向日葵

贝锐向日葵管理平台

使用手册

V1.5.0

202301121900

目录

1. 概述

向日葵是国内知名软硬结合的远程控制服务商，深耕远程行业十余年，自主研发向日葵远程控制软件及开机棒、开机插座、控控/方舟、插线板等多款智能硬件，实现远程开机-控制-关机一体化操作，支持电脑、手机、平板之间相互控制。满足 IT 远程运维、技术支持远程协助、企业远程办公、远程教学等场景需求。

贝锐向日葵管理平台为用户提供高效的远程管理系统，设备智能分组、第三方帐号对接、角色权限自定义、监控报警、文件/消息批量分发、IT 资产统计等管理功能，支持多种因子安全认证机制，数据可视化呈现，审计日志有效溯原，个性定制远程控制软件。让数据更安全，管理更有效，运维更简单。

2. 登录

访问向日葵管理平台，输入向日葵帐号密码登录，本文将详细介绍这些功能模块的使用。

3. 功能详解

本节主要介绍向日葵管理平台界面上的各项功能，向日葵管理平台主要有以下六大功能模块：**帐号体系、设备管理、IT 资产管理、审计日志、坐席管理、系统管理**。

3.1 帐号体系

企业管理员可通过角色和帐号模块功能，根据人员职权去授权远程运维企业设备，提高运维效率，企业信息安全更有保障。

3.1.1 角色权限

企业内部根据层级部门来划分不同权限，使各部门间权责清晰、分工明确。向日葵帐号体系中，为细分企业内各部门人员的远程访问权限，支持创建不同角色，并按照员工角色授权不同的远控权限。权限可随时回收，管理自由灵活。

举例：

①普通员工：仅开放基础的远程控制权限

②财务员工：为保障信息安全对财务人员关闭文件传输或设置单向文件传输等功能

除此以外，还可以对企业内的管理者进一步授权不同的管理权限。

控制端版本要求：

Windows 系统：企业控制端 v5.6.2 及以上版本

安卓系统：控制端 v13.0 及以上版本

iOS 系统：控制端 13.1 及以上版本

（1）角色类型

默认内置三个角色（不可删除）：「超级管理员」、「普通管理员」、「普通员工」；

超级管理员默认拥有企业的完整管理权限（不可更改）；

普通管理员和普通员工根据实际需求授权不同远控权限。

（2）权限类型

权限类型有「基础权限」、「控制端常规权限」和「管理权限」。

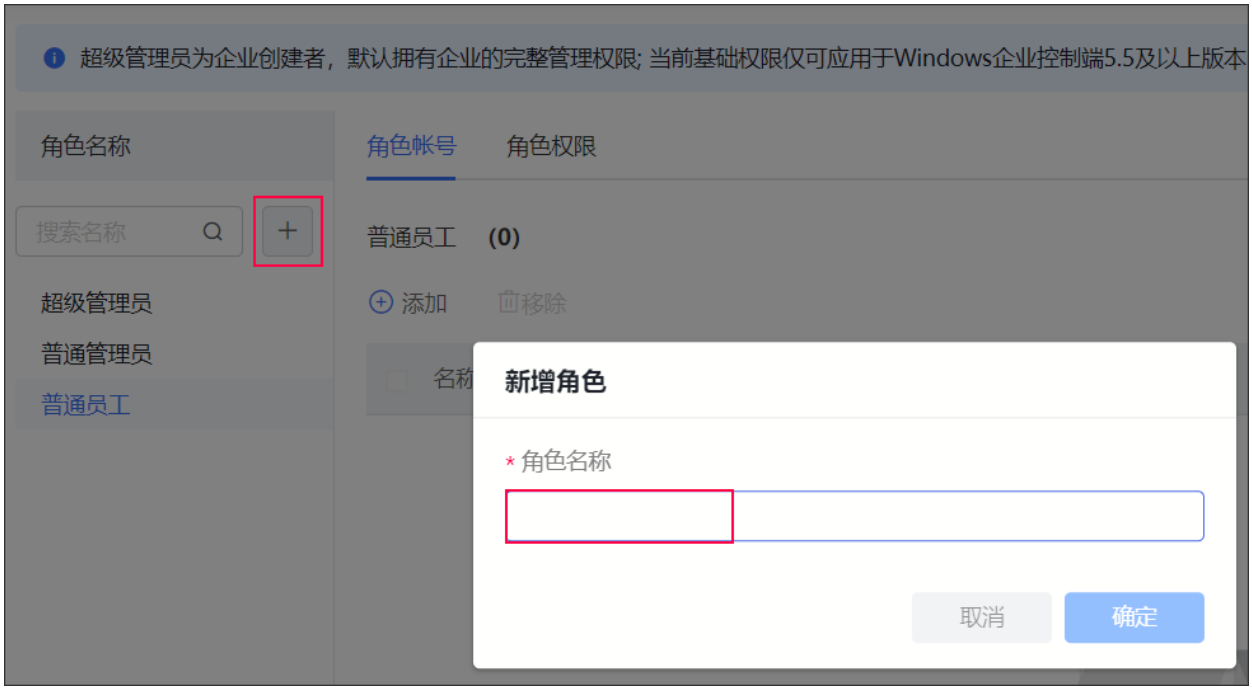
3.1.1.1 创建角色授权功能

企业可按研发、营销、测试、行政等部门划分组织架构，再给不同职能的人员授权不同的角色权限，清晰直观。

以财务部门为例，为保障信息安全，管理员对财务人员的角色设置禁止使用“传输文件”等功能，下面请看操作步骤。

（1）创建角色

点击“+”**新增角色**，为角色命名，如“财务人员”。



（2）授权角色权限

角色创建完成，选中角色。并点击“**角色权限**”，为角色授予相应权限。

下图例子为关闭角色的部分权限功能：

①基础权限（**发送文件、接收文件、剪贴文本、剪贴文件、录像、截屏**）

②控制端常规权限（**屏幕墙**）

3.1.1.2 创建帐号绑定角色

操作路径：管理平台->【帐号体系】->【帐号管理】

①为财务部门人员创建专属的帐号，点击【添加】->【添加帐号】

②填写创建帐号所需的信息

填写项	说明
帐号、名称	自定义
手机号、邮箱	填写使用者有效手机号码与邮箱，用于接收验证码
分配部门	设置该帐号所属部门 ，比如“财务部”
角色权限	为该帐号分配角色，如财务人员张颖所属角色为“财务人员”
有效期	设置帐号可用时间，可设长期或指定时间内有效

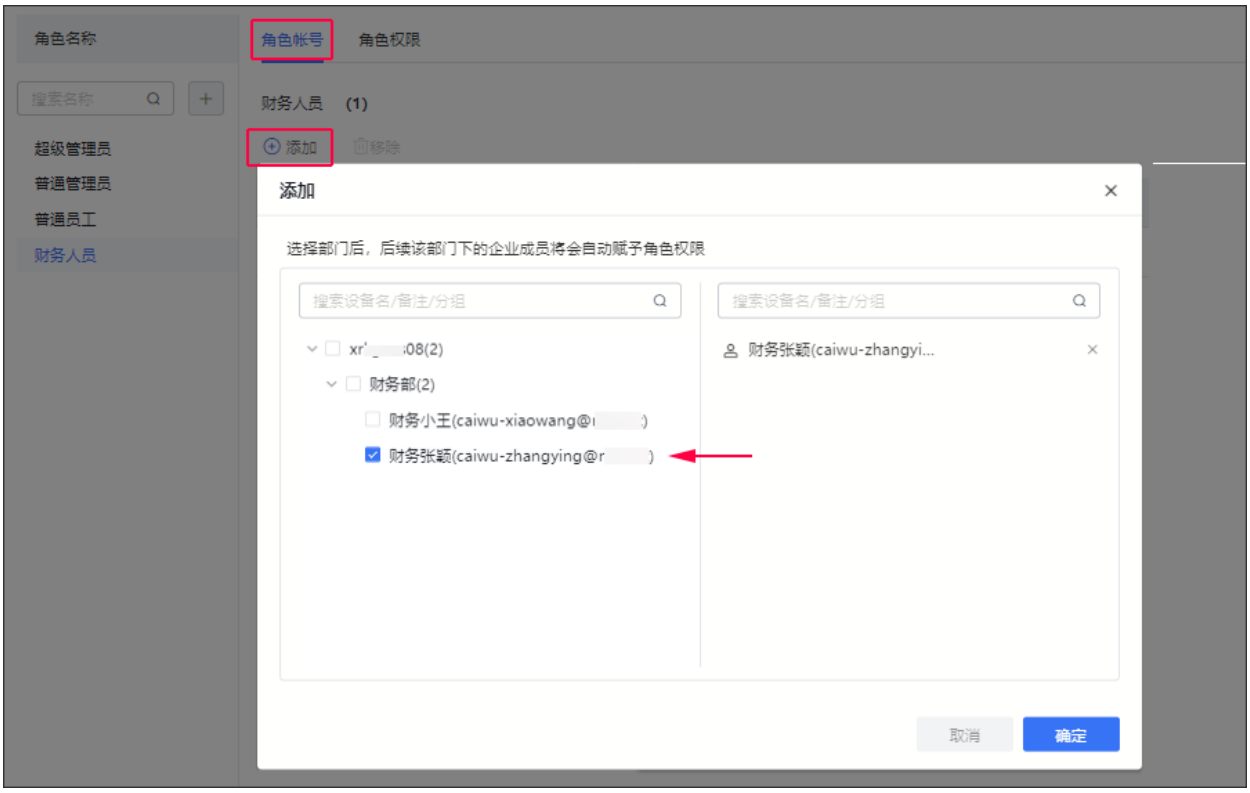
③您也可以创建帐号后，在已有的“**角色**”中，将角色快速赋予指定的员工帐号或部门。

在【**角色帐号**】->点击【**添加**】：

①**添加成员**：为单个成员授权角色权限，配置灵活

②**添加部门**：可自动赋予属于该部门中成员权限，无需为相同部门的成员重复配置权限

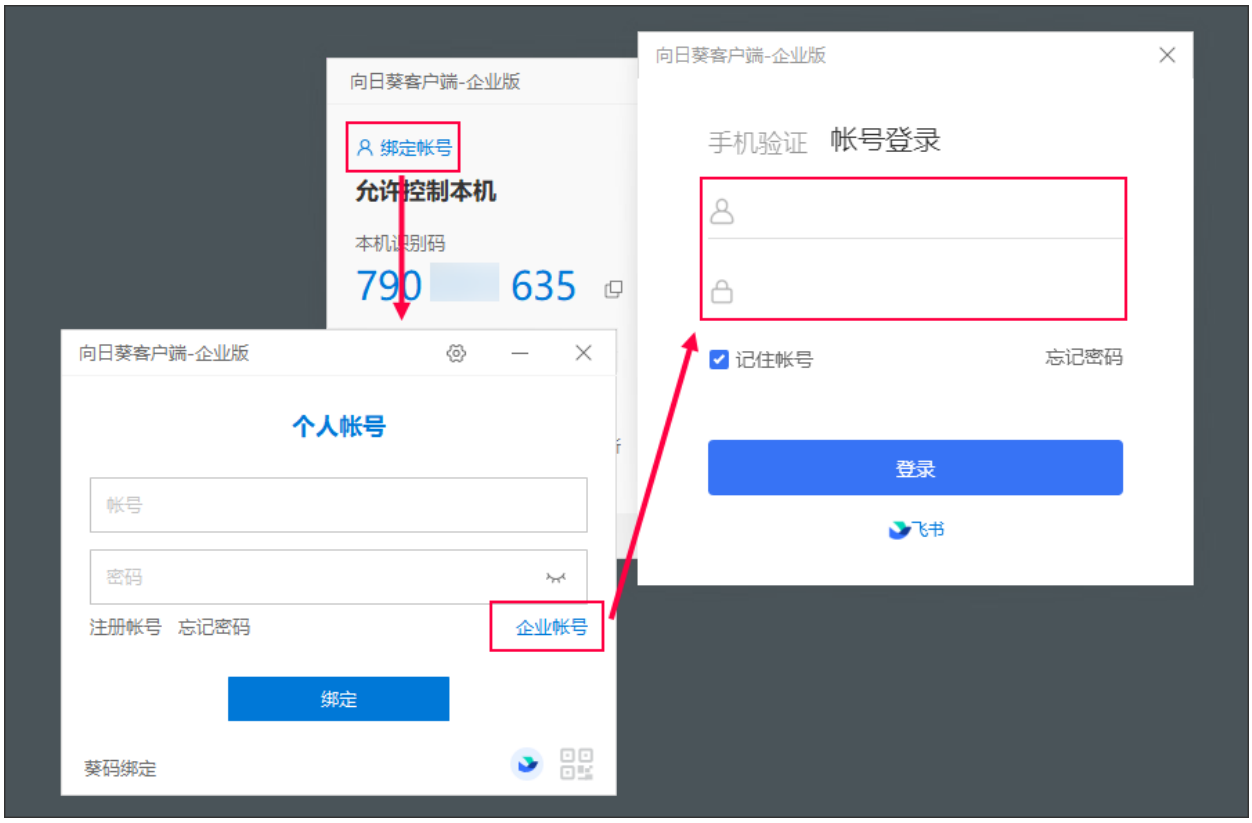
比如选择财务部，后续财务部增加新员工小李，将自动为小李赋予该角色的权限。



3.1.1.3 远控设备权限演示

（1）远控菜单权限

①财务电脑安装向日葵企业版客户端（Windows），输入财务人员帐号登录



②财务人员安装向日葵企业版控制端（以 Windows 版为例），以“企业帐号”方式登录

③控制端软件所拥有的功能，根据其登录的帐号来决定。在设备列表中，选中财务-张颖的设备，发起远程控制

④可以看到，在远控菜单栏中，仅有帐号所对应角色拥有的权限，**无文件传输、录像、截屏等权限**

附远控菜单完整功能图片：

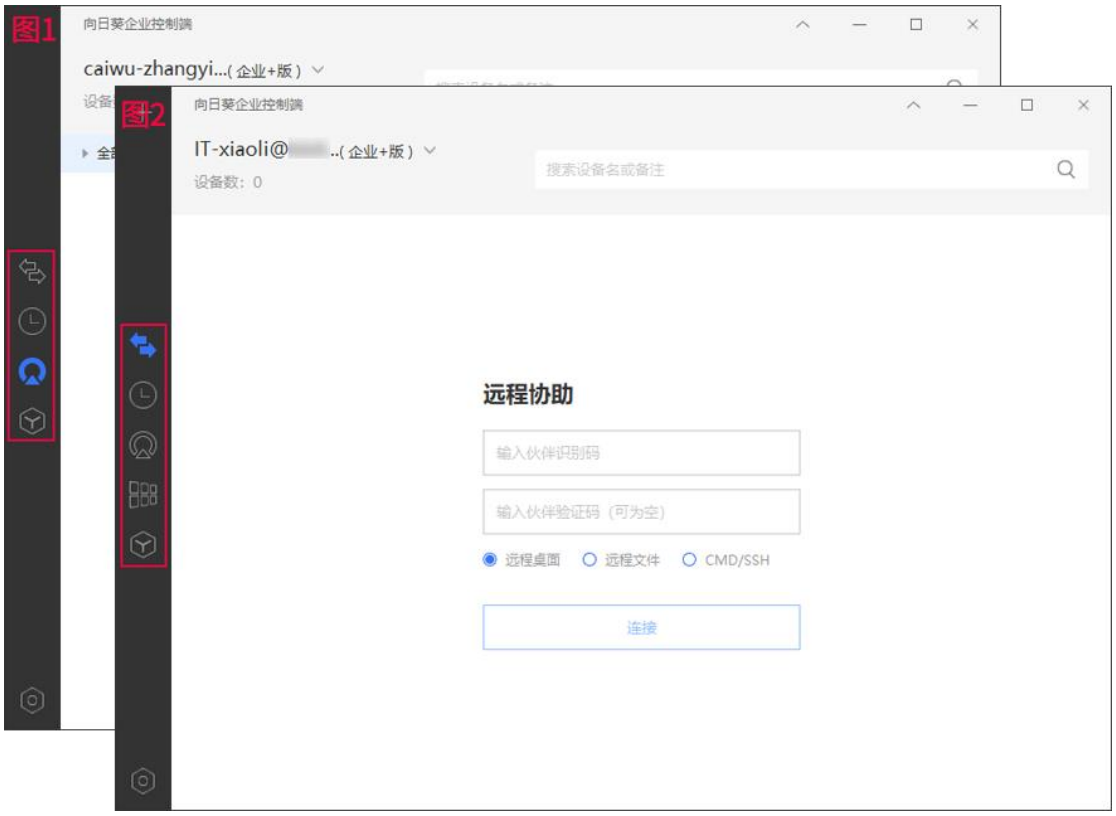
（2）控制端权限

控制端常规权限，由所登录的帐号决定哪些功能可用。

如下图所见：

图 1 帐号登录控制端后，左侧菜单栏功能中无“**屏幕墙**”功能；

图 2 所登录帐号具备控制端常规权限所有功能。



3.1.1.4 文件传输方向设置

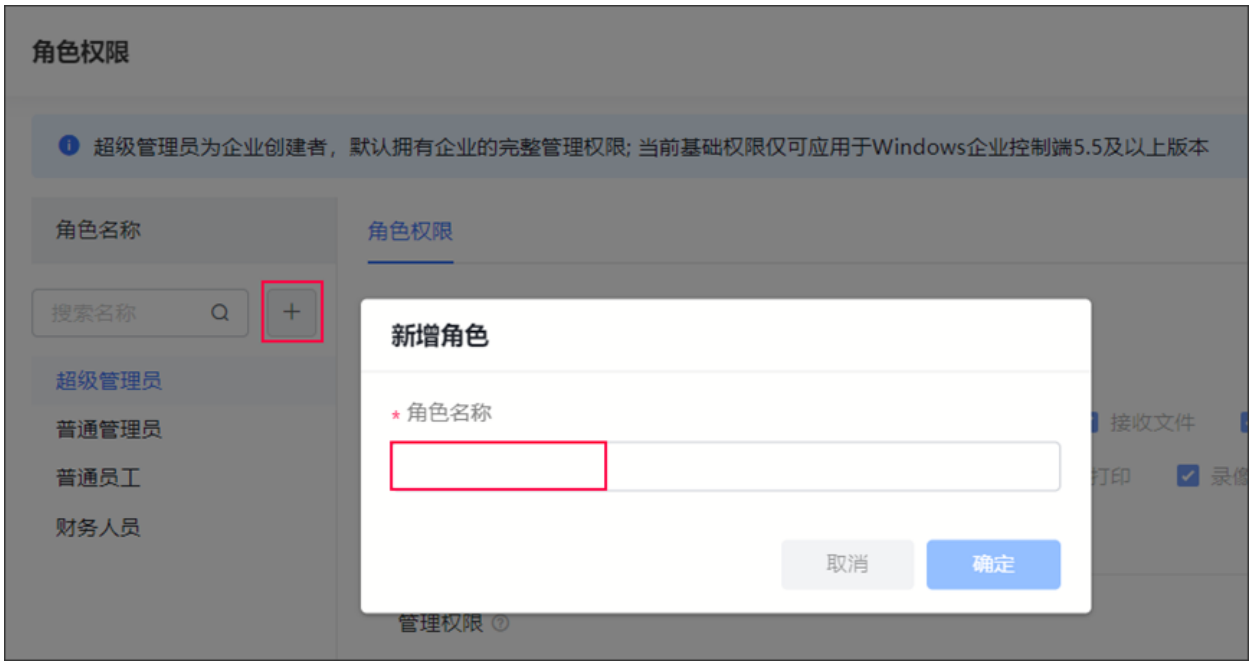
角色权限的设置中，还支持文件传输方向的设置。您可以根据实际应用场景，定制**单向传输文件（发送文件、接收文件、编辑文件）**。

比如出差在外的销售人员，仅支持往公司电脑发送文件（上传）和编辑文件，不支持接收文件（下载）。下面举例说明：

操作路径：管理平台-> **【帐号体系】-> 【角色权限】**

（1）新增“销售人员”角色

点击**“+”新增角色**，角色命名为“销售人员”。



（2）设置“销售人员”角色权限

在【基础权限】中，勾选“发送文件”、“编辑文件”，取消“接收文件”，点击保存。

（3）新增销售帐号并划分角色

在【帐号管理】中点击“添加帐号”，设置帐号名称/帐号等信息，设置其所属部门为销售部，角色为“销售人员”。

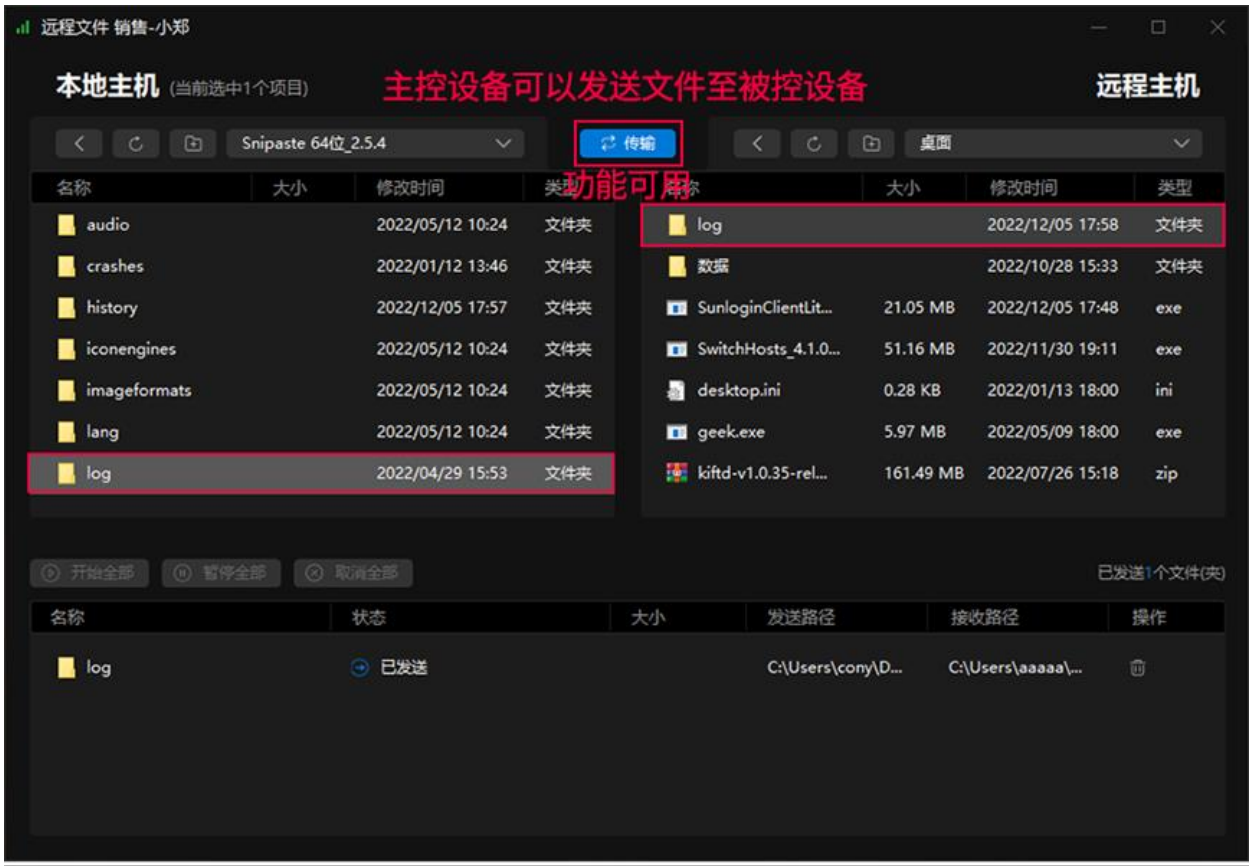
（4）远控功能

①销售小郑在公司电脑，安装企业版客户端并登录其所属帐号（sales-xiaozheng@****）

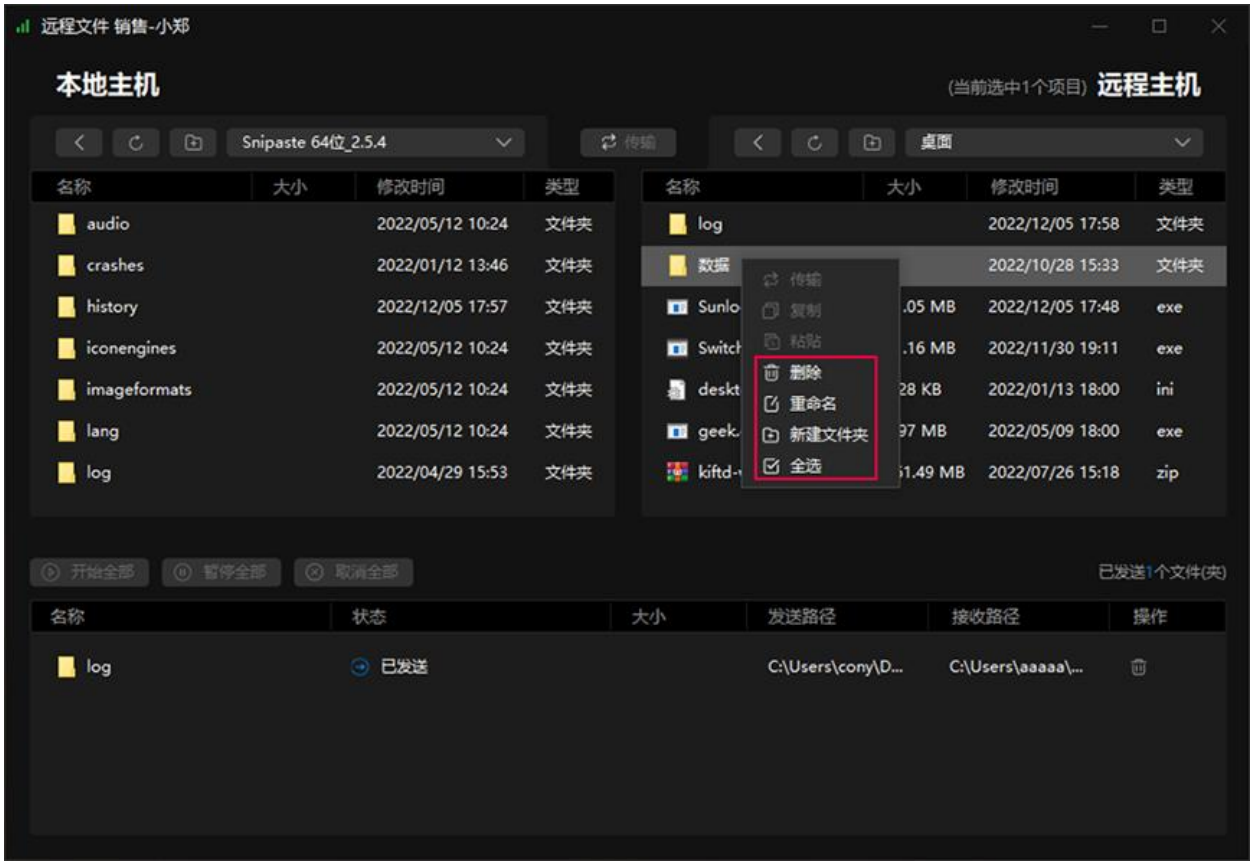
②外出时，在笔记本电脑上使用企业版控制端软件，以“企业帐号”方式登录帐号 sales-xiaozheng@****

