



# PortSIP PBX User Guide

Version: v12.6.6

Date: April 25, 2022

Copyright ©2022, PortSIP Solutions, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of PortSIP Solutions, Inc.

## Trademarks



PortSIP®, the PortSIP logo and the names and marks associated with PortSIP products are trademarks and/or service marks of PortSIP Solutions, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of PortSIP.

## End User License Agreement

By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the [PortSIP End User License Agreement](#) for this product.

## Open Source Software Used in this Product

This product may contain open source software. You may receive the open source software from PortSIP up to three(3) years after the distribution date of the applicable product or software at a charge not greater than the cost to PortSIP of shipping or distributing the software to you.

## **Disclaimer**

While PortSIP uses reasonable efforts to include accurate and up-to-date information in this document, PortSIP makes no warranties or representations as to its accuracy. PortSIP assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

## **Limitation of Liability**

PortSIP and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided “as is” without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall PortSIP and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if PortSIP has been advised of the possibility of such damages.

## **Summary of Changes**

### **Changes for Release v12.6.6**

This release includes the following changes:

- OpenSSL was updated to 1.1.1n to avoid CVE-2022-0778
- Resolve an issue where the SIP scanner generates ghost calls (calls that cannot be established but generate spam CDR)
- Fix an issue that might cause the media server to crash if there were a large number of calls on the PBX for a lengthy period of time - a few weeks
- Fix a bug that in some scenarios let the holiday appear as an office hour
- By default, the Flow-Timer(RFC5626) header is disabled
- Fix the CANCEL reason header format issue
- Before the delete operation, a message box pops up for the user to confirm
- Enhancement of performance

### **Changes for Release v12.6.5**

This release includes the following changes:

- Support the tel scheme
- Support mobile push notifications for the intercom group
- Replace the host IP in the Via header with the PBX public IP when the PBX sends a request to the trunk
- Corrected a problem that prevented multiple Timer tokens from being added to the Supported header
- Fixed the format of the Reason header
- If a mobile app hasn't been registered with the PBX within a week, clear the push information
- Fix an issue in which if the client register to PBX over TCP/TLS/WSS, the call would be hung up after 9-10 minutes
- Fixed a bug if the yealink phone performs an attended transfer, the call will not be hangup
- Fix a bug when send massive mobile push notifications cause PBX crashed

## Changes for Release v12.6.4

This release includes the following changes:

- When the PBX detects that the WSS/TLS/TCP client connection is down, then clean the established calls
- Fix a bug where there is no voice when a call is transferred to a mobile app that has enabled push notifications
- Fix a bug in the BYE message where the reason header format is wrong

## Changes for Release v12.6.3

This release includes the following changes:

- SSv2, v3, TLS 1.0, 1.1 have been disabled
- For the blind transfer and picked ringing call, combine the CDR and recording file into a single record
- Add a custom option "**no\_external\_recording**" to stop call recording when a call is made between two external numbers.
- Add a custom option called "**www-authentication**" that allows the PBX to use the www-authentication mechanism
- The call hold status is no longer displayed on the Web Portal

- For Android, fix the crash bug with push notifications
- In the HA deployment, fix the bug where the WebRTC client has no voice
- The WebSocket Interface (WSI) now allows a subscriber to subscribe from multiple locations
- When a queue/group member receives a call from a ring group/queue, add the queue number/group number to the Remote-Party-ID and P-Asserted-Identity headers
- Enhance High Availability, voice will no longer be interrupted if the master server is unavailable
- The recording files will be deleted after 180 days by default
- Fix the bug the caller will no longer hear the MOH if the callee repeats hold/unhold the call a few times
- Fix the bug of **/api/comm\_message/update** and **/api/comm\_message/list**
- Fix the bug that for long time running, the PBX stopped to send the email notification

## Changes for Release v12.6.2

This release includes the following changes:

- Support capture the SIP message and analyze it for troubleshooting on the Web UI with PortSIP Trace Server
- Force the extension and tenant use the strong password
- When an admin/tenant/extension changes his password, must enter the current password.
- Add the **queue\_member\_state** message event of topic **QUEUE\_EVENTS** for the WebSocket Publisher, when an agent of the call queue changed his state to ready/not-ready by REST API or dial code, this event will be pushed.
- Password settings in the Web Portal have been moved to a menu that appears when you click on the avatar.
- Remove the log file path from the log file list view
- Allow users to set a wildcard \* for the "**Exceptions**" of extension forwarding rules, allowing them to designate a break time during business hours
- Fix the BASIC authorization bug for CDR events and Extension events
- Fix the crash bug that occurs when two extensions set forward calls to each other when one of them is busy

- Fix the bug if caller make call to extension from PSTN, and caller hold the call, the MOH is not affected
- Set the minimize of registration time to 300 seconds
- Add the parameter "**member\_number**" of REST API "**api/call\_queues/member\_state/update**" to instead of the parameter **extension\_id**
- Improve the WebRTC client and Windows client App

## Changes for Release v12.6.1

This release includes the following changes:

- Removed the built-in backup/restore features, suggest use the VM snapshot to backup. Or user can simply backup the data directory:

a. Windows: by default it's

```
c:/programdata/portsip
```

b. Linux: by default it's

```
/var/lib/portsip
```

- Support store the recording and log files to the AWS S3.
- Support the Privacy header, if the UA makes call with the Privacy header, the PBX will forward this header to the callee.
- When there have the call reached agent of the ring group/queue, the event will be published to the WebSocket Publish subscriber.
- Provide a custom option allows includes the recording file ID in the CDR event JSON payload.
- The REST API for list the CDR, call recording, black list is changed.
- Fixed a crash bug if works with the MicroSIP App for presence.

