安全手册

Yeastar P 系列云 PBX

版本: 1.2
日期: 2023年12月16日

400-661-8815
0592-5503307
www.yeastar.cn

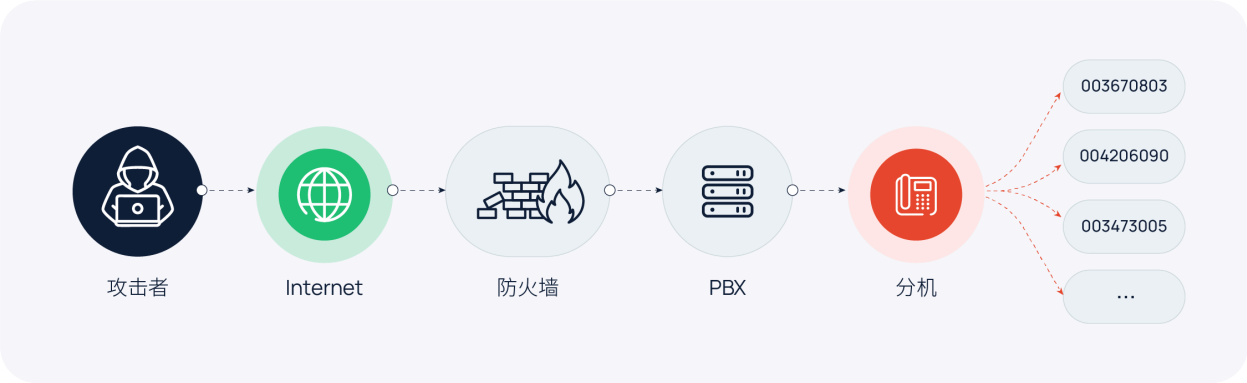
目录

Yeastar P 系列云 PBX 安全手册

PBX 遭受的恶意攻击一般来自网络或电话线路。攻击者总是通过各种手段来探测漏洞，从而入侵电话系统达到盗打电话的目的。最终，攻击者通过盗打电话获利，而你将遭受经济损失。此安全手册旨在指导你如何提高 PBX 安全，并降低电话盗打的风险。

攻击者如何入侵 PBX?

攻击者通常利用漏洞扫描工具在网络上探测企业防火墙是否存在安全漏洞 (如开放端口)。如果检测到有开放的端口，攻击者会向此端口发送大量数据包，尝试进行进一步的漏洞探测，最终可能会突破防火墙。一旦防火墙被攻破，攻击者就能访问 PBX，在 PBX 上建立一个后门，并利用这个后门肆意访问电话系统内的资源，最终通过分机盗打电话。



如何提高 PBX 安全并防止电话盗打?

企业的通信需求和黑客的技术水平是不断变化的，因此无法完全消除电话系统的安全漏洞。但是企业可以通过提高员工安全意识、部署安全防御机制、持续进行安全检查等方式尽可能地减少漏洞，降低风险。

规划企业通信的安全策略时，为增强系统安全，建议采用多层安全防御策略。部署多层防御机制后，每个保护层都成为一道安全防线，即使某一层防护被攻破，仍有其他安全屏障能够阻止攻击者入侵。


网络安全
国家 / 地区
IP 地址
系统安全
升级固件
禁用 SSH
终端安全
分机注册
账号锁定
注册凭证
同时注册数
用户代理
IP 地址
分机登录
账号锁定
单点登录
双因素身份验证
二维码 / 链接登录
密码
用户角色
外线通话安全
呼出路由
PIN 码
时间条件
国家 / 地区
电话号码
呼叫频率
通话并发
通话时长
应急方案
事件通知和记录
备份
系统安全
网络安全
终端安全
呼出安全
应急方案

系统安全

系统安全

系统安全是多层安全策略的第一道防线，为电话系统提供基本保护，有效防范已知的恶意攻击和安全漏洞。你可以通过 **升级固件** 和 **禁用 SSH** 来增强系统安全。

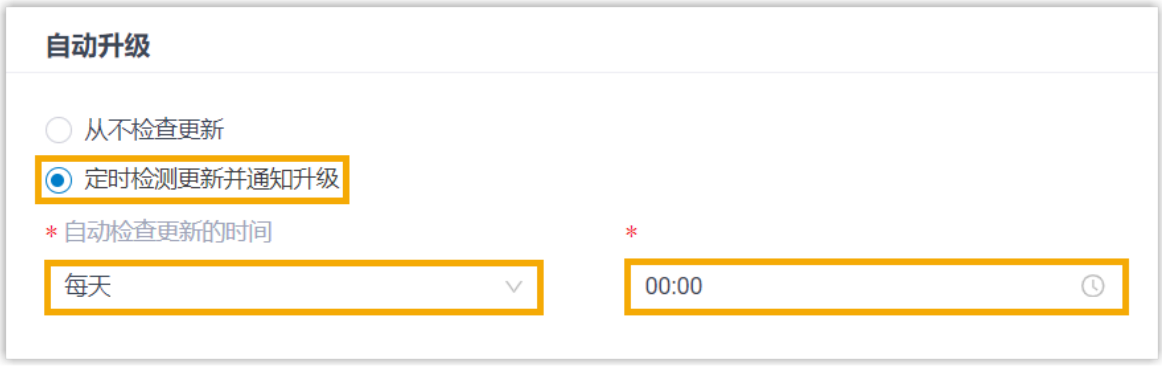
升级固件

通常情况下，固件版本越新，安全性越高，因为新版本总是不断修复安全漏洞以减少安全威胁。此外，随着技术的不断发展，新版本会引进新的安全补丁、安全策略、防御机制等。出于安全考虑，保持 PBX 固件更新至关重要。