③在【设备列表】中，选中主机，发起“远程文件”功能

④验证通过后，可往公司电脑发送（上传）文件，无法从公司电脑下载文件



⑤由于该角色支持编辑文件，右键点击公司电脑的文件，可以对远端主机文件进行删除、重命名、和新建文件夹操作



3.1.2 帐号管理

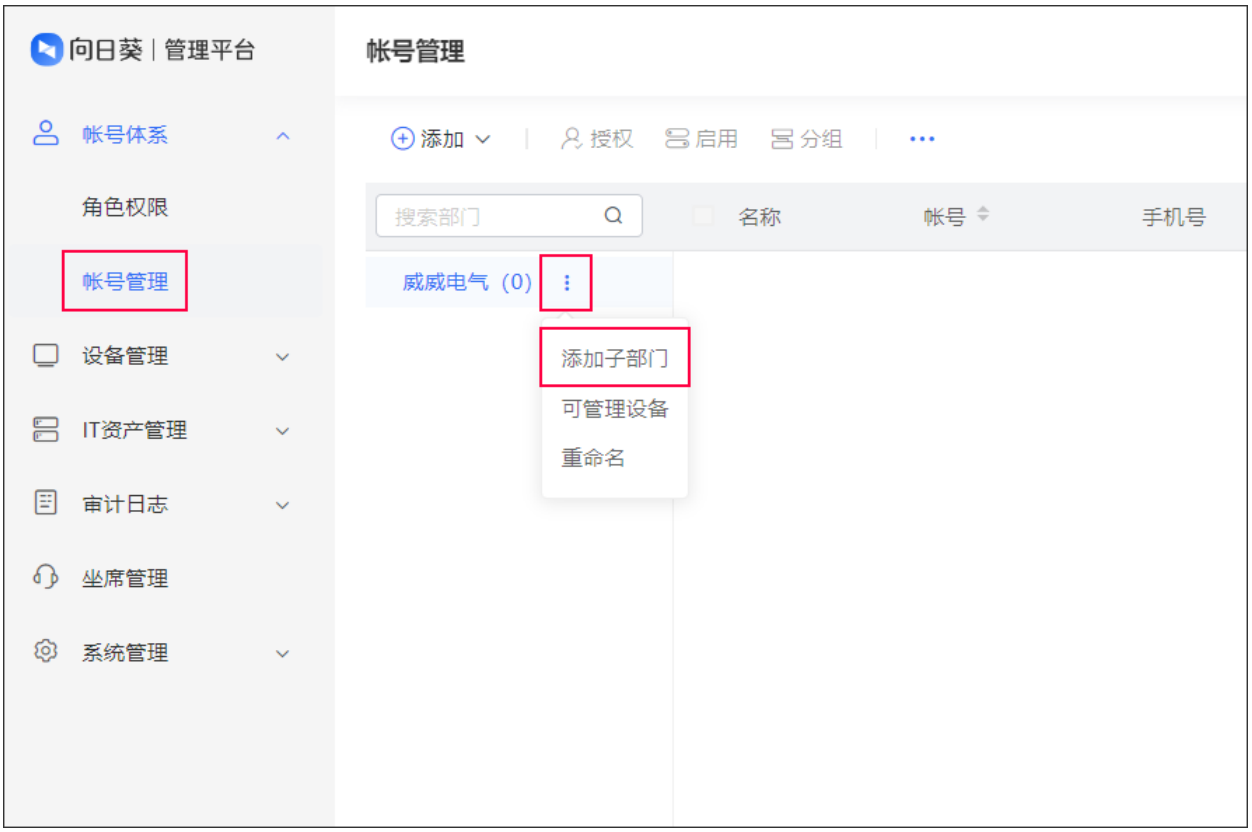
向日葵企业+解决方案具有完备的帐号体系，管理员可根据企业架构创建组织，并为每位员工创建帐号，以及划分所属部门和角色权限。员工远程办公使用独立帐号登录，互不干扰。还支持三方帐号对接，直接导入企业原有的组织架构及帐号信息，无需重复设置，轻量部署，提升管理效率。

3.1.2.1 创建组织架构

操作路径：管理平台->【帐号体系】->【帐号管理】

可添加子部门并划分其所属部门，支持创建多层级部门。支持重命名部门名称及调整部门的层级排序，亦可批量给整个部门授权可管理的设备。

①**添加部门**，根据企业组织架构新增部门



②添加子部门，在已有部门下添加对应子部门

3.1.2.2 添加帐号

操作路径：管理平台->【帐号体系】->【帐号管理】

可单个或批量添加员工帐号，以及按模板批量导入员工帐号。若需短时间分配多个帐号，使用批量导入功能无需单个设置，省时省力。

（1）单个添加

点击【添加】->【添加帐号】，手动添加单个帐号，需定义帐号名称等内容。

填写项	说明
帐号、名称	自定义
手机号、邮箱	填写使用者有效手机号码与邮箱，用于接收验证码
分配部门	设置该帐号所属部门
角色权限	为该帐号分配角色
有效期	设置帐号可用时间，可设长期或指定时间内有效

（2）批量导入

若企业部门与员工数量多，可一次性生成所需数量的帐号，节约运维人员时间，一次操作即可生成指定数量的帐号。

点击【添加】->【批量导入】， 下载模板后根据企业原有组织、角色、帐号信息填写，一次性导入，无需再次设置企业部门、角色，一步到位。

（3）第三方接入

点击【添加】->【批量导入】，选择【第三方接入】，支持从企业微信、飞书直接导入成员，根据企业原有组织架构导入。点击下方链接查看详细接入步骤：

①企业微信接入 ②飞书接入

3.1.2.3 可管理设备

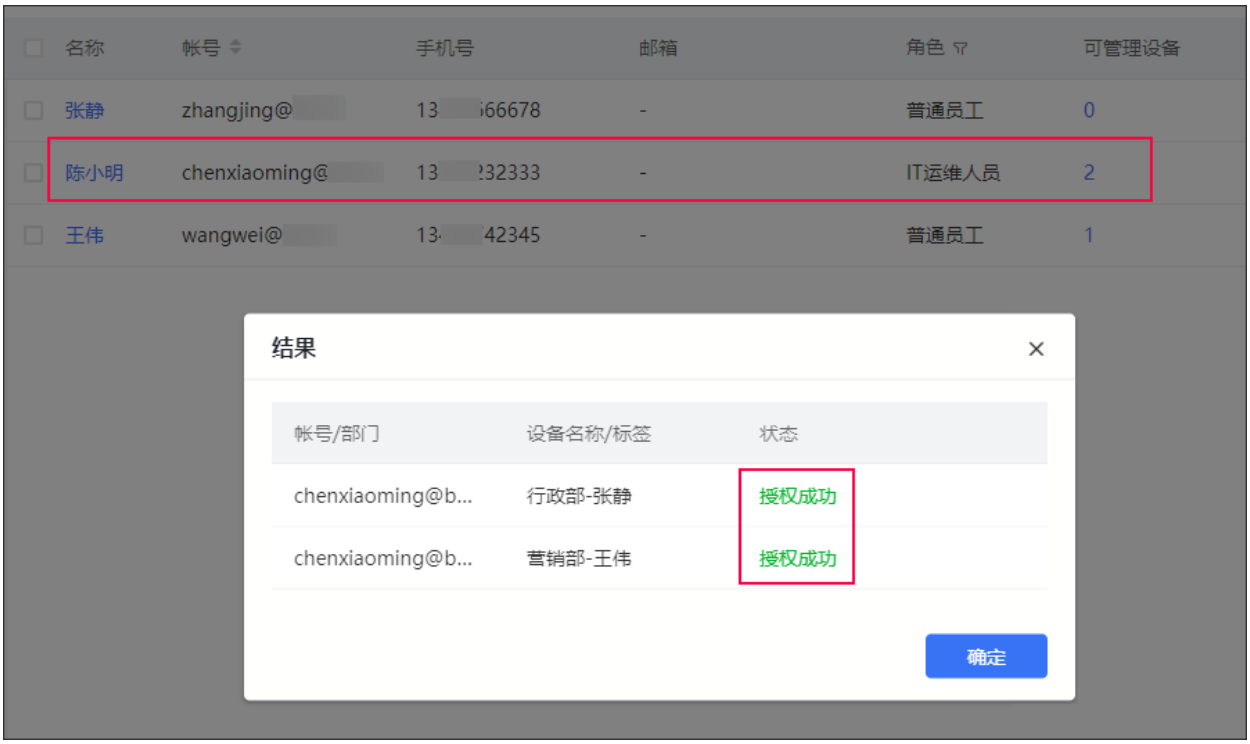
操作路径：管理平台->【帐号体系】->【帐号管理】

IT 运维管理者对不同等级的运维人员的权限和责任进行规范化管理，根据运维人力去分配授权所负责的设备。如：授权 IT 运维人员“陈小明”可管理多台设备。

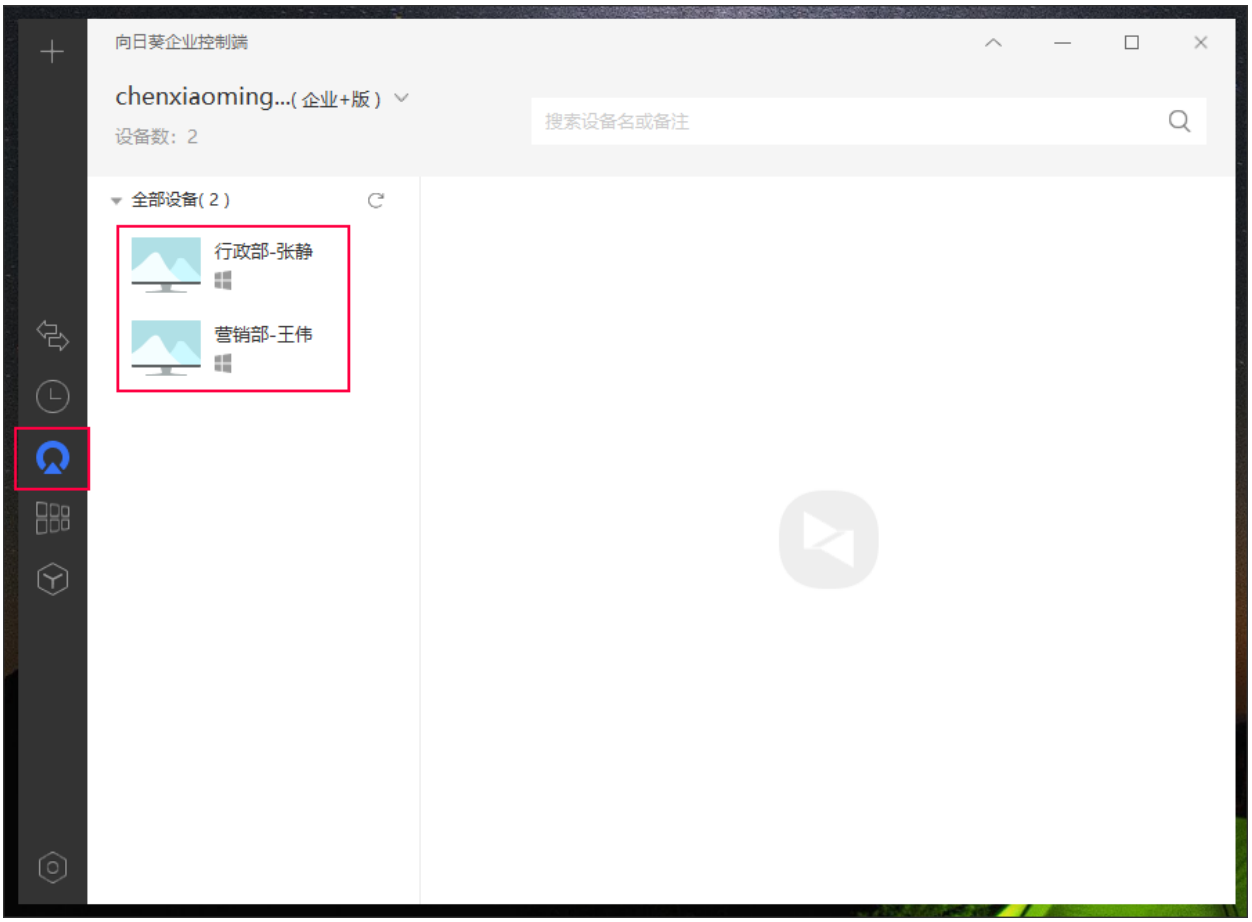
①点击帐号对应的可管理设备

②勾选“营销部-王伟”、“行政部-张静”两台设备，点击确定

③此时页面返回授权操作结果，提示授权成功，资深 IT 运维“陈小明”员工帐号上显示可管理设备数目为 2



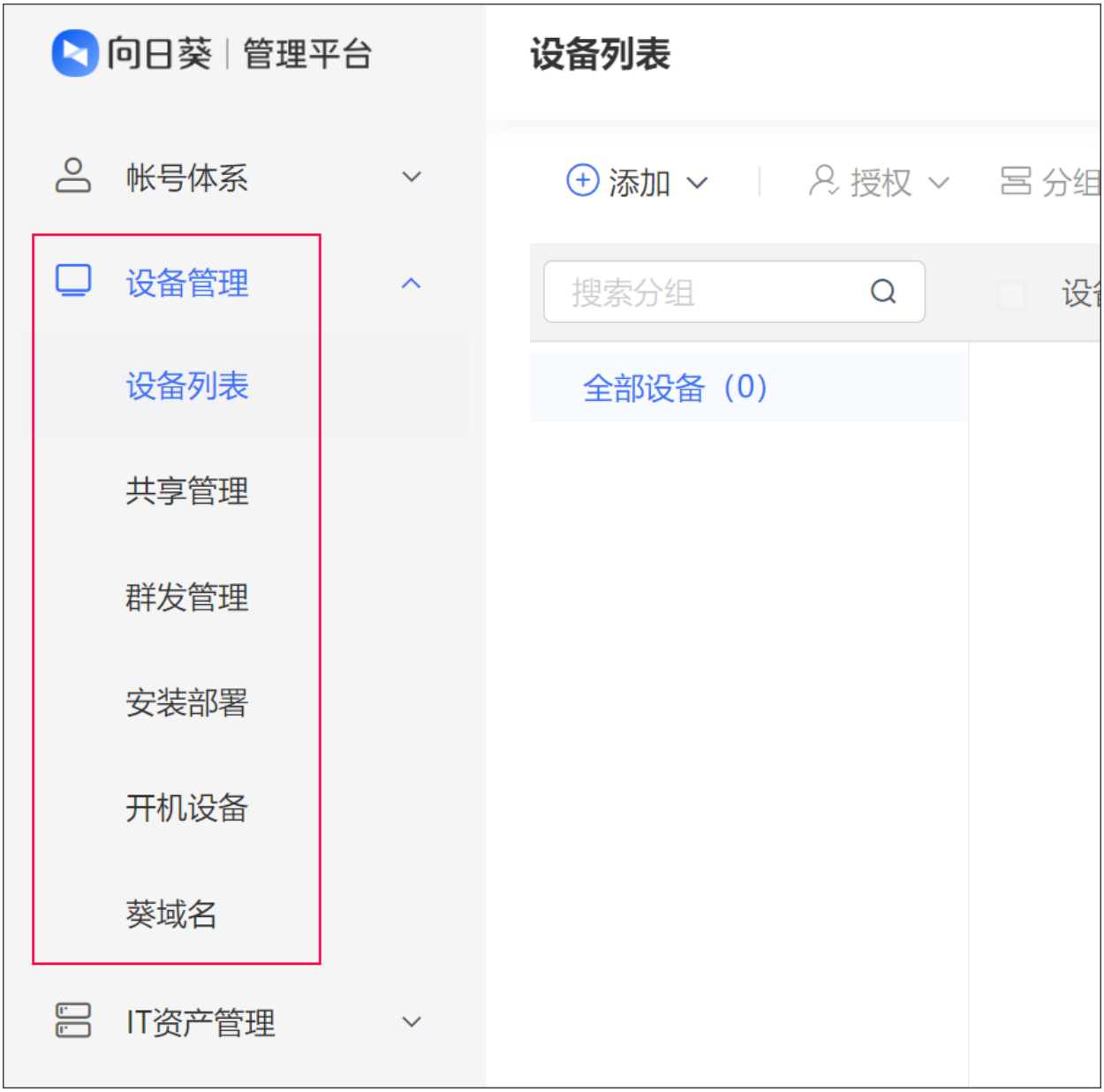
④资深 IT 运维“陈小明”使用其帐号登录向日葵企业控制端，设备列表中显示已授权给他管理的设备。



⑤若授权“资深 IT 运维陈小明”可管理多个分组的设备（如设计部、IT 部和测试部），若分组中每新增一个设备，会自动授权给“资深 IT 运维陈小明”进行管理。无需管理员再次为分组内的设备配置授权，有效减轻管理负担。

3.2 设备管理

企业管理员通过【**设备管理**】实现对帐号下所有的设备进行管理，如查看设备列表、设备的共享管理、群发管理、安装部署和硬件管理。



3.2.1 设备列表

操作路径：管理平台->【设备管理】->【设备列表】

点击左侧导航栏的【设备列表】，可详细查看不同分组下的设备详情信息。

3.2.1.1 列设置

管理员可根据自己所需查看的设备信息，手动选择列表展示的内容。

①页面上方点击“...”

②选择“列设置”，在下拉菜单中选择如：**识别码、系统、分组、版本号、域名访问、绑定的开机设备等**

只有勾选的选项才会在列表中展示，不勾选则不展示。

3.2.1.2 设备分组

设备分组功能是指将具备相同属性的设备归类到一个分组内，例如企业内部以部门划分组别：财务部、销售部、物流部、IT 部等，方便管理者对不同部门的设备进行高效的管理。

在设备列表页面可以查看设备当前的分组情况，如：**分组名称、分组里的设备数量。**

①点击“+添加”添加新分组，在输入框中填写分组名称即可

②在已有的分组后，可以添加子分组、重命名分组名称、移动和删除分组

③每台设备后都会显示其所属的分组

3.2.1.3 设备设置

在设备列表页面，选择需操作的设备，点击“操作”，可以对设备进行更多设置。

（1）设备详情

在“**设备详情**”处可查看客户端设置和详细信息。

①**基本信息**：展示设备当前名称、备注、在线状态和设备分组的信息

②**客户端设置**：查看客户端设置，出于安全方面的考虑，管理员如需通过管理平台更改终端设备的设置，点击变更按钮，需通过**身份验证**以及**安全认证**，才能进行更改设置

③**详细信息**：展示设备的登录时间、IP、AMC 地址、系统版本等信息

（2）设备日志

查询设备近期的日志记录，**可查询的周期取决于服务级别。**

事件包括：桌面控制、远程文件、远程摄像头、CMD。

不同等级服务支持查看的设备日志时效如下表：

服务	入门版	精英版	游戏版	旗舰/行业版	企业+
日志时效	7 天	14 天	30 天	30 天	180 天

（3）共享设备

功能说明：共享设备指将设备 A 从原帐号共享给其他帐号，一台设备可以同时共享给多个帐号，接受共享的帐号在设备列表中也可以管理这台设备。

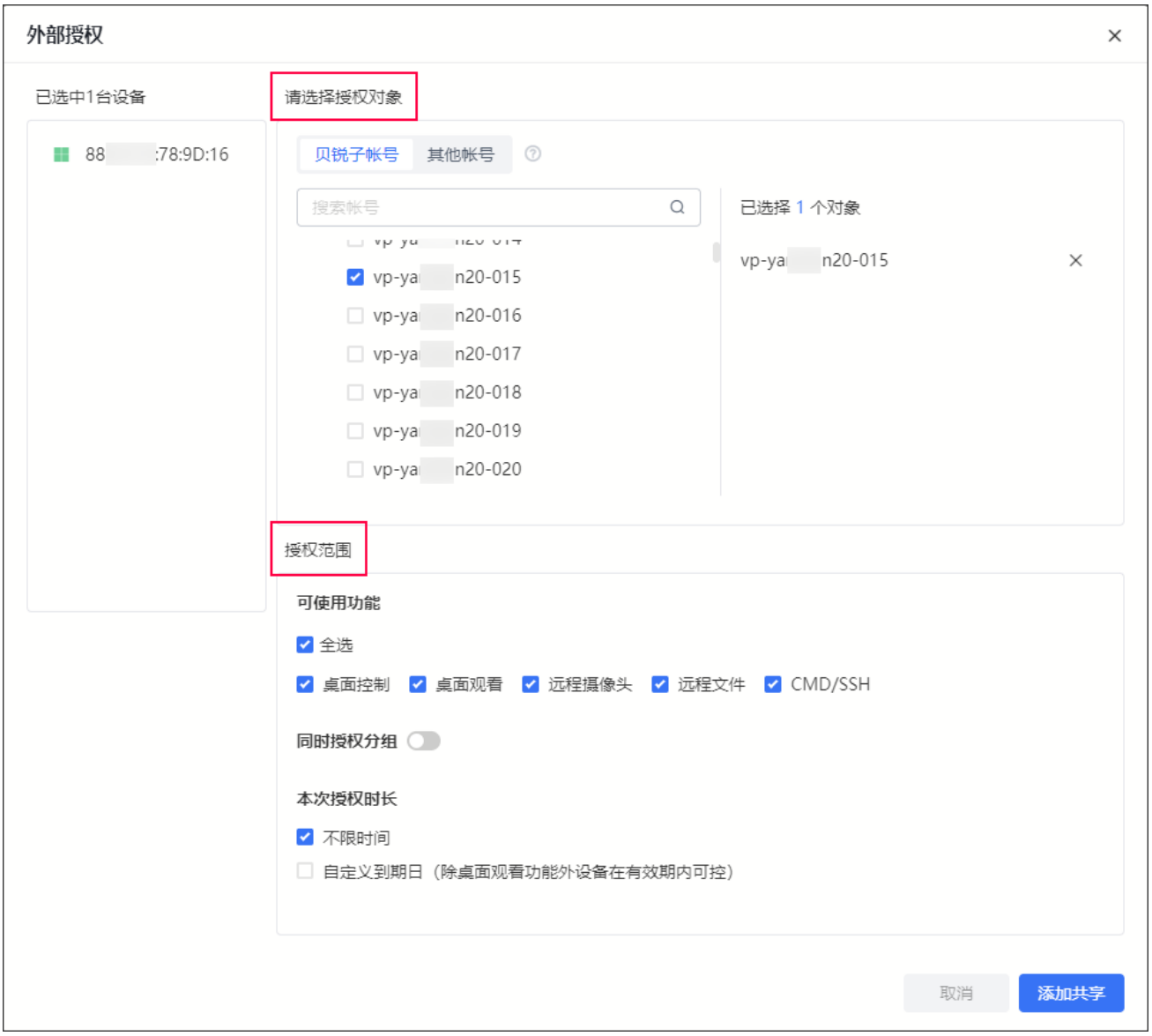
应用场景：可将设备共享给企业外部人员，如果不想为外部人员单独创建企业帐号，可以采用设备共享的方式。如果可以为外部人员创建企业帐号，建议采用设备授权方式，权限管理更灵活和精细。

