

星连_管理员手册（v2.1.0）

南凌科技股份有限公司

2023 年 8月

目录

1. 概述	6
1.1 注意事项	6
1.2 功能概述	6
2. 身份管理	7
2.1 功能介绍	8
2.2 管理部门	9
2.3 管理成员	11
2.4 管理角色	16
2.5 管理星连帐号体系	18
2.6 配置 LDAP 帐号登录星连	21
2.7 调整帐号策略	25
2.8 同步第三方数据源	27
2.9 配置多因素认证	27
2.10 配置扩展字段	30
2.10.2 管理扩展字段	31
3. 终端管理	32
3.1 功能简介	32
3.2 管理终端分组	33
3.3 在分组内移除设备	37
3.4 查看终端设备信息	37
3.5 采集客户端日志	39
3.6 导入设备扩展字段	39

3.7 添加终端登记策略.....	42
3.8 管理终端登记策略.....	47
3.9 审核终端登记申请.....	48
3.10 查看软件统计情况.....	49
3.11 分发软件至员工设备.....	50
3.11.5 管理软件清单.....	55
3.11.6 管理分发记录.....	55
4. 动态安全.....	56
4.1 功能介绍.....	56
4.2 管理安全状态.....	57
4.3 使用动态决策.....	59
4.4 查看处置记录.....	63
5. 虚拟专有网络.....	63
5.1 功能介绍.....	63
5.2 功能概览.....	66
5.3 节点部署建议与要求.....	66
5.4 添加 VPN 节点.....	68
5.5 设置 VPN 使用权限.....	73
5.6 设置 VPN 节点的网络模式.....	74
5.7 管理极速模式网络资源.....	75
5.8 管理 VPN 访问权限.....	81
5.8.2 相关操作.....	87
5.9 配置 VPN 节点的可见对象.....	88
5.9.1 注意事项.....	88

5.9.2 操作步骤.....	89
5.10 查看或编辑 VPN 节点信息	89
5.11 查看员工的 VPN 权限信息	94
5.12 配置 VPN 策略.....	94
6. WiFi与有线网络.....	95
6.1 功能简介.....	95
6.2 服务器部署建议与要求.....	97
6.3 添加 RADIUS 服务器	100
6.4 添加无线路由.....	102
6.5 添加交换机.....	105
6.6 编辑或删除 RADIUS 服务器.....	106
6.7 编辑或删除路由设备.....	109
6.8 设置 Wi-Fi SSID.....	113
6.9 管理访客 Portal Server.....	115
6.10 管理员工入网.....	119
6.11 管理访客入网.....	126
6.12 管理哑终端入网.....	129
7. 系统服务	133
7.1 消息通知.....	133
7.1.4 管理邮件配置.....	135
7.1.5 管理第三方 IM	137
7.1.6 添加飞书机器人.....	139
7.1.7 添加钉钉机器人.....	142
7.1.8 添加企业微信机器人.....	146

7.2 配置客户端.....	149
7.3 配置全局白名单.....	151
7.3.1 编辑或删除白名单.....	153
7.4 系统设置	154
7.4.1 配置与查看企业信息.....	154
7.4.2 定制星连门户网站.....	155
7.4.3 定制客户端 Banner.....	157
7.4.4 定制访客 Wi-Fi 认证页.....	160
7.4.5 查看星连日志审计.....	161
7.4.6 配置日志外发.....	164
7.4.7 添加管理员.....	166
7.4.8 编辑或删除管理员.....	167
7.4.9 配置管理员告警策略.....	169

1. 概述

管理员操作手册主要介绍星连管理后台所有功能模块及操作说明，以帮助企业管理员快速理解并上手使用星连功能。本章节将概述星连管理后台中所有功能模块。

1.1 注意事项

企业应与员工签署相关使用协议及授权协议，即企业应在要求雇员安装星连前（时），以明确清晰且具体的方式告知星连收集的数据类型、使用的目的方式和范围。

用户指南中的所有操作均需由企业管理员操作完成，企业员工不具备星连管理后台的访问权限。如果您需要为企业员工设置星连管理员权限，则需要登录星连管理后台进行配置。

1.2 功能概述

1.2.1 身份管理

身份管理模块包含对企业的子公司、部门、成员以及角色的管理能力。一个平台打通企业内部办公系统，通过建立员工身份统一认证体系，实现企业细粒度、全流程的员工在职生命周期管理，并在此基础上实现自动化授权调整，避免帐号安全风险。

1.2.2 终端管理

终端是企业办公交互的基本单位。对终端设备（PC 端、移动端）的安全管控也是数字化办公当中重要的一环。当企业员工在各自终端登录星连客户端后，星链即可获取员工终端设备的软硬件信息，后续可基于终端维度进行权限管理、软件分发、安全检测。

1.2.3 动态安全

星连内置了全面、灵活的办公安全策略框架，大幅降低企业安全制度落地难度与成本。动态控制联动身份、网络与终端管理模块，在全面判断安全状态的基础上完成动态风险处置，当设备状态或者员工行为发生变化时实时触发。在星连动态决策引擎的帮助下，您只需要调整各项动态控制策略的参数配置与策略逻辑，即可构建定制化的企业动态安全控制能力。

1.2.4 虚拟专有网络（VPN）管理

星连虚拟专用网络 VPN 采用全新网络隧道技术，支持 UDP/TCP 双协议与多节点自动优选，提供高效安全的网络连接体验。此外，由星连底层架构的多

活设计弥补了硬件单机容灾性不足的缺陷，实现了网络高稳定、高可用。

在星连管理后台，您可以统一配置企业 VPN 节点、授予 VPN 节点使用权限与访问权限，为员工构建安全稳定的远程办公环境。

1.2.5 Wi-Fi与有线网络管理

Wi-Fi 管理模块包含 Wi-Fi 网络与有线网络环境构建的能力，并结合员工数字化身份认证，无论是企业内部员工还是外部访客，均可实现一人一帐号的网络访问行为控制。您可以基于企业员工的部门、角色或者设备状态，设置可访问不同网络资源的多个权限组，以规定不同员工、设备的不同入网方式。此外，支持哑终端入网，在企业网络环境内统一管理企业设备。

1.2.6 系统服务

通用配置集成了消息通知、客户端配置以及白名单配置模块。

消息通知：您可以消息通知内配置企业邮件网关，统一邮件消息通知的内容格式；可以关联第三方 IM 机器人，将星连的消息通知通过机器人推送至第三方 IM。

客户端配置：结合企业安全要求，可配置星连客户端的安全性与启动方式，以确保员工稳定使用星连客户端。

白名单配置：该白名单是星连内的全局白名单，您可以为一个或多个功能模块设置白名单，在白名单生效范围内的员工或者设备将不受指定功能模块的策略影响。

系统设置：系统设置集成企业配置、企业文化、日志审计、管理员权限模块。

企业配置：管理企业基本信息、获取客户端安装链接、配置企业用户协议与隐私政策。

企业文化：为企业提供个性化终端展示的能力。

日志审计：你可以查看或者外发星连记录的各项日志数据，包括员工或管理员操作日志、VPN 连接与访问日志、Wi-Fi 连接日志以及哑终端网络连接日志。

管理员权限：统一管理星连管理员、权限范围以及安全策略。

2. 身份管理

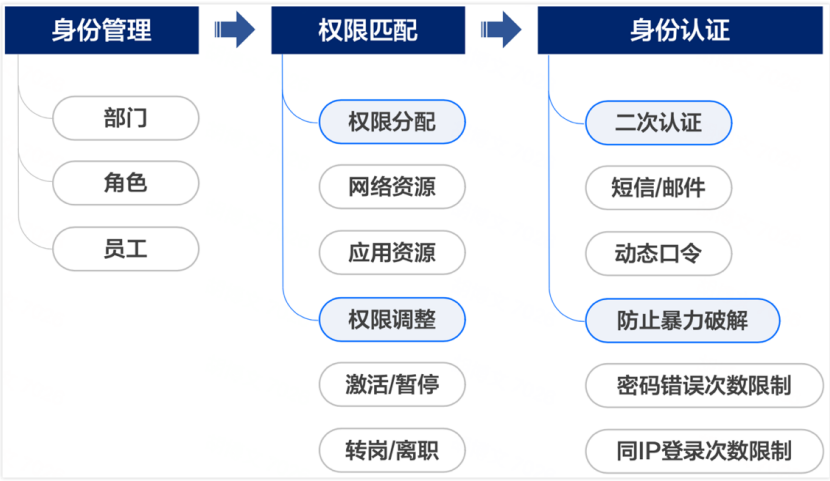
通过星连的身份管理功能模块，您可以构建企业组织架构、管理星连帐号的认证方式与帐号安全策略。通过本文您可以了解身份管理在星连服务中的作

用，以及该功能模块对应的操作文档说明。

2.1 功能介绍

身份管理功能包含了对企业子公司、部门、成员、角色的创建、更新、查询、删除功能。通过该功能您可以在星连中构建企业完整的组织架构（支持手动构建组织架构或者通过第三方导入企业已有的组织架构）。

身份管理是星连的核心配置，也是其他功能模块的前置功能。主要体现在：构建企业组织架构并录入员工信息后，即可为员工分发星连帐号，员工可以通过星连帐号下载并登录星连客户端，进而开启安全高效的数字化办公。星连内的 VPN 管理、Wi-Fi 管理、应用管理、终端管理、终端安全检测等功能，均依赖于身份管理进行权限差异化划分、风险事件准确溯源等操作。支持设置星连自身的登录二次认证、防止暴力破解等能力，以提高星连平台与客户端的安全性。



2.2 管理部门

当您通过星连构建数字化安全办公平台时，需要先构建企业组织架构。星连支持以下方式构建企业组织架构：

手动配置：手动添加企业部门与员工信息。同时，员工在企业内的入离调转等动作，也需要您在星连管理后台手动配置。具体操作，请参见本章节以及《2.3 管理成员》。

接入第三方数据源：星连支持将钉钉或飞书中存量的组织架构快速导入星连。该方式省去了企业管理员手动配置企业组织架构的耗时。具体操作，请参见《2.5 管理星连帐号体系》。

2.2.1 添加部门或子公司

1. 登录星连管理后台。
2. 在左侧导航栏，选择**身份管理** > **部门与成员**。
3. 在**部门架构**右侧，单击加号（+），然后选择**部门或子公司**。



如果选择**新建子部门**，则需要**在新建部门对话框**，配置**部门名称与上级部门**，然后单击**确定**。

如果选择**新建子公司**，则需要**在新建子公司对话框**，配置**子公司名称与上级部门**，然后单击**确定**。

2.2.2 添加子部门

1. 登录星连管理后台。
2. 在左侧导航栏，选择**身份管理** > **部门与成员**。
3. 在指定的子公司或者部门名称右侧单击图标，并选择**新建子部门**。



2.2.3 重命名部门或子公司的名称

1. 登录星连管理后台。
2. 在左侧导航栏，选择身份管理 > 部门与成员。
3. 在指定的子公司或者部门名称右侧单击图标，并选择重命名部门。



2.2.4 删除部门或者子公司

说明：

删除操作不可恢复，请您谨慎操作。具体影响说明：

删除一个有子部门，但子部门没有成员的部门或子公司时，该部门或子公司包含的子部门也将一并删除。

删除一个有成员的部门或子公司时，如果包含子部门，但子部门没有成员，则该部门或子公司所包含的成员将移至父级部门。

删除一个有子部门，且子部门有成员的部门或子公司时，需先删除子部门或移除子部门成员，然后才可以删除部门或子公司。

1. 登录星连管理后台。
2. 在左侧导航栏，选择身份管理 > 部门与成员。
3. 在指定的子公司或者部门名称右侧单击图标，并单击删除部门。



4. 在**删除提示**对话框，单击**删除**。

2.3 管理成员

您可以在星连内手动录入员工信息并激活员工帐号，录入方式支持逐条录入或批量导入。后续当员工身份在企业内发生变化时，星连支持跟进调整员工部门、离职状态等信息。

2.3.1 注意事项

本章节介绍的成员管理方式，仅适用于在星连内手动构建组织架构以及员工信息的业务场景。

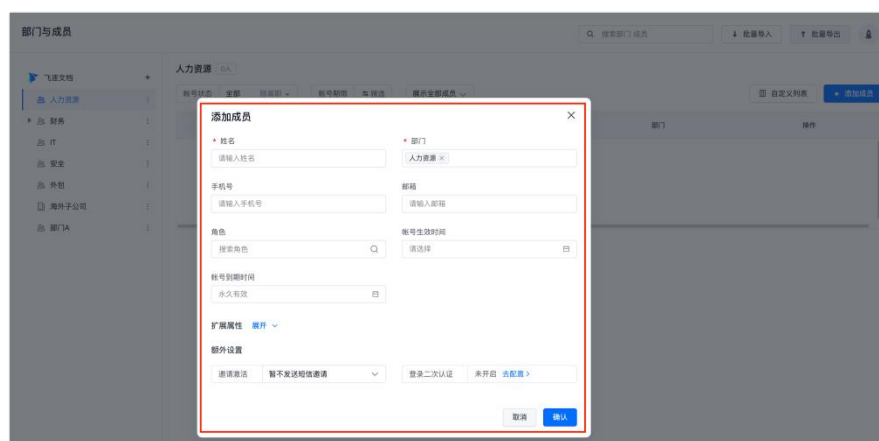
如果您的企业组织架构是通过第三方数据导入的方式构建的，则建议您在第三方数据源维护员工信息，后续在星连管理后台同步第三方数据源即可。如果您必须进行手动操作，则需要先停止数据源导入，再进行手动操作，但该方式也会导致您第三方数据源中的增量数据无法再继续同步至星连管理后台。因此请您谨慎操作。关于第三方数据源导入的更多信息，请参见《3.5 管理星连帐号体系》。

2.3.2 添加成员

1. 登录星连管理后台。
2. 在左侧导航栏选择**身份管理** > **部门与成员**。
3. 在**部门架构**列表，选择指定的部门。
4. 在右侧部门区域，添加成员。

方式一：逐条添加员工信息

单击**添加成员**，然后在**添加成员**对话框完成以下配置，并单击**确认**。



方式二：批量导入员工信息

- i. 在部门与成员页面右上角，单击**批量导入**。



- ii. 在**批量导入成员**页面的**第一步**区域，下载人员导入模板。

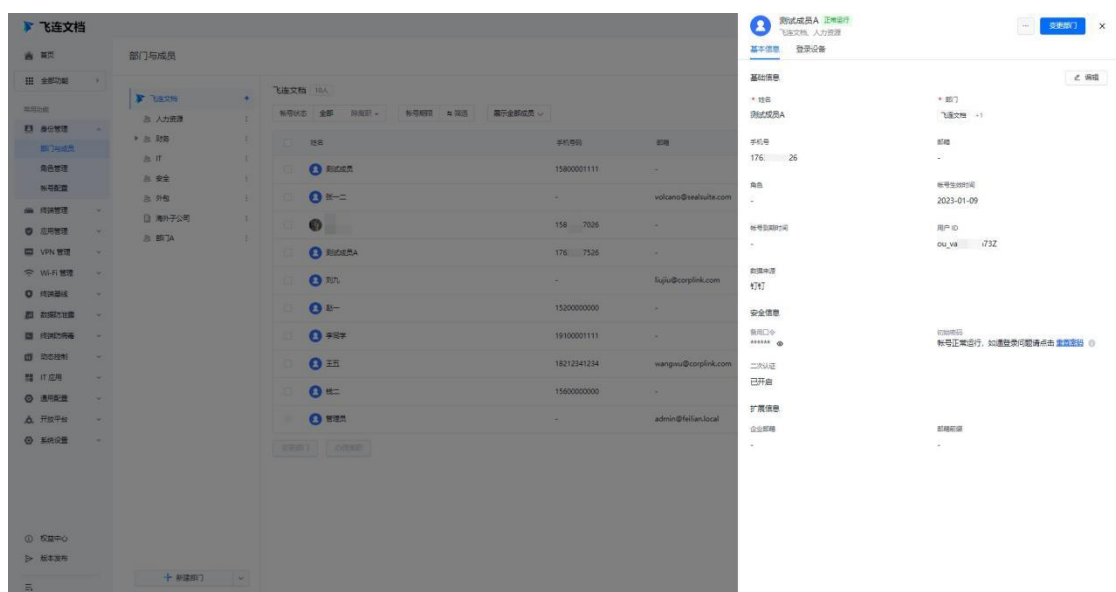


- iii. 在本地打开模板，录入员工信息并保存。
- iv. 返回星连管理后台，在**批量导入成员**页面的**第二步**区域，将本地已编辑好的成员导入模板上传至星连。
- v. 配置员工帐号激活短信的发送策略，以及是否开启员工登录的二次认证，然后单击**确认导入**。

2.3.3 查看或调整成员信息

1. 登录星连管理后台。
2. 在左侧导航栏选择**身份管理** > **部门与成员**。
3. 在**部门架构**列表，选择指定的部门。
4. 在部门内，找到指定的成员，单击成员名称，在右侧**基本信息**页签查看成员信息。

包括：查看或编辑成员的基本信息、管理登录设备、变更成员部门等操作。



2.3.4 变更成员部门

1. 登录星连管理后台。
2. 在左侧导航栏选择**身份管理** > **部门与成员**。
3. 在**部门架构**列表，选择指定的部门。
4. 在部门内找到成员，通过以下任一方式变更成员部门。

方式一：调整某一成员部门

在指定成员列右侧单击**操作**，然后单击**变更部门**。



方式二：批量调整成员的部门

在成员列表，选中需要调整部门的成员前的复选框，并单击**变更部门**。



2.3.5 暂停成员帐号的使用

1. 登录星连管理后台。
2. 在左侧导航栏选择**身份管理** > **部门与成员**。
3. 在**部门架构**列表，选择指定的部门。
4. 在部门内找到需要暂停帐号的成员，在成员列右侧单击**操作**，并单击**暂停使用**。

暂停使用后，该员工如果正在登录星连，则会被强制登出，且无法继续使用该帐号。此时您再次单击成员右侧的**操作**后，仅提供**恢复使用**的按钮。



暂停使用的帐号登录星连客户端时，会出现“帐号已离职或停用，请联系管理员”的报错信息。

2.3.6 重置成员帐号密码

将成员帐号的密码重置为随机字符的初始密码。重置密码后，如果员工正在登录星连，则会被强制登出，此时需要员工手动使用新密码再次登录。

1. 登录星连管理后台。
2. 在左侧导航栏选择**身份管理** > **部门与成员**。
3. 在**部门架构**列表，选择指定的部门。

4. 在部门内找到需要重置密码的成员，在成员列右侧单击**操作**，并单击**重置密码**。



2.3.7 办理成员离职

2.3.7.1 注意事项

员工离职来源获取：星连、第三方软件（钉钉、飞书）。

若离职来源为星连，则直接参考本章节在星连管理后台办理离职即可。

若离职来源为第三方软件，则需要第三方软件中订阅员工状态，并在星连管理后台同步第三方数据源。否则星连无法直接获取到离职信息，导致离职员工仍可使用星连。第三方离职来源如下：

飞书：员工离职。

钉钉：通讯录用户离职。

离职员工的星连功能下线。

Wi-Fi 或有线网络功能：员工离职后，星连管理后台会自动将离职员工当前的在线设备下线，客户端将会立即断开连接。

离职员工相关数据无法编辑。

员工离职后，管理后台的离职员工数据将无法编辑，仅支持查看员工信息，方便管理员日后审计。

离职员工与第三方的交互立即停止使用。

员工在离职后，短信、邮件、第三方 IM 通知将立即停止使用。

2.3.7.2 操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏选择**身份管理** > **部门与成员**。
3. 在**部门架构**列表，选择指定的部门。
4. 在部门内找到需要办理离职的成员，通过以下任一操作为成员办理离职。

方式一：为指定成员办理离职

在指定成员列右侧，单击**操作**，并单击**办理离职**。



方式二：批量办理离职

在需要办理离职的多个成员列左侧选中复选框，然后在**变更部门**右侧单击下拉按钮，并单击**办理离职**。



为成员办理离职后，您可以在成员列表上方的**帐号状态**下拉列表中选择**已离职**，进而可以查看到已离职成员信息。后续您可以根据成员变动，在操作列选择**返聘**或者**删除**。



返聘：恢复该成员在企业内的帐号使用权限，但需要重新激活帐号。

删除：彻底删除该成员信息，且不可恢复。

2.4 管理角色

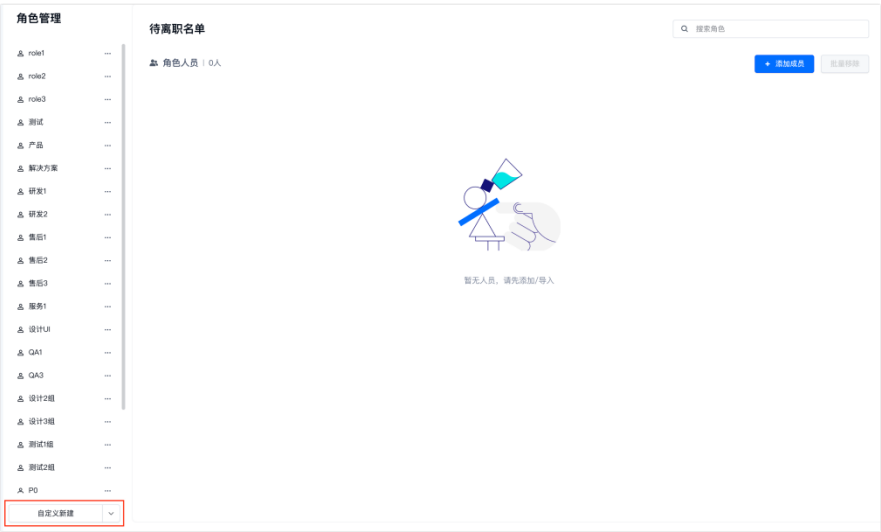
您可以根据企业成员的不同分工设置不同的角色，目前角色的作用主要是

授权应用或策略。

2.4.1 添加角色

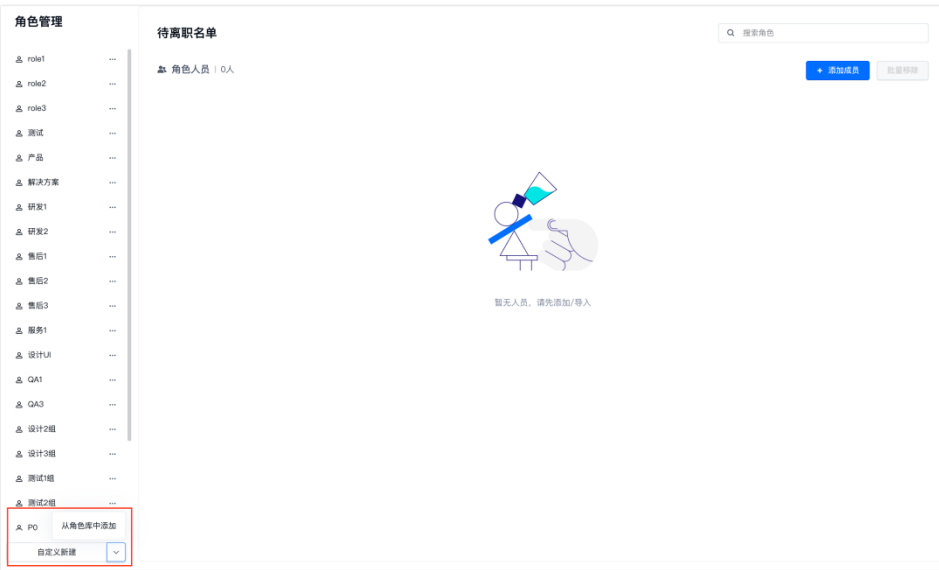
1. 登录星连管理后台。
2. 在左侧导航栏，选择身份管理 > 角色管理。
3. 在角色管理页面，支持以下任一方式添加角色。

单击自定义新建进行添加。



单击从角色库中添加进行添加。

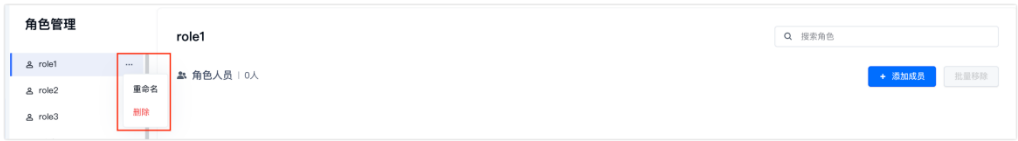
角色管理中已存在的角色，不支持重复选取。



2.4.2 重命名或删除角色

1. 登录星连管理后台。
2. 在左侧导航栏，选择身份管理 > 角色管理。

3. 在**角色管理**页面，找到指定的角色，在角色名称右侧单击 **...**。
4. 选择**重命名**或者**删除**角色。

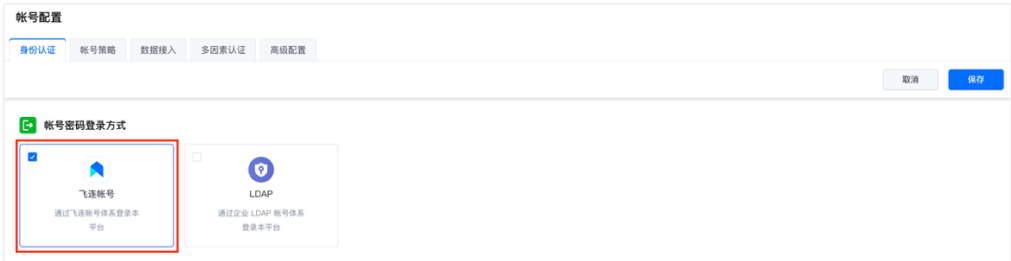


2.5 管理星连帐号体系

星连默认使用星连帐号体系供企业员工进行身份校验。根据企业需要，您可以在星连管理后台调整星连帐号体系的相关配置，包括登录方式、第三方授权登录以及防止暴力破解等。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**身份管理** > **帐号配置**。
3. 在**帐号配置**页面的**身份认证**页签右上角，单击**编辑**。
4. 在**帐号密码登录方式**区域，选择**星连帐号**。



5. 在**星连帐号**区域，根据企业管理需要，选择进行以下配置。

配置项	说明
登录帐号	即星连帐号的登录方式，可选手机号、邮箱方式登录。 注意：如果仅选择手机号或者邮箱，则需要注意未录入手机号或者邮箱的帐号将无法登录。例如，登录帐号仅选择手机号登录，但员工 A 仅录入了邮箱信息，则员工 A 将无法以帐号密码的方式登录星连。

登录认证方式	支持选择密码、短信验证码、动态口令以及邮箱验证码中至多三种登录认证方式。 密码：星连帐号对应的密码。 短信验证码：通过员工手机号接收验证信息，具体操作，请参见《13.1.3 管理短信网关》。 动态口令：星连客户端（移动端）提供的动态口令。 邮箱验证码：通过员工邮箱接收验证信息。该方式需要您提前配置好企业邮件网关，具体操作，请参见《13.1.4 管理邮件配置》。
浏览器快速登录	开启后，如果星连桌面端登录成功，则在同一设备内使用浏览器访问星连时将会自动获取星连帐号的登录态，无需重复手动登录。
星连桌面端授权登录确认	开启后，在浏览器点击快速登录后，在星连桌面端进行授权登录二次确认，确保帐号安全性。
登录态有效期	为星连客户端以及星连门户网站设置员工帐号登录态的有效时长。支持设置默认 20 天、1 天、3 天、7 天、14
第三方授权登录	天。单击配置，进入第三方授权登录配置页面关联第三方平台，配置生效后可通过第三方授权登录星连。 2. 选择第三方平台并进行参数配置，支持多选。 3. 在认证失败提示文案区域，自定义设置认证失败时的提示消息。 4. 在页面底部单击立即生效。

自动创建帐号	开启自动创建帐号后，当第三方数据源未及时同步入职员工帐号时，该员工登录星连后会自动创建帐号。 功能效果示例： 关闭效果：第三方数据源中有 A 帐号，但星连后台组织架构中还未同步 A 帐号，此时若用帐号 A 进行第三方登录，客户端会登录失败并报错。 开启效果：第三方数据源中有 B 帐号，但星连后台组织架构中还未同步 B 帐号，此时若用帐号 B 进行第三方登录，将自动在星连创建帐号，且客户端登录成功。
登录方式展示优先级	如果您开启了 LDAP 登录方式，或者授权了第三方平台认证登录星连，则在该配置项中可调整帐号登录方式的优先级。排序越靠左侧优先级越高。其中第一优先级为星连的默认登录方式，其他为可选登录方式。
防止暴力破解选项	星连提供了以下自动处置方案，在需要时可选中方案前的复选框以开启方案。 密码输入错误够指定次数时，限制当前帐号在指定时间段内无法登录。 同一 IP 登录连续出错达到指定次数时，限制该 IP 在指定时间段内无法发送登录请求。

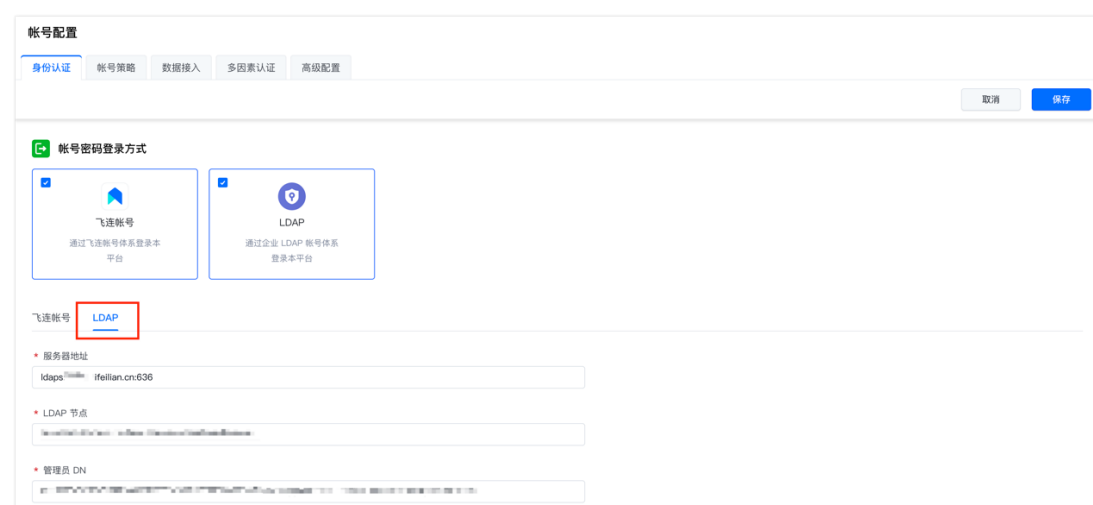
6. 在页面右上角，单击**保存**，使配置生效。

2.6 配置 LDAP 帐号登录星连

轻型目录访问协议 LDAP（Lightweight Directory Access Protocol）常用于管理企业员工帐号并支持单点登录。星连内除星连帐号体系之外还支持关联企业 LDAP 帐号体系，您可以将企业的 LDAP 服务器关联至星连管理后台，使员工可以通过 LDAP 帐号登录星连。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择身份管理 > 帐号配置。
3. 在帐号配置页面的身份认证页签右上角，单击编辑。
4. 在帐号密码登录方式区域，选择 LDAP。



5. 单击 LDAP 页签，并完成 LDAP 相关配置。

配置项说明：

配置项	说明
服务器地址	LDAP 所属服务器的地址。建议遵循安全的轻型目录访问协议 ldaps，地址格式：<code>ldaps://<host>:<post></code>。 <code><host></code> 指服务器域名或 IP 地址。 <code><post></code> 指端口号。ldap 协议默认为 389，ldaps 协议默认为 636。
LDAP 节点	设置 LDAP 节点后，星连会以该节点为根节点查询组织对象。示例值：<code>dc=feilian, dc=com</code>。
管理员 DN	指定可以用来连接 LDAP 服务器且拥有管理权限的用户。 示例值：<code>cn=admin, dc=feilian, dc=com</code>。
管理员密码	管理员 DN 对应的密码信息。
用户对象类	用户对象（objectclass）。示例值如下： OpenLDAP: <code>inetOrgPerson</code> 基于 LDAP 的 AD 域: <code>user</code> 或 <code>organizationalPerson</code>
用户唯一标识	LDAP 中每个用户实例的唯一标识属性。示例值如下： OpenLDAP: <code>uid</code>、<code>dn</code> AD 域: <code>sAMAccountName</code>
手机号	LDAP 中用户的手机号属性，与邮箱二选一进行配置。示例值如下： OpenLDAP: <code>phoneNumber</code> AD 域: <code>mobile</code>
邮箱	LDAP 中用户的邮箱属性，与手机号二选一进行配置。示例值如下： OpenLDAP: <code>mail</code>

	AD 域: mail
用户离职字段	可选项，如果 LDAP 中存在表示用户离职的属性，请填写。示例值如下： OpenLDAP: employeeType

	AD 域: UserAccountControl
用户离职字段值	表示用户离职状态的关键字。示例值如下: OpenLDAP: separated 基于 LDAP 的 AD 域: 514 (十进制)
员工登录时, 允许自动更新员工信息	开启后, 员工使用第三方数据源授权登录时, 将自动更新员工信息。
连通性测试	单击 连通性测试 , 确保 LDAP 服务器与星连管理后台网络互通。
第三方授权登录	支持配置其他第三方平台授权登录星连。 1. 单击配置, 进入第三方授权登录配置页面关联第三方平台, 配置生效后可通过第三方授权登录星连。 2. 选择第三方平台并进行参数配置, 支持多选。 3. 在认证失败提示文案区域, 自定义设置认证失败时的提示消息。 4. 在页面底部单击立即生效。
自动创建帐号	开启自动创建帐号后, 当第三方数据未及时同步到星连时, 新员工登录星连后会自动创建帐号。 功能效果示例: 关闭效果: 第三方数据源中有 A 帐号, 但星连后台组织架构中还未同步 A 帐号, 此时若用帐号 A 进行第三方登录, 客户端会登录失败并报错。 开启效果: 第三方数据源中有 B 帐号, 但星连后台组织架构中还未同步 B 帐号, 此时若用帐号 B 进行第三方登录, 将自动在星连创建 LDAP 帐号, 且客户端登录成功。
登录方式展示	如果您开启了星连帐号登录方式, 或者授权了第三方平台认