你可以设置固件自动检测，并手动升级到新版本。

1. 进入 **维护 > 升级**。
2. 在 **自动升级** 栏，选择 ，并指定频率和时间。

> **注：**
> 建议在非工作时间升级，以免 PBX 服务中断。



3. 点击 **保存** 并 **应用**。

禁用 SSH

黑客经常不断扫描 SSH 服务器，并在几秒钟内重复尝试数千个用户名和密码组合，直到获得服务器的访问权限。 一旦黑客获得访问权限，他们就可以利用获取到的信息进行电话盗打或其他恶意行为。 为防止出现这种情况，我们建议你禁用 SSH，并仅在需要排查问题时启用 SSH。

要禁用 SSH，进入 **安全 > 安全设置 > 控制台/SSH访问**，关闭 **SSH通道** 的开关。

网络安全

网络安全

网络安全是多层安全策略的第二道防线，它的作用在于监控入站流量，并根据预定义的安全规则允许或阻止入站流量。你可以通过 **允许的国家 IP** 和 **IP 允许名单** 增强网络安全。

基于国家 / 地区限制访问 PBX

根据地理位置限制特定国家或地区访问 PBX。PBX 将仅允许来自信任的地理位置的访问，并自动拒绝其他区域的访问。

要设置基于地理位置限制访问，执行以下操作：

1. 进入 **安全 > 安全设置 > 允许的国家IP**。
2. 打开 **启用国家地区IP访问防御** 开关。

> **重要：**
> 如果出现弹窗，你必须确认授权你所在国家或地区的访问，否则你将无法访问你的电话系统。

3. 在右上角的搜索框中，搜索你要允许访问的国家或地区，并在 **操作** 栏打开开关。

4. 点击 **应用**。

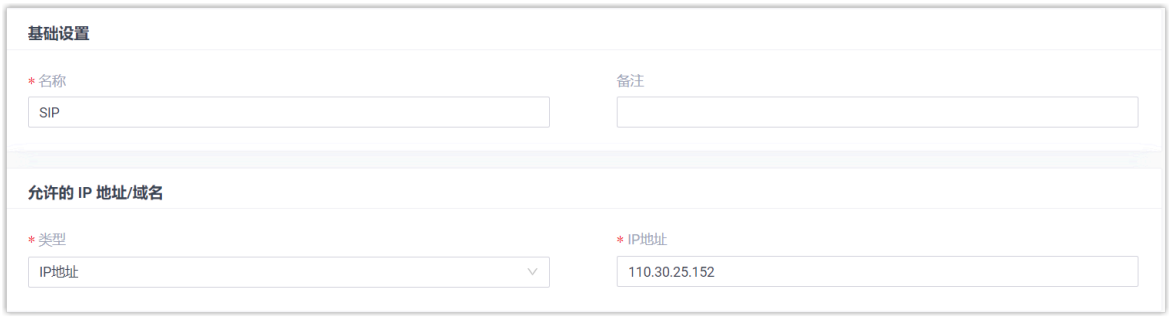
允许指定 IP 地址访问 PBX

Yeastar P 系列云 PBX 内置多条规则来保护可信连接 (如与自动配置设备和 Yeastar 服务的连接)，并通过监控指定时间内发送到特定端口的数据包数量来识别并防御未知威胁。

为防止你信任的设备因发送过多数据包而被误拉黑，你可以将信任的设备地址添加到白名单中。 PBX 将始终接受受信任设备的连接。

1. 登录 PBX 管理网页，进入 **安全 > 安全规则**。

2. 在 **IP允许名单** 页签下，点击 **添加**，添加自定义规则。



3. 点击 **保存** 并 **应用**。

终端安全

分机注册安全

终端安全是多层安全策略中的第三道防线，防止攻击者注册、登录分机账号。Yeastar P 系列云 PBX 内置防御规则，通过监控 SIP 分机的 **注册尝试次数** 防止恶意注册。你也可以通过限制 **注册凭证**、 **同时注册数**、**用户代理**、 以及 **IP 地址** 来增强分机注册安全。