①当需共享设备给其他帐号时，点击页面的“**共享设备**”**按钮**

②需确定「**授权对象**」和「**授权范围**」

「**授权对象**」：可以是贝锐子帐号，和其他帐号

「**授权范围**」：包括设备共享后的可用功能、是否授权分组、授权时长



③查看已共享的设备及共享详情

设置共享时若定义了共享时长，设备在有效期内可被远控，到期后将自动取消共享，无需管理员手动操作取消。

（4）域名访问

指控制端设备无需安装软件，可通过指定域名访问该设备，同样需经过被控设备的系统账户密码或访问密码验证。

向日葵提供 2 种类型的域名选择：**葵域名（一次付费终身使用）和默认域名（由系统提供免费域名）**。

3.2.1.4 授权管理

授权管理指企业内部给员工授权指定设备进行运维/使用/管理，将设备授权到企业的员工帐号上。可根据员工职能与角色需求进行授权可管理的设备，权限可随时回收，保障信息安全。

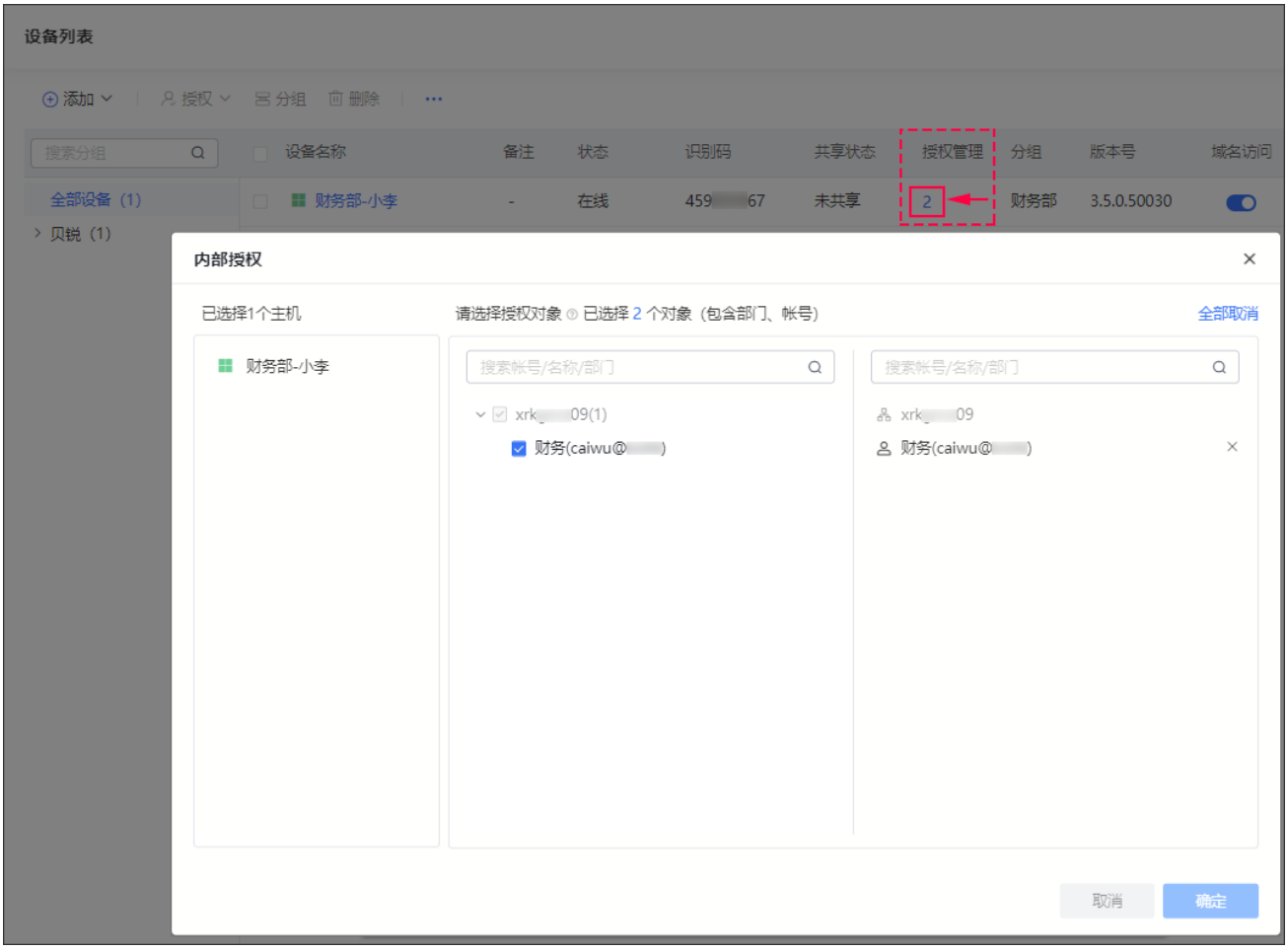
举例：财务小李电脑，仅授权小李的帐号 caiwuxiaoli@****可管理，其他未授权的帐号不可管理此设备。

操作路径：管理平台->【设备管理】-【设备列表】

①在设备列表左侧选中设备，在「**授权管理**」一栏中点击显示的数字

②在弹窗中，为该设备授权可管理的帐号/部门

授权成功后，在设备列表中显示可管理此设备的帐号数，其他未授权的帐号无法管理该设备。如果是以部门为单位进行设备授权，部门新增员工后将自动授权设备给新增员工。



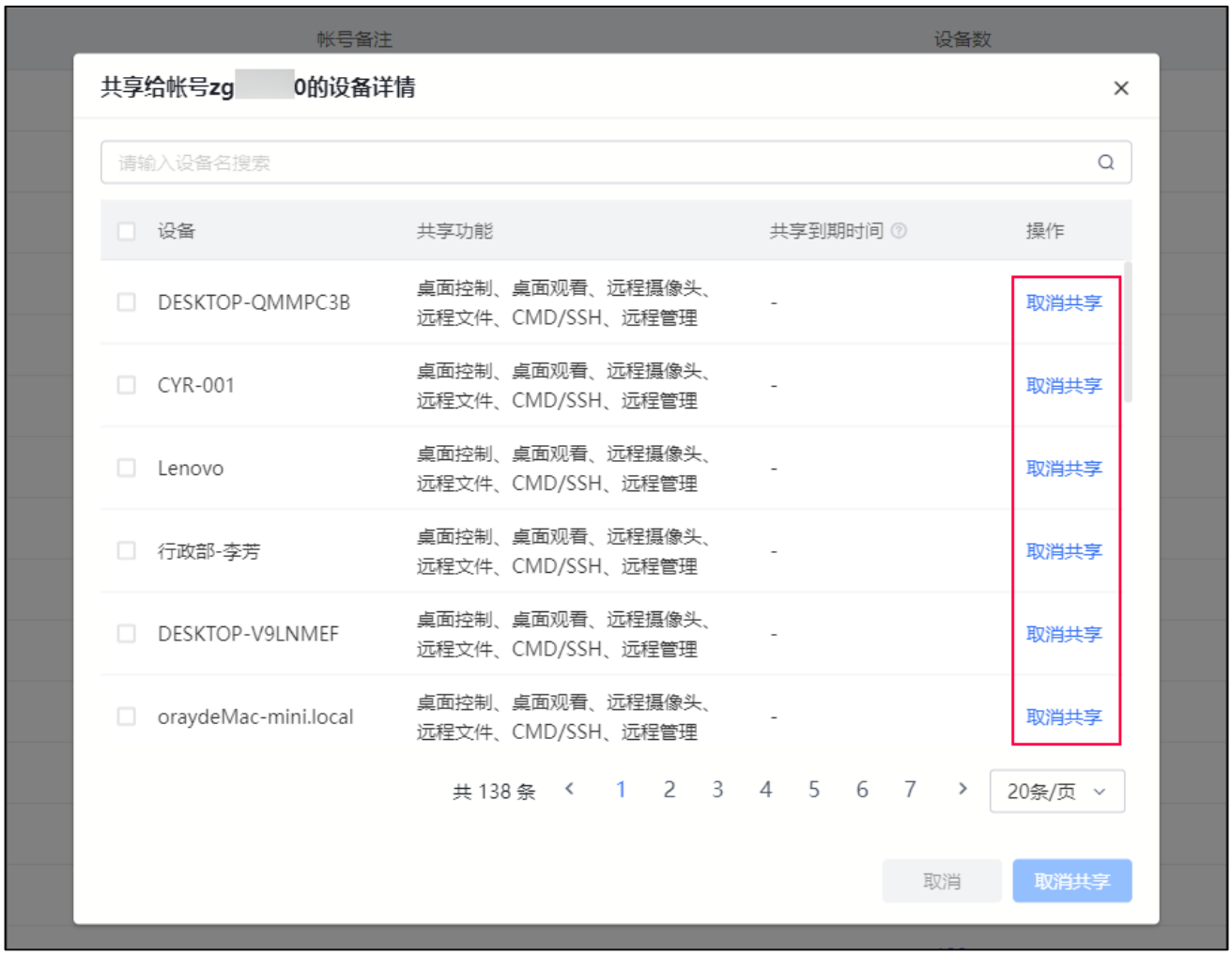
3.2.2 共享管理

操作路径：管理平台->【设备管理】->【共享管理】

在“共享管理”中高效管理已共享的设备：

（1）查看共享概览，列表中显示接收共享的帐号、设备数等信息；

（2）在“共享详情”中可查看对应帐号所接收共享的设备及功能，可随时取消共享。



3.2.3 群发管理

“**群发管理**”有消息群发和文件分发功能，是企业专属的特色功能，作用是定向给企业内多主机群发消息或文件。

3.2.3.1 消息群发

可定时定向给多设备群发消息，支持添加文本和链接地址。企业内有紧急通知、突发状况、故障告警、会议公告等消息，均可在规定时间内将信息传达到指定的员工电脑上。

操作路径：管理平台->【设备管理】->【群发管理】

（1）选择“**消息群发**”，点击页面的“**+添加**”按钮；

（2）在页面弹窗中配置群发消息的内容和接收对象，如：

①**标题**：自定义群发的消息标题

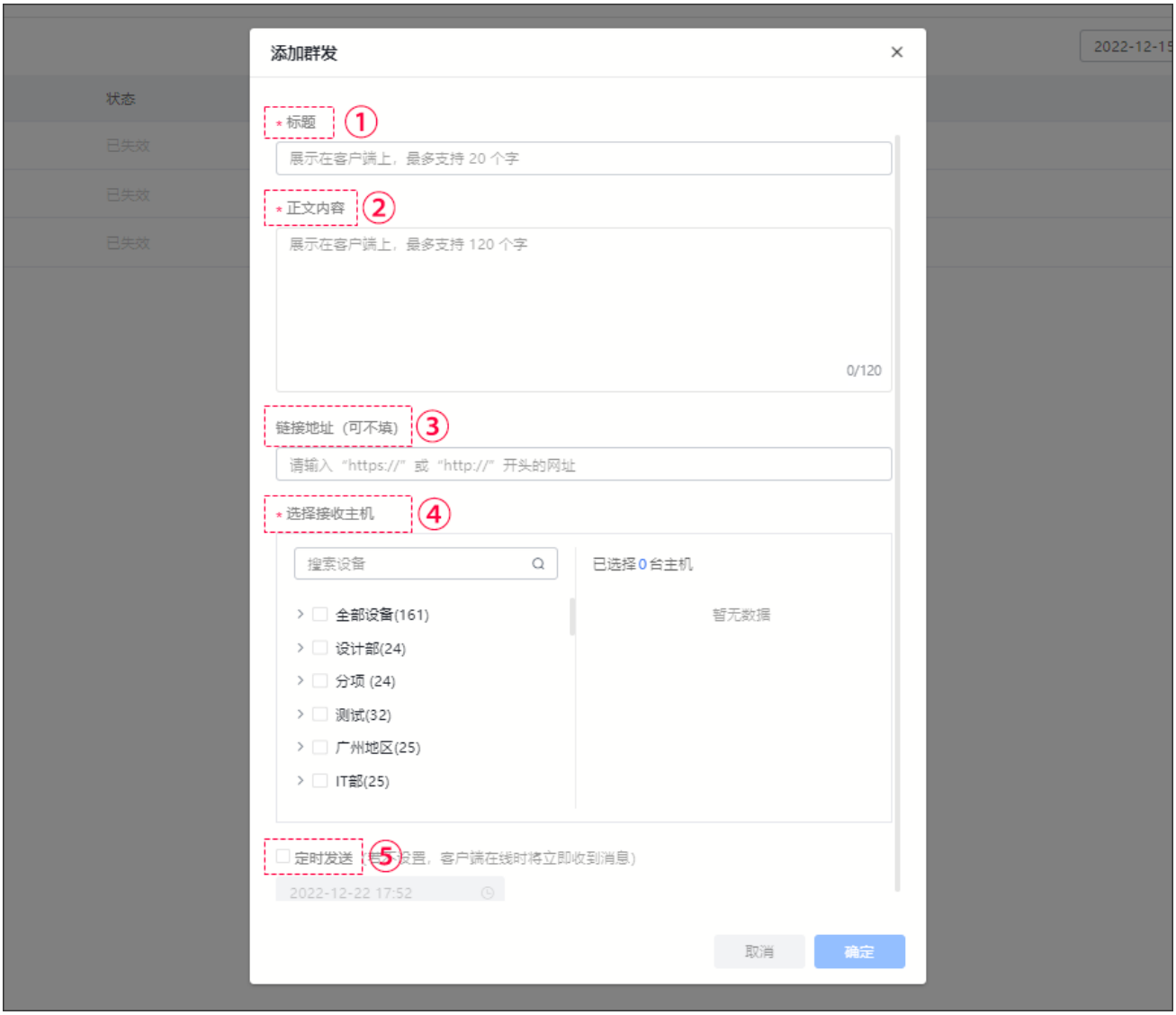
②**正文内容**：填写群发消息的详细内容

③**链接地址**：支持附带 http://或 https://开头的网址，非必填

④**选择接受主机**：选择接收群发消息的设备对象

⑤**是否定时发送**：可以设置消息在指定的时间发送到设备，不设置默认客户端在线时立即收到消息

以上配置完成后点击“**确定**”。



（3）在消息群发列表中，可以看到管理员已创建的消息群发任务，点击“**详情**”可查看消息群发的概况和发送进度，也可以删除群发消息任务；

（4）系统将群发消息任务按照配置发送到指定设备，客户端只要在线即可接收消息。如客户端未在线，需尽快通知客户端尽快上线接收。（群发消息任务在 24 小时内有效，超过时限客户端未上线无法再接收消息）

注意：群发消息的接收当前仅支持 Windows 和 Linux 平台的企业版客户端。

3.2.3.2 文件分发

可用于企业管理者向员工电脑发送指定文件，文件可设置定时定向发送，多主机文件传输可限流量，可新建、删除文件分发，和查看以往的分发记录。

操作路径：管理平台->【设备管理】->【群发管理】

（1）选择“文件分发”，点击页面的“+添加”按钮；

（2）在弹窗页面中配置文件分发的内容：

①选择分发文件：支持选择/拖拽文件，限额 1G

②填写分发任务名称：设置分发任务的名称

③选择接收的主机：选择接收文件的设备对象

④填写文件保存路径：设置分发的文件保存路径，若为空则为默认保存路径

⑤是否覆盖相同文件名的文件：勾选即覆盖文件名相同的原文件，不勾选则不覆盖

⑥设置客户端下载时段：设置客户端在指定的时间下载分发的文件，若不设置则客户端在线时立即下载

⑦下载速度：限制企业版客户端下载分发的文件的速度，最大支持限制 500KB/S，不勾选则不限速

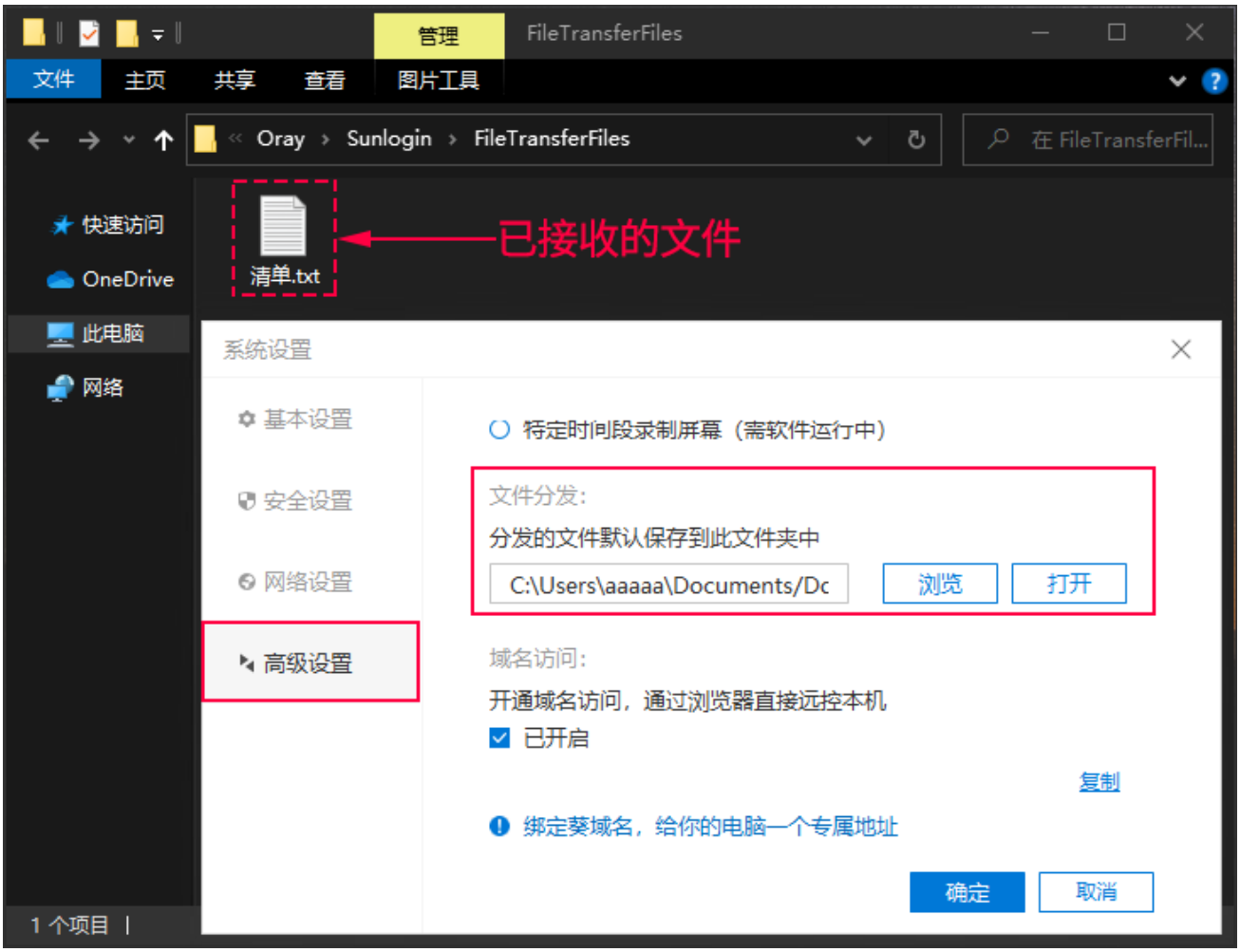
⑧**是否下载后自动执行：**勾选后，客户端主机下载分发的文件后自动执行，不勾选则不执行

（3）以上配置内容填写完成后，点击“**确定**”，文件会上传到向日葵服务器；

（4）文件成功上传到向日葵服务器后，新建分发文件任务成功。分发任务的有效期为 7 天，需要在有效期内通知客户端设备上线接收文件；

（5）在文件分发列表中，可以看到已创建的文件分发任务，可查看具体“详情”和“删除”文件分发任务；

（6）系统将文件按照配置要求发送到指定的客户端设备上。



文件保存路径注意事项：

①若不填，Windows 客户端默认是安装目录的 SunloginClient\SunloginFiles；Linux 客户端默认是\home\xxx\Documents\Oray\Sunlogin\FileTransferFiles

②请确保输入的盘符在客户端设备是存在的，否则将导致分发失败

③同时分发给 Windows、Linux 客户端时，请使用默认路径，否则将导致分发失败

3.2.4 安装部署

安装部署是向日葵企业服务级别的特色功能，提供两种定制安装包的方式，分别是批量部署和定制软件，适应不同场景需求的企业用户使用。

3.2.4.1 批量部署

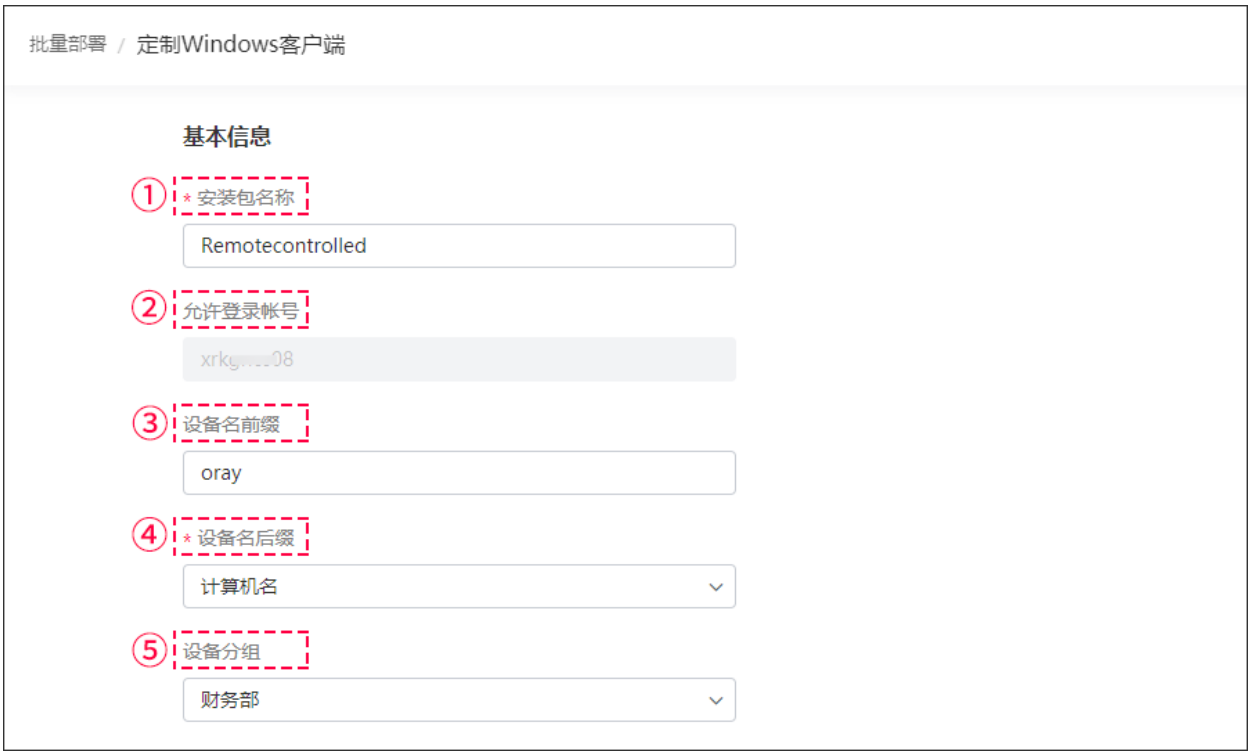
适用于大型企业（拥有大量电脑设备）以及连锁门店（如超市、酒店、服装店）等行业，预先配置向日葵客户端安装包的属性、访问密码等，被控设备下载安装自带配置信息的向日葵客户端安装包并自动绑定到帐号，控制端即可对远端设备发起远程控制，达到快速大批量部署的目的，免去逐台电脑配置的麻烦。

