iOA 零信任安全管理系统

操作指南（SaaS 版）11.1.1版



腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2026 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

操作指南（SaaS 版）11.1.1版
快速入门（11.1.1版）
资产管理（11.1.1版）
资产运维（11.1.1版）
终端运维（11.1.1版）
终端信息（11.1.1版）
终端扩展（11.1.1版）
硬件变更与预警（11.1.1版）
软件运维（11.1.1版）
软件清单（11.1.1版）
软件仓库（11.1.1版）
盗版软件检测（11.1.1版）
存储空间（11.1.1版）
终端管控（11.1.1版）
合规检测（11.1.1版）
风险终端（11.1.1版）
合规检测策略配置（11.1.1版）
合规检测审计日志（11.1.1版）
外设管控（11.1.1版）
外设管控审计日志（11.1.1版）
外设管控策略配置（11.1.1版）
加密U盘（11.1.1版）
系统加固（11.1.1版）
系统加固审计日志（11.1.1版）
系统加固策略配置（11.1.1版）
防火墙管控（11.1.1版）
上网行为管控（11.1.1版）
上网行为管控审计日志（11.1.1版）
上网行为管控策略配置（11.1.1版）
上网拦截（11.1.1版）
网络访问隔离（11.1.1版）
水印保护（11.1.1版）
文件管控（11.1.1版）
文件管控审计日志（11.1.1版）
文件管控策略配置（11.1.1版）

版权所有：腾讯云计算（北京）有限责任公司

进程管控（11.1.1版）
服务管控（11.1.1版）
信息采集（11.1.1版）
软件管控（ 11.1.1版）
分发管控（ 11.1.1版）
运行管控（ 11.1.1版）
安装管控（11.1.1版）
软件卸载（11.1.1版）
终端防入侵（11.1.1版）
病毒查杀（11.1.1版）
策略配置（11.1.1版）
病毒风险（11.1.1版）
任务列表（11.1.1版）
审计日志（11.1.1版）
漏洞扫描与修复（11.1.1版）
漏洞风险（11.1.1版）
漏洞修复策略配置（11.1.1版）
任务列表（11.1.1版）
审计日志（11.1.1版）
实时防护（11.1.1版）
策略配置（11.1.1版）
实时风险（11.1.1版）
审计日志（11.1.1版）
高级威胁防护EDR（11.1.1版）
功能简介（11.1.1版）
策略规则（11.1.1版）
行为检测（11.1.1版）
行为检测白名单（11.1.1版）
行为采集（11.1.1版）
数据存储策略（11.1.1版）
存储目标管理（11.1.1版）
存储目标策略（11.1.1版）
威胁事件（11.1.1版）
威胁告警（11.1.1版）
威胁响应（11.1.1版）
威胁狩猎（11.1.1版）
敏感数据保护（11.1.1版）
风险调查（11.1.1版）

数据地图（11.1.1版）
数据地图（11.1.1版）
数据地图扫描策略（11.1.1版）
管控策略（11.1.1版）
管控策略（11.1.1版）
事件聚合规则（11.1.1版）
通道白名单（11.1.1版）
审批流配置（11.1.1版）
概述（11.1.1版）
企业微信（11.1.1版）
钉钉（11.1.1版）
飞书（11.1.1版）
内部地址（11.1.1版）
数据存储（11.1.1版）
存储目标策略（11.1.1版）
存储目标管理（11.1.1版）
本地存储策略（11.1.1版）
文件鉴定（11.1.1版）
文件鉴定使用指引（11.1.1版）
部署边缘节点（11.1.1版）
文件鉴定接口使用指引（11.1.1版）
数据分级分类（11.1.1版）
分级分类规则（11.1.1版）
敏感词库（11.1.1版）
模型聚类（11.1.1版）
文档类型库（11.1.1版）
文件来源（11.1.1版）
数据分级与评分（11.1.1版）
远程接入（11.1.1版）
身份及认证对接（11.1.1版）
iOA SaaS 本地自建账户（11.1.1版）
iOA SaaS 企业微信对接（11.1.1版）
iOA SaaS 钉钉对接（11.1.1版）
iOA SaaS 飞书（11.1.1版）
方案1：飞书认证（11.1.1版）
方案2：OAuth2 认证（11.1.1版）
iOA SaaS SCIM2.0 用户同步（11.1.1版）
连接器部署（11.1.1版）

版权所有：腾讯云计算（北京）有限责任公司

连接器排障指南（11.1.1版）
启用零信任网关（11.1.1版）
业务资源创建及授权（11.1.1版）
隧道类资源创建及授权访问（11.1.1版）
Web 类资源创建及授权访问（11.1.1版）
动态访问控制（11.1.1版）
动态访问控制策略配置（11.1.1版）
测试用例（11.1.1版）
限制指定访问时间（11.1.1版）
IP 分组联动挑战认证（11.1.1版）
应用访问联动挑战认证（11.1.1版）
终端合规检测联动挑战认证（11.1.1版）
区分设备类型的访问隔离（11.1.1版）
客户端运维（11.1.1版）
客户端管理（11.1.1版）
客户端策略（11.1.1版）
客户端自保护（11.1.1版）
客户端升级（11.1.1版）
模块定制（11.1.1版）
零信任接入配置（11.1.1版）
客户端通用设置（11.1.1版）
客户端自定义（11.1.1版）
软件弹窗拦截（11.1.1版）
客户端性能管理（11.1.1版）
客户端垃圾清理（11.1.1版）
远程协助（11.1.1版）
客户端操作日志（11.1.1版）
个性化设置（11.1.1版）
客户端首页（11.1.1版）
Banner库（11.1.1版）
帮助中心（11.1.1版）

版权所有：腾讯云计算（北京）有限责任公司

操作指南（SaaS 版）11.1.1版
快速入门（11.1.1版）

最近更新时间：2026-02-13 17:55:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

iOA 零信任安全管理系统分为管理后台（服务端）与员工客户端，开通 iOA 后，企业管理员需要在管理后台配置组织架构、分发客户端安装包和设置安全防护策略等基础操作。本文提供产品的基础功能使用步骤，便于企业管理员快速上手。

步骤一：配置企业组织架构

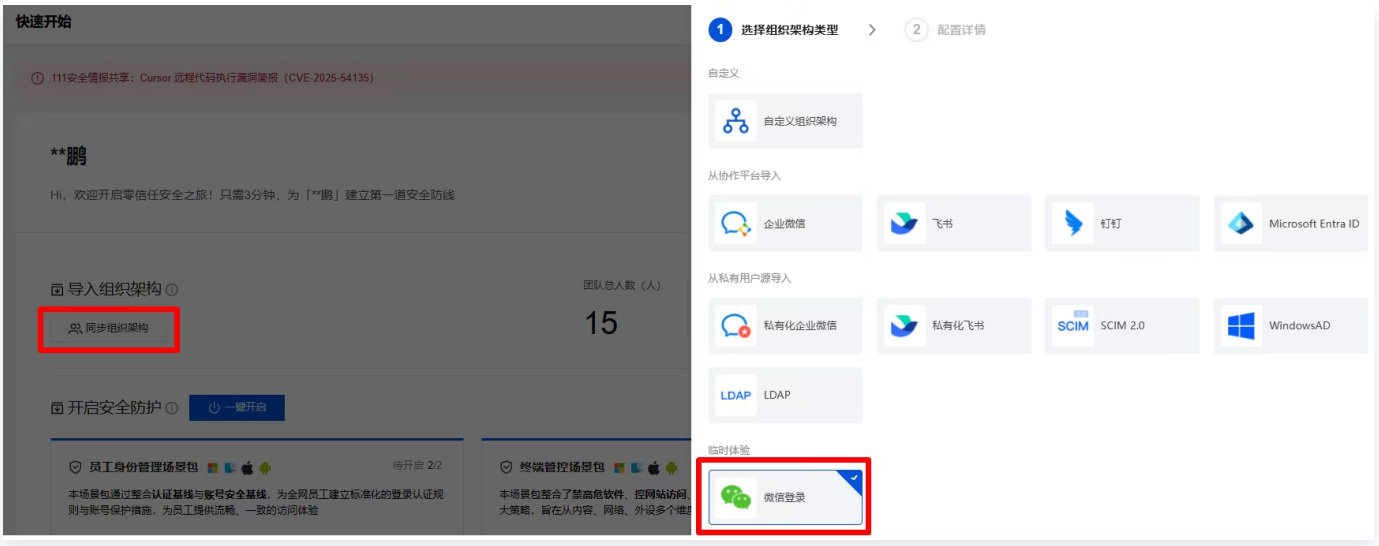
本章节仅介绍**无第三方数据源**如何配置企业组织架构与成员。您也可以从第三方数据源导入账号，具体请参见：身份及认证对接（11.1.1版）。

场景1：快速体验/测试产品场景

若在测试阶段希望快速体验 iOA 功能，推荐使用微信扫码登录。只需完成客户端安装（详见 客户端操作手册），即可扫码进入。系统会在首次登录时，自动创建“微信临时组织”目录和微信认证源。

> **说明：**
> 关于微信扫码登录的限制
> - 安全机制：此方式无法验证用户组织架构信息，任何人都可扫码进入。
> - 使用建议：仅建议在测试阶段临时用于快速体验，不可作为长期登录方案。
> - 人数限制：最多允许10人通过扫码登录。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择 快速上手。
2. 单击**同步组织架构**，选择**微信登录**。



3. 将以下客户端链接发送给需要邀请的人员。



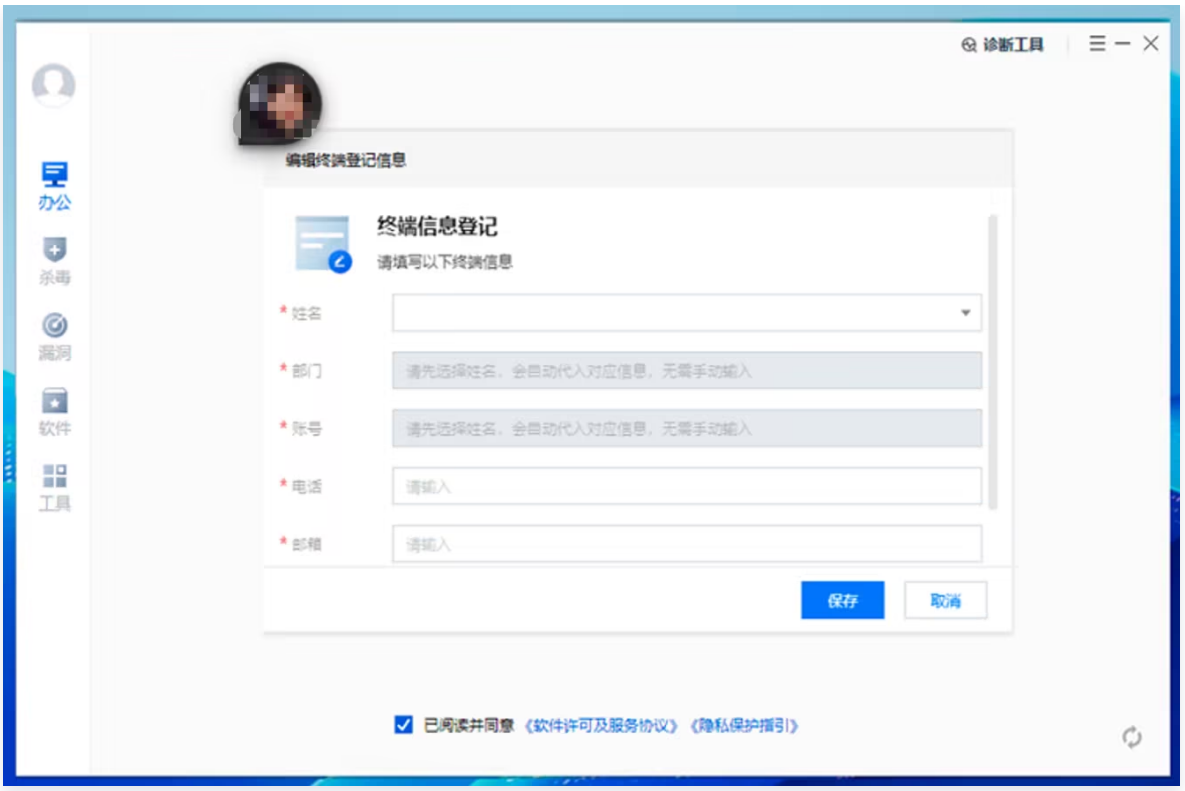
4. 员工完成客户端安装后，打开客户端，认证源选择：**微信扫码进行登录**。

> **说明：**
> 若企业用户目录下，不存在其他非微信和非自建的目录，企业默认认证策略则设为**“微信扫码”**。





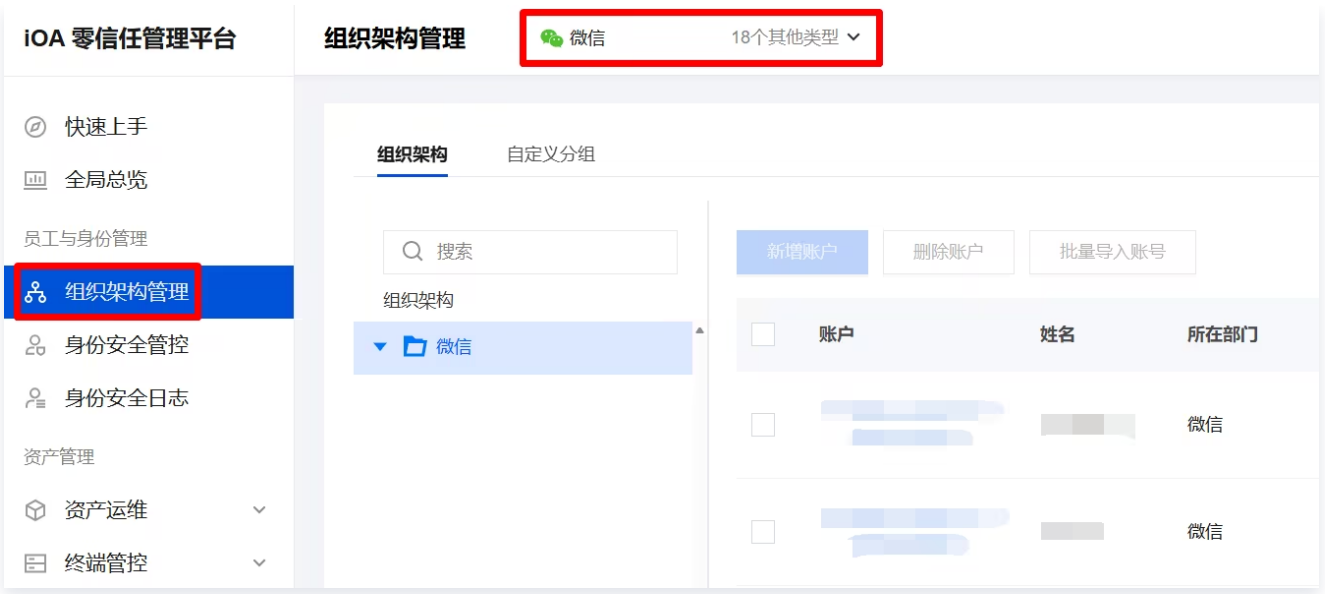
5. 完成扫码后，需要按要求登记员工个人信息，单击**保存**。



6. 登记个人信息后，即完成 iOA 登录。



7. 员工完成客户端扫码登录后，会在 iOA 控制台的：**员工与身份管理** > 组织架构管理 自动创建“微信临时组织”目录。
   - 管理员可在此目录内查看和管理员工的账号信息。

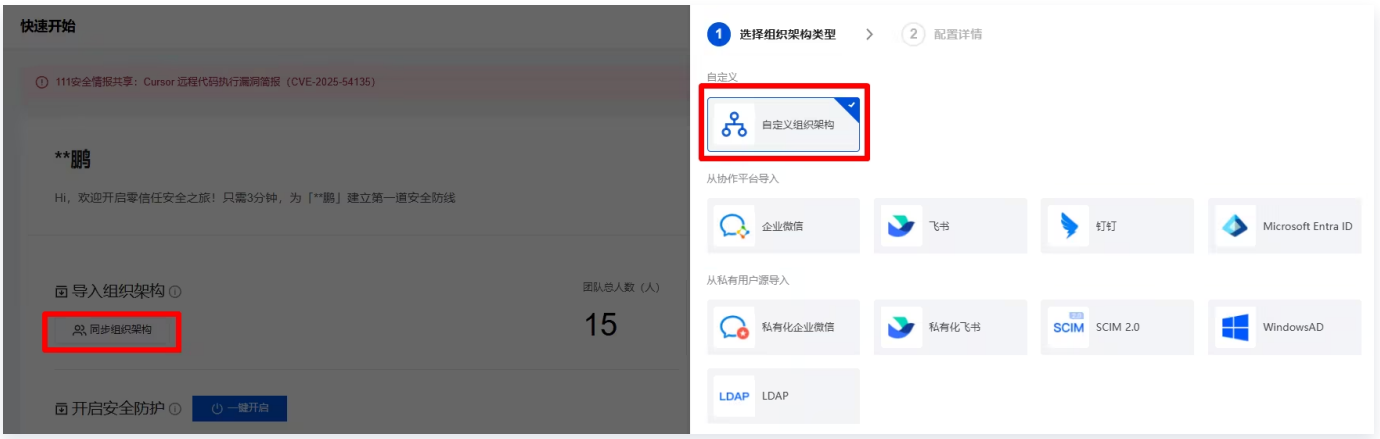


- 自动创建“微信临时组织”目录的同时自动创建微信认证源。



场景2:手动创建组织架构

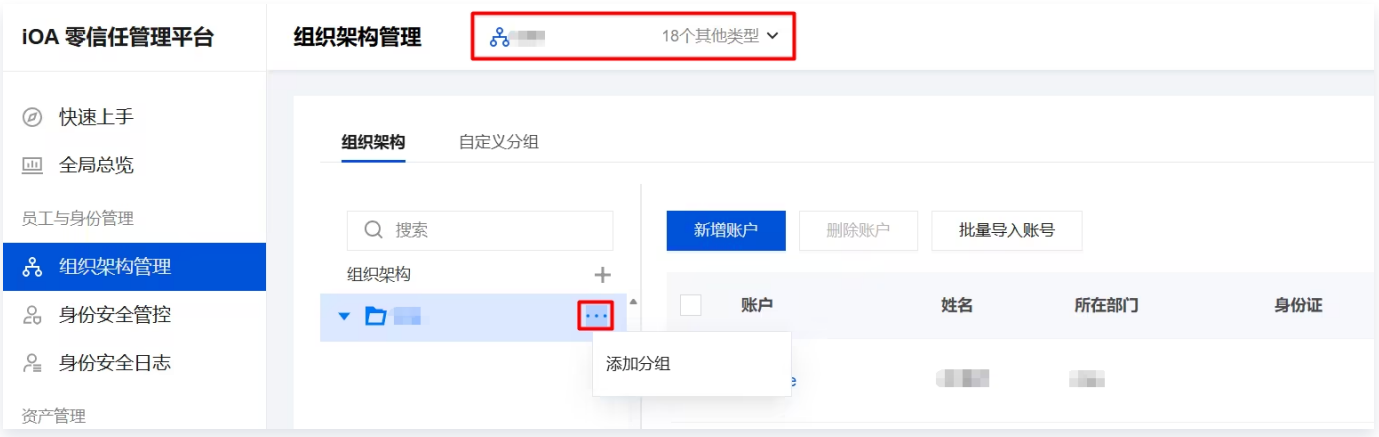
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择 快速上手 。
2. 单击同步组织架构，选择**自定义组织结构**。



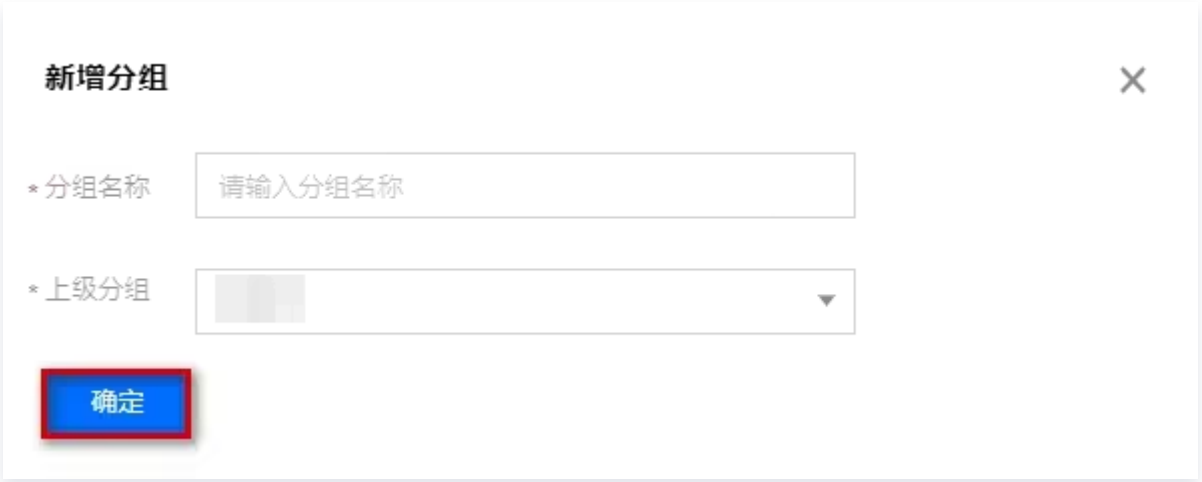
3. 输入组织机构名称后，单击**完成**。



4. 在**员工与身份管理** > 组织架构管理 页面，展示目录组织架构下的账户分组以及账户情况。单击**添加分组**，可以在此分组下新增次级分组。



5. 在新增分组弹窗中，输入分组名称，选择上级分组，单击**确定**。



6. 完成分组创建后，可以在分组下创建账户，单击**新增账户**。



7. 在账户管理页面，配置相关参数，单击**确定**。



8. 打开客户端，输入自建的账号密码，即可完成登录。

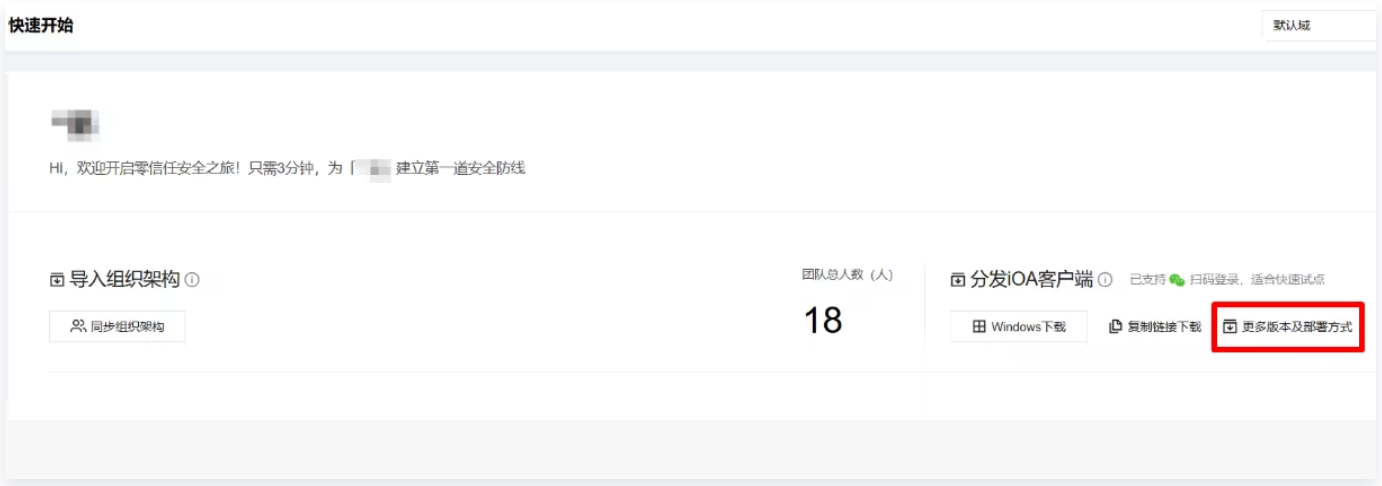
步骤二：分发 iOA客户端

场景1：员工自助部署

适合能够让员工自助安装的电脑，以邀请或企业公告的方式告知员工安装。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择 快速上手 。

2. 默认提供了客户端下载地址，企业管理员可以将客户端下载链接直接发送/邮件发送给员工，员工单击**链接**即可下载 iOA 客户端。



3. 用户将链接复制到浏览器后，会自动拉起浏览器下载 iOA 客户端，下载完双击安装 iOA 客户端。



4. 安装完成后输入 PIN 码，客户端即可完成对应控制台的关联。



场景2：手动安装包部署

适合需要管理员手动安装的电脑，例如公共或无人值守电脑。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择 快速上手 。
2. 在快速上手页面，单击 Windows 下载或 macOS 下载，下载对应的安装包。



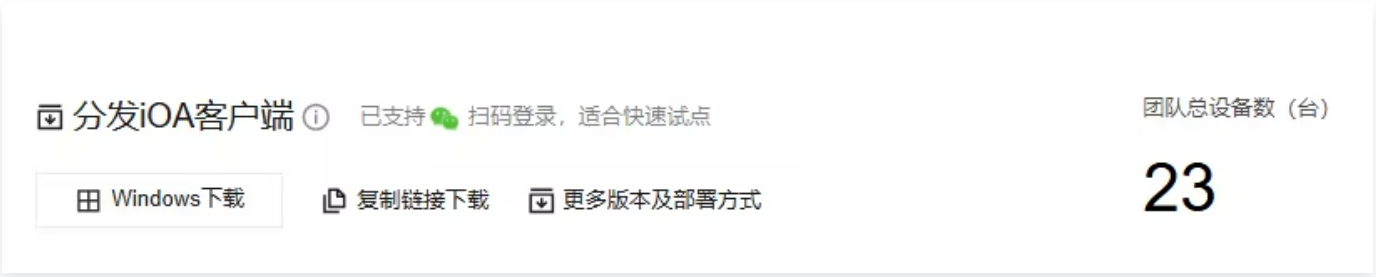
3. 下载完双击安装 iOA 客户端，安装包自带 PIN 码，无需输入自动关联控制台。

场景3：桌管分发部署

部分企业内部已经有了桌面管理的相关产品，可以使用桌面管理软件的软件分发功能对 iOA 安装包进行统一分发，员工终端设备接收到 iOA 安装包后，一键安装即可。

此处以腾讯电脑管家（小团队版）为例：

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择 快速上手 。
2. 在快速上手页面，单击 Windows下载，下载对应的安装包。



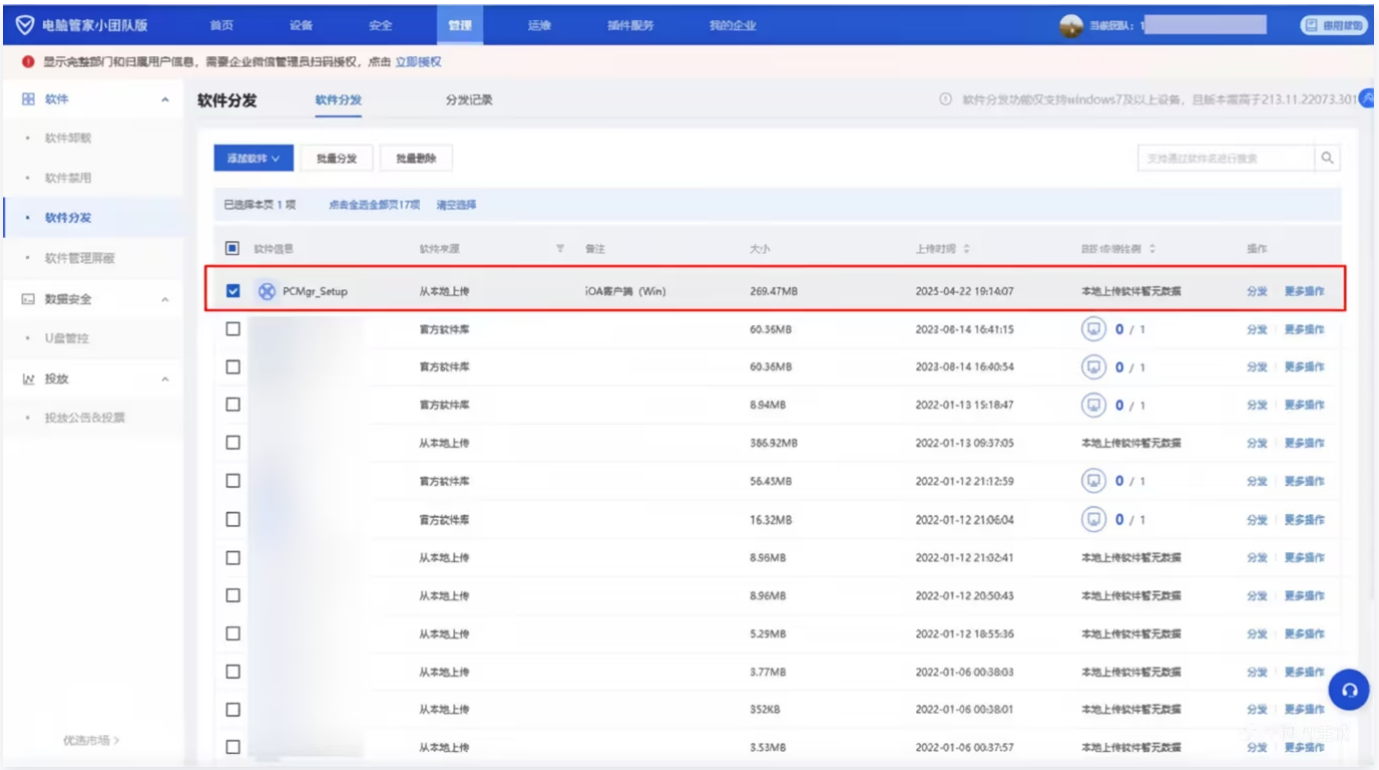
3. 登录腾讯电脑管家（小团队版）控制台，在左侧导航栏，选择**软件分发**，单击**添加软件**。



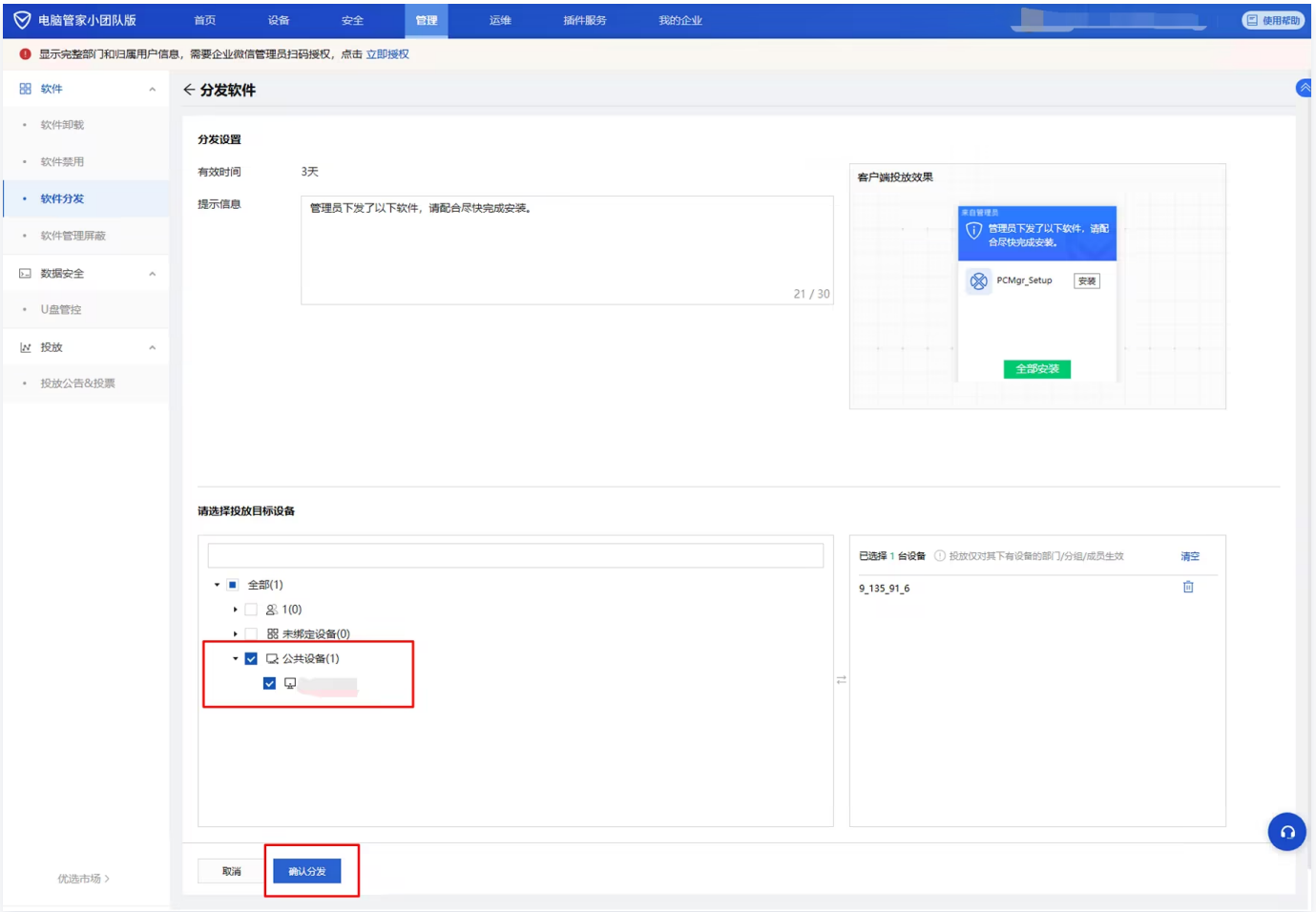
4. 选择本地软件，客户端静默安装参数（建议填写）：`/s ##qqpcmgr=0`，单击**开始上传**



5. 上传成功后分发给指定 PC：上传成功后，即可在软件分发页面看到 iOA 客户端，选择目标客户端，单击操作列的**分发**，即可对指定 PC 进行分发。



6. 选择指定的设备，单击**确认分发**。



7. PC 接到管理员分发的安装包，单击**立即安装**，后续进入 iOA 客户端安装流程，到此顺利完成客户端分发和安装环节。



场景4：域控环境部署

许多客户已采用 AD域来管理企业内部 PC，因此可借助该平台进行客户端推广。这里为用户提供两种 AD域相关的推广方案，详情请参见：iOA 客户端域控推广方案 。

步骤三：开启防护策略

通过预设场景化安全策略包，实现企业安全防护的“开箱即用”，降低安全配置门槛，快速覆盖终端防护、行为管控、账号安全等核心场景，兼顾标准化基线与个性化调优需求。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择 快速上手 。
2. 单击任意场景包的**了解更多**，可查看对应策略的详情。



3. 在场景包的策略详情内，单击**策略名称**，可快速跳转至对应策略配置页面。


策略包详情
终端管控
本场景包整合了禁高危软件、控网站访问、防拍屏泄密、管外设接入和合规检测五大策略，旨在从内容、网络、外设多个维度建立安全屏障，规范员工终端使用
属于终端防护模块，包含策略
策略
适用终端
是否付费开启
开启类型
开启状态
软件禁止运行策略
免费开启
一键开启
上网行为管控
免费开启
一键开启
水印保护策略
免费开启
一键开启
外设管控策略
免费开启
一键开启
合规检测基线PC端策略
免费开启
默认开启
合规检测基线移动端策略
付费开启
默认开启

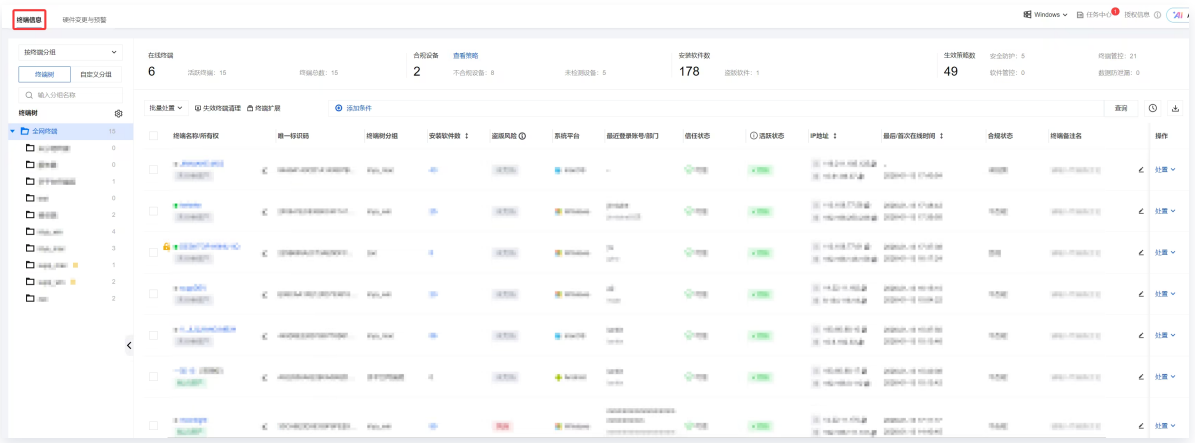
资产管理（11.1.1版）
资产运维（11.1.1版）
终端运维（11.1.1版）
终端信息（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

提供全网终端设备资产集中管控入口，实现对设备在线状态、安全合规状态、分组策略、批量处置等一站式可视化管理。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **终端运维**。
2. 在终端运维页面，选择**终端信息**。



3. 页面顶部可直观查看终端整体运行状态：
   - 在线终端：当前与控制台保持连接的活跃设备数量。
   - 合规终端：符合企业安全策略要求的终端数量。
   - 安装软件数：当前终端已安装的软件总数量。
   - 生效策略数：当前终端已应用并生效的安全管控策略总数。



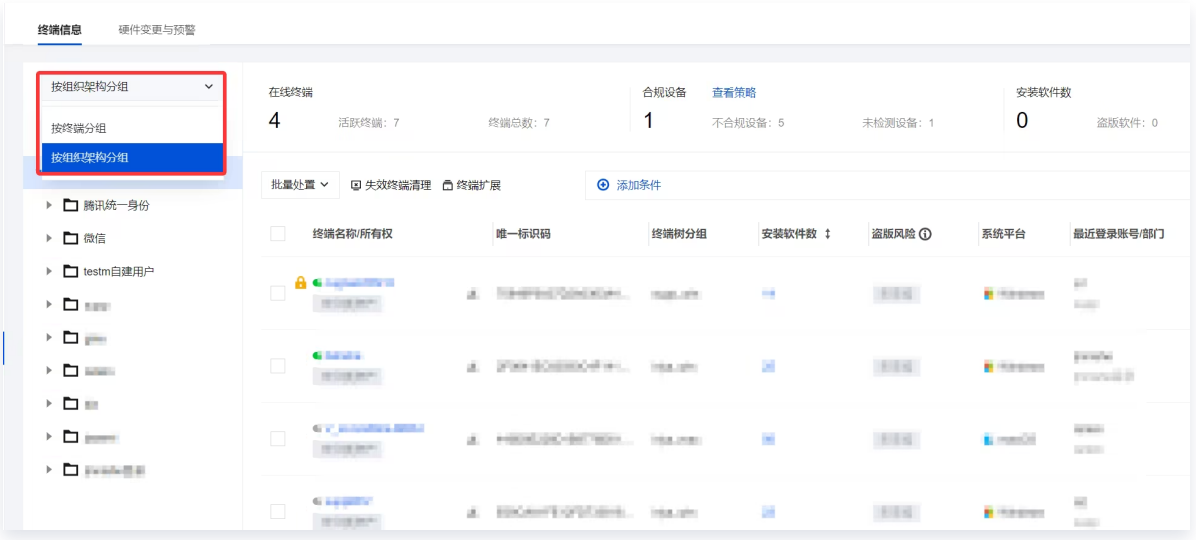
4. 在终端运维顶部单击**展示的数字**，快速联动筛选。



5. 单击**查看策略**，可一键进入策略详情页，查看所有下发策略的执行状态。



6. 支持按终端分组、按组织架构分组（人员视角）展示终端信息。



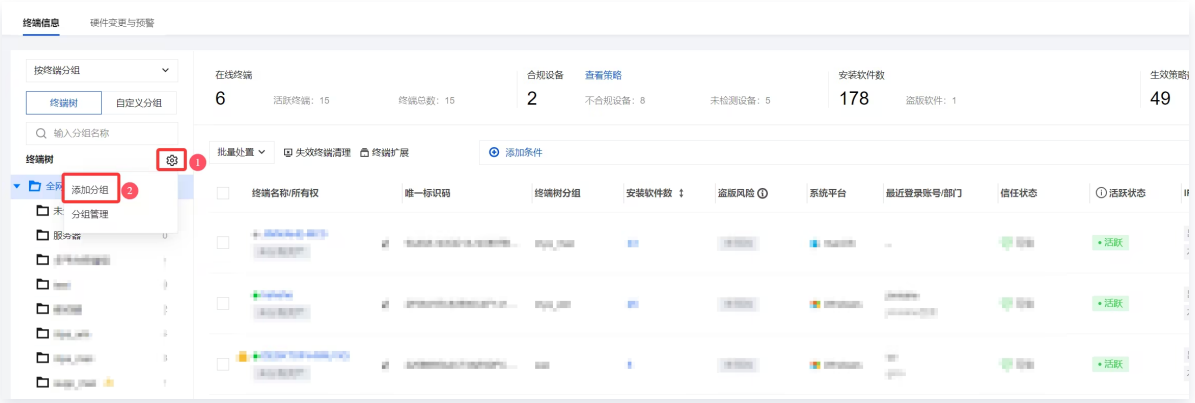
终端分组

1. 首次部署 iOA 的终端默认在“未分组终端”组，需要对终端进行分组，以便管理。

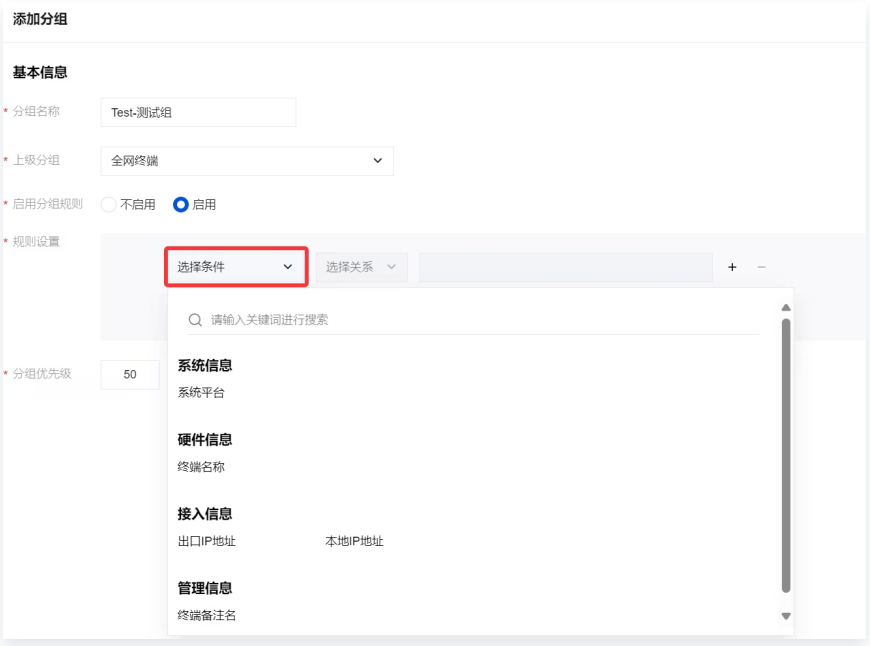
> **说明：**

> 若管理员配置了自定义分组规则，终端将定时自动划入对应分组。具体配置方法请参见 自定义分组 。

2. 单击 ，选择**添加分组**。

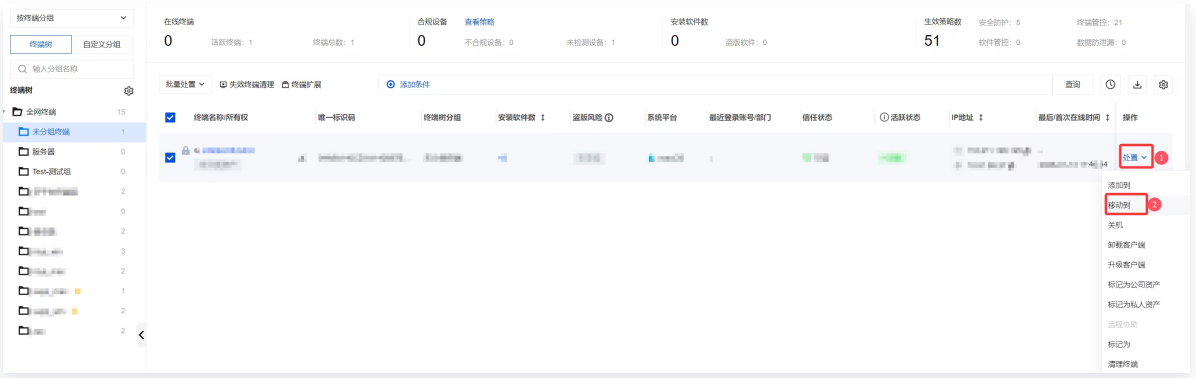


3. 编辑分组信息，配置完成单击**确定**。

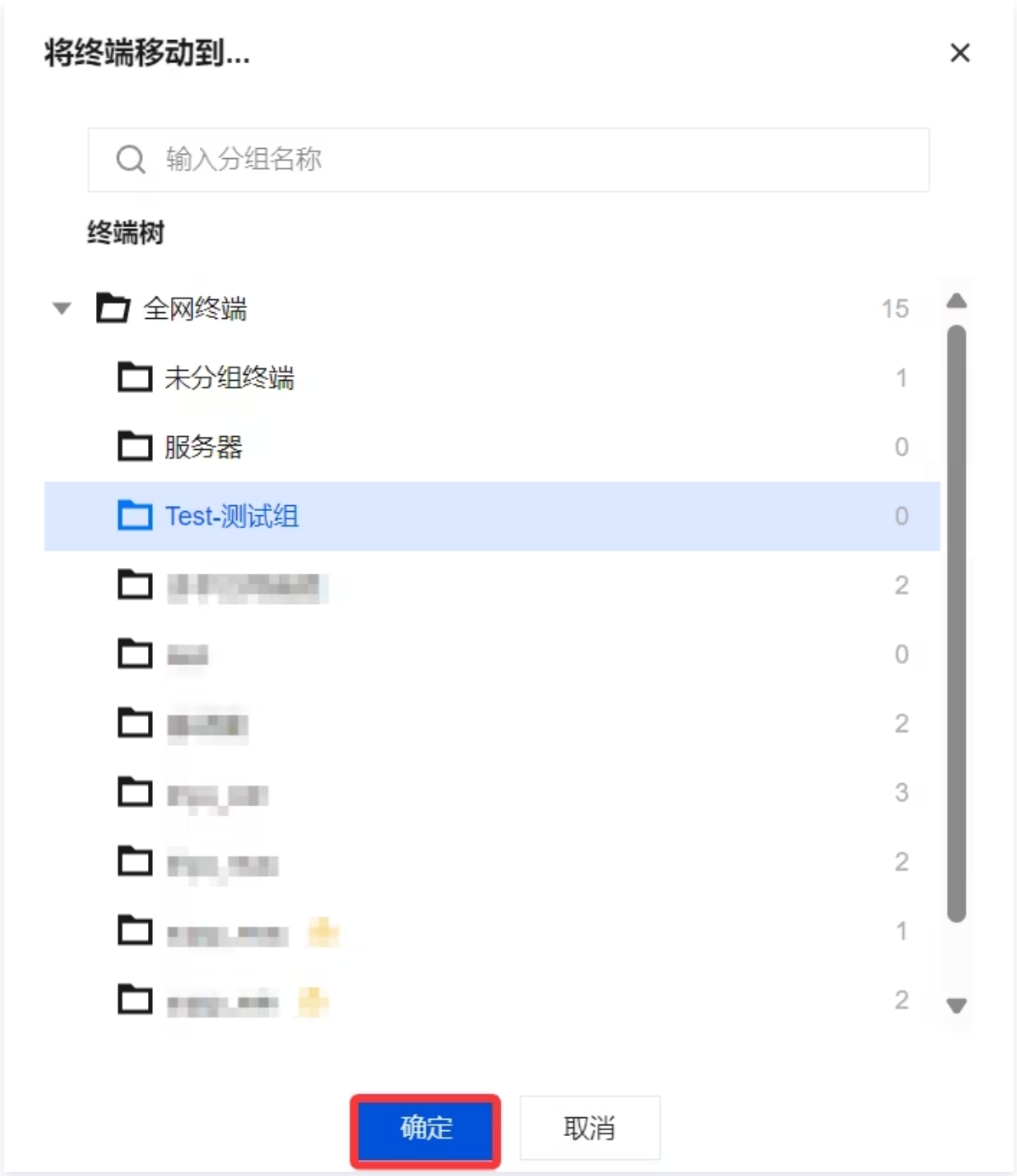
参数名称	说明
分组名称	自定义名称，各终端所在的分组名称。
上级分组	下拉选择终端所在的上级分组，默认全网终端，支持选择现有终端分组作为当前分组的上级组织。
启用分组规则	• 不启用：终端不进行自动分组。 • 启用：终端树分组支持根据本地 IP、终端名称、终端备注名等设定分组规则，终端设备将根据这些分组规则自动归入相应的指定分组。 

分组优先级	当终端同时满足多个分组规则时，可通过设置更高的优先级，确保终端优先加入目标分组（分组优先级设置越高，终端将优先归属至该分组）。

4. 分组创建完成，可将未分组终端移动到刚创建的分组中，勾选终端名称，单击**处置 > 移动到**。



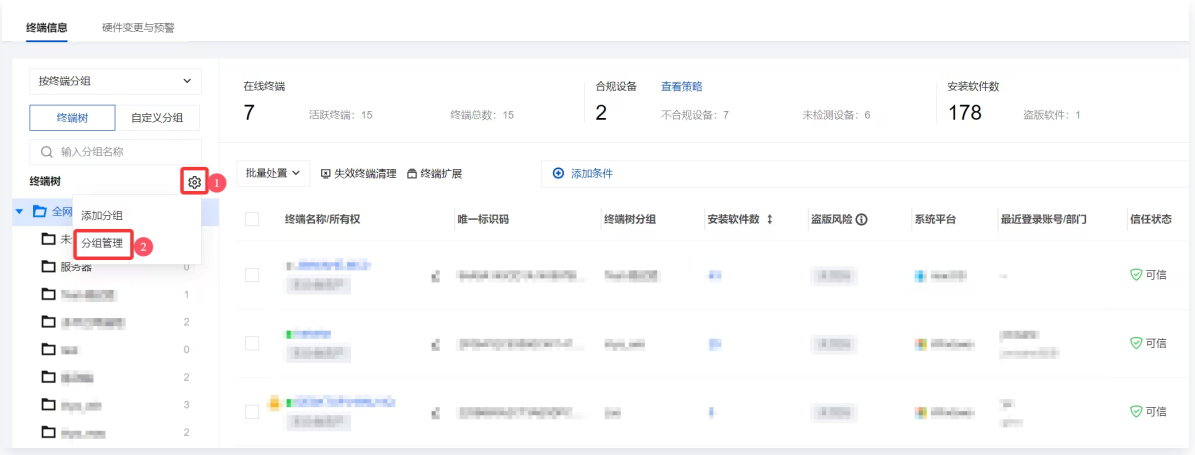
5. 选择需要移动到的组，单击**确定**。终端移动至对应的分组中。



分组管理

终端分组管理器

1. 单击 ，选择**分组管理**。



2. 终端自动分组设置：按终端对应的组织架构移动到对应的分组，不勾选则不会移动。

使用场景示例：各个部门的组织架构与终端绑定后，员工登录之后会自动移动到对应的部门。

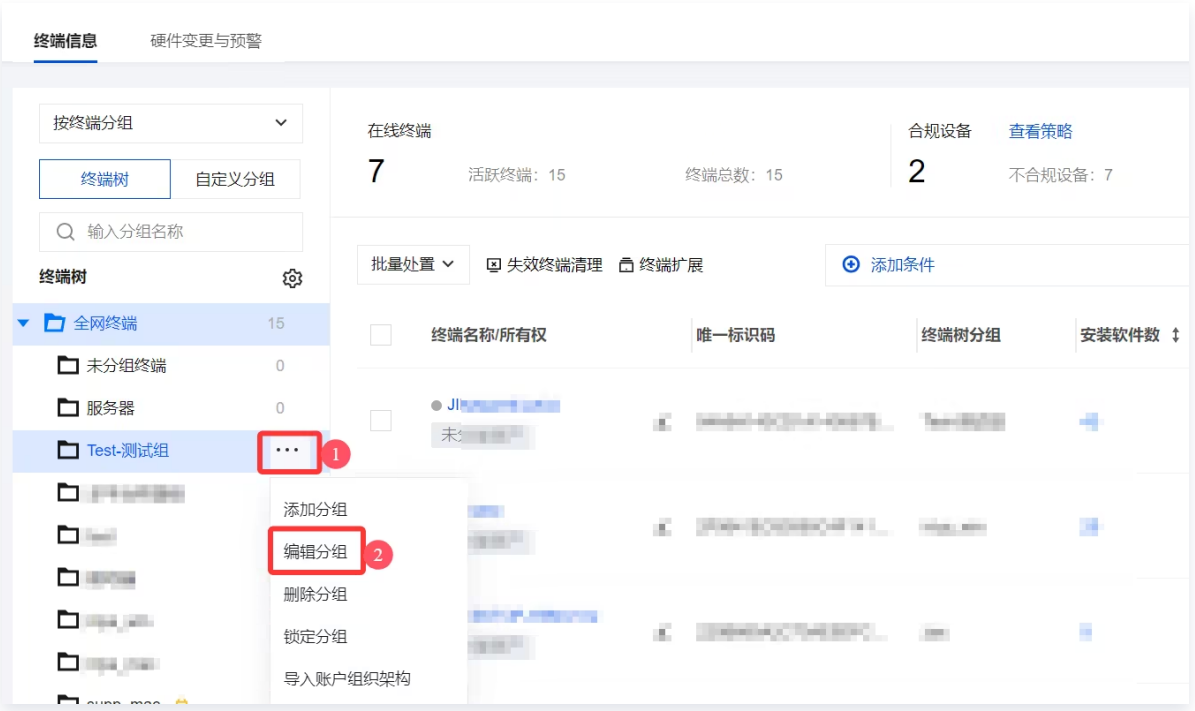


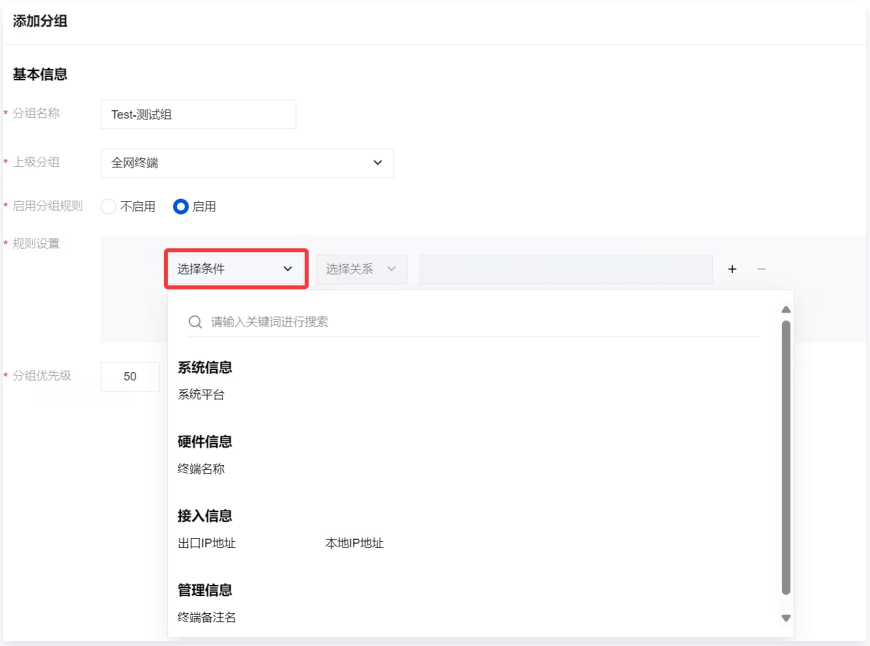
3. 终端手动分组：可移动终端至任意静态分组。



编辑分组

1. 单击 **• • •** ，选择**编辑分组**，可修改分组名称、分组信息。



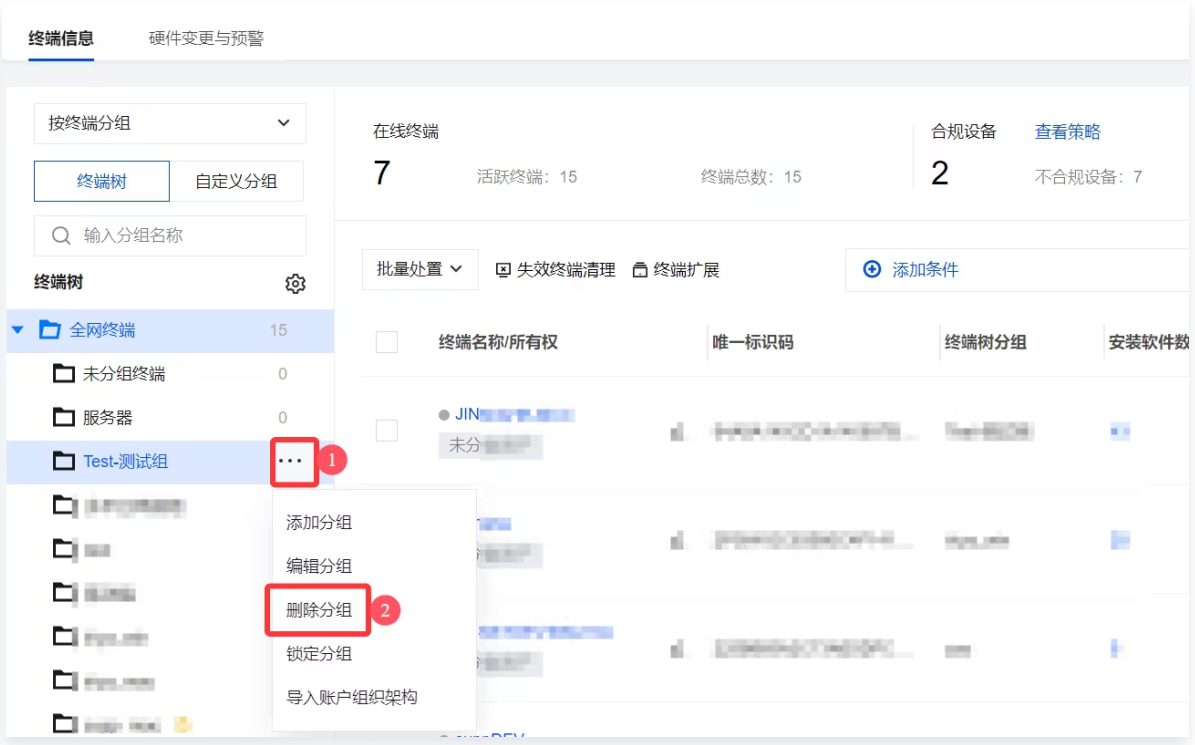
参数名称	说明
分组名称	自定义名称。
上级分组	默认全网终端，支持下拉选择其余终端组。
启用分组规则	• 不启用：终端不进行自动分组。 • 启用：终端树分组支持根据本地IP、终端名称、终端备注名等设定分组规则，终端设备将根据这些分组规则自动归入相应的指定分组。 

分组优先级	当终端同时满足多个分组规则时，可通过设置更高的优先级，确保终端优先加入目标分组（分组优先级设置越高，终端将优先归属至该分组）。

删除分组

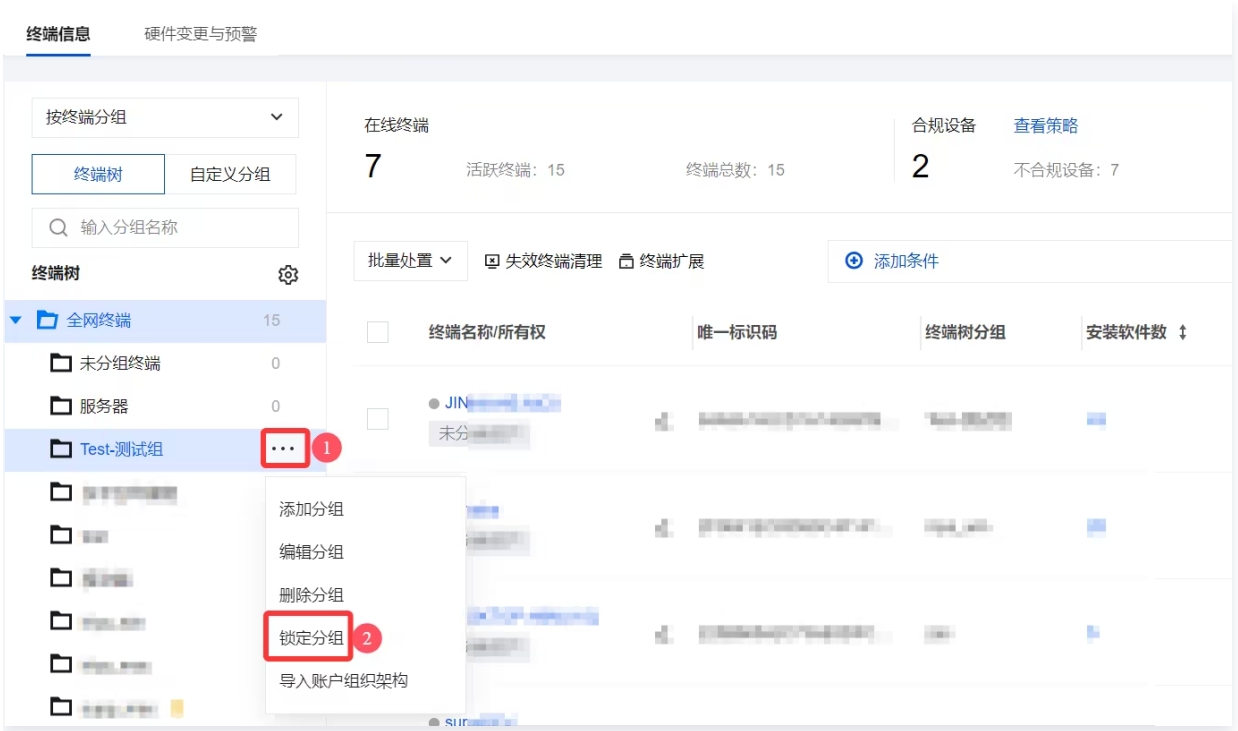
1. 删除对应分组后，原分组内的终端需要重新分配组，请在删除分组前做好分类。

2. 单击 ···，选择**删除分组**，失去分组的终端，将移动至您选择的分组中。



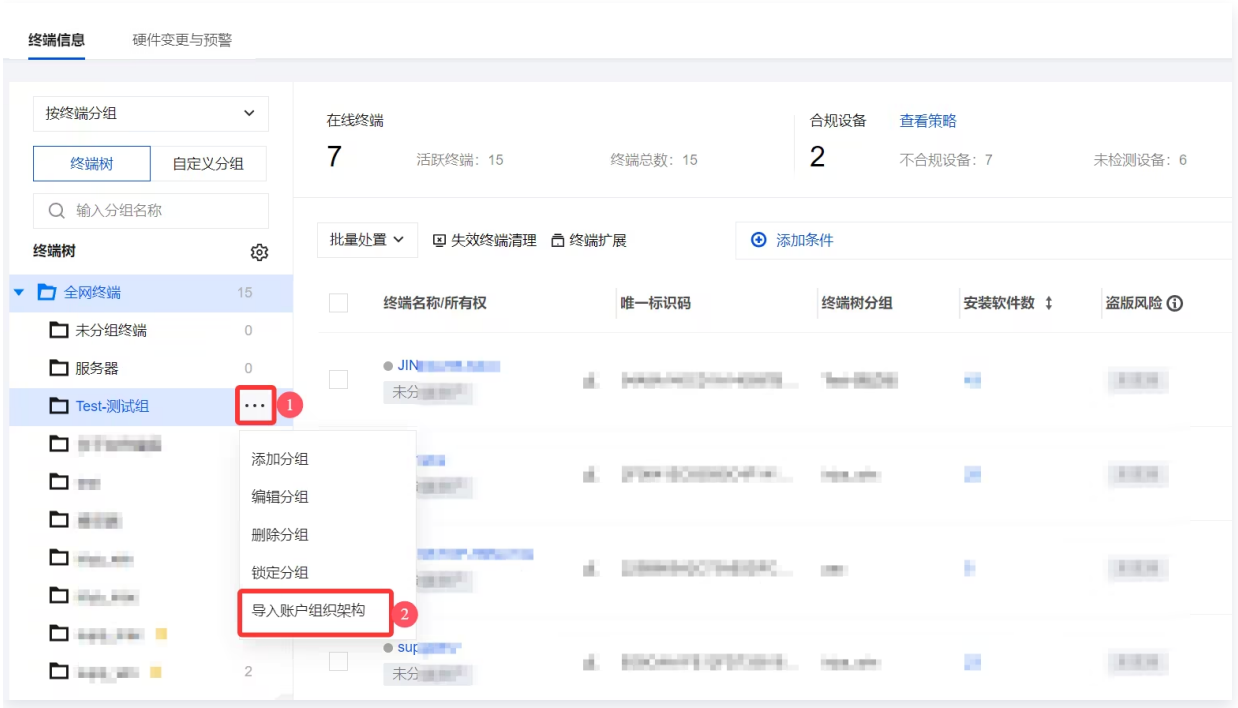
锁定分组

单击 ···，选择**锁定分组**，提示锁定成功。锁定后，终端将不跟随组织架构同步或其他自动移动策略进行分组变更，仅可通过手动移动所属分组。



导入账户组织架构

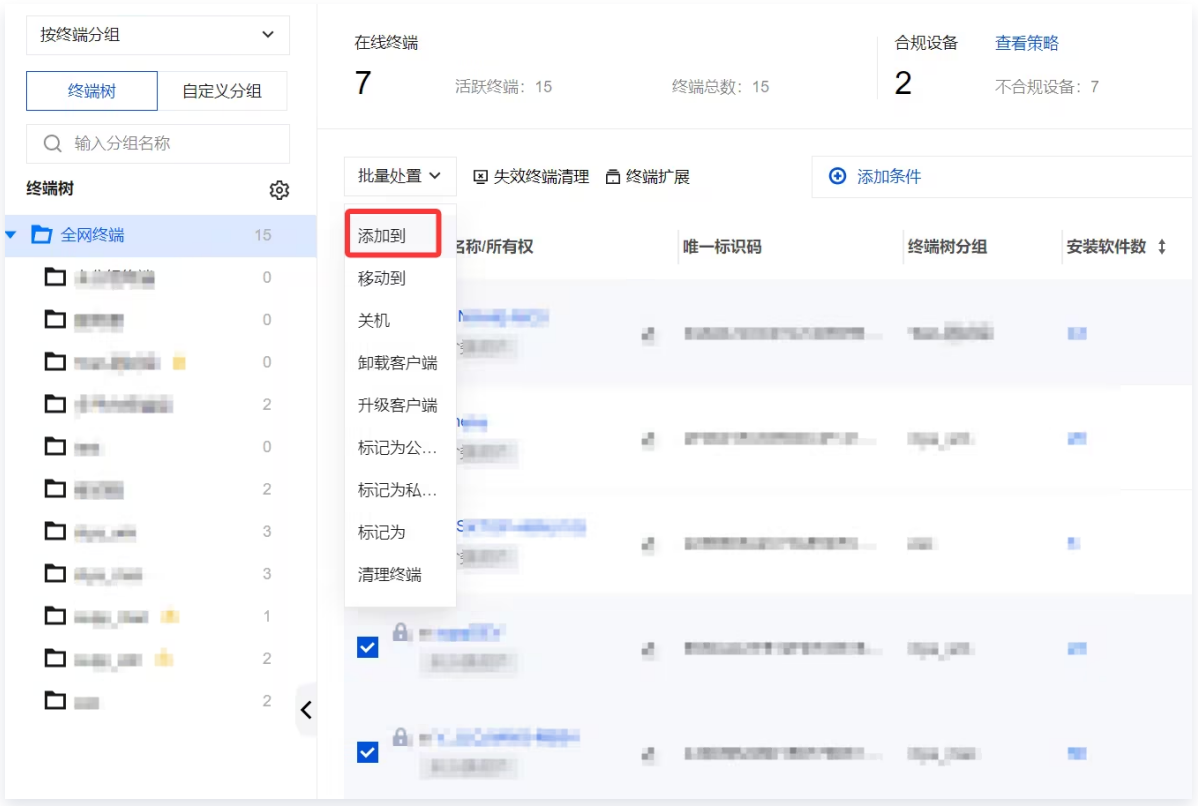
单击 • • • ，选择**导入账户组织架构**，导入用户与授权管理处的组织架构，客户端通过账号登录时，该终端就会按照账号所处的架构自动移动到分组。



批量处置

添加到

1. 将终端添加到自定义分组中，单击**添加到**，将已选中的终端批量添加到指定自定义分组中。



2. 勾选创建的自定义分组，单击**确定**，完成将终端添加到自定义分组的操作。

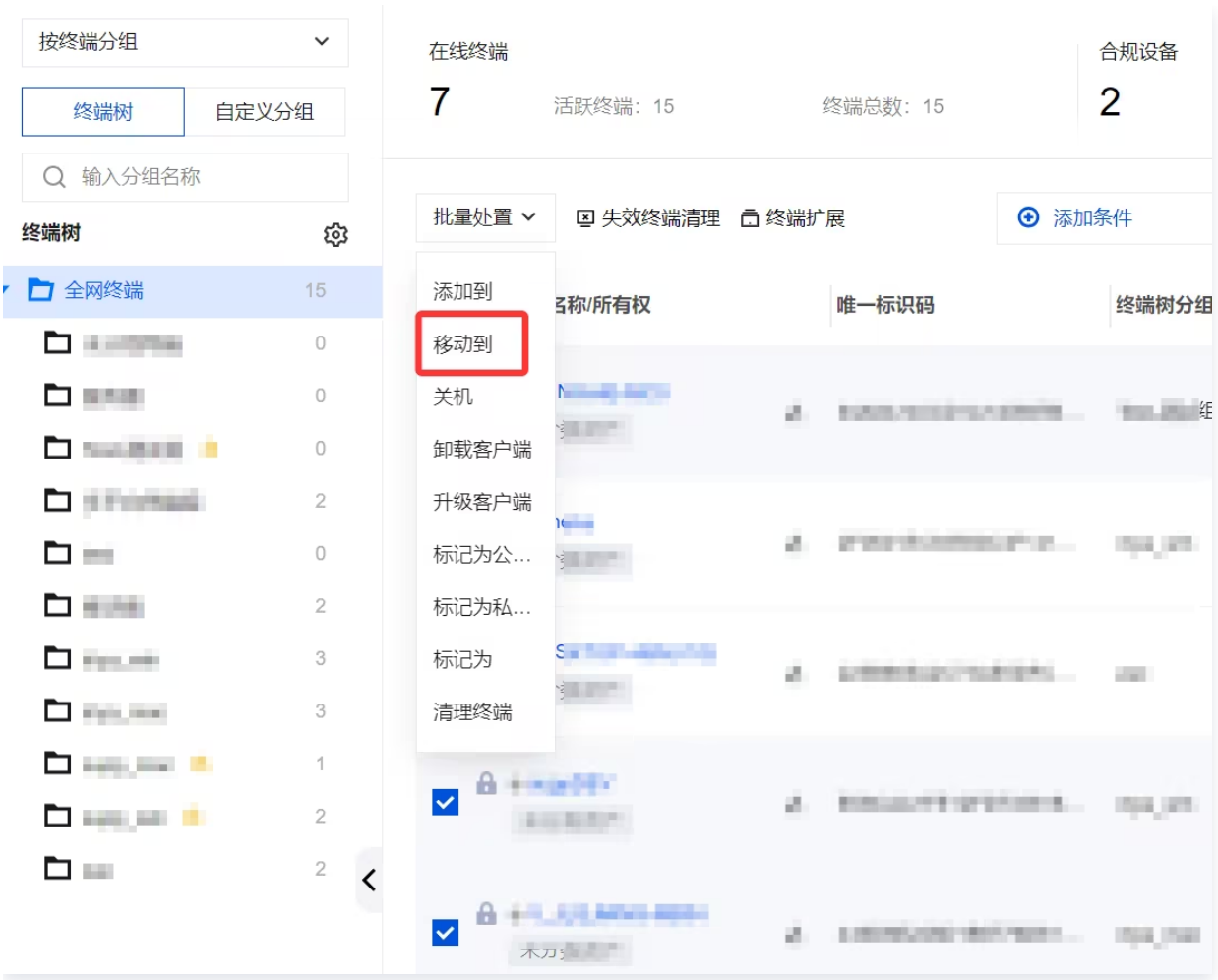


3. 若当前终端分组无法满足需求，您可单击**新增自定义分组**，输入自定义名称并保存。完成自定义分组创建后，勾选创建的自定义分组，将终端添加到自定义分组中。



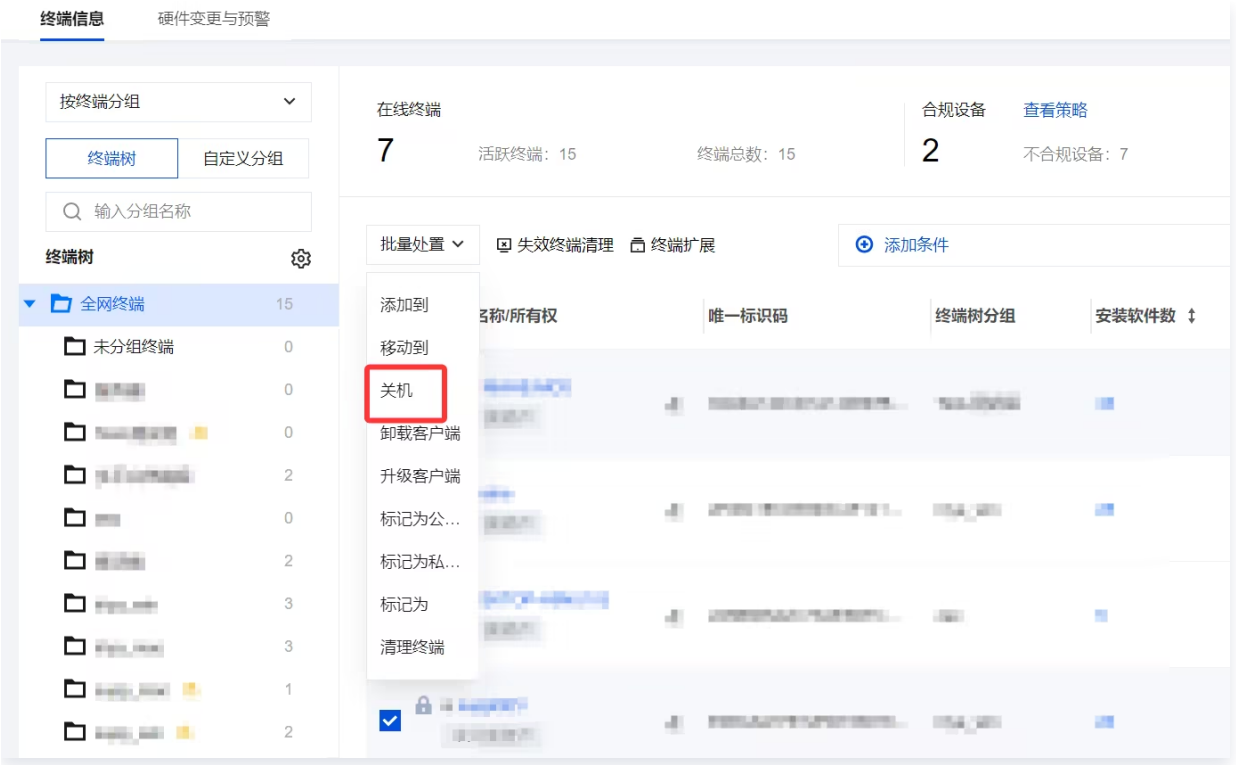
移动到

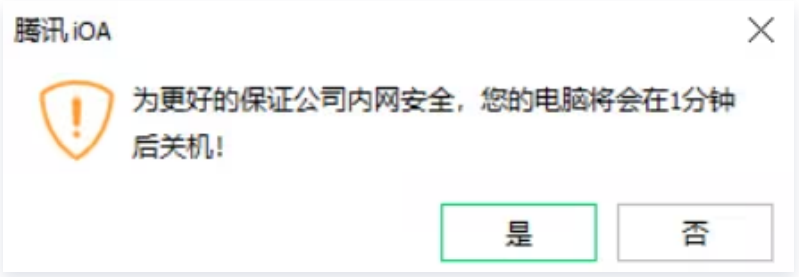
将终端移动到对应分组，选择需要移动到的组，单击**确定**。



关机

远程控制终端关机，勾选需关机的终端，单击关机。

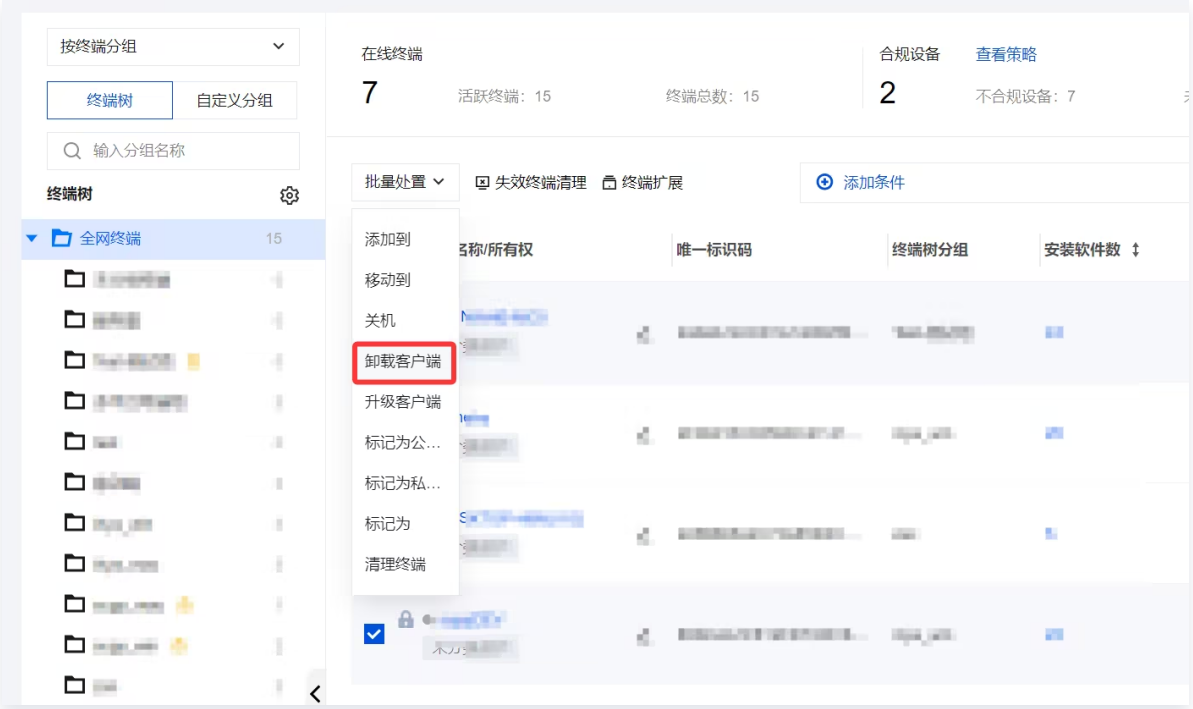


参数名称	说明
关机前提醒	• 勾选**关机前提醒**，终端在关机前弹窗提醒用户电脑将在**分钟后关机。  • 不勾选**关机前提醒**，则到达时间后直接关机，终端无弹窗提示。
超时后默认不执行	• 勾选**超时后默认不执行**，则用户如果在提示时间内没有响应，默认不执行关机。 • 不勾选**超时后默认不执行**，关机提醒的提示时间内用户无响应，执行关机。
关机**分钟前，用户收到**信息	• 自定义时间，设置后终端在您设置的时间到达后自动关机。 • 自定义信息，下拉选择自定义信息，可编辑终端的弹窗内容。

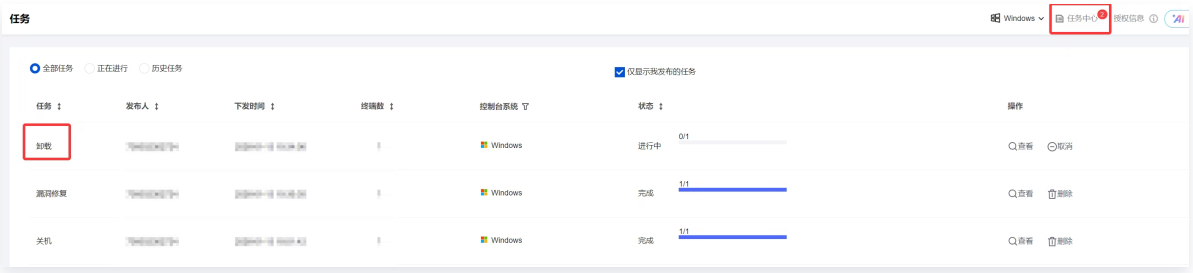


卸载客户端

1. 勾选需卸载 iOA 客户端的终端，单击**卸载客户端**。



2. 任务中心下发卸载任务， 终端收到任务执行卸载操作。



升级客户端

1. 可校验终端的 iOA 版本，如果不是最新版，会下发升级提示。勾选需升级的终端，单击**升级客户端**。

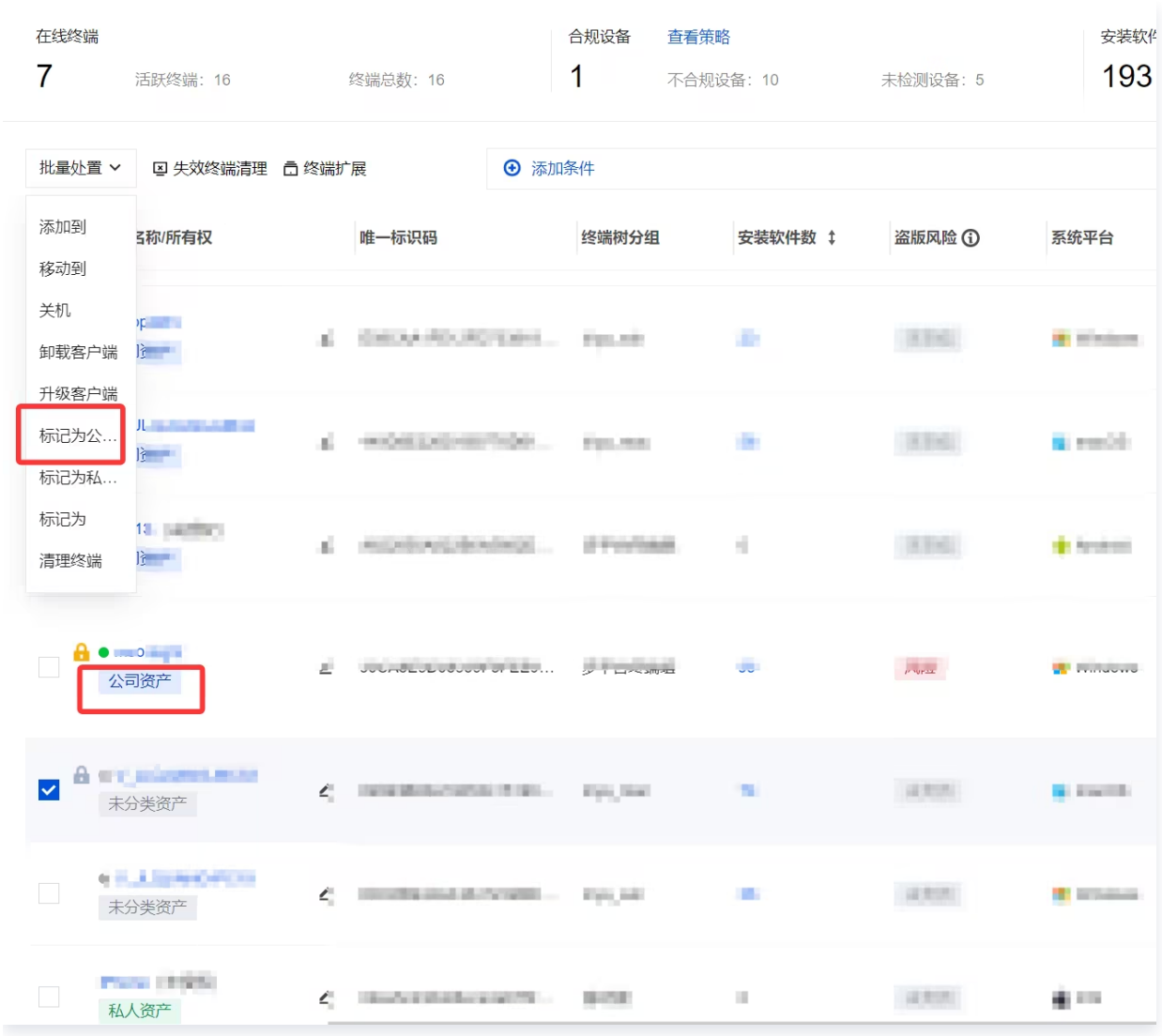


2. 提示已成功建立任务，单击**任务中心**，可查看升级任务。



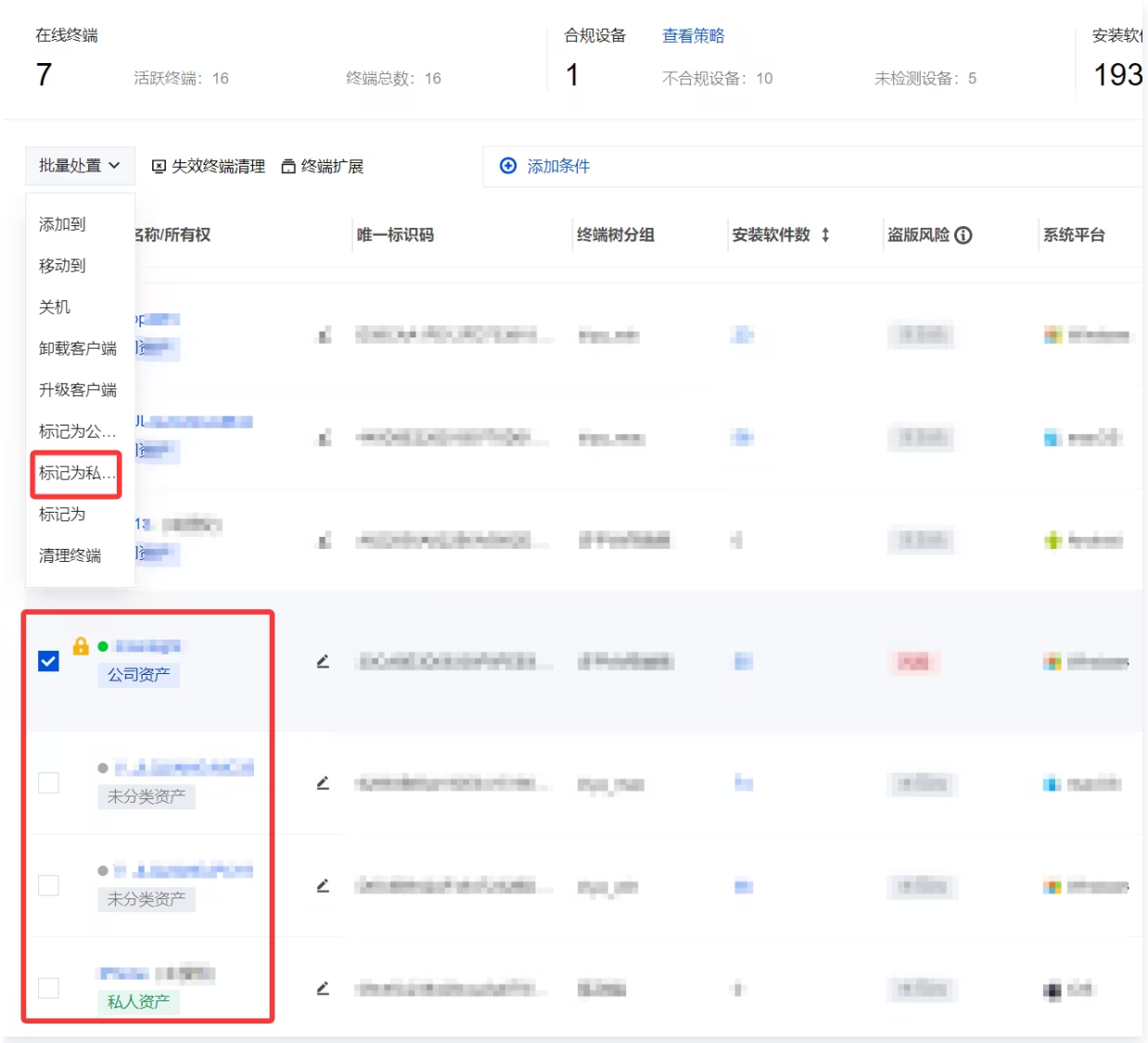
标记为公司资产

标记为公司资产的终端，未分类资产/私人资产的标记变更为公司资产。



标记为公司资产

标记为私人资产的终端，未分类资产/公司资产的标记变更为私人资产。



标记为

1. 为终端增加标签，可以根据终端的标签信息搜索查询，单击**标记为**，编辑标签后保存。



2. 标记后可在终端列表中查看标签。



清理终端

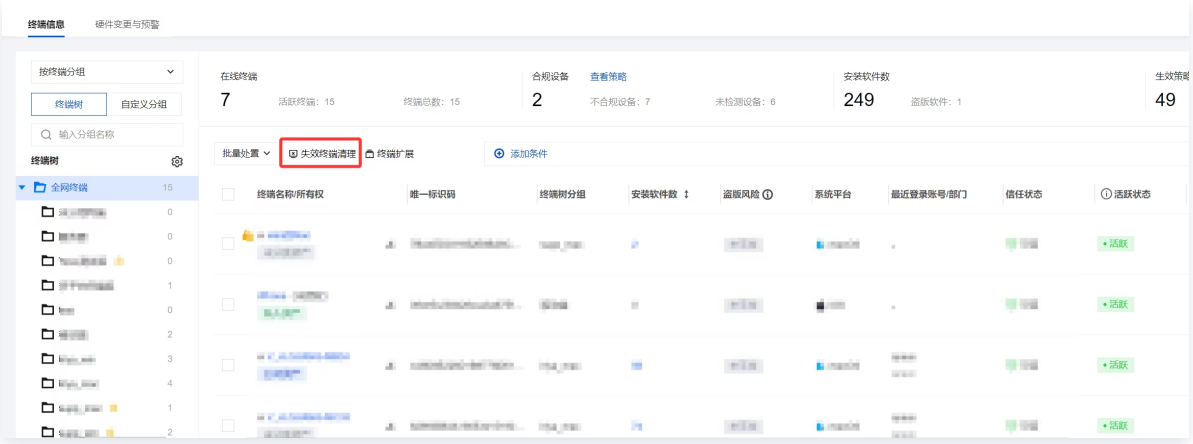
1. 清理终端后，该终端将被移出终端信息列表，不再受控制台管控。
2. 终端为离线状态时，单击批量处置，选择清理终端。
3. 经二次确认后，终端已清理完毕并移除不可见状态，同时回收相关授权。
4. 已清理的终端再次上线时授权将自动恢复。



失效终端清理

1. 清理过期终端，释放授权数量，单击**失效终端清理**。

> **注意：**
> 会同步清理**无边界办公 > 应用管理 > 接入设备管理**页面的设备项数据。



2. 活跃状态设置：自定义天数，X天内有登录则判定为活跃终端，否则为非活跃终端。

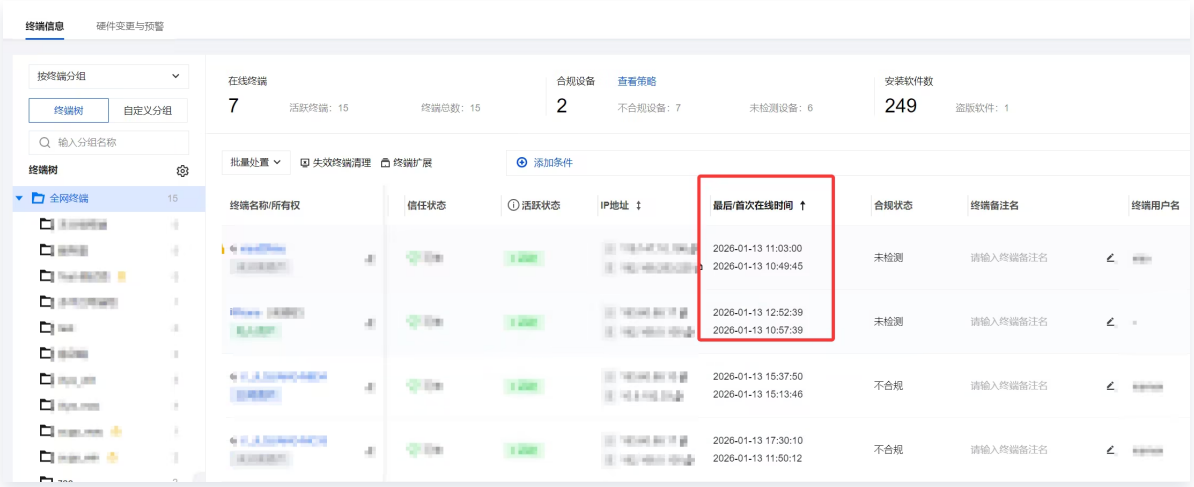


3. 过期终端清理：默认设置为“不清理过期终端”，若设置自动清理离线X天（示例：5天）及以上的终端后，系统将在设定时间内定时清理终端（整点及半点后开始清理，非实时清理），配置完成单击**确定**保存。



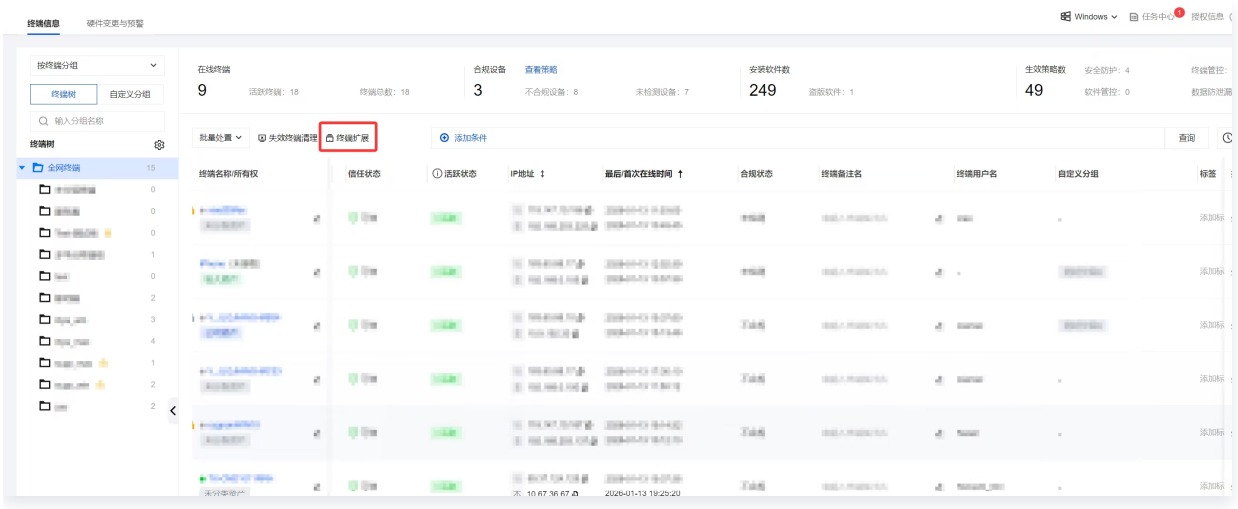
4. 清理完成后再次打开**终端信息**页，最后在线时间距今时间大于5天的终端被清理，不再显示。

> **说明：**
> - 终端被清理后重新上线，会再次显示在终端信息中。
> - 终端被清理后，若有超出授权的终端，也会显示上线。



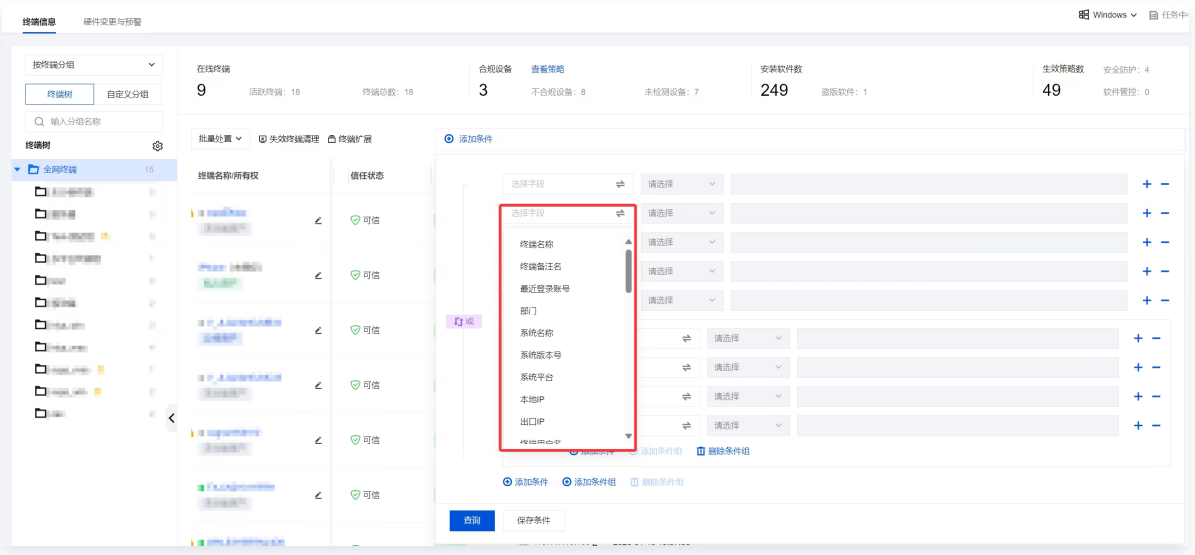
终端扩展

统一登记和管理企业内外终端的所属权与信息，终端扩展配置请参见文档**终端扩展**。

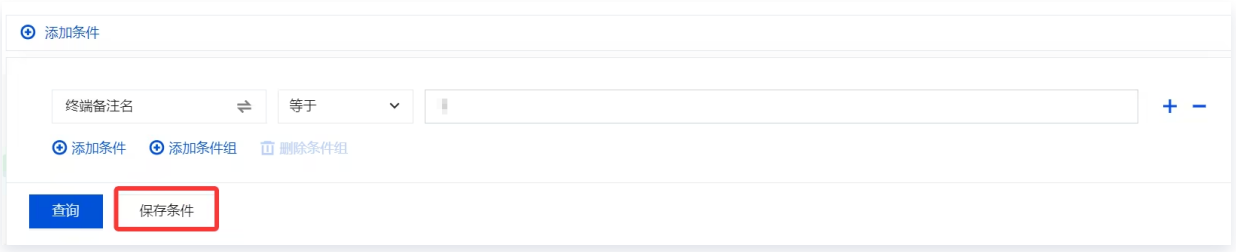


添加条件

1. 允许管理员通过组合多个条件，从海量终端设备中定位目标设备。支持按终端名称、IP、账号、部门、系统属性等多维度进行交叉筛选。
2. 添加筛选条件：单击**添加条件**，从字段列表（如“终端名称”、“部门”）中选择一个维度，在右侧设置具体值（如输入终端名称、选择部门）支持创建“且/或”逻辑分组。
3. 组合复杂条件：单击**添加条件组**可创建“且/或”逻辑分组，实现更复杂的多条件组合查询。



4. 执行与保存：条件设置完毕后，单击**查询**查看结果。如需常用该组合，可单击**保存条件**并为其命名。



5. 单击保存的查询 ，可直接选择查询条件名称(单击蓝色的查询条件名称)，查询该条件范围内的终端。



导出

1. 单击导出按钮 ，导出终端信息表。您可前往任务中心查看进度并下载数据。

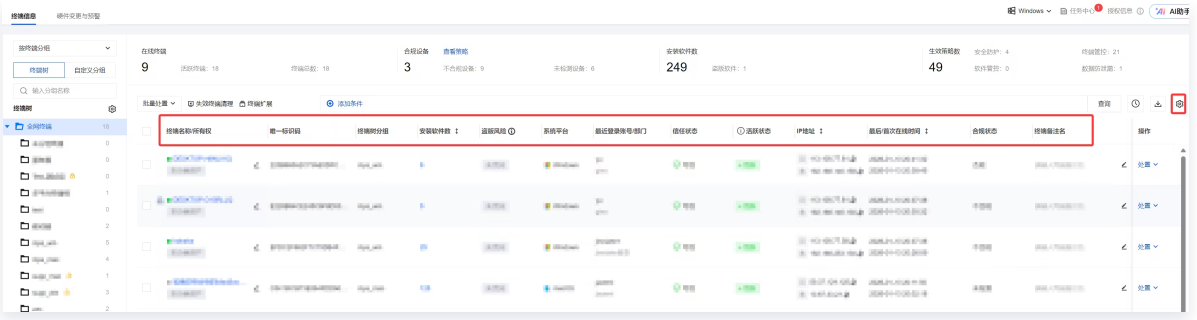


2. 在任务中心单击**下载**，查看导出的终端数据。

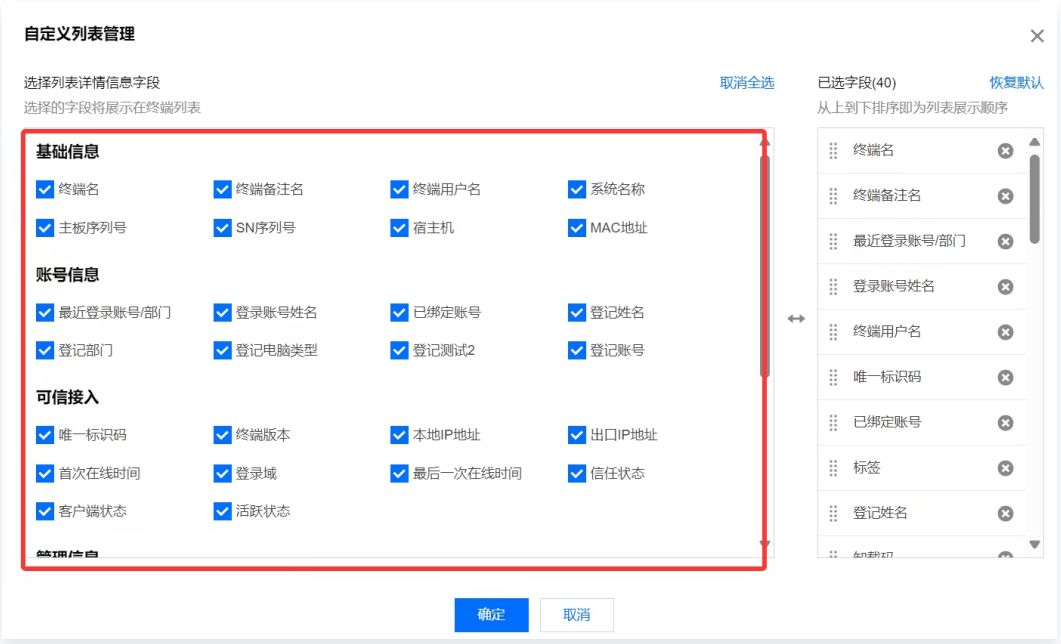


自定义列表管理

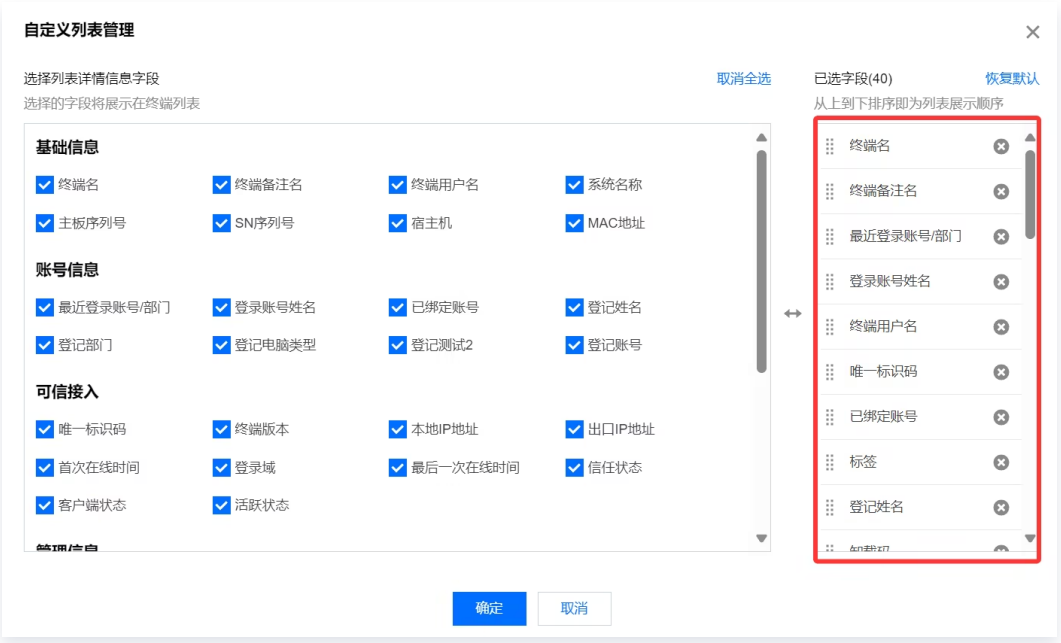
1. 终端树列表字段可自定义配置是否展示，单击**设置**。



2. 终端列表各信息字段支持分类显示，勾选的字段将展示在列表中，不勾选则列表不展示该字段。



3. 支持设置字段在列表的顺序，拖拽字段名，即可调整该字段在列表的展示顺序。



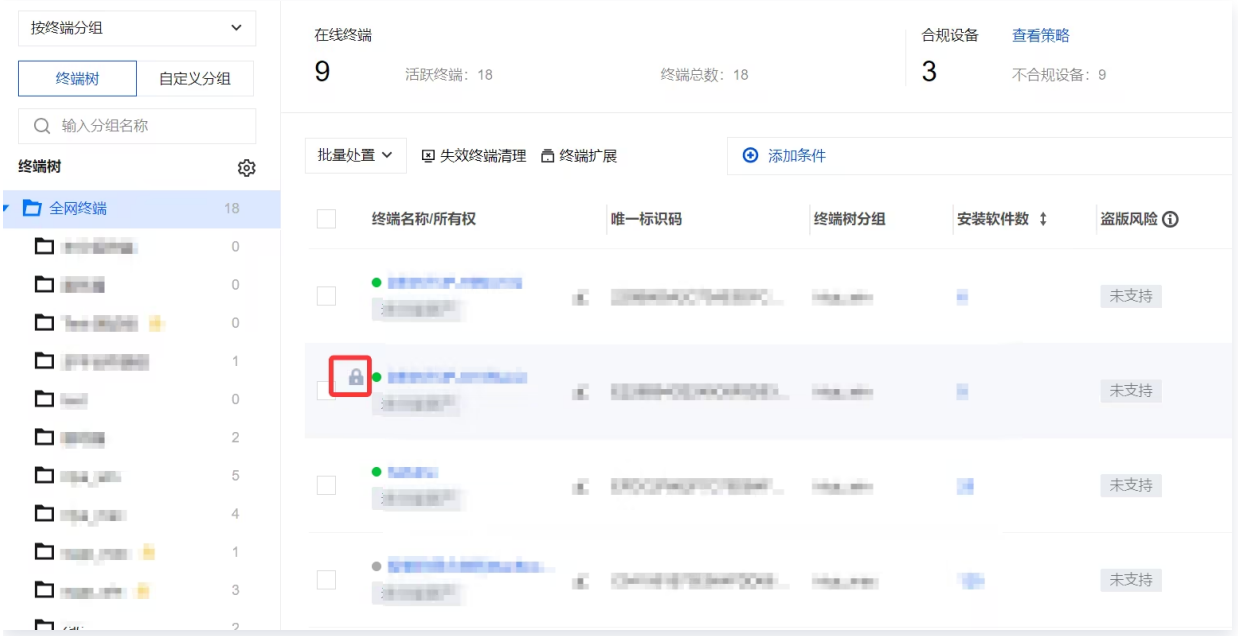
终端更名

在终端列表/终端详情页面中，支持终端名称修改功能，编辑新名称后将向终端下发名称修改指令，**新名称将在终端重启后完全生效**。管理员无需逐台登录终端设备即可完成终端名称统一管理。



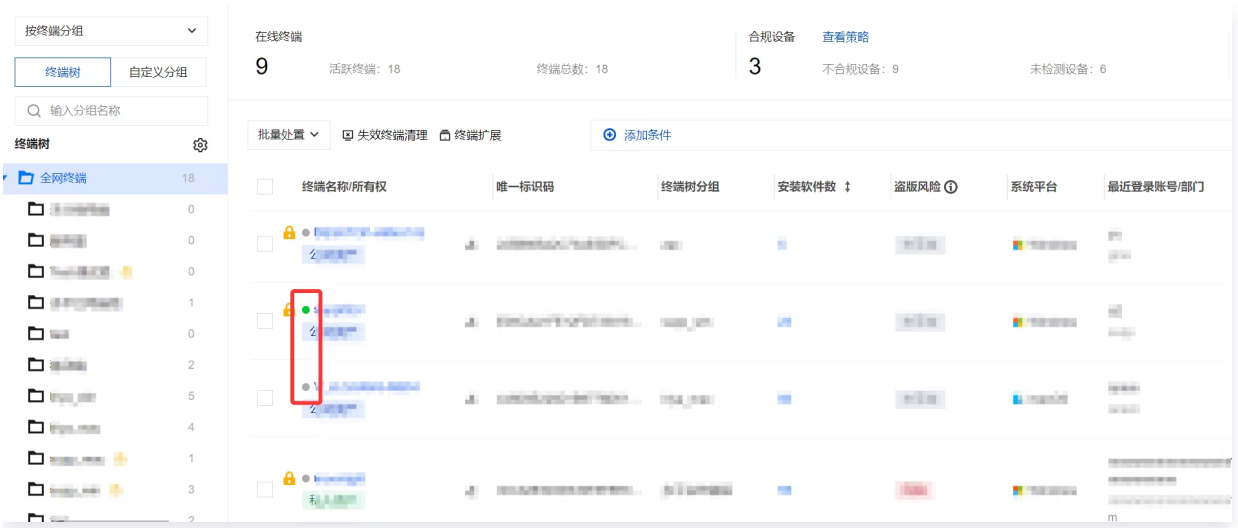
锁定终端

终端不会被自动移动(不受组织架构更新及IP自动分组影响)，仅支持手动移动。



在线终端标识

在线终端为绿色圆形图案，离线终端为灰色圆形图案。



AI 健康度分析

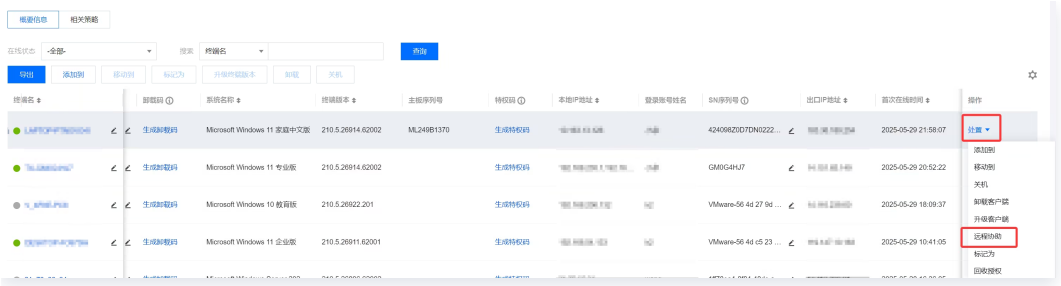
支持 AI 健康度分析，结合终端硬件信息与近期性能监控情况，支持对指定终端进行硬件健康情况分析并输出更换建议（支持结果导出），帮助 IT 管理员发现/分析资产老旧情况，降低资产运营成本。

- 未进行分析的终端：单击**健康分析**可对该终端的健康度进行分析并输出结果，
- 已进行分析的终端：展示上次分析结果，展示 AI 分析详情，支持对当前结果进行重新生成，支持复制。
- 已分析且检测到硬件信息更新的终端：展示上次分析结果，并提示有硬件信息更新。



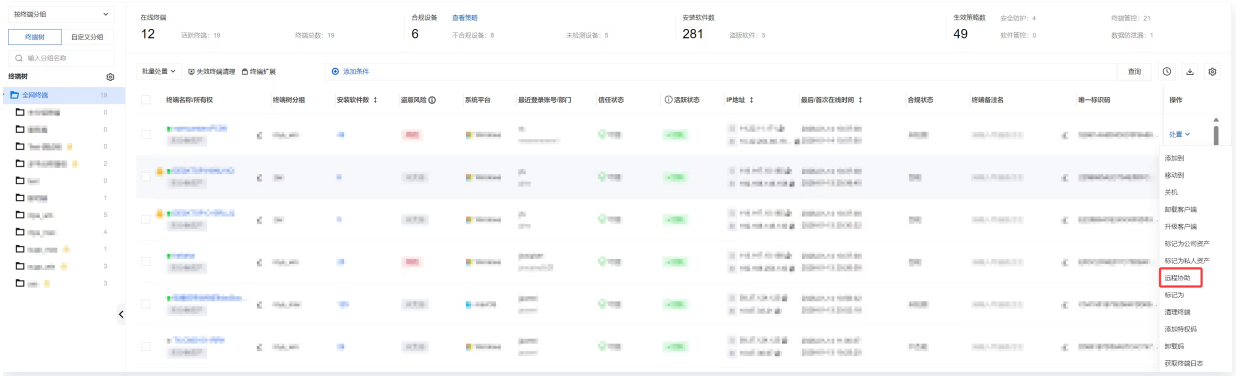
处置

下拉处置菜单栏，用于对选定对象进行不同的操作，如添加、移动、关机、卸载客户端等。



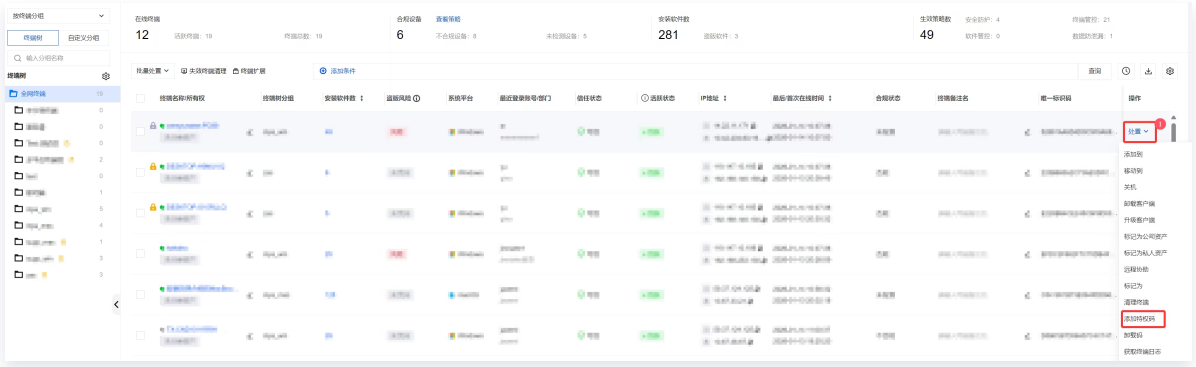
远程协助

选择需要远程的在线终端，单击**远程协助**，终端接受远程后，即可通过控制台远程控制终端。



添加特权码

1. 单击**添加特权码**，获取终端特权码信息。



2. 该特权码仅在当天对该设备有效。您需将特权码发送给用户，用户在终端设备上输入该特权码后，进入特权模式，特权模式将会完全屏蔽所有安全、管控等策略以模拟卸载后的环境，常用于客户端排障。详细配置请参见 允许客户端进入特权模式 。



卸载码

单击卸载码，获取终端卸载码信息，该卸载码仅在当天对该设备有效。您需将卸载码发送给用户，用户在终端设备上输入该卸载码后，iOA 客户端成功卸载。详细配置请参见 允许客户端卸载 。



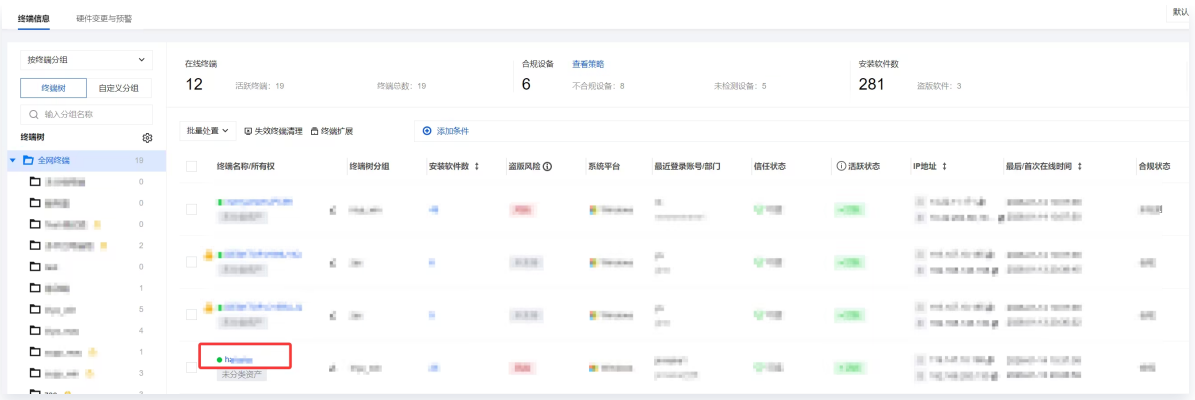
获取终端日志

单击获取终端日志，获取终端全量日志信息。

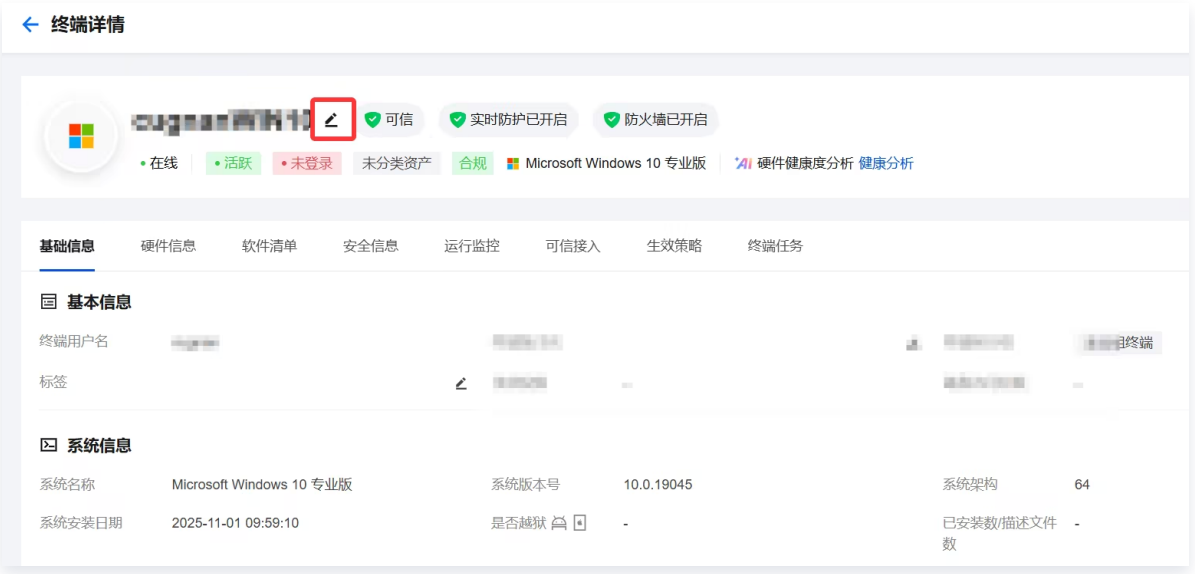


终端详情

1. **单击终端名称（蓝色字体），进入终端详情。**



2. 终端详情页的终端名称支持修改，修改终端名称后，可前往**资产运维 > 终端运维 > 硬件变更与预警 > 硬件变更**查看操作的日志记录功能，硬件变更中展示终端名称修改的前后信息，便于追溯管理员修改终端名称的操作历史。



3. 终端详情页包含清理终端、远程协助、基础信息、硬件信息、软件清单、安全信息、运行监控、可信接入、生效策略、终端任务等信息，iOA 客户端支持实时同步采集终端性能参数，并上传服务端做数据展示，方便观察终端使用情况，为相关问题处理及设备更换提供依据。
4. 清理终端：终端为离线状态时，可单击**清理终端**，清理后终端移除不可见，并回收授权。



5. 支持对在线终端进行远程协助，远程协助请查看章节：控制台到端使用远程协助 。



基础信息

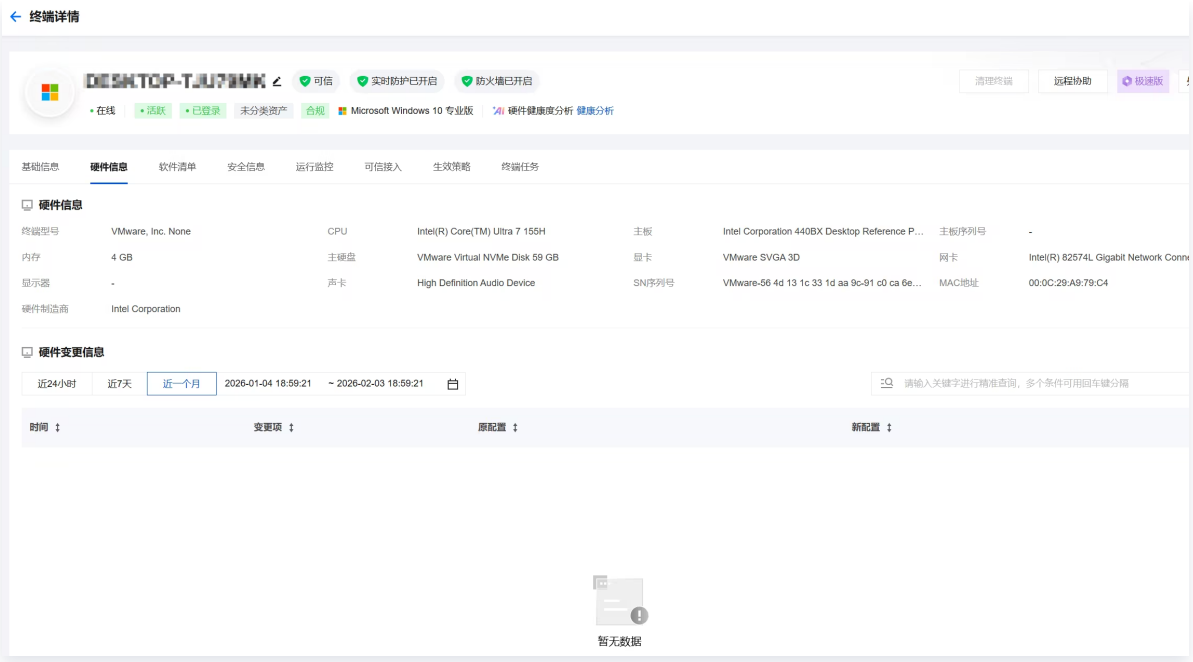
1. 终端基础信息展示硬件信息、系统信息、账号信息、客户端信息。支持在终端详情获取该终端卸载码与特权码。



硬件信息

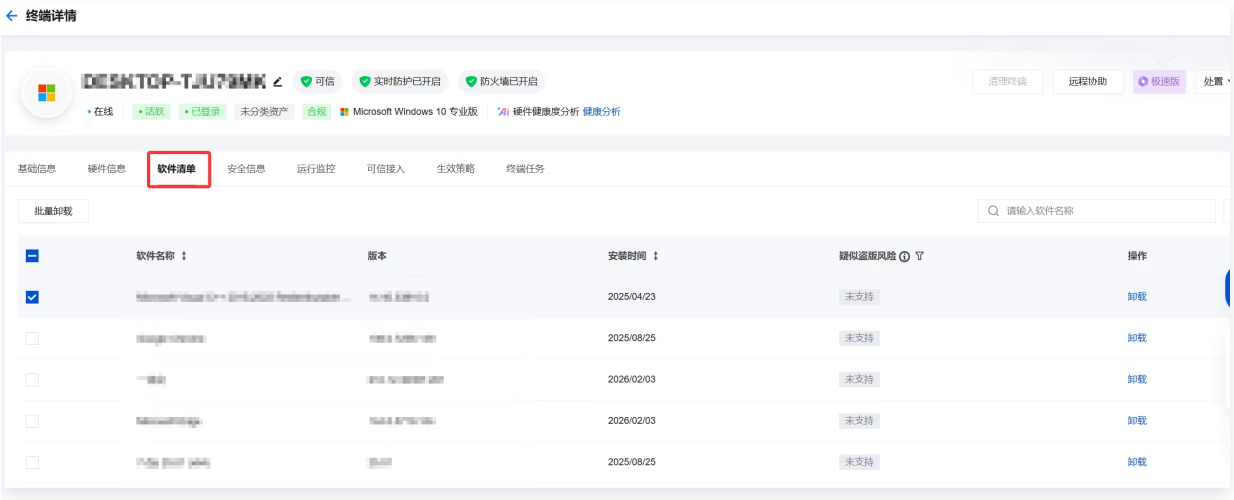
1. 硬件信息：显示终端设备的详细配置：CPU、内存、硬盘、显卡、主板、网卡、声卡等关键组件信息。
2. 硬件变更信息：追踪硬件配置的变更历史，可按时间维度（近24小时/近7天/近30天/自定义）筛选查看变更详情。

版权所有：腾讯云计算（北京）有限责任公司



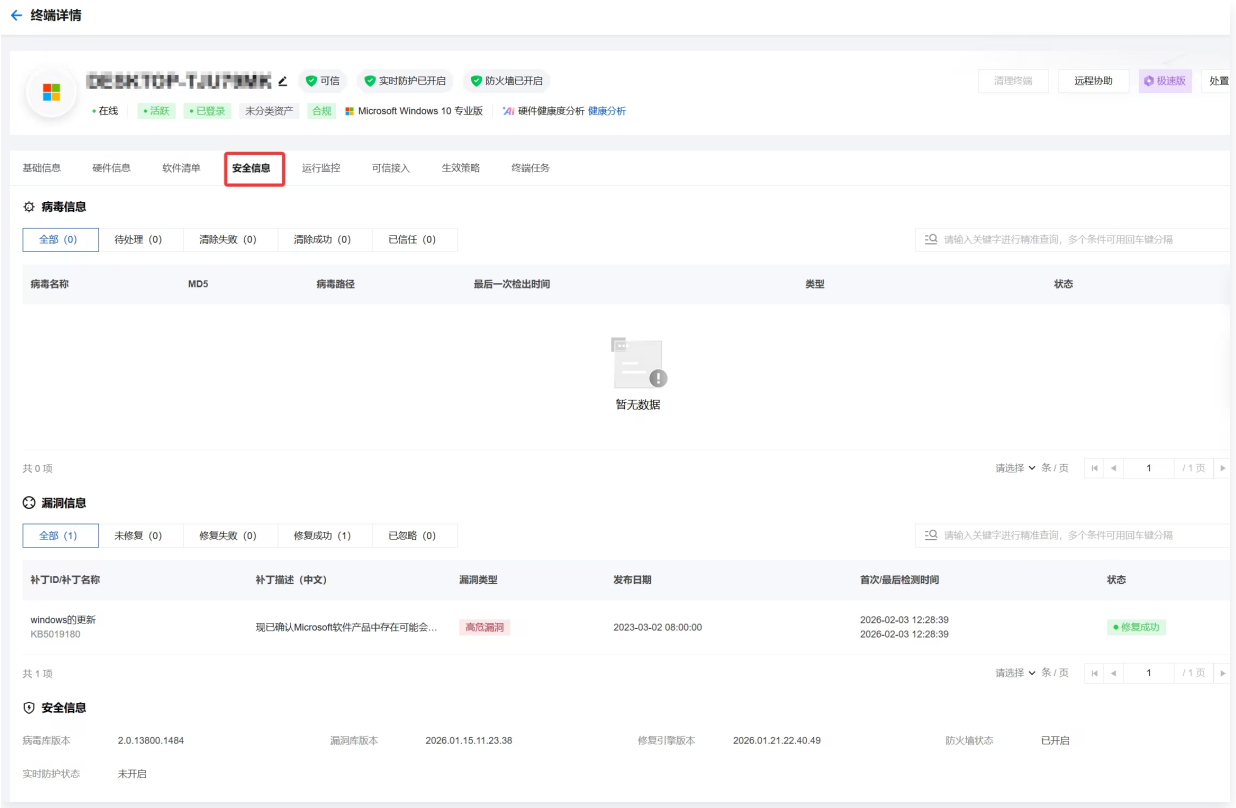
软件清单

展示终端已安装软件列表，支持批量卸载和按软件名称搜索，同时支持软件疑似盗版风险检测。



安全信息

集中展示病毒查杀记录、系统漏洞修复状态（含高危漏洞标识）及安全组件运行状态，支持按处理状态筛选查询。



运行监控

1. 运行监控请在**客户端管理 > 客户端策略 > 客户端通用设置 > 终端运行状态监测**中**开启终端运行状态监测**，开启后，收到此策略的终端将在其**终端信息 > 终端详情 > 运行监控**内上报显示本机 CPU、内存、存储空间使用情况。



2. 运行监控支持查看存储空间\CPU监控、内存监控、网络信息、进程信息、服务信息、共享目录。



监控类型	详情

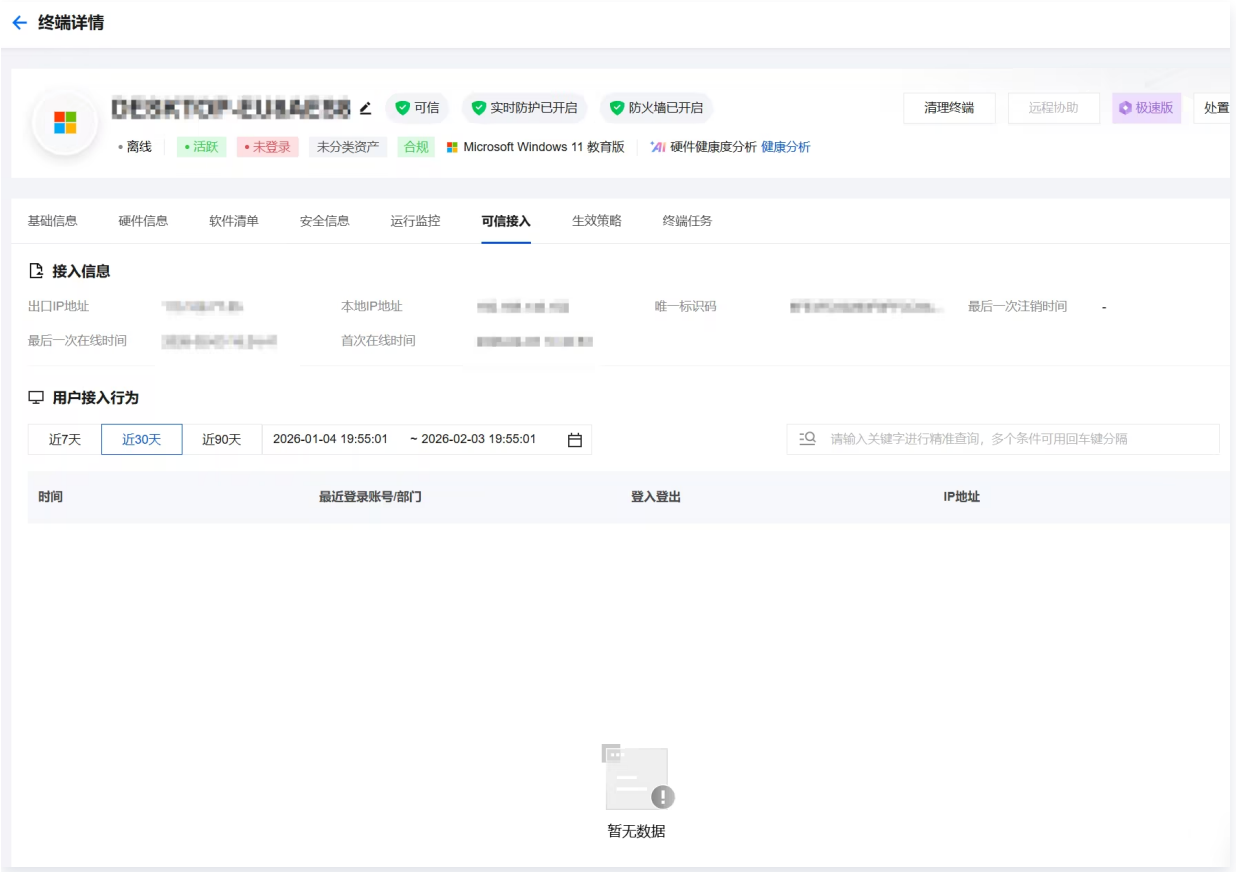
存储空间	• 显示磁盘存储使用情况。
	• 不同平台存储空间计算方法不同
	  ○ Windows: 1GB=1024MB
	  ○ macOS: 1GB=1000MB

CPU 监控	• 获取终端 CPU 温度监控请在**客户端管理 > 客户端策略 > 客户端通用设置 > 终端运行状态监测**中开启终端运行状态监测开关。并重启设备后，终端将每十五分钟更新一次数据。 • 当设备为虚拟机时，CPU 温度会显示为0，原因：CPU 温度获取依赖于硬件支持，若设备为虚拟机（虚拟机本身并非真实硬件），因此无法模拟出硬件所具有的温度特性，同时也难以穿透虚拟环境去读取真实物理机硬件的温度数据。
内存监控	• 内存监控信息包含（内存使用量、iOA 内存使用量、CPU 使用量）。 • 获取内存监控数据请在**客户端管理 > 客户端策略 > 客户端通用设置 > 终端运行状态监测**中开启终端运行状态监测开关。并重启设备后，终端将每十五分钟更新一次数据。
网络信息	展示协议、进程名称、本地地址、本地端口、远程地址、远程端口、状态信息；网络信息仅支持 Windows 系统，此页面数据需要实时获取，请确保终端在线。

进程信息	展示进程名称、用户、命令行、内存占用、进程路径信息；进程信息仅支持 Windows 系统，此页面数据需要实时获取，请确保终端在线。
服务信息	展示服务名称、描述、用户、启动类型、状态、命令行信息；服务信息仅支持 Windows 系统，此页面数据需要实时获取，请确保终端在线。
共享目录	共享目录需在**终端管控 > 文件管控 > 策略配置**中开启共享目录审计，开启后，收到此策略的终端将在其终端详情页内枚举显示本机共享文件夹。

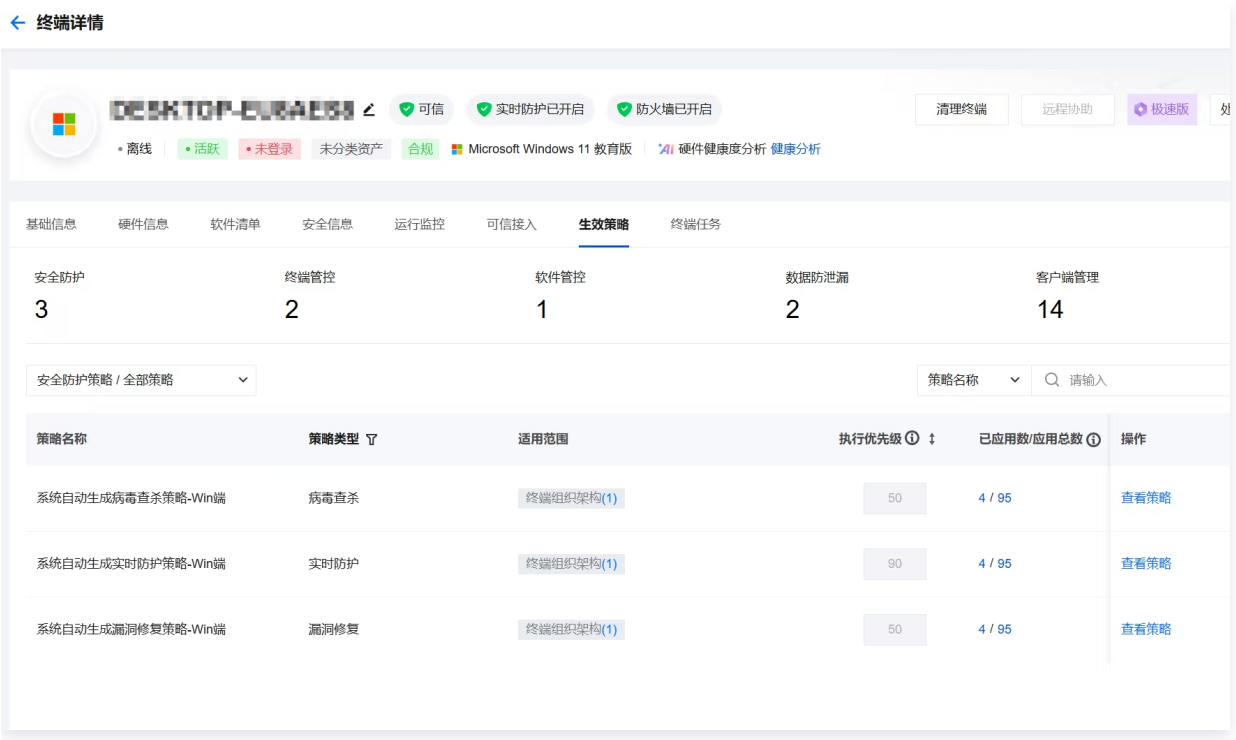
可信接入

展示账号信息、接入信息（出口 IP 地址、本地 IP 地址）等信息。



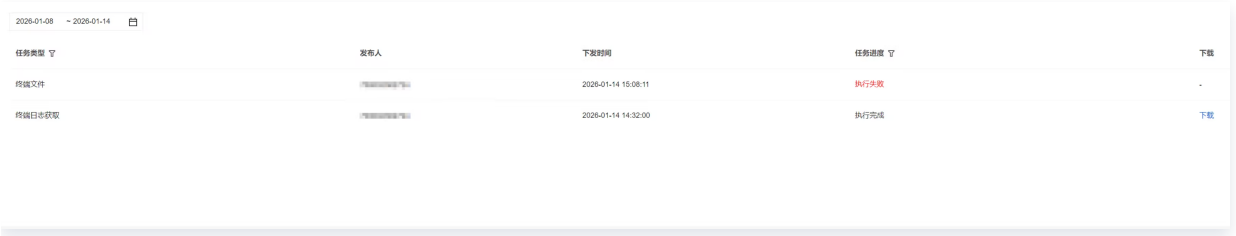
生效策略

查看该终端关联的安全防护策略、终端管控策略、软件管控策略、数据防泄漏、客户端管理策略等，常用于故障排查，例如查看哪些策略影响了该终端，以便快速发现并解决问题。



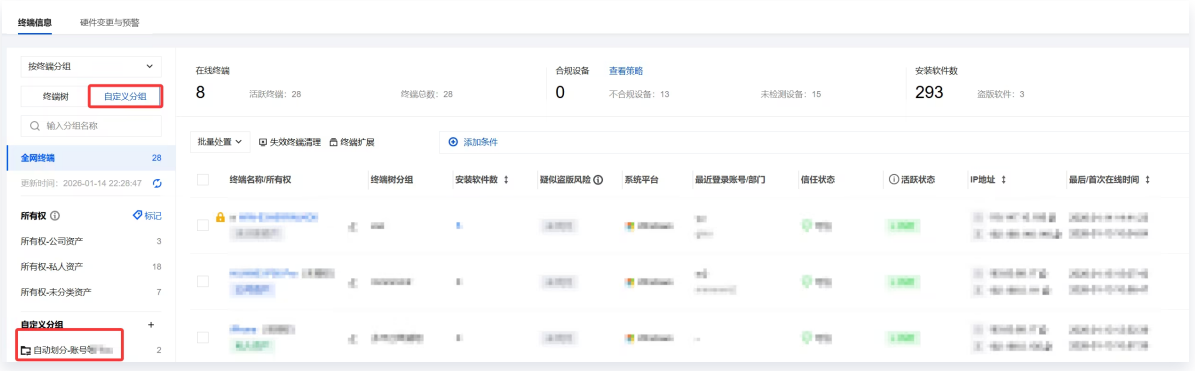
终端任务

查看终端任务执行情况。支持下载任务文件。



自定义分组

1. 系统根据所有权、登录状态、实时防护和内外网等条件自动分组，单击**分组**即可快速查看该分组下的相关终端。

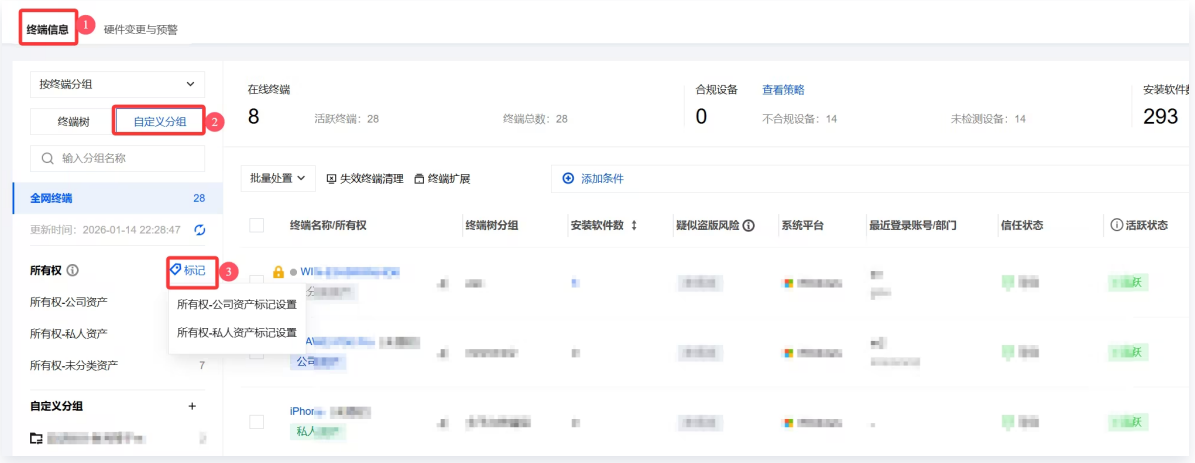


2. 支持标记所有权与自定义分组，配置方式如下：

标记所有权

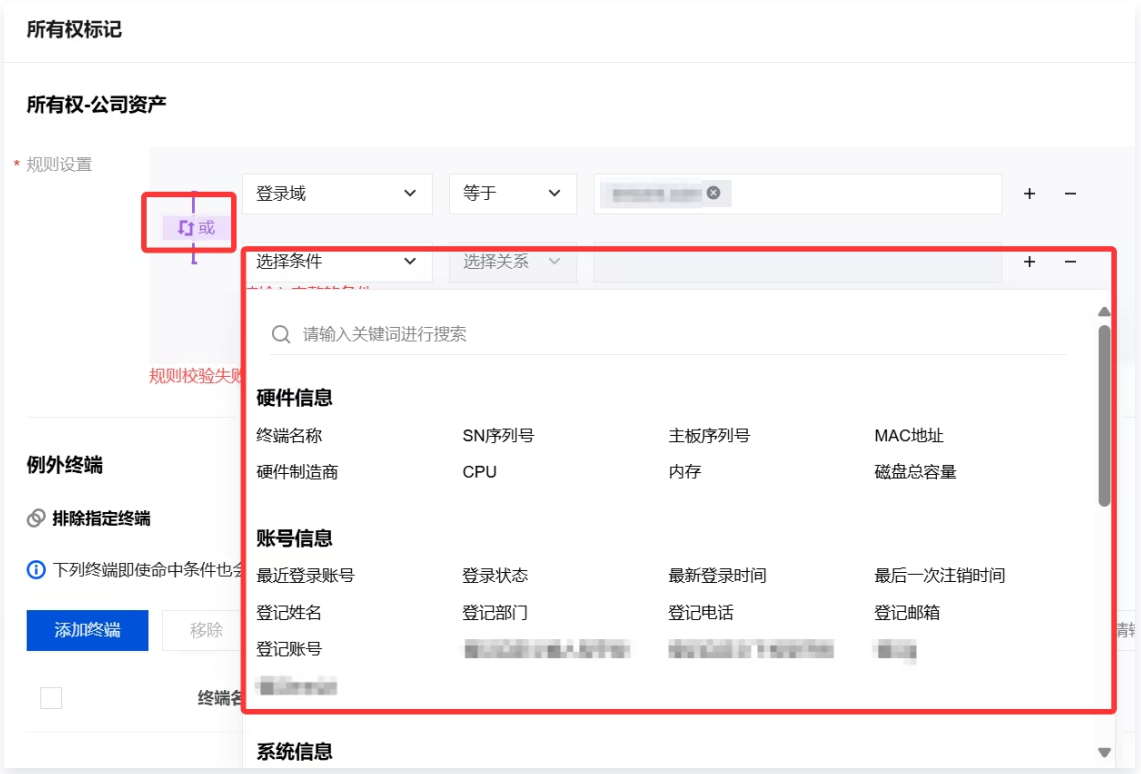
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **终端运维** > **终端信息**。

2. 在终端信息页面，选择**自定义分组**，单击**标记**。

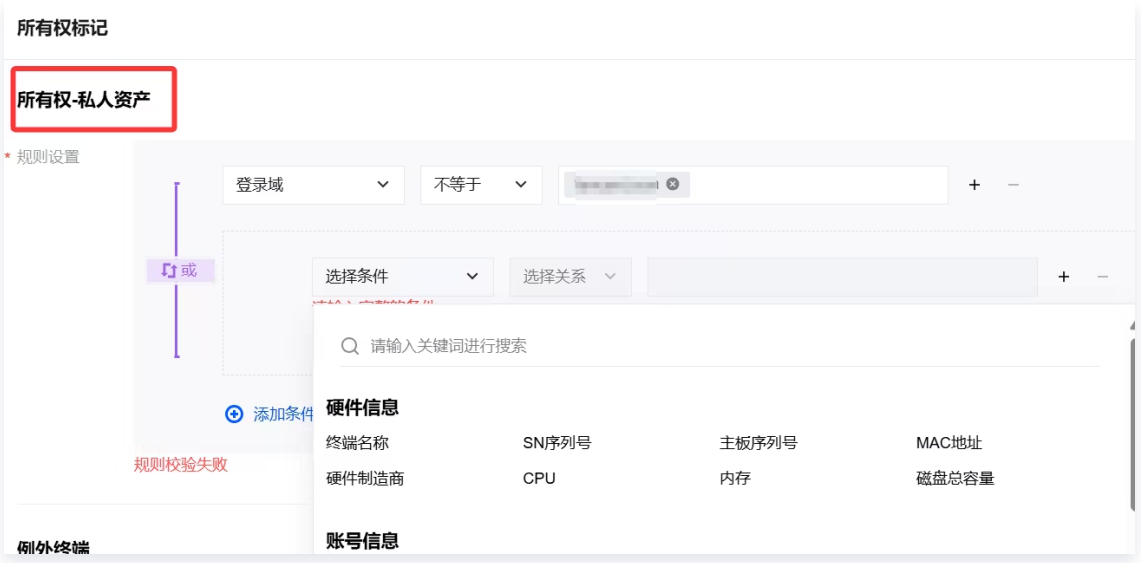


3. 在内容分组页签中，按分组规则统计终端数据，单击**标记并选择**：

- 公司资产标记设置：配置公司资产的规则，当终端与规则匹配时，将标记为公司资产，支持配置多条件组合，支持配置且/或条件。



- 私人资产标记设置：配置私人资产的规则，当终端与规则匹配时，将标记为私人资产，支持配置多条件组合，支持配置且/或条件。



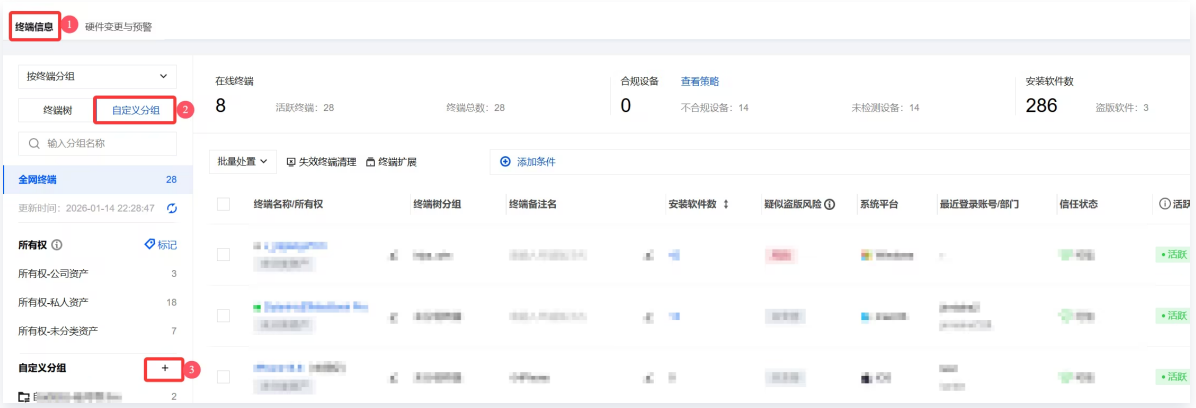
4. 排除指定终端：单击**添加终端**，勾选需排除的终端，单击**确定**。终端即使命中条件也会被排除出该内置分组。



自定义分组

当需要将策略下发给具有共性特征但分散在不同终端分组中的终端时，可以通过创建自定义分组来解决这一问题。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **终端运维** > **终端信息**。
2. 在终端信息页面，选择**自定义分组**，单击 ＋ 添加自定义分组。



3. 编辑分组名称，并选择终端添加方式（手动添加、终端定时自动划分）。

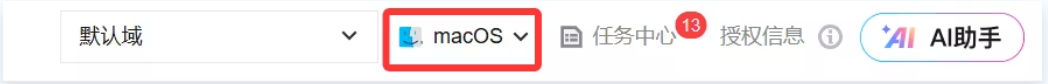
手动添加

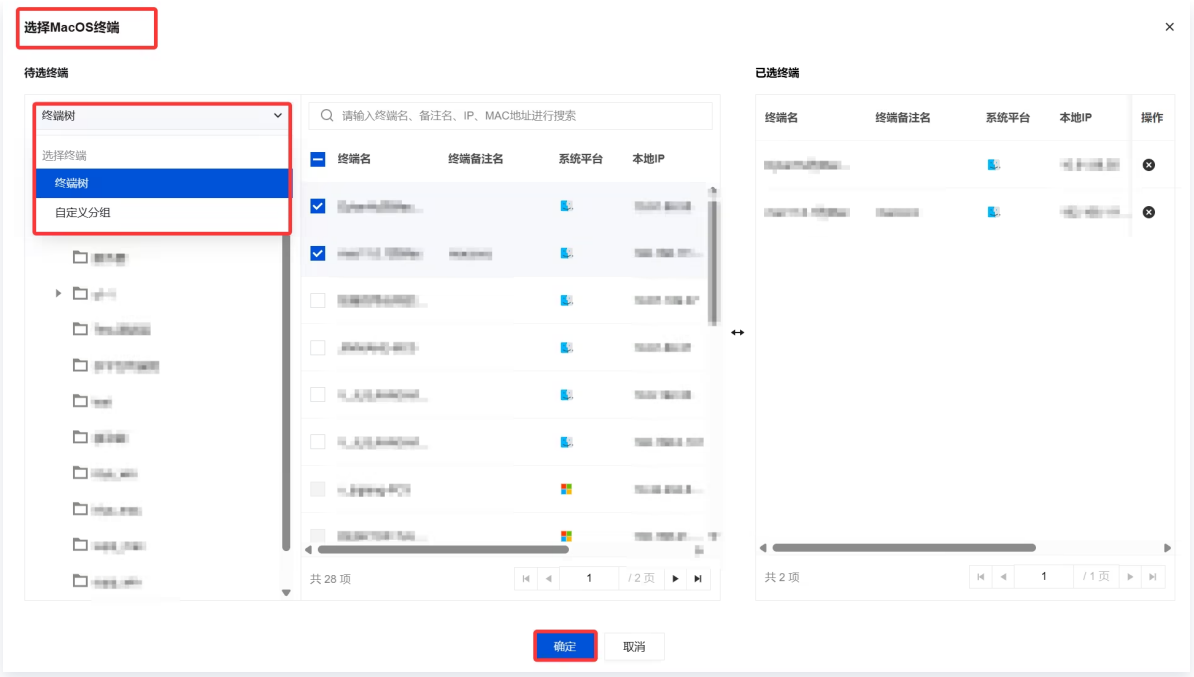
1. 终端添加方式选择**手动添加**，单击**添加终端**。



2. 支持按终端树、自定义分组筛选终端，勾选需加入到自定义分组的终端（支持多选），单击**确定**。

> **说明：**
> - 若您选择的系统平台为 Windows 平台，则终端只能选择 Windows 的终端。
> - 如下图示例，当系统平台为 macOS 时，则终端只能选择 macOS 系统的终端

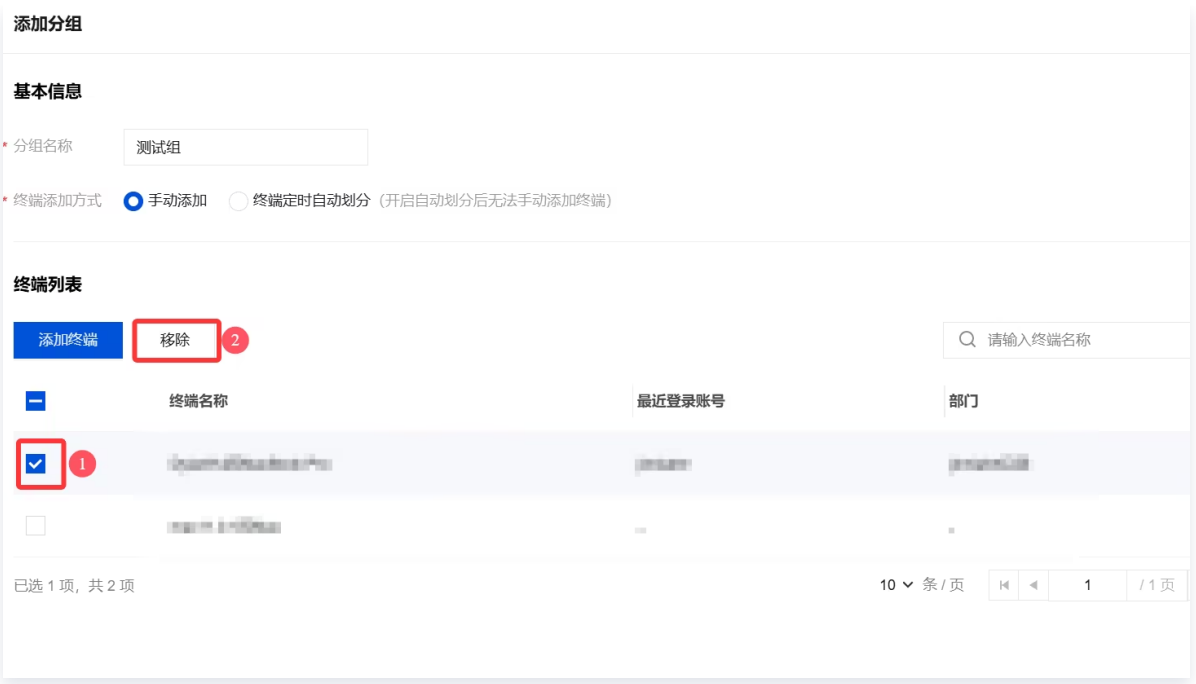




3. 自定义分组中展示勾选的终端，单击**确定**保存，完成手动添加终端到自定义分组。

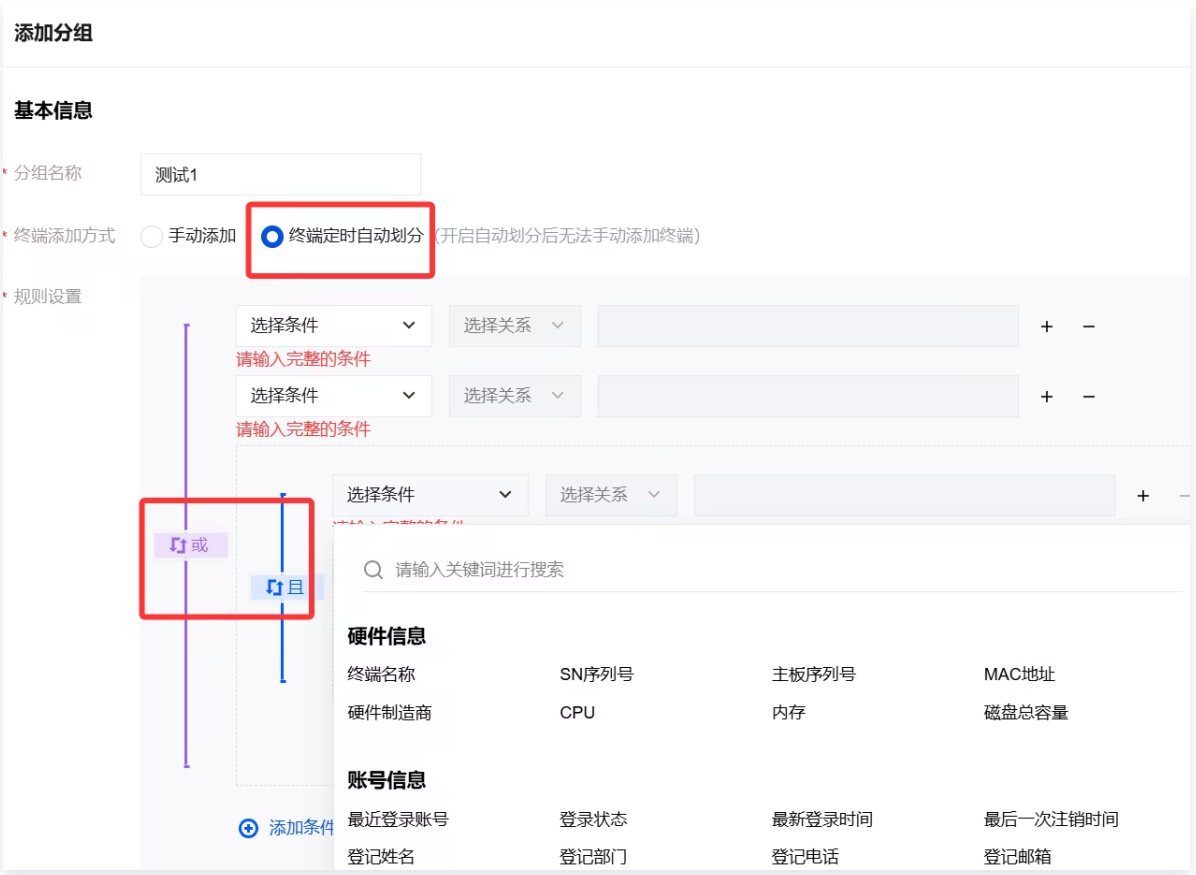


4. 如需移除终端，请勾选需要移除的终端名称，单击**移除**。



终端定时自动划分

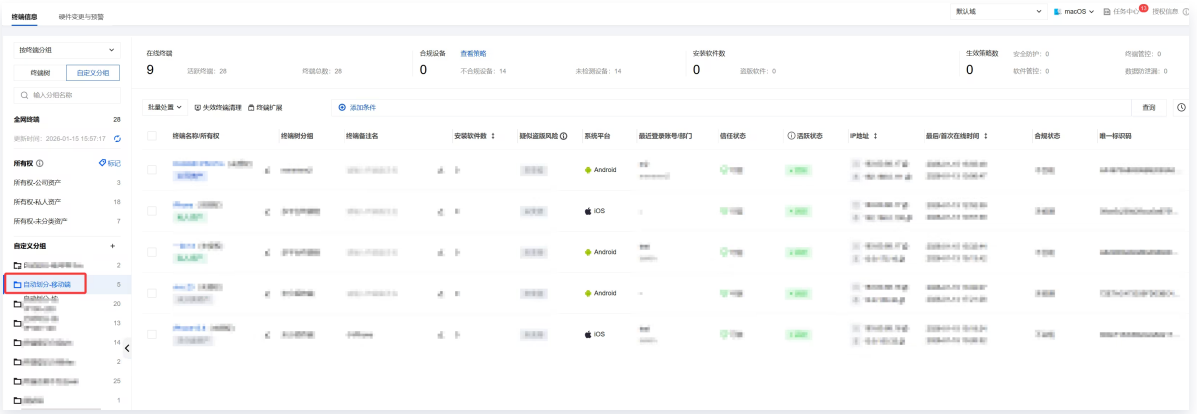
1. 终端添加方式选择**终端定时自动划分**，配置分组规则，配置完成单击**确定**保存。



参数名称	说明
分组名称	自定义。

终端添加方式	此处选择终端定时自动划分。
规则设置	• 支持以终端名称、登录账号、IP 地址、未处理风险数、登录域、终端备注名等规则设置。 • 支持添加多条分组规则并修改规则之间的且或关系来自定义分组，规则灵活组合，高效管理终端设备。
时间设置	支持每小时执行一次、每天执行一次，支持自定义设置执行周期，配置后终端按照分组规则定时划分终端到对应分组中。 **说明：** 自定义周期支持以五分钟为单位进行递增，若输入的数字无法被5整除，则向上转换，如6分钟转换为10分钟，11分钟转换为15分钟，以此类推。
例外终端	支持自定义排除终端与添加指定终端，方便针对不同分组实施差异化的管理策略，提升管理效率。

2. 终端依据分组规则，自动完成分组。

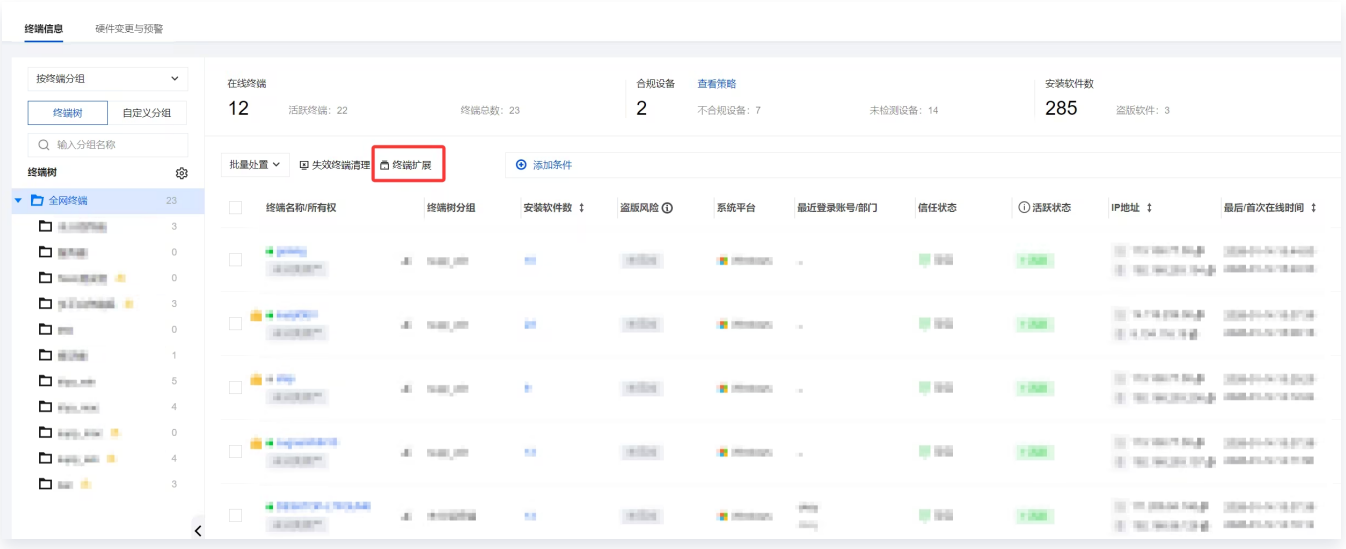


终端扩展（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **终端运维**。
2. 在终端运维页面，选择**终端信息**，单击**终端扩展**。



3. 在终端扩展页，展示终端登记与客户端自助登记信息。

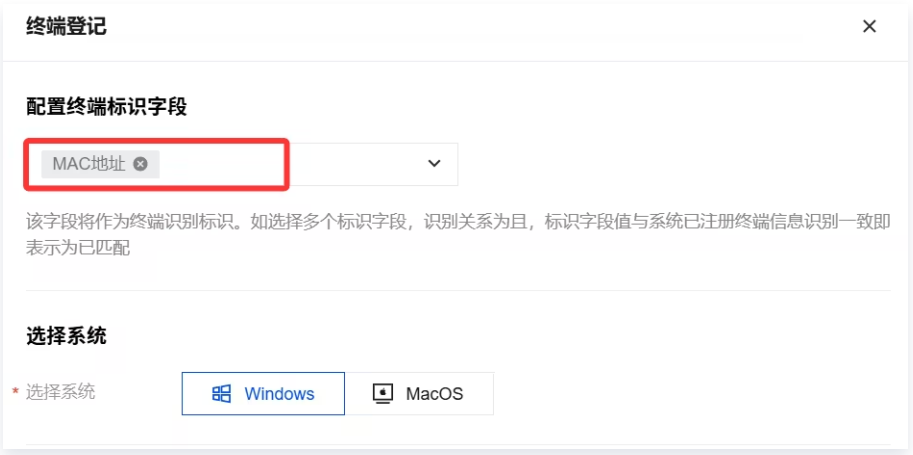
终端登记

> **说明：**
> 终端登记功能要求客户端版本10.11.1及以上支持该功能，如客户端版本低于10.11.1请升级客户端。

终端登记主要用于解决企业设备和个人设备的区分，支持对终端及分组信息进行批量导入上报。



1. 在终端扩展页，单击**终端登记**，配置终端标识字段等参数。

参数名称	说明
配置终端标识字段	• 可选择 MAC 地址 / SN序列号/终端名称。 ○ 示例：若只选择 MAC 地址，当导入的表中填写了 MAC 地址、SN 序列号、终端名称，则使用导入的表中的 MAC地址的数据列匹配；  ○ 若选择 MAC 地址、SN 序列号、终端名称三项，则使用导入的表的 MAC 地址、SN 序列号、终端名称的数据列来匹配。 
选择系统	导入Windows / macOS系统的终端。
上传文件	1. 请先单击**下载导入模板**。  2. 根据模板信息，填写需导入的数据。 3. 如选择多个标识字段，识别关系为且，标识字段值与系统已注册终端信息识别一致即表示为已匹配。 4. 为避免匹配失败，请确保“选择为终端标识的字段 ”值不为空。

	说明： 当配置终端标识字段勾选后，则要确保勾选的字段在导入文件中有数据。 示例：勾选了 MAC 地址和 SN 序列号，则导入的文件中 MAC 地址和 SN 序列号中不能为空，否则会匹配失败。  5. **点击上传**.xlsx格式文件。
终端预分组–所有权	导入的这些终端的分组属于公司资产/个人资产/未分类资产中的哪一类。
自定义分组	可选择已有的分组或新建自定义分组，配置后终端将归入**资产运维** > **终端运维** > **终端信息** > **自定义分组** 中。 

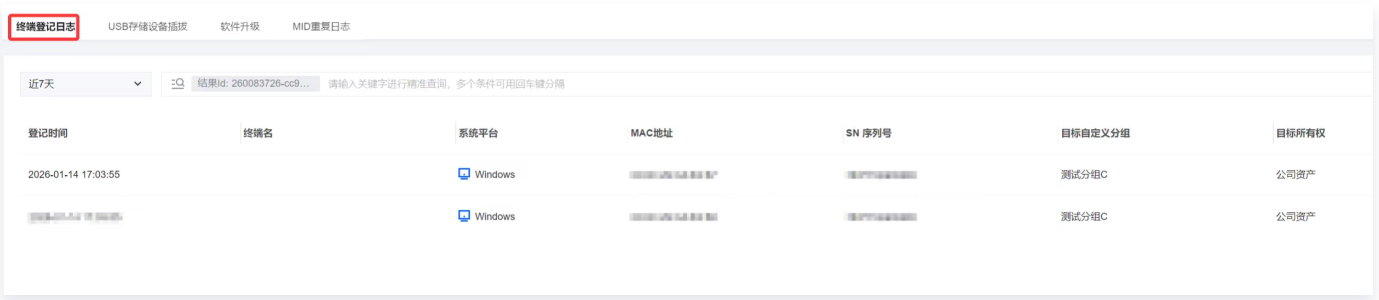
2. 配置完成单击**保存**，终端登记页展示导入后的信息。



3. 单击**更新分组**，将重新匹配已注册终端和上传终端，并会对匹配成功终端的自定义分组及所有权进行更新。



4. 单击**查看日志**，跳转至**其他日志与报表** > **资产运维日志** > **终端登记日志**，可查看终端登记详细信息。

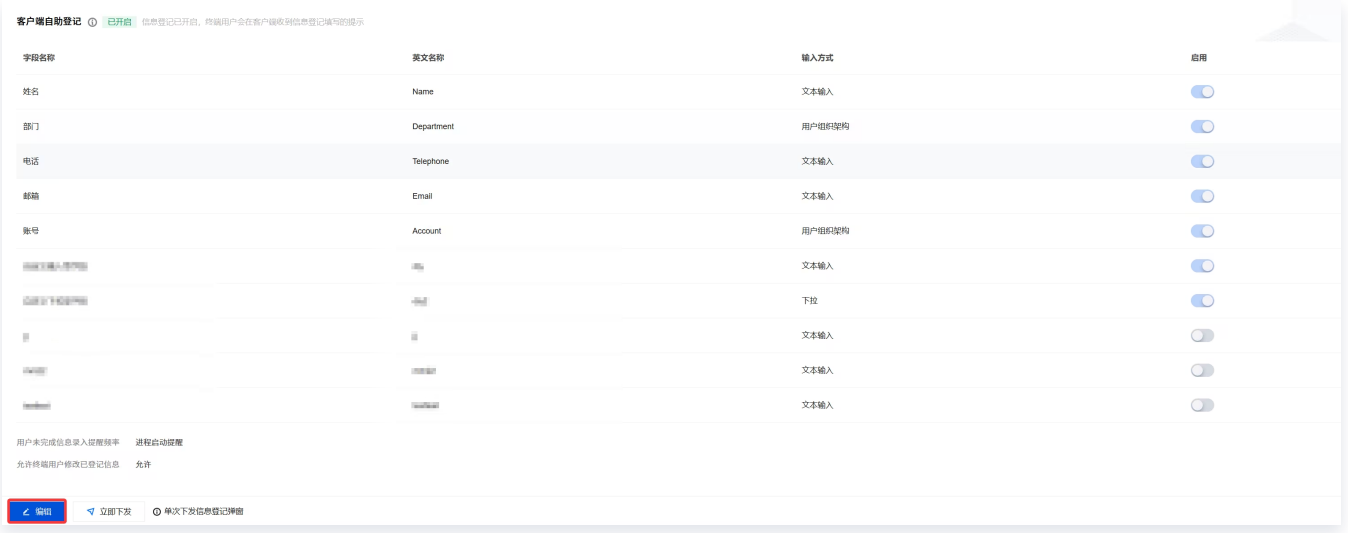


客户端自助登记

配置客户端自助登记规则，用户填写后自动上报终端登记信息至 iOA 控制台，并在**资产运维** > **终端运维** > **终端信息**列表中实时展示。

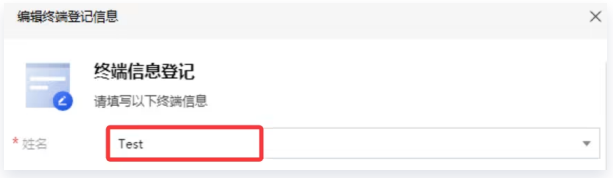
> **说明：**
> 客户端自助登记功能多平台（Windows、macOS）互通，配置后多平台同时生效。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **终端运维**。
2. 在终端运维页面，选择终端信息，单击**终端扩展**。
3. 在终端扩展页面，单击**编辑**客户端自助登记信息。

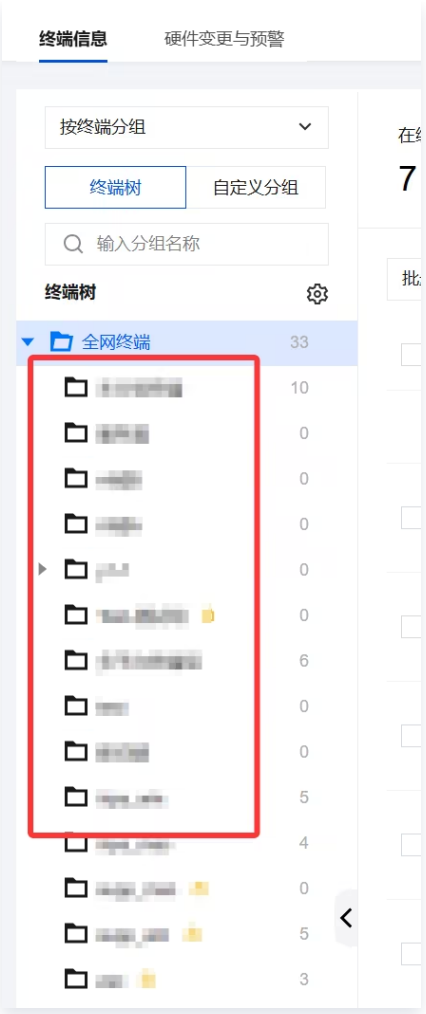


4. 选择系统内置字段，单击**编辑**。



参数名称		说明
姓名	名称	自动获取，客户端姓名样式示例：
	英文名称	自动获取。
	是否必填项	默认为是。
	是否启用	• 是：启用该字段。 • 否：不启用该字段，示例：不启用该字段（不收集用户该字段信息）。 
	输入类型	输入类型在该信息类别新建后无法修改，请谨慎选择。 • 输入框：iOA 客户端弹窗自助登记信息，在姓名栏显示文本输入框。客户端示例：  • 下拉框：姓名不支持下拉框。

部门	名称	自动获取。
	英文名称	自动获取。
	是否必填项	默认为是。
	是否启用	• 是：启用该字段，示例：启用该字段（收集用户该字段信息）。 • 否：不启用该字段。 
	输入类型	输入类型在该信息类别新建后无法修改，请谨慎选择。 • 终端组织架构：支持下拉展示对应的终端树分组，用户手动选择分组后，终端将归入到该分组下。 a. 配置示例：选择终端组织架构后单击**确定**保存。  b. 下发至客户端，客户端弹窗“终端信息登记”。登记信息处 "部门" 可根据终端组织架构筛选分组。  c. 对应控制台终端组织架构示例：



- 用户组织架构：

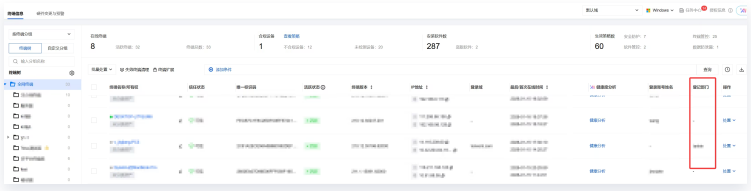
  a. 配置示例：选择用户组织架构后单击**确定**保存。



  b. 下发至客户端，客户端弹窗“终端信息登记”。输入姓名后自动代入用户的组织架构部门信息（部门自动填充）。客户端示例：



c. 用户填写完成上报至 终端信息，示例：



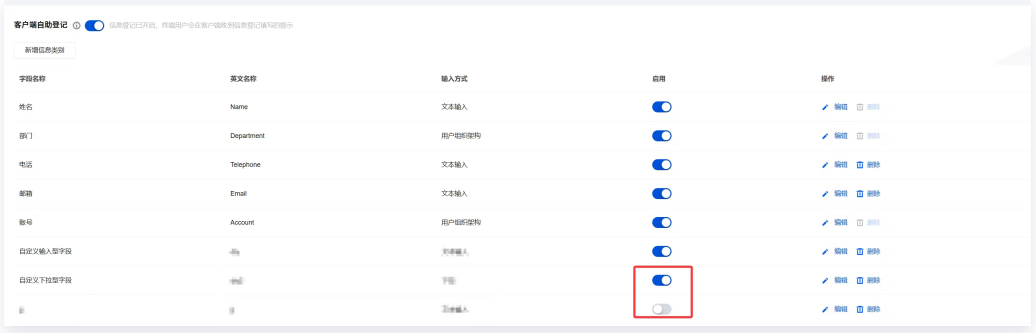
账号	名称	• 当“部门”的输入类型配置为终端组织架构并保存后，终端扩展页将不展示“账号”字段。（仅当“部门”的输入类型配置为用户组织架构并保存后，“账号”字段才会展示。）  • 名称自动获取，客户端账号样式示例： 
	英文名称	自动获取。
	是否必填项	自定义。

	是否启用	• 是：启用该字段。 • 否：不启用该字段，示例：不启用该字段（不收集用户该字段信息）。
	输入类型	默认为用户组织架构。

说明：
iOA 基础版用户支持勾选**终端组织架构**，暂不支持选择用户组织架构，升级后可选择该类型，支持自动代入部门。

5. 支持向终端用户**下发自定义字段**，终端用户可通过 iOA 客户端自主上报并完善该信息，单击**新增信息类别**，填写下发的名称等信息。



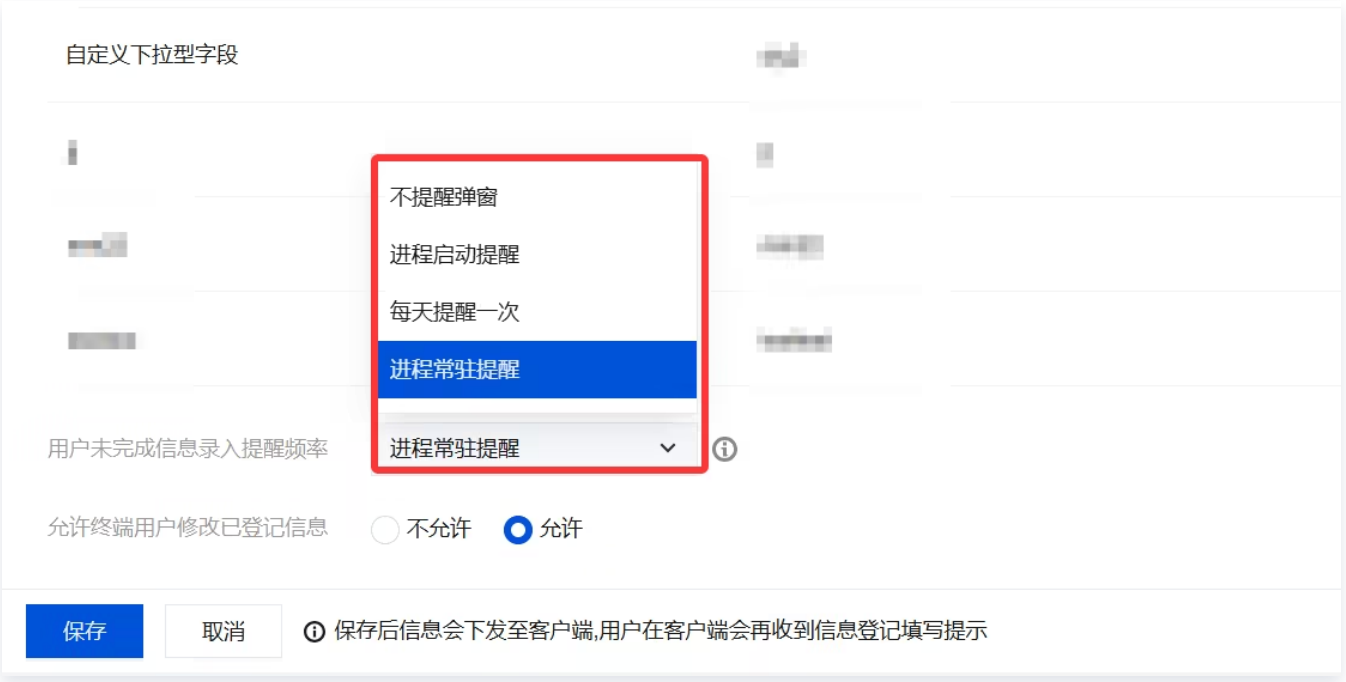
参数名称	说明
名称	填写需要下发至客户端登记的信息名称字段。示例：电脑类型。
英文名称	填写对应的英文名称。示例：Computer type。
是否必填项	是/否。
是否启用	• 是：启用该字段。 • 否：不启用该字段。 
输入类型	输入类型在该信息类别新建后无法修改，请谨慎选择。 • 输入框：客户端自助登记信息显示文本输入框。 • 下拉框：客户端自助登记信息下拉选择字段；示例：办公电脑、服务器。



- 配置完成单击**确定**保存。
- 客户端样式示例：

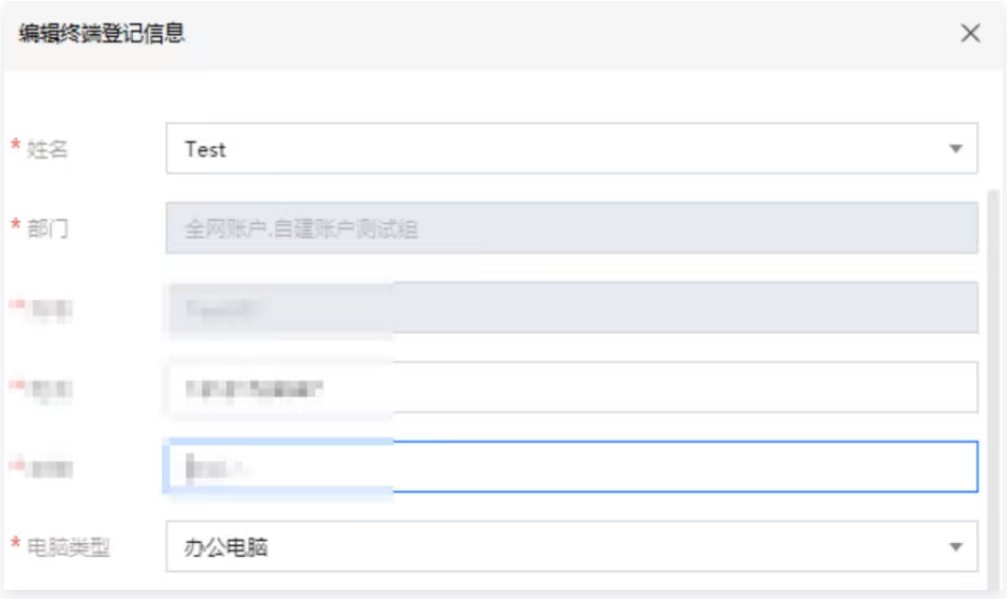


6. 用户未完成信息录入提醒频率：自定义设置提醒频率。



参数名称	说明
不提醒弹窗	不进行弹窗提醒。
进程启动提醒	Windows 系统启动即会提醒，macOS 系统进程初次启动或重启后均会提醒。
每天提醒一次	每天下午16:00弹窗提醒一次。
进程常驻提醒	客户端弹窗隐藏“取消”按钮，用户必须填写保存后方可关闭弹窗。

7. 允许终端用户修改已登记信息。
   - 允许：登记信息一经上报，若管理员重新下发该信息，客户端将自动弹出“终端自助登记”窗口，用户可再次修改已登记内容。



- 不允许：登记信息上报后，用户无法再次修改（置灰）。



> **说明：**
> 设置为不允许用户修改已登记信息，当管理员重新下发客户端自助登记信息，若登记内容发生变更（如新增、删除或调整信息类别及字段），客户端仍会自动弹出 “终端自助登记” 窗口。

8. 配置完成单击**保存**，保存后信息会下发至客户端，客户端弹窗提醒用户完善登记信息，单击**立即填写**。



9. 终端用户信息填写完成，单击**保存**。



10. 管理员前往**终端管理** > **终端信息**，查看用户上报的信息。

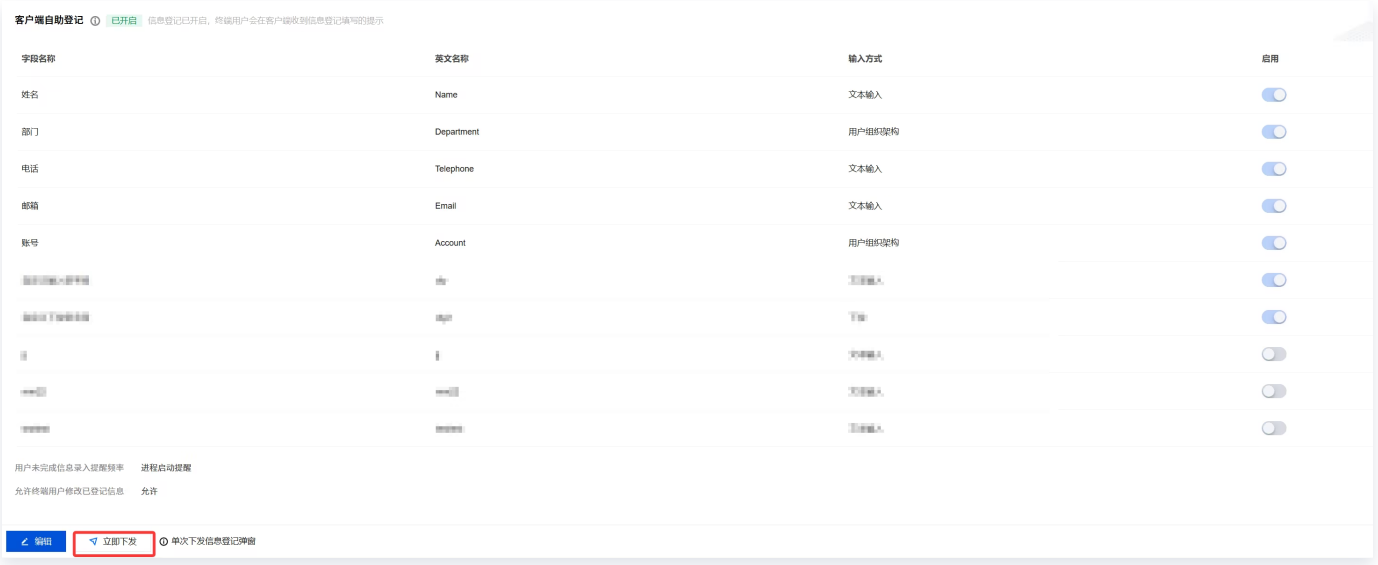
> **说明：**
> 如终端信息列表未展示您设置的自定义字段，请单击**设置自定义列表管理**，选择的字段将展示在终端列表。





11. 客户端自助登记信息支持手动下发，单击**立即下发**后客户端收到对应的登记弹窗。

> **说明：**
>
> - 使用场景：修改客户端登记字段并保存后，系统将自动下发登记弹窗。若管理员未修改字段内容，但仍希望用户重新填写，可单击**立即下发**推送登记弹窗。
> - 立即下发功能要求客户端版本10.11.1及以上支持该功能，如客户端版本低于10.11.1请升级客户端。



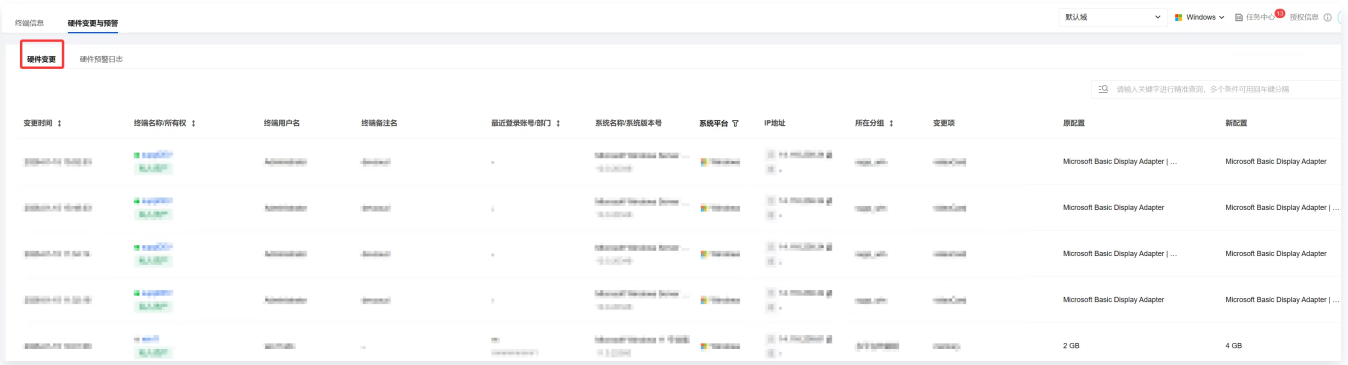
硬件变更与预警（11.1.1版）

最近更新时间：2026-02-13 09:41:02

对终端硬件的物理变更、性能波动及健康状态进行实时监测、记录与主动预警，构建从变更审计到健康守护的硬件安全管理能力。

硬件变更

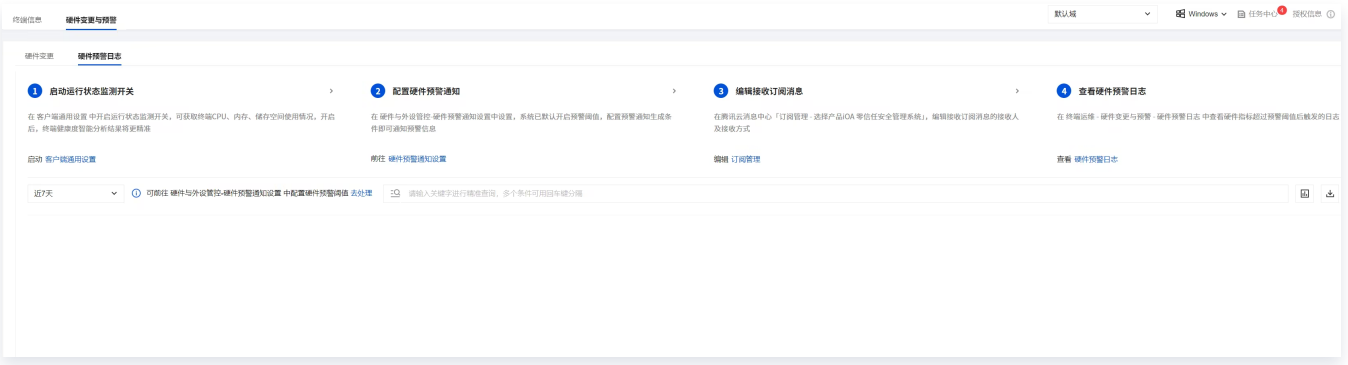
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **终端运维**。
2. 在终端运维页面，选择**硬件变更与预警**，单击**硬件变更**。



3. 硬件变更页面是硬件资产的“审计日志”。它记录并展示了终端设备上发生的所有物理硬件变更记录，例如硬盘、内存、网卡等组件的更换。
4. 管理员可以此追溯硬件资产的物理变更历史，明确“谁、何时、对哪台设备、变更了什么”，是资产盘点、合规审计、安全事件调查的参考记录。

硬件预警日志

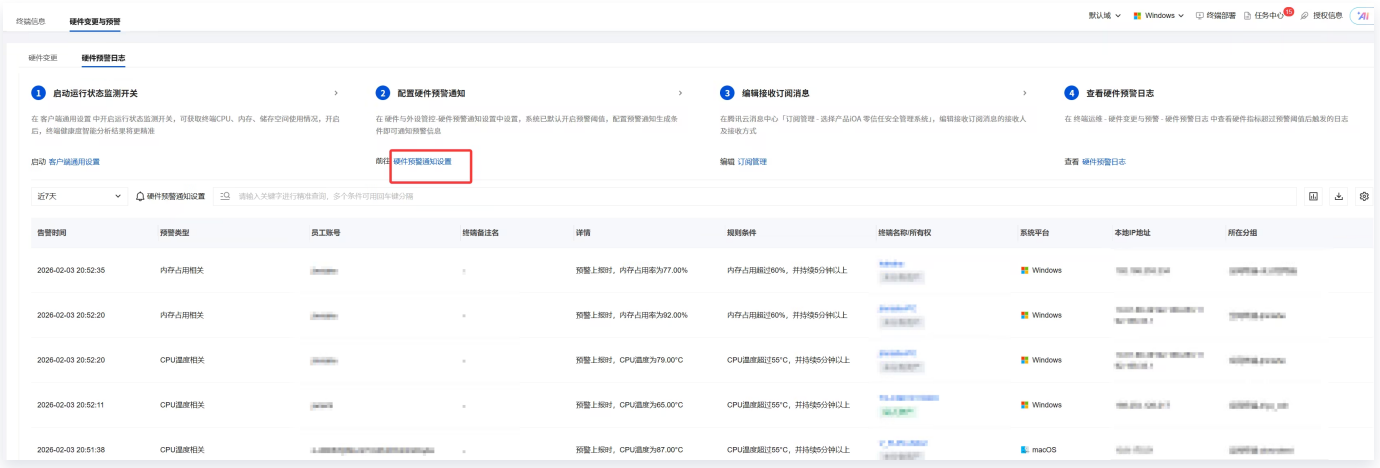
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **终端运维**。
2. 在终端运维页面，选择**硬件变更与预警**，单击**硬件预警日志**。
3. 当指标超过预设阈值（例如 CPU 使用率 > 90%）时，会在此生成预警日志。管理员可构建硬件预警检测体系，在设备出现性能瓶颈、磁盘爆满等问题前收到预警，从而提前干预，避免业务中断。



4. 在**客户端管理** > **客户端策略** > **客户端通用设置**中启动终端运行状态监测开关。



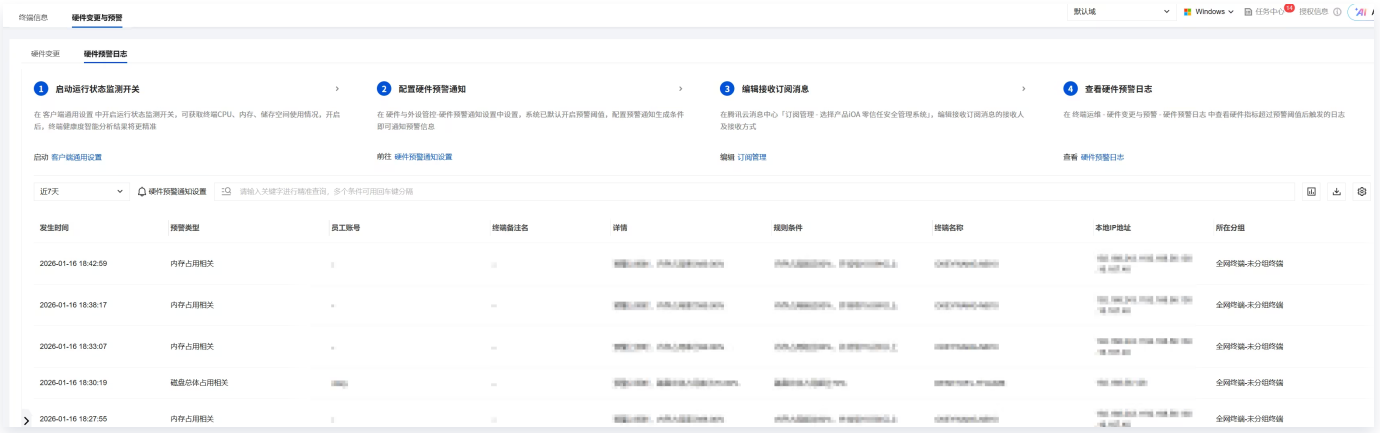
5. 在**资产运维 > 终端运维 > 硬件变更与预警 > 硬件预警日志**中单击**硬件预警通知设置**



6. 前往**腾讯云消息中心 > 订阅管理** 中选择产品**iOA 零信任安全管理系统**，编辑接收订阅消息的接收人及接收方式。



7. 当硬件指标超过预警阈值后触发告警，可在硬件预警日志中查看详情。

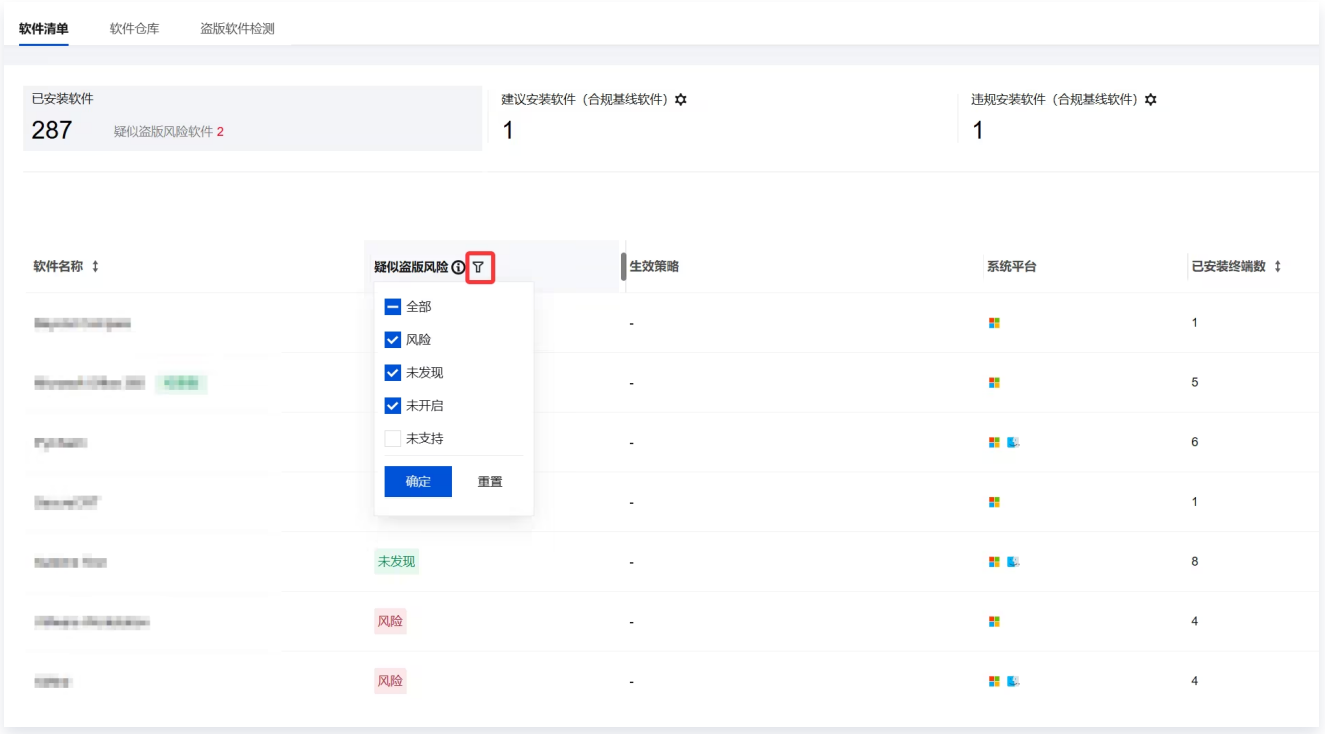


软件运维（11.1.1版）
软件清单（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **软件运维** > **软件清单**。
2. 软件清单支持查看公司内全量软件的安装情况，支持按照如下类型筛选软件：
   - 风险：检测出可能存在盗版安装。
   - 未发现：未检测出存在盗版安装。
   - 未开启：软件未开启盗版检测，可前往**资产运维** > **软件运维** > **盗版软件检测**开启检测功能。
   - 未支持：暂未支持盗版检测。



3. 在软件清单页面，单击**详情**，展示软件详情信息，可对指定终端的指定软件执行卸载。



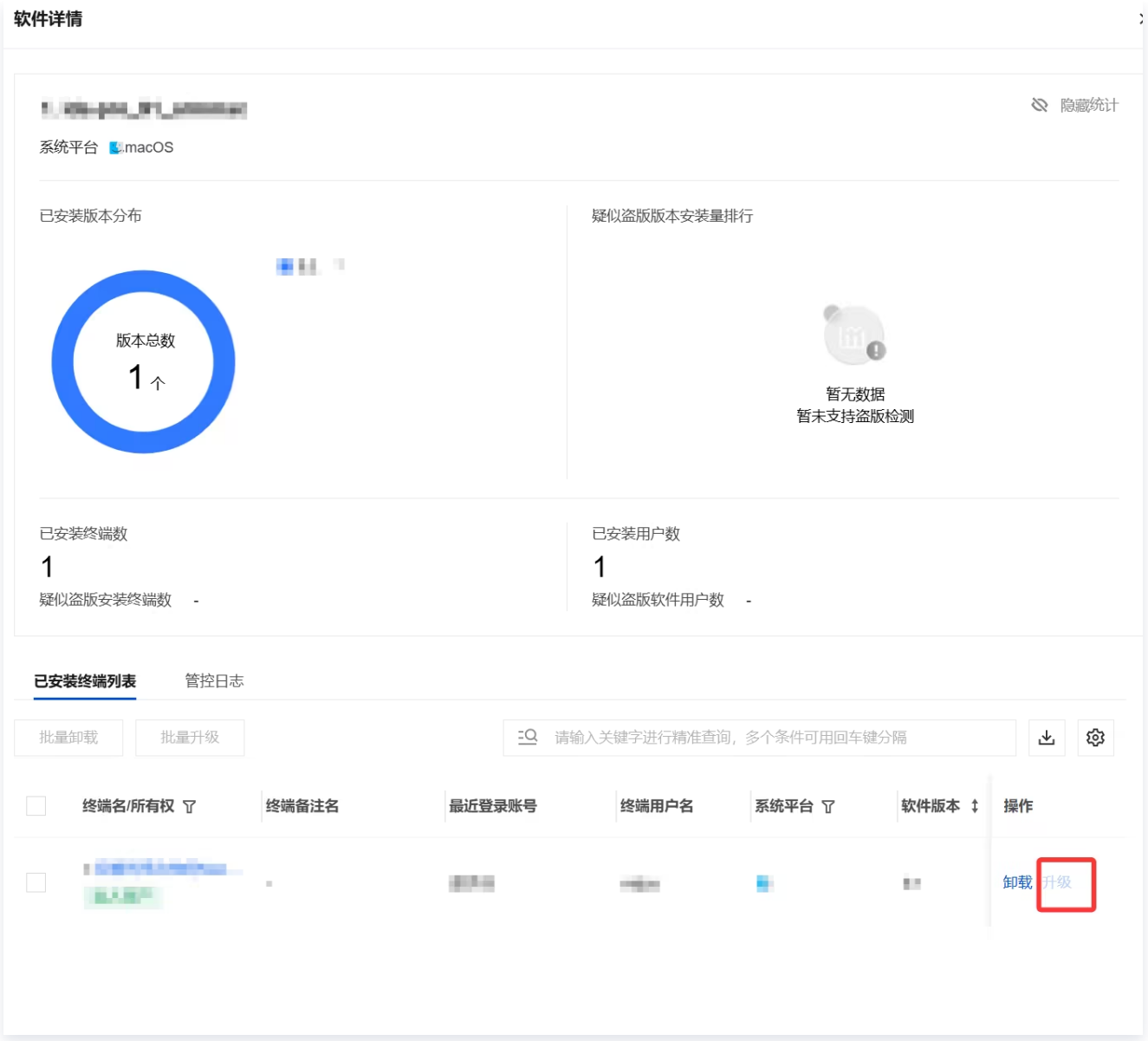
4. 在软件详情页面，单击**卸载**：
   - 提醒卸载：选择提醒卸载后，用户终端会收到软件卸载提醒。



   - 输入静默卸载命令：静默命令填写/s /S -s，需根据软件支持的静默命令进行填写，在注册表（HKEY_LOCAL_MACHINE|SOFTWARE\WOW6432Node|Microsoft\Windows\CurrentVersion|Uninstall）查询软件信息 QuietUninstallString，若有参数则支持静默卸载。

> **说明：**
> 软件静默卸载功能需要卸载的软件本身支持静默卸载。

5. 在软件详情页面，部分软件支持版本升级功能，支持对单个或批量终端下发升级任务，并实时更新版本信息。
   - 如该软件支持通过软件运维升级，则升级按钮显示为蓝色。
   - 如该软件不支持通过软件运维升级，则升级按钮不可点击。



6. 管控日志：命中**软件管控 > 运行管控 > 策略设置**的终端，可在此查看该终端管控日志。


已安装终端列表
管控日志
近30天
请输入关键字进行精准查询，多个条件可用回车键分隔
时间
软件名称
终端名/所有权
最近登录账号/部门
系统平台
命中策略
管控类
软件安
软件安
软件安
软件运

软件仓库（11.1.1版）

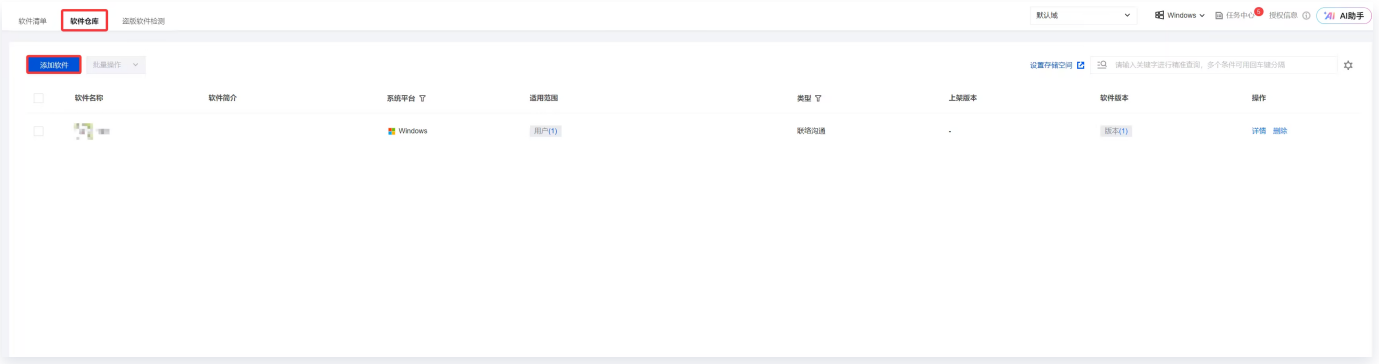
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

在软件仓库上架企业内常用软件，员工即可在客户端软件仓库自行下载，实现软件高效管理与便捷使用。

> **说明：**
> - 在将软件上架至仓库前，建议您先配置存储空间，详情请参见 存储空间 。
> - 软件仓库功能要求客户端版本10.9.1及以上支持该功能，如客户端版本低于10.9.1请升级客户端。

1. 登录 iOA 零信任管理平台控制台 ，在左侧导航栏，选择**资产运维** > **软件运维** > 软件仓库 。
2. 在软件仓库页面，单击**添加软件**。



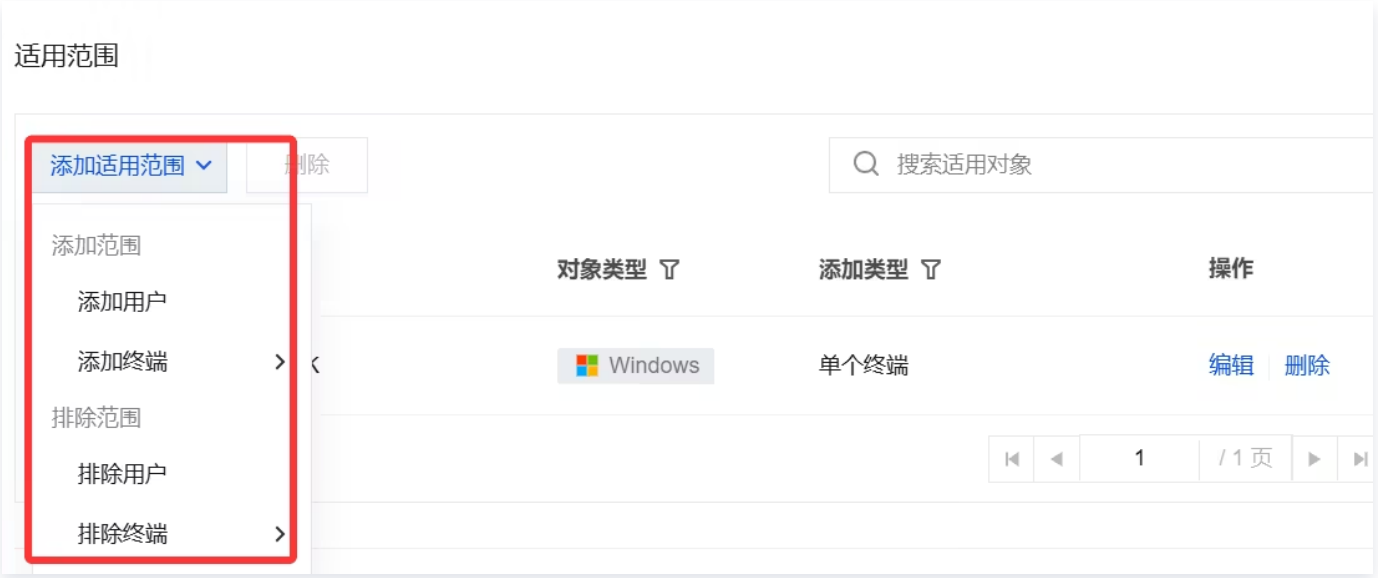
3. 在添加软件页面，添加软件基本信息。



参数名称	说明
软件名称	自定义该软件展示在客户端的名称。
Logo	上传48像素 x 48像素至150像素 x 150像素大小的方形图标，图片宽高比例为1:1，支持png、jpg等格式。
软件类型	下拉选择软件类型（输入法、浏览器、视频播放、游戏休闲、桌面主题、必装软件等）。
软件简介	自定义软件简介。
软件英文信息	如果未配置软件英文版信息，当客户端语言设置为英语时，仍将显示软件中文信息。

版权所有：腾讯云计算（北京）有限责任公司

4. 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。

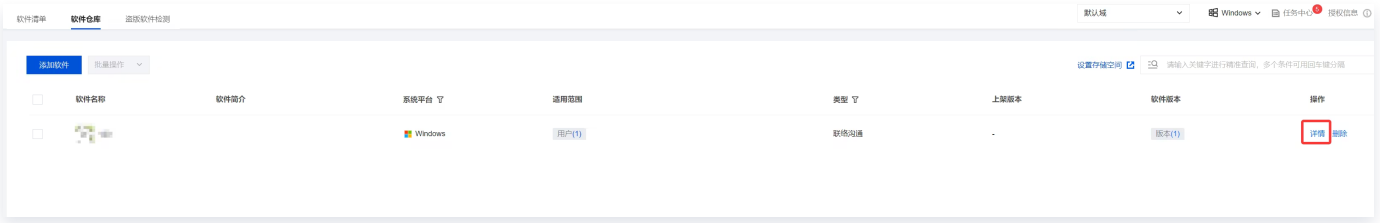


5. 在软件安装包中，选择版本、系统版本、版本号，并单击**确定**保存。

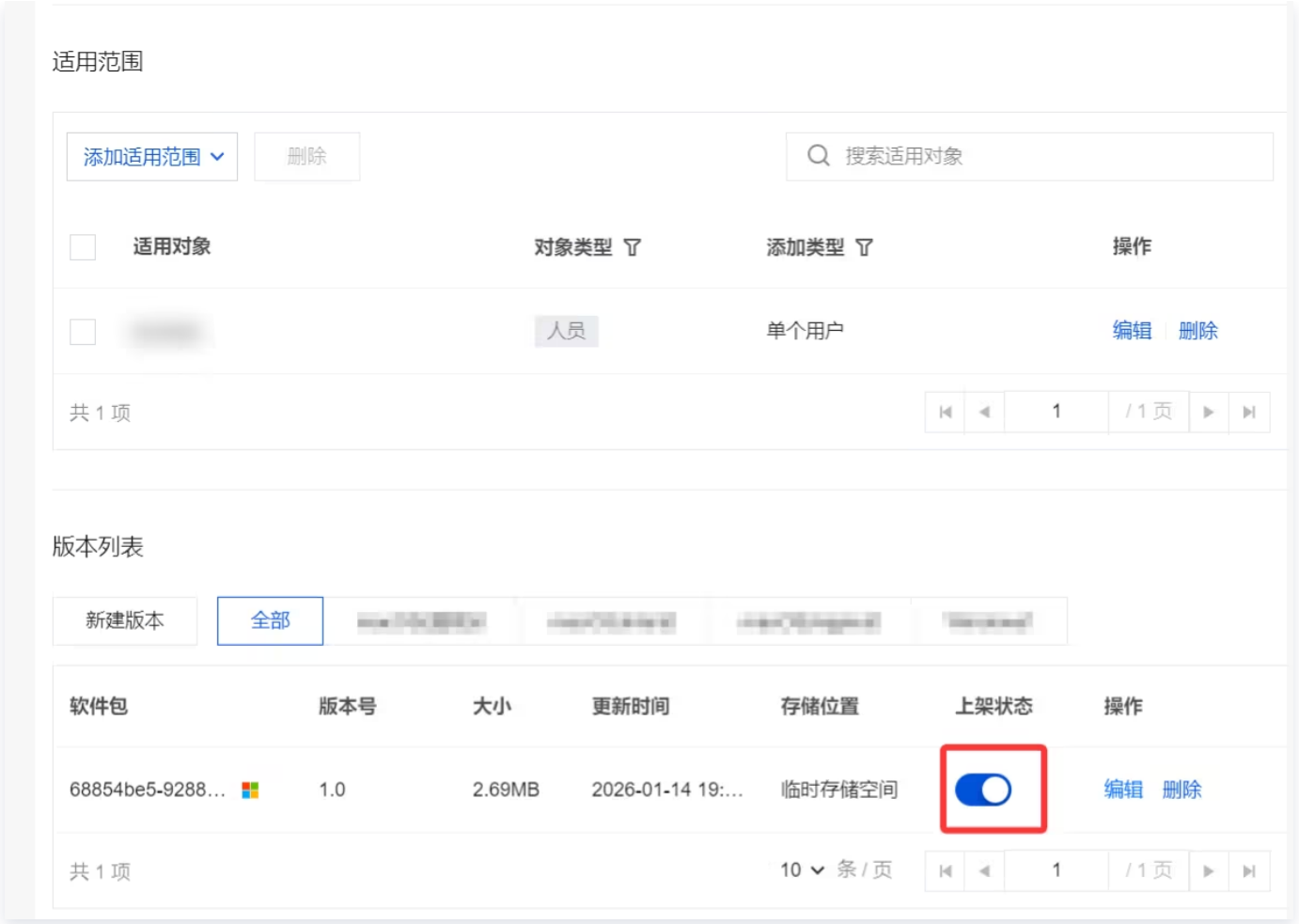
参数名称	说明
添加版本	• 文件上传：直接上传本地软件包（支持 exe、msi、zip、rar 等格式，大小不超过 2GB）。 • 链接上传：输入下载链接提交软件包。
系统版本	请选择目标操作系统：Windows 或 macOS，并确保上传的安装包与所选系统兼容。
版本号	填写软件版本号（如 1.0.0），便于区分和管理不同版本的安装包。