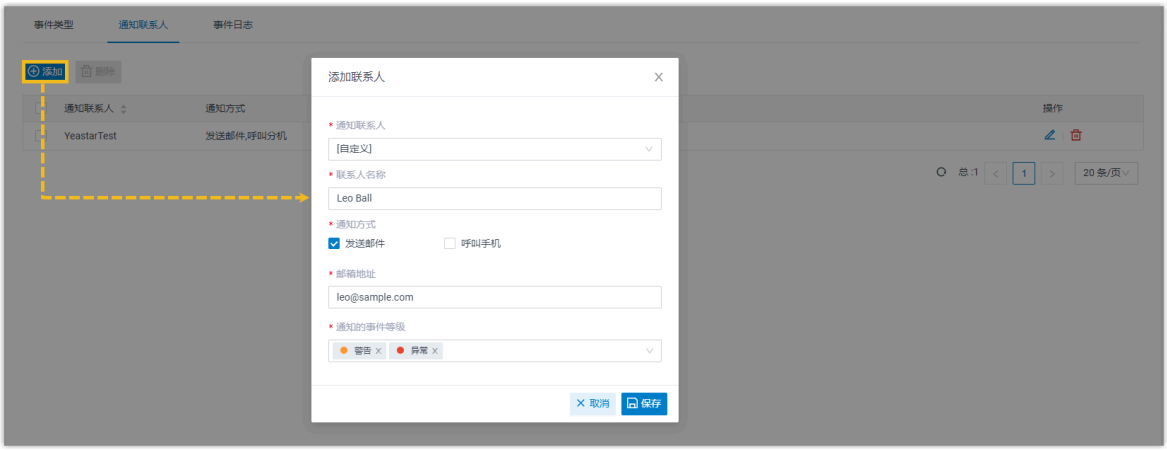
多次注册失败账号锁定

Yeastar P 系列云 PBX 内置账号锁定规则，当同一 IP 地址的注册失败次数达到上限后，系统会自动锁定账号，从而防止恶意注册。当账号被锁定时，PBX 会拉黑源 IP 地址，将此地址显示在 **IP 禁止名单** 中，并发送 **分机注册被锁定** 的事件通知给相关联系人。

为确保你能在账号锁定时及时收到通知，你需要启用事件通知，并设置接收通知的联系人。

1. 进入 **系统 > 事件通知**。
2. 在 **事件类型** 页签下，启用 **分机注册被锁定** 通知。

3. 在 **通知联系人** 页签下，添加联系人，用于接收事件通知。



收到事件通知后，你可以在 PBX 网页上查看详情 (路径：**安全 > 安全规则 > IP 禁止名单**)。

使用复杂的 SIP 注册凭证

简单的 SIP 注册凭证易给攻击者留下可乘之机。因此，需要设置复杂的名称和密码来保护分机的注册安全。

1. 进入 **分机和中继 > 分机**，编辑分机。
2. 在 **分机信息** 栏，设置复杂的认证名称和注册密码。

> **提示：**
> 以下是关于复杂凭证的一些建议：
> - 至少 10 个字符长。
> - 大写字母、小写字母和数字的组合。
> - 不包括 4 个重复或连续的数字。
> - 不包括分机号码或分机名称。

3. 点击 **保存** 并 **应用**。

限制分机的最大注册设备数

Yeastar P 系列云 PBX 默认允许 1 个分机注册到 1 台设备上。除非你确实需要将 1 个分机注册到多台设备上，否则不要更改此限制规则。如需更改，可参考以下说明，增加分机的同时注册数上限：

1. 进入 **分机和中继 > 分机**，编辑分机。
2. 在 **分机信息** 栏，从 **IP 话机同时注册数** 下拉列表中选择一个值。

3. 点击 **保存** 并 **应用**。

基于用户代理限制分机注册

通过验证用户代理来限制分机注册。当 SIP 话机发送注册包到 PBX 时，注册包会包含用户代理 (User Agent) 字段，该字段必须与预设值一致，否则注册会失败。

要基于用户代理限制分机注册，执行以下操作：

1. 进入 **分机和中继 > 分机**，编辑分机。
2. 在 **安全** 页签下，勾选 **启用用户代理注册认证**，设置用户代理。

3. 点击 **保存** 并 **应用**。

基于 IP 地址限制分机注册

只允许信任的 IP 地址注册分机。这样一来，当未受信的 IP 地址发起注册请求时，系统将丢弃请求，从而防止未经授权的注册。

要基于 IP 地址限制分机注册，执行以下操作：

1. 进入 **分机和中继 > 分机**，编辑分机。
2. 在 **安全** 页签下，勾选 **启用 IP 地址限制**，并添加允许的 IP 地址。

3. 点击 **保存** 并 **应用**。

分机登录安全

终端安全是多层安全策略中的第三道防线，防止攻击者注册、登录分机账号。Yeastar P 系列云 PBX 内置防御规则，通过监控 SIP 分机的 **登录尝试次数** 防止恶意登录。你也可以通过 **单点登录**、**双因素身份验证**、**二维码 / 链接登录**、**密码**、**账号锁定** 和 **用户角色** 增强分机的登录安全。

多次登录失败账号锁定

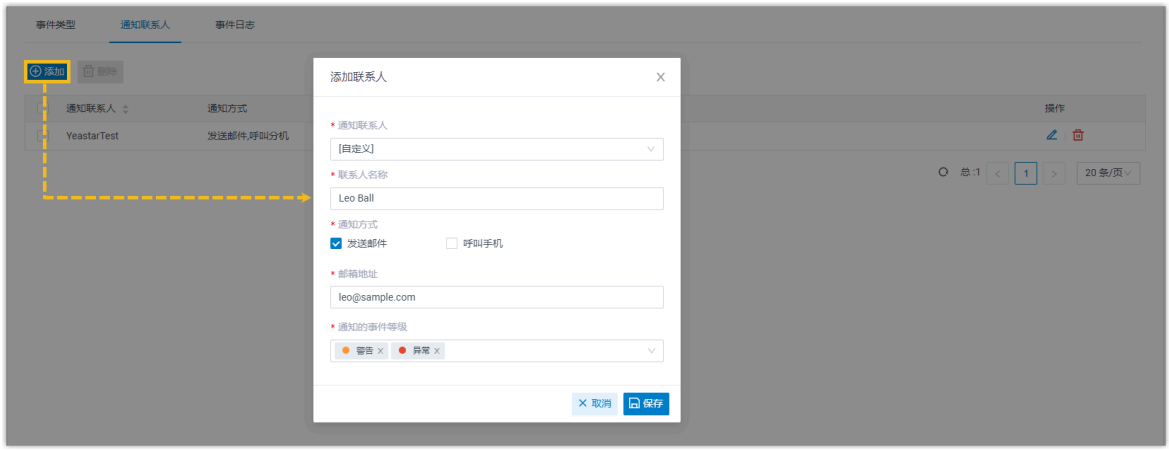
Yeastar P 系列云 PBX 内置账号锁定规则，用于防止他人未经授权访问 PBX 管理网页和 Linkus 客户端：