## Chapter 1. Getting Started with PortSIP® PBX

This guide is designed to assist administrators deploying PortSIP products in a Windows or Linux environment, and explain a number of deployment modes, architectures, and limitations of the solution.

## 1.1 What is PortSIP PBX

PortSIP PBX (also known as **PortPBX**, **PortSIP UC Server**) is a software-based Unified Communications system for Windows and Linux that works with SIP standard-based IP Phones, Softphones, SIP Trunks and VoIP Gateways to provide a complete PBX solution – without the inflated cost and management headaches of an "**antiquated**" PBX. The SIP PBX supports not only all traditional PBX features, but also includes many new mobility and productivity features.

Calls are sent as data packets over the computer data network instead of the traditional phone network. Phones share the network with computers so no separate phone wiring is required. With the use of a VoIP Provider, SIP Trunk, you can connect existing phone lines to the PortSIP PBX to make and receive phone calls via a regular PSTN line. You can also use a VoIP Provider, which removes the requirement for a gateway. PortSIP PBX interoperates with standard SIP softphones, IP phones or smartphones, and provides internal call switching.

## 1.2 Before Started

### Prerequisite knowledge for Linux

Deploying PortSIP PBX in a Linux environment requires planning and knowledge of session initiation protocol (SIP) audio, video call and presence, Instant Messaging (IM) administration. You should also have knowledge of the following Linux infrastructures:

#### A popular Linux distribution:

- CentOS 7.9 (64-bit)
- Debian 10.x (64-bit)
- Ubuntu 18.04 or 20.04 (64-bit)
- Docker 20.10 or higher
- IPv4/IPv6
- Systemd
- IP tables
- Firewallld
- UFW

This document assumes that the Linux OS is already deployed and administrators of PortSIP

PBX have been allocated with the root permission to Linux.

## **Prerequisite knowledge for Windows**

Deploying PortSIP PBX in a Windows environment requires planning and knowledge of session initiation protocol (SIP) audio, video call and presence, Instant Messaging (IM) administration. You should also have knowledge of the following Windows infrastructures:

A Windows desktop or Windows server OS:

- Windows 10 (64-bit)
- Windows Server 2012 R2
- Windows Server 2016 R2 or higher
- IPv4/IPv6
- Windows firewall

This document assumes that the Windows OS is already deployed and administrators of PortSIP PBX have been allocated with the administrator permission to Windows.

## **Cloud and Virtualization Environment Supported**

To build high-availability communication solution to help clients reducing cost and improving communication performance, PortSIP PBX commits support on cloud services and have confirmed compatibility with following cloud and virtualized environment:

- VMware ESX 5.X and above.
- Linux HyperV
- Microsoft HyperV 20012 R2 and above
- Microsoft AZURE
- Amazon AWS
- Google Cloud
- Digital Ocean
- UCloud

## **System performance depends on following key factors:**

- Maximum simultaneous calls needed for PBX
- Maximum online users needed for PBX
- Recordings for calls

- Recording audio only or both of audio and video
- Maximum online users for audio/video conferences on PBX
- Maximum IVRs (Virtual Receptionist) on PBX
- Maximum Call Queues on PBX
- Maximum Ring Groups on PBX

Depending on the key features listed above, PortSIP PBX is able to run on PCs and servers with various CPUs ranging from Intel i3 CPUs to Inter Xeon.

## Other Requirements

- Latest Firefox, Google Chrome, Edge browser
- Microsoft .NET Framework version 4.5 or higher
- Knowledge of Linux and Linux Internet administration
- Knowledge of Windows and Windows Internet administration
- A constant Internet connection to [stun4.l.google.com](https://stun4.l.google.com) on port 19302
- Ensure server date time is synced correctly.

## FQDN Support

Although PortSIP PBX is designed to be able to run on servers without FQDN specified, we recommend to specify FQGN with following advantages:

- Easier access to Web Portal for PortSIP PBX
- Easier management of IP phones and clients after IP address change for PBX
- Convenient access to HTTPS when accessing Web Portal
- Avoid browser warning when access the WebRTC Client

The FQDN you are using must be able to be resolved correctly into the server with PortSIP PBX installed in LAN. If PortSIP PBX is installed on public network, FQDN must be resolved correctly into the public network address for server with PBX installed.

## 1.3 Getting Help and Support Resources

You can find the guide, manual, video tutorials at the [PortSIP Knowledge Base](#), or send email to [support@portsip.com](mailto:support@portsip.com) to obtain the support.



