恩创安全运维管理系统

操作手册

AVCOMM恩创®

安全运维管理系统

操作手册

关于此操作手册

此用户手册旨在指导专业安装人员操作安全运维管理系统。包括帮助避免意外发生问题的步骤。

注意:

只有合格且经过培训的人员才能对此产品进行安装、检查和维修。

免责声明

AVCOMM保留随时更改本手册或产品硬件的权利，恕不另行通知。此处提供的信息目的是为了保证其准确可靠。但是可能不会涵盖所有的细节和更改，也并未提供在安装、操作或维护过程中遇到的所有可能的意外情况。如需更多信息，或出现未完全包含在此手册中的特定问题，应将此提交给AVCOMM。用户有责任确定手册是否有任何针对添加的新信息和/或纠正可能的无意造成的技术或印刷错误进行的不定期更新和修订。AVCOMM对其被第三方使用不承担任何责任

AVCOMM在线技术服务

在AVCOMM，您可以使用在线服务表来请求支持。提交的服务表保存在服务器上，供AVCOMM团队成员分配任务并监控您的服务状态。如遇任何困难，请随时发邮件至sales@n-tron.com.cn

目 录

1. 概述

恩创安全运维管理系统(以下简称:“SOM6006”）是用于对第三方或者内部运维管理员的运维操作行为进行集中管控审计的系统。SOM6006 可以帮助客户规范运维操作行为、控制并降低安全风险、满足等级保护以及其他法规对 IT 内控合规性的要求。

1.1 功能介绍

SOM6006 集中管理运维账号、资产设备，集中控制运维操作行为，能够实现实时监控、阻断、告警，以及事后的审计与统计分析。

SOM6006 支持常用的运维工具协议（如 SSH、TELNET、FTP、SFTP、RDP、VNC 等），并可以应用发布的方式支持图形化运维工具。

SOM6006 支持旁路模式和 VPN 模式两种方式，物理上旁路部署，灵活方面。

SOM6006 支持 IPv4、IPv6 网络下的管理、运维和审计。

SOM6006 在操作方式上，不改变用户的操作习惯，仍然可以使用自己本机的运维工具。

1.2 名词解释

控制台

指 SOM6006 提供给管理员实现对它进行管理的 Web 系统。

管理员

指 SOM6006 系统的管理员，按照角色分为系统管理员、部门管理员、密码管理员、审计管理员，按照权限分立的原则分别承担不同的职责。

系统管理员：是内置的最高权限管理员，可以创建其他管理员角色用户账号。

部门管理员：在部门内享有与系统管理员同等权限。

密码管理员：负责维护资产设备的账号密码；

审计管理员：只负责完成审计工作。

协议

指运维工具所用的通信协议，比如 PuTTy/SecureCRT/XShell 使用 TELNET/SSH 协议，MSTSC 支持 RDP/VNC 等协议。

工具

指运维人员实现对设备的维护所使用的工具软件。

设备账号

指运维目标资产设备的用于维护的系统账户。

自动登录

指为运维工具实现自动登录目标被管设备，而运维用户不需要输入目标设备的登录账号和密码，也称

为单点登录（SSO）。

命令阻断

指根据命令权限策略检查用户输入的操作指令，如果策略不允许执行此指令，平台会拒绝转发此操作命令目标设备，同时向操作员反馈拒绝执行的提示信息。这是实现实时操作控制的一种重要手段。

应用发布

指通过在应用发布服务器部署应用程序，提供给用户远程虚拟化方式进行使用，就如同安装在本地一样的效果。

1.3 环境要求

SOM6006 管理控制台为 Web 系统，客户端可采用支持基于 Chrome、Firefox、IE 等内核的浏览器登录。

2. 系统登录

SOM6006 系统采用 HTTPS 安全通信连接，默认端口是 443。管理员登录控制台的方式是，以 Chrome 为例，在浏览器地址栏输入：https://<安全运维管理系统-ip>

SOM6006 内置帐号列表：

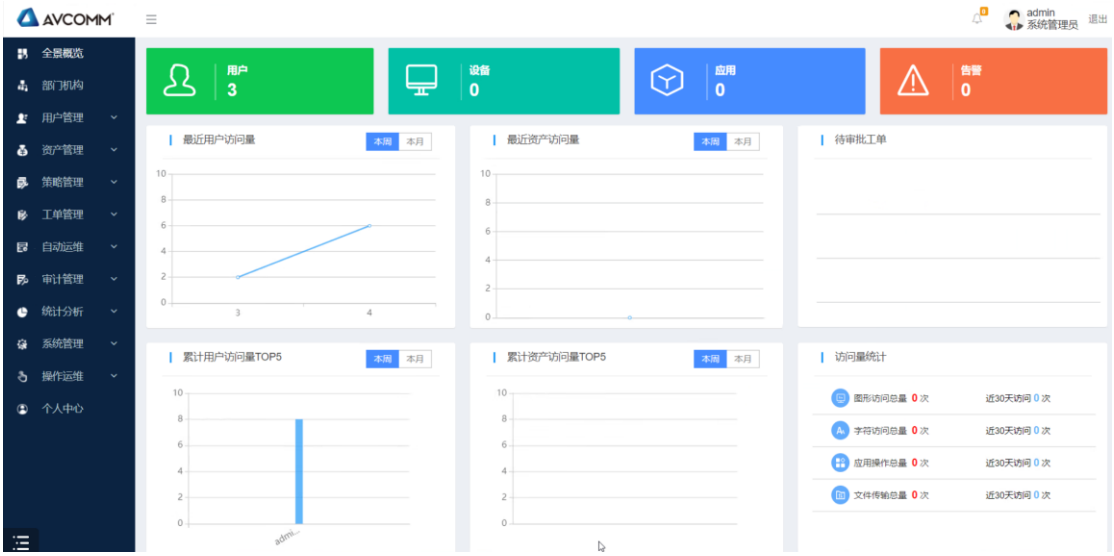
角色	帐号	初始密码
系统管理员	admin	admin@123
密码管理员	password	admin@123
审计管理员	audit	admin@123

SOM6006 系统默认开启安全配置“密码策略配置-新用户强制改密”，首次登录强制改密，拒绝将会退出系统。

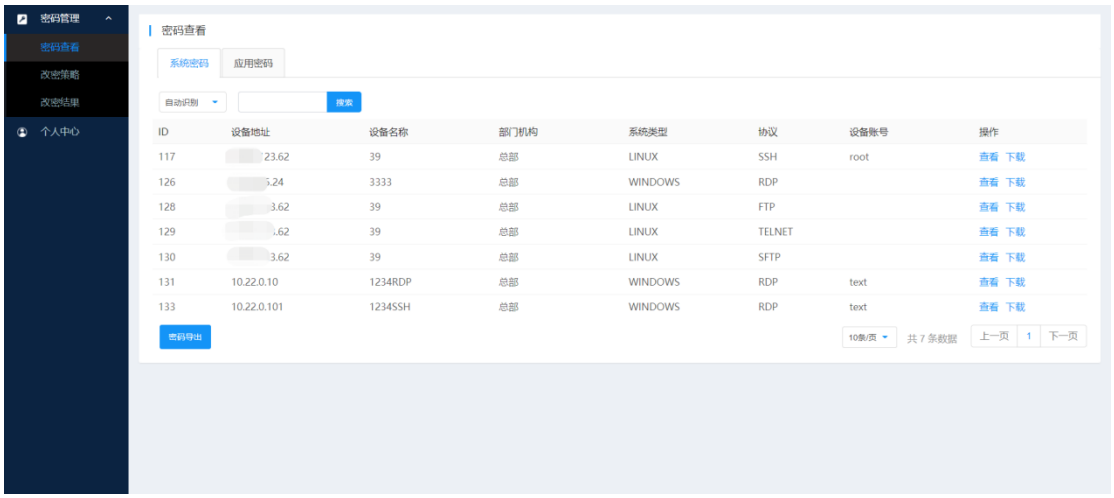
管理控制台登录界面如下图所示。

登录成功后界面如下图（以管理员 admin 为例），进入系统当前状态界面。然后管理员可以根据需要选择功能菜单执行预期的管理操作。

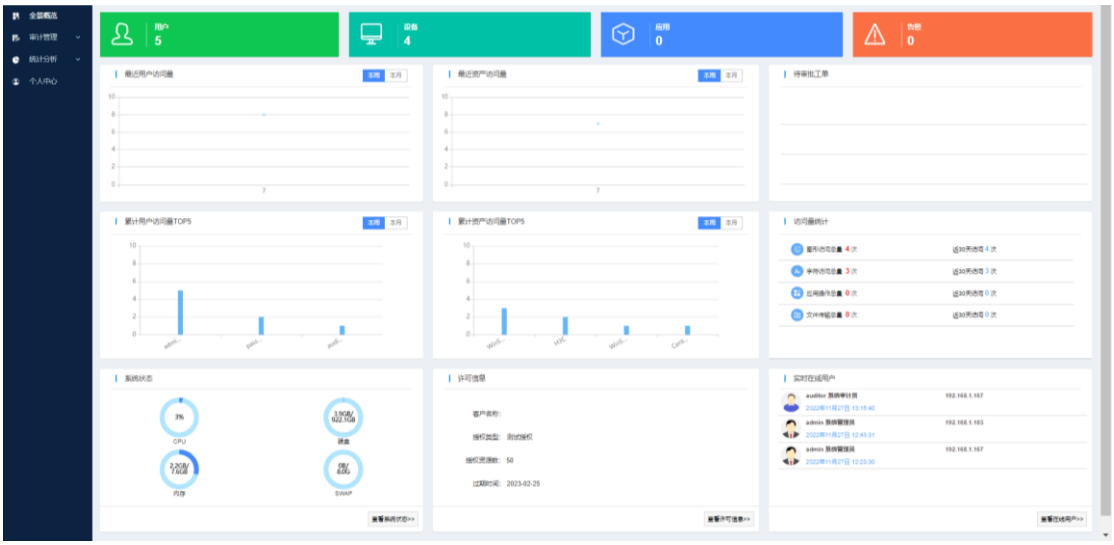
系统管理员密码登录后的操作界面，如下图所示：



密码管理员登录后的操作界面，如下图所示：



审计管理员登录后的操作界面，如下图所示：

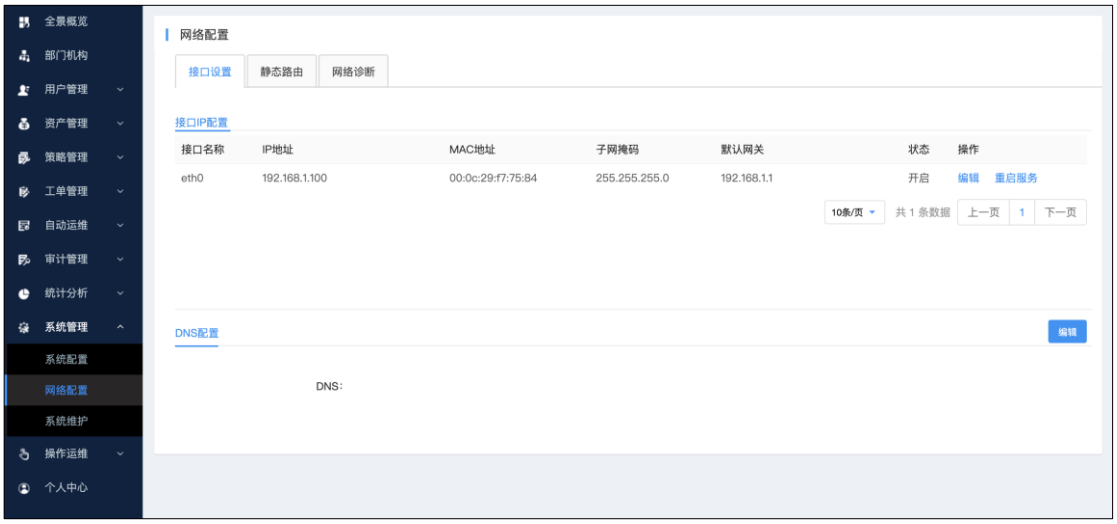


3. 初始基本配置

开始使用 SOM6006 时，管理员应先进行一下配置检查，根据实际应用需要配置必要的系统参数，构建适合本单位的系统工作环境。常见初始配置为：网络配置及许可导入。

网络配置

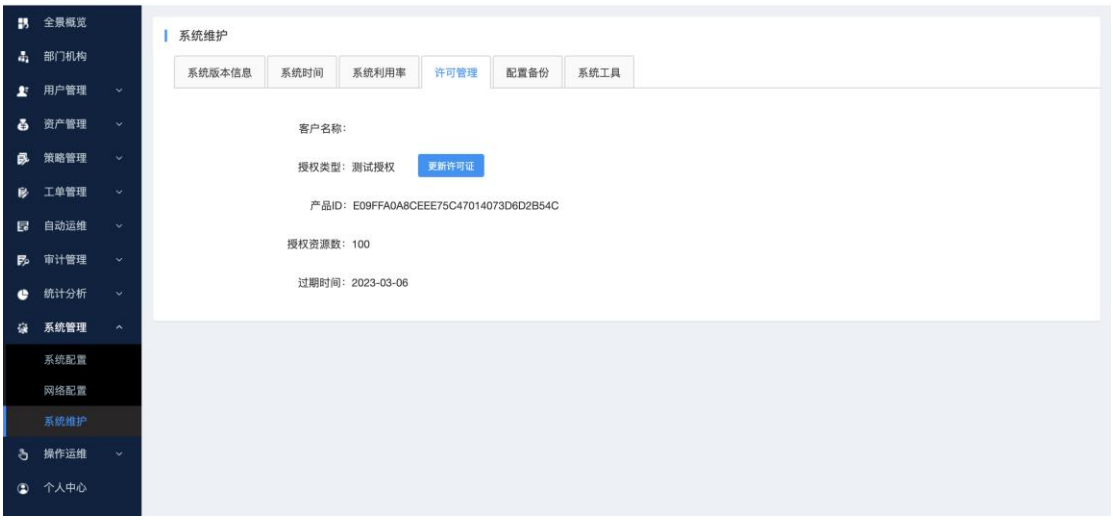
网络配置界面在系统管理→网络配置菜单中，点击后打开 eth0 口 IP 配置，界面如下:



输入参数后点击保存修改，点击[重启服务]以刷新网络配置。

许可导入

进入[系统管理]-[系统维护]，进入许可管理界面：



单击[更新许可证]，弹出更新许可界面：

单击[点击下载],进行下载申请文件，由服务人员进行生成申请授权许可文件，单击[选择文件]，许可文件会上传到系统，进行校验许可信息并更新。此时完成许可导入。

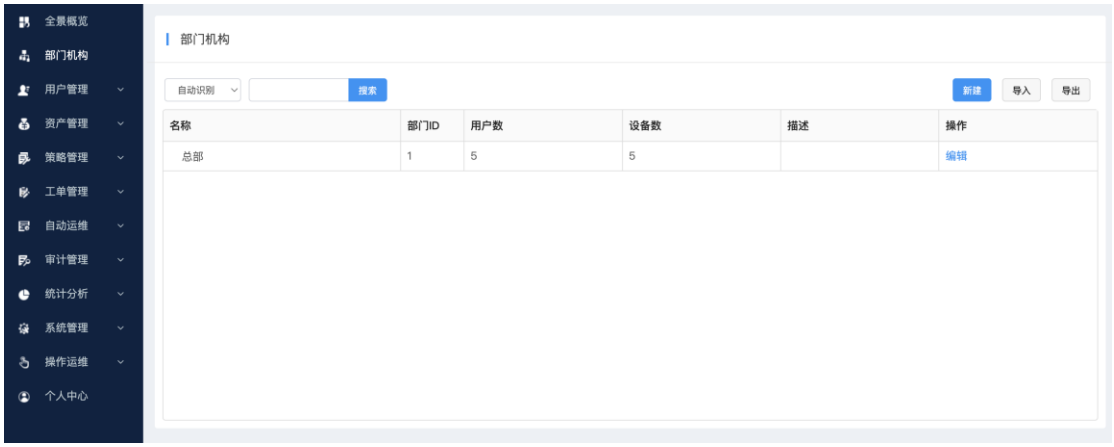
4. 部门管理

部门管理用于用户内部划分组织架构，标示用户、资产、权限等录属组织机构的管理归属方式。

界面路径：[部门管理]

4.1 新建部门

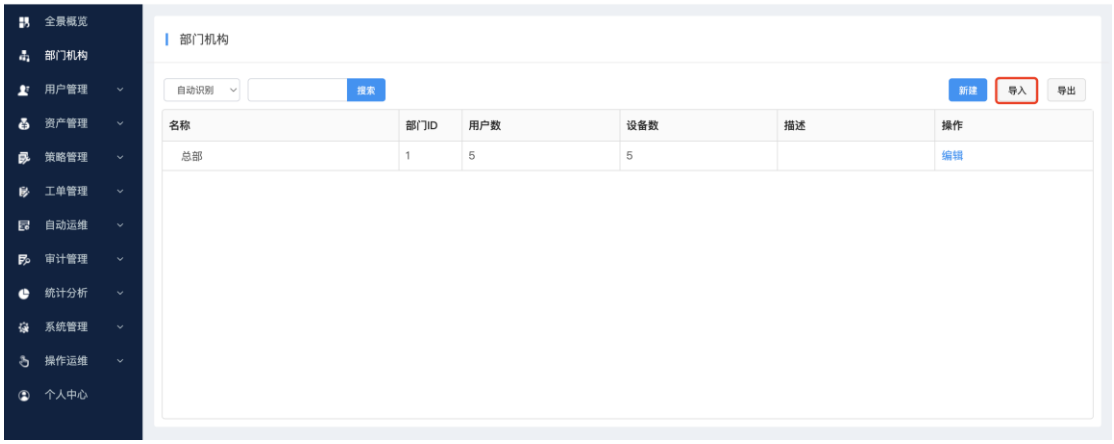
单击右上角[新建]，弹出新建部门操作界面



说明：根部门为系统一级部门，名称可做修改，但不可删除。其余新建部门均为一级部门下所属部门。

4.2 导入部门

单击右上角[导入]，弹出导入操作页面：



首先，在下载模板中，单击[点击下载]，下载导入的模板文件：

根据下载的模板文件对部门信息进行添加，添加完成保存文件后，单击导入页面[选择文件]，进行文件上传，单击确定，在列表中即可显示导入后的部门信息。

5. 用户管理

5.1 用户列表

SOM6006 设置了五个用户角色：系统管理员、审计管理员、部门管理员、密码管理员和运维用户，各角色具体权限如下表所示。

用户角色	角色权限
系统管理员	全景概览 部门机构 用户管理

用户角色	角色权限
	资产管理 策略管理 工单管理（工单审批） 自动运维 审计管理（查看权限） 统计分析（查看权限） 系统管理 操作运维 个人中心
审计管理员	全景概览 审计管理 统计分析 密码管理（改密结果） 个人中心
部门管理员	部门机构 用户管理（用户列表、用户分组、用户策略）

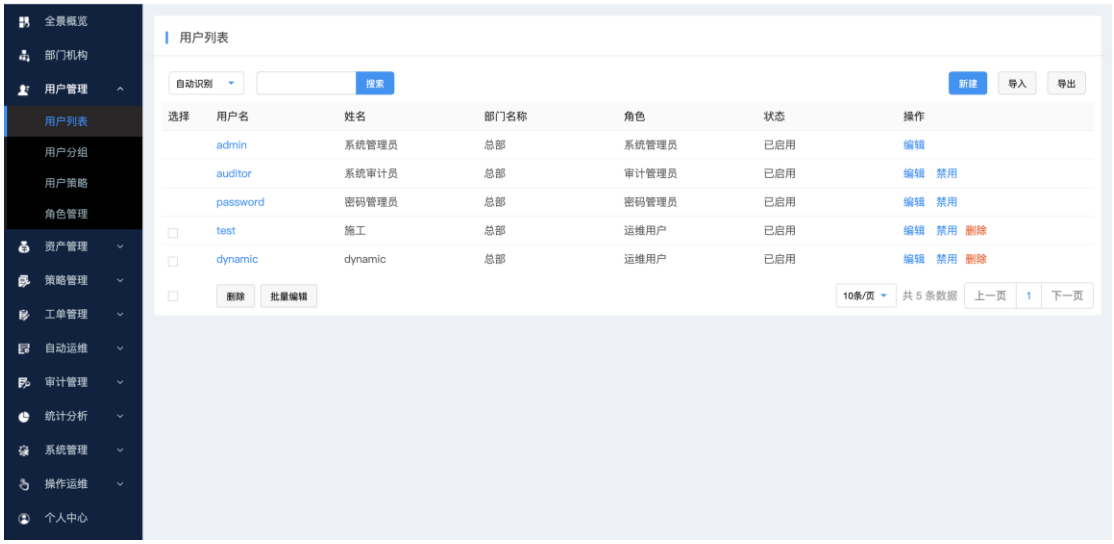
用户角色	角色权限
	资产管理（设备列表、设备分组、应用管理） 策略管理 工单管理 自动运维 审计管理（主机审计、应用审计、实时会话） 操作运维 个人中心
密码管理员	密码管理 个人中心
运维用户	工单管理（工单申请） 操作运维 个人中心
自定义角色	根据用户实际需求进行创建各种角色权限

SOM6006出厂内置三个管理员账户，分别是：

角色	帐号
系统管理员	admin
密码管理员	password

审计管理员	audit

点击左侧菜单“用户管理—用户列表”，打开用户列表界面。可以看到三个管理员账号。



每个运维账号含有大量资产权限信息，是运维控制的核心，下面详细介绍：

- 角色

选择创建用户的角色，默认为运维用户

- 分组

是为了明确用户录属组织机构设置的分组管理，可在左侧主菜单的“用户分组”选项卡中设置用户组，注意，用户在添加时，必须属于一个组。

- 用户名

用户登录标识信息、对应自然人信息和账户认证相关信息。

- 姓名

登录用户的真实姓名标示，便于识别管理

- 密码及确认密码

用户登录系统的密码，默认可设置 8 位数以上密码，也可通过系统管理设置符合复杂度要求的验证密码。

- Email

用户邮箱地址，便于策略发送相关邮件及通知信息。

- 认证方式

静态密码、静态密码+动态口令、指纹认证等。默认采用静态密码认证，如果使用其它认证，则选择其它认证方式。

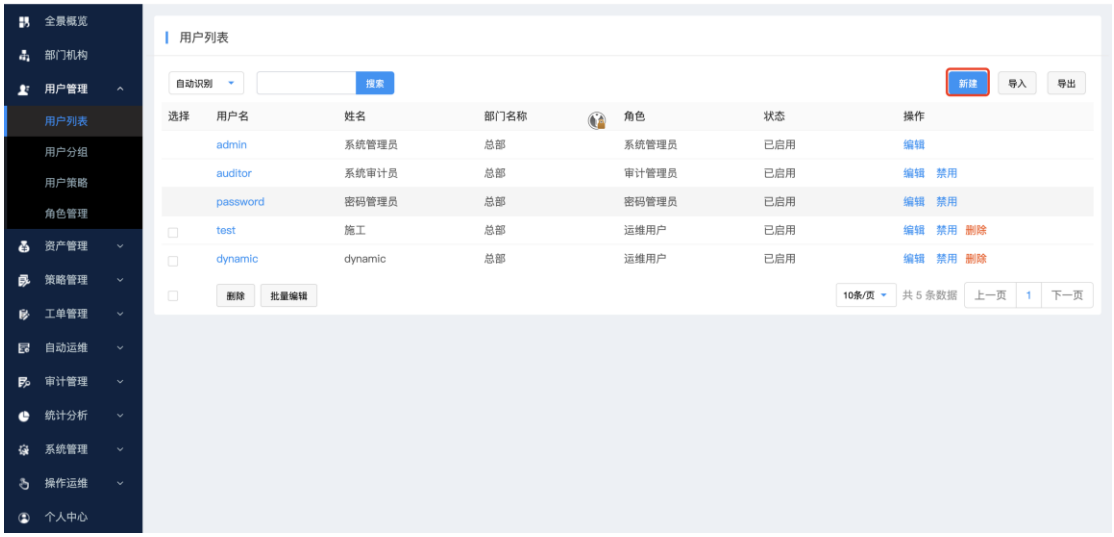
➢ 更多

是用户更多信息，根据需要进行配置：电话，QQ，微信，备注

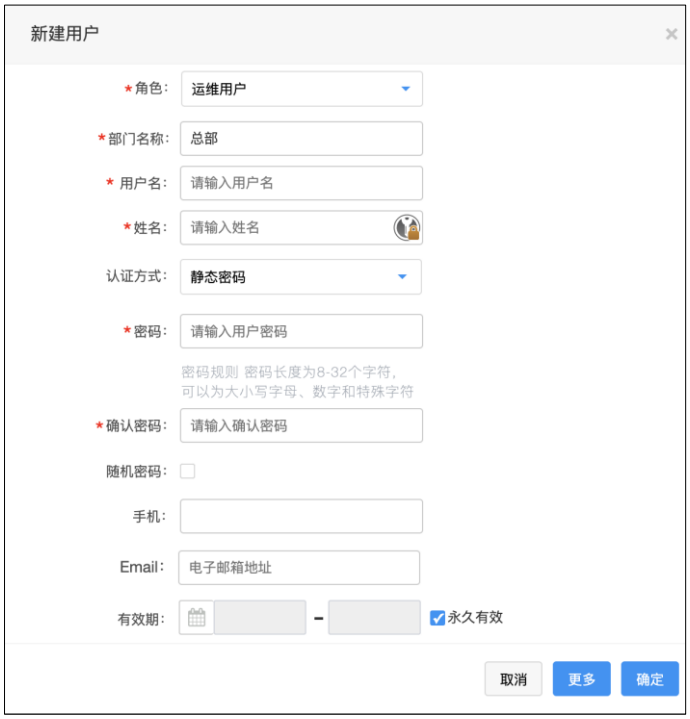
界面路径：[用户管理]-[用户列表]

