中科云量
ZKQCLOUD

中科云量网页防篡改系统 V1.0

用户操作手册

广东中科云量信息安全技术有限公司

目 录

前言

文档范围

本文将覆盖中科云量网页防篡改系统的产品规格和 Web 管理界面的功能特点，并详细介绍该系统的具体使用方法、产品的各用户可使用的安全功能和接口及其使用方法、用户可获取但受安全处理环境所控制的所有功能和权限、产品安全操作中用户所应承担的职责、与用户有关的 IT 环境的所有安全要求。

期望读者

期望了解本产品主要技术特性和使用方法的用户、系统管理员、网络管理员、网络安全专家等。本文假设您对下面的知识有一定的了解：

- 系统管理
- TCP/IP 协议
- HTTP 协议
- Windows 或 Linux 操作系统

内容简介

章节	概述
1 产品概述	介绍产品功能
2 快速使用指南	介绍 Web 管理页面的基本操作方法和使用指南
3 主机管理	介绍 Web 管理界面中的主机管理功能
4 策略管理	介绍 Web 管理界面中的扫描策略
5 系统管理	介绍 Web 管理界面中系统设置等内容
6 日志审计	介绍 Web 管理界面对操作日志进行查看和管理等操作

格式与名词约定

设备、产品、系统、网防——除非特指，本手册中均表示中科云量网页防篡改系统

【A】 —— 菜单名称和按钮名称的表示方式

【A】→【B】—— 菜单项选择的表示方式

 —— 使用技巧、建议和引用信息等

 —— 重要注意信息

第一章 产品介绍

1.1.产品简介

网站在信息发展中起到了重要的作用，现已渗透到了世界的各个领域。

根据 CNNIC 调查报告显示，截至 2008 年 7 月，我国的上网用户总数高达 1.1 亿，国内网站数量达 67 万。庞大的网民数量和网站群为互联网应用的快速发展奠定了良好的基础，网页的地位也得到了空前的提高。对于一个政府机构或企业来说，网页无异于自己的门面。2007 年全国共有 24516 个一级域名网站被篡改，其中 gov.cn 域名的政府网站仅 2007 年就有 708 个网站被篡改。这时对于能够保护网站防篡改的技术变得迫切需要。

中科云量网页防篡改系统是由广东中科云量信息安全技术有限公司自主研发的 WEB 整体安全系统的一个独立的应用单元产品。该系统基于 WINDOWS 和 LINUX 内核驱动的方式对用户指定的网站文件进行保护，同时通过内嵌的 WEB 安全模块对 SQL 注入等各类 WEB 攻击进行阻断和报警，该系统主要帮助用户保证单一的 WEB 篡改等影响恶劣行为的防护。

中科云量网页防篡改系统使用灵活的安全策略，用户通过制定灵活的安全策略来保护目标文件和目录系统。从操作系统核心来阻止非法篡改和攻击行为，使保护更加周全，同对合法的用户进行身份认证，并根据其身份，授权对保护文件进行合法的修改操作，并进行 SSL 加密，从而真正实现了安全与易用的结合。

功能菜单接口

功能菜单包括以下主菜单，每个主菜单下面又有若干子菜单。

当您点击主菜单后，会弹出其下的子菜单。各个菜单的主要功能如下。

【网站管理】主菜单

【增加网站】：添加监控网站。

【备份网站】：备份监控网站的数据。

【生成水印】：对监控网站的数据生成透明水印。

【监控策略】：自定义监控策略

【备份策略】：自定义备份策略

【同步策略】：自定义网站数据的同步策略

【状态设置】：自定义设置开启和关闭监控状态

【删除网站】：将已添加监控的网站从保护列表中删除

【主机管理】主菜单

【添加主机】：在系统中添加监控主机或备份主机

【主机状态】：管理、查看系统中各主机的连接、存活状态。

【日志管理】主菜单

【文件篡改日志】：管理、查看和导出文件篡改事件的审计日志。

【系统日志】：管理、查看和导出系统事件的审计日志

【操作日志】：管理、查看和导出用户对于系统的操作事件的审计日志

【系统管理】主菜单

【参数设置】：管理系统的服务策略。

【下发配置】：将系统设置下发到各个监控主机。

【用户管理】主菜单

【用户管理】：管理和配置、添加和修改系统用户的开启/关闭状态、用户信息、用户密码等

第二章 用户功能和权限

2.1 系统登录

使用浏览器访问管理后台地址，如：**https://192.168.0.1**

提示：

为了获得最佳的页面浏览效果，建议您使用 Firefox、Google Chrome、Microsoft Internet Explorer 11.0 版本的浏览器，推荐显示分辨率 1024×768 以上。

