KYLINSOFT
麒麟软件

麒麟天御安全域管平台 V4.1.0
管理员手册

麒麟软件有限公司

2024 年 8 月

商标声明

KYLINSOFT 麒麟软件和其他麒麟商标均为麒麟软件有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受麒麟软件有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，麒麟软件有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容有可能变更，麒麟软件有限公司保留在没有任何通知或提示的情况下对内容进行修改的权利。除非另有约定，本文档仅作为使用指导，并不确保手册内容完全没有错误。本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 概述

1.1 产品简介

麒麟天御安全域管平台（简称“麒麟天御”）是专为提升企业安全管理和操作效率而设计的企业级安全管理平台，旨在平滑替换 Windows AD。该平台致力于提高企业数据防护能力和管理效率，聚焦身份认证、终端安全、用户权限、软件管理、策略管控、高可用等场景，实现了对组织下的用户、主机、外设、软件、管控策略等全流程的统一管理。

1.2 产品架构

麒麟天御采用 B/S 与 C/S 混合架构，由服务端和客户端两大核心部分构成。这种架构设计不仅提升了系统的灵活性与扩展性，也确保了用户界面的友好性和操作的便捷性。服务端基于银河麒麟容器云平台设计，提供一体化 WEB 管理控制台，实现对组织、用户、终端等的全方位安全管理，支持多种单双园区高可用部署方案，确保业务系统运行的效率和连续性。客户端集成入域退域、数据同步、策略执行、策略取消、日志同步以及消息提醒等关键功能，并与麒麟通用桌面操作系统深度融合，有效应对系统统一认证、策略控制及维护升级等挑战，为业务信息系统管理提供坚实的保障。

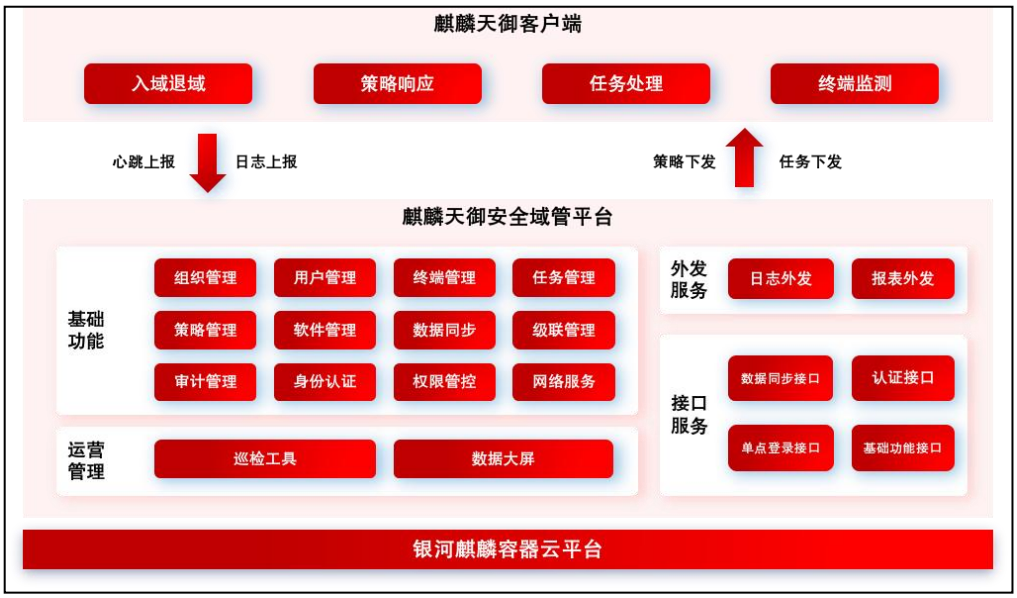

图 1-1 麒麟天御产品架构图

2 平台登录

在浏览器中打开麒麟天御安全域管平台，(访问地址:https://域名或 IP)，进入到登录界面，输入账号名、密码、图形验证码进行登录。

图 2-1 登录界面

管理员登录

admin 管理员用户登录成功后，可根据业务需要创建不同管理员账户，管理不同功能模块和组织范围。

点击系统管理-管理员权限配置-添加管理员，支持创建多个平台管理员。

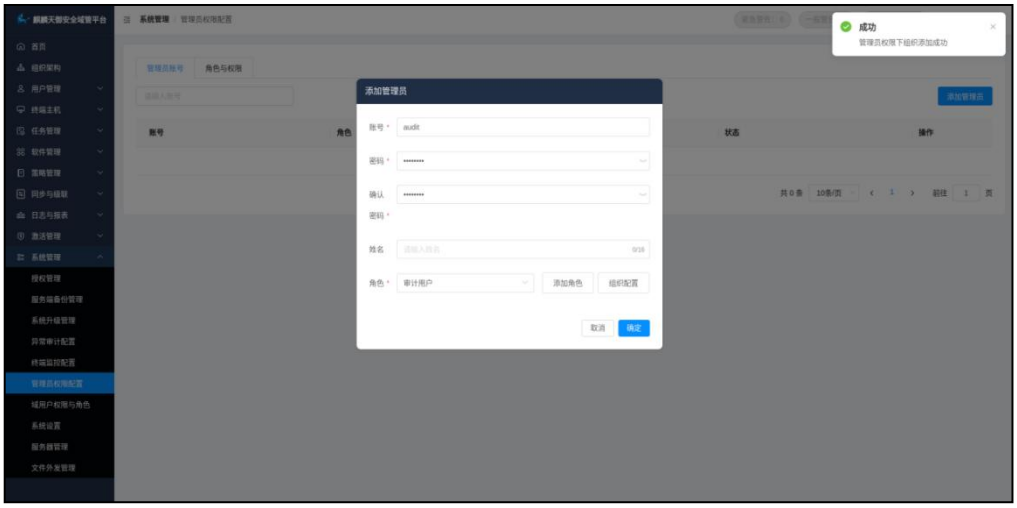

图 2-2 管理员权限配置界面

若为超级管理员用户，显示全部菜单。

初始账号用户名：admin，初始密码：Kcm.2021，输入验证码，点击登录，即可访问。

管理员登录完成后，点击右上角用户名，可进行密码修改、查看关于、服务端登出操作。

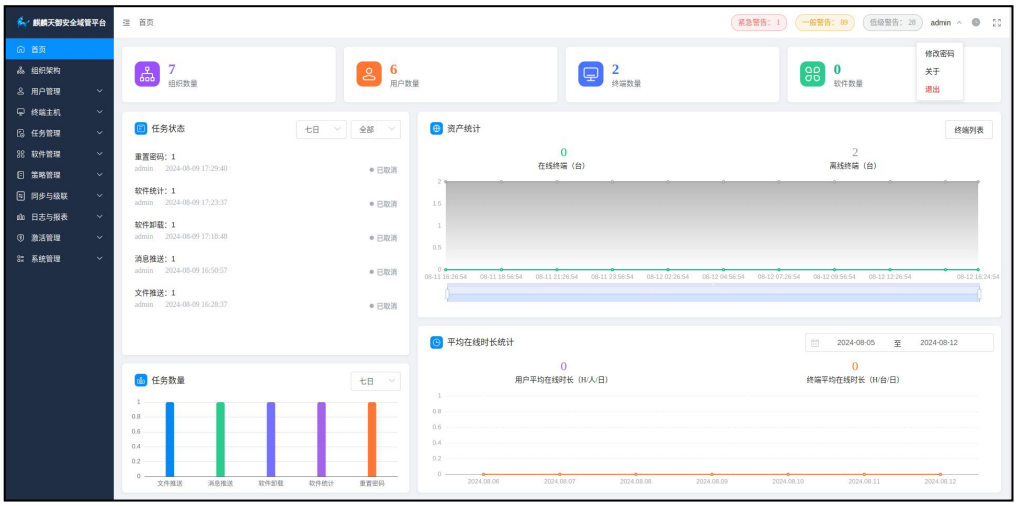

图 2-3 首页

若为普通平台管理员，显示该管理员下所配置的菜单权限，例如为管理员配置策略管理权限，则登录后仅能进行策略管理相关操作。

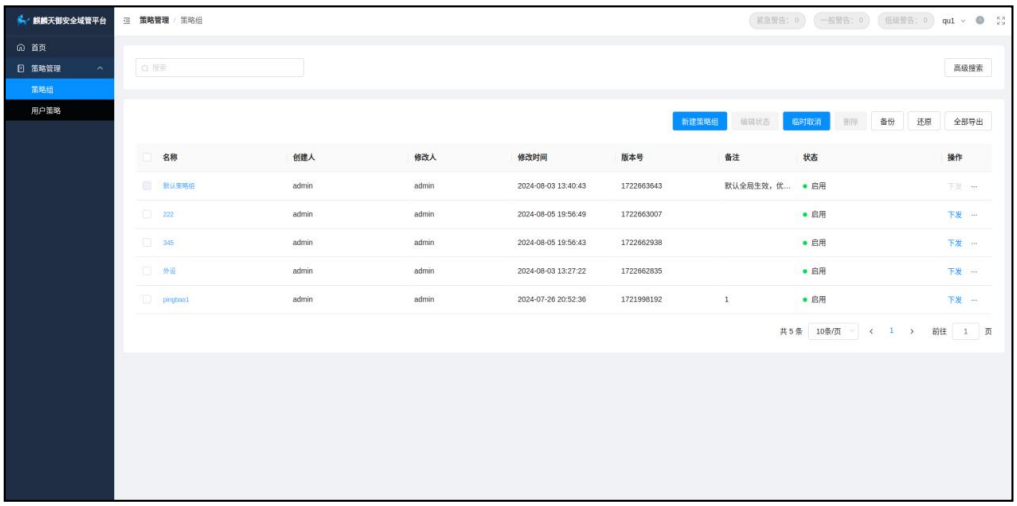

图 2-4 策略管理界面

3 首页

系统管理员可通过首页直观地查看当前系统中的数据概览，包括：组织数量、用户数量、终端数量和软件数量。支持图形化便捷查看，包括：任务状态、任务数量、资产统计、平均在线时长统计。

通过点击组织数量、用户数量、终端数量和软件数量可快速跳转至相应功能模块配置界面。

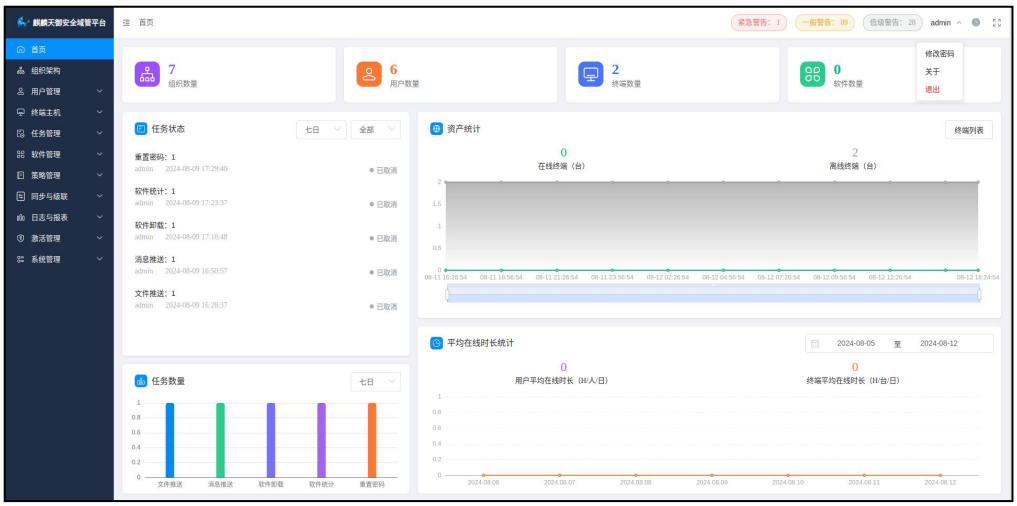

图 3-1 首页

4 组织架构

4.1 架构管理

架构管理支持新建组织、批量导入组织、导出全部组织、添加子组织、编辑组织、删除组织、组织保护、搜索组织功能。

点击【新建】按钮可新增一级组织，组织名称可自定义编辑。新建组织可配置组织匹配规则，支持终端按 IP 匹配或者按字符（主机名）匹配。当终端加域成功后，终端将按匹配规则自动加入相应组织。