优先级	证登录星连，则在该配置项中设置帐号登录方式的优先级。
	排序越靠左侧优先级越高。其中第一优先级为星连的默认登录方式，其他为可选登录方式。
防止暴力破解选项	星连提供了以下自动处置方案，在需要时可选中方案前的复选框以开启方案。 密码输入错误够指定次数时，限制当前帐号在指定时间段内无法登录。 同一 IP 登录连续出错达到指定次数时，限制该 IP 在指定时间段内无法发送登录请求。

6. 在页面右上角，单击**保存**，使配置生效。

2.7 调整帐号策略

在星连管理后台可调整员工帐号安全相关策略，包括开启忘记密码功能、配置企业邮箱域名、设置密码策略以及密码长度、配置离职员工帐号数据清理策略、是否同步第三方数据源角色等。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**身份管理** > **帐号配置**。
3. 在**帐号配置**页面，单击**帐号策略**页签。
4. 在页面右上角单击**编辑**，根据企业管理需要，选择进行以下配置。各配置项说明如下表：

配置项	说明
是否开启忘记密码	开启：在星连客户端可单击忘记密码，自助重置密码。 关闭：在星连客户端内不支持自助重置密码。您需要配置忘记密码提示文案，用于提示员工联系帐号问题联系人进行解决。

帐号问题联系人	选择企业内的一个员工作为帐号问题联系人。当未开启忘记密码功能时，如果员工登录时忘记密码，则可以根据界面提示信息联系帐号问题联系人进行解决。
企业邮箱域名	配置企业邮箱的域名后缀。如果企业需要统一邮箱后缀，则可以选中 仅支持添加该后缀邮箱 。
密码策略要求	指定设置密码时的字符要求。可选 大写字母 、 小写字母 、 数字 以及 特殊字符 ，支持多选。
密码最小长度	指定设置密码时的最小长度。
帐号状态	管理离职员工帐号的数据清理策略。单击数据清理策略，跳转至配置数据清理页面完成以下配置。 有效期：选择在员工离职 7 天、30 天、90 天后，自动删除终端管理中已勾选的数据。 终端管理：选择被删除的数据。可选终端列表数据、终端设备登记-审批记录、软件统计-已安装终端设备列表、软件分发记录，支持多选。
是否同步角色	如果星连内的组织架构是通过第三方数据源导入的方式构建，则开启是否同步角色后，如果第三方数据源内的员工信息包含角色属性，则星连会自动在角色管理中生成相同角色，并在角色中添加相应的员工。 不同第三方数据源支持同步角色的能力不同，具体说明如下： 飞书、钉钉、Authing：支持同步角色属性。 企业微信：不支持。企业微信没有角色属性。 LDAP：暂不支持自动同步，需要为 LDAP 内员工信息手动定义角色属性，然后通过星连扩展字段映射员工的角色属性。

强制修改 密码策略	开启后，员工在首次登录星连时，必须强制更新密码才能成功登录星连。
--------------	----------------------------------

5. 在页面右上角单击**保存**，使配置生效。

2.8 同步第三方数据源

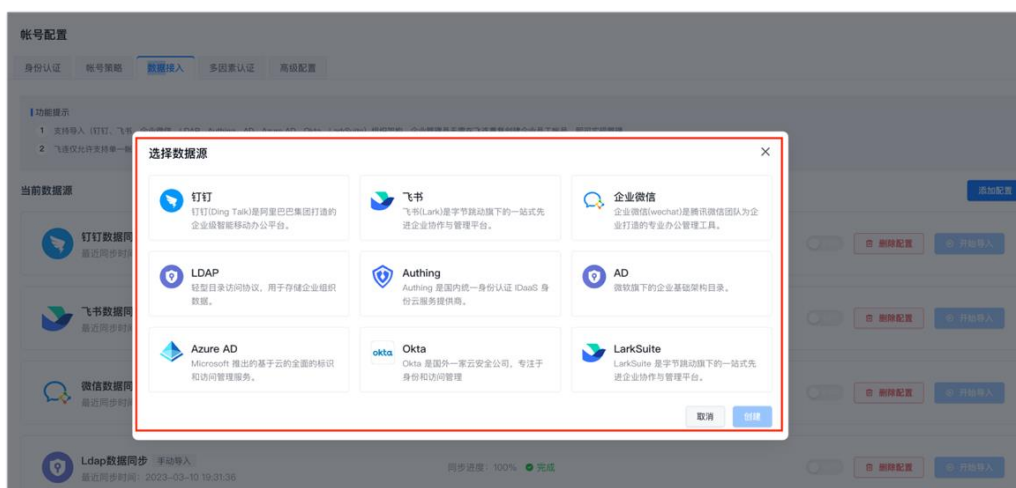
企业可以将第三方平台维护的组织架构、员工信息一键导入星连管理后台进行统一管理，免去在星连内重复创建企业员工帐号的步骤。目前星连支持接入的第三方数据源有钉钉、飞书、LarkSuite、企业微信、LDAP、Authing、AD、Azure AD、Okta。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**身份管理** > **帐号配置**。
3. 在**帐号配置**页面，单击**数据接入**页签。
4. 单击**添加配置**。

如果您是首次配置数据接入，则请单击**开始导入**。

5. 在**选择数据源**对话框，选择指定的数据源，并单击**创建**。



详情请参见组织架构导入与第三方登录配置指导手册。

2.9 配置多因素认证

多因素认证功能用于实现员工身份校验的二次认证，以增强员工帐号的安全性。

2.9.1 配置认证方式

1. 登录星连管理后台。

- 2. 在左侧导航栏，选择身份管理 > 帐号配置。
- 3. 在帐号配置页面，单击多因素认证页签。
- 4. 在认证方式区域，查看星连支持的认证方式，其中动态口令、短信验证码以及邮箱验证码支持手动配置。



认证方式说明：

认证方式	说明
动态口令	动态口令通过手机端的星连客户端查看。星连提供了自带的动态口令，同时也支持企业自建动态口令。单击配置可查看当前使用中的动态口令服务，您也可以根据实际需要调整所使用的动态口令服务。不同服务说明如下： • 星连动态口令：星连默认自带的动态口令服务。 • 自定义动态口令：当企业已将第三方组织架构导入星连，且需要使用第三方动态口令时，可以配置自定义动态口令关联第三方动态口令，配置生效后自定义动态口令只用于校验源自第三方数据源的员工身份。
邮箱验证码	星连服务向员工邮箱发送验证码进行认证。该方式需要您单击配置，前往消息通知的邮件配置功能中完成企业邮件网关配置。具体操作，请参见《13.1.4 管理邮件配置》。
短信验证码	星连服务向员工手机发送短信验证码进行认证，具体操作，请参见《13.1.3 管理短信网关》。
推送认证	该认证方式仅适用于员工连接 VPN 时进行二次认证。当员工在桌面端的星连客户端内进行 VPN 连接时，需要前往手机端的星连客户端完成推送认证。

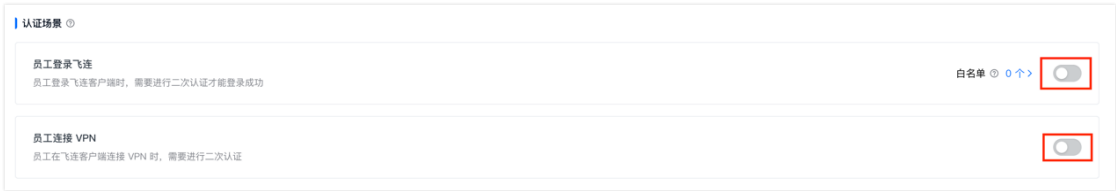
说明：

- 在生效场景说明右侧单击展开，可查看各类认证方式在移动端、桌面端、浏览器内的生效情况。
- 在各类认证方式的卡片内，单击示例可查看当前认证方式的实现效果。

2.9.2 在指定场景开启多因素认证

在多因素认证页签的认证场景区域，手动配置员工登录星连、员工连接VPN认证场景。

每个认证场景由独立开关控制，您可以选择启用指定场景的多因素认证。



场景一：配置员工登录星连认证场景

操作项	说明
开启二次认证	1. 在员工登录星连卡片右侧，打开开关。 2. 在配置认证方式对话框，完成以下配置，并单击确定。 主选认证方式：必选项，可选动态口令、短信验证码、邮箱验证码的其中一种方式。 备选认证方式：可选项，如果企业担心员工不能通过主选认证方式获取验证信息，则可以设置备选认证方式，后续将由员工自行选择二次认证的方式。可选动态口令、短信验证码、邮箱验证码的其中一种方式（已被主选认证方式占用的选项不支持选择）。

设置白名单	在 员工登录星连 卡片右侧单击白名单个数，可以设置 员工、部门、角色 维度的白名单范围。在白名单内的员工二次认证不随全局开关控制，管理员可至身份管理-对应员工信息详情页手动开启或关闭对应员工的二次认证。
开启手动关闭功能	开启 员工登录星连 场景的二次认证后，支持配置 手动关闭 功能，该功能用于限制企业员工是否可以在星连门户网站自行关闭二次认证。

场景二：配置员工连接 VPN 认证场景

操作项	说明
开启二次认证	1. 在员工登录星连卡片右侧，打开开关。 2. 在配置认证方式对话框，完成以下配置，并单击确定。 主选认证方式：必选项，可选动态口令、短信验证码、推送认证的其中一种方式。 备选认证方式：可选项，如果企业担心员工不能通过主选认证方式获取验证信息，则可以设置备选认证方式，后续将由员工自行选择二次认证的方式。可选动态口令、短信验证码、推送认证的其中一种方式（已被主选认证方式占用的选项不支持选择）。
设置连接时效	开启 员工连接 VPN 场景的二次认证后，支持配置 连接时效 功能，该功能用于限制星连客户端通过二次认证连接 VPN 后的有效时长。例如，选择 每次 表示每次连接 VPN 都需要二次认证。选择 2 小时 表示本次二次认证的有效时长为 2 小时，2 小时内重新连接 VPN 不需要二次认证，超过 2 小时后重新连接 VPN 需要二次认证。

2.10 配置扩展字段

星连管理后台的员工信息中，除系统默认提供的基础字段之外，还支持手动添加扩展字段。当星连基础字段不满足企业员工属性时，您可以手动添加扩展字段存储相应的员工信息。本文介绍如何在星连管理后台配置扩展字段。

2. 10. 1添加扩展字段

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择身份管理 > 帐号配置。
- 3. 在帐号配置页面的高级配置页签，单击添加字段。

如果您是首次使用该功能，则可以查看到系统默认添加的名为企业邮箱的自定义字段。该字段支持编辑与删除。

- 4. 在添加扩展字段对话框，完成以下配置，并单击确定。

添加扩展字段

* 字段 Key

请输入字段唯一 Key

* 字段名称

请输入

* 字段类型

字符串

是否必填

非必填

必填

取消

确定

配置项说明：

配置项	说明
字段 Key	扩展字段的唯一 Key 值。已被使用的字段 Key 不可重复添加。
字段名称	扩展字段的名称。
字段类型	设置字段的数据类型支持字符串、数字、布尔值、表达式。
是否必填	当字段类型选择字符串、数字或者布尔值时，需要设置当前字段是否为必填字段。
表达式值	仅当字段类型选择表达式时，需要设置表达式值。

2. 10. 2 管理扩展字段

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择身份管理 > 帐号配置。

- 3. 在帐号配置页面，单击高级配置页签。
- 4. 在高级配置页签，支持以下操作。



在星连扩展字段列表中，查看已有扩展字段的属性值。

在各个字段的操作列：

单击编辑，可手动调整扩展字段的属性值。

单击删除，可删除不再需要的扩展字段。

说明：如果扩展字段已存储员工信息数据，则删除后将无法找回数据，请您谨慎操作。

3. 终端管理

当企业员工登录星连客户端后，星连会收集客户端所在设备信息并上传至星连管理后台。您可以通过终端管理功能集中管理企业内所有已接入星连的终端设备，包括分组管理设备、查看与调整设备属性、统计软件安装情况、批量分发软件等能力。

3.1 功能简介

功能项	说明
终端列表	该功能包含以下能力： 分组管理设备。 查看设备基本信息、软件信息、系统状态以及员工登录记录。 主动采集星连客户端日志。 为员工设备添加扩展字段。

终端登记	该功能用于区分企业设备和个人设备，以及标记设备属性等需求。您可以通过一个或多个终端登记策略，为不同类型的终端设备配置登记内容。后续策略生效时，在生效范围内的员工可通过星连客户端主动登记设备分组或属性。
软件统计	该功能需手动启用，启用后星连会收集终端设备内已安装的软件信息，并上报管理后台供您查看。
软件分发	如果您的企业需要为员工设备统一安装软件，则可以通过软件分发功能批量分发软件至员工设备。

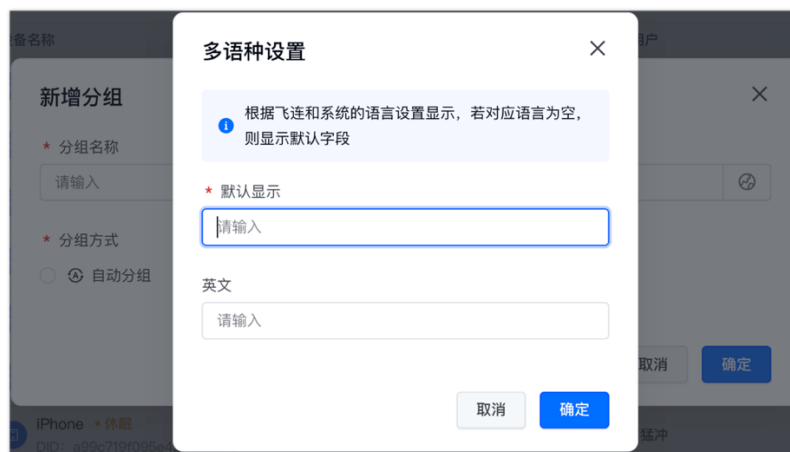
3.2 管理终端分组

已登录星连客户端的终端设备会被星连统计并展示在终端列表内，您可以根据企业设备管理要求，分组管理设备。

3.2.1 新增分组

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **终端列表**。
3. 在**终端分组**区域底部，单击**新增分组**。
4. 在**新增分组**对话框，完成以下配置，并单击**确定**。

分组名称：自定义名称。同时需要在输入框右侧单击多语种图标，配置多语种的**默认显示**和**英文**，其中**默认显示**配置项必填，填写后若对应语言为空则显示**默认显示**的值。



分组方式：

自动分组：基于设备的基础字段或扩展字段设置过滤条件，符合过滤条件的设备将会自动划分至该分组。该方式的分组内不支持手动增删设备。

例如，自动分组设置的过滤条件如下图所示，表示将所有操作系统为 Windows 的设备归为一组。

The screenshot shows a '新增分组' (New Group) dialog box. It has a title bar with a close button (X). The main content area is divided into sections. The first section is labeled '* 分组名称' (Group Name) and contains a text input field with the value 'Windows 设备组'. The second section is labeled '* 分组方式' (Grouping Method) and contains two radio buttons: '自动分组' (Automatic Grouping) and '手动分组' (Manual Grouping). The '自动分组' radio button is selected. Below the radio buttons, there are three dropdown menus: '操作系统' (Operating System), '属于' (Belongs to), and 'Windows'. The '操作系统' dropdown is open, showing a list of operating systems. The '属于' dropdown is also open, showing a list of categories. The 'Windows' dropdown is closed. At the bottom left of the dialog, there is a link '+ 添加条件' (Add Condition). At the bottom right, there are two buttons: '取消' (Cancel) and '确定' (Confirm).

手动分组：手动选择指定设备进行分组，该方式的分组内支持手动增删设备。

选择分组后需要设置**分组有效期**，设置说明：

如果设置了有效期，则有效期代表设备在分组内的有效时长。

到期后，设备将被踢出该分组。

不设置有效期则表示永久有效。

新增分组

* 分组名称

请输入

* 分组方式

☐ 自动分组 ☒ 手动分组

搜索员工、设备、设备id

已选择: 3个设备 清空

85

1

ro (2)

Carbon-Gen-8

3YX

分组有效期至

永久有效

取消 确定

3.2.2 重命名或删除分组

在**终端列表**页面的分组列表中，您可以单击分组名称后的 **...**，选择**重命名**或**删除**分组。

注意：

分组删除后不可恢复，请您谨慎操作。

如果设备只属于某一分组，则删除该分组后，设备会自动移动至未分组设备。

如果分组关联了星连相关功能的策略或者规则组，则分组删除后，会影响对应策略与规则组的生效状态。

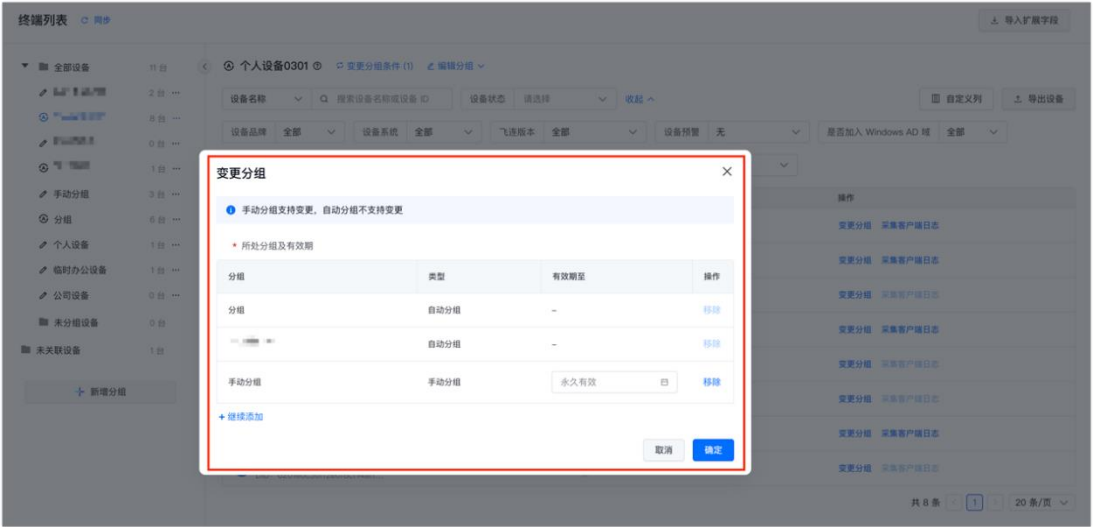


3.2.3 变更设备分组

在终端列表页面的指定分组中，找到指定设备，在操作列单击**变更分组**，在对话框中支持以下变更操作：

说明：只能变更**手动分组**类型的设备分组。设备已归属的**自动分组**类型的设备分组不可被手动移除，也不支持手动添加**自动分组**类型的设备分组。

- 已添加的**手动分组**类型的设备分组，支持单击**移除**，移除该分组。
- 单击**继续添加**，支持添加多个**手动分组**类型的设备分组。
- 手动分组**类型的设备分组可变更分组有效期。
 - 如果设置了有效期，则在分组到期后，设备将被踢出该分组。
 - 不设置有效期则表示永久有效。



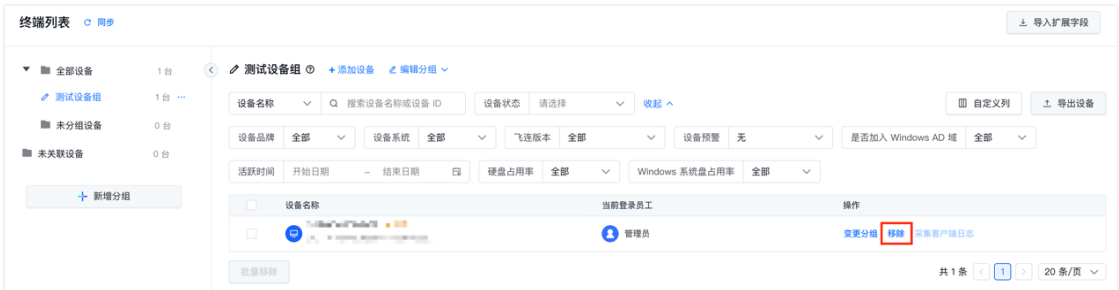
3.3 在分组内移除设备

在**终端列表**页面的指定分组中，找到指定设备信息，在**操作**列单击**移除**，可将设备移除当前分组。

注意：

仅手动分组类型的设备分组内可以移除设备。自动分组类型的设备分组内不能手动添加或者移除设备。

如果设备只属于某一分组，则在该分组内将设备移除后，设备会自动移动至未分组设备。



3.4 查看终端设备信息

当企业员工登录星连客户端后，星连会收集客户端所在设备的信息并上传至星连管理后台。您通过星连管理后台的终端列表，可查看终端设备的属性、已装软件或者系统运行状态等信息。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **终端列表**。
3. 在指定设备分组内，找到并单击指定设备名称。
4. 在设备详情界面，查看以下设备信息。



各信息页签说明如下表：

信息页签	说明
基本信息	查看设备所属分组、星连版本、操作系统、序列号、IP 地址以及 MAC 地址等基本信息。
软件列表	如果您已开启软件统计功能，则可以查看星连客户端（桌面端）对应设备已安装的软件信息。关于软件统计功能的更多信息，请参见《4.10 查看软件统计情况》。
登录记录	查看当前设备登录星连客户端时的时间、IP 地址、地理位置以及登录帐号等信息。
系统状态	查看设备的系统信息以及硬盘、CPU、内存的运行状态。 说明： 仅支持查看星连桌面客户端对应设备的系统状态，且需要设备为活跃状态才有监控数据。
日志采集	查看主动采集客户端日志的操作记录，并支持下载日志。关于客户端日志采集功能的更多信息，请参见《4.5 采集客户端日志》。

3.5 采集客户端日志

在星连管理后台的终端列表中，支持主动采集指定设备的客户端日志信息。该功能可以帮助企业管理员快速定位、排查员工设备存在的异常问题。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **终端列表**。
3. 在指定设备分组内，找到需要采集客户端日志的设备信息。
4. 在设备的**操作列**，单击**采集客户端日志**。

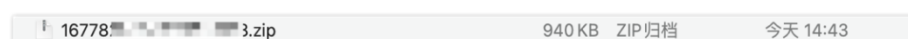
说明：采集客户端日志功能需要确保设备对应的星连客户端版本为 v2.1.0 及以上，否则无法采集日志。

5. 在弹出的**日志采集**界面中，等待系统采集结束，然后单击**下载日志**。

设备状态活跃且网络连通时，系统会立刻开始采集日志。如果设备状态不活跃，则系统会等待 24 小时，在此期间设备只要处于活跃状态且网络连通时，系统便会采集日志信息。如果超时则采集任务失败。



下载至本地的日志压缩包示例如下图，解压压缩包即可获取源自星连客户端的日志统计信息。



3.6 导入设备扩展字段

星连默认为终端设备提供了基础字段。如果您的企业有额外的终端属性管理需求，则可以在星连管理后台为设备预先导入扩展字段，待终端设备安装并登录星连客户端后，系统会通过 MAC 地址或者 SN 号匹配设备并自动填充扩展字

段信息。

操作步骤

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择**终端管理** > **终端列表**。
- 3. 在页面右上角，单击**导入扩展字段**。
- 4. 在**批量导入设备的扩展字段**页面，依次完成以下配置。
 - a) 在页面内的**第一步**区域，单击**修改配置**。

批量导入设备的扩展字段

第一步

配置 Excel 模板字段

修改配置

字段名称	字段类型	是否必填
deviceid	字符串	非必填
deviceid	布尔值	必填
deviceid	日期	必填
deviceid	整数	非必填
deviceid	枚举值	必填
deviceid	枚举值	必填
baseid	枚举值	必填
设备工区	枚举值	必填
设备公司资产	布尔值	非必填
设备公司设备	布尔值	必填
设备价格	小数	非必填
是否是公司设备	布尔值	非必填

第二步

选择设备标识字段

MAC 地址

SN 号

第三步

Excel 模板下载

设备导入模板

点击下载

第四步

上传准备好的 Excel

重新上传

确认导入

- b) 在**修改 Excel 模板字段**界面，单击**添加字段**。
 - c) 在**添加扩展字段**对话框，添加扩展字段并单击**确定**。

添加扩展字段

* 字段名称

请输入

* 字段类型

请选择

* 是否必填

必填

非必填

取消

确定

配置说明：

配置项	说明
字段名称	1. 自定义名称用于标识该字段。 2. 在字段名称输入框右侧，单击多语种图标，配置多语种的默认显示和英文，其中默认显示配置项必填，填写后若对应语言为空则显示默认显示的值。
字段类型	可选择的字段类型有 字符串 、 布尔值 、 整数 、 小数 、 日期 、 枚举值 。
枚举值	仅当 字段类型 选择 枚举值 后才会出现的配置项。您需要填写枚举值的中文与英文，单击 添加 支持添加多个枚举值。
是否必填	设置扩展字段 必填 或者 非必填 。

- d) 在页面内的第二步区域，选择设备标识字段，可选 MAC 地址或者 SN 号。
- e) 在页面内的第三步区域，下载设备导入模板。
- f) 在本地打开设备导入模板，编辑表格，填写设备对应的 MAC 地址或者 SN 号，以及自定义的设备扩展字段值。

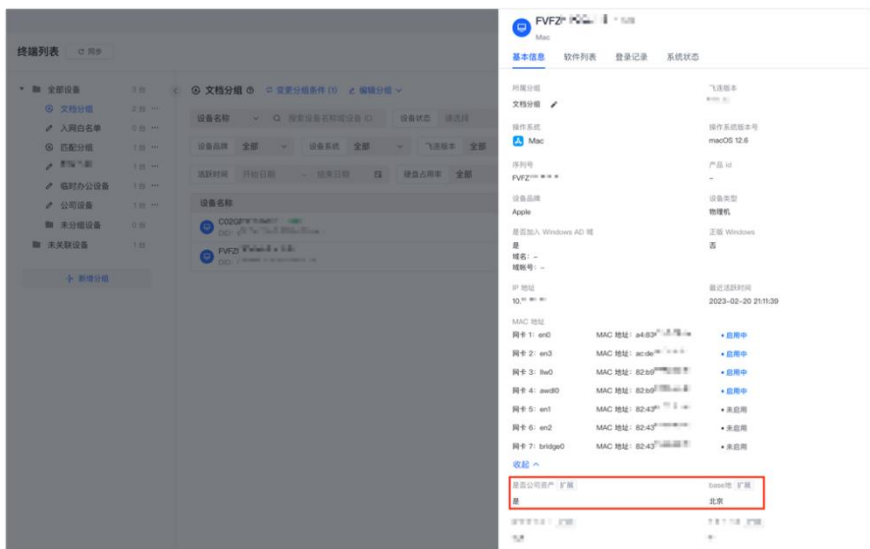
说明：如果存在枚举值类型的扩展字段，则在 Excel 模版中该字段对应的单元格为下拉列表。您需要保证选择的值与星连管理后台设置的枚举值完全匹配，否则后续上传文件可能导致异常报错。

- g) 返回星连管理后台，在页面内的**第四步**区域，单击**重新上传**，将本地已编辑好的文件上传至星连管理后台。
- h) 在页面底部单击**确认导入**。

成功导入后，您可以在**未关联设备**分组中查看预置的扩展字段信息。



待终端设备安装并登录星连客户端后，系统会自动补充设备的基础字段，并关联预置的扩展字段完善设备整体属性。在设备的详情页，您可以查看到设备的基本字段以及扩展字段。



3.7 添加终端登记策略

终端登记功能用于解决企业设备和个人设备的区分、标记设备属性等需求。在终端登记功能中添加一个或多个登记策略后，在策略生效范围内的员工可通过星连客户端自主发起变更设备分组或者设备属性的申请，例如员工可以申请将个人设备变更为办公设备。

3.7.1 使用说明

终端登记策略支持设置多个，以策略配置的优先级高低依次生效策略。您可以根据企业内员工设备实际的登记需求，灵活配置策略组合。

3.7.2 操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **终端登记**。
3. 在**终端登记**页面的**登记策略**页签，选择以下任意方式新建登记策略。

方式一：基于模板添加登记策略

星连默认提供了登记策略模板，您可以复制模板，在模板基础上添加登记策略。



方式二：自定义添加登记策略

单击**添加策略**，手动创建新的登记策略。

4. 配置策略的**基本信息**、**登记条件**、**登记内容**、**审批方式**、**生效对象**，并单击**确定**。

基本信息：自定义策略名称和匹配优先级。

匹配优先级用于指定当前策略的优先级，取值范围为 0~100，数值越高优先级越高。员工可以同时生效多条策略，按优先级数值大小依次匹配策略，策略命中后停止匹配，如果一直未命中，则执行完所有策略后停止匹配。如果存在两条数值相同的策略，则优先执行策略编辑时间最新的一条。

基本信息

策略名称

请填写

匹配优先级

0

100

0

登记条件：支持选择**设备分组**或者**设备属性**。设置登记条件的具体操作说明如下：

选择**设备分组**后，需要指定可选的分组范围。

登记条件

当员工的终端

设备分组

属于

匹配分组

公司设备

临时办公设备

继续添加

选择**设备属性**后，需要指定基础字段或者扩展字段，以及字段取

值。

例如下图所示的登记条件，表示设备属性内 **base 地**这个扩展字段值为**北京**或**杭州**的员工会触发该登记策略。

登记条件

* 当员工的终端

设备属性

base地

属于

北京

杭州

+ 继续添加

单击**继续添加**，可添加多条登记条件，多条之间的关系可选**且**或者**或**。

登记条件

* 当员工的终端满足以下条件时，需要进行登记

且

或

设备分组

属于

手动分组

设备属性

设备名称

不等于空

+ 继续添加

登记内容：设置展示在星连客户端的终端登记提示框的**中文**与**英文**内容。各内容配置项说明如下：

注意：

登记内容区分中文与英文，且各语种均配置了默认值。您在修改某一语种时务必同步修改另一语种，避免不同语种的终端登记内容不同。

设置过程中您可以在配置项右侧实时预览登记内容的效果。

标题：自定义提示框的标题。

描述：自定义提示框的描述信息。

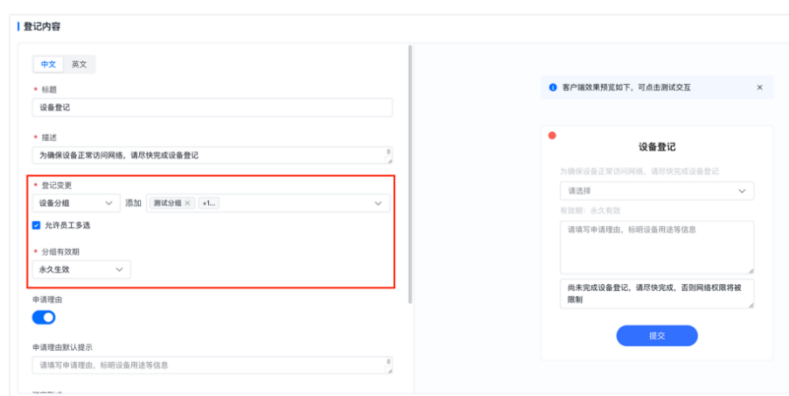
登记变更：选择**设备分组**或者**设备属性**。不同选项的具体配置有所不同，说明如下：

配置一：设备分组

选择**设备分组**后，需要设置可变更分组的范围，支持选择多个分组。

设置是否**允许员工多选**。如果**设备分组**设置了多个分组，则允许员工多选后，在客户端进行设备登记时，可手动选择多个分组。

设置**分组有效期**，分组有效期表示员工设备变更至新分组后，在该分组内的有效时长。到期后，该设备会自动移除分组。有效期默认为**永久有效**，支持设置为**7 天、30 天、90 天、180天**或者**自定义有效时长**。



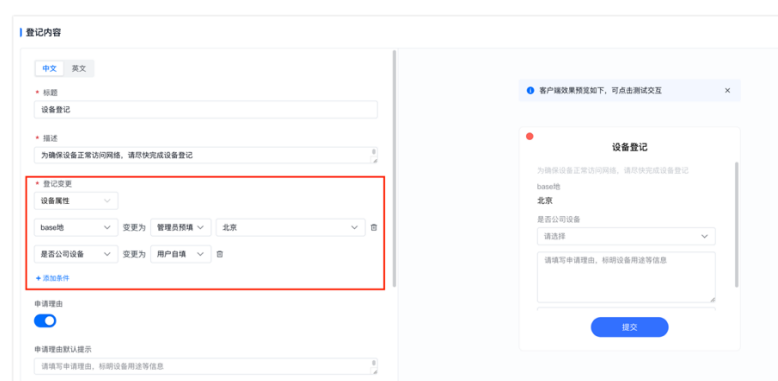
配置二：设备属性

选择设备属性内包含的任一扩展字段，并设置属性的变更方式。变更方式说明：

用户自填：变更后的扩展字段值需要员工在客户端内手动填写或者选择。

管理员预填：您需要配置预填写的值，后续员工在客户端内仅能查看到属性的预填值。

单击**添加条件**，可添加多个属性变更条件。



申请理由：您可以选择是否开启申请理由。

开启**申请理由**开关后，员工在星连客户端进行终端登记时需要填写申请理由。

关闭**申请理由**开关后，员工在星连客户端进行终端登记时无需填写申请理由。

申请理由默认提示：仅当开启**申请理由**开关后才会出现该配置项。星连已提供默认提示信息，支持自定义编辑。

弹窗形式：选择星连客户端内终端登记提示框的弹出方式。

全局提示内容：内容支持自定义编辑，最终会在星连客户端的界面顶部以条幅形式进行全局提示。

审批方式：支持选择自动审批通过或手动审批。

自动审批通过：无需手动操作，员工发起的申请会自动通过，星连管理后台仅做审批记录。

手动审批：需要手动操作，员工发起的申请需要您在星连管理后台的终端登记审批页面手动进行审批。

您可以自行选择**第三方通知给审批人**以及**第三方通知给申请人**，选择后需要设置第三方机器人，以便对应人员接收审批消息或审批结果。

注意：

- 如果您还未创建第三方机器人，请先创建机器人。具体操作，请参见《13.1.5 管理第三方 IM》。
- 星连默认提供了第三方通知内容，其中 **#员工**、**#部门**、**#操作时间**为变量，会根据实际信息动态传入值。第三方通知内容支持您自定义编辑，编辑后如果需要恢复至默认值，则请单击内容重置。

