伟思信安

边界接入平台探针监控管理系统 V3.0

使用说明书

**珠海经济特区伟思有限公司**

**2021年11月﹒珠海**

目录

[1 系统简介 1](#_Toc25459)

[1.1 产品定位 1](#_Toc23776)

[1.2 产品形态 1](#_Toc17784)

[2 运行环境 2](#_Toc11334)

[2.1 硬件运行信息 2](#_Toc30859)

[2.1.1 温度/湿度要求 2](#_Toc10847)

[2.1.2 纯净度要求 2](#_Toc18149)

[2.1.3 防静电要求 2](#_Toc14719)

[2.2 软件运行信息 3](#_Toc11936)

[3 安装部署 3](#_Toc14364)

[3.1 前置工作 3](#_Toc12795)

[3.2 设备上架 3](#_Toc20121)

[3.3 系统部署检查 3](#_Toc12926)

[4 业务操作指南 4](#_Toc4165)

[4.1 登录管理 4](#_Toc30333)

[4.1.1 准备工作 4](#_Toc12637)

[4.1.2 管理方式 4](#_Toc13206)

[4.1.3 Web页面管理 5](#_Toc25108)

[4.1.4 SSH管理 5](#_Toc3598)

[5 系统功能 5](#_Toc7921)

[5.1 系统登录 5](#_Toc15429)

[5.2 系统监管 6](#_Toc2305)

[5.3 用户管理 7](#_Toc13974)

[5.3.1 安全配置 8](#_Toc11436)

[5.4 系统配置 9](#_Toc24409)

[5.4.1 时间管理 9](#_Toc5174)

[5.4.2 系统授权 10](#_Toc11239)

[5.4.3 系统升级 10](#_Toc11049)

[5.4.4 系统皮肤 11](#_Toc24273)

[5.4.5 配置操作 11](#_Toc25155)

[5.4.6 系统重启 12](#_Toc9377)

[5.4.7 API管理 13](#_Toc16282)

[5.5 探针管理 13](#_Toc12260)

[5.5.1 MC探针 14](#_Toc9491)

[5.5.2 侦测探针 14](#_Toc5714)

1. **系统简介**

伟思信安边界接入平台探针监控管理系统（以下简称探针系统），探针系统是一款以内外网交换平台为基础，交换业务和交换设备单元为对象的监测系统，负责对外网区的网络状态实时检测评估。以目标网络的安全设备、网络设备和服务器/PC等设备为侦测目标对象，完成对该类设备的设备运行状态、网络健康度、服务器进程的监控和侦测，并上报到伟思信安边界接入集中监控管理系统。

* 1. **产品定位**

外网区的业务系统与内外网交换平台之间传输的过程是否完整、可靠、有效、健康，为保证平台持续在最优交换状态，进行实时的监控，解决管理员在跨域跨网的运维工作问题，预防突发性事件发生。

* 1. **产品形态**

产品由集控管理系统、集控探针和集控Agent组成，当前系统包括：集控探针及集控Agent：

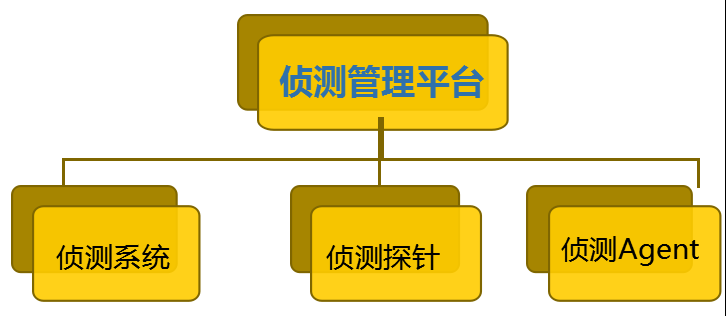


图 2 产品组成

1. 集控系统：部署在安全内网，负责内网被管业务的收集，全网业务的展示、预警等。
2. 集控探针：部署在安全外网，负责外网被管业务的收集。
3. 集控Agent：部署在被管业务部署的设备上，采用标准安全规范接口做应用数据的管理。



表 1 产品组成形态

1. **运行环境**
   1. **硬件运行信息**
      1. **温度/湿度要求**

探针系统服务器对空气温度、湿度的要求见下表。

|  |  |
| --- | --- |
| 温度 | 相对湿度 |
| 0~40℃ | 10%~90%（非凝露） |

表 2 温湿要求

* + 1. **纯净度要求**

探针系统服务器对空气灰尘浓度的要求见下表。

|  |  |  |
| --- | --- | --- |
| 机械活性物质 | 单位 | 含量 |
| 灰尘粒子 | 粒/m³ | ≤3×104 （3天内桌面无可见灰尘） |
| 注：灰尘粒子：直径≥5μm | | |

表 3 纯净度要求

* + 1. **防静电要求**

为防止静电损伤，应做到：

1. 设备良好接地；
2. 室内防尘；
3. 保持适当的温度、湿度条件；
4. 接触电路板时，应戴防静电手腕，穿防静电工作服；
5. 将拆卸下的电路板面朝上放置在抗静电的工作台上或放入防静电袋中；
6. 当观察或转移拆卸了的电路板时，请用手接触电路板的外边缘，避免用手直接触摸电路板上的元器件。
   1. **软件运行信息**

|  |  |
| --- | --- |
| 操作系统 | Linux 64位 |
| JDK | Jdk8 |
| WEB服务器 | Tomcat8 |

表 4 软件运行信息

1. **安装部署**
   1. **前置工作**
2. 设备加电操作；
3. 检查伟思信安网络隔离探针系统设备外观是否完整。
   1. **设备上架**

安装到 19 英寸的标准机柜上，安装前必须确定设备已断电，并且机柜接地良好、放置平稳。安装过程：

1. 用螺钉将固定挂耳固定在设备前面板或者后面板两侧；
2. 将设备放置在机柜的一个托盘上；在没有托盘的机柜上，请使用后挂耳。根据实际情况，沿机柜导槽移动设置至合适位置。
3. 用满足机柜安装尺寸要求的盘头螺钉将设备通过固定挂耳固定在机柜上，请保证位置水平并牢固。
   1. **系统部署检查**
4. 检查JAVA环境，必须1.8版本以上

