安恒信息
DAS-security 安全中国

AiLPHA 安全编排与协同响应管理平台

用户手册

目 录

前言

感谢您选择安恒信息的网络安全产品。本手册对安恒信息 AiLPHA SOAR 安全编排与协同响应管理平台(以下简称“AiLPHA SOAR 平台”）进行了简单介绍，并对平台的使用方法进行了详细描述。主要包括产品简介、用户登录/登出、快速入门、安全运营、任务管理、场景编排、系统管理、能力中心和用户权限管理。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于使用平台的人员，包括管理员、安全分析员、设备管理员、安全编排员。本文假设读者对以下领域的知识有一定了解：

- TCP/IP、SNMP、Syslog、HTTP、FTP、NFS、Samba 等基础网络通讯协议
- 数据库、服务器、网络安全设备、路由器、交换机等常见设备（系统）的基本工作原理和配置
- 网络安全相关知识，包括 DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段
- Syslog 协议的基本工作原理和配置

格式约定

本手册内容格式约定如下：

内容	说明
粗体字	Web 界面上的各类控件名称以及内容。例如：“在菜单栏中选择系统状态进入系统状态页面，选择接口状态页签”。
< >	Web 界面上的按钮。例如：“微信认证失败，点击<我要上网>不弹出微信认证界面”。
➤	介绍 Web 界面的操作步骤时，用于隔离点击对象（菜单项、子菜单、按钮以及链接等），例如：“在菜单栏选择‘策略配置➤认证管理➤认证策略’查看是否开启了认证策略”。

本手册图标格式约定如下：

图标	说明
	提示，操作小窍门，方便用户解决问题。
	说明，对正文内容的补充和说明。
	注意，提醒操作中的注意事项，不当的操作可能会导致设备损坏或者数据丢失。
	警告，该图标后的内容需引起格外重视，否则可能导致人身伤害。

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 https://bbs.dbappsecurity.com.cn 获取更多文档。

联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310052

电话：0571-88380999

传真：0571-28863666

官网：http://www.dbappsecurity.com.cn

邮箱：400-doc@dbappsecurity.com.cn

1. 产品简介

1.1 产品概述

AiLPHA 安全编排与协同响应管理平台结合专业的安全经验，依托雄厚的研发实力，兼顾未来业务的发展，重点解决了传统的安全运维及事件处置中“安全事件和威胁风险剧增、人力不足且经验难以固化、设备孤立且技术整合度低、突发状况处置慌乱难协作”的几大痛点。在日常安全运营的过程中，平台可与工控、能源、金融、科信等行业的安全平台或设备进行联动响应，通过剧本编排与自动化响应、在线协同作战等方式，极大降低了安全团队对安全事件的响应时间，加快安全事件的响应速度，大大降低了安全运营的成本，增强安全团队的协作能力。

1.2 功能模块概述

AiLPHA SOAR 平台包括安全运营中心、场景编排中心、能力中心、系统管理四大功能模块，具体如下图所示：

- **安全运营中心**汇聚了各种类型的安全事件数据，并对大量事件进行解析和合并处理；通过任务管理绑定剧本并通过不同的方式进行触发，任务下发并生成案件进行跟踪；对产生的案件进行全生命周期管

理，案件执行过程中可在线协同作战；对个人相关工作进行统一管理。包括案件调查、事件接入、任务管理、个人工作室。

- **场景编排中心**通过智能编排，把人、流程和技术整合起来，大幅提升安全运营工作效率，将分析人员从耗时且重复的分析工作中解放出来。支持拖拽式交互设计安全风险分析研判策略和联动响应剧本，支持多种策略编排动作，包括但不限于关联验证、告警聚合、联动、阻断。包括剧本管理和组件管理。
- **能力中心**实现平台内标准能力、剧本能力、设备能力的统一管理，可将平台的设备能力、标准能力、剧本能力接口化，方便平台内部或第三方调用。包括设备管理，标准能力，剧本能力。
- **系统管理**实现对平台内部进行全管理，包括案件类型、数据字典、标签管理、角色管理、用户管理。

1、 安全运营中心

安全运营中心包括案件调查、事件接入、任务管理、个人工作室几个子功能。

- 案件调查：
  - 支持案件的全生命周期管理，并对安全事件的处理过程进行跟踪管理；
  - 支持通过历史案件处理过程进行应急响应和调查取证；
  - 支持案件协同作战高效处理案件，通过聊天功能进行协同交流，使案件处理更高效；
- 事件接入：
  - 事件汇聚：联动其他平台或设备，如：AiLPHA 大数据平台、态势感知平台、SOC 等；
  - 事件处置：主要是根据样例日志对事件源产生的事件进行解析与标准化，将不同类型的事件都按照统一的格式进行存储。可过滤出用户重点关注的安全事件。并将不同来源表达相同事件的数据进行去重合并，消除数据冗余。

- 任务管理：通过不同的触发方式触发绑定的剧本从而产生不同类型的案件。
- 个人工作室：支持对个人相关工作进行统计；支持快捷查看相关工作，支持统一办理。

2、 场景编排中心

平台可将重复的工作整合成剧本，沉淀经验，解放人力；具备丰富的剧本库、组件库，支持可拖拽式灵活编排剧本，支持剧本嵌套调用，支持用户自研组件、剧本。

- 剧本管理：
  - 支持内置标准剧本，可对某些安全事件直接调用标准剧本工作流进行处置；
  - 支持自定义剧本编排，灵活应对安全事件；
  - 支持复杂剧本作为子剧本被其他剧本调用，增加剧本复用率；
  - 支持剧本按不同类型和标签进行分类。
- 编排调度：
  - 支持基于决策结果进行服务的编排和调度；
  - 支持预置或自定义自动化脚本进行闭环处置；
  - 支持多种策略编排动作，包括但不限于联动、阻断、隔离、取证、封堵，同时支持编排动作的灵活扩展机制；
  - 支持将威胁防护措施转化成安全策略控制任务，并下发。

3、 能力中心

打破能力孤岛，整合安全设备。平台支持安全设备标准化，剧本能力接口化，将 IT 能力抽象统

一，实现企业能力标准化调用。

- 设备管理：
  - 每一种类型的设备对应一个 APP，可将设备注册至 APP 下进行统一管理、调用。
  - 支持在每个 APP 下添加多个设备实例。
  - 支持标准化的接口，支持第三方、剧本联动设备进行查询、分析、处置、响应。
  - 支持对 APP、设备添加、注册进行权限控制，保证系统、设备安全性。
- 标准能力：
  - 支持将 APP 标准能力集合形成标准能力库；
  - 支持剧本查找标准能力指向对应的 APP；
  - 支持平台内或第三方调用标准能力 API 接口。
- 剧本能力：支持平台剧本接口化；支持第三方调用剧本能力 API 接口，实现剧本能力共享。

4、 系统管理

系统管理实现对平台内部用户、角色、标签、字段等等进行统一管理，包括案件类型、数据字典、标签管理、角色管理、用户管理。

- 事件类型：支持对案件分类标签进行统一配置和管理；
- 数据字典：支持对平台上的字段信息进行统一配置和管理，包括数据来源、数据的标准化字段格式说明、目标存储平台等基础信息以及攻击链、告警字典等数据；

- 标签管理：支持对平台功能模块使用到的标签进行统一配置和管理，包括“标准能力，剧本管理，设备管理，组件库，组件管理，剧本能力”几个功能模块；
- 角色管理：支持对平台涉及的用户角色进行统一查看；支持查看每个角色分类下对应的所有用户名称；
- 用户管理：支持对平台用户进行统一配置和管理；支持管理员进行账号分配、账号密码重置、账号删除、禁用等操作；

1.3 角色和权限说明

AiLPHA SOAR 安全编排与协同响应管理平台默认设置有四个角色，分别是管理员（包含 admin 账号和普通管理员账号）、安全分析员、安全编排员、设备管理员。其中 admin 账号拥有平台最高权限。有关角色和权限配置的更多详细信息，请参考用户权限管理。

如无特别说明，本文仅从 admin 视角进行描述，配置内容以 admin 用户操作举例说明。

2. 用户登录/登出

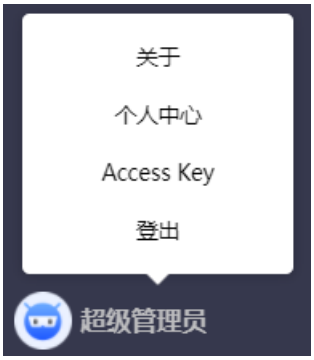
2.1 用户登录

设备安装上架并连接网线、电源后，用户可通过 Web 方式登录并管理 AiLPHA SOAR 平台。在浏览器中输入 https:// AiLPHA SOAR 平台 IP，进入登录窗口。

在登录窗口中输入用户名、密码，单击<**登录**>进入 AiLPHA SOAR 安全编排与协同响应管理平台。

管理员及拥有所有功能模块访问权限的用户登录后进入的默认页面如下：

页面布局分为功能菜单、操作区、用户信息三部分。

序号	名称	说明
1	功能菜单	以不同的角度提供各类管理功能的配置入口，方便用户根据实际需要进行切换，如下图所示。 
2	用户信息	显示当前登录用户，可在此区域进行修改用户信息、查看平台版本、查看用户绑定 Access Key 详情，退出登录等操作，如下图所示。 
3	操作区	该区域主要用于展示各类案件、任务信息等展示，以及执行相关的功能操作。详细操作请参考以下章节。

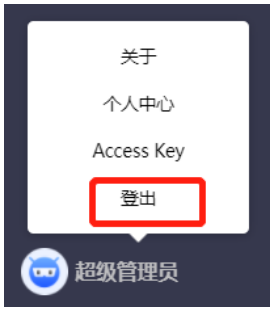
2.2 用户已被登录

用户登录，当出现当前用户已登录的消息，如下图，说明此用户在其他地方已经登录。

系统不支持用户多地同时登录。

2.3 用户登出

退出系统后，只有重新登录才能再次登入系统。点击右上角的<**登出**>，回到登录页面，如下图。



- 直接关闭浏览器标签的方式无法使已登录到设备上的用户退出。
- 在 AiLPHA SOAR 安全编排与协同响应管理平台页面右上角上单击用户名，在弹出的下拉框菜单选择<**登出**>，可以退出 Web 登录。

2.4 修改密码

登录系统，为了确保使用安全性，需修改密码。

修改密码有两种方式：

1） 初次登录：

✓ 在登录页输入账号及初次登录密码，点击登录按钮,会跳转至修改密码页面。

✓ 输入原密码、新密码、确认密码，点击**<确认修改>**按钮，则修改成功；

✓ 修改成功后，需重新登录进入系统。

💡 密码组成方式:需包括数字、大写字母、小写字母、特殊符号，且长度在 8-16 位。

2） 非初次登录或已重置过密码：点击右上角<**个人中心**>，点击<**修改密码**>按钮，跳转至修改密码界面，密码组合方式同上。

⚠
- ◆ 用户输入密码错误十次账号将被锁定半小时。
- ◆ 忘记密码可联系管理员进行密码重置。

3. 快速入门

3.1 基础概念快速理解

3.1.1 事件

事件是用来触发剧本流程的一个信标，事件的类型通常包含告警、邮件、工单、消息等。当检测到事件发生时可自动触发相应的剧本流程。

3.1.2 案件

案件是安全事件响应流程完整的生命周期体现。可实现安全事件的识别、防护、检测、响应。

- 案件的产生来源为：任务自动化运行生成；手动创建。
- 案件可支持多团队在线协同办理。

3.1.3 任务

任务是剧本触发的一种方式，通常情况下，创建任务是为了周期执行剧本或是根据不同的事件来源自动触发剧本。

- 任务可通过事件触发或周期触发方式自动化的触发剧本。
- 任务可生成案件。

3.1.4 组件

用户可将典型的安全事件响应流程拆解为标准组件。组件是组成剧本的单个动作元素。平台将组件分为四大类，包括动作、脚本、决策、人工组件，具体概念如下：

- 动作：平台内置。均为安全运营中的标准动作，动作可联动安全设备。
- 脚本：用代码实现的步骤流程，可被封装为脚本组件。
- 决策：在安全运营流程中，涉及到分支决策的步骤，可封装成决策组件。
- 人工：在安全运营流程中，涉及人工反馈的步骤，可封装成人工组件。

3.1.5 剧本

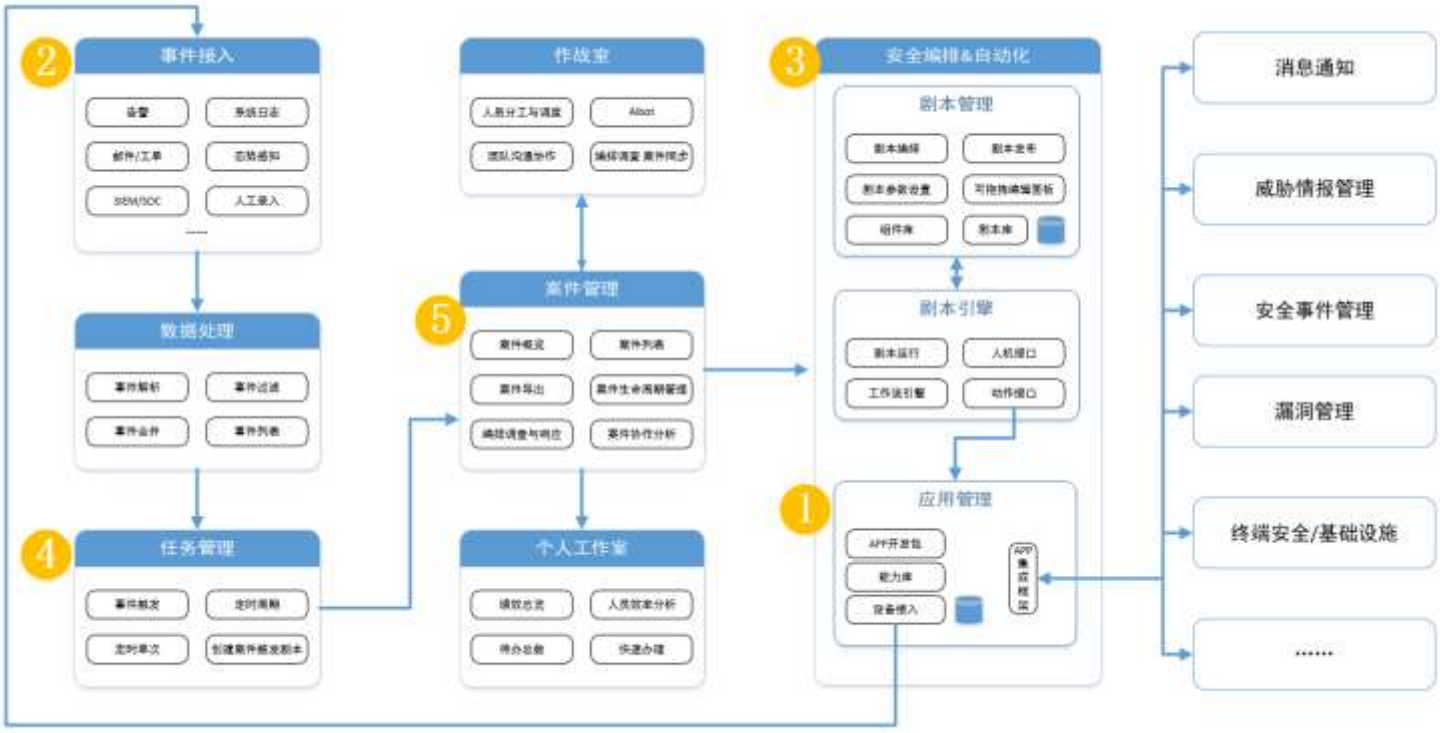
剧本是企业针对不同事件固化的的标准化处置流程。

3.1.6 APP

APP 是同类型设备的集合，可搭载多个设备实例。APP 具备标准能力和设备能力，同理，APP 下添加的多个设备具有该 APP 拥有的能力，如此便可支持同个动作一次性联动多个设备。

- **设备能力**：设备能力的动作参数，更细化，支持该设备本身的特性参数（无共性的动作参数）和返回结果。各个 APP 的设备能力互不相同。
- **标准能力**：从设备能力抽象出共性参数（其他联动参数以内置参数、内置逻辑等方式填充），实现只要输入少数共性参数即可完成能力的调用，返回的参数也抽象出共性返回结果。各个 APP 的标准能力可以复用共享。

3.2 平台最简使用旅程



1. APP 安装与设备管理（准备工作）

用户可**能力中心-设备管理**先安装或导入不同的 APP 包，并对设备进行接入与管理。方便后续接入设备的日志，以及联动设备下发指令等操作。

2. 事件源配置（准备工作）

安全事件数据来源于自主配置导入，或拉取平台在**设备管理**中已接入设备的数据。统一在**任务管理-事件源**进行手动接入并进行人工配置。

3. 剧本编排（准备工作）

用户可在**场景编排-剧本管理、场景编排-组件管理**进行自定义剧本和组件的编写，以及内置剧本和组件的查看等操作。

4. 任务管理（准备工作）

事件接入后，需要对不同的事件进行处置。可通过**任务管理**进行任务的创建，绑定预先编排好的默认事件处置剧本即可触发生成案件进行处置。

5. 案件调查与响应处置

在完成上述准备工作之后，用户可进行案件的创建。可在已经创建或已经生成的案件中查看案件以及事件详情，调用作战室进行协同作战。

在**安全运营-案件调查**的案件列表中，点击案件 ID 下钻至作战室窗口。作战室可下发不同类型的指令，可完成内部团队协同作战的工作，可实时交互作战，加速案件响应处置流程。

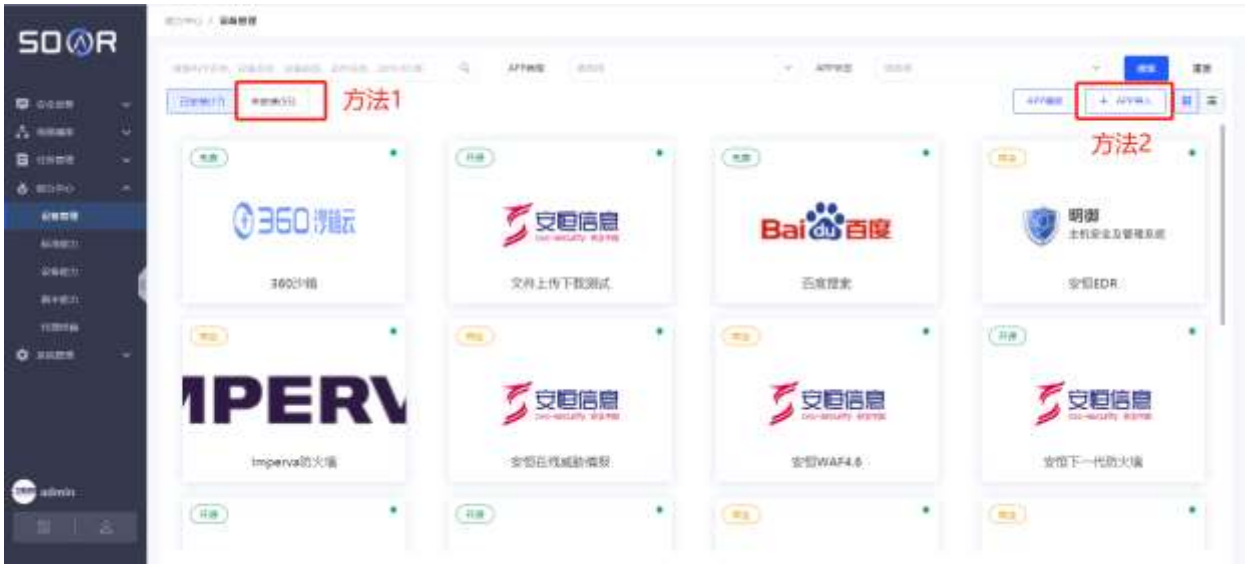
接下来的五章（第四章~第八章）将按以上最简流程的顺序进行讲解。剩余功能细节分布在剩余章节。

4. APP 安装与设备管理

4.1 APP 快捷安装说明

4.1.1 功能简介

APP 安装可以通过以下两种方式进行安装：方法 1，在线安装；方法 2，手动安装，如下图所示：



4.1.2 在线安装

在线安装方式支持用户可通过线上拉取最新 APP 商城数据，进行在线安装。通过一键式在线安装，可大大减少 APP 安装时间与安装复杂度。

选择“**能力中心➤设备管理**”进入**设备管理**页面。

1. 未安装页面说明

点击【未安装】按钮，该页面会自动拉取线上 APP 商城数据，如下图所示为数据载入中：

- 注：数据拉取有两种情况可能发生：

a.数据拉取失败，显示以下提示：

处理方法：

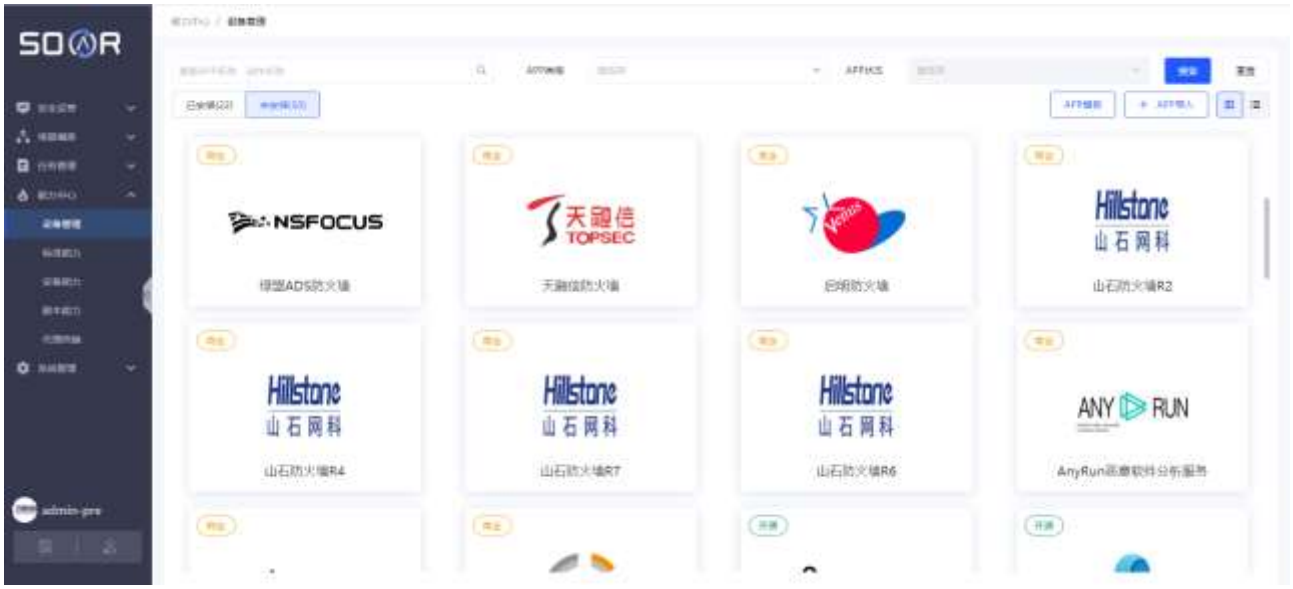
I.可点击【代理服务器配置】，进行代理配置，如下图所示：

可进行代理服务器的 IP、端口、用户名、密码的填写，并进行代理服务器连通性测试；

连通性测试通过会提示：“连通性测试成功“；失败会提示:”连通性测试失败，请重新配置“

II.用户可以选择自行前往 APP 商城，进行手动安装。具体操作见 4.1.3 手动安装

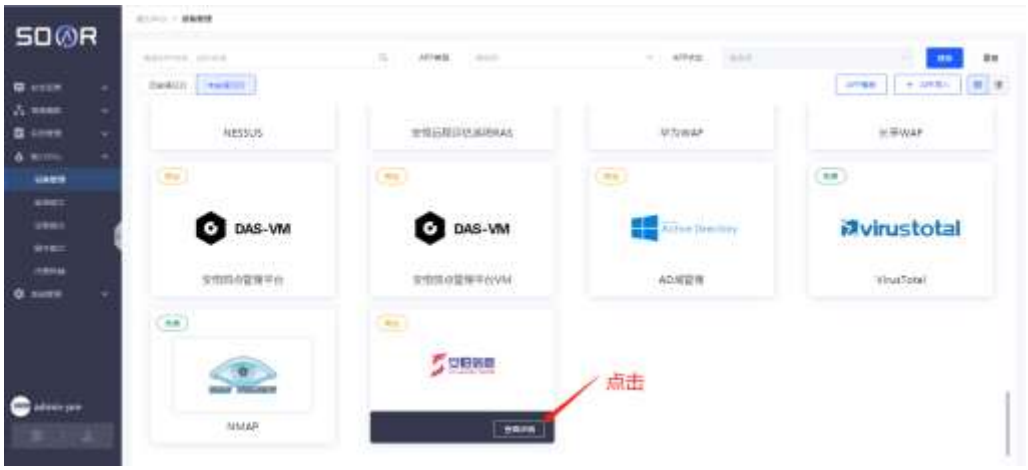
b.数据拉取成功，如下图所示，页面显示拉取的线上 APP 商城数据：



用户可继续进行下一步的在线安装操作。

2. APP 在线安装

【未安装】页面数据拉取线上 APP 商城数据成功后，可将鼠标悬浮至某个未安装 APP 上，浮出【查看详情】按钮，如下图所示：

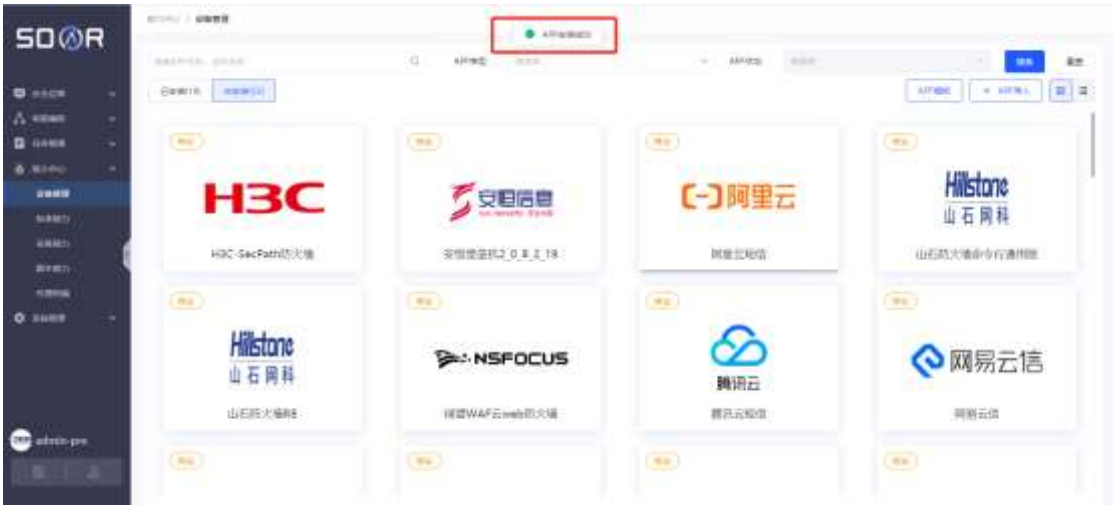


点击【查看详情】，弹出 APP 详情弹框，可查看该 APP 相关详情信息以及该 APP 具备的动作信息，点击【APP 安装】模块下的【在线安装】按钮，可进行 APP 在线安装，如下图所示：

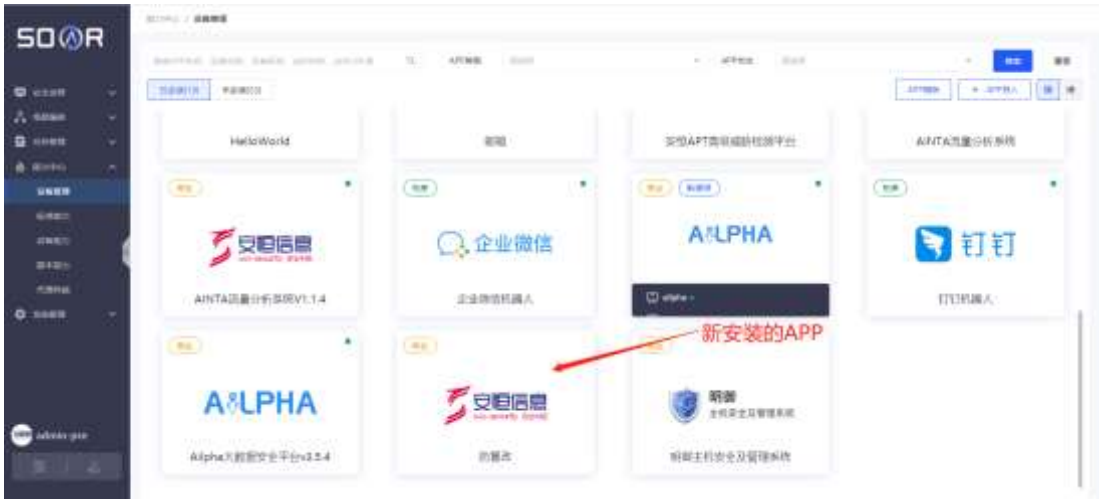
a.在线安装成功

点击【在线安装】按钮后，会进行下载地址解析，解析成功后会自动进行 APP 安装，如下图所示：

安装 APP 成功后，新安装 APP 自动归入至已安装的 APP 中，并弹出 “APP 安装成功 “提示，如下图所示：



用户可在【已安装】APP 页面看到新安装 APP 的所有信息，并继续进行接入设备等一系列操作：



b.在线安装失败

在线安装的过程中，可能会遇到以下问题，如下图所示：

- 解析地址失败
- APP 在线安装失败

如遇到以上两种问题，需检查网络或自行前往 APP 商城进行手动安装。

4.1.3 手动安装

若在线安装遇阻，可通过本小节完成手动 APP 安装，具体步骤如下：

1. APP 商城说明

打开 APP 商城页面， 在 APP 商城搜索栏可对 APP 名称、动作名称进行搜索，并支持根据类型进行 APP 搜索，如下图所示：

2. APP 安装包下载

鼠标悬浮至 APP，浮出【详情】按钮，如下图所示:

点击【详情】按钮，弹出如下 APP 详情弹框，点击【APP 安装】下的【下载 APP 安装包】按钮，则可自动进行 APP 安装包下载，如下图所示:

3. 手动导入 APP 安装包

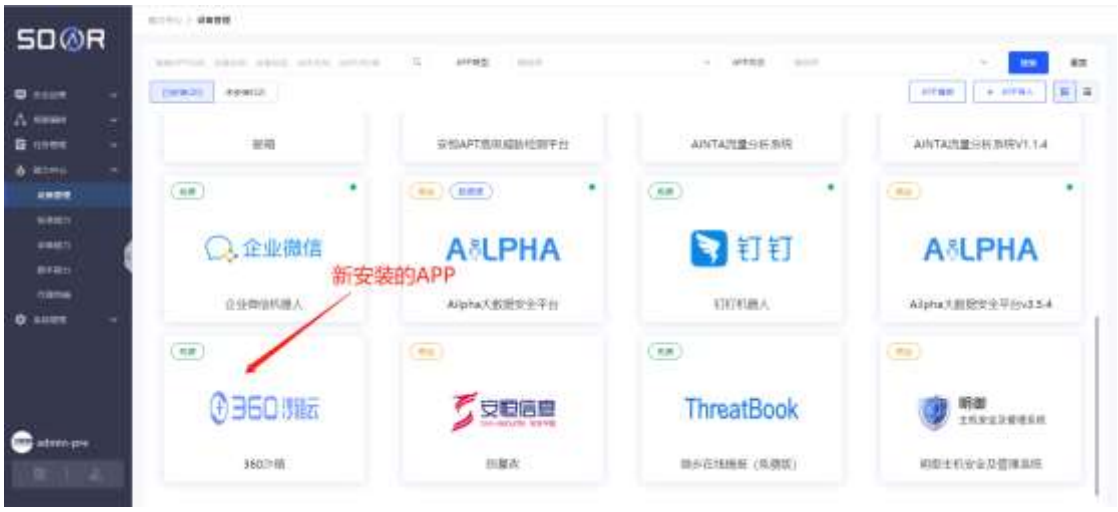
选择“**能力中心➢设备管理**”进入**设备管理**页面。点击右上角【APP 导入】，弹出 APP 上传对话框，选择刚刚在 APP 商城下载的 APP 安装包进行手动导入操作，如下图所示：

a.导入成功

点击【导入】，选择下载好的 APP 安装包，开始导入，上传成功后，如下图所示：

Tips：APP 导入需等待一小段时间，请您无需着急。

点击【确定】，则可在【已安装】页面查看安装好的 APP 包，如下图所示：



b.导入失败

如果下载的 APP 包有问题导致导入失败，可向 APP 商城中【联系我们】中的 dasca@dbappsecurity.com.cn 邮箱发送邮件，发送邮件时请务必说明导入失败的情况并将失败的 APP 包一并发回，以便团队帮助定位问题并解决，感谢您的配合。

