管理控制台使用手册

ieGuard

网页防篡改安全系统

V6.0

云尖（北京）软件有限公司
Cloud point (Beijing) software co., LTD

简介

ieGuard 网页防篡改安全系统 V6.0 管理控制台是基于 B/S 架构设计，支持 http 和 https 连接，支持 ipv4、ipv6 网络协议的管理控制系统。

ieGuard 网页防篡改安全系统 V6.0 管理控制台，由监控台、客户端、站点、同步、用户、操作日志、传输日志、告警日志、授权、邮件设置、系统状态 11 个部分组成。能完成针对于 ieGuard 网页防篡改安全系统 V6.0 的基于网页的简单配置，是管理系统的组成部分。

目录

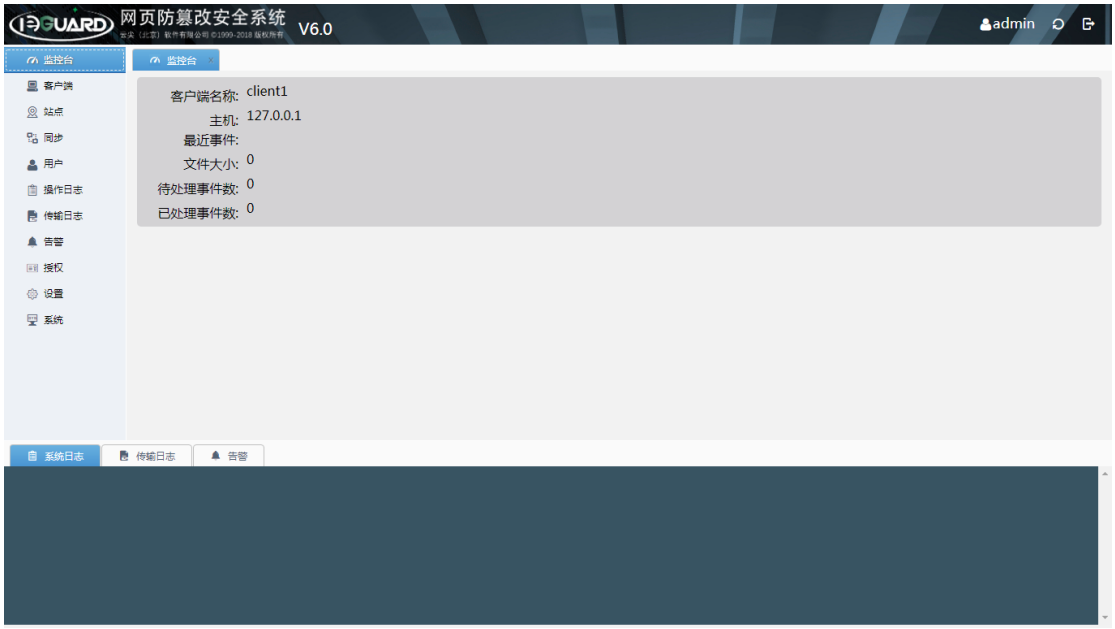
1 管理控制台登录

默认设置的登录端口为 http:9080，https:9443。默认登录方式为 https。
访问地址：https://127.0.0.1:9443
如果地址无法访问，请检查防火墙的设置，并检查服务是否已经正常启动。
默认登录界面如下：

图 1 ieGuard 网页防篡改安全系统 V6.0 控制台登录

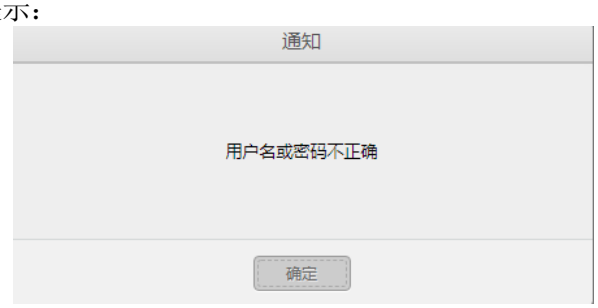
1.1 登录成功

登陆成功后会打开管理控制台，进入到监控台页面，参考监控台。



1.2 登录失败

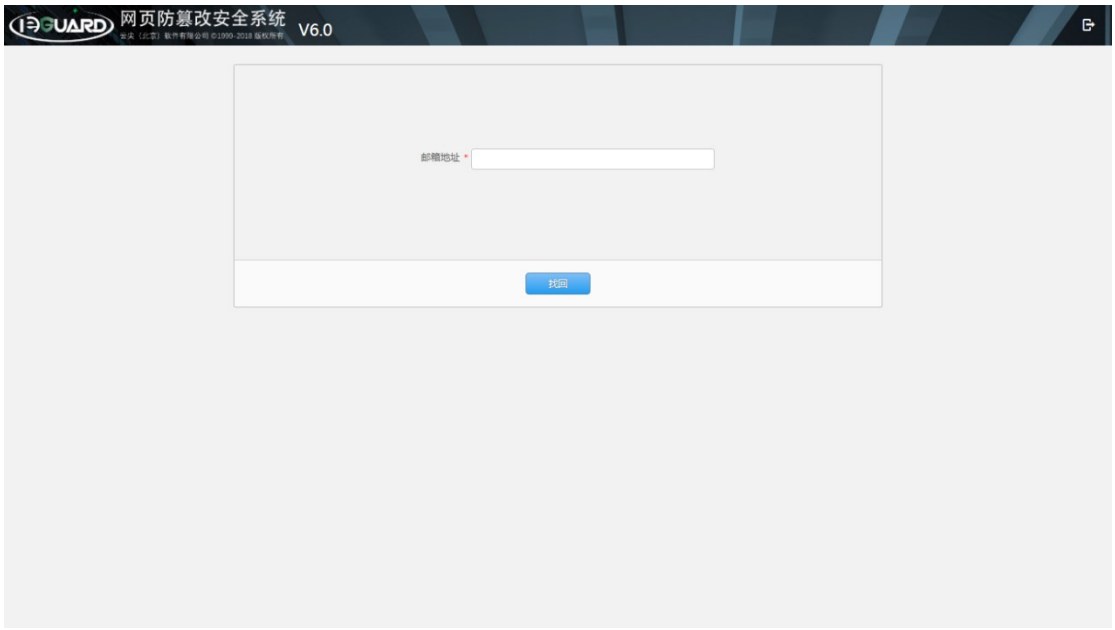
登录失败后会提示：



登录失败 5 次后限制下次允许登录的时间，每次登陆失败时间累计延长 5 秒。

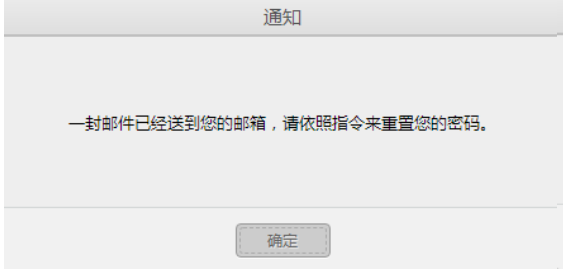
1.3 密码找回

配置正确的代理邮箱后密码找回功能可以正常使用，代理邮箱的配置参考设置。

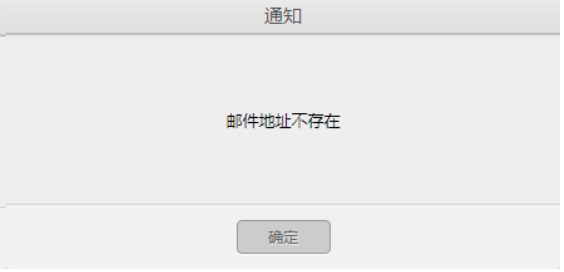


在输入框中输入要找回密码的使用者邮箱。

邮箱正确，发送密码找回邮件



邮箱错误，返回错误信息



2 管理控制台使用

2.1 管理控制台页面结构

管理控制台由五部分组成：

1、产品区：位于显示区域左上角，用于展示产品名称及版本信息；

2、登录区：位于显示区域右上角，用于显示登陆者、重启应用按钮、退出按钮；

3、功能区：位于显示区域左侧中间，用于选择及展示功能控件列表；

4、控件显示区：位于显示区中间，用于显示每个控件的具体信息列表；

5、信息区：位于显示区下方，有 3 组模块组成分别显示时时系统日志、传输日志和告警日志。

2.2 监控台

ieGuard 网页防篡改安全系统 V6.0 成功登录后，首先显示的是监控台页面，在监控台上会显示已经配置完成的所有应用端工作情况。

分别对每台应用端的信息进行详细显示，显示信息内容包括：客户端名称、客户端地址、客户端最新处理事件、事件涉及文件的大小、待处理的事件数量、已处理事件数量。

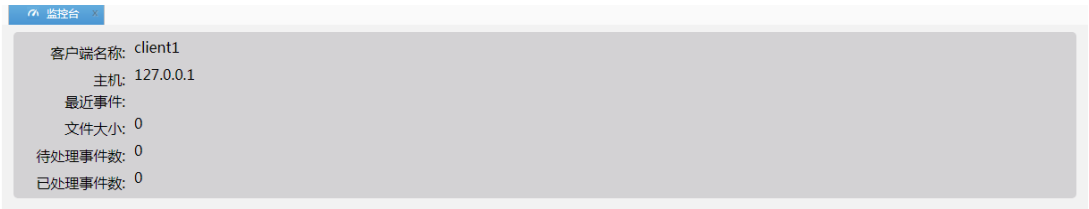
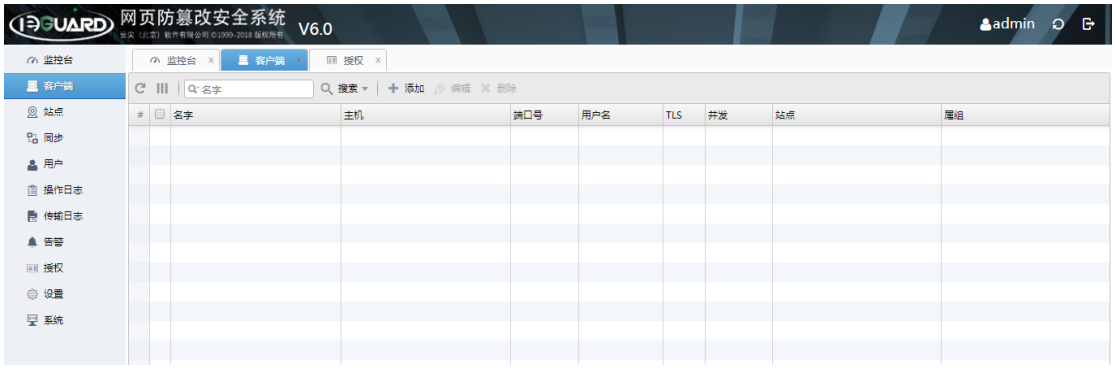