生效对象：支持选择全部员工或者部分员工。如果选择部分员工，则需要按**部门**维度设置生效范围。

5. 添加完成后，返回**登记策略**页签，找到新添加的策略，在**操作**列开启策略开关使策略生效。



3.8 管理终端登记策略

您可以在终端登记中，管理存量的终端登记策略，支持调整策略生效状态或者编辑、复制、删除策略。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **终端登记**。
3. 在**终端登记**页面的**登记策略**页签，选择以下操作。



如上图①区域，支持搜索、设置过滤条件或者排序的方式，查找登记策略。

如上图②区域，查看登记策略的名称、生效员工以及审批方式等信息。同时支持以下操作：

在**优先级**列，支持手动调整策略的优先级。

在**操作列**，支持控制策略的生效状态，以及**编辑、复制或删除**策略。

注意：

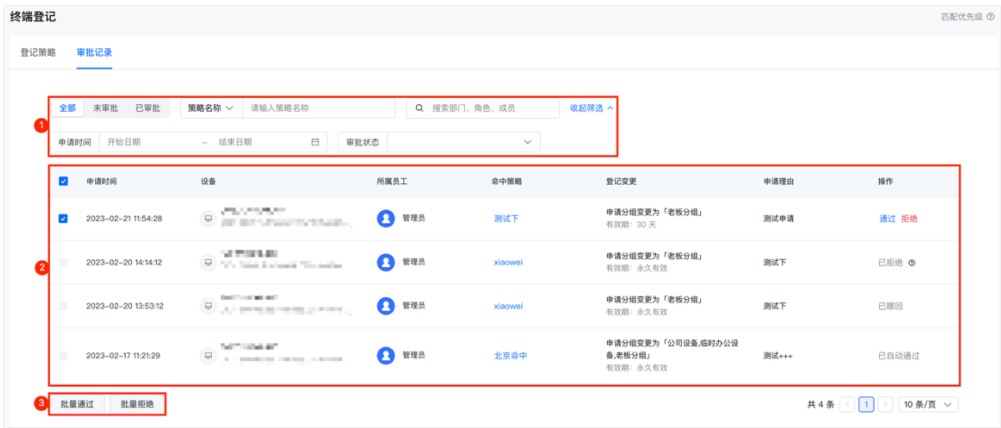
策略开关用于控制是否生效该策略，如果策略开关为关闭状态，则该策略不会生效至相应的员工客户端内。
策略一旦被删除则无法恢复，请您谨慎操作。

3.9 审核终端登记申请

如果生效中的终端登记策略内配置了手动审批，则当员工发起终端登记申请后，您需要在星连管理后台手动进行审批，审批结果以及历史审批记录均支持查看。

操作步骤

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择**终端管理** > **终端登记**。
- 3. 在**终端登记**页面，单击**审批记录**页签。
- 4. 在**审批记录**页签，审核终端登记申请。



如上图①区域，可选**全部、未审批、已审批**记录进行查看，也支持搜索或者设置过滤条件查找审批记录。

如上图②区域，在**操作列**选择**通过或拒绝**，逐个审批终端登记申请。

如上图③区域，支持**批量通过**或**批量拒绝**终端登记申请。

说明：

拒绝或**批量拒绝**时，您需要设置拒绝理由，该理由会同步至员工的星连客户端内。

审批后，**操作列**将展示审批结果。

3.10 查看软件统计情况

星连的软件统计功能用于统计终端设备上已安装的软件信息。本章节介绍如何在星连管理后台查看终端的软件统计情况。

3.10.1 注意事项

目前仅支持统计已安装并登录星连客户端（桌面端）的设备信息，包含 Mac、Windows、Linux 系统的设备。

3.10.2 操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **软件统计**。
3. 在**软件统计**页面，支持查看以下统计信息。

说明：首次使用软件统计功能时，需要根据页面提示手动开启该功能。

软件统计

已开启软件统计功能 导出列表

操作系统 All Windows Mac Linux 账号状态 请选择 软件状态 请选择 设备分组 请选择

设备状态 选择 × +1 部门 搜索部门 Q 软件名称 软件名称

软件名称	软件版本	操作系统	Bundle ID/厂商	已安装终端数	采集用户数	安装率
企业微信	4.0.9	Mac	com.tencent.WeWorkMac	1台	1人	33.33%
钉钉	7.0.0	Mac	com.alibaba.DingTalkMac	2台	2人	66.66%
飞书	5.31.0.29 5.31.0.23	Mac	com.electron.lark	2台	2人	66.66%
企业微信	4.0.9	Mac	com.tencent.WeWorkMac	1台	1人	33.33%
钉钉	7.0.0	Mac	com.alibaba.DingTalkMac	1台	1人	33.33%
飞书	5.31.0.29 5.31.0.23	Mac	com.electron.lark	1台	1人	33.33%
企业微信	4.0.9	Mac	com.tencent.WeWorkMac	2台	2人	66.66%
钉钉	7.0.0	Mac	com.alibaba.DingTalkMac	2台	2人	66.66%

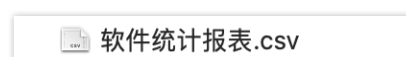
共 70 条 1 2 3 4 5 6 7

如上图①区域，支持设置**操作系统**、**帐号状态**、**软件状态**等过滤条件，或以**软件名称**等维度的关键词搜索指定软件。

如上图②区域，查看具体的软件统计信息，包括**软件名称**、**操作系统**和**已安装终端数**等信息，其中在**已安装终端数**列，单击对应的字段值可跳转至软件统计详情页（如下图所示），查看终端设备列表。



如上图③区域，单击**导出列表**，可以将软件统计列表导出至本地，导出的文件如下图所示。



3.11 分发软件至员工设备

通过星连的软件分发功能，您可以将企业办公所需的 Windows 或 Mac 端的指定软件批量分发至指定员工设备。

3.11.1 操作指引

软件分发提供安全校验功能，您可以选择启用。启用后，添加软件时需要录入分发私钥或软件签名，以保障安装包的安全性。关于功能启停的具体操作，请参见《3.11.2 选择开启安全校验》。

目前支持分发 Windows 或 Mac 端的软件包，分发软件需要以下操作步骤。

3.11.1.1 《3.11.3 添加软件》

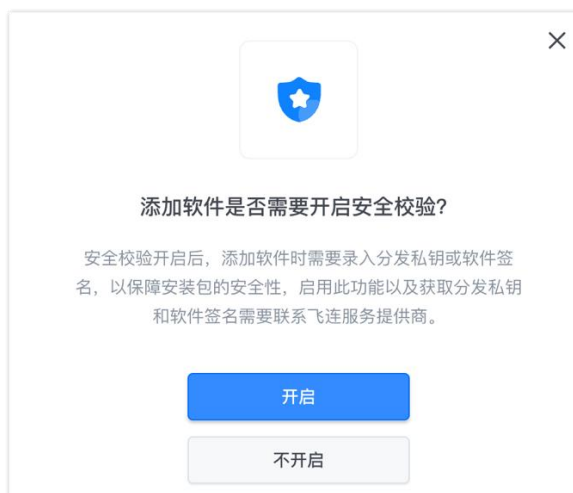
3.11.1.2 《3.11.4 分发软件》

软件分发功能包含软件清单和分发记录两个模块。管理这两个模块的具体操作，请参见《3.11.5 管理软件清单》、《3.11.6 管理分发记录》。

3.11.2 选择开启安全校验

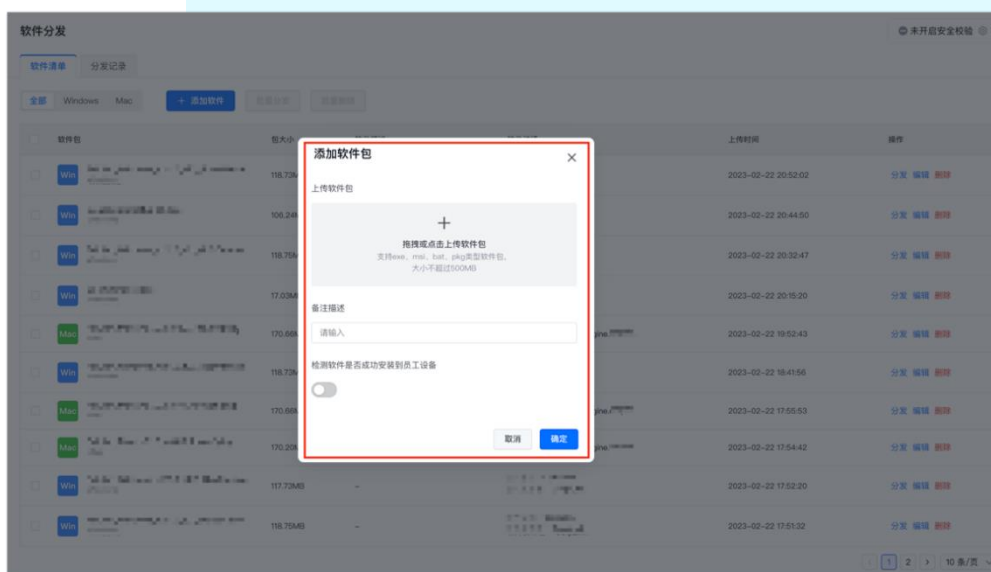
1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **软件分发**。
3. 在**软件分发**页面的右上角，单击**未开启安全校验**。
4. 在**添加软件是否需要开启安全校验**对话框，选择**开启**或**不开启**。

说明：安全校验开启后，添加软件时需要录入分发私钥或软件签名，以保障安装包的安全性。启用此功能以及获取分发私钥和软件签名需要联系星连服务提供商。



3.11.3 添加软件

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **软件分发**。
3. 在**软件分发**页面的**软件清单**页签，单击**添加软件**。
4. 在**添加软件包**对话框，完成以下配置，并单击**确定**。



配置项说明：

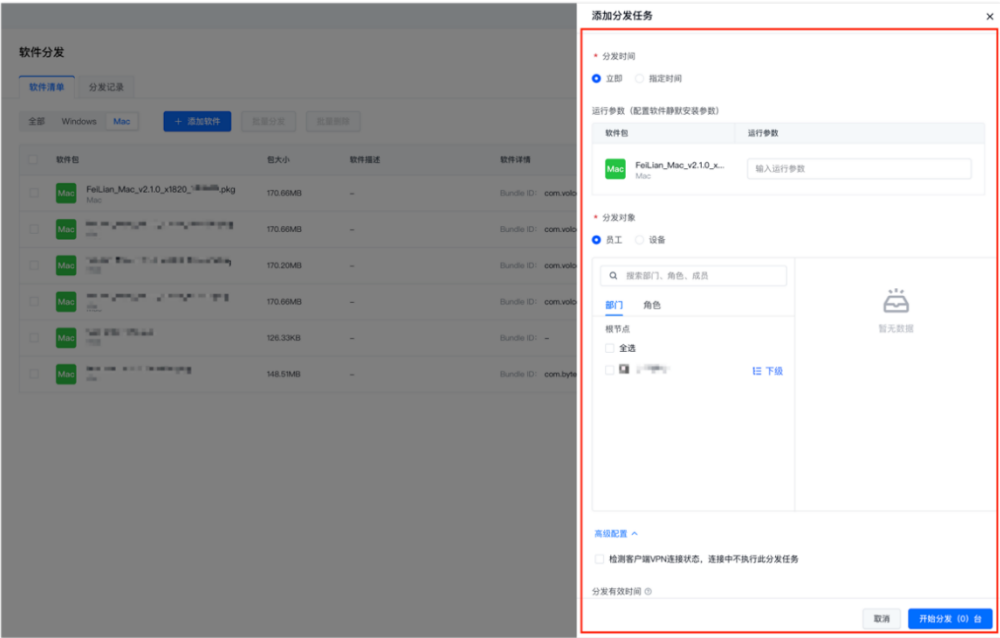
配置项	说明
-----	----

上传软件包	支持 exe、msi、bat、pkg 类型的软件包，软件包大小不能超过 500 MB。（超过该大小限制的软件建议让用户主动从软件库下载，配置方式请参见《12.5 为客户端配置软件库》。） 说明： 软件包上传后，星连会自动检测适配的操作系统（Windows 或 Mac），请确保您上传的软件包正确可用。 如果上传的软件包为星连服务提供（例如星连客户端软件包），则星连会自动检测并配置软件包信息，且默认已开启了检测软件是否成功安装到员工设备的功能，您只需要配置备注描述。
备注描述	自定义备注信息。
检测软件是否成功安装到员工设备	开启后，在分发软件包时可检测软件包是否成功安装到员工设备。注意开启后需要配置以下参数信息：
	Windows 软件包：配置软件全称和软件发布者，您可以根据页面提示信息手动获取参数值。 Mac 软件包：配置 Bundle ID，您可以根据页面提示信息手动获取参数值。
软件签名	如果您开启了安全校验，则需要设置软件签名。 您可以通过界面提示信息查看软件签名的获取方式。 在软件签名右侧，单击关闭私钥输入或者开启私钥输入，选配私钥信息（变更此功能后需要联系星连服务提供商配合修改火山引擎侧配置）。

3.11.4 分发软件

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **软件分发**。

- 3. 在**软件分发**页面的**软件清单**页签，找到指定的软件包。
- 4. 在软件包的操作列，单击**分发**。
- 5. 在**添加分发任务**界面，完成以下配置，并单击**开始分发**。

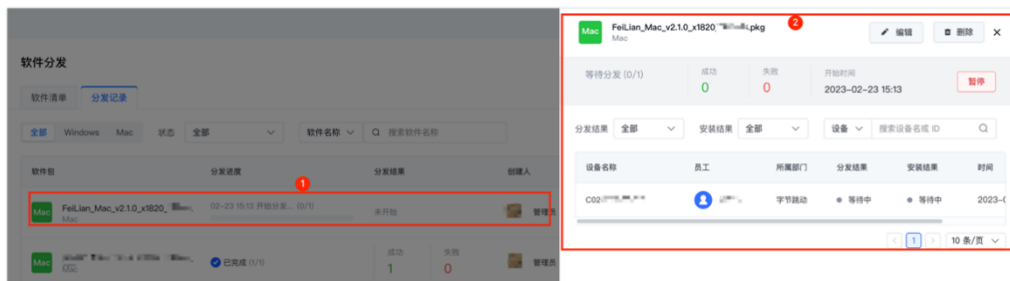


配置项说明：

配置项	说明
分发时间	立即：添加分发任务完成后，软件包立即分发至指定范围的员工设备内。 指定时间：手动设置固定时间进行软件分发。
运行参数（配置软件静默安装参数）	软件分发时，软件包采取静默安装（即安装时用户无需操作，通过默认方式直接安装）的方式完成安装。如果软件包静默安装时需要执行运行参数才能完成，则请设置运行参数。
分发对象	设置软件包在企业内的分发范围。如果选择 员工 ，则需要以 部门或角色 的维度设置员工范围。如果选择 设备 ，则需要以 设备名称或设备分组 的维度设置设备范围。
检测客户端 VPN 连接状态，连接中不执行此分发任务	选中该配置项后，设备如果处于 VPN 连接状态则不会执行分发任务，需等待 VPN 断开连接后才会执行分发任务。
分发有效时间	指定当前分发任务的有效时长，可选 一周 或者 指定时间 。仅在有效期内，分发任务会向员工设备分发软件包。如果超过有效期，则分发任务自动过期，不再分发软件包。
分发频率控制	控制同时分发的设备数。 如果选择不启用，则表示不控制分发频率。 如果选择启用，则需要设置每分钟分发设备的台数。
分发限速（单设备）	指定分发至单设备时软件包的传输速率。 如果选择不启用，则表示不限制分发的传输速率。 如果选择启用，则需要设置单设备传输速度，单位：KB/s。

6. 返回**软件分发**页面，在**分发记录**页签，查看分发任务执行状态。

在分发记录列表中您可以看到分发进度。单击软件包名称，可进入详情页查看具体的分发情况。



3.11.5 管理软件清单

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **软件分发**。
3. 在**软件分发**页面的**软件清单**页签，找到指定的软件包，选择**分发**、**编辑**或**删除**操作。



分发：配置分发任务将软件包分发至指定设备中。具体操作，请参见《3.11.4 分发软件》。

编辑：支持编辑软件包对应的备注描述、软件全称、软件发布者或者 Bundle ID 信息。

软件全称、软件发布者为 Windows 软件包参数，Bundle ID 为 Mac 软件包参数。如果参数没有默认值，则您可以根据页面提示信息手动获取参数值。

删除：该删除操作包含删除选中的软件包及对应未完成的软件分发任务。

说明：删除后资源不可恢复，请您谨慎操作。

3.11.6 管理分发记录

1. 登录星连管理后台。
2. 在左侧导航栏，选择**终端管理** > **软件分发**。
3. 在**软件分发**页面，单击**分发记录**页签。
4. 在**分发记录**页签，支持**查看**、**编辑**或**删除**分发任务。



在**操作**列单击**查看**，可查看分发任务的详细信息。

如果**指定时间**分发的任务还未开始分发，则在**操作**列，支持**暂停**分发任务，或者**编辑**分发任务。

如果软件包在上传时，未开启**检测软件是否成功安装到员工设备**功能，则在**安装结果**列会提示**无法获取**。

删除分发任务后不可恢复，请谨慎操作。

如果**删除**分发任务时，任务正在执行则任务不会中止，软件最终会分发至指定设备。

4. 动态安全

星连基于行业实践与威胁研究，内置了全面且灵活的办公安全策略框架。您可以根据企业安全风险要求、差异化管理需求等实际场景，通过星连动态控制功能构建企业定制化的动态安全能力，进而降低企业安全制度落地难度与成本。

4.1 功能介绍

星连的动态控制功能模块联动身份认证、终端管理、终端基线、数据防泄漏以及终端防病毒等功能模块，当您根据企业安全要求或业务管理需求手动配置了动态决策后，星连会对员工行为、终端风险持续检测并评估。当存在符合动态决策的行为或风险时，星连会实时做出响应，依照决策内指定的处置规则进行处理。此外，在动态控制模块，星连会统计各员工终端的安全状态，您可以通过该统计信息及时处理风险终端。关于动态控制内包含的所有功能说明如下表：

功能项	说明
安全状态	当您所在的企业已配置好组织架构，且员工终端已通过星连客户端接入星连管理后台后，您可以通过安全状态功能项查看到员工终端信息。后续星连会根据实际情况动态更新各个终端的风险事件、动态处置记录等信息。该功能便于您整体把控员工

4.2 管理安全状态

当星连管理后台已接入员工的多终端设备后，星连会将各个终端的信息统计在安全状态功能中。本文介绍在安全状态功能中统计的终端信息，以及支持的操作。

4.2.1 查看终端安全状态

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择动态控制 > 安全状态。
- 3. 在安全状态页面，支持以下操作。



操作说明：

如上图①区域，支持通过过滤条件筛选指定的终端设备。

如上图②区域，支持选择指定部门查看部门内各员工终端的安全状态。

如上图③区域，展示各个终端的安全状态信息。其中您需要注意：

单击设备名称，您可以在右侧界面查看设备的详细信息。

终端设备详细信息说明：

说明：星连中必须存在已生效的终端基线检测策略、数据防泄漏策略或者终端防病毒策略，并且任一策略检测到终端内存在风险事件后，您才可以查看到策略信息与风险项。

安全状态页签：终端基线、应用风险、进程风险、病毒风险的检测结果数据统计。

告警事件页签：终端基线、应用风险、进程风险、病毒风险、数据泄露的事件详情。

处置记录页签：触发动态决策规则组后，被规则组处置的记录详情。

生效策略：检测出来当前终端设备风险项的策略信息，包括数据防泄漏策略、终端基线检测策略、终端防病毒策略。

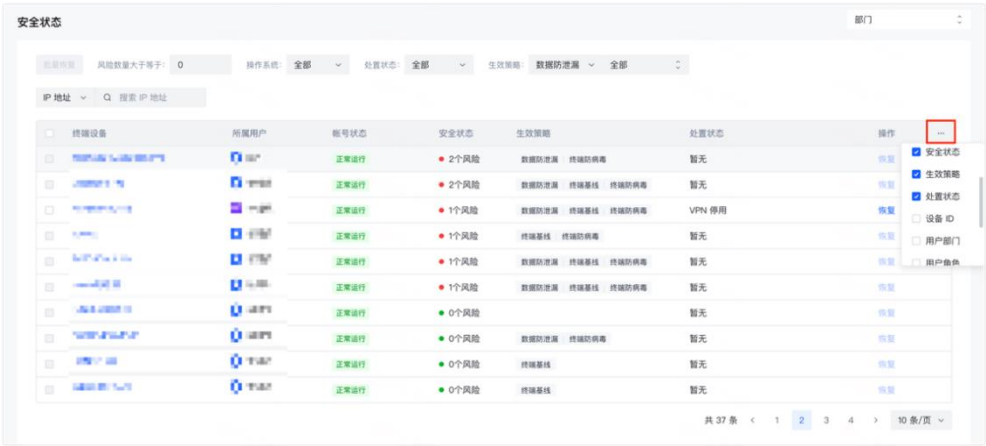
说明：星连中必须存在已生效的终端基线检测策略、数据防泄漏策略或者终端防病毒策略，并且任一策略检测到终端内存在风险事件后，您才可以查看到策略信息。

操作：如果当前终端被规则组处置，限制了部分功能的使用，您可以待终端恢复安全后，在**操作**列单击**恢复**，快速恢复终端原有的使用权限。

4.2.2 自定义安全状态列表参数

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择**动态控制** > **安全状态**。

在**安全状态**页面找到如下图红框所示图标，单击图标，手动调整列表参数。



4.3 使用动态决策

您可以在动态决策中添加规则组，以限制员工触发指定行为或者终端存在指定风险时，由星连自动进行处理。规则组的配置全面且灵活，可选星连提供的规则模板快速构建动态控制体系，也可选自定义规则组的触发方式与处置方式，使动态控制体系更符合企业实际需要。

4.3.1 手动添加规则组

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择**动态控制** > **动态决策**。
- 3. 在动态决策页面，单击**新建规则组**。
- 4. 在新增规则组页面，依次完成以下配置。

配置区域	配置项说明
基本信息	规则组名称：自定义名称，用于标识当前规则组。
触发条件	支持选择动态触发或者操作触发。 触发方式：动态触发和操作触发的触发方式可选项不同。 具体说明如下： 动态触发：当终端产生风险事件、病毒事件、数据防泄漏事件时，动态触发当前决策。部分触发方式说明： 终端风险检测是指星连客户端每次上报安全检测状态时触发。 终端风险变更是指当终端内的风险情况发生变化时触发，例如一个风险项变更为两个风险项。 支持设置周期触发当前决策。 操作触发：当员工在终端内进行 VPN 连接、入网、登录登出或访问应用等操作时，触发当前决策。 触发参数：支持设置一个或多个参数。参数包含帐号信息、设备信息、行为信息、设备安全状态、操作信息、内置函数多个维度，具体的可选参数请以实际页面展示的信息为准。

处置规则	默认仅有一条处置规则，您可以单击添加规则设置多条处置规则，规则存在优先级属性，越靠左的规则优先级越高。在一条处置规则内，您需要配置以下信息： 参数组合：设置触发参数的组合状态，通过运算符关联各个参数。支持的运算符如下： in：在某集合内 not in：不在某集合内 >：大于 >=：大于等于 ==：等于 !：非 !=：不等于 <：小于 <=：小于等于 ++：加 --：减 * /：除 &&（与）：与 （或）：或 处置方式：当触发当前规则组时，星连系统如何进行处置。包含方式如下： 网络：包含降级、禁用的处置方式，其中选择降级的处置方式时，还需要指定降级的策略（资源访问受限或者限制不可访问的资源）。 操作：包含强制退出登录、帐号停用、重置 Wi-Fi 密
--------------------	--

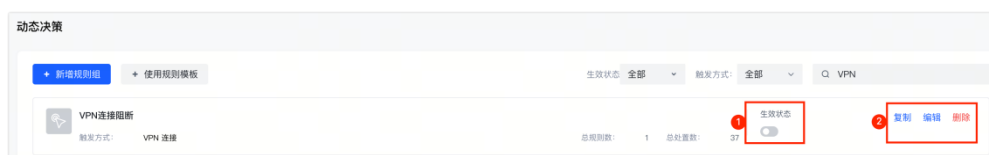
	码。
--	----

	通知：支持第三方通知员工、通知到星连客户端、恢复通知，其中： 第三方通知员工：需要关联第三方机器人进行消息通知。关于第三方机器人的管理操作，请参见《7.1.5 管理第三方 IM》。 通知到星连客户端：支持设置系统通知或者强提醒，并需要手动配置通知或强提醒的内容。 处置自动恢复后主动通知：开启该开关后，您可以选择设置第三方通知员工、通知到星连客户端。当终端风险被修复，VPN、Wi-Fi 等处置自动恢复的场景下，主动向员工发送通知。 第三方通知员工：需要关联第三方机器人进行消息通知。关于第三方机器人的管理操作，请参见《7.1.5 管理第三方 IM》。 通知到星连客户端：发送系统通知，您需要手动配置通知内容。
--	---

注意：如需最新动态安全最佳实践配置手册，请联系星连技术支持人员获取。

4.3.2 管理规则组

1. 登录星连管理后台。
2. 在左侧导航栏，选择**动态控制** > **动态决策**。
3. 在**动态决策**页面，找到指定的规则组，支持以下操作。



如上图①区域，可设置策略的生效状态。

当开关打开时，当前规则组生效，星连将会按照规则组配置处置终

端。

当开关关闭时，当前规则组不生效，终端行为不会触发该规则组。

如上图②区域支持**复制**、**编辑**或者**删除**策略。注意：

必须关闭**生效状态**开关，才可以编辑规则组。

规则组被删除后无法恢复，且星连将不会继续通过该规则组处置终端，但历史已处置的终端记录仍会保存在处置记录中。

4.4 查看处置记录

在处置记录功能中，星连统计了所有已触发动态决策的终端相应的处置结果。您可以通过处置记录查找指定的终端设备并查看设备信息、处置详情或源数据等信息。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**动态控制** > **处置记录**。
3. 在处置记录页面，查找对应的记录并查看详情。
4. 您可以在页面顶部设置自定义过滤条件，以查找指定的处置记录。

处置记录								
触发方式	全部	处置方式	全部	处置类型	全部	处置时间	开始日期 -- 结束日期	终端设备
处置类型	处置时间	命中规则	触发方式	终端设备	所属员工	账号状态	处置方式	操作
自动处置	2023.01.19 16:10:00	128 若15分钟内没有飞连心跳，则降级使用Wi-Fi	周期触发 (5分钟)	C02G1234567890	测试成...	正常运行	降级使用Wi-Fi	查看源数据
自动处置	2023.01.19 15:25:00	128 若15分钟内没有飞连心跳，则降级使用Wi-Fi	周期触发 (5分钟)	C02G1234567890	测试成...	正常运行	降级使用Wi-Fi	查看源数据
自动处置	2023.01.19 15:10:00	128 若15分钟内没有飞连心跳，则降级使用Wi-Fi	周期触发 (5分钟)	C02G1234567890	测试成...	正常运行	降级使用Wi-Fi	查看源数据

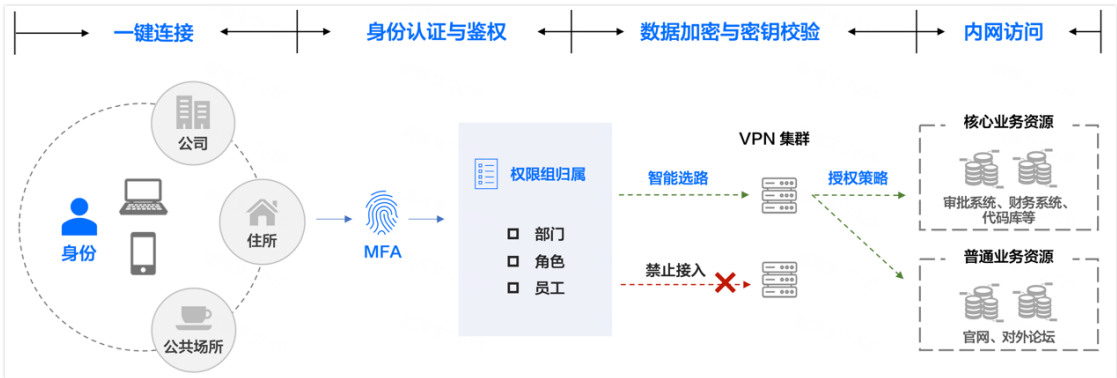
5. 虚拟专有网络

随着数字化办公的高速发展以及企业办公效率的提升，越来越多企业需要构建随时随地、多终端的无界办公模式，同时还需要兼具安全性与高效性。但构建无界办公模式面临着网络稳定性、终端兼容性、配置成本、运维成本以及数据安全等挑战。为此，星链以随时随地便捷办公，实现安全与效率的平衡为目标，提供了基于身份管理的**企业 VPN** 功能。

5.1 功能介绍

星链通过 **VPN** 管理功能帮助企业员工随时随地、安全接入办公网络。该功能具备细粒度资源管理与授权能力，并支持多因素认证（MFA），同时各 **VPN**节

点独立部署与运行，基于架构优势实现了灵活扩展与智能选路。此外，员工各类的终端设备免配置，提升了办公体验。星链 VPN 管理功能逻辑图如下：



星链 VPN 管理功能区分服务端与客户端。当企业购买星链后，需要由企业管理员在星链管理后台配置 VPN 节点，以及 VPN 的使用权限、访问权限等信息。管理员配置完成后，企业员工即可在终端设备的星链客户端中连接企业 VPN，连接后星链根据员工身份认证以及 VPN 权限配置，为员工分发指定的企业内网访问策略。具体说明如下：

身份管理与授权

星链 VPN 管理功能的实现基于身份认证功能。当您部署好 VPN 节点后，可以根据企业部门、角色、成员不同维度限制网络资源访问权，从而避免员工连通企业内网后无限制访问。

节点管理与授权

VPN 节点在默认情况下企业全员不可用，您需要配置 VPN 的使用权限，限制 VPN 使用权限的生效范围与生效时长。单个 VPN 节点内支持设置可见对象，仅可见对象范围内的员工可以查看并使用该 VPN 节点。

支持多因素认证（MFA）

您可以设置员工连接 VPN 时是否需要二次认证（动态口令、短信或邮箱验证码），仅符合准入策略的员工才能获取所属的网络资源访问权限，并且网络访问过程中均进行链路加密与密钥交换，保证端到端安全接入。

极速与全局模式

为了更好平衡安全与体验，星链在传统 VPN 默认提供的全局模式基础上新增了极速模式。与全局模式全部流量经加密隧道访问不同，极速模式需要您指定经 VPN 访问的域名站点，其他流量则通过本地网络访问。模式说明：

全局模式：当企业员工通过 VPN 连接企业内网后，终端上所有网络访问流量均通过企业内网。该模式下全量数据加密，可以保障员工的帐号与数据安全，但会增加 VPN 节点的负载压力。

极速模式：当企业员工通过 VPN 连接企业内网后，仅指定站点的访问流量通过企业内网，其他网络访问流量仍旧使用员工终端的本地网络进行访问。该模式下仅对指定站点做数据加密，但同时节省企业带宽，并减少 VPN 节点负载压力，提升了员工访问网络时的体验。

节点稳定与高可用

如果企业购买星链时选配了多个 VPN 节点，则星链可以通过 API 实现节点与域名解绑，智能选路以避免网络拥塞。企业管理员在配置好企业 VPN 后，星链会持续智能判断各节点的可用性与延时状态。无需管理员解析与配置，只需员工在星链客户端连接 VPN 时指定自动选择服务器，星链即可自动切换节点，以适配员工办公网络环境。

网络诊断与故障排查

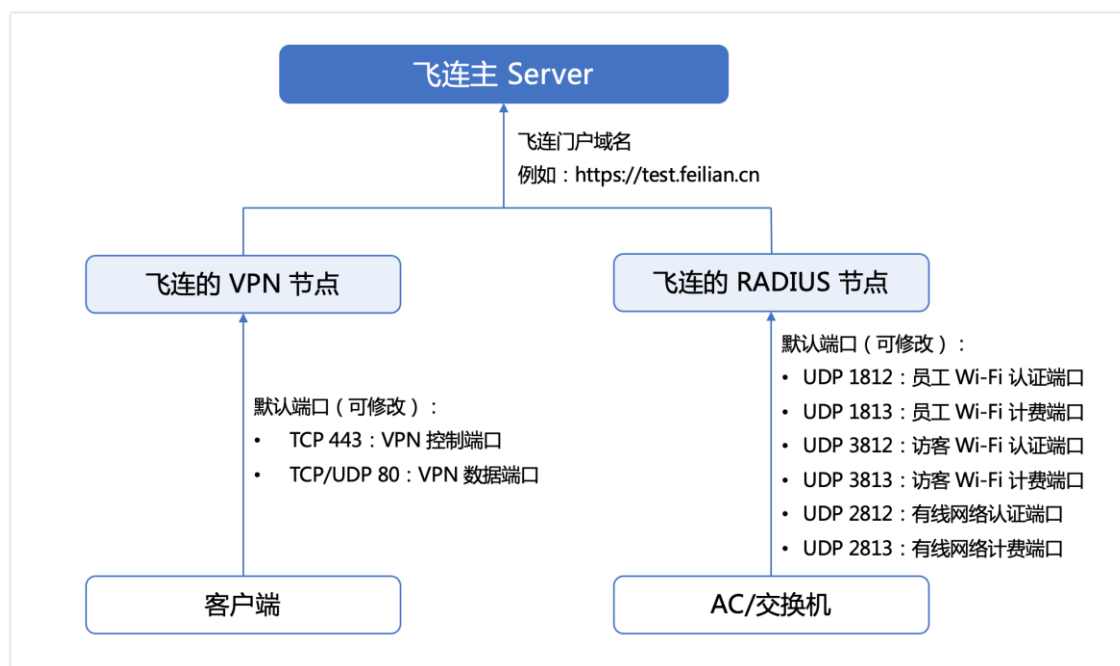
星链支持为企业构建在线 IT 管理能力，当终端发生网络故障或设备使用问题时，员工可以在星链客户端查看网络、路由以及本机信息，并支持一键反馈。反馈后由企业管理员在星链管理后台获取用户反馈以及相应的客户端日志，进行故障排查。