图 4-1 新建组织界面

点击组织后的【选项】按钮，可对该组织添加子组织、编辑组织和删除组织。

未分组为系统默认组织，该组织不可编辑，也不可删除。当终端加域成功后，未匹配到组织规则的终端将会被自动加入未分组。

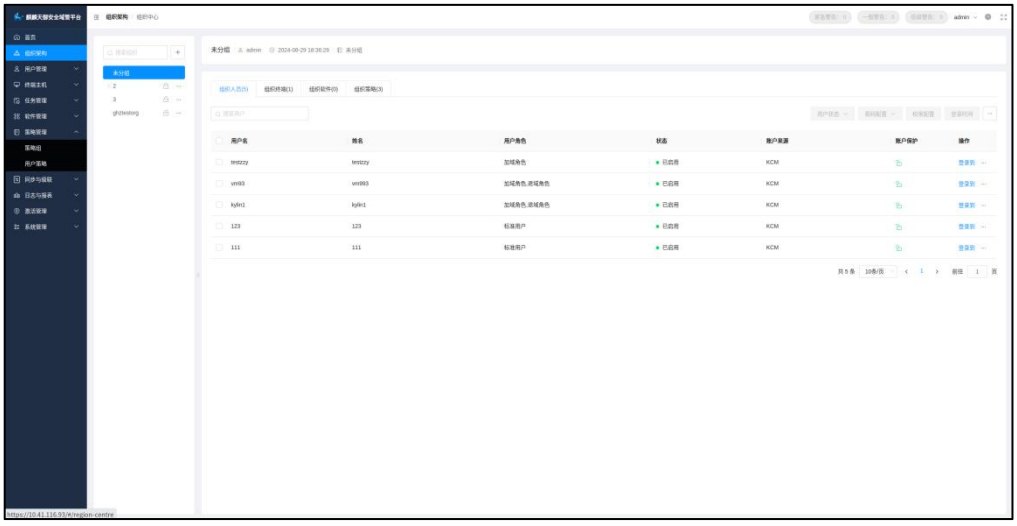

图 4-2 组织架构页面

4.2 组织详情

组织架构为树状结构。选择不同组织，可根据管理员分配的不同管辖权限管理不同组织的人员、终端、软件和策略。

组织人员

选择组织，支持对该组织添加用户、批量添加和关联用户操作。

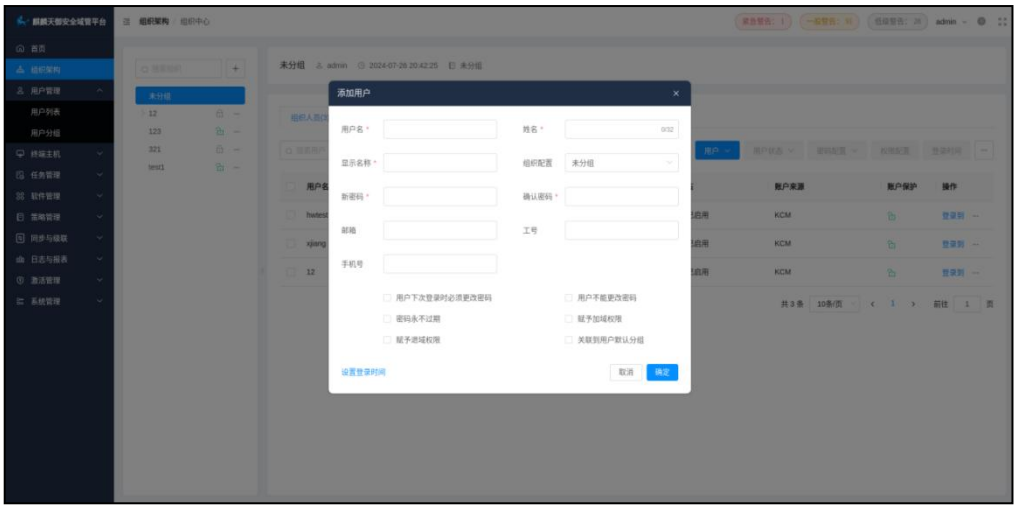

图 4-3 添加用户界面

支持对单个或多个用户进行批量启用、禁用、重置域用户与 AD 用户密码、权限配置、登录时间、全部导出、调整组织和移除操作。

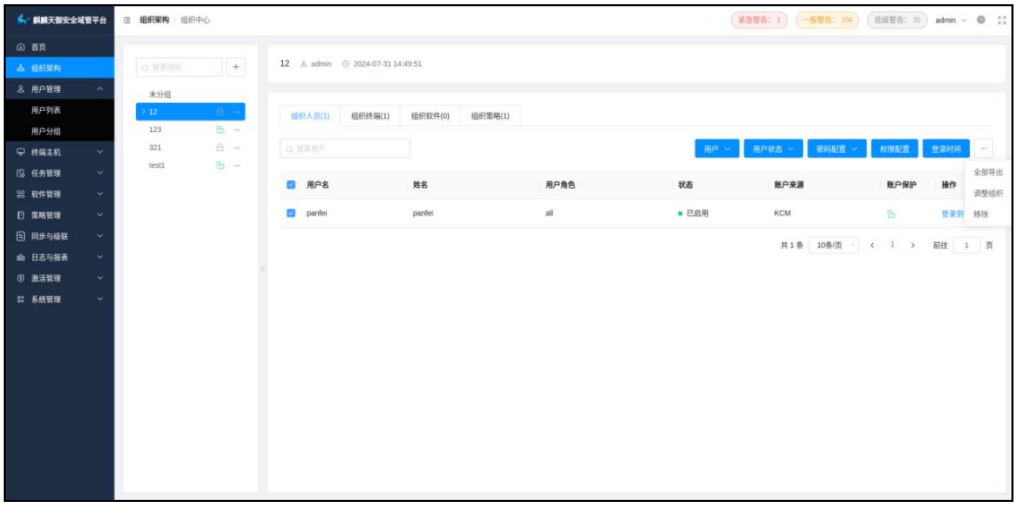

图 4-4 组织人员-人员批量操作界面

支持对单个用户进行编辑用户、解锁、账户保护和登录终端配置。

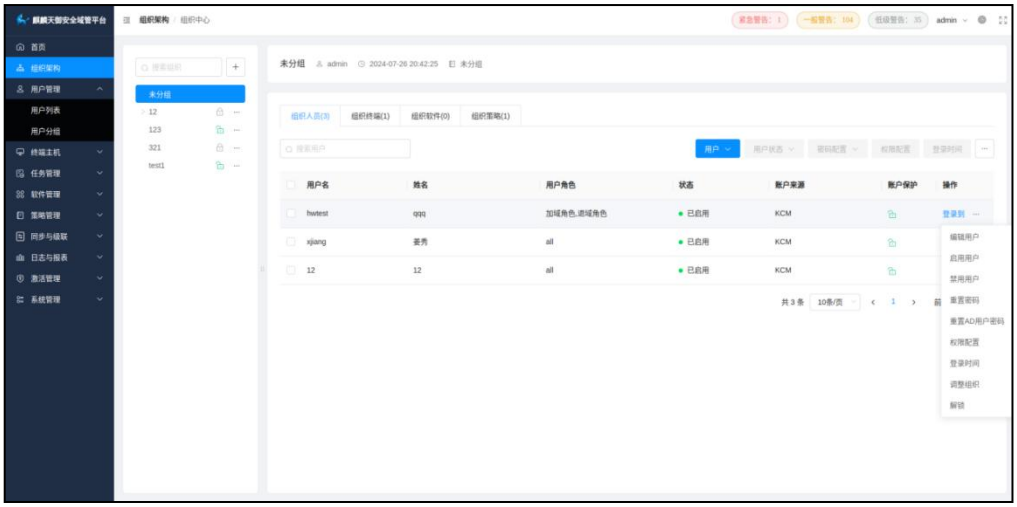

图 4-5 组织人员-人员操作界面

组织终端

支持关联终端，将未分组的终端关联当前组织。

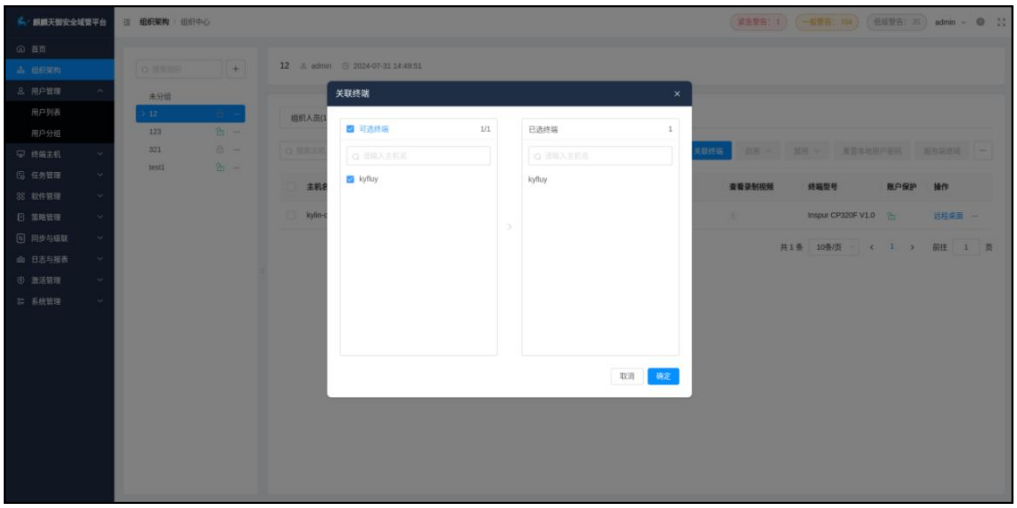

图 4-6 组织终端-关联终端界面

支持对单个或多个终端进行批量终端启用、终端禁用、本地用户启用、本地用户禁用，重置本地用户密码、服务端退域、全部导出、调整组织和移除操作。

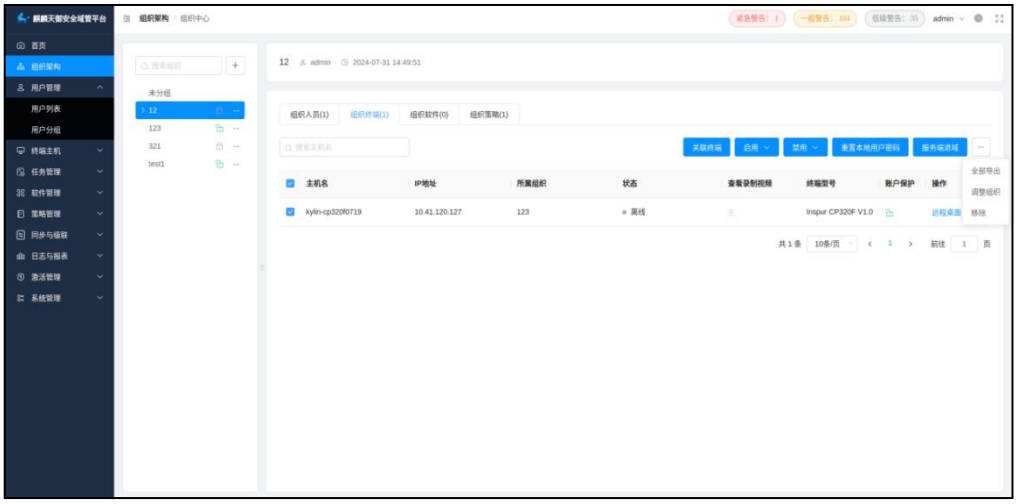

图 4-7 组织终端-批量操作界面

支持对单个终端进行远程桌面和账户保护操作。

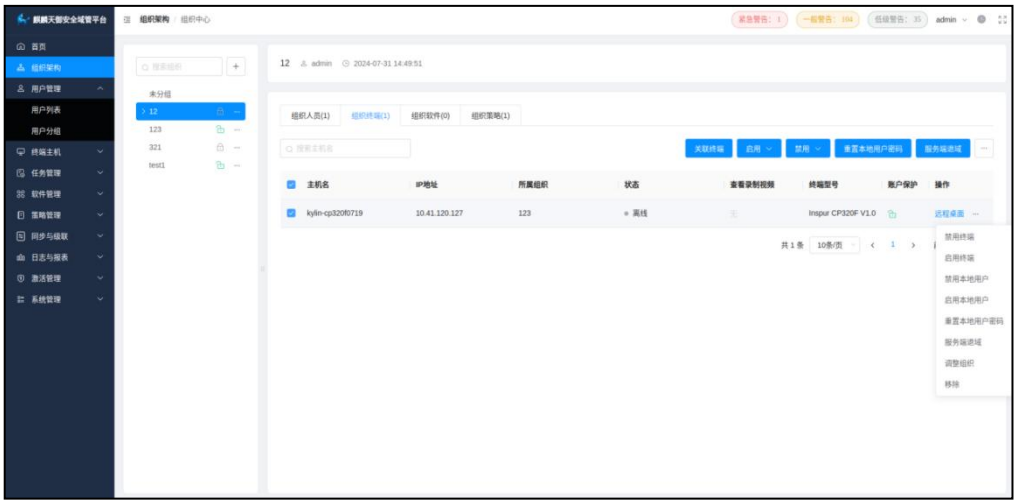

图 4-8 组织终端-终端操作界面

组织软件

支持对组织添加软件，添加后组织内用户可在终端通过麒麟软件商店客户端进行软件查看和下载。

未对组织分配软件时，麒麟软件商店客户端展示内容无限制；当为组织分配软件后，麒麟软件商店客户端仅能展示已添加的软件。

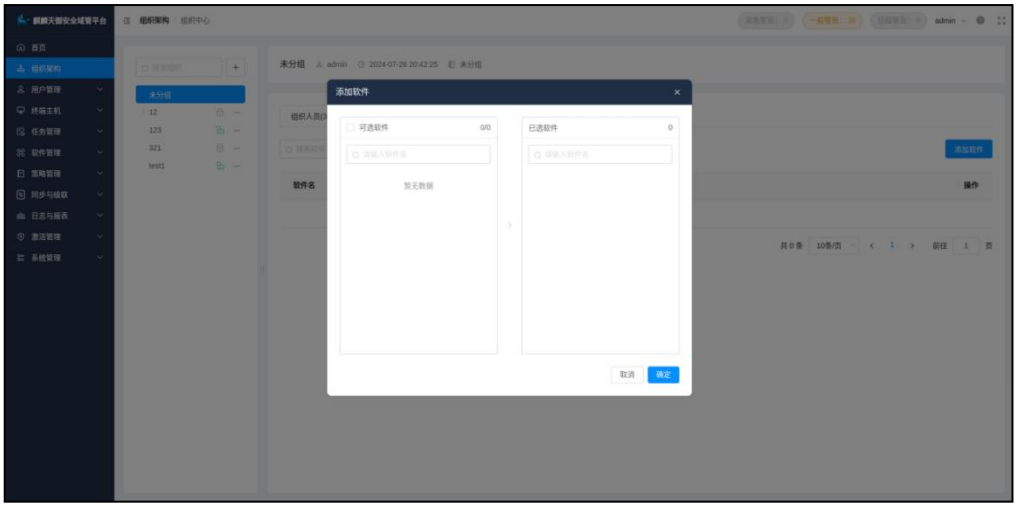

图 4-9 终端软件-添加软件界面

组织策略

支持查看对组织下发的策略，在链接策略页面，可手动链接策略组中的策略。

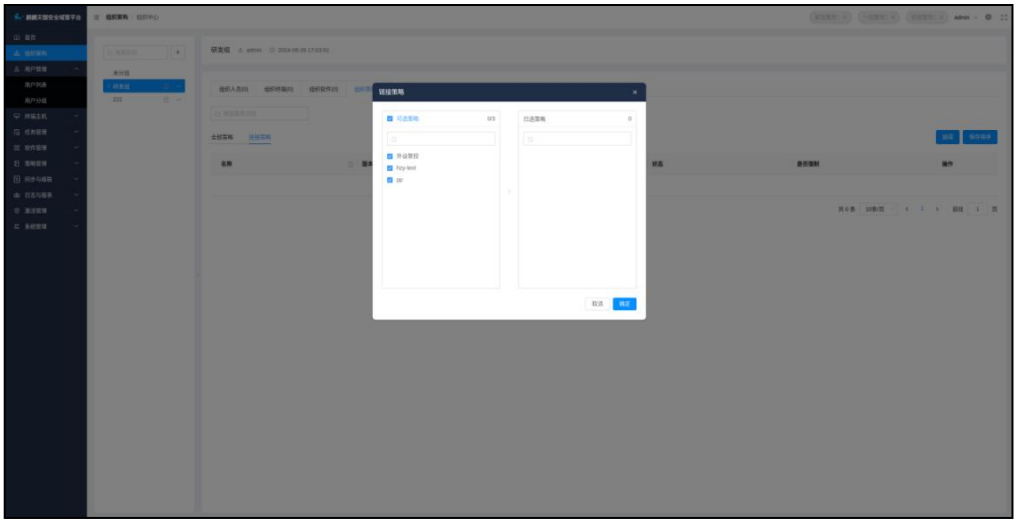

图 4-10 组织策略-链接策略组界面

支持拖动【 】手动调整策略优先级，点击保存排序，完成策略优先级调整。

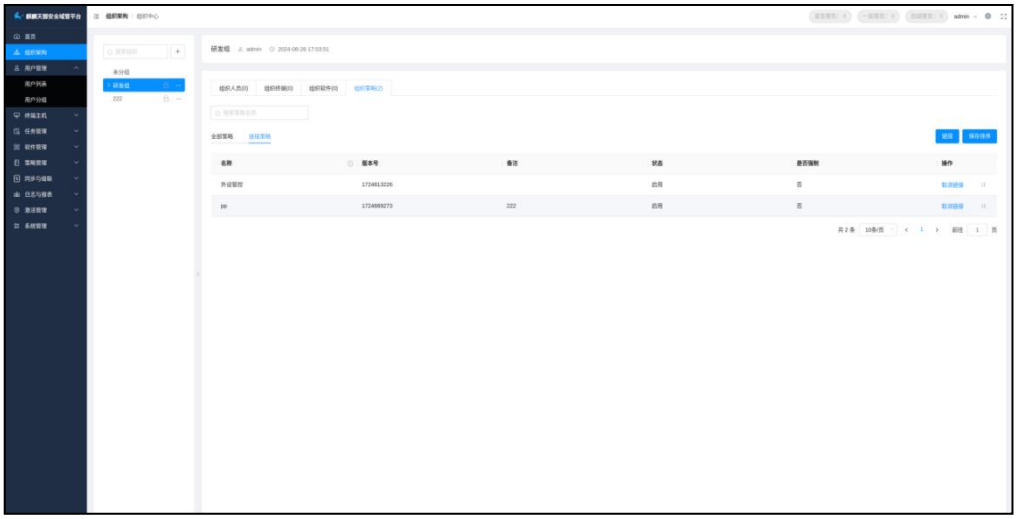

图 4-11 组织策略界面

5 账户管理

5.1 用户列表

用户管理模块展示的账户均为域账户，可通过平台管理员手动添加或批量添加，也可通过对接第三方数据源同步获取。

支持点击【 】自定义列，可自定义展示列名与列宽。

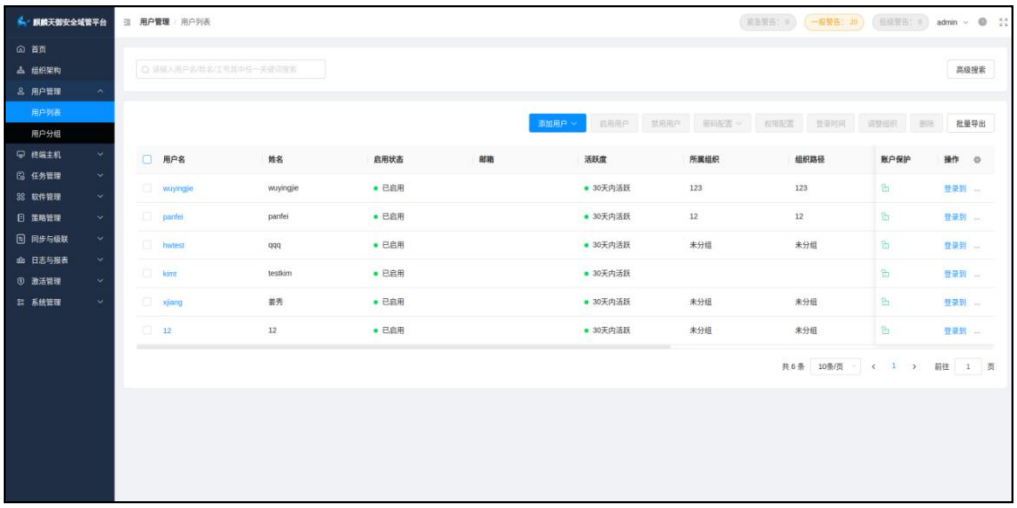

图 5-1 用户列表界面

域账户创建：进入用户管理-用户列表模块，点击【添加用户】按钮，填写用户信息进行域账户的创建。

赋予域账户加域权限：当勾选后，可使用该域账户进行加域。

赋予域账户退域权限：当勾选后，可使用该域账户进行退域。

关联到用户默认分组：当勾选后，该域账户自动关联到用户管理-用户分组-default 分组中。

图 5-2 添加用户界面

登录时间：可限制域用户允许登录时间。默认情况下，域账户可登录时间不受限制。

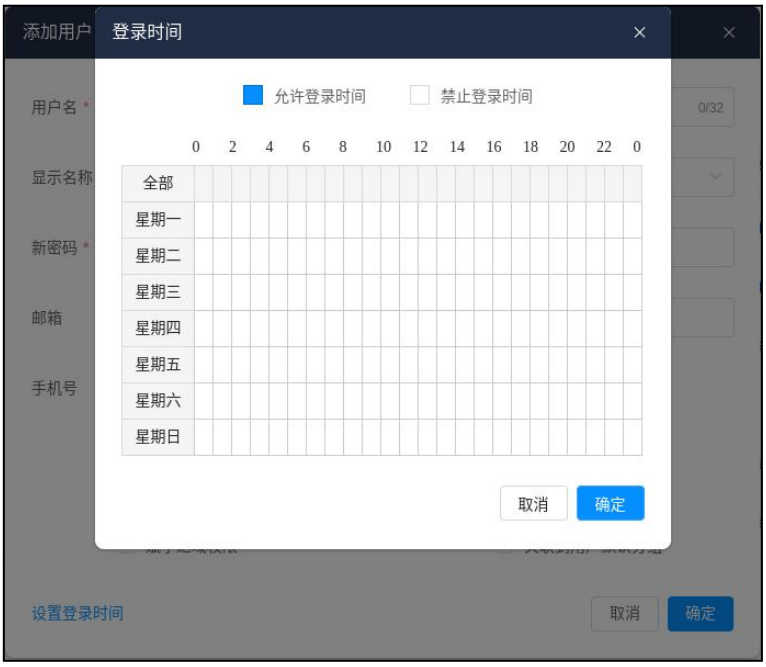

图 5-3 登录时间配置界面

支持对单个或者多个账户进行批量启用、禁用、重置密码、重置 AD 用户密码、权限配置、登录时间、调整组织和删除等。

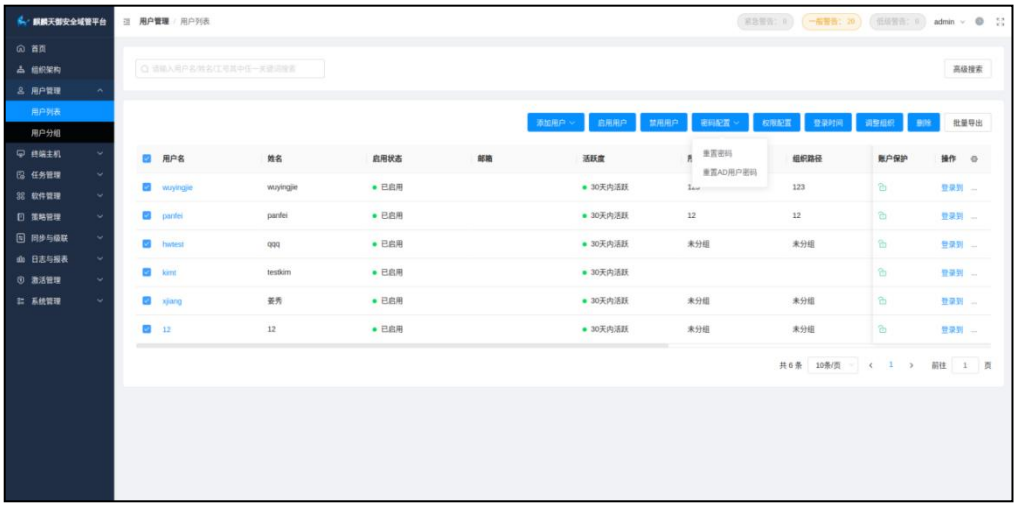

图 5-4 用户列表-用户批量操作界面

启用禁用：选择用户后，支持对用户做启用、禁用操作。启用后的用户允许登录终端，禁用后的用户无法登录终端。

重置密码：支持批量重置域用户密码。

重置 AD 用户密码：支持批量重置 AD 用户密码（仅在对接 Windows AD 后生效）。

权限配置：支持批量配置域用户权限（需要在域用户权限中新增用户角色）。

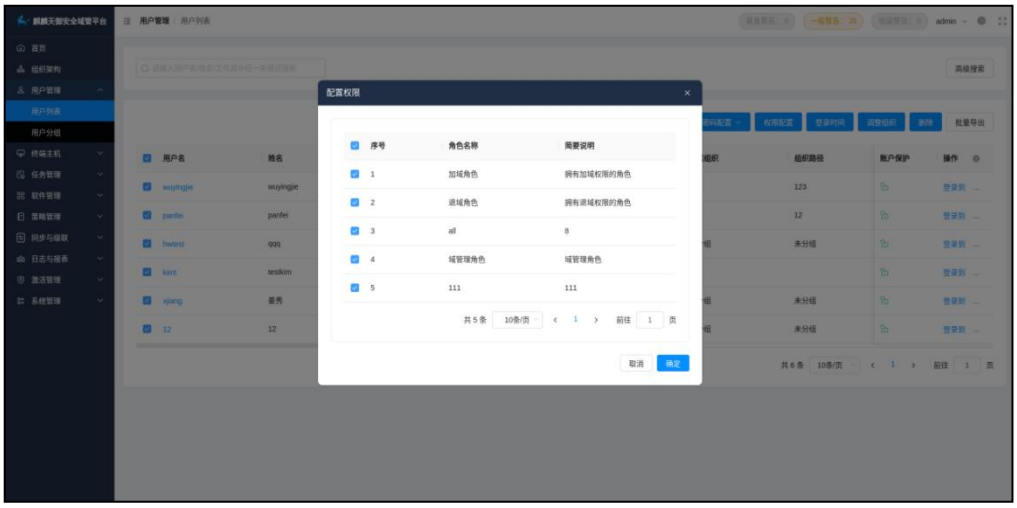

图 5-5 配置权限界面

调整组织：支持批量调整用户组织。

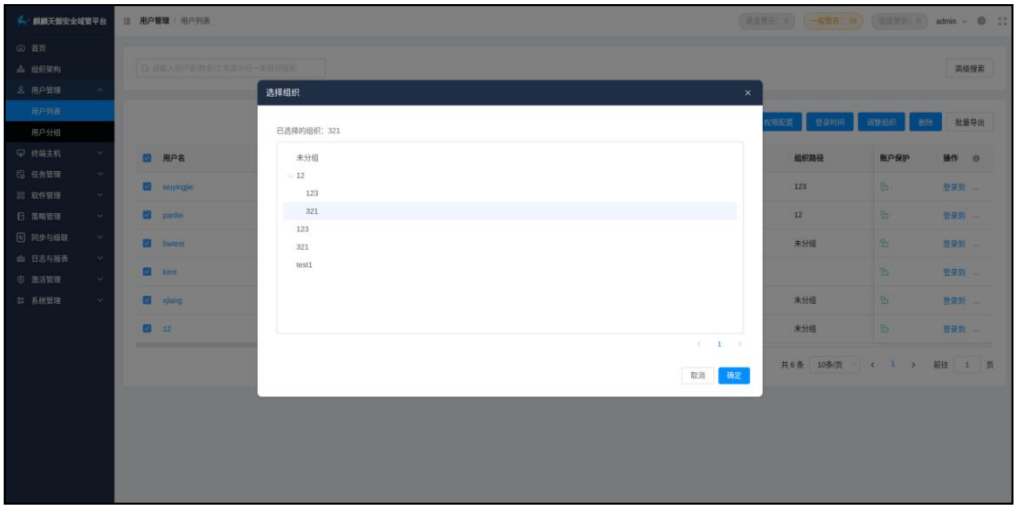

图 5-6 用户选择组织界面

编辑用户：支持对域账户进行编辑。除登录名外，支持对域账户其他配置信息进行修改，编辑设置该域账户的可登录时间。

图 5-7 编辑用户界面

解锁：支持对多次输入错误密码而导致锁定的域账户进行解锁。

账户保护：防止域账户被误删除。

登录主机：点击【登录到】按钮，支持为该域账户配置可登录的终端。默认情况下，只有在为域账户分配可登录终端后，域账户才具备登录终端的权限。通过配置可实现一个域用户登录单个终端或多个终端的场景。

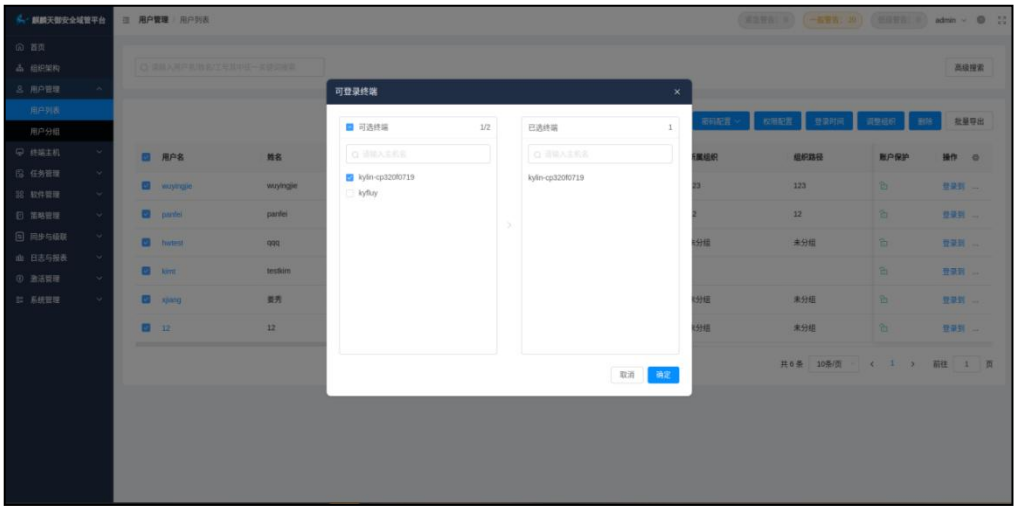

图 5-8 可登录终端配置界面

在用户列表的顶部栏支持多类型关键词搜索，点击【高级搜索】支持多条件搜索。

5.2 用户分组

可根据业务场景，创建不同用户分组，将不同用户加入分组。支持对分组进行批量导入、批量导出、配置权限和批量删除操作。在用户分组中，系统自带默认 default 分组。