图 2 ieGuard 网页防篡改系统 V6.0 监控台

2.3 客户端

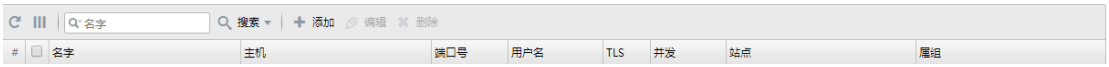
客户端即应用端，是连接管理服务器与应用服务器的唯一凭证。



客户端列表显示客户端的详细连接信息，包括：客户端的名称（名字）、ip 地址（主机）、端口号、用户名、加密传输（TLS）、并发数量（并发）、关联站点（站点）、客户端属于哪一个管理组管理（属组）。

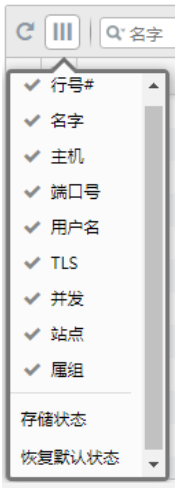
2.3.1 客户端导航

客户端导航包括：刷新、显示、搜索、添加、编辑以及删除选项：

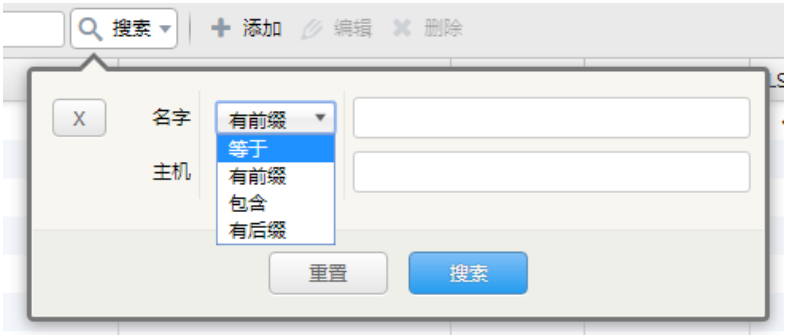


刷新：刷新客户端列表。

显示：在客户端列表中显示并存储可选信息。



搜索：根据名称和主机进行检索。查找并显示主机信息。



搜索包含 4 种匹配方式，完全匹配（等于）、前缀匹配、中间匹配（包含）、后缀匹配。

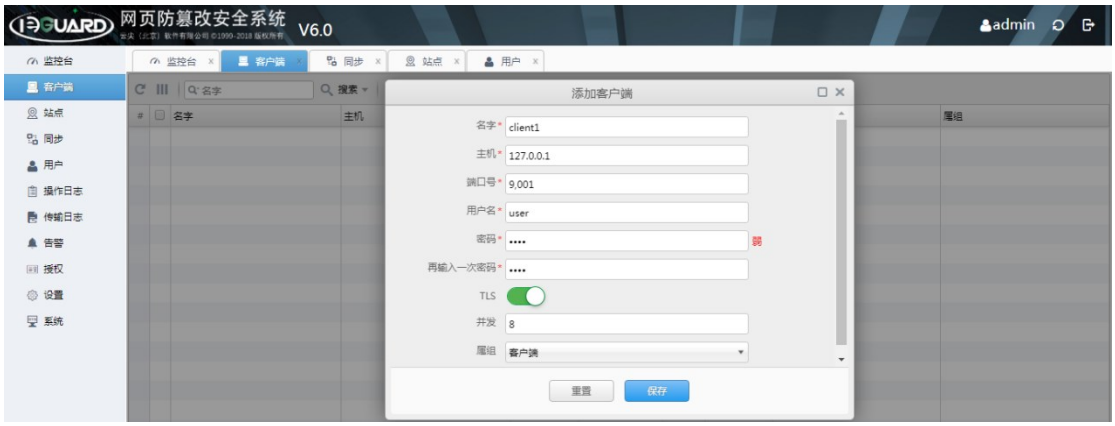
添加：添加新的客户端。

编辑：编辑客户端的信息。（未选择客户端时，此按钮为灰色。）

删除：删除客户端的信息。（未选择客户端时，此按钮为灰色。）

2.3.2 客户端的添加

点击客户端中的添加按钮，会弹出添加客户端对话框，根据应用服务器上 client 端的 app.conf 中配置的应用端名称、网卡 IP、端口号、用户名、密码如实填写。TLS 选项表示默认开启 TLS 加密传输，并发表示文件传输并行队列，属组表示客户端属于哪一用户组管理。添加完成后点击保存按钮进行保存。要使保存的信息生效请点击右上角的重启按钮。



如果点击添加按钮无反应，请参考授权检查产品的授权信息。

2.3.3 客户端的编辑

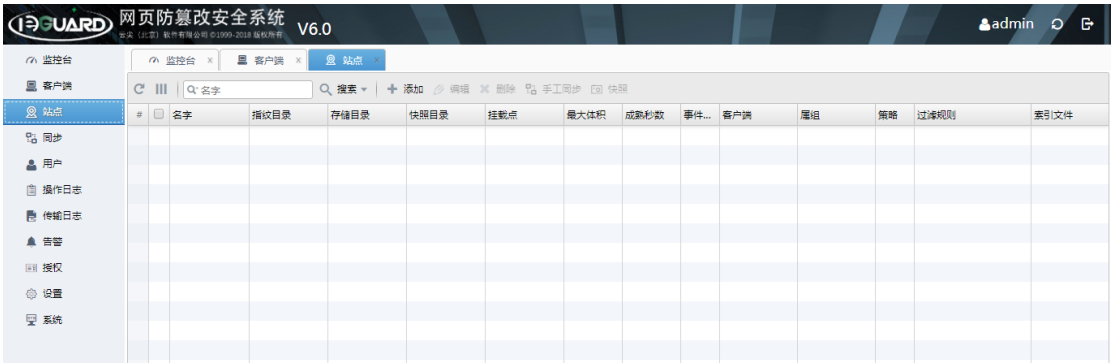
选择要编辑的客户端，点击编辑按钮编辑客户端配置，客户端名称禁止修改，客户端具体配置参考客户端的添加。要使编辑的信息生效请点击右上角的重启按钮。

2.3.4 客户端的删除

选择要删除的客户端，点击删除按钮，弹出“您确定想要删除选定的记录”，选择“是”完成对客户端的删除。删除客户端后，相应的同步策略也将自动删除。要使删除的信息生效请点击右上角的重启按钮。

2.4 站点

站点即要保护的网站内容在管理服务器上的位置。位置以站点为单位，区分每个管理组。站点是管理服务器对网站被保护页面的完整备份，用于数据的传输及恢复，是数据恢复类网页防篡改产品不可缺少的组成部分。

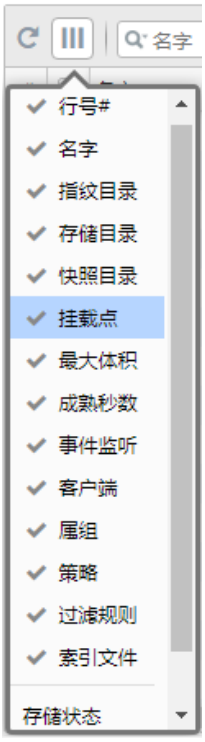


站点列表显示站点的名字、管理端指纹目录、站点存储目录、篡改页面快照目录、站点文件写入目录（挂载点）、文件先期校验对比大小（最大体积）、文件传输等待时间（成熟秒数）、文件发现检查方式（事件监听：与挂载点方式和 ieguardfs 程序不能同时使用）、站点被那些客户端使用（客户端）、站点属于哪一个管理组管理（属组）。全局策略（策略：包括检查与忽略）、与总规则相反的逻辑规则（过滤规则）、站点起始根页面（索引文件）。

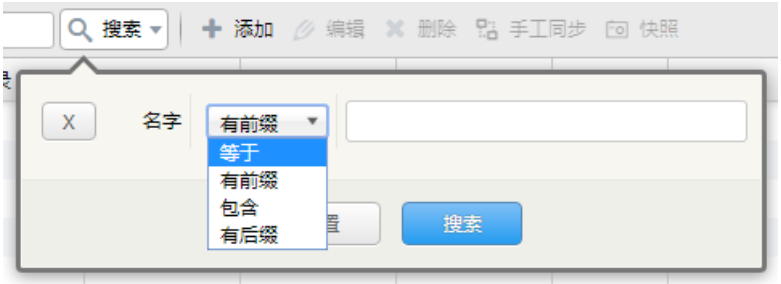
2.4.1 站点导航

站点导航包括：刷新、显示、搜索、添加、编辑、删除、手工同步以及快照选项：

刷新：刷新站点信息列表。
显示：在站点列表中显示并存储可选信息。



搜索：根据站点名字进行检索。查找并显示站点信息。

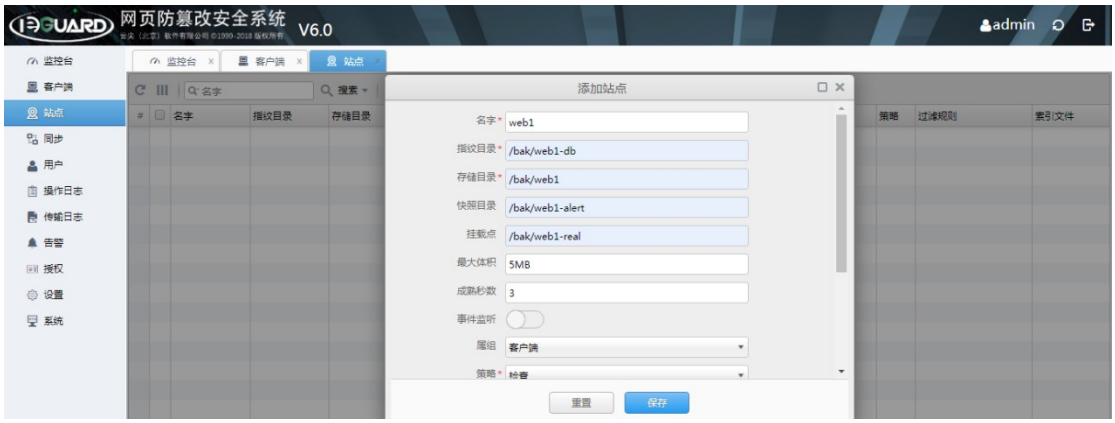


搜索包含 4 种匹配方式，完全匹配（等于）、前缀匹配、中间匹配（包含）、后缀匹配。

添加：添加新的站点。
编辑：编辑站点的信息。未选择站点时，此按钮为灰色。
删除：删除站点的信息。未选择站点时，此按钮为灰色。
手工同步：手动同步站点内的文件到应用端，未选择站点时，此按钮为灰色。详细配置参考站点的手工同步。
快照：本站点的被篡改页面的抓取备份。未选择站点时，此按钮为灰色。

