PortSIP® PBX 用户手册

商标信息

PortSIP® 以及与 PortSIP 产品相关的名称和标记均为博瞻信息技术有限公司的商标及/或服务标记，是该公司在中国，美国及其他国家或地区的注册及/或普通法商标。其他所有商标均为其各自所有者的资产。未经博瞻信息明确书面许可，不得将此文件的任何部分以任何方式进行复制或转载。

专利信息

随附产品受中国、美国和其它国家/地区的一项或多项专利或博瞻信息技术有限公司正在申请的专利所保护。

免责声明

由于某些国家或地区、州或省不允许对暗示担保有排除或限制，或不允许对提供给消费者的特定产品可能导致的任何意外的、连带性的损失有限制，或不允许对人身伤害的责任有限制，因此上述有关限制或责任排除的规定可能不适用于您。

当不允许将暗示担保整体排除时，它们将仅限于适用书面担保的期限。该担保赋予您可能随当地法律而异的特定法律权利。

博瞻信息

湖南长沙市岳麓区文轩路麓谷企业广场 C2-903

我们致力确保本手册上的信息准确。博瞻信息对印刷错误或笔误概不负责。本文档中的信息可予以更改，恕不另行通知。

目录

1.开始使用 PortSIP PBX

本用户手册将指引你将 PortSIP PBX 部署在 Windows 或 Linux 操作系统环境里，并展示了几个典型的部署方式以适用于不同的应用场景。

1.1 什么是 PortSIP PBX?

PortSIP PBX（也叫 PortPBX）是一个纯软件统一通信系统，支持 Windows 和 Linux 平台。可以与其他基于 SIP 标准实现的 IP 电话、软件电话、SIP 中继以及语音网关等一起组网工作，以比传统硬件 PBX 更低廉的价格和更便捷的管理提供完整的通信解决方案。

PortSIP PBX 不仅仅拥有和传统硬件 PBX 一样的功能，还包括更多新增功能，比如对移动和 WebRTC 的支持。PortSIP PBX 统一通信系统不像传统的 PBX 系统一样需要单独的电话线路，而是直接使用 Internet 或者局域网网络，所有的呼叫都以 IP 数据包的形式在 IP 网络上传输。同时，把 PortSIP PBX 和 VoIP 服务器运营商或者 SIP 中继链接在一起，就可以方便地与 PSTN 网络电话，手机进行通话。也可以使用 VoIP 服务器运营商而不需要通过网关。PortSIP PBX 具有良好的兼容性，能够和绝大多数厂商的 SIP 标准产品一起工作。

1.2 准备工作

Linux 安装先决条件

将 PortSIP PBX 部署在 Linux 的系统环境里，除了需要对 SIP 标准、音视频通话以及 IM 消息有初步的了解之外，还需要熟悉以下相关内容：

主流 Linux 版本

Redhat RHEL（64 位）、CentOS 7 或更高版本（64 位）、Debian 9 或更高版本（64 位）、Ubuntu 14.04 或更高版本（64 位）；

IPtables 和 Firewalld

本手册假定 Linux 操作系统已经安装并正常运行，PortSIP PBX 管理员拥有 Linux root 权限。

Windows 安装先决条件

将 PortSIP PBX 部署在 Windows 的系统环境里，除了需要对 SIP 标准、音视频通话以及 IM 消息有初步的了解之外，还需要熟悉以下相关内容：

Windows 桌面或者服务器操作系统：

Windows 7、Windows 8、Windows 10、Windows Server 2008 R2 + SP1、2012 R2、2016 R2

IPv4/IPv6

Windows 系统防火墙

本手册假定 Windows 操作系统已经安装并正常运行，PortSIP PBX 管理员拥有 Windows 系统管理员权限。

1.3 PortSIP PBX 的软硬件要求

PortSIP PBX 支持如下操作系统

Linux 服务器：

CentOS 7 或更高版本（64 位）； gcc/g++ 6.4 或更高版本

Ubuntu 16.04.4 或更高版本（64 位）； gcc/g++ 6.4 或更高版本

Debian 9.0 或更高版本（64 位）； gcc/g++ 6.4 或更高版本

Windows 桌面系统

Windows 7、8、10，64 位

Windows Server：

Windows Server 2008 R2 + SP1、2012 R2、2016 R2，64 位

重要提示：系统必须已升级到最新版本并安装了所有补丁。

PortSIP PBX 支持如下虚拟平台

为了帮助用户节约成本开支以及提高系统的性能，构造高可用通信系统，PortSIP PBX 支持虚拟化技术，已经在如下虚拟以及云平台上进行过严格测试：

● VMware ESX 5.X 及以上版本

- Linux HyperV
- Microsoft HyperV 2008 R2 及以上版本
- Amazon AWS
- UCloud
- 阿里云
- Linode
- Digital Ocean
- Godaddy VPS 和 云
- 腾讯云

PortSIP PBX 的性能取决于如下几个关键因素：

- PBX 系统需要支持多少路并发通话
- PBX 系统需要支持多少用户同时在线
- 是否对通话进行录音
- 仅对音频录音还是对音视频均录音
- PBX 系统需要支持多少人同时进行语音和视频会议
- PBX 需要支持多少 IVR（Virtual Receptionist）
- PBX 系统需要支持多少呼叫队列（Call Queue）
- PBX 系统需要支持多少振铃组（Ring Group）

基于以上几个关键的需求， PortSIP PBX 可以在从 Intel i3 CPU 到 Inter Xeon 多 CPU 的各种 PC 机以及服务器上顺畅运行。

其他要求

- 最新版本的 Firefox、Google Chrome 或者 IE 浏览器
- 微软 .NET Framework version 4.5 或者更高版本
- 了解 Linux 和 Linux 网络管理
- 熟悉 Windows 和 Windows 网络系统管理
- 与 service.portsip.com 通过端口 6881 的稳定网络连接

- 与 stun.portsip.com 和 stun1.portsip.com 通过端口 3478 的稳定网络连接
- 与 stun4.l.google.com 通过端口 3478 的稳定网络连接

域名 (FQDN) 支持

PortSIP PBX 可以在没有域名的机器上运行，但是我们推荐使用域名。使用域名有如下好处：

- 可以更方便地访问 PortSIP PBX 的管理控制台
- 如果安装 PBX 的机器更换了 IP 地址，使用域名可以让你更方便地管理 IP 电话机和客户端
- 访问管理控制台的时候，可以更方便地启用 HTTPS

你所使用的域名（FQDN）必须能在局域网里正确地解析到安装了 PortSIP PBX 的机器；如果 PortSIP PBX 安装在 Internet 上，那么域名必须能正确解析到安装 PBX 的机器的公网地址。

1.4 获取帮助和技术支持

如果您在安装使用中有任何问题，可随时联系博瞻信息技术支持团队，或者访问我们的知识库获取解决方案。

2.安装 PortSIP PBX

本章提供的内容将指导你如何将 PortSIP PBX 安装到 Windows 和 Linux。

本章包含以下内容：

2.1 下载 PortSIP PBX

你可以在博瞻信息的网站上免费下载最新版本的 PortSIP PBX。PortSIP PBX 分为 Windows 版本和 Linux 版本，只支持 64 位系统。

免费版的 PortSIP PBX 最大支持 3 路并发通话，无用户（分机）数量限制。如果您需要更多的并发通话数量支持，请参阅授权许可章节。

下载完成后，您即可获得安装包。

2.2 在 Linux 上安装 PortSIP PBX

2.2.1 准备 Linux 主机

在安装 PortSIP PBX 之前，必须准备好一台安装了 Linux 操作系统的电脑/服务器，并进行如下操作：

1. 如果你要安装 PBX 的 Linux 电脑/服务器位于局域网里，必须分配一个静态的局域网 IP 地址；如果位于公网，必须得有一个公网静态 IP。
2. 在安装 PortSIP PBX 之前安装所有可用的系统更新和补丁包。
3. 不要在这台电脑上安装 VPN 软件。
4. 确认已经禁用了系统和网络适配器的省电选项（将系统设置为高性能模式）。
5. 不要在主机上安装 TeamViewer VPN 软件。
6. 安装 PortSIP PBX 的主机必须不是 DNS 或 DHCP 服务器。
7. 在防火墙打开如下端口：
   UDP: 33000 – 65000、5078
   TCP: 8800 – 8900、10080、10043
   TCP：6459、5078、5079
8. 确保如下端口没有被其他程序占用

UDP: 33000 – 65000、5078

TCP: 8800 – 8900、10080、10043

TCP：6459、5078、5079

2.2.2 在 Linux 上安装 PortSIP PBX

升级安装

如果您已经安装了 PortSIP PBX 9.4.2 或者更高的版本，那么您只需用如下命令即可直接升级：

1. CentOS 和 RHEL

   *sudo rpm -Uvh **portsip_pbx_xxx.rpm***

   重要提示：在 CentOS/RHEL 上，如果您从 9.4.2/9.4.3/9.4.5 升级到 9.4.6，那么需要在升级完之后，再执行如下命令：

   sudo systemctl enable portsip-pbx.webrtcgw.service

2. Ubuntu 和 Debian

   *sudo dpkg -I **portsip_pbx_xxx.deb***

   安装程序将自动将您当前的版本升级到最新版。

从 PortSIP 9.4.0 升级

PortSIP PBX 9.4.0 的产品名为“portpbx”。从 9.4.2 开始，PortSIP PBX Linux 已重命名为“portsip-pbx”。**因此，如果您已经安装了 9.4.0 并且希望升级到更新版本，请按照以下步骤**：

1. 卸载 9.4.0
   a. CentOS/Redhat：sudo rpm -e portpbx
   b. Debian/Ubuntu：sudo dpkg -P portpbx

2. 卸载完成后，手动删除以下文件夹：

   sudo rm -r /var/lib/portpbx

   sudo rm -r /opt/portsip/pbx

接下来您可按照以下描述的安装步骤安装更新版本。

全新安装

要在 Linux 上全新安装 PortSIP PBX，您仅需要执行以下命令，即可完成安装。

1. CentOS 和 RHEL

   首先确认您的 Linux 已经安装了 uuid, 如果还没有安装，请执行如下命令：

   sudo yum install uuid

   sudo rpm -ivh portsip_pbx_xxx.rpm

2. Ubuntu 和 Debian

   首先确认您的 Linux 已经安装了 uuid, 如果还没有安装，请执行如下命令：

   sudo apt-get install uuid

   sudo dpkg -i portsip_pbx_xxx.deb

安装程序将检测 PortSIP PBX 的依赖关系，您需要根据提示信息安装全部所需的依赖关系。

成功安装后，PortSIP PBX 服务将自动启动，并将在每次启动服务器后自动运行。

如果需要卸载 PortSIP PBX，请执行如下命令：

CentOS 和 RHEL: ***sudo rpm -e portsip-pbx***

Ubuntu 和 Debian: ***sudo dpkg -P portsip-pbx***

要完整删除所有文件夹和文件，请在卸载后执行以下命令：

```
sudo rm -r /var/lib/portpbx
sudo rm -r /opt/portsip/pbx
```

注意：

1. 如果您收到类似“/usr/lib64/libstdc++.so.6: version `GLIBCXX_3.4.21' not found”的错误，即表示 gcc/g++ 版本过旧，您需要更新到最新的 gcc/g++。
2. 如果您收到以下错误：

   ```
   libc.so.6 is needed by portpbx-9.4.0-1.el7.centos.x86_64
   ```

libc.so.6(GLIBC_2.0) is needed by portpbx-9.4.0-1.el7.centos.x86_64

libc.so.6(GLIBC_2.1) is needed by portpbx-9.4.0-1.el7.centos.x86_64

libm.so.6 is needed by portpbx-9.4.0-1.el7.centos.x86_64

libpthread.so.0 is needed by portpbx-9.4.0-1.el7.centos.x86_64

请执行如下命令：

1. *sudo yum list "compat-libstdc*"*
2. 将输出以下内容：
   Available Packages
   compat-libstdc++-33.i686
   compat-libstdc++-33.x86_64

3. 现在执行以下命令：
   sudo yum install compat-libstdc++-33.i686
   sudo yum install compat-libstdc++-33.x86_64

如果您收到以下错误：

libxml2.so.2 is needed by portpbx-9.4.0-1.el7.centos.x86_64
libz.so.1 is needed by portpbx-9.4.0-1.el7.centos.x86_64

请执行以下命令：

sudo yum install libxml2
sudo yum install libxml2-devel
sudo yum install zlib

sudo yum install zlib-devel

2.2.3 配置 Linux 防火墙规则

在成功安装了 PortSIP PBX 之后，必须对 Linux 防火墙进行设置，否则 PBX 将无法正常运行。

如果防火墙拦截了相关端口，必须打开如下端口以使得 PortSIP PBX 正常运行。

UDP 端口：33000-65000。这些端口用于 RTP 传输媒体数据。

TCP 端口：6459、5078、5079、8800 – 8900、10080、10443。这些端口主要用于服务器控制和 WebRTC Gateway 传输。

UDP 端口：5060、5078。这是默认的 UDP 端口，用于传输 SIP 消息，发送和接收 SIP 信令。

如果以后在 PBX 里面增加了新的 SIP 传输协议，同时还需要在防火墙里面打开相对应的端口：

假如在 5063 端口上增加了 TLS 传输协议，必须在防火墙上打开 TCP 协议的 5063 端口。

假如在 5061 端口上增加了 TCP 传输协议，必须在防火墙上打开 TCP 协议的 5061 端口。

假如在 5065 端口上增加了 WS 传输协议，必须在防火墙上打开 TCP 协议的 5065 端口。

假如在 5067 端口上增加了 WSS 传输协议，必须在防火墙上打开 TCP 协议的 5067 端口。

假如在 5068 端口上增加了 UDP 传输协议，必须在防火墙上打开 UDP 协议的 5068 端口。

2.3 在 Windows 系统安装 PortSIP PBX

2.3.1 准备 Windows 主机

在安装 PortSIP PBX 之前，必须准备好一台安装了 Windows 的电脑/服务器，并进行如下操作：

1. 如果你要安装 PBX 的 Windows 电脑/服务器位于局域网里，必须分配一个静态的局域网 IP 地址；如果位于公网，必须得有一个公网静态 IP。
2. 安装所有的 Windows 系统更新和补丁包，在安装更新和服务包的过程中您的电脑可能会重启多次，每次重启后可能要求安装更多的更新。安装期间，需要尤其注意安装所有有关 Microsoft .Net 的更新。完成后即可运行 PortSIP 的安装。
3. 避免让杀毒软件扫描 *C:\Program Files\PortSIP* 目录，以免导致安装 PortSIP PBX 的过程过长以及写入访问延迟。
4. 不要在这台电脑上安装 VPN 软件。
5. 确认已经成功启动了 Windows 防火墙服务。
6. 确认已经禁用了系统和网络适配器的省电选项（将系统设置为高性能模式）。
7. 不要安装 TeamViewer 之类的软件。
8. 如果您使用的是一台 Windows 桌面系统，请禁用蓝牙设备。
9. PortSIP PBX 不能和如下软件安装在同一台电脑上：DNS 或者 DHCP 服务器、MS SharePoint 或 Exchange 服务器。
10. 在你的防火墙里打开如下端口：
    UDP: 33000 – 65000、*5078*
    TCP: 8800 – 8900、*10080*、*10043*
    TCP：6459、*5078*、*5079*
11. 需要确保如下端口没有被其他程序占用
    UDP: 33000 – 65000、*5078*
    TCP: 8800 – 8900、*10080*、*10043*
    TCP：6459、*5078*、*5079*
12. 请确认 Windows 防火墙已经启用

2.3.2 在 Windows 上安装 PortSIP PBX

要安装 PortSIP PBX，您只需要双击安装程序文件，然后根据安装程序的提示进行安装。

PortSIP PBX 的系统服务将在安装成功完成后自动运行，以及在以后每次 Windows 启动后都将自动运行。

2.3.3 配置 Windows 防火墙规则

在成功安装了 PortSIP PBX 之后，必须对 Linux 防火墙进行设置，否则 PBX 将无法正常运行。

在 Windows 控制面板里打开 Windows 防火墙，点击“**允许程序或者功能通过 Windows 防火墙**”>“**浏览**”。

然后选择允许如下程序通过防火墙：

C:\Program Files\PortSIP\PBX\bin\conf.exe

C:\Program Files\PortSIP\PBX\bin\callqueue.exe

C:\Program Files\PortSIP\PBX\bin\mediaserver.exe

C:\Program Files\PortSIP\PBX\bin\pbx.exe

C:\Program Files\PortSIP\PBX\bin\voicemail.exe

C:\Program Files\PortSIP\PBX\bin\vr.exe

C:\Program Files\PortSIP\PBX\bin\ webserver.exe

C:\Program Files\PortSIP\PBX\bin\moh.exe

C:\Program Files\PortSIP\PBX\bin\gateway.exe

C:\Program Files\PortSIP\PBX\bin\webrtcgw.exe

如果防火墙拦截了相关端口，必须打开如下端口以使得 PortSIP PBX 正常运行。

UDP 端口：33000-65000。这些端口用于 RTP 传输媒体数据，包括音视频包。

TCP 端口：6459、5078、5079、8800 – 8900、10080、10443。这些端口主要用于服务器控制和 WebRTC Gateway 传输。

UDP 端口：5060、5078。这是默认的 UDP 端口，用于传输 SIP 消息，发送和接收 SIP 信令。

如果以后在 PBX 里面增加了新的 SIP 传输协议，同时还需要在防火墙里面打开相对应的端口：

假如在 5063 端口上增加了 TLS 传输协议，必须在防火墙上打开 TCP 协议的 5063 端口。

假如在 5061 端口上增加了 TCP 传输协议，必须在防火墙上打开 TCP 协议的 5061 端口。

假如在 5065 端口上增加了 WS 传输协议，必须在防火墙上打开 TCP 协议的 5065 端口。

假如在 5067 端口上增加了 WSS 传输协议，必须在防火墙上打开 TCP 协议的 5067 端口。

假如在 5068 端口上增加了 UDP 传输协议，必须在防火墙上打开 UDP 协议的 5068 端口。

重要提示：如果您是在 AWS 等云平台上运行 PBX，并且云平台具有自己的防火墙，您还必须在云平台防火墙上打开这些端口。

2.4 规避 HTTPS 证书安全警告信息

PortSIP PBX 在 8888 端口监听并提供 HTTP 服务。

假定将 PortSIP PBX 安装在 IP 地址为 172.217.14.16 的服务器上，那么您可以使用 http://172.217.14.16:8888 来访问 PortSIP PBX 的 WEB 管理界面。注意：推荐使用 Chrome 和 Firefox 浏览器，请勿使用 IE 浏览器。

PortSIP PBX 在 8887 端口监听并提供 HTTPS 服务。假定将 PortSIP PBX 安装在 IP 地址为 172.217.14.16 的服务器上，那么您可以使用 https://172.217.14.16:8887 来访问 PortSIP PBX 的 WEB 管理界面。

注意： 推荐使用 Chrome 或者 Firefox 浏览器访问管理界面，不能使用 IE 浏览器。

默认情况下，HTTPS 使用自签名的 SSL 证书，将导致浏览器弹出 SSL 证书安全警告信息。

要避免 SSL 证书警告信息，您需要购买签名的证书（由可信任的证书机构发放的授权证书），替换自签名证书。要执行该操作，请遵循以下步骤：

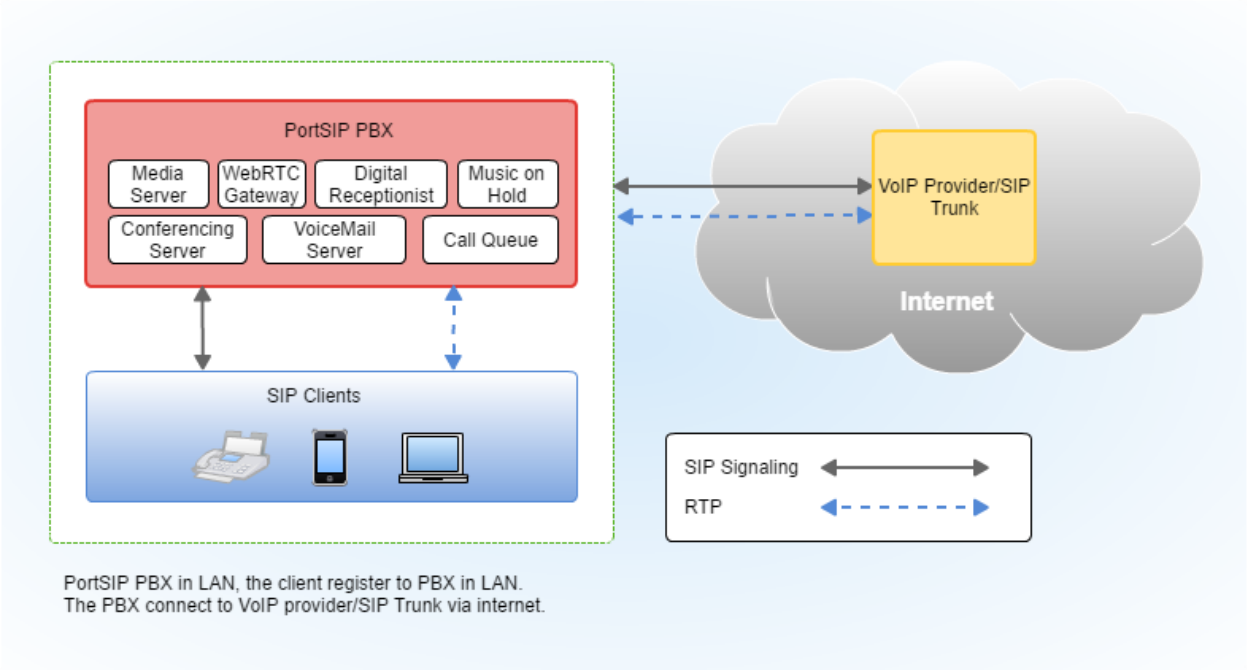
1. 联系 Thawte 或者 Versign 或其他证书提供商，购买 SSL 证书。将私有密钥保存为 **portsip.key**。
2. 在获取到 SSL 证书后，将其重命名为 **portsip.crt**。
3. 在 Linux 上，将 **portsip.key** 和 **portsip.crt** 复制到 PortSIP PBX 安装路径 (*/opt/portsip/pbx/bin*) 以替换现有 **portsip.key** 和 **portsip.crt**。
4. 在 Windows 上，将 **portsip.key** 和 **portsip.crt** 复制到 PortSIP PBX 安装路径 (C:/Program Files/PortSIP/PBX/bin)，替换现有 **portsip.key** 和 **portsip.crt**。
5. 登录到 *https://yourpbx.com:8887*，访问 PBX 管理控制台。