- 如果某一 IP 地址达到特定时间允许的登录尝试失败次数上限，系统将暂时禁止此地址的登录。
- 如果此 IP 地址达到允许的登录尝试失败次数上限，系统将永久禁止此地址登录此账号，并拉黑此地址，将其显示在 **IP 禁止名单** 中，然后发送 **网页用户被锁定** 或 **Linkus 用户登录被锁** 的事件通知给相关联系人。

为确保你能在 IP 地址被拉黑时收到通知，你需要启用事件通知，并设置接收通知的联系人。

1. 进入 **系统 > 事件通知**。
2. 在 **事件类型** 页签下，启用 **网页用户被锁定** 和 **Linkus 用户登录被锁** 通知。

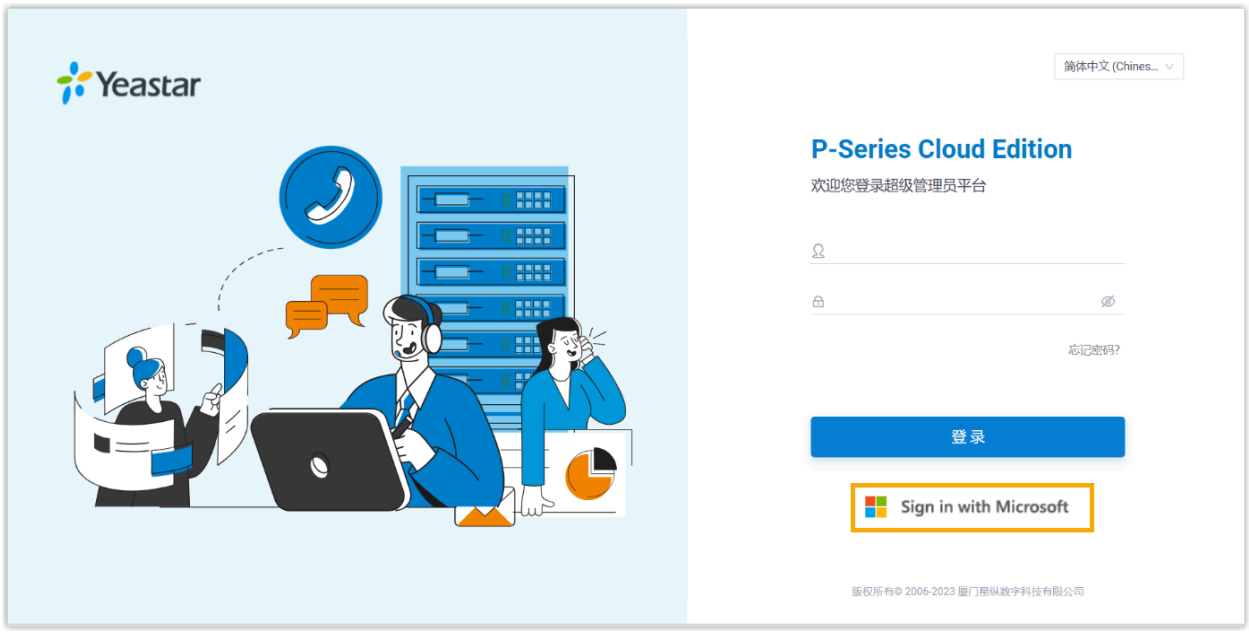
3. 在 **通知联系人** 页签下，添加联系人，用于接收事件通知。



收到事件通知后，你可以在 PBX 网页上查看详情 (路径：**安全 > 安全规则 > IP 禁止名单**)。

通过单点登录 (SSO) 实现第三方身份验证

集成 Yeastar P 系列云 PBX 与 **Microsoft 365** 后可实现单点登录，用户可以通过 Microsoft 账号登录 Linkus UC 客户端。此功能减少用户需要记住的登录凭证数量，此外，Microsoft 的多因素验证将进一步保障账号安全。



要允许用户使用 Microsoft 365 帐户登录 Linkus 客户端，你需要将 PBX 与 Azure Active Directory 或 Active Directory 集成，并启用单点登录。 关于如何集成，请参见 Azure AD 集成手册 和 活动目录 (AD) 集成手册。

通过双因素身份验证 (2FA) 增强安全性

双因素身份验证要求提供两个认证因素才能登录账号，从而为账号提供额外的安全保护。第一个认证因素是用来登录账号的密码，第二个认证因素是发送到指定设备的验证码。

分机用户可在 **Linkus 网页端** 或 **Linkus 桌面端** 上选择通过在手机上安装身份验证器或通过邮件启用双因素身份验证。启用后，登录账号时需要提供账号密码和验证码。关于如何在 Linkus 客户端上启用双因素身份验证，请参见 在 Linkus 网页端上启用双因素身份验证 和 在 Linkus 桌面端上启用双因素身份验证。

