iOA 零信任安全管理系统

常见问题

腾讯云

【版权声明】

【商标声明】

【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

常见问题
私有化版
终端安全管控场景

最近更新时间：2025-01-15 22:00:54

如何控制终端上安装指定的软件?

iOA 无法强制用户终端安装指定软件，但可以在**终端安全策略** > **终端管控** > **合规检测**页面通过设置合规检查功能，检查用户终端是否已安装必备软件。
支持配置用户未安装指定软件，禁止使用无边界接入（NGN）功能，通过限制用户访问业务资源的方式引导终端用户安装指定软件。

终端的合规检测触发时机是怎么样的?

合规检测的触发时机包含 iOA 客户端启动时、打开客户端主界面时、以及管理员配置的定时检测周期触发时；管理员可以配置最短每隔5分钟进行一次合规检测扫描。

配置了终端安全策略，为什么没有在终端上立即生效?

1. 策略配置完成后，可能需要2~4分钟时间下发到用户终端，此时会有一定时间差；您可以在**策略中心** > **终端安全策略**页面查看各策略下发状态。

2. 用户终端持续未接收到策略或策略未能有效执行，请使用客户端上的诊断工具，进行诊断后打包日志 联系我们 。

终端安全策略是否可以不依赖于登录或者用户维度进行管控?

终端安全策略主要是面向用户终端生效的策略内容，可以基于终端维度进行策略配置，也可以基于用户维度进行策略配置。
在**策略中心** > **终端安全策略**的新建策略页面，添加适用范围时根据企业实际需要进行下发策略对象的选择。

- 下发给终端时，策略会指定到具体的终端上。
- 下发给用户时，策略会根据用户登录行为，下发到被登录的终端上。

iOA 的病毒库、漏洞库的更新机制是怎么样的?

iOA 的病毒库和漏洞库由腾讯安全的专业运营人员持续运营，一般情况下，病毒库每周更新至少2次；漏洞库每月至少更新2次；企业客户的终端会自动请求更新到云上最新版本的病毒库、漏洞库。

部分文件需要免查杀的白名单，如何配置?

在**终端安全策略** > **安全防护** > **病毒查杀**页面新建病毒查杀策略时，云信任区添加对应文件即可。

> **说明:**
> MD5 为半文校验。


新建病毒查杀策略
基本信息
适用范围
编辑策略
社工防护引擎 未启用，继承其他策略或基线策略
云引擎查杀设置 未启用，继承其他策略或基线策略
病毒云查杀计划 未启用，继承其他策略或基线策略
网络路径扫描 未启用，继承其他策略或基线策略
定时杀毒扫描结果处理 未启用，继承其他策略或基线策略
病毒查杀引擎策略 未启用，继承其他策略或基线策略
病毒查杀资源占用策略 未启用，继承其他策略或基线策略
终端病毒样本文件自动上传 未启用，继承其他策略或基线策略
风险项信任操作提醒 未启用，继承其他策略或基线策略
客户端信任管理权限 未启用，继承其他策略或基线策略
TAV引擎病毒库升级设置 未启用，继承其他策略或基线策略
云信任区 未启用，继承其他策略或基线策略
文件与路径白名单
备注
操作
（结尾有“\”表示路径，无“\”表示文件）
可以填写备注信息，可为空
添加
扩展名白名单
备注
操作
（输入以“.”开头的数字或字母）
可以填写备注信息，可为空
添加
MD5白名单
备注
操作
输入32位长度的数字和字母
可以填写备注信息，可为空
添加
上传
注册表白名单
备注
操作
（结尾有“\”表示路径，无“\”表示键）
可以填写备注信息，可为空
添加
URL和IP地址白名单
备注
操作
（示例：http://www.qq.com/ 或 192.168.1.1）
可以填写备注信息，可为空
添加
风险名白名单
备注
操作
（示例：Malware.Win32.Gencirc.abcd）
可以填写备注信息，可为空
添加
云隔离区 未启用，继承其他策略或基线策略
保存
取消

操作指引相关
用户与授权管理

最近更新时间：2024-06-08 06:14:42

如何导入第三方用户源?

详情请参见 iOA 私有化企业微信对接 。

什么是自建账户目录?

在创建目录时选择不导入架构，用户需要通过手动或批量导入的方式在该目录中创建。
如果企业习惯于从用户维度管理终端安全策略，例如，一直采用 AD 域控方式进行安全策略的配置和管理，建议导入身份源。

1. 在**管理中心** > **用户与授权管理**页面，单击**新建**，根据企业身份源选择对应的导入类型。

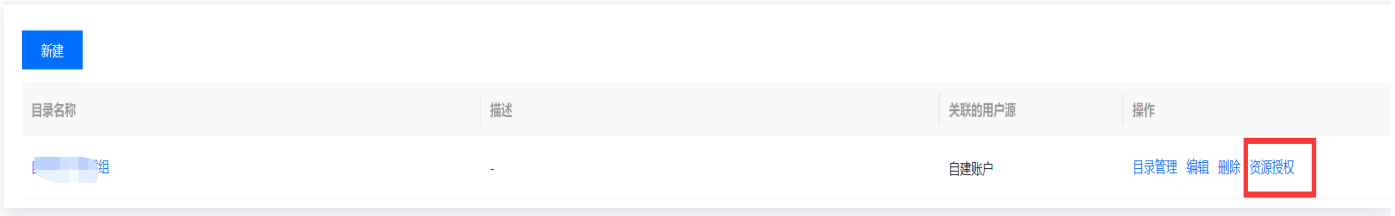
2. 在**终端管理** > **终端信息** > **终端树**页面，单击 + 选择**添加分组**。

3. 在分组管理窗口中，输入分组名称，上级分组选择**全网终端**，配置其他参数，单击**确定**。

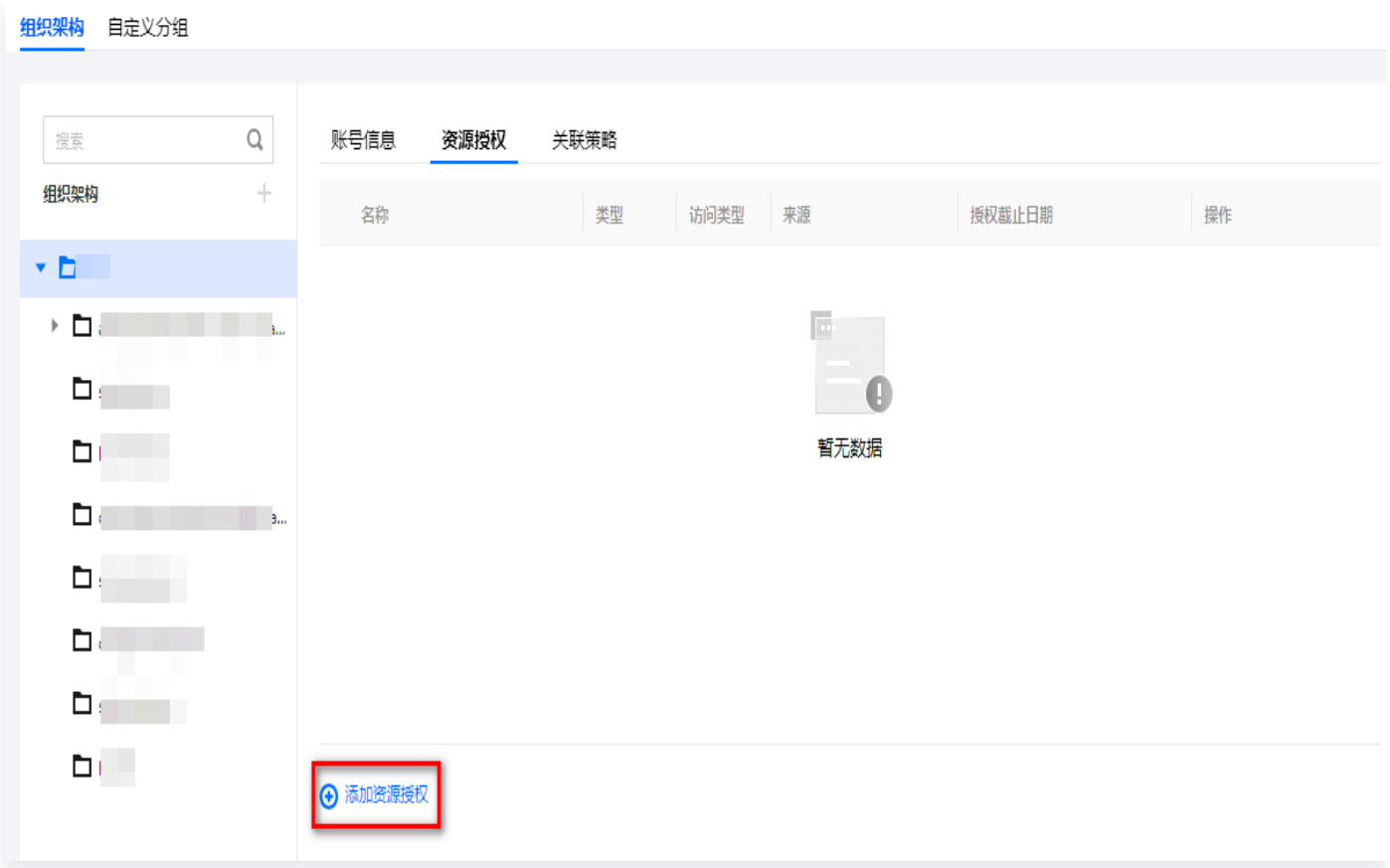
4. 在终端信息页面，选择已经创建好的分组，单击•••，选择**导入账户组织架构**。

在哪里进行资源授权?