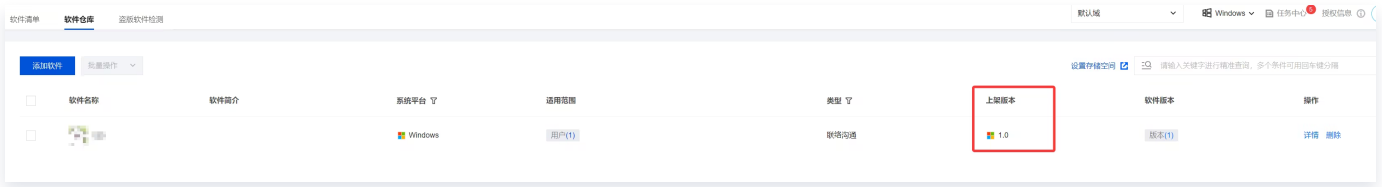
6. **软件默认不自动上架，需手动开启“上架状态”。若存在多版本，此操作尤为重要，**在软件仓库页单击**详情**。



7. **在版本列表中，选择目标软件包，开启上架状态。**



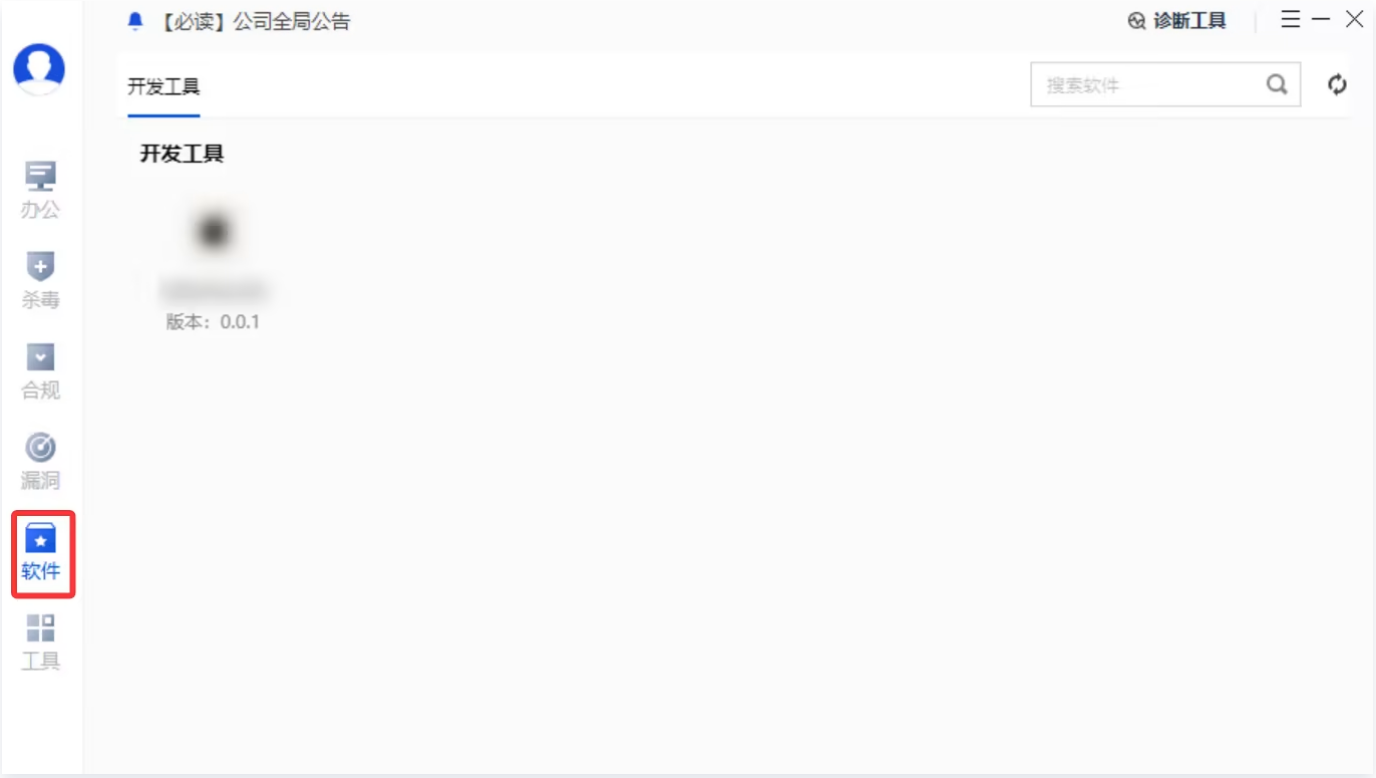
8. 开启上架状态后，软件仓库页展示软件版本信息，不开启上架状态，则不展示软件版本信息。



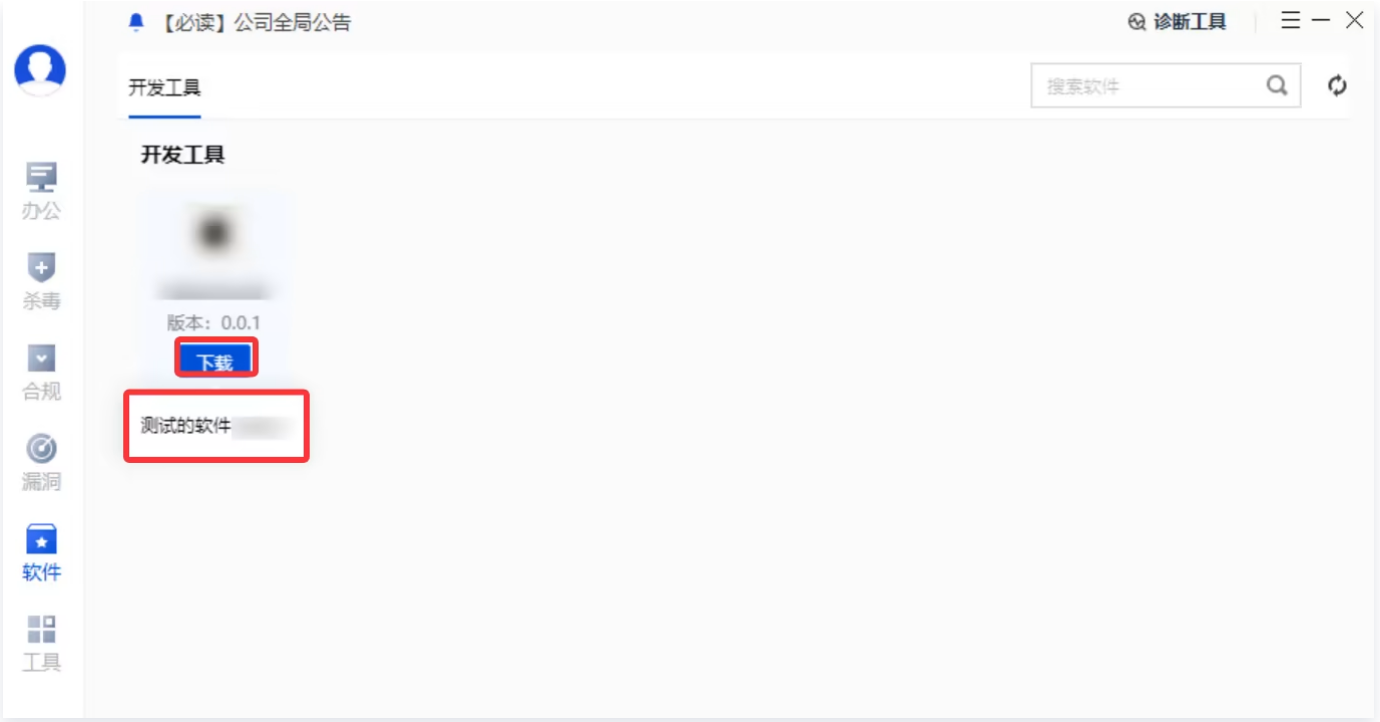
9. 软件仓库配置完成，请前往**客户端管理 > 客户端策略 > 模块定制**，**配置模块定制策略**，勾选软件仓库。勾选后软件仓库将在客户端功能模块中展示，不勾选软件仓库，则客户端无法查看该模块。



10. 员工登录 iOA 客户端，展示软件模块，单击**软件**，查看管理员上架的软件信息。



11. 单击**软件名称**查看软件简介，单击**下载**，将软件下载至终端。



12. 下载完成后可打开文件并安装，便捷使用该软件。



盗版软件检测（11.1.1版）

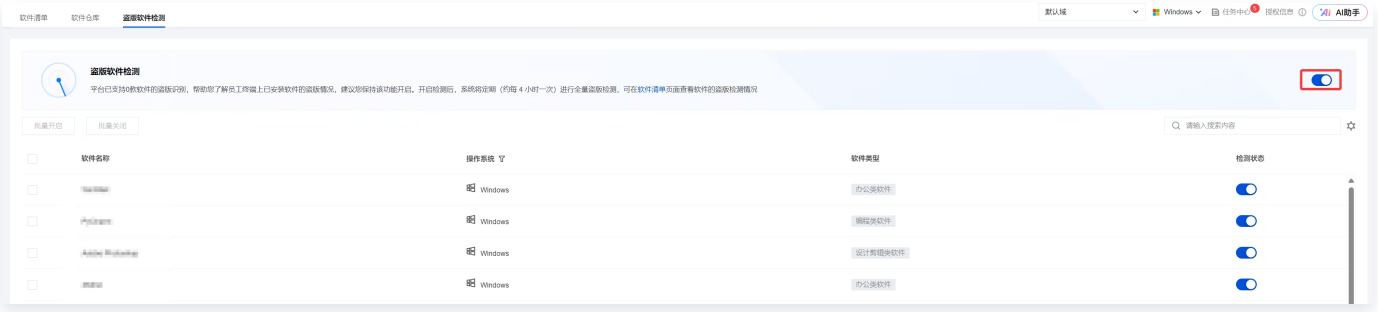
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

iOA 内置盗版软件识别能力，可通过下发盗版检测策略，对终端设备上的软件使用情况进行检测和分析。

> **说明：**
> 盗版软件检测功能仅是 iOA 基于部分盗版软件的通用安全特征进行分析，相关检测和分析结果仅供参考，并非完全精准和全面，且仅支持部分软件的盗版检测。

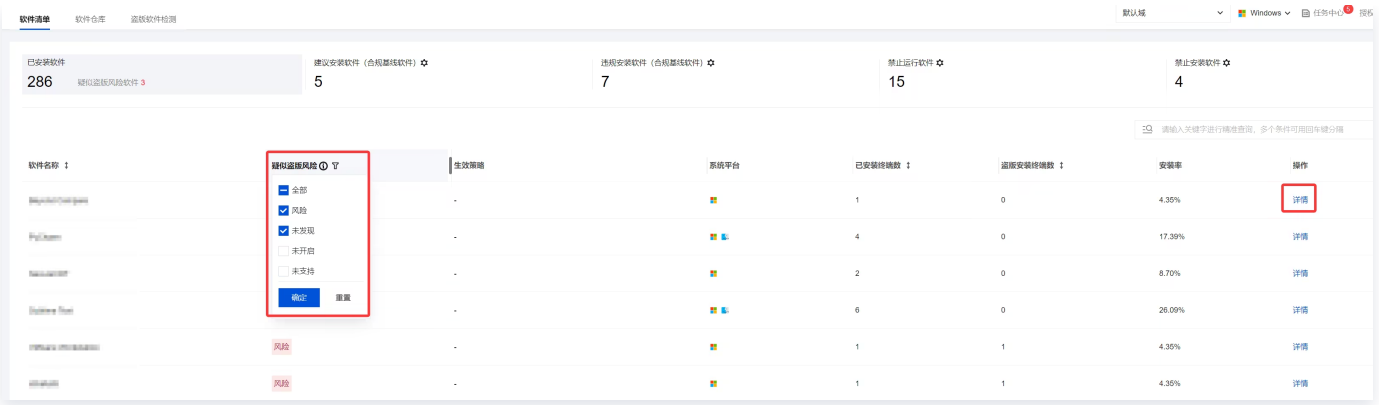
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **软件运维**。
2. 在软件运维页面，选择 **盗版软件检测**，单击**开启盗版软件检测**。



3. 勾选需开启检测的软件名称（支持批量勾选），勾选后单击**批量开启**。



4. 开启检测后，系统将定期（约每 4 小时一次）进行盗版检测，可在 软件清单页面 查看软件的盗版检测情况，单击**疑似盗版风险**，可快速筛选软件盗版情况。



5. 单击详情，查看疑似盗版软件的盗版原因，安装时间，并支持批量卸载。

软件详情

[redacted]

隐藏统计

系统平台 Windows macOS

已安装版本分布



疑似盗版版本安装量排行

暂无数据

未开启盗版检测。可前往软件运维-盗版软件检测页面开启检测功能

已安装终端数
3
疑似盗版安装终端数 2

已安装用户数
3
疑似盗版软件用户数 -

已安装终端列表 管控日志

批量卸载 批量升级 请输入关键字进行精准查询，多个条件可用回车键分隔

已选择 3 项 选中全部 取消勾选

终端名/所有权	终端备注名	最近登录账号	终端用户名	系统平台	软件版本	操作
[redacted]						卸载 升级
[redacted]						卸载 升级
[redacted]						卸载 升级

存储空间（11.1.1版）

最近更新时间：2026-02-06 14:23:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

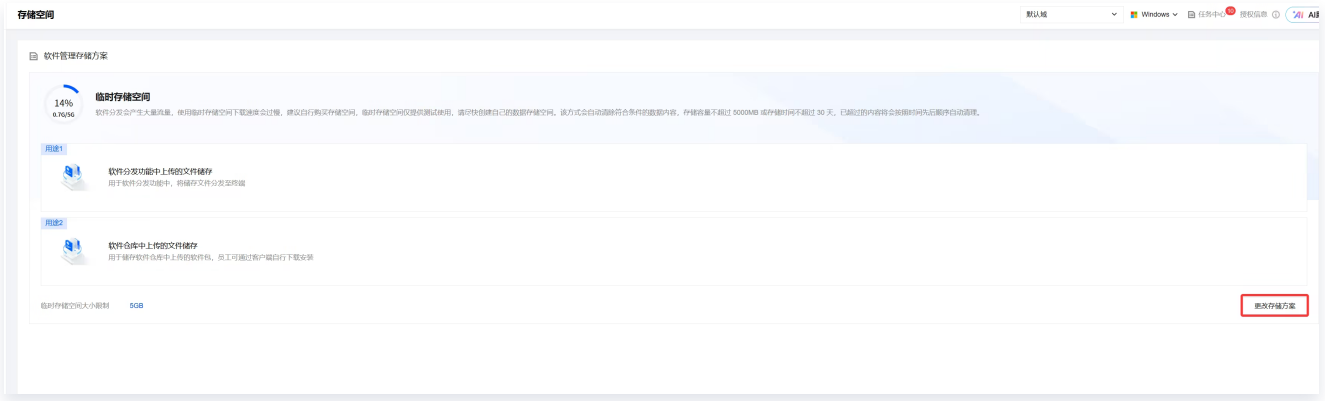
在资产运维模块中，**资产运维** > **软件运维** > **软件仓库**与 **软件管控** > **分发管控**功能均需配置存储空间，二者的存储空间配置方式完全一致，基于这一共性特征，为提升内容的简洁性与可读性，本文将对该存储空间的配置方式进行统一阐述。

- 若配置**软件仓库**存储方案，请登录iOA 零信任管理平台控制台，在左侧导航栏，选择**资产运维** > **软件运维** > **软件仓库**。

  a. 在软件仓库页面，单击**设置存储空间**。

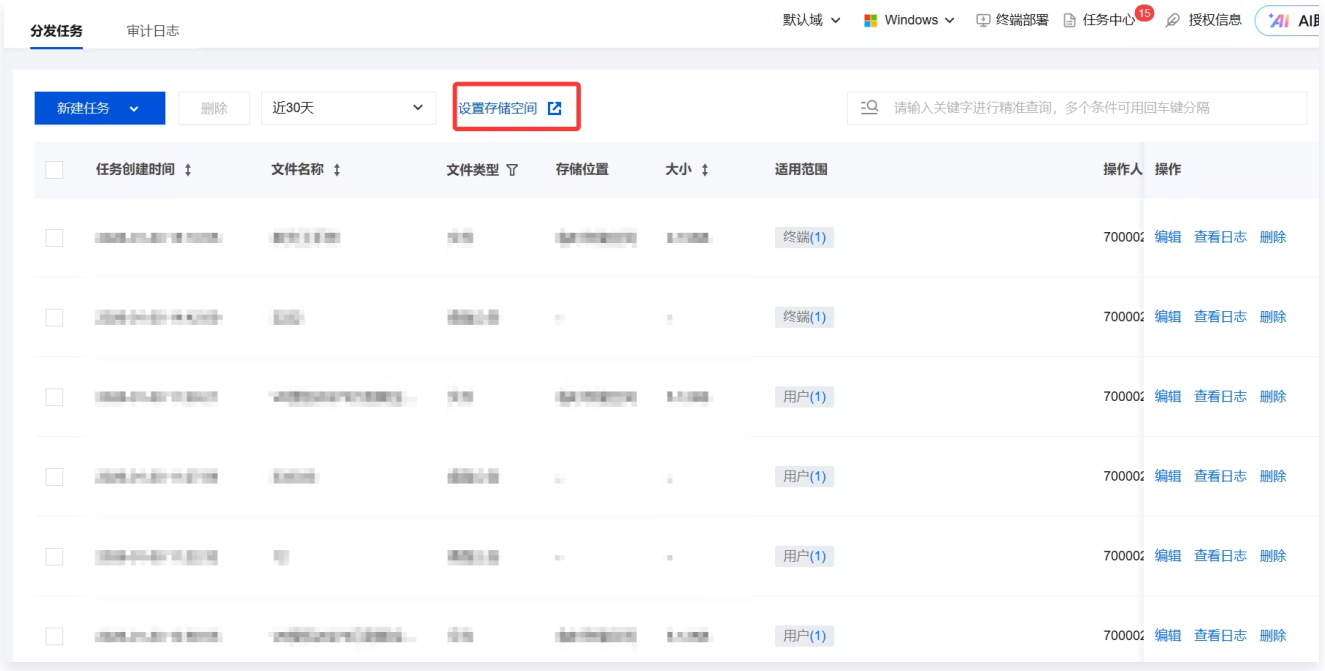


  b. 单击**更改存储方案**，配置腾讯云或S3协议存储。

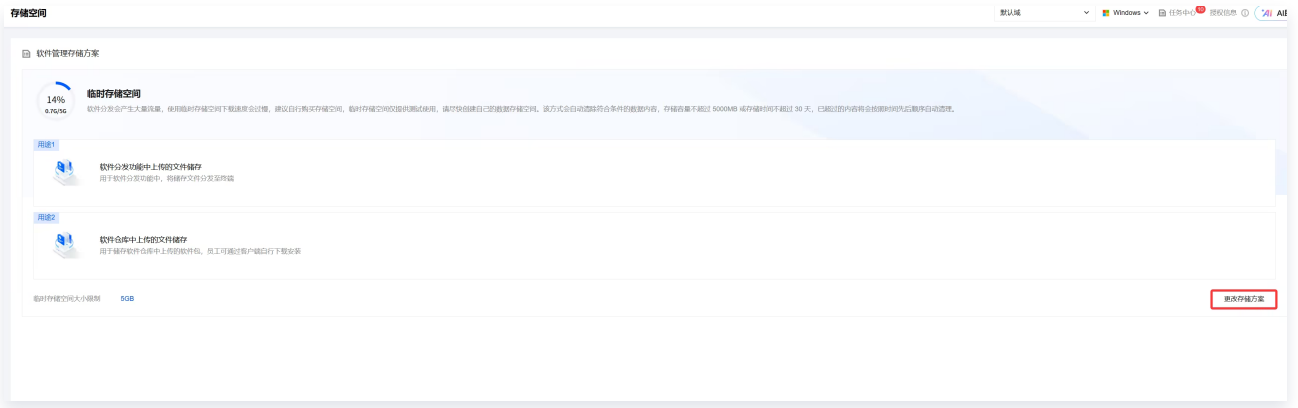


- 若配置**分发管控**存储方案，请登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**软件管控** > **分发管控**。

  a. 在分发管控页面，选择分发任务，单击**设置存储空间**。



b. 在存储空间页面，单击**更改存储方案**，根据需求选择 腾讯云 或 S3 协议 。



配置腾讯云存储服务

步骤1：新建存储桶

存储桶用于存储 iOA 审计日志中的敏感文件和取证截图。

> **说明：**
> 如您未开通腾讯云对象存储服务，请前往腾讯云开通 对象存储 COS 。

1. 登录 对象存储控制台 ，在左侧导航栏，选择**存储桶列表**。
2. 在存储桶列表页面，单击**创建存储桶**，新建一个存储桶。



3. 在创建存储桶窗口中，配置基本信息，单击**下一步**。



参数名称	说明
所属地域	选择所属地域，存储桶与相同地域的其他腾讯云服务内网互通，地域一旦选择，无法修改，请谨慎选择。
名称	填写存储桶名称，名称一旦创建，无法修改，请谨慎填写。
访问权限	可在私有读写、公有读私有写、公有读写3种访问权限中进行选择。**建议配置：私有读写权限。**

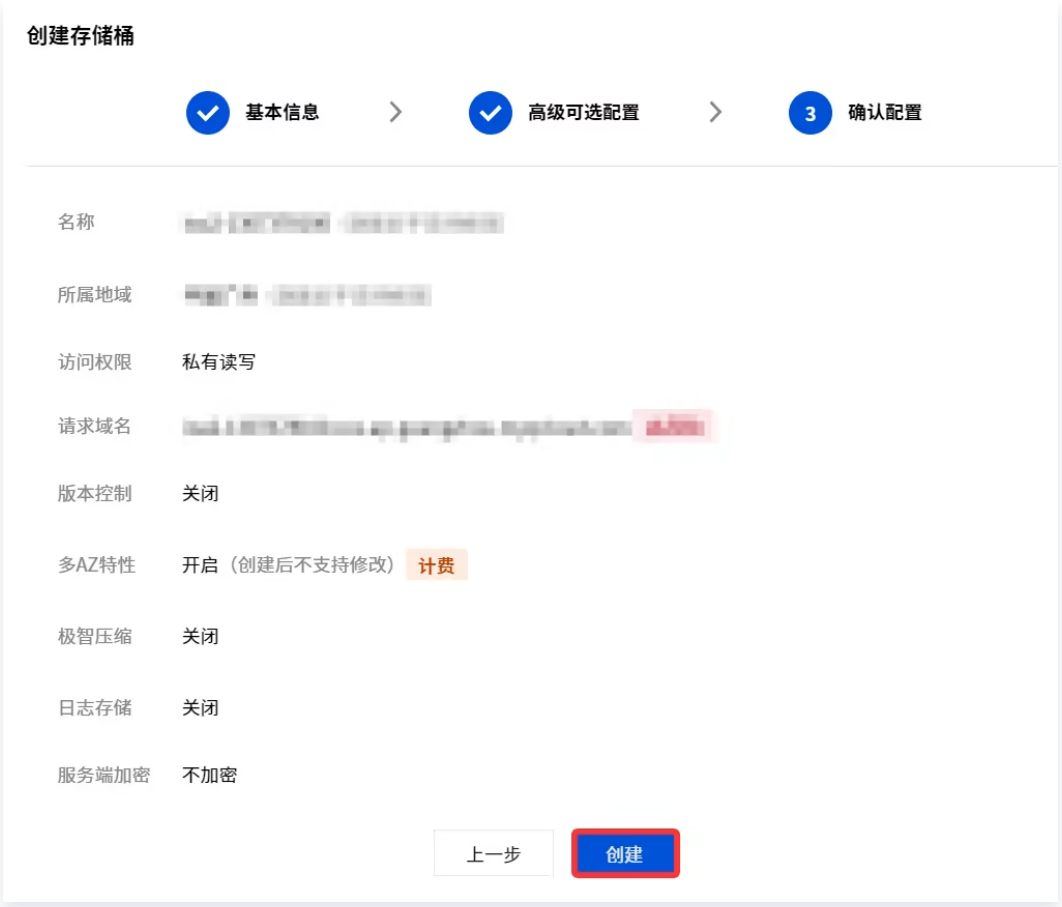
多 AZ 特性	• 部分地域支持多 AZ 特性，如不支持的地域，可通过设置存储桶跨区域复制。 • 多 AZ 特性允许用户将数据存储在同地理区域内的不同物理位置，提供同城容灾功能，推荐开启。

4. 在高级可选配置页签中，根据实际需求选择功能，单击**下一步**。



参数名称	说明
版本控制	可选择是否开启版本控制，开启版本控制后可以恢复因覆盖或误删丢失的数据。
极智压缩	极智压缩是在保证画质的前提下，尽可能地减小图片大小的功能。开启后，每次访问桶内的 JPG/PNG/GIF 格式的图片时将会实时压缩。
日志存储	可选择是否开启日志存储，开启后可记录跟存储桶操作相关的各种请求日志。
存储桶标签	支持输入标签键和标签值，可创建50个标签。
服务端加密	可选择不加密，或 SSE-COS 加密。

5. 配置信息确认无误后，单击**创建**，完成存储桶的创建。

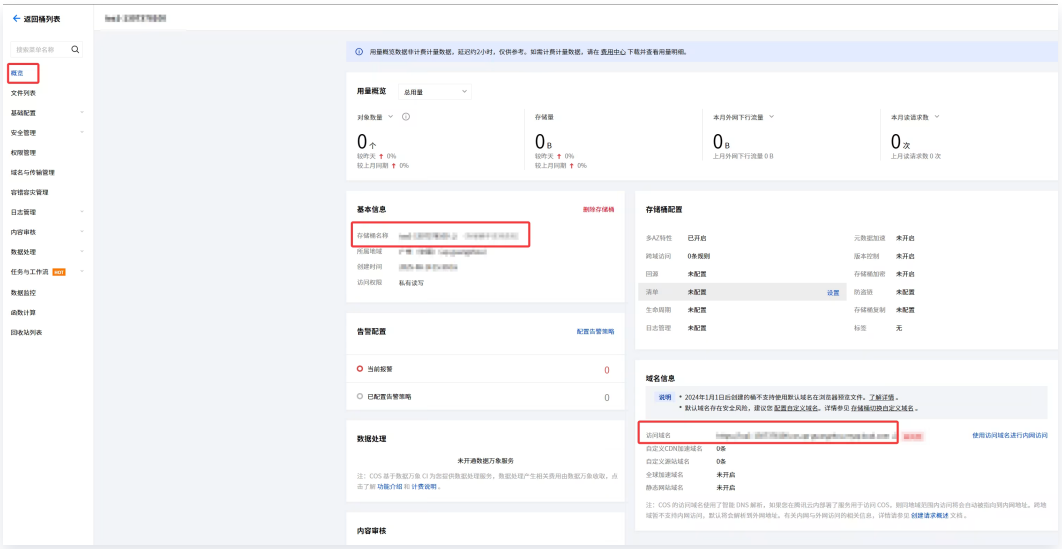


步骤2：获取 Bucket 和 Endpoint 参数

1. 完成存储桶的创建后，在 存储桶列表页面 ，单击**存储桶名称**，进入存储桶详情页面。



2. 单击**概览**，查看存储桶的概览页。找到**存储桶名称**和**访问域名**，分别作为 Bucket 和 Endpoint 参数。

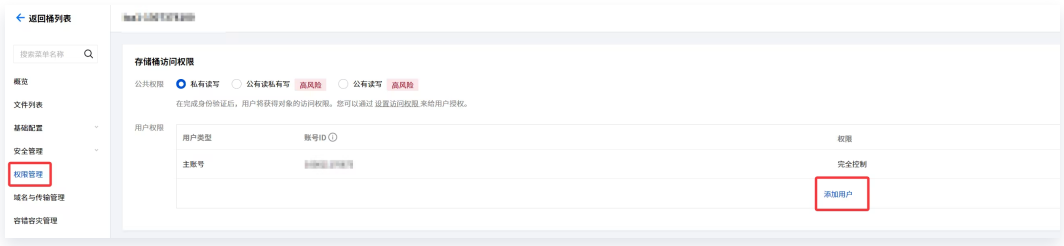


步骤3：为存储桶分配最小权限的子账号

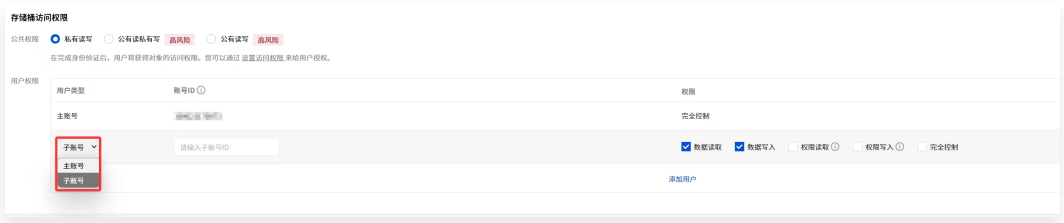
1. 完成存储桶创建后，在 存储桶列表页面 ，单击**存储桶名称**，进入存储桶详情页面。



2. 在存储桶详情页面，单击**权限管理 > 存储桶访问权限**。
3. 在存储桶访问权限页面，单击**添加用户**。



4. 添加用户时选择**子账号**，输入子账号 ID 并选择**数据读取**、**数据写入**两个权限，单击**确定**，即可为此存储桶分配一个具有读写权限（最小权限）的子账号。

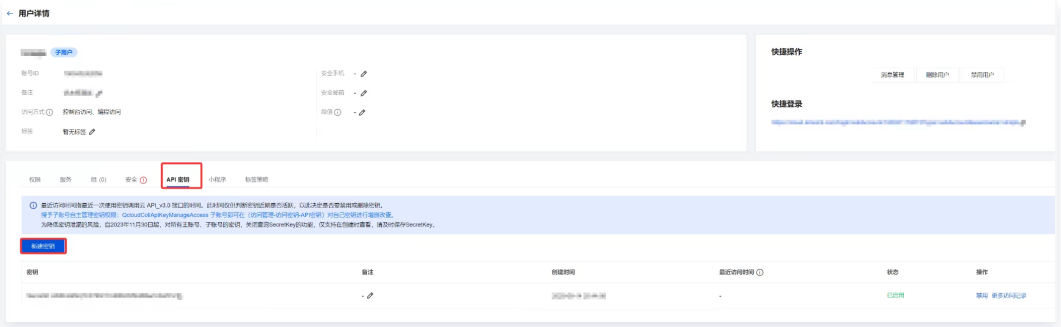


步骤4：获取子账号的 SecretId 和 SecretKey

1. 登录 访问管理控制台 ，在左侧导航栏，选择**用户 > 用户列表**。
2. 在用户列表页面，找到刚刚为存储桶分配的子账号，单击**用户名称**。

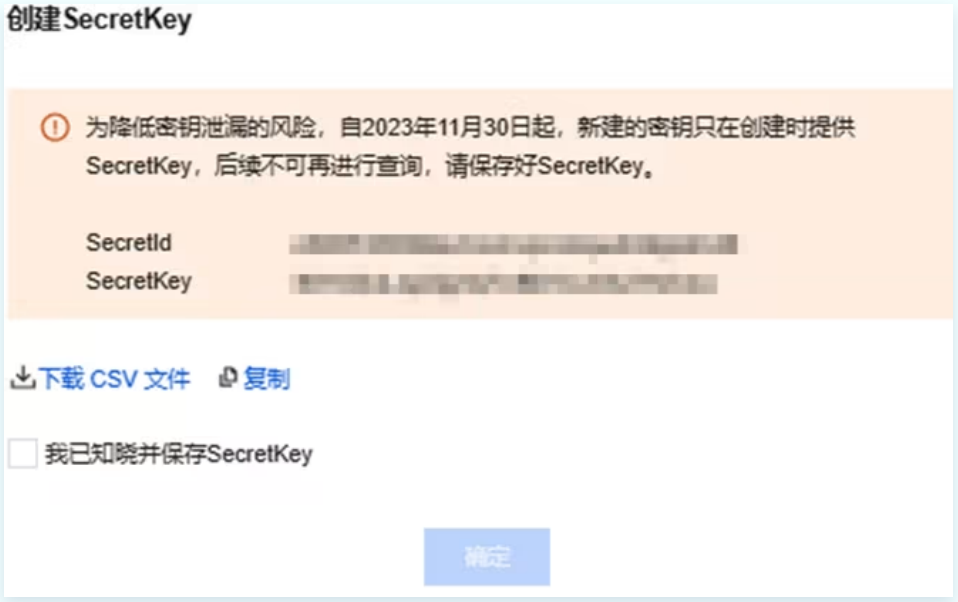


3. 在用户详情页面，单击 **API 密钥 > 新建密钥**，获取子账号的 SecretId 和 SecretKey。



注意：

为降低密钥泄露的风险，SecretKey 仅新建时提供，建议您保存好 SecretKey。



步骤5：回到 iOA 控制台，测试连通性

1. 完成各参数的获取后，返回 iOA 零信任管理平台控制台，在左侧导航栏，选择**管理中心** > **软件管理** > **软件仓库**或在**软件管控** > **分发管控** > **分发任务**页设置存储空间。
2. 存储目标选择**腾讯云**，依次填写上述获取的 **SecretId** 和 **SecretKey**、**Endpoint**、**Bucket**。填写完成后，单击**测试连通性**，若提示**测试成功**，即配置完成。



参数名称	说明
目标名称	腾讯云。
SecretId	步骤4 获取的子账号 SecretId。
SecretKey	步骤4 获取的子账号 SecretKey。
Endpoint	步骤2 获取的存储桶访问域名。
Bucket	步骤2 获取的存储桶名称。

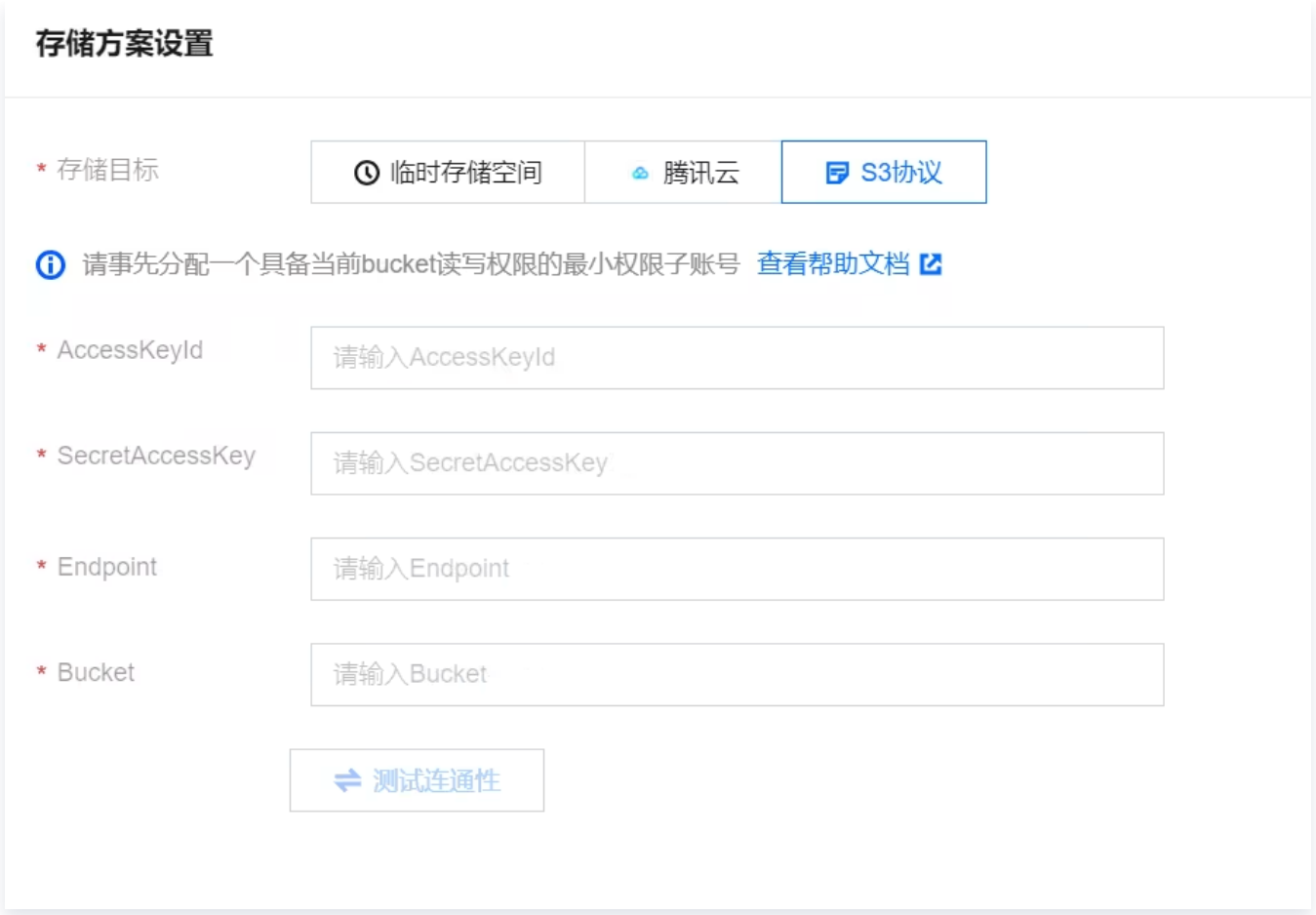
3. 配置完成单击**确定**保存。

配置 S3 协议存储服务

iOA 支持配置 S3协议的存储服务。

> **说明**
> 请事先分配一个具备当前 Bucket 读写权限的最小权限子账号。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管理中心 > 软件管理 ，在软件管理页面，根据需求选择 软件仓库**或**软件管控**，单击**更改存储方案**。
2. 存储目标选择为 **S3协议**，依次填写 **AccessKeyId** 和 **SecretAccessKey**、**Endpoint**、**Bucket**，单击**测试连通性**，若提示**测试成功**，即配置完成。



参数名称	说明
目标名称	S3协议。
AccessKeyId	唯一标识符，用于识别访问云存储服务的用户或应用程序。它通常与 SecretAccessKey 配合使用，以便在对云存储服务进行身份验证时提供安全访问。
SecretAccessKey	与 AccessKeyId 配对的私钥，用于对云存储服务进行身份验证。当创建一个新的 AccessKeyId 时，系统会自动生成一个与之关联的 SecretAccessKey。
Endpoint	云存储服务的 API 访问点。它是一个 URL，用于指向服务的特定区域和访问路径。客户端通过这个 URL与云存储服务进行通信。
Bucket	Bucket 名称。Bucket 是云存储服务中的一个基本容器，用于存储和组织数据。

3. 配置完成单击**确定**保存。

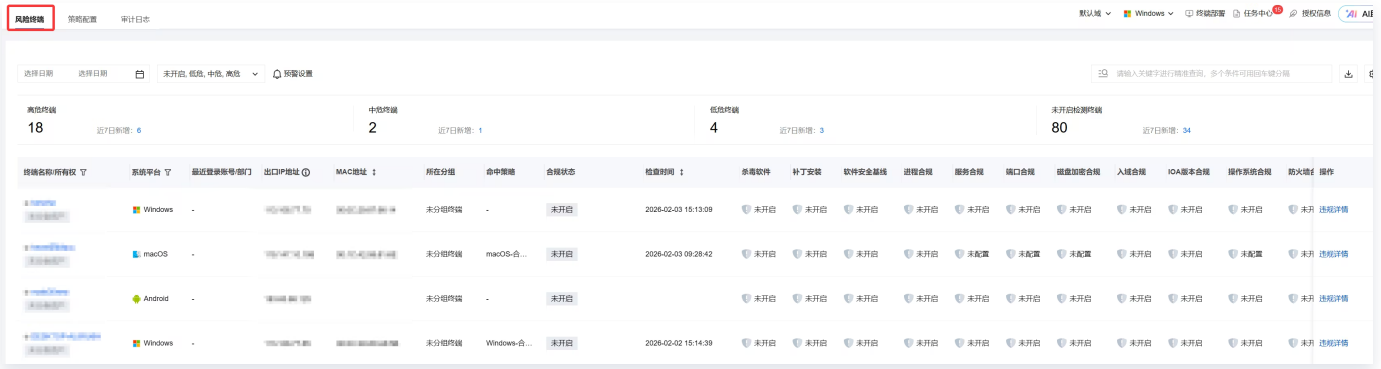
终端管控（11.1.1版）
合规检测（11.1.1版）
风险终端（11.1.1版）

最近更新时间：2026-02-06 14:23:31

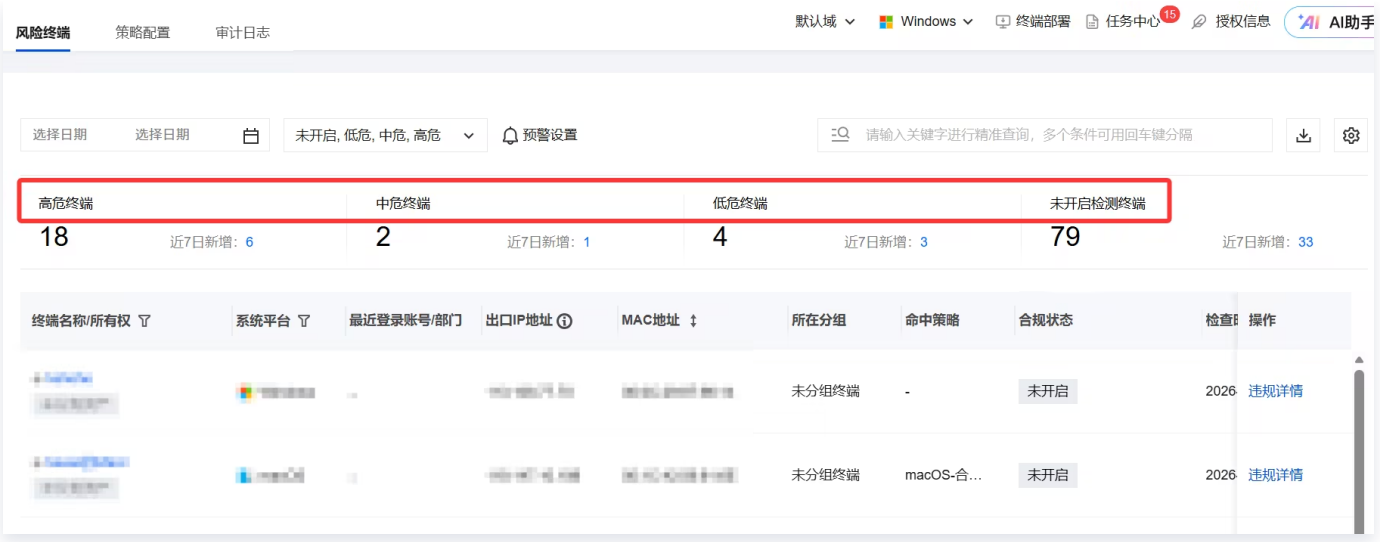
> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

风险终端展示全网终端设备的安全合规风险。通过预设的安全基线策略对终端进行持续或定时扫描，将发现的不合规项自动归类为“高、中、低”危等级，并以可视化看板和详情列表的形式集中呈现，为管理员提供“一眼看全局、一键下钻详情”的风险处置入口，是实现终端安全从被动响应到主动治理的关键工具。

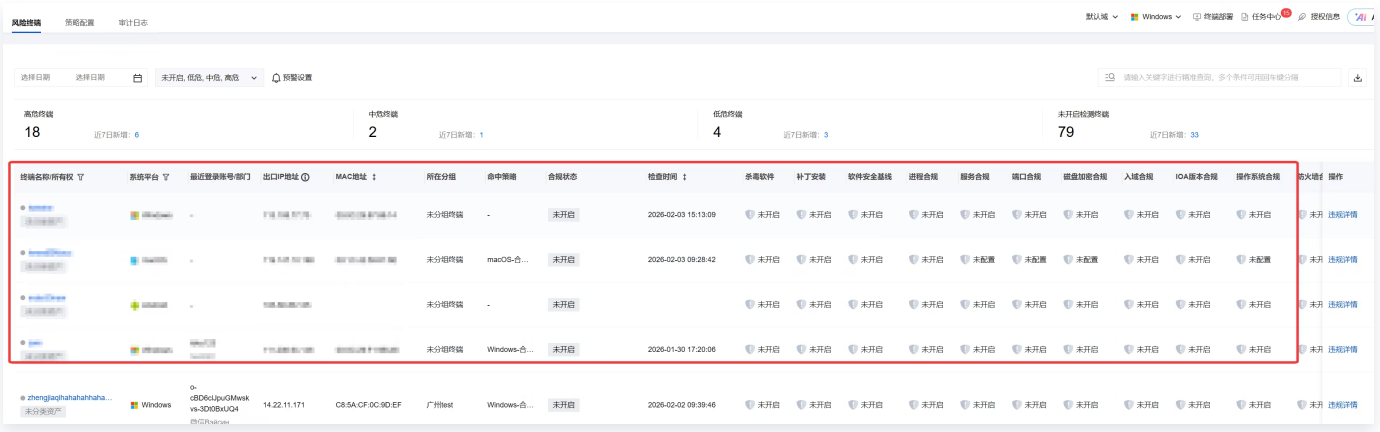
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **合规检测**。
2. 在合规检测页面，选择 **风险终端**，



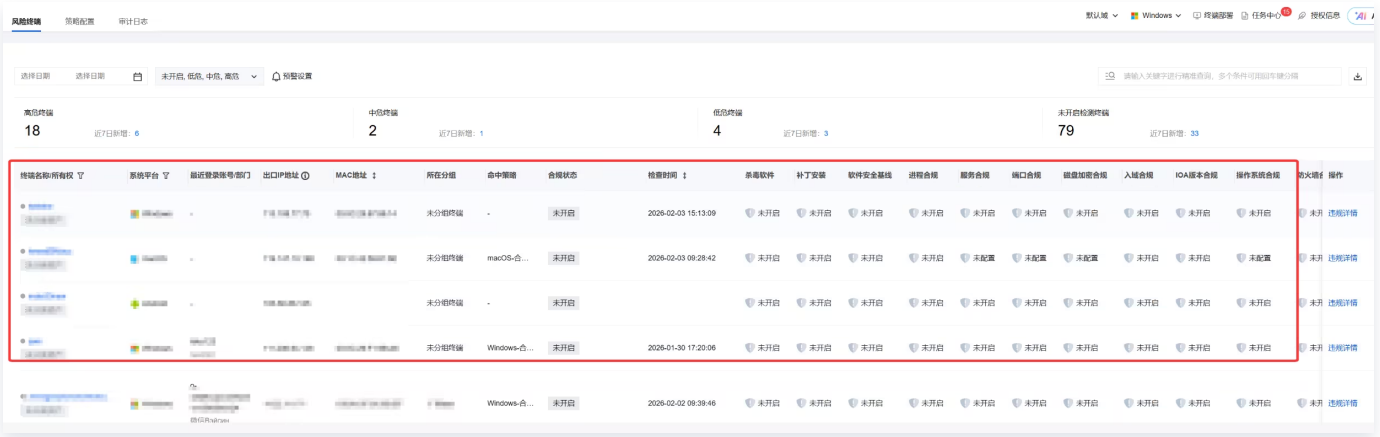
3. 风险分级统计：按风险等级分类统计终端安全状况，直观展示不同级别风险设备的分布与新增趋势，便于快速识别和优先处置高危设备。



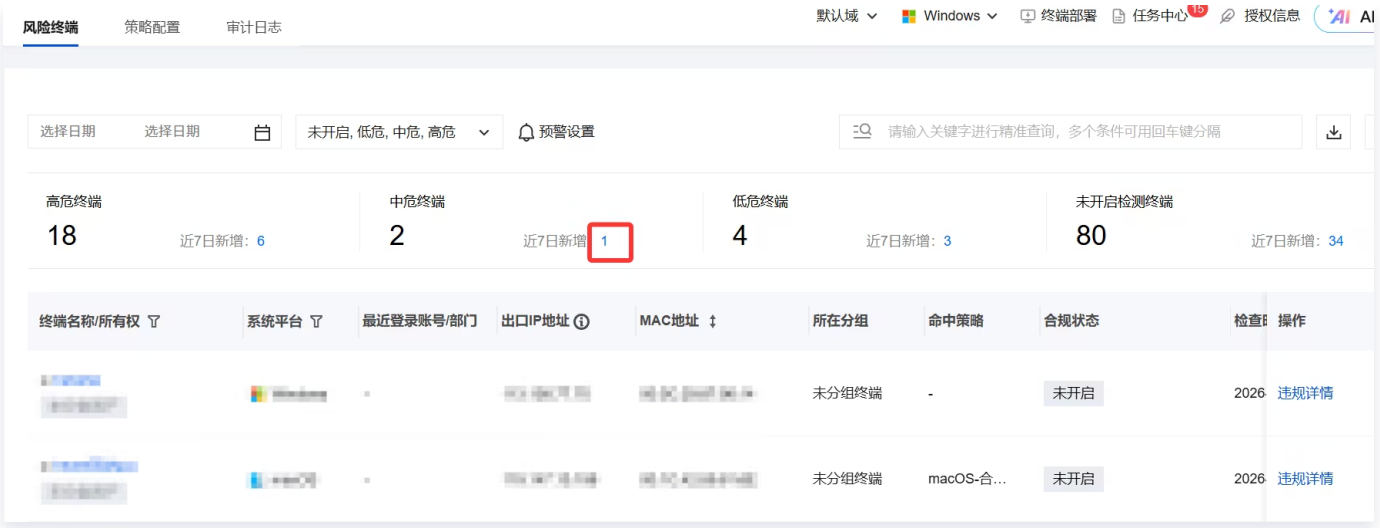
4. 合规状态总览：展示终端各项安全合规要求的达标状态，帮助管理员快速识别和处置不合规终端。



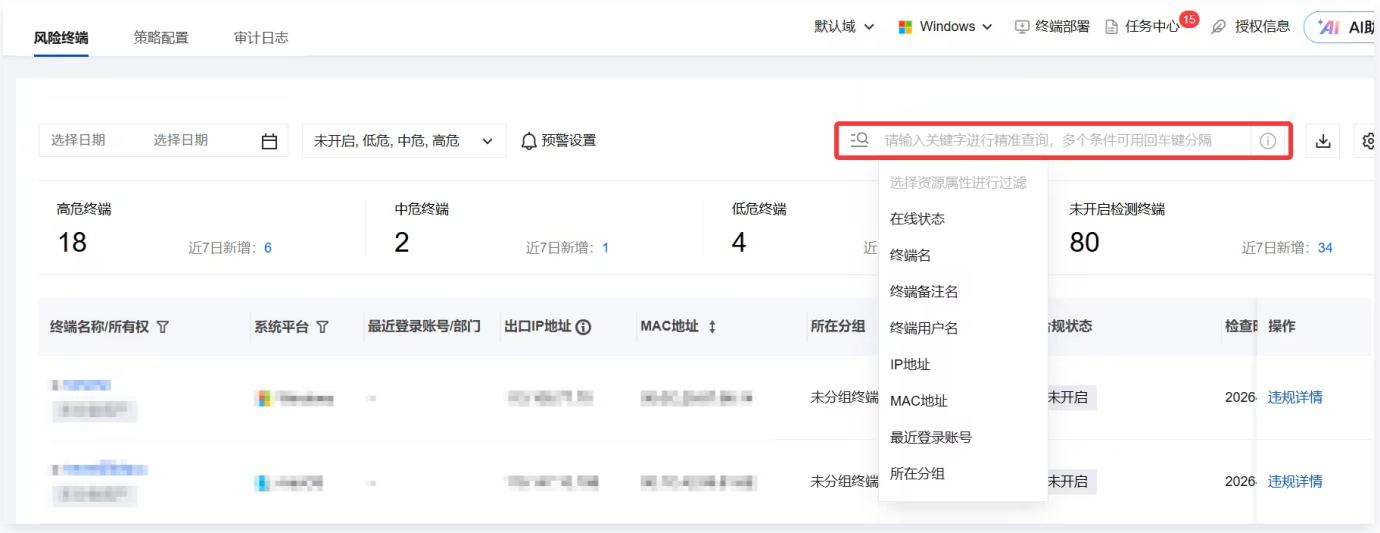
5. 支持在时间筛选框中选择您要查看的日期范围。



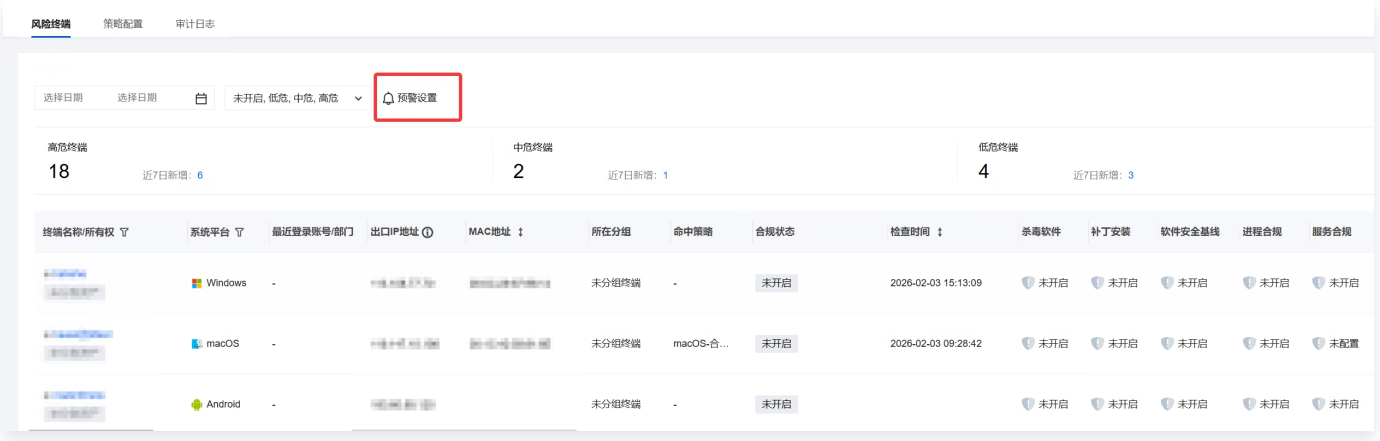
6. 单击列表中**近7日新增的蓝色数字**，显示过去7天内新增的终端数量。



7. 在搜索框中，输入终端名、MAC地址等信息，可直接定位特定设备。



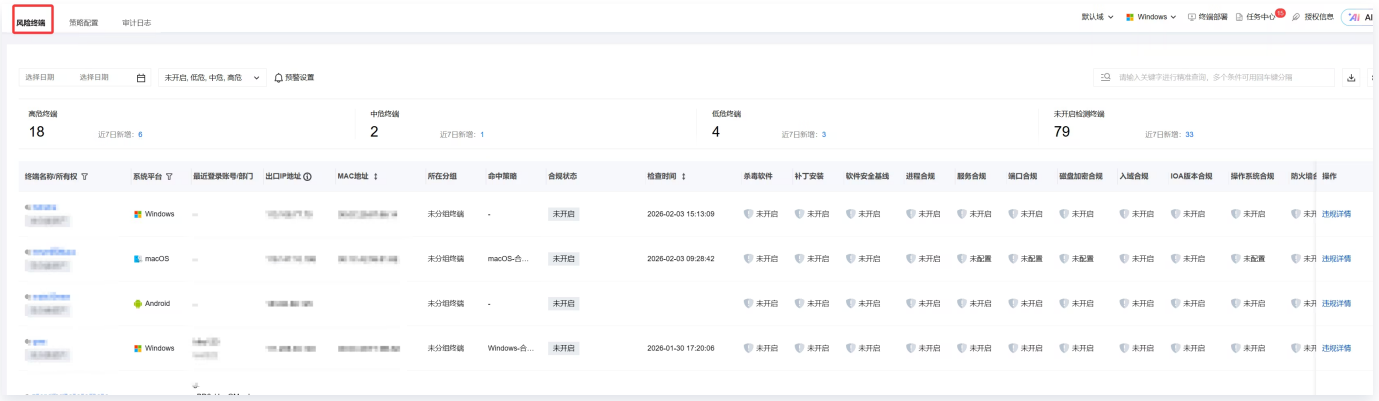
8. 单击**预警设置**，设置风险预警通知规则。



9. 前往**腾讯云消息中心 > 订阅管理** 选择产品**iOA 零信任安全管理系统**，编辑接收订阅消息的接收人及接收方式。



10. 当存在触发阈值的风险终端时，可在风险终端查看详情



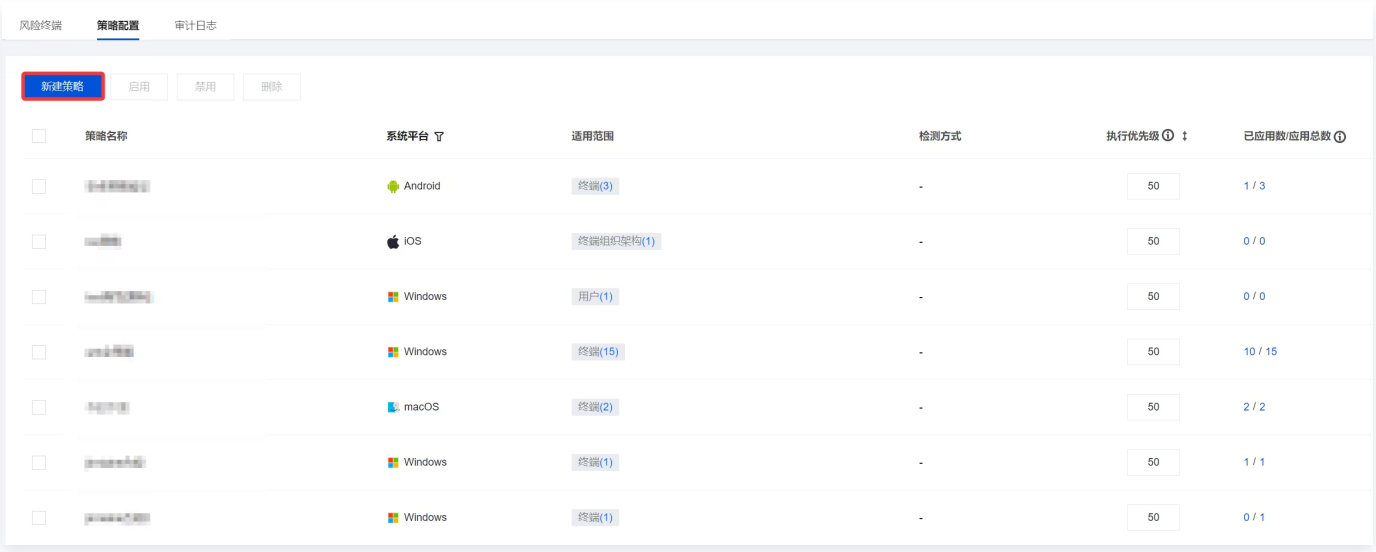
合规检测策略配置（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

对终端设备进行安全性要求的检测，检测结果可联动 iOA 零信任办公的接入。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **合规检测**。
2. 在合规检测页面，选择**策略配置**，单击**新建策略**。



3. 在新建策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。

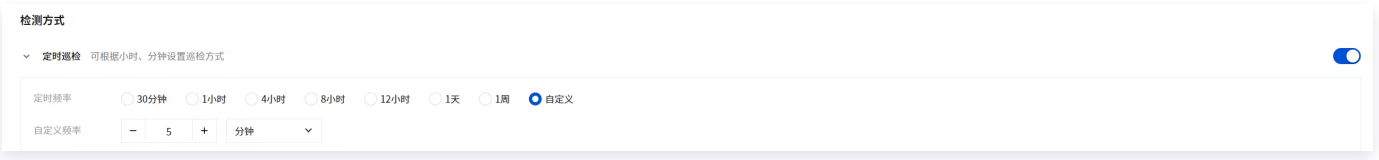


3.2 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**保存**。

4. 根据实际需求，选择如下**合规检测策略**，单击**保存**。

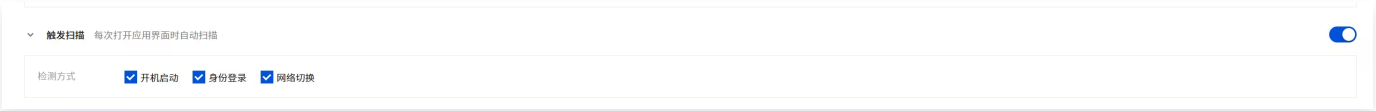
定时巡检

1. 可根据需要选择不同的巡检频率，包括30分钟、1小时、4小时、8小时、12小时、1天、1周或自定义。
2. 自定义选项允许用户通过输入框设置具体的分钟数，以分钟为单位调整巡检频率。
3. 频率最低支持设置5分钟，该分组下的终端到达满足条件的时间点，自动执行合规检查。



触发扫描

1. 该功能会在您每次打开应用界面时自动进行安全扫描。支持开机启动、身份登录、网络切换等多场景触发合规扫描，灵活适应用户使用环境，确保设备在这些关键时刻得到安全检查。
2. 如下勾选后在开机时、登录 iOA 客户端时、内外网切换时符合这三类情况都将扫描一次。



终端名

1. 检测终端名称是否合规，单击**开启检测**并单击**添加检测点**。



2. 配置检测规则、违规等级、修复方式、违规处置等参数。

参数名称		说明
检测方式	关键字	检测条件：匹配特定字词，适用于检测明确的字词信息。
	正则	正则表达式：通过灵活的模式规则匹配文本格式，适合检测变体等复杂规律。
违规等级		低、中、高。
修复指引		• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。 • 修复指引文档请参见 帮助中心 。
违规处置		• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

3. 配置完成后单击**保存**。



4. 客户端拉取策略后，打开客户端合规页面单击**立即检测**。



5. 终端不符合检测条件则判定为风险，触发相应修复及违规处置。



终端用户名

1. 检测终端用户名是否合规，单击**开启检测** 并单击**添加检测点**。



2. 配置检测规则，符合检测条件则判定为风险，触发相应修复及违规处置。



3. 客户端拉取策略后，打开客户端合规页面单击**立即检测**。



4. 终端上的用户名不包含检测条件，检测项合规。



第三方杀毒软件

1. 检测终端是否安装对应版本的第三方杀毒软件。
2. 单击**开启检测**，并单击**添加检测点**。



3. 在添加第三方杀毒软件弹窗中，配置相关参数，单击**保存**。



参数	说明
软件名称	根据管控需求自行选择第三方杀毒软件名称。
检查软件版本号	• 开启：选择开启时需设置软件版本号。 • 关闭：无需设置软件版本号。
检查病毒库版本号	• 开启：选择开启时需设置病毒库版本号。 • 关闭：无需设置病毒库版本号。
检查最新病毒库	• 开启：根据管控需求自行设置距最新病毒库检测更新的时间天数。 • 关闭：无需设置检查最新病毒库。
违规等级	低、中、高。
修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。
违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。

- 不合规时仅提醒：仅提醒是否合规。
- 不合规时禁用零信任办公（联动零信任网关）：强制登出企业账号，限制终端访问内网资源。

4. 配置完成后单击**保存**，配置参数可参考下图示例。



5. 完成添加后，单击**保存**。



6. 客户端拉取策略后，打开客户端合规页面单击**立即检测**。



7. 终端未安装对应的第三方杀毒软件，检测结果不合规。



补丁列表

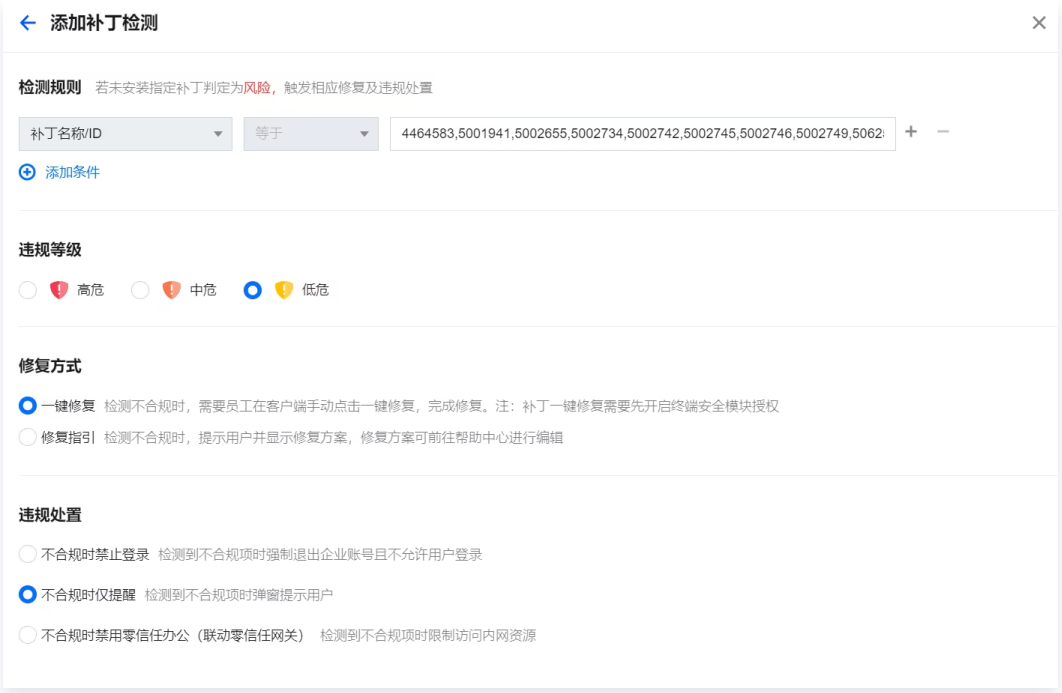
1. 检测终端是否存在必须安装但未安装的补丁。
2. 单击**开启检测**，并单击**添加检测点**。



3. 在添加补丁检测弹窗中，配置相关参数，单击**保存**。



4. 配置参数可参考下图示例：



5. 完成添加后，单击**保存**。



6. 客户端拉取策略后，打开客户端合规检测页面单击**立即检测**。



7. 终端未安装某个必须安装的补丁，检测结果显示设备不合规。



软件安全基线

1. 检测终端是否安装了违规软件，或未安装必备软件。
2. 在合规检测策略页面，单击**开启检测**，并单击**添加检测点**。



3. 在添加软件安全基线检测项弹窗中，配置相关参数，单击**保存**。



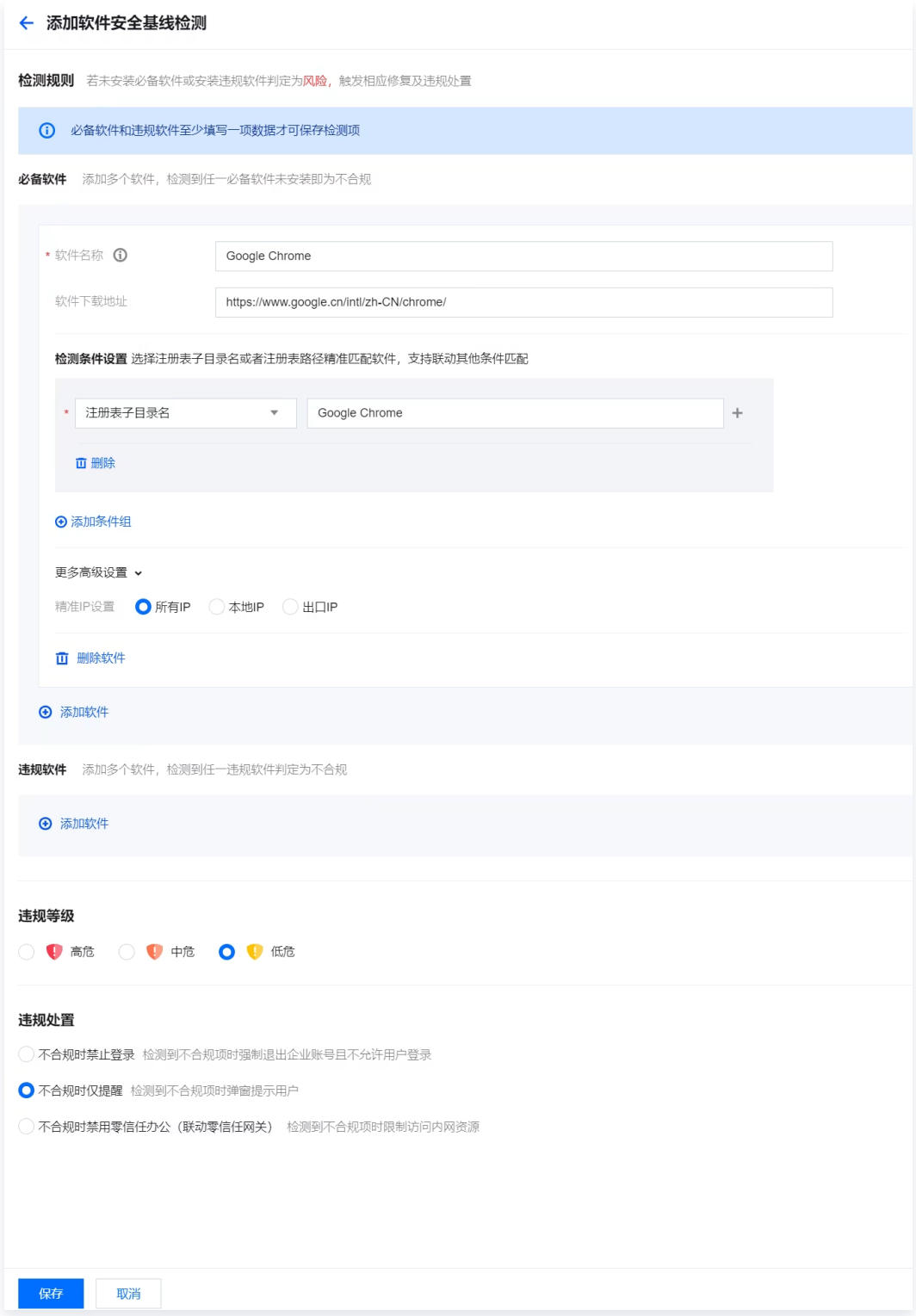
参数名称		说明
必备软件	软件名称	• 必填项。 • 仅用于在客户端展示必备软件名称，不作为检测判断条件。
	软件下载地址	• 非必填项。 • 下载此软件的链接地址（软件官网下载地址），填写后，客户端检测结果违规的情况下，页面会出现该软件下载链接。

注册表子目录名	• 选择注册表子目录名时，会从注册表卸载路径中搜索对应的子目录名，从而判定软件是否安装，例如：填写 Edge，则会到注册表卸载目录进行搜索。 • 可能部分软件未在卸载注册表路径写入子目录名导致无法判断，此时建议您选择通过“注册表路径”进行判断。 如何查找注册表子目录名： 1. 打开注册表编辑器：按下 Win + R 键，打开“运行”对话框，输入 regedit，然后按 Enter 键。 2. 导航到目标路径：在注册表编辑器中，依次展开目标路径，查看其子项名称。
注册表路径	选择“注册表路径”时，可对注册表全路径进行搜索，而判定软件是否安装，例： HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Edge 如何查找某个软件的注册表路径： 1. 打开注册表编辑器：按下 Win + R 键，打开“运行”对话框，输入 regedit，然后按 Enter。 2. 导航到可能的路径：大多数用户安装的应用软件注册表项位于 HKEY_LOCAL_MACHINE\Software或 HKEY_CURRENT_USER\Software。 3. 支持根据软件的安装路径或公司名称进行查找，例如： ○ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall：此路径下存储了已安装软件的卸载信息。 ○ HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\App Paths：此路径下存储了某些应用程序的可执行文件路径。 4. 搜索软件名称：在注册表编辑器中，使用“查找”功能（Ctrl + F），输入软件名称或相关关键词进行搜索。
软件版本号	• 非必填项。 • 自定义软件版本号。
版本号键名	• 非必填项。 • 查询版本号键名：在注册表编辑器中，软件版本信息通常存储在：HKEY_LOCAL_MACHINE\SOFTWARE\[软件厂商]\[软件名称] • 键名常见为：DisplayVersion、Version、ProductVersion。
版本号键值	• 非必填项。 • 查询版本号键值：可通过文件属性查看，右键程序文件 > 属性 > 详细信息 > 文件版本/产品版本。

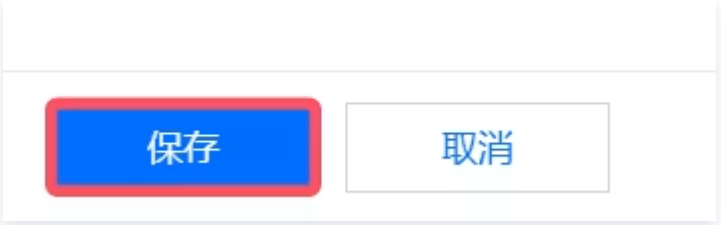
版权所有：腾讯云计算（北京）有限责任公司

	进程名称	• 非必填项。 • 如果已填写进程名称，会检测是否启动该进程，未启动时提示设备违规。
	MD5（32位）	• 非必填项。 • 软件的 MD5 值。
	更多高级设置	精准 IP 设置：支持按 IP 段精准匹配，客户端仅在指定网络范围内生效对应策略。
违规软件	软件名称	• 必填项。 • 仅用于在客户端展示必备软件名称，不作为检测判断条件。
	注册表子目录名	• 选择注册表子目录名时，会从注册表卸载路径中搜索对应的子目录名，从而判定软件是否安装。 • 例如：填写 Edge，则会到注册表卸载目录进行搜索。 • 可能部分软件未在卸载注册表路径写入子目录名导致无法判断，此时建议您选择通过“注册表路径”进行判断。 如何查找注册表子目录名： 1. 打开注册表编辑器：按下Win + R 键，打开“运行”对话框，输入 regedit，然后按 Enter 键。 2. 导航到目标路径：在注册表编辑器中，依次展开目标路径，查看其子项名称。
	软件版本号	• 非必填项。 • 自定义软件版本号。
	更多高级设置	精准 IP 设置：支持按 IP 段精准匹配，客户端仅在指定网络范围内生效对应策略。

4. 配置参数可参考下图示例：



5. 完成添加后，单击**保存**。



6. 客户端拉取策略后，打开客户端合规检测页面单击**立即检测**。



7. 终端上存在违规软件，或缺少指定的必装软件，检测结果设备不合规。



违规进程

1. 检测客户端是否存在违规进程。
2. 单击**开启检测**，并单击**添加检测点**。



3. 在添加违规进程检测项弹窗中，配置相关参数，单击**保存**。

> **说明：**
> 配置违规进程规则（支持通配符），例如：n*



参数名称	说明
违规进程	填写进程名称。
违规等级	低、中、高。
修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。 • 修复指引文档请参见 帮助中心 。
违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

4. 配置参数可参考下图示例：



5. 完成添加后，单击**保存**。



6. 客户端拉取策略后，打开客户端合规检测页面单击**立即检测**。



7. 终端上存在违规的进程，检测结果设备不合规。



违规服务

1. 检测客户端是否已启动违规服务。
2. 单击**开启检测**，并单击**添加检测点**。



3. 在添加违规服务检测项弹窗中，配置相关参数，单击**保存**。

> **说明：**
> 配置违规服务规则（支持通配符），例如：VM*。



参数名称	说明
违规服务	填写服务名称。

违规等级	低、中、高。
修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。
违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

4. 配置参数可参考下图示例：



5. 完成添加后，单击**保存**。



6. 客户端拉取策略后，打开客户端合规检测页面单击**立即检测**。



7. 终端上存在违规的服务，检测结果设备不合规。



违规端口

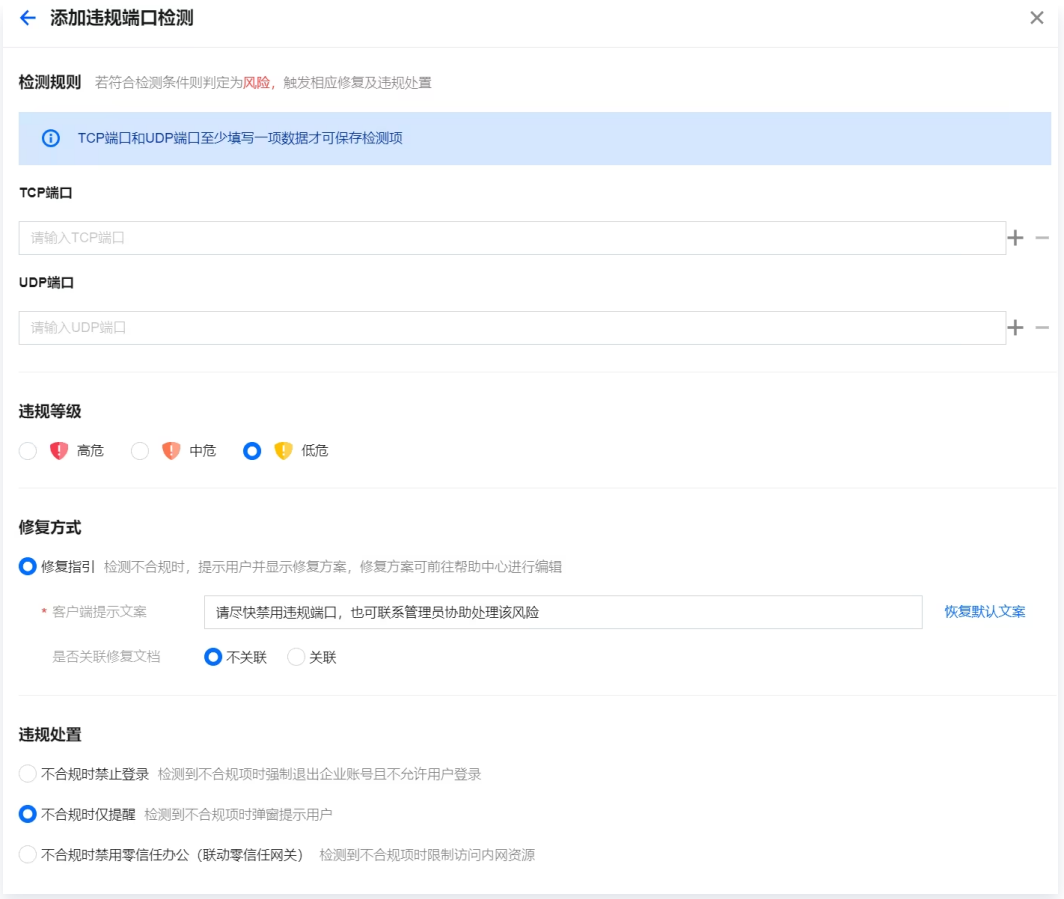
1. 检测客户端是否开启违规端口。

> **说明：**
> 违规端口项需关闭系统防火墙才能检测到。

2. 单击**开启检测**，并单击**添加检测点**。



3. 在添加违规端口检测项弹窗中，配置相关参数，单击**保存**。



参数名称	说明
违规端口	• 填写 TCP 端口。 • 填写 UDP 端口。
违规等级	低、中、高。
修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。 • 修复指引文档请参见 帮助中心 。
违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

4. 配置参数可参考下图:



5. 完成添加后，单击**保存**。



6. 客户端拉取策略后，打开客户端合规检测页面单击**立即检测**。



7. 终端开启了对应违规端口，检测结果不合规。



磁盘加密

1. 该策略检测所有磁盘是否全部加密，单击**开启检测**，**并单击添加检测点**。



2. 配置检测规则、修复方式等参数，配置参数可参考下图示例：



3. 客户端拉取策略后，打开客户端合规页面单击**立即检测**。



4. 终端未开启磁盘加密检测，检测结果不合规。

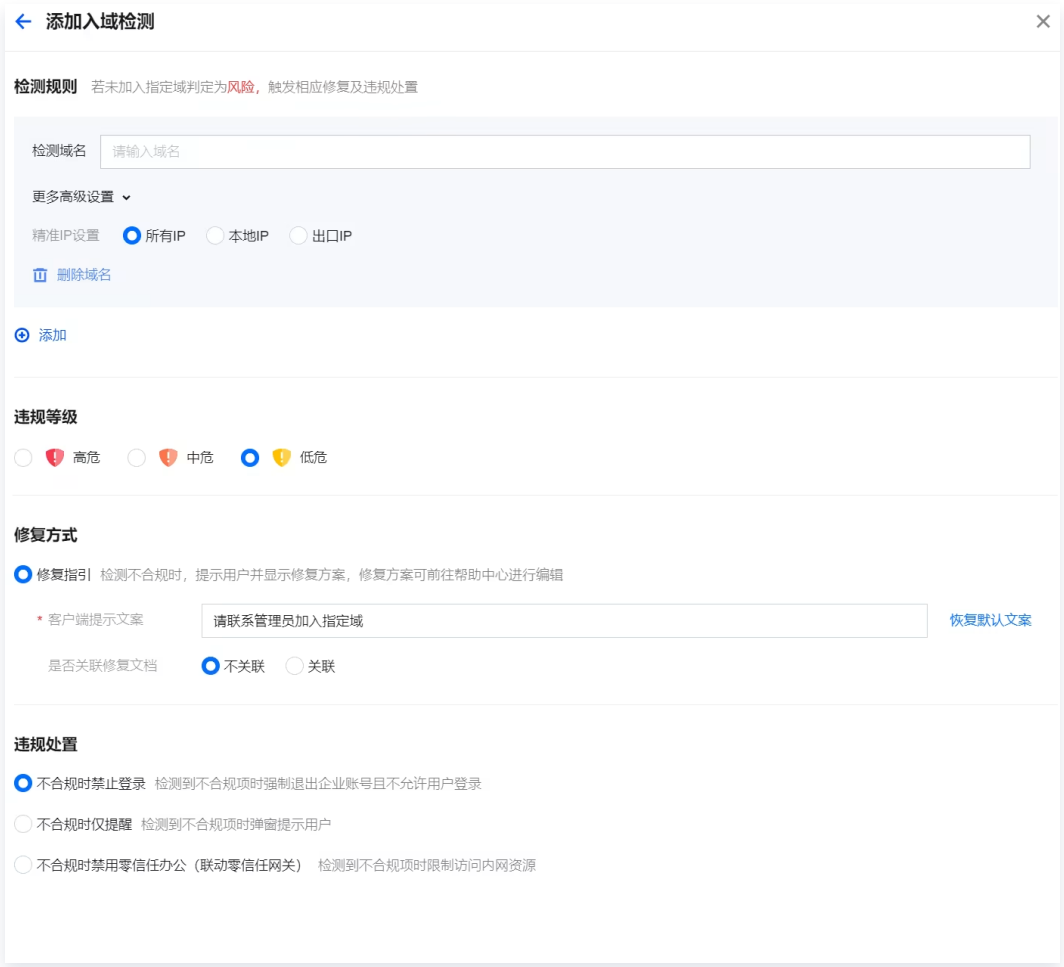


入域

1. 单击**开启检测**，并单击**添加检测点**。



2. 在添加入域检测项弹窗中，配置相关参数，单击**保存**。



参数名称	说明
检测域名	填写入域名称。

精准IP设置	所有 IP：在范围内的所有 IP 都会检测。 本地 IP：用于终端连接总控的 IP。 出口 IP：用于终端连接外网的 IP。
违规等级	低、中、高。
违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

3. 配置参数可参考下图示例：



4. 完成添加后，单击**保存**。



5. 客户端拉取策略后，打开客户端合规检测页面单击**立即检测**。



6. 终端未入域，检测结果终端不合规。



客户端版本

1. 单击**开启检测**，并单击**添加检测点**。



2. 在添加客户端版本检测项弹窗中，配置相关参数，单击**保存**。



参数名称	说明
检测客户端版本低于	根据您所在公司的管控需求，填写用户安装的客户端最低版本号。
违规等级	低、中、高。
修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。 • 修复指引文档请参见 帮助中心 。
违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

3. 配置参数可参考下图示例：



4. 完成添加后，单击**保存**。



5. 客户端拉取策略后，打开客户端合规检测页面单击**立即检测**。



6. 终端上的 iOA 客户端版本不满足最低版本要求，检测结果设备不合规。



操作系统

1. 单击**开启检测**，并单击**添加检测点**。



2. 在添加操作系统检测项弹窗中，配置相关参数，单击**保存**。



参数名称	说明
检测操作系统版本低于	下拉选择：Windows XP、Windows Vista、Windows 7、Windows Server 2012、Windows 8、Windows 10、Windows 11。
检测操作系统细分版本低于	输入系统版本号 系统版本号查看方式：Win+R，输入 cmd 后按 Enter 键，再输入ver 后按 Enter 键。

违规等级	低、中、高 。
修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。 • 修复指引文档请参见 帮助中心 。
违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

3. 配置参数可参考下图示例：



4. 完成添加后，单击**保存**。



5. 客户端拉取策略后，打开客户端合规检测页面单击**立即检测**。



6. 终端的操作系统版本过低，检测结果设备不合规。



弱密码

> **注意：**
>
> - **建议您谨慎开启此功能，开启后会读取终端的账号和密码哈希等敏感信息，可能导致其他终端安全软件误报风险。**
> - 在配置弱密码数量很多的情况下，终端计算弱密码的哈希会比较损耗系统性能（尤其是开启域账号检测的情况下），建议弱密码数量不超过一万条。
> - 域账号登录场景下，特殊服务器或经过特殊安全设置的系统，**如果系统没有缓存域账号的登录凭据，则域账号弱密码扫描功能无法使用。**

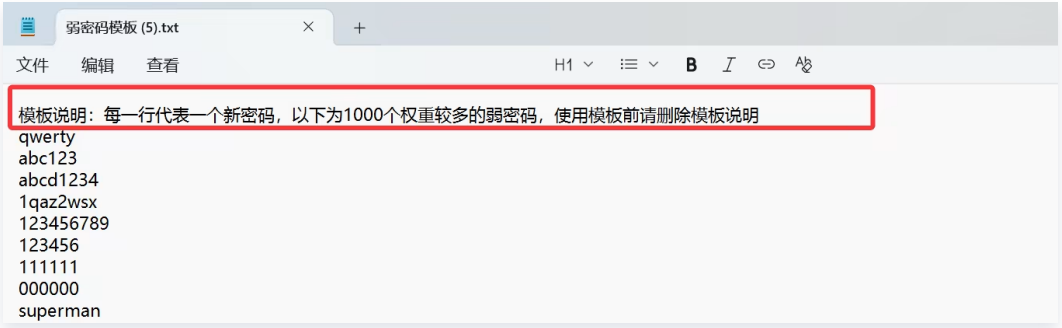
1. 单击**开启检测**，并单击**添加检测点**。



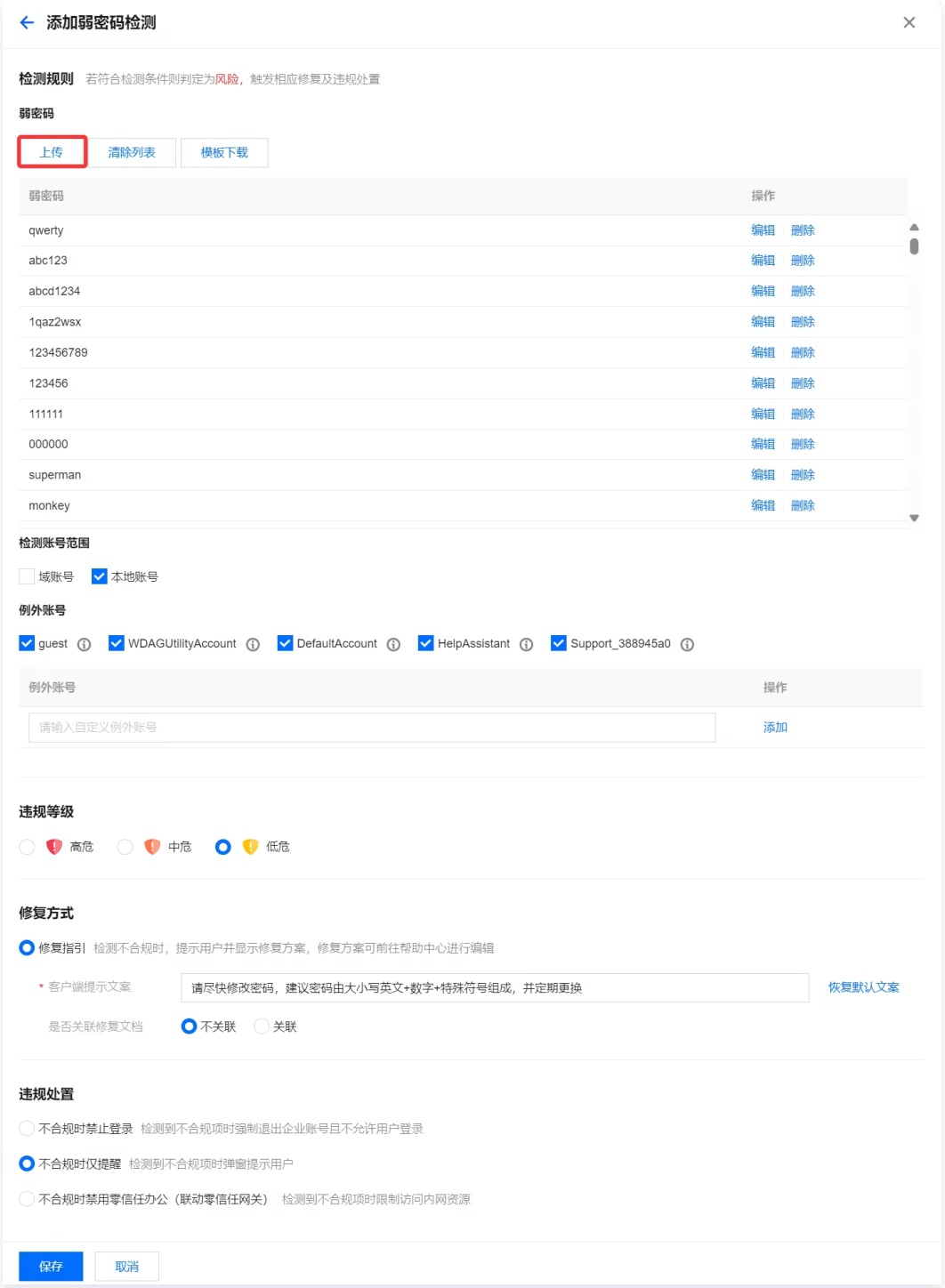
2. 在添加弱密码检测项弹窗中，单击**模板下载**。



3. 删除模板说明，并保存文档。



4. 配置参数可参考下图示例，单击**上传**，导入修改后的文档后单击**保存**。



5. 完成添加后，单击**保存**。



6. 客户端拉取策略后，打开客户端合规检测页面单击**立即检测**。



7. 终端账户的密码如为弱密码（必须在导入的文档内存在），例如：abc123。
8. 当终端账号密码命中了弱密码列表内的密码，检测提示不合规。



注册表

1. 单击**开启检测**，并单击**添加检测点**。



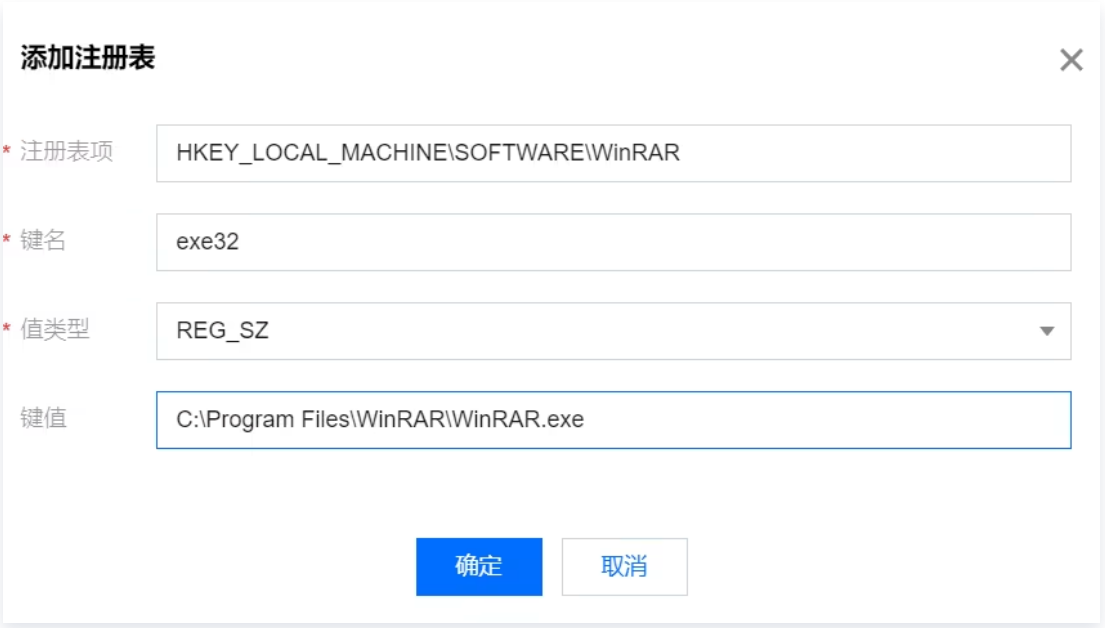
2. 在添加注册表检测项弹窗中，配置相关参数，单击**保存**。



参数名称		说明
注册表	注册表项	• 必填项。 • 填写示例：安装一个 WinRAR 解压缩软件。 • 注册表项填写示例：HKEY_LOCAL_MACHINE\SOFTWARE\WinRAR 。
	键名	• 必填项。 • 填写示例：exe32 。
	值类型	• 必填项。 • 下拉选择：REG_SZ、REG_DWORD(10进制)、REG_MULTI_SZ、REG_EXPAND_SZ、REG_QWORD(10进制)。
	键值	• 非必填项。 • 填写示例：C:\Program Files\WinRAR\WinRAR.exe。
违规等级		低、中、高。
修复指引		• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。

	• 修复指引文档请参见 帮助中心 。
违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

3. 配置参数可参考下图示例：



4. 完成添加后，单击**保存**。



5. 客户端拉取策略后，打开客户端合规检测页面并单击**立即检测**。



6. 终端上不存在违规的注册表，检测结果为设备合规。



防火墙

1. 配置此策略后，检查系统是否开启防火墙，单击**开启检测**  ，并单击**添加检测点**。



2. 配置违规等级、修复方式、违规处置等参数。

参数名称		说明
违规等级		低、中、高。
修复方式	一键修复	检测不合规时，需要用户在客户端手动单击一键修复后方可完成修复。
	修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。 • 修复指引文档请参见 帮助中心 。

违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

3. 配置参数可参考下图示例：



4. 配置完成后单击**保存**。



5. 客户端拉取策略后，打开客户端合规页面并单击**立即检测**。



6. 终端开启系统防火墙，检测结果为设备合规。



自动锁屏检测

1. 检测终端是否设置自动锁屏，单击**开启检测** 并单击**添加检测点**。



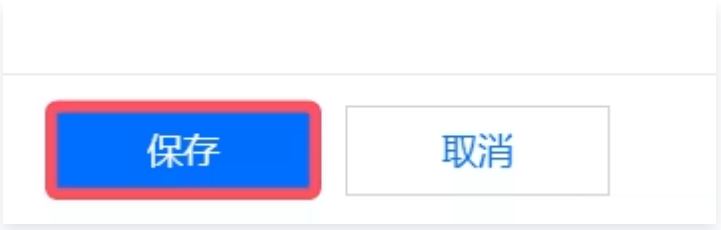
2. 在添加自动锁屏检测弹窗中，配置相关参数。

参数名称		说明
违规等级		低、中、高。
修复方式	一键修复	检测不合规时，需要用户在客户端手动单击一键修复后方可完成修复。
	修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。 • 修复指引文档请参见 帮助中心 。
违规处置		• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。

3. 配置参数可参考下图示例：



4. 完成添加后，单击**保存**



5. 客户端拉取策略后，打开客户端合规页面并单击**立即检测**。



6. 检测到未设置自动锁屏，可单击**一键修复**。



系统完整性（SIP）检测

> **说明：**
> macOS 系统功能，Windows 下无此功能。

1. macOS 系统完整性保护默认开启，若用户手动关闭可能会导致终端系统存在不可控风险，因此在合规检测中增加 SIP 开启的检测，单击**开启检测**，并单击**添加检测点**。



2. 配置不合规时处置策略：仅提醒或禁用零信任办公，配置完成后单击**保存**。

参数名称	说明
违规等级	低、中、高。
修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。 • 修复指引文档请参见 帮助中心 。
违规处置	• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。 • 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。



3. 客户端检测项示例：



安装安全响应和系统文件检测

> **说明：**
> macOS 系统功能，Windows 下无此功能。

系统版本低于 macOS15 检测到**检查更新**和**安装安全响应**任一项未开始判定为不合规，系统版本为 macOS15 及以上检测到**安装安全响应**未开启判定为不合规。

1. 单击**开启检查**，并单击**添加检测点**。



2. 配置违规等级、修复方式、违规处置等参数，配置完成后单击**保存**。

参数名称		说明
违规等级		低、中、高。
修复方式	一键修复	检测不合规时，需要用户在客户端手动单击一键修复后方可完成修复。
	修复指引	• 自定义客户端提示文案。 • 支持关联修复文档，引导用户依据定制的指引文档完成修复，提升合规修复效率。 • 修复指引文档请参见 帮助中心 。
违规处置		• 不合规时禁止登录：检测到不合规项时强制退出企业账号且不允许用户登录。 • 不合规时仅提醒：检测到不合规项时弹窗提示用户。

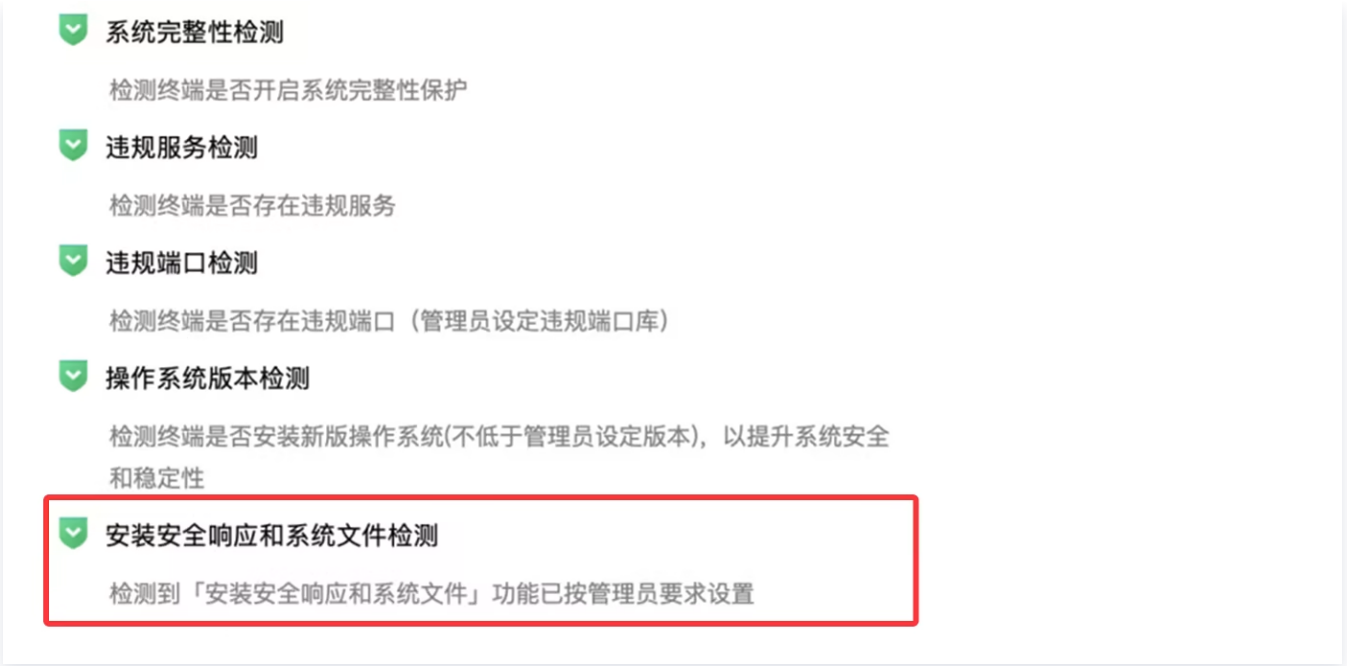
	• 不合规时禁用零信任办公（联动零信任网关）：检测到不合规项时限制访问内网资源。



3. 客户端拉取策略后，打开客户端合规检测页面后单击**立即检测**。



4. 终端上安装安全响应并进行系统文件检测，检测结果为设备合规。


系统完整性检测
检测终端是否开启系统完整性保护
违规服务检测
检测终端是否存在违规服务
违规端口检测
检测终端是否存在违规端口（管理员设定违规端口库）
操作系统版本检测
检测终端是否安装新版操作系统(不低于管理员设定版本)，以提升系统安全和稳定性
安装安全响应和系统文件检测
检测到「安装安全响应和系统文件」功能已按管理员要求设置

合规检测审计日志（11.1.1版）

最近更新时间：2026-02-13 09:41:02

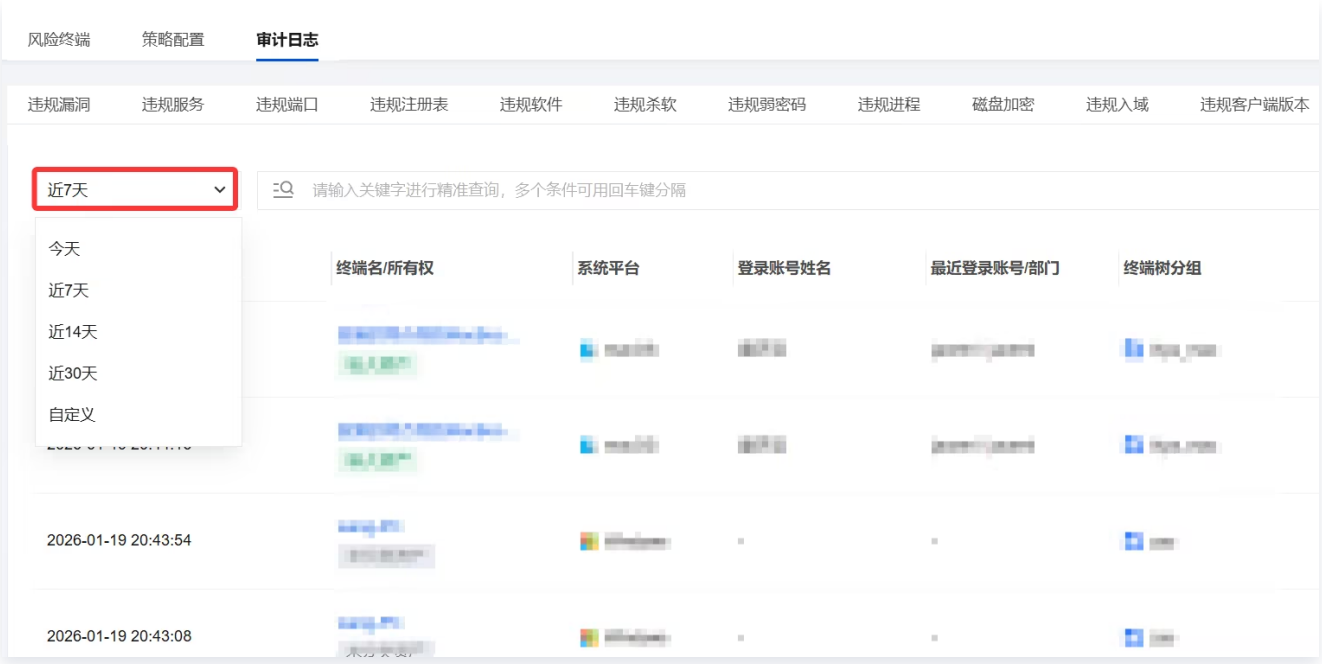
> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

日志功能概览

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **合规检测** > **审计日志**。
2. 审计日志集中记录并展示所有终端在软件、服务、端口、注册表、登录等多个维度上触发的安全策略违规事件，为管理员提供一套完整、可查、可溯的终端安全行为证据链。实现对全网终端合规性的透明化监控，满足内部审计与外部合规要求，并为安全事件调查、策略优化提供数据支撑。

①日期/时间筛选器

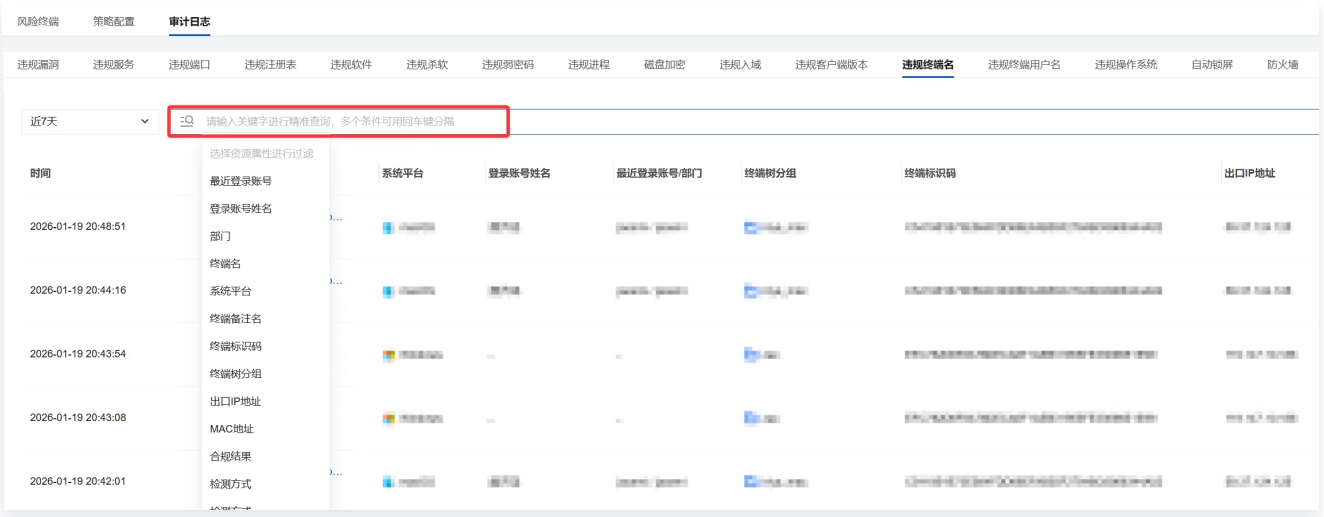
- 支持时间段筛选，提供标准时间筛选控件。
- 通过顶部左上角的 “近7天” 下拉选择框，您可以快速切换查看“今天”、“近7天” 、“近14天”、“近30天”、“自定义日期”等不同时间范围内的审计日志。



②基本搜索

- 关键字精准查询：在“请输入关键字进行精准查询”的搜索框内，您可以输入特定关键字（如：最近登录账号、部门、合规结果等），系统将筛选出包含此关键字的日志记录。

- 可搜索日志明细列表的所有字段。



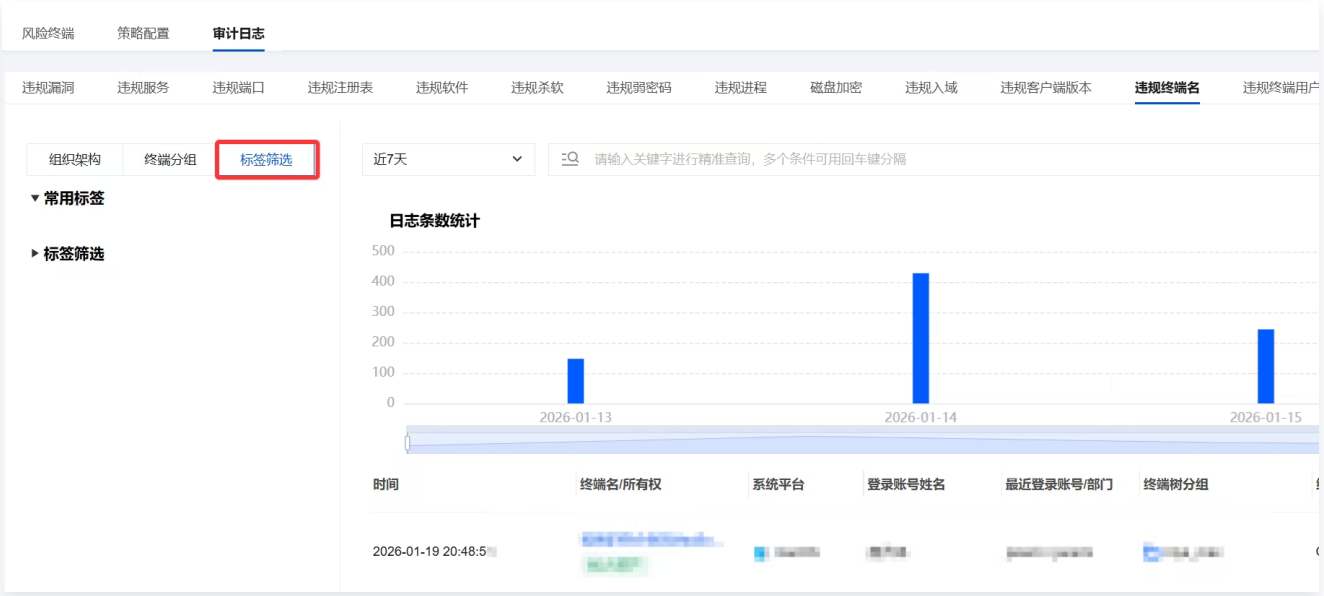
③日志条数统计

柱状图根据筛选周期展示日志条数，可左右滑动。



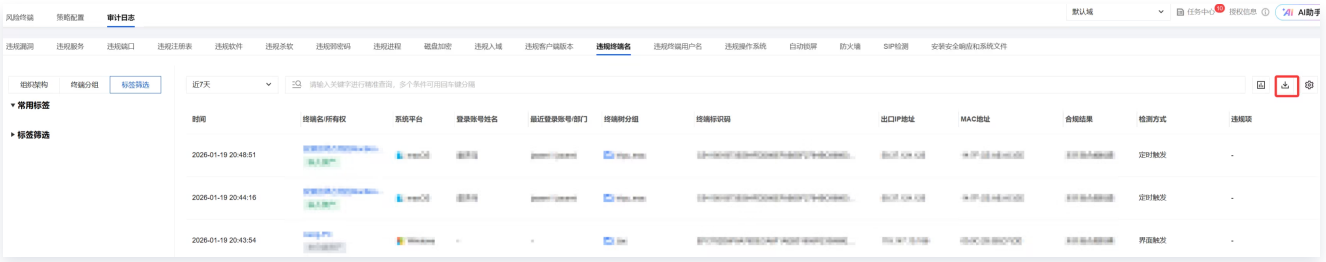
④筛选器

- 常用标签：日志字段的选项值（见具体日志）。固定标签，由后台确定，根据客户常见需求，提供快速筛选。
- 标签筛选：展示最近10个历史搜索记录。可变化标签，通过用户常用的检索工具，生成动态场景标签。



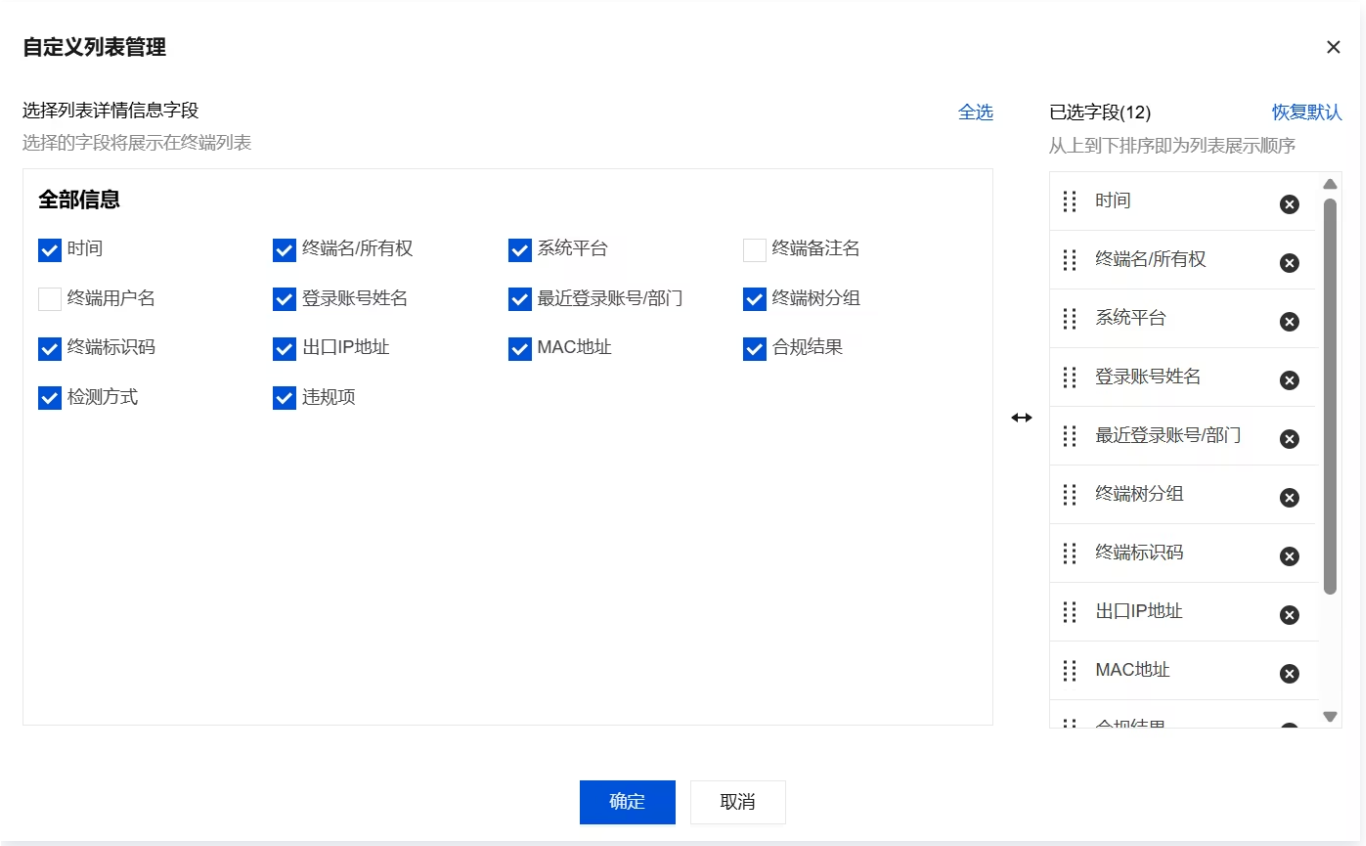
⑤日志导出

- 可选择导出字段：默认全选。
- 可选择日志导出时间：默认选择当前日志筛选时间。



⑥自定义表头

选择的字段将展示在列表字段中。



审计日志说明

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择 **审计日志**。
2. 在审计日志中，分为如下模块：

模块	日志名称	说明
合规检测审计日志	违规漏洞	展示终端违规漏洞的情况，关联：**终端管控** > **合规检测** > **策略配置** > **补丁列表**。

违规服务	展示终端违规服务的情况，关联：**终端管控 > 合规检测 > 策略配置 > 违规服务**。
违规端口	展示终端违规端口的情况，关联：**终端管控 > 合规检测 > 策略配置 > 违规端口**。
违规注册表	展示终端违规注册表的情况，关联：**终端管控 > 合规检测 > 策略配置 > 注册表**。
违规软件	展示终端违规软件的情况，关联：**终端管控 > 合规检测 > 策略配置 > 软件安全基线**。
违规杀软	展示终端违规杀软的情况，关联：**终端管控 > 合规检测 > 策略配置 > 第三方杀毒软件**。
违规弱密码	展示终端违规弱密码的情况，关联：**终端管控 > 合规检测 > 策略配置 > 弱密码**。
违规进程	展示终端违规进程的情况，关联：**终端管控 > 合规检测 > 策略配置 > 违规进程**。
磁盘加密	展示终端磁盘加密的情况，关联：**终端管控 > 合规检测 > 策略配置 > 磁盘加密**。
违规入域	展示终端违规入域的情况，关联：**终端管控 > 合规检测 > 策略配置 > 入域**。
违规客户端版本	展示终端违规客户端版本的情况，关联：**终端管控 > 合规检测 > 策略配置 > 客户端版本**。
违规终端名	展示终端违规终端名的情况，关联：**终端管控 > 合规检测 > 策略配置 > 终端名**。
违规用户名	展示终端违规用户名的情况，关联：**终端管控 > 合规检测 > 策略配置 > 终端用户名**。
违规操作系统	展示终端违规操作系统的情况，关联：**终端管控 > 合规检测 > 策略配置 > 操作系统**。
自动锁屏	展示终端自动锁屏的情况，关联：**终端管控 > 合规检测 > 策略配置 > 自动锁屏检测**。
防火墙	展示终端防火墙的情况，关联：**终端管控 > 合规检测 > 策略配置 > 防火墙**。
SIP检测	展示终端SIP检测的情况，关联：**终端管控 > 合规检测 > 策略配置 > 系统完整性（SIP）检测**。

	安装安全响应和系统文件	展示终端安装安全响应和系统文件的情况，关联：**终端管控 > 合规检测 > 策略配置 > 安装安全响应和系统文件检测** 。

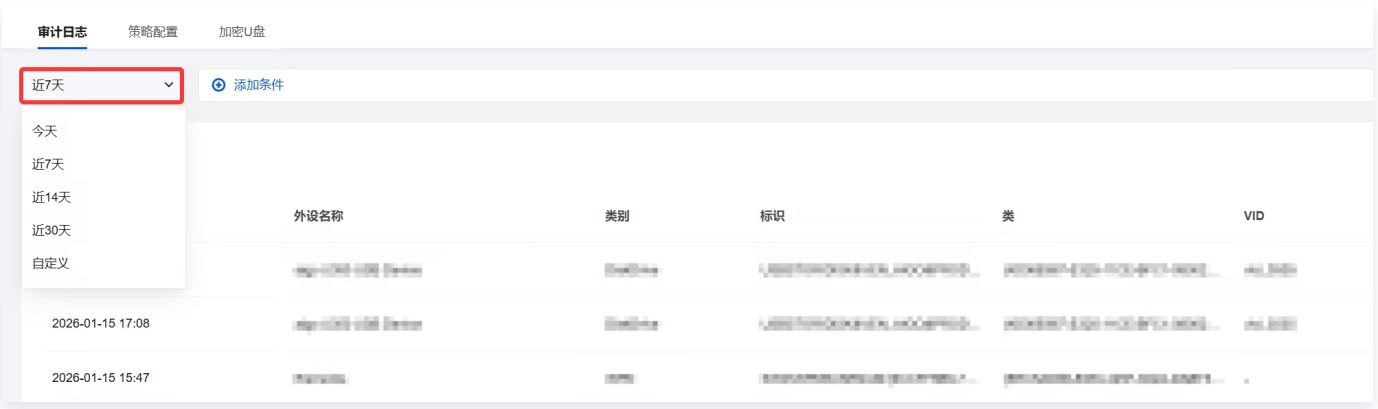
外设管控（11.1.1版）
外设管控审计日志（11.1.1版）

最近更新时间：2026-02-13 09:41:02

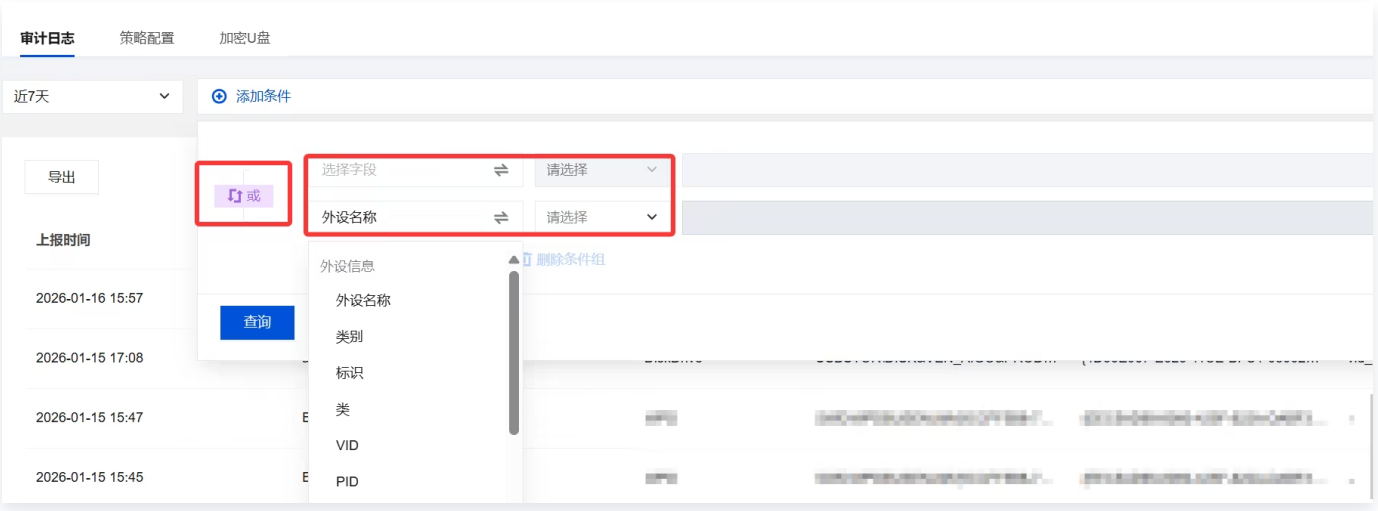
> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

用于记录、查询和导出终端用户近期的所有外设操作事件。通过此页面，管理员可查看 USB 设备等外设的使用情况，进行安全审计、事件追溯与合规性分析。

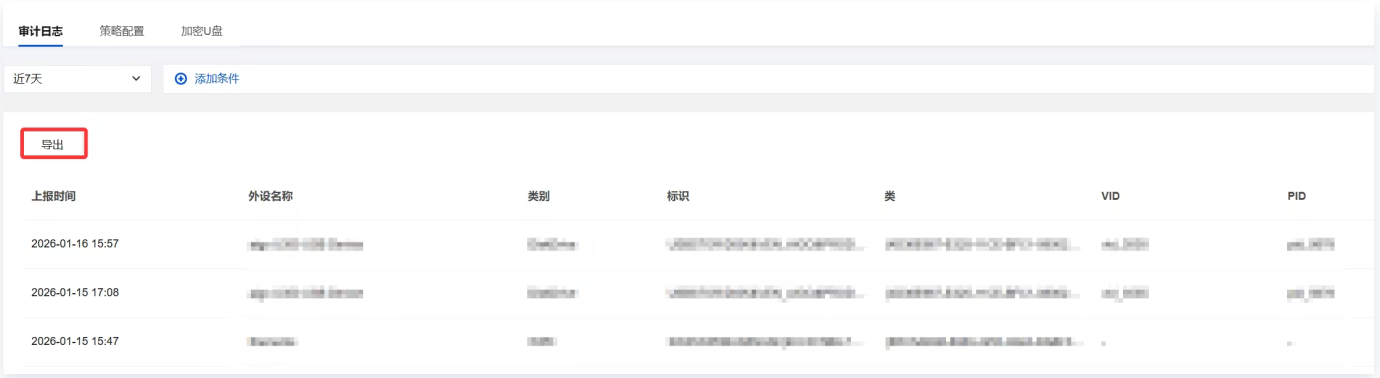
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **外设管控** > **审计日志**。
2. 支持时间段筛选，提供标准时间筛选控件：通过顶部左上角的 “近7天” 下拉选择框，您可以快速切换查看“今天”、“近7天”、“近14天”、“近30天”、“自定义日期”等不同时间范围内的审计日志。



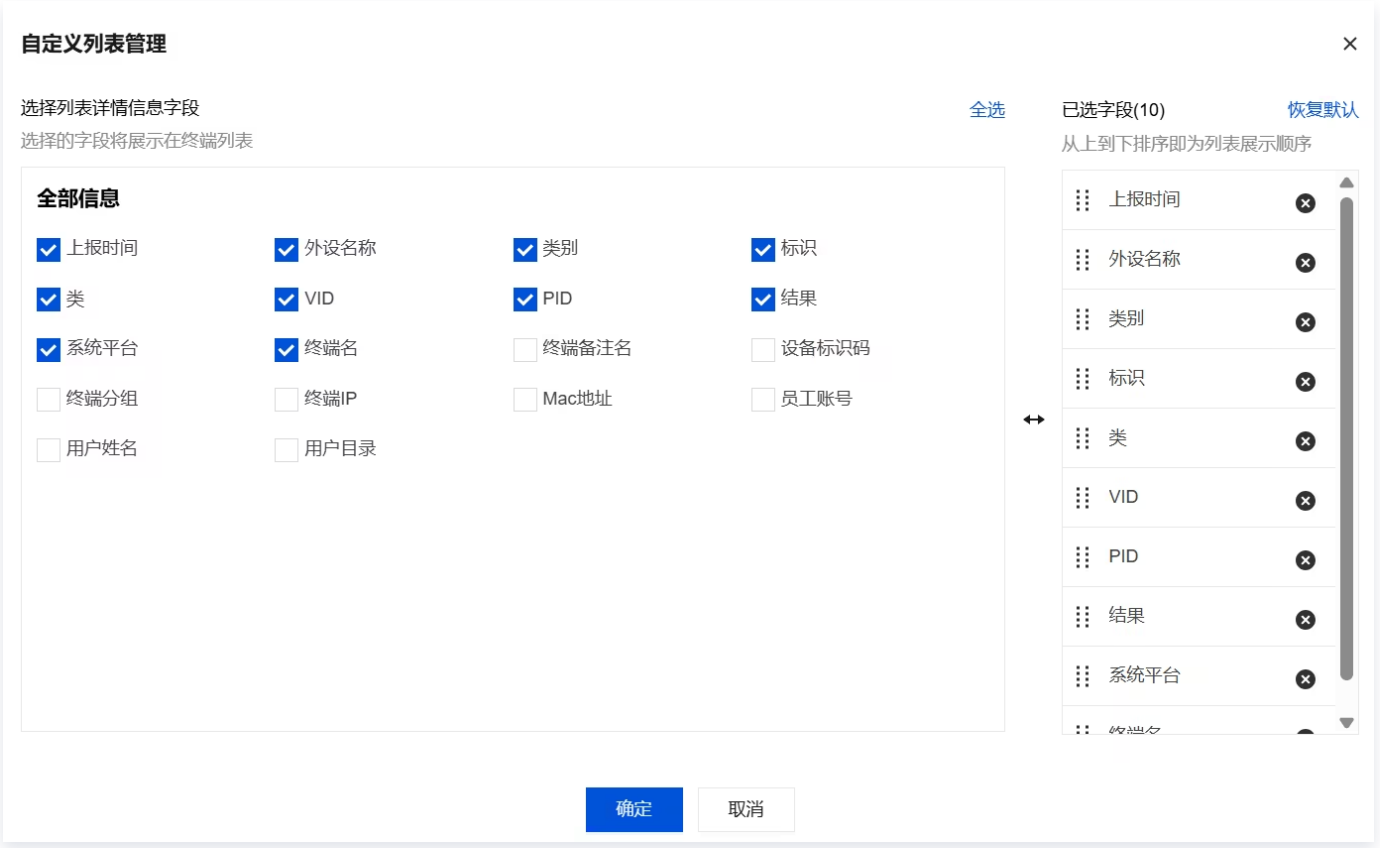
3. 支持多条件筛选，支持配置且/或关系筛选条件。



4. 可选择日志导出时间：默认选择当前日志筛选时间。



5. 单击 ☼，选择的字段将展示在列表字段中。

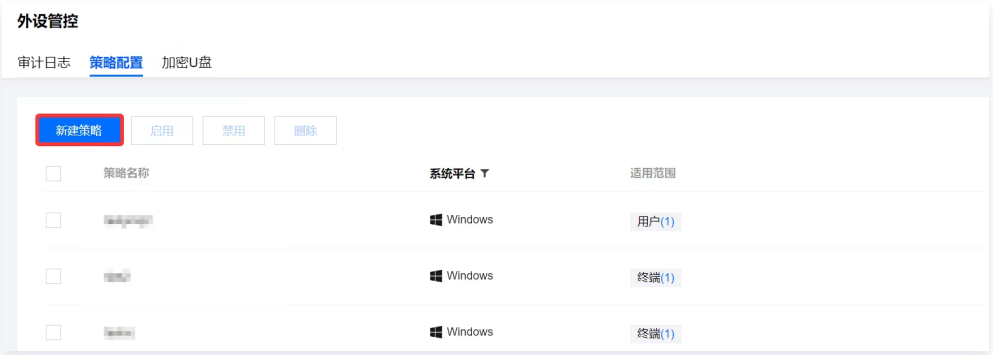


外设管控策略配置（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控 > 外设管控** 。
2. 在外设管控页面，选择 **策略配置** 。
3. 在策略配置页面，单击**新建策略**，配置相关参数。



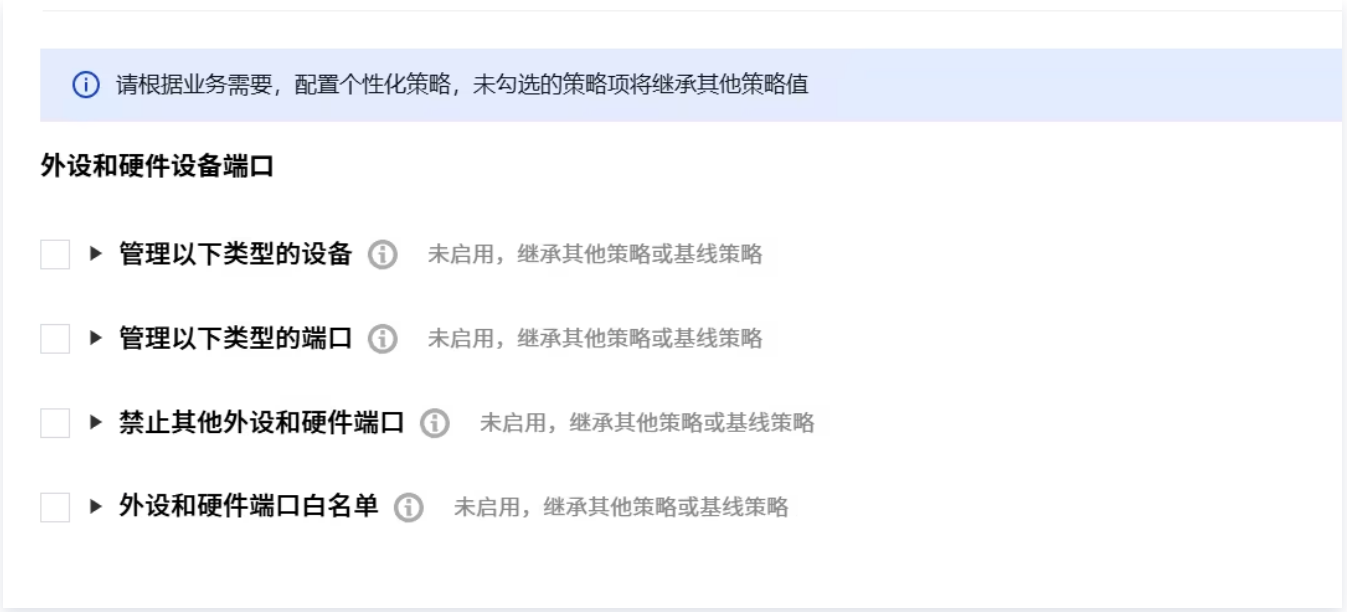
3.1 输入策略名称，并输入策略描述等参数。



3.2 单击**添加适用范围**，您可以通过添加或排除用户、组织架构、自定义用户组和终端，来进行精细化的管控范围设置。



4. 根据实际需求，勾选 管理以下类型的设备 、管理以下类型的端口 、禁止其他外设和硬件端口 、外设和硬件端口白名单 或 客户端手动安装外设和硬件设备端口策略描述文件，并配置相关参数，单击**保存**。

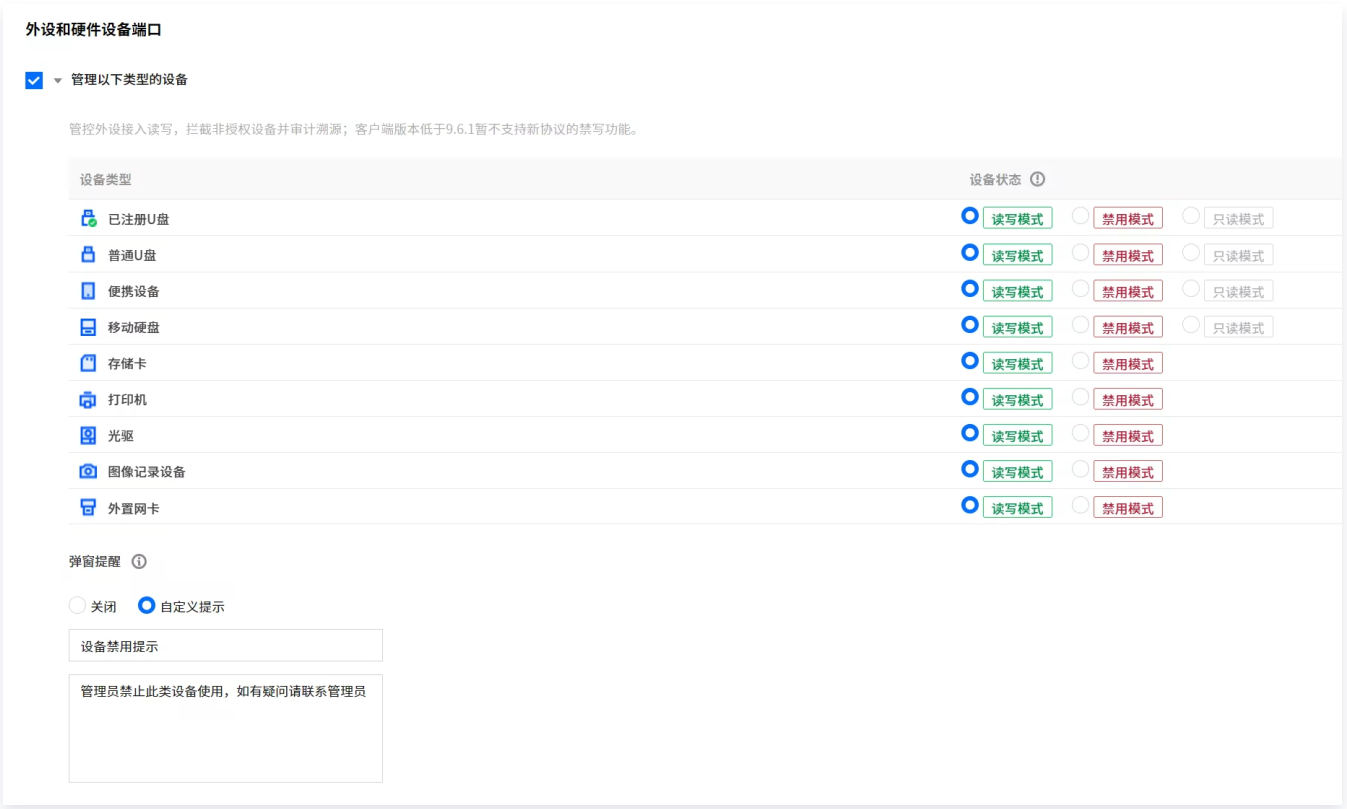


管理以下类型的设备

支持配置读写模式、禁用模式或只读模式。

- 读写模式：允许使用此设备，不对读写进行限制。
- 禁用模式：表示完全禁止使用，不允许外设插入电脑，无法读写该硬件设备。
- 只读模式：允许从外设设备中读取数据，让外设只能读取，这样可以禁止拷贝数据到这类外设上。

1. 勾选**管理以下类型的设备**，选择所需设备，**选择模式**。



说明：

> “已注册U盘”和“普通U盘”是互不干扰的，例如企业内只能使用“已注册U盘”，则可以禁用“普通U盘”，启用“已注册U盘”

2. 支持配置弹窗提示，支持自定义弹窗，策略配置完成单击**保存**。



3. 示例：配置禁用普通 U 盘并保存。



4. 策略下发后，当适用范围内的终端插入 U 盘，右下角弹出设备禁用提示。



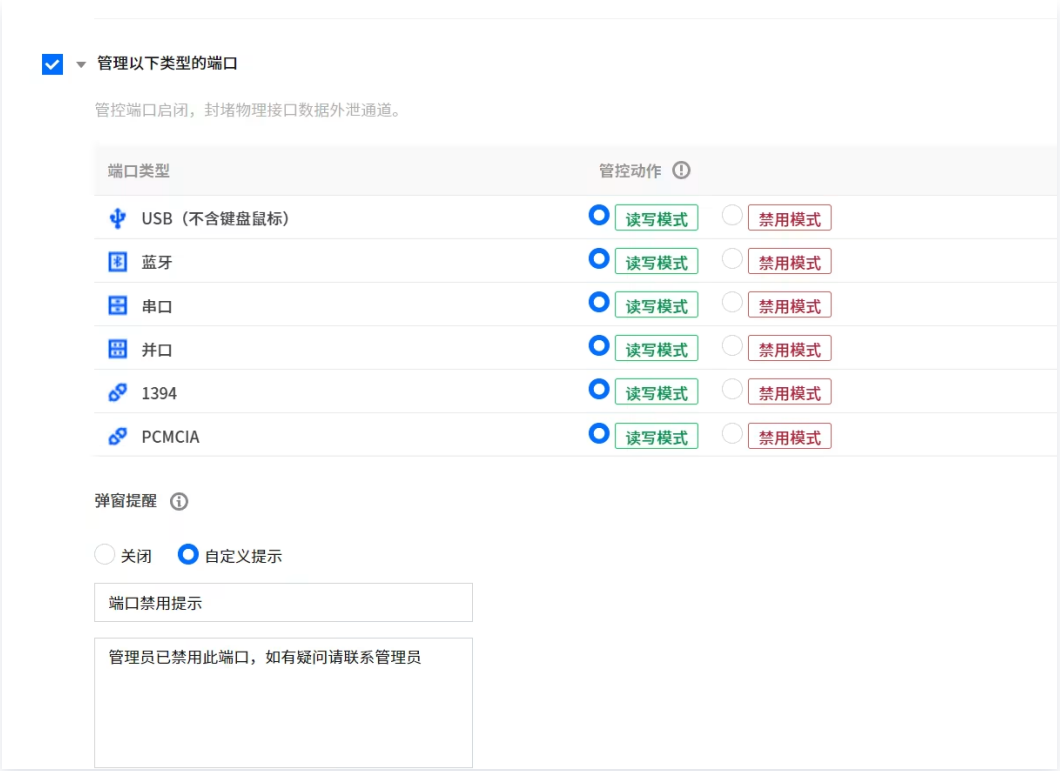
管理以下类型的端口

用来禁止或启用外部硬件端口。

> **说明：**
>
> - 读写模式：允许使用此设备，不对读写进行限制。
> - 禁用模式：表示完全禁止使用，不允许外设插入电脑，无法读写该硬件设备。

- USB 不会限制常见的鼠标和键盘设备。如果您使用了特殊的鼠标、键盘类 USB 接口，或蓝牙 USB 接口，可以通过 外设和硬件端口白名单放行策略来允许其使用。

1. 勾选**管理以下类型的端口**，选择所需端口，配置为读写或禁用模式。



2. 支持配置弹窗提示，支持自定义弹窗，策略配置完成单击**保存**。

禁止其他外设和硬件端口

说明：
禁止其他外设和硬件端口功能要求客户端版本10.11.1及以上支持该功能，如客户端版本低于10.11.1请升级客户端。

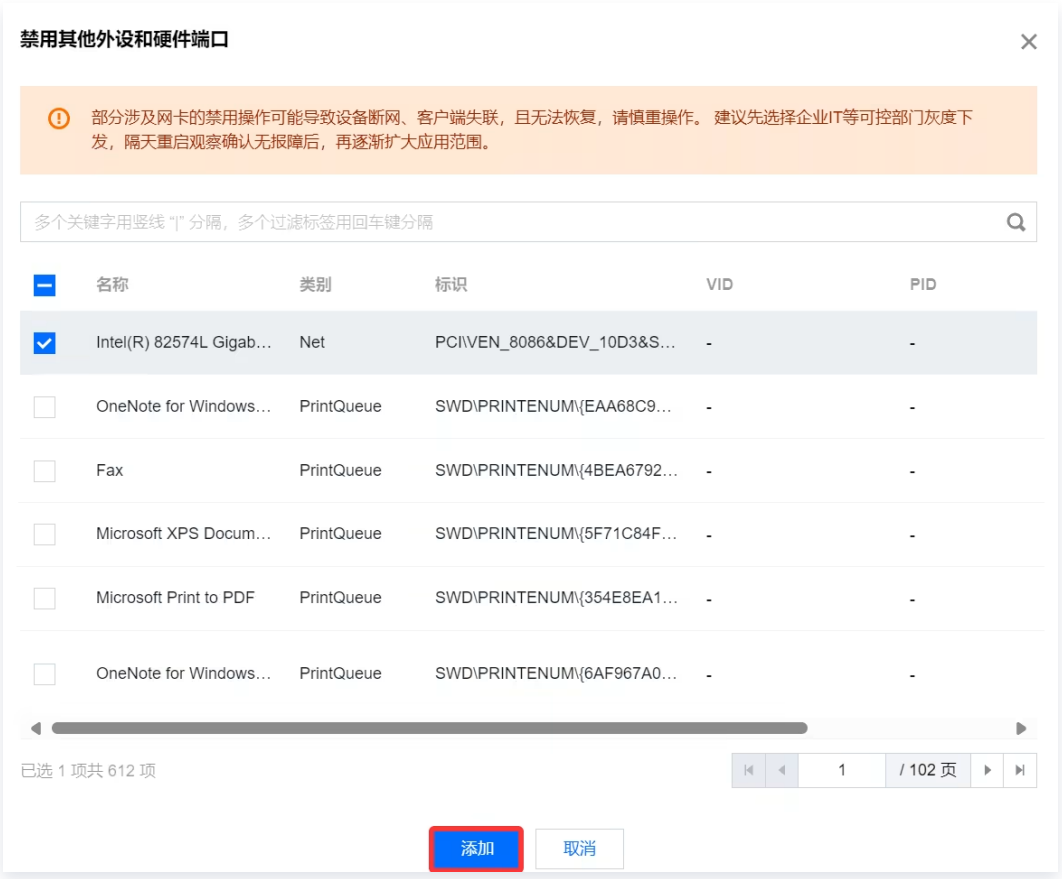
上报添加

禁用其他设备端口。通过遍历设备驱动来查找设备类型。如果已设置外设和端口的禁用，则无法使用此功能，可通过此处的硬件设备自定义禁用类型。

1. 单击**上报添加**，配置需禁止的外设和硬件端口。



2. 在禁用其他外设和硬件端口窗口中，选择所需设备，单击**添加**。



自定义添加

1. 自定义添加外设和硬件端口黑名单，单击**自定义添加**。



2. 支持按照名称、标识码识别唯一设备，支持添加通配符，支持批量添加，配置完成单击**保存**。



外设和硬件端口白名单

> **说明：**
> 外设和硬件端口白名单功能要求客户端版本10.11.1及以上支持该功能，如客户端版本低于10.11.1请升级客户端。

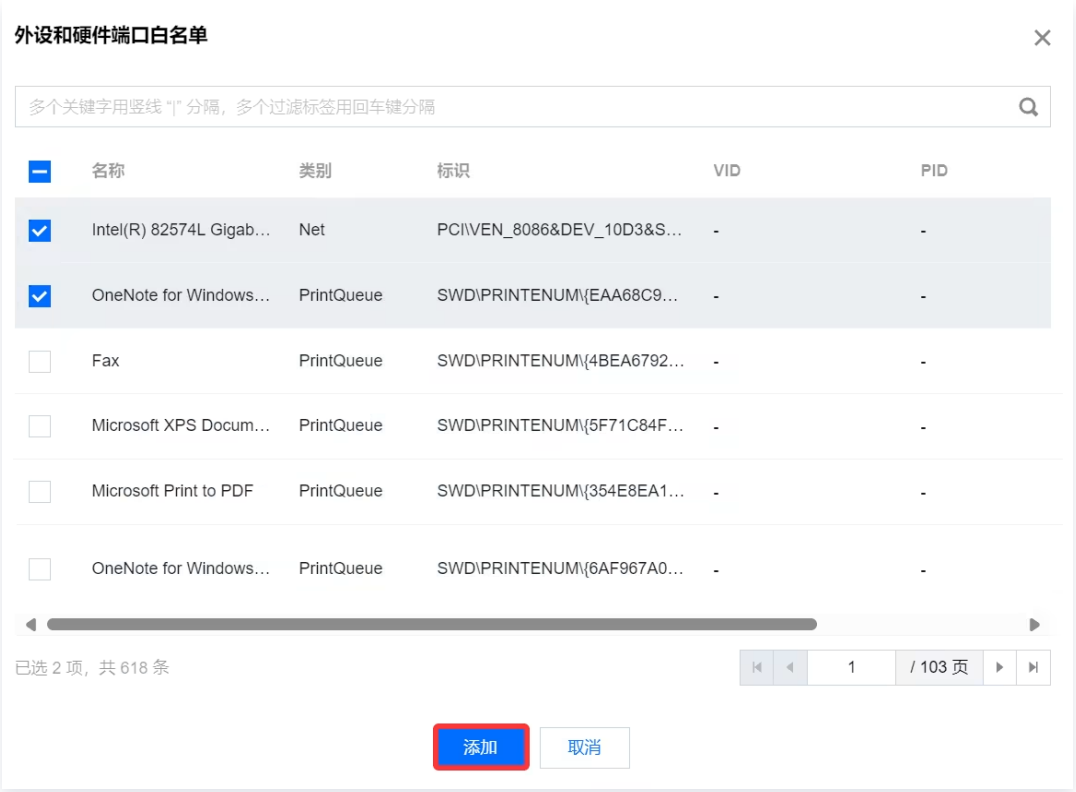
- 白名单放行策略，可以选择放行一些特殊设备，允许这类设备使用。例如：USB 接口类的设备、蓝牙接口类设备。
- U盘、移动硬盘等外接存储设备，通过“外设和硬件设备端口”策略禁用后，将不可使用，如有部分外设需要正常使用，可通过“外设和硬件端口白名单”进行加白处理。

上报添加

1. 单击**上报添加**，配置外设和硬件端口白名单。



2. 在外设和硬件端口白名单窗口中，选择所需设备，单击**添加**。



自定义添加

1. 自定义添加外设和硬件端口白名单，单击**自定义添加**。



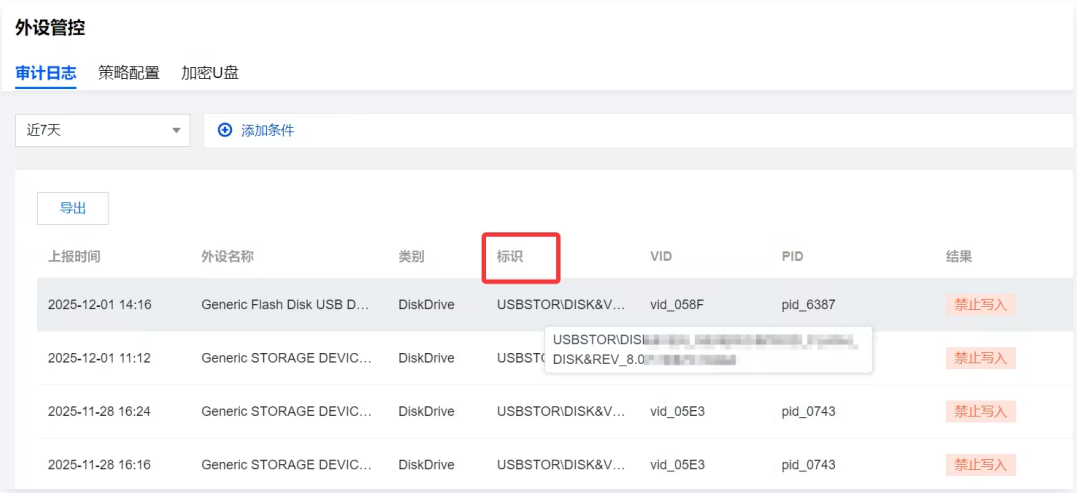
说明：

- 外设和硬件端口白名单仅能添加曾在安装 iOA 客户端的终端上插拔过的设备。
- 需要获取外设标识加白，您可以 通过审计日志中的标识路径加白，或者在计算机管理中 通过 VID 和 PID 加白。

方式1：通过审计日志中的标识路径加白

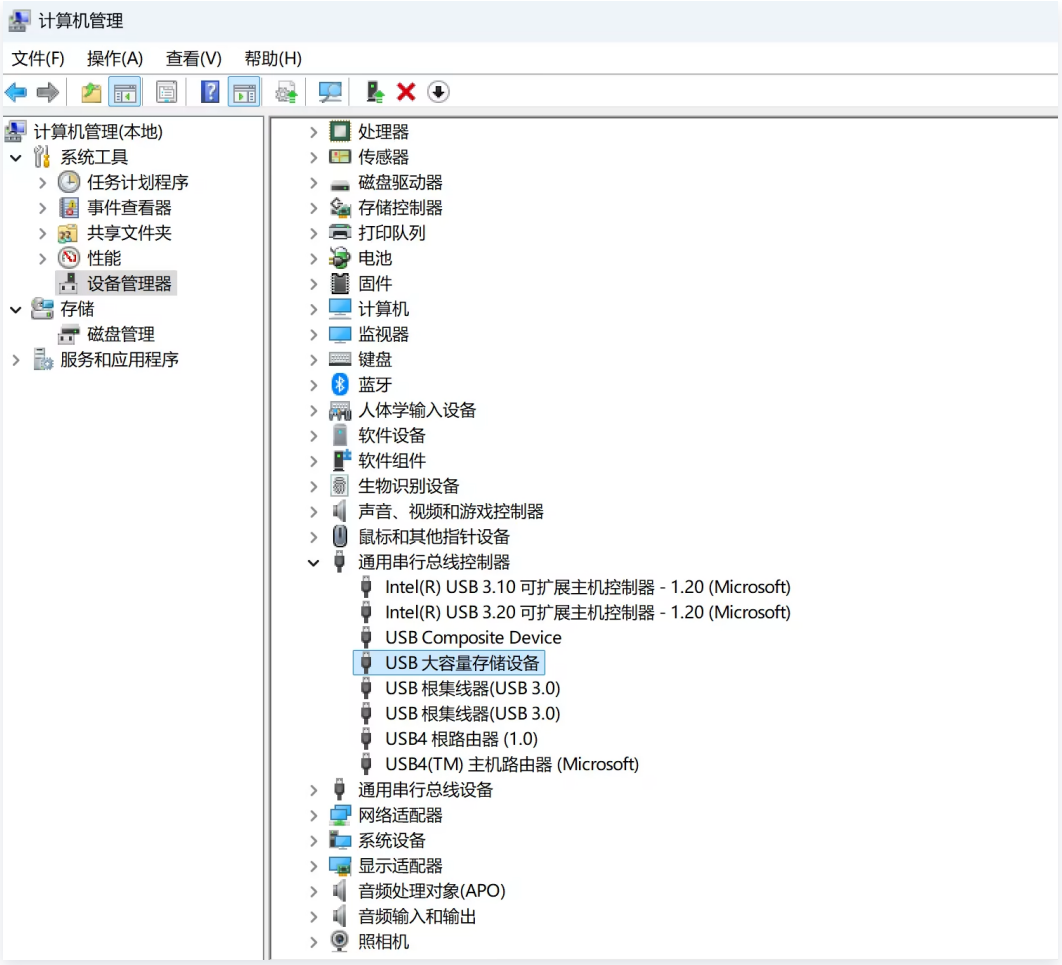
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **外设管控** > **审计日志**。
2. 在审计日志处，复制标识路径，获取厂商编号 VID 和产品编号 PID。

> **说明：**
> 复制的标识路径，厂商编号 VID 和产品编号 PID 将用于**策略配置** > **外设和硬件端口白名单**中。



方式2：在计算机上获取 VID 与 PID

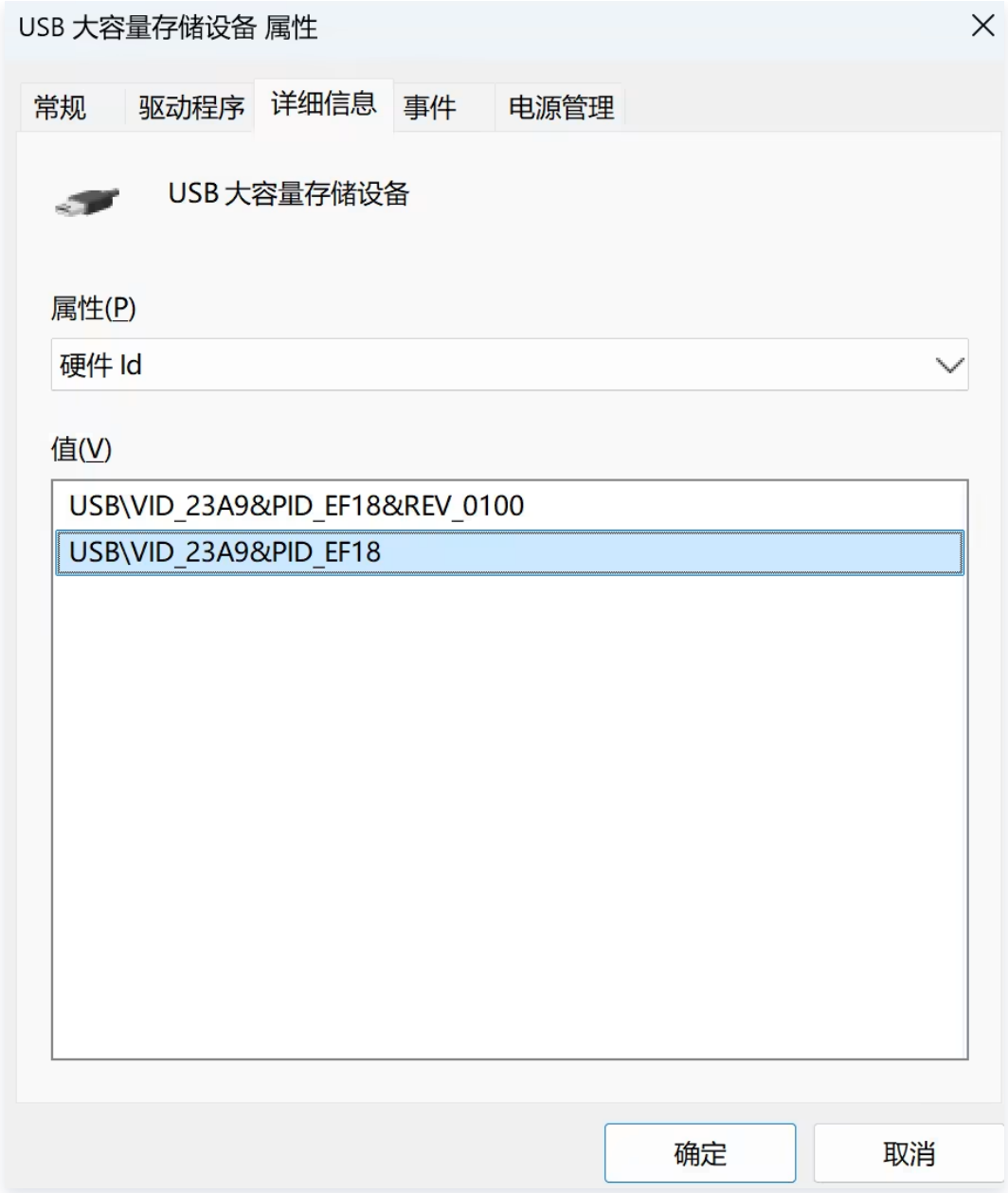
1. 打开**计算机管理** > **设备管理器**。



2. 插拔 U 盘，确定 U 盘设备，鼠标右键单击**属性**。

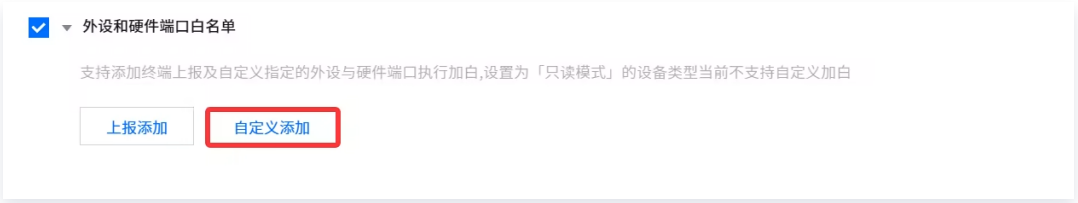


3. 在**详细信息** > **硬件 Id** 中，获取 VID、PID。



配置外设和硬件端口白名单

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **外设管控** > **策略配置**。
2. 单击**新建策略**，勾选外设和硬件端口白名单，单击**自定义添加**。



3. 粘贴获取的标识路径、VID、PID等信息，配置完成单击**保存**。



客户端手动安装外设和硬件设备端口策略描述文件

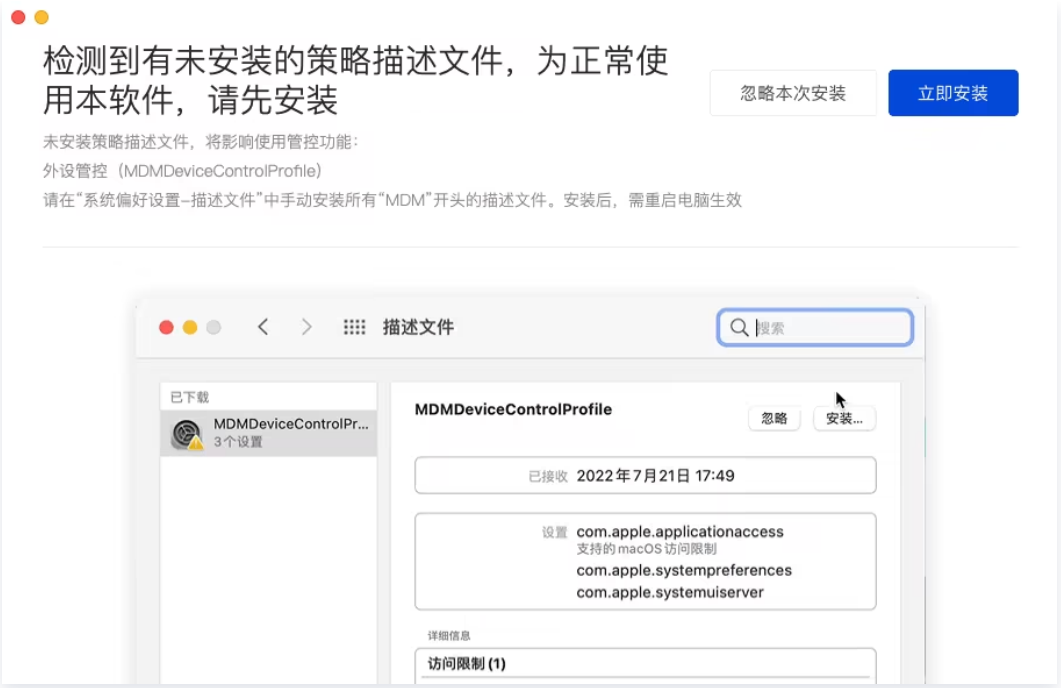
> **说明：**
> macOS 系统功能，Windows 下无此功能。

该功能允许管理员或终端用户在客户端手动安装外设和硬件设备端口的策略描述文件。策略描述文件用于定义外设和硬件端口的使用规则，例如限制某些设备的使用或配置端口的访问权限。管理员可以根据实际需求上传和安装相应的描述文件，以实施特定的外设管理策略。

1. 若已 配置MDM推送证书，则无需勾选；若未配置，请勾选**客户端手动安装外设和硬件设备端口策略描述文件**。



2. 勾选此策略后，系统下发一个策略描述文件给 iOA 客户端，单击**立即安装**此描述文件。



3. 当用户安装了新的策略描述文件后，终端需要重启才能使新策略生效。这是因为策略文件可能会影响系统底层的硬件配置和权限管理，而这些更改通常需要在系统启动时加载。在安装描述文件后及时重启终端，以保证策略的正确实施。
4. 如果未安装策略描述文件，终端将运行在默认配置下，可能无法对特定外设或硬件端口进行限制。

版权所有：腾讯云计算（北京）有限责任公司

加密U盘（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **外设管控** 。
2. 在外设管控页面，选择 **加密U盘** 。

> **说明：**
> iOA 基础版不支持加密 U 盘功能，该功能需 购买 终端安全专业版/远程接入专业版/高级版支持。

3. 展示所有已注册 U 盘的详细信息，管理员可对加密 U 盘进行启用或禁用操作。通过注册 U 盘，仅允许经过注册的 U 盘在企业内使用，保障企业数据安全。

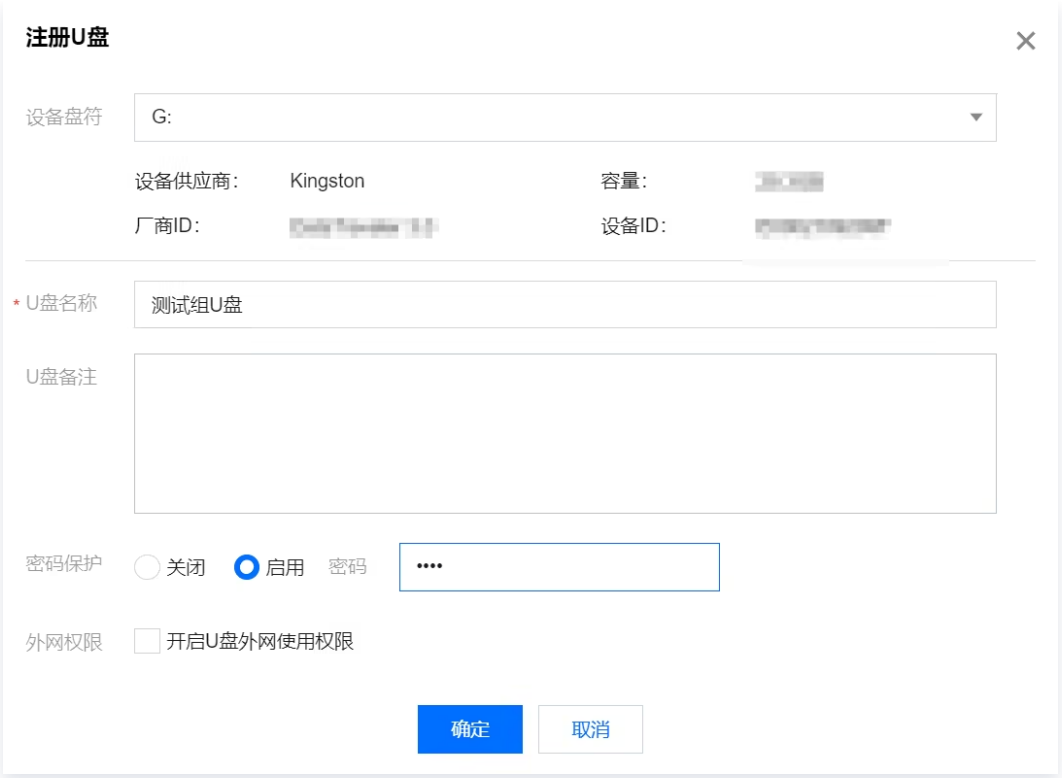


注册 U 盘

1. 将 U 盘插入终端，在 **加密U盘** 页面，单击**注册U盘**。



2. 配置注册U盘信息，配置完成单击**确定**保存。

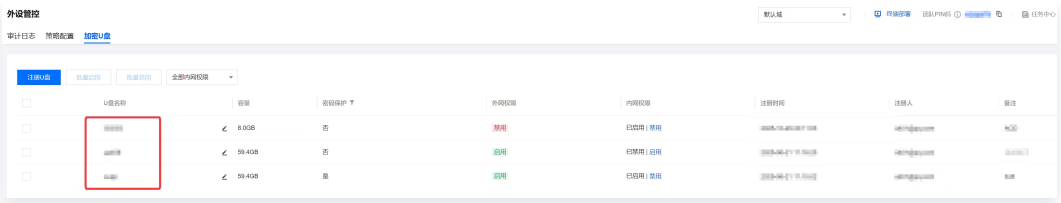


参数名称	说明
设备盘符	系统自动识别位于哪个盘符，识别 U 盘型号厂商。
U 盘名称	自定义。
U 盘备注	自定义。
密码保护	启用密码保护，启用后打开 U 盘需输入密码。
外网权限	• 可选择是否开启 U 盘外网权限。 • 开启后，将允许 U 盘在没有 iOA 或不同的 iOA 内网的环境中使用。 • 若关闭，无 iOA 环境或不同的 iOA 内网环境（连接同一控制中心）也将无法打开 U 盘。

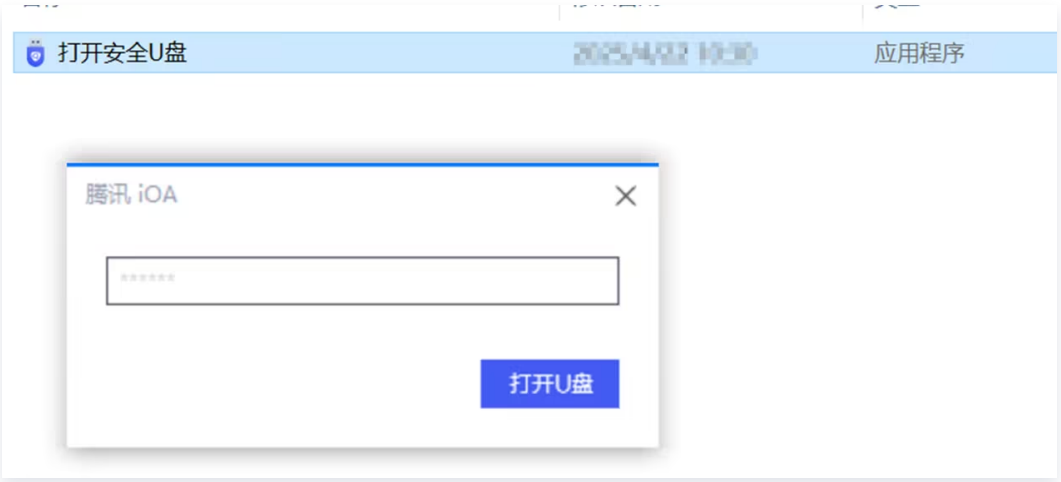
3. 注册 U 盘时提示注册 U 盘需先**格式化，将清除所有数据**，单击**确定**。



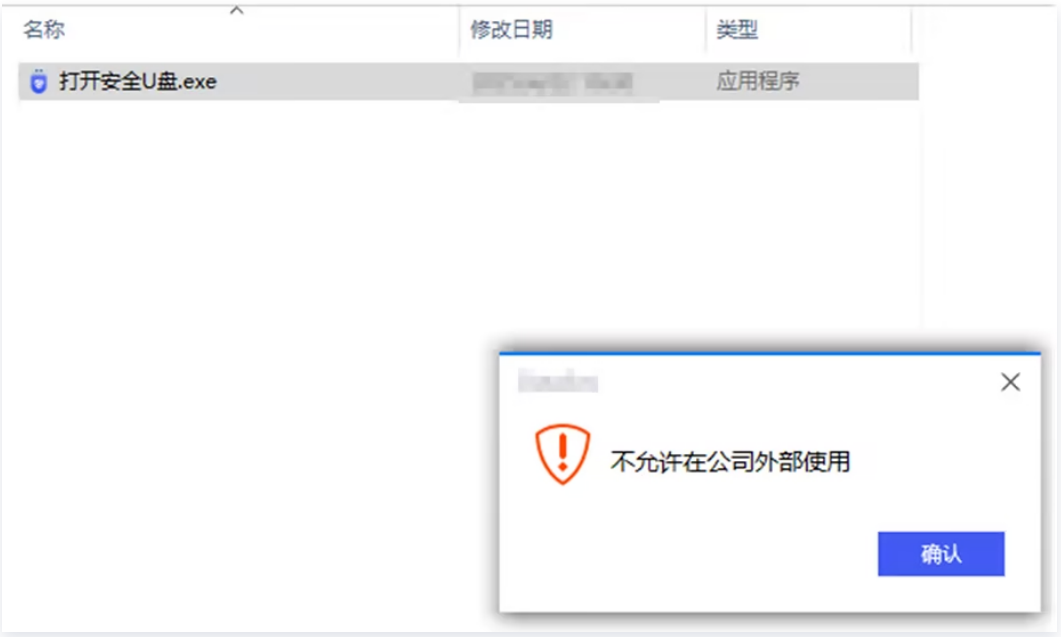
4. U 盘注册完成。



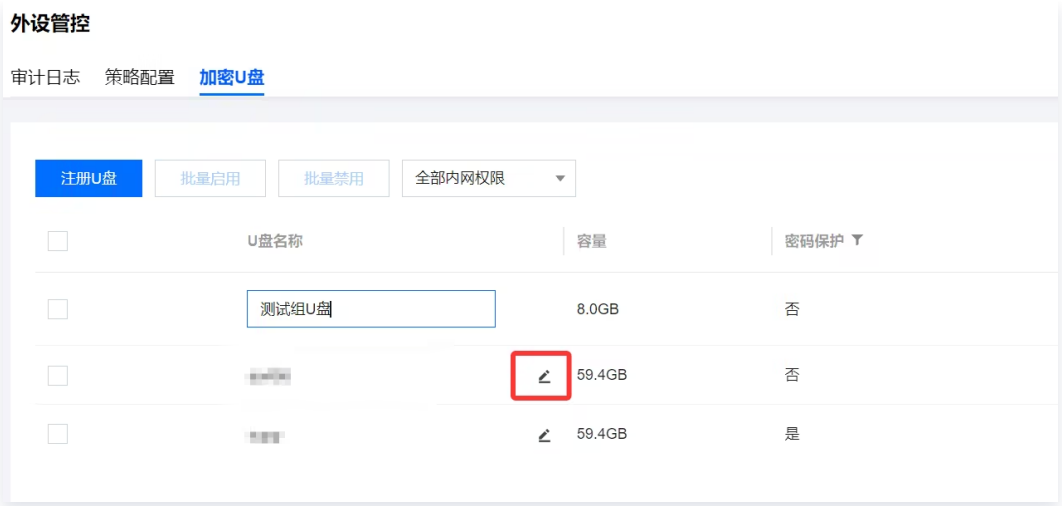
5. 终端插入该 U 盘，若设置了密码保护，打开需输入 U 盘密码。



6. 未开启 U 盘外网使用权限时，打开时将提示不允许在公司外部使用。



7. 支持修改 U 盘名称。



8. 支持修改内外网 U 盘使用权限。



取消注册 U 盘

如果用户不再希望已注册的 U 盘受到管控，可以随时取消注册。若注册 U 盘被人为异常格式化，将无法恢复原始存储空间大小，同时由于 U盘 中的"打开安全U盘.exe"文件被删除，将无法正常访问 U 盘内容。此时，需要联系管理员重新取消该 U 盘的注册。

> **注意：**
> 取消 U 盘注册将格式化 U 盘，并清除所有数据，请谨慎操作。

1. 管理员拿到 U 盘，插入终端，单击**取消注册**即可。



2. 取消注册过程，同样会格式化 U 盘。取消注册后，注册信息从当前列表删除，U 盘恢复成普通 U 盘。


该操作需格式化U盘，将清除所有数据，是否确定?
确定
取消

系统加固（11.1.1版）
系统加固审计日志（11.1.1版）

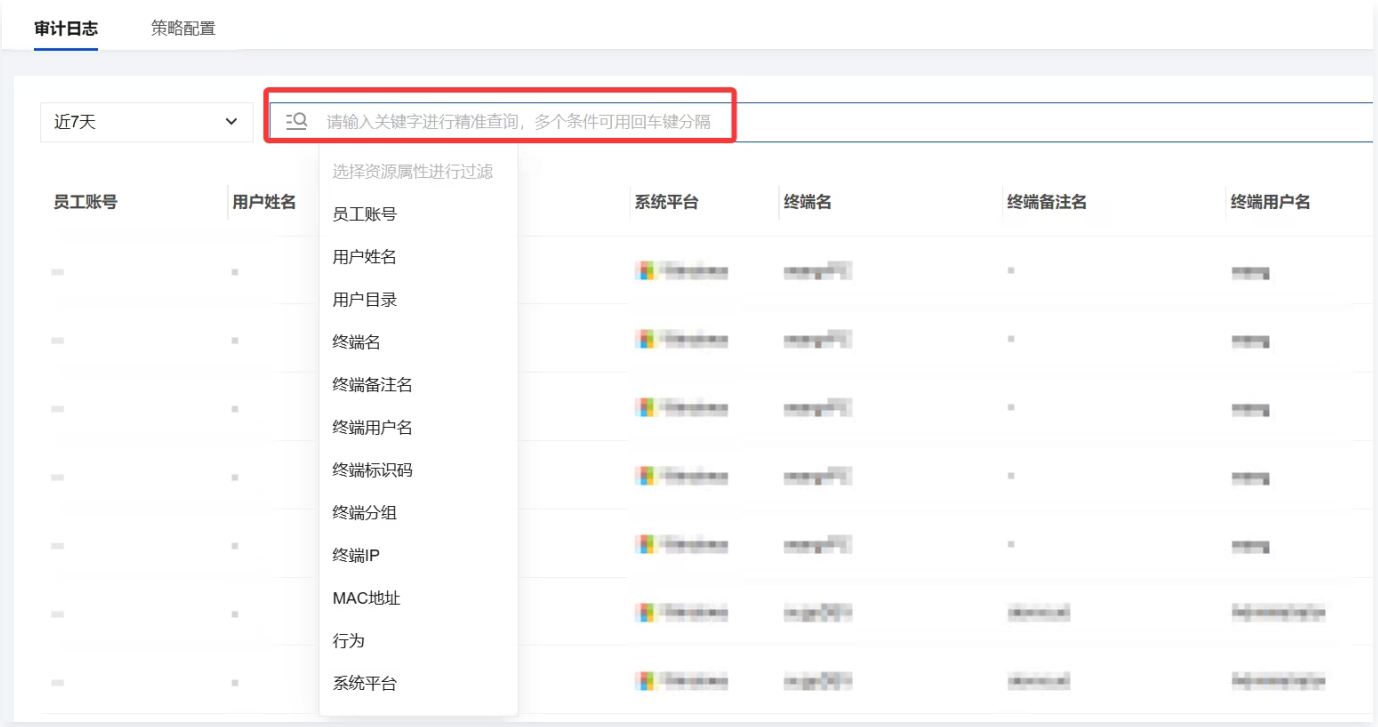
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

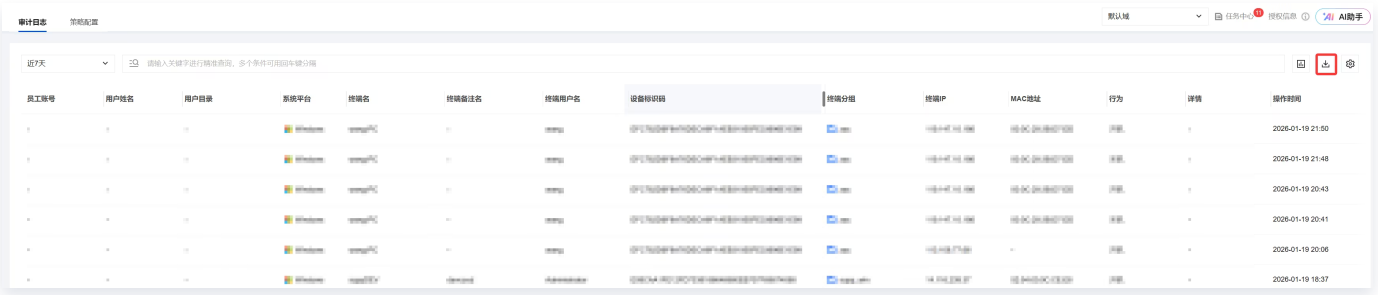
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **系统加固** > **审计日志**。
2. 支持时间段筛选，提供标准时间筛选控件：通过顶部左上角的 “近7天” 下拉选择框，您可以快速切换查看“今天”、“近7天”、“近14天”、“近30天”、“自定义日期”等不同时间范围内的审计日志。



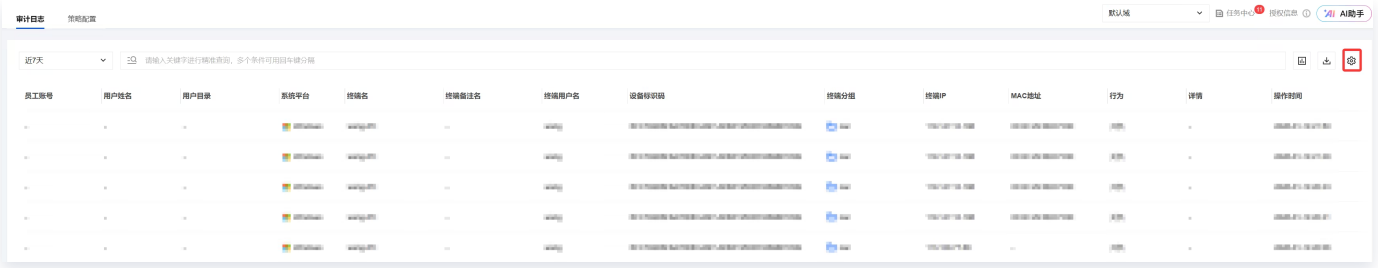
3. 关键字精准查询：在“请输入关键字进行精准查询”的搜索框内，您可以输入特定关键字（如：终端用户名、行为等），系统将筛选出包含此关键字的日志记录。



4. 可选择日志导出时间：默认选择当前日志筛选时间。



5. 单击 ，选择的字段将展示在列表字段中。

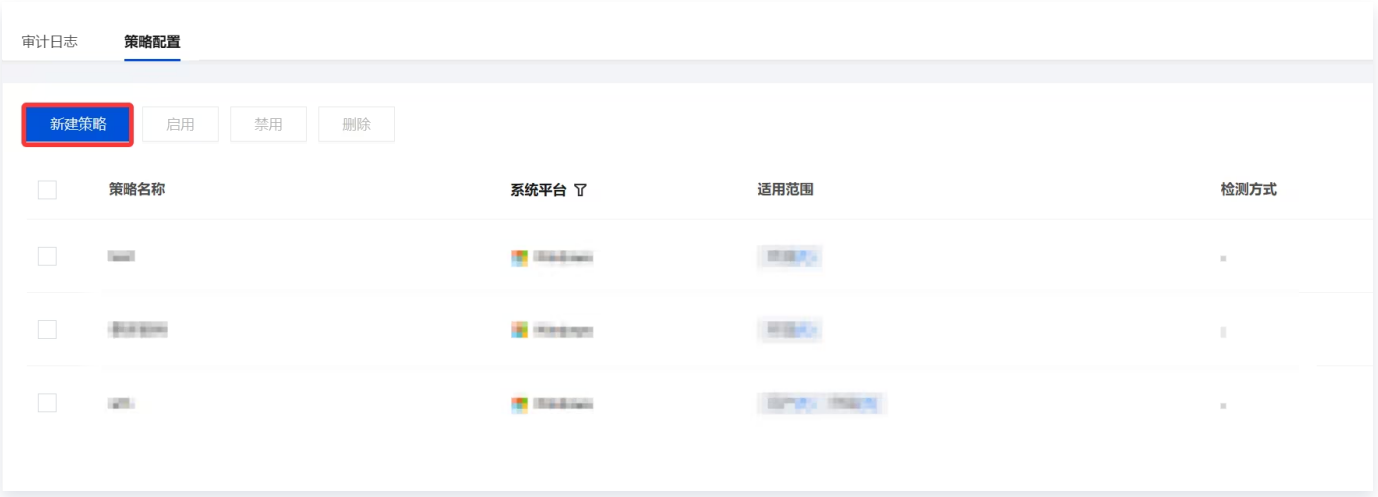


系统加固策略配置（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **系统加固**。
2. 在系统加固页面，选择**策略配置**，单击**新建策略**。



3. 在新建策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。



3.2 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。



4. 根据实际需求，选择如下**安全加固策略**，单击**保存**。

系统账号密码加固

1. 对终端配置加固策略，校验计算机系统账号密码长度、使用期限、复杂度等，以提升账号安全。
2. 勾选系统账号密码加固，开启加固，配置相关参数。



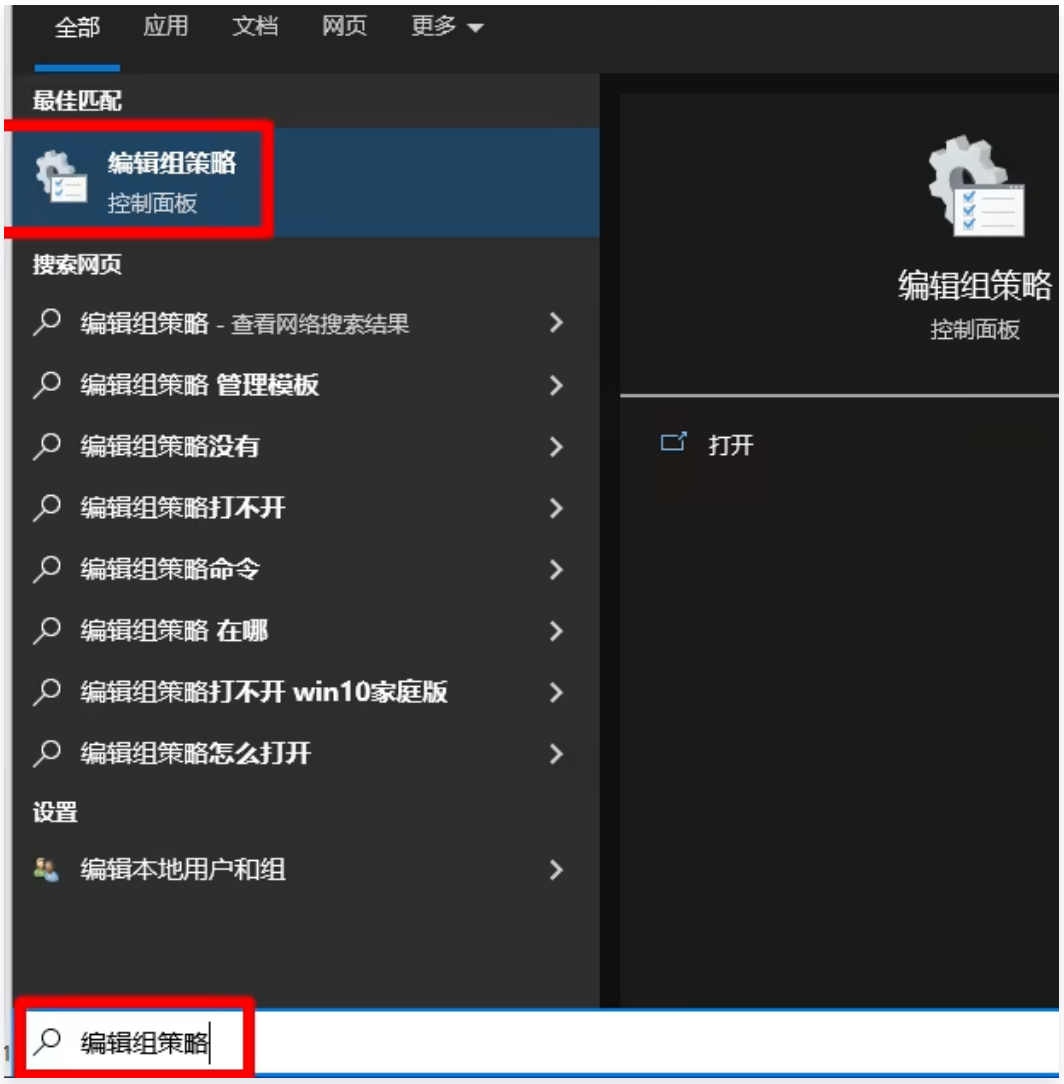
参数	说明
密码长度最小值	• win7系统密码长度最大值为14位。 • 若密码长度设置超过14位，win7系统客户端默认提取14位字符为密码（仅适用于非域账号）。 • 若密码长度设置为0，则密码长度不受限制并且可以设置为空密码。
密码使用有效期	• 若密码使用有效期设置大于0，则账号密码超过有效期后会强制要求用户修改密码。 • 若密码使用有效期设置为0，则账号密码永久有效不会强制用户进行修改。
强制密码历史	• 若强制密码历史设置大于0，则账号修改的新密码不能与对应数量的历史密码相同。 • 若强制密码历史设置为0，则账号修改的新密码可与任意历史密码相同。
账号锁定阈值	• 若账号锁定阈值大于0，则账号锁定时间必须大于或者等于本地组策略的重置时间。 • 若账号锁定时间设置为0，账号被锁定后保持锁定状态直至管理员手动解除。 **说明：** **可能存在第三方应用调用系统登录接口导致账号被锁定无法登录，请谨慎配置。**
账号锁定时间	• 若账号锁定阈值大于0，则账号锁定时间必须大于或者等于本地组策略的重置时间。 • 若账号锁定时间设置为0，账号被锁定后保持锁定状态直至管理员手动解除。

开启密码复杂性要求	如果启用此策略，密码必须符合下列最低要求。 • 不能包含用户的账号名，不能包含用户姓名中超过两个连续字符的部分； • 至少有六个字符长； • 包含以下四类字符中的三类字符：英文大写字母（A到Z）英文小写字母（a到z）10个基本数字（0到9）非字母字符（例如：！ ￥ # %）在更改或创建密码时执行复杂性要求。
禁用 Guest 账号	禁用 Guest 账号。

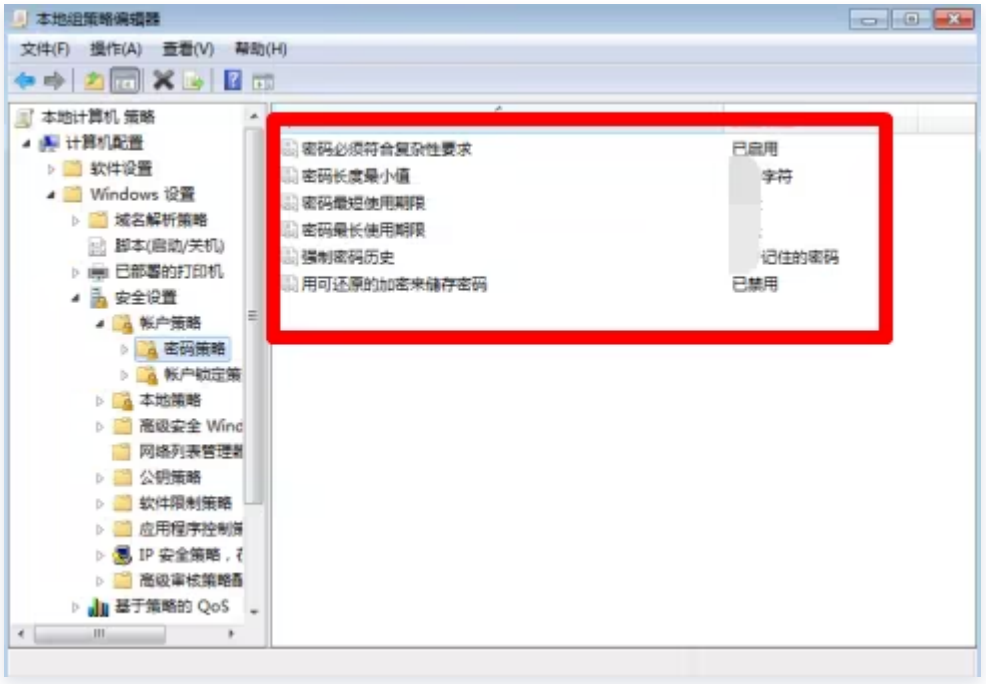
3. 配置完成后，单击**保存**。



4. 该分组下的终端机器上，通过“编辑组策略”查看账号密码状态。


全部
应用
文档
网页
更多
最佳匹配
编辑组策略
控制面板
搜索网页
编辑组策略 - 查看网络搜索结果
编辑组策略 管理模板
编辑组策略没有
编辑组策略打不开
编辑组策略命令
编辑组策略 在哪
编辑组策略打不开 win10家庭版
编辑组策略怎么打开
设置
编辑本地用户和组
编辑组策略
控制面板
打开
编辑组策略

5. 如下图所示：


本地组策略编辑器
文件(F)
操作(A)
查看(V)
帮助(H)
本地计算机 策略
计算机配置
软件设置
Windows 设置
域名解析策略
脚本(启动/关机)
已部署的打印机
安全设置
帐户策略
密码策略
本地策略
公钥策略
软件限制策略
基于策略的 QoS
密码必须符合复杂性要求 已启用
密码长度最小值 字符
密码最短使用期限
密码最长使用期限
强制密码历史 记住的密码
用可还原的加密来储存密码 已禁用

系统安全审计日志

1. 勾选系统安全审计日志，开启系统审计，配置相关参数。



2. 配置完成后，单击**保存**。



3. 该分组下的终端机器，系统审计日志达到事件日志最大时，按配置规则覆盖。

屏幕保护方式

1. 勾选屏幕保护方式，开启屏幕保护，配置相关参数。



2. 配置完成后，单击**保存**。



3. 该分组下的终端机器，屏幕保护时间会设置成**分钟。终端**分钟没有操作会进入屏幕保护模式，

若勾选恢复时需要密码登录，则再次操作需要密码认证才能登录桌面。

> **说明：**
> - 不勾选“恢复时需要密码登录”，这里就是息屏睡眠，触碰一下键盘等就会恢复桌面。
> - 勾选“恢复时需要密码登录”，这里就是锁屏睡眠（类似win窗口键+L键），触碰一下键盘等就需要输入开机密码，才能进入电脑桌面。
> - 勾选“恢复时需要密码登录”，需电脑有开机密码登录为前提。如果电脑本来就无密码，相当于不输入密码就可以进入系统，则勾选“恢复时需要密码登录”没有作用。

终端自动关机

1. 设置终端的自动关机时间。

参数名称	说明
允许空闲终端自动关机	• 启用该功能，管理员能够为终端设定空闲时间限制；当终端空闲时间超过限制时，终端将自动关机，方便管理员对无人值守或长期空闲的机器进行关机处理。 • 闲时定义：在设置时间内没有检测到键鼠流任何操作则会开始计时，视频播放及后台下载不会退出闲时状态。
终端定时关机	该功能适用于管理员对无人值守的终端进行自动关机处理。开启后，终端将根据策略在指定时间自动关机。
关机前是否提醒	• 开启时，在关机前 X 分钟对用户进行提示。 • 关闭时，将在不进行任何提示的情况下强制关机。

2. 配置终端自动关机规则，例如：



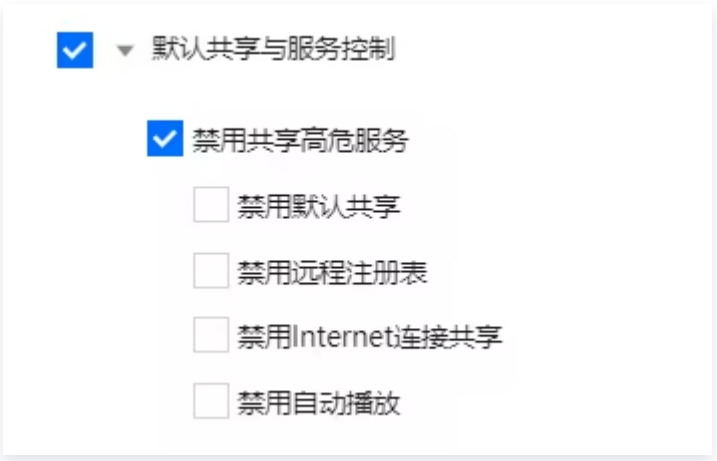
3. 配置完成后，单击**保存**。



4. 该分组下的终端机器，空闲时间超过24小时，会自动关机。

默认共享与服务控制

1. 管控客户端的共享和服务类不受侵入。
2. 勾选默认共享与服务控制，勾选禁用共享高危服务，配置相关参数。



参数	说明
禁用默认共享	该分组下的终端机器，会关闭默认共享。
禁用远程注册表	其他设备无法通过远程注册表的方式，进入终端机器。
禁用Internet连接共享	该分组下的终端机器，禁用 Internet 连接共享。
禁用自动播放	该分组下的终端机器，禁用自动播放 。例如：接入一个 U 盘，禁止自动播放运行。

3. 完成添加后，单击**保存**。



远程桌面端口

1. 设置终端机器的远程桌面端口。
2. 勾选远程桌面端口，勾选强制设定远程桌面端口，配置相关参数。

> **说明：**
> 如防火墙策略未放通将导致端口设置失败



3. 完成添加后，单击**保存**。

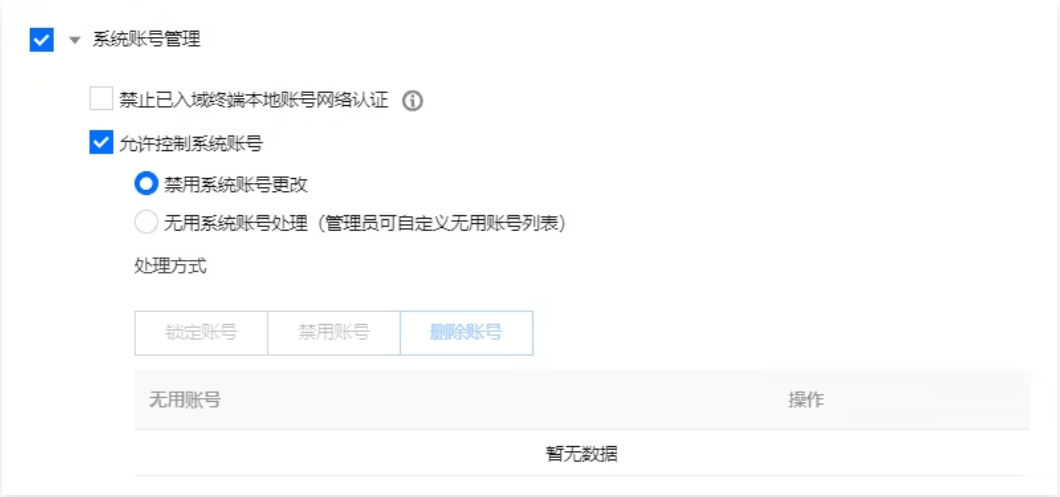


4. 如端口设置为8080，该分组下的终端机器，远程桌面端口会被设置为 8080，查看客户端 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumbe`

`r` 的键值是8080，且远程桌面功能正常。

系统账号管理

1. 勾选系统账号管理，配置相关参数。



参数	说明
禁止已入域终端本地账号网络认证	支持禁止已入域终端本地账号网络认证，可防止终端由于密码泄露导致的大面积终端失陷。

允许控制系统账号	• 允许控制系统账号，配置系统账号管理规则。
	• 禁用系统账号更改：管理系统账号不被随意篡改。
	• 无用系统账号处理（管理员可自定义无用账号列表）。
	  ○ 锁定账号。
	  ○ 禁用账号。
	  ○ 删除账号。

2. 完成添加后，单击**保存**。



域账号登录控制

1. 客户端非域账号登录提示和注销。
2. 勾选域账号登录控制，勾选仅允许域账号登录系统，配置相关参数。



参数	说明
非域账号登录时弹框提醒注销	• 如果终端机器没有入域，则规则不生效（不管是不是域账号都不受影响）。 • 如果是用域账号登录的 PC，则不受影响。 • 如果是用非域账号登录的 PC，则会弹窗提醒注销。 • 弹窗内容支持自定义。
非域账号登录时弹窗提示并自动注销	• 如果终端机器没有入域，则规则不生效（不管是不是域账号都不受影响）。 • 如果是用域账号登录的 PC，则不受影响。 • 如果是用非域账号登录的 PC，则会弹窗提示当前系统登录账号为本地账号，非域账号，限定时间后注销当前账号，请及时保留数据! 并且会在** 分钟后自动注销。 • 弹窗内容支持自定义。

3. 完成添加后，单击**保存**。



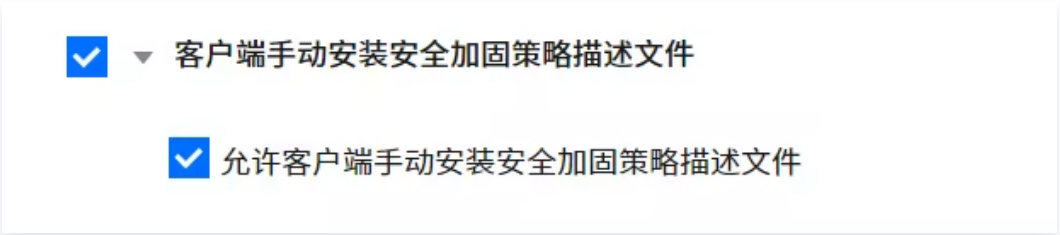
客户端手动安装安全加固策略描述文件

说明：

- macOS 系统功能，Windows 下无此功能。

- 需要配置 MDM 文件后该策略才会生效，描述文件安装后，需重启终端。
- MDM 文件支持自动下发或客户端手动安装安全加固策略描述文件。

1. 勾选此策略后，直接策略下发客户端拉取描述文件，无需配置 MDM 证书。



2. 进入系统，搜索描述文件，选择 MDMEAP 双击鼠标左键，手动安装安全加固策略描述文件。

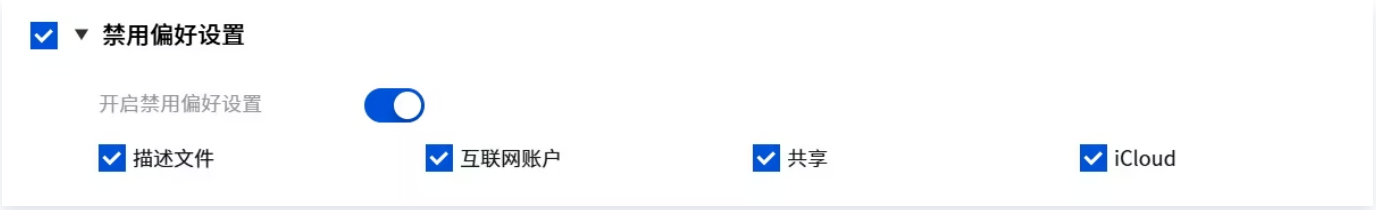


禁用偏好设置

说明：

- macOS 系统功能，Windows 下无此功能。
- 需要配置 MDM 文件后策略生效，描述文件安装后，需重启终端。

1. 勾选此策略并下发客户端收到策略后，描述文件、互联网账户、共享、iCloud，被禁用无法使用。



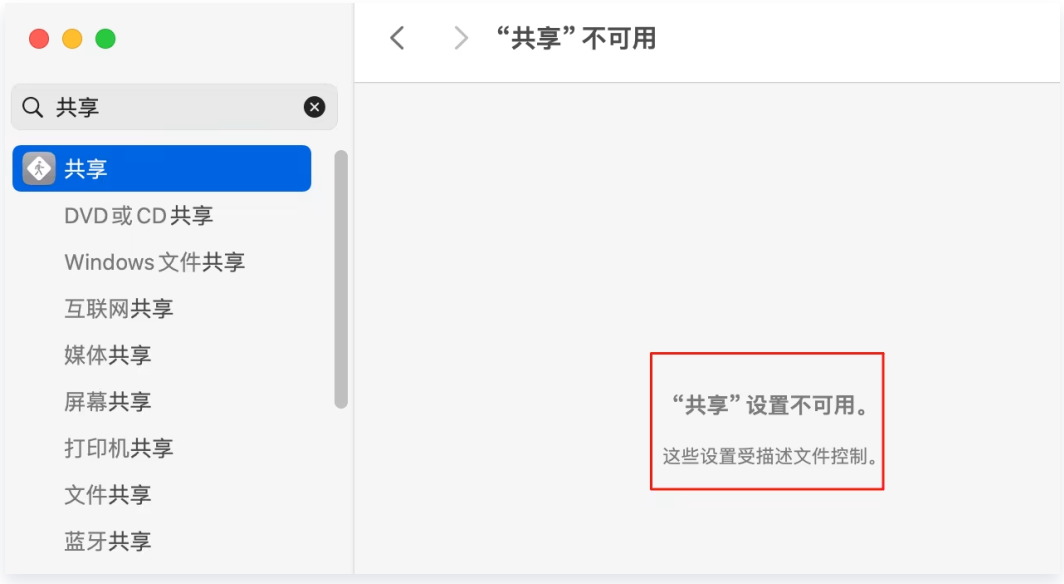
2. 描述文件：在电脑搜索描述文件，提示“描述文件”设置不可用。



3. 互联网账户：在电脑搜索互联网账户，提示“互联网账户”设置不可用。



4. 共享：在电脑搜索共享，提示“共享”设置不可用。



5. iCloud：在电脑搜索 iCloud，提示“登录”设置不可用。



禁用共享服务

说明：

- macOS 系统功能，Windows 下无此功能。
- 需要配置 MDM 文件后策略生效，描述文件安装后，需重启终端。

1. 勾选此策略并下发，终端收到策略后，勾选的共享服务将被禁用。



2. 禁用前电脑支持共享功能。



3. 禁用后无法使用共享功能（单击共享后，仅展示信息、提醒事项、编辑扩展...）。

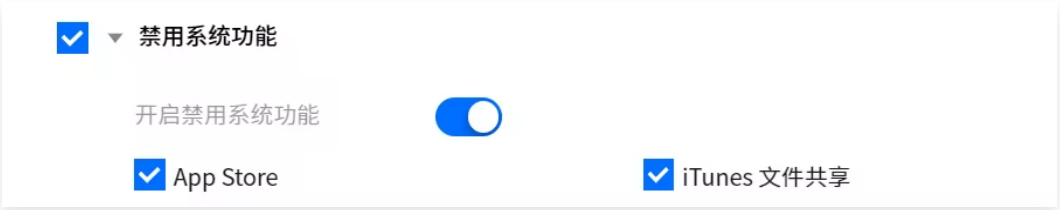


禁用系统功能

> **说明：**

- macOS 系统功能，Windows 下无此功能。
- 需要配置 MDM 文件后策略生效，描述文件安装后，需重启终端。

1. 勾选此策略并下发客户端收到策略后，勾选的系统功能将被禁用。



2. App Store：在电脑打开App Store，提示无权使用。



3. iTunes 文件共享：在电脑打开 iTunes，提示无权使用。

防火墙管控（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

禁止不必要的网络端口的入站或出站流量，收敛端口暴露面，减小被攻击的概率。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控 > 防火墙管控**，单击**新建策略**。



2. 在新建策略页面，配置相关参数。

   2.1 输入策略名称，并输入策略描述等参数。



2.2 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。

3. 根据实际需求，选择如下**策略**，单击**保存**。

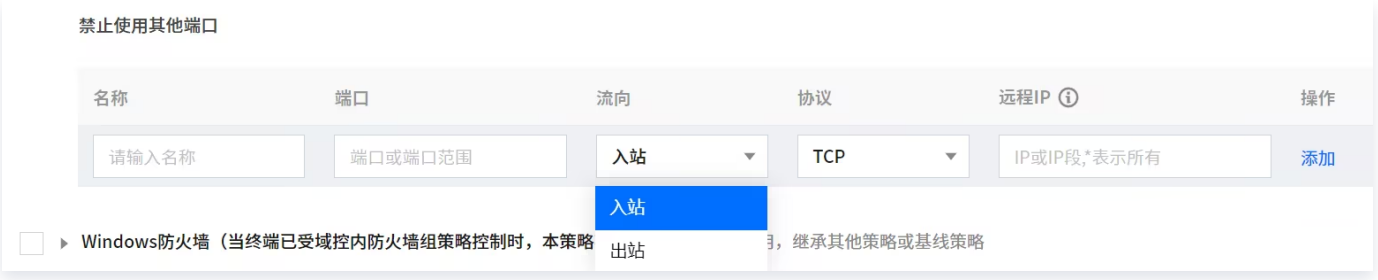
禁止使用以下端口

1. 勾选禁止使用以下端口，根据管控需求，勾选端口号。

> **说明：**
> 请保持 iOA 终端系统上 Windows 网络防火墙开启，否则功能将失效（利用了 Windows 网络防火墙机制）。



2. 支持自定义配置禁止使用其他端口，用于禁止 iOA 终端上网络端口的入站或出站流量，禁用一些特殊网络服务。



参数	说明
名称	自定义名称。
端口号	支持填写单个端口（例如：6666），或端口范围（例如：7777-7788）。

流向	• 入站，表示进入 iOA 终端的流量。 • 出站，表示从 iOA 终端出去的流量。
协议	支持选择 TCP 或 UDP 协议，分别设置禁用策略。
远程 IP	请输入IP或者IP段，*表示所有，IP段用-连接，多个IP段用英文逗号连接。如: 1.2.3.4-1.2.3.10

Windows 防火墙

根据管控要求，对终端配置防火墙开、关策略。

> **说明：**
> 当终端已受域控内防火墙组策略控制时，本策略不生效（入域的终端配置此策略不生效）。

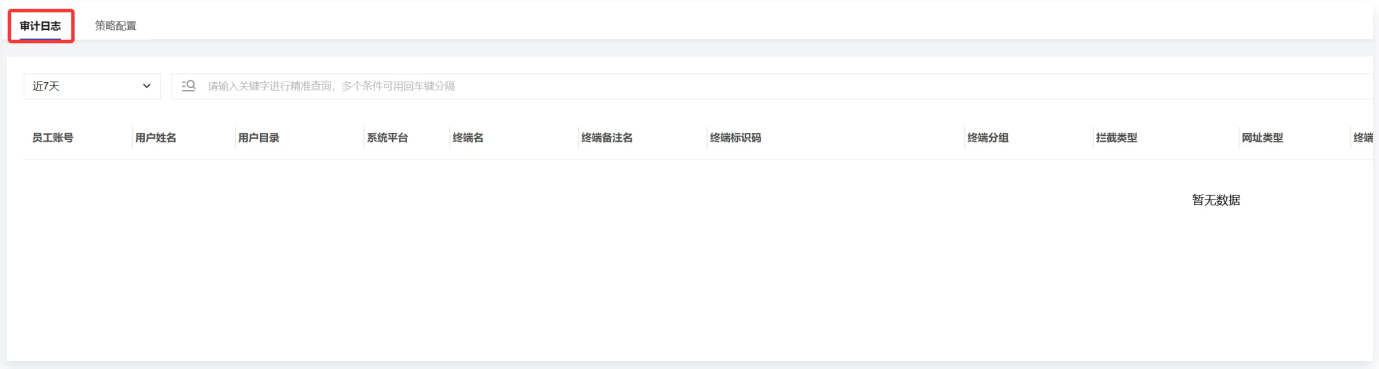


上网行为管控（11.1.1版）
上网行为管控审计日志（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **上网行为管控** > **审计日志**。
2. 在**上网行为管控** > **策略配置**中配置的上网拦截策略，上报的拦截报警日志在此展示。



3. 支持时间段筛选，提供标准时间筛选控件：通过顶部左上角的 “近7天” 下拉选择框，您可以快速切换查看“今天”、“近7天”、“近14天”、“近30天”、“自定义日期”等不同时间范围内的审计日志。



上网行为管控策略配置（11.1.1版）
上网拦截（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

管理员可根据需求，限制终端访问指定站点，并采集终端访问黑、白名单站点信息。上网拦截场景（例如：上班时间不允许访问与工作无关的网站），支持设备网络强管控场景（禁止设备访问任何网络，在保证设备基本正常网络通信的情况下，仅允许访问指定网址或资源，确保设备的安全性）。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **上网行为管控** > **策略配置**。
2. 在策略配置页面，单击**新建策略**。
   2.1 输入策略名称，并输入策略描述等参数。



   2.2 单击**添加适用范围**，您可以通过添加或排除用户、组织架构、自定义用户组和终端，来进行精细化的管控范围设置。



3. 根据实际需求，勾选**上网拦截**，并选择拦截方式：不拦截、Host 地址控制 、进程控制 、Host 地址和进程控制 ，并配置相关参数，单击**保存**。

Host 地址控制

1. 在**策略配置** > **新建策略**页面，勾选**上网拦截**，拦截方式选择 **Host 地址控制**。
2. 选择**控制类型**并设置所需的 Host，支持自定义和使用内置 Host。

> **说明：**
> - 黑名单：下发策略的终端，不能访问配置的黑名单站点，其他站点访问不受影响。
> - 白名单：下发策略的终端，只能访问配置的白名单站点，其他站点无法访问。
> - Host 地址控制拦截规则支持配置 UDP 协议。
> - 本文以设置黑名单为示例。



- 单击**添加自定义**，输入 Host 信息，单击**确定**保存。

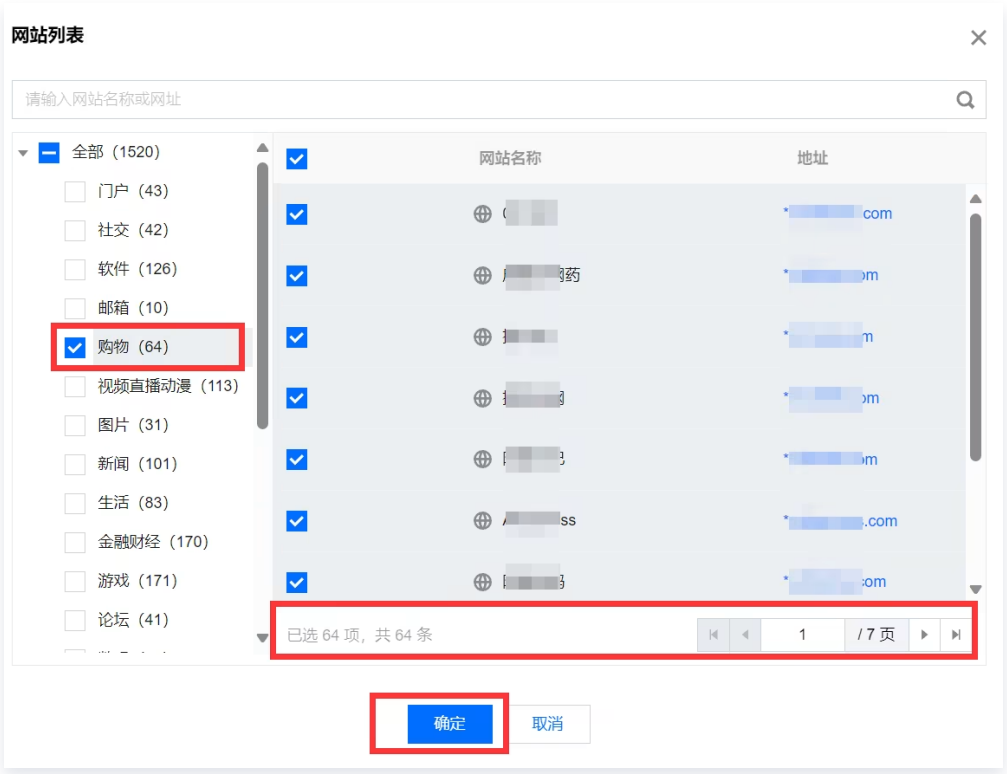
> **URL 填写说明：**
>
> - 支持填写域名或 IP，例如：www.abc.com 或112.0.0.1。
> - 不需要填写 http:// 或 https://，填写时直接填写域名，例如：www.abc.com（www.abc.com 仅为示例域名）。
> - 添加 www.abc.com 黑名单，只会拦截前缀为 www.abc.com 网站，子域名 oa.abc.com 不会拦截。
> - 如果需要拦截所有子域名，可以将 *.abc.com 添加为黑名单，则 abc.com 所有的子域名均会被拦截，目前仅支持 * 在域名的开头。



- 使用内置的网址大全，单击 开启内置网址大全 ，单击**编辑**。



示例：购物，勾选购物网站信息，单击确定。



3. 选择**不限时段**或**指定时段**，并设置**上报拦截报警日志**。

> **说明：**

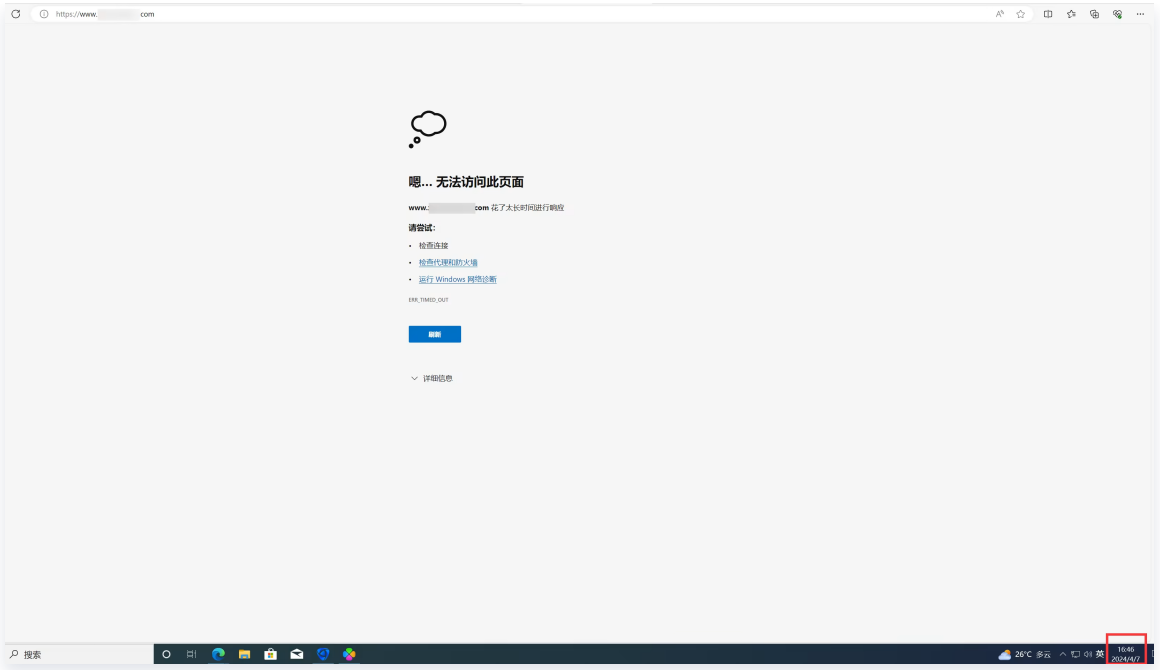
请参见 上网行为管控审计日志 以获取上报拦截报警日志的相关详情。



4. 弹窗提醒：在 Host 地址访问规则设置为“黑名单”时，系统支持自定义弹窗内容。弹窗样式可参考“上网拦截弹窗提醒”。



5. 配置完成单击**保存**。
6. Host 地址控制示例：8点~18点访问购物类网站失败。



进程控制

1. 在**策略配置** > **新建策略**页面，勾选**上网拦截**，拦截方式选择**进程控制**。
2. 选择**控制类型**，单击**添加**，配置进程列表信息，单击**确定**。

> **说明：**
> - 黑名单：不允许以下进程访问网络（不包含 IOA 客户端必要的进程）。
> - 白名单：仅允许以下进程访问网络（默认包含 IOA 客户端必要的进程）。
> - 白名单和黑名单只有一种类型同时生效，本文以设置黑名单为示例。



3. 选择**不限时段**或**指定时段**，并设置**上报拦截报警日志**。

> **说明：**

> 请参见 上网行为管控审计日志 以获取上报拦截报警日志的相关详情。



4. 弹窗提醒：在进程控制规则设置为“黑名单”时，系统支持自定义弹窗内容。弹窗样式可参考“上网拦截弹窗提醒”。



5. 配置完成单击**保存**。
6. 进程控制示例：8点~18点访问 QQ 进程失败。



Host 地址和进程控制

1. 在**策略配置** > **新建策略**页面，勾选**上网拦截**，拦截方式选择 **Host 地址和进程控制**。
2. 选择**控制类型**并设置所需的 Host，支持自定义和使用内置 Host。

> **说明：**
> - 黑名单：下发策略的终端，不能访问配置的黑名单站点，其他站点访问不受影响。
> - 白名单：下发策略的终端，只能访问配置的白名单站点，其他站点无法访问。
> - 本文以设置黑名单为示例。