6. 输入用户名和密码（设备初始用户名 **admin** 和密码 **admin@2018**）,正确输入验证码，点击【登录】按钮，进入“中科云量网页防篡改系统”欢迎界面。注意：默认情况下，输错密码超过 5 次，该用户即被锁定，锁定时间为 10 分钟，锁定期间内，使用正确的用户名、密码也不能登陆。登陆成功后，可修改管理员安全策略。

⚠注意：

如果登录失败，请检查是否为以下原因引起：

- **用户名输入错误**
- **密码输入错误**
- **没区分大小写。**

第三章 系统功能

3.1 Web 登录

Step1：通过浏览器登录到配置管理中心(https://IP:Port)，其中 IP 是配置管理中心的 IP 地址，Port 是配置管理中心的监听端口（默认值为:8088），以下是以默认管理中心 IP 为 192.168.0.1 示例，链接地址及其默认用户密码如下：

https://192.168.0.1:8088/

帐　号：admin

密　码：admin@2018

图 3-1 用户登录界面

图表说明：

位置 1：用户帐号

位置 2：用户密码

位置 3：验 证 码

提示：

为了获得最佳的页面浏览效果，建议您使用 Firefox、Google Chrome、Microsoft Internet Explorer 11.0 版本的浏览器，推荐显示分辨率 1024×768 以上。

Step2：输入用户密码登陆系统后，如下所示：

图 3-2 登陆初界面

图表说明：

位置 1：添加网站名称的区域。

位置 2：添加网站的步骤说明

3.2 网站管理

ⓘ注意：本节中对网站管理及其配置的改变将产生审计日志

3.2.1 添加网站

Step1：网站名称后面的输入框中，输入准备被监控的网站名称，然后点击“**增加网站**”即可，如下所示：

图 2-3 添加网站

Step2：在上一步中点击“**增加网站**”后进入到添加监控主机和备份主机的界面，如下所示：

图 2-4 添加监控机和备份机界面

图表说明：

位置 1：网站名称，自定义即可。

位置 2：添加监控主机，已安装监控端程序的机器。

位置 3：添加备份主机，已安装备份端程序的机器。

Step3：增加监控主机并设置其对应的目录名称和目录，如下所示：

图 2-5 添加监控主机

图表说明：

位置 1：监控主机名称，自定义即可。

位置 2：监控主机所在的 IP 地址。

位置 3：监控主机监听的端口**(默认是 60002)**，可以自定义设置。

图 2-6 监控主机设置

图表说明：

位置 1：添加监控主机(**选中前面选框，可显示后面位置 2，3，4**)