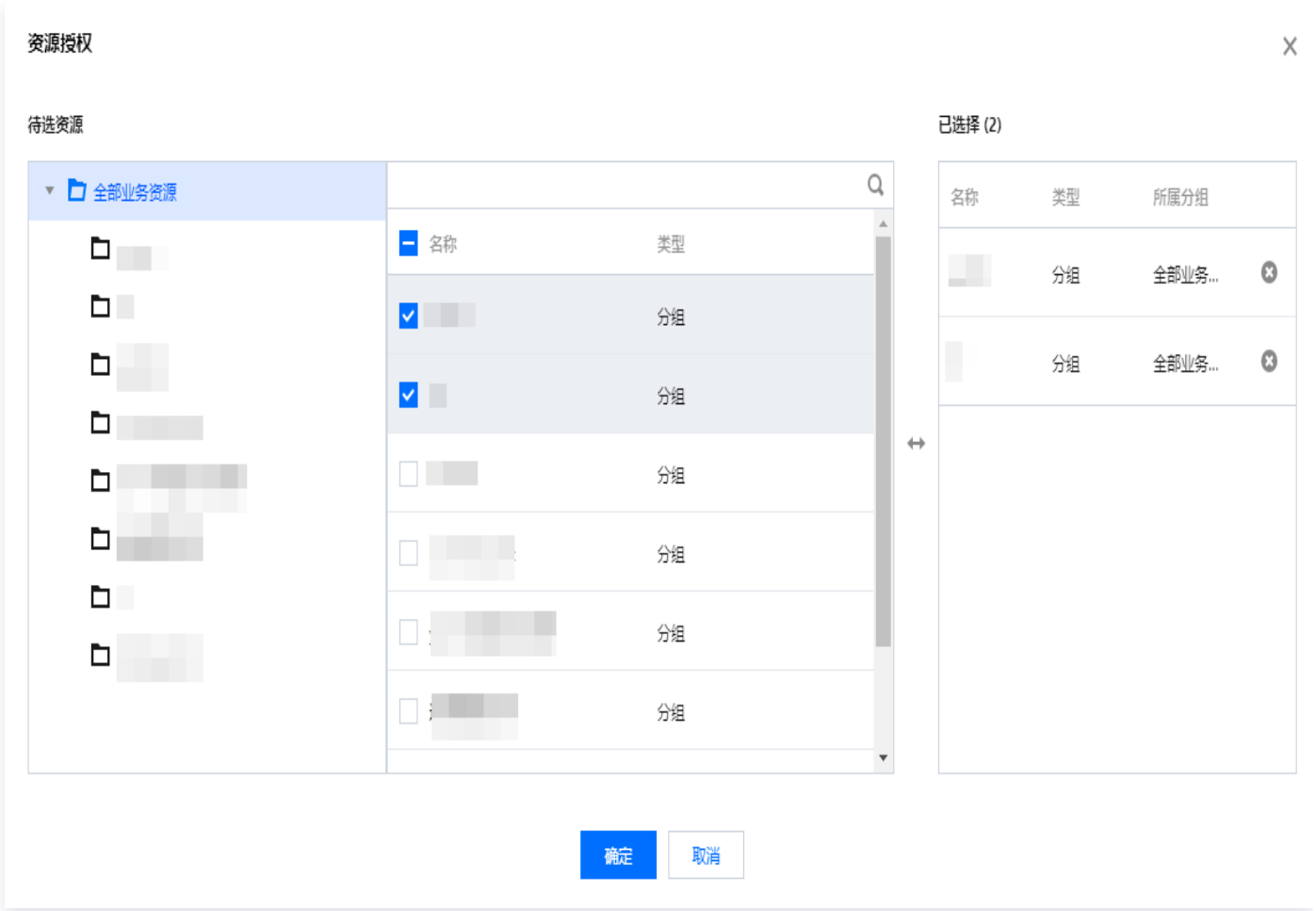
1. 在**管理中心 > 用户与授权管理**页面，选择目标目录，单击**资源授权**。



2. 在目录详情页面，单击**添加资源授权**。



3. 在资源授权窗口中，选择所需资源，单击**确定**。



用户登录时为什么要先选用户目录?

不同目录之间互相隔离，用户来源不同，选择对应的目录才可以正确匹配账户密码。

> **说明:**
> 目录只需要选择一次，登录成功后系统会记住上次选择的目录。

认证源配置

最近更新时间：2025-01-15 22:00:54

什么是认证源实例，如何配置?

1. 认证源实例是指企业客户在 iOA 控制台上配置的企业在用的认证源方式。配置完成后，可以在身份安全策略中使用。终端用户登录时，会通过配置的认证源方式进行身份校验。
2. 目前 iOA 支持多种认证源对接，包含：扫码认证、短信认证、邮箱认证、IAM 认证、AD 认证、Token 认证、OTP 认证。相关认证源配置指引请参见 认证对接 。

如何启用双因素认证策略?

在**身份安全策略** > **认证安全** > **认证策略**页面，选择所需目录的认证策略，单击**编辑**并启用双因素认证。

什么是挑战认证?

挑战认证是指当用户在特定条件下（时间、网络位置、发起访问的程序等）访问接入 iOA 的业务时，需再次进行登录认证，实现挑战认证要进行如下配置：

- 在**身份安全策略 > 认证安全 > 认证策略**页面，选择所需目录的认证策略，单击**编辑**并选择挑战认证方式认证源。

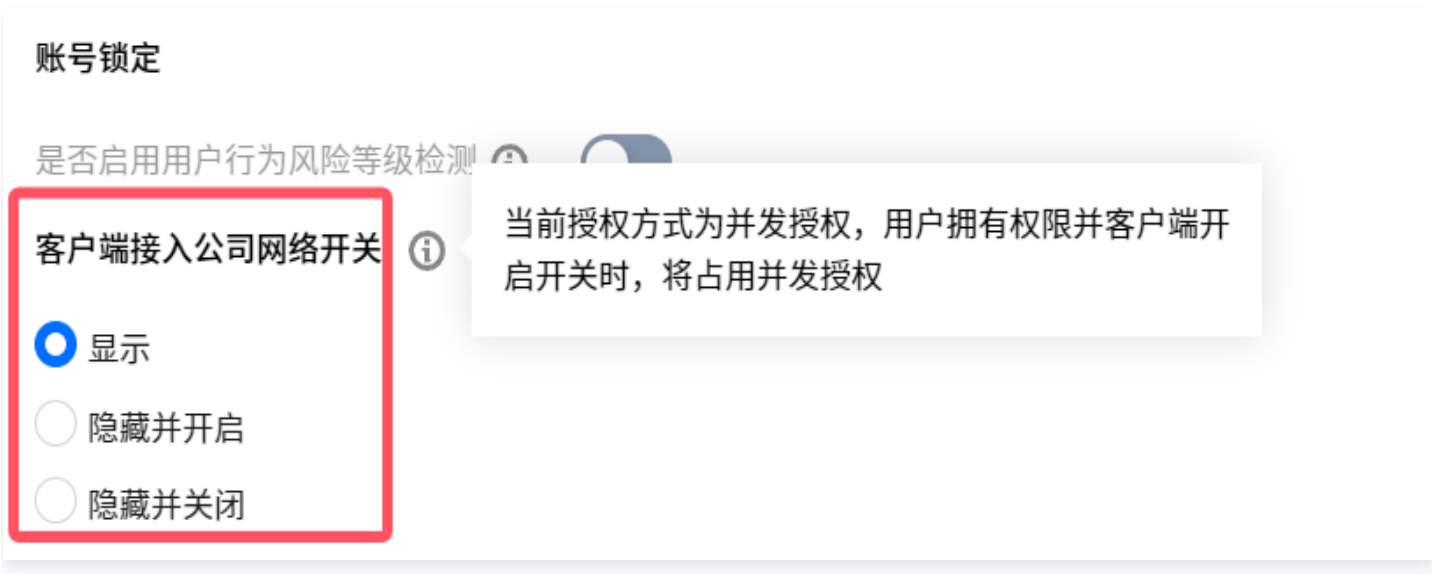
- 在**访问安全策略 > 业务资源访问 > 访问安全策略**页面，添加访问安全策略，访问策略设置为**挑战认证后可访问**。

如何查看登录日志?

您可单击**日志审计** > **身份安全日志**进行查看。

用户登录后就会占用并发账号授权吗?

是的，当用户登录并在客户端上启用“接入公司网络”开关时，将会占用一个并发登录账号授权；您可以在**身份安全策略** > **账号安全** > **账号策略**页面，配置用户是否默认开启该开关。


账号锁定
是否启用用户行为风险等级检测
客户端接入公司网络开关
当前授权方式为并发授权，用户拥有权限并客户端开启开关时，将占用并发授权
显示
隐藏并开启
隐藏并关闭

业务资源管理

最近更新时间：2024-06-08 06:14:42

隧道资源和 Web 资源有什么区别?