操作路径：管理平台->【设备管理】->【安装部署】->【批量部署】

（1）点击【添加安装包】；

（2）配置安装包的基本属性；

序号	定制项	说明
①	安装包名称	此名称为下载定制包时显示的程序名称，定制包名称必须为英文或数字组合
②	允许登录的帐号	默认是当前登录管理平台的帐号，不支持更改其他帐号
③	设备名前缀	定义设备安装客户端后设备名的前缀，如“vp”，则在设备名前统一加前缀 vp，不填则无前缀
④	设备名后缀	从选项框中选择设备名后缀的规则，方便管理员大批量部署安装包时区分设备
⑤	设备分组	安装软件包的设备将会默认加入指定分组，便于大批量部署后管理员进行设备分类



（3）针对定制客户端安装包的基础设置和安全设置，提供 5 种设置模版让您快速完成主机权限的设置；

序号	定制项	说明
①	通用版	常规设置，适用私密度较低的主机
②	无痕运行版	设备可通过 CMD 静默安装，安装后，不显示桌面快捷方式、托盘图标、气泡消息、卸载入口
③	增强安全版	适合中等私密的主机，设备被远程后会锁定向日葵客户端，每次远控后会更新主机验证码
④	最高安全版	适合高私密的主机，禁止对设备传输文件、复制文字等，每次远控后会更新设备验证码
⑤	自定义权限版	自行根据实际情况定义设备的基础设置和安全设置，比如：行政部员工使用向日葵远程办公过程中，禁止使用远程传输文件功能，避免公司内部敏感重要数据外泄

注：如果需要定制软件 VI 信息（比如自定义软件的皮肤颜色、软件名称、logo 和功能等），

请使用【**定制软件**】功能。

（4）设置授权设备，将此安装包生成的设备授权给其他帐号管理，授权后，其他帐号在设备列表会显示该设备并可对其操作。支持授权当前帐号及企业内其他帐号、指定帐号；不开启授权设备，则主机不会授权到其他帐号；

注：批量部署包定制完成后不支持改动，如要修改其中的配置项需重新定制安装包。

（5）填写完成后，需等待约 2 分钟生成安装包；

（6）创建好的安装包，在批量部署列表右侧点击“**下载**”。提供两种方式下载，任选一种方式将安装包下载到 Windows 电脑安装即可；

①可复制下载链接发送到给员工自行安装

②直接下载安装包到本地，将安装包发送给员工自行安装

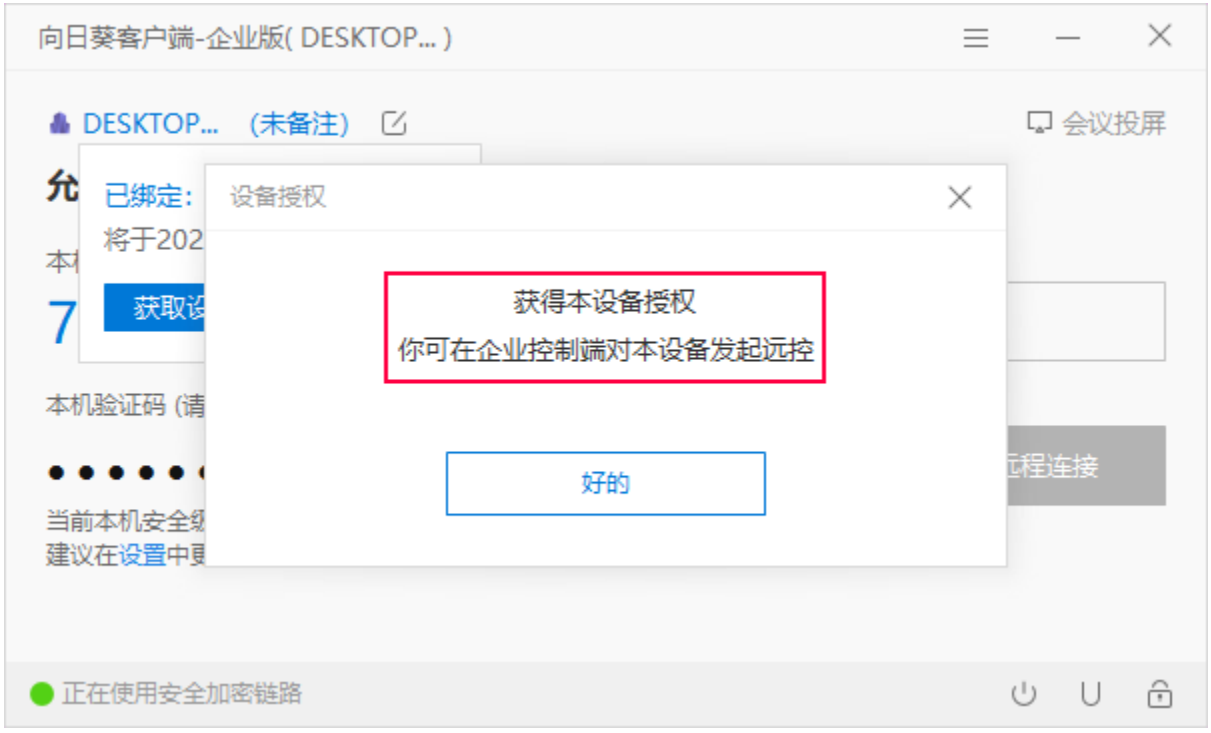
（7）在需被控的设备上安装企业专属的向日葵定制包后，软件自动绑定到帐号，无需手动登录；

（8）定制包安装后，员工可以登录自己的企业帐号，以认领此设备，认领即完成设备授权管理的操作；

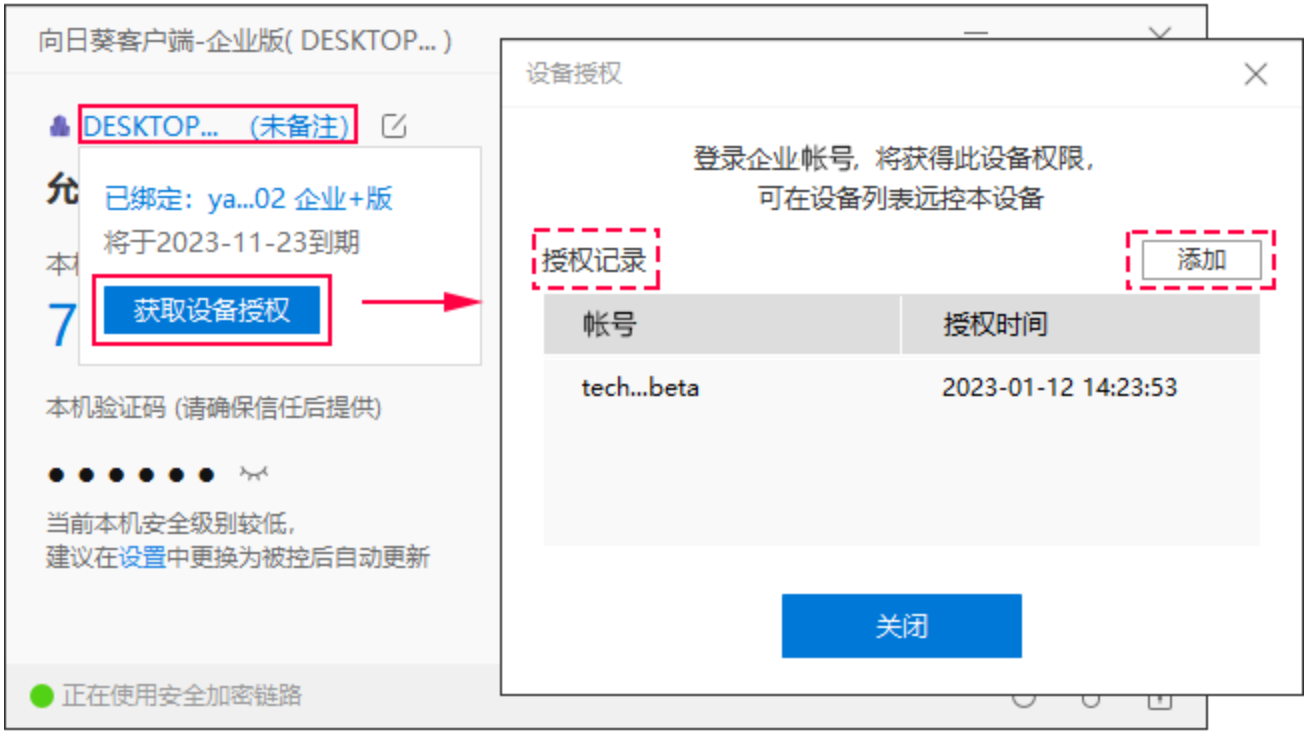
①把鼠标移动到客户端左上角显示的设备名称，点击**「获取设备授权」**

②在弹出的登录窗口，登录员工自己的企业帐号

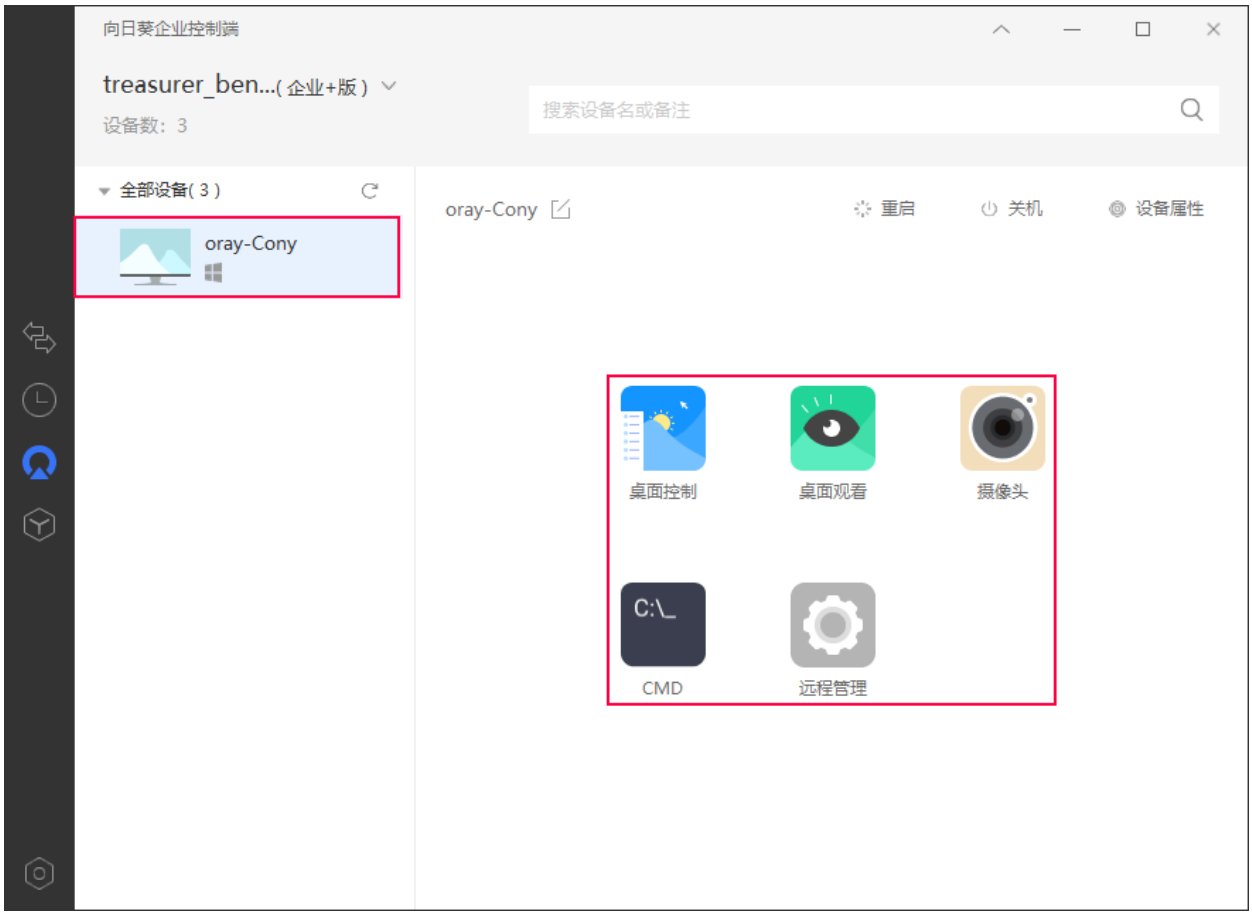
（9）员工的企业帐号登录完成后，即可获得此设备的授权。员工在企业控制端的设备列表中可对此设备发起远程控制；



（10）当设备已被员工认领后，把鼠标移动到客户端左上角显示的设备名称，点击「**获取设备授权**」，可查看当前设备的授权记录，也可以继续添加授权。



(8) 以定制财务部人员禁止使用文件传输功能的安装包为例，财务人员登录控制端软件，在【**设备列表**】选择对应设备，远控功能列表中无“远程文件”功能。



3.2.4.2 软件定制

指定制专属于企业品牌或具有企业风格的远程控制软件，可自定义软件的皮肤颜色、软件名称、logo、功能等，个性化程度高，可提升企业形象和员工归属感。支持定制以下平台的软件包：Windows 客户端、Windows 控制端、Android 客户端、Android 控制端和 Linux 客户端。（点击了解更多软件定制）

以 Windows 客户端为例演示软件定制的操作步骤：

操作路径：管理平台->【设备管理】->【安装部署】->【定制软件】

选择“Windows 客户端”，点击“立即定制”。

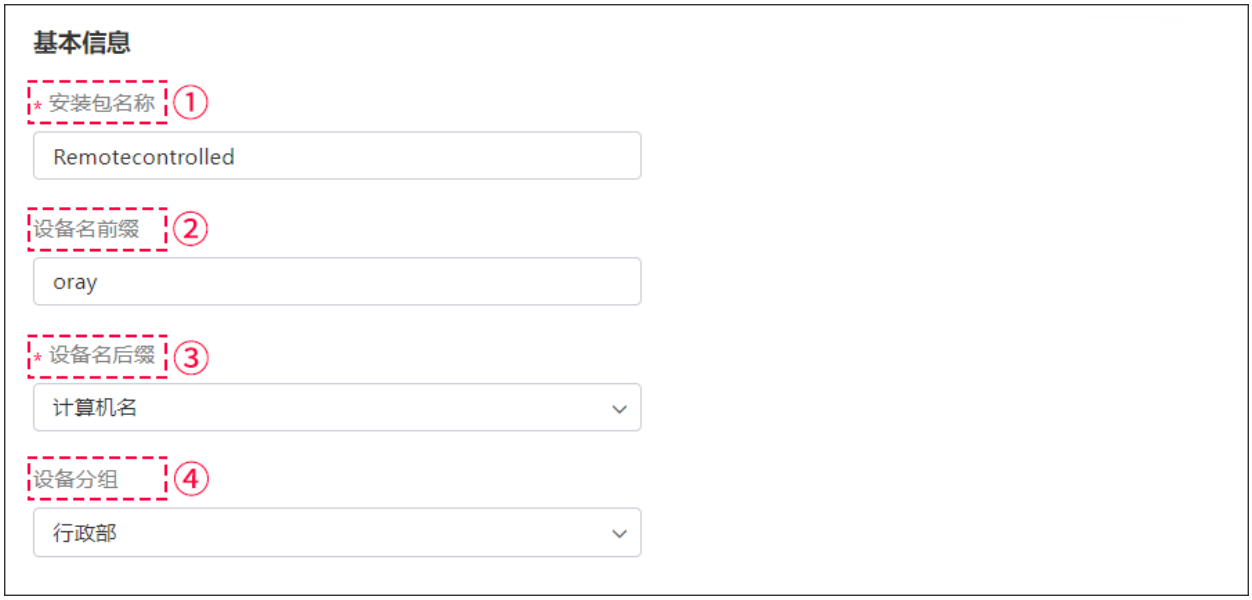
软件定制示意图如下：


皮肤设置
软件名称
远程被控
GZ-1170...(Oray-02)
会议投屏
已绑定：or...12 独立服务器
将于2022-01-30到期
升级 & 续费
允许控制本机
本机识别码
123 456 789
本机验证码
远程协助
输入伙伴识别码
输入伙伴验证码
可为空
远程连接
连接服务器成功
界面显示功能
Logo标识
远程控制
Ver.3.5.0.50030
www.xxx.com
Copyright(©)2009-2022 Oray. All Rights Researved
网站地址

根据页面要求，定义 Windows 客户端安装包的属性：

（1）基本信息

序号	定制项	说明
①	安装包名称	自定义安装包名称，此名称为下载安装包时显示的程序名称，安装包名称必须为英文或数字组合
②	设备名前缀	在设备名前加统一前缀（可不填）
③	设备名后缀	方便管理员大批量部署定制包时区分主机，后缀须在下拉列表中选其一
④	设备分组	为定制包设定所属的分组，安装定制包的设备将会默认加入指定分组，便于大批量部署后管理员进行设备分类



（2）外观信息

序号	定制项	说明
①	软件名称（中/英文）	设置 Windows 定制客户端的中/英文名称，可根据企业名称或软件用途等对定制包命名
②	皮肤设置	选择定制包皮肤主题颜色，可根据企业文化、风格或行业属性设定
③	网站地址	填写后，将在软件“关于”信息中查看企业网站地址，支持点击跳转至企业网站
④	logo 标识	支持自定义企业 logo，需按照页面要求上传指定尺寸和文件格式的 logo 图标，未上传的 logo 将使用通用 logo 代替）。员工在使用定

		制软件时，时刻能看到企业的 logo，可以树立品牌形象和提高员工的归属感。查看如何为定制安装包制作 ICO 图标
⑤	**界面显示功能**	①选择自定义功能：可根据使用者的权限、级别、用途灵活勾选定制包界面显示的功能，不勾选的功能则不在客户端显示；②绿色方案：预设客户端界面只显示远程协助功能，其他功能不显示

（3）设备权限设置

提供 5 种类型可选：

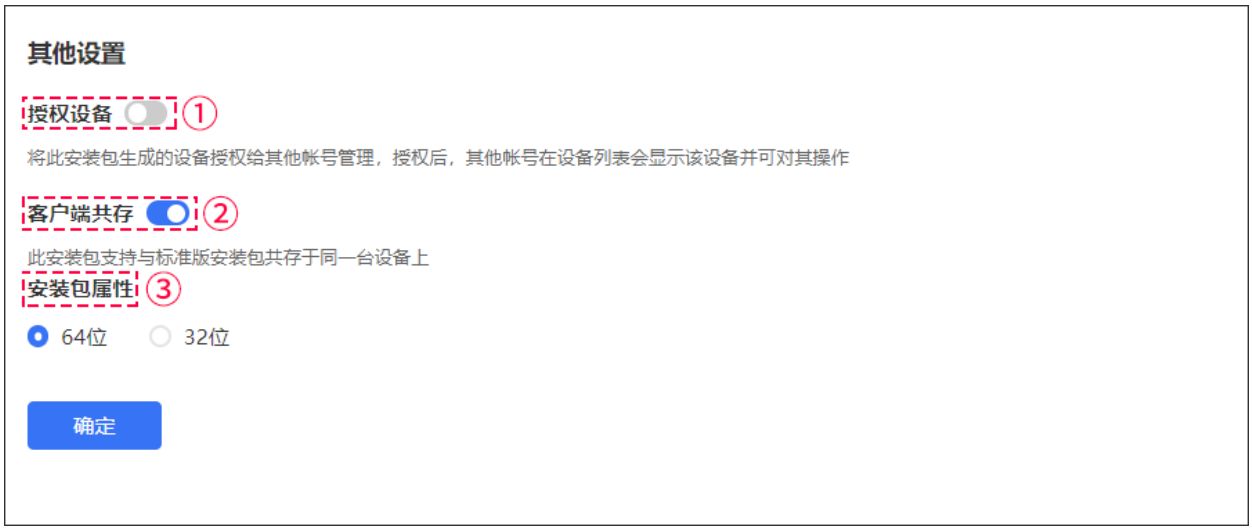
通用版、无痕运行版、增强安全版、最高安全版、自定义

企业根据实际情况设置主机的功能和权限，比如大型企业中根据部门、职位级别来划分设备支持的操作功能和权限。

（4）其他设置

序号	定制项	说明
①	**授权设备**	设置授权设备，将此安装包生成得设备授权给其他帐号管理，授权后，其他帐号在设备列表会显示该设备并可对其操作。支持授权当前帐号及企业内其他帐号、指定帐号；不开启授权设备，则主机不会授权到其他帐号
②	**客户端共存**	此安装包支持与标准版安装包共存于同一台设备上

③	**安装包属性**	安装包支持的系统位数



（5）下载

创建好的定制安装包，在批量列表右侧点击“**下载**”。提供 2 种方式下载，任选一种方式将安装包下载到 Windows 电脑安装即可。

①可复制下载链接发送到给员工自行安装

②直接下载安装包到本地

3.2.5 开机设备

【开机设备】当前支持管理开机设备：**开机棒、开机插座和开机插线板。**

3.2.5.1 开机棒

向日葵开机棒是用于远程开机的智能硬件，接入路由器后，配合向日葵远程控制软件，可以通过手机、平板、Windows 等设备，随时随地远程开启远端电脑主机。

（1）添加开机棒

需要先将已购买的向日葵开机棒添加到帐号下，并绑定指定设备，才可以实现远程开机。

①在【开机设备】中点击“**添加开机棒**”

②在页面弹窗中输入**开机棒的 SN 码和名称，点击“确定”**

③开机棒成功添加到帐号下，点击“**详情**”对开机棒进行管理

（2）设备详情

查看开机棒的在线状态，SN 码、MAC 地址、服务类型（独享版 or 局域网版），还可以对开机棒进行转赠和删除操作。

独享版：可绑定局域网内 1 台主机并实现远程开机

局域网版：自动扫描局域网内所有主机并绑定后即可开机

①**转赠开机棒**：可以将开机棒从 A 帐号转赠到 B 帐号，转赠后无法收回开机棒，**请谨慎确认转赠操作和接受者帐号**

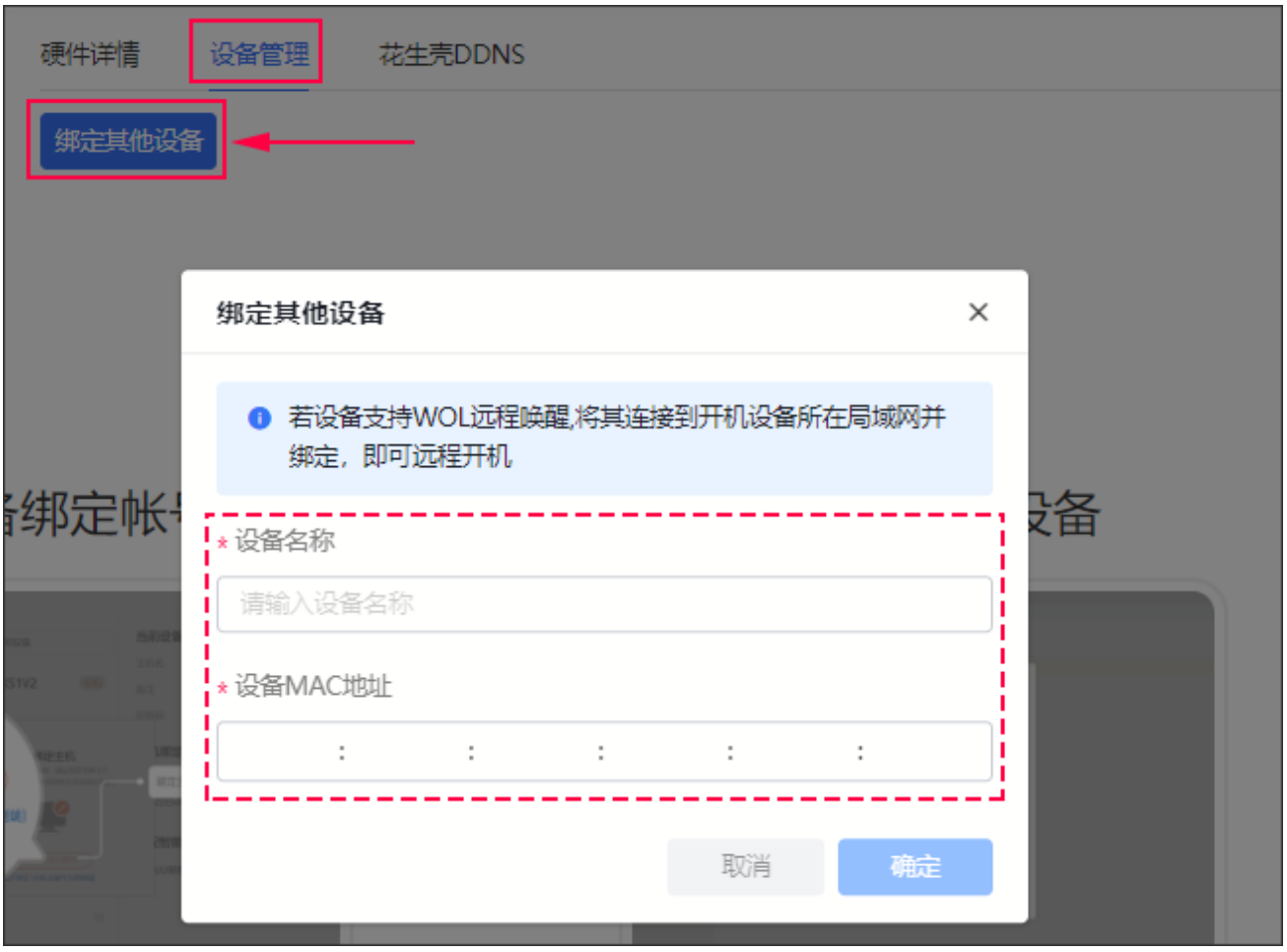
②**删除开机棒**：删除后，该开机棒原有的数据将会被清空且取消设备远程功能，开机棒可重新绑定任意帐号