5.1.1 添加用户

单击右上角[新建]，弹出新建用户操作界面

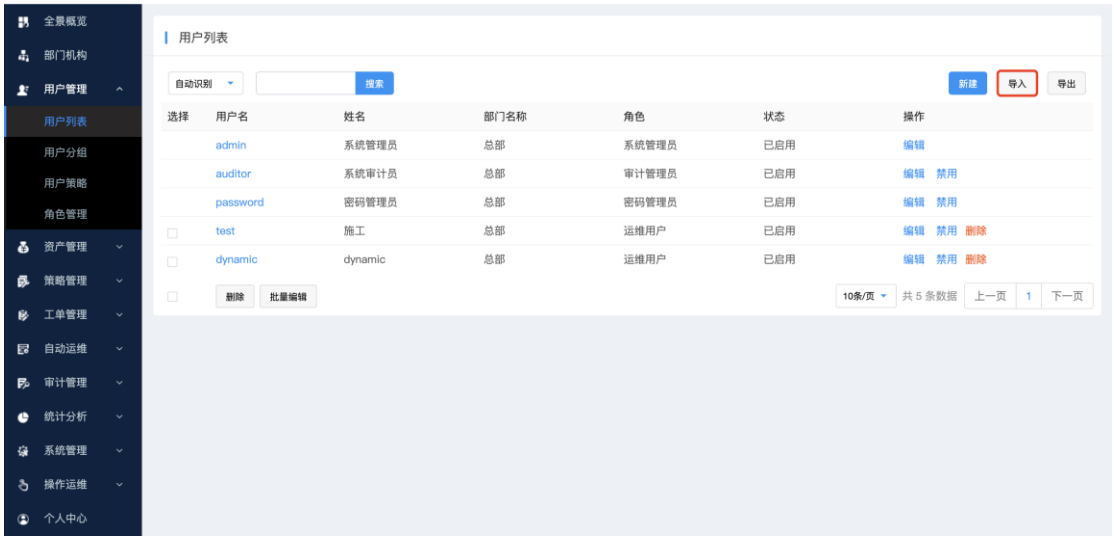


根据提示选择或输入相关用户信息。



5.1.2 导入用户

单击右上角[导入]，弹出导入操作页面：



首先，在下载模板中，单击[点击下载]，下载导入的模板文件：

根据下载的模板文件对用户信息进行添加，添加完成保存文件后，单击导入页面[选择文件]，进行文件上传，单击确定，在列表中即可显示导入后的用户信息。

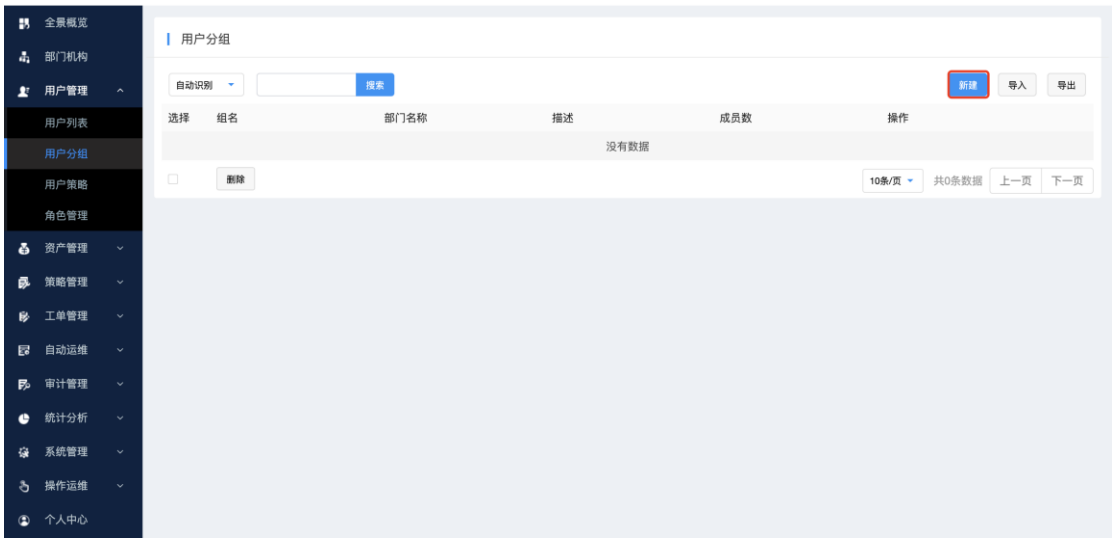
5.2 用户分组

用户组主要是为了将用户录属于的组织，实现快速设置访问控制、批量授权等功能，用户分组模块可对用户分组进行创建、编辑、删除、查询等功能。

界面路径：[用户管理]-[用户分组]

5.2.1 添加用户组

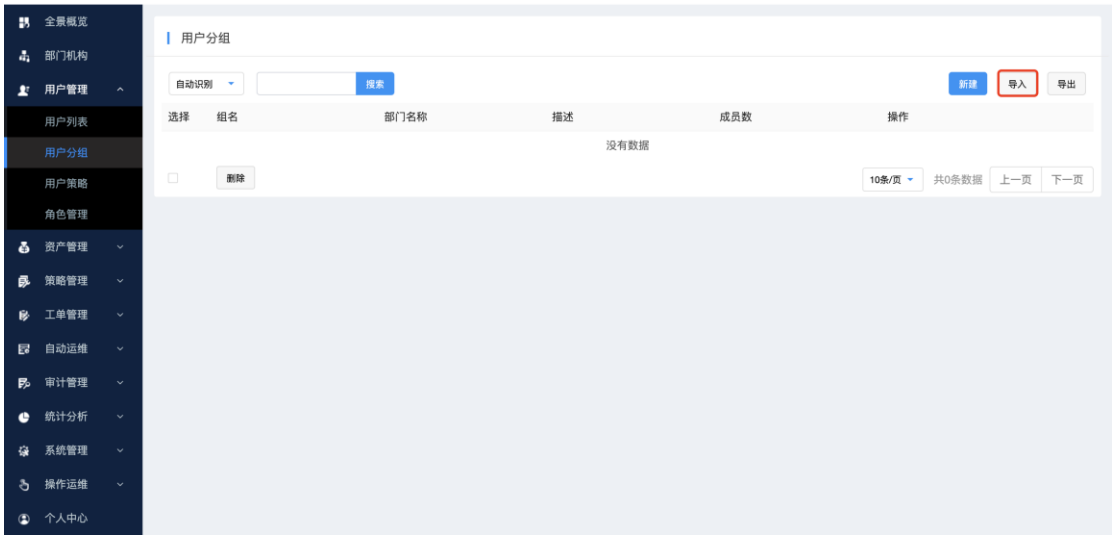
单击右上角[新建]，弹出新建用户分组操作界面：



根据提示，输入用户组名称，描述根据需要进行填写。完成后单击<确定>，进行保存。

5.2.2 导入用户组

单击右上角[导入]，弹出导入操作页面:

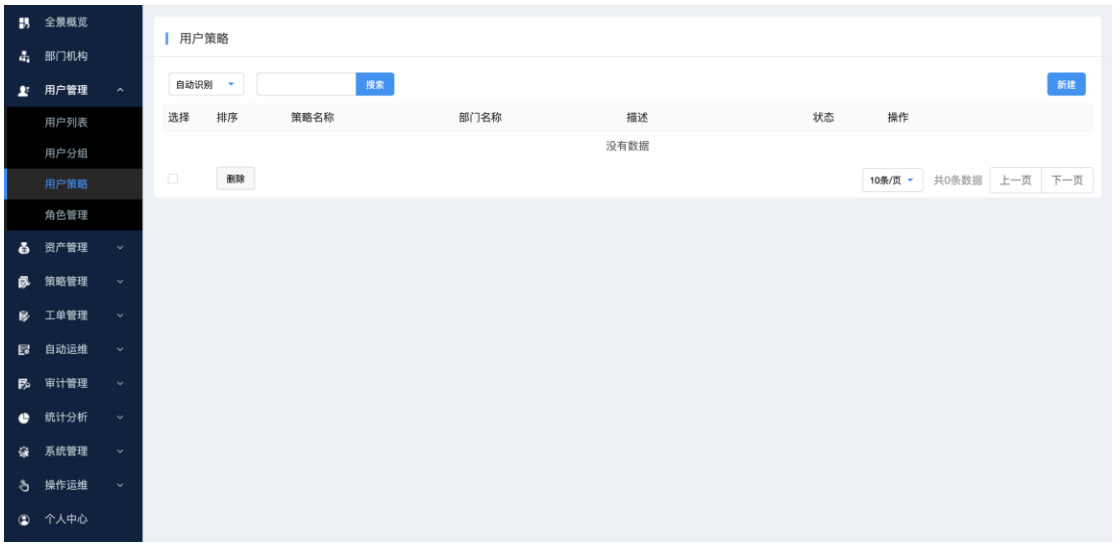


首先，在下载模板中，单击[点击下载]，下载导入的模板文件

根据下载的模板文件对用户分组信息进行添加，添加完成保存文件后，单击导入页面[选择文件]，进行文件上传，单击确定，在列表中即可显示导入后的用户分组信息。

5.3 用户策略

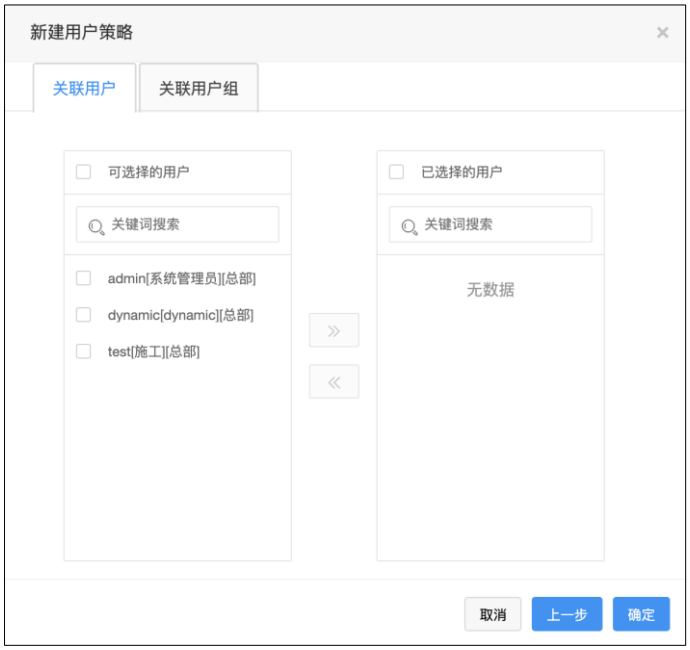
进入[用户管理]-[用户策略]，单击右上角[新建]，进入新建用户策略界面：



填写对应的输入项，具体功能说明如下：

输入项	说明
策略名称	策略名称标示
有效期	策略生效时间（默认为永久有效）
登录时间段限制	限制用户登录时间，周一~周日每天24小时时间段访问限制
IP限制	通过设置IP/IP端，允许/限制用户访问系统
描述	对策略的描述说明

完成后，单击[下一步]，进入关联用户/用户组界面：



左侧为可选择的用户，右侧为已选择的用户。关联完成后，单击[确定]，即可完成对此条策略的添加

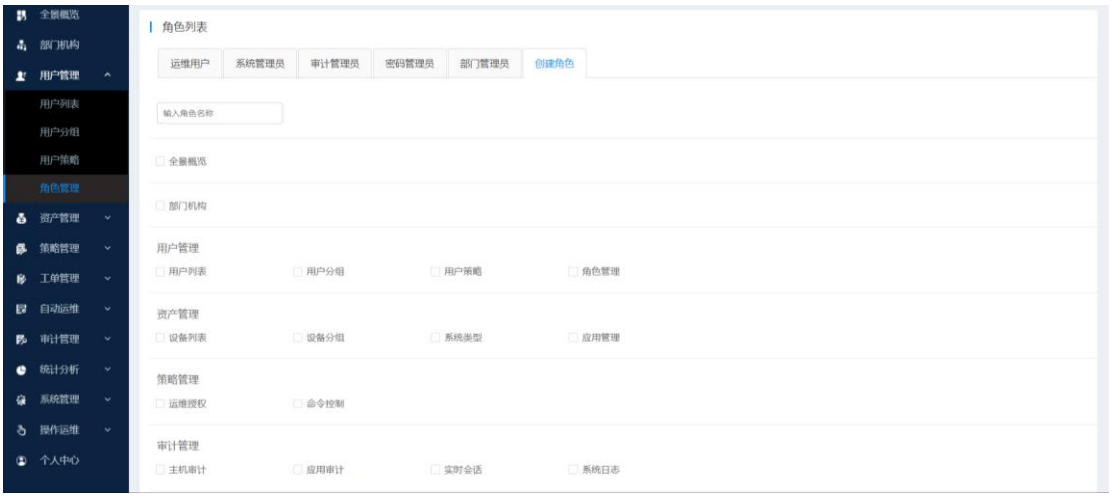
5.4 角色管理

角色管理初始角色包括运维人员、系统管理员、审计管理员、密码管理员（角色权限在 4.1 用户列表中已经给出），初始角色权限无法修改，其余可根据用户使用习惯自定义用户角色。

界面路径：[用户管理]-[角色管理]

5.4.1 创建角色

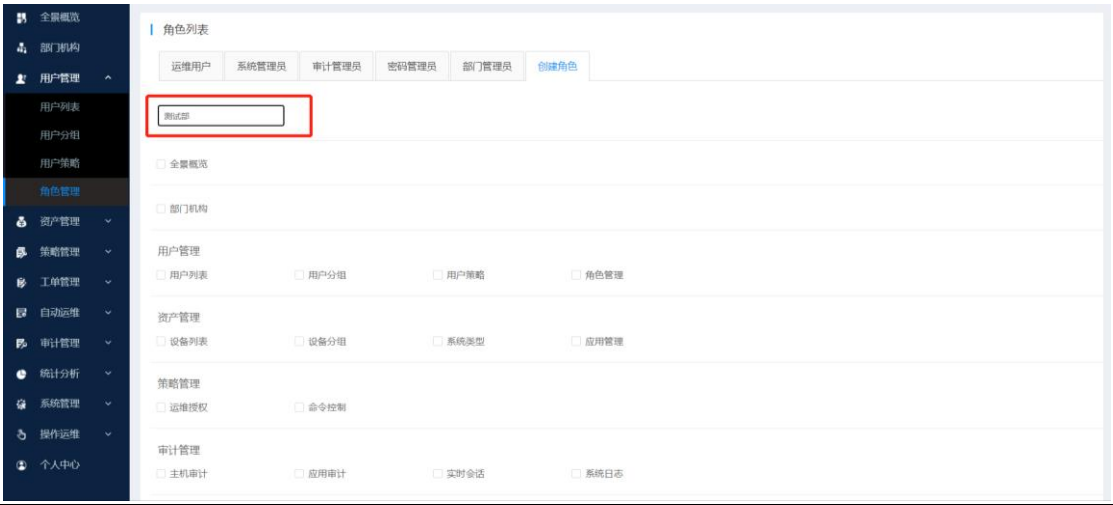
进入，单击[创建角色]，可进入创建角色界面：



输入角色名称，勾选所需的菜单权限信息，然后单击底部[保存]，完成角色创建。

5.4.2 编辑角色

如需要对已创建的角色进行修改，单击已创建的<角色名称>，进行对角色名称和权限进行修改。



修改完成后，单击底部[修改]，即可完成现有角色的编辑，如需删除角色，则直接单击底部[删除]，即可完成删除角色（注：如角色中已有用户绑定，则需将绑定的用户解绑后方可删除）。

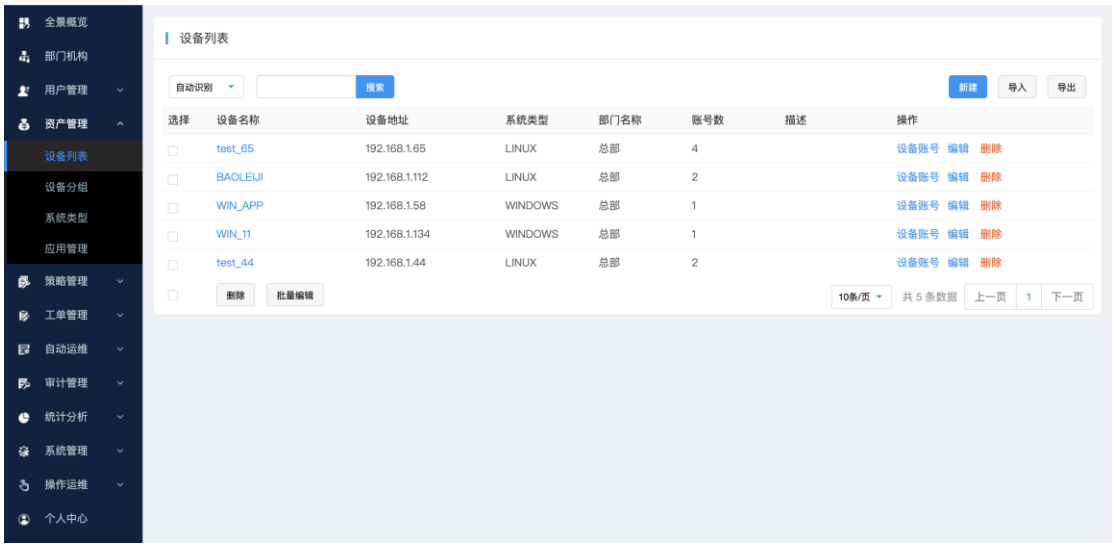
6. 资产管理

资产管理是用于对被管理主机的 IP、主机名、协议、账号、密码、应用资产等功能模块的管理。

6.1 设备列表

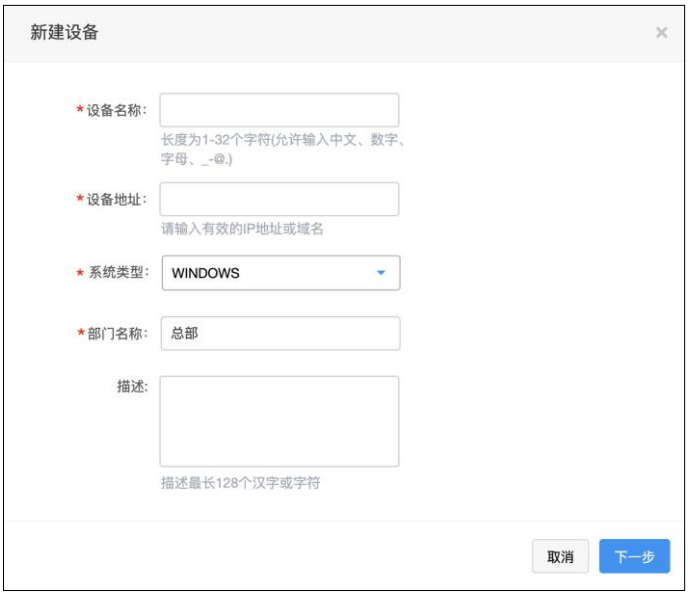
设备列表是用于对被管理主机的 IP、主机名、协议、账号、密码的增删改查等功能。

界面路径：[资产管理]-[设备列表]

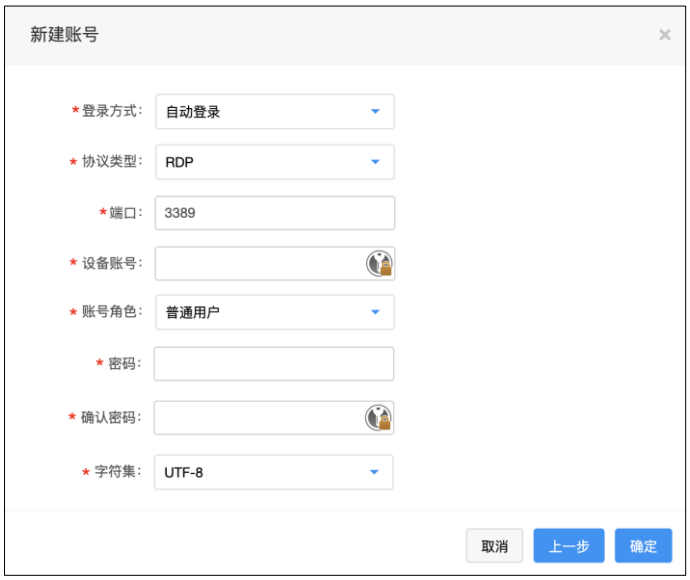


6.1.1 添加设备

单击右上角[新建]，弹出新建设备操作界面：



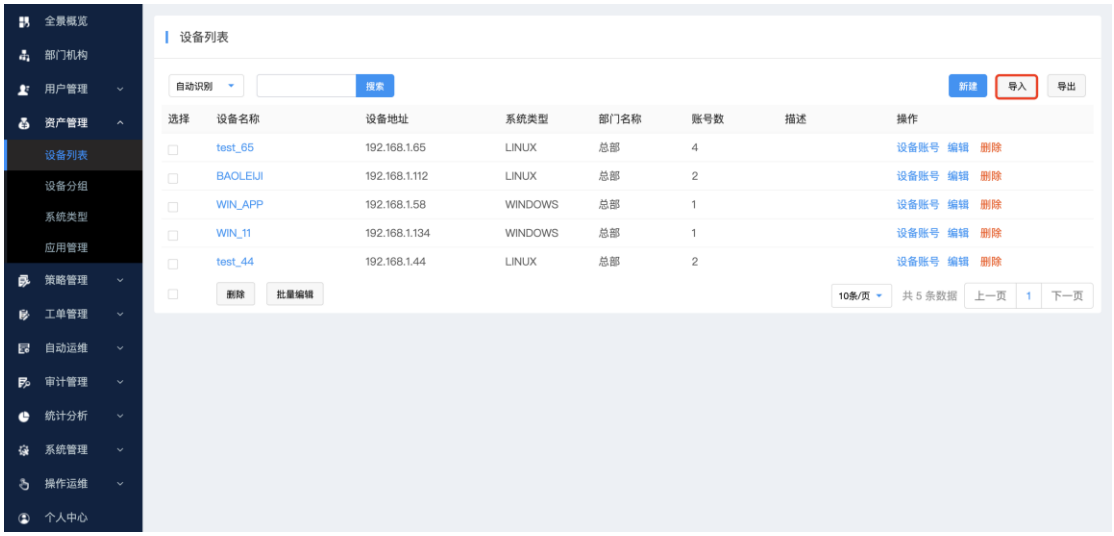
填写设备名称、设备地址，选择系统类型、设备分组，单击[下一步]，进入填写设备账号信息页面：



登录方式可选择自动登录/手动登录，默认自动登录（单点 SSO 登录目标设备），需要填写设备的账号、密码；如手动登录，账号、密码可选择填写，选择协议类型及端口。

6.1.2 导入设备

单击右上角[导入]，弹出导入操作页面：



首先，在下载模板中，单击[点击下载]，下载导入的模板文件

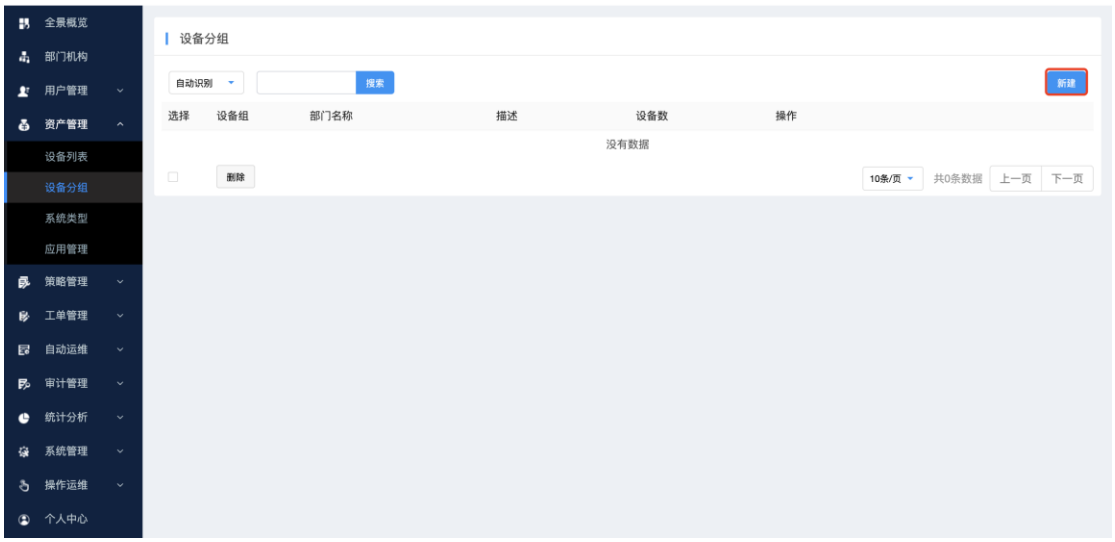
根据下载的模板文件对设备列表信息进行添加，添加完成保存文件后，单击导入页面[选择文件]，进行文件上传，单击确定，在列表中即可显示导入后的设备信息。

6.2 设备分组

界面路径：[设备管理]-[设备分组]