5.2 功能概览

功能项	说明
节点管理	在节点管理中添加 VPN 节点，可以为员工构建客户端连接 VPN 访问企业内网的远程办公环境。为确保 VPN 节点正常工作，星链为您提供了节点部署的建议与要求，更多信息，请参见《6.3 节点配置建议与要求》。 单个 VPN 节点最高并发员工数为 4000，在节点内支持自定义网络模式、可见对象等配置。
使用权限	配置好 VPN 节点后，节点默认全员不可用，您需要手动为员工配置 VPN 使用权限。配置权限时，支持为权限设置生效时长，到期后星链会自动回收权限，以满足需要临时使用 VPN 进行远程办公的场景。
访问权限	在访问权限功能页面，支持添加网络资源以及资源的访问策略，以限制员工通过 VPN 连接企业内网后允许访问的网络资源范围。
高级配置	在高级配置中，支持设置 VPN 策略（最大传输单元、客户端超时时间、二次认证、设备会话数等），以及配置 VPN 节点的极速模式网络资源。

5.3 节点部署建议与要求

关于 VPN 节点在星链服务中的部署架构如下图所示：



其中，VPN 节点服务器的防火墙策略说明如下：

对于 VPN 节点，允许访问目标为星链域名的 TCP 443 端口（域名的 IP 地址可通过 DNS 解析获取）。

对于 VPN 节点，允许公网客户端访问 VPN 节点 TCP 443 、TCP 和 UDP 80 端口（以实际设置的端口号为准）。

5.3.1 服务器资源配置参考

注意：请使用全新的服务器部署星链 VPN 节点。避免与其他运行中的应用服务发生冲突，而引起预期之外的网络转发问题。

服务器的配置参考如下表：

（建议）操作系统版本	最低配置	最大并发
CentOS 7、Debian 9 及 以上	4 核 CPU、4 G 内存	4000

上表为 VPN 单节点的配置资源参考，并发是指的单节点能够同时承载的用户数量。最大并发是指最大的单节点并发承载量，在该并发量下 VPN Server 的CPU、内存高负载运行，在该并发下建议服务器配置为 8 核 CPU、16 G 内存。如果您对并发数的需求超出 4000，则需要部署多个 VPN 节点。

5.3.2 网络要求

IP 地址要求

服务器	是否对公网开放	IP 地址示例	数量	备注
VPN Server	是	201.23.10.2（公网映射）	N，以订单中节点数量为准。	固定公网 IP 地址。
	否	192.168.1.2（内网）	N，以订单中节点数量为准。	固定内网 IP 地址。

网络端口开放要求

目的 IP	目的端口	协议	源 IP	是否可以修改	备注
VPN Server 映射到公网的 IP	443（默认端口，可修改）	TCP	任意	是	VPN 控制端口，外网开放。
	80（默认端口，可修改）	TCP、UDP	任意	是	VPN 数据端口，外网开放。

注意：VPN 节点需要访问星链门户域名的 TCP 443 端口。因此，如果您的 VPN 服务器配置了较为严格的防火墙规则（未全部放行出站规则），则需要出站规则放行 TCP 443 端口，并指定 IP 地址为星链门户域名解析对应的 IP 地址。

5.4 添加 VPN 节点

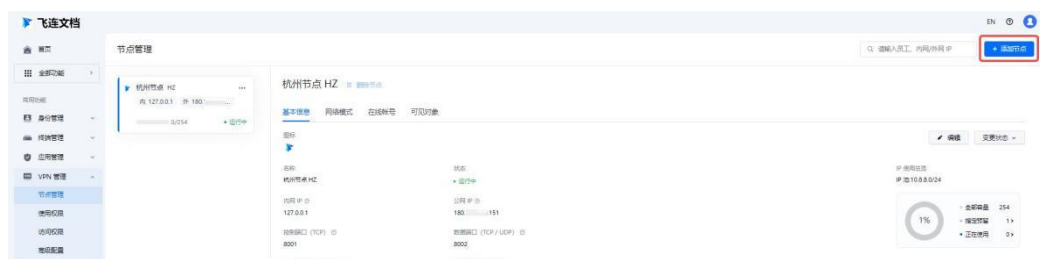
5.4.1 前提条件

已准备一台或多台 Linux 服务器（建议使用 CentOS 7、Debian 9 及以上版本的操作系统），这些服务器需要部署星链 VPN 组件作为 VPN 节点。

5.4.2 操作步骤

支持添加的 VPN 节点数量与您购买星链时选择的 VPN 节点数相关。例如您在购买星链时选配了 1 个 VPN 节点，则您只能在星链管理后台添加一个 VPN 节点。

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **VPN 管理** > **节点管理**。
3. 在**节点管理**页面的右上角，单击**添加节点**。



4. 在**配置 VPN 节点**界面，完成以下配置。
 - a) 配置基本信息，然后单击**下一步**。

配置 VPN 节点

1 配置基本信息

2 部署安装

3 连通性测试

1 重新上传

节点名称

中文: 例 中国

英文: 例 CN-Test

DNS 服务器 (主用)

请输入

DNS 服务器 (备用)

请输入

公网 IP

支持 IPv4

内网 IP

支持 IPv4; 本地节点请输入 127.0.0.1

控制端口 (TCP)

443

数据端口 (TCP / UDP)

80

IP 池

IPv4

是否启用网络地址转换(NAT)

启用使用虚拟 IP 池

不使用使用公司内网 IP 池

请输入 CIDR, 例如 10.0.0.0/24, 添加多个时请用英文逗号或空格隔开

IPv6

传输协议

自动选择 TCP 与 UDP

仅 TCP

仅 UDP

客户端上行限速 KB/s

0

客户端下行限速 KB/s

0

取消

下一步

配置项说明：

说明：涉及 IP 地址的配置项，您需要根据服务器实际环境与配置完成填写。

配置项	说明
节点名称	设置 VPN 节点的中文名称以及英文名称。
DNS 服务器 (主用)	通过 VPN 节点下发的 DNS 地址，一般输入为内网 DNS 地址。
DNS 服务器 (备用)	备用节点的 DNS 服务器 IP 地址。不能配置与主用 DNS 服务器相同的 IP 地址。
公网 IP	VPN 节点映射的公网 IP 地址。
内网 IP	VPN 节点的内网 IP 地址。本地节点请配置 127.0.0.1，且本地节点无需安装 VPN 组件。

控制端口 (TCP)	客户端探活及配置下发的端口，建议填写为 443，支持修改为其他端口号。
数据端口 (TCP / UDP)	VPN 数据传输的端口，建议填写为 80，支持修改为其他端口号。

是否启用网络地址转换 (NAT)	启用（使用虚拟 IP 池）：使用虚拟 IP 地址池，IP 地址池中的地址均属内网未规划的网段。 不启用（使用公司内网 IP 池）：使用内网 IP 地址池，IP 地址池中的地址均属内网已规划但未分配的网段。
IP 池	指定具体的 IP 池范围，填写 CIDR（例如，10.8.8.0/24）。不能和企业内网的现有地址段冲突。IP 池总量不能超过 1024，如果你需要配置大于 1024 个 IP，则需要添加多个 VPN 节点。
传输协议	星链客户端封包类型，支持选择自动选择 TCP 与 UDP、仅 TCP 或者仅 UDP。建议保持默认设置（即自动选择 TCP 与 UDP），因为某些网络会丢弃 UDP 包。
客户端上行限速	限制单个用户最大上行速度，单位 KB/s。取值为 0 代表不限速。
客户端下行限速	限制单个用户最大下行速度，单位 KB/s。取值为 0 代表不限速。

- b) 根据部署安装页面的提示信息，在指定服务器中部署安装 VPN 组件，然后单击下一步。
- c) 进行连通性测试，确保 VPN 节点所在服务器可以正常通信后，单击完成。

配置完成后，您可以在 VPN 节点管理页面查看节点信息。您需要等待节点部署完成。

5.4.3 相关操作

VPN 节点默认状态下全员不可用，您需要手动为员工配置 VPN 使用权限，限制 VPN 节点的使用范围以及使用权限的生效时长。具体操作，请参见

《5.5 设置 VPN 使用权限》。

VPN 节点的网络模式支持设置为全局模式和极速模式。关于网络模式的介绍和配置说明，请参见《5.6 设置 VPN 节点的网络模式》。

每个 VPN 节点内均可设置可见对象，仅在可见对象范围内的员工可以查看并使用相应的 VPN 节点。具体操作，请参见《5.9 配置 VPN 节点的可见对象》。

您可以为 VPN 节点设置访问权限，以限制员工连接 VPN 后允许访问的网络资源范围。具体操作，请参见《5.8 管理 VPN 访问权限》。

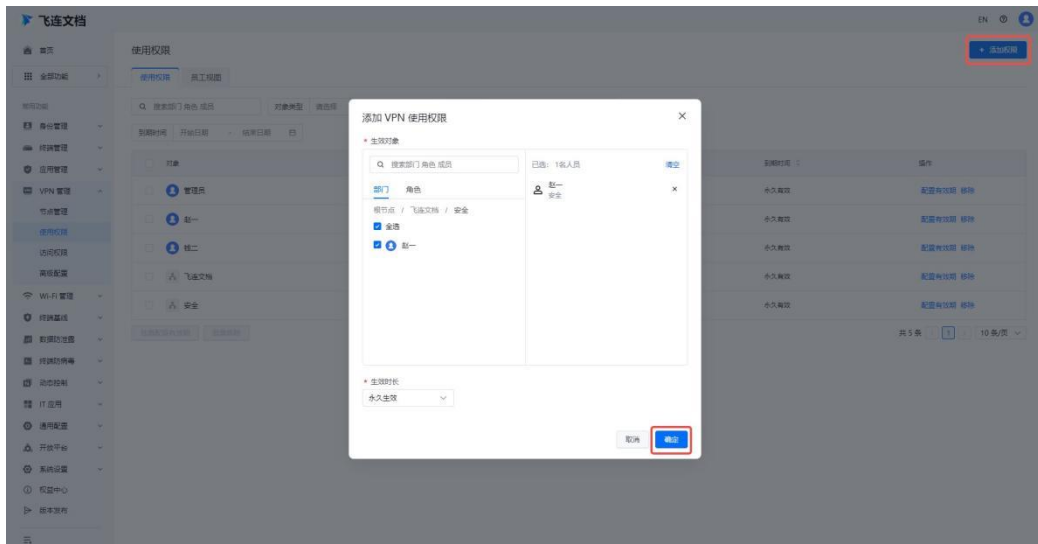
管理 VPN 节点的基本信息，请参见《5.10 查看或编辑 VPN 节点信息》。

5.5 设置 VPN 使用权限

在星链管理后台添加 VPN 节点后，节点默认全员不可用，您需要手动为员工配置 VPN 使用权限。配置权限时，支持为权限设置生效时长，到期后星链会自动回收权限，以满足临时使用 VPN 进行远程办公的场景。

操作步骤

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **VPN 管理** > **使用权限**。
3. 在**使用权限**页签右上角，单击**添加权限**。
4. 在**添加 VPN 使用权限**对话框，完成以下配置，并单击**确定**。



配置项说明：

配置项	说明
生效对象	以部门或者角色维度，设置生效的员工范围。
生效时长	可选永久生效、7 天、30 天、90 天、180 天或者自定义。 如 果选择自定义，还需要设置指定的天数。

成功添加后，您可以在使用权限列表中查看权限详情。在**操作**列，您可以：

单击**配置有效期**，调整权限生效的有效期。

单击**移除**，系统会收回指定对象的 VPN 使用权限。



5.6 设置 VPN 节点的网络模式

星链 VPN 节点的网络模式分为全局模式和极速模式两种。全局模式是指员工连接 VPN 后所有数据流量都走 VPN 隧道；极速模式是指员工连接 VPN 后仅访问指定的网络资源时走 VPN 隧道，其他流量均走本地网络。本文将介绍如何为 VPN 节点配置网络模式。

操作步骤

1. 登录星链管理后台。
2. 在左侧导航栏，选择 VPN 管理 > 节点管理。
3. 在节点管理页面，找到并单击指定节点卡片。
4. 在网络模式页签内，单击编辑。



5. 配置网络模式。

您可以根据实际需要选择**全局模式**、**极速模式**，支持多选。默认情况下，系统已选择了**全局模式**和**极速模式**。

全局模式：当企业员工通过 VPN 连接企业内网后，终端上所有网络访问流量均通过 VPN 隧道。该模式下全量数据加密，可以保障员工的帐号与数据安全，但会增加 VPN 节点的负载压力。

极速模式：当企业员工通过 VPN 连接企业内网后，仅指定网络资源的访问流量通过 VPN 隧道，其他访问流量使用本地网络进行访问。该模式下仅对指定网络资源做数据加密，但同时节省企业带宽，并减少 VPN 节点负载压力，提升了员工访问网络时的体验。

6. （可选）配置极速模式下单节点极速资源。

说明：如果 VPN 配置了极速模式，则需要设置极速模式网络资源。在极速模式下，仅访问这些被设置的网络资源时，流量会走 VPN 隧道。

极速模式网络资源分为全局极速资源和单节点极速资源，此处配置的是单节点资源。关于全局资源和单节点资源的区别以及具体配置操作，请参见

《6.7 管理极速模式网络资源》。

5.7 管理极速模式网络资源

当 VPN 节点配置了极速模式后，需要继续配置极速模式网络资源。该资源配置分为全局资源和单节点资源，本文将介绍不同资源的区别和配置方式。

5.7.1 极速模式网络资源介绍

极速模式是星链 VPN 的网络模式之一（关于 VPN 网络模式的配置操作，请参见《5.6 设置 VPN 节点的网络模式》），当 VPN 节点启用极速模式后，需要配置极速模式网络资源。后续当员工连接极速模式 VPN 节点后，仅访问

已配置的网络资源时流量会走 VPN 隧道。极速模式网络资源的配置分为全局资源和单节点资源，说明如下：

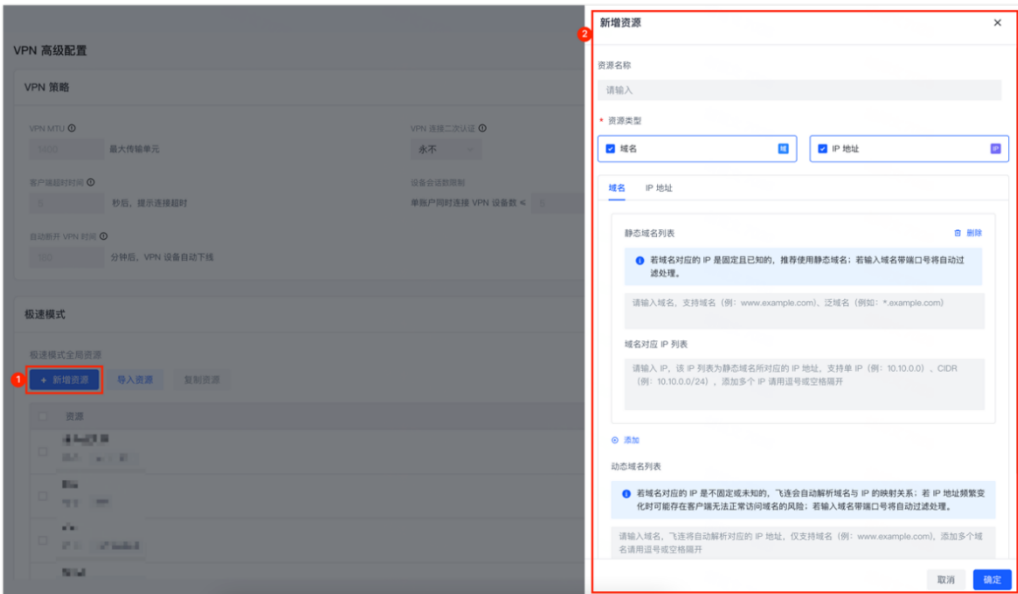
极速模式全局资源：生效于所有 VPN 节点的网络资源，在 VPN 管理的高级配置中添加，具体操作，请参见《5.7.2 配置极速模式全局资源》。

极速模式单节点资源：仅生效于指定 VPN 节点的网络资源，在指定 VPN 节点详情页内添加，具体操作，请参见《5.7.3 配置极速模式单节点资源》。

注意：极速模式单节点资源的优先级高于极速模式全局资源，即在 VPN 节点中配置了**极速模式单节点资源**后，会使高级配置中的**极速模式全局资源**对该节点失效。

5.7.2 配置极速模式全局资源

- 1. 登录星链管理后台。
- 2. 在左侧导航栏，选择 VPN 管理 > 高级配置。
- 3. 在 VPN 高级配置页面的极速模式区域，单击新增资源。
- 4. 在弹出的新增资源界面，设置资源名称以及资源类型，然后单击确定。

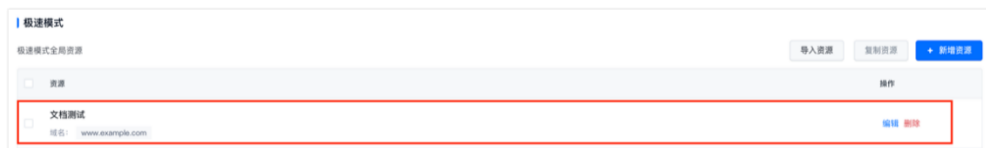


资源类型可选域名、IP 地址，支持多选。配置说明如下：

配置项	说明

域名	选择域名后，请根据实际需要填写静态域名列表、动态域名列表。
	静态域名列表：如果域名对应的 IP 地址是固定且已知的，建议您配置静态域名，配置时需要填写域名以及域名对应的 IP 地址列表。注意事项： 域名：支持填写域名（例如，<code>www.example.com</code>）、泛域名（例如，<code>*.example.com</code>），多个域名之间用逗号或者空格间隔。 IP 地址：支持填写单 IP（例如，<code>10.10.0.0</code>）、CIDR（例如，<code>10.10.0.0/24</code>），多个 IP 地址之间用逗号或者空格间隔。 如果填写域名时包含了端口号，端口号将被自动过滤。 在静态域名列表区域下方，单击添加，可添加多个静态域名。在右上角单击删除，可删除不再需要的静态域名。 动态域名列表：如果域名对应的 IP 是不固定的或者未知的，请配置为动态域名，星链会自动解析域名与 IP 的映射关系。注意事项： 仅支持填写域名（例如，<code>www.example.com</code>），多个域名之间用逗号或者空格间隔。 如果域名对应的 IP 地址频繁变化，则可能存在客户端无法正常访问域名的风险。 如果填写域名时包含了端口号，端口号将被自动过滤。
IP 地址	选择 IP 地址后，请根据实际需要填写 IP 列表。支持填写单 IP（例如， <code>10.10.0.0</code> ）、CIDR（例如， <code>10.10.0.0/24</code> ），多个 IP 地址之间用逗号或者空格间隔。

添加成功后，您可以在**极速模式全局资源**列表中查看资源配置，支持**编辑**或**删除**配置。



5.7.3 配置极速模式单节点资源

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **VPN 管理** > **节点管理**。
3. 在**节点管理**页面，找到指定节点并进入**网络模式**页签。
4. 在网络模式页签，单击**编辑**。
5. **网络模式**选中**极速模式**，并开启**极速模式下单节点资源**。



6. 在**极速模式下单节点资源**区域，单击**新增资源**。
7. 在右侧**新增资源**区域，设置**资源名称**以及**资源类型**，然后单击**确定**。

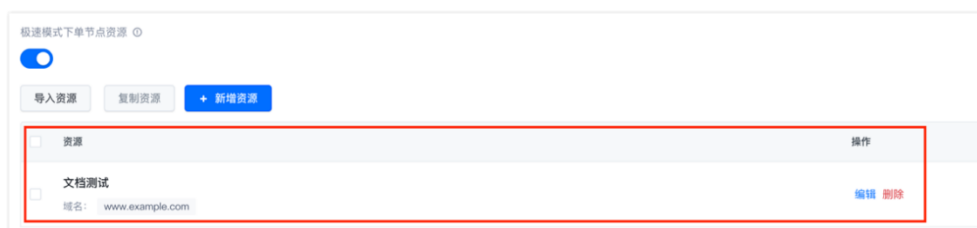


资源类型可选域名、IP 地址，支持多选。配置说明如下：

配置项	说明

域名	选择域名后，请根据实际需要填写静态域名列表、动态域名列表。 静态域名列表：如果域名对应的 IP 地址是固定且已知的，建议您配置静态域名，配置时需要填写域名以及域名对应的 IP 地址列表。注意事项： 域名：支持填写域名（例如，<code>www.example.com</code>）、泛域名（例如，<code>*.example.com</code>），多个域名之间用逗号或者空格间隔。 IP 地址：支持填写单 IP（例如，<code>10.10.0.0</code>）、CIDR（例如，<code>10.10.0.0/24</code>），多个 IP 地址之间用逗号或者空格间隔。 如果填写域名时包含了端口号，端口号将被自动过滤。 在静态域名列表区域下方，单击添加，可添加多个静态域名。在右上角单击删除，可删除不再需要的静态域名。 动态域名列表：如果域名对应的 IP 是不固定的或者未知的，请配置为动态域名，星链会自动解析域名与 IP 的映射关系。注意事项： 仅支持填写域名（例如，<code>www.example.com</code>），多个域名之间用逗号或者空格间隔。 如果域名对应的 IP 地址频繁变化，则可能存在客户端无法正常访问域名的风险。 如果填写域名时包含了端口号，端口号将被自动过滤。
IP 地址	选择 IP 地址后，请根据实际需要填写 IP 列表。支持填写单 IP（例如，<code>10.10.0.0</code>）、CIDR（例如，<code>10.10.0.0/24</code>），多个 IP 地址之间用逗号或者空格间隔。

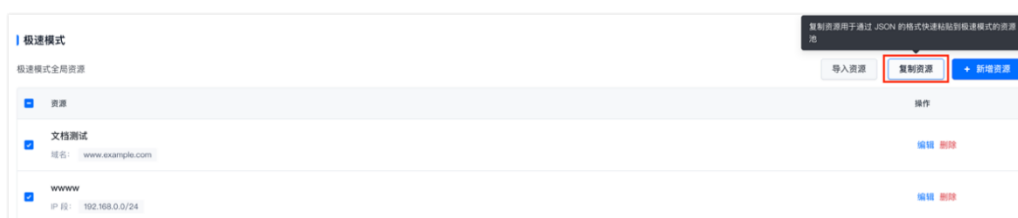
添加成功后，您可以在**极速模式**下单节点**资源**列表中查看资源配置，支持**编辑**或**删除**配置。



5.7.4 相关操作

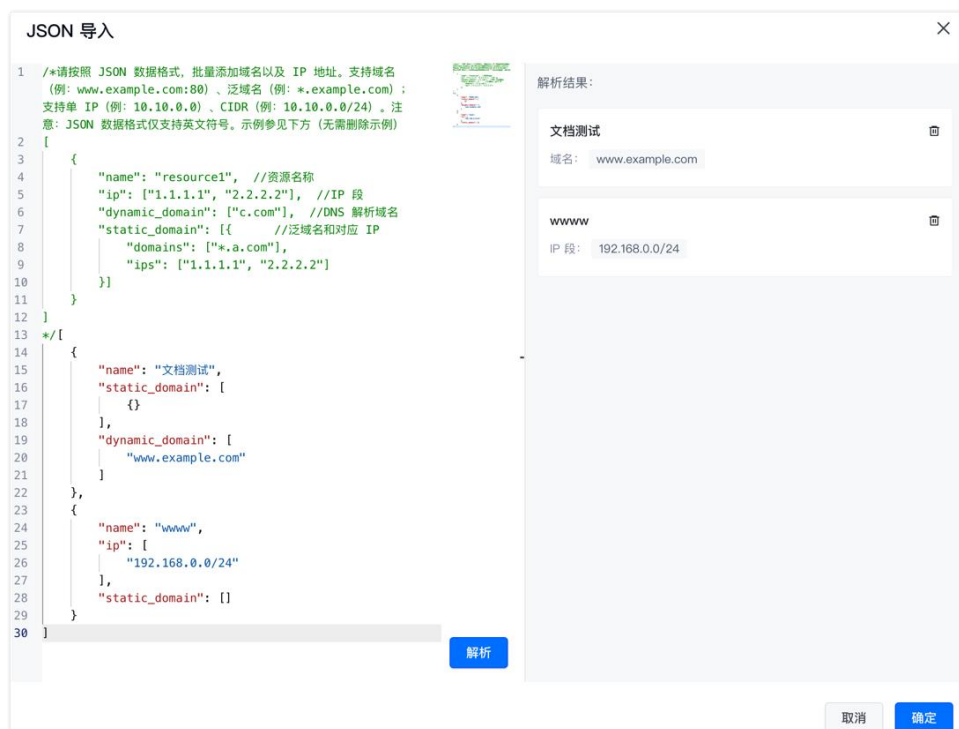
无论是全局资源配置页面还是单节点资源配置页面，均支持**复制资源**和**导入资源**，您可以选择复制存量的网络资源，快速新建其他资源。操作说明如下：

1. 在资源列表中，选中一个或多个资源前的复选框。
2. 单击**复制资源**。



3. 单击**导入资源**。
4. 在 **JSON 导入** 对话框，将复制的数据粘贴进来。

您可以参考页面提示信息，自定义 **JSON 数据**配置网络资源。



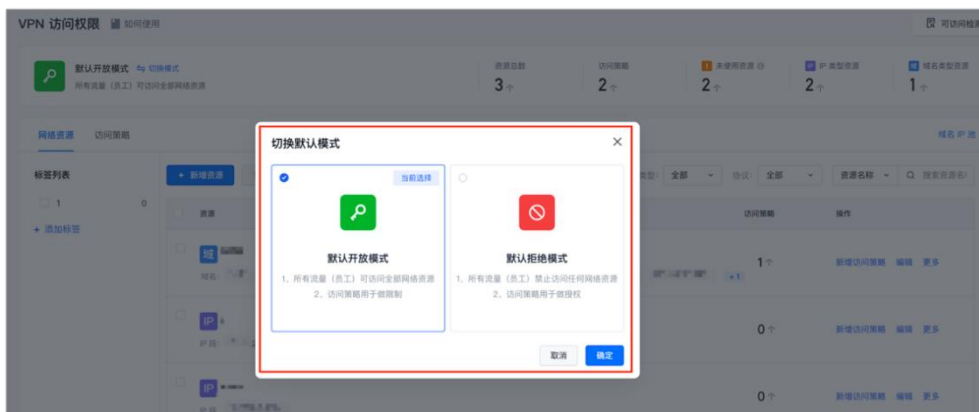
5. 单击**解析**，确认解析结果无问题后，单击**确定**。

5.8 管理 VPN 访问权限

您可以在星链管理后台为 VPN 节点配置访问权限，限制员工连接 VPN 后，允许或不允许访问的网络资源范围。

5.8.1 操作步骤

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **VPN 管理** > **访问权限**。
3. 在 **VPN 访问权限**页面上方，单击**切换模式**，然后在**切换默认模式**对话框中，选择模式并单击**确定**。



模式说明：

默认开放模式：该模式下所有员工可以通过 VPN 节点访问全部网络资源，后续手动设置的访问策略将用于限制指定网络资源的访问权限，适用于大部分网络资源均可对员工开放的场景。

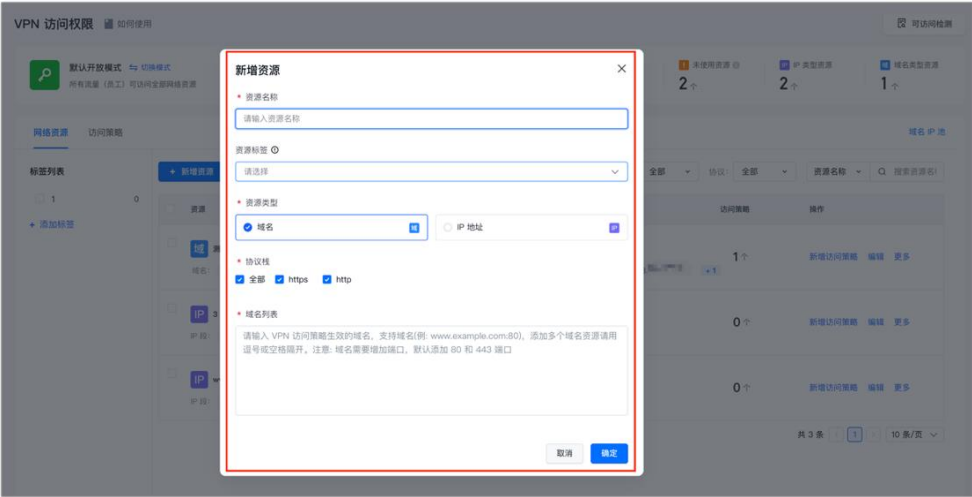
默认拒绝模式：该模式下所有员工禁止通过 VPN 节点访问任何网络资源，后续手动设置的访问策略将用于开放指定网络资源的访问权限，适用于仅少部分网络资源可对员工开放的场景。

您也可以在默认拒绝模式中，设置一个授权访问大范围网络资源权限的策略，并根据企业网络要求分别配置多个限制小范围网络资源权限的策略。

4. 添加网络资源。

网络资源本身不具有权限限制，需要后续结合访问策略进行配置，才可以生效相应的 VPN 访问权限。

- 在 VPN 访问权限页面，单击**网络资源**页签。
- 在**网络资源**页签中，单击**新增资源**。
- 在**新增资源**对话框，完成以下配置，并单击**确定**。



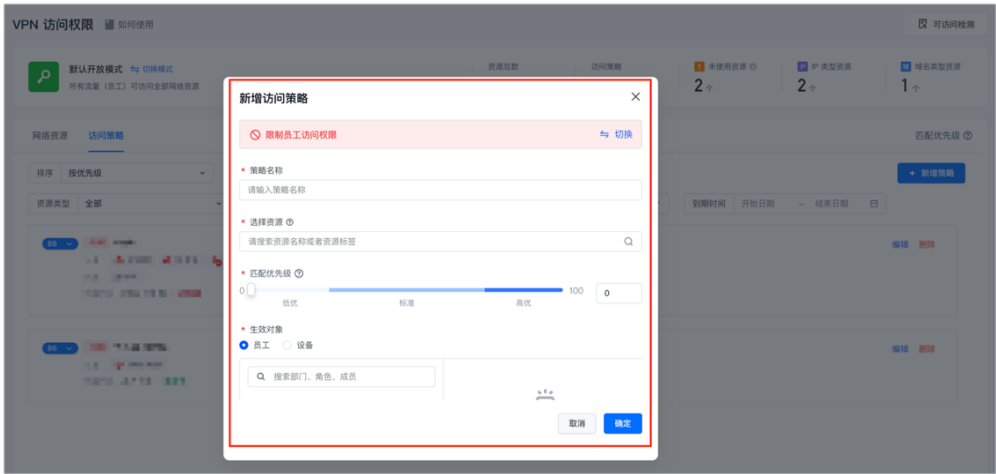
配置项说明：

配置项	说明
资源名称	自定义名称，用于标识该网络资源。
资源标签	网络资源支持通过标签进行分类，后续在配置访问策略时，您可以通过选择资源标签来批量设置网络资源。
资源类型	可选域名或者 IP 地址。 选择域名，需要配置以下信息： 协议栈：域名对应协议，支持选择全部、https 或者 http。 域名列表：设置该网络资源包含的域名，需要包含端口信息（默认添加 80 和 443 端口），格式示例： <code>www.example.com:80</code>。添加多个域名时需要使用逗号或者空格间隔。 选择 IP 地址，需要配置以下信息： 协议栈：IP 地址遵循的协议，支持选择全部、tcp、udp或者 icmp，支持多选。 IP 列表：设置网络资源包含的 IP 地址，支持单 IP（例如，<code>10.10.0.0</code>）、IP 地址范围（例如，<code>10.10.56.217-</code>

	10.10.56.218)、CIDR (例如, 10.10.0.0/24)。添加多个 IP 地址时需要使用逗号或者空格间隔。 端口列表: 设置网络资源所需的端口范围, 支持单端口 (例如, 80)、端口范围 (例如, 0-65535)。添加多个端口时需要使用逗号或者空格间隔。
--	---

5. 配置访问策略。

- a) 在 VPN 访问权限页面的访问策略页签, 单击**新增策略**。
- b) 在**新增访问策略**对话框, 完成以下配置, 并单击**确定**。



配置项说明:

配置项	说明
切换权限策略	在对话框顶部单击切换, 可选择限制员工访问权限或者授予员工访问权限。 限制员工访问权限: 一般在默认开放模式里选择该配置项, 在策略内添加网络资源后, 员工连接 VPN 时无法访问这些资源。 授予员工访问权限: 一般在默认拒绝模式里选择该配置项, 在策略内添加网络资源后, 员工连接 VPN 时可以访问这些资源。
策略名称	自定义名称, 用于标识该策略。

选择资源	选择指定的网络资源。支持选择一个或多个网络资源，或者选择资源标签批量添加网络资源。
匹配优先级	指当前策略的优先级。取值范围为 0 ~ 100，数值越大表示优先级越高。您可以同时生效多条策略，星链在对终端检测时，按优先级数值大小依次匹配策略，命中后停止匹配，如果一直未命中，则执行完所有策略后停止检测。如果存在两条优先级数值相同的策略，则优先执行策略修改时间最新的一条。
生效对象	支持选择员工或者设备。 如果选择员工，则需要以部门或者角色的维度指定该策略的员工生效范围。 如果选择设备，则需要以设备或者分组的维度指定该策略的设备生效范围。

6. （可选）使用星链提供的可访问检测功能，判断已配置网络资源以及访问策略是否成功生效。

a) 在 VPN 访问权限页面右上角，单击可访问检测。



b) 在可访问检测对话框，选择 IP 检测或域名检测，并完成以下配置。

The image shows the '可访问检测' (Access Detection) dialog box. It has two tabs: 'IP 检测' (IP Detection) and '域名检测' (Domain Detection). The 'IP 检测' tab is currently selected. The dialog contains the following fields:

- '* 对象' (Object): A search box with the placeholder '搜索部门、角色、成员' (Search department, role, member).
- '* 目的 IP' (Destination IP): A text box with the placeholder '请输入单个 IP' (Please enter a single IP).
- '目的端口' (Destination Port): A dropdown menu with the placeholder '请输入单个端口' (Please enter a single port).