（3）设备管理

①**独享版**：若开机棒版本为独享版，需要手动绑定局域网内 1 台主机

②**局域网版**：局域网版开机棒会自动扫描同物理局域网内已绑定相同帐号的主机

③**绑定其他设备**：如需开启网络内其他帐号下的设备、NAS、其他支持 WOL 唤醒的设备，点击“**绑定其他设备**”，需输入设备 MAC 地址与名称将设备绑定到帐号下



（4）花生壳 DDNS

向日葵开机棒内置花生壳 DDNS 功能，开机棒在线且当前网络具备真实的动态的公网 IP 前提下。启用该功能，帐号下的域名会自动解析到当前网络的公网 IP 地址，可用作发布网站服务的用途，支持“**本帐号登录**”和“**其他帐号登录**”。

①**本帐号登录**：默认为当前登录向日葵管理平台的帐号登录

②**其他帐号登录**：手动输入其他已注册了的贝锐帐号密码登录

3.2.5.2 智能插座

向日葵智能开机插座是一款可以实现远程开关机的插座，对电脑主板的适配更广泛，主板支持并开启 AC Recovery 即可。配合向日葵客户端，实现先关机再断电，还具有定时关机、倒计时关机、断电记忆等功能。

开机智能插座需要通过向日葵控制端软件（手机 APP 或 PC 端）添加后，才能在向日葵管理平台对设备进行管理。

（1）硬件详情

可查看开机插座的名称、版本、详细信息（包括状态开启/关闭、设备 SN 码、MAC 地址、固件版本和插座版本），点击下方的“**删除插座**”，可将插座从帐号下删除。

（2）设备管理

设备管理页面是引导用户从主机绑定帐号、设备绑定主机、到实现远程开机的流程，目前设备绑定主机的操作仅能通过向日葵手机控制端 APP 进行。

（3）使用日志

查看当前开机设备近期的使用记录日志。

3.2.5.3 智能插线板

向日葵智能插线板具有独立可控制的电源插口，可以分别设置开启/关闭状态，能更轻松管理多台主机设备。智能插线板支持断电记忆、指示灯开启/关闭、电量统计等功能，更好地契合学习工作中的使用需求。

智能插线板需要通过向日葵控制端软件（手机 APP 或 PC 端）添加后，才能在向日葵管理平台对设备进行管理。

（1）硬件详情

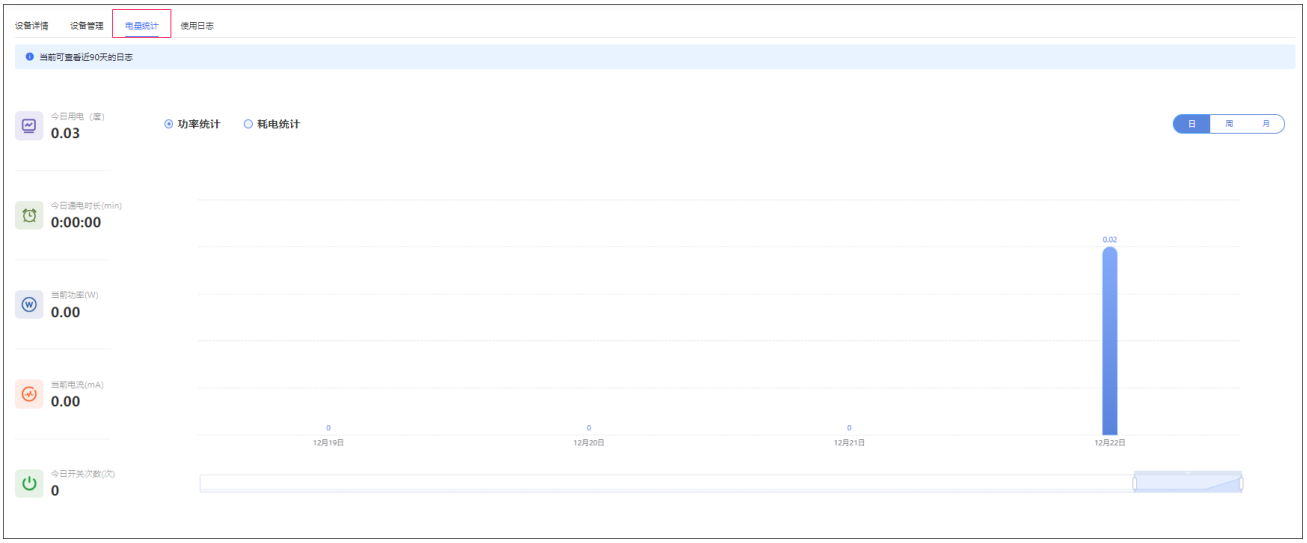
硬件详情中展示了插线板的名称、型号、在线状态，各插孔的开关情况还有详细信息（包括状态开启 or 关闭、当前功率、设备的 SN 码、MAC 地址、固件版本和插座版本）。下方的“**删除插线板**”按钮可将插线板从帐号中删除。

（2）设备管理

设备管理页面是引导用户从主机绑定帐号、设备绑定主机、到实现远程开机的流程，目前设备绑定主机的操作仅能通过向日葵手机控制端 APP 进行。

（3）电量统计

通过向日葵管理平台监控电脑每日、每周、每月用电，数值化呈现用电时长，有了它，更清晰了解电脑的用电情况。



（4）使用日志

展示插线板每个插孔近 30 天的开关日志信息。

3.3 IT 资产管理

向日葵 IT 资产管理可以为企业提供 IT 设备的管理功能，记录硬件信息和监测硬件变更记录，帮助企业了解系统资产的全景状况，全方位掌控企业资产。

“IT 资产管理”是向日葵**企业+版服务**享有的功能，企业员工电脑需安装登录最新版**向日葵企业版客户端**（或定制客户端），由向日葵企业版客户端获取员工主机硬件信息并自动上报到向日葵管理平台，企业 IT 管理人员通过向日葵管理平台对企业内所有的 IT 资产进行管理，如查看帐号下主机的硬件信息、硬件变更记录和导出资产数据。有效改善原有的 IT 管理业务流程，节省 IT 成本，并保证资产数据的一致性。

（1）在员工电脑安装最新版向日葵企业版客户端 3.2.1 及以上版本。

（2）安装成功，点击“**绑定帐号**”，自行选择方式登录。

（3）企业 IT 管理人员登录向日葵管理平台，并输入相同的向日葵企业+版帐号登录。

3.3.1 硬件信息

操作路径： 管理平台->【IT 资产管理】->【硬件信息】

3.3.1.1 硬件信息

（1）在“硬件信息”中，展示从向日葵企业版客户端上报的设备资产信息，资产信息包括：设备名称、所属帐号、分组、MAC 地址、IP 地址、系统版本、处理器、主板、内存等信息。清楚记录具体资产的所属分组、资产数量、使用者等，IT 管理人员及时掌控 IT 资产的使用状况，易于盘点和监控。

（2）可以手动设置硬件资产所展示的信息，点击页面的“列表展示”按钮，在下拉列表中勾选所需展示的信息，勾选即展示，不勾选不展示。

若发现硬件信息缺失，请尝试将企业版客户端升级到最新版本。

（3）支持资产报表一键导出，减负日常盘点。在页面下方点击“**导出资产数据**”，可选“导出全部”、“导出当前页”、“导出选择项”的硬件信息数据。

3.3.1.2 硬件变更记录

由于人员的流动、设备的更新换代，IT 资产会存在变更的情况。“**硬件变更记录**”全面记录企业的硬件资产信息，变更记录及时通知，避免防止员工私自更换配件，导致企业资产流失。

（1）点击“**硬件变更记录**”，可以查看员工的设备在近 180 天内具体的硬件变更记录详情，从左侧的分组中可以清晰地看出什么部门的设备变动最多，变更记录详情中包括：变更时间、变更设备名称、变更硬件（包括：显示器、硬盘、网卡、显卡、内存、主板、CPU）、原配置、新配置、MAC 地址、IP 地址、所属帐号、分组。

若发现硬件信息缺失，请尝试将客户端升级到最新版本。

（2）在页面下方点击“导出”，可选“导出全部”、“导出当前页”、“导出选择项”的硬件变更记录数据。

3.4 审计日志

企业用户通常会拥有大量主机，企业终端设备众多，在远程桌面、远程运维等功能的使用需求也是日益剧增，随之而来的是安全风险问题的增加。

审计日志中记录着远控日志/控制端日志/被控端日志等运维类型的日志，用于企业管理员查询和追踪各项操作记录。

不同等级服务支持查看的远控日志、被控日志、控制端日志、客户端日志时效如下表：

服务	入门版	精英版	游戏版	旗舰/行业版	企业+
日志时效	7 天	14 天	30 天	30 天	180 天

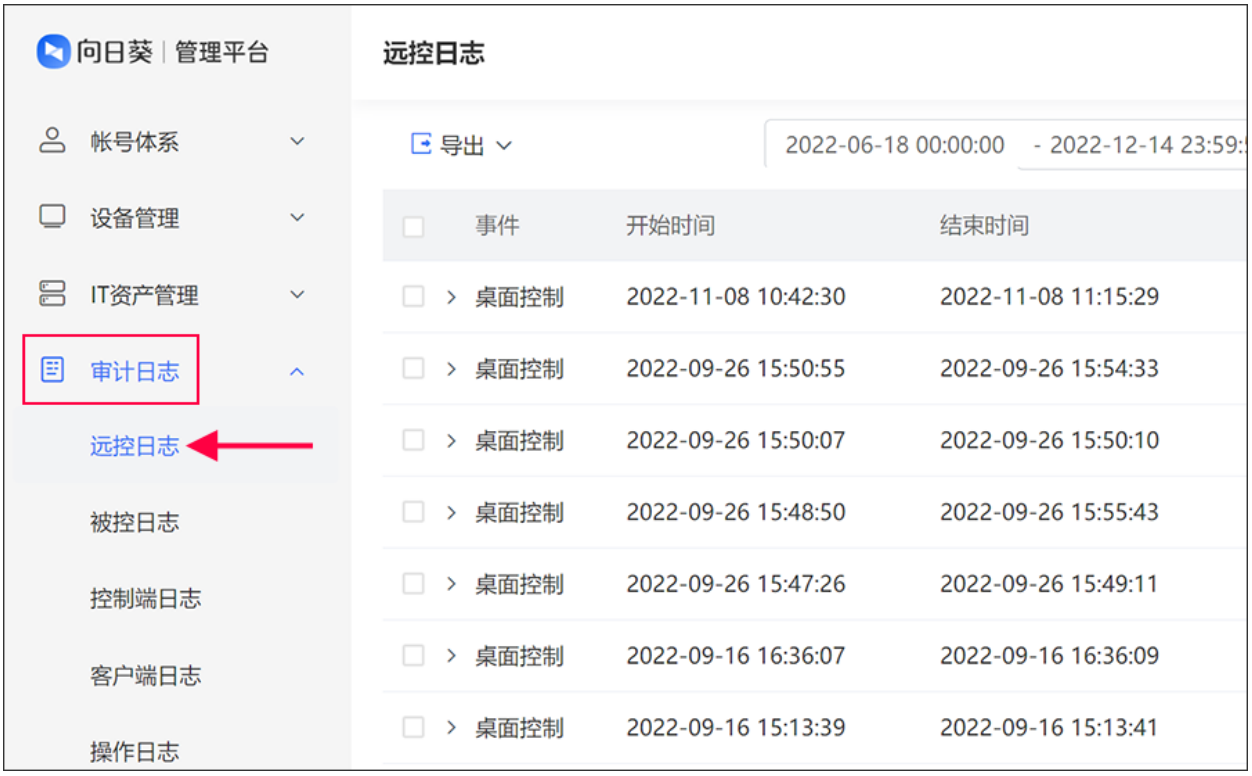
3.4.1 远控日志

操作路径：管理平台->【审计日志】->【远控日志】

（1）功能说明

【远控日志】功能，准确记录每项操作行为，企业管理者可全面掌控企业内部设备远控情况。支持查询/导出近 180 天内详细的远控日志记录，包括通过**设备列表**和**识别码方式**的远控，当发生安全问题或异常情况时通过远控日志排查。

远控“**事件**”类型包含：桌面控制（桌面控制+桌面观看）、远程文件、远程 CMD、远程摄像头。



（2）补充说明

①**旧帐号体系**：记录的是当前帐号远控设备的详细记录

②**新帐号体系**：记录当前帐号和帐号管理中的员工帐号远控设备的详细记录；且用员工帐号远控时，控制端帐号会记录为员工帐号的信息，而非超管帐号

（3）版本要求

若您发现管理平台未记录对应日志信息，请检查所使用的控制端版本是否符合要求：

①Android 控制端 V12.0

②iOS 控制端 V12.0

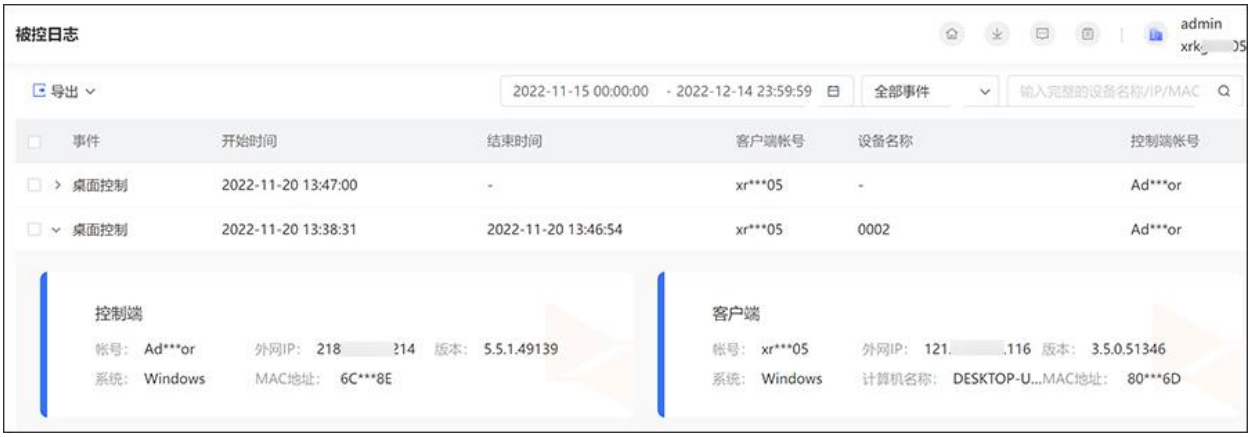
③Windows 企业控制端 V5.6.1 及以上版本

3.4.2 被控日志

操作路径：管理平台->【审计日志】->【被控日志】

记录本帐号下设备的被控记录，包括通过设备列表和识别码方式远控。

被控事件指：桌面控制（桌面控制+桌面观看）、远程文件、远程 CMD、远程摄像头。



3.4.3 控制端日志

控制端日志包括最近登录记录和登录告警记录。

操作路径：管理平台->【审计日志】->【控制端日志】

3.4.3.1 最近登录记录

“最近登录记录”可查看近 30 天内控制端的登录记录，内容包括控制端的登录时间、设备名称、控制端的帐号名、登录地的 IP 地址及登录应用等。

管理员可以通过查询帐号的登录时间、登录地点和登录平台，以此判断帐号是否存在安全问题。

【注意】当前仅支持查看 Windows 企业版控制端 5.4.1 及以上版本的登录记录，若您在查询时发现日志缺失，请尝试将控制端升级到最新版本。

3.4.3.2 登录告警记录

系统检测到控制端登录异常（异地登录）时，会触发登录告警。若非本人已知情况的登录操作，建议修改帐号的密码。

触发登录告警的条件：同台设备在不同地区登录相同帐号

3.4.4 客户端日志

操作路径：管理平台->【审计日志】->【客户端日志】

“客户端日志”记录向日葵客户端近 30 天的登录日志（上线、下线），当发生安全事件或异常情况时，可通过客户端日志排查和定位问题。

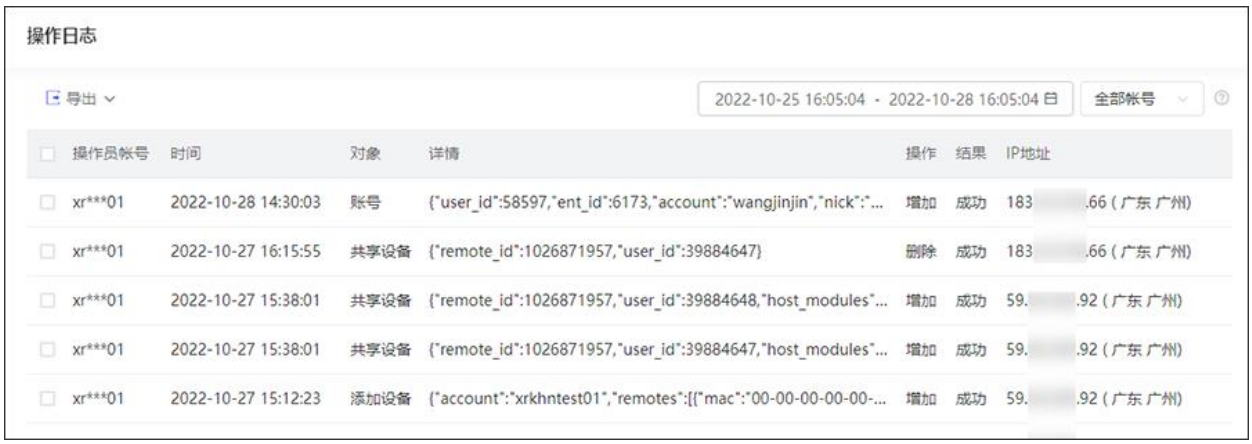
客户端日志包含以下信息内容：事件（上线和下线）、登录时间、客户端帐号、设备名称、登录 IP、登录应用。

3.4.5 操作日志

操作路径：管理平台->【审计日志】->【操作日志】

“操作日志”记录操作员帐号所操作的记录。

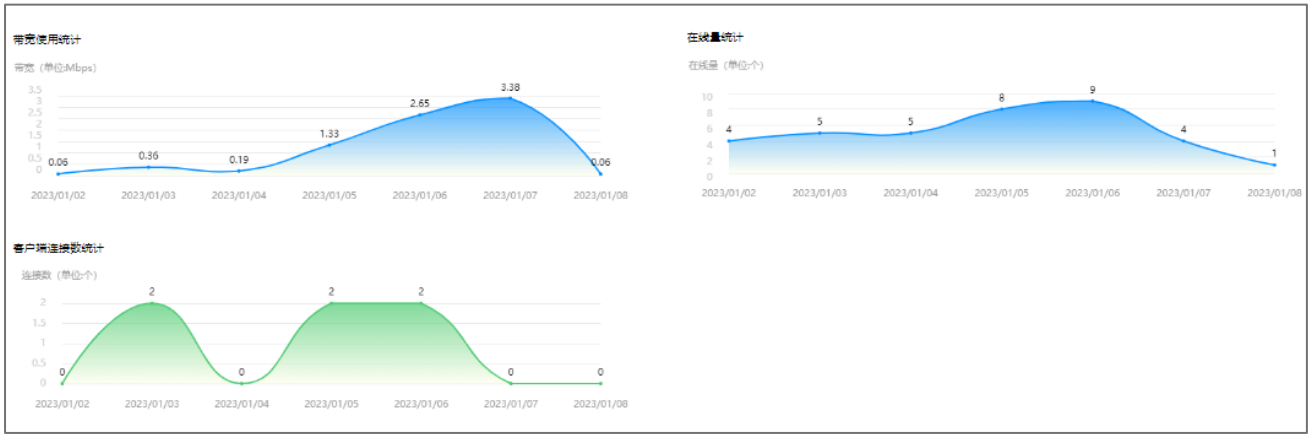
操作日志内容包括：操作员帐号、时间、对象、详情、操作类型、结果、IP 地址。



3.4.6 服务器周报

操作路径：管理平台->【审计日志】->【操作日志】

点击“服务器周报”可查看带宽使用统计、在线量统计及客户端连接数统计。支持在可查看日期范围内的周报导出。（仅企业+帐号服务支持服务器周报功能）



3.5 坐席管理

向日葵领航·坐席专门针对技术支持人群，提供高速、安全的远程支持解决方案，帮助技术人员处理复杂的现场问题。

优势简介：

① 每次远控均享受企业级远程通道，不限速、安全高效

② 支持同时发起多个远程连接，不限制远程连接数，提升工作效率

③ 通过坐席 ID 分配指定坐席员工使用，坐席只可维护自己的客户，管理更便捷

④ 支持设置星标客户，存档业务信息，并在控制台提供集中式客户管理，方便信息的审计和溯源

⑤ 坐席远程记录可追溯，让管理工作有据可依

购买领航服务后，管理员可以通过向日葵管理平台的【坐席管理】功能，进行添加/删除坐席、查看坐席日志、查看星标客户和安全设置的操作。

3.5.1 坐席成员

操作路径：管理平台->**【坐席管理】**->**【坐席成员】**

显示当前帐号下的坐席 ID 以及对应的坐席名、手机号和星标客户数，并提供删除坐席 ID 和重置坐席 ID 密码的操作。

生成坐席成员有 2 种模式：**帐号模式、ID 模式**，2 种模式不能同时存在，切换管理模式将会清空现有的坐席成员信息。

3.5.1.1 帐号模式

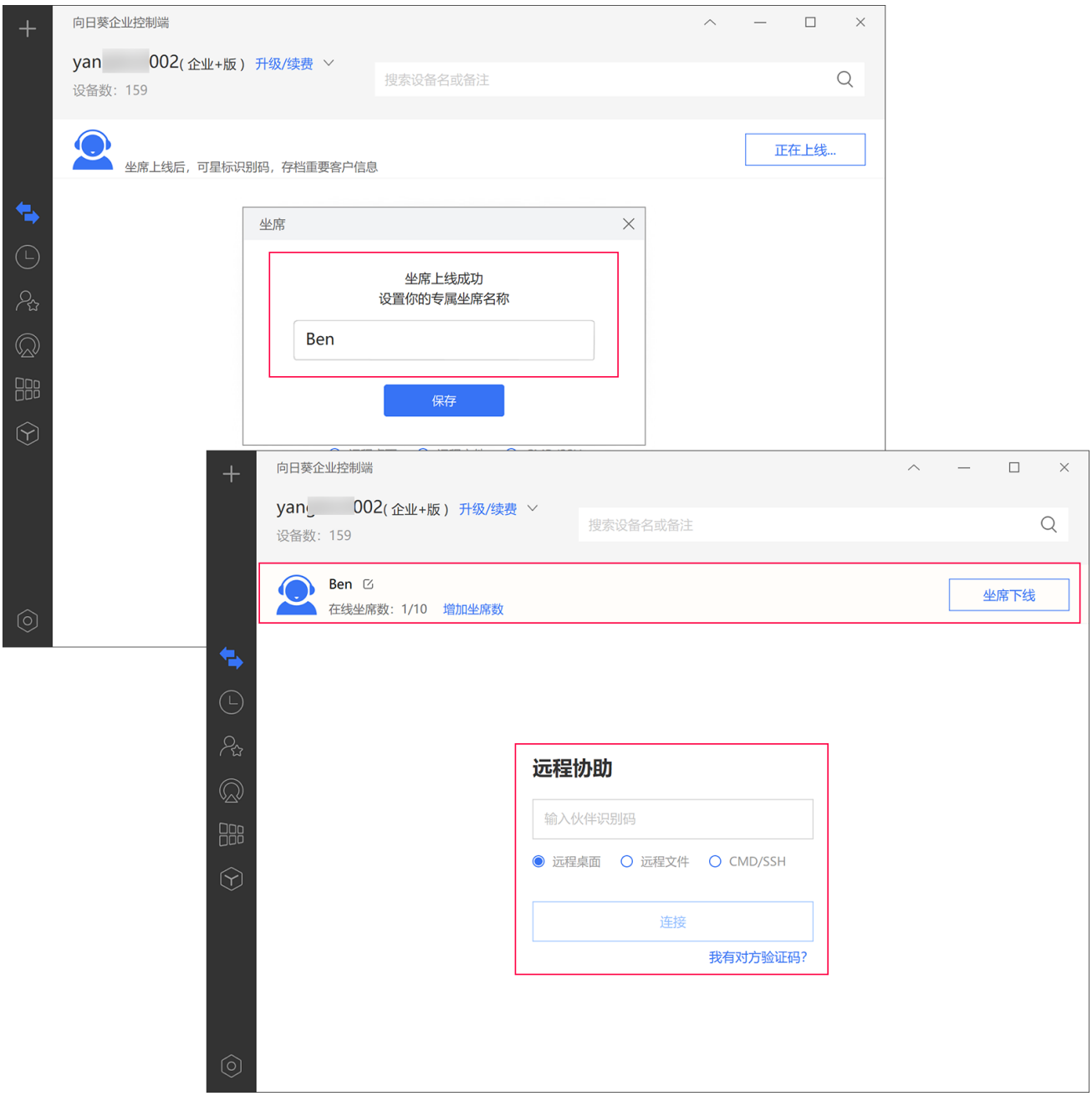
“**帐号模式**”是指在坐席成员使用帐号登录向日葵控制端并手动上线坐席，在“**坐席成员**”列表中便可查看上线的坐席成员，适用于售后支持人员数量不多或实现轮班制的场景下使用。