执行：java -version

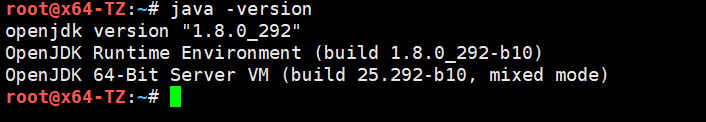


图 3 检查java版本

1. 检查Tomcat进程：

执行：ps -ef | grep tomcat

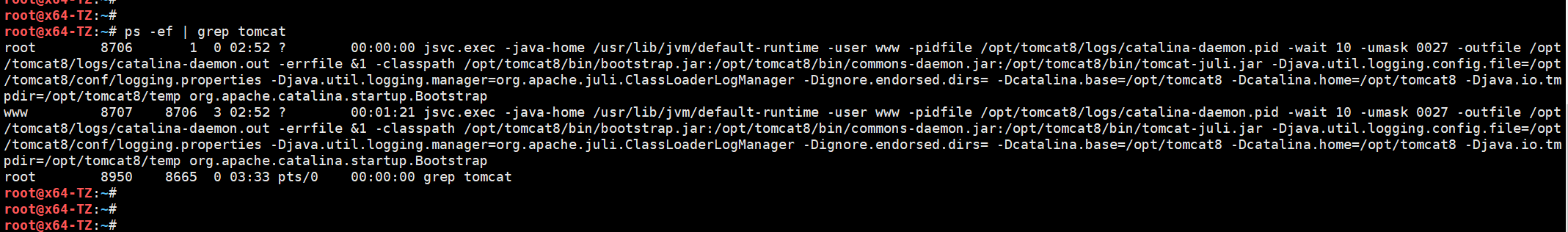


图 5 检查Tomcat进程

1. 检查端口是否存在：22、 10000、9999

执行：netstat -aptn

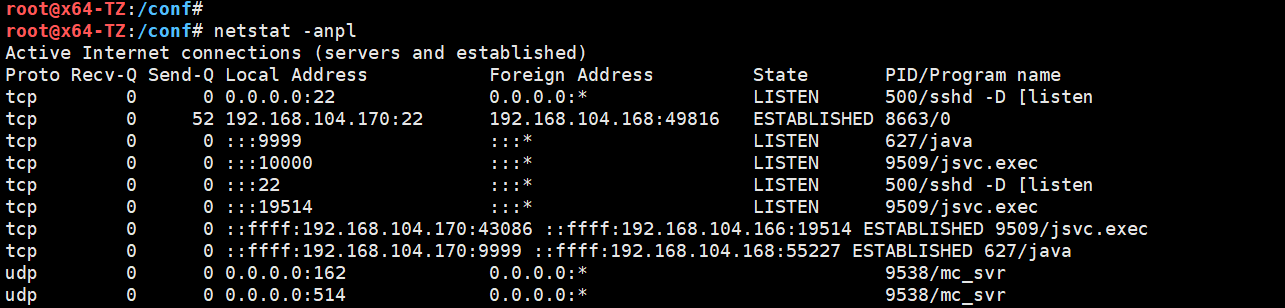


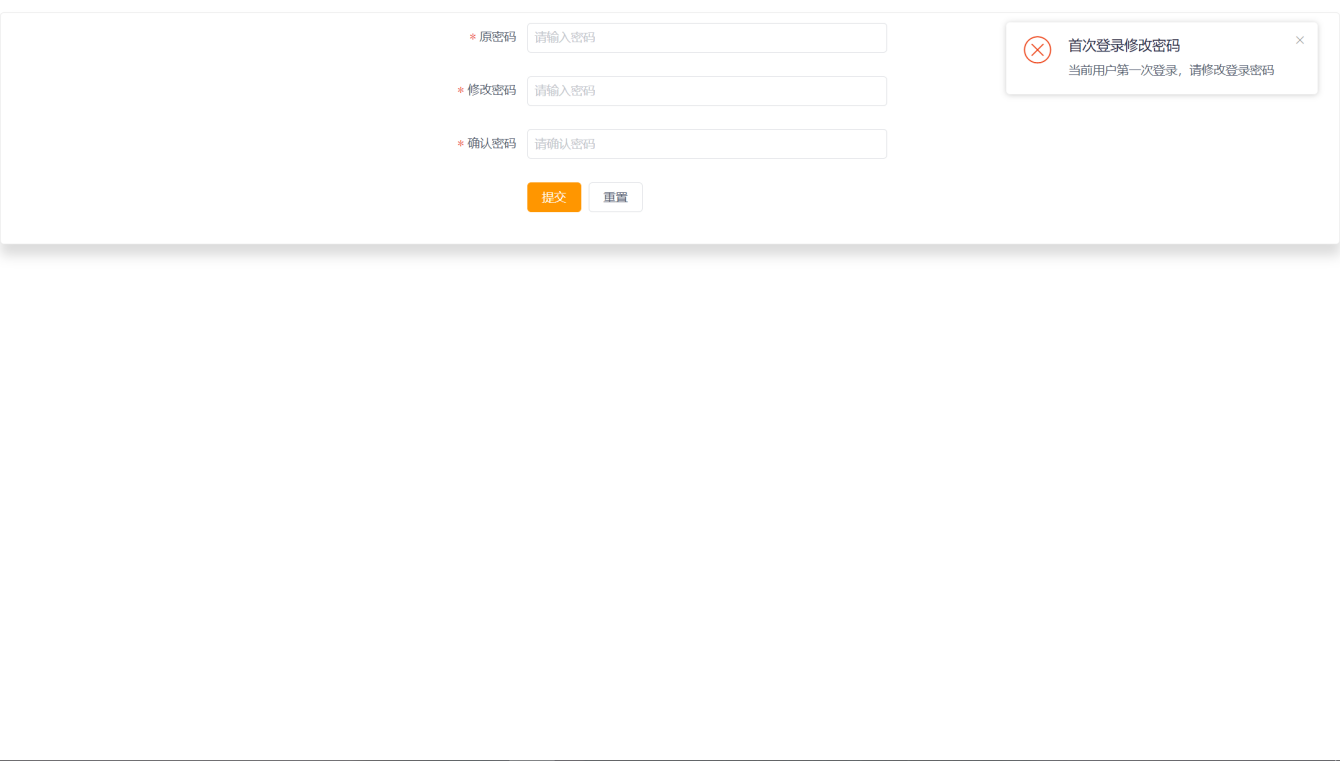
图 7 检查端口号

1. **业务操作指南**
   1. **登录管理**
      1. **准备工作**

* 接通电源，液晶屏显示序列号后表示启动完毕；
* 选用一带Windows系统PC作为管理主机；
* 使用交叉线，管理设备。
  + 1. **管理方式**
* 串口命令行管理 - 常用于恢复工作
* Web页面管理 ---- 常用于正常管理
* SSH远程管理 ---- 常用于管理调试
  + 1. **Web页面管理**
* 登陆入口：在管理主机输入https://192.168.10.254：9999，按证书提示点击“确定”；
* 管理员账号：在“用户名”一栏输入用户名admin，在“密码”一栏输入其对应默认口令“admin\*pwd” (管理人员应及时更改系统初始缺省管理员的用户名和口令)，在验证栏输入验证码。点击“登录”。



* 首次登录需要重新设置密码，重设密码后，再次登录即可，如下图：



* + 1. **SSH管理**
* 在管理主机上打开 SSH客户端， 输入IP地址；
* 输入管理员账号admin，密码admin\*pwd，连接后台。

初始缺省用户列表

|  |  |  |
| --- | --- | --- |
| 用户名 | 密码 | 备注 |
| admin | admin\*pwd | web系统管理员 |