位置 2：受监控的目录名称，自定义即可。

位置 3：受监控的目录(**可手动输入,也可点位置 4 进行选择**)。

位置 4：选择受监控的目录，自定义即可。

Step4：增加同步主机并设置其对应的目录名称和目录，如下所示：

图 2-7 添加同步主机

图表说明：

位置 1：同步主机名称，自定义即可。

位置 2：同步主机所在的 IP 地址

位置 3：同步主机监听的端口(**默认是 60003**)，可自定义设置。

图 2-8 同步主机设置

图表说明：

位置 1：添加同步主机**(选中前面选框，可显示后面位置 2，3，4)。**

位置 2：同步备份的目录名称，自定义即可。

位置 3：同步备份的目录(**可手动输入，也可点位置 4 进行选择**)。

位置 4：选择同步备份的目录，自定义即可。

Step4：点击“**确定**”确认后，如下所示：

图 2-9 添加网站管理主界面

图表说明：

位置 1：可以添加网站。

位置 2：启动或停止所有网站服务

位置 3：单个网站管理功能菜单

位置 4：网站设置列表

3.2.2 添加监控主机

点击“**添加监控主机**”添加监控主机功能，如下所示：

图 2-10 添加监控主机

图表说明：

位置 1：已经添加的监控主机列表

位置 2：新增主机表单信息

3.2.3 添加同步主机

点击“**添加同步主机**”添加同步主机功能，如下所示：

图 2-11 添加同步主机

图表说明：

位置 1：已经添加的同步主机列表

位置 2：新增主机表单信息

3.2.4 网站设置

3.2.4.1 编辑目录

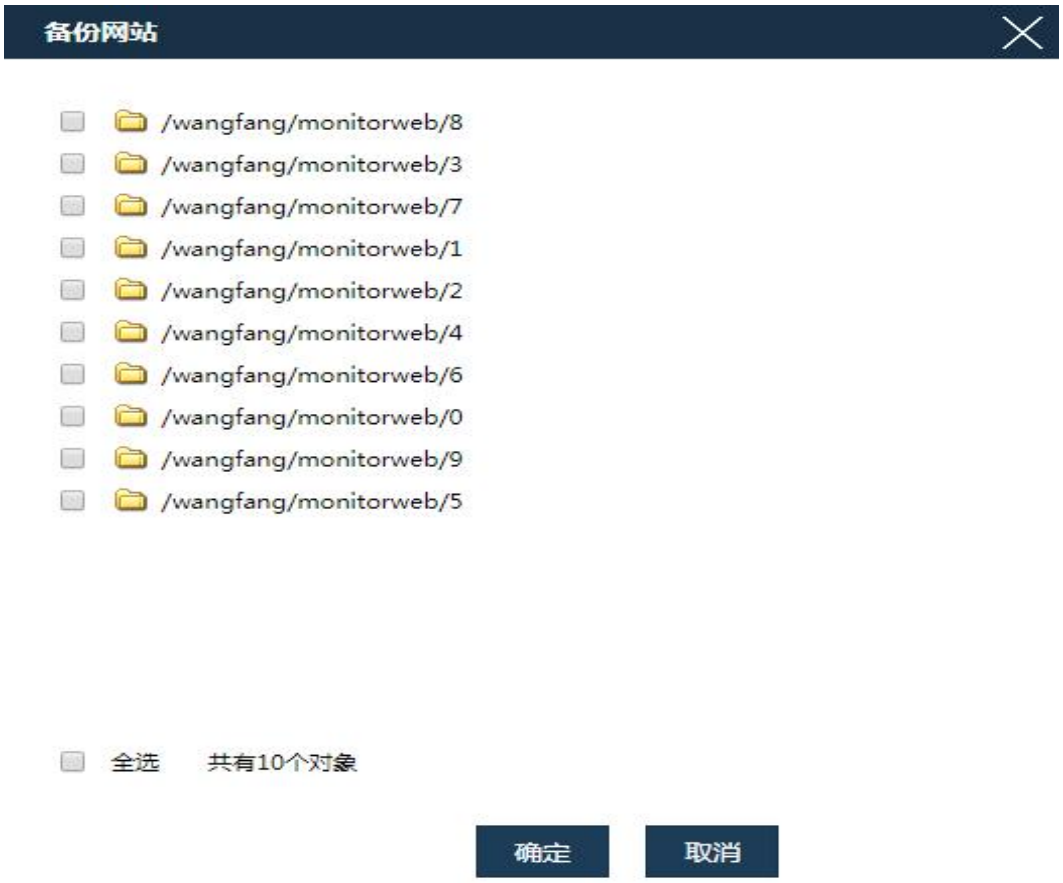
点击任何一个主机 IP 即可以进入目录编辑，如点击 192.168.37.152 ，如下所示：