可对分组进行关联用户，分配可登录终端、可登录终端分组、可登录组织和分组角色等操作。

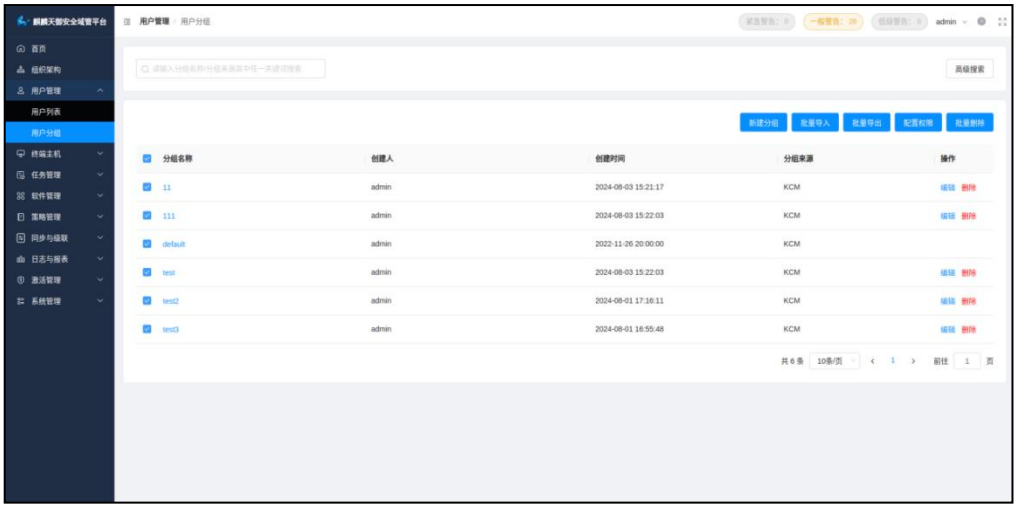

图 5-9 用户分组界面

点击分组名称，进入用户分组详情。

在分组详情中，点击【关联用户】按钮对用户分组添加用户。

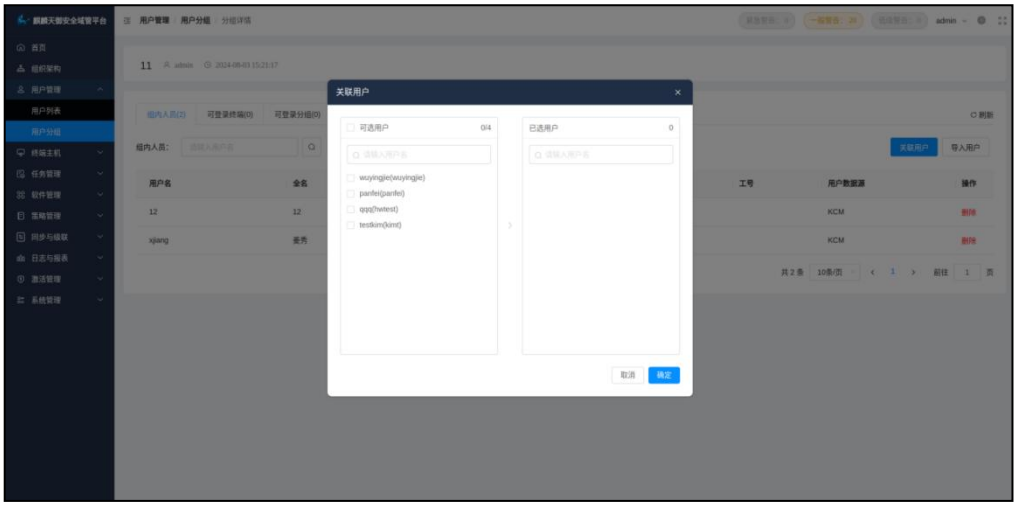

图 5-10 关联用户界面

在用户分组中，进入可登录终端页，点击【添加终端】，支持为组内人员分配可登录终端。

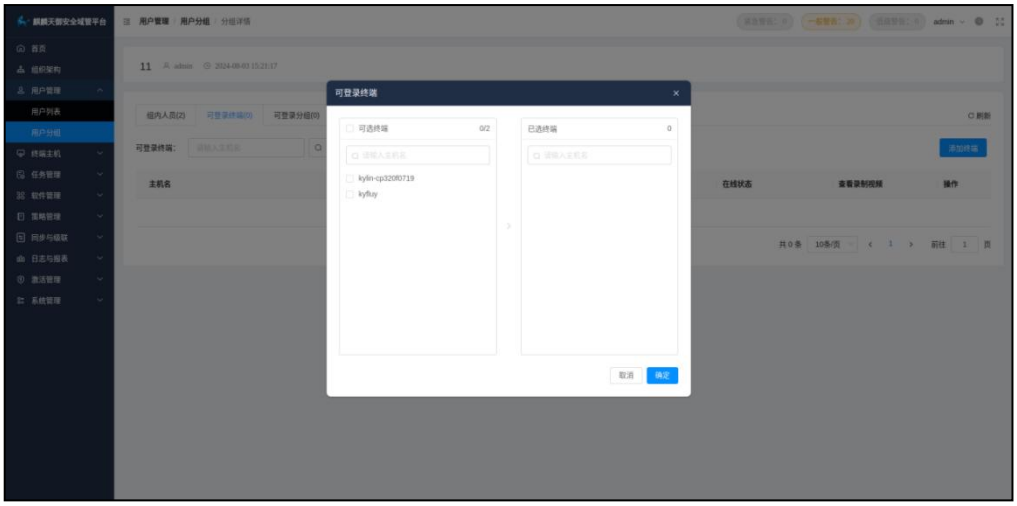

图 5-11 添加终端界面

在用户分组中，进入可登录分组页，点击【添加分组】，支持为组内人员添加可登录的终端分组。

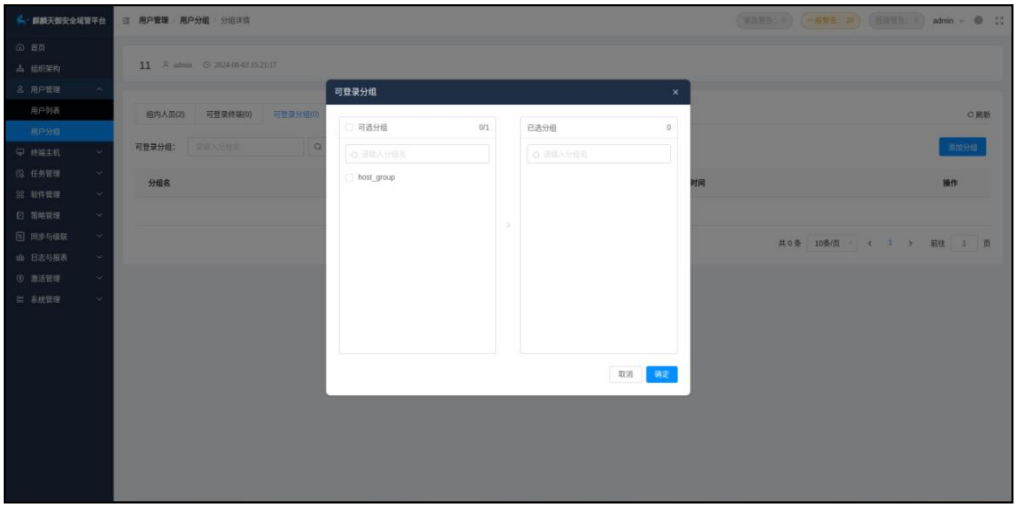

图 5-12 添加分组界面

在用户分组中，进入可登录组织页，点击【添加组织】，支持为组内人员添加可登录组织中的所有终端。

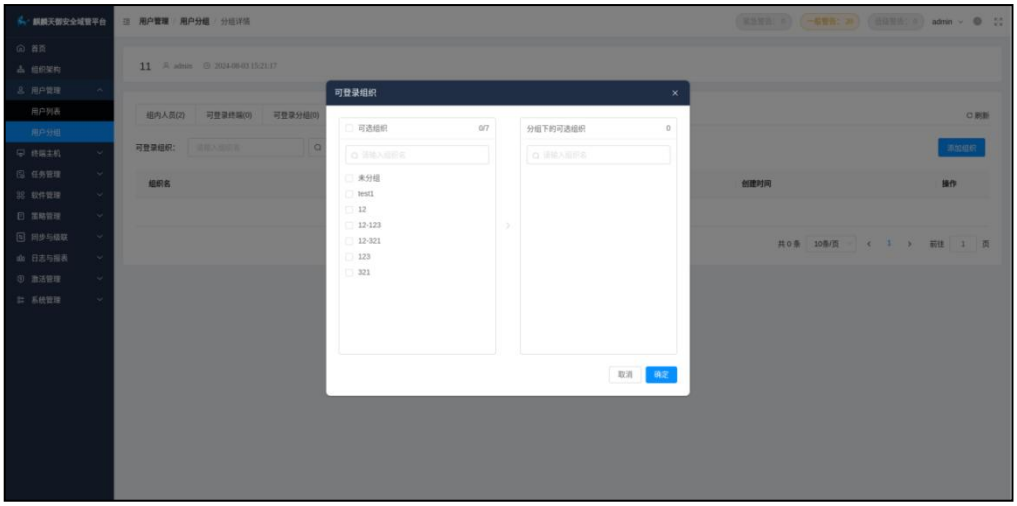

图 5-13 添加组织界面

进入分组角色页，可查看该分组的角色，即该分组中的域用户登录终端后具备的角色权限。

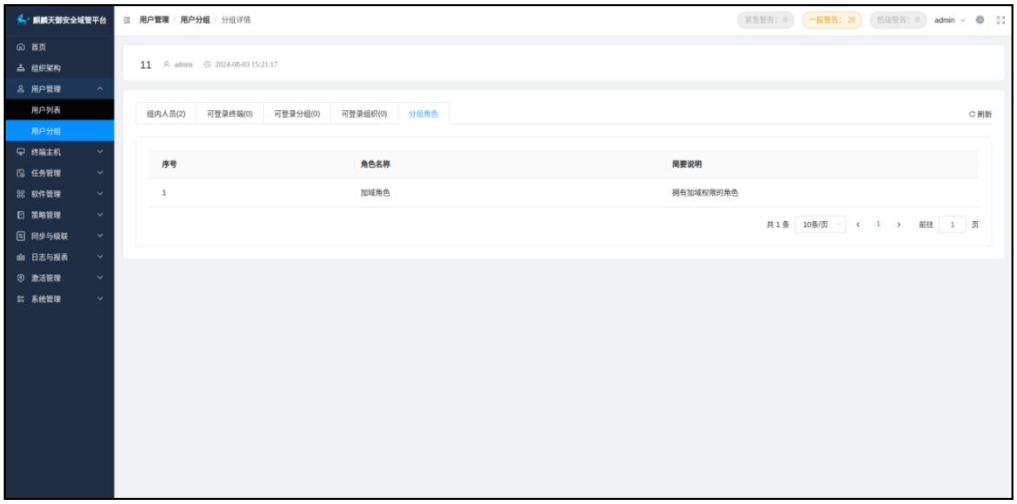

图 5-14 分组角色界面

6 终端管理

6.1 终端列表

通过麒麟天御客户端进行加域操作后，登录管理平台可在终端列表中查看终端信息。

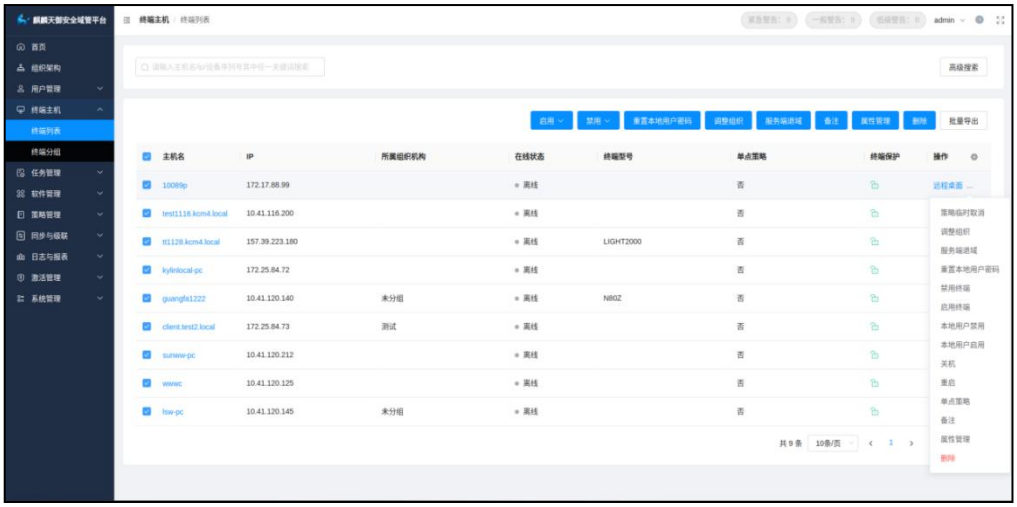

图 6-1 终端列表操作界面

支持查看终端属性：主机名、CPU 架构、IP、操作系统版本、内核版本、运行环境、客户端版本、MAC 地址、最后在线时间、最后登录时间、所属组织机构、所属分组、设备序列号、在线状态、活跃度、注册状态、本地用户状态、主机状态、最近使用人、最近使用账号、终端属性和终端型号等。

管理员支持对单个或多个终端进行启用终端、禁用终端、启用本地用户、禁用本地用户、重置本地用户密码、调整组织、服务端退域、属性管理和删除等操作。

启用禁用终端：选择终端后，支持对终端做启用和禁用操作。启用后用户允许登录终端，禁用后用户无法登录终端。

启用禁用本地用户：选择终端后，支持对启用和禁用本地用户操作。启用后本地用户允许登录终端，禁用后本地用户无法登录终端。

重置本地用户密码：支持重置本地用户密码。

调整组织：支持批量调整终端组织。

服务端退域：支持管理员批量下发终端退域。

属性管理：支持为终端配置个人机和公共机属性。配置公共机属性的终端将允许相同组织内的域用户登录。

图 6-2 修改终端属性界面

删除：选择点击删除按钮，则在服务端删除该条终端信息。删除后，该终端将无法正常使用域账户登录。

支持远程桌面、关机、重启，单点策略、终端保护和策略临时取消等操作。

远程桌面：支持管理员远程连接终端进行运维管理操作。

单点策略：支持单独为该终端创建终端策略并立即生效。

图 6-3 单点策略配置界面

终端保护：防止终端被误删除。

策略临时取消：支持对该终端生成策略临时取消的验证密码，在客户端输入相应验证密码后可临时取消策略。系统重启后，策略的临时取消状态将自动失效，并恢复为原有状态。

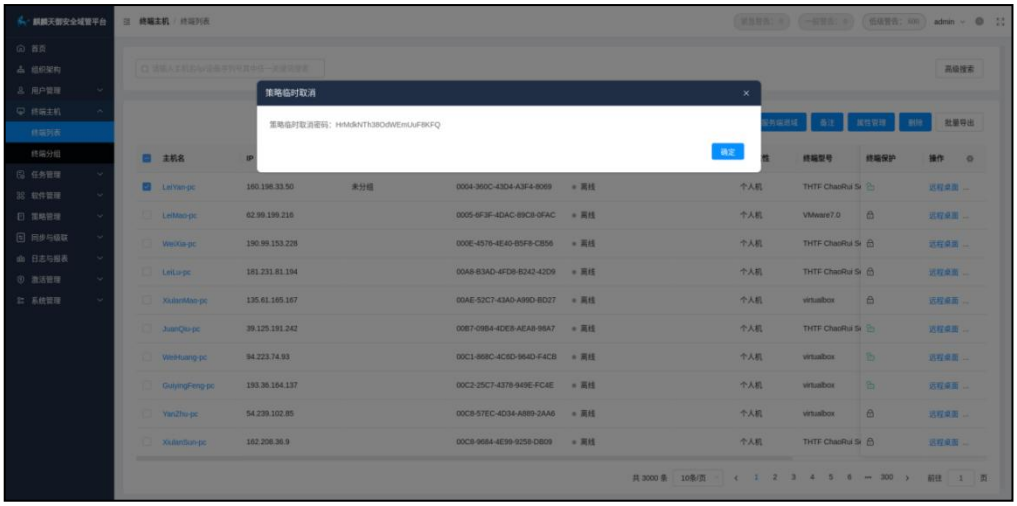

图 6-4 策略临时取消

搜索：终端列表的顶部栏支持多类型的终端搜索，输入搜索条件后，点击【查询】进行搜索。点击【重置】，对搜索条件进行清空。

终端详情

单击终端的主机名，进入终端详情页面。在终端详情页面可查看系统信息、系统图表、进程信息、终端策略、登录日志和已安装软件等。

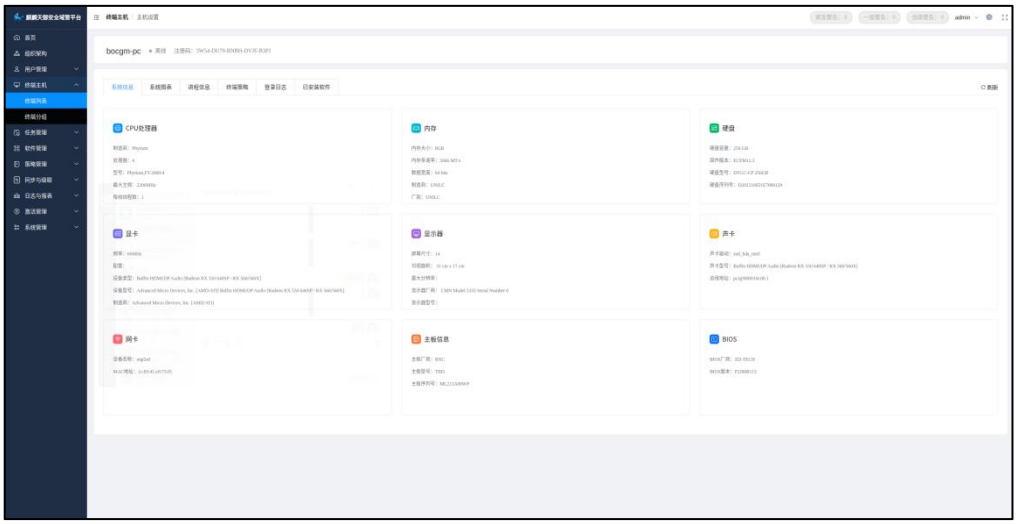

图 6-5 终端系统信息界面

系统信息：支持查看 CPU、内存、硬盘、显卡、显示器、声卡、网卡、主板和 BIOS 等硬件信息。

系统图表：支持查看 CPU 占用率、内存占用率和硬盘占用率。

进程信息：支持查看进程名称和核心占用率等指标信息。

终端策略：支持查看对该终端下发的链接策略、分组策略、组织策略和当前终端策略生效详情。其中，链接策略可手动链接策略组策略，并支持手动调整策略优先级。

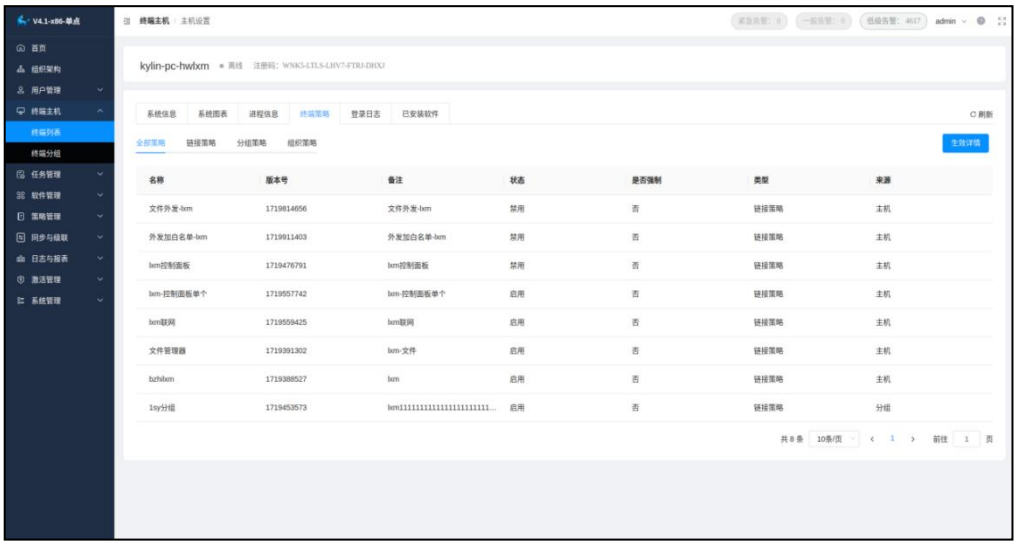

图 6-6 终端策略界面

登录日志：支持查看用户登录和登出行为信息。

已安装软件：支持查看该终端通过软件商店安装更新的软件信息。

6.2 终端分组

可根据业务场景，创建不同终端分组，并将不同终端加入分组。支持批量管理组内终端、分组软件和分组策略等。

支持新建分组、批量导入、批量导出和批量删除操作。

图 6-7 终端分组界面

进入终端分组详情，支持对组内终端、软件和策略进行查看和编辑。

在终端分组中，进入组内终端页，点击关联终端按钮，支持为分组添加终端。

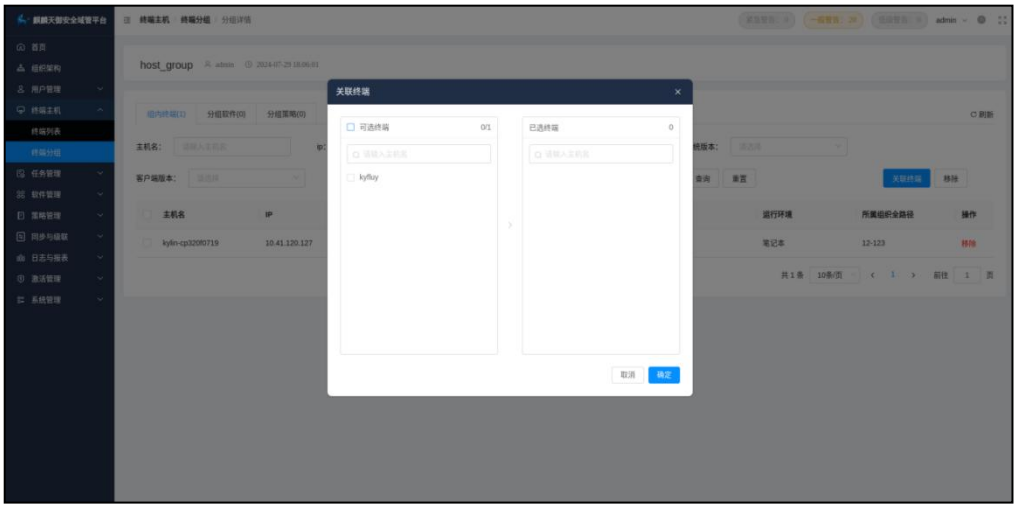

图 6-8 终端分组关联终端界面

在终端分组中，进入分组软件页，点击添加软件，支持为该终端分组添加终端从麒麟软件商店客户端可下载相应软件（麒麟天御服务端需在软件商店模块同步麒麟私有化软件商店平台数据）。

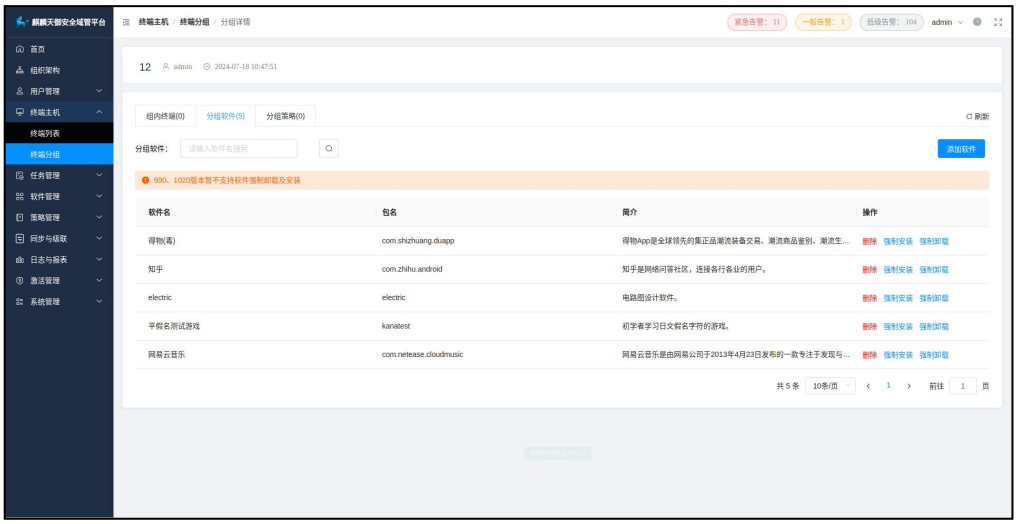

图 6-9 终端分组软件界面

在终端分组中，进入分组策略页，支持查看该终端分组的策略。

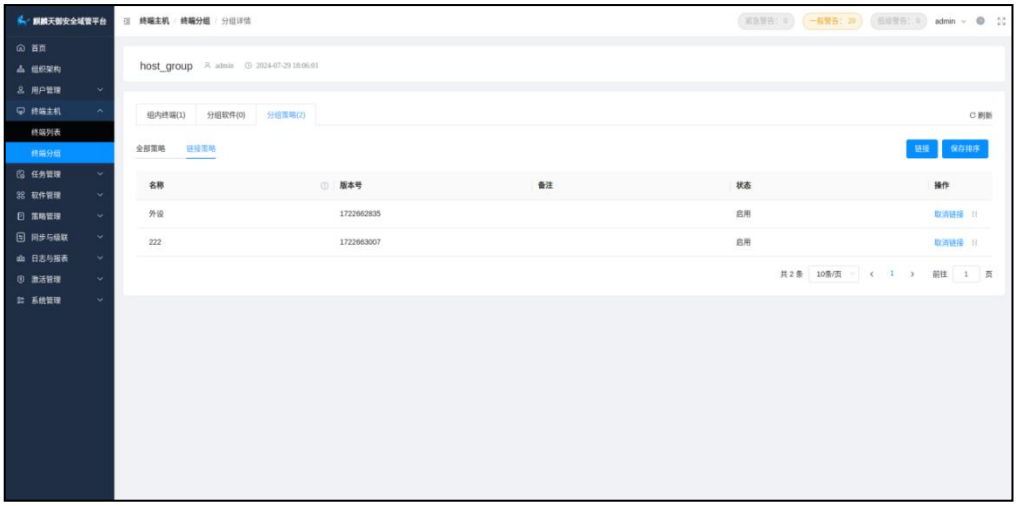

图 6-10 分组策略界面

7 任务管理

7.1 文件推送

在任务管理-文件推送模块，点击新建任务，支持文档、脚本、软件、补丁、浏览器证书和其他等多种文件类型下发。

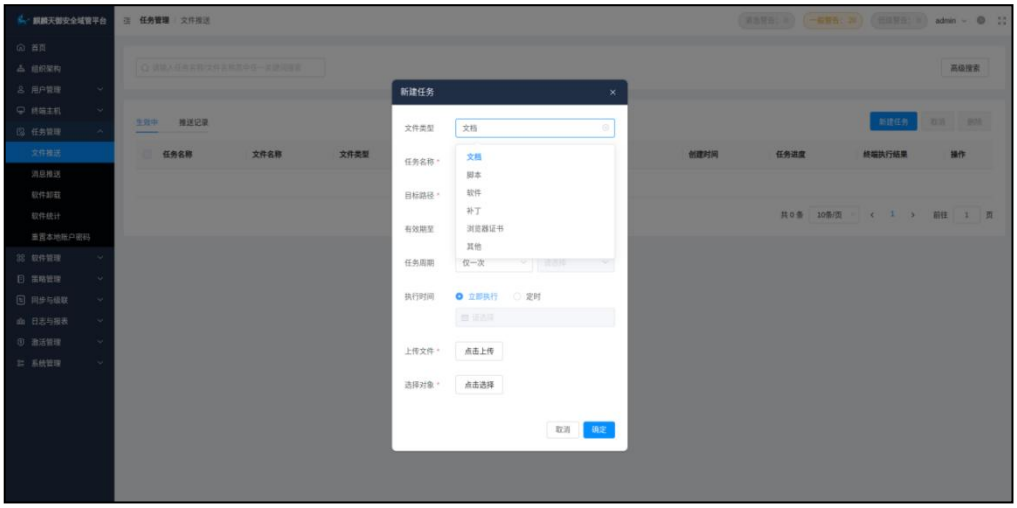

图 7-1 新建文件推送界面

支持设置目标路径、有效期、任务周期、执行时间和对象等。

其中选择脚本文件，推送方式为仅接收时，可设置目标路径，有效期、任务周期、执行时间和对象等。推送方式为接收并执行时，可设置脚本运行参数、运行时间、有效期、任务周期、执行时间和对象等。