2.4.2 站点的添加

点击站点中的添加按钮，会弹出添加站点对话框，根据管理服务器上站点的存储位置以及站点的目录的相关配置填写。如果使用了 ieguardfs 文件发现插件，请参考 ieguardfs 的 app.conf 配置文件填写。填写完成后点击保存，点击右上角的重启按钮使配置生效。



名称：启用 ieguardfs 着与 ieguardfs 配置文件中的 groups 组中配置的名称一致，如果未启用 ieguardfs 可自命名。

指纹目录：网页文件水印值在管理端备份的位置。不同站点必须区分不同位置。

存储目录：网页文件在管理服务器上存储的真实位置。

快照目录：网页被改文件在管理服务器上的存储位置。不同站点必须区分不同位置。

挂载点：网页文件在管理服务器上的写入位置。启动 ieguardfs 文件发现插件，不需要配置此项。

最大体积：网页文件传输前对比水印的最大大小。默认为 5MB。

成熟秒数：网站文件传输到管理服务器后等待传输到应用服务器的时间默认为 30 秒。

事件监听：文件发现的一种方式，与 ieguardfs 和挂载点为文件发现的可选方式。不能同时使用。

属组：站点所属的被管理组。

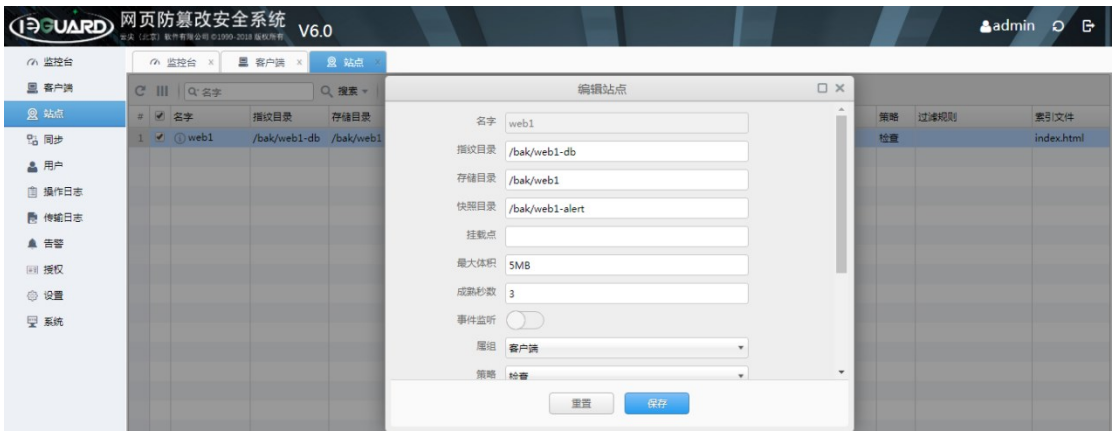
策略：指最基本整体策略级，分为检查和忽略两个级别。当匹配完过滤规则后对文件做的最后一步策略。站点的策略只针对于文件传输，不涉及文件是否保护。

过滤规则：过滤规则是先于基础策略检查的规则组，支持顺序逻辑和通配设置。具体配置参考过滤规则。

索引文件：即站点的跟文件，用于首要恢复的文件起始点。

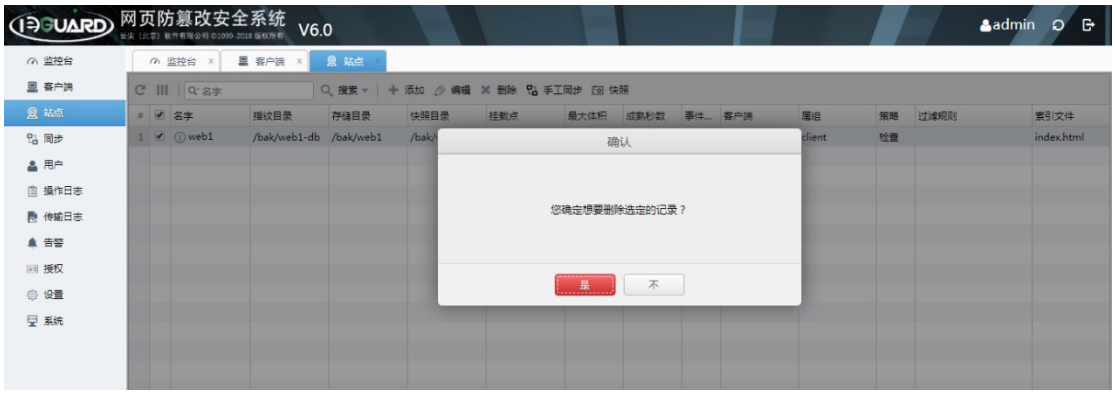
2.4.3 站点的编辑

选择要编辑的站点，点击编辑按钮编辑站点配置，站点名称禁止修改，站点具体配置参考站点的添加。要使编辑的信息生效请点击右上角的重启按钮。



2.4.4 站点的删除

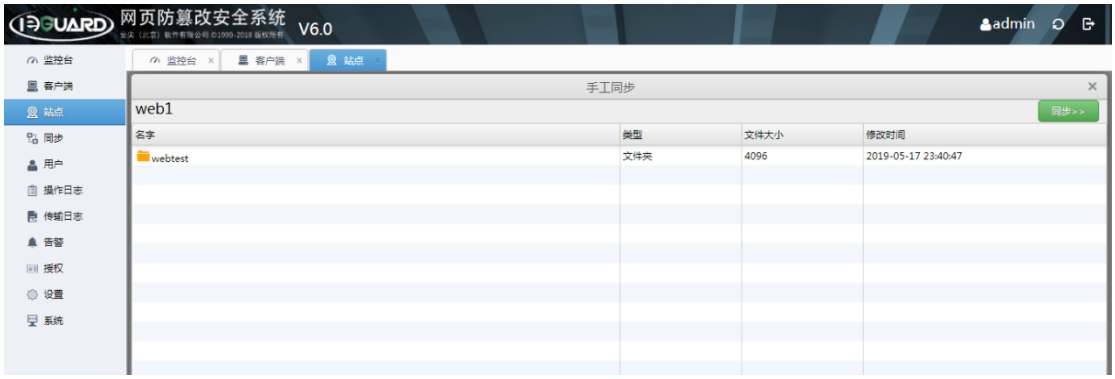
选择要删除的站点，点击删除按钮，弹出“您确定想要删除选定的记录”，选择“是”完成对站点的删除。删除站点后，相应的同步策略也将自动删除。要使删除的信息生效请点击右上角的重启按钮。



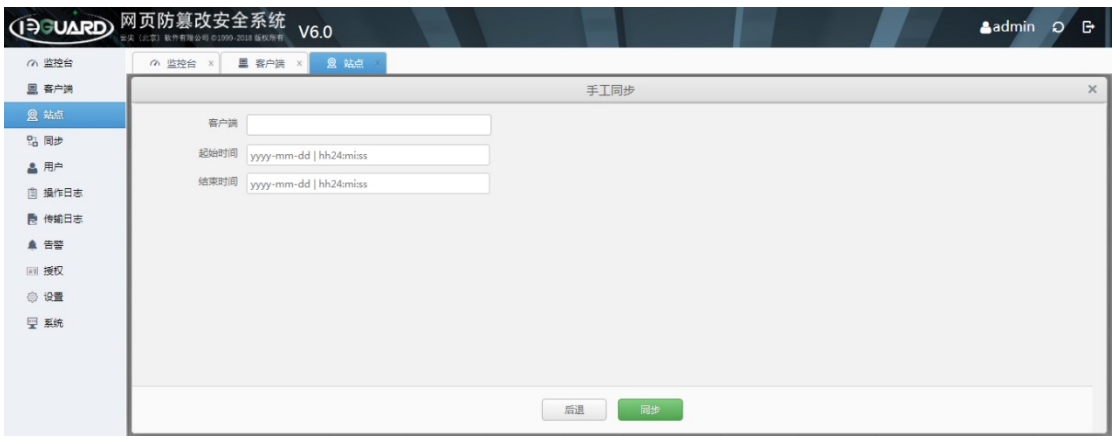
2.4.5 站点的手工同步

站点的手工同步是用于已存在站点的初次配置，以及个别异常情况下，处理紧急文件传输的设置。需配置好同步规则后方可以使用。

选择好站点后，点击手工同步按钮，会弹出“手工同步”框，在手工同步框中列出站点名称以及站点的文件结构，选择好要同步的文件或目录，点击右侧同步按钮。

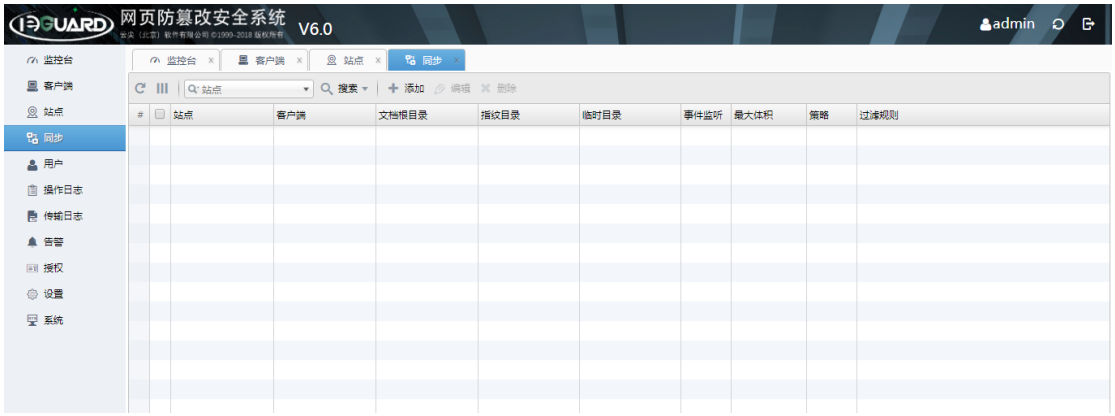


点击同步按钮后，弹出客户端及文件时间选项，选择要同步文件的客户端和文件的建立时间选项，完成按客户端和文件时间进行增量同步文件（不填写表示全部客户端和全部文件）。点击同步按钮进行文件同步。