> **注：**
> 你也可以为你的超级管理员账号启用双因素身份验证。更多信息，请参见 设置通过身份验证器进行双因素身份验证 或 设置通过邮件进行双因素身份验证。

通过二维码 / 链接免密登录

登录 Linkus 时，通过二维码或链接登录比传统的密码登录方式更安全，因为二维码和链接经过加密且只能使用一次。

你可以通过以下方式发送 Linkus 登录二维码 / 链接给用户：

为单个用户提供登录二维码 / 链接

1. 进入 **分机和中继 > 分机**，编辑分机。

2. 在 **Linkus 客户端** 页签下，点击 **登录二维码** 或 **PC 登录链接**，复制登录凭证并发送给用户。

为多个用户提供登录二维码 / 链接

1. 进入 **分机和中继 > 分机**，编辑分机。
2. 勾选分机，然后点击 **欢迎邮件**。

使用高强度的登录密码

使用弱密码易给攻击者留下可乘之机。如果用户需要手动登录 Linkus 客户端，建议设置高强度的登录密码。

1. 进入 **分机和中继 > 分机**，编辑分机。
2. 在 **用户信息** 栏，设置高强度的用户密码。

提示：

以下是关于强密码的一些建议：

- 至少 10 个字符长。
- 大写字母、小写字母和数字的组合。
- 不包括 4 个重复或连续的数字。
- 不包括分机号码或分机名称。

3. 点击 **保存** 并 **应用**。

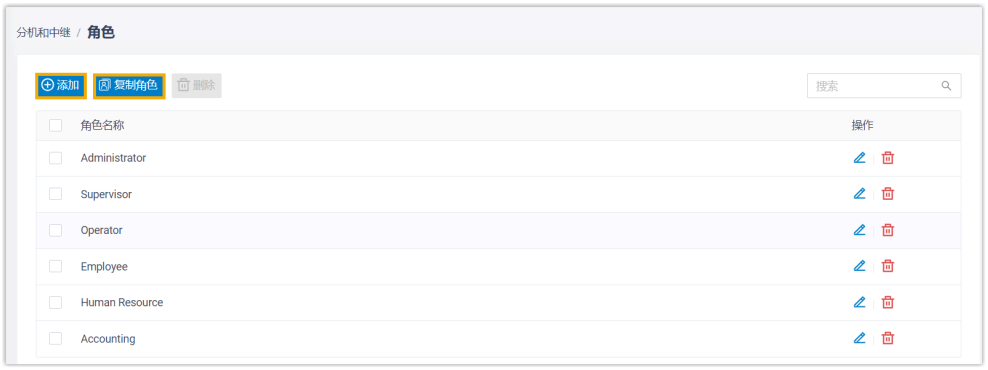
通过用户角色实现精细访问权限控制

基于角色的访问控制可根据用户在组织中的角色授予或限制用户的系统访问权限。有效的访问控制保证用户只能执行授权的管理操作，禁止用户访问未经授权的敏感信息或执行未经授权的管理操作。

Yeastar P 系列云 PBX 内置多个用户角色：**Super Administrator**、**Administrator**、**Supervisor**、**Operator**、**Employee**、**Human Resource** 和 **Accounting**。你可以将默认角色分配给员工，无需其他额外配置，也可以创建自定义角色，并设置权限。

创建自定义角色

1. 进入 **分机和中继 > 角色**。
2. 点击 **添加** 创建新角色，或者点击 **复制角色** 基于现有角色进行创建。



为用户分配角色

1. 进入 **分机和中继 > 分机**，编辑分机。
2. 在 **用户信息** 栏，从 **用户角色** 的下拉列表中选择一个角色。

3. 点击 **保存** 并 **应用**。

外线通话安全

外线通话安全

外线通话安全是多层安全策略的最后一道防线，根据预定义的安全规则限制 Yeastar P 系列云 PBX 的外线通话，在发生电话盗打的情况下可帮助你最大程度降低损失。你可以通过限制 **呼出路由使用权限**、**PIN 码**、**时间条件**、**国家 / 地区**、**电话号码**、**呼叫频率**、**通话并发** 和 **通话时长** 来增强外线通话安全。

基于呼出路由使用权限限制外线呼叫

企业员工职责分工不同，所需的呼叫权限也不同。为电话系统配置呼出规则时，建议为不同中继 (本地市话、国内长途、国际长途) 配置不同呼出路由，并仅为有需要的员工分配呼出路由的使用权限。