注意：您还可以从 Let's Encrypt 免费获取 SSL 证书。

3.配置部署 PortSIP PBX

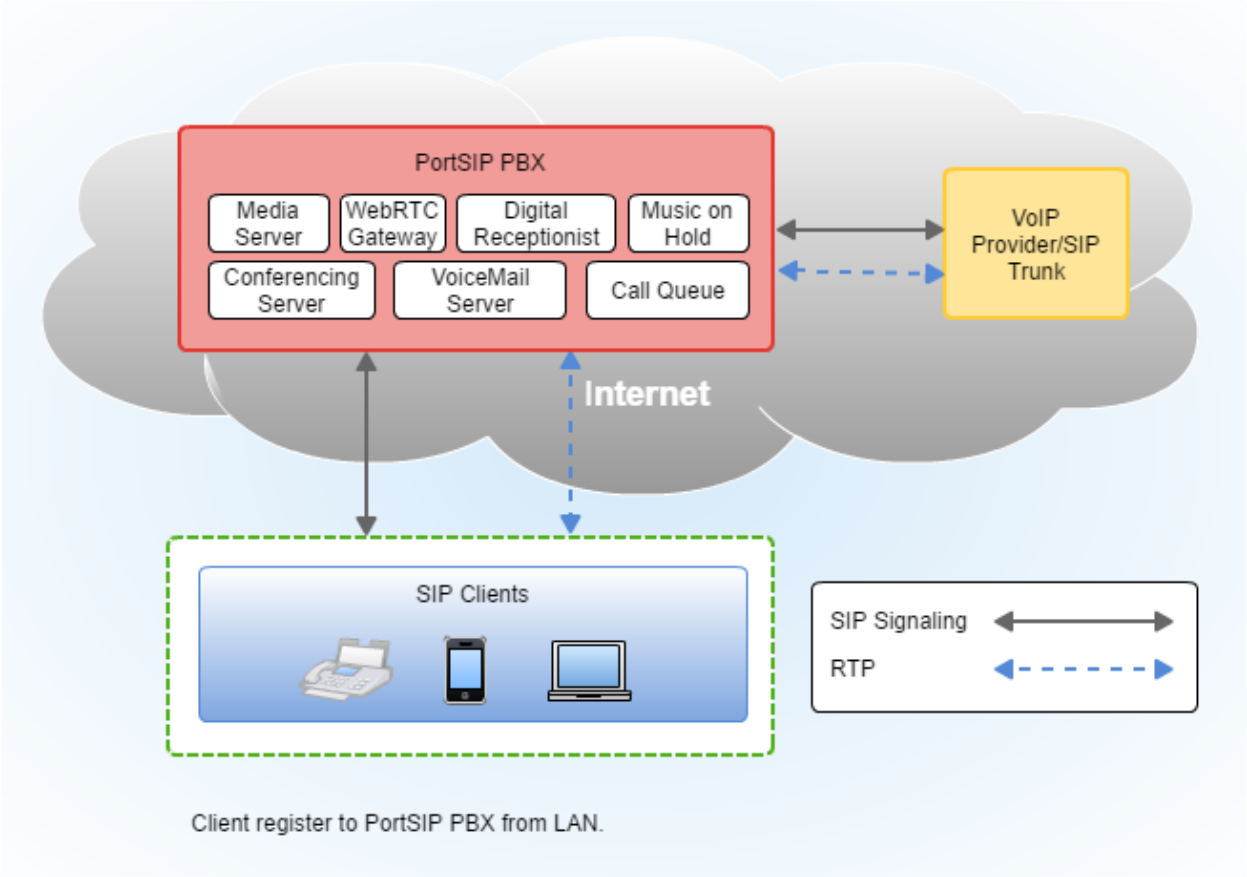
3.1 PortSIP PBX 的架构

图 1：PortSIP PBX 在局域网里的典型架构



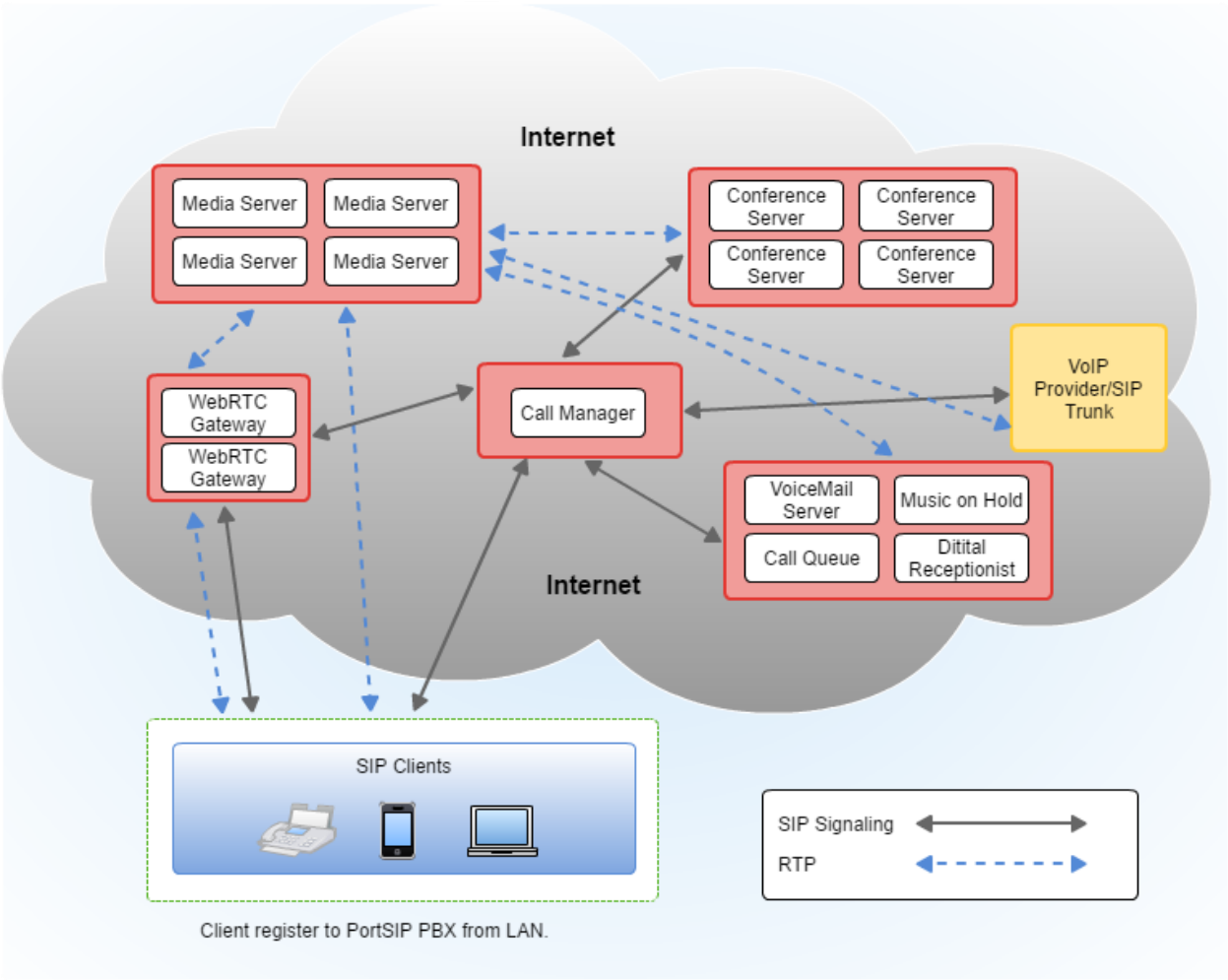
如图 1 所示，PBX 运行在局域网时，分机用户从局域网注册到 PBX，然后分机用户之间可以互相进行呼叫。同时，分机用户通过 PBX 所配置的 VoIP 运营商或者 SIP 中继，可以与传统的 PSTN 网络的固定电话以及手机（中国移动、电信、联通）进行通话。

图 2： PortSIP PBX 在 Internet 上的典型架构



如图 2 所示，PortSIP PBX 部署在 Internet 上面，拥有一个公网 IP 或者域名。分机用户可以从公网或者局域网注册到 PBX，并与其他的分机用户之间进行音视频通话。同时，分机用户通过 PBX 所配置的 VoIP 运营商或者 SIP 中继，可以与传统的 PSTN 网络的固定电话以及手机（中国移动、电信、联通）进行通话。

图 3：PortSIP PBX 在互联网上的大规模高扩展部署



如图 3 所示，PortSIP PBX 的 Call Manager 服务器部署在单独的服务器上，媒体服务器、会议服务器、WebRTC 网关、语音邮件服务器、虚拟接待服务器、呼叫队列服务器以及 Music On Hold 服务器分别部署在多台单独的服务器上，这些服务器之间组成一个集群。

SIP 客户端注册到 PortSIP PBX 的 Call Manager 服务器并进行呼叫，呼叫建立后，所有媒体流的 RTP 包以及音频视频会议、语音邮件等处理都将分别由不同的服务器进行处理，

采用集群方式部署的 PortSIP PBX 系统，可以轻松地支撑 10,000 路以上的并发呼叫通话，并且可以随着服务器数量地增加支持更多。

3.2 PortSIP PBX 的部署模式

PortSIP PBX 支持多种方式部署以适应不同的应用场景。支持在局域网或者 Internet 上的部署，支持各种虚拟化平台，支持多种主流云平台比如 AZURE、AWS、阿里云、UCloud、Linode，Digital Ocean、腾讯云等。

PortSIP PBX 成功安装后，只需要简单地点击几下鼠标就能够完成必要的设置，让 PortSIP PBX 正常运行。

运行 PortSIP PBX 配置向导

PortSIP PBX 提供的设置向导将指引你完成几项必须的设置，让系统运行起来。

PortSIP PBX 侦听 8888 端口并提供 HTTP 服务，并侦听 8887 端口以提供 HTTPS 服务。更多信息请参阅 2.4 节。

1. 在浏览器中打开 http://pbxserverip:8888，访问 PBX 管理控制台。

2. 输入管理员用户名和密码（默认为 admin/admin），然后点击**“登录”**按钮。注意：用户名和密码均区分大小写，请注意核对。输入正确的用户名和密码并成功登录之后，系统将会自动弹出配置向导，您只需要根据向导的指引逐步完成配置。

如果要修改 admin 的默认密码，请在登录管理控制台之后，点击左侧菜单**“用户资料”**>**“常规”**进行修改。

模式 1: 在局域网里部署 PortSIP PBX

假定我们需要将 PortSIP PBX 部署在一个局域网里，整个局域网通过路由器和 Internet 连接，安装 PortSIP PBX 的服务器 IP 地址是 *192.168.0.28*。同时在 PBX 里配置了 VoIP 运营商或者 SIP 中继，使得局域网里注册到 PBX 系统上的的分机用户不仅可以互相呼叫，还能通过配置好的 VoIP 运营商或者 SIP 中继与传统 PSTN 网络里的固定电话和手机进行呼叫通话。

第一步：登录 PortSIP PBX 的管理控制台，在弹出的配置向导的第一步，选择 PBX 运行在局域网，并在下面的输入框输入 PBX 的所在的服务器的局域网 IP 地址：*192.168.0.28*。PBX 支持 IPv4 或 IPv6 地址，在此示例中，我们使用 IPv4 地址。

注意：在这里，不能输入回路接口 IP 127.0.0.1，必须输入 PBX 所在服务器的正确局域网静态 IP（不能使 DHCP 动态 IP）。必须确保你的 IP 电话机或者其他的 SIP 客户端与 PBX 服务器之间的网络通畅。

此处输入的 IP 地址就是 PBX 的 SIP 服务器地址，在 SIP 客户端或者 SIP IP 电话注册到 PortSIP PBX 的时候，需要输入该地址。

第二步：现在需要输入要使用的 SIP 域名，通常是完全限定域名（FQDN）。如果没有 FQDN，也可以仅使用 PBX 服务器的 IP 地址（在本例中为 192.168.0.28）来做为 SIP 域名。SIP 域名仅用作 SIP 消息认证，不要求必须能解析。

设置 SIP 域名之后，所有的分机用户的 SIP 账号地址都是如下形式：

sip:xxx@domain

假如我们设置的 SIP 域名是 ***portsip.com*** 并创建了一个分机用户 101，那么 101 的 SIP 地址就是 sip:101@portsip.com

如果您不希望使用域名，请输入安装了 PortSIP PBX 的计算机/服务器的私有 IP（例如 192.168.0.28），用于替代域名 (FQDN)。在此情况下分机 101 的 SIP 地址就是 sip:101@192.168.0.28。

第三步：设置 SIP 消息的传输协议。系统默认设置 SIP 传输协议是 UDP 协议，绑定监听在 5060 端口。

注意：如果想要设置更多的 SIP 传输协议，可以在向导完成进入管理控制台后进行。

第四步：设置邮箱服务器。用户可以在该步骤设置电子邮件服务器，用于接收系统通知、语音信息、会议邀请及下载的文件等。PortSIP PBX 支持用户 SMTP 服务器或 Gmail SMTP 服务器。

注意：该步不是必填项，您可以根据需要进行设置。

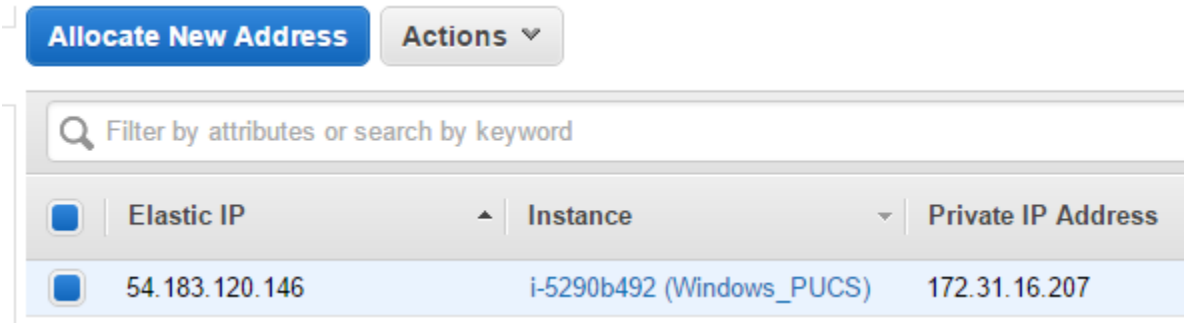
点击**“保存”**按钮，就完成了 PortSIP PBX 的基本设置。然后，系统会自动跳转到管理控制台界面。

模式 2: 在亚马逊的云平台 AWS 上部署 PortSIP PBX

亚马逊的云服务 AWS 是时下比较流行的云平台。我们可以简单地把 PortSIP PBX 部署在 AWS 上。

将 PortSIP PBX 部署在 AWS 上，分机用户可以通过 internet 上的 PortSIP PBX 进行呼叫通信，并通过配置的 VoIP 运营商或者和 SIP 中继与传统 PSTN 网络上的固定电话、手机进行呼叫通话。

如果你还没有亚马逊的 AWS 账号，请阅读 Creating an AWS account 并创建一个 AWS 账号。



第一步：在 AWS 的 EC2 管理界面左边的菜单里，选择“弹性 IP 地址”（Elastic IP），然后就可以看到“弹性 IP”(Elastic IP)并将它记录下来供后面使用。

如果没有看到弹性 IP，请点击左边的菜单列表里的**“分配新地址”**（Allocate New Address）来给你的 EC2 实例分配一个弹性 IP。

第二步：登录 PortSIP PBX 的管理控制台，在弹出的配置向导的第一步，选择在公网上运行 PBX，然后输入记录下来的 AWS 的弹性 IP 地址。

在这里输入的 IP 地址，就是 PBX 的 SIP 服务器的地址，在将 SIP 客户端或者 SIP IP 电话注册到 PortSIP PBX 的时候，需要输入该地址。

剩下的步骤，和模式一里面一样。

模式三: 在阿里云上部署 PortSIP PBX

阿里云是目前国内比较流行的云平台，PortSIP PBX 支持在阿里云上部署。

第一步：登录到阿里云的管理控制台，打开云服务器 ECS 实例，记录下云服务器的公网 IP，比如 120.25.246.106.

第二步：登录 PortSIP PBX 的管理控制台，在弹出的配置向导的第一步，选择在公网上运行 PBX，然后输入记录下来的阿里云服务器 ECS 的公网 IP。

在这里输入的 IP 地址，就是 PBX 的 SIP 服务器的地址，在 SIP 客户端或者 SIP IP 电话注册到 PortSIP PBX 的时候，需要输入该地址。

剩下的步骤，和模式一里面一样。

在其他应用场景安装部署 PortSIP PBX

如果要在上述没有提及的场景部署 PortSIP PBX，只需要将 PBX 安装在公网上还是局域网，并记住公网 IP 或者局域网 IP 地址，然后在配置向导的第一步选择正确的网络环境并输入相应的 IP 地址。

4.配置管理 PortSIP PBX

跟随配置向导的指引完成初始配置之后，接下来就可以在管理控制台里面对 PortSIP PBX 进行配置管理。

4.1 服务状态

服务状态

可以在“**概要**”>“**服务状态**”里面可以查看各项服务是否正常启动。 用户可以选中一项已停止/启动的服务，单击“**启动**”/“**停止**”按钮将其启动/停止。

在停止某项服务后，还可以单击“**启动**”按钮来启动该服务。也可以用“**重新启动**”按钮来对某项正在运行的服务进行重启。

如果同时存在多项服务处于运行状态，用户可以单击“**全部重启**”按钮将所有服务全部重新启动。

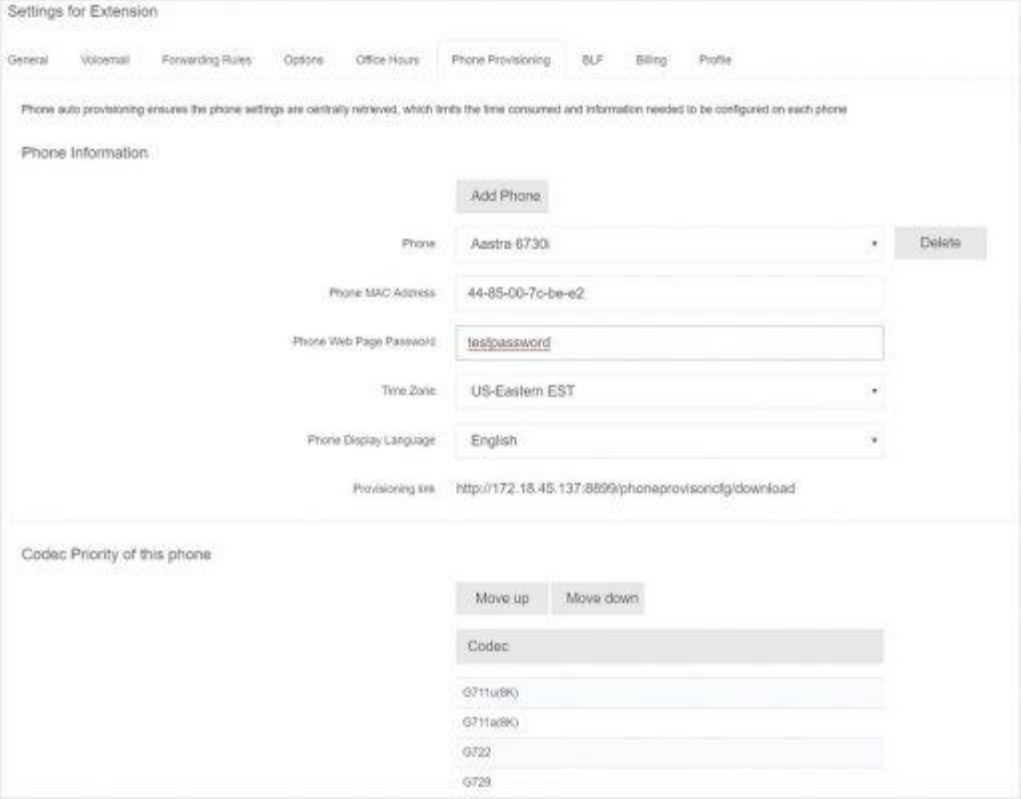
此外，服务状态的显示可能存在延迟，用户可以单击“**刷新**”按钮查看最新服务状态。

系统分机

PortSIP PBX 将 PBX 所使用的虚拟接待、会议、传真、呼叫队列、Music On Hold 等服务用到的分机号码识别成为系统分机，这些系统分机号码只能被 PBX 本身所使用。你可以在“**通话管理**”>“**系统分机状态**”里面查看各项系统服务是否正常注册到了 PBX。

4.2 话机配置

话机自动配置介绍



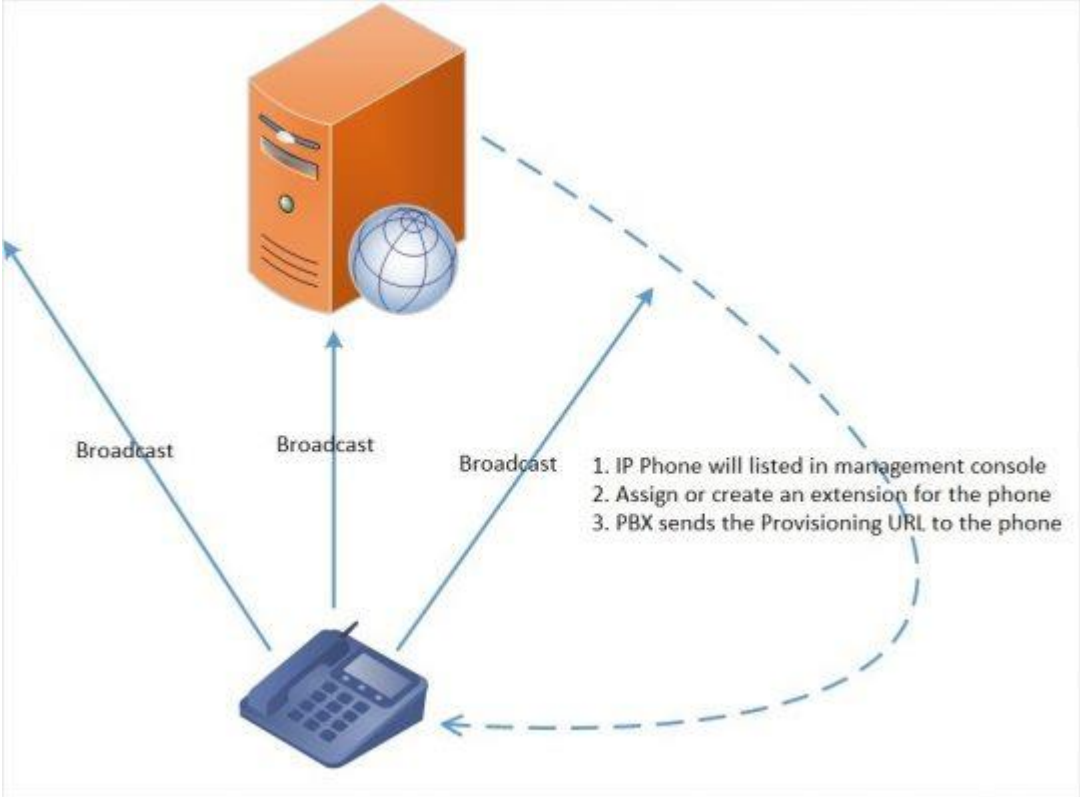
PortSIP PBX 系统安装完成后，您可以配置您的 IP 话机，为每台话机分配一个分机号。您可以选择通过话机网络页面手动逐个配置，该方法花费时间较多，且容易出错；此外您还可以使用 PortSIP PBX 提供的话机配置功能，集中远程管理话机，无须逐个登录话机的网络页面。使用话机配置功能，您可以允许话机从 PortSIP PBX 检索配置。

话机配置可从 PortSIP PBX 管理控制台集中执行更改分机密码、BLF 等操作，并将更改推送到所有话机，极大地简化了 IP 话机的日常管理。支持以下配置方法：

- **即插即用** – 支持的 IP 话机可使用即插即用功能，自动配置（适用于本地局域网的话机）
- **通过手动配置 URL** – 可将配置 URL 输入至话机的 web 页面，以此配置支持的 IP 话机（适用于本地、远程和 SBC 分机）
- **通过 DHCP 选项 66** – 旧有话机（从先前 PBX 安装版本配置，例如 Polycom、Cisco 或 Aastra）可通过 DHCP 配置，仅限在本地局域网使用。存在部分限制。

您可在此处查看支持的话机列表。只需多花半个小时配置话机，为未来节省无数精力！

使用即插即用功能配置话机（本地局域网）



注意：即插即用配置要求 PortSIP PBX 在默认 SIP 端口 5060 上运行，并且 IP 话机位于 PortSIP 所在的同一本地局域网子网。

要使用即插即用功能自动配置话机：

1. 将话机插入至网络。
2. 话机将在局域网络发送一条多点传播信息。该信息将由 PortSIP PBX 捡起。

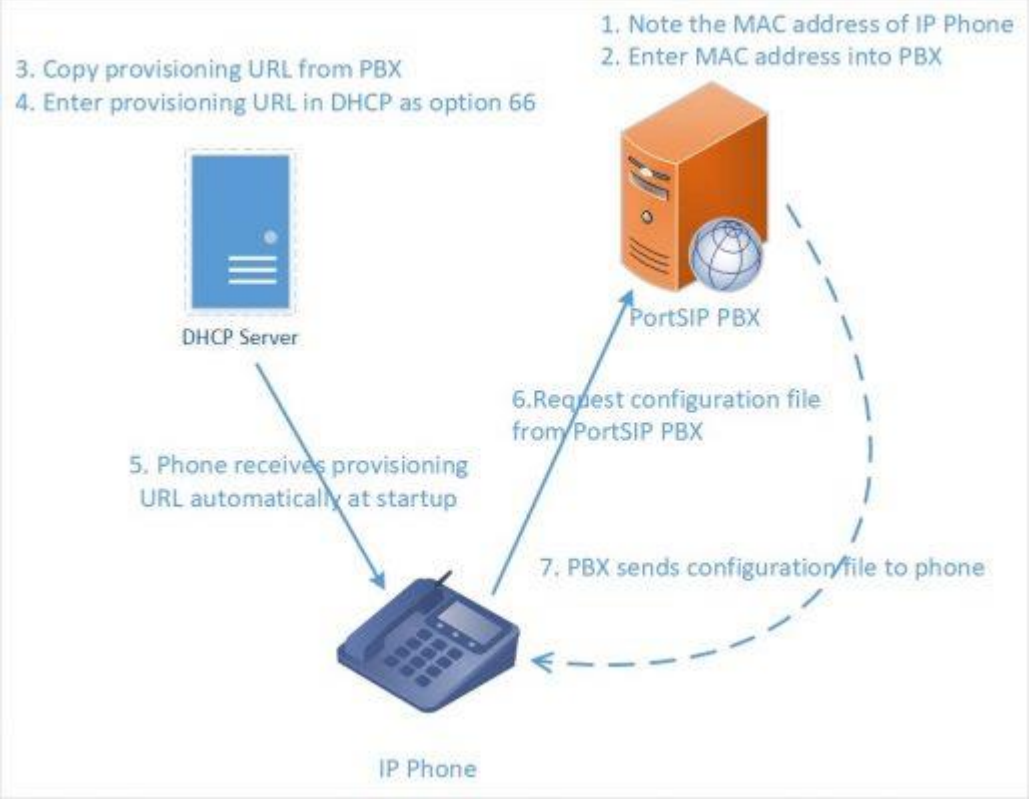
3. 话机作为新话机显示在 PortSIP PBX 管理控制台的“**话机**”页签。
4. 将话机指定给现有分机，或为其新建分机。
5. 转至分机的“**话机配置**”标签页，为话机指定其他配置设置。
6. 为话机选择“**话机显示语言**”和“**时区**”。
7. 单击“**确定**”。
8. 系统将向话机发送一条配置文件的链接，其中包含您指定的设置，可使用该配置文件自行配置话机。
9. 话机将应用这些设置，然后连接至 PortSIP PBX。现在您可以从 PortSIP PBX 管理控制台管理 IP 话机。
10.