2.5 同步

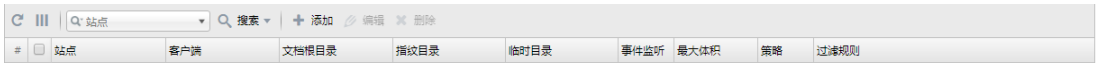
同步是客户端和站点之间的桥梁，起到文件同步传输、配置客户端文件保护逻辑关系及功能的作用。



同步列表显示站点、客户端、客户端文档存储目录（文档根目录）、客户端指纹目录（指纹目录）、客户端文件临时目录（临时目录）、客户端文件保护方式之一（事件监听）、文件二次验证的最大大小（最大体积）、全局策略（策略：包括检查与忽略）、与总规则相反的逻辑规则（过滤规则）。

2.5.1 同步导航

同步导航包括：刷新、显示、搜索、添加、编辑以及删除选项。



刷新：刷新同步列表。

显示：在同步列表中显示并存储可选信息。

搜索：根据站点和客户端进行检索。查找并显示规则信息。

搜索包含只有一种匹配方式，完全匹配（等于）。

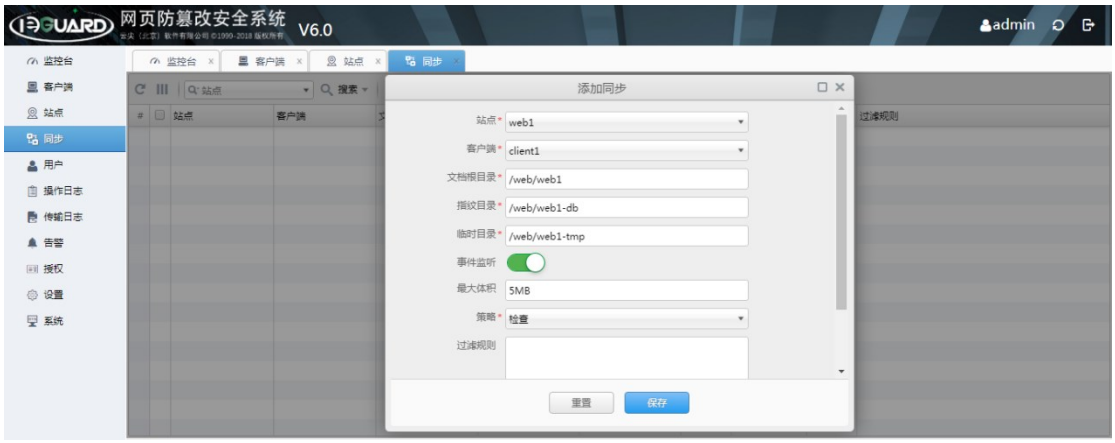
添加：添加新的同步规则。

编辑：编辑同步的信息。（未选择同步规则时，此按钮为灰色。）

删除：删除同步的信息。（未选择同步规则时，此按钮为灰色。）

2.5.2 同步的添加

点击同步中的添加按钮，会弹出添加同步对话框，选择或填写对应的站点及客户端名称，支持首字符段筛选提示，并完成文档根目录、指纹目录、临时目录、过滤规则等的填写，完成后点击保存，点击右上角的重启按钮使配置生效。



站点：要传输到应用服务器的站点，必须保证在站点中存在的名称。

客户端：站点要传输到的应用服务器客户端，须保证在客户端配置中已存在。

文档根目录：应用服务器要发布的网站的目录。

指纹目录：应用服务器存储的网页的水印值目录。

临时目录：用于在网站文件传输过程中，文件完整性缓存目录。文件传输完成后才会由缓存目录覆盖到文档根目录。

事件监听：网站网页防篡改的一种检查方式。

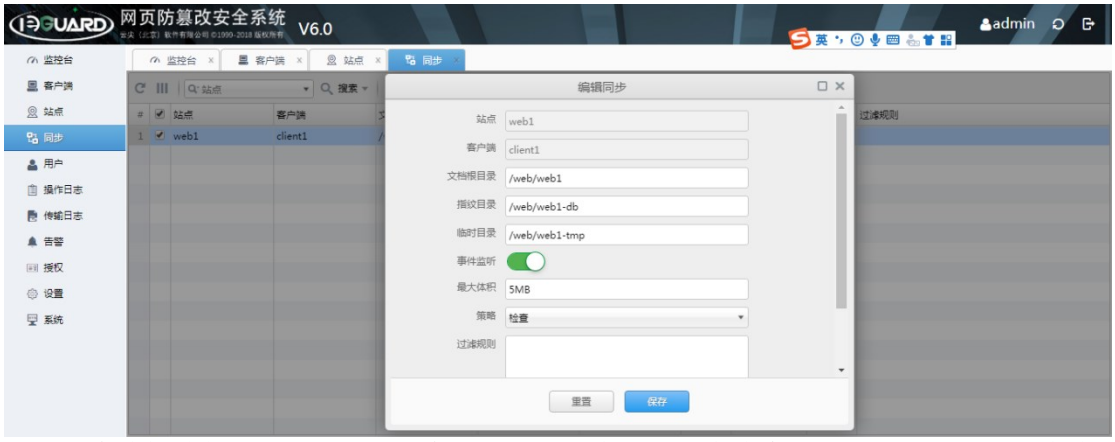
最大体积：二次校验文件的最大大小。

策略：指最基本整体策略级，分为检查和忽略两个级别。当匹配完过滤规则后对文件做的最后一步策略。同步的策略只针对于文件保护，不涉及文件是否传输。

过滤规则：过滤规则是先于基础策略检查的规则组，支持顺序逻辑和通配设置。具体配置参考过滤规则。

2.5.3 同步的编辑

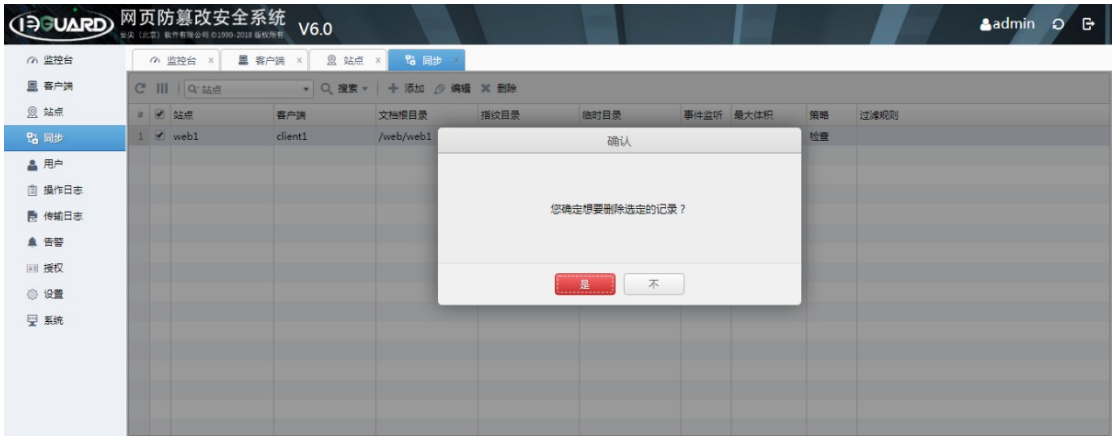
选择要编辑的同步规则，点击编辑按钮，编辑同步规则，站点和客户端的匹配规则禁止修改，同步具体配置参考同步的添加。要使编辑的信息生效请点击右上角的重启按钮。



同步编辑功能主要用于应用服务器相关站点发布目录发生变化或相应的匹配规则发生变化而变化，要根据站点的实际情况配置修改。

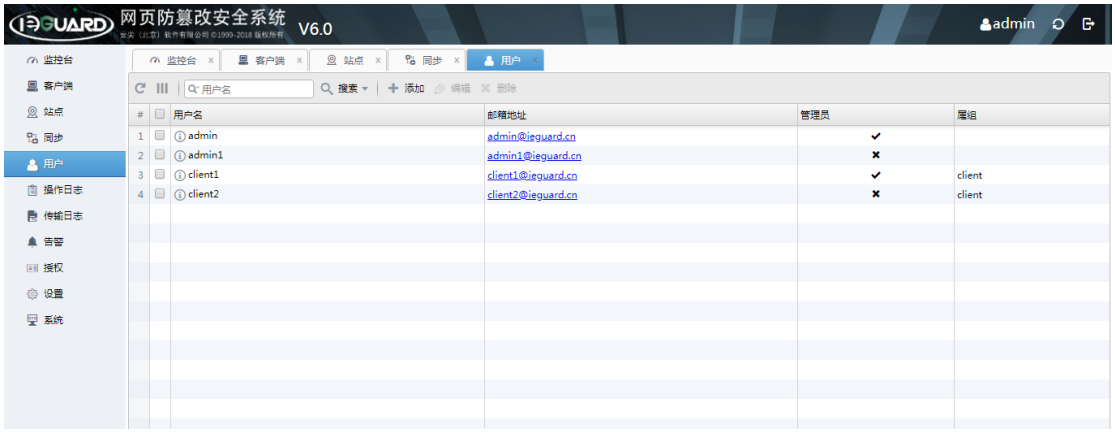
2.5.4 同步的删除

选择要删除的同步规则，点击删除按钮，弹出“您确定想要删除选定的记录”，选择“是”完成对同步规则的删除。删除同步规则后，相应的客户端和站点的匹配关系也将自动清除，客户端网站目录将不再受到保护和自动更新。要使删除的信息生效请点击右上角的重启按钮。



2.6 用户

控制台登录用户分为四种：全站管理员、全站审查员、属组管理员和属组审查员。
全站管理员：可以进行全部站点的配置及管理，可管理所有用户。（admin）
全站审查员：可以对全站的数据进行查看及审计。（admin1）
属组管理员：可以查看、管理本属组的全部站点配置和用户。（client1）
属组审查员：可以对本属组的数据进行审计。（client2）