（1）安装最新版**向日葵企业版控制端**(点击下载)，双击程序运行。在登录窗口选择“**帐号登录**”方式，输入已购买坐席服务的帐号密码，并点击“**登录**”；

（2）登录成功，在【远程协助】功能里，手动点击“坐席上线”，如下图：

PS：可上线的坐席数=购买的坐席数

（3）坐席上线成功，根据提示设置坐席名称后，即可开展远程支持工作；



（4）在向日葵控制端软件“坐席上线”后，进入“坐席成员”列表，可以看到通过帐号模式上线的坐席成员，可以对坐席进行**删除**和**强制下线**的操作。

操作路径：管理平台->【坐席管理】->【坐席成员】

3.5.1.2 ID 模式

“ID 模式”是由管理员在管理平台手动添加对应数量的坐席 ID，再分配坐席 ID 给不同的技术人员使用。其优点是每个坐席成员的帐号密码都是独立管理的，避免一号多用的麻烦。

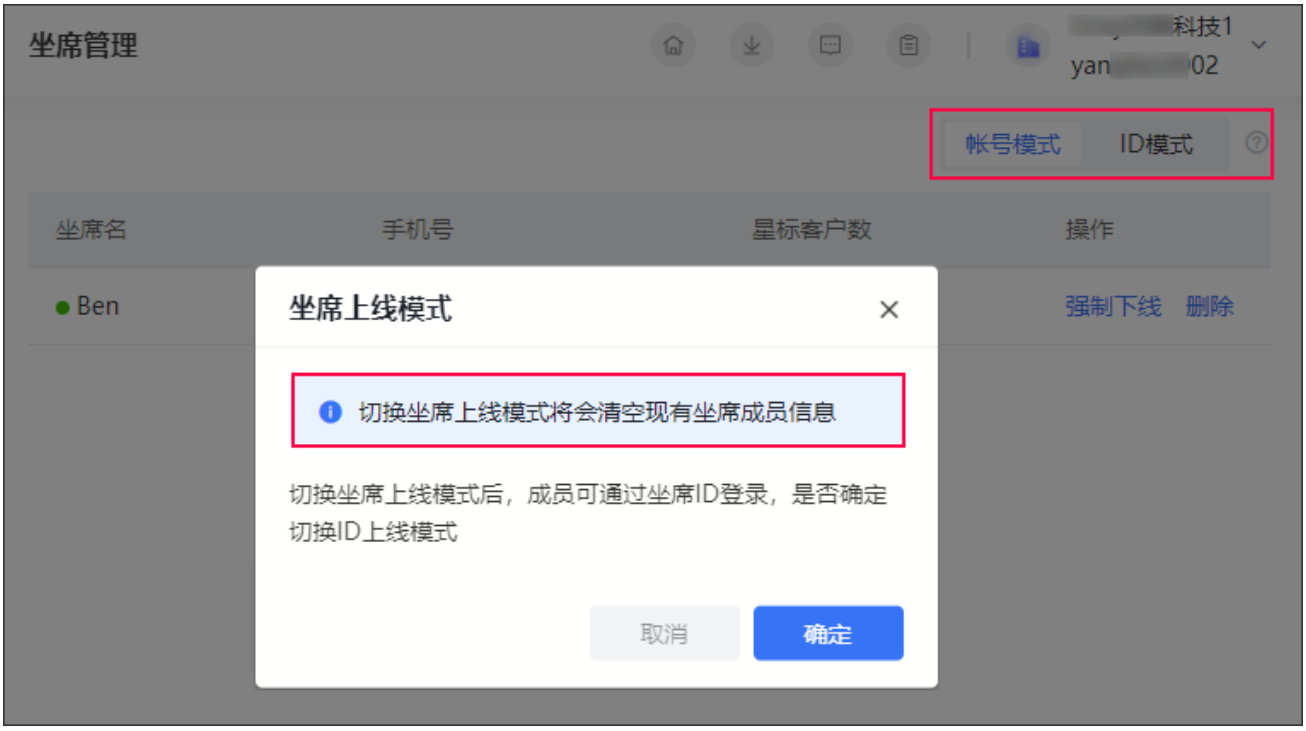
若技术支持人员同时多人在线，建议使用 ID 模式。管理员可以直接对所属的坐席 ID 进行统一管理，如果出现人事变动，管理者可以单独对坐席 ID 删除，但是其工作记录并不会消失，客户记录仍保留在管理平台。

3.5.1.2.1 添加坐席 ID

操作路径：管理平台->【坐席管理】->【坐席成员】

（1）若坐席是帐号模式上线的，点击页面右上角的“ID 模式”切换，可切换为 ID 模式；

注意：切换管理模式将会清空现有的坐席成员信息。



（2）切换为“ID 模式”后，页面上方出现出现“+添加”的按钮，并点击此按钮；

（3）在页面弹窗中填写坐席 ID 的相关参数，如：

①**坐席名**：自定义坐席员工的名称

②**手机号**：绑定坐席 ID 用于登录软件，或登录时进行安全校验

③**设置密码**：设置坐席登录的密码

④**重复密码**：重复输入坐席登录的密码

确认以上信息填写无误后，点击**“确定”**。

（4）系统自动生成坐席 ID 并展示在坐席成员列表中，支持修改坐席名称、修改绑定的手机号、强制下线、删除坐席和重置密码操作（可添加坐席数=购买的坐席数）。

3.5.1.2.2 坐席登录

（1）双击运行最新版向日葵企业版控制端(点击下载)，在登录窗口选择“坐席登录”。支持坐席 ID、手机号码+验证码方式登录。

①坐席 ID：输入前面步骤添加坐席成员时，系统生成的坐席 ID 和密码进行登录

②手机号登录：切换为坐席 ID 绑定的手机号码+验证码方式登录

（2）坐席登录成功，可以通过识别码发起远控请求，帮助客户解决问题。

（3）通过坐席独立 ID 上线，控制端界面只显示星标列表，不能查看主机列表。

3.5.2 坐席日志

在“坐席日志”中记录了近 30 天内坐席成员的操作的日志，日志记录了包括事件（远程桌面、远程文件、上下线、CMD）、事件、坐席 ID、客户识别码和事件记录等信息。

3.5.3 星标客户

操作路径：管理平台->【坐席管理】->【星标客户】

显示已标记为星标的客户列表，在“远控记录”查看客户被远程控制的操作记录，点击“删除”可以移除当前星标客户。

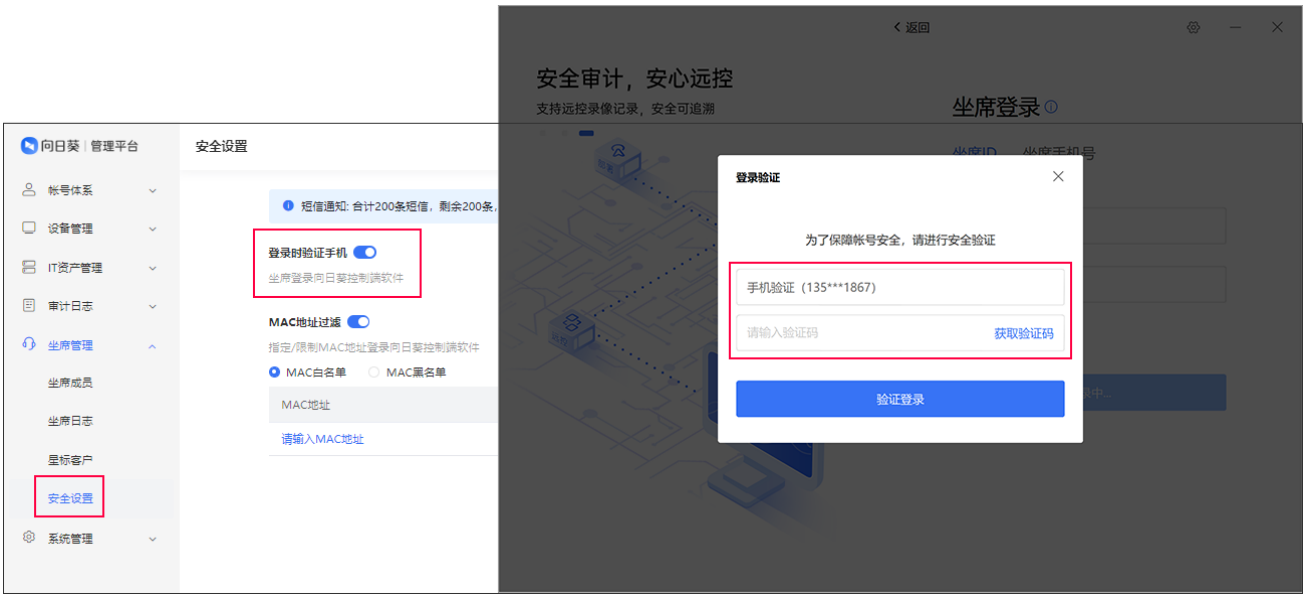
3.5.4 安全设置

操作路径：管理平台->【坐席管理】->【安全设置】

该设置项是对坐席成员登录控制端软件时做进一步的验证。

3.5.4.1 手机验证

勾选“登录时验证手机”此项，在向日葵控制端软件以「坐席登录」方式上线时，需要经过预留的手机号码完成短信验证方可成功登录。



3.5.4.2 MAC 地址过滤

勾选“MAC 地址过滤”，可选择设置“MAC 地址白名单”或“MAC 地址黑名单”来限制特定的 MAC 地址设备登录向日葵控制端。

举例：

管理员已设置 MAC 地址白名单，当非白名单内的设备以「坐席登录」方式上线，提示“限制 mac 地址登录”

3.6 系统管理

系统管理是针对登录向日葵控制端的设备进行监控和管理：

（1）企业在日常应用中，为安全起见，可设置设备验证登录保护。未经过安全验证的设备无法登录控制端，可保障远程运维工作在安全可信的设备上进行。

（2）支持添加异常告警联系人员，当控制端登录异常时，系统自动发送消息通知管理员，可及时对登录异常情况作出处理。

3.6.1 企业信息

企业信息所包含内容及说明如下：

序号	信息项	说明
①	**当前企业名称**	设置当前企业的名称，设置后企业名称会显示在管理平台右上角处，支持更改
②	**当前企业别名**	企业唯一标识，用于企业+登录帐号，建议使用企业邮箱等公司系统内部统一的别名
③	**企业人员**	显示当前已加入企业的人员数量
④	**企业认证**	企业实名认证入口，完成企业认证后，可使用完整功能

3.6.2 第三方接入

操作路径：管理平台->【系统管理】->【第三方接入】

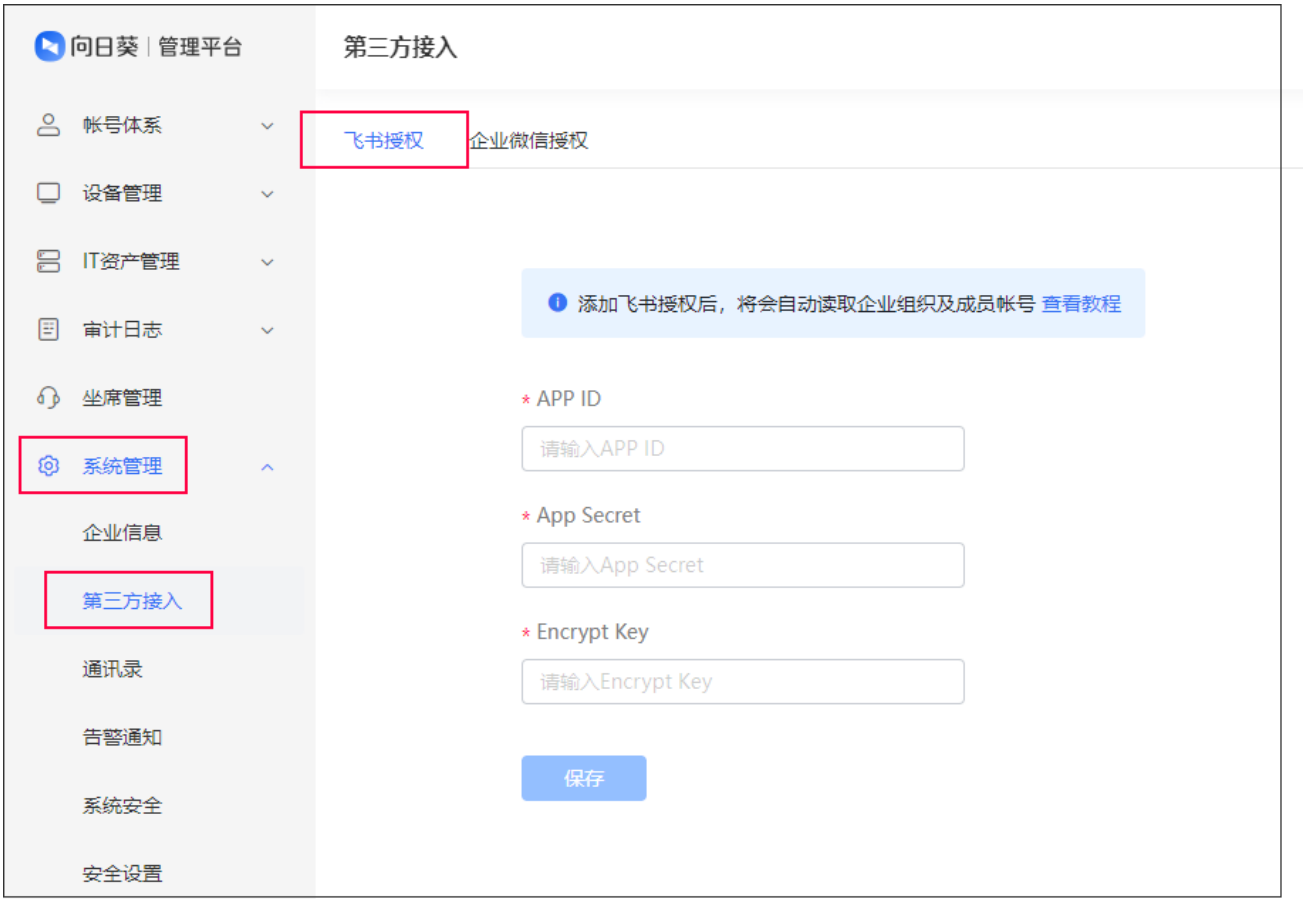
第三方接入功能是指管理员快速导入企业原有的飞书、企业微信组织架构成员，省去逐个添加员工帐号的繁琐操作，实现快速部署企业员工帐号。

（1）飞书授权（配置说明）

①管理员在飞书配置授权，获取 APP ID、App Secret、Encrypt Key

②在向日葵管理平台绑定授权飞书，添加飞书授权后，将会自动读取企业组织及成员帐号

③在飞书管理后台添加事件，可以满足应用及时响应飞书事件变更的需求，如部门及人员变更时，向日葵均会自动同步信息



（2）企业微信授权（查看详细教程）

添加企业微信后，将会自动同步企业成员。

①因企业微信不可读取成员姓名，你需要发送【邀请链接】给企业成员验证

②Windows 控制端扫码登录需 v5.6.2 及以上版本

3.6.3 通讯录

操作路径：管理平台->【系统管理】->【通讯录】

添加接收消息通知的联系人通讯录，用于管理员在各推送设置中，快速从联系人通讯录中选择消息推送的对象。

（1）添加联系人

在页面点击【添加】，需经过身份验证（手机号码或邮箱）后，才能添加联系人。

（2）修改/删除联系人

若接收通知消息的员工，其联系方式（手机、邮箱）变更或已离职，则可以在联系人列表中更改或删除对应的联系方式，统一取消所有的通知。

其他说明：

①**向日葵免费版/个人服务，不享受短信包服务，**所以在消息通知推送方式中仅可使用：邮箱通知、管理平台、企业控制端推送三种方式

②其他服务等级分别赠送相应的短信数量，具体区别如下表

	服务等级	短信数量
短信数量说明	免费版/个人版	/
	旗舰版	免费赠送 200 条
	行业版/行业青春版	免费赠送 500 条
	独立服务器/企业+	免费赠送 500 条