图 2-18 编辑目录

3.2.4.2 备份网站

点击列表中的监控主机上的“**备份网站**”进入备份网站，选中要备份的文件或文件夹，把监控目录的网站备份到同步主机的备份目录下，如下所示：

图 2-19 备份网站



3.2.4.3 生成水印

执行初始化，点击列表中的监控主机上的“**生成水印**”，对已备份的目录生成水印，做标记，如下所示：

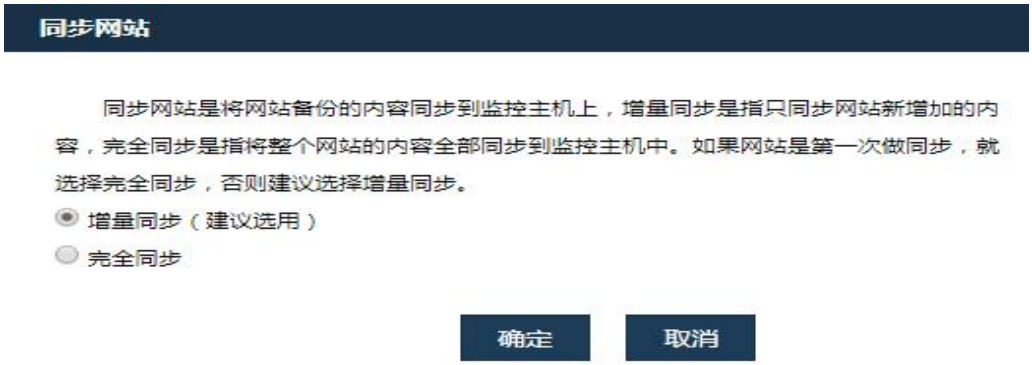
图 3-20 生成水印

注意：**只有生成水印后的文件，才可恢复回来**

3.2.4.4 同步网站

点击列表中的同步主机上的“**同步网站**”进入同步网站，包括增量同步和完全同步两种。同步网站是从备份端目录同步到监控端的目录，刚好跟备份网站是相反过程，如下所示：

图 2-21 同步网站

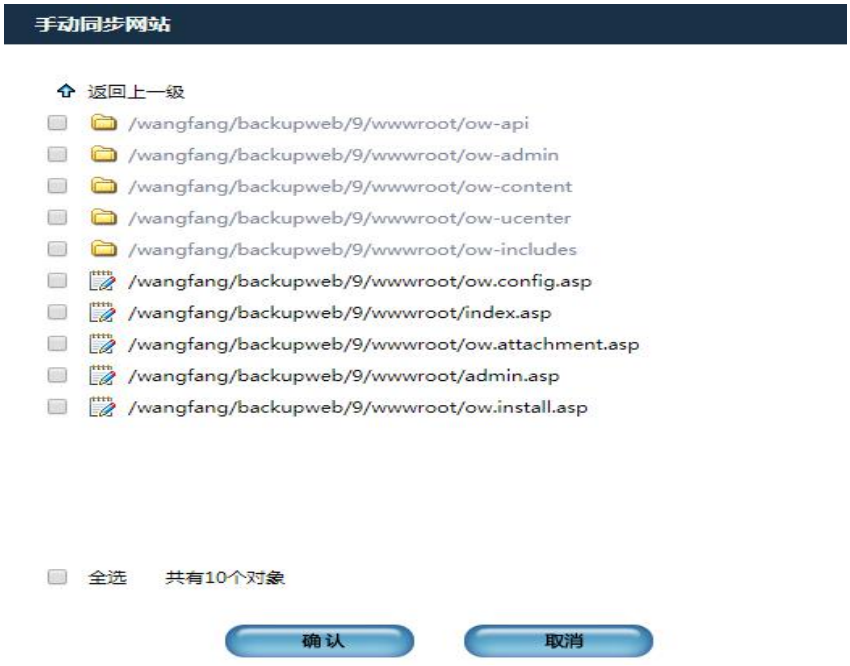


注意：**同步网站同时做了生成水印的操作，所以不用在重新做水印操作**

3.2.4.5 手动同步

点击列表中的同步主机上的“**手动同步**”进入手动同步，选择要同步的文件或文件夹，手工同步要同步的文件或者文件夹，如下所示：

图 2-22 手动同步



注意：**同步网站同时做了生成水印的操作，所以不用在重新做水印操作**

3.2.4.6 监控主机：状态设置

点击列表中监控主机的“**状态设置**”，进入状态设置，如下所示：

图 2-23 状态设置

图表说明：

位置 1：开启本主机状态功能，默认开启。

位置 2：开启监控网站目录监控功能（**注：只有在监控的状态开启下，防篡改功能才生效**）。

位置 3：开启监控网站目录的监控方式，事件监控器为默认监控器(建议保持默认配置)；扫描监控器就是设个定时器，定时去遍历目录文件，查看有没有篡改，比较耗费系统 CPU 资源，不建议开启；驱动监控器是指 windows 版本的，由驱动过滤实现监控。不过因为微软的数字证书签名问题，收费使用，所以也不建议使用。