用户列表显示用户名、邮箱地址、是否为管理员、属组。

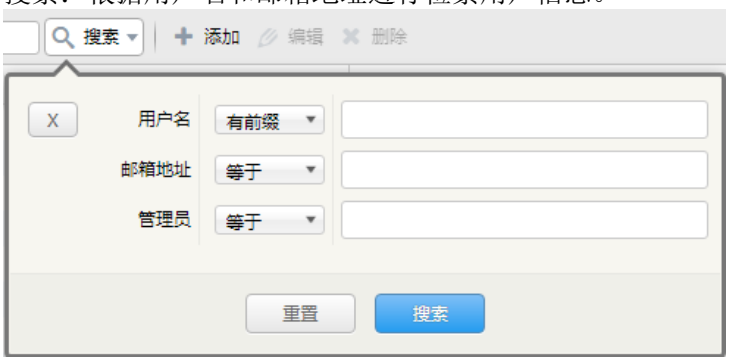
2.6.1 用户导航

用户导航包括：刷新、显示、搜索、添加、编辑以及删除选项。

刷新：刷新用户列表。

显示：在用户列表中显示并存储可选信息。

搜索：根据用户名和邮箱地址进行检索用户信息。



搜索包含 4 种匹配方式，完全匹配（等于）、前缀匹配、中间匹配（包含）、后缀匹配。

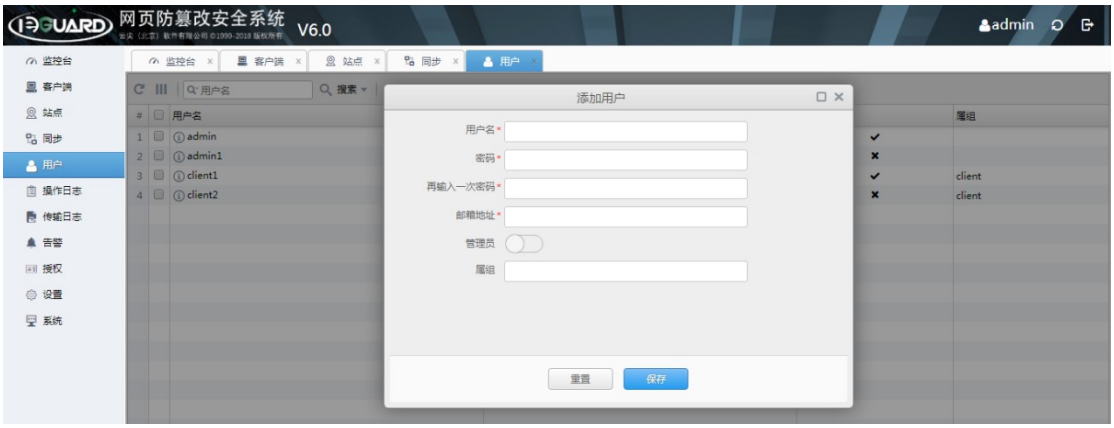
添加：添加新的用户。

编辑：编辑用户信息。（未选择用户时，此按钮为灰色。）

删除：删除用户信息。（未选择用户时，此按钮为灰色。）

2.6.2 用户的添加

点击用户中的添加按钮，会弹出添加用户对话框，在用户名中输入要填写的用户名称，依次填写密码、密码确认、邮箱地址（用于密码找回）是否属于管理员，是否属于组名称，完成后点击保存使配置生效。



用户名：用户的登录名称；

密码：用户的登录密码；

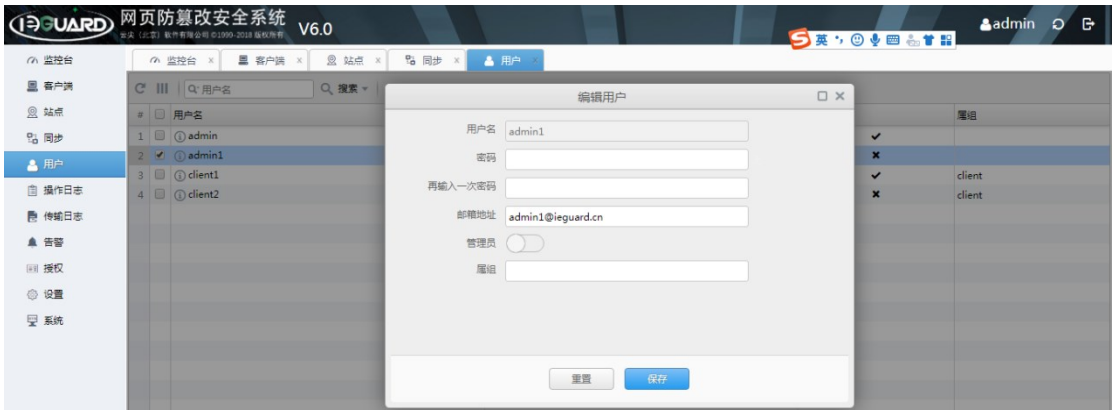
邮箱地址：用于用户的密码找回；

管理员选项：用于配置用户是否具有管理员权限；

属组：用户所属的组，全站管理属组配置为空。

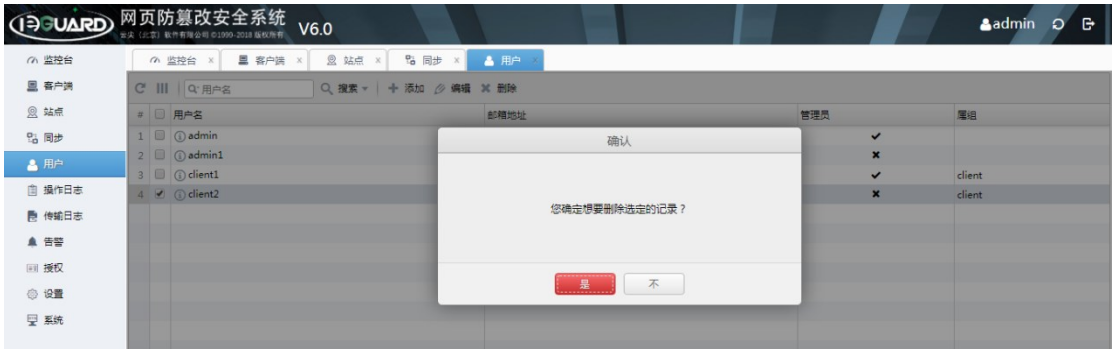
2.6.3 用户的编辑

选择要编辑的用户，点击编辑按钮编辑用户，可重置用户密码、用户邮箱，调整属组。具体配置参考用户的添加。



2.6.4 用户的删除

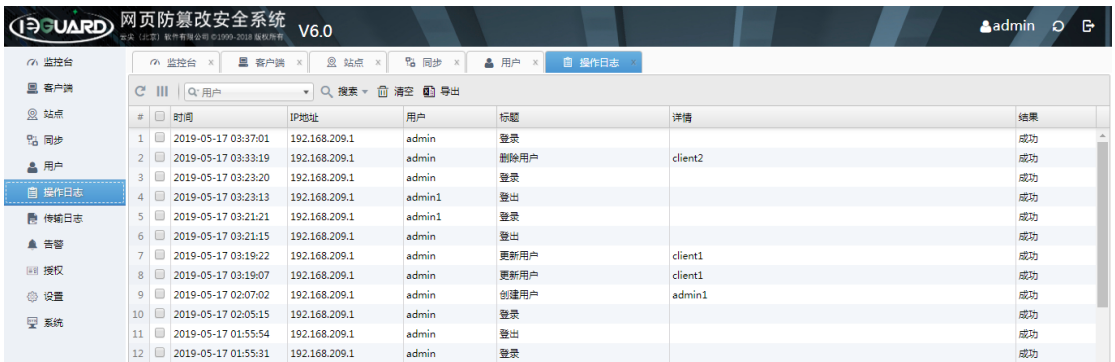
选择要删除的用户，点击删除按钮，弹出“您确定想要删除选定的记录”，选择“是”完成对用户的删除。



用户删除是不可逆的，删除时需谨慎。

2.7 操作日志

操作日志是系统记录的所有人员的在管理控制台上操作的日志信息。操作日志的审计内容包括操作的服务器时间、操作的 IP 地址、操作的用户、操作的种类、操作的具体内容、操作是否成功。

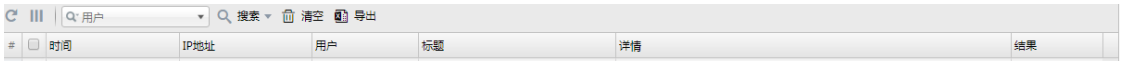


#	时间	IP地址	用户	标题	详情	结果
1	2019-05-17 03:37:01	192.168.209.1	admin	登录		成功
2	2019-05-17 03:33:19	192.168.209.1	admin	删除用户	client2	成功
3	2019-05-17 03:23:20	192.168.209.1	admin	登录		成功
4	2019-05-17 03:23:13	192.168.209.1	admin1	登出		成功
5	2019-05-17 03:21:21	192.168.209.1	admin1	登录		成功
6	2019-05-17 03:21:15	192.168.209.1	admin	登出		成功
7	2019-05-17 03:19:22	192.168.209.1	admin	更新用户	client1	成功
8	2019-05-17 03:19:07	192.168.209.1	admin	更新用户	client1	成功
9	2019-05-17 02:07:02	192.168.209.1	admin	创建用户	admin1	成功
10	2019-05-17 02:05:15	192.168.209.1	admin	登录		成功
11	2019-05-17 01:55:54	192.168.209.1	admin	登出		成功
12	2019-05-17 01:55:31	192.168.209.1	admin	登录		成功