1. 隧道资源支持 B/S、C/S 架构应用。必须安装 iOA 客户端才能进行资源访问，且仅支持通过业务后端地址进行访问。
2. Web 资源仅支持 B/S 架构应用。无需安装 iOA 客户端，可使用浏览器等方式访问业务，支持通过前端地址、自定义域名进行资源访问，不支持通过后端地址进行访问。

为什么 Web 资源没有在客户端显示?

Web 资源暂时不支持下发到客户端首页上。

如何为 Web 资源配置自定义域名?

1. 在**访问配置管理** > **业务资源管理**页面，单击**添加资源**，选择 **Web 资源**，在Web 资源中添加自定义域名。
2. 如自定义域名使用 HTTPS 进行访问，则选择对应域名 SSL 证书。

3. 在公网 DNS 解析平台，将自定义域名设置 CNAME 解析至该 Web 资源前端域名上。

SaaS 版
基本介绍

最近更新时间：2023-10-23 10:53:12

iOA 零信任安全管理系统是什么?

iOA 零信任安全管理系统是腾讯终端安全团队针对企业安全上云和数字化转型，提供的企业网络边界处的应用访问管控系统，为企业应用提供的统一、安全、高效的访问入口，同时提供终端安全加固、软硬件资产管理、文件/文件夹控制、外设控制审计、杀毒等终端安全管理模块。
在恶意威胁进入企业网络之前，可以监测和阻断病毒、木马入侵等各种恶意攻击，防止公司敏感数据泄露。iOA 零信任安全管理系统支持公有云和本地云部署模式，切实解决企业应用在边界处的安全访问问题。

iOA 零信任安全管理系统的技术原理是什么?

iOA 零信任安全管理系统通过应用层数据安全防护（防病毒、脱敏、安全加固等）+身份认证技术，授权用户可访问客户端集成的内网业务，可实现对访问者和访问资源的细粒度控制，以单个应用为最小控制单元，对网络边界的访问行为进行精准控制。

如何登录 iOA 零信任安全管理系统?

可通过平台 申请代理体验 iOA 零信任安全管理系统，申请审核通过之后，iOA 零信任安全管理系统团队将与您联系，并确认需求和商务洽谈。

如何通过 iOA 零信任安全管理系统访问企业资源?

安装 iOA 零信任安全管理系统客户端后，通过 iOA 零信任安全管理系统模块入口进行身份认证，包含企业微信扫码、token 双因子认证以及 LDAP、HTTP、本地身份、域身份等多种用户认证方式。

本地部署模式下，iOA 零信任安全管理系统对于服务器、存储、网络等资源有何具体要求?

一般需要根据客户实际业务场景和业务访问量来衡量服务器等资源需求，最小服务器资源投入数量不小于1台。

场景指引相关
终端安全管控场景

最近更新时间：2025-03-19 15:41:54

如何控制终端上安装指定的软件?

iOA 无法强制用户终端安装指定软件，但可以在 **终端管控** > **合规检测**页面通过设备合规检查功能，检查用户终端是否已安装必装软件。
如果您使用的是高级版，可以配置用户未安装指定软件，禁止使用无边界接入（NGN）功能，通过限制用户访问业务资源的方式引导终端用户安装指定软件。

终端的合规检测触发时机是怎么样的?

合规检测的触发时机包含 iOA 客户端启动时、打开客户端主界面时、以及管理员配置的定时检测周期触发时；管理员可以配置最短每隔5分钟进行一次合规检测扫描。

配置了终端管控策略，为什么没有在终端上立即生效?

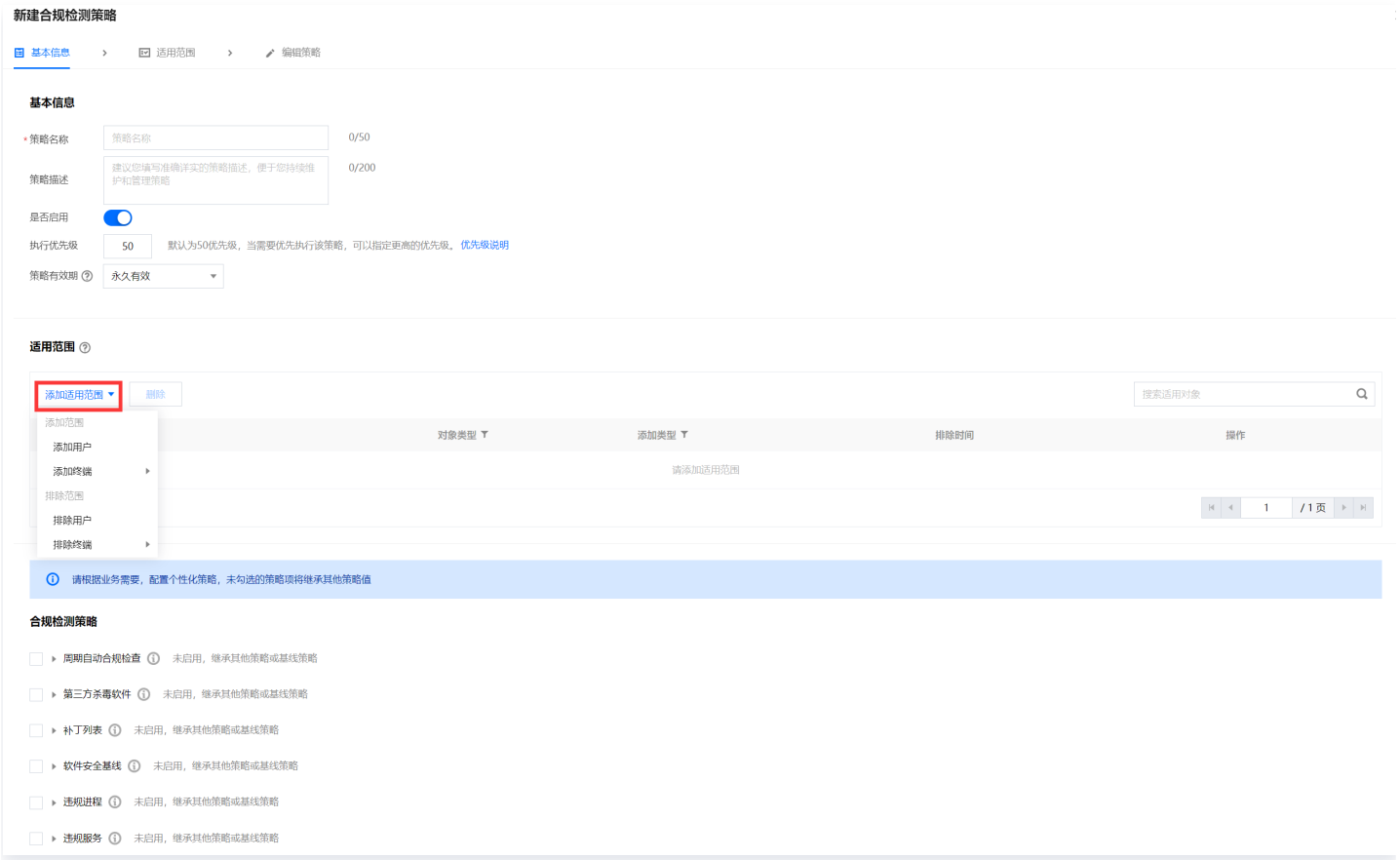
1. 策略配置完成后，可能需要2~4分钟时间下发到用户终端，此时会有一定时间差；您可以在策略列表上查看策略下发状态。

2. 用户终端持续未接收到策略或策略未能有效执行，请使用客户端上的诊断工具，进行诊断后打包日志 **联系我们** 。

终端管控策略是否可以不依赖于登录或者用户维度进行管控?

终端管控策略主要是面向用户终端生效的策略内容，可以基于终端维度进行策略配置，也可以基于用户维度进行策略配置。
在新建配置页面，添加适用范围时根据企业实际需要进行下发策略对象的选择。