4.1.4 APP 更新

APP 支持手动更新，点击<更新>按钮，弹出 APP 手动更新弹窗，导入新的 APP 工程包，即可触发 APP 更新机制。

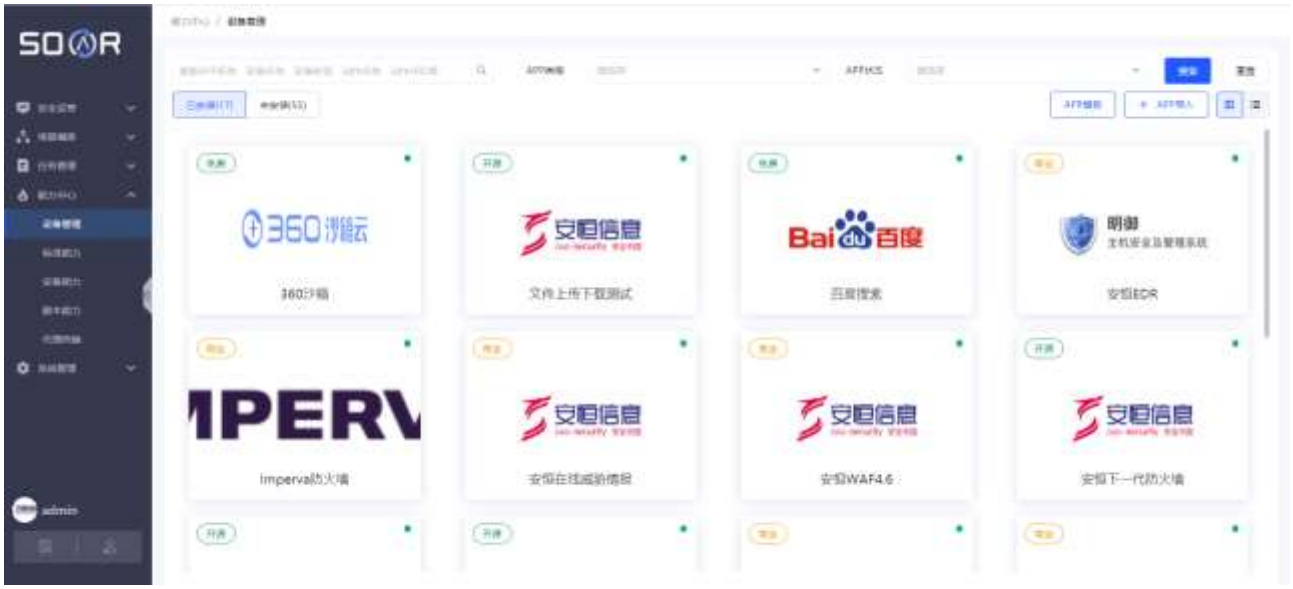
4.2 设备管理

4.2.1 功能简介

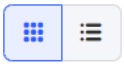
设备管理包括 APP 集成、APP 导入、添加设备等功能，便于用户添加剧本或操作中需要联动或作为事件接入事件源的设备。每个 APP 将具有相同能力的设备集成在一起，并绑定标准能力或设备能力，一个 APP 可接入具体多台设备（例：安恒防火墙 APP 可绑定/block/ip（阻断 IP 地址）能力，下接多个不同的安恒防火墙设备）。

4.2.2 功能详解

选择“**能力中心➢设备管理**”进入**设备管理**页面。该页面汇总了平台中 APP 及设备的信息并加以展示，使用户更方便了解设备详情。

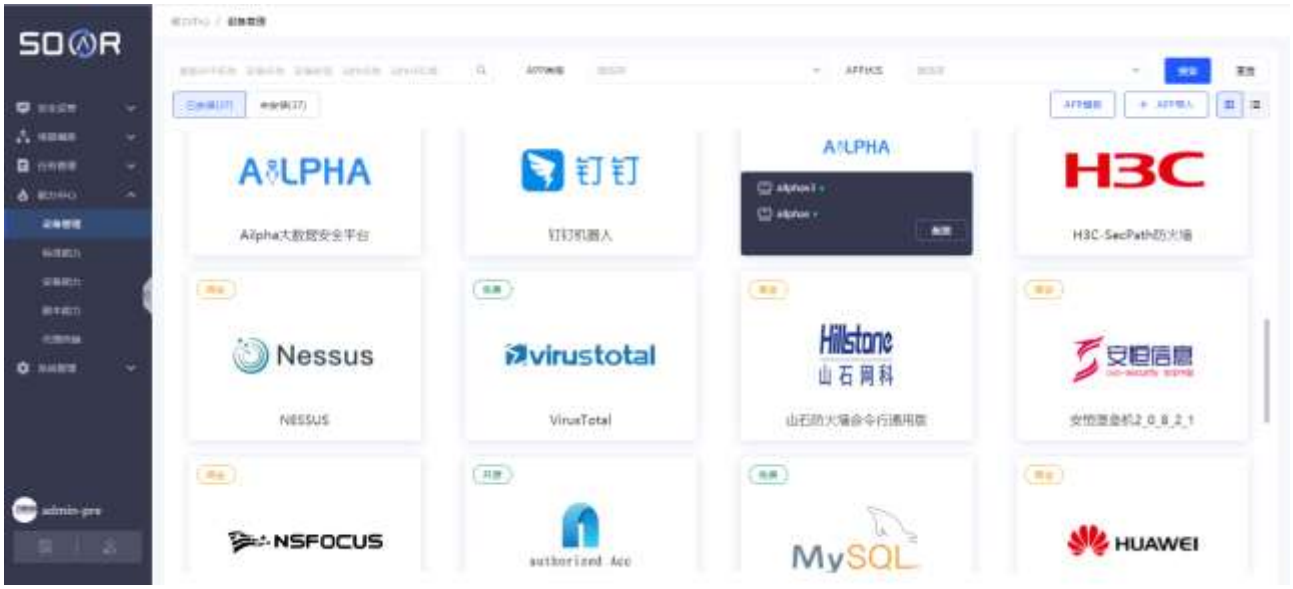


1. 视图切换

点击右上角  按钮，可随机切换 APP 块状视图（左）与 APP 目录视图（右）。

1.1 APP 块状视图

➢ APP 块状视图页面如下图所示：



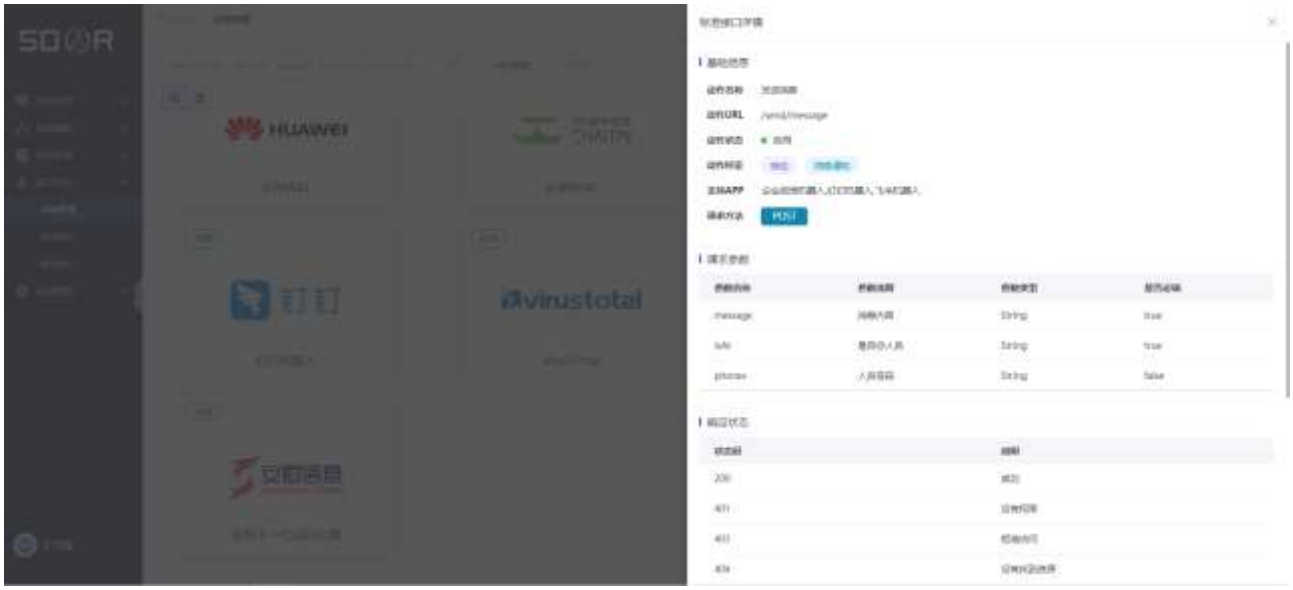
➢ 详情如下：

APP 块元素：包含 **APP 图标**、**APP 左上角标识**（开源、商业、免费、事件源四种标识）、**APP 启用状态**（位于每个 APP 块的右上角：绿色表示 APP 服务启用，没有该标识则标识 APP 服务未启用）、**APP 名称**；

鼠标悬浮至某一 APP 上，滑出绑定的设备名称及【配置】按钮，如下图所示：

【配置】按钮：点击【配置】按钮，弹出 APP 配置框，包括【APP 基本信息】、【APP 动作】、【设备实例】三块内容。如下图所示：

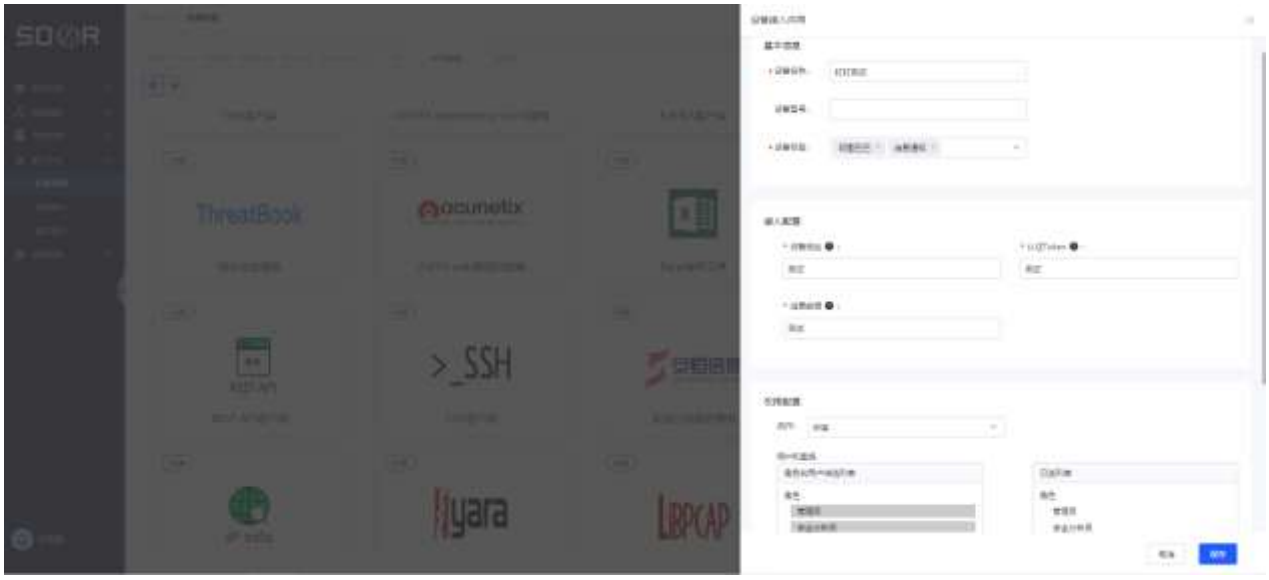
点击【APP 配置】-【APP 动作】中的某一动作，弹出该动作的标准接口详情框，包括【基础信息】、【请求参数】、【响应状态】三块内容，如下图所示：



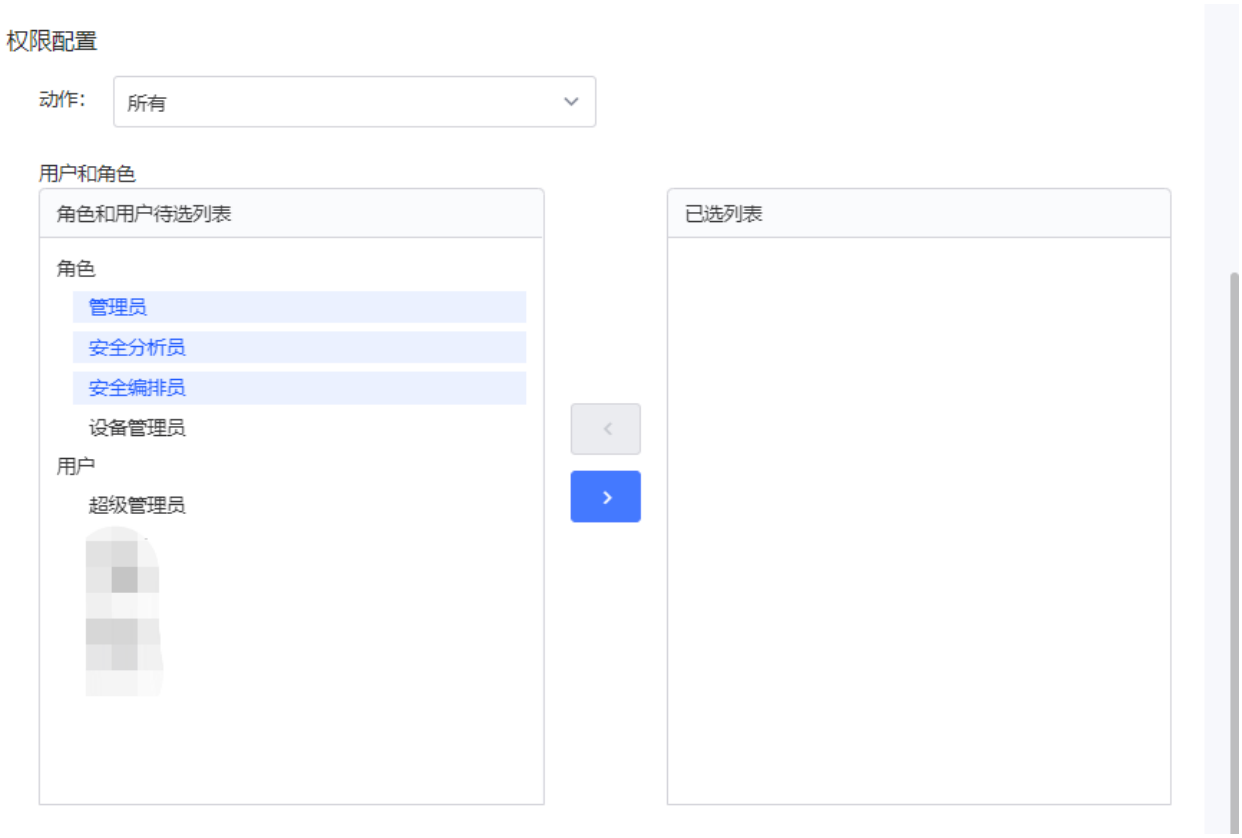
【APP 配置】-【设备实例】中，点击使用状态的开关按钮，可对该设备的使用状态进行控制，打开则可使用该设备，关闭则该设备不可用。除此之外，打开设备时，还会对设备的健康状态进行检测，绿色表示设备健康可用，灰色表示设备不可联通，如下图所示：

点击上图操作栏中的【查看】按钮，可查看该设备的具体信息，包括【设备基本信息】、【接入配置】、【权限配置】三块内容，说明：【接入配置】为联通该设备需要填写的接入参数；【权限配置】为可使用该设备的人员或角色。如下图所示：

点击操作栏中的【编辑】按钮，可对该设备的具体信息进行编辑，如下图所示：



【权限配置】中，可选择左侧的角色或者用户（可都选，也可只选择角色或者用户），点击  按钮，可见左侧选中的用户或角色加入到已选列表中，如下图所示：



注：默认管理员、安全分析员、设备管理员有设备动作权限。用户可根据需求进行权限变更或细化。

点击【保存】，可保存当前已经编辑好的内容。点击【取消】，可返回上级【APP 配置】菜单。

点击操作栏中的【删除】按钮，可删除该设备。

◆ 首次添加设备和删除最后一个设备所需时间较长，需耐心等待。

1.2 APP 目录视图

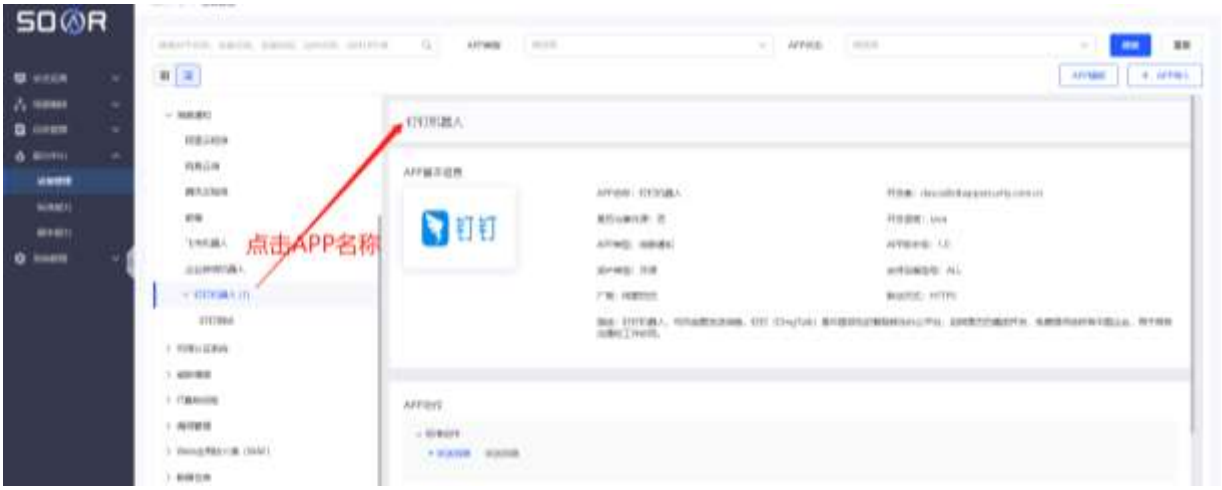
➢ APP 目录视图页面如下图所示：

➢ 详情如下：

左侧目录：分为三级目录：APP 类型—>APP 名称—>APP 绑定的设备名称。

点击【APP 类型】类目的 > 按钮，可展开该类型下的所有 APP 目录。

点击【APP 名称】，可查看该 APP 的详情，包括【APP 基本信息】、【APP 动作】、【设备实例】三块内容，如下图所示：



点击【APP 名称】前的 > 按钮，可展开该 APP 下的所有绑定设备目录，点击某设备名称，可查看该设备的所有信息，如下图所示：

其余按钮操作与 APP 块状视图相同，此处不再赘述。

2. 查询

点击【搜索】按钮，可通过 APP 名称、设备名称、设备标签、动作名称、动作 URL、APP 类型、APP 状态进行搜索。

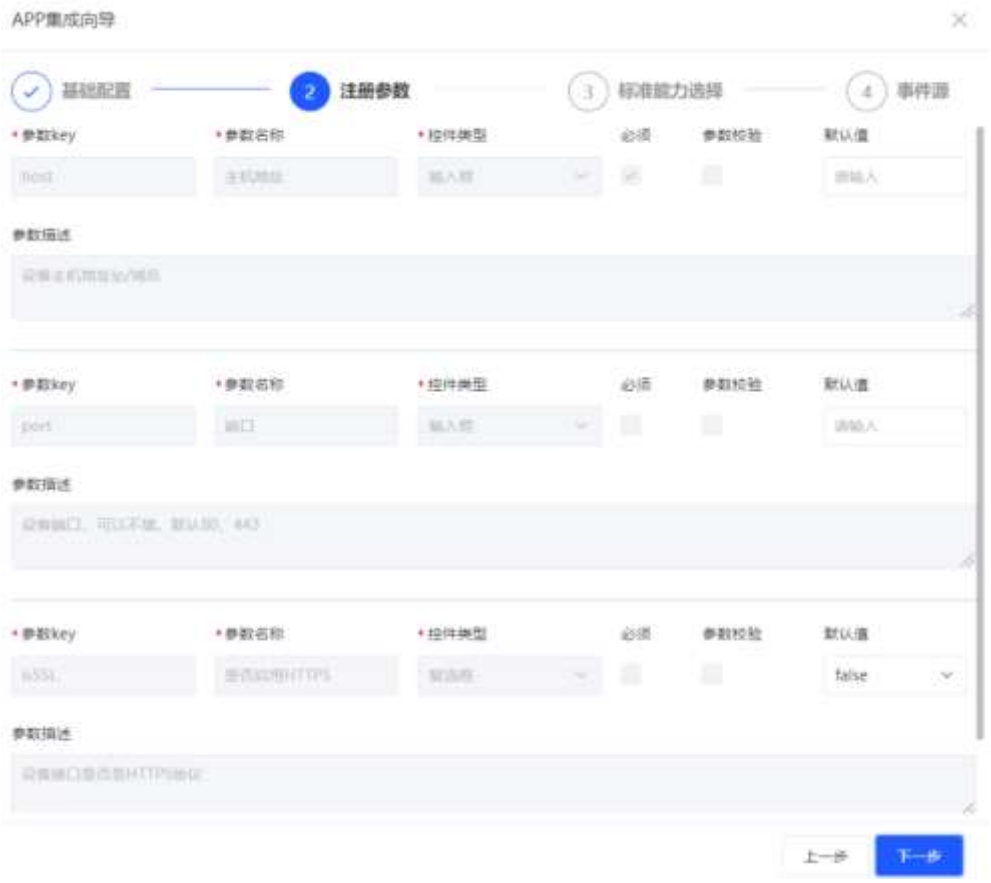
点击【重置】按钮，可对所有搜索条件进行清空重置。

3. APP 模板

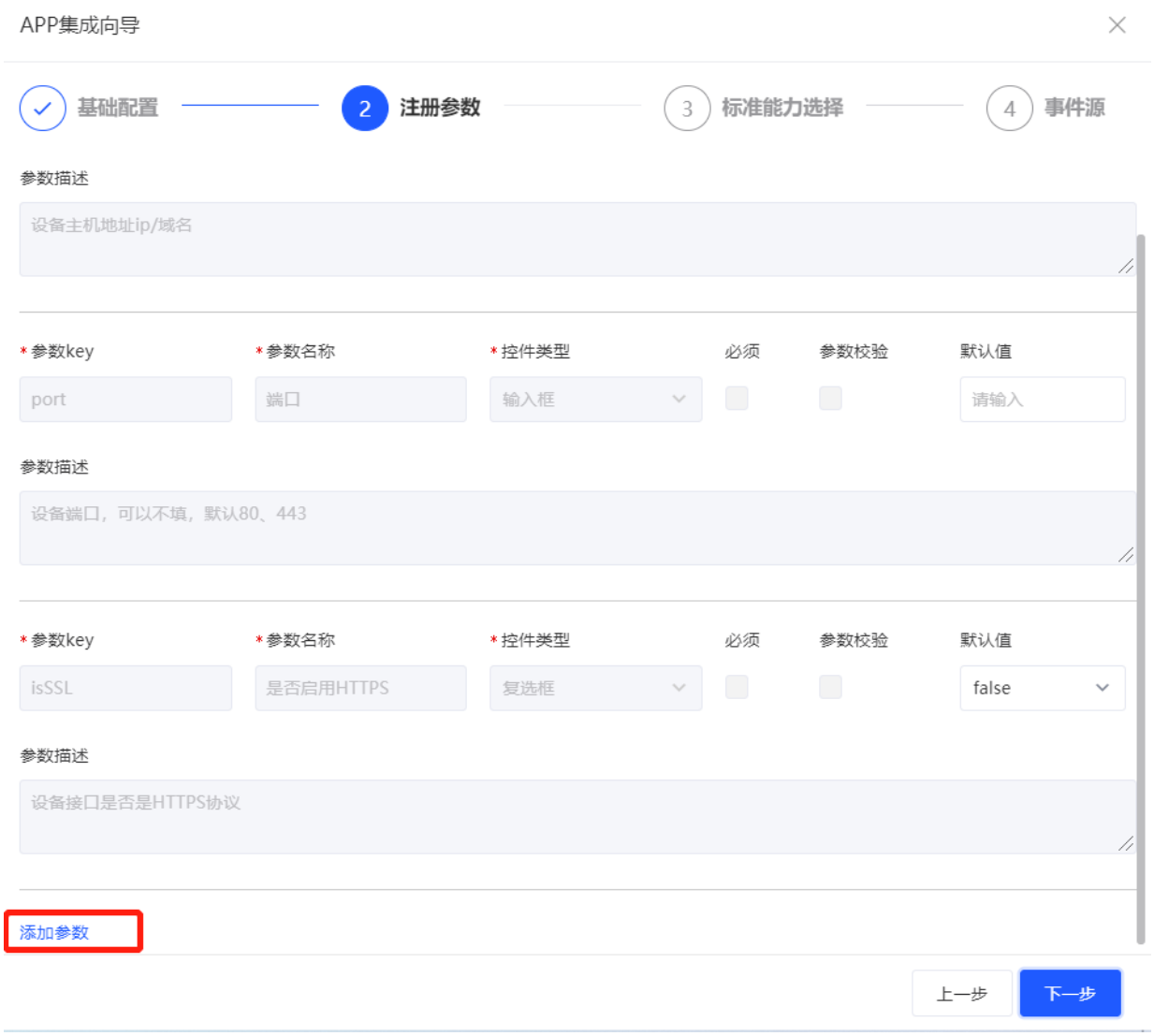
如果您需要自己进行 APP 开发，可在本功能进行 APP 模板定制及下载，根据模板内容导航完成 APP 开发。APP 模板制定分为“基础配置”，“注册参数”，“能力选择”，“事件源”四个集成步骤。

- 基础配置详情如下，需填写 APP 名称、APP 版本号、资产类型、厂商、联动方式、开发者邮箱、支持设备型号、APP 类型、语言、APP 描述及设备图标：

- 注册参数详情如下，可添加设备注册需要的参数，注意注册参数有三个参数必填：主机地址、端口、是否启用 https，系统已为您内置好以上三个参数，如下图所示：

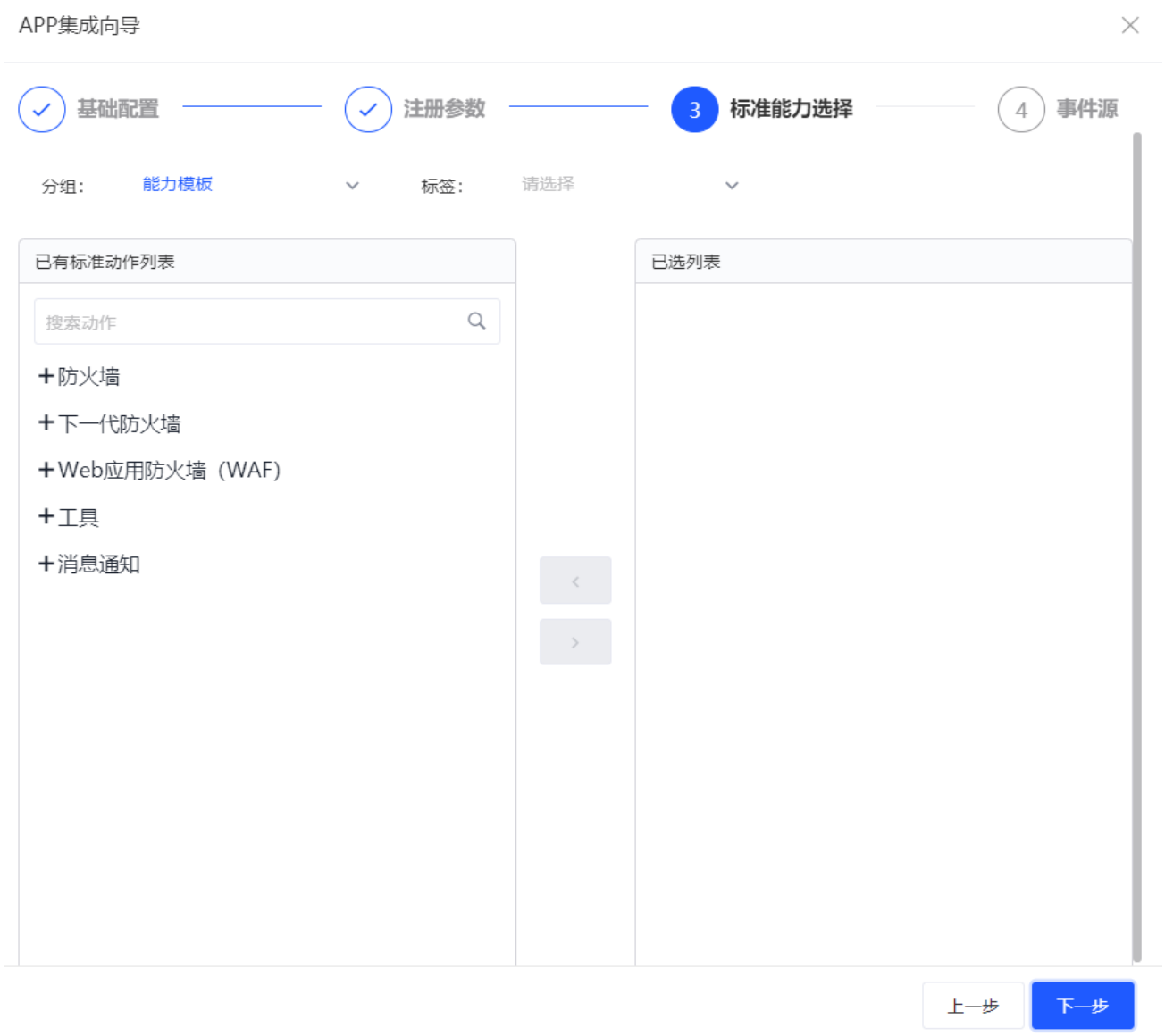


点击【添加参数】，可添加所需参数 key、参数名称等字段，为后续 APP 安装好后，接入设备做准备，如下图所示：

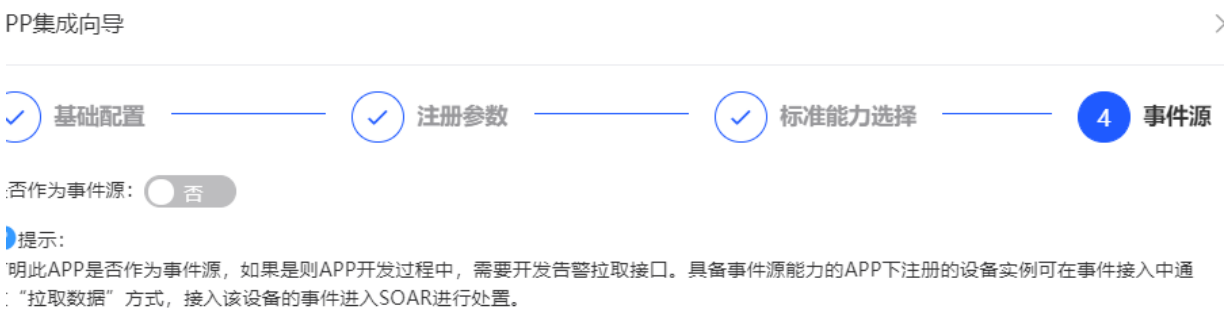


能力选择详情如下，可从左侧能力列表选择需要集成的 APP 具备的能力：

注：此处只可选择平台已安装 APP 具备的标准能力列表，设备能力不支持选择。



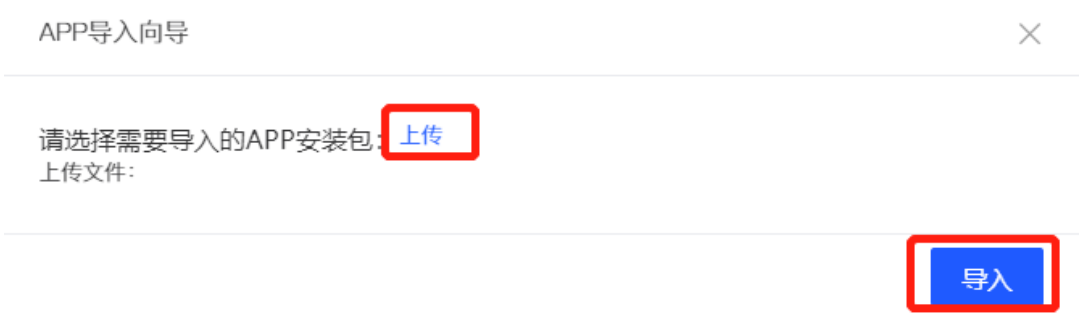
事件接入可选择该 APP 是否可以作为事件源进行事件接入：



点击“下载模板”，即可完成 APP 集成模板的下载，根据模板中的提示进行代码编写。

4. APP 导入

“APP 集成”代码编写完成后，可一键将 APP 安装包导入。点击“导入”后，即可看到安装好的 APP。



- APP 安装包名称不可重复、不可包含中文。
- APP 安装包工程文件有误不可导入。
- 自定义 APP 导入时需注意导入的新 APP 的设备动作应与其他 APP 不同，否则会导入失败！