支持按照组织、分组和设备进行推送下发。

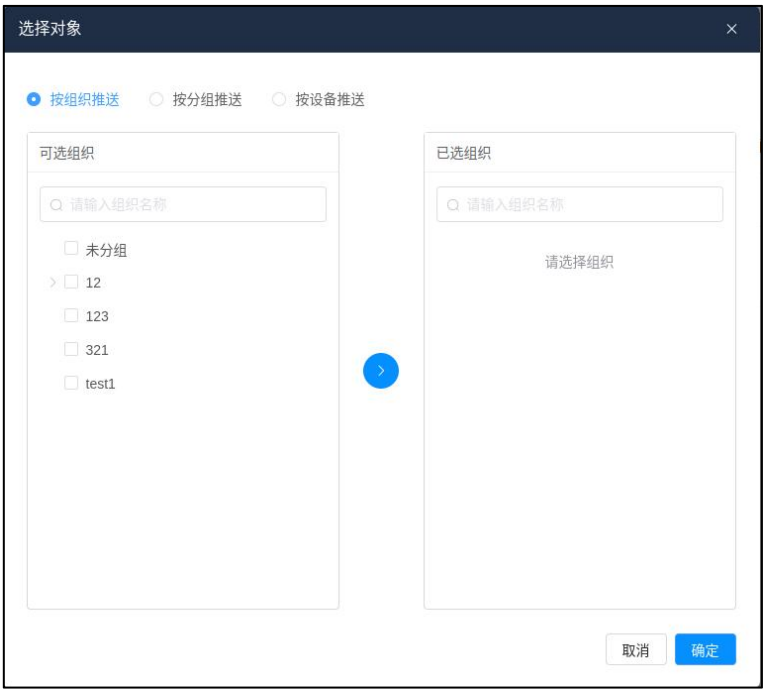

图 7-2 文件推送选择对象界面

推送任务生成后，支持查看任务进度、终端执行结果和执行记录等信息。支持对任务进行编辑、取消、删除和失败重试等操作。

进入推送记录页面，可查看历史任务情况，包括：任务进度、终端执行结果和执行记录等信息。

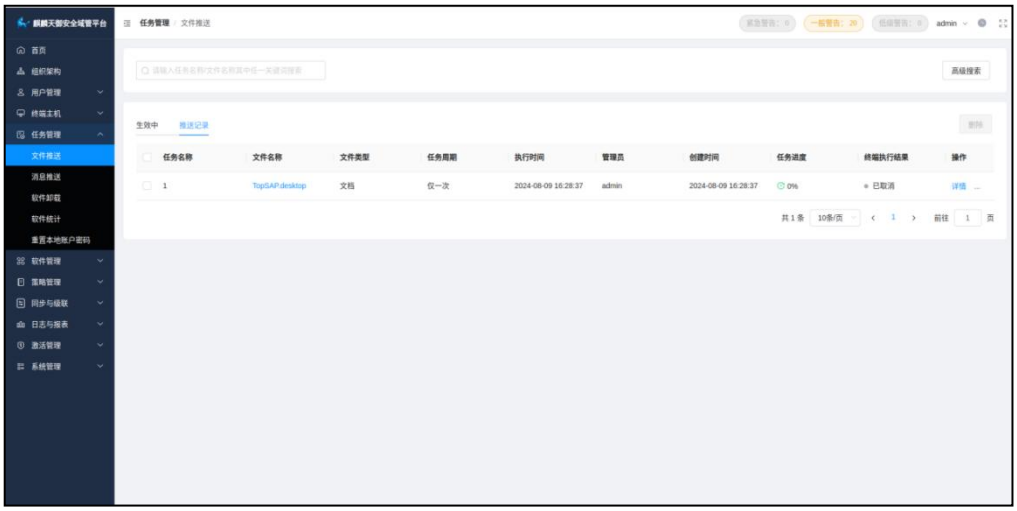

图 7-3 文件推送推送记录页面

7.2 消息推送

点击新建任务，支持管理员在麒麟天御服务端自定义创建消息，包括：消息标题、消息内容、消息等级、有效期和执行时间等。

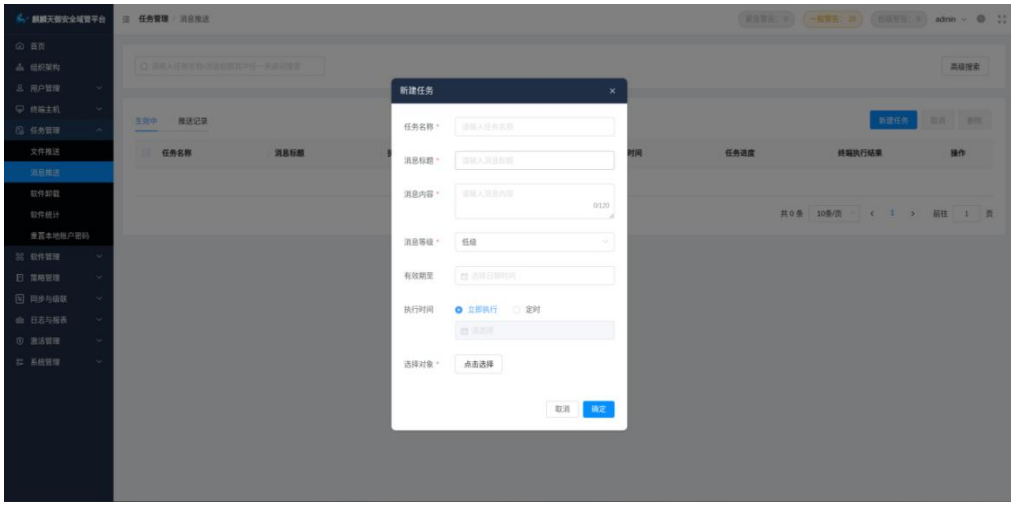

图 7-4 新建消息推送界面

支持按照组织、分组、设备、用户组织、用户分组和用户进行推送下发。

消息任务生成后，支持查看任务进度和终端执行结果等信息。支持对任务进行编辑、取消、删除和失败重试等操作。

进入推送记录页面，可查看历史任务情况，包括：任务进度、终端执行结果和执行状态等信息。

图 7-5 消息推送记录界面

支持查看任务详情。

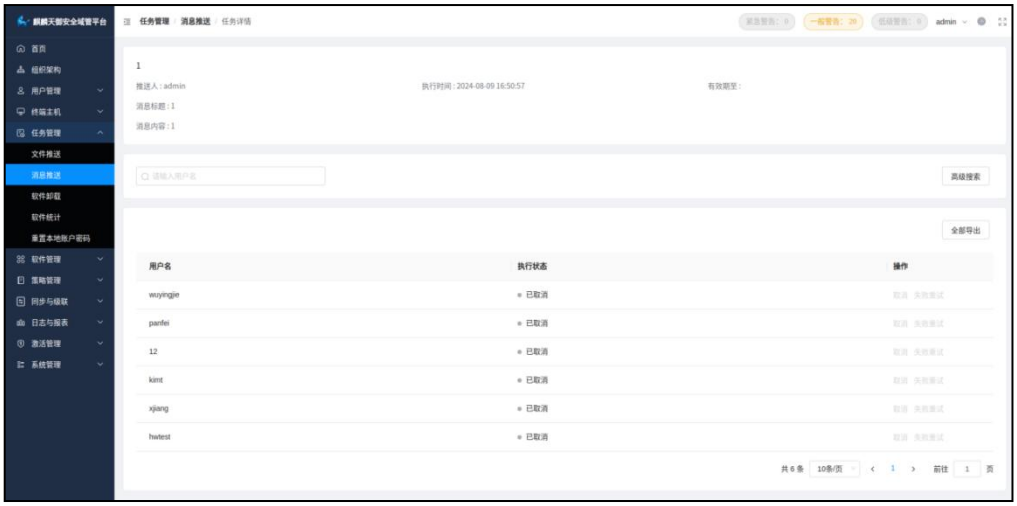

图 7-6 消息推送任务详情界面

消息有效期：在消息下发后，某些终端因为关机或网络问题等原因未成功接收到消息。如果这部分终端在消息任务有效期时间内再次开机或修复网络问题则会及时接收该消息。如果某些终端接收消息时间已经超过有效期后，则将无法再接收该消息。

7.3 软件卸载

点击新建任务，支持管理员在麒麟天御服务端对终端下发软件卸载任务。支持按照组织、分组和设备进行推送下发。

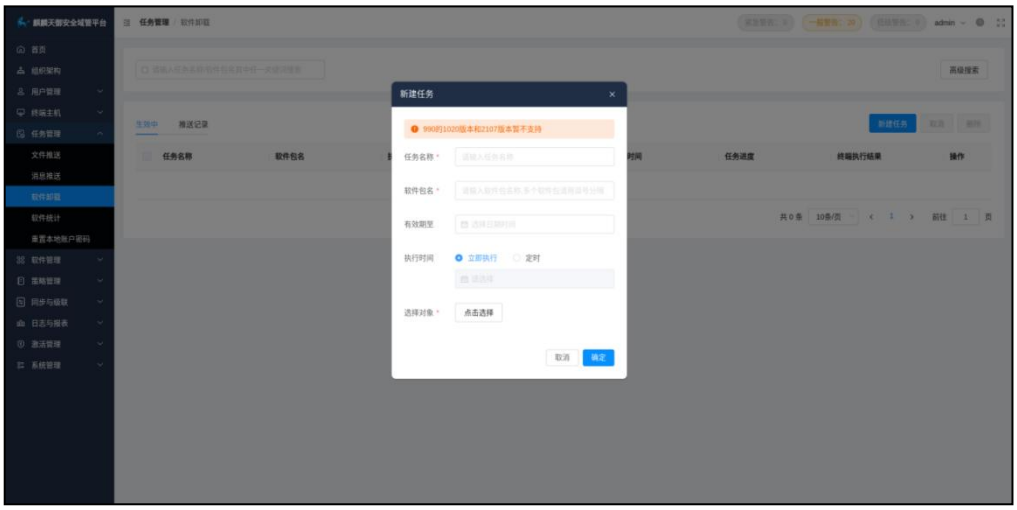

图 7-7 新建软件卸载任务界面

卸载软件包名查找方法：在终端操作系统下，打开 Terminal 命令行，进入 /usr/share/applications 路径，找到对应的预卸载的软件，填写.desktop 前的部分。

例如：卸载 360 浏览器，则填写 browser360-cn。

图 7-8 终端查询界面

软件包卸载任务生成后，支持查看任务进度和终端执行结果等信息。支持对任务进行编辑、取消、删除和失败重试等操作。

进入推送记录页面，可查看历史任务情况，包括任务进度和终端执行结果等信息。

7.4 软件统计

软件统计模块支持对终端上已经安装的软件发起统计，并将统计结果收集返回到麒麟天御安全域管平台软件管理>软件统计模块。

支持按照组织、分组和设备进行推送下发。

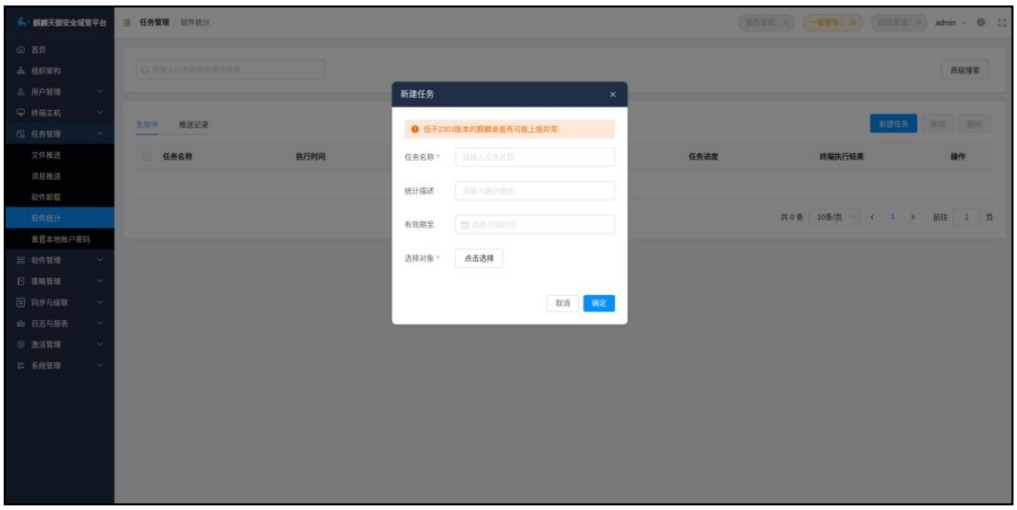

图 7-9 新建软件统计界面

软件统计任务生成后，支持查看任务进度和终端执行结果等信息。支持对任务进行编辑、取消、删除和失败重试等操作。

进入推送记录页面，可查看历史任务情况，包括任务进度、终端执行结果和执行状态等信息。

7.5 重置本地用户密码

重置本地账户密码支持对终端操作系统的本地账户进行密码重置，重置时需要设置账户名称和新密码。

点击新建任务，可输入重置账户名称、重置密码（可使用随机密码）、选择有效期、任务周期和执行时间等信息。

在创建密码重置时，支持使用随机密码，支持将推送条件设置为周期执行，实现对终端的本地账户定期修改密码的场景。

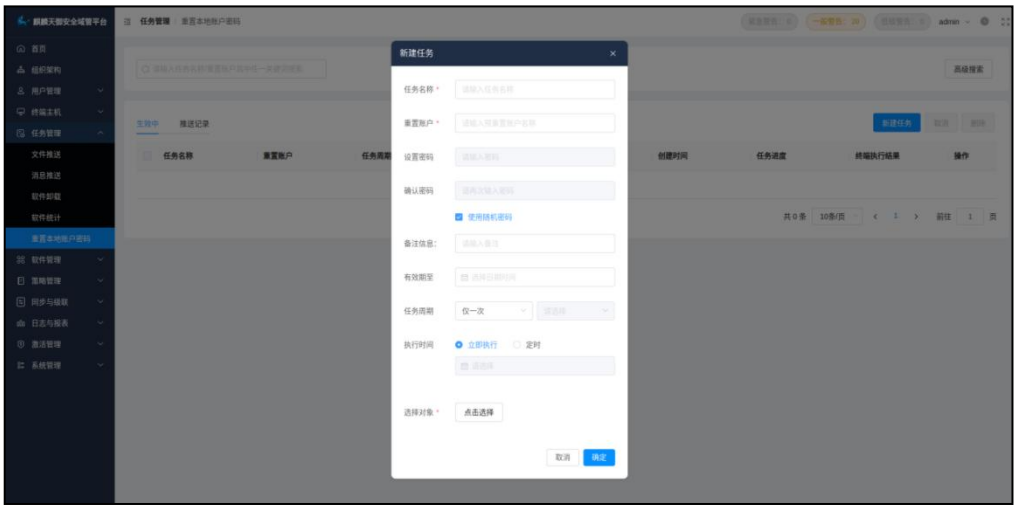

图 7-10 新建重置本地用户策略任务界面

支持按照组织、分组和设备进行推送下发。

重置本地账户密码任务生成后，支持查看任务进度和终端执行结果等信息。支持对任务进行编辑、取消、删除和失败重试等操作。

进入推送记录页面，可查看历史任务情况，包括任务进度、终端执行结果和历史执行记录等信息。

8 软件管理

8.1 软件商店

该模块支持对接麒麟私有化软件商店平台，能够实现对软件进行统一全生命周期管理。

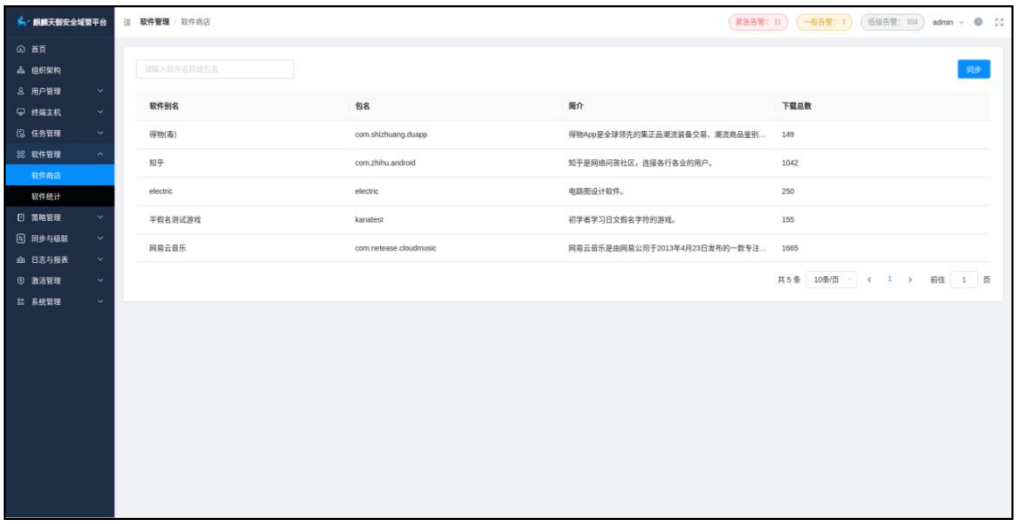

图 8-1 软件商店界面

点击右上角【同步】按钮，支持对接同步麒麟私有化软件商店平台可用软件列表。

支持给组织内的终端添加可用软件，添加后组织中的终端可在麒麟软件商店客户端进行软件下载安装。

图 8-2 添加软件界面

支持给终端分组添加可用软件，添加后分组中的终端可在麒麟软件商店客户端进行软件下载安装。

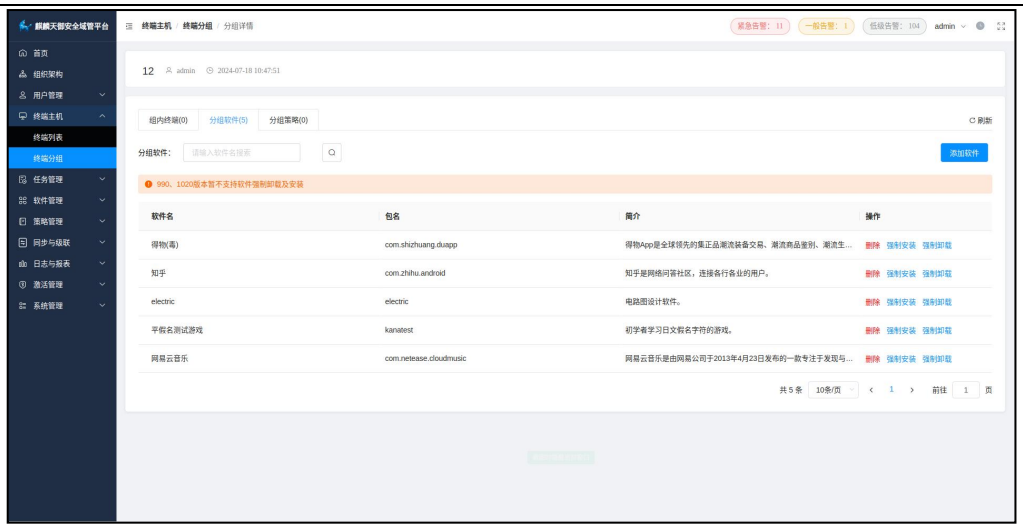

图 8-3 分组软件界面

注：未对终端分配软件时，麒麟软件商店客户端展示内容无限制。当为终端分配软件后，麒麟软件商店客户端仅能展示已添加的软件。

8.2 软件统计

软件统计模块支持对终端上已经安装的软件进行统计。支持按照软件维度与终端维度进行统计。

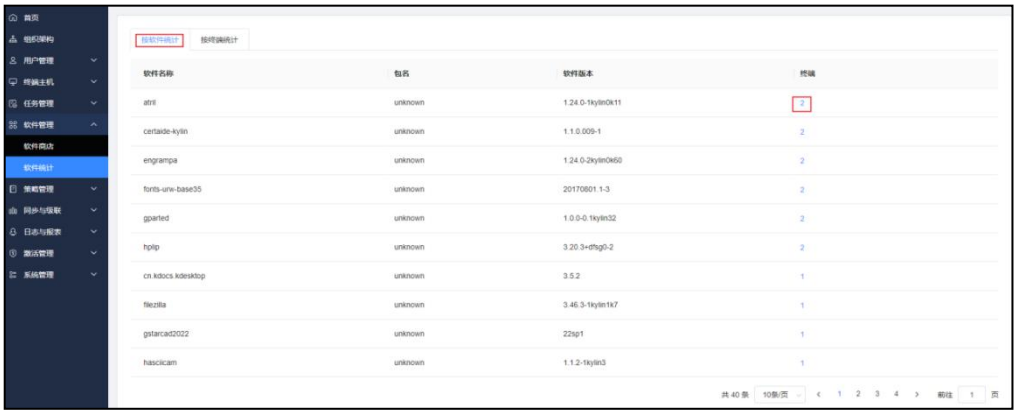

图 8-4 软件统计界面

以终端的维度展示已安装软件信息。

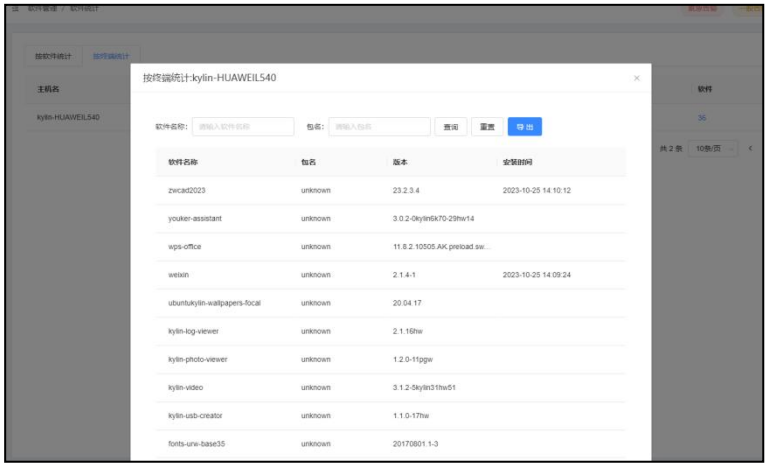

图 8-5 终端统计视图界面

9 策略管理

策略使用流程：策略创建-策略下发-查看详情-策略更新、取消和删除。

9.1 策略创建

点击新建策略组，可选择是否使用已有策略模板进行创建，减少重复步骤。

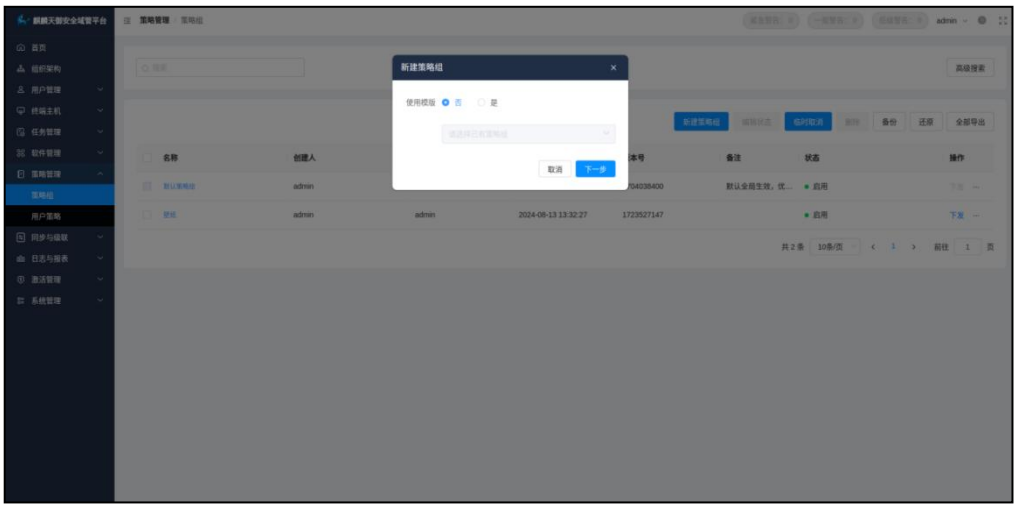

图 9-1 新建策略组界面

配置策略内容，当前版本支持 9 大类 150 余项策略管控项。包括：水印、系统管控、个性化、网络、外设、安全基线、控制面板和文件外发管控。

图 9-2 策略组配置界面

软件网络管控提供应用层面的联网控制、网络限速和流量监控等策略。

图 9-3 应用管控界面

实现管理敏感数据外传管控与审批，用于控制并审批通过 USB 和光盘通道的文件外传，下发管控后管理员可在系统管理-文件外发管理模块对终端的文件

外发行为进行审批。

图 9-4 文件外发管控界面

图 9-5 文件外发审批界面

配置完成后，可按照组织、终端、终端分组进行下发。其中组织可选择强制下发与例外终端。

强制下发：开启后，会对所有下级组织进行策略强制下发。

例外终端：可选择本策略组不下发的终端。

9.2 策略管理

可对策略组进行编辑、启用禁用、编辑生效条件、临时取消、删除、备份、还原和全部导出等操作。

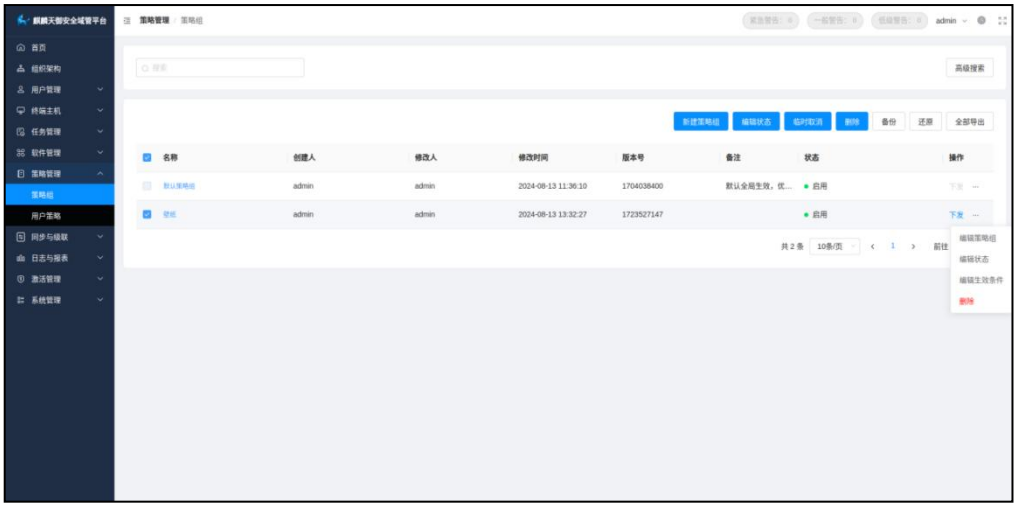

图 9-6 策略终端操作界面

默认策略组：默认全局生效，优先级最低的策略组，不可删除，支持自定义编辑。

策略临时取消：点击策略组临时取消，会生成策略临时取消的验证密码，在终端右键点击麒麟天御客户端，输入该验证密码，则应用的策略临时失效。系统重启后，策略的临时取消状态将自动失效，并恢复为原有状态。