6.2.1 添加设备组

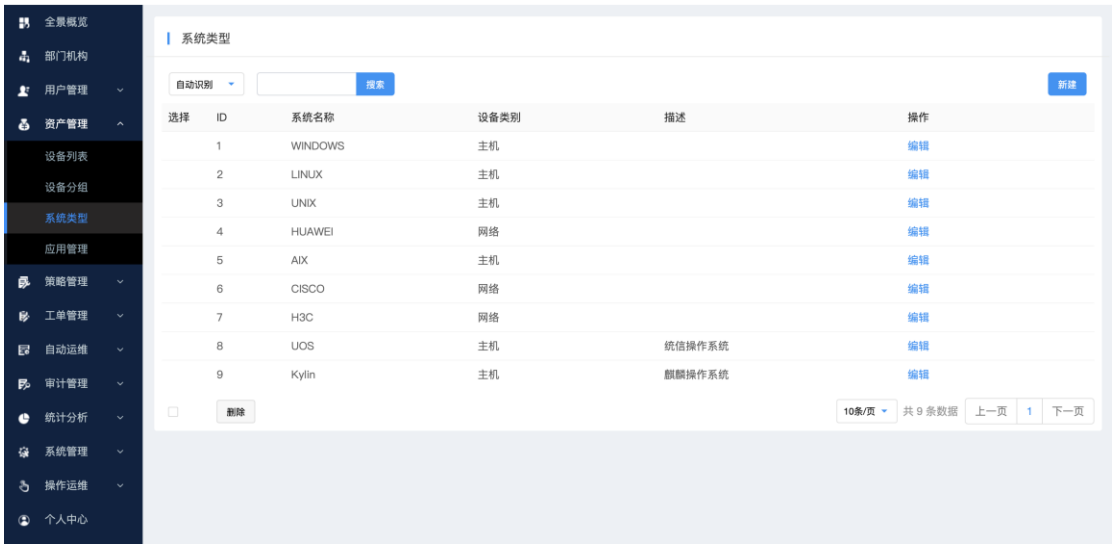
单击右上角[新建]，弹出新建设备分组操作界面：



根据提示，输入设备组名称，描述根据需要进行填写。填写完成后单击[确定]，进行保存。

6.3 系统类型

系统类型作为资产管理中设备的系统的类别区分，可区分当前资产设备的系统类型及协议的优先选择：



系统初始状态包含常见的部分系统类型，如有其它系统类别，可点击右上侧[新建]，进行系统类型的建立：

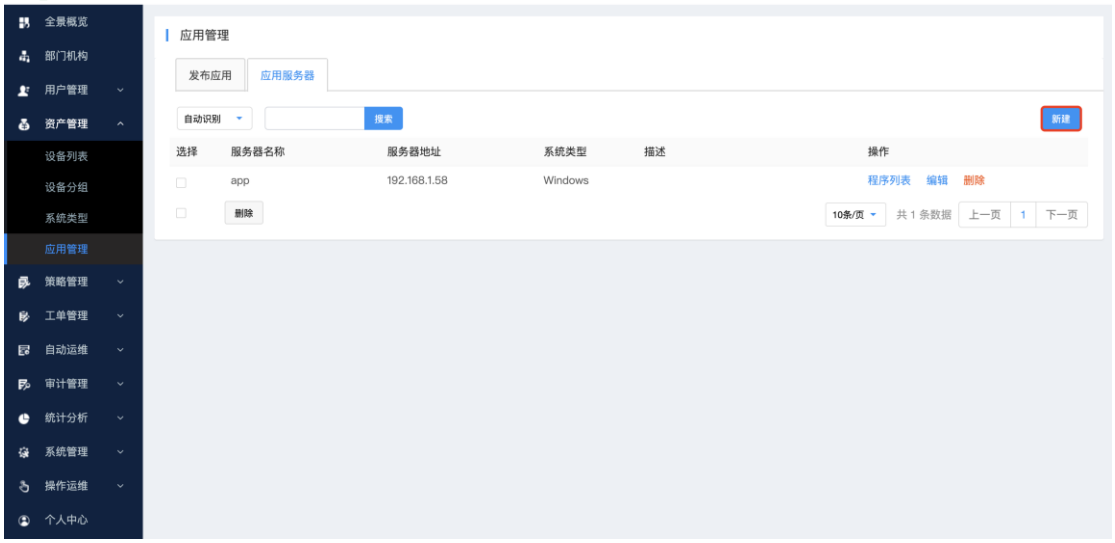
6.4 应用管理

应用管理可以管理应用发布服务器，发布服务器可以集中发布 B/S 或 C/S 应用，比如数据库客户端、防火墙、虚拟化管理软件等所使用的运维管理工具软件。

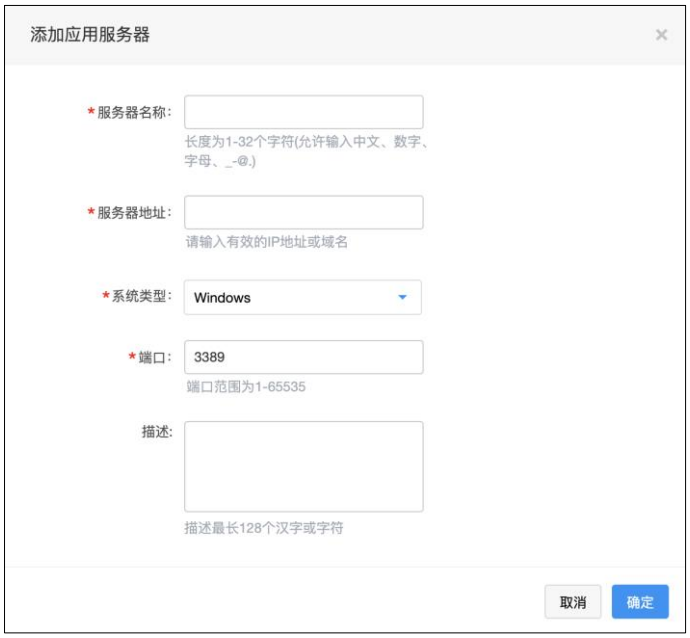
界面路径：[资产管理]-[应用管理]

6.4.1 添加应用服务器

单击[应用服务器]-[新建]，弹出新建应用服务器界面：

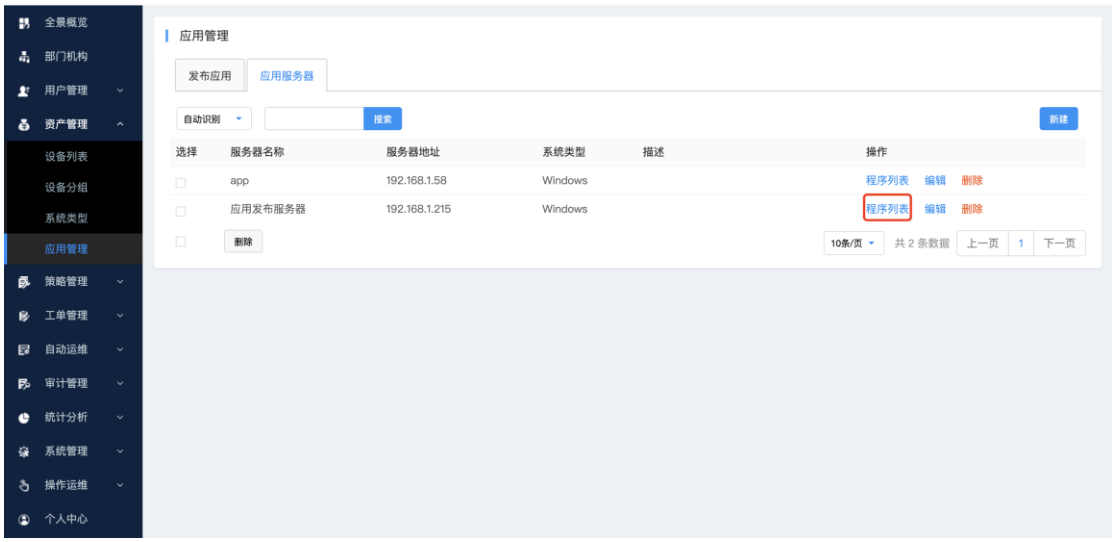


填写服务器名称、服务器地址、部门、端口等信息。完成后单击[确定]，应用发布服务器即可添加成功。（若应用发布服务器为内置发布机，可在服务器地址中直接输入 IP：192.169.12.2，其它默认即可）



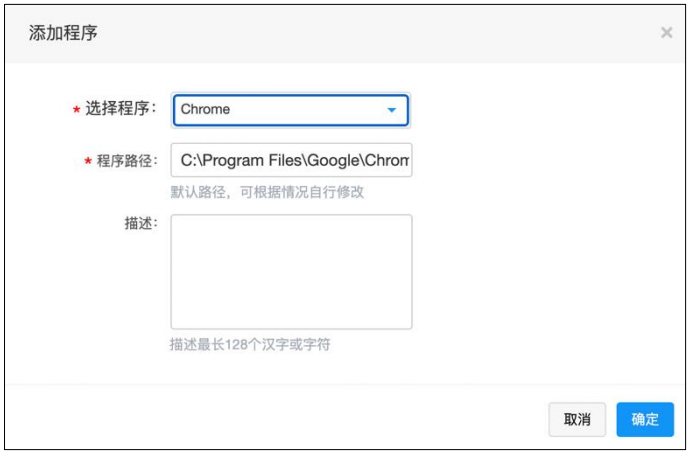
6.4.2 添加应用程序

应用服务器添加完成后，需要对应用发布服务器内的应用程序相关参数进行同步，单击新建的应用服务器右侧[程序列表]

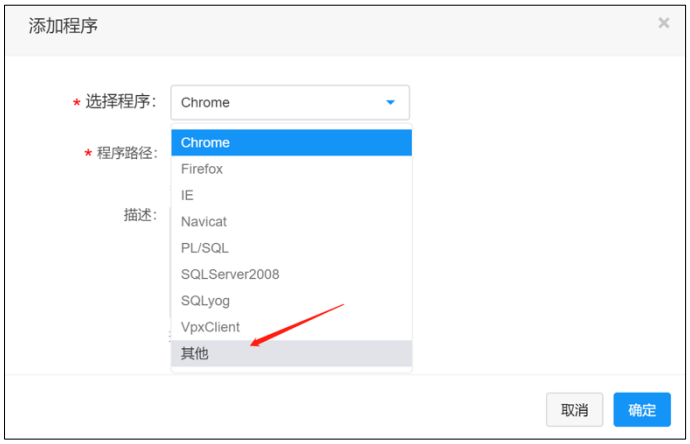


点击[添加程序]

选择需要添加的程序，并指定程序路径（目前内置的应用默认路径有 Chrome 和 Firefox 等，如发布服务器中安装目录有改动，则需要对应发布服务器应用程序的安装路径）



如需要其它程序进行发布管理，可先在应用发布服务器安装相关应用并复制路径后，在此界面添加程序：



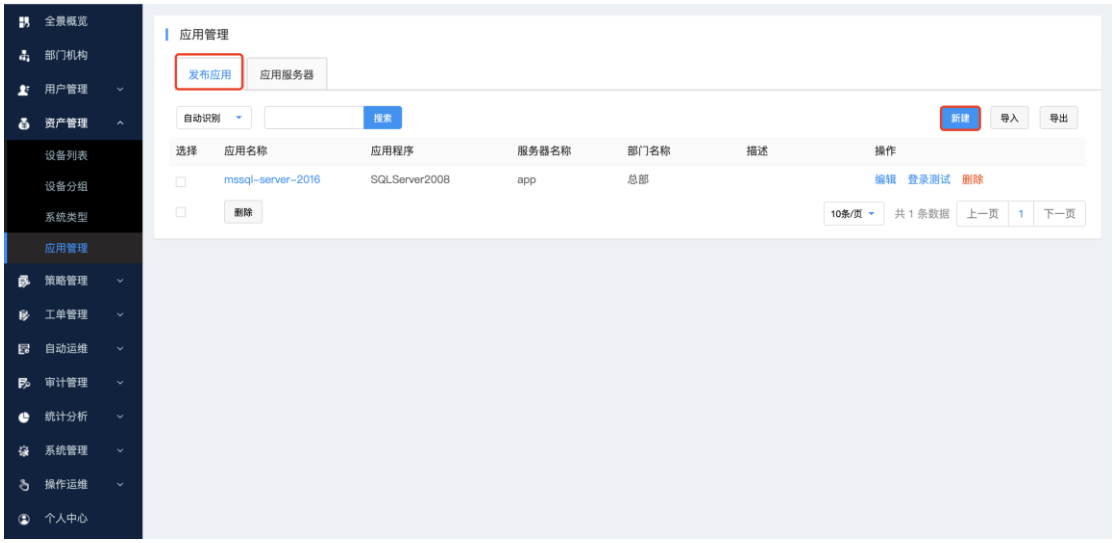
输入程序名称、完整路径，比如 SecureCRT 安装路径：

C:\Program Files(x86)\SecureCRT-CHS\SecureCRT.exe 复制录入到程序路径里，点击确定。

添加完成后，会有“新建成功”的提示，同时程序会自动显示到程序列表中

6.4.3 发布应用

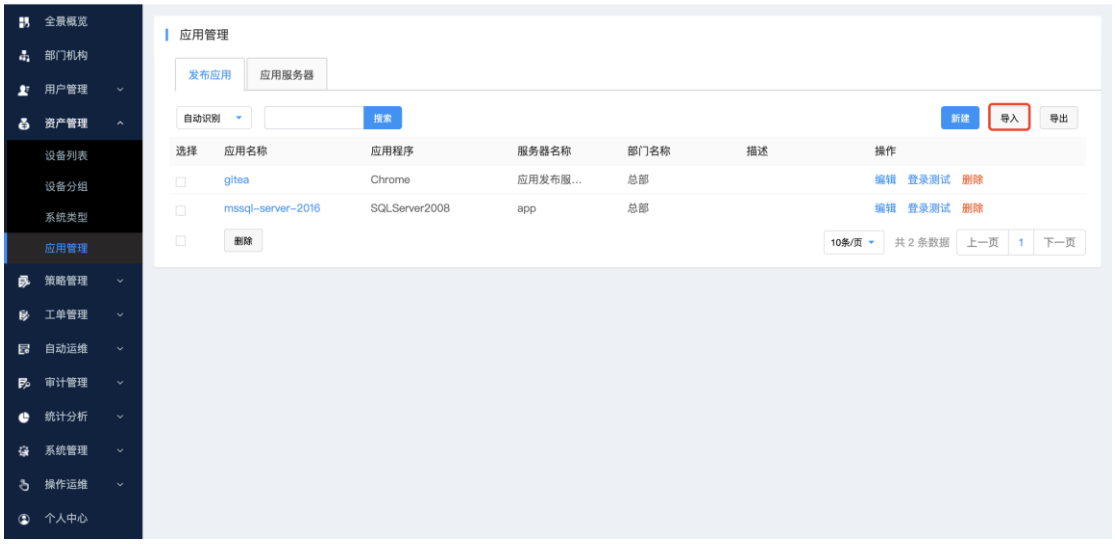
单击[发布应用]-右侧[新建]，进入发布应用界面：



根据提示填写应用名称、用户名、密码、访问地址，选择应用程序。单击<确定>，即可完成此应用的发布。

- **批量导入应用：**

单击右上角[导入]，弹出导入操作页面：



首先，在下载模板中，单击[点击下载]，下载导入的模板文件

根据下载的模板文件对发布的应用信息进行添加，添加完成保存文件后，单击导入页面[选择文件]，进行文件上传，单击确定，在发布应用中即可显示导入后的应用信息。

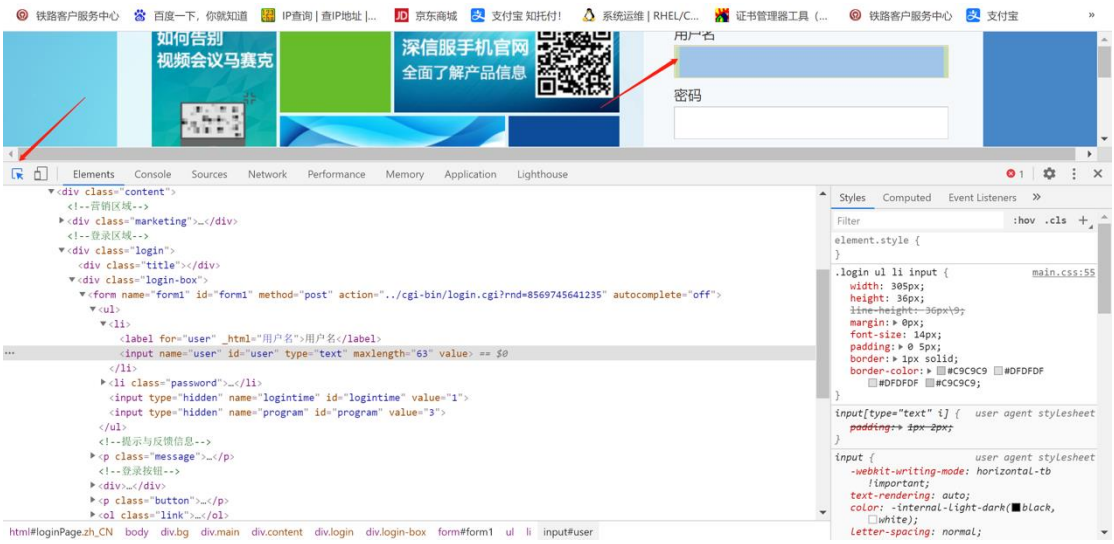
6.4.4 浏览器密码代填不成功处理办法

B/S 密码代填默认为通用方式，如页面比较特殊，无法进行默认自动代填（发布后，通过应用运维打开应用，用户名密码无法代填），则此时代填方式可选择，自定义。

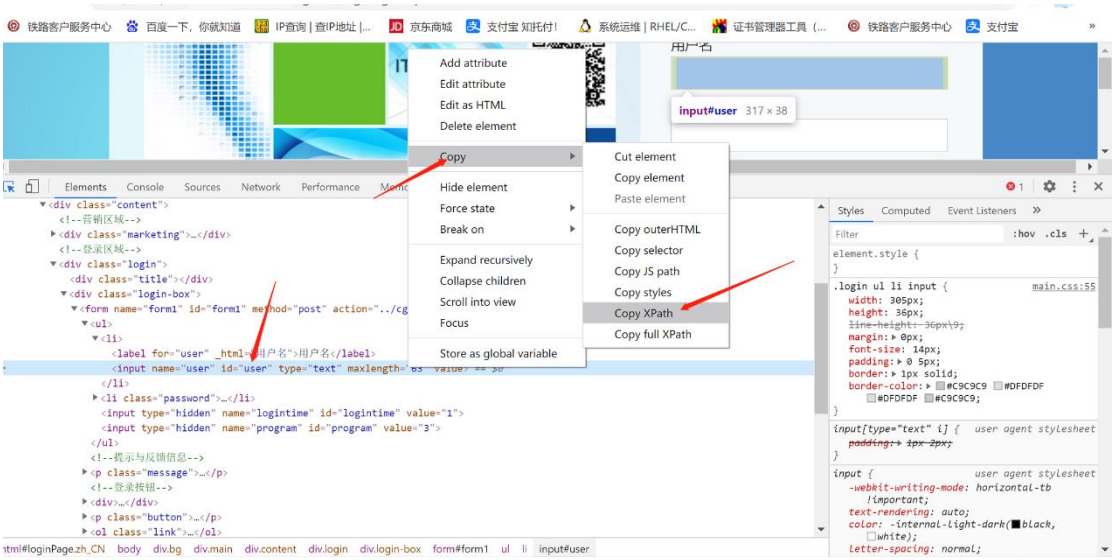
输入用户名 xpath 及密码 xpath 信息

xpath 信息获取方式：

首先通过浏览器打开需要发布的 web 应用界面，通过键盘 F12(开发者工具)，选择左上角图标，把鼠标放入用户名输入框中。



此时调试器会自动移动到用户名代码界面，鼠标右键选择：Copy-Copy XPath，此时，用户名 xpath 参数已拷贝，粘贴到发布应用的用户名 xpath 输入框中。



（例如：//*[@id="user"]）

保存后，即可再次登录测试代填情况。

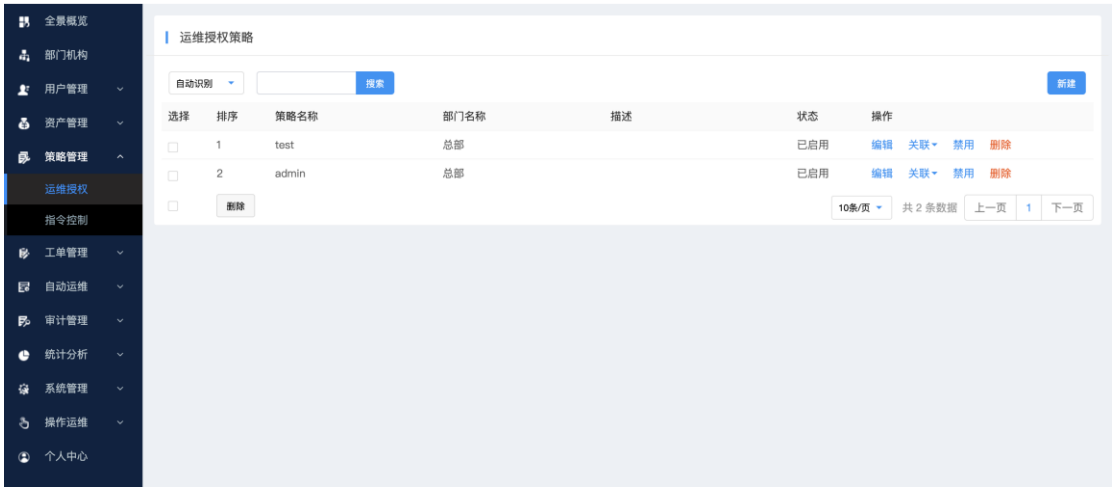
7. 策略管理

策略管理模块负责运维用户访问策略控制、设备授权及对操作指令的限制等安全访问策略功能。

7.1 运维授权

7.1.1 添加运维授权策略

进入[策略管理]-[运维授权]，单击右上角[新建]，进入新建运维授权策略界面：

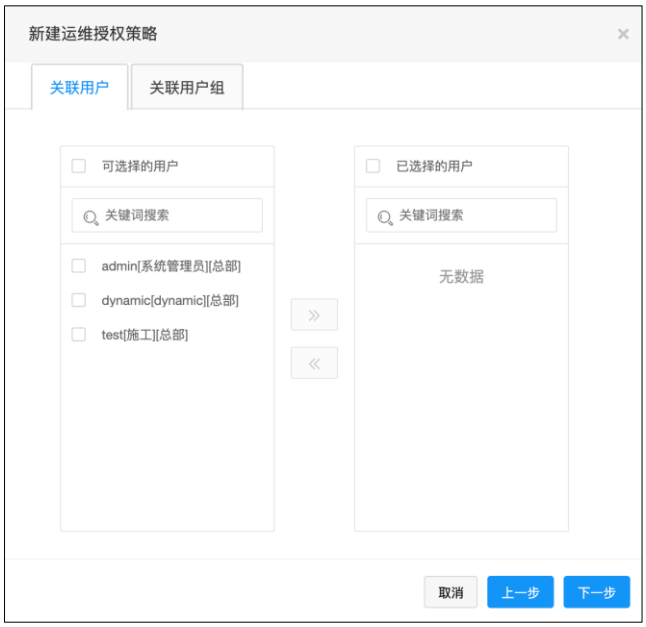


填写对应的输入项，具体功能说明如下：

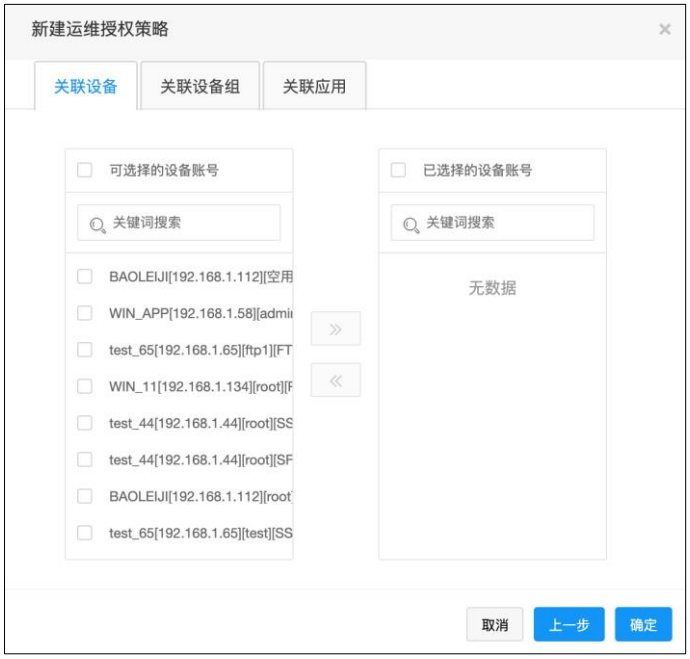
输入项	说明
策略名称	授权策略名称标示
有效期	策略生效时间（默认为永久有效）

文件传输	设置是否允许此策略下的运维用户再访问设备的上传/下载文件权限
登录时间段限制	限制用户登录时间，周一~周日每天24小时时间段访问限制
IP限制	通过设置IP/IP端，允许/限制用户访问系统
描述	对策略的描述说明