3. 单击**添加自定义**，输入 Host 信息，添加完成单击**确定**保存。

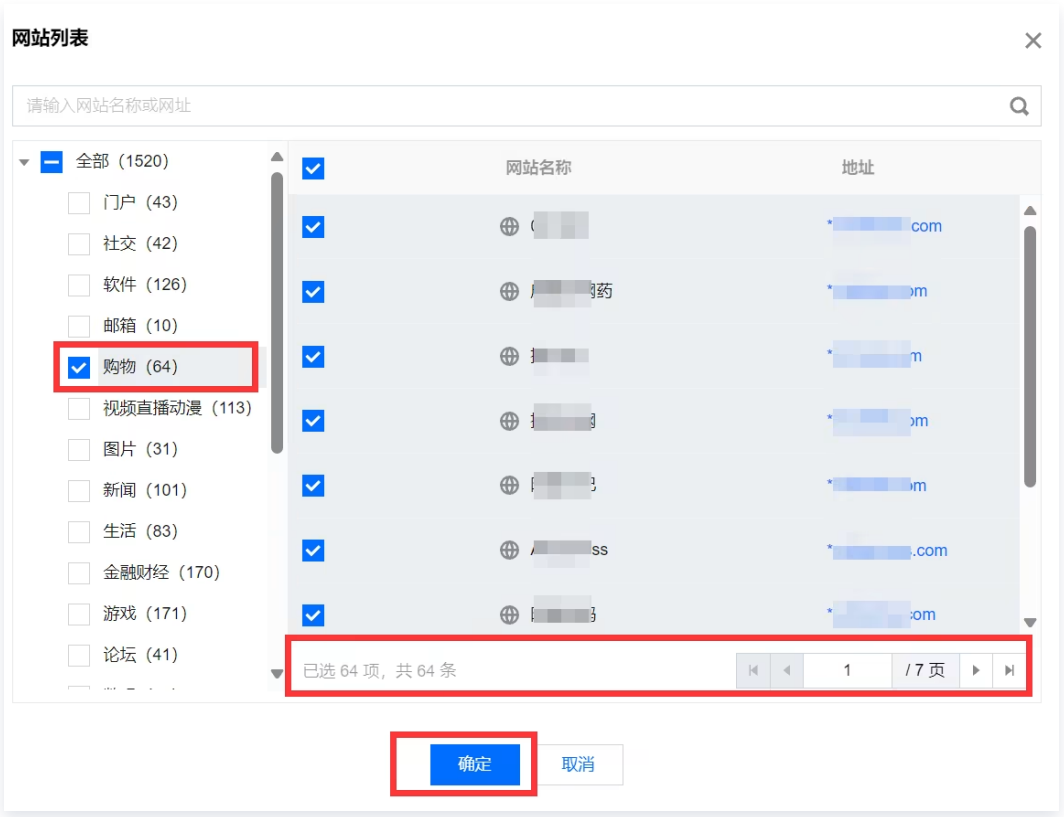
> **说明：**
>
> - Host 地址黑白名单与进程控制黑白名单独立，即可在开启 Host 白名单的同时，开启进程黑名单。
> - 进程控制规则优先级，总体高于 Host 黑白名单优先级。例如 `abc.com` 为白名单，但禁止 Word 进程访问网络的场景。即黑名单中有 Word 进程，Word 进程不允许访问任何域名，包括白名单内的 `abc.com` 域名。



- 使用内置的网址大全，单击 开启内置网址大全 ，单击**编辑**。



示例：购物，勾选购物网站信息，单击确定。



4. **进程管控规则：单击添加，输入进程信息，单击确定。**

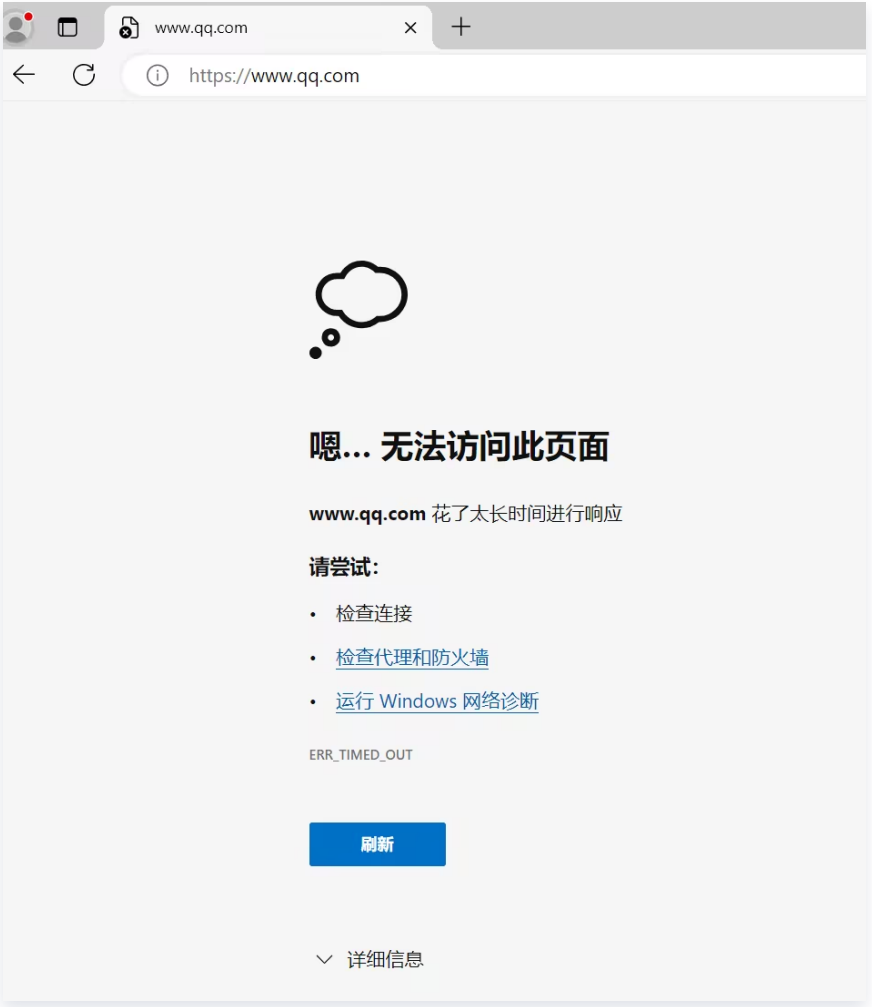


5. **选择不限时段或指定时段，并设置上报拦截报警日志。**

> **说明：**
> 请参见 上网行为管控审计日志 以获取上报拦截报警日志的相关详情。



6. 弹窗提醒：设置为“黑名单”时，系统支持自定义弹窗内容。弹窗样式可参考“上网拦截弹窗提醒”。
7. 配置完成单击**保存**。
8. Host 地址和进程控制示例：8：00-18：00，访问规则内的 Host 地址与进程信息，访问不成功。





上网拦截弹窗提醒

> **说明：**
> 上网拦截弹窗提醒功能要求客户端版本10.9.1及以上支持该功能，如客户端版本低于10.9.1请升级客户端。

1. 支持自定义上网拦截提示内容弹窗。



2. 拦截弹窗样式示例：



3. 支持对相同进程/Host 弹窗拦截频率进行设置。



4. 支持选择是否允许用户关闭弹窗提醒。

- 选择否：弹窗按钮仅有"确定"。
- 选择是：客户端弹窗将会展示“不再提醒”按钮，用户单击后当日内不再展示上网拦截弹窗。



网络访问隔离（11.1.1版）

最近更新时间：2026-02-13 09:41:01

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

配置背景

- 终端访问内网时禁止访问外网，访问外网时禁止访问内网。
- 终端默认属于内网。

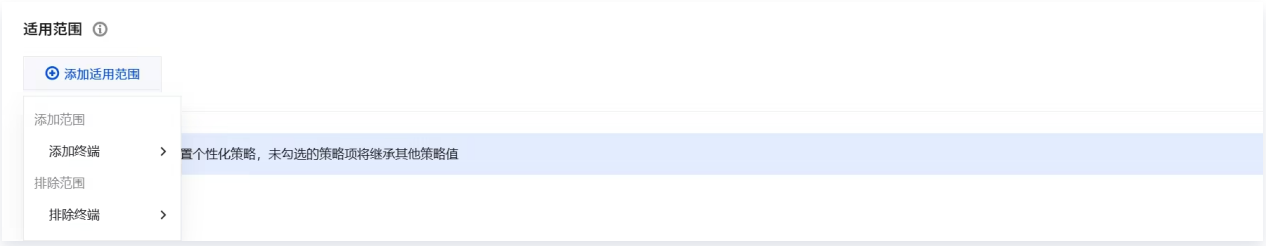
> **说明：**
> - 配置网络时，可以配置为黑名单模式或白名单模式，一个网络只能为一种模式。
> - 白名单模式：终端在此网络下仅能访问白名单范围内的地址，白名单外的地址禁止访问。
> - 黑名单模式：终端在此网络下禁止访问黑名单范围地址，可以访问黑名单范围外的 IP 地址。
> - 配置思路：首先明确一个网络的 IP 范围 A，网络名称为内网，另一个网络为外网，配置内网为白名单模式，并配置 IP 范围 A； 配置外网为黑名单模式，同样配置网络范围 A。以下是具体配置过程：（其他场景可根据上述黑白名单原理灵活配置）。

步骤1：开启终端网络访问控制

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端管理** > **客户端策略**。
2. 在客户端策略页面，选择 **模块定制**，单击**新建策略**。
3. 在新建模块定制策略页面，填写基本信息、适用范围和编辑策略。
   3.1 基本信息：输入策略名称、策略描述，并选择是否启用。



3.2 适用范围：该策略生效的对象范围。单击**添加适用范围**，您可以通过添加或排除终端，来进行精细化的管控范围设置。



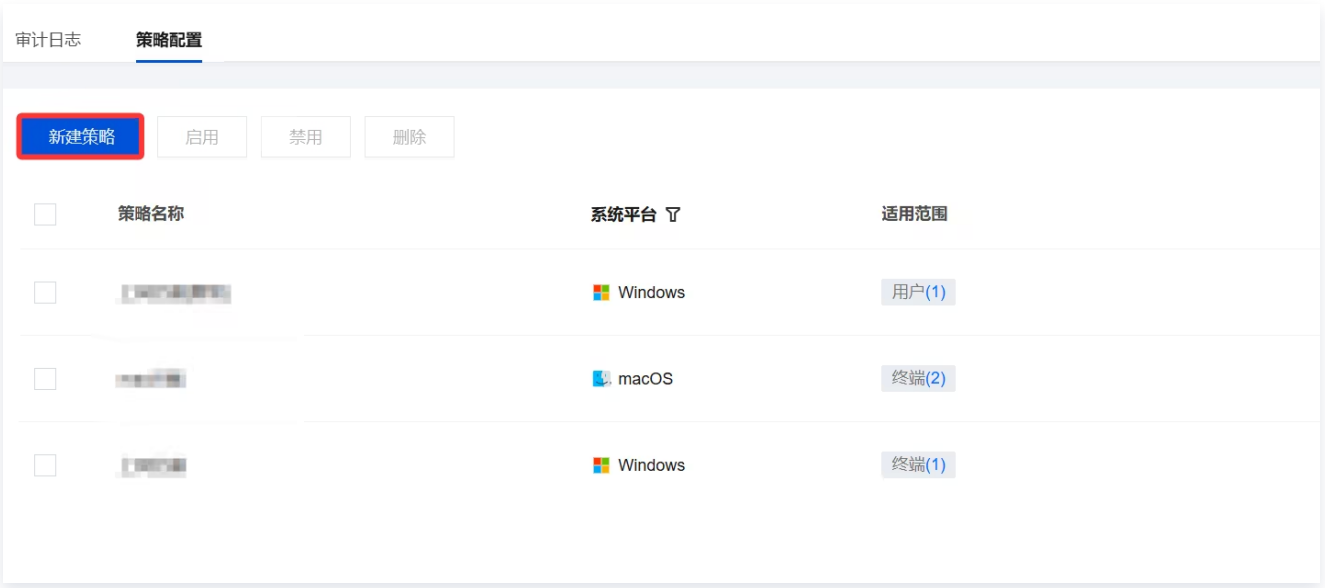
3.3 编辑策略：配置功能模块配置参数，勾选**终端网络访问控制**，单击**保存**。



步骤2：配置网络访问隔离

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **上网行为管控** > **策略配置**。

2. 在**策略配置**页面，单击**新建策略**。



3. 在新建策略页面，配置基本信息：输入策略名称、策略描述，并选择是否启用。



4. 适用范围：该策略生效的对象范围。单击**添加适用范围**，您可以通过添加或排除用户、组织架构、自定义用户组和终端，来进行精细化的管控范围设置。



5. 勾选**网络访问控制**，**开启隔离**开关，单击**编辑**设置**办公网**或**互联网**。



- **办公网：选择白名单模式，地址配置为内网网段，并根据需求配置其他参数。**



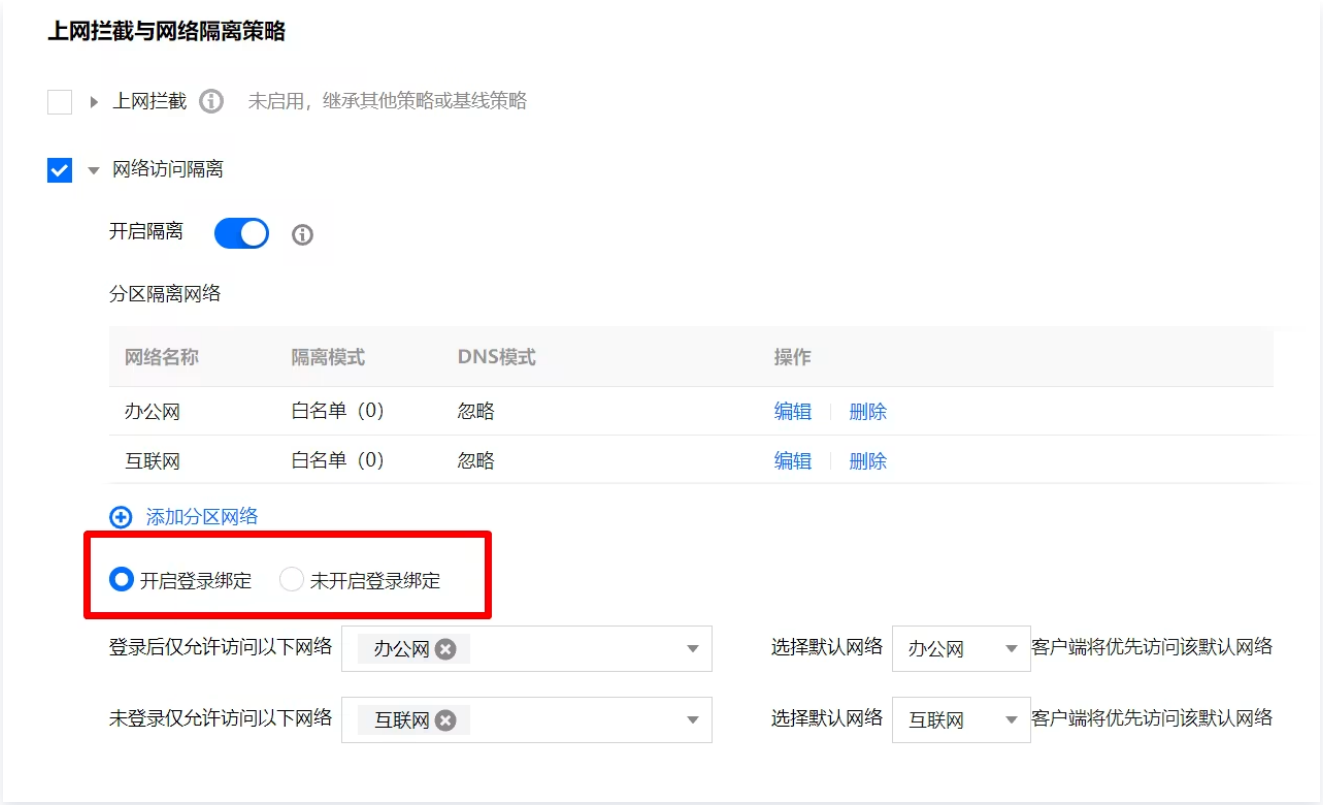
参数名称	说明
豁免指定目标	通常配置为两网下同时需要访问的 IP，两个网络（办公网&互联网）都需要配置。 **注意：** 此处需要将 iOA 服务器相关的所有内外网 IP（包括服务器前端的 LB）都添加到内网和外网的豁免 IP 中，以防止策略配置错误导致终端失联。

配置 DNS 管理	• 自动获取：客户端从网络中自动获取 DNS 地址。 • 使用下发地址：切换网络后 DNS 设置为下发地址。 **注意：** 若配置了下发 DNS 地址，则需要确保终端能够访问到下发的 DNS 地址。 建议内网和外网使用相同的 DNS 配置方式。 如果内网配置为下发 DNS，而外网配置为忽略，那么从内网切换到外网时由于外网配置为忽略，此时设备依然会保持为内网下发的 DNS 地址。若此时外网环境下无法访问这个 DNS 地址，则会导致网络异常。

- **互联网：选择黑名单模式，地址配置为内网网段，并根据需求配置其他参数。**



6. **登录绑定：根据实际情况选择，效果验证请参见 步骤3：效果验证 。**



7. 默认网络选择为**办公网**，单击**保存**。



步骤3：效果验证

> **说明：**
> 为了更好的用户体验，**我们强烈建议终端开启客户端弹窗功能**，以通知用户目前所处网络状态，防止网络切换导致业务无法访问。如果用户不小心单击了“不再提醒”，导致不出现提醒弹窗，可以通过卸载后重新安装来恢复弹窗提醒。仅覆盖安装无法解决此问题。

Windows 端弹窗由控制台弹窗开关控制

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端管理** > **客户端策略**。
2. 在客户端策略页面，选择**客户端自保护**，单击**新建策略**。
3. 在新建客户端自保护策略页面，填写基本信息、适用范围和编辑策略。

   3.1 基本信息：输入策略名称、策略描述，并选择是否启用。



   3.2 适用范围：该策略生效的对象范围。单击**添加适用范围**，您可以通过添加或排除终端，来进行精细化的管控范围设置。



   3.3 勾选**禁止客户端相关弹窗**，选择**不禁止**。



3.4 配置完成单击**保存**。

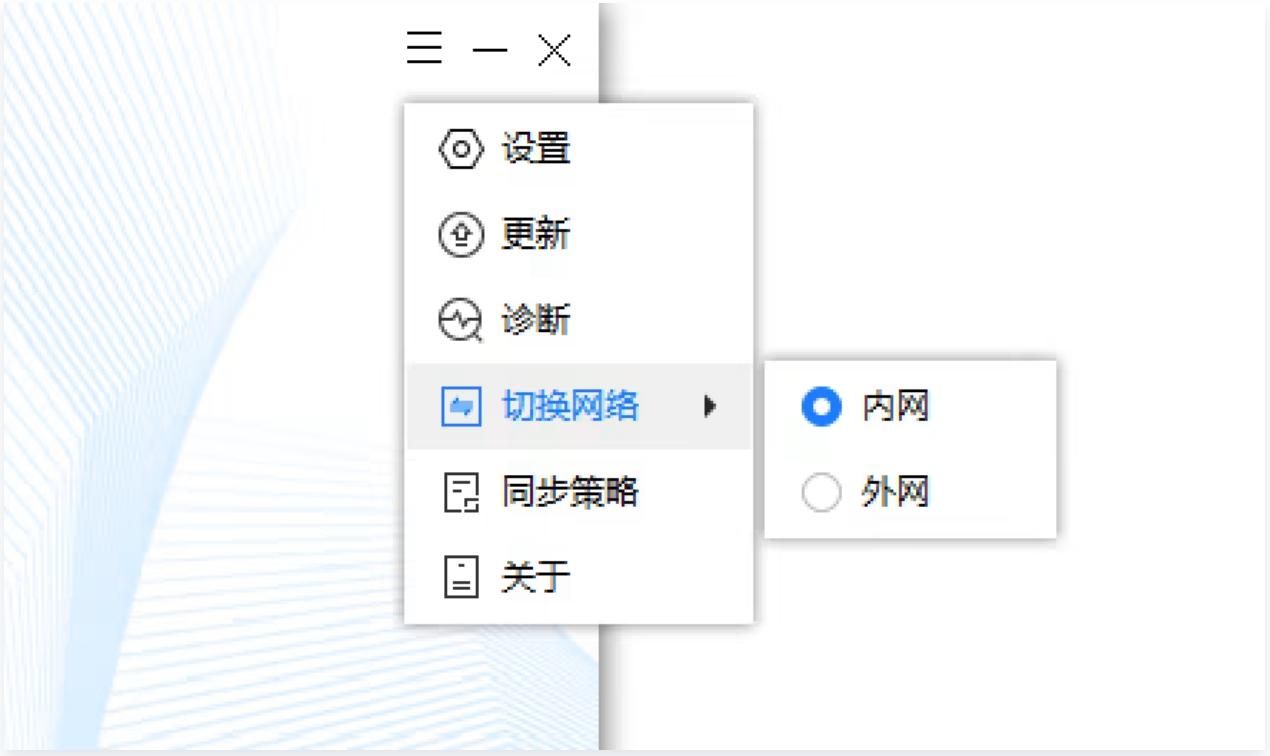
4. 在 步骤2 支持设置登录绑定场景：
   - **开启登录绑定的场景**，登录 NGN 后提示切换到内网，终端能正常访问内网范围地址，无法访问非内网范围地址。



注销 NGN 后提示切换到外网，终端无法访问内网范围地址，可以访问非内网范围地址。



- **未开启登录绑定的场景**：Windows 端表现如下图所示。

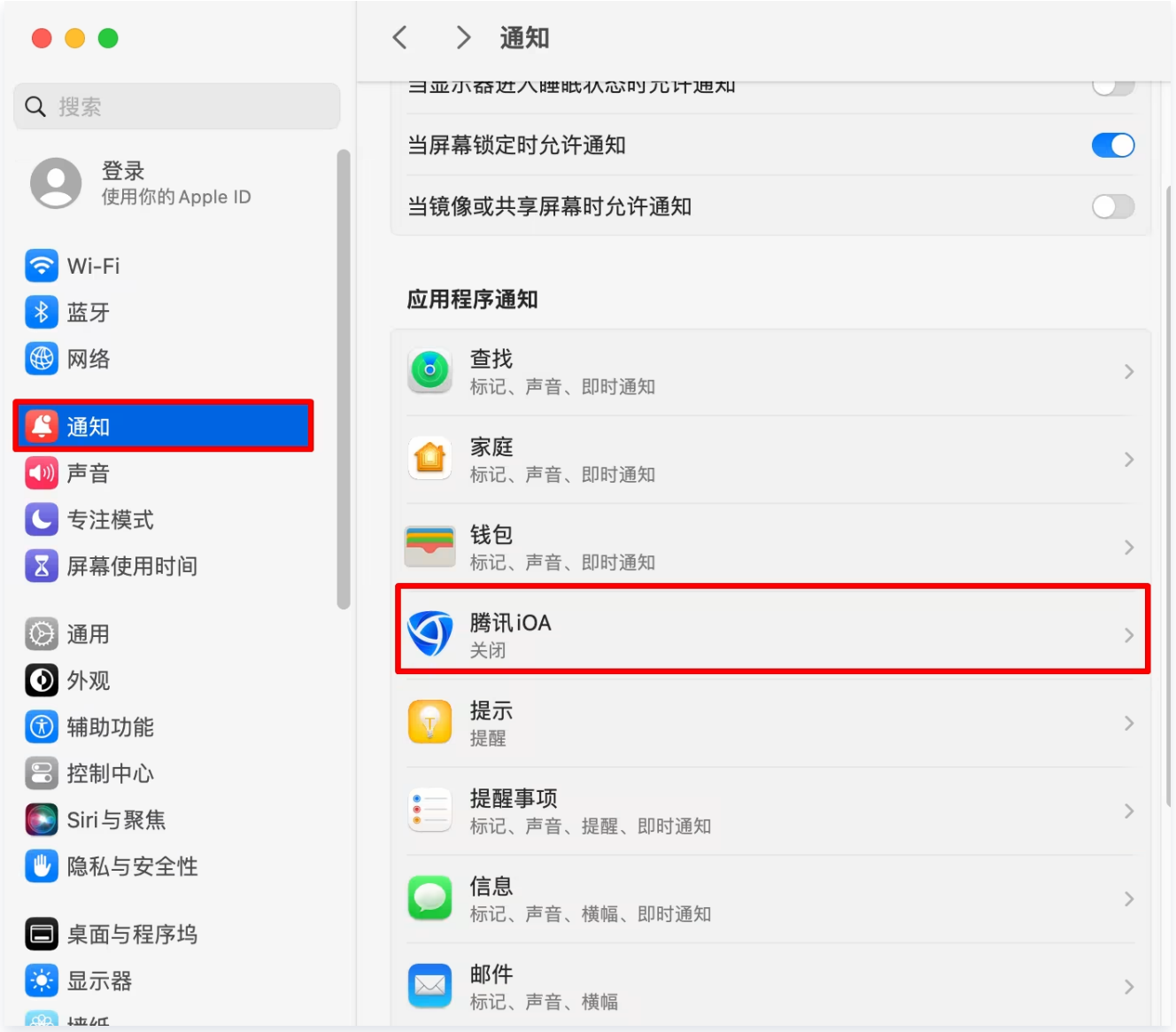


macOS 端可在系统通知中开启

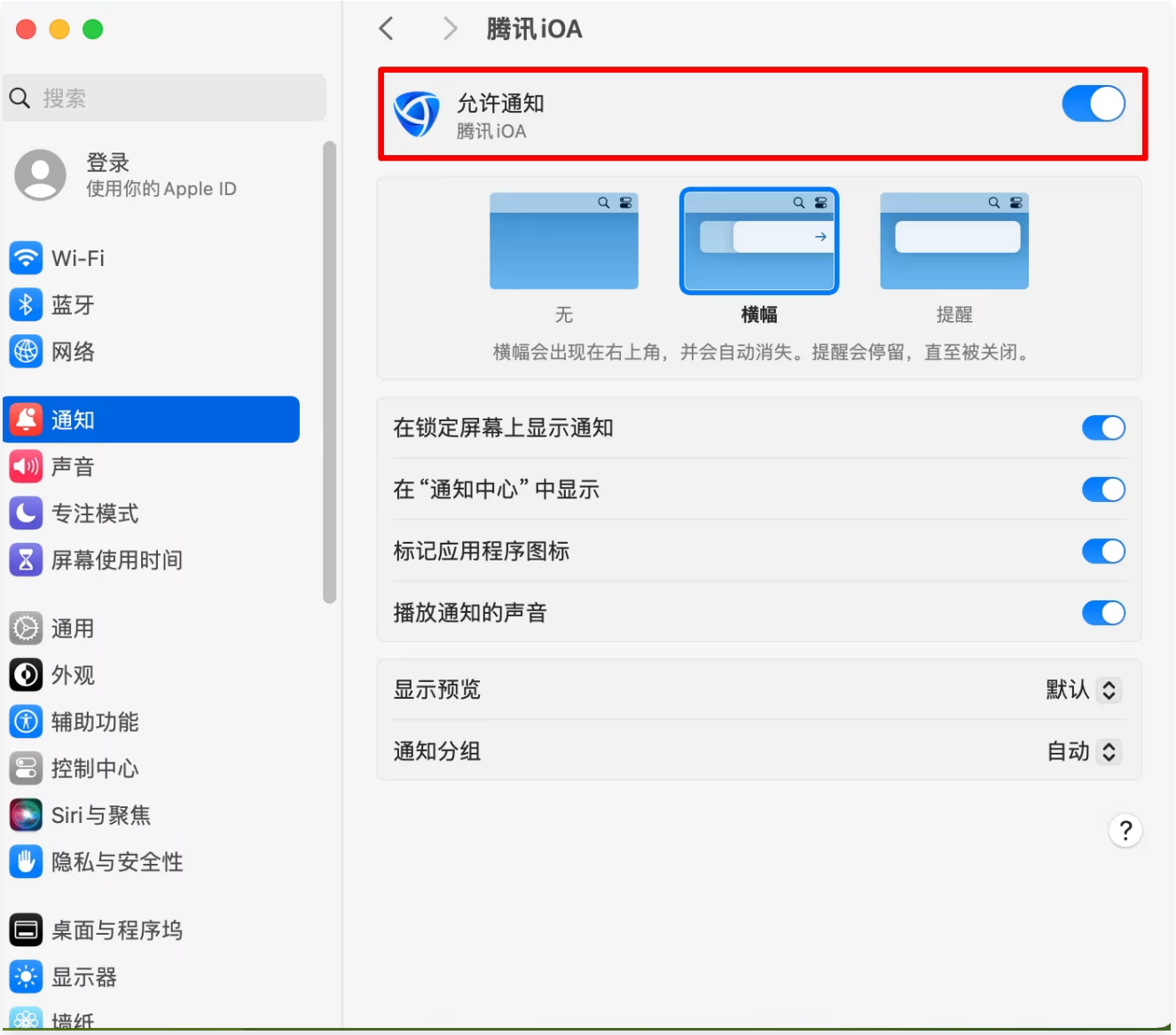
1. 在 macOS 系统中，选择**系统设置**。



2. 在通知页面，选择**腾讯 iOA**。


通知
搜索
登录
使用你的 Apple ID
Wi-Fi
蓝牙
网络
通知
声音
专注模式
屏幕使用时间
通用
外观
辅助功能
控制中心
Siri 与聚焦
隐私与安全性
桌面与程序坞
显示器
当屏幕锁定时允许通知
当镜像或共享屏幕时允许通知
应用程序通知
查找
标记、声音、即时通知
家庭
标记、声音、即时通知
钱包
标记、声音、即时通知
腾讯 iOA
关闭
提示
提醒
提醒事项
标记、声音、提醒、即时通知
信息
标记、声音、横幅、即时通知
邮件
标记、声音、横幅

3. 开启**允许通知**按钮。



4. 在步骤2 支持设置登录绑定场景：
   - **开启登录绑定的场景**：登录 NGN 后提示切换到内网，终端能正常访问内网范围地址，无法访问非内网范围地址。



注销 NGN 后提示切换到外网，终端无法访问内网范围地址，可以访问非内网范围地址。



- **关闭登录绑定的场景**：macOS 端切换网络显示内网/外网。

水印保护（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

屏幕水印

支持对终端设置屏幕水印及打印水印，对于截屏、拍照等泄露方式可追溯查找泄露源；支持设置字符、二维码等水印形式；支持设置水印信息、倾斜角度、透明度、大小、行列间距、位置、颜色等参数。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **水印保护** 。
2. 在 水印保护 页面，单击**新建策略**，进入新建水印保护策略页面。



3. 在新建策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。



3.2 单击**添加适用范围**，您可以通过添加或排除用户、组织架构、自定义用户组和终端，来进行精细化的管控范围设置。



4. 屏幕水印保护：勾选**屏幕水印保护**，单击 开启屏幕水印保护，配置相关策略，配置完成后单击**预览水印**



，预览完成关闭预览，单击**保存**。



参数名称	说明
开启屏幕水印保护	开启。
水印形式	• 字符水印：水印以字符样式展示。 • 二维码水印：水印以二维码样式展示。
设置水印信息	• 水印信息支持配置：员工账号、终端名称、终端时间、姓名、邮箱、电话、IP 地址、MAC 地址。 • 支持自定义水印信息。

版权所有：腾讯云计算（北京）有限责任公司

水印可视度	默认是隐约可见（20%），可自行调整。
其他参数	建议默认选择。

5. 水印下发成功后，桌面自动生成。



打印水印

打印水印在打印文档的时候，对文档添加水印记号，起到文档溯源和防复制的作用。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **水印保护**。
2. 在水印保护页面，单击**新建策略**。



3. 在新建策略页面，勾选**打印水印**，单击 开启打印保护，配置相关策略，单击**保存**。

> **说明：**
> 打印水印支持字符打印、二维码水印，是文件打印时输出的水印，常规的设置可参考屏幕水印的设置。
> 根据实际情况是否设置页眉页脚的水印。



4. 特殊位置打印水印：针对可区分页眉页脚的打印文档，支持字符水印、二维码水印，勾选页眉/页脚，配置相关策略，配置完成后单击**保存**。



5. 终端进行直接打印或者选择 XPS 打印，保存为.xps/.oxps格式后打开可看到效果。

> **说明：**
> XPS 格式，全称 XML Paper Specification，是一种电子文件格式，由微软公司开发，旨在提供一个文档保存和查看的规范，XPS 格式仅 Office 办公软件支持保存。



版权所有：腾讯云计算（北京）有限责任公司

文件管控（11.1.1版）
文件管控审计日志（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

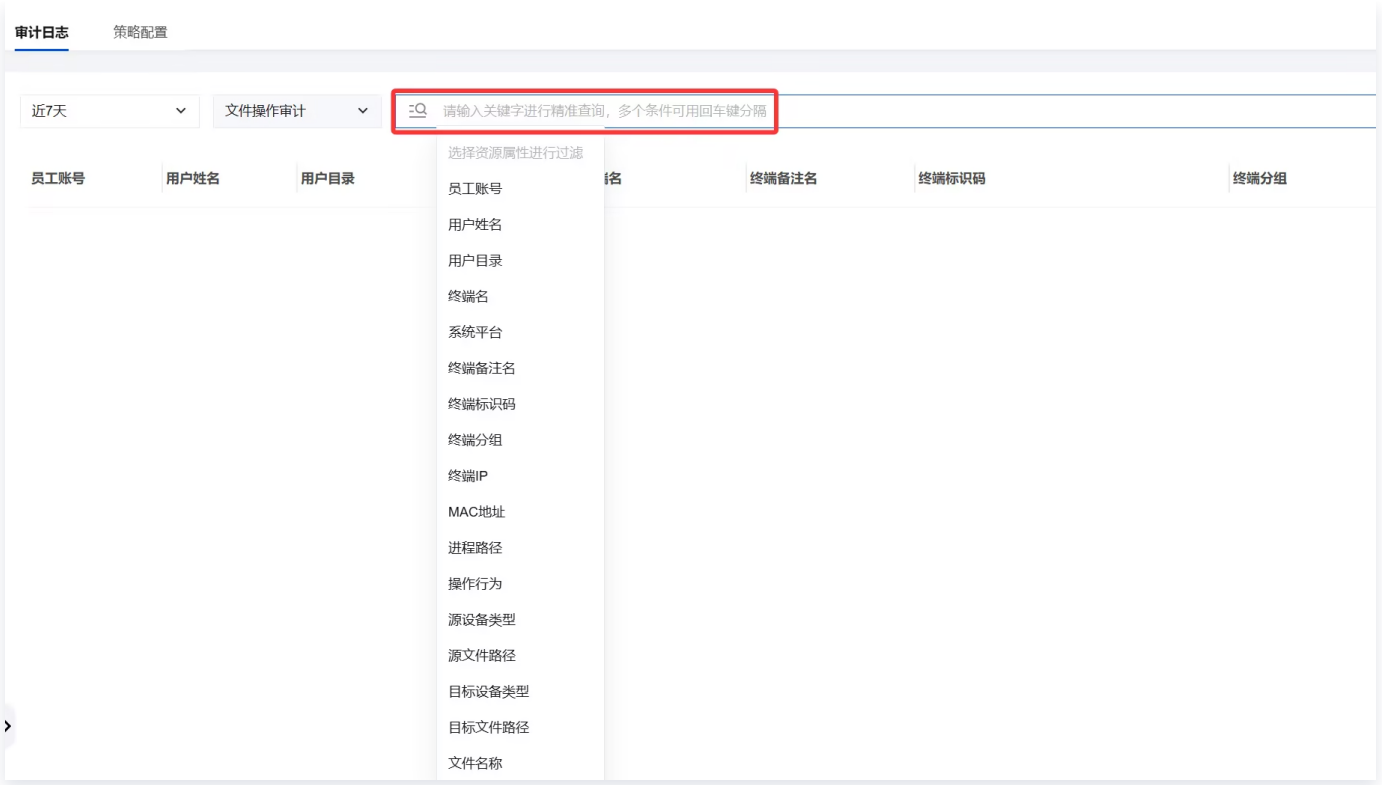
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控 > 文件管控 > 审计日志**。
2. 支持时间段筛选，提供标准时间筛选控件：通过顶部左上角的 “近7天” 下拉选择框，您可以快速切换查看“今天”、“近7天”、“近14天”、“近30天”、“自定义日期”等不同时间范围内的审计日志。



3. 文件操作审计：触发**终端管控 > 文件管控 > 策略配置 > 文件操作审计**配置的操作行为信息，在文件操作审计日志展示。



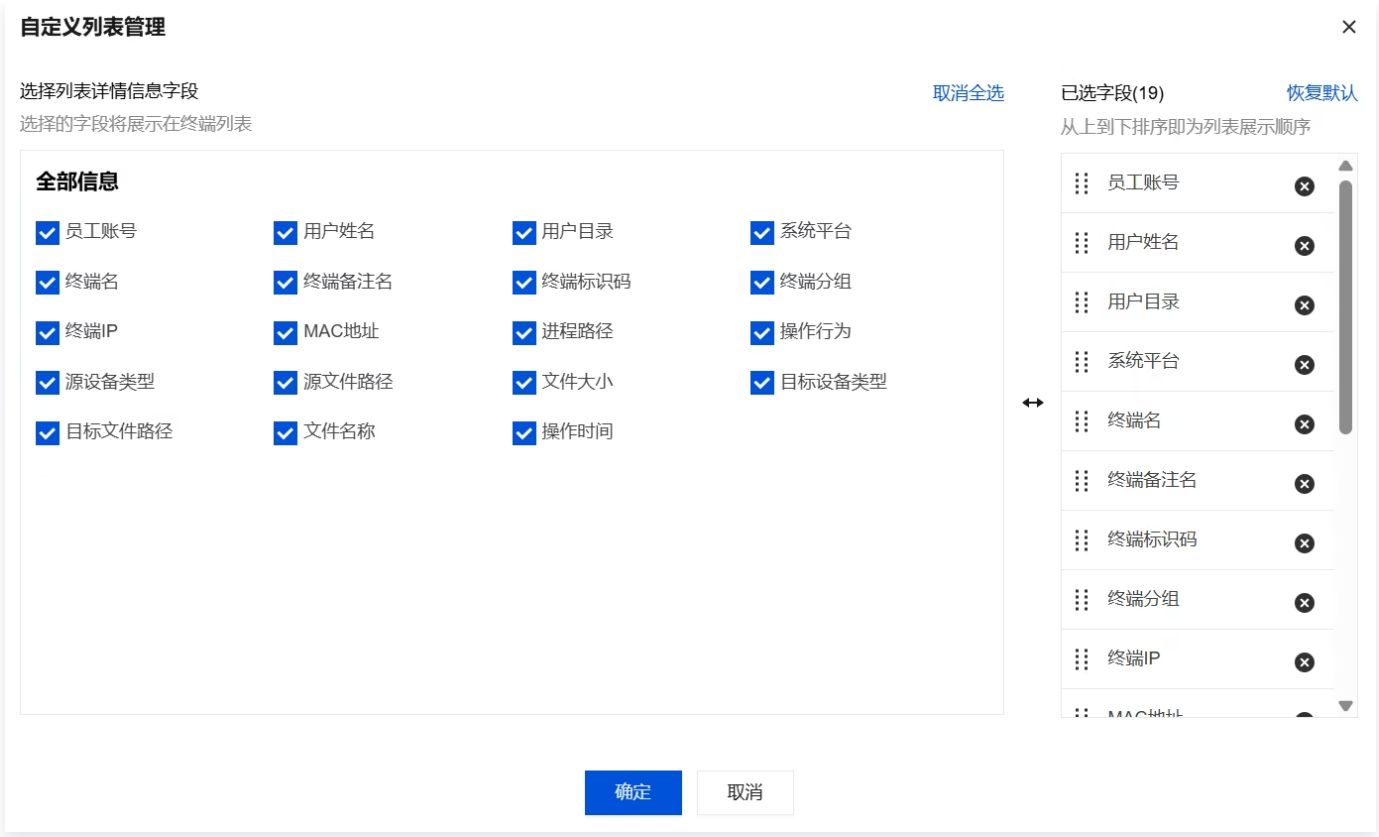
4. 文件访问与操作：触发**终端管控 > 文件管控 > 策略配置 > 文件访问管控**配置的访问/操作行为信息，在文件文件访问与操作日志展示。
5. 关键字精准查询：在“请输入关键字进行精准查询”的搜索框内，您可以输入特定关键字（如：员工账号、操作行为等），系统将筛选出包含此关键字的日志记录。



6. 可选择日志导出时间：默认选择当前日志筛选时间。



7. 单击 ⚙，选择的字段将展示在列表字段中。


自定义列表管理
选择列表详情信息字段
选择的字段将展示在终端列表
取消全选
全部信息
员工账号
用户姓名
用户目录
系统平台
终端名
终端备注名
终端标识码
终端分组
终端IP
MAC地址
进程路径
操作行为
源设备类型
源文件路径
文件大小
目标设备类型
目标文件路径
文件名称
操作时间
已选字段(19)
恢复默认
从上到下排序即为列表展示顺序
员工账号
用户姓名
用户目录
系统平台
终端名
终端备注名
终端标识码
终端分组
终端IP
确定
取消

文件管控策略配置（11.1.1版）

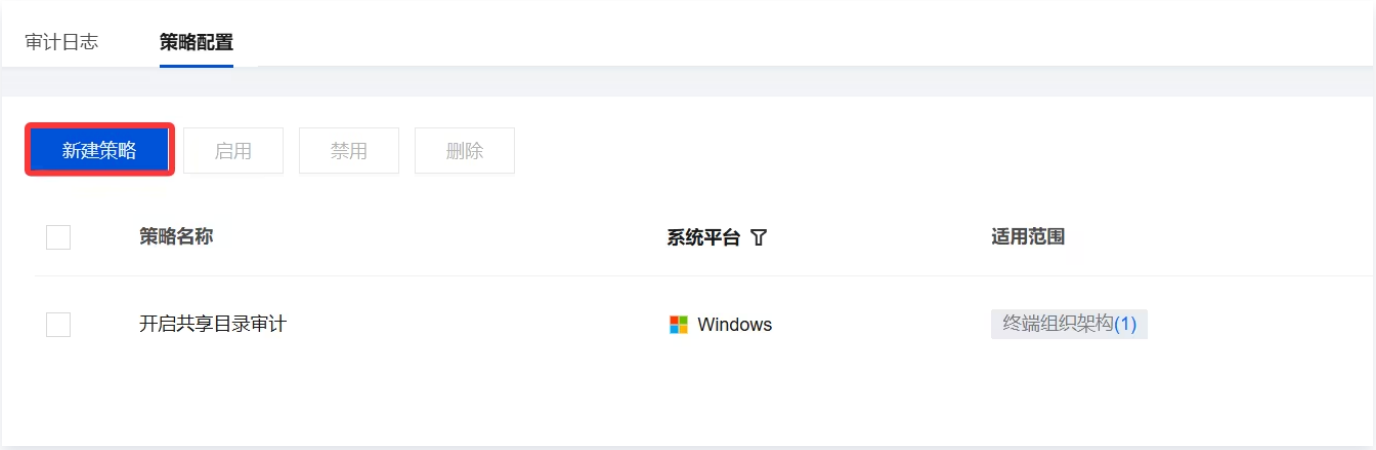
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

对策略设定的文件/文件夹进行监测和管控。

- 监测：记录创建、修改、删除和读取等操作行为。
- 管控：对企业敏感文件进行权限加固，例如：禁止修改、复制、移动和读取等操作。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **文件管控**。
2. 在文件管控页面，选择策略配置，单击**新建策略**。



3. 在新建策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。



3.2 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。



4. 根据实际需求，选择如下**文件管控策略**，单击**保存**。

文件访问管控

> **注意：**
> **开启后可能对终端的使用有一定影响（例如：管控范围较广时有可能影响文件的操作性能），请谨慎开启。**
> **在开启后，请做好测试验证，确认无异常之后再逐步灰度扩大影响范围。**

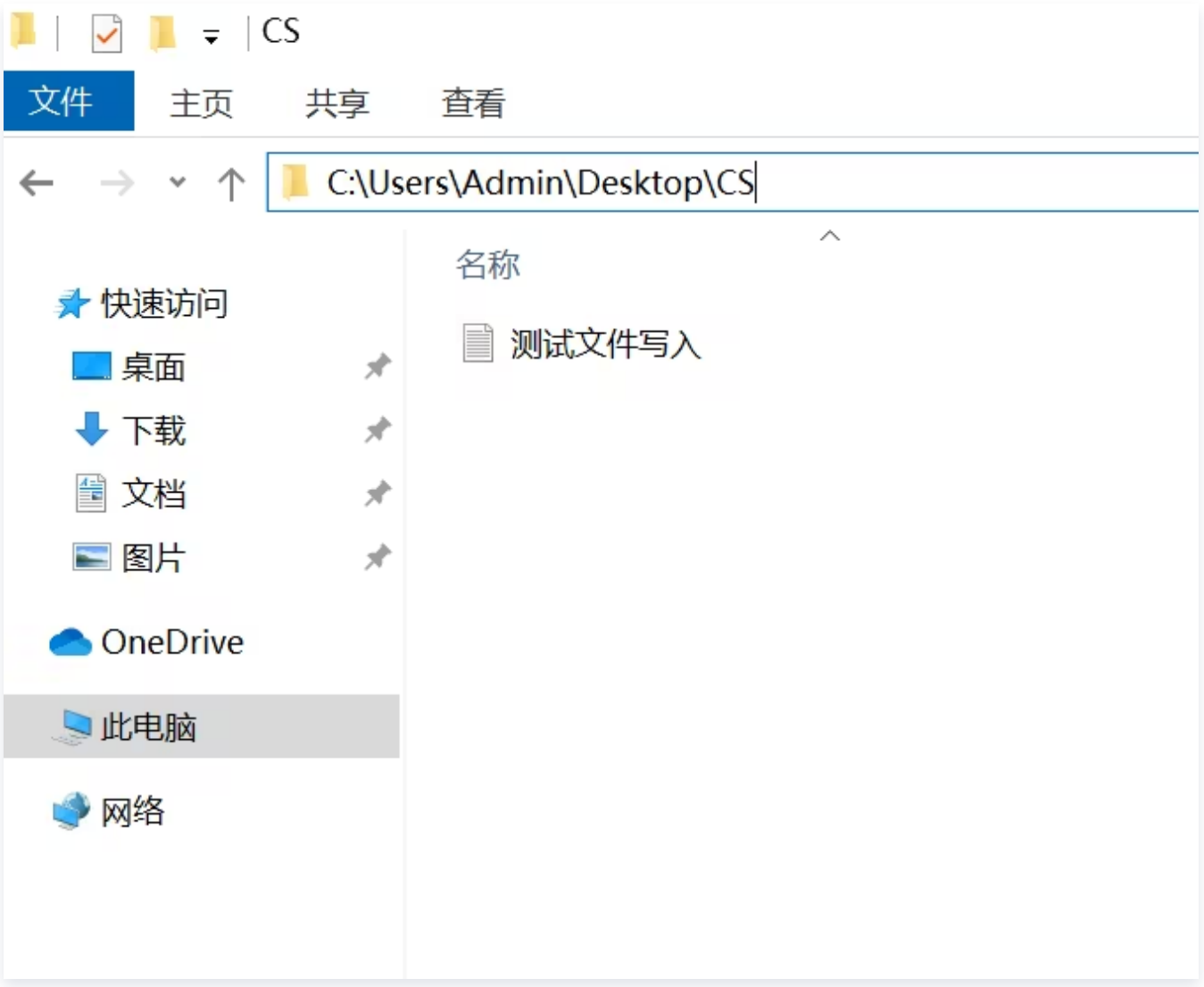
1. 勾选文件访问管控，单击 **开启文件访问与操作控制**。



参数名称	说明
禁止访问以下文件或文件夹路径	• 当配置文件名时，将会模糊匹配所有与输入文件名匹配的文件（例：note.doc将会匹配123note.docx） • 当配置路径，以“\”结尾时，将进行精确匹配（例：D:\windows\），无“\”结尾时，将会模糊匹配所有与输入路径名匹配的文件夹（例：D:\windows将会匹配D:\windows123） • 建议不要禁用C盘文件夹以避免系统崩溃，如需添加C盘文件夹，请选择禁止指定程序访问
是否对系统文件加白	• 开启加白后，系统目录下的文件将不会被禁止访问。 • 如果不开启对系统文件加白，建议选择"禁止指定程序访问"模式，以避免因系统文件无法访问而导致系统崩溃。
禁止对受控文件或文件夹执行以下操作	根据实际管控情况选择创建、复制、移动、写入、删除、重命名、读取。
受控访问程序	• 禁止任意程序访问：受控文件/文件夹禁止任意程序访问。 • 禁止指定程序访问：填写指定程序名称。

配置示例

1. 新建1个文档，文档名称为《测试文件写入》，文档格式：txt。



2. 禁止访问以下文件或文件夹路径：填写新建文档所在的路径 C:\Users\Admin\Desktop\CS 。



3. 开启对系统文件加白，加白后电脑系统文件将不会被禁止访问。
4. 禁止对受控文件或文件夹执行写入操作。
5. 受控访问程序选择禁止任意程序访问。
6. 完成添加后，单击**保存**。



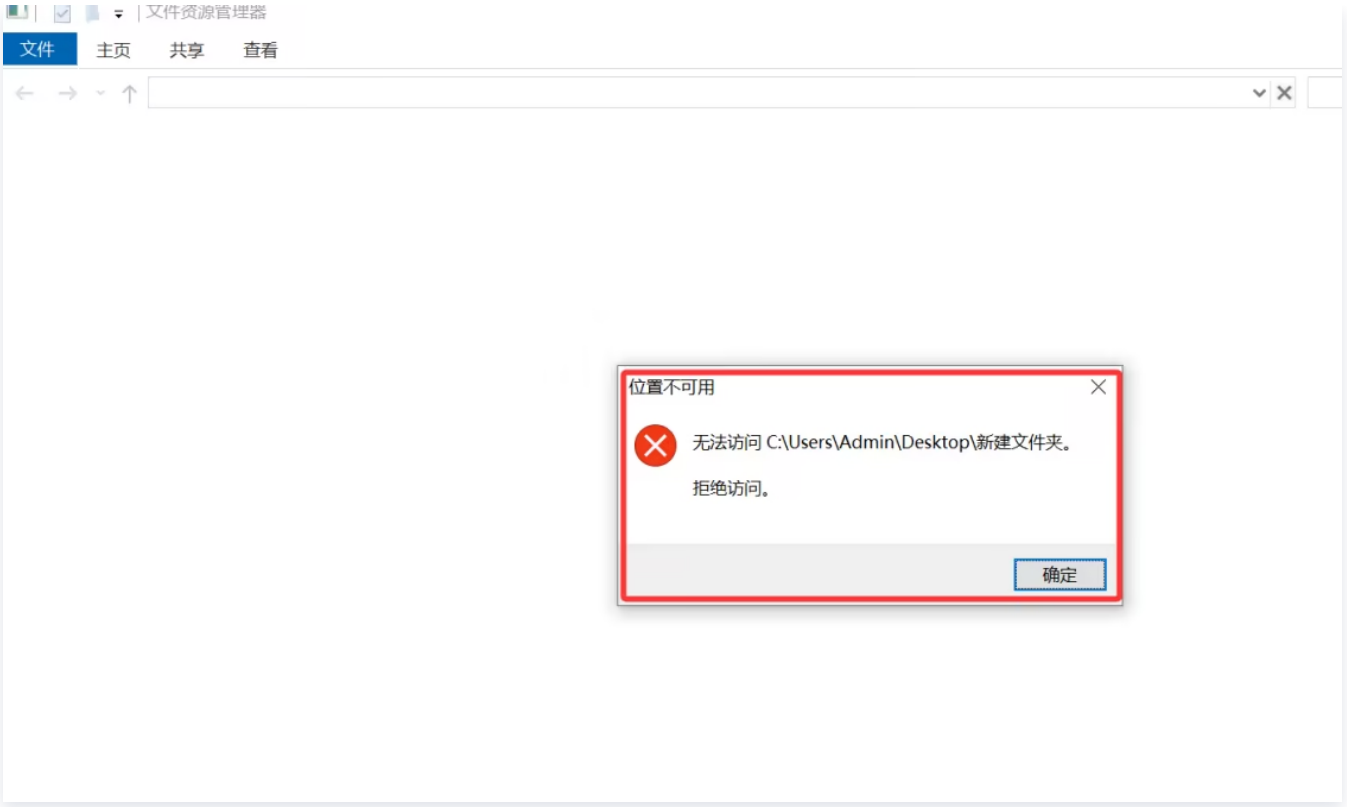
7. 在终端上打开指定的文件：《测试文件写入》.txt，写入内容后保存，提示操作成功完成。但文件大小未变化且内容并未写入，受控文件写入内容失败。



8. 若配置禁止对受控文件或文件夹执行创建，复制，移动等操作。



9. 当访问C:\Users\Admin\Desktop下文件或文件夹时，则提示系统的权限不足弹窗"拒绝访问" 。



文件操作审计

> **注意：**
> **开启后可能对终端的使用（例：审计范围较大有可能影响文件的操作性能）有一定影响，请谨慎开启。在开启后，请做好测试验证，确认无异常之后再逐步灰度扩大影响范围。**

1. 敏感文件操作审计行为可追溯。
2. 勾选**文件操作审计**，单击 **开启文件操作审计**。



参数名称	说明
审计文件操作行为	根据实际管控情况选择创建、复制、移动、写入、删除、重命名、读取。
设备存储监控	• 非本地硬盘存储介质（包括但不限于USB移动存储、光盘）。 • 本地硬盘（建议不选用，避免数据量过大；如果启用，需配置对应过滤参数文件夹或后缀名字）。
文件夹路径或关键字	• 当配置文件名时，将会模糊匹配所有与输入文件名匹配的文件（例：note.doc将会匹配123note.docx） • 当配置路径，以“\”结尾时，将进行精确匹配（例：D:\windows\），无“\”结尾时，将会模糊匹配所有与输入路径名匹配的文件夹（例：D:\windows将会匹配D:\windows123）
后缀	输入文件后缀名，例如 txt 等。

配置示例

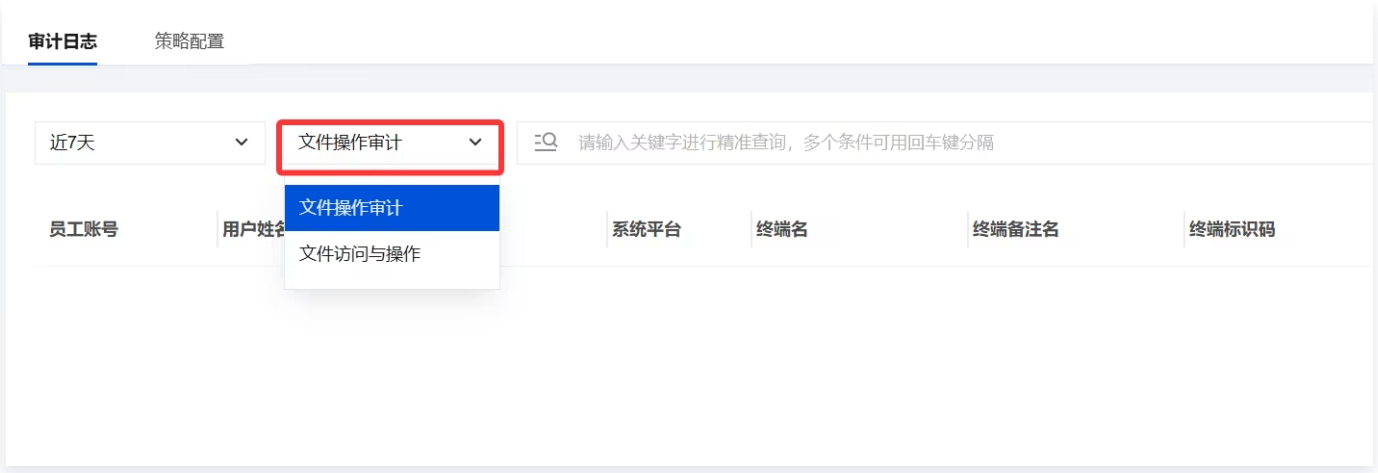
1. 勾选所有文件操作行为。



2. 设备存储监控为空（不勾选）。
3. 填写文件夹路径 C:\Windows 。
4. 输入txt，tmp，xml 文件后缀名 。
5. 完成添加后，单击**保存**。



6. 在终端C:\Windows下对 txt，tmp，xml 后缀的文件进行创建、复制、移动、写入、删除、重命名、读取操作。
7. 进入**终端管控 > 文件管控 > 审计日志**页面，选择**文件操作审计**，相关操作审计的日志上报到后台，并在 Web 端展示。



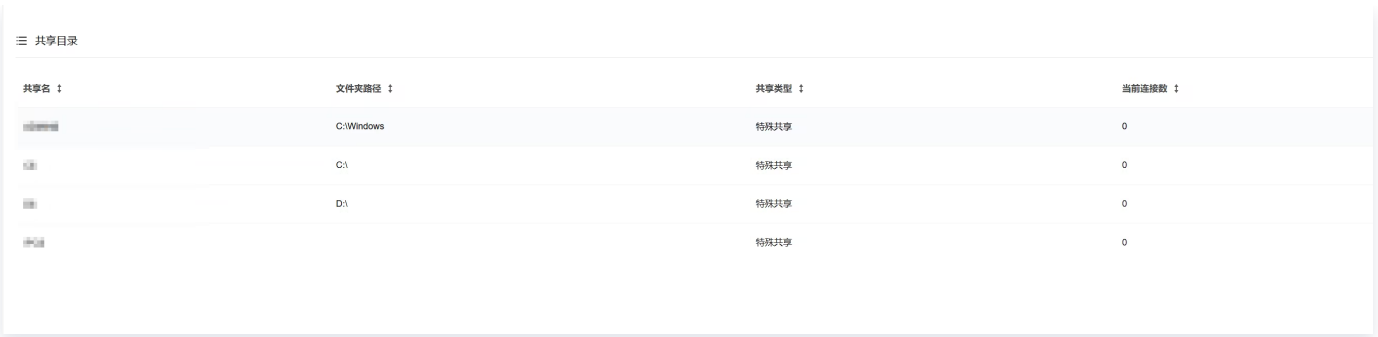
共享目录审计

1. 单击**开启共享目录审计**，开启后，收到此策略的终端上报本机共享文件夹信息。

> **说明：**
> 共享目录仅支持 Windows 系统。



2. 在**资产运维** > **终端运维** > **终端信息**页，单击**终端名称**进入终端详情，**运行监控** > **共享目录**页内枚举显示。


共享目录
共享名
文件夹路径
共享类型
当前连接数
C:\Windows
特殊共享
0
C:\
特殊共享
0
D:\
特殊共享
0
特殊共享
0

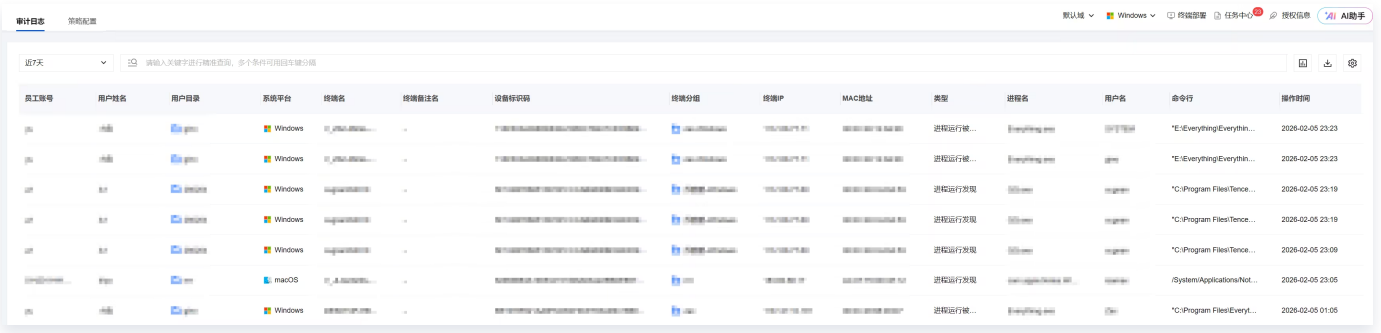
进程管控（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

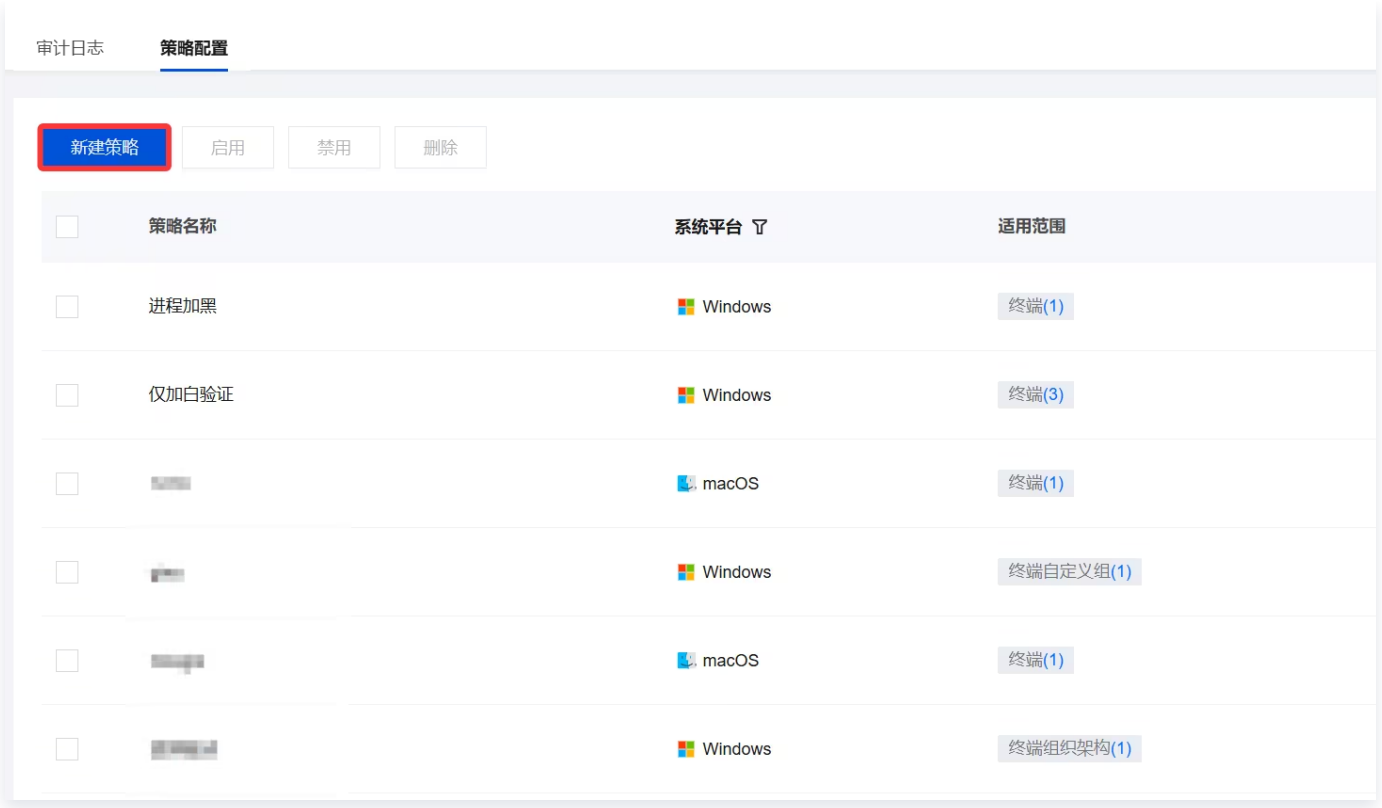
审计日志

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **进程管控**。
2. 在进程管控页面，选择**审计日志**。
3. 进程管控审计日志记录用户执行操作的程序进程、操作事件的类型分类及具体的操作命令内容，在**进程管控** > **策略配置**中配置的禁止程序运行或允许程序运行的记录在此展示。



策略配置

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **进程管控**。
2. 在进程管控页面，选择**策略配置**，单击**新建策略**。



3. 在新建策略页面，配置相关参数。

   3.1 编辑基本信息、添加适用范围。



参数名称		说明
策略名称		自定义，不超过50个字符。
是否启用		选择**开启**。
适用范围	添加用户	支持按组织架构、自定义分组选择用户。
	添加终端	支持按终端树、自定义分组选择终端。
	排除用户	支持从适用范围内排除例外用户。

	排除终端	支持从适用范围内排除例外终端。

3.2 设置进程管控策略。

支持配置**禁止以下程序运行**或**仅允许以下程序运行**策略，单击**添加规则**，配置相关参数，单击**确定**。

> **说明：**
> - 禁止程序运行：禁止某个软件的进程启动，或禁止某签名的软件启动，或禁止包含某个进程描述的软件启动。
> - 仅允许以下程序运行：仅允许某个软件的进程启动，或某签名的软件启动，或包含某个进程描述的软件启动。



参数名称		说明
规则名称		自定义。
类型	进程名	相对进程签名和进程描述而言，进程名是一种细粒度精确的策略，几乎不存在误拦。
	进程签名	每个正规软件的进程，都应该有签名，来表达身份，且不可伪造。签名通常绑定到某个公司，一个公司可能也会有多个签名，一旦使用进程签名策略，会覆盖范围更大（只要是该公司的签名软件，均会被拦截）。
	进程描述	一般用来表达软件的名称或称呼，或其他描述该进程的特征，没有统一规范，用来做策略，可能存在较多误拦。

4. 配置完成，单击**保存**。

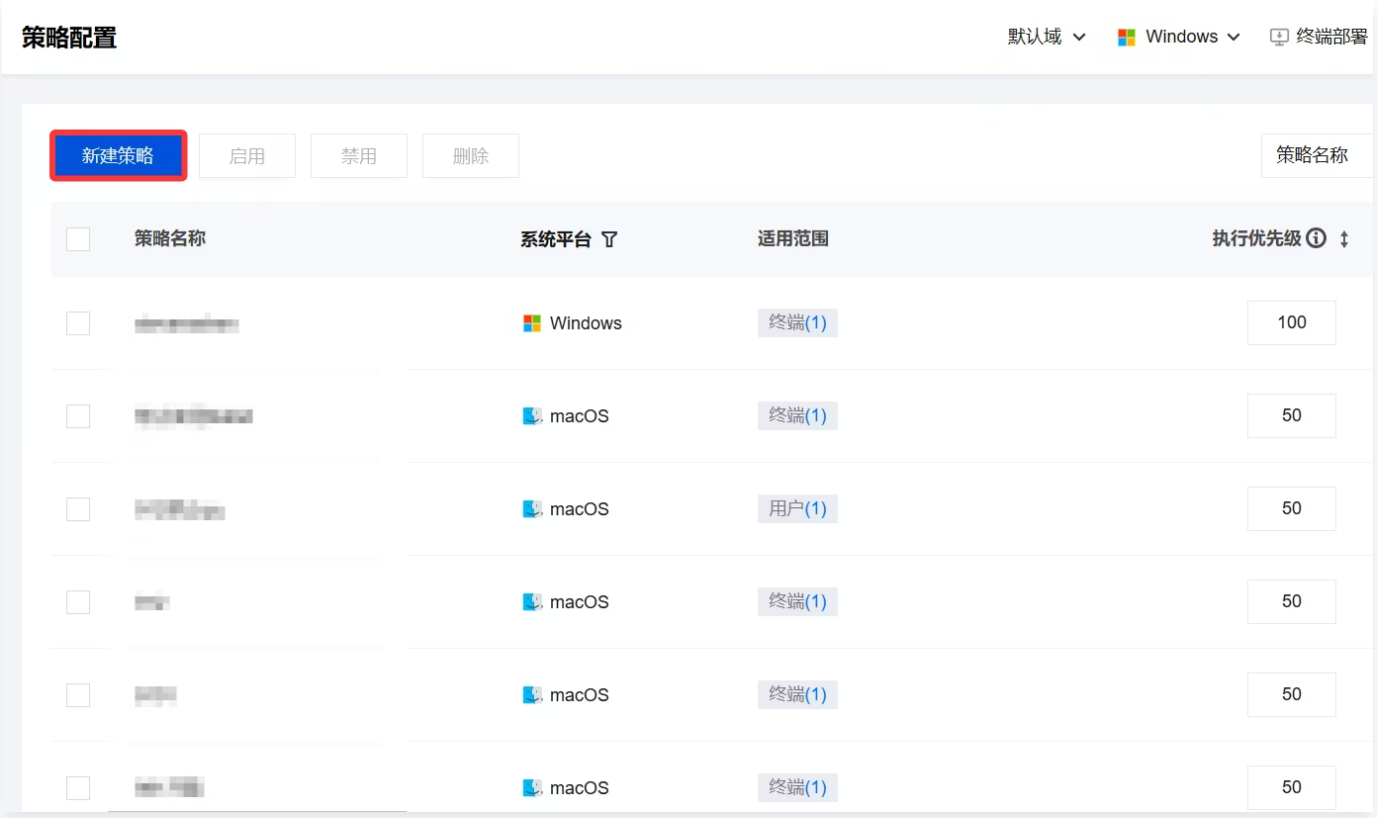
服务管控（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

对不必要的系统服务禁用，提升终端运行性能。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **服务管控**。
2. 在服务管控页面，单击**新建策略**。

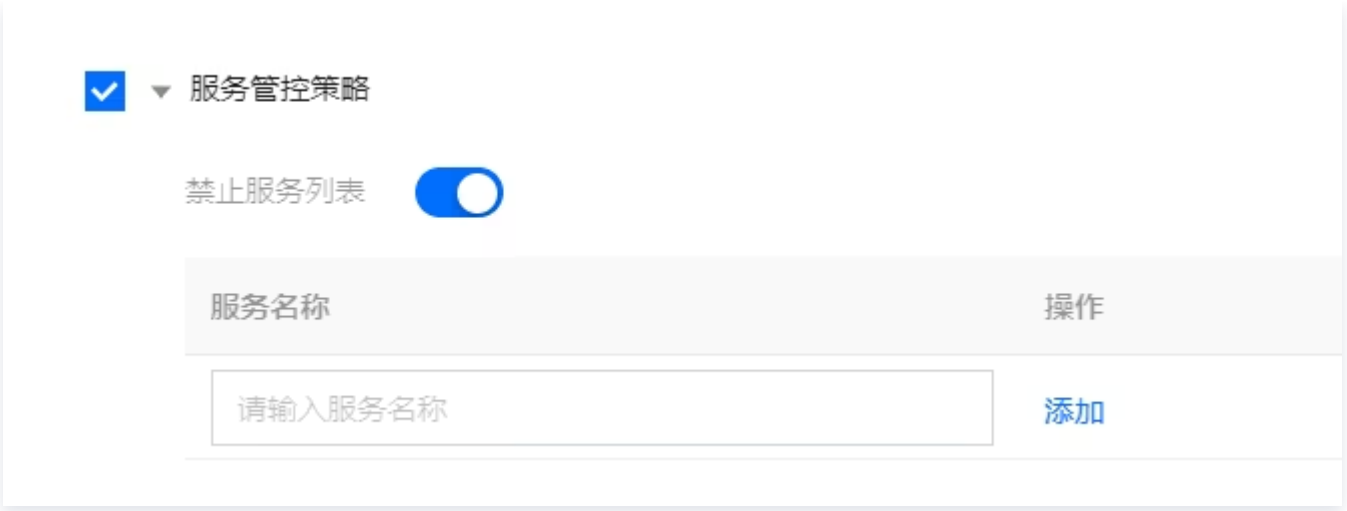


3. 在新建策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。

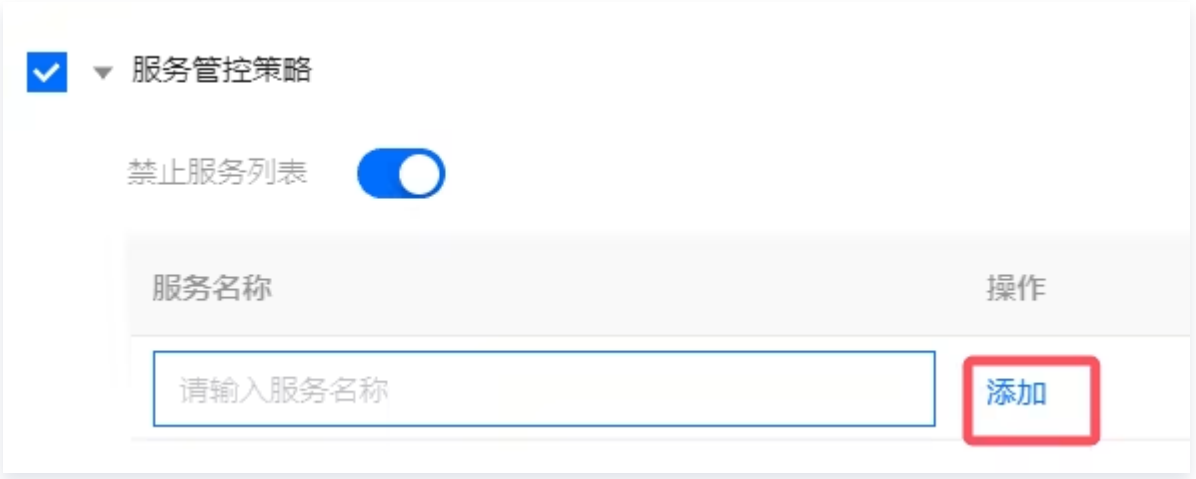


3.2 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。

4. 勾选**服务管控策略**，单击 **开启禁止服务列表**。



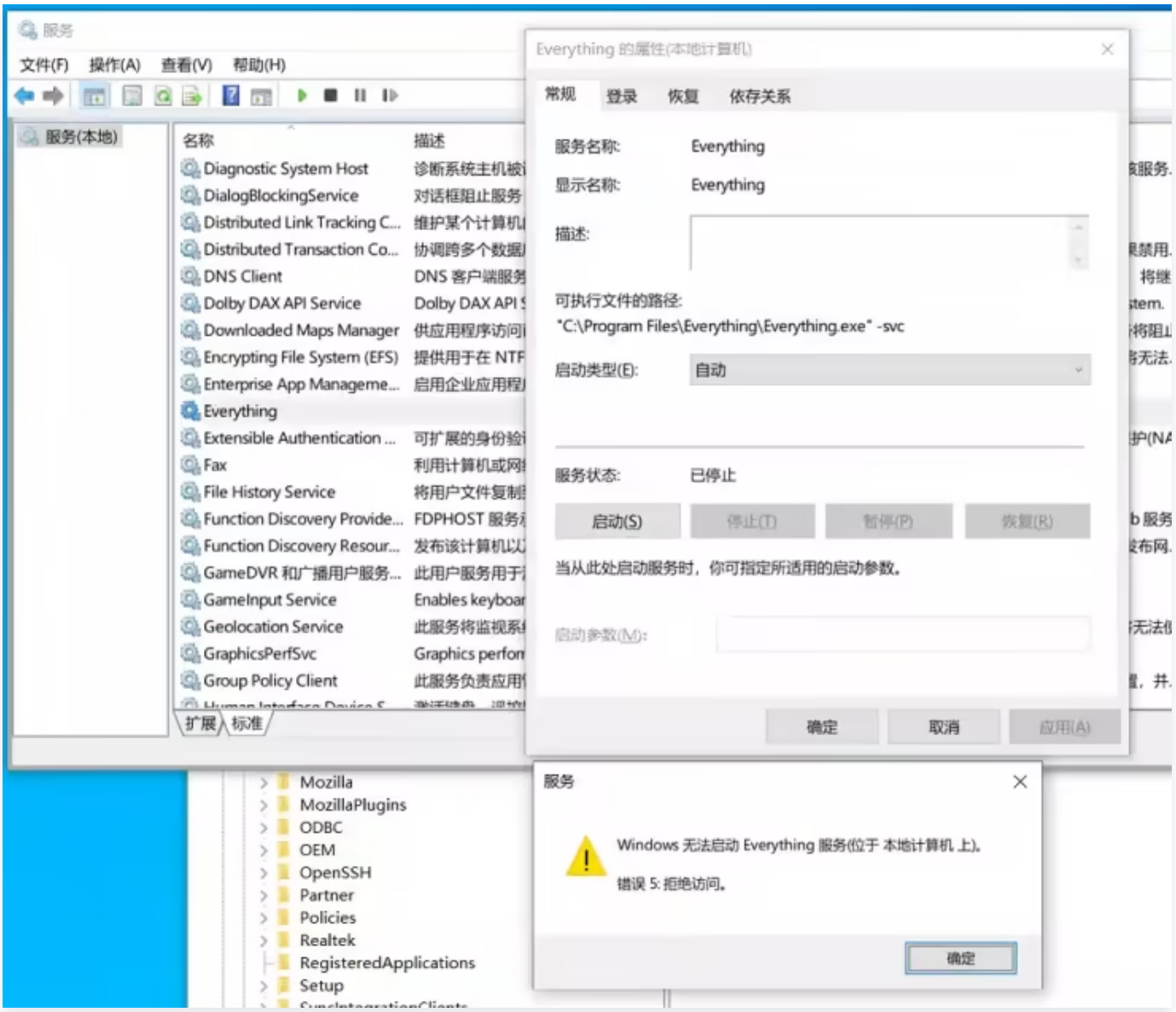
5. 输入服务名（支持通配符），单击**添加**。



6. 配置完成后，单击**保存**。



7. 系统服务运行被禁止并且弹窗提示拒绝访问。


服务
文件(F) 操作(A) 查看(V) 帮助(H)
服务(本地)
名称
描述
Diagnostic System Host
DialogBlockingService
Distributed Link Tracking C...
Distributed Transaction Co...
DNS Client
Dolby DAX API Service
Downloaded Maps Manager
Encrypting File System (EFS)
Enterprise App Manageme...
Everything
Extensible Authentication ...
Fax
File History Service
Function Discovery Provide...
Function Discovery Resour...
GameDVR 和广播用户服务...
GameInput Service
Geolocation Service
GraphicsPerfSvc
Group Policy Client
扩展
标准
Everything 的属性(本地计算机)
常规
登录
恢复
依存关系
服务名称: Everything
显示名称: Everything
描述:
可执行文件的路径:
"C:\Program Files\Everything\Everything.exe" -svc
启动类型(E): 自动
服务状态: 已停止
启动(S)
停止(T)
暂停(P)
恢复(R)
当从此处启动服务时，你可指定所适用的启动参数。
启动参数(M):
确定
取消
应用(A)
Mozilla
MozillaPlugins
ODBC
OEM
OpenSSH
Partner
Policies
Realtek
RegisteredApplications
Setup
服务
Windows 无法启动 Everything 服务(位于 本地计算机 上)。
错误 5: 拒绝访问。
确定

信息采集（11.1.1版）

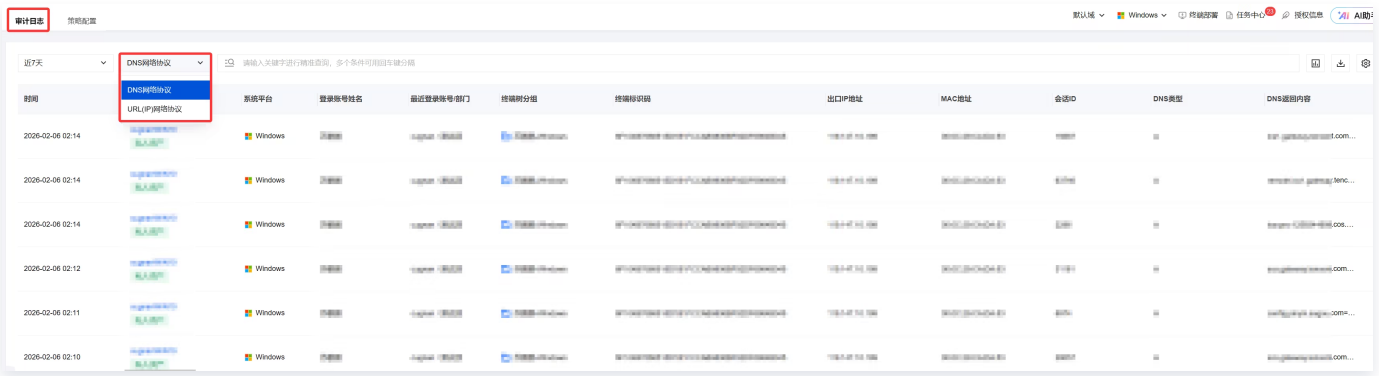
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

采集终端通过 DNS、URL 不同方式访问站点的信息并生成日志。

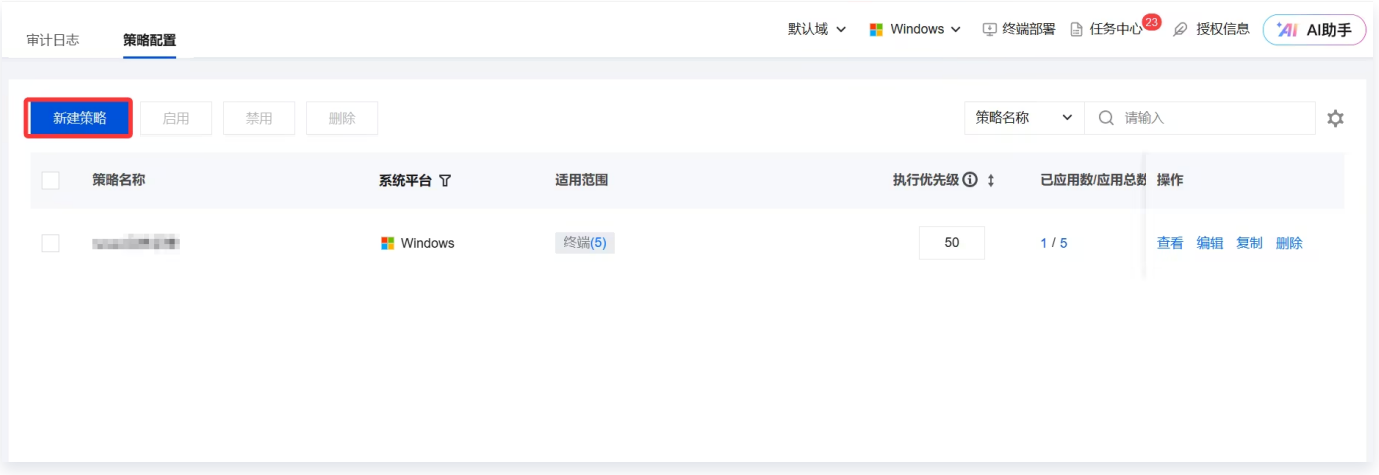
审计日志

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **信息采集**。
2. 在信息采集页，选择**审计日志**，审计日志用于记录和分析终端设备的 DNS（域名系统）解析行为。
3. 支持筛选查看 DNS 网络协议与 URL（IP)）网络协议，在**信息采集** > **策略配置**中审计的网络协议，在此展示。



策略配置

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端管控** > **信息采集**。
2. 在信息采集页面，选择**策略配置**，单击**新建策略**。



3. 在新建策略页面，配置相关参数。

3.1 输入策略名称，并输入策略描述等参数。



3.2 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。

4. 根据实际需求，配置**信息采集**策略，单击**保存**。

> **说明：**
> 采集终端通过 DNS、URL（包括 IP）不同方式访问站点的信息。
> - 白名单：选择白名单后，除了白名单，其他触发了就会采集。
> - 黑名单：选择黑名单后，只采集黑名单。


信息采集策略
终端网络访问日志审计
是否开启审计
审计的网络协议
DNS
URL(包括IP)
审计规则
记录所有终端网络访问日志
白名单
访问的Host地址白名单
Host地址
操作
输入Host地址（示例：test.com或112.0.0.1。支持通配符*）
添加
黑名单

软件管控（ 11.1.1版）
分发管控（ 11.1.1版）

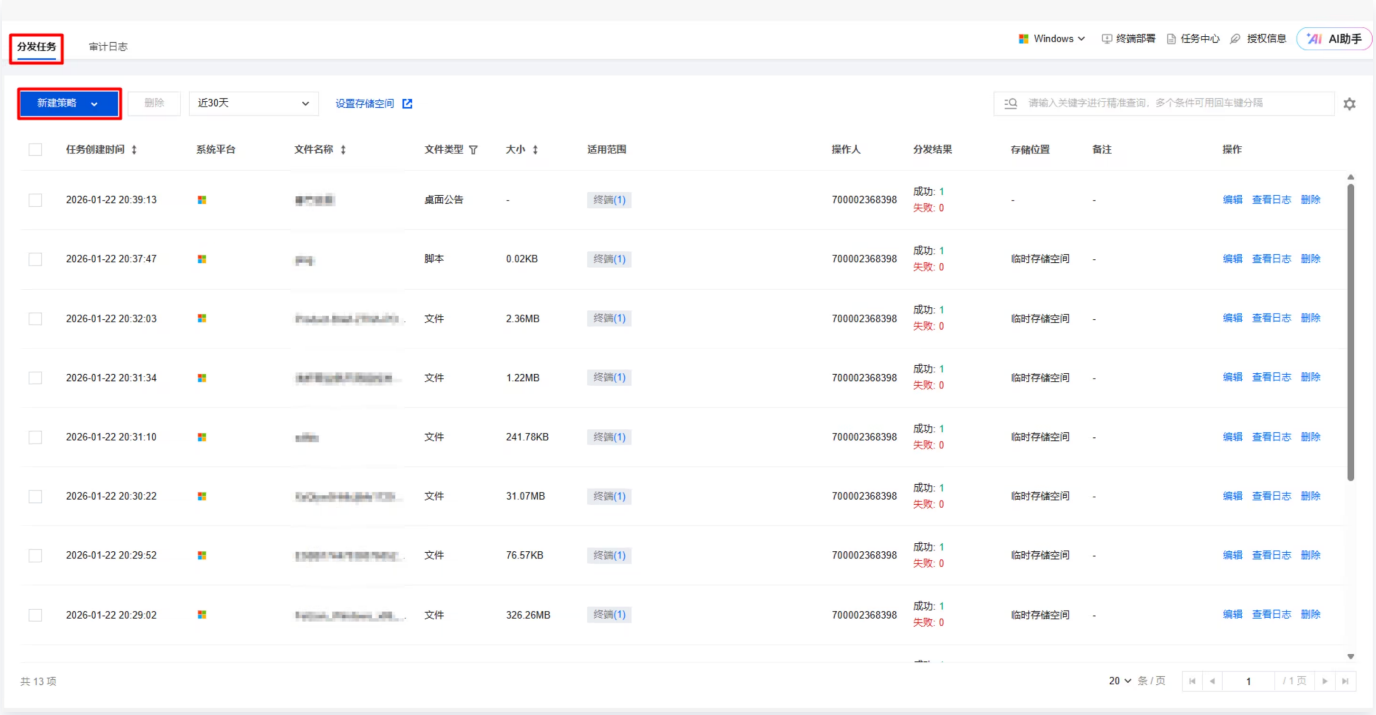
最近更新时间：2026-02-06 14:23:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

支持向指定终端范围统一分发软件、文件、脚本、壁纸、桌面公告、客户端补丁（Windows 支持）。

新建策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**软件管控** > **分发管控** > 分发任务 。
2. 在分发任务页面，单击**新建策略**。



配置项	功能描述
文件分发	• 支持从本地（文件不超过500 MB）进行文件上传，可编辑文件名称、备注等信息。 • 文件分发客户端弹窗样式示例：

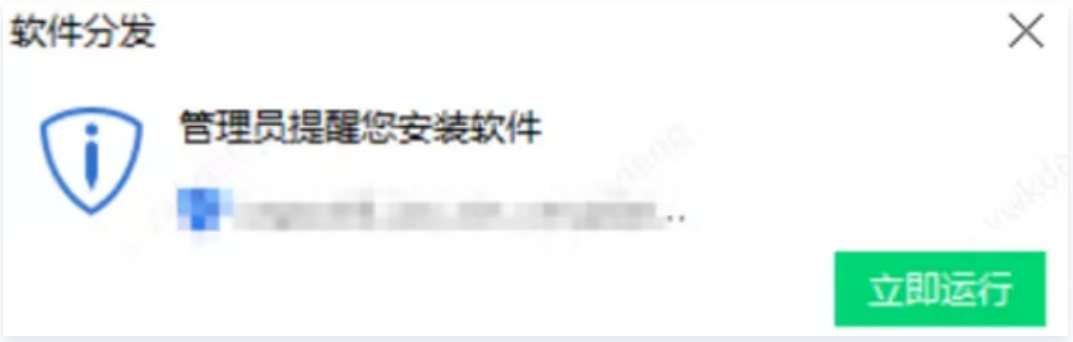


- 分发至终端的文件查看路径（临时路径，也可配置为桌面路径）：
  - Windows：C:\Users\Administrator\AppData\Local\Temp（Administrator是系统账户，根据终端实际系统账户路径查看）。
  - macOS：/Library/Application Support/QQPCiOA/DistributeDocument/software

脚本分发

- 功能：支持从本地选择脚本进行上传，可编辑脚本名称、备注及运行参数。
  - 支持 bat、cmd、vbs、js、exe 类型脚本。
  - 用户权限：在终端所登录的用户态权限下执行脚本或者应用。
  - 系统权限：在系统权限（session0）下执行脚本或者应用。
  - 平台分发脚本后，客户端会下载并执行该脚本，脚本的执行结果取决于终端环境及脚本内容。
- 脚本执行的注意事项：
  - PowerShell 脚本仅支持在 Win7 及以上系统运行。
  - macOS 支持 .sh 格式文件和可执行文件。
  - 脚本编写建议。
    - 脚本名称不包含空格、特殊字符（_除外）或任何非英文字符。例如：一个有效的脚本名称"update_database_2023.sh"。
    - macOS 脚本若涉及到文件保存，推荐保存到/tmp目录中并使用完整路径。pwd:为 iOA 程序包内部目录，切记不要使用"./"。
    - macOS 脚本编写需注意芯片以及运行架构的区分。arch：arch默认参数为"x86_64"。如果需要区分Apple芯片，请在命令行中指定运行模式，例如：arch -arm64 sudo installer -pkg /tmp/xxx.pkg -target /。
- 脚本分发客户端弹窗样式示例：

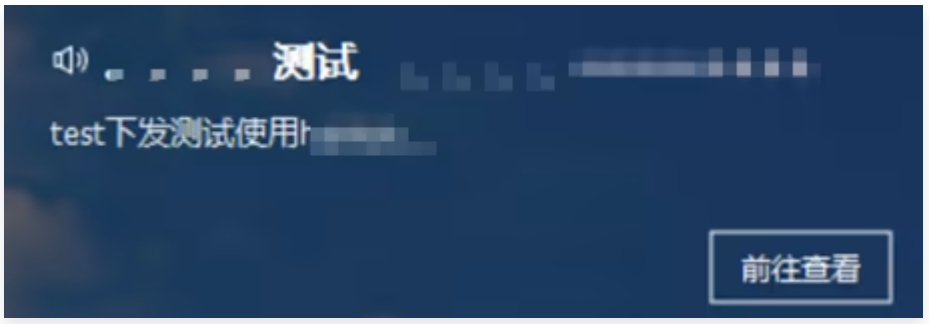


	• 分发至终端的脚本查看路径： ○ Windows：C:\Users\Administrator\AppData\Local\Temp（Administrator是系统账户，根据终端实际系统账户路径查看）。 ○ macOS：/Library/Application Support/QQPCiOA/DistributeDocument/bash
软件分发	• 支持本地软件上传，配置软件名称、备注和运行参数等。 • 软件分发客户端弹窗样式示例：  • 分发至终端的软件查看路径： ○ Windows：C:\Users\Administrator\AppData\Local\Temp（Administrator是系统账户，根据终端实际系统账户路径查看）。 ○ macOS：/Library/Application Support/QQPCiOA/DistributeDocument/software
壁纸分发	• 支持从本地选择文件进行上传，可编辑壁纸名称和备注，选择壁纸契合度。标准屏建议分辨率：1280*1024；宽屏建议分辨率1440*900 。 • 壁纸分发客户端弹窗样式示例：  • 单击**确定**后，电脑壁纸更换为分发的壁纸。 • 分发至终端的壁纸查看路径： ○ Windows：C:\ProgramData\Tencent\DeskUpdate\WallPaper ○ macOS：/Library/Application Support/QQPCiOA/DistributeDocument/software
客户端补丁分发	• 补丁包由厂商官方提供，用于修复客户端 bug。 • 支持的补丁类型包含：dat，最新补丁包总是兼容之前已发布过的所有补丁包内容。 • 客户端补丁样式示例：



桌面公告分发

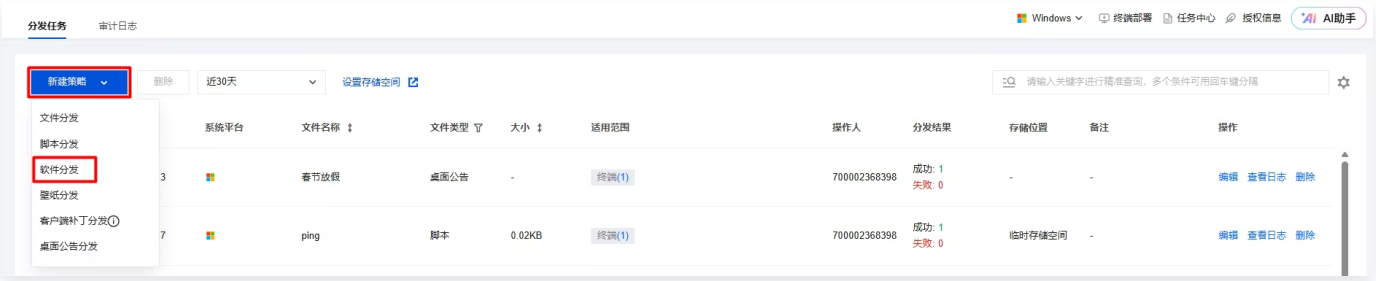
- 支持下发常驻公告、弹窗公告，便于员工在公告投放期间获悉公告内容。
- 常驻公告：公告浮窗将在投放时间内始终展示于终端桌面右上角，常驻公告样式示例：



- 弹窗公告：将即时下发至用户端桌面右下角，投放时间内每台设备仅触发一次，用户可确认关闭。弹窗公告样式示例：



3. **示例：**新建软件分发策略。

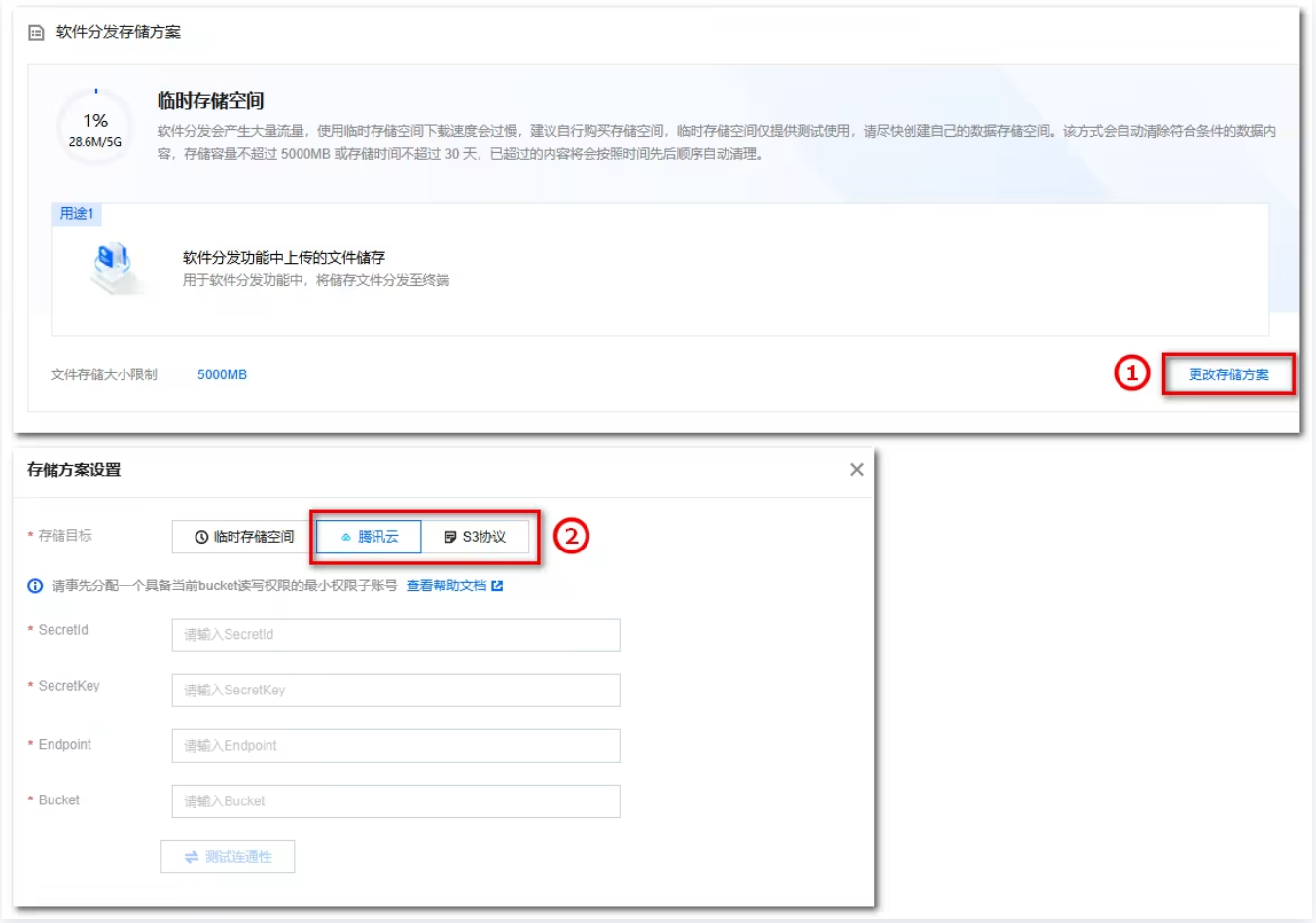


4. 在新建软件分发策略页面，单击**设置存储空间**。



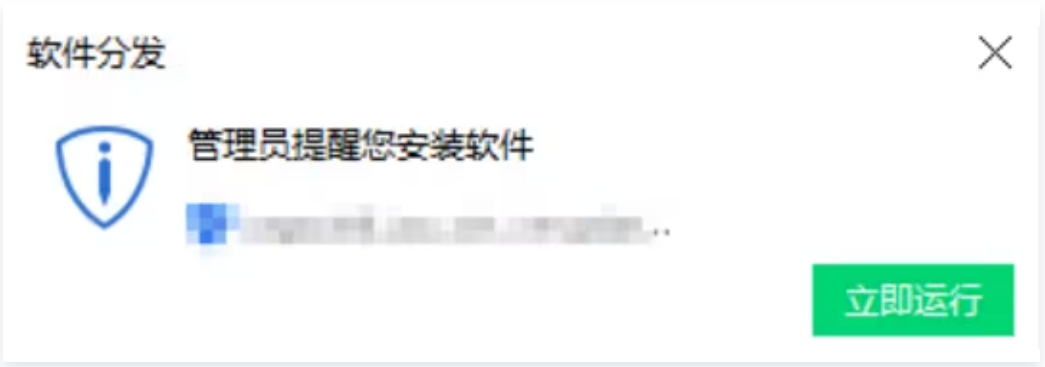
5. 在存储空间页面，单击**更改存储方案**，根据需求选择 腾讯云 和 S3协议 。

> **注意：**
> 临时存储空间：临时存储空间仅提供测试使用，请尽快使用自己的数据存储空间。



6. 在新建软件分发策略页面，依据参数配置如下基本信息：

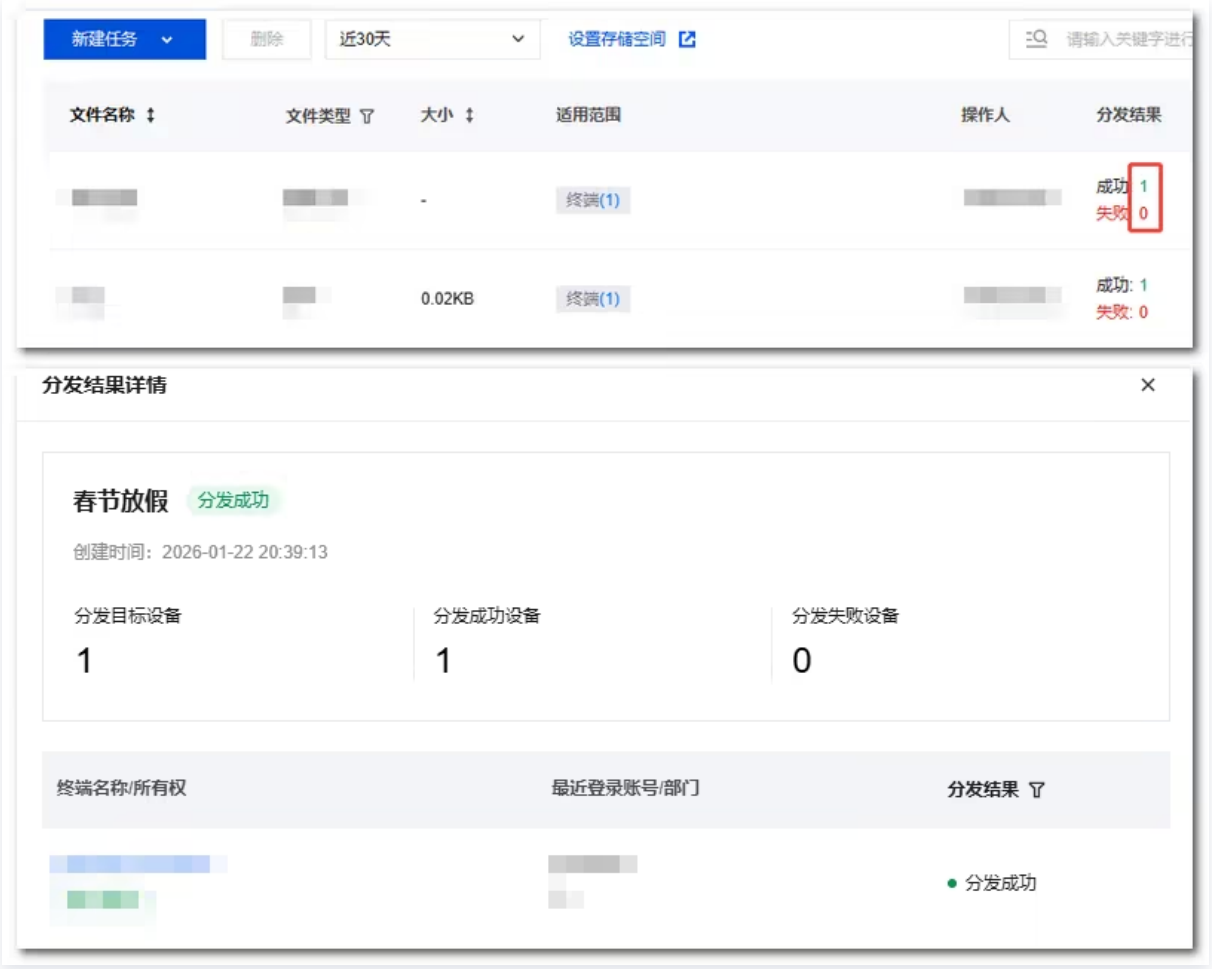
参数名称	说明
选择软件	点击本地文件，上传软件安装包。
软件名称	自定义。
软件备注	自定义。
运行参数	软件静默安装的运行参数，/S 或 /silent 或 /quiet：这些参数通常用于启动静默安装模式。软件将自动安装，不显示任何用户界面。
DisplayName	在测试机器手动安装软件，打开**控制面板** > **程序和功能**，找到目标软件名称，该名称即为 DisplayName。
特定注册表	填写安装软件一定会写入注册表，可参考以下注册表项，XXX 是软件名称。 HKEY_LOCAL_MACHINE\SOFTWARE\XXX HKEY_CURRENT_USER\SOFTWARE\XXX HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\XXX HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\XXX

	例如： 安装 QQ 时会写入 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\XXX 可在特定注册表输入以下内容： SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\XXX 如果是32位程序则是 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\XXX 可在特定注册表输入以下内容，两个注册表都会进行搜索。 SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\XXX 或者 SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\XXX
安装弹窗提醒	设置是否弹窗提醒用户分发消息。 
适用范围	添加需要分发软件的用户/终端。

7. 确认内容无误后，单击**保存**。
8. 在分发管控页面，查看分发状态：
   - 分发成功：当前分发范围内，已分发成功的终端/用户数。
   - 分发失败：当前分发范围内，已分发失败的终端/用户数。



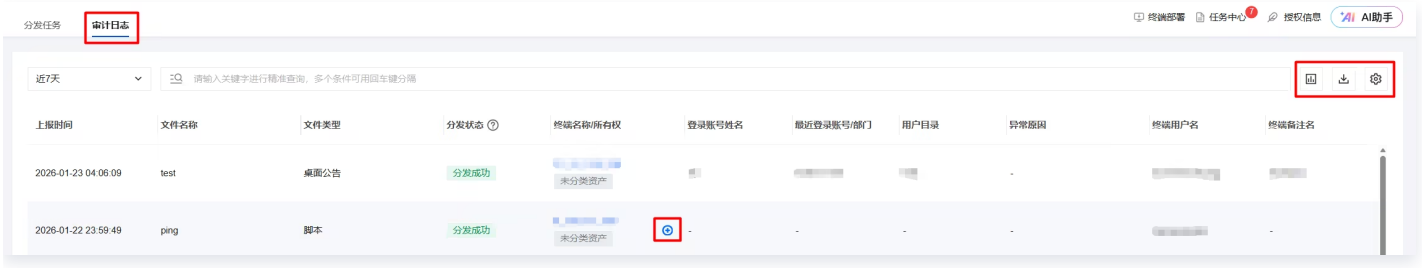
   - 分发详情：点击对应的分发结果数字，可查看分发结果详情。



审计日志

帮助企业 IT 管理员及时发现软件下发情况，为软件资产管理提供数据支持。

进入**软件管控** > **软件安装** > **审计日志** 。



软件分发审计覆盖所有 Windows、macOS 终端的分发行为。

图标	图标含义
	支持快速选择预设时间段（最近7天/近10天/近30天），支持自定义精确时间范围。

	数据统计图表以柱状图形式展示
	支持将审计数据导出为文件，便于离线分析。
	支持自定义展示报表字段
	支持快速搜索并展示报表内的相同内容

版权所有：腾讯云计算（北京）有限责任公司

运行管控（ 11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

管理员可创建软件禁止运行策略，限制特定软件运行，规范软件的安装与使用，实现对员工终端软件的统一管控。

1. 登录iOA 零信任管理平台控制台，在左侧导航栏，选择**软件管控** > 运行管控 。
2. 在运行管控页面，选择**策略设置**，单击**新建策略**。

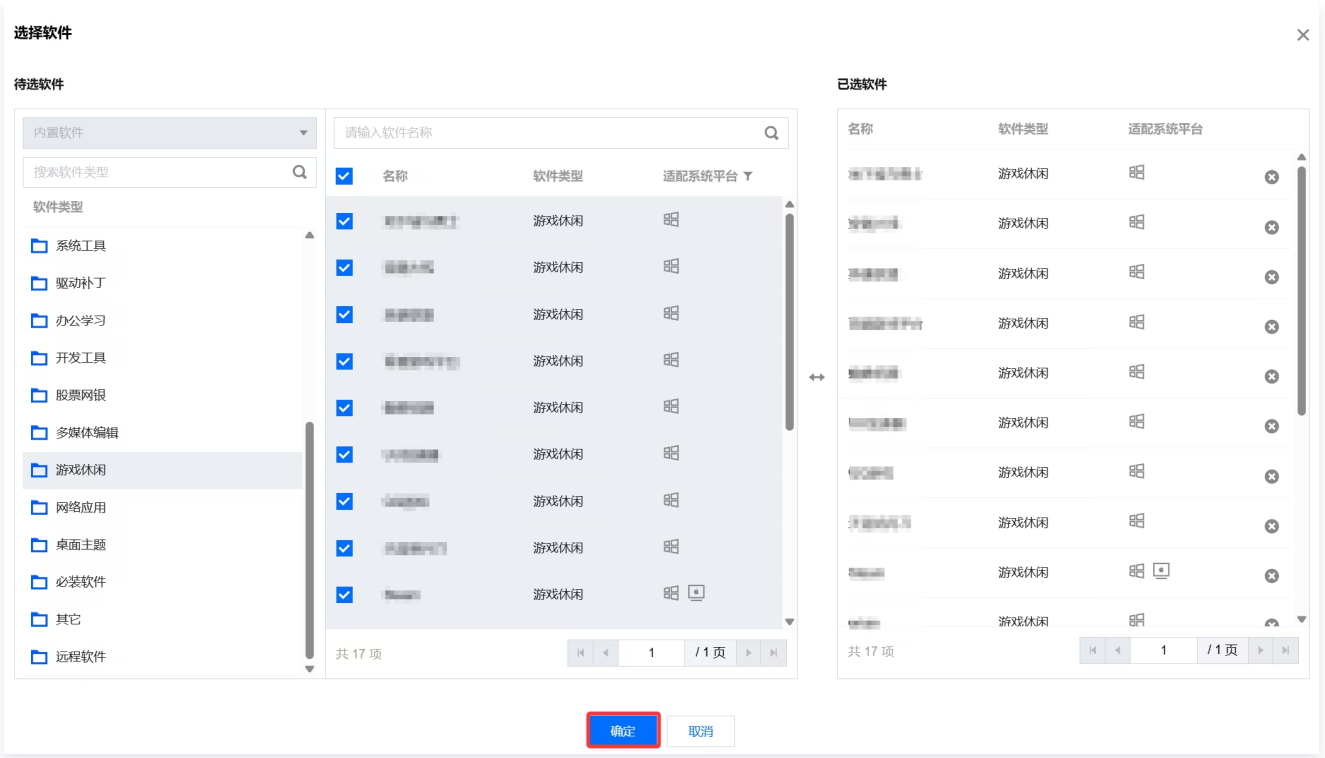


3. 配置软件禁止运行策略基本信息。
   3.1 输入策略名称，并输入策略描述等参数。

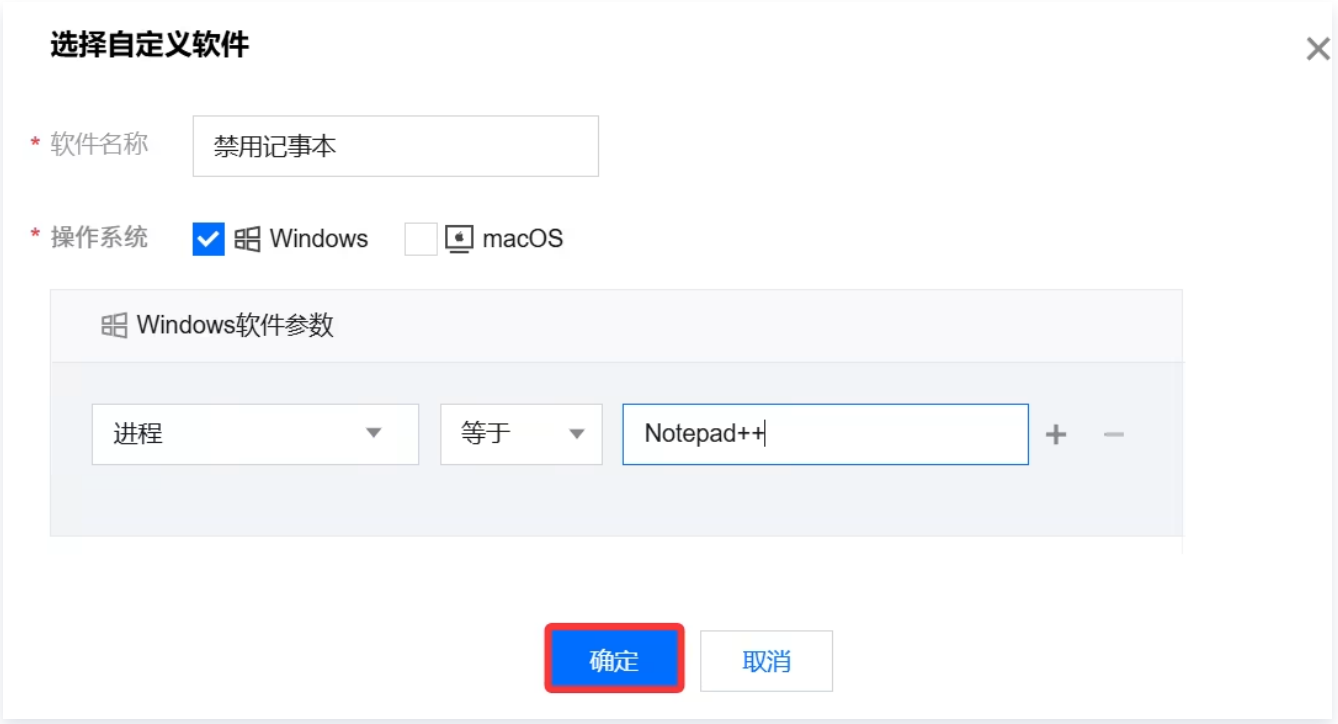


3.2 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。

4. **禁止运行管控软件：支持选择内置软件、自定义软件。**
   - **内置软件：系统内置的一些软件，可直接勾选需管控的软件并单击确定。**



- **自定义软件：配置相关参数，单击确定。**



参数名称	说明
软件名称	自定义。
操作系统	选择 Windows 或 macOS，选择后该系统下禁止运行自定义软件。

进程	填写该软件的进程名称。
进程签名	签名信息通过特定的加密算法生成一个唯一的签名值，操作系统或其他安全工具可以通过验证这个签名值来确认该进程是否由***有限公司发布，是否被篡改过，从而判断其可信度。
进程描述	该软件的进程描述信息。

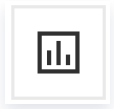
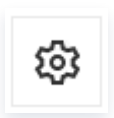
5. 终端验证，打开 Notepad++软件，提示禁止运行。

审计日志

帮助企业 IT 管理员及时发现违规运行行为，为软件资产管理提供数据支持。
进入**软件管控 > 运行管控 >** 拦截日志 **。**



审计覆盖所有 Windows、macOS 终端的拦截行为。

图标	图标含义
	支持快速选择预设时间段（最近7天/近10天/近30天），支持自定义精确时间范围。
	数据统计图表以柱状图形式展示。
	支持将审计数据导出为文件，便于离线分析。
	支持自定义展示报表字段。

	支持快速搜索并展示报表内的相同内容。

版权所有：腾讯云计算（北京）有限责任公司

安装管控（11.1.1版）

最近更新时间：2026-02-13 17:55:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

软件安装管控策略用于管理企业内部软件安装规则，确保只有经过验证的软件才能被安装在公司的计算机上，降低安全风险。系统提供了灵活的管控方式，包括安装黑名单模式和白名单模式，白名单模式下提供对非白名单软件安装的拦截、审计两种处置方式，以实现在多重场景下能确保软件安装规则符合公司的安全政策。

- 软件合规与安全提升场景：通过建立规范的软件使用流程和管理机制，要求员工从官方渠道或企业软件库下载安装软件，杜绝私自安装违规、盗版、来源不明或含恶意代码的软件，降低安全风险和合规风险。
- 办公效率提升场景：支持禁止员工在办公电脑上安装远程控制、娱乐等非工作相关软件，提高工作效率。

> **说明：**
> 软件安装功能要求客户端版本10.10.1及以上支持该功能，如客户端版本低于10.10.1请升级客户端。

软件安装策略

1. 登录 iOA 零信任管理平台控制台 ，在左侧导航栏，选择**软件管控** > 安装管控 。
2. 在安装管控页面，选择策略设置，单击**新建策略**。



3. 在新建软件安装策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。



3.2 单击添加适用范围，勾选需管控/排除的用户/终端名称。

3.3 勾选需要管控的动作仅审计或禁止安装，单击保存。

仅审计

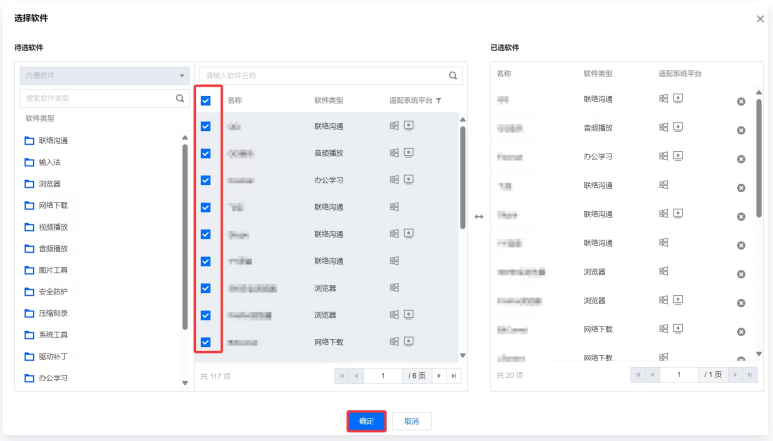
允许软件安装，安装记录将会自动上报至 审计日志 中。

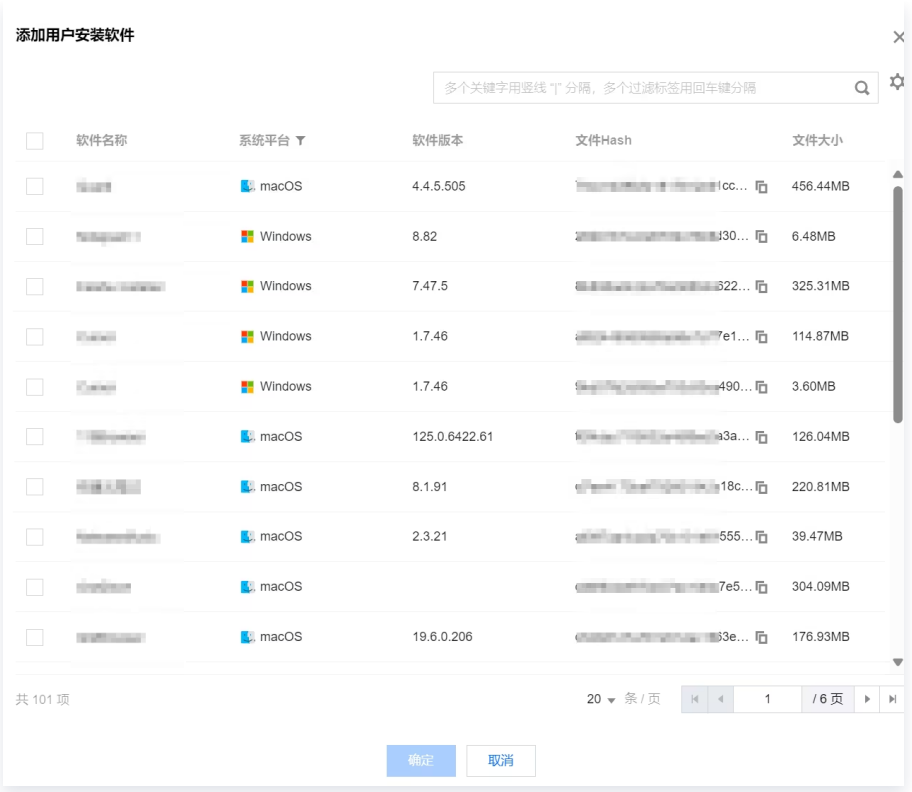


禁止安装

禁装软件列表

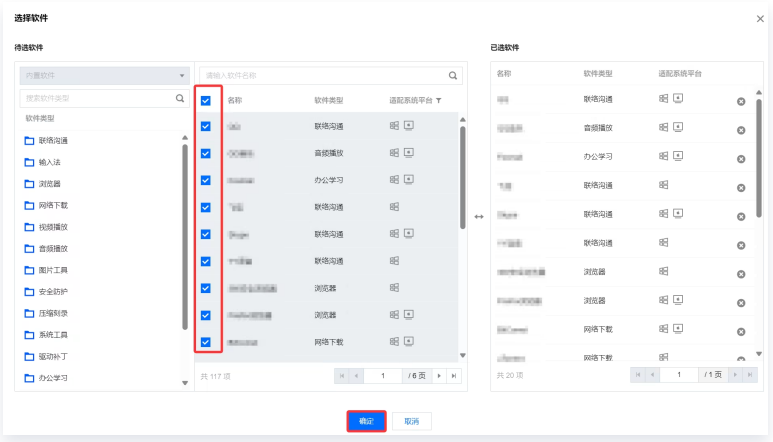
1. 管控范围内的软件，将被禁止安装，并自动上报审计日志。
   - 全部软件：禁止所有软件安装至终端。
   - 指定软件：添加禁装软件列表，可配置内置软件、自定义软件、用户安装软件。

类别	说明
内置软件	勾选 iOA 内置的禁装软件，勾选后单击**确定**保存。 
自定义软件	• 软件名称：自定义。 • 操作系统：勾选 Windows/macOS，勾选后可配置禁装软件参数。 
用户安装软件	初始化时没有软件，当软件安装策略下发至终端后，终端会审计员工的安装行为，采集并解析软件信息。成功安装的软件将被上报至用户安装软件列表。



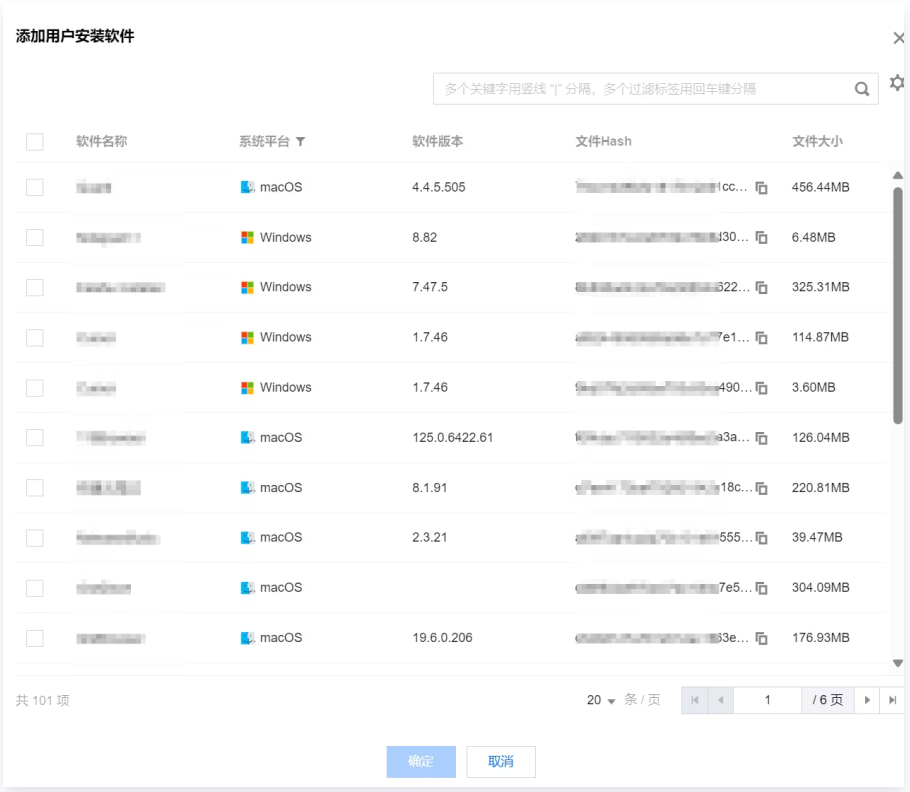
禁装软件白名单

1. 针对已禁用软件设置例外规则，允许指定范围内的软件执行安装操作。
   - 指定下载渠道的软件：勾选后，允许指定渠道的软件进行安装，若勾选软件仓库，则管理员在控制台上架软件后，员工即可在客户端软件仓库下载。
   - 指定例外软件：添加禁装软件白名单列表，可配置内置软件、自定义软件、用户安装软件、软件仓库。

类别	说明
内置软件	勾选 iOA 内置的禁装软件，勾选后单击**确定**保存。
自定义软件	• 软件名称：自定义。 • 操作系统：勾选 Windows/macOS，勾选后可配置禁装软件参数。



用户安装软件	初始化时没有软件，当软件安装策略下发至终端后，终端会审计员工的安装行为，采集并解析软件信息。成功安装的软件将被上报至用户安装软件列表。
软件仓库	在**软件管理** > **软件仓库**上架的软件信息在此展示，勾选软件名称后单击**确定**保存。





弹窗提醒

支持开启客户端提醒：当员工安装不允许的软件时，对员工进行提示。

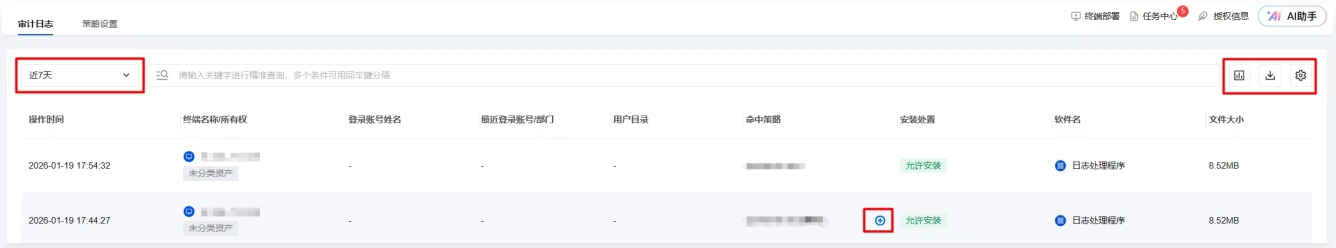


审计日志

帮助企业 IT 管理员及时发现违规安装行为，为软件资产管理提供数据支持。

1. 登录 iOA 零信任管理平台控制台 ，在左侧导航栏，选择安装管控 > 审计日志 。

2. 软件安装审计覆盖所有 Windows、macOS 终端的软件安装行为。



图标	图标含义
近7天	支持快速选择预设时间段（最近7天/近10天/近30天），支持自定义精确时间范围。
	数据统计图表以柱状图形式展示。
	支持将审计数据导出为文件，便于离线分析。
	支持自定义展示报表的字段。
	支持快速搜索并展示报表内的相同内容。

3. 软件安装记录列表展示详细的安装审计信息，包括：
   - 操作时间：软件安装的具体时间。
   - 命中策略：触发的安全策略名称。
   - 安装处置：允许安装或禁止安装。
   - 软件名称：安装的软件标识。
   - 文件大小：软件安装包大小。
   - 终端信息：安装设备的标识。

版权所有：腾讯云计算（北京）有限责任公司

软件卸载（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**软件管控** > 软件卸载 。
2. 在软件卸载页面，选择**策略设置**，单击**新建任务**。



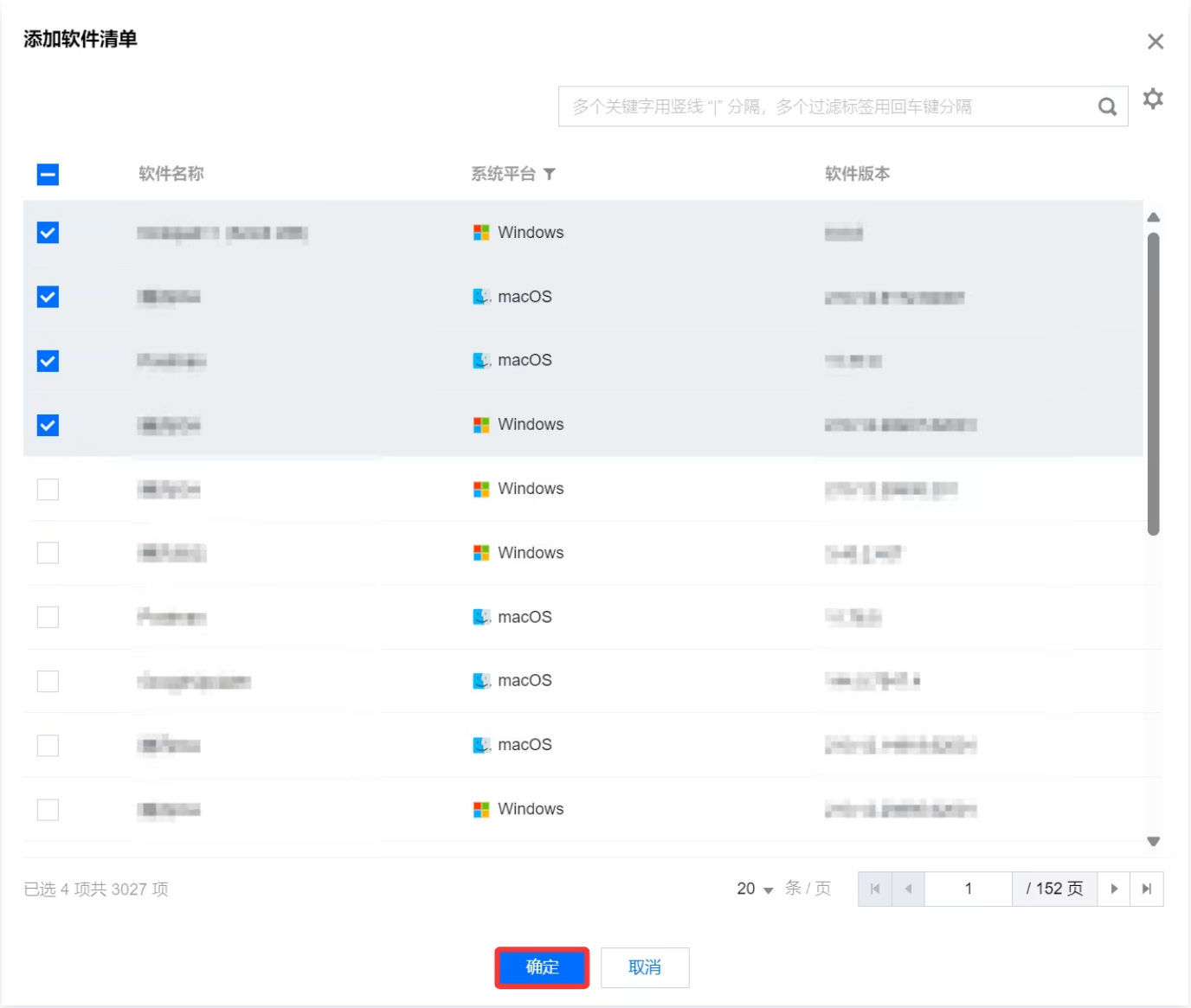
3. 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。



4. 在卸载软件中，单击**选择软件**，从软件清单中勾选需卸载的软件。



5. 在添加软件清单弹窗中，勾选需卸载的软件后单击**确定**保存。



6. 卸载方式支持静默卸载、提醒卸载：

- 静默卸载：输入静默卸载参数，例如 “/S”，可通过“参数查找指引”查看静默卸载方式。

> **说明：**
> 软件静默卸载功能需要卸载的软件本身支持静默卸载。



- **提醒卸载：选择提醒卸载并配置终端提示语后单击保存，客户端弹窗通知用户，用户确认后系统执行卸载程序。**



7. 客户端弹窗示例：


腾讯 iOA
以下软件不符合公司安全规范，已完成卸载！
我知道了

终端防入侵（11.1.1版）
病毒查杀（11.1.1版）
策略配置（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

按策略模板配置

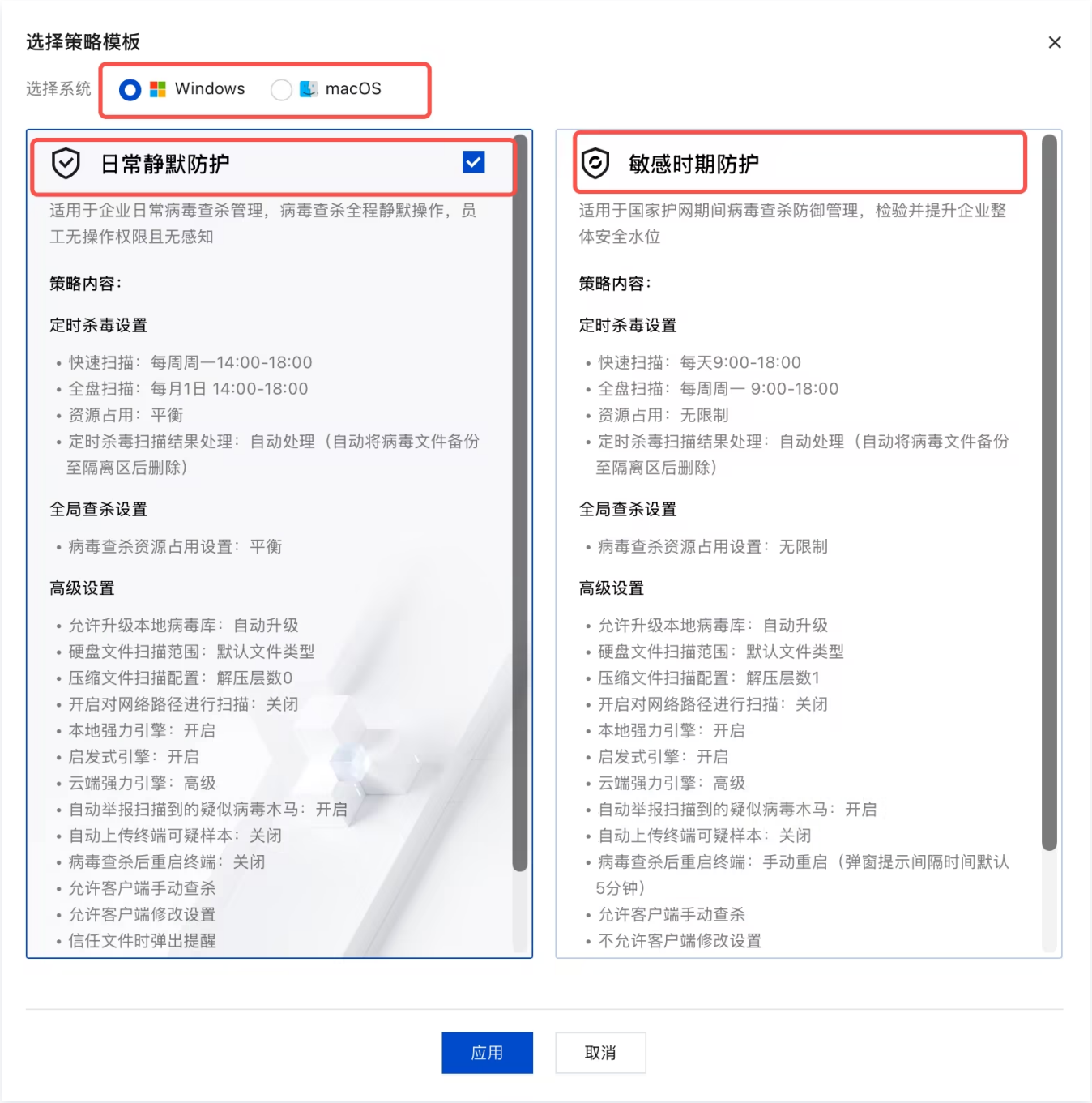
> **说明：**
> 杀毒属于最重要的安全防护策略之一，iOA 已为您提供默认的基线策略，基线策略可在**病毒查杀 > 策略配置**处查看，如需新建策略，请参考下述步骤。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 病毒查杀 > 策略配置**，单击**策略模板**。

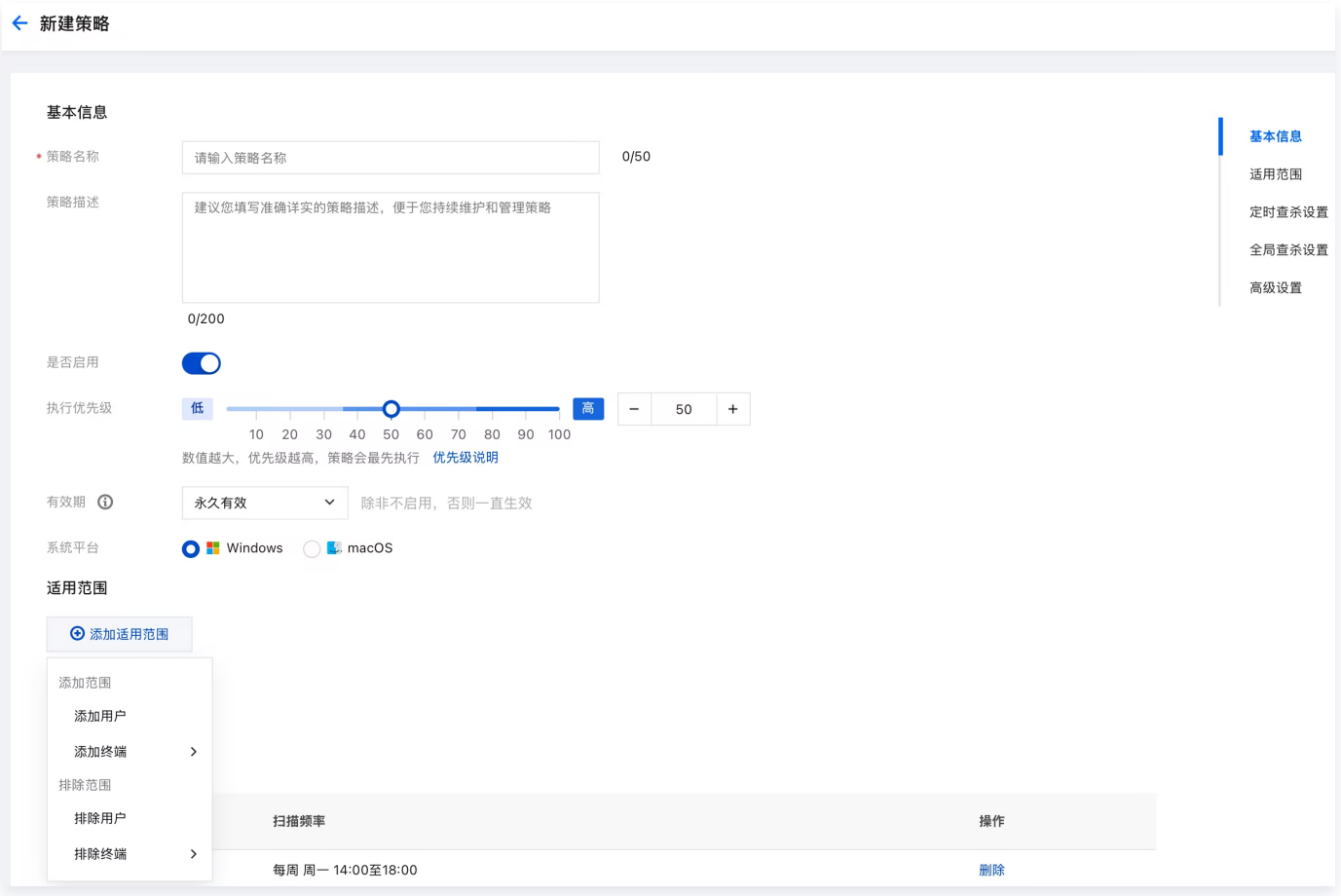


2. 根据需求，勾选 **Windows 或 macOS**，以及选择**日常静默防护**或**敏感时期防护**，单击**应用**。
   - 日常静默防护：适用于企业日常病毒查杀管理，病毒查杀全程静默操作，员工无操作权限且无感知。
   - 敏感时期防护：适用于护网攻防演练期间病毒查杀防御管理，检验并提升企业整体安全水位。

版权所有：腾讯云计算（北京）有限责任公司



3. **在策略编辑页面，输入策略名称、策略描述、优先级等参数，单击添加适用范围，勾选需管控/排除的用户/终端，单击确定。**



4. 配置好以上参数后，单击**保存**即可，**其他相关配置可以按照系统默认推荐配置**。

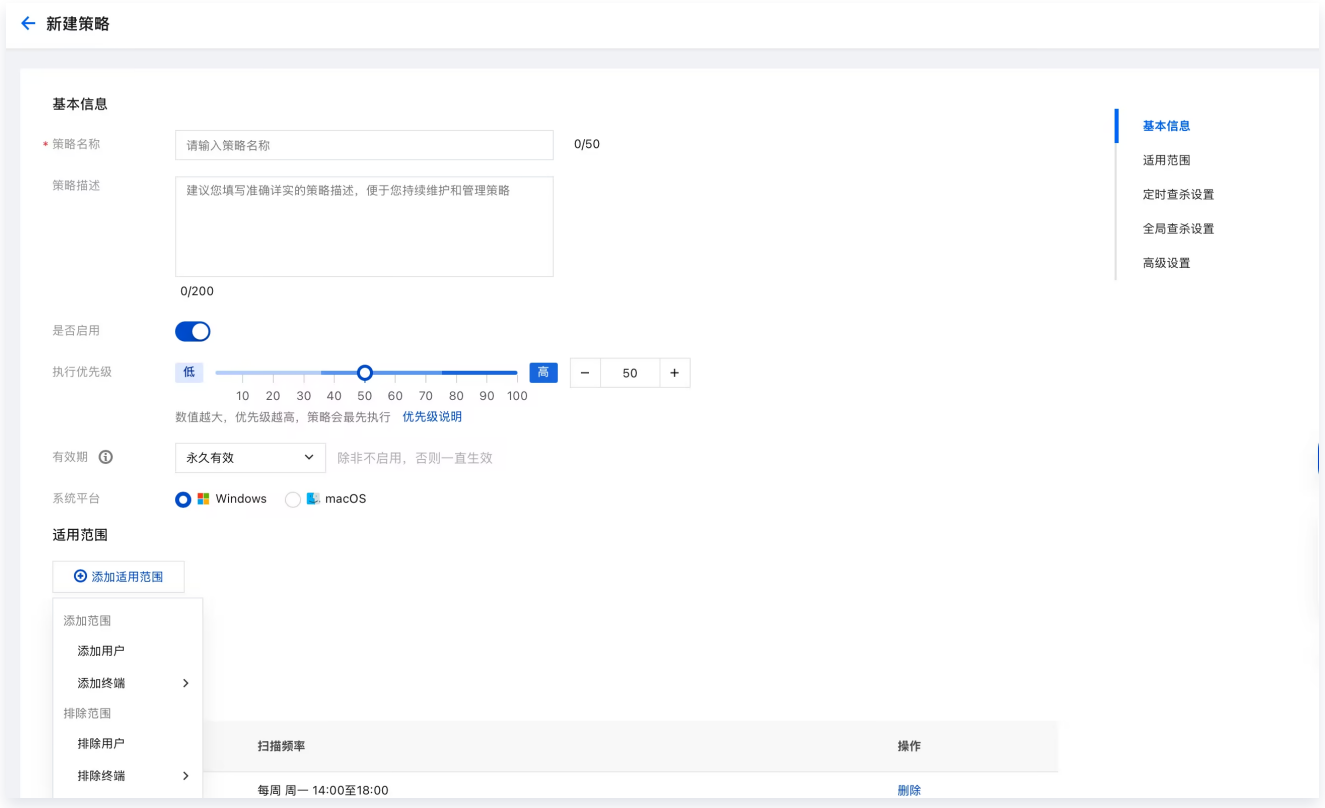
新建自定义策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **病毒查杀** > **策略配置**，单击**新建策略**。



2. 在策略编辑页面，填写策略名称、策略描述、执行优先级、勾选 Windows 或 macOS，单击**添加适用范围**，勾选需管控/排除的用户/终端，单击**确定**。

版权所有：腾讯云计算（北京）有限责任公司



3. 根据需求，配置下面定时查杀、全局查杀策略配置及高级设置。

热点问题

同时创建多个策略如何生效?

多个策略同时存在时，可能出现一个用户或终端同时命中多条策略的情况，系统执行多个策略合并生效逻辑，不同策略设置的策略项若存在冲突，此时系统将通过优先级来决定如何执行策略。
例如：同时设置 A、B 两条策略，均命中某终端 X，其中A策略开启了「病毒库升级设置」和「资源占用设置」，B策略仅开启了「病毒库升级设置」，由于「资源占用设置」无策略冲突，那么终端 X 对应资源占用策略项会按照 A 策略的设置生效，而「病毒库升级设置」有策略冲突，那么终端 X 的病毒库升级设置项会按照 A、B 策略优先级更高的策略设置生效。

> **说明：**
> 黑白名单如果在 A、B 策略中有不同设置内容，则均会对终端 X 生效，不区分优先级。

执行优先级的逻辑是什么?

- 优先级数字越大，策略越优先执行；
- 优先级可配置的范围是1~100；
- 优先级允许相同，将通过系统内置的优选策略执行；
- 兜底的全局基线策略优先级为0，不允许修改。

系统内置优选策略逻辑是什么?

系统内置优选对比维度包含：策略管控对象、策略严格度、策略创建时间。

- 策略管控对象：粒度越精准越优先，单个终端/用户>自定义组>组织架构；
- 策略严格度：策略项内配置的越严格，越优先；
- 策略创建时间：策略越新创建，越优先执行。

定时查杀设置

病毒查杀的定时任务，到点自动扫描，支持如下三种功能：

- 快速扫描：也称为“闪电杀毒”，仅扫描系统关键位置、关键内存、注册表及其他活跃区域。耗时较短。推荐快速扫描设置每天任务。
- 全盘扫描：扫描系统整个磁盘路径、内存、注册表。耗时比较长，一般是快速扫描的20倍耗时左右。推荐全盘扫描设置每周任务。
- 定时杀毒时客户端资源占用：杀毒会占用客户端性能，可以使用“平衡”模式或“低占用”模式，采用平滑的方式，来降低对企业员工的办公效率影响，但是会耗费更长的时间。如果需要更快完成任务，不担心性能损耗带来的影响，可以使用“无限制”模式。
- 定时查杀处置设置：
  - 自动处理：自动将病毒文件备份至隔离区后删除（备份至隔离区的文件可以在 iOA 客户端**病毒查杀 > 信任管理 > 隔离区**进行恢复）。
  - 仅扫描：扫描后，病毒文件将不被处理，扫描结果仅用于风险摸底。

> **说明：**
> 建议选择自动处理（推荐），备份到隔离区的病毒，将不再具有安全威胁。



全局查杀设置

- 黑白名单设置：

- 针对 iOA 客户端病毒查杀或实时防护的风险，为防止误报，可以添加白名单；白名单支持加白递归子文件夹，支持对文件夹下更深路径进行扫描但不上报病毒，支持对防钓鱼相关策略生效。
- 针对 iOA 客户端病毒查杀或实时防护的风险，可以设置黑名单，禁止黑样本在企业内部流传。



- 参数说明

参数名称	说明
文件与路径白名单	加白文件所在路径。如：C:\Program Files\App\ (路径) 、C:\tool.exe (文件) 。
扩展名白名单	针对文件扩展名进行加白。（如：.dll、.ps1、.txt 、.zip 等）
MD5白名单	支持上传文件自动提取 MD5 值并进行加白。
注册表白名单	针对注册表进行加白。如：HKEY_CURRENT_USER\Software\App\ (路径)。
URL/IP地址白名单	如：http://internal-tool.com/10.0.0.1。
风险名白名单	输入安全软件识别的风险名称。如：Malware.Win32.Gencirc.abcd。

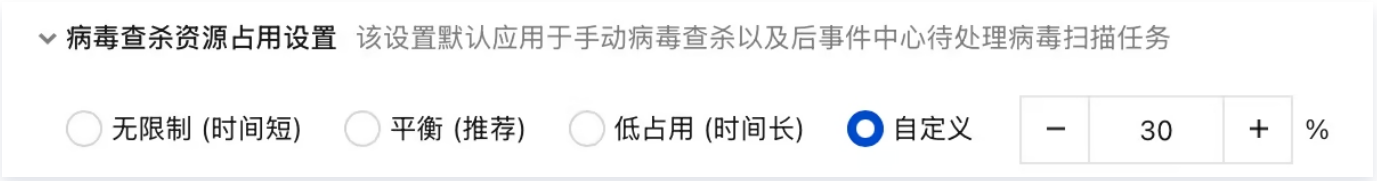
- 典型使用场景

场景类型	说明
内部工具/脚本信任	• 场景：企业自研脚本（如.ps1）被误报病毒 • 加白方式： 文件路径白名单 （添加脚本路径）或 MD5白名单 （精确匹配文件指纹）。
开发/测试环境豁免	• 场景：开发中的程序频繁触发安全警报。

	• 加白方式： 扩展名白名单（如临时文件.tmp）或注册表白名单（调试用注册表键值）。
误报排除	• 场景：安全软件将正规软件（如某财务系统）报毒。 • 加白方式： 风险名白名单（添加误报的病毒名称）或 MD5白名单（标记可信文件）。
内部服务访问放行	• 场景：内部系统 URL/IP 被拦截（如监控平台 http://192.168.1.50）。 • 加白方式： URL/IP 地址白名单（添加服务地址）。
自动化流程防干扰	• 场景：自动安装程序被中断。 • 加白方式： 文件与路径白名单（添加安装包路径）或注册表白名单（安装所需的注册表项）。

- **病毒查杀资源占用设置：**

  支持用户自定义病毒查杀占用的 CPU 资源，客户端手动病毒查杀时，CPU 占用率控制台可控。配置杀毒资源占用率，有效改善用户 CPU 和磁盘使用问题。



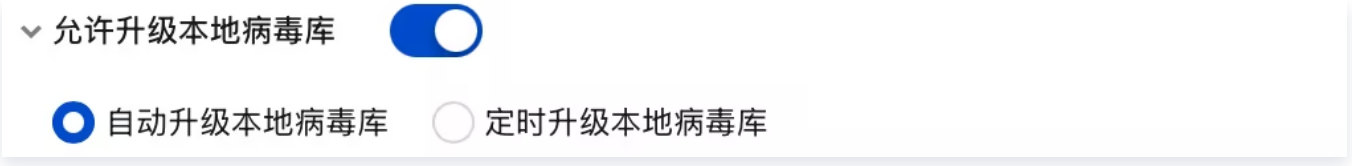
高级设置

根据实际需求，选择如下高级设置后，单击保存。



本地病毒库升级设置

- **自动升级本地病毒库：采用自动平滑策略，每天多次尝试更新病毒库，通常频率为每4小时左右。**
- **定时升级本地病毒库：按时间定时升级。**



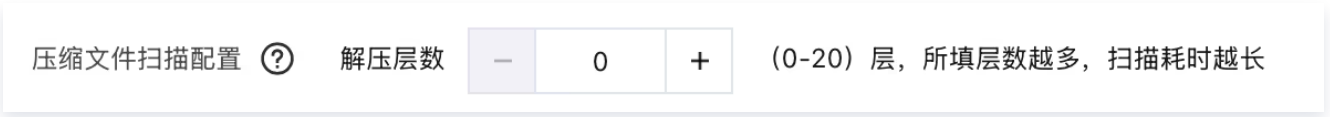
扫描设置

- **硬盘文件扫描范围**
  - **支持无后缀或特定后缀文件的文件落盘查杀。**

- 支持通过添加文件后缀名，扩展可选择的扫描范围。该范围将影响：控制台手动下发全盘查杀任务、定时查杀策略中自动全盘查杀、客户端手动全盘杀毒。



- 压缩文件扫描配置
  - 该配置影响范围：
    - 控制台下发查杀任务及定时查杀策略中的全盘查杀模式（闪电扫描不解压扫描）。
    - 客户端手动全盘杀毒（闪电杀毒不解压扫描）。
    - 客户端指定位置杀毒和用户右键扫描压缩文件时不受该配置影响，仅支持解压3层扫描。
  - 解压层数说明：
    - 解压层数填为0时，将不对压缩文件进行解压，直接扫描，性能影响最小。
    - 解压层数为1~20时，将对压缩文件进行逐层解压后扫描，需解压的层数越多，性能影响越大。
  - 扫描限制：
    - 不支持对带密码的压缩包自动解压扫描。
    - 不支持100M以上的压缩包扫描（用户右键扫描压缩文件时，不受该大小限制）。



- 网络路径扫描

  开启后，客户端处将会枚举显示网络挂载盘路径，允许管理员后台下发任务和终端用户自行开启对网络路径进行扫描。

> **注意：**
> 请避免多用户同时发起网络路径扫描。



病毒查杀引擎设置

选择病毒查杀等级。等级越高，防护范畴越广，但是可能产生部分误报。

- 本地强力引擎：开启后，本地杀毒引擎能力增强，能识别更多未知病毒样本，但可能会带来少量误报。

- 启发式引擎：开启后，本地杀毒引擎对宏病毒识别能力增强（例如：识别 Office 文件中的宏是否带病毒），但可能会带来少量误报。
- 云端强力引擎：开启后，云端杀毒引擎对灰样本识别能力大幅增强并可动态调整查杀力度，识别更多未知病毒样本，但可能会带来误报。
  - 标准：对于高可疑的灰样本进行检出（检出量更小）。
  - 高级：对于低可疑的灰样本进行检出（检出量更大）。

> **说明：**
> 建议开启，即使误报，也能从隔离区中找回文档。



病毒云查杀计划

当智能行为引擎判断出可疑病毒时，是否允许将病毒信息上传至 iOA 后台（不涉及用户隐私）。



客户端设置

- 病毒查杀后重启设置
  - 手动重启：定时查杀扫描完成后弹窗提示用户，需用户手动重启电脑。
  - 自动重启：定时扫描完成，弹窗提示用户。用户未操作则按设置时间强制重启，选择稍后提示则重启前按设置间隔重复弹窗。



- **允许客户端手动查杀**



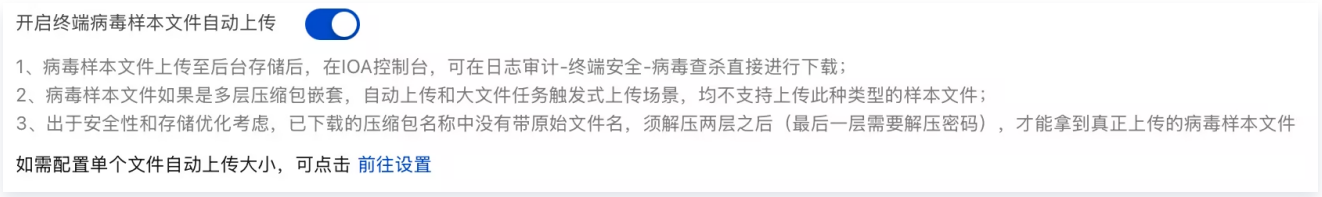
- **风险项信任操作提醒**
  - **允许客户端修改设置：开启后客户端支持彻底删除/恢复风险项。**
  - **信任文件操作时弹出提醒：用户选择信任检测出的风险文件时，将弹出二次确认提醒。**



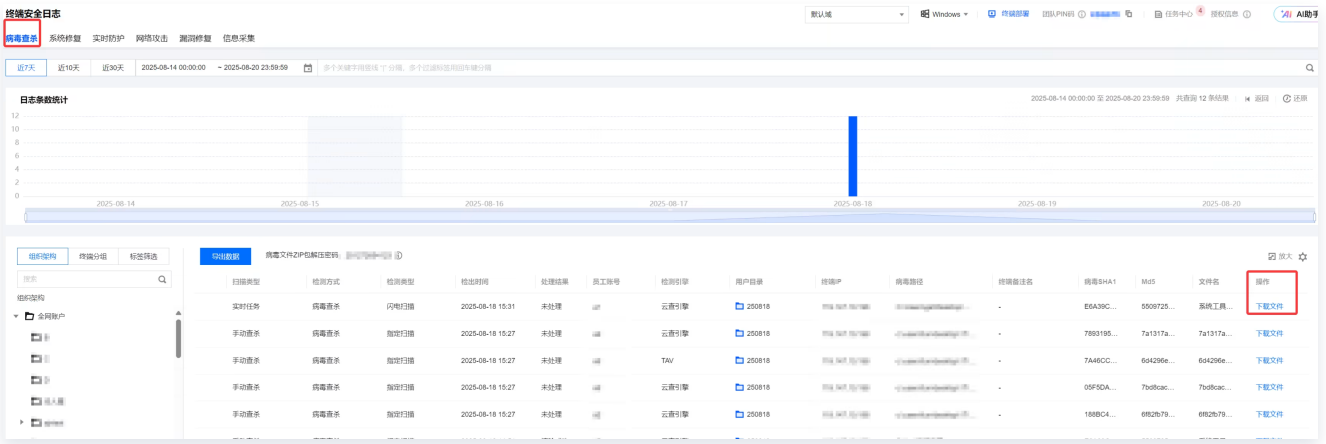
- **客户端信任管理权限**
  - **允许客户端修改隔离区：发现病毒后进行清除，病毒进入隔离区，用户可在隔离区进行彻底删除/恢复操作。**
  - **允许客户端修改信任区：在发现病毒后，单击允许或信任将其加入信任区域。此外，用户也可以直接访问信任区进行操作。**



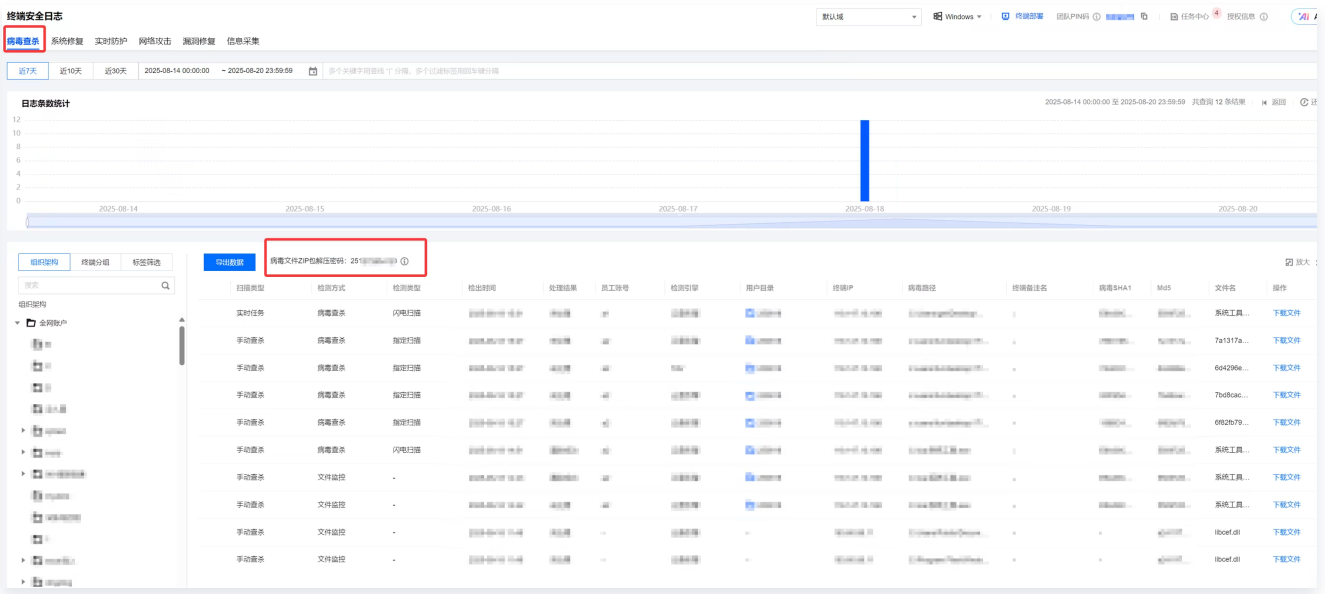
- 终端病毒样本文件自动上传
  - 开启**终端病毒样本文件自动上传**。



  - 病毒样本文件上传至后台存储后，可在**病毒查杀 > 审计日志**直接进行下载。



  - 病毒样本文件如果是多层压缩包嵌套，自动上传和大文件任务触发式上传场景，均不支持上传此种类型的样本文件。
  - 查看病毒文件 ZIP 包解压密码：出于安全性和存储优化考虑，已下载的压缩包名称中没有带原始文件名，须解压两层之后（最后一层需要解压密码），才能拿到真正上传的病毒样本文件，请在导出数据旁查看解压密码。



  - 存储的病毒样本文件自动上传至后台存储桶，支持在**系统通用设置 > 基础设置 > 终端病毒样本上传设置**上传文件大小。


终端病毒样本上传设置
存储空间设置
存储空间不超过
10
GB（超过存储空间限制时，新文件会覆盖掉旧文件）
自动上传设置
单个样本文件大小不超过
3
MB，自动上传至后台存储
保存设置
恢复默认
取消修改

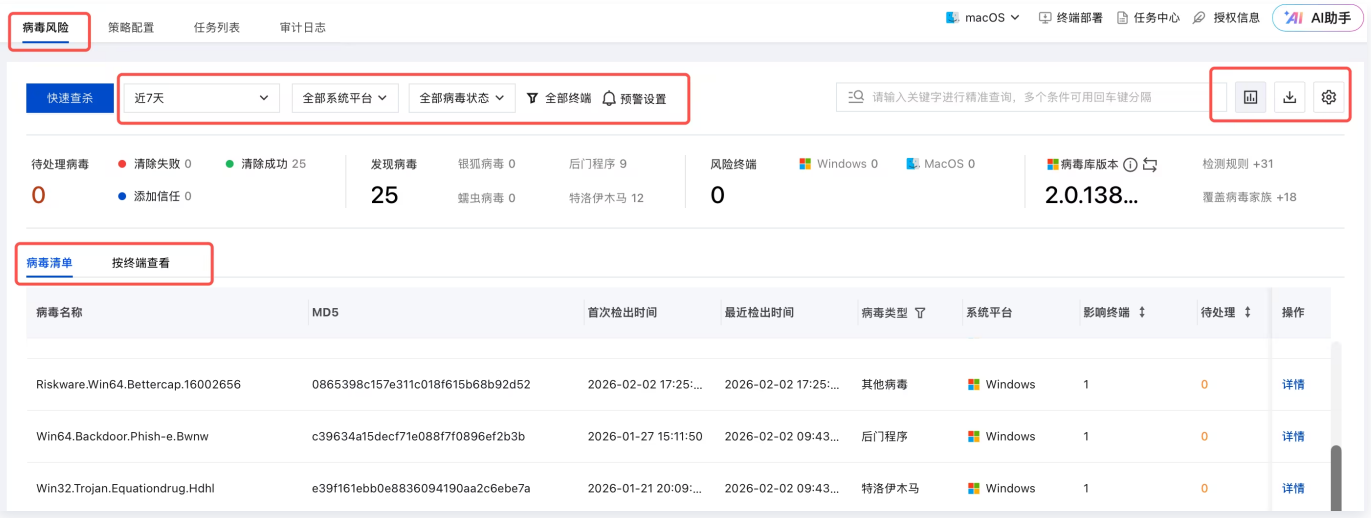
病毒风险（11.1.1版）

最近更新时间：2026-02-13 09:41:02

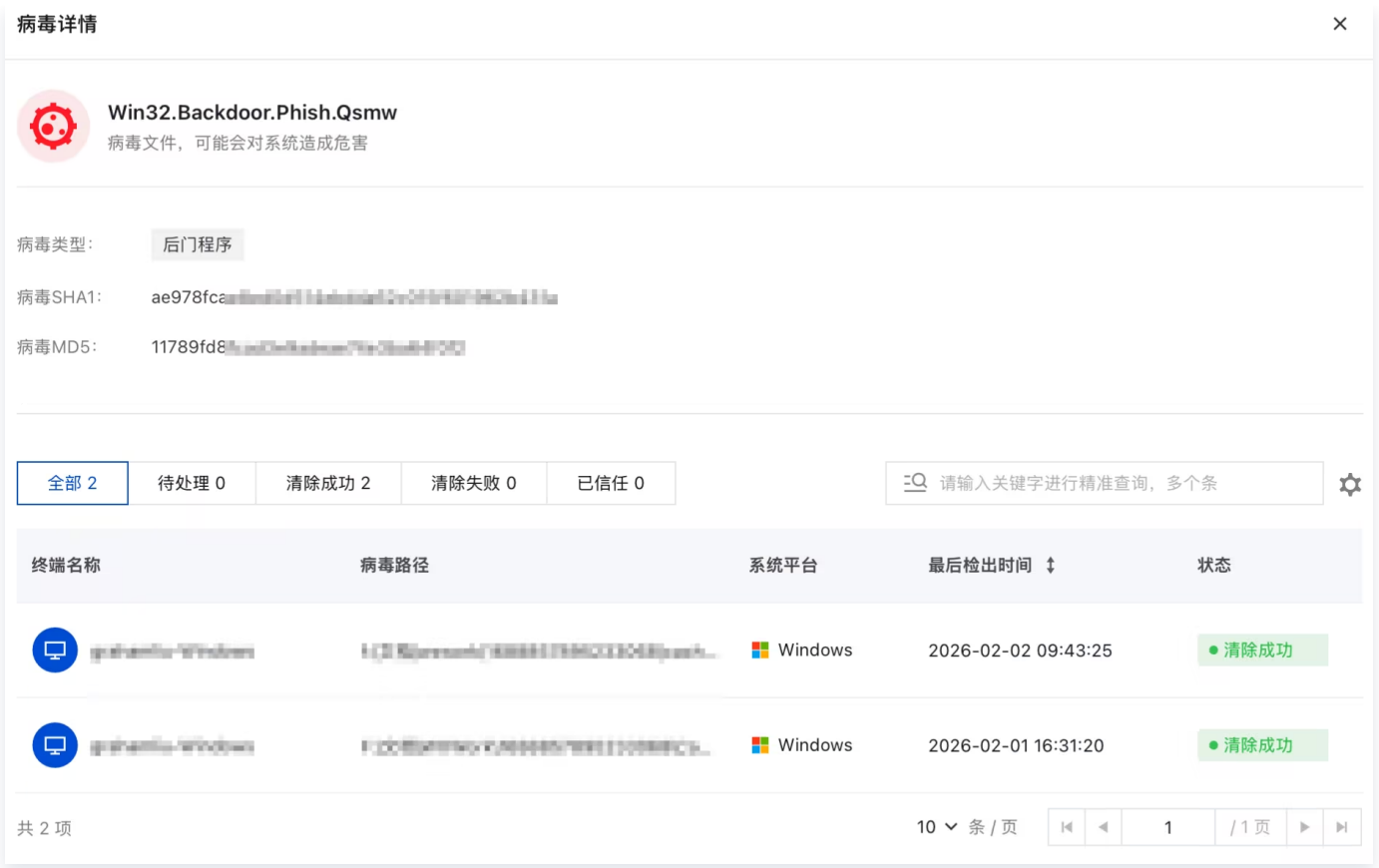
> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

统计和筛选数据

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **病毒查杀** > **病毒风险**。
2. 在病毒风险页面，展示扫描到的病毒风险详情，支持数据筛选及统计：
   - 时间筛选：默认7天，支持用户自定义筛选范围。
   - 系统平台：支持筛选 Windows / macOS。
   - 病毒状态：支持筛选待处理、清除成功、清除失败、添加信任状态。
   - 终端范围：单击展示终端筛选组件，对应展示目标终端下的病毒相关数据，默认全部终端。
   - 支持按病毒清单视角及终端视角查看。

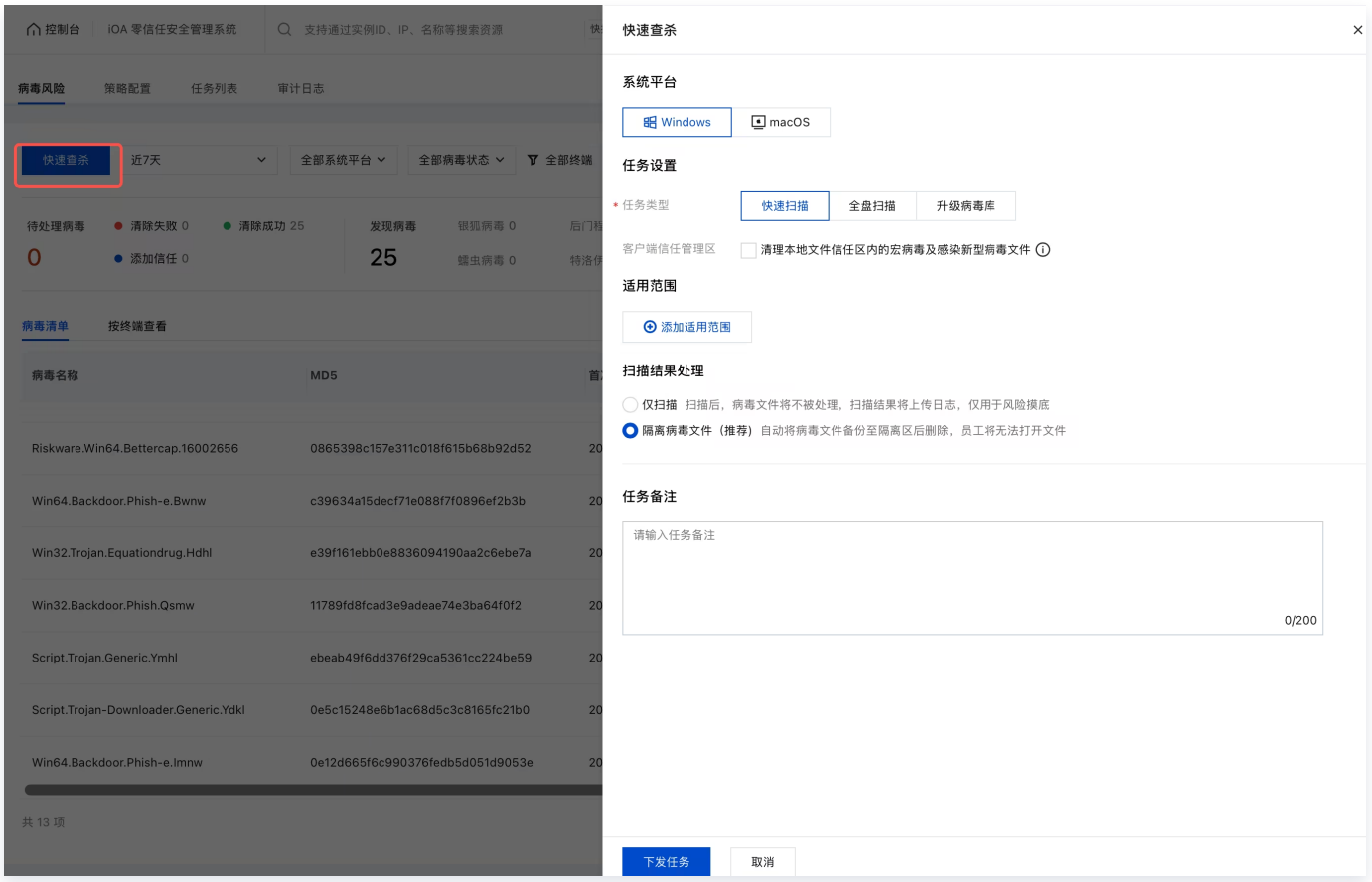


3. 单击**详情**，查看病毒具体信息。



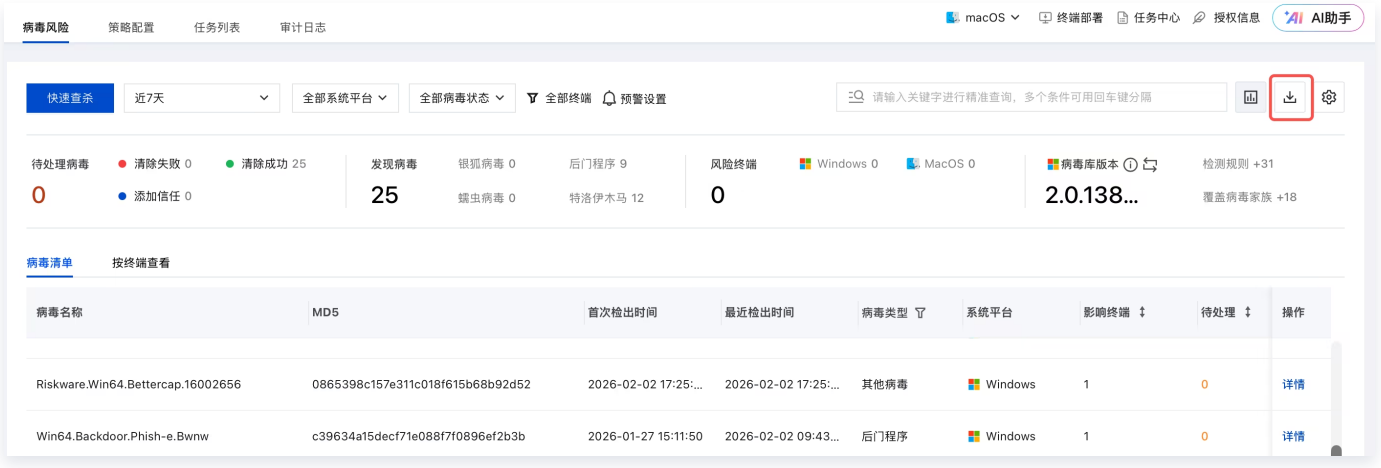
一键查杀/升级病毒库

1. 在病毒风险页面，单击**快速查杀**。
2. 在快速查杀页面，配置系统平台、任务设置、适用范围、扫描结果处理、任务备注等参数，单击**下发任务**。



导出数据

1. 在病毒风险页面，单击右上角  。



2. 勾选自定义表头、导出时间参数，单击**导出**。


导出预设
数据超过8000条，将生成单独的导出任务，请到 任务中心 查看导出进度
自定义表头
全选
病毒名称
MD5
首次检出时间
最近检出时间
病毒类型
系统平台
影响终端
待处理
清除成功
清除失败
已信任
病毒导出时间
近7天
近10天
近30天
2026-01-09 17:14:37 ~ 2026-01-16 17:14:37
目标导出时间：2026-01-09 17:14:37～2026-01-16 17:14:37
导出天数：7天0小时0分0秒
其他信息
导出格式：CSV
预计导出条数：0条
导出
取消

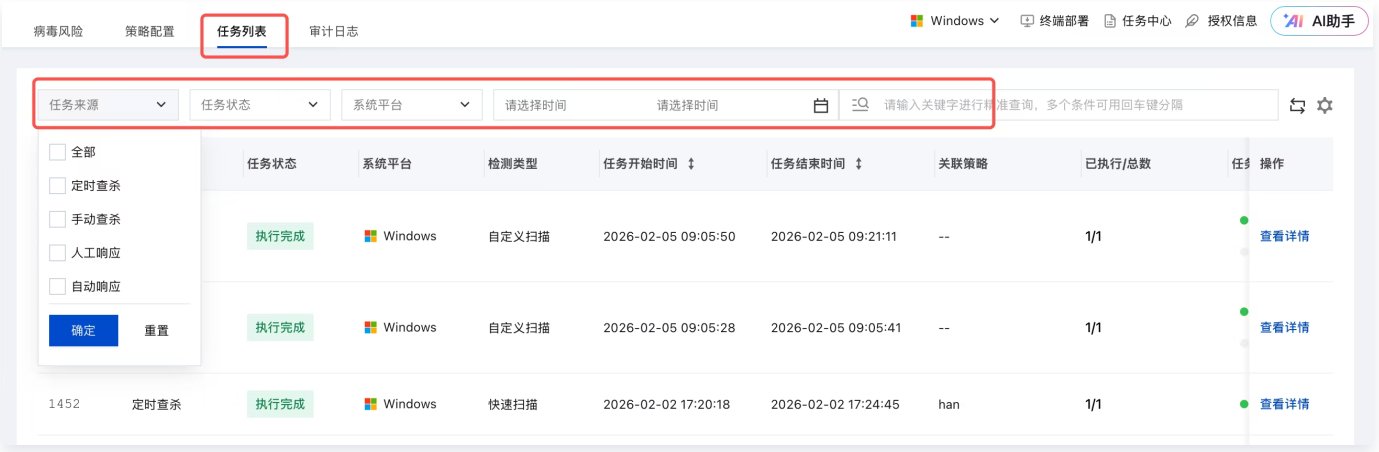
版权所有：腾讯云计算（北京）有限责任公司

任务列表（11.1.1版）

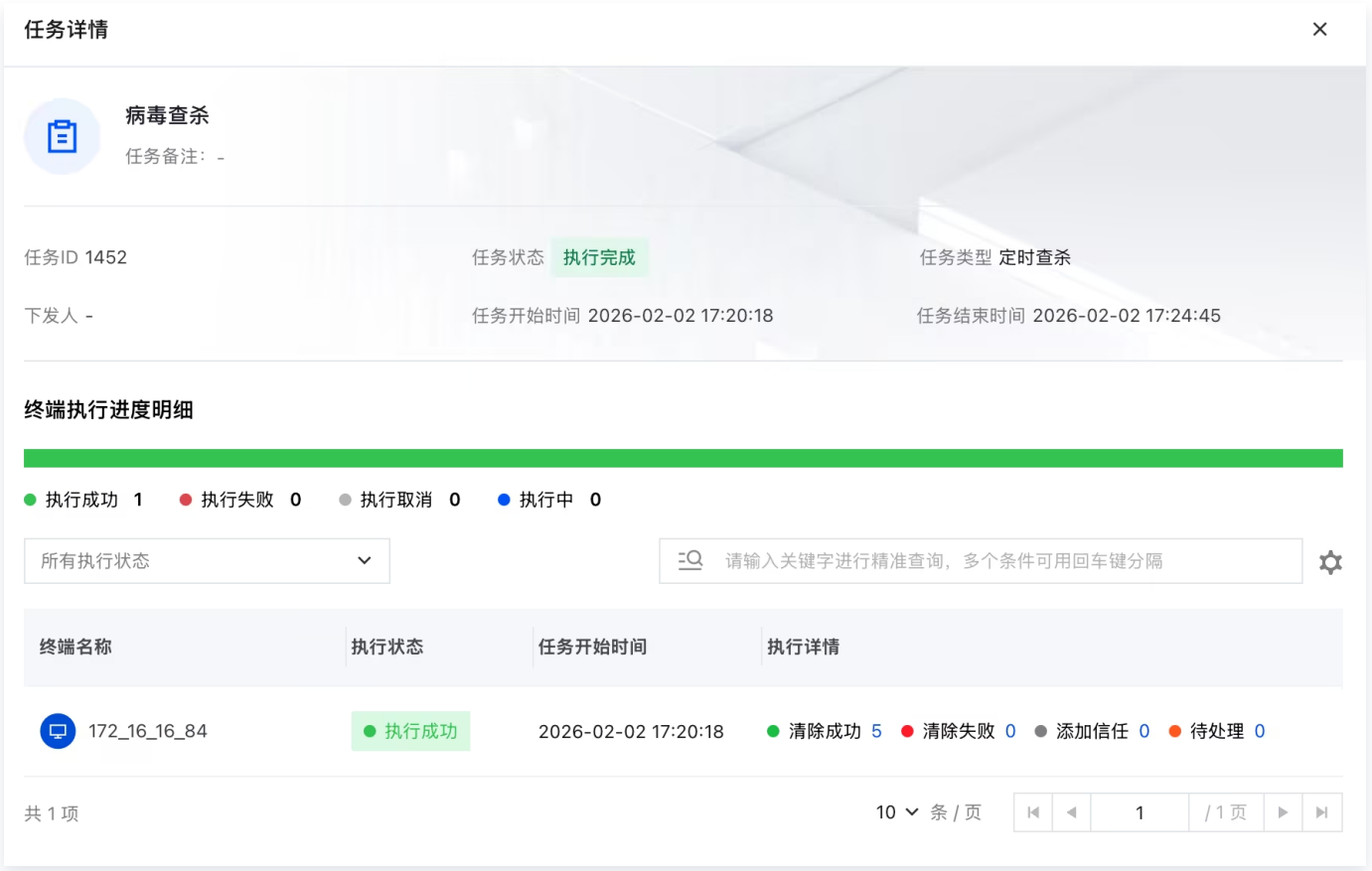
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **病毒查杀** > **任务列表**。
2. 在任务列表页面，展示相关查杀或响应策略的执行情况，支持按照任务来源、任务状态、系统平台、时间进行筛选。



3. 选择目标任务，单击**查看详情**，查看具体任务信息。


任务详情
病毒查杀
任务备注：-
任务ID 1452
任务状态 执行完成
任务类型 定时查杀
下发人 -
任务开始时间 2026-02-02 17:20:18
任务结束时间 2026-02-02 17:24:45
终端执行进度明细
执行成功 1
执行失败 0
执行取消 0
执行中 0
所有执行状态
请输入关键字进行精准查询，多个条件可用回车键分隔
终端名称
执行状态
任务开始时间
执行详情
172_16_16_84
执行成功
2026-02-02 17:20:18
清除成功 5
清除失败 0
添加信任 0
待处理 0
共 1 项
10 条 / 页
1
/ 1 页

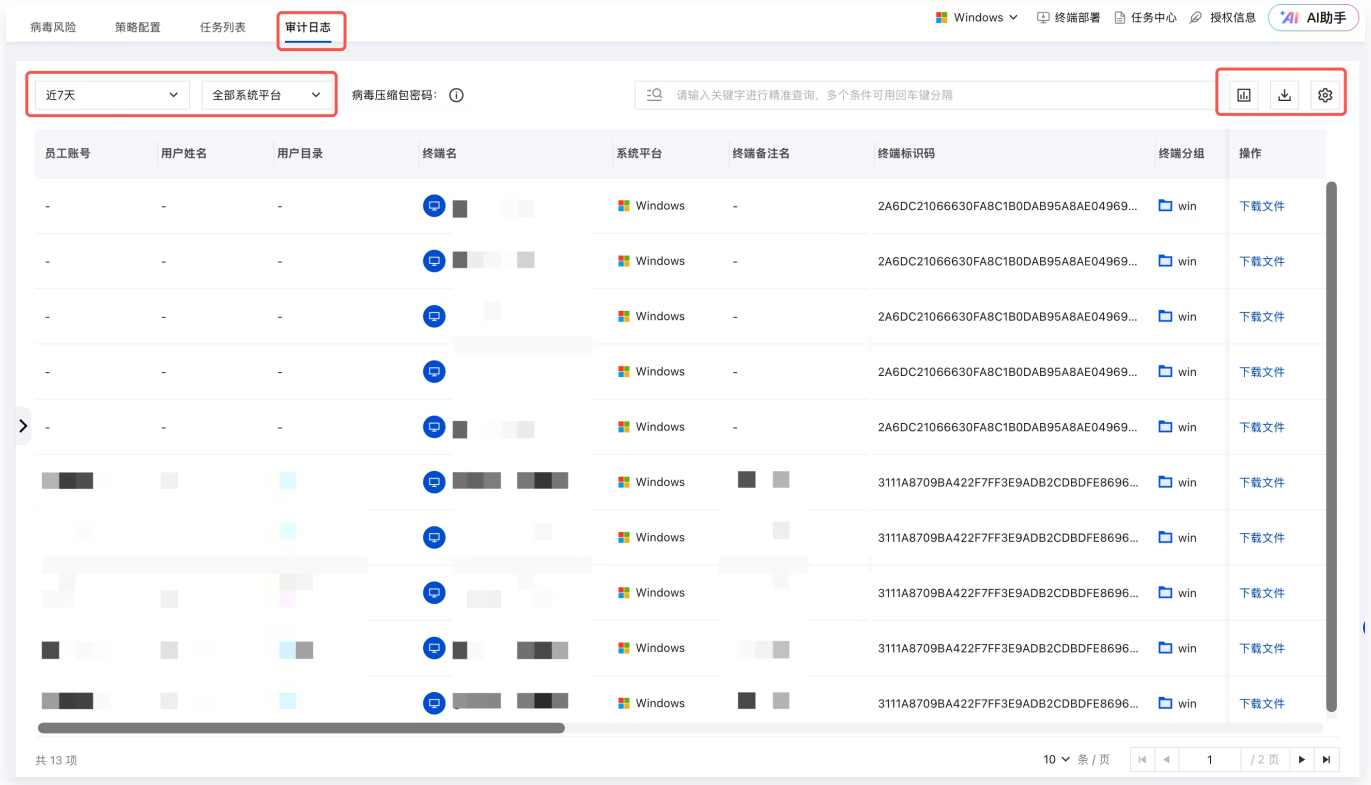
审计日志（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

日志列表

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **病毒查杀** > **审计日志**。
2. 在审计日志页面，展示所有病毒查杀日志情况，支持按时间以及各字段属性筛选。



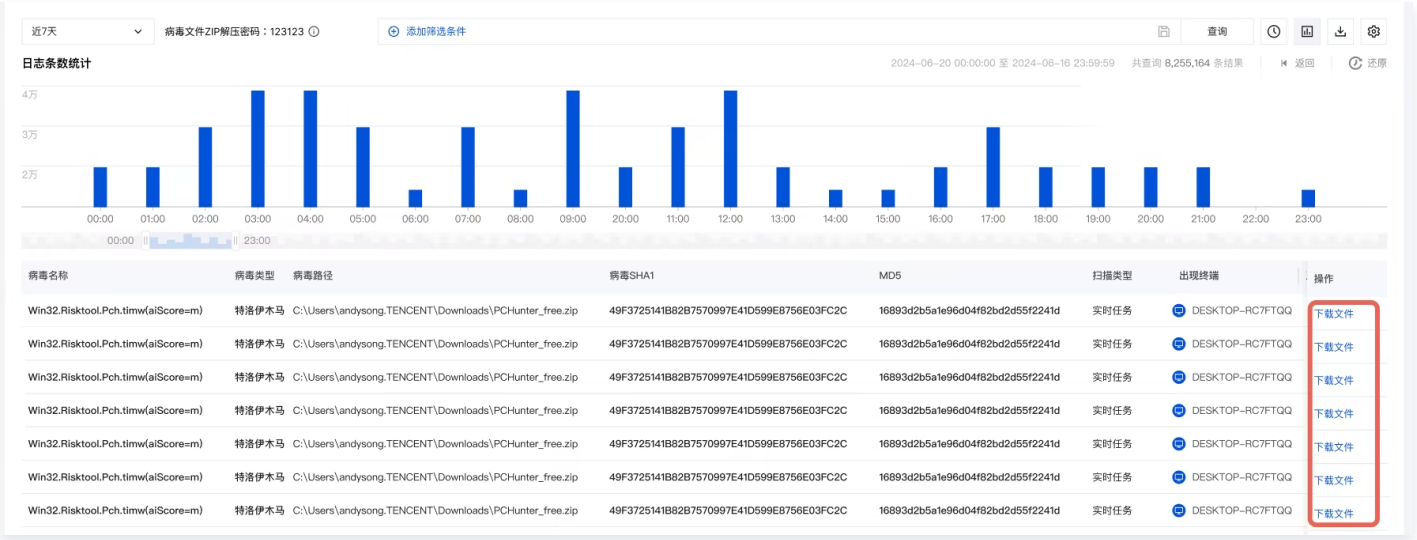
导出日志

在审计日志页面，单击右上角 ，勾选自定义表头、导出时间参数，单击**导出**。


导出预设
数据超过8000条，将生成单独的导出任务，请到 任务中心 查看导出进度
自定义表头
全选
员工账号
用户姓名
用户目录
终端名
终端备注名
终端标识码
终端分组
终端IP
MAC地址
病毒名称
病毒类型
病毒路径
病毒SHA1
Md5
扫描类型
检测方式
检测类型
检测引擎
检出时间
处理结果
文件名
操作
日志导出时间
近7天
近10天
近30天
2026-01-10 00:00:00 ~ 2026-01-16 23:59:59
目标导出时间：2026-01-10 00:00:00～2026-01-16 23:59:59
导出天数：6天23小时59分59秒
其他信息
导出格式：CSV
预计导出条数：0条
导出
取消

下载病毒文件

在审计日志页面，单击**下载文件**，可提取病毒文件。



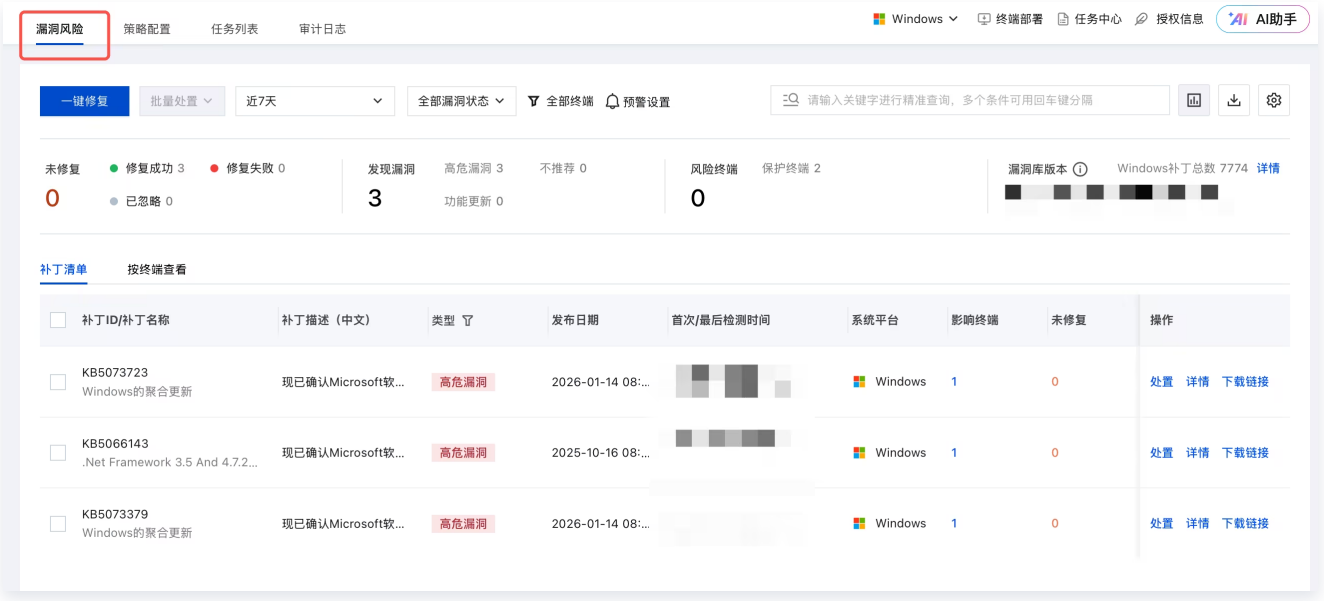
漏洞扫描与修复（11.1.1版）
漏洞风险（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

漏洞报表展示

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **漏洞修复** > **漏洞风险**。
2. 在漏洞风险页面，展示扫描到的漏洞详情，支持数据筛选及统计：
   - 时间筛选：默认7天，支持用户自定义筛选范围。
   - 漏洞状态：支持筛选未处理、修复成功、修复失败、已忽略状态。
   - 终端范围：单击展示终端筛选组件，对应展示目标终端下的漏洞相关数据，默认全部终端。
   - 支持按补丁清单视角及终端视角查看。



3. 选择目标补丁，单击**详情**查看漏洞具体信息。



一键修复

1. 在漏洞风险页面，单击**一键修复**。
2. 在一键修复页面，配置任务类型、适用范围、任务备注等参数，单击**下发任务**。



导出数据

1. 在漏洞修复页面，单击右上角 按钮。



2. 勾选自定义表头、导出时间参数，单击**导出**。


导出预设
数据超过8000条，将生成单独的导出任务，请到 任务中心 查看导出进度
自定义表头
全选
补丁ID
补丁名称
补丁描述（中文）
类型
发布日期
首次检测时间
最后检测时间
系统平台
影响终端
未修复
修复失败
修复成功
已忽略
漏洞导出时间
近7天
近10天
近30天
2026-01-13 00:00:00 ~ 2026-01-19 23:59:59
目标导出时间：2026-01-13 00:00:00～2026-01-19 23:59:59
导出天数：6天23小时59分59秒
其他信息
导出格式：CSV
预计导出条数：8条
导出
取消

版权所有：腾讯云计算（北京）有限责任公司

漏洞修复策略配置（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

配置修复终端系统漏洞的方式，防止病毒和木马通过漏洞进行攻击。

按策略模板配置

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **漏洞修复** > **策略配置**，单击**策略模板**。



2. 根据需求，勾选**日常静默防护**或**敏感时期防护**，单击**应用**。
   - 日常静默防护：适用于企业日常漏洞修复管理，漏洞修复全程静默操作，员工无操作权限且无感知。
   - 敏感时期防护：适用于国家护网期间漏洞修复防御管理，检验并提升企业整体安全水位。



3. **在策略编辑页面，输入策略名称、策略描述、优先级等参数，单击添加适用范围，勾选需要管控或排除的用户/终端范围，单击确定。**



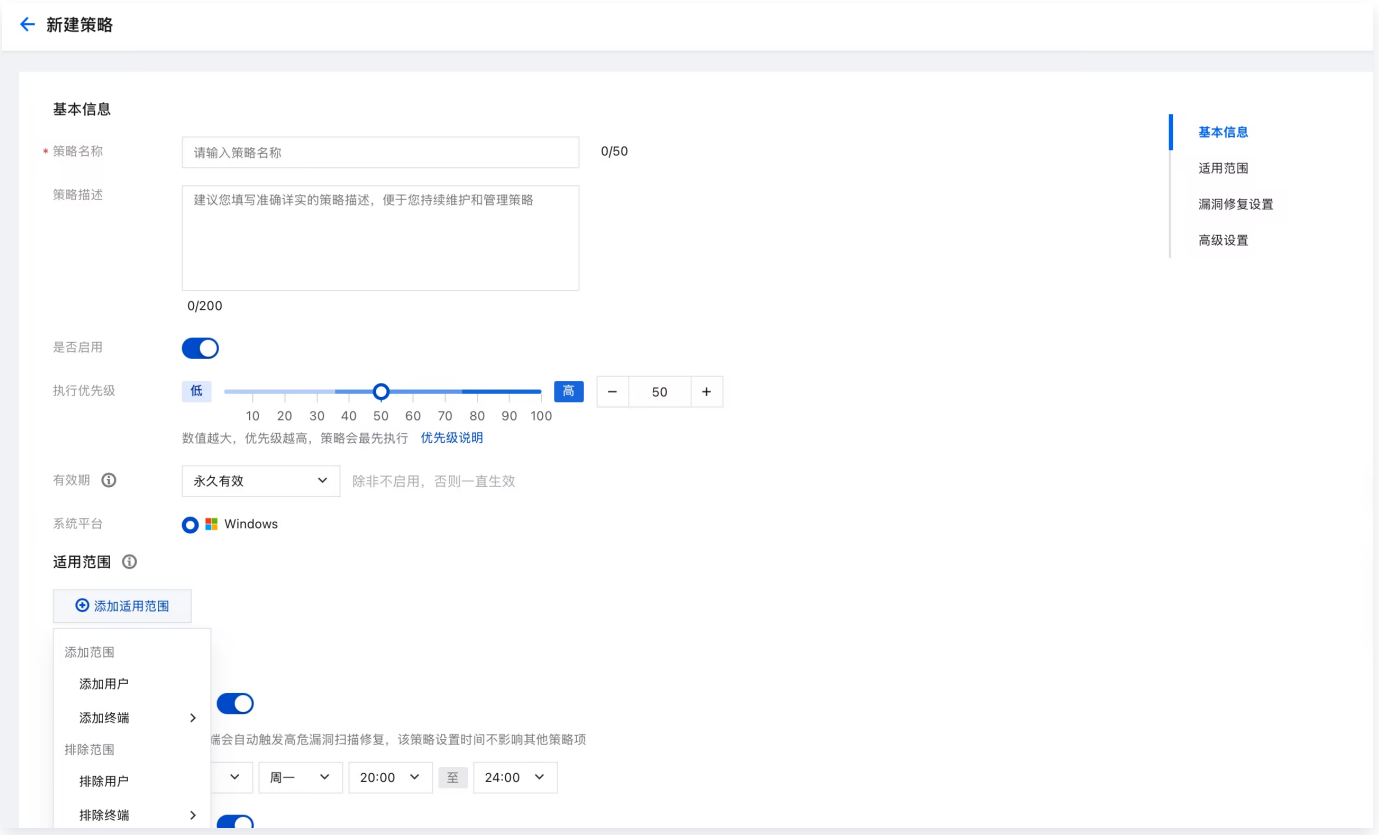
4. 配置好以上参数后，单击**保存**即可，其他相关配置可按照系统默认推荐配置。

新建自定义策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **漏洞修复** > **策略配置**，单击**新建策略**。



2. 在策略编辑页面，输入策略名称、策略描述、优先级等参数，单击**添加适用范围**，勾选需要管控或排除的用户/终端范围，单击**确定**。



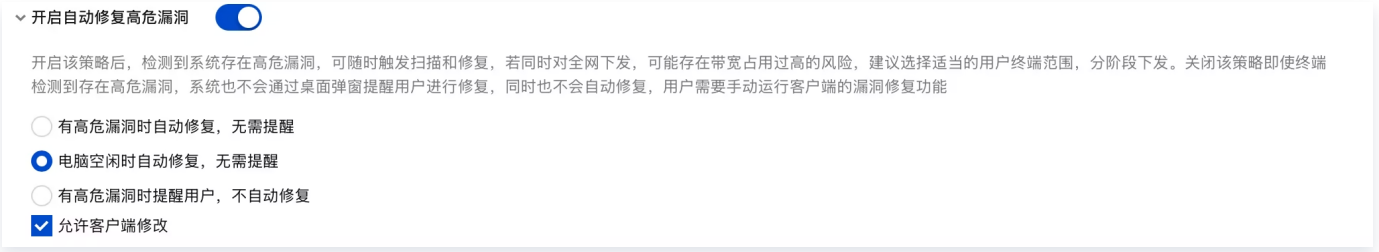
3. 根据需求，配置以下漏洞修复设置，配置后单击**保存**。

漏洞修复设置

- 定期修复高危漏洞
  - 功能：设置漏洞修复的定时任务。
  - 建议：开启每天定时修复漏洞任务

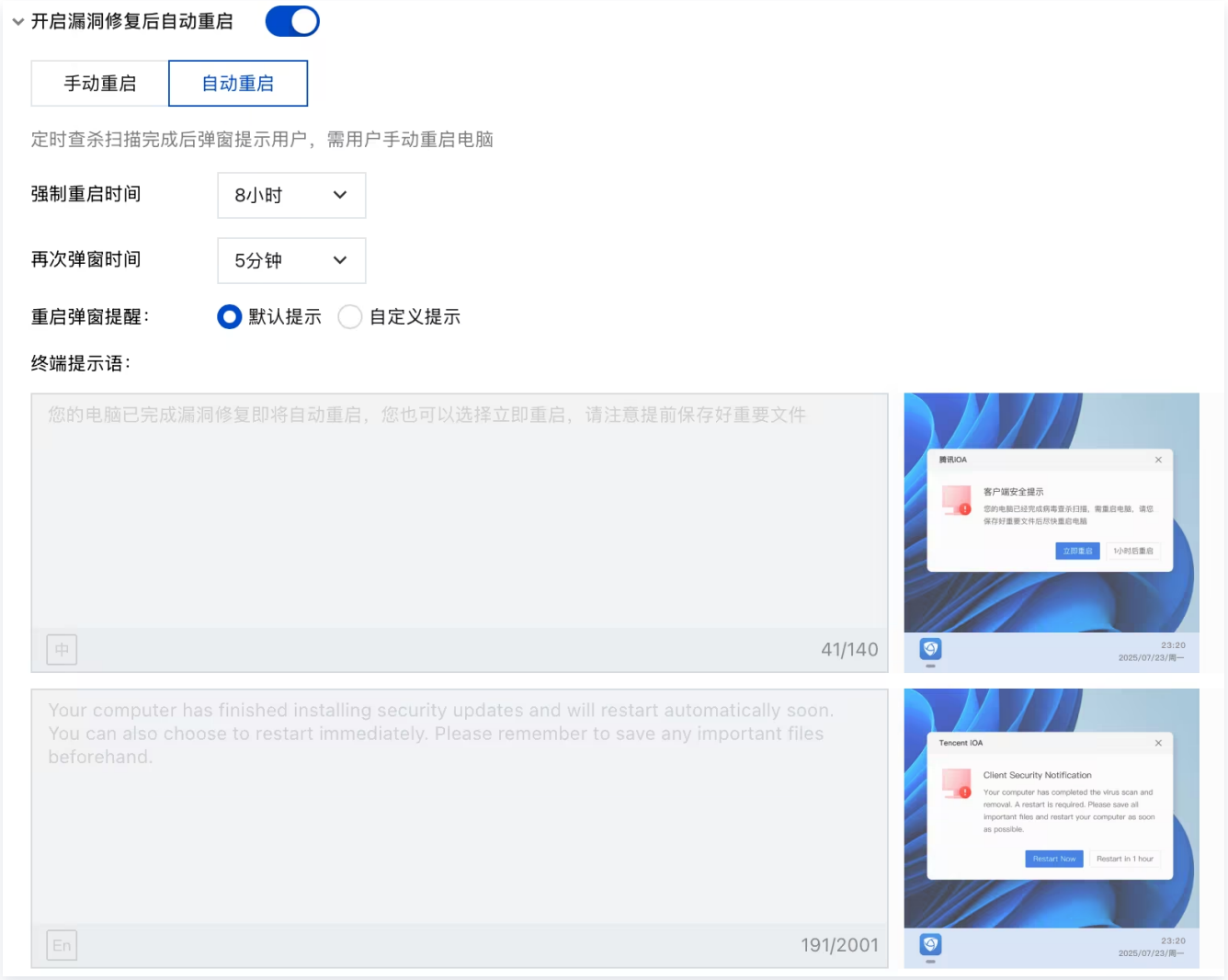


- 自动修复高危漏洞：控制高危漏洞的修复提醒方式。



选项名称	详情
有高危漏洞时自动修复，无需提醒	表示如果终端系统存在高危漏洞，系统将自动进行修复，用户不会收到任何提醒。iOA 客户端将每天定期检查是否存在高危漏洞，并且后台控制中心也会下发检测策略。一旦发现高危漏洞，系统将立即修复，而不会等待电脑处于空闲状态。
电脑空闲时自动修复，无需提醒	与自动修复高危漏洞且无需提醒用户的设置相同，系统将自动静默修复漏洞，但修复将仅在电脑处于空闲状态时进行（例如：用户未进行任何操作时）。
有高危漏洞时提醒用户，不自动修复	这意味着如果终端系统存在被微软定义为高危的漏洞（即漏洞一旦被利用，可能造成严重危害）时，系统将在桌面右下角弹出窗口提醒用户，让用户自行决定是否进行修复。
允许客户端修改	勾选后客户端设置支持修改其他设置在自己客户端的配置。其他设置仍以控制台设置为准。

- 漏洞修复后重启设置
  - 支持管理员通过策略对目标终端进行重启设置。
  - 部分系统补丁在更新后需要重启终端生效，开启漏洞修复后重启设置策略，iOA 安装补丁后会提示用户重启电脑。



高级设置

单击展开，根据需求配置如下高级设置。



开启Office 漏洞修复提醒

- **勾选后，系统将下发 Office 补丁任务。如果检测到客户端正在运行 Office 软件，系统将弹出提醒通知，提示员工保存 Office 数据。**
- **若不勾选，将不会有此提示，可能因 Office 补丁更新导致数据丢失。**

> **注意：**
> **当此提醒和高危漏洞修复提醒发生冲突时，优先执行此提醒逻辑。**



开启蓝屏修复功能

开启蓝屏修复功能（推荐）：主要运用场景为系统打补丁，当遇到不兼容，可能会导致系统蓝屏无法启动时，重启并从蓝屏修复启动入口进入，即可修复问题。



允许更改操作系统自动更新配置

允许更改操作系统自动更新配置：勾选该选项可能会导致用户操作系统配置变化，请谨慎开启。



其他设置

- 开启漏洞智能忽略：腾讯会自动运营一些与系统不兼容的补丁，开启这个功能，就可以尽可能减少不兼容导致的问题发生。
- 允许用户手动忽略漏洞：勾选后可忽略漏洞。

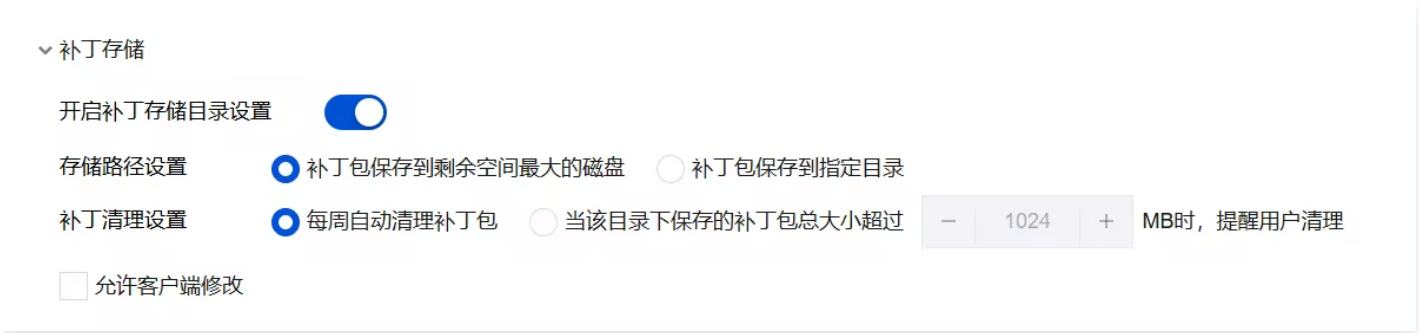


全局补丁设置

补丁存储

配置补丁保存及清理策略，单击 开启补丁存储目录设置。

选项名称	详情
存储路径设置	• 补丁包保存到剩余空间最大的磁盘。 • 补丁包保存到指定目录：因为每台终端的用户保存路径的习惯不同，通过自定义/保存到空间最大的磁盘很好地解决了固定路径下可能出现的磁盘空间不足的问题。
补丁清理设置	• 每周自动清理补丁包：由于补丁包占用大量磁盘空间，系统默认会在补丁修复完成后自动清理已完成或已忽略的补丁。然而，仍会存在许多用户未修复的低危补丁以及未修复完成的补丁。用户可以选择不进行修复，但是可能因为使用一键下载功能，占用了较多磁盘空间导致磁盘不足。建议定期清除这类补丁，用户在需要时可以再次下载安装。 • 当该目录下保存的补丁包总大小超过 X MB时，提醒用户清理：超过设置的补丁包大小后，弹窗提醒用户清理。
允许客户端修改设置	勾选后客户端设置支持修改实时防护在自己客户端的配置，实时防护设置仍以控制台设置为准。



开启补丁库修复/排除清单

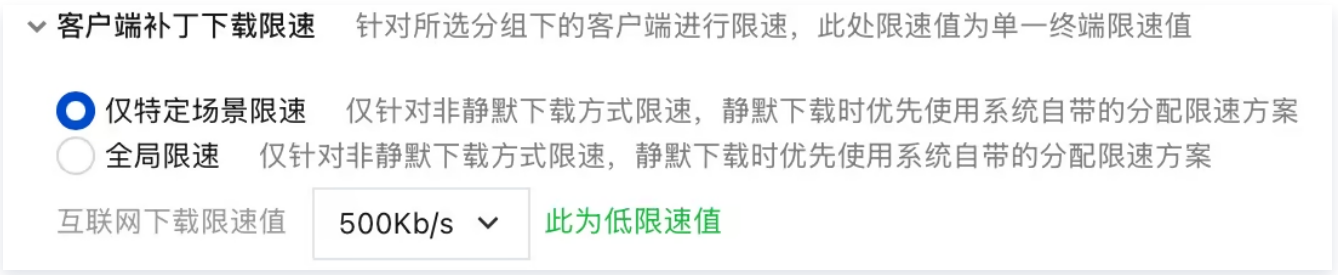
当需要自定义排除掉一些不安装的补丁（与系统不兼容，或无用的低危补丁），可以使用此功能，添加排除列表；当需要自定义只修复某些补丁时，添加修复列表。



客户端补丁下载限速

- 针对所选分组下的客户端进行限速，此处限速值为单一终端限速值。

- **仅特定场景限速：仅针对非静默下载方式限速，静默下载时优先使用系统自带的分配限速方案。**
- **全局限速：包括静默下载在内的所有方式统一限速。**

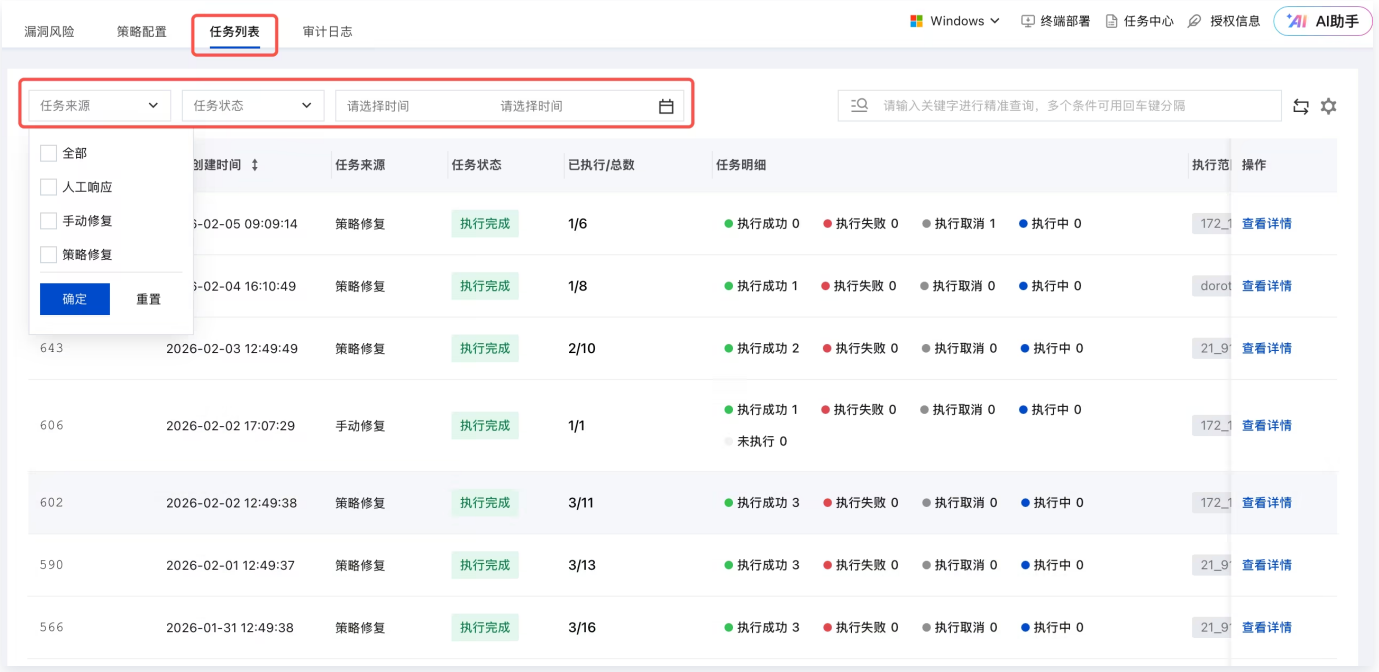


任务列表（11.1.1版）

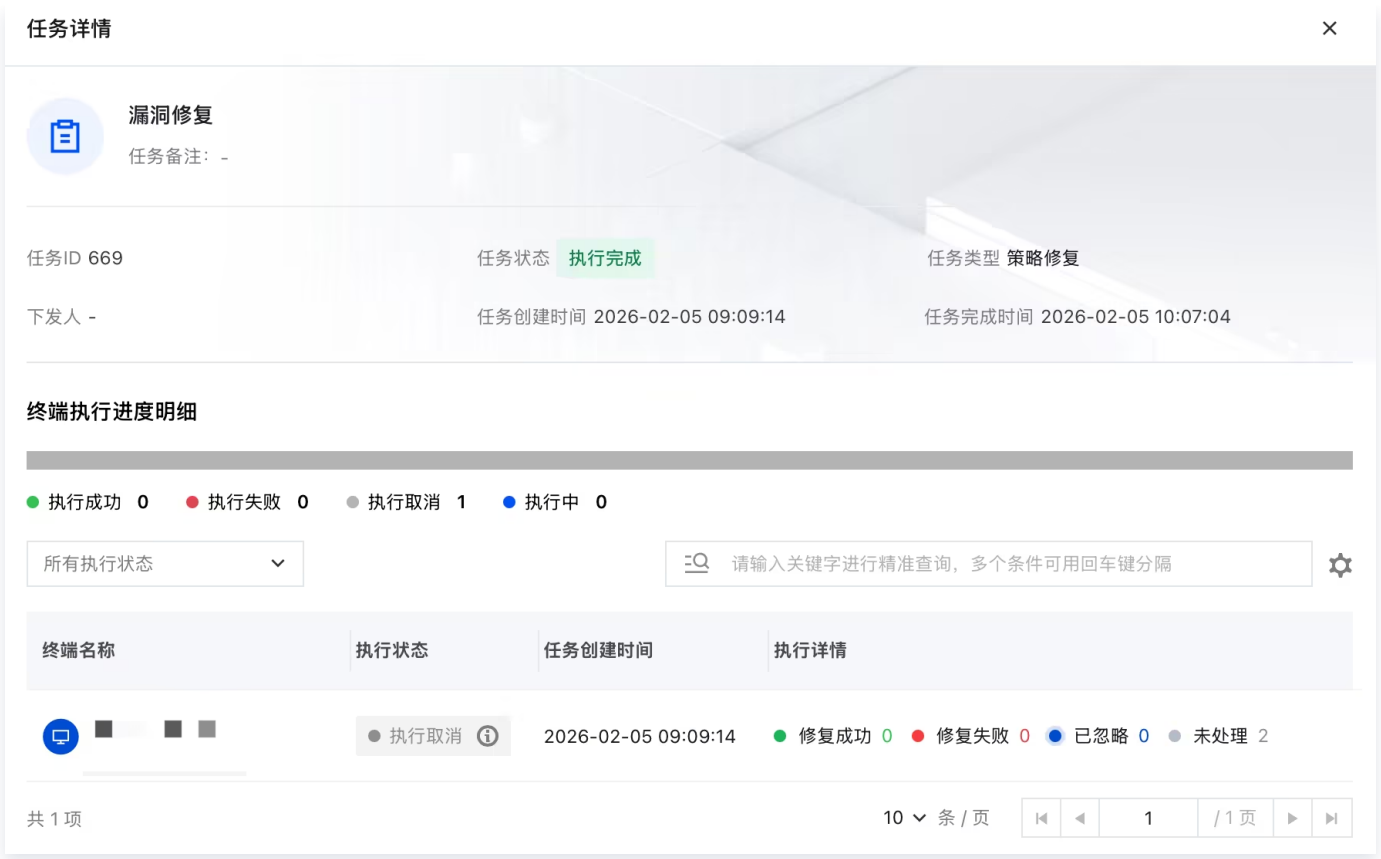
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **漏洞修复** > **任务列表**。
2. 在任务列表页面，展示所有漏洞修复任务情况，可按任务来源、任务状态、时间进行筛选。



3. 选择目标任务，单击**查看详情**查看具体任务信息。


任务详情
漏洞修复
任务备注：-
任务ID 669
任务状态 执行完成
任务类型 策略修复
下发人 -
任务创建时间 2026-02-05 09:09:14
任务完成时间 2026-02-05 10:07:04
终端执行进度明细
执行成功 0
执行失败 0
执行取消 1
执行中 0
所有执行状态
请输入关键字进行精准查询，多个条件可用回车键分隔
终端名称
执行状态
任务创建时间
执行详情
执行取消
2026-02-05 09:09:14
修复成功 0
修复失败 0
已忽略 0
未处理 2
共 1 项
10 条 / 页
1
/ 1 页