直接使用话机配置链接配置话机

未与 PortSIP PBX 位于同一局域网的远程话机必须通过话机配置链接进行配置。要配置远程话机：

1. 在 PortSIP PBX 管理控制台的“**话机**”页签选择“**添加话机**”。
2. 选择话机所要使用的分机。
3. 输入话机的 Mac 地址，可在话机底部找到。
4. 从下拉菜单选择对应的话机型号。
5. 为话机选择“**话机显示语言**”和“**时区**”。
6. 复制配置链接。
7. 将配置链接手动插入话机，链接可在分机配置的“**话机配置**”页签找到。

配置旧话机：Cisco、Polycom 和 Aastra



Cisco、Polycom 和 Aastra 话机使用 Let’s encrypt Root CA 证书或自签名证书，不支持即插即用或安全 HTTPS 配置。他们仅可在本地局域网上使用，必须按以下方式进行配置：

1. 下载已经博瞻信息使用旧有话机测试过的固件。
2. 将话机恢复出厂设置，确保没有可能与新配置冲突的旧设置。请参考话机的用户手册了解更多信息。在此查看如何为 Aastra、Cisco、Cisco SPA 和 Polycom SoundPoint / SoundStation 恢复出厂设置。
3. 现在将话机添加到分机。您可以从管理控制台的话机界面执行该操作，或直接转至分机的话机配置页签，点击“**添加话机**”。
4. 选择话机型号。
5. 输入话机 Mac 地址，您将转至话机配置页面。
6. 为话机选择“**话机显示语言**”和“**时区**”。
7. 将“**话机网页密码**”字段保留为默认值。
8. 单击“**确定**”以将话机添加到分机。
9. **注意**：请记录下“**自动话机配置**”页签的配置链接。

现在配置话机，以从 PortSIP 配置文件夹检索配置。使用 DHCP 选项 66 或通过话机的网页界面使用 PortSIP 配置链接手动配置话机。Cisco 7940/7960 必须使用 TETP 和 DHCP 选项 66 进行配置。

旧版话机逐步设置指南：

- 配置 Polycom IP 话机
- 配置 Cisco 7940/ 7941/ 7960 /7961 话机
- 配置 Cisco SPA 302, 303,501G, 502G, 504G, 508G, 509G, 525G/G2
- 配置 Aastra 6730i, 6731i, 6739i, 6751i, 6753i, 6755i, 6757i

其他参考

正在使用远程话机？请阅读配置远程话机指南。

使用通过 DHCP 66 配置 IP 话机，为旧版话机配置话机配置 URL。

查看 PortSIP PBX 支持的 IP 话机列表。

设置 TFTP 服务器以进行固件升级。

为 Aastra、Cisco、Cisco SPA、Gigaset、Panasonic、Polycom SoundPoint、Polycom Soundstation、Yealink 恢复出厂设置

4.3 话机管理

PortSIP PBX 可让您通过网络轻松监测和管理话机和软电话。通过 PortSIP PBX 管理控制台的“**话机**”页签，您可以执行以下操作：

- 查看网络中的所有话机，包括 IP 和 MAC 网络。
- 查看连接的所有处于软电话模式的 PortSIP 客户端。
- 检查话机运行的固件版本。
- 远程重启一台或多台话机。
- 重新配置话机
- 启动话机管理界面
- 监测分机密码和 PIN 码。分机密码和 PIN 码太弱可能导致大部分安全漏洞。

添加话机

您可以通过以下方式向 PortSIP PBX 添加话机：

- 即插即用 – 插入本地局域网的话机
- 通过 MAC 添加 – 用于旧话机

即插即用（局域网和 SBC）

如果连接的话机和 PortSIP PBX 位于同一局域网内，您将看到该话机出现在话机页面上，且其名称显示为粗体。这表示 PortSIP PBX 在网络上检测到了新的话机，您需要进行处理。

选择话机，并决定如下操作：

1. 将话机指定给现有分机。单击“**指定分机**”。系统将提示您分机号码。
2. 为话机创建现有分机。单击“**添加分机**”按钮。您将被指向创建分机页面，系统将提示您填写分机名和号码。单击“**确定**”创建分机。
3. 拒绝话机。如果话机看起来比较陌生，或其尚未授权供 PortSIP PBX 使用，您可以“**拒绝**”以删除话机配置请求。

配置远程分机

如果您需要添加远程安装的话机，也即位于远程网络的话机，您必须执行以下操作：

1. 在“**话机**”页签单击“**添加话机**”按钮。
2. 选择要应用此话机的分机。
3. 选择话机型号。
4. 输入设备 MAC 地址，然后单击“**确定**”。
5. 您还可以选择为话机配置其他设置。
6. 完成后，单击“**保存**”以将话机添加至分机。
7. 复制配置链接，将其手动插入至您的 IP 话机。

通过 MAC 添加 – 用于旧话机

您可以通过以下方式，添加不支持即插即用的老旧话机：

1. 在“**话机**”页签单击“**添加话机**”按钮。
2. 选择要应用此话机的分机。

3. 选择话机型号。
4. 输入设备 MAC 地址，然后单击“**确定**”。
5. 您将跳转到分机的话机配置页面
6. 您还可以选择为话机配置其他设置。
7. 完成后，单击“**保存**”以将话机添加至分机。
8. 配置 DHCP 服务器以供配置 URL 使用，或从话机 Web 界面配置 URL。

访问话机 UI

PortSIP PBX 让您能够轻松访问已配置话机的使用密码保护的 Web 界面。PortSIP PBX 会为其配置用户名和独特密码，并管理您的凭证。要访问话机 UI，请执行以下操作：

1. 选择话机，然后单击“**话机 UI**”。
   - 对于大部分话机，您将自定跳转至话机 UI 页面。
   - 对于部分老旧话机，您可能需要输入话机的密码。在此情况下，单击“**密码**”按钮以显示密码，并复制密码为该话机配置的密码，将其粘贴到话机认证页面。

更改话机设置

通过“**话机**”部分“**通用**”页签或“**设置**”部分的“**话机自动配置**”页签对某话机的话机配置进行的更改将于 24 小时内生性。您可以重新配置话机以使其马上应用新的配置。如果您需要重新配置话机，例如在您进行配置更改后，请执行如下操作：

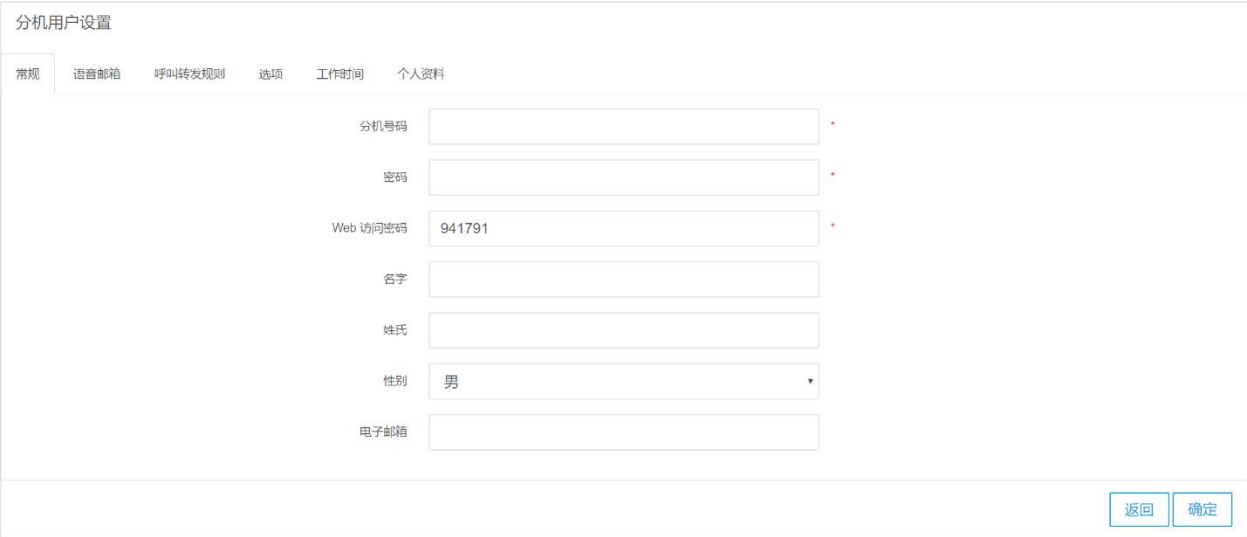
1. 选择要重新配置的话机。
2. 单击“**重新配置**”。
3. 如果需要重启话机，将会自动执行。此后无需再次重启话机。

4.4 分机用户管理

本节指导您如何在 PortSIP PBX 的管理控制台里创建以及管理分机用户。PortSIP PBX 支持以多种方式创建分机用户：

- 当提供一个新的 IP 电话的时候，可以选择创建一个新的分机用户
- 在“**通话管理**”>“**分机用户**”菜单里点击“**新建分机用户**”手动创建一个分机用户
- 可以从 CSV 文件批量导入分机用户，其中包含 DID 等参数信息

● 通过调用 REST API 创建分机



在 PBX 管理控制台里，点击左边的“**通话管理**”>“**分机用户**”，然后点击“**新建分机用户**”就可以创建新的分机，或者选中已有的分机用户，单击右边的“**编辑**”图标可以对已经存在的分机用户进行配置管理。其中“**Web 访问密码**”在分机用户登录 WEB 管理控制台的时候使用。

常规

在“**常规**”选项卡，可以输入要创建的分机号码、密码、用户名、性别以及电子邮箱地址。其中分机号码和密码是必填项，可以是纯数字也可以是英文字符。成功创建分机用户后，PBX 系统将会自动发送一封欢迎邮件到分机用户的邮箱。

字段“**Web 访问密码**”用于供分机用户登录到管理控制台。

语音邮件

在“**语音信箱**”选项卡里，可以设置分机用户的语音邮件选项，包括收听语音邮件时候的密码，启用或者禁用语音邮件，启用或者禁用收到语音邮件时候的认证，以及是否让 PortSIP PBX 系统在你收听语音邮件的时候播放呼叫者的 ID、分机号码以及时间和日期。

在分机用户创建成功之后，可以在“**语音信箱**”选项卡的“**语音信箱问候语**”部分对语音信箱的问候语音文件进行管理。

点击“**浏览**”按钮以上传新的 wav 格式的问候语文件。上传成功后，点击锁定图表来将文件指定为语音信箱的问候语。

呼叫转发规则

每一个分机用户都可以设置一系列的来电转发规则让 PortSIP PBX 在分机用户无法接听的时候，按照设置的规则来转发呼叫。这些转移规则基于如下几个因素：

- 分机用户当前的状态，比如在线或者离线、忙碌或离开。
- 当前的时间

对于分机用户的每一个状态都可以设置一个来电转移规则。例如，如果分机当前状态是在线，但是忙碌，那么可以将这个呼叫转发给语音邮箱。同时，也可以设置当前时间如果是非工作时间，将呼叫转移到手机等外部号码 (external number)。注意，将呼叫转移到手机等外部号码需要配置相应的 VoIP 运营商/SIP 中继，并设置相应的外拨规则。

选项

在“**选项**”选项卡里，可以设置或者限制分机用户的一些功能。

- 通话录音 – 如果选中了该选项，这个分机用户的所有通话都将被录制为 .wav 文件。
- 视频录制 – 如果选中了该选项，该分机用户的所有视频通话都将录制为 AVI 文件。
- 外呼方主叫方 ID – 可以在这里设置分机用户的外呼主叫 ID，这样在该分级用户通过某个运营商/SIP 中继进行外呼通话后，可以指定用外呼主 ID 来替代某个指定的 SIP 字段，详情请查阅 4.7 节。
- 已启用– 如果未选中该选项，分机用户将被禁用。
- 允许使用传呼/对讲功能 – 如果选中了该选项，分机用户可以发起传呼/对讲。
- 允许呼叫外部号码 – 如果选中了该选项，分机用户可以通过已经配置的 VoIP 运营商/SIP 中继呼叫外部号码（包括手机和固定电话）。
- 允许登录管理控制台 – 如果选中了该选项，分机用户可以登录到 PBX 的管理控制台。

工作时间

工作时间功能允许指定分机用户的上班时间，分机用户可以根据工作时间来设置相应的来电转移规则以将来电转移给不同的号码。

可以选择让分机用户使用 PBX 的全局上班时间设置，也可以选择让分机用使用自己定义的上班时间。点击选择使用指定的上班时间后，在下面的输入框里选好时间并点击向左或向右按钮来设置。设置完成后，点击“**确定**”按钮以使设置生效。

话机配置

您可以通过话机配置页签为此分机添加话机或编辑其话机设置。可在“话机配置”查看如何管理 IP 话机设置。

BLF

您可在此页签为 IP 话机配置 BLF 灯。将分机与 BLF 按钮匹配，以使该按钮显示分机状态。各话机的可用 BLF 按钮数可能不同。

BLF 提供以下可用选项：

- BLF – 显示其他分机用户的在线状态。
- 快速拨号 – 链接到一个电话号码，让您轻松快捷发起呼叫。
- 自定义快速拨号。
- 更改状态。

计费

管理员/租户可以为分机用户设置余额。在启用计费的情况下，余额不足会导致通话失败（请参阅 13.1 节）。

个人资料

在用户资料的选项卡里，可以设置分机用户的个人资料。其中公司名和公司网址是不能修改的，所有由 admin 用户创建的分机用户的公司名和公司网址都沿用 admin 的公司名和公司网址。

4.5 分机组

在通话管理下的“**分机组**”菜单里，可以对分机用户进行分组管理，通过分机组区分用户和管理员，并确定要对各分机显示何种信息。PortSIP PBX 系统有一个默认组，通常命名为 Default，默认组不能被删除和修改。 每一个分机用户至少属于一个组。当一个分机用户被创建之后，自动归属于系统默认组。

分机用户可以在加入某个分机组之后被赋予各种权限，PortSIP PBX 对分机用户的权限管理是基于分机组来进行的。当某个分机组被赋予某项权限之后，这个分机组的所有组员自动拥有该项权限。分机用户加入某个分机组后，可以查看组内其他成员的信息，分机组管理员的权限高于组内

其他分机用户的权限。系统会根据组成员关系分配权限，群管理员可以查看其组内任何成员的呼叫详细信息，包括接入及外拨呼叫。

创建分机组

在管理控制台左边的菜单，选择 **通话管理** > **分机组** 菜单，然后点击“**新增**”，在组信息选项卡输入组名以及描述信息，并选择需要设置的组权限。

点击组成员选项卡，你可以将已存在的分机用户添加进分机组，然后点击确定按钮，分机组将被创建。

当一个分机组被授予“**允许访问管理控制台**”权限后，所有的属于这个分机组的分机用户都可以登录 PortSIP PBX 管理控制台。假如 101 分机用户密码是 101，admin 在 PBX 系统设置的 SIP 域名是 portsip.com，101 分机用户属于系统默认组，该组被赋予了系统管理控制台的登录权限，那么 101 分机用户可以以如下方式登录：

用户名：101@portsip.com

密码：101 分机用户的 Web 登录密码

分机用户可以同时属于不同的用户组，并拥有这些分机组权限的合集。

4.6 SIP 域名和传输协议管理

SIP 域名管理

在 PBX 里设置 SIP 域名之后，SIP 客户端注册到 PBX 时所使用的 SIP 地址里的域名必须和 PBX 里设置的 SIP 域名相同。同时，当其他分机用户呼叫你的时候，也必须使用 SIP 域名做为你的 SIP 地址的一部分，否则你将无法收到呼叫。SIP 域名可以是一个 FQDN，也可以是一个 IP 地址。比如 portsip.com 或者 192.168.0.28。

SIP 域名是在你第一次登录管理控制台时显示的 PBX 配置向导第二步设置的。如果你要修改 SIP 域名，请点击管理控制台左侧的菜单“**通话管理**”>“**域名和传输协议**”。然后点击“**编辑**”按钮输入新的 SIP 域名并保存。

SIP 传输协议管理

PortSIP PBX 支持所有的主流传输协议来收发 SIP 消息，包括 UDP、TCP、TLS、WS (WebSocket) 和 WSS (WebSocket Security)，你必须设置至少一个传输协议以便 PBX 正常接收和发送来自客户端的 SIP 消息。

默认的传输协议是在你第一次登录管理控制台时显示的 PBX 配置向导的第三步设置的。如果你要修改传输协议，请点击管理控制台左侧的菜单“**通话管理**”>“**域名和传输协议**”。然后在“**传输协议**”部分点击“**新增**”按钮。在增加新的传输协议之前，你必须先成功设置 SIP 域名。

注意：SIP 传输协议只有 admin 用户才有权创建和删除，并且需要保留至少一个传输协议。

增加 UDP/TCP/WS 传输协议

增加 UDP/TCP/WS 传输协议的步骤如下：

1. 点击“**新增**”按钮，然后在增加传输协议的窗口里，在协议的下拉框里选择 UDP、TCP 或者 WS，UDP/TCP/WS 传输协议的默认端口分别为 5060/5063/5062，你也可以使用其他的端口。你需要确保你所使用的端口没有被其他程序所占用。

2. 点击确定按钮即可成功增加新的传输协议。

增加 TLS/WSS 传输协议

增加自签名证书的 TLS/WSS 传输协议之前，具体步骤如下：

在增加 TLS/WSS 传输协议的时候，必须提供相关的 SSL 证书。

1 如果没有从第三方证书机构购买证书，那么你需要生成自签名证书。请从博瞻信息的网站下载证书生成工具并运行（或者运行 PBX 安装目录下的 **PortCertMaker.exe**），输入你的公司名称（英文或者拼音），以及给 PBX 设置的 SIP 域名，然后点击“**生成**”按钮，证书工具将生成自签名证书。

2 生成的证书包括如下三个文件（假设你的 SIP 域名是 portsip.com）：

domain_key_portsip.com.pem

domain_cert_portsip.com.pem

root_cert_portsip.com.pem

如果你从第三方证书证书提供商（比如 Thawte、versign）处购买了证书，那么请按照如下步骤（假设为 portsip.com 购买证书）：

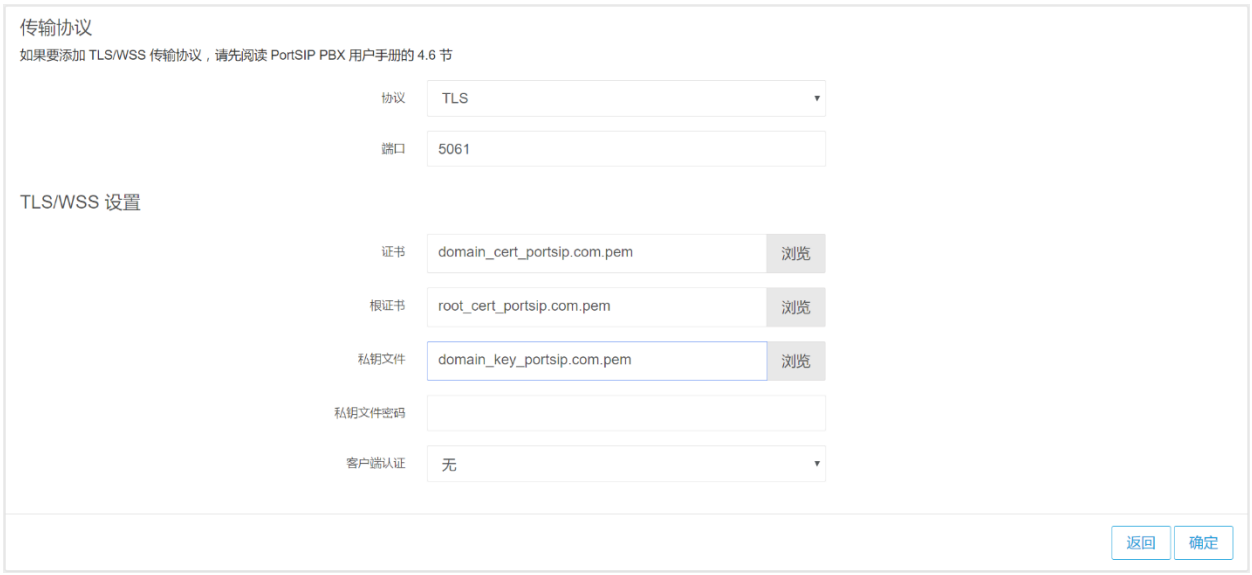
a) 根据证书提供商的指示生成 CSR 文件和私有证书文件并保存。如果你在生成私有证书的时候设置了密码，请记录下来。

b) 将私有证书文件重命名为 domain_key_portsip.com.pem。

c) 将 CSR 提交给证书提供商，在你的证书申请被通过之后，请从证书提供商处下载你的证书文件，证书文件通常有两个：Intermediate CA 证书 和 SSL 证书.

d) 用一个纯文本编辑器（不能用 WORD）分别打开 Intermediate CA 证书 和 SSL 证书，然后将 Intermediate CA 证书的全部内容复制后粘贴在 SSL 证书内容的后面，将合并后的 SSL 证书文件另存为 domain_cert_portsip.com.pem。

e) 从你的证书提供商处下载根证书文件并保存为 root_cert_portsip.com.pem。



3 点击“**新增**”按钮，然后在增加传输协议的窗口里，在协议下拉框里选择 TLS 或者 WSS，TLS/WSS 传输协议的默认端口分别为 5063/5065。您也可以使用其他的端口，需要确保你所使用的端口没有被其他程序所占用。

4 点击证书文件后面的“**上传**”按钮选择域名证书文件，即以 domain_cert_ 开头的 pem 文件：为“**证书文件**”选择“**domain_cert_portsip.com.pem**”，为“**私钥文件**”选择“**domain_key_portsip.com.pem**”，为“**根证书文件**”选择“**root_cert_portsip.com.pem**”。

5 输入**私钥文件密码**，用博瞻信息公司证书工具生成的证书没有密码，这里不需要输入，保持为空；如果你是从第三方证书提供商那里购买的证书并且在生成私有证书的时候设置了密码，请在这里输入你设置给私有证书的密码，如果没有设置就保持为空。

6 点击“**确定**”按钮，完成设置。

为新添加的传输协议设置防火墙

在成功添加新的传输协议之后，必须更改防火墙规则来允许新增的传输协议进行网络通信。假设在 PortSIP PBX 里面增加了如下的传输协议：

UDP: 5060

TCP: 5061

TLS: 5063

WS: 5064

WSS: 5065

那么必须在防火墙规则里允许如下协议和端口：

UDP: 5060　from IP: 0.0.0.0(anywhere)

TCP: 5061 from IP: 0.0.0.0(anywhere)

TLS: 5063 from IP: 0.0.0.0(anywhere)

TCP: 5064 from IP: 0.0.0.0(anywhere)

TCP: 5065 from IP: 0.0.0.0(anywhere)

4.7 配置 VoIP 运营商以及 SIP 中继

VoIP 运营商通过 IP 传送语音，取代了传统电话网。VoIP 运营商可以在一个或多个城市分配本地号码，并将其传送至电话系统，并且大多支持号码转携。

VoIP 运营商或者 SIP 中继运营商采用互联网来传送语音和视频数据。因此，可以以更优惠的费率提供和传统的 PSTN 电信运营商一样的电话服务，特别是在国际长途通话中，费率远远低于传统的电话服务。因此，使用 VoIP 运营商或者 SIP 中继可以大幅度降低企业的通信成本。

博瞻信息推荐使用 PortSIP PBX 支持的 VoIP 运营商/SIP 中继，所有支持的运营商和 SIP 中继都经过了严格测试，可以和 PortSIP PBX 很好地工作在一起。PortSIP PBX 提供的设置向导可以让你简单快速地配置你的 VoIP 运营商和 SIP 中继。

PortSIP PBX 支持如下两种 VoIP 运营商：

● 基于注册认证 – 此类服务运营商要求 PortSIP PBX 使用认证 ID 和密码注册到运营商的服务器，其中大部分已在 PortSIP 预定义。

● 基于 IP 认证 – 基于 IP 认证的 VoIP 运营商/SIP 中继不要求 PBX 注册到运营商的服务器，而是根据 PBX 的 IP 地址来进行认证以设置拨出通话时的接通目标。

配置 VoIP 运营商/SIP 中继

第一步：需要在 VoIP 运营商处注册申请一个账号。PortSIP PBX 支持市场上绝大多数主流的 VoIP 运营商/ SIP 中继。我们推荐使用经过我们兼容性测试的服务运营商，在 PortSIP PBX 的 VoIP 运营商配置向导里已经预置了这些服务运营商的配置参数。

在 VoIP 运营商处申请账号之后，需要在 PortSIP PBX 里配置账号：

1 登录到 PortSIP PBX 的 管理控制台，在左侧菜单依次选择“**通话管理**”>“ **VoIP 运营商/SIP 中继**”>“**新增**”。

2 为这个服务运营商输入一个便于记忆辨认的名字。

3 选择服务运营商所在国家，或者选择“**Generic**”以输入没有列出的运营商。

4 在运营商的下拉列表选择运营商。如果你的服务运营商不在列表里，请在上面的国家下拉列表里选择“**Generic**”。

5 选择一个运营商后，该运营商的服务器 IP 地址和端口以及其他的一些参数会被自动填写。请将这些信息和参数与你从 VoIP 运营商处收到的参数进行核对。基于你选择的运营商，有些参数输入框已经被禁用，意味着你不需要填写这些参数。点击“**下一步**”继续。

注：对于选择的 Generic VoIP 运营商，你需要自己填写服务器等参数，详情请询问你的运营商。

6 如果你的运营商不需要注册，是基于 IP 地址认证，请不要勾选“**该 VoIP 运营商要求注册**”。

7 如果运营商是你自己配置的运行于和 PBX 同一个局域网的 E1 网关或者其他的 PBX/SIP 服务器，请勾选“**运营商位于 PBX 所在的局域网**”。

8 如果您希望允许所有租户使用此提供商/中继，请选中“**对所有租户可用**”。

9 输入你在 VoIP 运营商处申请的账号和密码，指定运营商允许的最大并发呼叫数据，仔细核对，然后点“**确定**“按钮完成配置。

在左侧菜单依次点击“**通话管理**”>“**VoIP 运营商/SIP 中继**”，你可以看到所有已经配置的 VoIP 运营商。

完成对运营商的设置后，用户还可以点击“**通话管理**”>“**VoIP 运营商/SIP 中继**”>“**编辑**”按钮，编辑运营商的外呼/接入参数。

● 在“**外呼参数**”页签，用户可以设置一些规则对发往 VoIP 运营商/SIP 中继的 INVITE 消息的各个头域的值进行修改。比如将“**to**”头域的“**user**”的值设置为发起该呼叫的分机用户的“**外呼主叫方 ID**”。

● 在“**呼入参数**”页签，用户可以设置规则对呼入的 SIP 消息各个头域的字段值进行修改。

注意：外呼/呼入参数属于高级选项，推荐使用系统默认值。配置该信息需要了解 SIP 知识，配置出错可能导致 PBX 运行异常。

4.8 配置接入规则和外拨规则

接入和外拨规则决定 PortSIP PBX 如何根据一些特定的规则来转发路由呼叫。比如，你可以配置一些规则用来控制哪些呼叫需要通过哪个 VoIP 运营商/SIP 中继来进行以实现最低的费用。