1. **系统功能**
   1. **系统登录**

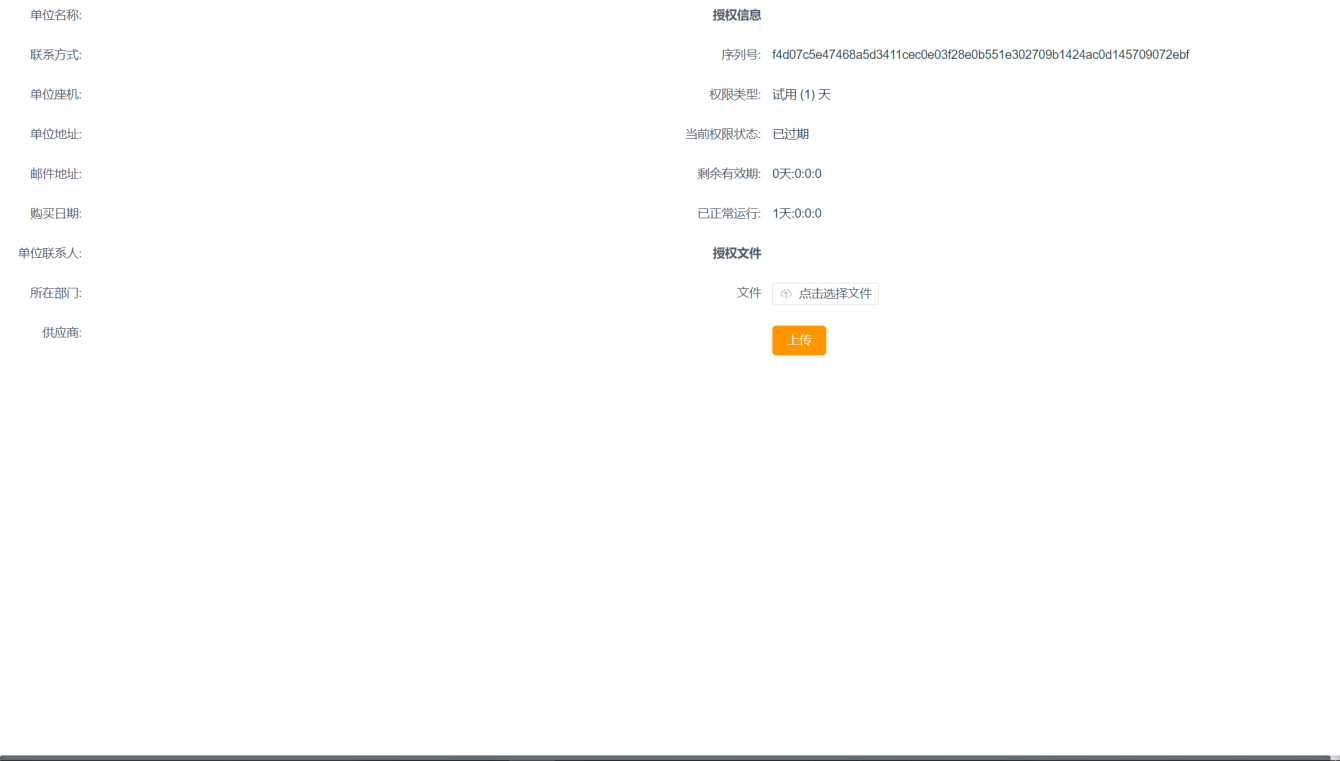
探针系统开机自动启动后，进入可访问探针系统URL进入登录页面。

* **说明**

例如：打开浏览器，访问系统部署地址（如：管理口IP为192.168.10.254则访问https://192.168.10.254:9999）



注意：如果出现以下页面，联系管理员生成license文件进行注册



* 1. **修改用户密码及退出系统**

登录系统后，可以在页面右上角修改用户的密码以及退出系统



1. 修改密码



点击修改密码，输入原密码、密码、以及确认密码，点击提交后，原密码验证成功后即可修改密码。

1. 退出系统

点击退出系统，即可登出当前系统，返回登录页面。

* 1. **系统监管**
     1. 运行监控

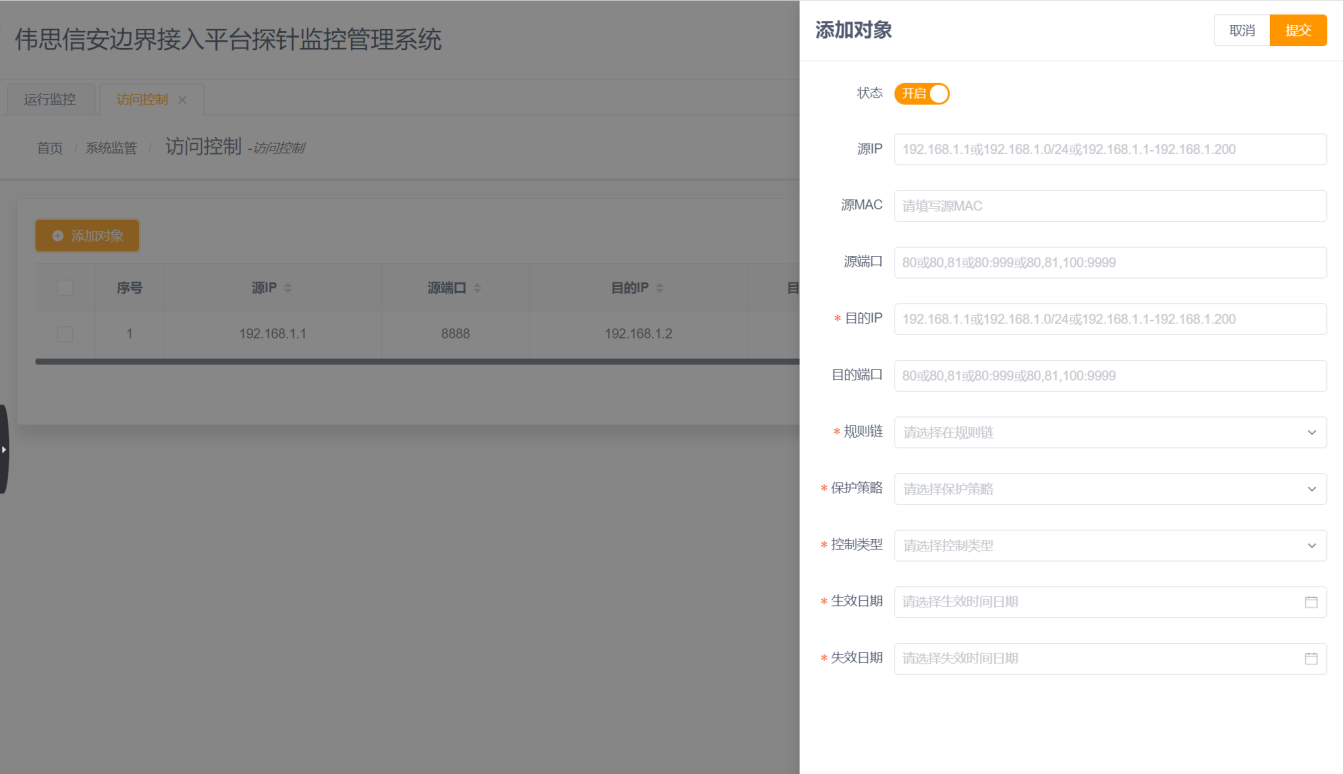
探针系统的系统监管页面,显示当前系统设备的运行信息（网卡流量、CPU、内存、磁盘等）。