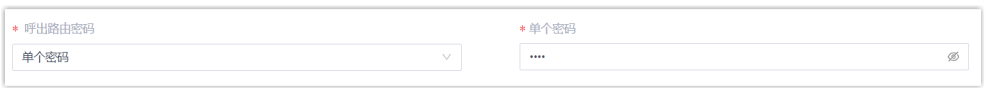
基于 PIN 码限制外线呼叫

为呼出路由设置密码，要求主叫呼叫前必须输入一个 PIN 码。只有当主叫输入正确的 PIN 码时，才能通过此呼出路由发起呼叫。

你可以为呼出路由设置单个 PIN 码或多个 PIN 码。

为呼出路由设置单个 PIN 码

1. 进入 **呼叫控制 > 呼出路由**，编辑呼出路由。
2. 在 **呼出路由密码** 下拉列表中，选择 **单个密码** 并设置一个密码。

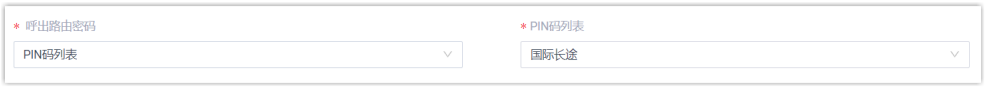


3. 点击 **保存** 并 **应用**。

为呼出路由设置多个 PIN 码

1. 进入 **呼叫功能 > PIN 码列表**，创建一个 PIN 码列表。

2. 进入 **呼叫控制 > 呼出路由 > 呼出路由密码**，绑定呼出路由和 PIN 码列表。

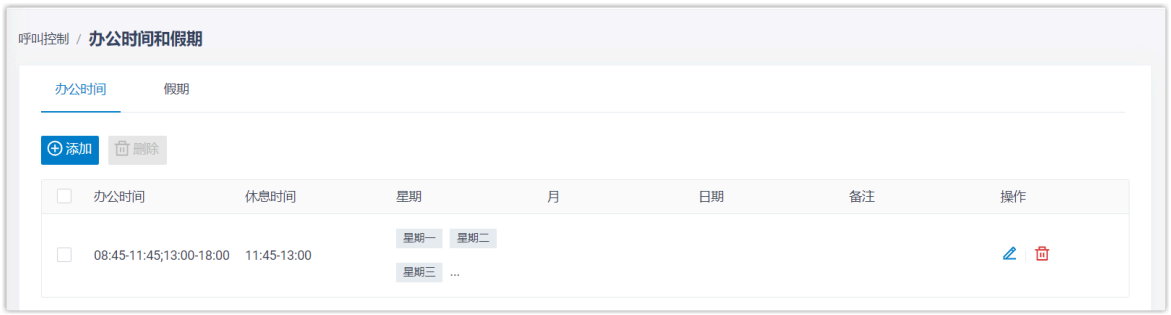


3. 点击 **保存** 并 **应用**。

基于时间条件限制外线呼叫

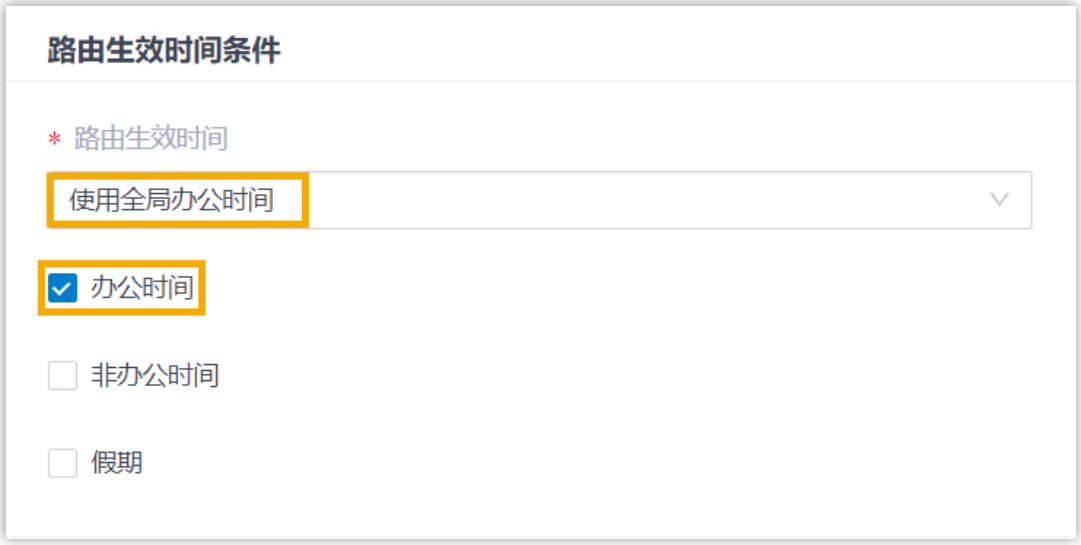
攻击者通常在无人值守期间攻击电话系统，如下班时间、周末或节假日。你可以针对不同时间段设置不同的呼出规则。例如，你可以创建一个 “办公时间” 的时间条件，通过将此时间条件应用到呼出路由，来限制用户只能在办公时间拨打外线电话。示例操作如下：

1. 进入 **呼叫控制 > 办公时间和假期**，创建时间条件。



2. 应用时间条件到呼出路由。

a. 进入 **呼叫控制 > 呼出路由**。
b. 在 **路由生效时间条件** 栏，选择一个时间条件来限制使用呼出路由呼出的时间。



c. 点击 **保存** 并 **应用**。

注：
有关 **时间条件** 的详细介绍和配置说明，请参见 办公时间和假期概述。

基于国家 / 地区限制外线呼叫

如果企业业务有国际往来，且员工需要通过电话与合作伙伴或客户沟通，你可以在 PBX 上配置国际拨号。但是，这会带来国际电话盗打的安全隐患，可能给你造成巨大损失。

为降低盗打风险，我们建议你仅为需要拨打国际电话的用户分配呼叫权限，并且仅允许呼叫到你信任的国家或地区。

1. 为用户分配国际拨号权限。
   a. 进入 **分机和中继 > 分机**，编辑分机。
   b. 在 **安全** 页签下，取消勾选 **禁止呼叫国际长途**。