完成后，单击[下一步]，进入关联用户/用户组界面：



左侧为可选择的用户，右侧为已选择的用户。关联完成后，单击[下一步]，进入关联设备/设备组/应用界面：

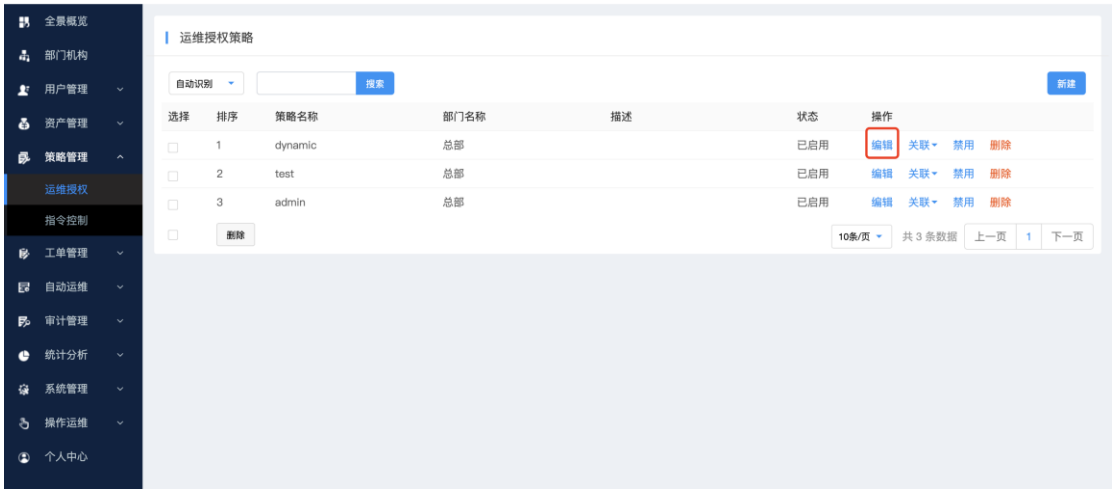


左侧为可选择的设备/设备组/应用，右侧为已选择的设备/设备组/应用。关联完成后，单击<确定>，即可完成对此条策略的添加。

7.1.2 编辑/维护控制策略

编辑策略信息：

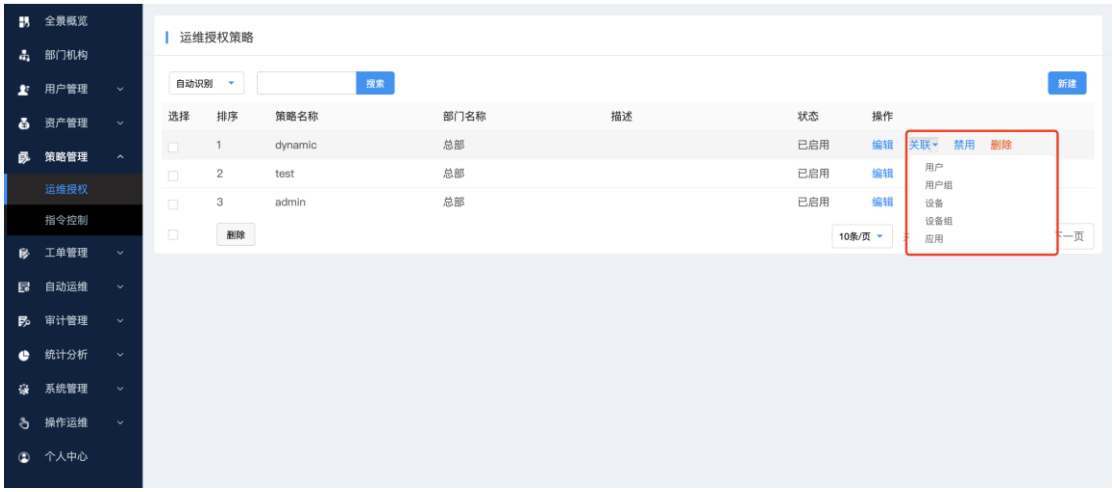
单击新建策略列表中有右侧[编辑]，进入编辑策略页面



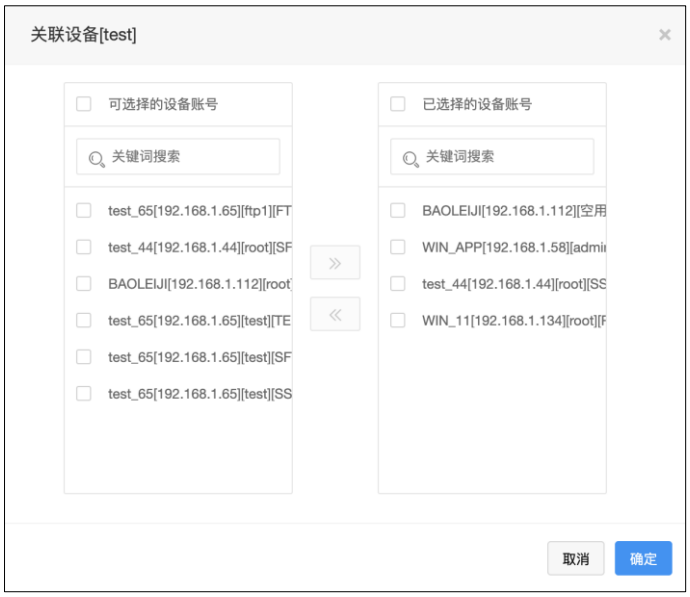
根据制定策略，进行对策略的编辑。

关联用户/资产信息：

单击新建策略列表中有右侧[关联]，弹出关联功能：



可关联用户/用户组/设备/设备组等权限信息：



7.2 指令控制

“指令控制”策略，是通过设置命令/命令集，实现实时监控操作的命令，并根据命令危险级别做出响应。

7.2.1 指令策略

界面路径：[策略管理]-[指令控制]

对指令的控制，分为允许执行、指令申请、指令阻断、会话阻断四种方式，具体说明如下：

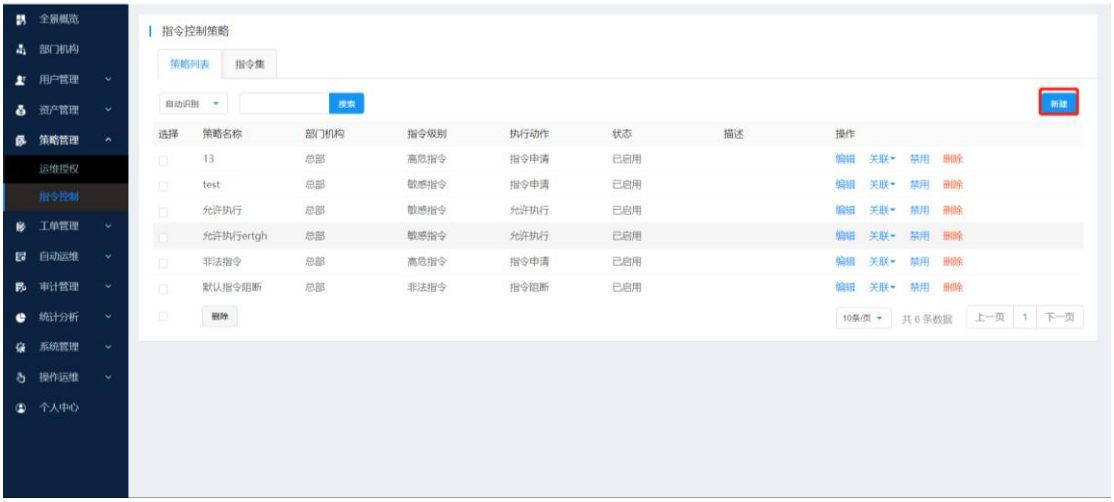
执行动作	说明
允许执行	当触发策略后，只有此策略下的动作指令可以执行，其它指令无法执行

指令申请	当触发策略后，需要授权人进行再次授权后，当前动作才能执行
指令阻断	当触发策略后，当前动作执行无效
会话阻断	当触发策略后，当前动作会触发会话自动断开

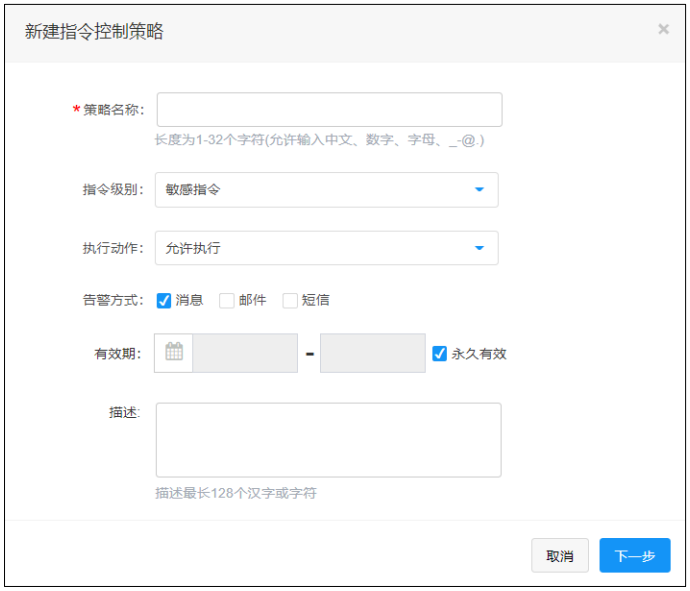
指令级别分为敏感指令、高危指令、非法指令三种级别，具体说明如下：

指令级别	说明
敏感指令	执行动作范围为允许执行、指令申请、指令阻断、会话阻断
高危指令	执行动作范围为指令申请、指令阻断、会话阻断
非法指令	执行动作范围为指令阻断、会话阻断

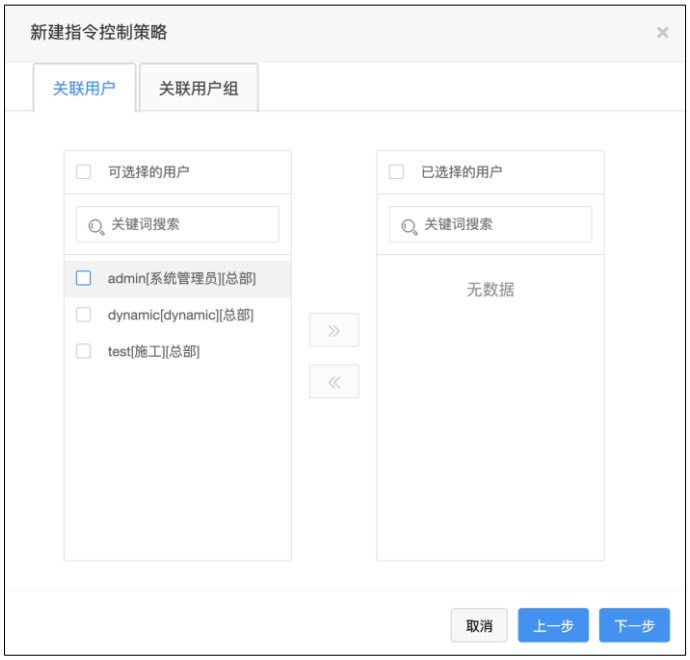
具体配置：单击右侧[新建]，进入指令控制策略界面：



填写策略名称、指令级别、执行动作（上页已经说明）、有效期、描述：



填写完成后，单击[下一步]，进入关联用户/用户组界面：

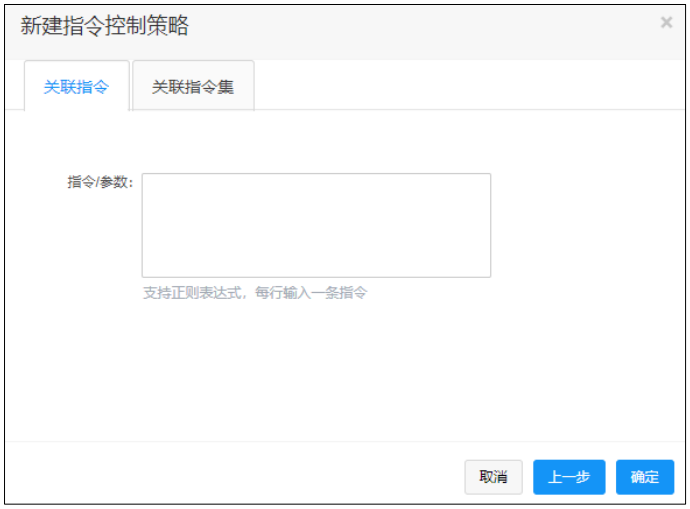


左侧为可选择的用户，右侧为已选择的用户。关联完成后，单击[下一步]，进入关联设备/设备组界面：

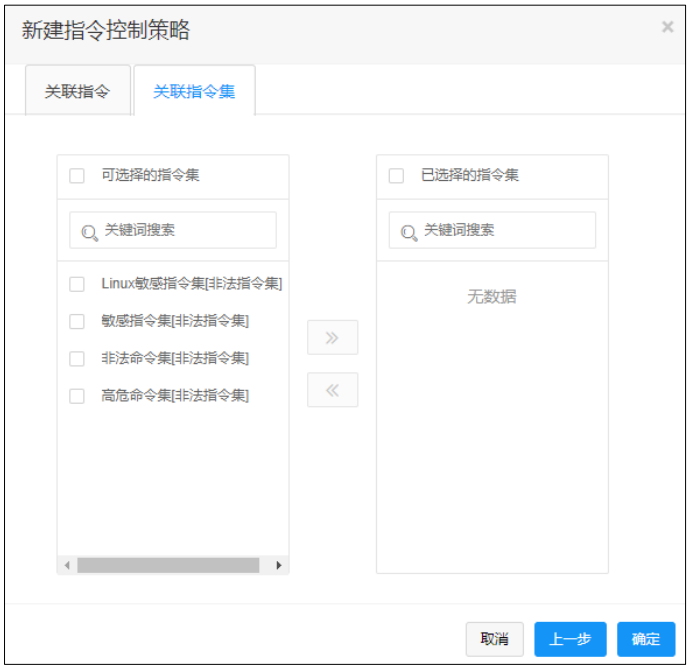
注：应指令控制只是关联命令行（SSH/TELNET）设备信息，故关联设备/关联设备组中只显示 SSH/TELNET 协议的设备信息。

左侧为可选择的设备/设备组，右侧为已选择的设备/设备组。关联完成后，单击[下一步]，进入关联命令/命令集界面：

[关联命令] 可直接填写具体命令进行关联，关联界面如下：



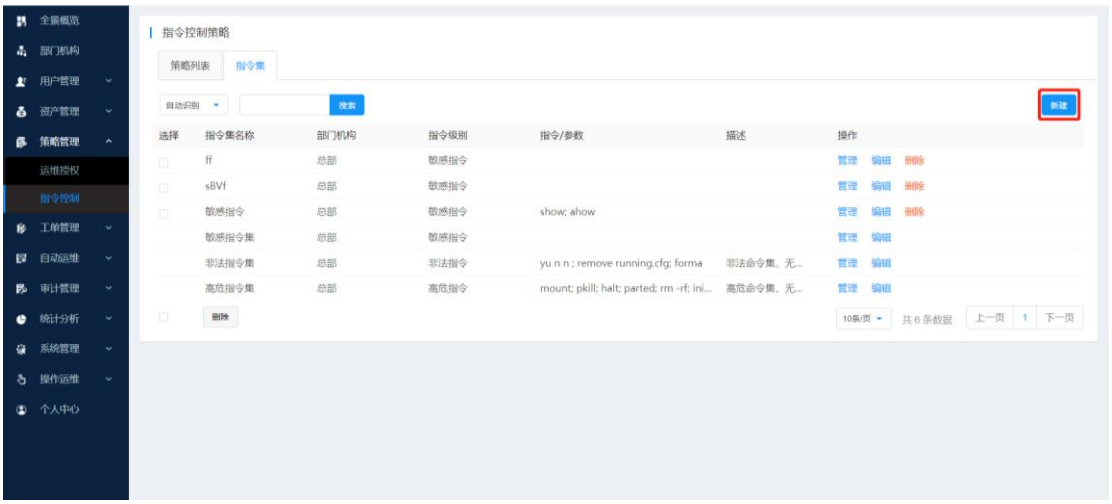
[关联指令集] 如需多个指令同时下发同一策略，可使用关联指令集方式（指令集配置 7.2.2 说明）进行关联，关联界面如下：



7.2.2 指令集配置

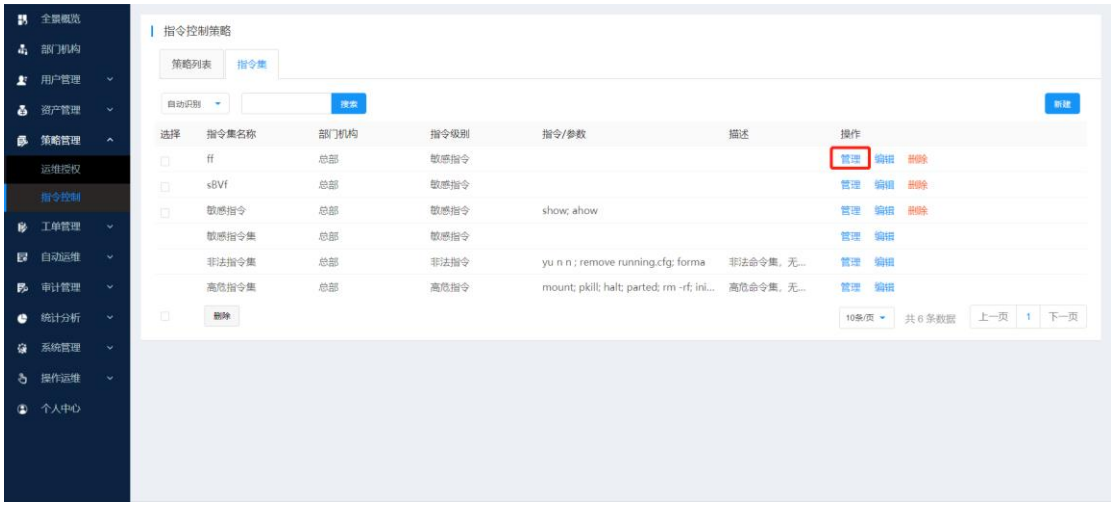
指令集可设置多个指令在一个指令集中，方便快速建立策略及关联相同策略的多个指令的集合。具体步骤如下：

单击右侧[新建]，进入新建指令集界面：



填写指令集名称、指令级别。

单击指令控制策略列表中有右侧<管理>，进入指令集管理页面。



单击右侧<添加指令>，填写指令/参数、风险描述等，进入添加指令界面：

<指令/参数>说明：支持正则表达式。

填写完成后，单击[确定]，完成添加指令操作，具体关联策略可参照 7.2.1 说明。

8 工单管理

工单管理-运维用户向管理员提交访问设备的申请，管理员可批准申请或驳回申请，部门管理员也有提交申请工单以及审批运维用户工单的权限。

8.1 工单申请

运维用户申请工单流程：

[工单管理]-[工单申请]-[新建]-“添加工单申请”引导-提交工单申请

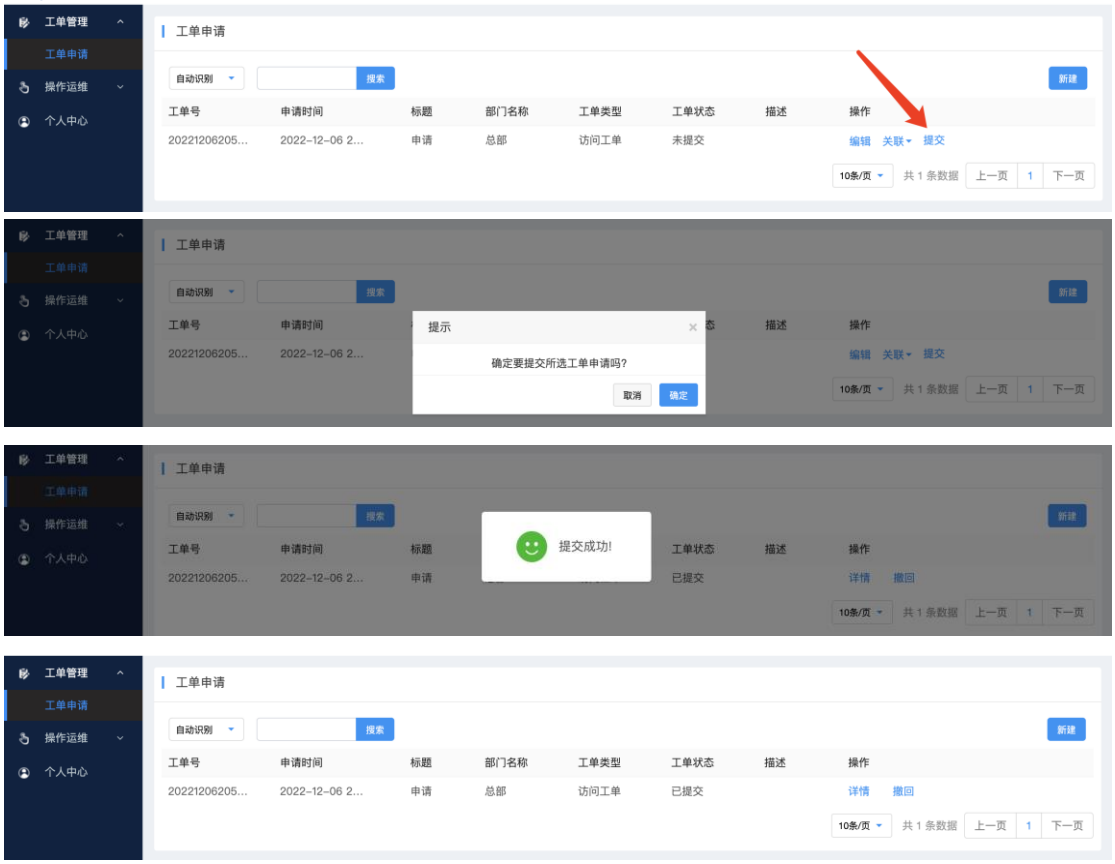
进入**[工单管理]-[工单申请]**新建工单申请。

编辑标题，设置运维时间、文件选项、描述，并选择 [下一步]

在[关联设备]中，从“可选择的设备帐号”导引到“已选择的设备帐号”，并点击[确认]完成引导，看到提示[新建成功！]则表示工单申请记录创建成功。

在点击[提交]按钮之前，您仍可以继续修改工单申请记录，提交申请记录之后，则不能再修改已提交

的工单申请记录，但可以撤回之前的申请。



当管理员批准工单后，则可以获得相关资产的访问权限。

下图所示为工单申请批准前后可访问运维资产对比：

图8-1 工单申请批准前

图8-2 工单申请批准后

8.2 工单审批

管理员在**[工单管理]-[工单审批]**中进行批准或驳回操作。

补充：部门管理员也能够审批运维用户提交的工单以及向管理员提交工单申请。

9 自动运维

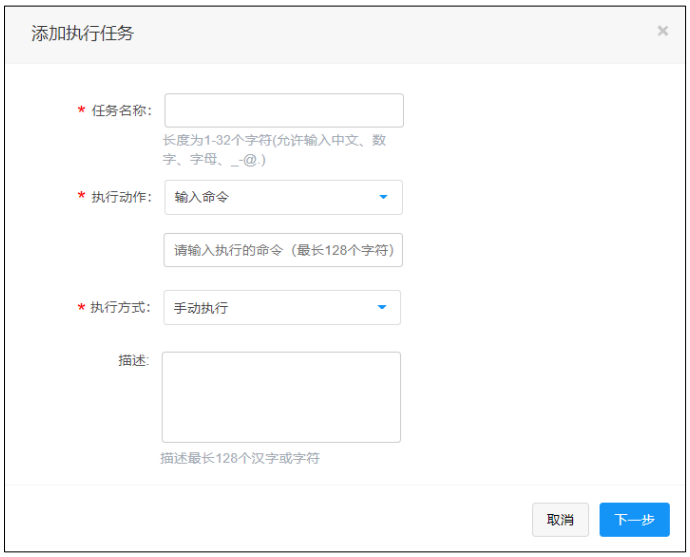
自动运维是指根据管理员需要，通过设置执行策略，按命令/脚本按计划自动执行关联目标，输出执行结果。

9.1 任务列表

界面路径：[自动运维]-[任务列表]

执行任务中列出任务名称等信息，如需创建自动运维任务，点击[新建]

填写执行任务信息，包括：任务名称、执行命令/脚本、执行方式等信息。



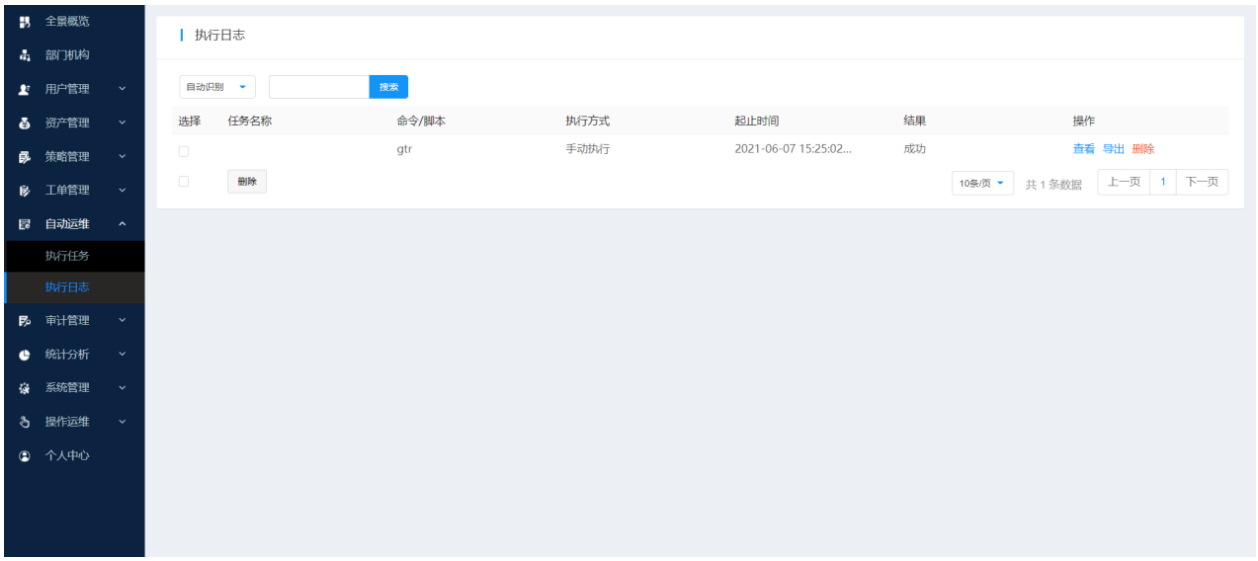
说明：执行方式可按照手动执行、定时执行和周期执行三个方式进行对命令/脚本进行执行。

点击<下一步>，进入关联设备界面

左侧为可选择的设备/设备组，右侧为已选择的设备/设备组。关联完成后，单击<确定>，即可完成对此条任务的添加。

9.2 执行日志

执行日志是对执行任务的执行情况及输出详细结果进行记录，形成详细的执行日志；



点击[查看]，可显示执行日志的详细记录及输出情况：

点击[导出]，通过EXCEL形式导出本次任务条目详细日志信息。

	A	B	C	D	E	F	G	H
1	设备地址	设备端口	设备用户	命令/脚本	开始时间	结束时间	执行结果	
2	47.93.55.22	22	longer	pwd	2020/8/27 16:43	2020/8/27 16:43	/home/longer	
3								
4								
5								
6								