你也可以基于 DID 号码来创建接入规则以让外部的呼叫直接转发给分机用户，而不用通过 IVR 或者虚拟接待来转接。

创建接入规则

很多公司都给用户或者部门提供直拨号码 (DID) 以便于可以直接呼叫到用户而不用通过转接。在英国 DID 又称为 DDI，在德国则称为 MSN 号码。虽然你在公司可以使用虚拟接待来自动应答呼叫，但是使用 DID 直拨号码是更常见的选择，因为他更简单便捷。

用户可以很容易地在“**通话管理**”>“**接入规则**”这里配置 DID 直拨号码。DID 号码是 VoIP 运营商/SIP 中继或者电话公司提供分配给你的电话线路的虚拟号码，通常是分配一定范围内的一系列号码。具体详情请咨询你的电话公司或者 VoIP 运营商。

在创建接入规则之前，您至少应该配置一个 VoIP 运营商或者 SIP 中继。创建接入规则的步骤如下：

1.在 PortSIP PBX 的管理控制台里，选择“**通话管理**”>“**接入规则**”>“**新建** “。

2.在“接入规则”的界面，输入一个容易理解记忆的接入规则名称，然后在类型的下拉列表里，选择 DID 或者 CID。

3.在 DID/DDI 号码/掩码的输入框，输入应用于本条接入规则的 DID 号码，该号码将用作主要或首要 DID 号码。当收到外部呼叫的时候，PortSIP PBX 会将该 DID 号码/掩码和 SIP 消息里的”to”字段进行匹配，并以此来决定如何转发该呼叫。

你可以指定精确匹配某个号码，或者使用通配符来进行粗略匹配。例如，如果你的 DID 号码是 2345，那么如下掩码将会被匹配到到你的接入规则。

2345

*

**345 or *45 or *5*

2 or 23* or 234**

2* or *23* or *234

1-2346　（因为 2345 在 1 – 2346 范围内）

4.如果你在**类型**下拉列表里选择的是“**CID**”，PortSIP PBX 系统将会根据收到的呼叫消息的”**from**”字段进行匹配。比如，当你选择接入规则类型是 CID，并指定掩码是 2345，那么来自 2345 号码的呼叫将会被匹配上该接入规则，和 DID 类型一样，CID 的规则也支持通配符。

5.选择要与此 DID 关联的提供商/SIP 中继。一个 DID 号码可与多个提供商关联。

6.指定如何路由转发呼往这条接入规则的呼叫：

挂断通话

连接到分机

连接到振铃组

连接到虚拟接待

连接分机的语音信箱

转接到外部号码

7.你还可以根据收到的呼叫是否在工作时间内而设置不同的转发路由。

导出以及导入接入规则

如果需要将已经创建的接入规则导出到 CSV 文件里，请按照如下步骤进行：

1. 登录到 PortSIP PBX 的管理控制台。

2. 点击左侧菜单“**通话管理**”>“**接入规则**”。

3. 点击“**导出**”按钮，开始导出接入规则

4. 选择存放导出的 CSV 文件的位置以及文件名，然后点击“**确定**”按钮。所有的接入规则将保存在指定的 CSV 文件里。

要创建多条导入规则，请通过使用正确格式在 CSV 文件内插入必要字段值，然后使用导入功能将其导入至 PortSIP PBX。

要使用 CSV 文件将接入规则导入至 PortSIP PBX，请按照如下步骤：

1. 登录到 PortSIP PBX 的管理控制台。

2. 点击左侧菜单“**通话管理**”->“**接入规则**”，点击“**导入**”按钮。

3. 选择存放导出的 CSV 文件的位置以及文件名并点击“**确定**”按钮，CSV 文件里的所有接入规则都将导入至 PortSIP PBX。

创建外拨规则

在创建外拨规则之前，你至少应该配置一个 VoIP 运营商/ SIP 中继。

一条外拨规则用来指示 PortSIP PBX 收到一个外拨呼叫的时候，这个呼叫应该通过哪一个 VoIP 运营商/SIP 中继进行。外拨规则一般是基于发起外拨呼叫的分机用户号码（或者号码范围段）、发起呼叫的分机用户组、被呼叫号码的前缀、被呼叫号码的长度等因素来确定的。

请按照如下步骤创建外拨规则：

1. 登录到 PortSIP PBX 的管理控制台，选择“**通话管理**”>“**外拨规则**”菜单，点击“**新建**”按钮，然后输入一个简单易记的规则名。
2. 指定触发外拨规则的匹配条件，在“将本规则应用于如下呼叫”部分，可以指定如下选项：

   被呼叫号码以指定前缀开始的呼叫：所有以指定的前缀开头的被叫号码。例如，输入“00”，那么所有以 00 开头的被叫号码都将匹配上本规则，包括 0012345，0002345 等等。您可以指定多个前缀，以“;”分隔。例如，“00;123;88”将指定前缀 00、123 和 88，如果被叫号码匹配其中一个前缀，则会触发该规则。

   来自指定分机用户的呼叫：可以指定从某个分机用户或者某个分机用户号码段发起的呼叫。可以指定单个或多个分机用户。指定多个分机用户时，需要使用分号隔开；如果要指定分机用户号码段，需要用“-”符号，例如 100-120 表示从 100-200 这个范围内的分机用户发起的呼叫都将被匹配到该外拨规则。

被呼叫号码长度：根据被呼叫号码的数字长度来匹配。比如指定为 8，那么所有长度为 8 位的被呼叫号码都将匹配到本规则。可以在不指定被呼叫号码前缀的情况下用来路由本地呼叫和国际长途呼叫。

来自指定分机组的呼叫：根据发起呼叫的分机属于哪些分机组来决定是否触发本规则。

3 接下来设置满足该外拨规则条件的呼叫的路由。在“**通过如下路由发起外拨呼叫**”部分，可以为外拨呼叫选择最多三个路由。所有被成功添加的 VoIP 运营商/SIP 中继都被列在三个下拉列表里。当第一个路由不可用或者正忙（达到了最大通话数）的时候，PortSIP PBX 将自动尝试第二个和第三个路由。如果三个路由都不可用或者正忙，呼叫失败。

4 在分机用户发起的呼叫触发某条外拨规则之后以及被 PBX 转发到被选中的 VoIP 运营商/SIP 中继网关之前，可以在“**截除号码位数**”和“**号码前缀**”两处分别对被呼叫号码进行修改，从头部开始截除部分号码或者在头部增加一些号码数字：

截除号码位数 使用该选项可以从被叫号码移除一个或多个数字，在转发到网关或服务运营商之前移除不需要的前缀数字。比如某个分机用户发起一个呼叫到号码 002345，你可以指定截除号码数为 2 以将前面的 2 位号码 00 移除，这样最终 PBX 发往 VoIP 运营商/SIP 中继的被叫号码就是 2345。

号码前缀 指定需要添加到被呼叫号码前缀的号码。例如某个分机用户发起一个呼叫到 002345，在“截除号码位数”处指定位数为 2，然后在前置号码这里指定“0086”，这样 PBX 最终发往 VoIP 运营商/SIP 中继的被叫号码就是 00862345。

4.9 配置振铃组/传呼组/对讲组

振铃组（Ring Group）是 PortSIP PBX 的重要功能，可以让你不会漏接任何一个客户的电话。而传呼/对讲功能能够像公共广播系统一样，对组成员发送通知。

创建一个振铃组之后，客户可以直接呼叫这个振铃组的号码，振铃租的所有分机成员都将同时或者依次收到这个呼叫，直到其中一个成员接听。比如你可以给销售部创建一个号码为 1000 的振铃组，将 3 个销售人员使用的分机号码 101、102、103 添加到这个组。当客户呼叫销售部的号码 1000 的时候，3 个销售人员的分机会同时或者依次响起直到某个销售人员接听了电话。

请按如下步骤创建振铃组：

1 在 PBX 管理控制台，点击“**通话管理**”>“**振铃组**”>“**新建**”。

2 设置振铃组的参数选项：

组号码：用来标识振铃组的号码，你可以随便指定一个号码，但是不能和已经存在的分机号码相同。**注意：这个号码是虚拟分机号码，由 PBX 使用，不能用做普通的分机用户。**

组名：为组指定一个容易记忆辨认的名字，比如销售部或者技术支持部。

振铃时长：指定群分机成员收到呼叫后振铃的时长。

振铃方式 – 给组选择一个适合的响铃方式:

同时振铃: 组所有的的分机成员将同时振铃

组次序振铃：按照成员添加到组里的顺序依次振铃

上次来电后接听次序振铃：按照成员添加到组里的顺序依次振铃，在之前呼叫中没有被振铃过的成员优先振铃。

最短通话时长次序振铃：按照成员添加到组里的顺序依次振铃，在之前呼叫中还没有接听过呼叫的成员优先振铃。

传呼/对讲：这是一个传呼/对讲组，详情请看下一节内容。

3 在“**组成员**”部分你可以设置组的成员，仅需选中你要添加的分机用户就可以把成员添加进组，或者点击组中的成员将其从组中删除。

4 在“**如果无人接听**”部分，设置来电如果在振铃时长内没有被任何一个成员接听则 PBX 该如何处理来电。可以选择将来电直接结束，或者转移给其他的分机用户/振铃组/虚拟接待，或者某个分机用户的语音信箱。

传呼

创建振铃组的时候，如果将响铃方式设置为传呼/对讲，那么某个分机用户可以呼叫到这个群组，给所有属于组的分机用户成员发送通知。收到呼叫的组成员不需要手动接听，IP 话机或者客户端会自动应答，然后播放通知。在传呼/对讲中，呼叫方不会听到接听方的声音。

对讲

创建振铃组的时候，如果将响铃方式设置为传呼/对讲，那么某个分机用户可以呼叫这个组给，所有属于组的分机用户成员发送通知。收到呼叫的组成员不需要手动去接听，IP 话机或者客户端会自动应答，然后播放声音，在应答后的通话过程中中，呼叫方不会听到接听方的声音。

如果组的某个用户分机想和呼叫方对话，那么接听方的分机用户需要按 * 键开始和呼叫方对讲，呼叫方可以听到接听方的声音；接听方分机用户可以随时按下 # 键来结束对讲，恢复为只能接听方用户分机听到呼叫方声音的单向通话。

重要提示:

在使用传呼/对讲功能之前，你必须指定传呼/对讲功能的前缀号码：

1. 在 PortSIP PBX 的管理控制台，选择左侧菜单“**设置**”>“**高级**”，在“**用于传呼/对讲的拨号前缀码**”这里，输入传呼/对讲功能的前缀号码。例如 *11。

2. 确认呼叫方的分机用户拥有传呼/对讲功能的权限。例如分机用户 100 想进行传呼/对讲呼叫，在 PortSIP PBX 管理控制台，选择“**通话管理**”>“**分机组**”，然后编辑分机用户 100 所在的分机组，选中“**允许传呼/对讲**”复选框，然后点确定按钮。

要使用传呼/对讲功能，有以下两种办法：

a. 假设您已创建振铃组 9000，且“振铃方式”设置为“传呼/对讲”。用户拨打 9000 后，振铃组的所有成员都将自动应答该呼叫，并且能够听到呼叫发起人的声音，但呼叫发起人无法收听到成员的声音。振铃组的成员可以按“*”号键与呼叫发起人对话，并按“#”号键结束对话。

b. 如果分机用户 100 需要与分机用户 101 对讲，可以按“*11101”组合键，分机用户 101 将自动应答该通话，并与呼叫人 100 对讲。这里的*11 是在“**设置**”>“**高级**”里设置的“用于传呼/对讲的拨号前缀码”。

4.10 配置虚拟接待/自动总机

虚拟接待（也叫自动总机）功能可以让 PortSIP PBX 自动应答接收到的呼叫。在接收到呼叫之后，PBX 自动应答呼叫，并播放语音提示给呼叫者，让呼叫者根据语音提示来按键选择接下来的操作。你可以用这个功能实现自定义的语音菜单。

例如，“欢迎致电博瞻信息，销售部请按 1，售后支持部请按 2，继续等待将被转移到人工服务。”

你可以配置多个不同的虚拟接待，每一个虚拟接待都将有自己的号码，并可以配置不同的参数来对针对用户的选择进行操作。您可以设置根据来电线路播放语音菜单，以及在工作和休息时间是否接听电话。例如，在休息时间，没有工作人员接听来电，可以修改语音提示，不包含将来电转接到人工服务群组/等待队列的选项。

录制语音提示

在创建一个新的虚拟接待之前，你需要先确定需要播放给用户的语音菜单的选项，并录制成 wav 格式的语音文件。例如：“欢迎您致电博瞻信息公司，销售部请按 1，售后支持部请按 2，继续等待将被转移到人工服务。”

注意：对于语音菜单，通常推荐将要选择的数字放在选择描述之后。例如：“销售部请按 1”，而不是“按 1 转接到销售部”，避免用户等待选项而忘记了对应的数字。

创建虚拟接待

你可以创建多个虚拟接待，步骤如下：

1 在 PortSIP PBX 系统的管理控制台菜单，选择“**通话管理**”>“**虚拟接待**”>“**新建**”。

2 指定要创建的虚拟接待的名字。比如销售部、售后支持部。

3 PBX 默认使用系统自制的“Default.WAV”语音提示，用户可以点击“浏览”按钮来选择已经录制好的语音提示文件。语音提示文件格式必须是 PCM，8kHz，16 位单声道 WAV 模式。如果你是使用 Windows 录音机录制，那么你需要使用“另存为”选项来设置保存这些格式。此外，用户还可以在“虚拟接待语言”选择虚拟接待的提示语言，当前支持英语和中文两个语种。

4 指定语音菜单选项，选择语音提示菜单里的数字键，为每一个数字键选择对应的操作。默认值是“无操作”，即对数字键无响应。如果需要转接到指定分机用户、振铃组、呼叫队列或其他虚拟接待，则需输入对应的分机号。

5 用户输入：该设置让您决定自动接待何时开始搜索满足用户输入值的分机。可用选项包括：

分机匹配时：自动接待会等待主叫方的顺序号匹配现有账户。自动接待发现匹配项后，则会呼叫该分机。在账户使用了不同长度的名称时，这种机制非常有用。但是，如果主叫方输入了一个不存在的号码，自动接待则不会开始搜索，可能会比较恼人。

输入 1/2/3/4/5 数字后：自动接待会等待输入正确的数字位数后开始搜索匹配的账号。如果账号不存在，系统会播放一条语音提示，告知该分机不存在。

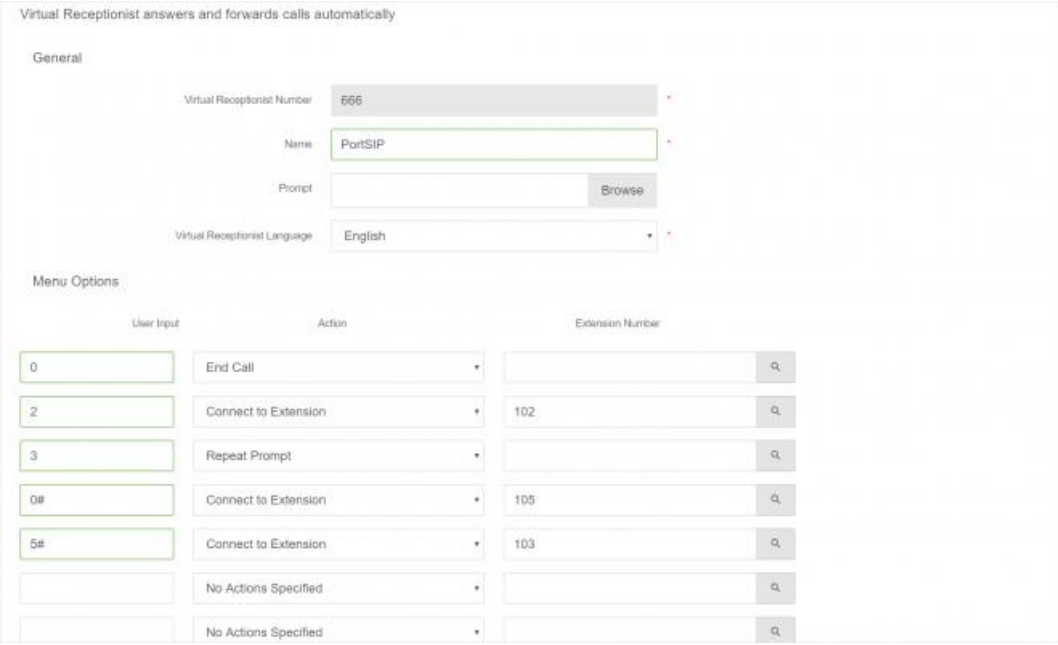
用户必须按下#号键：自动接待会等待用户按下 # 键后开始搜索分机。该模式在号码长度长短不一的场景下非常有用。

6 在**超时**设置中，可以设置 PortSIP PBX 等待用户按键的时长。如果用户没有输入任何内容，系统将自动执行该操作。该情况用于用户不理解菜单的内容或没有支持 DTMF 的话机。点击“确定”按钮，保存虚拟接待。

7 当分机用户输入的 DTMF 值或按键值超出指定范围时（即第 4 步指定的操作），操作将失败。用户可以在“**转发呼叫失败**”指定该情况下的后续操作以及对应的分机号（如果必要）。

直接转发到目标号码

直接转发到目标号码功能类似 IVR 系统的内置版本。要将接入呼叫转接到指定分机，您可以使用预先配置的目标字段并将其链接到预先录制的语音提示和用户输入选项。指定下方示例设置后，自动接待将播放一下欢迎信息：“销售部，请按 1；技术支持部，请按 2；会计部，请按 3；其他咨询服务请按 0”。（用户输入的按键选项会将其链接到分机 555、518、511 和 570。）



配置直接简单的自动接待时，直接转发到目标号码解决方案是一个很好的选择。 但是，配置需要高级 IVR 开发和功能的自动接待时，建议使用 IVR 功能。

建立直接转发到目标链接后（例如“1 #”），系统将在主叫方输入关联的号码后呼叫目标号码。在上方示例中，主叫方按下 1 后，该通话将被转发至分机 555。

输入直接目标号码后按下 # 键（例如“1 #”），系统将等待三秒，然后呼叫目标号码。如果您的分机号在 100 范围内（例如 101）。3 秒延迟确保系统能处理主叫方的完成输入（例如 101），而非直接出发第 1 个数字。

> **输入号码**：该号码可以是 1 个或多位数字；但是，系统会在用户按键后立即拨打目标号码，因此如果直接目标号码与分机号码数字存在重叠，可能导致问题。例如，例如，以“1”开头的分机将与直接目标号码“1”冲突，因为系统将无法拨打分机号码。避免这种情况的最佳解决方案选择未育直接目标号码或邮箱、外拨呼叫前缀号码重叠的分机号码。介于 4xx 至 7xx 间的分机号码可满足这些标准。另外也可在此字段使用通配符。
>
> - 如果出现难以更改分机分配（例如分机号码已通过名片流通）的情况，则可以使用超时机制。通过在直接目标号码后按下 # 键（例如，“1 # ”），系统将等待 3 秒钟，然后拨打目标号码。

- 要将传真信息重新发送至特定目标号码，您可以使用直接目标号码“F”。CNG 语音提示会发出传真音，系统识别该语音并将其解析为“F”键。

目标号码：该号码可以是内部号码（例如分机号或会议室号码）或外部号码（必须为其配置相应的 VoIP 提供商和外拨规则）。

根据用户的按键输入发送 HTTP 请求至第三方服务器

在**新增虚拟接待**界面，提供了“**虚拟接待**”和“**Action URL**”两个页签。用户可在“**虚拟接待**”页签设置普通虚拟接待选项，也可以选择在“**Action URL**”设置 HTTP 请求，以及对应的虚拟接待规则。

Action URL 的主要应用场景如下：

当用户呼叫虚拟接待，并输入指定的 DTMF 键之后，虚拟接待将根据事先的设置，发送指定的 HTTP 请求到指定的第三方服务器的 URL，然后再从第三方服务器的返回消息里解析出最终目的号码，再将用户的呼叫转移到最终目的号码。

名称：在此输入自定义的便于理解记忆的 HTTP 请求名称。此字段为必填。

操作类型：在此指定触发 Action URL 的方式。PortSIP PBX 支持两种方式：根据用户输入的 DTMF 按键或者根据用户号码（呼叫者的号码）来触发。用户可以选择“**DTMF**”或“**主叫方号码**”。选择“**DTMF**”后，如果输入的 DTMF 匹配号码和“**虚拟接待**”页签定义的 DTMF 设置重复，那么虚拟接待页签的设置将失效，系统始终优先处理“**Action URL**”页签的设置。

DTMF 匹配号码/被叫方匹配号码：根据“操作类型”的选项，用户可以相应地设置“**DTMF 匹配号码**”或“**被叫方主叫号码**”。用户可以在此字段同时指定多个号码，以逗号分隔，例如“101,102,103”。输入的号码必须唯一，不能重复。

Action URL 设置被触发后，虚拟接待将向第三方服务器发出 HTTP 请求。用户可以在“**用于向第三方服务器进行 HTTP 基本认证的凭证**”设置认证的用户名和密码（此为选填项）。并选择发送 HTTP 请求的方法，目前支持 POST 和 GET。还可以设置“**连接超时值**”、“**等待响应超时值**”以指定虚拟接待和第三方服务器通信的超时时间。

操作（URL 或号码）：这里用于指定当已设置的操作被触发后，虚拟接待所要执行的操作。如果此处输入的是 HTTP URL，那么虚拟接待将发送 HTTP 请求给第三方服务器并根据返回值转移呼叫。如果输入的是一个号码，那么虚拟接待将直接将用户的呼叫转移给这个指定的号码。

HTTP 请求消息格式

PortSIP PBX 定义如下变量，用于构造发送给第三方服务器的 HTTP 请求消息，消息格式为 JSON。

"from": "var_caller_number" - 通话呼叫方的号码，即和虚拟接待通话的主叫方号码

"to": "var_callee_number" - 通话被叫方的号码，即虚拟接待的分机号码

"input":"var_input_dtmf" - 用户输入的 DTMF

"from_name": "var_caller_display_name" - 通话呼叫方（主叫方）的用户名显示名，如果没有则为空

"account_name": "var_account_name" - 虚拟接待的名称

例： 假如我们创建了一个虚拟接待，号码为 888，名字为 Sales。

并定义了如下 Action URL：

名称: Action1

操作类型: DTMF

DTMF 匹配号码：22, 33

HTTP 方法: GET

操作（URL 或号码）：http://www.appserver.com/dest.php（此处如果是一个号码而不是 URL，那么虚拟接待将直接将用户转移给这个号码而不是发送请求给第三方服务器）。

现在用户 101（显示名为 Jason）呼叫 888，虚拟接待 888 将会自动应答呼叫，并播放语音给 101。当 101 按键输入 22 或者 33，虚拟接待将会用 GET 方法发送如下 HTTP 请求：

http://www.appserver.com/dest.php?from=101&to=888&input=22&from_name=Jason&account_name=Sales

如果在 HTTP 方法这里设置的是 POST，那么虚拟接待将会用 POST 方法发送如下 HTTP 请求，消息体为 JSON 格式：

```
{
    “from” : “101”,
    “to” : “888”,
    “input”: “22”,
    “from_name” : “Jason”,
```

“account_name” : “Sales”

}

HTTP 消息响应格式

对于虚拟接待发送的 HTTP 请求，PortSIP PBX 定义了如下格式：

"status_code"：状态码，200 或者其他，200 表示成功，其他状态码表示失败。

"action"：取值为“call”、“hangup”或者“repeat”，用于指示虚拟接待下一步操作。

call – 将呼叫转移给“destination”（后面定义）指定的号码。

hangup – 直接挂断呼叫

repeat – 重复播放提示语音

"destination"：目的号码，当“action”的值为 call 的时候，“destination”才有具有意义，其他情况下将被忽略。

{

“status_code” : 200,

“action” : “call”,

“destination” : “222”

}

虚拟接待收到如上回应之后，就会将呼叫转移给用户 222 这个号码。

允许主叫方直接呼叫已知分机用户

在播放虚拟接待提示音时，主叫方可以直接输入分机号码，连接到对应的分机用户。该操作允许知道其目标被叫方分机号码的主叫方能够直接呼叫被叫方，而不需要经过虚拟接待。此选项默认启用。如果您希望利用该功能，请在语音提示中解释指导主叫方。

例如，“欢迎致电博瞻信息公司。如果您知道对方联系人的分机号，可以直接输入。如果不清楚，销售部请按 1，技术支持请按 2”

4.11 配置呼叫队列

呼叫队列可以让拨打给 PortSIP PBX 系统的呼叫在自动应答后排队等待话务员来接听，PBX 会在用户等待的时候播放提示语音，直到某个话务员（呼叫队列成员）将这个呼叫转接过去。

例如：创建一个呼叫队列，将销售人员的分机加入到这个呼叫队列，把呼叫队列的分机号码做为销售部号码。当客户拨打销售部（呼叫队列号码）的号码，呼叫被呼叫队列自动应答。如果所有的销售人员都正忙，客户将被排在队列里面等待，并会听到 PBX 播放的语音提示，直到某个销售人员有空之后将该客户的呼叫接听过去。

创建呼叫队列的步骤如下：

在 PortSIP PBX 的管理控制台，选择“**通话管理**”>“**呼叫队列**”，然后点击“**新增**”，输入如下参数：

1. **呼叫队列号码** – 指定一个用于要创建的呼叫队列的号码。注意，不能使用已经存在的分机用户号码。

2. **呼叫队列名** – 指定一个容易理解且便于记忆的队列名称。

3. **振铃时长** – 指定在队列里等待话务员（队列成员）接听的最大等待时长。

4. **通话等待音乐** – 指定播放给在队列里等待的用户的语音提示。

5. **振铃方式** – 用来指定呼叫队列以何种方式振铃话务员（队列成员）

   同时振铃：组所有的分机成员将同时振铃

   组次序振铃：按照成员添加到组里的顺序依次振铃

   上次来电后接听次序振铃：按照成员添加到组里的顺序依次振铃，在之前呼叫中没有被振铃过的成员优先振铃。

   最短通话时长次序振铃：按照成员添加到组里的顺序依次振铃，在之前呼叫中还没有接听过呼叫的成员优先振铃。

配置呼叫队列

接下来可以设置队列的各项参数，比如增加或删除队列成员（话务员），以及所有话务员都正忙可以接听或者队列已经达到了允许的最大等待人数，或者在队列里等待话务员接听的时间已经超过了允许时长的情况下，PBX 该如何处理该呼叫。