* + 1. 访问控制

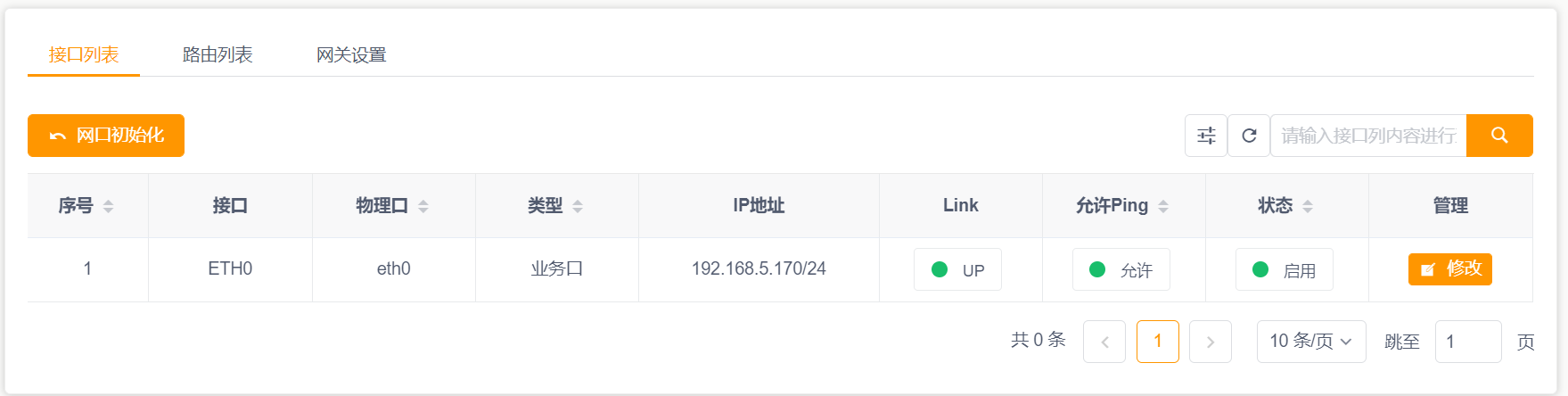
系统可自定义操作（新增、修改、删除）访问控制，访问规则包括：状态、源IP、源MAC、源端口、目的IP、目的端口、规则链、保护策略、控制类型、生效日期、失效日期。