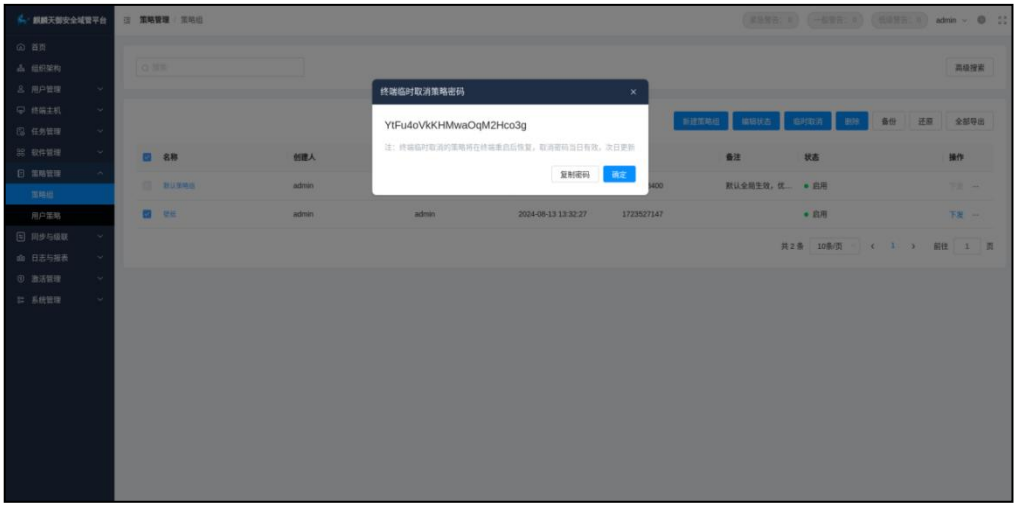

图 9-7 策略组临时取消界面

策略生效条件：可对策略的生效范围做限制，包括：操作系统、生效场景、芯片架构、系统版本、终端类型和管理员管辖范围。

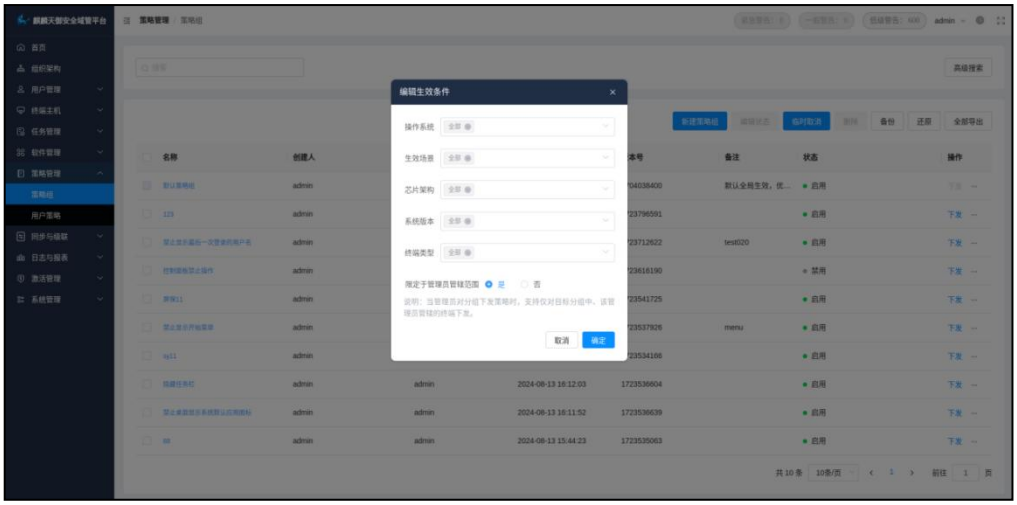

图 9-8 策略组生效条件

管理员管辖范围：当管理员对分组下发策略时，支持仅对目标分组中和该管理员管辖的终端下发。

9.3 用户策略

当前版本用户策略为全局域账户密码安全策略。

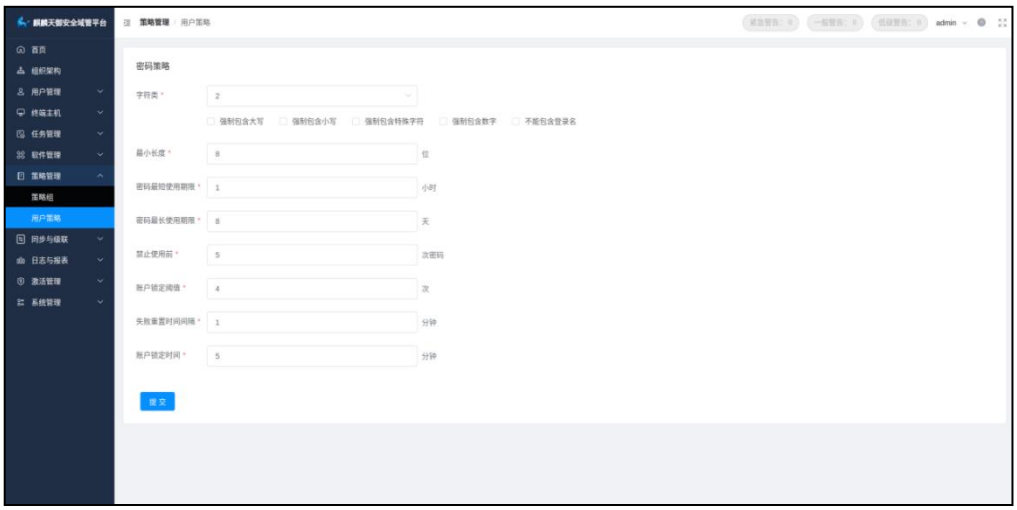

图 9-9 用户策略配置界面

支持的配置项为字符类、最小长度、最短使用期限、最长使用期限、密码历史、账户锁定阈值、锁定时间以和失败重置的间隔等。

10 同步与级联

该模块是与外部平台进行数据同步的配置模块，支持与 Windows AD 进行数

据同步。同时，支持将本平台日志外发和报表外发。

10.1 用户策略

LDAP 数据同步模块，支持标准第三方 LDAP 协议数据同步。

图 10-1 数据同步配置界面

配置项包括：

同步的 AD 类型：支持 ldap、ldap over tls 和 ldaps。

数据源名称：自定义名称。

数据源类型：支持 AD、OpenLDAP。

数据源属性：支持配置主从数据源。

同步地址：填写 AD 服务器的域名或者 IP。

同步端口：同步端口号。

Base DN：检索根目录，定义检索的起始位置。

管理员 DN：填写 AD 服务器用于数据同步的管理员账户 DN。

管理员密码：填写管理员账户的密码。

认证地址：一般情况下与同步的 AD 主机地址保持一致。

认证端口：认证端口号。

域名称：AD 域名。

同步范围：组织、用户组、用户。

同步类型选择：手动同步、自动同步。

周期：支持分、时、天。

例外时间设置：设定某个时间段，该时间段内停止数据同步。

其他配置：纯数字用户是否添加下划线、是否将用户加入默认用户组、是否同步删除操作、是否给同步用户添加加域权限和是否同步修改用户所属组织。

同步根组织：未赋予组织属性的用户/用户组自动同步的组织位置。

注：如果在同步时，纯数字用户是否添加下划线置为关闭，需要确认桌面系统的对应版本支持纯数字用户才能正常登录。

支持查看同步状态和同步详情。支持立即同步、启用、停用和删除等操作。

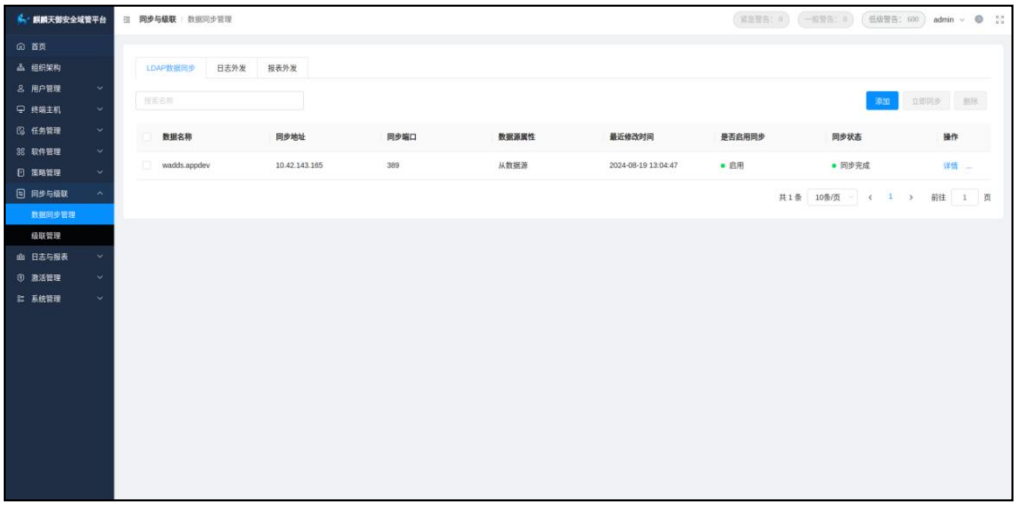

图 10-2 数据同步管理界面

10.2 日志外发

日志外发模块支持将系统中的日志通过 syslog 日志的形式发送到外部平台。

配置外发：点击【新增】按钮-填写外部平台的相关信息。

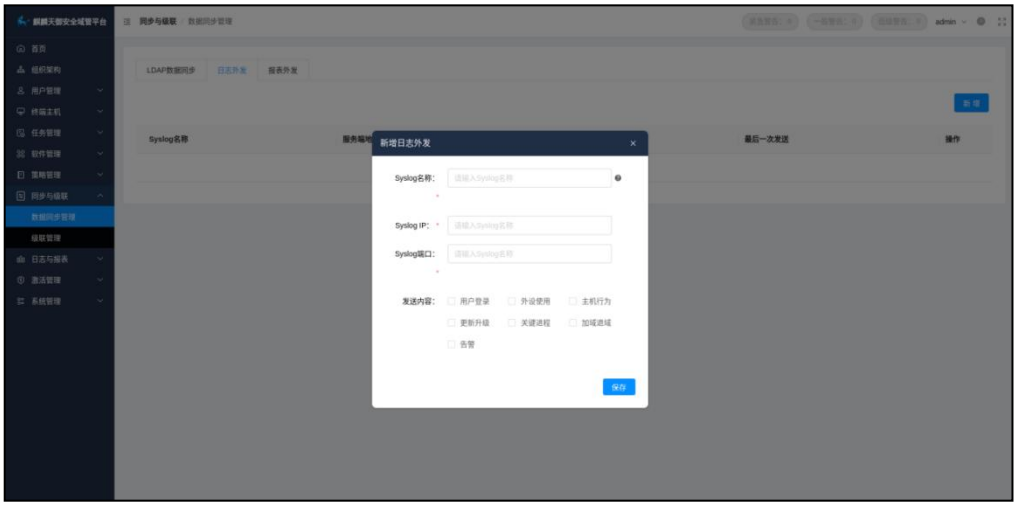

图 10-3 日志外发配置界面

支持发送的数据，包括：用户登录、外设使用、主机行为、更新升级、关键进程、加域退域和告警等。

10.3 报表外发

报表外发模块支持将报表通过邮件的方式发送给客户的邮箱。

新增报表外发：点击【新增】按钮，填写邮箱的相关信息。

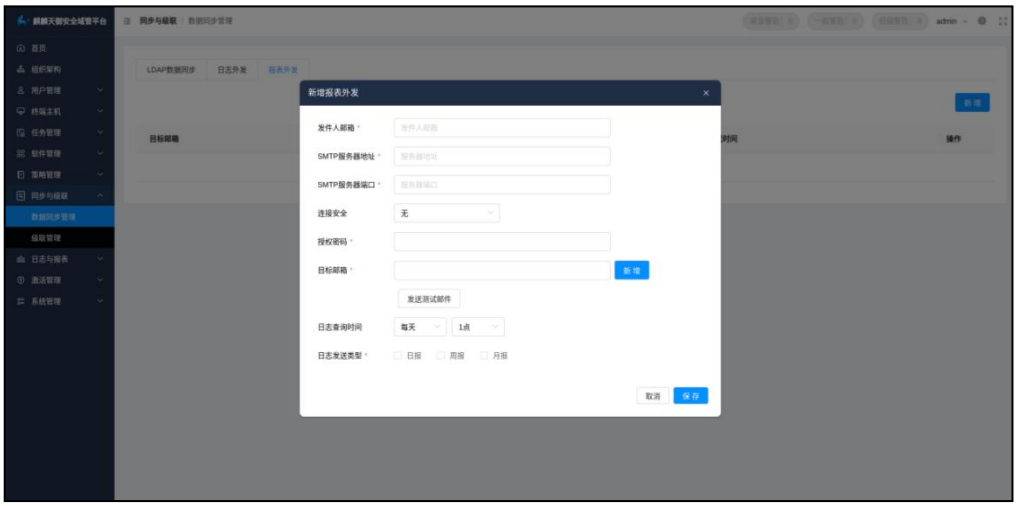

图 10-4 报表外发配置界面

支持发送的数据，包括：日报、周报和月报。

当选择日志发送类型后，按照配置的日志查询时间点进行数据查询，查询范

围为近一日、一周和一月的数据，并将数据发送至目标邮箱。

10.4 级联管理

在大规模、集团型网络环境中，一般需要采用分级部署，即总部部署一套管理平台，各分支机构分别部署一套管理平台，分支机构与总部之间进行级联，以进行数据上报与策略下发等。