At the bottom, there are two buttons: '执行检测' (Execute Detection) and '清空信息' (Clear Information).

IP 检测：指定**对象**（即员工）、**目的 IP** 以及**目的端口**，进行

检测。

域名检测：指定**对象**（即员工）、目的**域名**，进行检测。

c) 单击**执行检测**。

根据检测结果可以判断相应的访问策略是否正常生效。

5.8.2 相关操作

5.8.2.1 管理网络资源



在**网络资源**页签，支持以下操作：

标签列表

在**标签列表**单击**添加标签**，可以手动添加标签，后续在新增网络资源时可以选择标签进行归类。

资源列表

在资源列表中，找到指定资源并在操作列单击**新增访问策略**，可以基于该资源快速创建 VPN 访问策略。

每一条网络资源，均支持**编辑**原有配置信息，或者被**删除**。

注意：资源被删除后不可恢复，请谨慎操作。

选中一条或多条网络资源后，可以单击**复制资源**，资源被复制后保存为 JSON 格式的数据，您可以粘贴到极速模式网络资源内。

例如，配置允许访问的 VPN 访问策略后，可以将策略内的网络资源复制到极速模式网络资源。后续员工可以通过极速模式 VPN 访问相应的网络资源。

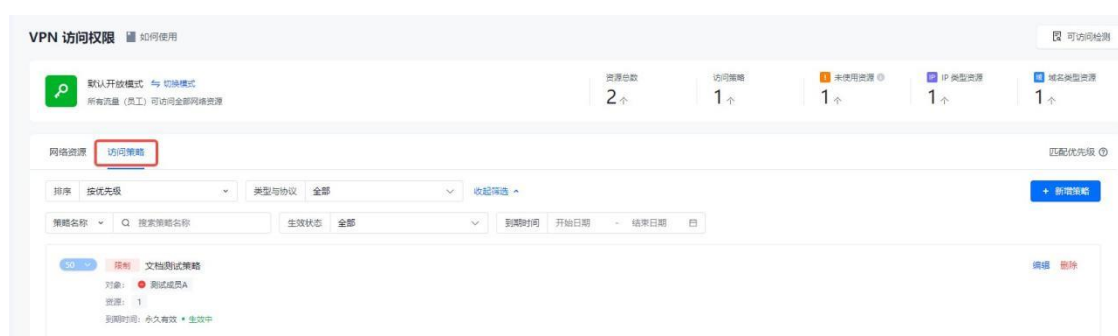
在资源列表中单击某一指定的网络资源，可以查看该网络资源的基本信

息，以及相关的访问策略。

域名 IP 池

在页签右上角单击**域名 IP 池**，可以选择配置受控域名直接解析的 IP 地址。默认情况下已配置了 0.0.0.0 IP 地址，表示系统默认对所有 IP 进行解包，建议您保持默认配置即可。如果您觉得将所有 IP 解包影响数据转发效率，则可以根据受控域名指定小范围的 IP 池。

5.8.2.2 管理访问策略



在**访问策略**页签，支持以下操作：

在指定访问策略右侧单击**编辑**，可手动调整策略内容，包括策略名称、网络资源、匹配优先级以及生效对象等信息。

在指定访问策略右侧单击**删除**，可删除策略，策略删除后将不再继续限制 VPN 的访问权限。

注意：策略被删除后无法恢复，请谨慎操作。

5.9 配置 VPN 节点的可见对象

您可以为指定的 VPN 节点配置可见对象，在可见范围内的员工才可以查看和使用 VPN 节点。

5.9.1 注意事项

如果您在星链管理后台的动态控制中配置了**调整可见 VPN 节点**相关的规则组，则规则组的生效优先级要高于在 VPN 节点内配置的**可见对象**生效范围。

5.9.2 操作步骤

- 1. 登录星链管理后台。
- 2. 在左侧导航栏，选择 VPN 管理 > 节点管理。
- 3. 在节点管理页面，单击指定卡片，并单击可见对象页签。



- 4. 在可见对象页签，单击添加对象。
- 5. 在添加节点可见对象对话框，完成以下配置，并单击确定。



配置项说明：

配置项	说明
生效对象	以部门、角色或者员工的维度设置生效员工范围，在该范围内的员工才可以查看和使用指定的 VPN 节点。
可见节点	默认当前节点可见，您也可以为可见对象配置其他 VPN 节点，支持同时配置多个节点。

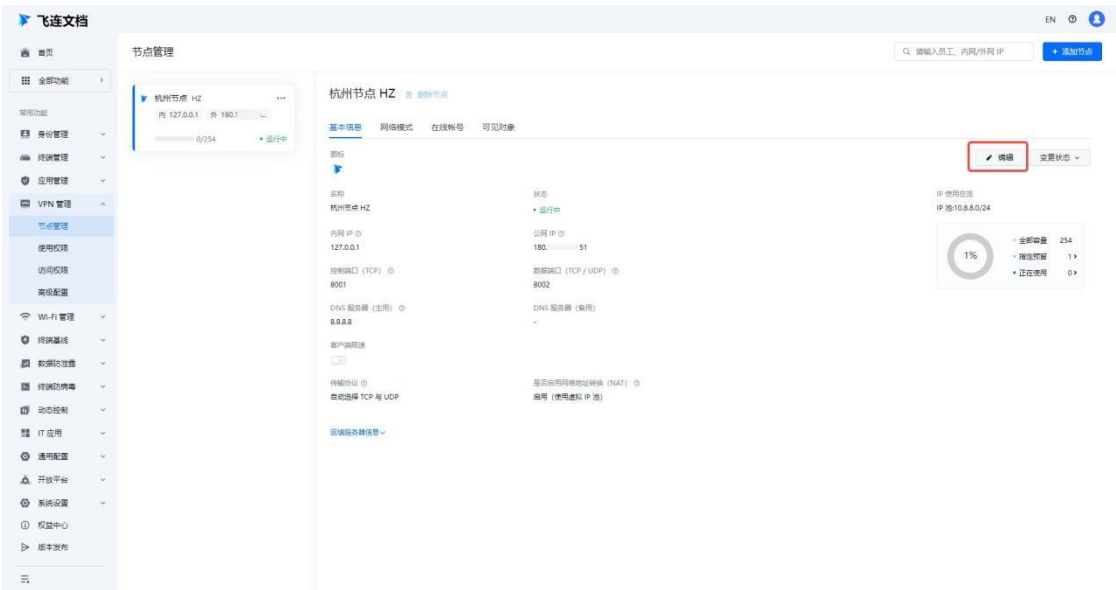
5.10 查看或编辑 VPN 节点信息

添加 VPN 节点后，您可以进入节点详情页查看基本信息。基本信息支持编

辑，后续您可根据网络实际情况调整 VPN 节点的基本信息。

操作步骤

- 1. 登录星链管理后台。
- 2. 在左侧导航栏，选择 VPN 管理 > 节点管理。
- 3. 在节点管理页面，找到并单击指定的 VPN 节点卡片。
- 4. 在节点内的基本信息页签，查看节点信息，或者单击编辑调整节点配置。



各配置项说明：

配置项	说明
图标	节点的图标，可编辑。
名称	节点的名称，名称由中文名称 + 英文名称构成，可编辑。
状态	节点当前的运行状态。您可以在页面右上角的变更状态下拉列表中，选择变更节点的运行状态。 运行中的节点，需要先变更为测试运行状态，然后才可以变更为下线状态。

	下线的节点，需要先变更为测试运行状态，然后才可以变更为运行中状态。 说明：下线 VPN 节点后，员工将无法通过该 VPN 节点连接企业内网。
内网 IP	创建 VPN 节点时配置的 VPN 内网 IP 地址，不可编辑。
公网 IP	VPN 节点的公网 IP 地址，可编辑。
控制端口 (TCP)	用于客户端探活以及配置下发的端口，仅当 VPN 节点为下线状态时可编辑。
数据端口 (TCP/UDP)	VPN 数据传输端口，仅当 VPN 节点为下线状态时可编辑。
DNS 服务器 (主用)	通过 VPN 节点下发的 DNS 地址，一般为内网 DNS 地址，可编辑。
DNS 服务器 (备用)	备用节点的 DNS 服务器 IP 地址，可编辑。不能配置与主用 DNS 服务器相同的 IP 地址。
客户端限速	设置客户端连接 VPN 节点后的网络速率限制，可编辑。 单用户上行限速 kbps：自定义限速的数值，单位为 kbps。如果填写 0 表示不限速。 单用户下行限速 kbps：自定义限速的数值，单位为 kbps。如果填写 0 表示不限速。
传输协议	星链客户端封包类型。可编辑，支持选择 自动选择 TCP 与 UDP、仅 TCP 或者仅 UDP。

是否启用网络地址转换（NAT）	不可编辑启用状态，但在节点下线状态时支持修改 IP 池配置。 启用（使用虚拟 IP 池）：使用虚拟 IP 地址池，IP 地址池中的地址均属内网未规划的网段。在 VPN 节点处于下线状态时，支持修改 IP 池，支持 CIDR 格
-----------------	---

	式的 IP 地址，多个网段之间使用半角逗号（,）间隔，示例值：10.8.8.8/24。 不启用（使用公司内网 IP 池）：使用内网 IP 地址池，IP 地址池中的地址均属内网已规划但未分配的网段。在 VPN 节点处于下线状态时，支持修改 IP 池，支持 CIDR 格式的 IP 地址，多个网段之间使用半角逗号（,）间隔，示例值：192.168.0.0/20。修改 IP 池时，您需要前往交换机或路由设备同步修改配置，否则将会导致已修改的 IP 池不可用。 说明：IP 池大小总量不能超过 4096。
回填服务器信息	组件 ID：由星链生成的组件唯一标识。支持复制组件 ID 到 VPN 服务器进行 VPN 服务的校验。 组件 Secret：组件 ID 对应的 Secret，与组件 ID 结合使用，用于在 VPN 服务器内校验 VPN 服务。 在 组件 Secret 右侧支持显示 Secret 或者复制 Secret。
IP 使用总览	展示当前 VPN 节点内 IP 池的资源使用情况。 单击指定预留，在指定预留 IP对话框内，可以为指定的设备或者员工配置预留 IP 地址。后续当指定的设备或者员工连接该 VPN 节点时，会分配预留的 IP 地址。 单击正在使用，可以查看当前 VPN 节点的在线帐号信息。

5. 在“在线帐号”页签，支持查看正在连接该 VPN 节点的员工信息，信息包含连接时间、姓名、流量、IP 地址、设备型号等，最后一列支持从后台手动与该设备断开连接。

杭州节点 HZ📍 当前节点

基本信息

网络模式

在线帐号

可见对象

在线帐号 2 / 254

🔍 搜索内网 IP、外网 IP、人名

连接时间	姓名	当前模式	上行流量	下行流量	公网 IP	内网 IP	设备型号	设备名称	
2023-05-11 22:07:15	👤 管理员	安全模式	1.77MB	2.00MB	124	194	LENOVO/20UAA05VCD	PF2X8GV4-CTF	🔗

5.11 查看员工的 VPN 权限信息

在星链管理后台的员工视图中，您可以统一查看企业所有员工的 VPN 使用权限，包括可见的 VPN 节点、授权的状态、到期时间等信息。

操作步骤

1. 登录星链管理后台。
2. 在左侧导航栏，选择 VPN 管理 > 使用权限。
3. 在使用权限页面的员工视图页签，查看员工的 VPN 权限信息。

在员工视图中，以设置过滤条件或者搜索员工的方式，找到指定员工并查看对应的权限信息，包括可见节点、权限来源、授权状态、授权时间、到期时间。

使用权限

使用权限

员工视图

搜索成员

可见节点 请选择

授权状态 全部

收起筛选

导出全部

授权来源 请选择

到期时间 开始日期 结束日期 日

员工	部门	可见节点	权限来源	授权状态	授权时间	到期时间
管理员	飞道文档	杭州节点 HZ	部门授权 +1	生效中	2023-04-20 21:51:10	永久生效
李同学	飞道文档	杭州节点 HZ	部门授权	生效中	2023-04-20 21:51:10	永久生效
赵一	安全	杭州节点 HZ	部门授权 +1	生效中	2023-04-20 21:51:10	永久生效
钱二	飞道文档		部门授权 +1	生效中	2023-04-20 21:51:10	永久生效
王五	飞道文档		部门授权	生效中	2023-04-20 21:51:10	永久生效

5.12 配置 VPN 策略

在 VPN 管理的高级配置功能页，您可以手动调整 VPN MTU（最大传输单元）、客户端超时时间、自动断开 VPN 时间、二次认证以及设备会话数限制的相关策略。

操作步骤

1. 登录星链管理后台。
2. 在左侧导航栏，选择 VPN 管理 > 高级配置。
3. 在 VPN 高级配置页面的 VPN 策略区域右上角，单击编辑。
4. 在 VPN 策略区域内，选择调整以下配置，并单击保存。

VPN 高级配置

VPN 策略

取消保存

VPN MTU ⓘ

1400

最大传输单元

连接 VPN 时，触发二次认证

未开启修改

客户端超时时间 ⓘ

5

秒后，提示连接超时

设备会话数限制

单账户同时连接 VPN 设备数 ≤ 5 台

自动断开 VPN 时间 ⓘ

180

分钟后，VPN 设备自动下线

配置项说明：

配置项	说明
VPN MTU	最大传输单元。
客户端超时时间	员工连接 VPN 节点时如果超过指定时间未响应，则在客户端提示连接超时。
自动断开 VPN 时间	星链根据客户端心跳判断 VPN 使用状态，在指定时间未检测到客户端心跳组自动断开 VPN。
连接 VPN 时，触发二次认证	可查看当前是否开启了二次认证，如果需要调整二次认证方式，请单击修改，然后跳转至多因素认证配置 VPN 二次认证。相关操作请参见《3.9 配置多因素认证》。
设备会话数限制	限制单个员工帐号可以同时连接 VPN 的设备数量上限。

6. WiFi与有线网络

星链 Wi-Fi 管理功能用于帮助企业构建 Wi-Fi 或有线网络。您可以配置员工 Wi-Fi 或有线网络使企业员工设备或者哑终端接入企业网络，也可以配置访客 Wi-Fi 为到访人员提供临时网络环境。当个人或企业设备接入企业 Wi-Fi 或有线网络后，您可以在星链管理后台集中管理已接入企业网络的设备。

6.1 功能简介

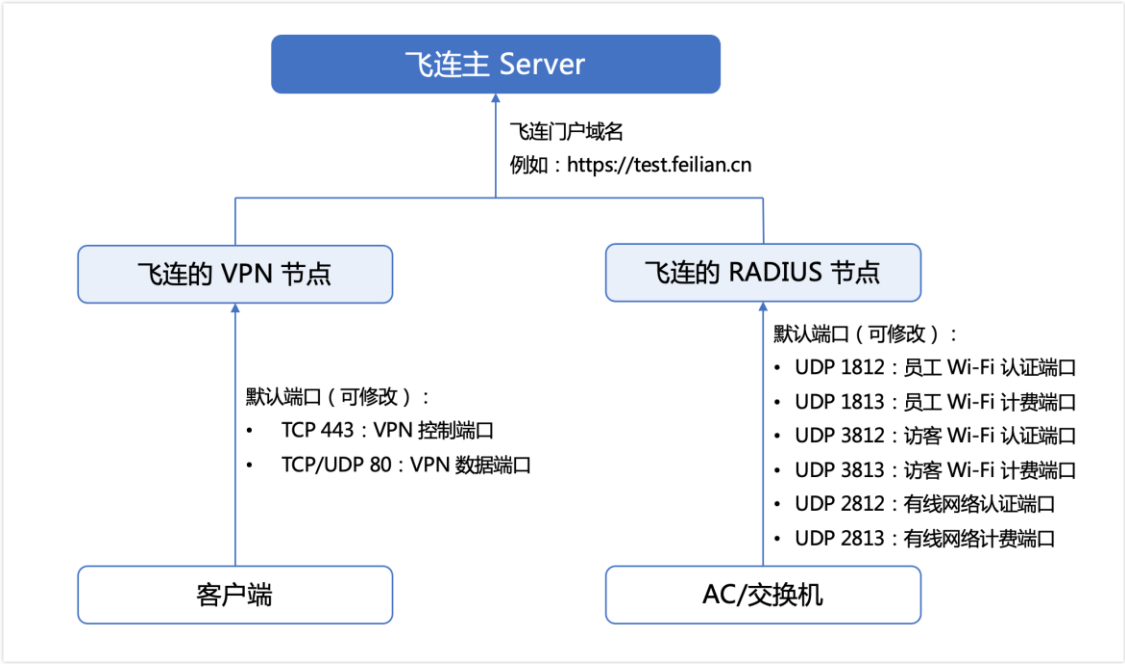
功能项	说明
构建企业网络环境	根据企业实际办公场景所需，在 Wi-Fi 管理功能中选择构建适用的网络环境，支持同时配置多种网络。

	场景一：员工 Wi-Fi 通过配置 RADIUS 节点、无线路由设备（开启员工 Wi-Fi 能力）、员工 Wi-Fi SSID，可以为企业员工构建 Wi-Fi 办公网络。后续员工在企业 Wi-Fi 信号覆盖范围内，可通过客户端或者 Wi-Fi 帐号认证连接企业办公网络。 场景二：访客 Wi-Fi 通过配置 RADIUS 节点、无线路由设备（开启访客 Wi-Fi 能力）、访客 Wi-Fi SSID 以及访客 Portal Server，可以为企业到访人员构建 Wi-Fi 网络。后续访客在企业访客 Wi-Fi 信号覆盖范围内，可通过 Portal 认证连接 Wi-Fi。 场景三：有线网络 通过配置 RADIUS 节点、交换机，可以为企业员工构建有线办公网络。后续员工设备插入企业网线后，可通过客户端或者 Wi-Fi 帐号认证连接企业办公网络。此外，支持将企业的哑终端设备接入有线网络进行统一管理。 注意：构建企业办公网络均需要配置 RADIUS 服务器，在您正式开始配置之前，请您务必了解由星链提供的 RADIUS 服务器部署建议与要求。详情请参见《6.2 服务器部署建议与要求》。
员工入网	星链为企业员工提供一人一 Wi-Fi 帐号，员工通过相应 Wi-Fi 帐号可实现一键连接入网，有效收敛了密码泄露风险，降低企业管理员运维负担。 您可以通过员工入网功能统一维护员工 Wi-Fi 帐号，设置员工入网权限。同时，支持多种帐号形式认证入网、免密认证等安全策略，满足您对网络准入的诉求。

访客入网	在访客入网功能中，记录了申请访客 Wi-Fi 的人员与设备信息，提升企业网络安全性。同时，支持手动调整访客 Wi-Fi 的通知策略与数据收集策略，使您可以自定义配置访客 Wi-Fi 属性。
哑终端入网	企业哑终端（例如打印机）通过有线网络接入企业内网后，您可以在星链管理后台统一管理哑终端的信息以及使用权限。

6.2 服务器部署建议与要求

在购买星链服务时，如果选购了 VPN 管理或者 Wi-Fi 管理功能，则在初始化星链时涉及 VPN 节点或者 RADIUS 节点的部署。部署架构如下图所示，其中，对于 RADIUS 节点，允许内网 AC 或交换机访问 RADIUS 节点的 UDP 1812/1813/3812/3813/2812/2813 端口（以实际设置的端口号为准）。



在星链内添加 RADIUS 节点时，需要您在本地准备服务器并在服务器内部署安装 RADIUS 组件，使该服务器作为 RADIUS 服务器。为保障企业网络稳定，星链针对服务器的配置与网络提供了以下建议与要求。

6.2.1 服务器资源配置参考

RADIUS 服务器的配置参考如下表：

（建议）操作系统版本	配置	QPS
CentOS 7、Debian 9 及以上	2 核 CPU、2 G 内存	300/s
	4 核 CPU、4 G 内存	600/s
	8 核 CPU、8 G 内存	1000/s

其中 QPS 为每秒认证用户数，QPS 为 300/s 即每秒认证 300 个用户，如果有 400 个用户，则有 100 个用户排队到下一秒进行认证，不会挤掉已经通过认证的用户。

6.2.2 网络要求

IP 地址要求

服务器	是否对公网开放	IP 地址示例	数量	备注
RADIUS	建议仅开	192.168.1.3	N，以订单中节	固定外网或内网

Server	放内网		点数量为准。	IP 地址。
--------	-----	--	--------	--------

网络端口开放要求

目的 IP	目的端口	协议	源 IP	是否可以修改	备注
RADIUS Server IP	1812	UDP	无线控制器	是	员工 Wi-Fi 认证端口，内网开放。若 RADIUS 服务器和无线控制器通过互联网通信，则对互联网开放。
	1813	UDP	无线控制器	是	员工 Wi-Fi 计费端口，内网开放。若 RADIUS 服务器和无线控制器通过互联网通信，则对互联网开放。
	3812	UDP	无线控制器	是	访客 Wi-Fi 认证端口，内网开放。若 RADIUS 服务器和无线控制器通过互联网通信，则对互联网开放。
	3813	UDP	无线控制器	是	访客 Wi-Fi 计费端口，内网开放。若 RADIUS 服务器和无线控制器通过互联网通信，则对互联网开放。
	2812	UDP	有线交换机	是	有线网络认证端口，内网开放。若 RADIUS 服务器和有线交换机通过互联网通信，则对互联网开放。
	2813	UDP	有线	是	有线网络计费端口，内网开

			交换机		放。若 RADIUS 服务器和有线交换机通过互联网通信，则对互联网开放。
--	--	--	-----	--	--------------------------------------

注意：RADIUS 节点需要访问星链门户域名的 TCP 443 端口。因此，如果您的 RADIUS 服务器配置了较为严格的防火墙规则（未全部放行出站规则），则需要在出站规则放行 TCP 443 端口，并指定 IP 地址为星链门户域名解析对应的 IP 地址。

6.3 添加 RADIUS 服务器

在构建企业 Wi-Fi 或有线网络之前，您需要先在星链管理后台配置 RADIUS 服务器，以统一管理入网请求与用户认证。

6.3.1 前提条件

已准备一台或多台 Linux 服务器。这些服务器需要部署星链 RADIUS 组件作为 RADIUS 服务器。

注意：请您务必了解 RADIUS 服务器部署建议与要求，详情请参见《7.2 服务器部署建议与要求》。

6.3.2 操作步骤

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理** > **使用配置**。
3. 在 **RADIUS 服务器** 页签，单击**点击配置**。



4. 配置 RADIUS 服务器。

a) 在配置基本信息界面，完成以下配置并单击下一步。

配置 RADIUS 服务器

1 配置基本信息

2 部署安装

3 连通性测试

* RADIUS 名称

请输入

* 内网 IP

支持 IPv4，本地节点请输入 127.0.0.1

* 员工 Wi-Fi 认证端口

1812

* 员工 Wi-Fi 计费端口

1813

* 有线网络认证端口

2812

* 有线网络计费端口

2813

* 访客 Wi-Fi 认证端口

3812

* 访客 Wi-Fi 计费端口

3813

配置项说明：

配置项	说明
RADIUS 名称	自定义名称，用于标识当前 RADIUS 服务器。
内网 IP	在内网中，将通过该 IP 地址识别 RADIUS 服务器。 本地节点请配置 127.0.0.1，且无需安装 RADIUS 组件。
员工 Wi-Fi 认证端口	RADIUS 服务器通过该端口对客户端员工 Wi-Fi 进行身份认证。默认占用 1812 端口，支持自定义修改端口。
员工 Wi-Fi 计费端口	RADIUS 服务器通过该端口实现员工客户端 Wi-Fi 的计费。默认占用 1813 端口，支持自定义修改端口。
有线网络认证端口	RADIUS 服务器通过该端口对客户端员工有线网络进行身份认证。默认占用 2812 端口，支持自定义修改端口。
有线网络计费端口	RADIUS 服务器通过该端口实现员工客户端有线网络的计费。默认占用 2813 端口，支持自定义修改端口。

访客 Wi-Fi 认证端口	RADIUS 服务器通过该端口对客户端的访客 Wi-Fi 进行身份认证。默认占用 3812 端口，支持自定义修改端口。
访客 Wi-Fi 计费端口	RADIUS 服务器通过该端口实现客户端访客 Wi-Fi 的计费。默认占用 3813 端口，支持自定义修改端口。

- b) 参考部署安装界面提供的命令，登录已准备好的 Linux 服务器安装 RADIUS 组件。安装完成后返回星链管理后台单击下一步。
- c) 在连通性测试界面，单击开始检测，检测 RADIUS 服务器与星链服务网络是否互通，确保连通性正常后单击完成。

6.3.3 后续步骤

配置 RADIUS 服务器后，选择配置无线路由或者交换机。

配置无线路由用于构建企业 Wi-Fi 网络。具体操作，请参见《6.4 添加无线路由》。

配置交换机用于构建企业有线网络。具体操作，请参见《6.5 添加交换机》。

完成星链后台配置后，请按照各品牌网络设备对接手册在 AC/交换机后台完善相关配置（各品牌网络设备对接手册请联系星链技术支持人员获取）。

6.4 添加无线路由

添加 RADIUS 服务器后，您可以添加无线路由设备为企业构建 Wi-Fi 网络，包括员工 Wi-Fi 和 访客 Wi-Fi。本文主要介绍如何添加无线路由设备。

6.4.1 前提条件

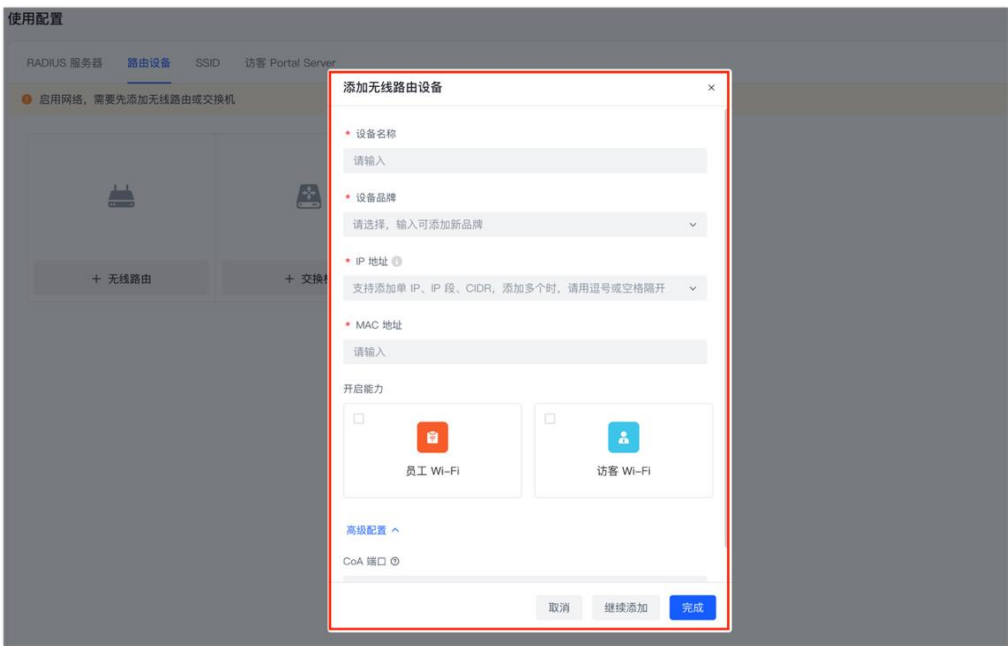
已添加 RADIUS 服务器。具体操作，请参见《6.3 添加 RADIUS 服务器》。

操作步骤

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理** > **使用配置**。
3. 在使用配置页面，单击**路由设备**页签。

4. 在路由设备页签，单击无线路由。
5. 在添加无线路由设备对话框，完成以下配置，并单击完成。

说明：如果您需要添加多个无线路由设备，则可以在完成当前配置后，单击继续添加。



配置项说明：

配置项	说明
设备名称	自定义名称，用于标识无线路由。
设备品牌	选择路由的设备品牌。如果下拉列表中没有相应的品牌，则可以直接在输入框手动添加品牌名称。
IP 地址	无线路由设备的源 IP 地址。支持以下 IP 地址格式，可避免配置多个设备模版，请根据实际设备情况填写。 IP 地址（例如，10.10.0.0）
	IP 地址段（例如，10.10.0.0 - 10.10.0.5） CIDR
MAC 地址	无线路由设备的 MAC 地址，请根据实际设备情况填写。

开启能力	选择员工 Wi-Fi、访客 Wi-Fi，可多选。 员工 Wi-Fi：提供企业员工连接企业 Wi-Fi 的能力。 选中该配置后，需要在高级配置中配置 CoA 端口。 访客 Wi-Fi：提供访客连接企业 Wi-Fi 的能力。选中该配置项后，需要配置访客认证信息接收地址，并在高级配置中配置访客认证相关信息。
访客认证信息接收地址	仅当开启能力选择访客 Wi-Fi 后需要配置的接收地址。该地址是无线路由设备对外提供的外部 Portal 认证的对接地址，外部 Portal 服务使用此地址提交访客用户名和密码。
高级配置	CoA 端口：当员工连接网络认证成功后，您可以通过 RADIUS 服务器来动态修改在线员工的入网权限或者进行重认证，此配置需要与无线路由设备的 CoA 端口保持一致，默认为 3799。 访客认证协议类型：仅当开启能力选择访客 Wi-Fi 后需要配置，支持选择 Portal 认证 或 PEAP 认证。 选择 Portal 认证：客户端将支持选择帐号密码或者员工扫码协助，来进行访客认证。该认证方式还需要配置以下信息： 访客认证用户名字段：无线路由设备使用的用户名字段，不同设备厂商的字段值有所差异。 访客认证密码字段：无线路由设备使用的密码字段，不同设备厂商的字段值有所差异。

	输入自定义 JSON：根据不同设备品牌的实际情况，当访客认证需要额外字段时，可通过自定义 JSON 输入自定义的数据。 说明：选择 Portal 认证后，如果相应的无线路由设备需要配置访客 Portal Server 以实现 Portal 认证，请参见《7.9 管理访客 Portal Server》。 选择 PEAP 认证：客户端仅支持通过帐号密码认证访客入网，且在星链管理后台的访客入网申请日志中，不支持对访客网络下线。
--	---

6.4.2 后续步骤

添加无线路由后，需要为企业 Wi-Fi 设置 SSID，SSID 为终端设备内显示的企业 Wi-Fi 名称。后续员工或访客连接指定 Wi-Fi SSID 即可访问企业内网。关于 SSID 的配置说明，请参见《6.8 设置 Wi-Fi SSID》。

完成星链后台配置后，请按照各品牌网络设备对接手册在 AC 后台完善相关配置（各品牌网络设备对接手册请联系星链技术支持人员获取）。

6.5 添加交换机

添加 RADIUS 服务器后，您可以添加交换机为企业构建有线网络。本文主要介绍如何添加交换机。

6.5.1 前提条件

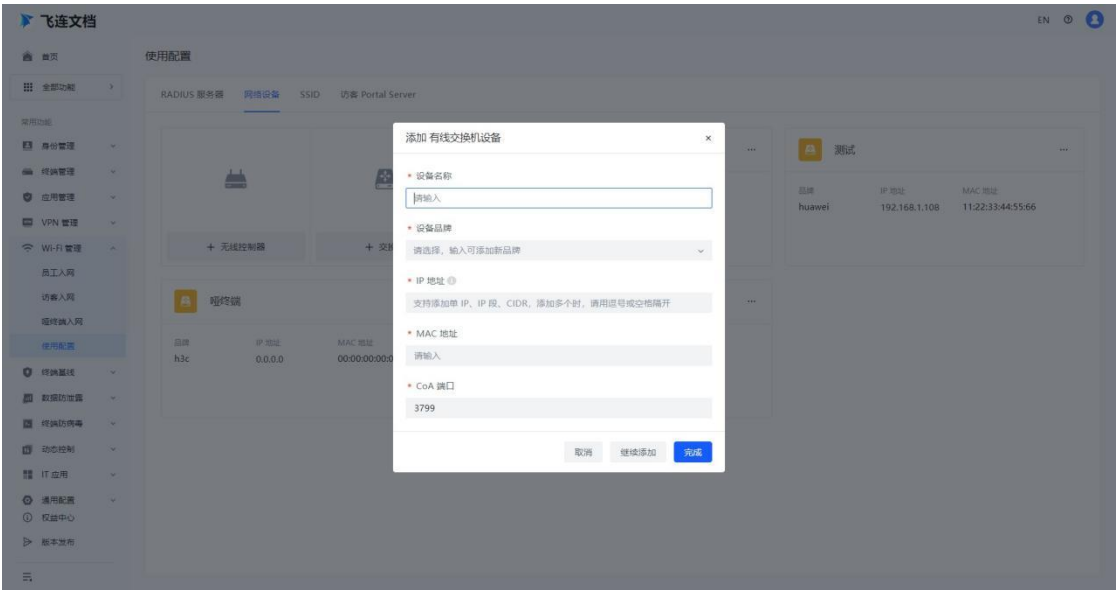
已添加 RADIUS 服务器。具体操作，请参见《6.3 添加 RADIUS 服务器》。