1. “**如果无人接听**”选项，指定用户在队列里等待话务员接听的时间超过了最大等待时长 PBX 该如何处理/转移这个呼叫。如果所有的话务员（队列成员）都不在线，这个选项将会被立即触发。

2. 在“**其他选项**”部分，可以上传自定义语音提示文件（wav 格式），也可以设置是否播放语音提示文件，是否完整地播放语音提示文件，是否定时播放呼叫者在呼叫队列里的位置，以及在队列里的最大等待时长。
3. “**SLA 时间**”：

SLA 指服务水平协议。设置该选项后，每次通话队列中的通话超出指定的 SLA 时间时，您都会接到通知。

SLA 用于确保来电方在队列中的等待时间不会超出您指定的时间。

例如，如果您选择您队列内接到的所有呼叫都会在 3 分钟内应答，您需要将队列的 SLA 时间设置为 180 秒。一旦超出这个时限后，队列管理员会收到一条警报，告知某个通话等待时间超出了 SLA。

4.12 配置会议

成功安装了 PortSIP PBX 之后，在 PBX 管理控制台，选择左边的菜单“**通话管理**”>“**会议**”，然后点击“**新增**”就可以创建会议。

创建会议的步骤如下：

1. 选择左侧菜单“**通话管理**”>“**会议**”，然后点击“**新增**”按钮。
2. 在会议模式的下拉框里选择创建音频会议还是视频会议。
3. 指定会议房间要使用的**分机号码**，会议的参与方将通过拨打这个号码加入会议。**这个号码不能和已有的分机号码相同。**
4. 输入**会议主题。**
5. 可以为会议设置一个**密码**，会议参与者加入会议的时候必须输入正确的密码才能加入。

6 可以为会议设置一个**管理密码**。当管理员管理会议的时候，需要输入这个密码来确认管理员身份。

7 可以设置会议**最多参与人数**来限制与会人数。

8 指定视频会议的**画面布局**，支持 1、2、3、4、6 或 9 个分屏。

9 **视频会议码流**，设置视频会议的时候使用的带宽，取值范围 128 Kbps – 2048 Kbps，值越高表示视频质量越好。

10 **视频会议帧率**，取值范围 5 – 30，取值越高视频流畅度越高。

11 **视频会议分辨率**，支持从 QCIF 到 1080P 等各种分辨率，分辨率越高，对带宽占用越多。

12 **提示语言**，进入视频会议时候 PBX 的提示音的语言。。

13 点击“**确认**”按钮，完成创建。

4.13 管理会议

加入会议

创建会议之后，将会议房间分机号码告诉会议参与者。假定创建的时候将会议房间分机号码设置为 8008，会议的参与方可以使用任意 SIP 客户端拨打 8008 加入会议。

邀请参与者加入会议室

您还可以邀请分机号或手机号码/固定电话加入该会议，具体信息请阅读以下章节。

管理会议室

在成功创建会议房间之后，选择菜单“**通话管理**”>“**会议**”可以列出当前所有的会议房间，你可以在这里修改会议参数或者删除会议。

管理：点击管理按钮可以对会议房间和会议参与者进行管理，详情请见下一节内容。

编辑：点击编辑按钮可以对房间的一些设置进行修改，比如会议密码、管理员密码、会议最大参与人数等。

删除：关闭/结束会议

管理会议参与者

在会议列表点击选中某个会议，然后点击“**管理**“按钮，可以对会议参与者进行管理。

邀请成员：点击“**邀请成员**”按钮，在分级成员列表界面，可以直接输入被邀请者的分机号码，或者从列表选择一个分机用户， PortSIP PBX 将主动发起一个呼叫到这个分机用户，一旦分机用户接听了这个呼叫，该分机号将自动加入到会议。

在这里也可以输入手机号码或者 PSTN，以邀请手机用户或者 PSTN 电话用户加入会议。

锁定：会议锁定后，任何用户都无法加入到会议当中。

录音：点击这个按钮可以开始/停止录制会议的音频和视频，录制的文件保存在 PBX 安装目录 ***“data\mcu\record”*** 下。

静音：会议设置为静音后，所有的会议参与者都无法听到其他人的声音。

静音参与者：在会议参与者列表中，点击某个会议参与者后面的静音按钮，该参与者将被静音，其他人无法听到他的声音。

设置为主画面：将该会议参与者的视频画面设置为主画面（仅对视频会议有效）。

挂断：将指定的会议参与者移出会议。

5.设置管理租户

PortSIP PBX 系统是基于多租户的架构。在一台服务器上安装了 PortSIP PBX 之后，可以创建多个租户，每一个租户将拥有一套自己独立的 PBX 系统，租户之间互相看不到其他租户的信息，这样可以同时为多个企业服务。

5.1 创建租户

在 PortSIP PBX 管理控制台，点击左边的菜单“**租户**”>“**新增**”可以创建新的租户。

创建租户的时候，您可以指定租户的登录名、密码、SIP 域名和工作时间等信息。这些信息在租户登录管理控制台后可以自己修改。

你还可以在“**选项**”的选项卡这里指定租户能够使用的 PBX 资源限额，包括能创建的最大分机用户数、最大并发通话数、最大振铃组数、最大会议房间数以及最大呼叫队列数等。

点击“**存储空间配额**”，在这里可以设置 PBX 的存储空间配额。

录音文件：指定存储录音文件的空间，默认值是 0，表示无限制。

语音邮件：指定存储语音邮件的空间，默认值是 0，表示无限制。

通话记录：指定存储通话记录的空间，默认值是 0，表示无限制。

设置录音文件和语音邮件文件以及日志文件的**最大保留天数**：输入这些文件的最大保留天数，点击“**确定**”按钮。

5.2 停用租户

要停用租户，在 PortSIP PBX 管理控制台点击左边的菜单“**租户**”，列出所有的租户，然后在租户列表里选择要停用的租户，点击“**编辑**”图标，取消选中“**启用此租户**”选项后点击“**确定**”按钮，租户将被停用，所有这个租户创建的分机用户都将无法使用。 如果想要启用这个租户，选中“**启用此租户**”选项然后点确定按钮，租户将被重新启用。

5.3 删除租户

在 PortSIP PBX 管理控制台，点击左边的菜单“**租户**”，所有的租户都将被列出。在租户列表里选择要删除的租户，点击“**删除**”图标，租户将被删除，这个租户所创建的所有分机用户也将被一同删除。

5.4 管理租户

PortSIP PBX 允许管理员账户对租户及其分机用户的设置进行管理。要使用管理功能，请访问管理控制台，浏览至“**租户**”页面，选中一个租户并单击页面上方的“**管理**”按钮。此时，系统将切换至对应的租户账户。用户可以根据需要对租户及其分机用户进行修改、设置。

设置完成后，用户可单击用户图标下方的“**切换至管理员用户**”，直接返回至管理员账户，而无须退出登录租户的登录状态后重新登录管理员账户。

6.通话录音

您可在 PortSIP PBX 管理控制台点击“通话录音”菜单，快速在 PortSIP PBX 列出所有录音的通话以及其详细信息。

通话录音文件的命名格式是：目标号码_主叫方-域名_被叫方-域名_租户_日期_通话 id.wav。例如：

> *internal_102-sipiw.com_101-sipiw.com_admin_2018_12_08-10_33_21_1512729201_-oK7QaacDrwk1uD1VtC9Sg…wav*

以上录音文件名指示这是两个分机间（内部）的通话：主叫方是 sip:101@sipiw.com，被叫方是 sip:102@sipiw.com，其租户是 admin，通话日期是 2018 年 12 月 8 日，时间是上午 10:33:21，通话 ID 是 **-oK7QaacDrwk1uD1VtC9Sg..**。该通话 ID 也就是 SIP 消息的 call-id 消息头。

您可以选择要播放的通话录音并单击“**播放**”按钮，或将其下载或删除。

7.WebRTC

从 V9.0 开始，PortSIP PBX 默认集成了 WebRTC Gateway。

登录至管理控制台并完整设置向导后，WebRTC 即已默认配置。您可以单击“**WebRTC**”>“**HTTP 客户端**”或“**WebRTC**”>“**HTTPS 客户端**”，WebRTC 客户端即会在浏览器中打开，您可在此客户端拨打或接听通话。

重要提示：部分浏览器要求使用 HTTPS，无法与 HTTP 客户端兼容，因此我们推荐使用 HTTPS 客户端。

设置 WebRTC

通过单击“**WebRTC**”>“**设置**”菜单，您可以更改 WebRTC 设置。

侦听 WS：将要侦听 WebRTC Gateway 的默认 WS 端口。WS 传输端口是 10080。

在 WSS（网络套接字安全性）端口启用 WebRTC 服务：您可以允许或/禁止 WebRTC Gateway 侦听 WSS 端口。Google Chrome 要求使用 WSS 访问相机和麦克风。您必须选中该选项才可在 Google Chrome 中使用。

选中“**侦听 WSS**”后，您需要填写以下字段：

WSS 侦听端口：设置 WSS 端口，例如 10443。

网关域名：您的 WebRTC Gateway 域名，可移除。如果您不知道域名，请输入 PortSIP PBX IP。注意：默认情况下，域名已配置，不需要修改。

证书文件：对于 WSS，您必须上传证书文件。您可以自行生成 SSL 证书文件，或从 Thawte 或 Digicert 等证书提供商购买证书。证书必须与 WebRTC Gateway 域名匹配（即先前的网关域名）。

专用密钥文件：可与证书一起生成。

专用密钥密码：专用密钥文件的密码即是您生成证书文件时生成的密码。如若没有，请将其保留为空。

*重要提示：默认情况下，WSS 证书已配置，不需要上传。默认证书文件是“**自签名**”证书，因此在您使用浏览器打开 WebRTC 客户端时会弹出安全警告。您可以从第三方证书提供商购买证书，以避免安全警告。有关更多信息，请参考下一节“**使用授权证书设置 WebRTC**”。*

使用授权证书设置 WebRTC

您可以从 Thawte 或 Digicert 等证书提供商购买官方证书，以避免安全警报和手动添加安全礼物。

购买证书时，您需要自行生成专用密钥和 CSR，具体请阅读证书提供商的指示信息或联系提供商支持。我们建议您不要设置专用密钥文件密码，并且您必须自行保存专用密钥文件。

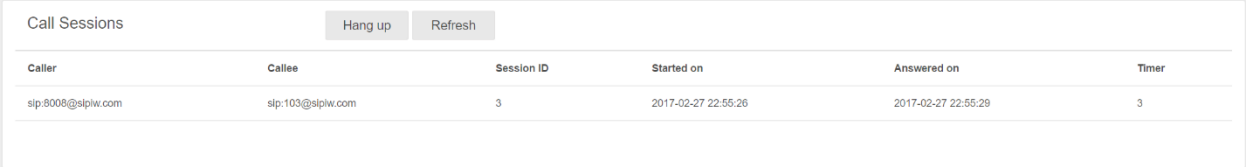
假设您已从 Thawte 购买证书（在此我们以 Thawte SSL123 证书为例），用于您的 WebRTC 域名 example.com。在下载 certificate .zip 文件后，您需要将其解压缩，并获得两个文件：IntermediateCA.crt 和 ssl_certificate.crt。您需要使用平文本编辑器（例如 Windows 记事本，请勿使用 MS Word）将两个证书合并为一个，将 IntermediateCA.crt 的所有文字附加到 ssl_certificate.crt 的文字后方。

1. 确保域名 examplertc.com 已正确解析到 PortSIP PBX 所在的服务器的 IP。
2. 登录 PortSIP PBX 管理控制台，单击菜单“**WebRTC**”>“**设置**”，选中“**在 WSS（网络套接字安全性）端口启用 WebRTC 服务**”，在“**网关域名**”输入“**exmaple.com**”，然后单击“**浏览**”按钮以上传 ssl_certificate.crt 和专用密钥文件。完成后，请单击“**确定**”按钮以保存设置。

现在，您可从“**WebRTC**”菜单单击“**HTTPS 客户端**”以打开 WebRTC 客户端，输入您的分机号和密码以及 SIP 域名（分机的 SIP 域名，而非网关域名），按下“**登录**”按钮以登录至 WebRTC 客户端，然后发起或接听通话。

8.当前通话

通过 PortSIP PBX 管理控制台的“**当前通话**”菜单，您可以在 PortSIP PBX 监控当前所有通话及其详细信息。



点击某个通话的“**挂断**“按钮可以将这个通话挂断。点击“**刷新**”按钮可以刷新当前通话的状态。

9.通话详情及通话记录报告

通话记录报告功能可以让你审阅 PBX 的通话记录，以及根据指定的参数生成 CSV 格式的报告文件并发送到指定的电子邮箱。

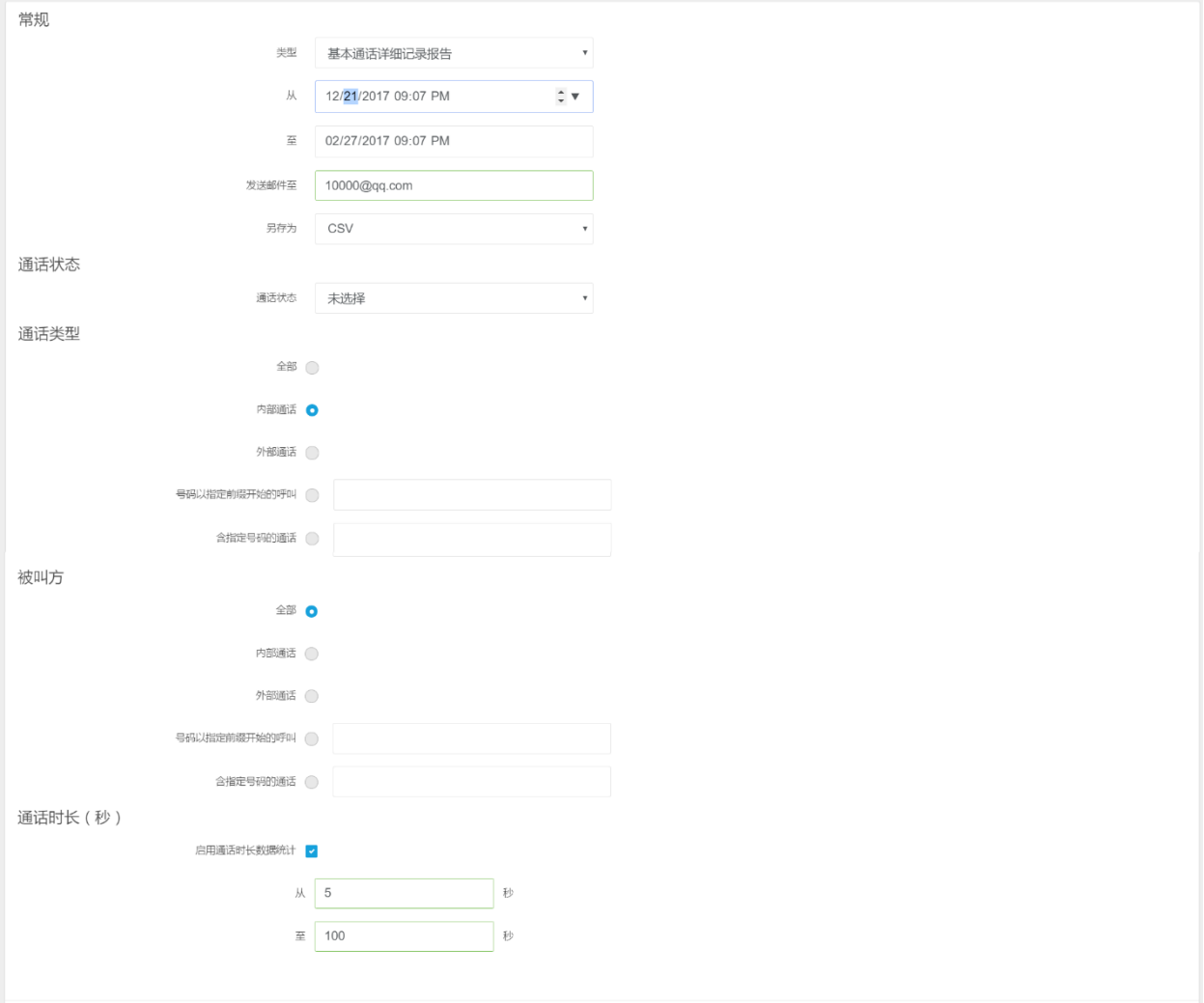
9.1 查看通话记录

在 PortSIP PBX 管理控制台，点击左边的菜单“**通话详情**”将列所有历史通话记录，你可以点击“**下一页**”按钮来查看更多的通话记录。

9.2 生成通话记录报告

除了在 PortSIP PBX 管理控制台里查看历史通话记录之外，你也可以让 PBX 根据指定的参数条件，自动生成通话记录报告，并发送到指定的邮箱。该过程以较低优先级执行，不会影响 PBX 运行。

注意：要接收导出的通话记录报告，请确保您已正确配置 SMTP 邮件服务器。要设置该服务器，请转至设置向导的第 4 步或转至**个人资料** > **邮件服务器。**



要生成通话记录报告并发送到信箱，请按照如下步骤执行：

1. 点击管理控制台左侧的菜单“**通话记录报告**”，然后点击“**生成报告**”按钮来创建新的通话记录查询报告。
2. 选择通话记录的日期段范围。
3. 输入接收通话记录报告的邮箱地址。
4. 在文件格式下拉框里选择通话记录报告的格式，默认为 CSV。
5. 选择根据呼叫发起方过滤，可以指定精确匹配整个号码，或者只匹配前缀，或者匹配包含有指定号码的呼叫发起方。也可以按照呼叫发起方是外部号码还是 PBX 内部的分机号码来筛选通话记录。
6. 选择根据呼叫接收方过滤，可以指定精确匹配整个号码，或者只匹配前缀，或者匹配包含有指定号码的呼叫接收方。也可以按照呼叫接收方是外部号码还是 PBX 内部的分机号码来过滤通话记录。
7. 选择根据通话状态过滤，指定为“**全部**”则不做过滤，如果指定为“**已应答**”，那么呼叫记录报告将只包括成功应答的通话记录。

8. 选择根据通话时长过滤，选中“**启用通话时长数据统计**”选项，然后输入一个通话时长的起始范围（以秒为单位），比如从 10 到 20，那么通话记录报告里将只包括所有时长在 10 秒与 20 秒之间的通话记录。

点击“**确定**”按钮，PBX 将会自动根据指定的条件生成通话记录报告，并发送到指定的邮箱。

10.计费

PortSIP PBX 允许客户自定义呼叫费率，要实现该功能，可访问管理控制台，转至“计费”部分进行设置。

10.1 新增费率

用户可在管理控制台的“计费”部分点击“新增”来添加新的费率规则，并输入如下必填信息：

名称：在此字段输入费率的名称。

号码前缀：在此字段输入特定号码前缀，一旦指定后，该费率将应用到符合此号码前缀的所有相关通话。

接入费率：收到外部接入通话时应用的费率，输入的值必须大于或等于 0。

外拨费率：向外部号码发起通话时应用的费率，输入的值必须大于或等于 0。

费率计时单位：计费所使用的计时单位。

10.2 编辑/删除费率

创建完成后，用户可在“**计费**”部分查看所有费率的完整列表，也可单击页面上方的“**编辑**”或“**删除**”按钮来编辑或删除选中的费率。

注意：创建费率完成后，用户不可编辑修改已创建的费率的“**号码前缀**”。

10.3 导入/导出费率

PortSIP PBX 允许用户通过“**计费**”部分的“**导入**”按钮，批量导入计费规则。导入完成后，“**计费**”页面将列示所有已成功导入的计费规则。如果现有的费率规则和需要导入的费率规则相同，则会导入失败。**注意**：导入/导出功能仅支持 CSV 文件格式。

此外，用户还可以选择将服务器上的所有费率信息导出，方法是单击“**计费**”页面上方的“**导出**”按钮。下载完成后，用户将获得一份 CSV 格式的文件，里面列示了所有的计费规则。

11. 设置

在安装成功后，第一次进入 PortSIP PBX 管理控制台的时候，配置向导会引导你完成一些基本的配置。在这之后，如果你想对 PBX 进行更多细微的调整和设置，可以通过管理控制台左侧的“**设置**”菜单进行。

重要提示：只有 administrator 用户才有权限修改“**设置**”菜单下的各个选项，租户和分机用户都没有权限对设置进行修改。

11.1 常规

点击管理控制台中的“**设置**”，在这里可以调整 PBX 的一些参数。

注意：我们推荐用户使用默认设置。

日志级别：指定 PBX 如何生成日志文件“portpbx.log”。

启用 IPv6：可使用该选项启用/禁用 IPv6 支持。

禁用 DIGEST 认证：如果这个选项被选中，分机用户登录到 PBX 的时候，PBX 将不验证分机用户的密码。除非已经明确知道这个选项的作用及可能的风险，否则不推荐勾选这个选项。

禁用 auth-int 认证：选中此选项后，将在认证中不执行认证完整性保护（Disable auth-int quality of protection）。

禁用会话中的后续请求认证：选中此选项后，PBX 不再在一个会话的所有后续请求中要求验证。

收到错误的 nonce 后发送 403：如果勾选了这个选项，用户在进行身份认证的时候发送了错误的 nonce 给 PBX，PBX 将回应 403 消息给用户。如果未选中该选项，PBX 将发送一个新的认证挑战给用户。

允许注册消息的 to 消息头的 tag 参数：允许分机用户注册到 PBX 的时候，REGISTER 消息的“**to**”消息头带有 tag 参数。

统计数据的间隔时长：指定将 PB X 协议栈的统计数据写到日志文件里的间隔时长，默认值是 10 分钟。

启用拥塞管理：通过这个选项来启用/禁用 PBX 系统的拥塞管理机制。

拥塞管理指标：推荐使用系统默认的 WAIT_TIME 值，这个值是基于系统内部每一个队列的等待时间，通过使用等待时间乘以平均每次服务时间计算的。。

拥塞强度管理：设置系统对不同的拥塞强度处理方式。该选项确定拒绝操作策略，默认值是80。

取值	*描述*
80	80% 强度的拥塞，系统正常处理请求，不拒绝任何请求。
80 - 100	80% - 100%的拥塞度，达到这个范围内的强度。所有新的请求都将被拒绝，现有正在处理的请求将不再继续处理。
> 100	大于 100%的拥塞，超过系统负载，将拒绝所有系统不必要的工作。如果停止某些任务可能导致泄露、系统不稳定或动荡，则不停止；所有其他任务将全部停止。

注册不存在的分机用户时，自动创建该用户：如果勾选这个选项，当 PBX 收到一个不存在的分机用户的登录请求的时候，会自动创建这个分机用户，新创建的分机用户默认密码是“portsip”。

启用 PRACK（临时响应可靠性）：如果选中了此选项，则会启用**临时响应可靠性** (RFC3262)。

启用 Flow Routing： 启用 RFC5626。

指定时间内没有 RTP 数据，则挂断电话（秒）：PBX 会跟踪每个进行中的通话的空闲实际（即没有接收到数据包的时长），如果通话在指定的时间内， PBX 没有收到通话双方的 RTP 包，就自动关闭这个通话。默认值是 2 分钟。

启用通话定时器 (RFC4028)：启用 RFC4028 定义的通话定时器来检测通话双方是否还在线。该选项被选中之后，PBX 将定时发送 INVITE 消息给通话的双方，如果某一方在规定的时间内没有正确响应，PBX 将会终止这个通话。

通话定时器时长：指定 PBX 在每个通话中多长时间发送一次 INVITE 来检测通话双方是否在线。默认是 120 秒，最小值不得小于 90 秒。

Presence 模式：PortSIP PBX 支持如下两种 Presence 模式:

Presence 模式	*描述*
点对点	PortSIP PBX 会转发该出席状态，但不会对其进行更改。
Presence 服务器	PortSIP PBX 会使用内部 presence 服务器处理分机的 presence 状态，此模式要求客户端支持 PUBLISH SIP 方法。

警告：如果 Presence 模式发生更改，PBX 会自动重启。

DNS 服务器：指定 PortSIP PBX 使用的 DNS 服务器，该值会覆盖默认的操作系统检测到的 DNS 服务器列表。如果这里没有指定，PBX 将使用 Windows 系统的默认 DNS 服务器。

11.2 高级选项

在管理控制台点击“**设置**”>“**高级**”，在这里可以设置 PortSIP PBX 的高级选项。

用于传呼/对讲的拨号前缀码：在这里可以指定传呼和对讲的拨号前缀码。如果一个呼叫的被叫号码以这个前缀码开始，PBX 将把这个呼叫当着传呼/对讲呼叫来处理。详情请见**振铃组**小节“**传呼**”和“**对讲**”相关内容。

使用 Alert-Info 消息头用于自动应答：选择在传呼/对讲呼叫的 SIP 消息里面插入的“Alert-Info”消息头的值。选择了下拉框中的选项后，在传呼/对讲的呼叫消息中，会自动插入“Alert-Info”字段以及选择的字段值。

例如选择“alert-autoanswer”，如下消息头将会被插入到 SIP INVITE 消息中：

“Alert-Info:info=alert-autoanswer”

用户分机检测到“Alert-Info”后，会自动应答呼叫并打开外放喇叭。

为自动应答启用 Call-Info 消息头：选择在传呼/对讲呼叫的 SIP INVITE 消息里面插入的“Call-Info”消息头。

例如，如果勾选该选项，在传呼/对讲的呼叫消息中，如下消息头将会被插入到 SIP INVITE 消息中：

“Call-Info: sip:portsip.com;answer-after=0”