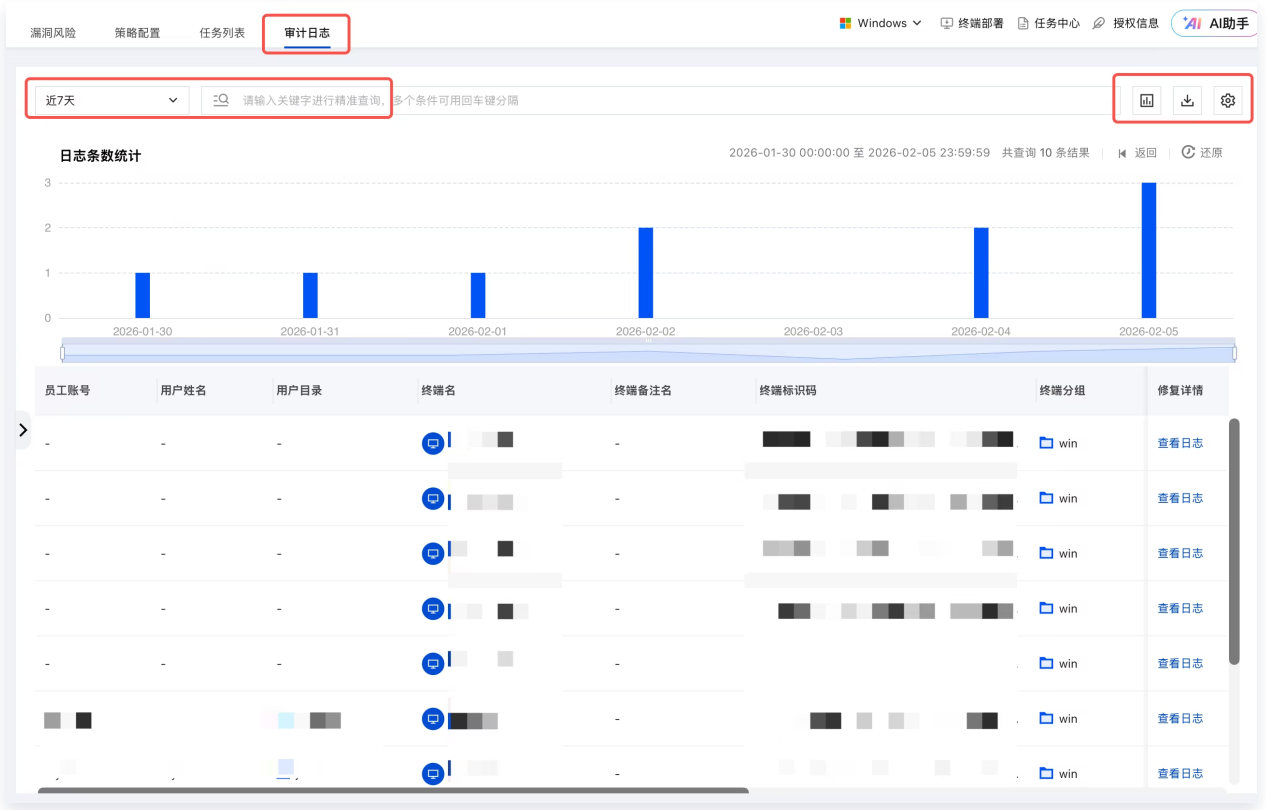
审计日志（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

日志列表

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **漏洞修复** > **审计日志**。
2. 在审计日志页面，展示所有漏洞修复日志情况，支持按时间以及各字段属性筛选。



导出日志

在审计日志页面，单击右上角 ，勾选自定义表头、导出时间参数，单击**导出**。


导出预设
数据超过8000条，将生成单独的导出任务，请到 任务中心 查看导出进度
自定义表头
全选
员工账号
用户姓名
用户目录
终端名
终端备注名
终端标识码
终端分组
终端IP
MAC地址
补丁ID
类型
检出时间
处理结果
日志导出时间
近7天
近10天
近30天
2026-01-13 00:00:00 ~ 2026-01-19 23:59:59
目标导出时间：2026-01-13 00:00:00～2026-01-19 23:59:59
导出天数：6天23小时59分59秒
其他信息
导出格式：CSV
预计导出条数：28条
导出
取消

版权所有：腾讯云计算（北京）有限责任公司

实时防护（11.1.1版）
策略配置（11.1.1版）

最近更新时间：2026-02-13 17:55:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

实时对网络下载、聊天工具文件传输、U 盘等易感染病毒的途径进行严密安全防护。

按策略模板配置

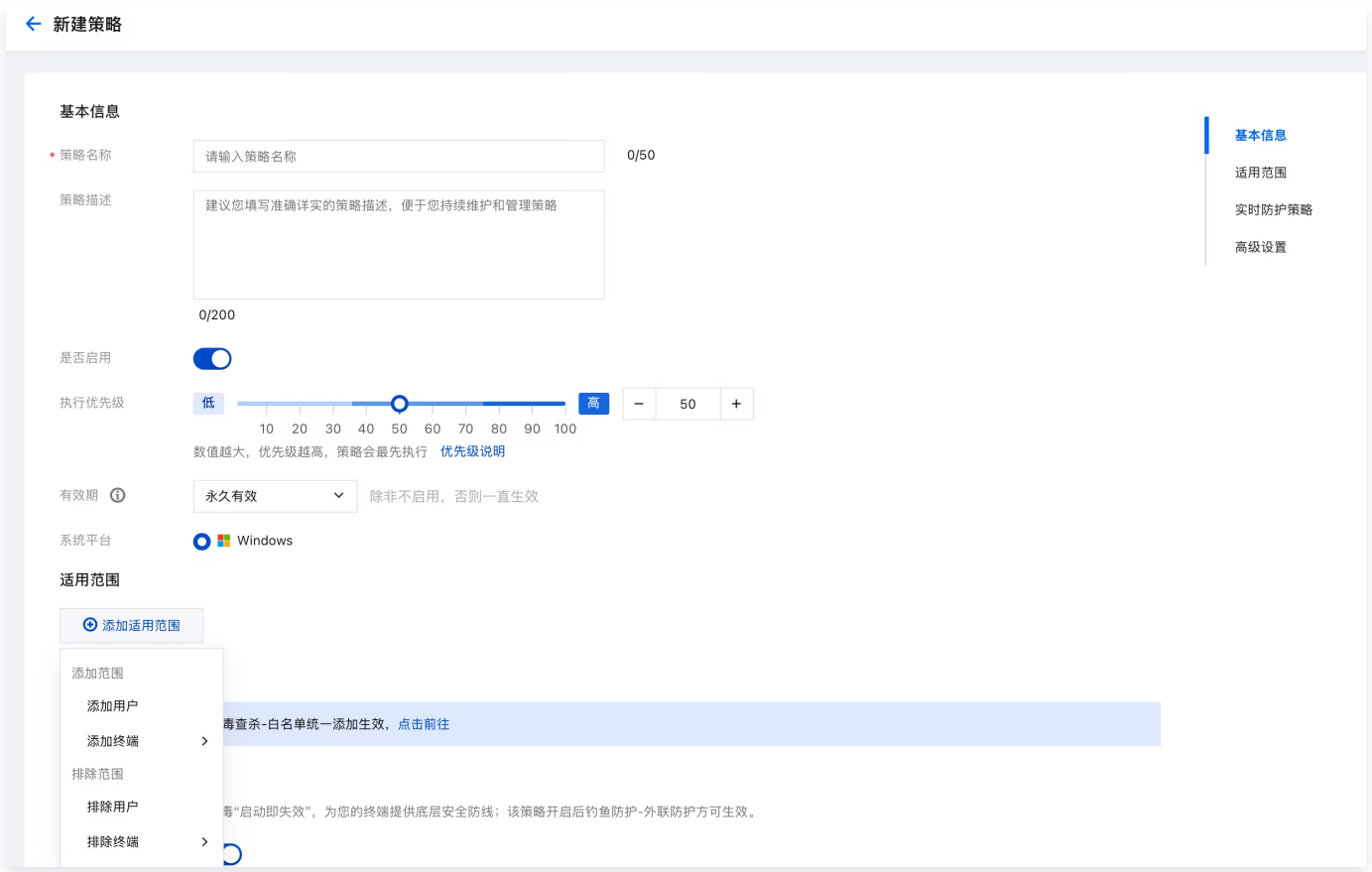
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **实时防护** > **策略配置**，单击**策略模板**。



2. 勾选**日常静默防护**或**敏感时期防护**，单击**应用**。
   - 日常静默防护：适用于企业日常防护管理，可以实时对网络下载、聊天工具文件传输等场景严密防护。
   - 敏感时期防护：适用于国家护网期间，对潜在危险行为进行严格管控防护，有效识别银狐病毒，钓鱼恶意文件等。



3. **在策略编辑页面，输入策略名称、策略描述、优先级等参数，单击添加适用范围，勾选需要管控或排除的用户/终端范围，单击确定。**



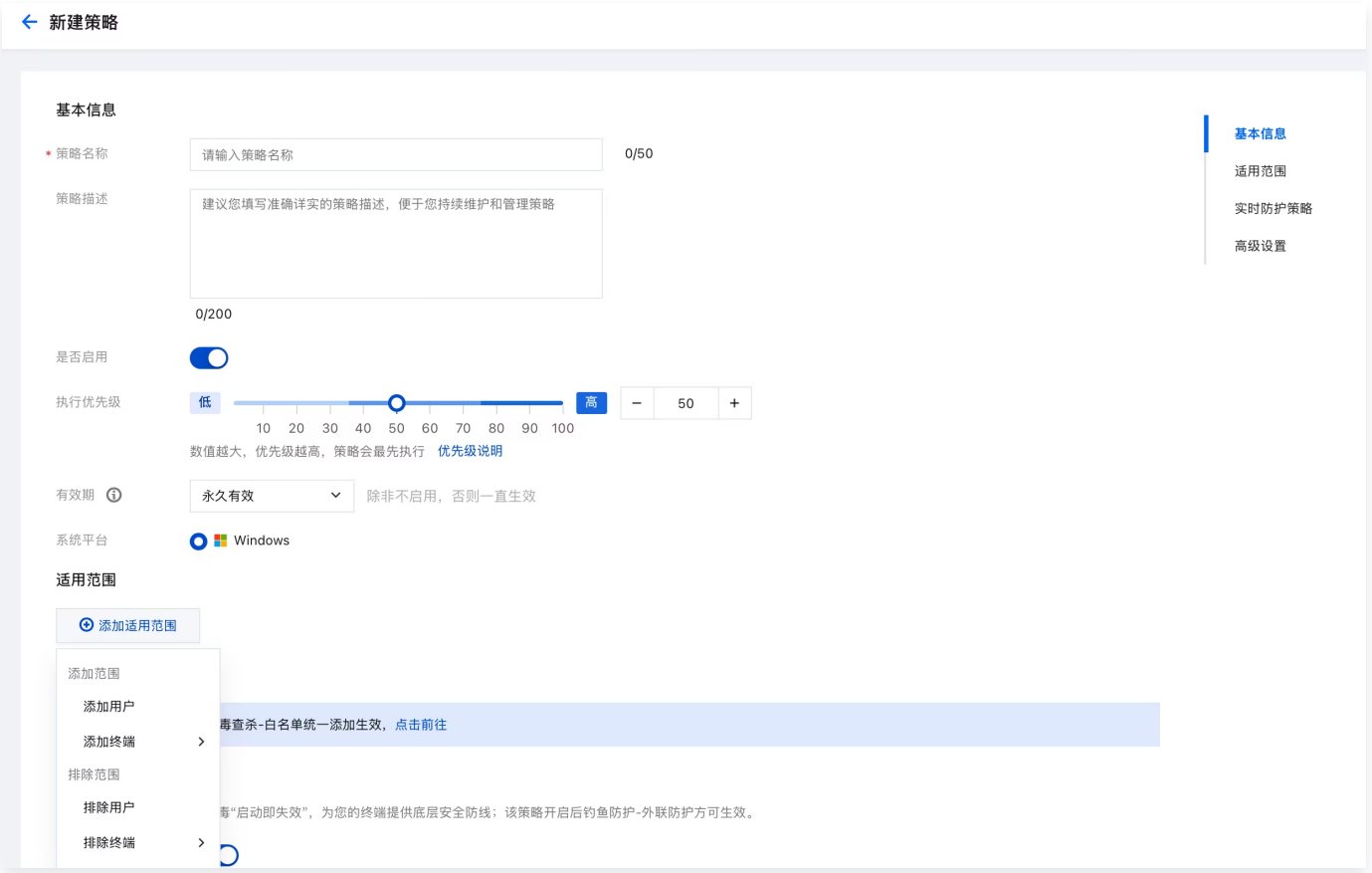
4. 配置好以上参数后，单击**保存**即可，**其他相关配置可按照系统默认推荐配置**。

新建自定义策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **实时防护** > **策略配置**，单击**新建策略**。



2. 在策略编辑页面，输入策略名称、策略描述、优先级等参数，单击**添加适用范围**，勾选需要管控或排除的用户/终端范围，单击**确定**。



3. 根据需求，配置以下实时防护策略，配置后单击**保存**。

开启进程防护

- 实时扼杀危险进程，让病毒“启动即失效”，为您的终端提供底层安全防线，单击**开启进程防护开关**。



- 开启进程防护后，当存在危险进程时，客户端弹窗示例：



开启文件下载防护

- **开启文件下载防护**开关，将自动扫描所有网络下载文件。



  - 对安装有 iOA 的终端，从浏览器下载的文件进行监控和防护。针对银狐通过利用仿冒下载站点下载钓鱼样本以及白加黑攻击手法，加强浏览器等渠道下载文件的检测及阻断能力。
  - 对所有下载的文件进行安全提醒：分为“未知”、“安全”、“风险”三种类型的弹窗提醒。

> **说明：**
> 建议配置为“对所有下载的文件进行安全提醒”，此配置方式可鉴别文件安全/未知状态，对于未知的文件，也需要加以防范，可疑度也可能很高。

  - 只对危险文件进行安全提醒：只有“风险”类型的文件才会弹窗提醒。
- 当存在下载文件或危险文件时，客户端弹窗示例：



开启文件系统防护

- 开启**文件系统防护**开关，自动监控文件创建、读写、删除等关键操作。



- 针对客户端本地文件操作的防护等级，等级越高，监控的操作行为越多，但同时对文件的读写性能消耗（IO 操作或磁盘读写速度的影响）也会越大。
- 自动监控文件创建、读写、删除等关键操作，0秒阻断勒索加密、恶意篡改等攻击，确保数据完整可信。
- 发现风险时的处理方式：推荐**自动处理**，自动将风险文件备份至隔离区后删除。

> **说明：**
> 实时文件监控设置建议保持中等，可阻断大部分执行和改写行为，对于只读行为放过。（设置为“低”等级，将使得针对文件的改写相关的保护无效；设置为“高”等级，除了监控执行和写入，还会监控读操作，一般只读操作的危害相对较小，且性能影响较大）。

开启应用层防护

- 启用各项防护功能：包括桌面图标防护、摄像头防护、网页防火墙、注册表防护、驱动防护、黑客入侵防护、U 盘防护。

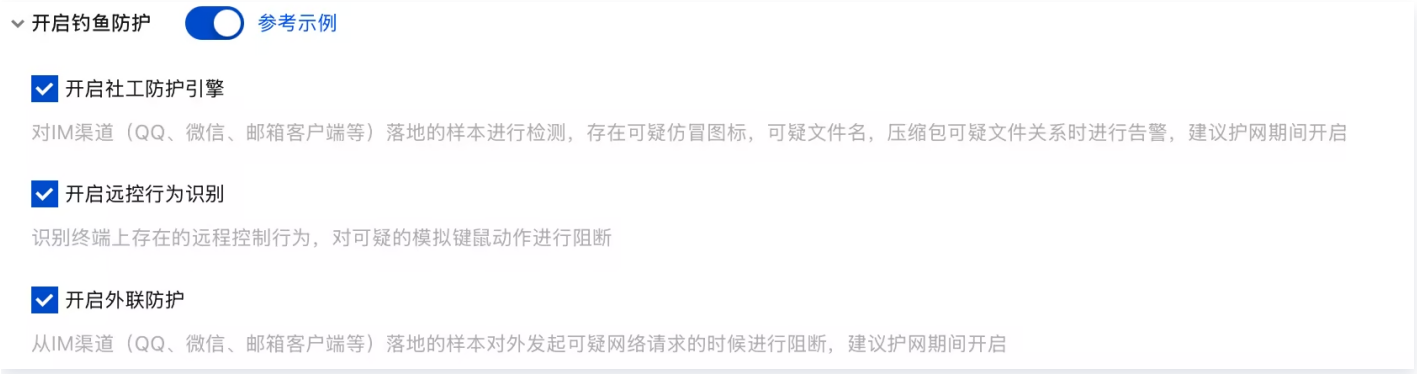
> **注意：**
> 建议其他基础防护全部开启，任何一项关闭，都可能导致防护能力的缺失。

- U 盘防护：针对安装有 iOA 的终端，插入 U 盘后的行为管控防护策略。
  - 禁用系统自动播放（重启后生效）：此操作将阻止系统在插入 U 盘或移动硬盘后自动执行 autorun 文件。
  - 使用 U 盘时，自动扫描 U 盘的病毒木马：插入 U 盘后，会自动扫描 U 盘中是否存在风险，如存在，则弹窗提醒或自动清除。
  - 自动清除 U 盘中的病毒木马：针对使用 U 盘时，自动扫描 U 盘中的病毒木马中发现的风险，配置是否自动清除，勾选后将自动清除 U 盘中的病毒木马，不勾选弹窗提醒，需手动清除。



开启钓鱼防护

开启**钓鱼防护**开关并自定义配置社工防护引擎、远控行为识别、外联防护能力；钓鱼防护可针对银狐常利用的正规软件进程进行防御规避和持久化等战术，采取主动防御措施予以阻断；针对银狐伪装的知名软件安装包，基于其安装行为进行识别，守护系统安全。



- **开启社工防护引擎：开启社工防护引擎后，将检测从邮件、通信工具、浏览器等渠道接收或下载的外部文件是否使用社工欺骗类技术，有效提升对钓鱼、水坑等攻击方式的防护效果。**
- **远控行为识别：识别终端上存在的远程控制行为，对可疑的模拟键鼠动作进行阻断。**
- **开启外联防护：从IM 渠道（QQ、微信、邮箱客户端等）落地的样本对外发起可疑网络请求的时候进行阻断。**

高级防护手段

根据需求，配置如下高级防护手段，单击展开。



开启文档保护

单击开启文档保护开关，守护文档不被黑客攻击，通过文档备份支持对误删文档进行找回。

- **开启文档防护：拦截勒索病毒加密文件。**
  - **允许客户端修改文档立体防护：开启后，用户可在客户端自行开启或关闭文档防护功能，文档备份设置仍以控制台设置为准。**



- 开启文档备份：选择开启/关闭文档备份。
  - 允许客户端修改文档备份：开启后，文档备份设置以客户端设置为准。
  - 备份占用磁盘空间：根据实际情况设置备份占用磁盘空间上限。
  - 文档保护周期：可找回时间内的文档。
  - 备份目录：智能模式：除过滤目录外，全盘备份。自定义目录：可自行在客户端处添加需要备份的重要文档目录。
  - 文档备份类型：单击**添加/删除**，添加/删除文档备份类型，大于100MB的文件将不会备份。



- 开启卷影备份防护：勾选后允许删除/修改卷影文件（默认勾选允许修改卷影大小）。



配置示例1：找回误删文档

1. 加载文档守护者。
   1.1 在客户端中单击**文档守护者**。

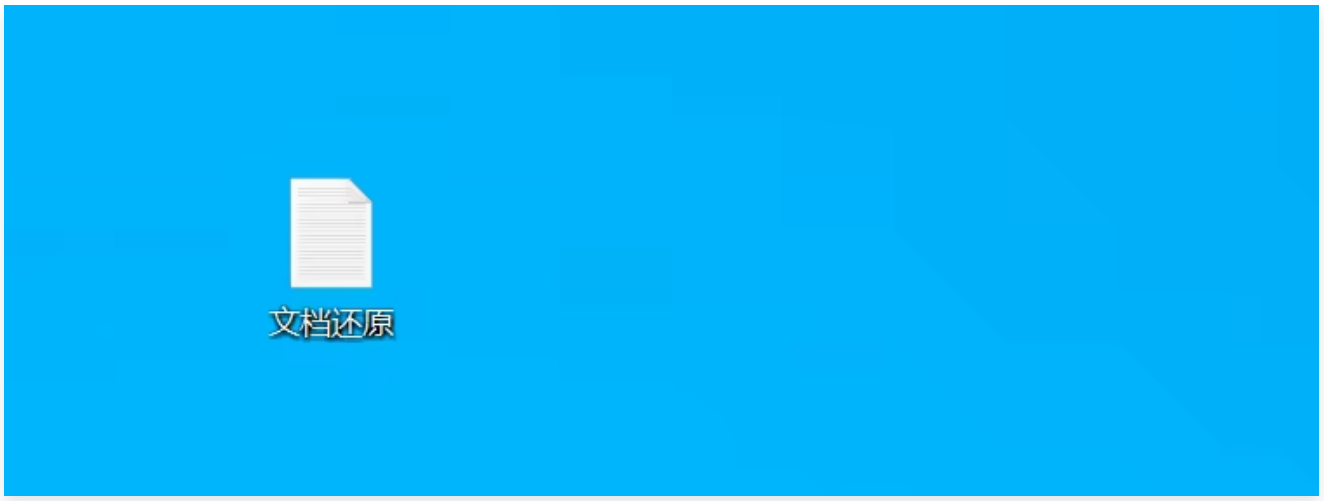


1.2 完成加载后出现如下页面。



2. 创建一个 txt 文档。

2.1 文档名称：文档还原.txt。



2.2 文档内容：11111111。



3. 删除**文档还原.txt**，并在回收站内继续删除。
4. 文档还原。
   4.1 在文档守护者3.0 中，单击**文档找回** > **误删文档找回**。



4.2 选择需要找回的文档，单击**开始还原**。



5. 验证：打开还原的文档，查看内容是否与删除前一致。

配置示例2：找回文档历史版本

1. 加载文档守护者。

1.1 在客户端中单击**文档守护者**。



1.2 完成加载后出现如下页面。

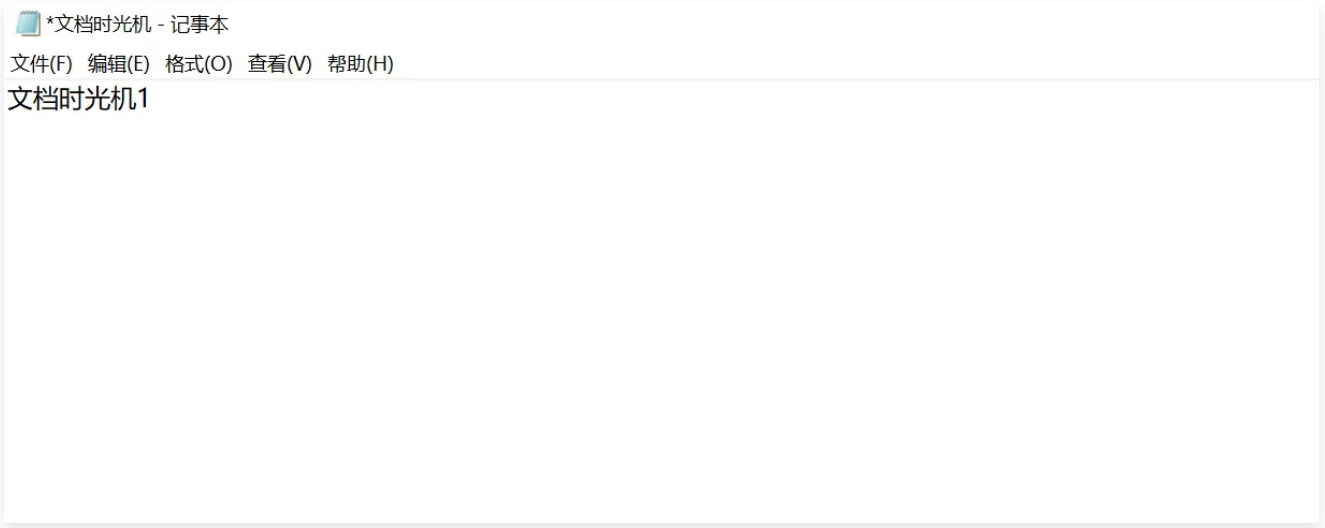


2. 创建一个 txt 文档。

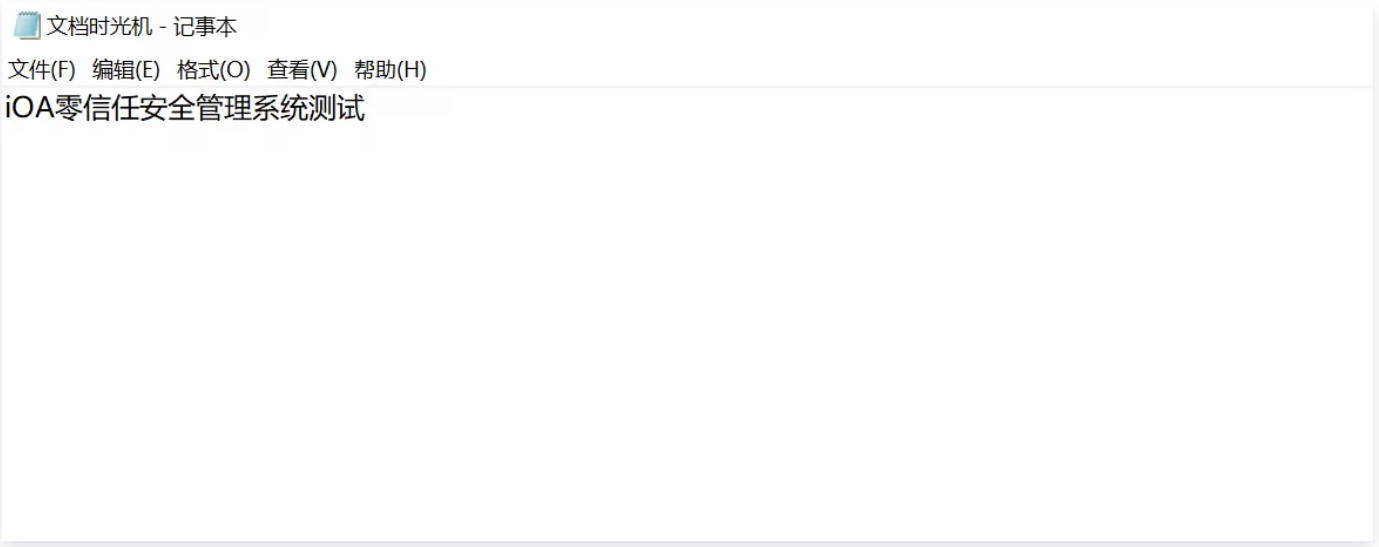
2.1 文档名称：文档时光机.txt。



2.2 文档内容：文档时光机1。



3. 修改文档内容并保存。将文档内容从**文档时光机1**修改为**iOA零信任安全管理系统测试**，单击**保存**。



4. 找回文档历史版本。

4.1 在文档守护者3.0 中，单击**文档找回 > 文档时光机**。



4.2 勾选需要还原的文档，并单击**开始还原**。



5. 验证：打开还原的文档，查看内容是否与删除前一致。

横向渗透防护

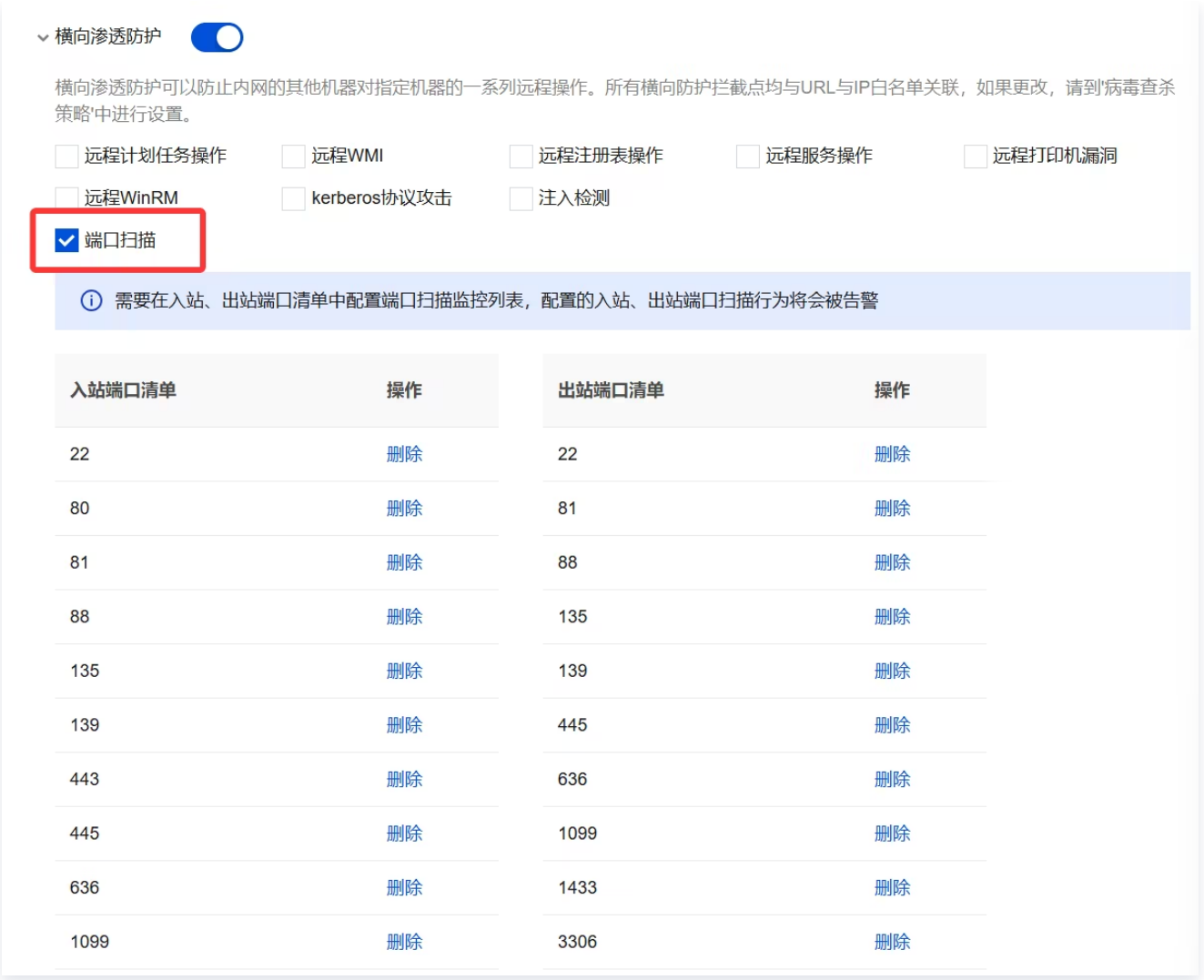
- 横向渗透防护可以防止内网的其他机器对指定机器的一系列远程操作。

> **说明：**
> 所有横向防护拦截点均与 URL 与 IP 白名单关联，如果更改，请到**病毒查杀** > **策略配置** 中进行设置。



  - 远程计划任务操作：防止内网其他机器在本机创建计划任务。
  - 远程 WMI：防止内网其他机器在本机执行 WMI 命令。
  - 远程注册表操作：防止内网其他机器修改本机注册表。
  - 远程服务操作：防止内网其他机器在本机中创建服务。
  - 远程打印机漏洞：防止内网其他机器在本机中连接打印机。
  - 远程 WinRM：防止内网其他机器在本机执行 WinRM 命令。
  - Kerberos 协议攻击：防止利用 Kerberos 协议在域环境内发起攻击。
  - 注入检测：检测可疑的本机进程注入行为。
  - 端口扫描：需要在入站端口清单、出站端口清单中配置端口扫描监控列表，配置的入站、出站端口扫描行为将会被告警。

版权所有：腾讯云计算（北京）有限责任公司



- 远程 DCOM：全局唯一标识符（GUID，Globally Unique Identifier）是一种由算法生成的二进制长度为128位的数字标识符。需要在下方输入远程 COM 的 GUID 拦截点进行使用。

> **注意：**
> 不建议用户自行配置，配置远程 DCOM 需要一定的安全专业知识。默认如下四种，为常用的 DCOM 攻击的手法，已经适用于常规需求。




```
GUID：49B2791A-B1AE-4C90-9B8E-E860BA07F889
dcom 组件：MMC20.Application
GUID：9BA05972-F6A8-11CF-A442-00A0C90A8F39
dcom 组件：ShellWindows
GUID：C08AFD90-F2A1-11D1-8455-00A0C91F3880
dcom 组件： ShellBrowserWindow
GUID：0002DF01-0000-0000-C000-000000000046
dcom 组件：InternetExplorer
```

- 远程共享文件：需要在下方对指定路径进行开启和禁用，启用的目录内的文件将受到防护。



终端欺骗

支持向终端下发勒索诱饵、Web 业务诱饵及 RDP 应用诱饵，并在指定目录下自动生成诱饵文件以引诱攻击者进行攻击进而保护真实网络资产，并触发告警。



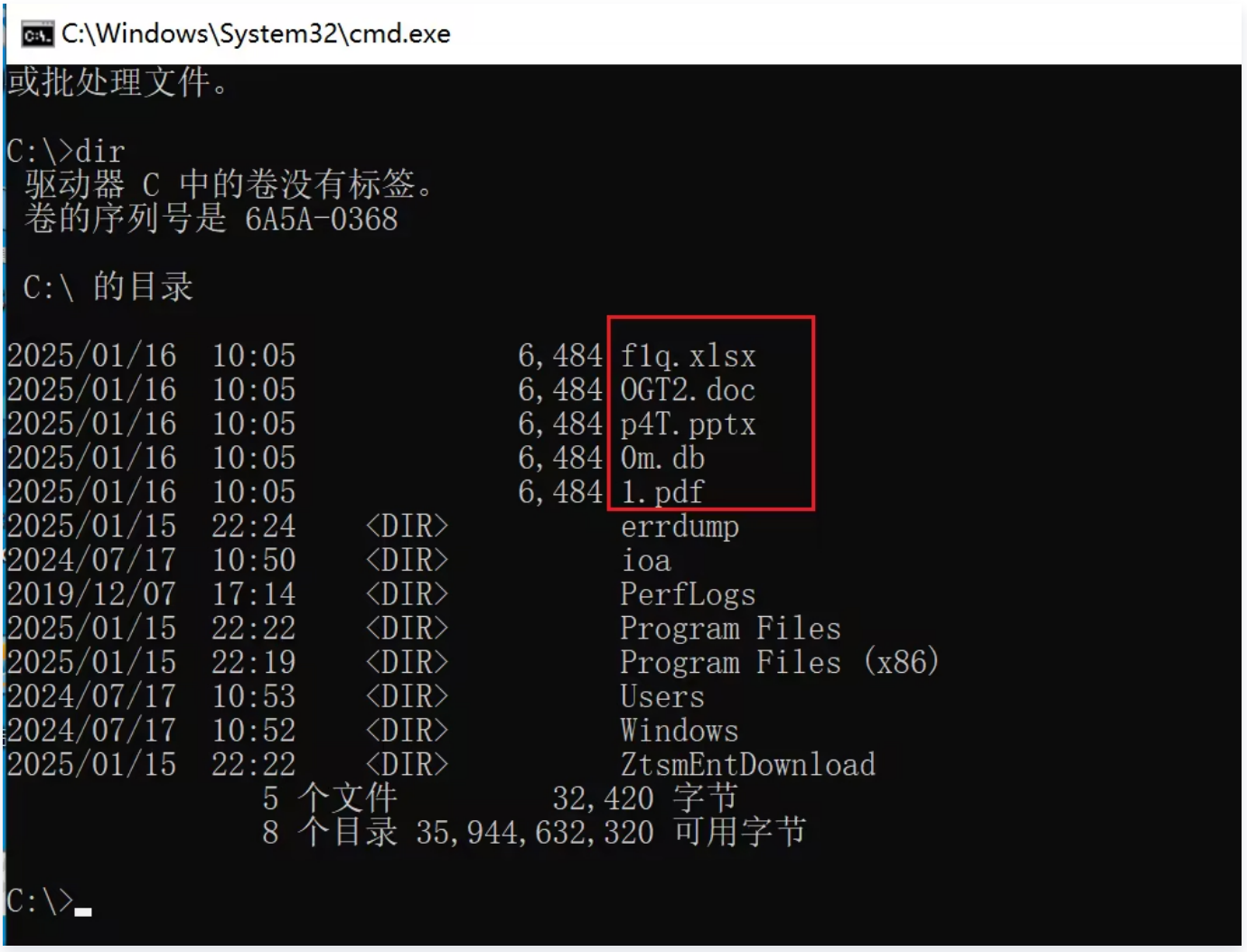
开启勒索欺骗

系统会自动生成勒索诱饵文件到指定目录下，用户对文件有删除和修改等行为会自动触发告警。

1. 勾选**开启勒索欺骗**。



2. 系统自动在盘符根目录下随机生成诱饵文件。



3. 攻击者对诱饵文件进行删除修改等操作。
4. iOA 系统管理员进入**终端防入侵 > 实时防护 > 实时风险**，在实时风险页面筛选**终端欺骗**，查看告警信息。

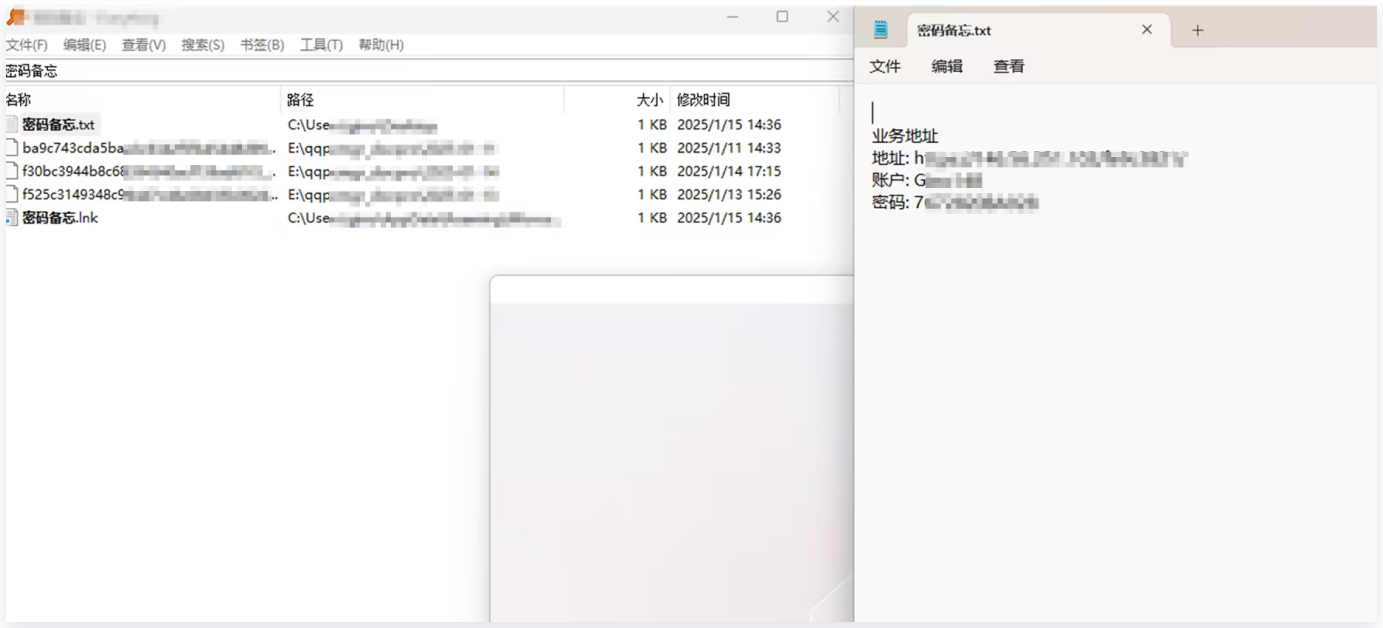
开启 Web 业务诱饵

场景1：系统随机在某盘符下生成密码文件引诱攻击者访问

1. 系统会随机在某个盘符下生成文件夹，其中包含「密码备忘.txt」文件，文件内容包含 URL 以及系统随机生成的账密欺骗信息。
2. 勾选开启 Web 业务诱饵。



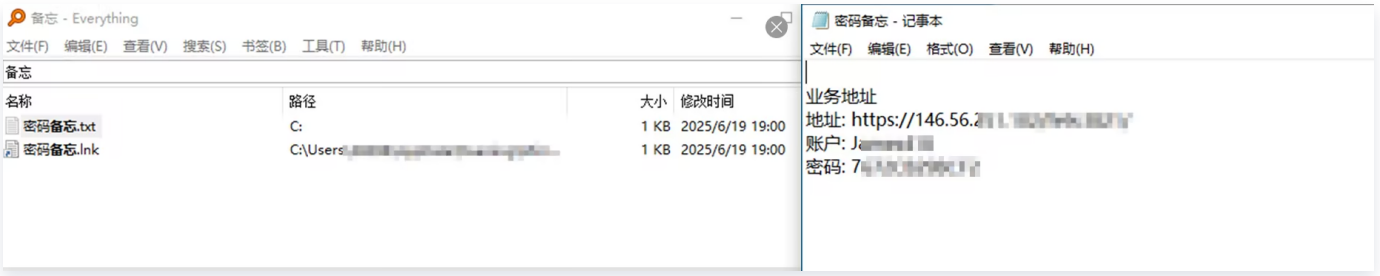
3. 系统自动生成密码文件，攻击者查看密码文件获取系统随机生成的欺骗业务地址密码等信息。



4. 攻击者使用浏览器访问获取的业务地址。
5. iOA 系统管理员进入**终端防入侵** > **实时防护** > **实时风险**，在实时风险页面筛选**终端欺骗**，查看告警信息。

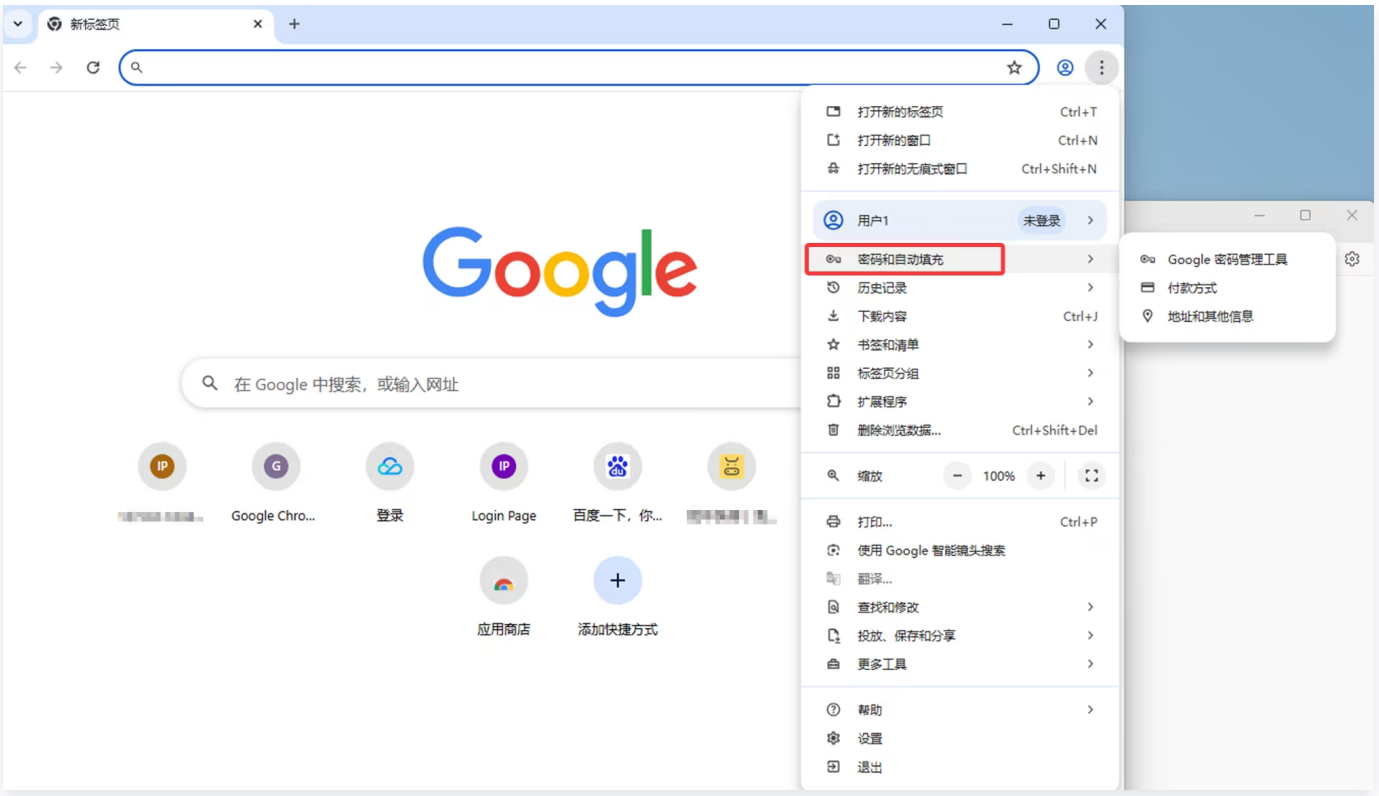
场景2：系统自动在 Chrome/Edge 内核浏览器的密码数据库中插入 URL 账号密码引诱攻击

1. 勾选开启 Web 业务诱饵。
2. 开启 Web 业务诱饵后，系统随机在某个盘符下生成密码文件。

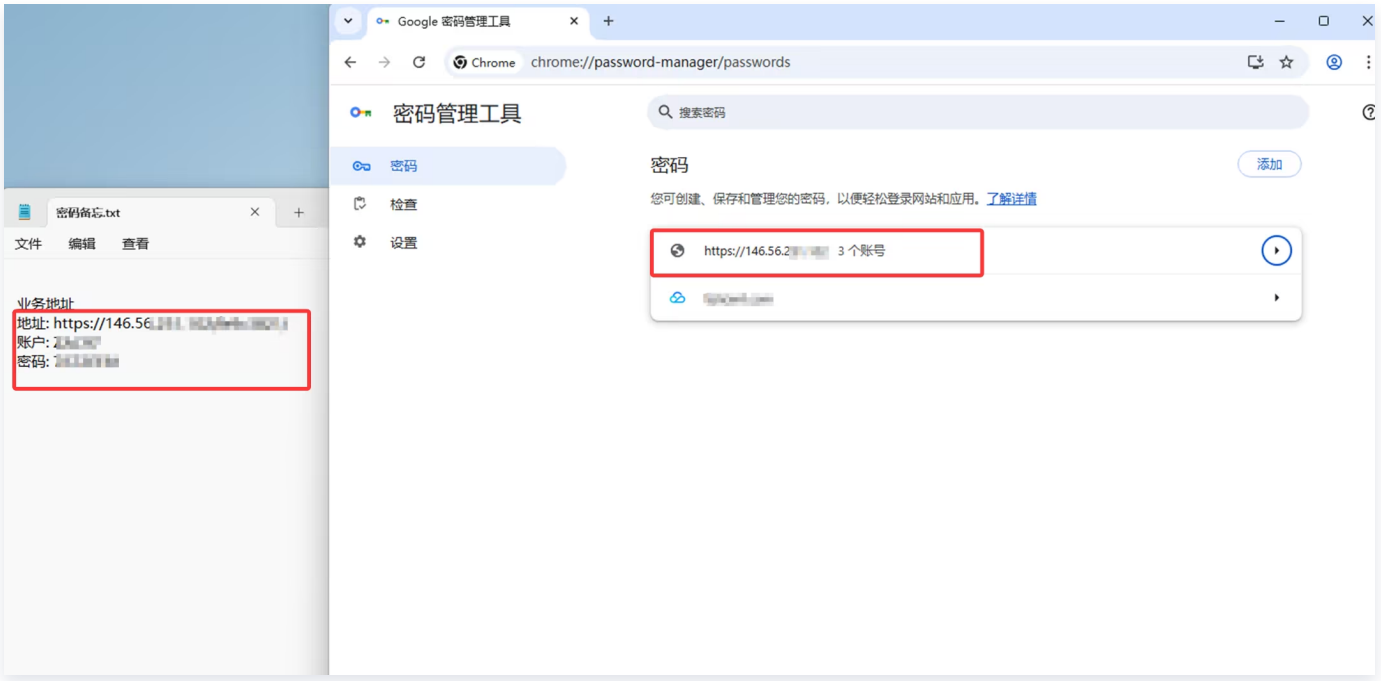


3. 在 Chrome 浏览器中，单击**密码和自动填充**。

> **说明：**
> Edge 浏览器查看已保存密码的路径请以浏览器官方指定的路径为准。



4. 系统自动在 Chrome/Edge 内核浏览器的密码数据库中插入 URL 链接，账号密码。



5. 攻击者使用浏览器访问获取的业务地址。
6. iOA 系统管理员进入**终端防入侵 > 实时防护 > 实时风险**，在实时风险页面筛选**业务欺骗事件**，查看告警信息。

开启RDP 应用诱饵

场景1：系统随机在某盘符下生成密码文件引诱攻击者访问

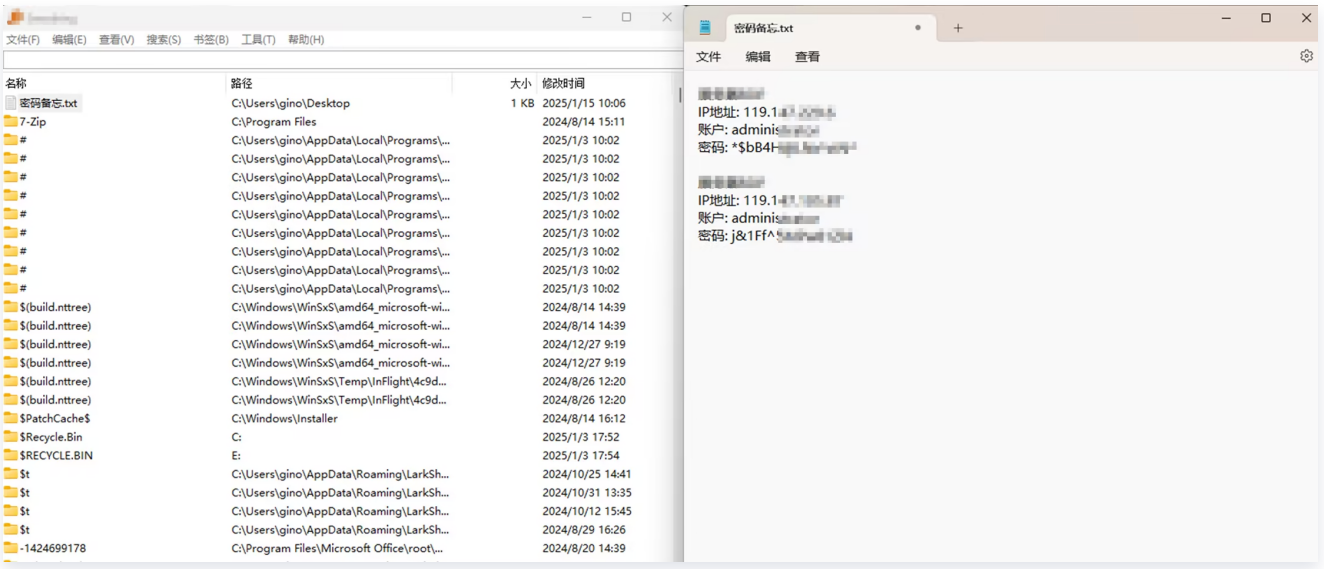
1. 系统会随机在某个盘符下生成文件夹，其中包含「密码备忘.txt」文件，文件内容包含 IP 地址（随机生成两个）以及系统随机生成的账密欺骗信息。
2. 勾选开启 RDP 应用诱饵，单击**添加**。



3. 系统自动生成 IP 地址，您无需填写 IP 地址信息，输入备注后单击**确定**。



4. 终端验证。
   4.1 系统随机在某个盘符下自动生成密码文件，文件内容包含 IP 地址（随机生成两个）、以及系统随机生成的账户，密码信息。



4.2 攻击者远程连接服务器，连接失败。

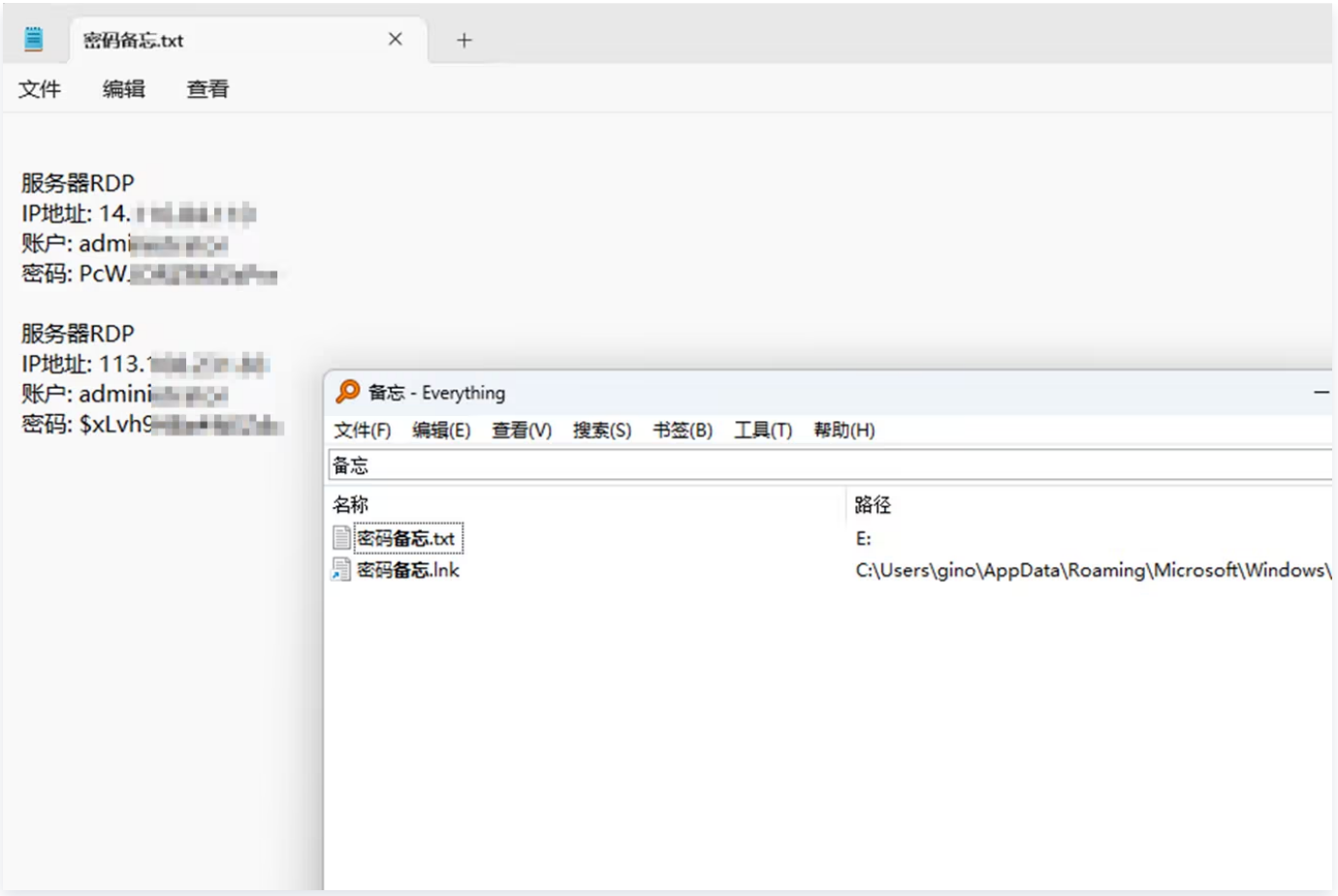
4.3 iOA 系统管理员进入**终端防入侵 > 实时防护 > 实时风险**，在实时风险页面筛选 **RDP 欺骗事件**，查看告警信息。

场景2：在 Windows 系统登录凭据中插入 RDP 的 IP、账号、密码引诱攻击

1. 勾选 RDP 应用诱饵，单击**添加**。
2. 系统自动生成 IP 地址，您无需填写 IP 地址信息，输入备注后单击**确定**。



3. 系统随机在某个盘符下自动生成密码文件，文件内容包含 IP 地址（随机生成两个）、以及系统随机生成的账户，密码信息。



4. 进入Windows 电脑**控制面板 > 用户账户 > 凭据管理器 > Windows 凭据**。



5. 在系统登录凭据中自动插入 RDP 的 IP、账号、密码信息，该IP地址账户密码信息为系统随机生成的欺骗信息。



6. 攻击者远程连接服务器，触发告警。
7. iOA 系统管理员进入**终端防入侵 > 实时防护 > 实时风险**，在实时风险页面筛选 RDP 欺骗事件，查看告警信息。

漏洞利用防御

支持多种漏洞利用攻击的防御，一旦发现网络入侵攻击，会进行告警。

> **注意：**
> 开启后可能对终端的网络性能有一定影响，请谨慎开启。在开启后，请做好测试验证，确认无异常之后再逐步灰度扩大影响范围。



开启密码爆破防御

可根据企业的防护安全等级，进行选择性开启，一般建议开启，支持爆破阈值设置。

> **说明：**
> **开启后可能对终端的网络性能有一定影响，请谨慎开启。**在开启后，请做好测试验证，确认无异常之后再逐步灰度扩大影响范围。



热点问题

多个策略执行逻辑是什么?

- 可能出现在一个用户命中多条策略，系统执行多个策略合并生效的逻辑，不同策略设置的策略项若存在冲突，此时系统将通过优先级来决定如何执行策略。
- 例如：同时设置A、B两条策略，均命中某一终端X，其中A策略开启了「文档防护」「钓鱼防护」，B策略仅开启了「钓鱼防护」，由于「文档防护」无策略冲突，那么终端X的文档防护策略项会按照A策略的设置生效，而

「钓鱼防护」有策略冲突，那么终端X的钓鱼防护策略项会按照A、B策略优先级更高的策略设置生效。

执行优先级的逻辑是什么?

- 优先级数字越大，策略越优先执行；
- 优先级可配置的范围是1~100；
- 优先级允许相同，将通过系统内置的优选策略执行策略。

系统内置优选策略逻辑是什么?

系统内置优选对比维度包括：策略管控对象、策略严格度和策略创建时间。

- 策略管控对象：粒度越精准越优先，单个终端/用户>自定义组>组织架构；
- 策略严格度：策略项内配置得越严格，越优先；
- 策略创建时间：策略越新创建，越优先执行；
- 详细策略请查看使用手册，或联系我们 。

实时风险（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

风险告警查看

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **实时防护** > **实时风险**。
2. 在实时风险页面，展示扫描到的风险详情，支持数据筛选及统计：
   - 时间筛选：默认7天，支持用户自定义筛选范围。
   - 处置结果：支持筛选全部处置结果、系统自动处置、客户端问询、拦截失败、仅审计等状态。
   - 检出引擎：支持按全部引擎、云引擎、TAV引擎、威胁情报筛选。
   - 关联策略：支持按进程防护、文件下载防护、U盘防护、应用层防护等策略检测项筛选。
   - 终端范围：单击展示终端筛选组件，对应展示目标终端下的病毒相关数据，默认全部终端。
   - 支持按风险视角及终端视角查看。



3. 选择目标风险，单击**详情**查看风险详情。



导出数据

1. 在实时风险页面，单击右上角的按钮 。



2. 勾选自定义表头、导出时间参数，单击**导出**。


导出预设
数据超过8000条，将生成单独的导出任务，请到 任务中心 查看导出进度
自定义表头
全选
风险名称
处置结果
操作者
操作目标
攻击详情
检出时间
攻击时间
检出引擎
关联策略
关联检测项
终端名
病毒导出时间
近7天
近10天
近30天
2026-01-12 00:00:00 ~ 2026-01-19 23:59:59
目标导出时间：2026-01-12 00:00:00～2026-01-19 23:59:59
导出天数：7天23小时59分59秒
其他信息
导出格式：CSV
预计导出条数：0条
导出
取消

审计日志（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **实时防护** > **审计日志**。
2. 在审计日志页面，展示所有检出实时风险的日志情况，支持按时间以及各字段属性筛选。



导出日志

单击右上角 ，勾选自定义表头、导出时间参数，单击**导出**。


导出预设
数据超过8000条，将生成单独的导出任务，请到 任务中心 查看导出进度
自定义表头
全选
终端名
检出时间
攻击时间
风险名
操作者进程名称
子进程路径
线程模块名
命令行
处置结果
GUID
本机身份
网络攻击类型
网络攻击详情
网络攻击流量
关联策略
关联检测项
日志导出时间
近7天
近10天
近30天
2026-01-13 00:00:00 ~ 2026-01-19 23:59:59
目标导出时间：2026-01-13 00:00:00～2026-01-19 23:59:59
导出天数：6天23小时59分59秒
其他信息
导出格式：CSV
预计导出条数：0条
导出
取消

高级威胁防护EDR（11.1.1版）
功能简介（11.1.1版）

最近更新时间：2026-02-06 14:23:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

iOA 零信任安全管理系统的 EDR（Endpoint Detection and Response）是一种基于端点的安全解决方案，旨在实时监控和检测恶意活动，保护企业网络以降低受攻击的风险和数据泄露的可能性。同时，EDR 作为安全运营的利器，能够提供从风险检测到告警，再到威胁事件链条式的威胁响应，帮助企业的终端安全运营工作由被动转为主动，有效防御 APT 攻击。

使用场景

应对/预防变化多端的商业化 APT 攻击场景

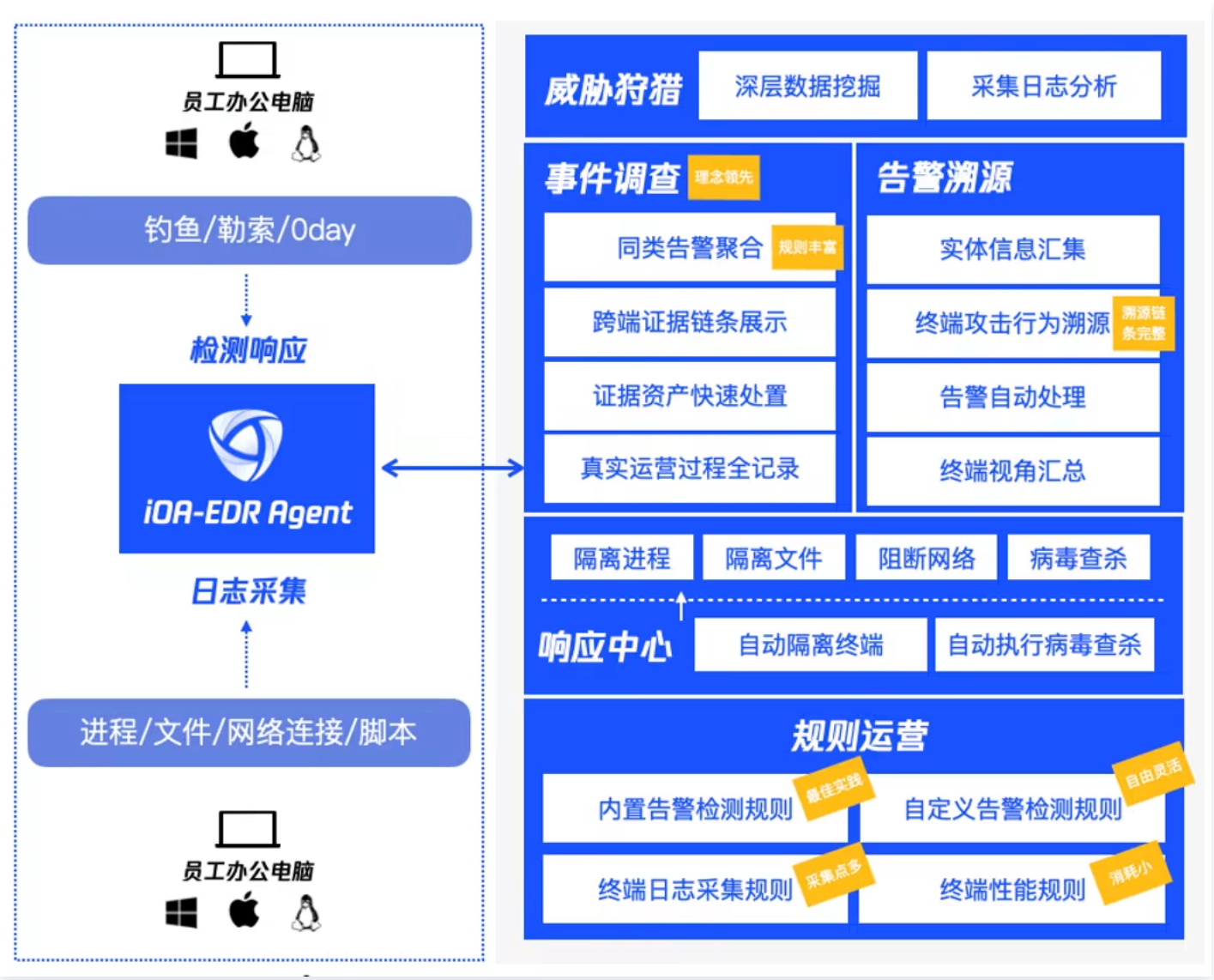
随着全球数字化进程的加速，企业和组织的信息安全面临着越来越严重的威胁。其中，高级持续性威胁（Advanced Persistent Threat，简称 APT）已成为当今极具破坏力的网络攻击手段之一。商业化 APT 攻击更是结合了高度定制化的恶意软件、0day漏洞利用、精确的社会工程学等手段，易对企业资产造成重大损失。

多设备协同办公，终端安全建设升级场景

企业拥有大量员工，而员工在多个地点使用不同的设备（例如笔记本电脑、平板电脑和智能手机）进行协同办公的趋势也日益明显。企业需要检测评估这些设备的安全性，防范数据泄露和网络攻击风险，并落实数据安全等相关合规要求。

EDR 架构

功能架构



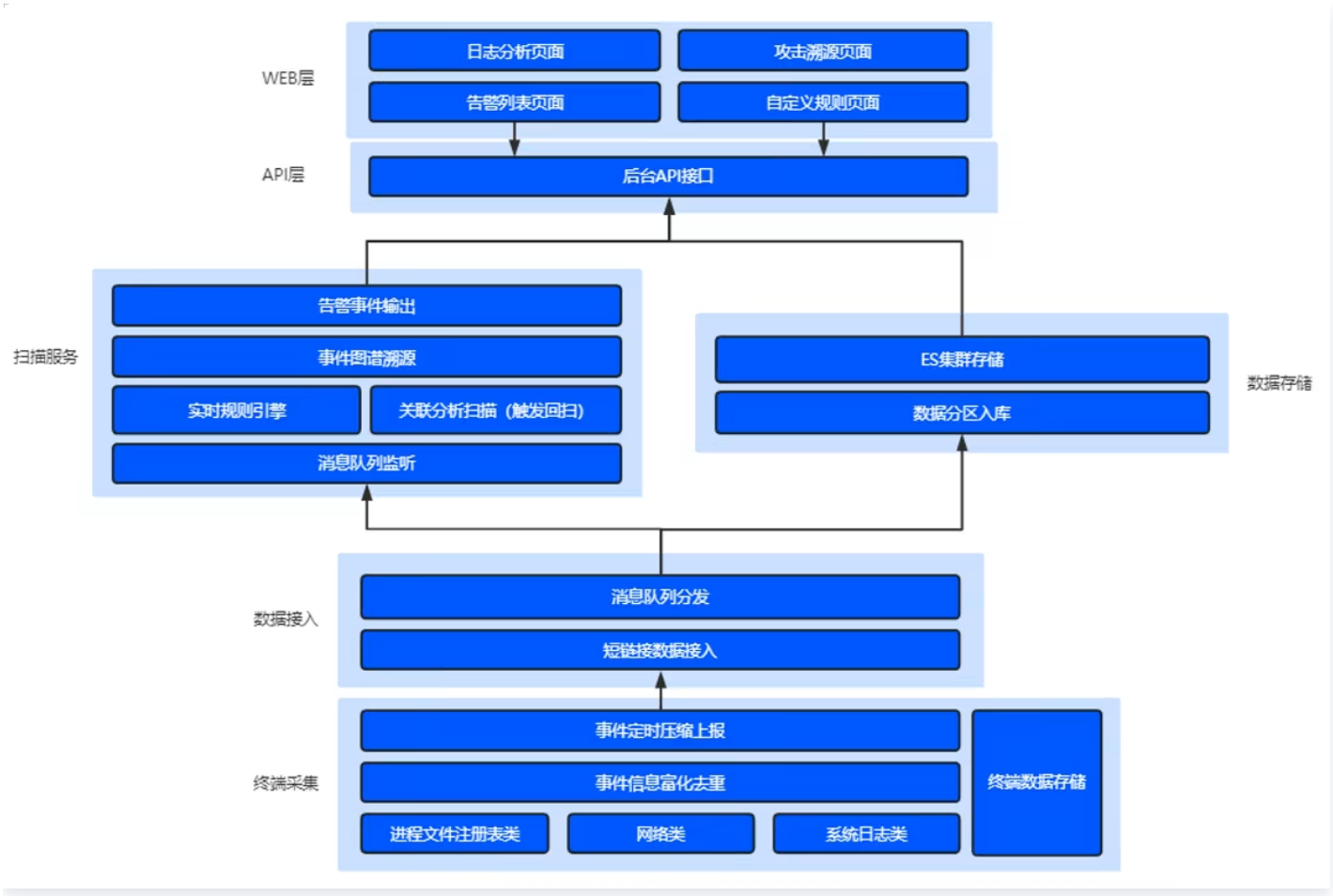
ATT&CK 模型下的腾讯安全运营规则实践教程与灵活的自定义能力。

- 运营规则多方面覆盖 ATT&CK 攻击链路，对勒索病毒、挖矿病毒等高危威胁实现重点检测。
- 通过丰富多样的运营规则，针对钓鱼攻击、无文件攻击，东西向横移，远程漏洞利用等场景可以实现准确识别；除了丰富的内置规则外，另支持用户灵活自定义规则，适应于更多的用户使用场景以及个性化需求。
- 证据视角下的跨终端安全事件调查与全网响应。
- 事件调查：从证据视角切入、根据事件的风险性进行研判、最终对该事件进行处置，形成整体安全运营流程。
- 告警溯源：多点行为关联，弱链、断链补全，还原完整攻击事件。
- 威胁响应：支持自动响应与人工全网处置结合。
- 性能占用小与跨平台能力：终端性能占用小且能够有效兼容老旧客户端设备，同时支持包括 Windows、macOS、Android、iOS 在内的多种主流操作系统。

能力逻辑架构

终端数据采集、实时规则检测、关联分析溯源到上层应用展示的完整安全事件处理流程。

版权所有：腾讯云计算（北京）有限责任公司



终端采集

采集 EDR 所需的各类终端数据，对采集数据富化和过滤，数据同时本地存储和上报到后台处理。

扫描服务

支持实时的威胁检测规则，支持多行为的关联模型规则，支持对告警做溯源分析挖掘。

数据存储

数据按终端分区存储，提供快速查询，ES 集群实现大数据的存储。

页面功能

支持标准的 API 接口，运营规则开放自定义。

版权所有：腾讯云计算（北京）有限责任公司

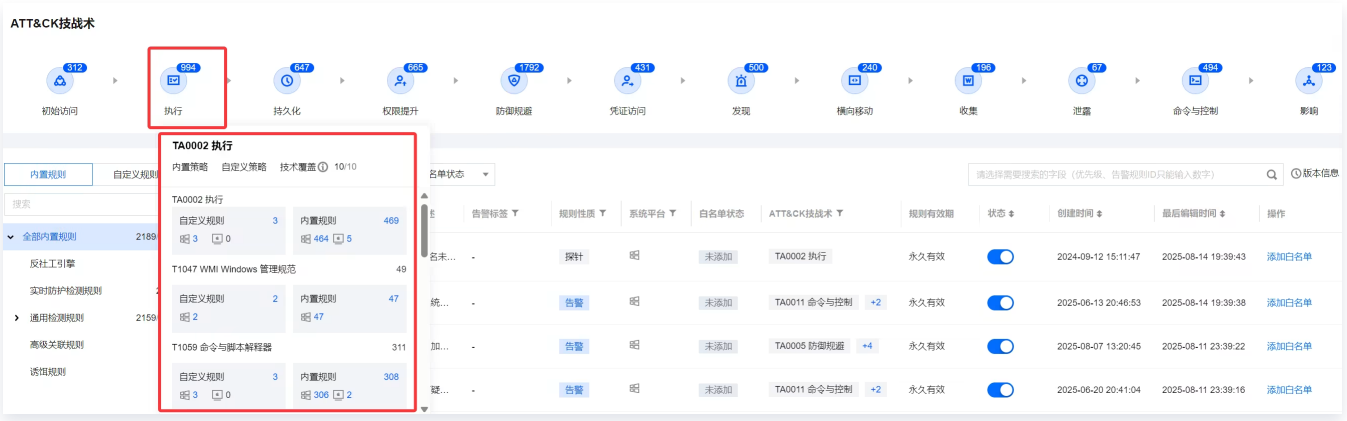
策略规则（11.1.1版）
行为检测（11.1.1版）

最近更新时间：2026-02-13 09:41:02

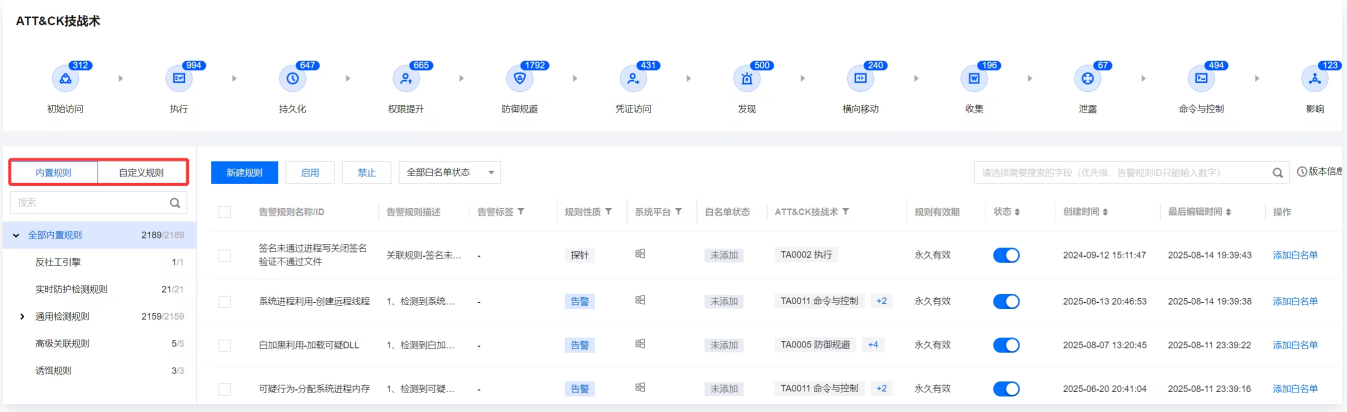
> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

策略分布统计

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 策略规则 > 行为检测**。
2. 在行为检测页面，支持以 ATT&CK 技战术全流程视角查看当前规则分布，鼠标单击**展示栏各项**，可看到细分技战术的内置规则以及自定义规则统计数据。



3. 用户可以通过左侧目录查看**内置规则**以及**自定义规则分类**，并且可以自主创建子目录的形式将规则进行归纳整理。



规则创建和运营

内置规则

1. 在规则运营的内置规则页面，支持用户针对目标规则**启用、禁用、拷贝、删除、导出、导入**功能。



2. 支持用户选择目标文件、MD5等加入白名单，该规则对于白名单文件将不会产生告警。选择一条规则，单击**添加白名单**，该白名单为单一规则白名单入口，配置后仅针对该规则生效。

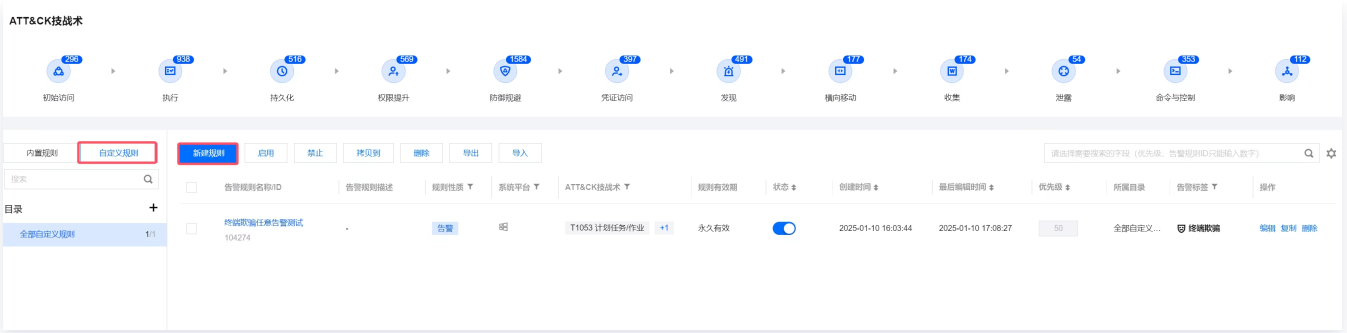


3. 配置白名单规则信息，选择加白的字段与条件关系，配置完成单击**确定**保存。

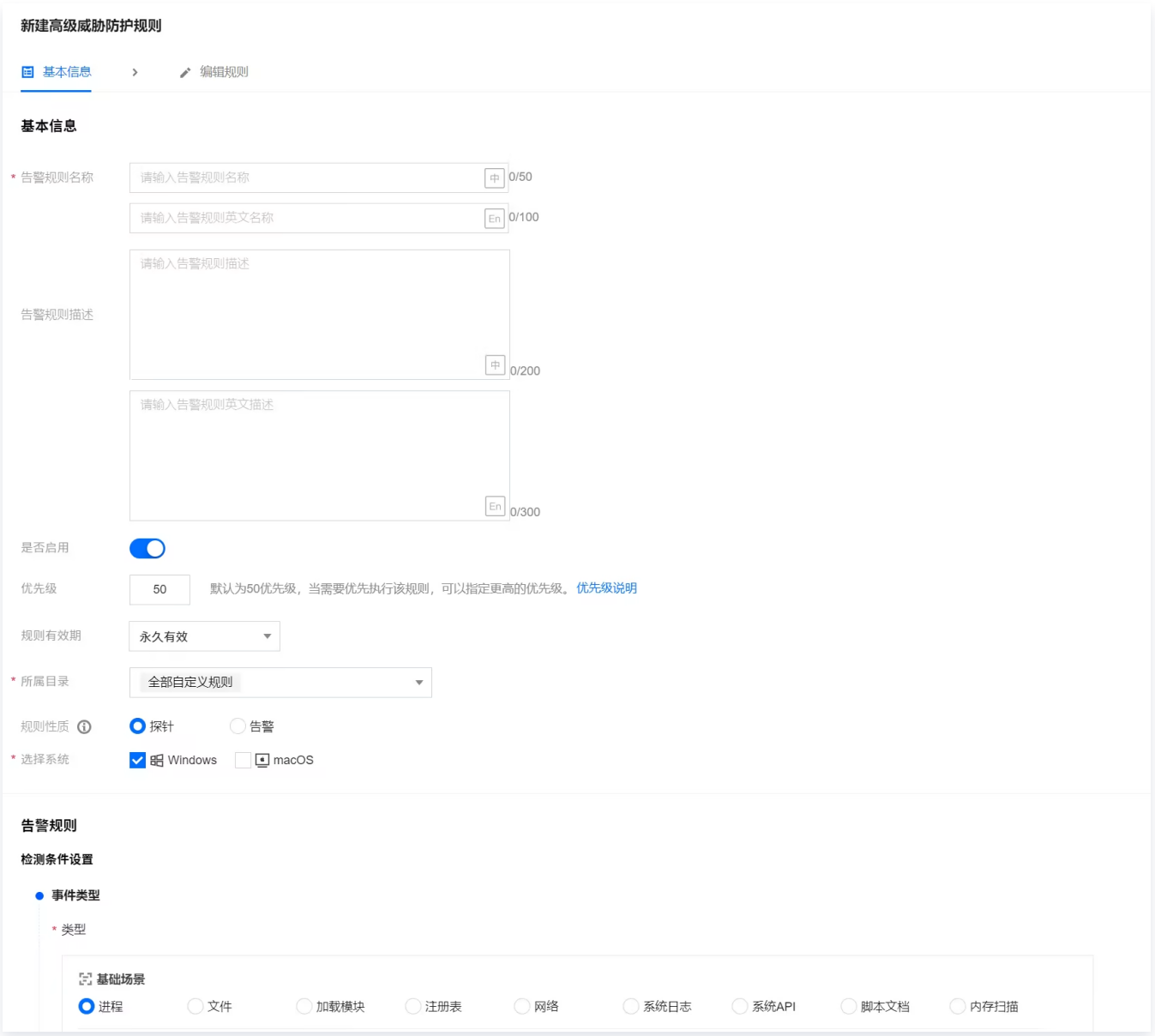


自定义规则

1. 在规则运营的自定义规则页面，支持对企业的独特规则或者是应急响应，灵活配置安全规则，以适用于企业的安全运营需求，单击**新建规则**。



2. 在新建高级威胁防护规则页面，配置相关参数。



参数名称	说明
告警规则名称	自定义告警规则名称，支持1-50字符。

告警规则描述	自定义规则描述，支持1-200字符。
是否启用	默认开启。
优先级	默认为优先级50，当需要优先执行该规则，可以指定更高的优先级。 • 优先级数字越大，规则越优先执行。 • 优先级可配置的范围是1~100。 • 优先级允许相同，将通过系统内置的优选规则执行规则。 • 兜底的全局基线规则优先级为0，不允许修改。
规则有效期	支持自定义时间/永久有效。
所属目录	选择所属目录。
规则性质	需要选择**告警**、**探针**，如选择探针。该信息日志在威胁调查狩猎页面可查询。
检测条件	支持选择基础日志类型、高级威胁类型、行为。
告警条件	支持选择多个并匹配对应目标内容，同时多个字段/字段组可选择或/且的关系进行组合。新增「操作者父信息」日志采集分类，行为告警更精准。
告警频率	在一个终端 X 分钟内告警一次。
ATT&CK 技战术	根据当前规则所属的技术阶段选择对应的技战术，对于特殊场景的规则，例如钓鱼、勒索、横移场景，会根据对应的技战术在告警和事件页面对应分场景展示。
告警标签	告警标签类型在威胁告警和威胁事件中展示。
定义严重级别	标识告警严重程度，以此判定触发该规则产生的告警风险等级。
添加自动响应规则	在创建告警规则的同时直接添加对应的响应策略（系统将自动保存此条行为检测规则，并将规则信息带入至自动响应规则中）。

3. 配置完成单击**保存**。

行为检测白名单（11.1.1版）

最近更新时间：2026-02-13 09:41:02

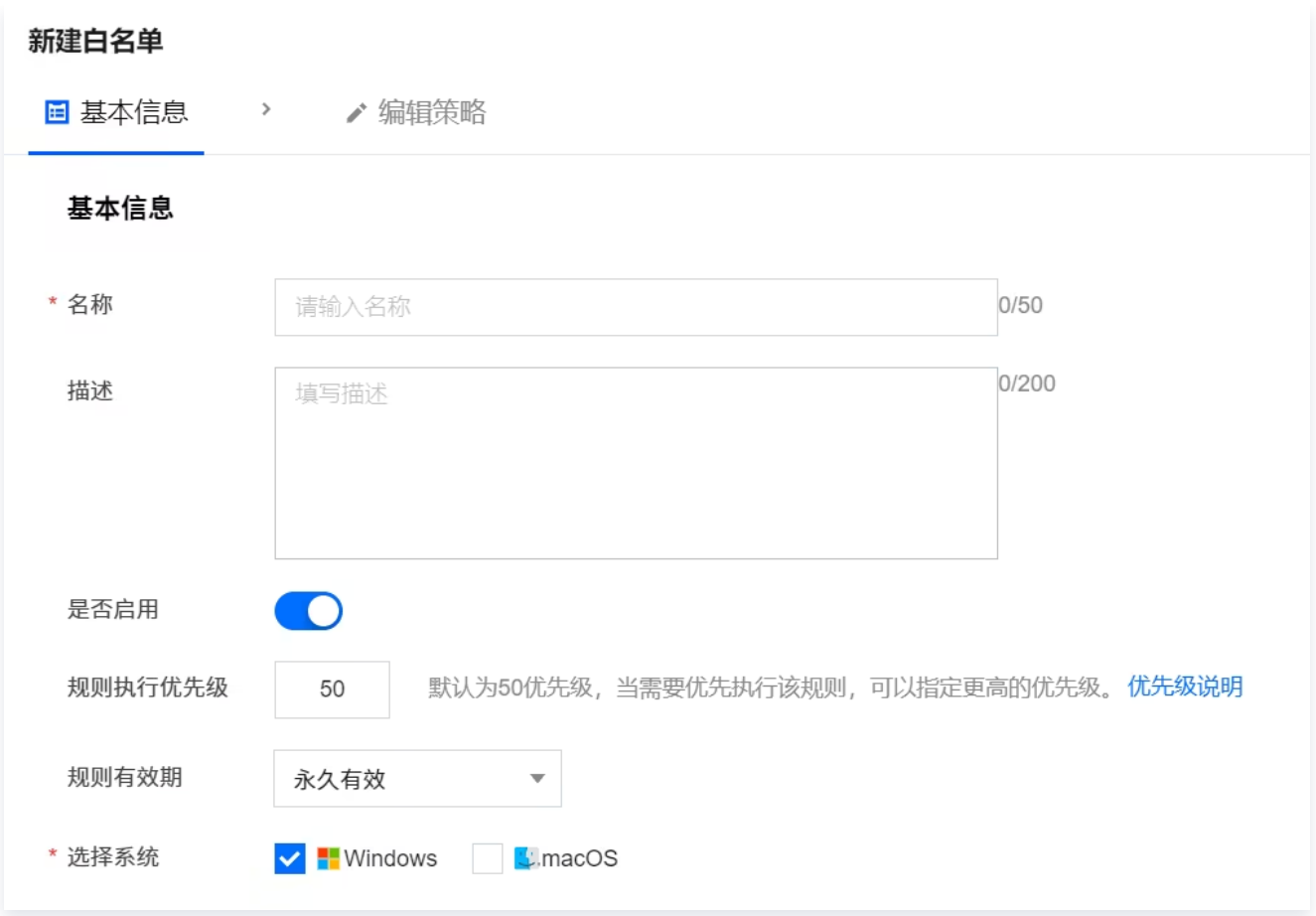
> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

行为检测白名单支持全局信任规则配置，针对性优化现有告警策略的精准度，降低因误报导致的无效告警量，减少无效告警处理时间，降低运维压力。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **高级威胁防护（EDR）** > **策略规则** > **行为检测白名单**。
2. 在行为检测白名单页面，单击**新建白名单**。



3. 在新建白名单策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。



3.2 选择系统：支持配置 Windows / macOS，勾选后的系统白名单策略生效。

3.3 配置检测条件，单击**选择配置的字段信息**。支持对指定字段（如进程 PID、文件 md5）等添加信任规则，匹配到对应内容时直接忽略告警。



3.4 支持添加条件或条件组，条件之间可使用或/且，单击**更改或/且**的关系式。



4. 配置完成单击**确定**保存。

行为采集（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

通过下发策略采集终端进程、文件、模块、注册表、网络等内核事件，及终端系统日志、APIHOOK 事件、脚本事件信息，并最终生成日志。

新建策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **高级威胁防护（EDR）** > **策略规则** > **行为采集**。
2. 在行为采集页面，单击**新建策略**。
   2.1 基本信息。



参数名称	说明
策略名称	填写策略名称（例：EDR 信息采集基线策略）。
策略描述	建议明确该策略关键信息，避免后续无法查询。
是否启用	默认开启。
优先级	默认50，如需优先执行该策略，可以提高优先级数值。
策略有效期	默认永久有效，可指定失效时间。

选择系统	支持按照 Windows、Mac 不同系统调整策略。

2.2 适用范围。

支持按照适用终端、适用用户、例外终端以及例外用户等维度指定策略生效范围，其中终端与账号都支持指定具体的终端名称以及账号名称，同时支持按照组织架构和自定义分组批量勾选。



2.3 终端数据采集。

勾选该模块后选择数据采集范围，根据 行为采集范围说明 ，支持一键勾选目标事件库作为采集点，同时支持针对该事件库中包含的具体行为采集点进行**勾选/取消勾选**。



2.4 性能配置：支持端性能的控制，可以自定义选择终端性能要求。



参数名称	说明
终端性能配置	用于限制 EDR 进程 CPU 占用，防止 CPU 占用过高，影响终端性能；如果没有严格的终端性能要求，建议仅限制按进程维度的事件处理流；如果终端性能不高，建议综合考虑总体事件处理流限制和 CPU 限制。
网络带宽	用于限制带宽占用，防止带宽占用过高，影响终端传输性能。
内存配置	用于限制 EDR 进程内存占用，防止内存占用过高，影响终端性能。
本地存储配置	• 通过设定最大存储空间，可控制磁盘总容量，防止存储无限增长； • 配置最大存储时间，确保数据按周期保存，及时清理陈旧文件； • 限定最大返回结果，优化日志检索效率，避免单次查询数据量过大影响性能。

3. 确认内容无误后，单击**保存**。

行为采集范围说明

事件规则库	事件名称	事件详情
内核事件库	进程事件（ProcEvents）	存储由终端探针采集上报的数据，包含执行进程创建、打开、注入等进程相关的动作数据。
	文件事件（FileEvents）	存储由终端探针采集上报的数据，包含执行文件创建、读写、映射、删除等文件相关的动作数据。
	文件统计事件（FileStatisticsEvents）	存储由终端探针采集上报的数据，包含执行文件的写、重命名、删除等操作，在目录、后缀等维度上的统计数据，用来发现和识别勒索加密类攻击。

	文件磁盘事件（FileDiskEvents）	存储由终端探针采集上报的数据，包含直接对磁盘的读、写等动作数据，用来发现和识别系统底层的绕过和破坏攻击。
	模块事件（ModuleEvents）	存储由终端探针采集上报的数据，包含执行驱动加载、模块加载等加载相关的动作数据。
	注册表事件（RegEvents）	存储由终端探针采集上报的数据，包含执行注册表创建、设置、删除等注册表相关的动作数据。
	网络事件（NetworkEvents）	存储由终端探针采集上报的数据，包含执行 DNS 查询、各类网络请求等网络相关的动作数据。
系统日志库	WMI 事件（WMIEvents）	存储由 Windows 日志采集上报的数据，包含执行 WMI 操作、WMI 创建进程等 WMI 相关的动作数据。
	系统变更事件（SystemChangeEvents）	存储由 Windows 日志采集上报的数据，包含执行关闭事件日志、清除安全日志等系统变更相关的动作数据。
	登录事件（LoginEvents）	存储由 Windows 日志采集上报的数据，包含执行用户登录、凭据登录等系统登录相关的动作数据。
	特权操作事件（PrivilegeEvents）	存储由 Windows 日志采集上报的数据，包含特权对象执行、特权对象变更等特权操作相关的动作数据。
	计划任务事件（ScheduleTaskEvents）	存储由 Windows 日志采集上报的数据，包含执行计划任务创建、删除、更新等计划任务相关的动作数据。
	用户账户事件（AccountEvents）	存储由 Windows 日志采集上报的数据，包含执行用户账号创建、更改、重置等用户账户相关的动作数据。
	网络共享事件（NetShareEvents）	存储由 Windows 日志采集上报的数据，包含执行网络共享对象访问、添加、修改等网络共享对象相关的动作数据。
系统 API 事件库	高级威胁事件（ThreatEvents）	存储由终端探针采集上报的数据，包含执行事件日志关闭、反调试等威胁对抗相关的动作数据。
	加密事件（CryptEvents）	存储由终端探针采集上报的数据，包含执行加密文件、调用加密组件等加密相关的动作数据。

版权所有：腾讯云计算（北京）有限责任公司

	远程注入事件（RemoteInjectEvents）	存储由终端探针采集上报的数据，包含执行远线程注入、APC 注入，内存修改等远程注入相关的动作数据。
	提权事件（PrivilegeEscalationEvents ）	存储由终端探针采集上报的数据，包含执行获取令牌、模拟登录，查询特权进程等提权相关的动作数据。
	用户凭据事件（CredentialsEvents）	存储由终端探针采集上报的数据，包含对账户组或凭据执行枚举、备份、解析等账户凭据相关的动作数据。
	服务器探测事件（ServerDetectEvents）	存储由终端探针采集上报的数据，包含对服务器执行共享资源检索、账户组枚举、域信息检索等服务器探测相关的动作数据。
	网络访问事件（InternetEvents）	存储由终端探针采集上报的数据，包含调用 WinINET 发起的网络请求等网络访问相关的动作数据。
	进程文件信息收集（ProcFileInfoEvents）	存储由终端探针采集上报的数据，包含执行进程和文件的快照、枚举等进程文件信息相关的动作数据。
	文件操作事件（DirOperationEvents）	存储由终端探针采集上报的数据，包含执行文件和目录的网络拷贝、移动、删除等文件网络相关的动作数据。
	系统信息收集（SystemInfoEvents）	存储由终端探针采集上报的数据，包含对磁盘空间、系统版本、计算机名称、网络连接进行检索等系统信息收集相关的动作数据。
	信息窃取（InfoTheftEvents）	存储由终端探针采集上报的数据，包含对键盘输入、剪贴板、窗口输入进行监听等信息窃取相关的动作数据。
	服务事件（ServiceEvents）	存储由终端探针采集上报的数据，包含服务的创建、启动、修改、删除、停止等操作服务相关的动作数据。
脚本文档事件库	脚本事件(ScriptEvents)	存储由终端探针采集上报的数据，包含对 PowerShell、VBS、JS 等脚本相关的动作数据。
	Office 事件（DocumentOpen）	存储由终端探针采集上报的数据，包含打开文档的动作数据。

断链事件库	压缩包关联事件（ArchiveAssocEvents）	存储由终端探针采集上报的数据，通过持续监测压缩包创建、解压、释放等行为，包含解压释放的文件关联到压缩包母体的动作数据。
	Rundll 关联事件（RundllAssocEvents）	存储由终端探针采集上报的数据，包含执行Rundll32执行文件的动作数据。
	命令行关联事件（CmdLineAssocEvents）	存储由终端探针采集上报的数据，通过解析命令行关联攻击文件，包含执行脚本，无文件利用、远程下载等断链绕过的动作数据。
	快捷方式启动关联事件（LnkAssocEvents）	存储由终端探针采集上报的数据，包含快捷方式启动脚本、可执行文件、命令等断链绕过的动作数据。
横移事件库	远程服务事件（RemoteServiceEvents）	存储由终端探针采集上报的数据，包含服务的创建、启动、修改、删除、停止等远程操作服务相关的动作数据。
	远程计划任务事件（RemoteTaskEvents）	存储由终端探针采集上报的数据，包含 at、schtasks 等计划任务远程执行命令的动作数据。
	远程注册表事件（RemoteRegEvents）	存储由终端探针采集上报的数据，包含注册表创建、设置、删除等远程操作注册表相关的动作数据。
	远程 WMI/DCOM 事件（RemoteWMI-DCOMEvents）	存储由终端探针采集上报的数据，包含远程调用 DCOM 和 WMI 等相关的动作数据。
	远程漏洞事件（RemoteCVEEvents）	存储由终端探针采集上报的数据，包含各类远程执行的漏洞等相关的动作数据。
	共享文件事件（WriteShareDirEvents）	存储由终端探针采集上报的数据，包含对共享文件进行修改等相关的动作数据。
	远程访问事件（RemoteControlEvents）	存储由终端探针采集上报的数据，包含对远程终端访问、控制等相关的动作数据。
勒索事件库	勒索诱饵事件（DocTrapEvents）	存储由终端探针采集上报的数据，包含修改诱饵文件相关的动作数据。
	RDP 欺骗事件（RDPTrapEvents）	存储由终端探针采集上报的数据，包含命中终端欺骗 URL 陷阱等相关的动作数据。

	业务欺骗事件（BusinessTrapEvents）	存储由终端探针采集上报的数据，包含传输文件、压缩包然后联网等钓鱼攻击方式的数据。
钓鱼事件库	钓鱼事件（PhishingEvents）	存储由终端探针采集上报的数据，包含钓鱼相关的动作数据。
	内存扫描事件（MemoryScanEvents）	存储由终端探针采集上报的数据，包含 YARA 内存扫描等相关动作的数据。

版权所有：腾讯云计算（北京）有限责任公司

数据存储策略（11.1.1版）
存储目标管理（11.1.1版）

最近更新时间：2026-02-09 20:57:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

数据存储用于存储本地捕获的恶意文件，为后续的安全研究和防御策略制定提供可靠的依据。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **高级威胁防护（EDR）** > **策略规则** > **数据存储策略**。
2. 在数据存储策略页面，选择**存储目标管理**，单击**添加存储目标**。



配置腾讯云存储服务

> **说明：**
> 支持使用其他对象存储，请同样按下述步骤获取相关配置参数。

步骤1：新建存储桶

存储桶用于存储 iOA 审计日志中的敏感文件和取证截图。

> **说明：**
> 如您未开通腾讯云对象存储服务，请前往腾讯云开通 对象存储 COS 。

1. 登录 对象存储控制台，在左侧导航栏，选择**存储桶列表**。

2. 在存储桶列表页面，单击**创建存储桶**，新建一个存储桶。



3. 在创建存储桶窗口中，配置基本信息，单击**下一步**。



参数名称	说明
所属地域	选择所属地域，存储桶与相同地域的其他腾讯云服务内网互通，地域一旦选择，无法修改，请谨慎选择。
名称	填写存储桶名称，名称一旦创建，无法修改，请谨慎填写。

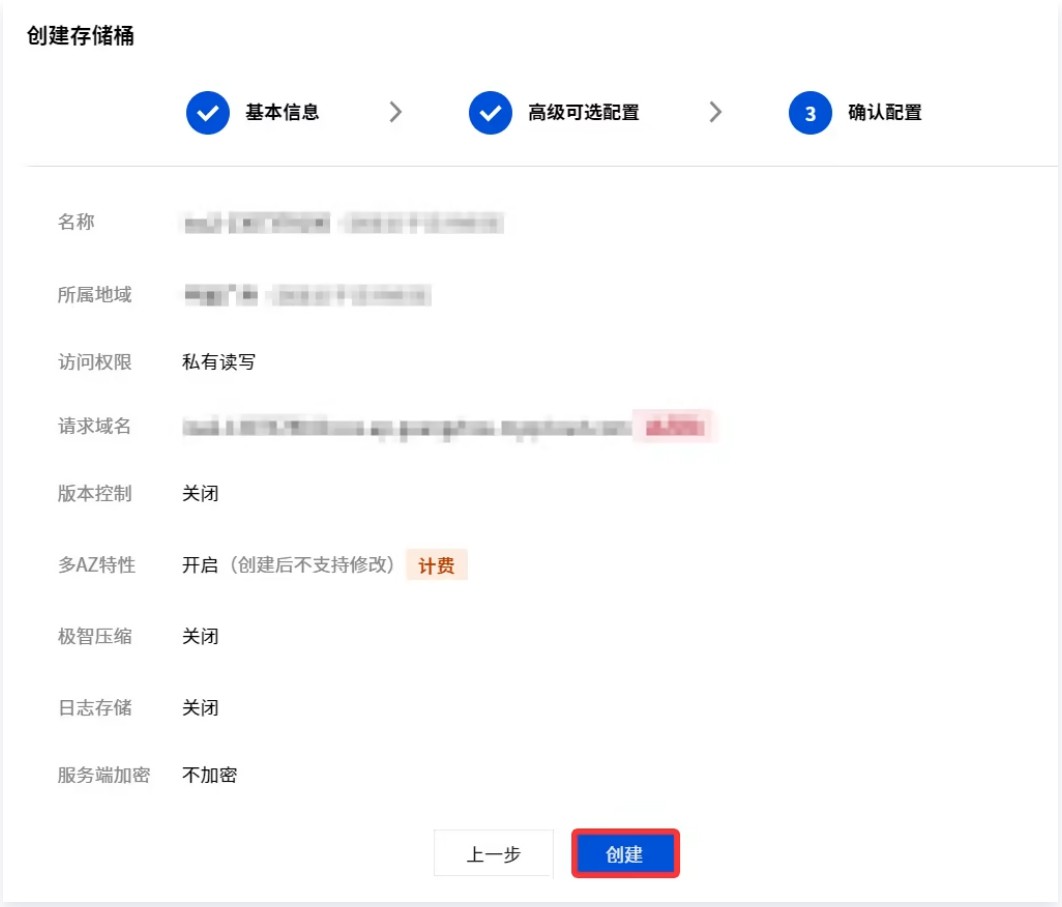
访问权限	可在私有读写、公有读私有写、公有读写3种访问权限中进行选择。**建议配置：私有读写权限。**
多 AZ 特性	• 部分地域支持多 AZ 特性，如不支持的地域，可通过设置存储桶跨区域复制功能。 • 多 AZ 特性允许用户将数据存储在同地理区域内的不同物理位置，提供同城容灾功能，推荐开启。

4. 在高级可选配置页签中，根据实际需求选择功能，单击**下一步**。



参数名称	说明
版本控制	可选择是否开启版本控制，开启版本控制后可以恢复因覆盖或误删丢失的数据。
极智压缩	极智压缩是在保证画质的前提下，尽可能地减小图片大小的功能。开启后，每次访问桶内的 JPG/PNG/GIF 格式的图片时将会实时压缩。
日志存储	可选择是否开启日志存储，开启后可记录跟存储桶操作相关的各种请求日志。
存储桶标签	支持输入标签键和标签值，可创建50个标签。
服务端加密	可选择不加密，或 SSE-COS 加密。

5. 配置信息确认无误后，单击**创建**，完成存储桶的创建。

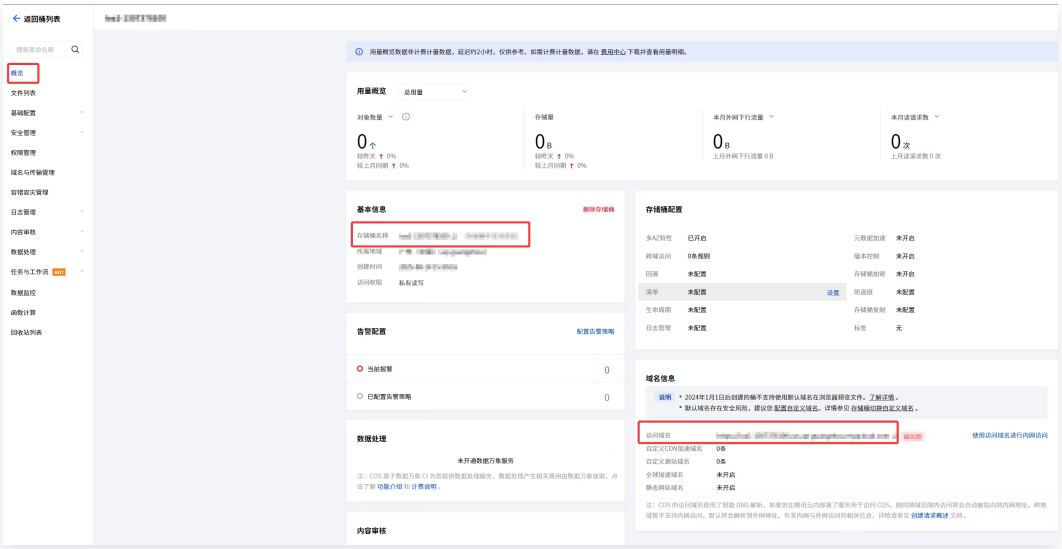


步骤2：获取 Bucket 和 Endpoint 参数

1. 完成存储桶的创建后，在 存储桶列表页面 ，单击**存储桶名称**，进入存储桶详情页面。



2. 单击**概览**，查看存储桶的概览页。找到**存储桶名称**和**访问域名**，分别作为 Bucket 和 Endpoint 参数。

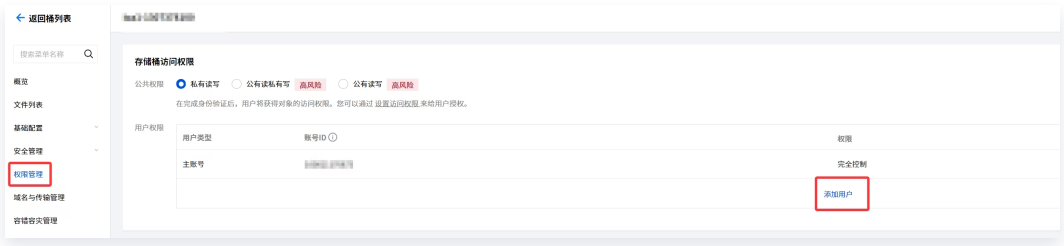


步骤3：为存储桶分配最小权限的子账号

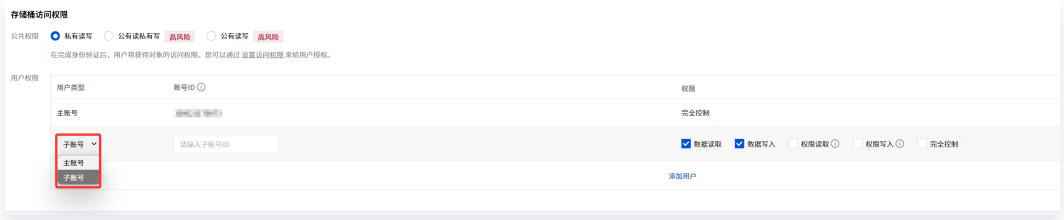
1. 完成存储桶创建后，在 存储桶列表页面 ，单击**存储桶名称**，进入存储桶详情页面。



2. 在存储桶详情页面，单击**权限管理 > 存储桶访问权限**。
3. 在存储桶访问权限页面，单击**添加用户**。



4. 添加用户时选择**子账号**，输入子账号 ID 并选择**数据读取**、**数据写入**两个权限，单击**确定**，即可为此存储桶分配一个具有读写权限（最小权限）的子账号。

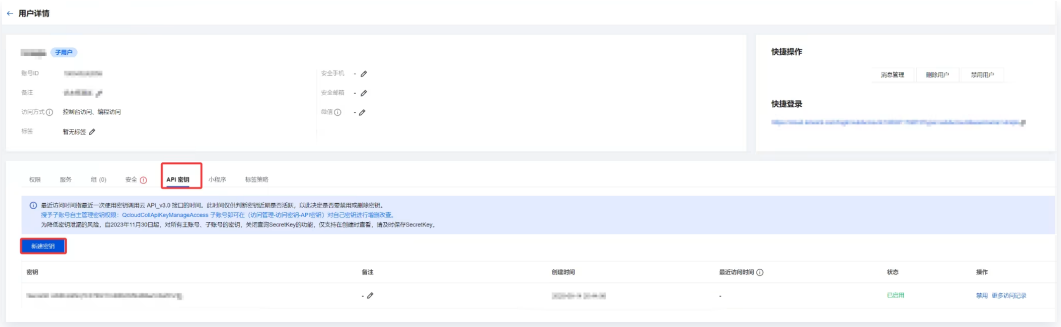


步骤4：获取子账号的 SecretId 和 SecretKey

1. 登录 访问管理控制台 ，在左侧导航栏，选择**用户 > 用户列表**。
2. 在用户列表页面，找到刚刚为存储桶分配的子账号，单击**用户名称**。

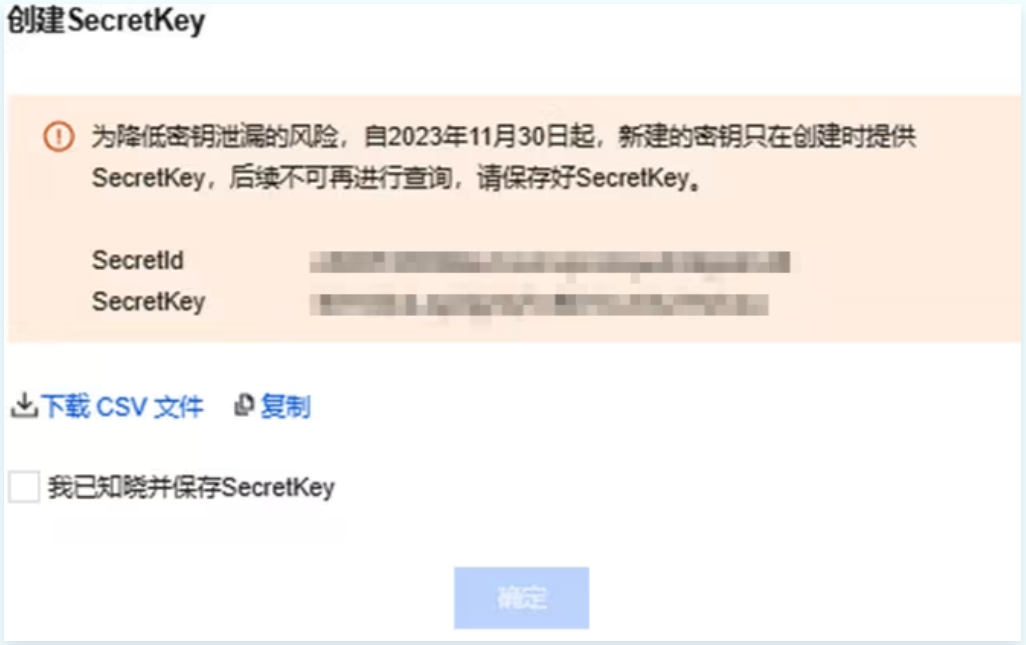


3. 在用户详情页面，单击 **API 密钥 > 新建密钥**，获取子账号的 SecretId 和 SecretKey。



注意：

为降低密钥泄露的风险，SecretKey 仅新建时提供，建议您保存好 SecretKey。



步骤5：回到 iOA 控制台，测试连通性

1. 完成各参数的获取后，返回 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 策略规则 > 数据存储策略**。
2. 在数据存储策略页面，选择**存储目标管理**，单击**添加存储目标**。



3. 存储目标选择**腾讯云**，依次填写上述获取的 **SecretId** 和 **SecretKey**、**Endpoint**、**Bucket**。填写完成后，单击**测试连通性**，若提示**测试成功**，即配置完成。



参数名称	说明
目标名称	腾讯云。
SecretId	步骤4 获取的子账号 SecretId。
SecretKey	步骤4 获取的子账号 SecretKey。
Endpoint	步骤2 获取的存储桶访问域名。
Bucket	步骤2 获取的存储桶名称。

4. 开启存储空间自动清理：该方式会自动清除符合条件的数据内容，如下图示例配置：存储容量超过100GB或存储时间超过100天，则自动清理。

> ⚠ **注意：**

- 仅配置**保存数据空间上限**时，存储数据到达上限采用滚动清理方式，即按照时间顺序，从最早的文件开始删除。
- 自动清理后，将无法查看最早的采集日志，请谨慎选择。



5. 配置完成后单击**确定**保存。

配置 S3 协议存储服务

iOA 支持配置 S3协议的存储服务。

> **说明**
> 请事先分配一个具备当前 Bucket 读写权限的最小权限子账号。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **高级威胁防护（EDR）** > **策略规则** > **数据存储策略**。
2. 在数据存储策略页面，选择**存储目标管理**，单击**添加存储目标**。
3. 存储目标选择 **S3协议**，依次填写 **AccessKeyId** 和 **SecretAccessKey**、**Endpoint**、**Bucket**，单击**测试连通性**，若提示**测试成功**，即配置完成。



参数名称	说明
目标名称	S3协议。
AccessKeyId	唯一标识符，用于识别访问云存储服务的用户或应用程序。它通常与 SecretAccessKey 配合使用，以便在对云存储服务进行身份验证时提供安全访问。
SecretAccessKey	与 AccessKeyId 配对的私钥，用于对云存储服务进行身份验证。当创建一个新的 AccessKeyId 时，系统会自动生成一个与之关联的 SecretAccessKey。
Endpoint	云存储服务的 API 访问点。它是一个 URL，用于指向服务的特定区域和访问路径。客户端通过这个 URL与云存储服务进行通信。
Bucket	Bucket 名称。Bucket 是云存储服务中的一个基本容器，用于存储和组织数据。

4. 开启存储空间自动清理：该方式会自动清除符合条件的数据内容，如下图示例配置：存储容量超过100GB或存储时间超过100天，则自动清理。

> **注意：**
> - 仅配置**保存数据空间上限**时，存储数据到达上限采用滚动清理方式，即按照时间顺序，从最早的文件开始删除。
> - 自动清理后，将无法查看本地存储的恶意文件，请谨慎选择。



5. 配置完成后单击**确定**保存。

存储目标策略（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **高级威胁防护（EDR）** > **策略规则** > **数据存储策略**。
2. 在数据存储设置页面，选择**存储目标策略**，单击**新建策略**。



3. 在存储目标策略页面，填写基本信息、适用范围和编辑策略。

3.1 基本信息：输入策略名称、策略描述，并选择是否启用。



3.2 适用范围：该策略生效的对象范围。单击**添加适用范围**，勾选需管控的用户/终端，单击**确定**。



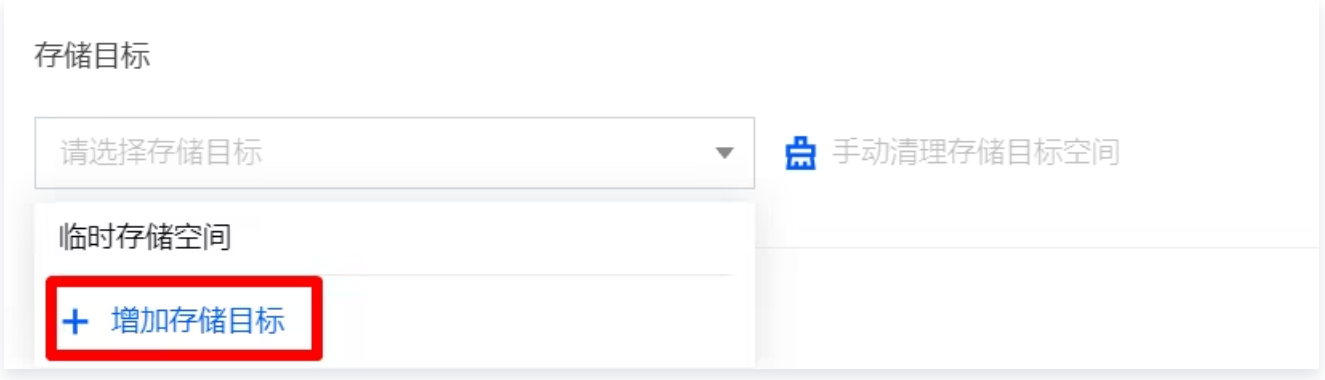
3.3 文件存储大小设置：当开启 文件存储大小限制后，超过限制的文件将不保存（默认100MB，上限10GB）。



3.4 上传速度限制：用于控制文件上传时的速度，避免占用过多网络带宽，影响其他网络活动。可根据网络状况和需求，自定义上传速度的上限。



3.5 存储目标：下拉选择存储目标，存储目标配置方式详情请参见 增加存储目标 。



3.6 限定位置或出口 IP。

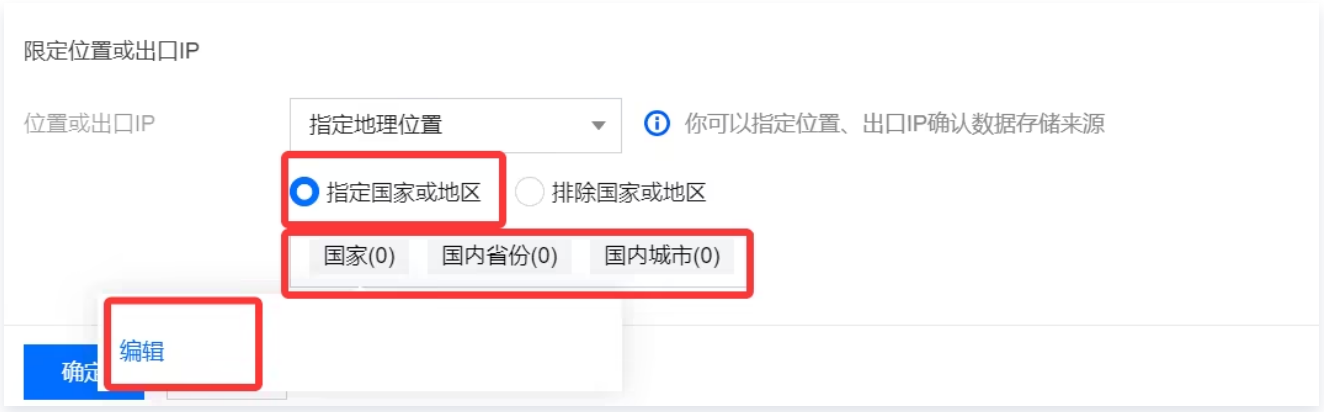
- 不指定地理位置或出口 IP：选择不指定地理位置或出口 IP，则不指定用户接入的地理位置/出口 IP。



- 指定出口 IP：存储支持按照 IP 段方式选择地区。



- 指定地理位置：指定国家或地区时，选择指定国家或地区，单击**编辑**，勾选国家/国内省份/国内城市后单击**确定**。



- 排除国家或地区：选择排除国家或地区后，单击**编辑**，勾选国家/国内省份/国内城市后单击**确定**，则排除当前选择的国家或地区。



4. 填写完成后，单击**确定**保存存储目标策略。

威胁事件（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

数据统计&筛选

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 威胁事件**。
2. 在威胁事件统计页面，支持查看威胁事件发生趋势，同时会按照钓鱼、勒索、横向移动进行场景化数据统计。
   ①支持时间段选择：今天、近7天、近30天以及自由选择时间查询。
   ②单击**事件数据信息**，可按统计数据筛选。



③单击**导出**，导出日志信息。



3. 事件聚合区分精准模式以及ATT&CK模式，选择精准模式即可将含有恶意文件和威胁情报的事件一键过滤展示，突出重要事件，降低运营压力。



4. 事件聚合时间支持自定义，默认1天，可通过缩短聚合时间查看最近关联的告警。



批量处理调查状态

- 某个事件调整：单击调查状态 ，可以调整事件调查状态为**新事件、调查中、已完成**。



- 批量调整：支持勾选多个威胁事件，单击**批量处理调查状态**，选择将事件状态调整为**新事件**、**调查中**、**已完成**。

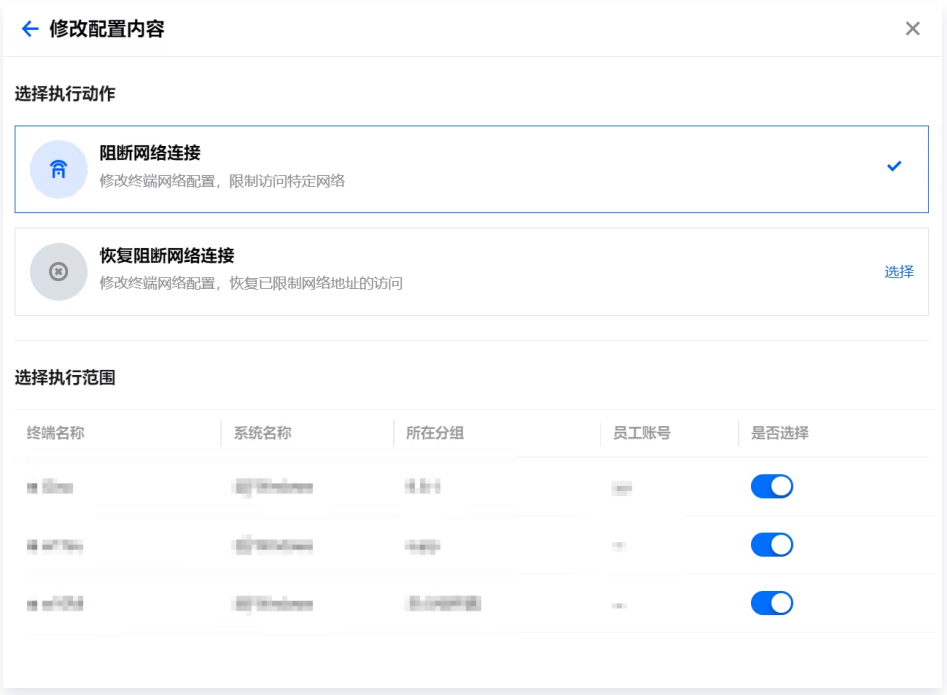


事件关联告警和处置

1. 单击事件名称右侧的 > 以展开威胁事件并展示该事件关联的告警。单击威胁事件的**处置**，可查看该事件下所有可处置的证据。



2. 在处置页面，单击**配置**，支持调整需要处置的证据/终端。
   - 配置：可以对该证据下发阻断网络连接等处置任务。选择阻断/恢复阻断，单击**确定**。



- 终端：支持针对该事件关联的终端进行处置，选择隔离终端/恢复终端隔离，单击**确定**。



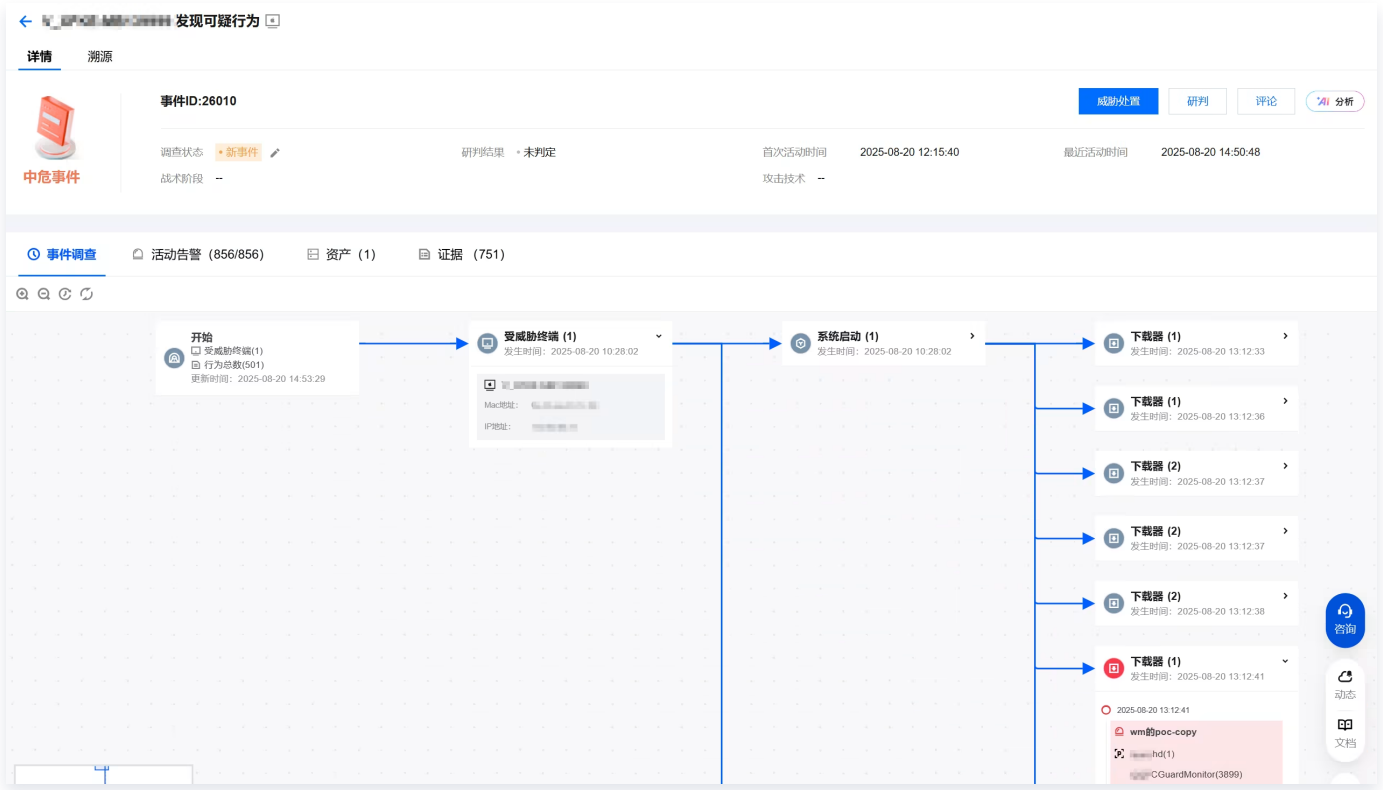
威胁事件调查

在事件调查页面，用户可以看到整个威胁事件中证据、告警与终端的关联关系，通过溯源图可以梳理整个威胁事件的发生流程，进而对该事件进行研判以及处置。

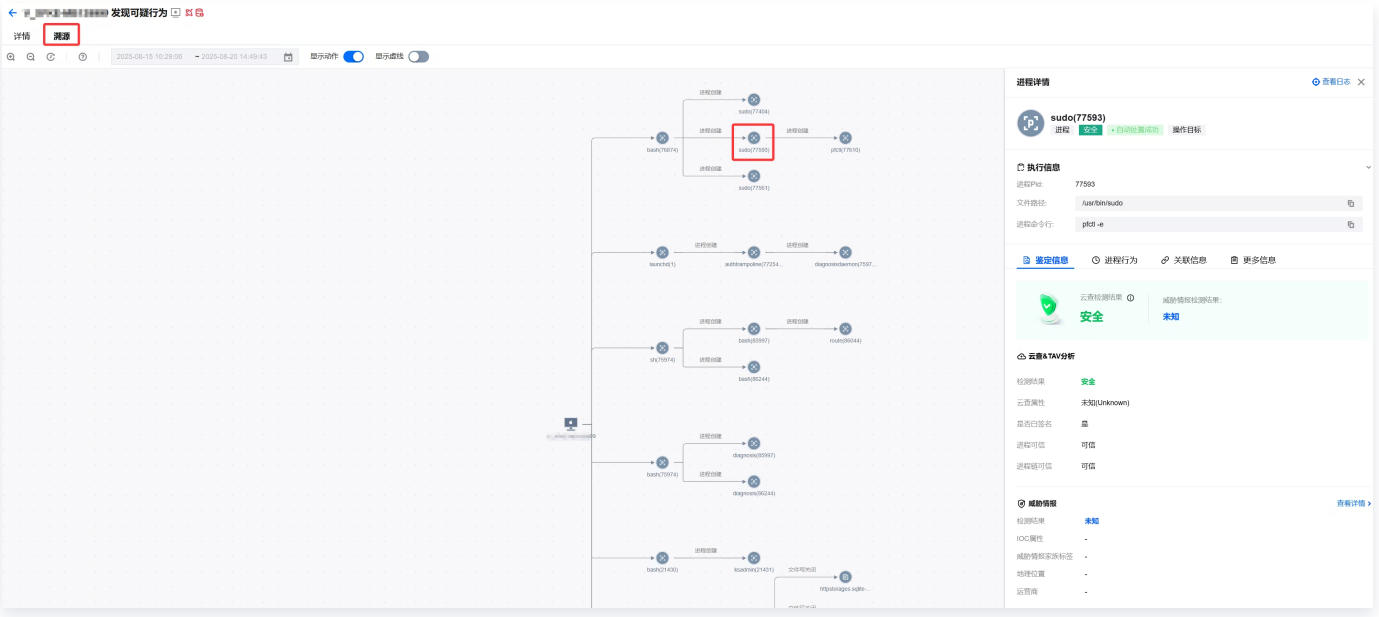
1. 在威胁事件列表中，单击**调查**或**事件名称**，进入事件调查页面。



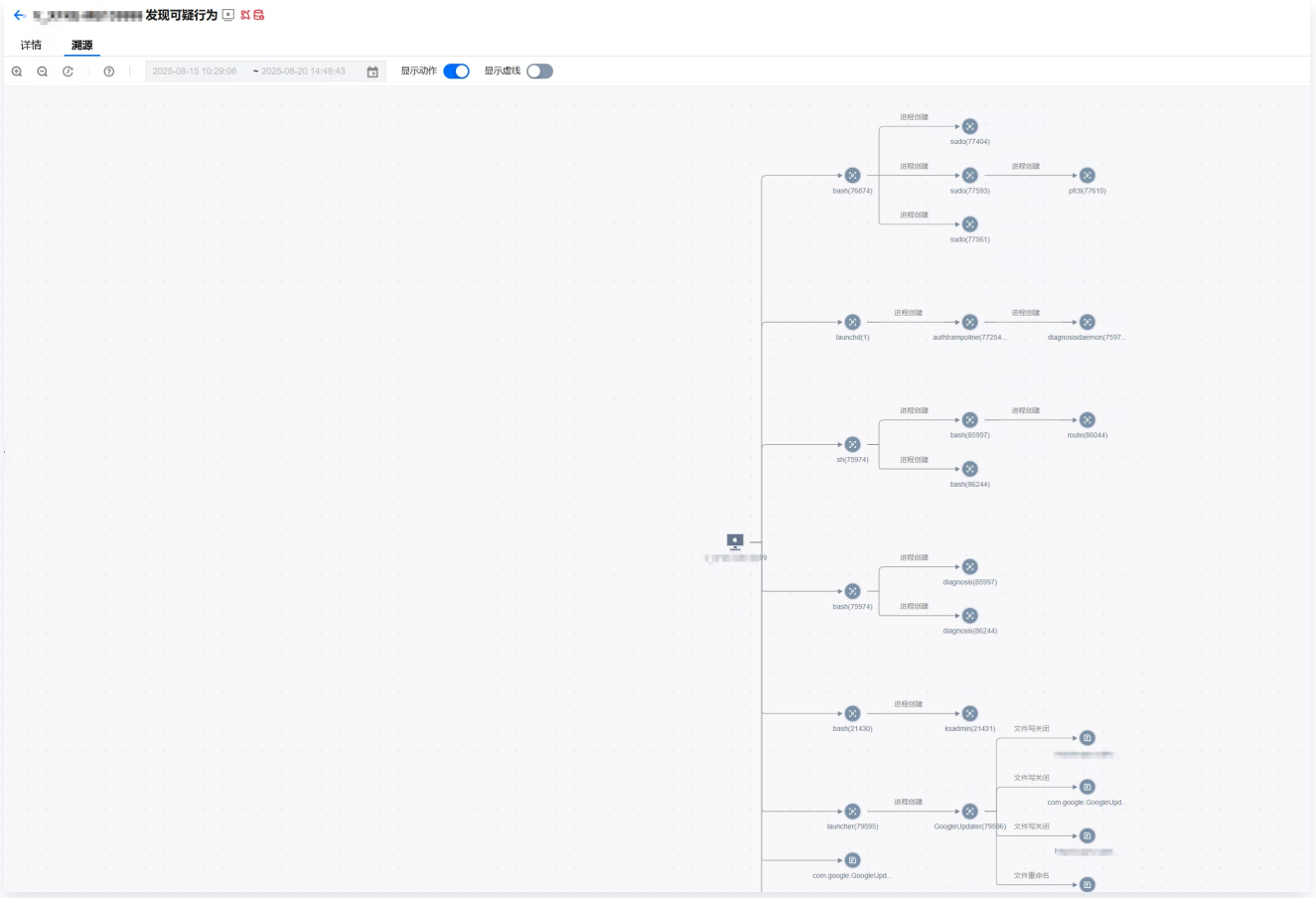
2. 在事件调查页面，单击**详情**查看复现攻击者行为链路。



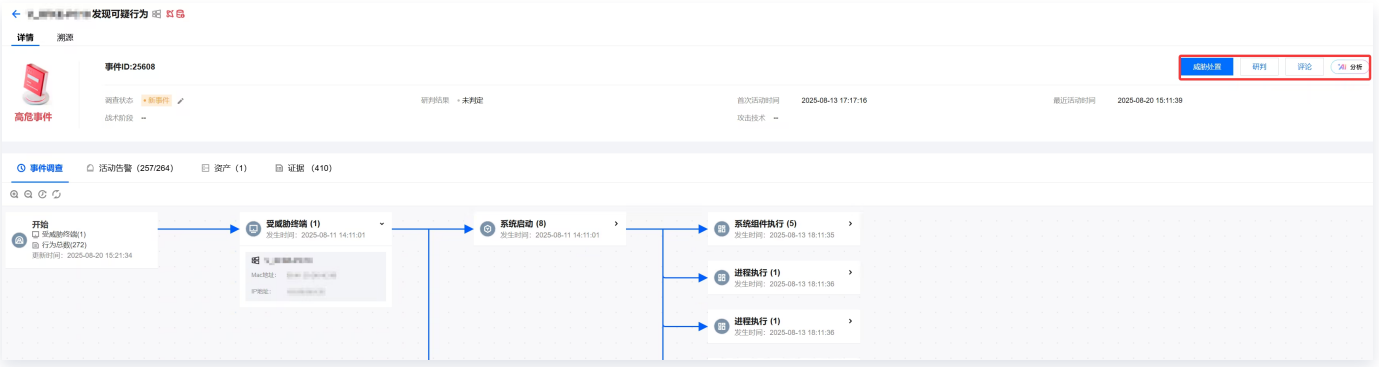
3. 在溯源图中单击**实体**，左侧展示该实体的具体信息，包含鉴定信息、进程行为、关联信息（关联告警、资产）。



3.1 单击**溯源**查看溯源图，在溯源图中可以明确知悉恶意文件/进程创建的过程，进而帮助用户更好地确认威胁事件发生的关键，并针对性解决问题，溯源图中的每一个节点都可以单击展示该节点的详细信息，查看恶意文件/进程创建的过程。



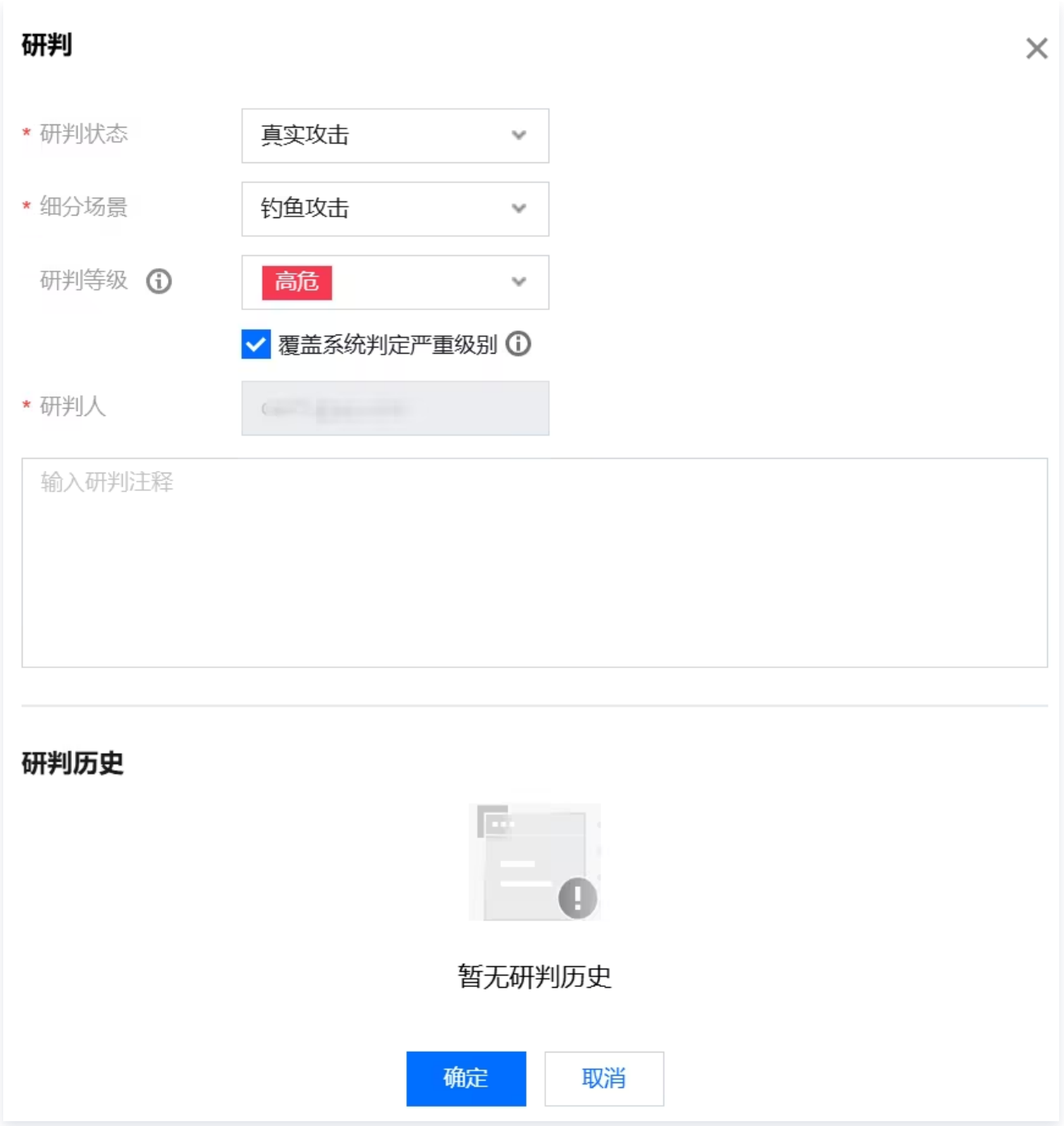
4. 支持对该事件进行威胁处置，研判、评论、以及 AI 分析威胁事件。



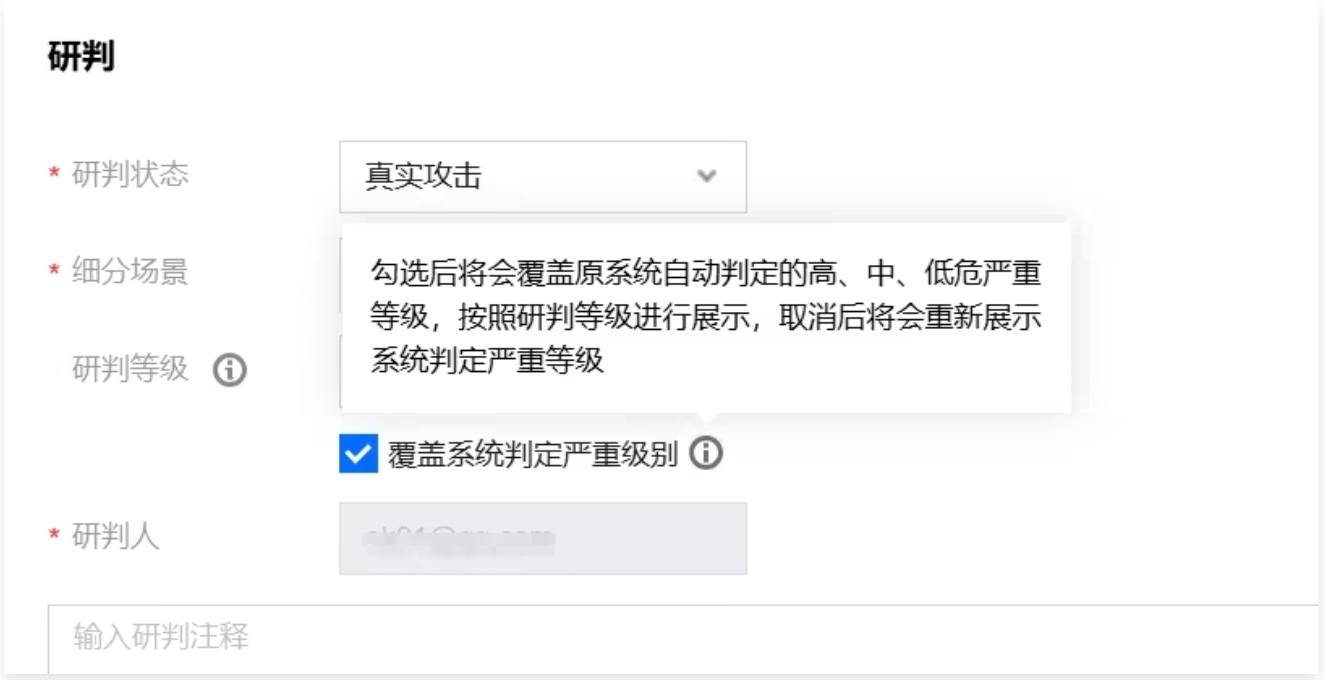
4.1 单击**威胁处置**，选择目标实体，单击**配置**，可隔离/恢复隔离终端。



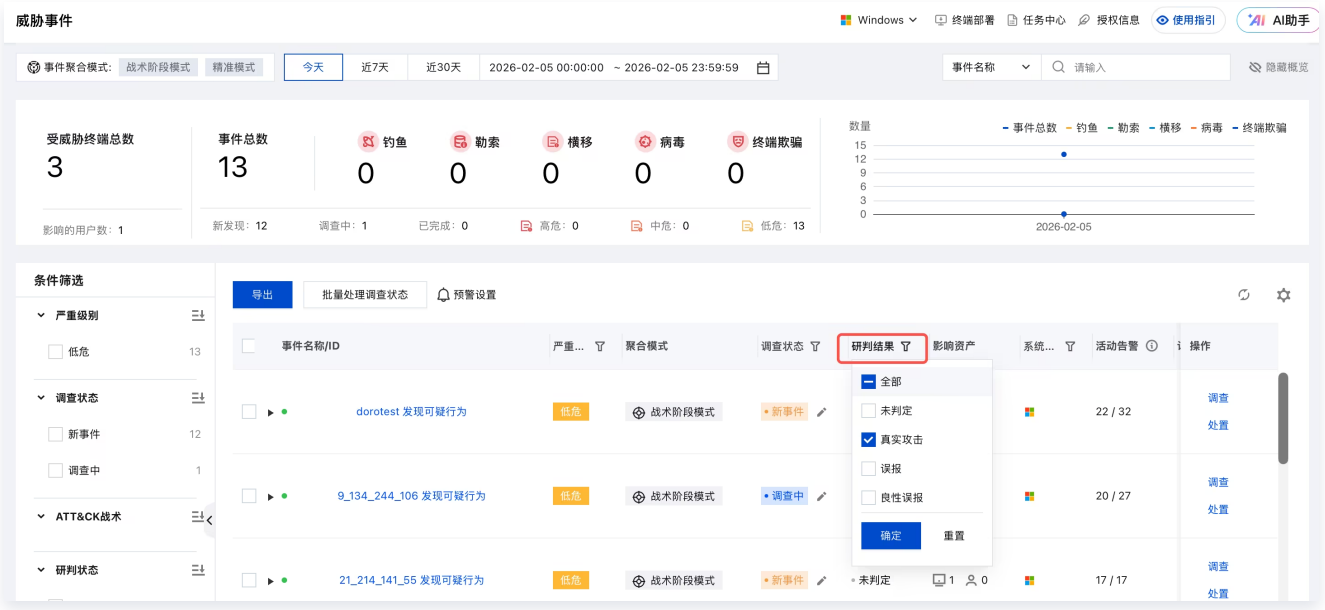
4.2 单击**研判**，支持手动标注（研判）等级，支持对事件的严重等级进行手动标注为高、中、低危风险。



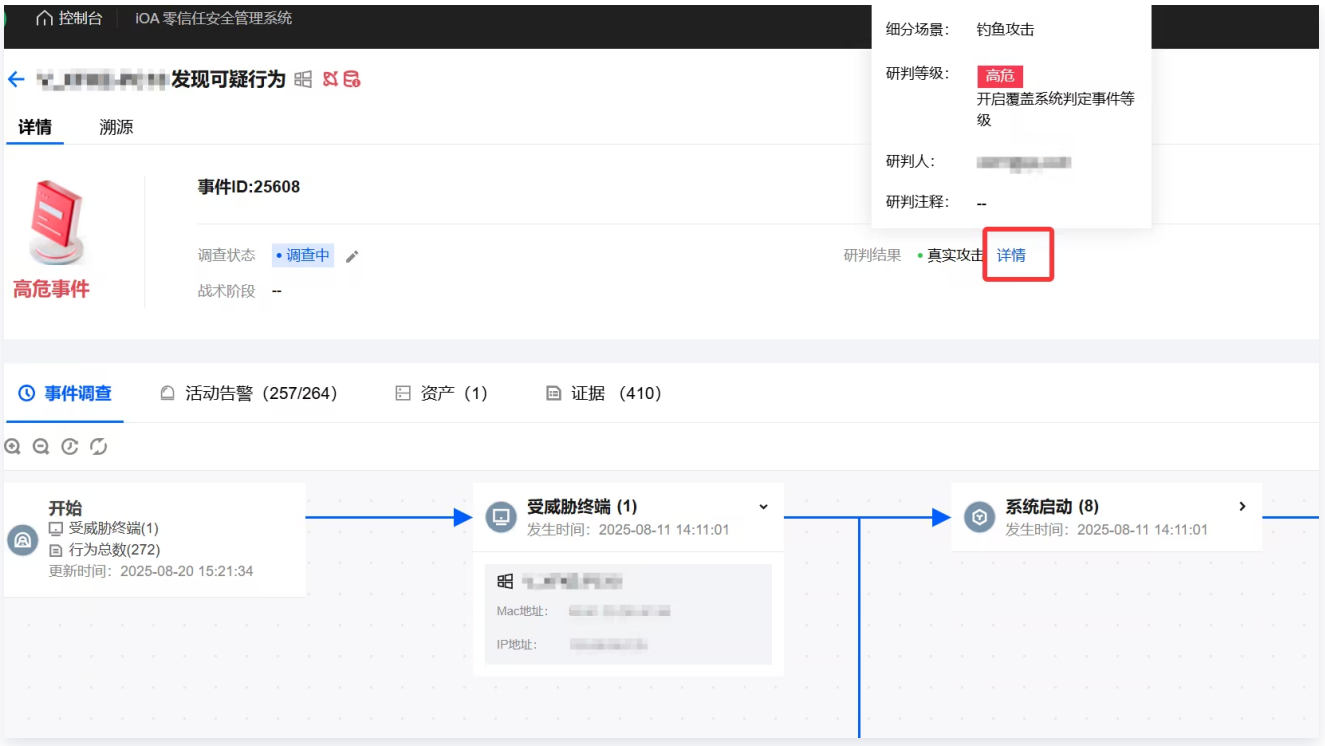
4.3 支持将手动研判的等级覆盖系统判定的严重等级，进而在威胁事件页可直观看到风险数统计。



4.4 若配置为覆盖系统判定严重级别后，在威胁事件页，将按照新的研判等级进行展示。



4.5 威胁事件研判结果新增详情，经过人工研判的事件可查看历史研判详情。



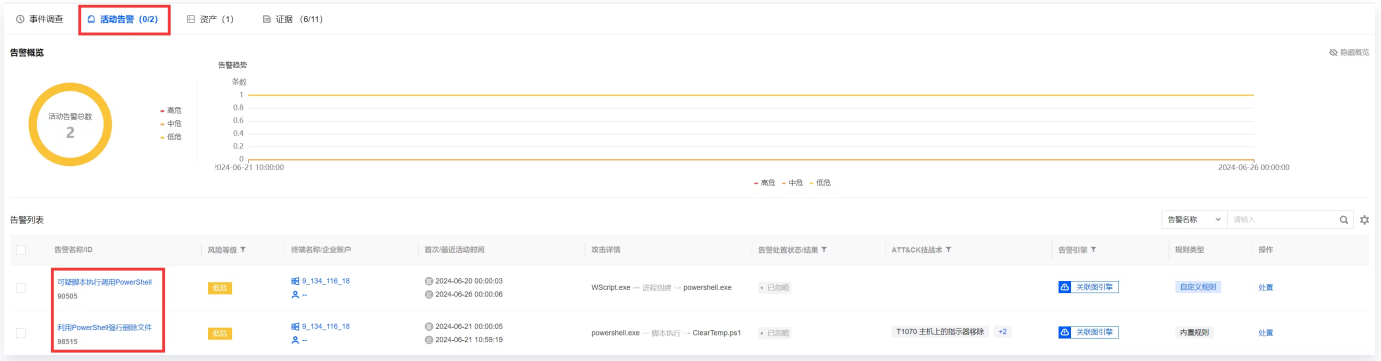
4.6 评论：对该事件添加评论。



4.7 AI分析：AI智能分析该威胁事件。



5. 切换页面到活动告警，支持查看该事件下所有的告警信息，单击具体的**告警名称/ID**可以查看告警详情。



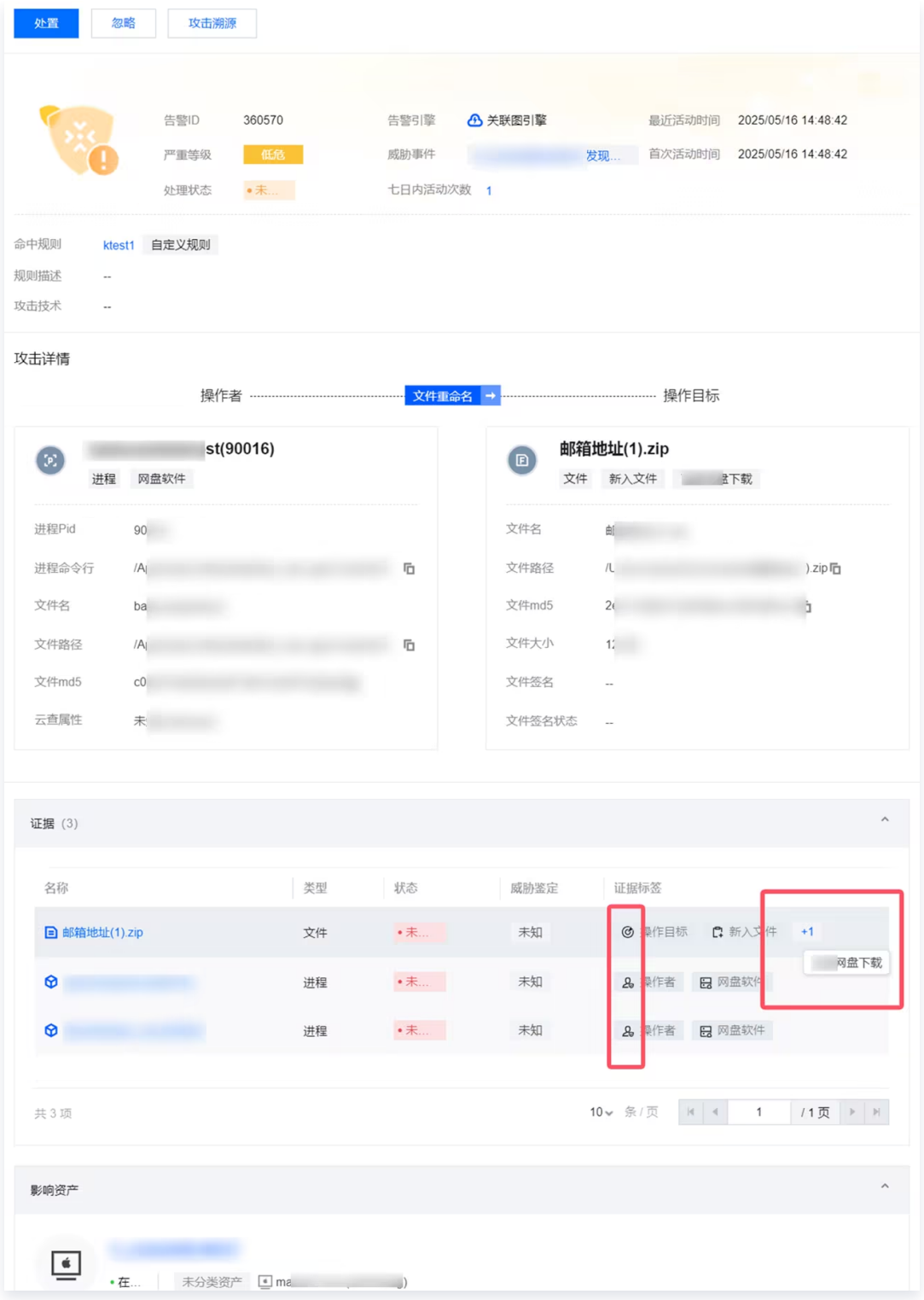
6. 切换页面到资产，可以看到对应产生告警的终端，单击**展开**可以看到该终端下所有的告警信息，单击**终端名称**可看到对应的终端信息。



7. 切换页面到证据，可以看到当前威胁事件下所有的证据信息，按照全部、进程、文件、网络进行分类，单击**名称**可以看到该证据详情以及关联的资产和告警。



8. 证据列表根据文件标签进行分类呈现，仅展示有标签的证据，减少非关键性证据。


处置
忽略
攻击溯源
告警ID 360570
告警引擎 关联图引擎
最近活动时间 2025/05/16 14:48:42
严重等级 低危
威胁事件 发现...
首次活动时间 2025/05/16 14:48:42
处理状态 未...
七日内活动次数 1
命中规则 ktest1 自定义规则
规则描述 --
攻击技术 --
攻击详情
操作者
文件重命名
操作目标
st(90016)
进程 网盘软件
进程Pid 90
进程命令行 /A
文件名 ba
文件路径 /A
文件md5 c0
云查属性 未
邮箱地址(1).zip
文件 新入文件
文件名
文件路径).zip
文件md5
文件大小
文件签名 --
文件签名状态 --
证据 (3)
名称 类型 状态 威胁鉴定 证据标签
邮箱地址(1).zip 文件 未... 未知 操作目标 新入文件 +1
网盘下载
进程 未... 未知 操作者 网盘软件
进程 未... 未知 操作者 网盘软件
共 3 项
10 条 / 页
1 / 1 页
影响资产
在...
未分类资产

威胁告警（11.1.1版）

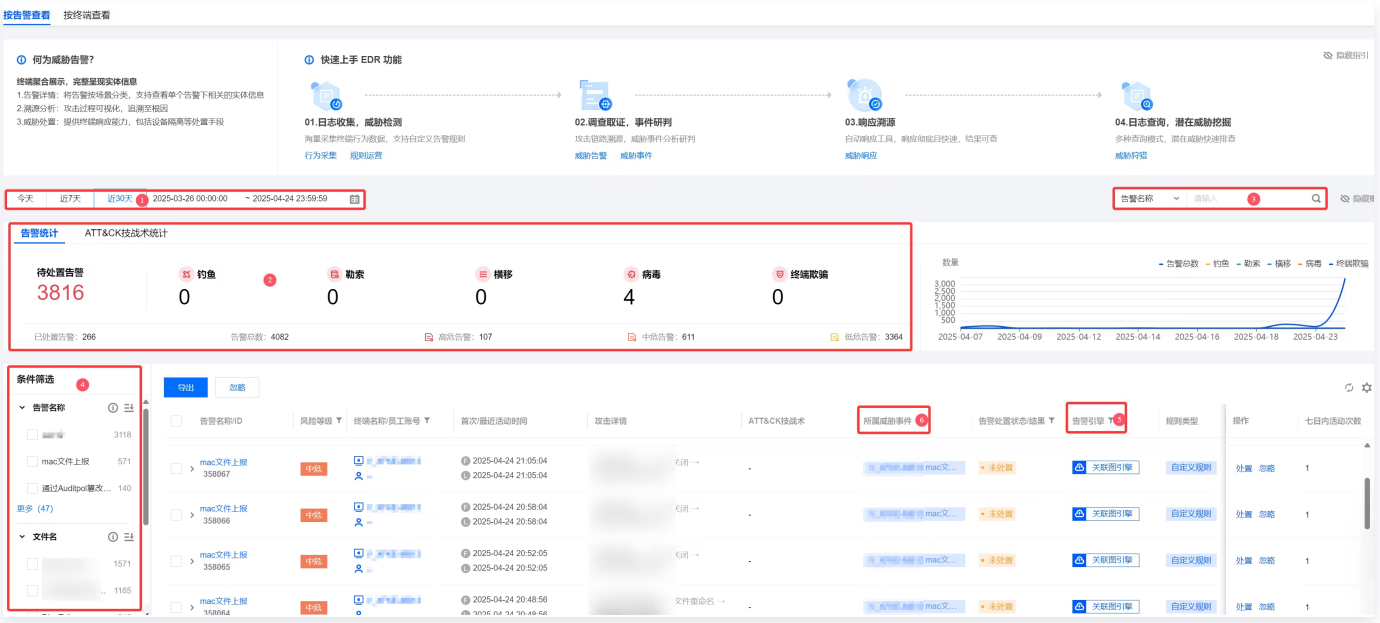
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

统计和筛选数据

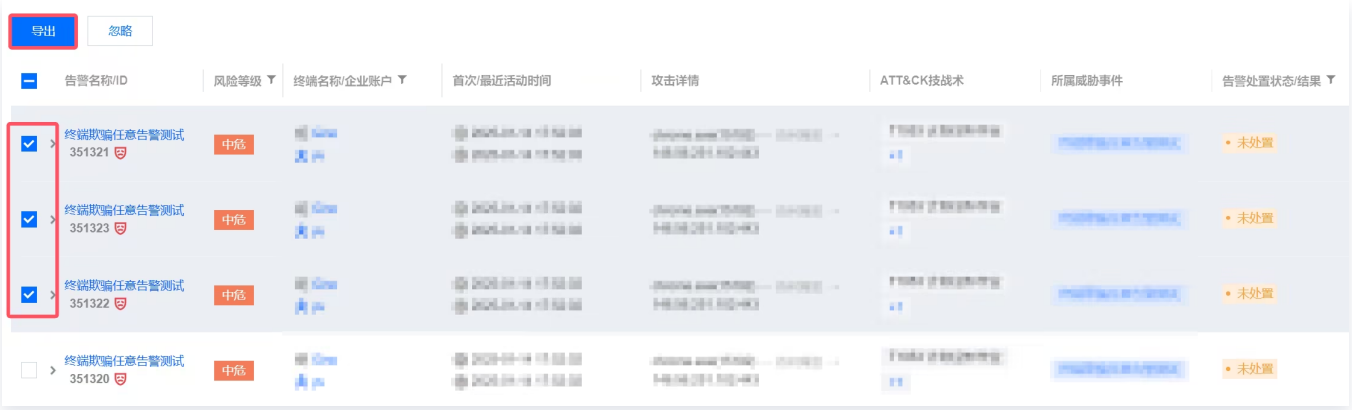
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 威胁告警**。
2. 在告警展示统计页面，支持根据告警维度以及 ATT&CK 技术战术维度统计相应的告警信息及其发生趋势图，同时会根据钓鱼、勒索、横移、病毒、终端欺骗进行场景化数据统计。

   ①时间筛选，近7天、10天、30天自定义。
   ②统计筛选，在统计页面，可以直接单击钓鱼告警、勒索告警、横移告警的统计数据对列表内容进行筛选。
   ③支持按告警名称、终端名称、企业账户、告警 ID、攻击详情快速搜索。
   ④条件筛选，展开左侧导航可按照告警名称、文件名、源 IP、目标 IP、风险等级、攻击场景等条件进行筛选。
   ⑤表内筛选，在列表内部，用户可在表头直接对目标内容进行检索。
   ⑥威胁事件命名逻辑，按照威胁情报 > 恶意文件 > 单一告警规则 > 战术阶段优先级来展示告警名称，突出核心要素，便于直接获取告警关键信息。



导出数据

1. 在威胁告警页面，勾选告警列表目标数据，单击**导出**。



2. 在导出页面，支持自定义表头，可选择目标导出的字段以及导出时间范围，导出格式默认为 CSV，单击**确定**。

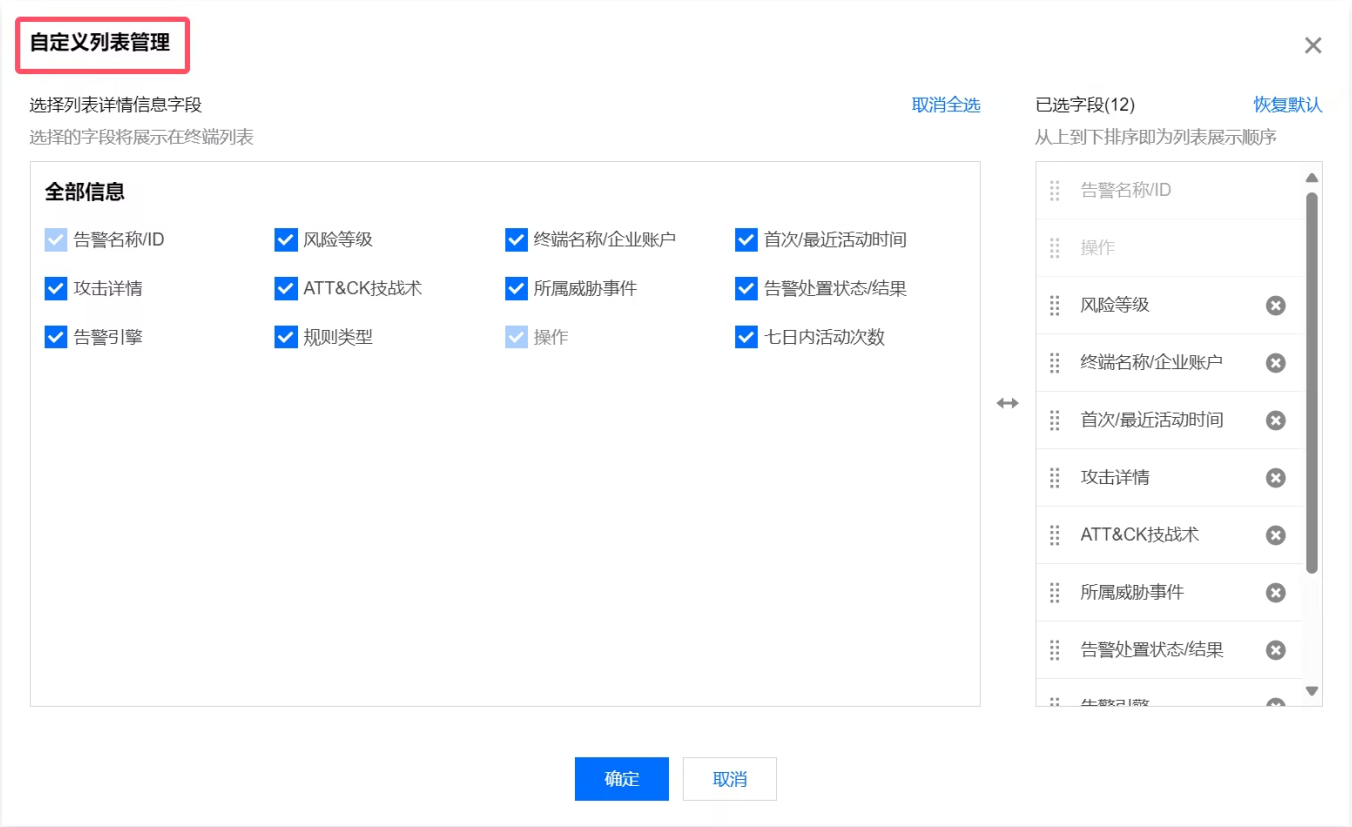


自定义列表管理

1. 在威胁告警列表中，单击右上角  。

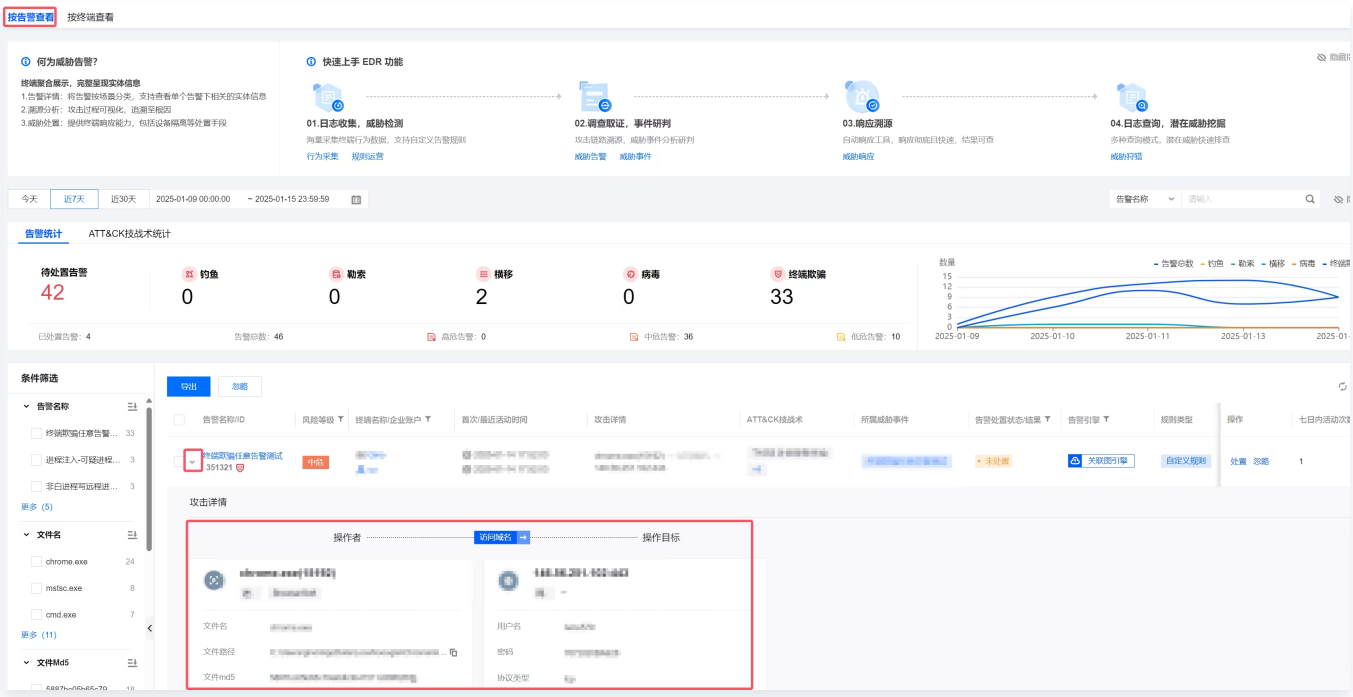


2. 展示当前表头所有字段，可根据需求自定义目标字段，确认后列表会刷新展示目标内容。

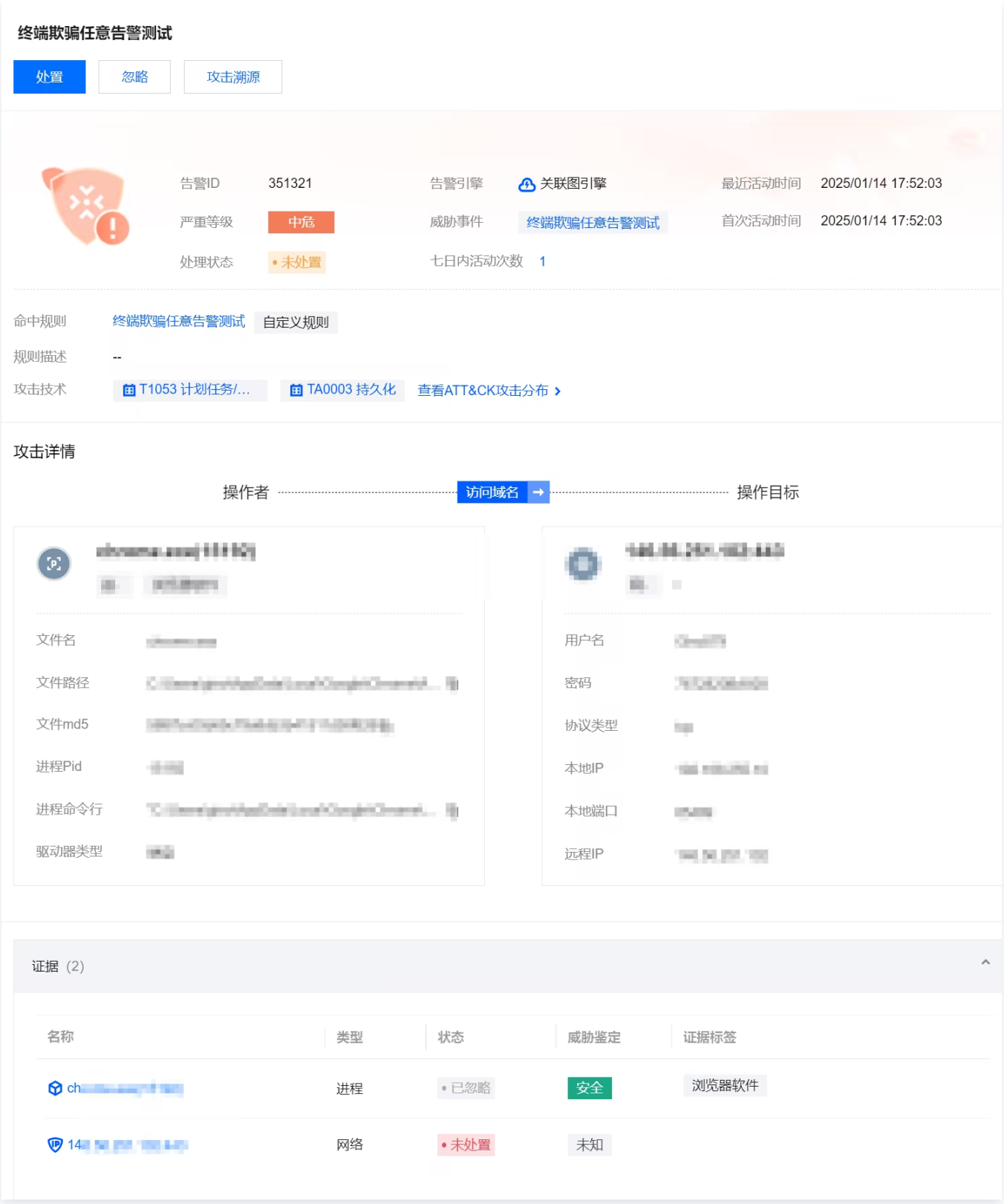


按告警查看

1. 在按告警查看页面，单击 > 展开具体的告警列表，可查看该告警的操作者以及操作目标，单击**对应文件、进程**，左侧弹出展示该实体的详情信息。



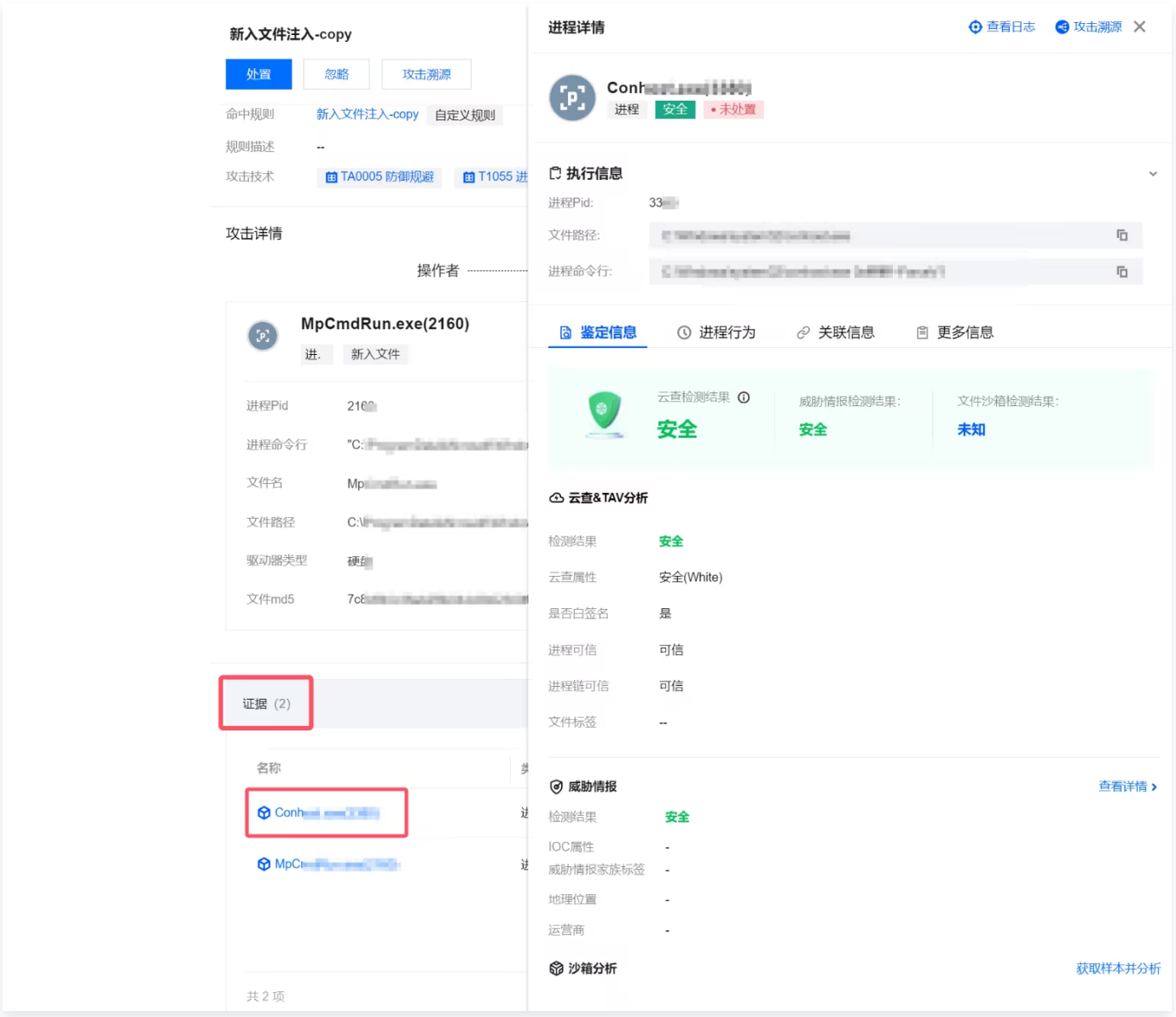
2. 单击**告警名称/ID**，将展示告警详情。这些详情信息包括告警基础信息、命中规则、攻击详情、证据列表以及相应的影响资产。



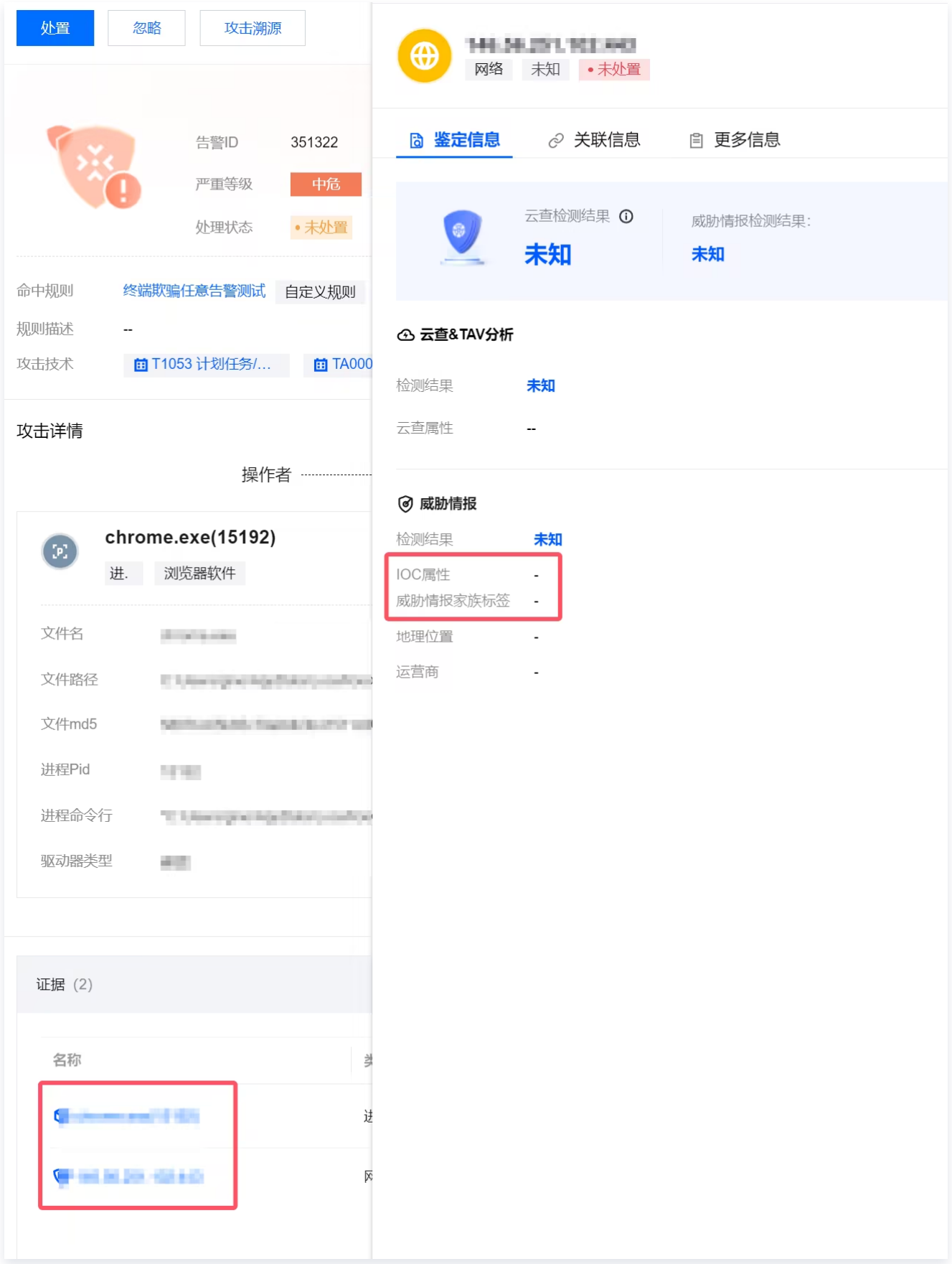
3. 在告警详情的证据列表中，单击**证据名称**。



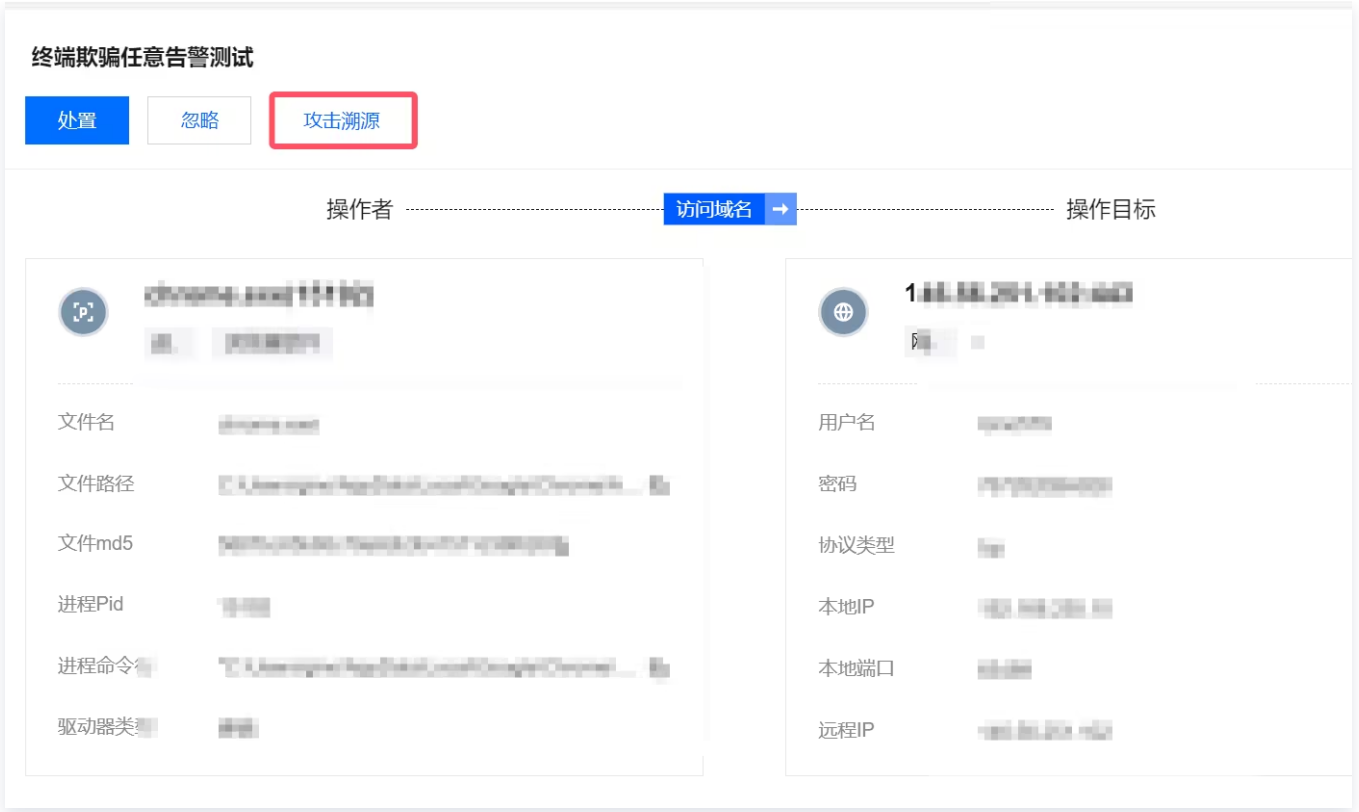
4. 展示该告警证据实体信息，包含进程、文件、网络等实体，其中每个实体除展示证据基本信息外，也会展示该证据关联告警信息以及影响资产。



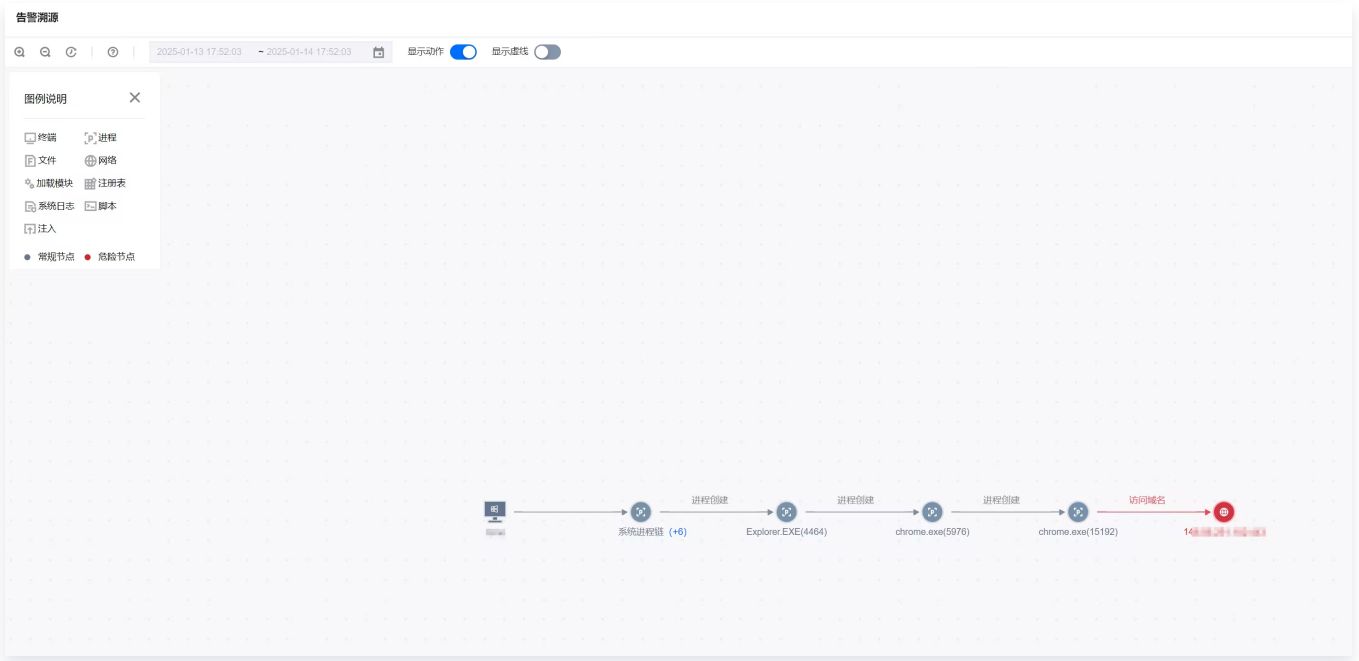
5. 新增文件、进程类威胁情报信息，网络实体新增威胁情报家族标签，并支持已分析过的节点在溯源图突出展示。



6. 攻击溯源：单击**攻击溯源**。



7. 可以查看引发该告警的进程/文件创建溯源图。

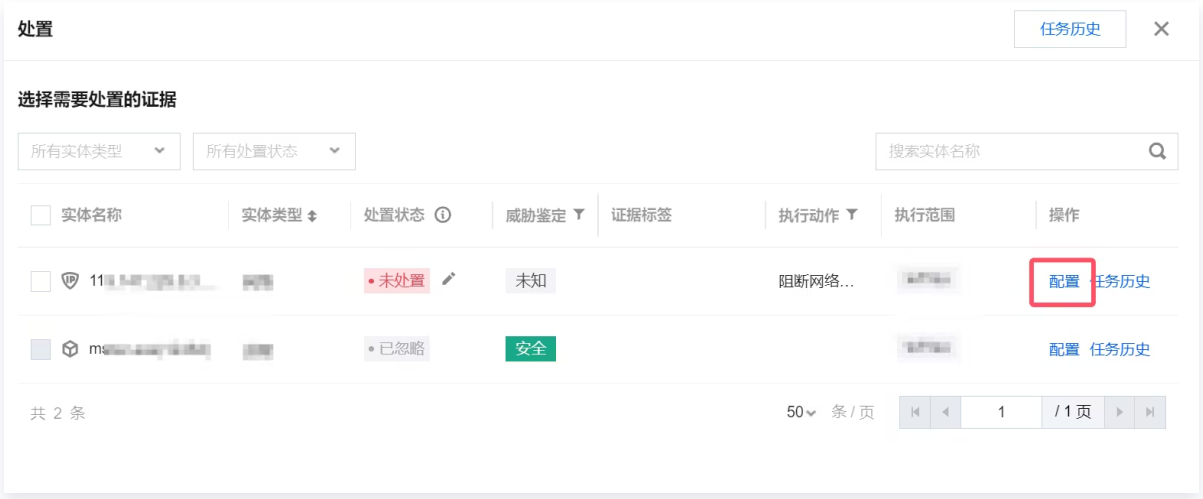


8. 告警处置。

- 单击**忽略**，可以直接忽略该告警。



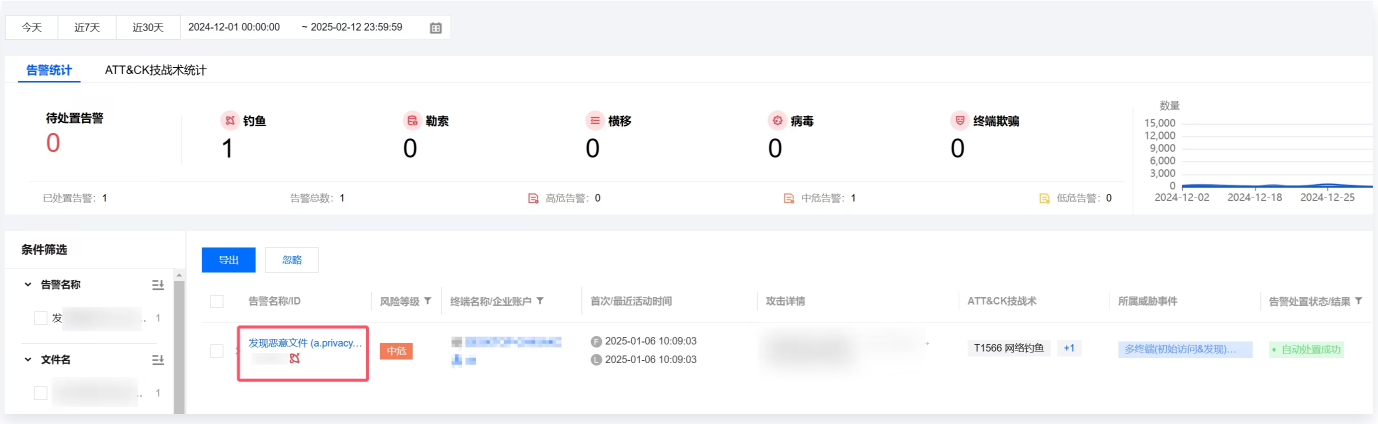
- 单击**处置**，可以处置该告警相关有威胁的实体，其中鉴定为安全的实体不可处置，鉴定为恶意和未知的实体可以下发阻断网络连接等任务。同时支持查看历史任务。



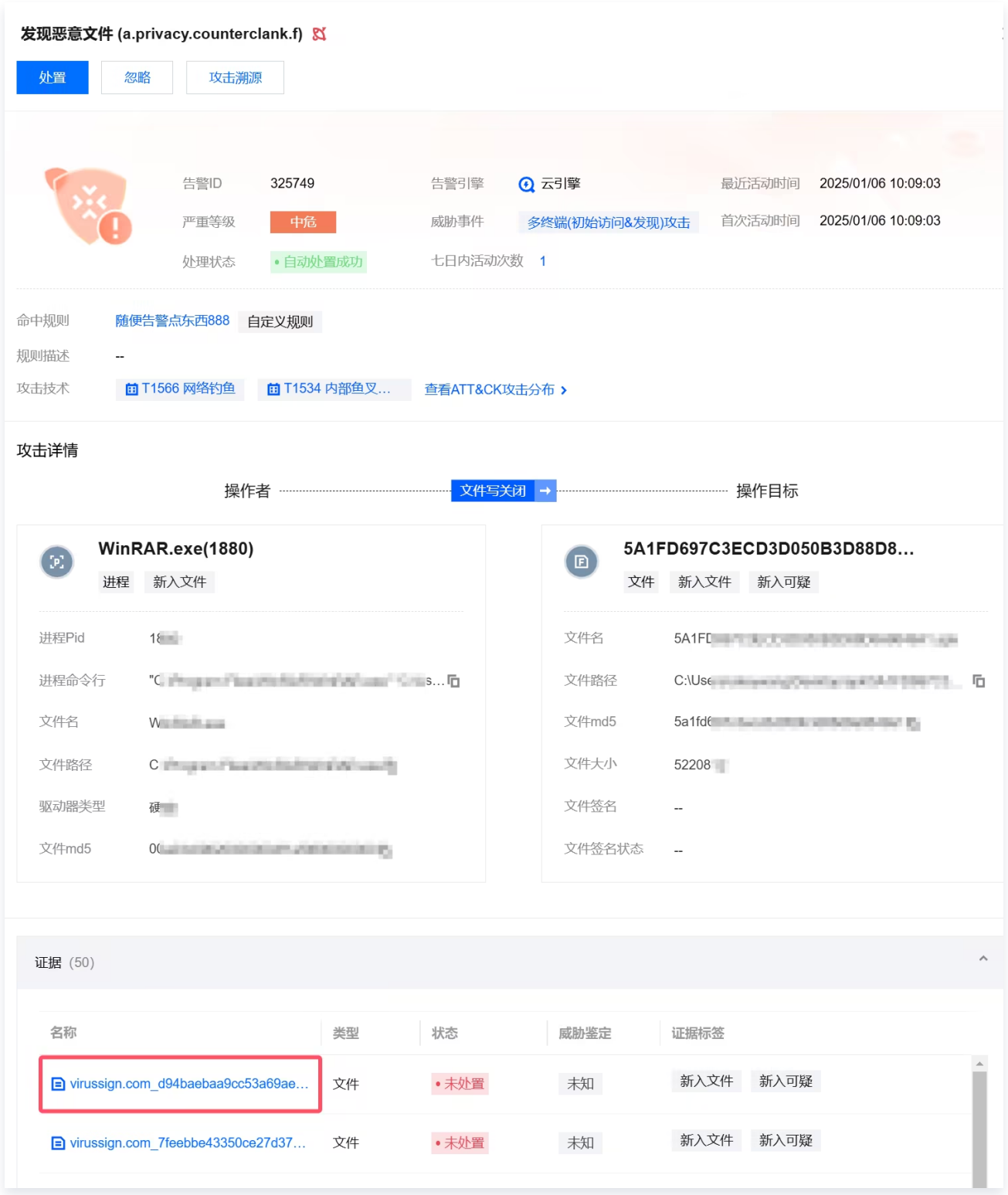
> **说明：**
> 威胁鉴定为安全的证据暂不支持处置。

告警实体联动云沙箱

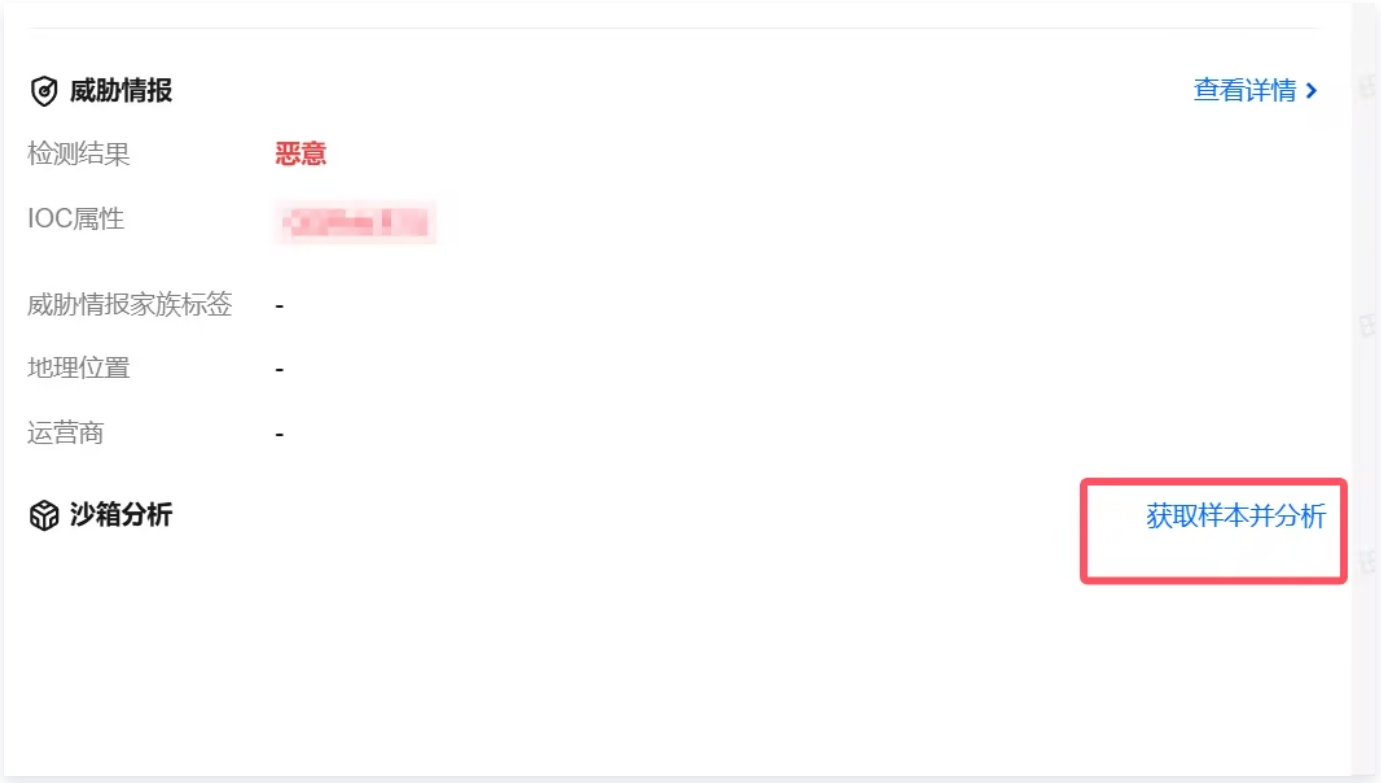
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 威胁告警**。
2. 在告警展示统计页面，单击**告警名称/ID**。



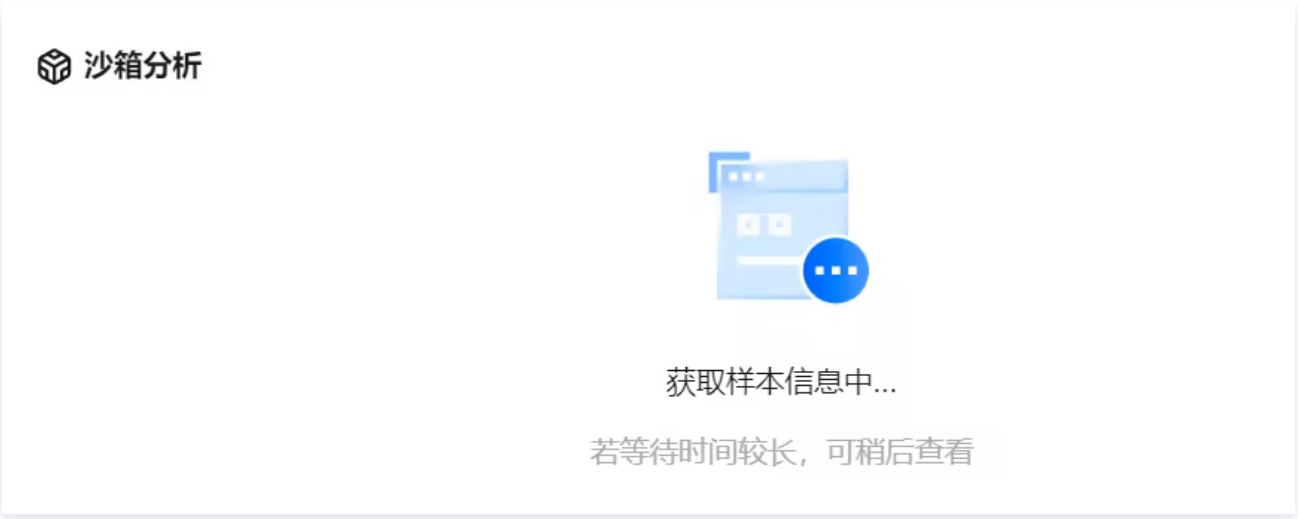
3. 针对文件、进程、网络类的实体信息中支持展示沙箱分析模块，单击**证据名称**。



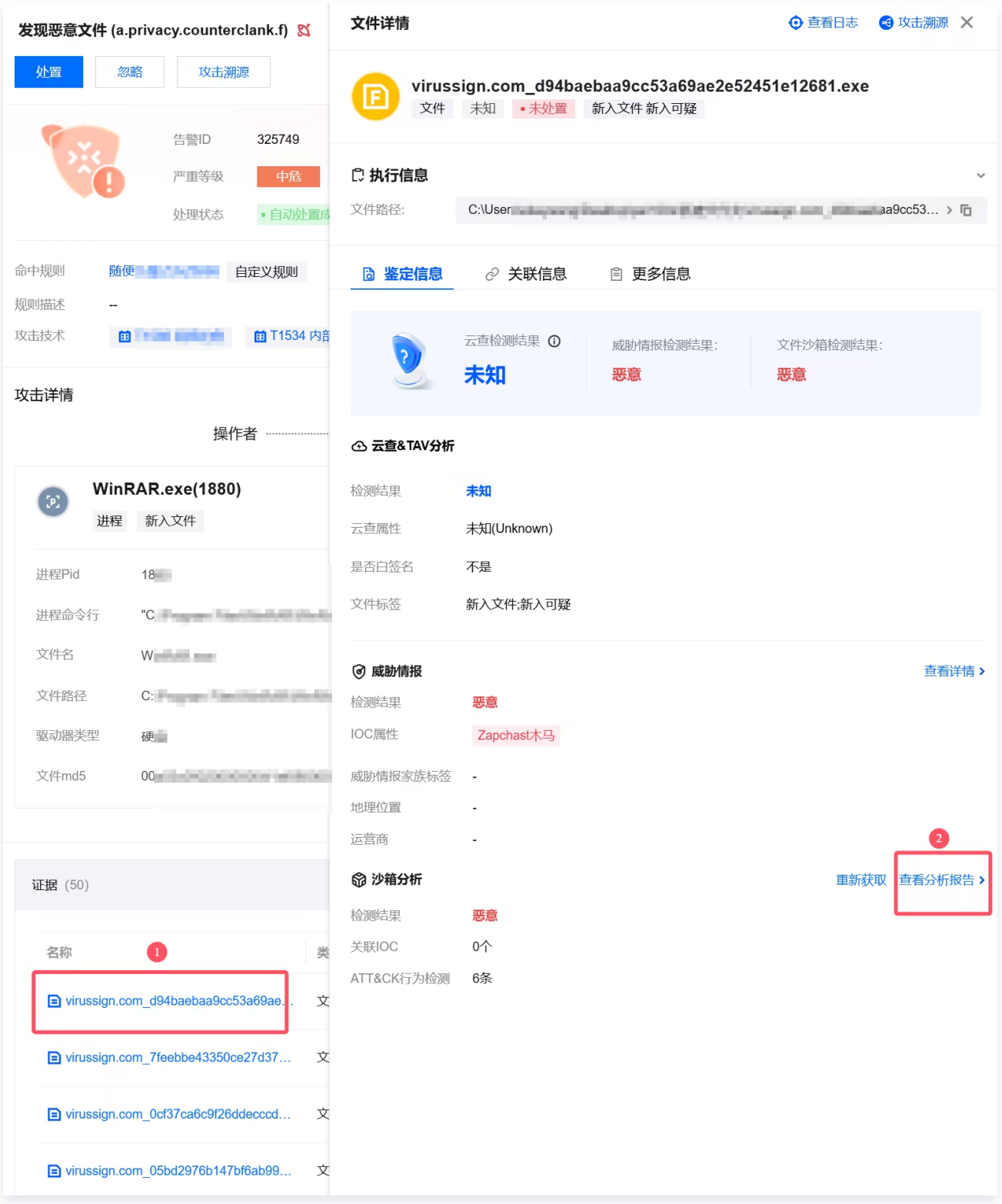
4. 对于未进入过沙箱分析的实体，需要用户手动单击**获取样本并分析**。



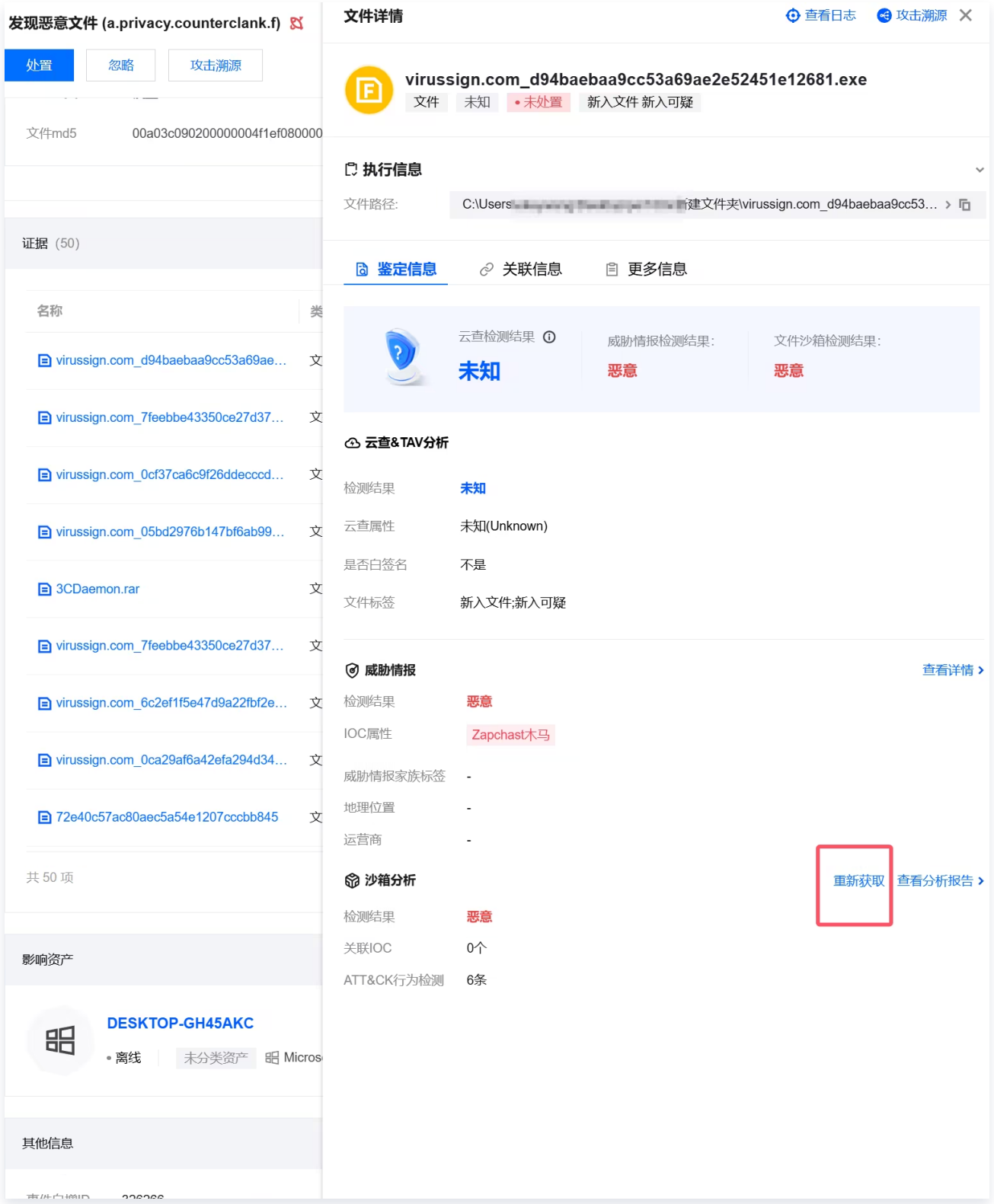
5. 对于初次分析的样本会存在分析时间较长的现象，用户可稍后查看。



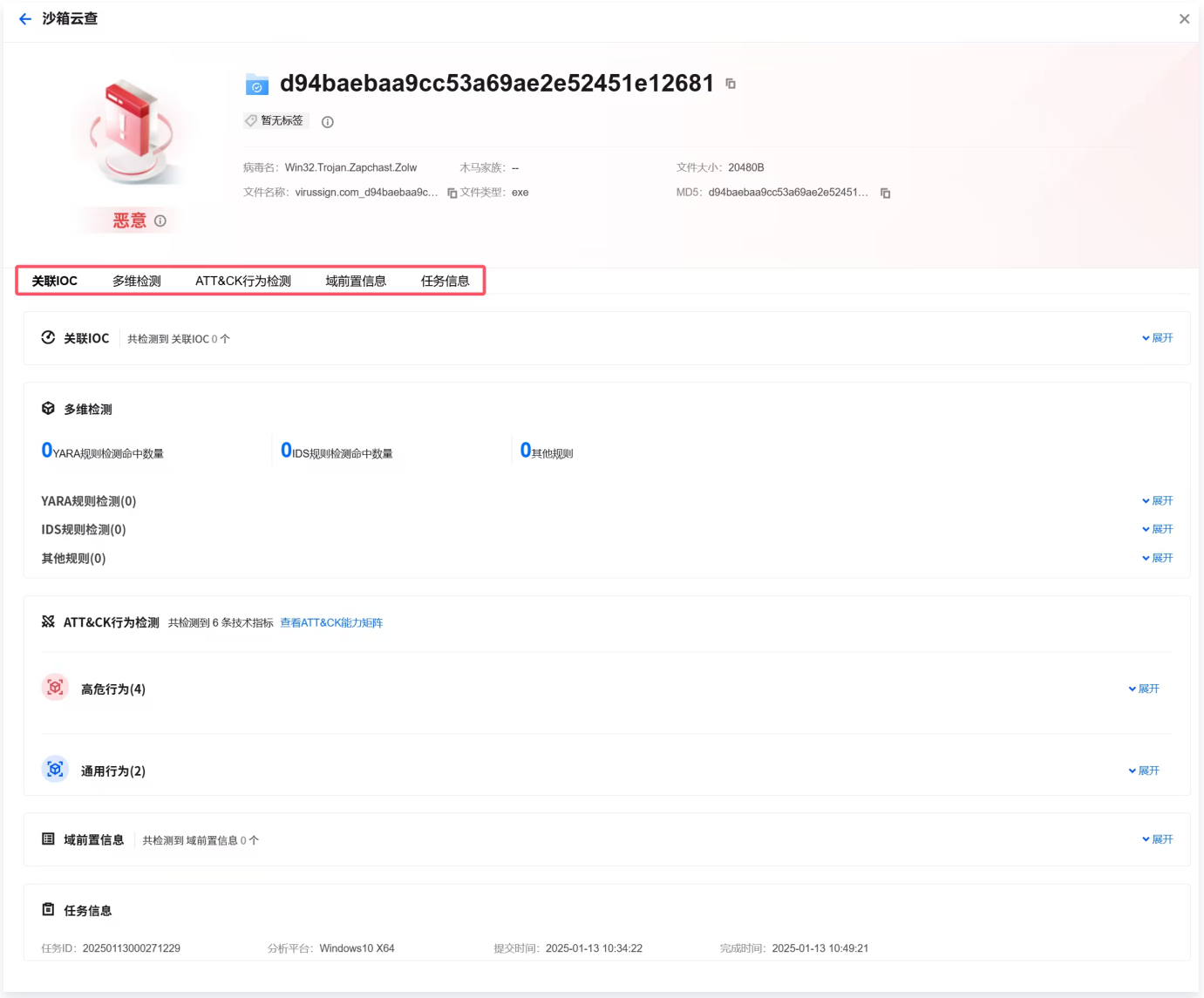
6. 对于已经进入过沙箱分析的实体，会直接展示包含检测结果、IOC 属性、处置建议等基础信息，如需获取更多信息，单击**查看分析报告**了解详情。



7. 由于病毒库的更新，扫描报告也会不断更新，支持用户单击**重新获取**以获取最新的沙箱分析报告。

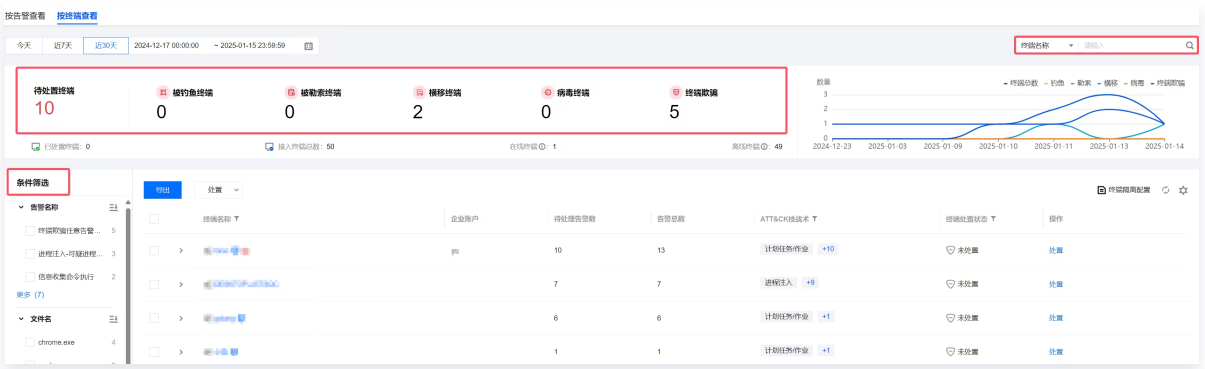


8. 分析过程中若获取样本失败，用户可单击**重新获取样本**重新投入沙箱进行分析。
9. 查看分析报告详情，支持查看该样本关联 IOC、多维检测、ATT&CK 行为检测、域前置信息、静态分析等多维度的详情信息。



按终端查看告警

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 威胁告警**。
2. 在威胁告警页面，支持按照终端查看产生的告警，用户可切换到该**按终端查看**页，查看产生告警的终端数据。
   - 支持多维度检索。



- 单击 > 支持查看某终端下的全部告警。



- 支持单击**告警名称/ID**查看告警详情以及处置该告警。



- **支持直接处置终端，单击处置，隔离终端。**



版权所有：腾讯云计算（北京）有限责任公司

威胁响应（11.1.1版）

最近更新时间：2026-02-13 09:41:02

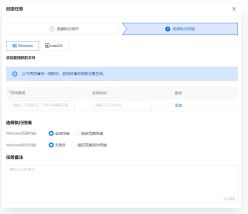
> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

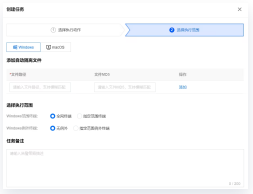
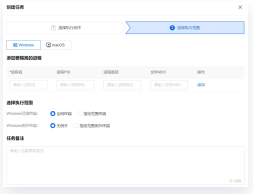
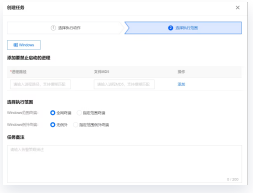
人工响应

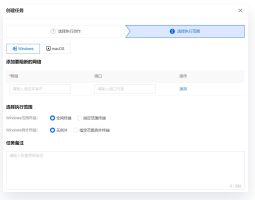
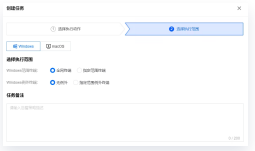
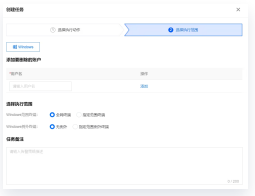
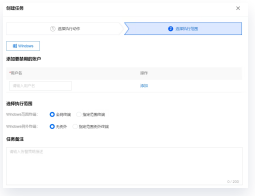
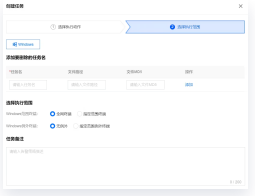
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵** > **高级威胁防护（EDR）** > **威胁响应**。
2. 在威胁响应页面，选择人工响应模块，可以单击**创建任务**，支持对威胁文件、进程、终端、账户等采用隔离、阻断等处置手段，同时也支持恢复隔离的进程、文件等，可以按照自身需求实时下发处置任务快速清除安全风险。

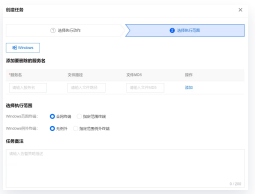
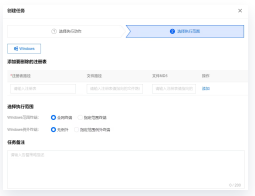
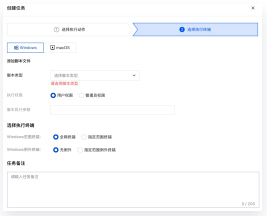


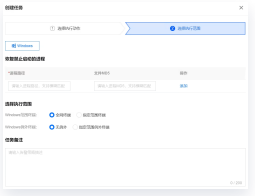
3. 在创建任务页面，选择执行动作和执行范围，单击**下发任务**。

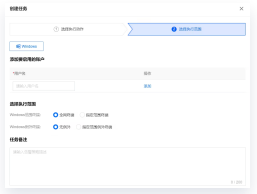
模块	处置任务	具体操作	示例
威胁处置	捕获文件	将终端文件捕获到指定位置，根据选择的触发条件支持对指定文件类型进行捕获，保存到本地。 • 选择系统：Windows、macOS。 • 添加文件路径、MD5，支持添加多个。 • 选择范围，支持选择执行范围或者是例外的范围。 • 添加备注，回溯任务更清晰。 • 填写完成后下发任务执行操作。	
	隔离文件	将文件加入隔离区限制其运行。 • 选择系统：Windows、macOS。 • 添加文件路径、MD5，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	

删除文件	根据选择的触发条件支持对指定文件类型进行删除操作 • 选择系统：Windows、macOS。 • 添加文件路径、MD5，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
自动隔离文件	创建目标文件后，该文件将会自动添加到隔离区。 • 选择系统：Windows、macOS。 • 添加文件路径、MD5，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
隔离进程	结束运行进程，并将进程文件加入隔离区限制其运行。 • 选择系统：Windows、macOS。 • 添加进程名、进程PID、进程路径、文件MD5，支持添加多个。 • 选择范围，支持选择执行范围或者是例外的范围。 • 添加备注备注，回溯任务更清晰。 • 填写完成后下发任务执行操作。	
禁止启动进程	禁止进程启动后，将无法创建该进程。 • 仅适用于 Windows 系统。 • 添加进程PID、进程路径、文件 MD5，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	