5. 已安装、未安装页面说明

详见 4.1 APP 快捷安装说明 小节。

5. 事件源配置

5.1 事件源接入

5.1.1 功能简介

“事件源”模块可手动添加事件源，从而接入外部事件。接入的事件类型包括但不限于威胁告警、工单、邮件等任意形式的消息。

进入“**任务管理➤事件源**”页面，如下图所示:

5.1.2 新增事件源

点击“**新增事件源**”按钮，弹出如下框图:

1、 基础配置

用户需填写“事件源名称“，且可以为其增加描述。接入数据的方式可选择“kafka（客户端）“、“kafka（服务器）“、”拉取数据“、“syslog”。

Kafka 方式可直接填写 kafka 服务器的地址以及消息队列（topic）获取数据；拉取数据是通过平台中**设备管理**模块支持事件接入的设备来获取的。

- 用户如果需要拉取数据应提前添加好设备并选择其为事件接入的设备。
- 设备支持多选。
- 不能将不同格式的日志在同一个事件接入任务中拉取。

若接入方式为”kafka（客户端）“，则弹框页面如下所示：

填写客户端地址与消息队列 topic 名称，进行配置。

若为“kafka（服务器）“方式，则弹框页面如下所示：

服务器地址为本平台地址，可在服务器上创建 topic 后，进行事件接入，填写的消息队列为服务器上创建的 topic 名称。

若为“拉取数据“方式，则弹框页面如下所示：

目标设备：选取【能力中心】-【设备管理】中标记为“事件源” APP 挂载的设备

拉取周期：选择设备拉取告警的间隔时间例如：10 分钟（10 分钟拉取一次设备的告警）

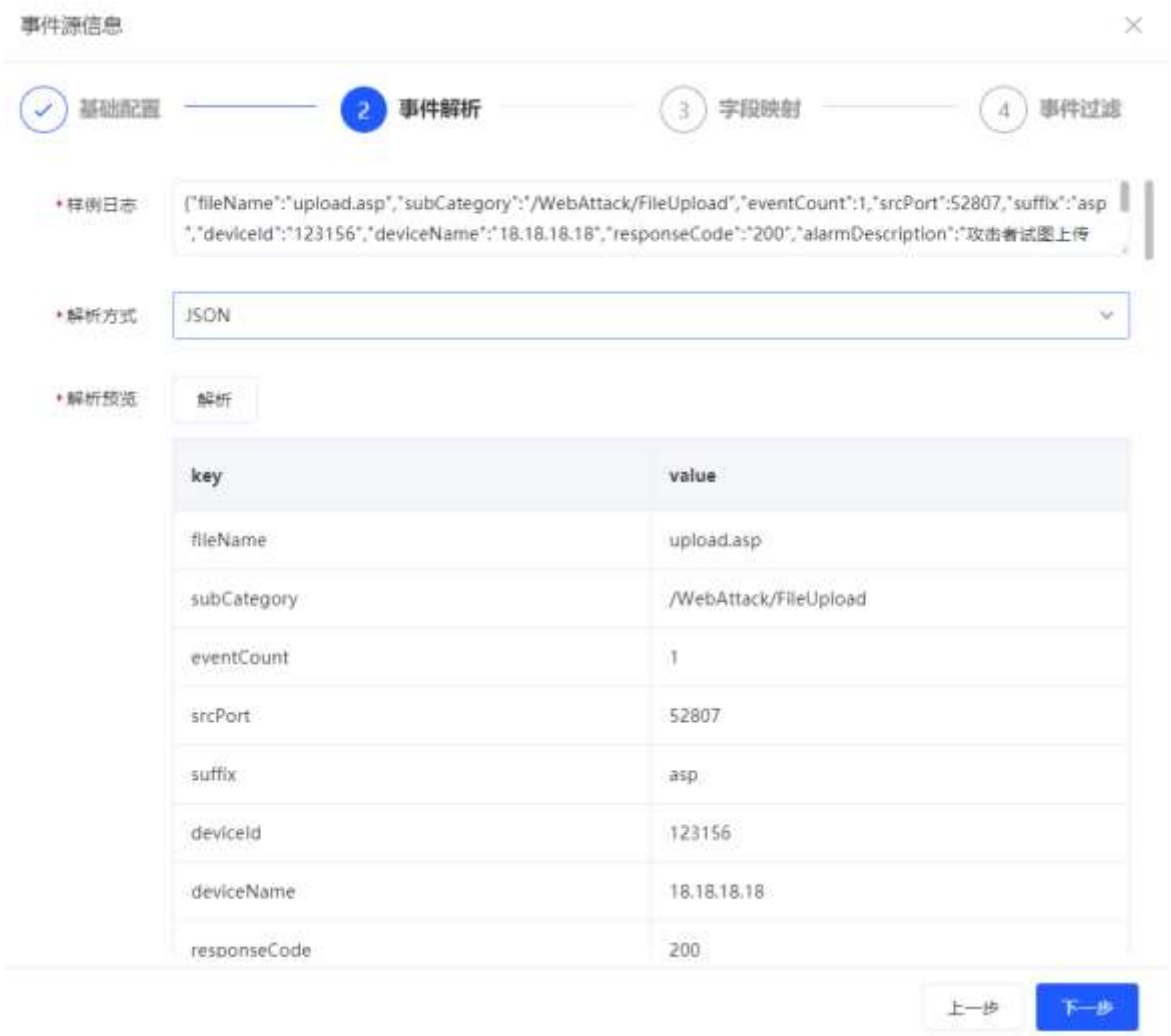
延迟时间：支持延迟平台拉取数据的时间，可有效降低由于数据落库时间差导致的数据丢失。例：拉取周期 10 分钟，延时拉取时间 2 分钟，表示平台将在 12 分时拉取前述 10 分钟周期内产生的告警数据。

若为“syslog“方式，则弹框页面如下所示：

服务器端口：可下拉选择对应端口

2、 事件解析

填写完“基础配置”后，点击**<下一步>**，输入 JSON、GROK 任意一种类型的样例日志，点击**<解析>**，若解析成功，可在“解析预览”中看到解析后的 key，value 值，解析成功才可点击**<下一步>。**“事件解析”如下图所示。



3、 字段映射

“事件解析”成功后，点击**<下一步>**，进入“**字段映射**“。**“日志字段”**和**“匹配结果”**为事件解析成功后自动提取的结果。下拉选择**“映射字段”**内容，可将事件解析成功后的日志字段与平台内置的字段（可在**系统管理>数据字典**模块中查看）形成映射从而实现标准化。

默认值：当解析后，匹配结果为空时，可以填写**默认值**赋予字段；

添加值映射：点击<**添加值映射**>，可选择正则/文本包含两种映射类型将需要匹配的值映射到字段对应的枚举值中。

支持新增字段和删除字段。详情如下图：

映射字段下拉框支持查询，详情如下：

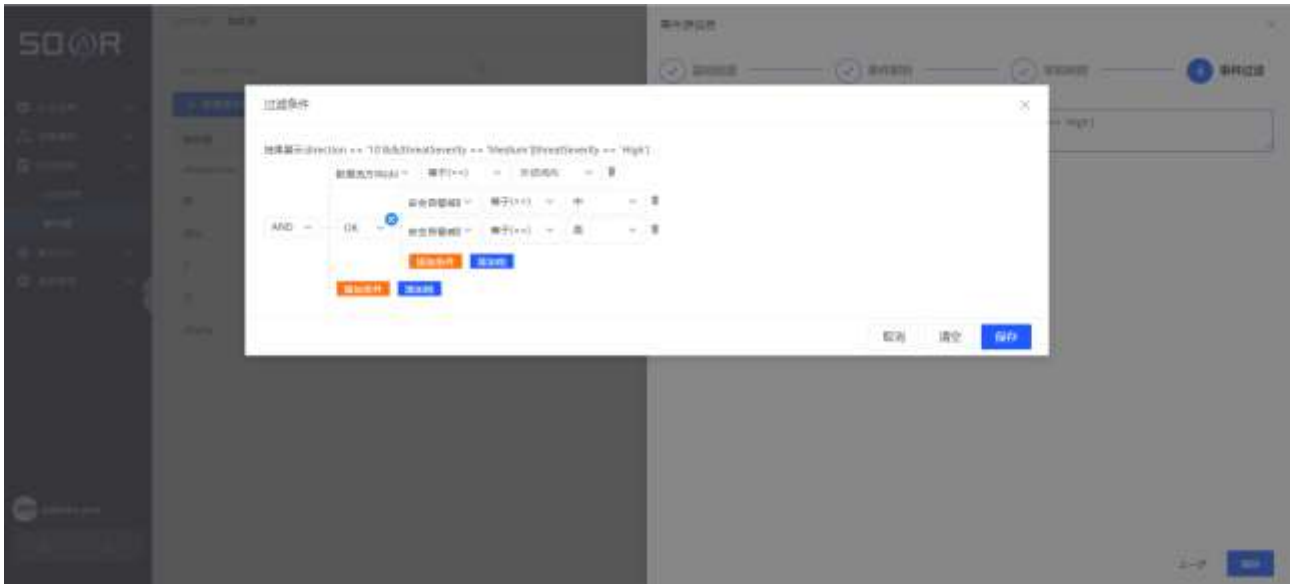
例：

添加值映射详情如下：

- 告警子类型、安全告警威胁等级、事件名称三个字段必须映射，若不存在相关信息请手动添加字段并填写默认值。
- 首次接入事件时，字段可自动映射，接入事件后如若修改，需手动修改映射关系。

4、 事件过滤

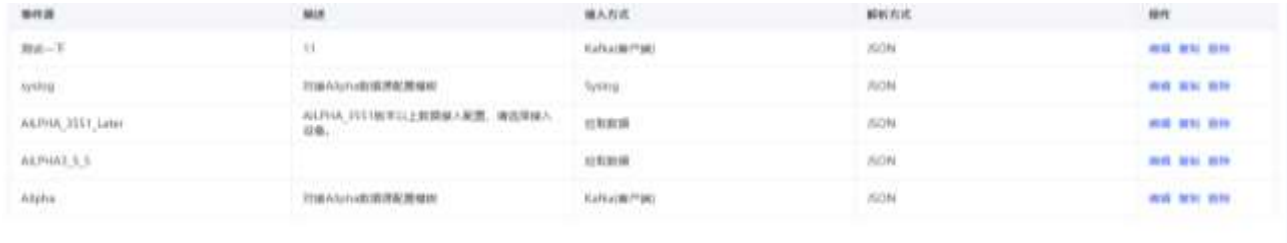
“字段映射”成功后，点击**<下一步>**，进入 “ 事件过滤 “。如需要过滤出某些事件，可填写**“过滤条件”**表达式。可点击输入框，弹出过滤条件表达式配置框。详情如下图：



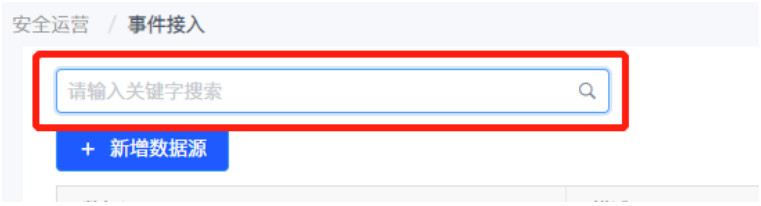
5.1.3 事件源管理

事件源接入成功之后，事件源列表可以看到已接入的事件源相关信息：事件源名称、描述、接入方式、解析方式、操作（编辑，复制，删除）。点击【编辑】可对其进行配置修改。点击【删除】可删除该事件源，前提是相关该事件源没有被任务所引用，否则应先删除相关任务，再删除事件源。点击【复制】可直接复

制该事件源。



列表支持搜索，详情如下：



6. 场景编排

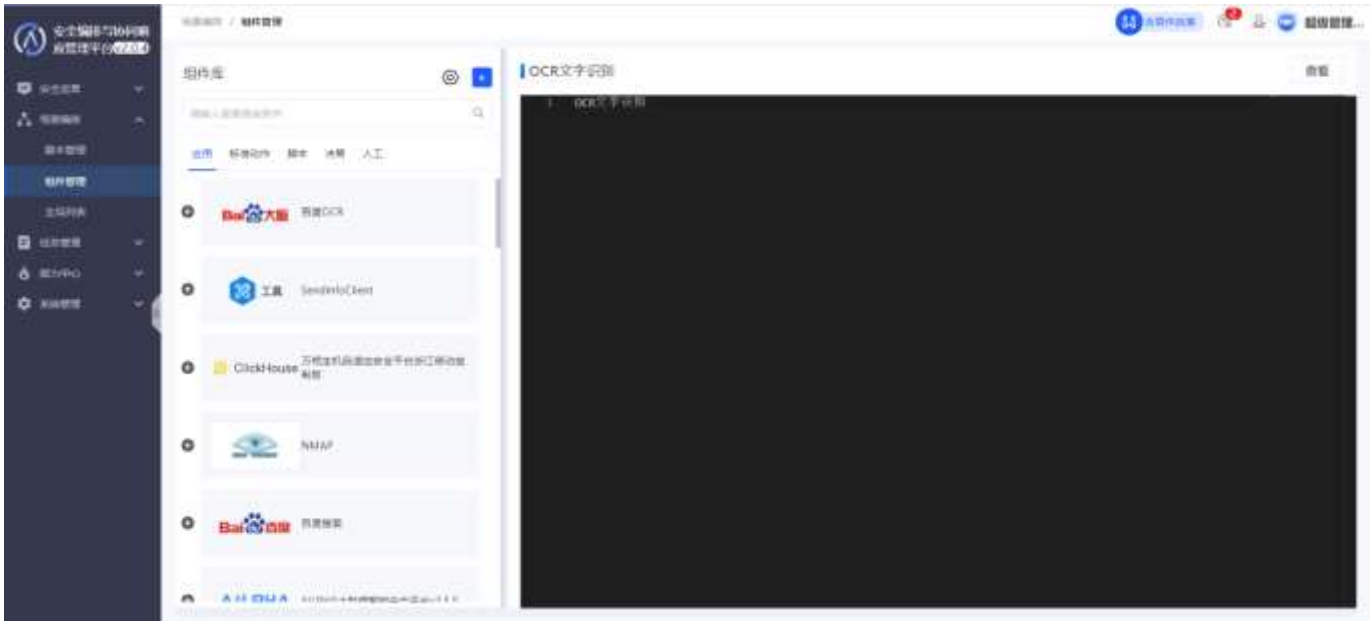
6.1 组件管理

6.1.1 功能简介

组件管理模块支持子组件的新建、编辑、查看、复制、删除、搜索、排序的操作。组件分为普通脚本组件、决策脚本组件、人工组件。用户可将传统安全运营的流程拆解为组件，以实现组件的灵活运用，达到灵活编排剧本的能力。实现简单易用，降低运维成本，提高运维效率的目的。

6.1.2 区块概要

点击“**场景编排➢组件管理**”，进入**组件管理**页面，如下图所示。



页面由“组件库”列表和组件编辑面板组成，区块概要见下表。

区块	说明	详细
组件库	1）平台内置和用户创建的所有组件列表。 2）支持子组件的搜索、新建的操作。 3）支持子组件的按标签分组、排序的操作。	
组件查看/编辑面板	1）点击组件库列表的某个组件，面板显示该子组件的详细内容。 2）支持子组件的查看、复制、删除、编辑的操作。	

详情如下：

1、 内置组件说明

- 应用

AiLPHA SOAR 平台 V2.0.4 版本内置 11 个 APP，此处展示该 11 个 APP 以及每个 APP 支持的动作。其他 APP 用户可在【能力中心】-【设备管理】安装好后，即可在此处看到已安装的 **APP 与动作**信息。

- 标准动作

此处展示已安装 APP 具备的标准动作列表。用户在【设备管理】安装好 APP 后，即可在此处看到相关**标准动作**信息。点击动作可查看相关配置。

- 脚本

平台内置 19 个脚本，包括列表决策脚本、密码生成器等等，用户可按需查看和使用，支持组件复制并按需更改。

- 决策

平台内置 2 个决策脚本：常规决策、是否为内网地址（脚本决策）。决策分为常规类型决策、脚本类型决策。常规决策可直接根据配置参数进行决策，无需编写脚本；脚本决策支持无需配置决策参数进行决策。

- 人工

平台内置 13 个人工任务组件，用户可直接使用。其中自定义人工任务支持用户自由配置。

- 内置脚本（剧本编排时可见）

平台内置拼接式入参、删除全局元素、添加全局元素获取案件 URL、修改案件状态、修改案件级别等组件。

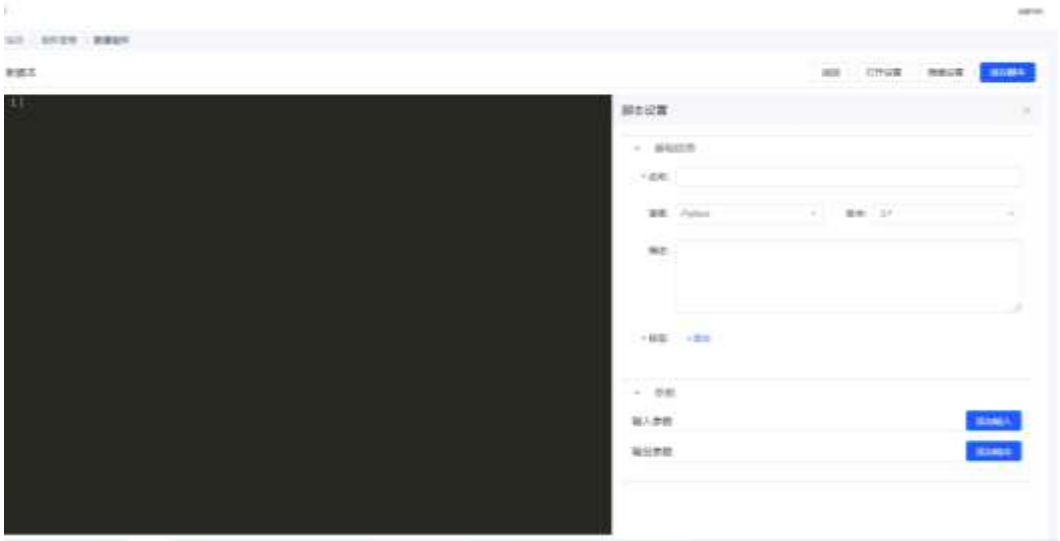
2、 组件新建

点击组件库  按钮，可以新建组件。新建组件类型分为普通脚本、决策脚本、人工任务。

类型说明：

- 普通脚本为基本的输入输出工具类型。
- 决策脚本在网关中进行配置，根据输入参数的值进行决策判断，输出决策结果。
- 人工组件可将涉及到人工的操作集成到组件中，可指定办理人，添加人工决策结果及表单。

组件新建如下图所示：



✧ **普通脚本**配置如下图所示，左侧可编写相应代码，右侧填写相关的配置信息，包括**基础信息**、**参数**（输入/输出参数）。**基础信息**需填写组件名称，选择脚本语言及版本，为组件添加描述，添加标签。**参数**需填写输入参数、输出参数，其中，**参数 key**，**参数名**，**参数类型**必填。

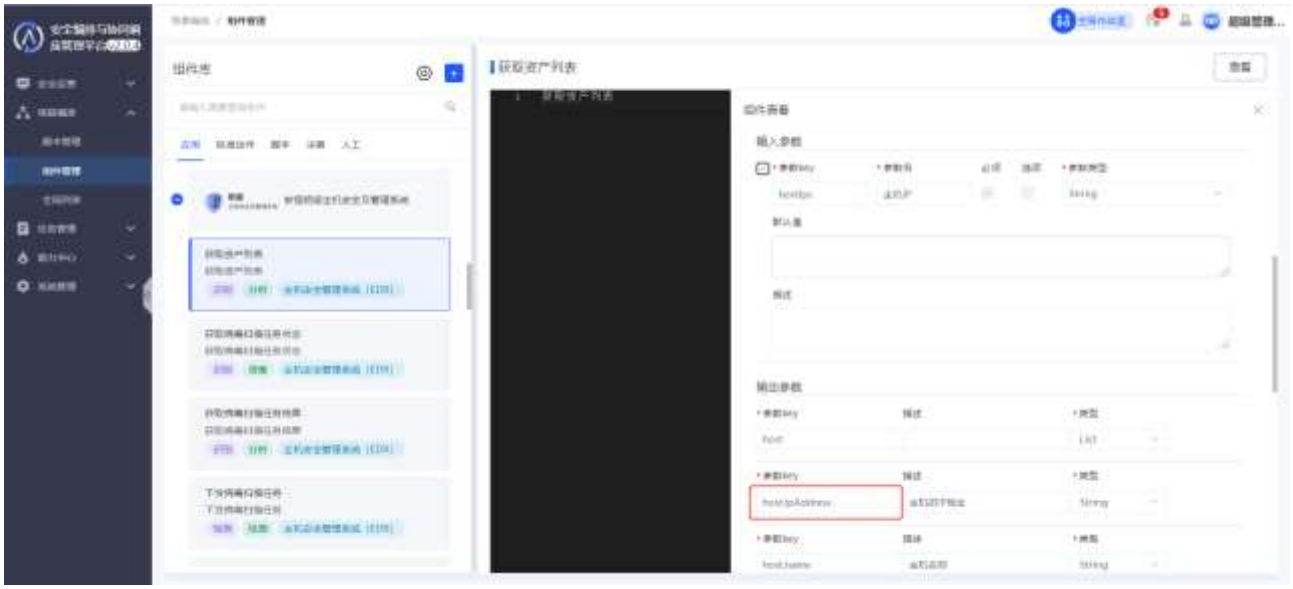
例：

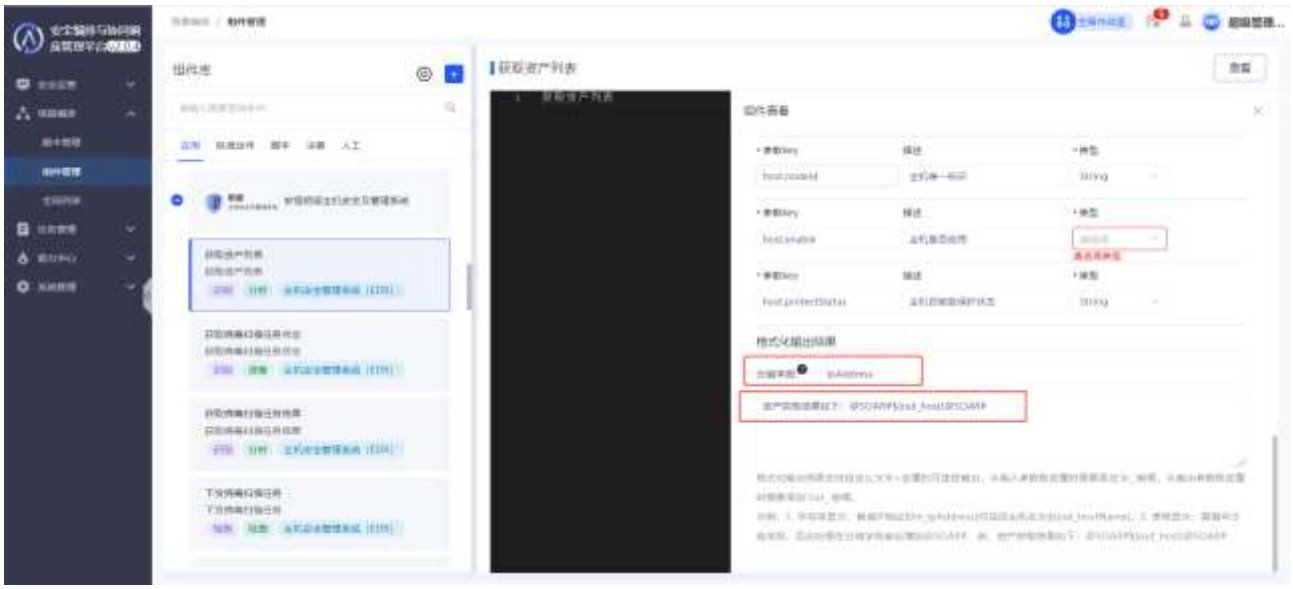
格式化输出结果填写说明：格式化输出结果支持自定义文本+变量的可读性输出，从输入参数取变量时需要添加'in_'前缀，从输出参数取变量时需要添加'out_'前缀。

分组字段：填写该字段后，该组件的格式化输出将按照该字段进行分组，最终以表格的形式展现。例：输出字段包括 host、host.ipAddress、host.name、host.protectStatus，则分组字段可填写 ipAddress，输出结果 host 可根据其中的 ipAddress 字段进行分组。

示例：1. 字符串显示：查询 IP 地址${in_ipAddress}对应的主机名为${out_hostName}。2. 表格显示：需填写分组字段，且此处需在输出参数字段前后增加@SOAR#，例，资产获取结果如下：@SOAR#${out_host}@SOAR#

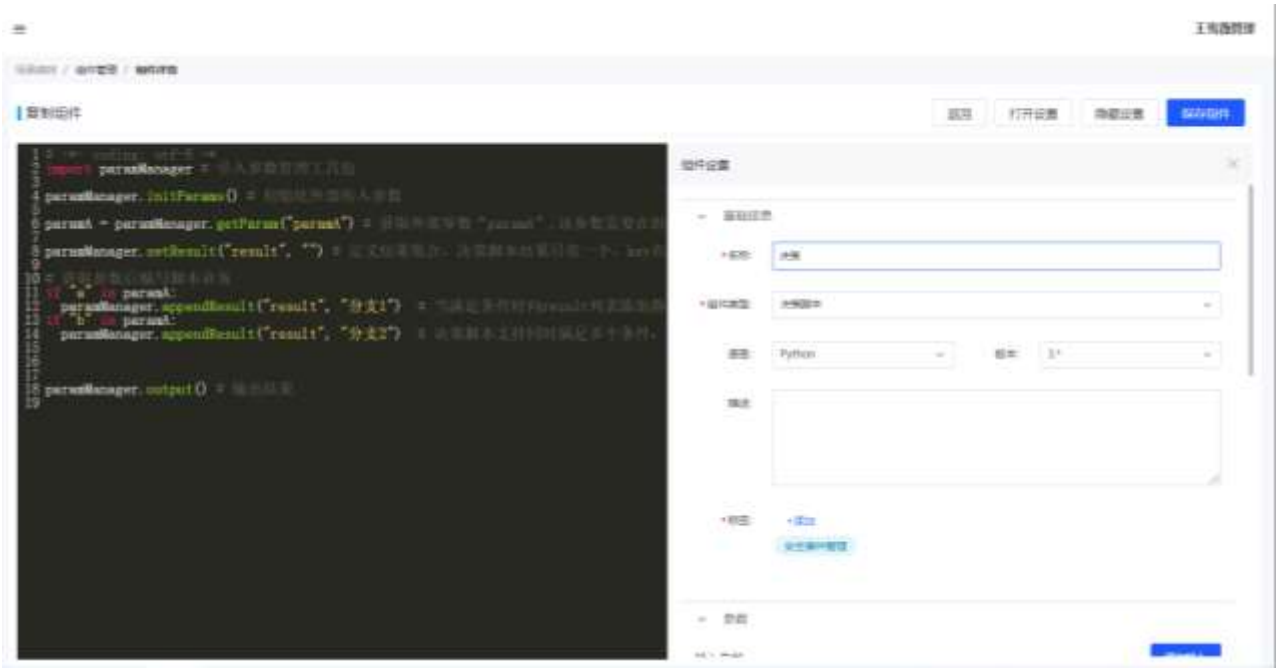
分组示例：可查看“获取资产列表”动作配置，输出 host 可根据 ipAddress 分组呈现。



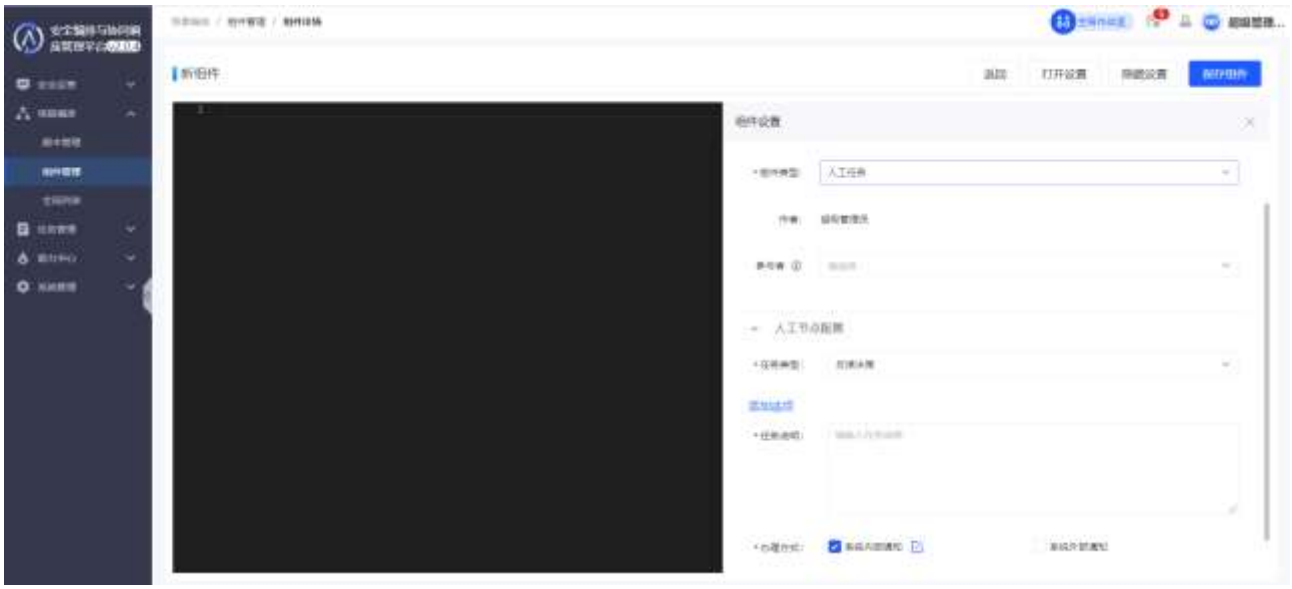


✧ **决策脚本**配置如下图所示，左侧可编写相应代码，右侧填写相关的配置信息。基础信息与参数填写同上。参数需填写输入参数、输出参数，其中输出参数可添加多个分支。

