

# 系统安全设置建议

适用范围

产品型号：S 系列

软件版本：30.4.0.25 或以上

硬件版本：任意

安全设置：

1. 分机设置复杂注册密码，比如使用随机密码（不要使用有规则的密码）

2. 设置复杂登录密码, linkus 使用登录密码的，开启 Linkus 后一定要自行改成自己的密码

**编辑分机 ( 1008 )**

基本    功能    高级    呼叫权限

**常规**

分机类型:  SIP     IAX     FXS

分机: 1008    显示号码: 1008

注册名称: 1008    注册密码: Jsqpds45

同时注册数: 1

**用户信息**

姓名: 1008    用户密码: .....

邮箱地址:    手机号码: 用户登录密码，默认为“pass”+分机号。

提示音语言: 系统默认值

**char中间件**

模式: 普通分机

保存    取消

3. 使用 UDP 非 5060 端口，比如改成 5566，不要开启 TCP

1) 如果路由器支持 5566 映射到内网端口 5060，则这样配置：

常规设置    特征码    语音信箱    **SIP**    IAX    二次开发接口

常规    NAT    编解码    TLS    会计定时器    QoS    T.38    高级    抖动缓冲

UDP端口: 5060     TCP端口: 5060

RTP端口: 28000 -- 30000     本地SIP端口: 5062 -- 5082

**配置**

分机    中继    呼叫控制    呼叫功能    提示音    **常规设置**    录音    紧急号码

常规设置    特征码    语音信箱    **SIP**    IAX    二次开发接口

常规    **NAT**    编解码    TLS    会计定时器    QoS    T.38    高级    抖动缓冲

NAT类型: 公网IP地址

公网IP地址: 110.87.98.11    5566

本地网络地址: 192.168.0.0 / 255.255.0.0

NAT模式: Yes

2) 如果路由器不支持端口 5566 映射到内网 5060，那么这样改：

常规设置 特征码 语音信箱 SIP IAX 二次开发接口

常规 NAT 编解码 TLS 会话计时器 QoS T.38 高级 抖动缓冲

UDP端口: 5566  TCP端口: 5060

RTP端口: 28000 -- 30000  本地SIP端口: 5062 -- 5082

注册时间

常规设置 特征码 语音信箱 SIP IAX 二次开发接口

常规 NAT 编解码 TLS 会话计时器 QoS T.38 高级 抖动缓冲

NAT类型: 公网IP地址

公网IP地址: 110.87.98.11 : 5566

本地网络地址: 192.168.0.0 / 255.255.0.0 +

NAT模式: Yes

3. 设置防火墙，以下是默认配置，如果更改了 SIP 端口（默认 5060，比如改成 5566），那么以下防火墙的 5060 端口也应该改成 5566，如图：

默认：

配置 防火墙规则 IP自动防御 服务 证书 数据库授权

自动防御规则 IP黑名单

端口	协议	速率	编辑	删除
<input type="checkbox"/> 5060	UDP	120/60s	<a href="#">编辑</a>	<a href="#">删除</a>
<input type="checkbox"/> 5060	UDP	40/2s	<a href="#">编辑</a>	<a href="#">删除</a>
<input type="checkbox"/> 8022	TCP	10/60s	<a href="#">编辑</a>	<a href="#">删除</a>
<input type="checkbox"/> 5062:5082	UDP	120/60s	<a href="#">编辑</a>	<a href="#">删除</a>

修改成：

配置 防火墙规则 IP自动防御 服务 证书 数据库授权

自动防御规则 IP黑名单

端口	协议	速率	编辑	删除
<input type="checkbox"/> 5566	UDP	120/60s	<a href="#">编辑</a>	<a href="#">删除</a>
<input type="checkbox"/> 5566	UDP	40/2s	<a href="#">编辑</a>	<a href="#">删除</a>
<input type="checkbox"/> 8022	TCP	10/60s	<a href="#">编辑</a>	<a href="#">删除</a>
<input type="checkbox"/> 5062:5082	UDP	120/60s	<a href="#">编辑</a>	<a href="#">删除</a>

4. 设置 useragent，每个注册终端都会提交 useragent 名称，比如亿联话机是 yealink，朗视的设备是 yeastar，如图设置，这个账号只有亿联或朗视的设备可以注册上来。

编辑分机 (1008)

基本 功能 高级 呼叫权限

NAT  Qualify

远程注册  语音加密 (SRTP)

支持T.38 DTMF模式: RFC4733

协议: UDP

启用户代理注册认证

用户代理: yealink

用户代理: yeastar

**IP地址限制**

启用IP地址限制

允许的IP/子网掩码: /

保存 取消

4. 只允许指定的 IP（或范围）可以注册这个账号

编辑分机 (1008)