3.2.4.7 同步主机：状态设置

点击列表中同步主机的“状态设置”，进入状态设置，如下所示：

图 2-24 状态设置

图表说明：

位置 1：开启本主机状态功能，默认开启。

位置 2：开启网站同步的自动同步功能，开启自动同步功能后，在备份端备份目录做增、删、改、重命名等操作都会实时同步到监控端目录。

3.2.4.8 监控策略

点击列表中监控主机的“**监控策略**”，选择要排除不受监控的列项，如下所示：

图 2-25 监控策略

图表说明：

位置 1：指定要排除的目录。

位置 2：指定要排除的文件。

位置 3：指定要排除的文件类型。

位置 4：指定要排除的文件或目录（模糊匹配文件）。

位置 5：指定要排除文件或目录事件（修改、删除、新建）。

3.2.4.9 备份策略

点击列表中监控主机的“**备份策略**”，选择排除不需要备份的列项，如下所示：

图 2-26 备份策略

图表说明：

位置 1：指定要排除的目录。

位置 2：指定要排除的文件。

位置 3：指定要排除的文件类型。

位置 4：指定要排除的文件或目录（模糊匹配文件）。

位置 5：指定要排除属性为以下条件的文件（大小及时间）。

3.2.4.10 自动同步策略

点击列表中同步主机的“**自动同步策略**”，选择排除不需要自动同步的列项，如下所示：

图 2-27 自动同步策略

图表说明：

位置 1：指定要排除的目录。

位置 2：指定要排除的文件。

位置 3：指定要排除的文件类型。

位置 4：指定要排除的文件或目录（模糊匹配文件）。

位置 5：指定要排除文件或目录事件。

注意：修改、删除、新建仅针对目录

3.2.4.11 完全同步策略

点击列表中同步主机的“**完全同步策略**”，针对同步网站的完全同步选项，选择排除不需要同步的列项，如下所示：

图 2-28 完全同步策略

图表说明：

位置 1：指定要排除的目录。

位置 2：指定要排除的文件。

位置 3：指定要排除的文件类型。

位置 4：指定要排除的文件或目录（模糊匹配文件）。

位置 5：指定要排除属性为以下条件的文件（大小及时间）。

3.3 删除网站

删除网站有两种方法，第一种方法：可以直接点击“**删除网站**”，把网站删除，但是主机保留着，主机可以在主机管理那里进行删除；第二种方法：要先把网站设置下的主机删除，再点击“**删除网站**”即可，如下所示：

图 3-29 删除网站

注意：该操作不可逆，删除后该网站的所有策略、历史信息都将清空，且无法恢复。该操作将产生审计日志。

3.4 主机管理

点击主菜单中的“**主机管理**”即可进入主机管理模块，如下图所示：

图 2-30 主机管理界面

图表说明：

位置 1：添加主机（可以增加监控或同步主机）。

位置 2：主机列表(可以删除或修改主机、智能防御)。

位置 3：对应主机的监控或备份网站，其中篡改日志详细见第四章系统维护。

3.4.1 添加主机

点击“**添加主机**”，即可进入添加主机界面，选择主机类别、填写主机名称、IP 及其监听端口即可，如下所示：

图 2-31 添加主机

3.4.2 修改主机 IP

点击对应的“**主机图像**”即可以进入修改主机 IP，如下所示：

图 2-32 修改主机信息

3.4.3 智能防御

点击“**主机管理->监控主机图像**”下面的“**智能防御**”，可以查看监控主机的一些系统信息，包括主机状态、进程监控、网络连接等，如下图所示。

主机状态：

进程监控：

进程监控

进程名称(红色为可疑进程)	PID	CPU	内存使用	下载速度	上传速度	操作
init	1	0	1.40Mb	0b/s	0b/s	关闭
udevd	546	0	1.18Mb	0b/s	0b/s	关闭
vmware-vmblock-fuse	1604	0	1.14Mb	0b/s	0b/s	关闭
vmtoolsd	1640	0	6.32Mb	0b/s	0b/s	关闭
VGAuthService	1712	0	8.19Mb	0b/s	0b/s	关闭
ManagementAgentHost	1784	0	6.82Mb	0b/s	0b/s	关闭
dhclient	1972	0	996Kb	0b/s	0b/s	关闭
auditd	2017	0	868Kb	0b/s	0b/s	关闭
rsyslogd	2042	0	1.63Mb	0b/s	0b/s	关闭
rpcbind	2084	0	892Kb	0b/s	0b/s	关闭
dbus-daemon	2099	0	1.70Mb	0b/s	0b/s	关闭
rpc.statd	2117	0	1.29Mb	0b/s	0b/s	关闭
rpc.idmapd	2155	0	500Kb	0b/s	0b/s	关闭
cupsd	2170	0	3.00Mb	0b/s	0b/s	关闭
acpid	2195	0	644Kb	0b/s	0b/s	关闭
hald	2204	0	3.33Mb	0b/s	0b/s	关闭