例：



✧ **人工组件**配置如下图所示，需在【组件设置】中填写相关的配置信息。基础信息填写同上。人工节点参数配置需选择任务类型，任务类型分为“反馈决策”、“反馈表单”、“反馈文本”；任务说明、办理方式。



任务类型配置如下：

若任务类型为“反馈决策”，点击 添加选项 ，配置决策选项，例：

若任务类型为“反馈表单”，点击 配置表单 ，进行表单的配置，例：

点击确定后，如下图所示：

若任务类型为“反馈文本”，则无需进行其他配置。

办理方式配置如下：系统支持两种办理方式：系统内部通知、系统外部通知

系统内部通知：支持指定系统内部成员办理该人工任务，每次下发该人工任务时，若无修改，则默认为该处指定的成员办理。勾选“系统内部通知”，点击<编辑>按钮，弹出“系统内部通知配置“框，如下图所示：

支持选择多个用户。若为空，则默认@所有人进行办理。

系统外部通知：支持系统外办理该人工任务。任务下发后，支持将该人工任务根据配置好的发送方式发送至指定的渠道进行办理，系统外办理结果将会反馈至平台。注：若要将任务发送至外网，需进入【系统管理】-【系统配置】进行“系统外办理地址“配置。详情见 9.9 系统配置

勾选“系统外部通知”，点击<编辑>按钮，弹出“系统外部通知配置“框，如下图所示：

发送方式：支持“发送邮件“、”发送到人“、”发送到群“；

执行设备：需进入【能力中心】-【设备管理】页面进行设备配置。发送邮件需安装“邮箱“APP 并接入设备；发送到人需安装” 钉钉应用工作通知“/” 企业微信应用工作通知“APP 并接入设备；发送到群需安装”钉钉机器人“/”企业微信机器人“等 APP 并接入设备。配置完成后，需选中一个健康设备进行发送。

其余信息请根据提示进行填写。

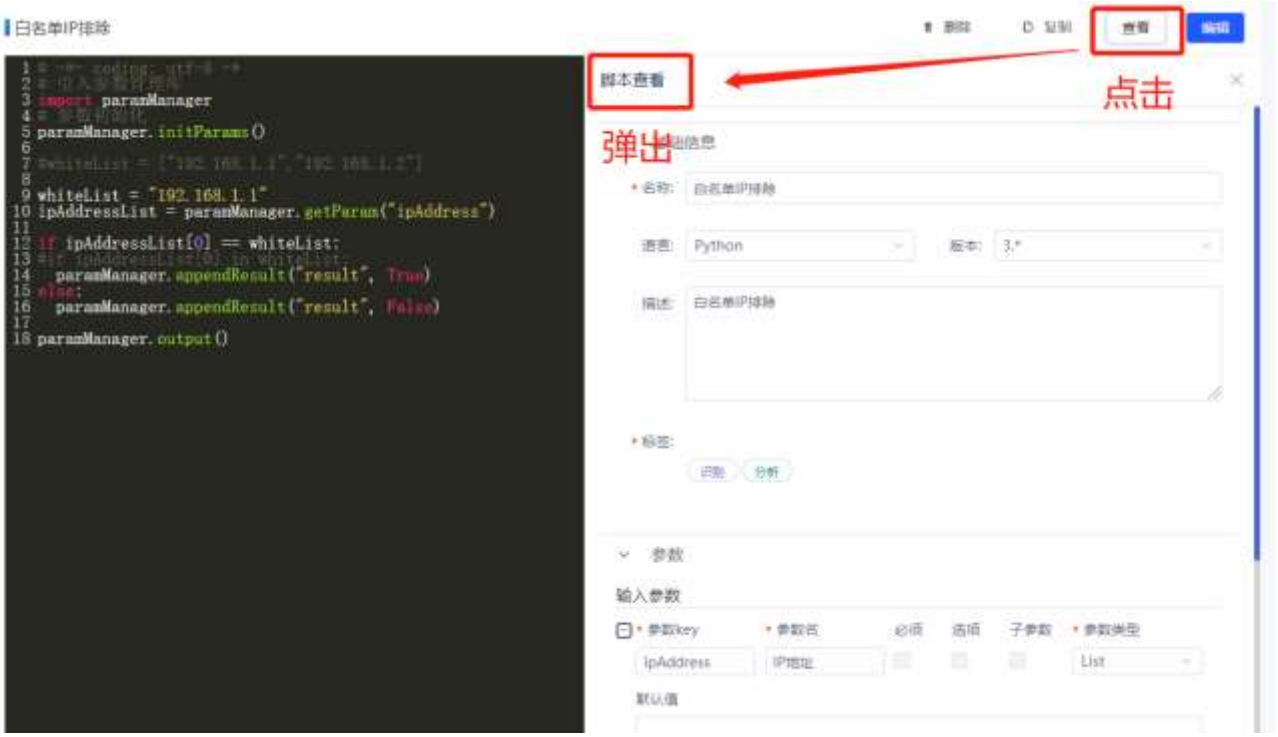
支持同时选中和配置系统内、外两种通知方式。

审批系统内、外通知配置与人工任务通知配置相同，不再赘述。

任务下发前，建议先进行试发送，以检测设备的可用性。设备不可用会导致系统外通知失败。

3、 组件查看

点击<**查看**>按钮，弹出**“脚本查看”**弹框，可查看当前选中脚本的详细设置信息，如下图所示：



4、 组件编辑

点击<**编辑**>按钮，可进行组件的编辑。子页面跳转至修改组件界面。编辑面板中显示未修改的组件。具体参数同“组件新建”。

5、 组件复制

点击图中<**复制**>按钮，可以实现当前组件的复制操作，同时子页面跳转至组件编辑界面，且组件的编辑面板上有复制好的组件内容。用户可继续进行组件内容的编辑。

6、 组件删除

点击<**删除**>按钮，弹出是否确认删除的对话框。点击<**确定**>按钮，可以删除当前脚本。

注：内置组件不可删除；被剧本引用的组件不可删除（若要删除需先删除相应的剧本）。

7、 组件搜索

点击 按钮，可对组件进行搜索。

8、 组件分组

分组标签与“系统管理”的“标签管理”相同，“标签管理”可手动添加自定义类型。

9、 组件排序

点击 按钮，可按名称或时间进行排序。

10、 组件导入

点击组件库【导入】按钮，可导入组件，如下图所示：

点击【导入】，进行组件导入操作，如下图所示：

点击【取消】或关闭，并刷新当前页面，即可看到导入的组件。

◆ 组件导入若名称重复，或 ID 重复，会创建新副本组件。

11、 组件导出

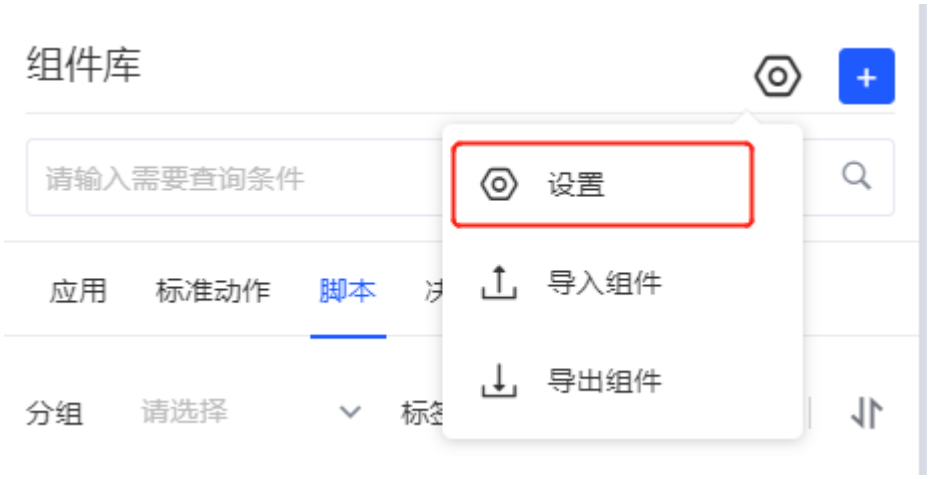
点击组件库【导出】按钮，可导出自定义组件，如下图所示：

点击导出组件，弹出以下组件导出框：

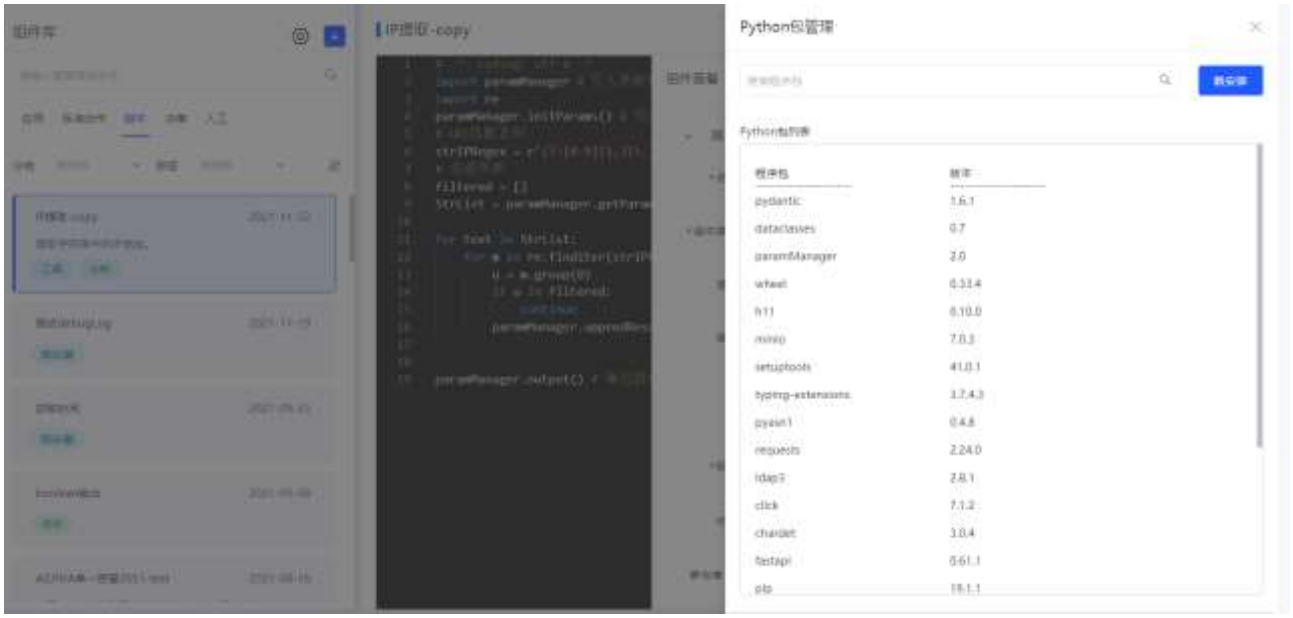
选择组件类型过滤出该类型的所有自定义组件，勾选需要导出的组件，点击【导出】，生成导出压缩包，或点击【全部导出】，可导出已选择类型的所有自定义组件。

12、 Python 包安装

点击【设置】按钮，可进行 python 包安装。

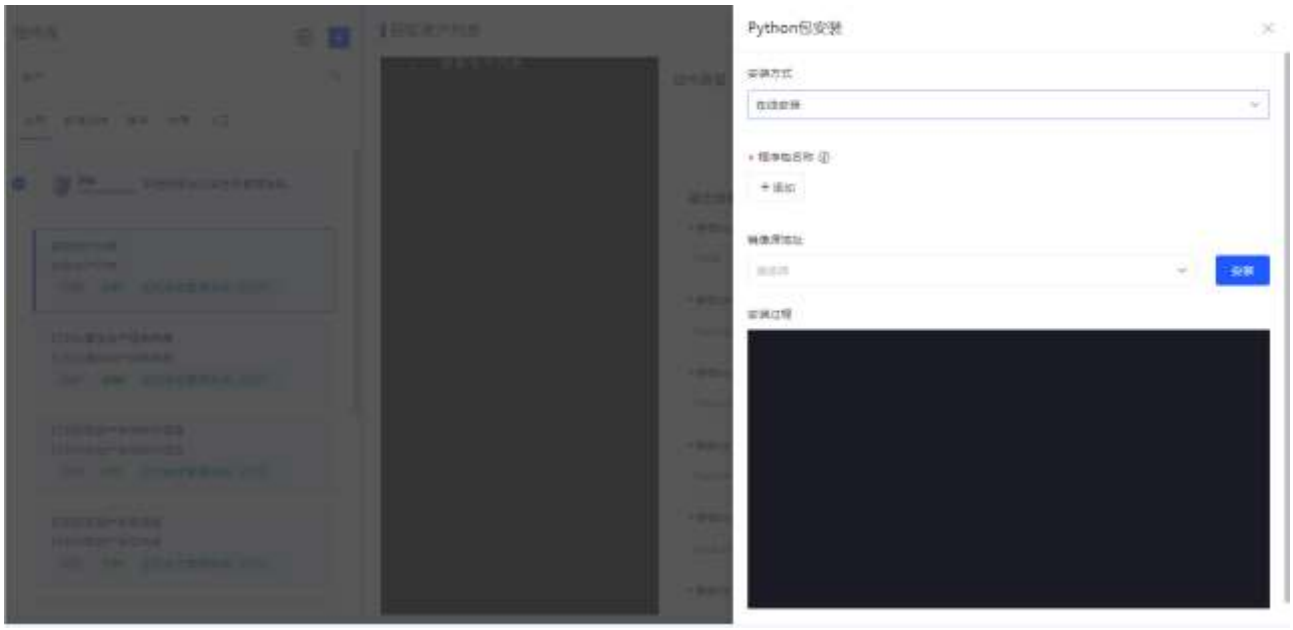


【python 包管理】页可查看当前平台已安装的所有 python 包列表，并支持搜索。



点击【新安装】，则可安装所需的 python 包，如下图所示：

可选择在线安装、在线安装 Requirements、离线安装三种安装方式。



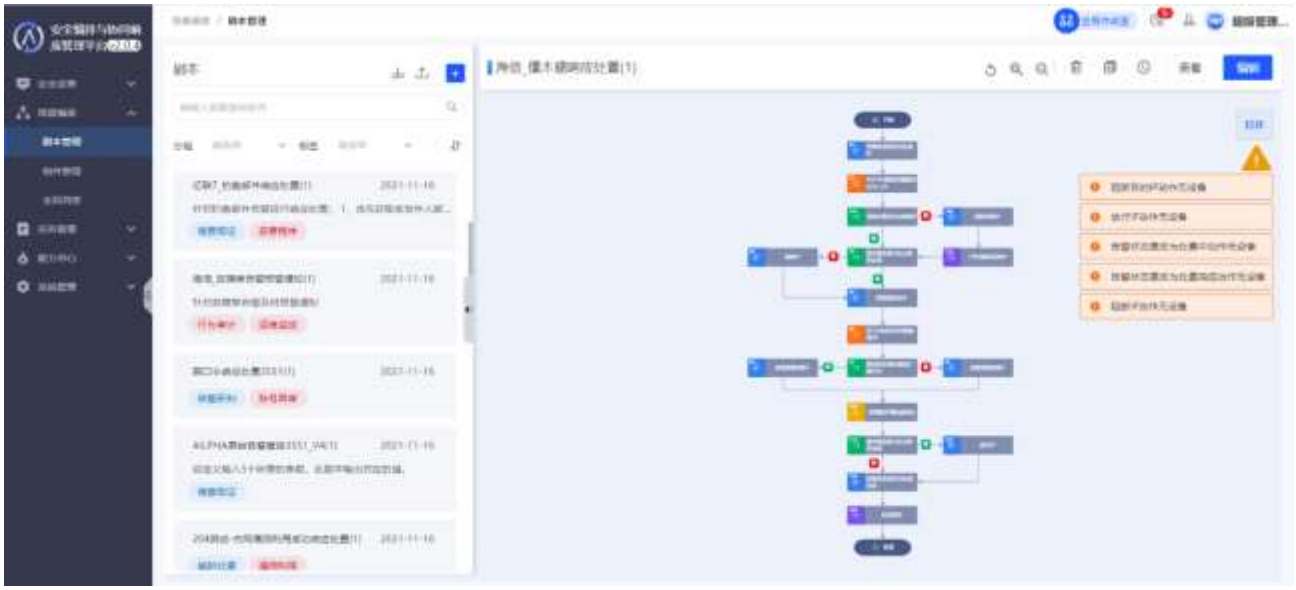
6.2 剧本管理

6.2.1 功能简介

剧本管理模块支持将不同类型组件进行流程化编排，支持子剧本与组件的灵活调用，通过合理配置参数实现自动化流程处置。系统内置丰富的剧本库，支持自定义剧本，从而实现系统剧本库的丰富化以及多样化，最终将用户的安全能力进行积累沉淀。该模块支持剧本的新建、编辑、查看、复制、删除、搜索、排序的操作。

6.2.2 区块概要

点击“**场景编排>剧本管理**”，进入剧本管理页面，如下图所示。



区块	说明	详细
剧本库	1）平台内置和用户创建的所有剧本列表 2）支持剧本的搜索、新建、导入、导出的操作。 3）支持剧本库的按标签分组、排序的操作。 4）支持查看剧本的状态：草稿/发布。	
剧本查看/编辑面板	1）点击剧本库列表的某个剧本，面板显示该剧本的详细内容 2）支持剧本的查看、复制、删除、编辑等操作。	

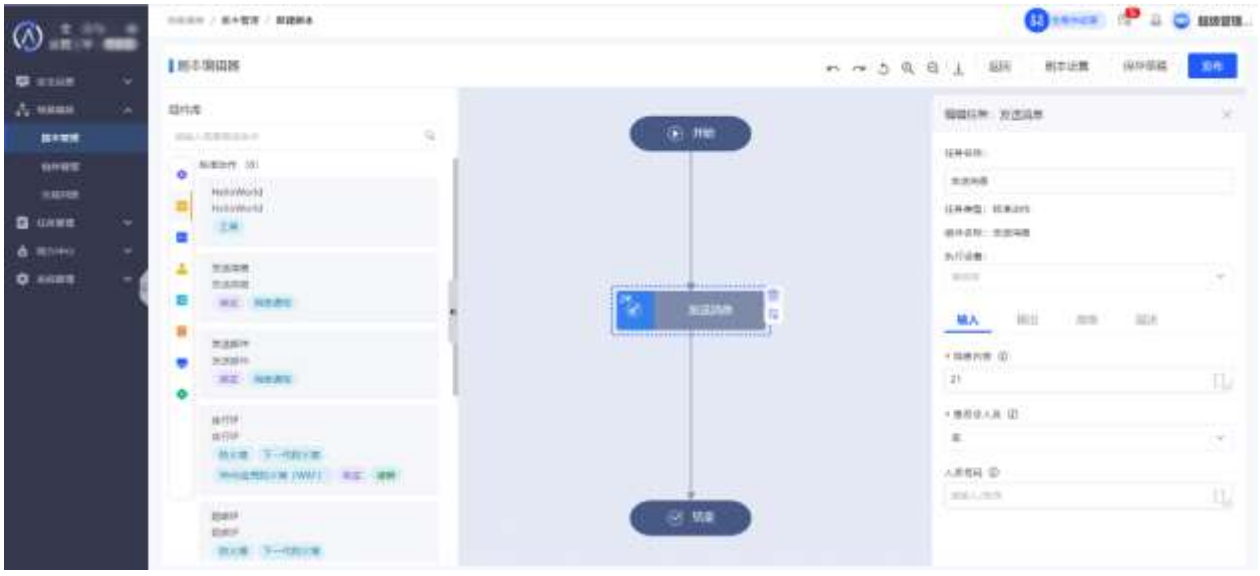
详情如下：

1、 剧本新建

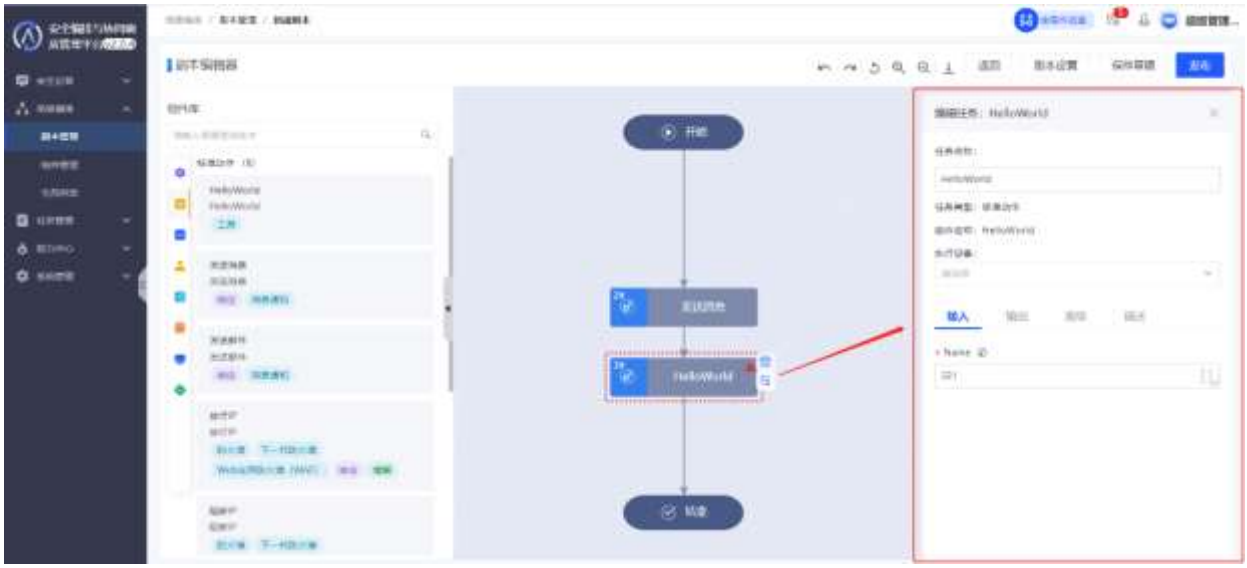
点击剧本库 按钮，可以新建剧本。可拖拽左侧组件库列表至剧本编辑面板中，拖拽出的组件会根据拖

拽顺序进行编号，方便重复组件的区分。支持对拖拽出的组件进行参数缺失、无 APP、无设备检验。如下图所示：

点击下图中每个子组件的 按钮，可将每个组件进行连接形成剧本流程图，点击<删除>，可将该组件删除。如下图所示：

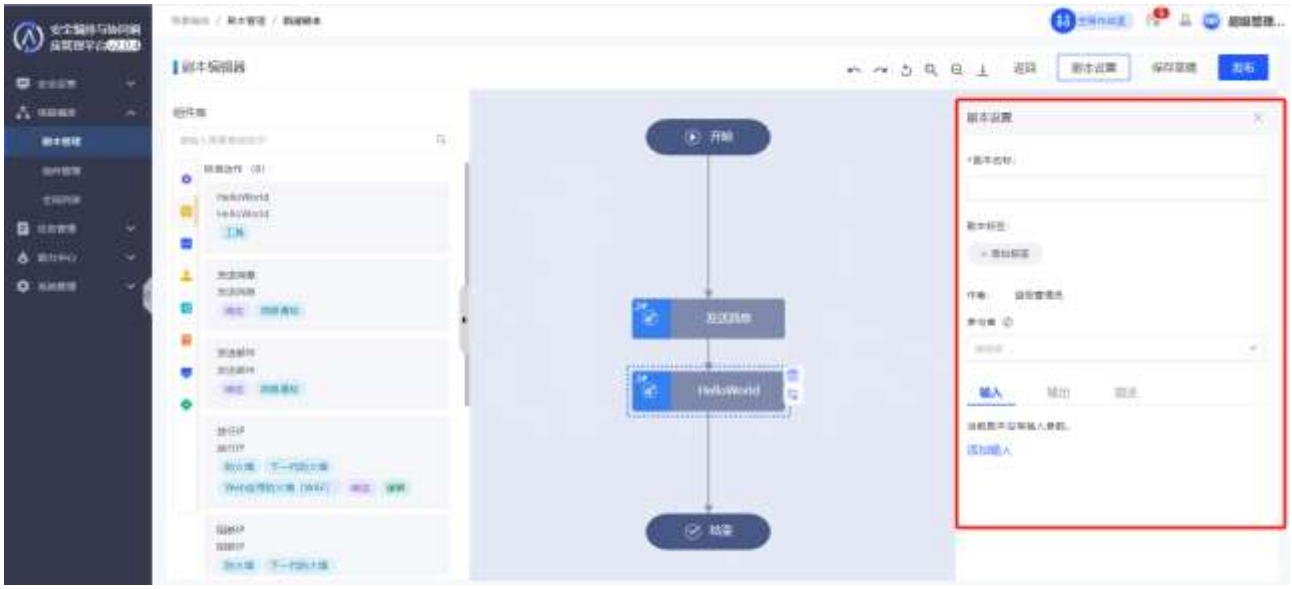


点击每个组件进行配置，填写输入、输出参数（配置详情见 6.2.3 小节），填写的信息系统会自动保存：



对每个组件配置完毕之后，填写剧本相关的参数，点击<**保存草稿**>/<**发布**>，即可在剧本列表中看到刚刚保存好的剧本。剧本设置如下图所示：

包括剧本名称、剧本标签、剧本参与者、剧本输入、输出、描述。



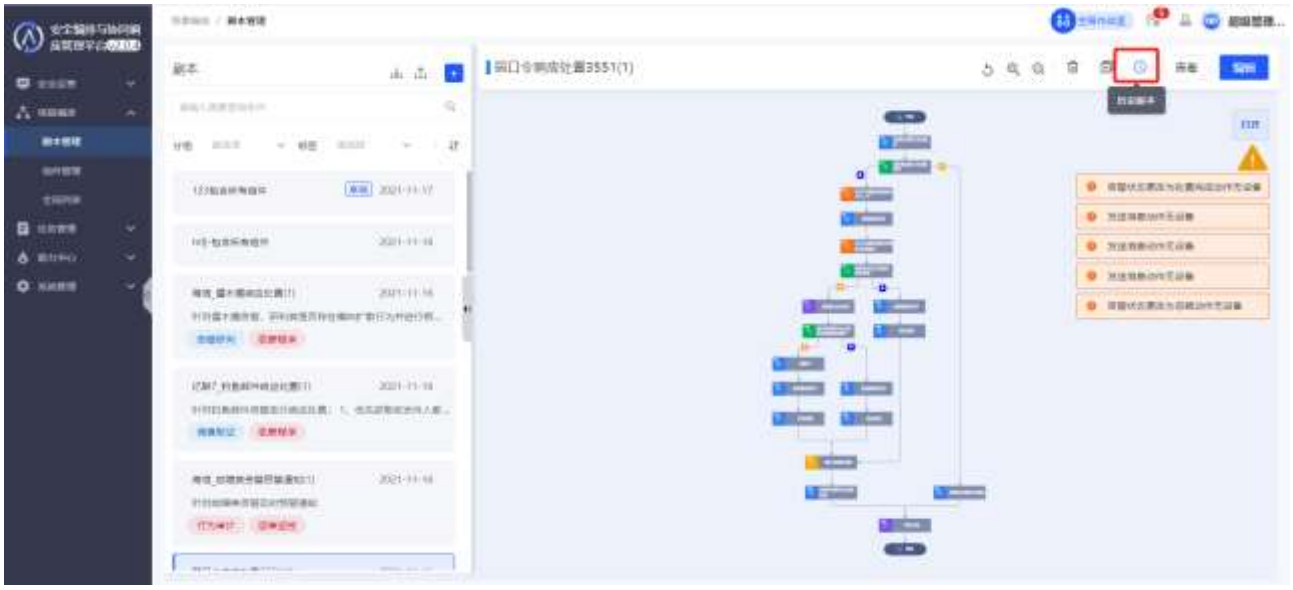
2、 剧本保存/发布

点击<**保存草稿**>按钮，可将当前内容保存成剧本草稿，草稿将不会被运行，也不会被保存成版本。

点击<**发布**>按钮，可将当前剧本内容发布成为剧本的一个版本，当在作战室中执行剧本时，执行内容为剧本的最新版本内容。

3、 剧本的历史版本

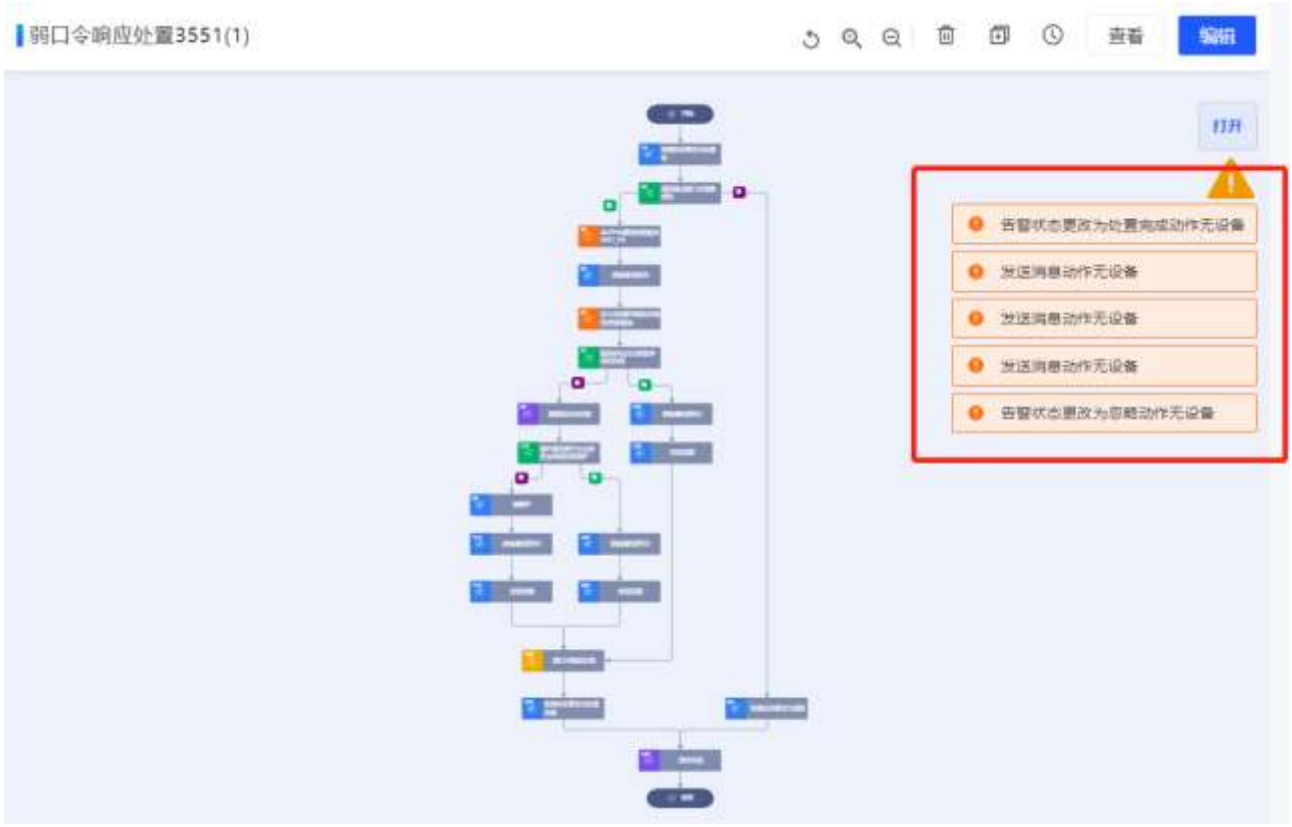
点击<**历史版本**>按钮，可查看当前剧本的所有历史版本信息。



点击<**预览**>，可查看历史版本的具体内容；点击<**重新载入**>，则可重新载入选中的版本，并进入剧本编辑模式进行编辑(若您想执行历史版本，需重新载入后进行重新发布，方可作为最新版本执行)；点击<**删除**>，可将选中的剧本版本内容进行删除。