确认本平台是做为根域平台还是做为子域平台，在使用过程中需要子域平台申请向上级级联。

申请向上级级联配置，进入上级节点，点击【级联设置】，填写上级平台的相关信息。包括上级节点域名、上级节点端口和是否允许上级直接登录。

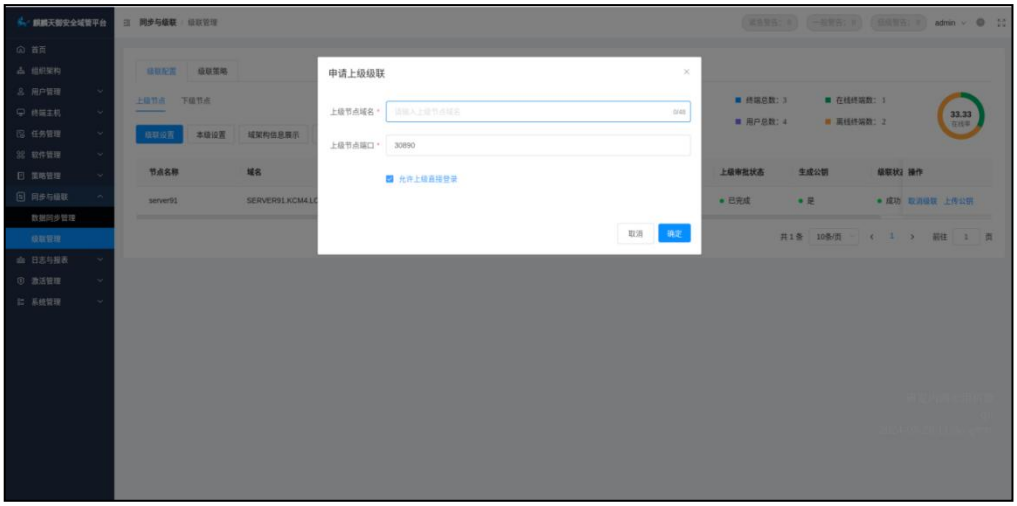

图 10-5 申请上级级联配置界面

进入下级节点，点击【本级设置】，填写本级节点名称和本级通讯地址等。填写完成后，上级节点会接受到审批请求，点击审批通过，即级联成功。

级联成功后，则在级联管理-级联配置-下级管理节点页签中能够查询到下级节点的管理平台信息。

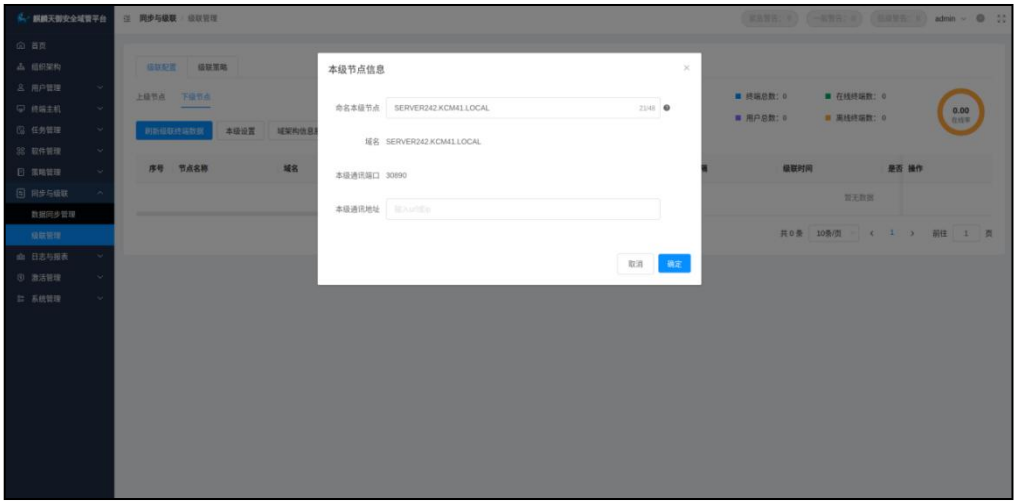

图 10-6 本级节点信息界面

管理下级平台的策略

级联管理-级联策略支持按节点下发平台的策略。在上级平台中，能够对下级平台的策略进行管理。

图 10-7 新建策略组界面

说明：来自上级平台的策略优先级会高于本平台自行配置的策略。

11 日志与报表

日志与报表模块记录了用户日志、终端日志、平台操作日志、接口日志和终端异常日志等审计信息，支持日志采集和导出。

11.1 用户日志

用户日志以用户维度记录域用户登录和登出等审计信息。

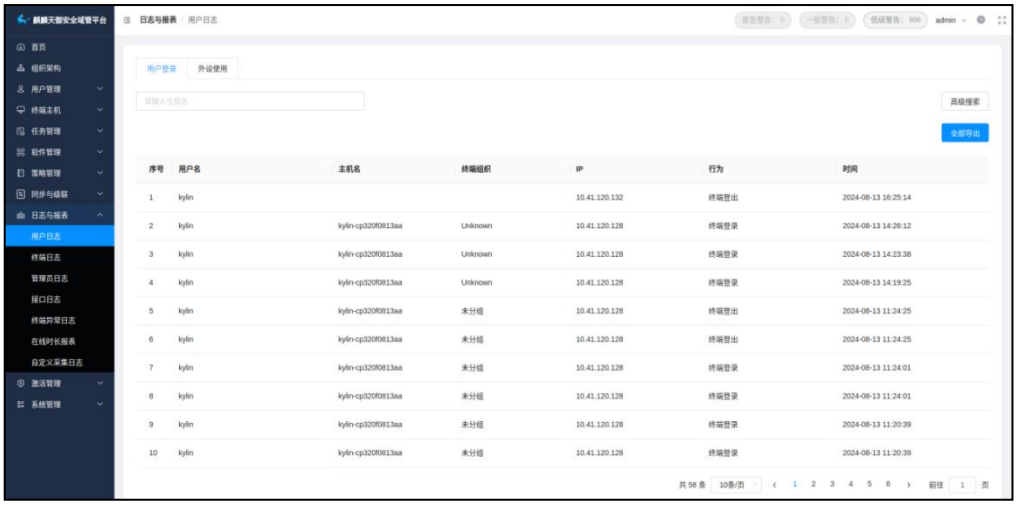

图 11-1 用户日志界面

外设使用日志以设备维度记录外设使用记录等审计信息。

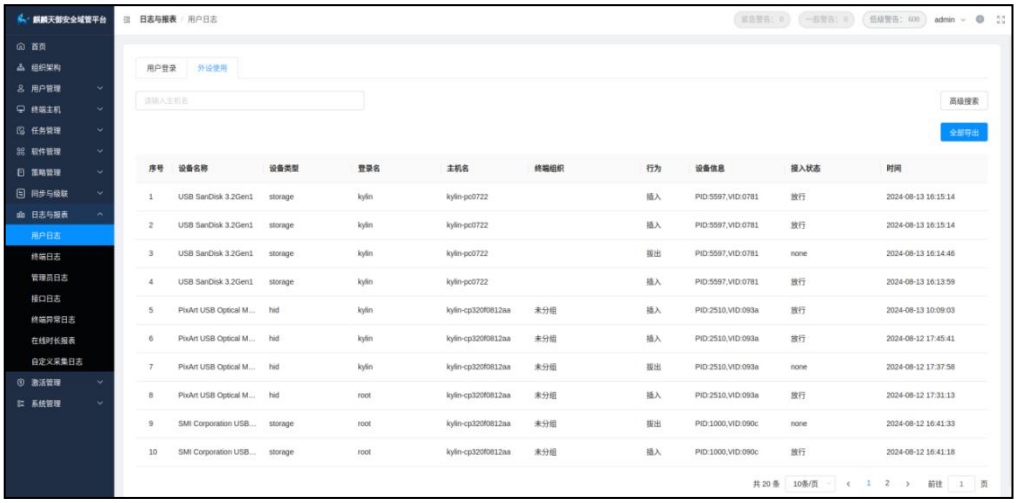

图 11-2 外设使用界面

11.2 终端日志

终端日志，记录终端主机行为、更新升级、关键进程监控和加域退域等审计信息。

终端主机行为审计日志，包括：终端维度用户登录、登出和软件卸载等。

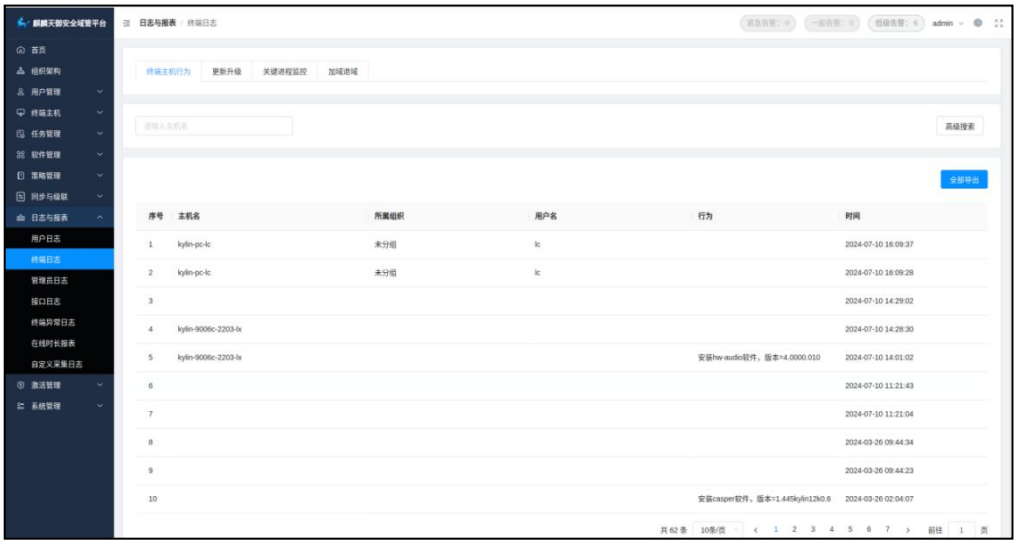

图 11-3 终端主机行为界面

更新升级审计日志，包括：终端补丁安装更新等审计信息。

关键进程监控审计日志，包括：进程信息和进程状态等审计记录。

加域退域审计日志，包括：终端加域、退域和登录账户等信息。

11.3 管理员日志

管理员日志，包括：平台管理员具体操作和远程协助审计信息。

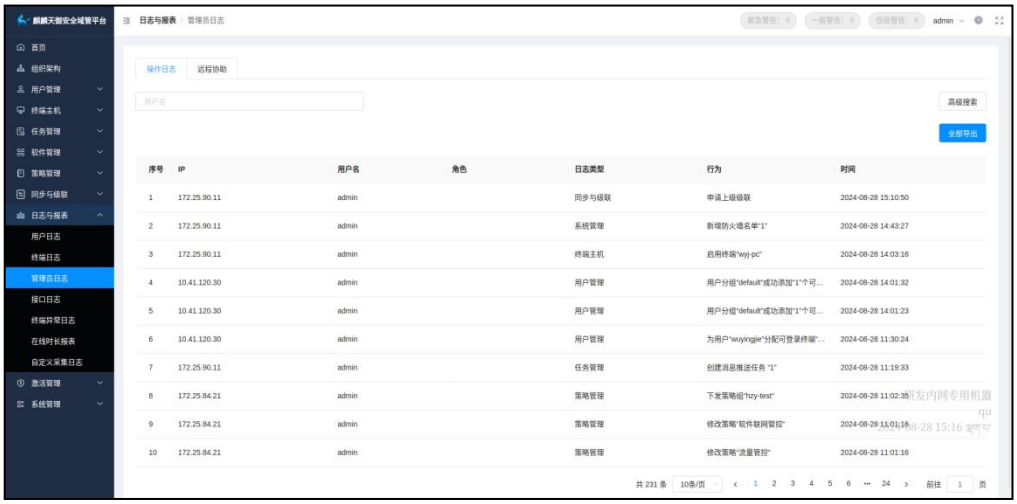

图 11-4 管理员日志界面

11.4 接口日志

接口日志，记录了本平台与外部平台对接过程中的数据传输记录，包括：LDAP 数据同步和 Syslog 日志外发等。

LDAP 对接日志，包括：数据同步模块的用户信息、组织信息和用户组信息等。

图 11-5 LDAP 对接日志界面

syslog 外发日志，包括：用户登录、外设使用、主机行为、更新升级、关键进程、加域退域和告警等状态信息。

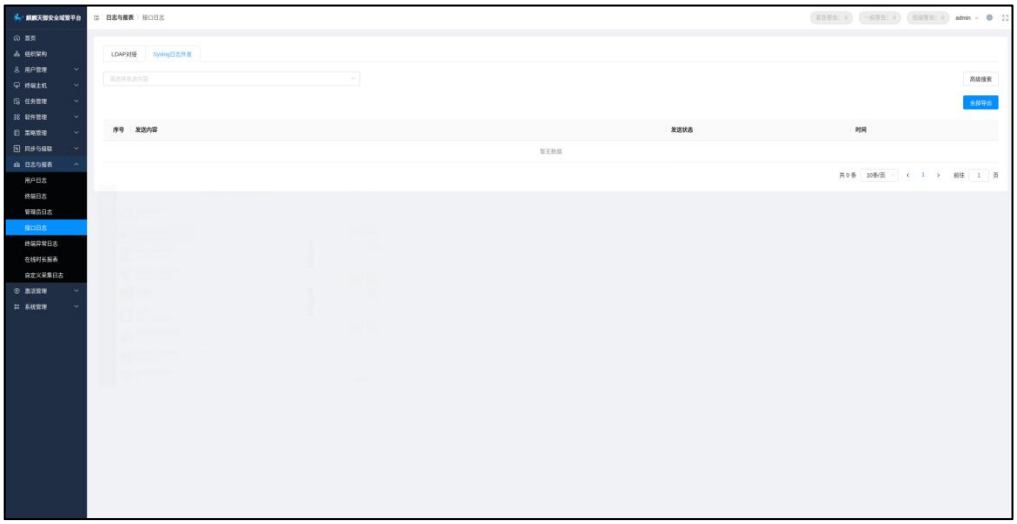

图 11-6 Syslog 外发日志界面

11.5 终端异常日志

终端异常日志，包括：策略管控异常行为和硬件指标异常审计事件。

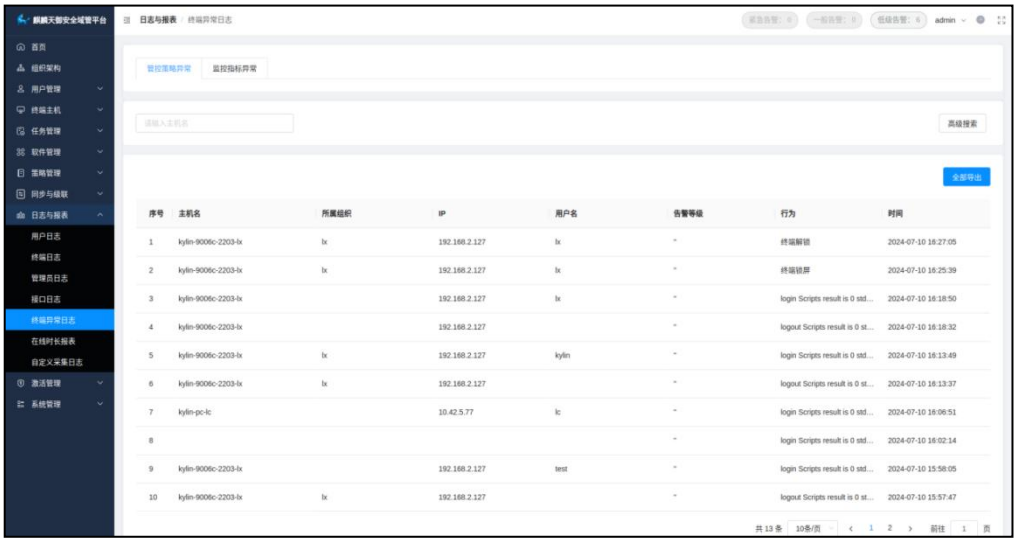

图 11-7 终端异常日志界面

管控策略异常日志，包括：终端策略执行、信息同步和更新等异常情况审计。

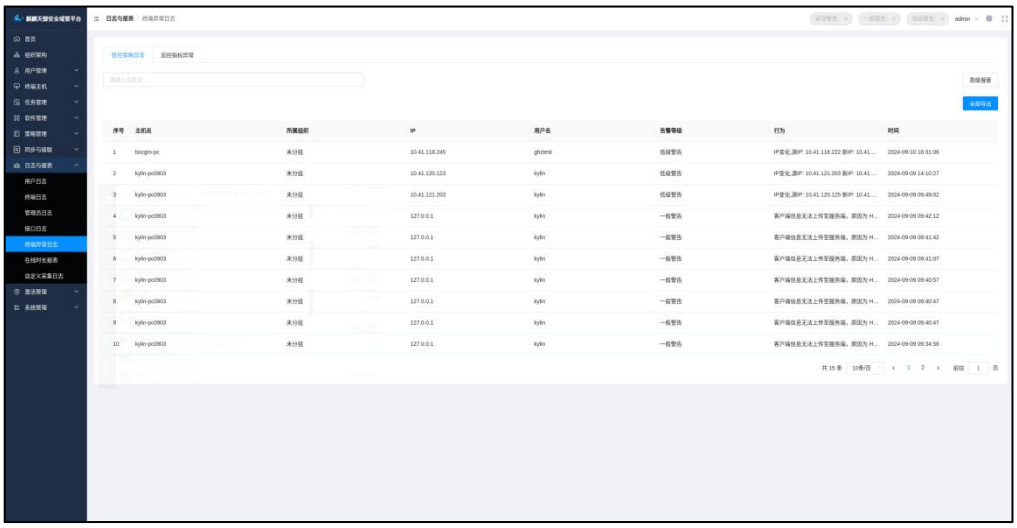

图 11-8 终端管控策略异常日志界面

监控指标日志，包括：CPU 占用、硬盘占用和内存占用等阈值监控预警审计。

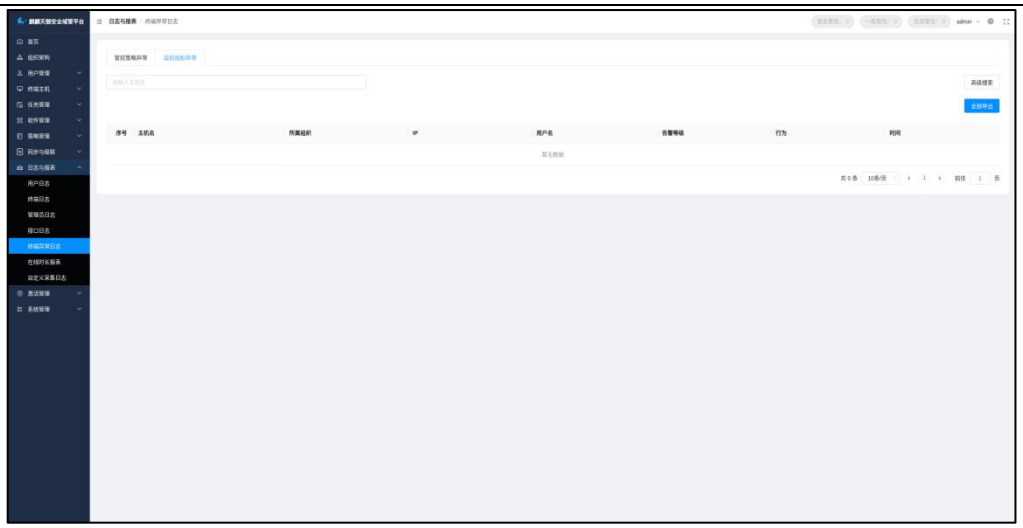

图 11-9 终端监控指标异常日志界面

11.6 在线时长日志

在线时长报表以用户与终端维度统计组织中设备与用户的在线时长。

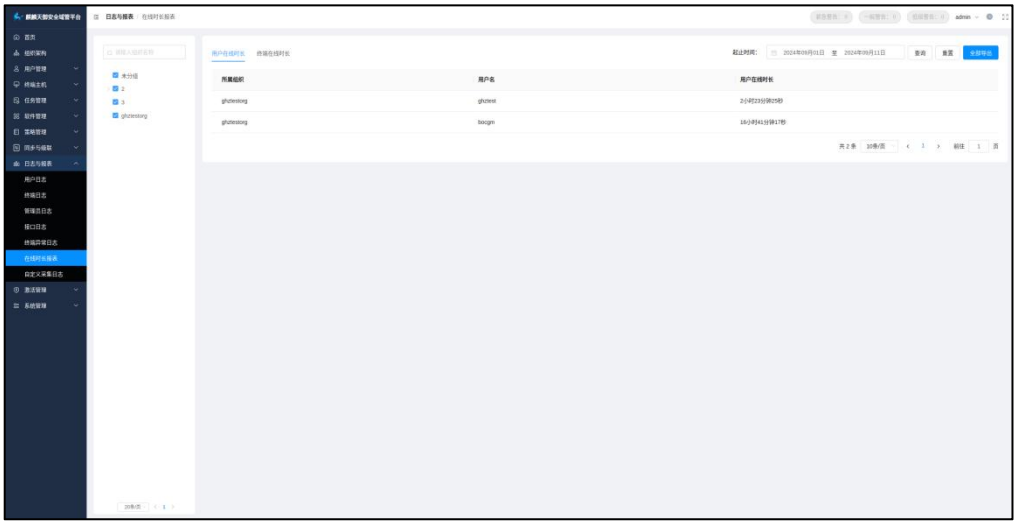

图 11-10 用户在线市场报表界面

11.7 自定义采集日志

支持管理员自定义采集日志信息，输入完整日志文件路径即可采集。

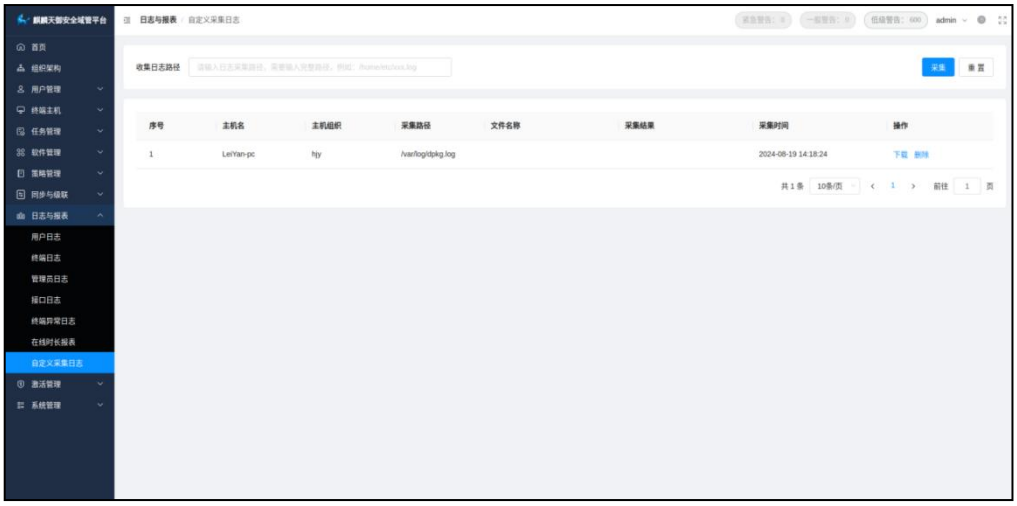

图 11-11 自定义采集日志界面

12 激活管理

该模块支持对终端操作系统进行批量激活。当终端加域成功后，在该模块能够查询到终端系统的激活状态，对于未激活的终端操作系统，支持通过该模块进行批量激活。

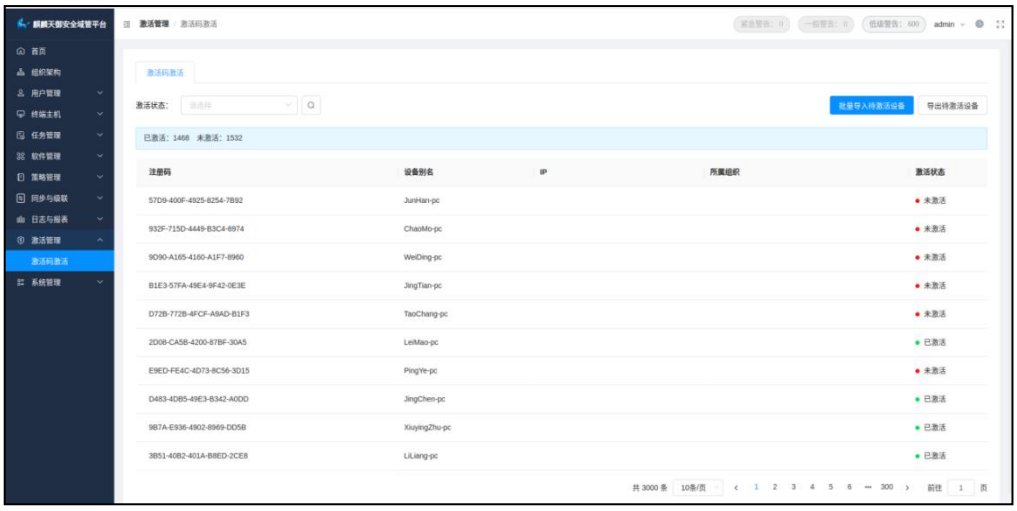