* + 1. 网络管理

网络管理模块分为：接口管理、路由管理、网关设置



* + - 1. 接口管理

点击【网口初始化】，配置如下图：接口、物理口、类型（通道口、管理口、业务口）、IP地址/子网掩码、link状态

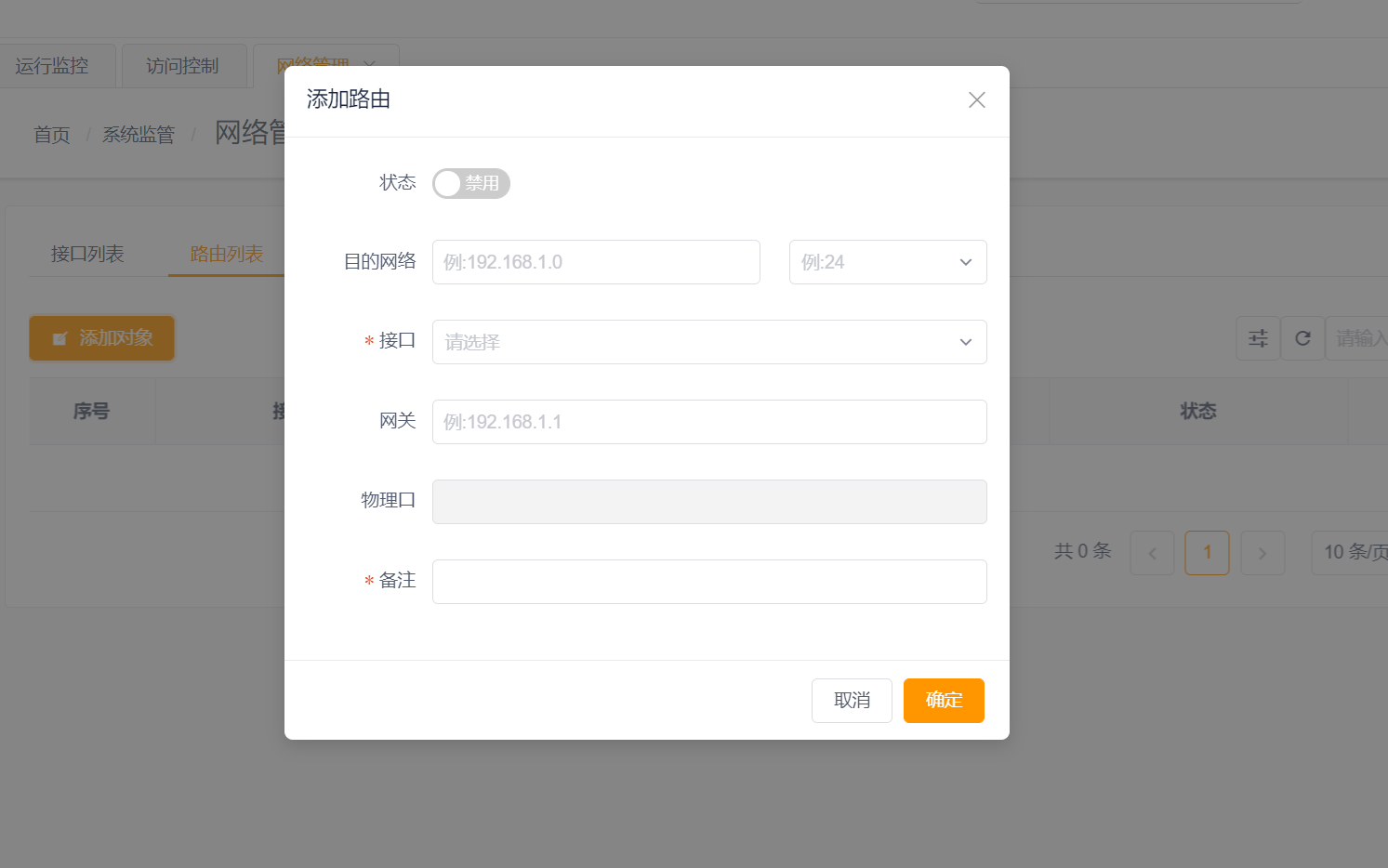


* + - 1. 路由管理

路由列表展示：

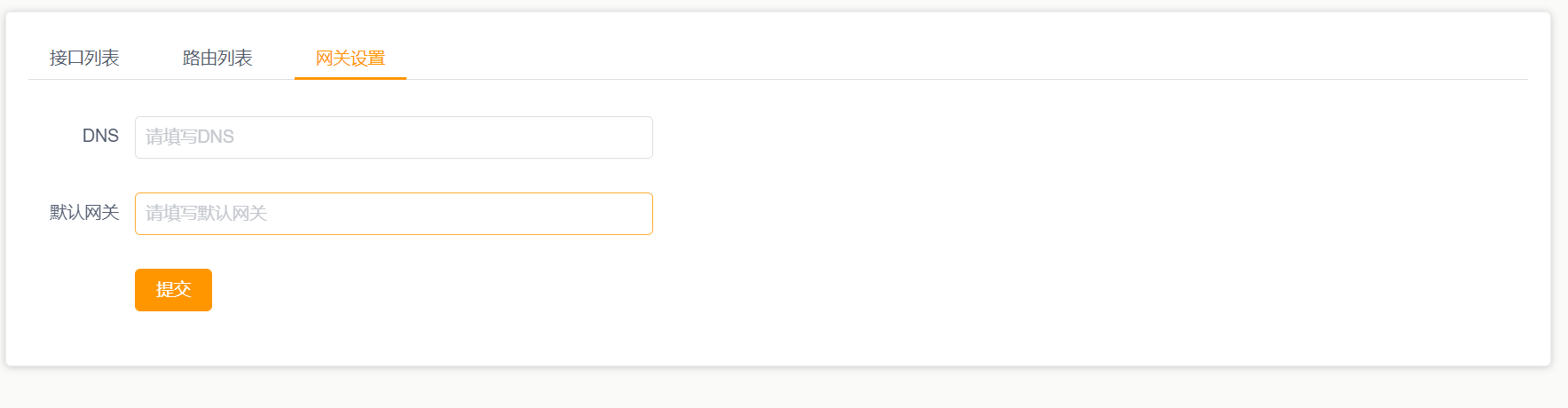


点击【添加对象】，配置包括：状态、目的网络、掩码、接口、网关、物理口、备注



* + - 1. 网关设置

用户可自定义网关，配置有：DNS、默认网关。

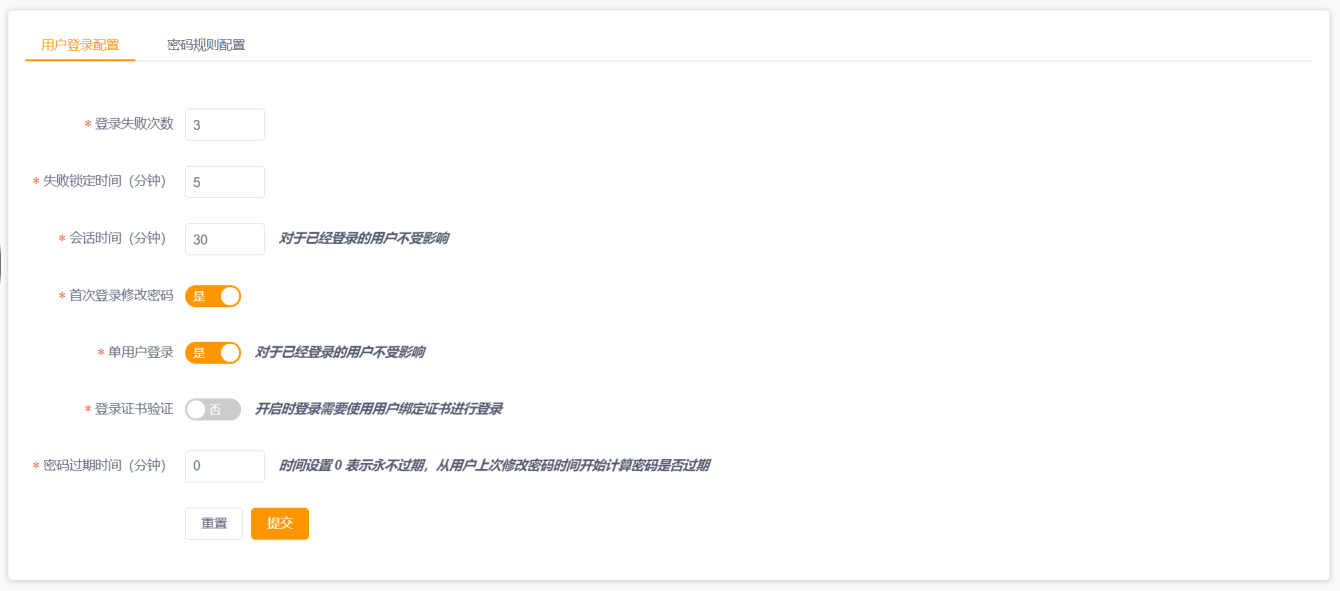


* 1. **用户管理**

探针系统的用户管理模块，可配置用户登录安全配置以及系统用户的管理。

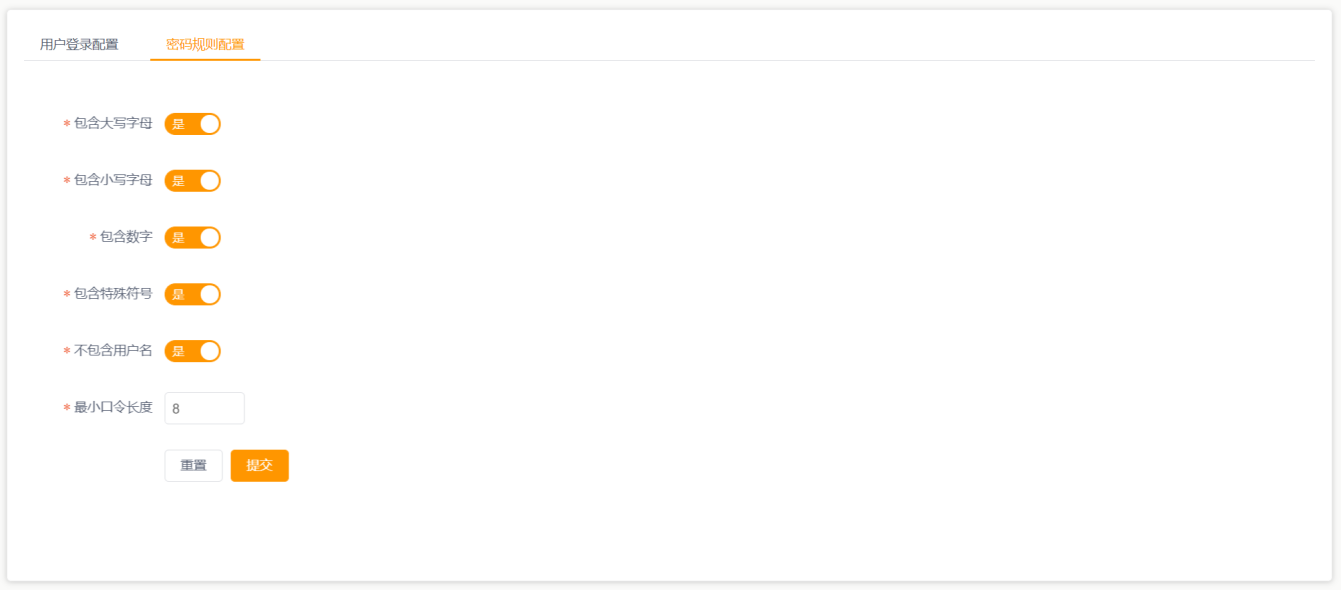