4、 剧本查看

剧本查看页面，可查看剧本中无设备的动作，如下图所示：



点击<**查看**>按钮，弹出**“剧本查看”**框，可查看当前选中剧本的详细设置信息，如下图所示：

点击不同组件可查看组件的配置信息。

5、 剧本编辑

点击<**编辑**>按钮，可进行剧本的编辑。子页面跳转至修改剧本界面。编辑面板中显示未修改的剧本。

6、 剧本复制

点击图中<**复制**>按钮，可以实现当前剧本的复制操作，同时子页面跳转至剧本编辑界面，且剧本的编辑面板上有复制好的剧本内容。用户可继续进行剧本内容的编辑。

7、 剧本删除

点击<**删除**>按钮，弹出是否确认删除的对话框。点击<**确定**>按钮，可以删除当前剧本。

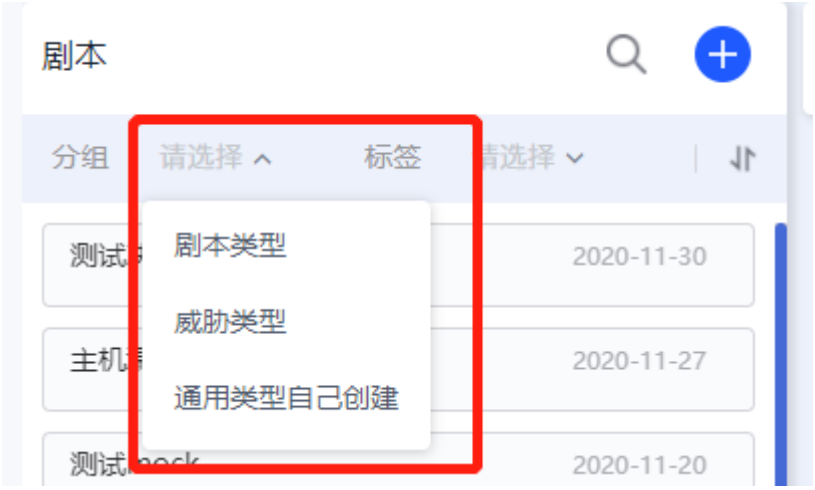
注：内置剧本不可删除。

8、 剧本搜索

点击  按钮，可对剧本进行搜索。

9、 剧本分组

分组标签与“系统管理”的“标签管理”相同，“标签管理”可手动添加自定义类型。



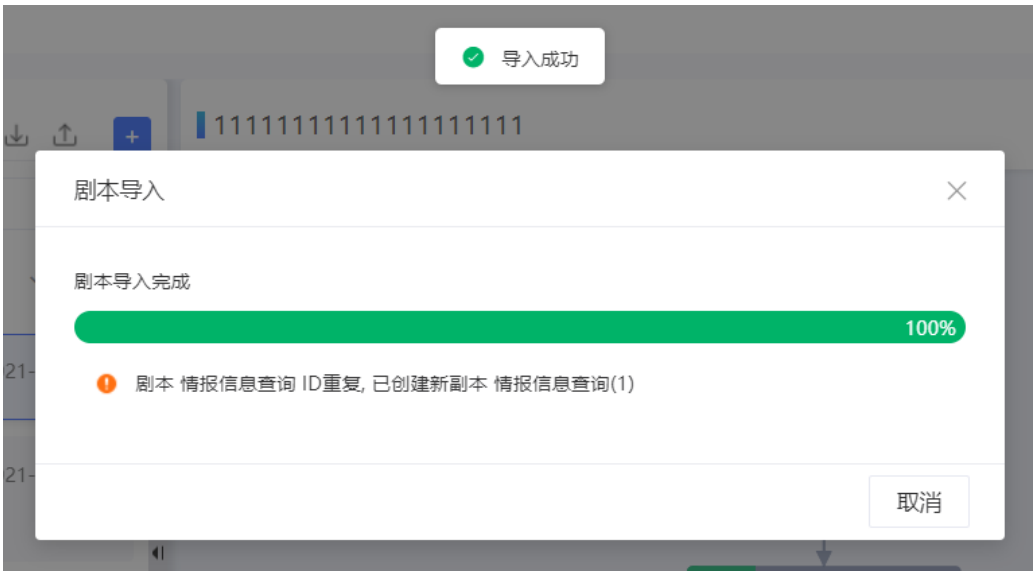
10、 剧本排序

点击 按钮，可按名称或时间进行排序。

11、 剧本导入

点击剧本管理【导入】按钮，可导入组件，如下图所示：

点击【导入】，进行剧本导入操作，如下图所示：



刷新当前页面，即可看到导入的剧本。

◆ 剧本导入若名称重复，或 ID 重复，会创建新剧本。

12、 剧本导出

点击剧本管理【导出】按钮，可导出自定义剧本管理，如下图所示：

点击导出剧本，弹出以下剧本导出框：

点击【全部导出】，则自动导出所有自定义剧本。

勾选需要导出的剧本，点击【导出】，生成导出压缩包。

6.2.3 剧本配置详细说明

1. 剧本配置

剧本配置框如下所示：

详情：

- 剧本名称：填写该剧本的名称，为必填项。
- 剧本标签：可在“剧本类型“、”威胁类型“、或自定义类型标签组（在**系统管理>标签管理**中进行配置）中选择符合该剧本的标签。
- 设置为默认剧本：对应不同的事件类型，可选择该剧本是否其作为默认剧本，默认剧本可被自动触发。
- 输入参数：需填写该剧本入参的字段名称，添加输入参数的描述。填写方式如下图所示：

若非事件自动触发，则可在左侧输入框中输入自定义名称。若为事件触发，也可点击上图红框内的“[ ]“按钮，弹出如下框图，可选择系统内置的相关事件字段。选择字段弹框如下所示，可输入关键字进行搜索：

- 输出参数：配置同输入参数。
- 描述：添加该剧本的相关描述语言。方便用户调用相关剧本。

2. 人工任务配置

人工任务组件配置框详情如下图所示：

详情：

将“自定义人工节点”拖拽至右侧画板后，人工任务需要进行配置。配置内容可见 6.1.2 小节中的人工任务配置部分。

若将其他人工任务拖入，则仅需要配置办理时间、办理方式，其他输入框内容为创建组件时的配置，不可更改。

办理时间：支持填写小时、分钟；即该任务从下发开始计时，超过填写的时间段则视为任务办理超时。

3. 子剧本配置

子剧本组件配置框详情如下图所示：

详情：

剧本作为子剧本时，原剧本的输入参数和输出参数均可配置，输入参数可手动输入值，也可选择字段。

输出参数可作为字段被其他组件所引用，如下图所示：

4. 网关配置

目前系统内置并行网关和等待节点网关。并行网关的下级任务节点为并行执行，需要 2 个并行网关进行闭合，两个并行中间的任务节点是并行逻辑；等待节点可进行时间设置，时间单位可选择小时、分钟、秒。

并行网关详情页面：

例：如下图所示，该剧本中有 AA'和 BB'两条分支，如果 AA'线路比 BB'线路运行的快，则并行网关可以控制两条线路都执行完毕，再执行下一步的 C 节点。

等待节点网关详情页面：

5. 脚本配置

普通脚本组件配置框详情如下图所示：

详情：

不同脚本组件的输入输出参数不同，需根据组件进行相关配置。

6. 决策配置

决策组件配置框详情如下图所示：

详情：

决策脚本可选择红框中的**<常规>、<脚本>**单选按钮，若为**<脚本>**，则执行的是组件的脚本内容，输入参数可配置，且可选择其他决策组件作为脚本执行。

若为**<常规>**决策，输入参数可手动添加，可为该组件添加决策信息，包括决策结果和表达式的配置，配置详情如下所示。

普通决策表达式的配置如下所示：

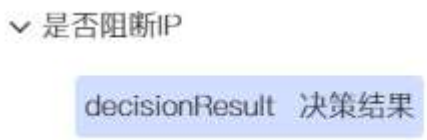
假设有以下剧本流程：人工组件**[是否阻断 IP]** → 决策组件**[决策组件示例]** → 阻断 IP/发送消息

其中，人工组件**[是否阻断 IP]**的反馈决策的结果可作为决策组件**[决策组件示例]**的输入，可根据该输入进行决策结果的配置。例：若人工组件反馈结果为 yes，则决策结果为阻断；若反馈结果为 no，则决策结果为不阻断。

点击**<添加决策>**按钮，可为该组件添加常规决策信息。决策结果可手动输入。表达式配置如下所示：

- 点击表达式输入框的“**[ ]**“按钮，可进行表达式的配置，详情如下：

- 左方红框内按钮可选择人工组件的反馈结果字段：



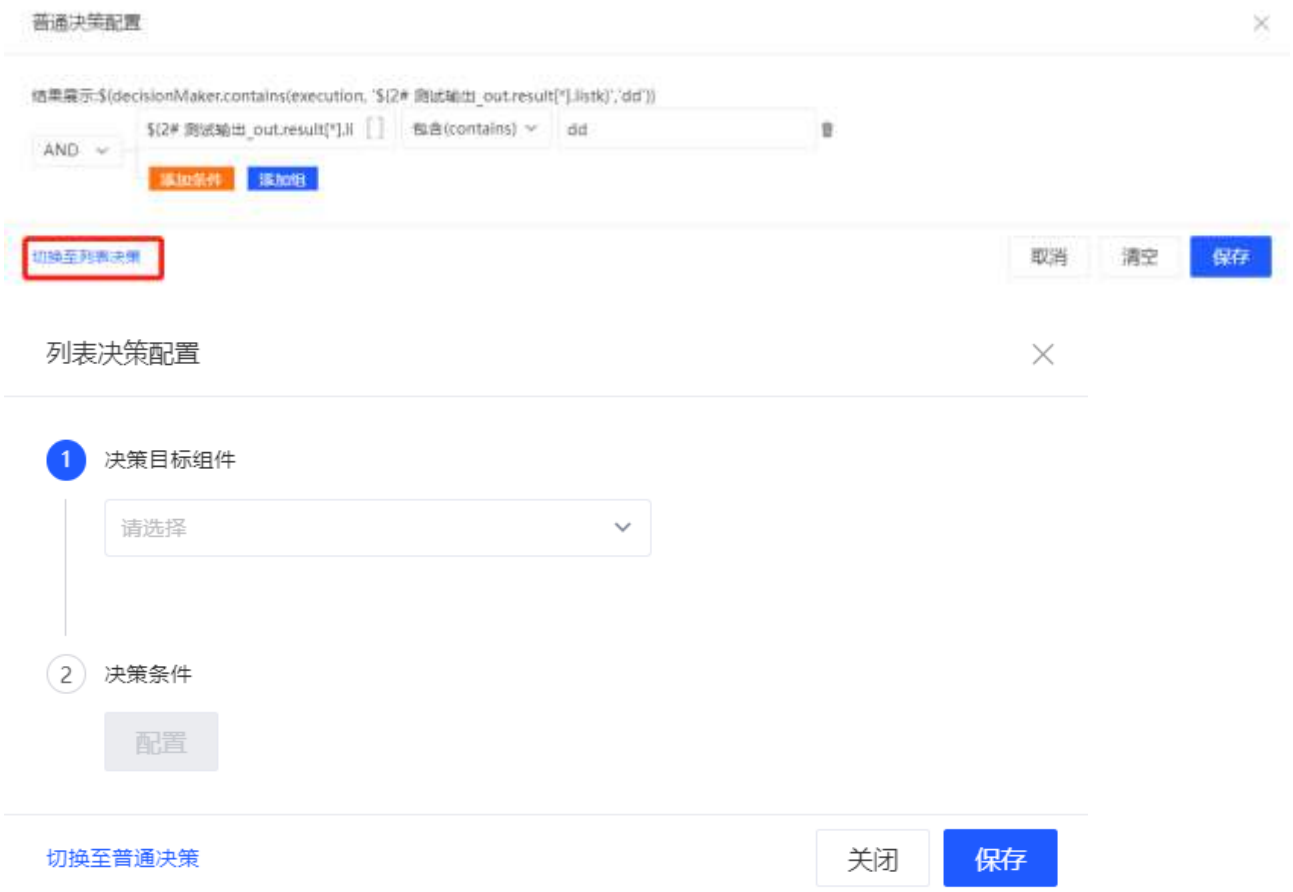
- 判断条件可选择等于、不等于、包含等等。

- 右侧输入框可填写反馈结果的具体值。

列表决策表达式的配置如下所示：

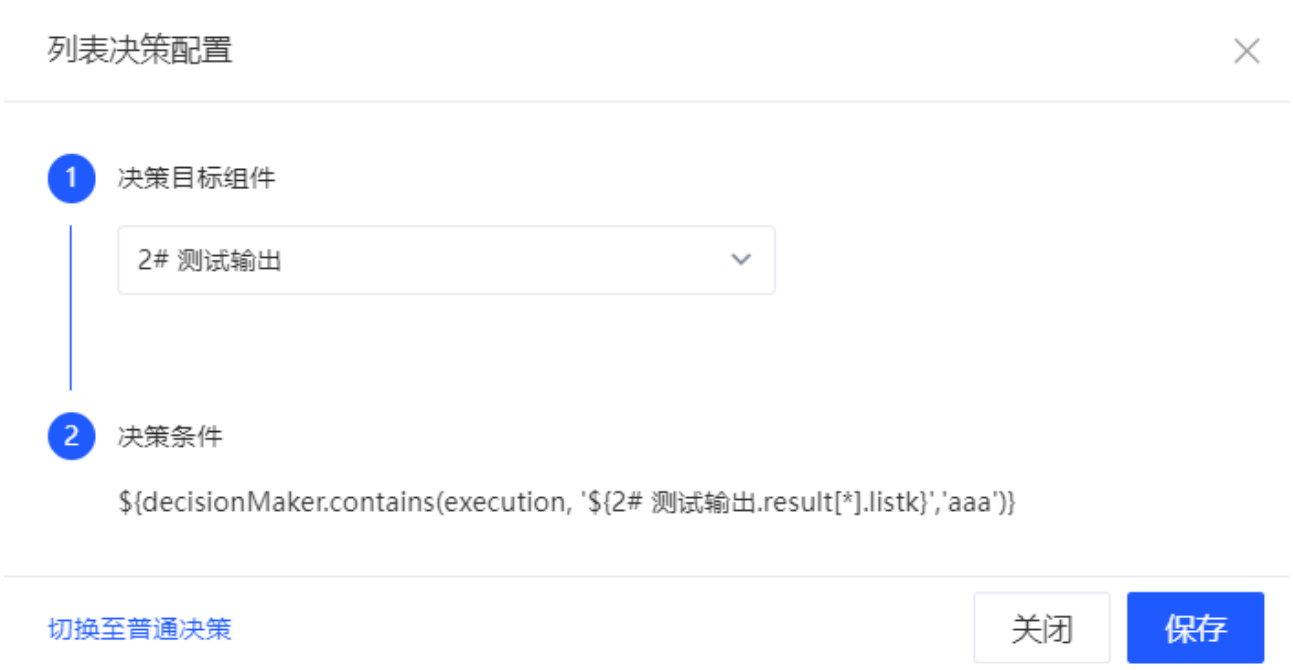
说明：列表决策支持对输入的列表参数进行分流。例如下图中的“测试输出“组件，输出 DataList，DataList 中包含多个对象，该输出作为决策组件的输入。若决策配置使用列表决策，可分裂出多个新的符合条件的 DataList 组合，不同的决策的下游节点，只能获取组件该路径下过滤出的新 DataList 上下文信息。

点击“[]“按钮，弹出决策配置框，点击<**切换至列表决策**>，可切换至列表决策配置框，如下图所示：



第一步：选择目标组件，此处选中“测试输出“组件。(此处仅可选择单一组件)

第二步：配置决策表达式，此处配置输出结果的对象中 listk 字段包含“aaa“。配置成功后如下图所示：

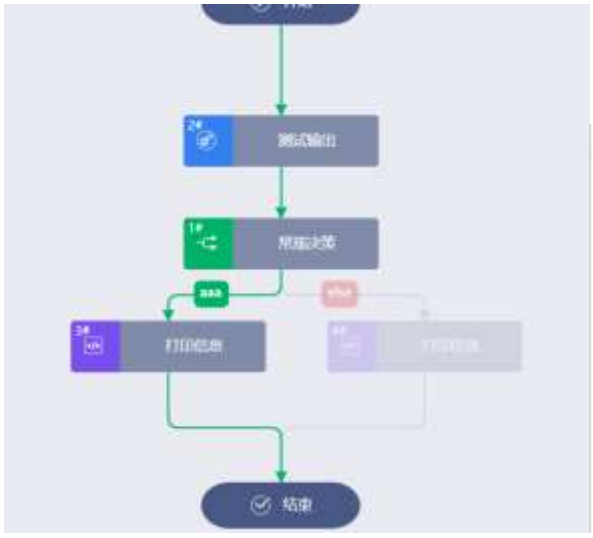


运行情况如下：

“测试输出“组件的输出参数中包含 listk：["aaa","bbb","ccc"]和 listk：["dd","ee"]，如下图所示：


```
{
    "result":[
        {
            "intk":1,
            "boolk":true,
            "datek":"2021-11-22T07:50:51.609+00:00",
            "listk":[
                "aaa",
                "bbb",
                "ccc"
            ]
        },
        {
            "intk":2,
            "boolk":false,
            "datek":"2021-11-22T07:50:51.610+00:00",
            "listk":[
                "dd",
                "ee"
            ]
        }
    ]
}
```


则满足条件的为["aaa","bbb","ccc"]所在的对象，如图所示“打印信息“成功打印出了该结果。



注：下游组件的输入也可选择["aaa","bbb","ccc"]所在对象的其他字段（比如 intk、boolk、datek）。

快去平台上自己动手试试吧！~~

7. 标准动作配置

标准动作组件配置框详情如下图所示：

详情：

不同标准动作组件的输入输出参数不同，需根据组件进行相关配置。

8. 失败忽略配置

支持组件失败忽略配置，组件配置页面点击【高级】，可打开、关闭失败忽略开关，开启后当组件运行失败时不会终止流程。关闭后，组件失败则剧本流程终止。

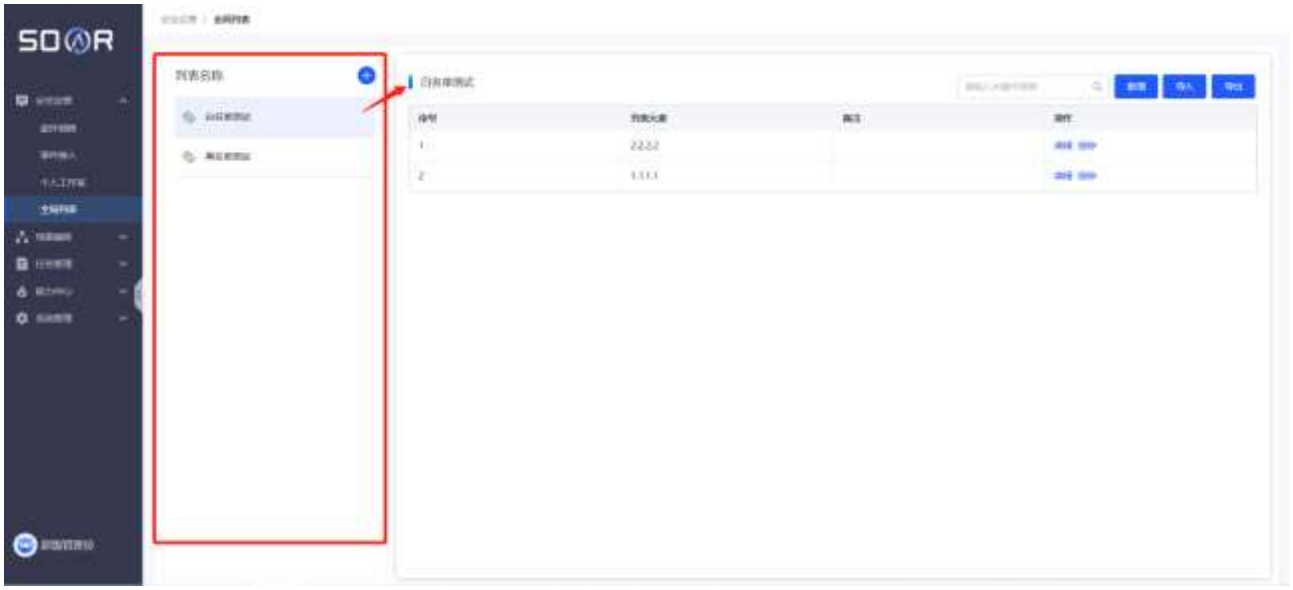

编辑任务：修改案件级别
任务名称：
修改案件级别
任务类型：内置
组件名称：修改案件级别
输入
输出
高级
描述
失败忽略
关

6.3 全局列表

6.3.1 功能简介

全局列表模块可对在剧本编排中被引用的全局元素进行汇总管理，也可单独对某一类使用频率较高的元素进行管理。本模块支持手动添加全局列表及单个全局元素，也支持批量导入全局元素，除此之外，【场景编排】➤【组件管理】中的“添加全局元素”和“删除全局元素”也支持在运行剧本时自动化的添加或删除某个全局元素。

进入“**场景编排➤全局列表**”页面，页面详情如下图所示：



左侧为全局列表名称，点击某个全局列表可在右侧板块中查看该列表中的所有全局元素。

6.3.2 功能详解

1、 添加全局列表

点击左侧【列表名称】栏的【+】按钮，可增加全局列表，如下图所示：

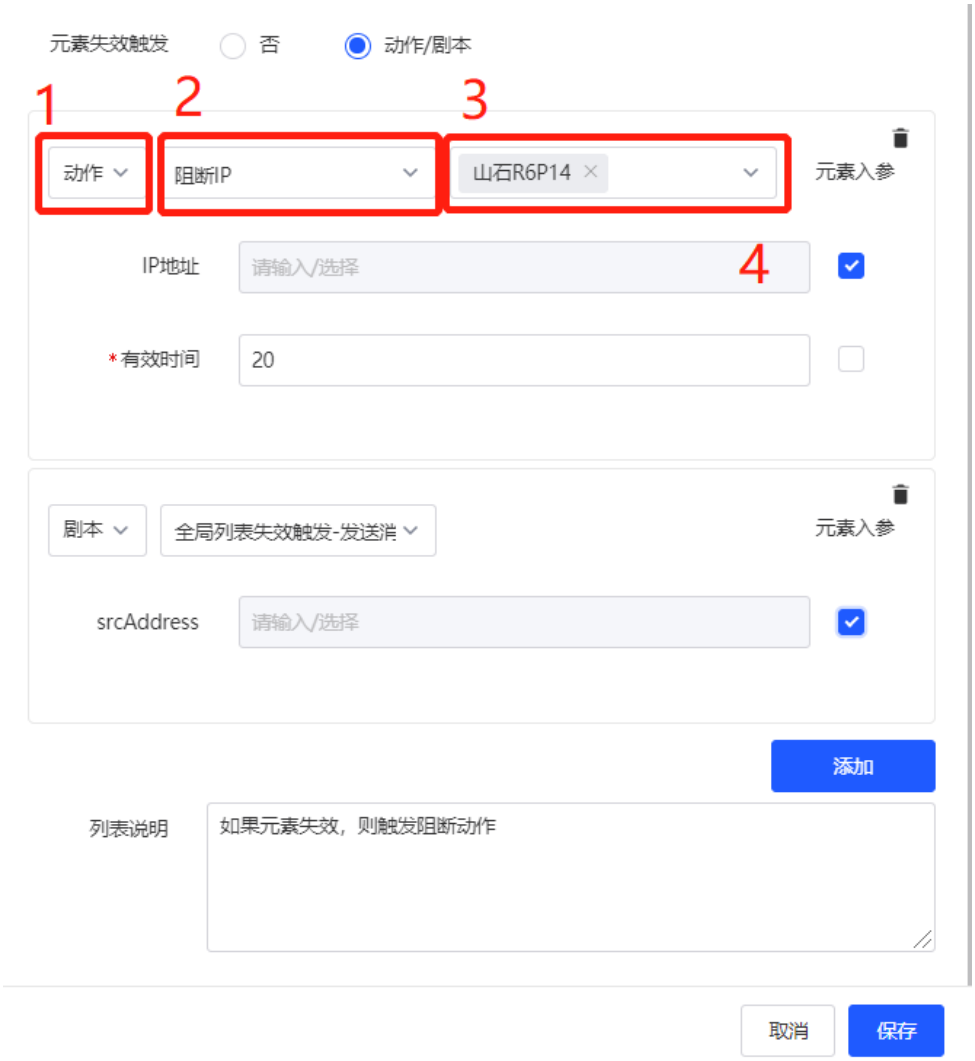
列表名称：必填，不可重复，只支持英文、中文、数字和下划线；

列表类型：必填，可下拉选择“字符串”或“IP”；

元素失效触发：默认为“否”，单选，可选择“否”或“动作/剧本”。如果选择“否”，则该列表下的元素在失效时不触发任何动作或剧本；如果选择“动作/剧本”，则该列表下的某些元素在指定时间失效之后，即触发相应的动作或剧本（注：全局元素中会指定单个元素失效时间）。

选择“否”，如下图所示：

选择“动作/剧本”，如下图所示：



图中 1 下拉框可选择剧本或动作，图中 2 下拉框可选择平台现有的剧本或动作，图中 3 下拉框可选择动作执行的设备标签，如果剧本或动作有输入参数，则可选择当前全局元素作为其中的一个入参（如图中 4，可勾选某个入参输入框后的复选框来确定），必填参数需填写。

列表说明：可填写对该全局列表的相关详细说明。

点击【保存】，即可保存以上信息；点击【取消】，则返回全局列表页面。

鼠标悬浮至某个全局列表名称，显示【编辑】、【删除】按钮。

编辑全局列表：点击【编辑】按钮，弹出列表信息框，可对当前列表信息进行编辑。

删除全局列表：点击【删除】按钮，可删除当前全局列表。

2、 添加全局元素

点击需要添加元素的某个全局列表，点击右上角的【新增】按钮，弹出【元素信息】弹框，如下图所示：

元素类型：必选，若当前列表类型为字符串，则元素类型可选项为字符串全匹配、字符串前缀、字符串后缀、正则表达式；若列表类型为 IP 类型，则元素类型默认为 IP 地址，可选项为 IP 地址区间、子网掩码、IP 地址；

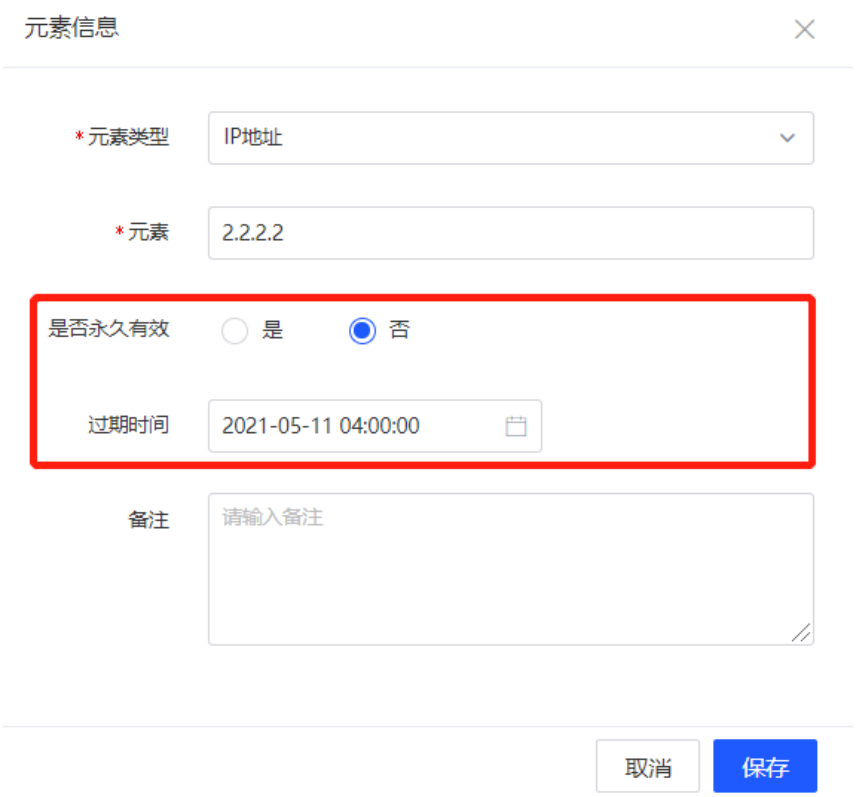
元素：必填，根据不同的元素类型进行填写；

是否永久有效：默认为“是”，单选，可选项为“是”、“否”。

若选择“是”，则表示元素永久有效；

若选择“否”，则需选择该元素的过期时间，则表示该元素在该时间点之后失效（如过期时间为 2021-3-10

12：00:03，则在 2021-3-10　12：00:04 元素在当前列表失效，自动被删除且触发“元素失效触发”绑定的相应的动作)。

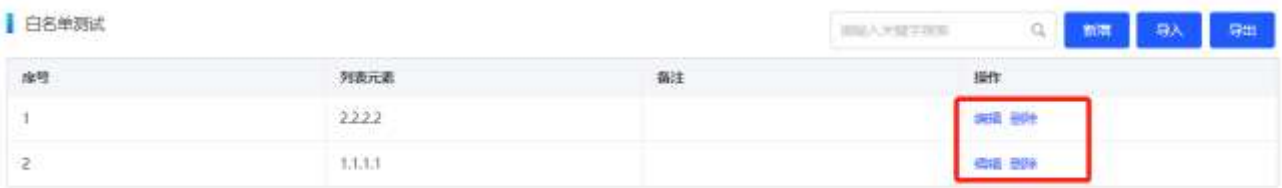


备注：可填写有关该元素的相应备注。

点击【保存】，信息填写无误则可成功添加该元素；点击【取消】，则页面返回至【全局列表】。

点击全局元素操作栏中的【编辑】按钮，即可对该元素进行编辑；

点击全局元素操作栏中的【删除】按钮，即可删除当前元素，如下图所示：



3、 有效时间说明

全局元素存在有效时间，在【元素信息】【是否永久有效】中进行配置。元素可永久有效。

该元素所在的全局列表可设置元素失效触发的剧本/组件。若选择了某些剧本/组件，则该元素失效时将会立即触发。

4、 批量导入、导出全局元素

点击【导入】，弹出【导入元素】框，如下图所示：

点击【下载模板】，可下载导入元素的 excel 模板，可直接在模板上进行修改。

导入模式：可选项为增量导入、覆盖导入。增量导入重复的元素不再重复添加；覆盖导入则将覆盖当前全局列表元素。

附件上传：可选择需要导入的文件。

点击【导入】，则可进行元素批量导入。

点击【导出】，即可下载当前全局列表元素。

5、 搜索

可支持对元素名称进行模糊搜索。

6、 内置组件自动添加、删除全局元素说明

【场景编排】中有两个内置组件可通过剧本编排自动化添加删除全局元素。

【添加全局元素】组件：

元素：需要添加的元素

列表名称：需要添加到的全局列表名称

元素类型：可下拉选择，需与已选的全局列表类型保持一致

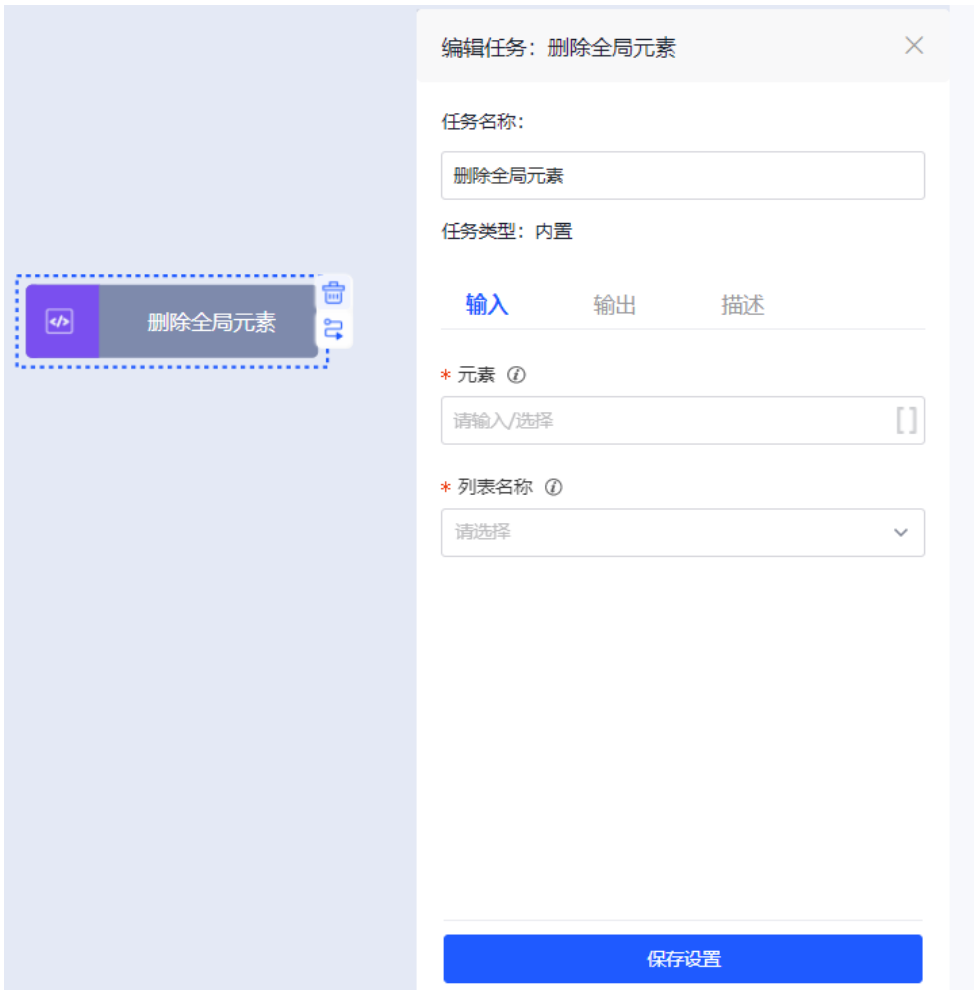
有效时间：不填即永久有效；填写时间单位默认为分钟，注意只可填写数字

备注：可填写对该元素的描述语言。

【删除全局元素】组件：

元素：需要删除的元素

列表名称：该元素所在的全局列表名称。


删除全局元素
编辑任务：删除全局元素
任务名称：
删除全局元素
任务类型：内置
输入
输出
描述
* 元素
请输入/选择
* 列表名称
请选择
保存设置

7. 任务管理

7.1 任务管理

7.1.1 功能简介

任务管理模块可以设置剧本的触发方式，包括事件触发（当系统监测到选中的事件发生时，则触发绑定的剧本），定时周期，定时单次（比如需要设置定期扫描等任务，可选择定时触发方式）三种，通过不同的触发方式触发绑定的剧本从而产生不同类型的案件。