图 12-1 激活码激活界面

激活步骤：导出待激活设备列表-联系销售申请激活码-批量导入激活码-激活状态更新。

13 系统管理

13.1 授权管理

该页面展示平台的授权信息，支持对授权文件的导入和导出。

图 13-1 授权管理界面

点击【上传授权文件】按钮，替换当前授权。

点击【下载授权文件】按钮，将当前授权下载到本地。

13.2 服务端备份管理

该模块支持对麒麟天御安全域管平台服务端数据进行备份。

注：备份期间，后台数据会短暂为只读状态，备份结束后恢复，请谨慎操作。

手动备份：点击【立即备份】按钮，填写备份备注，即进行手动备份。

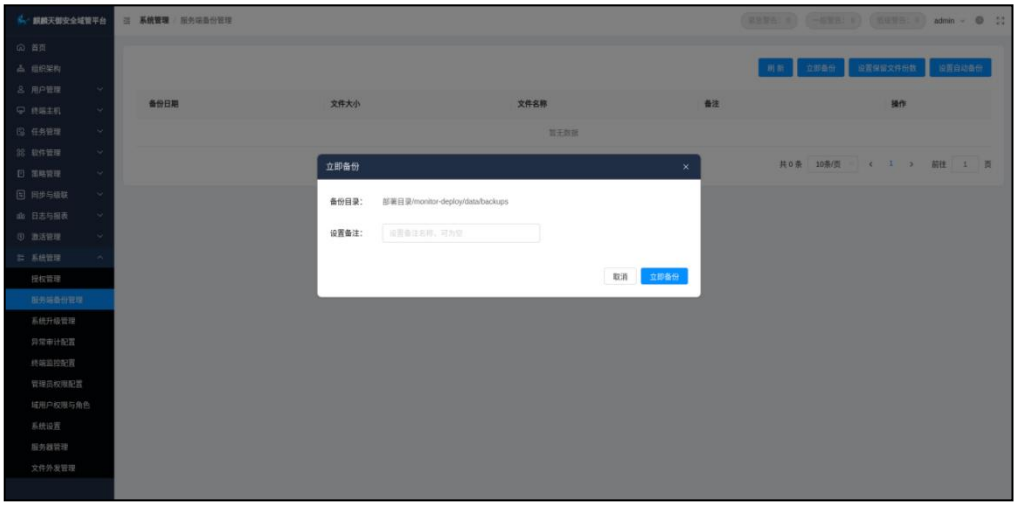

图 13-2 立即备份界面

自动备份：点击设置自动备份，填写自动备份的时间，即可进行自动备份。

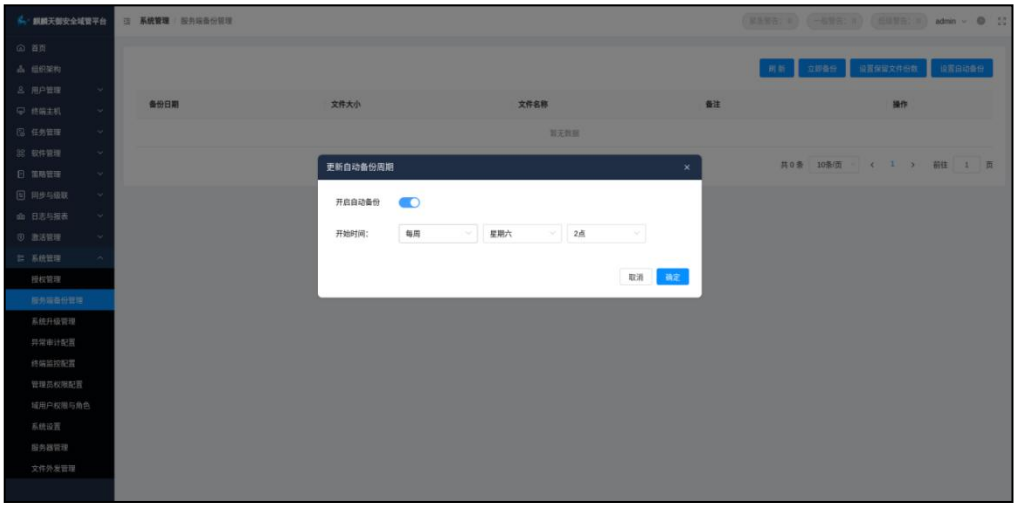

图 13-3 自动备份周期配置界面

设置备份文件份数：点击【设置文件保留份数】按钮，支持设置备份文件的保留份数。

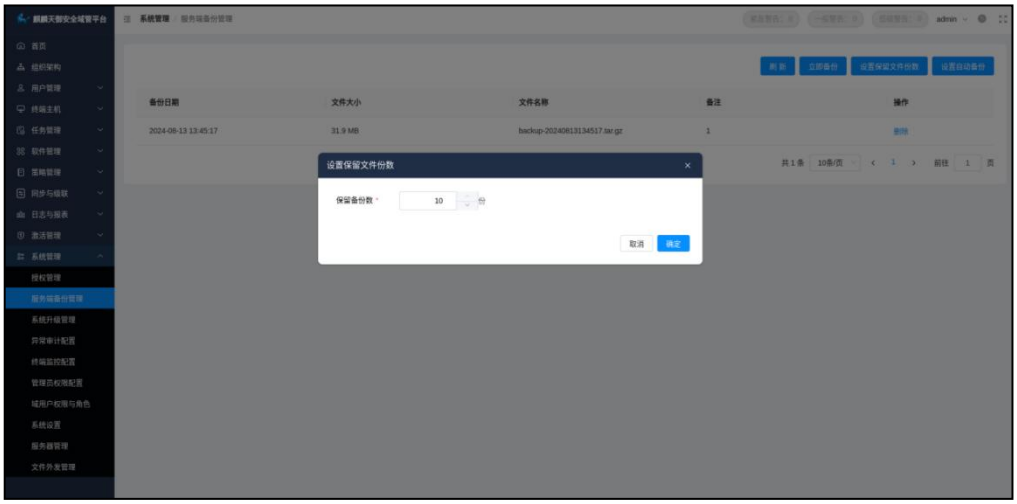

图 13-4 设置保留文件份数界面

13.3 系统升级管理

支持自动化升级域控组件，同时支持版本回滚和取消升级。

详细记录后台版本升级、升级结果和版本回滚日志。

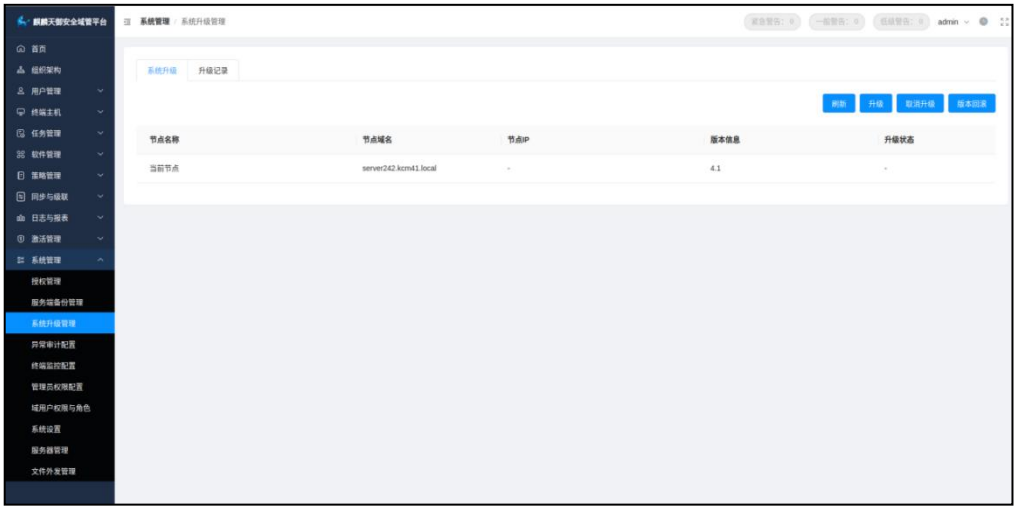

图 13-5 系统升级管理界面

13.4 异常审计配置

管理员可自定义配置终端硬件监控阈值，当使用率超过阈值时，在终端异常日志中生成监控指标异常日志。

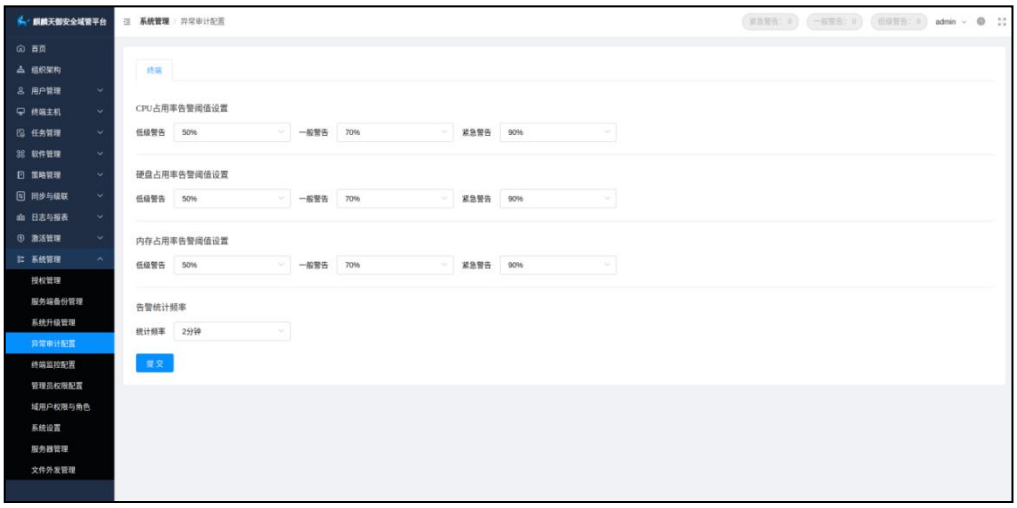

图 13-6 异常审计配置界面

13.5 终端监控配置

该模块支持对终端运行的关键进程进行监控与保护。

进程监控：添加进程名称，则对终端上的该进程运行情况进行监控。

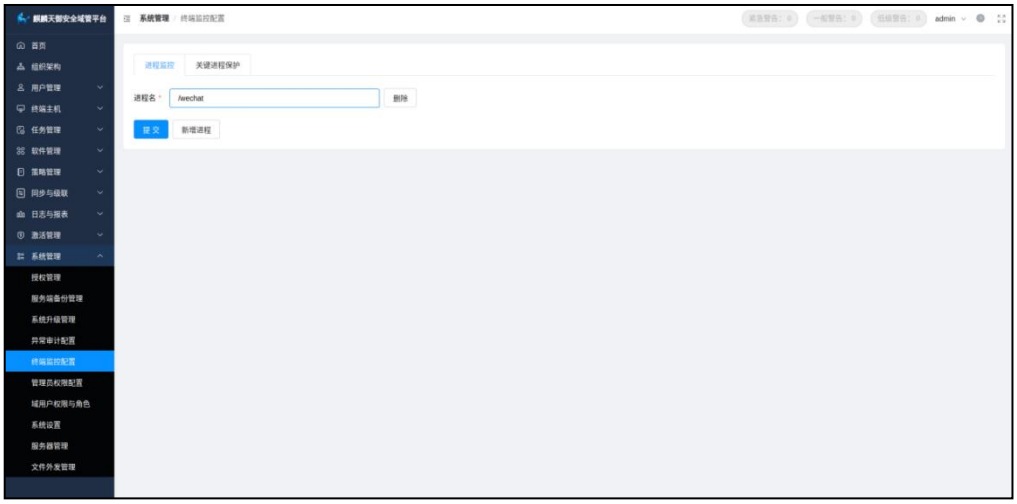

图 13-7 终端监控配置界面

关键进程保护：对终端上运行的进程进行保护，防止进程被意外杀死。

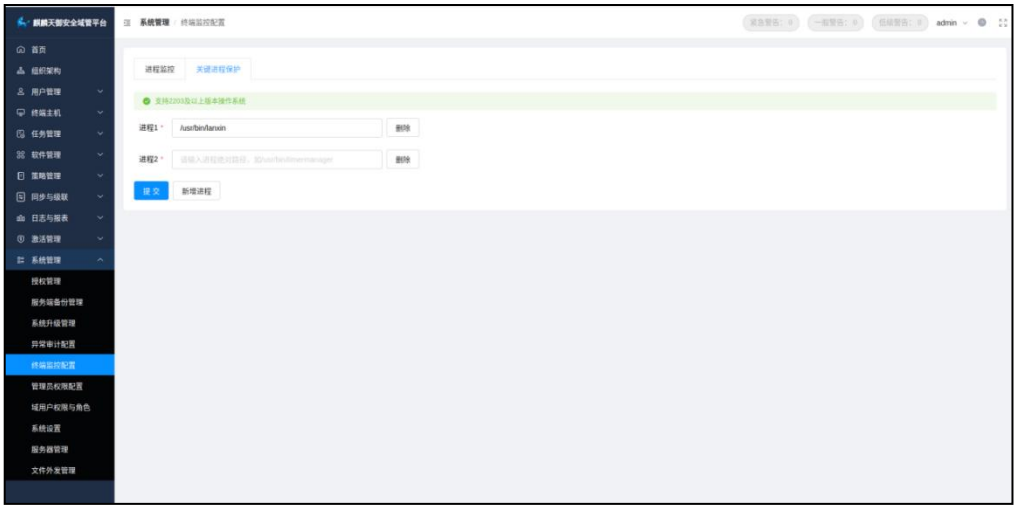

图 13-8 关键进程保护界面

13.6 管理员权限配置

该模块为平台管理员账号与管理员角色权限配置模块。

角色与权限

该模块支持创建平台管理角色，超级管理员 admin 根据业务需求，为不同业务场景创建不同的平台管理权限。

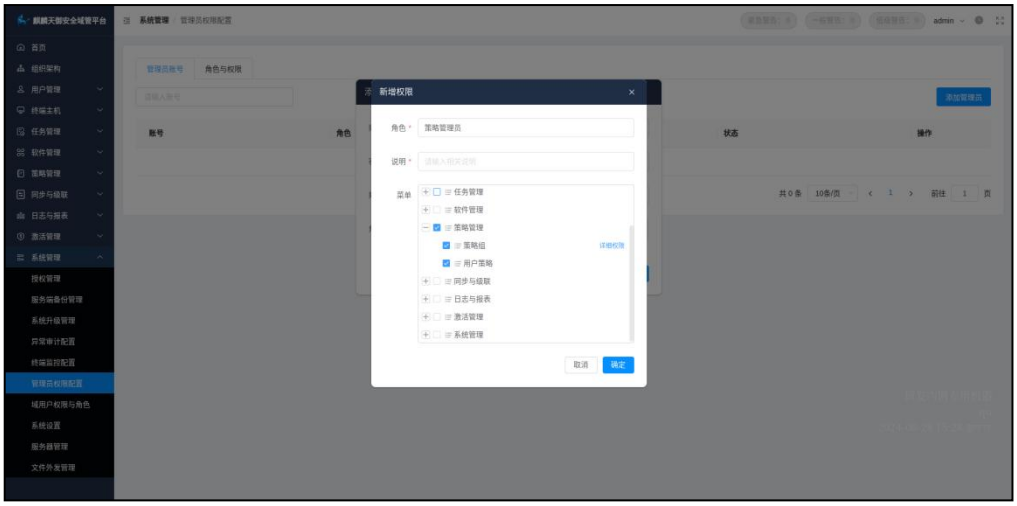

图 13-9 配置平台管理权限界面

选择菜单，点击详细权限，支持配置页面按钮级别操作权限。

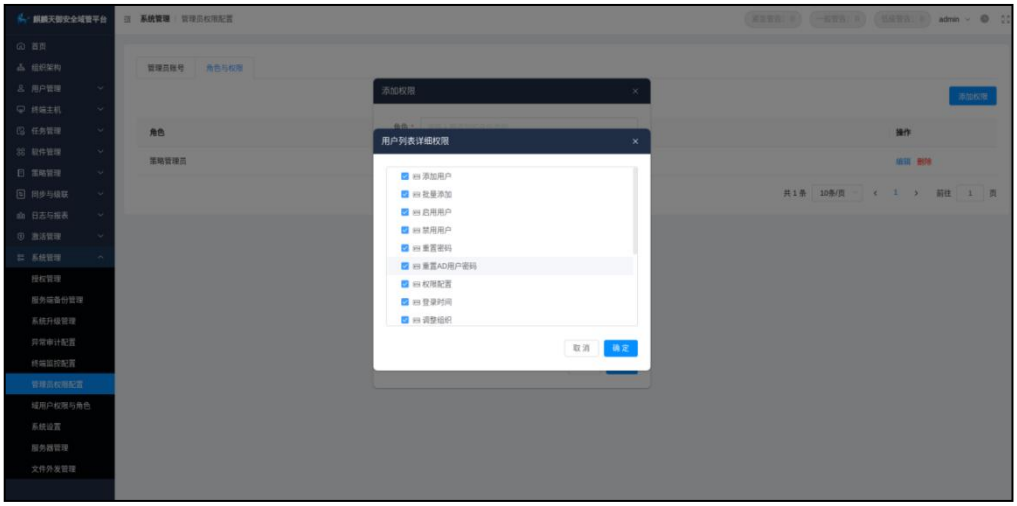

图 13-10 配置角色详细权限界面

管理员账号

管理员角色创建完成后，可进行管理员账号的创建。

创建管理员账号时，需要输入新管理员的账号登录名，密码，姓名，角色，和配置可管理的组织。

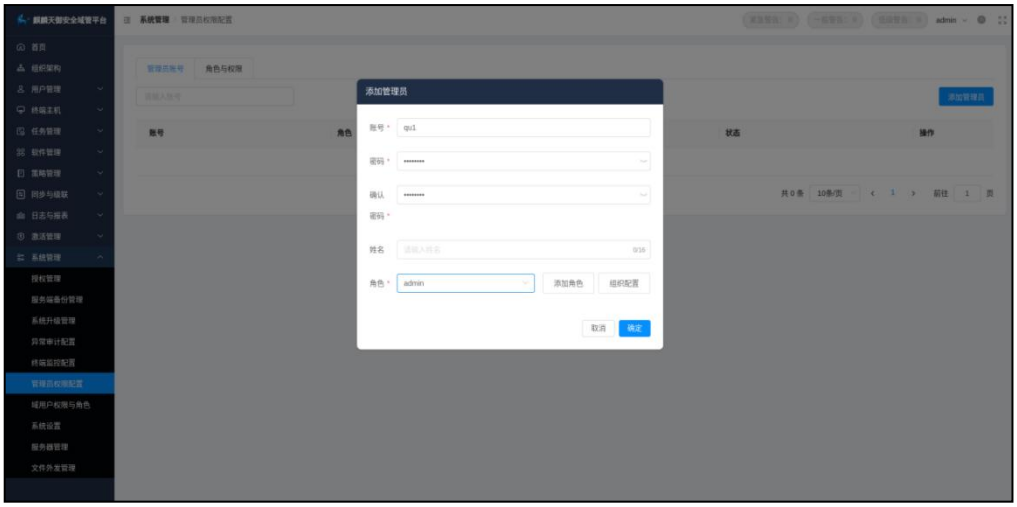

图 13-11 创建平台管理员界面

管理员账户创建完成后，使用新账号进行登录，按照角色权限进行系统管理。如下为管理员配置策略管理权限，则管理员登录后仅能进行策略管理相关操作。

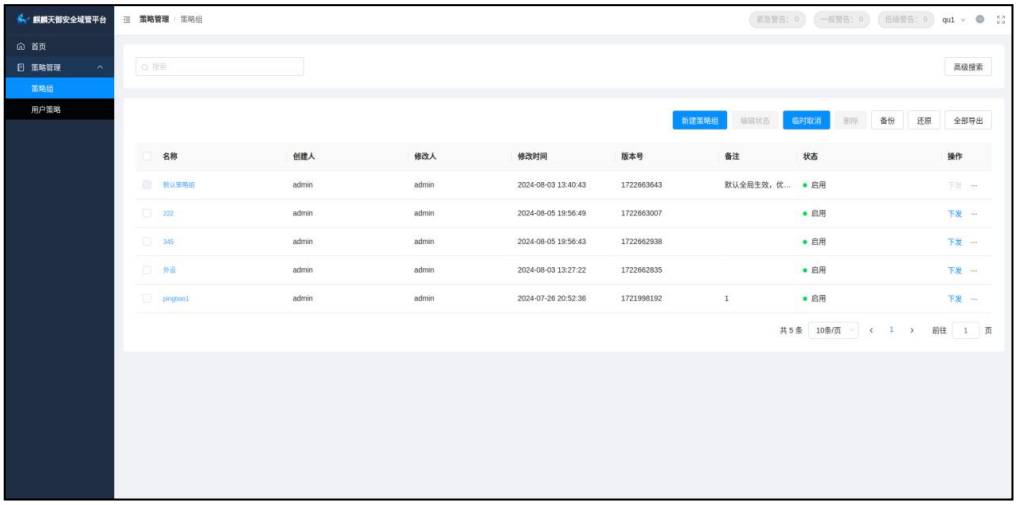

图 13-12 策略管理界面

13.7 域用户权限与角色

该模块支持对域账户的权限进行配置。默认情况下，域账户执行的命令与访问的功能受限。支持对域账户进行特殊权限配置，满足用户不同业务的资源访问控制需求。

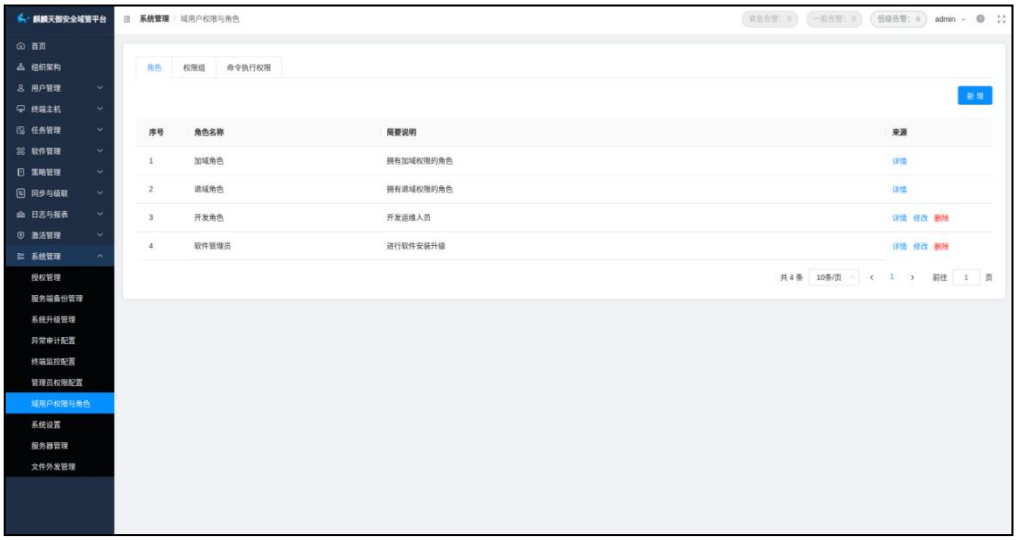

图 13-13 域用户权限与角色界面

命令执行权限

命令执行权限模块支持添加终端执行的具体命令，如 vim，ifconfig 等。

点击【新增】按钮，支持添加命令。

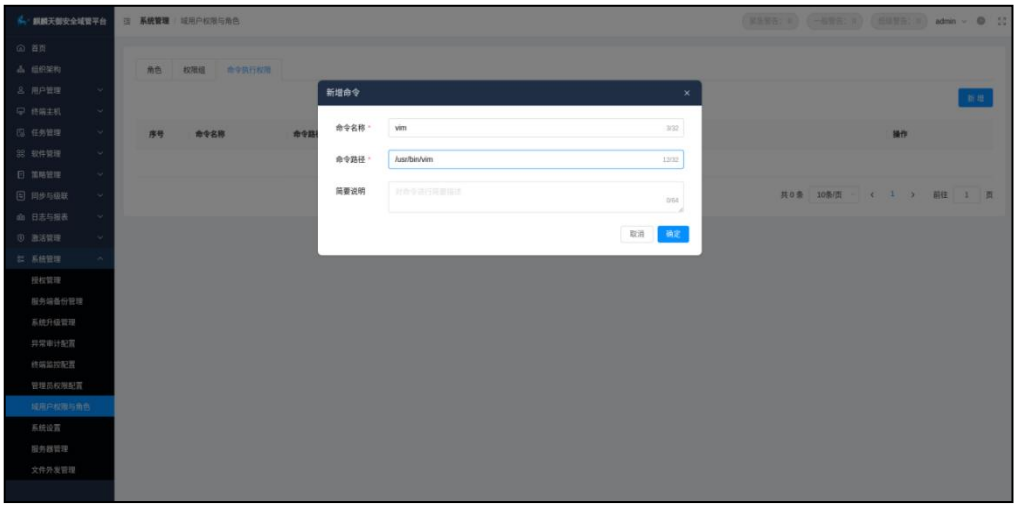

图 13-14 命令执行权限配置界面

权限组

该模块是域账户在终端操作系统上的权限配置。默认情况下，域账户对于终端操作系统上的配置修改是受限的，如网络配置模块、打印机和软件安装等。通过权限组，使得域账户具备配置的权限。