6.5.2 操作步骤

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理** > **使用配置**。
3. 在**使用配置**页面，单击**路由设备**页签。
4. 在**路由设备**页签，单击**交换机**。

5. 在添加有线交换机设备对话框，完成以下配置，并单击完成。

如果您需要添加多个交换机，则可以在完成当前配置后，单击继续添加。



配置项说明：

配置项	说明
设备名称	自定义名称，用于标识交换机。
设备品牌	选择路由的设备品牌。
IP 地址	交换机的源 IP 地址。支持以下 IP 地址格式，请根据实际交换机设备情况填写。 IP 地址（例如，10.10.0.0） IP 地址段（例如，10.10.0.0 – 10.10.0.5） CIDR
MAC 地址	交换机的 MAC 地址，请根据实际交换机设备情况填写。
CoA 端口	CoA 是指员工认证成功后，管理员可以通过 RADIUS 协议来修改在线员工的权限或对其进行重认证，此配置和有线交换机的 CoA 端口保持一致。默认为 3799。

6.5.3 后续步骤

完成星链后台配置后，请按照各品牌网络设备对接手册在交换机后台完善相关配置（各品牌网络设备对接手册请联系星链技术支持人员获取）。

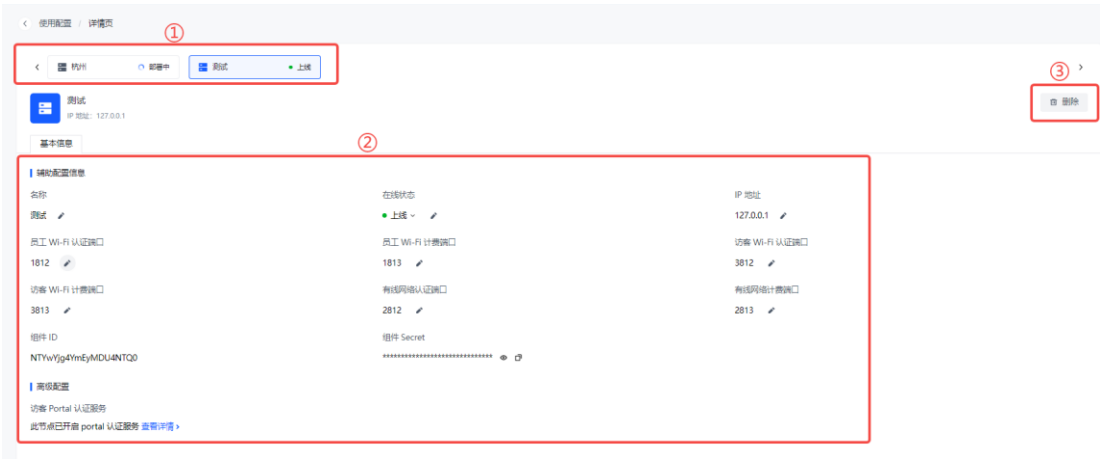
6.6 编辑或删除 RADIUS 服务器

在 RADIUS 服务器详情页，支持编辑服务器的名称、IP 地址以及状态等信息，同时支持下载服务器日志或删除服务器。

操作步骤

- 1. 登录星链管理后台。
- 2. 在左侧导航栏，选择 **Wi-Fi 管理 > 使用配置**。
- 3. 在 **RADIUS 服务器**页签，找到并单击指定服务器进入详情页。

在服务器详情页，支持以下管理操作：



如上图①区域，可手动切换至其他 RADIUS 服务器详情页。

如上图②区域，支持查看或编辑 RADIUS 服务器的以下信息。

配置项	说明
名称	RADIUS 服务器的名称，可编辑。
在线状态	RADIUS 服务器当前的运行状态，可编辑，支持 上线 或 下线 。
IP 地址	RADIUS 服务器的 IP 地址。如需编辑 IP 地址，需要先下线 RADIUS 服务器。
员工 Wi-Fi 认证端口	实现对客户端员工 Wi-Fi 身份认证。监听端口为 1812（默认端口）或者自定义端口，可编辑。
员工 Wi-Fi 计费端口	实现对客户端员工 Wi-Fi 计费。监听端口为 1813（默认端口）或者自定义端口，可编辑。

访客 Wi-Fi 认证端口	实现对客户端访客 Wi-Fi 身份认证。监听端口为 3812（默认端口）或者自定义端口，可编辑。
访客 Wi-Fi 计费端口	实现对客户端访客 Wi-Fi 计费。监听端口为 3813 或者自定义端口，可编辑。
有线网络认证端口	实现对客户端有线网络身份认证。监听端口为 2812（默认端口）或者自定义端口。可编辑。
有线网络计费端口	实现对客户端有线网络计费。监听端口为 2813（默认端口）或者自定义端口，可编辑。
组件 ID	每个 RADIUS 节点都会对应生成唯一的组件 ID。复制组件 ID 到 RADIUS 安装包可用于校验 RADIUS 服务。
组件 Secret	每个 RADIUS 节点都会对应生成唯一的组件 Secret。复制组件 Secret 到 RADIUS 安装包可用于校验 RADIUS 服务。
高级配置	星链 RADIUS 服务器内置了 Portal Server，主要用于访客 Wi-Fi 的 Portal 认证。当您添加无线路由为企业构建访客 Wi-Fi 后，可以在指定 RADIUS 服务器内的 访客 Portal 认证服务 区域单击 去配置 ，配置访客 Portal 认证服务。具体配置操作，请参见《7.9 管理访客 Portal Server》。

如上图③区域，支持删除服务器。

RADIUS 服务器被删除后，新用户无法连接企业 Wi-Fi，已连接企业 Wi-Fi 的用户将会自动断开 Wi-Fi 连接。删除后，请同步在无线路由设备或交换机内手动删除 RADIUS 配置才可生效。

注意：服务器一旦被删除不可恢复，请您谨慎操作。

6.7 编辑或删除路由设备

在路由设备页面，您可以对存量的无线路由或者交换机进行统一管理。

6.7.1 注意事项

所有删除操作均不可逆，一旦删除无法恢复，请您谨慎操作。

6.7.2 编辑或删除无线路由

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理** > **使用配置**。
3. 在使用**配置**页面的**路由设备**页签，找到指定无线路由。
4. 在无线路由卡片内，支持以下编辑操作。

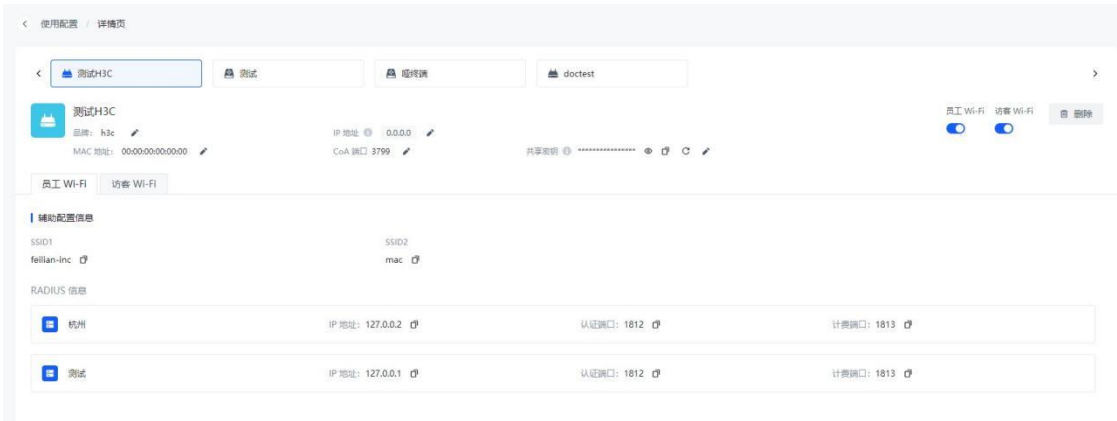


开启或关闭**员工 Wi-Fi**、**访客 Wi-Fi** 能力。

单击**编辑**：在**编辑无线路由设备**对话框，手动调整设备的基本信息、开启能力以及高级配置。

单击**删除**：删除当前无线路由，删除后该 **Wi-Fi** 网络将会自动断开。

5. 单击无线路由卡片，进入详情页。



在详情页支持以下操作：

在页面顶部，可手动切换至其他无线路由或交换机详情页。

查看或编辑无线路由设备的以下信息。

配置项	说明
品牌	无线路由设备的品牌名，可编辑。
IP 地址	无线路由设备的源 IP 地址，可编辑，编辑时支持设置以下 IP 地址格式。 IP 地址（例如，10.10.0.0） IP 地址段（例如，10.10.0.0 – 10.10.0.5） CIDR
MAC 地址	无线路由设备的 MAC 地址。
CoA 端口	当员工连接网络认证成功后，您可以通过 RADIUS 服务器来动态修改在线员工的入网权限或者进行重认证，此配置需要与无线路由设备的 CoA 端口保持一致，默认为 3799，可编辑。
共享密钥	共享密钥是指通过判断对方是否掌握相同密码，来确认对方身份是否合法。此处的共享密钥是指该设备创建 RADIUS 服务器时的共享密钥，由星链随机生成，支持以下操作： 设置密钥可见性 复制密钥 重置密钥
	编辑密钥 注意：重置或编辑密钥后，网络设备需要更新共享密钥，员工将无法连接网络，请谨慎操作。
员工 Wi-Fi 页签	查看员工 Wi-Fi SSID、对应 RADIUS 服务器的信息。

访客 Wi-Fi 页签	查看或编辑访客认证信息。 访客认证协议类型：支持选择 Portal 认证 或 PEAP 认证。 选择 Portal 认证：客户端将支持选择帐号密码或者员工扫码协助，来进行访客认证。该认证方 式还需要配置以下信息： 访客认证接收地址：该地址是无线路由设备对外提供的外部 Portal 认证的对接地址， 外部 Portal 服务使用此地址提交访客用户名和密码。 访客认证用户名字段：无线路由设备使用的用户名字段，不同设备厂商的字段值有所差异。 访客认证密码字段：无线路由设备使用的密码字段，不同设备厂商的字段值有所差异。 输入自定义 JSON：根据不同设备品牌的实际情况，当访客认证需要额外字段时，可通过自定义 JSON 输入自定义的数据。 选择 PEAP 认证：客户端仅支持通过帐号密码认证访客入网，且在星链管理后台的访客入网申请日志中，不支持对访客网络下线。 查看访客 Wi-Fi SSID、对应 RADIUS 服务器的信息。
---------------------------	---

在页面右上角，单击删除可删除当前无线路由。

注意：删除后该 Wi-Fi 网络将会自动断开，请谨慎操作。

6.7.3 编辑或删除交换机

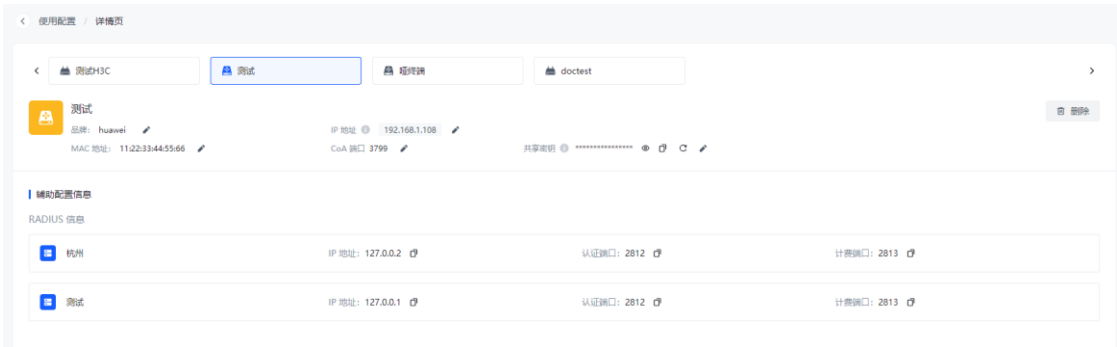
- 1. 登录星链管理后台。
- 2. 在左侧导航栏，选择 Wi-Fi 管理 > 使用配置。
- 3. 在使用配置页面的路由设备页签，找到指定交换机。
- 4. 在交换机卡片内，支持以下编辑操作。



单击**编辑**：在**编辑有线交换机设备**对话框，手动调整设备的名称、品牌、IP 地址以及 CoA 端口等信息。

单击**删除**：删除当前交换机，删除后该有线网络将会自动断开。

- 5. 单击交换机卡片，进入详情页。



在详情页支持以下操作：

在页面顶部，可手动切换至其他无线路由或交换机详情页。

查看或编辑交换机的品牌、IP 地址或共享密钥等配置信息。

配置项	说明
品牌	交换机的品牌名，可编辑。

IP 地址	交换机的源 IP 地址，可编辑，编辑时支持设置以下 IP 地址格式。 IP 地址（例如，10.10.0.0） IP 地址段（例如，10.10.0.0 - 10.10.0.5） CIDR
MAC 地址	交换机的 MAC 地址。
CoA 端口	当员工连接网络认证成功后，您可以通过 RADIUS 服务器来动态修改在线员工的入网权限或者进行重认证，此配置需要与无线路由设备的 CoA 端口保持一致，默认为 3799，可编辑。
共享密钥	共享密钥是指通过判断对方是否掌握相同密码，来确认对方身份是否合法。此处的共享密钥是指该设备创建 RADIUS 服务器时的共享密钥，由星链随机生成，支持以下操作： 设置密钥可见性 复制密钥 重置密钥 编辑密钥 注意：重置或编辑密钥后，网络设备需要更新共享密钥，员工将无法连接网络，请谨慎操作。

在页面右上角，单击删除可删除当前交换机。

注意：删除后该有线网络将会自动断开，请谨慎操作。

6.8 设置 Wi-Fi SSID

当您配置 RADIUS 服务器、无线路由后，需要设置 Wi-Fi 对应的 SSID。Wi-Fi SSID 是指在用户设备中显示的 Wi-Fi 名称，需与无线接入点 WLAN 名称保存一致。

6.8.1 注意事项

Wi-Fi SSID 的设置包含员工 Wi-Fi 和访客 Wi-Fi。

如果无线路由中开启了员工 Wi-Fi 能力，则需要设置员工 Wi-Fi SSID。

如果无线路由中开启了访客 Wi-Fi 能力，则需要设置访客 Wi-Fi SSID。

6.8.2 操作步骤

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理** > **使用配置**。
3. 在**使用配置**页面，单击 **SSID** 页签。
4. 在**员工 Wi-Fi** 或者**访客 Wi-Fi** 右侧，单击**添加**。



5. 在生成的文本框内输入 SSID，并单击对号进行保存（SSID 名称需与 AC 侧



配置保持一致）。

您可以在指定的 Wi-Fi SSID 卡片右上角单击 **...**，选择**编辑** SSID 或者**删除** SSID。



6.9 管理访客 Portal Server

星链访客 Wi-Fi 是基于 HTTP 协议的 Portal 认证流程，对于不支持 HTTP 对接方式的路由设备（例如锐捷 AC、TP-Link 等）需要部署外部的 Portal Server 以实现 Portal 认证。星链管理后台的 RADIUS 服务器内已集成 Portal Server，您只需要在管理后台手动配置 Portal Server 即可实现访客 Wi-Fi 的 Portal 认证。

6.9.1 前提条件

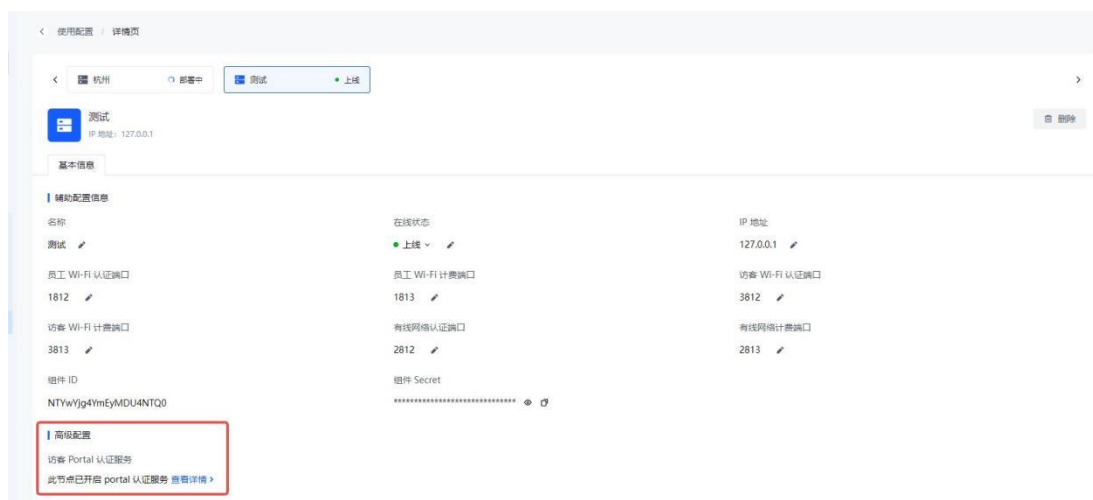
已添加 RADIUS 服务器。具体操作，请参见《7.3 添加 RADIUS 服务器》。

已添加无线路由设备并开启了访客 Wi-Fi 能力。具体操作，请参见《7.4 添加无线路由》。

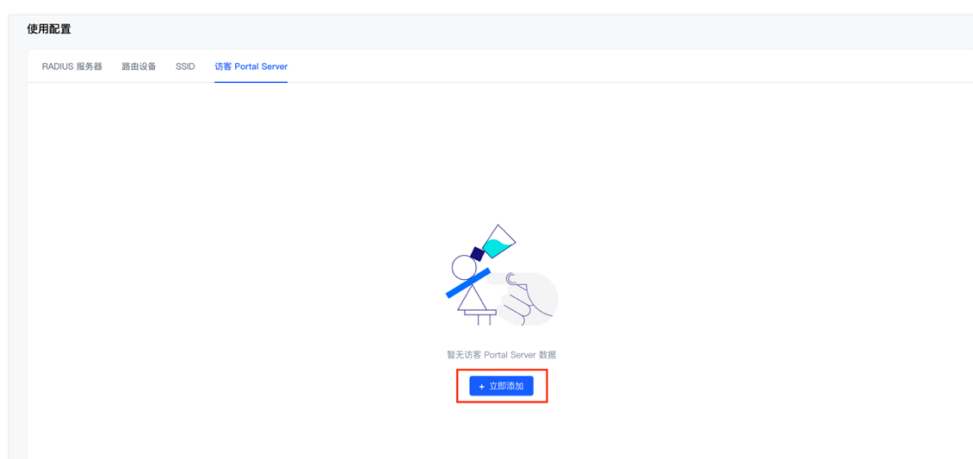
6.9.2 操作指引

访客 Portal Server 的配置入口有以下两个，您可以通过任一入口配置访客 Portal Server。

入口一：在 RADIUS 服务器详情页，**基本信息**页签的**高级配置**区域单击**去配置**。



入口二：在 **Wi-Fi 管理** > **使用配置** 页面，单击**访客 Portal Server** 页签，然后单击**立即添加**。



6.9.3 配置访客 Portal Server

进入**访客 Portal 认证服务**界面后，需要完成以下配置，并单击**确定**。

访客 Portal 认证服务

Portal 认证服务名称

选择 RADIUS 节点

请输入名称

选择 RADIUS 节点

无线控制器对接地址 ②

Portal 服务端口 ②

请输入 IP 地址:端口号

9100

Portal 协议端口 ②

认证协议类型

50100

v1

v2

PAP

CHAP

认证成功跳转地址

认证失败跳转地址

https://w /product/feilian

https:// /mult

用户 IP 字段名 ②

无线控制器 IP 字段名 ②

userip

nasip

配置项说明：

配置项	说明
Portal 认证服务器名称	自定义名称，用于标识该服务。
选择 RADIUS 节点	指定需要部署 Portal Server 的 RADIUS 服务器。 说明：如果您是通过 RADIUS 服务器内的高级配置打开的访客 Portal 认证界面，则默认已选择了 RADIUS 节点。
无线控制器对接地址	无线路由设备的对接地址，端口默认为 2000。地址格式示例：192.168.1.1:2000。
Portal 服务端口	Portal 认证服务 HTTP 监听端口，用于对接 Portal 认证页面，接受访客认证信息。若无特殊配置需求，保持默认端口 9100 即可。
Portal 协议端口	Portal 协议监听端口，用于接收控制器发送的 Portal 协议报文。若无特殊配置需求，保持默认端口 50100 即可。

Portal 协议版本	可选 v1、v2。目前多数无线路由设备品牌主要是用 v2 版本。
认证协议类型	可选 PAP、CHAP。目前多数无线路由设备品牌两种协议均支持，任选其一即可。
认证成功跳转地址	访客 Wi-Fi 认证成功后，Web 页面跳转的地址。例如配置为企业官网首页。
认证失败跳转地址	访客 Wi-Fi 认证失败后，Web 页面跳转的地址。例如配置为 Web 认证页面地址 <code>https://<Feilian Server 域名>:<端口>/multiple-pages/guest-wifi-login.html</code> 。
用户 IP 字段名	用户 IP 地址字段名。用于从 Portal 认证 URL 中获取用户 IP 地址信息。
无线控制器 IP 字段名	无线控制器 IP 地址字段名。用于从 Portal 认证 URL 中获取控制器地址，该配置项优先级高于无线控制器对接地址。

6.9.4 编辑或删除访客 Portal Server

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理** > **使用配置**。
3. 在**使用配置**页面，单击访客 Portal Server 页签。
4. 在**访客 Portal Server** 页签内，查看指定 Portal 服务器信息。



在页面右侧，支持**编辑或删除** Portal Server。

注意：

编辑 Portal Server 原有的配置后，可能影响访客认证服务的连通性，请您谨慎操作。

删除 Portal Server 后，对应的访客 Wi-Fi 无法进行访客认证，且一旦删除无法恢复，请您谨慎操作。

6.9.5 后续步骤

完成星链后台配置后，请按照各品牌网络设备对接手册在 AC 后台完善相关配置（各品牌网络设备对接手册请联系星链技术支持人员获取）。

6.10 管理员工入网

在员工入网功能中，您可以集中管理员工 Wi-Fi 帐号、设置网络使用权限或者调整入网相关的通用配置项。

6.10.1 前提条件

已在星链管理后台构建了 Wi-Fi 或有线网络。更多信息，请参见《6.3 添加 RADIUS 服务器》。

6.10.2 管理员工 Wi-Fi 帐号

1. 登录星链客户端。
2. 在左侧导航栏，选择 **Wi-Fi 管理** > **员工入网**。
3. 在**员工入网**页面的 **Wi-Fi 帐号**页签，支持以下管理操作。

员工入网							
Wi-Fi 帐号		权限配置		通用配置			
在线状态: 全部		入网帐号状态: 全部		员工帐号状态: 全部		最近在线: 开始日期 - 结束日期	
						员工姓名, IP 地址 Q	
员工名称	Wi-Fi 帐号	Wi-Fi 密码	最近在线时间		在线状态	入网帐号状态	操作
▼ 管理员	admin@feilian.local	*****	2022-12-02 17:52:10		离线	生效中	重置密码 停用帐号
设备名称	接入类型	IP 地址	在线状态	最近在线时间	Group ID	MAC 地址	设备 ID
PF2X8GV4-CTF	Wi-Fi	192.168.0.3	离线	2022-12-02 17:52:14	DEFAULT	58:6c:1c:9	6381892e1b3c2c5ad74a
iPhone	Wi-Fi	192.168.0.5	离线	2022-11-29 18:04:15	DEFAULT	a2:b3:1b:b	f84b54153d8c4fa8c13d
▶ 李同学	19100001111	*****	-	-	-	生效中	重置密码 停用帐号
▶ 赵一	15200000000	***** 显示	-	-	-	生效中	重置密码 停用帐号
▶ 刘二	15600000000	*****	-	-	-	生效中	重置密码 停用帐号

在页面顶部，支持设置过滤条件，或者关键词搜索指定的员工 Wi-Fi 帐号。

过滤或搜索项	说明
在线状态	设置设备接入网络的在线状态进行过滤，支持设置全部、在线、离线、未连接。
入网帐号状态	设置 Wi-Fi 帐号对应的入网状态进行过滤，支持设置全部、生效中、已停用。
员工帐号状态	设置星链员工帐号的状态进行过滤，支持设置全部、正常运行、暂停使用、已离职、未激活。
最近在线	设置时间段进行过滤，时间段细粒度到天级，格式为 yyyy-mm-dd。
员工姓名、IP 地址	支持输入员工姓名或者 IP 地址搜索。

在帐号列表，可查看员工名称、Wi-Fi 帐号、Wi-Fi 密码、最近在线时间、在线状态与入网帐号状态等的信息。

在操作列，支持重置密码或停用帐号。

重置密码：如果员工忘记了 Wi-Fi 密码，您可以重置密码并告知员工。重置密码后，员工会下线网络，需要输入新密码重新认证入网。

停用帐号：根据实际需求，可选择停用指定员工的 Wi-Fi 帐号。

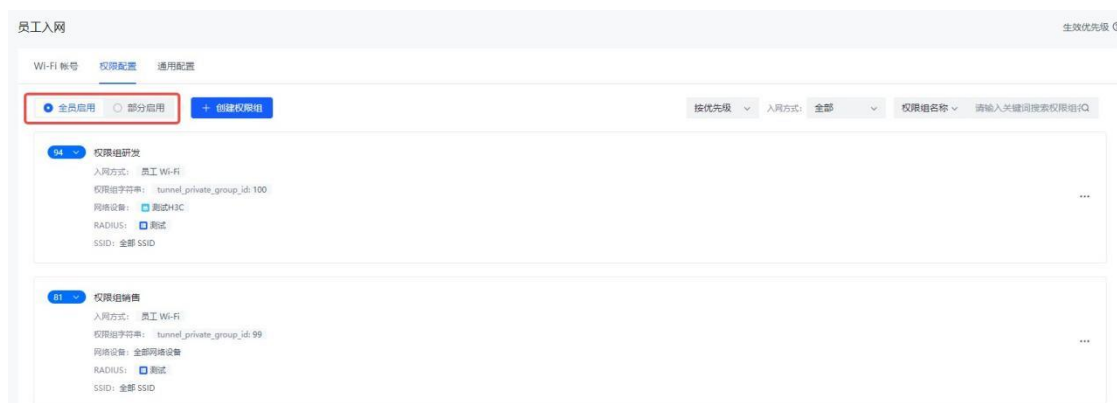
停用后，员工不可以使用该帐号连接企业内网。

在指定帐号行的左侧单击箭头图标，可查看该帐号的历史设备登录信息，信息包括设备名称、接入类型、IP 地址、在线状态、最近在线时间、网络权限（权限组 ID）以及 MAC 地址等信息。

6.10.3 配置权限组

您可以从部门、角色、员工的维度，配置企业网络的使用权限。

1. 登录星链客户端。
2. 在左侧导航栏，选择 **Wi-Fi 管理 > 员工入网**。
3. 在**员工入网**页面，单击**权限配置**页签。
4. 在**权限配置**页面，选择企业网络的使用范围。



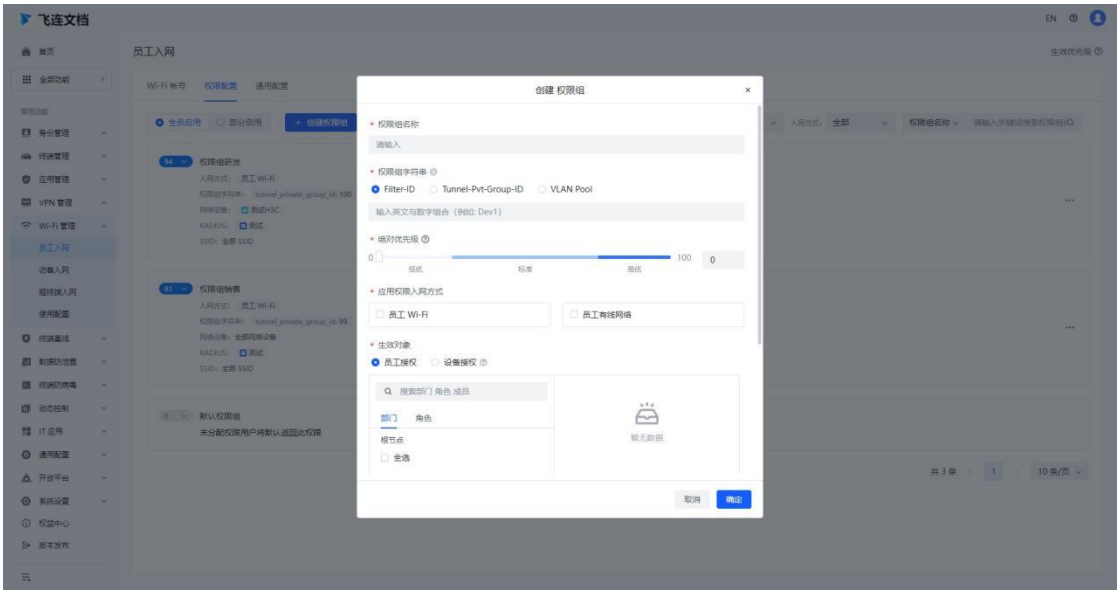
如果选择**全员启用**，系统会自动生成默认权限组，所有设备都可以入网。您也可以选择创建权限组，以员工或者设备的维度自定义入网权限生效范围。

如果选择**部分启用**，则您必须创建权限组，以员工或者设备的维度自定义入网权限生效范围。若未创建权限组则员工的网络帐号将处于停用状态。

5. （可选）创建权限组。

注意：创建权限组后，当新权限组优先级高于旧权限组且覆盖已有生效对象范围时，该对象范围内的员工重新连接网络时将生效于新权限组。

- a) 在**权限配置**页签，单击**创建权限组**。
- b) 在**创建权限组**对话框，完成以下配置，并单击**确定**。



配置项说明：

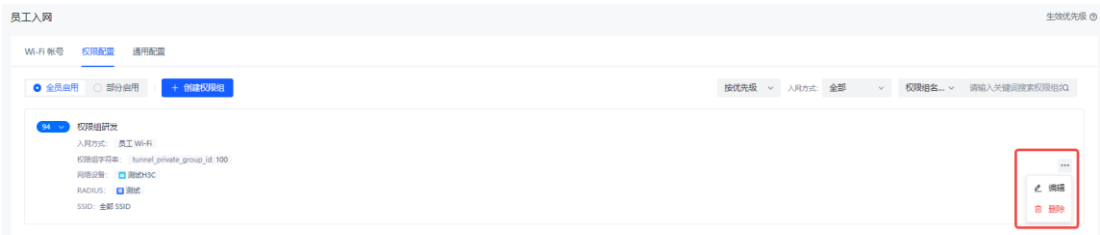
配置项	说明
权限组名称	自定义名称，用于标识当前权限组。
权限组字符串	在接入设备的控制台配置权限组时，查看权限组字符串。可选择 Fliter-ID、Tunnel-Pvt-Group-ID 或者 VLAN Pool。 Filter-ID：一般对应路由设备的预设角色或者用户组，填写英文与数字组合。例如 Dev1。如果填写纯数字，可用于对应 ACL ID。 Tunnel-Pvt-Group-ID：一般对应路由设备的 VLAN ID，填写纯数字。例如 97。 VLAN Pool：VLAN 池。星链根据每个 VLAN 所填的容量权重比均匀下发 VLAN。
绝对优先级	当前权限组的优先级。取值范围为 0 ~ 100，数值越大表示优先级越高。您可以同时生效多条权限组，星链在对终端检测时，按优先级数值大小依次匹配策略，命中后停止匹配，如果一直未命中，则执行完所有权限组后停止检测。如果存在两条优先级数值相同的策略，则优先执行策略修改时间最

	新的一条。
--	-------

应用权限入网方式	指定权限组生效的入网方式，可选 员工 Wi-Fi 或 员工有线网络 ，支持多选。
生效对象	以 员工授权 或者 设备授权 维度设置当前权限组的生效对象。 员工授权 ：以 部门 或 角色 维度划分员工范围。 设备授权 ：通过 设备名称 或者 设备分组 指定设备范围，该授权方式仅在星链客户端入网方式下生效。

创建权限组后，在**权限配置**页签可查看权限组信息，此外单击 **...**，可选择

注意：编辑权限组后，当新权限组优先级高于旧权限组且覆盖已有生效对象范围时，该对象范围内的员工重新连接网络时将生效于新权限组。



编辑或者**删除**权限组。

6.10.4 调整通用配置

- 1. 登录星链管理后台。
- 2. 在左侧导航栏，选择 **Wi-Fi 管理 > 员工入网**。
- 3. 在**员工入网**页面，单击**通用配置**页签。
- 4. 在页面右上角单击**编辑**，可选择调整以下配置。

配置项	说明
员工 Wi-Fi 的帐号形式	选择 员工手机号 或者 员工邮箱 作为员工 Wi-Fi 的帐号。
隐藏员工 Wi-Fi 与有线网络密码	开启该功能后，员工无法通过星链客户端获取 Wi-Fi 帐号的密码，仅可以查看帐号，支持通过客户端