- 下发给终端时，策略会指定到具体的终端上。
- 下发给用户时，策略会根据用户登录行为，下发到被登录的终端上。



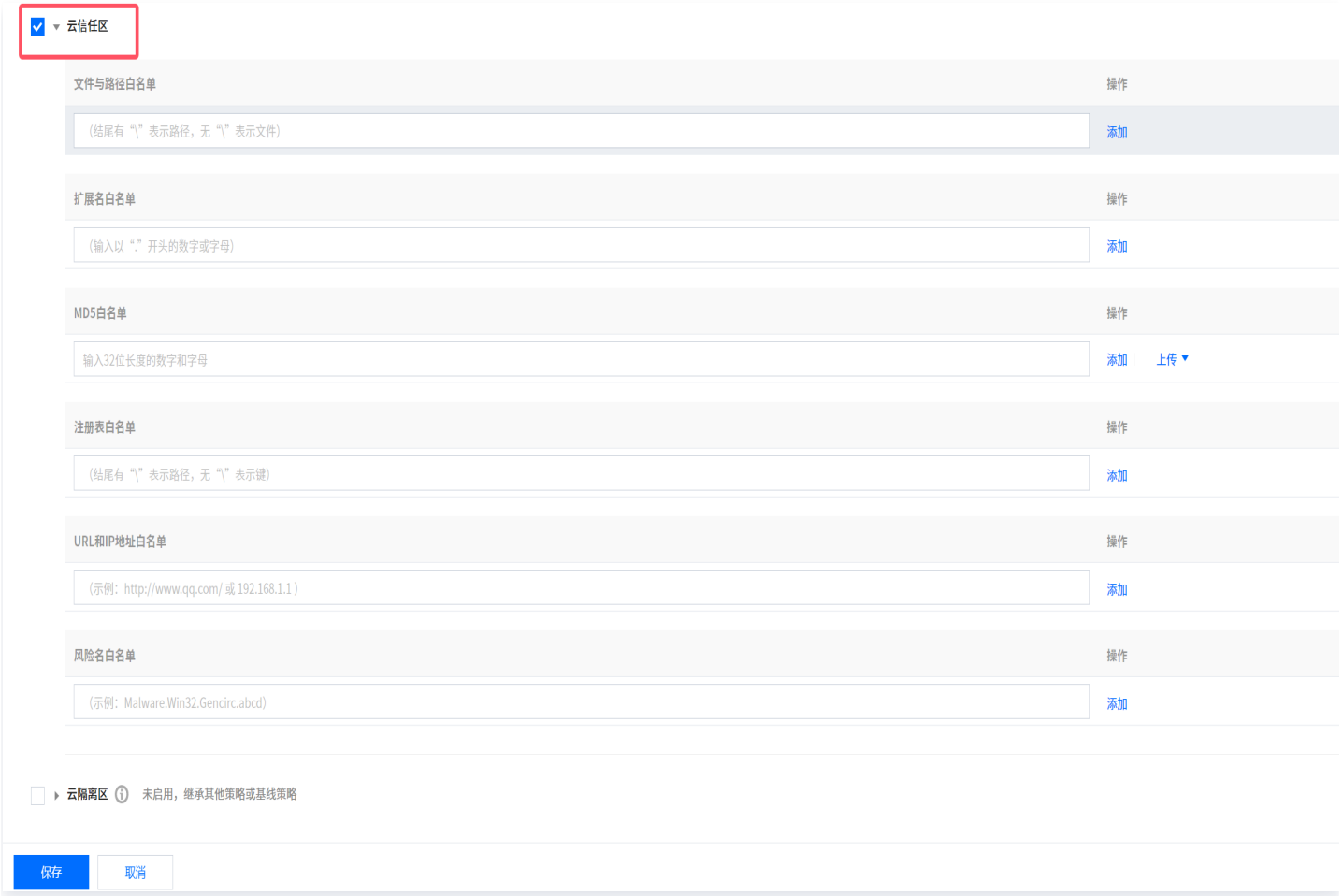
iOA 的病毒库、漏洞库的更新机制是怎么样的?

iOA 的病毒库和漏洞库由腾讯安全的专业运营人员持续运营，一般情况下，病毒库每周更新至少2次；漏洞库每月至少更新1次；企业客户的终端会自动请求更新到云上最新版本的病毒库、漏洞库。

部分文件需要免查杀的白名单，如何配置?

在 规则运营 页面新建病毒查杀策略时，云信任区添加对应文件即可。

> **说明：**
> MD5 为半文校验。


云信任区
文件与路径白名单
操作
(结尾有“\”表示路径，无“\”表示文件)
添加
扩展名白名单
操作
(输入以“.”开头的数字或字母)
添加
MD5白名单
操作
输入32位长度的数字和字母
添加
上传
注册表白名单
操作
(结尾有“\”表示路径，无“\”表示键)
添加
URL和IP地址白名单
操作
(示例：http://www.qq.com/ 或 192.168.1.1)
添加
风险名白名单
操作
(示例：Malware.Win32.Gencirc.abcd)
添加
云隔离区
未启用，继承其他策略或基线策略
保存
取消

防勒索防入侵场景

最近更新时间：2025-03-13 10:37:32

如何通过 iOA 有效防御勒索病毒攻击?

iOA 基于勒索攻击链（爆破入侵-破坏杀软-病毒运行-加密数据-横向移动）构建五维立体化防御体系，覆盖全生命周期。

使用场景	详情
阻断入侵控制	• 爆破防护：RDP二次身份认证（动态验证码），即使账密泄露也无法登录。 • 端口隐藏：关闭非必要暴露端口，减少攻击面。
防杀软破坏	• 内核级自保护：禁止非法终止 iOA 进程，卸载需管理员密码授权。 • 异常退出告警：实时推送进程强退事件至管理端。
拦截加密行为	• 智能诱饵：在关键目录部署隐藏诱饵文件，首个被加密时立即阻断进程。 • 行为分析：识别高危动作（如删除卷影副本、批量修改文件头），实时拦截。
数据无损恢复	• 双备份机制：卷影备份（实时快照）+ 无格式备份（分布式存储），支持加密/误删文件还原。 • 解密支持：内置100+勒索病毒解密工具，覆盖 Phobos、WannaCry 等主流家族。
抑制内网扩散	• 横向渗透防护：拦截远程命令执行、敏感共享目录访问等12类横移行为。 • 域控加固：防御 Kerberos PTH 攻击、伪造票据等域渗透手法。

如何查看终端上受到勒索攻击的记录和日志信息?

您可以通过单击 网络攻击日志，查看终端上受到勒索攻击的相关记录和日志信息。

iOA 五维防勒索体系的核心优势是什么?

1. 防控制设备：RDP二次认证阻断爆破。
2. 防破坏杀软：内核级自保护防卸载。
3. 防加密行为：诱饵拦截+三大检测引擎。
4. 防数据损失：双备份机制（卷影+无格式备份）。
5. 防内网扩散：12种远程命令攻击拦截+域控防护。

iOA 如何应对人工入侵式攻击（如 RDP 爆破）?

提供三重防护：

1. 爆破前：隐藏端口+密码加固。
2. 爆破中：行为关联分析拦截。
3. 爆破后：RDP 二次认证（需身份验证码），确保账密泄露仍无法登录。

遭遇勒索攻击后应如何快速止损?

遵循三步原则：

1. 隔离：断网防止横向扩散 。
2. 溯源：检查 爆破日志 、异常进程（如 ProcessHacker）。
3. 恢复：使用 iOA 文档守护 备份或联系腾讯安全专家解密。

为什么有些勒索病毒没有被 iOA 检出?

1. 无论是勒索病毒还是其他类别的木马病毒，在传播过程中都会有针对安全软件的对抗，所以无论哪款安全软件追求高查杀率，都无法保证100%查杀和无误报两个目标。
2. 针对勒索攻击的防御，iOA 的思路一直是不能局限在勒索病毒的检测上，即使能100%检出勒索病毒，也无法阻止主流勒索攻击方式--人工入侵控制设备，破坏安全软件防御后投毒。

多分支场景

最近更新时间：2024-03-28 17:43:31

连接器所在机器的推荐配置是什么?

Centos7.6 CPU：2-4核，内存4-8G，硬盘100G以上；建议最少部署2个连接器实现高可用。

如何放通网络?

1. 确保连接器所在机器的防火墙已经放通 iOA 网关地址。
2. 确保连接器所在网络出口防火墙已经放通 iOA 网关地址
3. iOA 网关地址可前往 专线管理页面 上获取。

连接器部署如何命令 Windows 版?

双击 connector.exe 程序运行即可。

连接器部署如何命令 Linux 版?

依次输入如下命令：

```
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
```

连接器部署如何配置开机自启动服务 Windows 服务?

- 双击 connector.exe 程序运行时已自动设置开机自启动。
- 如需手动设置，命令提示符 cmd 中进入连接器所在目录，依次输入如下命令：

```
connector.exe -h 回车 //查看安装、卸载命令
connector.exe install 回车  //执行安装命令
start connector?lY/N：选择 Y 回车  //同意安装
NET START connector //启动服务
```

连接器部署如何配置开机自启动服务 Linux 服务?

- 安装连接器时已自动配置开机自启动。
- 如需手动设置请参考以下命令：

  1.1 进入连接器所在的目录执行 `./connector install` 。

1.2 启动服务 `systemctl start connector` 。

1.3 检查服务状态 `systemctl status connector` 。

如何通过 iOA 快速实现多分支机构快速接入?

1. 根据不同分支机构，支持配置如下：
   1.1 配置一个或多个用户目录，不导入组织架构（手动自建账密方式）。
   1.2 配置一个或多个专线分组（不同分支机构对应一个或者多个专线分组），在专线分组中创建专线，将专线部署在对应分支机构内网服务器上。
   1.3 配置一个或多个资源分组（不同分支机构资源对应一个或者多个资源分组），添加资源时绑定对应分支机构的专线组。
2. 对用户进行资源授权。

同传统的 SD-WAN 相比，iOA 使用的多分支接入有什么优点?

- 高可靠性：iOA 提供了冗余路径和备用连接，以确保在一个分支或连接出现故障时，其他分支仍然可以正常工作。这种冗余性可以提高网络的可靠性和可用性。
- 数据更安全：iOA 可以通过在每个分支点上实施安全策略和加密措施来保护数据的安全性。
- 灵活性和可扩展性：iOA 可以根据组织的需求进行灵活配置和扩展。它可以适应不同的网络拓扑和分支规模，并支持快速部署和管理。

云上业务安全访问场景

最近更新时间：2025-03-13 10:37:32

业务云化后，为何需要采用 SaaS 化安全访问服务?