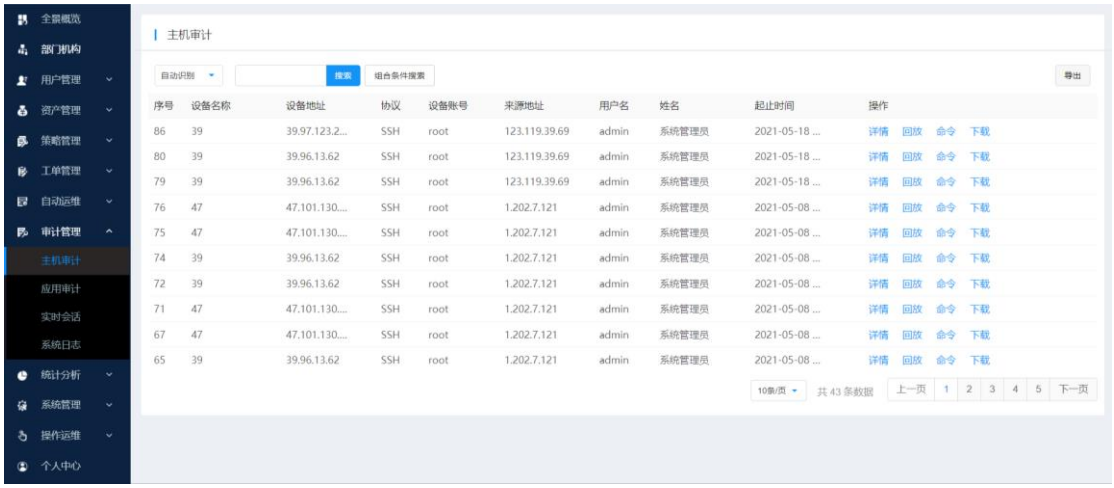
10 审计管理

审计管理是系统的主要核心模块，用于审计和管理运维人员对主机的访问操作的全部日志。

10.1 主机审计

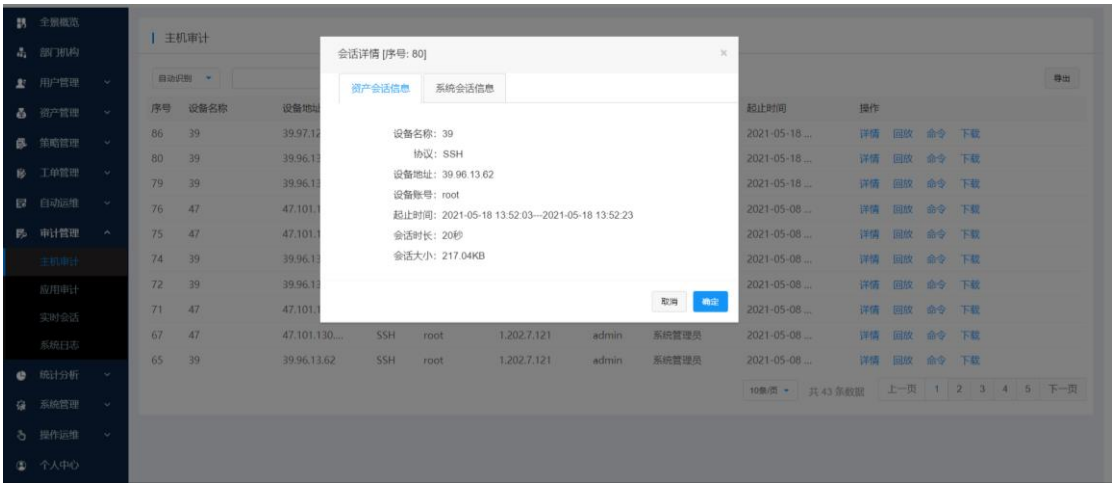
主机审计主要用户对图形、字符、文件传输协议的会话的过程进行记录并形成完整审计会话。审计内容包括:

设备名称、设备地址、协议、设备账号、来源地址、运维用户、姓名、起止时间等信息。



右侧<操作>，可进行会话详细查看、回放和下载审计录像功能。

会话详情：

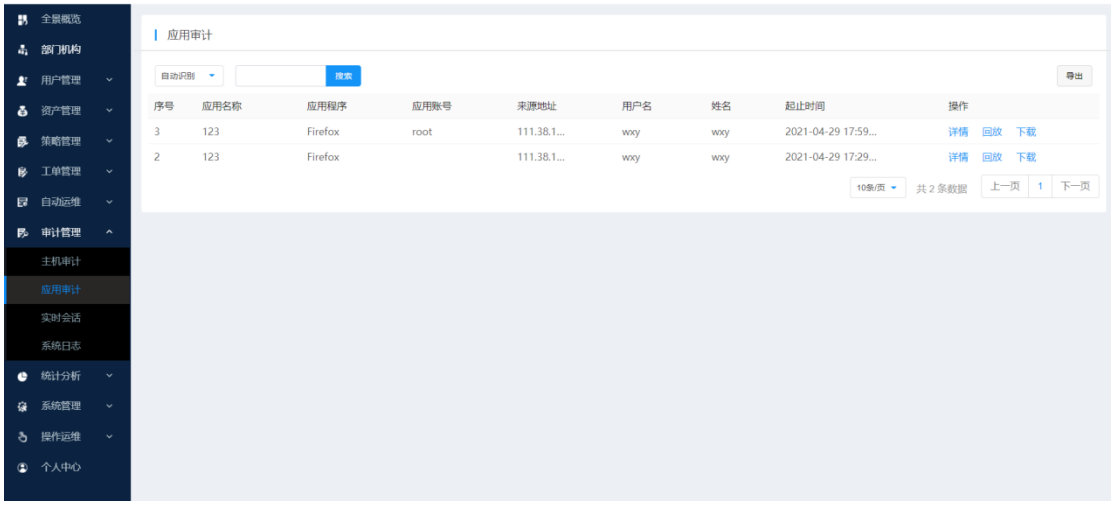


审计回放：

10.2 应用审计

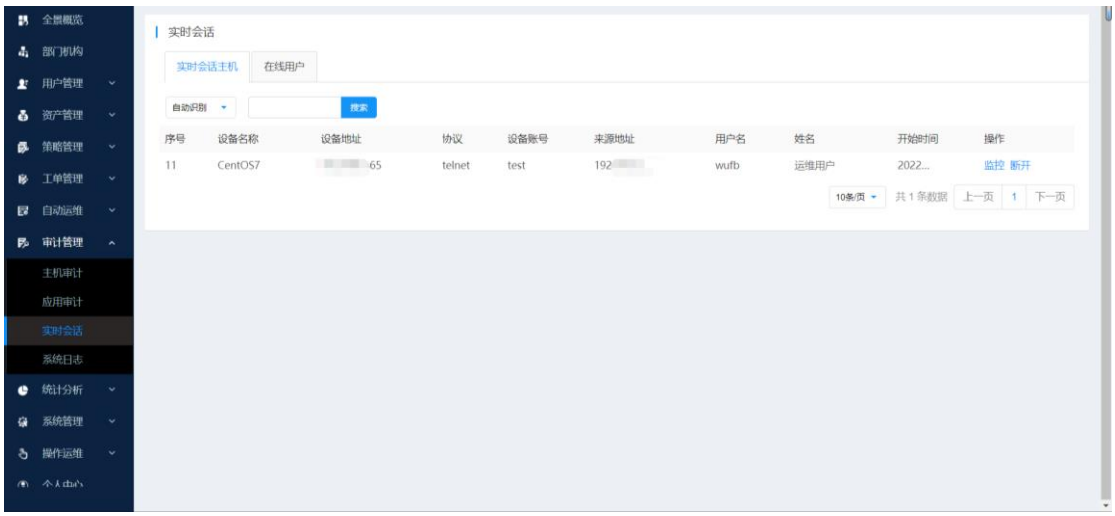
应用审计主要用户对通过应用发布服务器使用的的应用会话的过程进行记录并形成完整审计会话。审计内容包括：

应用名称、应用程序、应用账号、来源地址、运维用户、姓名、起止时间等。



10.3 实时会话

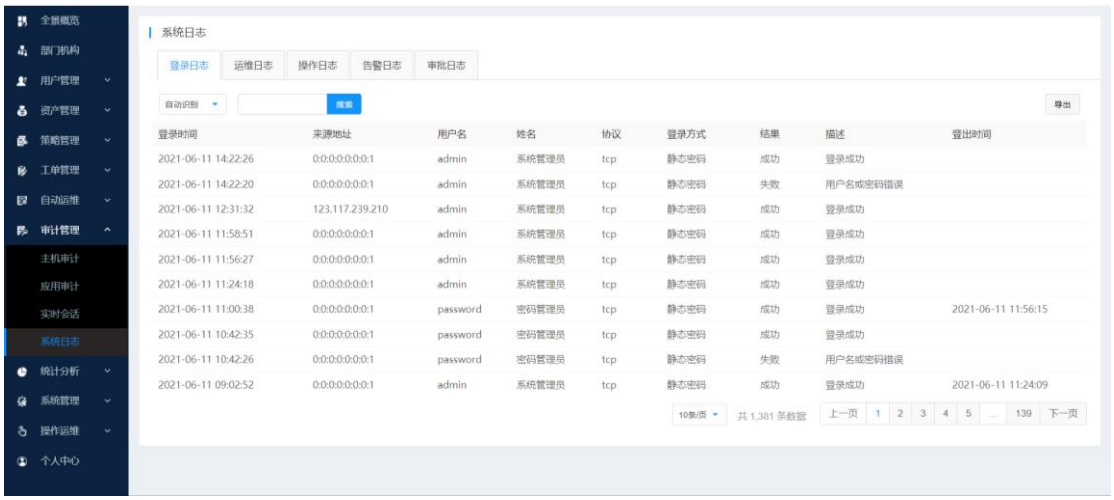
实时会话为系统当前运维用户访问设备的实时画面，管理员可实时监控运维人员访问设备的画面，必要时可断开当前会话信息。



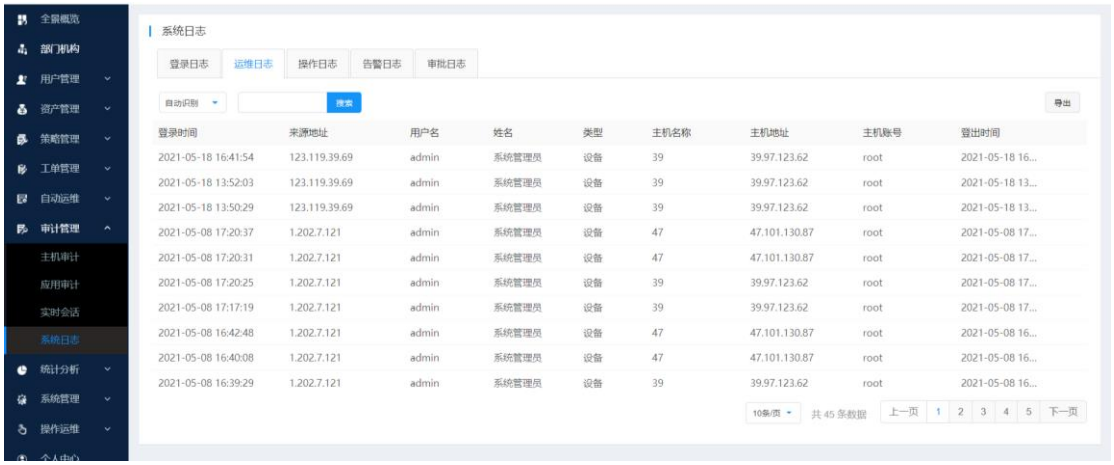
10.4 系统日志

系统日志功能可以查看系统运行的日志，包括系统登录日志、运维日志、操作日志、告警日志以及审批日志。

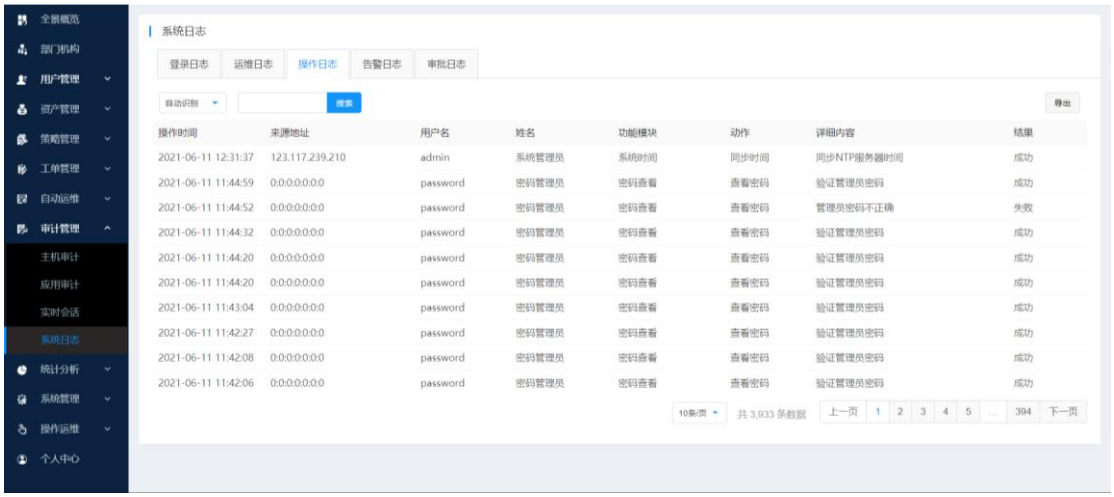
登录日志：


全景概览
部门机构
用户管理
资产管理
策略管理
工单管理
自动运维
审计管理
主机审计
应用审计
实时会话
系统日志
统计分析
系统管理
操作运维
个人中心
系统日志
登录日志
运维日志
操作日志
告警日志
审批日志
自动识别
搜索
导出
登录时间 来源地址 用户名 姓名 协议 登录方式 结果 描述 登出时间
2021-06-11 14:22:26 0:0:0:0:0:0:0:1 admin 系统管理员 tcp 静态密码 成功 登录成功
2021-06-11 14:22:20 0:0:0:0:0:0:0:1 admin 系统管理员 tcp 静态密码 失败 用户名或密码错误
2021-06-11 12:31:32 123.117.239.210 admin 系统管理员 tcp 静态密码 成功 登录成功
2021-06-11 11:58:51 0:0:0:0:0:0:0:1 admin 系统管理员 tcp 静态密码 成功 登录成功
2021-06-11 11:56:27 0:0:0:0:0:0:0:1 admin 系统管理员 tcp 静态密码 成功 登录成功
2021-06-11 11:24:18 0:0:0:0:0:0:0:1 admin 系统管理员 tcp 静态密码 成功 登录成功
2021-06-11 11:00:38 0:0:0:0:0:0:0:1 password 密码管理员 tcp 静态密码 成功 登录成功 2021-06-11 11:56:15
2021-06-11 10:42:35 0:0:0:0:0:0:0:1 password 密码管理员 tcp 静态密码 成功 登录成功
2021-06-11 10:42:26 0:0:0:0:0:0:0:1 password 密码管理员 tcp 静态密码 失败 用户名或密码错误
2021-06-11 09:02:52 0:0:0:0:0:0:0:1 admin 系统管理员 tcp 静态密码 成功 登录成功 2021-06-11 11:24:09
10条/页 共 1,381 条数据 上一页 1 2 3 4 5 ... 139 下一页

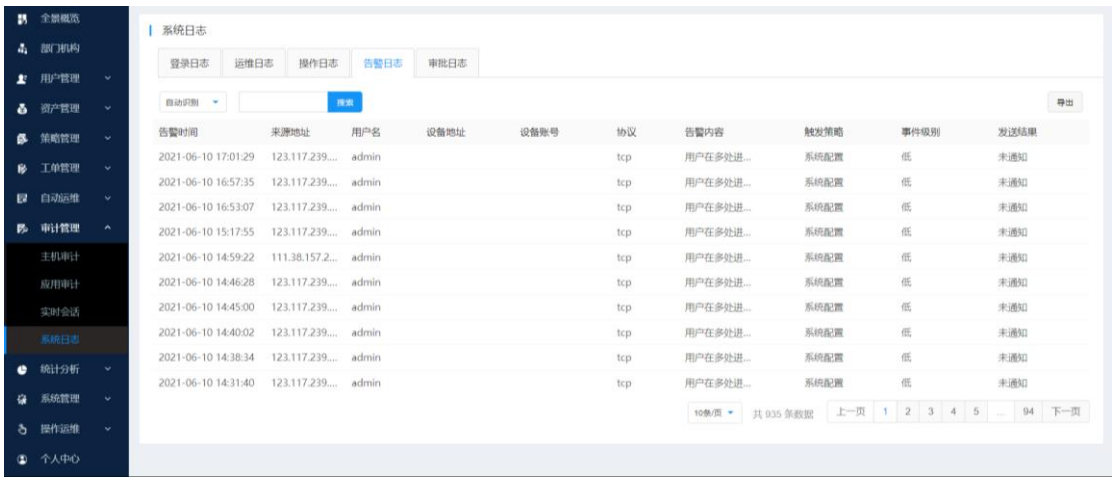
运维日志：


全景概览
部门机构
用户管理
资产管理
策略管理
工单管理
自动运维
审计管理
主机审计
应用审计
实时会话
系统日志
统计分析
系统管理
操作运维
个人中心
系统日志
登录日志
运维日志
操作日志
告警日志
审批日志
自动识别
搜索
导出
登录时间 来源地址 用户名 姓名 类型 主机名称 主机地址 主机账号 登出时间
2021-05-18 16:41:54 123.119.39.69 admin 系统管理员 设备 39 39.97.123.62 root 2021-05-18 16...
2021-05-18 13:52:03 123.119.39.69 admin 系统管理员 设备 39 39.97.123.62 root 2021-05-18 13...
2021-05-18 13:50:29 123.119.39.69 admin 系统管理员 设备 39 39.97.123.62 root 2021-05-18 13...
2021-05-08 17:20:37 1.202.7.121 admin 系统管理员 设备 47 47.101.130.87 root 2021-05-08 17...
2021-05-08 17:20:31 1.202.7.121 admin 系统管理员 设备 47 47.101.130.87 root 2021-05-08 17...
2021-05-08 17:20:25 1.202.7.121 admin 系统管理员 设备 39 39.97.123.62 root 2021-05-08 17...
2021-05-08 17:17:19 1.202.7.121 admin 系统管理员 设备 39 39.97.123.62 root 2021-05-08 17...
2021-05-08 16:42:48 1.202.7.121 admin 系统管理员 设备 47 47.101.130.87 root 2021-05-08 16...
2021-05-08 16:40:08 1.202.7.121 admin 系统管理员 设备 47 47.101.130.87 root 2021-05-08 16...
2021-05-08 16:39:29 1.202.7.121 admin 系统管理员 设备 39 39.97.123.62 root 2021-05-08 16...
10条/页 共 45 条数据 上一页 1 2 3 4 5 下一页

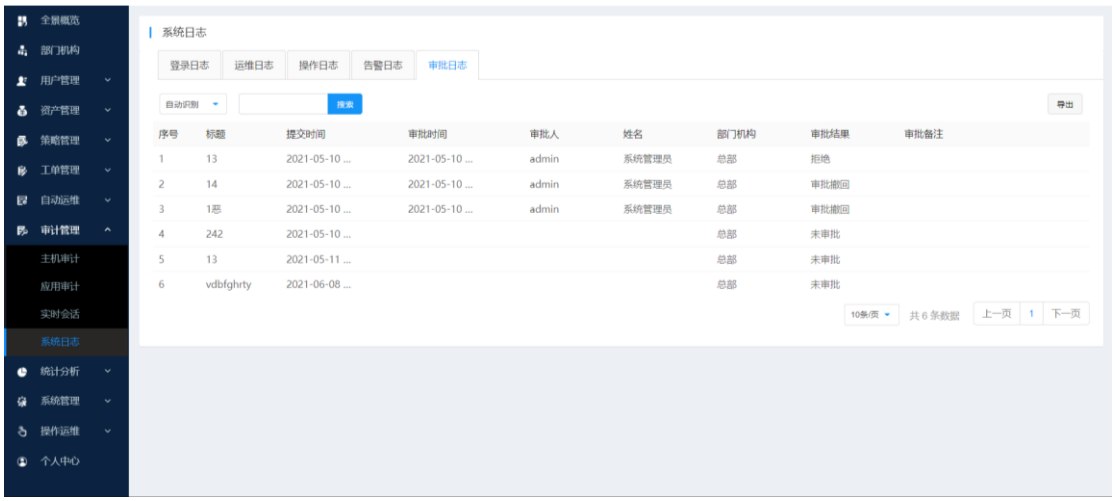
操作日志：


全景概览
部门机构
用户管理
资产管理
策略管理
工单管理
自动运维
审计管理
主机审计
应用审计
实时会话
系统日志
统计分析
系统管理
操作运维
个人中心
系统日志
登录日志
运维日志
操作日志
告警日志
审批日志
自动识别
搜索
导出
操作时间 来源地址 用户名 姓名 功能模块 动作 详细内容 结果
2021-06-11 12:31:37 123.117.239.210 admin 系统管理员 系统时间 同步时间 同步NTP服务器时间 成功
2021-06-11 11:44:59 0:0:0:0:0:0:0:0 password 密码管理员 密码查看 查看密码 验证管理员密码 成功
2021-06-11 11:44:52 0:0:0:0:0:0:0:0 password 密码管理员 密码查看 查看密码 管理员密码不正确 失败
2021-06-11 11:44:32 0:0:0:0:0:0:0:0 password 密码管理员 密码查看 查看密码 验证管理员密码 成功
2021-06-11 11:44:20 0:0:0:0:0:0:0:0 password 密码管理员 密码查看 查看密码 验证管理员密码 成功
2021-06-11 11:44:20 0:0:0:0:0:0:0:0 password 密码管理员 密码查看 查看密码 验证管理员密码 成功
2021-06-11 11:43:04 0:0:0:0:0:0:0:0 password 密码管理员 密码查看 查看密码 验证管理员密码 成功
2021-06-11 11:42:27 0:0:0:0:0:0:0:0 password 密码管理员 密码查看 查看密码 验证管理员密码 成功
2021-06-11 11:42:08 0:0:0:0:0:0:0:0 password 密码管理员 密码查看 查看密码 验证管理员密码 成功
2021-06-11 11:42:06 0:0:0:0:0:0:0:0 password 密码管理员 密码查看 查看密码 验证管理员密码 成功
10条/页 共 3,933 条数据 上一页 1 2 3 4 5 ... 394 下一页

告警日志：



审批日志：



11 统计分析

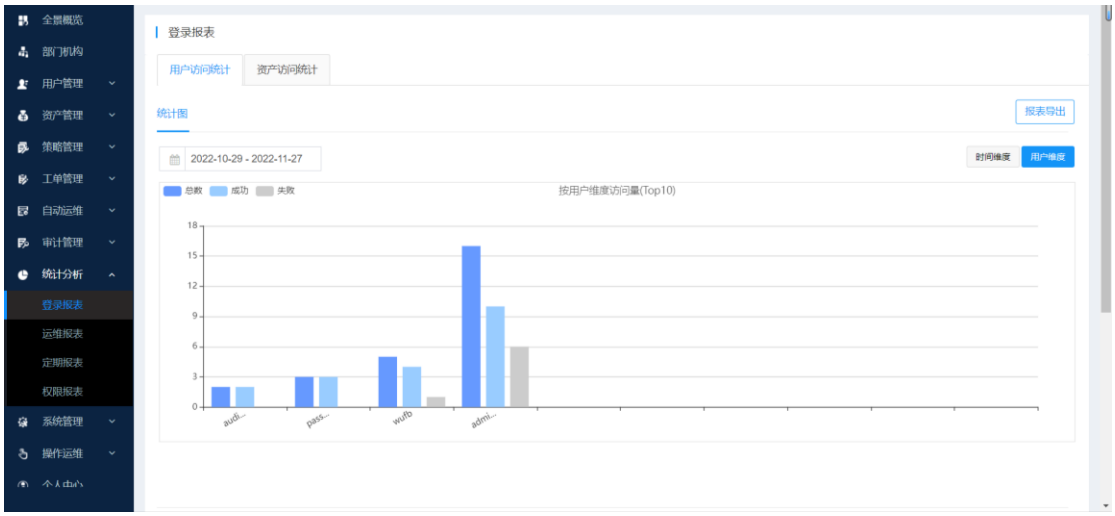
统计分析模块为系统业务数据功能，主要包括：登录报表、运维报表、定期报表和权限报表。展示格式主要包括趋势图和详细数据。