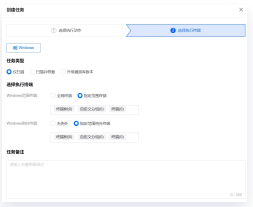
阻断网络连接	修改终端网络配置，限制访问特定网络。 • 选择系统：Windows、macOS。 • 添加网络（域名或 IP）、端口，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
隔离终端	修改终端防火墙策略配置，限制终端与外界通信。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
删除账户	将特定的账户从电脑系统中移除。 • 仅适用于 Windows 系统。 • 添加用户名，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
禁用账户	将特定的账户从电脑系统中禁用。 • 仅适用于 Windows 系统。 • 添加用户名，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
计划任务清理	删除恶意任务相关文件，阻止计划任务执行。 • 仅适用于 Windows 系统。 • 添加任务名、文件路径、文件 MD5，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	

	系统服务清理	删除恶意服务相关文件，阻止服务在未来重新执行。 • 仅适用于 Windows 系统。 • 添加服务名、文件路径、文件 MD5，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
	注册表清理	删除恶意注册表项，防止恶意软件运行传播。 • 仅适用于 Windows 系统。 • 添加注册表路径、文件路径、文件 MD5，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
	脚本执行	运行指定脚本文件应对威胁告警。 • 选择系统：Windows、macOS。 • 选择脚本类型、执行权限。 • 配置脚本执行参数。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
隔离恢复	恢复隔离文件	将文件从隔离区恢复。 • 选择系统：Windows、macOS。 • 添加文件名称、文件路径、文件MD5，支持添加多个。 **说明：** 文件名称、文件路径、文件MD5任填其中一项即可，若同时填写会取交集生效。 • 选择执行范围，支持选择执行范围或者是例外的范围。	

	• 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
恢复自动隔离文件	将自动隔离文件从隔离区恢复。 • 选择系统：Windows、macOS。 • 添加文件名称、文件路径、文件 MD5，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
恢复禁止启动进程	取消被禁止启动的进程，允许目标进程创建。 • 仅适用于Windows系统。 • 添加进程路径、文件MD5，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
恢复阻断网络连接	修改终端网络配置，恢复已限制网络地址的访问。 • 选择系统：Windows、macOS。 • 添加网络（域名或IP）、端口，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	
恢复隔离终端	排除终端内网横移风险后，恢复已隔离终端的网络通信。 • 选择系统：Windows、macOS。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	

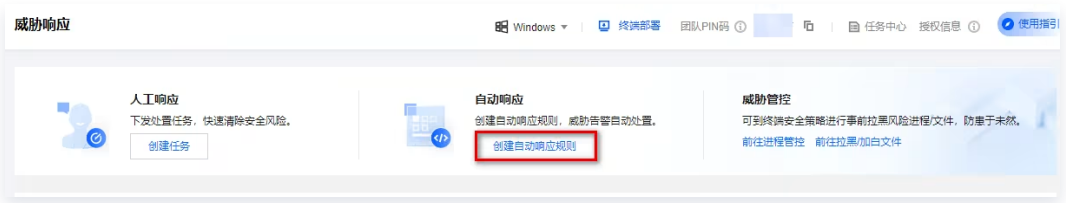
	启用账户	排除风险后，启用已禁止的账户。 • 仅适用于 Windows 系统。 • 添加用户名，支持添加多个。 • 选择执行范围，支持选择执行范围或者是例外的范围。 • 添加任务备注，回溯任务更清晰。 • 填写完成后注意下发任务执行操作。	

病毒查杀	病毒查杀	针对终端操作系统易感染的位置进行病毒扫描，用时较少。
		• 选择系统：Windows、macOS。
		• 扫描设置：
		  ○ 扫描类型，可选择全盘或者快速扫描，全盘扫描占用内存以及耗时较久。
		  ○ 扫描结果处置：仅扫描或者将病毒文件隔离后删除。
		  ○ 客户端信任区管理：勾选后，信任区内威胁较大的病毒文件将被清理并重新纳入扫描检测范围。
		  ○ 硬盘文件扫描范围：勾选后，本次扫描的硬盘文件类型仅覆盖文档文件，以缩短扫描耗时。
		• 选择执行范围，支持选择执行范围或者是例外的范围。
		• 添加任务备注，回溯任务更清晰。
		• 填写完成后注意下发任务执行操作。
			

漏洞修复	漏洞修复	针对系统漏洞风险下发对应扫描以及修复任务。
		• 选择系统：Windows。
		• 任务类型：
		  ○ 仅扫描。
		  ○ 扫描并修复。
		  ○ 升级漏洞库版本。
		• 选择执行范围，支持选择执行范围或者是例外的范围。
		• 添加任务备注，回溯任务更清晰。
		• 填写完成后注意下发任务执行操作。
			

自动响应

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 威胁响应**。
2. 在威胁响应页面，选择自动响应模块，单击**创建自动响应规则**，在命中该规则后，系统将会自动将对应的文件进行处置，包含隔离终端以及病毒查杀等处置任务。



3. 在新建自动响应页面，配置相关参数，单击**保存**。

3.1 编辑基本信息。



参数名称	说明
规则名称	自动响应规则名称。
规则描述	添加该处置规则的描述，便于后续查看以及修改。
是否启用	默认启用。

3.2 适用范围。

支持同时多选Windows、macOS，每勾选一个系统都需要确认生效范围，默认终端为全网终端，支持例外终端配置。



3.3 规则自定义。

3.3.1 触发条件配置：支持单独添加**条件**或者**条件组**，其中条件选择字段类型包含告警名称、动作、操作者节点、目标节点，选择字段后可以设置对应字段值和逻辑关系，每个字段条件关系默认为**且**，可以修改为**或**。



3.3.2 响应任务配置：当满足触发条件时，会自动下发响应任务。



任务名称	说明
隔离终端	修改终端防火墙策略配置，限制终端与外界通信。
病毒查杀	针对终端操作系统易感染的位置进行病毒扫描，用时较少。
捕获文件	根据选择的触发条件支持对指定文件类型进行捕获，保存到本地。

版权所有：腾讯云计算（北京）有限责任公司

删除文件	根据选择的触发条件支持对指定文件类型进行删除或者隔离响应操作。
脚本执行	根据选择的触发条件支持执行用户自行上传脚本文件。
隔离进程	根据选择的触发条件支持对指定进程类型进行隔离响应操作。
阻断网络连接	根据选择的触发条件，操作目标为网络时可以直接进行阻断处理 。

威胁管控

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 威胁响应**。
2. 在威胁响应页面，选择威胁管控模块。
   - 单击**前往进程管控**，跳转至进程管控（11.1.1版）策略。



   - 单击**前往拉黑/加白文件**，跳转至病毒查杀（11.1.1版）策略。



人工响应任务列表

- 单击**任务列表**，数据概览统计图可查看进行中任务/任务总数、进行中的重点任务分布、任务处置趋势图。



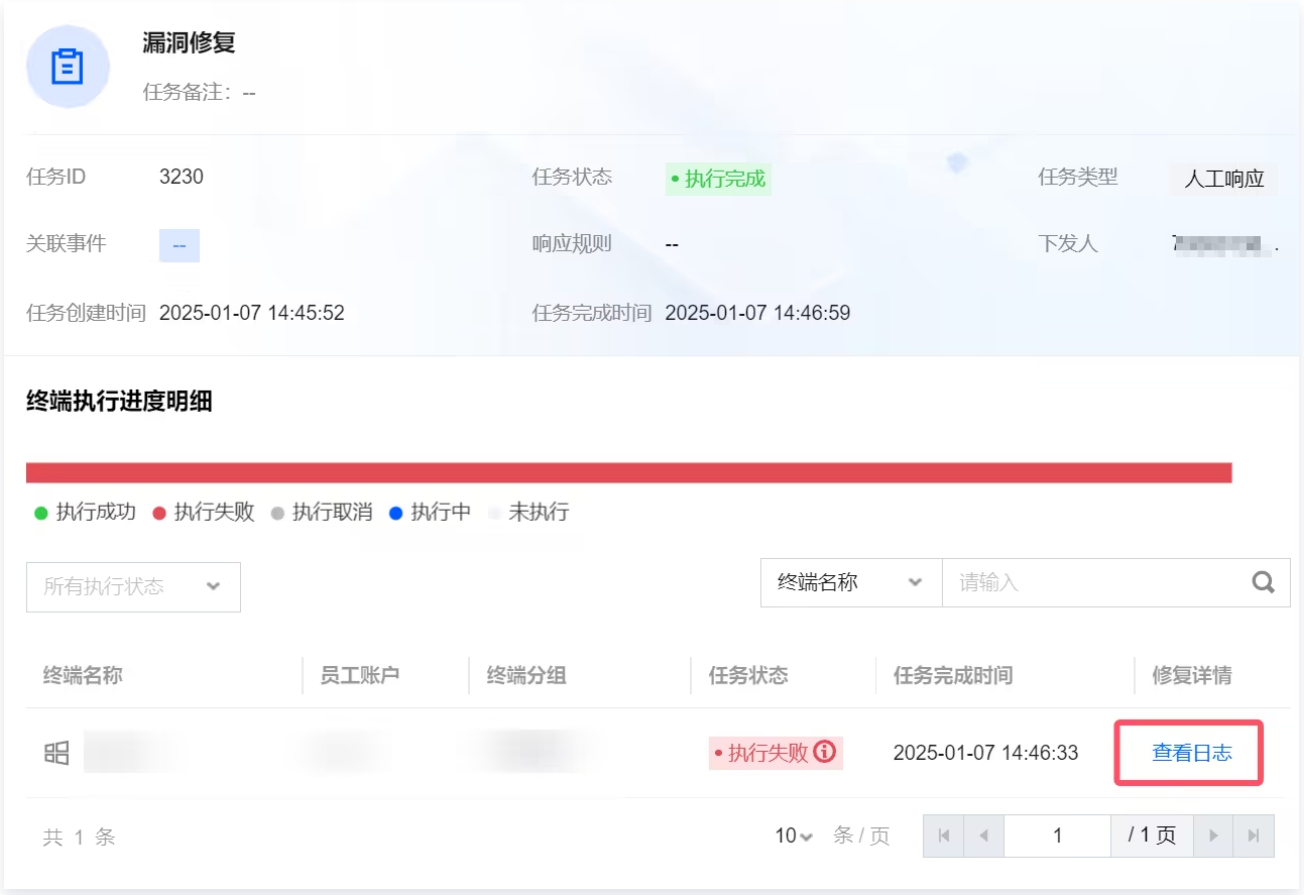
- 在任务列表中，可以看到具体的任务类型、任务状态、任务对象、执行动作等字段信息，单击⚙支持自定义列表字段。



- 在任务列表中，单击**查看详情**。

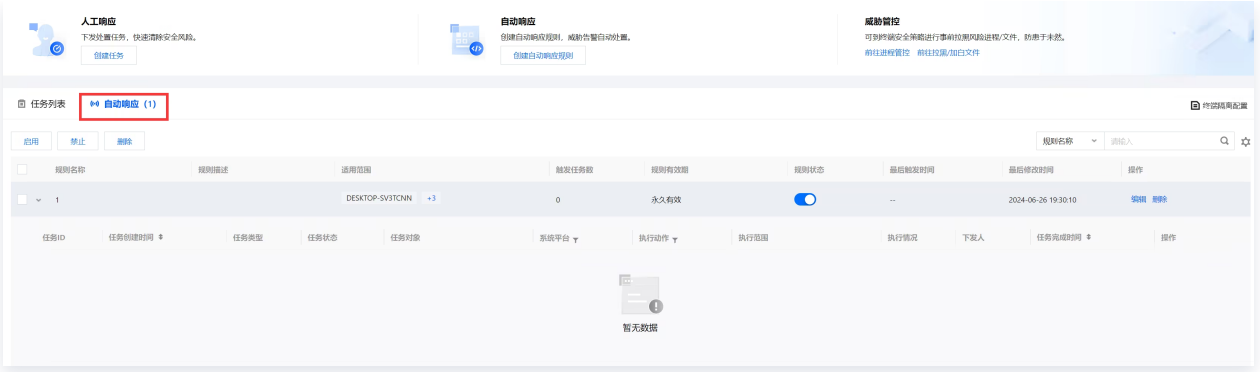


- 查看任务执行详细信息，单击**查看日志**，可查看并下载日志。



自动响应列表

- 在自动响应列表中，以规则维度进行展示，单击展开列表可以看到触发该规则的任务 ID、任务类型、任务对象等信息，支持查看详情。



- 在自动响应列表中，规则可直接进行**编辑、删除、启用、禁止**等操作。



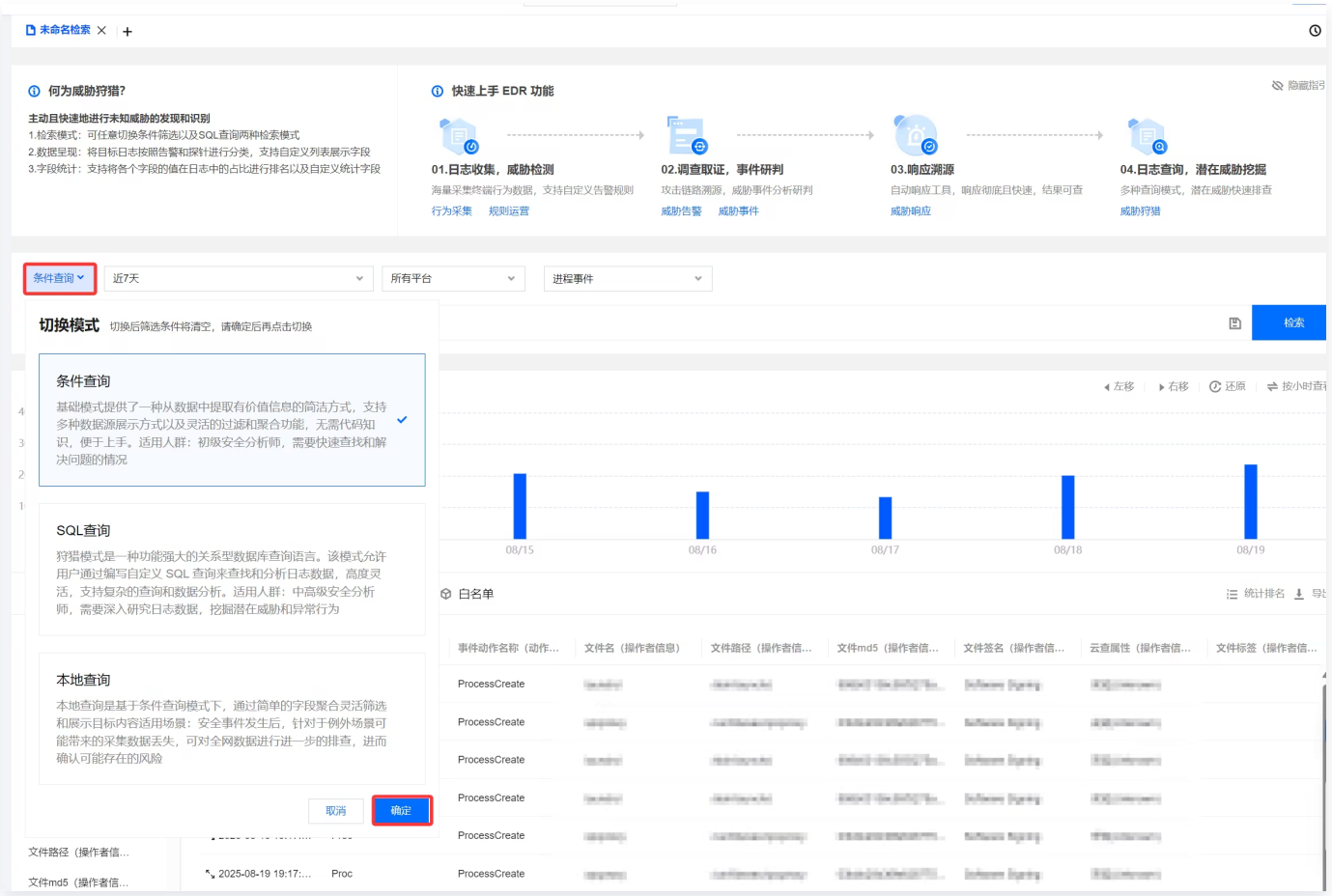
威胁狩猎（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

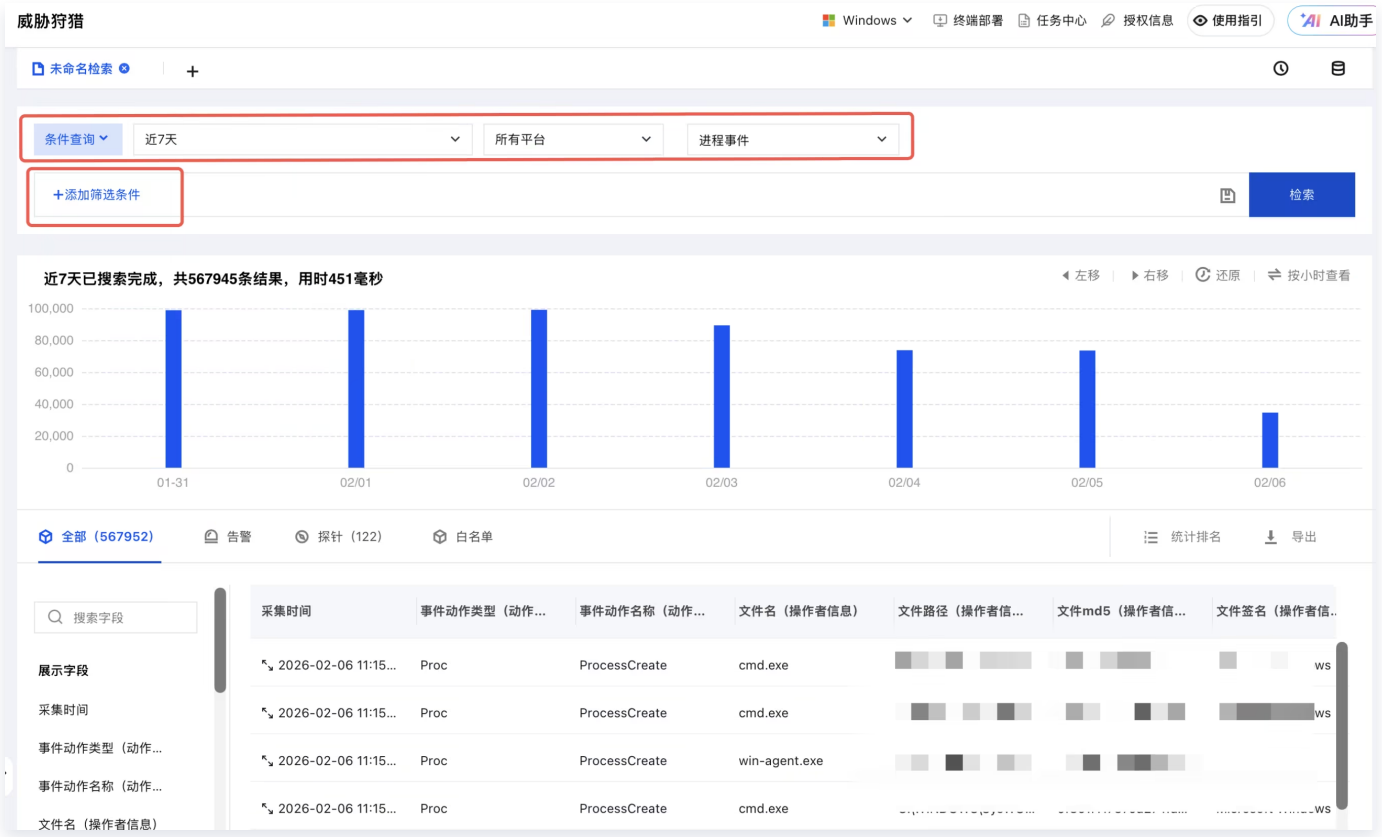
条件查询模式

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 威胁狩猎**。
2. 用户进入页面之后可以按照查询习惯自行选择查询方式，支持条件查询，SQL 查询模式，本地查询，默认用户进入后选择条件查询。
3. 从条件查询切换到 SQL 查询时，支持将查询条件自动转换为SQL语句，便捷查询，当前暂不支持从 SQL 查询切换为条件查询时反向代入。

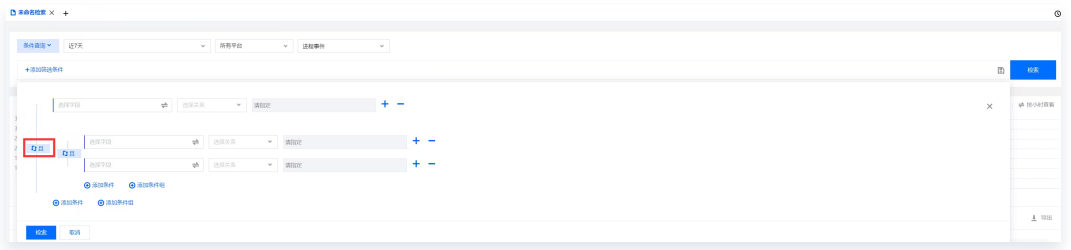


4. 在选择条件查询之后，支持用户选择时间范围（默认为7天）、系统平台（默认为 Windows 和 Mac）以及数据库表。

5. 单击**添加筛选条件**，展示所有字段弹框，可按照字段分类选择目标字段，支持选择该字段的逻辑关系（等于、不等于...），支持指定具体的检索值，若当前选择字段有枚举值，则会自动展示枚举值可选择，若没有枚举值，则需手动输入目标检索内容。



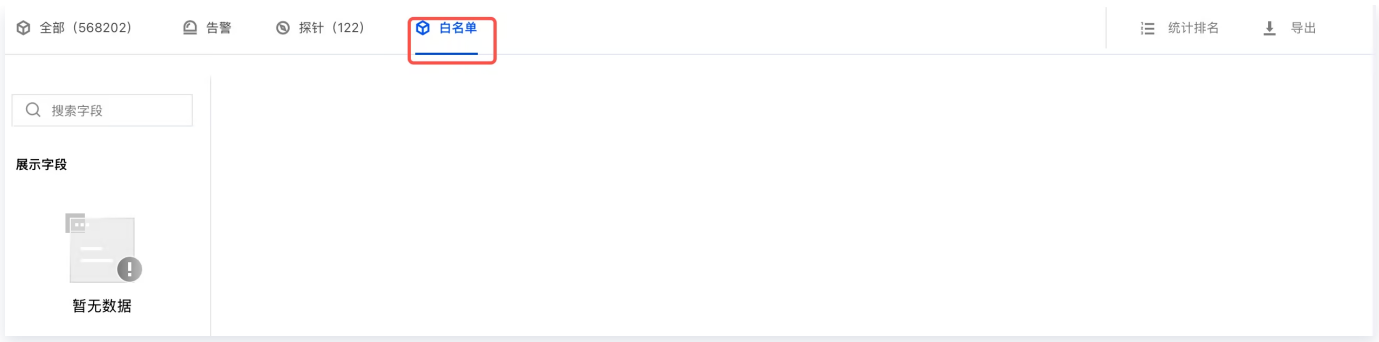
6. 多个字段组合检索：可以添加字段或者添加条件组，默认关系为**且**，整体逻辑与规则运营中添加告警条件保持一致。



7. 检索后页面会展示以日为维度的统计图，支持进行拖拽。检索结果分为全部、告警、探针、白名单等以当前日志命中的规则类型进行分类，支持切换 Tab 进行区分。



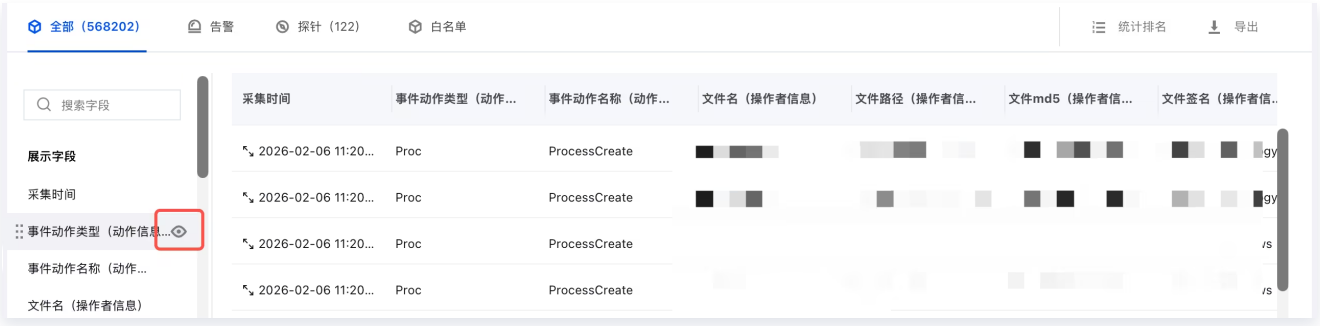
8. 白名单支持从 行为检测 页面直接跳转至该标签页，并自动代入相关条件，从而快速掌握白名单规则的生效状况。



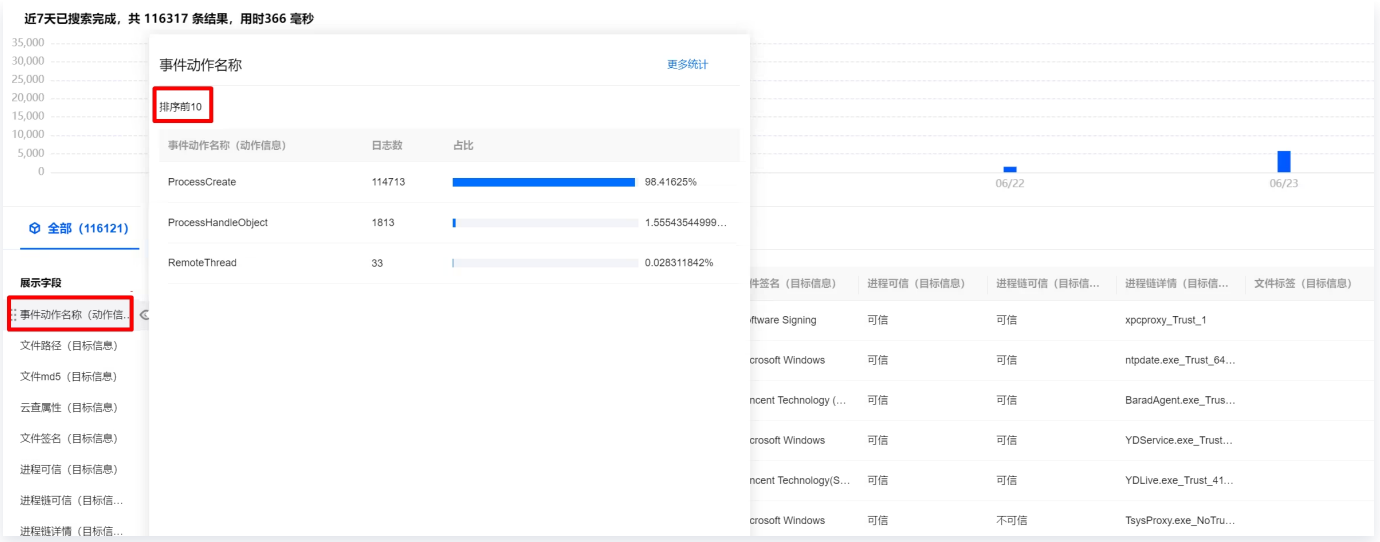
9. 左侧会展示检索结果的所有字段信息，展示字段会在右侧列表进行展示。



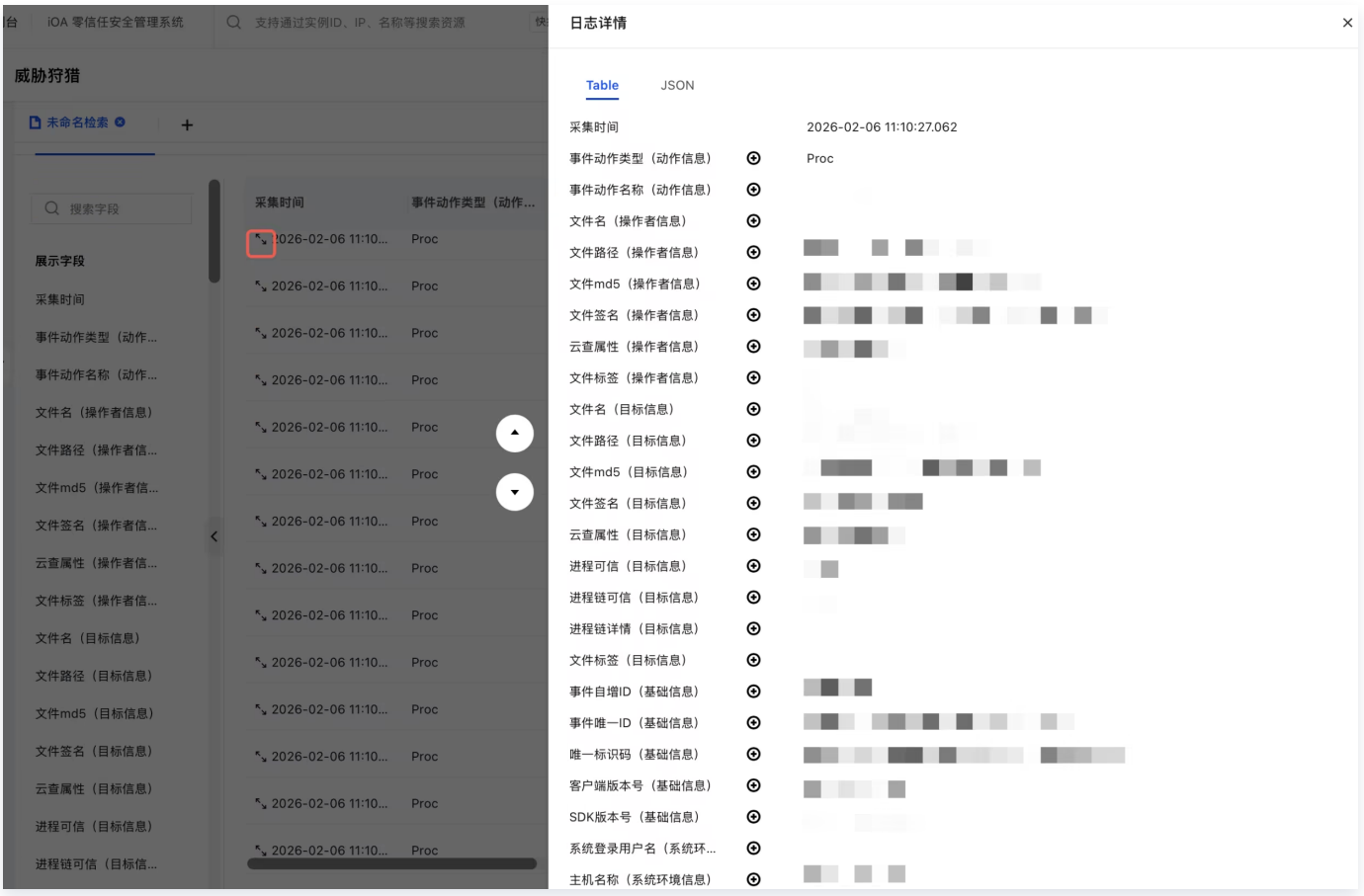
9.1 单击 隐藏该字段，隐藏字段不在右侧列表进行展示。



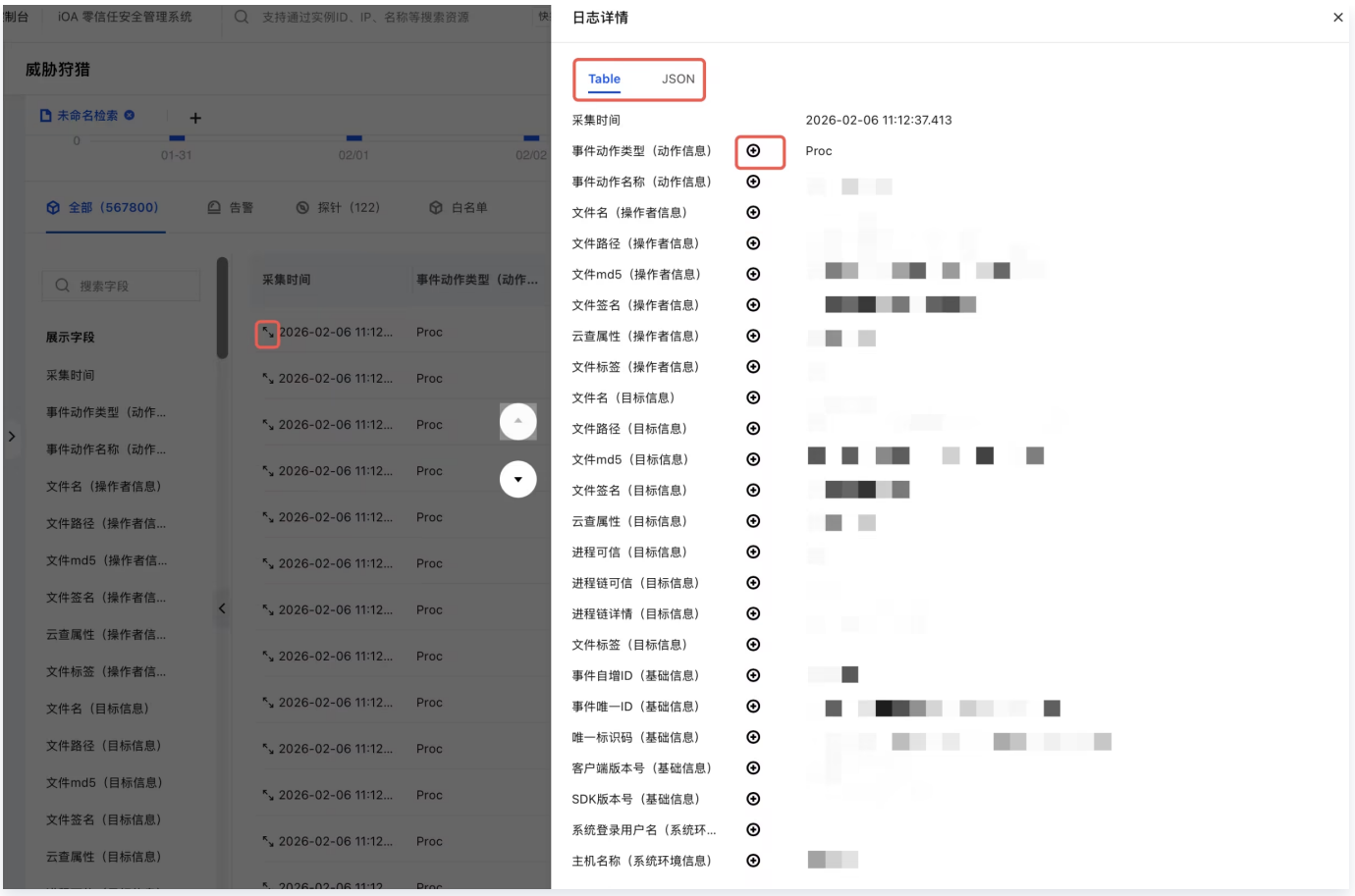
10. 支持自定义，将鼠标悬停在特定字段上时，会展示该字段下所有数值信息的统计Top10，单击**更多统计**可弹出展示对应抽屉，可以统计目标值的统计数据。



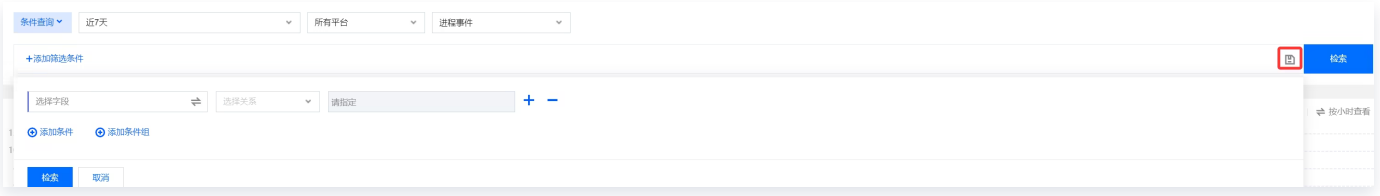
11. 数据栏展示具体的事件信息：每一条日志单击 ↘ 都可以展示详情信息。



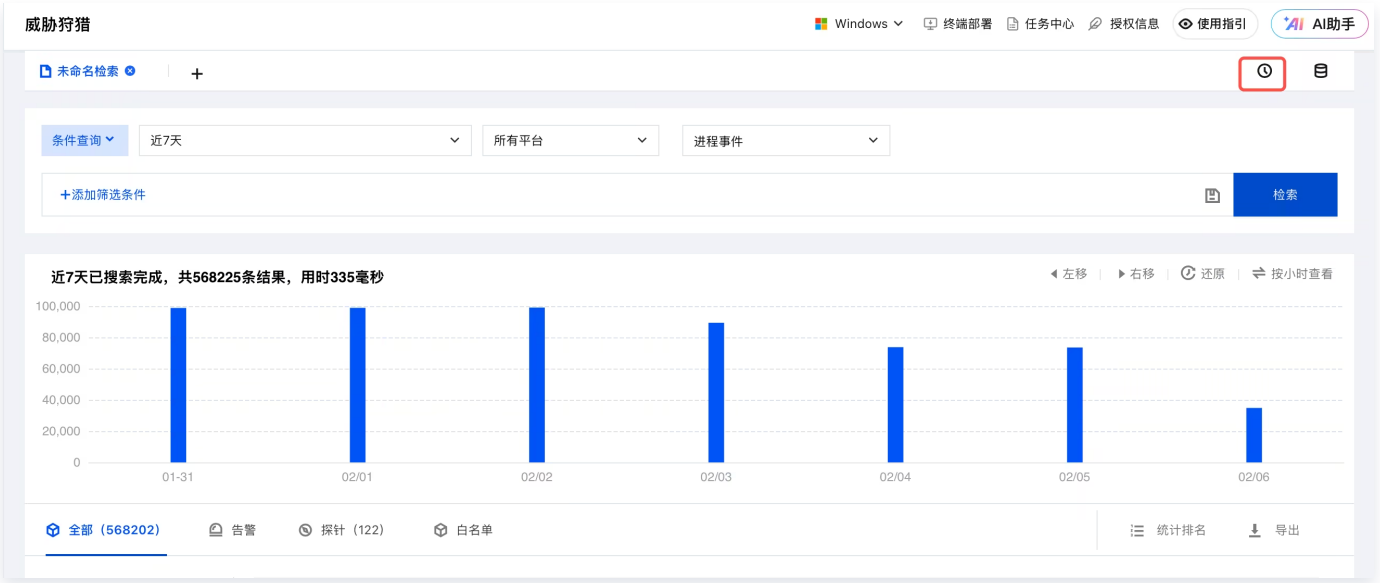
12. 支持以 tab 和 JSON 的形式进行展示。其中，每一个字段的数值都可以进行进一步的筛选。单击 ⊕ 可以筛选出包含该目标值的日志信息，单击 ⊖ 可以排除所有包含目标值的日志信息。



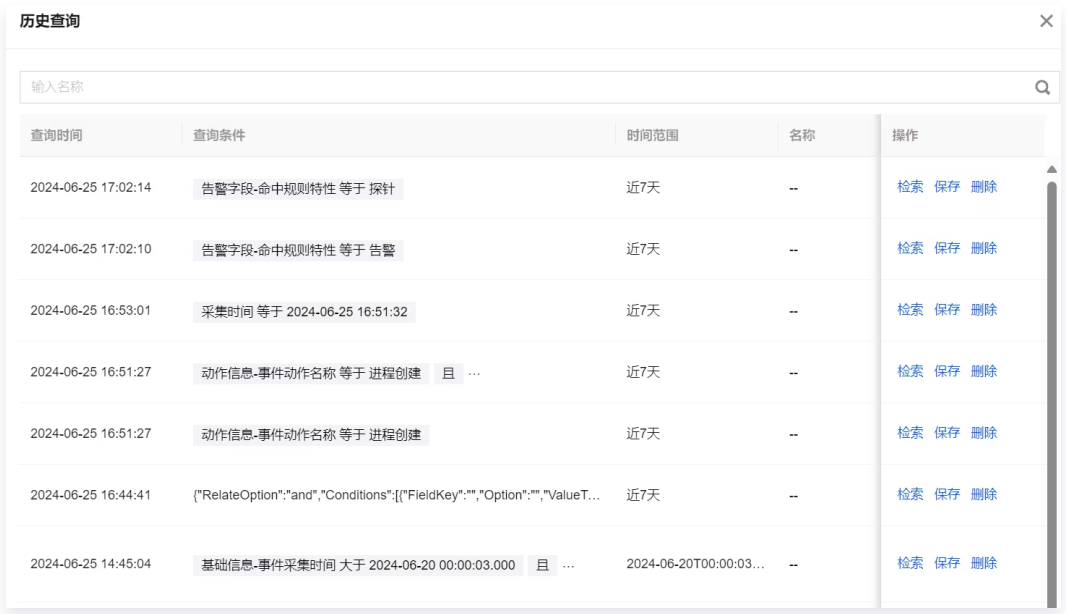
13. 在搜索框最右侧单击，输入名称以及上级目录可以保存该查询条件。



14. 在搜索框最右侧单击**查询历史**，可查看历史条件信息。

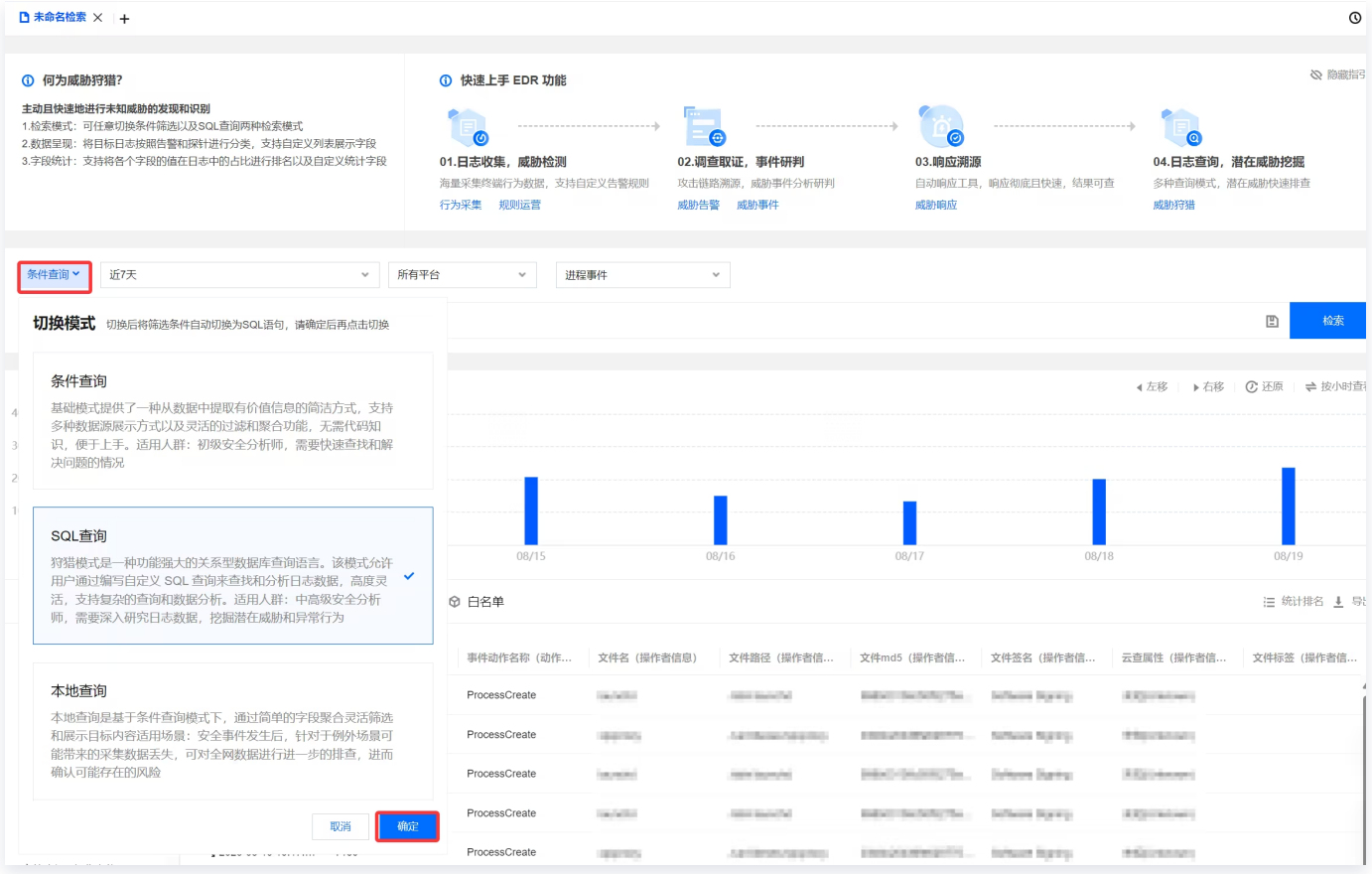


15. 历史查询支持检索、保存、删除。

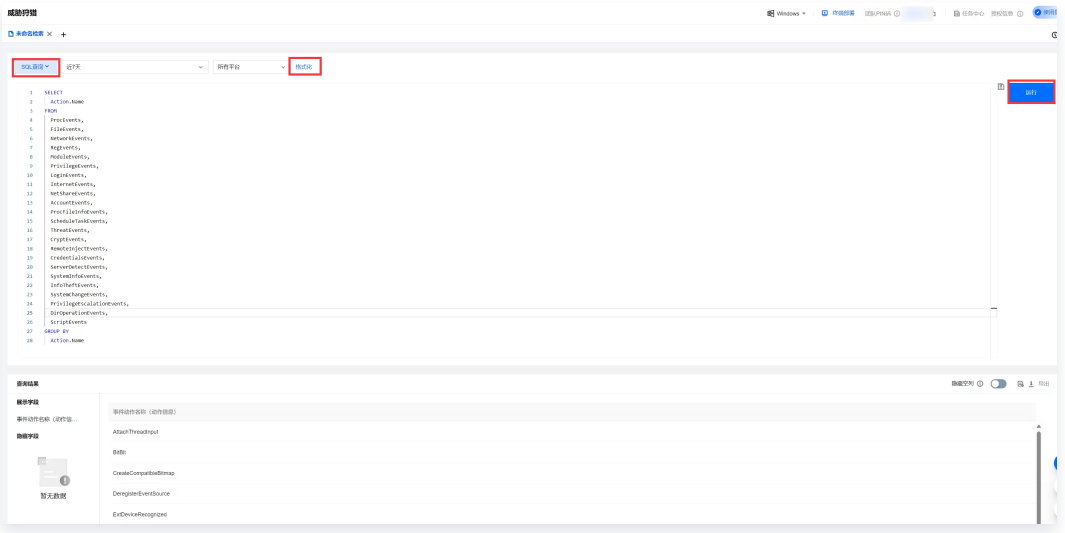


SQL 查询模式

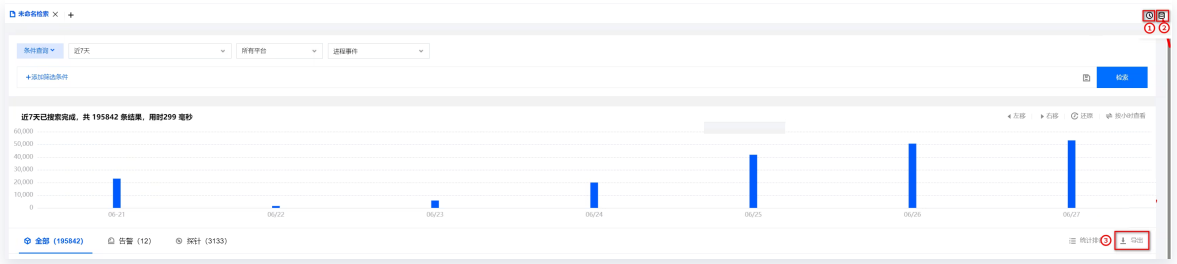
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 威胁狩猎**。
2. 在威胁狩猎页面，单击**条件查询**，选择**SQL 查询**，单击**确定**。



3. 在选择 SQL 查询模式之后，支持基于 SQL 的高级搜索模式，协助安全运营人员主动且快速地进行未知威胁的发现和识别。



4. 重点图标说明：①查询历史、②展开数据库、③下载查询数据。



常用 SQL 语句说明

分组名称	语句名称	SQL 语句
运行检查	查询事件动作列表	SELECT Action.Name FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents GROUP BY Action.Name
	统计所有事件总数	SELECT COUNT(1) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoThe

		ftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents
	统计终端维度所有动作总数排序	SELECT Common.Mid,Environment.HostName,COUNT(uuid) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents GROUP BY Common.Mid,Environment.HostName ORDER BY COUNT(uuid) DESC
	统计动作维度事件总数排序	SELECT Action.Name, COUNT(1) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents GROUP BY Action.Name ORDER BY COUNT(uuid) DESC
	统计有事件上报的终端总数	SELECT COUNT(DISTINCT Common.Mid) from ProcEvents
性能分析	统计进程维度文件动作总数排序	SELECT Parent.FileName,Action.Name,COUNT(uuid) FROM FileEvents GROUP BY Parent.FileName,Action.Name ORDER BY COUNT(uuid) DESC
	统计进程维度所有动作总数排序	SELECT Parent.FileName, COUNT(1) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents GROUP BY Parent.FileName ORDER BY COUNT(uuid) DESC
	查询指定终端进程的文件动作	SELECT Action.Name, Parent.FileName, Child.FilePath FROM FileEvents WHERE Common.Mid = 'FAA210E266DEFB880E23A3504315945B61EEAF0B' AND Parent.FileName = 'QQMusic.exe'

	统计指定终端动作总数排序	SELECT Action.Name, COUNT(uuid) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents WHERE Common.Mid = 'F72A41F496988F89B0CA6936939D04A86257CFB8' GROUP BY Action.Name ORDER BY COUNT(uuid) DESC
	统计终端维度所有事件上报量	SELECT Common.Mid,COUNT(1) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents GROUP BY Common.Mid
安全运营	查询指定终端和文件名的进程创建事件	SELECT * FROM ProcEvents WHERE Common.Mid = '2F2DE5496C00F0522C974FABCE7000A862761B98' AND Parent.FileName LIKE 'cmd.exe' and Child.FileName LIKE 'notepad.exe'
	查询指定终端进程文件信息收集	SELECT * FROM ProcFileInfoEvents WHERE Environment.HostName = 'kael-pc'
	查询指定文件操作事件	SELECT * FROM FileEvents WHERE Environment.HostName = 'kael-pc'
	查询指定终端模块事件	SELECT * FROM ModuleEvents WHERE Environment.HostName = 'kael-pc'
	查询指定终端注册表事件	SELECT * FROM RegEvents WHERE Environment.HostName = 'kael-pc'
	查询指定终端网络事件	SELECT * FROM NetworkEvents WHERE Environment.HostName = 'kael-pc'
	查询指定终端WMI事件	SELECT * FROM WMIEvents WHERE Environment.HostName = 'kael-pc'
	查询指定终端系统变更事件	SELECT * FROM LoginEvents WHERE Environment.HostName = 'kael-pc'

版权所有：腾讯云计算（北京）有限责任公司

查询指定终端特权操作事件	SELECT * FROM PrivilegeEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端计划任务事件	SELECT * FROM ScheduleTaskEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端用户账户事件	SELECT * FROM AccountEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端网络共享事件	SELECT * FROM NetShareEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端加密事件	SELECT * FROM CryptEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端远程注入事件	SELECT * FROM RemoteInjectEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端提权事件	SELECT * FROM PrivilegeEscalationEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端用户凭据事件	SELECT * FROM CredentialsEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端服务器探测事件	SELECT * FROM ServerDetectEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端网络访问事件	SELECT * FROM InternetEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端系统信息收集	SELECT * FROM SystemInfoEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端信息窃取	SELECT * FROM InfoTheftEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端脚本事件	SELECT * FROM ScriptEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端文件统计事件	SELECT * FROM FileStatisticsEvents WHERE Environment.HostName = 'kael-pc'
查询指定终端注入采集统计	SELECT * FROM AgentInjectHookStatics WHERE Common.HostName = 'kael-pc'
查询进程事件中命中规则名称包含	SELECT * FROM ProcEvents WHERE Alert.RuleName LIKE '%powershell%'

	PowerShell 的事件	
	查询文件事件中命中规则为12604的事件	SELECT * FROM FileEvents WHERE Alert.RuleId = '12604'
	安全运营-查询 PowerShell 模块加载事件	SELECT * FROM ModuleEvents WHERE Parent.FileName = 'powershell.exe'
	查询设置注册表键值包含 SystemRoot 的事件	SELECT * FROM RegEvents WHERE Action.Name = 'RegSetValue' and Child.RegValData LIKE '%systemroot%'
	查询访问192.168.0.4的事件	SELECT * FROM NetworkEvents WHERE Child.DstIp = '192.168.0.4'
	查询指定主机利用 WMI 调用 Win32_Process 的事件	SELECT * FROM WMIEvents WHERE Child.ClientMachine = 'DC01' AND Child.Operation LIKE '%Win32_Process%'
	查询清除日志事件	SELECT * FROM ThreatEvents WHERE Action.Name = 'ClearEventLogW'
	查询枚举域控名称事件	SELECT * FROM ServerDetectEvents WHERE Action.Name = 'DsGetDcNameW'
	查询 PowerShell 遍历文件事件	SELECT * FROM ProcFileInfoEvents WHERE Action.Name = 'FindFirstFileW' AND Parent.FileName = 'powershell.exe'
	查询 PowerShell 修改注册表事件	SELECT * FROM RegEvents WHERE Parent.FileName = 'powershell.exe'
文件审计	某文件全网首次出现时间	SELECT min(@collection) FROM FileEvents WHERE Child.FileName = 'xx'
	某文件全网机器覆盖量	SELECT Environment.HostName FROM FileEvents WHERE Child.FileName = 'xx' GROUP BY Environment.HostName
	全网新入文件	

		SELECT @collection,Child.FileName FROM FileEvents ORDER BY @collection DESC
网络审计	xx 网络请求全网首次出现时间	SELECT min(@collection) FROM NetworkEvents WHERE Child.DstIp = 'xx'
	xx 网络请求全网访问量	SELECT count(Child.DstIp) FROM NetworkEvents WHERE Child.DstIp = 'xx'
探针规则统计	全网探针规则命中的事件量排序	SELECT Alert.RuleName,COUNT(1) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents WHERE Alert.RuleNature = '0' GROUP BY Alert.RuleName ORDER BY COUNT(1) DESC
	全网探针规则命中的Top事件	SELECT Alert.RuleName,COUNT(1) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents WHERE Alert.RuleNature = '0' GROUP BY Alert.RuleName ORDER BY COUNT(1) DESC LIMIT 10
告警统计	查询探针总数	SELECT COUNT(1) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents WHERE Alert.RuleName != ''
	全网告警、探针命中 Top按规则名排序	SELECT Alert.RuleName,COUNT(1) FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,D

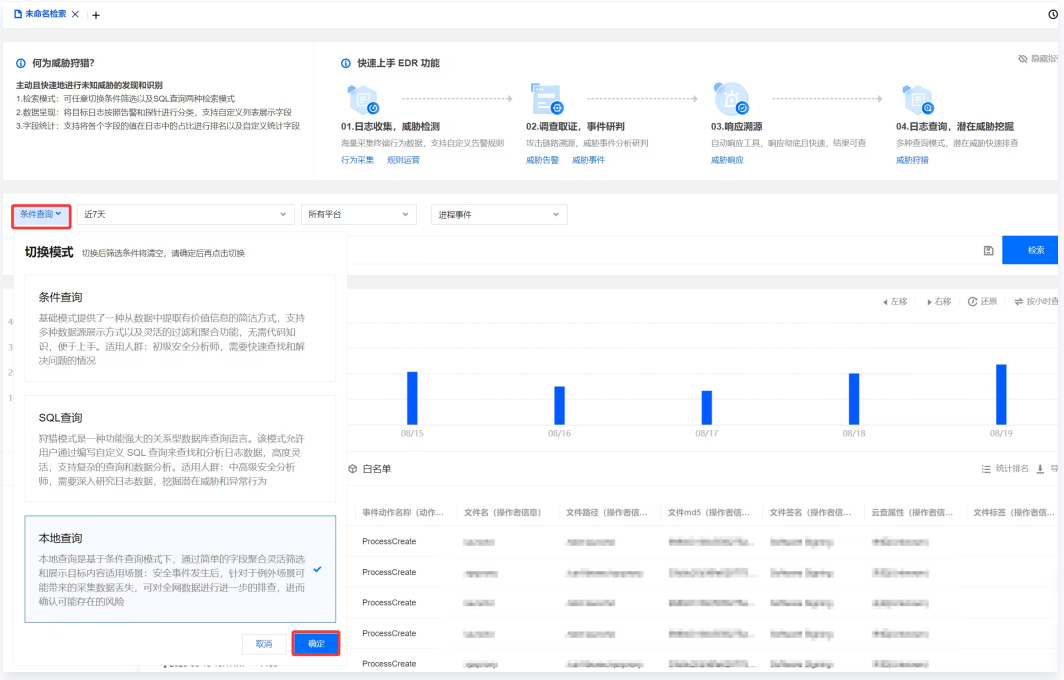
版权所有：腾讯云计算（北京）有限责任公司

		irOperationEvents,ScriptEvents WHERE Alert.RuleId > 0 GROUP BY Alert.RuleName ORDER BY COUNT(1) DESC
	查询指定探针数据	SELECT Parent.FilePath,Parent.ProcPid,Action.Name,Alert.RuleName,Alert.RuleId FROM ProcEvents,FileEvents,NetworkEvents,RegEvents,ModuleEvents,PrivilegeEvents,LoginEvents,InternetEvents,NetShareEvents,AccountEvents,ProcFileInfoEvents,ScheduleTaskEvents,ThreatEvents,CryptEvents,RemoteInjectEvents,CredentialsEvents,ServerDetectEvents,SystemInfoEvents,InfoTheftEvents,SystemChangeEvents,PrivilegeEscalationEvents,DirOperationEvents,ScriptEvents WHERE Alert.RuleName != ''

本地查询模式

> **说明：**
> 使用本地查询模式，需先配置**规则策略 > 行为采集 > 本地数据采集**。

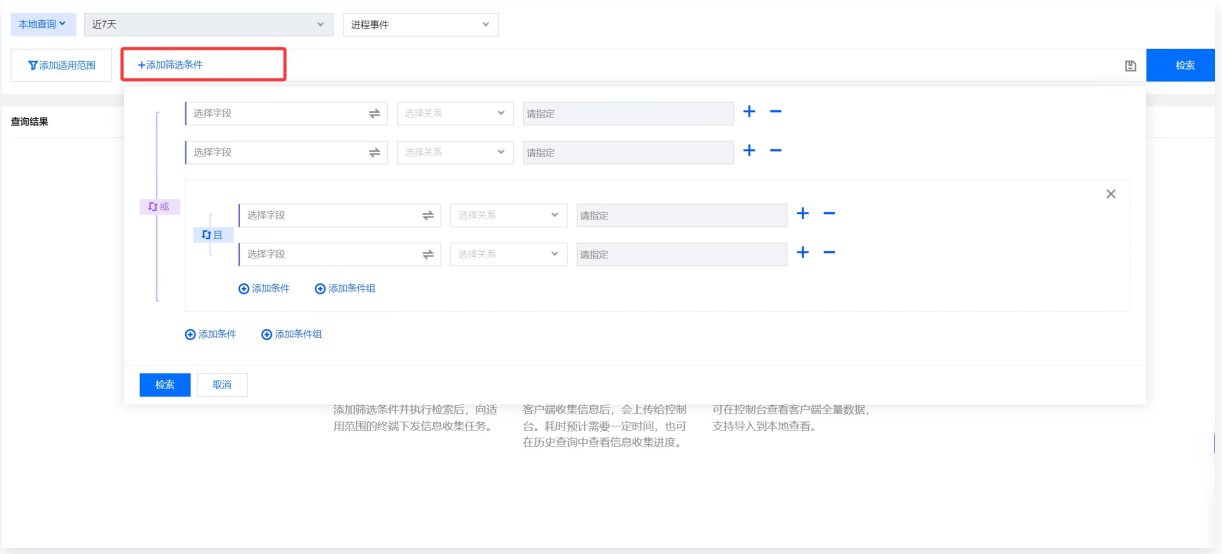
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**终端防入侵 > 高级威胁防护（EDR）> 威胁狩猎**。
2. 在威胁狩猎页面，单击**条件查询**，选择**本地查询**，单击**确定**。
3. 基于条件查询的模式下，支持对采集并存储在用户终端的数据进行检索，可对全网数据进行更深入的排查。



4. 单击**添加适用范围**，勾选需管控排除的终端，添加终端用于确定检索范围，本地检索是对指定终端范围进行检索，单击**存为预设**后可在预设范围中查看。



5. 单击**添加筛选条件**，展示所有字段弹框，可按照字段分类选择目标字段，支持选择该字段的逻辑关系（等于、不等于...），支持指定具体的检索值，若当前选择字段有枚举值，则会自动展示枚举值可选择，若没有枚举值，则需手动输入目标检索内容。



敏感数据保护（11.1.1版）
风险调查（11.1.1版）

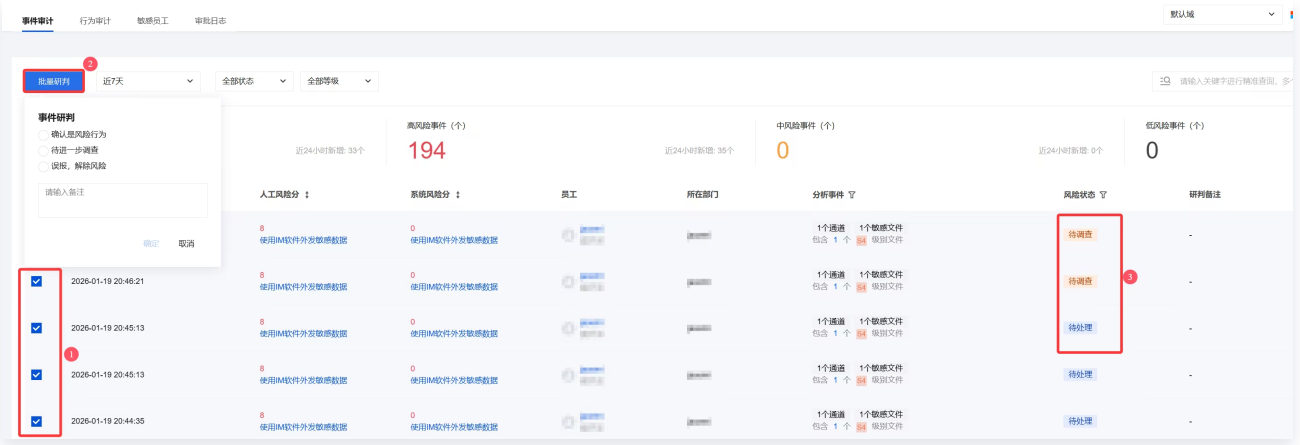
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

识别、分析和处置员工在终端设备上的敏感数据外发行为，为安全管理员提供统一的风险事件研判与响应入口，实现从风险发现到闭环处置的全流程管理。

事件审计

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**风险调查** > **事件审计** 。
2. 在**管控策略** > **事件聚合规则** 中，命中事件聚合规则的行为在 事件审计 中展示。
3. 批量研判：勾选**风险事件**，单击**批量研判**，示例：选择**待进一步调查**后，风险状态字段下，该事件由待处理变更为待调查。



4. 时间范围：支持时间段筛选，提供标准时间筛选控件：通过顶部左上角的 “近7天” 下拉选择框，您可以快速切换查看“今天”、“近7天” 、“近14天”、“近30天”、“自定义日期”等不同时间范围内的审计日志。
5. 状态筛选：选择事件处理状态（全部状态/待处理/无风险/有风险/待调查）。
6. 等级筛选：选择风险等级（高/中/低风险）。
7. 单击**详情**，查看单个风险事件的完整信息，进行行为溯源和研判处置。支持分析外发敏感数据的具体操作、涉及文件及风险等级，实现从告警到处置的闭环管理。



8. 单击**查看详情**，查看行为审计详情信息。



9. **研判：为安全管理员提供人工复核风险事件的决策入口，单击研判，支持将系统检测到的告警标记为确认是风险行为、待调查或误报，并填写备注说明，实现人机协同的精准化事件定性。示例：选择误报，解除风险后，风险状态由待处理变更为无风险。**



行为审计

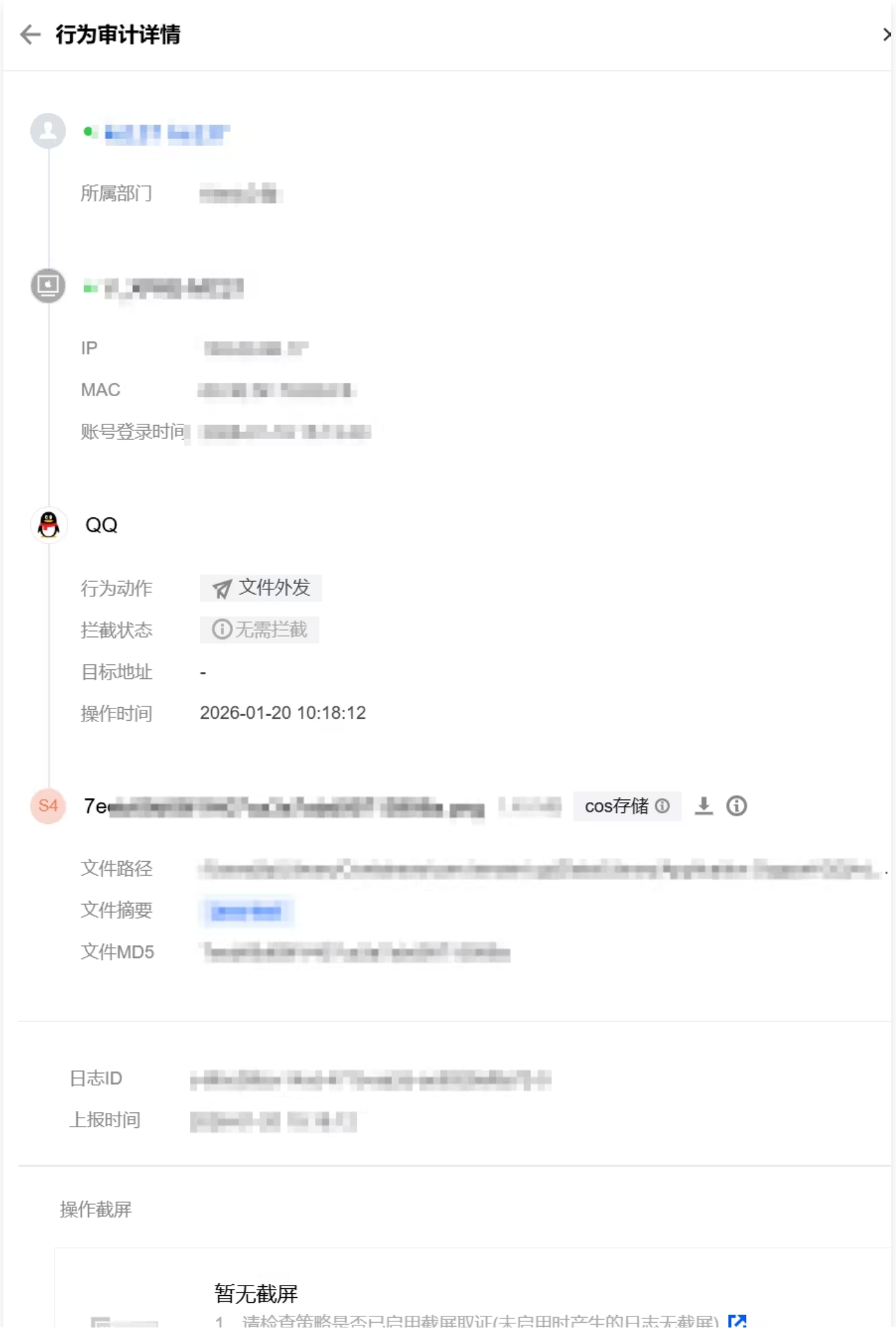
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**风险调查** > **行为审计**。
2. 在行为审计页面，展示所有命中**分级分类规则**的文件外发行为的信息，包括告警时间、告警动作、文件名称、外发通道、目标地址等信息，触发**管控策略** > **管控策略** > **审计策略**的信息在此展示。
3. 支持按时间、操作类型、风险等级等筛选审计日志。

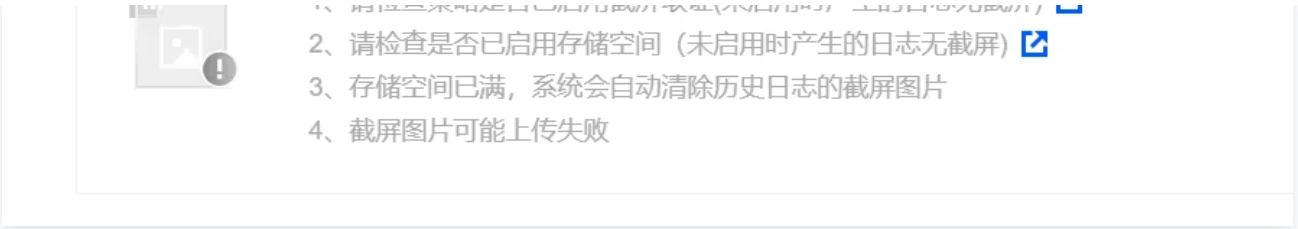


4. 单击**更多统计维度**，展示该页面，敏感数据页用于统计和分析员工外发敏感数据的风险态势，通过可视化图表展示不同风险等级员工数量、各外发通道（即时通信、浏览器、网盘、远程控制工具等）的文件数量与数据总量，支持按时间维度筛选并下钻分析具体渠道（如QQ、企业微信、飞书）的泄密风险详情。



5. 在**行为审计**页面，选择所需告警，单击操作列的**详情**，即可查看行为审计详情信息。


行为审计详情
所属部门
IP
MAC
账号登录时间
QQ
行为动作
文件外发
拦截状态
无需拦截
目标地址
-
操作时间
2026-01-20 10:18:12
S4
cos存储
文件路径
文件摘要
文件MD5
日志ID
上报时间
操作截屏
暂无截屏

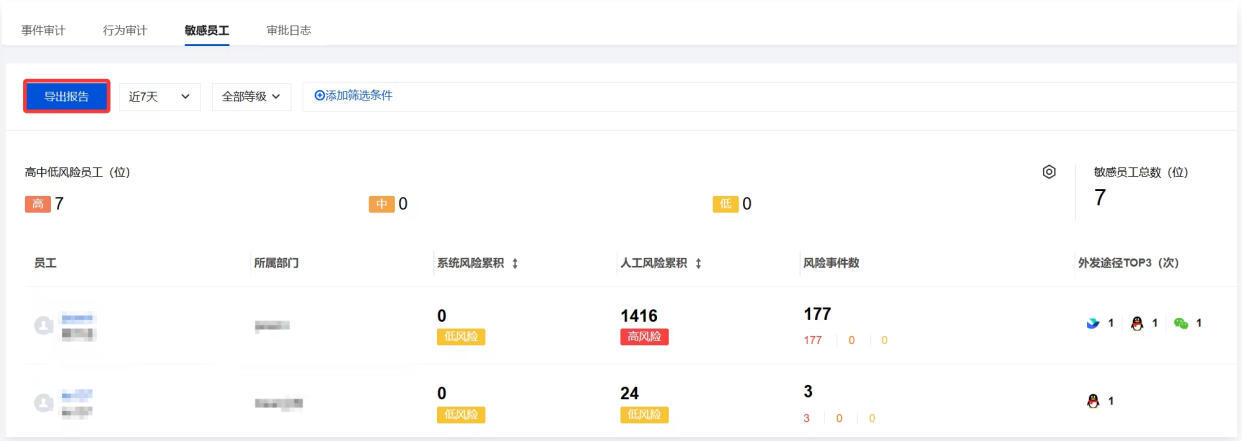


敏感员工

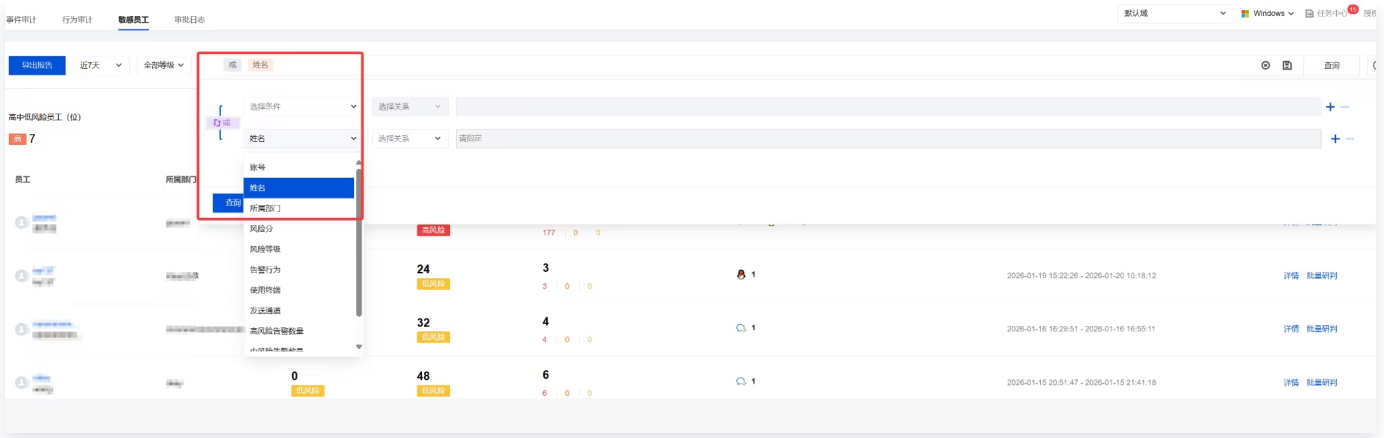
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**风险调查** > **敏感员工**。
2. 在风险员工页面，展示风险员工趋势图以及过去一段时间的风险等级数据。
   - 支持时间段选择：今天、近7天、近30天以及自由选择时间查询。
   - 支持展示员工异常行为人数，并分为高危、中危以及低危三类风险员工。



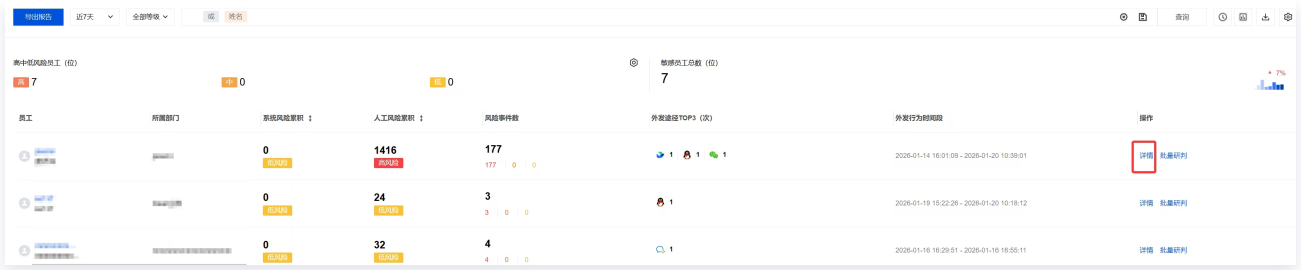
3. 单击**导出报告**，可一键汇总导出一定时间范围内的数据安全运营情况，报告涵盖终端安装情况、策略规则、审计结果三个方面：
   - 终端安装部分统计了全网不同操作系统的终端数量及占比；
   - 策略规则部分包括敏感文件规则（敏感词库、文档类型、数据分级分类规则）和安全响应策略（风险告警、拦截、通道审计策略数量）；
   - 审计结果部分从外发情况（外发通道、文件级别、文件类型、部门分布）、数据安全响应（风险告警、外发拦截）以及风险员工（风险等级、部门分布、Top10 员工）三个维度进行详细分析。



4. 添加筛选条件栏支持按风险分、风险告警数、告警行为等信息筛选，支持筛选触发了特定告警策略的风险员工，支持且/或复杂条件组合筛选。



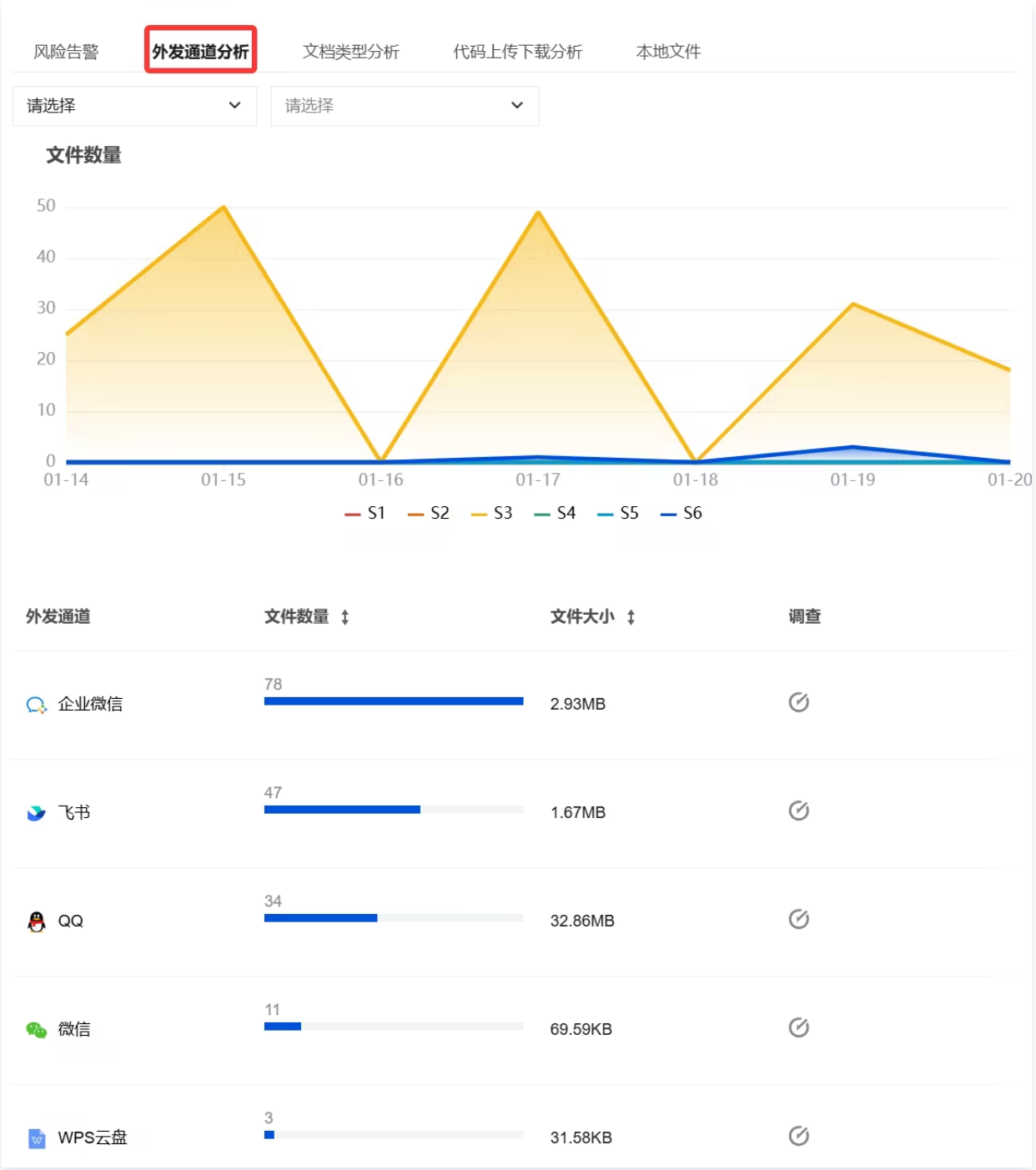
5. 单击**详情**，可查看风险员工详情信息。



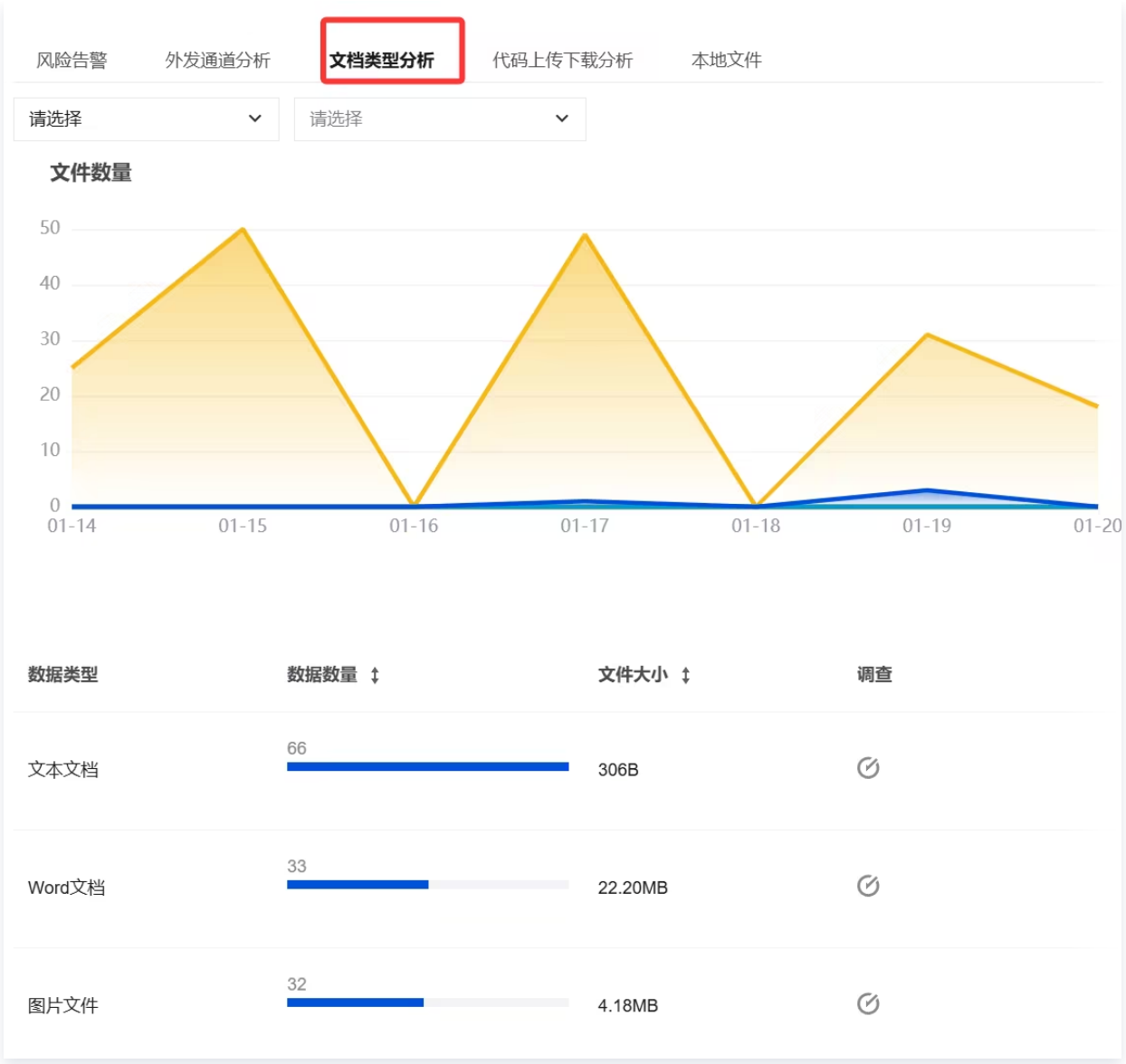
- **风险告警：以时间轴的方式展示单个员工触发安全事件，包含安全事件标题、外发文件类型、数量、大小、敏感数据类型、外发通道以及发生时间等详情。**



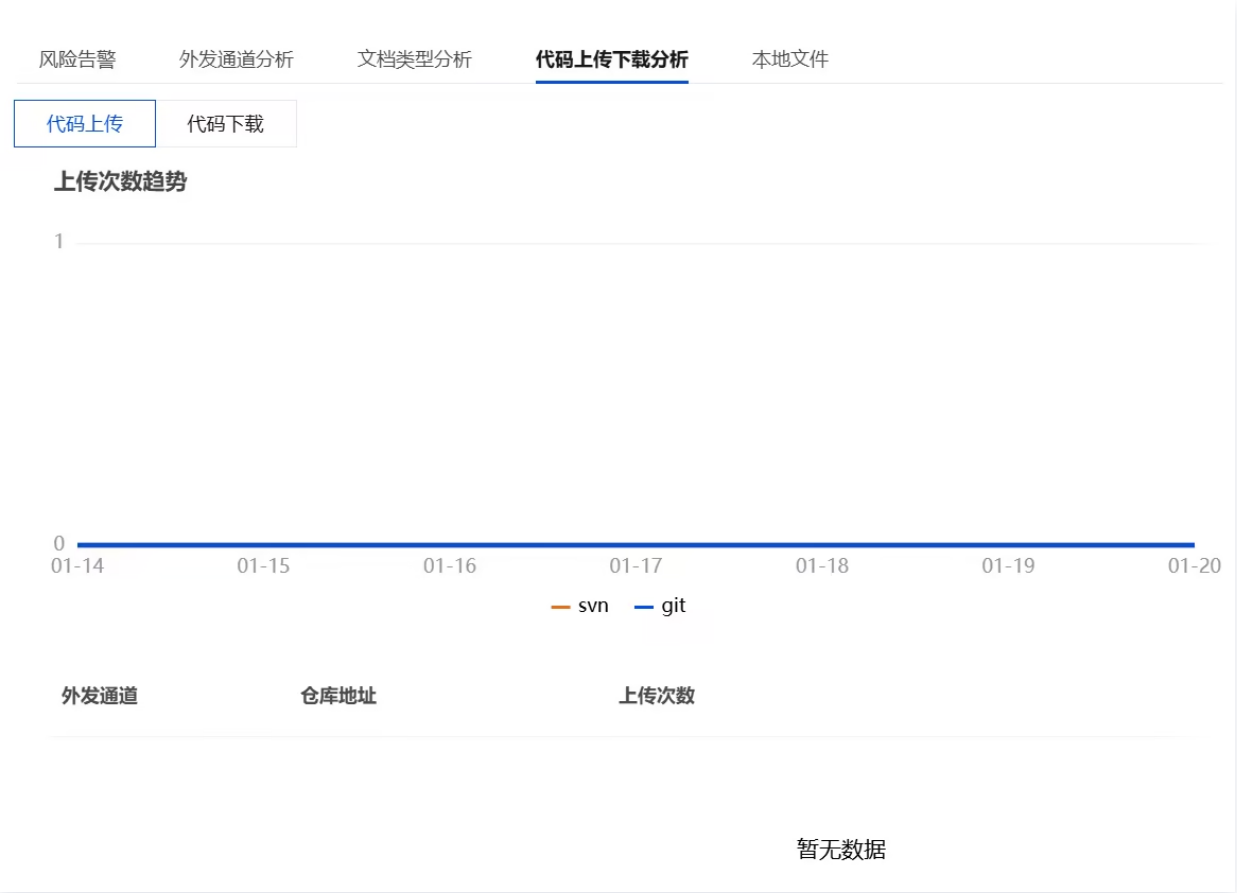
- **外发通道分析：展示单个员工所有外发通道发送数据敏感等级、文件数量、数据大小、发生时间等信息统计。**



- 文档类型分析：展示单个员工所有外发文件类型分布统计，包括敏感等级、文件类型、数据数量、文件大小等信息聚类展示。



- **代码上传下载分析：展示单个员工代码上传下载次数及趋势，包括外发通道、仓库地址、上传次数/下载次数信息聚类展示。**



- 本地文件：可提取/下载文件，支持删除文件信息。单击**删除**，下发删除终端文件的任务后，终端删除该文件。本地文件来源**数据地图** > **数据地图扫描策略**，终端扫描上报的文件信息。



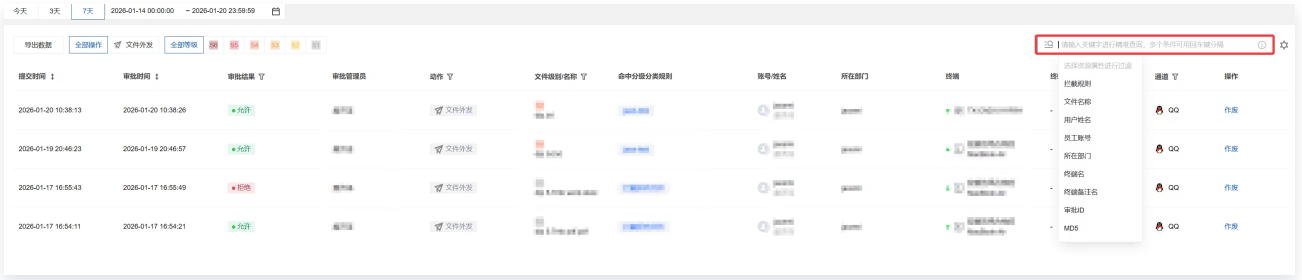
审批日志

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**风险调查** > **审批日志**。
2. 在管控策略配置的拦截策略包含的审批设置信息。当审批流中的管理员完成审批后，审批结果将在审批日志展示。

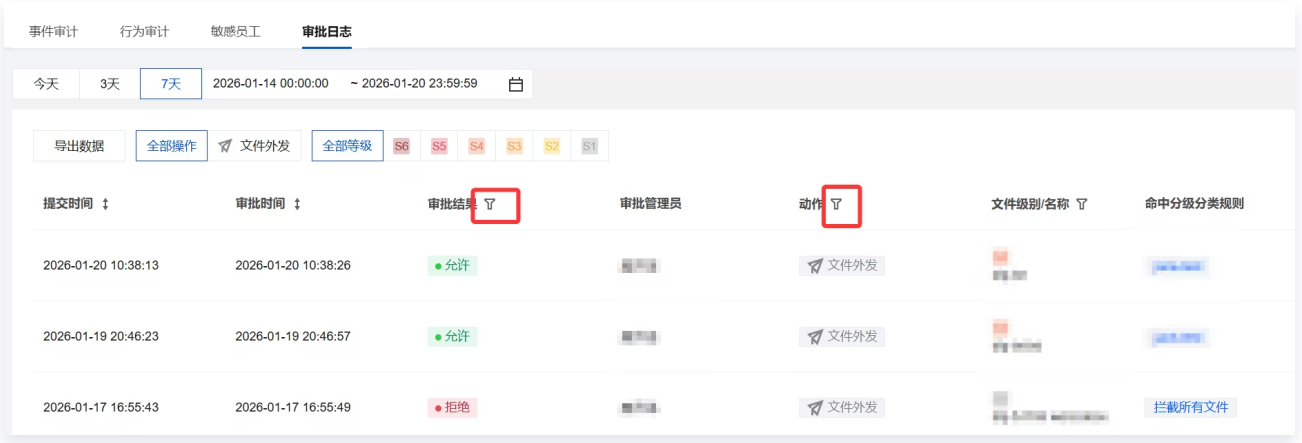
3. 审批日志页面，展示过去一段时间的审批数据。
   - 支持时间段选择：今天、3天、7天以及自由选择时间查询。



   - 支持通过拦截规则、文件名称等关键字，以及用户姓名/账号等过滤标签查询。



   - 单击  ，自定义筛选审批结果、动作等。



   - 单击**作废**，用户可重新提交相同 MD5文件进行审批。



数据地图（11.1.1版）

数据地图（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

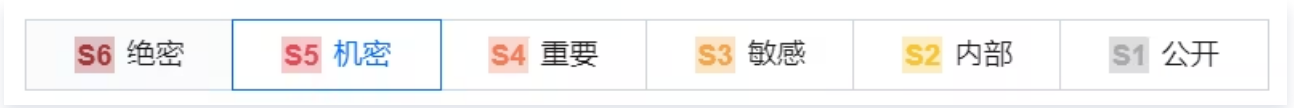
通过数据地图对终端敏感文件进行采集与管控。

- 敏感数据采集：支持扫描全网终端文件，并根据分级分类规则对敏感文件进行采集上报。
- 敏感数据管控：支持对已采集敏感文件进行检索、导出、提取、远程删除等操作。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据地图** > **数据地图**。
2. 在数据地图页面，展示敏感数据趋势图以及过去一段时间的敏感文件、人员、设备数据。
   - 支持时间段选择：今天、近7天、近30天以及自由选择时间查询。
   - 支持文件类型、规则分类查询。



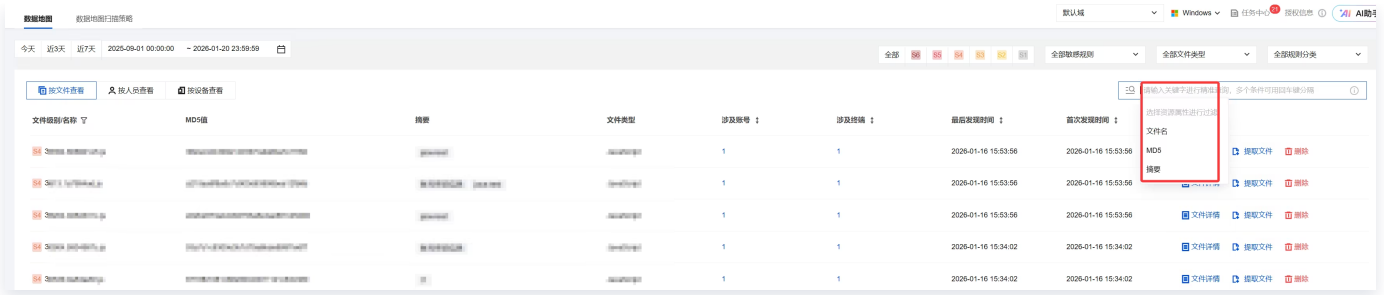
   - 支持按敏感程度分级，分为S6、S5、S4、S3、S2、S1，并分别展示目前外发数据中各敏感等级下数据数量。



3. 在数据地图列表中，支持按 文件 、按人员 、设备 查看敏感信息。

按文件查看

1. 在文件列表中，支持按文件名称、MD5、摘要进行搜索。



2. 在文件列表中，单击对应的“涉及账号数”和“涉及终端数”，支持查看文件涉及账号/终端。



3. 在文件列表中，单击**文件详情**，支持查看对应的文件名称、风险等级、类型等。



4. 在文件列表中，单击**提取文件 > 提取**，提取成功后该文件支持下载。



按人员查看

1. 在人员列表中，展示员工的相关文件信息，并支持通过账号、姓名、所在部门、终端名称进行搜索。



2. 在人员列表中，单击“涉及文件数”，可以查看文件级别、摘要、类型、最后发现时间、首次发现时间等信息。



按设备查看

1. 在设备列表中，展示设备的相关文件信息，并支持通过账号、姓名、所在部门、终端名称进行搜索。



2. 在设备列表中，单击“涉及文件数”，可以查看文件级别、摘要、类型、最后发现时间、首次发现时间等信息。



数据地图扫描策略（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

通过数据地图扫描展示终端本地敏感文件分布，完善企业数据安全防泄漏事前防护环节。

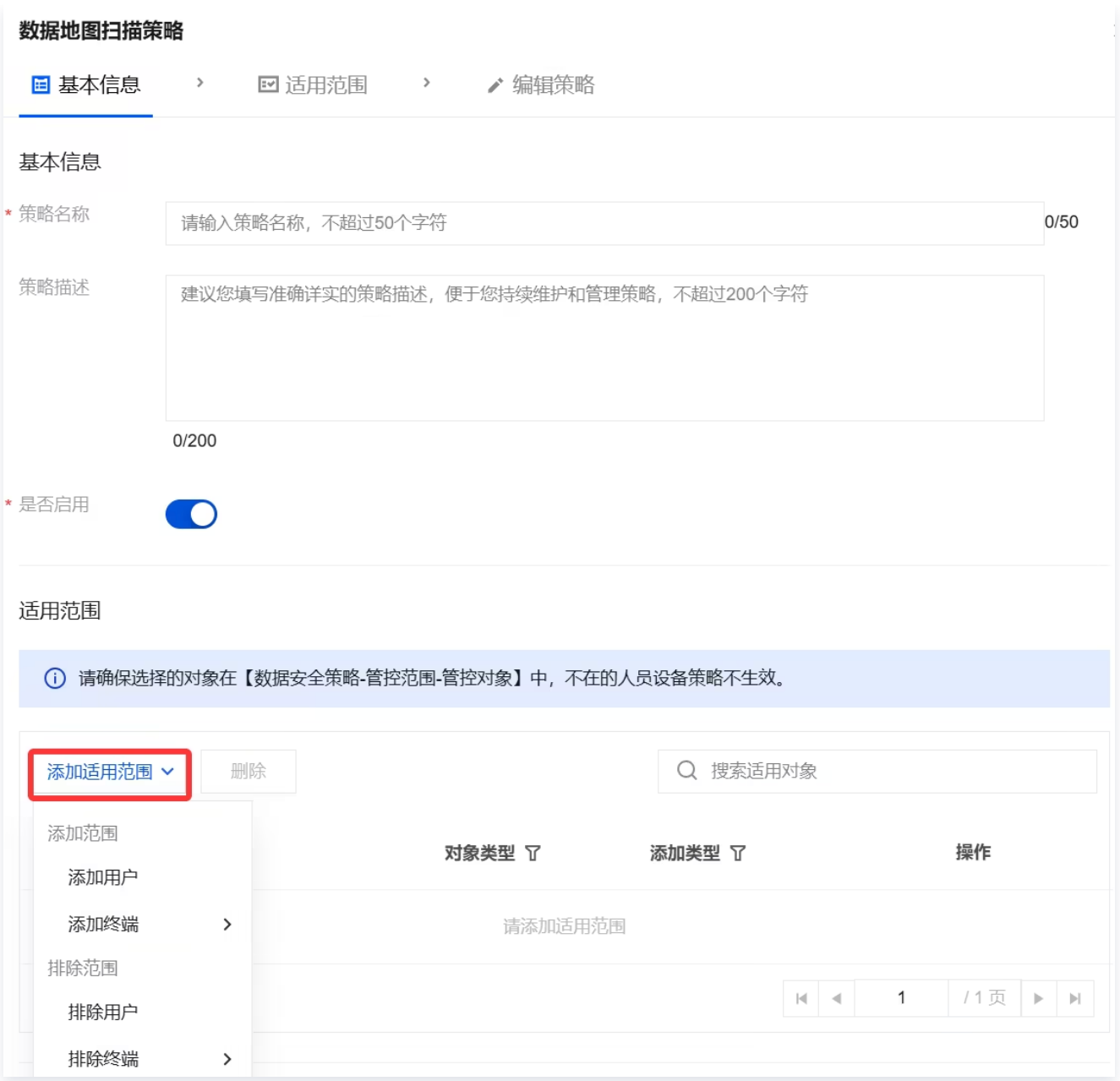
> **说明：**
> macOS 设备扫描功能系统版本需大于 10.15.7 且开启“完全磁盘访问”权限。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据地图** > **数据地图扫描策略**，单击**新建策略**。



2. 在数据地图扫描策略页面，配置相关参数，单击**保存**。

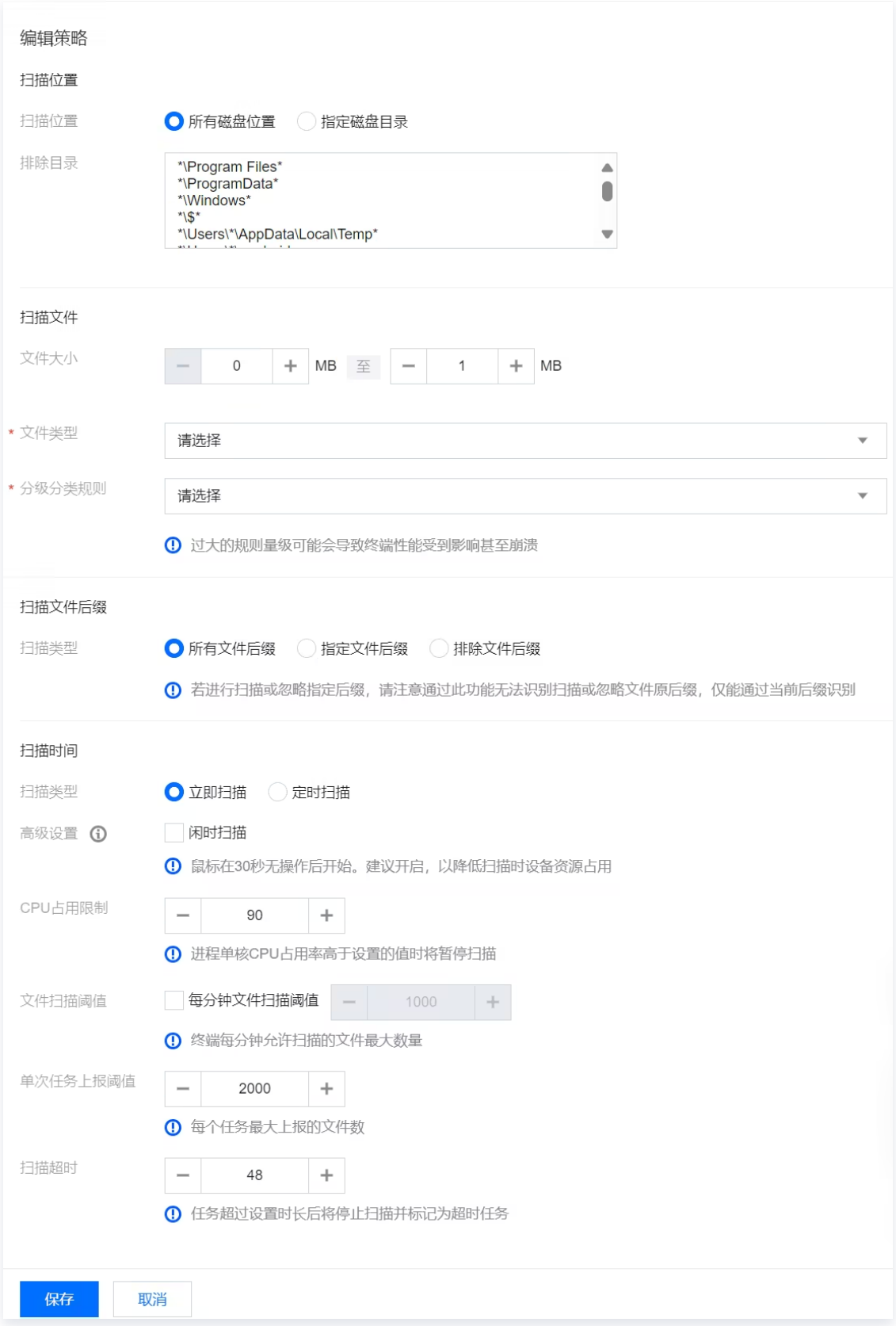
   2.1 编辑基本信息、添加适用范围。



参数名称		说明
策略名称		自定义，不超过50个字符。
是否启用		选择**开启**。
适用范围	添加用户	支持按组织架构、自定义分组选择用户。
	添加终端	系统自动分类 Windows/macOS，单击**添加 Windows/macOS 终端**。
	排除用户	支持从适用范围内排除例外用户，例外用户即使命中条件也会被排除出该范围。

	排除终端	支持从适用范围内排除例外终端，例外终端即使命中条件也会被排除出该范围。

2.2 在编辑策略中，根据如下参数，配置数据地图扫描策略。



参数名称		说明
扫描位置	所有磁盘位置	当前终端所有的目录。
	指定磁盘目录	系统默认提供不同操作系统的系统目录。用户可自定义添加指定目录/排除目录。
	指定目录	除了用户指定的这些目录以外，其他的目录都不会扫描。
	排除目录	排除的目录不会扫描，其他的目录都会扫描。
扫描文件	文件大小	在设置的范围内的文件会被扫描，小于或大于该配置范围的文件都不会被扫描。
	文件类型	关联 文档类型库 。
	分级分类规则	关联 分级分类规则 。
扫描文件后缀	所有文件后缀	扫描所有文件的当前后缀。
	指定文件后缀	指定文件后缀进行扫描。
	排除文件后缀	不扫描指定的文件后缀。
扫描时间	立即扫描	策略配置完成终端拉取策略后立即扫描电脑磁盘。
	定时扫描	定时扫描配置扫描频率为每天/每周/每月。
	闲时扫描	鼠标在30秒无操作后开始。建议开启，以降低扫描时设备资源占用。
扫描类型	CPU 占用限制	进程单核 CPU 占用率高于设置的值时将暂停扫描。
	文件扫描阈值	终端每分钟允许扫描的文件最大数量。
	单次任务上报阈值	每个任务最大上报的文件数。
	扫描超时	任务超过设置时长后将停止扫描并标记为超时任务。

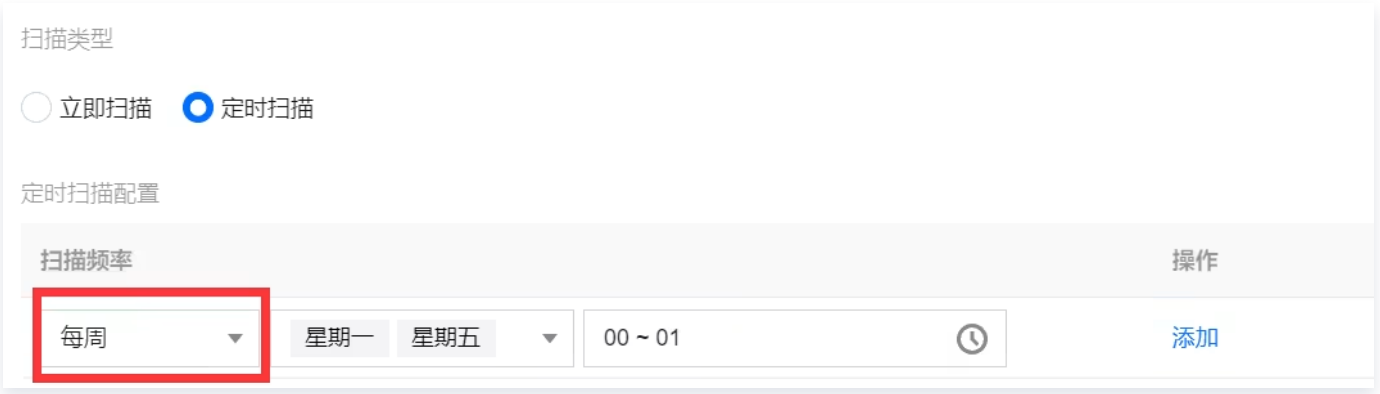
3. 查看扫描详情，单击已执行扫描列中的**蓝色数字**。



4. 在已执行扫描页面，可查看任务执行时间对应的扫描类型（立即扫描、定时扫描或闲时扫描）。



5. **单击终止，停止该策略本次扫描任务，如配置了周期策略，则下次进入周期时间自动执行下一个任务，周期任务示例：**



6. **扫描完成可在 数据地图中 查看扫描文件详情，命中风险等级、敏感规则的文件将实时上报至控制台。**

管控策略（11.1.1版）

管控策略（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **管控策略**，单击**新建策略**。



2. 支持配置拦截策略（用户的敏感文件外发行为将会被“拦截”，同时后台会产生一条告警）与审计策略（用户的敏感文件外发行为将会被“放行”，后台会产生一条告警）、支持配置自定义通道与拦截超时设置。

拦截策略

1. 在管控策略页面单击**新建策略**，选择**拦截策略**，配置拦截策略后，当管控对象触发规则时，系统将直接拦截文件的外发。同时，在客户端上会弹窗提示员工，并将该记录上报至 iOA，帮助管理员实时监控和阻止潜在数据泄漏风险。



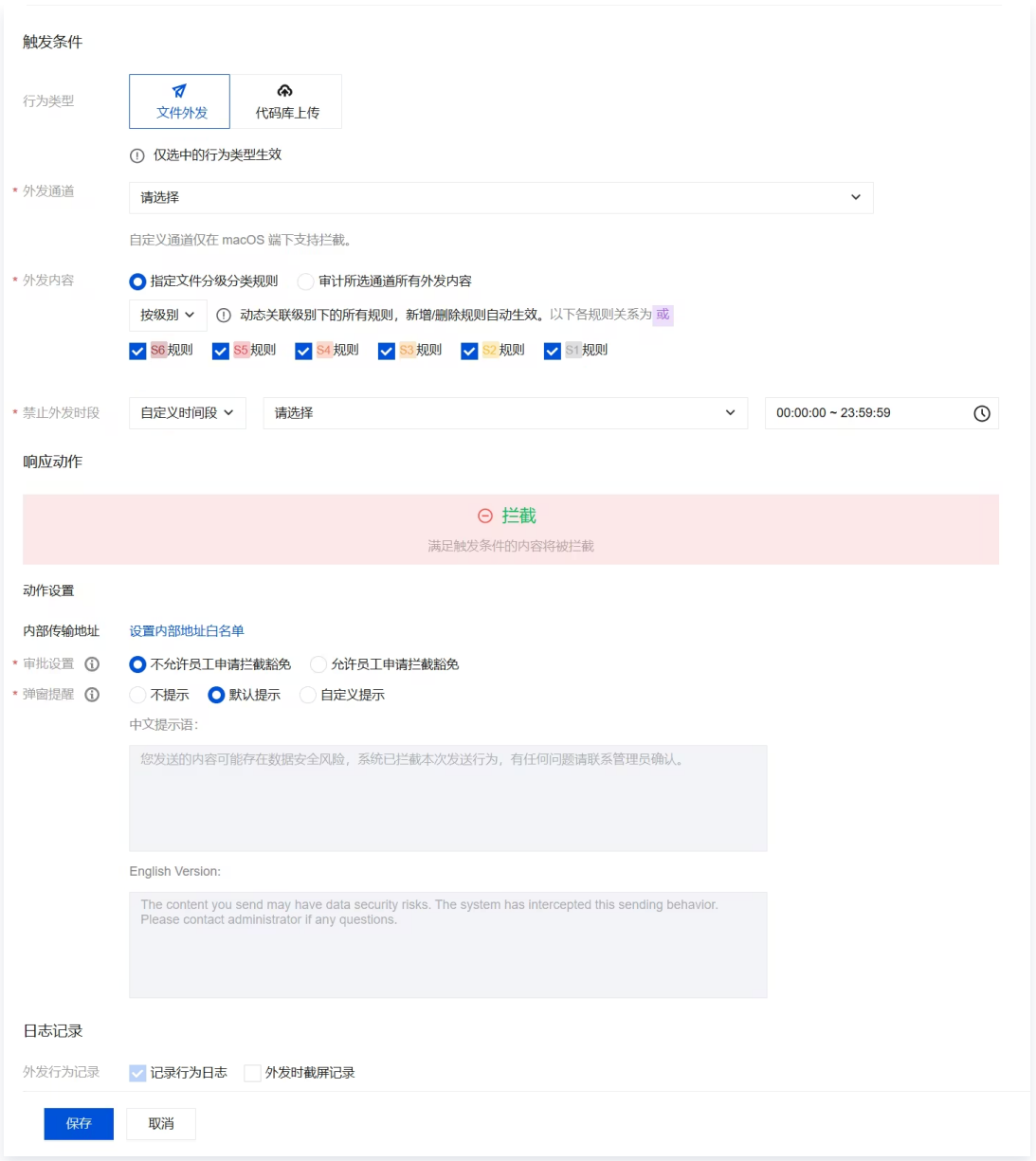
2. 在新建拦截策略页面，配置相关参数。

2.1 输入策略名称，并输入策略描述等参数。



2.2 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。

2.3 选择拦截行为类型，配置拦截策略的相关参数。



参数名称	说明
行为类型	需要拦截的操作类型； • 文件外发：拦截文件外发行为。 • 代码库上传：拦截代码库上传行为。
外发通道	需要拦截的外发通道。
外发内容	需要拦截的发送内容： • 指定文件分级分类规则：选择已定义的分级分类规则作为触发拦截的敏感内容。 ○ 按级别：管控所选级别下的所有分级分类规则（所选级别下的规则都会被管控），示例：在**数据分级分类** > **分级分类规则**中新建一个S4的规则，此处的按级别会动态关联级别下的所有规则，新增/删除规则自动生效（新建的S4规则也会被管控）

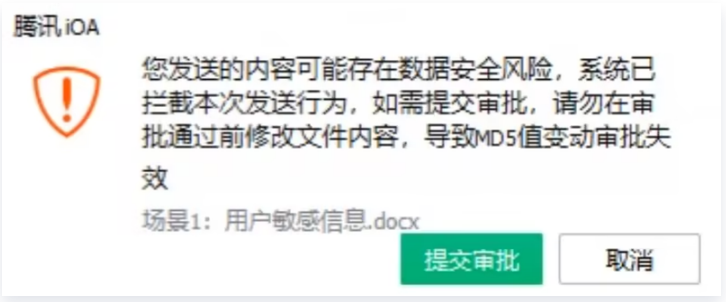


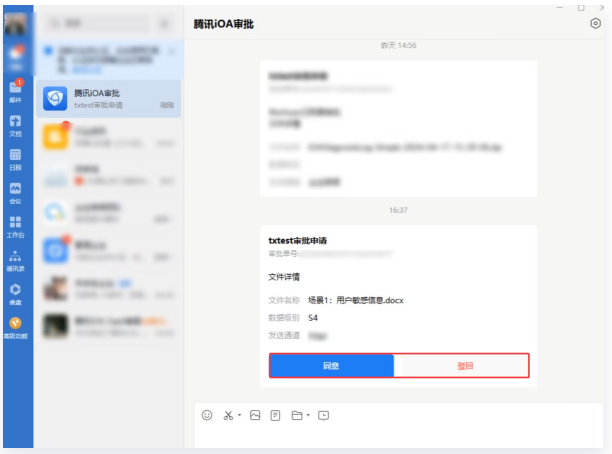
- 按规则：管控所选级别下的规则（例如：当选择S4中的规则，将S4中的规则一个个勾选，勾选完后并不是展示S4的标签，而是将规则展示出来）示例：在**数据分级分类** > **分级分类规则** 中新建一个S4的规则，此处的按规则不会将新建的S4的规则罗列进来，只会管控已选择的规则。

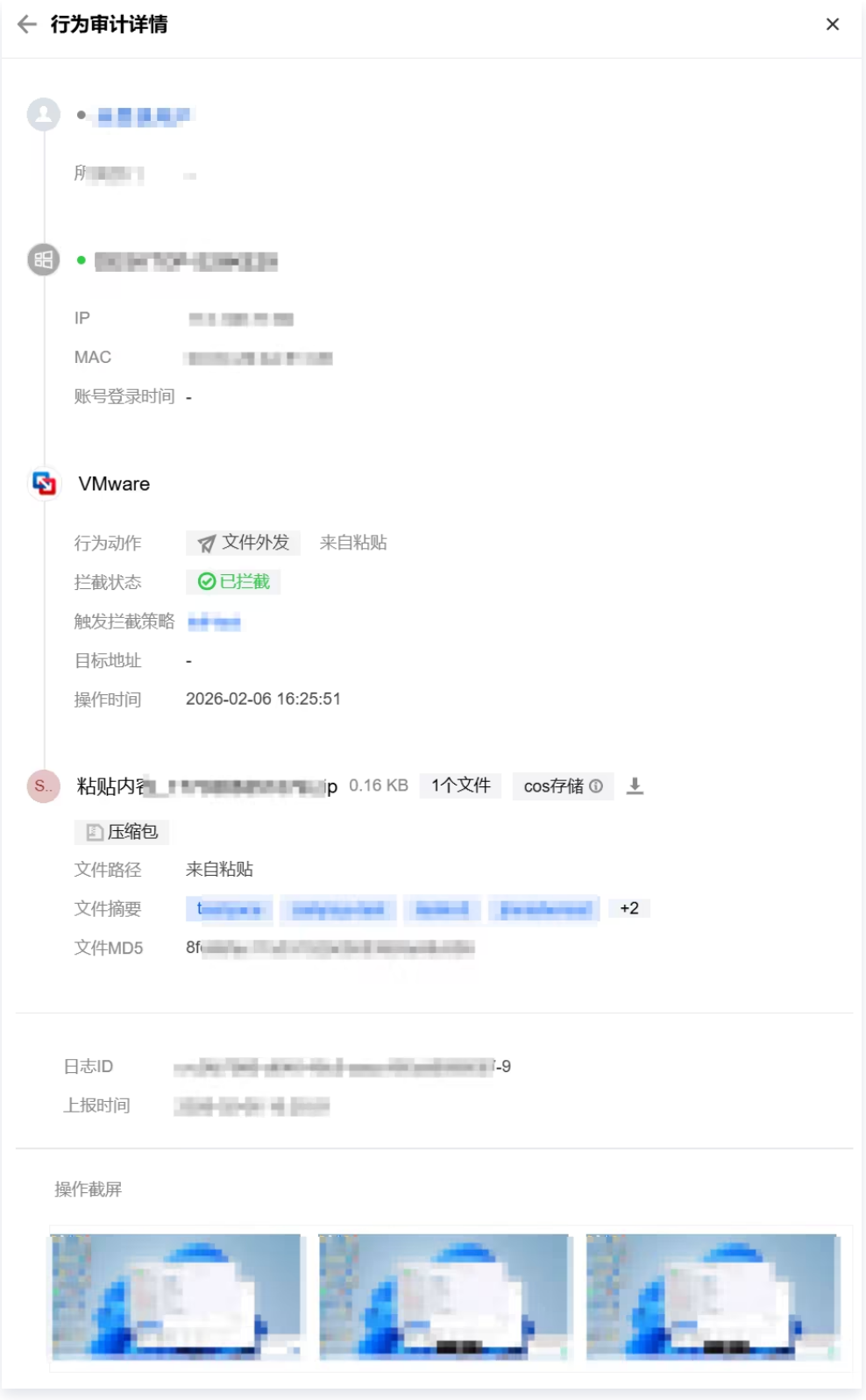


- 审计所选通道所有外发内容：在外发通道中配置的通道，都将被拦截。示例：配置电子邮箱，则电子邮箱通道相关文件外发都会被拦截。



禁止外发时段	需要拦截的发送时间。支持自定义时间段和非工作时间。
内部传输地址	单击**设置内部地址白名单**，页面跳转至**管控策略** > **内部地址** 页面，请参见 内部地址 文档。
审批设置	• 不允许员工申请拦截豁免：外发直接拦截，员工无法申请豁免。 • 允许员工申请拦截豁免：添加对应的 审批流，当员工外发被拦截时，iOA弹窗提醒（弹窗提醒支持自定义），弹窗示例：  • 当员工提交审批时，审批流上的管理员可单击**同意/驳回**审批。示例：企业微信审批。

	
弹窗提醒	自定义拦截时的弹窗提醒内容。
日志记录	• 记录行为日志：默认勾选，且不可取消。可在**风险调查** > **行为审计** 查看触发规则的日志信息。 • 外发时截屏记录：勾选后，留存敏感数据外发时的截图，用于事后的溯源审计。可在**风险调查** > **行为审计**，单击**详情**查看触发规则的截屏信息。



3. 填写完成后，单击**保存**，拦截策略创建完成。

审计策略

1. 在管控策略页面单击**新建策略**，选择**审计策略**，支持对敏感文件外发行为进行审计，审计日志在**风险调查** > **行为审计**中体现。



2. 在新建审计策略页面，配置相关参数。

2.1 输入策略名称，并输入策略描述等参数。



2.2 单击**添加适用范围**，勾选需管控/排除的用户/终端名称，单击**确定**。

2.3 配置触发条件、日志记录等信息。



参数名称	说明
外发通道	需要审计的外发通道。
外发内容	需要审计的发送内容： • 指定文件分级分类规则：选择已定义的分级分类规则作为触发审计的敏感内容。 ○ 按级别：管控所选级别下的所有分级分类规则（所选级别下的规则都会被管控），示例：在**数据分级分类** > **分级分类规则** 中新建一个S4的规则，此处的按级别会动态关联级别下的所有规则，新增/删除规则自动生效（新建的S4规则也会被管控）  ○ 按规则：管控所选级别下的规则（例如：当选择S4中的规则，将S4中的规则一个个勾选，勾选完后并不是展示S4的标签，而是将规则展示出来）示例：在**数据分级分类** > **分级分类规则** 中新建一个S4的规则，此处的按规则不会将新建的S4的规则罗列进来，只会管控已选择的规则。

<table>
<tr><td></td><td>

审计所选通道所有外发内容：在外发通道中配置的通道，都将被审计。示例：配置电子邮箱，则电子邮箱通道相关文件外发都会被审计。

</td></tr>
<tr><td>审计记录时段</td><td>需要审计的发送时间。支持自定义时间段和非工作时间。</td></tr>
<tr><td>内部传输地址</td><td>单击设置内部地址白名单，页面跳转至管控策略 > 内部地址 页面，请参见 内部地址 文档。</td></tr>
<tr><td>日志记录</td><td>记录行为日志：默认勾选，且不可取消。可在风险调查 > 行为审计 查看触发规则的日志信息。
外发时截屏记录：勾选后，留存敏感数据外发时的截图，用于事后的溯源审计。可在风险调查 > 行为审计，单击详情查看触发规则的截屏信息。</td></tr>
</table>



3. 填写完成后，单击**保存**，审计策略创建完成。

自定义通道

iOA 零信任管理平台提供自定义管控通道来扩大通道覆盖面，您可以按照以下步骤添加自定义通道信息。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **管控策略**，单击**自定义通道**。



2. 单击**添加自定义通道**，在添加自定义通道页面，输入自定义通道的基本信息，具体内容如下：



参数名称	说明
通道名称	自定义管控通道的名称。
通道类型	选择该管控通道的类别。
通道图标	上传36x36像素至150x150像素大小的正方形通道图标，图片宽高比例为1：1，支持PNG、JPG 格式。
是否启用	默认开启。

Windows

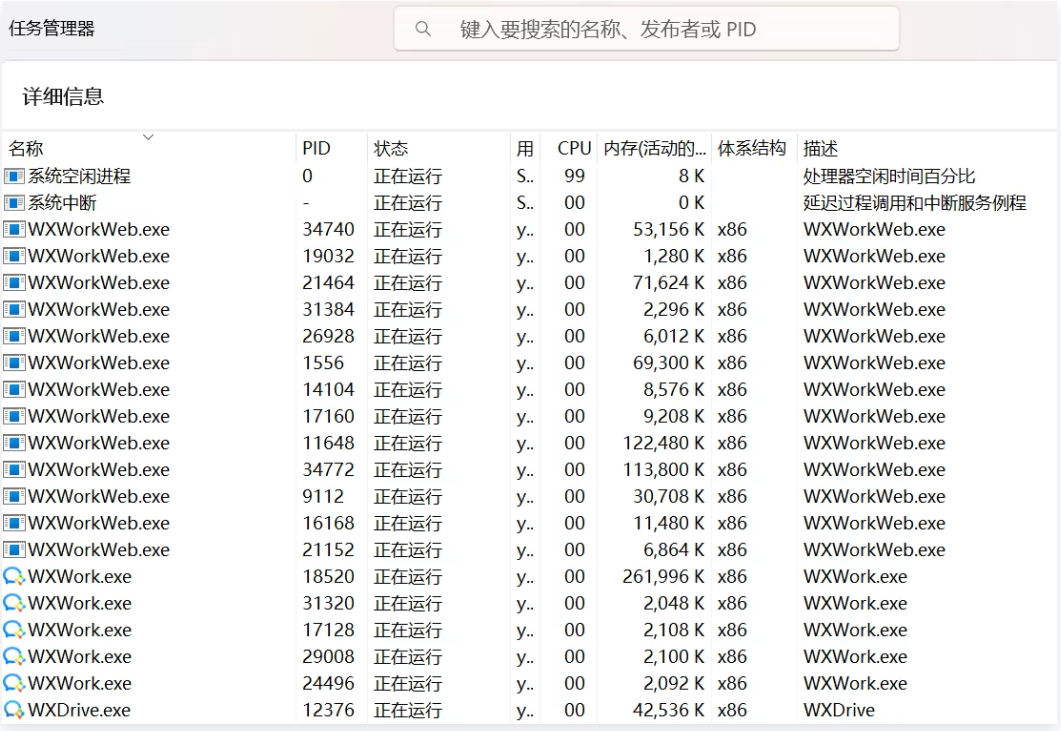
1. 配置该通道在 Windows 环境下的进程信息，具体包括通道进程名和文件路径白名单。



参数名称	说明
通道进程名	必选，可输入多个进程名，利用换行符分隔，每一行表示一个进程名。
文件路径白名单	文件路径白名单：必选，可用于加白不需要管控的系统文件、应用配置文件路径，支持正则匹配；可输入多个白名单路径，使用换行符分隔，一行表示一个文件路径。例如，需要加白 `C:\Windows` 路径下的所有文件，可配置为 `C:\\Windows\\.*` 。

进程名获取方法如下：

菜单栏右键打开任务管理器，单击详细信息。找到需要检测的进程，第一列的名称即为所需通道进程名。



名称	PID	状态	用	CPU	内存(活动的...	体系结构	描述
系统空闲进程	0	正在运行	S..	99	8 K		处理器空闲时间百分比
系统中断	-	正在运行	S..	00	0 K		延迟过程调用和中断服务例程
WXWorkWeb.exe	34740	正在运行	y..	00	53,156 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	19032	正在运行	y..	00	1,280 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	21464	正在运行	y..	00	71,624 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	31384	正在运行	y..	00	2,296 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	26928	正在运行	y..	00	6,012 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	1556	正在运行	y..	00	69,300 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	14104	正在运行	y..	00	8,576 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	17160	正在运行	y..	00	9,208 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	11648	正在运行	y..	00	122,480 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	34772	正在运行	y..	00	113,800 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	9112	正在运行	y..	00	30,708 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	16168	正在运行	y..	00	11,480 K	x86	WXWorkWeb.exe
WXWorkWeb.exe	21152	正在运行	y..	00	6,864 K	x86	WXWorkWeb.exe
WXWork.exe	18520	正在运行	y..	00	261,996 K	x86	WXWork.exe
WXWork.exe	31320	正在运行	y..	00	2,048 K	x86	WXWork.exe
WXWork.exe	17128	正在运行	y..	00	2,108 K	x86	WXWork.exe
WXWork.exe	29008	正在运行	y..	00	2,100 K	x86	WXWork.exe
WXWork.exe	24496	正在运行	y..	00	2,092 K	x86	WXWork.exe
WXDrive.exe	12376	正在运行	y..	00	42,536 K	x86	WXDrive

macOS

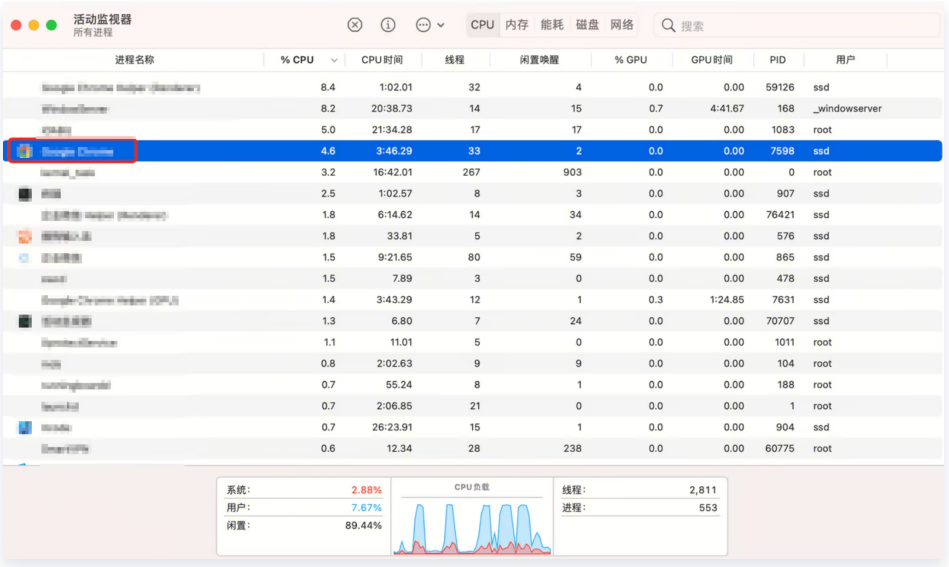
1. 配置该通道在 macOS 环境下的进程信息，具体包括通道进程名和 Bundle ID。



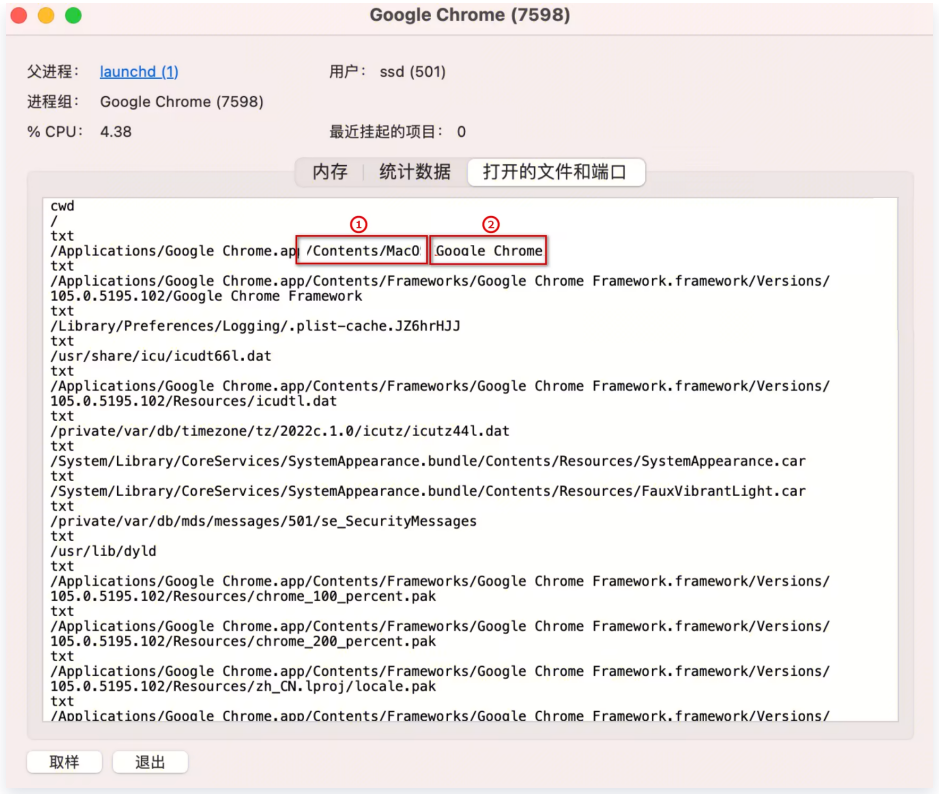
具体获取方法如下：

1.1 获取通道进程名

1.1.1 打开活动监控器（Activity Monitor），找到应用进程信息，双击**打开进程的详细信息**。



1.1.2 单击**打开的文件和端口**，找到①处包含 `/Contents/MacOS/` 的字符串，后面的②内容即为所需进程名。



1.2 获取 Bundle ID

打开终端命令行（Terminal），在终端命令行中执行：`defaults read 安装的软件路径/Contents/Info CFBundleIdentifier`，回显即为软件的 Bundle ID。

例如：软件一般安装在 `/Applications/` 目录下，例如需要查看微信（Wechat.app），则微信的路径为 /Applications/Wechat.app，即执行命令 `defaults read /Applications/Wechat.app/Contents/Info CFBundleIdentifier`，如下图，得到 Bundle ID：`com.tencent.xinWeChat`。



2. 配置完上述参数后，单击**确定**保存。

拦截超时

> **说明：**
> 拦截超时设置功能要求客户端版本10.10.1及以上支持该功能，如客户端版本低于10.10.1请升级客户端。

拦截超时设置页面用于配置系统在敏感文件识别过程中，出现超时的处理策略，属于全局兜底策略；系统将根据配置通道的对应响应动作进行放行或拦截。平衡安全性与用户体验。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **管控策略**，单击**拦截超时**。



2. 在拦截超时设置页面中，配置超时时间以及审批设置等参数。

拦截超时设置

1、拦截时将进行敏感文件识别，并且可导致软件卡顿，为保证使用体验，您可以配置超时时间和超时后的处理动作

2、超时放行：识别超时后，直接不拦截； 超时拦截：识别超时后，直接拦截

3、截屏取证功能也会受影响，识别超时后才截屏，可能会导致截屏时机不精准

通道超时时间 − 5 + 秒

剪贴板超时 − 600 + 毫秒

剪贴板对检测的卡顿体验较为明显，超时后将默认放行，建议配置400-600毫秒

通道超时处理

全部放行 全部拦截

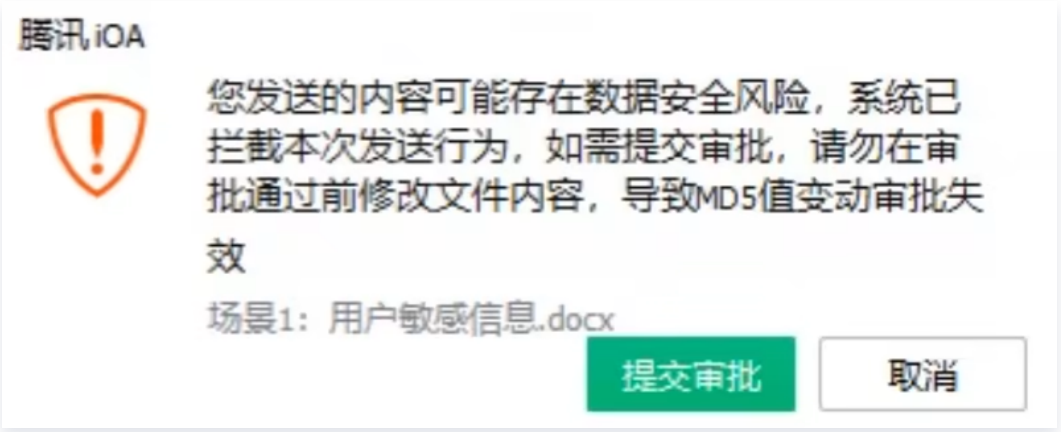
	通道名称	通道类型	超时处理	
	[redacted]	[redacted]	超时放行	超时拦截
	[redacted]	[redacted]	超时放行	超时拦截
	[redacted]	[redacted]	超时放行	超时拦截
	[redacted]	[redacted]	超时放行	超时拦截
	[redacted]	[redacted]	超时放行	超时拦截
	[redacted]	[redacted]	超时放行	超时拦截
	[redacted]	[redacted]	超时放行	超时拦截
	[redacted]	[redacted]	超时放行	超时拦截
	[redacted]	[redacted]	超时放行	超时拦截
	[redacted]	[redacted]	超时放行	超时拦截

版权所有：腾讯云计算（北京）有限责任公司



参数名称	说明
通道超时时间	定义各通道进行敏感文件识别的最大等待时间。
剪贴板超时	设置剪贴板内容识别的专用超时阈值。
通道超时处理	勾选通道，启用该通道的超时检测功能，为每个通道单独设置超时后的处理动作（放行/拦截）。 • 超时放行：当识别超时后，系统将直接放行文件而不拦截。 • 超时拦截：当识别超时后，系统将直接拦截文件。
审批设置	控制是否允许员工提交拦截豁免申请，若允许员工申请拦截豁免，则设置豁免申请的 审批流程 。

3. 弹窗提醒：允许管理员定制专属的拦截提醒内容。



4. 配置完成后单击**确定**保存，完成拦截超时设置。

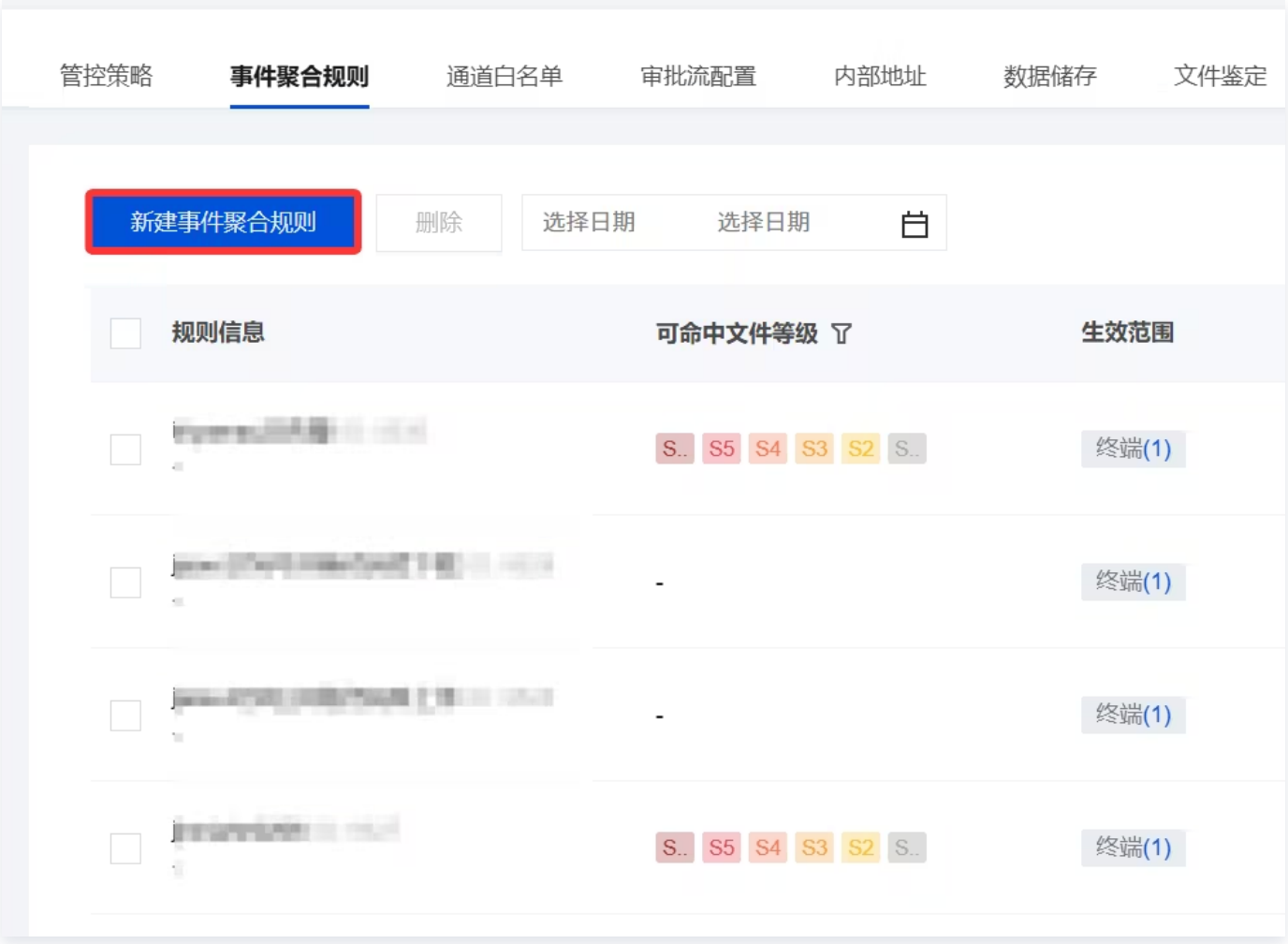
事件聚合规则（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

配置事件聚合规则，对用户的敏感文件外发行为进行聚合形成安全告警，日志在**风险调查** > **事件审计** 中体现。当管控对象触发其规则时，将上报 iOA 平台，帮助管理员实时监控和识别潜在数据泄漏风险。产品内置多个告警策略模板，您可以通过现有的模板快速创建自定义规则。

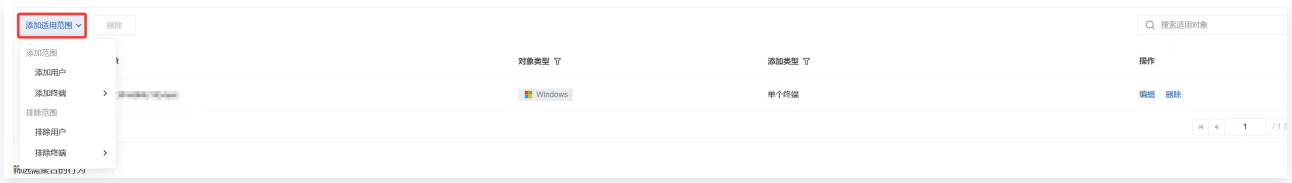
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **事件聚合规则**。
1. 在 事件聚合规则 页，单击**新建事件聚合规则**。



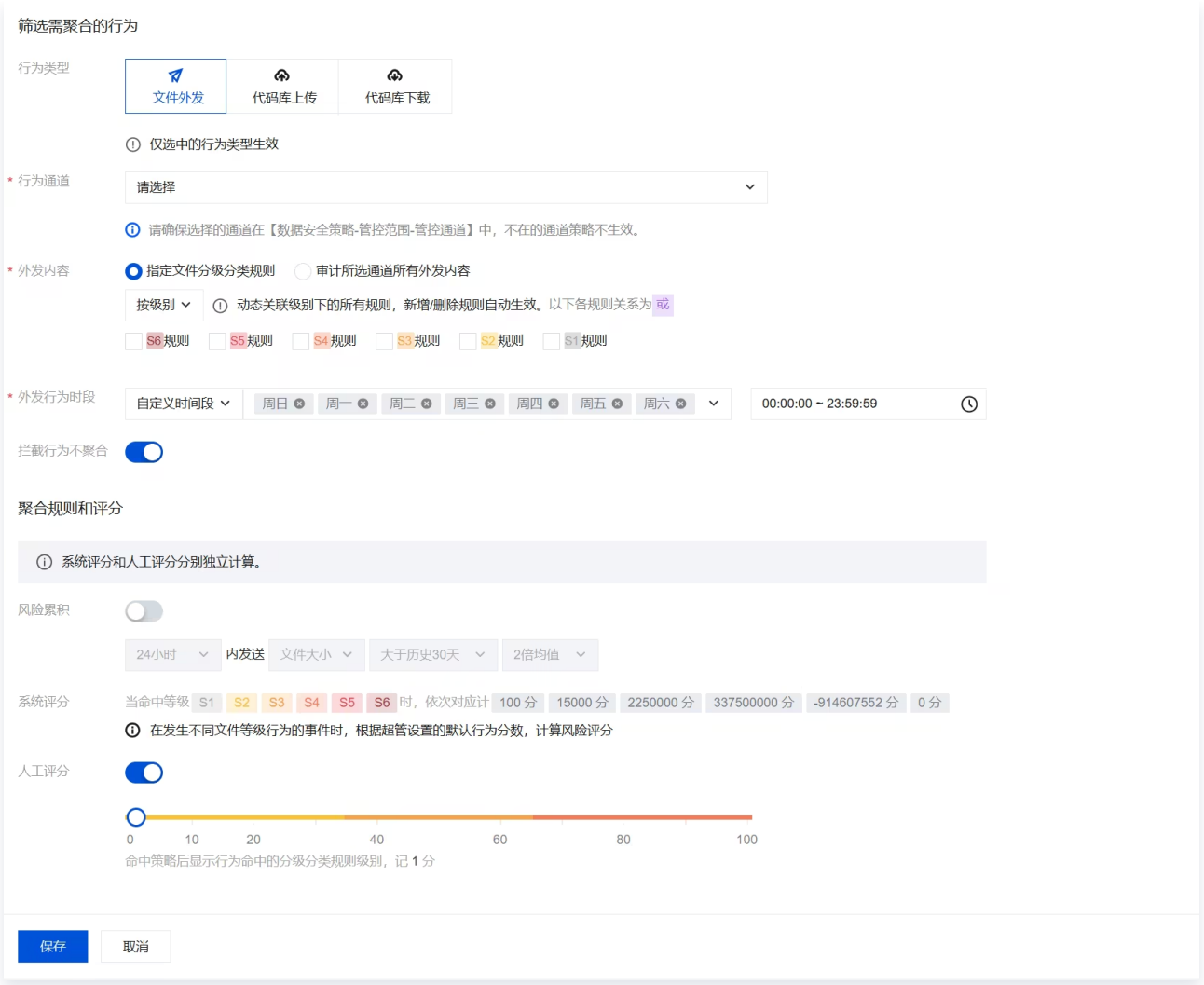
2. 在新建事件聚合规则页填写基本信息、适用范围和编辑策略。
   - 基本信息：输入策略名称、策略描述，并选择是否启用。

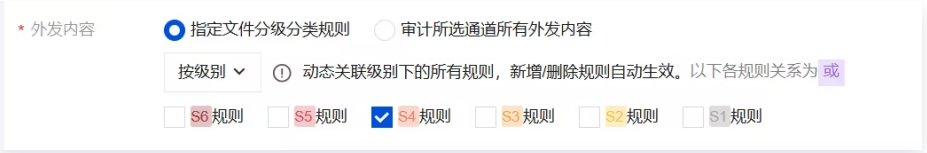


- **适用范围：该策略生效的对象范围。单击添加适用范围，勾选需管控/排除的用户/终端，单击确定。**



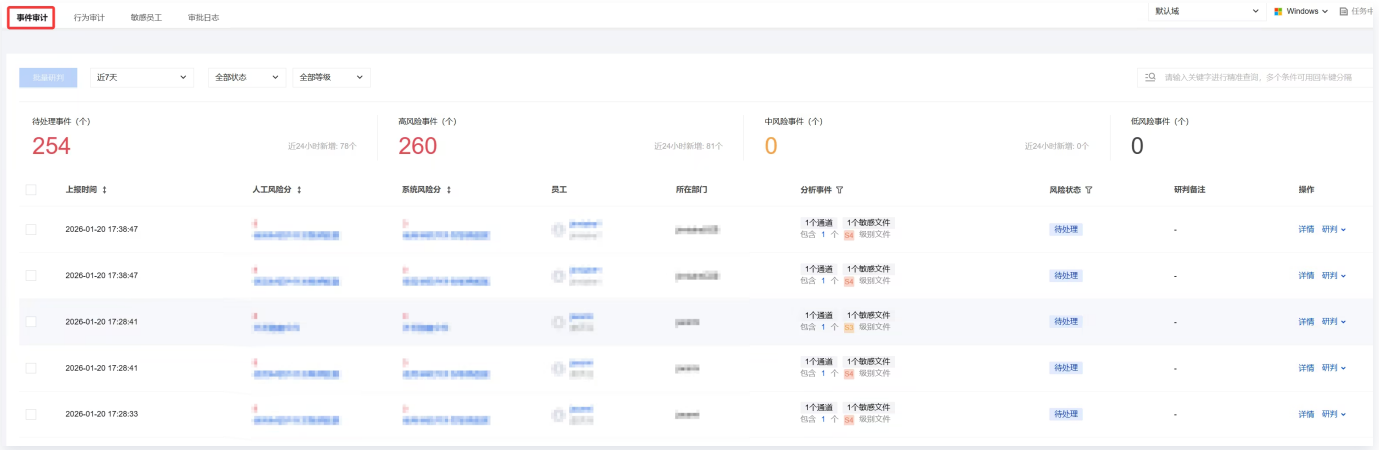
- **编辑策略：配置聚合的行为、规则和评分等参数。**



参数名称	说明
行为类型	需要告警的操作类型（文件外发/代码库上传/代码库下载）
行为通道	需要告警的外发通道。
外发内容	需要告警的发送内容： • 指定文件分级分类规则：选择已定义的分级分类规则作为触发审计的敏感内容。 ○ 按级别：管控所选级别下的所有分级分类规则（所选级别下的规则都会被管控），示例：在**数据分级分类** > **分级分类规则** 中新建一个 S4 的规则，此处的按级别会动态关联级别下的所有规则，新增/删除规则自动生效（新建的 S4 规则也会被管控）  ○ 按规则：管控所选级别下的规则（例如：当选择 S4 中的规则，将 S4 中的规则一个个勾选，勾选完后并不是展示 S4 的标签，而是将规则展示出来）

	示例：在**数据分级分类** > **分级分类规则** 中新建一个 S4 的规则，此处的按规则不会将新建的 S4 的规则罗列进来，只会管控已选择的规则。  • **审计所选通道所有外发内容**：在外发通道中配置的通道，都将被审计。示例：配置电子邮箱，则电子邮箱通道相关文件外发都会被审计。 
外发行为时段	需要告警的发送时间。支持自定义时间段和非工作时间。
拦截行为不聚合	• 控制拦截行为是否聚合进入 **事件审计** ，开启**拦截行为不聚合**，对于已经拦截的行为，不将其聚合至 **事件审计** 中。 • 开启**拦截行为不聚合**的作用：对于已拦截的行为，iOA 已阻断了风险发生，则不聚合进入事件审计，减少安全运营人员审计量。
风险累积	累计发送文件大小超过指定大小或文件数量超过指定数量就告警。
系统评分	该评分关联数据**分级分类** > **数据分级与评分** 里的评分。
人工评分	单击 开启人工评分，命中该策略后显示行为命中的分级分类规则级别，记 X 分。

3. 填写完成后，单击**保存**，即可生效。
4. 配置的事件聚合规则，当用户的敏感文件外发行为聚合形成安全告警后，可前往**风险调查** > **事件审计** 查看。



版权所有：腾讯云计算（北京）有限责任公司

通道白名单（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

iOA 零信任管理平台支持添加通道白名单，添加后，将根据配置的生效范围加白通道的审计或拦截。适用于内部地址加白不审计、内部地址仅审计不拦截、内部地址不审计不拦截等场景。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略**>**通道白名单**，单击**新建策略**。



2. 配置通道白名单策略

2.1 基本信息



参数名称	说明
策略名称	自定义名称，支持1-50字符。
策略描述	自定义策略描述，支持1-288字符。
是否启用	默认开启。

2.2 适用范围：单击**添加适用范围**，您可以通过添加或排除用户、组织架构、自定义分组和终端，来进行精细化的管控范围设置。



2.3 单击**添加白名单**，配置相关参数，单击**确定并保存**即可生效。

> **说明：**
> 添加到通道白名单后，将根据配置的生效范围加白。例如：配置“拦截加白”时，则不进行拦截，仍审计。



参数名称	说明
选择通道	选择需要加白的管控通道。
制订条件	填写加白的具体条件，当选择的通道为**浏览器或任意浏览器通道**时，制订条件中可选择 URL（用户可放通具体网址外发行为**审计/拦截**），帮助企业灵活配置内外部访问地址下的外发审计与拦截。 • 包含任一：只要文件路径或地址包含任意一条内容就加白，多条内容用换行符分隔，如填写"test11 \n test22"，则文件路径或请求地址中包含test11或test22就会被加白。 • 不包含：仅管控填写范围的地址，如填写"test11 \n test22"，则仅当外发文件路径或请求地址中包含test11或test22的才会被审计、拦截。 • 正则匹配：支持以正则表达式针对文件路径或地址加白，如填写".*\\WeChat\\.*\.db"，则 WeChat 目录下的所有 db 文件都被加白，不会被审计、拦截。
加白设置	• 选择审计加白，即仅拦截不审计。 • 选择拦截加白，即仅审计不拦截。

2.4 配置完成，单击**保存**。通道白名单适用于内部地址加白不审计、内部地址仅审计不拦截、内部地址不审计不拦截等场景。

审批流配置（11.1.1版）
概述（11.1.1版）

最近更新时间：2026-02-06 14:23:31

将第三方审批应用接入 iOA，通过消息推送功能发送审批文件的详情（如文件名称、管控通道、敏感级别等），实现管理员对外发送文件的快速审批。

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

当前支持应用如下：

- **企业微信**
- **钉钉**
- **飞书**

企业微信（11.1.1版）

最近更新时间：2026-02-06 14:23:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **审批流配置**。
2. 在审批流配置页面，单击**添加审批流**。



3. 在添加审批流页面，选择**企业微信**，输入流程名称，示例：**企微审批配置测试**，选择**审批管理员**。

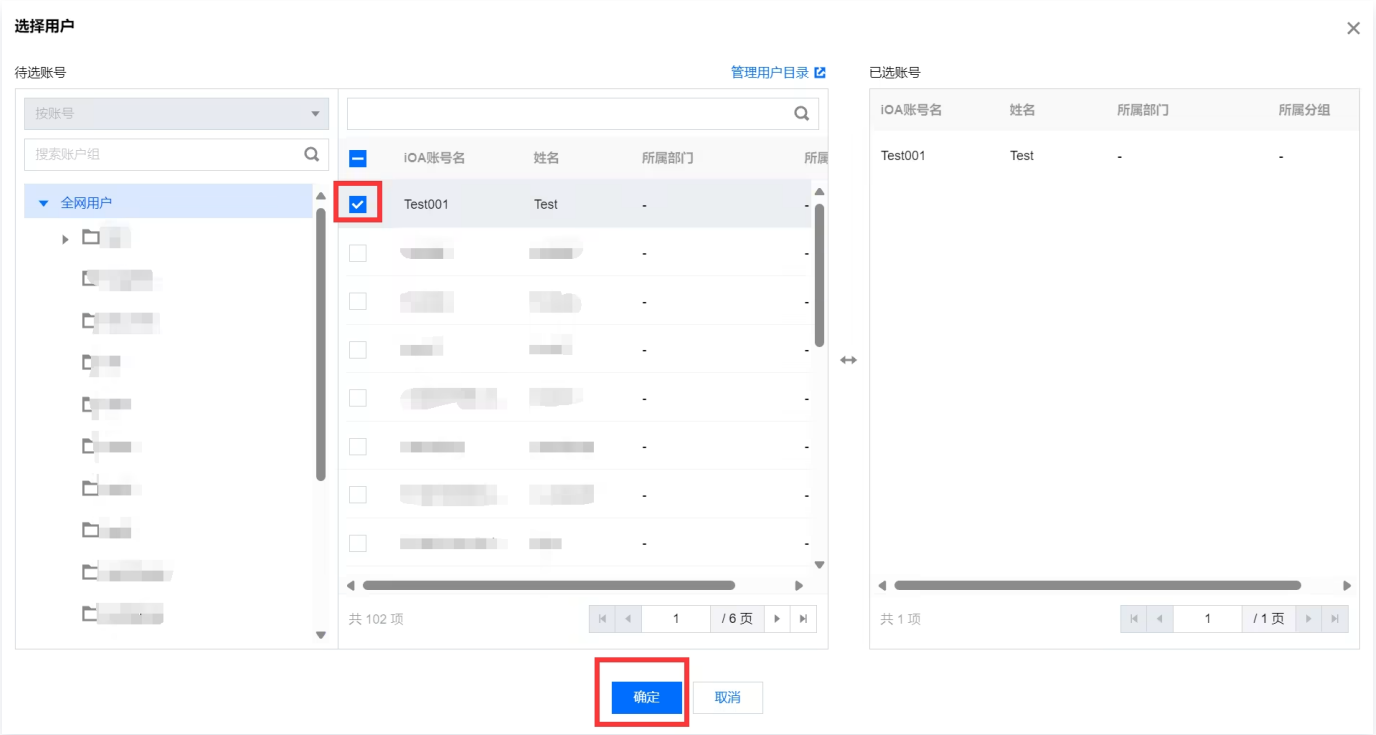


参数名称		说明
审批管理员	直属 leader	自动将审批信息发送至企微中对应的 leader，此选项无法在配置页面进行测试，请在配置完成后，在对应终端上登录并进行审批测试。

	指定用户	选择组织架构中的单个或多个用户，对应用户名需要与企微中的一致，请确保在收到审批测试信息后进行保存。 • 勾选单个用户：仅1个用户审批。 • 勾选多个用户：选中的多个用户都会收到审批消息，多个用户收到的审批消息中以第1个决策的为准，例如01用户号第一个看到审批消息并审批通过，则以01用户的审批结果为准。
	自定义	填写对应审批管理员的企微用户名，请确保在收到审批测试信息后进行保存。
备用管理员		选择直属 leader 审批，必填备用管理员，当直属 leader 字段为空时，审批信息将发送给备用审批员。

4. 审批测试发起人：单击**选择发起人**，单击**确定**保存。

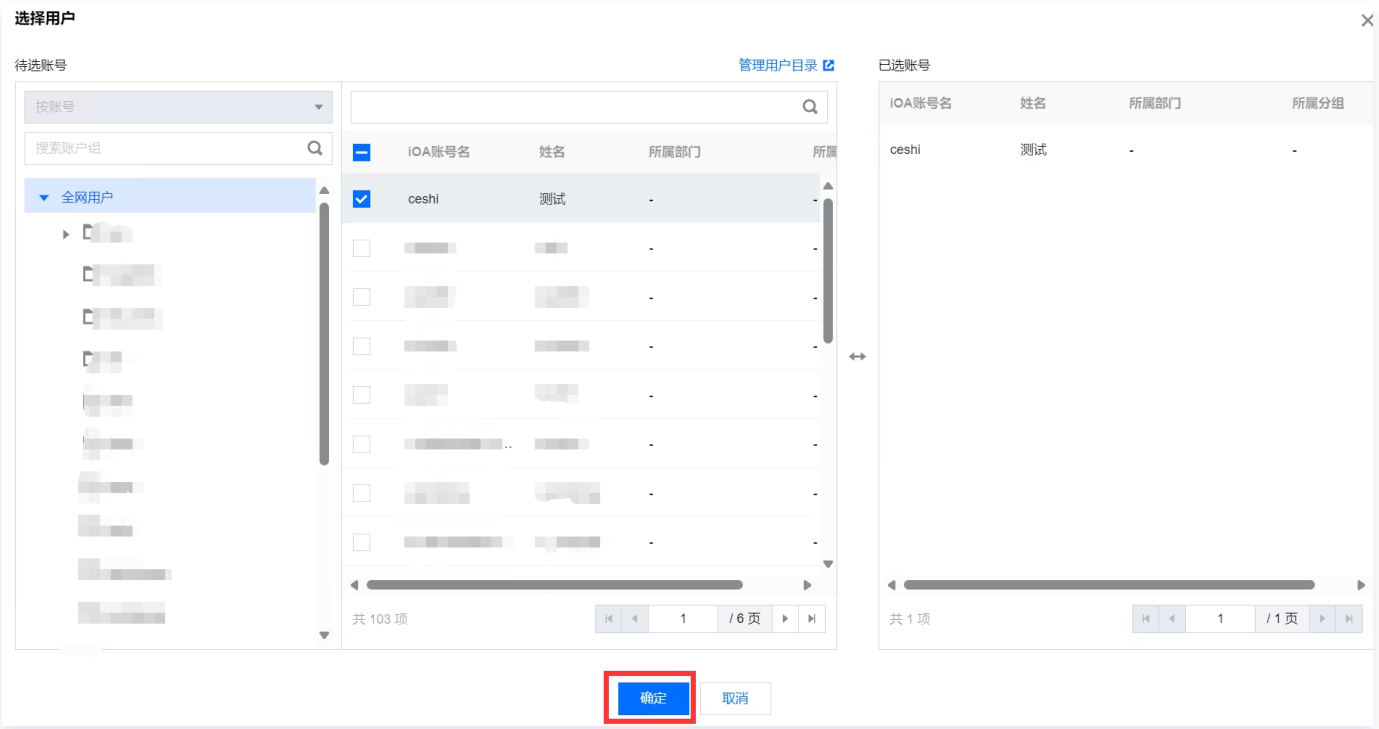
> **说明：**
> 审批测试发起人是作为测试功能使用，目的是测试该流程是否能正常发起审批流程。
> 例如：在配置企业微信审批流程后，需要先测试发起人是否能正常发起审批流程，因此需在审批测试发起人处，先勾选1个用户，测试勾选的用户是否能正常发起，因此发起人仅支持勾选1个用户做测试用。



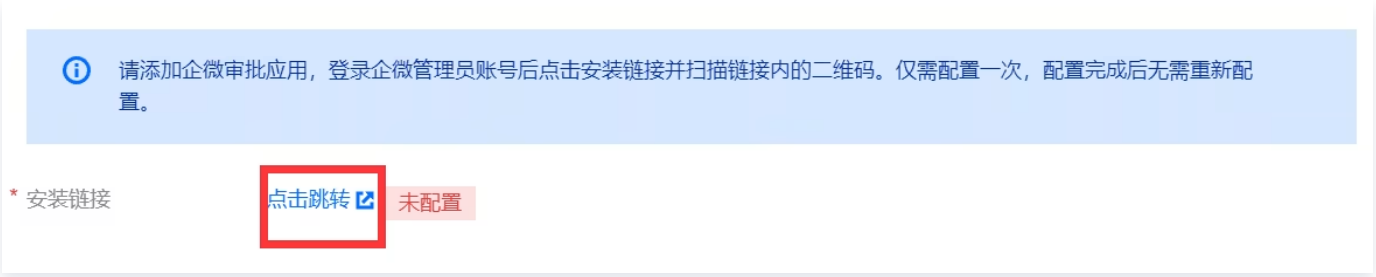
5. 审批测试接收人：单击**选择接收人**，单击**确定**保存。

> **说明：**
> 审批测试接收人是作为测试功能使用，目的是测试该流程是否能正常接收审批信息。

> 例如：配置企业微信审批流程后，需要测试接收人是否能正常接收审批流程信息，因此需在审批测试接收人处，先勾选1个用户，测试勾选的用户是否能正常接收，因此接收人仅支持勾选1个用户做测试用。



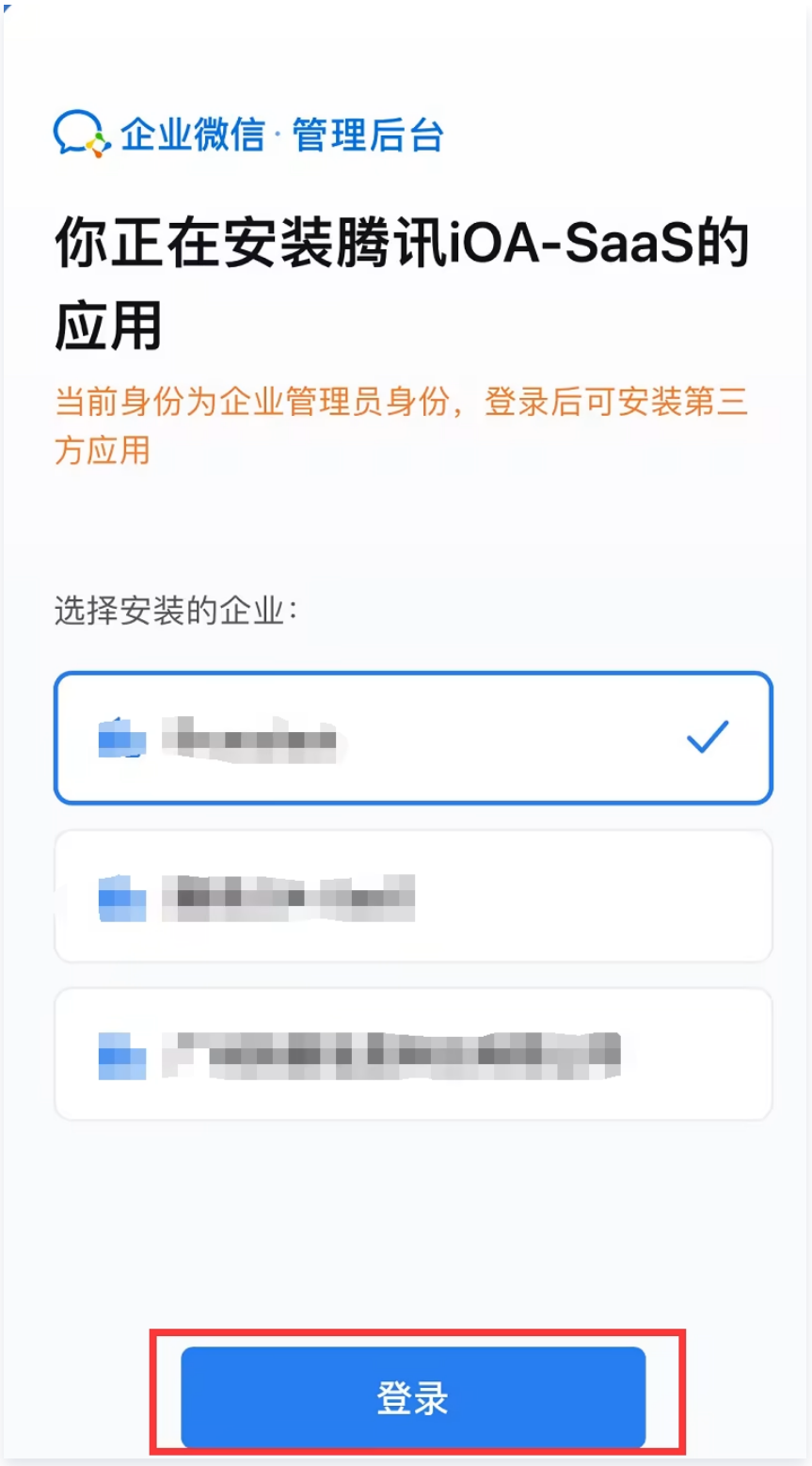
6. 安装链接：单击**跳转**。



6.1 企业微信管理员打开**手机企业微信 > 扫一扫**，扫描对应二维码。



6.2 扫码成功后提示正在安装腾讯 iOA-SaaS 的应用，单击**登录**。



6.3 登录后设置可见范围，建议可见范围设置整个组织架构或涉及审批流的部门，单击**同意以上授权并添加**。

> ⚠ **注意：**
> 1：系统默认仅扫码登录的当前管理员1人可见。
> 2：建议可见范围设置整个组织架构或涉及审批流的部门。

> 3：如未设置可见范围，系统默认仅扫码登录的当前管理员1人可见，其余审批人员无法看见审批流。



7. 在添加审批流页面，单击**测试**，发送审批流测试信息。



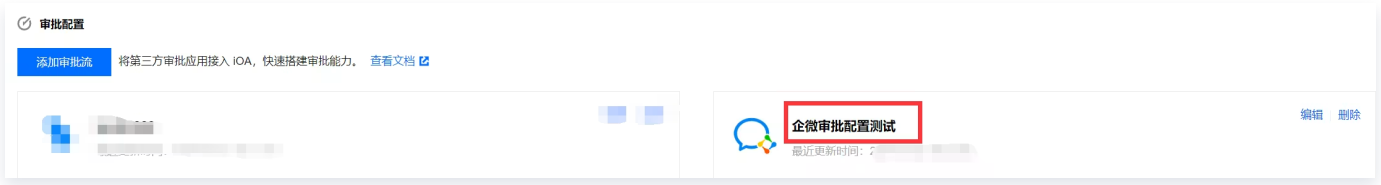
7.1 单击确定，发送审批测试信息。



7.2 企业微信收到审批信息，审批流发起测试成功。



8. 单击**保存**，完成企微审批流配置。



钉钉（11.1.1版）

最近更新时间：2026-02-06 14:23:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **审批流配置**。
2. 在审批流配置页面，单击**添加审批流**。



3. 在添加审批流页面，选择**钉钉**，输入审批流程名称，选择**审批管理员**。



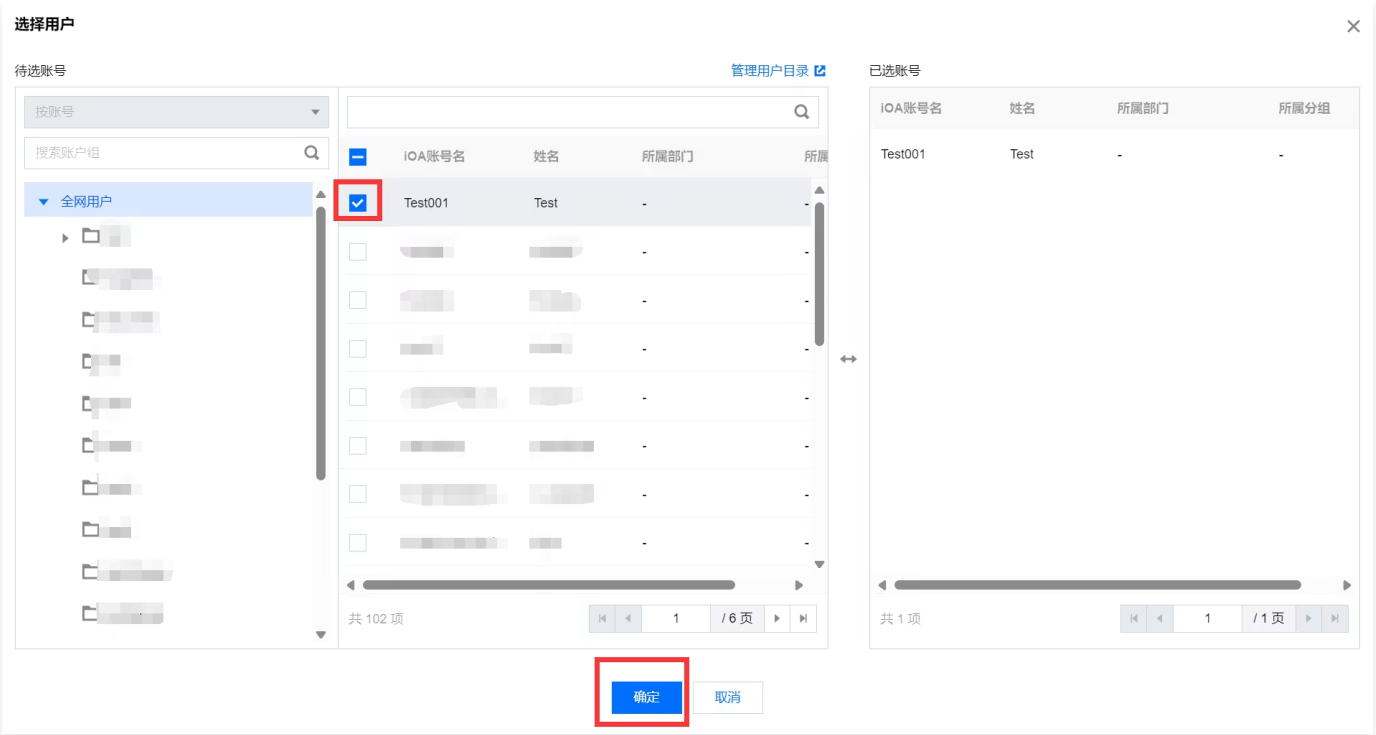
参数名称		说明
审批管理员	直属 leader	自动将审批信息发送至钉钉对应的 leader，此选项无法在配置页面进行测试，请在配置完成后，在对应终端上登录并进行审批测试。
	指定用户	选择组织架构中的单个或多个用户，对应用户名需要与钉钉中的一致，请确保在收到审批测试信息后进行保存。 • 勾选单个用户：仅1个用户审批。 • 勾选多个用户：选中的多个用户都会收到审批消息，多个用户收到的审批消息中以第1个决策的为准，例如01用户号第一个看到审批消息并审批通过，则以01用户的审批结果为准。
	自定义	填写对应审批管理员的钉钉用户名，请确保在收到审批测试信息后进行保存。
备用管理员		选择直属 leader 审批，必填备用管理员，当直属 leader 字段为空时，审批信息将发送给备用审批员。

4. 审批测试发起人：单击**选择发起人**，单击**确定**保存。

说明：

审批测试发起人是作为测试功能使用，目的是测试该流程是否能正常发起审批流程。

例如：在配置钉钉审批流程后，需要先测试发起人是否能正常发起审批流程，因此需在审批测试发起人处，先勾选1个用户，测试勾选的用户是否能正常发起，因此当前发起人仅支持勾选1个用户做测试用。



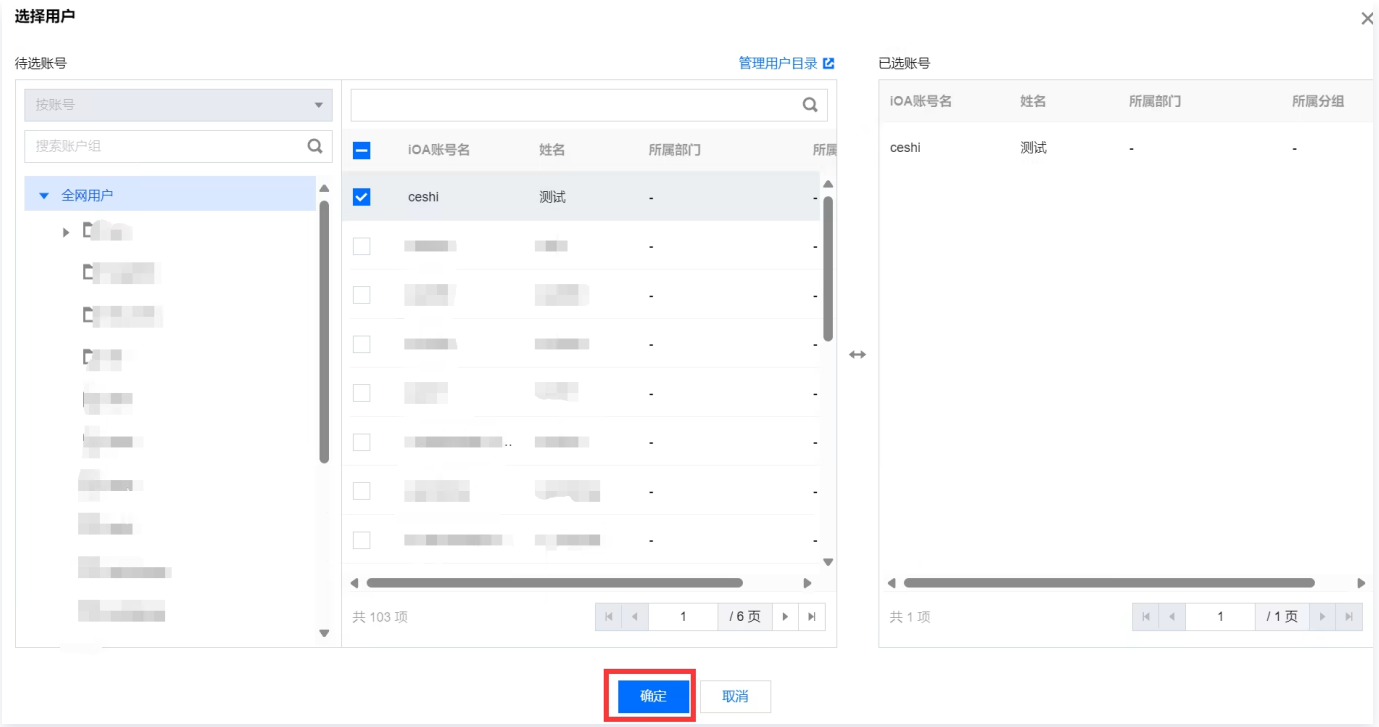
5. 审批测试接收人：单击**选择接收人**，单击**确定**保存。

说明：

审批测试接收人是作为测试功能使用，目的是测试该流程是否能正常接收审批信息。

例如：配置钉钉审批流程后，需要测试接收人是否能正常接收审批流程信息，因此需在审批测试接收人处，先勾选1个用户，测试勾选的用户是否能正常接收，因此当前接收人仅支持勾选1个用户做测试用。

版权所有：腾讯云计算（北京）有限责任公司



6. 安装配置：单击**下拉框** > **新建配置**。



7. 在新建安装配置窗口中，输入安装配置名称，根据如下描述配置相关参数。



7.1 安装配置名称：根据实际需求，自定义名称。

7.2 获取 App Key，App Secret 参数。

7.2.1 登录钉钉开放平台-开发者后台，进入应用开发，单击**创建应用**，填写应用名称、应用描述后单击**保存**。



7.2.2 选择创建的应用，单击查**看版本详情**，单击 编辑版本详情信息后保存并发布。

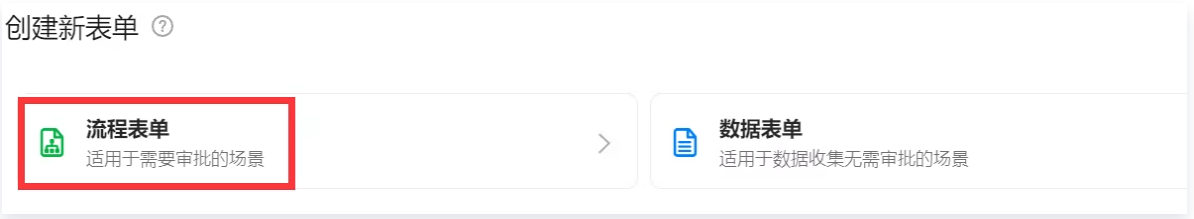


7.2.3 单击**凭证与基础信息**，获取凭证与基础信息，查看 App Key，App Secret。



7.3 获取审批流程 ID。

7.3.1 进入钉钉审批管理后台，单击**创建审批表单 > 流程表单**。



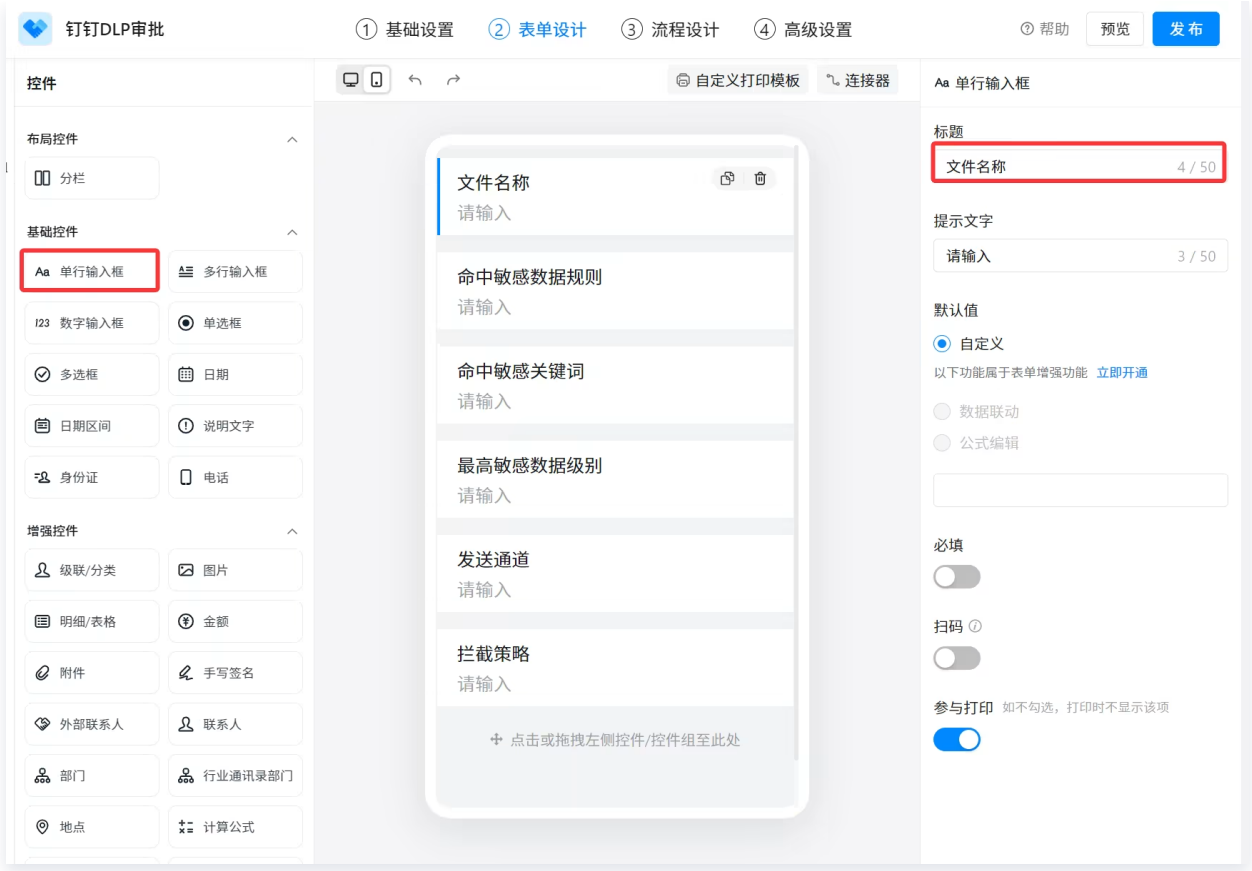
7.3.2 基础设置：根据公司管理需求配置人员发起权限并设置表单管理员，同时在页面最下方展示表单 ID，请您**复制表单 ID**。



7.3.3 用于填写至 iOA 管控策略 > 审批流配置 > 钉钉审批 > 安装配置 > 新建安装配置的审批流程 ID 中。



7.3.4 表单设计：请拖动6个单行输入框控件至表单设计中，并依次命名为：文件名称、命中敏感数据规则、命中敏感关键词、最高敏感数据级别、发送通道、拦截策略。



7.3.5 流程设计与高级设置无需配置，单击**发布**即可。



7.4 获取 aes_key 参数。

7.4.1 登录钉钉开放平台，在**开发者后台** > **应用开发**页面，单击**创建的应用**。



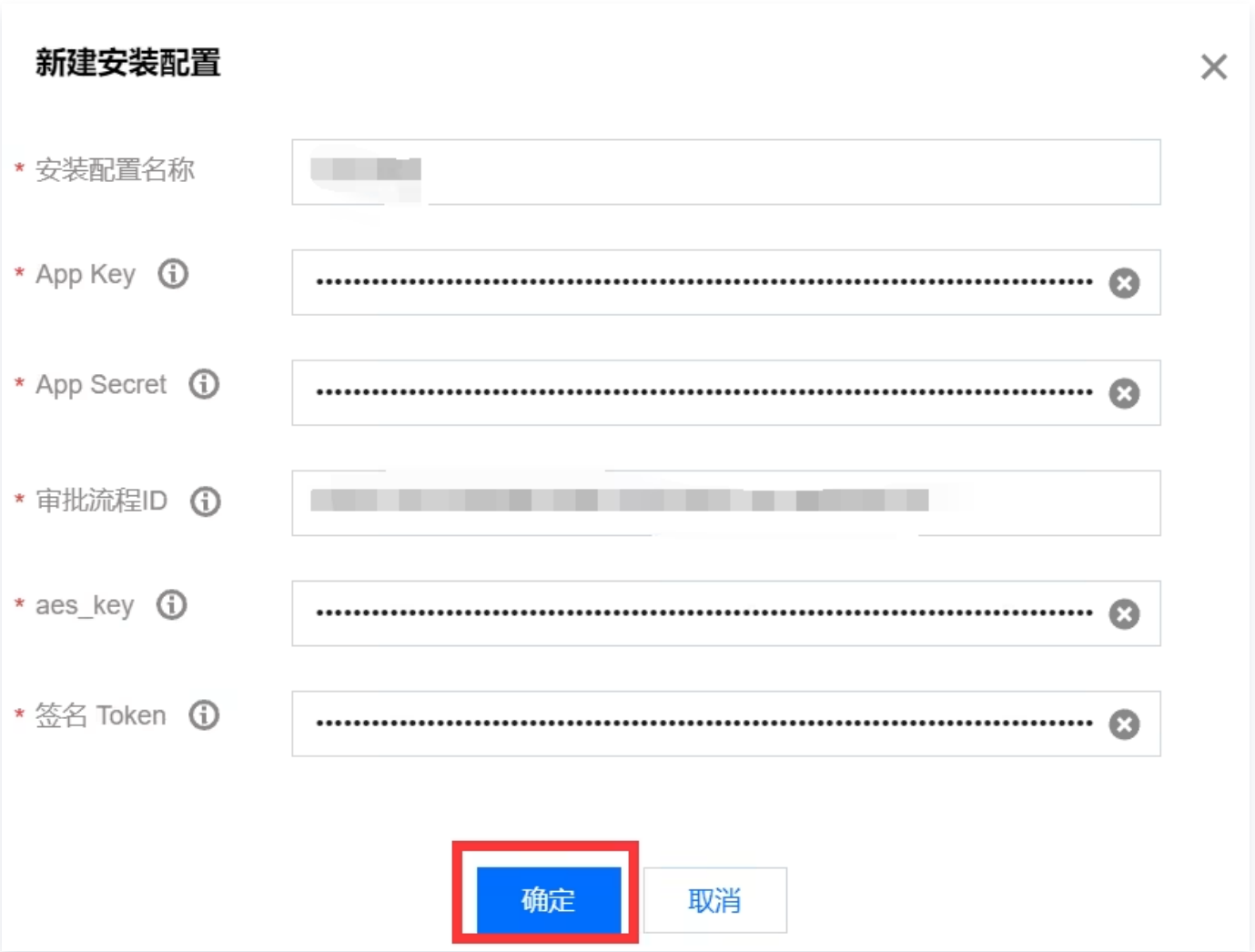
7.4.2 选择事件订阅，配置事件订阅信息，单击重置，获取 aes_key、签名 token。

- **推送方式：选择HTTP推送。**
- **加密 aes_key：单击重置，获取 aes_key，单击 ，查看 aes_key。**
- **签名 token：单击重置。获取签名 token，单击 ，查看 签名 token。**



> **说明：**
> 请求网址获取方式详细配置如下：参看8~8.2。

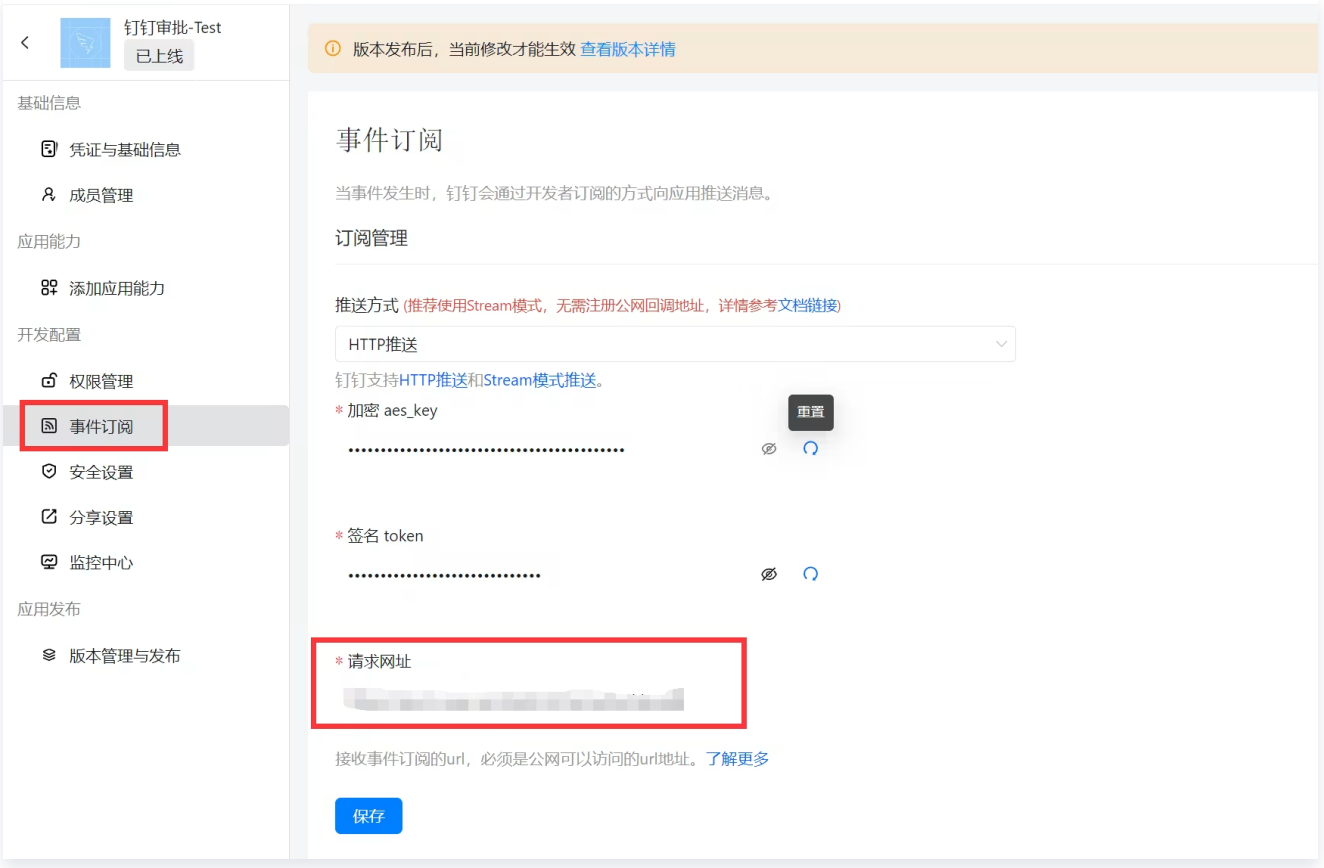
8. 将获取的安装配置信息依次录入，单击**确定**。



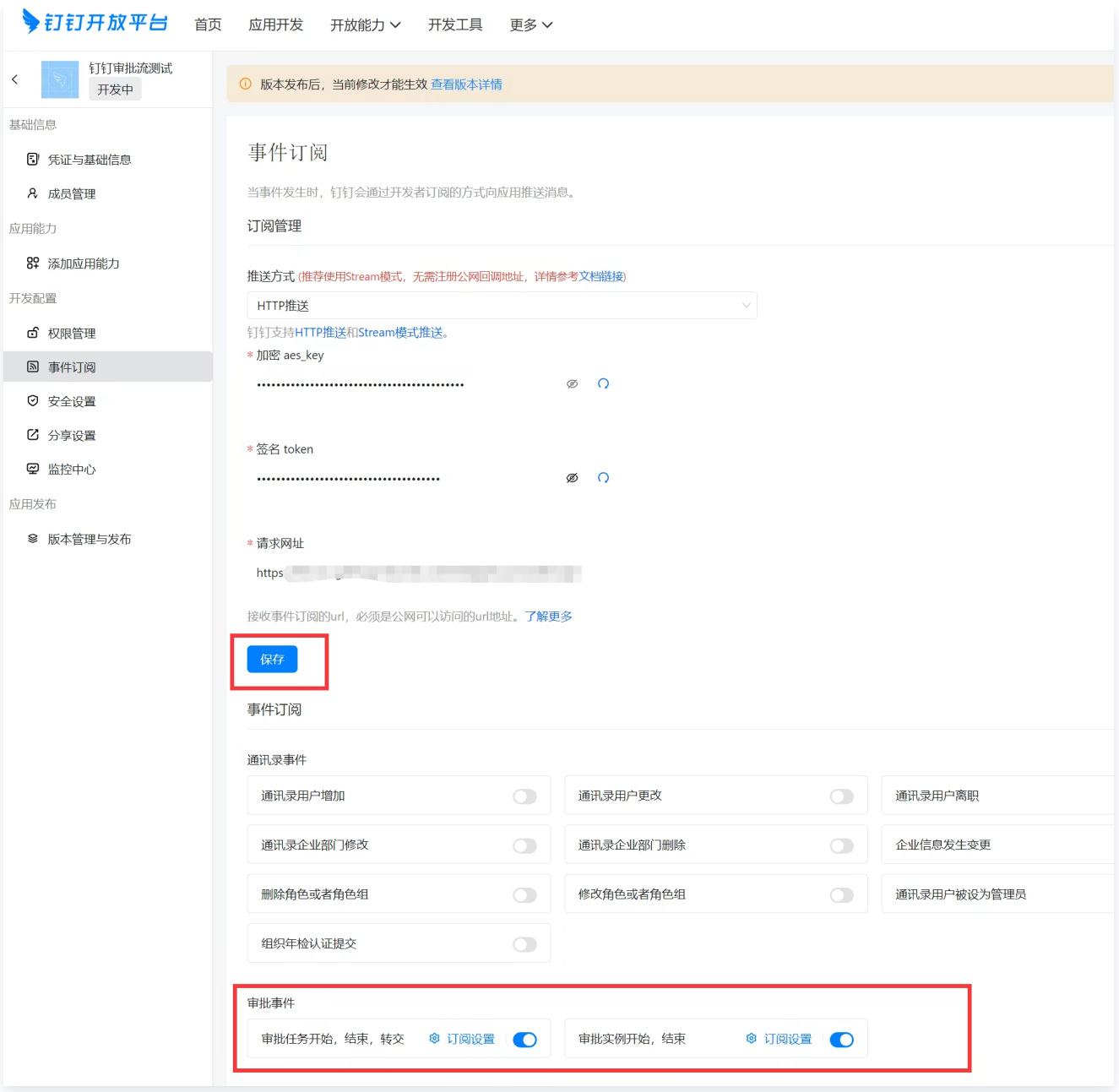
8.1 下拉选择安装配置名称，后台自动生成**回调地址**，单击**复制**。



8.2 将生成的回调地址，复制到**事件订阅>请求网址**中，单击**保存**。



8.3 配置审批事件，确认开启审批事件的按钮（审批任务开始、结束、转交；审批实例开始，结束）。



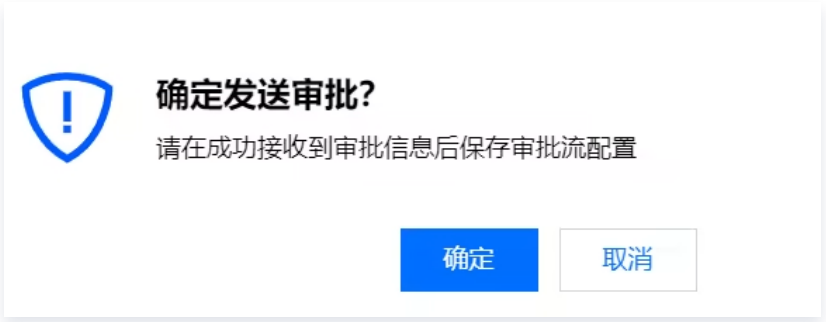
8.4 进入权限管理，勾选个人权限、通讯录管理、OA 审批，单击批量申请。



9. 在添加审批流页面，单击**测试**，发送审批流测试信息。



9.1 单击**确定**，发送审批测试信息。



9.2 钉钉收到审批信息，审批流发起测试成功。



10. 单击**保存**，完成钉钉审批流配置。



飞书（11.1.1版）

最近更新时间：2026-02-06 14:23:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **审批流配置**。
2. 在审批流配置页面，单击**添加审批流**。



3. 选择飞书审批，审批流支持配置内置审批模板与自定义审批模板。
   - 使用内置的审批模板：内置为单节点审批流，添加飞书审批流中的指定审批人员。



- 使用自定义审批模板：自定义审批流可支持多节点和条件判断，需自行在 飞书管理后台 创建和配置审批流程；iOA 零信任安全管理系统支持在飞书后台自定义配置审批流模板，增强审批流程的灵活性适用于企业多样化的审批需求。



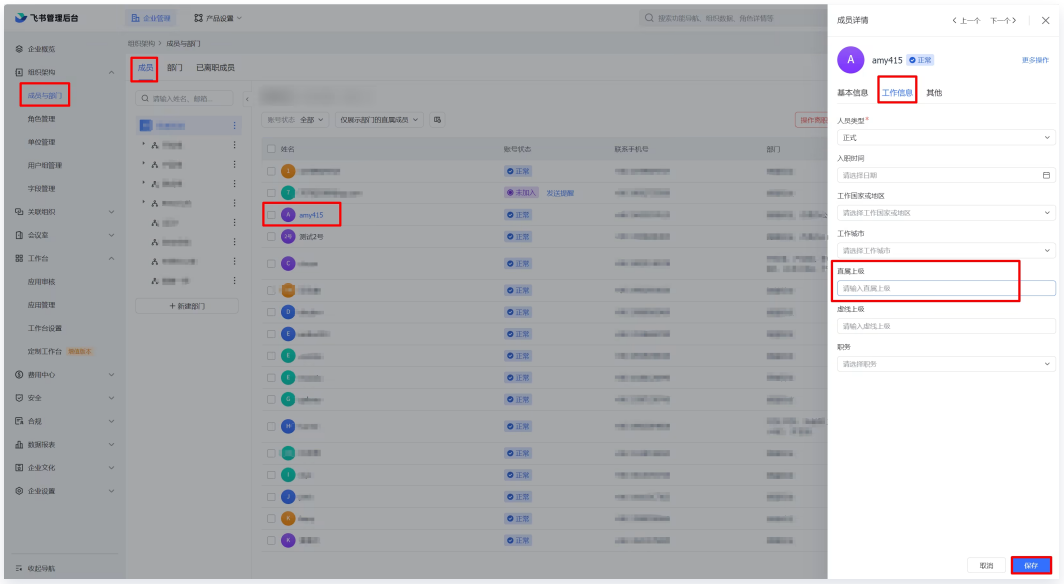
内置审批模板

1. 输入审批流程名称，选择内置审批模板，配置**审批管理员**。



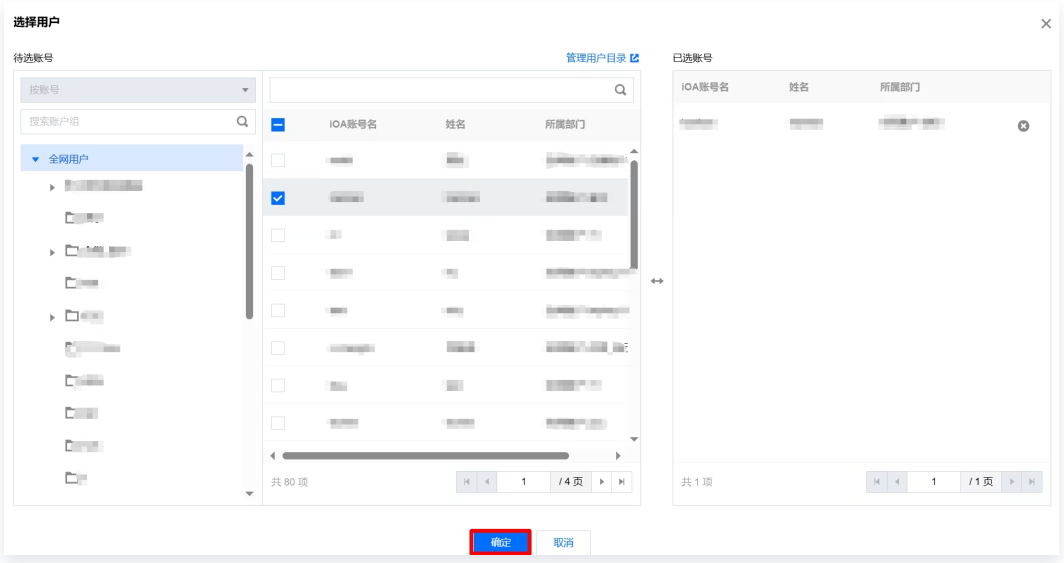
参数名称		说明
审批管理员	直属 leader	自动将审批信息发送至飞书中对应的 leader，此选项无法在配置页面进行测试，请在配置完成后，在对应终端上登录并进行审批测试。
	指定用户	选择组织架构中的单个或多个用户，对应的用户名需要与飞书中的一致，请确保在收到审批测试信息后进行保存。 • 勾选单个用户：仅1个用户审批。 • 勾选多个用户：选中的多个用户都会收到审批消息，多个用户收到的审批消息中以第一个决策的为准，例如01用户第一个看到审批消息并审批通过，则以01用户的审批结果为准。
	自定义	填写对应审批管理员的飞书用户名，请确保在收到审批测试信息后进行保存。
备用管理员		选择直属 leader 审批，必填备用管理员，当直属 leader 字段为空时，审批信息将发送给备用管理员。

- 直属 leader 在 飞书管理后台 > **组织架构** > **成员与部门** > **姓名** > **工作信息** > **直属上级**中配置，如未配置，当直属 leader 字段为空时，审批信息将发送给备用管理员。



2. 审批测试发起人：单击**选择发起人**，单击**确定**保存。

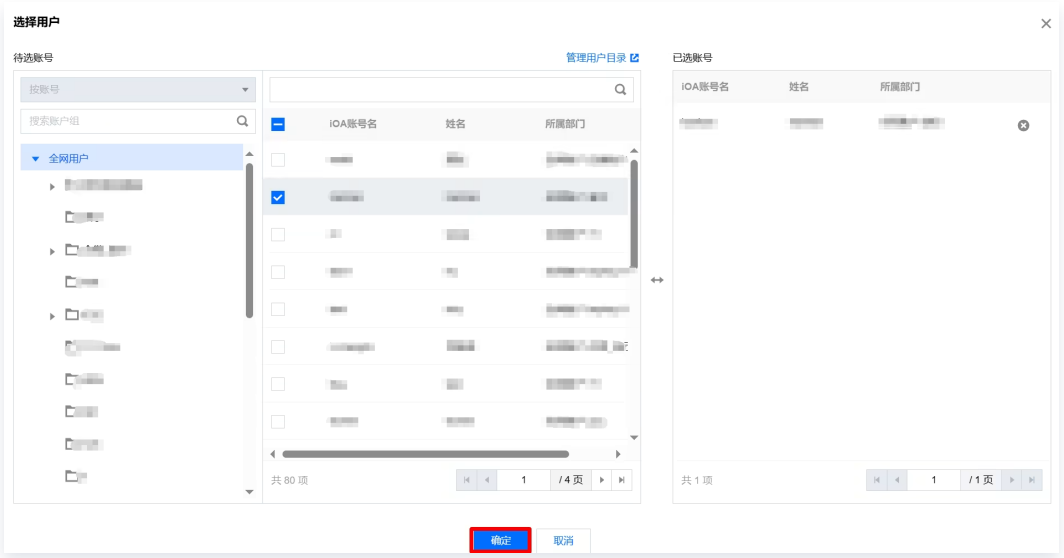
> **说明：**
> 审批测试发起人是作为测试功能使用，目的是测试该流程是否能正常发起审批流程。
> 例如：在配置飞书审批流程后，需要先测试发起人是否能正常发起审批流程，因此需要在审批测试发起人处，先勾选1个用户，测试勾选的用户是否能正常发起，因此当前发起人仅支持勾选1个用户做测试用。



3. 审批测试接收人：单击**选择接收人**，单击**确定**保存。

> **说明：**
> 审批测试接收人是作为测试功能使用，目的是测试该流程是否能正常接收审批信息。
> 例如：配置飞书审批流程后，需要测试接收人是否能正常接收审批流程信息，因此需要在审批测试接收人处，先勾选1个用户，测试勾选的用户是否能正常接收，因此当前接收人仅支持勾选1个用户做测试

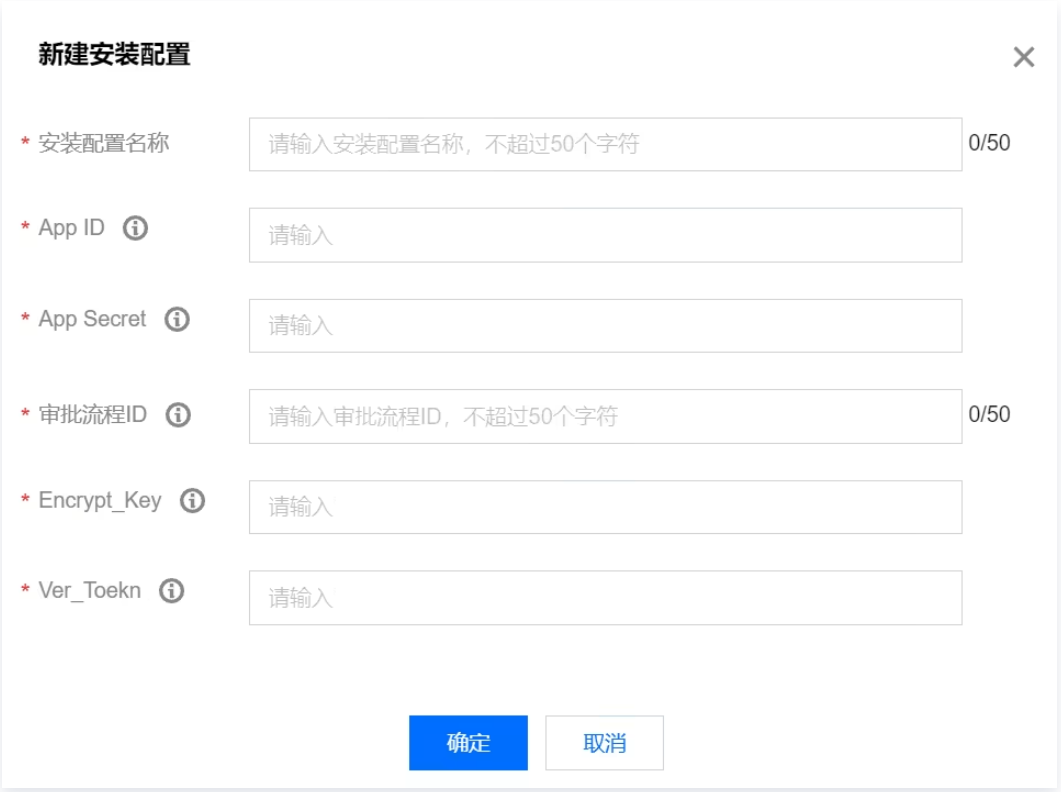
用。



4. 安装配置：单击**下拉框** > **新建配置**。



5. 在新建安装配置窗口中，输入安装配置名称，根据如下描述配置相关参数。



5.1 安装配置名称：根据实际需求，自定义名称。

5.2 获取 App ID，App Secret 参数。

5.2.1 如您是首次使用，未创建企业自建应用：

5.2.1.1 未创建企业自建应用，需要创建一个企业自建应用，登录 飞书开放平台，选择**企业自建应用**，单击**创建企业自建应用**。



5.2.1.2 在创建企业自建应用窗口中，配置相关参数，单击**创建**，即可完成创建。



5.2.2 如您未开通飞书开发者账号：

5.2.2.1 请先前往飞书开放平台，创建一个开发者账号。

5.2.2.2 在开发者后台，选择企业自建应用，单击创建企业自建应用。



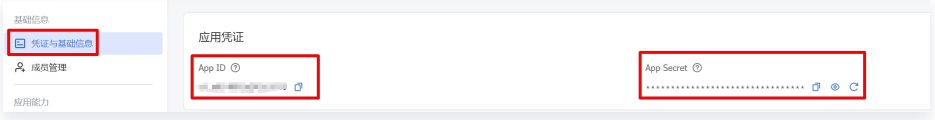
5.2.2.3 应用名称示例：腾讯 iOA；应用描述：xxxx（任意说明），单击创建。



5.2.3 在企业自建应用页面，单击刚刚创建的**自建应用**，进入应用详情页面。

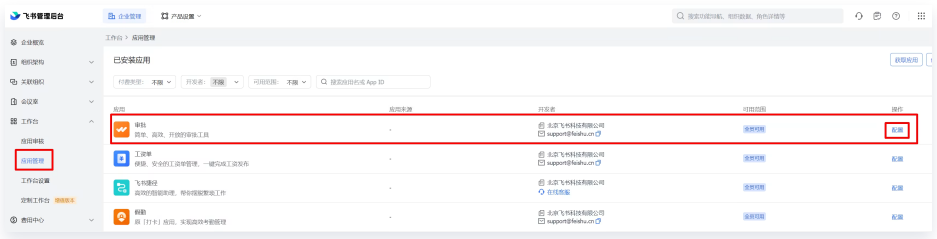


5.2.4 在凭证与基础信息页面，选择应用凭证，获取 App ID 和 App Secret。其中：飞书的 App ID 对应 iOA 控制台上的 App ID，飞书的 App Secret 对应 iOA 控制台的 App Secret。



5.3 获取审批流程ID：

5.3.1 登录飞书管理后台，展开工作台，在应用管理页选择审批，单击配置。



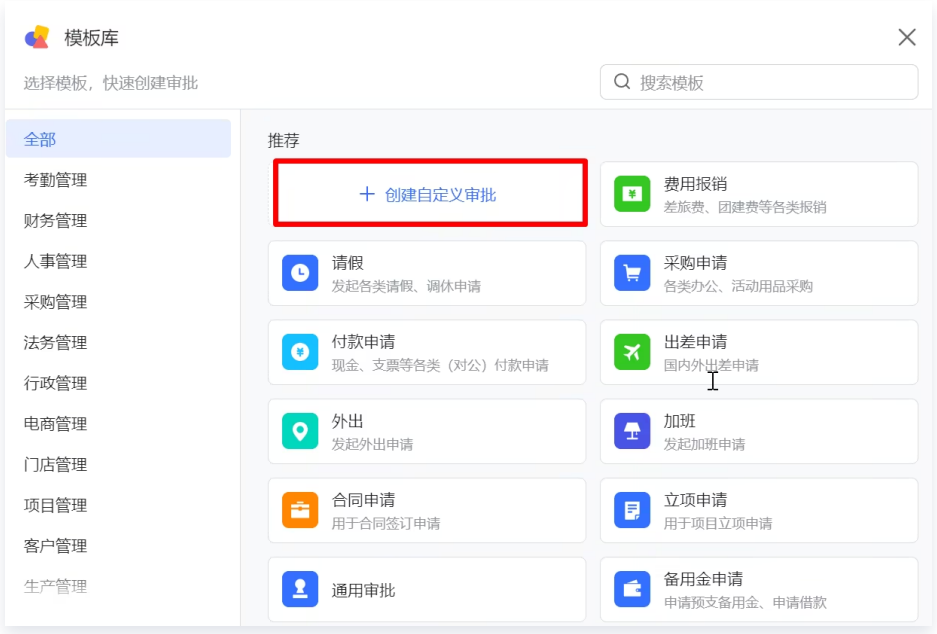
5.3.2 单击前往应用后台。



5.3.3 进入审批管理后台页面，单击创建审批。



5.3.4 单击创建自定义审批。



5.3.5 设置审批流程基础信息：



参数名称	说明
名称	自定义
说明	自定义
分组	自定义
谁可以提交该审批	建议选择**全员**
流程管理员	无特别要求，自定义或默认的流程管理员都可

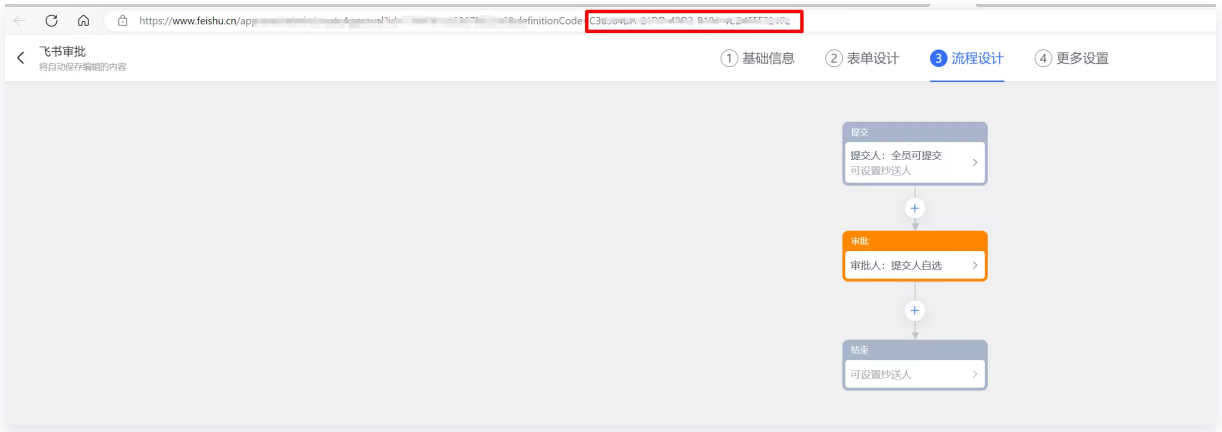
5.3.6 表单设计：拖拽左侧控件“单行文本”至表单设计处，请拖拽3个单行文本控件，并将3个单行文本控件分别命名为：通道名称、文件名称、文件级别，如下图所示：



5.3.7 流程设计：如下图所示，流程设计保持不变，按默认的样式就可以，单击**发布**。



5.3.8 发布完成，单击发布的流程表单，查看审批流程 ID。



5.4 获取 Encrypt_key：登录 飞书开放平台，在事件与回调页，选择加密策略 **Encrypt_key**，单击**重置**，飞书的 Encrypt Key 对应 iOA 控制台上的 Encrypt_key。



5.5 获取Ver_Token：在事件与回调页，选择加密策略 **Ver_Token**，单击**重置**，获取 Token，飞书的 Verification Token 对应 iOA 控制台上的Ver_Token。