- 成本优化：替代传统私有化部署，减少 IDC 机房维护成本。
- 敏捷适配：动态扩展云资源，匹配业务弹性需求。
- 统一管控：集中管理多云/混合云环境的安全策略，降低运维复杂度。

当业务资源分布在多个网络、地域或机房时，如何实现统一连接?

您可通过配置多个专线分组，将不同网络（如公有云、私有云、本地 IDC）的业务资源划分到对应分组中。在每个分组内添加专线，并部署专线连接器至目标机器，实现跨网络、跨地域的安全连接。

连接器应部署在什么位置? 是否支持多 IDC 共享?

- 部署要求：部署在可同时访问内网业务资源与 iOA 云上网关的服务器。
- 若多 IDC 网络互通，仅需在任一 IDC 部署连接器即可代理跨机房访问其他 IDC 的业务。

SaaS 应用存在 IP 白名单，如何接入到 iOA 网关访问中?

1. SaaS 应用 IP 白名单添加连接器出口公网 IP 地址。
2. 将连接器部署至可访问 SaaS 应用、iOA 云上网关的机器上。
3. 将 SaaS 应用地址添加到 iOA 资源中，绑定对应连接器。

如何在客户端首页添加企业业务资源的快捷入口?

1. 单击 客户端首页，在此页面中，添加业务资源对应的站点域名或 IP。
2. 目前仅支持将隧道应用的URL下发至客户端首页。
3. 用户仅能查看到其已被明确授权的业务资源站点。未被授权的站点资源（如未分配权限或权限过期）不会在客户端首页展示，实现“最小权限”访问控制。

如何配置内网直连与公网代理的智能切换?

1. 内网直连条件：终端 IP 属于在 企业内网管理 中配置的企业公网 IP 段； 业务资源配置 中勾选“启用内网直连”。
2. 公网代理触发：非内网 IP 终端自动通过 iOA 网关访问。

直连白名单的作用是什么?

白名单内的 IP 地址（业务地址）无论终端位于内网还是外网，均直连访问；适用于核心数据库等无需代理的高安全业务。

为什么业务大部分是正常的，但 iOA 资源连通性大部分显示为未检测？

全端口隧道资源会显著增加连接器对业务连通性探测的压力。如果业务无需全端口隧道，建议改为精确配置所需端口。此操作仅影响业务连通性的展示效果，不会对实际业务访问产生任何影响。

轻量化移动办公场景

最近更新时间：2024-03-28 17:43:31

配置好的 Web 资源，为什么无法访问?

1. 查看连接器所有服务器是否可以正常访问。
2. 检查后端地址子路径是否正确。
3. 业务资源中尝试配置 Host。

> **说明：**
> 仅配置 host 地址，请勿添加端口信息。

Web 资源的前端地址和后端地址指的是什么？如何配置?

1. 后端地址为连接器去访问的地址（内网或业务网中可以访问的地址或域名）。
2. 前端地址为 iOA 提供的安全域名，该域名经过腾讯云 Web 应用防火墙防护，只需要对该域名配置前面的自定义子域即可。

域名已经在 ICP 备案，如果想要在 Web 资源中使用自定义域名的访问方式，是否还需要在腾讯云上二次备案?

需要在腾讯云上二次备案。

如何在企业微信工作台上快速访问 Web 资源?

1. 配置企微身份源和认证源，详情请参见 iOA SaaS 企业微信对接 。
2. 将业务配置为 Web 资源，启用自定义域名配置，将自定义域名在公网 DNS 解析平台做 CNAME 解析到该资源前端域名。
3. 对用户进行资源授权。
4. 在企微管理后台增加一个自建应用，完成可信域名校验后，将应用主页设置为配置在 iOA 上的自定义域。

Web 资源的前端地址和后端地址对于端口是否有限制?

1. Web 资源不限制后端地址端口。
2. Web 资源前端地址端口仅支持80和443端口。

已安装 iOA 客户端并登录，访问 Web 资源时，为何仍需在浏览器中登录?

Web 资源和隧道资源访问使用了不同的技术方案，因此访问方式也是不同的，二者并无直接关联。

Web 资源是否支持跨域?

支持，业务侧实现跨域则将所需域名和端口配置成 Web 资源即可。

远程接入场景

最近更新时间：2024-03-28 17:43:31

Web 资源和隧道资源有什么区别?

1. 隧道资源支持 B/S、C/S 架构应用。必须安装 iOA 客户端才能进行资源访问，且仅支持通过业务后端地址进行访问。
2. Web 资源仅支持 B/S 架构应用。无需安装 iOA 客户端，可使用浏览器等方式访问业务，支持通过前端地址、自定义域名进行资源访问，不支持通过后端地址进行访问。

是否所有的流量都需要引流到 iOA 网关?

仅接入 iOA 的业务流量会引流到 iOA 网关。

如何理解隧道资源优先级？优先级的作用是什么?

当多个隧道资源存在冲突时（例如：访问资源时，可能同时命中泛域名与精准域名，IP 段或 IP 的场景），此时需要通过资源的优先级来判断，优先命中哪个资源。隧道资源访问的优先级。

1. 隧道资源可以配置泛域名，这个场景下可能存在部分需要直连的域名，可以再单独配置想直连的域名资源调高优先级。
2. 同个隧道资源想走不同的网关。

配置好资源后，为什么无法立即访问?

资源配置到 iOA 控制台后需经过 iOA 网关下发，一般需等待1-2分钟才可进行访问。

客户端支持的代理模式有几种？和我现有的 VPN 冲突了，在测试/灰度阶段应该如何处理?

客户端有3种代理模式：

- 全局代理：所有的流量和访问都走 iOA 进行代理，都通过虚拟网卡进行拦截，根据 IP 查询 iOA 自己的 DNS 进行规则判断是否拦截，在某些终端上可能存在兼容性问题。
- PAC 模式/浏览器代理：浏览器拦截访问请求，转发给 NGN 模块，判断是否拦截，不会启动虚拟网卡。即只有配置到 iOA 后台的隧道资源才会进行引流，其他走直连，通常用于和其他 VPN 的共存过度阶段使用。
- WFP 模式：微软防火墙驱动拦截访问请求，对于请求包进行拦截，然后将请求包转发给 NGN 模块进行规则判断，是否进行代理；因为是微软官方的驱动，兼容性较好，是全局代理的替代方案，但是只能在 Windows 端使用。

如上所述，和现有的 VPN 冲突了，在测试/灰度阶段可使用 PAC 模式/浏览器代理、WFP 模式。

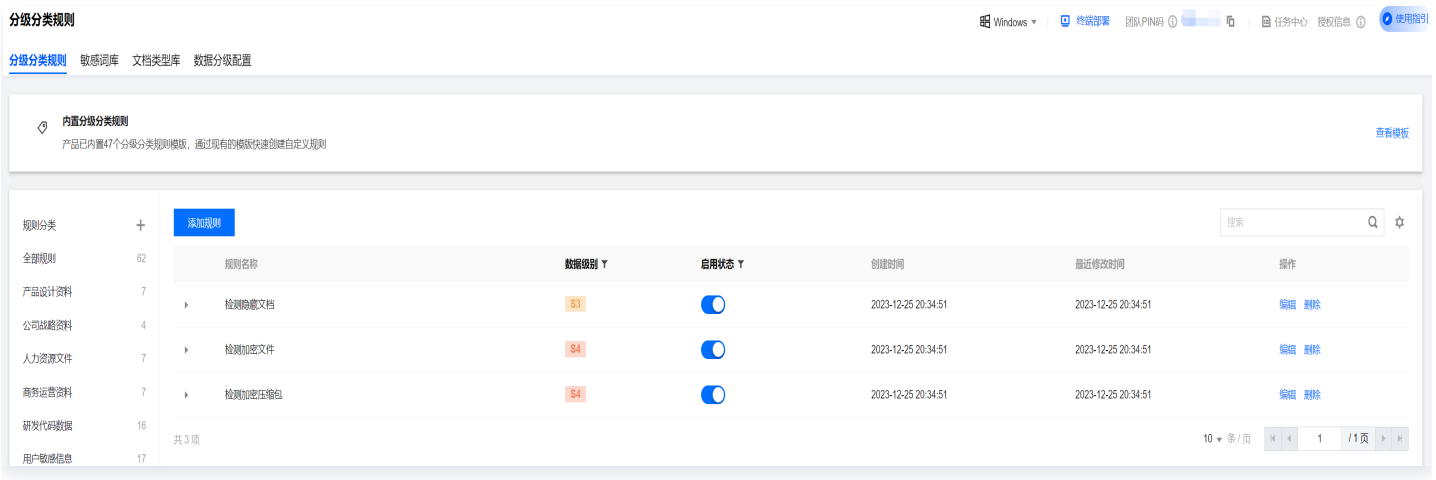
终端数据防泄漏场景

最近更新时间：2025-03-19 15:41:54

员工将敏感文件加密/压缩/改文件后缀名后外发，是否能被检测到?

iOA 目前已内置 分级分类规则，可针对加密/压缩/改文件后缀名等常见绕过手段进行检测，无需特殊配置，仅需在配置拦截、告警策略时勾选对应的分级分类规则。

> **说明：**
> 目前仅支持检测加密的压缩包、Office 文档、PDF 文件，针对加密文件的正文内容暂时不作识别。



如何确保 iOA 检测进程正常运行，无法被用户手动关闭?

iOA 默认开启自保护功能，且默认情况下用户无法关闭自保护功能，因此终端用户无法手动终止 iOA 进程。

对应控制台的策略配置如下：

1. 在 客户端管理页面，单击**新建策略** > **客户端保护策略**，开启客户端自保护，可防止木马恶意破坏。

该配置项以及对应客户端的界面表现如下：

- **若勾选允许客户端修改设置：自保护设置以客户端设置为准，用户在客户端可手动修改是否开启/临时关闭自保护。**

- 若取消勾选（不勾选）允许客户端修改设置：自保护设置以控制台设置为准，客户端自保护按钮置灰，用户无法手动修改/设置客户端自保护模式。

如何针对员工外发的敏感文件取证分析?