11.1 登录报表

登录报表包括协议访问统计、用户访问统计和登录尝试统计。

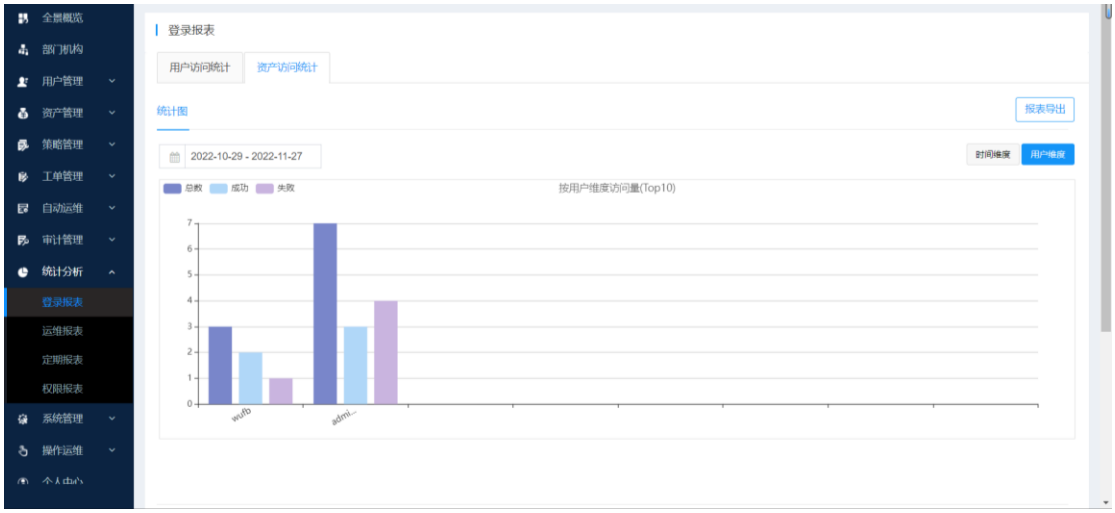
11.1.1 用户访问统计

访问明细可以按照时间进行展示近期时间段内系统被访问的次数统计：



11.1.2 资产访问统计

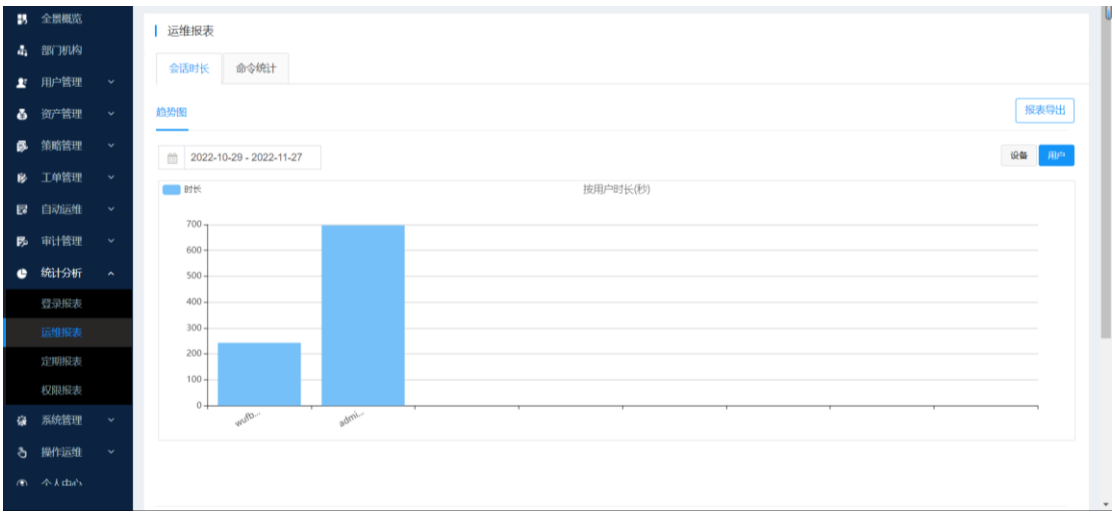
登录统计是系统账号的访问量的统计数据，包括运维用户、姓名及各种登录协议：



11.2 运维报表

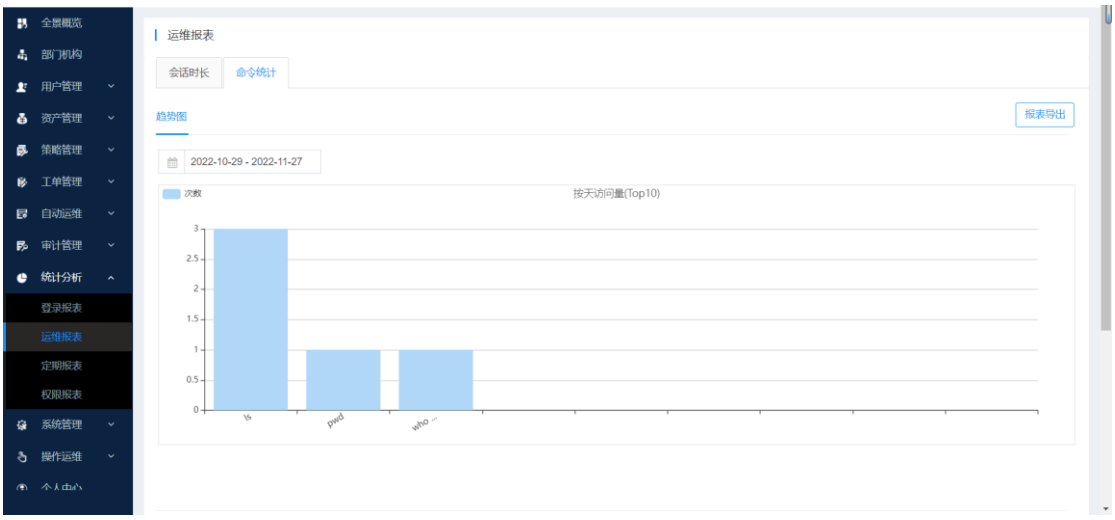
11.2.1 会话时长

统计运维人员/设备的操作时间进行统计。



11.2.2 命令统计

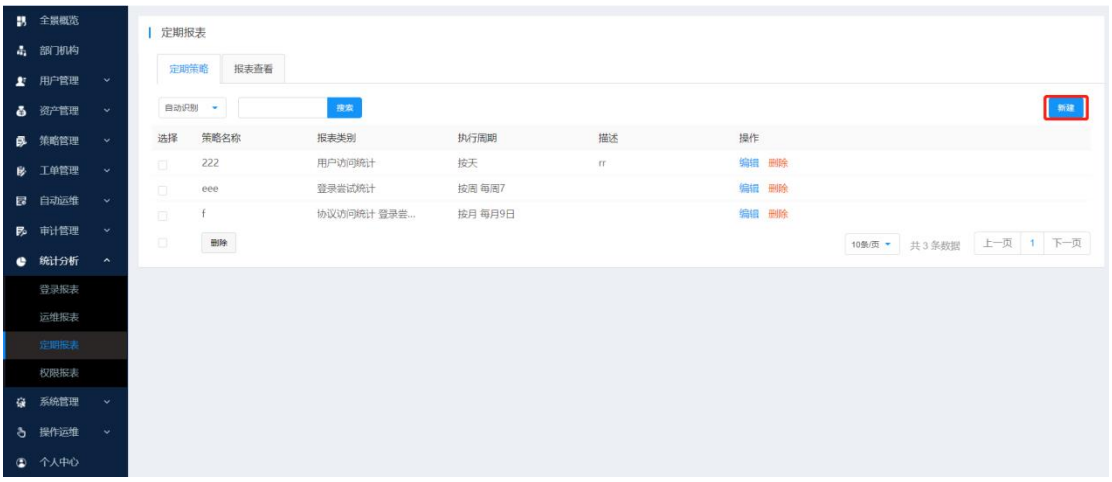
展示系统命令记录累计统计。



11.3 定期报表

定期报表包括定期策略、报表查看。

11.3.1 定期策略

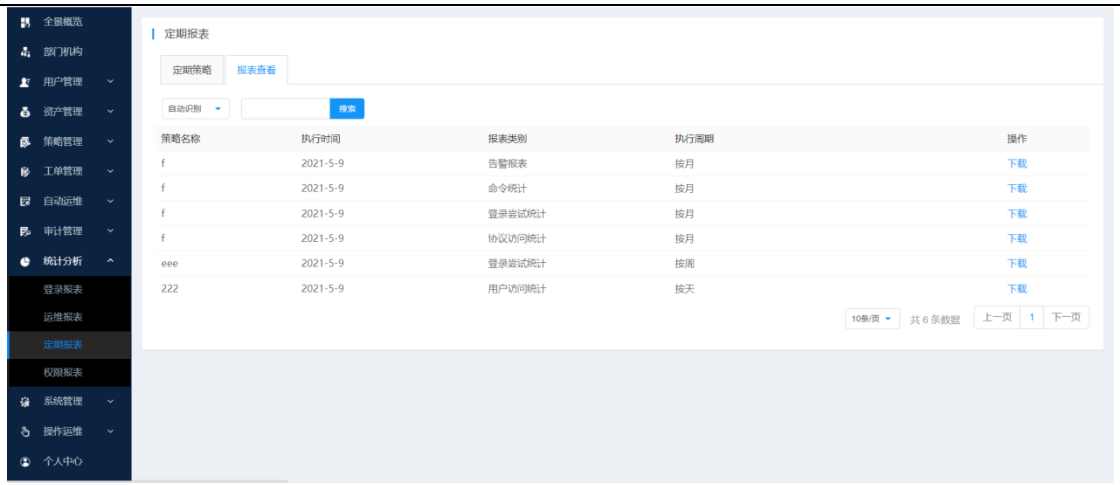


单击右侧<新建>，进入定期策略界面：

填写信息，包括：策略名称、报表类型、执行周期等信息。

11.3.2 报表查看

可以查看各个定期策略的报表，并且可以下载查看：

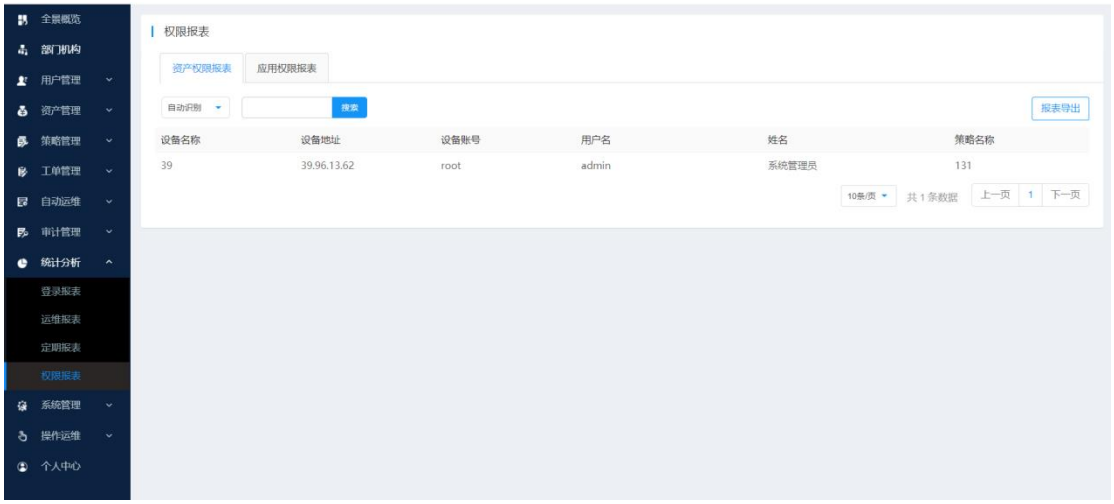


11.4 权限报表

资源报表包括两类：资产权限报表和资产账号报表。

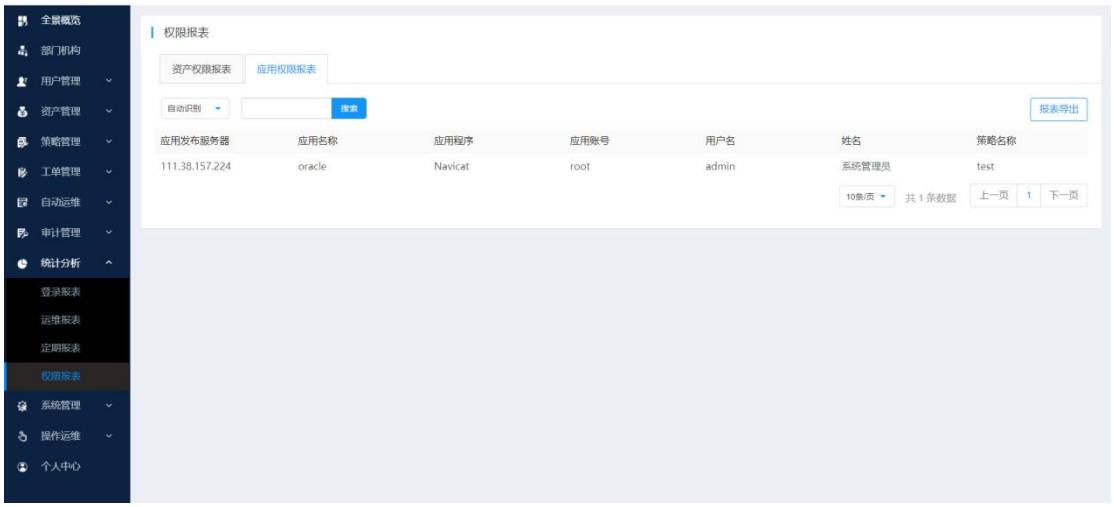
11.4.1 资产权限报表

根据运维用户/系统用户/设备地址条件进行查询当前系统，所有符合关联的权限信息报表展现。



11.4.2 应用权限报表

根据运维用户/应用服务器地址/应用名称条件进行查询当前系统，所有符合关联的权限信息报表展现。



12 系统管理

系统管理是对平台自身的系统配置、网络配置、系统维护等配置的集合。

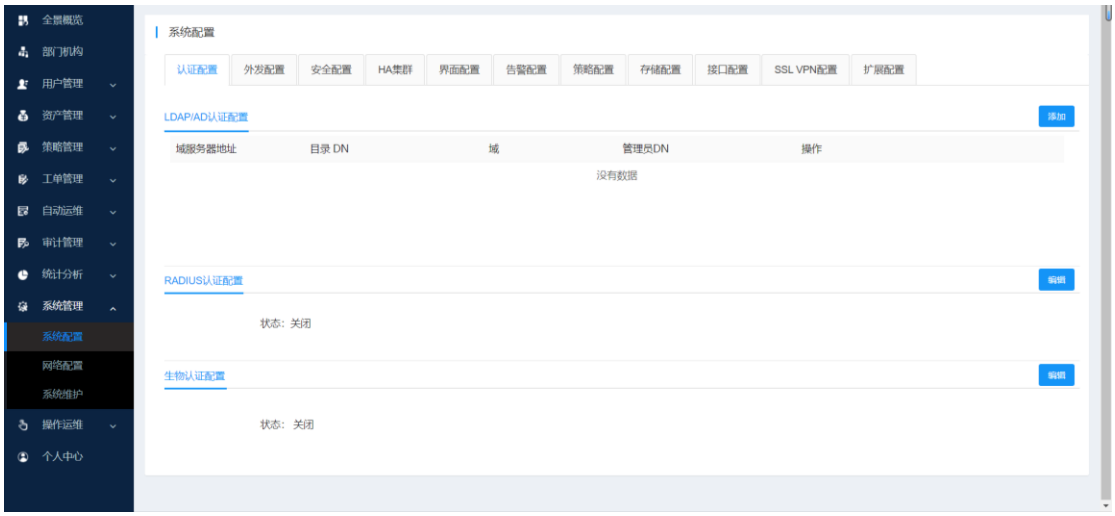
12.1 系统配置

12.1.1 认证配置

认证配置包括：AD 认证配置、RADIUS 认证配置、生物指纹认证配置

以 AD/LDAP 为例：

单击右侧<新建>，弹出 AD/LDAP 认证配置界面：

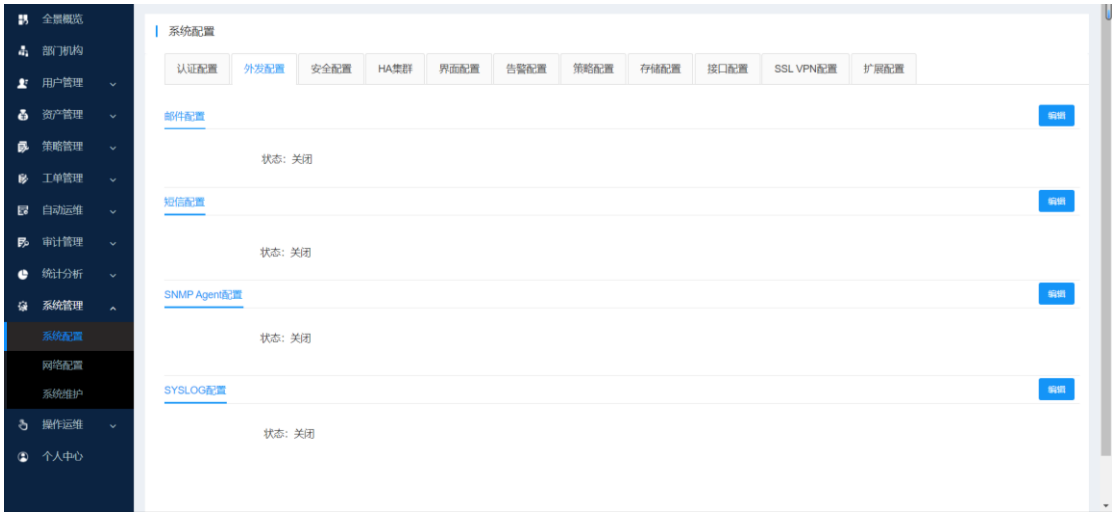


填写 AD/LDAP 认证配置的相关参数：

配置完成后，单击<确定>，即可创建 AD/LDAP 认证服务。

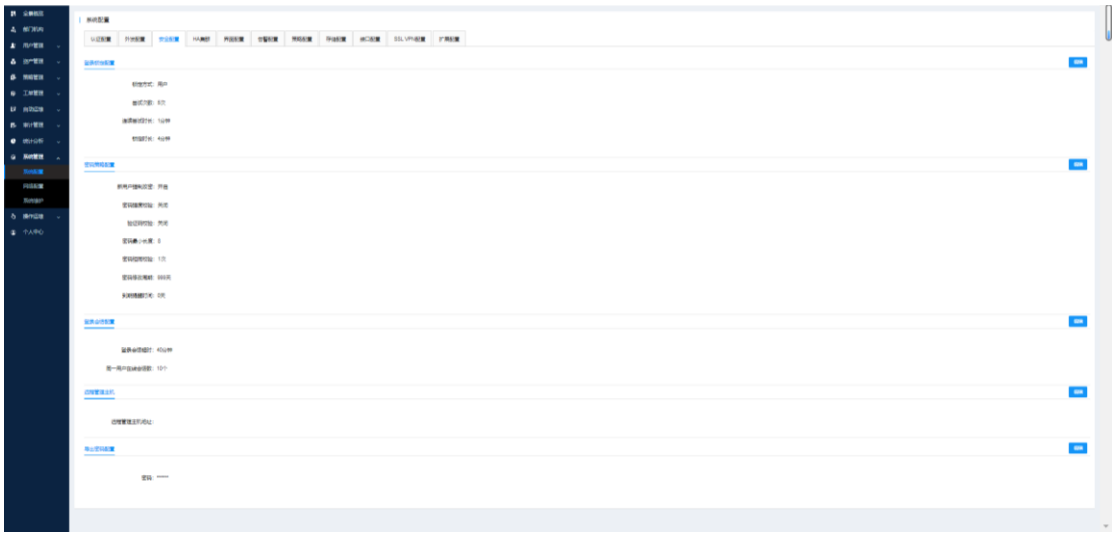
12.1.2 外发设置

外发设置支持邮件、短信、SNMP 和 SYSLOG。用户可根据实际环境需求进行配置和修改。



12.1.3 安全配置

安全配置包括：登录锁定配置、密码策略配置、Web 登录配置和远程管理主机。



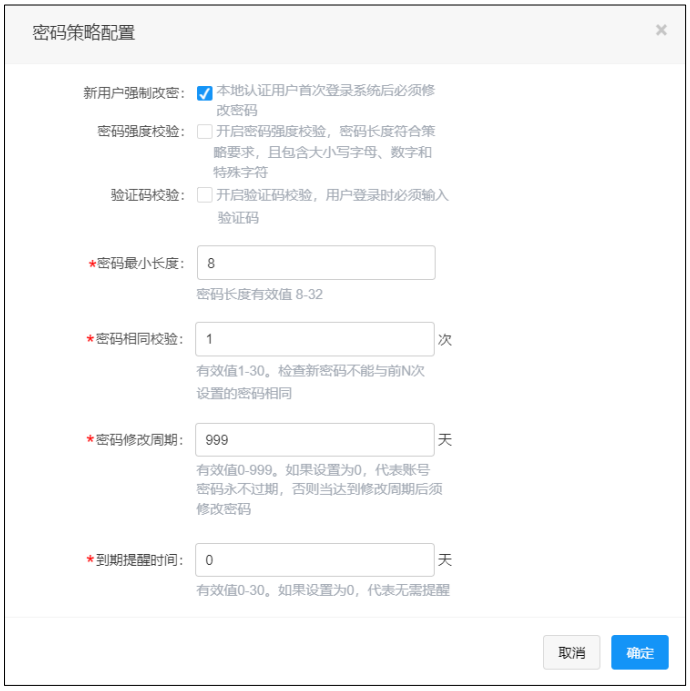
登录锁定配置说明：

功能	说明
锁定方式	可根据用户名或来源IP进行锁定
尝试次数	试密码次数是指可以输错密码的次数，有效值：0-1000
连续尝试时长	用户连续输错密码规定时间.有效值: 1-2880
锁定时长	用户输错密码被锁定的时间值，有效值：0-1000

密码策略配置说明：

功能	说明
密码强度校验	指是否强制用户使用强密码；必须包含大小写母、数字和特殊字符
新用户强制改密	新用户首次登录系统是否强制修改密码

密码最小配置	设置允许密码输入长度,有效值 8-32
密码相同校验	指用户修改密码时不能跟前N次相同。有效值0-20，0为不校验
密码修改周期	指运维账号密码修改周期，当达到修改周期时，登录后将自动弹出修改密码框，有效值0-999，0为无限期
到期提醒时间	提前x天提醒用户修改



登录会话配置：设置页面会话等待时长。默认 20 分钟，有效值：1-3600 分钟。

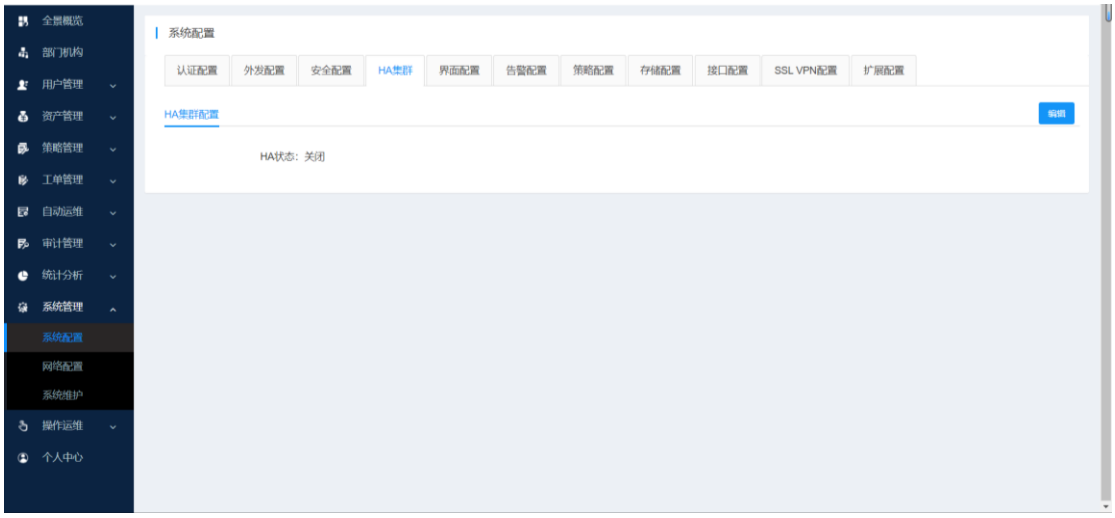
同一用户在线会话数：设置 web 同一用户在线会话数量，有效值：0-100,0 为不限制。

远程管理主机配置：可设置系统管理员只能通过以下 IP 进行访问。空地址为不限制地址登录。

导出密码配置：可设置导出文件时的密码。

12.1.4 HA配置

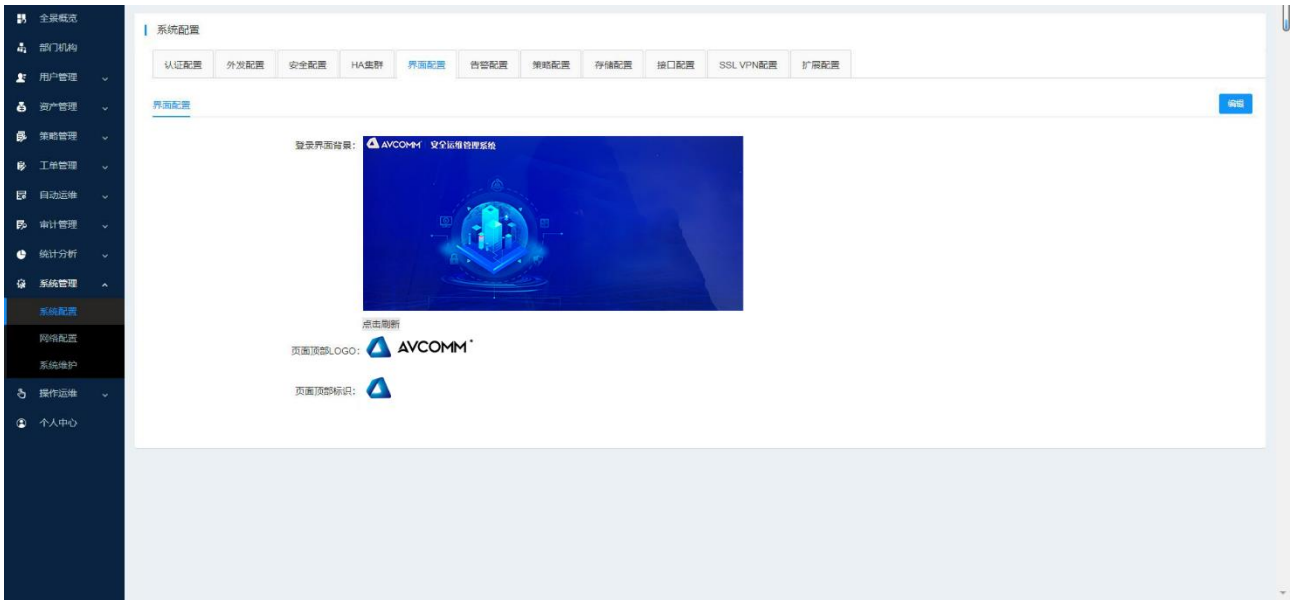
系统支持双机 HA 模式部署，进入[系统管理-系统配置-HA 配置]，单击<编辑>，进入 HA 配置界面：



