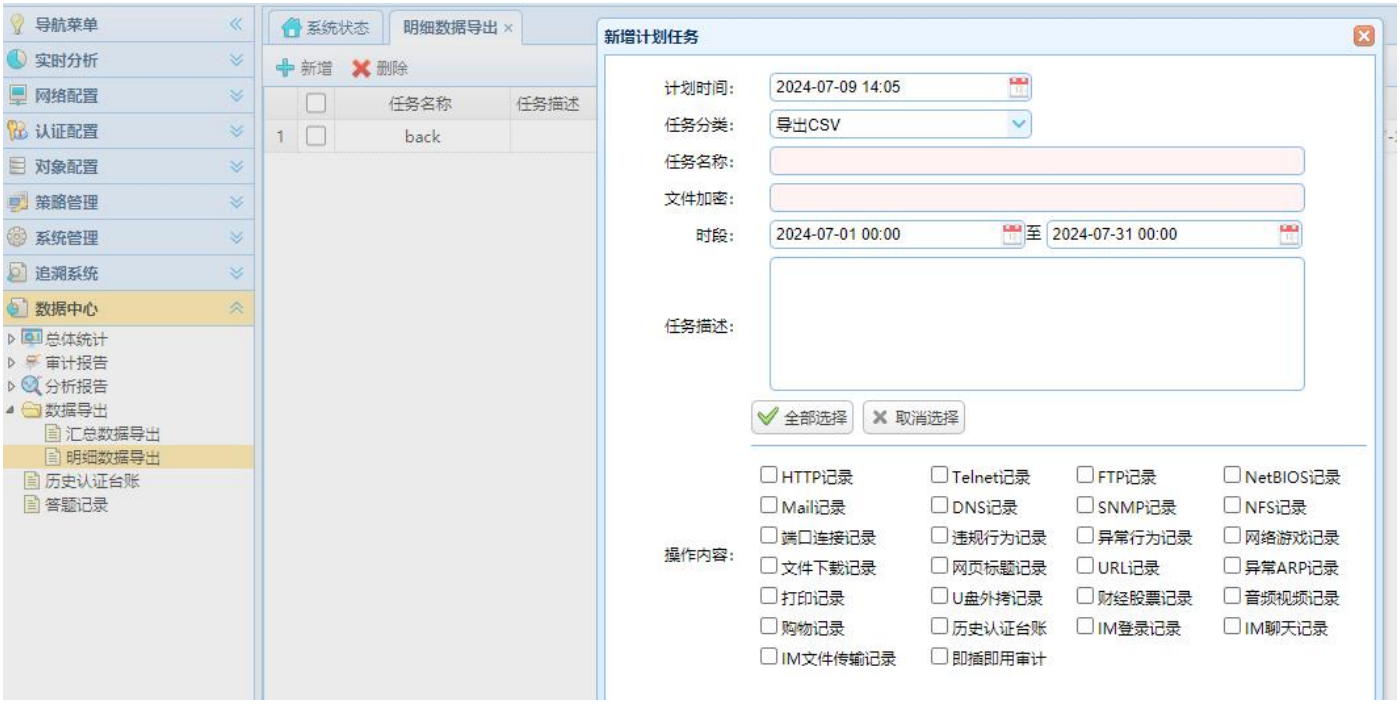
导航到【数据中心/汇总数据导出】，如下图：



2 明细数据导出

明细数据导出可以导出上网人员的具体行为记录，供网络管理员查看。导出时勾选需要导出的表格即可。注意文件加密密码设置，导出的文件会整个打包，打开时解压需要密码。

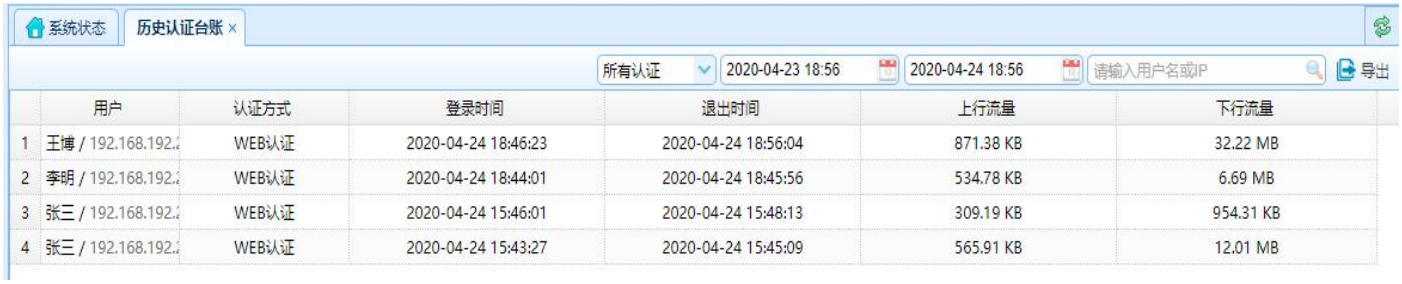
导航到【数据中心/明细数据导出】，如下图：



3 历史认证台账

历史认证台账展示的是之前用户认证的记录，时间可以自己选择，也可以选择认证方式，导出表格。

导航到【数据中心/历史认证台账】，如下图：



	用户	认证方式	登录时间	退出时间	上行流量	下行流量
1	王博 / 192.168.192.2	WEB认证	2020-04-24 18:46:23	2020-04-24 18:56:04	871.38 KB	32.22 MB
2	李明 / 192.168.192.2	WEB认证	2020-04-24 18:44:01	2020-04-24 18:45:56	534.78 KB	6.69 MB
3	张三 / 192.168.192.2	WEB认证	2020-04-24 15:46:01	2020-04-24 15:48:13	309.19 KB	954.31 KB
4	张三 / 192.168.192.2	WEB认证	2020-04-24 15:43:27	2020-04-24 15:45:09	565.91 KB	12.01 MB

八 网络培训

每周四下午 2：30 网上 QQ 电话会议，涉及产品实施安装部署，技术难点答疑；产品选型、升级、新功能点等介绍；保密检查注意事项分享等多个方面，通过用户与厂商的不断互动，我们会在上网防泄密这个领域越做越专业。