网络连接状态：

网络连接

进程名(红色为可疑进程)	协议	本地地址与端口	远程地址与端口	状态
rpc.statd	TCP	0.0.0.0:44236	0.0.0.0:0	监听
rpcbind	TCP	0.0.0.0:111	0.0.0.0:0	监听
sshd	TCP	0.0.0.0:22	0.0.0.0:0	监听
cupsd	TCP	127.0.0.1:631	0.0.0.0:0	监听
BDWGManager	TCP	0.0.0.0:8088	0.0.0.0:0	监听
master	TCP	127.0.0.1:25	0.0.0.0:0	监听
BDWGManager	TCP	0.0.0.0:60001	0.0.0.0:0	监听
BDWGMonitor	TCP	0.0.0.0:60002	0.0.0.0:0	监听
BDWGBacker	TCP	0.0.0.0:60003	0.0.0.0:0	监听

3.5 系统管理

3.5.1 用户管理

点击“**系统管理**”下拉列表中的“**用户管理**”，即可进入用户管理界面，如下所示：

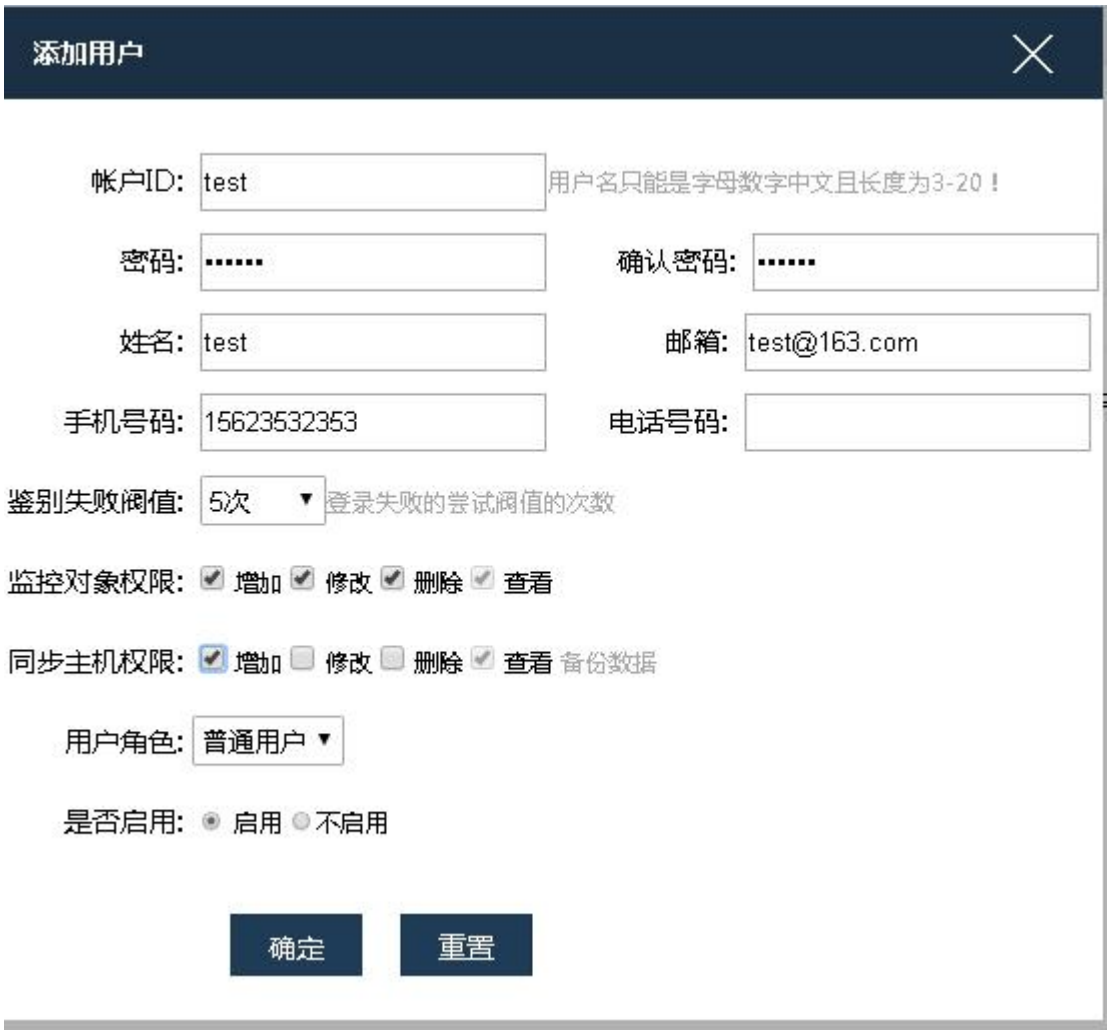
图 2-33 用户管理界面

注意：用户列表及其状态使能和操作，只能修改本身用户资料的功能。

3.5.1.1 添加用户

点击“**添加用户**”，进入添加用户界面，填写用户信息后，包括鉴别失败阀值、监控对象权限、同步主机权限、用户角色等参数，确定即可，如下所示：

图 2-34 添加用户



点击确定后，如下所示：

图 2-35 用户列表

3.5.1.2 修改资料

用户普通用户登录，点击“**编辑**”，进入修改界面，填写用户信息后确定即可，如下所示：

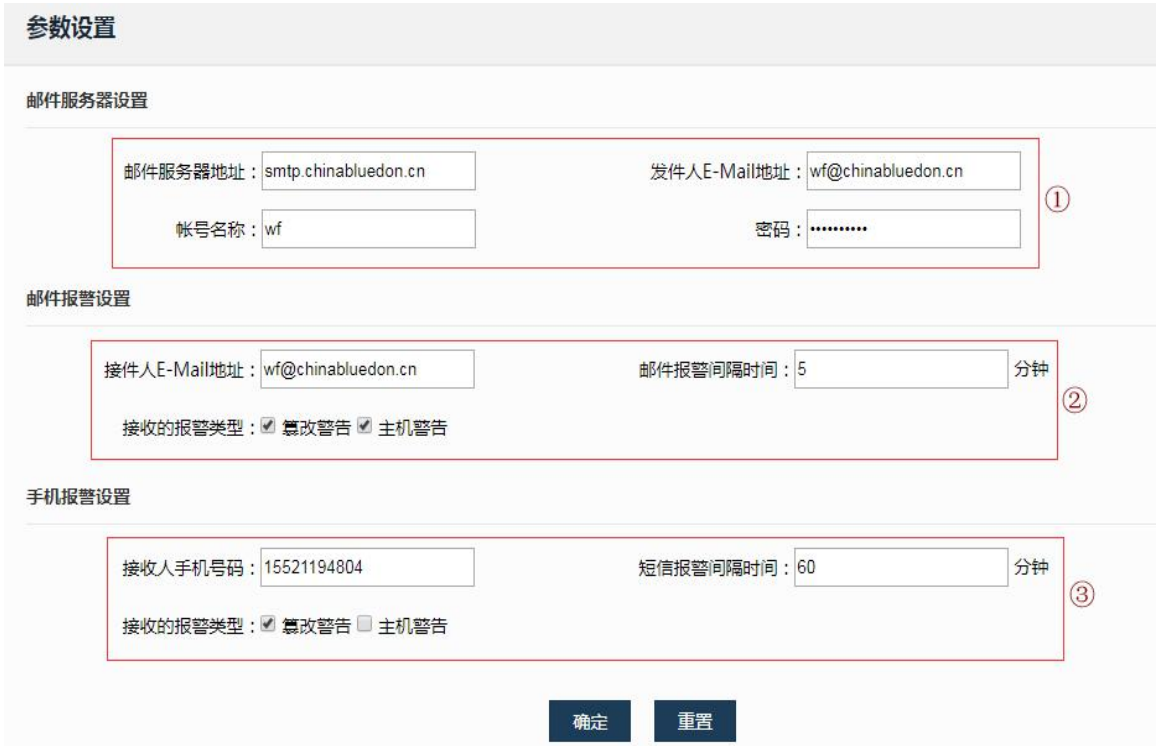
图 2-36 修改资料

注意：**修改资料只能修改当前用户（即自己）的资料。**

3.5.2 参数设置

点击“**系统管理**”的下拉列表中的“**参数设置**”，即可进入参数设置，如下图所示：