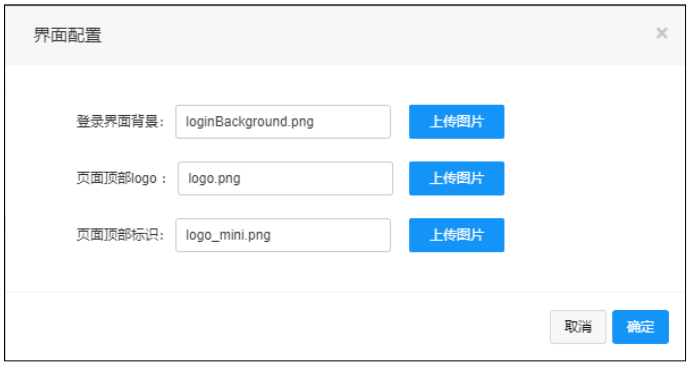
填写正确的相关配置信息。

12.1.5 界面配置

配置控制台界面

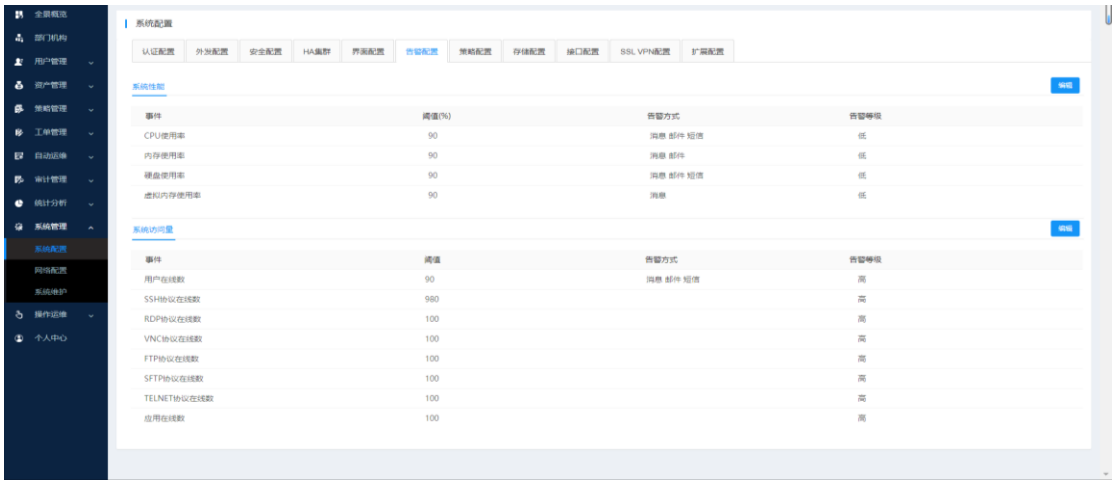


可选择登录界面背景,页面顶部logo,页面顶部标识;



12.1.6 告警配置

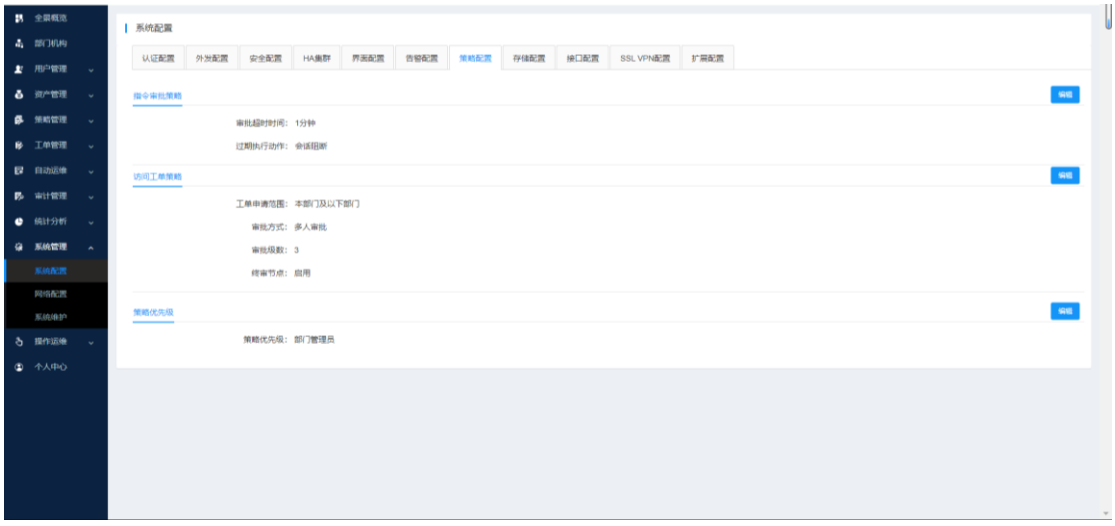
配置各类功能告警参数，达到设定的阈值后，进行触发告警。



告警方式包含：消息、邮件、短信三类告警方式；告警等级分为：高、中、低三个不同等级。

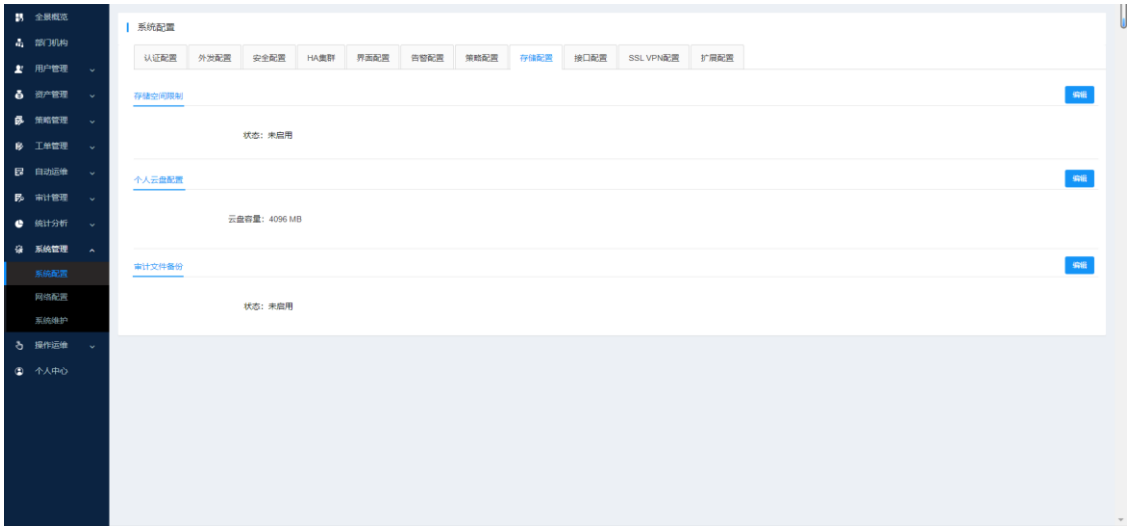
12.1.7 策略配置

策略配置功能包含：指令审批策略、访问工单策略和策略优先级。



12.1.8 存储配置

存储配置功能包含：存储空间限制、个人云盘配置和审计文件备份。

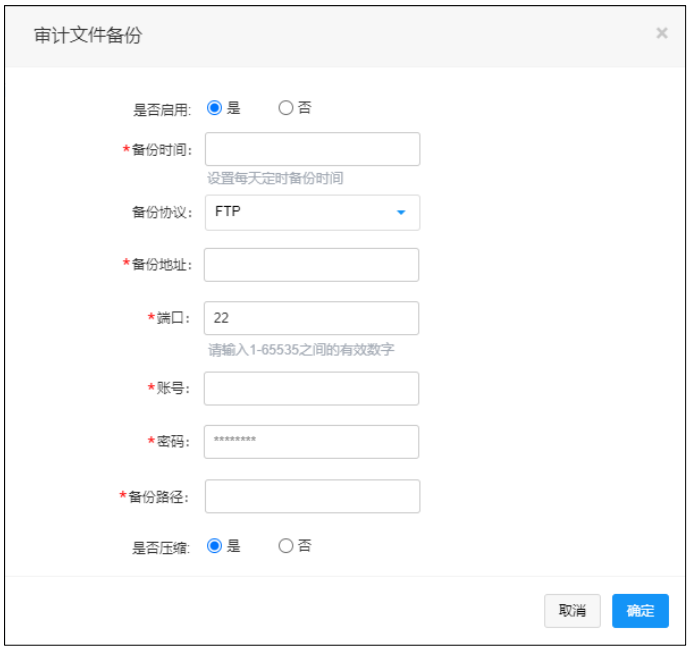


存储空间限制功能项说明：

功能项	说明
是否启用	是否启用此功能
存储百分比	存储达到百分比阈值选择
动作选择	到到选择的百分比阈值后执行的动作，覆盖最早文件和停止录像审计
日志条数限制	规定存储的日志数量