用户分机检测到“Call-Info”后，会自动应答呼叫并打开外放喇叭。

使用 RFC 5373 的 Require Answer Mode：选择在传呼/对讲呼叫的 SIP INVITE 消息里面插入的“AnswerMode”消息头。如果勾选该选项，在传呼/对讲的呼叫消息中，会自动插入“**AnswerMode**”消息头。

比如选择该选项，如下消息头将会被插入到 SIP INVITE 消息中：

“AnswerMode: auto”

用户分机检测到“AnswerMode”的值是 auto，会自动应答呼叫并打开外放喇叭。

不同的 IP 话机/客户端支持不同的自动应答模式，你需要阅读话机手册来选择相应的应答选项。

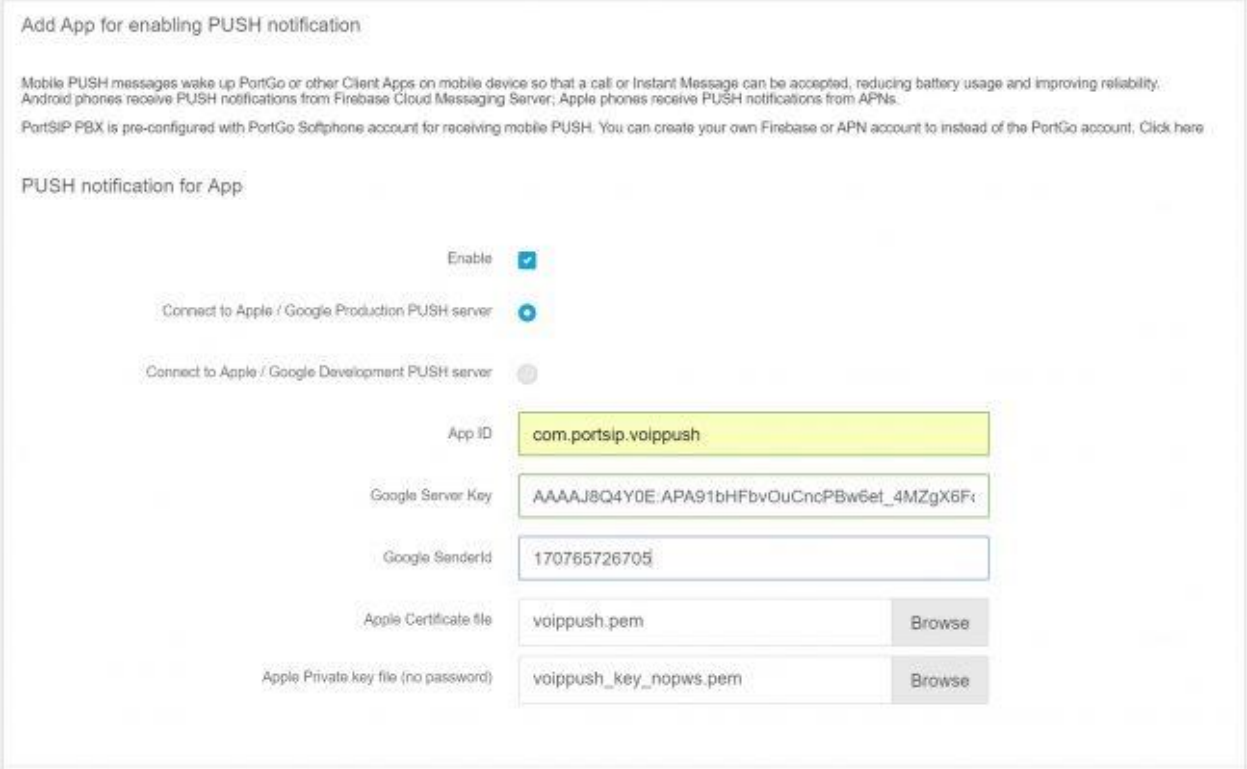
Busy Lamp Field 设置：在此部分中，用户可以选择选中“**启用会话状态监测**”来启用该功能，并设置对应的“**用于代接正在振铃的会话的号码前缀**”和/或“**用于代接处于保持状态的会话的号码前缀**”，以对满足条件的呼叫启用该功能。默认值为 ** 和 ##。

例如：

1. 总经理的秘书在 IP 话机里设置对公司总经理的分机 101 的通话状态进行监测。当 101 分机收到一个呼叫并振铃，但是总经理此时不在办公室，秘书可以通过用自己的 IP 话机拨打 **101 来代接总经理的这个来电呼叫。
2. 总经理因为有其他的急事将一个呼叫进行 HOLD 之后很长时间内没能回来继续恢复通话，此时秘书可以用自己的 IP 话机拨打 ##101 来将被 HOLD 的这个通话代接过来。

11.3 配置移动推送信息

PortSIP PBX 使用 PUSH 技术，在客户端收到呼叫时唤醒智能设备。移动推送信息会唤醒 PortSIP Softphone 或其他客户端应用以接受呼叫或即时通讯，同时减少电池用量并改进可靠性。Android 话机从 Firebase Cloud Messaging Server 接收推送通知，苹果话机则从 APN 接收推送通知。



默认情况下，PortSIP PBX 已内置 PortSIP Softphone 推送服务，如果您需要启用其他应用，可以自行创建 Firebase 或 APN 账号，替换 PortSIP Softphone 账号。

配置 PortSIP PBX，接收移动推送信息

1. 登录到 PortSIP PBX 管理控制台。
2. 浏览到“**设置**”>“**移动推送信息**”>“**添加新应用**”，设置用于接收推送信息的新应用。
3. 选择“**启用**”，以启用推送信息。
4. 输入应用 ID。
5. 如有必要，为 Android 客户端输入 **Google Server Key** 和 **Google SenderID**，并为苹果客户端上传**苹果证书文件**和**苹果专用密钥文件**。
6. 单击“**确定**”以应用设置，并重启所有客户端，以便重新配置并应用最新设置。

要了解如何配置移动推送通知以与您的应用和 PortSIP PBX 配合使用的详细指南，请参考以下主题：

1. 使用 PortSIP PBX 在本地 iOS 应用中实施推送通知
2. 使用 PortSIP PBX 在 Android 应用中实施推送通知

11.4 管理媒体服务器

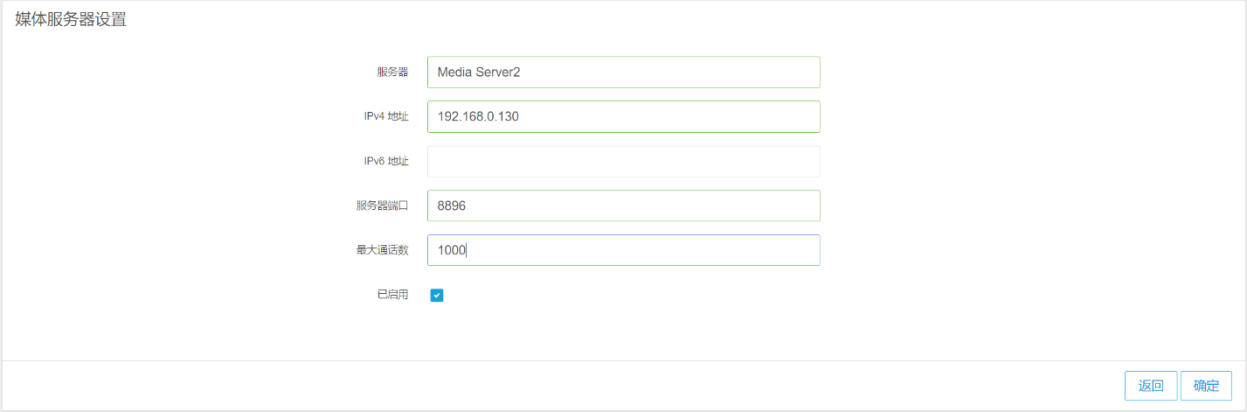
媒体服务器用来处理 NAT 穿透的场景以及作为媒体转发网关来转发通话时候的 RTP 包。

在成功安装 PortSIP PBX 后，系统自动启动内置的默认媒体服务器 (Built-in Server)。在每一个通话的过程中，媒体服务器负责做 IP 和端口转换，并在通话双方之间转发 RTP 包。

添加外部媒体服务器

因为 PortSIP PBX 使用默认媒体服务器来转发通话双方的 RTP 包，如果很多个通话同时进行会导致 PBX 所在的服务器 CPU、网络带宽及内部负载过高，引发声音延迟，无法处理新的通话等问题。

在这种情况下，为了减轻 PBX 所在的服务器负载压力，我们可以增加更多的媒体服务器来处理 RTP 包的转发，以此减轻 PBX 服务器的压力，降低通话的语音和视频等媒体的延迟。



选择菜单“**设置**”>“**媒体服务器**”，点击“**新增**”按钮，然后给要新增加的媒体服务器输入一个容易理解记忆的名字、IP 地址（可以是 IPv4 或 IPv6 地址）和端口（默认端口 8896），以及设置该媒体服务器最大可以同时为多少条通话转发 RTP 数据。

编辑媒体服务器

点击左侧菜单“**设置**”>“**媒体服务器**”将会列出所有的媒体服务器，并可以查看各个媒体服务器的状态，比如是否已经启用，是否已经和 PBX 正常连接。点击“**编辑**”图标按钮可以对某个指定的媒体服务器的参数进行修改。

在“**最大通话数**”输入框，输入该媒体服务器最多可以支持多少条通话。

你也可以在媒体服务器列表里，点击某个媒体服务器的“**启用**”开关来禁用该服务器。

移除媒体服务器

点击左侧菜单“**设置**”>“**媒体服务器**”将会列出所有的媒体服务器，在媒体服务器列表里，可以选中某个服务器，单击页面顶部的“**删除**”图标按钮来移除该服务器。服务器被删除后，PortSIP PBX 在后续的通话中将不再使用它来转发 RTP 数据。

注意：系统默认内置的媒体服务器 (Buit-in Server) 不能被移除。不过你可以用“启用”开关按钮来禁用默认内置的媒体服务器 (Buit-in Server)。

如果你禁用了默认内置的媒体服务器 (Built-in Server) 并且没有增加其他媒体服务器，那么在所有的通话中，RTP 数据将会直接在通话双方之间发送，如果 PBX 运行在 Internet 上，那么有可能会导致通话没有声音和视频。

11.5 配置语音邮箱

设置语音邮箱分机号

PortSIP PBX 成功安装后，默认情况下即启用了语音邮箱服务。您可以单击左侧菜单的“设置”>“语音邮箱”，指定语音邮箱服务分机号。用户可以拨打该号码查看其语音邮件。默认语音邮箱号码是 999。

设置语音邮箱存储空间限额

PortSIP 允许您指定保存语音邮件的存储限额。默认值为 200MB。您可以输入语音邮件保存期限（按天计）。

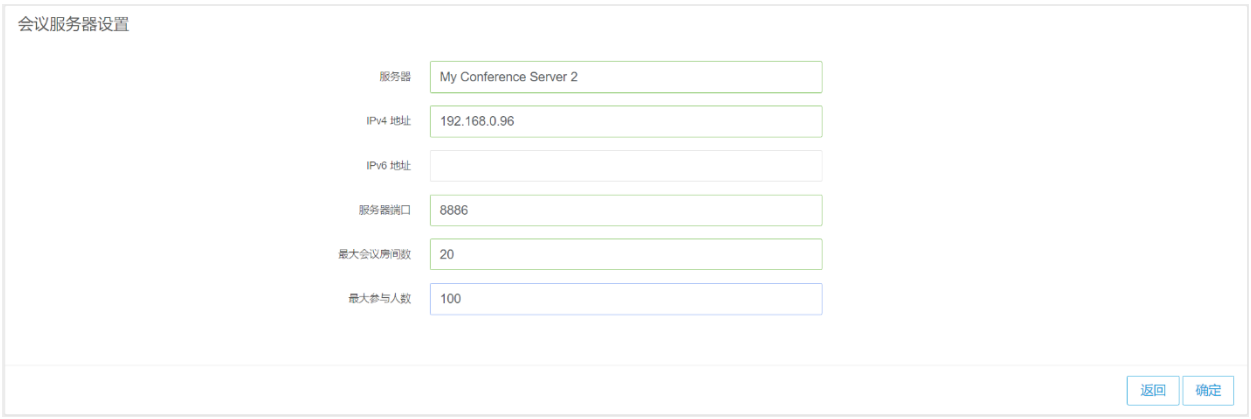
11.6 管理会议服务器

PortSIP PBX 系统提供了多方音视频会议功能，在安装 PortSIP PBX 系统之后，PBX 自动启动内置的默认会议服务器 (Built-in Server)，在你的 PBX 服务器系统资源（包括 CPU、内存、网络带宽）足够的情况下，你可以创建多个音频或者视频会议。

添加外部会议服务器

PortSIP PBX 使用会议服务器来处理会议请求，如果 PBX 同时处理大量的呼叫以及多个会议，会导致 PBX 所在服务器的 CPU、网络带宽和内存负载过大，从而使得呼叫声音延迟增大，以及无法处理新的通话呼叫。

可以通过增加一个或者多个会议服务器的方式来解决上述情况，当多个会议服务器被加入到 PBX 系统之后，PBX 将把会议分配到这些新加入的服务器，以降低 PBX 的负载压力和减缓网络延迟。



在 PortSIP PBX 管理控制台里，选择左侧的“**设置**”>“**会议服务器**”菜单，点击“**增加**”按钮，然后给新增的会议服务器输入一个容易理解记忆的名字，以及该服务器的 IP（可以是 IPv4 或 IPv6 地址）、会议服务器的默认端口 8886，然后输入该会议服务器允许的最大会议房间数以及会议参与人数，点击“**确定**”。

编辑会议服务器

点击左侧菜单“**设置**”>“**会议服务器**”将会列出所有的会议服务器，并可以查看各个会议服务器的状态，比如是否已经启用，是否已经和 PBX 正常连接。点击“**编辑**”图标按钮可以对某个指定的会议服务器的参数进行修改。

在“**最大会议房间数**”处输入该媒体服务器最多可以创建多少个会议。你也可以在会议服务器列表里，点击某个会议服务器的“启用”开关来禁用该服务器。

移除会议服务器

点击左侧菜单“**设置**”>“**会议服务器**”将会列出所有的会议服务器，在会议服务器列表里，可以单击选中某台服务器，然后点击页面顶部的“**删除**”图标按钮来移除该服务器。服务器删除后，PortSIP PBX 将不再使用该服务器创建会议。

注意：系统默认内置的会议服务器 (Built-in Server) 不能被移除。可以使用“启用”开关来禁用默认内置的会议服务器 (Built-in Server).

如果你禁用了默认内置的会议服务器(Built-in Server)并且没有增加其他会议服务器，那么 PBX 的会议功能将不能使用。

11.7 备份和还原

PortSIP PBX 提供备份和还原功能，用户可访问“**设置**”>“**备份和还原**”，备份系统设置和数据，以便需要时轻松恢复系统和数据，或者将 PBX 迁移到另一机器。

常规备份

要对系统设置进行常规备份，请执行以下操作：

1. 访问管理控制台，进入“**设置**”>“**备份**”，单击页面上方的“**备份**”按钮。
2. 在“**备份文件名称**”为备份输入文件名称，并选择要备份的内容。
3. 单击“**确定**”开始备份。
4. 备份开始后，一般需要一段时间才能完成。一旦备份完成，刷新页面在列表中将会出现备份文件，此时可以选择列表中的备份文件然后点击“**下载**”按钮将文件下载到本地。或者点击“**还原**”按钮将 PBX 从备份文件还原。

将现有的 PBX 迁移到另外一台机器

如果需要将现有的 PortSIP PBX 迁移到另外一台机器，请按照如下步骤：

1. 访问管理控制台，进入“**设置**”>“**备份**”，单击页面上方的“**备份**”按钮。
2. 在“**备份文件名称**”为备份输入文件名称，并选择要备份的内容。
3. 单击“**确定**”开始备份。
4. 刷新页面，从备份文件列表中将备份文件下载后保存。

现在，您可通过如下方式还原 PBX：

1. 将 PortSIP PBX 安装到新机器上后，登录至管理控制台，单击“**设置**”>“**备份**”按钮，单击“**导入**”按钮以上传您的备份文件。备份文件成功导入后，将其选中并单击“**还原**”按钮。还原进程完成后，PBX 即会还原到先前设置。注意：如果备份任务较小，推荐使用该方法。

计划备份

除了普通常规备份，用户还可以设置“**计划备份**”，对 PBX 设置和数据进行定期备份。

要设置“**计划备份**”，请访问管理控制台，进入“**设置**”>“**备份**”，单击页面上方的“**计划备份**”按钮，并根据需要设置如下项：

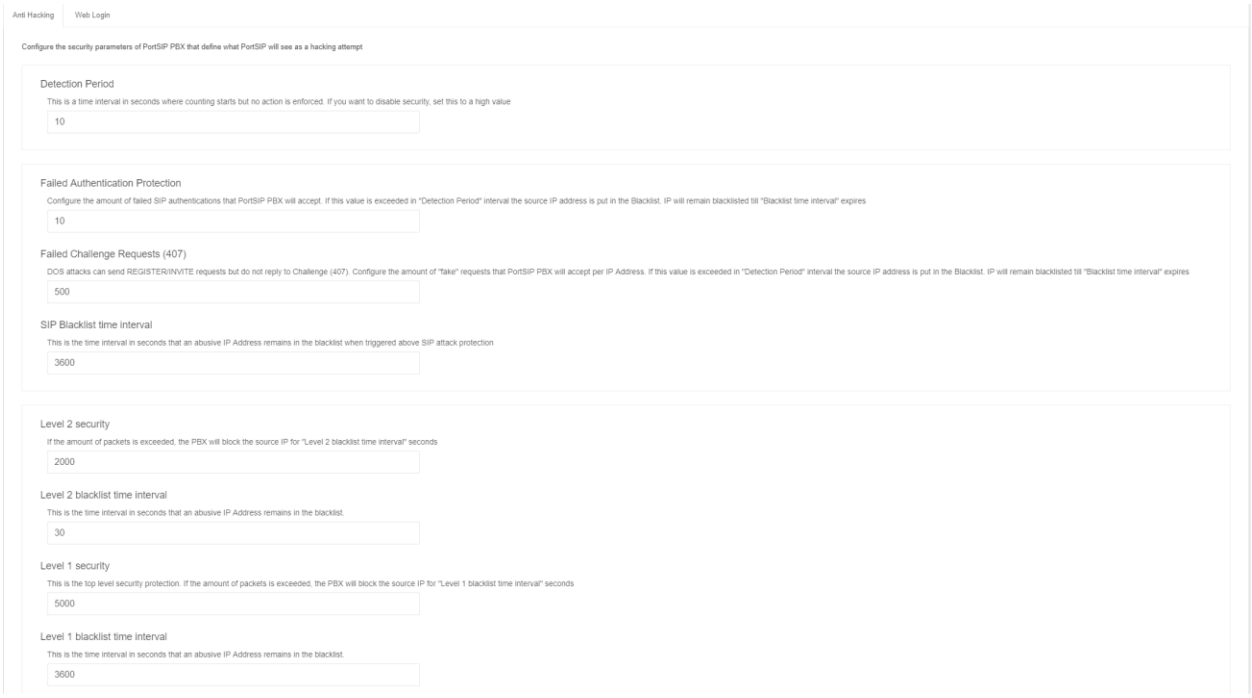
启用/禁用计划备份：要启用“**计划备份**”，请选中该复选框。

选择要备份的文件类型：此部分列出了所有可备份的文件类型，包括“**PBX 核心数据**”、“**系统语音提示**”、“**语音邮件**”等。用户勾中文件类型后方的复选框，表示需要备份该类文件。

计划备份时间：用户可以选择每日或每周备份一次，方法是勾中“**每天**”或“**每周**”后面的复选框。选定后，可以设置具体的备份开始时间。对于每周备份，用户还需要设置备份日期。

11.8 安全

PortSIP PBX 提供了安全功能，其主要目的是在管理员未采取防火墙级别的预防措施情况下，阻止针对 PortSIP PBX 的恶意攻击。它通过检测和阻止可识别和破解分机号码和密码的数据包洪流/DoS 攻击或强力字典攻击。



以上截图显示了 PortSIP PBX “Anti Hacking”配置页面的主界面。您可通过单击菜单“**设置**”>“**安全**”访问。

检测周期

检测单位时间段，以秒计。如果您需要禁用安全功能，请将此字段设置为较大的值。

失败认证保护

该保护措施用于在攻击者尝试使用字典攻击来猜测特定分机的密码时提供防护。要实现此攻击，攻击者需要发送多次请求，服务器发送“代理认证所需信息”后，攻击者将发送认证凭据。而有了这个功能，如果一个 IP 地址在“**检测周期**”内对 PortSIP PBX 发起了 指定次数的错误身份验证尝试，则该 IP 地址将被阻止并放入黑名单，直至达到“**SIP 黑名单时间间隔**”参数中指定的时间限制为止，该值默认为 1 小时。

失败的认证请求 (407)

DOS 攻击可以发送 REGISTER / INVITE 请求，但不会回应认证挑战请求 (407)。配置 PortSIP PBX 可接受的各 IP 地址的“虚假”请求数。如果在“**检测周期**”内超出了此值，源 IP 地址会被加入黑名单，直至超出“**SIP 黑名单时间间隔**”为止，该时间间隔的默认值为 1 小时。

2 级安全

这是第 2 层保护。您可在此指定从单个 IP 地址发送的数据包数量。默认值为每秒 2000 个数据包。如果一个 IP 地址每秒发送了 2000 个以上的数据包，即表示出现异常。此时，攻击者 IP 将被阻止，直至超过“**2 级黑名单时间间隔**”。

1 级安全

这是第一层保护。 如果 IP 地址发送的数据包数量超过了指定的每秒数量，它将在“**1 级黑名单时间间隔**”内被列入黑名单。默认值是每秒 5000 个数据包。在这一层，一旦数据包速率超过这一层，则会强制加入黑名单。

IP 地址由于以上规则被阻止后，它会显示在“**黑名单**”页面，您可在此处将其手动添加至白名单。

12. 黑名单和代码

12.1 代码和 E164

PortSIP PBX 允许设置允许的国家/地区代码和禁止的国家/地区代码，以此阻止分机用户拨打特定国家/地区的号码。

要允许或禁止某个国家/地区代码，请单击“黑名单和代码”>“代码和 E164”>“允许的国家/地区代码”，您可选择或取消选择一个或多个国家/地区。

12.2 号码黑名单

PortSIP PBX 支持将分机用户号码/用户名加入到黑名单里，PBX 将会阻止所有来自黑名单号码或者发往黑名单号码的呼叫。

可以按照如下步骤将一个号码加入到黑名单：

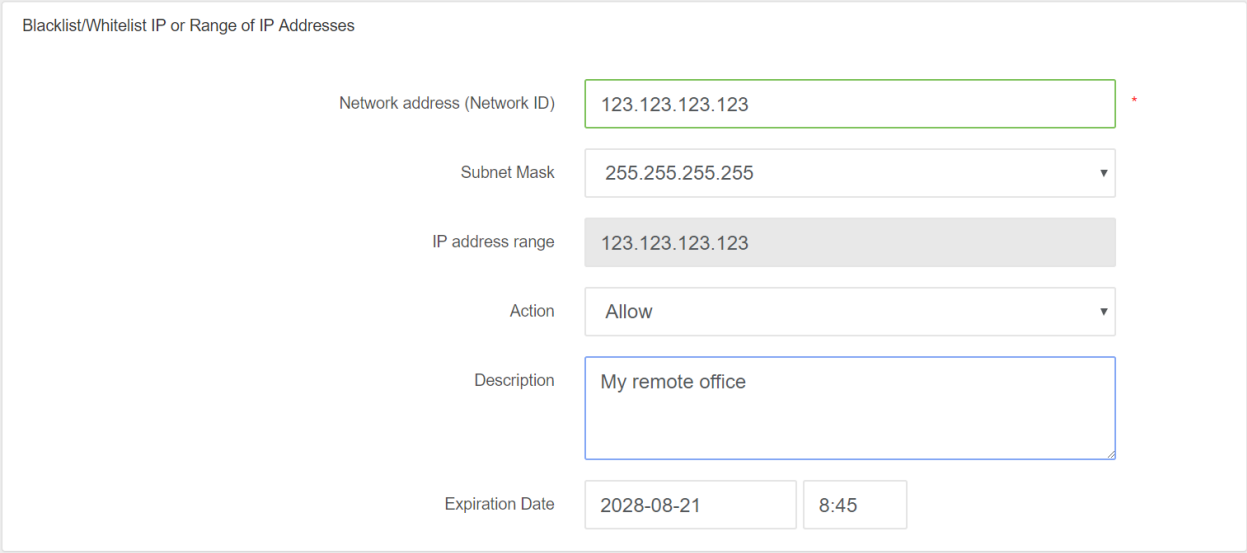
1. 登录到 PortSIP PBX 的管理控制台。
2. 选择左侧菜单“**号码黑名单**”。
3. 点击“**新增**”按钮新增一个条目。
4. 输入需要加入到黑名单里的号码以及备注。

12.3 IP 黑名单

您可以在 PortSIP PBX 中将 IP 地址添加至黑名单和白名单。所有来自白名单 IP 地址的流量都可不经过反入侵功能的检查，直接通过。而所有来自黑名单 IP 地址的流量会被直接丢弃。