【关于短信数量的说明】

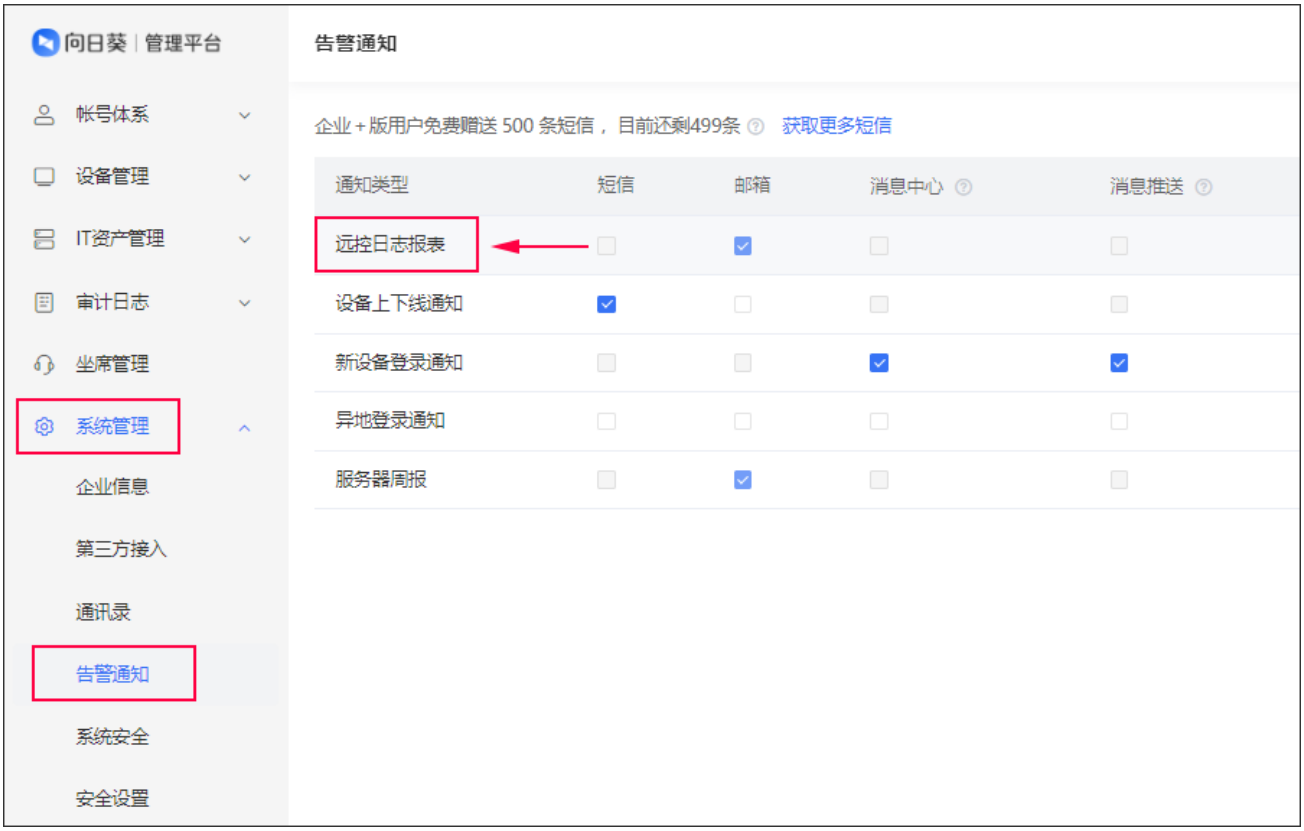
3.6.4 告警通知

告警通知为企业用户提供的专属功能，可根据实际情况开启远程日志邮件通知、设备上下限通知及服务器周报，为用户实时推送异常告警消息，方便用户及时了解设备异常诊断问题。

3.6.3.1 远控日志邮件通知

操作路径：管理平台->【系统管理】->【告警通知】

企业专属远控日志邮件通知功能，可订阅每周/每月的远控日志，发送到指定邮箱，可以更详细地查看所有客户端的使用情况。



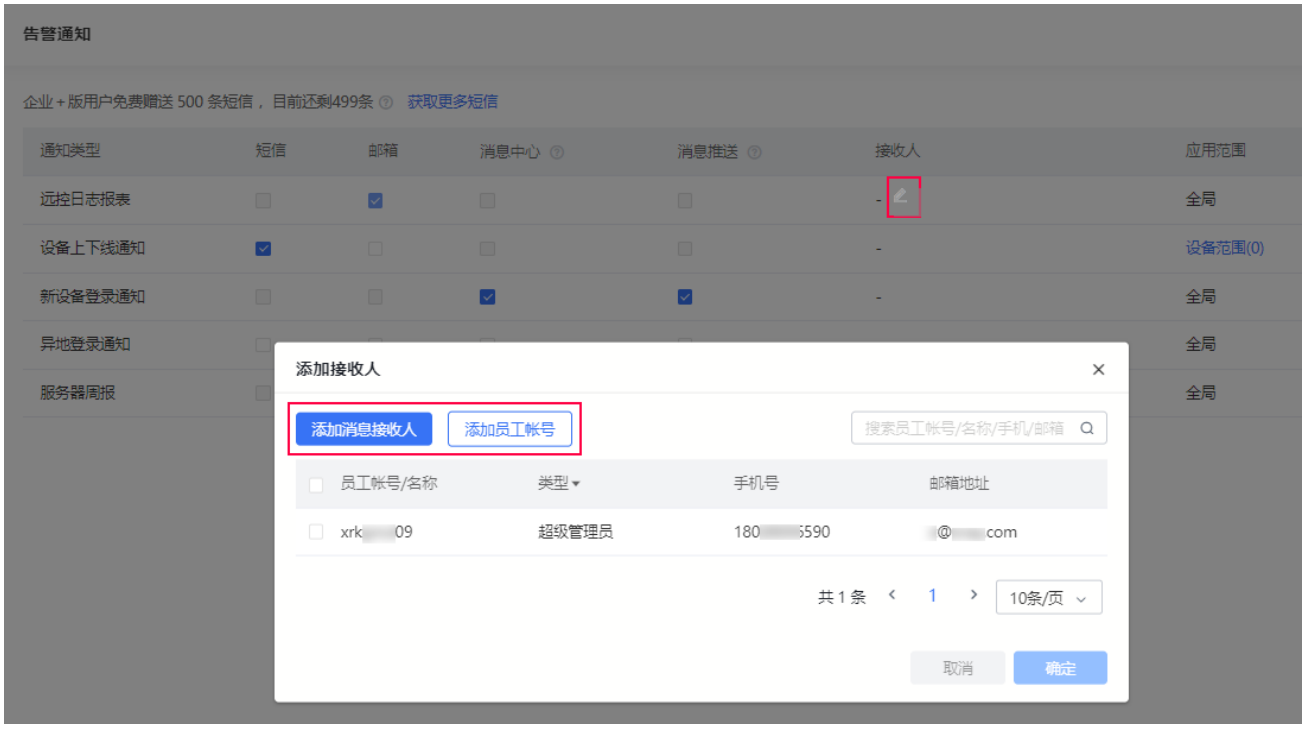
（1）添加告警信息接收人：

①在“**接收人**”下方点击编辑图标

②添加需要接收告警的人员（支持选择多个接收人）

③点击确定即可设置成功

④若还未设置接收人，可点击“**添加消息接收人**”或“**添加企业+帐号**”进行设置



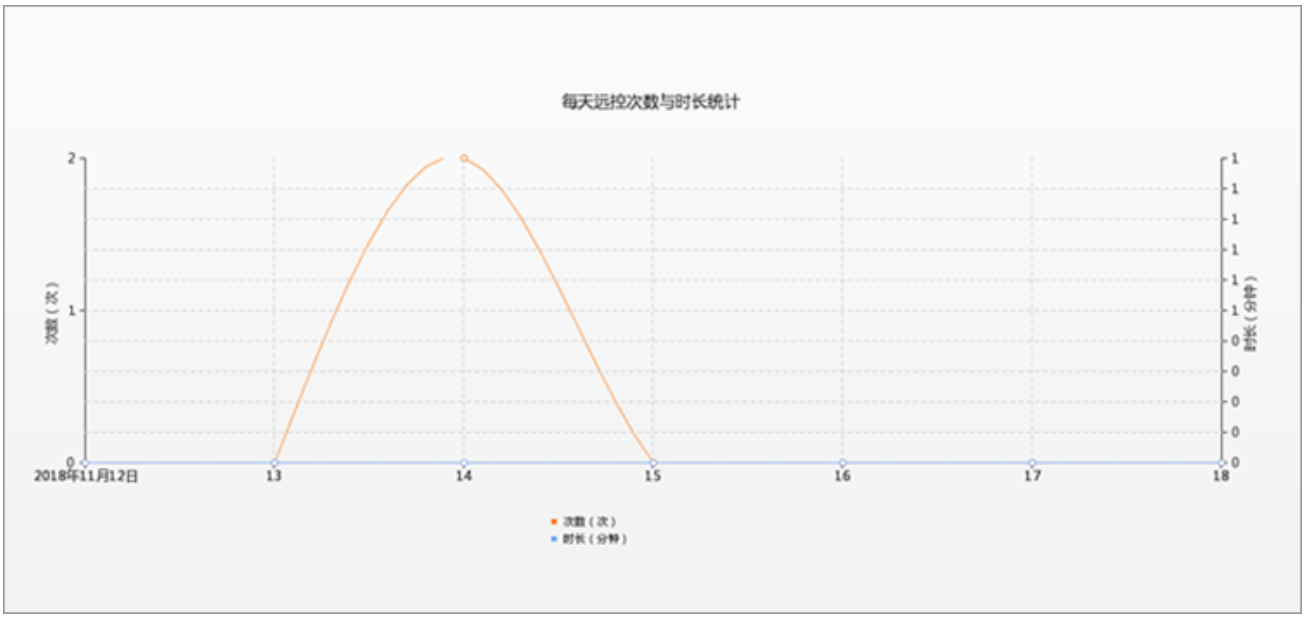
（2）设置告警频率：

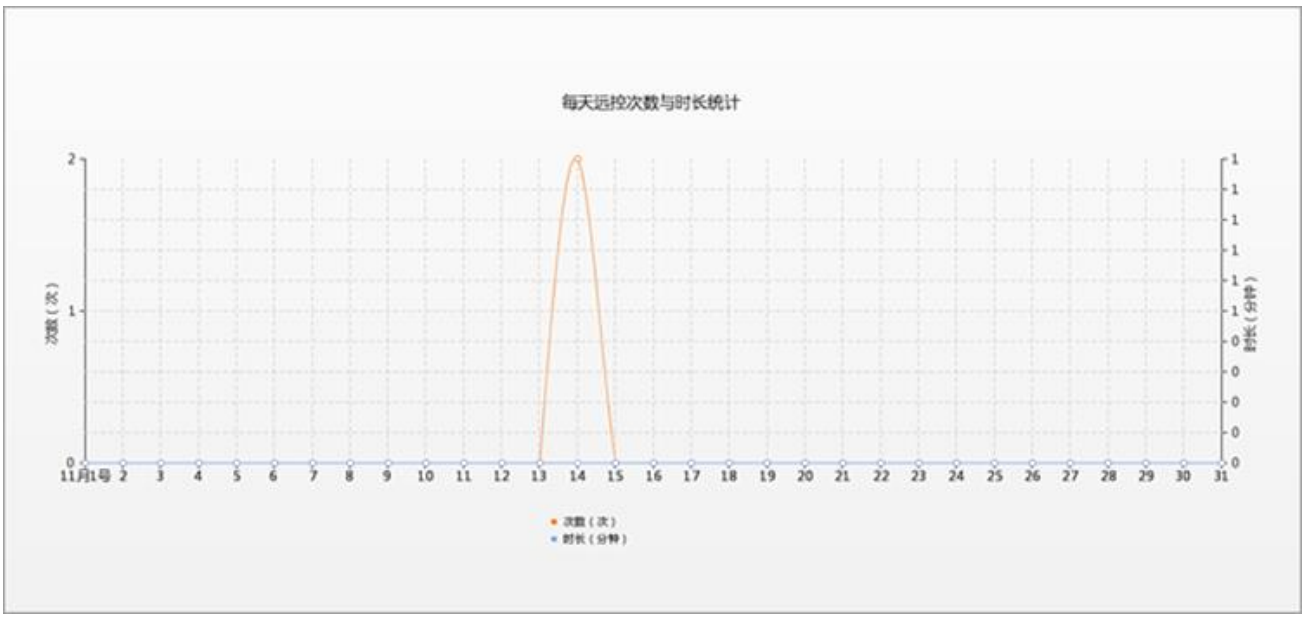
①在发送/告警频率下方点击编辑图标按钮

②设置每月 1 号接收上月报表或每周一接收上周报表，点击“**确定**”完成设置

（3）添加完成后，在列表中可以看到已设置的**接收人、发送频率**；

（4）设定好发送频率之后，每周一/每月 1 号的时候，对应邮箱内就会收到一封来自贝锐的远控日志报表，报表效果如下图所示（每周/每月）；





3.6.3.2 设备上下线通知

企业专属设备上下线通知功能，订阅短信或邮箱通知后，可获取设备的上下线通知推送，管理员实时掌握远程设备的在线状态，如遇突发情况、便于及时做出应对策略。

（1）设备上下线的通知**接收方式**（短信或邮箱方式二选一）：

①短信方式通知，告警频率为”每次“，即一旦触发告警项，即可推送告警通知

②邮箱方式通知，告警频率为”每日“，即每天凌晨 1 点会汇总前一天的告警事件发送至指定邮箱

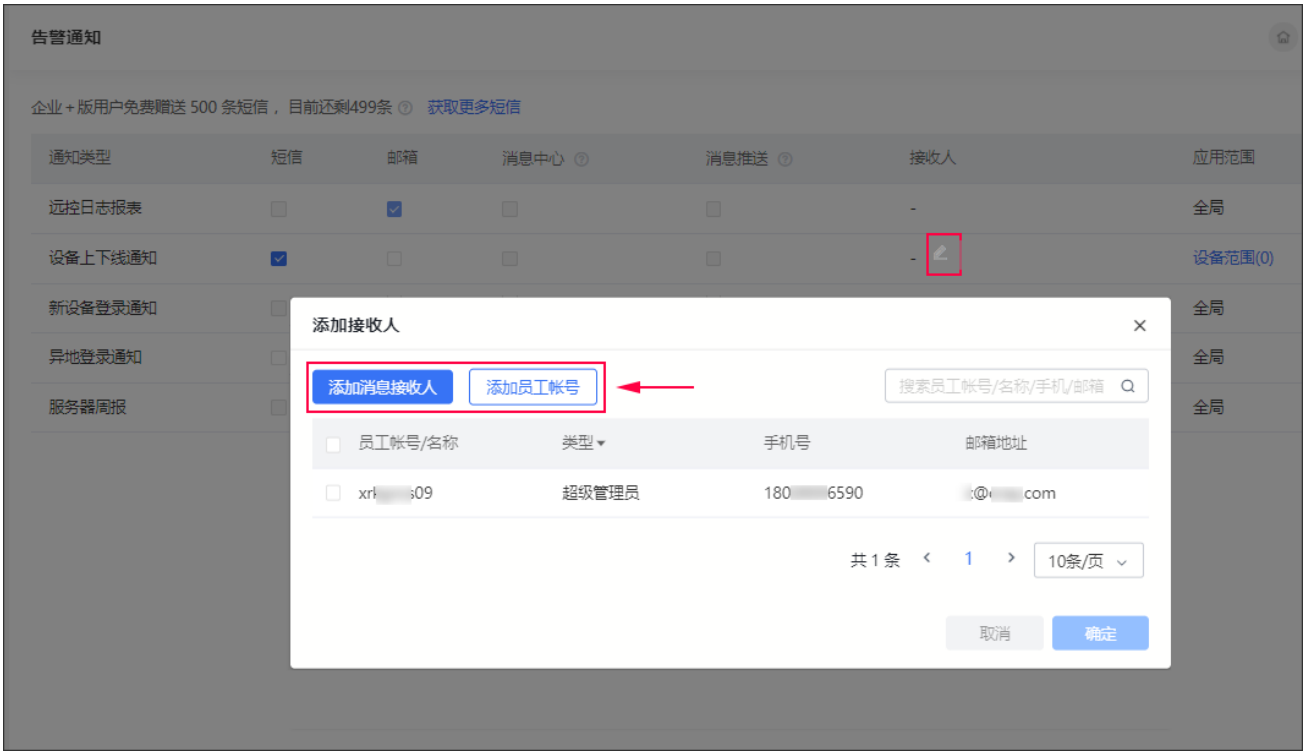
（2）添加通知消息接收人：

①在“**接收人**”下方点击编辑图标；

②添加需要接收告警的人员（支持选择多个接收人）

③点击确定即可设置成功

④若还未设置接收人，可点击“**添加消息接收人**”或“**添加企业+帐号**”进行设置

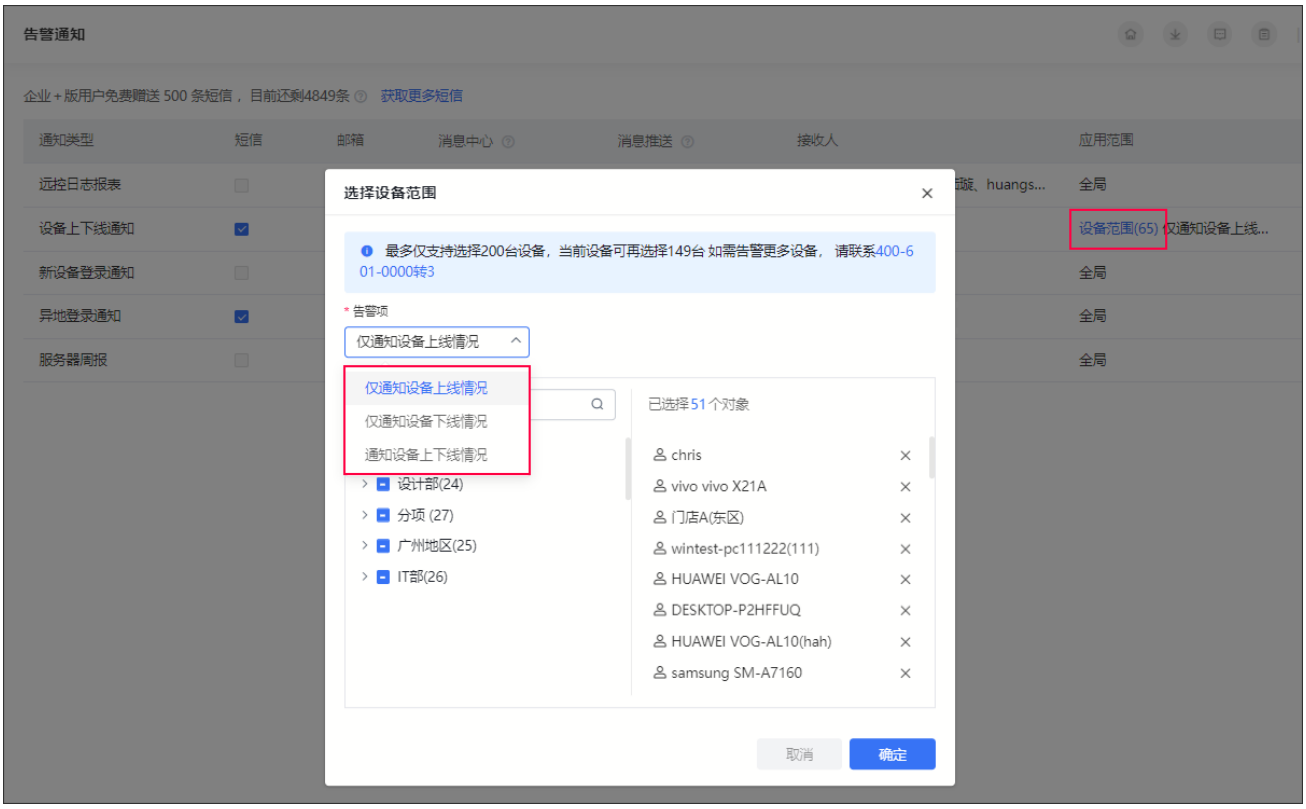


（3）设置告警项及监控设备对象：

①点击“**设备范围**”，选择告警项，可设置：**仅通知通知主机上线情况、仅通知主机下线情况、通知主机上下及下线**

②选择需要监控上下线情况的设备

③最后点击“**确定**”完成订阅



注意

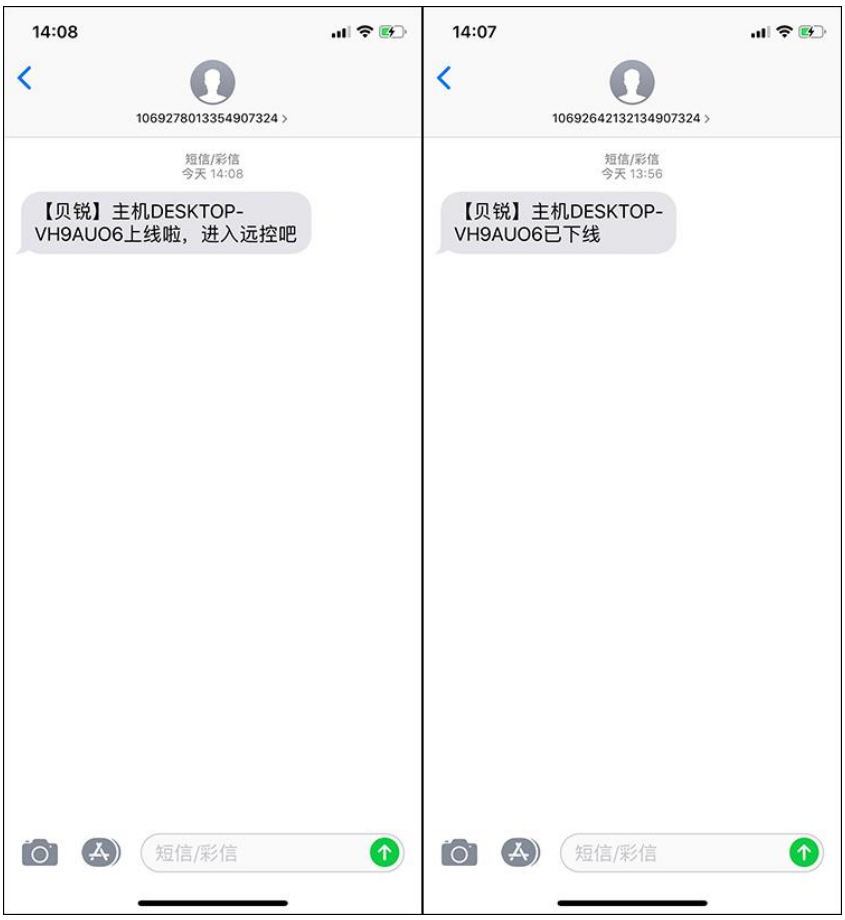
①设备上下线通知，最多支持选择 200 台设备，如需告警更多设备，请联系 020-2919609

②选择监控设备数量超过 100 台，建议使用邮件告警方式

（4）添加完成后，在列表中可以看到已设置的**接收人、告警项、发送频率。**

（5）消息推送举例

①短信通知：当已订阅的设备上线或下线时，指定手机号会收到监控设备上下线的信息推送（**旗舰版用户赠送 200 条短信，行业青春版/行业版及企业+用户赠送 500 条短信**）