7.1.2 功能详解

进入“**任务管理➢任务管理**”页面，查看任务页面，如下图所示。分为任务统计，新增任务，任务列表及管理三个区块。

1、 任务统计

可查看总任务数，正在运行中的任务数，已停止的任务数，触发方式为定时周期、定时单次、事件触发的任务数。

2、 新增任务

点击【**创建任务**】按钮，弹出“任务信息”对话框，进行任务相关参数的配置。

填写新建的任务名称，任务类型，cron 表达式（运行时间周期），开始时间，结束时间。以及该任务触发生成案件的相关信息，包括案件类型、案件级别、默认需要执行的剧本、案件归属人、案件参与角色和参与人。

任务名称：填写该任务的名称。

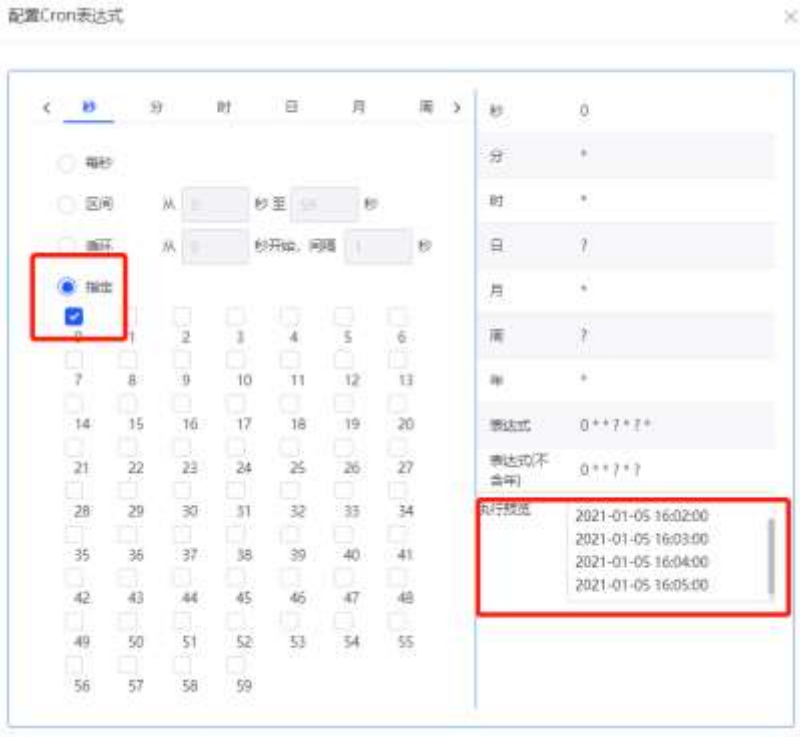
任务类型分为下面三种：

- a.定时周期，即每个周期内执行一次任务。

其中，cron 表达式配置如下所示：

cron 表达式需分别配置秒、分、时、日、月、周、年。

例：如果需要设置每分钟执行一次，则配置如下：



- b.定时单次，即指定某个时间执行任务。

- c.事件触发，即当检测到有相关事件则触发任务。

数据来源：选择已经配置好的事件源即可；

数据过滤：与【事件源】中“事件过滤“填写方式相同；

合并字段&合并时间：需指定**合并字段**及**合并时间**（即去重时间），当后入的事件在去重时间范围内，存在指定字段内容相同的案件时，事件不触发剧本，合并入相关案件。去重条件支持多个字段。**例如**选择：eventname、srcAddress，指定合并时间为 10 分钟，那么当第一条案件产生后，10 分钟内所有 eventname 与 srcAddress 相等的事件都合并入该案件。超过 10 分钟后产生新的案件，以此类推。

案件类型：选择触发后生成案件的类型；

案件级别：选择生成案件的级别；

归属人：选择生成案件的归属人；

参与角色：选择生成案件的参与角色；具备该角色的用户均为该案件的参与人；新增该角色的用户也会自动加入该案件参与人中；

参与人：选择生成案件的参与人；参与人可查看并在该案件作战室中进行协同作战；

剧本：选择生成案件后需要执行的剧本；注：若为事件触发方式，则此处可不选择剧本，若该案件类型绑定了默认剧本（系统管理—事件类型中进行绑定），且此处未选择剧本，则该案件生成后会自动执行默认剧本，否则不执行任何剧本。

3、 任务启用/禁用

点击 

按钮，启用任务，任务运行并根据触发条件产生相应的案件。点击 

按钮，禁用任务，任务停止，相关案件停止产生。

4、 任务删除

点击  按钮，删除该任务。

5、 任务编辑

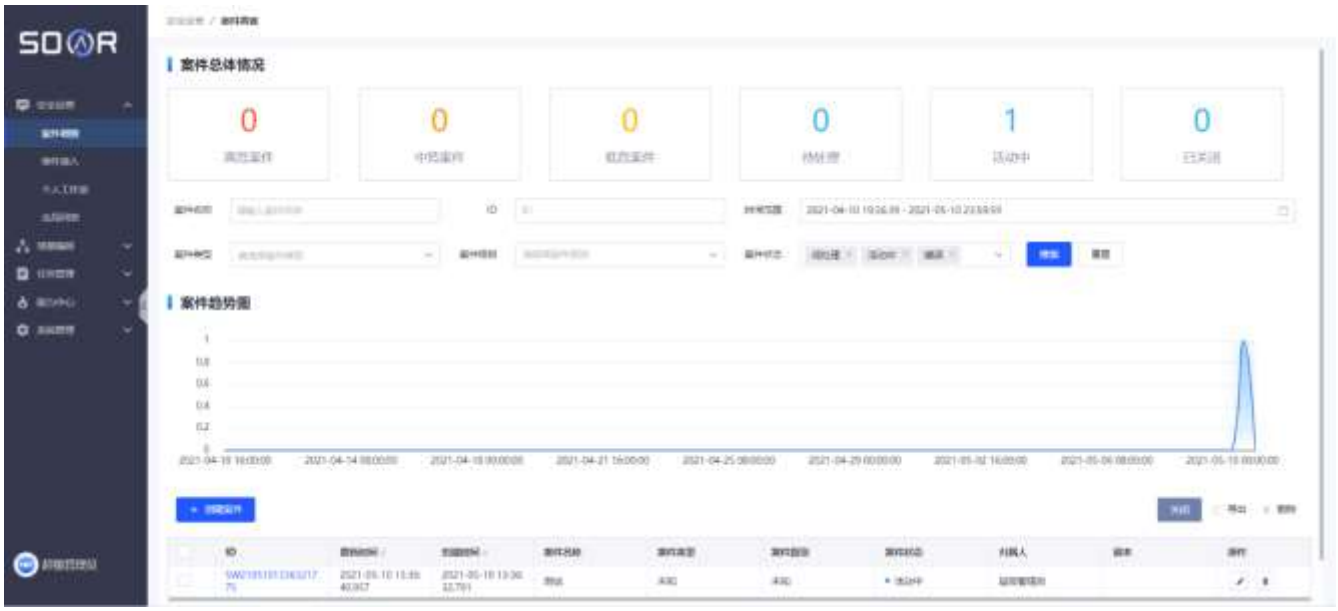
点击  按钮，对任务进行编辑。

8. 安全运营

8.1 案件调查

8.1.1 功能简介

进入“**安全运营➤案件调查**”页面，包括案件总体情况，案件趋势图，案件列表三个子板块。如下图所示。



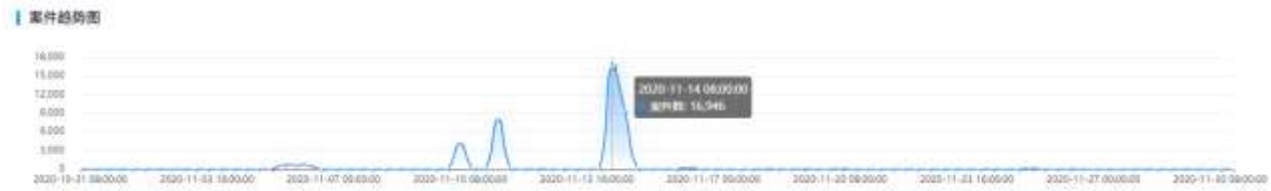
8.1.2 案件总体情况

案件总体情况可从“高危案件，中危案件，低危案件，待处理，活动中，已关闭”这几个维度进行统计查看相关案件的个数。也可以通过“案件名称，ID，时间，案件类型，案件级别，案件状态”进行相关案件搜索查询。如下图所示。

◆ 案件状态默认选择“待处理、活动中、错误”三种状态。

8.1.3 案件趋势图

案件趋势图可查看某段时间案件个数的变化，鼠标悬浮至曲线上，可查看当前时间具体案件的个数。案件趋势图会根据搜索结果进行相应变化。如下图所示：



8.1.4 案件列表

案件列表可展示生成的所有案件，如下图所示。

1. 创建案件

点击**<创建案件>**按钮，可支持手动创建新的案件，弹出“案件信息”配置框图，如下图所示：

案件名称：输入案件的名称；

案件类型：与“**系统管理>事件类型**”同步。可选择相应的案件类型。也可到“**系统管理>事件类型**”自定义案件类型；

案件级别：分为“高、中、低、未知”；

归属人：案件归属人默认为当前登录的用户；管理员角色创建案件可以指定其他归属人，除管理员外创建案件归属人只能为自己；

参与角色：管理员、安全分析员角色默认为所有案件参与人；

参与人：若参与角色为空，则默认参与人为本人和 Aibot；若参与角色为安全分析员、管理员，则归属于这两种角色的用户、本人和 Aibot 默认为该案件的参与人，后续该角色新增用户自动加入参与人中。创建案件后，在作战室中不可移除归属参与角色的用户，只可在案件编辑时将该角色删除。

剧本：可选择是否绑定剧本。案件创建成功后会自动执行。

剧本入参：若绑定的剧本有输入参数时，需要填写该参数。

2. **案件关闭**

勾选相应的案件，点击 

，同时提交案件关闭原因（误报、重复、处理完成、其他）附加说明，则可关闭案件，案件状态切换为“已关闭”。

3. **案件导出**

选中需要导出的案件，点击 

，即可导出案件列表。

4. **案件删除**

点击 

按钮，可删除案件。

5. **案件编辑**

点击  按钮，对案件进行编辑。

6. **创建案件发起审核**

如果用户在创建案件，绑定剧本的过程中，该剧本中涉及到用户无权限的动作，则用户需要进行发起审批操作，如下图所示。点击<提交>，则发起审批成功。待相应人员审核完毕后，案件即可创建。审批支持系统外审批，配置方式与人工任务系统外办理别无二致，详情见人工任务配置。

审批流程可在**安全运营-个人工作室**中，**我的申请-剧本流程**中可见。如下图所示。

8.1.5 案件详情（作战室）

点击案件 ID，可下钻查看案件信息，事件信息，剧本运行情况，作战室情况。

8.1.5.1 案件信息

案件信息窗口可查看该案件的相关信息，包括“创建时间、案件类型、案件名称”等信息，以及相关的事件信息，如下图所示。

8.1.5.2 剧本信息

剧本信息窗口如下图所示：

- 剧本信息窗口可查看该案件绑定的相关剧本的运行情况，若节点和连接线为彩色，则表示运行成功，若节点或连接线为灰色，则表示未运行或者运行失败。

- 点击剧本中任何一个节点，可显示该节点的相关信息。

- 若在该案件处置过程中，在作战室发起调用其他剧本的指令之后，在剧本信息窗口可查看新调用剧本的运行情况，如下图所示：

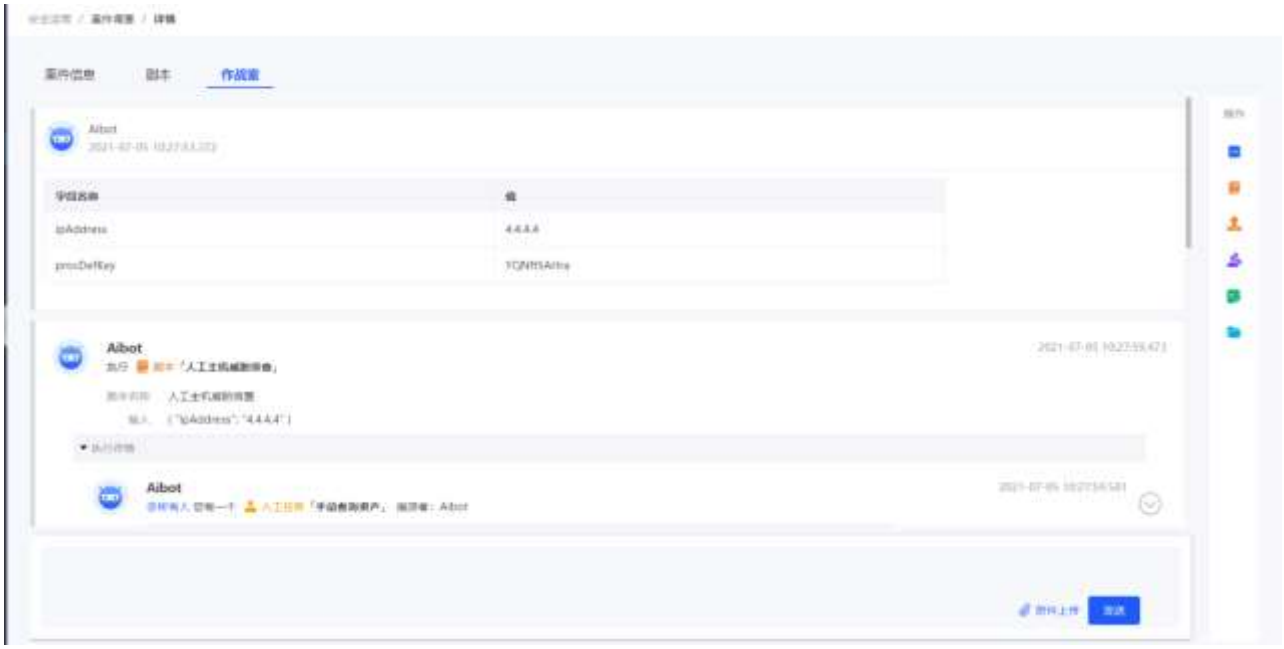
切换后，展示新调用剧本的运行情况，如下图所示：

8.1.5.3 作战室

功能简介：

作战室对应一个案件，用户可在作战室查看剧本执行情况，也可直接下发动作、任务、剧本等指令操作。除此之外，用户可团队作战，管理该案件的相关成员，并且可在线聊天。

作战室窗口如下图所示：



- 左侧为节点详情子页面，可查看每个节点执行的输入、状态、结果。
- 右侧一列为快捷操作按钮列表。包括（从上到下）指令快捷下发、待办记录快捷查看、审核记录快捷查看、作战室成员管理、任务记录快捷查看、查看全部节点/与我相关的节点、查看包含评论/忽略评论的所有节点，右下角为聊天按钮。

功能详解：

1. 指令快捷下发

点击 按钮，弹出指令快捷下发框，如下图所示：

详情：

可快捷下发动作、脚本、剧本、人工四种指令。其中参数的填写详情可参考 6.2.3 小节。

若当前用户无该动作执行权限，则需发起审批。审批流程进展可见**个人工作室-我的申请-动作**。如下图：

2. 待办记录快捷查看

点击 按钮，可快速查看当前案件需要本人待办的所有记录，如下图所示：

详情：

点击某条记录，可快速跳转至该节点查看详情信息。

3. 审核记录快捷查看

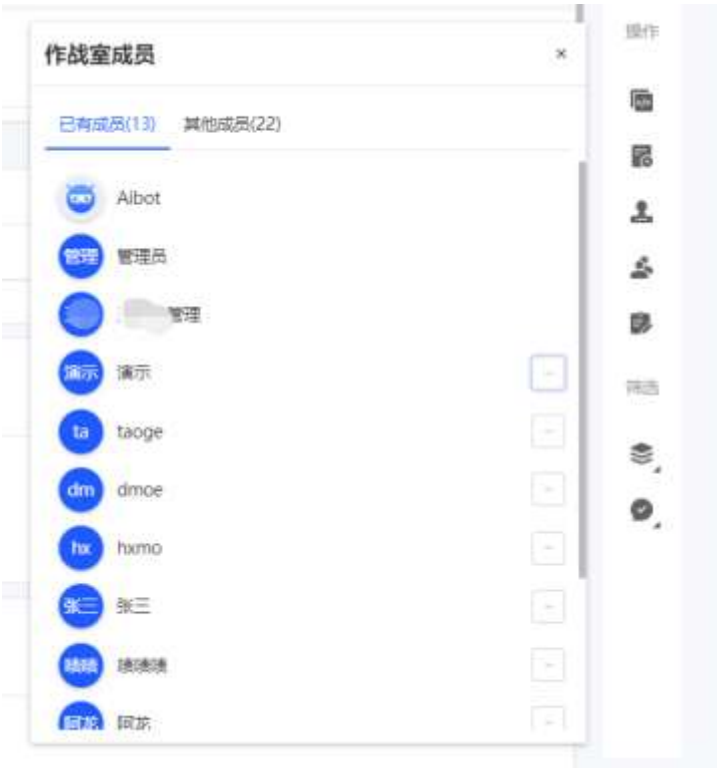
点击 按钮，可快速查看当前案件需要待本人审核的所有记录，如下图所示：

详情：

点击某条记录，可快速跳转至该节点查看详情信息。

4. 作战室成员管理

点击  按钮，可查看当前与该案件的所有参与成员，如下图所示：



详情：

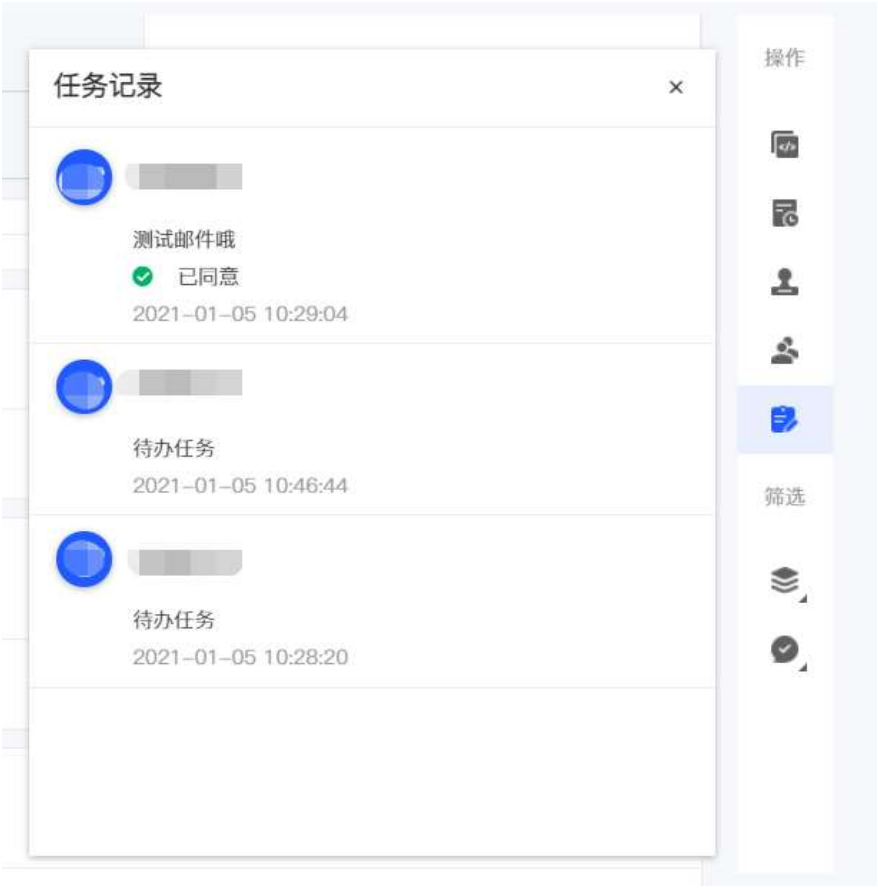
其他成员列表中，点击 + 按钮，可将其他成员添加至该案件的作战室中。

已有成员列表中，点击 − 按钮，可将该成员移除当前作战室。

- ◆ 管理员（admin）与 Aibot 为默认的案件参与人，不可移除。
- ◆ 不在该作战室的成员，不可查看该作战室信息。
- ◆ 不可移除归属参与角色的用户，只可在案件编辑时将该角色删除。

5.任务记录快捷查看

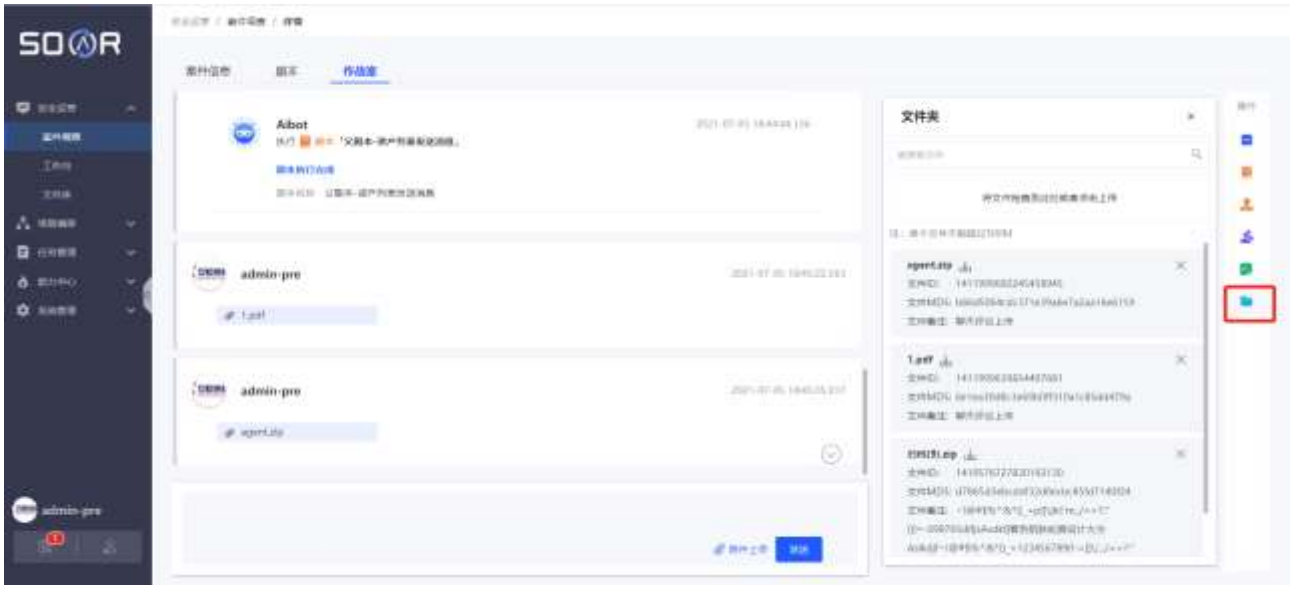
点击 按钮，可快速查看当前案件的所有任务记录，如下图所示：



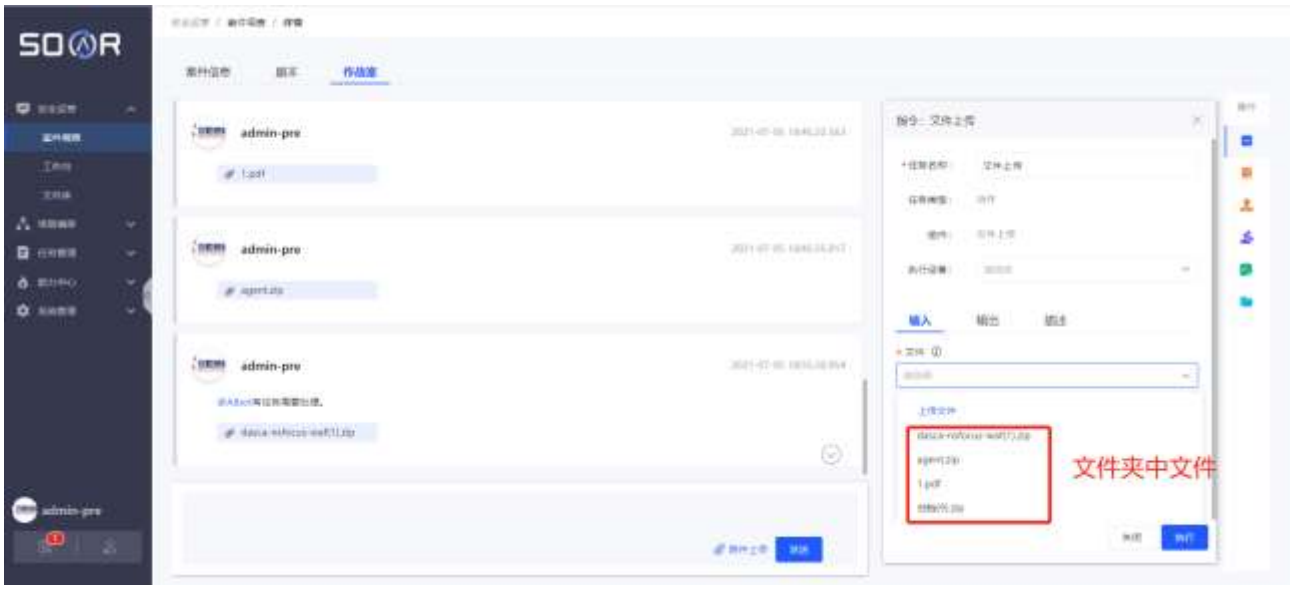
详情：

点击某条记录，可快速跳转至该节点查看详情信息。

6.文件夹



点击 按钮，可快速查看当前案件相关的所有文件，本案件上传的文件会自动关联至文件夹，并同步更新至文件库中。如下图所示，有关文件作为输入的动作，可上传文件或直接选择本文件夹中的文件作为入参。

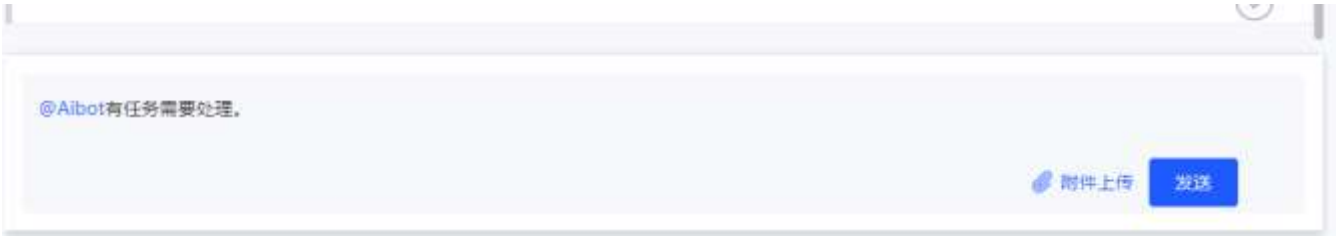


点击下载按钮，即可下载该文件；

点击删除按钮，可以解除该文件与该案件的关联关系，如果该文件没有关联除本案件以外的任何案件，则点击删除后，直接从文件库删除该文件。

7.聊天框

聊天对话框，如下图所示：



详情：

聊天输入框可输入文字等信息，点击<**发送**>，即可在左侧节点详情看到聊天内容，可@作战室内部人员。

点击<**附件上传**>，即可上传不超过 20M 大小的文件，点击<**发送**>，即可在左侧节点详情看到该内容，并支持作战室内成员进行附件下载。

8. 快速到达底部

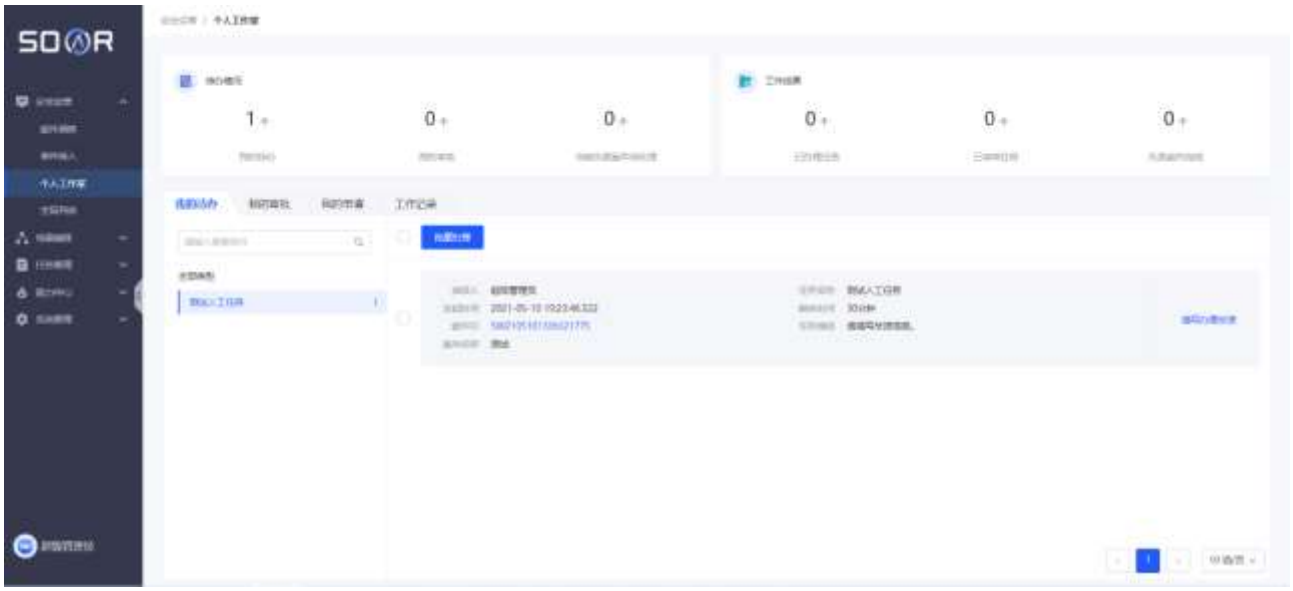
点击**作战室**页面右下角的 按钮，可快速抵达本页面的底部。

8.2 工作台

8.2.1 功能简介

个人工作室可查看所有关于我的任务，包括我的待办、我的审批、我的审批申请、工作记录几块内容，用户可在本模块快速办理任务、快速审批。需要注意的是，每个任务都有剩余时间，用户需要在指定时间内办理完成，否则将无法办理。