6. 将获取的安装配置信息依次录入，单击**确定**。



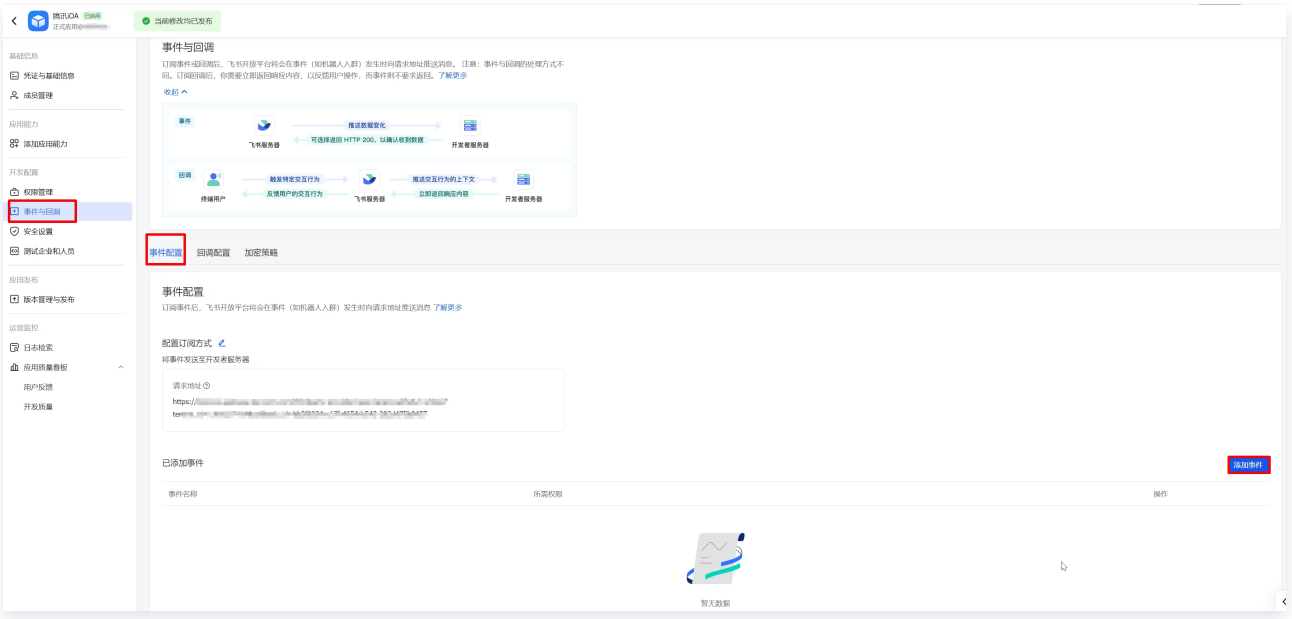
6.1 下拉选择安装配置名称，后台自动生成**回调地址**，单击**复制**。



6.2 登录 飞书开放平台 ，进入创建的企业自建应用，将生成的回调地址，复制到**事件与回调>事件配置**中，单击**保存**。



6.3 添加事件：在**事件与回调 > 事件配置**中，单击**添加事件**。

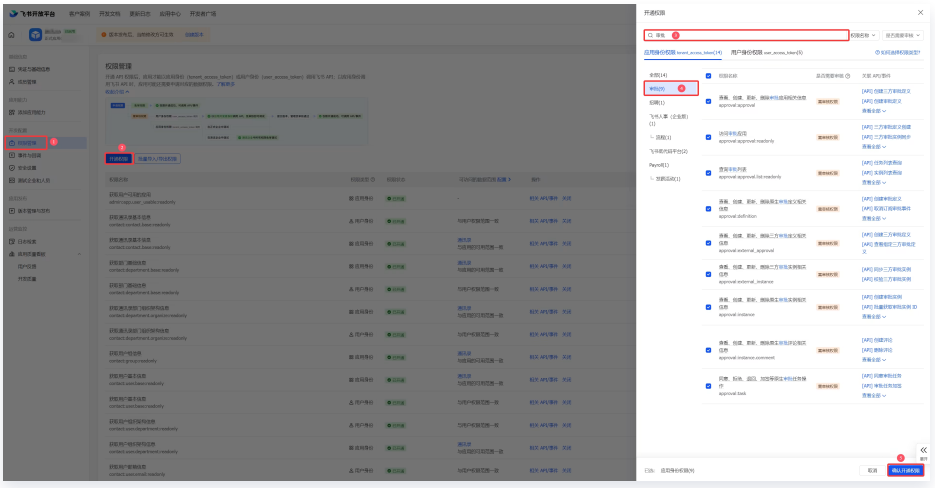


6.3.1 选择审批事件，勾选“审批实例状态变更”，“审批任务状态变更”，单击**确认添加**。

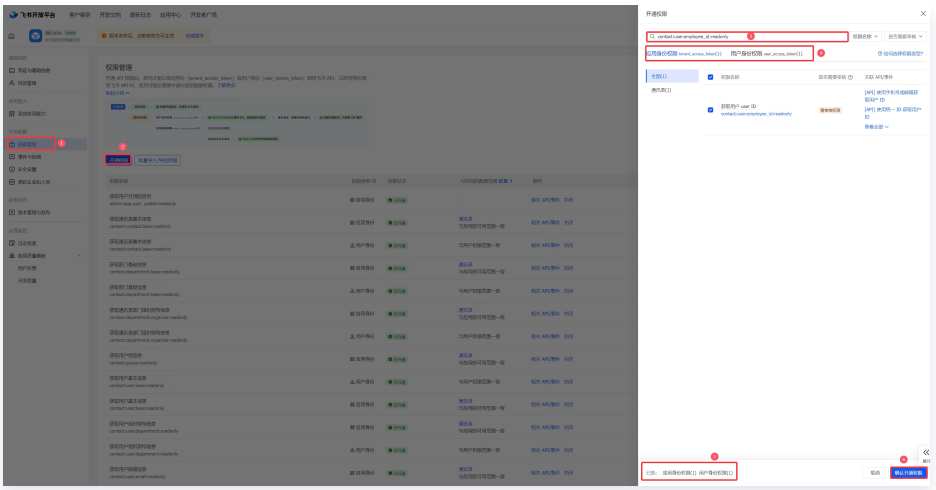


6.4 权限管理设置：

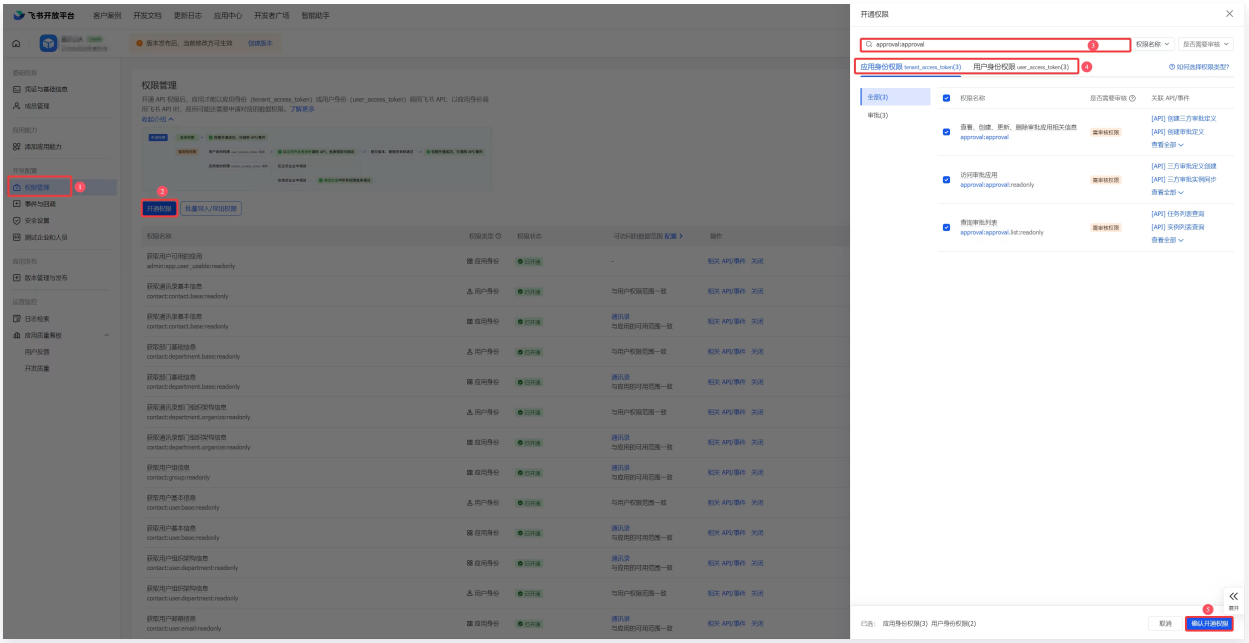
6.4.1 在**权限管理 > 开通权限**中，筛选审批，勾选**所有审批权限**，单击**确认开通权限**。



6.4.2 在**权限管理 > 开通权限**中，搜索框输入 contact:user.employee_id:readonly，**同时勾选应用身份权限和用户身份权限**，单击**确认开通权限**。

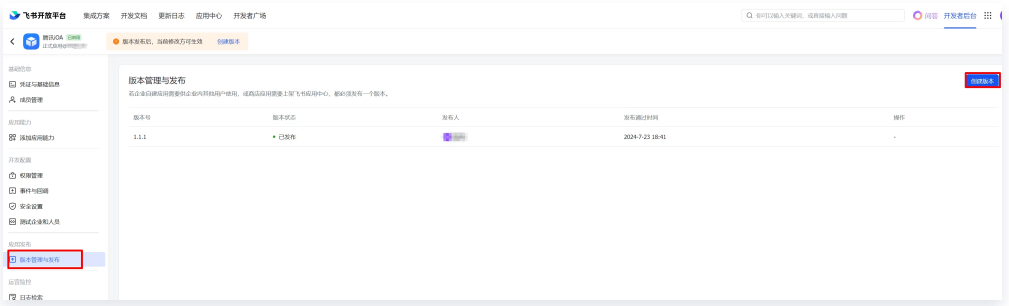


6.4.3 在**权限管理 > 开通权限**中，搜索框输入 approval:approval，**同时勾选应用身份权限和用户身份权限，单击确认开通权限。**



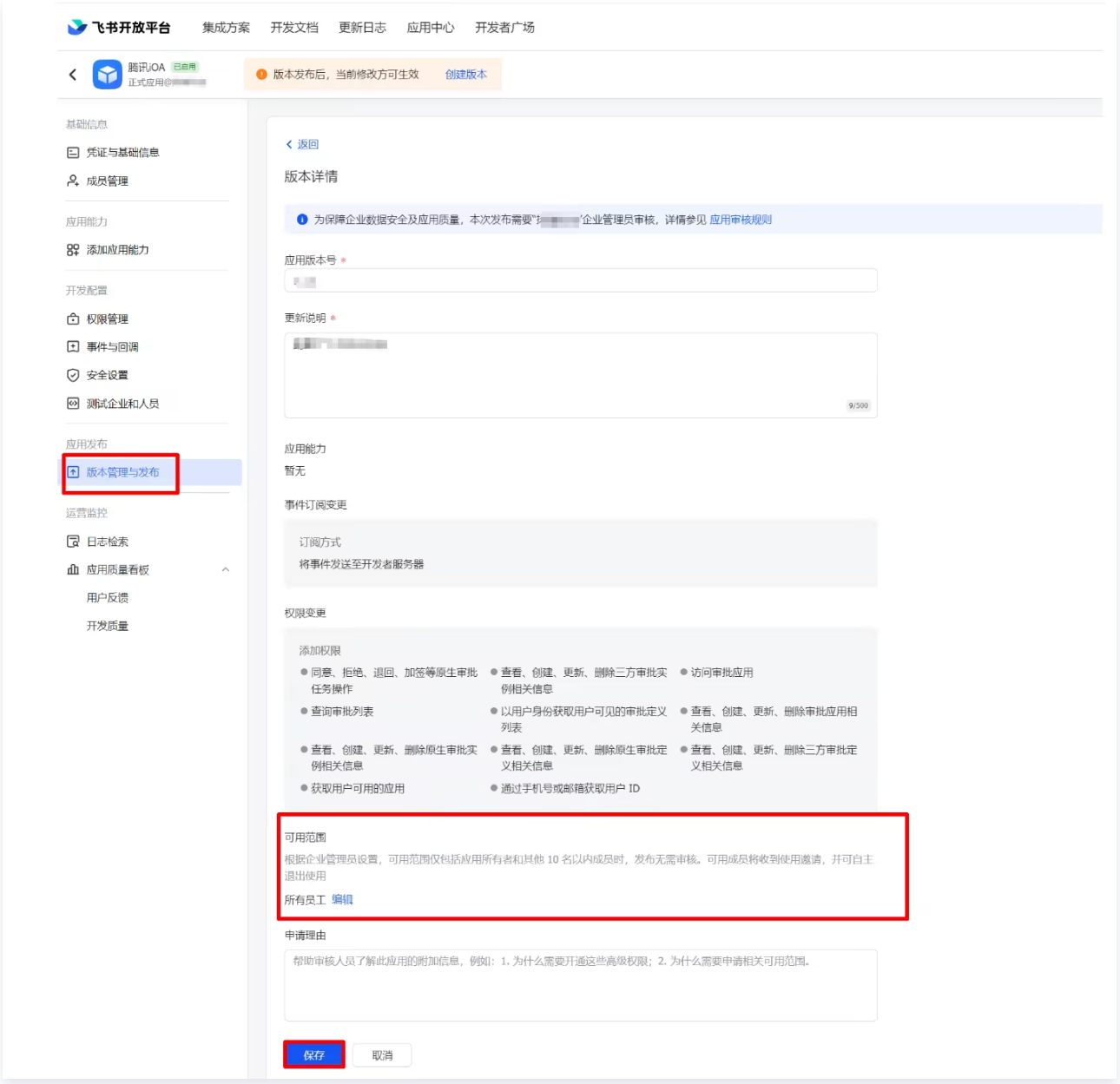
6.5 发布应用：在版本管理与发布页面，单击右上角的**创建版本**。

> **说明：**
> 配置权限后，需要重新发布应用才能生效。



6.6 在版本详情页面，填写应用版本号（格式如 1.0.0）和更新说明，设置可用性状态，单击**保存**。

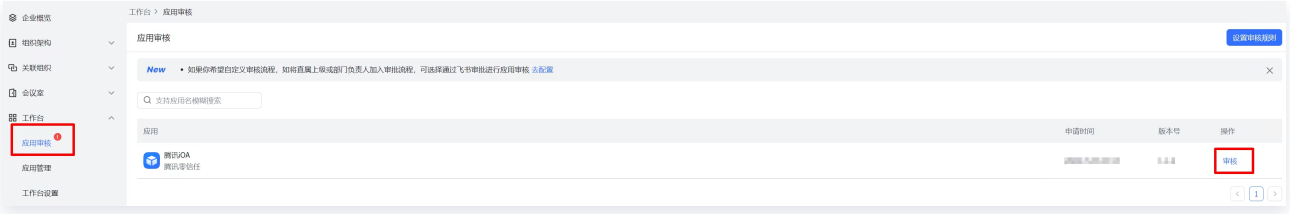
> **注意：**
> 可用范围：选择所有员工（除非只同步指定部门）。



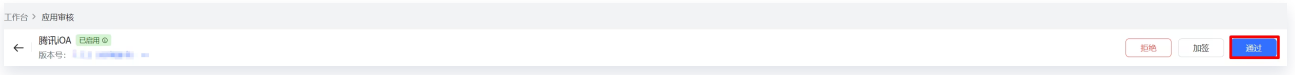
6.7 保存完成后，单击**申请线上发布**。



6.8 应用审核：管理员在 **应用审核页面** ，选择目标应用，单击**审核**。



6.9 在审核详情页面，单击**通过**。



> **说明：**
>
> - 提交申请后，企业管理员会进行审核。
> - 审核结果会通过飞书和开发者后台发送给您。
> - 更多详情请见 **飞书文档 – 开发企业自建应用** 。

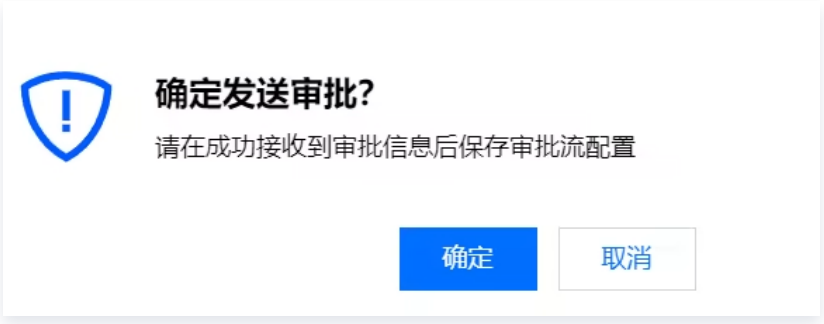
6.10 管理员应用审核通过后，自建应用状态显示为当前修改均已发布。



7. 飞书后台&审批流配置完成，在添加审批流页面，单击**测试**，发送审批流测试信息。



7.1 单击**确定**，发送审批测试信息。



7.2 飞书收到审批信息，审批流发起测试成功。

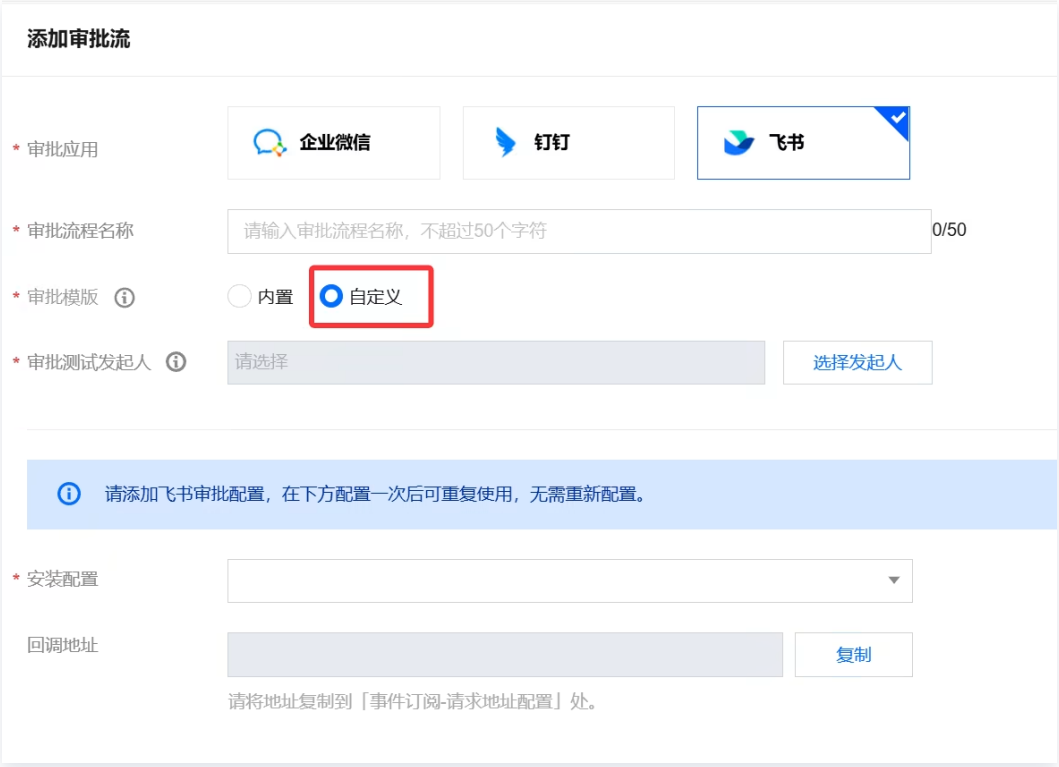


8. 单击**保存**，完成飞书审批流配置。



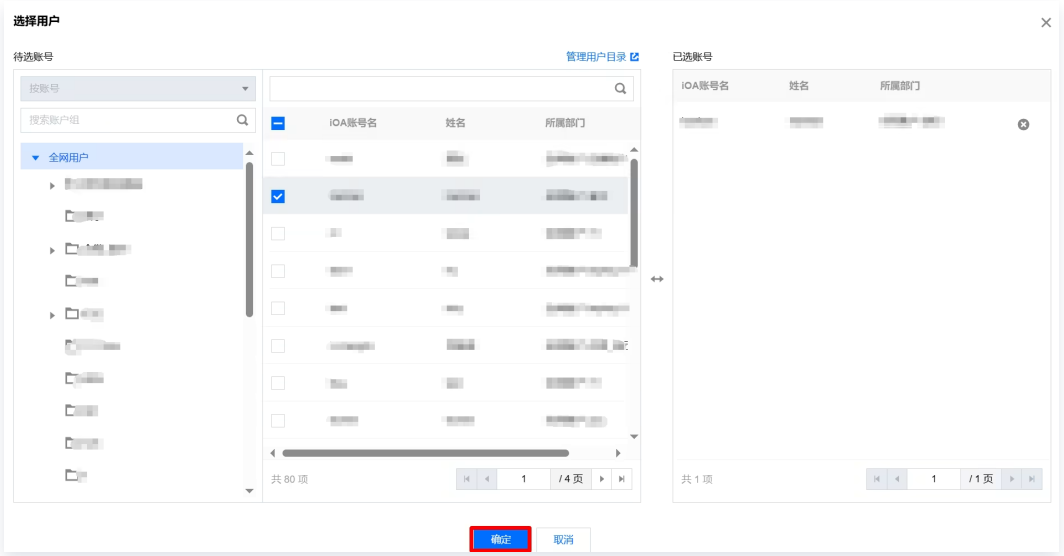
自定义审批模板

1. 输入审批流程名称，选择**自定义审批模板**。



2. 审批测试发起人：单击**选择发起人**，单击**确定**保存。

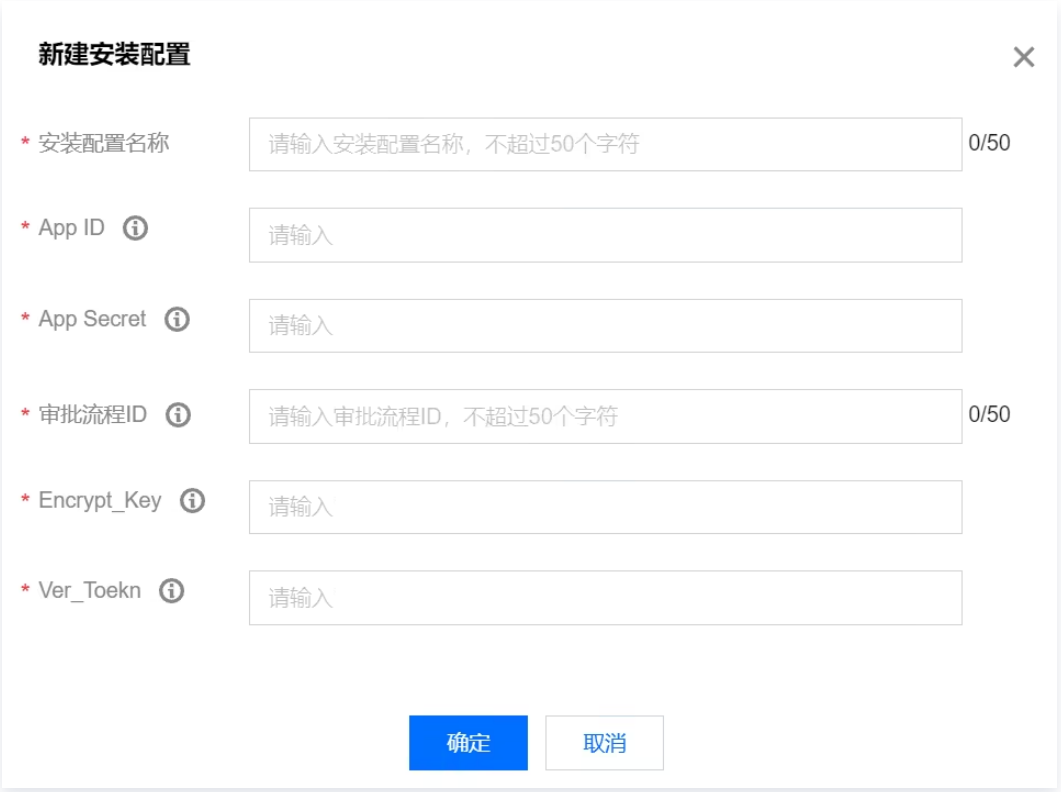
> **说明：**
> 审批测试发起人是作为测试功能使用，目的是测试该流程是否能正常发起审批流程。
> 例如：在配置飞书审批流程后，需要先测试发起人是否能正常发起审批流程，因此需要在审批测试发起人处，先勾选1个用户，测试勾选的用户是否能正常发起，因此当前发起人仅支持勾选1个用户做测试用。



3. 安装配置：单击**下拉框 > 新建配置**。



4. 在新建安装配置窗口中，输入安装配置名称，根据如下描述配置相关参数。



4.1 安装配置名称：根据实际需求，自定义名称。

4.2 获取 App ID，App Secret 参数。

4.2.1 如您是首次使用，未创建企业自建应用：

4.2.1.1 未创建企业自建应用，需要创建一个企业自建应用，登录 飞书开放平台，选择**企业自建应用**，单击**创建企业自建应用**。



4.2.1.2 在创建企业自建应用窗口中，配置相关参数，单击**创建**，即可完成创建。



4.2.2 如您未开通飞书开发者账号：

4.2.2.1 请先前往 飞书开放平台，创建一个开发者账号。

4.2.2.2 在 开发者后台，选择**企业自建应用**，单击**创建企业自建应用**。



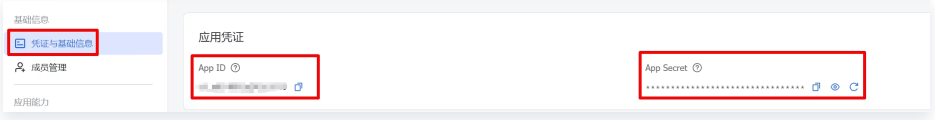
4.2.2.3 应用名称示例：腾讯 iOA；应用描述：xxxx（任意说明），单击**创建**。



4.2.3 在企业自建应用页面，单击刚刚创建的**自建应用**，进入应用详情页面。

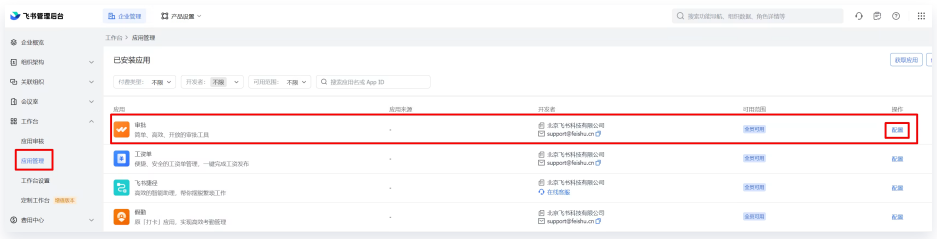


4.2.4 在凭证与基础信息页面，选择应用凭证，获取 App ID 和 App Secret。其中：飞书的 App ID 对应 iOA 控制台上的 App ID，飞书的 App Secret 对应 iOA 控制台上的 App Secret。



4.3 获取审批流程ID：

4.3.1 登录飞书管理后台，展开工作台，在应用管理页选择审批，单击**配置**。



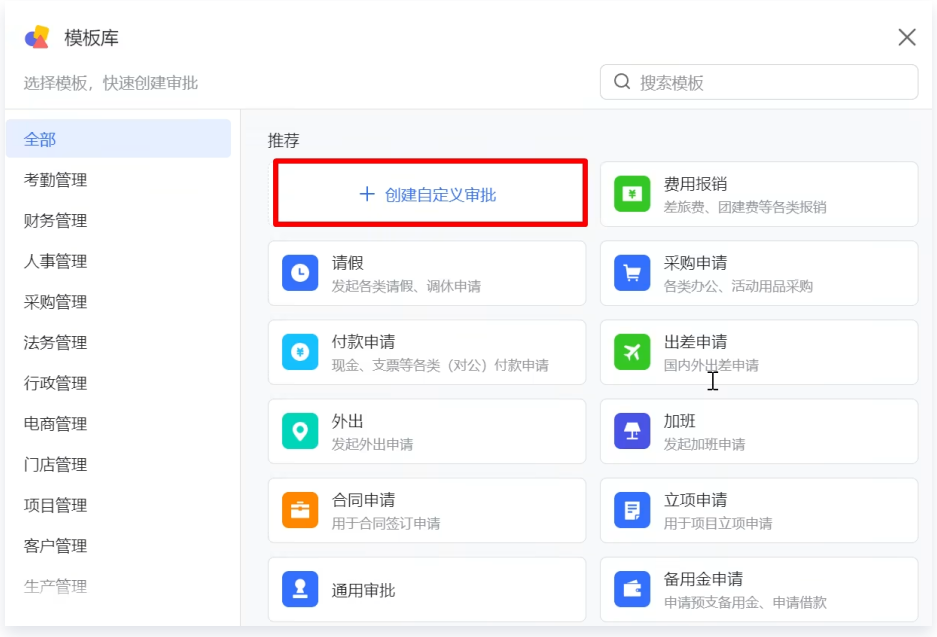
4.3.2 单击**前往应用后台**。



4.3.3 进入审批管理后台页面，单击**创建审批**。



4.3.4 单击**创建自定义审批**。



4.3.5 设置审批流程基础信息：



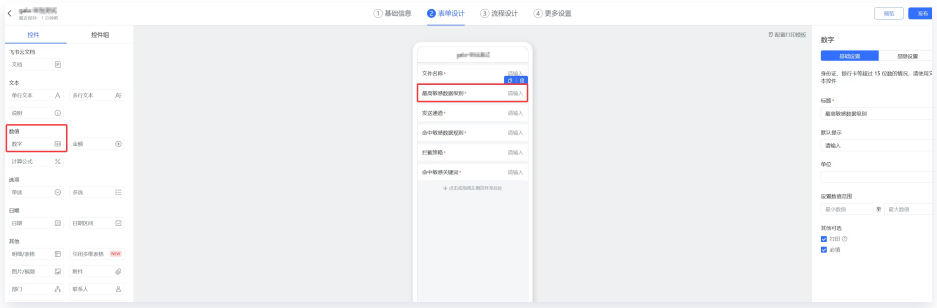
参数名称	说明
名称	自定义
说明	自定义
分组	自定义
谁可以提交该审批	建议选择**全员**
流程管理员	无特别要求，自定义或默认的流程管理员都可

4.3.6 表单设计：

- 拖拽左侧控件“单行文本”至表单设计处，请拖拽5个单行文本控件，并将5个单行文本控件分别命名为：文件名称、发送通道、命中敏感数据规则、拦截策略、命中敏感关键词，如下图所示：



- 拖拽左侧控件“数值控件”至表单设计处，请拖拽一个数值控件，并将数值控件命名为：最高敏感数据级别，如下图所示：



> **说明：**
> 控件的顺序不影响，请拖拽5个单行文本控件（命名为：文件名称、发送通道、命中敏感数据规则、拦截策略、命中敏感关键词）一个数值控件（命名为：最高敏感数据级别）即可。

4.3.7 流程设计：配置公司的飞书审批流程，此处配置的流程发布后，在安装配置里引用此流程 ID，则飞书审批使用此处的审批流程。

> **说明：**
> 自定义模板的审批流程是各公司自行配置，根据各公司的管理流程配置即可，配置完成单击发布。



- 若审批模板为内置审批模板，则在飞书流程设计中，审批人配置为“提交人自选”。



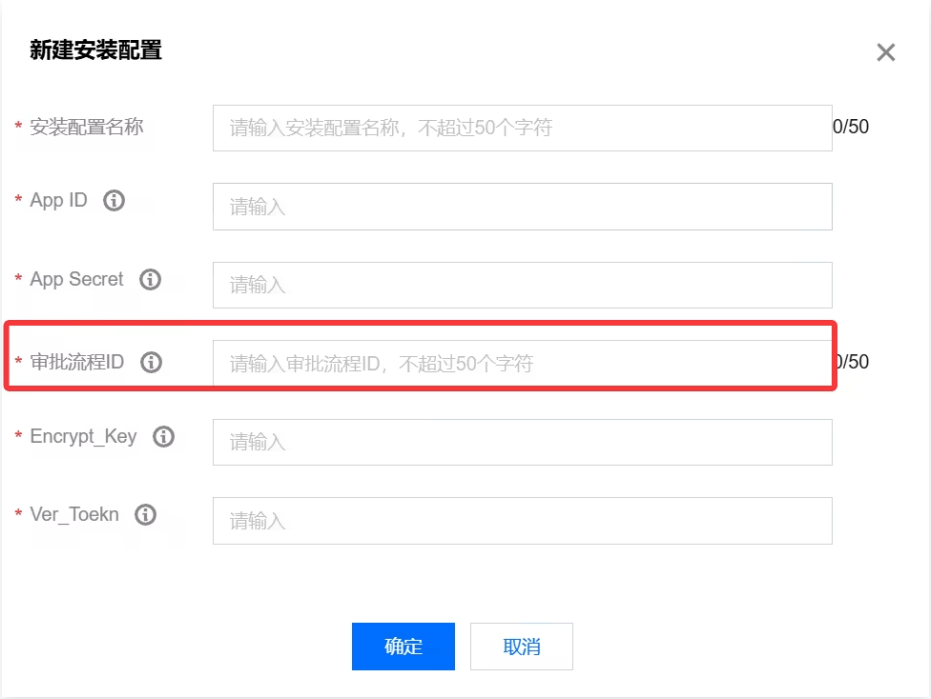


- 若审批模板为飞书自定义审批模板，则在飞书流程设计中，审批人配置为指定人员。

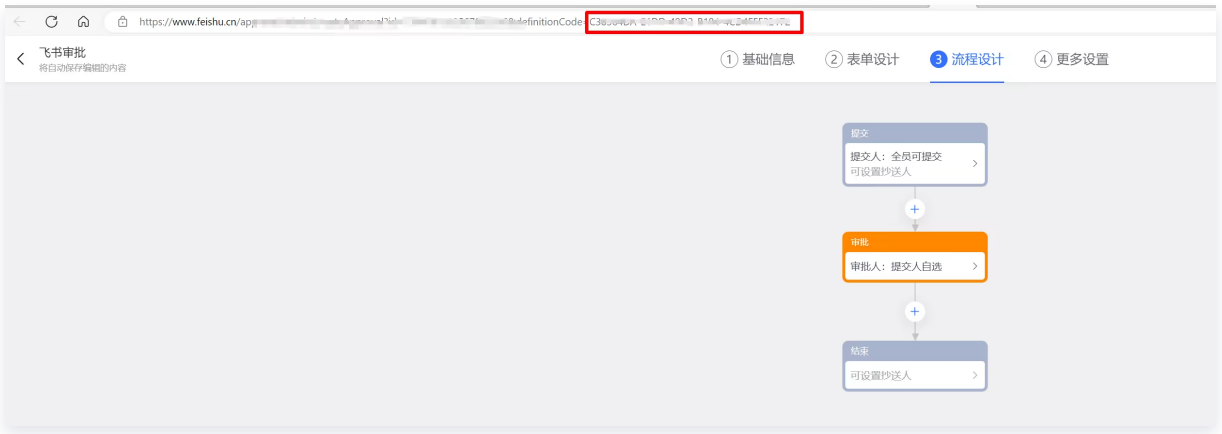




- 安装配置里引用此流程 ID 图示：



4.3.8 发布完成，单击发布的流程表单，查看审批流程 ID。



4.4 获取 Encrypt_key：登录 飞书开放平台，在事件与回调页，选择加密策略 **Encrypt_key**，单击**重置**，飞书的 Encrypt Key 对应 iOA 控制台上的 Encrypt_key。



4.5 获取Ver_Token：在事件与回调页，选择加密策略 **Ver_Token**，单击**重置**，获取 Token，飞书的 Verification Token 对应 iOA 控制台上的Ver_Token。



5. 将获取的安装配置信息依次录入，单击**确定**。



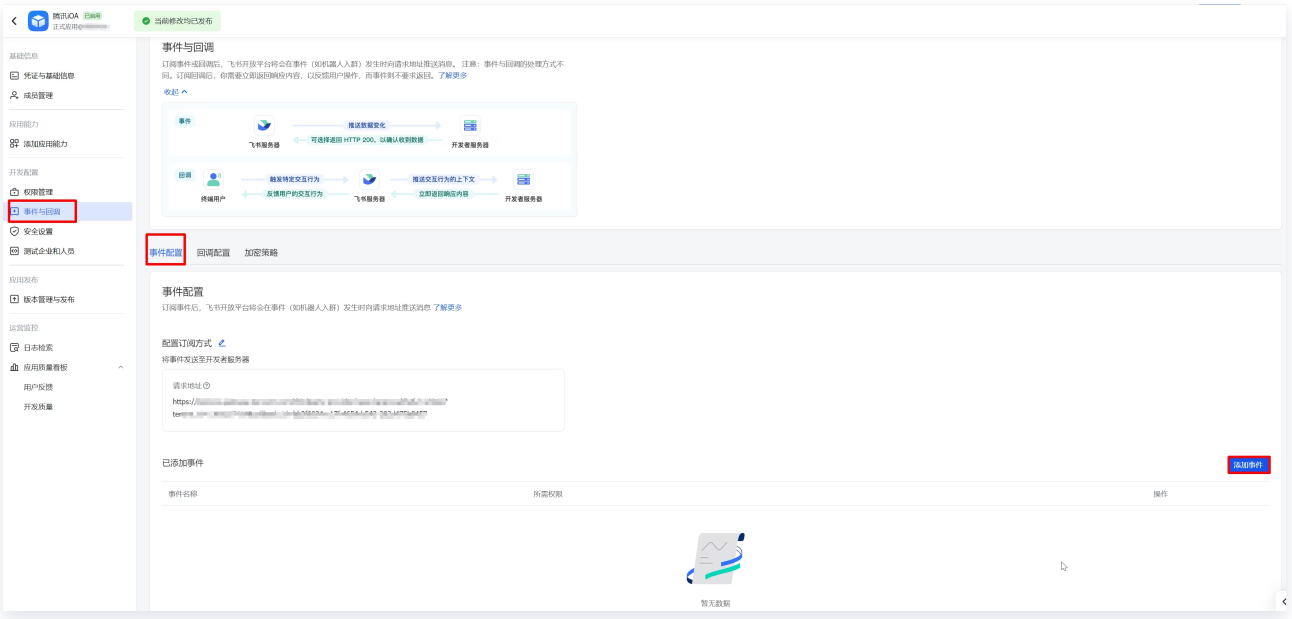
5.1 下拉选择安装配置名称，后台自动生成**回调地址**，单击**复制**。



5.2 登录 飞书开放平台 ，进入创建的企业自建应用，将生成的回调地址，复制到**事件与回调>事件配置**中，单击**保存**。



5.3 添加事件：在**事件与回调 > 事件配置**中，单击**添加事件**。

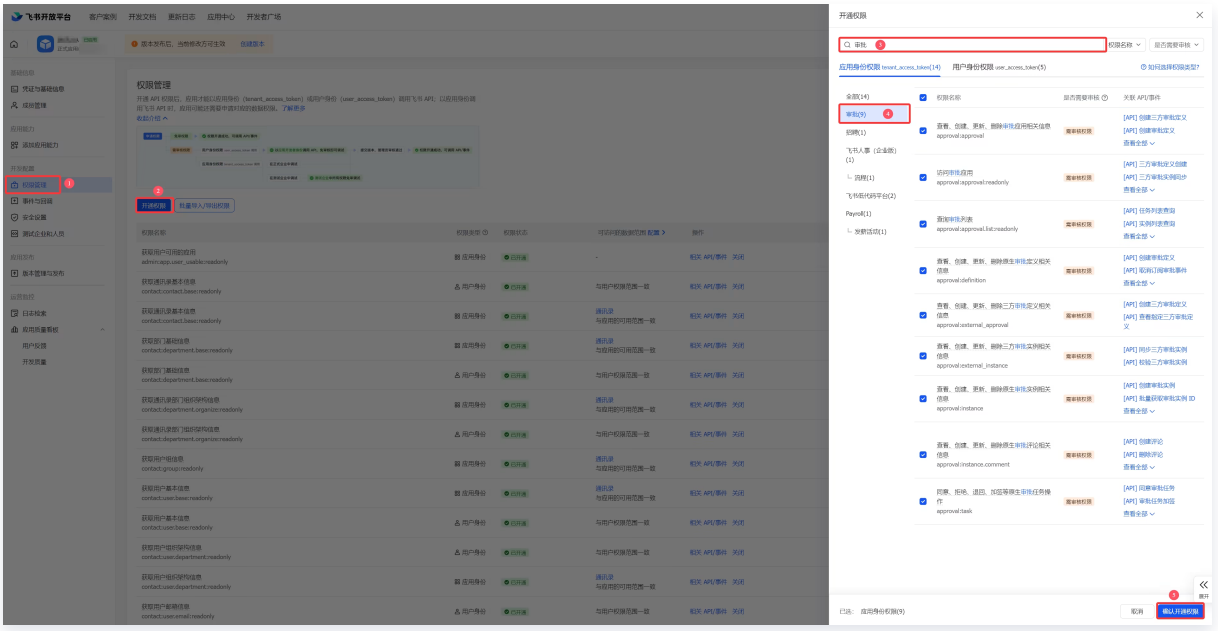


5.3.1 选择审批事件，勾选“审批实例状态变更”，“审批任务状态变更”，单击**确认添加**。

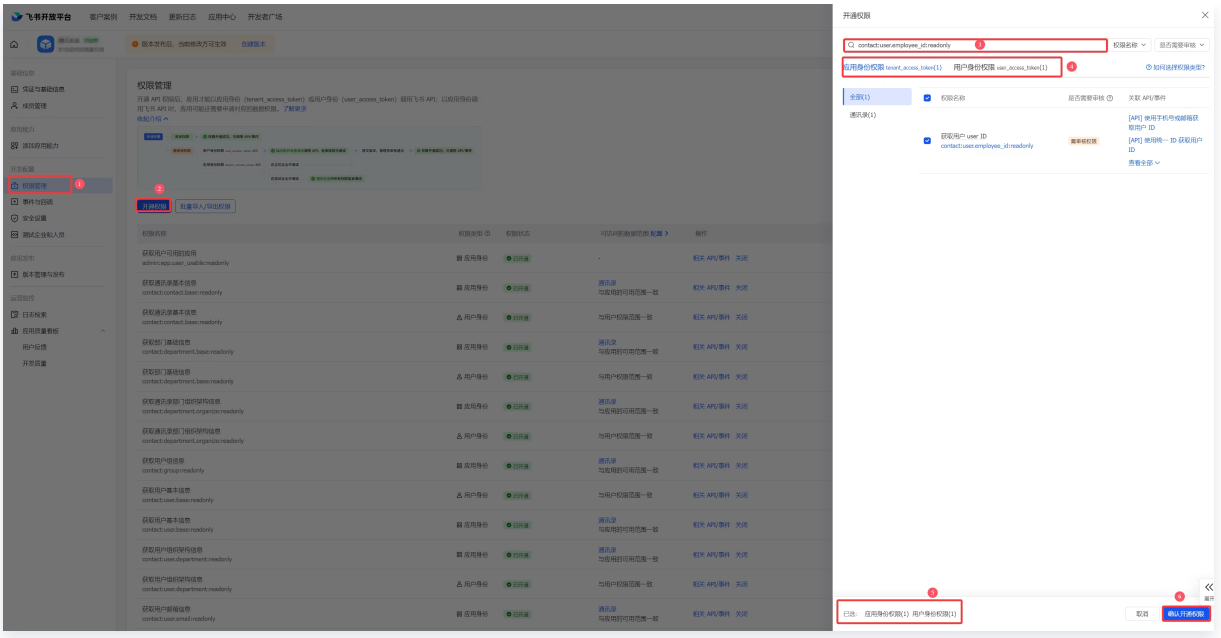


5.4 权限管理设置：

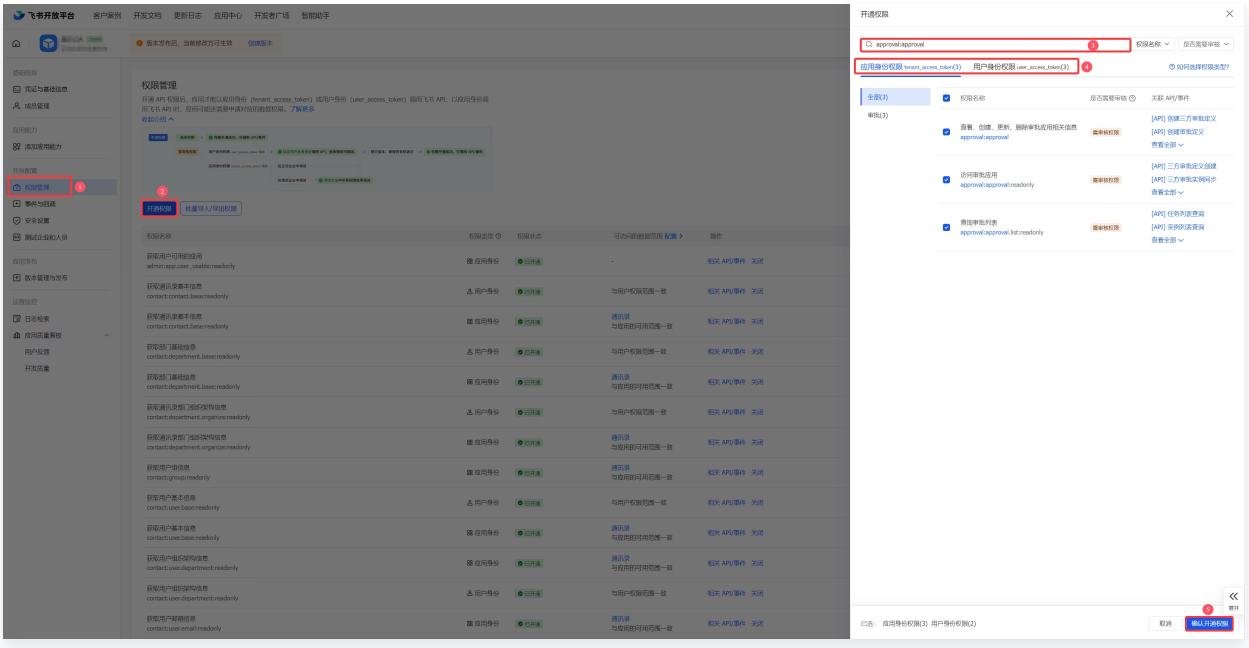
5.4.1 在**权限管理 > 开通权限**中，筛选审批，勾选**所有审批权限**，单击**确认开通权限**。



5.4.2 在**权限管理 > 开通权限**中，搜索框输入 contact:user.employee_id:readonly，**同时勾选应用身份权限和用户身份权限，单击确认开通权限。**

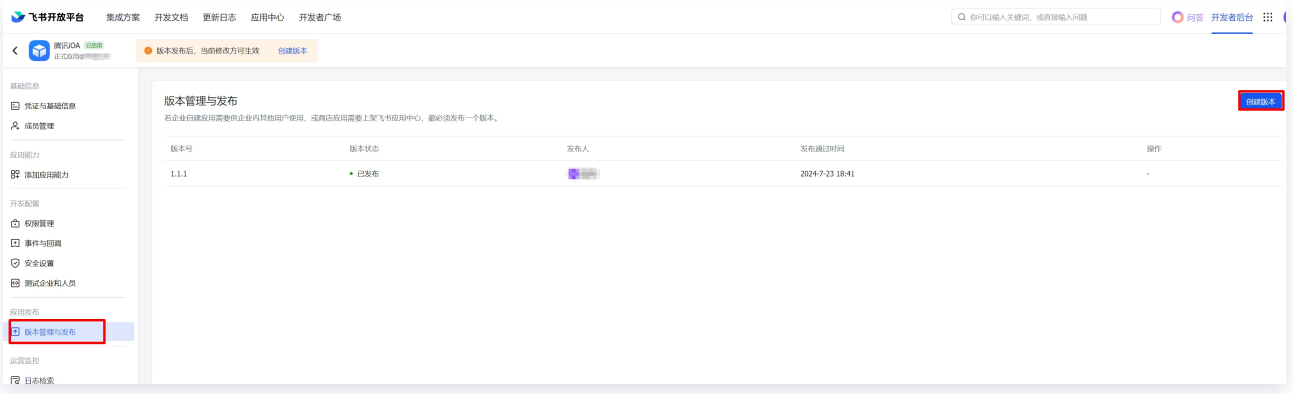


5.4.3 在**权限管理 > 开通权限**中，搜索框输入 approval:approval，**同时勾选应用身份权限和用户身份权限，单击确认开通权限。**



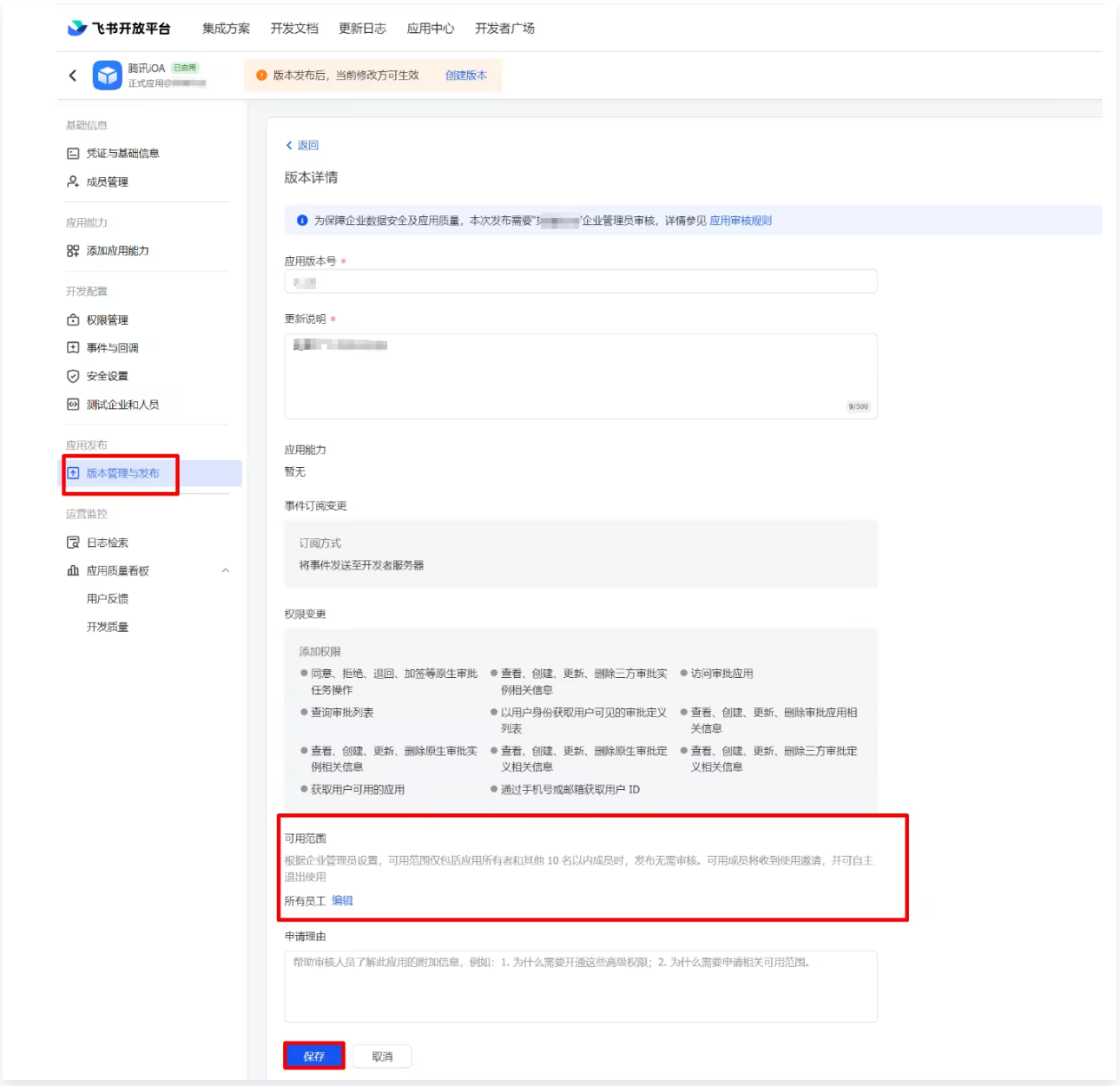
5.5 发布应用：在版本管理与发布页面，单击右上角的**创建版本**。

> **说明：**
> 配置权限后，需要重新发布应用才能生效。



5.6 在版本详情页面，填写应用版本号（格式如 1.0.0）和更新说明，设置可用性状态，单击**保存**。

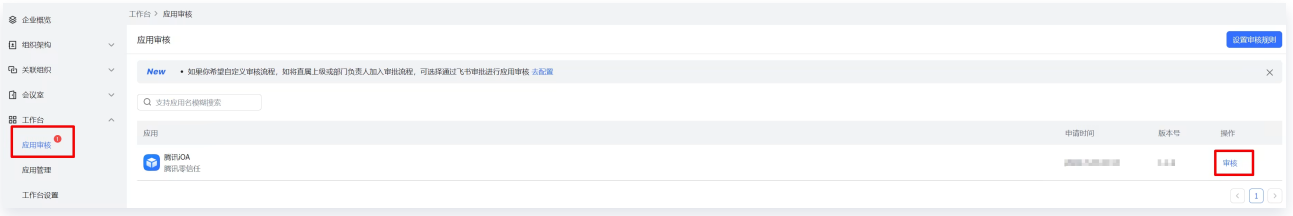
> ⚠ **注意：**
>
> 可用范围：选择所有员工（除非只同步指定部门）。



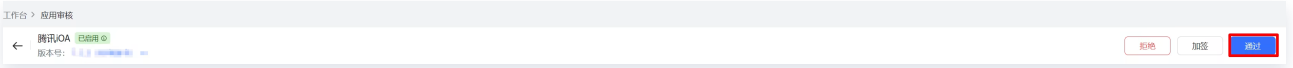
5.7 保存完成后，单击**申请线上发布**。



5.8 应用审核：管理员在 应用审核页面 ，选择目标应用，单击**审核**。



5.9 在审核详情页面，单击**通过**。



> **说明：**
>
> - 提交申请后，企业管理员会进行审核。
> - 审核结果会通过飞书和开发者后台发送给您。
> - 更多详情请见 飞书文档 – 开发企业自建应用 。

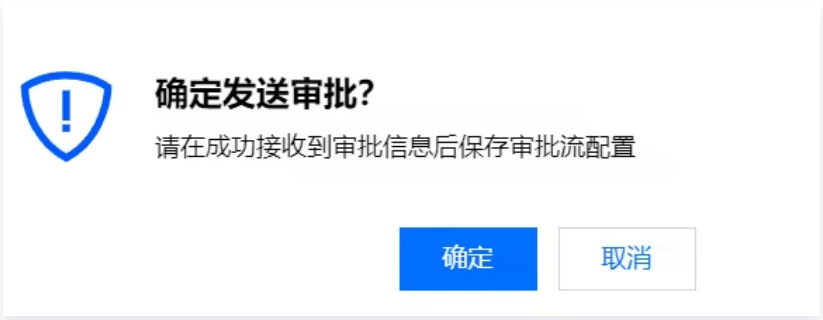
5.10 管理员应用审核通过后，自建应用状态显示为当前修改均已发布。



6. 飞书后台&审批流配置完成，在添加审批流页面，单击**测试**，发送审批流测试信息。



6.1 单击**确定**，发送审批测试信息。



6.2 飞书收到审批信息，审批流发起测试成功。



7. 单击**保存**，完成飞书审批流配置。

内部地址（11.1.1版）

最近更新时间：2026-02-13 09:41:02

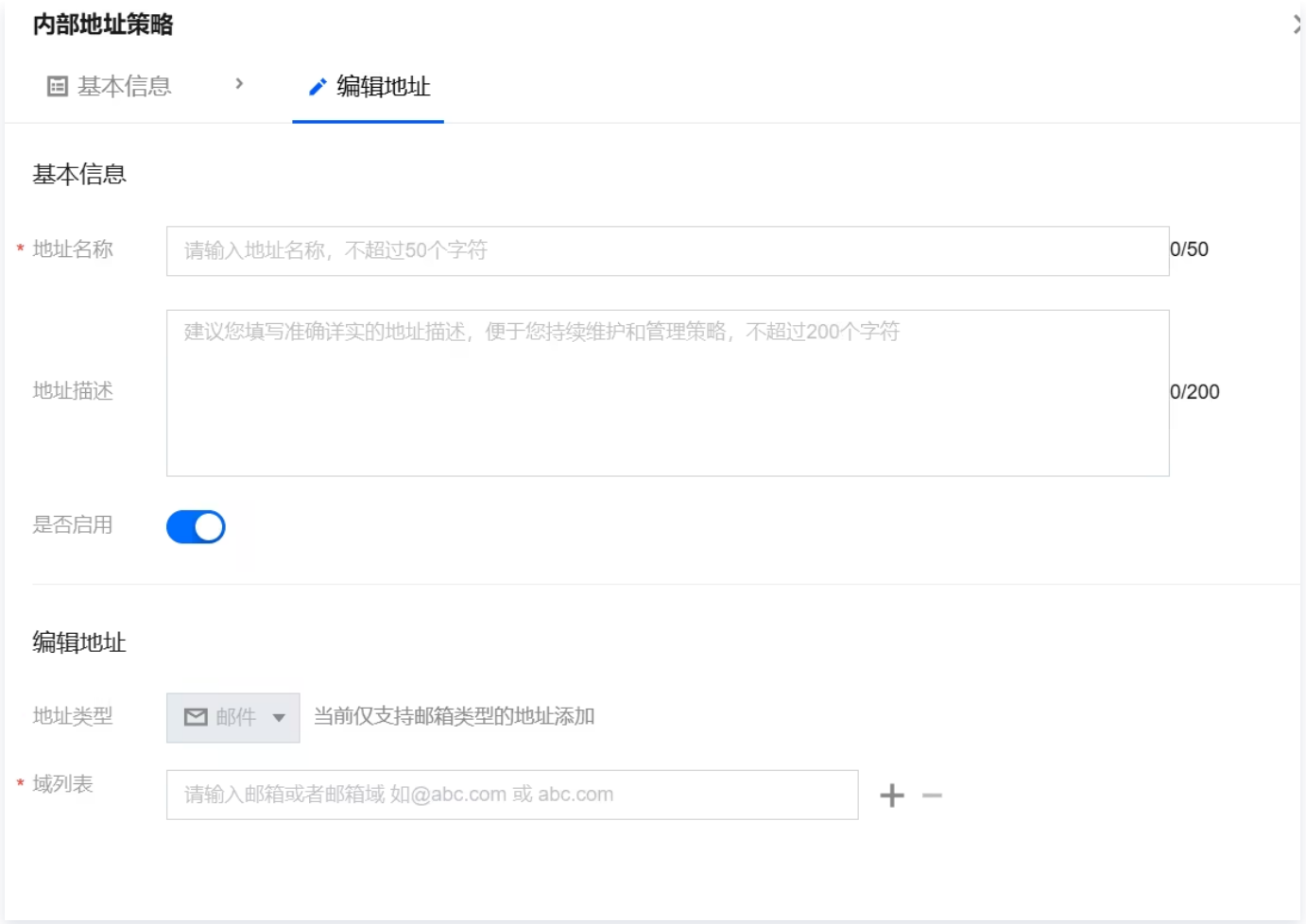
> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

配置和管理内部地址策略，填写必要信息并编辑地址，可对内部邮件进行有效管理和控制。iOA 支持在风险告警策略中豁免内部邮箱告警，并通过终端行为审计日志区分内外部邮箱审计。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略 > 内部地址**。
2. 在内部地址页面，单击**新建内部地址**。

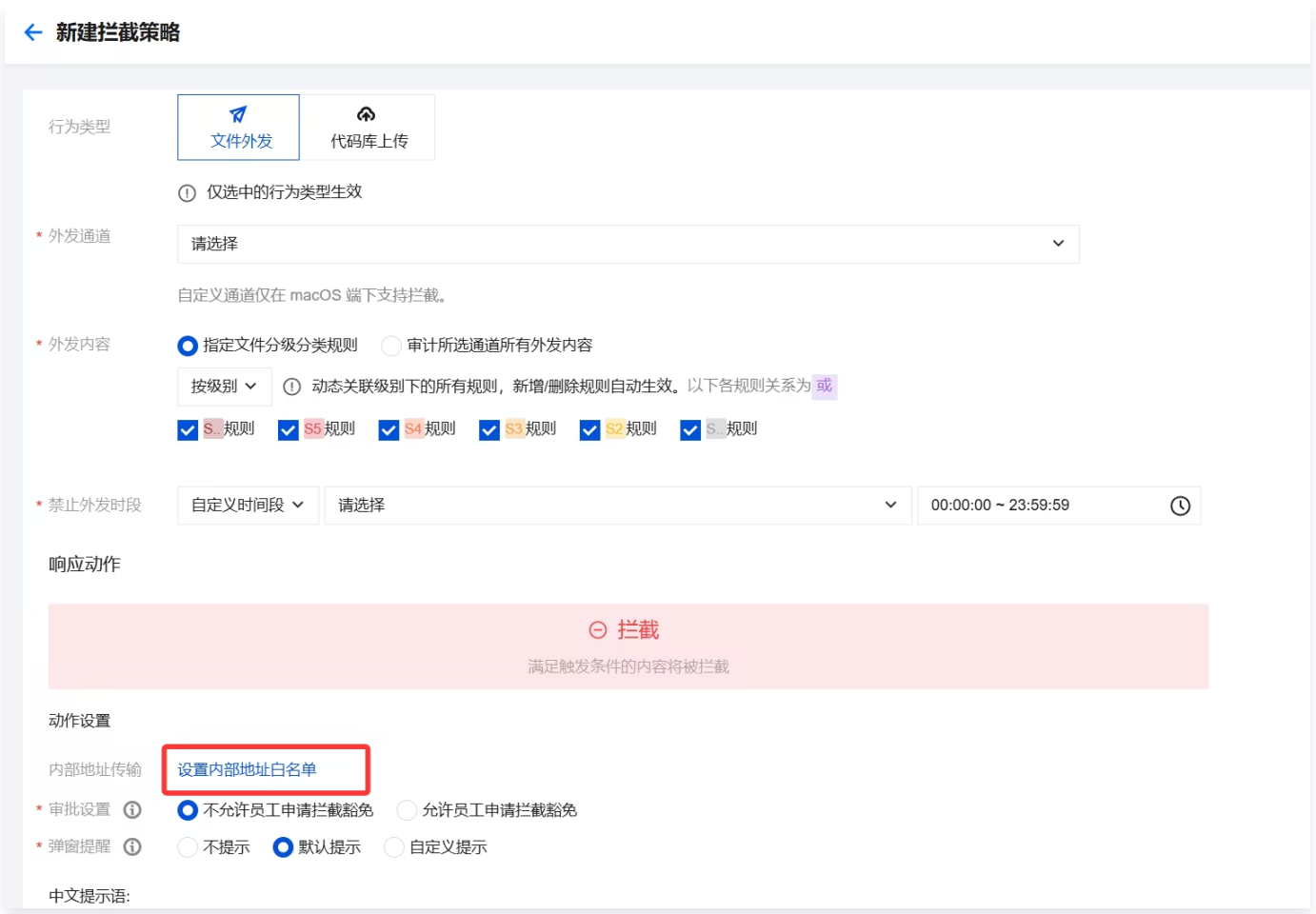


3. 在内部地址策略页面，配置基本信息等参数。



参数名称	说明
地址名称	自定义，不超过50个字符。
地址描述	自定义。
是否启用	是否开启此策略。
地址类型	邮件（当前仅支持邮箱类型的地址添加）。
域列表	请输入邮箱或者邮箱域，如 @abc.com 或 abc.com 。

4. 配置完成单击**保存**，配置的内部地址，用于**管控策略** > **管控策略** > **拦截策略/审计策略**，当发送通道为电子邮箱时，可配置内部地址，以实现内部地址不告警的能力。
5. 配置示例：邮件地址为 XX 公司邮箱，触发拦截策略的 XX 公司邮箱不产生拦截/审计。


新建拦截策略
行为类型
文件外发
代码库上传
仅选中的行为类型生效
* 外发通道
请选择
自定义通道仅在 macOS 端下支持拦截。
* 外发内容
指定文件分级分类规则
审计所选通道所有外发内容
按级别
动态关联级别下的所有规则，新增/删除规则自动生效。以下各规则关系为 或
S..规则
S5规则
S4规则
S3规则
S2规则
S..规则
* 禁止外发时段
自定义时间段
请选择
00:00:00 ~ 23:59:59
响应动作
拦截
满足触发条件的内容将被拦截
动作设置
内部地址传输
设置内部地址白名单
* 审批设置
不允许员工申请拦截豁免
允许员工申请拦截豁免
* 弹窗提醒
不提示
默认提示
自定义提示
中文提示语:

数据存储（11.1.1版）
存储目标策略（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **数据存储**。
2. 在数据存储页面，选择**存储目标策略**，单击**新建策略**。



3. 在存储目标策略页面，填写基本信息、适用范围和编辑策略。
   3.1 基本信息：输入策略名称、策略描述，并选择是否启用。



3.2 适用范围：该策略生效的对象范围。单击添加适用范围，勾选需管控/排除的用户/终端，单击确定。



3.3 定制文件分级存储：仅存储指定敏感级别的文件，例如：勾选所有文件级别，则当前存储所有级别的文件。



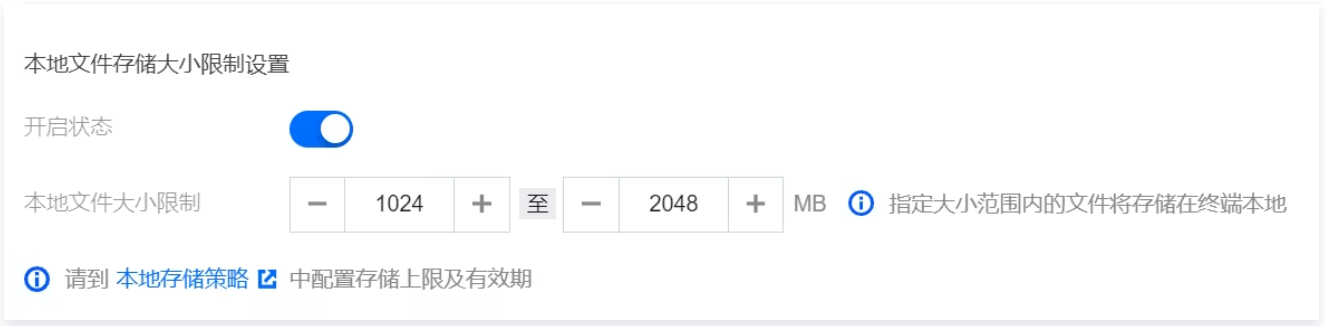
3.4 定制对应文件分级截屏取证：仅存储指定敏感级别的截图，例如：勾选S6，S5，S4级文件，则当前存储S6，S5，S4级文件的截屏取证图片。



3.5 文件存储大小设置：当开启 文件存储大小限制后，超过限制的文件将不保存（默认100MB，上限10G）。



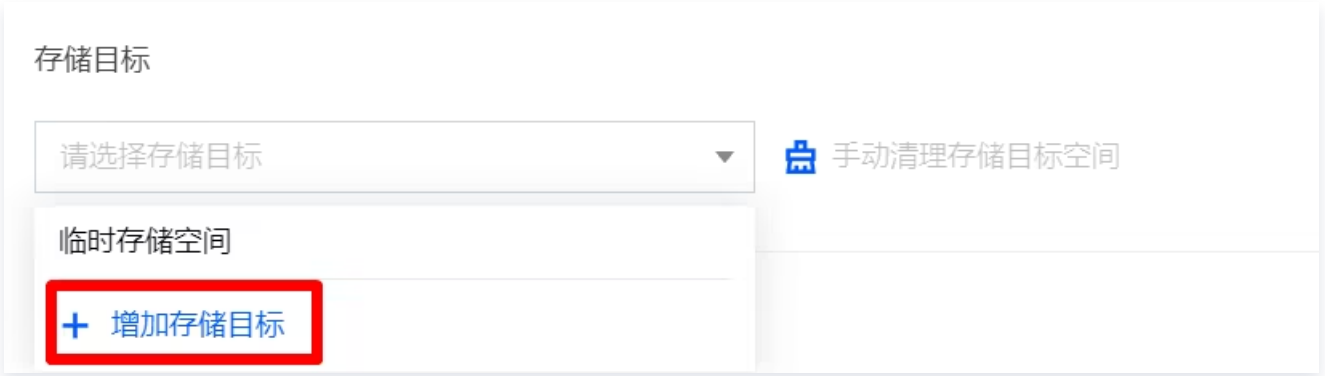
3.6 本地文件存储大小限制设置：支持在文件外发时将指定大小的文件存储到终端本地进行备份。



- 请到 本地存储策略 中配置存储上限及有效期。

3.7 存储目标：下拉选择存储目标，存储目标配置方式详情请参见 增加存储目标 。

> **说明：**
> 临时存储空间仅提供测试使用，请尽快使用自己的数据存储空间。



3.8 限定位置或出口 IP。

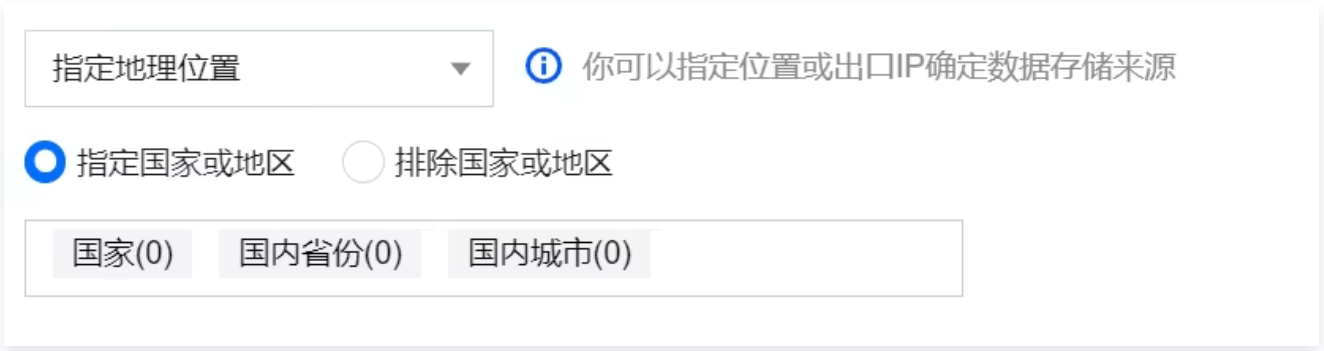
- 不指定地理位置或出口 IP：选择不指定地理位置或出口 IP，则不指定用户接入的地理位置/出口 IP。



- 指定出口 IP：存储支持按照 IP 段方式选择地区。



- **指定地理位置：指定国家或地区。**



- **指定国家或地区时，选择指定国家或地区，单击编辑，勾选国家/国内省份/国内城市后单击确定。**



- **排除国家或地区：选择排除国家或地区后，单击编辑，勾选国家/国内省份/国内城市后单击确定，则排除当前选择的国家或地区。**



- **指定网络位置：支持指定存储位置及 IP 限制，支持通过配置 IP/IP 段、选择网络所在网址或网络类型，以支持用户内外网或不同所在地公司使用不同存储目标的需要。**



4. **填写完成后，单击确定保存存储目标策略。**

存储目标管理（11.1.1版）

最近更新时间：2026-02-06 14:23:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

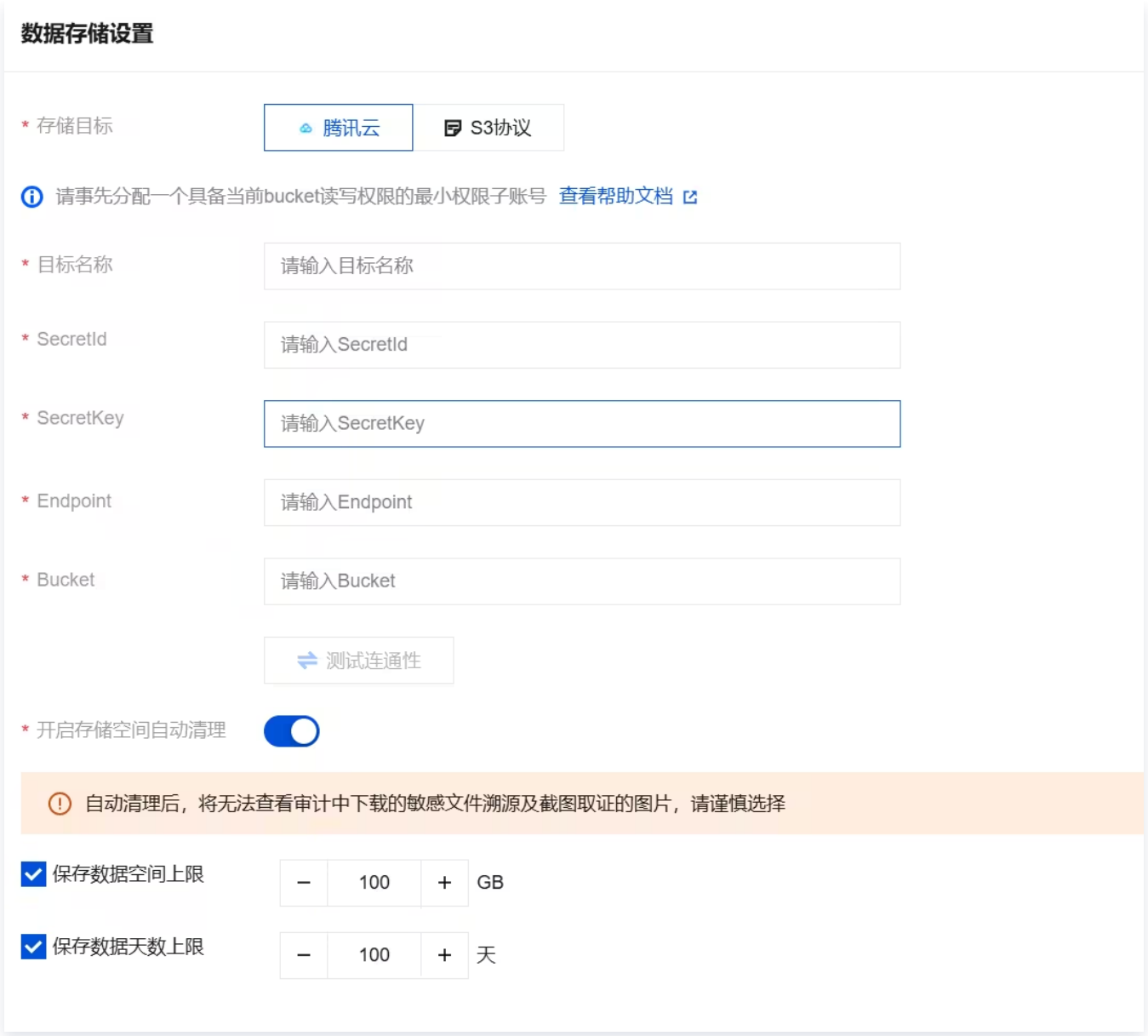
数据存储空间用于存储审计日志中的敏感文件和取证截图。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **数据存储**。
2. 在数据存储页面，选择**存储目标管理**，单击**添加存储目标**。



> **说明：**
> 我们为您提供了10GB的临时存储空间，仅供测试使用。请您尽快切换至自己的数据存储空间进行功能测试。

3. 在数据存储设置页面，选择存储目标，获取配置参数请参考 配置腾讯云存储服务 和 配置 S3协议存储服务。



配置腾讯云存储服务

步骤1：新建存储桶

> **说明：**
> 如您未开通腾讯云对象存储服务，请前往腾讯云开通 对象存储 COS 。

存储桶用于存储 iOA 审计日志中的敏感文件和取证截图。

1. 登录 对象存储控制台 ，在左侧导航栏，选择 存储桶列表 。



2. 在存储桶列表页面，单击**创建存储桶**，新建一个存储桶。
3. 在创建存储桶窗口中，配置基本信息，单击**下一步**。



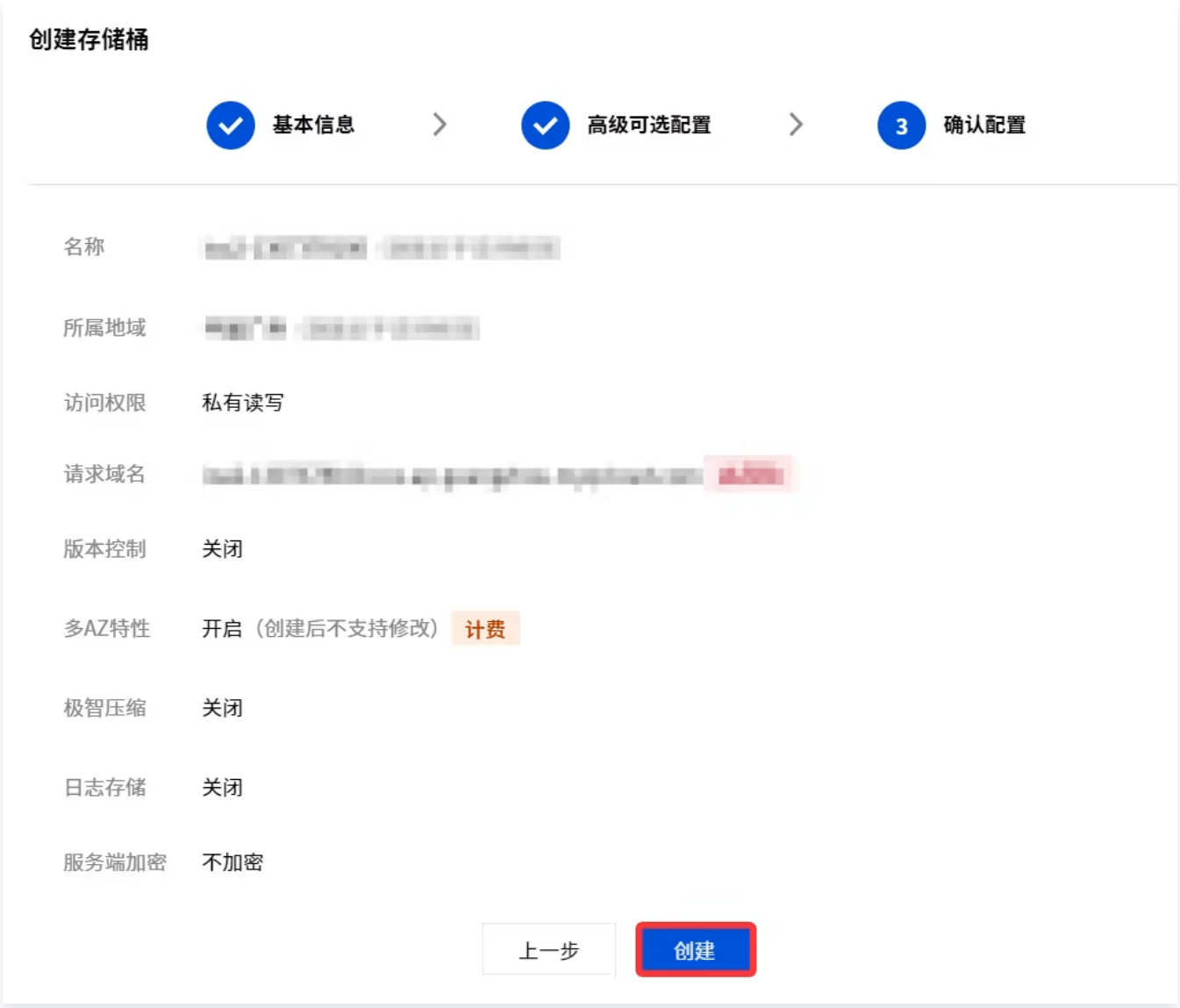
参数名称	说明
所属地域	选择所属地域，存储桶与相同地域的其他腾讯云服务内网互通，地域一旦选择，无法修改，请谨慎选择。
名称	填写存储桶名称，名称一旦创建，无法修改，请谨慎填写。
访问权限	可在私有读写、公有读私有写、公有读写3种访问权限中进行选择。**建议配置：私有读写权限**
多 AZ 特性	• 部分地域支持多 AZ 特性，对于不支持的地域，可通过设置存储桶跨区域复制功能。 • 多AZ特性允许用户将数据存储在同地理区域内的不同物理位置，提供同城容灾功能，推荐开启。

4. 在高级可选配置页签中，根据实际需求选择功能，单击**下一步**。



参数名称	说明
版本控制	可选择是否开启版本控制，开启版本控制后可以恢复因覆盖或误删丢失的数据。
极智压缩	极智压缩是在保证画质的前提下，尽可能地减小图片大小的功能。开启后，每次访问桶内的 JPG/PNG/GIF 格式的图片时将会实时压缩。
日志存储	可选择是否开启日志存储，开启后可记录跟存储桶操作相关的各种请求日志。
存储桶标签	支持输入标签键和标签值，可创建50个标签。
服务端加密	可选择不加密，或 SSE-COS 加密。

5. 配置信息确认无误后，单击**创建**，完成存储桶的创建。

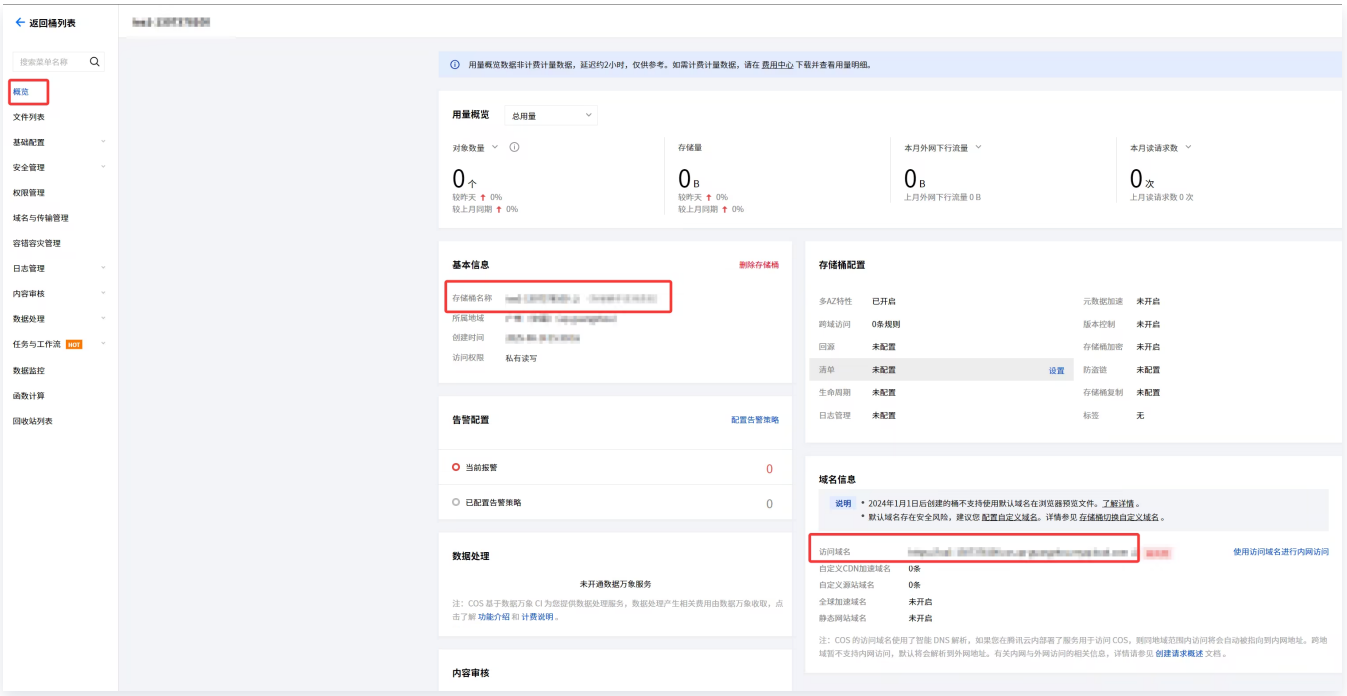


步骤2：获取 Bucket 和 Endpoint 参数

1. 完成存储桶的创建后，在 存储桶列表页面 ，单击**存储桶名称**，进入存储桶详情页面。



2. 单击**概览**，查看存储桶的概览页。找到**存储桶名称**和**访问域名**，分别作为 Bucket 和 Endpoint 参数。

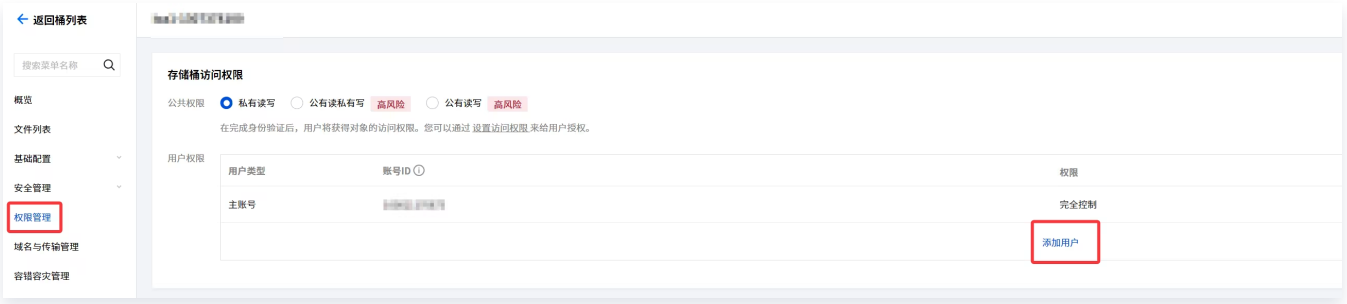


步骤3：为存储桶分配最小权限的子账号

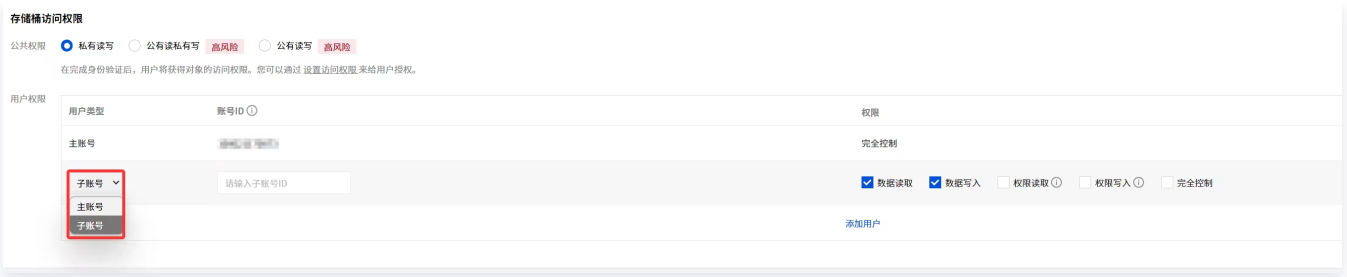
1. 完成存储桶创建后，在 存储桶列表页面 ，单击**存储桶名称**，进入存储桶详情页面。



2. 在存储桶详情页面，单击**权限管理 > 存储桶访问权限**。
3. 在存储桶访问权限页面，单击**添加用户**。



4. 添加用户时选择**子账号**，输入子账号 ID 并选择**数据读取**、**数据写入**两个权限，单击**确定**，即可为此存储桶分配一个具有读写权限（最小权限）的子账号。

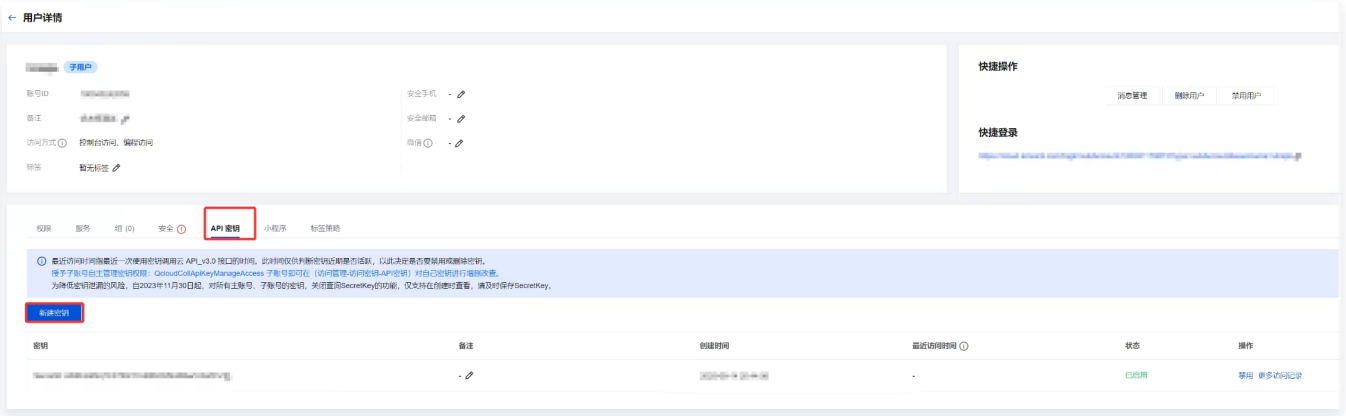


步骤4：获取子账号的 SecretId 和 SecretKey

1. 登录 访问管理控制台，在左侧导航栏，选择**用户 > 用户列表**。
2. 在用户列表页面，找到刚刚为存储桶分配的子账号，单击**用户名称**。



3. 在用户详情页面，单击 **API 密钥 > 新建密钥**，获取子账号的 SecretId 和 SecretKey。



步骤5：回到 iOA 控制台，测试连通性

1. 完成各参数的获取后，返回 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **数据存储**。
2. 在数据存储设置页面，选择 存储目标管理，单击**添加存储目标**。



3. 存储目标选择**腾讯云**，依次填写上述获取的 SecretId 和 SecretKey、访问域名、存储桶名称。



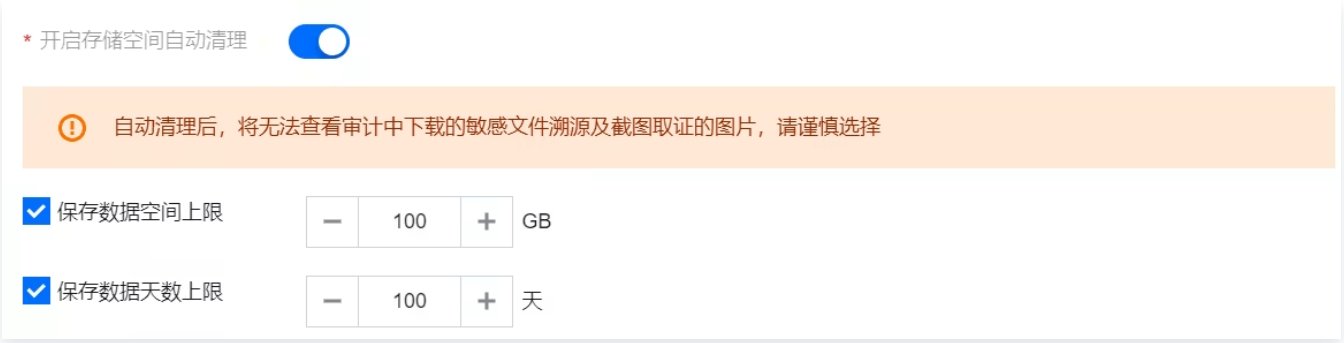
参数名称	说明
存储目标	腾讯云。
目标名称	自定义。
SecretId	步骤4 获取的子账号 SecretId。
SecretKey	步骤4 获取的子账号 SecretKey。
Endpoint	步骤2 获取的存储桶访问域名。
Bucket	步骤2 获取的存储桶名称。

4. 开启存储空间自动清理

该方式会自动清除符合条件的数据内容，如下图示例配置：存储容量超过100GB或存储时间超过100天，则自动清理。

> ⚠ **注意：**

- 仅配置**保存数据空间上限**时，存储数据到达上限采用滚动清理方式，即按照时间顺序，从最早的文件开始删除。
- 自动清理后，将无法查看审计记录中的敏感文件溯源及截图取证的图片，请谨慎选择。



5. 填写完成后，单击**测试连通性**，若提示**测试成功**，即配置完成。

配置 S3 协议存储服务

说明：
请事先分配一个具备当前 Bucket 读写权限的最小权限子账号。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **数据存储**。
2. 在数据存储设置页面，选择**存储目标管理**，单击**添加存储目标**。



3. 存储目标选择 **S3协议**，依次填写**目标名称**、**AccessKeyId** 和 **SecretAccessKey**、**Endpoint**、**Bucket**。

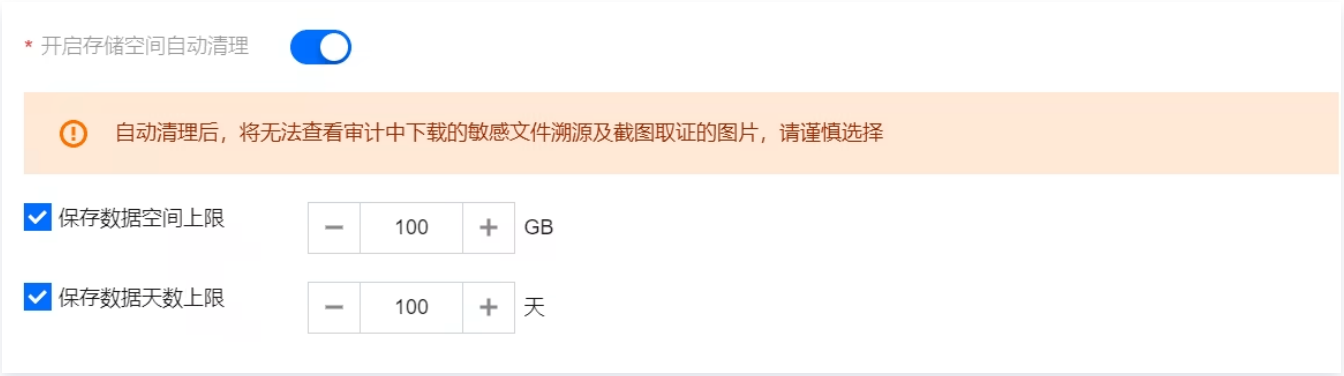


参数名称	说明
存储目标	S3协议。
目标名称	自定义。
AccessKeyId	唯一标识符，用于识别访问云存储服务的用户或应用程序。它通常与 SecretAccessKey 配合使用，以便在对云存储服务进行身份验证时提供安全访问。
SecretAccessKey	与 AccessKeyId 配对的私钥，用于对云存储服务进行身份验证。当创建一个新的 AccessKeyId 时，系统会自动生成一个与之关联的 SecretAccessKey。
Endpoint	云存储服务的 API 访问点。它是一个 URL，用于指向服务的特定区域和访问路径。客户端通过这个 URL与云存储服务进行通信。
Bucket	Bucket 名称。 Bucket 是云存储服务中的一个基本容器，用于存储和组织数据。

4. 开启存储空间自动清理：该方式会自动清除符合条件的数据内容，如下图示例配置：存储容量超过100GB或存储时间超过100天，则自动清理。

> ⚠ 注意：

- 仅配置**保存数据空间上限**时，存储数据到达上限采用滚动清理方式，即按照时间顺序，从最早的文件开始删除。
- 自动清理后，将无法查看审计记录文件溯源及截图取证的图片，请谨慎选择。



5. 单击**测试连通性**，若提示**测试成功**，即配置完成。

本地存储策略（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **数据存储**。
2. 在数据存储设置页面，选择 **本地存储策略**，单击**新建策略**。



3. 在本地存储页面，填写基本信息、适用范围和编辑策略。
   3.1 基本信息：输入策略名称、策略描述，并选择是否启用。



3.2 适用范围：该策略生效的对象范围。单击**添加适用范围**，勾选需管控/排除的用户/终端，单击**确定**。



3.3 本地最大存储上限：设置终端本地最大存储上限，超过最大存储上限后将按时间顺序清除本地文件。



3.4 本地最大存储时间：设置终端本地最大存储时间，超过最大存储时间后将按时间顺序清除本地文件。

3.5 配置本地文件存储范围参见：存储目标策略 。

4. 填写完成后，单击**保存**。

版权所有：腾讯云计算（北京）有限责任公司

文件鉴定（11.1.1版）
文件鉴定使用指引（11.1.1版）

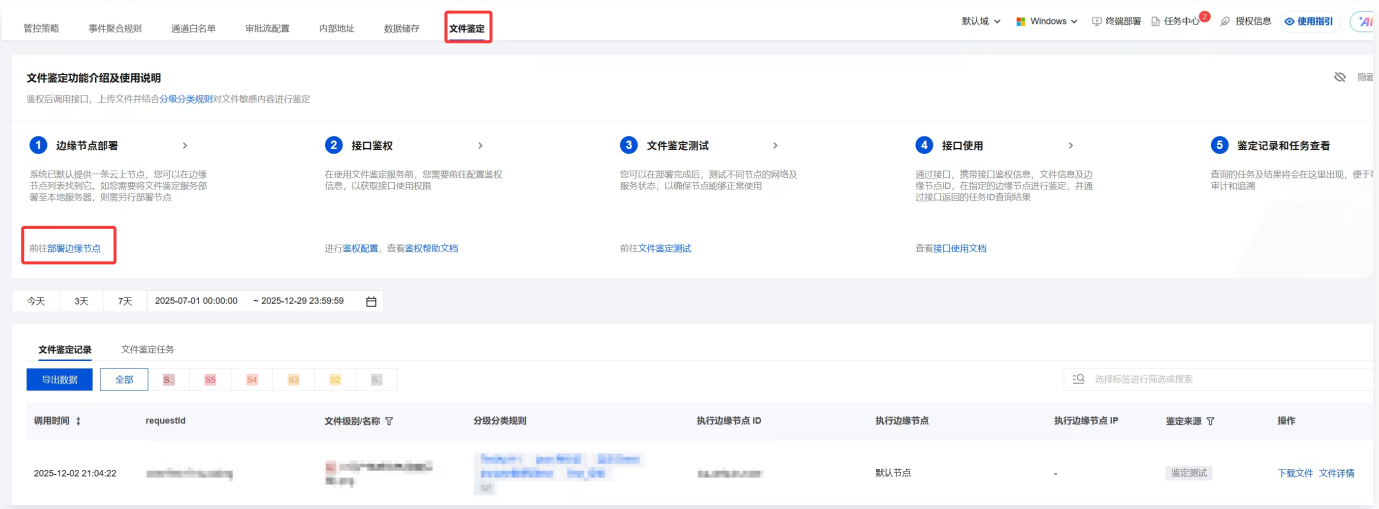
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

文件鉴定可选择在私有化本地服务器上部署边缘节点，以实现数据不出本地网络的情况下进行鉴定的功能，鉴定时将根据分级分类规则识别文件中的敏感信息（如身份证号、银行卡号、商业机密等）并通过接口输出鉴定结果；若未部署边缘节点，则默认使用系统自带的服务（需上传文件至外部服务器）进行文件鉴定。

部署边缘节点

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **文件鉴定**。
2. 在文件鉴定页面，单击**部署边缘节点**，即可在企业内部部署边缘节点（私有化文件鉴定服务），确保数据不出本地网络。详情请参见 部署边缘节点。



鉴权配置

配置 API 密钥用于 API 调用。如需了解鉴权，详情请参见 签名方法 v3。



文件鉴定测试

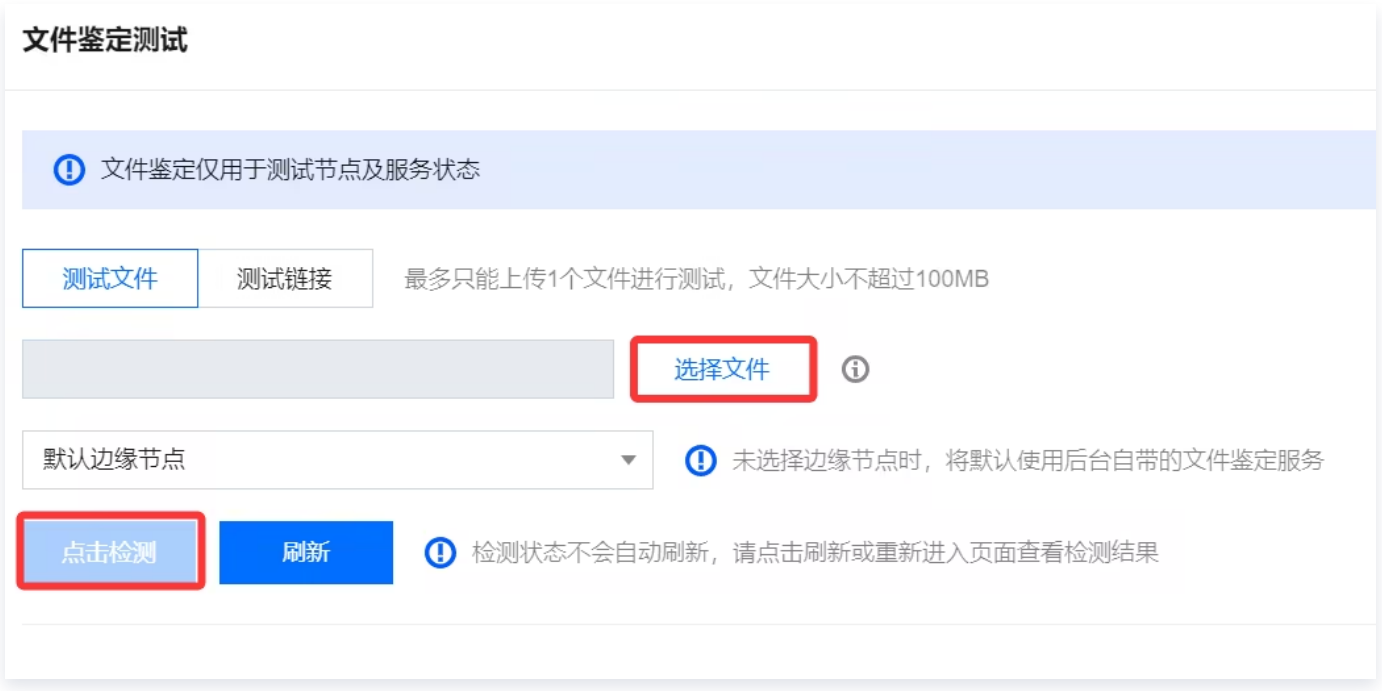
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **文件鉴定**。
2. 在文件鉴定页面，单击**文件鉴定测试**，在边缘节点部署完成后，测试不同节点的网络及服务状态，以确保节点能够正常使用。



3. 在文件鉴定测试页面，可上传文件或链接以测试节点及服务状态。

   3.1 测试文件：单击**选择文件**，上传文件后单击**检测**，检测连通状态。

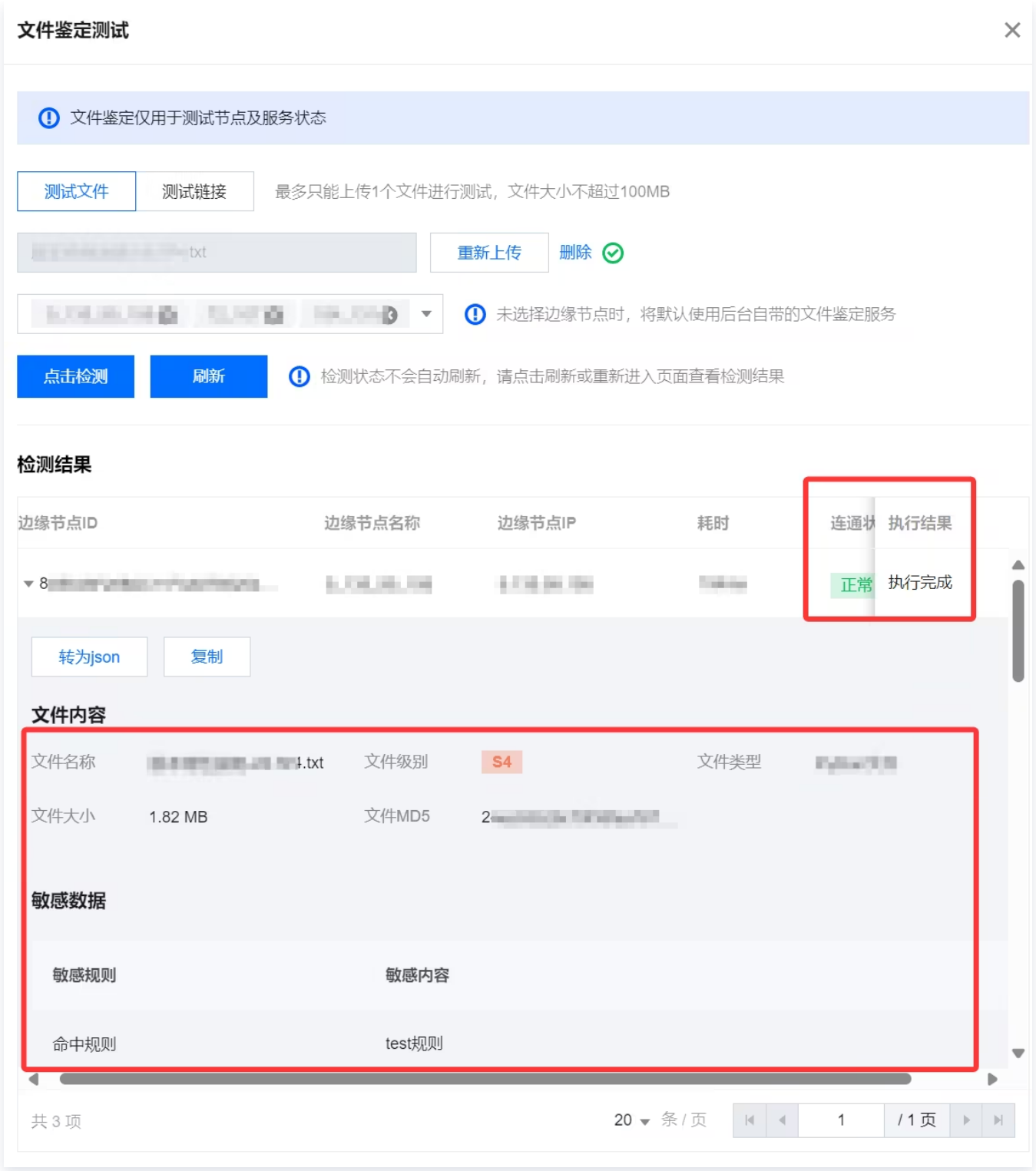
> **说明：**
> 内网终端上传文件，需放通地址，放通内网访问 iOA 服务的域名后可实现内网上传文件。详情请参见 放通地址。



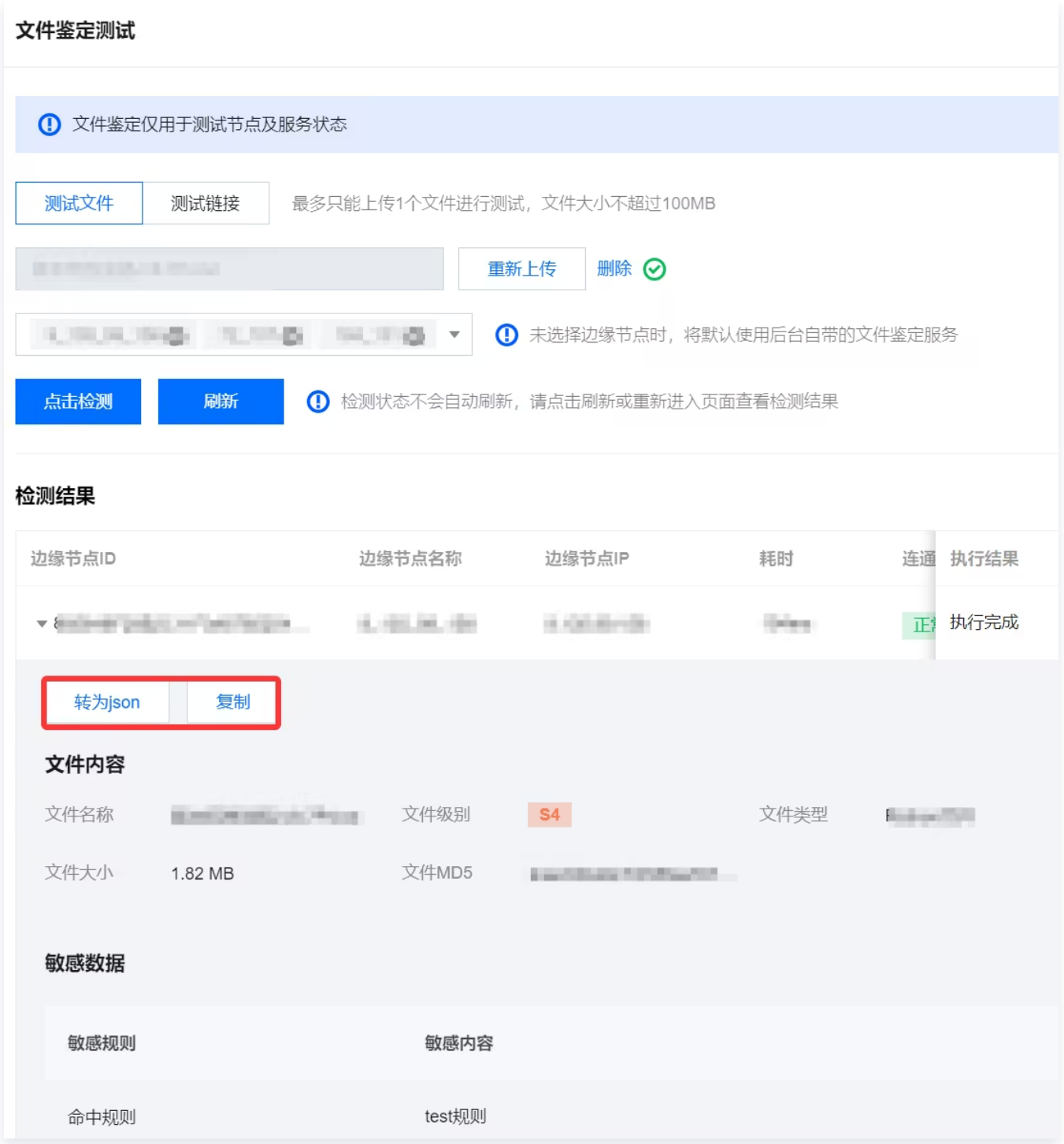
3.2 测试链接：填写需要鉴定文件的链接后单击**检测**，检测连通状态。



4. 查看检测结果：单击 ▶ 展开，查看文件名称、连通状态等，连通状态为正常，则符合预期。



5. 转为 JSON：该功能用于将系统的文件鉴定结果从网页的可视化格式，一键转换为标准化的 JSON（JavaScript Object Notation）数据格式（如文件 MD5、命中规则），结合**复制**按钮，可快速将 JSON 数据粘贴至其他系统。



接口使用

通过接口，携带接口鉴权信息，文件信息及边缘节点 ID，在指定的边缘节点进行鉴定，并通过接口返回的任务 ID 查询结果。详情请参见： 文件鉴定接口使用指引 。

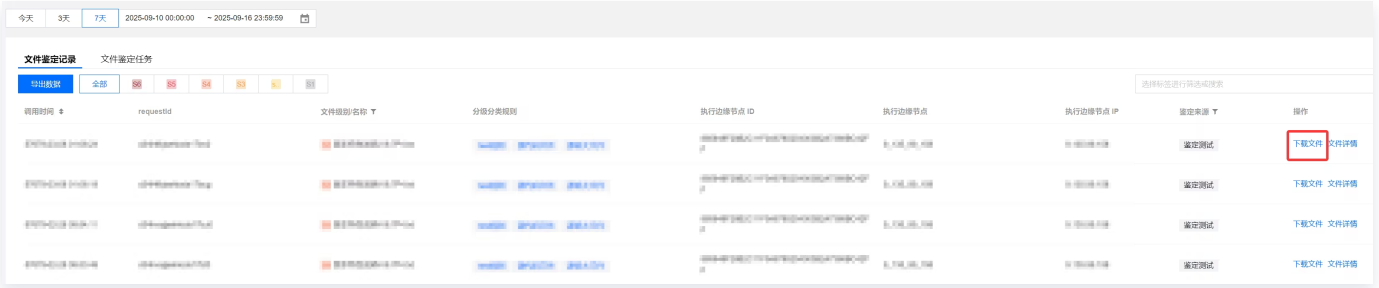
文件鉴定记录和任务查看

文件鉴定记录

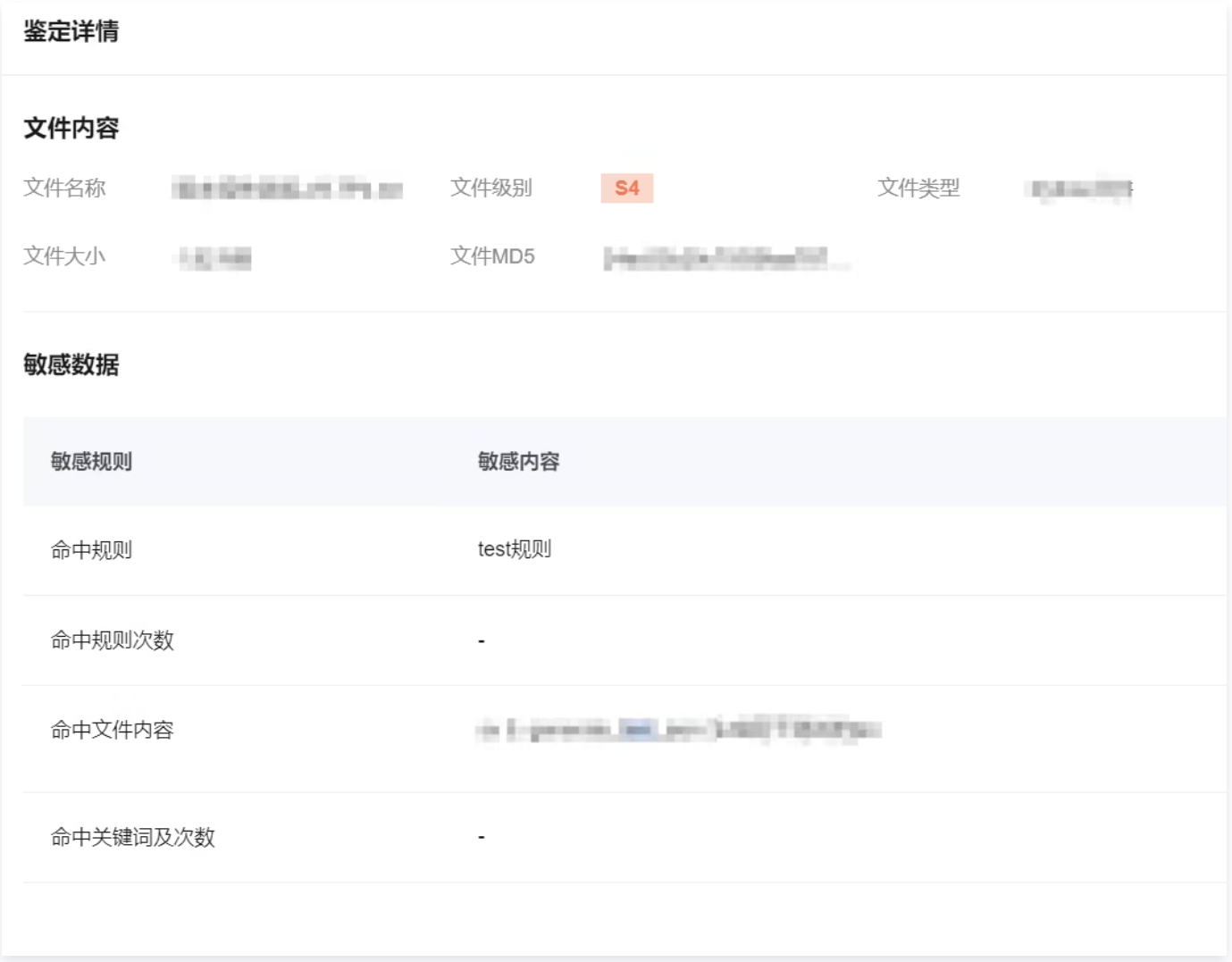
记录执行完成后产生上报日志，提供文件鉴定历史操作的全量审计与追溯能力，用于存储和展示所有用户发起的文件鉴定任务及其最终结果。您可通过此功能：

- 鉴定审计：查阅任意历史时间点的文件鉴定操作，包括鉴定人、鉴定文件、鉴定时间及结果详情。
- 结果复查：对已完成的鉴定任务进行二次检查或确认，用于事件复盘或合规性审查。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **文件鉴定**。
2. 在文件鉴定页面，选择**文件鉴定记录**，单击**下载文件**，可将用户提交的、已完成鉴定的原始文件下载至管理员本地设备（若管理员无权限，则在下载文件时提示失败）。



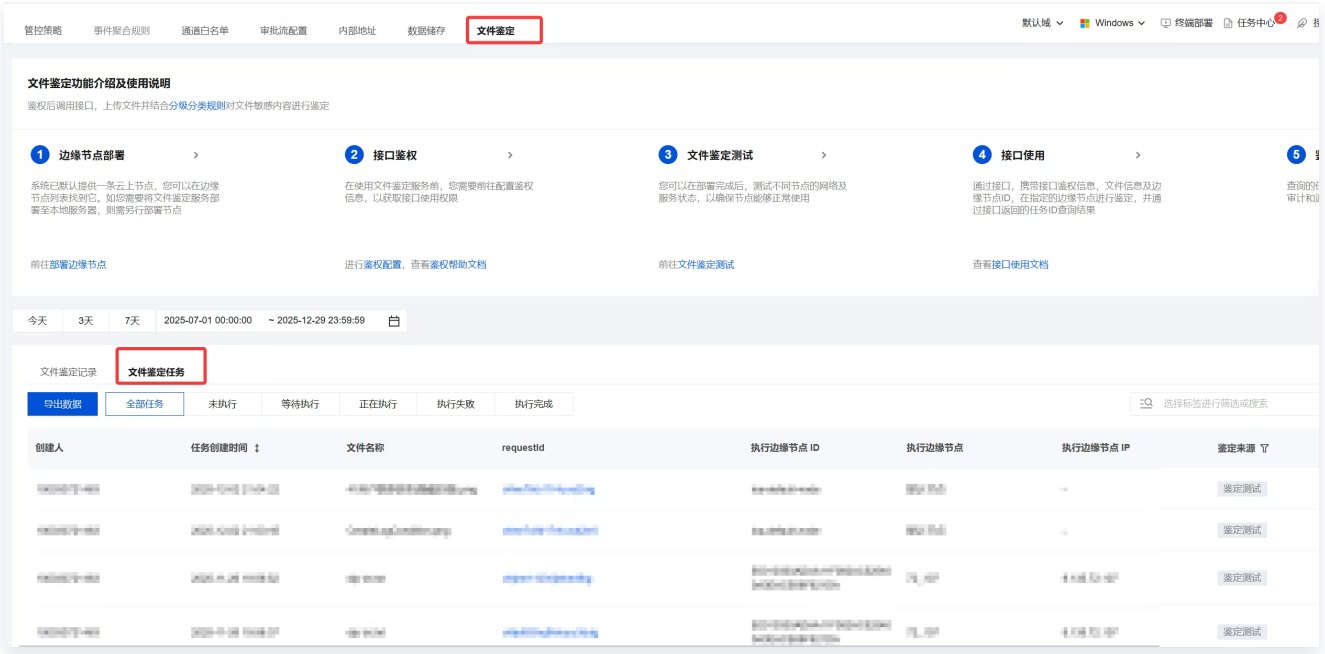
3. 单击**文件详情**，展示该次文件鉴定任务的全过程详细信息与判定依据。



文件鉴定任务

调用创建鉴定任务的时候，就会有鉴定记录，例如：调用接口就会创建鉴定任务，提供对鉴定任务生命周期的实时监控与主动管理能力。

1. 登录 iOA 零信任管理平台控制台 ，在左侧导航栏，选择**管控策略** > **文件鉴定** 。
2. 在文件鉴定页面，选择**文件鉴定任务**，以“任务”为维度，实时展示所有鉴定请求的当前状态。管理员可通过此功能及其状态筛选器（全部任务/未执行/等待执行/正在执行/执行失败/执行完成）：
   - 全局监控：一键总览所有任务的整体健康状态。
   - 精准筛选：快速定位到特定状态的任务进行处理。
   - 未执行/等待执行：用于排查因队列堆积、资源不足等原因导致的延迟任务。
   - 正在执行：实时监控当前系统处理进度。
   - 执行失败：快速发现并集中处理失败任务，排查失败原因（如文件过大、网络超时、节点失联等）。
   - 执行完成：快速查看最新已成功处理的任务结果。



部署边缘节点（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

将边缘文件鉴定系统部署在用户本地，结合接口方案，当收到文件鉴定任务时，使用用户本地部署的文件鉴定系统进行识别，给出对应文件的敏感内容，并通过 API 接口给出文件鉴定结果。用户可自行调用接口，并利用结果在 OA 系统进行审批。若未部署边缘节点，则默认使用部署在 iOA 后台的文件鉴定能力。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **文件鉴定**。
2. 在文件鉴定页面，单击**部署边缘节点**。



边缘节点部署教学

为保障边缘节点与云端服务之间通信，您需要在服务器防火墙的出方向放行以下地址及端口。**强烈建议优先使用域名方式进行配置**，以应对后端IP地址可能发生的变更。

步骤1：放通地址

核心服务地址为建立连接、传输数据和升级所需访问的所有关键云端服务的具体地址。请根据下表，在您的服务器防火墙策略中，为出方向流量添加允许规则，放通上述域名和端口。

名称	地址	类型
节点服务地址	edge-ws1.ioa-sec.tencent.com:8080	TCP
升级节点地址	dlp-cos1.ioa-sec.tencent.com:443	TCP
控制面上报数据地址（总控地址）	scs.gateway.tencent.com:443	TCP

步骤2：边缘节点部署教学

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **文件鉴定**。

2. 在文件鉴定页面，单击**部署边缘节点**。



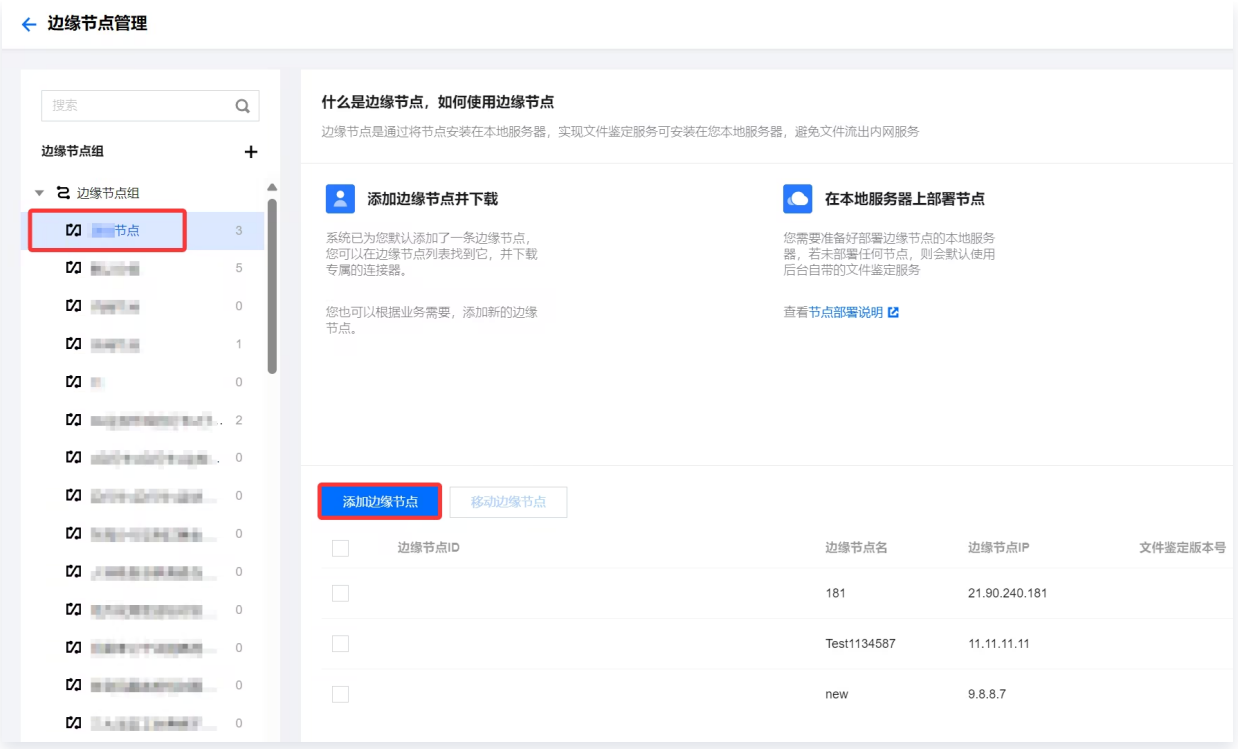
3. 在边缘节点管理页面，单击**边缘节点组右侧的+** 。



4. 在节点组管理窗口中，设置节点组名称后，单击**确定**保存。



5. 在新建的边缘节点组下，单击**添加边缘节点**。

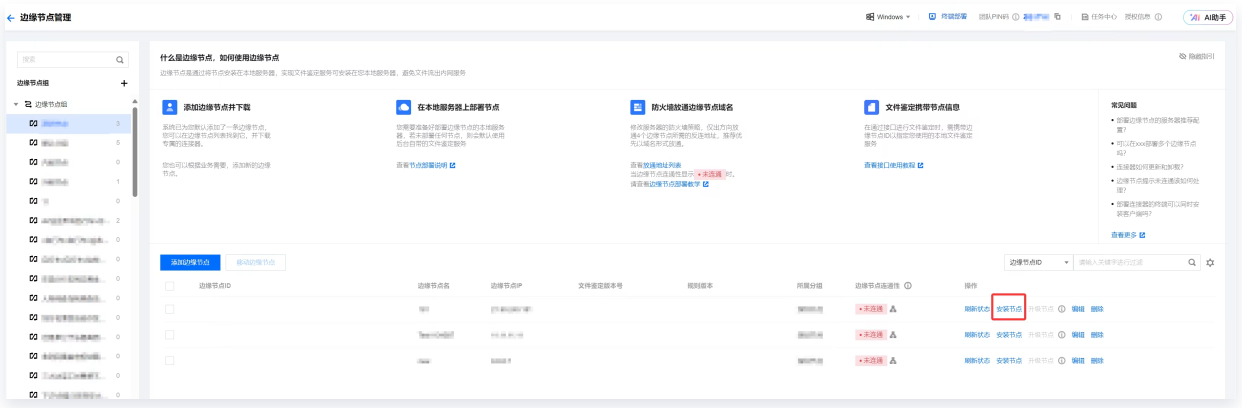


6. 配置节点 IP 等信息，配置完成单击**确定**保存。



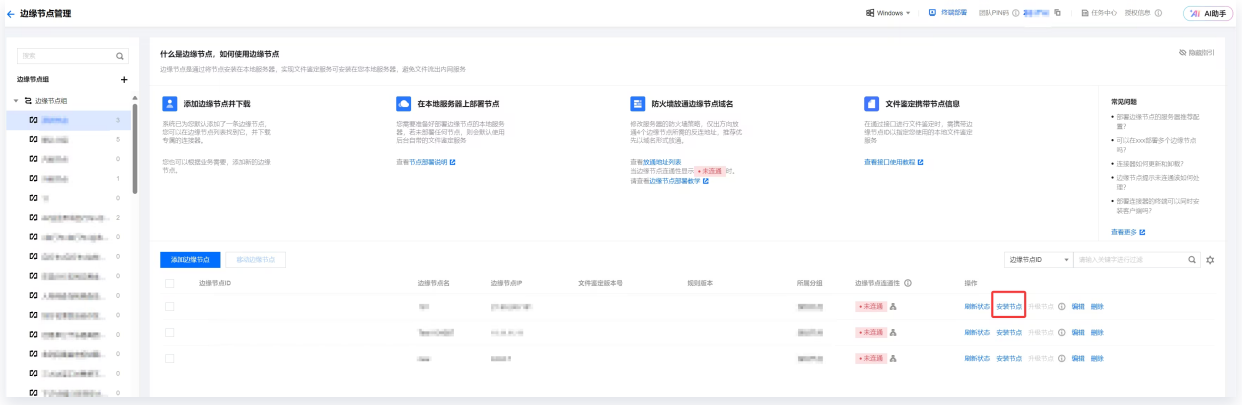
参数名称	说明
节点名称	自定义节点名称。
节点组	自定义选择节点组。
节点 IP	填写部署边缘节点服务器的 IP。

7. 在创建的节点中，单击**安装节点**，支持将命令行复制到服务器上进行在线安装与离线安装。



方式1：在线安装

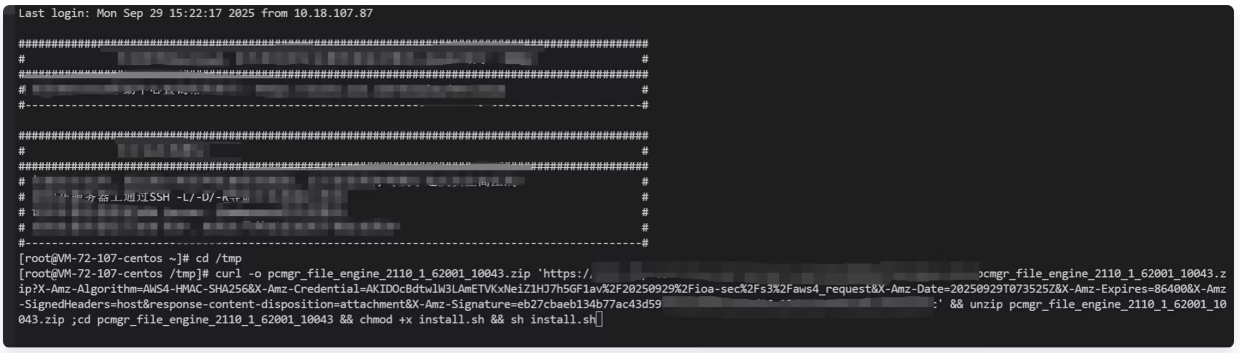
1. 登录 iOA 零信任管理平台控制台 ，在左侧导航栏，选择**管控策略** > **文件鉴定** 。
2. 在文件鉴定页面，单击**部署边缘节点**。在创建的节点中选择目标节点，单击**安装节点**。



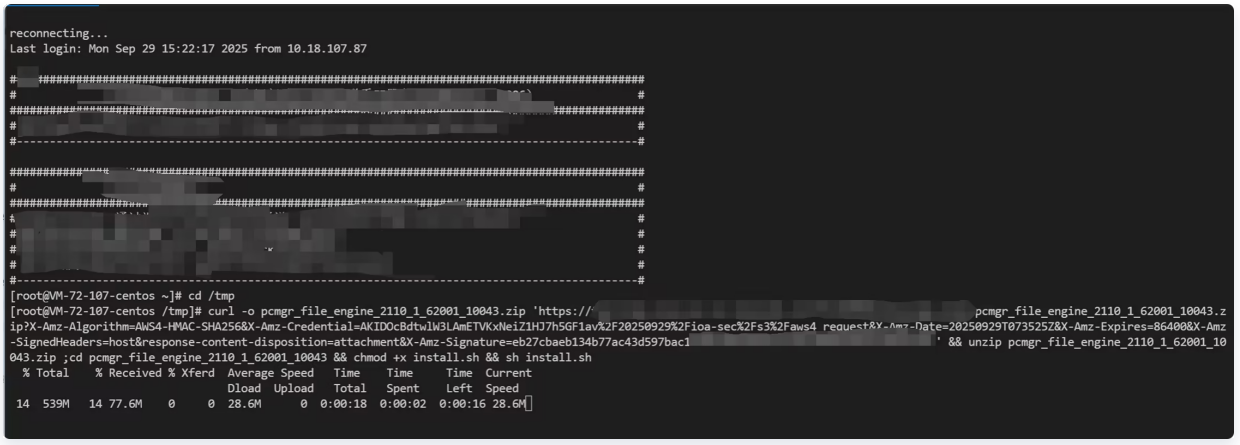
3. 单击 复制，将命令行复制到服务器上进行安装。



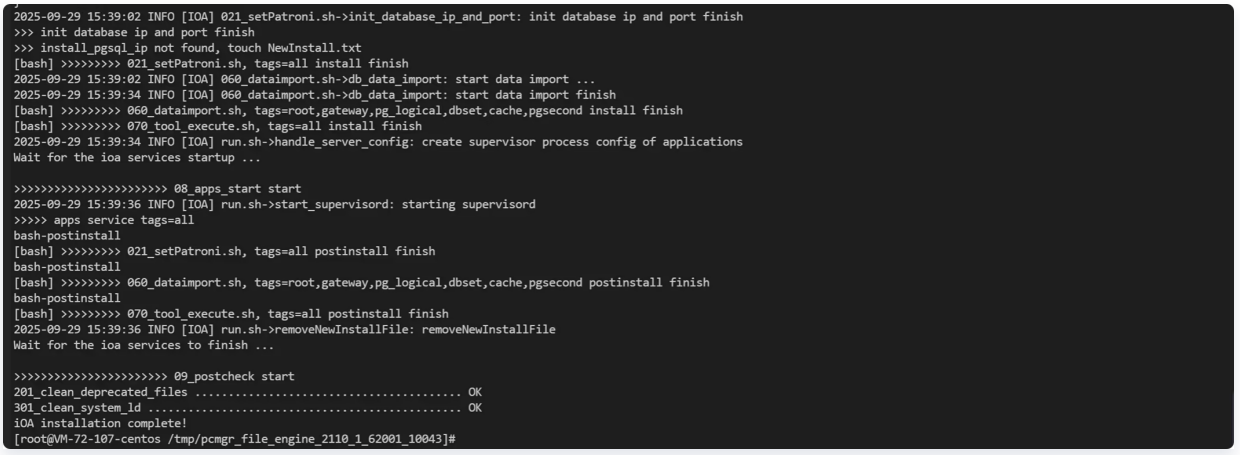
4. 复制命令至服务器，然后按 Enter 键执行命令。



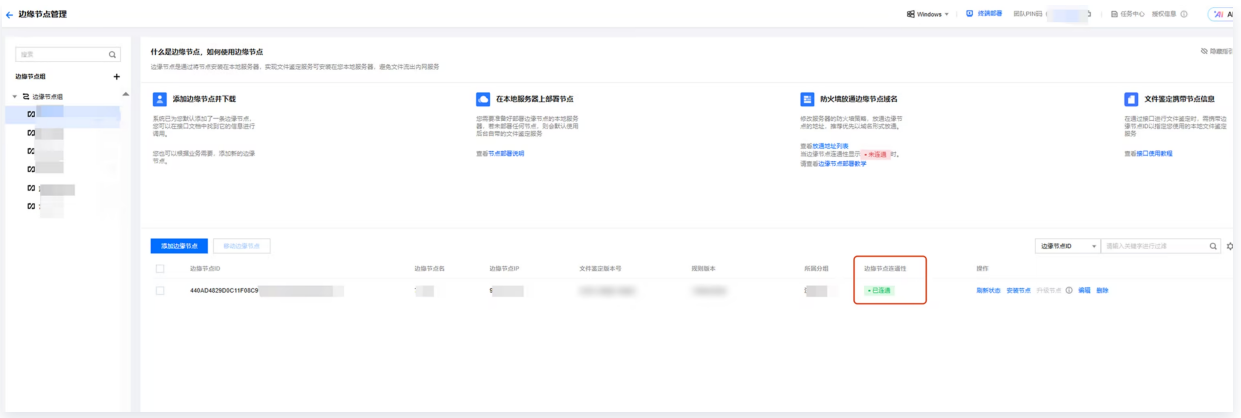
5. 自动下载安装包。系统成功接收安装指令后，自动启动后台下载任务，无需您手动干预下载过程。



6. 安装完成，核心服务初始化成功，关键组件部署就绪。

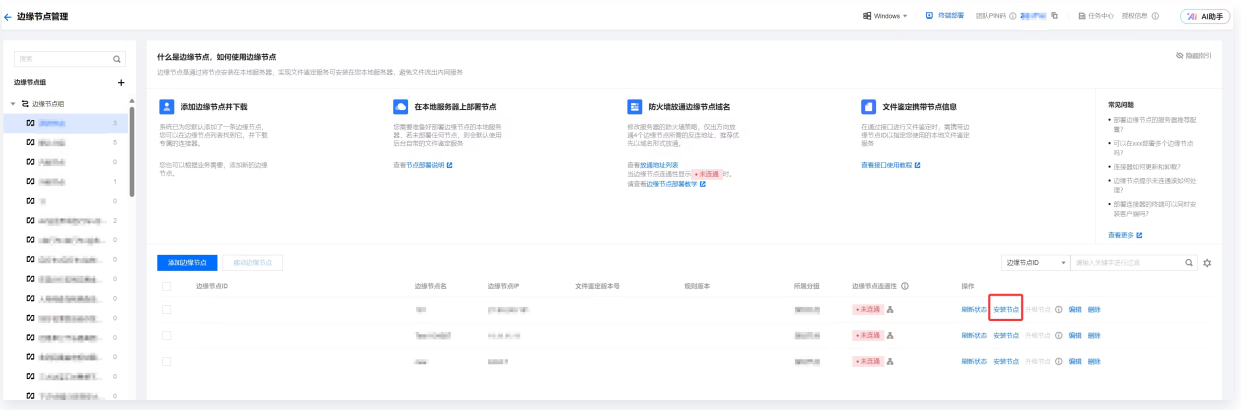


7. 安装完成后，边缘节点连通性由未连通转换为已连通状态。



方式2：离线安装

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **文件鉴定**。
2. 在文件鉴定页面，单击**部署边缘节点**。在创建的节点中选择目标节点，单击**安装节点**。

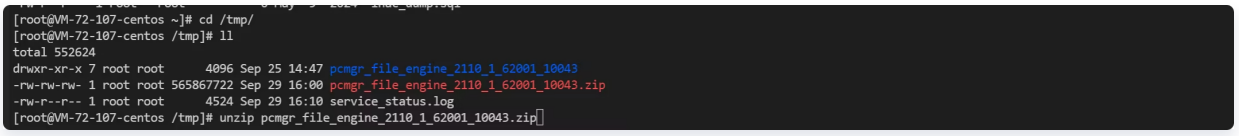


3. 在离线安装模块中，单击**下载Linux版本边缘节点**。



4. 请将下载的边缘节点安装包上传至目标机器上进行安装。

5. 解压安装包，执行 `unzip [安装包名]` 。



6. 安装边缘节点包，执行以下命令。

6.1 在安装包解压后的同级目录下， `cd [安装包名]` 。

```
[root@VM-72-107-centos /tmp]# cd pcmgr_file_engine_2110_1_62001_10043
[root@VM-72-107-centos /tmp/pcmgr_file_engine_2110_1_62001_10043]# ll
total 92
drwxr-xr-x  2 root root  4096 Sep 25 14:46
-rw-r--r--  1 root root  3951 Dec 31  1979
-rw-r--r--  1 root root  1598 Dec 31  1979
-rw-r--r--  1 root root  1679 Dec 31  1979
-rw-r--r--  1 root root    61 Sep 25 14:4
drwxr-xr-x 12 root root  4096 Sep 25 14:47
drwxr-xr-x 13 root root  4096 Sep 25 14:45
-rwxr-xr-x  1 root root  5662 Sep 25 14:45 install.sh
drwxr-xr-x 16 root root  4096 Sep 25 14:47
drwxr-xr-x  2 root root  4096 Sep 25 14:46
-rw-r--r--  1 root root    62 Sep 25 14:46
-rw-r--r--  1 root root   242 Dec 31  1979
-rw-r--r--  1 root root  6927 Sep 25 14:46
-rw-r--r--  1 root root  5163 Sep 25 14:46
-rwxr-xr-x  1 root root 20115 Sep 25 14:45
-rw-r--r--  1 root root  2638 Sep 25 14:47
[root@VM-72-107-centos /tmp/pcmgr_file_engine_2110_1_62001_10043]#
```

6.2 接着执行 `sh install.sh` 。

```
[root@VM-72-107-centos /tmp/pcmgr_file_engine_2110_1_62001_10043]# sh install.sh

######################## iOA ENTERPRISE EDITION ########################
    Copyright @ 1998 - 2023 Tencent. All Rights Reserved


>>>>>>>>>>>>>>>>>>>>>>> check_platform start
iOA platform: x86

>>>>>>>>>>>>>>>>>>>>>>> deploy_tmp_python start
iOA tmp python prepared

>>>>>>>>>>>>>>>>>>>>>>> check_mode start
execute mode: install

>>>>>>>>>>>>>>>>>>>>>>> parse_args start
install input:
{
    "$(skip_precheck)": "1",
    "$(install_master_ip)": "me",
    "$(srv_type)": [
        "all",
        "agent"
    ],
    "$(install_async)": "no",
    "$(install_tags)": "all",
    "$(install_role)": "default",
    "$(ignore_precheck)": "0"
}
```

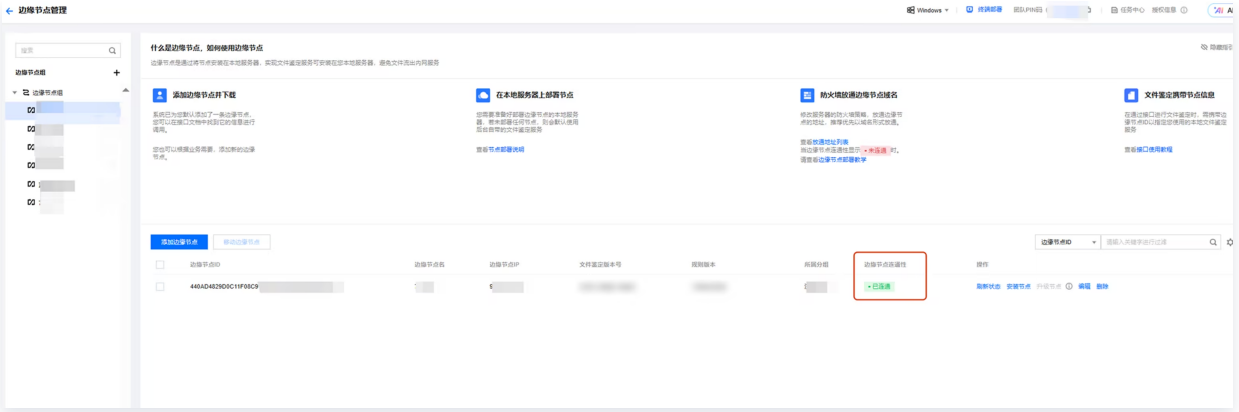
7. 安装完成，系统完成核心组件的部署与初始化。

```
}
2025-09-29 16:15:05 INFO [IOA] 021_setPatroni.sh->init_database_ip_and_port: init database ip and port finish
>>> init database ip and port finish
>>> install_pgsql_ip not found, touch NewInstall.txt
[bash] >>>>>>>>> 021_setPatroni.sh, tags=all install finish
2025-09-29 16:15:05 INFO [IOA] 060_dataimport.sh->db_data_import: start data import ...
2025-09-29 16:15:33 INFO [IOA] 060_dataimport.sh->db_data_import: start data import finish
[bash] >>>>>>>>> 060_dataimport.sh, tags=root,gateway,pg_logical,dbset,cache,pgsecond install finish
[bash] >>>>>>>>> 070_tool_execute.sh, tags=all install finish
2025-09-29 16:15:33 INFO [IOA] run.sh->handle_server_config: create supervisor process config of applications
Wait for the ioa services startup ...

>>>>>>>>>>>>>>>>>>>>>>> 08_apps_start start
2025-09-29 16:15:35 INFO [IOA] run.sh->start_supervisord: starting supervisord
>>>>> apps service tags=all
bash-postinstall
[bash] >>>>>>>>> 021_setPatroni.sh, tags=all postinstall finish
bash-postinstall
[bash] >>>>>>>>> 060_dataimport.sh, tags=root,gateway,pg_logical,dbset,cache,pgsecond postinstall finish
bash-postinstall
[bash] >>>>>>>>> 070_tool_execute.sh, tags=all postinstall finish
2025-09-29 16:15:36 INFO [IOA] run.sh->removeNewInstallFile: removeNewInstallFile
Wait for the ioa services to finish ...

>>>>>>>>>>>>>>>>>>>>>>> 09_postcheck start
201_clean_deprecated_files ..................................... OK
301_clean_system_ld ..................................... OK
iOA installation complete!
[root@VM-72-107-centos /tmp/pcmgr_file_engine_2110_1_62001_10043]#
```

8. 安装完成后，边缘节点连通性由未连通转换为已连通状态，部署边缘节点完成。


边缘节点管理
什么是边缘节点，如何使用边缘节点
添加边缘节点并下载
在本地服务器上部署节点
防火墙放通边缘节点域名
文件鉴定携带节点信息
添加边缘节点
边缘节点ID
边缘节点名
边缘节点IP
文件鉴定版本号
规则版本
所属分组
边缘节点连通性
操作
已连通

文件鉴定接口使用指引（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

通过明确指定节点唯一 ID 或节点分组唯一 ID，系统可将鉴定任务精准下发至指定的节点服务器或分组下的某个节点中。

1. 调用接口前：请先**设置公共参数并完成请求签名，具体接口调用方式**请参考以下文档：

> **说明：**
> 在请求接口前，请务必完整阅读下列文档。

- 请求结构
- 公共参数
- 签名方法 v3
- 签名方法
- 返回结果
- 参数类型

2. 文件鉴定调用涉及的接口如下：

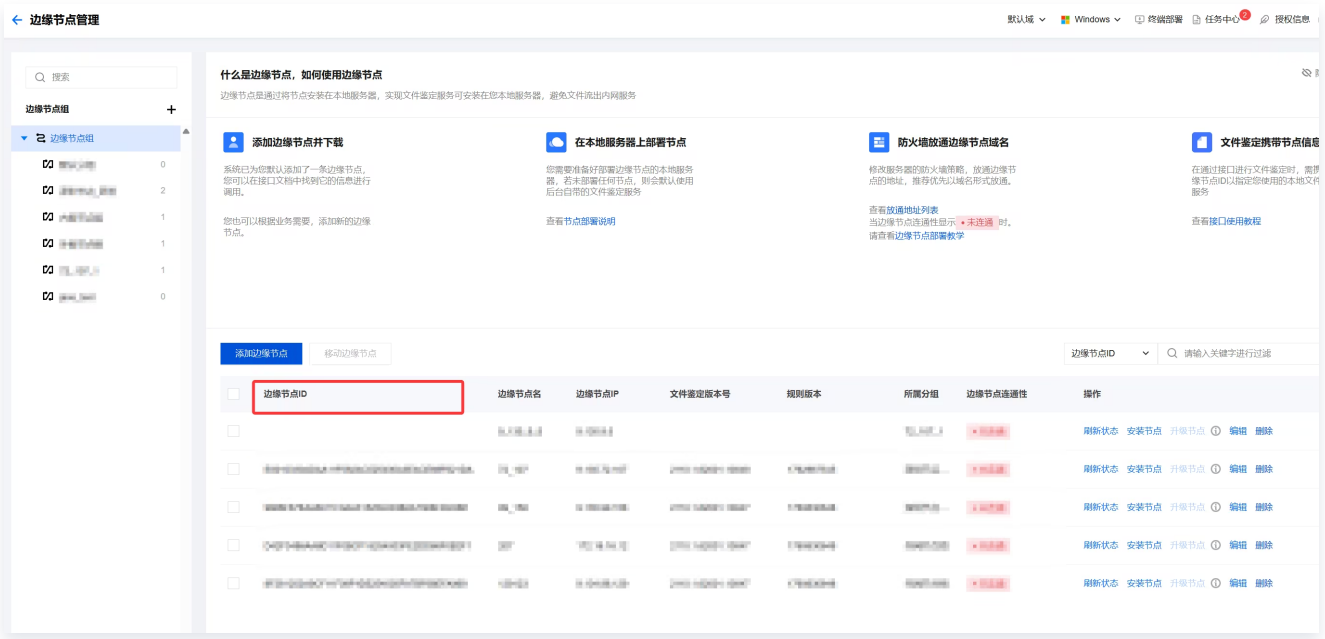
接口名称	说明
DescribeDLPEdgeNodeGroups	查询 DLP 边缘节点分组（获取节点组唯一 ID）
DescribeDLPEdgeNodes	查询边缘节点列表（获取节点组下所有节点唯一 ID）
CreateDLPFileDetectTask	创建文件鉴定任务
DescribeDLPFileDetectTaskResult	查询文件鉴定任务结果

> **说明：**
> 详细的 API 概览请参见 API 概览 。

3. 使用文件鉴定功能，调用接口的步骤为：

3.1 先调用 CreateDLPFileDetectTask（创建文件鉴定任务），接口所涉及的参数：

- 节点组唯一ID：可通过 DescribeDLPEdgeNodeGroups 接口获取。
- 节点 ID：通过 DescribeDLPEdgeNodes 接口查看，或者登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**管控策略** > **文件鉴定** > **部署边缘节点**，在边缘节点管理页查看**边缘节点ID**。



3.2 再调用 DescribeDLPFileDetectTaskResult 接口查看检测结果。

数据分级分类（11.1.1版）
分级分类规则（11.1.1版）

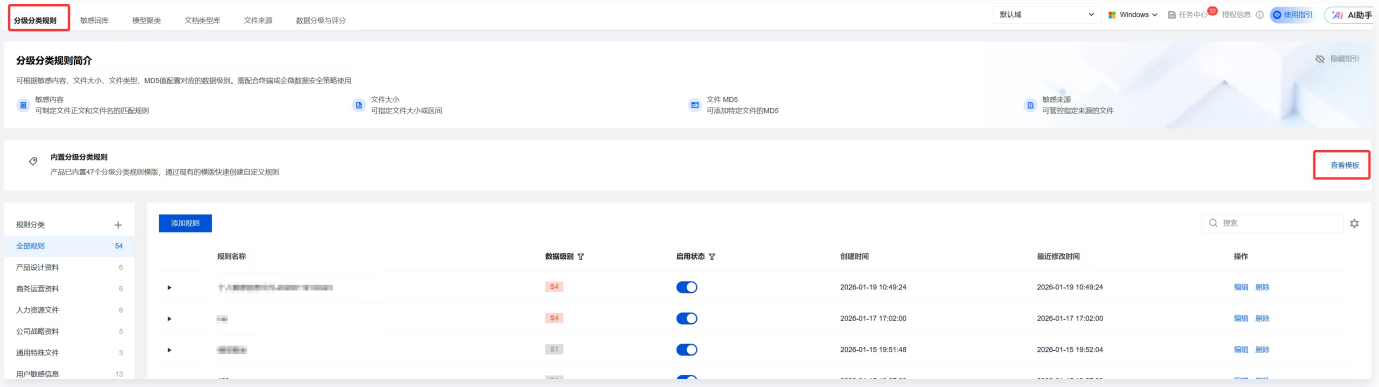
最近更新时间：2026-02-06 14:23:32

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

为不同敏感级别数据制定各自的识别策略，以实现精细化的策略管控，iOA 内置七大分类、47个常见规则模板，您可以通过引用 内置规则，或添加 自定义分级分类规则，快速构建敏感数据规则库。

内置规则

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据分级分类** > **分级分类规则**。
2. 在分级分类规则页面，单击**查看模板**。



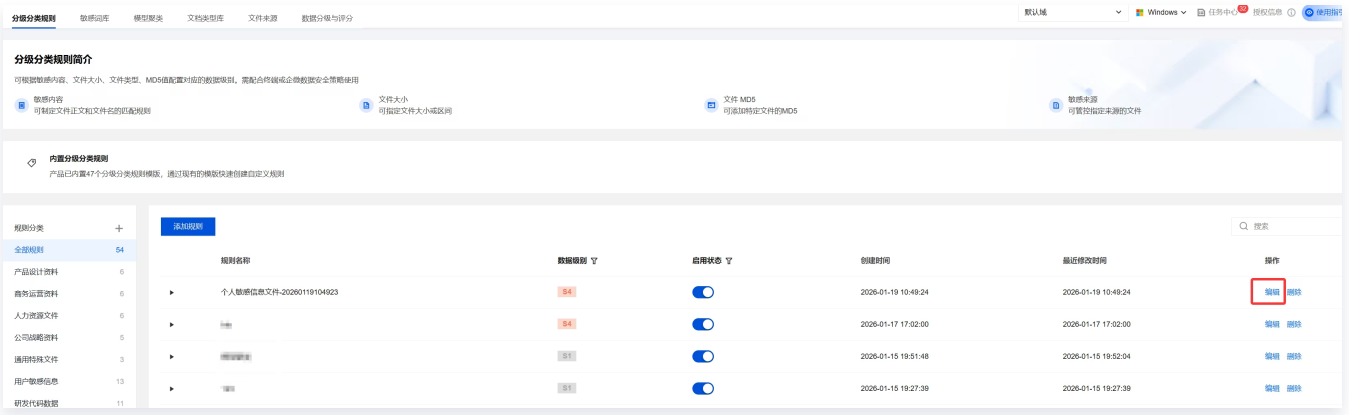
3. 支持查看模板详情，单击**详情**，查看内容匹配规则。



4. 单击**创建**，快速创建分级分类规则模板。



5. 内置模板支持在创建后编辑，单击**编辑**，配置符合管理需求的规则。

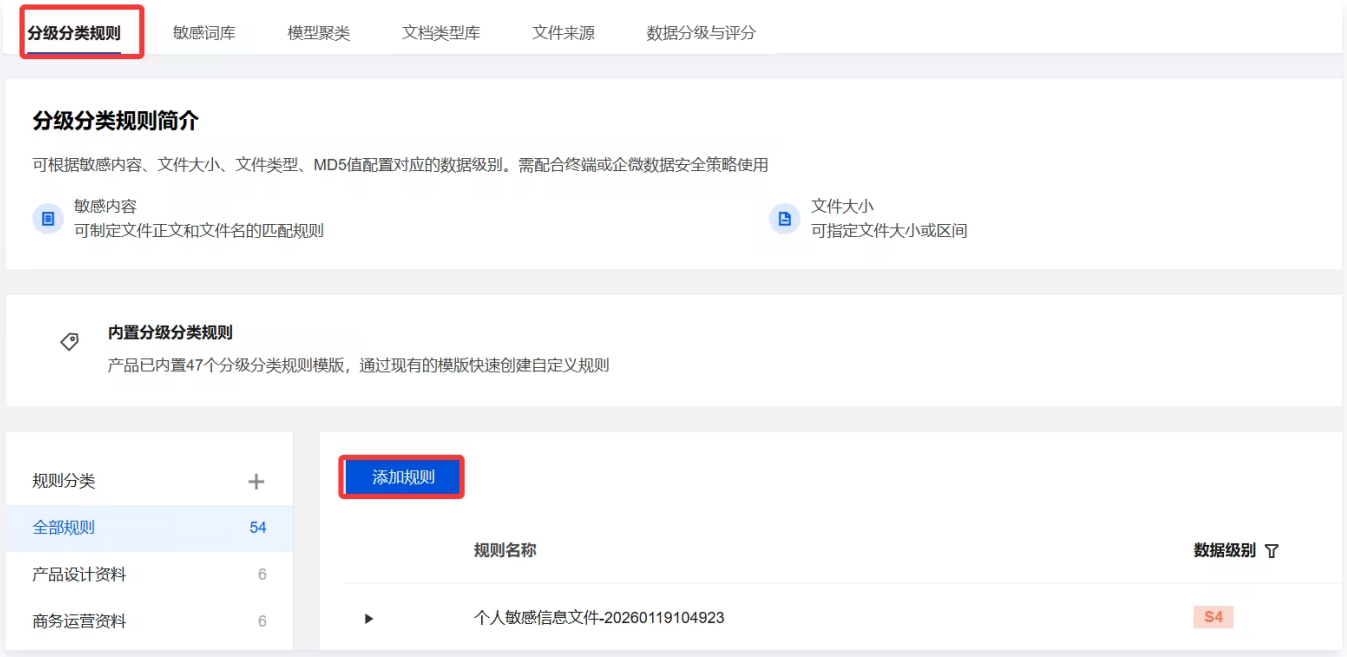


6. 配置完成后单击**保存**。



自定义分级分类规则

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据分级分类** > **分级分类规则** 。
2. 在分级分类规则页面，单击**添加规则**。



3. 在新建规则页面，输入基本信息。



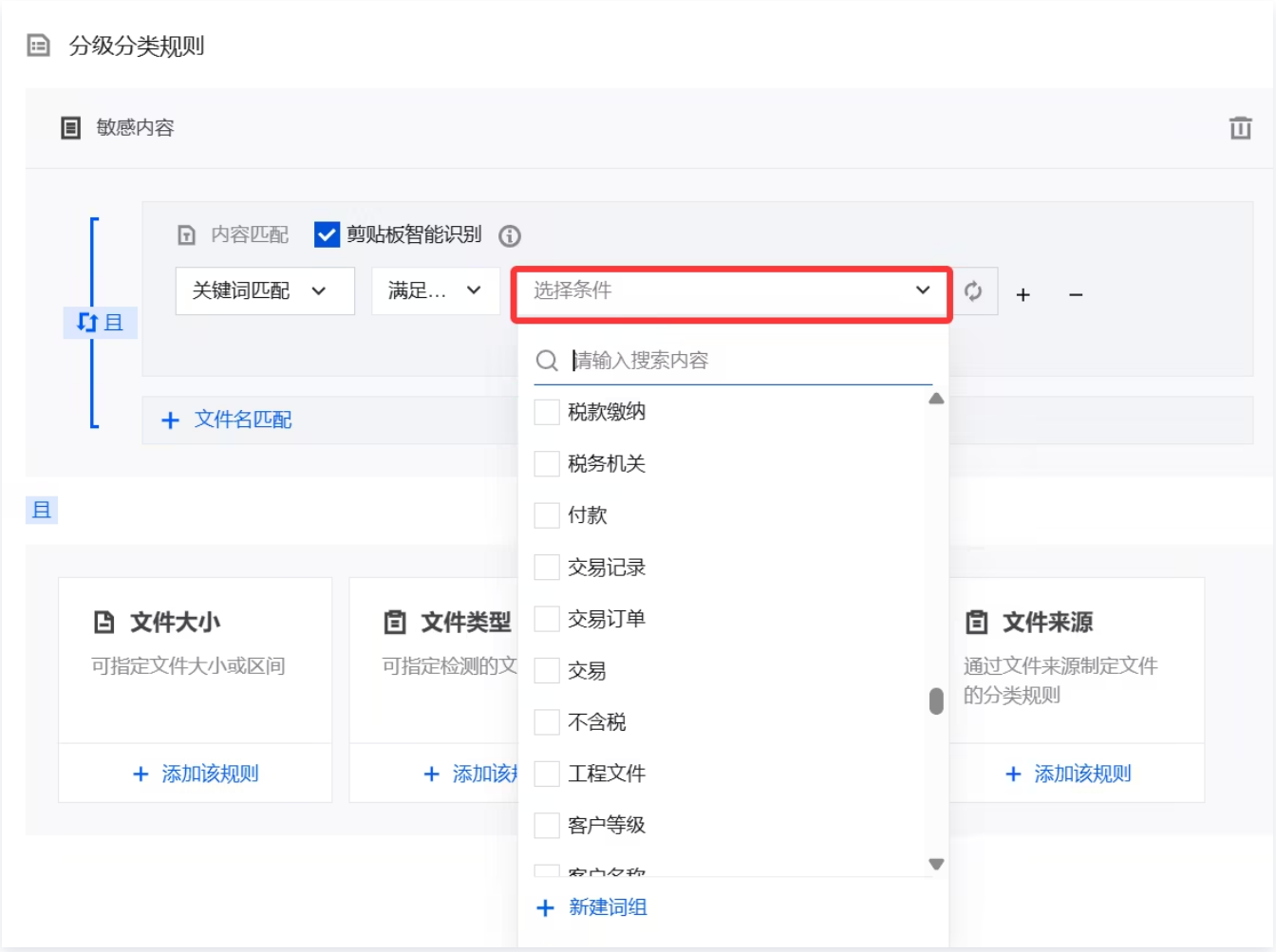
参数名称	说明
规则名称	自定义名称，支持1-50字符。
规则描述	自定义规则描述，支持1-288字符。
管控级别	该规则定义的文件管控级别。
规则分类	请选择已存在的规则分类，如果需要，可以在上级页面新增。
是否启用	开启后，该分级分类规则将会用于敏感文件识别，命中规则的文件外发时触发审计、告警、拦截等策略。

版权所有：腾讯云计算（北京）有限责任公司

4. 在新建规则页面，您可以根据自身业务需求组合不同的敏感数据规则，包括 敏感内容 、文件大小 、文件类型 、文件 MD5 、文件来源 。
5. 选择所需规则类型后，单击**添加该规则**，配置相关参数，单击**保存**，即可创建规则，创建的分级分类规则可用于管控策略 、事件聚合规则 等配置，防止敏感数据泄露或滥用。

敏感内容

1. 敏感内容包括文件正文和文件名。支持关键词、正则、字典匹配。支持满足任一条件、满足所有条件或满足部分条件。在选择敏感词类型后，可以从系统内置的敏感词组或自定义敏感词组中选择，支持根据敏感词名称和标签进行搜索。



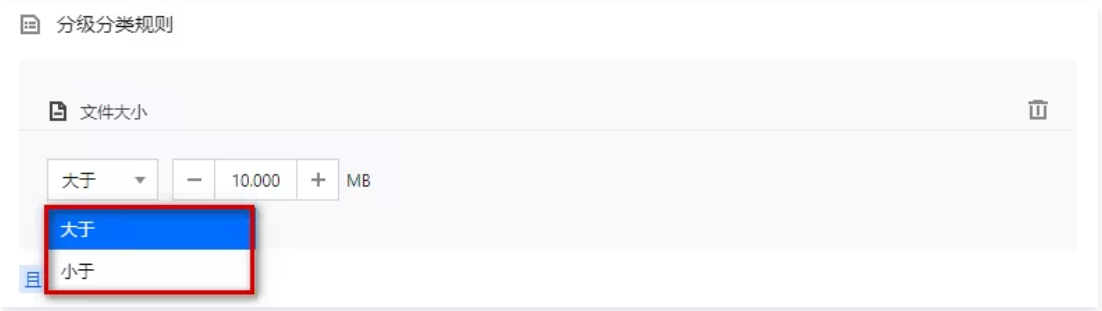
2. 开启剪贴板智能识别：开启后，将通过 OCR 识别结果，在以下对应场景匹配分级分类规则后，触发审计、拦截和告警：
   - 仅以文字形式粘贴通过已启用管控通道进行外发时（仅支持 Windows 系统）。
   - 仅以截图形式粘贴通过已启用管控通道进行外发时（支持 Windows 与 macOS 系统）。
   - 同时将文字及截图粘贴通过已启用管控通道进行外发时（仅支持 Windows 系统）。
   - 在无本地文件的情况下，进行网页或复制文字打印操作时（仅支持 Windows 系统）。

版权所有：腾讯云计算（北京）有限责任公司



文件大小

可指定文件大小或区间，支持选择大于或小于，配置后只对特定大小范围内的文件进行深度敏感数据检测，排除明显无关的文件。



文件类型

勾选文件类型并选择所需条件，支持勾选内置文件类型或添加 自定义扩展名 。



参数名称	说明
文件类型	• 文件类型的识别通过文件头信息实现，即使文件后缀被修改，iOA零信任安全管理系统仍能准确识别文件的原始类型； • 支持识别变形文件，包括加密文件和后缀重命名文件。 • 文件类型与特殊文件类型之间是并集关系，例如同时选择"源代码"和"加密文件"时，表示识别的是"加密的源代码文件"。

	• 支持多种文件类型，包括源代码、办公文档、设计文件、文本文档、图像文档、音频文档、数据库文件、视频文件、邮件文件、压缩文件、应用文件、二进制文件和证书文件等。详情请参见 支持文件类型 。
仅识别该文件类型被加密的文件	选中后，只有配置的文件类型被加密会被识别。由于加密文件无法识别文件正文，请避免配置文件内容属性。目前，只支持 Office 类文档和压缩文件。
仅识别该文件后缀名被更改的文件	选中后，系统将仅识别该文件类型被更改后缀名的敏感文件。此功能适用于将高价值文件的后缀名修改为低价值文件的场景，例如，将压缩文件的后缀名修改为 JPG，使之看起来像一张图片。目前，只支持识别 Office 类文档和压缩文件。

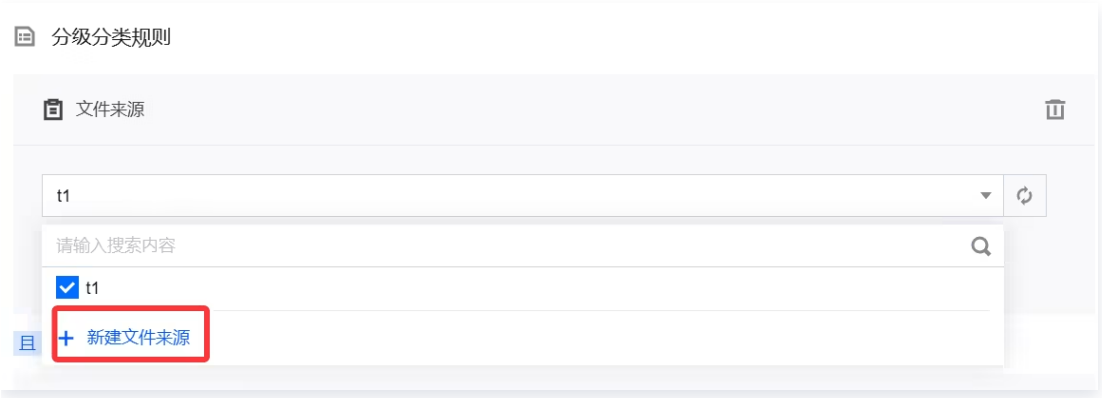
文件 MD5

文件 MD5 值作为文件唯一性标识，用于快速比对文件是否是已知敏感文件，支持添加特定文件的 MD5。



文件来源

文件来源作为规则判断选项，管理员可根据文件来源制定分级分类规则，对来自敏感系统的文件进行细致的检测。单击**新建文件源**，详细配置请参见 文件来源 。



敏感词库（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

内置敏感词库可帮助您快速定义常用敏感数据。您可以自定义敏感词，支持关键字、正则表达式、字典等多种匹配方式，添加的自定义敏感词将应用于文件识别，为不同类型的数据信息提供精准匹配方案：

- 结构化数据（如身份证号）：建议采用正则表达式精确匹配。
- 非结构化数据（如客户隐私文本）：建议使用关键字匹配。
- 复杂文本内容：建议通过字典匹配结合权重计算，判定是否为敏感文件。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据分级分类** > **敏感词库**。
2. 在敏感词库页面，单击**添加词库**。



3. 在添加词组页面，选择所需**词组类型**，并配置相关参数。
   - **关键字：**使用关键字来标识敏感内容。如果文件中的某部分内容与关键字匹配，就会触发规则，将其判定为敏感文件。



- **正则：使用正则表达式来标识敏感元素的内容。如果文件中的某部分内容与正则表达式匹配，并且匹配次数达到或超过您设定的次数，那么就会触发规则，文件将被判定为敏感文件。**



- **字典：当文档中的检测到的关键字加权分值超过设定的阈值，该文档便被判定为敏感文件。在此检测过程中，字典内的关键字不会被重复计算（即使多次出现也只计算一次）。每当文档中出现一个关键字，权重值就会增加相应的分值。总权重值的设定范围最低为1，最高不超过所有关键字权重值的总和。**

  示例：如下图所示：4个关键字，总权重分是400分，每个关键字命中加100分，总权重分数达到或超过299，就会判定为敏感文件。这意味着只要命中了3个关键字，就会触发规则。



4. 敏感词库配置完成，单击**保存**，配置的敏感词库，用于**数据分级分类 > 分级分类规则 > 敏感内容**中，用于识别、定位和处理敏感数据。通过预设的关键字、模式或规则，帮助系统快速发现如个人身份信息、财务信息等敏感内容。


新建规则
基本信息
编辑规则
基本信息
* 规则名称
请输入规则名称，不超过50个字符
0/50
* 规则描述
建议您填写准确详实的规则描述，便于您持续维护和管理规则，不超过288个字符
0/288
* 管控级别
S6
S5
S4
S3
S2
S1
* 规则分类
请选择
* 是否启用
分级分类规则
敏感内容
内容匹配
且
关键词匹配
满足所有
选择条件
关键词匹配
正则匹配
字典

模型聚类（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

支持用户上传样本数据。借助自然语言处理（NLP）和上下文分析技术，系统能够对敏感样本进行智能学习，并支持以聚类或添加词典形式，将学习结果中获得的关键词作为规则，在分级分类规则的敏感内容中进行引用。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据分级分类** > **模型聚类**。
2. 在模型聚类页面，单击**添加模型**。



3. 在添加模型页面，单击**上传文件**，可上传单个文件或批量相似文件，上传完成后单击**开始学习**。

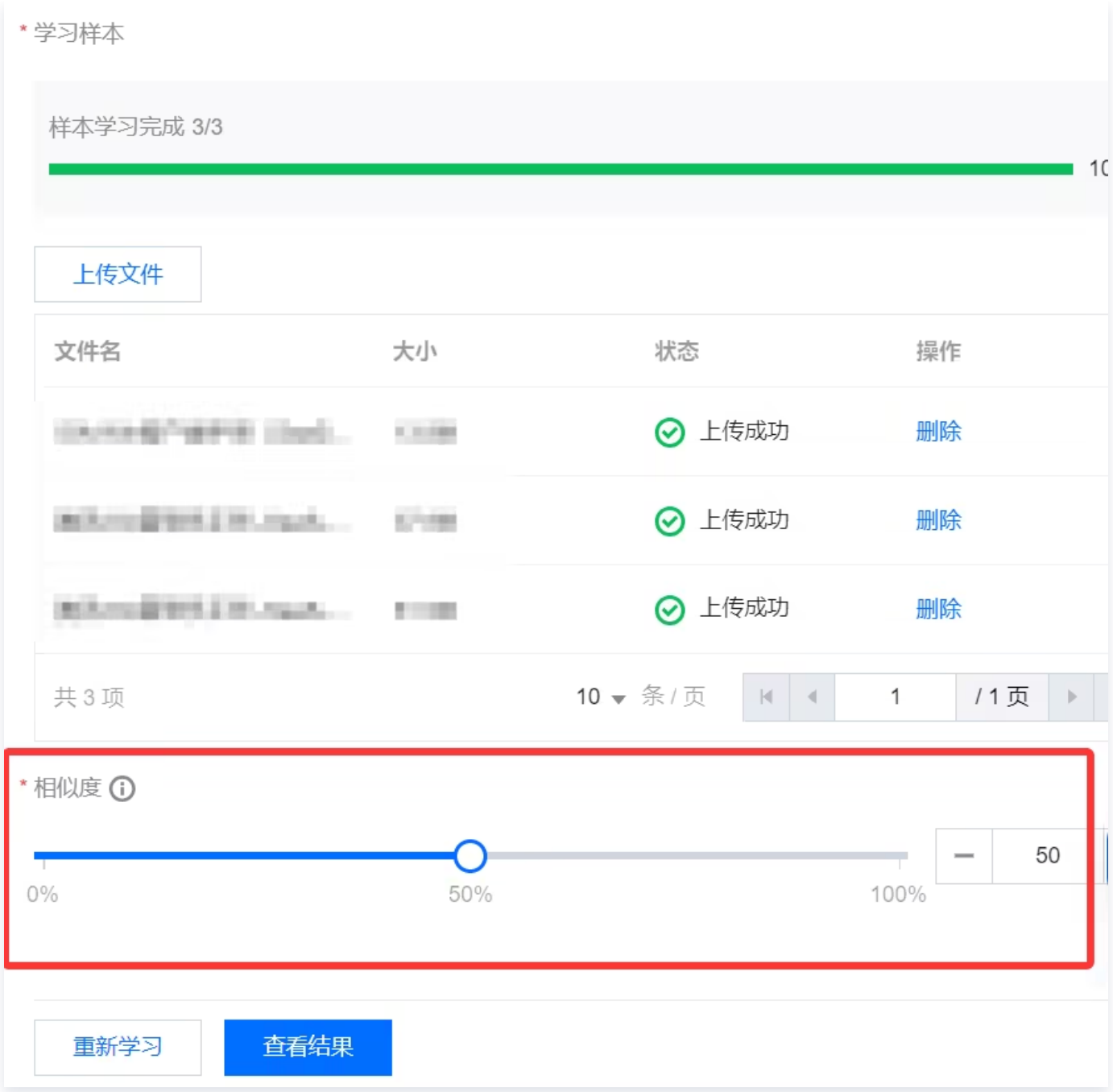


4. 相似度：自定义相似度的值，相似度仅影响机器学习文件分组结果，不影响敏感内容的提取。

   4.1 模板文件/代码文件：上传单个文件，并将相似度调整至100% 。

   4.2 多数据实际应用场景：可将不同后缀样本进行分析，相似度代表相似文件分类严格程度，阈值越高即分类越严格，学习结果分组会越多。可根据最终学习结果调整相似度阈值，以适配不同业务场景，请至少使用3个及以上样本文件进行学习。

版权所有：腾讯云计算（北京）有限责任公司



5. 学习结果说明：

5.1 模型可由多个文档组成，多个文档进行聚合，将多个文档中所有的关键词按照权重进行汇总计算。

5.2 模型的数量与相似度关系：

- 示例：当上传的 3 个文档中有 2 个文档高度相似且相似度设置百分比较低时，系统会自动将它们聚合为 1 个聚类（1个模型）。
- 如果是3个完全不同的文件，而 相似度设置百分比较高时，就会形成 3 个不同的聚类（3个模型）。
- 以下图为例：上传3个文档，设置相似度50%，因上传的管理员手册本身相似度较高，当设置相似度百分比为50%时，则自动聚合为1个聚类。



6. 文件组合为1个聚类，关键词众多，但并非所有关键词都具有实际价值。这种情况下，可勾选您认为有实际价值的关键词；支持编辑模型或字典模式。

6.1 编辑模型

6.1.1 单击**编辑模型**，完成编辑后单击**确定**保存，系统会从所选的关键词中生成模型。



6.1.2 勾选您认为有实际价值的关键词，完成编辑后单击**确定**保存，系统会从所选的关键词中生成模型。



6.1.3 生成的模型如下图：

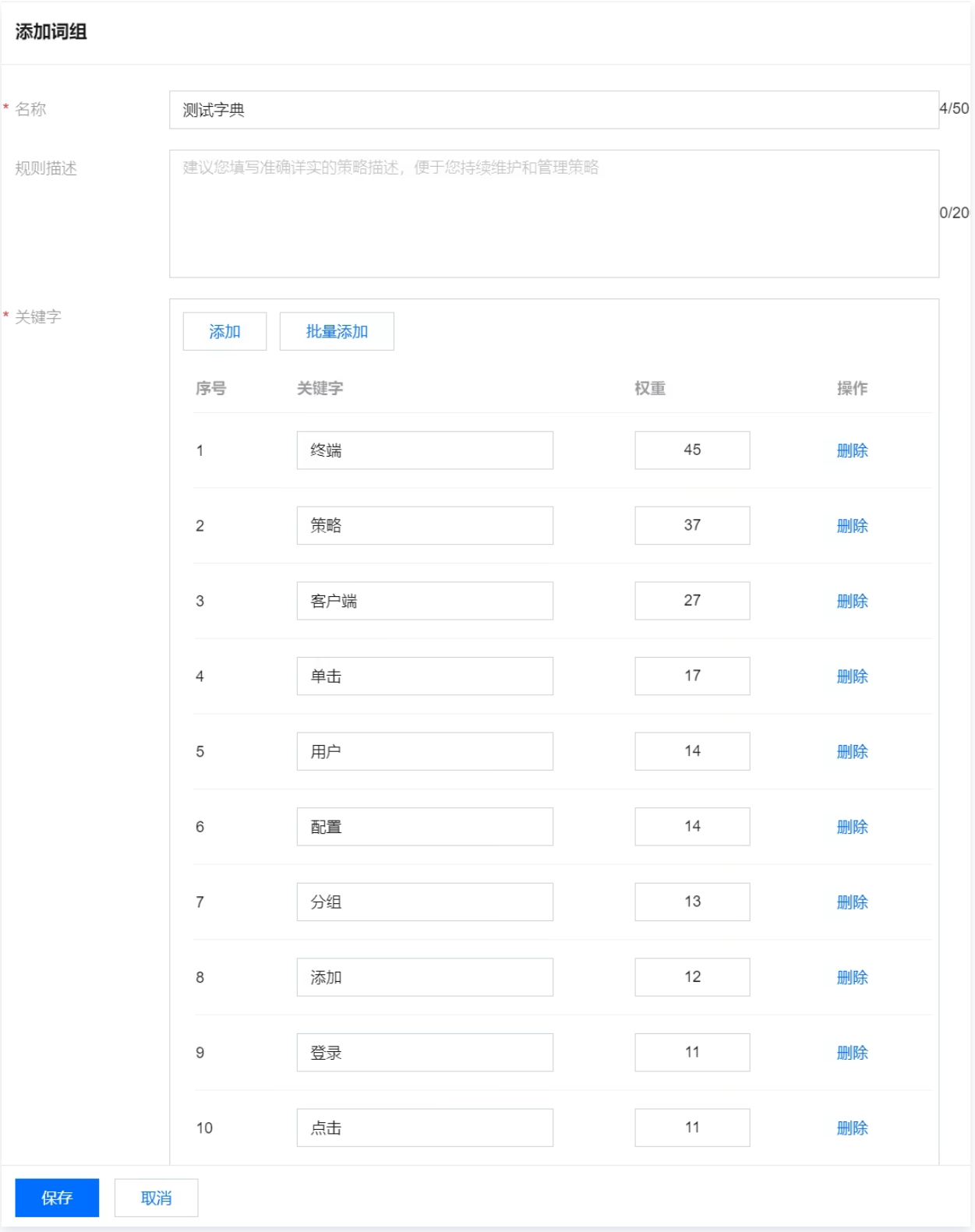


6.2 字典模式

6.2.1 支持配置字典模式，单击**字典模式**，可将已计算出权重的模型，快速添加为字典。



6.2.2 选中的关键词保存在字典，可在**数据分级分类 > 分级分类规则 > 敏感内容**中选择字典，引用该规则。



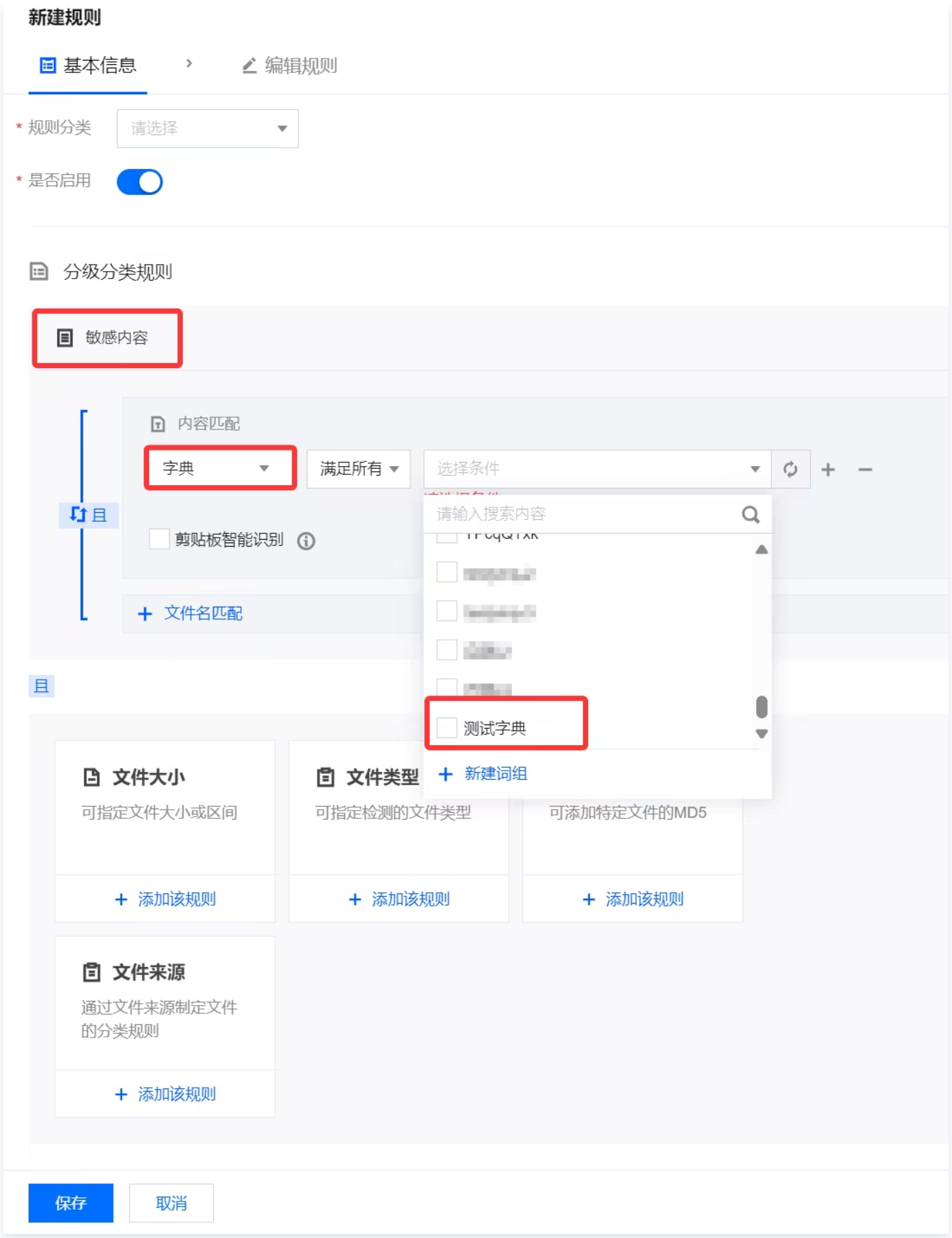
7. 以词云或表格视角展示关键词。
   - 词云视角：词云中仅显示学习结果后，进行保存的关键词，大小按照权重进行排列。
   - 表格视角：按关键词权重结果生成列表（关键词+权重比例）。



8. 聚类文件：根据学习结果，将符合相似度及以上的文件进行聚类（显示该模型所有聚类的文件名及 MD5值）。



9. 机器学习后的使用方式：通过“字典模式”生成字典后，在**数据分级分类 > 分级分类规则 > 敏感内容**中选择字典。


新建规则
基本信息
编辑规则
* 规则分类
请选择
* 是否启用
分级分类规则
敏感内容
内容匹配
字典
满足所有
选择条件
且
请输入搜索内容
剪贴板智能识别
文件名匹配
且
测试字典
新建词组
文件大小
可指定文件大小或区间
添加该规则
文件类型
可指定检测的文件类型
添加该规则
可添加特定文件的MD5
添加该规则
文件来源
通过文件来源制定文件的分类规则
添加该规则
保存
取消

文档类型库（11.1.1版）

最近更新时间：2026-02-06 14:23:32

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

内置九大类文档类型，帮助您快速选择文档/文件格式。您还可以添加扩展名，根据一级二级分类自定义扩展名。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据分级分类 > 文档类型库**。
2. 在文档类型库页面，展示目前已存在的一级、二级文档类型和扩展名，单击**添加扩展名**，录入新的文件扩展名称，按 **Enter 键**选定后单击**确定**保存。



3. 在文档类型页面，单击 ×，经过二次确认后，即可删除扩展名。

> **说明：**
> - 内置的扩展名不支持删除。
> - 自定义扩展名支持删除。
> - 若该扩展名已被分级分类规则引用，删除后，关联的规则将不再识别该扩展名。



已内置300+种文件后缀，具体类型如下：

文件大类	文件类型	文件后缀
源代码文件	Java 文件	java
	Python 文件	py
	SQL 文件	sql
	PowerShell 文件	ps、ps1、ps2
	BAT 文件	bat、cmd
	JavaScript	js、vue
	PostScript 文件	eps、epsf、epsi
	Rust 文件	rs
	Shell 脚本	sh、bash
	ASP 文件	asp
	Aspdotnet 文件	aspx
	Assembly 文件	s、S、asm
	CSS 文件	css、sass、scss

HTML 文件	html、htm
C++ 文件	hpp、hxx、h++、hp、HPP、cpp、cxx、c++、CPP
C 文件	H、C、h、c、cc、hh
Dart 文件	dart
DM 文件	dm
Elixir 文件	exs
Kotlin 文件	kt
Swift 文件	swift
TypeScript 文件	ts
CoffeeScript 文件	coffee
C# 文件	cs、cshtml、csproj
Go 代码文件	go
Groovy 文件	groovy
Java 文件	java
JSP 文件	jsp
Less 文件	less
Lua 文件	lua
Objective-C 文件	m、mm
Pascal 文件	p、pp、pas、PAS、dpr
Perl 文件	pl、pm、al、perl
PHP 文件	php、php3、php4

版权所有：腾讯云计算（北京）有限责任公司

	Python 文件	py
	Ruby 文件	rb
	Scala 文件	scala
	SQL 文件	sql
	TCL 文件	itk、tcl、tk
	VB.NET 文件	vb
	VBScript 文件	vbs
办公文档	Word 文档	\wps、wpt、doc、dot、docx、dotx
	Excel 文档	et、ett、xls、xlm、xla、xlc、xlt、xlw、xll、xld、xlam、xlsb、xlsm、xltm、xlsx、xltx
	PDF 文档	pdf
	RTF 文档	rtf
	Keynote 文档	key
	Page 文档	pages
	WPS 文档	wks、wcm、wdb
	Numbers 文档	numbers
	FDF 文档	fdf
	PowerPoint 文档	ppt、ppz、pps、pot、ppa、ppam、pptm、sldm、ppsm、potm, pptx、thmx、sldx、ppsx、potx
	MS 文档	docm、dotm
数据库文件	数据库文件	apr、dbf、dbt、dbase、dbase3、mdb、db、accdb、MYI、MYD、sqlite3、odb、frm、ibd、ora
邮件文件	邮件文件	msg、pst、ost、eml、mime、emlx

压缩文件	压缩文件	gz、tgz、jar、aar、ser、apk、cab、7z、ar、a、bz、tbz、bz2、tbz2、boz、z、lz4、lz、lzma、rar、sz、tar、ear、war、xz、zip、vsix、suo、nupkg、zstd
二进制文件	二进制文件	exe、dll、com、com、scr、pif、so、dms、lha、lzh、pkg、dump
设计文件	Photoshop 文件	psd、psb
	三维动画文件	ma、mp、mb、b3d、lwo、lws、pmx、q3o、q3s、rhp、3ds、max、bip、x3d、c4g、c4d、c4f、c4p、c4u、x_t、x_b、xmt_bin、xmt_txt、3dm、3mf、amf、ase、dae、fbx、glb、gltf、ply、step、stp、u3d、usd、usdz、usda、usdc、3dml、vsdx、vssx、vstx、dwg、dxb、dxf、igs、iges、msh、mesh、silo、dwf、dwfx、gdl、gtw、vtu
	建筑设计文件	rfa、rft、rvt、nwd、nwf、nwc
	工业设计文件	pho、drl、des、rvm、xgl、zgl
	原型设计文件	rp、rplib、fig、xd、vsd、vst、vss、vsw、sketch
文本文档	文本文档	json、vcf、mht、mhtml、ics、ifb、iso19139、txt、text、def、list、in、INSTALL、KEYS、LICENSE、NOTICE、README、abs-linkmap、abs-menulinks、aart、ac、am、apt、bsh、classpath、cnd、cwiki、dcl、dsp、dsw、egrm、ent、ft、fn、fv、grm、g、htaccess、handlers、htc、ihtml、jmx、junit、jx、manifest、m4、mf、MF、meta、mdo、n3、pen、pod、pom、project、rng、rnx、roles、schemas、tld、types、vm、vsl、wsdd、xargs、xcat、xegrm、xgrm、xlex、xlog、xmap、xroles、xsamples、xsp、xtest、xweb、xwelcome、dsc、rtx、sgml、sgm、t、tr、roff、nroff、man、me、ms、uri、uris、urls、curl、dcurl、mcurl、scurl、fly、flx、gv、spot、anpa、jad、wml、wmls、vtt、as、ada、adb、ads、applescript、asciidoc、adoc、ad、aj、awk、bas、Bas、BAS、cgi、clj、cbl、Cbl、CBL、cob、Cob、COB、cfm、cfml、cfc、cl、jl、lisp、lsp、config、conf、cfg、xconf、d、diff、patch、e、el、erl、exp、4th、f、F、for、f77、f90、haml、hs、lhs、hx、idl、properties、l、log、Makefile、GNUmakefile、ml、m3、i3、mg、ig、ocaml、mli、pro、rexx、r、rest、rst、restx、sed、etx、st、uu、cls、Cls、CLS、frm、Frm、FRM、vcs、v、vhd、vhdl、md、mdtext、

版权所有：腾讯云计算（北京）有限责任公司

		mkd、markdown、y、yaml、yml、gnucash、xml、xsl、xsd、svg、svgz

版权所有：腾讯云计算（北京）有限责任公司

文件来源（11.1.1版）

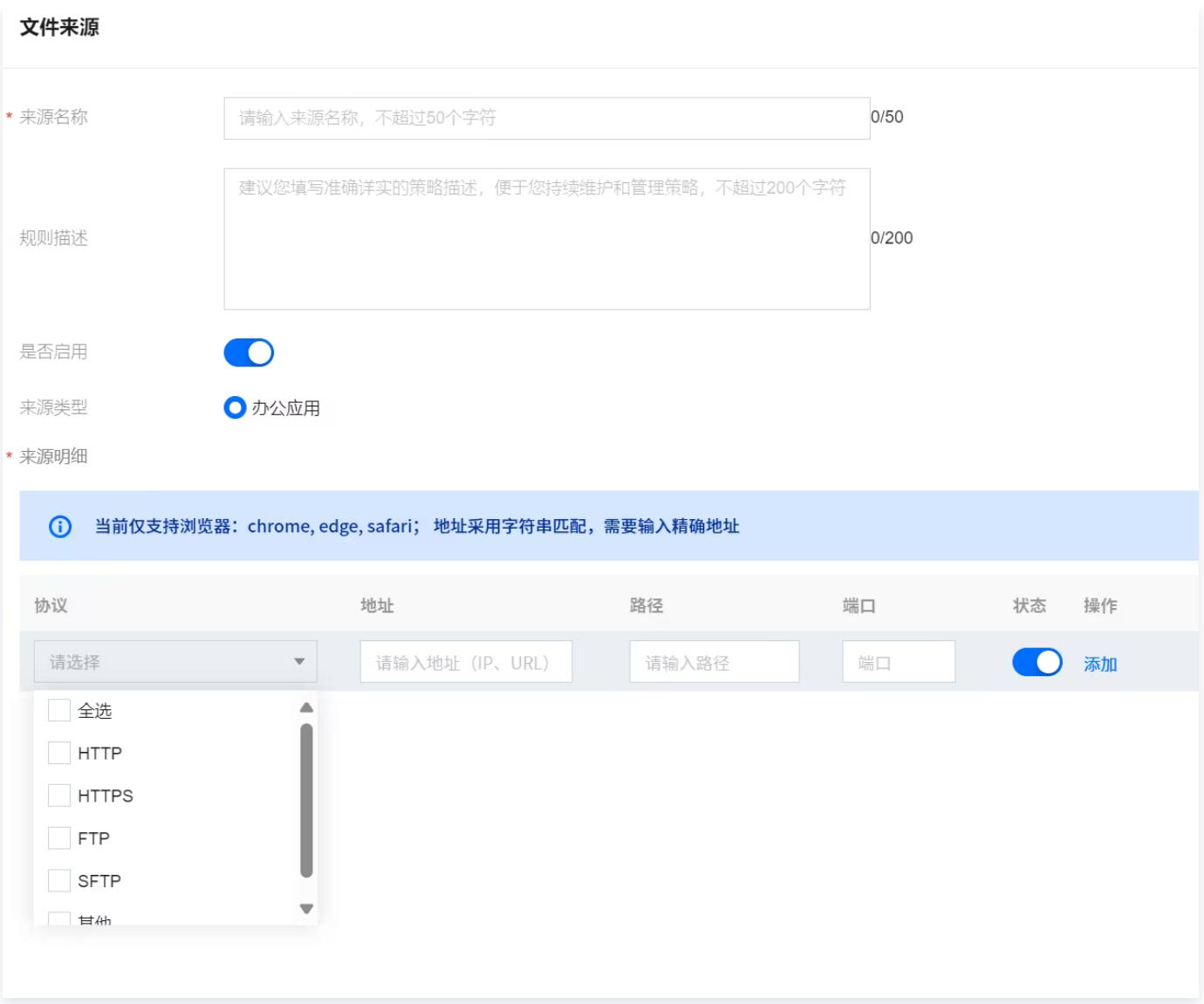
最近更新时间：2026-02-06 14:23:32

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据分级分类** > **文件来源**。
2. 单击**添加来源**，支持配置协议及地址，审计对应浏览器的下载行为。

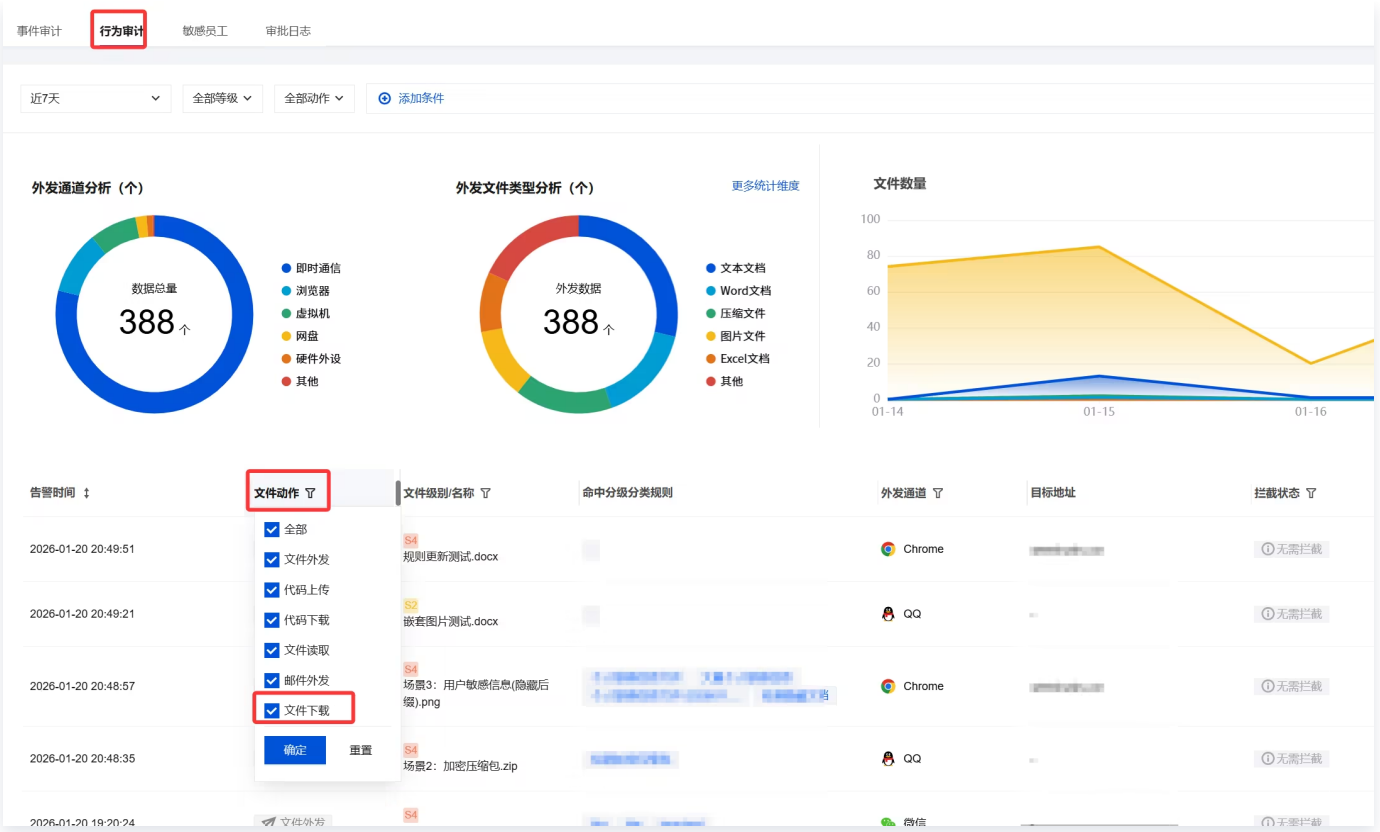


3. 在文件来源页面，配置来源名称，是否启用等参数。



参数名称	说明
来源名称	自定义名称，支持1-50字符。
规则描述	自定义规则描述，支持1-200字符。
是否启用	是否启用此策略。
来源	办公应用
来源明细	• 配置协议类型、地址、路径、端口信息。 • 协议、地址为必填信息，路径与端口非必填。 • 当前仅支持浏览器：Chrome、Edge、 Safari；地址采用字符串匹配，需要输入精确地址。

4. 配置完成单击**确定**保存，在**数据分级分类** > **文件来源**进行配置后，结合**管控策略** > **管控策略** > **审计策略**，符合规则的行为将在**风险调查** > **行为审计**日志进行记录。

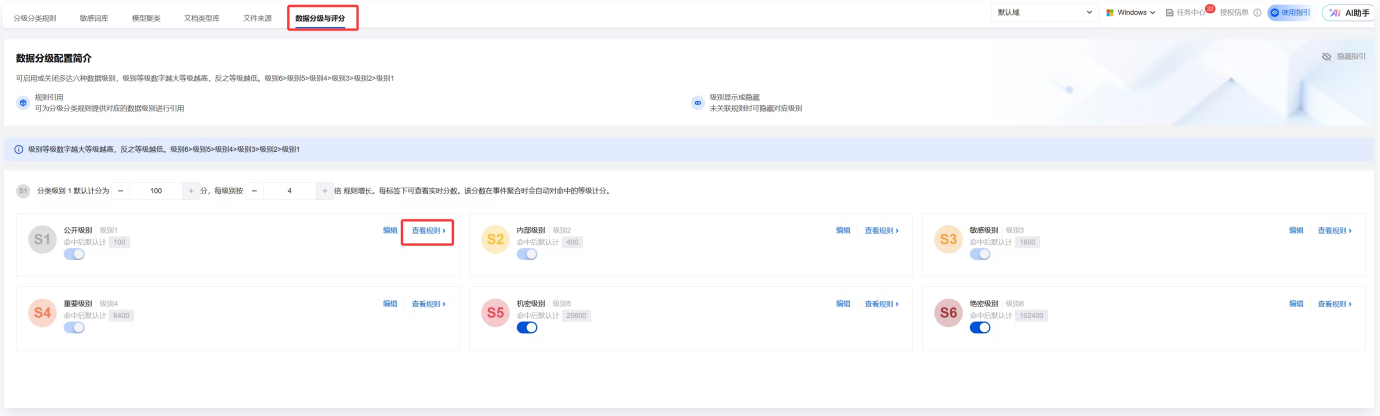

事件审计
行为审计
敏感员工
审批日志
近7天
全部等级
全部动作
添加条件
外发通道分析（个）
数据总量
388 个
即时通信
浏览器
虚拟机
网盘
硬件外设
其他
外发文件类型分析（个）
更多统计维度
外发数据
388 个
文本文档
Word文档
压缩文件
图片文件
Excel文档
其他
文件数量
100
80
60
40
20
0
01-14
01-15
01-16
告警时间
文件动作
文件级别/名称
命中分级分类规则
外发通道
目标地址
拦截状态
全部
文件外发
代码上传
代码下载
文件读取
邮件外发
文件下载
确定
重置
2026-01-20 20:49:51
规则更新测试.docx
Chrome
无需拦截
2026-01-20 20:49:21
嵌套图片测试.docx
QQ
无需拦截
2026-01-20 20:48:57
场景3：用户敏感信息(隐藏后缀).png
Chrome
无需拦截
2026-01-20 20:48:35
场景2：加密压缩包.zip
QQ
无需拦截

数据分级与评分（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**数据分级分类** > **数据分级与评分**。
2. 在数据分级与评分页面，单击**查看规则**可快速筛选并查看该数据级别的分级分类规则。当文件匹配多个数据等级时，默认定义为较高等级文件。



3. 单击**编辑**，支持修改数据级别标签，以适配不同公司对内部合规等级命名差异的需求。确保企业能够根据自身合规要求灵活调整数据级别标签。

版权所有：腾讯云计算（北京）有限责任公司


编辑数据级别标签
级别等级数字越大等级越高，反之等级越低。级别6>级别5>级别4>级别3>级别2>级别1
分类级别
级别1
* 级别名称
S1
2/10
* 级别描述
公开级别
4/50
开启状态
确定
取消

远程接入（11.1.1版）
身份及认证对接（11.1.1版）
iOA SaaS 本地自建账户（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

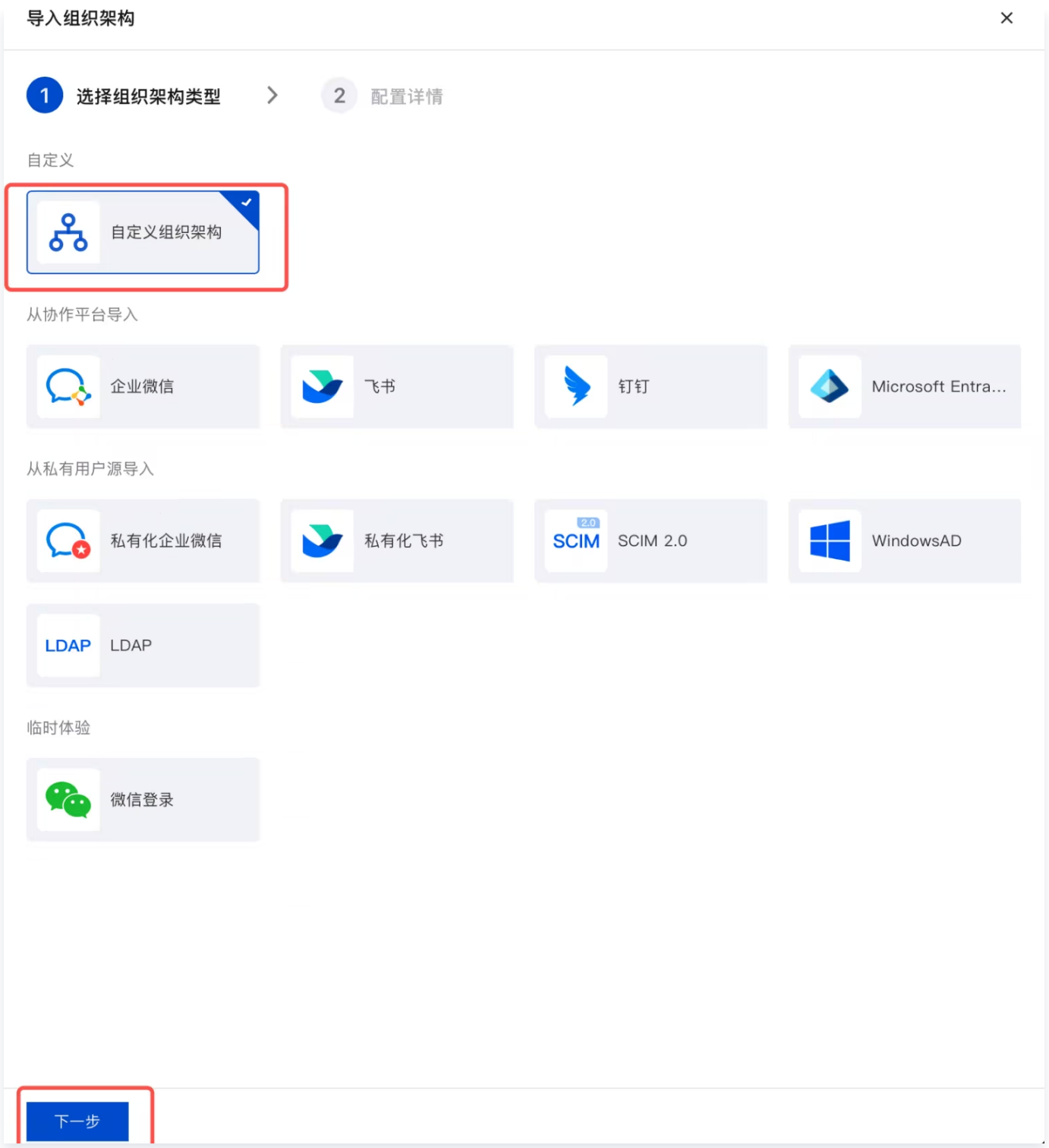
本文将介绍如何在本地自建账户并使用自建账户登录客户端。

新增目录

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择 组织架构管理 。
2. 在组织架构管理页面，单击**新增组织架构**。



3. 在导入组织架构页面，选择**自定义组织架构**，单击**下一步**，输入组织架构名称，单击**完成**。



添加分组

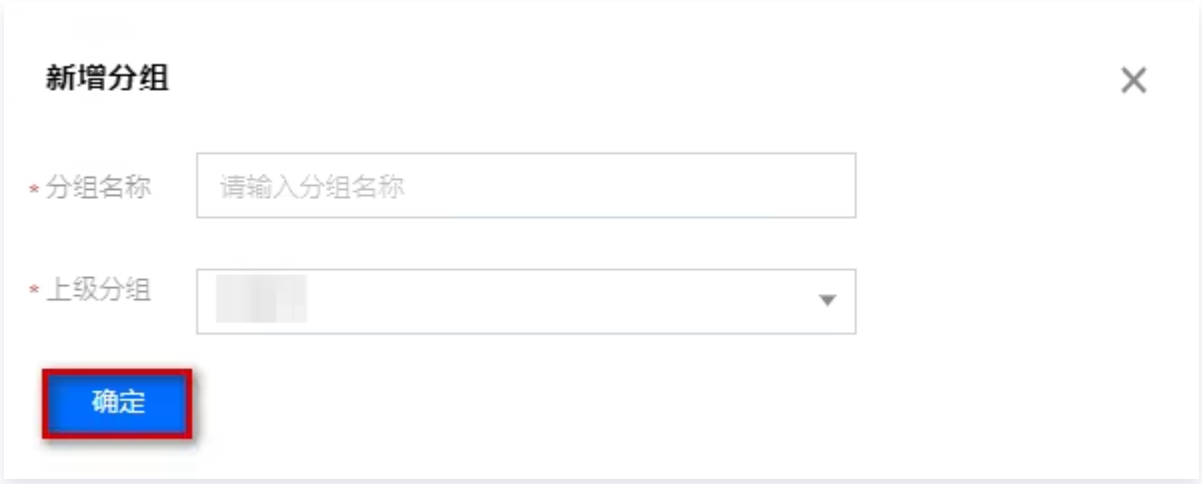
1. 在 组织架构管理 页面，选择所需目录，单击**目录名称**。



2. 在组织架构页面，展示目录组织架构下的账户分组以及账户情况。单击 ... > **添加分组**，可以在此分组下新增次级分组。



3. 在新增分组弹窗中，输入分组名称，选择上级分组，单击**确定**。



新建单个账户

1. 在组织架构页面，单击**新增账户**。



2. 在账户管理页面，配置相关参数，单击**确定**。



登录客户端

打开客户端，任意输入自建的账号密码，即可完成登录。

iOA SaaS 企业微信对接（11.1.1版）

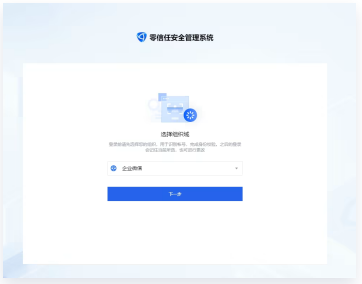
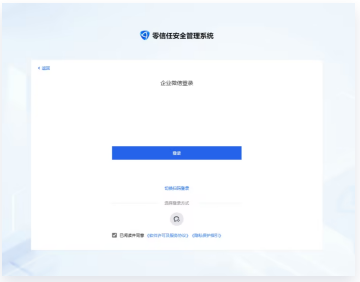
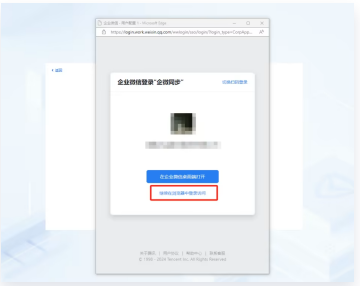
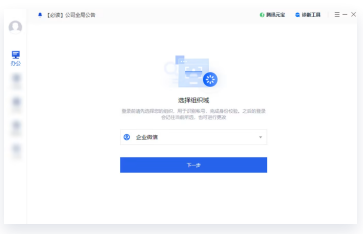
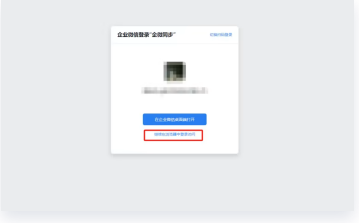
最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

- 身份源：您导入组织架构的企业微信会和使用的 iOA 产品进行绑定，您可以给已导入的企业微信身份源创建多个身份目录进行同步。
- 认证源：您创建的企业微信认证源需要和您导入企业微信身份源保持一致。相同企业微信的认证源可以创建多个，不受此影响。

> **说明：**
> iOS 端如需使用“企业微信对接”，请联系 iOA 项目技术支持人员，我们需要在后台配置登录参数，可以提供 iOS 端的登录 Demo。

1. 实现效果

类型、操作步骤	选择组织域	选择登录方式	登录效果
浏览器登录效果			
客户端			

2. 企业微信认证准备

2.1 资源准备

由于企业微信需要通过受信域名才能进行对接，所以需要您提前准备：

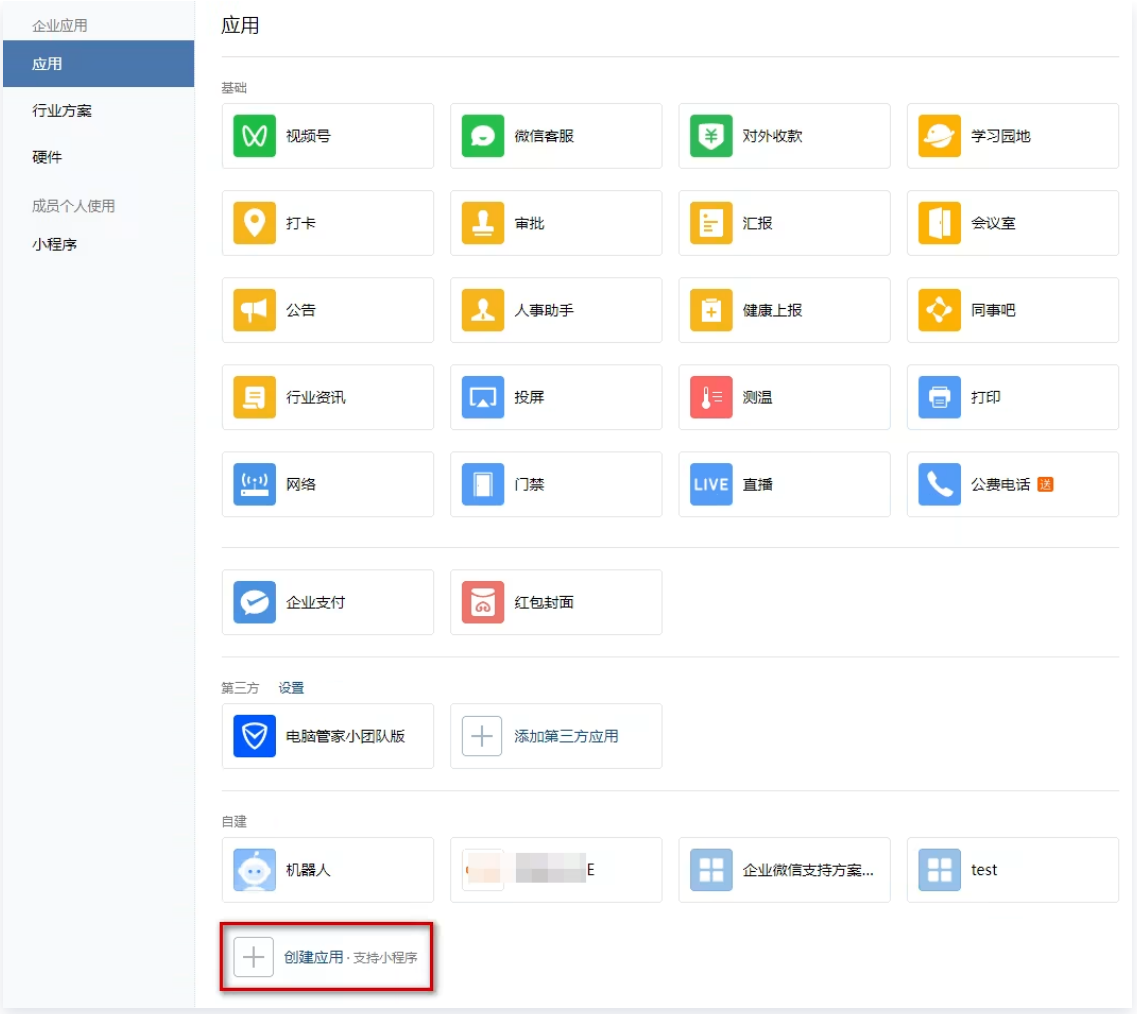
> **说明：**
> - 需配置备案主体与当前企业主体相同或有关联关系的域名，详情请参见 企业内部开发配置域名指引 。
> - 如果已有二级域名且通过了备案，可跳过下文步骤1和步骤2。

- 步骤1： 申请一个域名 。
- 步骤2： 域名备案 。
- 步骤3： 申请或上传域名的SSL证书 。
- 步骤4：准备部署连接器的服务器（建议配置：Centos7.6 CPU：2-4核，内存4-8G，硬盘100G以上）。

2.2 配置企业微信自建应用

2.2.1 新建自建应用

1. 登录 企业微信管理后台 ，单击上方的**应用管理**，默认进入应用页面。
2. 在应用页面，单击**自建** > **创建应用**。



3. 在创建应用页面，配置相关参数，单击**创建应用**。

> **注意：**
> 可见范围务必包含需要同步的组织范围，否则无法同步组织；建议设置为根目录。



2.2.2 设置可信域名

1. 登录 企业微信管理后台 ，单击上方的**应用管理**，在应用页面，单击刚刚创建的**自建应用**。
2. 在应用详情页面，选择**网页授权及JS-SDK**，单击**设置可信域名**。



3. 在设置可信域名窗口中，单击**申请校验域名**。



4. 在设置可信域名窗口中，单击**下载文件**。



5. 可先关闭页面，待iOA SaaS 控制台配置完成后再输入可信域名，单击**确定**，完成可信域名校验。

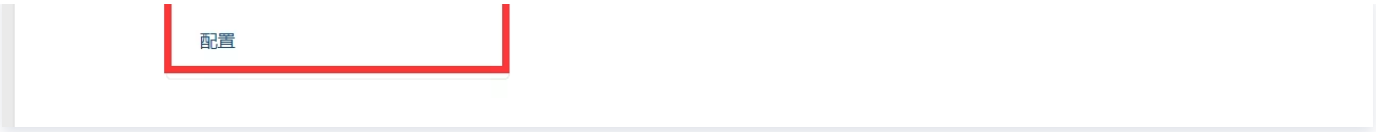
> **说明：**
> 可信域名由 3.2 认证源配置 后获取，再填写到此处，进行可信域名校验。因此当前先跳过此可信域名填写步骤。



2.2.3 设置企业可信 IP

1. 在应用页面，单击刚刚创建的**自建应用**。
2. 在应用详情页面，选择开发者接口，单击企业可信 IP 中的**配置**。


企业微信
API文档 | 联系客服 | 退出
首页
通讯录
协作
应用管理
客户与上下游
高级功能
安全与管理
我的企业
返回
企微DLP
企微DLP
暂无应用介绍
已启用
AgentId
编辑
Secret
查看
可见范围
未命名企业
管理员
应用负责人
设置 将企业成员配置为应用负责人，成员即可在企业微信内管理此应用
应用主页
设置 从工作台点击进入的网页/小程序
功能
发送消息
使用管理工具中的"消息群发"或API发送消息
发消息 历史消息
接收消息
接收用户发送的普通消息以及菜单操作、外部联系人变更回调等事件信息
查看消息 设置API接收
自动回复
通过接收用户的消息，可配置规则进行自动回复
设置
自定义菜单
可在应用会话的底部配置快捷操作菜单
设置
配置到聊天附件栏
将应用页面配置到聊天附件栏，方便成员快捷发送到聊天，提高沟通效率
配置
配置到聊天工具栏
将应用页面配置到聊天工具栏，方便成员在与客户的聊天中查看和使用，提高服务效率
配置
工作台自定义展示
工作台应用入口展示为预设模板样式，可通过API实时更新内容
当前配置： 未配置
进入
开发者接口
网页授权及JS-SDK
可信域名：
m
已启用
企业微信授权登录
使用企业微信账号登录已有的Web网页或移动APP
设置
审批接口
使用企业微信审批能力，在非审批应用内设置流程、发起审批。还能订阅通知消息，接收审批状态变化情况。
设置
企业可信IP
仅所配IP可通过接口获取企业数据，已配置1个IP。



3. 在企业可信 IP 窗口中，输入 IP 地址，单击**确定**。

> **说明：**
> 可信 IP 由 3.2 认证源配置 后获取，再填写到此处。因此当前先跳过此企业可信 IP 填写步骤。



2.2.4 设置企业微信授权回调域

1. 在应用页面，单击刚刚创建的**自建应用**。
2. 在应用详情页面，选择开发者接口，选择**企业微信授权登录**。



3. 单击**设置授权回调域**，填写web网页授权回调域：`scs.gateway.tencent.com` 。



2.3 获取企业 ID 、自建应用 AgentId 和 Secret

2.3.1 获取企业 ID

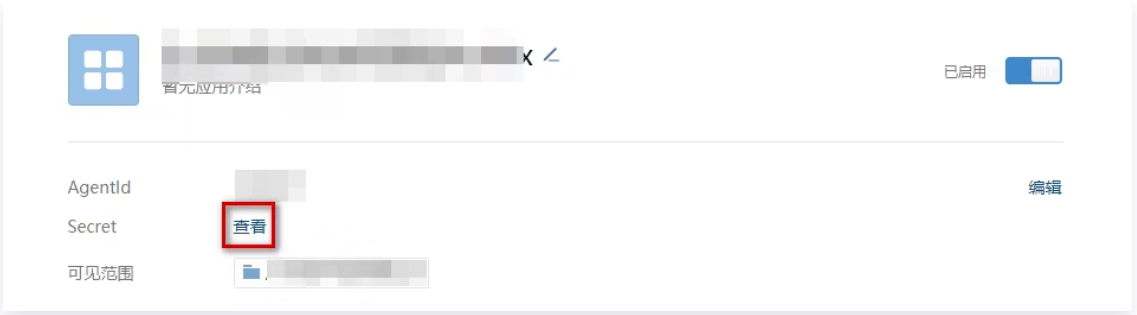
1. 登录 企业微信管理后台 ，单击上方的**我的企业**，默认进入企业信息页面。
2. 在企业信息页面的最下方，获取企业 ID。