* + 1. **安全配置**
       1. 用户登录配置

可配置用户登录失败次数、失败锁定时间、会话时间、首次登陆修改密码、单用户登录、登陆证书验证、密码过期时间。



* + - 1. 密码规则配置

可以对用户密码的规则进行配置，规则有：包含大写字母、包含小写字母、包含数字、包含特殊字符、不包含用户名、最小口令长度。

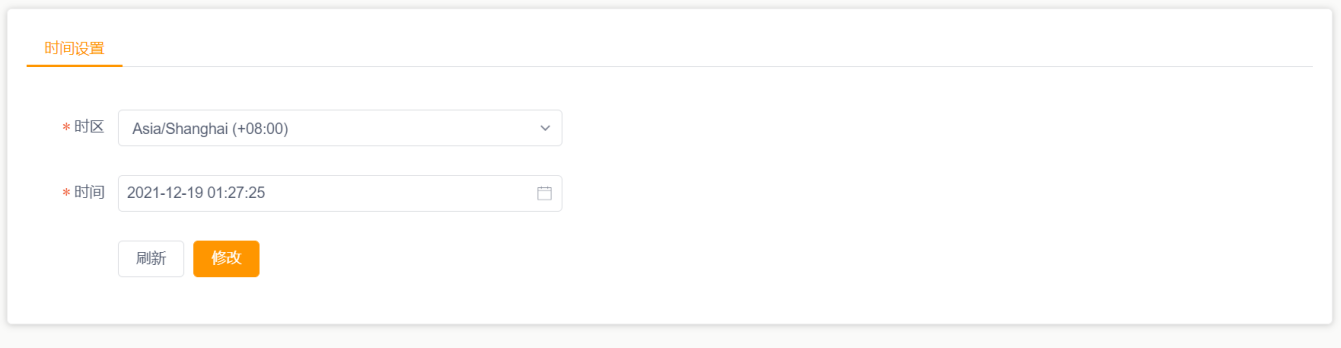


* 1. **系统配置**

探针系统的系统配置，包括：时间配置、系统授权、系统升级、配置操作、系统重启。

* + 1. **时间管理**

设置系统时间。



* + 1. **系统授权**

系统在此注册license证书



* + 1. 系统升级

探针系统提供页面系统升级功能，可上传正确的更新包升级探针系统。

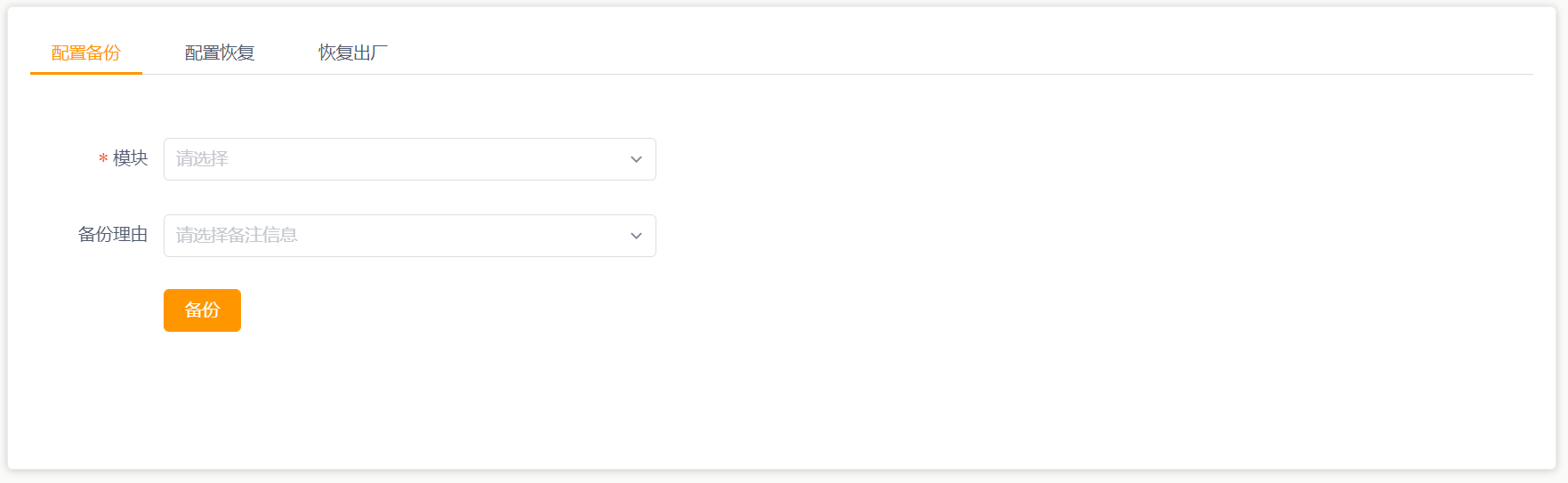