一键连接入网。

此外支持设置**管理员**。管理员设置效果说明：

	设置管理员后信息会被展示在星链客户端，员工可联系管理员索要密码。 不设置管理员，星链客户端内不会展示管理员信息。
Windows 有线网络识别方式	配置 Windows 操作系统内有线网络连接后的生效账户。 如果选择所有系统账户生效，则网络权限根据联网设备识别，切换系统帐号不影响网络连接状态。 如果选择当前系统账户生效，则网络权限根据系统帐号识别，切换系统帐号需重新连接网络。
连接员工网络后，忘记访客网络 SSID	开启该功能后，需要添加指定的访客 Wi-Fi SSID。 当员工一键连接企业员工网络后，会自动忘记访客 Wi-Fi SSID，忘记后不会再主动连接该 Wi-Fi。

5. 调整后，单击**保存**。

6.11 管理访客入网

为企业配置访客 Wi-Fi 后，您可以在星链管理后台管理访客 Wi-Fi 申请记录以及配置访客 Wi-Fi 的基本信息。

6.11.1 前提条件

已在星链管理后台构建了访客 Wi-Fi 网络。具体操作，请参见《7.4 添加无线路由》。

6.11.2 填写访客 Wi-Fi 通用配置

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理 > 访客入网**。
3. 在**访客入网**页面，单击**通用配置**页签。
4. 在页面右上角单击**编辑**，完成以下配置。

访客入网

申请记录

通用配置

通用配置

取消

保存

访客 Wi-Fi 名称

demo-guest

员工申请/认证访客权限

全体成员

部分成员

访客认证协议类型（生效至全部路由器）

Portal 认证

PEAP 认证

Portal 认证支持短信帐号绑定成员员工扫码协助

访客认证方式

帐号密码

访客输入帐号密码的方式连接 Wi-Fi。可发送短信

扫码

员工申请后，可以通过飞信扫码协助访客快速连接

短信自助认证

访客到门店，输入手机号自助认证访客 Wi-Fi

访客帐号密码通知方式

短信通知

申请人员自行通知

必须设备信息

访客手机号

来访时间

来访原因

有效期时长（自申请成功时计算）

1天

2天

3天

7天

自定义

配置项	说明
访客 Wi-Fi 名称	自定义名称，用于标识当前访客 Wi-Fi。
员工申请/认证访客权限	设置可以申请或认证访客权限的员工范围，可选 全体成员 或者 部分成员 。如果选择 部分成员 ，则需要以 部门、人员或者角色 维度添加生效范围。
访客认证协议类型（生效至全部路由器）	可选 Portal 认证 或者 PEAP 认证，其中 Portal 认证 支持员工 扫码协助的认证方式。
访客认证方式	选择 Portal 认证 后，访客认证方式支持帐号密码或者扫码。 选择 PEAP 认证 后，访客认证方式仅支持帐号密码。认证方式说明： 帐号密码： 访客输入帐号密码的方式连接 Wi-Fi。设置该方式后，还需要指定帐号密码的通知方式，可选： 短信通知： 发送短信告知访客帐号与密码。

	申请人员自行通知：员工申请访客 Wi-Fi 权限后，自行通知访客帐号与密码。 扫码：员工申请访客 Wi-Fi 权限后，可通过星链扫码协助访客连接 Wi-Fi。 短信自助认证：用户连接访客 Wi-Fi 对应的 SSID 后，可在弹窗页面内自行输入手机号，获取验证码后进行认证。 
收录访客信息	开启该功能后，可选访客手机号、来访时间、来访原因，支持多选。选择后访客连接 Wi-Fi 时星链会收录访客信息，并展示在访客入网的申请记录页面。
有效时长（自来访日 0 时起算）	设置访客连接访客 Wi-Fi 的有效时长。可设置 1 天、2 天、3 天、7 天或者自定义有效时长，同时请您注意访客入网安全。

5. 完成后，单击**保存**。

6.11.3 查看访客 Wi-Fi 申请记录

访客 Wi-Fi 一般由员工发起申请后使用，在星链管理后台的访客入网申请记录页面，您可以查看所有访客 Wi-Fi 的申请记录。

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理 > 访客入网**。

3. 在**访客入网**页面，单击**申请记录**页签。
4. 在申请记录页签，选择查看访客 Wi-Fi 的申请时间、申请人、申请方式、密码、访客手机号以及到访时间等记录。
5. （可选）在**操作**列，可手动下线指定设备连接访客 Wi-Fi。

注意：

手动下线功能需要访客 Wi-Fi 对应的星链无线路由中添加了 CoA 端口才可以实现。星链无线路由中的 CoA 端口默认为 3799，您需要确保在本地路由设备中同步配置了 CoA 端口为 3799。

CoA 端口的默认值由无线路由设备的品牌决定。例如，Huawei 设备 CoA 默认值 3799、Cisco 设备 CoA 默认值 1700。

6.12 管理哑终端入网

企业的哑终端设备可以通过企业有线网络接入办公网络环境，接入后您可以在星链管理后台查看哑终端的信息，并支持管理哑终端的使用权限。

6.12.1 前提条件

已在星链管理后台构建了有线网络。具体操作，请参见《6.5 添加交换机》。

6.12.2 添加哑终端

1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理** > **哑终端入网**。
3. 在**哑终端入网**页面的**设备列表**页签，支持单个添加哑终端或者批量导入哑终端。

设备名称	设备类型	MAC 地址	IP 地址	权限字符串	状态	最近在线时间	操作
测试手机	普通	a2:11:11:bb	-	-	● 离线	-	编辑 启用 删除
测试机器	F1	11:22:33:55:66:77	-	-	● 离线	-	编辑 启用 删除
1号楼1	打印机	00:00:11:11:22:22	-	-	● 离线	-	编辑 启用 删除
1号楼2	打印机	00:00:11:11:22:23	-	-	● 离线	-	编辑 停用 删除
1号楼3	打印机	00:00:11:11:22:24	-	-	● 离线	-	编辑 停用 删除
1号楼4	打印机	00:00:11:11:22:25	-	-	● 离线	-	编辑 停用 删除
门禁1	普通	00:00:11:11:22:26	-	-	● 离线	-	编辑 停用 删除
门禁2	普通	aacc:22:33:dd:ee	-	-	● 离线	-	编辑 停用 删除

方式一：单个添加哑终端

- 在设备列表页签，单击**添加设备**。
- 在**添加哑终端设备**对话框，完成以下配置并单击**完成**。

设备名称：根据哑终端实际情况自定义名称。

设备类型：设置哑终端的类型，用于分类管理哑终端。在下拉列表中，支持手动添加设备类型。

* 设备类型

请选择

212 编辑 删除

请输入 + 设备类型

MAC 地址：哑终端设备的 MAC 地址。

- (可选) 单击**继续添加**，可继续添加其他哑终端设备。

方式二：批量导入哑终端

- 在设备列表页签，单击**批量导入**。
- 在**批量导入设备**页面的**第一步**区域，下载**设备导入模板**。
下载至本地后，文件名称为 `import-dumb-template`。
- 在本地打开设备导入模板，批量配置哑终端的**设备名称、设备类型、MAC 地址**。
- 配置完成后，保存并关闭文件。
- 返回星链管理后台，在**批量导入设备**页面的**第二步**区域，上传本地已保存的 `import-dumb-template` 文件。

vi. 单击**确认导入**。

6.12.3 启停哑终端

在哑终端入网页面的设备列表页签内，您可以在指定哑终端的操作列，单击**停用**或**启用**管理哑终端的可用状态。停用哑终端后，该哑终端在企业网络内不再可用。

设备名称	设备类型	MAC 地址	IP 地址	权限字符串	状态	最近在线时间	操作
☐ 测试手机	普通	a2:1:1:bb	-	-	● 离线	-	编辑 启用 删除
☐ 测试机器	F1	11:22:33:55:66:77	-	-	● 离线	-	编辑 启用 删除
☐ 1号楼1	打印机	00:00:11:11:22:22	-	-	● 离线	-	编辑 启用 删除
☐ 1号楼2	打印机	00:00:11:11:22:23	-	-	● 离线	-	编辑 停用 删除
☐ 1号楼3	打印机	00:00:11:11:22:24	-	-	● 离线	-	编辑 停用 删除

6.12.4 编辑或删除哑终端

注意：

修改哑终端的 MAC 地址可能影响哑终端正常入网，请您谨慎操作。
删除哑终端后，哑终端将会断开企业有线网络的连接，且删除操作不可恢复，请您谨慎操作。

在哑终端入网页面的设备列表页签内，您可以在指定哑终端的操作列，**编辑**哑终端的信息，或者**删除**哑终端。

设备类型: 全部 状态: 全部 最近在线 开始日期 结束日期

MAC 地址 回车搜索MAC 地址

添加设备 批量导入 批量导出 批量删除

设备名称	设备类型	MAC 地址	IP 地址	权限字符串	状态	最近在线时间	操作
☐ 测试机器	F1	11:22:33:55:66:77	-	-	● 离线	-	编辑 启用 删除
☐ 1号楼1	打印机	00:00:11:11:22:22	-	-	● 离线	-	编辑 启用 删除
☐ 1号楼2	打印机	00:00:11:11:22:23	-	-	● 离线	-	编辑 停用 删除
☐ 1号楼3	打印机	00:00:11:11:22:24	-	-	● 离线	-	编辑 停用 删除
☐ 1号楼4	打印机	00:00:11:11:22:25	-	-	● 离线	-	编辑 停用 删除
☐ 门禁1	普通	00:00:11:11:22:26	-	-	● 离线	-	编辑 停用 删除
☐ 门禁2	普通	aacc:22:33:dd:ee	-	-	● 离线	-	编辑 停用 删除

共 7 条 1 10 条/页

6.12.5 设置哑终端使用权限

设置哑终端使用权限后，仅在权限生效范围内的哑终端设备可用。

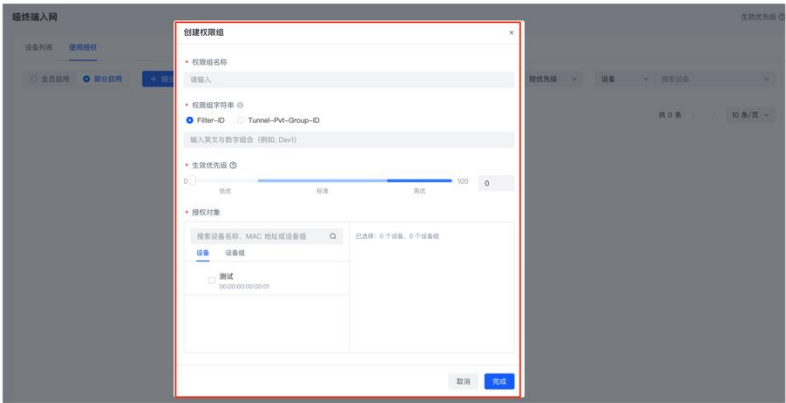
1. 登录星链管理后台。
2. 在左侧导航栏，选择 **Wi-Fi 管理 > 哑终端入网**。
3. 在哑终端入网页面，单击**使用授权**页签。
4. 在**使用授权**页签，设置哑终端权限为**全员启用**或者**部分启用**。

选择**全员启用**后，系统会自动生成默认权限组，所有设备都可以入网。

您也可以选择创建权限组，设置可以入网的设备范围。

选择**部分启用**后，您必须手动创建权限组，配置哑终端入网权限。若未创建权限组则哑终端无法入网。

5. （可选）单击**细分权限组**，在**创建权限组**对话框，完成以下配置并单击**完成**。



配置项说明：

配置项	说明
权限组名称	自定义名称，用于标识当前权限组。
权限组字符串	在接入设备的控制台配置权限组时，查看权限组字符串。 可选 Filter-ID 或者 Tunnel-Pvt-Group-ID 。 Filter-ID ：一般对应路由设备的预设角色或者用户组。填写英文与数字组合，例如 Dev1。如果填写纯数字，可用于对应 ACL ID。 Tunnel-Pvt-Group-ID ：一般对应路由设备的 VLAN ID。填写纯数字，例如 97。
生效优先级	当前权限组的优先级。取值范围为 0 ~ 100，数值越大表示优先级越高。您可以同时生效多条权限组，星链在对终端检测时，按优先级数值大小依次匹配权限组，命中后停止
	匹配，如果一直未命中，则执行完所有权限组后停止检测。如果存在两条优先级数值相同的权限组，则优先执行权限组修改时间最新的一条。

授权对象	以设备或者设备组维度设置当前权限组的生效对象。 设备：指定一个或多个设备。 设备组：指定一个或多个设备组。
------	--

7. 系统服务

7.1 消息通知

在消息通知功能中，您可以查看或管理星连各类的通知方式。

7.1.1 功能介绍

功能项	说明
星连配置	在星连配置中，星连默认提供了桌面客户端的消息通知模板文案。这些文案会在员工触发动态策略时进行推送。目前模板文案仅支持查看，不支持修改。
邮件配置	在邮件配置中，您可以添加企业邮件的网关以及邮件内容模板，后续当星连系统有验证码、初始帐号、重置密码、告警通知的消息推送时，即可通过企业邮箱下发企业邮件来完成。
第三方 IM	在第三方 IM 中，您可以配置第三方消息通知机器人进行消息通知。目前支持关联飞书、钉钉或企业微信内的机器人。

7.1.2 查看星连配置

在星连配置中，您可以查看星连桌面客户端推送的模板文案。如果有员工触发动态策略，则会根据该类文案进行消息通知。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **消息通知**。
3. 在**消息通知**页面，单击**星连配置**页签，即可查看**通知推送文案**。



7.1.3 管理短信网关

短信网关配置用于星连发送二次认证等消息通知，您需要根据企业实际需要，选择配置短信网关。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **消息通知**。
3. 在短信配置页签右上角，单击**编辑**。
4. 根据企业实际情况，选择**国内短信（中国大陆）**或者**国际/港澳台短信**。
5. 选择短信服务供应商。

国内短信（中国大陆）和**国际/港澳台短信**所支持选择的服务供应商有所不同，请您根据实际页面信息选择配置。如果您不需要使用短信网关，则请选择**暂不使用短信服务**。

6. 选择服务供应商后，需要依次完成以下配置。
 - a) 根据页面提示信息，配置服务供应商参数信息。
 - b) 在**通知场景**区域，查看通知场景对应的短信通知模版内容，并支持手动设置短信模板 Code。
 - c) 在**发送测试短信**区域，支持设置通知场景与手机号，发送短信测试配置是否存在问题。
7. 配置完成后，在页面右上角单击**保存**。

在短信网关配置页面右上角，您可以单击**暂停使用**，停止使用短信网关。暂停使用后，**暂停使用**按钮将变更为**恢复使用**，单击**恢复使用**即可继续使用短信网关。

7.1.4 管理邮件配置

您可以在邮件配置中，设置企业的邮件网关，包括 SMTP 服务器地址、邮箱地址以及邮件内容模板等配置信息。后续即可通过企业邮箱发送源自星连系统的消息通知邮件。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **消息通知**。
3. 在**邮件配置**页签右上角，单击**编辑**。
4. 完成以下配置，并单击**保存**。

配置项说明：

配置项	说明
SMTP 服务器地址 SMTP 端口	您需要获取企业邮箱的 SMTP HOST，并输入对应的信息。 举例如下： 阿里云企业邮箱发件服务器地址：SMTP 服务器地址为 <code>smtp.qiye.aliyun.com</code> ，SSL 加密端口为 465。 腾讯企业邮箱发件服务器地址：SMTP 服务器地址为 <code>smtp.exmail.qq.com</code> ，SSL 加密端口为 465。 Gmail 发件服务器地址：SMTP 服务器地址为 <code>smtp.gmail.com</code> ，SSL 加密端口为 465。
邮箱地址	您可以为星连的消息通知单独创建一个邮件组。格式例如： <code>feilian@<企业邮箱>.com</code> 。
发件邮箱地址	完整电子邮箱地址，可选配置。
邮箱密码	企业邮箱对应的密码。
自定义模板	可选启用或不启用。

	选择不启用，星连将根据系统默认提供的验证码模板、初始帐号模板、重置密码模板以及告警配置模板文案推送消息通知。 选择启用，您可以手动调整的验证码模板、初始帐号模板、重置密码模板以及告警配置模板的内容，后续系统将按照自定义文案推送消息通知。
验证码模板	当星连通过企业邮箱发送验证码消息时使用的模板内容，动态变量使用%v 占位。 星连提供了默认的模板内容，如果您启用了自定义模板，则支持手动调整模板内容，后续的消息通知将按自定义文案进行发送。
初始帐号模板	当星连通过企业邮箱发送新员工帐号通知时使用的模板内容，动态变量使用%v 占位。 星连提供了默认的模板内容，如果您启用了自定义模板，则支持手动调整模板内容，后续的消息通知将按自定义文案进行发送。
重置密码模板	当星连通过企业邮箱发送重置密码通知时使用的模板内容，动态变量使用%v 占位。 星连提供了默认的模板内容，如果您启用了自定义模板，则支持手动调整模板内容，后续的消息通知将按自定义文案进行发送。
告警配置模板	当星连通过企业邮箱发送告警事件通知时使用的模板内容，动态变量使用%v 占位。 星连提供了默认的模板内容，如果您启用了自定义模板，则支持手动调整模板内容，后续的消息通知将按自定义文案进行发送。
发送测试邮件	用于验证企业的邮件网关配置是否正常。可选择验证码、初始化、重置密码、告警信息，并指定一个可以正常接收邮件的邮箱地址，然后单击发送测试，查看指定邮箱是否
	可以接收到来自星连的消息通知，邮件接收过程存在一定延时，请耐心等待。

7.1.5 管理第三方 IM

在星连管理后台的动态策略、管理员告警策略等功能模块中，可以添加消息通知机器人用于接收星连的消息通知。目前星连支持关联飞书、钉钉以及企业微信来添加消息通知机器人，本文主要介绍如何在星连内管理第三方 IM 机器人。

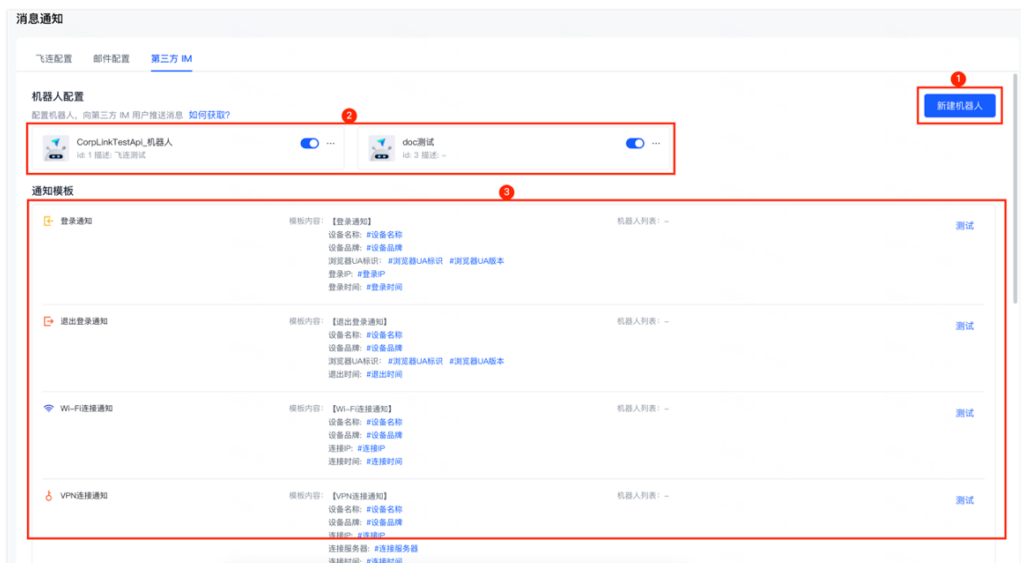
✧ 背景信息

如下图所示，当您在星连管理后台的**动态控制** > **动态决策**中配置规则组时，如果设置了**第三方通知员工**的通知方式，则需要指定第三方机器人以及通知内容。这些机器人与通知内容的模板，均来自于星连的第三方 IM 功能模块。



✧ 操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **消息通知**。
3. 在**消息通知**页面，单击**第三方 IM** 页签。
4. 在**第三方 IM** 页签内，支持以下操作。



如上图①区域，单击**新建机器人**，可选择添加飞书、钉钉或者企业微信的机器人。具体操作，请参见：

《13.1.6 添加飞书机器人》

《13.1.7 添加钉钉机器人》

《13.1.8 添加企业微信机器人》

如上图②区域，已添加的机器人支持编辑操作。



机器人卡片内的开关，用于管理机器人的生效状态。打开开关即可使用该机器人接收消息通知，关闭开关则不可使用该机器人接收消息通知。

单击 **...**，支持**编辑**或**删除**机器人。

如上图③区域，您可以查看各类通知的模板信息。当您配置好机器人后，可以单击**测试**，测试消息通知是否可以成功发送至机器人。

7.1.6 添加飞书机器人

在星连管理后台的动态策略、管理员告警策略等功能模块中，可以添加消息通知机器人用于接收星连的消息通知。本文将为您介绍如何在星连管理后台添加飞书机器人，使您可以通过飞书接收来自星连的消息通知。

✧ 操作指引

在星连内支持配置飞书应用或者群机器人接收星连消息通知。

通过飞书应用接收消息通知

该方式适用于星连内的部门、员工信息来自飞书数据源的场景，后续星连将通过飞书应用向指定员工推送消息通知。具体操作，请参见《13.1.6.2 通过飞书应用接收消息通知》。

通过群机器人接收消息通知

该方式无需关注企业员工信息的来源，只要您在飞书群聊中添加自定义机器人并获取机器人的 WebHook，即可在星连中添加相应的消息通知机器人，后续星连将通过群机器人推送消息通知。

✧ 通过飞书应用接收消息通知前提条件

已在星连内导入飞书组织架构。具体操作，请参见《2.8 同步第三方数据源》。

步骤一：在飞书内创建企业自建应用

1. 登录[飞书开放平台](https://open.feishu.cn/)（https://open.feishu.cn/）。
2. 在页面右上角单击**开发者后台**。
3. 在企业自建应用区域，单击**创建企业自建应用**。

创建飞书企业自建应用的具体配置说明，请参见[企业自建应用的开发流程](https://open.feishu.cn/document/home/introduction-to-custom-app-development/self-built-application-development-process)

（https://open.feishu.cn/document/home/introduction-to-custom-app-development/self-built-application-development-process）。

4. 创建企业自建应用后，进入应用详情页，在**凭证与基础信息**页面，查看并保存 App ID 和 App Secret。



步骤二：在星连管理后台配置消息通知机器人

1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **消息通知**。
3. 在**消息通知**页面，单击**第三方 IM** 页签。
4. 在页面右上角，单击**新建机器人**。
5. 在**新建机器人**对话框，完成以下配置，并单击**确**

定。配置项说明：

配置项	说明
第三方 IM	选择 飞书 。
通知方式	选择 应用 。
名称	自定义名称，用于标识当前的消息通知机器人。
描述	自定义描述，可选填写。
App ID	飞书应用对应的 App ID 信息。
App secret	飞书应用对应的 App Secret 信息。

6. 在**第三方 IM** 页签的**通知模板**区域，单击任一模板右侧的**测试**，设置飞书消息通知机器人以及测试对象，进行消息通知测试。

单击**确定**后，指定的测试对象可以在飞书中接收到消息通知。

✧ 通过群机器人接收消息通知

步骤一：在飞书群中添加自定义机器人

具体添加方式，请参见[自定义机器人指南](#)

(<https://open.feishu.cn/document/ukTMukTMukTM/ucTM5YjL3ETO24yNxkjN>)

。添加后需要保存群机器人的 webhook 地址。

步骤二：在星连管理后台配置消息通知机器人

1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **消息通知**。
3. 在**消息通知**页面，单击**第三方 IM** 页签。
4. 在页面右上角，单击**新建机器人**。
5. 在**新建机器人**对话框，完成以下配置，并单击**确定**。配置项说明：

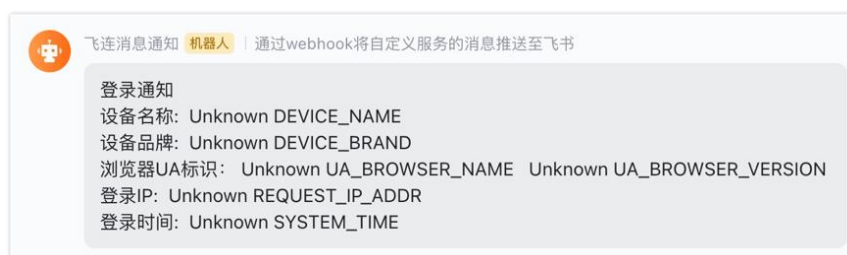
配置项	说明
第三方 IM	选择飞书。
通知方式	选择 WebHook。
名称	自定义名称，用于标识当前的消息通知机器人。
描述	自定义描述，可选填写。
WebHook	群机器人对应的 WebHook 地址。

6. 在**第三方 IM** 页签的**通知模板**区域，单击任一模板右侧的**测试**，设置飞书

消息通知机器人以及测试对象，进行消息通知测试。



单击**确定**后，您可以在飞书群聊中接收到消息通知。



7.1.7 添加钉钉机器人

在星连管理后台的动态策略、管理员告警策略等功能模块中，可以添加消息通知机器人用于接收星连的消息通知。本文将为您介绍如何在星连管理后台添加钉钉机器人，使您可以通过钉钉接收来自星连的消息通知。

✧ 操作指引

在星连内支持配置钉钉应用或者群机器人接收星连消息通知。

通过钉钉应用接收消息通知

该方式适用于星连内的部门、员工信息来自钉钉数据源的场景，后续星连将通过钉钉应用向指定员工推送消息通知。

通过群机器人接收消息通知

该方式无需关注企业员工信息的来源，只要您在钉钉群聊中添加群机器人并获取机器人的 WebHook，即可在星连中添加相应的消息通知机器人，后续星连将通过群机器人推送消息通知。

✧ 通过钉钉应用接收消息通知

前提条件

已在星连内导入钉钉组织架构。具体操作请参见 《2.8同步第三方数据源》。

步骤一：在钉钉内创建应用



测试机器人

* 发送机器人

钉钉机器人 (应用) 新增机器人

该机器人属于应用类型机器人，通知将发送至个人

* 测试对象

管理员

取消 确定

单击**确定**后，指定的测试对象可以在钉钉中接收到消息通知。

✧ 通过群机器人接收消息通知

步骤一：在钉钉群中添加自定义机器人

具体添加方式，请参见[自定义机器人接入](#)

(<https://open.dingtalk.com/document/orgapp/custom-robot-access>)，其中，您需要注意：

安全设置可选择**自定义关键词**，并配置可以命中星连通知模板内容的关键词，例如：通知。



* 安全设置

说明文档

☒ 自定义关键词

通知

+ 添加 (最多添加 10 个)

☐ 加签

☐ IP地址 (段)

请保存自定义机器人的 **Webhook**。



步骤二：在星连管理后台配置消息通知机器人

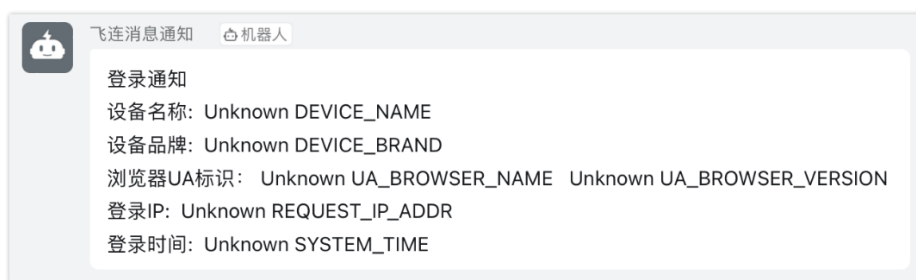
1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **消息通知**。
3. 在**消息通知**页面，单击**第三方 IM** 页签。
4. 在页面右上角，单击**新建机器人**。
5. 在**新建机器人**对话框，完成以下配置，并单击**确定**。配置项说明：

配置项	说明
第三方 IM	选择钉钉。
通知方式	选择 WebHook。
名称	自定义名称，用于标识当前的消息通知机器人。
描述	自定义描述，可选填写。
WebHook	群机器人对应的 WebHook 地址。

6. 在**第三方 IM** 页签的**通知模板**区域，单击任一模板右侧的**测试**，设置钉钉消息通知机器人以及测试对象，进行消息通知测试。



单击**确定**后，您可以在钉钉群聊中接收到消息通知。



7.1.8 添加企业微信机器人

在星连管理后台的动态策略、管理员告警策略等功能模块中，可以添加消息通知机器人用于接收星连的消息通知。本文将为您介绍如何在星连管理后台添加企业微信机器人，使您可以通过企业微信接收来自星连的消息通知。

✧ 操作指引

在星连内支持配置企业微信应用或者群机器人接收星连消息通知。

通过企业微信应用接收消息通知

该方式适用于星连内的部门、员工信息来自企业微信数据源的场景，后续星连将通过企业微信应用向指定员工推送消息通知。

通过群机器人接收消息通知

该方式无需关注企业员工信息的来源，只要您在企业微信群聊中添加群机器人并获取机器人的 WebHook，即可在星连中添加相应的消息通知机器人，后续星连将通过群机器人推送消息通知。

✧ 通过企业微信应用接收消息通知前提条件

已在星连内导入企业微信组织架构。具体操作，请参见《2.8 同步第三方数据源》。

步骤一：联系星连技术支持代开发企业微信应用

基于企业微信数据安全要求，详情请参见[企业内部开发配置域名指引](#)

(<https://open.work.weixin.qq.com/wwopen/common/readDocument/40754>)，

您需要联系星连技术支持，协助您在企业微信内代开发应用。

步骤二：在星连管理后台配置消息通知机器人

1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **消息通知**。
3. 在**消息通知**页面，单击**第三方 IM** 页签。
4. 在页面右上角，单击**新建机器人**。
5. 在**新建机器人**对话框，完成以下配置，并单击**确定**。配置项说明：

配置项	说明
第三方 IM	选择企业微信。
通知方式	选择应用。
名称	自定义名称，用于标识当前的消息通知机器人。
描述	自定义描述，可选填写。
Corp ID	企业微信对应的企业 ID。获取方式请参见 什么是企业 ID (https://open.work.weixin.qq.com/help2/pc/17377)。
Secret	代开发应用的 Secret。当您联系星连技术支持代开发应用后，技术支持会向您提供应用的 Secret。
Agent ID	代开发应用的 AgentId。在企业微信管理后台的应用管理中，进入代开发应用的详情页即可查看 AgentId 信息。

6. 在**第三方 IM** 页签的**通知模板**区域，单击任一模板右侧的**测试**，设置企业微信消息通知机器人以及测试对象，进行消息通知测试。



单击**确定**后，指定的测试对象可以在企业微信中接收到消息通知。



✧ 通过群机器人接收消息通知

步骤一：在企业微信群中添加群机器人

具体添加方式，请参见[创建群聊机器人](#)

(<https://developer.work.weixin.qq.com/tutorial/detail/54>)。创建后需要保存群机器人的 Webhook。



步骤二：在星连管理后台配置消息通知机

器人1. 登录星连管理后台。

2. 在左侧导航栏，选择**通用配置** > **消息通知**。

3. 在**消息通知**页面，单击**第三方 IM** 页签。

4. 在页面右上角，单击**新建机器人**。

5. 在**新建机器人**对话框，完成以下配置，并单击**确定**。

配置项说明：

配置项	说明
第三方 IM	选择 企业微信 。
通知方式	选择 WebHook 。
名称	自定义名称，用于标识当前的消息通知机器人。
描述	自定义描述，可选填写。
WebHook	群机器人对应的 WebHook 地址。

6. 在**第三方 IM** 页签的**通知模板**区域，单击任一模板右侧的**测试**，设置企业微信消息通知机器人以及测试对象，进行消息通知测试。



单击**确定**后，您可以在企业微信群聊中接收到消息通知。



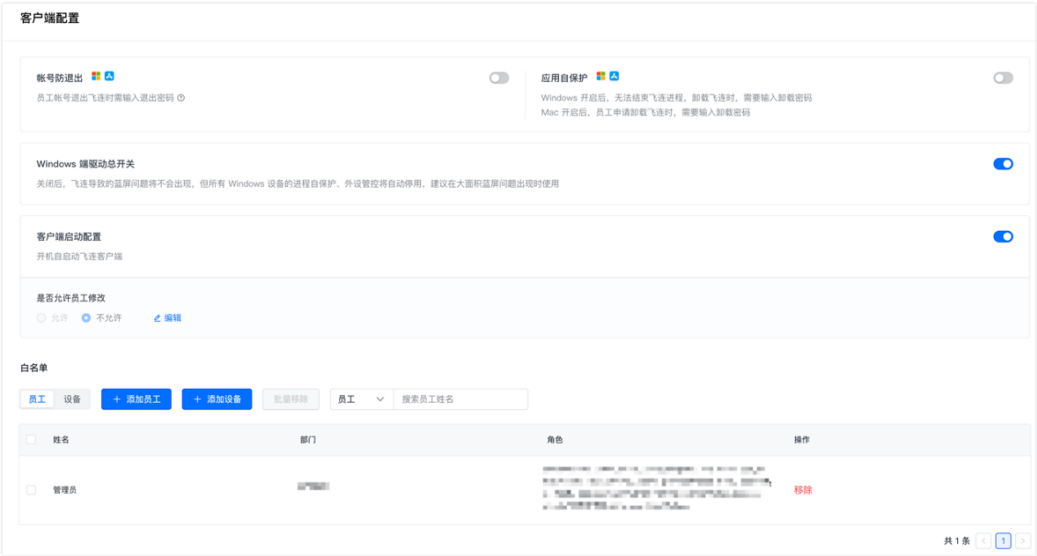
7.2 配置客户端

在客户端配置中，您可以设置星连客户端的帐号防退出、应用自保护、开机自启动等策略，以提高数字化办公的安全性。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **客户端配置**。