图 2-37 参数设置



图表说明：

位置 1：设置邮件服务器的地址及其发件人。

位置 2：设置告警信息的邮件接收者。

位置 3：设置告警信息的短信手机接收者。

3.5.3 下发配置

点击“**系统管理**”的下拉列表中的“**下发配置**”，即可自动下发配置到监控模块。

提示：

下发配置主要是开启监控状态、重新修改监控主机、备份主机、重新安装监控端、备份端程序等操作，才需要重新下发配置。

注意：

同步任务过程中，请不要下发配置，不然可能出现不可预估的系统错误。

4 系统维护

点击主菜单中的“**日志管理**”进入系统维护，根据相应的列项对系统进行维护，如下所示：

图 3-1 系统维护

4.1 查看日志

点击“**日志**”按钮进入日志查看界面，可以根据设置对应的时间段、事件、网站名称等条件进行查询日志，如下所示：

图 3-2 查看日志

5 系统授权

5.1 查看授权

点击主菜单中的“**系统管理**”下拉列表中的“**系统注册**”，即可进入系统授权界面，如下所示：

图 4-1 系统授权

图表说明：

位置 1：本系统的信息，其中序列号就是机器码，申请授权所用。

位置 2：可以进入产品注册页面。

6 常见问题

6.1 怎样开始网站监控保护？

用户在需要保护网站之前，请务必手工完全备份网站目录下所有目录和文件，然后再进行下面的操作。

第一步：添加网站。操作方法见用户手册 3.2.1。

第二步：完全备份网站目录。操作方法见用户手册 3.2.5.2。

第三步：生成水印。操作方法见用户手册 3.2.5.3。

第四步：添加监控策略。如果网站目录下有数据库文件或用户上传文件目录等需要经常变动的目录和文件，请在监控策略里添加排除监控文件或目录策略，操作方法见 3.2.5.8，如无此需求请略过此步。

第五步：开始监控。通过网站状态设置来开启监控，在保证监控主机和同步主机都处于开启的前提下，开启监控状态开关，对网站开启监控。

6.2 怎样发布网站更新？