* + 1. 配置操作

系统提供配置操作，功能包括：配置备份、配置恢复、恢复出厂。

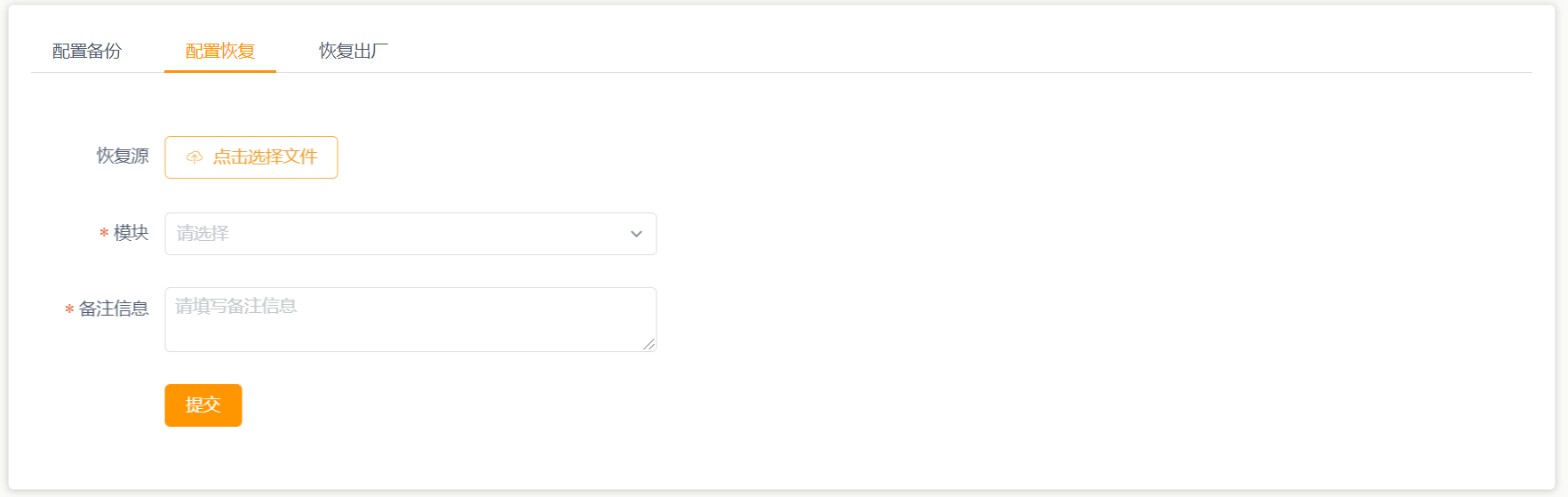
1. 配置备份

选择备份模块，添加备份理由，即可进行备份。



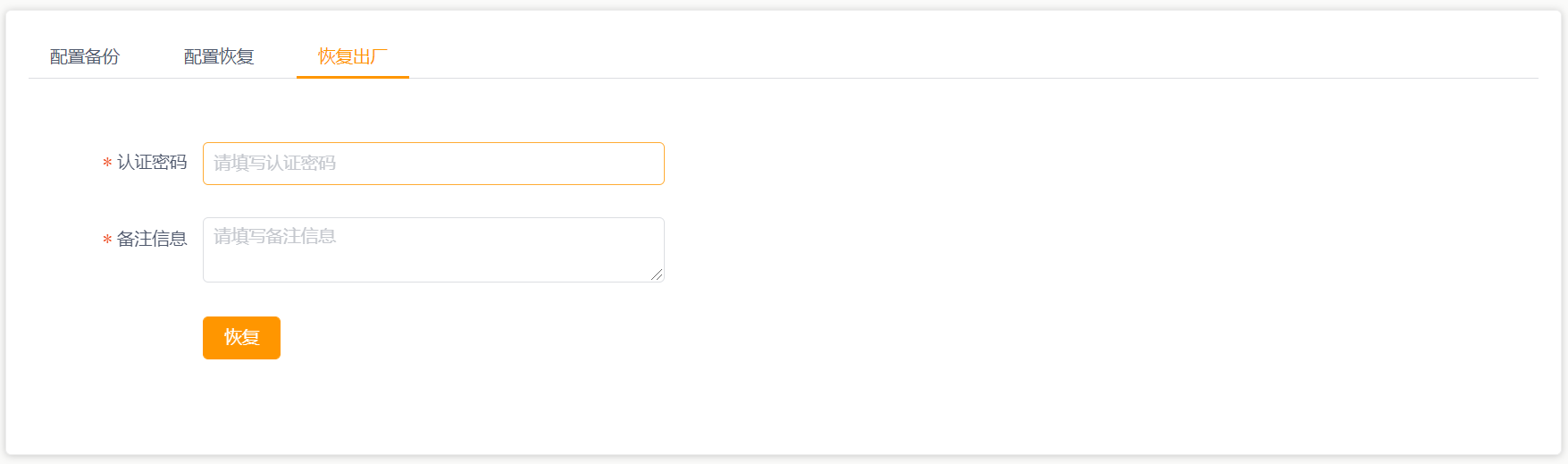
1. 配置恢复

选择恢复源、模块及备注信息，即可进行配置恢复。



1. 恢复出厂

所有配置都还原出厂配置。

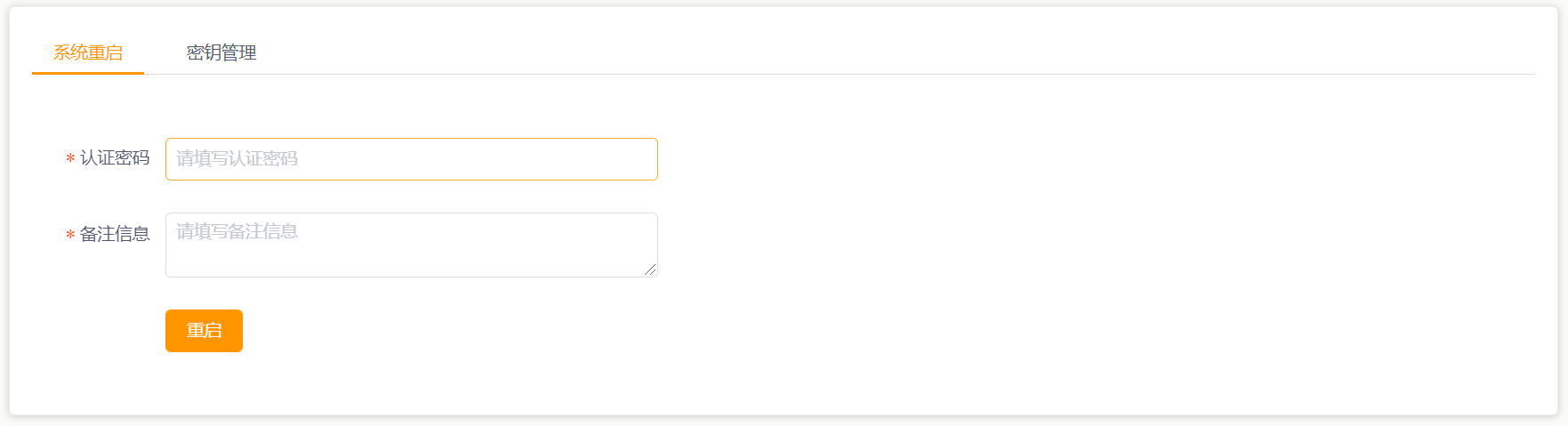


* + 1. 系统重启

分为：系统重启、密钥管理

1. 系统重启

输入认证密码，成功验证后重启系统。



1. 密钥管理

更新密钥，输入认证密码以及备注，验证成功后将会修改密钥。

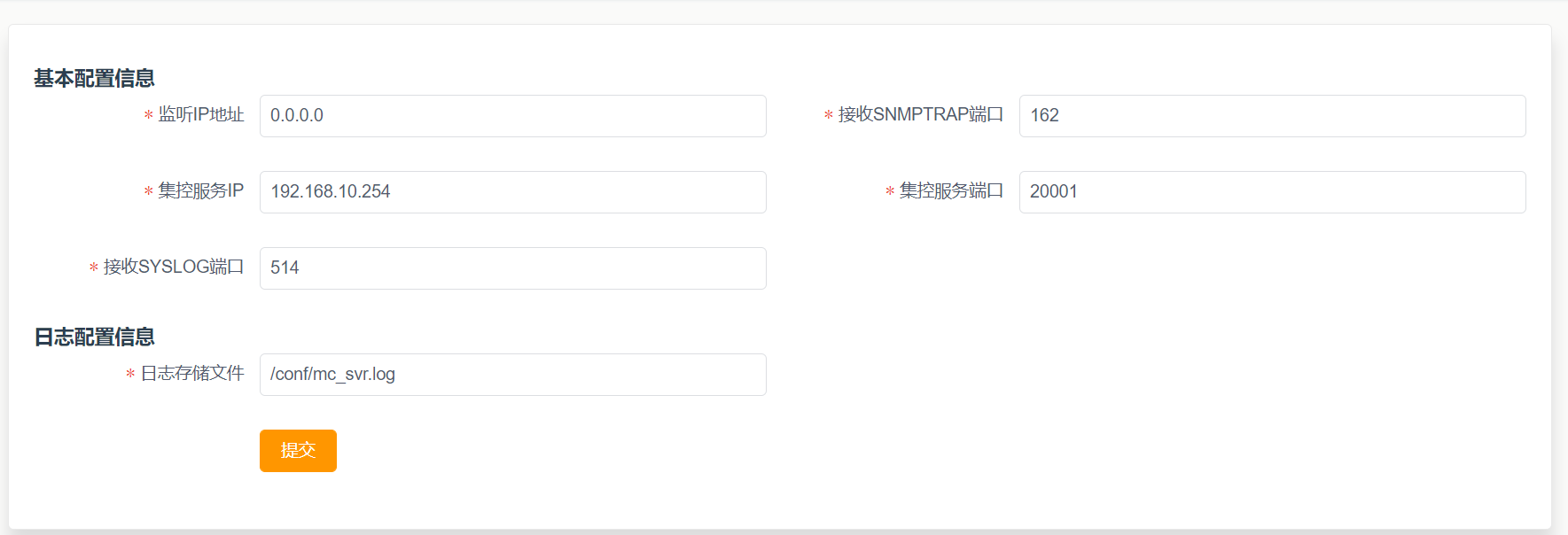


* 1. **探针管理**