1. 外发文件备份：默认情况下，触发了 iOA DLP 模块检测的敏感文件或敏感剪贴板内容均会上传至临时存储空间（10G），另外 iOA 支持对接自购的腾讯云 COS 桶或支持 S3协议的存储服务，可根据实际需求购买存储服务。

> **说明：**
> 1. 需已开启**数据安全策略** > **截屏取证**中对应系统以及对应截屏通道。
> 2. COS 服务器需要有剩余存储空间，默认提供10G的临时存储空间。

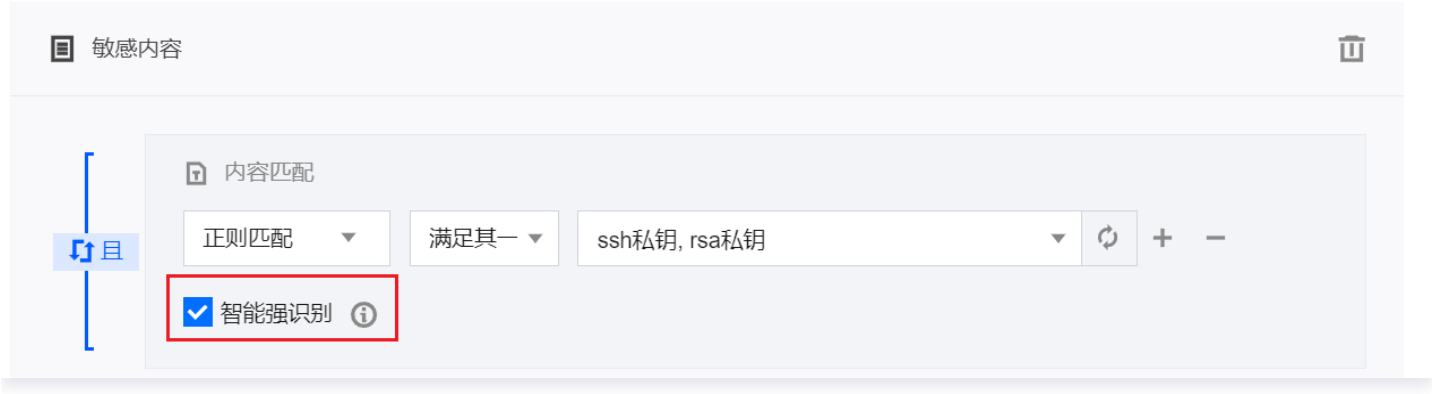
2. 截屏取证：分别在外发动作发生的第一时间和之后2s，4s截取三张屏幕截图，用于事后取证分析。
3. 查看外发详情：在**告警调查审计** > **行为审计**页面， 选择**目标文档外发的告警**，单击操作列的**详情**，可以查看外发的原文件和操作截屏。

如何检测剪贴板或截图文件内容?

iOA 支持剪贴板中敏感文字和屏幕截图的识别和检测，针对屏幕截图会使用 OCR 技术提取文字内容并检测是否包含敏感信息。

若 分级分类规则 需要应用于剪贴内容的识别，需要开启**智能强识别**功能。

分级分类规则



操作指引相关
用户与授权管理

最近更新时间：2025-05-08 14:15:33

如何导入第三方用户源?

详情请参见示例： iOA SaaS 企业微信对接-身份源配置 。

什么是自建账户目录?

创建目录时选择创建自建账户，在该目录需要通过手动创建或批量导入的方式添加用户。

终端安全版本也需要导入用户源吗?

终端安全版并非必须要导入用户源，可以通过终端列表的终端树（终端目录架构）维度进行终端管控及安全策略下发。

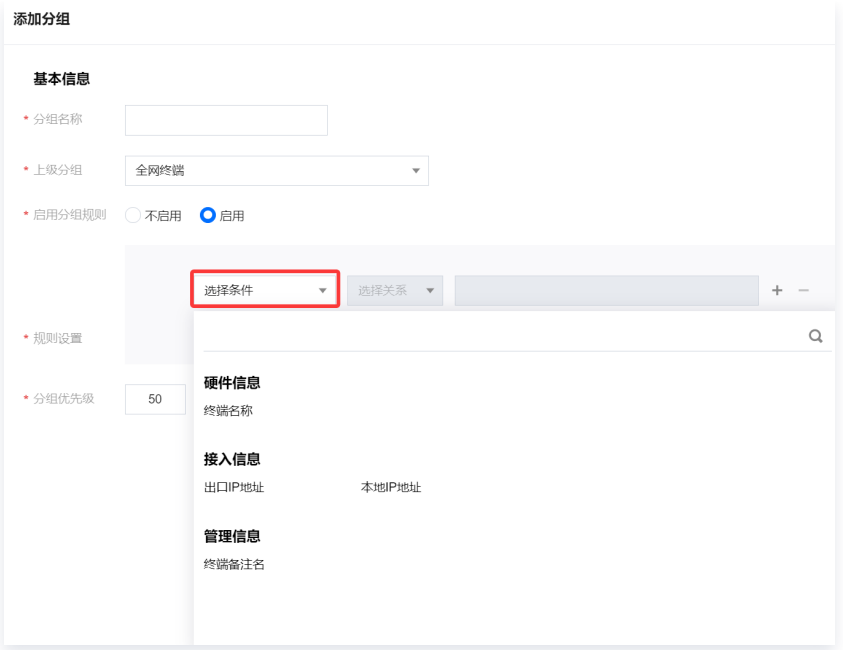
如果企业本身习惯于用户维度管理终端安全策略，例如：企业本身一直采用 AD 域控方式进行安全策略配置管理，建议导入身份源。

1. 在 用户与授权管理页面 ，导入企业身份源。

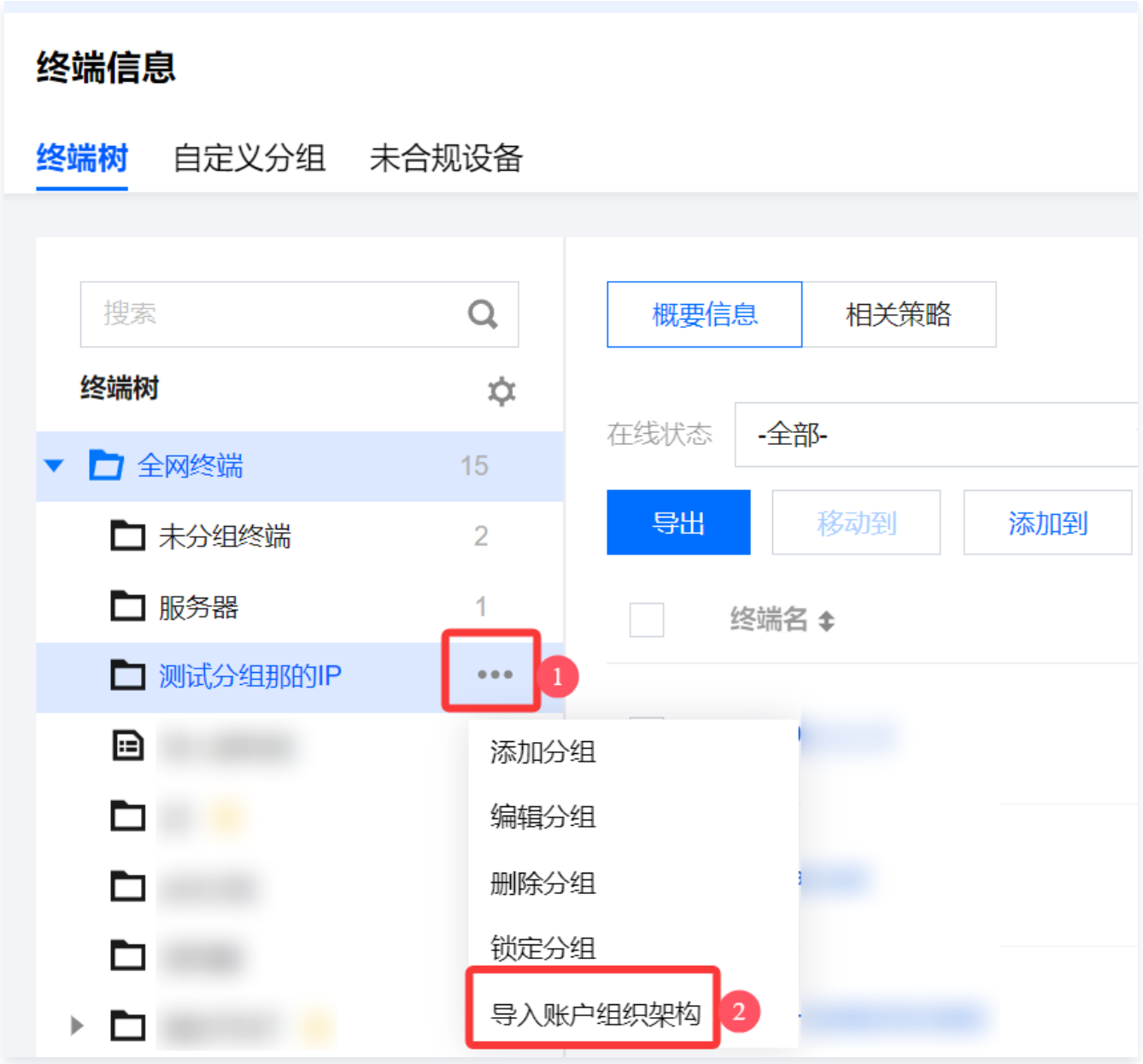
2. 在 终端信息页面，单击⚙，选择添**加分组**。

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。（**此处选择不启用**） • 启用：终端树分组支持根据本地 IP、终端名称、终端备注名设定分组规则，终端设备将根据这些分组规则自动归入相应的指定分组。