将白名单条目添加至 PortSIP PBX

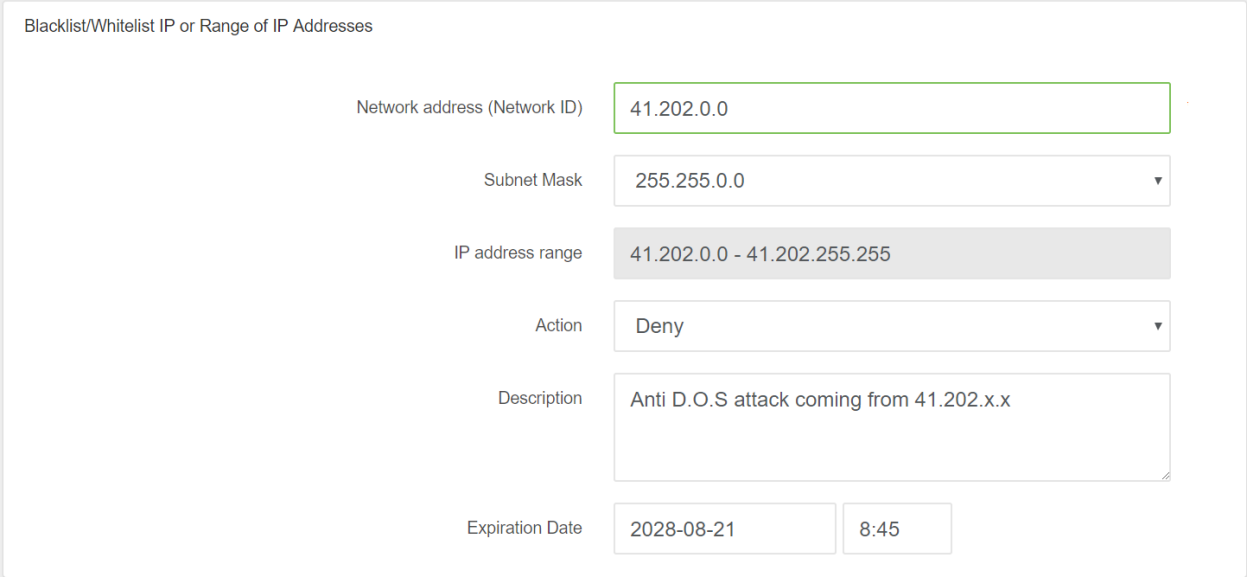
假设您的某个远程办公室可以连接到您的 PortSIP PBX。您的远程办公室的公网 IP 地址是 123.123.123.123。来自此 IP 地址的流量可以信任。要将此 IP 地址添加至白名单，您需要执行以下操作：



1. 登录至 PortSIP PBX 管理控制台。
2. 单击“黑名单和外拨代码”>“IP 黑名单”。
3. 单击“添加”以添加一个条目。
4. 输入要允许的 IP 地址。在此示例中，请输入 123.123.123.123（您也可以输入 123.123.123.0，然后选择子网掩码，以允许一个 IP 范围）。
5. 在“操作”字段选择“允许”。
6. 为此 IP 地址添加一条描述，例如“我的远程办公室”。
7. 单击“确定”。已加入白名单的 IP 地址会在 IP 黑名单页面显示一个允许条目。所有来自该 IP 地址的流量均可不经检查，反入侵算法也不会对其生效。

阻止单个 IP 地址或一个 IP 地址范围

现在看看另一个场景。假设系统遭受了来自以下 IP 的分布式入侵 - 41.202.160.2 和 41.202.191.5。这两个 IP 地址已被 PortSIP PBX 的反入侵自动检测机制加入了黑名单。为了确保不会受到来自该 IP 范围的任何流量，您决定将整个 IP 范围加入黑名单。在此情况下，我们会将 41.202.0.0 到 41.202.255.255 的整个 IP 范围加入黑名单，也就是说，所有以 41.202. 开头的 IP 地址都将被阻止。



1. 登录至 PortSIP PBX 管理控制台。
2. 单击“**黑名单和外拨代码**”>“**IP 黑名单**”。
3. 单击“**添加**”以添加一个条目。
4. 在“**网络地址**”内输入要阻止的网络范围的第一个 IP 地址。在此示例中，输入 41.202.0.0。
5. 由于我们希望阻止以 41.202 开头的所有 IP 地址，因此，我们需要选择子网掩码 255.255.0.0。此掩码中包含的所有 IP 地址范围都会显示在下方。
6. 在“**操作**”字段选择“**拒绝**”。
7. 为此 IP 地址添加一条描述，方便您记忆添加此条目的理由，例如“**防御来自 41.202.x.x 的 D.O.S. 攻击**”。
8. 单击“**确定**”。IP 黑名单页面显示一个拒绝条目。所有来自该 IP 地址的流量均可会被检查，反入侵算法随即生效，来自该 IP 地址的所有数据包均会被丢弃和忽略。
9. PortSIP 黑名单/白名单机制不能完全替换防火墙。它仅提供了一种防御机制，帮助区分可信任和不可信任的流程。如果您需要阻止所有面向您忘了的流量，而仅允许来自您的 VoIP 提供商 IP 地址的流量，您则需要在防火墙上进行设置。

在黑名单中配置 IP 地址范围时，您需要确保该范围未包含 PBX 的 IP 地址。

13. 个人资料

管理员 admin 或者租户用户登录到 PBX 的管理控制台之后，可以点击左侧的菜单“**个人资料**”来管理他们的个人资料。

13.1 常规

在“**常规**”选项卡部分，admin 或者 tenant 用户可以修改自己的个人资料，包括如下选项：

用户名：admin 或者 tenant 用户的用户名。

密码：可以在这里修改用户的密码，密码修改之后，登录的时候必须得输入新密码。

公司名和公司网站：Admin 或者租户用户的公司名和网站，所有分机用户的公司名和网站都将沿用于创建他们的 admin 或者租户用户。

邮箱：用于接收 PBX 发送的各种通知邮件的 admin 或租户用户的信箱。

时区以及货币：设置 admin 或者租户用户的时区以及货币，该项设置对 admin 或者该租户创建的所有分机用户均产生影响。

对所有的外呼通话计费：选中此选项后，分机用户通过中继/VoIP 提供商发起外拨通话并且分机余额不足，则通话失败；如果通话期间余额不足，通话会自动挂断。

对所有的接入通话计费：选中此选项后，分机用户收到来自中继/VoIP 提供商的接入通话并且分机余额不足，则通话失败；如果通话期间余额不足，通话会自动挂断。

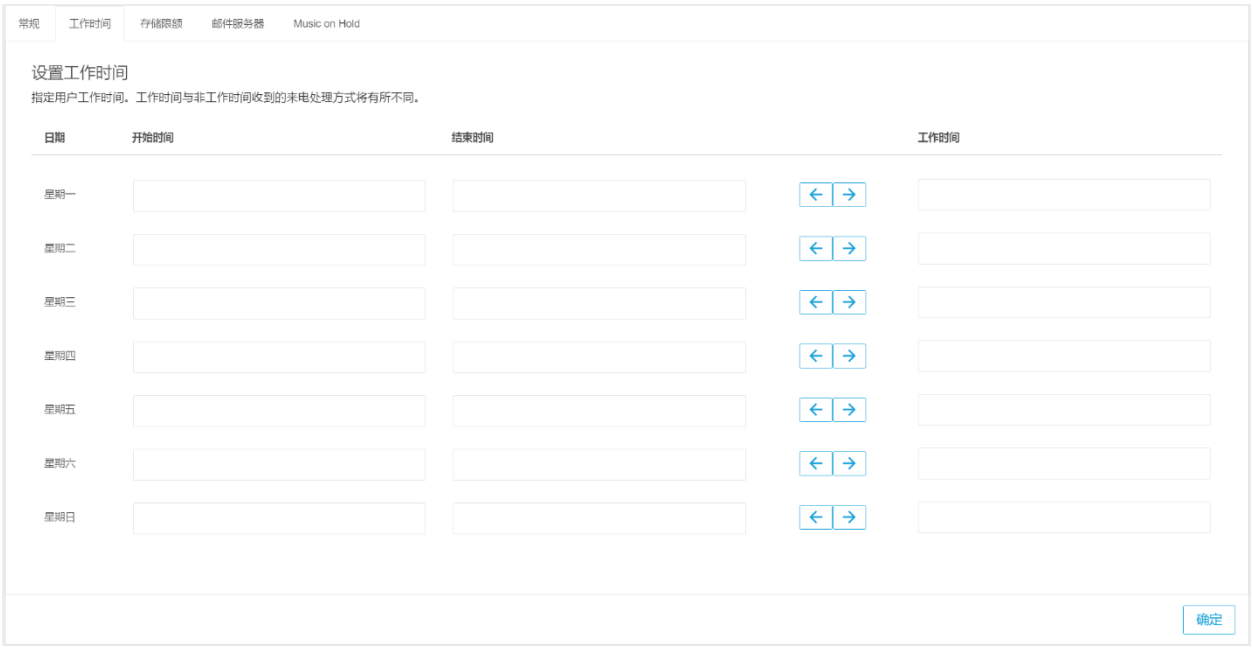
允许分机用户修改个人 SIP 密码：如果未选中此选项，分机无法修改其个人 SIP 密码。

分机音频录音：如果选中了此选项，分机的所有通话将被录制为 wav 文件。

分机视频录音：如果选中了此选项，分机的所有视频通话都会被录制为 AVI 视频文件。

13.2 工作时间

在 PortSIP PBX 里面可以指定工作时间，然后根据工作时间和休息时间设置来电路由。比如将在工作时间内收到呼叫转移到分机号码，将非工作时间收到的呼叫转移到语音信箱。



选择 PortSIP PBX 管理控制台左侧的“**个人资料**”菜单，点击“**工作时间**”，然后点击左右箭头按钮来设置上班时间。

13.3 存储限额

点击“**存储空间配额**”，在这里可以看到被分配的存储空间配额。

录音文件：指定存储录音文件的空间，默认值是 0，表示无限制。

语音邮件：指定存储语音邮件的空间，默认值是 0，表示无限制。

通话记录：指定存储通话记录的空间，默认值是 0，表示无限制。

要设置录音文件、语音邮件和通话记录文件的最大保留期限，请输入保留天数，然后单击“**确定**”。

13.4 邮件服务器

如果想让 PortSIP PBX 发送邮件通知，比如发送欢迎邮件给新创建的分机用户，发送通话记录报告、语音邮件通知等，那么你必须转到“个人资料”>“邮件服务器”设置 SMTP 服务器。

如果使用 Google SMTP Server 来发送邮件，请需要确保已经为 Gmail 账户启用了“**允许不够安全的应用访问您的帐户**”选项，请阅读下列链接了解更多详细信息。

允许不够安全的应用访问您的帐户

允许安全性较低的应用访问帐户

如果使用的是 Google SMTP Server，你还需要选择通过 SMTP 服务器发送邮件的时候使用 TLS 还是 SSL 来连接 SMTP 服务器发送邮件。

13.5 Music on Hold

利用“Music on Hold”功能，用户可以设置通话保持音乐及播放模式。

已启用：用户可以选中该选项，启用“Music on Hold”功能。这样在某个通话处于保持状态时，系统会为被保持通话的呼叫一方播放设置的音乐。要启用该功能，用户必须至少指定一个“Music on Hold”音乐文件。

随机播放音乐：选中此选项后，系统将为被保持通话的一方随机播放音乐。默认值为“每日随机播放”。

按通话随机播放：在选中启用“随机播放音乐”后，用户可以选择“按通话随机播放”，那么为每个被保持的通话播放的音乐可能不同。

每日随机播放：“随机播放音乐”的默认值。

Music on Hold：用户可在此处指定播放音乐，方法是通过“上传”按钮上传自定义的音乐。要启用“Music on Hold”功能，此选项为必填项。目前仅支持 .WAV 格式。

音乐文件 1：

.....

音乐文件 9：用户可在此选择上传更多的音乐文件，用于随机播放。

13.6 事件 URL

事件 URL

通过设置事件 URL，PortSIP PBX 可使用 POST 方法通过 HTTP 请求向第三方服务器发送 CRD（通话详情报告）和分机活动详细信息。CDR 以 JSON 格式编码。

要设置该值，请转至管理控制台的“**个人资料**”>“**事件 URL**”。

CDR URL

通过对 CDR URL 的设置，我们可以让 PortSIP PBX 在每一个呼叫结束后，将 CDR（通话详细记录）通过 HTTP POST 方法根据指定的 URL 发送到第三方服务器，CDR 的格式为 JSON。

在 PortSIP PBX 的管理控制台，点击“**个人资料**”>“**CDR URL**”即可进行设置，并提供以下信息：

认证方式：向第三方服务器发送请求时候的认证方式。PortSIP PBX 支持 HTTP Basic Authentication 和 HTTP Digest Authentication。如果不需要认证，选择“**无**”即可。

用户名：认证用户名

密码：认证密码

CDR URL：发送 CDR 给第三方服务器的 URL。例如：http://www.cdrserver.com/add.php。

设置完成后，CDR 将以如下 JSON 格式发送：

{“

call_answered_time”: 1489482637,

“call_cost”: “0.0001”,

“call_direction”: “outbound”,

“call_ended_reason”: “CALLED_DISCONNECT”,

“call_ended_time”: 1489482652,

“call_fail_code”: 0,

“call_final_destination”: “sip: 008618817182298 @callcentric.com”,

“call_id”: “irZ8nUlnUuPM3NFVcwL32g..”,

“call_prefix”: “188”,

“call_rate”: “0.0001”,

“call_start_time”: 1489482609,

“call_status”: “ANSWERED”,

“call_talk_time”: 15,

“call_targets”: [{“

target_add_time”: 1489482609,

```
                “target_answered_time”: 1489482637,

                “target_end_reason”: “DISCONNECT”,

                “target_number”: “008618817182298”,

                “target_domain”: “callcentric.com”,

                “target_ended_time”: 1489482652,

                “target_fail_code”: 0,

                “target_status”: “ANSWERED”,

                “target_ring_duration”: 10,

                “target_talk_time”: 15

        }],

        “call_trunk_name”: “callcentric”,

        “callee”: “sip: 18817182298 @test.com”,

        “caller”: “sip: 101 @test.com”,

        “caller_display_name”: “”,

        “cost_duration_unit”: 60,

        “caller_display_name”: “James”,

        “recording_file_name”: “internal_102 - sipiw.com_101 - sipiw.com_admin_2018_12_08 - 10
_33_21_1512729201_ - oK7QaacDrwk1uD1VtC9Sg… wav”,

        “tenant_id”: “admin”

}
```


发送的 CDR 消息中，**call_start_time**、**call_answered_time**、**call_ended_time**、**target_add_time**、**target_answered_time** 和 **target_ended_time** 都采用 UNIX 时间格式，表示 UTC 时间从 1970 年 1 月 1 日起始经过的时间秒数，用户需要自己根据时区来计算实际的时间。

talk_time 表示实际通话时间的秒数。

分机事件

要将分机事件活动发送给第三方服务器，应提供以下选项值：

认证方式：向第三方服务器发送请求时使用的认证方式。PortSIP PBX 支持 HTTP Basic Authentication 和 HTTP Digest Authentication。如果无需认证，请选择“**无**”。

用户名：认证用户名。

密码：认证密码。

事件 URL：向第三方服务器发送事件所使用的 URL，例如 http://www.eventsserver.com/add.php。

设置完成后，分机事件将通过如下方式发送：

```
{

    “event_type”: “extension_registered”,

    “tenant_id”: “admin”,

    “extension_number”: “101”,

    “source_ip”: “192.168.0.98”,

    “time”: 1489482652,

    “domain”: “sip.portsip.net”

}
```

13.7 SMS

SMS

通过设置 SMS，PortSIP PBX 能够在从分机收到短信时发送 SMS 消息。要设置该功能，请转至管理控制台的“**个人资料**”>“**SMS**”。

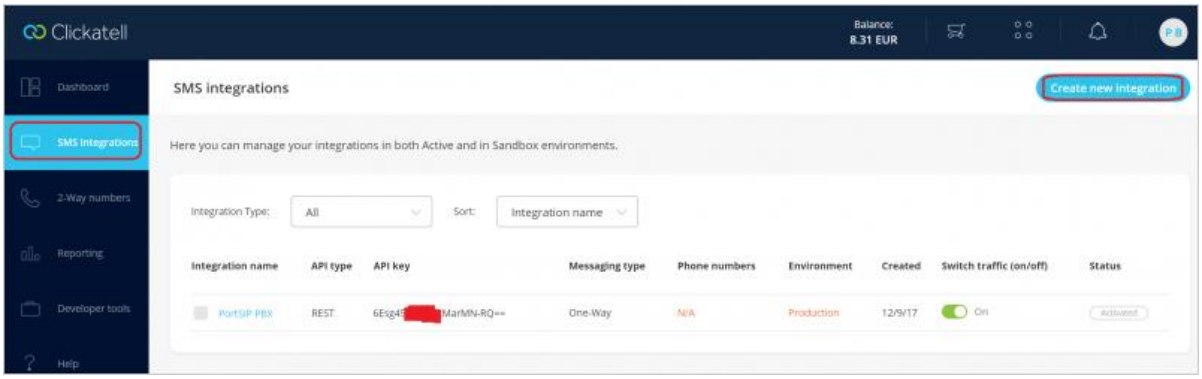
要启用 SMS 功能，应提供以下选项值：

启用：通过选中/取消选中该选项，您即可启用/禁用 SMS 功能。

SMS 提供商：PortSIP PBX 当前支持的 SMS 提供商包括 Twilio、Clickatell、Nexmo、SMSAPI。您可以从这些提供商注册一个账号。

设置 Clickatell

Clickatell 是一个 SMS 提供商，您可以通过访问 https://www.clickatell.com 注册账号并登录。

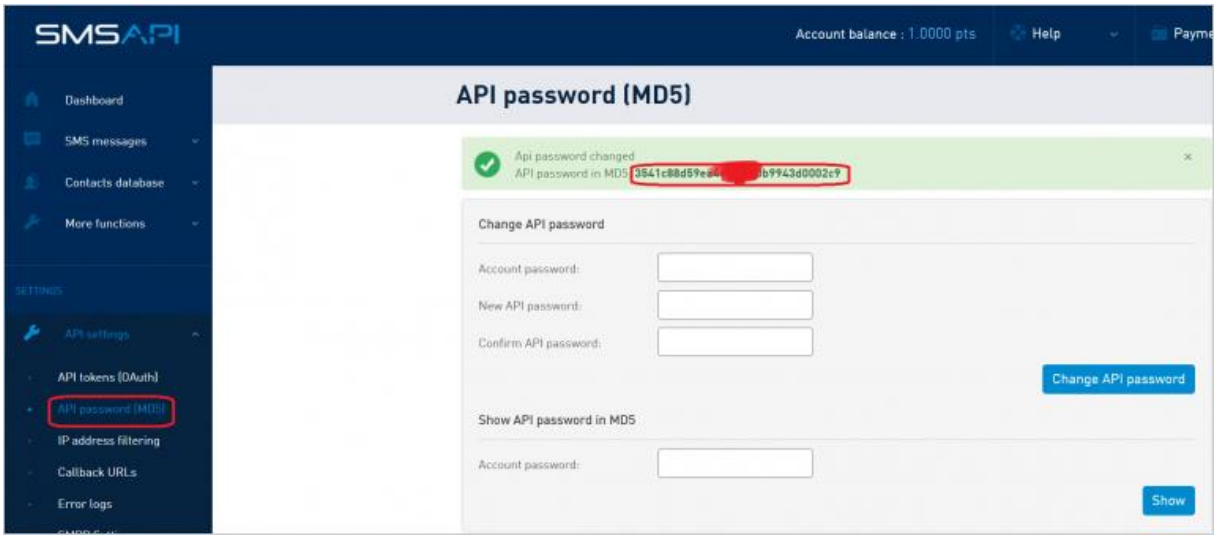


单击左侧菜单的“**SMS 集成**”，然后单击右上角的“**创建新集成**”。跟随设置向导创建集成，并在创建完成后复制 API 密钥。请为 API 类型选择“**REST**”。

现在，在 PortSIP PBX 中，请选择 SMS 提供商“**Clickatell**”，将复制的 API 密钥粘贴到“**API 密钥/令牌**”。

设置 SMSAPI

SMSAPI 是一个 SMS 提供商，您可以通过访问 https://www.smsapi.com 注册账号并登录。

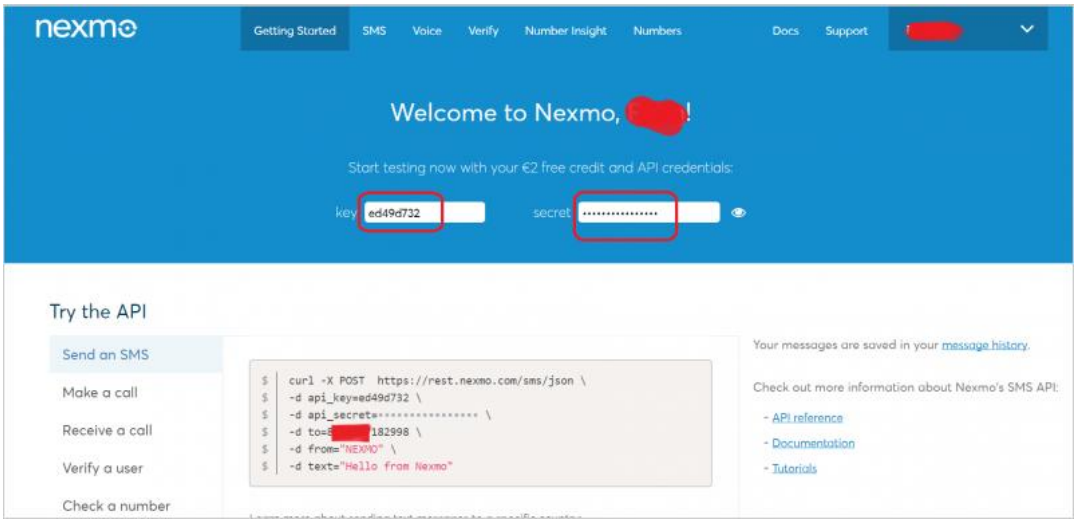


单击左侧菜单的“**API 密码 (MD5)**”。在显示的“**更改 API 密码**”版块，输入您的账号密码和新 API 密码，单击“**更改 API 密码**”。该页面随即显示“**MD5 API 密码**”，请复制该 MD5 字符串。

现在，在 PortSIP PBX 中，请选择 SMS 提供商“**SMSAPI**”，将复制的 API MD5 字符串粘贴到“**API 密钥/令牌**”，为“**用户名**”输入您的 SMSAPI 账号。如果您需要指定 SMS 发送人，请在“**发送人**”字段输入名称。

Nextmo

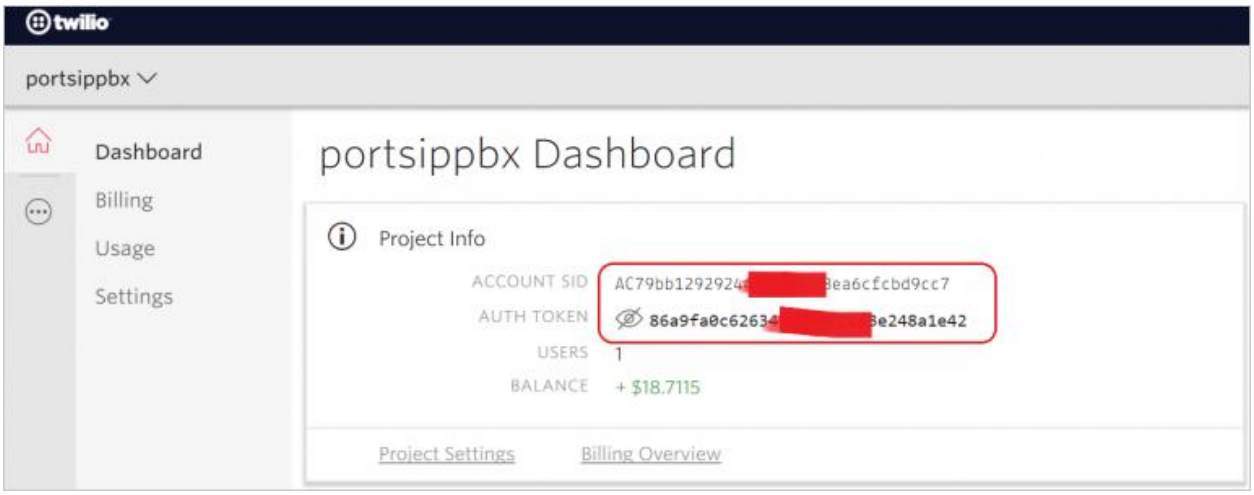
Nextmo 是一个 SMS 提供商，您可通过访问 https://www.nextmo.com 注册账号并登录。



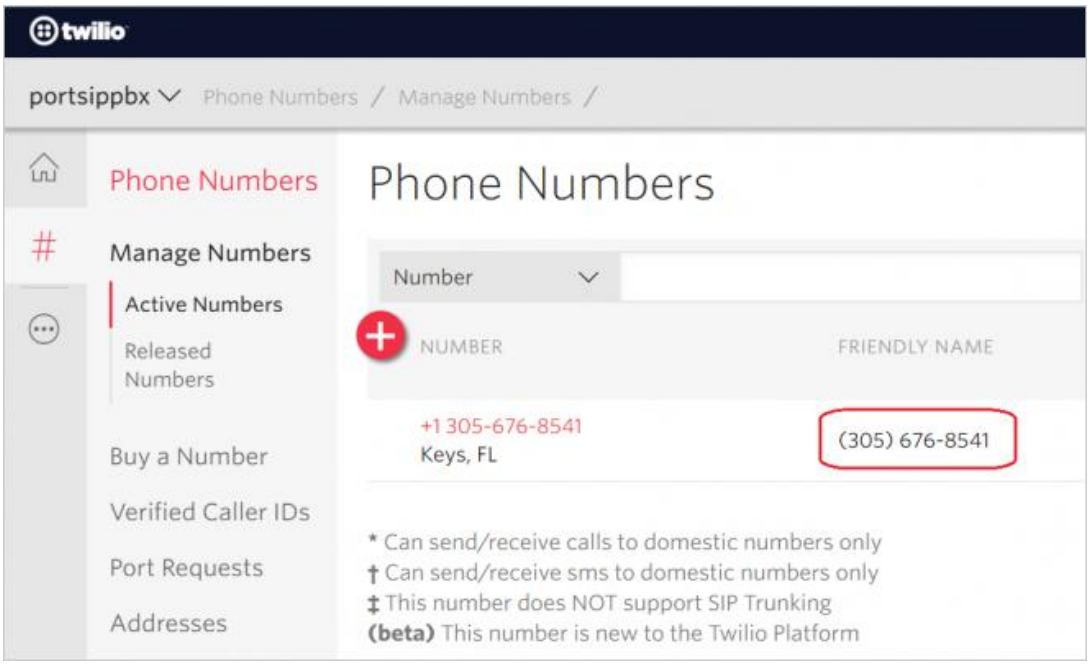
在 PortSIP PBX 中，选择 SMS 提供商“**Nextmo**”，将 Nextmo 的“**密钥**”粘贴到 PortSIP PBX 的“**用户名**”字段，并将 Nextmo 的“**密码**”粘贴到 PortSIP PBX 的“**密码**”字段。如果您需要指定 SMS 发送人，请在“**发送人**”字段输入一个名称。