2.3.2 获取自建应用 AgentId 和 Secret

1. 登录 企业微信管理后台，单击**应用管理**，并选中刚刚创建好的**自建应用**。
2. 在应用详情页面，查看AgentId，单击 Secret 右侧的**查看**，将 Secret 内容复制并保存。

> **注意：**
> 为确保数据安全，请确认为企业内部使用，切勿将 Secret 泄漏给第三方。



2.3.3 获取自建应用 Schema

1. 登录 企业微信管理后台，单击**应用管理**，并选中刚刚创建好的**自建应用**。
2. 在应用详情页面，进入“企业微信授权登录”，Schema 参数是企微平台自动生成的，直接获取即可，将 Schema 内容复制并保存。



3. 填写企业微信授权登录信息。
   - Web 网页：设置授权回调域 `scs.gateway.tencent.com` 。
   - iOS：设置 Bundle ID `com.tencent.ioa.saas` 。
   - Android：设置应用签名 `9e4e6594cd64562c6ae8e3ae0288dd5a` ， 应用包名 `com.tencent.ioa.saas` 。



3. iOA SaaS 控制台配置

3.1 连接器部署

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**无边界办公 > 连接器管理**。

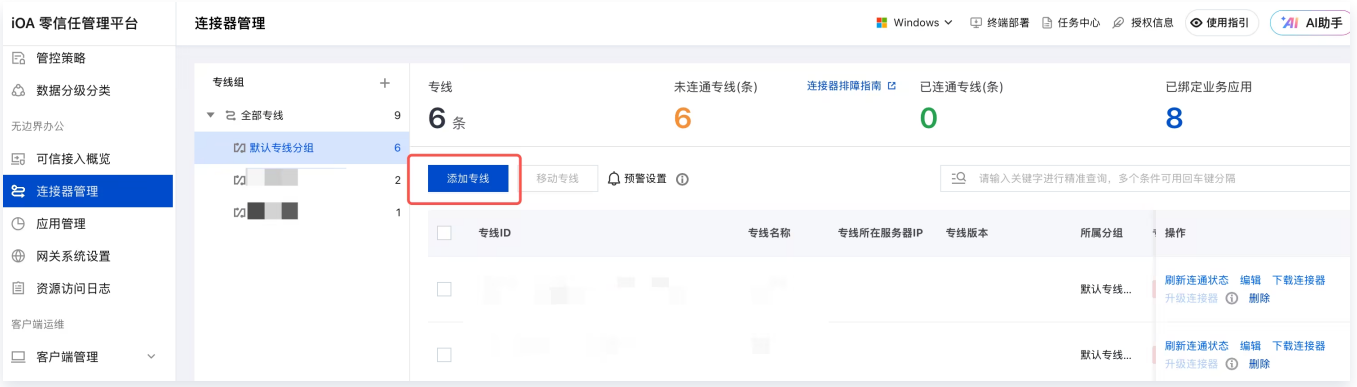
2. 在专线管理页面，单击 ＋ ，新建专线分组。



3. 编辑专线组名称：示例：企业微信对接，单击**确定**。



4. 在连接器管理页面，单击**添加专线**。



5. 按提示完成连接器部署。详细步骤可参考 连接器部署（11.1.1版）。



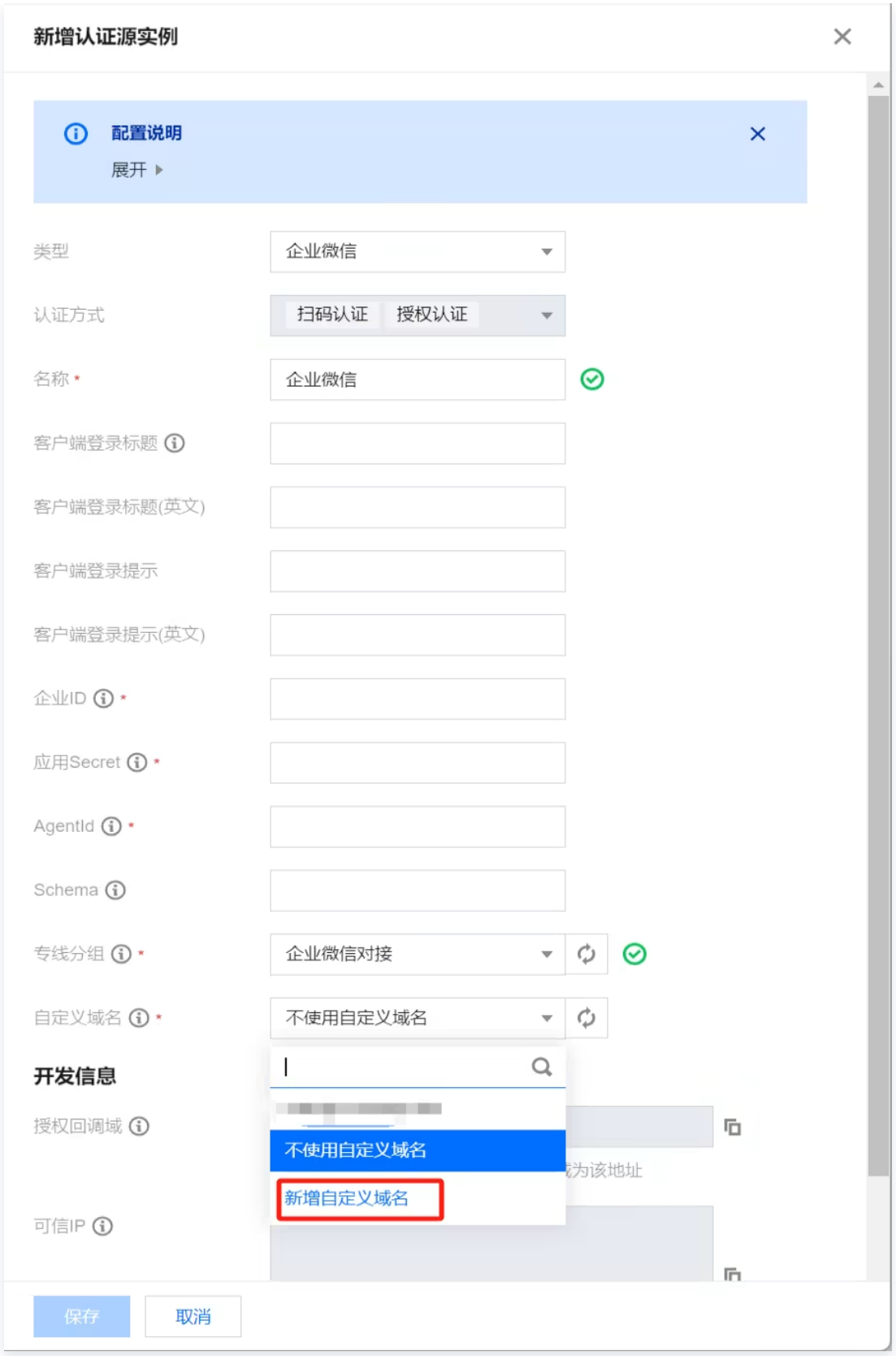
说明：
部署完成后该专线分组下不建议再添加专线，如需添加，应将新加连接器出口 IP 添加至企业微信自建应用的可信IP处。

3.2 认证源配置

1. 登录 iOA 零信任管理平台控制台，在左侧导览中，单击**身份安全管控 > 认证源配置**。



2. 在认证源配置页面，单击**新增认证源实例**。



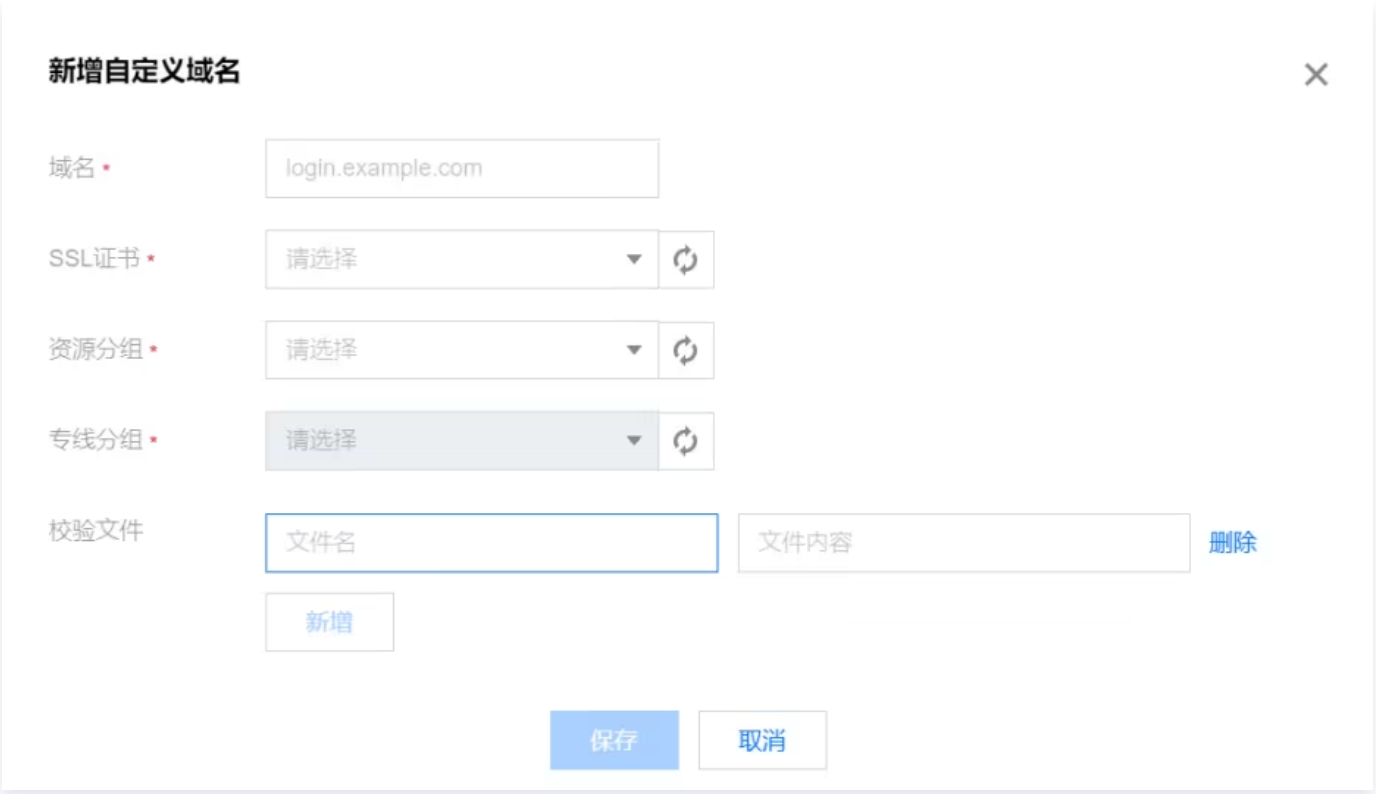
参数名称	说明
类型	企业微信。
名称	自定义。

客户端登录标题	自定义。
客户端登录标题（英文）	自定义。
客户端登录提示	自定义。
客户端登录提示（英文）	自定义。
企业 ID	详情请参见：2.3.1 获取企业 ID 。
应用 Secret	详情请参见：2.3.2 获取自建应用 AgentId 和 Secret 。
AgentId	详情请参见：2.3.2 获取自建应用 AgentId 和 Secret 。
Schema	详情请参见：2.3.3 获取自建应用 Schema（移动端）。
专线分组	选择 连接器部署（11.1.1版） 新建的专线分组。
自定义域名	选择 “新增自定义域名 ”，参数请参看下文填写说明。

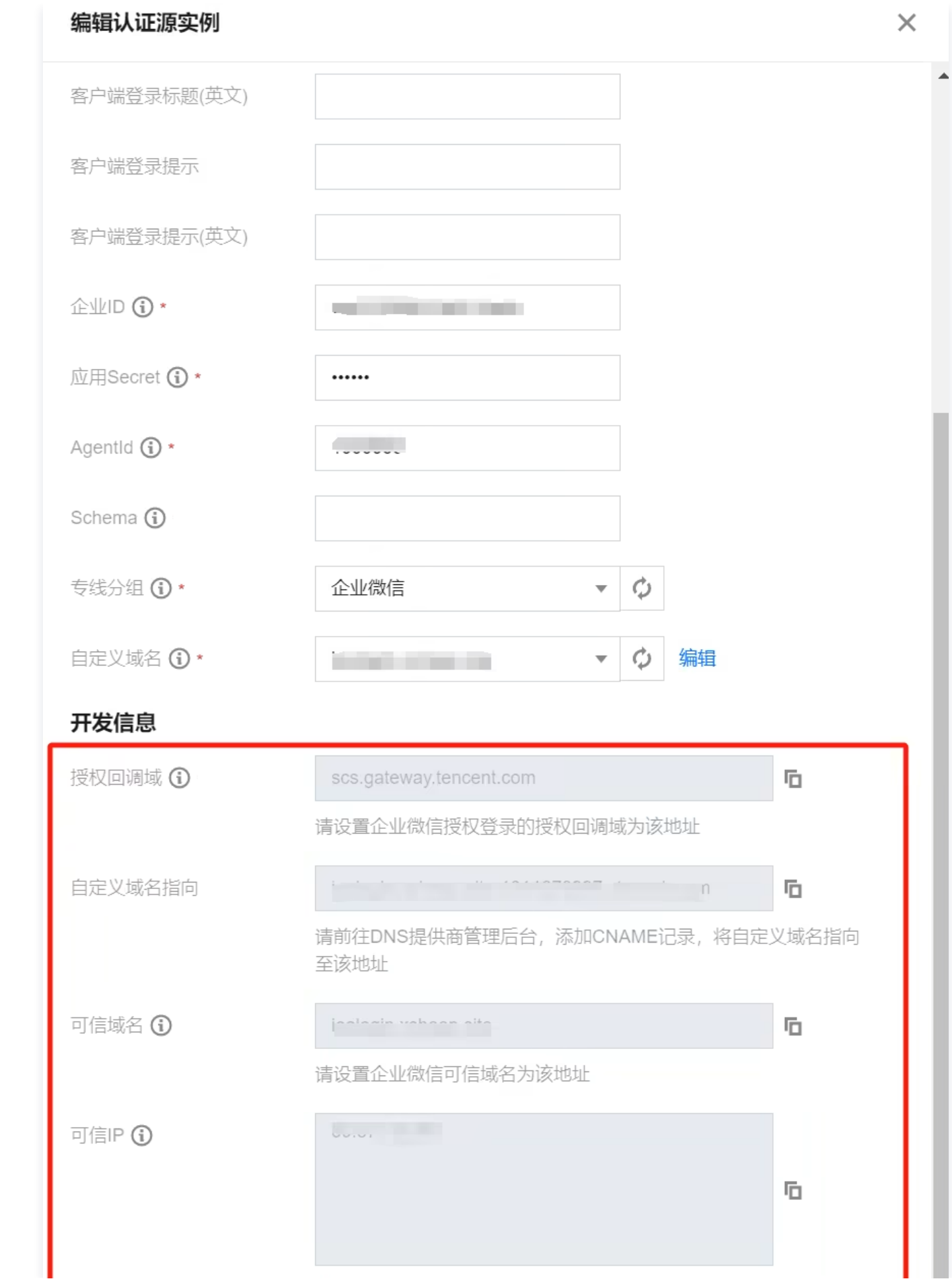
新增自定义域名填写说明：

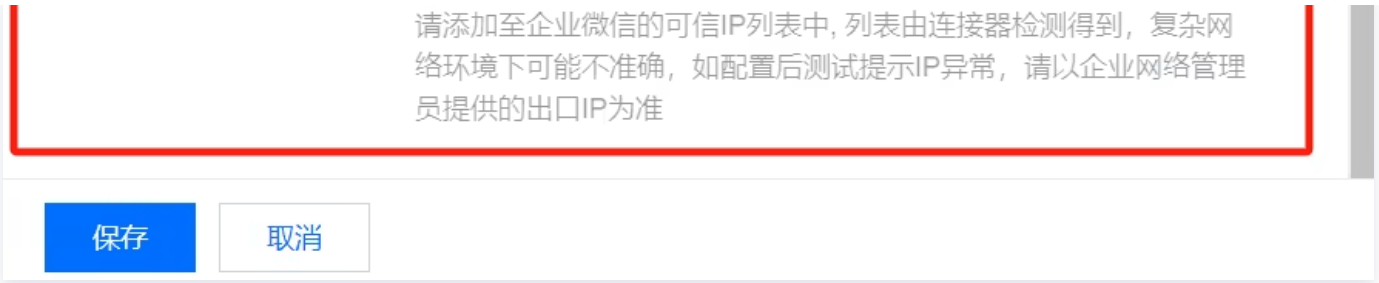
参数名称	说明
域名	填写准备的子域名。
SSL证书	选择该域名的SSL证书。
资源分组	建议一个资源分组并选择该分组。
专线分组	选择 3.1 连接器部署 新建的专线分组。
校验文件	填写 2.2.2 设置可信域名 获取的校验文件名（需加后缀，如：WW_xx.txt）及文件内容。

说明：
特别说明：新增自定义域名后会在所选择的资源分组下自动生成两个web资源，该资源禁止修改，建议新建一个资源分组存放。



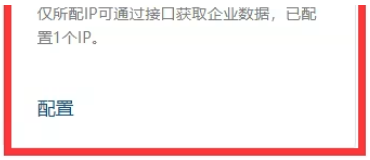
3. 将下方生成的信息保留，并单击**保存**。
   - 将自定义域名修改CNAME解析指向‘自定义域名指向’的域名。
   - 待解析生效后，返回2.2 配置企业微信自建应用，将‘授权回调域’、‘可信域名’、‘可信IP’填写到企微自建应用处。


编辑认证源实例
客户端登录标题(英文)
客户端登录提示
客户端登录提示(英文)
企业ID *
应用Secret *
AgentId *
Schema
专线分组 *
企业微信
自定义域名 *
编辑
开发信息
授权回调域
scs.gateway.tencent.com
请设置企业微信授权登录的授权回调域为该地址
自定义域名指向
请前往DNS提供商管理后台，添加CNAME记录，将自定义域名指向至该地址
可信域名
请设置企业微信可信域名为该地址
可信IP



4. 登录 企业微信管理后台 。
   - 授权回调域填写至：2.2.4 设置企业微信授权回调域 。
   - 可信域名填写至：2.2.2 设置可信域名 。
   - 可信 IP 填写至：2.2.3 设置企业可信 IP 。


企业微信
API文档 | 联系客服
首页
通讯录
协作
应用管理
客户与上下游
高级功能
安全与管理
我的企业
« 返回
企微DLP
已启用
AgentId
编辑
Secret
查看
可见范围
未命名企业
管理员
应用负责人
设置 将企业成员配置为应用负责人，成员即可在企业微信内管理此应用
应用主页
设置 从工作台点击进入的网页/小程序
功能
发送消息
使用管理工具中的"消息群发"或API发送消息
发消息 历史消息
接收消息
接收用户发送的普通消息以及菜单操作、外部联系人变更回调等事件信息
查看消息 设置API接收
自动回复
通过接收用户的消息，可配置规则进行自动回复
设置
自定义菜单
可在应用会话的底部配置快捷操作菜单
设置
配置到聊天附件栏
将应用页面配置到聊天附件栏，方便成员快捷发送到聊天，提高沟通效率
配置
配置到聊天工具栏
将应用页面配置到聊天工具栏，方便成员在与客户的聊天中查看和使用，提高服务效率
配置
工作台自定义展示
工作台应用入口展示为预设模板样式，可通过API实时更新内容
当前配置： 未配置
进入
开发者接口
网页授权及JS-SDK
可信域名：dev.scs.gateway.tencent.com
已启用 >
企业微信授权登录
使用企业微信账号登录已有的Web网页或移动APP
设置
审批接口
使用企业微信审批能力，在非审批应用内设置流程、发起审批。还能订阅通知消息，接收审批状态变化情况。
设置
企业可信IP

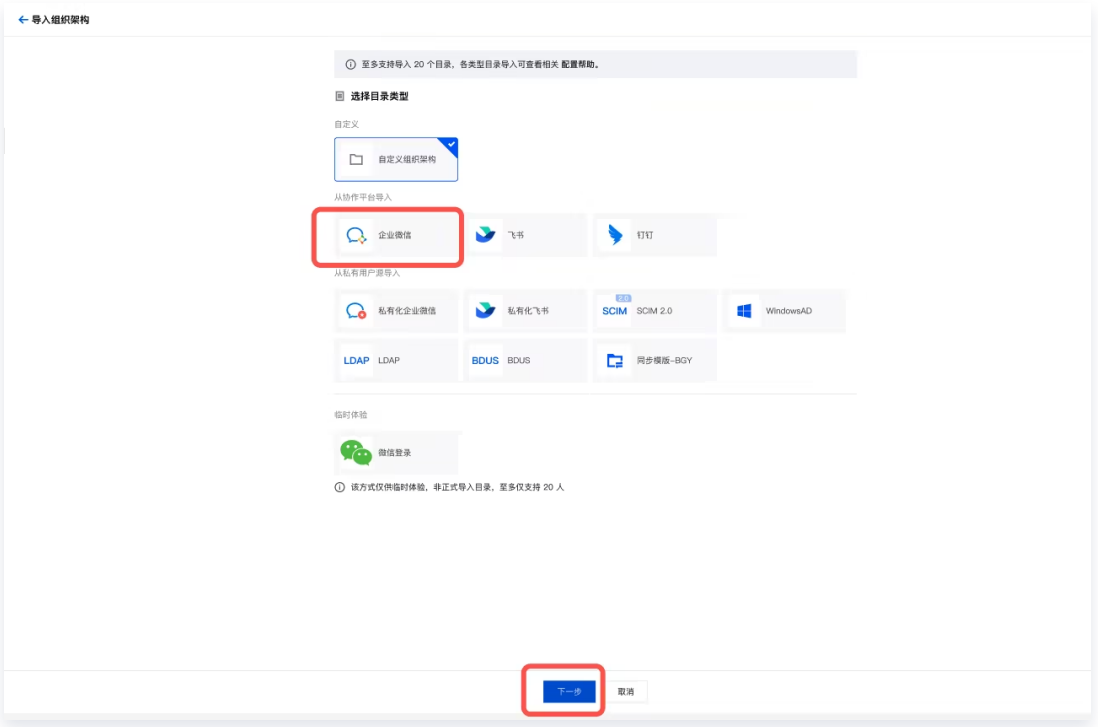


3.3 身份源配置

1. 登录 iOA 零信任管理平台控制台，在左侧导览中，单击**组织架构管理**。
2. 在组织架构管理页面，单击**新增组织架构**。

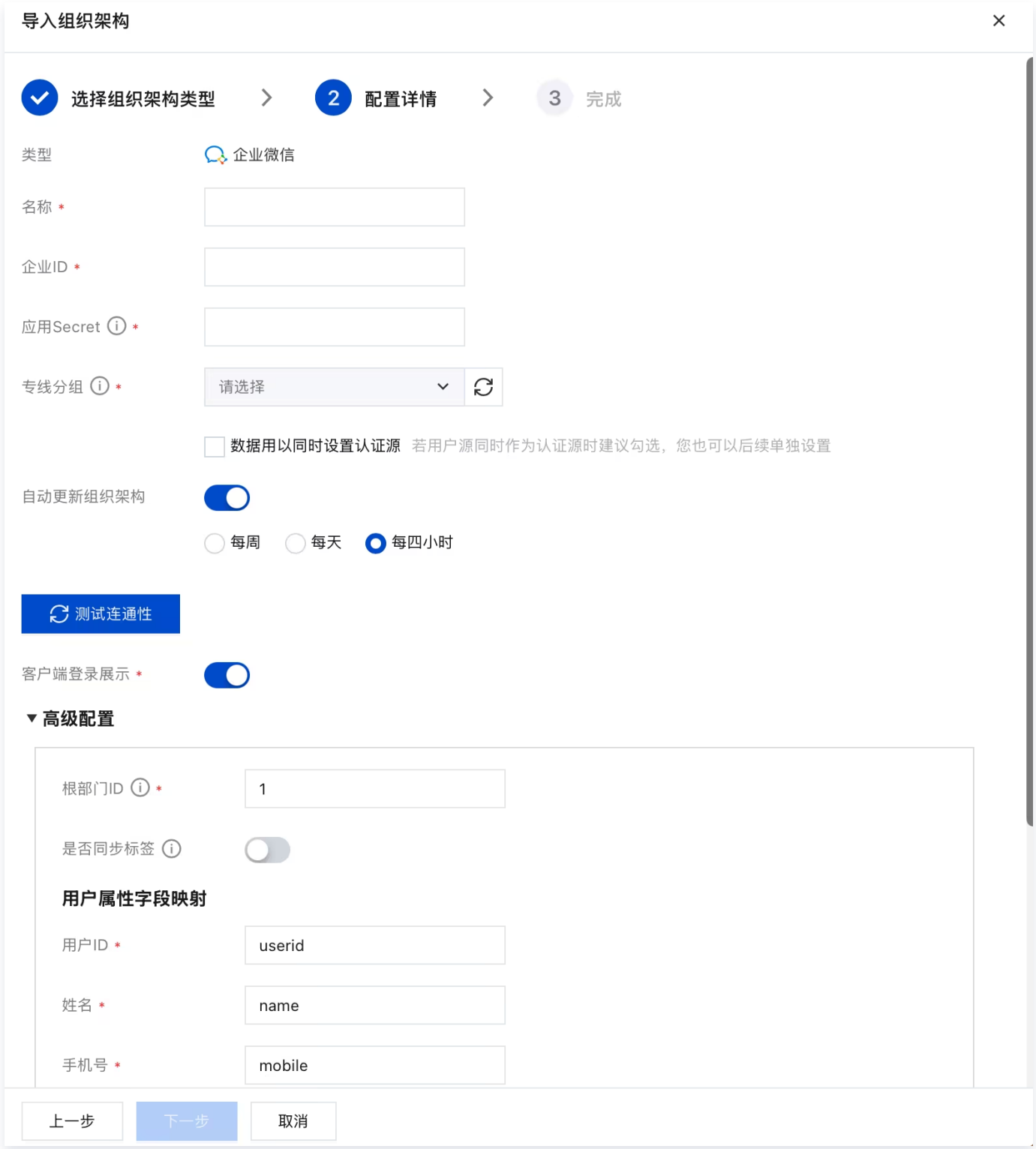


3. 在导入组织架构页面，选择**企业微信**，单击**下一步**。



4. 在组织架构配置页面，配置相关参数。

> **注意：**
>
> 请确认已经准备好了企业自建应用，连接器已部署完毕，具体操作：
>
> - 输入企业ID、企业自建应用 Secret 和选择专线分组后可进行连通性测试，会同时检查基础配置是否有效（企业 ID、应用 Secret 详细请参见：2.3 获取企业 ID 、自建应用AgentId和Secret ）。
> - 状态字段如果不映射，将会用系统定义的状态，其中 0 表示用户异常状态， 1 表示用户正常状态。映射支持三种数据类型，且必须填写【正常状态的值】
>
> ① 对于 Bool 类型和 String 类型，相同的值会关联到状态 1，不相同的统一到 0；
>
> ② 对于 Int 类型，相同的值会关联到状态 1，其他值会默认保留。
> - 属性映射中，若映射字段不存在或不想同步相应字段，则输入任意不存在的属性名即可，同步时会将对应属性置为空。
> - 相同企业微信的认证源可以创建多个。



参数名称	说明
类型	企业微信
企业 ID	获取方式请参见 获取企业 ID 和自建应用 Secret 。
应用	获取方式请参见 获取企业 ID 和自建应用 Secret 。

Secret	
专线分组	选择 连接器部署（11.1.1版）创建的专线分组名称。
连通性测试	输入企业 ID、应用 Secret 、专线分组后可进行连通性测试，会同时检查基础配置是否有效。
自动更新组织架构	根据实际需求设置。
根部门ID	如果只需要特定部门，请输入正确的部门ID。如无必要，请勿修改，配置已经正常同步数据的情况下，随意变更可能会导致数据异常
是否同步标签	同步的标签数据会写入自定义分组
用户属性字段映射	如无特殊需求，请勿修改。 其中字段如果不映射，将会用系统定义的状态，其中0 表示用户异常状态，1 表示用户正常状态。 映射支持三种数据类型，且必须填写正常状态的值： 1. 对于 Bool 类型和 String 类型，相同的值会关联到状态 1，不相同的统一到 0； 2. 对于 Int 类型，相同的值会关联到状态 1，其他值会默认保留。 属性映射中，若映射字段不存在或不想同步相应字段，则输入任意不存在的属性名即可，同步时会将对应属性置为空。

5. 配置完成后单击**下一步**并保存。
6. 在组织架构管理页面，找到刚刚创建的目录，单击**目录管理**，查看组织架构信息。



3.4 认证策略配置

说明：

- 企业微信认证源需要和您导入企业微信身份源(目录)保持一致。
- 可以为不同身份源（目录）配置不同的认证策略，互不影响。
- 如果针对单个身份源（目录）添加主认证源，需要在该身份源（目录）的**基础策略中**增加认证源。

1. 在**身份安全管控** > **认证策略**页面，选择目标目录，单击**编辑**。



2. 在编辑认证策略页面，PC 端将刚刚添加的企业微信认证源作为主认证方式。



3. 单击**添加**，完成编辑。


PC端
主认证方式的认证源
企业微信
AD域环境免认证
双因素认证
是否启用
二次认证方式的认证源
请选择
指定主认证登录豁免双因素
请选择
挑战认证方式认证源
企业微信
移动端
主认证方式的认证源
企业微信
双因素认证
是否启用
二次认证方式的认证源
请选择
指定主认证登录豁免双因素
请选择
挑战认证方式认证源
企业微信
添加
取消

版权所有：腾讯云计算（北京）有限责任公司

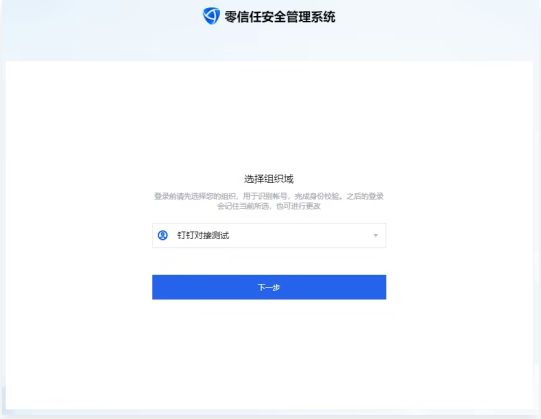
iOA SaaS 钉钉对接（11.1.1版）

最近更新时间：2026-02-13 09:41:01

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 实现效果

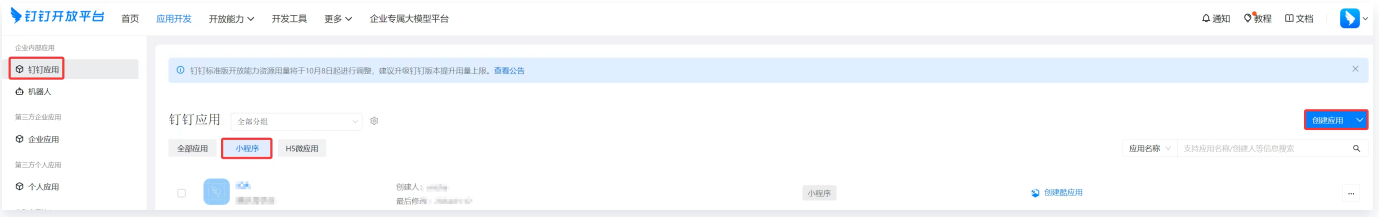
> **说明：**
> iOS 端如需使用“钉钉对接”，请联系 iOA 项目技术支持人员，我们需要在后台配置登录参数，可以提供 iOS 端的登录 Demo。

类型	选择组织域	登录效果
浏览器登录效果		
客户端登录效果		

2. 钉钉认证准备

2.1 配置钉钉自建应用

1. 登录 钉钉管理后台，在左侧导航栏中，单击**钉钉应用**。
2. 创建一个自建应用：**应用开发** > **钉钉应用** > **小程序**，单击**创建应用**。



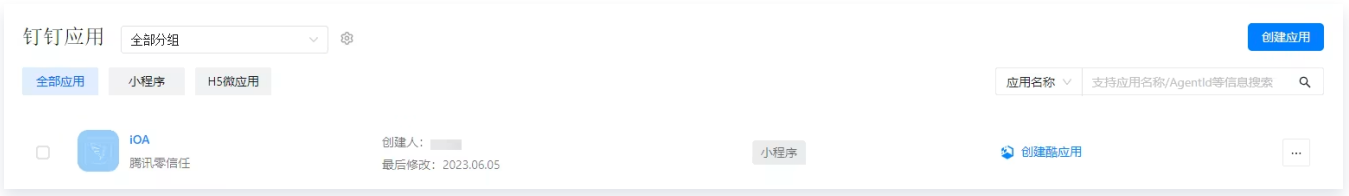
3. 在创建应用窗口中，配置相关参数，单击**保存**即可完成创建。



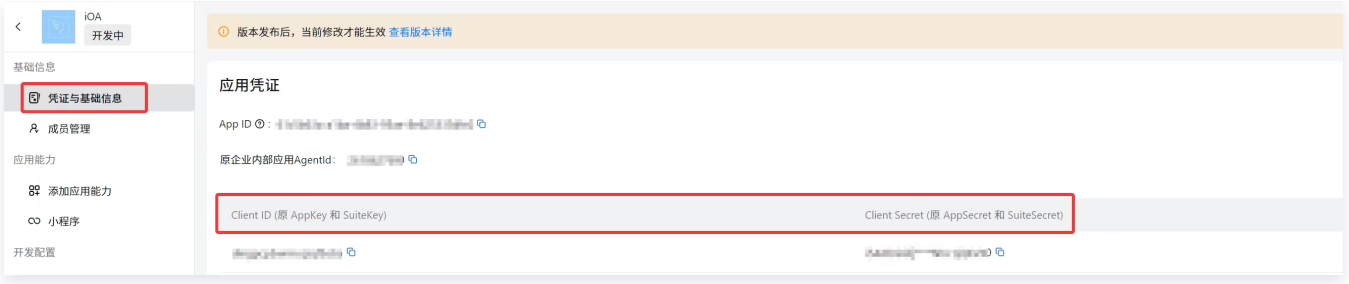
参数名称	说明
应用名称	自定义，示例：腾讯 iOA。
应用描述	自定义描述。

2.2 获取该应用的 AppKey 和 AppSecret

1. 在**应用开发**页面，单击选择刚刚创建的**自建应用**。



2. 在**凭证与基础信息**页面，复制 AppKey 和 AppSecret，其中钉钉的 Client ID (原 AppKey 和 SuiteKey) 对应 iOA 控制台上的 AppKey，钉钉的Client Secret (原 AppSecret 和 SuiteSecret)对应 iOA 控制台的 AppSecret，请妥善保存，在接下来的 iOA 控制台常规配置会用到。

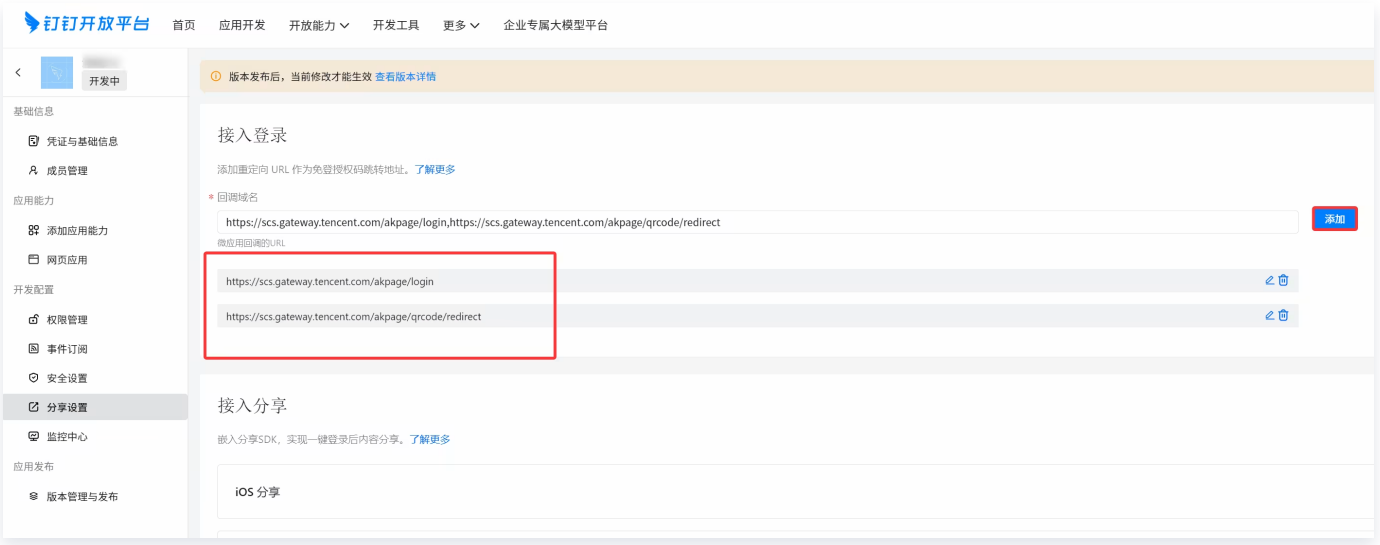


2.3 获取回调域名

1. 在**分享设置**页面，您可将以下 iOA 的网关回调域名链接添加到**回调域名**列表中。

   回调域名： `https://scs.gateway.tencent.com/akpage/qrcode/redirect` 。

   微应用回调的URL： `https://scs.gateway.tencent.com/akpage/login`。



2. 单击**添加**，即可将 iOA 的网关回调域名添加到钉钉的回调域名列表中。

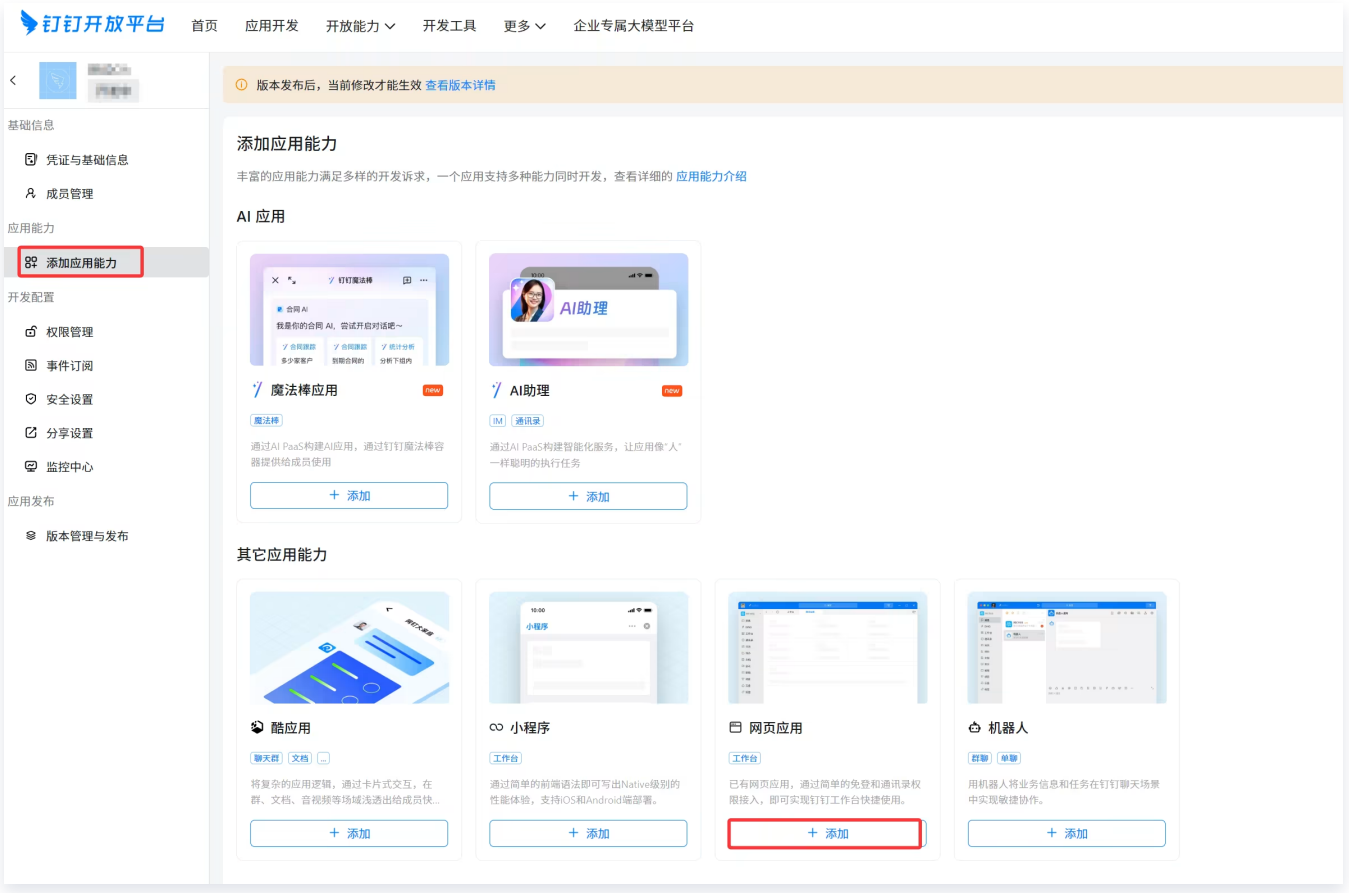
2.4 配置权限管理

1. 钉钉应用详情页面，单击**权限管理**，选择该应用所需的权限，如：
   - 调用企业 API 基础权限；
   - 调用 SNS API 时需要具备的基本权限；
   - 企业员工手机号信息；
   - 邮箱等个人信息；
   - 通讯录部门信息读权限；
   - 成员信息读权限；
   - 根据手机号获取成员基本信息权限；
   - 通讯录部门成员读权限；
   - 个人手机号信息；
   - 通讯录个人信息读权限。
2. 选中目标权限后，单击操作列的**申请权限**，即可为该应用开通所需权限。



2.5 配置首页地址

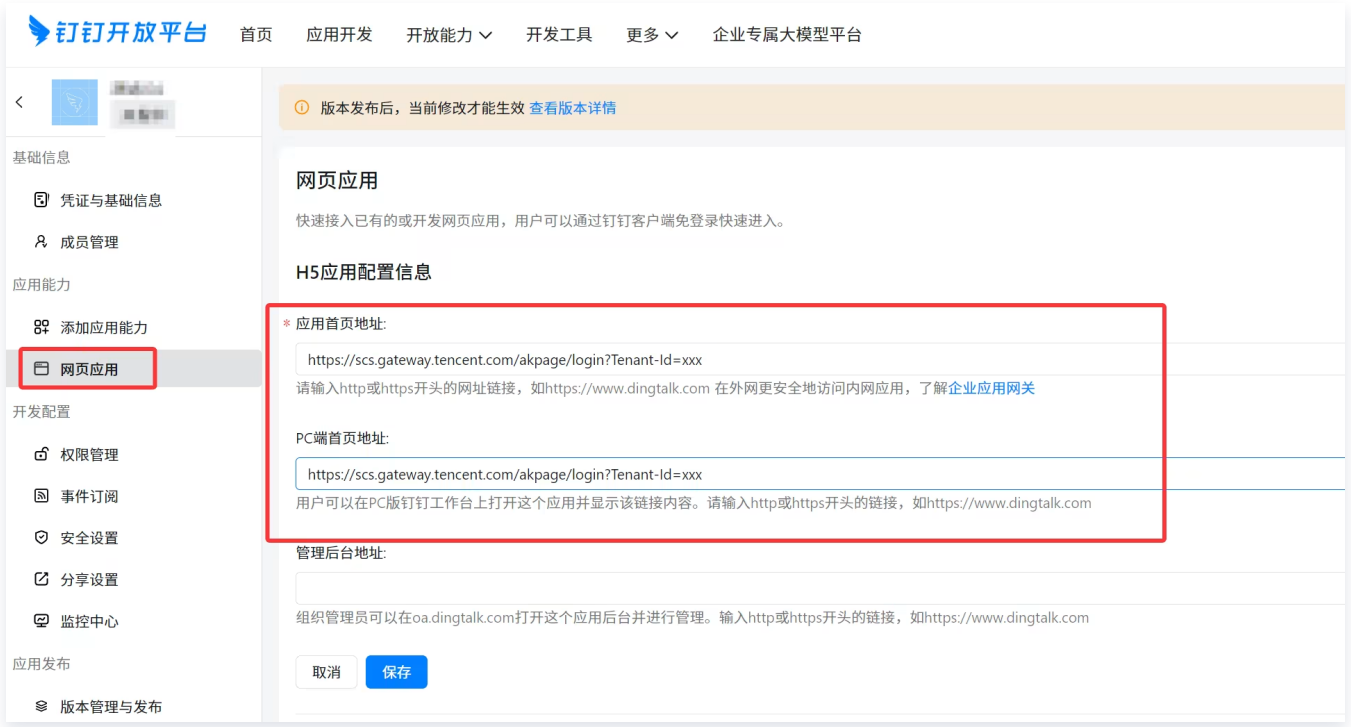
1. 在**应用能力 > 添加应用能力**页面，添加网页应用。



2. 进入网页应用界面，添加应用首页地址和 PC 端首页地址。

- **格式：** `https://scs.gateway.tencent.com/akpage/login?Tenant-Id=xxx（appid）`。

> **注意：**
> 需将链接结尾 xxx 替换为 appid。

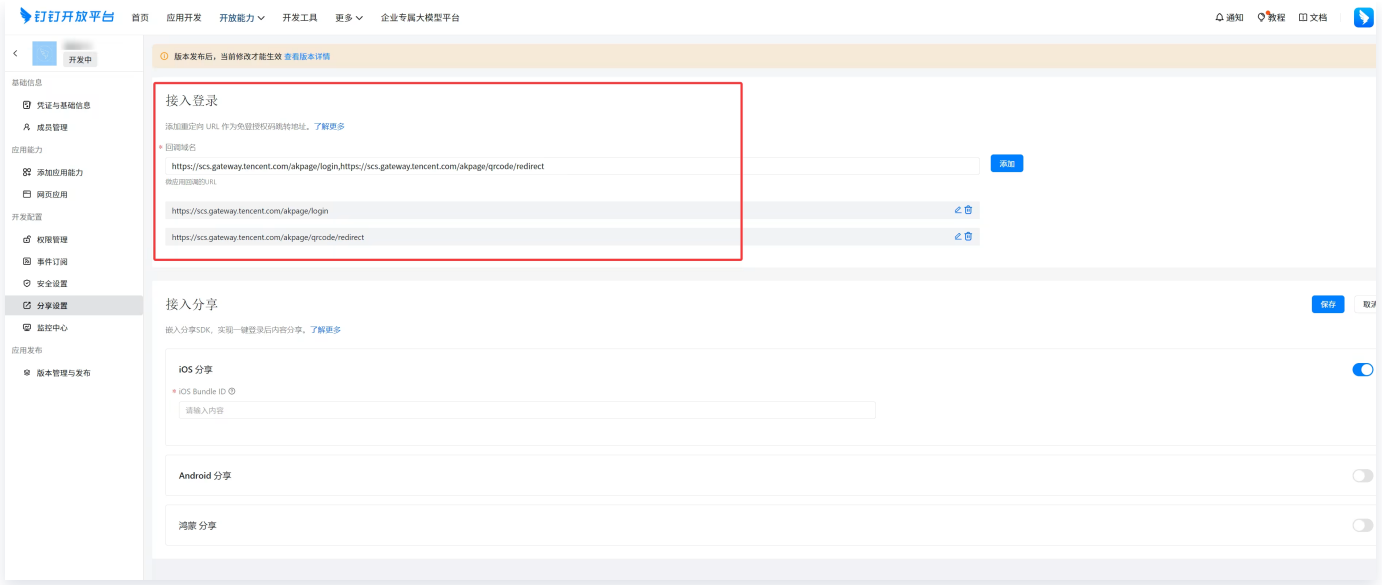


- AppID 获取地址：`https://console.cloud.tencent.com/developer`。



2.6 开启钉钉移动应用登录功能（选配）

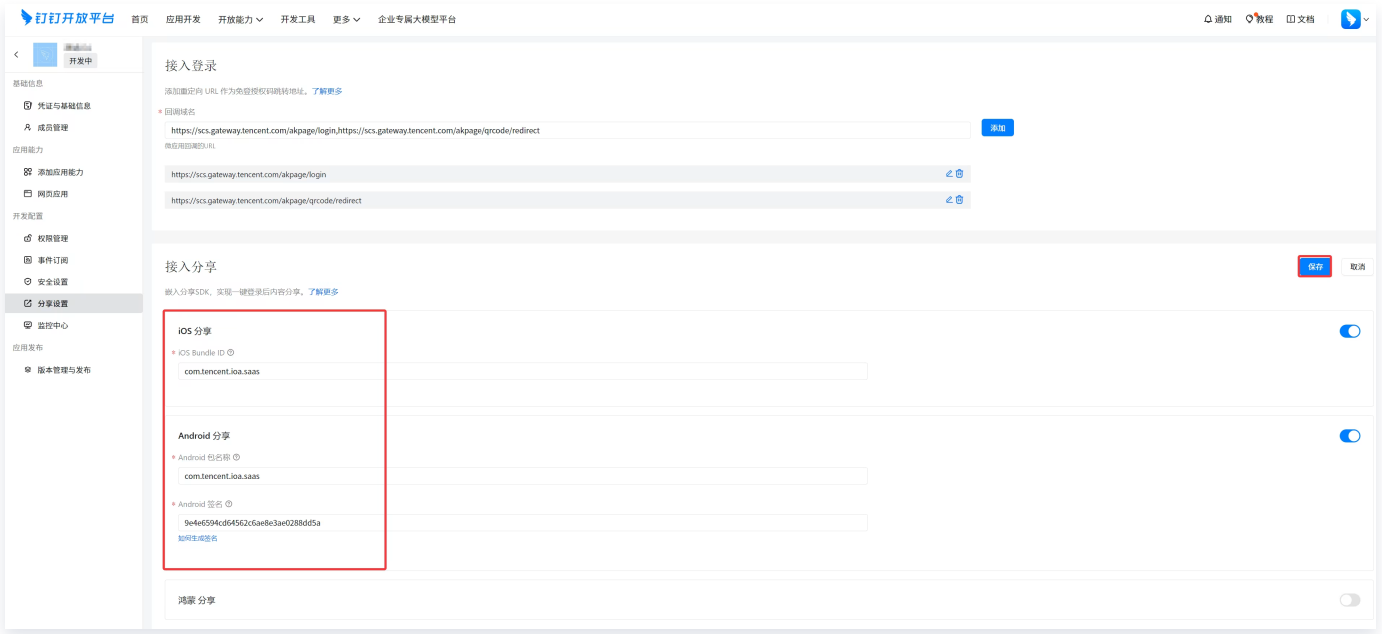
1. 如果移动端也需要使用钉钉方式调用登录，需要配置钉钉移动应用登录功能。
2. 在**开发配置** > **分享设置**中，配置接入分享。
3. 接入登录在 2.3 获取回调域名 中已配置。



4. 在接入分享中，请按如下信息配置：

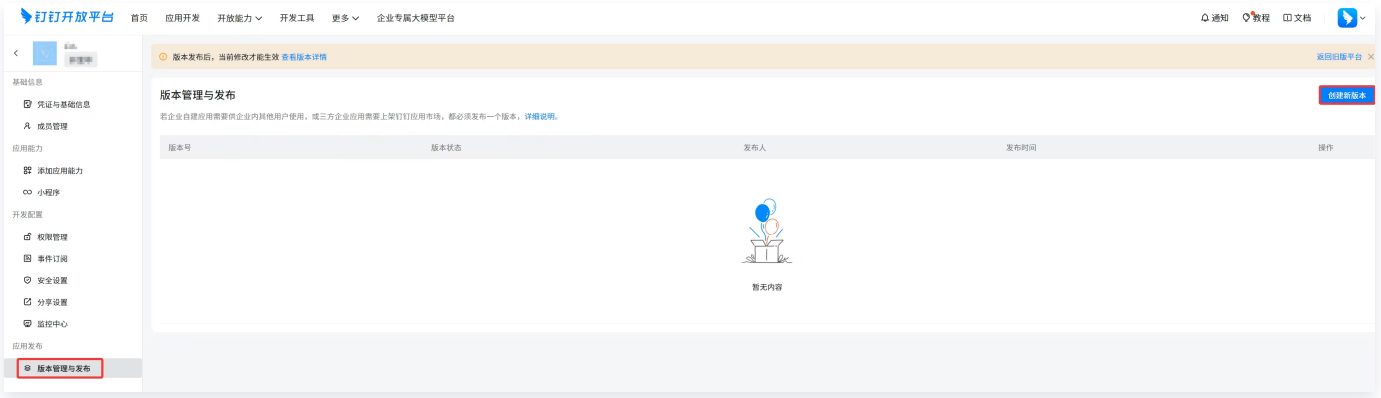
参数名称		说明
iOS 分享	iOS Bundle ID	com.tencent.ioa.saas
Android 分享	Android 包名称	com.tencent.ioa.saas
	Android 签名	9e4e6594cd64562c6ae8e3ae0288dd5a

5. 配置完成后，单击**保存**。



2.7 应用发布

1. 在应用发布–版本管理与发布处，**创建新版本**。



> **注意：**
> **应用修改了任意配置都需要重新发新版本（每一次更新配置，都需要发布新版本才会生效）。**

2. **应用可用范围需选择全部员工。**



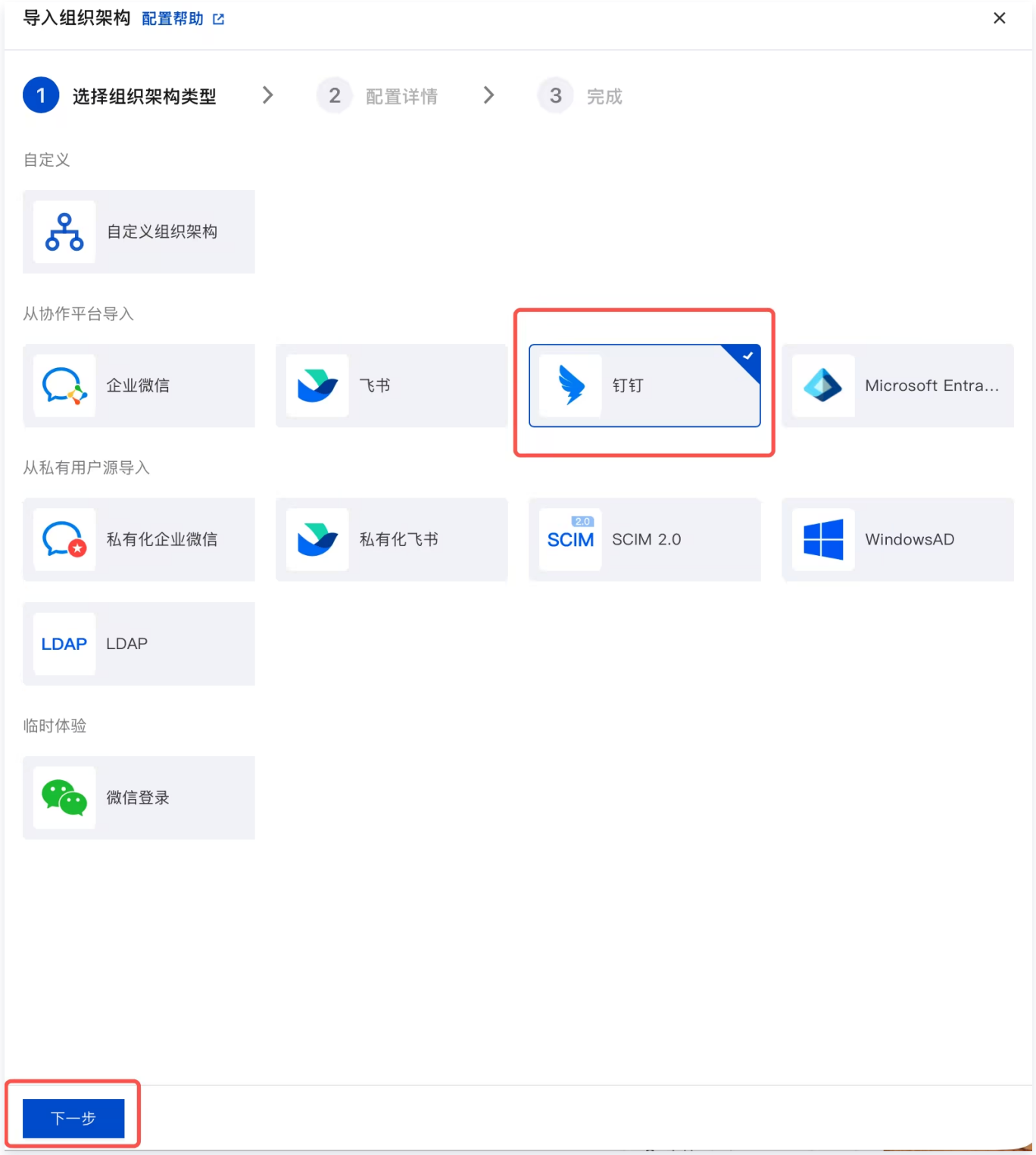
3. 配置 iOA SaaS 控制台

3.1 新建目录

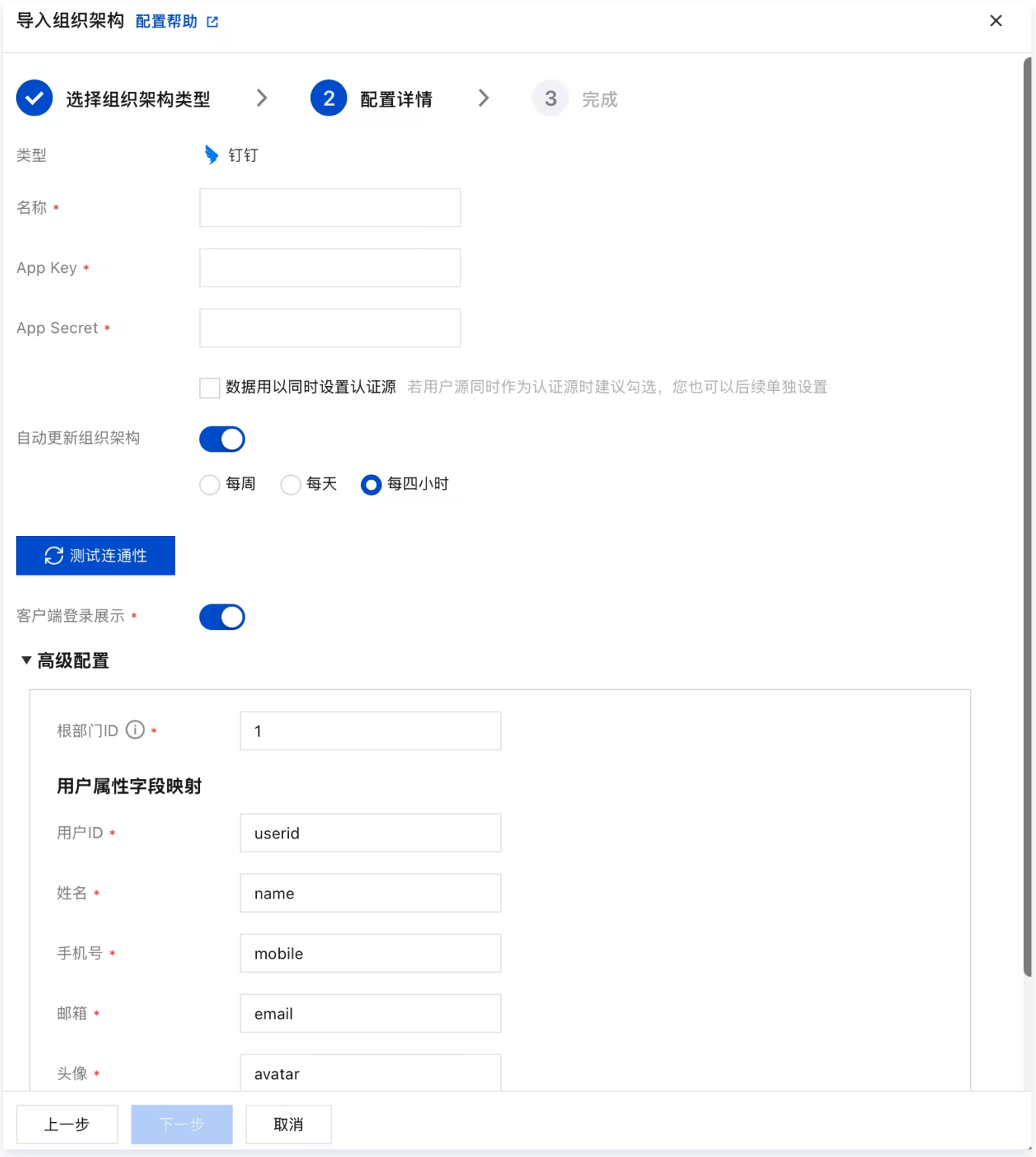
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏中，单击**员工与身份管理** > **组织架构管理**。
2. 在组织架构管理页面，单击**新增组织架构**。



3. 在导入组织架构页面，导入类型选择**钉钉**，单击**下一步**。



4. 在导入组织架构页面，输入 AppKey和 AppSecret，以及其他参数。



5. 单击**测试连通性**，测试通过后单击**下一步并保存**。



3.2 配置认证源

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏中，单击**身份安全管控** > **认证源配置**。

2. 在认证源配置页面，单击**新增认证源实例**。



3. 在新增认证源实例页面，类型选择**钉钉**，并配置其他参数，单击**保存**。

> **说明：**
> - AppKey：为钉钉的 AppKey 。
> - AppSecret：为钉钉的 AppSecret 。
> - CorpId：为钉钉的 CorpId 。



- CorpId 获取方式：**钉钉开放平台** > **首页**。



4. 填写完成后，单击**保存**。

3.3 设置认证策略

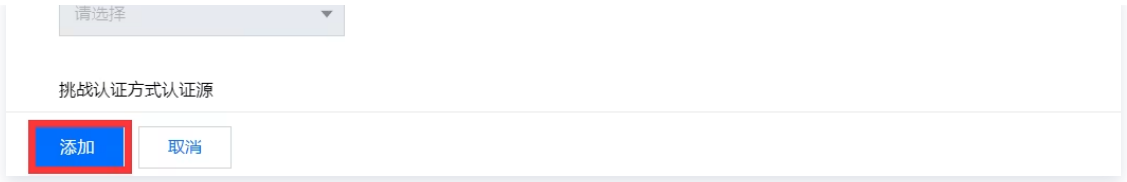
1. 在**身份安全管控** > **认证策略**页面，选择目标目录，单击**编辑**。



2. 在编辑认证策略页面，可根据自身需要设置 PC 端的主认证方式认证源和挑战认证方式认证源，认证源可设置多种（下图以认证源实例名称“钉钉对接测试”为例）。

> **注意：**
> 如您要使用钉钉 App 内的应用免登录，您还需要设置移动端的主认证方式认证源和挑战认证方式认证源，设置方式与 PC 端相同。


编辑认证策略
基本信息
适用范围
配置认证安全策略
基本信息
* 策略名称
基础策略
4/144
策略描述
填写描述
0/288
策略执行优先级
最低
优先级标记为 1，当策略冲突时,会优先执行该策略
适用范围
适用对象
类型
操作
钉钉
组织架构
删除
设定适用范围
配置认证安全策略
单个目录下的主认证方式由基础策略决定，如需调整主认证方式，请修改基础策略的主认证源选择
PC端
主认证方式的认证源
钉钉对接测试
AD域环境免认证
双因素认证
是否启用
二次认证方式的认证源
请选择
指定主认证登录豁免双因素
请选择
挑战认证方式认证源
钉钉对接测试
移动端
主认证方式的认证源
钉钉对接测试
双因素认证
是否启用
二次认证方式的认证源
请选择
指定主认证登录豁免双因素



3. 单击**添加**，完成认证策略配置。

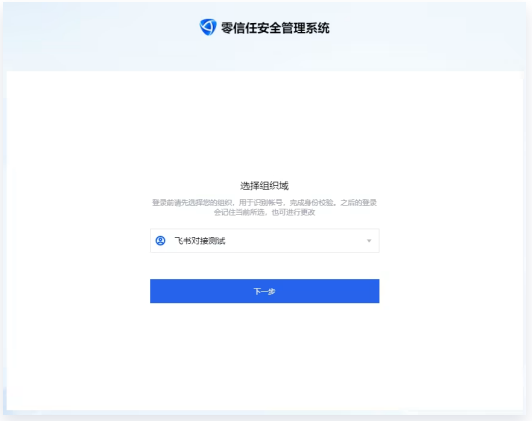
iOA SaaS 飞书（11.1.1版）
方案1：飞书认证（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录效果

> **说明：**
> - **iOS 端如需使用“飞书认证”，请联系 iOA 项目技术支持人员，我们需要在后台配置登录参数，可以提供 iOS 端的登录 Demo。**
> - iOA SaaS 飞书对接配置推荐使用方案1：飞书认证。

类型	选择组织域	登录效果
浏览器		

客户端		

2. 飞书认证准备

2.1 配置飞书信息

1. 如您是首次使用，未创建企业自建应用：

   1.1 未创建企业自建应用，需要创建一个企业自建应用，登录 飞书开放平台 ，选择**企业自建应用**，单击**创建企业自建应用**。



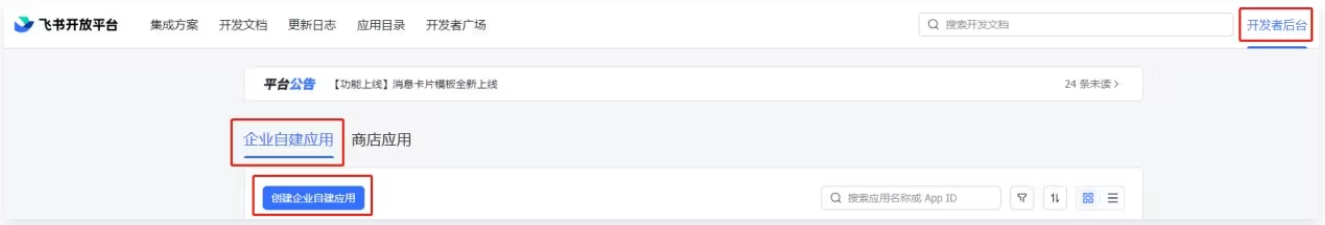
   1.2 在创建企业自建应用窗口中，配置相关参数，单击**创建**，即可完成创建。



2. 如您未开通飞书开发者账号：

2.1 请先前往飞书开放平台，创建一个开发者账号。

2.2 在开发者后台，选择**企业自建应用**，单击**创建企业自建应用**。

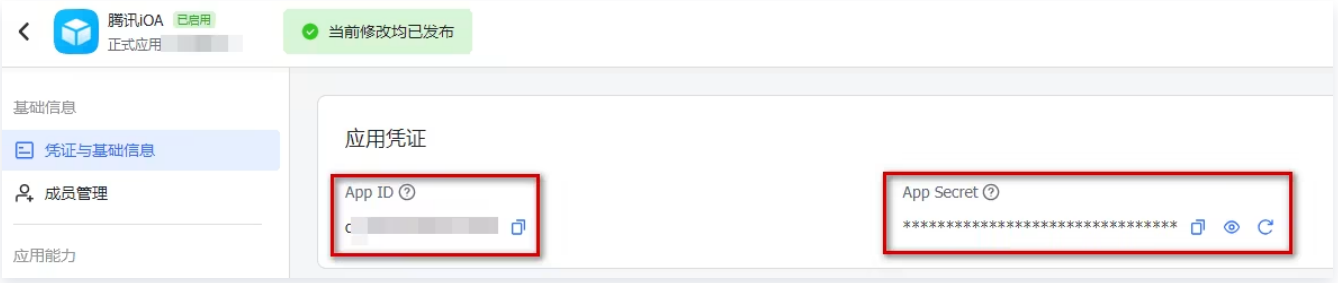


2.3 应用名称示例：腾讯 iOA；应用描述：xxxx（任意说明）。



2.2 获取 App ID 和 App Secret

1. 在企业自建应用页面，单击刚刚创建的**自建应用**，进入应用详情页面。
2. 在凭证与基础信息页面，选择应用凭证，获取 App ID 和 App Secret。其中：飞书的 App ID 对应 iOA 控制台上的 App ID，飞书的 App Secret 对应 iOA 控制台的 App Secret。



2.3 配置重定向 URL

1. 在凭证与基础信息页面，单击**安全设置**。
2. 在重定向 URL 页面，输入以下 iOA 的网关回调域名，单击**添加**，即可添加到重定向 URL 列表中。
   - SSO 的回调域名1：`https://scs.gateway.tencent.com/akpage/sso/redirect` 。
   - SSO 的回调域名2：`https://scs.gateway.tencent.com/akpage/login` 。

     > **说明：**
     > SSO 回调域名填写：上文 SSO 的回调域名1，SSO 的回调域名2都需填写。

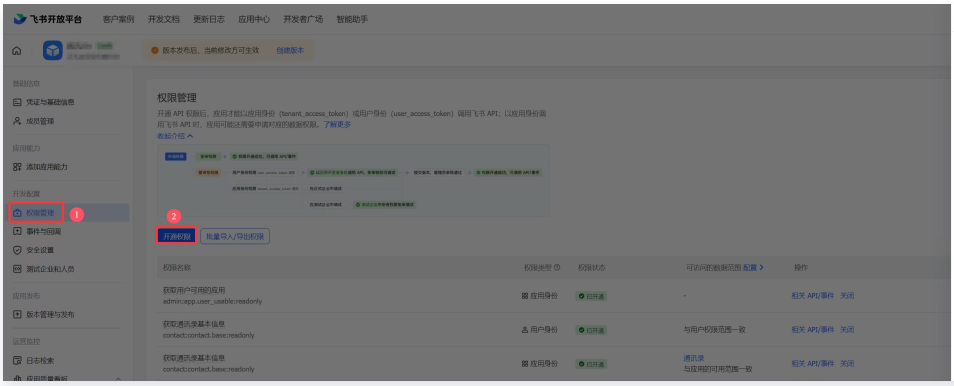
   - 二维码的回调域名：`https://scs.gateway.tencent.com/akpage/qrcode/redirect` 。



2.4 配置权限管理

1. 在权限管理页面，单击**开通权限**，选择该应用所需的权限，建议优先使用英文版查询：

> **⚠ 注意：**
>
> - 以下权限均需开通，如果未全部开通，则可能出现配置类型的报错信息。
> - 在**权限管理** > **开通权限**中，查询的权限如果存在应用身份权限和用户身份权限，则都需勾选。
> - 示例：查询contact:user.base:readonly，查询后在应用身份权限和用户身份权限中都存在contact:user.base:readonly，则都需开通权限。





英文权限名称	中文权限名称
contact:user.department_path:readonly	获取成员所在部门路径
contact:user.base:readonly	获取用户基本信息
contact:contact.base:readonly	获取通讯录基本信息
contact:department.organize:readonly	获取通讯录部门组织架构信息

版权所有：腾讯云计算（北京）有限责任公司

contact:department.base:readonly	获取部门基础信息
corehr:department.organize:read	获取部门组织架构信息
contact:group:readonly	获取用户组信息
contact:user.department:readonly	获取用户组织架构信息
contact:user.email:readonly	获取用户邮箱信息
contact:user.employee_id:readonly	获取用户 user ID
contact:user.id:readonly	通过手机号或邮箱获取用户 ID
contact:user.phone:readonly	获取用户手机号
tenant:tenant:readonly	获取企业信息

2. 选中目标权限后，单击操作列的**确认开通权限**，即可为该应用选中所需权限。

> **说明：**
> 配置权限后，需要重新发布应用才能生效。

2.5 发布应用

1. 在权限管理页面，单击**版本管理与发布**。
2. 在版本管理与发布页面，单击右上角的**创建版本**。



3. 在版本详情页面，填写应用版本号（格式如 1.0.0）和更新说明，设置可用性状态，单击**保存**。

> **注意：**
> 可用范围：选择所有员工。



4. 保存完成后，单击**申请线上发布**。



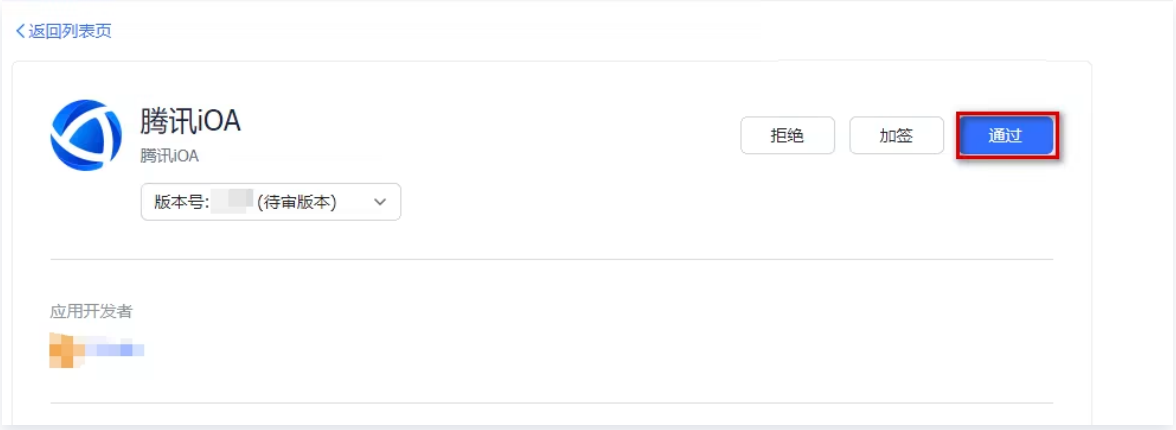
> **说明：**
> - 提交申请后，企业管理员会进行审核。
> - 审核结果会通过飞书和开发者后台发送给您。
> - 更多详情请见 飞书文档 – 开发企业自建应用 。

2.6 应用审核（如无需审核，请跳过）

1. 在 应用审核页面 ，选择目标应用，单击**审核**。



2. 在审核详情页面，单击**通过**。



2.7 开启飞书移动应用登录功能（选配）

1. 登录 飞书开放平台，选择**企业自建应用**，并单击需要开启移动登录功能的**自建应用**。



2. 在应用详情页面，单击**添加应用能力 > 按能力添加**。
3. 找到**移动应用登录**，单击**添加**。



4. 在移动应用登录页面，配置相关参数，单击**保存**。



参数类型	参数名称	参数详情	备注
用户登录协议	OAuth 2.0	建议默认选择OAuth 2.0。	-
	OIDC	建议默认选择OAuth 2.0。	-

应用类型	iOS 应用	iOS Bundle ID：正式版 `com.tencent.ioa.saas`；其他体验版或测试版请联系腾讯项目对接人。	如不需要移动端授权，无需填写
	Android 应用	正式版是固定的，其他体验版或测试版请联系腾讯项目对接人。 Android 包名称：`com.tencent.ioa.saas` Android 签名：`9e4e6594cd64562c6ae8e3ae0288dd5a`	

2.8 开启邮箱/手机号账号身份关联功能（选配）

> **说明：**
> 如果需要开启**手机验证码**或**邮箱验证码**作为二次认证/挑战认证的实例，则建议从飞书同步字段时，开通手机号或邮箱的同步权限。在 iOA 控制台添加**短信验证码**或**邮箱验证码**时，将通过飞书同步过来的手机号/邮箱作为字段映射和身份认证的依据。

1. 登录 飞书开放平台，选择**企业自建应用**，并单击目标**自建应用**。
2. 在应用详情页面，单击**权限管理**，下滑至**权限配置**。
3. 在权限配置模块，分别开启以下两个功能：
   - 开启手机号账号身份关联功能：搜索**获取用户手机号**，单击**开通权限**。



   - 开启邮箱账号身份关联功能：搜索**获取用户邮箱信息**，单击**开通权限**。



4. 配置上述权限后，需要重新 发布应用版本 才能生效。

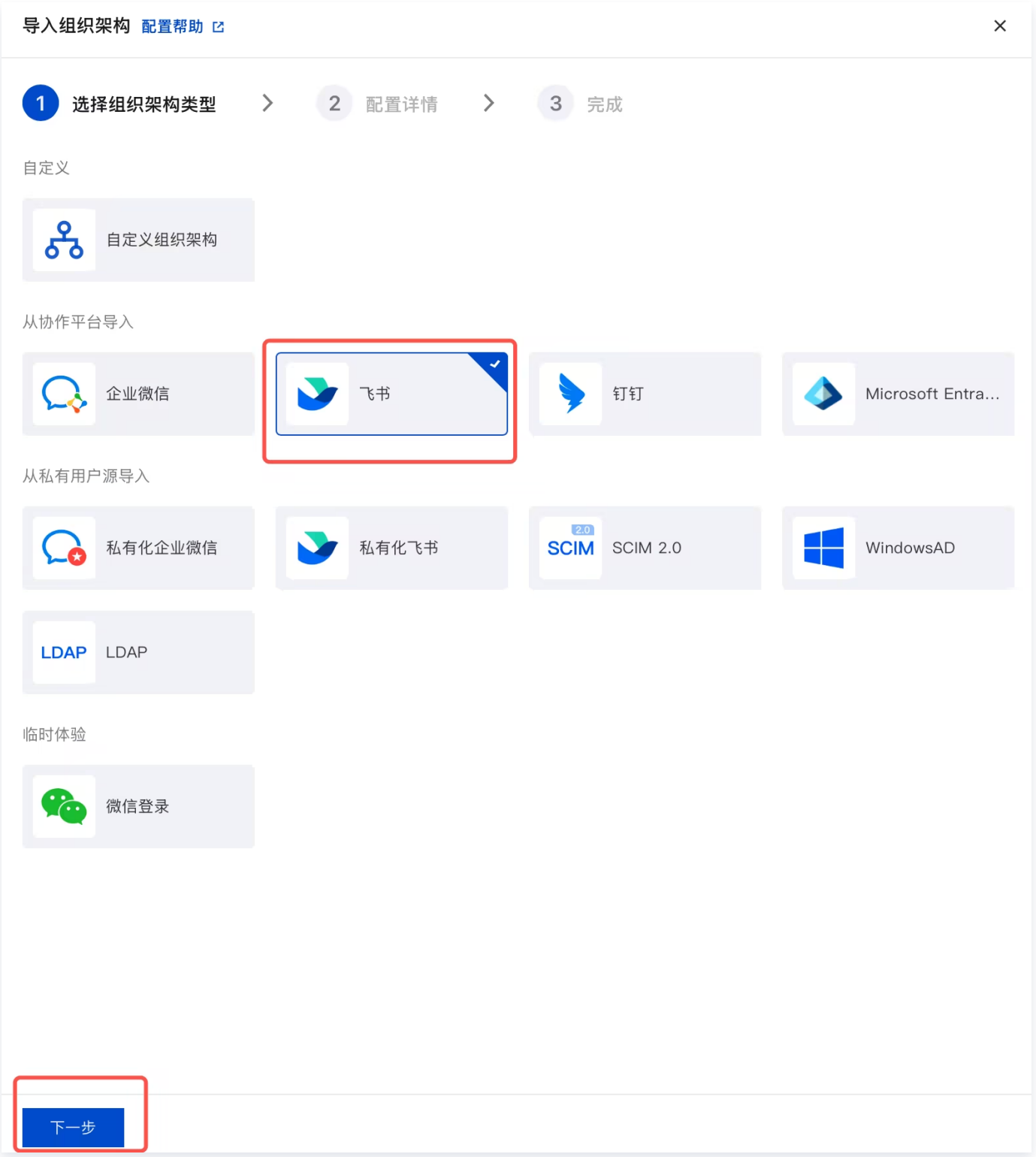
3. iOA 控制台配置

3.1 新建目录

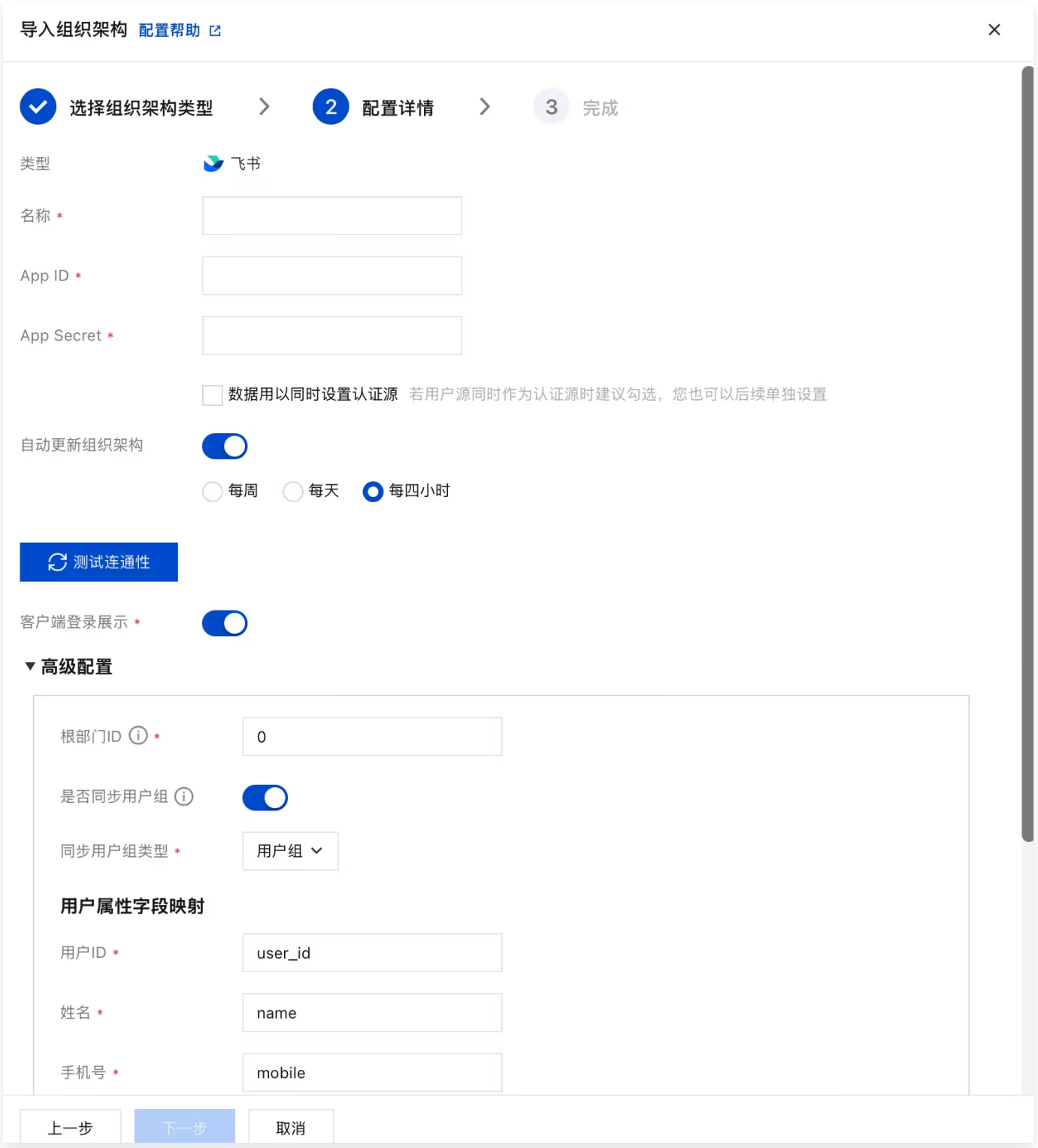
1. 登录 iOA 零信任管理平台控制台，在左侧导览中，单击**员工与身份管理** > **组织架构管理**。
2. 在组织架构管理页面，单击**新增组织架构**。



3. 在新增组织架构页面，导入类型选择**飞书**，单击**下一步**。



4. 在新增目录页面，输入 App ID 和 App Secret，以及其他参数。



5. 单击**测试连通性**，测试通过后单击**下一步并保存**。

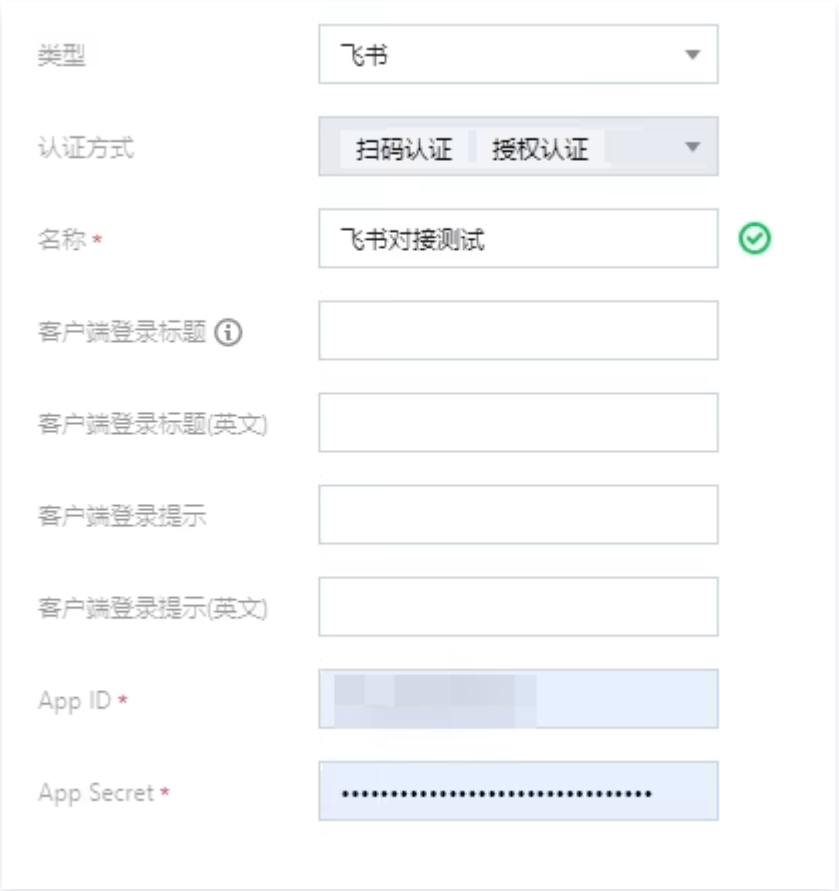
3.2 配置认证源

1. 登录 iOA 零信任管理平台控制台，在左侧导览中，单击**身份安全管控** > **认证源配置**。
2. 在认证源配置页面，单击**新增认证源实例**。



3. 在新增认证源实例页面，类型选择**飞书**，并配置其他参数，单击**保存**。

> **说明：**
> - App ID：为飞书的 App ID。
> - App Secret：为飞书的 App Secret。



3.3 设置认证策略

1. 在 身份安全管控 > **认证策略**页面，选择目标目录，单击**编辑**。



2. 在编辑认证策略页面，设置 PC 端的主认证方式认证源和挑战认证方式认证源。

> **说明：**
> 如您要使用飞书 App 内的应用免登录，您还需要设置移动端的主认证方式认证源和挑战认证方式认证源，设置方式与 PC 端相同。



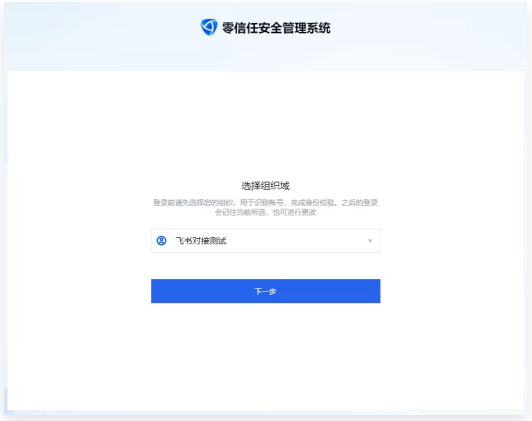
3. 单击**添加**，完成编辑。

方案2：OAuth2 认证（11.1.1版）

最近更新时间：2026-02-13 09:41:02

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录效果

类型	选择组织域	登录效果
浏览器		
客户端		

2. 飞书认证准备

2.1 配置飞书信息

1. 如您是首次使用，未创建企业自建应用：

1.1 未创建企业自建应用，需要创建一个企业自建应用，登录 飞书开放平台，选择**企业自建应用**，单击**创建企业自建应用**。



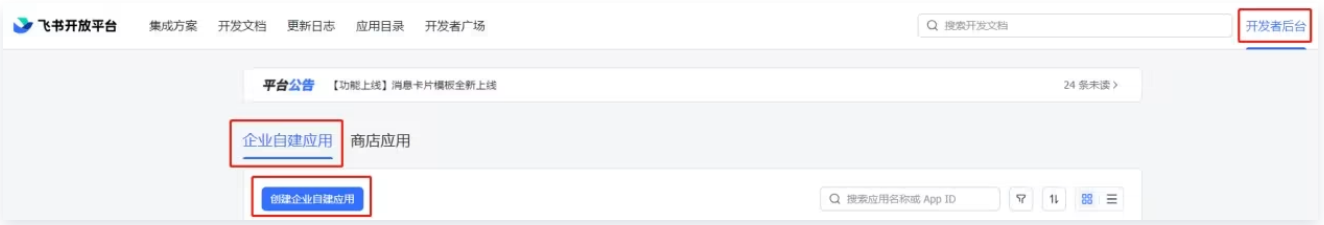
1.2 在创建企业自建应用窗口中，配置相关参数，单击**创建**，即可完成创建。



2. 如您未开通飞书开发者账号：

2.1 请先前往飞书开放平台，创建一个开发者账号。

2.2 在开发者后台，选择**企业自建应用**，单击**创建企业自建应用**。



2.3 应用名称示例：腾讯 iOA，应用描述：xxxx（任意说明）。



2.2 获取 App ID 和 App Secret

1. 在企业自建应用页面，单击刚刚创建的**自建应用**，进入应用详情页面。
2. 在凭证与基础信息页面，选择应用凭证，获取 App ID 和 App Secret。其中：飞书的 App ID 对应 iOA 控制台上的 App ID，飞书的 App Secret 对应 iOA 控制台上的 App Secret。



2.3 配置重定向 URL

1. 在凭证与基础信息页面，单击**安全设置**。
2. 在重定向 URL 页面，输入 iOA 重定向地址：`https://服务地址:27800/akpage/sso/redirect`。
3. 单击**添加**，即可添加到重定向 URL 列表中。

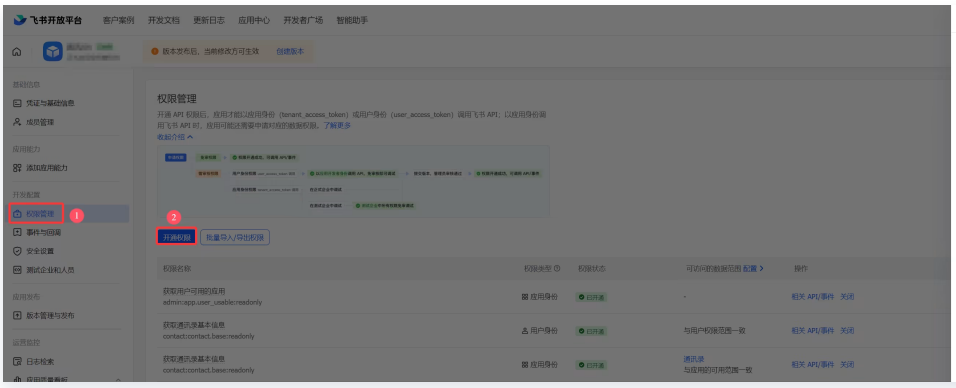
> **注意：**
> OAuth 2.0 认证方案的飞书认证准备步骤中，其他步骤都与飞书认证方案一样，唯有重定向URL与飞书认证方案的重定向 URL 不同。



2.4 配置权限管理

1. 在权限管理页面，单击**开通权限**，选择该应用所需的权限，建议优先使用英文版查询：

> **⚠ 注意：**
>
> - 以下权限均需开通，如果权限未全部开通，则可能出现配置类型的报错信息。
> - 在**权限管理** > **开通权限**中，查询的权限如果存在应用身份权限和用户身份权限，则都需勾选。
> - 示例：查询contact:user.base:readonly，查询后在应用身份权限和用户身份权限中都存在contact:user.base:readonly，则都需开通权限。





英文权限名称	中文权限名称
contact:user.department_path:readonly	获取成员所在部门路径
contact:user.base:readonly	获取用户基本信息
contact:contact.base:readonly	获取通讯录基本信息
contact:department.organize:readonly	获取通讯录部门组织架构信息
contact:department.base:readonly	获取部门基础信息
corehr:department.organize:read	获取部门组织架构信息
contact:group:readonly	获取用户组信息
contact:user.department:readonly	获取用户组织架构信息

版权所有：腾讯云计算（北京）有限责任公司

contact:user.email:readonly	获取用户邮箱信息
contact:user.employee_id:readonly	获取用户 user ID
contact:user.id:readonly	通过手机号或邮箱获取用户 ID
contact:user.phone:readonly	获取用户手机号
tenant:tenant:readonly	获取企业信息

2. 选中目标权限后，单击操作列中的**确认开通权限**，即可为该应用选中所需权限。

> **说明：**
> 配置权限后，需要重新发布应用才能生效。

2.5 发布应用

1. 在权限管理页面，单击**版本管理与发布**。
2. 在版本管理与发布页面，单击右上角的**创建版本**。

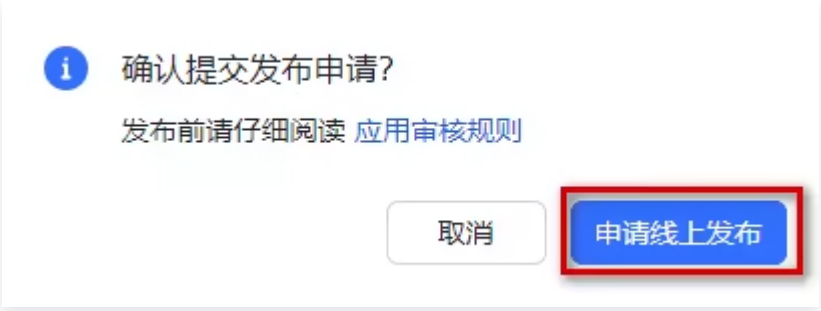


3. 在版本详情页面，填写应用版本号（格式如 1.0.0）和更新说明，设置可用性状态，单击**保存**。

> **注意：**
> 可用范围：选择所有员工。



4. 保存完成后，单击**申请线上发布**。



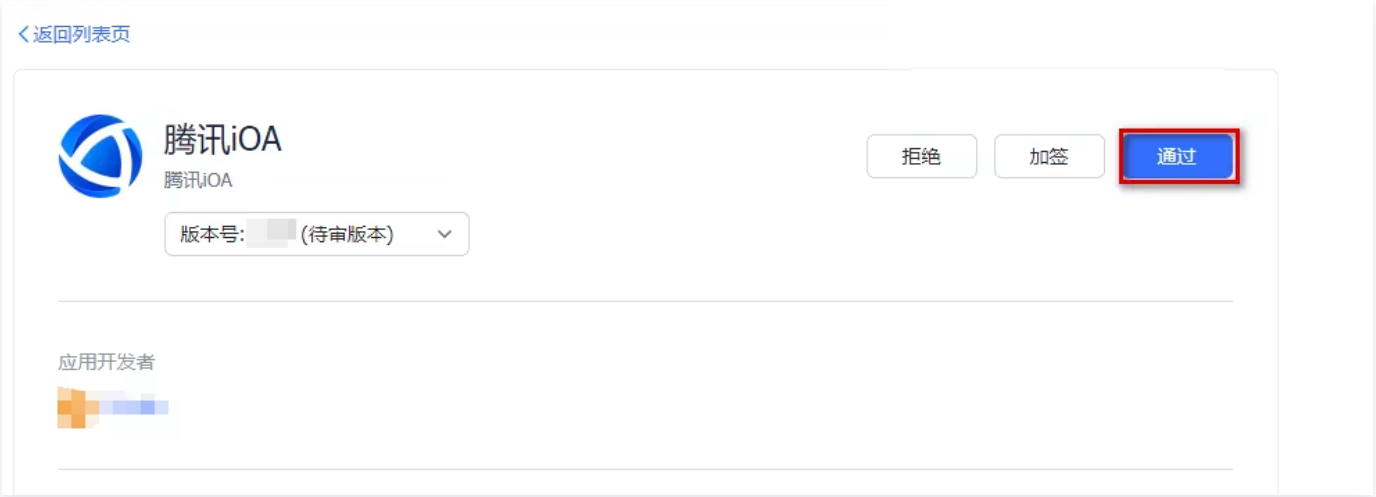
> **说明：**
> - 提交申请后，企业管理员会进行审核。
> - 审核结果会通过飞书和开发者后台发送给您。
> - 更多详情请见 飞书文档 – 开发企业自建应用 。

2.6 应用审核（如无需审核，请跳过）

1. 在 应用审核页面 ，选择目标应用，单击**审核**。



2. 在审核详情页面，单击**通过**。



2.7 开启飞书移动应用登录功能（选配）

1. 登录 飞书开放平台，选择**企业自建应用**，并单击需要开启移动登录功能的**自建应用**。



2. 在应用详情页面，单击**添加应用能力 > 按能力添加**。
3. 找到**移动应用登录**，单击**添加**。



4. 在移动应用登录页面，配置相关参数，单击**保存**。



参数类型	参数名称	参数详情	备注
用户登录协议	OAuth 2.0	建议默认选择OAuth 2.0。	–

	OIDC	建议默认选择OAuth 2.0。	-
应用类型	iOS 应用	iOS Bundle ID：正式版 `com.tencent.ioa.saas`；其他体验版或测试请联系腾讯项目对接人。	如不需要移动端授权，无需填写
	Android 应用	正式版是固定的，其他体验版或测试请联系腾讯项目对接人。 Android 包名称：`com.tencent.ioa.saas` Android 签名：`9e4e6594cd64562c6ae8e3ae0288dd5a`	

2.8 开启邮箱/手机号账号身份关联功能（选配）

> **说明：**
> 如果需要开启**手机验证码**或**邮箱验证码**作为二次认证/挑战认证的实例，则建议从飞书同步字段时，开通手机号或邮箱的同步权限。在 iOA 控制台添加**短信验证码**或**邮箱验证码**时，将通过飞书同步过来的手机号/邮箱作为字段映射和身份认证的依据。

1. 登录 飞书开放平台，选择**企业自建应用**，并单击目标**自建应用**。
2. 在应用详情页面，单击**权限管理**，下滑至**权限配置**。
3. 在权限配置模块，分别开启以下两个功能：
   - 开启手机号账号身份关联功能：搜索**获取用户手机号**，单击**开通权限**。



   - 开启邮箱账号身份关联功能：搜索**获取用户邮箱信息**，单击**开通权限**。



4. 配置上述权限后，需要重新 发布应用版本 才能生效。

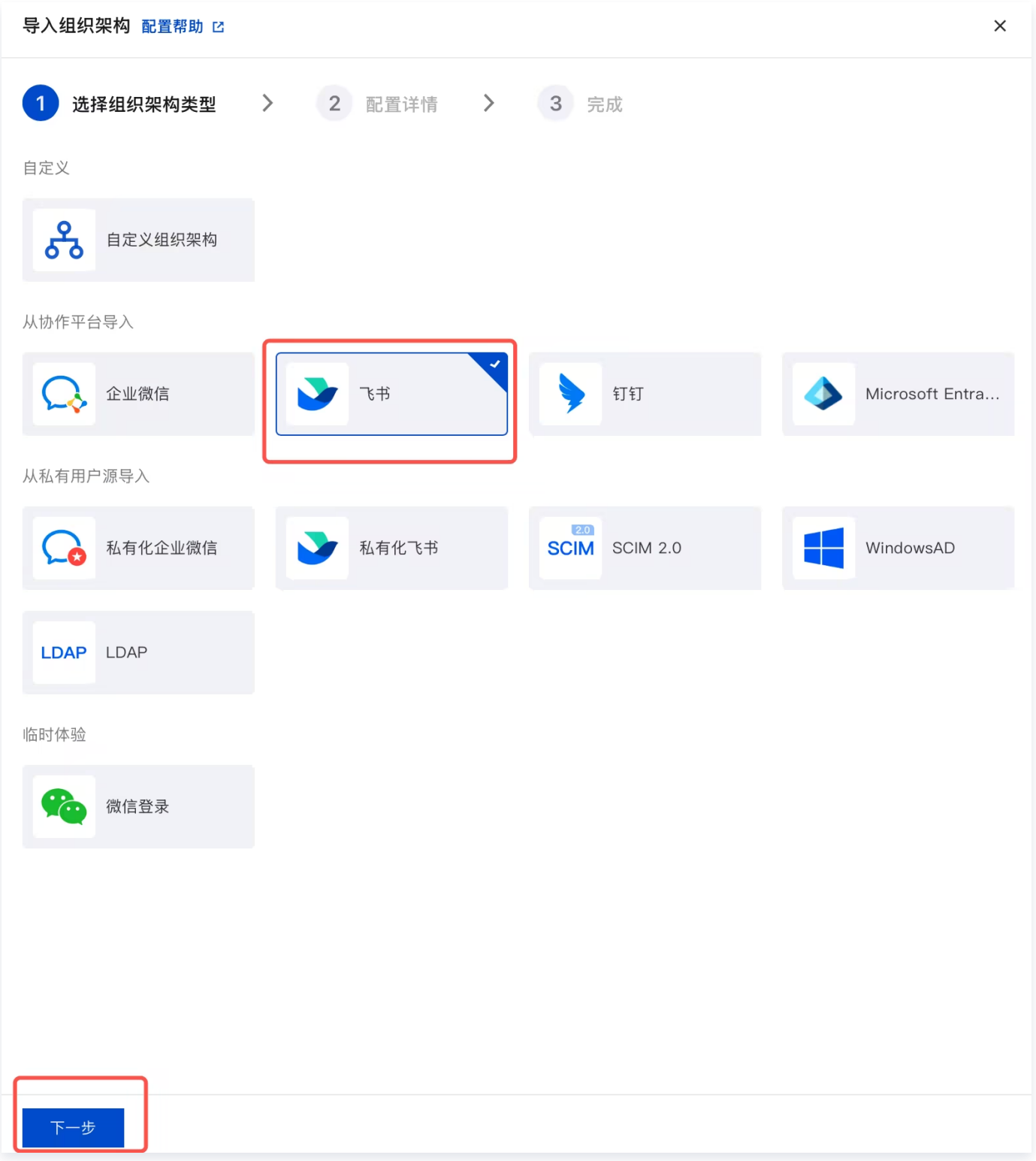
3. iOA 控制台配置

3.1 新建目录

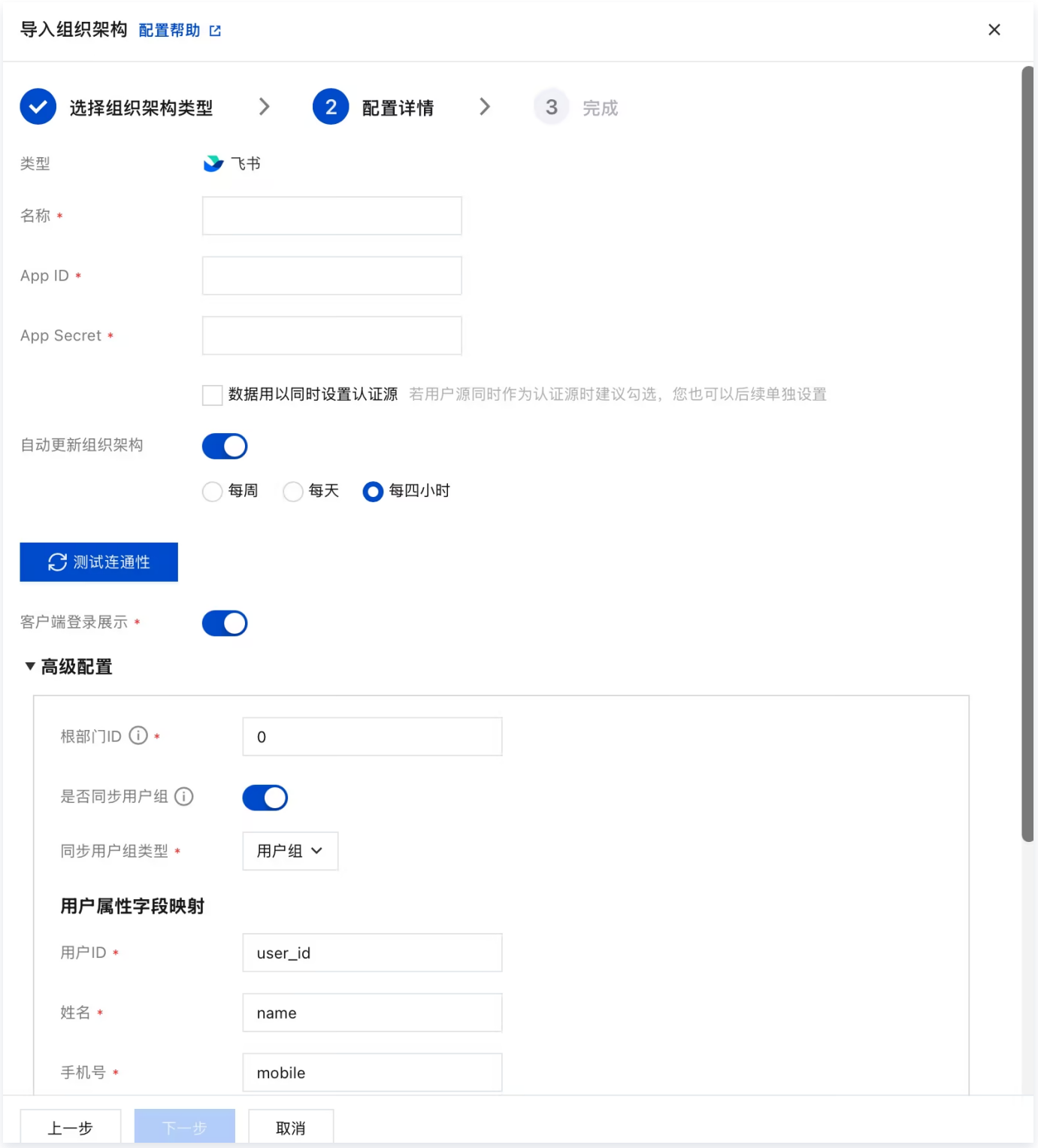
1. 登录 iOA 零信任管理平台控制台，在左侧导览中，单击**员工与身份管理** > **组织架构管理**。
2. 在组织架构管理页面，单击**新增组织架构**。



3. 在新增组织架构页面，导入类型选择**飞书**，单击**下一步**。



4. 在新增目录页面，输入 App ID 和 App Secret，以及其他参数。



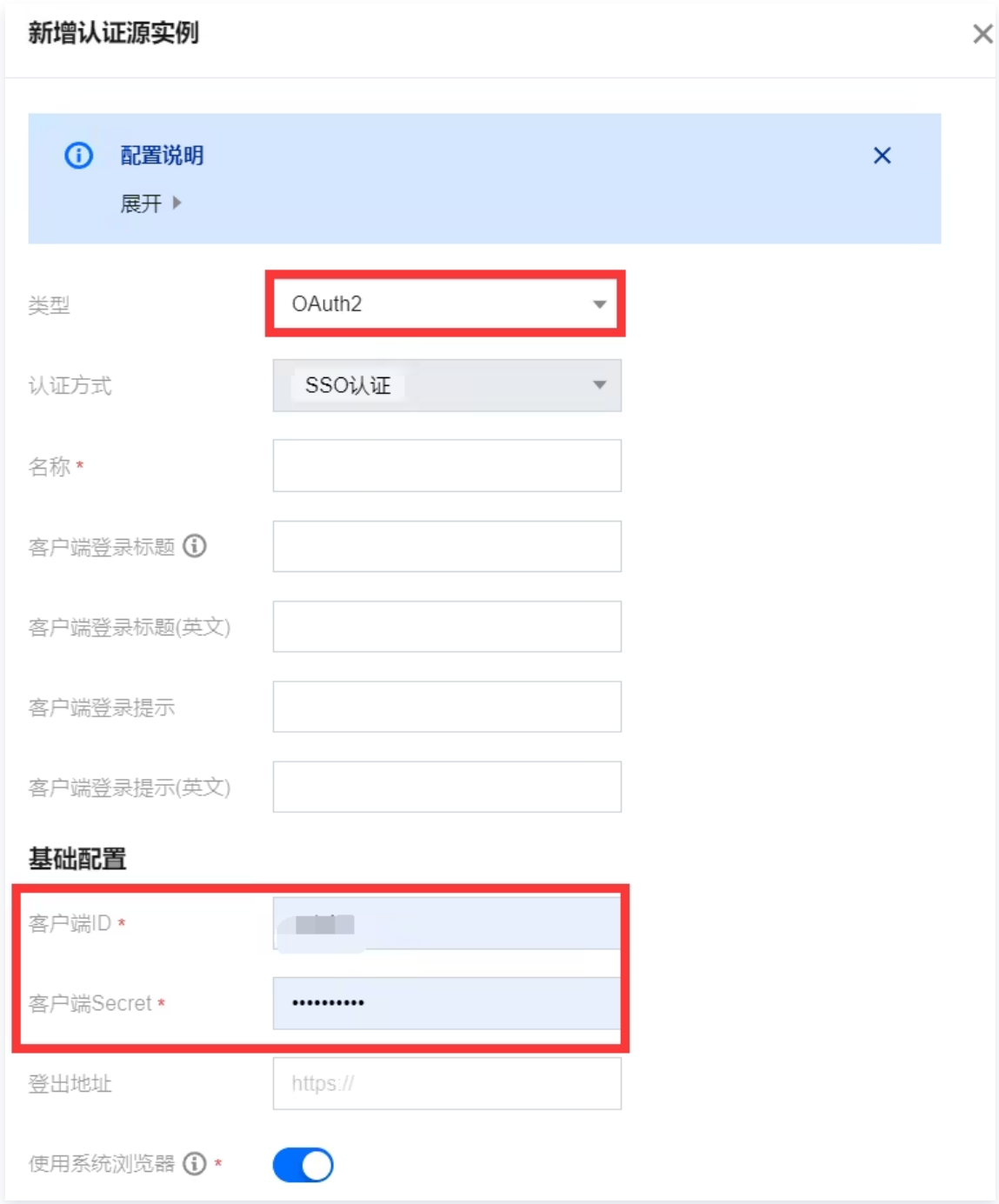
5. 单击**测试连通性**，测试通过后单击**下一步并保存**。

3.2 配置认证源

1. 登录 iOA 零信任管理平台控制台，在左侧导览中，单击**身份安全管控** > **认证源配置**。
2. 在认证源配置页面，单击**新增认证源实例**。



3. 在新增认证源实例页面，类型选择 OAuth2。



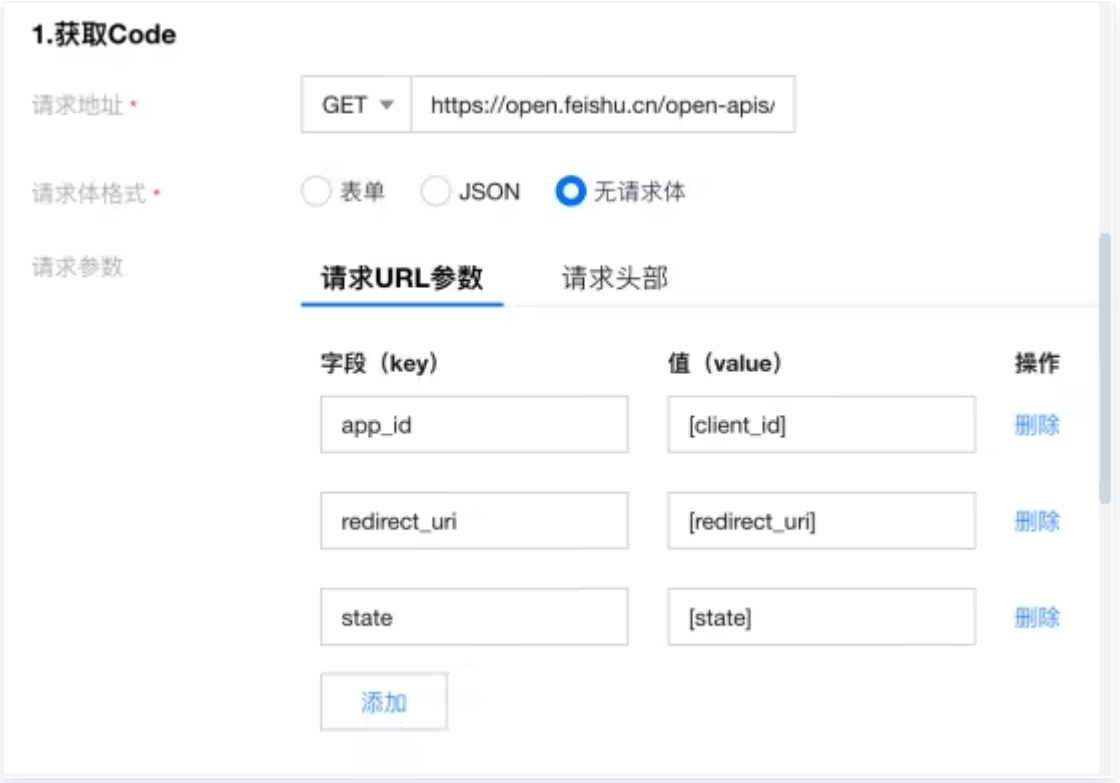
参数名称	说明

类型	OAuth2。
认证方式	默认SSO认证。
名称	自定义填写认证源实例名称。
客户端登录标题	自定义。
客户端登录标题（英文）	自定义。
客户端登录提示	自定义。
客户端登录提示（英文）	自定义。
客户端ID	为飞书的 App ID，详情请参见：2.2 获取 App ID 和 App Secret 。
客户端Secret	为飞书的 App Secret，详情请参见：2.2 获取 App ID 和 App Secret 。
登出地址	可不填，如果填写，可支持从 iOA 跳到浏览器清理登录态能力。识别方式：URL 以 logout 结尾。
使用系统浏览器	建议关闭。 • 如果开启，则会跳到系统浏览器认证，可以共享已经 SSO 登录的状态； • 如果关闭，全程在 iOA 内完成 SSO 认证。
专线分组	使用专线组访问服务接口，自行选择专线分组。

3.1 获取 code：

- 请求地址：https://open.feishu.cn/open-apis/authen/v1/index 。
- 请求体格式：无请求体。
- 请求参数：请求 URL 参数。

字段（key）	值（value）
app_id	[client_id]
redirect_uri	[redirect_uri]
state	[state]



3.2 获取 access token：

- 请求地址：open.feishu.cn/open-apis/auth/v3/tenant_access_token/internal 。
- 请求体格式：JSON。
- 请求 Body 参数配置如图。

字段（Key）	值（Value）
app_id	[client_id]
app_secret	[client_secret]

- response 错误路径：msg。
- access token 路径：tenant_access_token。



3.3 获取用户信息：

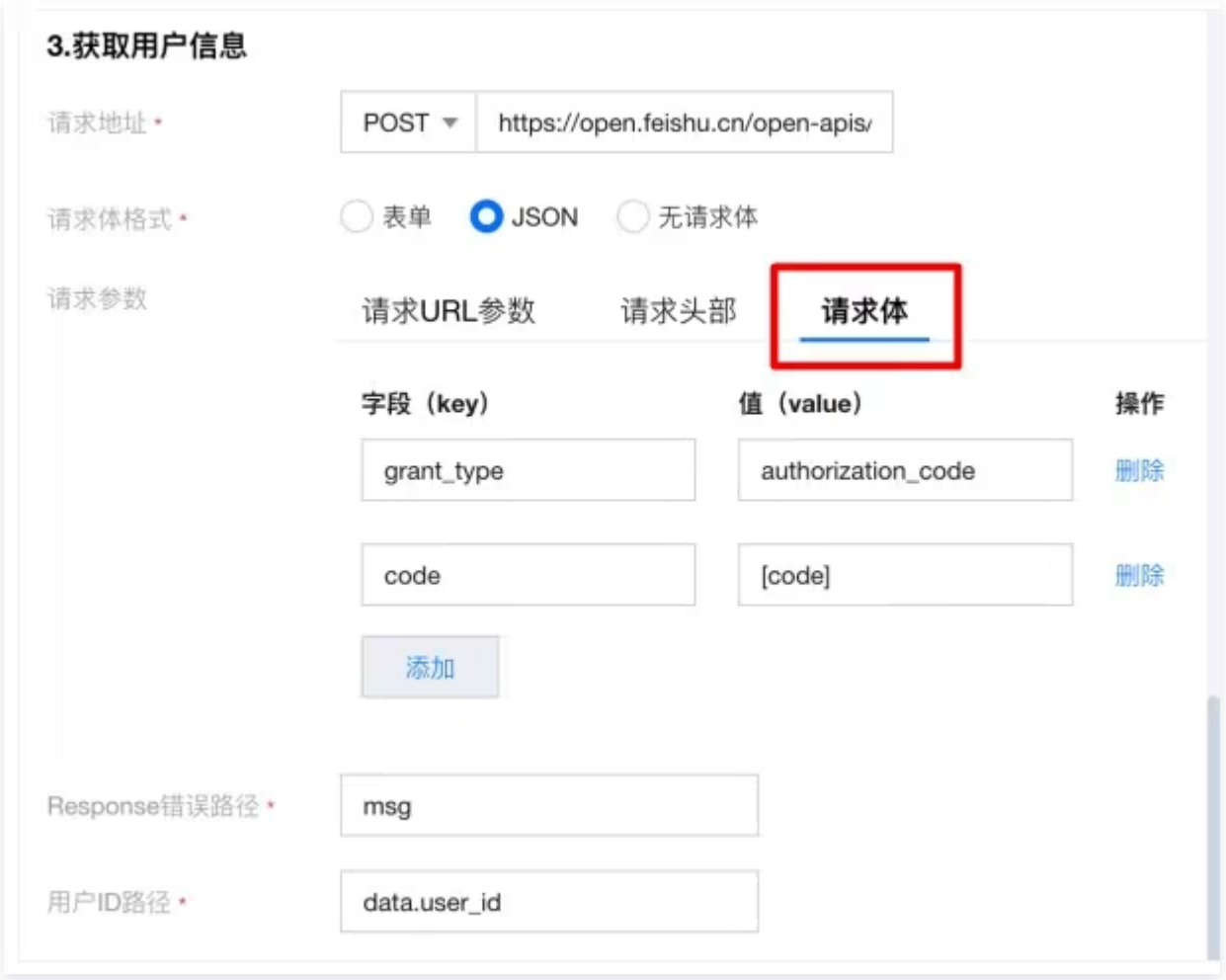
- 请求地址：https://open.feishu.cn/open-apis/authen/v1/access_token 。
- 请求头配置：

字段（key）	值（value）
Authorization	Bearer [access_token]



- **请求体配置：**

字段（Key）	值（Value）
grant_type	authorization_code
code	[code]



- response 错误路径：msg 。
- 用户 ID 路径：data.user_id 。
- 用户头像路径：选填/自定义。

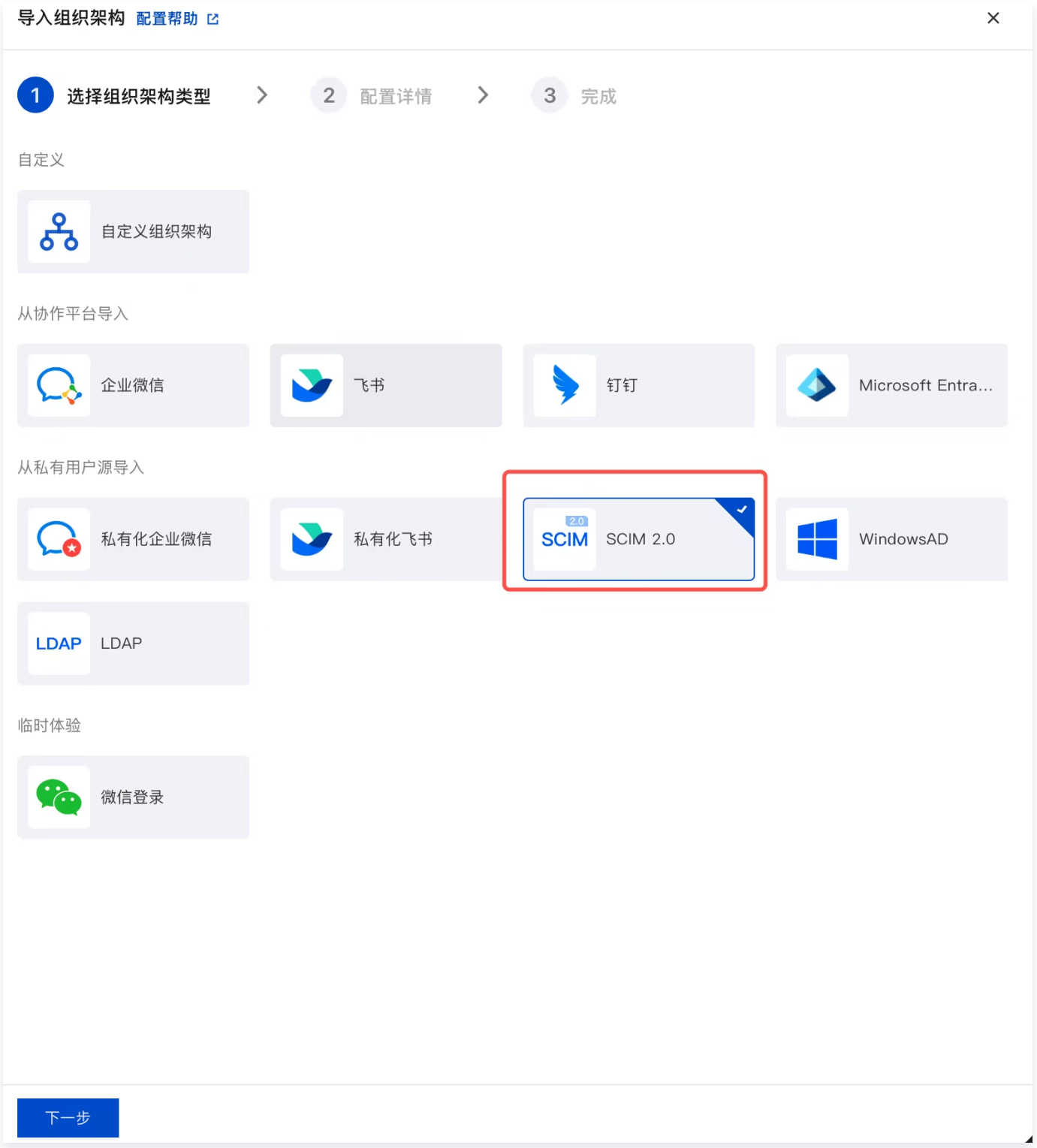
4.配置完成单击**保存**。

iOA SaaS SCIM2.0 用户同步（11.1.1 版）

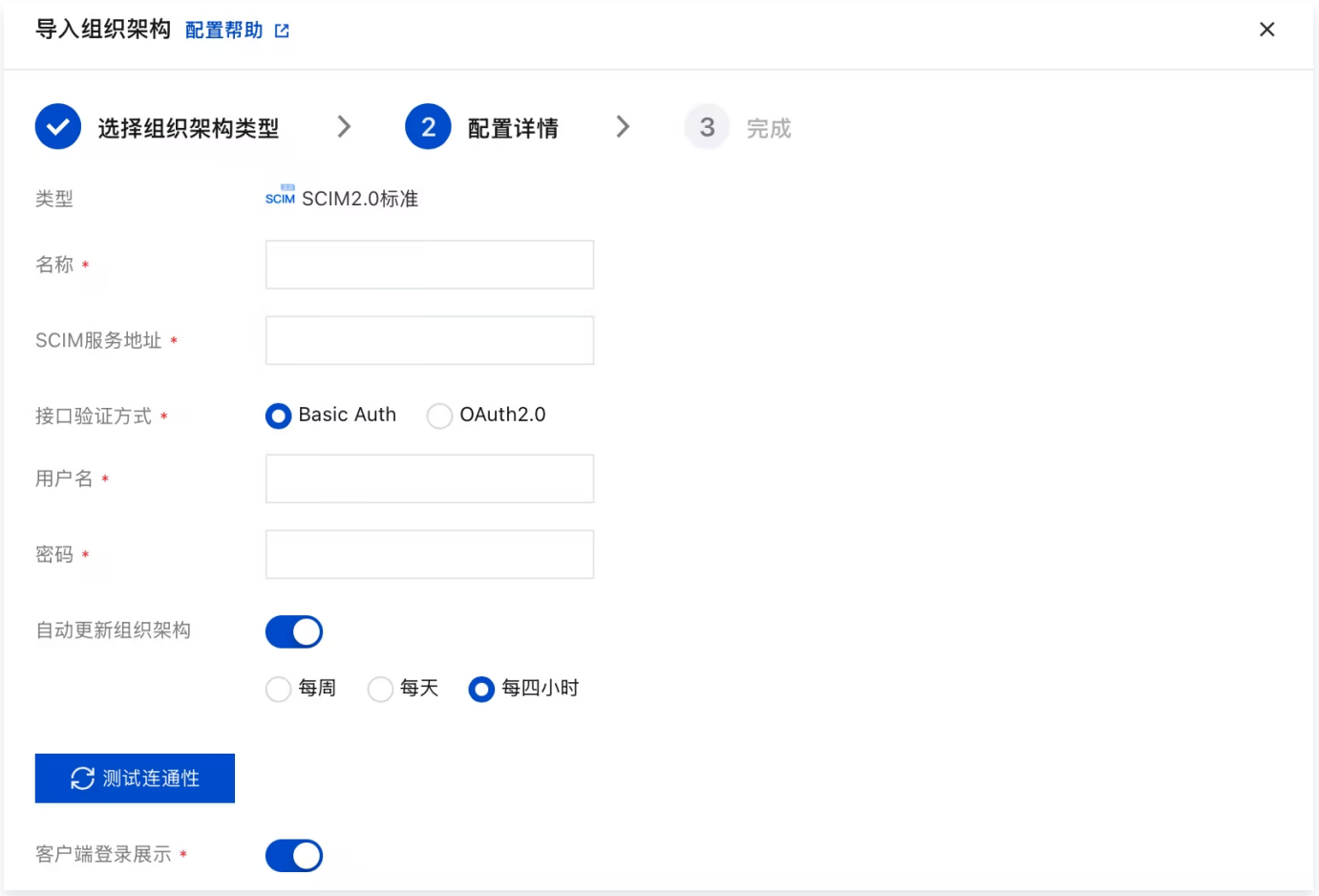
最近更新时间：2026-02-13 09:41:03

说明：
iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导览中，单击**员工与身份管理** > 组织架构管理 。
2. 在组织架构管理页面，单击**新增组织架构**，选择 **SCIM2.0**，单击**下一步**。



3. 在导入组织架构页面，配置基础信息。



参数名称		说明
名称		定义组织架构名称。
SCIM 服务地址		IAM 平台地址。
接口验证方式	Basic Auth	用户名和密码可能是 IAM 平台管理员的账号密码，如不正确，请通过查找 API 请求头字段 Authorization，值是 Basic Base64(用户名:密码)。
	OAuth2.0	• 获取 token 地址：access_token 的地址必须是完整的 URL。只支持标准的 OAuth2 方式，即请求形如 `GET https://xxxx` 。 • 客户端 ID：iOA 在 IAM 平台上注册的应用 ID。 • 客户端 SECRET：iOA 在 IAM 平台申请时提供的应用 Secret。
组织架构更新设置		开启自动更新后，可选择每周/每天/每四小时同步更新组织架构。

4. （可选）高级配置：配置专线分组、组织架构接口、用户组接口、用户接口、用户属性字段映射等。

高级配置

始终信任服务端证书

专线分组 * 不使用专线分组

组织架构接口配置

接口URI * /scim/v2/Organizations

是否使用分页 *

每页最大数量 * 10

父级组织ID字段 * parent

用户组接口配置

接口URI * /scim/v2/Groups

是否使用分页 *

每页最大数量 * 10

用户接口配置

接口URI * /scim/v2/Users

是否使用分页 *

每页最大数量 * 10

组织架构列表字段 * organization

用户组列表字段

用户属性字段映射

用户ID * userName

姓名 * displayName

手机号 * phoneNumbers.#.value

邮箱 * emails.#.value

头像 * avatar

状态 不映射状态 表示状态的属性字段 表示正常状态的值

其他属性 添加

上一步 下一步

参数类型	参数名称	说明
始终信任服务端证书		支持手动信任自签 LDAP 证书。
专线分组		使用专线组访问服务接口。
组织架构接口配置	接口 URI	默认 `/scim/v2/Organizations`，如果接口特殊，可以参考默认格式填写接口名称。
	是否使用分页	• 开启分页后会进行分页拉取；分页只支持标准的参数，startIndex 表示开始项的位置，count 表示一页的数量。 • 不开启分页则默认 count=-1拉取全量数据。
	每页最大数量	每页数据量最少为10。
	父级组织 ID 字段	组织架构必须包含表示父级目录 ID 的字段，否则无法构建目录树。
用户组接口配置	接口 URI	默认 `/scim/v2/Groups`，如果接口特殊，可以参考默认格式填写接口名称。
	是否使用分页	• 开启分页后会进行分页拉取；分页只支持标准的参数，startIndex 表示开始项的位置，count 表示一页的数量。 • 不开启分页则默认 count=-1拉取全量数据。
	每页最大数量	每页数据量最少为10。
用户接口配置	接口 URI	默认 `/scim/v2/Users`，如果接口特殊，可以参考默认格式填写接口名称。
	是否使用分页	• 开启分页后会进行分页拉取；分页只支持标准的参数，startIndex 表示开始项的位置，count 表示一页的数量。 • 不开启分页则默认 count=-1拉取全量数据。
	每页最大数量	每页数据量最少为10。
	组织架构列表字段	用户必须包含所属组织架构的 ID 字段，用于将用户放入特定的组织架构目录。
	用户组列表字段	填写默认字段即可，如果字段特殊，可填写自己的列表字段。
用户属性字段映射	用户 ID	用户在 iOA 用来登录的 ID，可以是用户名/手机号/邮箱等等，但是必须保证唯一。 注意：用户在系统中的其他 ID 无特殊用途。

	状态	映射状态是指，将身份源的状态字段关联到 iOA 的锁定/非锁定状态；支持三种类型：Int/Bool/String，这里关联状态的值必须是正常状态的值。所有星号为必填项目，但是对于无法映射的属性或存在映射关系但不想同步过来的属性，可以赋予一个错误的属性值，那么属性会被赋予空值。
		• 如果用户对象是 JSON 格式的，只需用语法来获取嵌套属性，以姓名属性为例。例如：
		`{ "name":{ "name256":"xxx" } }`
		• 指定 name256 为头像，那么可以输入 name.name256。
		`{ "name":[ { "value":"xxx" } ] }`
		• 指定对象数组的元素的值，可以输入 name.#.value。

注意：
用户属性字段映射如无特殊需求，请勿修改。

5. 单击**测试连通性**，测试通过后单击**下一步**并**保存**。

连接器部署（11.1.1版）

最近更新时间：2026-02-13 09:41:01

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

连接器部署要求

连接器（专线）是通过反向连接方案，单向连通腾讯云网关和您的内网资源、SaaS 资源等。实现业务系统无需对外暴露端口的效果，仅需出方向放通下述地址：

类型	详情
网络	出方向放通所需地址，请优先以域名模式进行放通。需放通地址如下： • 专线管理服务地址：ch1.channel.gateway.tencentwsd.cn:30226 ——TCP • （示例）专线反连服务地址：ch2-(租户ID).channel.gateway.tencentwsd.cn:(端口号) ——TCP • 控制面上报数据地址（总控地址）：scs.gateway.tencent.com:443 ——TCP • WireGuard 通道服务地址：wg1.channel.gateway.tencentwsd.cn:13303 ——UDP
建议操作系统	• CentOS7.6及以上，TencentOS 3.1及以上，Ubuntu 20及以上，Debian 11及以上。 • CPU：2-4核，内存4-8G，硬盘100G以上。
出口带宽	不低于当前 iOA 带宽（10Mbps）。 在 全局总览页面，单击右上角的**授权信息**，即可获取出口带宽等信息。
专线数量	建议同一个资源部署2个专线，实现灾备。
部署区域	支持部署于 DMZ 区。 DMZ 区是指为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。

连接器部署适用的场景

场景1：针对同一个业务资源部署多个专线，实现高可用

在同一个专线分组中添加多条专线，并将这些专线连接器分别部署在不同机器上。当发起业务访问时，系统会随机使用相同专线分组中状态为**已连通**的专线连接器去建立连接。



场景2：业务资源分布在不同网络、地区、机房

当业务资源分布在不同网络、不同地域、或不同机房（公有云、私有云、本地 IDC 等）时，可以配置多个专线分组，在不同专线分组中添加专线，将这些专线连接器部署在相关机器上，同时也支持 场景1 部署。



场景3：连接器迁移

每个连接器都有唯一 ID 用于向 iOA SaaS 网关注册，因此每个连接器只能同时运行在一台机器上。如需迁移连接器，为了避免业务出现中断，建议在原连接器所属专线分组中新增专线，将新专线连接器部署在新机器，再根据需要在原连接器机器上停止连接器进程服务，并在 iOA SaaS 控制台将旧连接器专线删除。

连接器安装部署示例

步骤1：添加专线分组

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择 连接器管理 。
2. 在专线管理页面，单击专线组右侧的 ＋ 。



3. 在专线组管理窗口中，输入专线组名称，单击**确定**。



步骤2：添加专线连接器

1. 在 连接器管理 页面，选择刚刚创建的分组，单击**添加专线**。



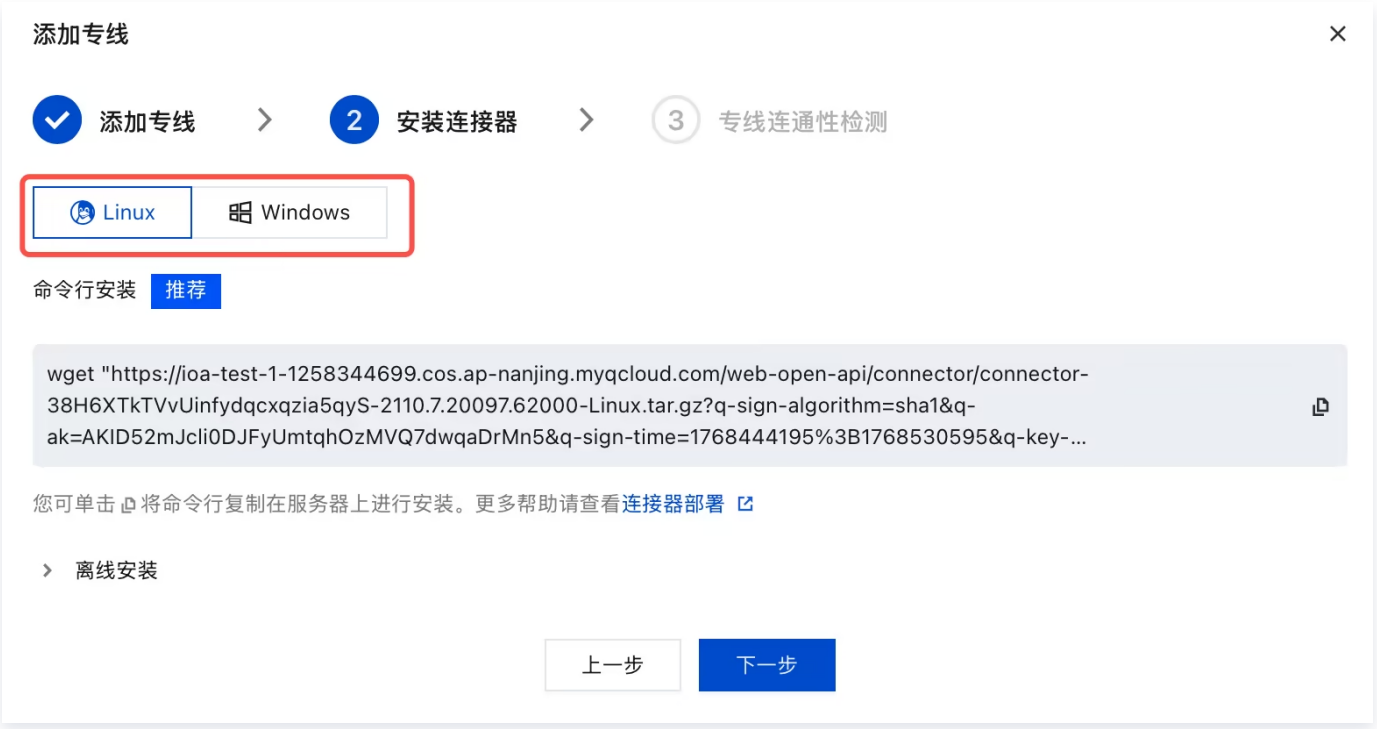
2. 在添加专线窗口中，输入专线名称，单击**下一步**。



说明：

- **零信任网关：零信任安全网关是将网关部署于本地的接入解决方案。如需要就近接入或获取终端内网 IP 建议选购零信任网关。加购后，支持在 连接器管理 配置并 启用零信任网关（如有）。资源访问时将优先与零信任网关建联，如果零信任网关未开启或未连通，将切换走腾讯云网关。**
- **是否透传 IP：开启后，访问源 IP 替换为 iOA 分配的虚拟 IP 。**

3. 根据实际需求，单击 Windows 或 Linux，复制命令下载连接器。

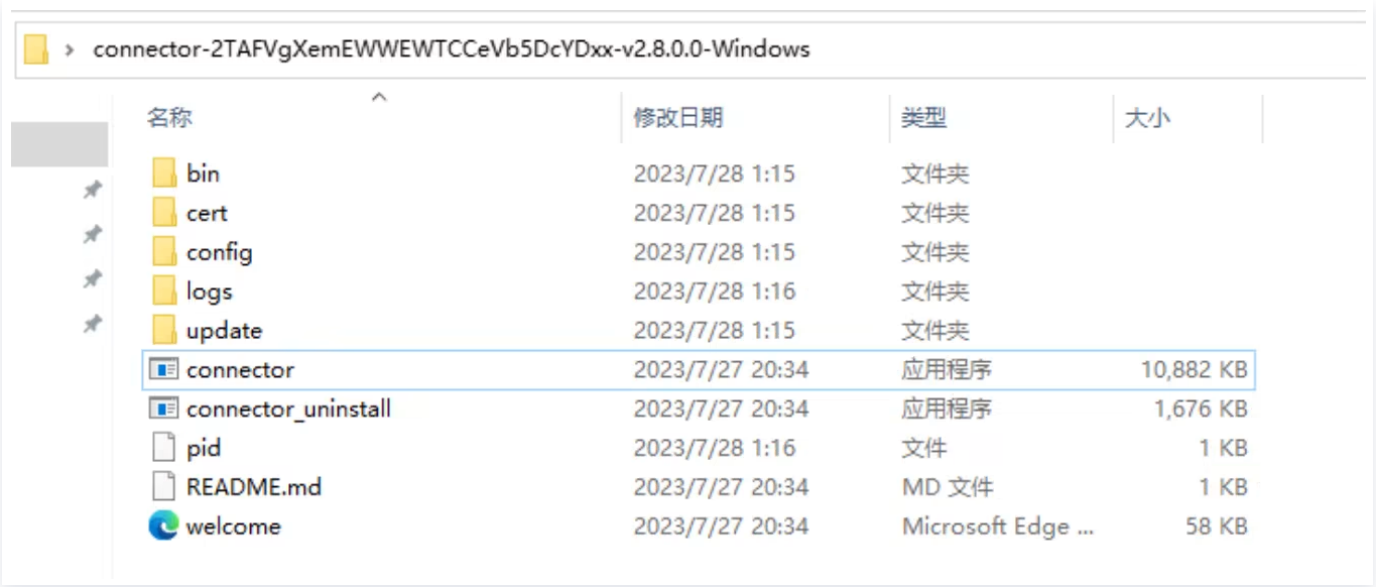


4. 请将下载的专线连接器安装包上传至目标机器上进行安装。

步骤3：卸载当前已安装的连接器（如果机器上未安装过连接器，可跳到步骤4）

卸载 Windows 连接器

1. 找到旧的 Windows 连接器安装目录。



2. 将 connector.exe 拖入命令提示符中。



3. 输入参数 uninstall 后回车，执行卸载。



4. 如果遇到如下图报错：



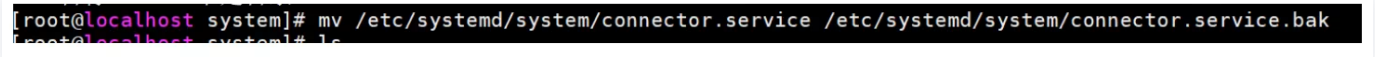
使用管理员身份打开命令提示符，再次执行上述命令即可。



卸载 Linux 连接器

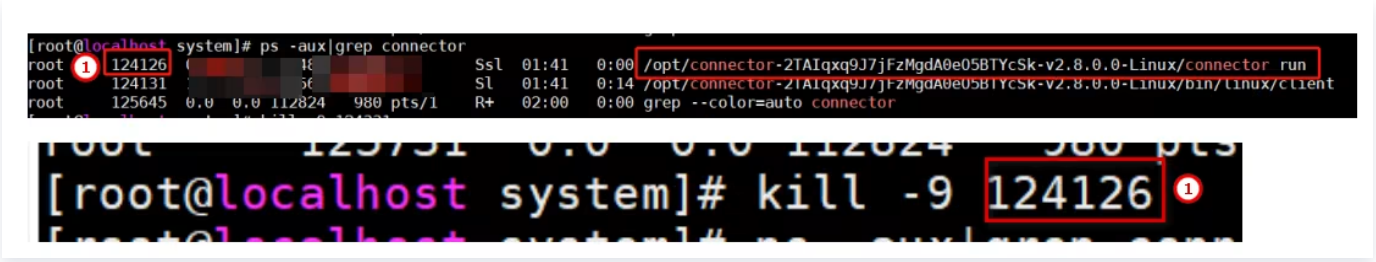
1. 输入如下命令，修改连接器自启动文件。

```
mv /etc/systemd/system/connector.service
/etc/systemd/system/connector.service.bak
```



2. 输入如下命令，终止旧连接器进程。
   - ps -aux|grep connector。
   - kill -9 进程 id。

> **说明：**
> ①处为进程 id。

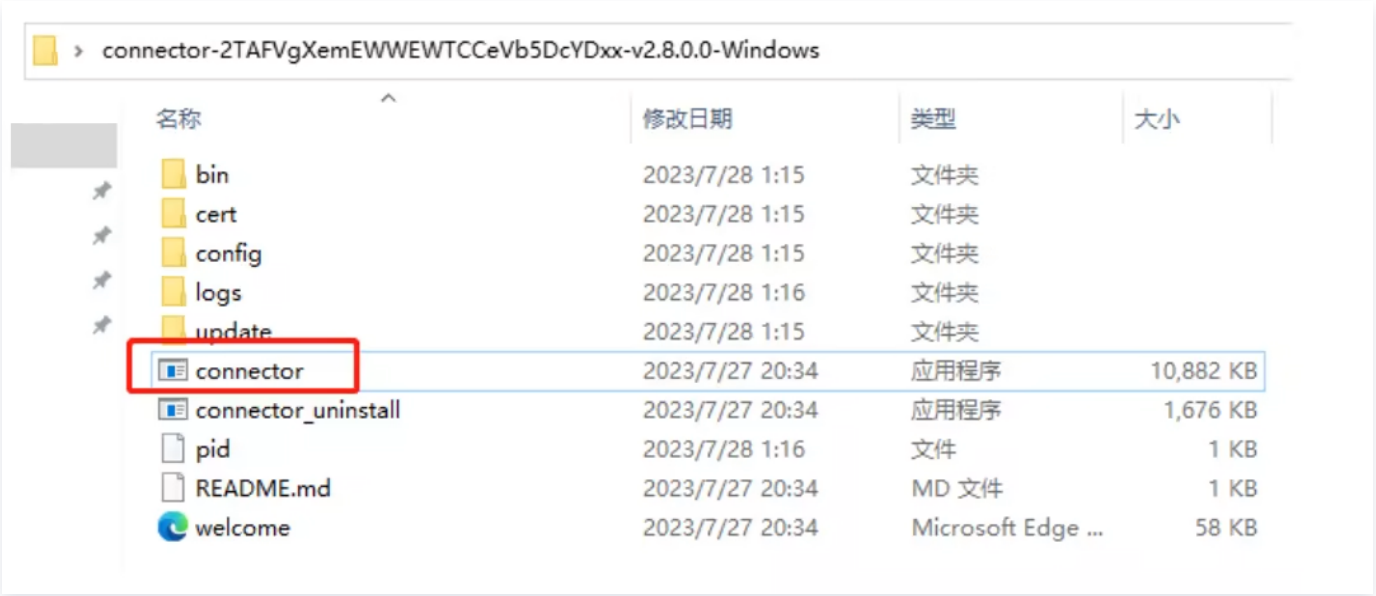


步骤4：安装新的连接器

Windows 安装新连接器

1. 将压缩包拷贝到准备好的内网服务器上解压缩，双击运行 connector.exe。

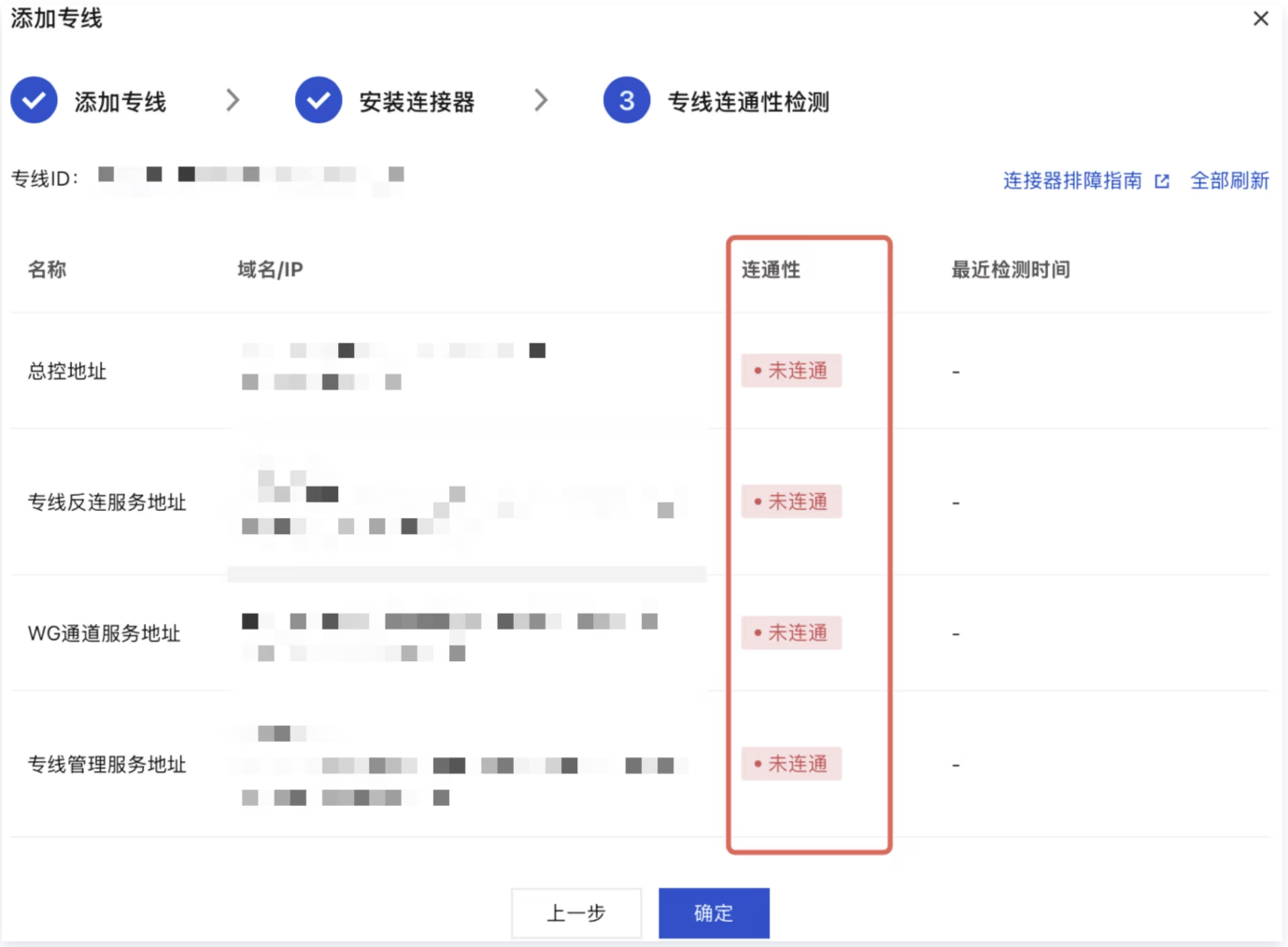
> **说明：**
> 此操作会自动设置连接器开机自启动。



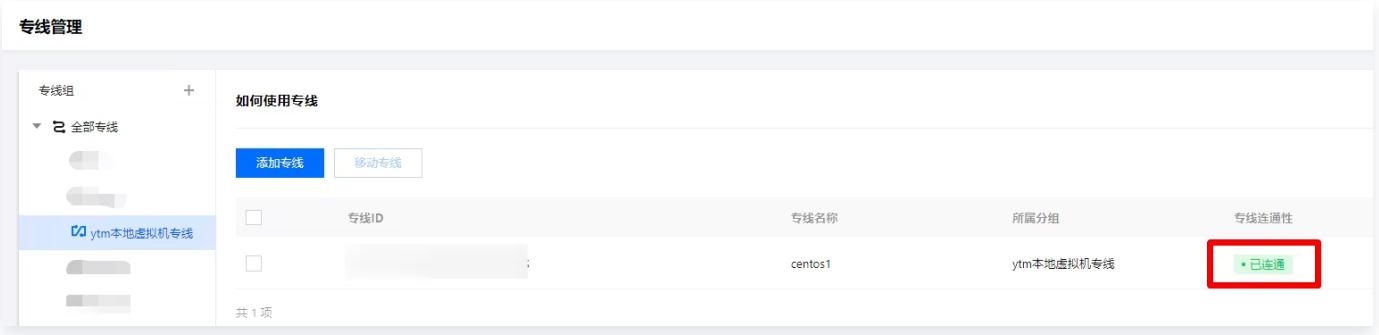
2. 在任务管理器的服务页签，检查 connector 进程的运行状态为**正在运行**。



3. 在添加专线页面，查看连接器连通状态。



4. 在专线列表页面，查看专线连接状态。

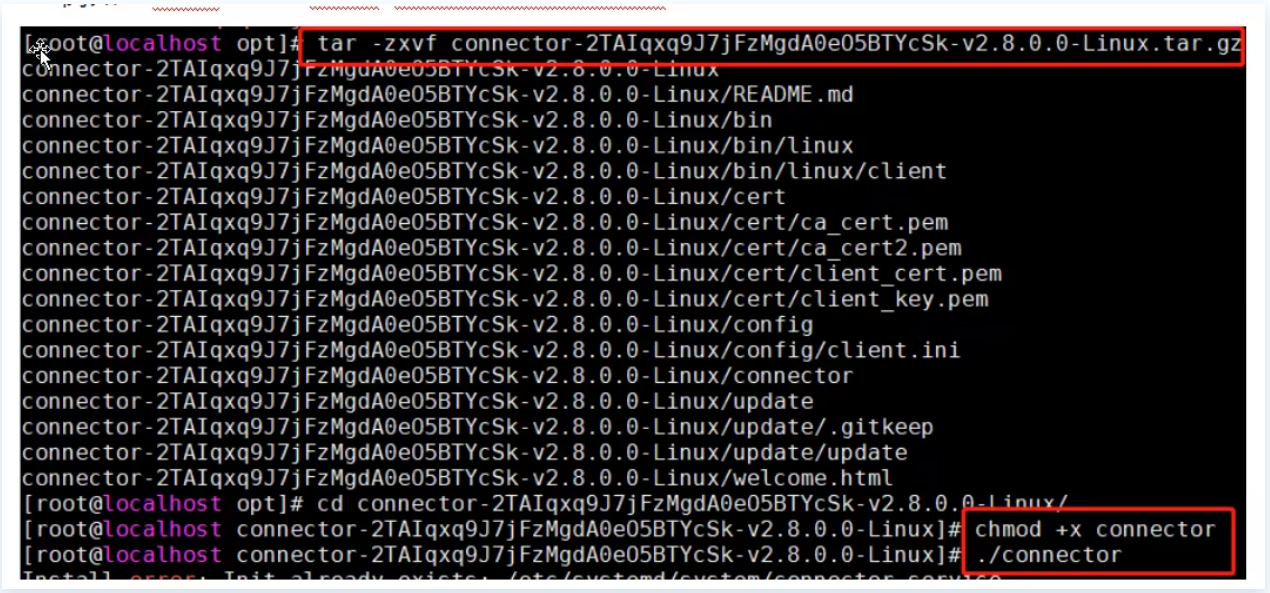


Linux 安装新连接器

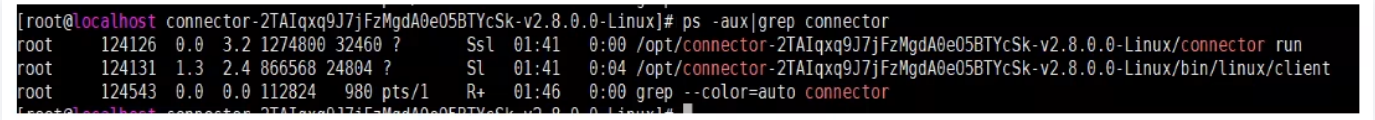
1. 将压缩包拷贝到准备好的内网服务器上，依次执行如下命令：

```
tar -zxvf connector-xxxxxx.tar.gz//解压缩
cd connector-xxxxxx//进入解压后的目录
chmod +x connector//给连接器程序执行权限
./connector//运行连接器。注：会自动设置连接器开机自启动
```

说明：
root 权限直接执行上面命令即可，非 root 权限，命令前面需添加 sudo。例如：sudo tar -zxvf connector-xxxxxx.tar。



2. 输入 `ps -aux |grep connector` 检测进程是否正常运行。



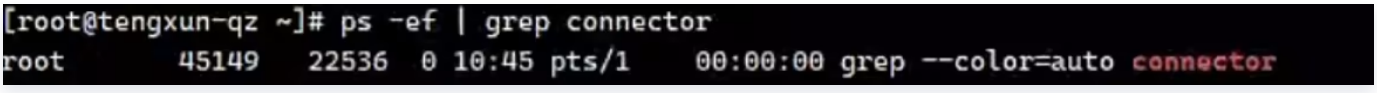
查看 SELinux 是否关闭

若部署连接器后查看进程未启动，服务启动异常，需要检查 SELinux 状态，部署连接器需要关闭 SELinux。

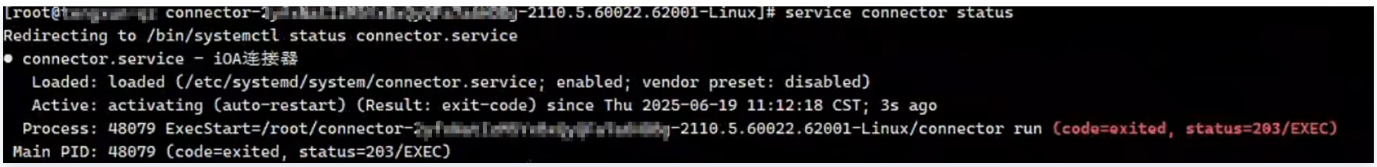
SELinux 对连接器的影响

SELinux 开启会影响 connector 服务向 systemd 注册。

- ps 查看 connector 进程未启动。



- systemctl status 查看服务启动报错。



SELinux 三种模式介绍

- Enforcing：强制模式。代表 SELinux 在运行中，且已经开始限制 domain/type 之间的验证关系。
- Permissive：宽容模式。代表 SELinux 在运行中，不过不会限制 domain/type 之间的验证关系，即使验证不正确，进程仍可以对文件进行操作。不过如果验证不正确会发出警告。
- Disabled：关闭模式。SELinux 并没有实际运行。

查看 SELinux 状态

使用 getenforce 命令查看 SELinux 状态。

```
[root@localhost]# getenforce
Disabled
```

关闭 SELinux

临时关闭（无需重启机器）

使用 setenforce 命令临时关闭 SELinux（不用重启机器即可生效，但是重启机器该命令会失效）。

```
setenforce 0 #转换为Permissive宽容模式
```

> **说明：**
> - setenforce 无法设置 SELinux 为 Disabled 模式。
> - 开启 SELinux：setenforce 1 #转换为 Enforcing 强制模式。

修改配置文件（需要重启机器生效）

```
vim /etc/selinux/config #修改/etc/selinux/config 文件
SELINUX=disabled #将SELINUX=enforcing改为SELINUX=disabled
reboot #重启机器
```

连接器排障指南（11.1.1版）

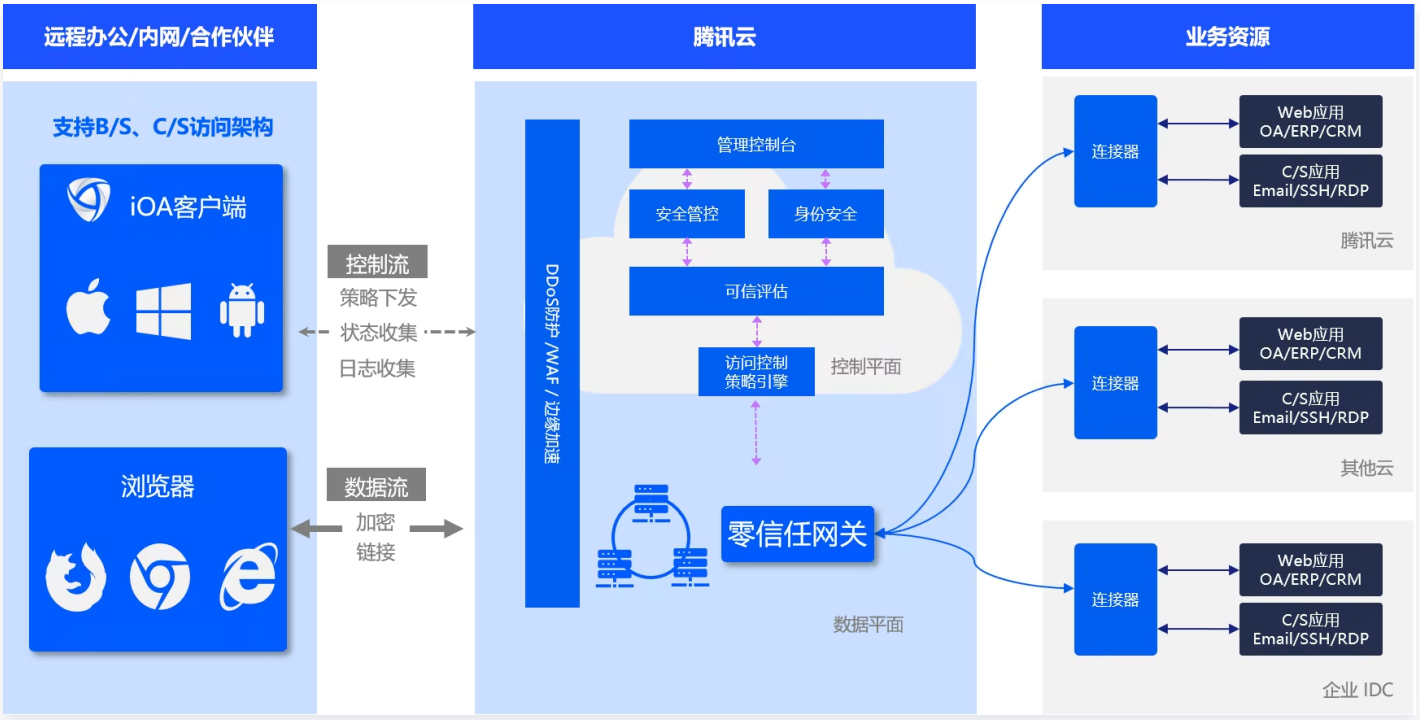
最近更新时间：2026-02-06 14:23:32

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

原理概述

连接器的作用

连接器主要起到连通网络的作用，同时可以做到业务隐身（连接器反向连通网关，不开监听端口），使得业务处于更安全的网络环境。本地的服务器需要具备这个条件：一侧网络可连通腾讯云，一侧网络可连通业务。在这样一台服务器上部署连接器，本质作用是从业务侧向腾讯云上的 iOA 零信任网关反向连通双向加密的隧道，以供流量通行。



连接器的技术原理

1. 连接器启动，向连接器管理服务注册(TLS 双向认证)，长连接定期发送心跳信息。
2. 用户发起访问，iOA 客户端流量拦截转发给 SaaS 网关。
3. SaaS 网关鉴权成功后，拦截并保持客户端的连接，发送控制命令(包含连接器 ID、网关地址、资源 ID 等信息)给连接器管理服务。
4. 连接器管理服务根据连接器 ID，获取连接器的长连接，通知该连接器访问业务资源并连接网关。

5. 连接器向业务资源发起连接(四层)，连接器向对应的网关发起反向连接(四层/TLS 双向认证)， 连接成功后，将业务和网关进行通信。
6. 网关将客户端连接和反向连接对接，iOA 客户端到业务资源的隧道建立完毕。
7. 请求和响应数据包通过隧道进行转发。

连接器部署机器软硬件要求

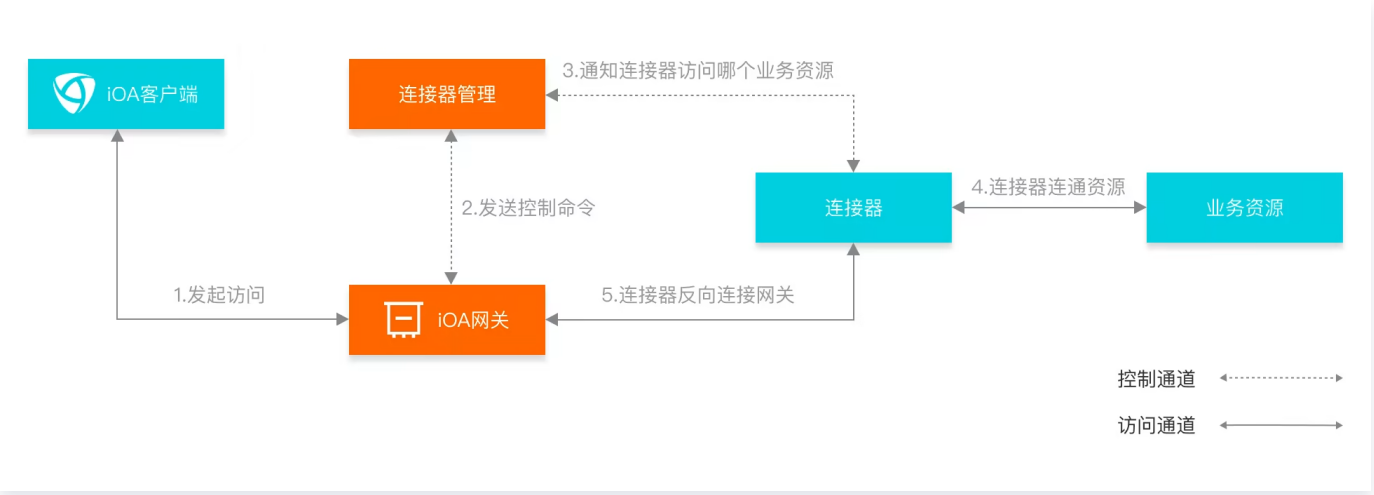
机器类型	操作系统	CPU	内存	存储	其他
本地主机/云服务器	• 建议使用 CentOS7.6及以上或其他 Linux 内核系统。 • 也支持 Windows 和 Windows Server 系统。	2-4核	4-8G	100G以上	建议单独使用机器部署，不同时运行其他业务系统

如何部署连接器

连接器部署场景、安装、卸载请参见 连接器部署（11.1.1版）。

连接器排障

1. iOA 代理资源访问的链路



排查与连接器相关组件故障而导致的iOA代理资源访问异常时，需注意以下几点：

- 控制通道是连通的，才能接收控制命令。
- 访问通道是连通的，才能成功访问业务资源。

- 需保障 iOA 客户端网络功能正常，完成客户端与控制面（申请小票）和数据面（网关）建立连接。
- 需保障连接器连通状态正常（连接器能接收从连接器管理组件下发的控制通道指令）。
- 需保障资源连通状态正常（确保连接器所在服务器的网络与业务资源打通）。
- 需保障连接器到网关的连通状态正常（连接器所在服务器网络与网关打通）。
- 连接器问题排查主要关注链路2-4，在此之前可先前往 iOA 控制台查看 资源访问日志 的**错误信息**列。

2. 查看代理访问日志错误信息

在 资源访问日志 页面，选择目标日志，查看错误信息。



错误信息	备注	处理方式
打通通道超时	连接器出口网络异常	排查连接器所属机器网络
租户分组连接器不存在	资源配置异常	控制台网关资源列表重新配置专线分组

3. 查看连接器连通状态

在 连接器管理页面，单击**刷新连通状态**，获取连接器的最新状态并检查专线连通性。



4. 查看资源连通状态

在 应用管理页面，查看资源连通状态。



> **说明：**
> 资源连通状态依赖于连接器到业务侧的连通性、连接器到 iOA 网关侧的连通性，因此请确保连接器对两侧的网络可达。

连接器通过周期性向业务发起探测包，并将探测结果上报控制台，有以下几种状态：

连通状态	备注	处理方式
正常	连接器到业务/iOA 网关网络连接正常	无需处理。
异常	连接器到业务/iOA 网关网络连接异常	1. 检查连接器到业务的网络是否连通。 2. 检查连接器到 iOA 网关的网络是否连通。 3. 如果配置地址段、端口段、泛域名等方式，由于连接器会随机探测，因此可能会探测到本身无法访问的地址导致显示异常。
检测中	资源连通性检测中	1. 等待连通检测通过。 2. 如果隧道资源配置了泛域名，可能会一直处于检测中的状态，可将资源修改成明细域名。如不影响使用则可以忽略。

5. 查看连接器到网关的网络连通性

详细地址请前往 连接器管理页面 说明栏中获取。

地址类型	示例	说明
连接器管理服务地址	`ch1.channel.gateway.tencentwsd.cn:30226`	连接器注册、上报心跳信息（连接器连通状态）。
反向连接服务地址	`ch2-{租户id}.channel.gateway.tencentwsd.cn:30225`	• 连接器访问资源，反向连接该服务，再对接网关，打通后即可访问资源。 • 对于共享带宽的用户，反向连接服务地址的端口是30225-30324其中的一个，在您的 iOA 初始化时进行分配。
控制面上报数据地址	`scs.gateway.tencent.com:443`	上报 NGN 代理访问日志、资源连通状态日志、连接器连通状态日志。

WireGuard 通道服务地址	wg1.channel.gateway.tencentwsd.cn(ip:13303)	网关 WireGuard 服务地址（UDP 协议）。

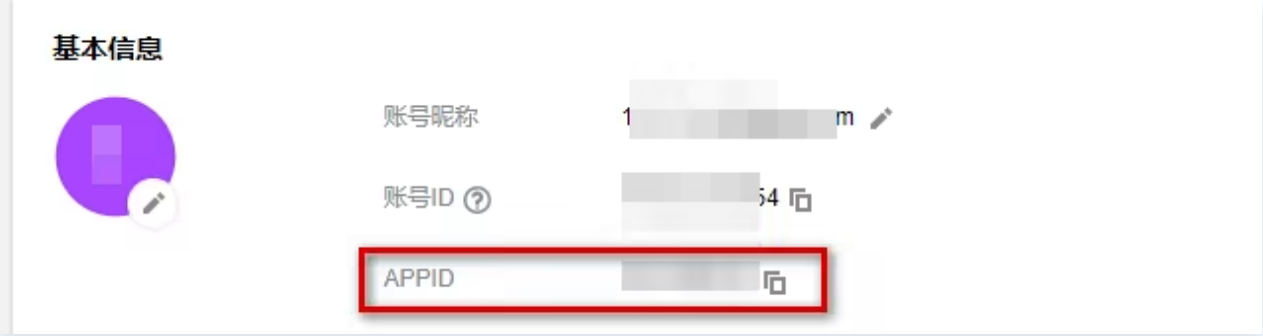
6. 如何确认连接器与网关的连通性

在连接器所属机器，执行 Telnet 命令：

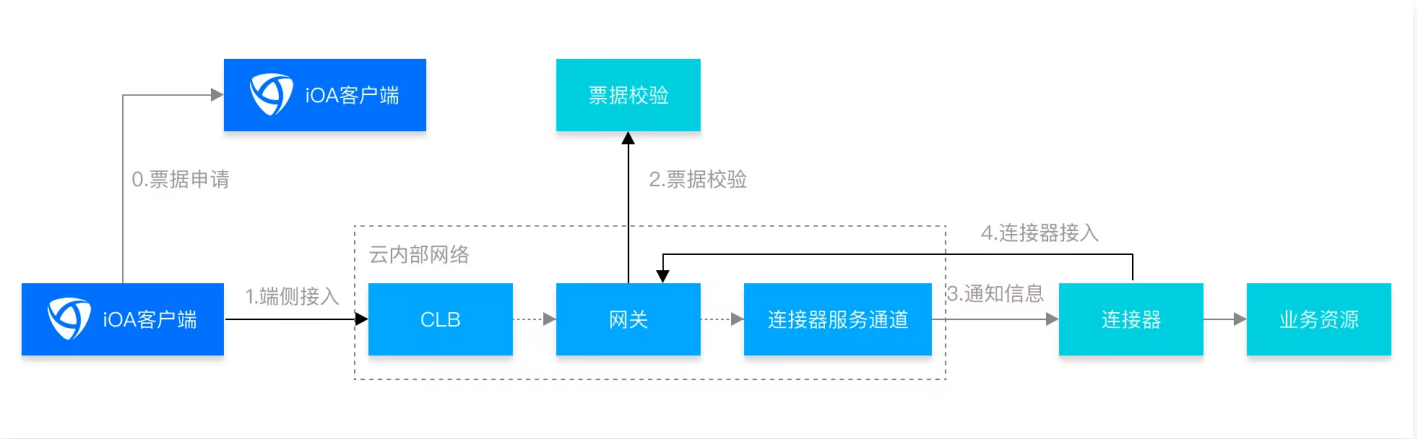
```
telnet ch1.channel.gateway.tencentwsd.cn 30226
telnet ch2-{租户id}.channel.gateway.tencentwsd.cn 30225
telnet scs.gateway.tencent.com 443
```

说明：

- 上述地址仅为示例，详细地址请前往 连接器管理页面 说明栏中获取。
- 域名可以换成从控制台上获取的 IP。
- WireGuard 通道服务地址使用 UDP 协议，只需放通无需使用 Telnet 测试。
- 租户 ID 是指腾讯云账号 APPID，可在账号信息处查看。



7. 连接器与客户端访问业务延迟测试



客户端访问业务延迟测试图例说明：

流程序号	说明
0	票据申请：影响资源的第一次访问，同一资源申请票据之后，本地会缓存30分钟。
1	端侧接入：使用您的网络运营商的主干网络，这部分网络质量依赖于网络运营商。
2	票据校验，目前网关可以增加缓存的方式，减少跟票据服务的网络交互。
3	通知信息：使用您的网络运营商的主干网络，这部分网络质量依赖于网络运营商。
4	连接器接入：使用您的网络运营商的主干网络，这部分网络质量依赖于网络运营商。

当前延迟测试主要集中在 iOA 客户端侧（用户侧）接入和连接器接入这两个流程，测试方法使用附件的工具，示例如下：

```
ssl-handshake -i 1000 -c 500 网关地址 //网关地址为： ch2-{腾讯云账号appid}.channel.gateway.tencentwsd.cn:9443//建议使用 IP 格式，详细地址获取见下方说明。
```

> **说明：**
> 详细 IP 地址可以前往 iOA 控制台 > 连接器管理 获取。



在不同系统平台上测试时，需选择对应平台测试工具，可通过以下链接获取：

平台	下载链接
Windows	iOA 测速工具-Windows
Mac	iOA 测速工具-Mac
Linux	iOA 测速工具-Linux

连接器文件说明

文件/文件夹名称	备注	处理方式
bin	存放软件执行库	无需变动
cert	存放证书文件	无需变动
config	存放程序配置文件	无需变动
connector	连接器运行程序	运行启动/关闭
logs	存放连接器日志文件	排查错误时使用
pid	连接器运行时进程 ID	无需变动
update	升级相关文件	无需变动
indep_update_info	版本信息	无需变动
welcome.html	本地开箱页面（HTTP 服务）	无需变动
README.md	存放连接器部署文档 md 文件	按需查阅，或在 连接器部署（11.1.1版）中获取

版权所有：腾讯云计算（北京）有限责任公司

启用零信任网关（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

零信任网关也称为本地网关，即将代理网关本地化部署，实现客户端访问业务流量通过本地部署的网关转发。业务资源所绑定专线分组下的连接器开启了零信任网关功能时，则终端访问业务时优先连接本地网关进行代理访问，当终端请求本地网关不通时，会再尝试连接云上 SaaS 网关进行代理访问。

> **说明：**
> 本地网关适用场景为存在内网用户访问内网业务也想走零信任访问控制的情景，如无需本地网关，请跳过此步骤，继续下一步 业务资源创建及授权 。

前提条件

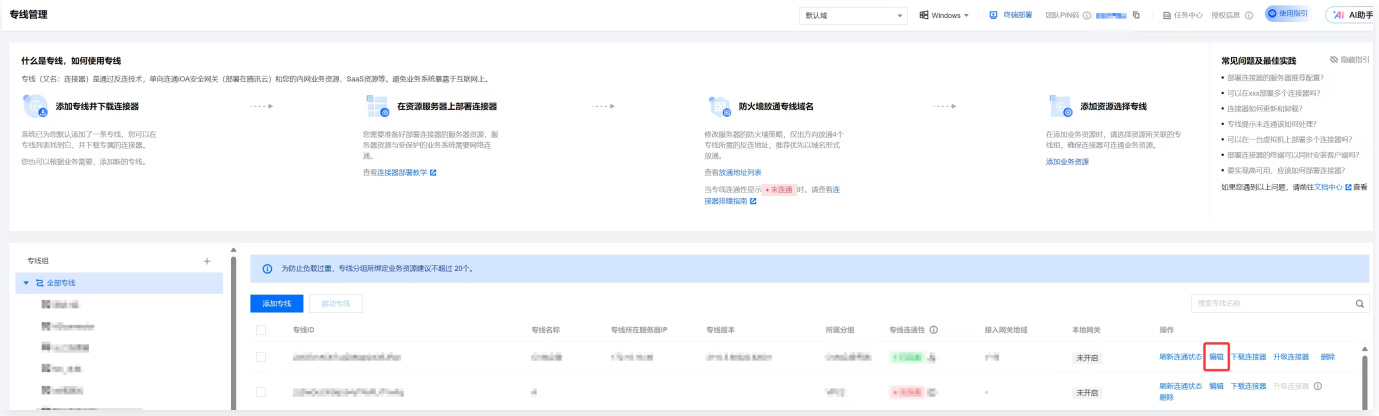
1. 已完成 连接器部署（11.1.1版） 。
2. 已 开通本地网关 功能授权。



3. 网络要求：开通客户端到零信任网关TCP 9443端口通信，若需要外网终端也通过本地网关访问时，需要将本地网关的9443端口映射到互联网。

启用配置

1. 登录 iOA 零信任管理平台控制台 ，在左侧导航栏，选择 连接器管理 。
2. 在连接器管理页面，找到需要启用本地网关功能的专线，单击**编辑**。



3. 在添加专线窗口中，开启**零信任网关开关**，并配置以下参数：
   - 网关出口 IP /域名：填写客户端访问本地网关的 IP 地址或域名。
   - 端口：默认值为9443。



4. 配置完成，单击**确定**保存，资源访问时将优先与零信任网关建联。

业务资源创建及授权（11.1.1版）
隧道类资源创建及授权访问（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

添加业务资源

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **应用配置信息**。
2. 在应用配置信息页面，单击**添加资源**。



3. 在添加资源页面，访问类型选择**隧道资源**，配置相关参数，单击**保存**。



参数名称	说明
访问类型	隧道资源。
资源名称	自定义。
资源分组	下拉选择资源分组或添加资源分组。
专线分组	选择的专线可以连通当前添加的业务资源。
协议类型	访问业务系统的协议类型，一般为 TCP 协议，根据实际情况选择。

资源类别	• 域名：支持使用通配符（支持泛域名和特殊符号）。 • IP：支持一次添加多个 IP。 • IP 段：支持一次添加多个 IP段。 • 域流量：添加域名。
端口	支持选择所有端口或指定端口，可一次添加多个端口。

4. 资源访问方式：启用内网直连功能后，当员工的客户端所处网络环境为您配置的办公内网中，将在办公内网中直连您所配置的隧道资源，不由 iOA 进行代理。
5. 配置完成单击**保存**。

业务资源授权

当资源添加后，还需要对用户进行资源授权。

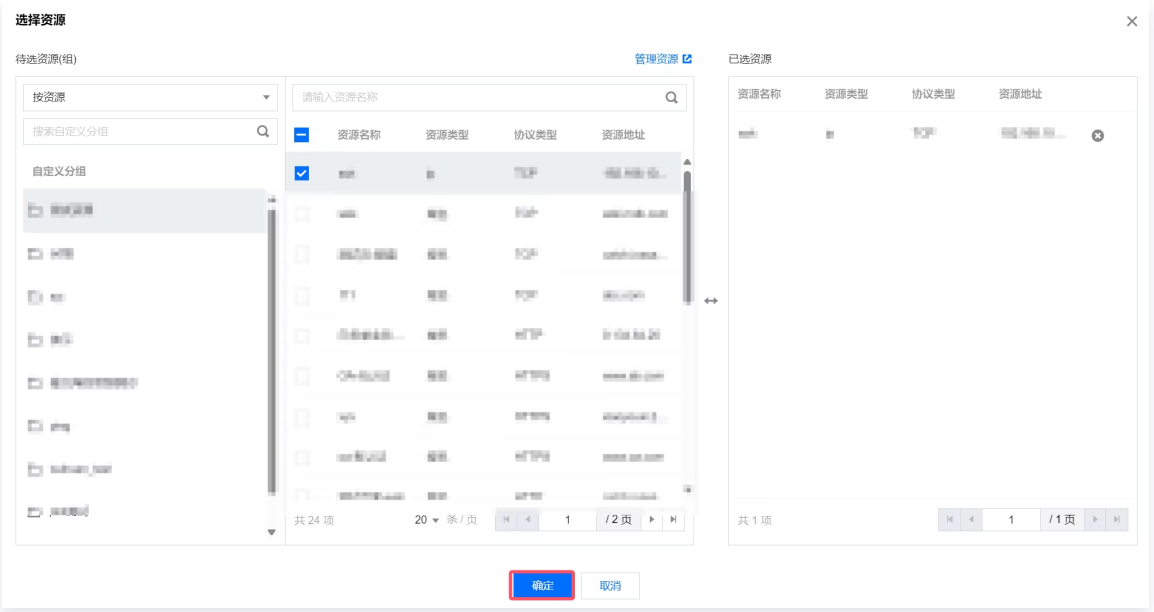
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **应用授权**。
2. 在用户与授权管理页面，选择所需目录，单击**目录名称**，选择需要授权的分组/账号，进行授权操作：

2.1 授权分组操作

2.1.1 选择需要授权的分组，单击**添加资源授权**。



2.1.2 在资源授权弹窗中，选择所需资源，单击**确定**。

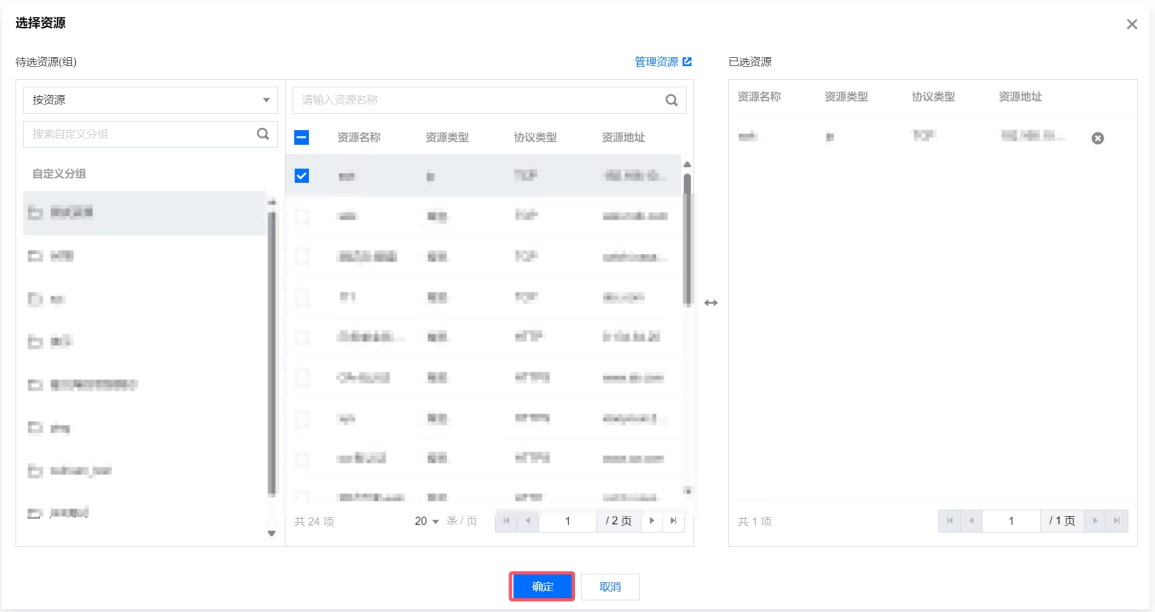


2.2 授权账户操作

2.2.1 在**组织结构 > 账户信息**页面，单击**目标账户**，单击**资源授权**。

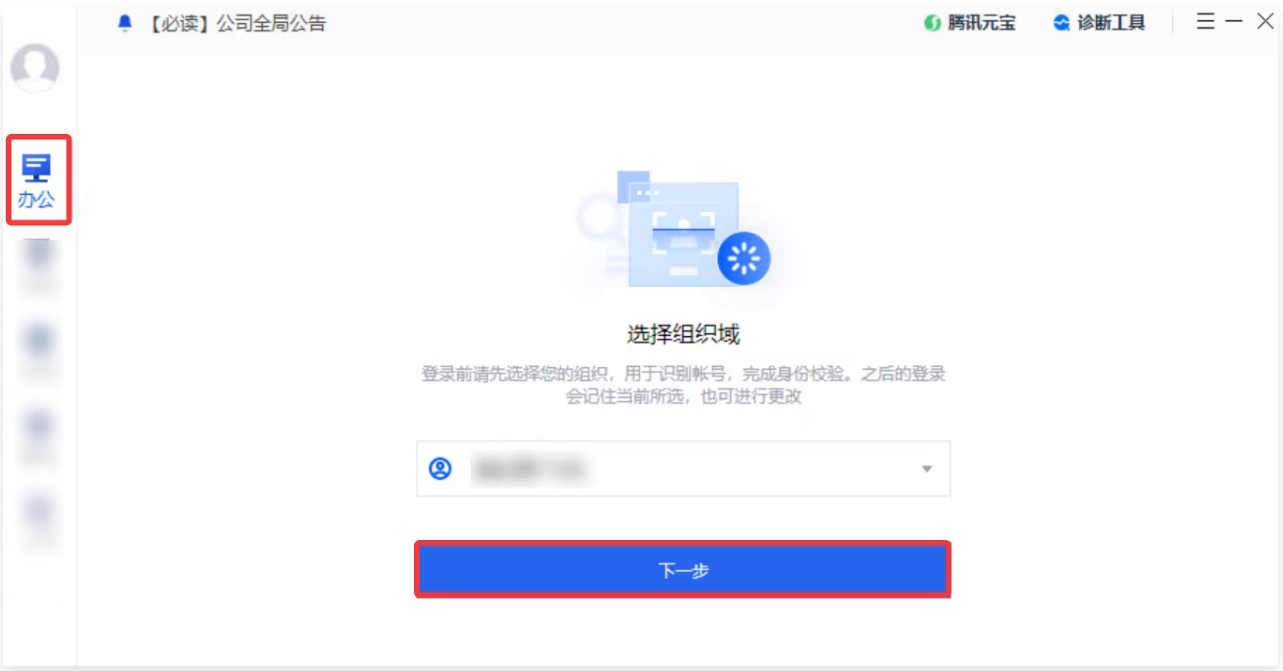


2.2.2 在资源授权弹窗中，选择所需资源，单击**确定**。



隧道资源认证与访问

1. 打开腾讯 iOA 客户端。
2. 选择对应的组织域，并完成用户登录。



3. 访问该用户拥有权限的业务资源成功。
4. 退出该账号，访问刚刚的业务资源失败。

客户端访问日志

查询日志

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**无边界办公** > **资源访问日志** > **客户端访问日志**。
2. 在客户端访问日志页面，支持按照如下方式查询日志。
   - 支持按时间范围查询。
   - 支持按终端访问日志/动态访问控制日志/代理访问日志查询。
   - 单击**搜索框**，出现日志表头的列表，可以对表头元素进行筛选查询。



日志条数统计

在日志条数统计模块中，支持左移查看昨日及之前的日志，以及鼠标悬浮展示具体数量，如：2025-07-14 8:00 单小时产生0条日志。

- 标签筛选：与查询框的联动，标签筛选展示近期查询过的表头标签。
- 修改用户姓名、用户目录、资源名称等信息时，日志字段同步。



Web 类资源创建及授权访问（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

添加业务资源

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **应用配置信息**。
2. 在应用管理页面，单击**添加资源**。



3. 在添加资源页面，访问类型选择 **Web 资源**，配置相关参数，单击**保存**。

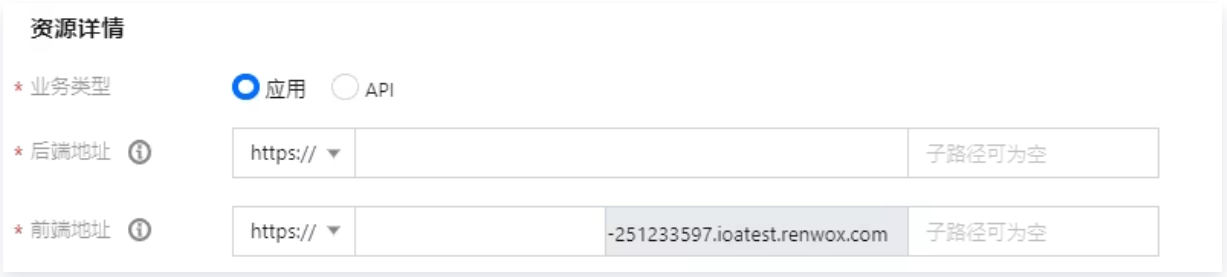
3.1 基本信息



参数名称	说明
资源名称	根据实际情况填写
资源分组	根据实际情况选择已有分组或者新建分组。
专线分组	选择的专线可以连通当前添加的业务资源。

3.2 资源详情

- **业务类型-应用：**应用（Web）类型资源适用于业务系统的远程办公场景，例如：OA 系统接入到 iOA 防护，企业员工可以在外网通过 iOA 访问内部的 OA 系统。



参数名称	说明
后端地址	业务资源的内网地址，支持填写域名、IP、子路径。例如：`https://192.168.10.8:843`。
前端地址	外网环境下可访问的地址。

> **注意：**
> 支持 HTTPS 和 HTTP 协议，当协议为 HTTPS 时，需要添加 SSL 证书。

- **业务类型-API：**API 类型资源适用于小程序的 API 接口调用，或合作伙伴远程调用 API 接口的防护，例如：A 公司为 B 公司提供物资查询接口 API，该API 需要经过 iOA 防护。



参数名称	说明
API 密钥	自动生成 API 密钥，为了您的服务安全，请定期更换密钥。您可以在**网关系统设置** > **密钥管理**进行查看与管理。
后端地址	业务资源的内网地址，支持填写域名、IP、子路径。例如：`https://192.168.10.8:843`。
前端地址	业务资源在外网环境下的访问地址。

访问 API 资源示例：访问资源 `https://api.myproxy.com:8080/api` 时，需要在请求头上增加 key 为 Proxy-Authentication，值根据密钥字符串生成请求密钥 authValue（使用该密钥请求 API 密钥类资源）。密钥获取请见控制台**网关系统设置** > **密钥管理**。

```
secret := "控制台密钥内容"

// 当前时间戳
tm := time.Now().Unix()
// 时间戳和密钥组成授权 Json
authJson = "{tm: tm, sign:sha256(secret+tm)}"
//授权 Json 进行base64即可获取请求密钥
authValue=base64_encode(authJson)

//验证 API 密钥资源是否生效
curl-X POST "https://api.myproxy.com:8080/api" -H "Proxy-
Authentication:base64(密钥内容)"
```

3.3 更多设置



参数名称	说明
SSL 证书	协议为 HTTPS 时需要添加，根据要求上传证书和密钥。
Host	可选配置，若业务地址需要检查 Host，则需要配置此选项。

启用依赖地址	适用于 Web 页面下有很多子应用的场景。例如门户网站：`www.qq.com`，进入首页后，下属还有 `news.qq.com`、`sports.qq.com` 等。将下属站点的地址写入到依赖地址中，网关会对其做前端访问地址的改写。

业务资源授权

当资源添加后，还需要对用户进行资源授权。当授权用户访问前端地址并通过认证后跳转到对应的业务资源页。

> **注意：**
> 非授权用户不可访问。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **应用授权**。
2. 在用户与授权管理页面，选择所需目录，单击**目录名称**，选择需要授权的分组/账号，进行授权操作：

2.1 授权分组操作

2.1.1 选择需要授权的分组，单击**添加资源授权**。



2.1.2 在资源授权弹窗中，选择所需资源，单击**确定**。

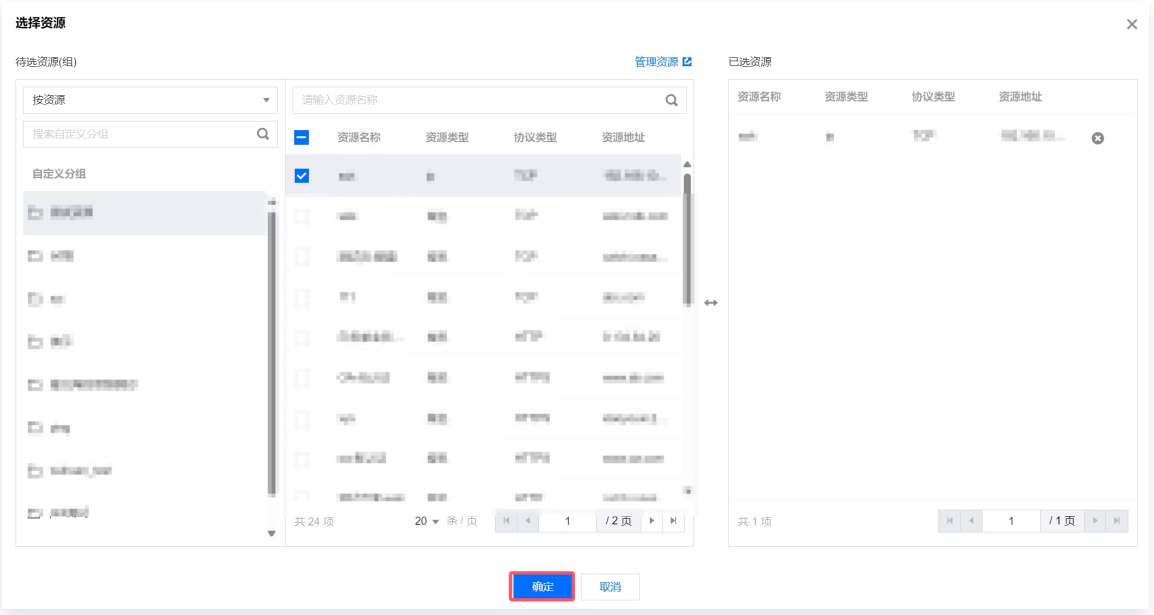


2.2 授权账户操作

2.2.1 在**组织结构 > 账户信息**页面，单击**目标账户**，单击**资源授权**。

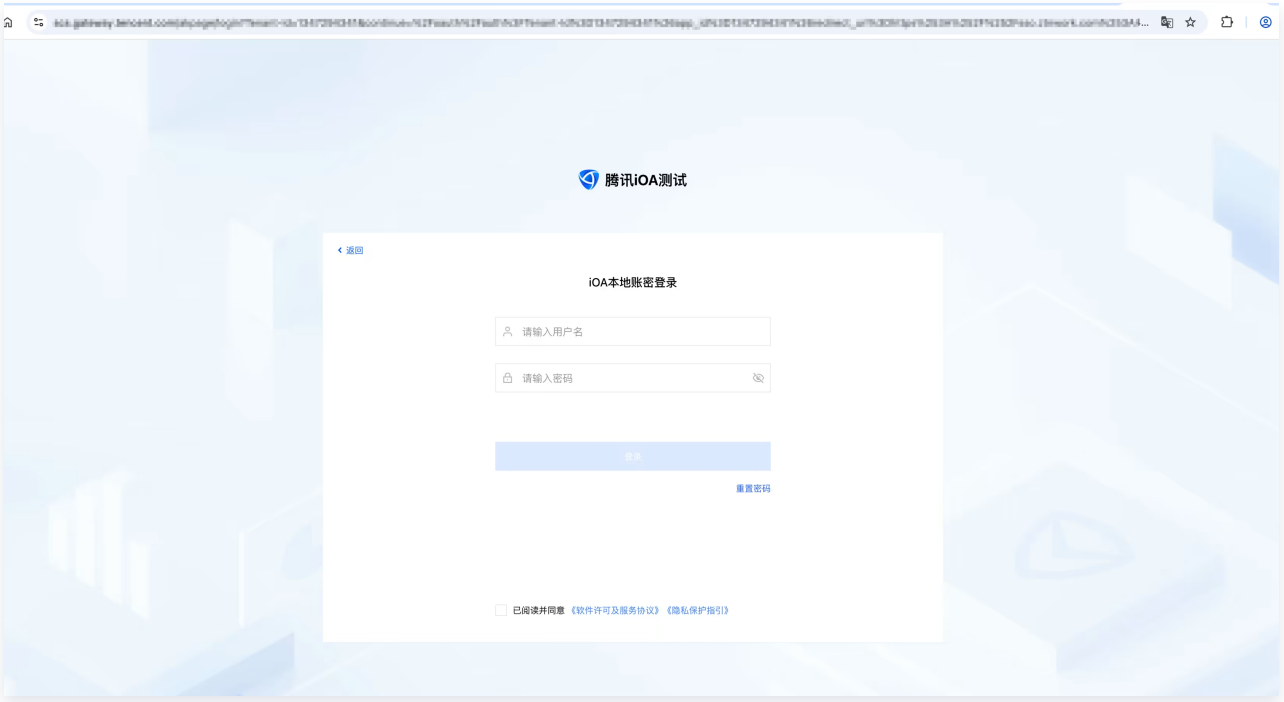


2.2.2 在资源授权弹窗中，选择所需资源，单击**确定**。

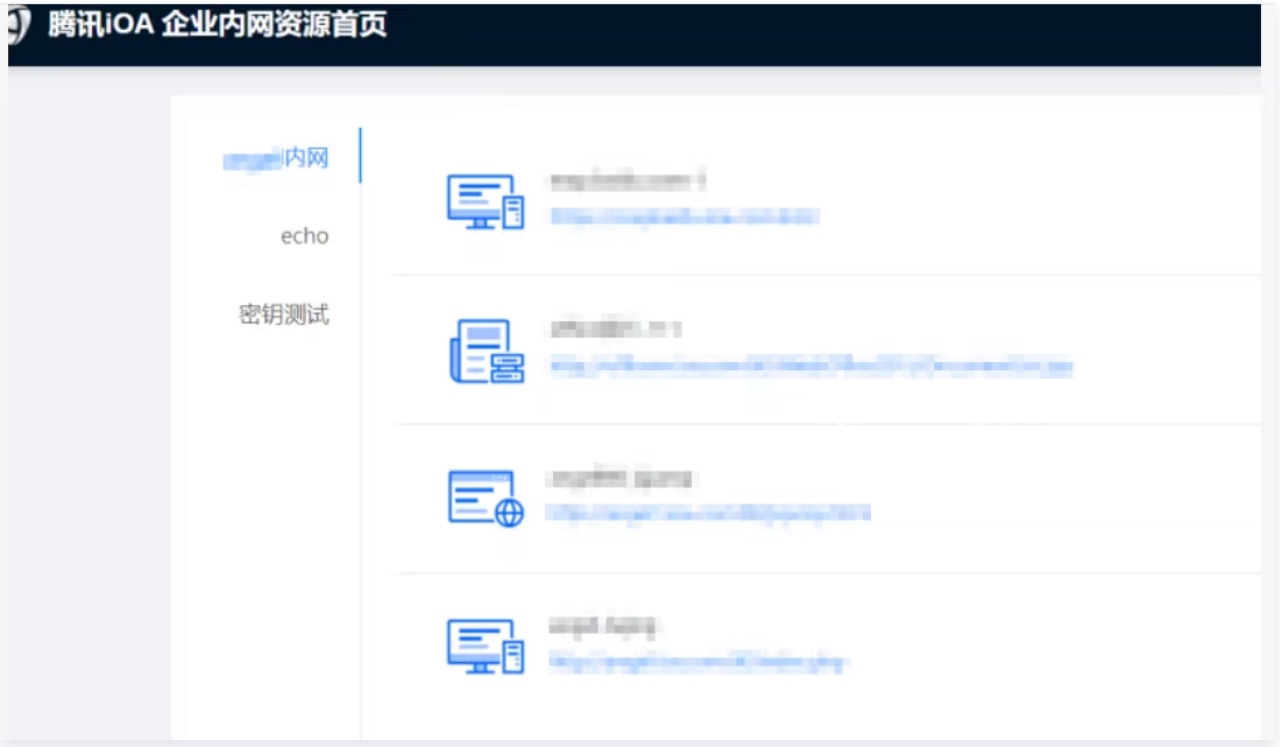


认证与访问 Web 资源

1. 参考 添加业务资源 和 业务资源授权，配置 Web 资源。
2. 打开浏览器，输入 iOA 零信任管理平台控制台上配置的**前端地址**，完成账户认证。



3. 认证通过后，即可访问账户对应权限的业务资源。



关联模块介绍

Web 访问日志

查询日志

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**无边界办公** > **资源访问日志** > **Web 访问日志**。
2. 在 Web 访问日志页面，支持按照如下方式查询日志。

- 支持操作时间范围查询。
- 支持时间范围+搜索组合查询。
- 单击**搜索框**，出现日志表头的列表，可以对表头元素进行筛选查询。



日志条数统计

在日志条数统计模块中，支持左移查看昨日及之前的日志，以及鼠标悬浮展示具体数量，如：2025-07-14 8:00 单小时产生0条日志。

- 标签筛选：与查询框的联动，标签筛选展示近期查询过的表头标签。
- 修改用户姓名、用户目录、资源名称等信息时，日志字段同步。
- Web 资源访问日志在该日志审计页不支持删除，可在 **基础设置** > **系统日志清理** 进行统一的删除。



动态访问控制（11.1.1版）
动态访问控制策略配置（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

功能简介

传统 VPN 采用静态访问权限，一旦用户认证成功就赋予访问权限。如果员工账号被盗取、冒用将带来极大的信息安全风险。基于终端访问风险模型进行动态访问控制，可实现动态感知风险、响应治理风险并收缩访问权限。

> **说明：**
> 该功能仅支持隧道类资源。



终端访问风险模型采用风险要素综合评估、动态访问控制策略组合，有效管控用户访问资源。如上图所示，用于评估的风险要素包括应用进程、网络位置、访问时间、设备合规等级，其中设备合规等级评估要素包括密码强度、网络端口、系统服务、系统进程、应用软件等安全基线。动态访问控制策略包括受限访问、挑战认证后访问、禁止访问。

策略规则说明

- 策略将从上到下匹配，数字越小最先匹配。

- 当请求命中一条策略后，则不会继续匹配。
- 策略的顺序会决定最终的策略效果，需谨慎考虑策略的具体位置。
- 尽量指明具体需要管控的人员或资源组内容，为了您的业务安全，**谨慎使用完全放通或完全禁止的策略**。

查询策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **访问策略**。
2. 在访问安全策略页面，可查看用户（组）名下的全部策略权限，便于回溯、排障、查看策略冲突情况等。



新增策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **访问策略**，单击**添加访问策略**。



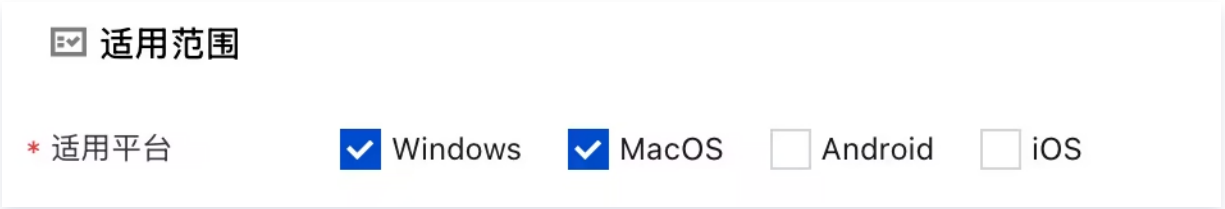
2. 在新建策略页面，配置相关参数，单击**保存**。

2.1 基本信息：输入策略名称、策略说明等参数。

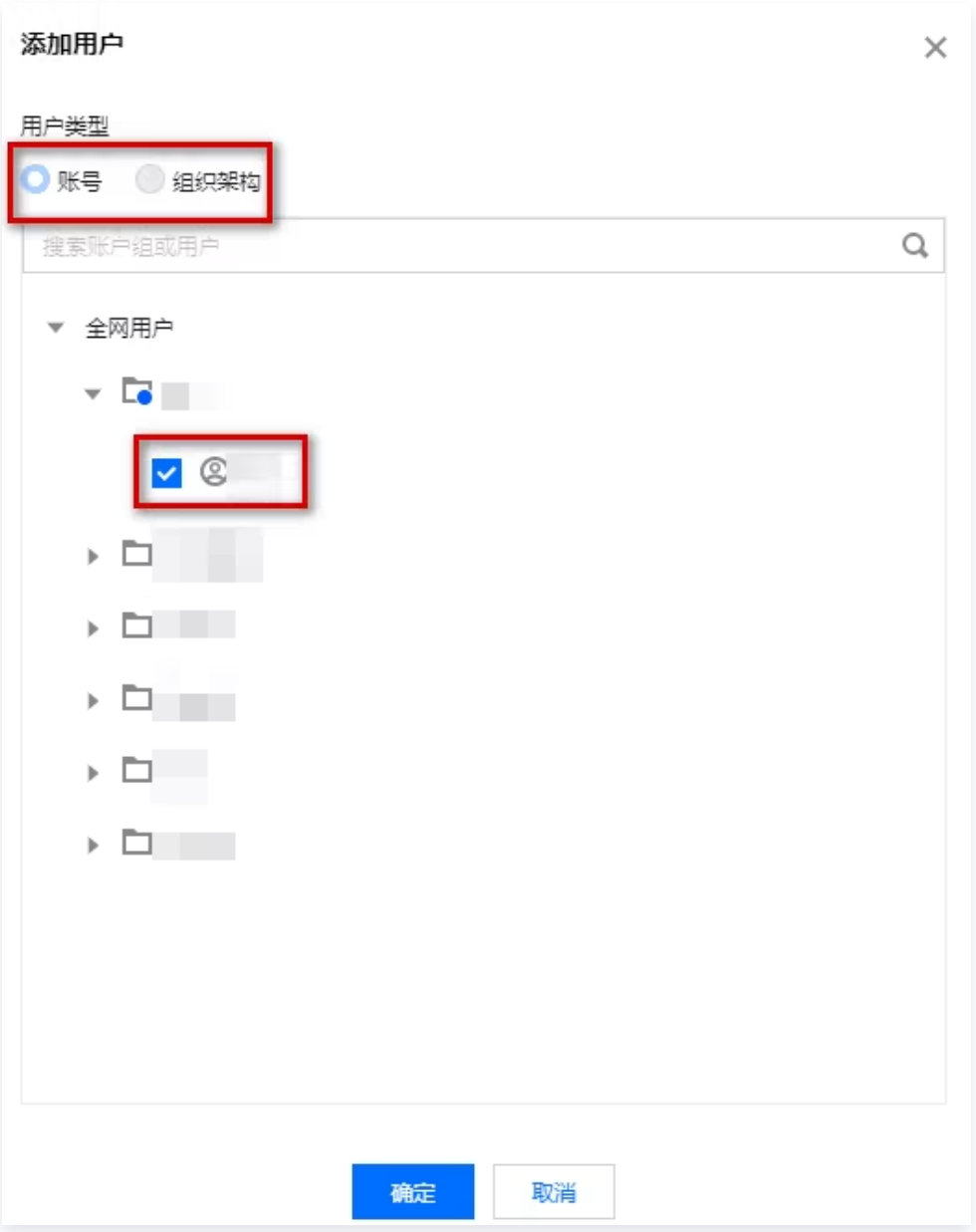


2.2 适用范围：当用户卡片中的人员尝试访问指定的资源时才会执行对应的访问处置。

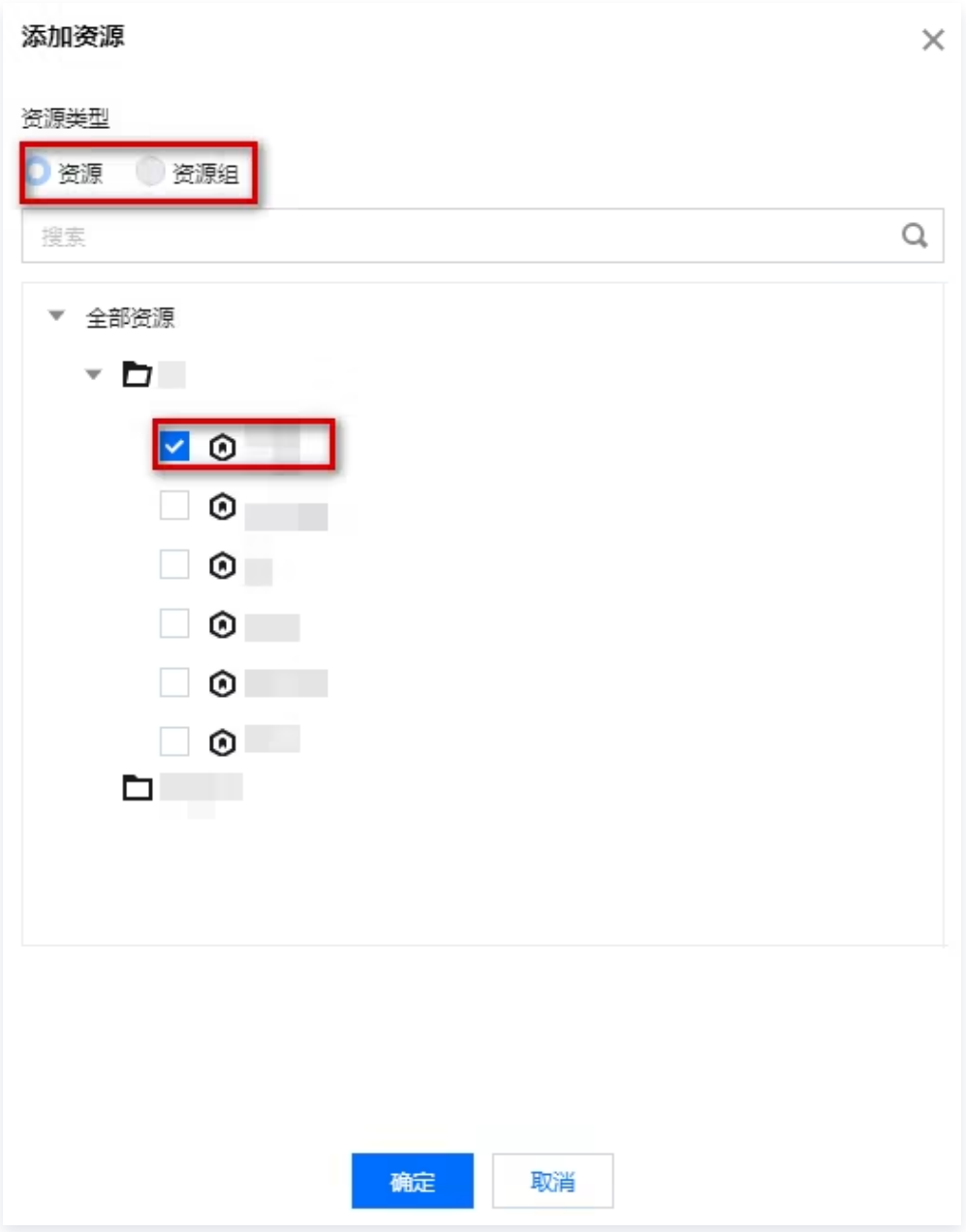
2.2.1 勾选适用平台，从对应平台终端发起访问才会执行对应的访问处置。



2.2.2 单击**添加用户**，选择需要配置策略的账号/组织架构，单击**确定**。



2.2.3 单击**添加资源**，根据实际情况选择单个资源/资源组，单击**确定**。



2.3 访问处置：设定匹配适用范围下访问请求的处置类型，以达到您的管理诉求。

- 禁止访问：用户禁止访问业务资源。
- 挑战认证后访问：用户完成挑战认证后可访问业务资源。
- 允许访问：不做处置，直接放通访问。

> ⚠ **注意：**
> 需要先在认证策略配置中对用户/用户组选择 挑战认证的方式 。

2.4 高级条件设置：单击**添加该条件**，增加以下选项将细化访问处置的执行条件，匹配适用范围的请求会在满足高级条件时执行相应处置。



功能名称	详情
访问时间段	• 可选访问的时间段，在范围内执行策略响应动作；超出访问时间覆盖范围即阻断访问。 • 单击**限制指定访问时间**，自动弹出设置时间。 • 基于精准时间段/星期/日期（且的关系）。 • 时间点精确到分钟。
指定网络位置	可以通过指定网络来实现特定条件的访问，任意区域意味着不校验终端所在的网络环境。 • IP 分组：关联 IP 分组。支持按 IP 组名模糊搜索；支持全选。 • 地理位置：选项对应地区即可，（后台内置国家标准 IP 库，此库变动较少，若变动后台会周期性更新（类病毒库））。
应用程序	• 目前仅支持 Windows 和 macOS。 • 关联的是可信应用-分组详情，根据实际情况选择。

违规风险等级	• 终端发起业务访问时，检测上一次的合规检测结果与动态策略的匹配情况。
	• 自定义检测周期，下限可配“5分钟”。
	• 在添加合规检测时设置该合规项违规等级。
	  ○ 违规等级高：命中至少1条高违规项。
	  ○ 违规等级中：未命中高违规项，至少命中1条中违规项。
	  ○ 违规等级低：未命中高及中违规项，至少命中1条低违规项。
	  ○ 检测项违规等级配置路径：**资产管理** > **终端管控** > **合规检测**（任一检测项内）。

	
设备范围	• 设备范围关联：资产管理–终端运维–终端信息–自定义分组。 • 自定义分组中创建的设备组，在设备范围处展示。

编辑策略

1. 在 访问策略 页面，选择所需策略，单击**编辑**。



2. 在编辑策略页面，修改相关参数，单击**保存**。

删除策略

1. 在 访问策略 页面，选择所需策略，单击**删除**。



2. 在确认删除弹窗中，单击确定，即可删除该策略。

> **注意：**
> 策略删除后将无法恢复，请确保设置了合适的替代策略。

调整策略顺序

1. 在 访问策略 页面，单击**顺序框**，输入相应数字，单击**空白处**。



2. 在确认调整弹窗中，单击**确定**，即可调整顺序。



修改认证方式

如需修改账户认证方式（例如：账密认证改为短信验证码认证），请参考以下步骤：

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**身份安全管控** > **认证策略**。
2. 在认证策略页面，选择所需目录，选择需要修改认证方式的策略名称，并单击**编辑**。



3. 在编辑认证策略页面，修改认证方式（例如：勾选短信验证码），单击**添加**，即可完成认证方式修改。

> **说明：**
> 单个目录下的主认证方式由基础策略决定，如需调整主认证方式，请修改基础策略的主认证方式的认证源。

配置认证安全策略

单个目录下的主认证方式由基础策略决定，如需调整主认证方式，请修改基础策略的主认证源选择

PC端

主认证方式的认证源

iOA本地账密, AD认证源, 短...