第一步：首先将需要更新的网站内容上传到备份端所在设备上。

第二步：将更新的内容覆盖到备份端该网站备份目录下。

第三步：同步网站。操作方法见 3.2.5.4。

注：同步网站分为增量同步、完全同步、手动同步三种方式，其中增量同步为默认选项。

6.3 怎样处理网站下经常变动的目录和文件，如数据库文件或用户上传目录？

对于网站目录下经常会被网站程序正常修改的目录和文件，应该在中科云量网页防篡改

系统中排除在保护之外，在开始监控之前请添加排除策略。

第一步：添加网站监控信息，如果已经添加请略过此步。

第二步：添加网站监控策略。在监控策略里添加排除目录或文件列表。

第三步：启动该网站的监控。

6.4 如何开启网站监控主机的智能防御功能？

进入 “**系统管理->主机管理界面**”，点击“**智能防御**”进入智能防御设置界面进行设置。如下所示：

6.5 操作注意事项

1. 如果重新更换备份端、监控程序，导致出现备份中断现象，程序的通信已断开。需要重新下发配置，否则自动同步、增量同步不生效。

2. web 管理界面，受系统防火墙的影响，会导致 web 无法访问，需要开放对应的端口或者禁用防火墙。

3. 新建监控端的时候，同一个监控端，不要被多个管理端进行管理，不然引起其中一个管理端的监控端 IP、目录等配置信息错误，引起备份、同步失败。

4.网防有多个监控端时，可以通过开启监控的总开关，同时开启或者关闭监控状态。当偶尔出现个别开关开启或者关闭失败时，可以通过点击开启或者关闭失败的监控主机，独立手动开启或者关闭监控状态。

5.同个网站多服务器（负载均衡模式、且每个服务器都部署监控端）情况下，单一服务器维护或宕机会（单一监控端失效）时，需要先手动停止失效的监控端，等服务器正常后，重新进行对要更新的网站数据进行同步。

6. 当用 winscp 重命名文件，恢复日志显示删除和新建日志。系统认为 winscp 工具这种操作是删除和新建事件，属于正常情况。

7. 需要调整系统的正确时间，系统时间变更会影响个别日志输出（时钟变更前后），对业务无影响。