c. 点击 **保存** 并 **应用**。

2. 允许呼叫指定国家或地区的号码。

a. 进入 **安全 > 安全设置 > 允许呼叫的国家地区**。

b. 启用 **启用国家/地区号码呼叫防御**。

c. 在 **国际拨号代码** 栏，输入你所在国家 / 地区的国际电话拨号前缀。

d. 在 **操作** 列，启用所需的国家或地区。

3. 确保至少有一条匹配国际拨号代码的呼出路由，且允许分机用户使用此路由呼出。

基于电话号码限制外线呼叫

攻击者入侵电话系统后，通常会向高收费号码发起大量呼叫。最终，攻击者通过盗打电话获利，而你将遭受经济损失。建议限制呼叫此类高收费号码。你可以通过限制呼叫具体号码或特定号码模式实现此目的。

1. 进入 **呼叫功能 > 禁止/允许号码 > 禁止号码**。
2. 点击 **添加**，添加禁止用户呼叫的电话号码。

> **提示：**
> 你可以输入具体号码或特定号码模式。关于号码模式的详细介绍，请参见 号码模式。

3. 点击 **保存** 并 **应用**。

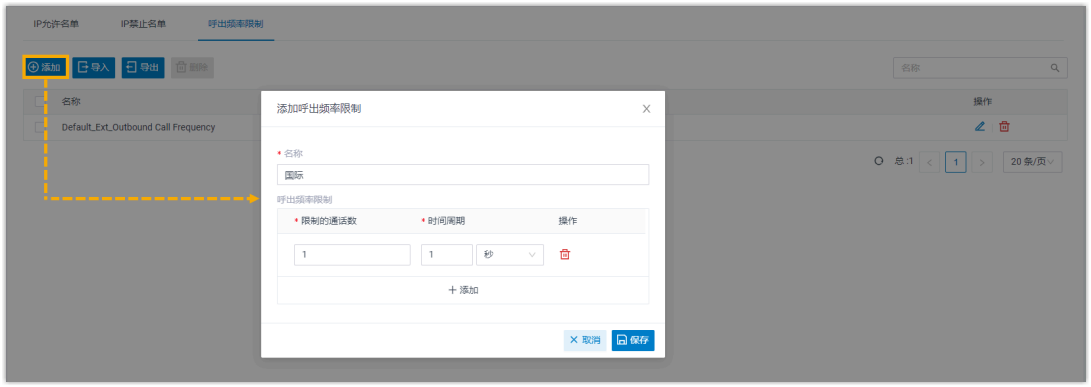
基于呼叫频率限制外线呼叫

限制分机用户在一定时间内可拨打的外线电话数量。 达到限制后，此分机不能再发起外线呼叫。

Yeastar P 系列云 PBX 内置默认规则，限制每个分机用户每秒最多能拨打 5 通外线电话。 你可以使用默认规则，也可以自定义规则并将其与特定分机用户绑定。

1. 创建自定义规则。

a. 进入 **安全 > 安全规则 > 呼出频率限制**。
b. 点击 **添加**，添加自定义规则。



c. 点击 **保存**。

2. 将此规则与分机用户绑定。
a. 进入 **分机和中继 > 分机**，编辑分机。
b. 在 **安全** 页签下，从 **呼出频率限制** 的下拉列表中选择自定义的规则。

c. 点击 **保存** 并 **应用**。

基于通话并发限制外线通话

限制 SIP 中继的同时通话数，防止攻击者无限制地通过中继大量拨打电话。

1. 进入 **分机和中继 > 中继**，编辑 SIP 中继。
2. 在 **高级** 页签下，在 **最大通话并发数** 字段中填写或选择一个值。

3. 点击 **保存** 并 **应用**。

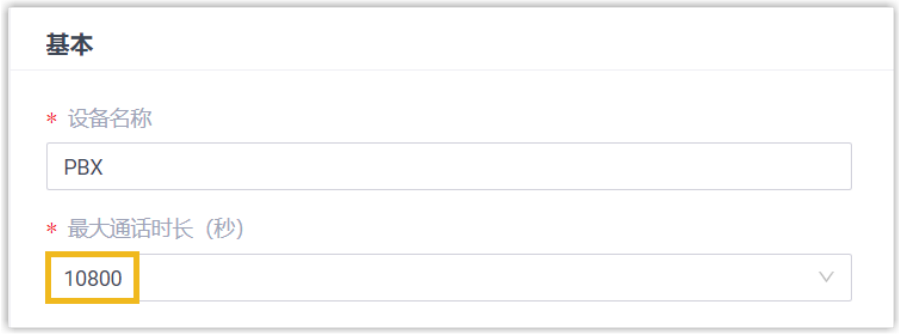
基于通话时长限制外线通话

限制外线通话时长，到达指定时间后系统会自动挂断通话。此方式可有效防止通信资源滥用，帮助你控制通话费用。

你可以设置全局的最大通话时长，也可以为分机用户自定义。

限制所有用户的呼出通话时长 (全局设置)

1. 进入 **PBX 设置 > 常规设置**。
2. 在 **基本** 栏，在 **最大通话时长 (秒)** 字段中填写或选择一个值。



3. 点击 **保存** 并 **应用**。

限制特定用户的呼出通话时长 (单个用户设置)