探针系统提供对MC探针以及侦测探针进行配置管理。

* + 1. **MC探针**
* **说明**

对系统的MC探针进行配置，保存配置后自动重启MC探针。配置包括：监听IP地址、接收SNMP trap端口、集控服务IP、集控服务端口、接收SYSLOG端口以及日志存储文件。



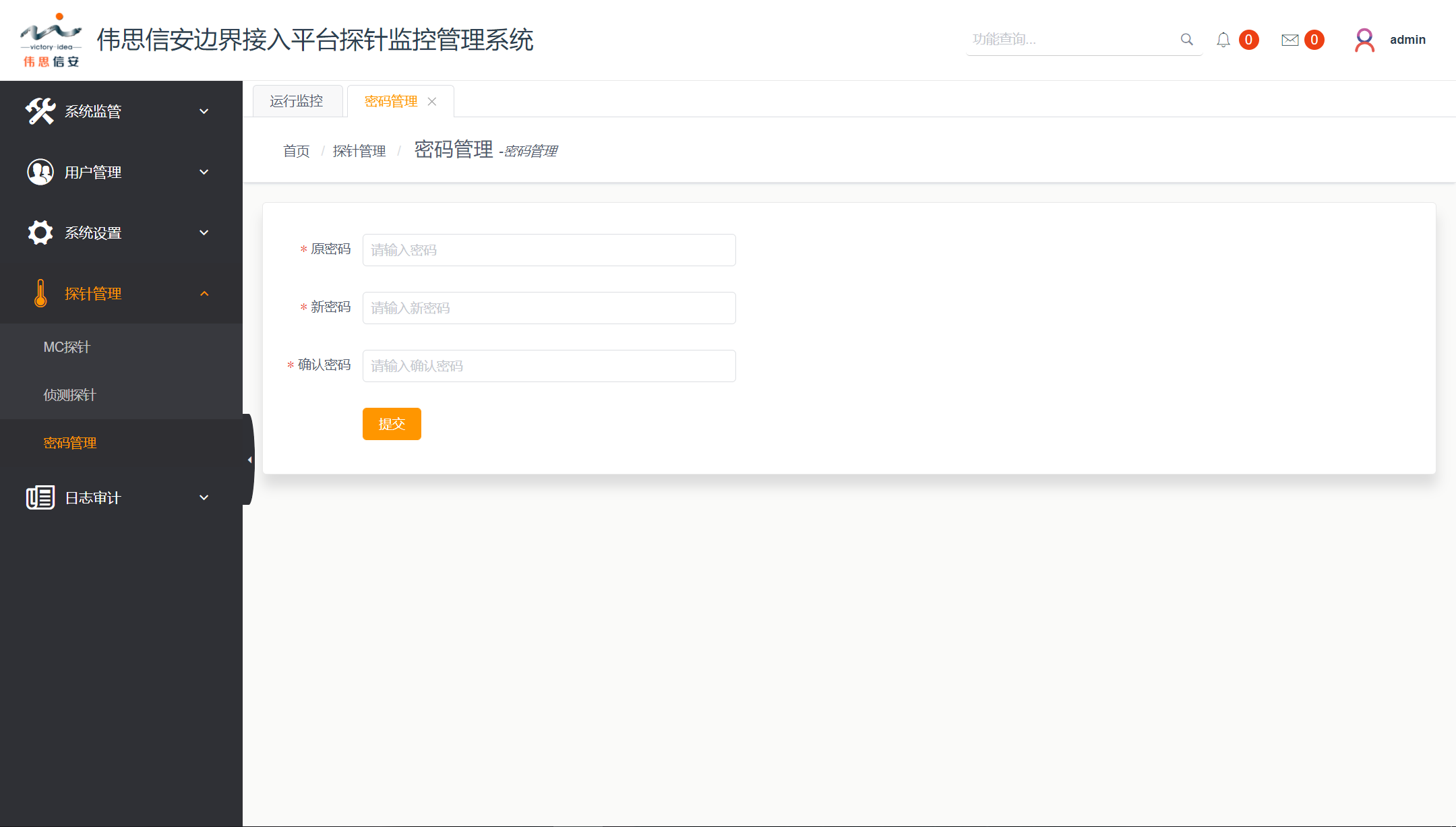
* + 1. **侦测探针**
* **说明**

对系统的侦测探针进行配置，保存配置后自动重启侦测探针。配置包括：探针IP（为空默认为：0.0.0.0）、探针端口、侦测IP、侦测端口；探针注册信息：设备名称、出厂标识、设备IP、设备位置。



* + 1. 密码管理

进入密码管理页面，提供SSH admin账号密码更新功能，输入原密码、新密码以及确认密码，点击【提交】，即可修改。



* 1. **日志审计**
     1. 日志审计

系统日志-操作日志，可通过时间筛选查看日志；日志支持导出。