九 保密检查注意事项

1 需要开启上网实名认证，建议用客户端认证；不建议通过绑定 ip 或者 mac 来实现实名。
2 不推荐使用无线，如需使用，无线要以 ap 方式部署，不能用路由模式。
3 如果单位有除“秘密、机密、绝密、保密”之外的特殊涉密关键字，需要把特殊关键字加到对应策略里面。
4 如有加密网页和邮件审计需求，需要开启 ssl。加密审计需求可咨询当地保密局或者本单位保密咨询机构。
5 上网电脑需要全部做审计，不建议部分审计。
6 不推荐使用旁路模式，无法管控和认证，会扣分。
7 要知道策略如何设置、数据如何查看及导出。

十 售后服务

1 全国统一售后服务热线：4006886502。
2 全国统一在线服务 QQ：4006886502。
3 上班时间：工作日上午 8：30--12：00，下午 13：30--18：00；晚上 18：00--19：00 有电话值班。
4 周末和节假日电话值班：时间上午 8：30--12：00 下午 13：30--18：00，值班电话：4006886502。
5 设备返修邮寄地址：深圳市南山区高新技术产业园 R2-A 栋 3 层 358 室。

惠尔顿
WHOLETON
上网防泄密专家

深圳市惠尔顿信息技术有限公司
Shenzhen, Wholeton Information Technology Co., Ltd.
地址：深圳市南山区高新技术产业园R2-A栋3层358室
总机：(0755) 26546529 销售电话：0755-26635560
服务热线&QQ：4006886502
网　址： www.wholeton.com