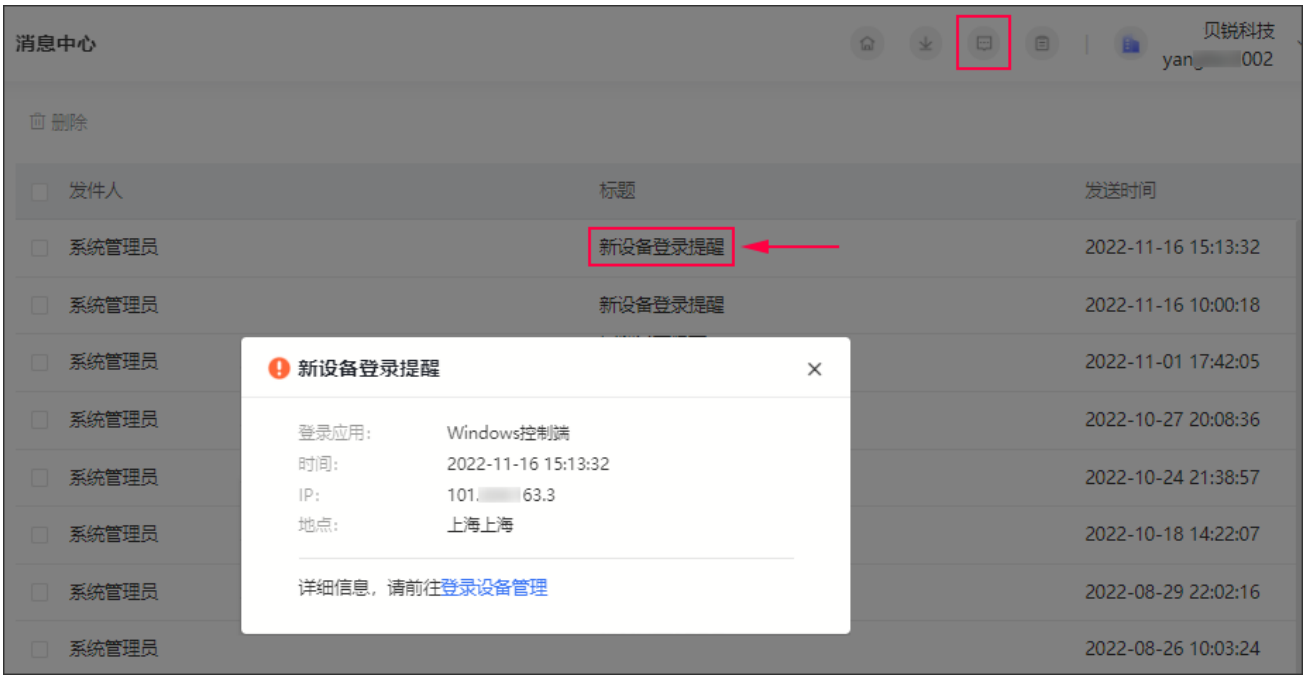


②邮件通知:指定的邮箱将在每日凌晨 1 点接收到前一天的设备上下线消息事件邮件

3.6.3.3 新设备登录通知

企业可根据自身使用需求接收“新设备登录通知”消息，管理员通过查看新设备登录的通知消息，来判断帐号是否存在登录异常的问题。

管理员在管理平台的【消息中心】中查看新设备登录提醒的消息详情。



3.6.3.4 异地登录通知

异地登录通知指系统检测到控制端软件在异地登录时，即会触发登录告警，管理员可设置通过短信、邮箱或管理平台途径来接收通知消息。

触发登录告警的条件：同台设备在不同地区登录相同帐号

例如：同个帐号同台设备原登录地点为广州，当登录地点变更为上海时，系统会发登录异常告警消息给指定联系人。若非本人已知情况的登录操作，建议修改帐号的密码。

添加通知消息接收人：

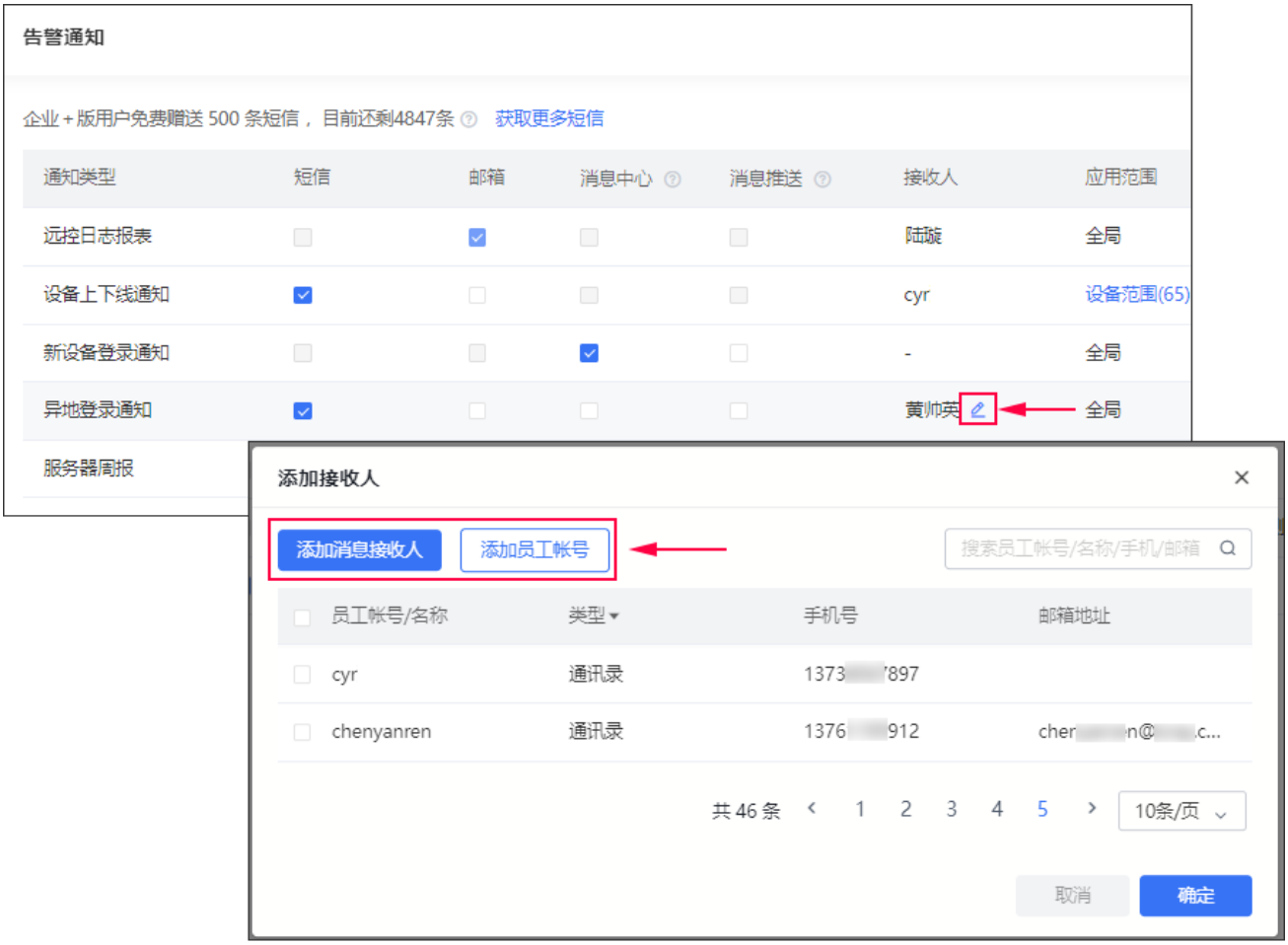
①在“**接收人**”下方点击编辑图标

②在弹窗中添加需要接收异地登录告警消息的的人员（支持选择多个接收人）

③点击确定即可设置成功

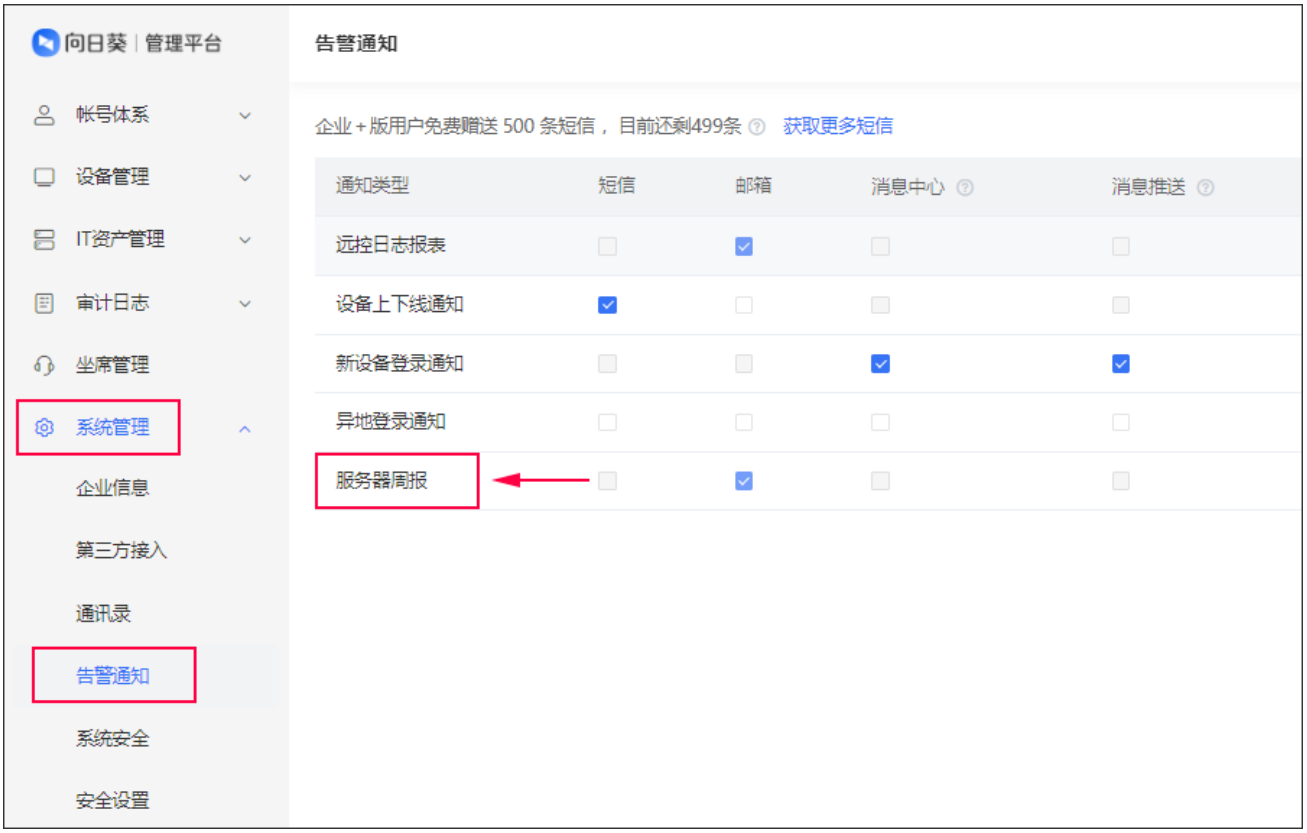
④若还未设置接收人，可点击“**添加消息接收人**”或“**添加员工帐号**”进行设置

已在接收异常告警信息列表中的联系人，将会接收到系统发送的通知消息。



3.6.3.5 服务器周报

企业专属服务器周报功能，可订阅每周报表推送，发送到指定邮箱，可以查看设备的带宽使用统计、在线量统计以及客户端连接数统计。

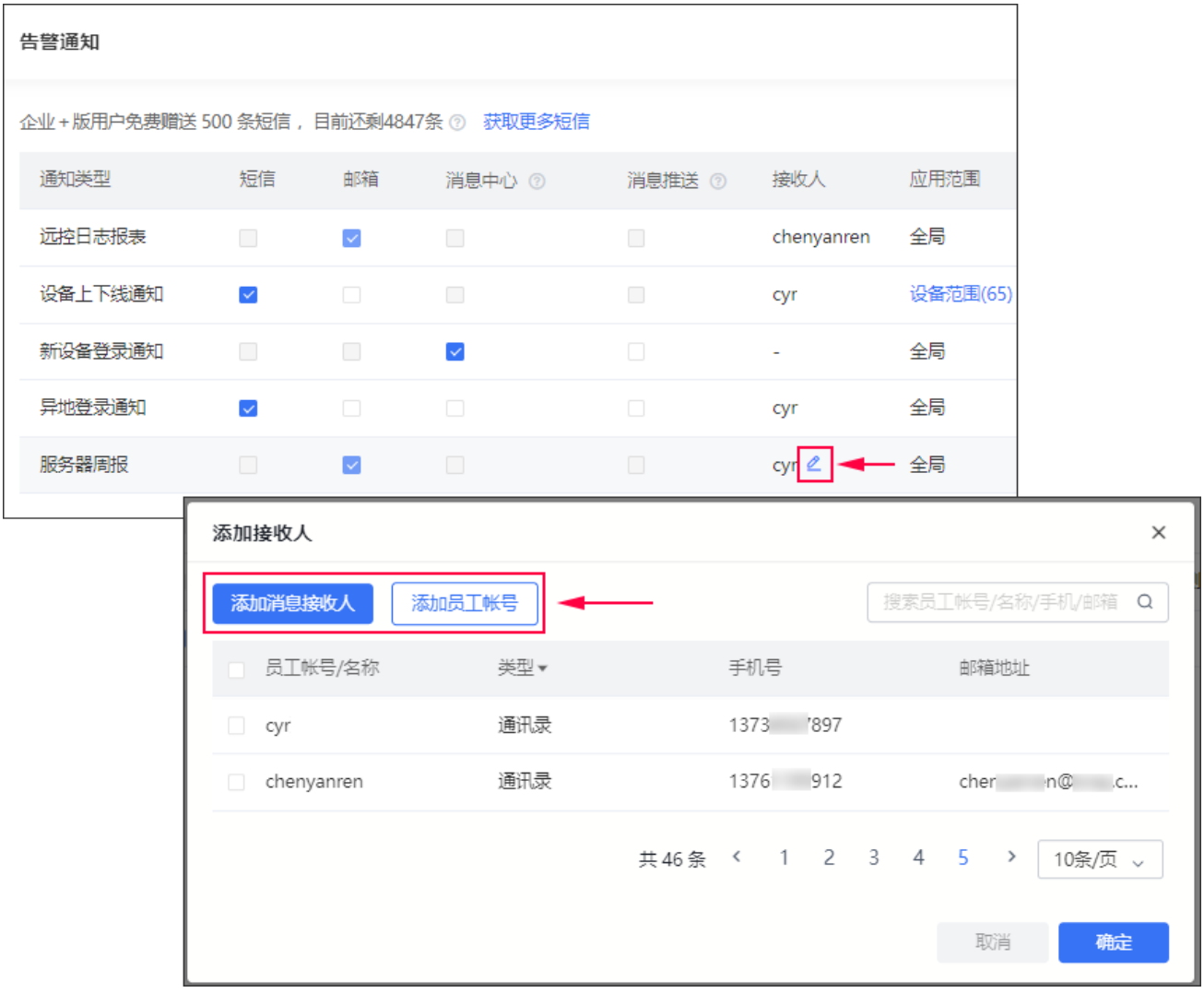


（1）添加服务器周报的接收人：

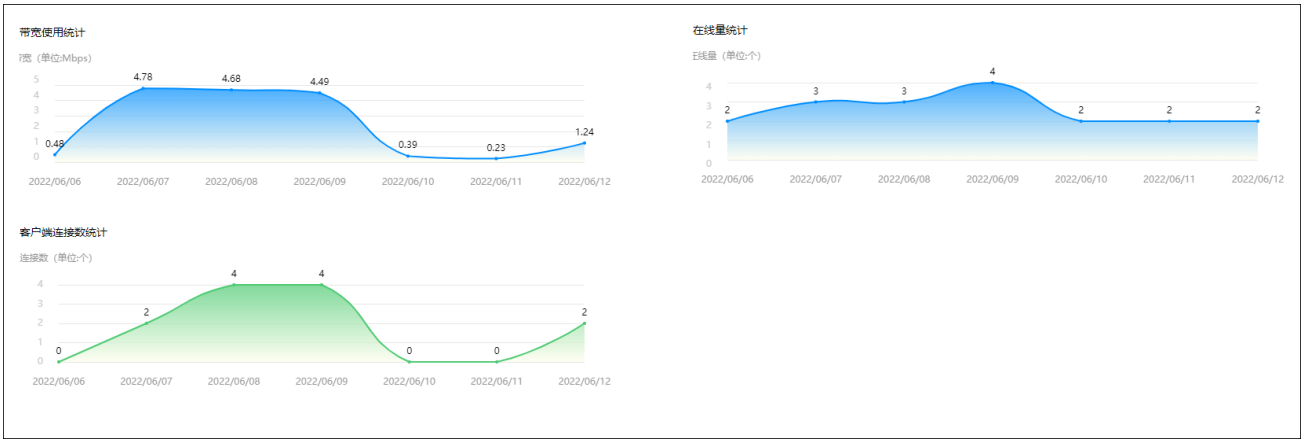
①点击“接收人”下方的编辑图标

②加需要接收告警的人员（支持选择多个接收人），点击确定即可设置成功

③若还未设置接收人，可点击“**添加消息接收人**”或“**添加员工帐号**”进行设置



(2) 订阅服务器周报后可查看设备的带宽使用统计、在线量统计以及客户端连接数统计。



3.6.5 系统安全

3.6.5.1 帐号保护

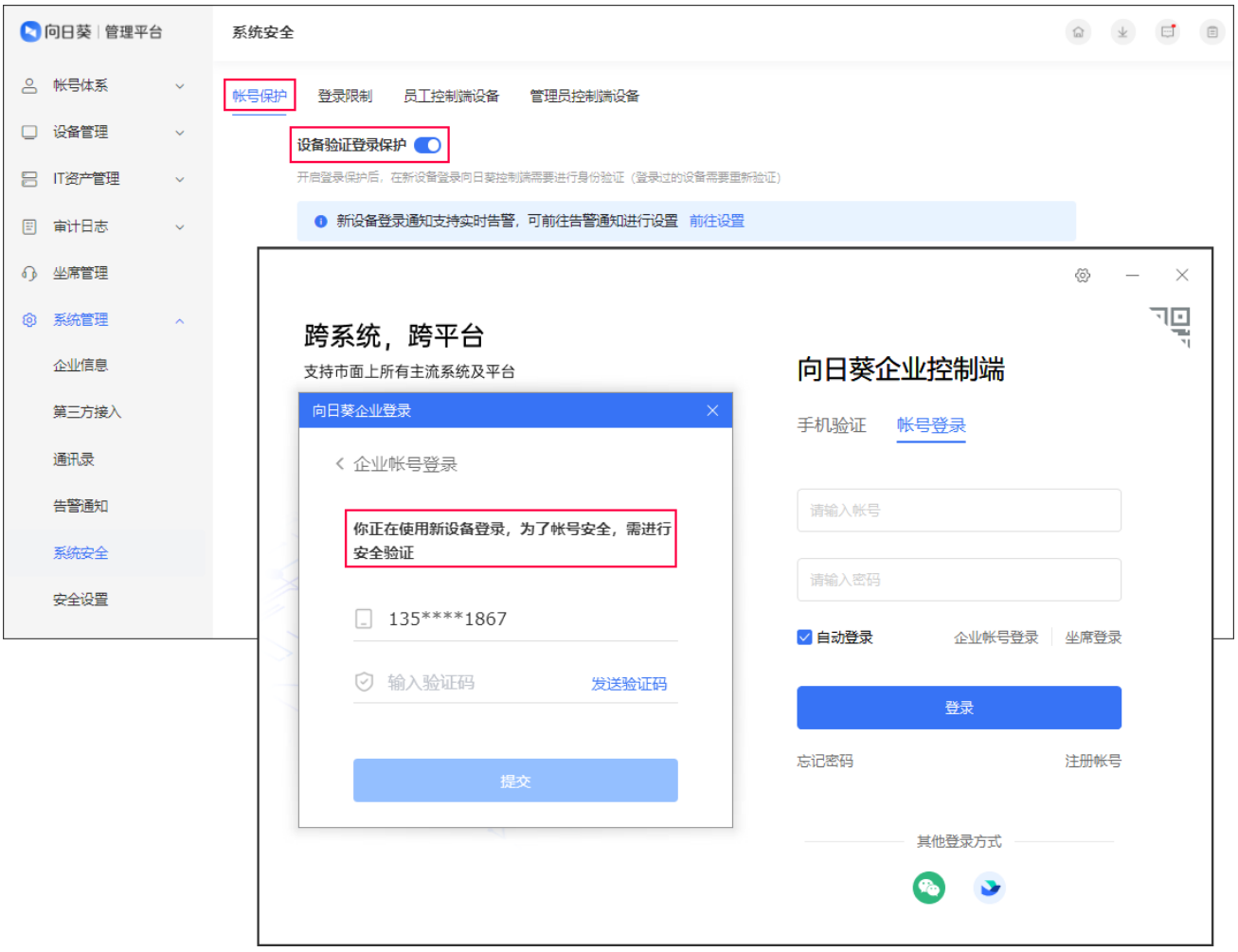
操作路径：管理平台->【系统管理】->【系统安全】->【帐号保护】

设备验证登录保护功能是指，用户在新设备登录向日葵控制端需要进行身份验证。如帐号绑定的手机及邮箱非本人所有，需管理员提供验证码后，才可成功登录。

开启登录保护后，以前登录过控制端的设备也需要重新验证手机/邮箱才能登录。

当前仅支持管理平台、控制端 V5.6.1 及以上版本。若需要使用登录保护功能，**请升级软件到最新版本**。

举例：小王原控制端登录设备为公司电脑，管理员开启【**设备验证登录保护**】后，在家里电脑（未登录过该帐号）登录控制端时，需经过身份验证才能登录。



3.6.5.2 登录限制

“登录限制”是对向日葵企业帐号登录**「管理平台」**、**「控制端」**时，设置 MAC 地址、IP 地址、时间段的登录限制，3 种限制登录方式可根据实际需求叠加使用。

开启登录限制后，企业帐号在登录控制端或管理平台时，系统除了校验帐号密码外，还会

检验登录设备是否符合登录限制设定的条件规则，为帐号安全提供更高级别的保障。

序号	限制方式	说明	限制对象
①	MAC 地址限制	员工仅在 MAC 地址限制条件下**允许/不允许**登录控制端	PC 控制端
②	IP 地址限制	员工仅在 IP 地址限制条件下**允许/不允许**登录控制端/管理平台	PC 控制端 管理平台
③	时间段限制	员工仅在时间段限制条件下**允许/不允许**登录控制端/管理平台	PC 控制端 管理平台
④	因子验证	在控制端或管理平台登录受到限制时，支持使用二次身份认证通过验证	PC 控制端 管理平台
⑤	域名访问登录验证	开启后，通过域名方式远控企业设备时，需要进行登录校验	Web 页面

操作路径：管理平台->【系统管理】->【系统安全】->【登录限制】

（1） MAC 地址限制

为帐号开启 MAC 地址登录限制，保证帐号在安全环境下登录控制端软件。开启后，为登录控制端软件的设备设置 MAC 地址**白名单** or **黑名单**。

①**MAC 地址白名单**：仅允许在 MAC 地址白名单内的设备登录 PC 控制端

②**MAC 地址黑名单**：禁止 MAC 地址黑名单列表内的设备登录 PC 控制端

（2）IP 地址限制

为帐号开启 IP 地址登录限制，保证帐号在安全环境下登录 PC 控制端/管理平台。开启后，根据企业实际需求选择设置 IP 地址白名单 or 黑名单。

①IP 地址白名单：仅允许 IP 地址白名单内设备登录 PC 控制端及管理平台

②IP 地址黑名单：禁止 IP 地址黑名单内设备登录 PC 控制端及管理平台

（3）时间段限制

为帐号设置登录 PC 控制端/管理平台的时间限制。

①**白名单时间段**：仅允许帐号在指定时间段内登录 PC 控制端及管理平台

②**黑名单时间段**：禁止帐号在指定时间段内登录 PC 控制端及管理平台

（4）因子验证

当帐号登录控制端及管理平台时受到登录限制（如 MAC 地址限制、IP 地址限制、时间段限制），可开启“因子验证”进行二次验证，即可解除登录限制。

开启因子验证开关步骤：

①开启“因子验证”开关

②点击“添加帐号”，在弹窗中选择可使用因子验证的帐号，并确认

①管理员设置了员工在 20:30:00~23:59:59 时间段内禁止登录控制端及管理平台

②针对员工王津津需全天候运维设备的需求，管理员开启“因子验证”开关，并添加其帐号在因子验证列表中

③当员工王津津于黑名单时间段内登录控制端时，通过手机/邮箱验证后，即可成功登录控制端及管理平台

当前支持因子验证的渠道：

管理平台

Windows 企业控制端 V5.6.1 及以上版本

其他系统敬请期待

（5）域名访问登录验证

开启后，通过域名访问方式远控企业设备，需进行登录校验。

区别：

①未开启域名访问登录验证：通过域名方式远控企业设备，无需验证企业帐号

②已开启域名访问登录验证：通过域名方式远控企业设备，需验证企业帐号

设备开启域名访问方式的步骤：

①在【设备管理】->【设备列表】中，在对应设备的操作栏处选择“域名访问”

②为设备开启域名访问功能

3.6.5.3 员工控制端设备

操作路径：管理平台->【系统管理】->【系统安全】

「员工控制端设备」仅记录企业员工的登录设备数据，方便管理员查看整个企业的登录设备记录，如发现非常用设备或其他异常情况时，可以随时将异常设备踢下线。

3.6.5.4 管理员控制端设备

操作路径：管理平台->【系统管理】->【系统安全】

「管理员控制端设备」仅记录管理员的登录设备记录，当管理员发现某项登录记录存在异常时，可将其踢下线或删除。

3.6.6 安全设置

操作路径：管理平台->【系统管理】->【安全设置】

向日葵为企业提供水印策略功能，管理员开启水印策略后，员工远控公司设备时远控窗口自动添加水印，加强终端的信息安全，以防止员工泄漏企业信息，即使信息遭泄漏也有迹可循。

服务版本与软件版本要求

①面向企业版服务，对所有企业帐号生效

②面向坐席服务，对所有坐席成员生效

若企业版搭配坐席服务，则策略同时对企业帐号和坐席帐号生效。

当前仅支持 Windows 控制端 v5.5.3 及以上版本，若需使用水印功能，请将控制端升级到最新版本。

开启步骤如下：

①**水印策略**：开启

②**水印内容**：下拉列表可选展示：员工帐号、MAC 地址后六位、开始远控时间

③**水印清晰度**：配置水印清晰度，不影响员工正常操作和工作

以上内容配置完成后，点击“**保存**”即可。

水印策略设置完成，下面分别展示企业版服务和坐席服务版本的水印效果。

（1）帐号远控

举例：当前水印内容设置为“远控帐号+MAC 地址后六位+远控开始时间”，不透明度为30% 。

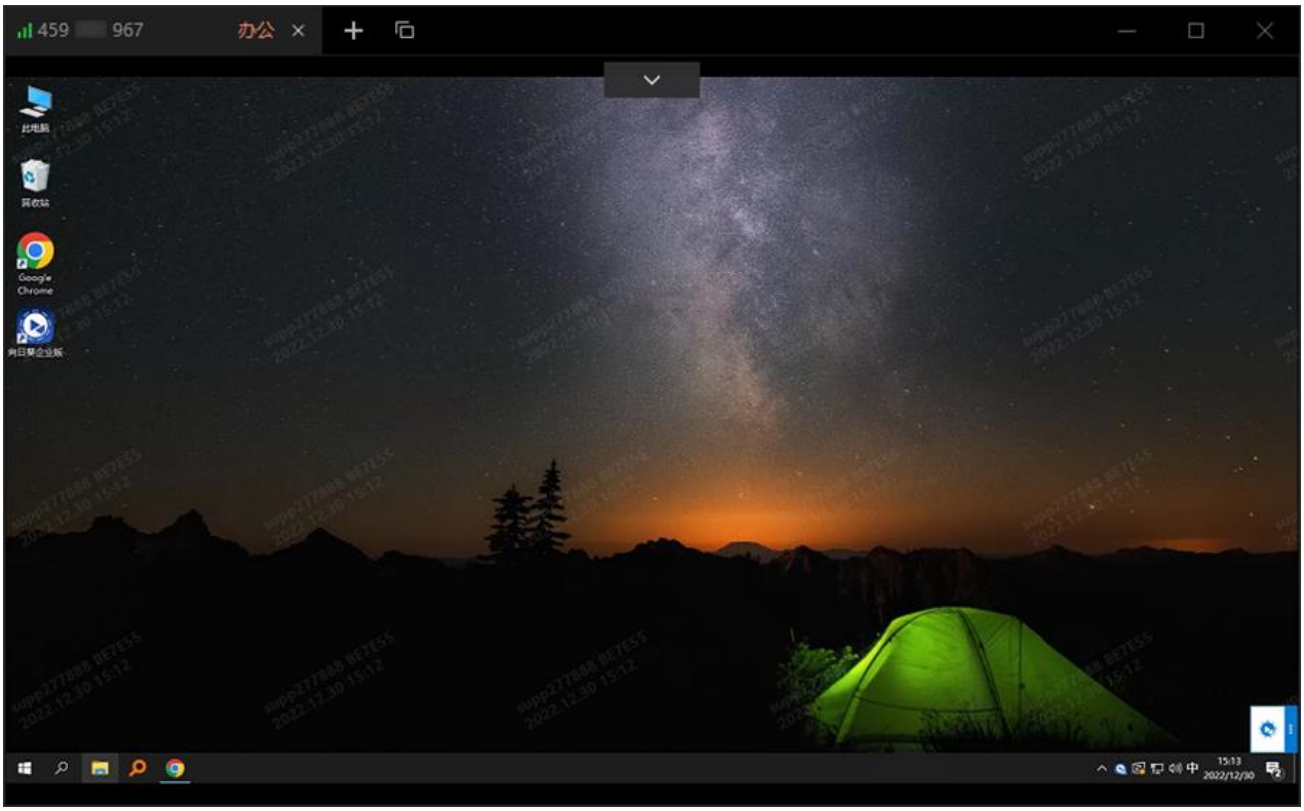
①员工使用管理员分配的企业帐号登录控制端，在【设备列表】对公司电脑发起桌面控制

②远程桌面连接成功后，水印内容始终显示在远控窗口上，即使信息被泄密，也可以通过员工帐号、设备信息和远控时间这些信息进行溯源

（2）坐席远控

①技术支持人员通过帐号模式或 ID 模式上线后，在【远程协助】功能中，对客户设备发起远程桌面请求

②客户授权同意后技术人员安全进入设备桌面进行远程协助，在远控过程中水印始终显示在远控窗口。水印内容根据管理员设置的规则显示，如下图显示为“坐席 ID+MAC 地址后六位+远控开始时间”，加强保护客户终端信息，防止截屏、泄密



（3）隐性水印

如果管理员设置的为隐性水印，则肉眼看不见，请点击查看教程。

向日葵管理平台的功能和使用已介绍完毕，若您在使用过程中遇到任何问题，请前往官网发起工单咨询我们的技术工程师。