此信息用于审计是不允许单独删除某一条或几条的。操作日志的保存天数在设置中设置。

2.7.1 操作日志导航

操作日志导航包括：刷新、显示、搜索、清空以及导出选项。



刷新：刷新操作日志列表。

显示：在操作日志列表中显示并存储可选信息。

搜索：根据时间段、用户名和执行结果进行检索操作信息。

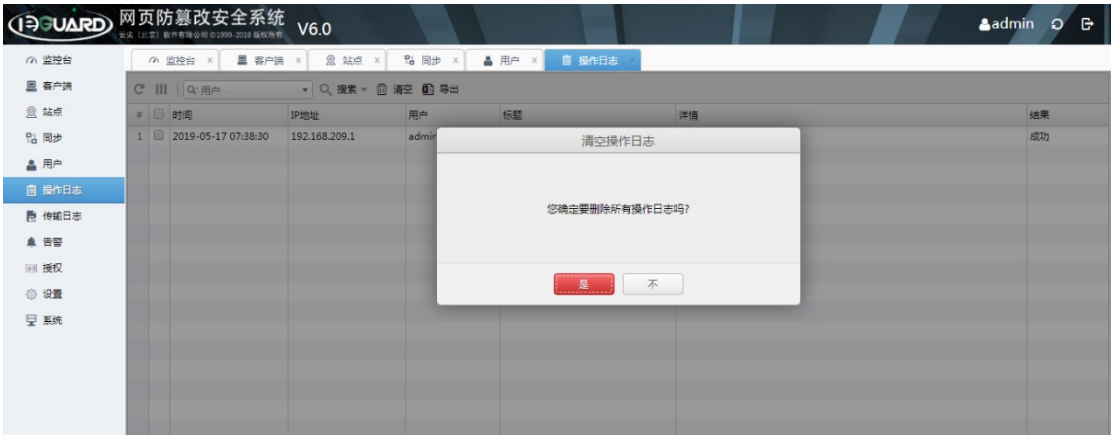
搜索包含只有一种匹配方式，完全匹配（等于）。

清空：清空全部操作日志，记录最后清空者信息。

导出：导出全部日志用于审计。

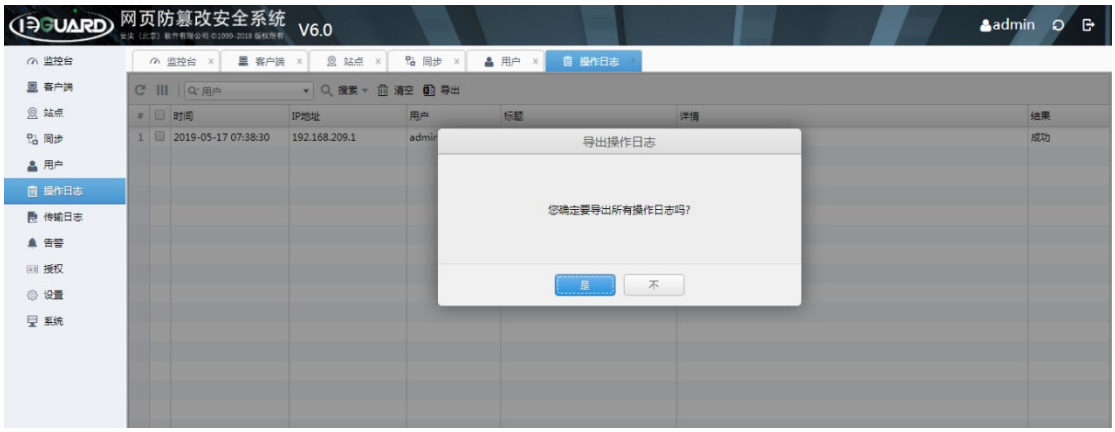
2.7.2 操作日志的清空

根据审计要求操作日志必须保证日志连贯性不支持单独删除事件，点击清空按钮，弹出“清空操作日志”对话框，选择“是”可清空整个操作事件，并记录清空者信息。



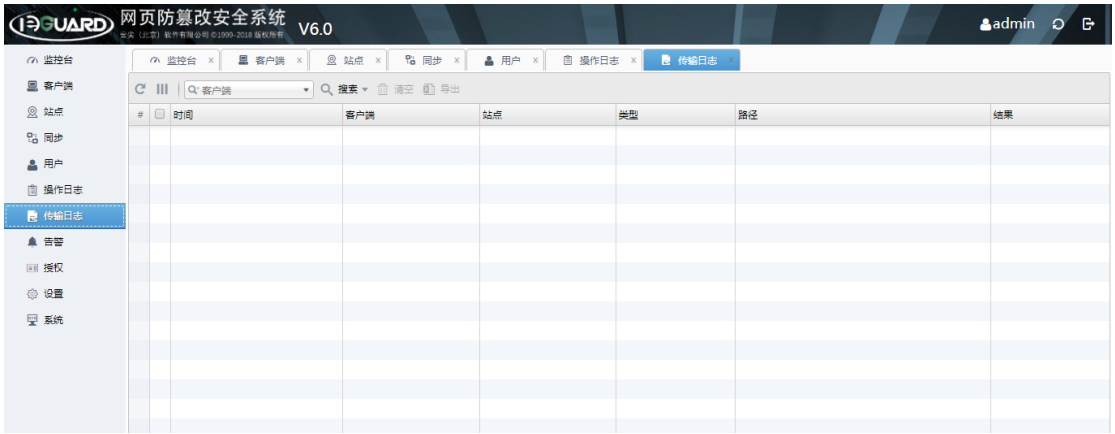
2.7.3 操作日志的导出

要导出操作日志，点击导出按钮，弹出“导出操作日志”对话框，选择“是”导出操作日志。导出的操作日志格式为 csv 格式，默认命名规则是 ieGuard 操作日志_“时间”.csv，选择存储路径进行存储。



2.8 传输日志

传输日志是系统记录所有文件动作的日志信息。传输日志的审计内容包括操作的服务器时间、客户端名称、站点名称、操作的动作类型（新建、删除等）、操作的文件信息（路径）、操作是否成功（结果）。



此信息用于审计是不允许单独删除某一条或几条的。传输日志的保存天数与操作日志的保存天数一致，在设置中设置。

2.8.1 传输日志导航

传输日志导航包括：刷新、显示、搜索、清空以及导出选项。

刷新：刷新传输日志列表。

显示：在传输日志列表中显示并存储可选信息。

搜索：根据时间段、用户名和执行结果进行检索操作信息。

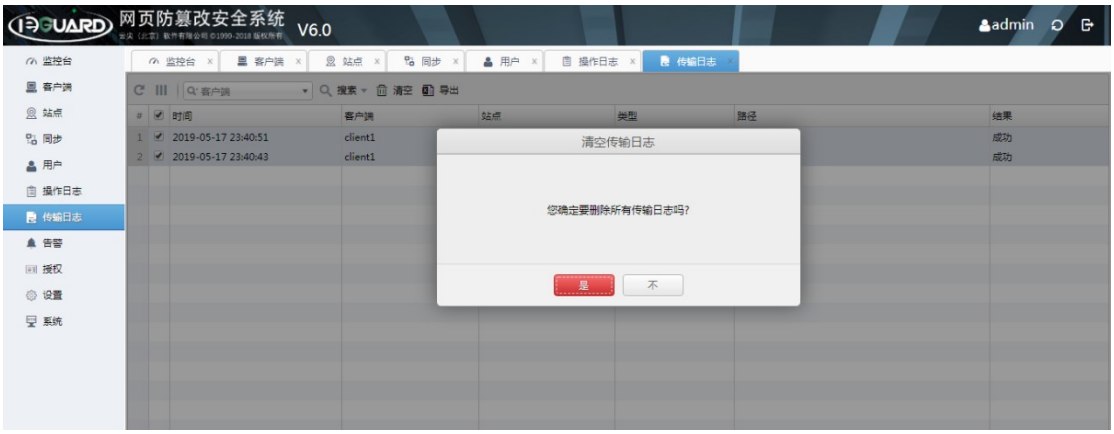
搜索包含只有一种匹配方式，完全匹配（等于）。

清空：清空全部操作日志，记录最后清空者信息。

导出：导出全部日志用于审计。

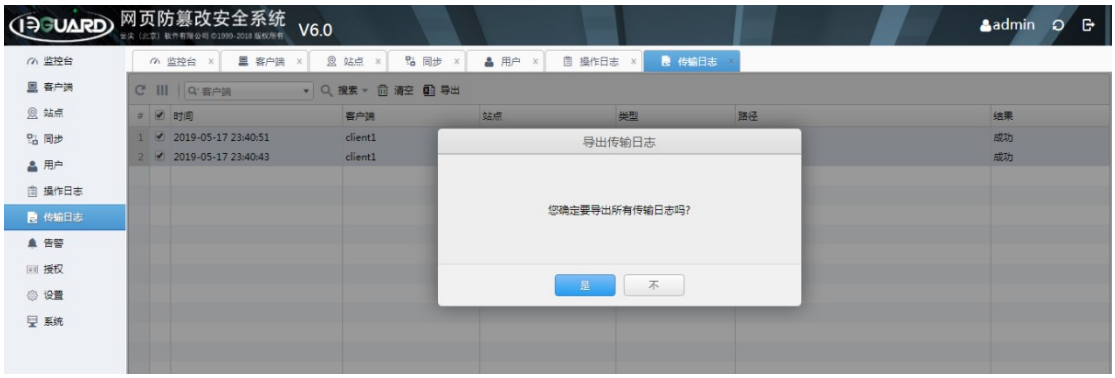
2.8.2 传输日志的清空

根据审计要求传输日志必须保证日志连贯性，不支持单独删除事件，点击清空按钮，弹出“清空传输日志”对话框，选择“是”可清空整个传输信息。



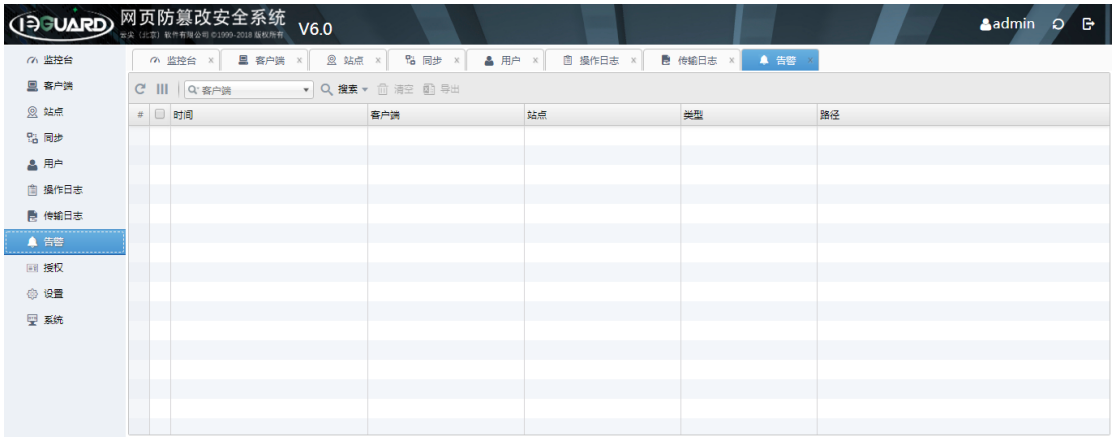
2.8.3 传输日志的导出

要导出传输日志，点击导出按钮，弹出“导出传输日志”对话框，选择“是”导出传输日志。导出的传输日志格式为 csv 格式，默认命名规则是 IEGuard 传输日志_“时间”.csv，选择存储路径进行存储。



2.9 告警

告警是系统记录所有异常信息的日志信息。告警日志的审计内容包括操作的服务器时间、客户端名称、站点名称、操作的动作类型（新建、删除等）、操作的文件信息（路径）。



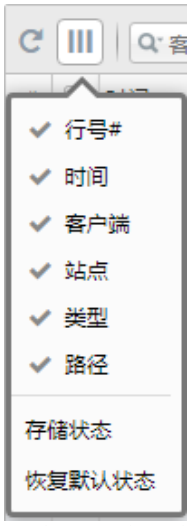
告警信息用于审计是不允许单独删除某一条或几条的。告警的保存天数与操作日志的保存天数一致，在设置中设置。