新企业微信
企微测试
钉钉对接测试
企微认证
短信验证码
AD认证源

确定 重置

素

挑战认证方式认证源

iOA本地账密, 短信验证码

移动端

主认证方式的认证源

iOA本地账密

双因素认证

是否启用

二次认证方式的认证源

请选择

指定主认证登录豁免双因素

添加 取消

测试用例（11.1.1版）
限制指定访问时间（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

测试目的

在指定访问时间内，访问业务资源触发挑战认证，认证通过后访问成功。

前提条件

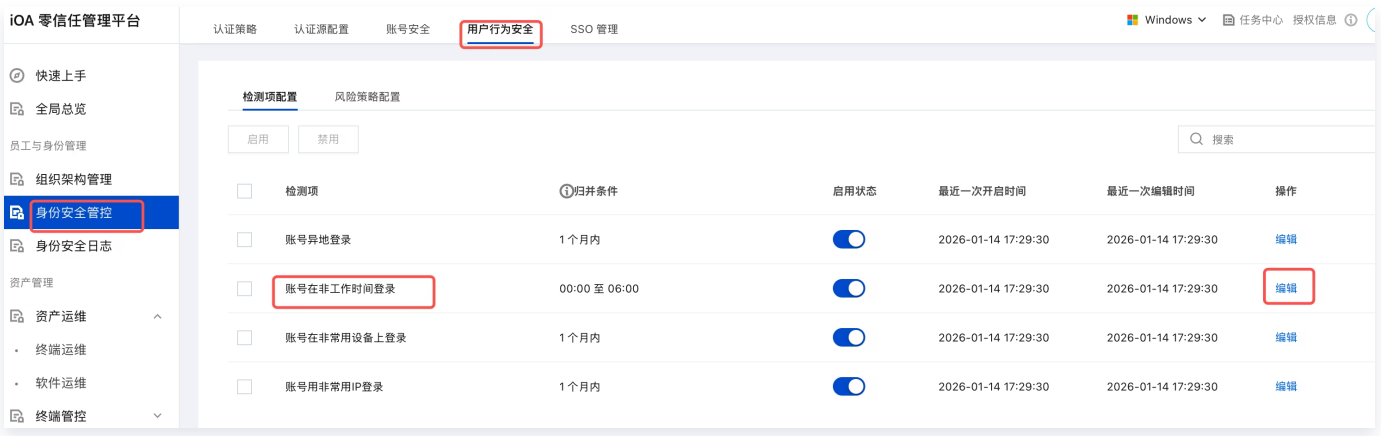
1. iOA 客户端成功部署。
2. 完成账号创建以及认证源配置。
3. 完成业务资源的添加。
4. 完成对应用户和资源的授权。

测试示例

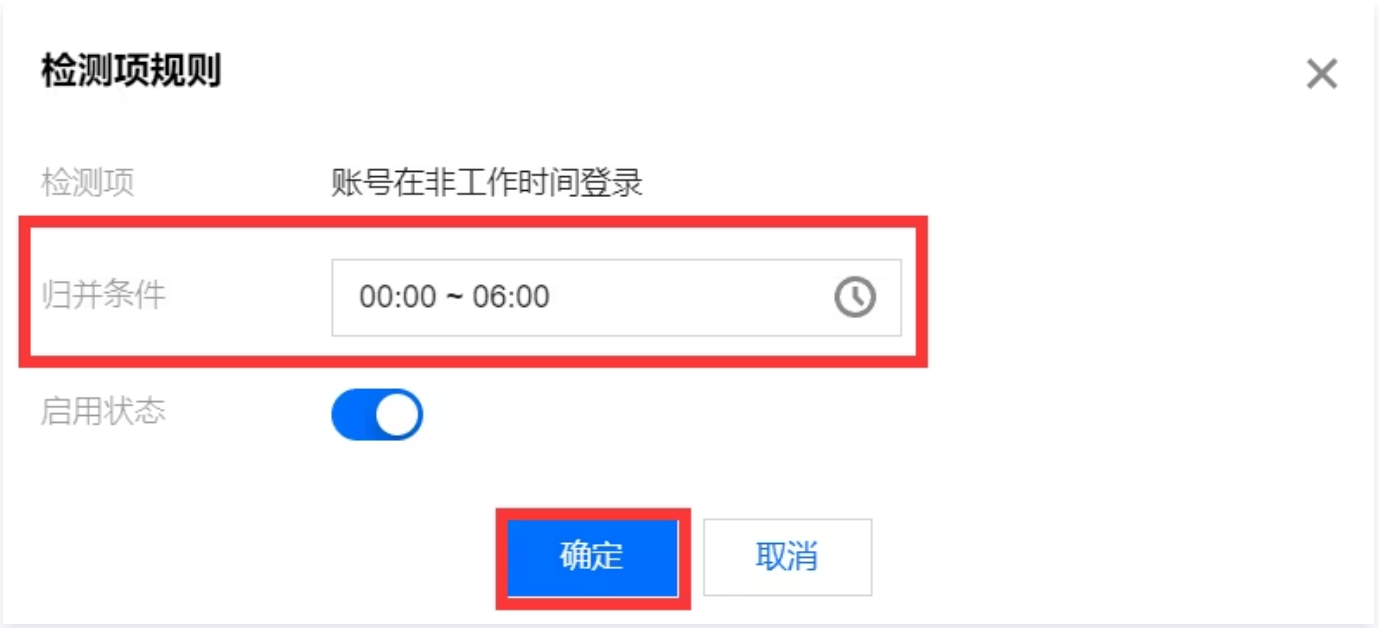
场景举例：非工作时间：00:00~6:00，访问指定业务资源触发挑战认证。

步骤1：定义非工作时间

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**身份安全管控** > **用户行为安全**。
2. 在用户行为安全页面，选择**检测项配置**，单击**账号在非工作时间登录**的**编辑**。

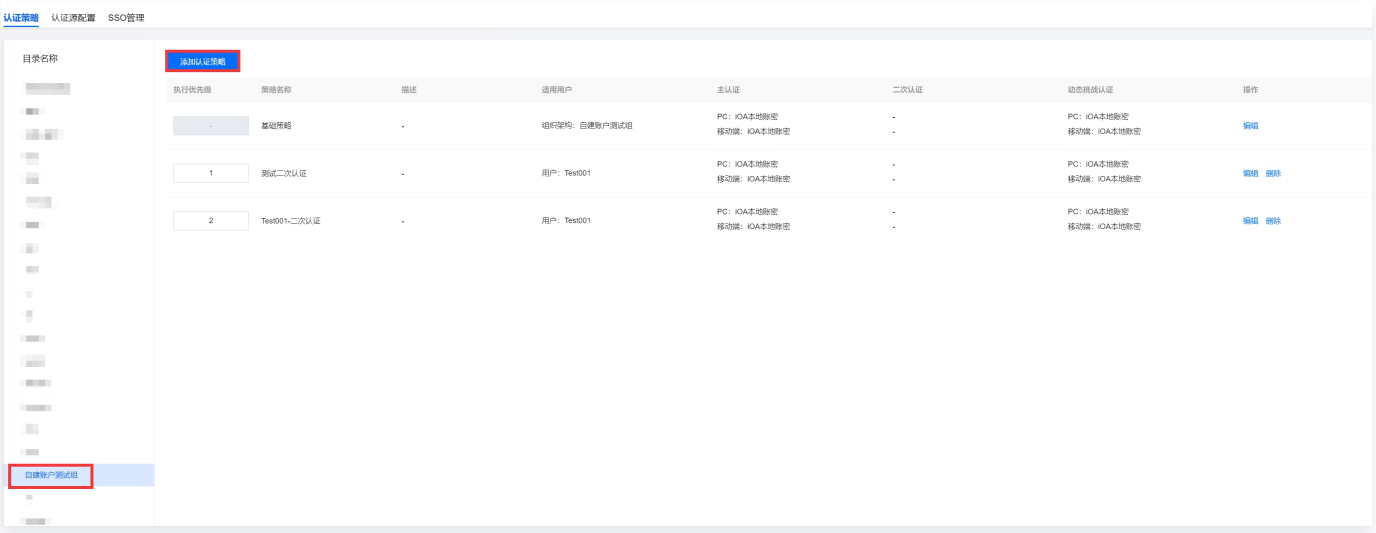


3. 示例：设置账号在非工作时间登录：0:00~6:00，单击**确定**。



步骤2：配置认证策略

1. iOA 零信任管理平台控制台，在左侧导航栏，选择**身份安全管控** > **认证策略**。
2. 选择**目录名称**，单击**添加认证策略**。



3. 配置示例：设置 PC 端挑战认证方式认证源为 **iOA 本地账密**，单击**添加**。

编辑认证策略

基本信息 > 适用范围 > 配置认证安全策略

基本信息

* 策略名称 Test001-二次认证 12/144

策略描述 填写描述 0/288

策略执行优先级 自定义 − 2 + 数字越小越早执行,若数字已存在,指定数字之后的策略依次+1顺延

适用范围

适用对象	类型	操作
Test001	用户	删除

设定适用范围

配置认证安全策略

单个目录下的主认证方式由基础策略决定，如需调整主认证方式，请修改基础策略的主认证源选择

PC端

主认证方式的认证源

iOA本地账密

AD域环境免认证

双因素认证

是否启用

二次认证方式的认证源

扫码认证, 企微认证

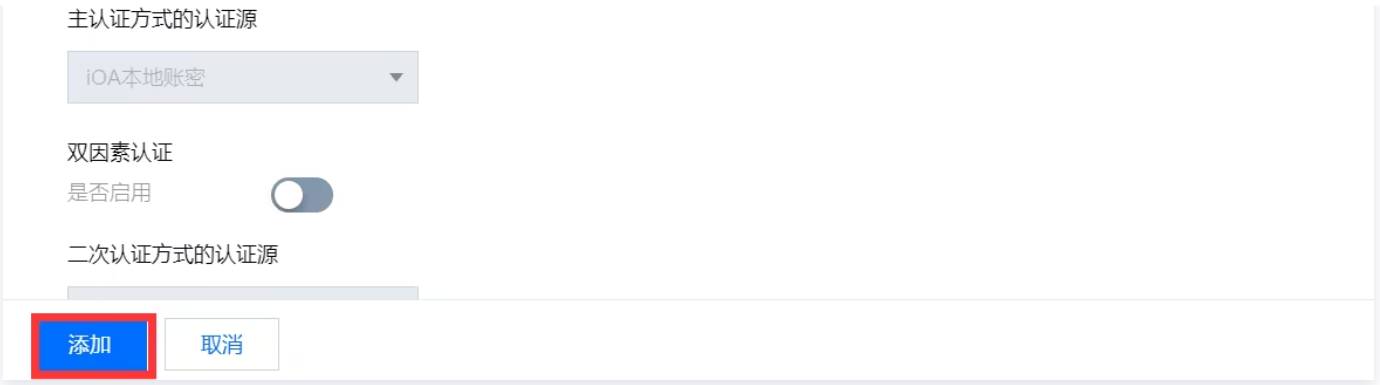
指定主认证登录豁免双因素

请选择

挑战认证方式认证源

iOA本地账密

移动端



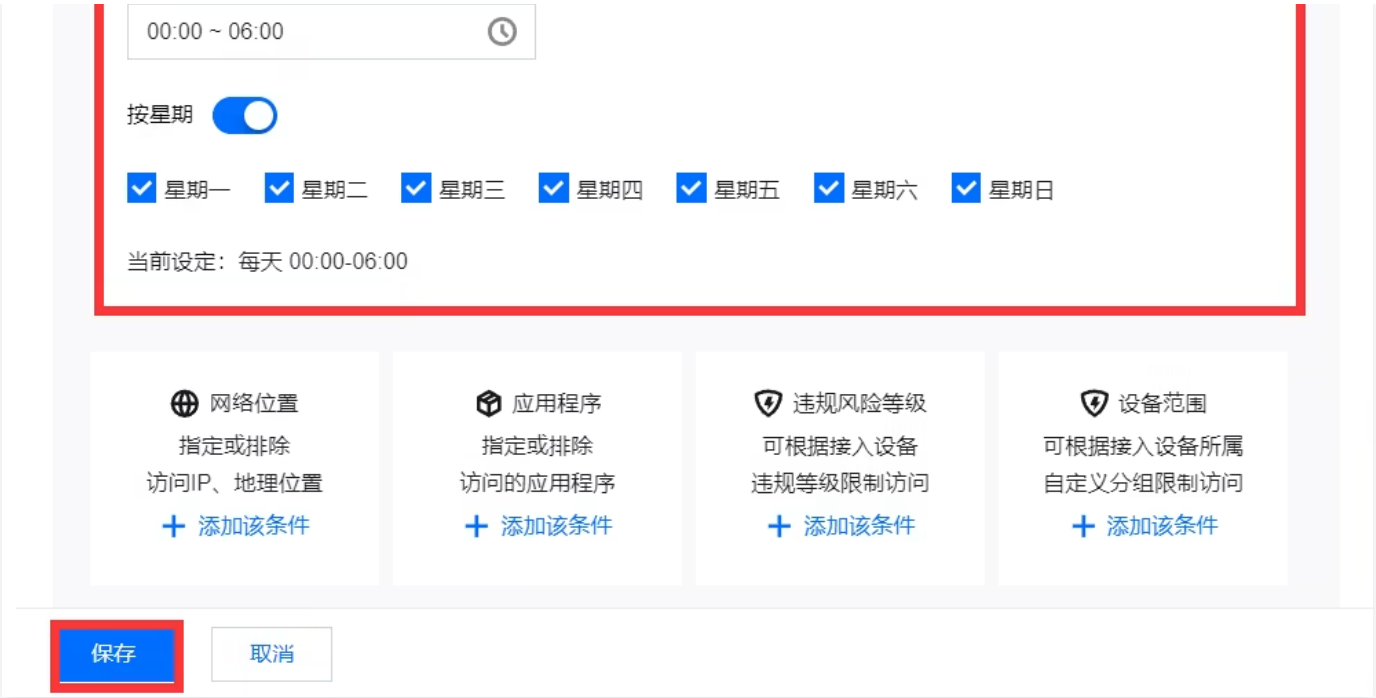
步骤3：配置访问安全策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **访问策略**，单击**添加访问策略**。



2. 在新建策略页面，配置相关参数，其中访问处置选择**挑战认证后访问**，访问时段设置为**00:00~6:00**，单击**保存**。


编辑策略
* 是否启用
当前保存后即刻生效.选择关闭可手动启用
* 策略顺序位置
列表最前
列表最后
指定位置
适用范围
当用户卡片中的人员尝试访问指定的资源时才会被执行对应的访问处置
用户
1条记录，共1人
Test001
添加用户
资源
1条资源
wiki
添加资源
访问处置
设定匹配适用范围下访问请求的处置类型,以达到您的管理诉求
禁止访问
挑战认证后访问
允许访问
高级条件设置
启用或增加以下选项将细化访问处置的执行条件.匹配适用范围的请求会在满足高级条件时执行相应处置.
可以通过条件运算建立复杂的场景需求,运算的结果和添加的顺序无关
访问时间段
删除
按时间



步骤4：终端验证

账号在非工作时间登录（0:00~6:00），访问指定业务资源触发挑战认证。其余时间访问不触发挑战认证。


安全提醒
为保障资源安全，请在此窗口完成二次认证，随后刷新访问
iOA本地账密确认
Test001
请输入密码
登录
选择登录方式

IP 分组联动挑战认证（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

测试目的

指定 IP 的终端访问业务资源时，需要通过挑战认证才能访问对应业务资源。

前提条件

1. iOA 客户端成功部署。
2. 完成账号创建以及认证源配置。
3. 完成业务资源的添加。
4. 完成对应用户和资源的授权。

测试示例

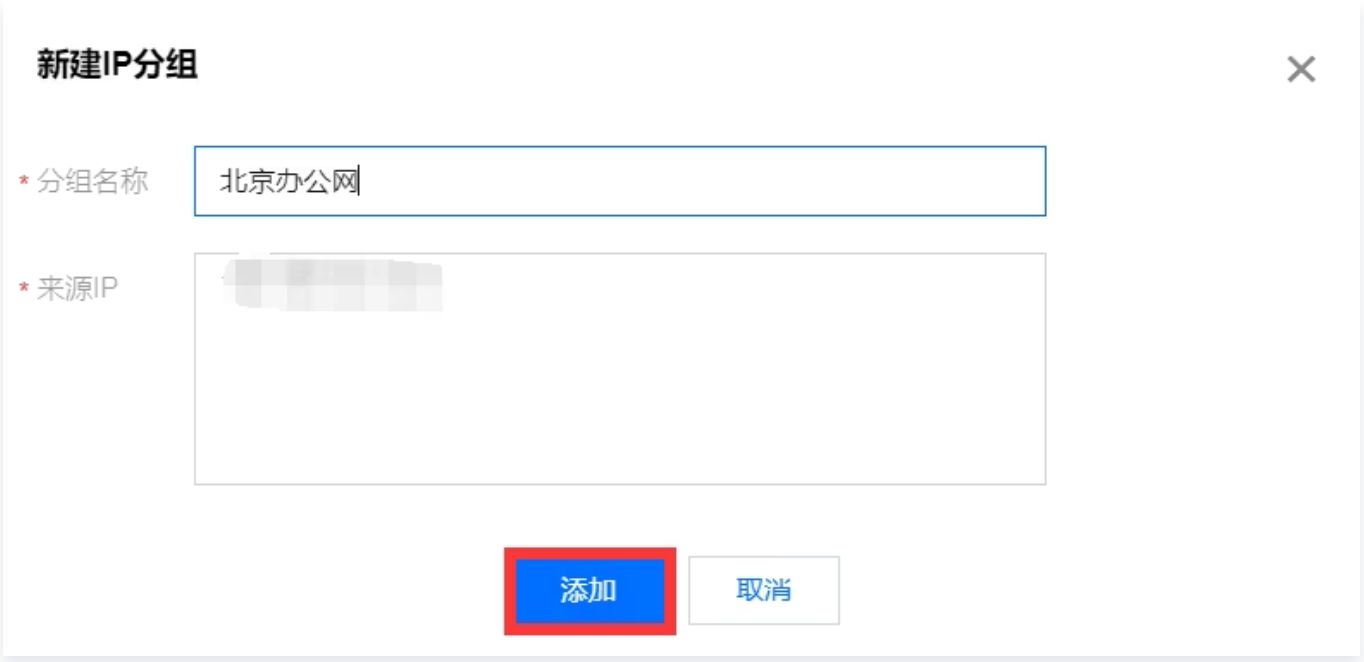
场景举例：分配“北京-办公网”，指定“北京-办公网”的访问权限。

步骤1：新建 IP 分组

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**无边界办公** > **网关系统设置** > **IP 分组管理**。
2. 在 IP 分组管理页面，单击**新建 IP 分组**。



3. 在新建 IP 分组弹窗中，配置相关参数，单击**添加**。



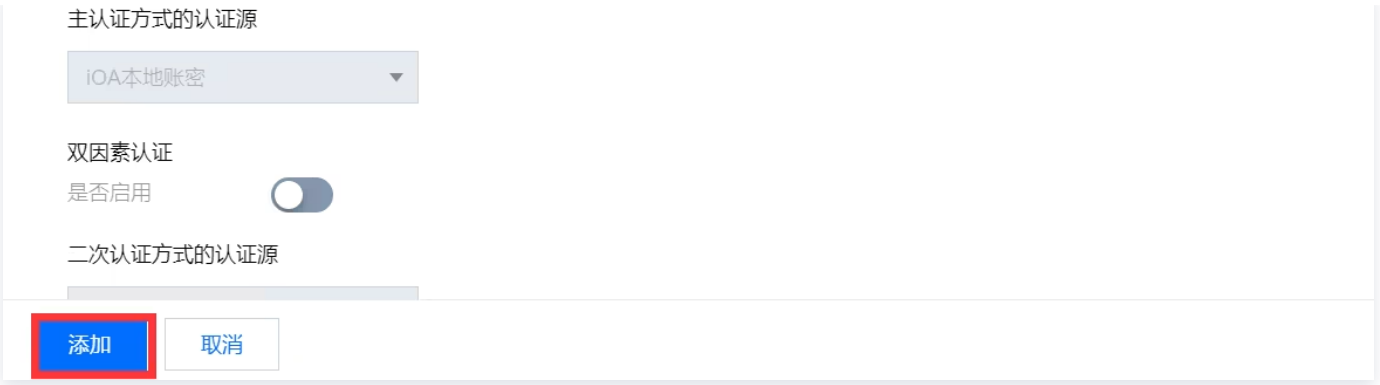
步骤2：配置认证策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**身份安全管控** > **认证策略**。
2. 在认证安全页面，选择**认证策略**，选择**目录名称**，单击**添加认证策略**。



3. 配置示例：设置 PC 端挑战认证方式认证源为 **iOA 本地账密**，单击**添加**。


编辑认证策略
基本信息
适用范围
配置认证安全策略
基本信息
* 策略名称
Test001-二次认证
12/144
策略描述
填写描述
0/288
策略执行优先级
自定义
2
数字越小越早执行,若数字已存在,指定数字之后的策略依次+1顺延
适用范围
适用对象
类型
操作
Test001
用户
删除
设定适用范围
配置认证安全策略
单个目录下的主认证方式由基础策略决定，如需调整主认证方式，请修改基础策略的主认证源选择
PC端
主认证方式的认证源
iOA本地账密
AD域环境免认证
双因素认证
是否启用
二次认证方式的认证源
扫码认证, 企微认证
指定主认证登录豁免双因素
请选择
挑战认证方式认证源
iOA本地账密
移动端



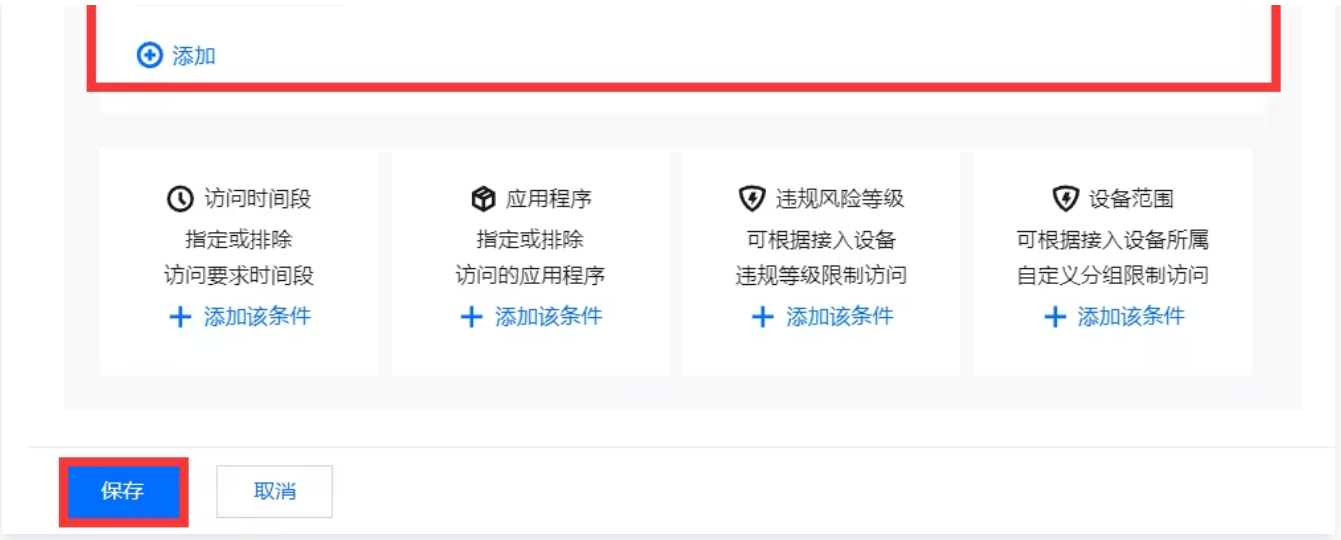
步骤3：配置访问安全策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **访问策略**，单击**添加访问策略**。



2. 在新建策略页面，配置相关参数，其中访问处置选择**挑战认证后访问**，网络位置选择**北京办公网**，单击**保存**。


* 策略名称
IP分组联动挑战认证
10/144
策略说明
0/288
* 是否启用
当前保存后即刻生效.选择关闭可手动启用
* 策略顺序位置
列表最前
列表最后
指定位置
适用范围
当用户卡片中的人员尝试访问指定的资源时才会被执行对应的访问处置
用户
1条记录，共1人
Test001
添加用户
资源
1条资源
wiki
添加资源
访问处置
设定匹配适用范围下访问请求的处置类型,以达到您的管理诉求
禁止访问
挑战认证后访问
允许访问
高级条件设置
启用或增加以下选项将细化访问处置的执行条件.匹配适用范围的请求会在满足高级条件时执行相应处置.
可以通过条件运算建立复杂的场景需求,运算的结果和添加的顺序无关
网络位置
删除
北京办公网



步骤4：终端验证

终端 IP 指定分组内，需要完成挑战认证才能访问业务资源。



版权所有：腾讯云计算（北京）有限责任公司

应用访问联动挑战认证（11.1.1版）

最近更新时间：2026-02-13 09:41:03

说明：
iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

测试目的

指定应用组内的应用访问业务资源，触发挑战认证，认证成功后，访问业务资源成功。

前提条件

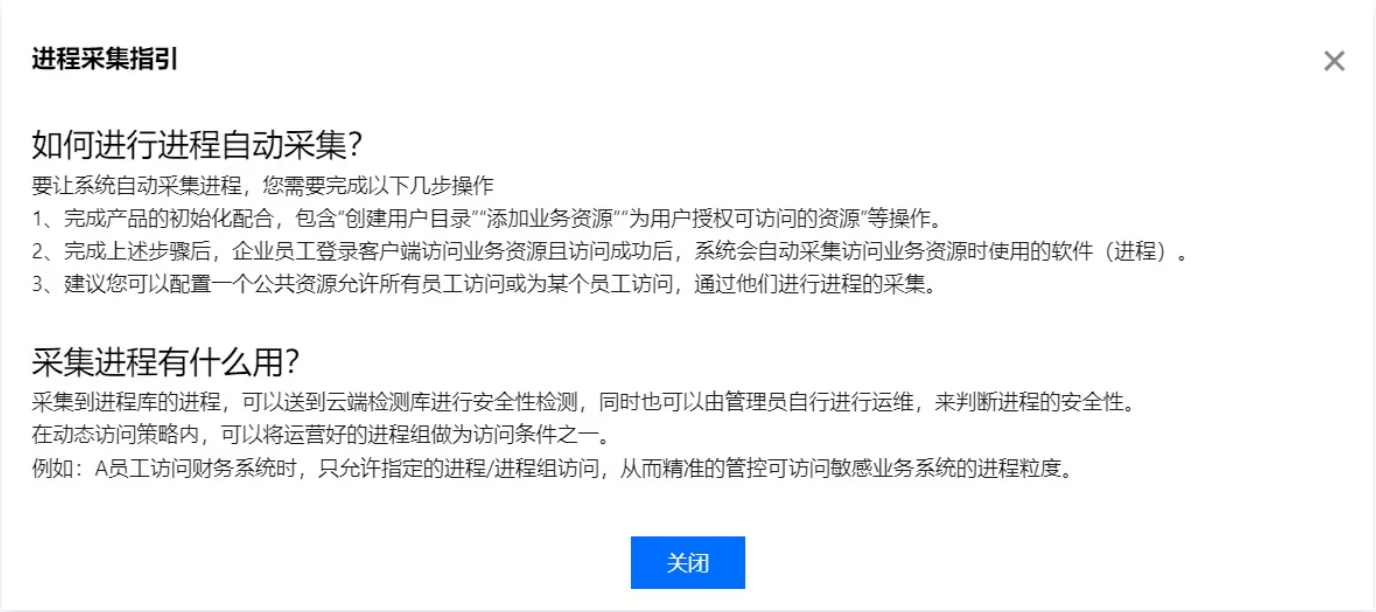
1. iOA 客户端成功部署。
2. 完成账号创建以及认证源配置。
3. 完成业务资源的添加。
4. 完成对应用户和资源的授权。

测试示例

场景说明：例如出于运维工具安全考虑，PuTTY 访问运维系统时，需要通过挑战认证后才能访问。

步骤1：安装 PuTTY 并设置为可信应用

1. 在安装有 iOA 客户端的任意一台终端上安装 PuTTY。
2. 等待 iOA 控制台自动采集进程。



3. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **可信应用管理**。
4. 在可信应用管理页面，选择**未分组应用**，将 PuTTY 设置为可信应用，单击**标为可信**。



步骤2：创建应用分组

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **可信应用管理**。
2. 选择分组详情，单击 > **添加应用分组**。



3. 在添加应用分组弹窗中，输入分组名称，并选中系统类型，单击**确定**。



4. 选择所需分组，单击**添加应用**，将 PuTTY 添加到分组内，单击**确定**。



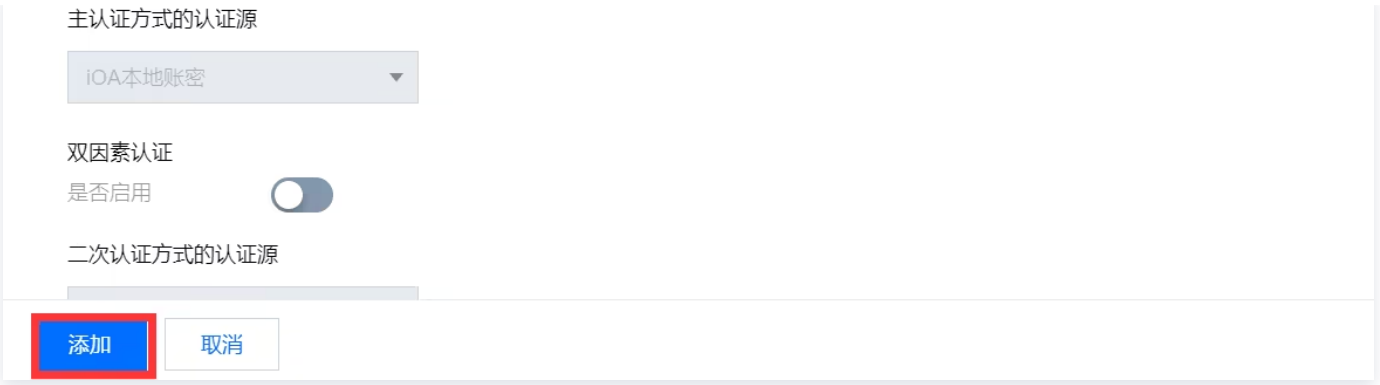
步骤3：配置认证策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**身份安全管控** > **认证策略**。
2. 选择**目录名称**，单击**添加认证策略**。



3. 配置示例：设置 PC 端挑战认证方式认证源为 **iOA本地账密**，单击**添加**。


编辑认证策略
基本信息
适用范围
配置认证安全策略
基本信息
* 策略名称
Test001-二次认证
12/144
策略描述
填写描述
0/288
策略执行优先级
自定义
2
数字越小越早执行,若数字已存在,指定数字之后的策略依次+1顺延
适用范围
适用对象
类型
操作
Test001
用户
删除
设定适用范围
配置认证安全策略
单个目录下的主认证方式由基础策略决定，如需调整主认证方式，请修改基础策略的主认证源选择
PC端
主认证方式的认证源
iOA本地账密
AD域环境免认证
双因素认证
是否启用
二次认证方式的认证源
扫码认证, 企微认证
指定主认证登录豁免双因素
请选择
挑战认证方式认证源
iOA本地账密
移动端



步骤4：配置访问安全策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **访问策略**，单击**添加访问策略**。



2. 在新建策略页面，配置相关参数，其中访问处置选择**挑战认证后访问**，添加 PuTTY 应用，单击**保存**。

* 策略名称 指定进程挑战认证 8/144

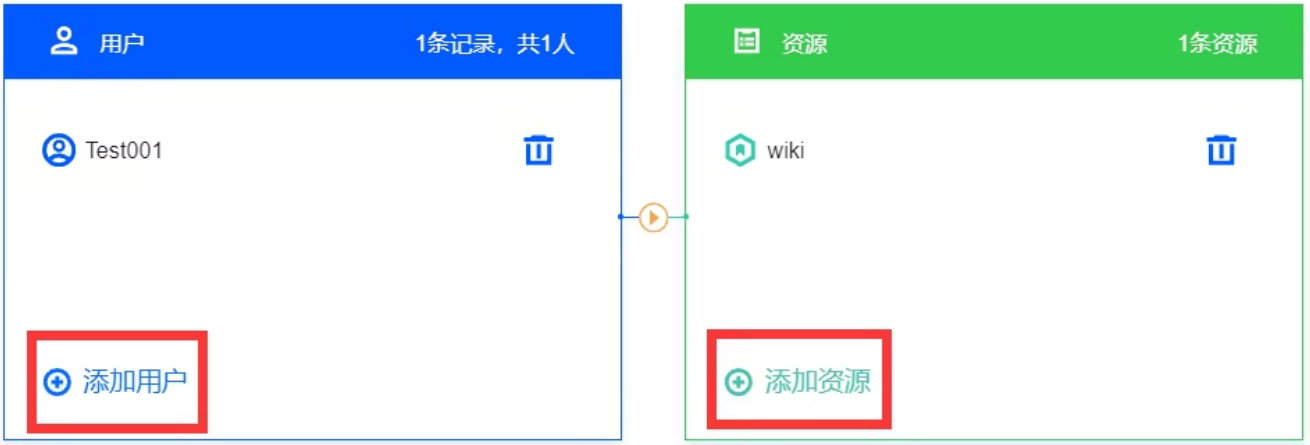
策略说明 0/288

* 是否启用 当前保存后即刻生效.选择关闭可手动启用

* 策略顺序位置 列表最前 列表最后 指定位置

适用范围

当用户卡片中的人员尝试访问指定的资源时才会被执行对应的访问处置



访问处置

设定匹配适用范围下访问请求的处置类型,以达到您的管理诉求

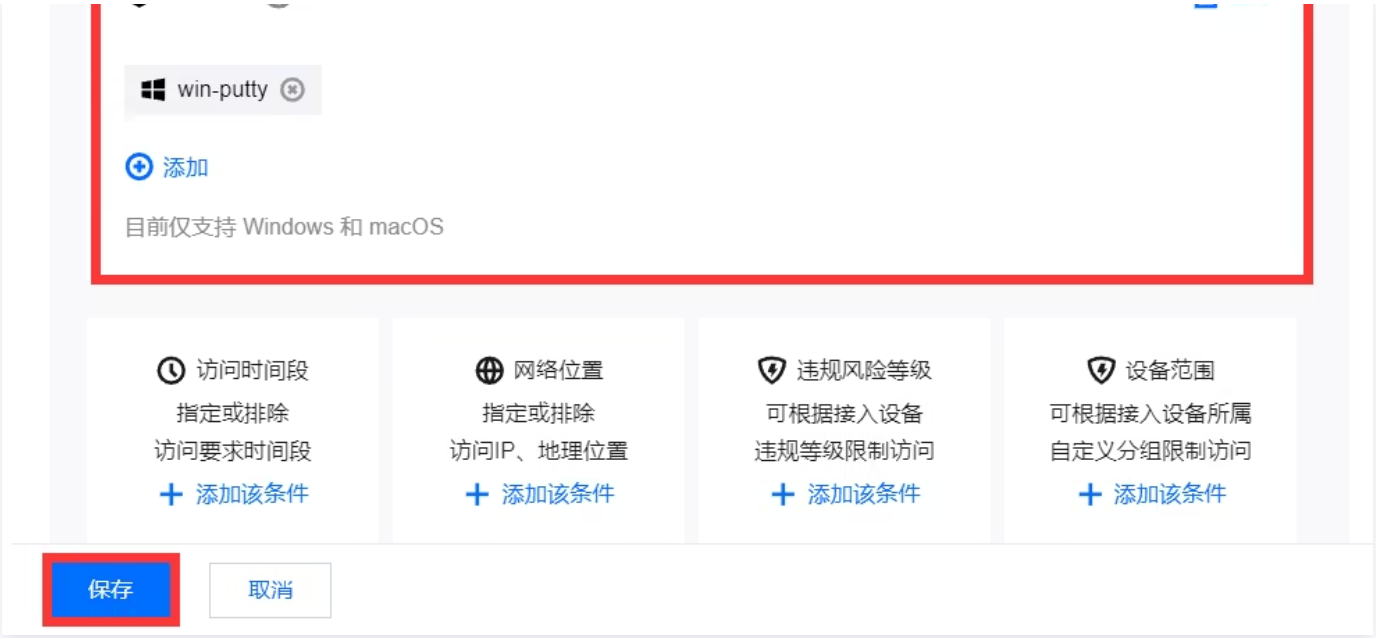
禁止访问 挑战认证后访问 允许访问

高级条件设置

启用或增加以下选项将细化访问处置的执行条件.匹配适用范围的请求会在满足高级条件时执行相应处置.

可以通过条件运算建立复杂的场景需求,运算的结果和添加的顺序无关

应用程序 删除



步骤5：终端验证

打开 PuTTY，访问对应的业务资源，完成挑战认证后访问成功。


安全提醒
为保障资源安全，请在此窗口完成二次认证，随后刷新访问
iOA本地账密确认
Test001
请输入密码
登录
选择登录方式

终端合规检测联动挑战认证（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

测试目的

通过终端设备合规情况来管控访问业务资源的权限。

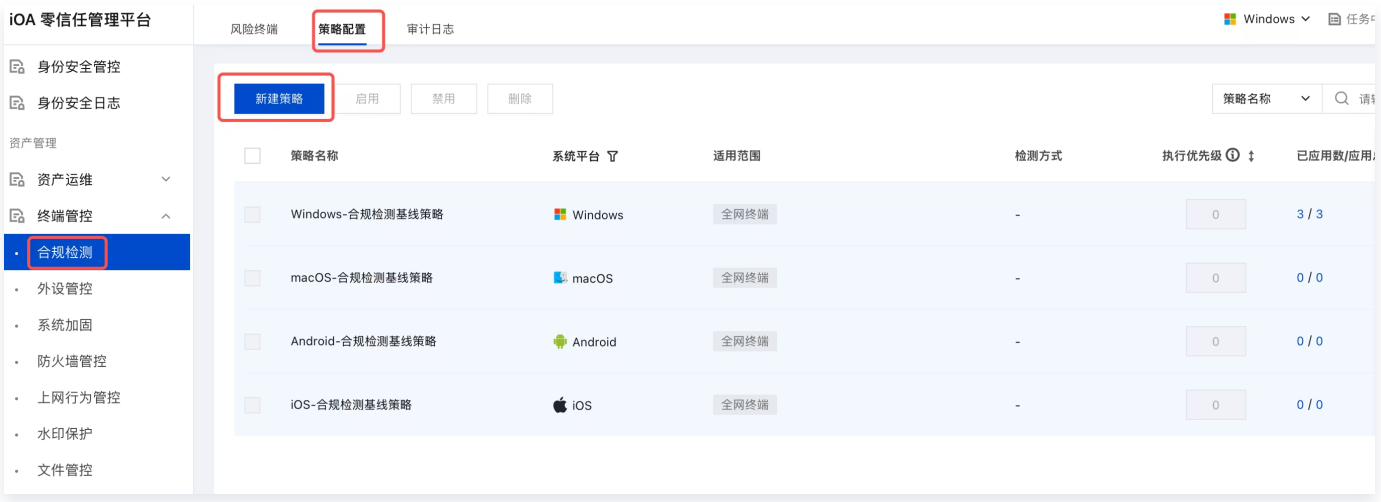
前提条件

1. iOA 客户端成功部署。
2. 完成账号创建以及认证源配置。
3. 完成业务资源的添加。
4. 完成对应用户和资源的授权。

测试示例

步骤1：配置合规策略，

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产管理** > **终端管控** > **合规检测**。
2. 在合规检测页面，选择**策略配置**，单击**新建策略**。



3. 在新建合规检测策略页面，配置相关参数，单击**保存**。

   3.1 基础信息：填写基础信息并启用该功能。

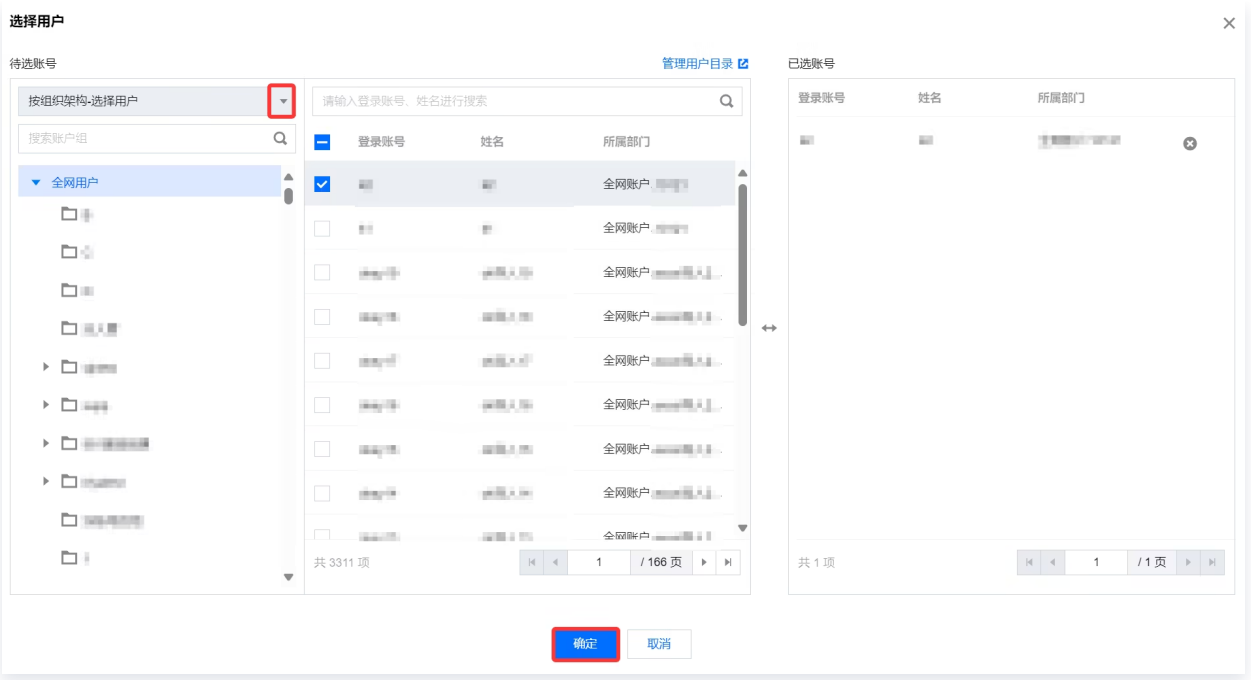


3.2 适用范围。

3.1.1 单击**添加适用范围 > 添加用户**。



3.1.2 在添加用户弹窗中，选择需管控的账号名，单击**确定**。

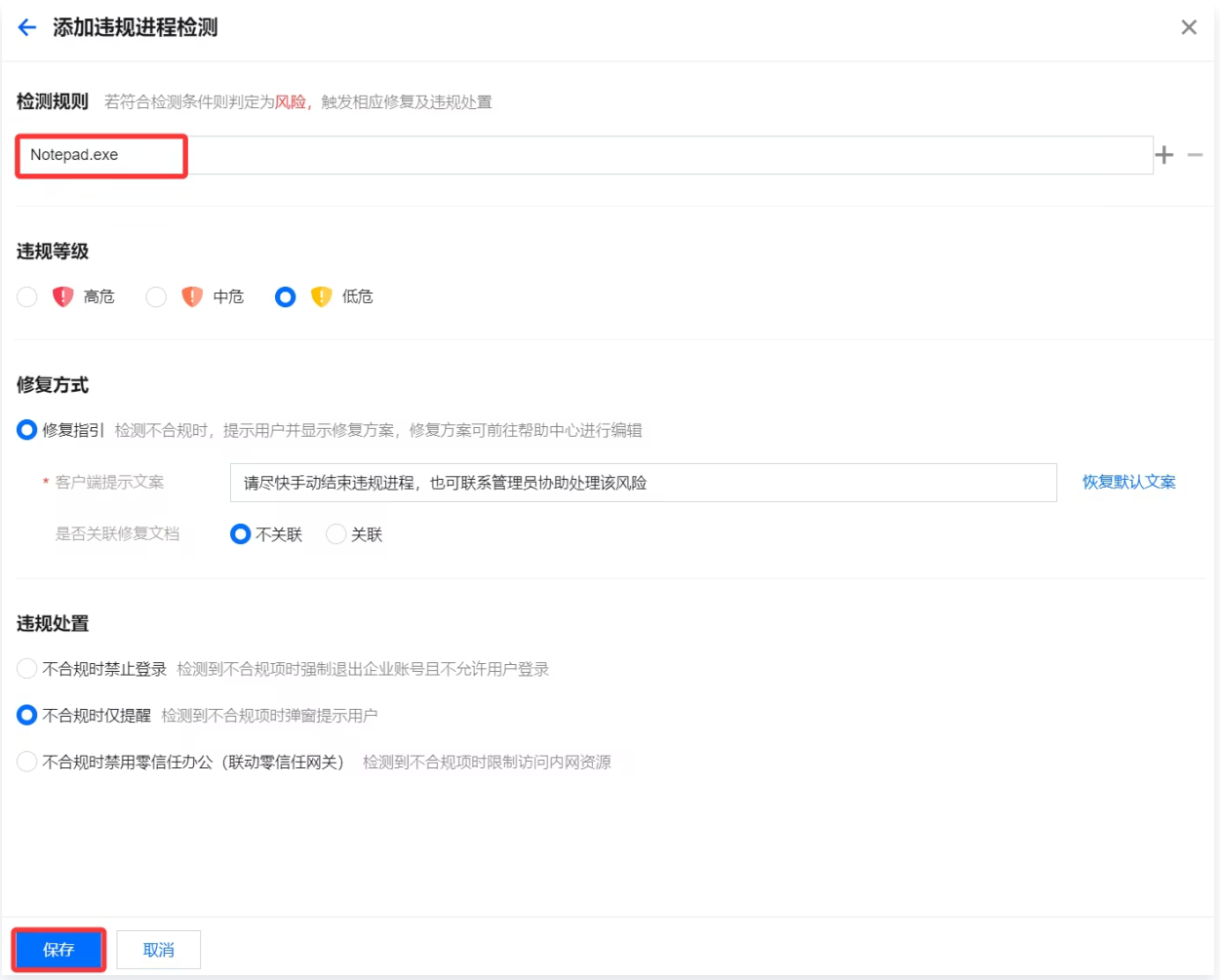


3.2 合规检测策略。

3.2.1 选择违规进程，单击 开启该功能，并单击**添加检测点**。



3.2.2 在添加违规进程检测项中，配置相关参数，此处以记事本（Notepad.exe）进程为例，配置完成单击**保存**。



步骤2：配置认证策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**身份安全管控** > **认证策略**。
2. 选择**目录名称**，单击**添加认证策略**。



3. 配置示例：设置 PC 端挑战认证方式认证源为 **iOA 本地账密**，单击**添加**。

编辑认证策略

基本信息 > 适用范围 > 配置认证安全策略

基本信息

* 策略名称 Test001-二次认证 12/144

策略描述 填写描述 0/288

策略执行优先级 自定义 − 2 + 数字越小越早执行,若数字已存在,指定数字之后的策略依次+1顺延

适用范围

适用对象	类型	操作
Test001	用户	删除

设定适用范围

配置认证安全策略

单个目录下的主认证方式由基础策略决定，如需调整主认证方式，请修改基础策略的主认证源选择

PC端

主认证方式的认证源

iOA本地账密

AD域环境免认证

双因素认证

是否启用

二次认证方式的认证源

扫码认证, 企微认证

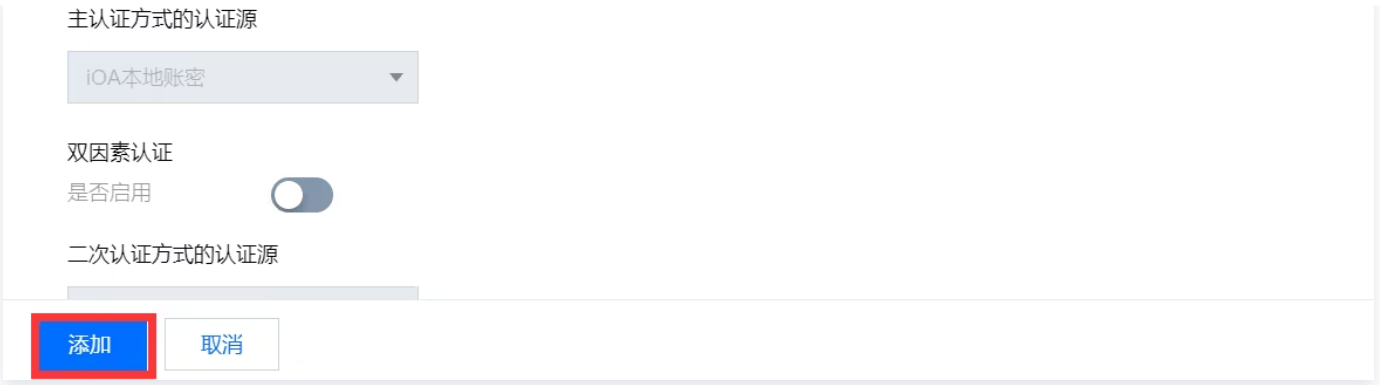
指定主认证登录豁免双因素

请选择

挑战认证方式认证源

iOA本地账密

移动端

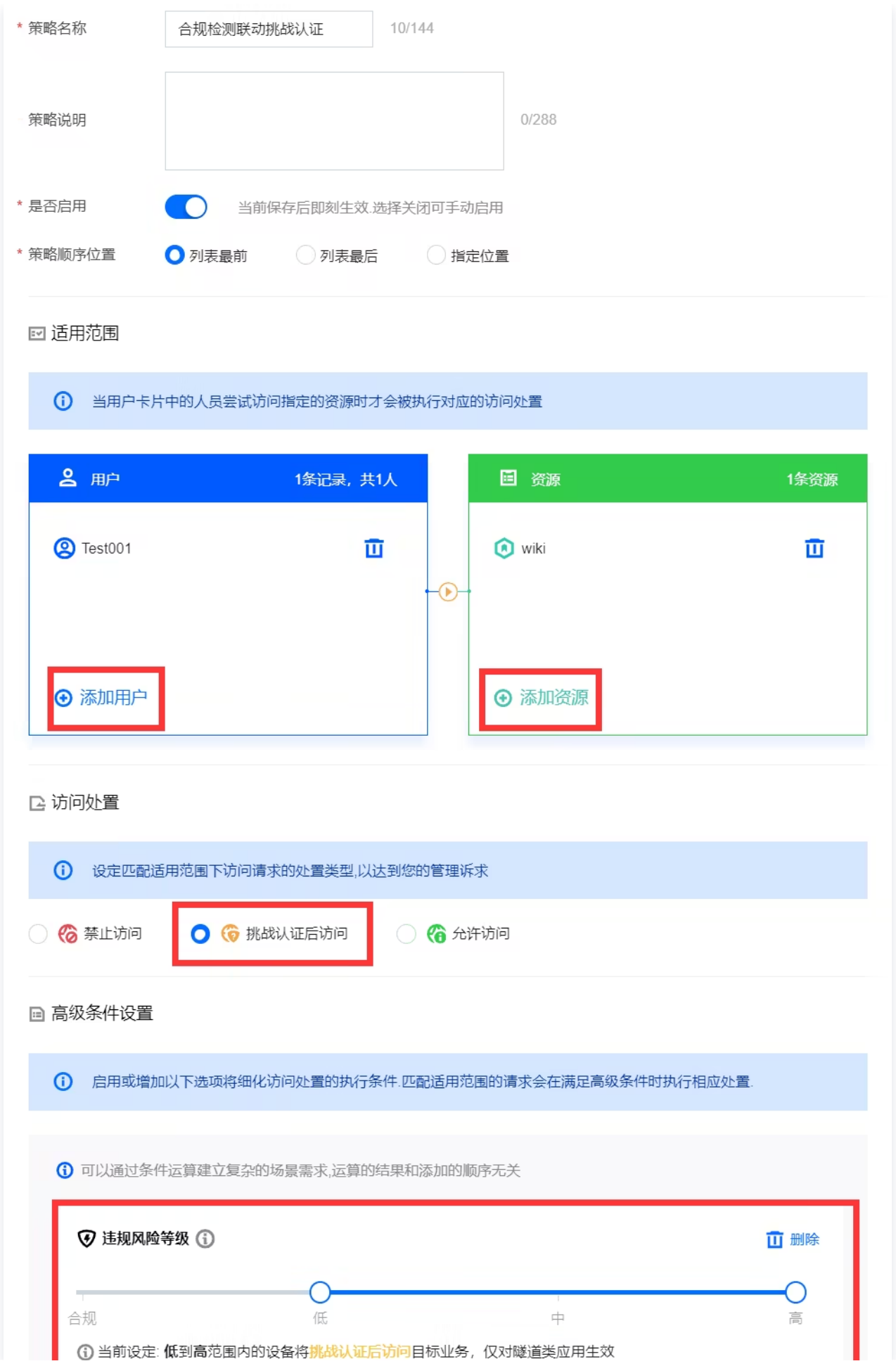


步骤3：配置访问安全策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**应用管理** > **访问策略**，单击**添加访问策略**。



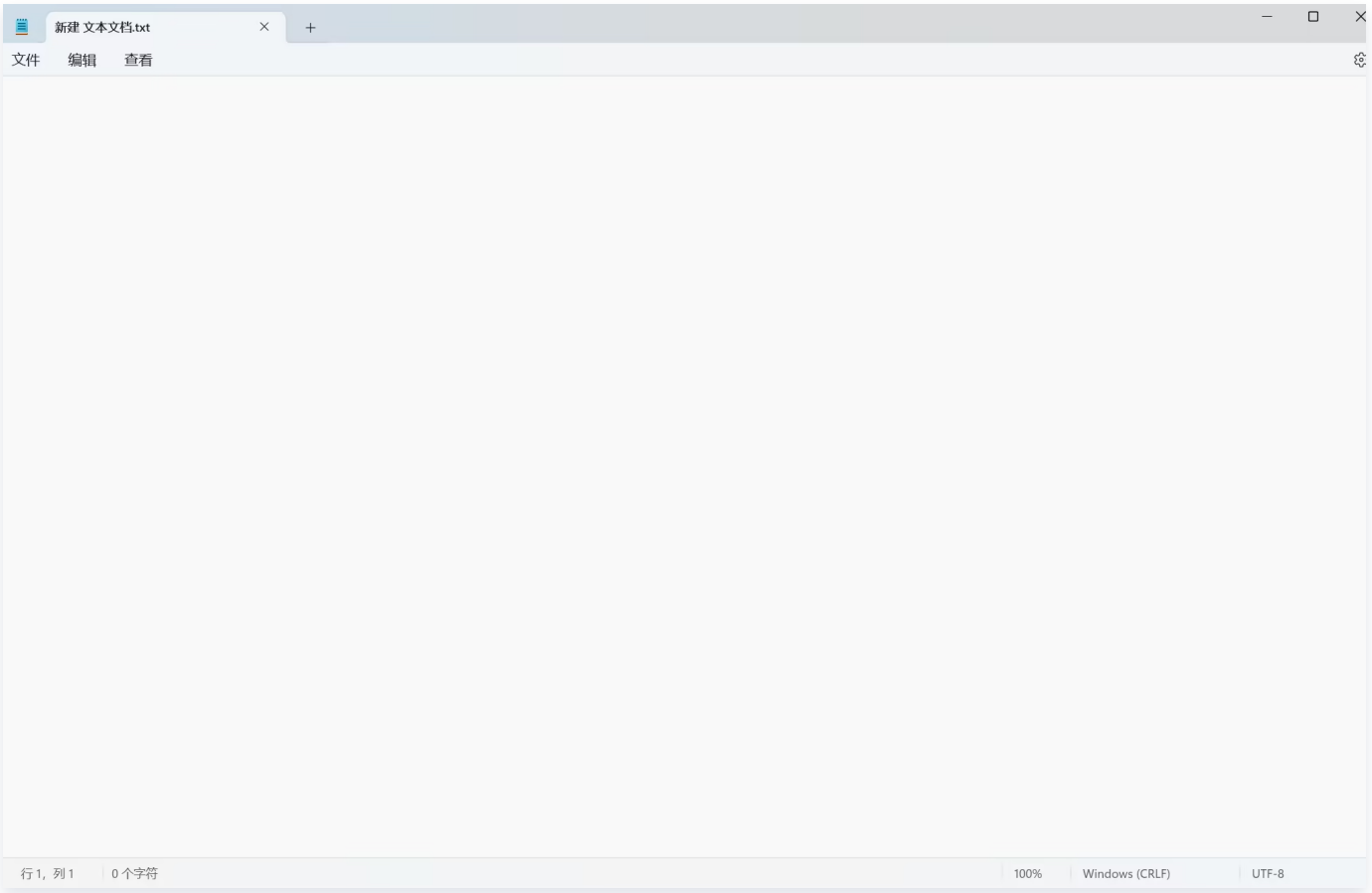
2. 在新建策略页面，配置相关参数，其中访问处置选择**挑战认证后访问**，设置**违规风险等级**，单击**保存**。


* 策略名称
合规检测联动挑战认证
10/144
策略说明
0/288
* 是否启用
当前保存后即刻生效.选择关闭可手动启用
* 策略顺序位置
列表最前
列表最后
指定位置
适用范围
当用户卡片中的人员尝试访问指定的资源时才会被执行对应的访问处置
用户
1条记录，共1人
Test001
添加用户
资源
1条资源
wiki
添加资源
访问处置
设定匹配适用范围下访问请求的处置类型,以达到您的管理诉求
禁止访问
挑战认证后访问
允许访问
高级条件设置
启用或增加以下选项将细化访问处置的执行条件.匹配适用范围的请求会在满足高级条件时执行相应处置.
可以通过条件运算建立复杂的场景需求,运算的结果和添加的顺序无关
违规风险等级
删除
合规
低
中
高
当前设定: 低到高范围内的设备将挑战认证后访问目标业务，仅对隧道类应用生效



步骤4：终端验证

1. 终端运行记事本，鼠标左键双击文本文档打开记事本。



2. 客户端合规检测提示不合规。



3. 终端不合规，访问指定**业务资源**需要二次认证。



4. 输入账号密码，二次认证通过后，访问成功；账号密码输入错误，访问失败。

版权所有：腾讯云计算（北京）有限责任公司

区分设备类型的访问隔离（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

测试目的

适用场景：终端通常根据公司组织架构进行分组，资源授权也是如此。

- 在执行特定项目的时候，可能需要从不同部门抽调员工组成一个新的项目组，需要对这些员工的终端进行管理和授权。
- 每个部门都拥有一些特殊设备，需要区别管理。

预期效果：

- A 账号在自定义分组的终端上访问特定资源，触发挑战认证。
- A 账号在其他终端上访问特定资源，未触发挑战认证。

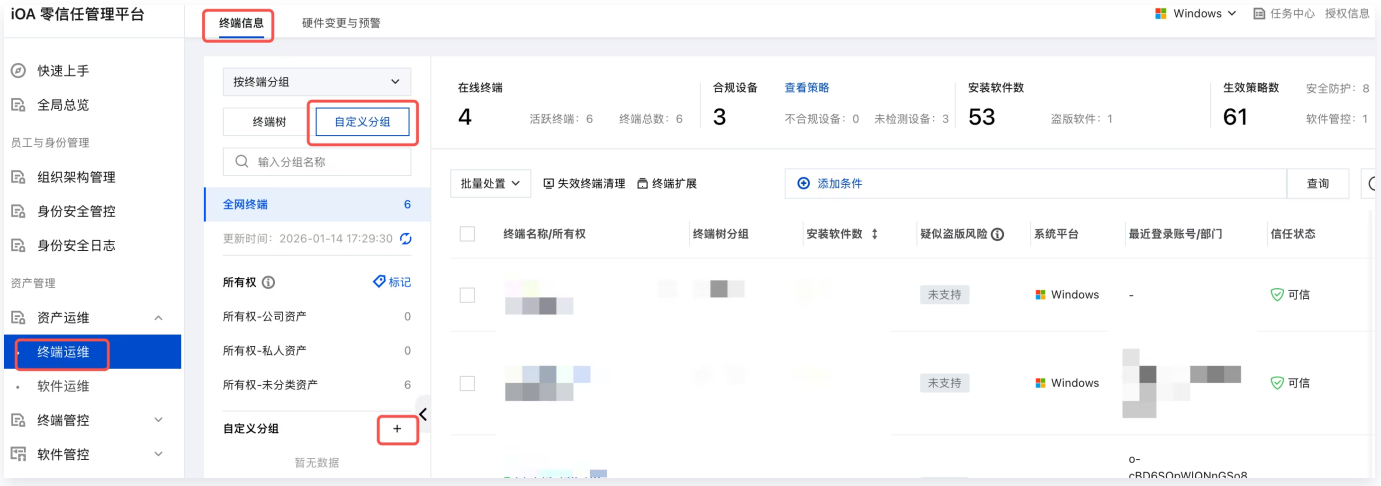
前提条件

1. iOA 客户端成功部署。
2. 完成账号创建以及认证源配置。
3. 完成业务资源的添加。
4. 完成对应用户和资源的授权。

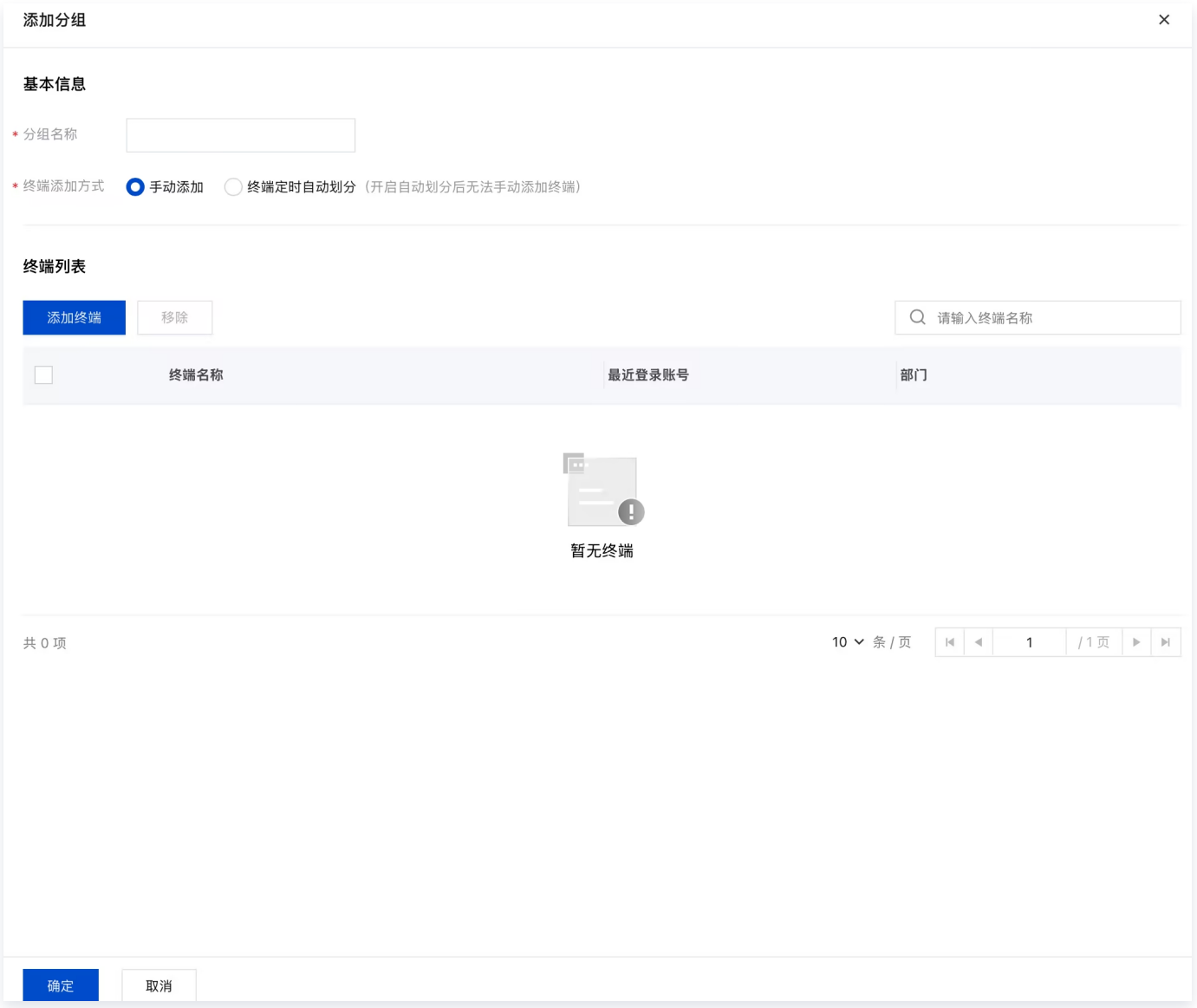
测试示例

步骤1：新建自定义分组

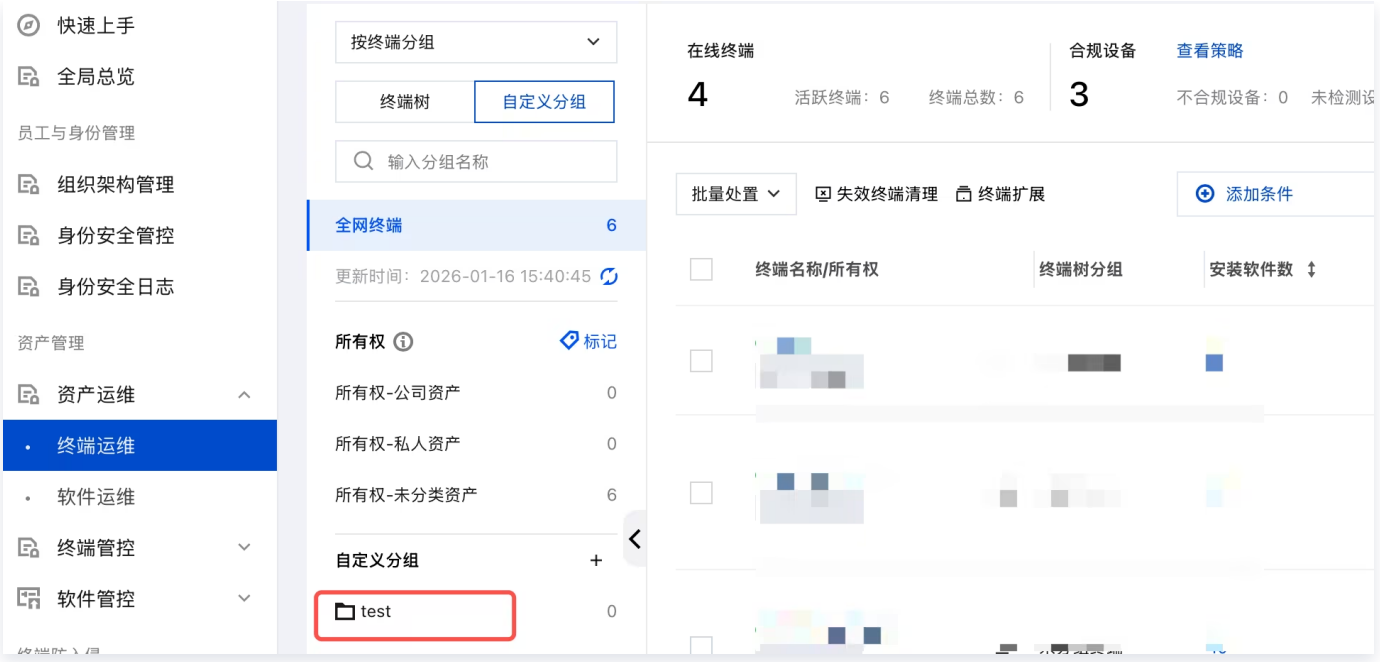
1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**资产管理** > **资产运维** > **终端运维**。
2. 在终端信息页面，选择**自定义分组**，单击 ＋ 添加自定义分组。



3. 在添加分组页面，输入**基本信息**并**添加终端**，单击**确定**。



4. 在自定义分组页面，可以看到刚刚创建的分组。



步骤2：配置认证策略

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**身份安全管控** > **认证策略**。
2. 在认证安全页面，选择**认证策略**，选择**目录名称**，单击**添加认证策略**。



3. 配置示例：设置 PC 端挑战认证方式认证源为 **iOA 本地账密**，单击**添加**。

编辑认证策略

基本信息 > 适用范围 > 配置认证安全策略

基本信息

* 策略名称 Test001-二次认证 12/144

策略描述 填写描述 0/288

策略执行优先级 自定义 − 2 + 数字越小越早执行,若数字已存在,指定数字之后的策略依次+1顺延

适用范围

适用对象	类型	操作
Test001	用户	删除

设定适用范围

配置认证安全策略

单个目录下的主认证方式由基础策略决定，如需调整主认证方式，请修改基础策略的主认证源选择

PC端

主认证方式的认证源

iOA本地账密

AD域环境免认证

双因素认证

是否启用

二次认证方式的认证源

扫码认证, 企微认证

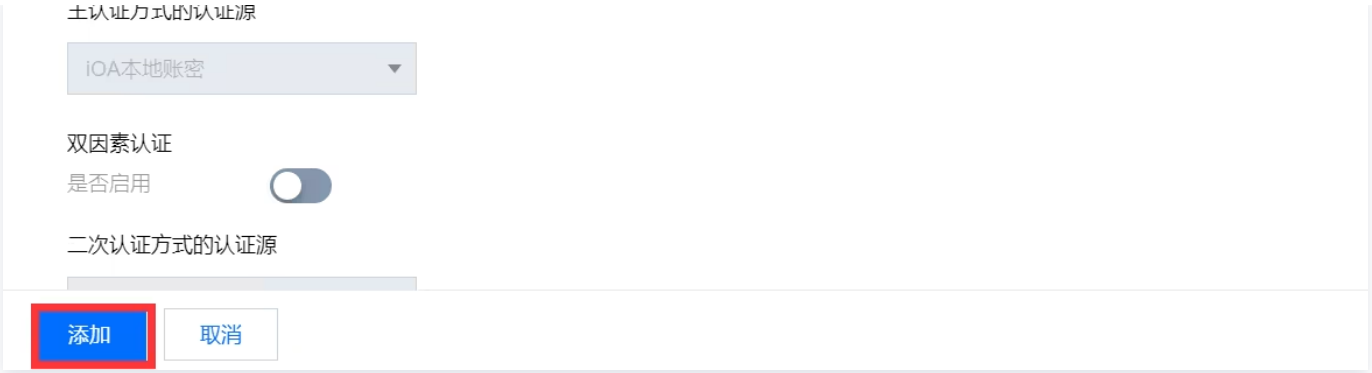
指定主认证登录豁免双因素

请选择

挑战认证方式认证源

iOA本地账密

移动端



步骤3：配置访问安全策略

1. 登录 iOA 零信任管理平台控制台，选择**应用管理** > **访问策略**，单击**添加访问策略**。

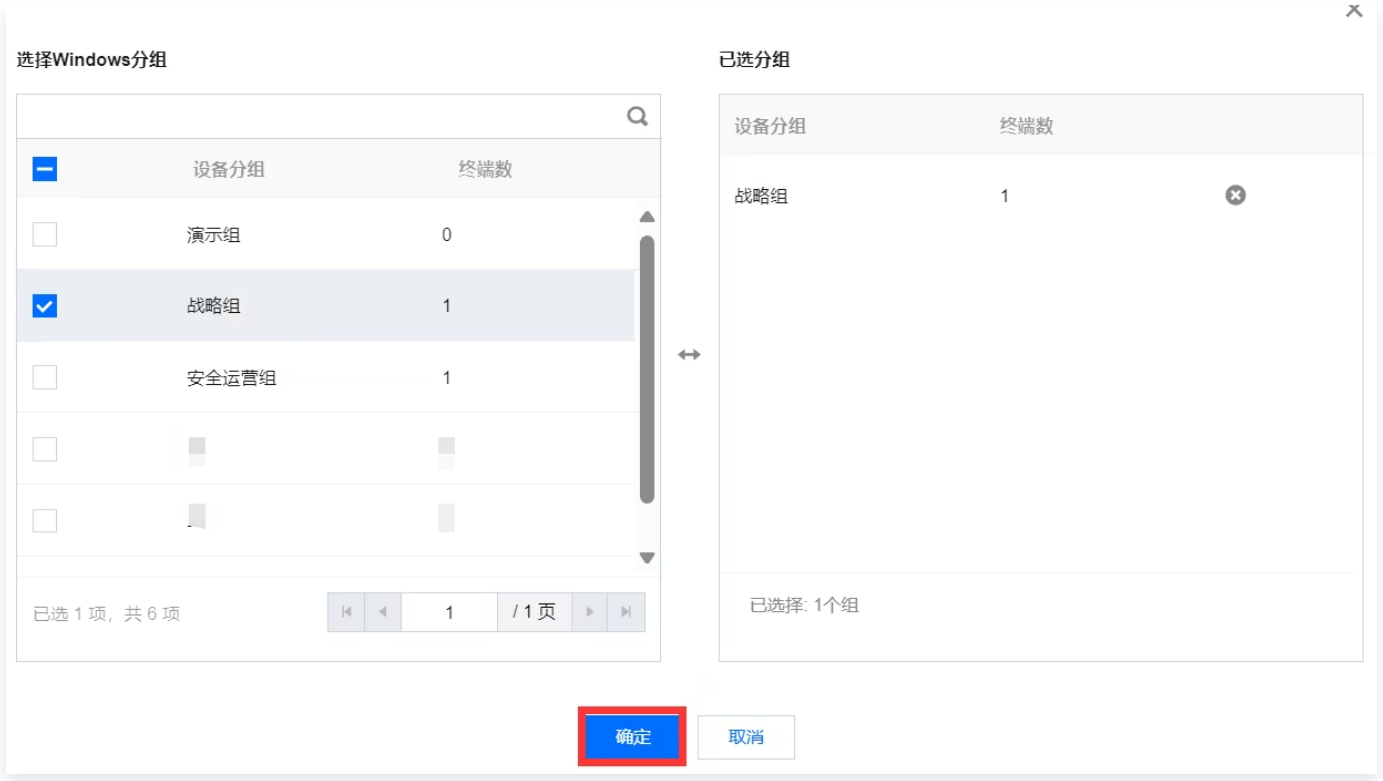


2. 在新建策略页面，配置相关参数，其中访问处置选择**挑战认证后访问**，选择**设备范围**，单击**添加该条件**。


* 策略名称
区分设备类型的访问隔离
11/144
策略说明
0/288
* 是否启用
当前保存后即刻生效,选择关闭可手动启用
* 策略顺序位置
列表最前
列表最后
指定位置
适用范围
当用户卡片中的人员尝试访问指定的资源时才会被执行对应的访问处置
用户
1条记录，共1人
Test001
添加用户
资源
1条资源
wiki
添加资源
访问处置
设定匹配适用范围下访问请求的处置类型,以达到您的管理诉求
禁止访问
挑战认证后访问
允许访问
高级条件设置
启用或增加以下选项将细化访问处置的执行条件.匹配适用范围的请求会在满足高级条件时执行相应处置.
可以通过条件运算建立复杂的场景需求,运算的结果和添加的顺序无关
设备范围
删除
战略组



3. 勾选 步骤1 中创建的自定义分组，单击**确定** > **保存**。



步骤4：终端验证

1. 在自定义分组-战略组内的终端上登录 A 账号，访问特定资源触发挑战认证，认证成功后通过。
2. A 账号在其他终端上访问特定资源，未触发挑战认证，访问成功。

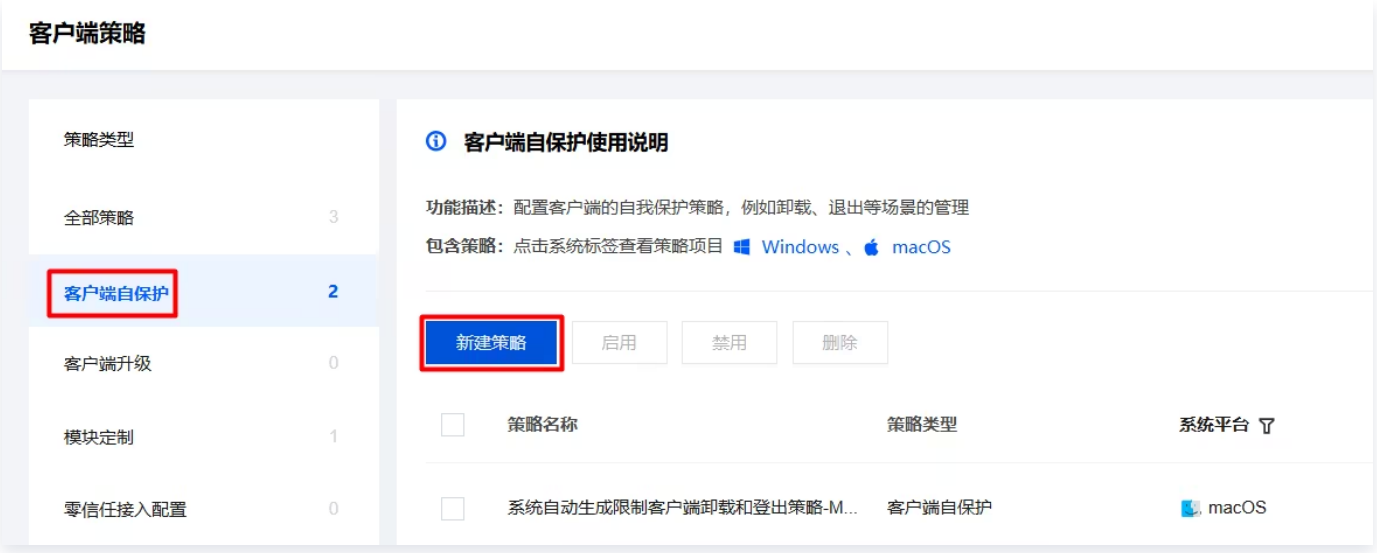
客户端运维（11.1.1版）
客户端管理（11.1.1版）
客户端策略（11.1.1版）
客户端自保护（11.1.1版）

最近更新时间：2026-02-06 14:23:32

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

配置客户端的自保护策略，防止客户端软件被恶意卸载或关闭，例如卸载、退出等场景的管理，从而确保安全防护功能的持续运行。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端运维** > **客户端管理** > 客户端策略 。
2. 在客户端管理页面，选择 客户端自保护 ，单击**新建策略**。



3. 在新建客户端自保护策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。



3.2 单击**添加适用范围**，勾选需管控/排除的终端名称，单击**确定**。

4. 根据实际需求，选择如下**客户端自保护策略**。

允许客户端卸载

设置为卸载客户端需要密码。

1. 勾选**允许客户端卸载**，单击 开启允许客户端卸载，

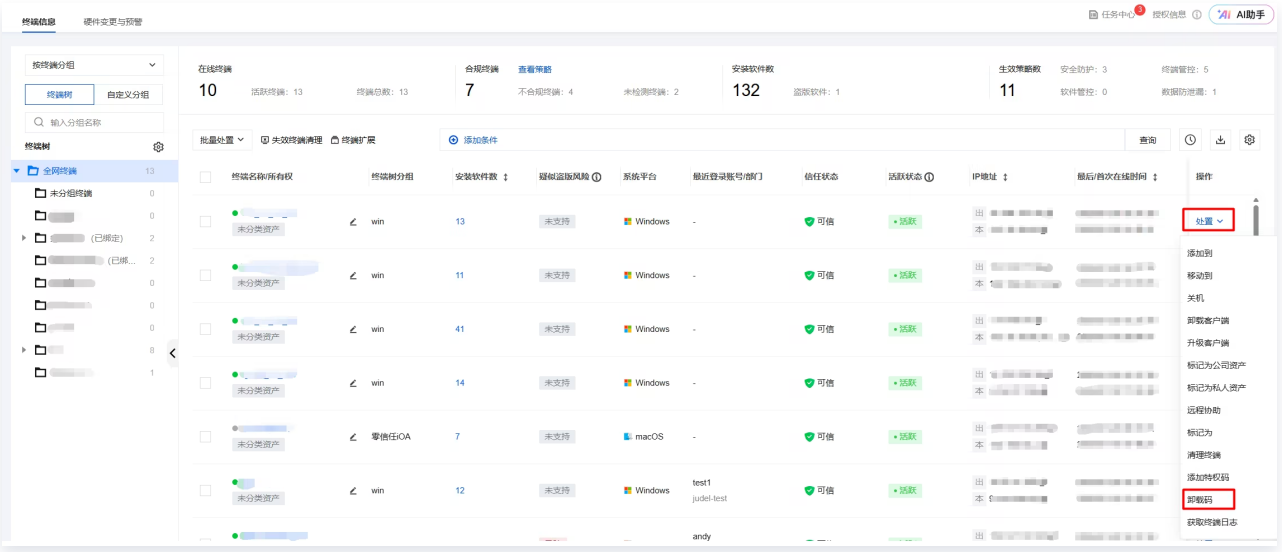


2. 选择**卸载客户端无需密码**或**卸载客户端需要密码**，配置完成单击**保存**。



3. 前往**资产运维** > **终端运维** > 终端信息，选择目标计算机，单击**处置**，获得**卸载码**。

> **说明：**
> 卸载码仅对该设备当天有效。



4. 在客户端卸载界面输入卸载码，单击**确定**完成卸载。



允许退出客户端

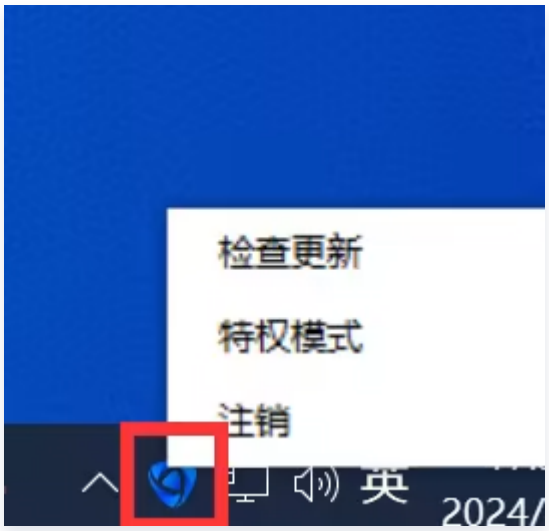
1. 勾选**允许退出客户端**，选择**允许**或**不允许**。



2. 配置完成单击**保存**。



- 允许：右击桌面任务栏的 iOA 图标，用户的终端可以退出客户端。
- 不允许：右击桌面任务栏的 iOA 图标，无退出选项，iOA 客户端无法退出。



允许手动注销客户端

1. 勾选**允许手动注销客户端**，选择**允许**或**不允许**。



2. 配置完成单击**保存**。

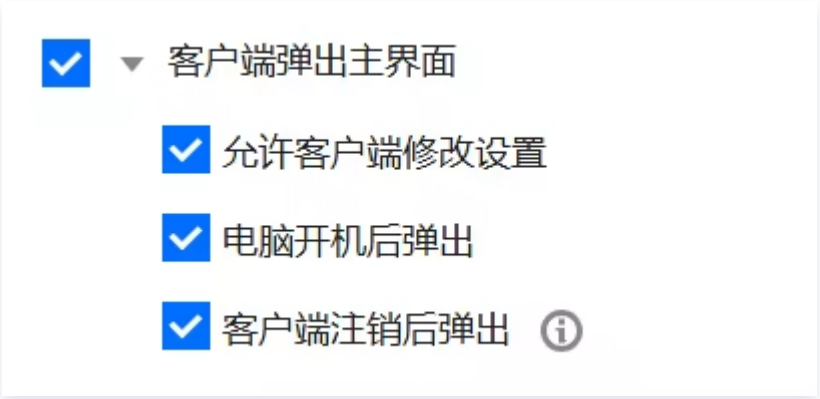


- 不允许：右击桌面任务栏的 iOA 图标，用户的客户端不展示注销，不支持注销账号。
- 允许：右击桌面任务栏的 iOA 图标，用户的客户端显示注销，支持注销账号。



客户端弹出主界面

勾选**客户端弹出主界面**，配置允许客户端修改设置/电脑开机后弹出/客户端注销后弹出策略，配置完成单击**保存**。



- 勾选允许客户端修改设置：前往**客户端设置** > **常规设置**，客户端支持修改主界面配置，支持设置为终端开机后弹出和客户端注销后弹出。



- 电脑开机后弹出：
  - 勾选时，电脑开机后自启 iOA 时，弹出主界面。
  - 未勾选，开机自启 iOA 时主界面不弹出。
- 客户端注销后弹出：
  - 勾选时，选择注销登录，注销的同时，iOA 客户端 UI 主界面展示，注销后弹出主界面。



- 未勾选：客户端注销后 iOA 客户端 UI 主界面不展示，注销后不弹出主界面。



允许第三方产品升级及卸载客户端

说明：

此策略与 允许客户端卸载 策略互不影响，各自独立运行。

- 升级或卸载时退出第三方产品，会导致执行失败。
- 升级和卸载均为静默执行。

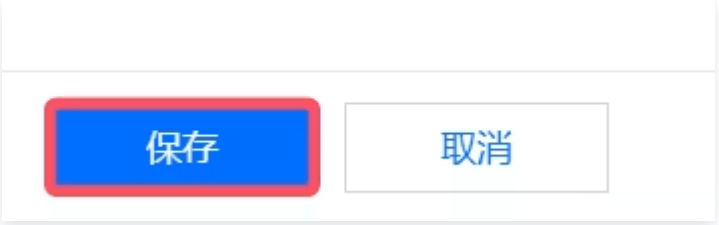
1. 勾选**允许第三方产品升级及卸载客户端**，单击 开启允许第三方产品升级及卸载。



2. 配置校验签名及签名名称后执行。



3. 配置完成单击**保存**。



开机时自动运行客户端

勾选开机时自动运行客户端，

- **允许：开机时自动运行客户端，以便第一时间保护员工电脑。**

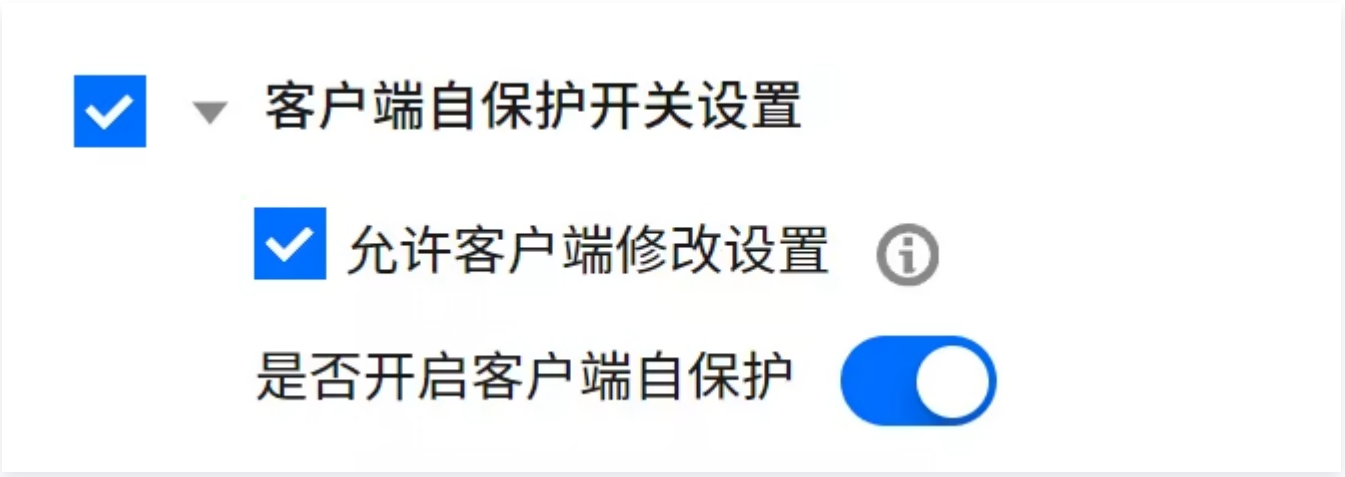
- 不允许：开机后客户端无法自动运行。



客户端自保护开关设置

> **说明：**
> - 该功能支持保护客户端软件不受破坏，例如：会自动禁止改写 iOA 客户端安装目录下的文件、以及一些其余的配置文件等。
> - 正常情况下，禁止关闭客户端自保护开关。
> - **建议仅问题调试时关闭客户端自保护开关。**

1. 勾选**客户端自保护开关设置**，单击 开启客户端自保护。



2. 勾选允许客户端修改设置，勾选后，自保护设置以客户端设置为准。
3. 在客户端页面，单击右上角**设置**。



4. 在常规设置页面，客户端支持修改设置为开启自保护/临时关闭自保护。



允许客户端进入特权模式

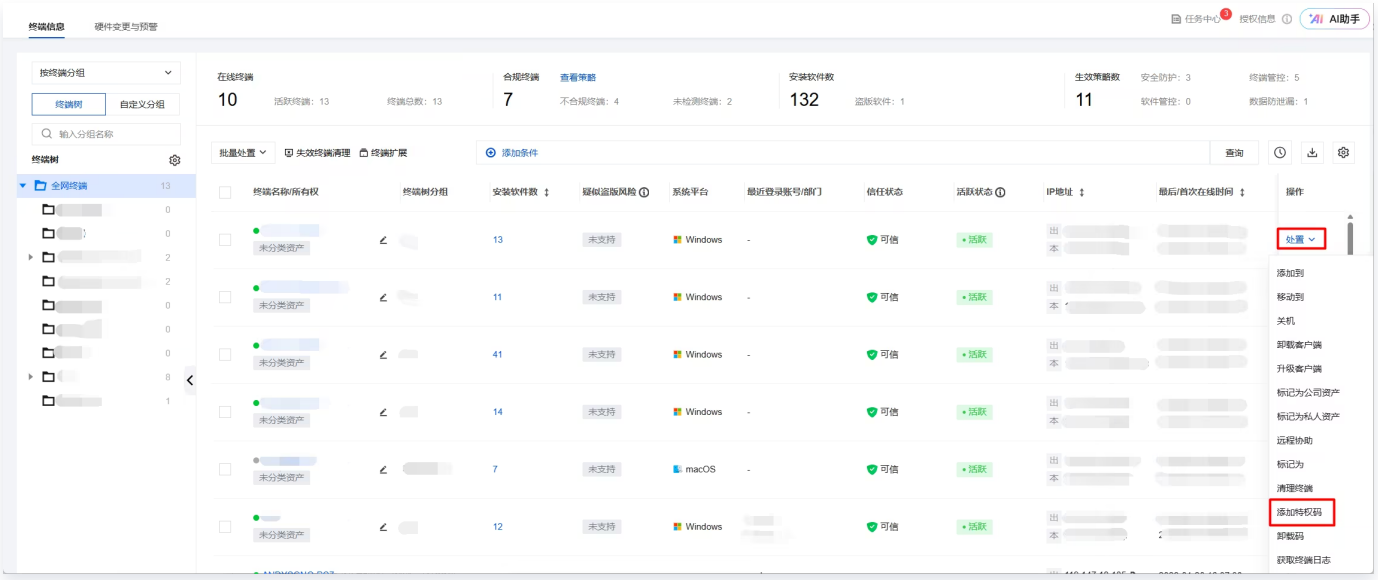
> ⚠ **注意：**

进入特权模式将会完全屏蔽所有安全、管控及准入策略以模拟卸载后的环境进行排障，此模式存在很大的风险和隐患，请谨慎使用。

1. 勾选**允许客户端进入特权模式**，选择允许并设置时间段。



2. 前往**资产运维 > 终端运维 > 终端信息**，选择目标计算机，单击**处置 > 添加特权码**，获得**特权码**。



3. 在客户端页面。单击右上角**设置 > 特权模式**。



4. 提示输入终端特权码，将生成的特权码填写到此处。



禁止客户端相关弹窗

勾选**禁止客户端相关弹窗**，禁止客户端相关弹窗后，包括病毒查杀、漏洞修复、终端提示、高危信息等弹窗将不会弹出，**无法及时通知风险，请谨慎使用**。



客户端重启

勾选**客户端重启**和**客户端定时重启**，设置时间段，单击**保存**。

- 仅在需要重启的终端执行重启策略：勾选后，仅在终端有需要重启后清除的病毒或重启后生效的补丁时，会进行重启。反之则不会进行重启。
- 重启前提醒：
  - 勾选：会弹出 tips，让用户选择。
  - 不勾选，直接重启。
- 超时后默认不执行：结合重启前提醒，tips 弹出后，倒计时结束视为超时。
  - 勾选：超时就不重启了
  - 不勾选，超时后直接强制重启。重启 x 分钟前提示 y 信息：x 分钟即为 tips 的倒计时时间；y 信息可默认可编辑。

版权所有：腾讯云计算（北京）有限责任公司



- 配置客户端重启策略后，到达所设置的重启时间，iOA 弹出重启提示。



远程协助设置

稳定连接终端，帮助 IT 运维人员高效管理分散在各地的设备，实现远程协助，更多详情请参见 远程协助 。

客户端升级（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端管理 > 客户端策略**。
2. 在客户端管理页面，选择**客户端升级**，单击**新建策略**。



3. 在新建客户端升级策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。

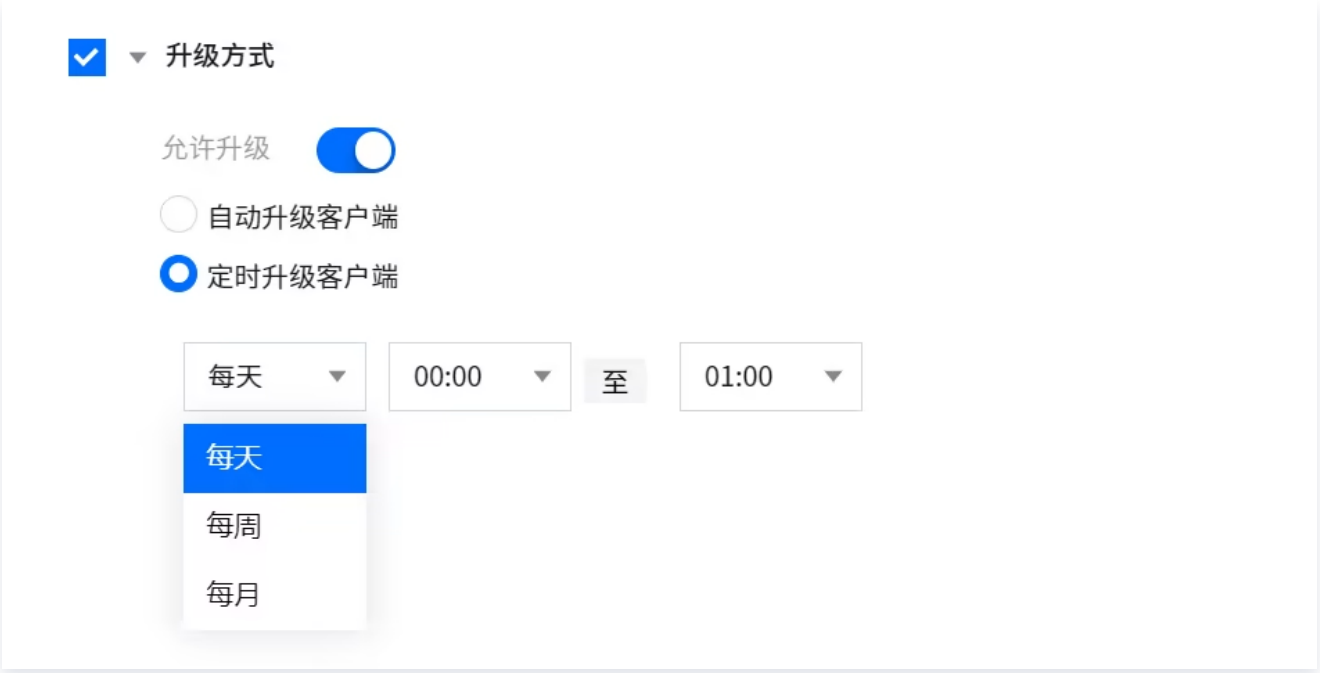


3.2 单击**添加适用范围**，勾选需管控/排除的终端名称，单击**确定**。

4. 升级方式。

4.1 自动升级客户端：当 iOA客户端有新版本更新时，自动升级客户端版本。

4.2 定时升级客户端：自定义每天/周/月的时间，当存在新版本时，根据定时升级时间，自动升级。



5. 配置完成单击**保存**。



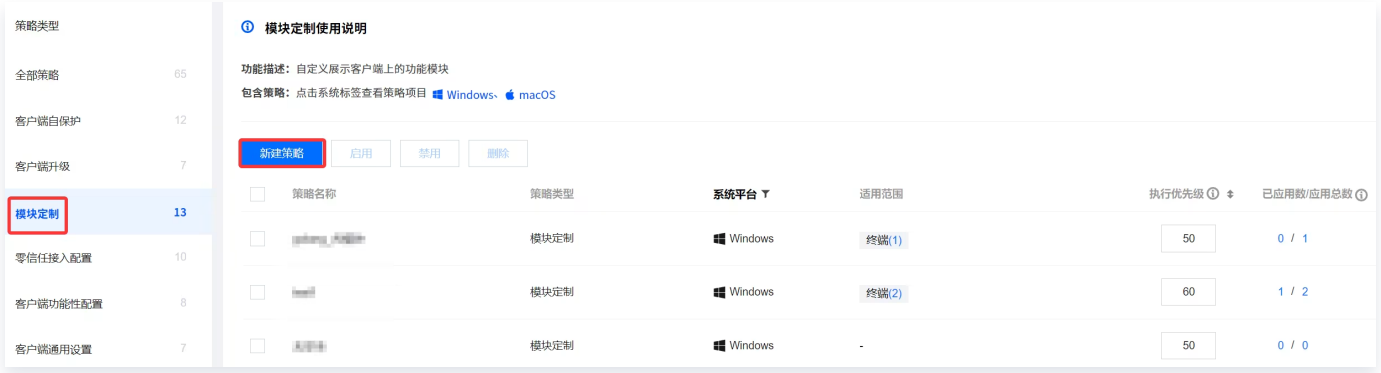
版权所有：腾讯云计算（北京）有限责任公司

模块定制（11.1.1版）

最近更新时间：2026-02-13 09:41:03

说明：
iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端管理 > 客户端策略**。
2. 在客户端策略页面，选择 **模块定制**，单击**新建策略**。



3. 在新建模块定制策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。

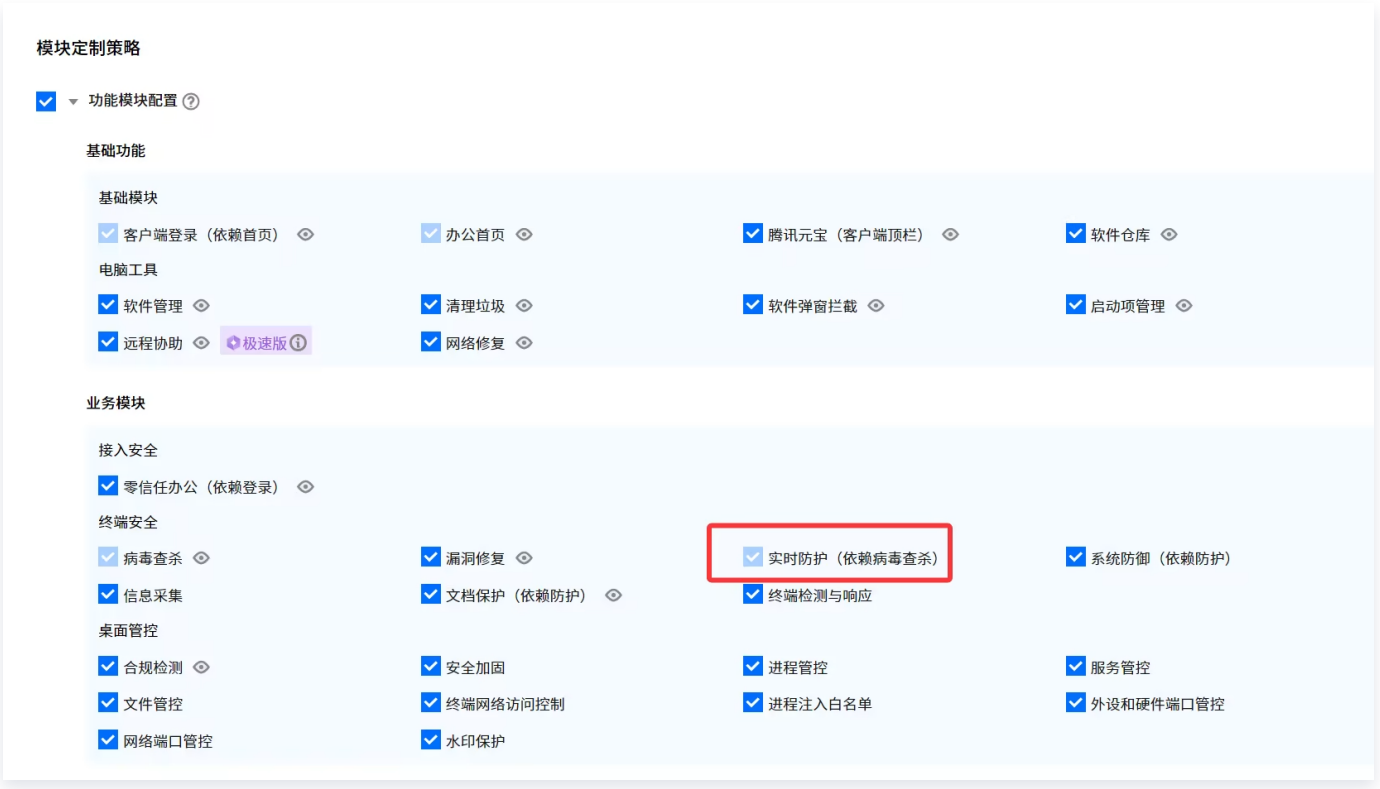


3.2 单击**添加适用范围**，勾选需管控/排除的终端名称，单击**确定**。

4. 根据实际需求，选择如下**模块定制策略**。

功能模块配置

1. 勾选**功能模块配置**，勾选需在客户端展示的基础功能/业务模块名称，单击**保存**。



重点功能模块名称	说明
实时防护（依赖病毒查杀）	• iOA 支持远控行为识别功能，对远程操控行为实时弹窗提示预警，有效提升防护体验。 • 威胁情报识别能力升级，iOA 基础版支持 IOC 实时查询，覆盖 URL、IP、域名等关键信息；网络访问时进行 IOC 查询，对恶意目标实时阻断，实现事前拦截，提升防护效率。 • 勾选实时防护开关，即可启用此功能。 **说明：** 远控行为识别功能与威胁情报识别能力要求客户端版本10.11.1及以上支持该功能，如客户端版本低于10.11.1请升级客户端版本。
病毒查杀	• iOA 支持进程内YARA规则扫描，针对银狐内存特征进行扫描，增强银狐检测能力；主动快速查杀与全盘查杀场景自动调用内存特征扫描逻辑，扩大检测范围，提升查杀效率。 • 勾选病毒查杀功能，即可启用此功能。 **说明：** 进程内YARA规则扫描能力要求客户端版本10.11.1及以上支持该功能，如客户端版本低于10.11.1请升级客户端版。

说明：

- 不允许勾选的功能模块表示您未获得该模块的授权。
- 未勾选的功能模块，客户端不会运行该功能，不会显示功能界面。
- 为保证客户端正常运行，请至少开启一个有功能界面显示（含有图标）的功能模块。
- 更新授权且新增功能模块时，为保证客户端兼容性与稳定性，需手动开启新功能模块，建议您按照灰度教程进行灰度验证逐步开启，若灰度过程中遇到任何问题，请 联系我们 获得支持。

2. 勾选各模块后，客户端展示配置的基础功能/业务模块。



3. iOA 客户端内置腾讯元宝，您可配置客户端顶栏是否显示腾讯元宝，示例：勾选腾讯元宝。

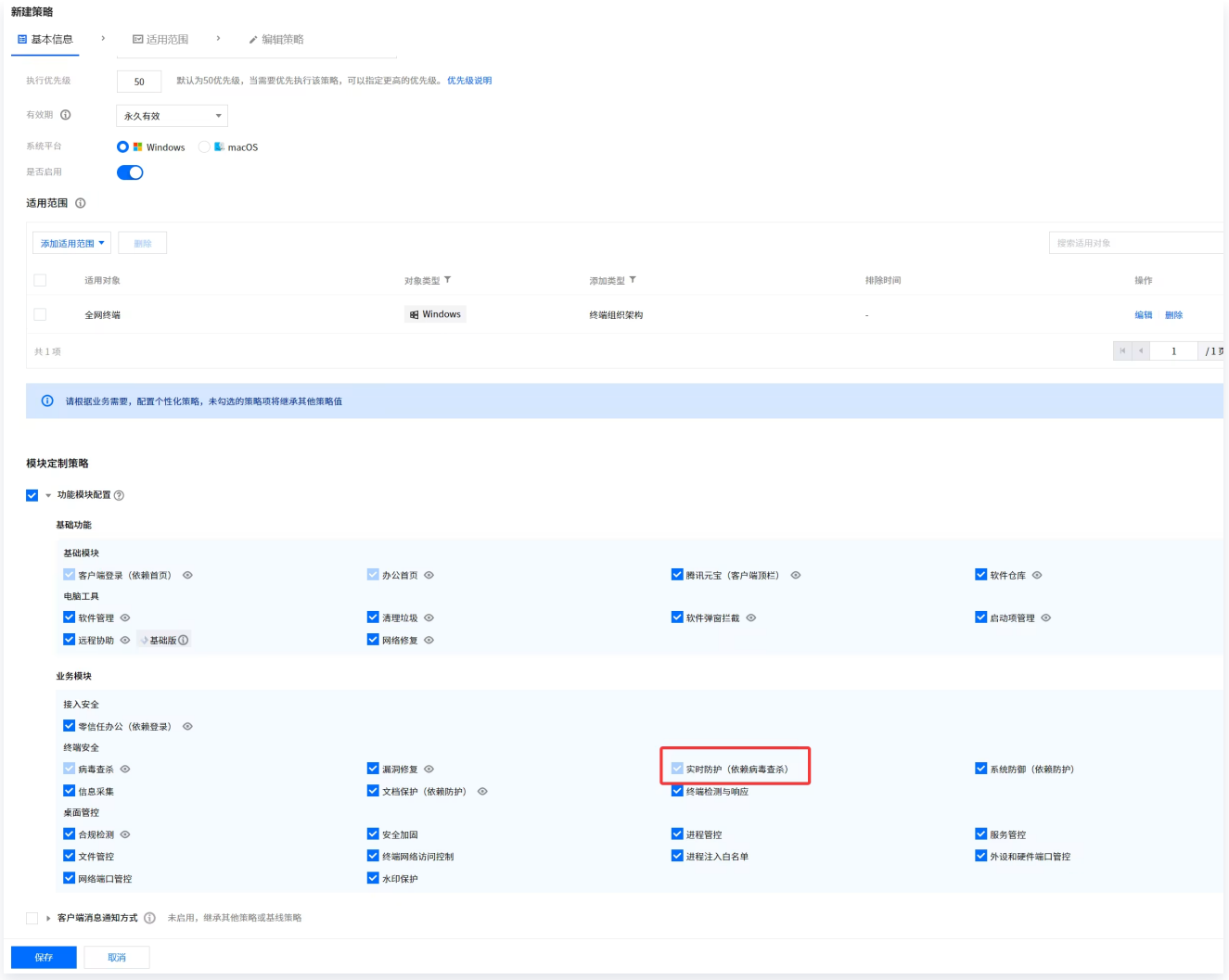


4. 勾选后，单击**客户端顶栏**入口可唤起腾讯元宝，助力办公效率提升。



5. 实时防护（IOC 实时查询联动腾讯威胁情报中心）配置示例：

5.1 管理员在**客户端管理** > **客户端策略** > 模块定制 中开启实时防护开关。



5.2 用户访问恶意 IP、域名，IOC 联动腾讯威胁情报中心，阻断访问，触发告警。



5.3 管理员前往**终端防入侵 > 高级威胁防护 > 威胁告警 > 按告警查看**，单击**告警名称**，查看相关告警。



5.4 管理员前往**终端防入侵 > 实时防护 > 审计日志**查看**实时防护日志**。



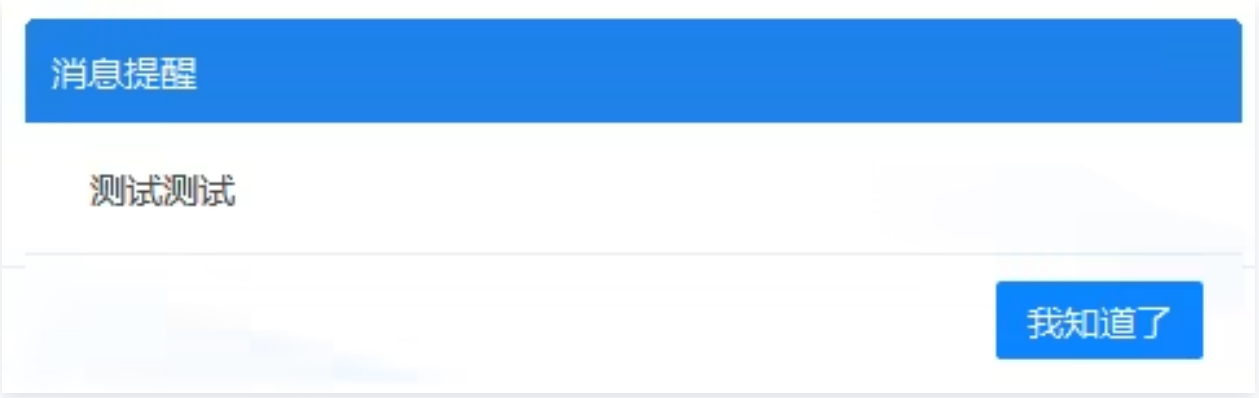
客户端消息通知方式

给指定的终端下发一个页面右下角弹窗的通知。

1. 勾选**客户端消息通知方式**，单击 **开启客户端提醒**，选择弹窗模式，单击**保存**。



2. 通知样式如下图，“ 测试测试”为可编辑的自定义弹窗提示内容。



零信任接入配置（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台 ，在左侧导航栏，选择**客户端管理** > 客户端策略 。
2. 在客户端管理页面，选择**零信任接入设置**，单击**新建策略**。



3. 在新建零信任接入配置策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。

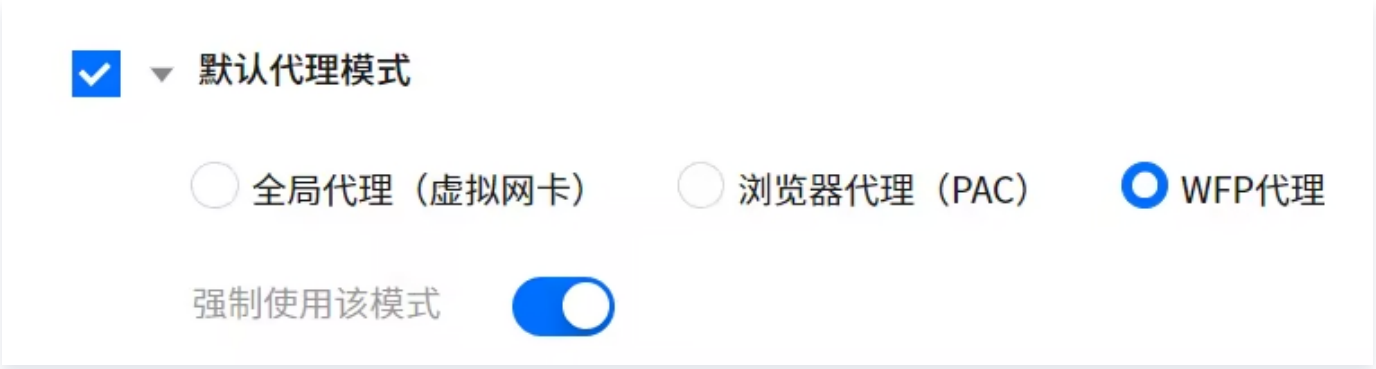


3.2 单击**添加适用范围**，勾选需管控/排除的终端名称，单击**确定**。

4. 根据实际需求，选择如下**零信任接入配置策略**，单击**保存**

默认代理模式

1. 勾选**默认代理模式**，选择所需模式，单击**保存**。



- 全局代理（虚拟网卡）：本地会启动一个虚拟网卡，所有流量都经过虚拟网卡。
- 浏览器代理（PAC）：本地会启动一个代理服务，然后设置一个 PAC链接系统支持 PAC的链接到系统，会用本地服务做代理，仅支持 http相关的代理。
- WFP 代理：WFP是 Windows支持的模式，跟全局代理类似，就是通过wfp的技术将流量引入到本地的一个代理服务。
- 开启强制使用该模式：配置为强制使用该模式，客户端代理模式切换选项不可点击。（置灰）

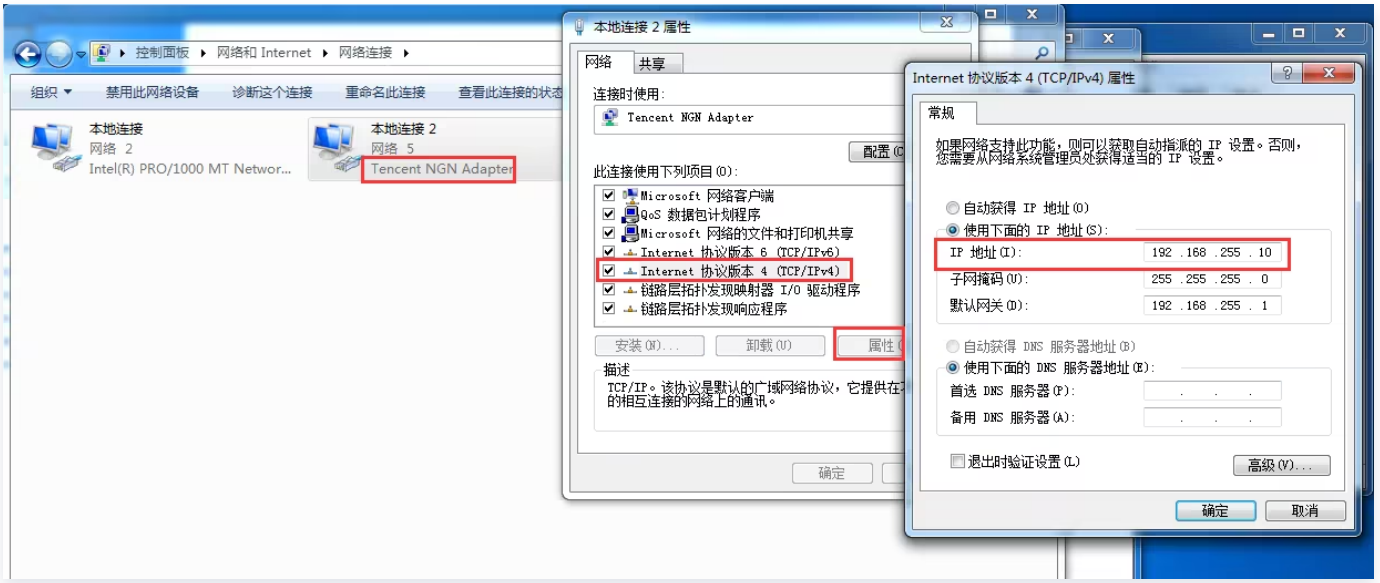


虚拟网卡 IP 配置

勾选虚拟网卡 IP 配置，选择所需模式，单击保存。

- iOA 系统预置 IP：客户端登录 iOA ，smartvpn.exe 进程启动后，虚拟网卡安装完成，打开网络和共享中心，查看 NGN 网卡属性。
- 自定义 IP：填入正确的 IP 地址，重新登录客户端，打开网络和共享中心，查看 NGN 网卡属性，IP 变成自定义的地址。

> **说明：**
> 虚拟网卡 IP 请配置 `192.168.255.2~192.168.255.254` 的网段，**请勿配置公司 IP 以及环回 IP 、广播 IP 此类特殊 IP，否则会导致服务失败。**



DNS 时间间隔

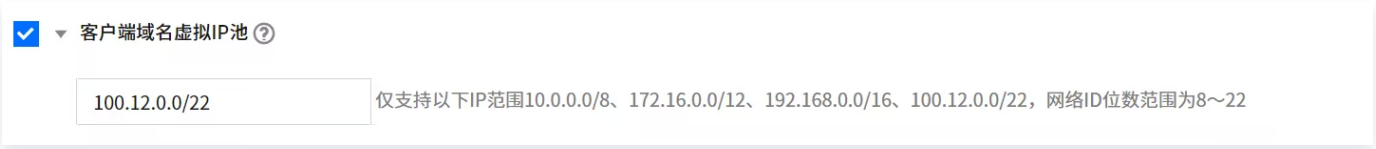
勾选 **DNS 时间间隔**，修改时间，单击**保存**。

> **说明：**
> - 可手动设置 DNS间隔时间，默认值2秒。
> - 此设置用于发生 DNS 服务器故障时修改，减少域名解析的异常重试频次。
> - 正常情况下不建议修改。



客户端域名虚拟 IP 池

1. 客户添加的内网业务资源是域名的情况下，需要做 DNS 域名解析，由于客户端是在外网，解析不出来或者解析到公网域名。因此，需要 iOA 提供解析的虚拟 IP 用来建立 NGN 访问连接。100.12.0.0/22是默认的虚拟IP网段，但使用该网段用谷歌浏览器访问一些 HTTP+HTTPS 混用的业务时，会出现提示跨域的问题。因此，网段允许的情况下，优先使用10.0.0.0/8、172.16.0.0/12、192.168.0.0/16。
2. 勾选**客户端域名虚拟 IP 池**，设置 IP 地址，单击**保存**。



HTTPS 通道复用

默认开启，增加建立连接及传输性能，降低服务器及客户端负载。



域流量拦截配置

默认关闭，开启后，客户端登录前就会启动 NGN。

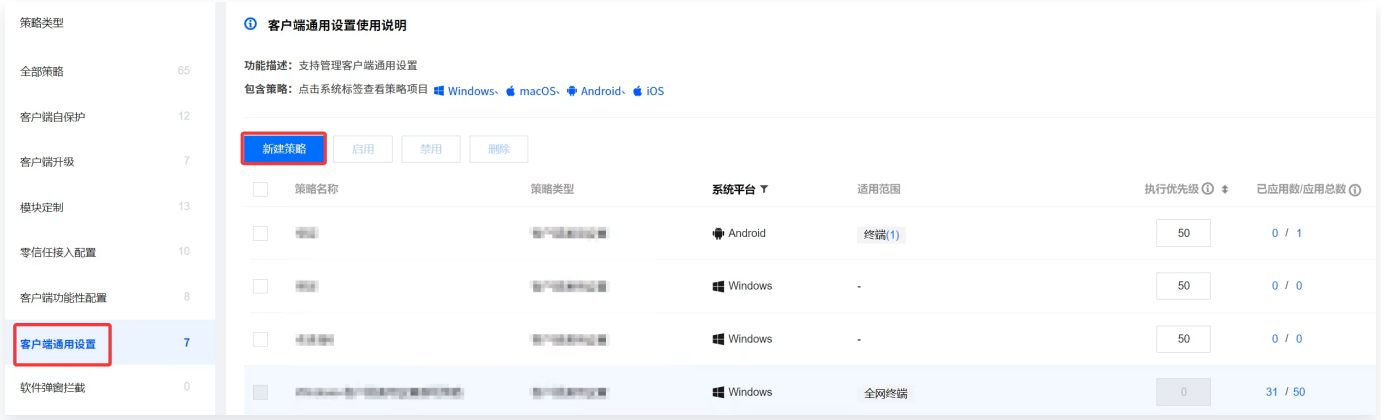


客户端通用设置（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端管理** > 客户端策略 。
2. 在客户端策略页面，选择**客户端通用设置**，单击**新建策略**。



3. 在新建客户端通用设置策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。



3.2 单击**添加适用范围**，勾选需管控/排除的终端名称，单击**确定**。

4. 根据实际需求，选择如下**客户端通用设置策略**，单击**保存**。

设备绑定策略

注意事项

- 通过配置账号与设备绑定，管理客户端登录方式。
- 账号与设备绑定开关默认关闭。
- 关闭（不允许设备被账号绑定）终端可以登录任意账号。
- 开启（允许设备被账号绑定）：选择开启，初次登录设备的客户端即自动绑定登录账号，其他账号无法在该设备上登录，实现设备与账号双向绑定管理，当注销后换账号登录时，会提示账号与设备绑定。

配置示例

1. 前往**身份安全管控** > 账号安全，单击**新建策略**。



2. 单击**开启账号绑定策略**，设置账号可绑定的终端数量，支持按照 PC/移动端类型分别设置，编辑完成后，单击**保存**。



3. 前往**客户端管理** > **客户端策略** > 客户端通用设置，单击**新建策略**。



4. 配置设备绑定策略。

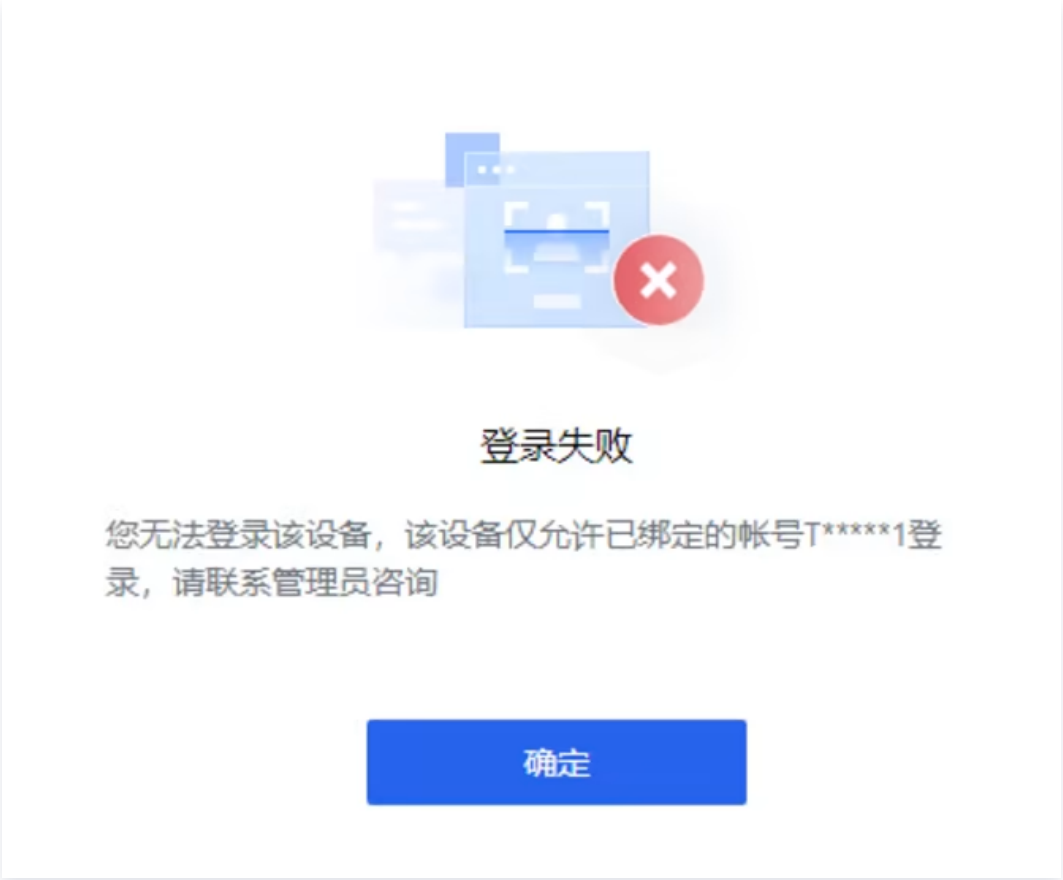


5. 打开 iOA 客户端并登录账号，终端与账号绑定完成。

6. 6.前往**资产运维 > 终端运维 > 终端信息**，查看已绑定账号状态。



7. 在该终端的客户端上登录其他账号，其他账号无法在该设备登录，登录失败。



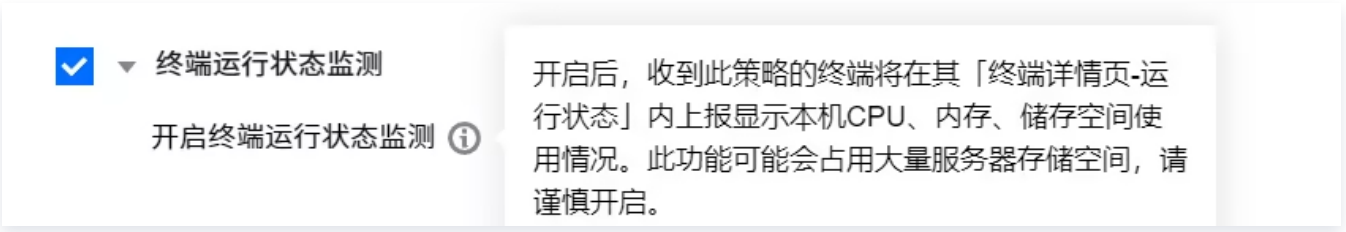
8. 如需解绑账号与设备的关系，可单击**解绑**，解除账号与设备的绑定。



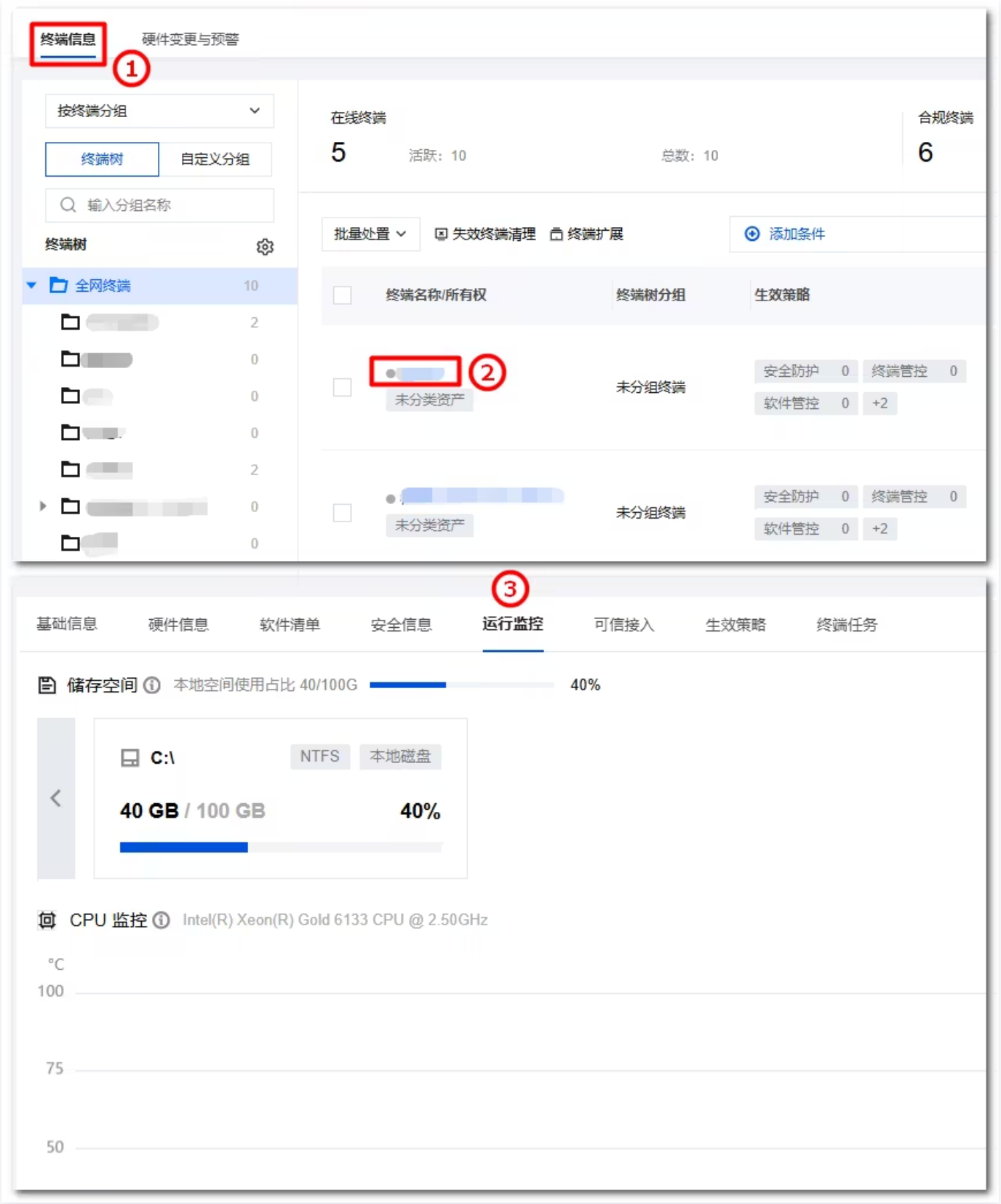
终端运行状态监测

1. 开启终端运行状态监测。

> **说明：**
> 开启「客户端管理-客户端策略-客户端通用设置」中的终端运行状态监测开关并重启设备后，终端将每五分钟一次更新数据。

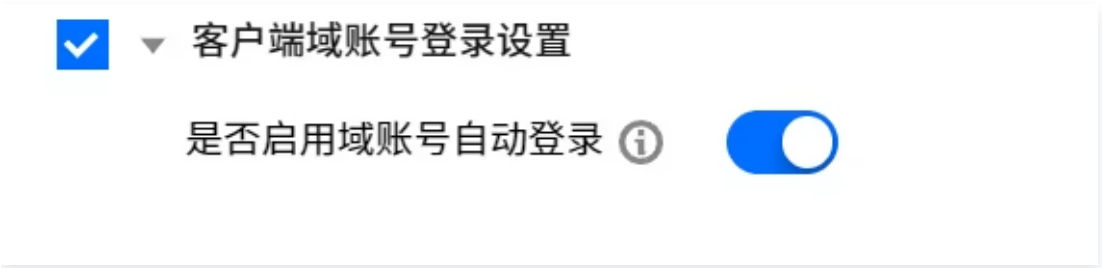


2. 收到此策略的终端将在其**资产运维** > **终端运维** > 终端信息 > **单击终端名称** > **终端信息** > **运行监控**内上报显示本机 CPU 温度、CPU 占用率、内存占用率、iOA 内存占用率使用情况。


终端信息
硬件变更与预警
1
按终端分组
终端树
自定义分组
输入分组名称
终端树
全网终端 10
在线终端
5
活跃：10
总数：10
合规终端
6
批量处置
失效终端清理
终端扩展
添加条件
终端名称/所有权
终端树分组
生效策略
2
未分类资产
未分组终端
安全防护 0
终端管控 0
软件管控 0
+2
3
基础信息
硬件信息
软件清单
安全信息
运行监控
可信接入
生效策略
终端任务
储存空间
本地空间使用占比 40/100G
40%
C:\
NTFS
本地磁盘
40 GB / 100 GB
40%
CPU 监控
Intel(R) Xeon(R) Gold 6133 CPU @ 2.50GHz
°C
100
75
50

客户端域账号登录设置

勾选客户端域账号登录设置，单击 **启用域账号自动登录**。



说明：

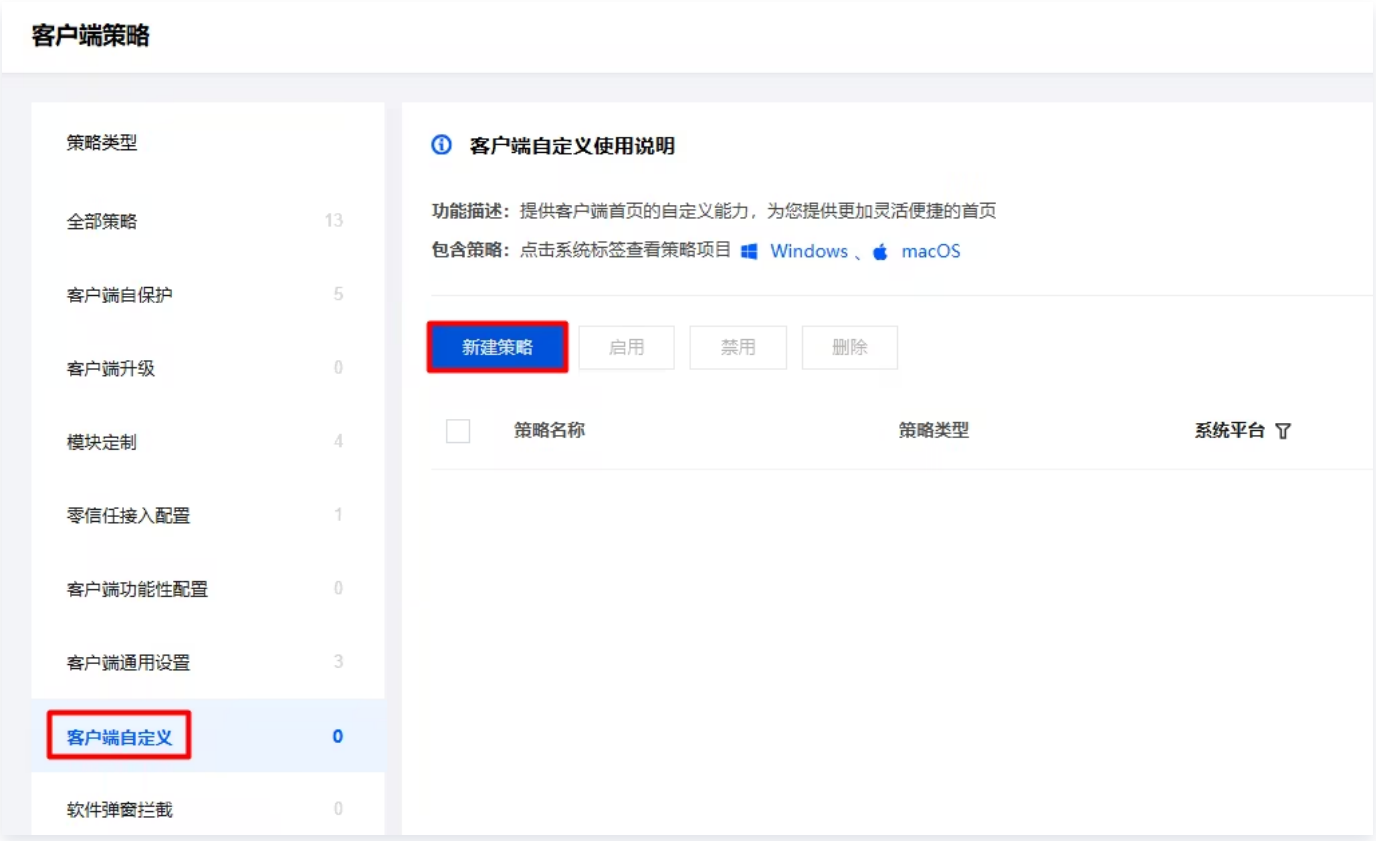
- 启用域账号自动登录设置前，请前往**员工与身份管理** > **身份安全管控** > **认证策略**主认证源选择 AD 认证源作为主认证方式的认证源，并**勾选 AD 域环境免认证**。
- 系统用域账号和密码完成登录后，客户端无需再次输入账号密码即可登录。
- 功能开启后，将接管和控制终端系统的登录界面。
- 该功能只支持 Win7以上系统。

客户端自定义（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端管理** > 客户端策略 。
2. 在客户端策略页面，选择**客户端自定义**，单击**新建策略**。



3. 在新建客户端自定义策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。

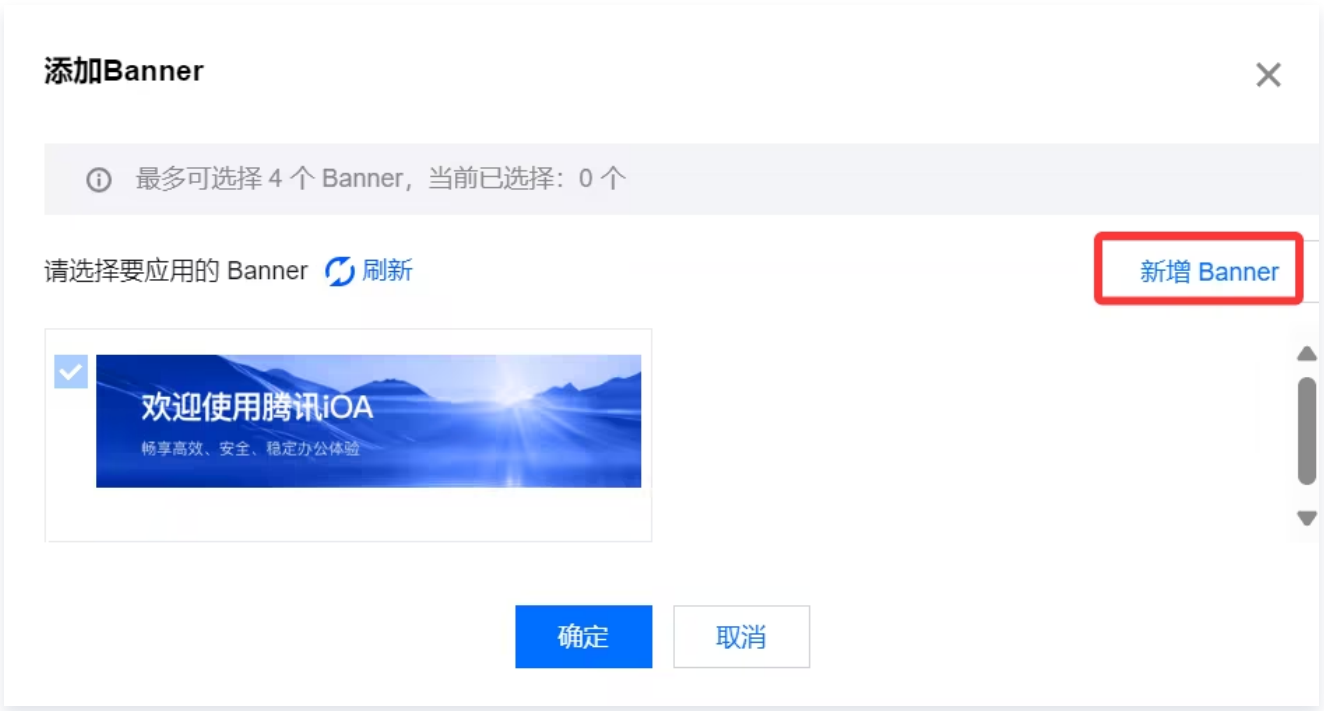


3.2 单击**添加适用范围**，勾选需管控/排除的终端名称，单击**确定**。

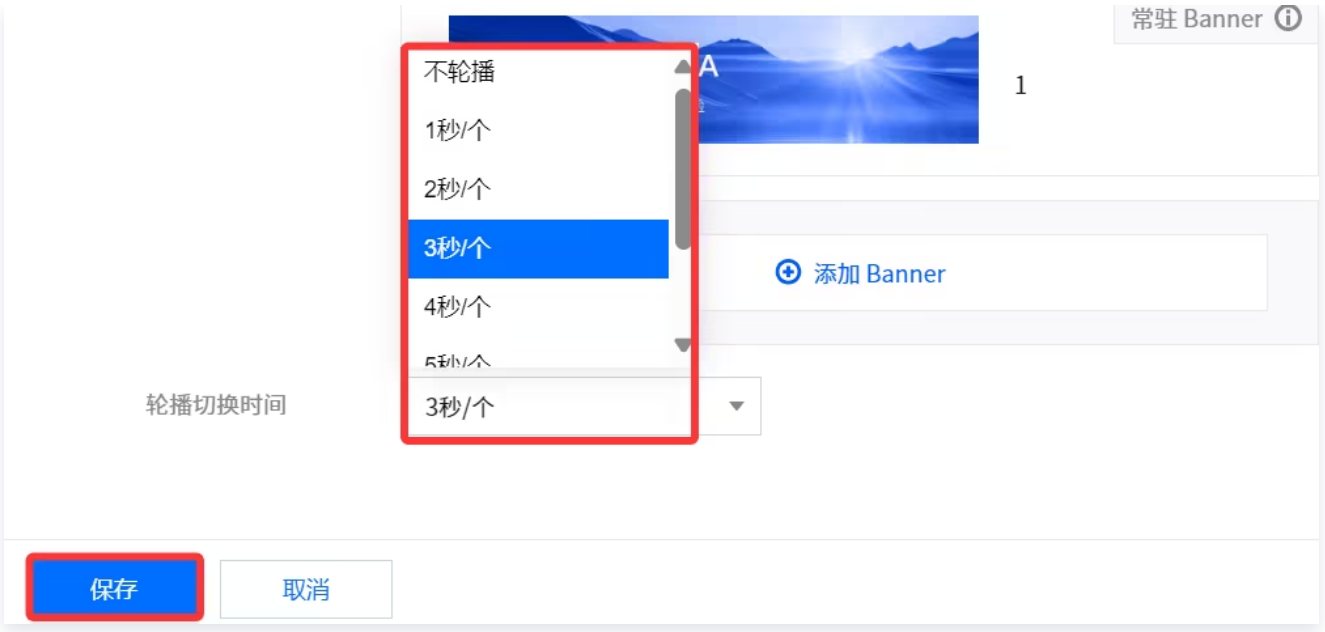
3.3 勾选 Banner 配置，单击**开启 Banner**，单击**添加 Banner**。



3.4 单击**新增 Banner**，上传尺寸为976×236像素的 JPG 或 PNG 图片，文件大小不超过2MB，单击**确定**。



3.5 若需展示多个Banner，请设置轮播切换时间，设置完成后单击**保存**。



4. 配置完成后，客户端的 Banner 展示如下：



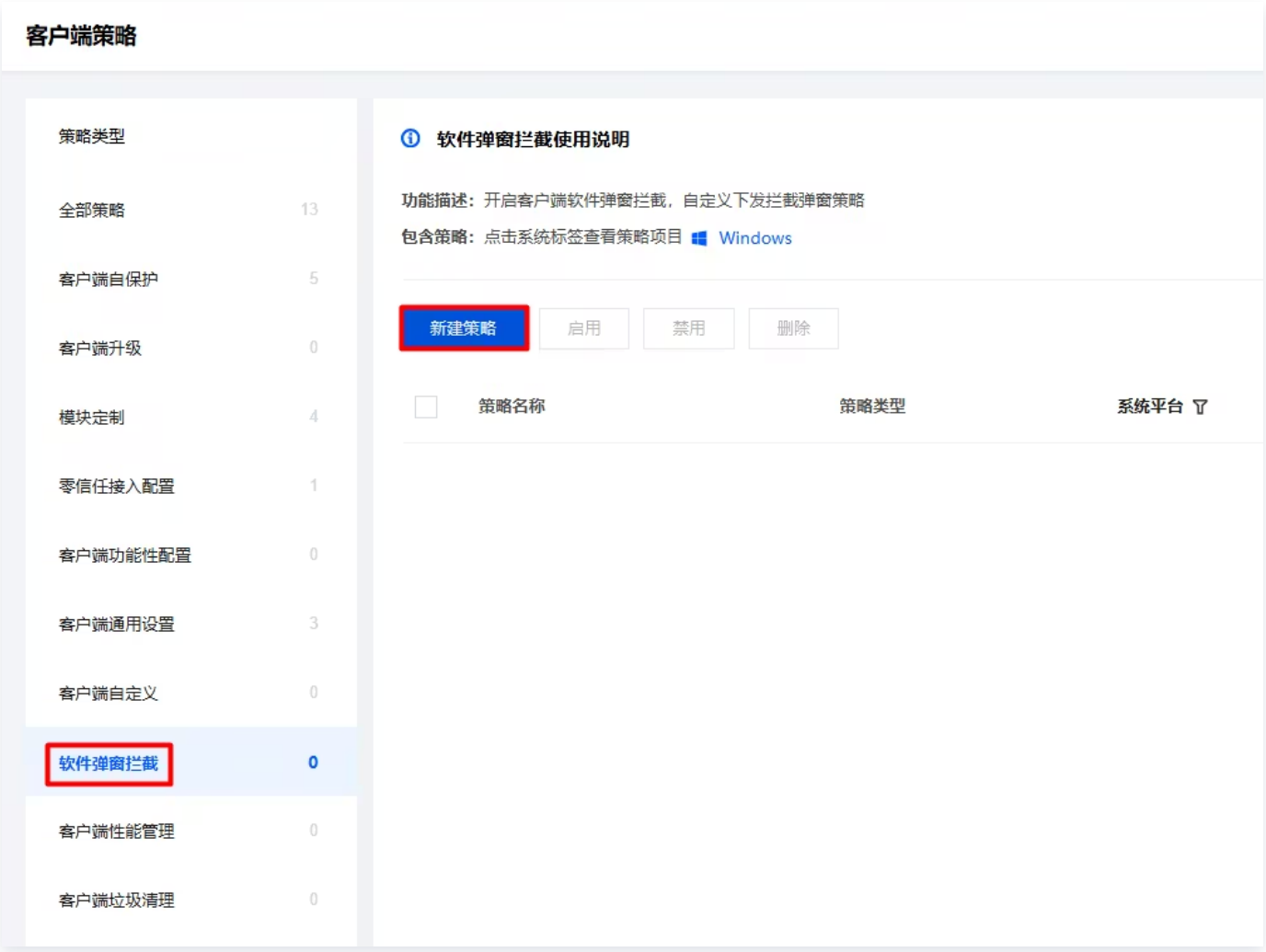
软件弹窗拦截（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

阻止或限制软件在用户终端界面上弹出广告窗口、恶意弹窗以及其他不必要的干扰性弹窗。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端管理** > 客户端策略 。
2. 在客户端管理页面，选择软件弹窗拦截，单击**新建策略**。



3. 在新建软件弹窗拦截策略页面，配置相关参数。
   3.1 输入策略名称，并输入策略描述等参数。



3.2 单击**添加适用范围**，勾选需管控/排除的终端名称，单击**确定**。

4. **勾选**软件弹窗拦截设置，开启软件弹窗拦截，单击**保存**。



说明：

- 软件弹窗里的拦截规则为特殊规则配置，正常情况下管理员仅需**勾选**软件弹窗拦截设置，开启软件弹窗拦截，单击**保存**即可。
- 如需添加弹窗拦截特殊规则，请单击链接选择人工服务 在线支持，我们的工作人员会及时与您沟通。

5. 前往**客户端管理** > **客户端策略** > 模块定制 界面配置是否在客户端启用软件弹窗拦截，配置完成单击**保存**。



6. iOA 客户端电脑工具 Tab 展示弹窗拦截。



版权所有：腾讯云计算（北京）有限责任公司

客户端性能管理（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

设置 iOA 的 CPU、内存占用限制，针对受控进程组进行资源管控，旨在确保多个进程在运行过程中对系统资源的消耗总体处于可控范围，系统在性能异常时能够自动采取措施，从而保障整个系统的稳定性和可用性。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端管理** > 客户端策略 。
2. 在客户端策略页面，选择**客户端性能管理**，单击**新建策略**。



3. 在新建客户端性能管理策略页面，配置相关参数。
   3.1 输入策略名称和策略描述等参数。



3.2 单击**添加适用范围**，勾选需管控/排除的终端名称，单击**确定**。

3.3 勾选**客户端性能控制**，配置客户端总体性能控制参数。



参数名称	说明
客户端核心业务总体 CPU 占用超过 XX%，则通知耗时业务降频运行	此项配置通过监控整体 CPU 使用情况，避免因核心业务占用过多资源而导致系统性能下降。
核心业务进程 CPU 占用超过 XX%，并持续 XX 分钟，则结束相关进程并重启	此项配置主要用来限制核心业务进程的 CPU 占用，防止 CPU 持续占用过高，影响终端性能。
核心业务进程内存占用超过 XXMB，并持续 XX 分钟，则结束相关进程并重启	此项配置主要用来限制核心业务进程的内存占用，防止内存占用过高，影响终端性能。

4. 配置完成后，单击**保存**。

客户端垃圾清理（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

辅助管理员管理长期未进行垃圾清理的终端，确保终端安全运行。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端管理** > 客户端策略 。
2. 在客户端管理页面，选择**客户端垃圾清理**，单击**新建策略**。



3. 在新建客户端垃圾清理策略页面，配置相关参数。

   3.1 输入策略名称，并输入策略描述等参数。



3.2 单击**添加适用范围**，勾选需管控/排除的终端名称，单击**确定**。

4. 勾选**客户端垃圾清理设置**，开启**垃圾定时清理**，配置需清理的类型，配置后由 iOA 控制台向客户端下发垃圾清理任务。



5. 清理频率支持选择定时清理以及自定义时间设置，配置清理频率和时间后单击**保存**。
6. 达到指定时间周期后，自动清理所选终端下的垃圾文件，前往**客户端管理** > **客户端操作日志** > **客户端垃圾清理日志**查看清理详情。



远程协助（11.1.1版）

最近更新时间：2026-02-06 14:23:32

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

功能简介

稳定连接终端，帮助 IT 运维人员高效管理分散在各地的设备，实现远程协助。

- 远程协助基础版：购买终端安全或者高级版的基础功能，未升级为远程协助极速版时，显示“基础版”标签，并仅支持使用基础功能。
- 远程协助极速版：升级为极速远程协助，显示“极速版”标签，并支持使用高级功能。

前提条件

- 终端完成客户端的安装（至少两台）。
- 完成账户/用户的创建（至少2个）。
- 远程协助的终端为在线状态（离线关机终端无法远程连接）。

远程协助方式说明

- 场景1：通过控制台进行远程协助。在控制台的终端详情页面中打开远程终端。用户需要登录到相应的控制台，找到目标终端的详情页面，单击**远程协助**，连接远程终端。
- 场景2：终端间远程协助。登录客户端，用户在自己的终端机上通过客户端单击**远程协助**，连接远程终端。

> **说明：**
> 远程协助仅将 macOS 用作控制端（macOS 支持发起远程协助，但暂不支持接收远程协助）。

场景1：控制台到端使用远程协助

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端运维** > **客户端管理** > 客户端策略 。
2. 在客户端管理页面，选择**客户端自保护**，单击**新建策略**。

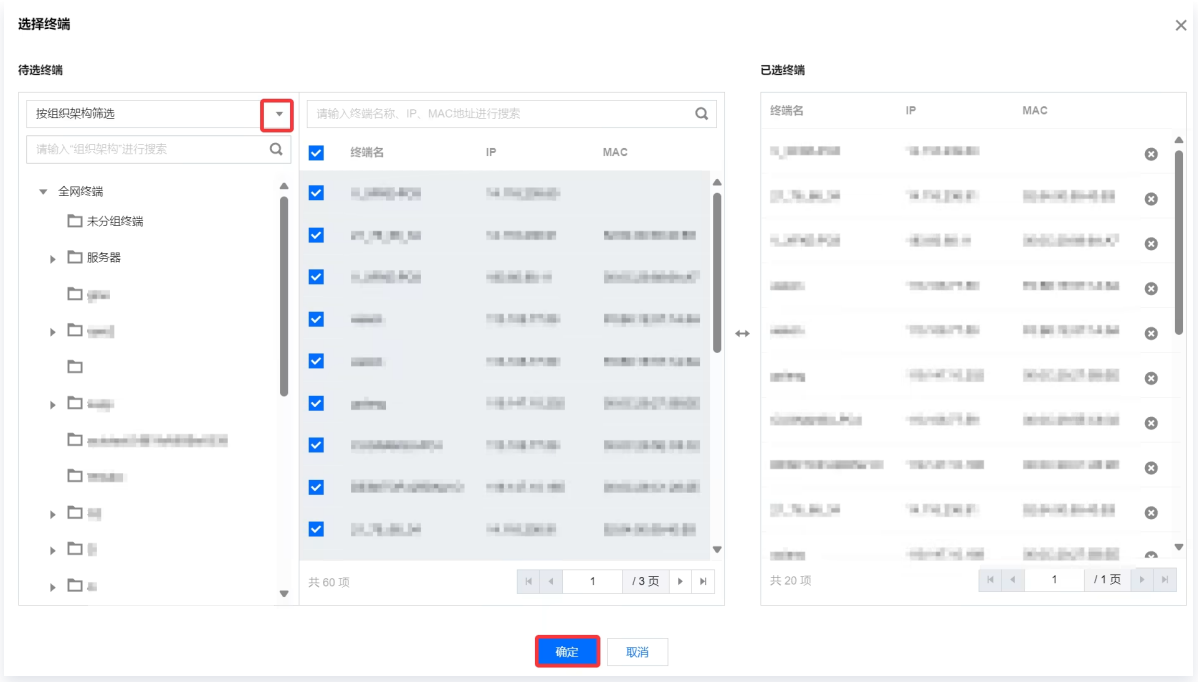


3. 在基本信息页面，配置相关参数。

3.1 输入策略名称，例如：远程协助，并输入策略描述等参数。



3.2 单击**添加适用范围 > 添加终端**，勾选需远程协助的终端名称，单击**确定**。



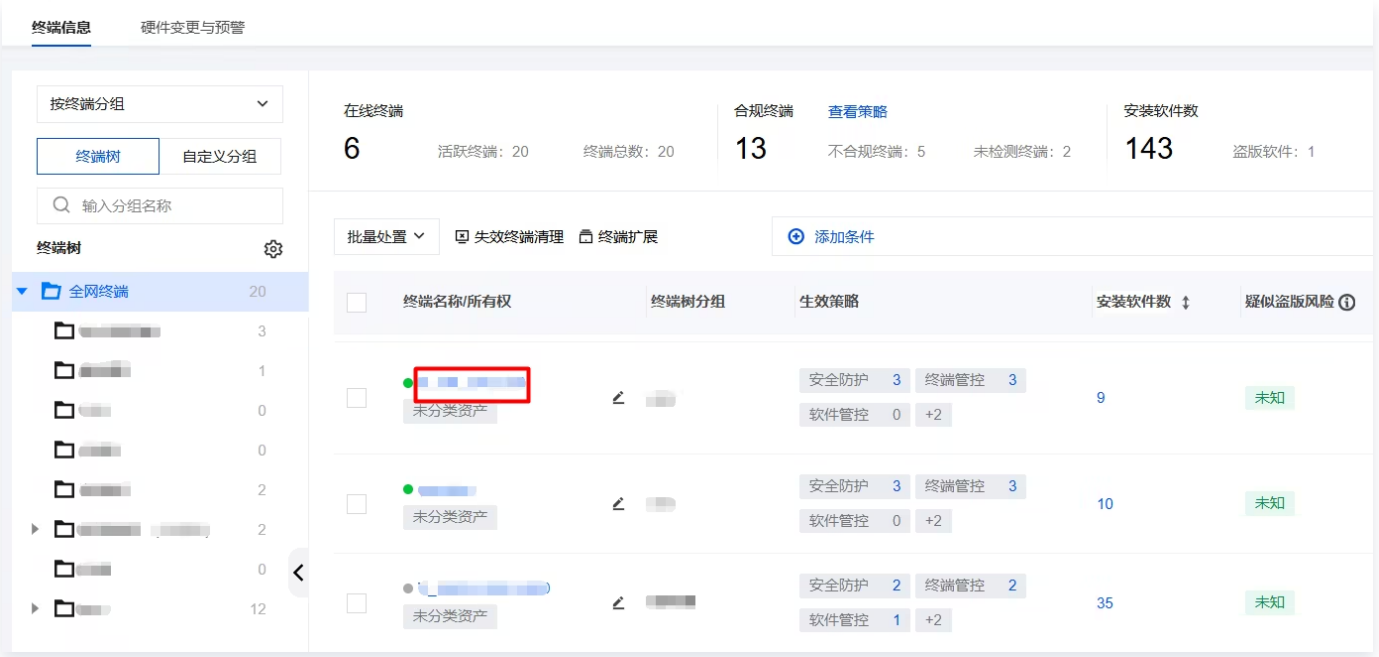
3.3 选择远程协助设置，勾选**远程协助场景**，单击**保存**。



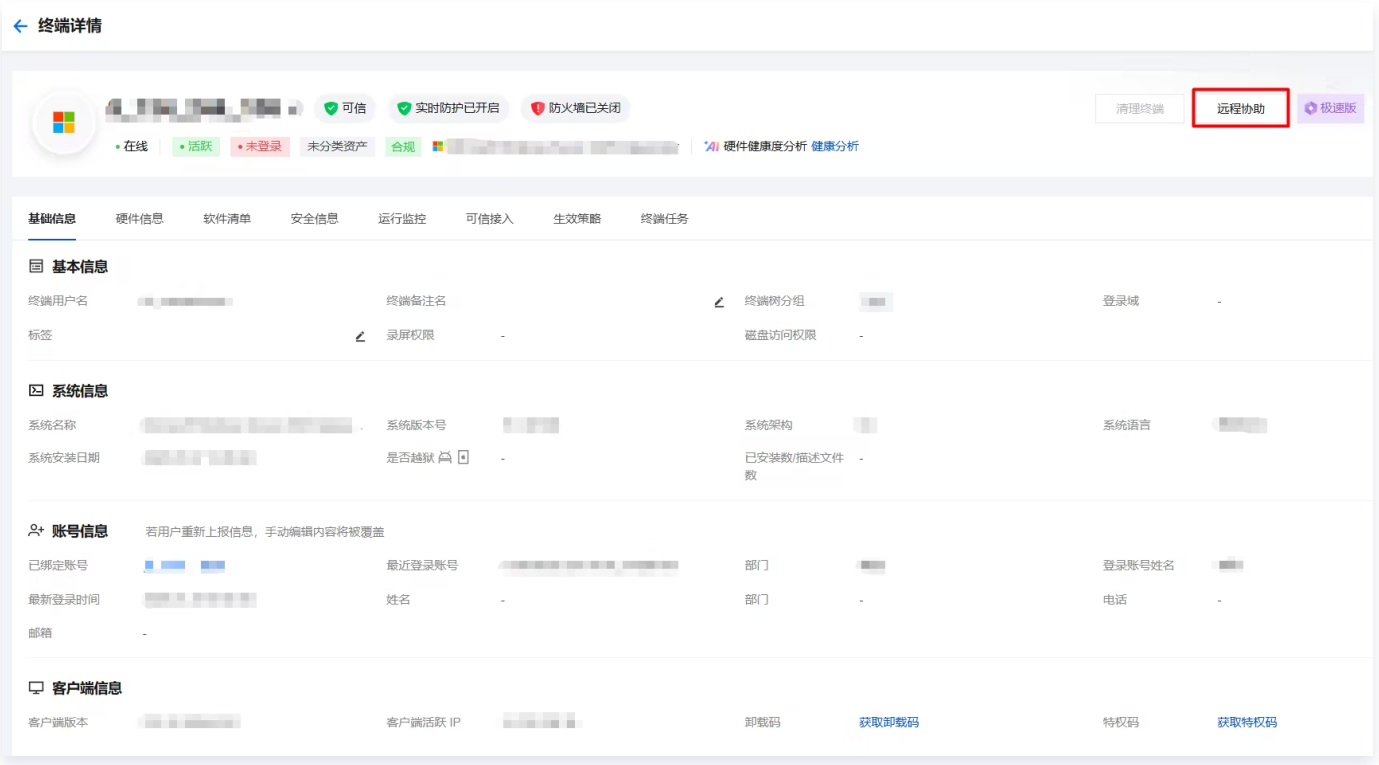
4. 在 终端树页面 ，单击**全网终端**分组下的**在线终端名**。

> **说明：**
>
> - 终端名左侧为灰色表示终端不在线。

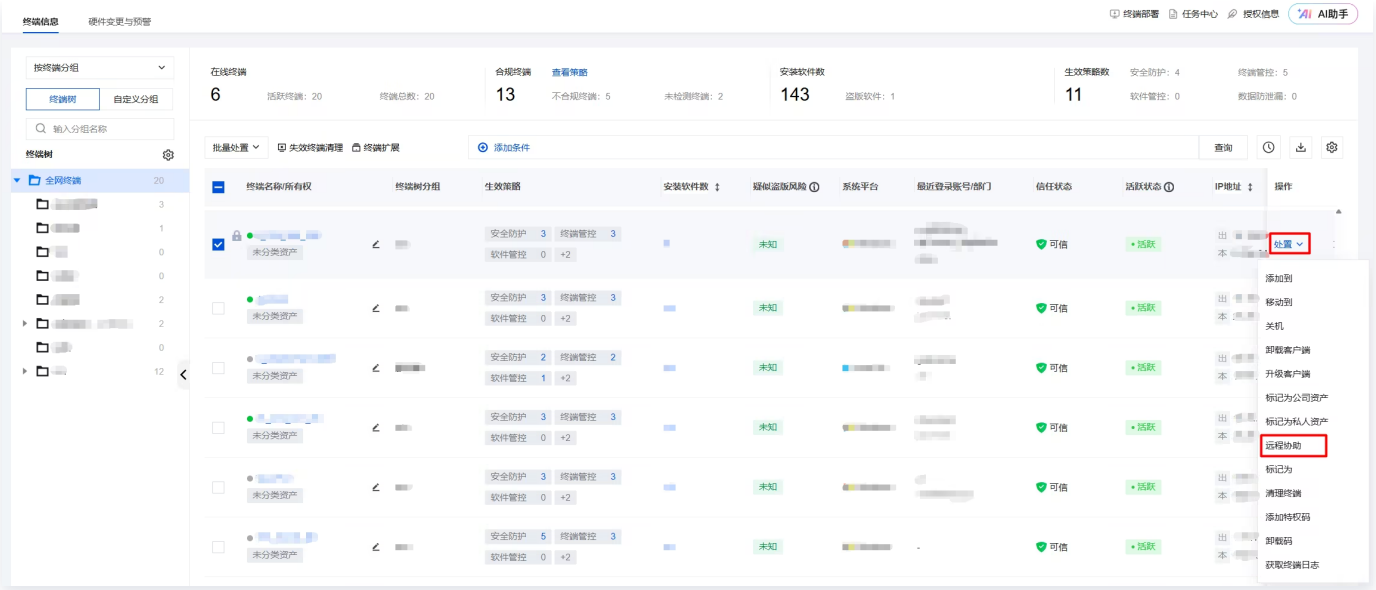
- 终端名左侧为绿色表示终端在线。



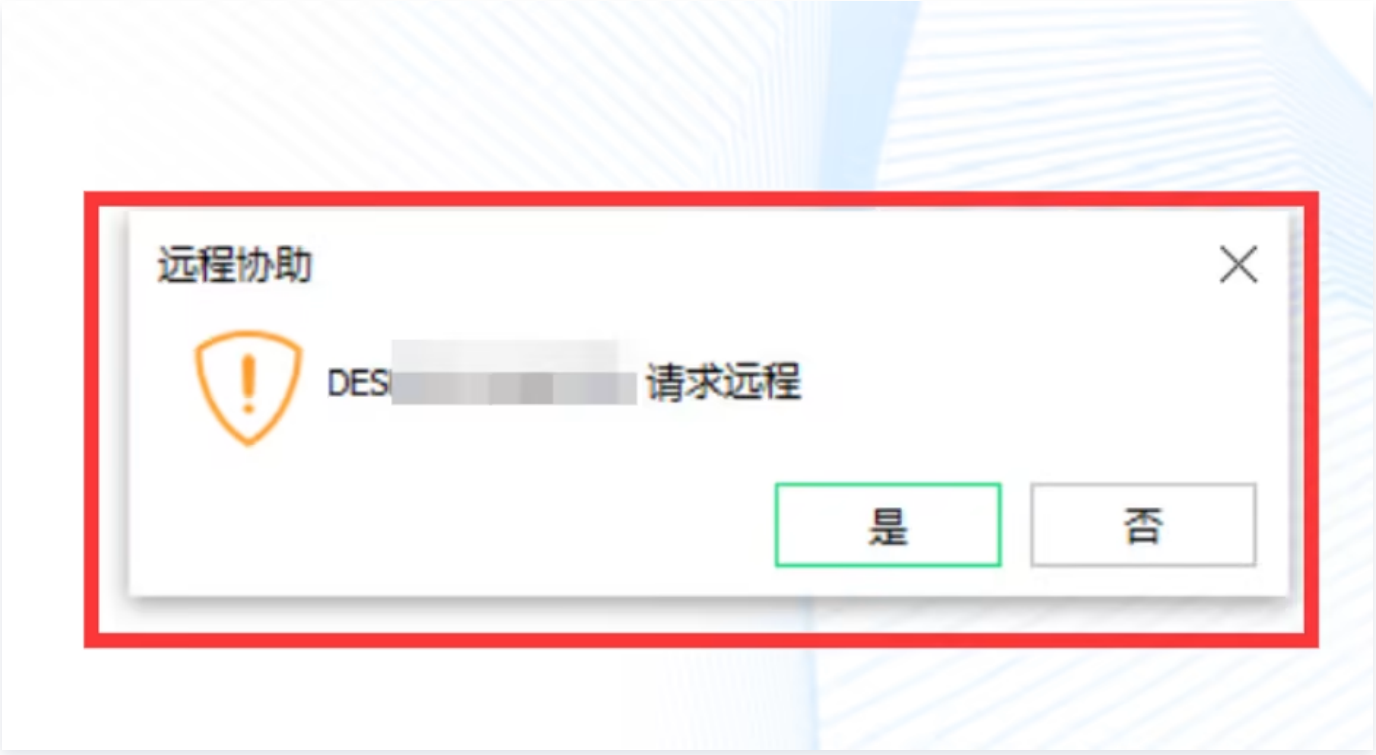
5. 在终端详情页面，单击**远程协助**。



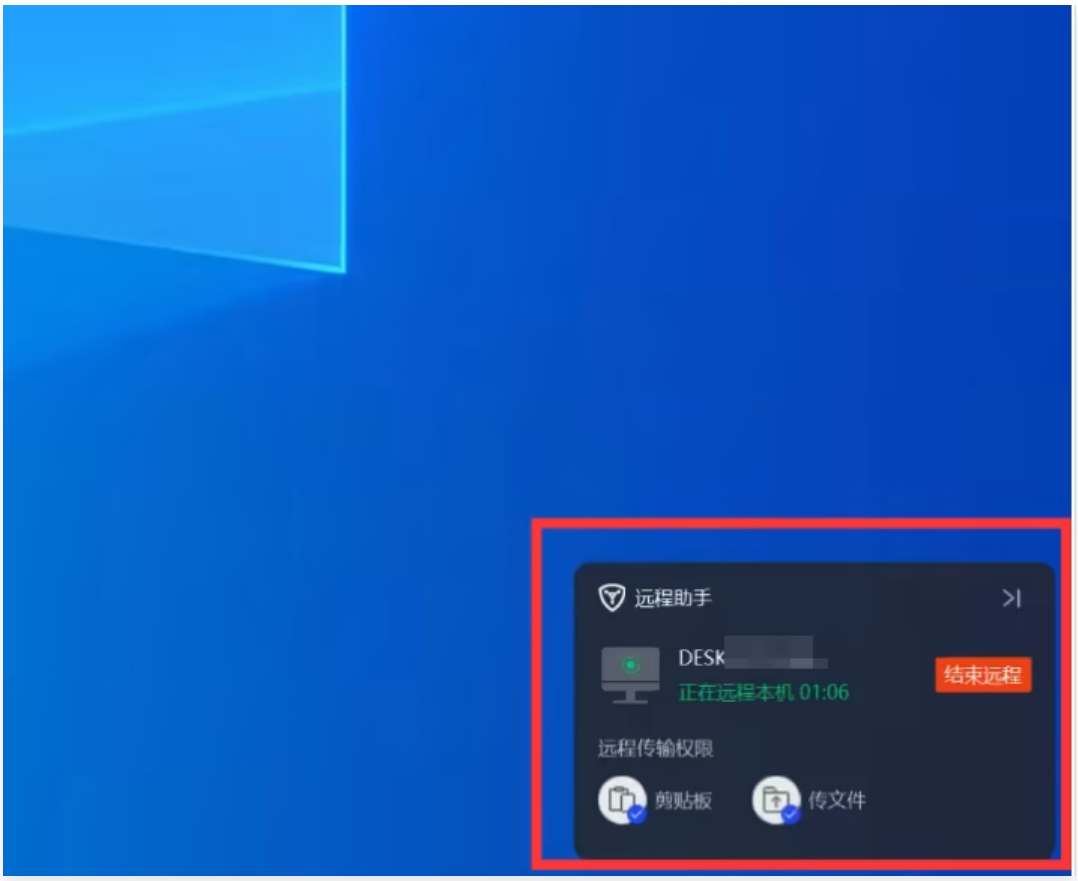
6. 您也可通过终端列表“处置”菜单栏单击**远程协助**，方便您快速发起远程协助操作，提升运维效率。



7. 终端收到远程协助请求，单击**是**。



8. 如下图所示，控制台到终端远程协助成功。



场景2：终端之间使用远程协助

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端运维** > **客户端管理** > 客户端策略 。
2. 在客户端管理页面，选择**客户端自保护**，单击**新建策略**。

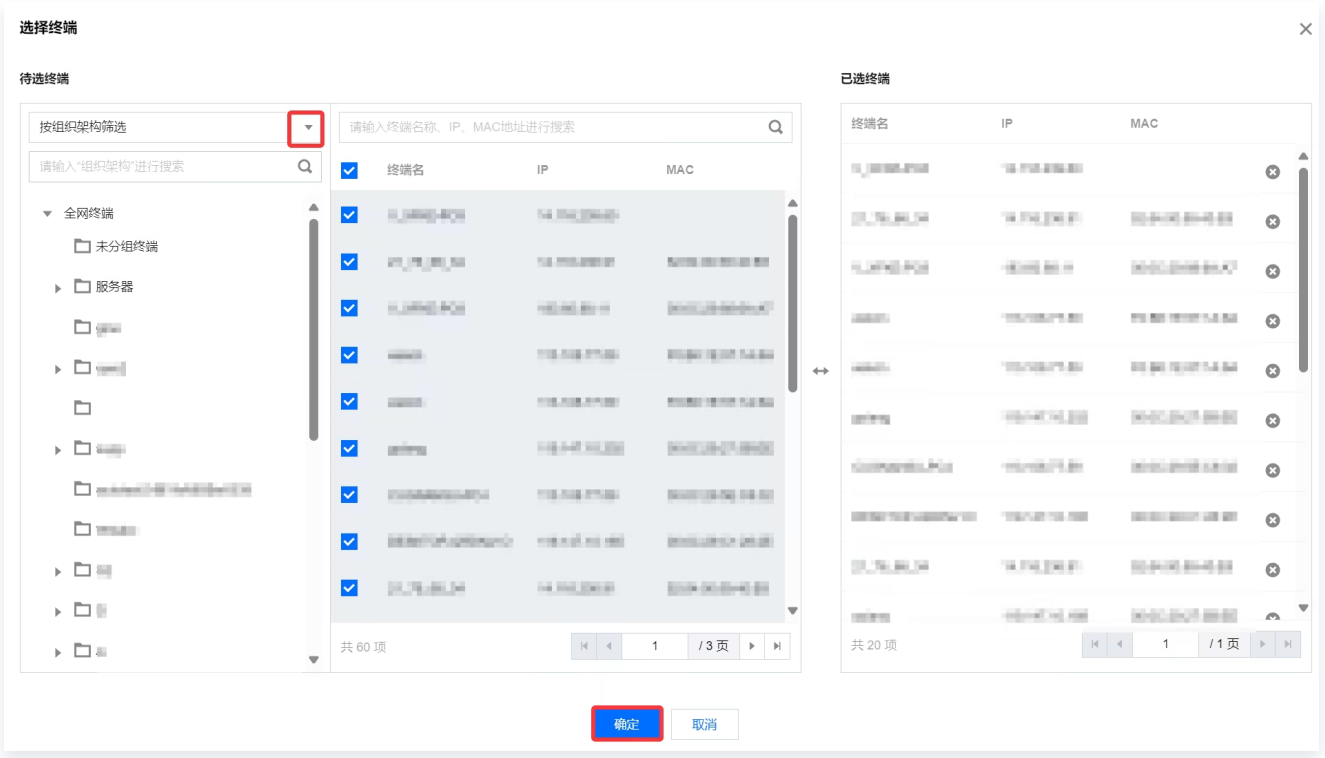


3. 在基本信息页面，配置相关参数。

   3.1 输入策略名称，例如：远程协助，并输入策略描述等参数。



3.2 单击添加适用范围 > 添加终端，勾选需远程协助的终端名称，单击确定。



3.3 选择远程协助设置，勾选远程协助场景，单击保存。



4. 在客户端策略页面，选择**模块定制**，单击**新建策略**。

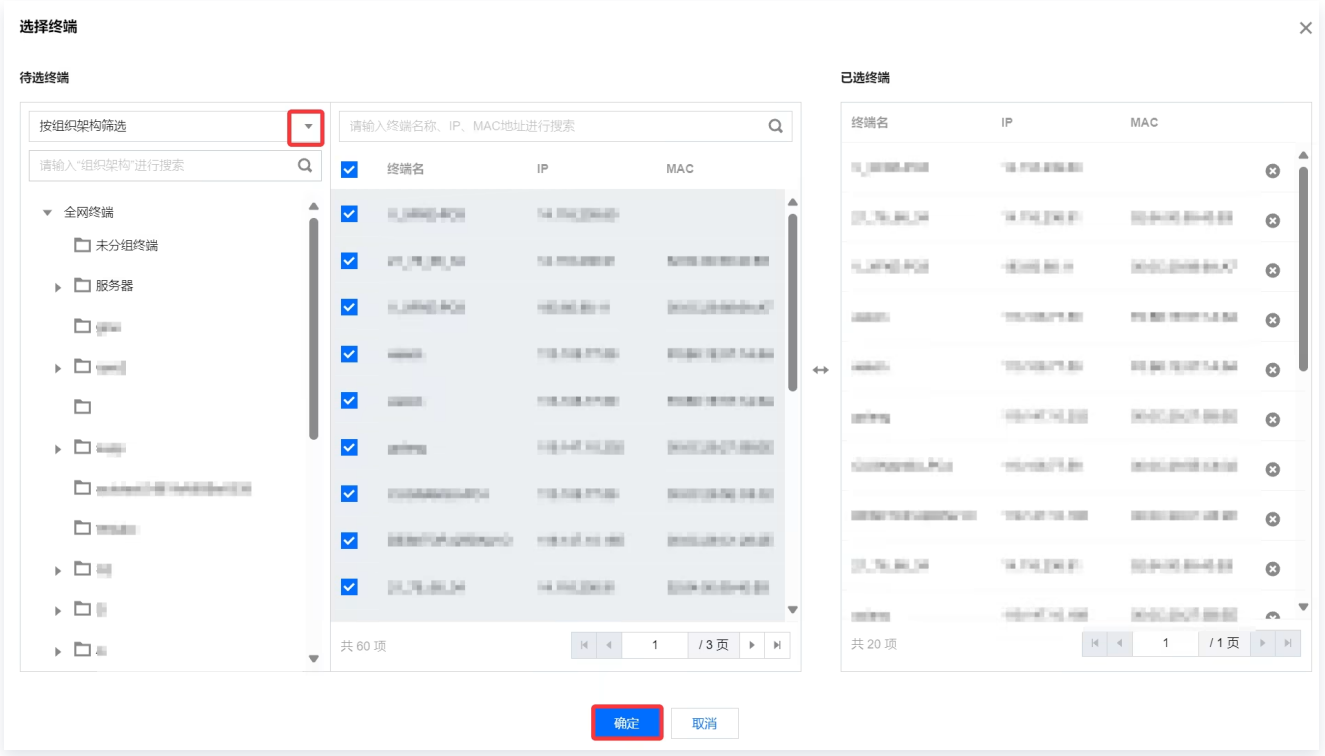


5. 在基本信息页面，配置相关参数。

5.1 输入策略名称，例如：开启远程协助功能模块，并输入策略描述等参数。



5.2 单击**添加适用范围 > 添加终端**，勾选需远程协助的终端名称，单击**确定**。



5.3 勾选功能模块配置中的**远程协助**，单击**保存**。



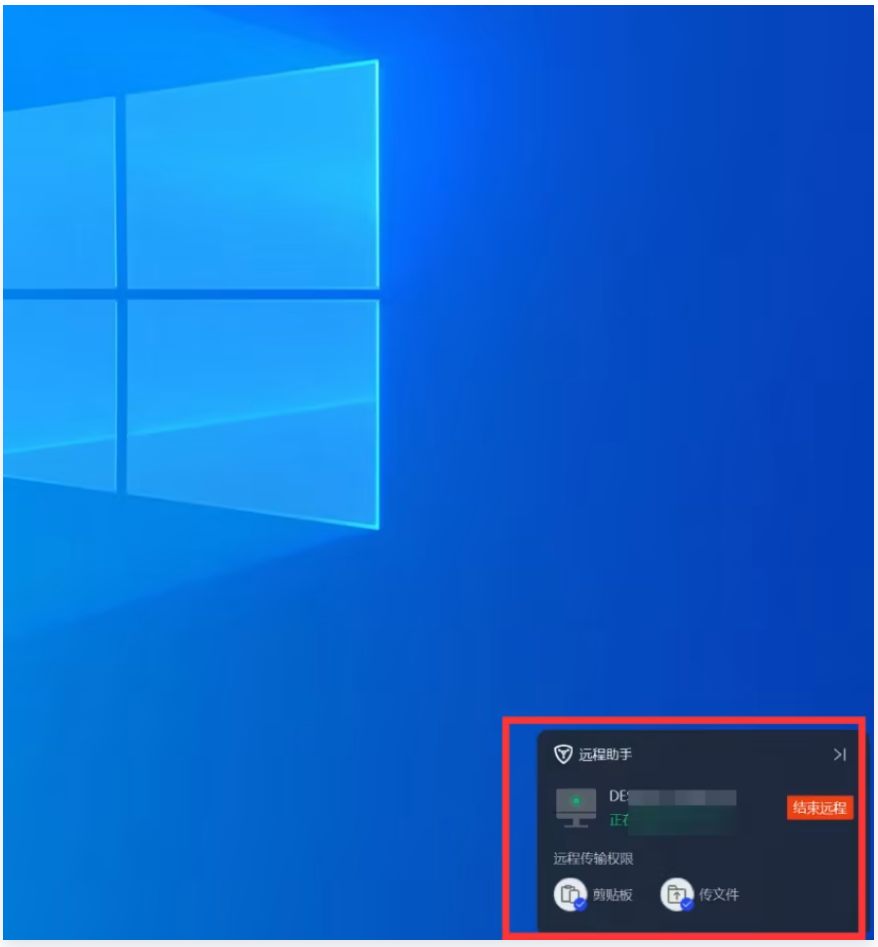
6. 使用账号**登录客户端**，首页展示远程协助模块，单击 > **远程协助**。



7. 输入**控制远程电脑的机器识别码**，单击**开始远程**。



8. 如下图所示，终端之间使用远程协助连接成功。



客户端操作日志（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

日志功能概览

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏， 选择**客户端运维** > **客户端管理** > 客户端操作日志 。
2. 在客户端操作日志页面，支持查看安装卸载、客户端升级、开机关机等日志。



图标	图标含义
近7天	支持快速选择预设时间段（最近7天/近10天/近30天），支持自定义精确时间范围。
	数据统计图表以柱状图形式展示
	支持将审计数据导出为文件，便于离线分析。
	支持自定义展示报表字段

	支持快速搜索并展示报表内的相同内容

审计日志说明

在日志审计中，分为如下模块：

客户端操作日志	日志内容
安装卸载	展示 iOA 客户端的安装卸载启动退出日志。
客户端升级	展示 iOA 客户端的升级日志。
开机关机	展示 iOA 客户端的开机关机日志。
特权模式	展示 iOA 客户端启动特权模式的情况。
远程协助日志	展示 iOA 客户端的远程协助情况。
自保护日志	查看自保护相关告警和日志信息，展示任意终端尝试破坏 iOA 的行为，如停止进程、停止服务、删除文件等行为都会触发客户端自保护策略并生成自保护日志。
客户端垃圾清理日志	展示 iOA 客户端垃圾清理情况。

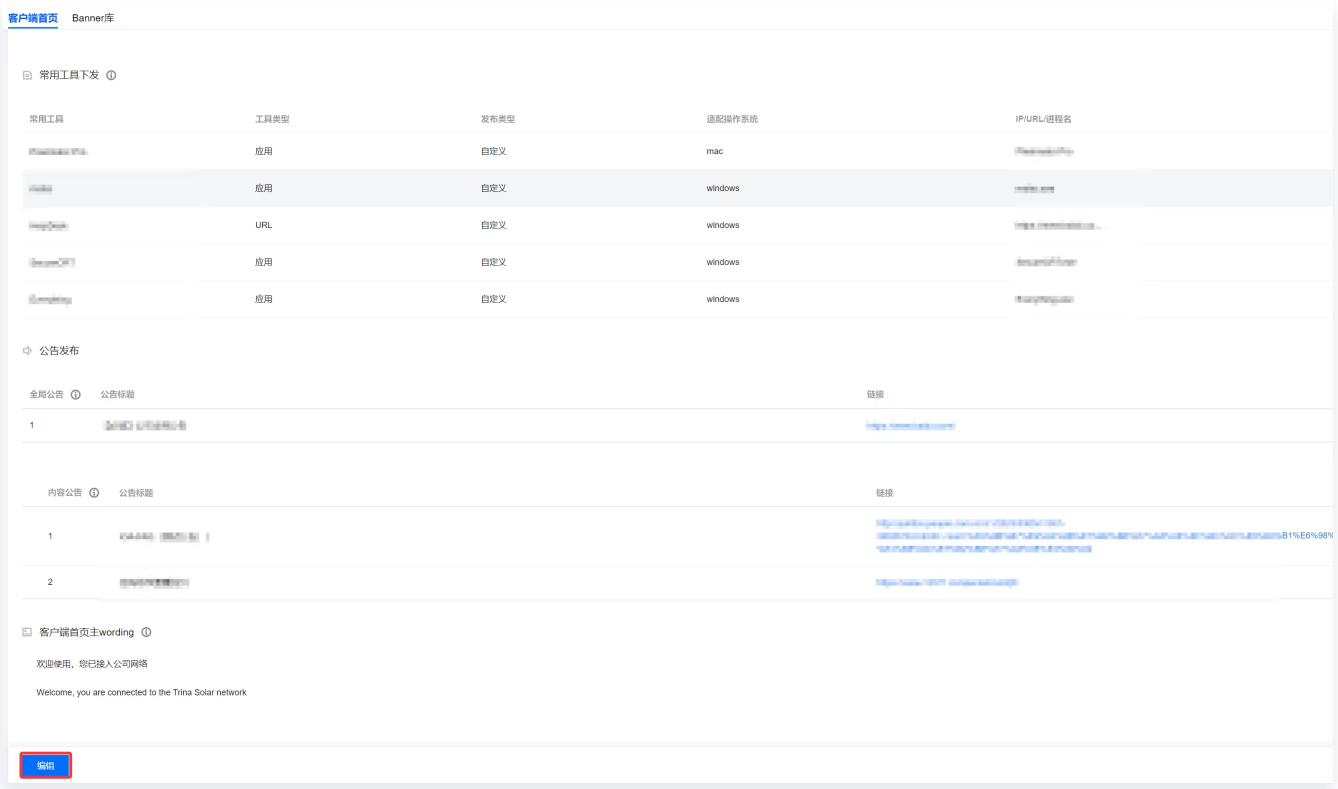
版权所有：腾讯云计算（北京）有限责任公司

个性化设置（11.1.1版）
客户端首页（11.1.1版）

最近更新时间：2026-02-13 17:55:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择客**户端运维** > 个性化设置 。
2. 在**客户端首页**，单击左下角的**编辑**。

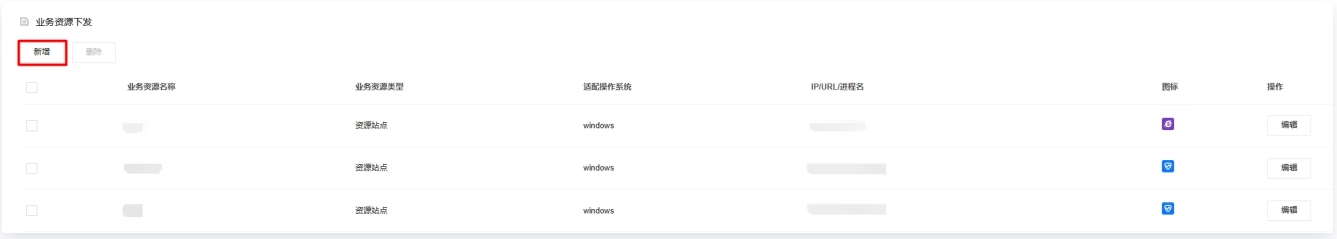


业务资源下发

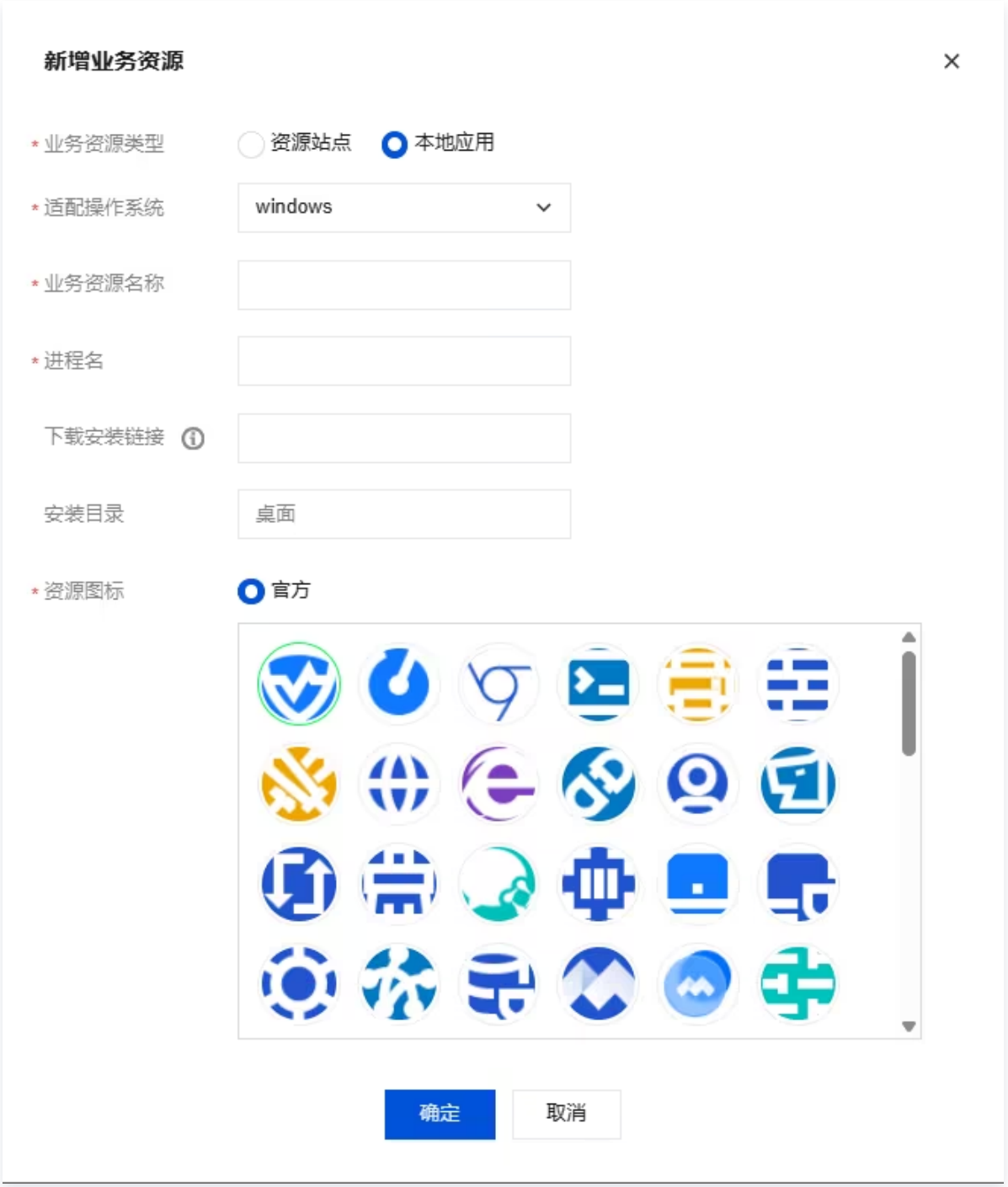
> **说明：**
> - 请在此表添加已收敛到零信任网关之后的业务资源站点域名或 IP，目前仅支持隧道应用的 URL下发至首页。
> - 业务站点发布后，用户仅能查看到自己已被授权的业务资源站点，没有被授权的站点资源不会在客户端首页展示。
> - 最多创建并下发500个业务资源站点。

- 关联业务资源**无边界办公** > **应用管理** > 应用配置 信息中的**隧道资源**，隧道资源配置请参见 隧道类资源授权访问 。
- 发布业务资源站点到客户端首页，用户仅能查看到自己有权访问的业务资源站点，权限设置请参见 隧道类资源授权访问 。

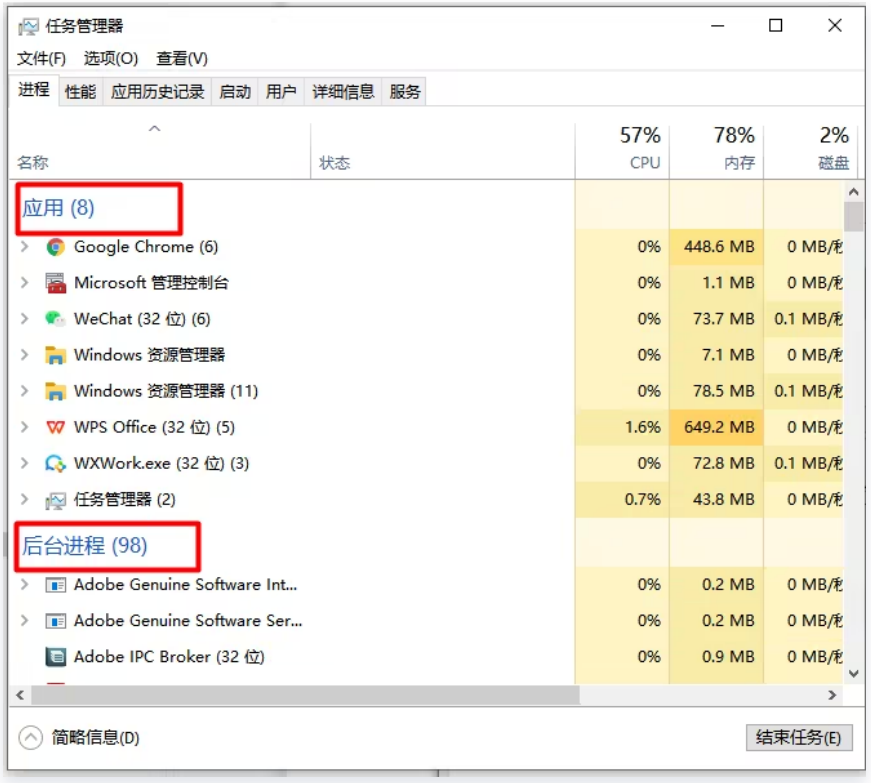
1. 在业务资源下发模块中，单击**新增**。

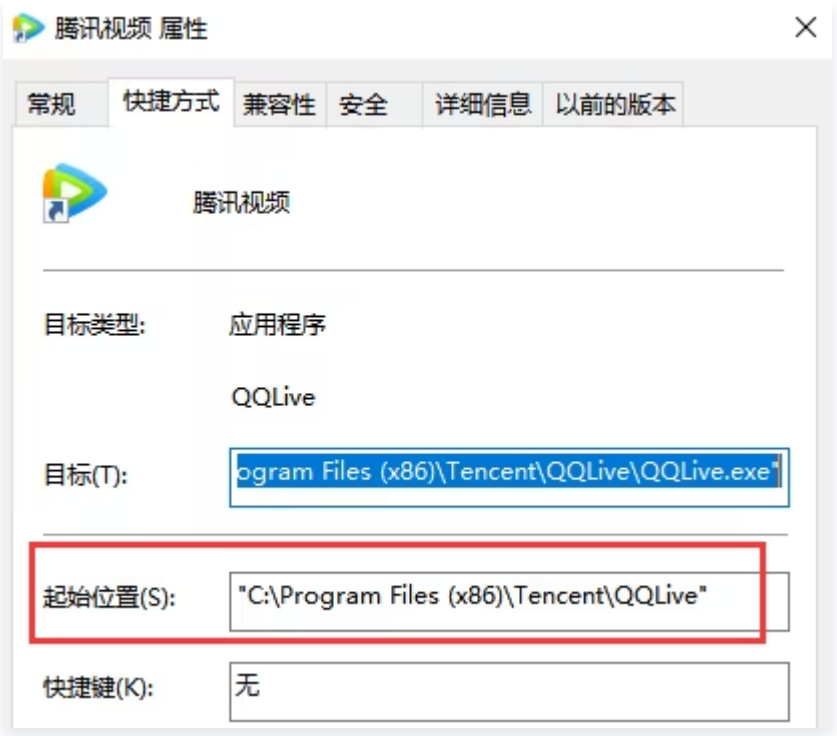


2. 在新增业务资源弹窗中，配置相关参数，单击**确定**。



业务资源类型	参数名称	说明
资源站点	适配操作系统	• 支持对Windows、Mac、Android和iOS系统进行配置。配置完成后，相关资源将在所配置的系统中展示。若未对某系统进行配置，则该系统中将不展示相关资源。 • 支持多选。
	业务资源名称	展示在客户端的资源名称。

	URL	• 关联**管理中心** > **访问配置管理** > 业务资源管理 中的隧道资源。 • URL 地址必须以 http:// 或者 https:// 开头。 • URL地址必须和隧道资源配置的业务资源地址相同，可自行搭配子路径。
	资源图标	由官方提供，所选图标将展示在客户端中。
本地应用	适配操作系统	• 支持对 Windows、Mac 系统进行配置。配置完成后，相关应用将在所配置的系统中展示。若未对某系统进行配置，则该系统中将不展示相关应用。 • 单选。
	业务资源名称	展示在客户端的应用名称。
	进程名	在任务管理器中可查看进程名称。 
	下载安装链接	下载安装链接必须以 http:// 或者 https:// 开头，如果某终端上无该应用，客户端则弹窗提供下载链接，点击下载即可。
	安装目录	• 默认桌面。 • 支持自定义设置应用安装的路径，应用路径查询参照下图。



- 每台终端安装的路径不一定相同，当管理员设置的路径与终端实际不符，客户端会弹窗提示，允许用户设置应用路径信息。



资源图标	由官方提供，所选图标将展示在客户端中。

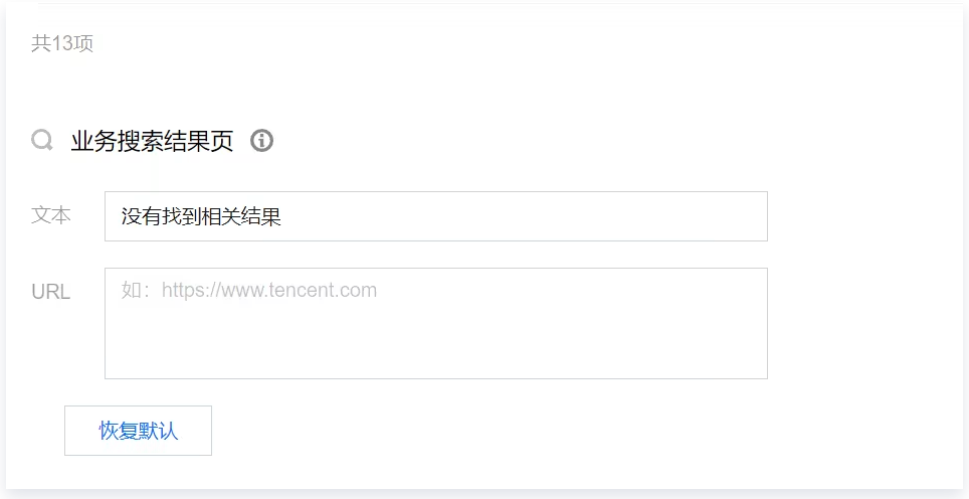
3. 确认内容无误后，单击**保存**。
4. 客户端样式。



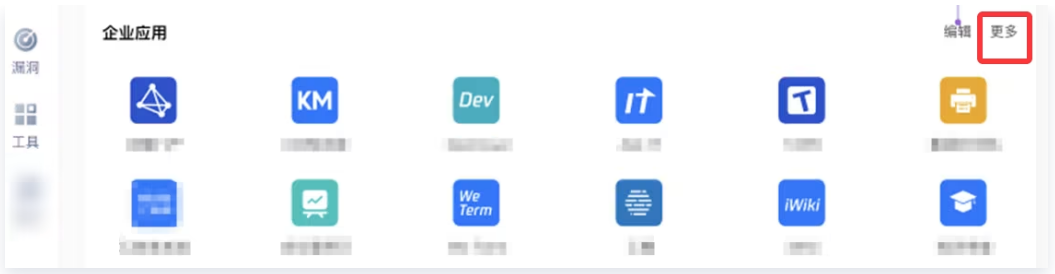
业务搜索结果页

1. 前往**个性化设置** > 客户端首页，配置业务搜索结果页。当搜索结果为空时，显示配置的文案。
2. 如果添加了 URL，则文本内容自动添加该URL为超链接。作用：当搜索不到时，提供管理员可自定义搜索不到结果的文案，引导员工申请权限。

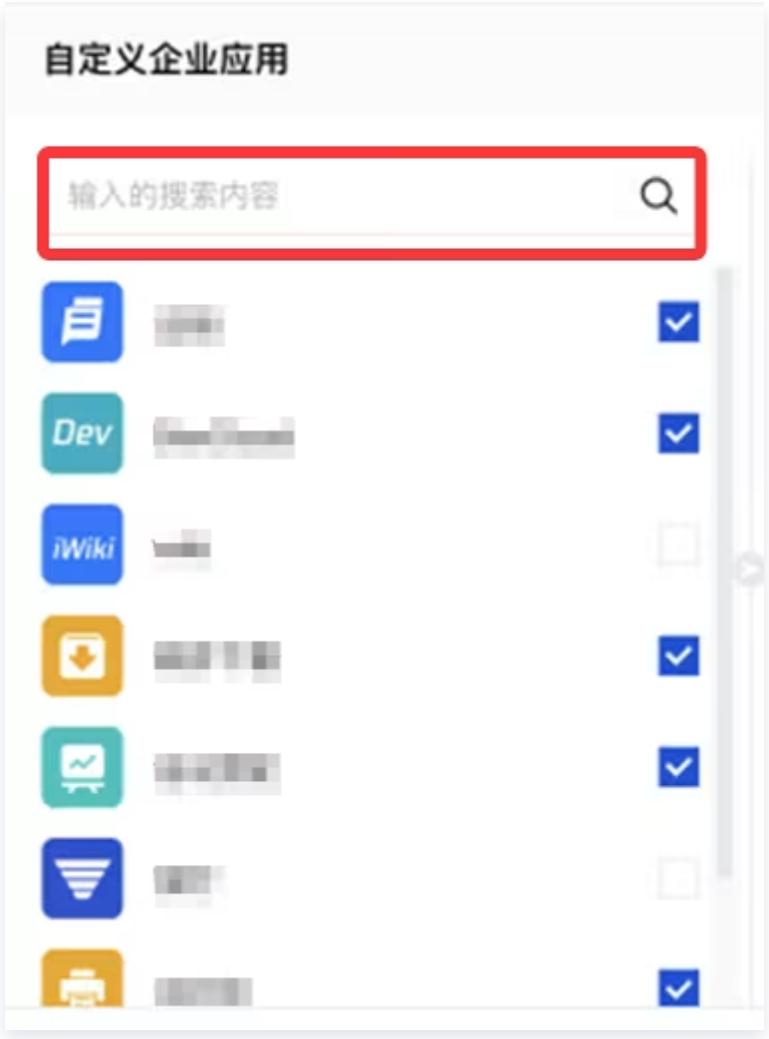
> **说明：**
> 搜索逻辑：输入关键字对应的名称进行模糊匹配搜索。



3. 确认内容无误后，单击**保存**，在企业应用中单击**更多**。

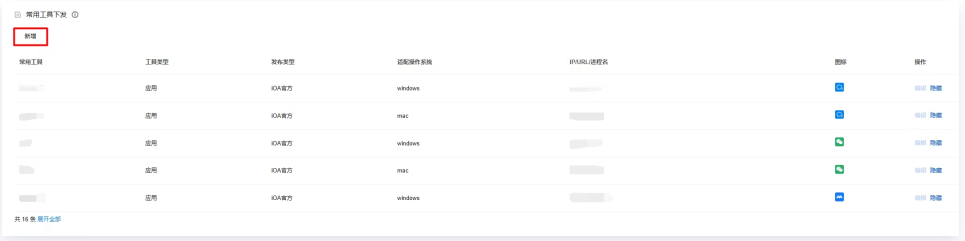


4. 搜索框搜索查询企业应用，输入关键字对应的名称进行模糊匹配搜索，若搜索结果为空，显示配置的文案。



常用工具下发

1. 前往**个性化设置** > **客户端首页**，配置常用工具。常用工具为全员通用可见的工具，将显示在客户端的常用工具区。
2. 常用工具支持配置 exe 文件、链接等形态，支持引导员工下载并安装常用工具。
3. 在常用工具下发模块中，单击**新增**。

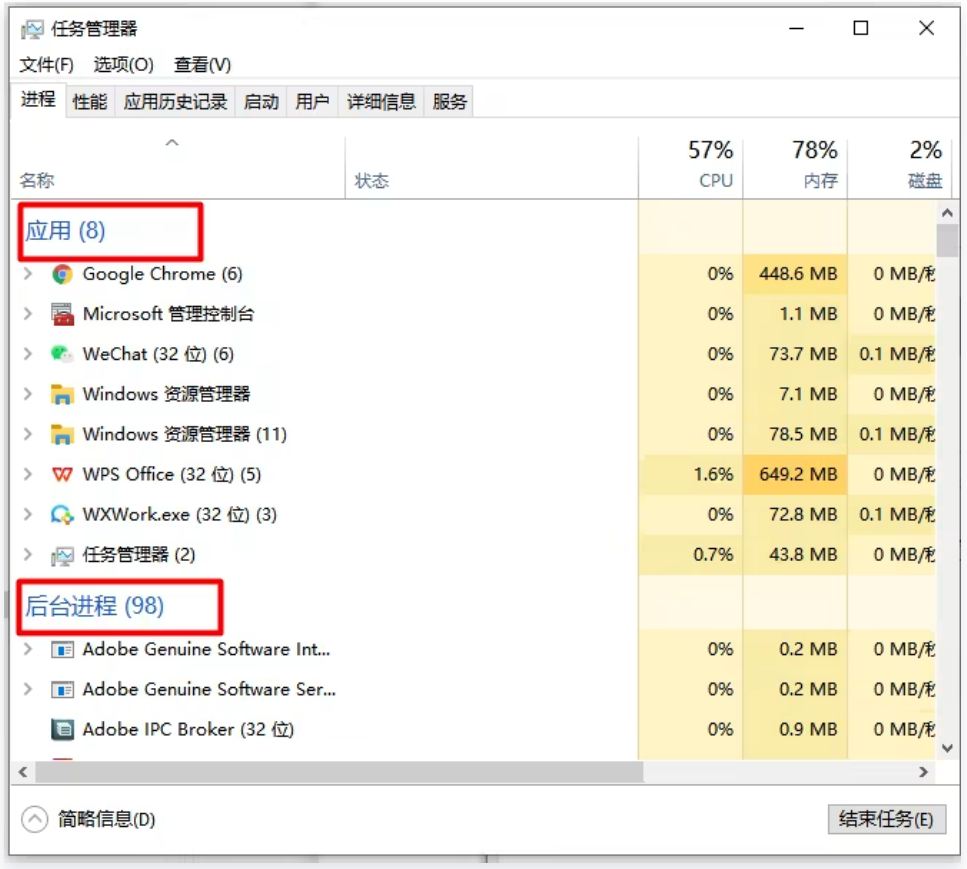


4. 在新增常用工具弹窗中，配置相关参数，单击**确定**。



类别	参数名称	说明
应用	工具分组	选择对应的工具分组，配置后可使工具在客户端电脑工具 tab 页分组展示。



操作系统	支持 Windows、Mac的配置。
应用名	应用的名称。
进程名	在任务管理器中可以查看进程名称。 

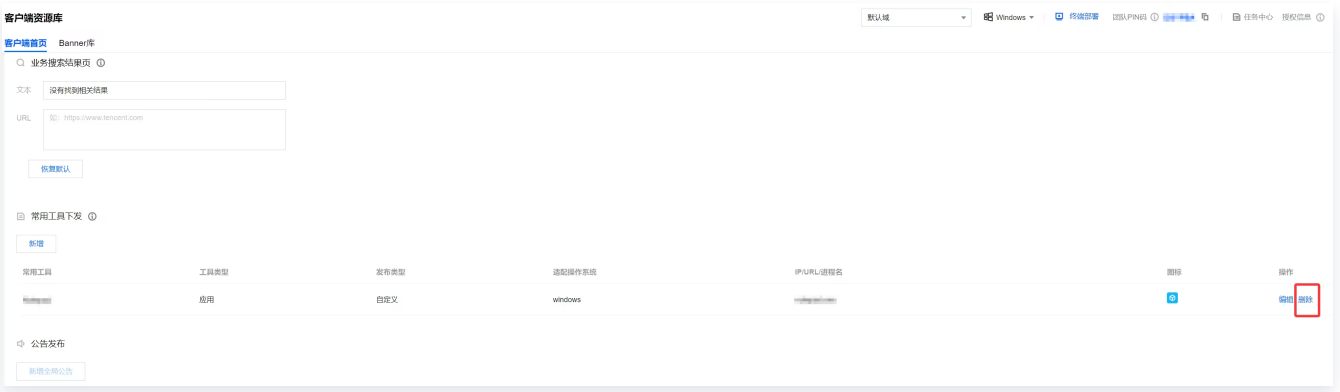
	下载安装链接	下载安装链接必须以 http:// 或者 https:// 开头，如果某终端上无该应用，客户端则弹窗提供下载链接，单击**下载**即可。
	安装目录	• 默认桌面。 • 支持自定义设置应用安装的路径。 • 每台终端安装的路径不一定相同，当管理员设置的路径与终端实际不符，客户端会弹窗提示，允许用户设置应用路径信息： 
	图标选择	由官方提供，所选图标将展示在客户端中。
URL	工具分组	选择对应的工具分组，配置后可使工具在客户端电脑工具 tab 页分组展示。 
	操作系统	• 支持对 Windows、Mac 系统进行配置。配置完成后，相关URL将在所配置的系统中展示。若未对某系统进行配置，则该系统中将不展示此 URL。

		• 支持多选。
	URL名	URL 名称。
	URL	URL 地址必须以 http:// 或者 https:// 开头。
	图标选择	由官方提供，所选图标将展示在客户端中。

5. 确认内容无误后，单击**保存**。
6. 客户端常用工具样式。



7. 若需删除 iOA 客户端不常用的工具，可前往**个性化设置** > **客户端首页**，在配置常用工具下发处，选择不常用的工具，单击**删除**即可。



公告发布

前往**个性化设置** > 客户端首页，配置公告。在公告发布模块中，分为全局公告和内容公告。

全局公告

1. 位于客户端上方，员工无需登录都可看到，常用于客户端 FAQ指引内容，全局公告仅能添加1条。



2. 单击**编辑**，填写标题和链接，单击**保存**。

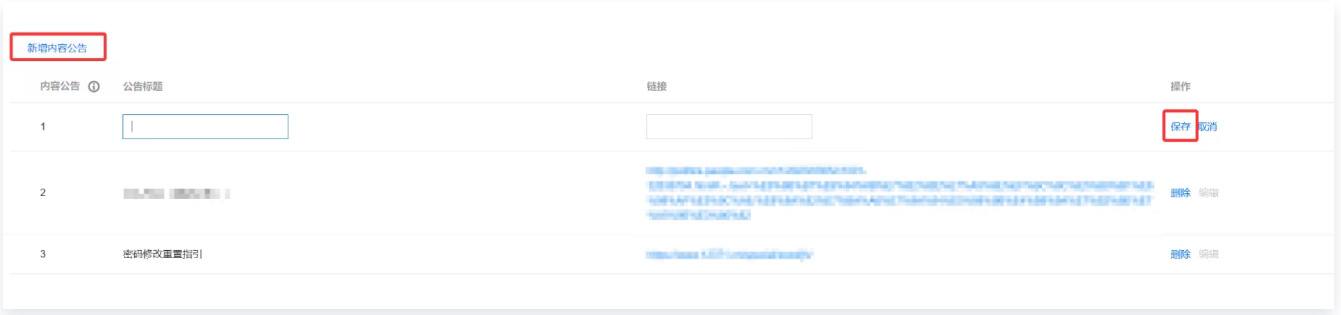


内容公告

1. 员工登录后，在首页公告栏内展示，常用于企业内网行政通知、内网业务指引等。

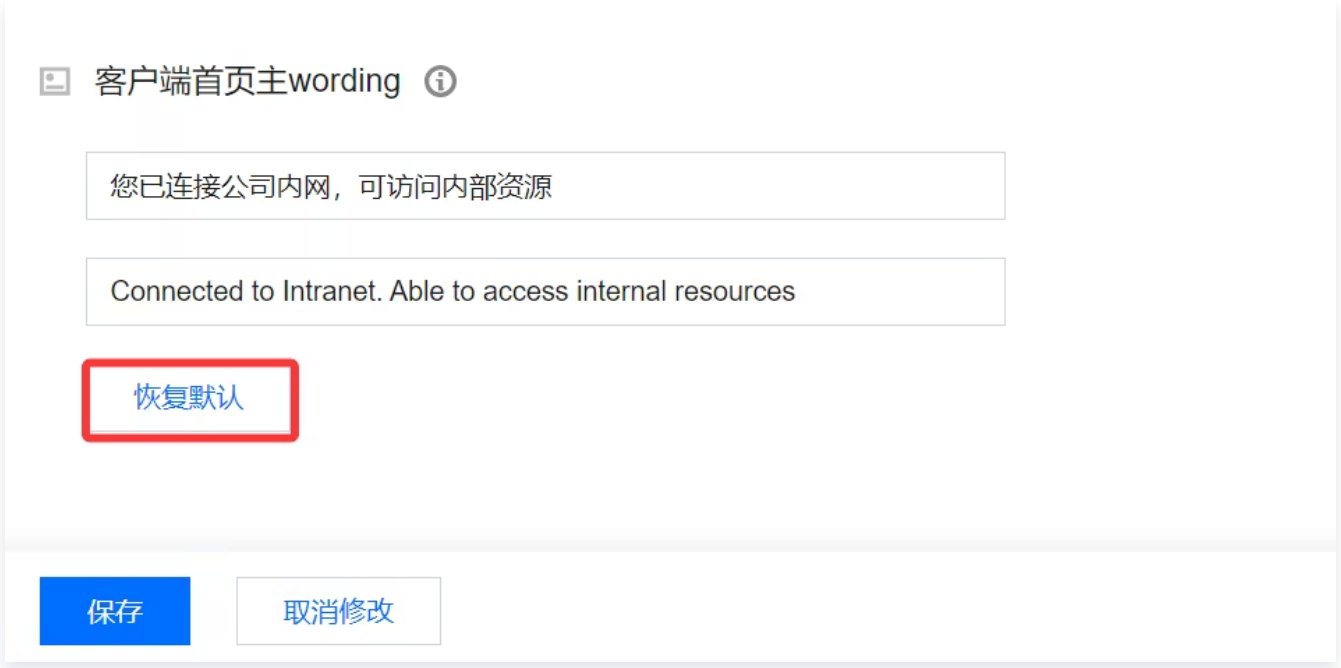


2. 单击**新增内容公告**，填写标题和链接，单击**保存**。



客户端首页主 wording

1. 前往**个性化设置** > **客户端首页**，配置客户端首页主 wording。支持自定义，如无需修改可单击**恢复默认**。



2. 确认内容无误后，单击**保存**。
3. 客户端样式。



Banner库（11.1.1版）

最近更新时间：2026-02-13 09:41:03

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**个性化设置** > **客户端首页**。
2. 在客户端首页，选择**Banner库**，单击**新增**。



3. 上传 976×236 像素的 JPG 或 PNG 格式图片，文件大小需控制在 2MB 以内。如需添加网页链接，请填写完整链接地址。配置完成后单击**确定**保存设置。



4. 前往**客户端运维** > **客户端管理** > 客户端策略 > **客户端自定义**，单击**新建策略**，请参见**客户端自定义**配置文档，将 Banner下发至客户端。



5. 配置完成后，客户端 Banner 示例：


【必读】公司全局公告
您已连接公司内网，可访问内部资源
欢迎使用腾讯iOA
畅享高效、安全、稳定办公体验
办公
杀毒
合规
漏洞
工具
代理模式 全局代理
在线时长：-
企业应用

帮助中心（11.1.1版）

最近更新时间：2026-02-13 17:55:31

> **说明：**
> iOA 零信任安全管理系统（SaaS）11.1.1版本灰度发布中，当前暂未全量更新。
> 如您需体验11.1.1新版本功能，请通过 在线支持 确认您的企业是否已在开放名单中，或提交新版本体验申请。如有任何疑问，请随时联系我们的技术支持团队。

当终端存在不合规项时，帮助中心可通过定制指引文档引导用户完成修复，提升合规修复效率。

1. 登录 iOA 零信任管理平台控制台，在左侧导航栏，选择**客户端运维** > **个性化设置** > **帮助中心**。
2. 在帮助中心页面，单击**添加分类**。



- 添加分类：单击**添加分类**，填写分类的中英文名称。
- 若已建分类，您也可单击**添加子分类**，下拉选择一级分类后，填写子分类名称信息后单击**确定**保存。

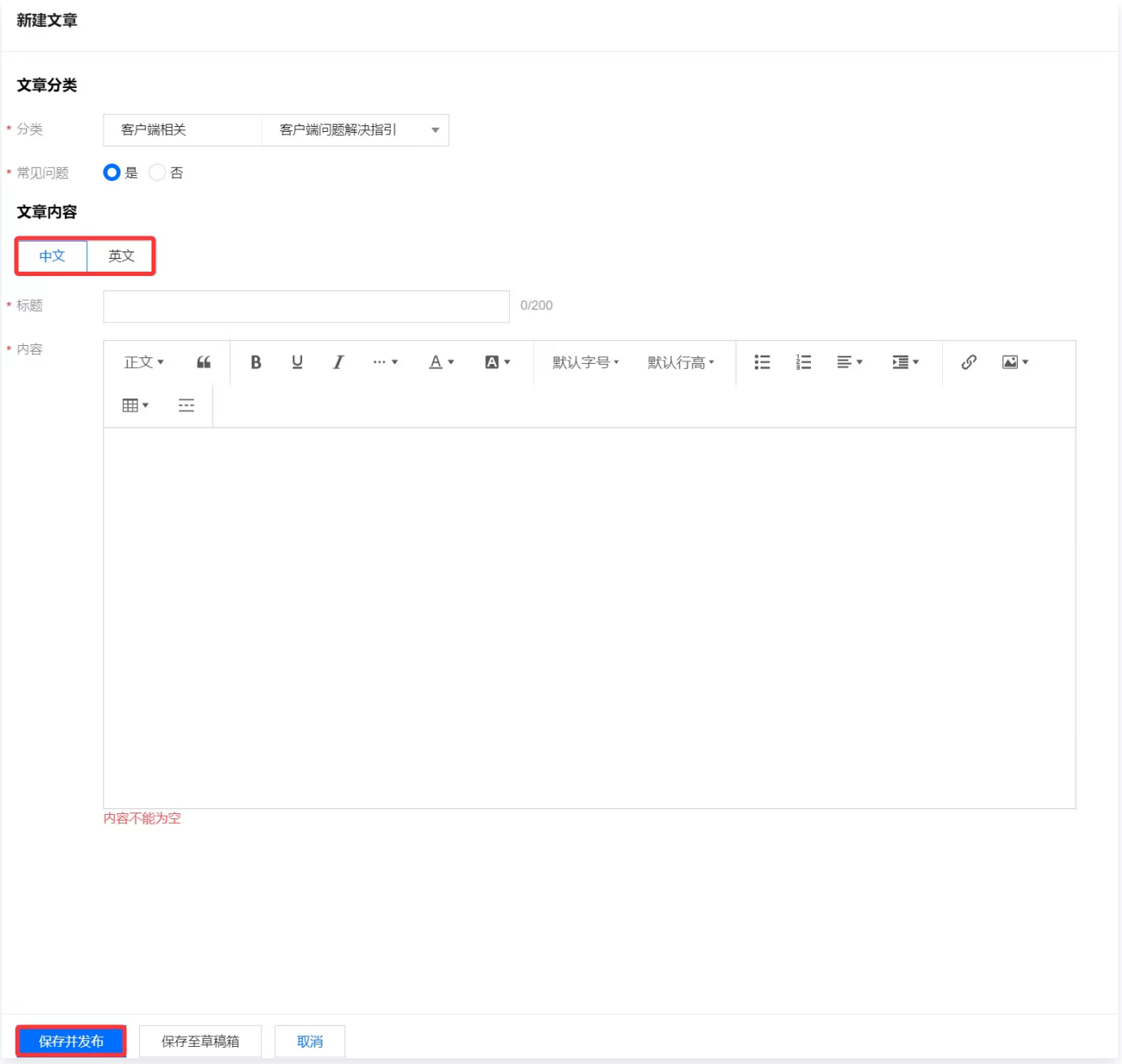


3. 创建分类完成，单击**添加文章**，将文章发布在该分类下。



4. 在新建文章页，填写文章分类、文章内容等信息，并将文档内容的中/英文配置完成后单击**保存并发布**。

> **说明：**
> - 常见问题请任意选择是或者否，因为在 iOA 客户端合规页展示时无明显区分。
> - 当填写完中文文章内容后，必须接着填写英文文章内容，填写完成后，方可保存并发布。



5. 前往**资产管理** > **终端管控** > 合规检测 > **策略配置**，单击**新建策略**，配置修复指引时关联帮助中心的文档。



6. 以加密磁盘策略为例：开启策略开关后，单击**添加检测点**。



7. 是否关联修复文档处，单击**关联**，选择对应已编辑好的文档即可。



8. 当客户端提示检测不合规时，可引导用户完成修复，提升合规修复效率。