3. 在**客户端配置**页面，支持以下操作。



操作说明：

配置项	说明	支持的客户端
帐号防退出	开启后，员工在设备上退出星连客户端的登录帐号时，需要输入 退出/卸载通用密码 ，且员工登录状态自动到期后，无法切换帐号，仅能重新登录当前帐号。 退出/卸载通用密码： 每 15 分钟刷新一次。 配置密码联系人： 当员工想要退出帐号时，可联系管理员获取通用密码。	Windows 、 macOS
应用自保护	开启后：	Windows
	Windows 系统内无法结束星连进程，员工在设备上卸载星连客户端时需要输入 退出/卸载通用密码 。 Mac 系统内卸载星连客户端时需要输入 退出/卸载通用密码 。配置项说明： 可选择开启 Windows 退出任务栏托盘时需要输入退出密码 。 退出/卸载通用密码： 每 15 分钟刷新一次。 配置密码联系人： 当员工想要卸载星连客户端时，可联系管理员获取通用密码。	

Windows 端 驱动总开关	关闭后，星连导致的蓝屏问题将不会出现，但所有 Windows 设备的进程自保护、外设管控将自动停用，建议在大面积蓝屏问题出现时关闭此开关。	Windows
客户端启动配置	开启后，星连客户端将会在设备开机时自启动。	Windows、 macOS、 Linux
是否允许员工 修改	允许：允许员工修改开机自启动星连客户端的配置。 不允许：不允许员工修改开机自启动星连客户端的配置。	Windows、 macOS、 Linux

7.3 配置全局白名单

在星连管理后台有部分功能模块需要配置策略，您可以通过全局白名单功能为指定的一个或多个功能模块设置白名单，在白名单生效范围内的员工或者设备将不受指定功能模块的策略影响。

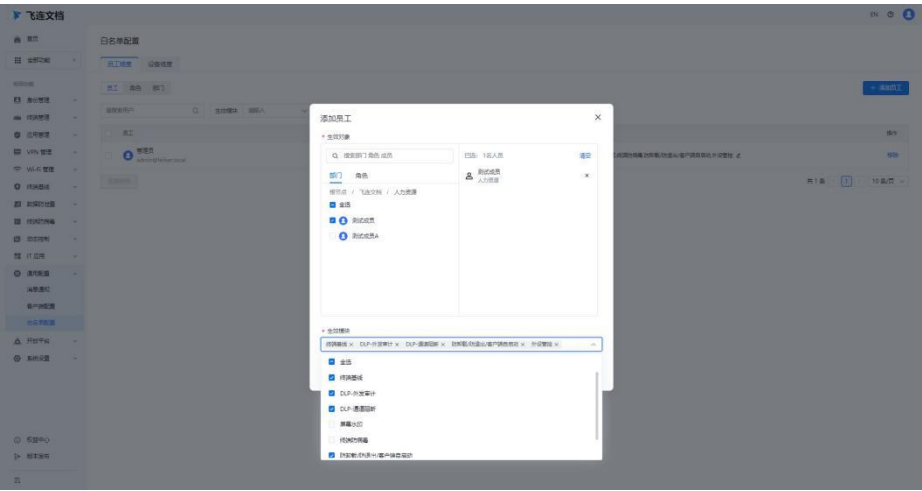
添加白名单

1. 登录星连管理后台。
2. 在左侧导航栏，选择**通用配置** > **白名单配置**。
3. 在**白名单配置**页面，选择**员工维度**或者**设备维度**页签。

全局白名单区分员工维度和设备维度。在员工维度内，您需要指定角色或者部门以确认白名单生效的员工范围。在设备维度，您需要指定某一设备或者指定设备分组以确认白名单生效的设备范围。各维度的配置方式说明如下：

员工维度

- i. 在**员工维度**页签，单击**添加员工**。
- ii. 在**添加员工**对话框，完成以下配置。



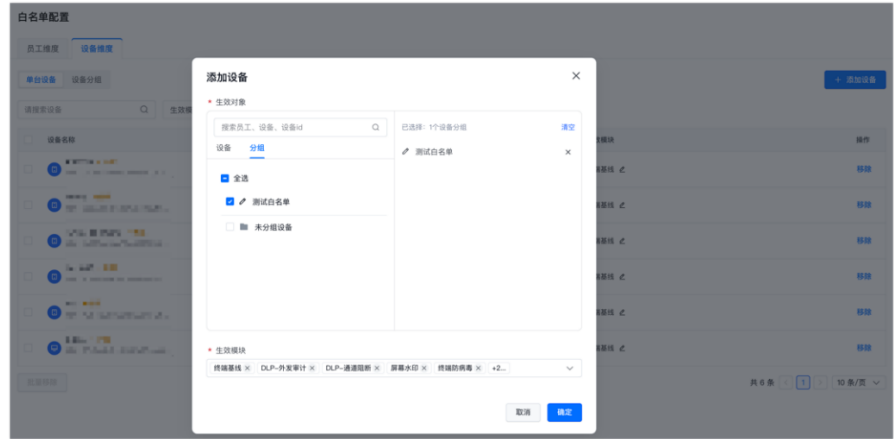
配置项说明：

配置项	说明
生效对象	以部门或角色维度，指定当前白名单生效的员工范围。
生效模块	支持选择一个或多个星连功能模块，或者全选所有功能模块。后续在生效模块内的策略配置将不会影响白名单内的员工。

iii. 单击**确定**，保存白名单配置。

设备维度

- i. 在**设备维度**页签，单击**添加设备**。
- ii. 在**添加设备**对话框，完成以下配置。



配置项说明：

配置项	说明
-----	----

生效对象	以 设备 或 分组 维度，设置白名单生效的设备范围。
生效模块	支持选择一个或多个星连功能模块，或者全选所有功能模块。后续在生效模块内的策略配置将不会影响白名单内的设备。

iii. 单击**确定**，保存白名单配置。

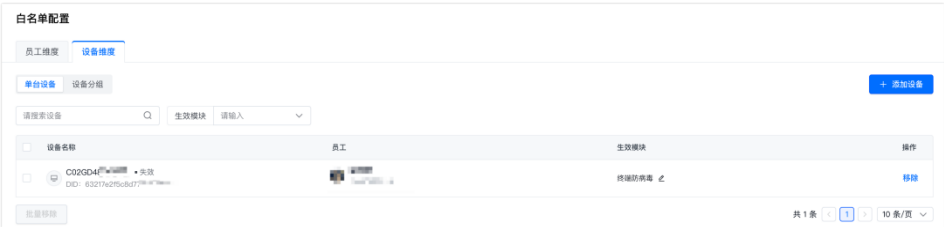
7.3.1 编辑或删除白名单

在**白名单配置**页面，支持分别查看员工维度、设备维度的白名单配置信息。

员工维度页签：查看员工、角色或部门白名单生效的功能模块情况。



设备维度页签：查看单台设备、设备分组白名单生效的功能模块情况。



其中支持以下操作：

在**生效模块**列，单击编辑图标，可手动调整白名单生效的功能模块。

如果不再需要某一白名单配置，可单击**操作**列的**移除**。

注意：

单击移除后，对应模块的白名单会被立即移除，但是部分模块的白名单被移除后，仍需要一定时间才会重新生效。例如，防退出、防卸载需要 15 分钟。
白名单移除后不可恢复，请您谨慎操作。

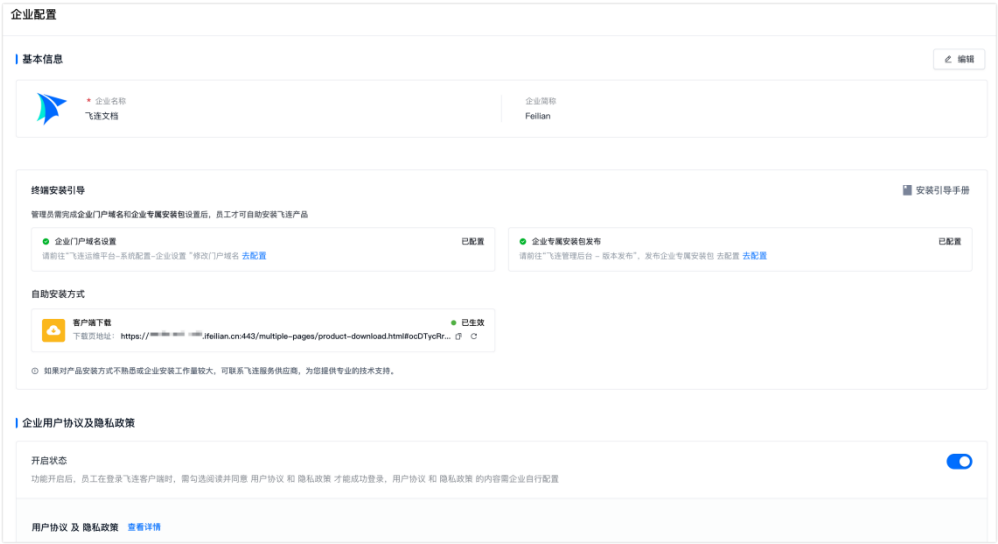
7.4 系统设置

7.4.1 配置与查看企业信息

在系统设置功能的企业配置中，支持编辑或查看星连内的企业基本信息、星连客户端安装包信息、企业用户协议与隐私政策信息、星连内的系统时间。

操作步骤

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择**系统设置** > **企业配置**。
- 3. 在企业配置页面，支持以下操作。



各模块操作说明：

模块	说明
基本信息	包含企业 Logo、企业名称与企业简称信息。在页面右上角单击 编辑 ，可修改企业 Logo、名称与简称。修改完成后需要单击 保存 。
客户端安装说明	支持查看星连客户端安装包的发布情况、下载页生成情况以及下载页地址。

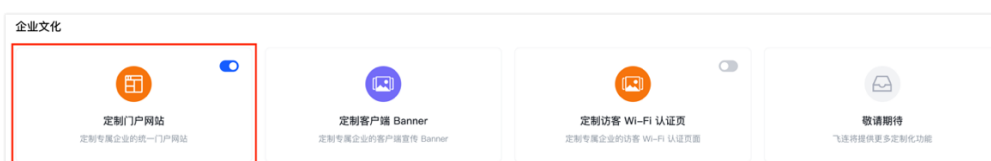
	发布企业专属安装包：当您在星连管理后台的版本 发布功能中上传并发布了客户端安装包，则此处状态会展示为已配置。 分发客户端下载页：当您发布客户端安装包后，星连将自动生成客户端下载页。成功生成客户端下载页 后，此处状态会展示为已生成。 下载页地址：复制该地址信息分发给企业员工，员工访问该地址后可选择下载设备适配的星连客户端。单击重置按钮可以重新生成下载页地址，您可以根据实际需要选择是否重置下载页地址。
企业用户协议及隐私政策	自行配置企业的用户协议与隐私政策，配置说明如下： 开启状态：当您配置好用户协议与隐私政策后，可选择打开该开关。开启后，员工在登录星连客户端时需要先勾选协议与政策前的复选框，才可以继续登录。 用户协议 及 隐私政策：单击查看详情，在对话框中完成企业用户协议与隐私政策的录入（支持录入英文协议，若不配置则只展示中文协议），并单击完成。
系统时间	展示星连管理后台的系统时间。当员工使用动态口令 OTP 时，客户端和管理后台的时间需保持一致，否则可能会导致登录失败。

7.4.2 定制星连门户网站

在星连管理后台企业文化功能中，您可以调整星连门户网站的对外展示风格。此外，星连在门户网站内预留了自定义区域，在自定义区域内，支持通过图片或文字的形式展示企业相关信息。例如，企业公告、重要通知或者帮助文档等。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**系统设置** > **企业文化**。
3. 在企业文化页面，单击**定制门户网站**卡片。



4. 在定制门户网站页面的门户端页签右上角，单击**编辑**。

5. 根据实际需要选择页面类型，可选**控制台型**或者**通知型**，并完成相关配置。

说明：您在填写配置项的过程中，可以通过页面右侧实时查看门户网站的预览效果，以确保配置符合预期。

以**控制台型**配置为例，说明如下：

配置项说明：

配置项	说明
头部背景	设置门户网站页面头部的背景图。
自定义区域	设置区域名称与展示方式，其中，展示方式内支持配置图片或文字任意一种。具体配置说明如下： 配置图片 a) 单击添加图片。 b) 通过上传按钮添加图片并上传。
	c) （可选）根据实际需要选择添加 跳转地址 。如果设置了跳转地址，配置生效后员工点击图片会跳转访问指定的地址。 d) 设置 生效范围 ，可选 全部员工 或 部分员工 。如果选择部分员工，则需要以 部门 或 角色 维度设置生效的员工范围。 e) （可选）继续单击 添加图片 进行配置，多图片以滚动形式在自定义区域展示。 图片要求：

	• 图片仅支持 JPG、JPEG、PNG 格式，大小不超过 500 KB。 • 图片推荐尺寸：336px * 189px。 配置文字 a) 单击添加文字。 b) 设置内容与跳转地址。跳转地址为可选配置，如果设置了跳转地址，配置生效后员工单击文字内容会跳转访问指定的地址。 c) （可选）继续单击添加文字进行配置，多条文字会同时展示在自定义区域。
--	--

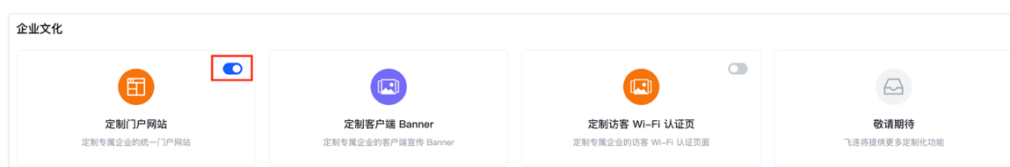
6. 单击**提交**，**暂不生效**或者**提交**，并立即生效。

提交，暂不生效：仅保存当前配置，但不会立刻生效配置，您需要继续下一步开启生效状态开关。

提交，并立即生效：保存当前配置，并立即生效配置。

7. （可选）开启生效开关。

如果您的门户网站配置生效开关未打开，或者定制门户网站时选择了**提交，暂不生效**，则需要在企业文化页面的定制门户网站卡片中，开启配置的生效开关。



7.4.3 定制客户端 Banner

客户端 Banner 是指展示在星连客户端内的横幅图片，一般用于展示企业 Logo 或者统一企业风格的图片。

操作步骤

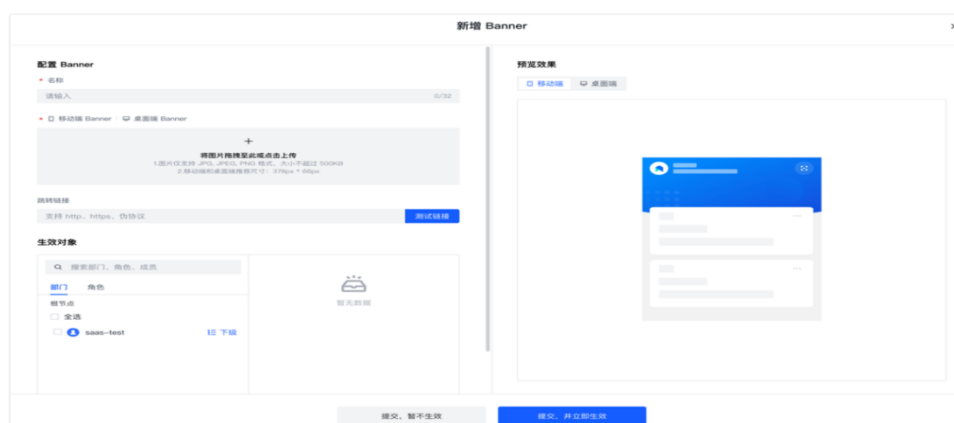
1. 登录星连管理后台。
2. 在左侧导航栏，选择**系统设置** > **企业文化**。
3. 在企业文化页面，单击**定制客户端 Banner** 卡片。



4. 在**客户端 Banner** 页面，单击**新增 Banner**。

5. 在**新增 Banner** 页面，完成以下配置

说明：在页面左侧配置 Banner 区域填写配置项后，可以在页面右侧**预览效果**区域实时查看**移动端**与**桌面端**的效果。



配置项说明：

配置项	说明
名称	Banner 的名称，仅用于在后台标识当前 Banner，不会展示在星连客户端。
移动端 Banner 桌面端 Banner	同步设置移动端与桌面端的星连客户端 Banner 图片。以拖拽或上传的方式，将 Banner 图片添加至该配置项。图片要求：图片仅支持 JPG、JPEG、PNG 格式，大小不超过500KB。移动端和桌面端推荐尺寸为 378px * 66px。
跳转链接	可选配置。 如果设置了跳转链接，则配置生效后在客户端内点Banner会条转发访问该链接。如果没有设置跳转链接，则配置生效后客户端内仅展示 Banner。
生效对象	设置当前 Banner 配置的生效范围，您需要以 部门或角色 维度设置生效的员工范围。

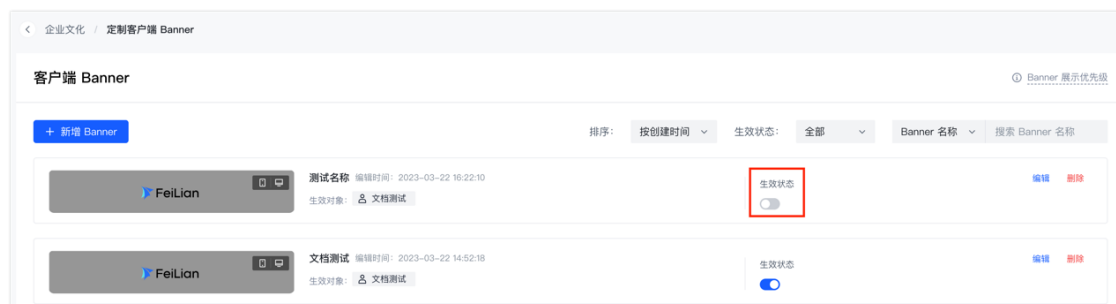
6. 单击**提交，暂不生效**或者**提交，并立即生效**。

提交，暂不生效：仅保存当前配置，但不会立刻生效配置，您需要继续下一步开启生效状态开关。

提交，并立即生效：保存当前配置，并立即生效配置。

7. （可选）开启生效开关。

如果您的客户端 Banner 配置生效开关未打开，或者添加客户端 Banner 配置时选择了**提交，暂不生效**，则需要在客户端 Banner 列表中，开启相应配置的生效开关。



7.4.4 定制访客 Wi-Fi 认证页

配置访客 Wi-Fi 后，访客 Wi-Fi 认证页面的 Logo、背景图片支持自定义配置。本文介绍如何自定义配置访客 Wi-Fi 认证页的 Logo 与背景图片。

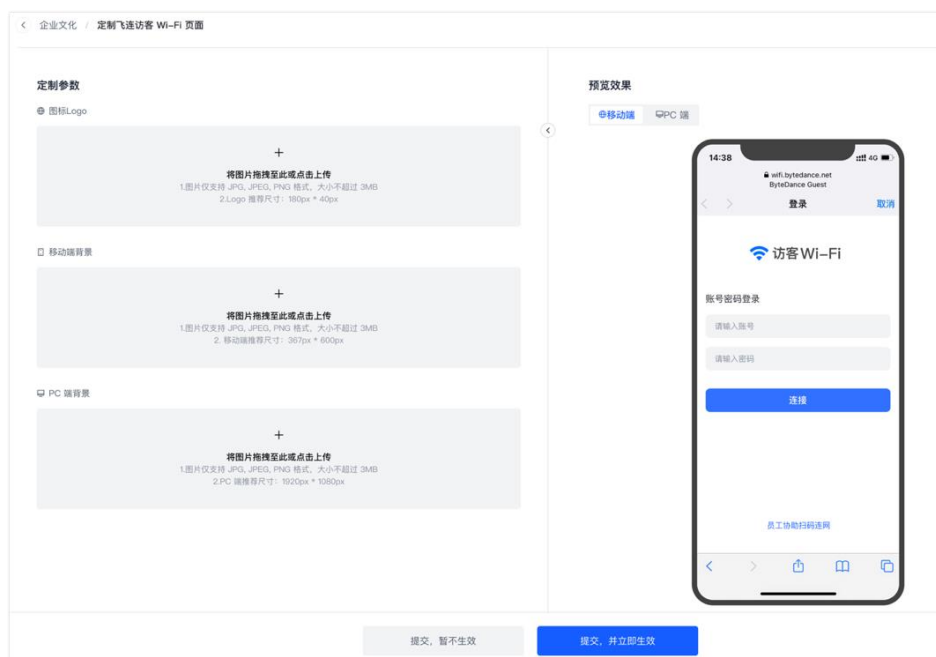
操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**系统设置** > **企业文化**。
3. 在**企业文化**页面，单击**定制访客 Wi-Fi 认证页**卡片。



4. 在**定制星连访客 Wi-Fi** 页面，根据实际需要选择上传**图标 Logo**、**移动端背景**、**PC 端背景**。

说明：在页面左侧**定制参数**区域填写配置项后，可以在页面右侧**预览效果**区域实时查看**移动端**与**PC 端**的效果。



5. 单击**提交，暂不生效**或者**提交，并立即生效**。

提交，暂不生效：仅保存当前配置，但不会立刻生效配置，您需要继续下一步开启生效状态开关。

提交，并立即生效：保存当前配置，并立即生效配置。

6. （可选）开启生效开关。

如果您的访客 Wi-Fi 认证页配置生效开关未打开，或者定制访客 Wi-Fi 认证页时选择了**提交，暂不生效**，则需要在企业文化页面的定制访客 Wi-Fi 认证页卡片中，开启配置的生效开关。



7.4.5 查看星连日志审计

在日志审计功能中支持查看员工活动日志、管理员操作日志，以及 VPN、Wi-Fi 相关的员工与设备连接日志。

7.4.5.1 注意事项

当有员工或设备活动后，才会生成相应的日志。

例如，新员工入职连接访客 Wi-Fi 配置办公环境时，会生成一条访客 Wi-Fi 连接日志。

部门日志列表的列字段较多，在页面内支持左右滑动列表查看完整列字段。

7.4.5.2 操作步骤

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择**系统设置** > **日志审计**。
- 3. 在**日志审计**页面，支持查看以下信息。

员工活动日志

包含员工登录登出、修改个人信息、访问应用操作类型的日志，支持条件过滤或者关键词搜索指定日志。

日志审计						
员工活动日志 管理操作日志 员工 VPN 连接日志 员工 VPN 访问日志 员工 Wi-Fi 连接日志 访客 Wi-Fi 连接日志 超管访问日志						
操作类型	操作时间	操作来源	操作时间	操作设备	飞信版本	IP
管理操作	2023-05-12 19:22:08	用户名为"admin@hellan.local"	Mac 2.1.12	Apple MacBook Pro11,1	v2.1.12	124.1.....194

管理员操作日志

包含企业管理员在星连管理后台各个模块操作的日志，支持条件过滤或者关键词搜索指定日志。

日志审计						
员工活动日志 管理操作日志 员工 VPN 连接日志 员工 VPN 访问日志 员工 Wi-Fi 连接日志 访客 Wi-Fi 连接日志 超管访问日志						
操作类型	操作时间	操作来源	操作时间	操作设备	飞信版本	IP
管理操作	2023-05-12 20:36:05	用户名为"admin@hellan.local"	Mac 2.1.12	Apple MacBook Pro11,1	v2.1.12	124.1.....194

员工 VPN 连接日志

包含企业员工通过客户端连接星连 VPN 节点的日志信息，支持条件过滤或者关键词搜索指定日志。

日志审计

日志外发配置

员工活动日志 管理员操作日志 员工 VPN 连接日志 员工 VPN 访问日志 员工 Wi-Fi 连接日志 访客 Wi-Fi 连接日志 有线网络连接日志

操作系统 选择器 飞流版本 选择器 网络模式 选择器 设备名称 选择器 设备状态 选择器 连接时间 开始时间 结束时间 回

开始时间 开始日期 结束日期 回 员工 输入关键字或设备人员 导出

姓名	设备名称	网络模式	连接时间	开始时间	操作设备	飞流版本	用户 IP	内网 IP
管理机 win10phillan.local	杭州节点	有线模式	2023-05-11 23:37:13	2023-05-11 23:39:49	windows Windows10_x1 型号: WINXOYDZJANASDVC	v2.5.14	124...154	10.8.8.37

在员工 VPN 连接日志列表中，未完全展示所有列字段，您可以单击列表右侧 **...**，自定义列字段信息。

日志审计

日志外发配置

员工活动日志 管理员操作日志 员工 VPN 连接日志 员工 VPN 访问日志 员工 Wi-Fi 连接日志 访客 Wi-Fi 连接日志 有线网络连接日志

操作系统 选择器 飞流版本 选择器 网络模式 选择器 设备名称 选择器 设备状态 选择器 连接时间 开始时间 结束时间 回

开始时间 开始日期 结束日期 回 员工 输入关键字或设备人员 导出

姓名	设备名称	网络模式	连接时间	开始时间	操作设备	飞流版本	用户 IP	内网 IP
管理机 win10phillan.local	杭州节点	有线模式	2023-05-11 23:37:13	2023-05-11 23:39:49	windows Windows10_x1 型号: WINXOYDZJANASDVC	v2.5.14	124...154	10.8.8.37
管理机 win10phillan.local	杭州节点	有线模式	2023-05-11 22:26:35	2023-05-11 22:42:16	windows Windows10_x1 型号: WINXOYDZJANASDVC	v2.5.14	124...154	10.8.8.125
管理机 win10phillan.local	杭州节点	无线模式	2023-05-11 22:07:15	2023-05-11 22:29:32	windows Windows10_x1 型号: WINXOYDZJANASDVC	v2.5.14	124...154	10.8.8.100
管理机 win10phillan.local	杭州节点	无线模式	2023-05-11 22:06:27	2023-05-11 22:06:40	windows Windows10_x1 型号: WINXOYDZJANASDVC	v2.5.14	124...154	10.8.8.120
管理机 win10phillan.local	杭州节点	有线模式	2023-05-11 22:06:17	2023-05-11 22:06:25	windows Windows10_x1 型号: WINXOYDZJANASDVC	v2.5.14	124...154	10.8.8.0

姓名
 设备名称
 网络模式
 连接时间
 开始时间
 操作设备
 飞流版本
 用户 IP
 内网 IP

员工 VPN 访问日志

包含企业员工连接星连 VPN 节点后，访问网络资源的日志信息。该类型的日志数据量较大，仅支持通过 elasticsearch 或 syslog 协议外发后查看，因此您必须配置日志外发。具体配置操作，请参见《15.6 配置日志外发》。

说明：员工 VPN 访问日志列表的列字段支持自定义，单击**点击下载字段**进行配置。



员工 Wi-Fi 连接日志

包含企业员工连接员工 Wi-Fi 的日志信息，支持条件过滤或者关键词搜索指定日志。

日志外发配置

×

* 外发协议类型

☐ syslog

☐ elasticsearch

外发日志类型

☐ VPN连接日志

☐ 员工 Wi-Fi 连接日志

☐ 访客 Wi-Fi 连接日志

☐ 哑终端 Wi-Fi 连接日志

☐ 员工 VPN 访问日志

☐ 动态控制处置日志

☐ 数据防泄漏-审计日志

☐ 数据防泄漏-阻断日志

☐ 终端防病毒日志

☐ 设备信息日志

☐ 员工登录日志

取消

确定

配置项说明：

配置项	说明
外发协议类型	可选 syslog 或者 elasticsearch 。
外发日志类型	在需要外发的日志类型前，选中复选框，然后配置外发信息。 如果外发协议选择 syslog ，则需要配置 地址 ，该地址是指向 syslog 程序所在服务器的 TCP/UDP 地址。 如果外发协议选择 elasticsearch ，则需要配置以下信息： 服务地址 ：elasticsearch 程序所在服务器的地址。 索引名称 ：日志数据外发至 elasticsearch 后，保存的索引位置。 用户名和密码 ：用于连接 elasticsearch 时用户认证的用户名和密码信息。

7.4.7 添加管理员

您可以根据企业员工的职责所需，在星连管理后台设置多个管理员。管理员权限以功能划分，您可以为不同的管理员分配不同功能的管理权限。本文介绍如何在星连管理后台添加管理员。

7.4.7.1 注意事项

在添加管理员时支持授予该管理员修改其他管理员权限的能力，因此建议您以最小权限的策略安排所添加管理员的权限范围，以避免产生权限管理相关的安全风险。

7.4.7.2 操作步骤

- 1. 登录星连管理后台。
- 2. 在左侧导航栏，选择**系统设置** > **管理员权限**。
- 3. 在**管理员配置**页面右上角，单击**添加管理员**。
- 4. 在**添加管理员**页面，完成以下配置，并单击**确认添加**。配置项说明如下表：

配置项	说明
管理员名称	在下拉列表选择或者搜索指定员工的名称，该员工将被添加为管理员。
权限组	星连默认提供了 IT 管理员、人事管理员 以及 超级管理员 三类权限组，该配置项非必选。您可以选择权限组快速指定管理员的权限范围，也可以在下文的细分权限中手动指定管理员的权限范围。 说明：选中指定权限组后，可以在细分权限配置项内查看具体管理权限。权限组内默认权限为必选项，不可取消选中，您可以继续添加未选中的细分权限项。

管理范围	设置当前管理员权限管理的范围。可选项说明如下： 全公司：可在企业范围内进行管理。 所在部门及下级：可在指定管理员所在的部门范围内进行管理。 特定部门：管理员可在指定部门范围内进行管理。在选择部门下拉列表中支持选中一个或多个部门，选中部门时不包含其中的子部门，子部门需要单独选择。
可以修改管理范围内管理员的权限	选中可以修改管理范围内管理员的权限复选框后，默认会选中细分权限里系统设置 > 管理员权限。如果当前管理员（示例名称管理员 A）管理范围内存在其他员工也是管理员身份（示例名称管理员 B），则管理员 A可以修改管理员 B的管理权限。
细分权限	根据星连管理后台的功能模块细分权限，您可以选中指定功能前的复选框，为当前管理员授予管理权限。如果您配置了权限组，权限组内默认包含的功能模块前的复选框不可取消。

7.4.7.3 相关操作

添加管理员后，您可以根据组织或人员变化动态调整管理员的权限。具体操作，请参见《7.4.8 编辑或删除管理员》。

您可以为管理员配置告警策略，当管理员帐号连续多次登录认证失败时向指定渠道发送通知，帮助您及时发现潜在的安全风险。具体操作，请参见《7.4.9 配置管理员告警策略》。

7.4.8 编辑或删除管理员

在管理员权限功能中，可以编辑指定管理员的权限范围，或者删除指定管理员。

7.4.8.1前提条件

您当前登录的帐号需要拥有星连管理员权限，且权限内包含了管理其他管理员权限的能力。

7.4.8.2编辑管理员权限

1. 登录星连管理后台。
2. 在左侧导航栏，选择**系统设置** > **管理员权限**。
3. 在**管理员权限**页签，找到指定的管理员，在**操作**列单击**编辑**。

说明：不可编辑当前正在登录的管理员权限。



管理员配置					
搜索部门、成员 + 添加管理员					
管理员权限 管理员配置					
姓名	邮箱	手机号	部门	权限	操作
管理员	admin@feilan.cn	13900000000	系统管理	超级管理员	编辑 删除
管理员	admin@feilan.cn	13900000000	系统管理	超级管理员	编辑 删除
管理员	admin@feilan.cn	13900000000	系统管理	统一认证	编辑 删除

4. 在修改管理员页面，根据需要调整管理员的管理范围与权限范围，并单击**确认修改**。

7.4.8.3 删除管理员

当管理员身份被删除后，对应的帐号将无法继续登录和使用星连管理后台。

1. 登录星连管理后台。
2. 在左侧导航栏，选择**系统设置** > **管理员权限**。
3. 在**管理员权限**页签，找到指定的管理员，在**操作**列单击**删除**。

说明：不可删除当前正在登录的管理员权限。



管理员配置					
搜索部门、成员 + 添加管理员					
管理员权限 管理员配置					
姓名	邮箱	手机号	部门	权限	操作
管理员	admin@feilan.cn	13900000000	系统管理	超级管理员	编辑 删除
管理员	admin@feilan.cn	13900000000	系统管理	超级管理员	编辑 删除
管理员	admin@feilan.cn	13900000000	系统管理	统一认证	编辑 删除

4. 在**删除提示**对话框，单击**删除**。

7.4.9 配置管理员告警策略

您可以设置管理员帐号在连续登录失败时向指定的手机、邮箱或者第三方 IM 发送告警通知，使您可以及时发现管理员帐号可能存在的安全风险。

操作步骤

1. 登录星连管理后台。
2. 在左侧导航栏，选择**系统设置** > **管理员权限**。
3. 在**管理员配置**页签，设置管理员帐号连续几次登录失败，并选中复选框。
后续当管理员帐号连续登录失败达到指定次数时，会按照告警策略的配置发送告警通知。
4. 在**管理员告警策略**区域右侧，单击**通知策略**。
5. 在**编辑通知策略**页面，完成以下配置，并单击**立即生效**。

告警通知支持选择**短信通知**、**邮箱通知**或者**第三方 IM 通知**，支持多选，当触发告警时会同时向指定渠道发送告警通知。

各通知渠道说明：

通知渠道	说明
------	----

短信通知	配置 通知手机号 。可以添加多个手机号码，以回车键 Enter 间隔。
邮箱通知	配置 通知邮箱 。可以添加多个邮箱地址，以回车键 Enter 间隔。
第三方 IM 通知	在下拉列表中选择第三方 IM 机器人。该通知方式要求提前配置好 IM 机器人，您可以单击下拉列表中的 新增机器人 ，前往添加机器人。添加机器人的具体配置方式，请参见《7.1.5 管理第三方 IM》。