1. 进入 **分机和中继 > 分机**，编辑分机。
2. 在 **安全** 页签下，在 **最大通话时长 (秒)** 字段中填写或选择一个值。

3. 点击 **保存** 并 **应用**。

应急方案

应急方案

虽然有多种防御方法可以保护 PBX 免受攻击或渗透，但仍可能存在安全漏洞。因此，你需要制定应急方案，以便在攻击者成功渗透 PBX 或攻击 PBX 导致其出现故障时，能够及时、有效地采取应对措施。你可以通过 **事件通知和日志** 实时监控并接收关键事件通知，通过 **备份** 备份数据和配置，确保在系统故障或数据丢失时能快速恢复。

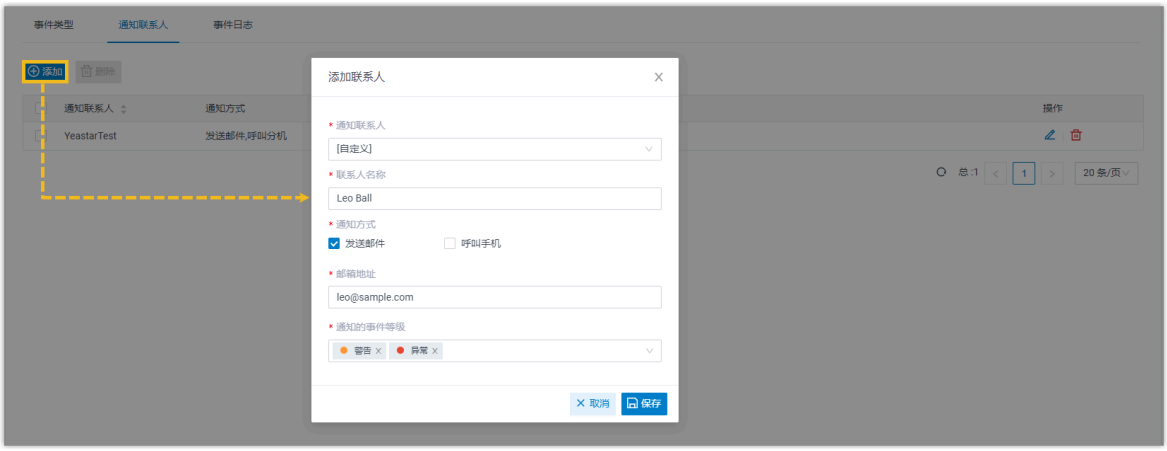
事件通知和日志

Yeastar P 系列云 PBX 支持监控和记录系统事件，并在事件发生时通知相关联系人。

你可以选择要监控的事件，并设置接收事件通知的联系人、发送通知的方式 (发送邮件、呼叫分机或呼叫手机) 以及要发送的内容。

1. 进入 **系统 > 事件通知**。
2. 在 **事件类型** 页签下，启用事件通知，并按需自定义事件等级和通知邮件模板。

3. 在 **通知联系人** 页签下，添加联系人，用于接收事件通知。



收到事件通知后，你可以在 PBX 网页上查看详情 (路径：**系统 > 事件通知 > 事件日志**)。

注：
有关 **事件通知和日志** 的详细介绍和配置说明，请参见 事件通知概述。

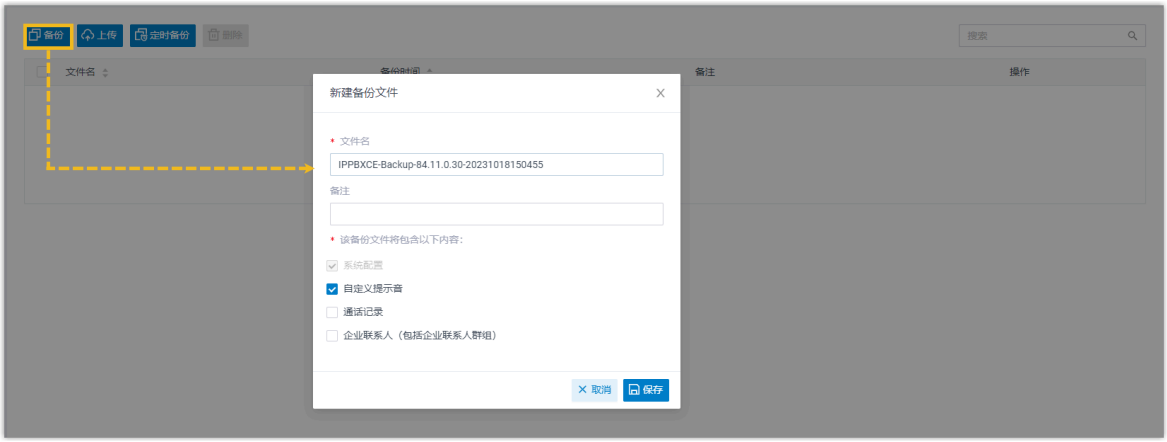
备份

Yeastar P 系列云 PBX 支持备份 PBX 的数据和配置。系统故障时，这将帮助你最大限度地减少停机时间和数据丢失，保证业务连续性。

你可以按需设置自动备份或手动备份。

1. 进入 **维护 > 备份和还原**。
2. 要设置自动备份，点击 **定时备份**，设置并保存此备份任务。

3. 要手动备份，点击 **备份**，选择要备份的数据和配置，并保存此任务。



注：
有关 **备份** 的详细介绍和配置说明，请参见 备份和还原概述。