基本 功能 高级 呼叫权限

NAT  Qualify

远程注册  语音加密 (SRTP)

支持T.38 DTMF模式: RFC4733

协议: UDP

启用户代理注册认证

用户代理: yealink

用户代理: yeastar

**IP地址限制**

启用IP地址限制

允许的IP/子网掩码: 192.168.9.0 / 255.255.255.0

保存 取消

5. 不要开启 SSH FTP，系统默认是没有开 SSH 和 FTP 的，如果有调试需求会开，调试完毕后要记得关闭，如果有长期的开启需求切记不要把这些端口映射到外网，或者设置更强更长的密码（SSH 和 FTP 使用的同一个账号密码）：



6. 如果有使用 Auto-P, 建议关闭 WAN 口的 TFTP 访问

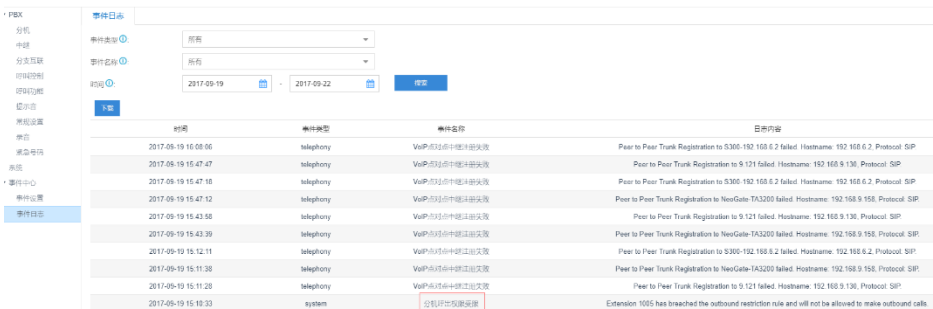
7. 进入 Call control 的 outbound Restriction 中设置分机的呼出限制（30.6.0.x 自动增加一条规则：1 分钟内只允许拨打 5 通外线，超过会被限制），客户可以依据实际需求做修改。

如果话机呼出外线太频繁（超过限制），分机会被限制呼出

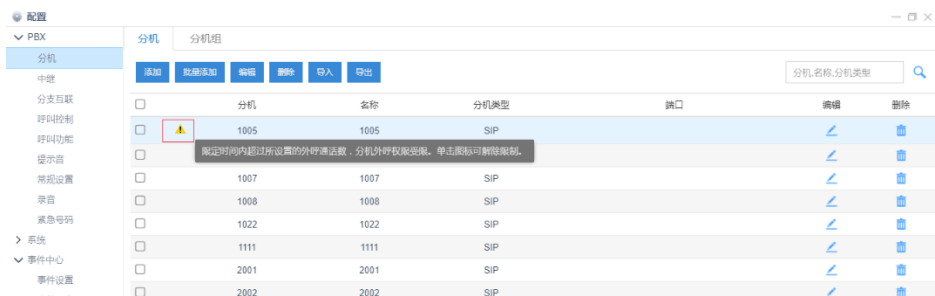


呼叫限制的现象：

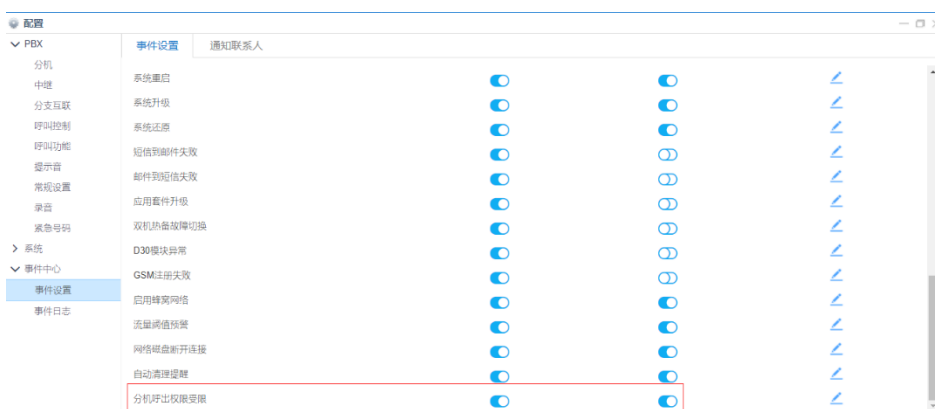
事件记录：



分机状态，可以直接点击“！”解除限制：



8. 事件通知，一定要设置好通知：



9. 终极：外线不要开通国际长途。