Twilio

Twilio 是一个 SMS 提供商，您可通过访问 https://www.twilio.com 注册账号并登录。



要配合使用 Twilio，您还需要购买一个号码以发送 SMS。请单击“**电话号码**”版块的“**管理号码**”，根据提示信息购买号码。



现在，登录到 PortSIP PBX，选择 SMS 提供商“**Twilio**”，将 Twilio 控制台仪表板的“**账号 SID**”复制到 PortSIP PBX 的“**用户名**”字段，将 Twilio 控制台仪表板的“**认证令牌**”复制到 PortSIP PBX 的“**密码**”字段，并将该电话号码复制到 PortSIP PBX 的“**发送人**”字段。

注意，在将电话号码复制到 PortSIP PBX 前，请移除“(”、“-”和空格。例如，(305) 676-8541 应更改为 3056768541。

重要提示：在将 SMS 提供商信息填写至 PortSIP PBX 前，建议您在 SMS 提供商管理控制台/面板发送一些测试信息，确保 SMS 正常运行。

示例：

如果您已设置 SMS 提供商，现在分机需要向 PortSIP PBX 发送一条寻呼信息，并指示该寻呼信息是一条 SMS 信息。

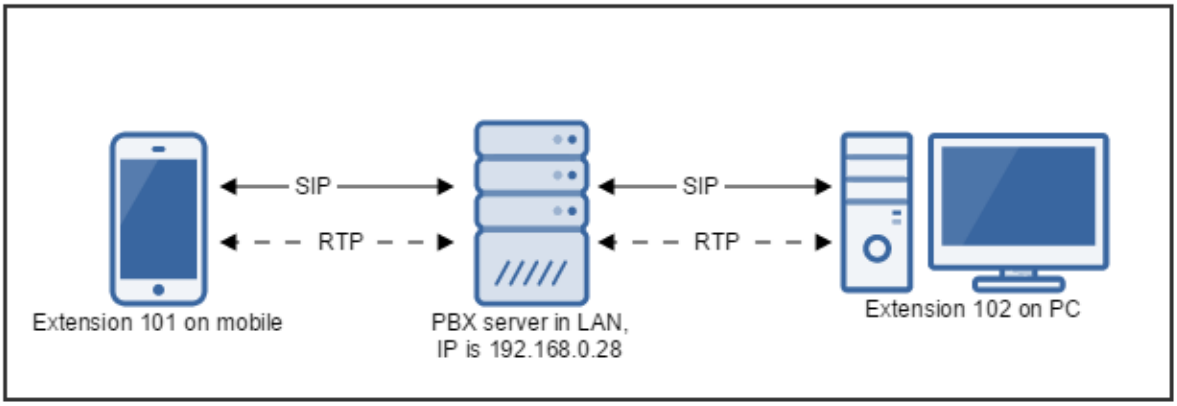
To: <sip:102@sipiw.com>;messagetype=SMS

如果参数“messagetype”出现在“**发送人**”字段，并且值为“**SMS**”，PBX 会将此寻呼信息中继至配置的 SMS 提供商。

14. 部署实例

很多时候，错误的部署方式将导致系统不能发挥出最佳的性能。本章内容将帮助你更好地理解怎样在实际的应用场景合理地部署 PortSIP PBX，并提供了一些有关部署的最佳实践。

14.1 将 PortSIP PBX 部署在局域网

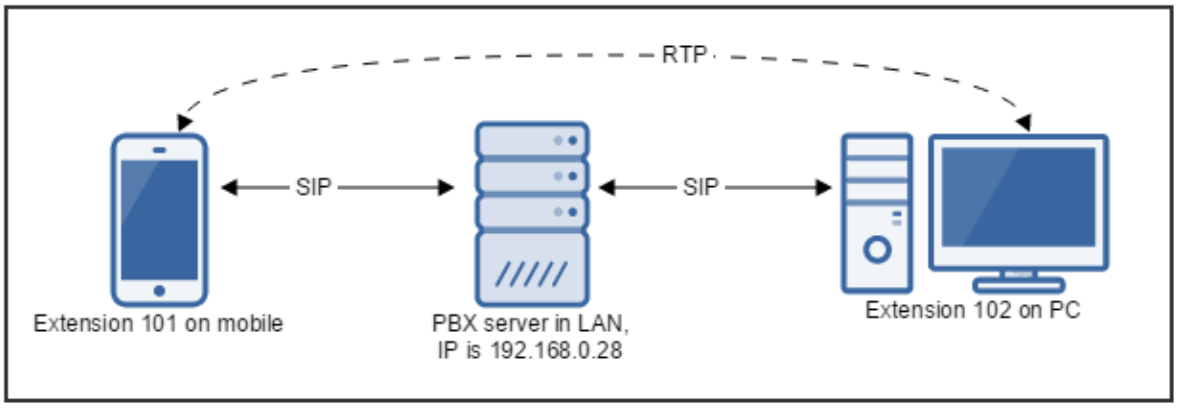


这是一个最简单典型的部署场景，PortSIP PBX 安装在局域网里，在同一局域网里的分机用户注册到 PBX，他们之间可以互相呼叫通话。SIP 信令消息以及 RTP 数据（视频和音频 RTP 包）默认都通过 PBX 中转。

14.2 在局域网里部署大容量并发的 PortSIP PBX

上节 12.1 的部署方式有一个缺点，当有很多并发呼叫的时候，因为所有的 RTP 数据包都是通过 PBX 中转，这样会导致 PBX 所在的服务器 CPU 和网络带宽负载过大。为了降低服务器的 CPU 和网络带宽负载，我们可以在 PBX 里禁用 RTP 转发功能，这样通话双方的 RTP 数据包将直接通过在局域网内以 P2P 的方式收发。

以 admin 用户身份登录 PortSIP PBX 管理控制台，选择左边菜单“**设置**”>“媒体服务**器**”。在媒体服务器列表里，关闭默认媒体服务器的“**启用**”开关，然后点击“**确定**”。



当媒体服务器被禁用后，经过媒体服务器转发的 RTP 包将直接在通话双方之间发送，不再经过媒体服务器，但是 SIP 信令消息依然捅过 PBX。请参考上图。

注意：*如果 PortSIP PBX 部署在 Internet 上，请不要禁用媒体服务器，这样会导致通话时无法传送音频和视频数据。*

14.3 在局域网里部署支持超过 1 万并发通话的 PortSIP PBX

本节将在 12.1 节和 12.2 节的基础上，讲解如何在局域网内定制管理 PBX 规模部署，支持超过 1 万并发通话。

规模部署媒体服务器

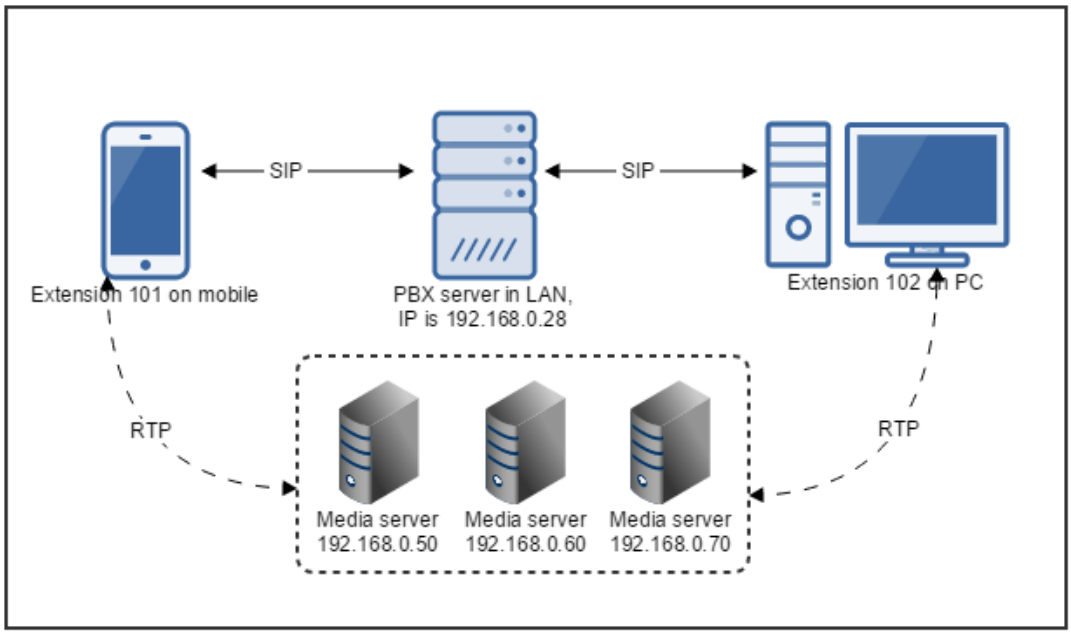
为了在有大量并发呼叫的情况下降低 PBX 服务器的负载，我们可以在 PortSIP PBX 系统里启用负载平衡功能。

第 1 步：从博瞻信息的网站上下载 PortSIP Media Server 独立安装包。

第 2 步：在 PBX 管理控制台里选择左侧菜单“**设置**”>“**媒体服务器**”，所有的媒体服务器都将列出。点击“Built-in Server”的“**启用**”开关，禁用默认媒体服务器，然后点击“**确定**”按钮。

第 3 步：将媒体服务器独立安装包安装在局域网里多台服务器上，并记下服务器的 IP 地址，例如 192.168.0.60、192.168.0.60、192.168.0.70。

第 4 步：在 PortSIP PBX 管理控制台，选择左侧菜单“**设置**”>“**媒体服务器**”，然后点击“**新增服务器**”按钮。输入以上安装在 192.168.0.50、192.168.0.60、192.168.0.70 的三个媒体服务器的名称、IP 地址以及端口等相关信息。



设置完成后，PBX 将根据每个媒体服务器的负载情况，将通话中的 RTP 数据包均衡地通过以上三个媒体服务器进行转发，SIP 信令消息还是继续通过 PBX。详情请参考上图。

按照上述方法，你还可以增加更多的媒体服务器以让 PortSIP PBX 支持更多的并发通话。

规模部署会议服务器

我们可以用规模部署媒体服务器的方式来规模部署会议服务器，以此减轻 PortSIP PBX 会议服务器负载。

第 1 步：从博瞻信息的网站上下载 PortSIP Conference Server 独立安装包。

第 2 步：在 PBX 管理控制台里选择左侧菜单“**设置**”>“**会议服务器**”，所有的会议服务器都将列出。点击“Built-in Server”的“**启用**”开关，禁用默认会议服务器，然后点击“**确定**”按钮。

第 3 步：将会议服务器独立安装包安装在局域网里多台服务器上，并记下服务器的 IP 地址，例如 192.168.0.80、192.168.0.81、192.168.0.82。

第 4 步：在 PortSIP PBX 管理控制台里，选择左侧菜单“**设置**”>“**会议服务器**”，然后点击“**新增服务器**”按钮。输入以上安装在 192.168.0.80、192.168.0.81、192.168.0.82 的三个会议服务器的名称、IP 地址及端口等相关信息。

设置完成后，你可以在 PortSIP PBX 创建多个会议，PBX 将根据每个会议服务器的负载情况，将会议均衡地分别创建在上述的三个会议服务器。

按照上述方法，你还可以增加更多的会议服务器，让你的 PortSIP PBX 能支持更多音频视频会议。

14.4 在阿里云上部署 PortSIP PBX

本节内容将详细介绍怎样在阿里云平台上部署 PortSIP PBX，提供用户之间在互联网上的互相呼叫通话服务；以及怎样将 PBX 连接到 VoIP 运营商/SIP 中继，让用户可以同 PSTN 网络的电话/手机之间进行通话。

注册阿里云账号

如果你已经有了阿里云账号，请跳过这部分内容。

打开阿里云网站，然后点击**“注册”**，按照网站的指示注册账号。

购买云服务器 ECS

第 1 步：在成功注册账号之后，登录到阿里云管理控制台，然后选择购买“云服务器 ECS”，在购买过程中，需要注意如下选项：

> **选择服务器所在地区：**建议根据你的主要用户所在区域来选择，服务器所在地区距离你的用户距离越近越好。
>
> **网络类型：**根据你的实际需求选择网络类型，默认选择经典网络就行。
>
> **安全组：**为你的云服务器选择一个安全组，如果还没有安全组，你可以新创建一个然后选择该安全组。对于选择的安全组，需要按照如下规则配置将内网和公网的入方向以及出方向的所有端口都打开，并且把所有的授权地址段都打开。
>
> 其中 UDP 端口 35000 – 65000 供 PBX 用于转发 RTP 媒体数据。TCP 端口 8800 – 8900 用于服务器管理控制。另外 TCP 6459 以及 3389 端口也必须打开。UDP 端口 5060 是 PBX 用于发送和接收 SIP 消息的，必须打开。
>
> **注意：**如果以后你在 PortSIP PBX 里面增加了新的 SIP 传输协议，比如在端口 5080 增加了 TCP、TLS、WS、WSS 中的任何一个，那么你需要安全组里打开 TCP 5080 端口；如果在端口 5066 增加了一个 UDP 的 SIP 传输协议，那么需要打开 UDP 端口 5066。
>
> **选择实例的 CPU 和网络带宽等：**根据你的需求选择 CPU 和带宽，如果你的 PBX 需要服务多个用户，那么需要将选择更强大的 CPU 和更多带宽。
>
> **镜像选择：**建议选择公共镜像中的 Windows 2008 -2016 的 64 位版本。
>
> **设置密码：**为你选择的 Windows 镜像设置密码。

根据提示付款，云服务器 ECS 购买成功，然后进入阿里云管理控制台，启动你的云服务器 ECS，并记录下公网 IP 地址以备后用。

在阿里云 ECS 服务器上安装 PortSIP PBX 统一通信系统

第 1 步：在使用“ Windows 远程桌面连接”之前，请确认已在安全组里打开了 TCP 3389 端口，并请仔细阅读“远程连接服务器 For Windows”。

第 2 步：使用“Windows 远程桌面连接”登录到你的阿里云 ECS 服务器，从博瞻信息网站上下载 PortSIP PBX，然后进行安装。安装完成后，双击桌面上“PortSIP PBX 管理控制台”图标，输入管理员账号和密码（默认值分别是 admin/admin）登录。

第 3 步：在配置向导的第一步，选择 PBX 运行环境为“**公用网络**”，然后输入开始记录下来的云服务器 ECS 的 IP 地址并点击“**下一步**”按钮。

注意：PBX 的运行环境一定要选择正确，否则将导致 PBX 不能正常工作。

第 4 步：在配置向导第二步, 输入你想使用的 SIP 域名。你可以使用在第一步里设置的 IP 地址做为域名，也可以指定一个其他的域名。该域名仅用于 PBX，不要求必须能够解析。

第 5 步：在配置向导第三步，设置 PBX 的 SIP 传输协议，建议默认设置为 UDP 5060。点击“**确定**”按钮完成设置向导。

第 6 步：在配置向导第四步，设置 SMTP 服务器信息，你也可以跳过此步。

第 7 步：在 PortSIP PBX 管理控制台，选择左侧菜单“**通话管理**”>“**分机用户**”，然后点击“**新增**”按钮创建两个分机用户，例如 101、102。

现在你可以在 IP 电话机或者其他的 SIP 客户端输入刚创建的分机用户信息，然后注册到 PortSIP PBX。

用 SIP 客户端登录到 PortSIP PBX：

1. 从博瞻信息公司网站或者 Apple App Store、Google Play 下载 PortGo Softphone，然后输入如下信息：

   用户名 – 分机用户号码，例如 101。

   密码 – 101 分机用户的密码。

   SIP 服务器 – 阿里云 ECS 服务器的公网 IP，服务器端口为 5060。

   SIP 域名 – 输入在 PBX 配置向导第二步所设置的 SIP 域名。

   SIP 传输协议 – 选择 UDP。

2. 你也可以下载安装其他的 SIP Softphone，比如 CounterPath 的 XLITE/Bria，或者 GrandStream、Yealink、Snom、Polycom、Cisco 等公司的 IP 话机来注册到 PortSIP PBX。

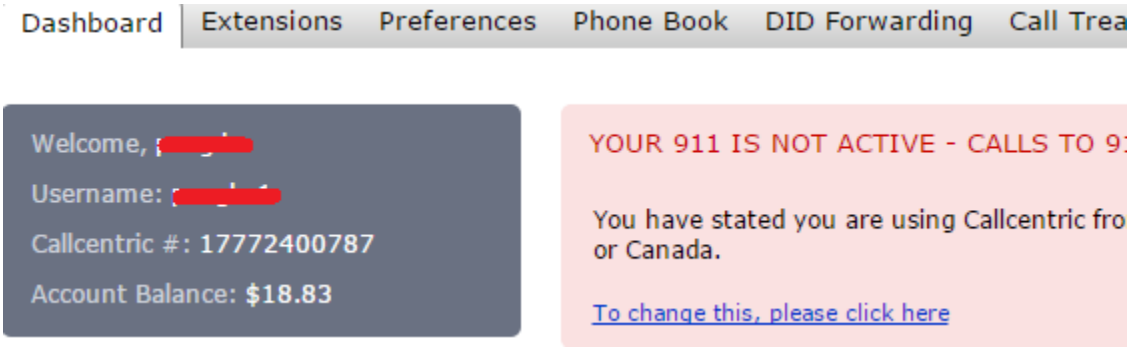
申请 VoIP 运营商/SIP 中继账号

要想通过 PBX 来拨打和接听 PSTN 网络的电话（固定电话或者手机），首先我们需要注册一个 VoIP 运营商/ SIP 中继账号。在这里我们以 CallCentric 为例。

Callcentric 是一家美国的 VoIP 运营商，在世界范围内提供个人或者商业的互联网通信服务。你可以点击这里申请 Callcentric 账号。

在成功注册了 CallCentric 账号之后，需要给账号充值，以及购买一个电话号码 (DID)，具体的详情请浏览 CallCentric 网站或者联系其服务支持人员。

在 CallCentric 的管理控制台里，记录下你的 **Callcentric #号码，**例如 **17772400787**，以及电话号码 (DID) **15169261408。**



配置 VoIP 运营商/SIP 中继

1. 选择菜单“**通话管理**”>“**VoIP 运营商/SIP 中继**”，点击“**新增**”按钮。
2. 给要创建的运营商输入一个容易理解记忆的名字，例如 Test_CallCentric；在国家下拉框选择 US，在“运营商”下拉框选择“CallCentric”。在用户名处输入记录下来的 **Callcentric #号码 17772400787** 并输入密码，其他的选项都保持默认值，然后点击“**确定**”按钮。

点击“**通话管理**”>“**VoIP 运营商/SIP 中继**”，所有已增加的 VoIP 服务运营商/SIP 中继将被列出。如果已经成功连接上 CallCentric 的服务器，状态将显示为“**在线**”。

配置接入规则

选择“**通话管理**”>“**接入规则**”菜单，然后点击“**新增**”，输入如下信息：

规则名称：输入一个容易理解记忆的名字。

类型：选择“DID”。

DID/DDI 号码/掩码：输入在 CallCentric 的 DID 号码（非 Callcentric #）**15169261408。**

接入规则应用于如下服务运营商/SIP 中继：选中之前设置的 Test_CallCentric 运营商。

上班时间：为上班时间接收到的呼叫选择转移规则，勾选“**连接到分机**”，然后选择分机用户

101。

下班时间：为上班时间之外收到的呼叫选择转移规则，选择“**挂断通话**”。

点击“**确定**”按钮完成接入规则的创建。

当某个 callcentric 用户或者 PSTN 用户拨打 DID 号码 **15169261408** 的时候，CallCentric 将把这个呼叫转发到 PortSIP PBX，PBX 用创建的接入规则去匹配这个呼叫。匹配成功后，如果当时时间是上班时间或者没有配置上班时间，呼叫将被转移给分机用户 101；如果上班时间已经被设置，而当时时间是下班时间，则直接挂断呼叫。

配置外拨规则

假定我们想让 PortSIP PBX 将来自分机用户且符合如下条件的呼叫转发给之前添加的 Test_CallCentric 服务运营商：

1 被呼叫的号码是以“00”开头。

2 呼叫是来自 101 或者 102 分机用户，或者来自 110-120 之间的分机用户。

3 现在选择“**通话管理**”>“**外拨规则**”，点击“**新建**”按钮，然后输入以下信息：

规则名称：输入一个容易理解记忆的名字。

号码以指定前缀开始的呼叫：输入 00。

来自指定分机用户的呼叫：输入 101,102,110-120。

通过下列路由发起外拨呼叫：在路由 1 里选择我们开始设置的 VoIP 运营商 Test_CallCentric。假定我们要将被呼叫的号码前缀 00 移除，然后在被叫号码之前增加 0086，那么需要在“截除号码位数”这里选择 2，在“ 号码前缀”这里增加 0086。

点击“**确定**”按钮保存外拨规则。

现在如果分机用户 101 或者 102，或者 110-120 之间的任何一个分机用户呼叫 2213711002986，PBX 都将把呼叫路由至我们设置的 Test_CallCentric VoIP 运营商，并将被叫号码修改为 008613711002986。

多个 SIP 传输协议

在 PortSIP PBX 配置向导里默认配置的 SIP 传输协议是 5060 端口上的 UDP。你也可以在 PortSIP PBX 控制管理台里面增加设置更多的 SIP 传输协议，比如 TCP 和 TLS。

可按照如下步骤增加 TCP 传输协议：

1 在 PBX 控制管理台里选择左侧菜单“**通话管理**”>“**域名和传输协议**”，点击“**新增**”按钮。

2 在传输协议下拉列表里选择 TCP。

3 默认的 TCP 端口是 5063。如果要给 PBX 设置传输协议，那么他们的端口不能相同。

点击“**确定**”按钮保存。

现在你可以在 PortGo Softphone 或者其他 SIP Softphone 里将传输协议设置为 TCP，并将服务器端口设置为 5063 登录到 PBX，或者在 IP Phone 里设置传输协议为 TCP，服务器端口为 5063 登录到 PBX。

增加 TLS 传输协议：请阅读 4.6 节内容。

在阿里云上部署支持大容量并发通话的 PortSIP PBX

本节内容主要说明如何在阿里云上对 PortSIP PBX 进行大规模部署以支持 10000 个以上的并发通话。

我们可以在阿里云用 **12.3** 节的方法部署 PortSIP PBX 以支持大容量并发通话。

规模部署媒体服务器：

第 1 步：从博瞻信息的网站上下载 PortSIP Media Server 独立安装包。

第 2 步：在 PBX 管理控制台里选择左侧菜单“**设置**”>“**媒体服务器**”，所有的媒体服务器都将列出。点击“已启用”开关禁用默认媒体服务器。

第 3 步：在阿里云控制管理台购买新的云服务器 ECS，将媒体服务器独立安装包安装在上面，记下服务器公网 IP 地址，并在云服务器的安全组规则里打开 45000-65000 的 UDP 端口，以及 8896 的 TCP 端口。

第 4 步：在 PortSIP PBX 管理控制台里，选择左侧菜单“**设置**”>“**媒体服务器**”，然后点击“**新增**”按钮。输入安装有媒体服务器的云服务器 ECS 的公网 IP 地址以及端口 8896 等相关信息。

第 5 步：重复第三步和第四步可增加更多的媒体服务器。

规模部署会议服务器：

第 1 步：从博瞻信息的网站上下载 PortSIP Conference Server 独立安装包。

第 2 步：在 PBX 管理控制台里选择左侧菜单“**设置**”>“**会议服务器**”，所有的会议服务器将被列出。点击“已启用”开关禁用默认会议服务器。

第 3 步：在阿里云控制管理台购买新的云服务器 ECS，将会议服务器独立安装包安装在上面，记下服务器公网 IP 地址，并在云服务器的安全组规则里打开 43000 – 44999, 8828 - 8833 的 UDP 端口，以及 8886 的 TCP 端口。

第 4 步：在 PortSIP PBX 管理控制台里，选择左侧菜单“**设置**”>“**会议服务器**”，然后点击“**新增**”按钮。输入安装有会议服务器的云服务器 ECS 的公网 IP 地址以及端口 8878 等相关信息。

第 5 步：重复第三步和第四步增加更多的会议服务器。

激活 PortSIP PBX 授权许可

PortSIP PBX 的免费版本最多支持 3 条并发通话，如果你想要支持更多的并发通话，请联系博瞻信息购买 (sales@portsip.cn) 或者联系博瞻信息的分销商购买商业授权许可。

当你收到你的 PBX 密钥之后，进入 PBX 管理控制台，点击左侧的“设置” -> “授权许可”，然后输入即可。

PortSIP PBX 系统需要定期连接 http://service.portsip.com:6881 服务器的 8880 端口来校验许可证信息，你需要保证安装了 PBX 的机器和 http://service.portsip.com:6881 网络通畅.。否则，PBX 校验许可密钥失败后，会降级成为试用版本，只能进行最大 3 条并发通话。

请不要将你的许可密钥泄露给他人使用，一旦 PortSIP PBX 检测到许可密钥被多人使用，将会将它设置为非法的许可密钥，PBX 会降级成为试用版本，只能进行最大 3 条并发通话。

如果你遇到许可密钥问题，请及时和 PortSIP 支持部门或者代理商取得联系。