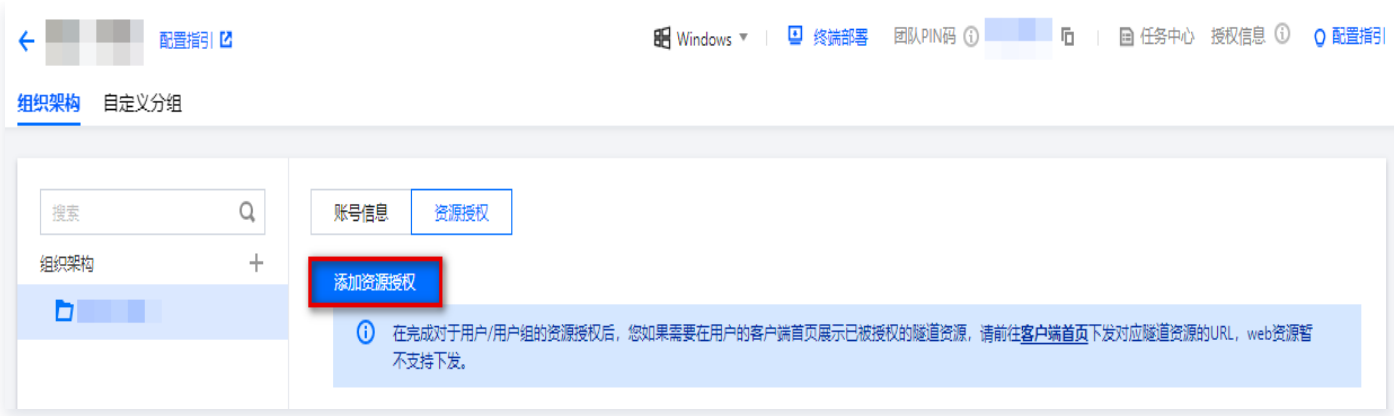
4. 在终端信息页面，选择已经创建好的分组，单击 ••• ，选择**导入账户组织架构**，导入目录后该目录会与组织架构信息同步。



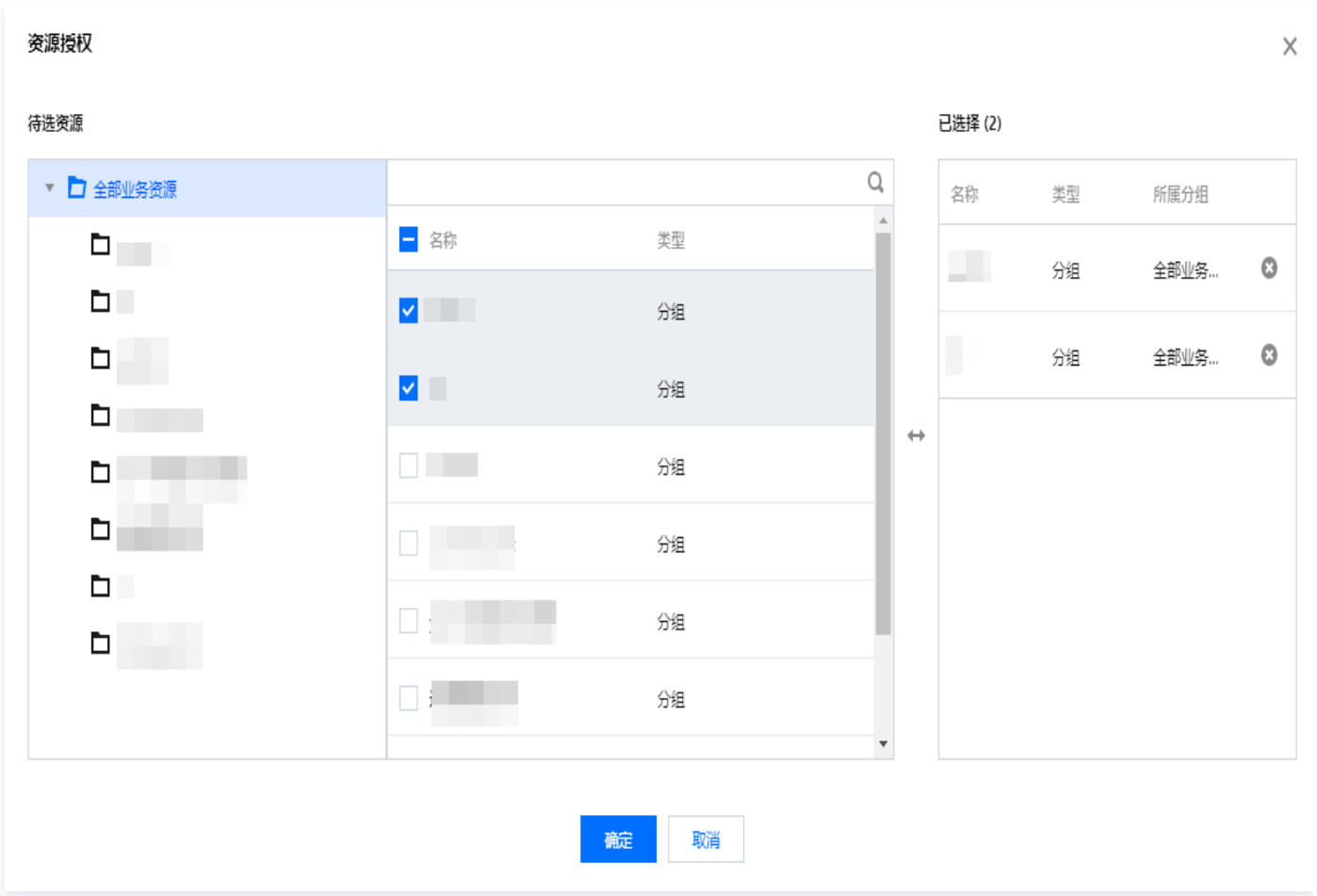
在哪里进行资源授权?

1. 在 **用户与授权管理页面**，选择目标目录，单击**资源授权**。

2. 在目录详情页，单击**添加资源授权**。



3. 在 资源授权窗口中，选择所需资源，单击**确定**。



用户登录时为什么要先选用户目录?

不同目录之间互相隔离，用户来源不同，选择对应的目录才可以正确匹配账户密码。

> **说明:**
> 目录只需要选择一次，登录成功后系统会记住上次选择的目录。

认证源配置

最近更新时间：2025-05-08 14:15:33

什么是认证源实例，如何配置?

认证源实例是指企业客户在 iOA 控制台上配置的企业在用的认证源方式。配置完成后，可以在身份安全策略中使用。终端用户登录时，会通过配置的认证源方式进行身份校验。

目前 iOA SaaS 支持多种认证源对接，包含：扫码认证、短信认证、邮箱认证、IAM 认证、AD 认证、Token 认证、OTP 认证。相关认证源配置指引请参见 认证对接 。

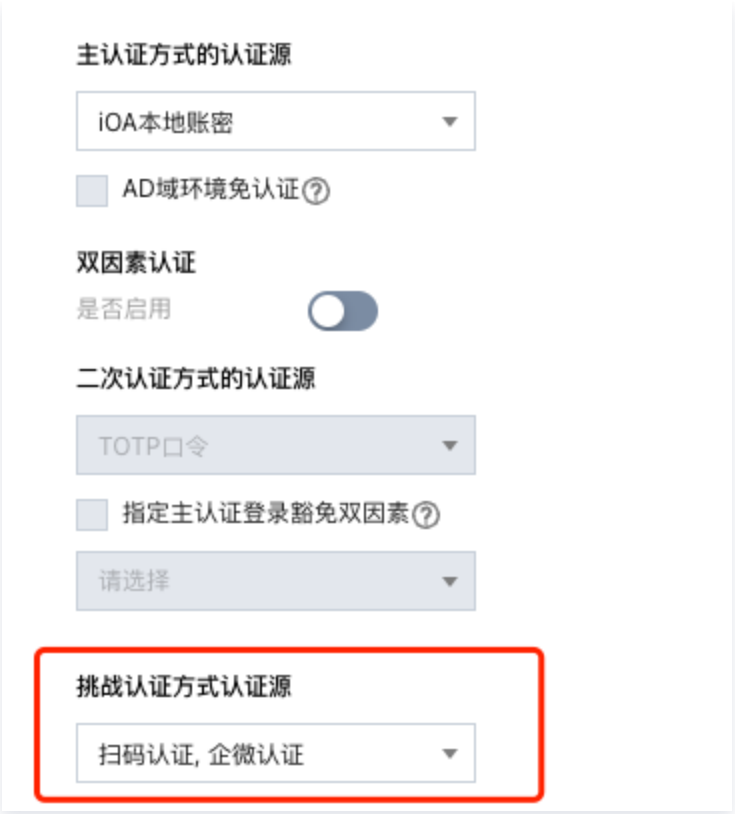
如何启用双因素认证策略?