添加权限组：点击新增，配置权限组的名称，勾选该权限组中允许执行的命

令。

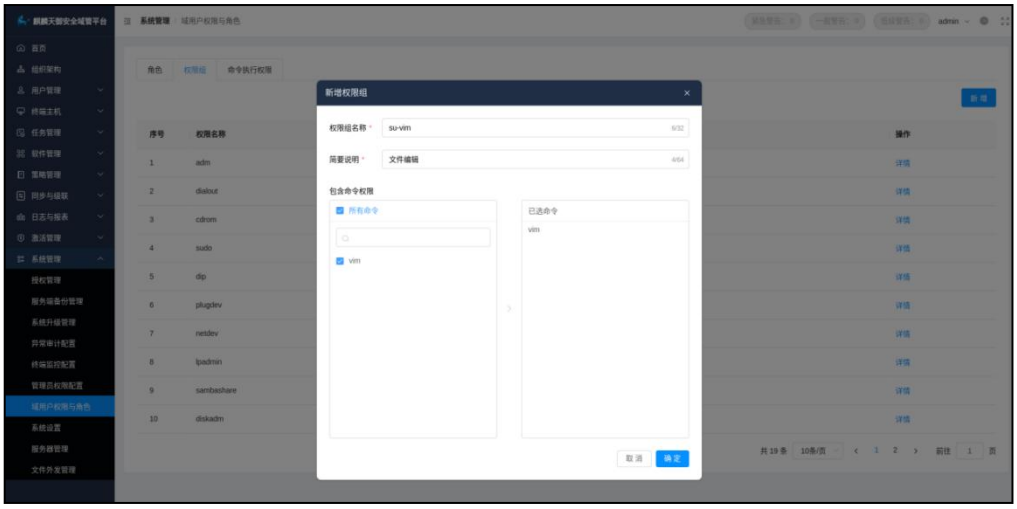

图 13-15 添加权限组界面

角色

通过配置基本的命令执行权限和权限组，并将其关联到角色，可以为域账户分配角色。系统默认内置了“加域”和“退域”角色。

新增角色：点击新增，输入角色名称与说明，并勾选对应的权限组。

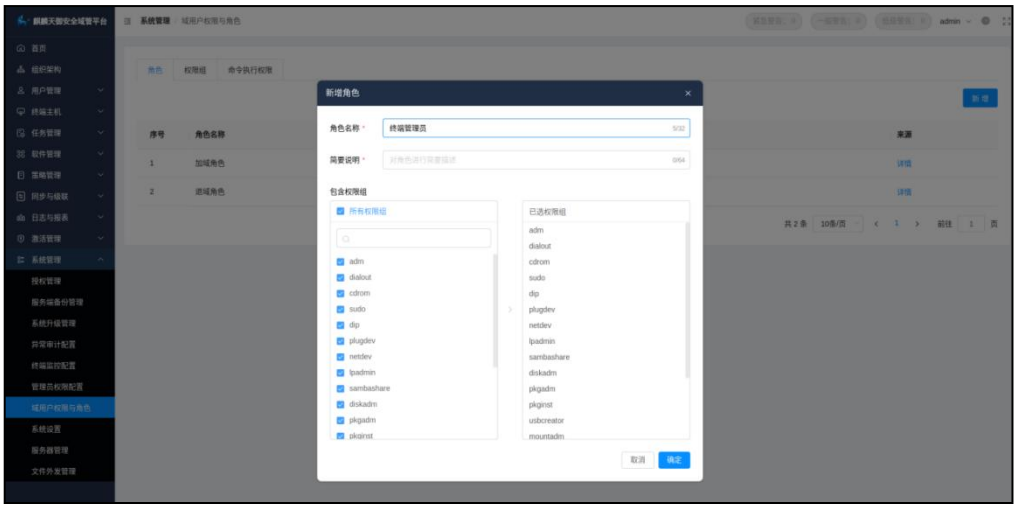

图 13-16 新增角色界面

给用户组分配权限流程

用户分组-勾选分组-权限配置-勾选角色-赋予权限。

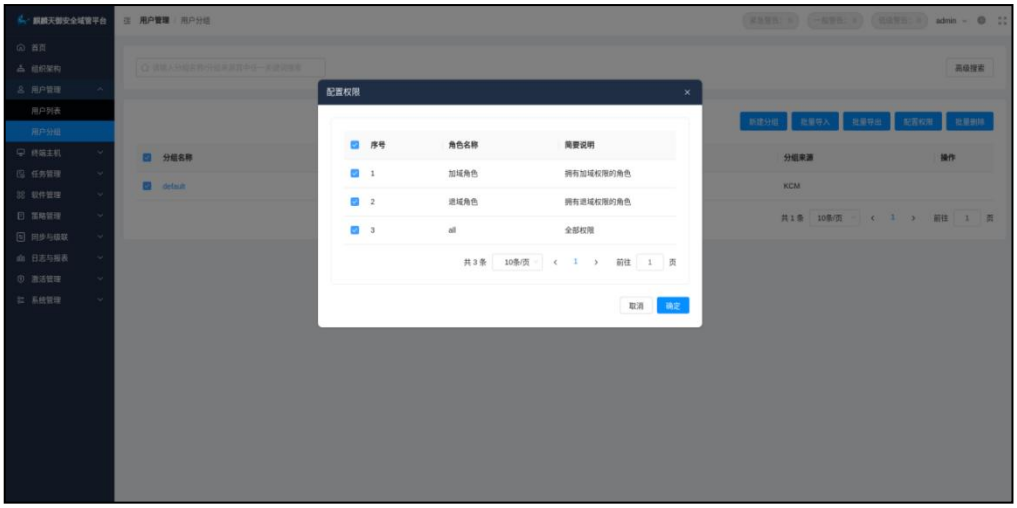

图 13-17 域用户分组配置权限界面

给用户分配权限

用户列表-勾选用户-权限配置-勾选角色-赋予权限。

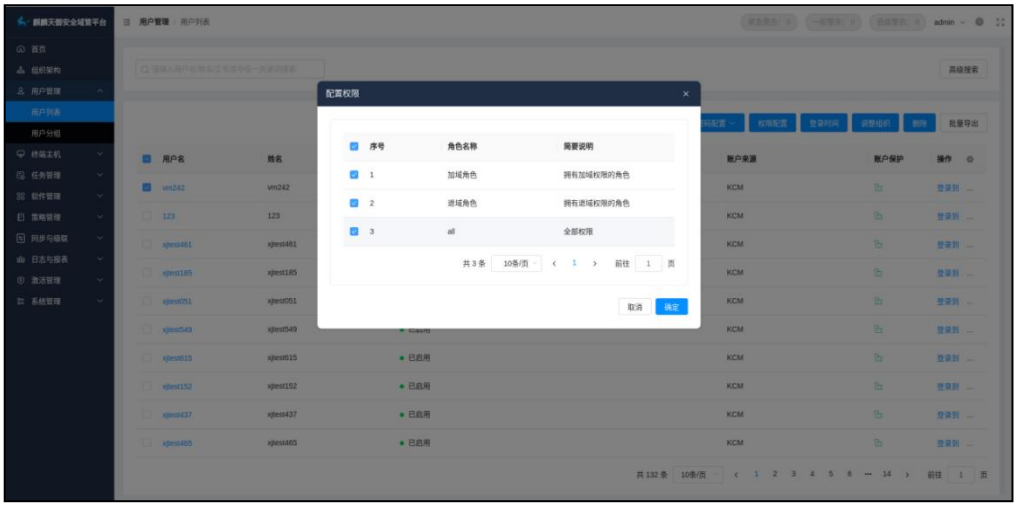

图 13-18 域用户配置权限界面

13.8 系统设置

系统设置模块支持对平台的基础信息进行配置。

支持的配置内容包括：LOGO 替换、平台名称修改、NTP 地址设置、心跳设置、离线登录有效期设置和加域设置等。

图 13-19 系统设置界面

平台名称修改：最大支持 16 个字符。

NTP 地址设置：桌面系统连接的 NTP 服务端地址，不填写则保持桌面系统默认的设置，可按需修改为域控服务端的 IP 或域名。

心跳设置：终端与服务端通信的时间间隔，最低 30 秒，可按需设置。触发心跳时，终端会向服务端上报状态、同步信息并更新策略。

离线登录有效期：终端与服务端通信异常后，曾经在该终端登录过的域账户可以继续登录的时间。

加域设置

支持设置是否赋予域用户加域权限、是否赋予域用户退域权限、终端关联组织方式、账户加域次数、域名后缀和服务端退域有效期。

终端关联组织方式：终端加域后，该终端进入组织时匹配的规则。

手动关联：使用域账户 A 对终端加域后，该终端不进入任何组织，需手动加入组织。

按加域用户所在组织关联：使用域账户 A 对终端加域后，该终端进入与 A 相同的组织。

按组织 IP 匹配规则关联：在组织管理中，支持设置组织的 IP 匹配规则，如果终端的 IP 地址与该规则匹配，则终端加域后进入到对应的组织。

按组织字符匹配规则关联：在组织管理中，支持设置组织字符匹配规则，如

果终端的主机名与该规则匹配，则终端加域后进入到对应的组织。

策略名单配置

该类名单为在下发策略时，支持调用的自定义名单。包括 BSSID 名单、MAC 名单、软件名单、防火墙名单和外设名单等。

BSSID 名单：支持在网络管控-WiFi 管控黑白名单处进行下发。

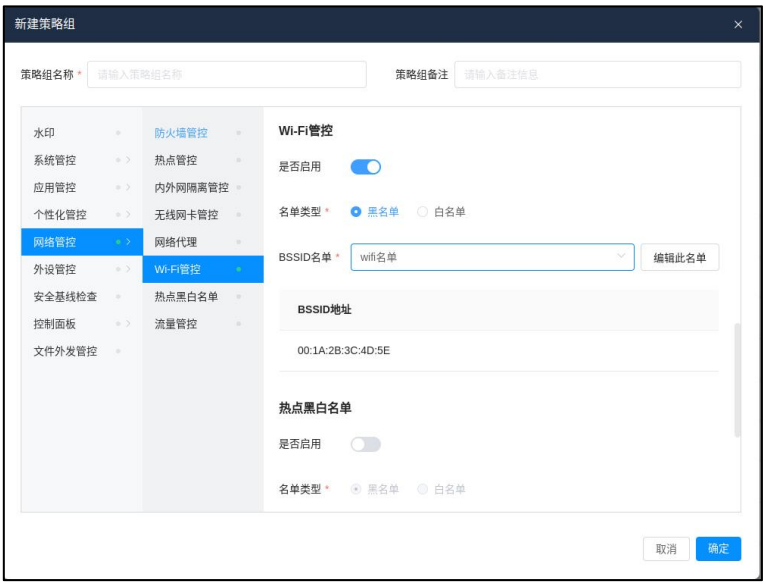

图 13-20 Wifi 管控策略项配置界面

MAC 名单：支持在网络管控-热点黑白名单处进行下发。

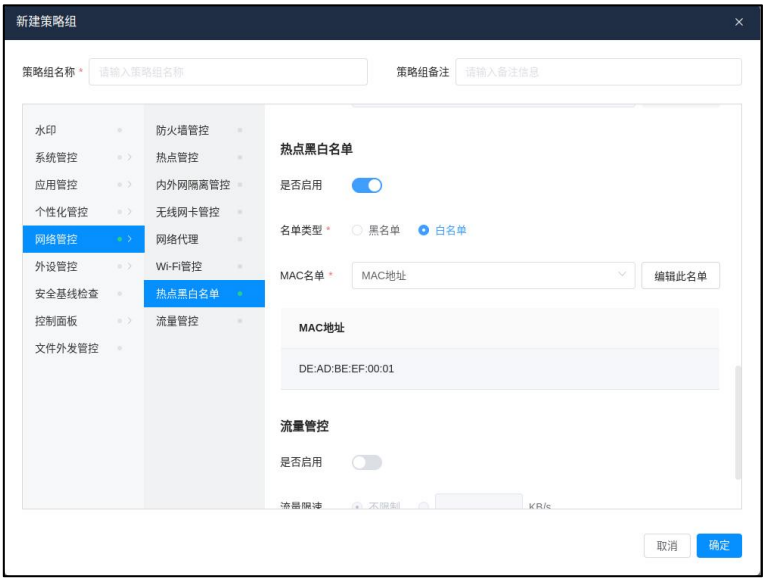

图 13-21 热点黑白名单策略项配置界面

软件名单：支持在软件运行限制、软件联网管控和软件防卸载管控处进行下发。

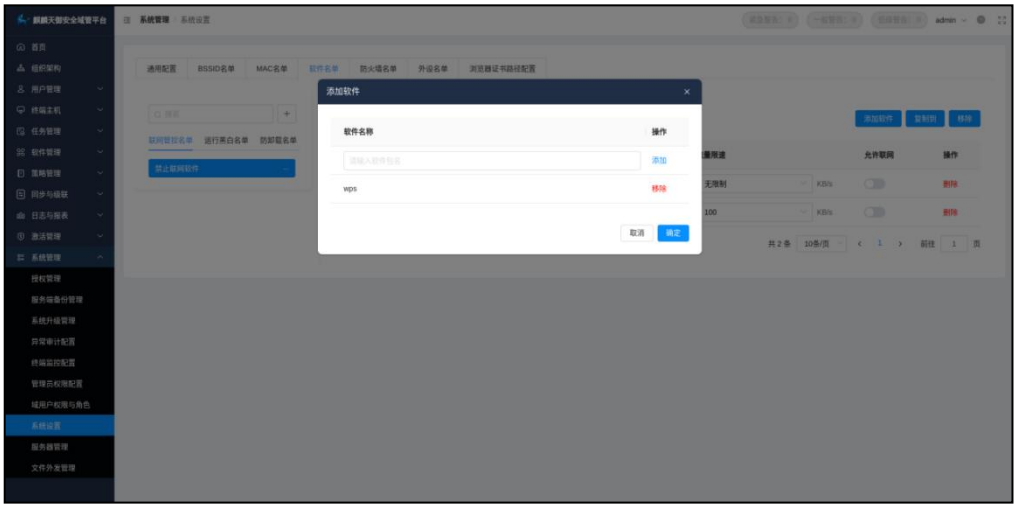

图 13-22 软件名单配置界面

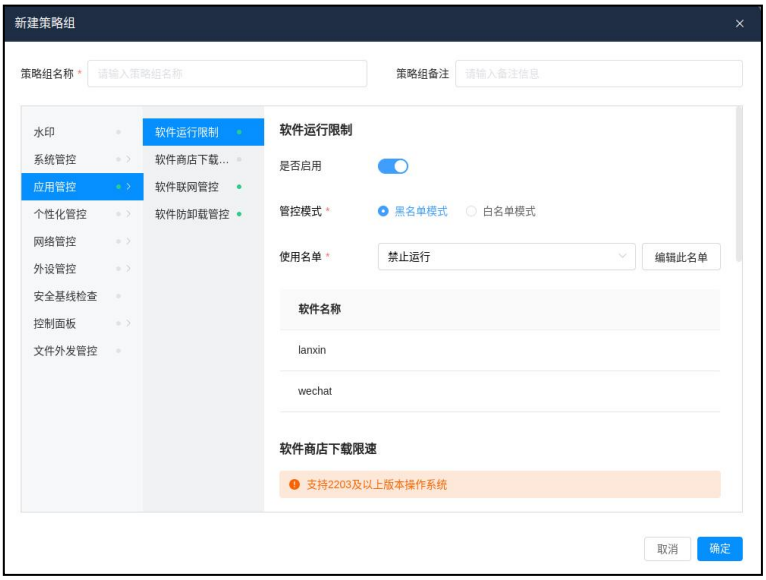

图 13-23 软件运行限制策略项配置界面

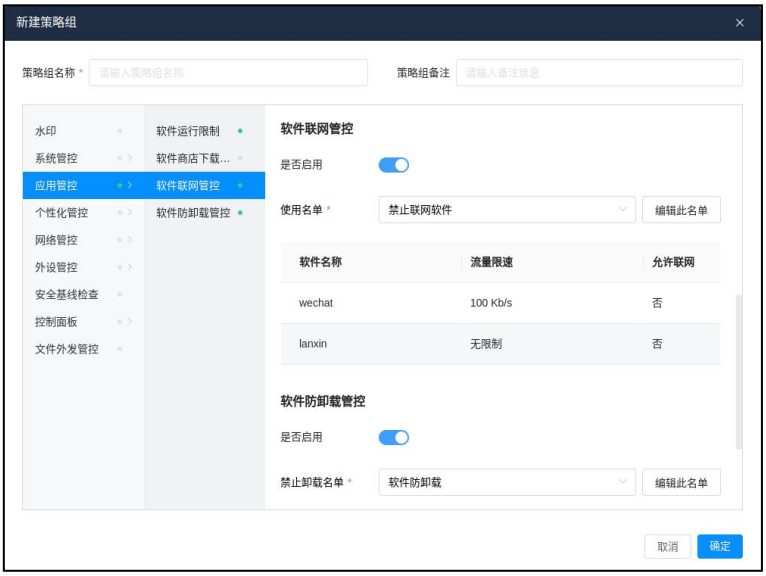

图 13-24 软件联网管控策略项配置界面

防火墙名单：支持在网络管控-防火墙管控处进行下发。

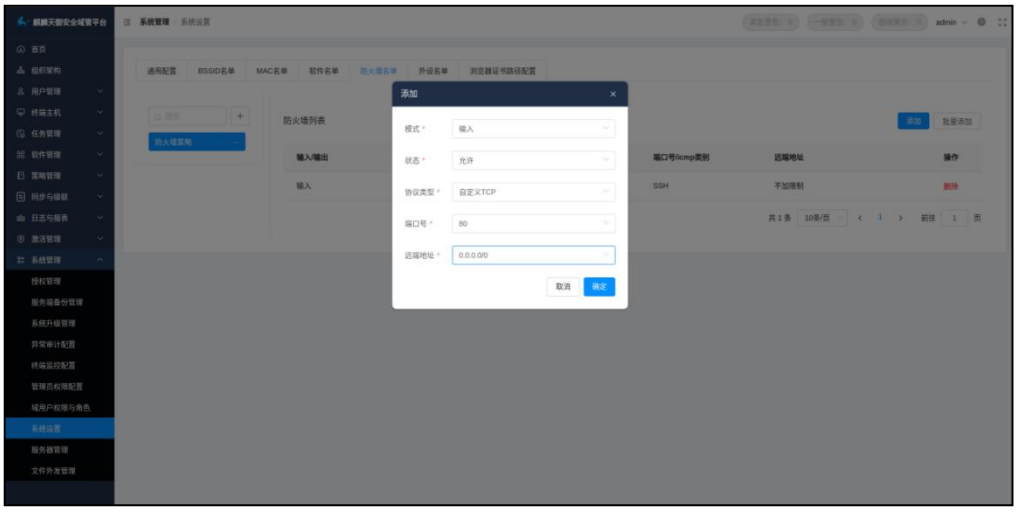

图 13-25 防火墙列表配置界面

图 13-26 防火墙管控策略配置界面

外设名单：支持在外设管控-外设黑白名单处进行下发。

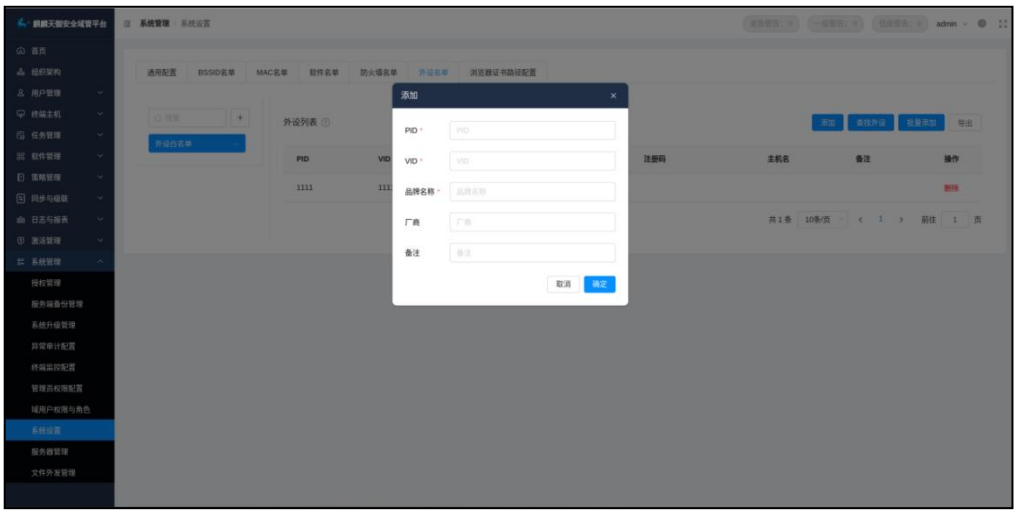

图 13-27 外设名单配置界面

图 13-28 外设黑白名单策略项配置界面

支持浏览器证书下发配置。点击【新增】，输入浏览器名称与证书路径。

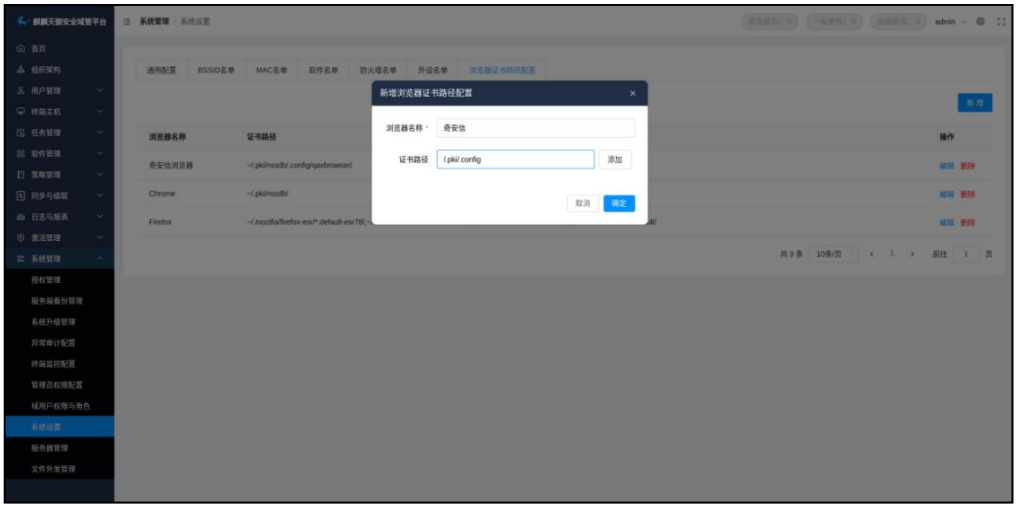

图 13-29 浏览器证书路径配置界面

13.8 服务器管理

该模块支持 NTP、DNS、DHCP 等服务配置管理。

NTP 设置：支持设置上级域名或 IP，在设置完成后可进行连接测试。支持限制允许连接网段，仅在该网段内可正常连接。另外，提供 nomodify、noquery、notrap、notrust、nopeer 等通用 NTP 设置。

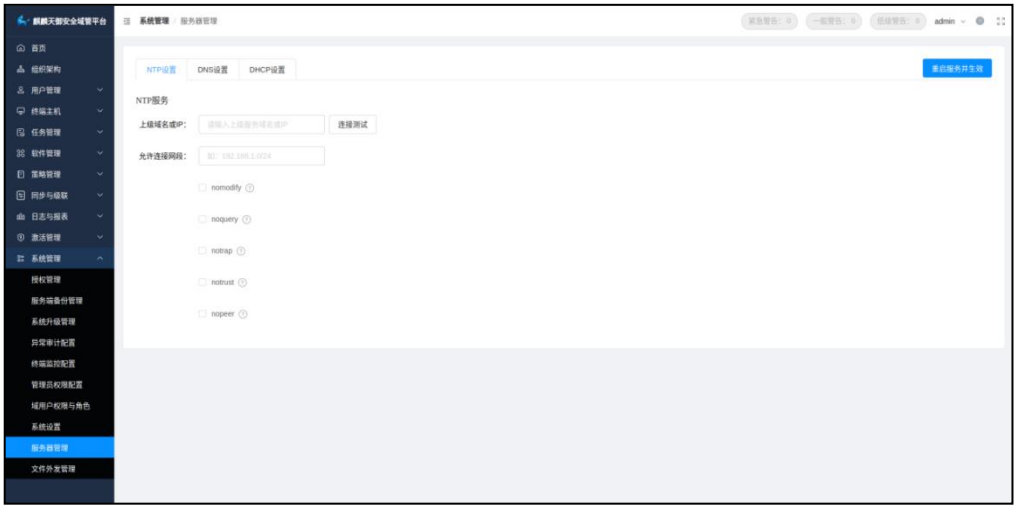

图 13-30 服务器管理界面

DNS 设置：支持新建正向区域、反向区域、条件转发 DNS 服务。

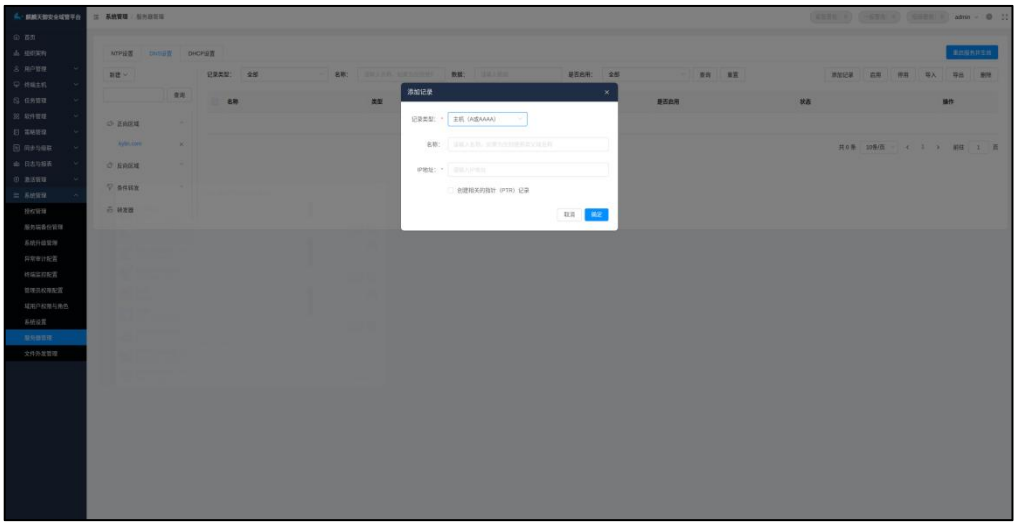

图 13-31 DNS 设置界面

DHCP 设置：支持新建并配置 DHCP 服务。支持单个 DHCP 服务重启、mac-ip 绑定配置、添加子网、全局设置。

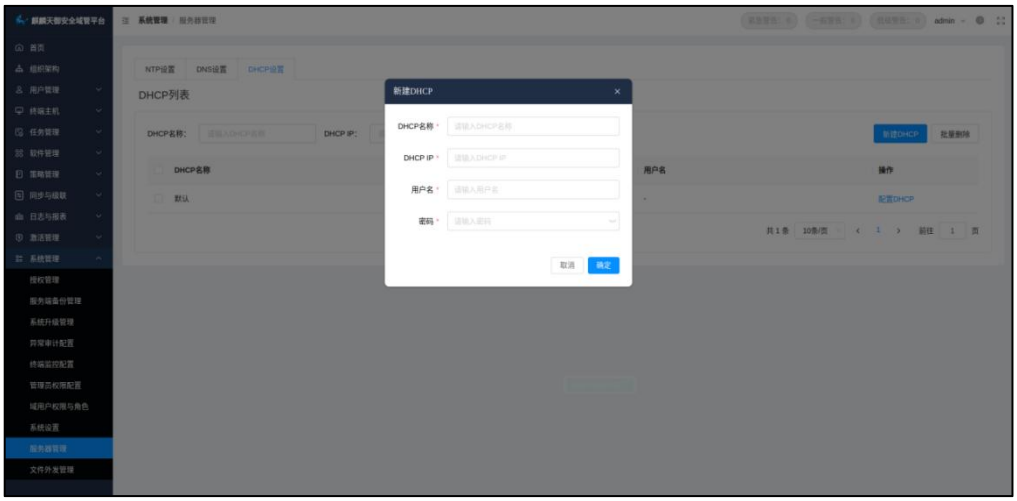

图 13-32 DHCP 设置界面

13.9 文件外发管理

当策略下发启用文件外发管控策略后，可在文件外发管理进行外发审批，只有审批通过的申请用户才能进行文件外发。

终端发起文件外发申请，记录并上报文件名称、申请人、主机名、外发类型、申请时间、失效时间。管理员可对单个文件外发申请事件进行审批，可查看已审批、已失效文件外发申请事件。

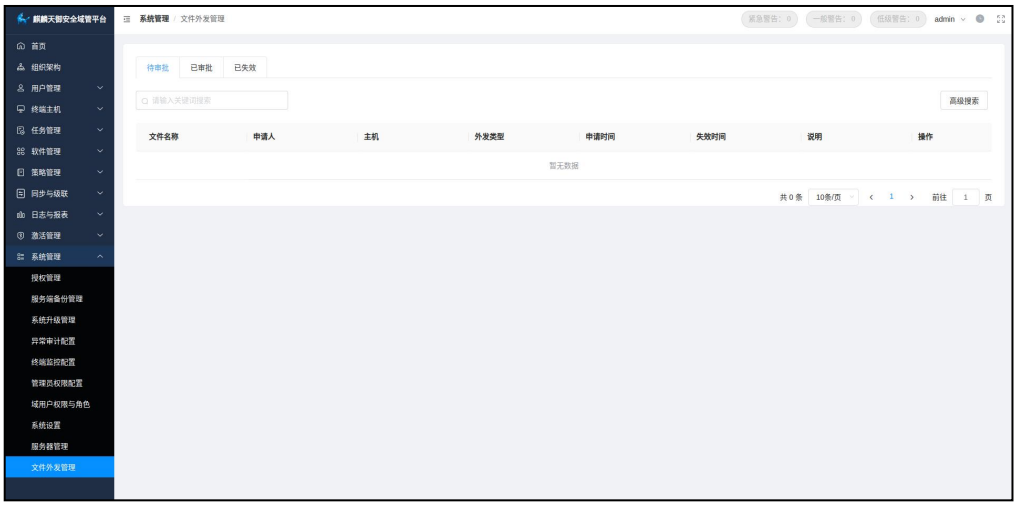

图 13-33 文件外发管理界面