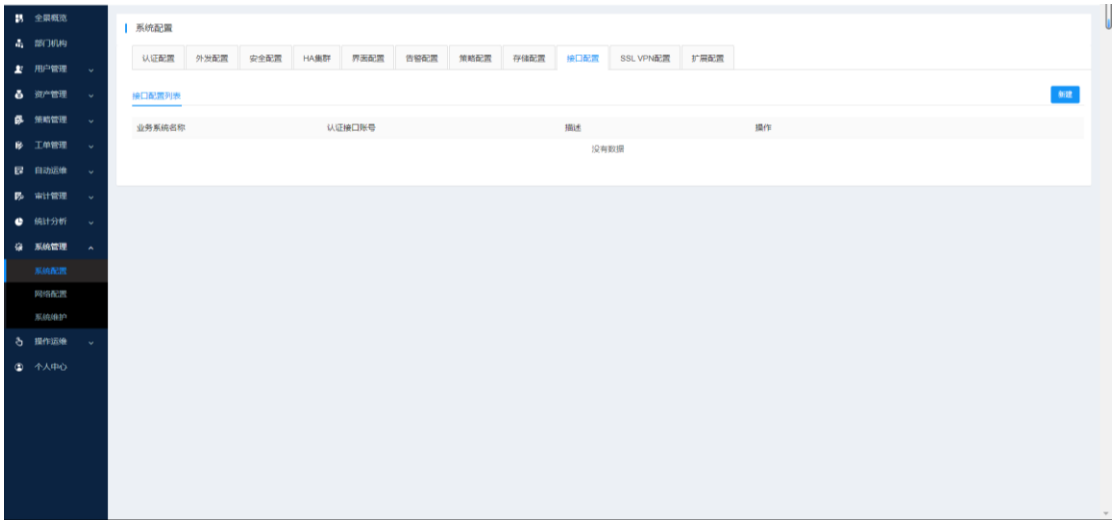
个人云盘配置：可对云盘空间存储大小进行设置，有效值为 1-10000。

审计文件备份：可对审计的录像文件进行定时备份到指定的FTP/SFTP服务器目录下，进行保存备份。

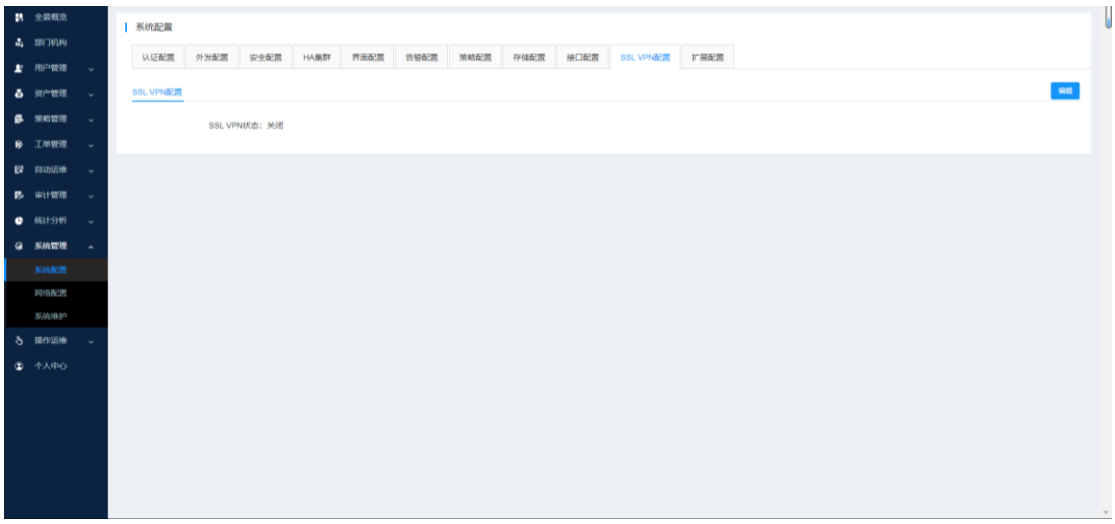


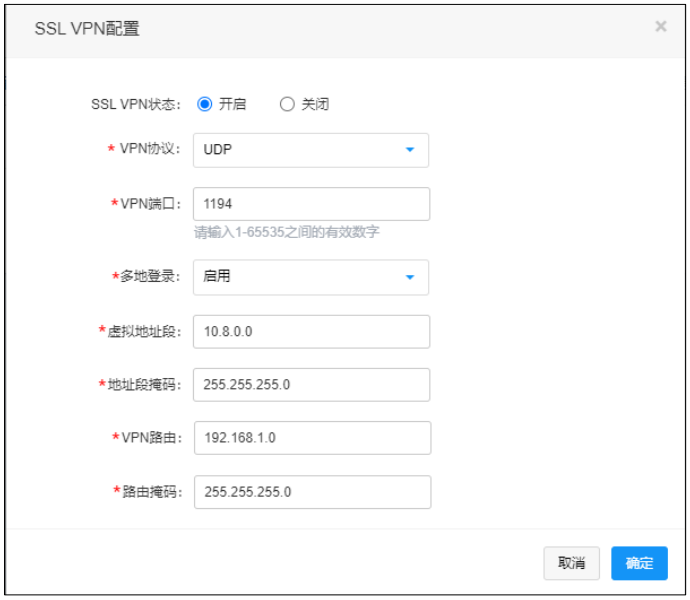
12.1.9 接口配置

接口配置的功能包含:业务系统名称,认证接口账号,认证接口密码,确认密码,描述等。

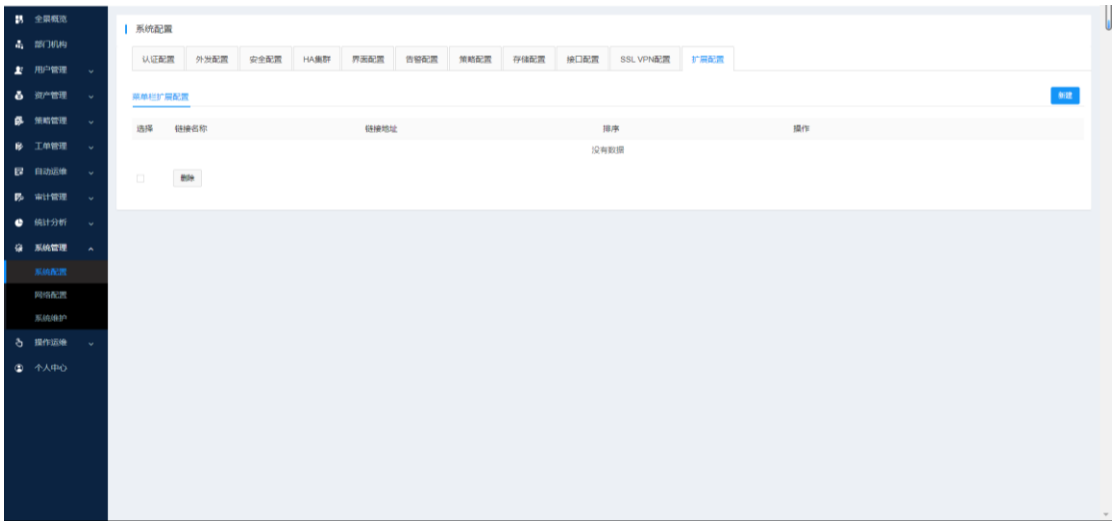


12.1.10 SSL VPN配置





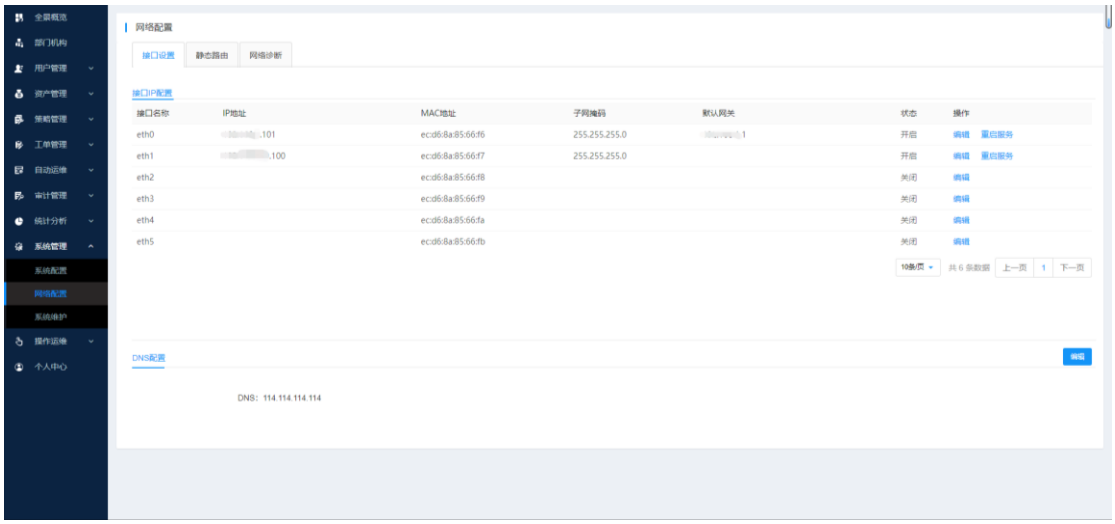
12.1.11 扩展配置



12.2 网络配置

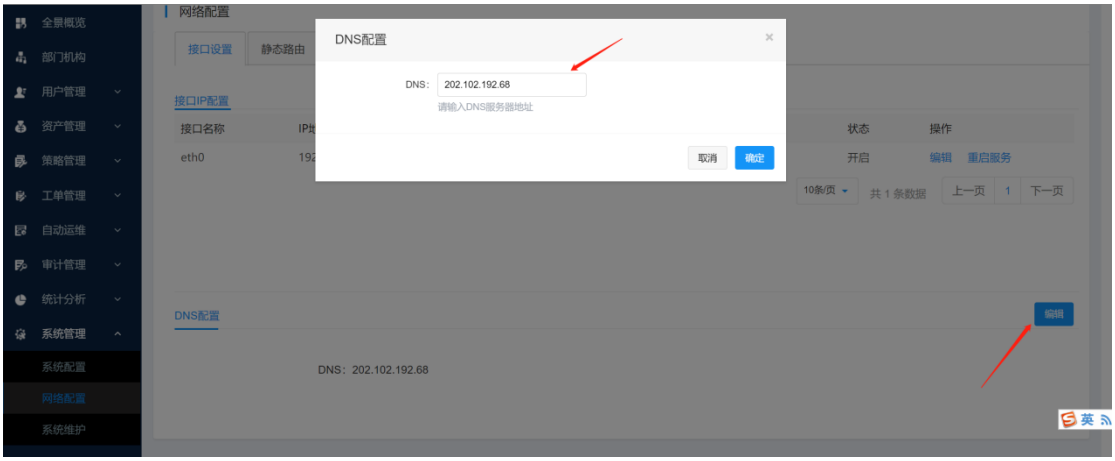
12.2.1 接口设置

配置系统网口地址信息。



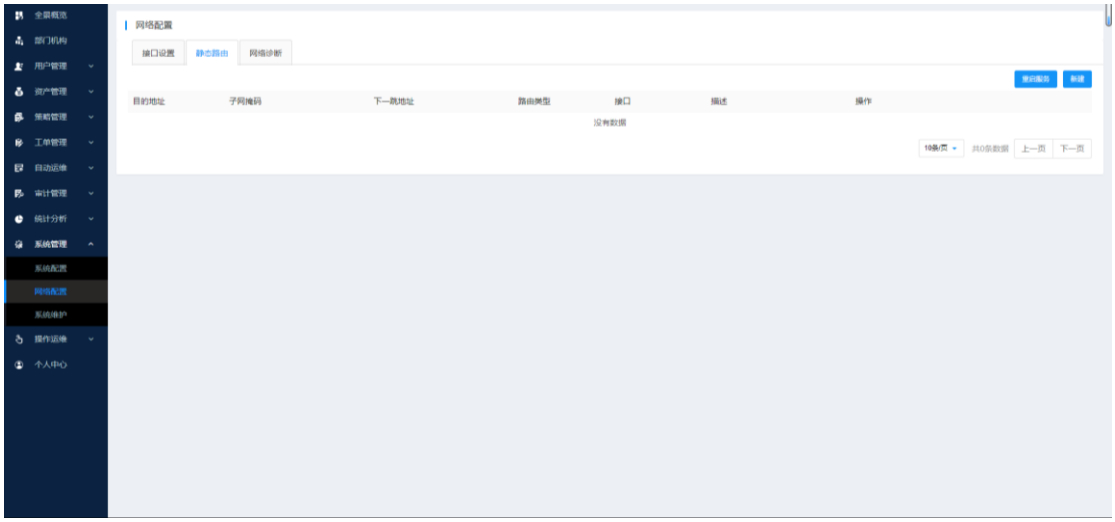
输入参数后保存修改， 系统自动重启网卡服务，立即生效。

DNS配置：点击编辑，进行配置DNS服务器。

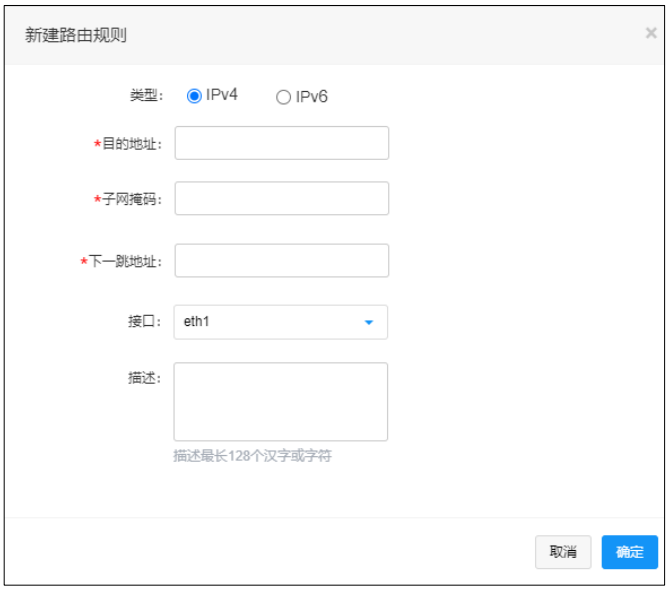


12.2.2 静态路由

单击[新建]，弹出添加静态路由界面：

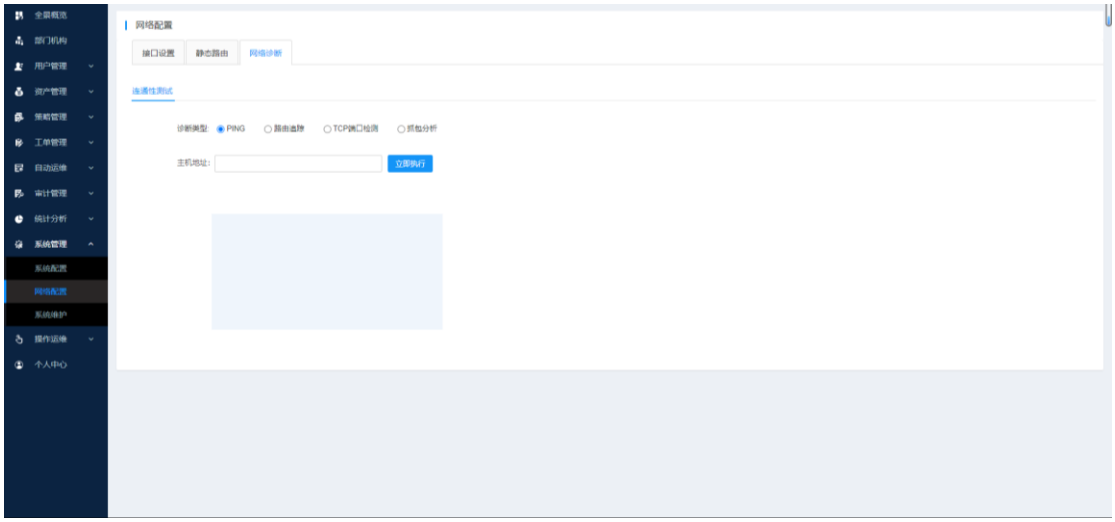


根据需要填写静态路由信息。



12.2.3 网络诊断

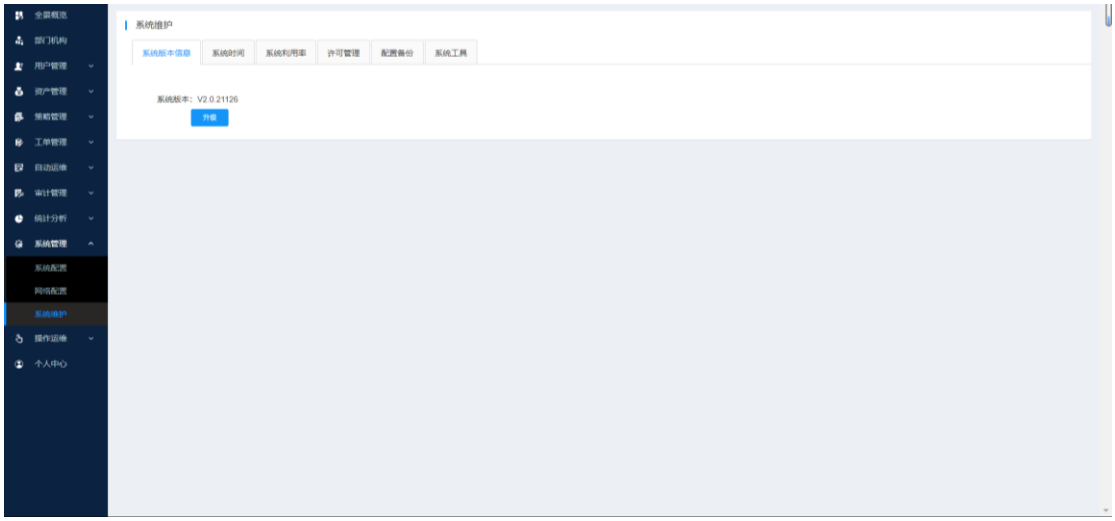
支持 PING、路由追踪、TCP 端口检测和抓包分析常见的四种网络诊断方法。



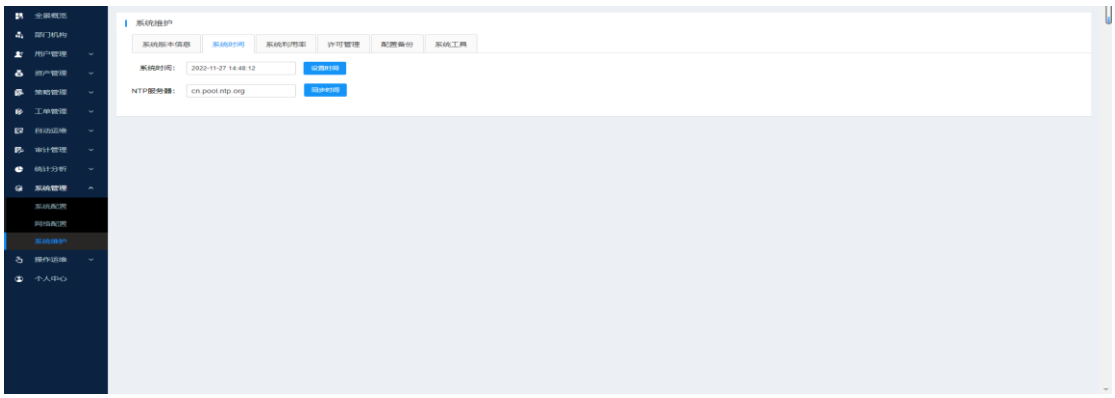
12.3 系统维护

12.3.1 系统版本

显示当前版本号及升级功能，单击[升级]，可进行手动升级。

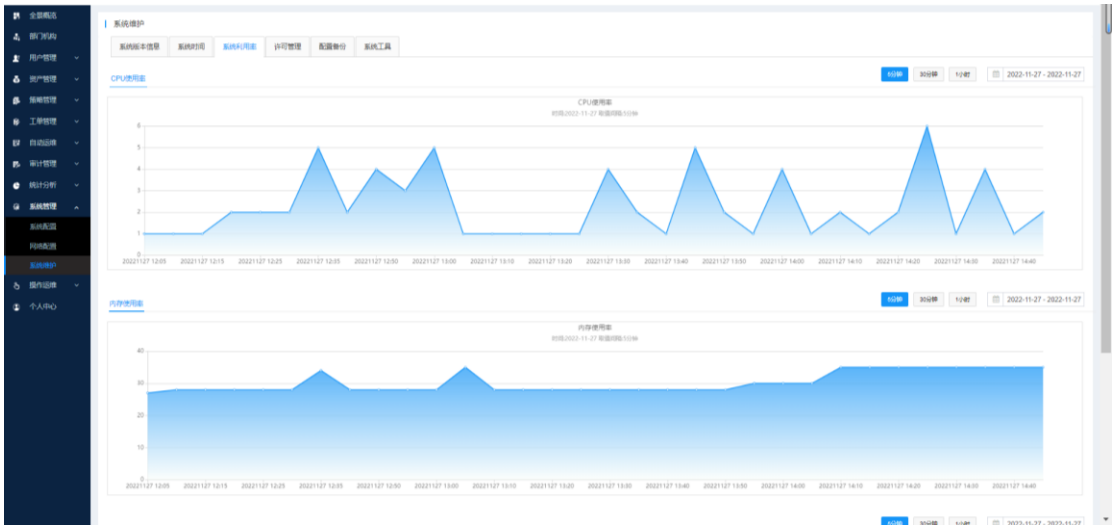


12.3.2 系统时间



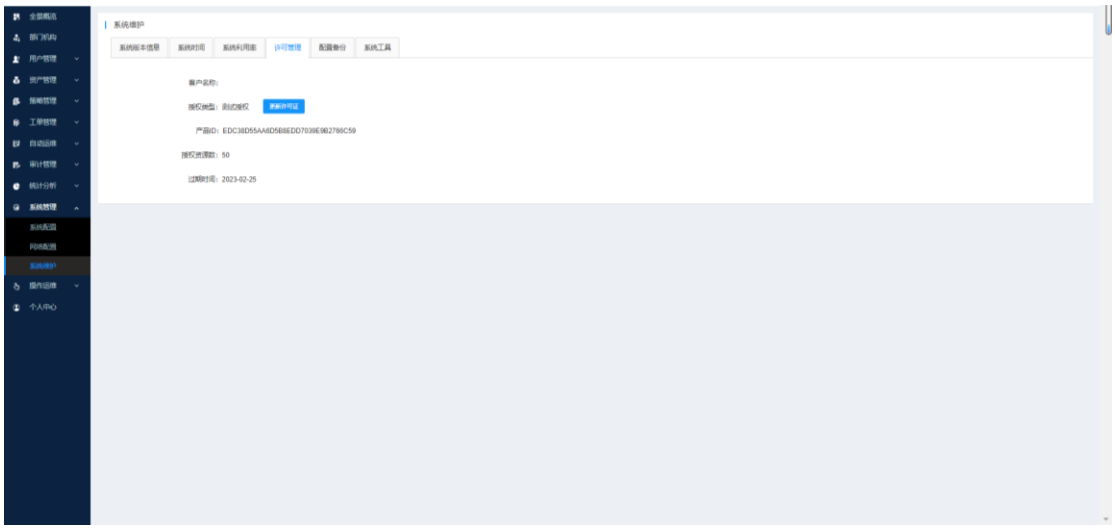
12.3.3 系统利用率

展示系统 CPU、内存、磁盘一段时间内的利用率。



12.3.4 许可管理

许可管理可查看当前设备系统许可信息，进入[系统管理-系统维护-许可管理]页面，显示系统当前授权信息。“授权资源数”显示当前系统最多可添加资源数（包含：设备、应用资源），“授权并发连接数”指可同时登录资源数（包含：设备、应用资源）。

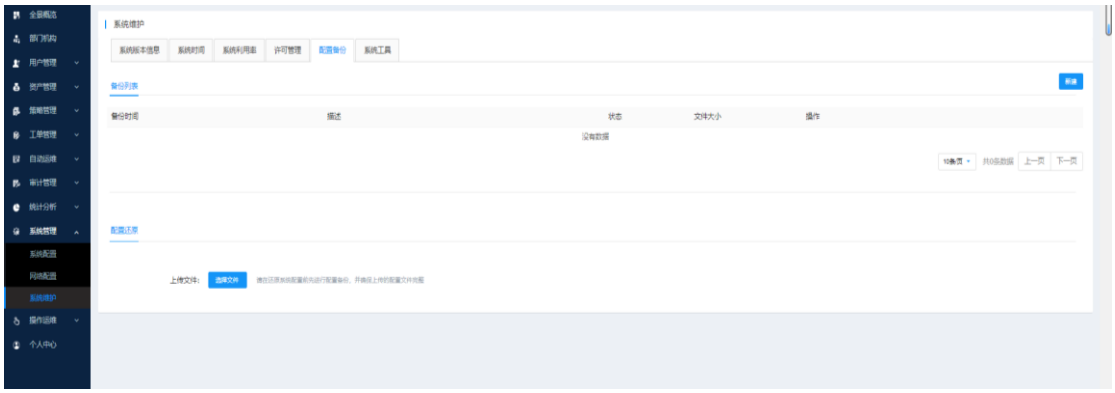


单击[更新许可证]，弹出更新许可界面：

单击[点击下载],进行下载申请文件，由服务人员进行生成申请授权许可文件，单击[选择文件]，许可文件会上传到系统，进行校验许可信息并更新。此时完成许可导入。

12.3.5 配置备份

配置备份功能主要对系统数据库的手动备份和还原。

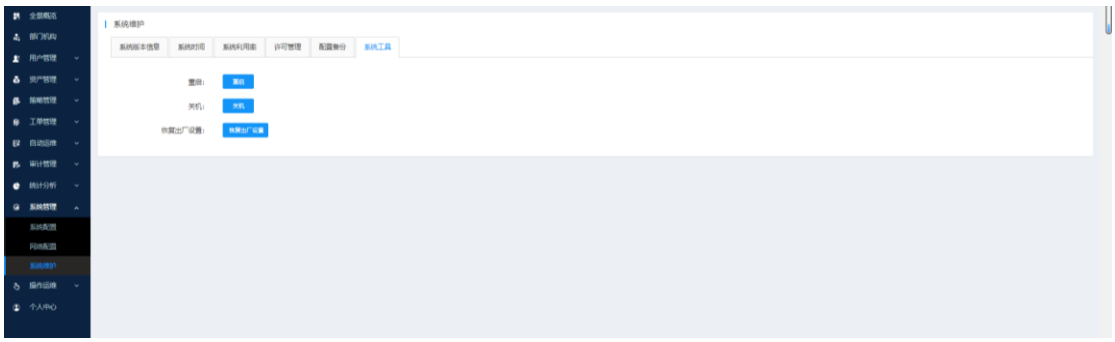


12.3.6 系统工具

系统工具主要包括以下功能项：

功能项	说明
重启	对系统重新启动
关机	对系统关机操作
恢复出厂设置	对系统进行初始化，还原到出厂设置

以上功能操作都会对系统业务造成中断，如需必要操作，建议在空闲时间进行操作维护。

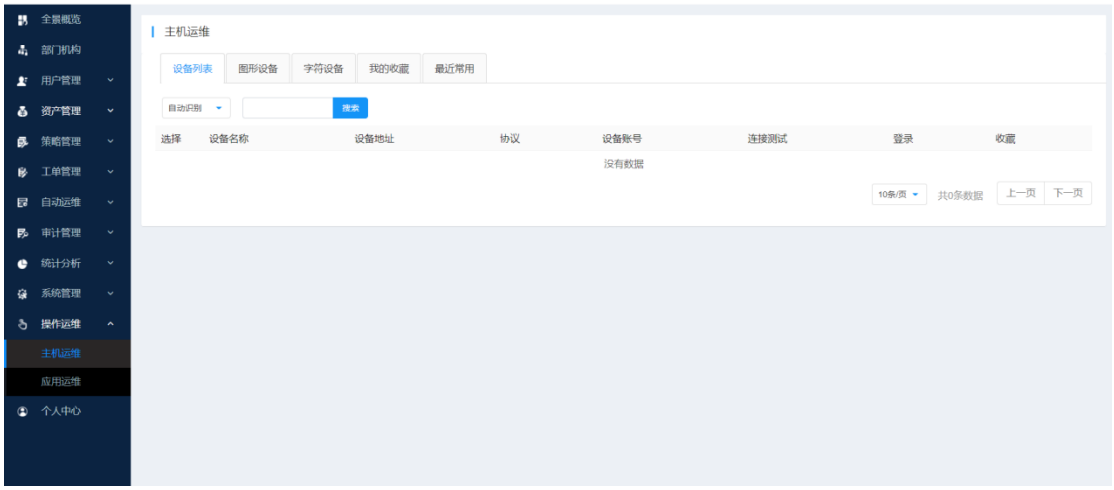


13 操作运维

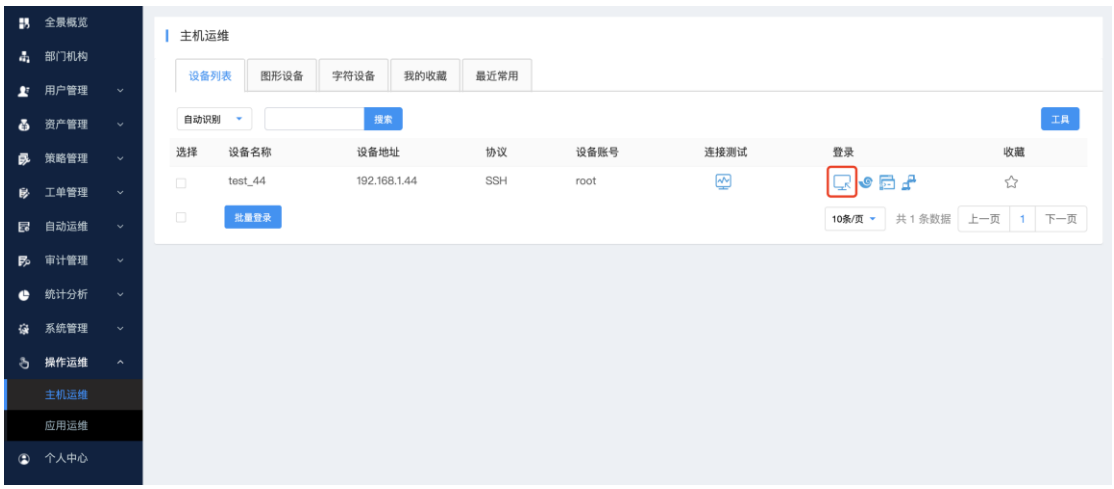
操作运维用于运维人员登录主机、应用的功能。

13.1 主机运维

进入[操作运维]-[主机运维]，默认为设备列表页面，列出有权限的主机设备。



单击设备右侧[登录]图标，即可访问登录目标设备。



字符型协议访问：

图形协议访问：

提示：为方便用户使用，主机运维内含不同标签分类，包括：设备列表、图形设备、字符设备、我的收藏、最近常用。用户可根据实际情况灵活使用。

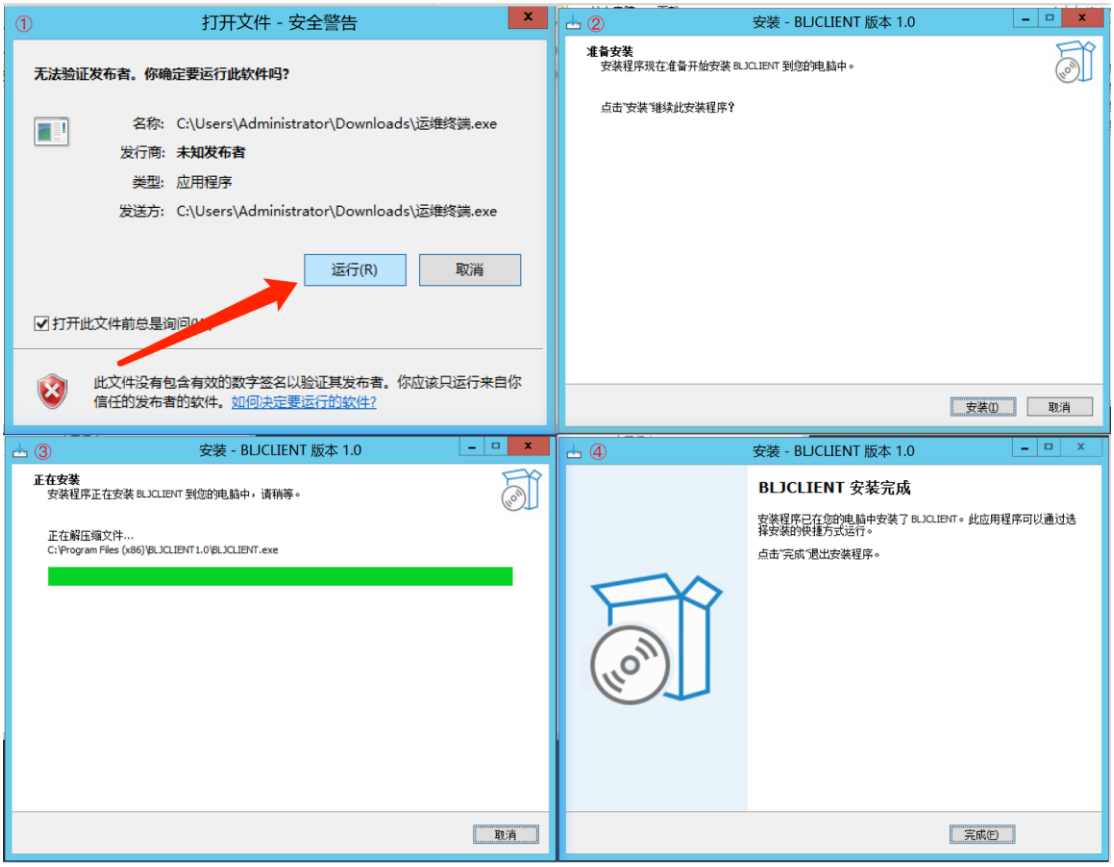
13.1.1 H5运维

13.1.2 客户端运维

（1）控件下载与安装

下载：[操作运维]-[主机运维]-[工具]-[运维终端.exe]右侧[下载]按钮

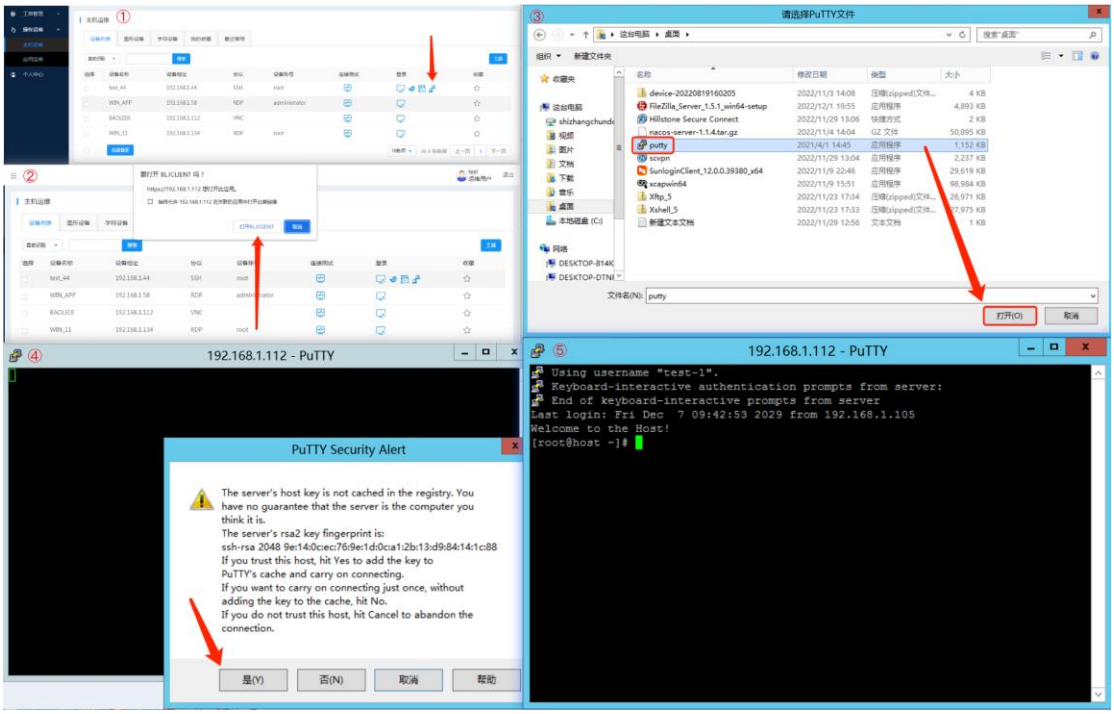
安装：



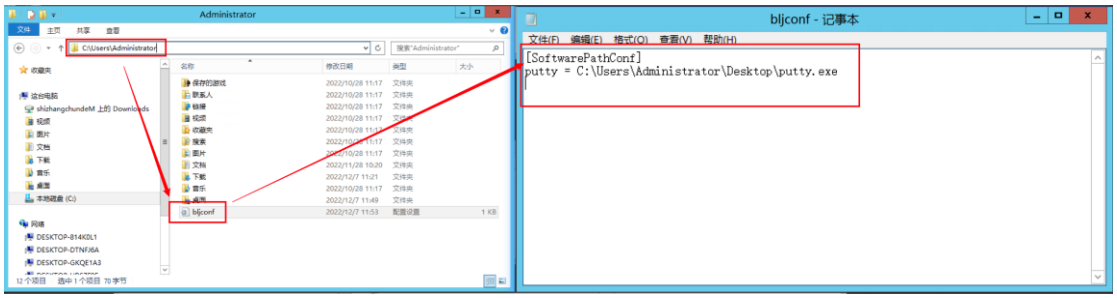
目前支持的客户端列表如下：

- XShell
- SecureCRT
- putty

这里以putty为例，操作引导如下：



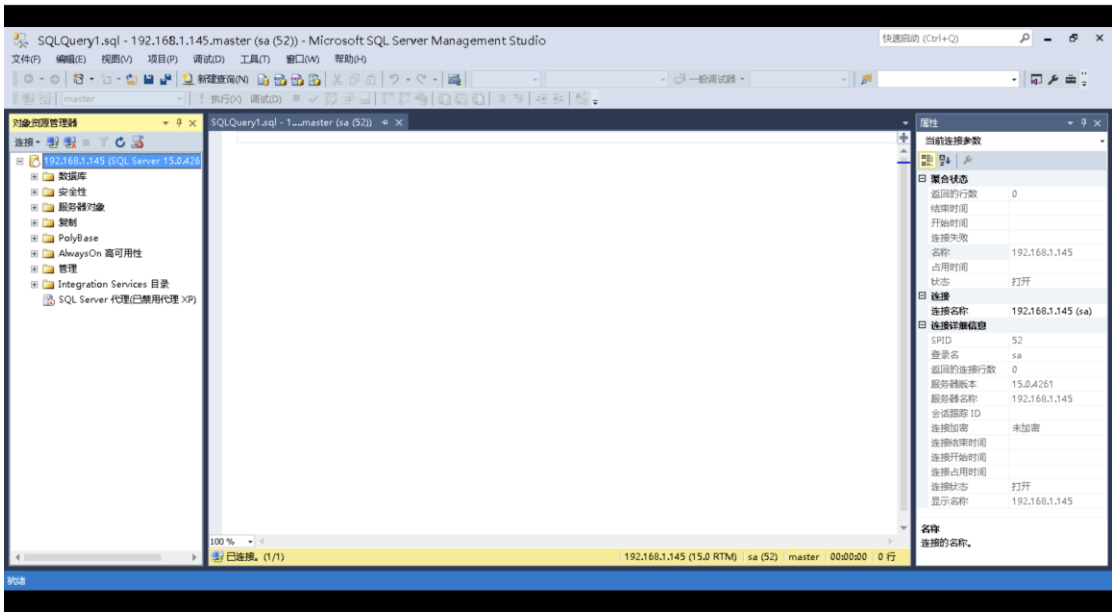
注意：若在使用客户端运维过程中误绑定错误的程序路径，可以修改存放在用户路径的 bljconf 文件，这里以 administrator 为例：



13.2 应用运维

进入[操作运维]-[应用运维]，应用名称右侧单击[登录]对应图标：

通过和应用服务器建立数据连接后，推送出指定应用：

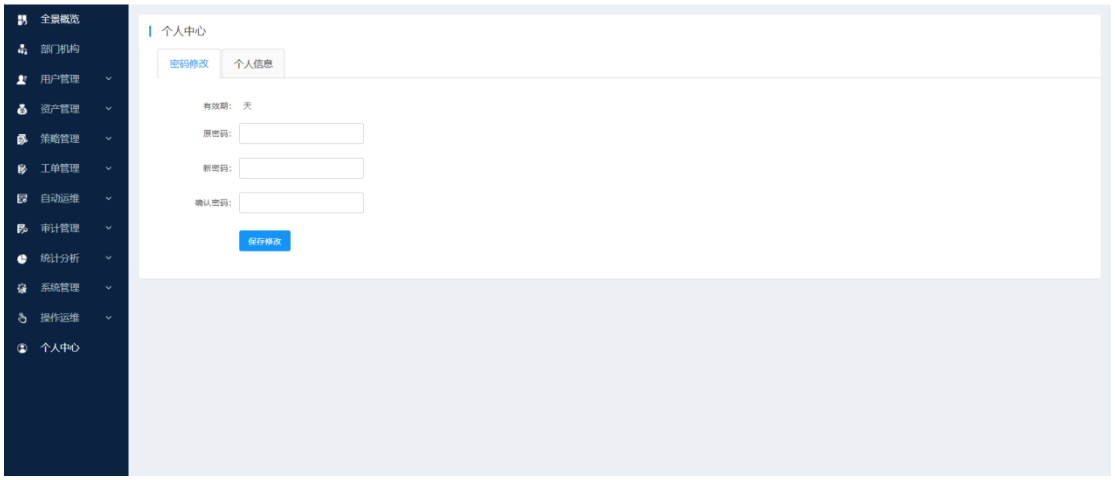


14 个人中心

个人中心包括个人密码修改和个人信息。

14.1 密码修改

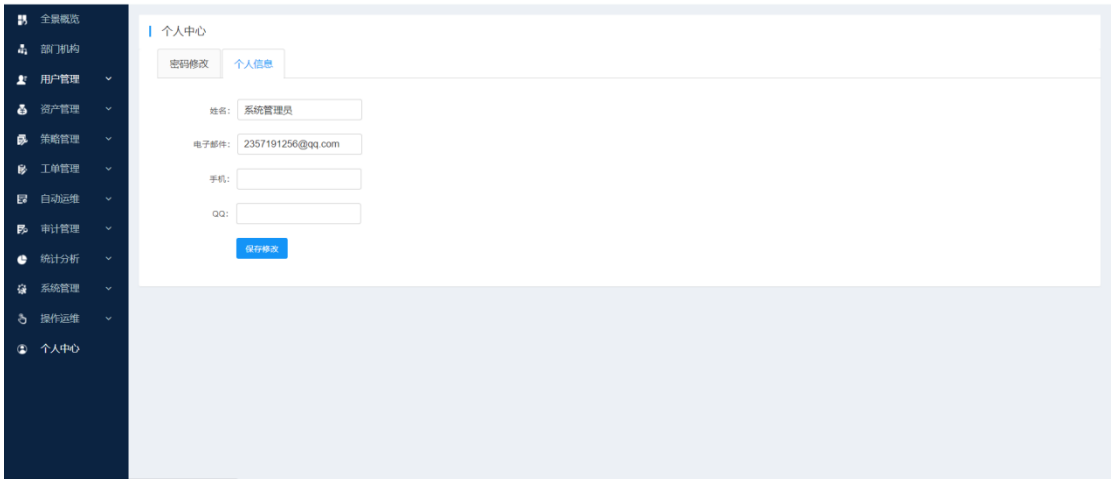
单击[密码修改]，进入密码修改界面：



根据页面提示进行修改密码。

14.2 个人信息

单击[个人信息]，进入个人信息界面：



根据页面提示，进行更新修改。