在 身份安全策略 > 认证安全 > 认证策略 页面，在对应目录的认证策略中启用双因素认证。

什么是挑战认证?

挑战认证是指当用户在特定条件下（时间、网络位置、发起访问的程序等）访问接入 iOA 的业务时，需再次进行登录认证，实现挑战认证要进行如下配置：

1. 在 身份安全策略 > 认证安全 > 认证策略 页面，在对应目录的认证策略中启用挑战认证。



2. 在 业务资源访问 > 访问安全策略 页面，对所选目录配置访问安全策略，且访问策略设置为**挑战认证后访问**。

登录日志在哪里查看?

您可单击 日志审计 > 身份安全日志 进行查看。

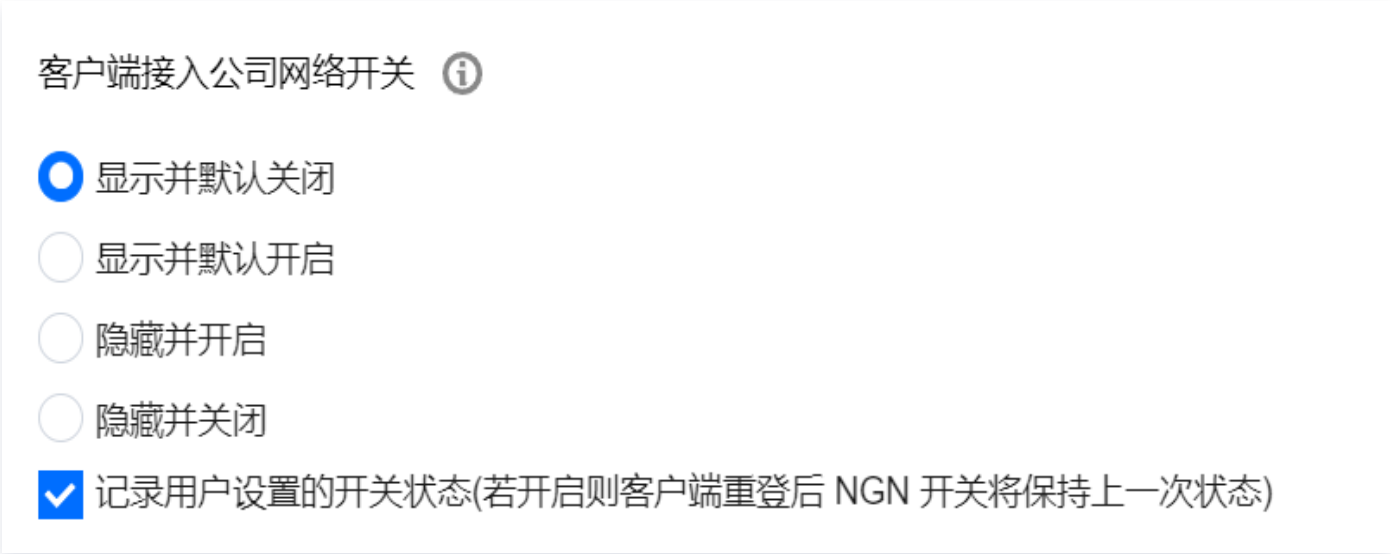
用户登录后就会占用并发账号授权吗?

1. 用户登录后，并且在客户端上打开了“接入公司网络”开关时，即会占用并发账号授权。
2. 您可以在 身份安全策略 > 账号安全 > 账号策略 ，配置用户是否默认开启该开关。

参数名称	说明
显示并默认开启	首次登录时自动接入公司网络，用户可以在客户端自行选择是否接入。

显示并默认关闭（客户端需升级10.3.1版本及以上）	首次登录时不接入公司网络，用户可以在客户端自行选择是否接入。
隐藏并开启	自动接入公司网络并隐藏开关，用户不能更改。
隐藏并关闭	不接入公司网络并隐藏开关，用户不能更改。
记录用户设置的开关状态	若开启则客户端重登后 NGN 开关将保持上一次状态。

3. 应用场景说明：管理员按需设置**是否记录用户设置的开关状态**：若为了避免用户开启 NGN 后不关闭导致长期占用并发，可以设置开关策略为**显示并默认关闭+不勾选记录用户设置的开关状态**；若优先用户体验，为避免用户每次手动调整开关状态，则可以设置为**显示并默认关闭+勾选记录用户设置的开关状态**。



4. 对应客户端开关位置如下图。


腾讯iOA
Test
注销
无边界办公
病毒查杀
合规检测
漏洞修复
电脑工具
欢迎使用，您已接入公司网络
账号已登录
设备已合规
设备环境安全防护中
接入公司网络
连接时长： 00:00:33
开启后接入公司网络，可访问公司网络内已授权的资源。关闭后将无法访问已授权资源。

专线管理

最近更新时间：2024-09-11 09:26:51

部署连接器的服务器推荐配置?

- Centos7.6 CPU：2-4核，内存4-8G，硬盘100G以上。
- 建议最少部署2个连接器实现高可用。

可以部署多个连接器吗?

iOA 不限制连接器安装数量。

连接器如何更新和卸载?

- 更新：
  - iOA 可自动更新。
  - 如需手动更新，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上，再根据需要在原连接器机器上停用连接器进程服务，删除原连接器配置文件，并在 iOA SaaS 控制台将旧连接器专线删除。详细配置请参见 连接器部署 。
- 连接器卸载：详细配置请参见 连接器部署 。

专线提示未连通该如何处理?

1. 确保连接器进程正常运行。
2. 确保连接器所在机器的防火墙已经放通 iOA 网关地址。
3. 确保连接器所在网络出口防火墙已经放通 iOA 网关地址
4. iOA 网关地址可前往 专线管理页面 使用指引栏中获取。

可以在一台服务器上部署多个连接器吗?

同一台服务器不建议同时部署多个连接器，可能会导致流量转发异常。

支持在部署连接器的终端同时安装客户端吗?

不支持。登录 iOA 客户端后流量将被劫持，导致流量无法正常转发到连接器上。

要实现高可用，应该如何部署连接器?

1. 针对同一个资源，可在同一个专线组中增加多条专线，并将这些专线分别部署在不同内网机器上。
2. 应保证连接器可访问需接入 iOA 的业务资源、iOA 云上网关。
3. 访问业务时，iOA 云上网关会自动选择一条状态为**已连通**的专线进行连接。

业务资源管理

最近更新时间：2025-02-20 10:14:42

隧道资源和 Web 资源有什么区别?

1. 隧道资源支持 B/S、C/S 架构应用。必须安装 iOA 客户端才能进行资源访问，且仅支持通过业务后端地址进行访问。
2. Web 资源仅支持 B/S 架构应用。无需安装 iOA 客户端，可使用浏览器等方式访问业务，支持通过前端地址、自定义域名进行资源访问，不支持通过后端地址进行访问。

为什么 Web 资源没有显示在客户端上?

Web 资源暂时不支持下发到客户端首页上。

Web 资源自定义域名该如何配置?

1. 为 Web 资源中添加自定义域名，请确保该自定义域名已在腾讯云备案。
2. 如自定义域名使用 HTTPS 进行访问，则选择对应域名 SSL 证书。
3. 在公网 DNS 解析平台，将自定义域名设置 CNAME 解析至该 Web 资源前端域名上。

为什么要进行备案?

自定义域名需要被 CNAME 解析到 iOA 的 Web 资源访问的云服务器上，相当于通过 iOA 腾讯云网关进行了接入。根据国家相关规定（具体政策法规请参见 工信部平台 政策文件专栏），对非经营性互联网信息服务实行备案制度。备案信息需要与接入服务商进行关联，未获取许可或未履行备案手续的，互联网接入服务商（腾讯云）不得对其提供互联网接入服务。

> **说明：**
> - 如果不使用自定义域名，而是使用 iOA 提供的前端域名（ztnwork.com），则无需在腾讯云上进行备案。
> - 更多备案操作指引请参见文档：ICP 备案-备案流程 。

客户端相关

最近更新时间：2024-09-06 16:55:01

修改自定义品牌及 logo 后，需要重新下载安装吗?

不需要，大概等待3-5分钟客户端自动同步。

新增一个用户源架构，iOA 客户端是否需要重新下载安装?

无需重新下载安装客户端，客户端自动同步新增的用户源架构。在存在多个用户源的情况下，客户端将显示所有用户源架构。