进入“**安全运营➤个人工作室**”页面，分为“我的待办，我的审批，我的申请，工作统计”几个子页面。可处理与我相关的工作，页面详情如下图所示：



◆ 待办和审批均有剩余时间，所有任务在剩余时间内均可办理。注意超时后不可办理。

8.2.2 总体情况

个人工作室总体情况分为**“待办情况”，“工作成果”**两个子版块。其中**“待办情况”**可查看我的待办、我的审批、当前负责案件待处理总数；**“工作成果”**分为已办理任务、已审核任务、负责案件完成总数。页面详情如下图所示：

8.2.3 我的待办

点击 我的待办 ，展示当前待办列表，如下图所示：

1. 待办列表

左侧为“我的待办“列表，所有待办根据任务类型进行分类。点击某任务类型，列表右侧显示相应类型的待办任务详情。如下图所示：

2. 单条处理

在某条待办任务的右侧，点击 填写办理反馈 ，弹出如下框图，可填写该任务的相关反馈信息：

3. 批量处理

勾选需要办理的任务，点击  ，可批量处理待办任务。

4. 统一处理

点击右上角 统一处理 ，可对当前类型的待办任务进行统一反馈处理。

8.2.4 我的审批

点击 我的审批 ，展示当前审批列表，可对某条审批进行同意或拒绝操作。如下图所示：

1. 审批列表

左侧为“我的审批“列表，分为动作和剧本流程两种审批类型。点击某类型，列表右侧显示相应类型的审批详情。

2. 单条处理

点击某审批任务右侧的 

按钮，完成该审批操作。

3. 批量处理

勾选需要办理的任务，点击 同意 或 拒绝 ，可批量处理审批任务。

4. 统一处理

点击右上角 全部同意 或 全部拒绝 ，可对当前类型的所有审批任务进行统一处理。

8.2.5 我的申请

点击 我的申请 ，展示“我的申请”列表。从两种维度对我的申请工作进行统计，包括动作和剧本流程。详情如下图所示：

点击 详情 ，可显示该条申请节点的详情，包括摘要、输入、输出、错误、耗时详细信息，如下图所示：

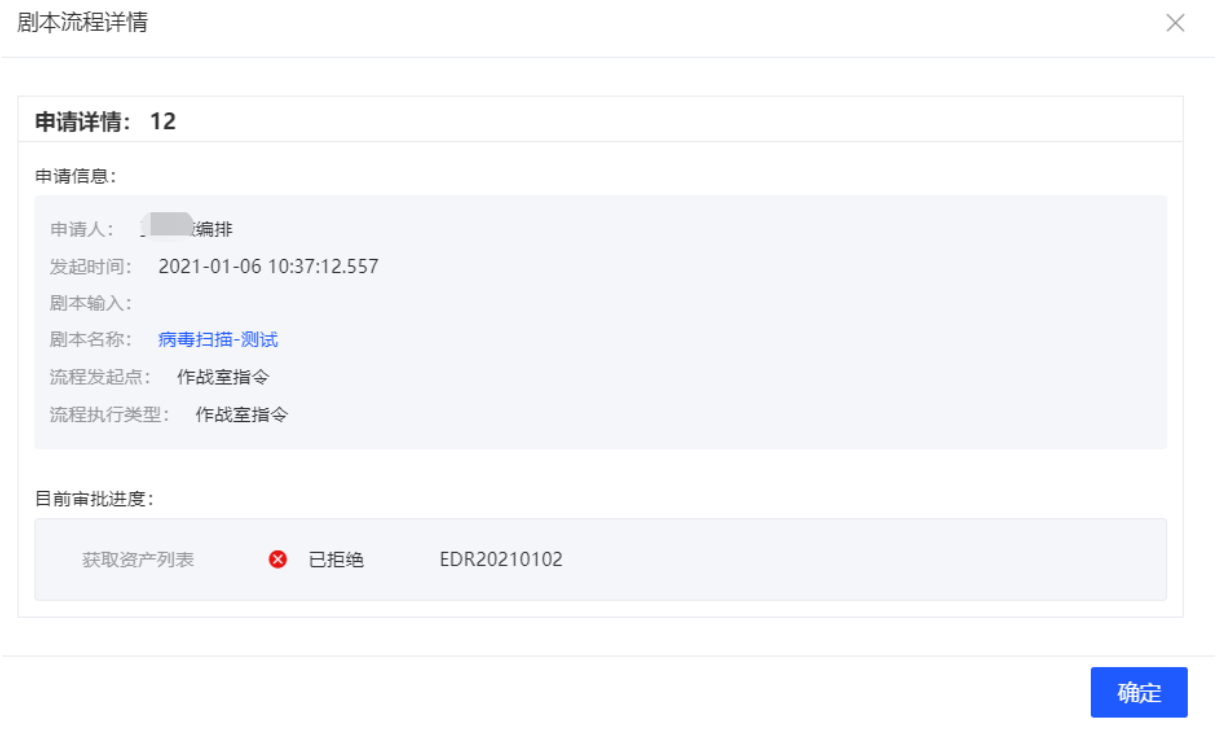
8.2.6 工作记录

点击 工作记录 ，从多种维度对“我”的所有工作进行统计，如下图所示：

点击记录类型下拉框可选择不同的类型的工作记录。包括：我的审批任务中的动作以及剧本流程的审批、以及我的待办任务统计。

点击动作（审批）列表中的某条工作记录的<**详情**>按钮，可显示该动作节点的详情信息，如下图所示：

点击剧本流程（审批）列表中的某条工作记录的<**详情**>按钮，可显示该剧本流程的详情信息，如下图所示：



点击待办任务列表中的某条工作记录的<**详情**>按钮，可显示该剧本流程的详情信息，如下图所示：

8.3 文件库

8.3.1 功能简介

文件库对平台所有上传的文件进行管理，并支持案件之间文件相互共享，且支持直接进行文件上传。

进入“**安全运营➤文件库**”页面，页面详情如下图所示：

8.3.2 功能详解

1. 文件上传

点击【上传文件】，可直接在文件库上传文件，并直接关联至案件，支持直接填写案件 ID 或直接选择需要共享的某类案件。如下图所示：

2. 文件共享

点击【文件共享】按钮，可将该文件直接分享给某案件，案件文件夹可查看，如下图所示：

3. 文件下载

点击【下载】，可直接进行文件下载。

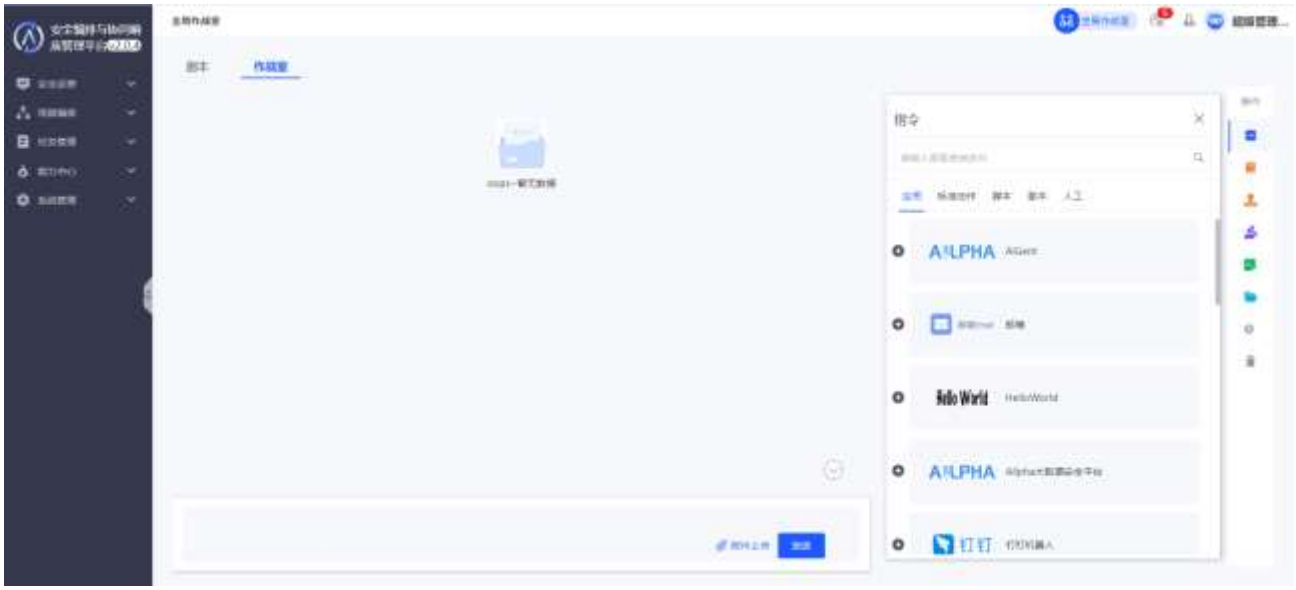
4. 文件删除

点击【删除】，可直接删除文件，需注意文件删除后不可恢复。

8.4 全局作战室

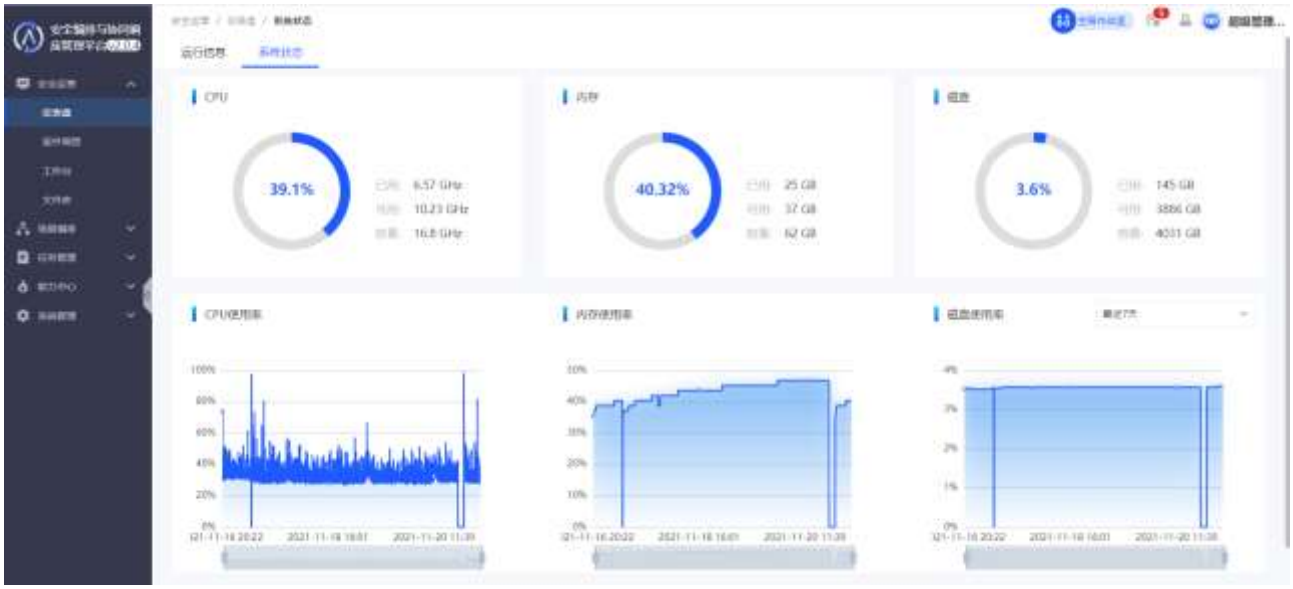
全局作战室为全平台用户参与的作战室，该作战室成员不支持新增/删除，其余功能与普通案件作战室一致，不再赘述。详情可见 8.1.5.3 作战室。

点击  按钮，可直接进入全局作战室界面。如下图所示：



8.5 仪表盘

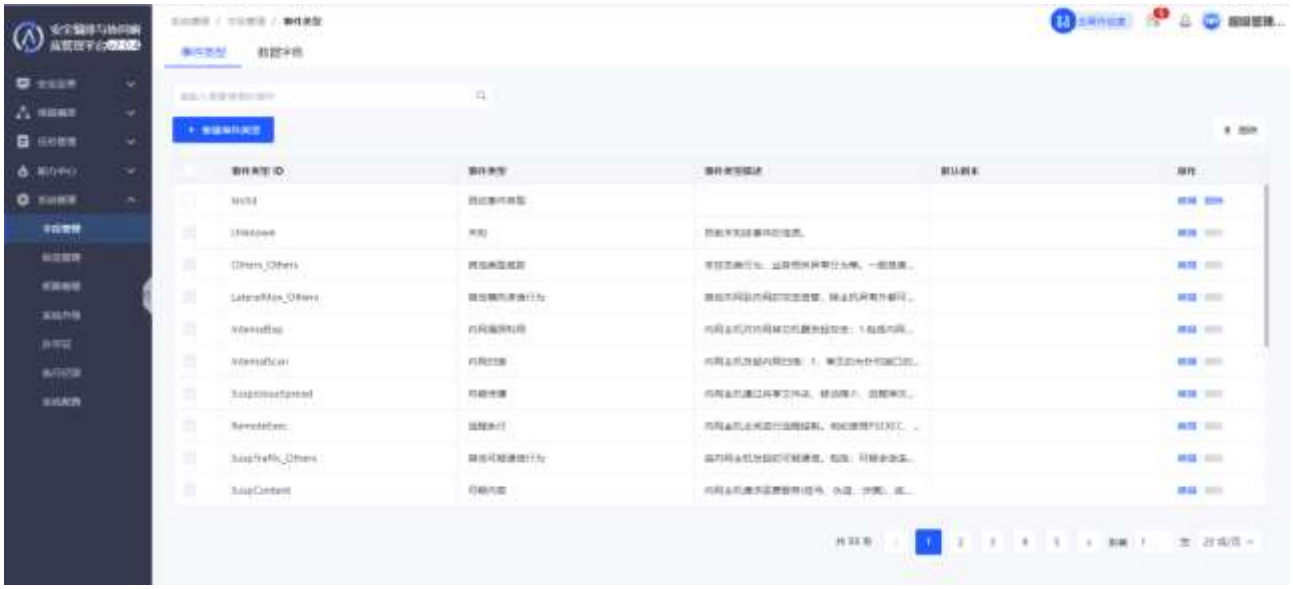
进入【安全运营】-【仪表盘】，支持查看平台的运行信息、系统状态。如下图所示：



9. 系统管理

9.1 事件类型

进入“**系统管理➤字段管理➤事件类型**”界面，事件类型主要是对平台事件类型标签进行统一管理。事件类型页面布局如下图所示：



注：事件类型与案件类型相对应。

1. 新建事件类型

点击<新增事件类型>，弹出如下图配置框：

事件类型 ID：支持输入中文,英文,数字，不可重复。

事件类型名称：支持输入中文,英文,数字，不可重复。

默认剧本：可选择是否绑定该类型的默认剧本，若绑定了默认剧本，则创建任务时可不选择剧本，系统会根据事件类型自动判断。

事件类型描述：可添加对该事件类型的详细描述。

2. **删除事件类型**

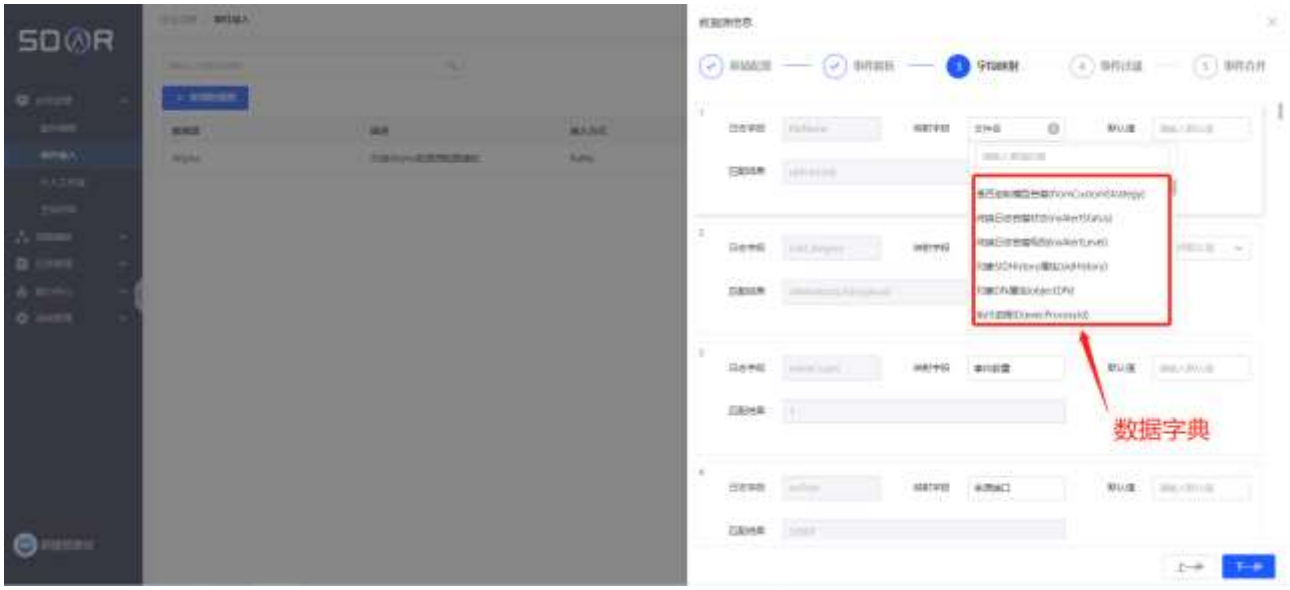
自定义事件类型可删除，内置类型不可删除

3. **编辑事件类型**

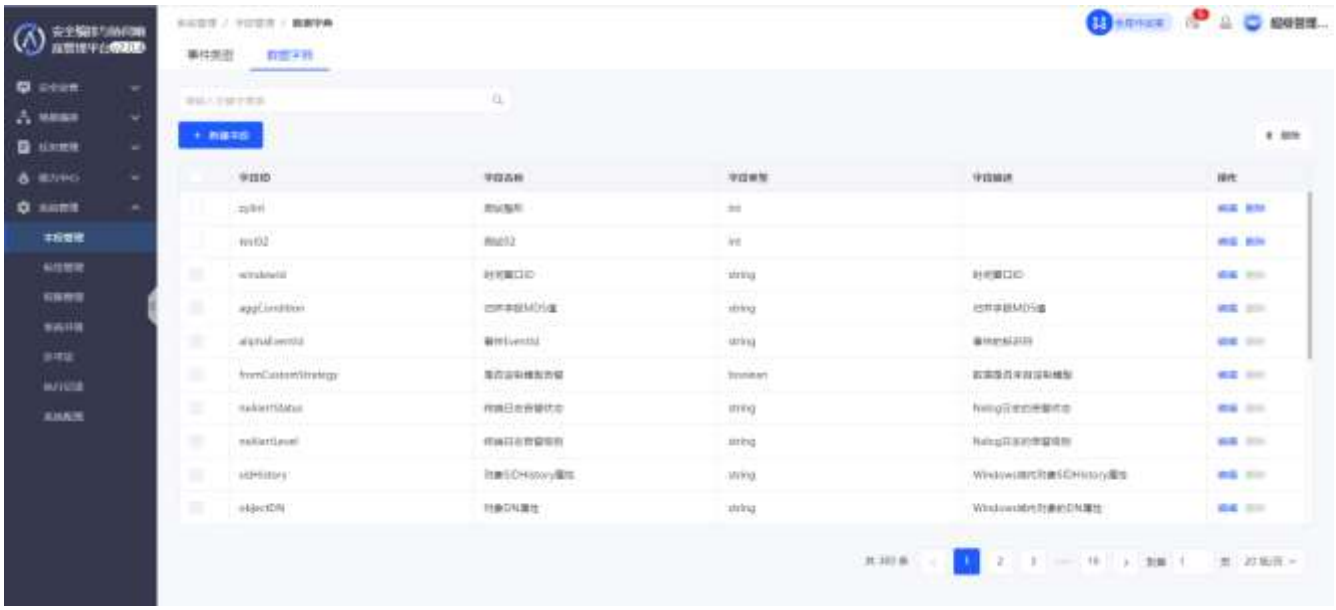
自定义事件类型可编辑，内置类型不可编辑。

9.2 数据字典

进入“**系统管理➤字段管理➤数据字典**”界面，可对“**事件接入➤字段映射➤映射字段**”进行统一管理。如下图所示：



数据字典页面布局如下图所示。



1. 新增字段

点击<新增字段>，弹出如下图配置框：

字段 ID：字段 ID 不可重复；只可输入中文、英文、数字；

字段名称：字段名称不可重复；只可输入中文、英文、数字；

字段类型：可选“Boolean”，“string”，“double”，“ip”，“float”，“long”，“int”，“enum”，“timestamp”几种类型；

字段描述：可为当前字段添加描述。

2. **编辑字段**

自定义字段可编辑，内置字段不可编辑。

3. **删除字段**

自定义字段可删除，内置字段不可删除。

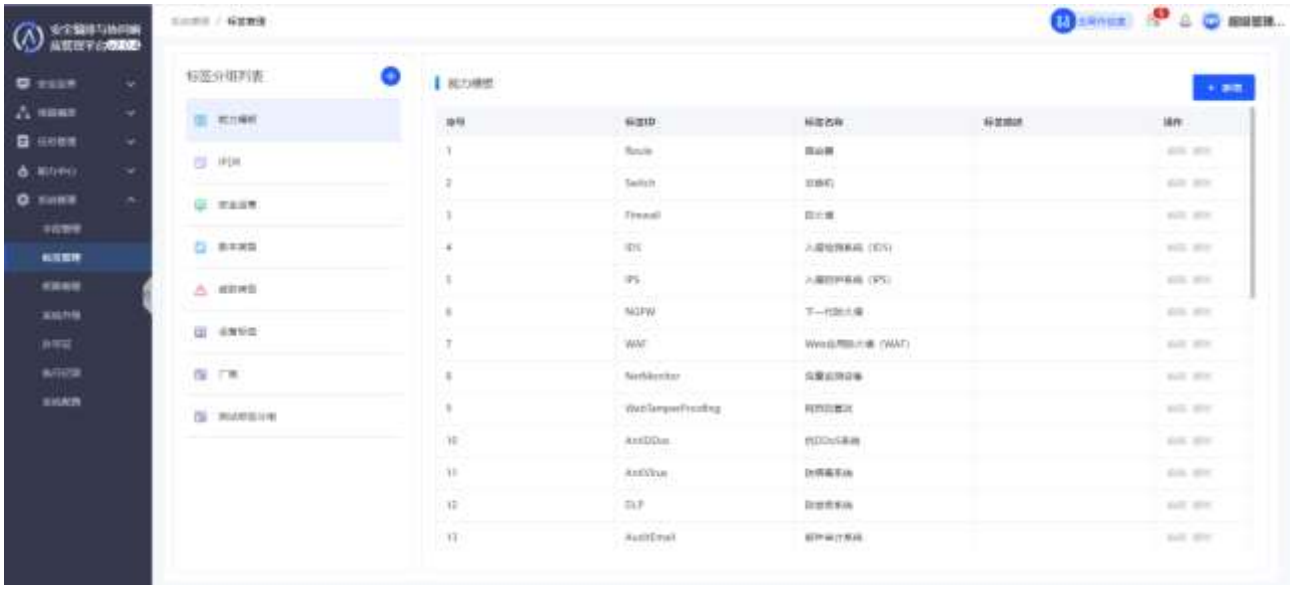
4. **字段搜索**

支持对字段 ID、字段名称、字段描述进行搜索。支持模糊搜索。

9.3 标签管理

进入“**系统管理➤标签管理**”界面，可对不同菜单模块使用的标签进行统一管理。可添加标签分组，并在

分组下新增自定义标签。标签管理页面布局如下图所示。



1. 新增标签分组

点击 

按钮，弹出下图标签分组配置框:

分组 ID：ID 不可重复；只可输入中文、英文、数字；

分组名称：名称不可重复；只可输入中文、英文、数字；

应用菜单：选择该标签分组需要被应用在哪个功能菜单下，可选择 “标准能力，剧本管理，设备管理，组件库，组件管理，剧本能力”，可多选；

分组描述：可添加对该分组的具体描述。

2. **标签分组中新建标签**

点击 

按钮，弹出下图标签分组配置框:

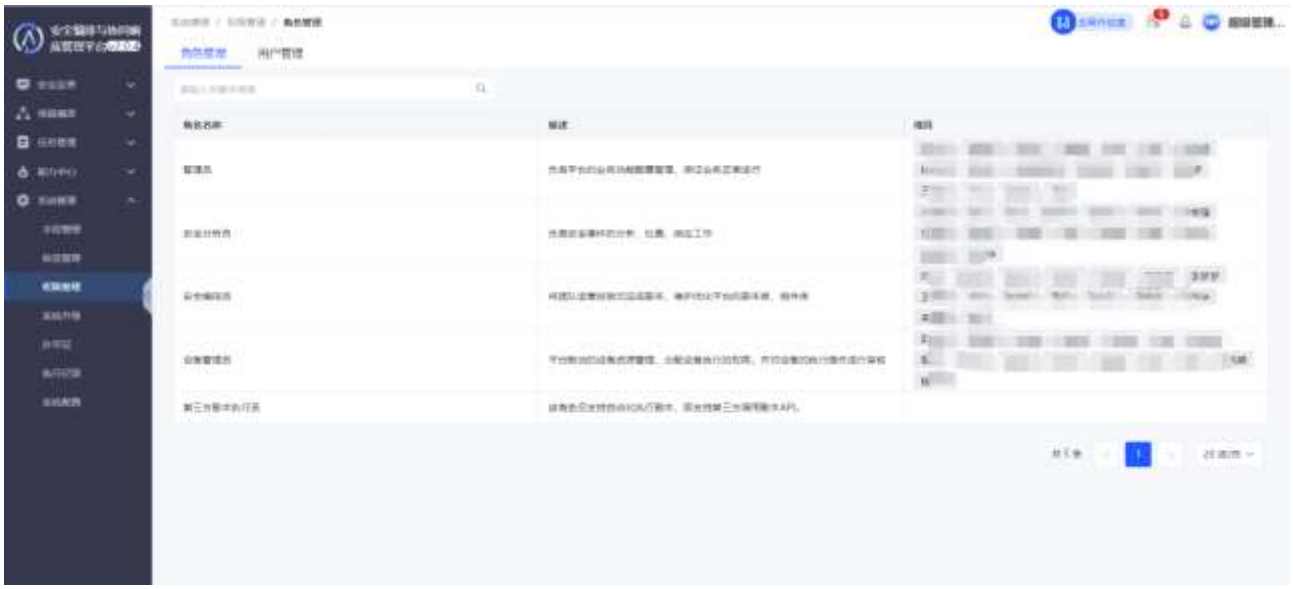
标签 ID：不可重复；只可输入中文、英文、数字；

标签名称：不可重复；只可输入中文、英文、数字；

标签描述：可添加描述语句。

9.4 角色管理

点击菜单“**系统管理➤权限管理➤角色管理**”进入角色管理界面，如下图所示：



说明：

可对角色名称进行搜索。

系统内置 4 个角色，分别为：管理员、安全分析员、安全编排员、设备管理员。不同的角色拥有不同的权限。角色权限说明详见【9.1 角色说明】。

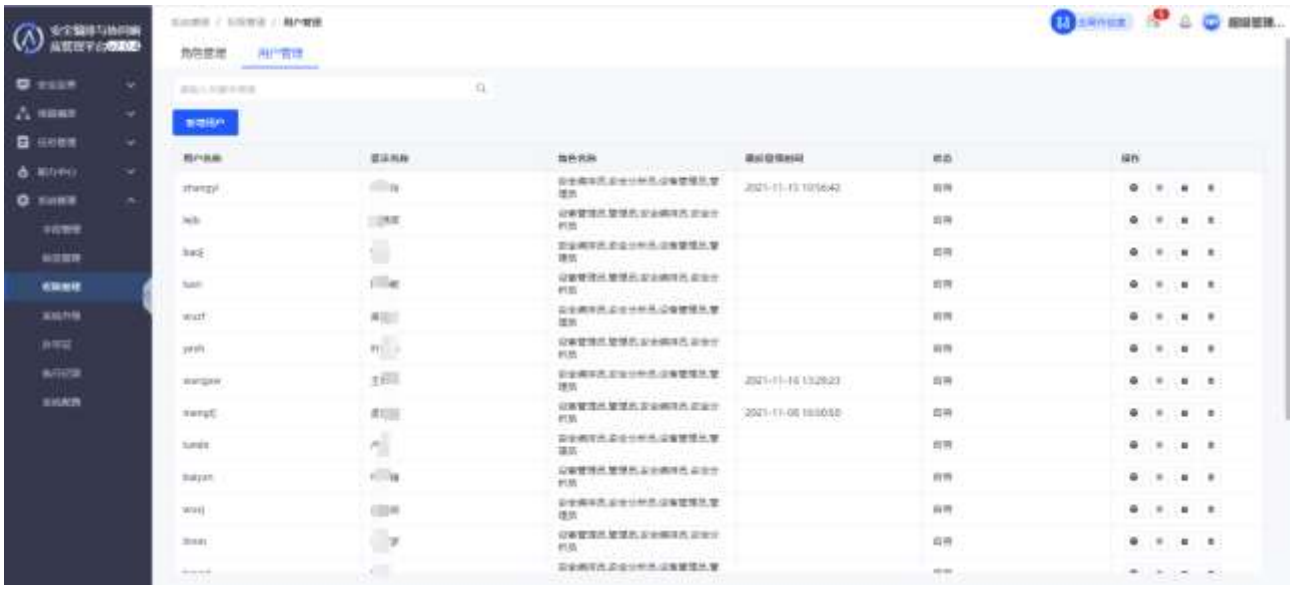
系统内置的角色不可用修改或者删除。目前平台不支持新增角色。

V2.0.4 版本中第三方剧本执行员角色仅供支持第三方调用剧本 API。

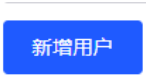
9.5 用户管理

点击“**系统管理➤权限管理➤用户管理**”进入用户管理界面，如下图所示：

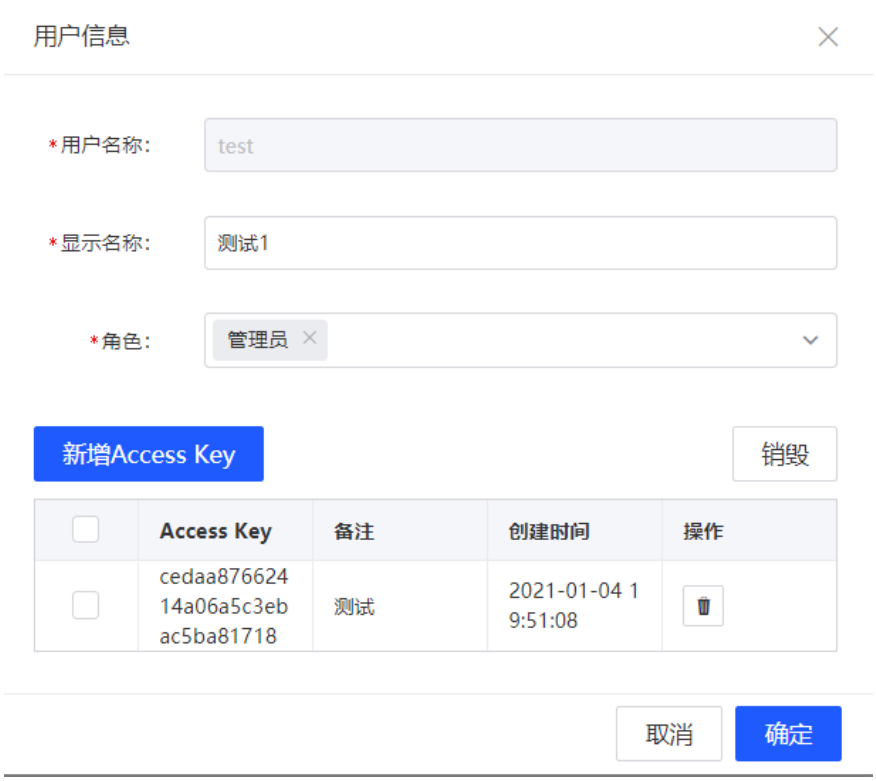
可对用户名称、显示名称字段进行搜索。



1、 用户新增

点击  按钮，弹出新增框图，如下图所示。

例:



点击<**新增 Access Key**>按钮，添加备注信息，为用户增加 Access Key。

1）基本信息包括：用户名称、显示名称、角色。不可与已有用户重复。

2）Access Key：可配置。需先创建用户，再进行 Access Key 配置。

3）角色信息：用户角色选择使用户拥有角色赋予的菜单功能。

4）完成账户创建，默认密码可复制。

◆Access Key 的创建需要在用户账号创建之后进行。

◆用户名称必须英文字母开头，可输入数字，下划线（_）长度 4-20 位。

◆角色可多选。

2、 用户编辑

点击操作列  按钮，支持用户编辑。内置用户不可编辑。

3、 用户删除

点击操作列  按钮，支持用户删除。内置用户不可删除。

4、 重置密码

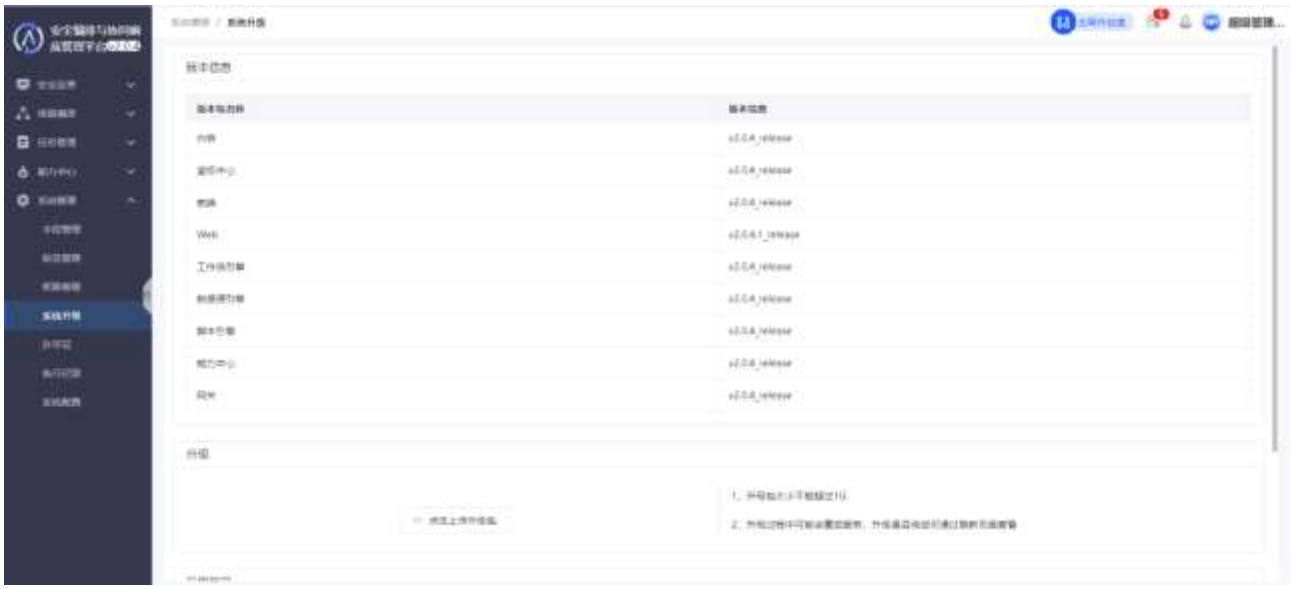
点击操作列  按钮，支持用户密码重置。

5、 禁用

点击操作列  按钮，支持将用户禁用。禁用之后该用户不可登录。

9.6 系统升级

admin 账号拥有对平台进行系统升级的权限，页面如下图所示：



点击【上传安装包】，选择安装文件，可对系统进行升级。系统升级记录可在【升级历史】中进行查看。

9.7 许可证

admin 账号拥有对平台许可证进行查看、导入、导出的权限，页面如下图所示：

点击【许可延期】，可进行许可证的导入和导出，如下图所示：

点击【导入】，可进行文件的选择并导入选中的许可文件，如下图所示：

点击【导出】，即可下载当前产品的许可文件。

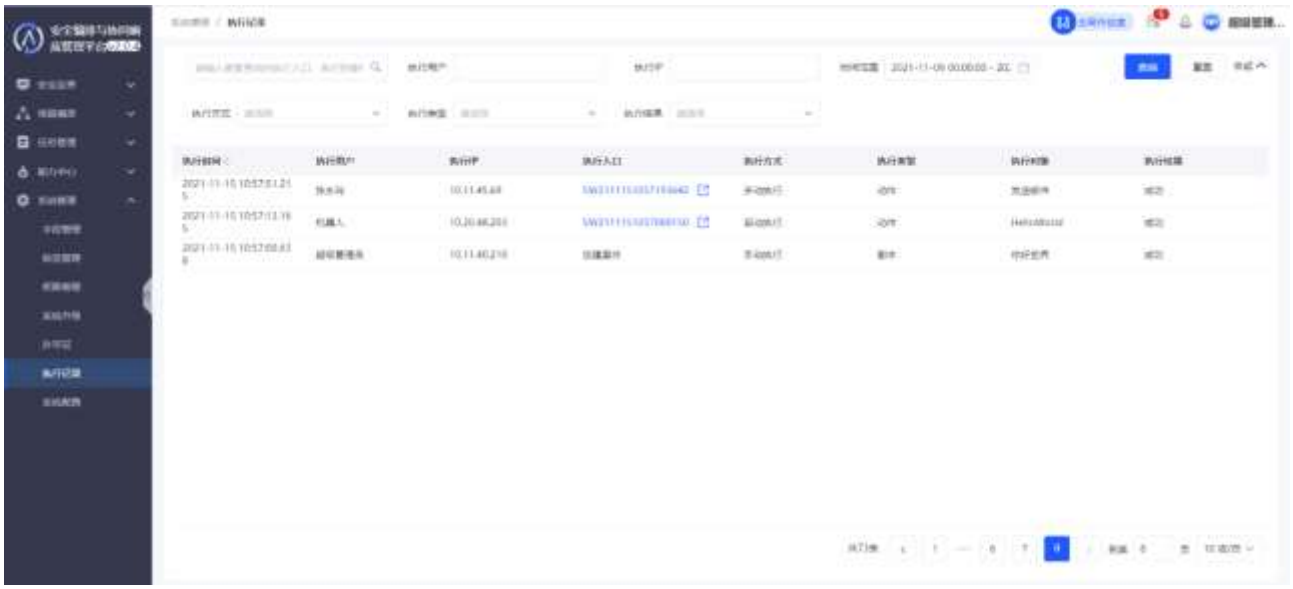
- 在升级维保期内，产品可正常使用且可以正常升级。

⚠

- 许可证无效或有问题时，不可登录本系统。
- 许可证过期无法享受升级和维保服务。

9.8 执行记录

进入“**系统管理➢执行记录**”界面，可查看平台业务类的所有操作执行记录，包括：动作执行；脚本执行；人工任务下发、办理、超时；剧本下发；发起审批、审批操作。页面如下图所示：



1、 执行记录列表说明

对执行操作的执行时间、执行用户、执行 IP、执行入口、执行方式、执行类型、执行对象、执行结果进行统计。其中，执行入口支持点击跳转至相应案件或全局作战室中查看执行详情或执行上下文。

注：2.0.4 版本存在执行动作时对象缺失的情况，原因是该动作未安装（或已安装之后卸载）。

2、 执行记录搜索说明

搜索条件如下：点击【收起】可将第二行搜索栏收起，点击【更多】可展开第二行搜索栏

9.9 系统配置

进入“**系统管理➤系统配置**”界面，可对平台网络配置、系统维护、存储管理、功能参数等基础参数进行配置，页面如下所示。

1、 网络配置

进入“**系统管理➤系统配置➤网络配置**”界面，可对平台网络信息进行修改配置，如下图所示：

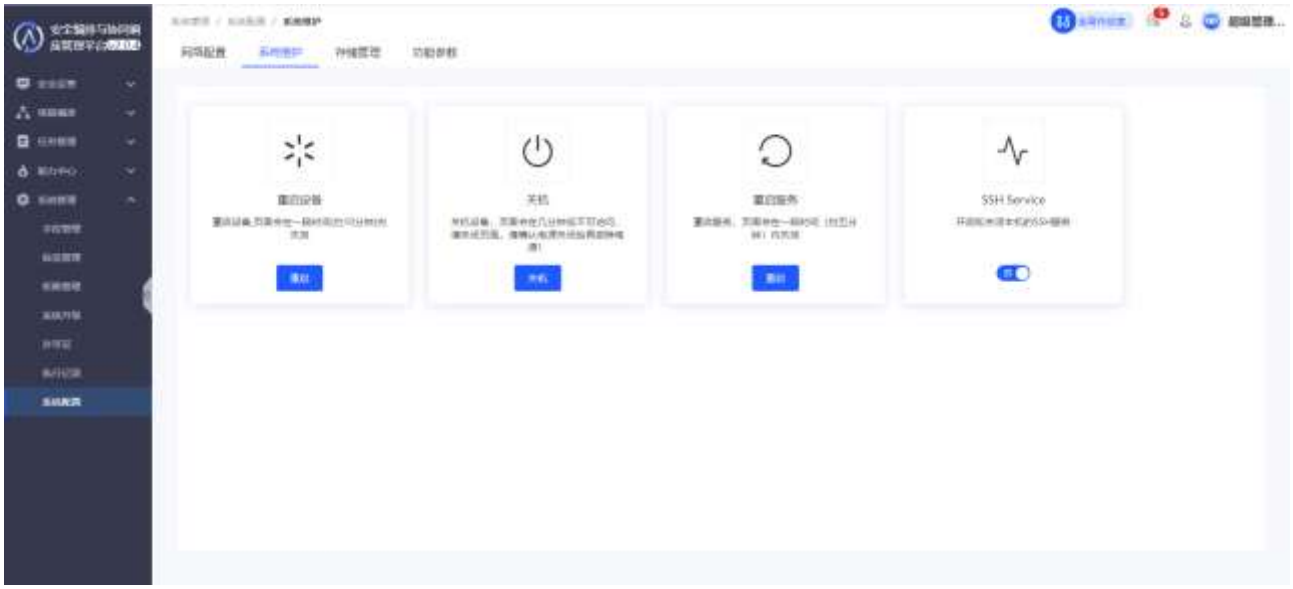
点击【修改】，弹出修改网络配置抽屉，如下图所示：

修改 IP 需慎重操作，修改网络配置会导致网络服务重启。若配置不当会导致无法进入页面。

2、 系统维护

进入“**系统管理➤系统配置➤网络配置**”界面，可重启设备、关机、重启服务、开启/关闭 SSH 服务，如下

图所示：



3、 存储管理

进入“**系统管理➢系统配置➢存储管理**”界面，可对平台存储模式进行管理，如下图所示：

当【是否自动清除数据】按钮打开时，平台数据达到设置的存储上限时，将自动清理 x 月以前的数据。当按钮关闭则不会自动清理数据。

清除数据记录会将每一次清除历史进行记录。

4、 功能参数

进入“**系统管理➤系统配置➤功能参数**”界面，可对平台业务类参数进行修改配置，如下图所示：

包括全局作战室、系统外办理配置、常用参数三部分。

全局作战室：可对全局作战室数据存储时限进行设置。

是否保存全部数据：选择是，则数据全部保留且不删除；选择否，则需填写数据保存期限，在期限内的数据予以保留，不在期限内的数据将在参数保存之后予以删除，删除后不可恢复。

系统外办理配置：若您有审批系统外办理、人工任务系统外办理的需求，需进行系统外办理配置，包括系统外办理地址（如果需要在外网办理需要进行外网映射）、是否开启验证。

常用参数：可对最多执行任务数、最多启动 APP 数、剧本线程数进行配置。

10. 能力中心

可对平台进行设备管理、标准能力管理、设备能力管理、剧本能力管理、APP 集成等操作，通过将平台的标准能力、设备能力、剧本能力接口化，方便平台内部或第三方调用。

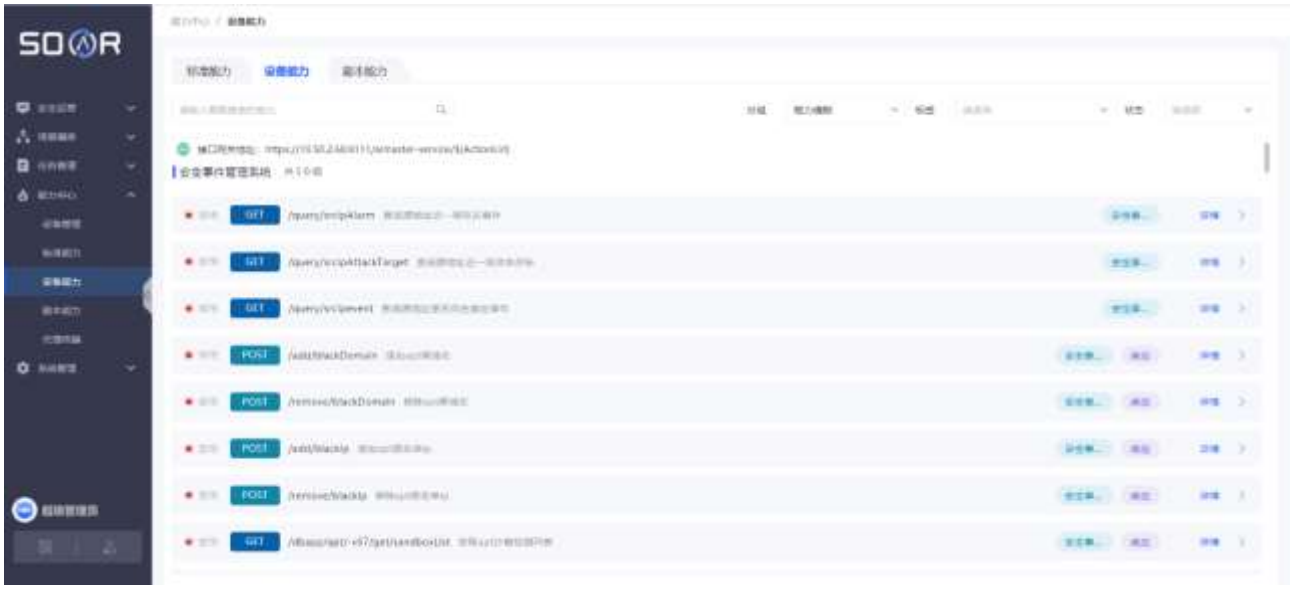
10.1 设备能力

10.1.1 功能简介

设备能力的动作参数较细化，支持该设备本身的特性参数（无共性的动作参数）和返回结果。各个 APP 的设备能力互不相同。注：APP 导入时需注意导入的新 APP 的设备动作与其他 APP 不同，否则会导入失败！

10.1.2 功能详解

选择”**能力中心➢设备能力**”进入**设备能力**页面，如下图所示：



1. 查询

可通过分组、标签、状态、动作名称、动作 URL 进行设备能力搜索。

2. 查看动作详情

点击某个设备能力后的【详情】按钮，展示出该能力的参数信息，可供第三方调用，如下图所示：

此处具体内容与【能力中心】-【设备管理】-【APP 配置】-【APP 动作】设备动作中展示的内容相同。

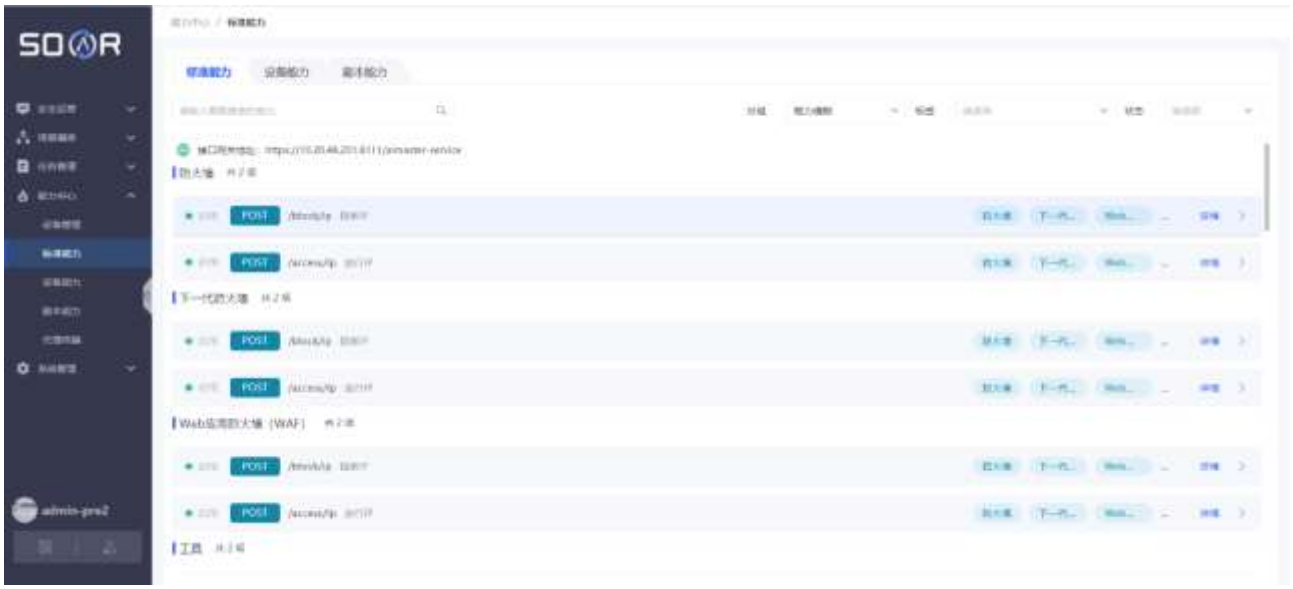
10.2 标准能力

10.2.1 功能简介

标准能力从设备能力抽象出共性参数（其他联动参数以内置参数、内置逻辑等方式填充），实现只要输入少数共性参数即可完成能力的调用，返回的参数也抽象出共性返回结果。各个 APP 的标准能力可以复用共享。

10.2.2 功能详解

选择”**能力中心➤标准能力**”进入**标准能力**页面，如下图所示：



3. 查询

可通过分组、标签、状态、动作名称、动作 URL 进行标准能力搜索。

4. 查看动作详情

点击某个标准能力后的【详情】按钮，展示出该能力的参数信息，可供第三方调用，如下图所示：

此处具体内容与【能力中心】-【设备管理】-【APP 配置】-【APP 动作】中展示的内容相同。

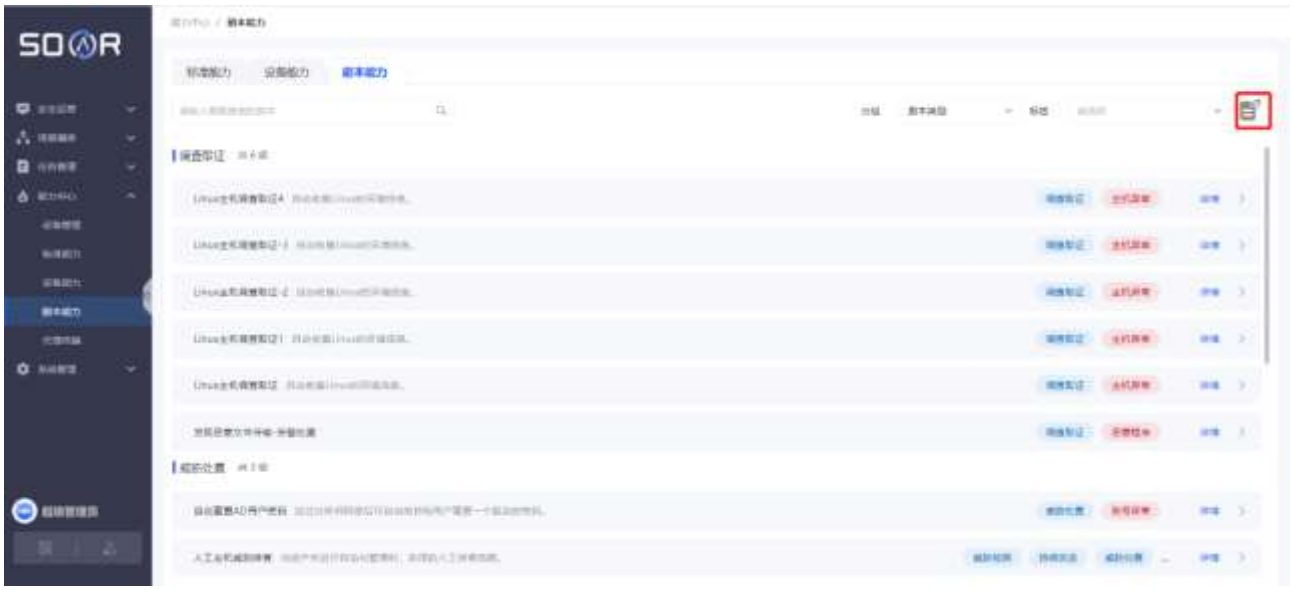
10.3 剧本能力

10.3.1 功能简介

剧本能力作为平台三大能力之一，将平台的所有剧本封装成标准化 API，支持平台内或第三方调用。通过调用剧本能力 API 的模式，可实现不登陆系统即可启动剧本流程并获得流程的结果，从而实现平台剧本能力的灵活使用。

10.3.2 功能详解

选择“**系统管理➤剧本能力**”进入**剧本能力**页面，如下图所示：

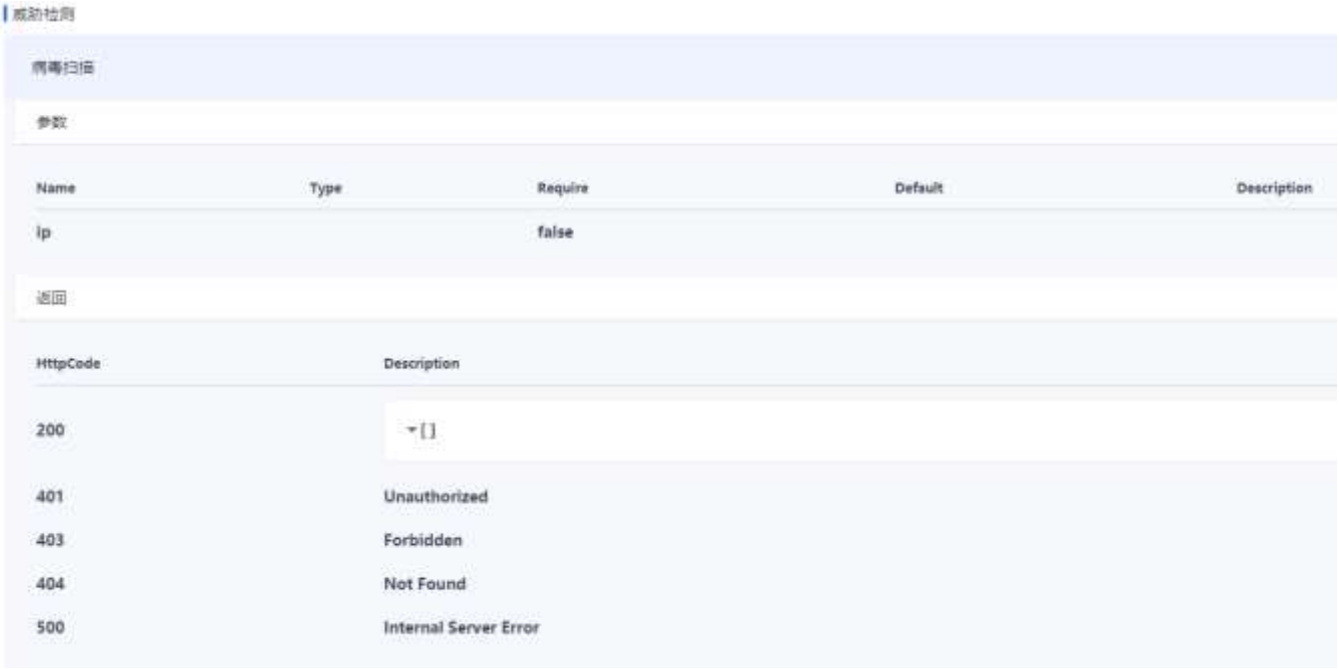


1. 查询

可通过分组、标签、能力名称进行标准能力搜索。

2. 查看动作详情

点击某个剧本能力，展示出该能力的参数信息，可供第三方调用，如下图所示：


威胁检测

病毒扫描

参数

Name	Type	Require	Default	Description
ip		false		

返回

HttpCode	Description
200	▾[]
401	Unauthorized
403	Forbidden
404	Not Found
500	Internal Server Error

3. 剧本接口帮助文档

点击右上角剧本接口调用帮助文档，即可查看第三方调用剧本接口方法详情。

注：第三方调用剧本接口前，需申请具备“第三方剧本执行员”角色用户的 Access Key 方可调用。

10.4 代理终端

10.4.1 功能简介

该模块提供跨隔离网解决方案，支持正向、反向代理，可解决网络隔离无法联动场景。通过添加代理终端，并在接入设备中选择合适的代理终端，即可在网络不通的情况下，成功联动设备。

10.4.2 功能详解

1. 下载代理安装包

点击右上角【下载代理安装包】，即可进行安装包下载，下载后进行解压，点击文件夹中 readme 文件并打开，如下图所示，并按照步骤进行运行脚本，即可成功安装。

2. 添加代理

点击【添加代理】，弹出以下框图：

3. 测试

点击【测试】，可对代理终端的连通性进行测试，联通成功状态则为通信成功，联通失败则为通信失败。

4. 修改

点击【修改】，可对已经添加的代理终端进行编辑。

5. 删除

点击【删除】，可删除已添加的代理。

11. 用户权限管理

11.1 角色说明

系统内置 4 个角色，分别为：管理员、安全分析员、安全编排员、设备管理员。不同的角色拥有不同的权限。

- **管理员：**职责：团队管理者。权限：较高权限，对全平台进行管理。
- **安全分析员：**职责：整合团队所拥有的资源，调动团队内部人力、设备能力等。权限：主要负责案件和任务的创建、管理，以及作战室的管理。
- **安全编排员：**职责：将团队运营经验沉淀成剧本，维护本团队的剧本库、组件库。权限：主要负责剧本和组件的编辑、管理。
- **设备管理员：**职责：管理团队内部设备资源，严格把控设备动作权限。权限：主要负责 APP、设备以及对设备的调用权限进行管理。

11.2 权限详细说明

一般情况下，角色权限如下：

	管理员	安全分析员	安全编排员	设备管理员
创建案件	√	√		
创建任务	√	√		
作战室指令调用	√	√		√
剧本、组件编辑	√		√	
设备管理	√			√

11.2.1 菜单权限

1. **<用户管理>、<角色管理>、<系统升级>、<许可证>**子页面仅 admin 账号可见；

2. **<设备管理>**页面的”设备详情”仅设备管理员角色和管理员可见，其他角色均不可见。

3. 其他页面无菜单权限控制。

11.2.2 数据权限

1.安全运营

案件调查：

- **创建案件：**管理员角色、安全分析员才可以创建案件，其他用户无法创建案件。若启动的剧本中具有”无权限动作”，则需要逐个发起审核，等所有人审批完成后任务、案件才会发布、创建，剧本流程不需要审批鉴权。

- **案件列表：**案件列表只展示自己参与的案件，管理员、安全分析员默认为所有案件参与人；只有案件参与人可查看相关案件内容（案件详情、剧本、作战室）；作战室、案件修改功能中可添加、移出参与人；

- **作战室：**

  - 默认管理员角色、安全分析员、设备管理员拥有所有联动权限，其他人员屏蔽下发指令的按钮（指令、快速工具栏）；

  - 当前用户无权使用该指令时，“执行”按钮变成发起审核；单机“发起审核”按钮后填写审核人（有权使用该指令的人列表）、申请说明；

  - 管理员和 Aibot 不可移出；管理员和 Aibot 默认拥有所有案件权限；

- **设备联动：**

  - 每个设备的每个动作都可以赋予不同的权限，当该设备的该动作被调用时，检查当前用户是否有权限，若没有则需要提交审批；审批人为该设备该动作的权限所有人，选中一个审批人进行审批；

2.场景编排

- **剧本管理：**

  - 剧本所有人可查看。

  - 安全编排角色和管理员角色才可以新建剧本，自定义的剧本会带上作者信息；

  - 管理员和该剧本作者可以编辑、删除自定义剧本；可以赋予其他人员剧本修改权限；

  - 点击剧本修改按钮时，判断剧本是否被任务调用，若被调用则需要暂停任务才可以修改剧本；

- 安全编排角色和管理员角色可以复制任意剧本。

➢ **组件管理：**

- 只有安全编排角色和管理员角色才可以新建组件，自定义的组件会带上作者信息；
- 管理员和该剧本作者可以编辑、删除自定义组件；可以赋予其他人员组件修改权限；
- 组件修改时，提示被剧本引用的信息，确认和保存修改，进行同步。（脚本、决策、人工，都需要同步）；
- 安全编排角色和管理员角色可以复制任意组件；

3.任务管理

- 管理员角色、安全分析角色才可以创建、修改、暂停、删除任务，其他用户无法创建、修改、暂停、删除任务。

4.设备管理

- 只有管理员角色和设备管理员角色才可以导入 APP、接入、修改、删除、查看设备详情。其他用户只能查看设备摘要信息（设备名称、标签、状态），也无法修改状态。
- 资产权限控制：添加编辑资产可用人员、角色，细粒度控制到 设备+动作。默认：管理员角色、安全分析角色、设备管理员角色具备所有设备动作的调用权限，当注册新的设备将默认添加这 3 名角色控制权限。可通过添加、移出角色、用户，编辑设备+动作的权限控制。

11.3 Access Key

11.3.1 功能简介

Access Key 可用于用户给“第三方”调用授权。如果授权成功，则“第三方”对于设备动作的调用权限与分发该 Access Key 的用户相同。一个用户可以分发多个 Access Key ，这些 Access Key 权限相同。Access Key 支持创建、撤销。

注：平台内置“第三方剧本执行员”的角色，拥有该角色用户的 Access key 则可直接调用剧本接口。其余角色的 Access Key 均不支持第三方调用剧本接口。

11.3.2 功能详解

点击右上角 

<Access Key>按钮，转到 Access Key 配置页面，如下图所示：

详情：

点击 

按钮，可新增 Access Key，填写相关备注信息，即可创建新的 Access Key。

点击某个 Access Key 后的  ，即可选择是否销毁该 Access Key。

点击 

，即可选择是否销毁全部 Access Key。

12. 术语和缩略语

术语	解释
AI	人工智能（Artificial Intelligence），英文缩写为 AI。它是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。
SOAR	SOAR（Security Orchestration Automation and Response，安全编排自动化与响应）是一种帮助组织能够收集不同来源与安全相关的风险和告警数据的技术，并且根据标准的工作流帮助明确定义、定优先级、标准化的进行事件响应活动。SOAR 的核心，就是将安全流程或预案，即将安全运营循环的每一个实例，比如蠕虫爆发处理流程、挖矿病毒告警处理流程、疑似钓鱼邮件处理流程等等，数字化管理起来形成 Playbook。用自动化完成其中所有可能自动化的动作，无法自动的仍然交由人来处理，通过可视化编排工具将人、技术和流程有机的结合起来，形成标准统一的、可重复的、更高效的安全运营流程。
DASCA	DASCA（DBAPPSecurity Capability API ，安全能力中心）负责统一管理企业内部的设备，并对外提供统一的安全能力接口，支持从外部通过 DASCA 统一调用企业内部安全能力。DASCA 提供设备调用能力。工作流引擎调用 DASCA 接口时，需提供设备的信息：IP、端口、认证信息等。DASCA 提供的服务都注册到服务中心。工作流引擎需要具备从服务中心获取所有的服务列表信息。同时本地需缓存所有服务列表信息，在服务中心崩溃后，仍能根据缓存的信息进行服务调用。