2.9.1 告警导航

告警导航包括：刷新、显示、搜索、清空以及导出选项。

刷新：刷新告警列表。

显示：在告警列表中显示并存储可选信息。



搜索：根据时间段、客户端、站点和事件类型进行检索操作信息。

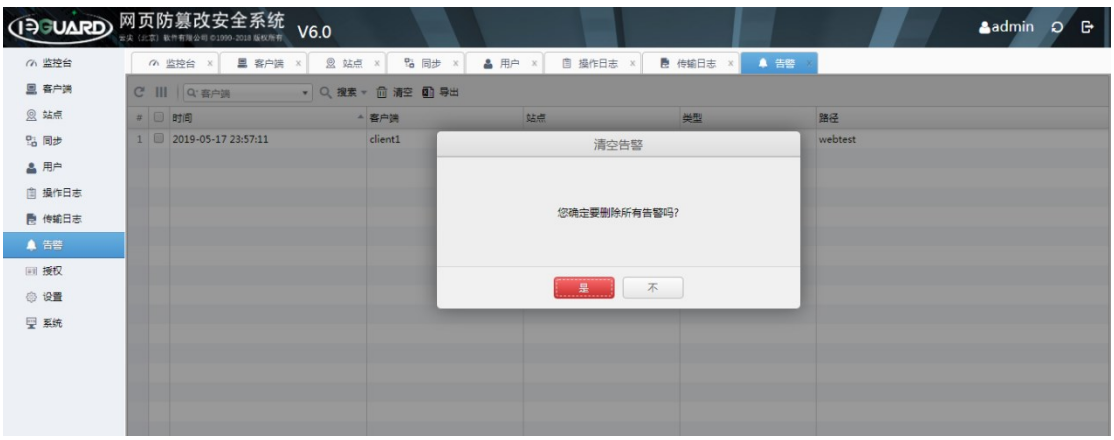
搜索包含只有一种匹配方式，完全匹配（等于）。

清空：清空全部告警。

导出：导出全部日志用于审计。

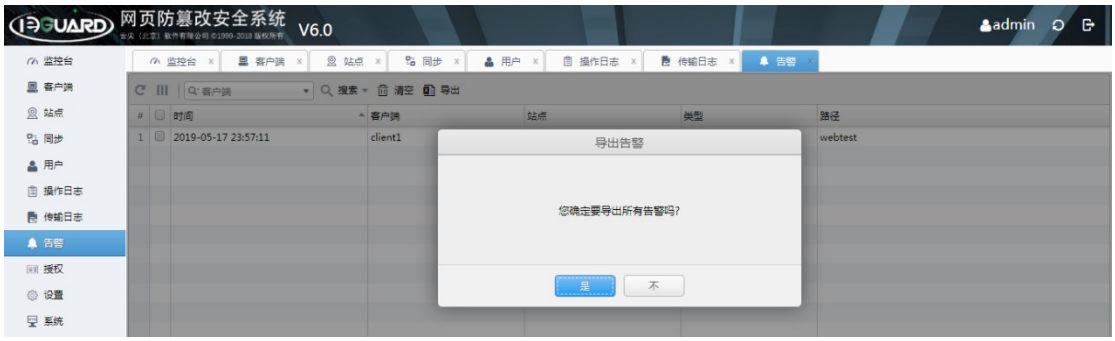
2.9.2 告警的清空

根据审计要求告警必须保证日志连贯性，不支持单独删除事件，点击清空按钮，弹出“清空告警”对话框，选择“是”可清空整个告警信息。



2.9.3 告警的导出

要导出告警信息，点击导出按钮，弹出“导出告警”对话框，选择“是”导出告警。导出的告警日志格式为 csv 格式，默认命名规则是 IEGuard 告警_“时间”.csv，选择存储路径进行存储。

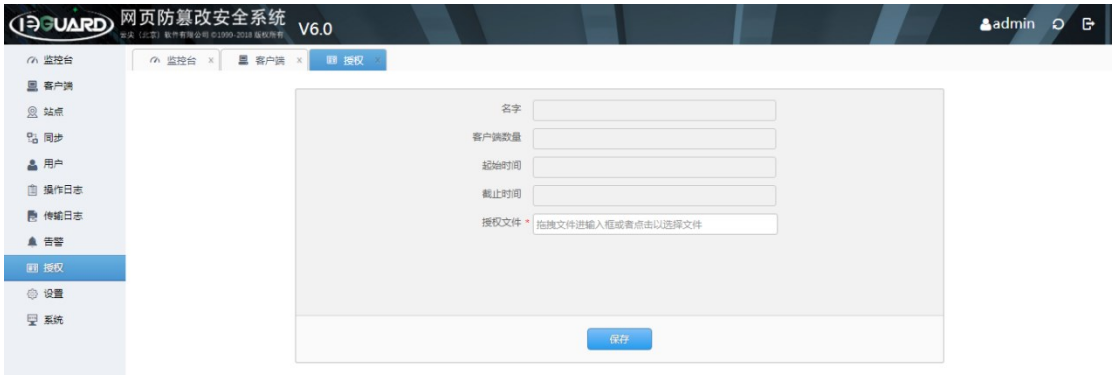


2.10 授权

首次登陆管理控制台，授权显示为空，这时您将无法对管理控制台的客户端进行添加配置，需要导入授权文件对产品进行授权（如无授权文件，请联系厂商销售代表获取授权）。

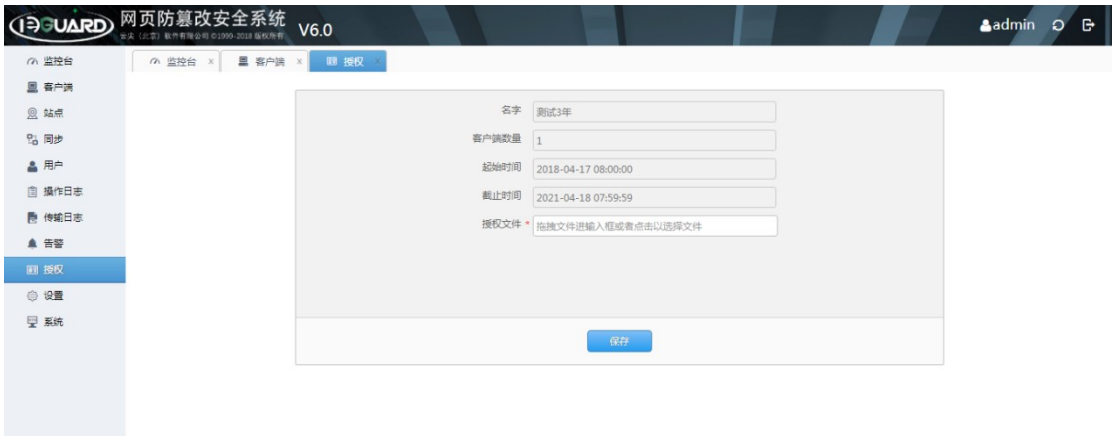
2.10.1 授权页面的显示

授权页面包含信息：授权用户的名称（名字）、授权支持的最大客户端数量（客户端数量）、授权时间（起始时间和截止时间）和授权导入功能。



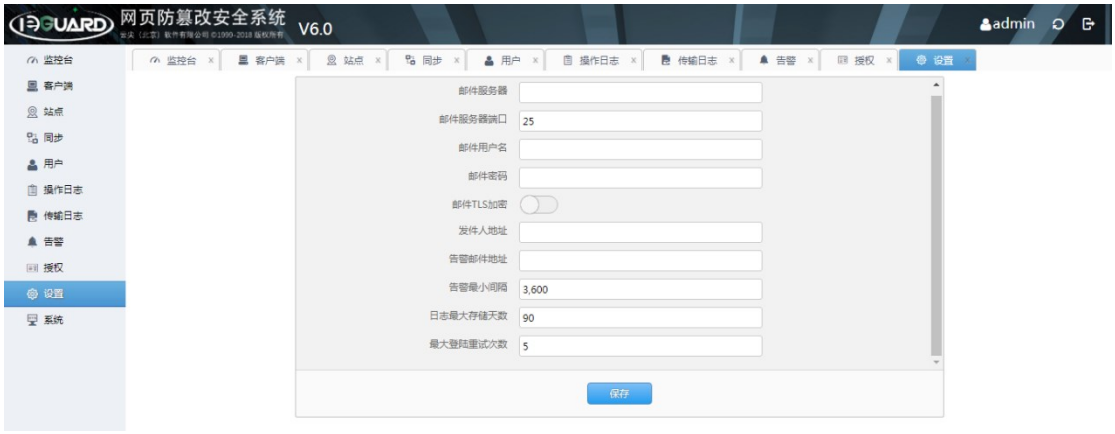
2.10.2 授权的导入

点击授权文件框，选择授权文件的位置或直接将授权文件拖拽到框内，点击保存。保存完成后会显示对应的授权信息。



2.11 设置

设置页面是针对产品基础的一些基本设置，主要用于设置邮件服务器的配置、告警信息配置和登录的配置。

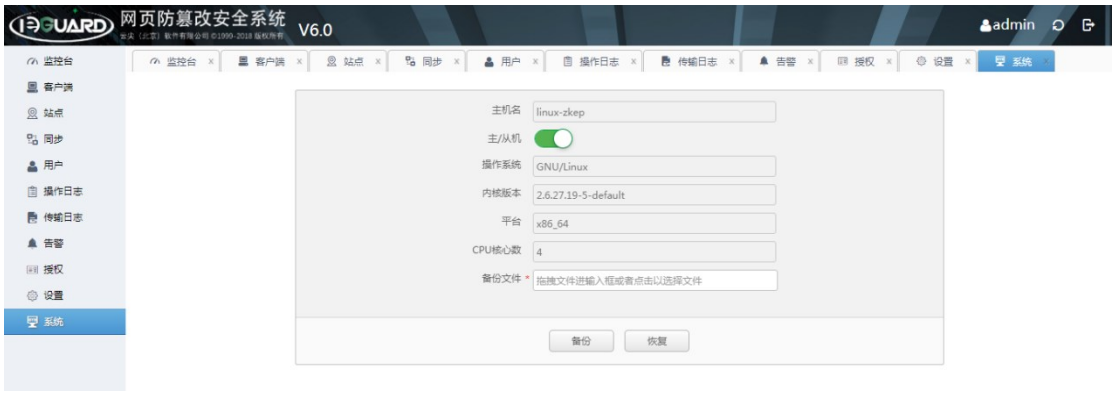


邮件服务器的设置参考转发邮箱设置，主要用于发送用户找回密码和网页被改信息告警。　　日志的保存天数默认为 90 天。 登录密码重试次数默认为 5 次。

2.12 系统

系统页面主要显示管理服务器信息，包括主机名、是否为工作状态（绿色为工作状态，灰色为不工作状态）、主机的操作系统、内核版本、平台架构、CPU 内核数量。

备份文件是对整个管理平台的当前配置状态进行备份。点击备份即备份整个管理服务器信息，选择备份文件导入即可恢复全部管理服务器配置信息。



3 管理控制台设置

3.1 过滤规则设置

在某些特定的站点上，需要设置与基础规则相反的配置规则，如某个站点文件目录中有些文件或目录不想传输到客户端应用服务器上，或者客户端的客户应用中有部分目录需要忽略保护着。需要配置对应的过滤规则。

过滤规则配置主要出现在站点和同步的配置中，站点的过滤规则表示文件是否进行传输，同步的过滤规则表示文件是否进行保护。

策略是规则的基础包括检查和忽略。过滤规则是基础规则的补充，优于规则项，按照从上到下的顺序进行逻辑匹配。

忽略规则支持*通配符。如文件类别忽略 *.avi ，目录忽略 upload/*。

3.1.1 过滤规则的添加

点击过滤规则弹出过滤规则添加对话框，选择规则模式是否忽略。填写需要添加的匹配规则。点击添加按钮添加匹配规则，添加完成的过滤规则会在规则前端出现 3 个按钮，分别表示规则的删除、向下调整和向上调整，点击保存，保存整体规则，点击右上角重启按钮使规则生效。

3.1.2 过滤规则的调整

添加完成的过滤规则会在规则前端出现 3 个按钮，点击上下箭头按钮调整规则顺序。

3.1.3 过滤规则的删除

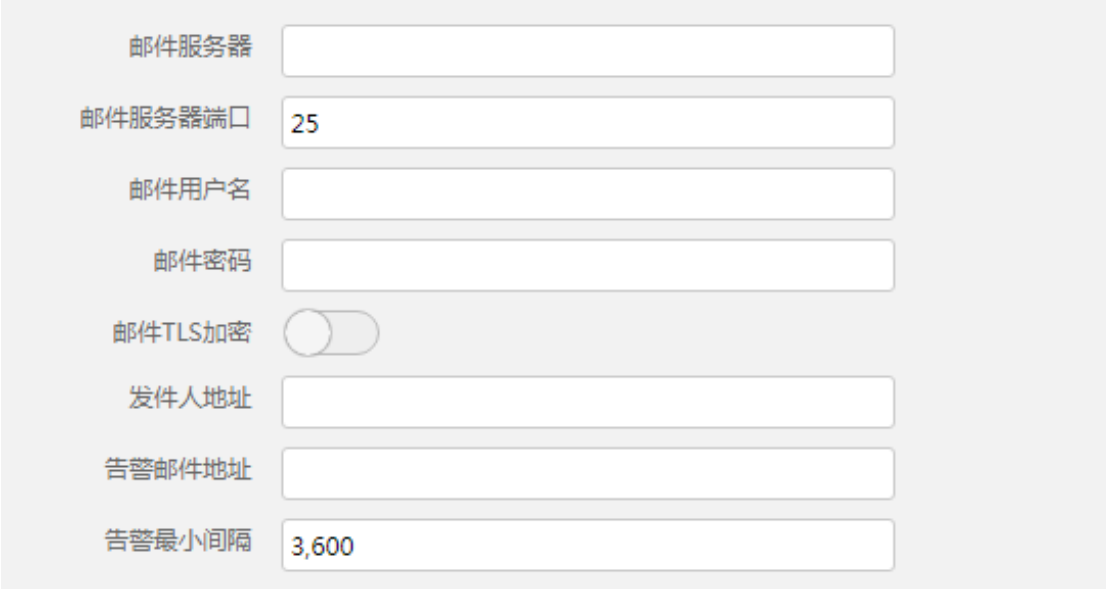
点击 x 按钮删除规则。

3.2 转发邮箱设置

管理平台邮箱设置是在管理控制台设置项中进行设置。

管理平台对外发送邮件使用的方式是，通过 SMTP 方式登录到配置好的邮件服务器，通过邮件服务器向外发送邮件，这样需要配置对应邮件服务器的信息，邮件设置要根据邮件服务提供商提供的配置信息进行配置，具体配置如下信息：

1、邮件服务器的名称：例如 139 邮箱 smtp.139.com；
2、邮件服务器的端口：例如 139 邮箱 25 ；
3、使用的发件人邮箱用户名：139******* （手机号）；
4、邮箱登录密码：********；
5、邮件 TLS 加密：（如需使用加密邮件，需按照邮件服务器提供商提供的加密配置方式配置上面 1-4 行）；
6、发件人地址：收件者邮件显示的发件人地址信息；
7、告警邮件地址：收件人地址；
8、告警最小间隔：表示两封邮件之间的时间差以秒为单位。默认是 1 小时。



发送邮件要保证管理服务器能访问到邮件服务提供商提供的邮件服务器地址。某些邮件服务提供商需要在邮箱中开启响应的服务设置。

如 139 邮箱：

服务器地址：

	地址	端口（不带SSL）	端口（带SSL）
POP3服务器	pop.139.com	110	995
SMTP服务器	smtp.139.com	25	465
IMAP服务器	imap.139.com	143	993

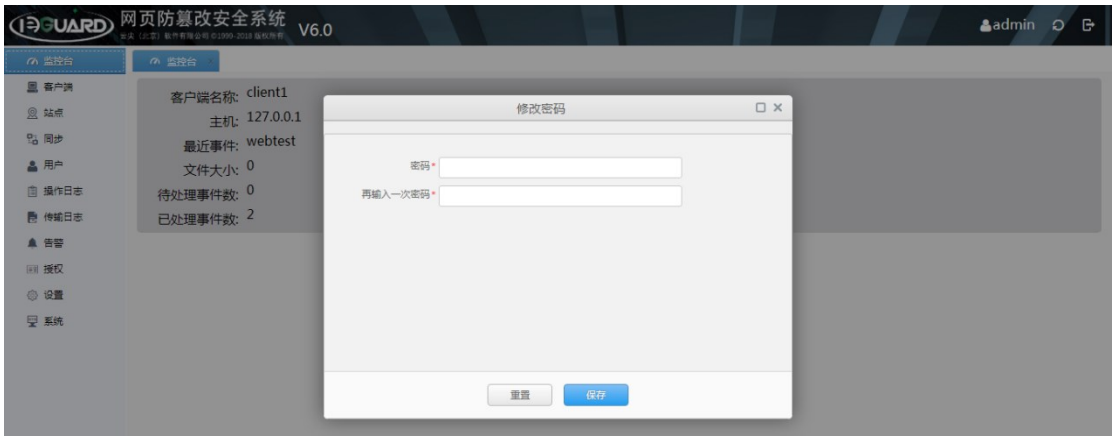
密码设置

3.2.1 密码修改

管理控制台用户的密码修改分为用户自行修改和有权限的管理员修改。

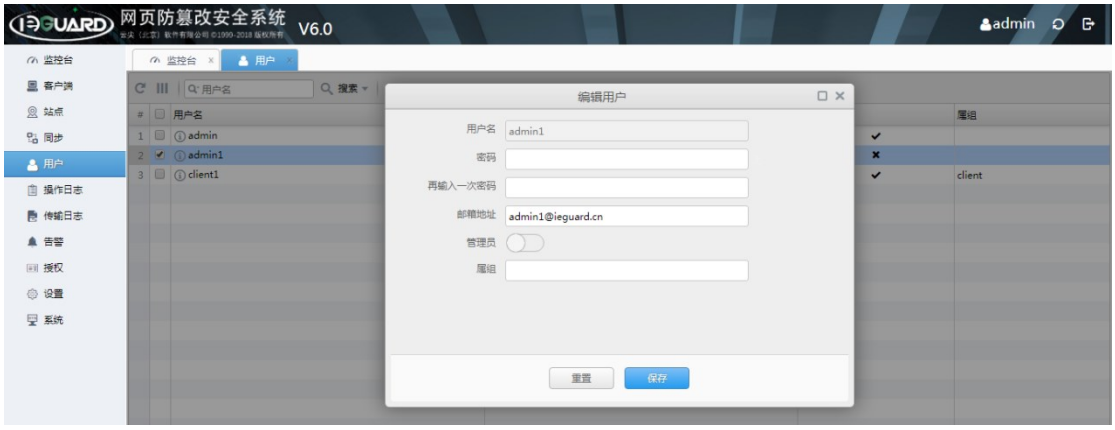
✎ 用户自行修改

用户登录到管理控制台后，点击右上角用户名称，出现修改密码提示，进入修改密码提示框，输入新的用户名密码，点击保存按钮保存新的密码。



✎ 管理员帮助修改密码

管理员可通过用户选项点击用户，编辑用户密码，编辑完成点击保存按钮，保存用户信息。参考用户的编辑。



3.2.2 密码复杂度强制认证设置

在管理控制台输入密码都会显示密码的强弱，当需要配置相关的密码强度等级强制认证时，修改下述文件可达到对应功能模块的密码强度要求。此配置属于强制认证，只能在管理服务器内部设置不能通过管理控制台进行配置。在修改配置前请确保全站管理员密码已经符合相对应强度。

static/user.html 用户页面密码强度设置。

static/reset_password_main.html 密码重置页面密码强度设置。

static/top.html 密码管理页面密码强度设置。

强度等级定义的字段为：“minStrength: ”字段。

密码强度等级为 5 级，包括弱，中，强，好和完美，默认设置密码为弱。

minStrength: 'weak',、'medium',、'strong ',、'good ',、'perfect ',。选择一种进行配置。

4 管理控制台信息

在管理控制台下方有 3 个显示模块，分别对应系统日志、传输日志和告警，显示内容更精确。

4.1 管理控制台系统日志

系统日志显示内容除了用于审计的操作日志外，还显示相关的系统调用日志和错误信息。有明显的颜色区分。方便及时发现问题。

4.2 管理控制台传输日志

传输日志显示内容与用于审计的传输日志一致。有明显的颜色区分。方便及时发现问题。

4.3 管理控制台告警

告警显示内容与用于审计的告警信息一致。有明显的颜色区分，方便及时发现问题。