# Chapter 2. Installation of PortSIP® PBX

This chapter provides the instructions for installing the PortSIP PBX on Windows and Linux.

## 2.1 Downloading PortSIP PBX

The latest free edition of PortSIP PBX could always be found and downloaded at [PortSIP Website](#). It's available for both 64-bit Windows and Linux, but not for 32-bit version.

The free edition of PortSIP PBX offers a maximum of 3 simultaneous calls and 10 extension registrations. If you require more simultaneous calls/extensions, please refer to [License Section](#11.10 License) for more details.

You will get the installer after download completed.

## 2.2 Installing PortSIP PBX on Linux

PortSIP PBX Linux edition is migrated to docker environment, which does not support RPM and Deb installer.

### The OS required:

- CentOS: 7.9
- Ubuntu: 18.04, 20.04
- Debian: 10.x
- Only supports 64bit OS

### Important

From v12.6.1, the PortSIP PBX requires running with the above Linux OS versions. If there already installed the PortSIP PBX which less than v12.6.1, and wish to upgrade to v12.6.1 or a later version, must upgrade the Linux OS to the above version before upgrade the PortSIP PBX.

### Preparing the Linux Host Machine for Installation

Tasks that MUST be completed before installing PortSIP PBX:

- If the Linux on which PBX will be installed is located in LAN, assign a static LAN IP

address; if it's in public network, please assign static IP address for public network

- Install all available updates & service packs before installing PortSIP PBX
- Do not install VPN software on your PortSIP PBX Server
- Do not install **PostgreSQL** on your PortSIP PBX Server
- Ensure that all power saving options for your System and Network adapters are disabled (by setting the system to High Performance)
- Do not install TeamViewer, VPN and other similar software on the host machine
- PortSIP PBX must not be installed on a host which is a DNS or DHCP server
- Below ports must be permitted by your firewall.

UDP: 45000– 65000, 25000- 34999

TCP: 8899– 8900、 8887-8888、 8881-8885

- Make sure that below ports have not been used by other programs:

UDP: 45000– 65000, 25000- 34999

TCP: 8899– 8900、 8887-8888、 8881-8885

**IMPORTANT:** If you running the PBX on the cloud platform such as AWS, and the cloud platform has the firewall itself, you **MUST** open the ports on the cloud platform firewall too.

## Installing a fresh PortSIP PBX v12.6.5 for Linux

To install the PortSIP PBX for Linux, please refer to: [Setup PortSIP PBX for Linux](#)

## Configuring Linux Firewall Rules

After having successfully installed PortSIP PBX, the PortSIP PBX ports has been opened with Linux firewall.

If your server has a firewall which is blocking the ports, you must open the below ports in order to make the PortSIP PBX working properly.

- UDP ports: **45000– 65000, 25000- 34999**. These ports are used for the RTP sessions.
- TCP: **8899– 8900、 8887-8888、 8881-8885**. These ports are used for the Server control and WebRTC client.
- UDP: **5060**. This is the default UDP transport for SIP communications (to send and receive SIP signaling).
- TCP: **5065**. This is the default WSS transport for SIP communications in browser (to send and receive SIP signaling).

You also need to open the port that you are using for adding new transport:

- Assume you have added a TLS transport on port 5063, you must open TCP port 5063 in your Linux firewall and
- Assume you have added a TCP transport on port 5061, you must open TCP port 5061 in your Linux firewall
- Assume you have added a UDP transport on port 5068, you must open UDP port 5068 in your Linux firewall

**IMPORTANT:** If you running the PBX on the cloud platform such as AWS, and the cloud platform has the firewall itself, you **MUST** open the ports on the cloud platform firewall too.

## 2.3 Installing PortSIP PBX on Windows

### Preparing the Windows Host Machine for Installation

Tasks that **MUST** be completed before installing PortSIP PBX.

- If the Windows PC / server on which PBX will be installed is located in LAN, assign a static LAN IP address; if it's in public network, assign a static IP address for public network.
- Install all available Windows updates & service packs before installing PortSIP PBX. The reboot after installing Windows updates may reveal additional updates. Pay particular attention to install all updates for Microsoft .Net before running the PortSIP PBX installation.
- Anti-virus Software should not scan the following directories to avoid complications and write access delays: C:\Program Files\PortSIP; C:\Programdata\PortSIP
- Do not install VPN, TeamViewer software on your PortSIP PBX Server
- Do not install **PostgreSQL** on your PortSIP PBX Server
- Ensure the “**Windows Firewall**” service has been started.
- Ensure that all power saving options for your System and Network adapters are disabled (by setting the system to High Performance).
- Disable Bluetooth adapters if it is a Windows client PC.
- PortSIP PBX must not be installed on a host which is a DNS or DHCP server, or that has MS SharePoint or Exchange services installed.
- Below ports must be permitted by your firewall:  
UDP: 45000– 65000, 25000- 34999

TCP: 8899– 8900、 8887-8888、 8881-8885

- Make sure that below ports have not been used by other programs:

UDP: 45000– 65000, 25000- 34999

TCP: 8899– 8900、 8887-8888、 8881-8885

- Ensure your Windows Firewall is enabled

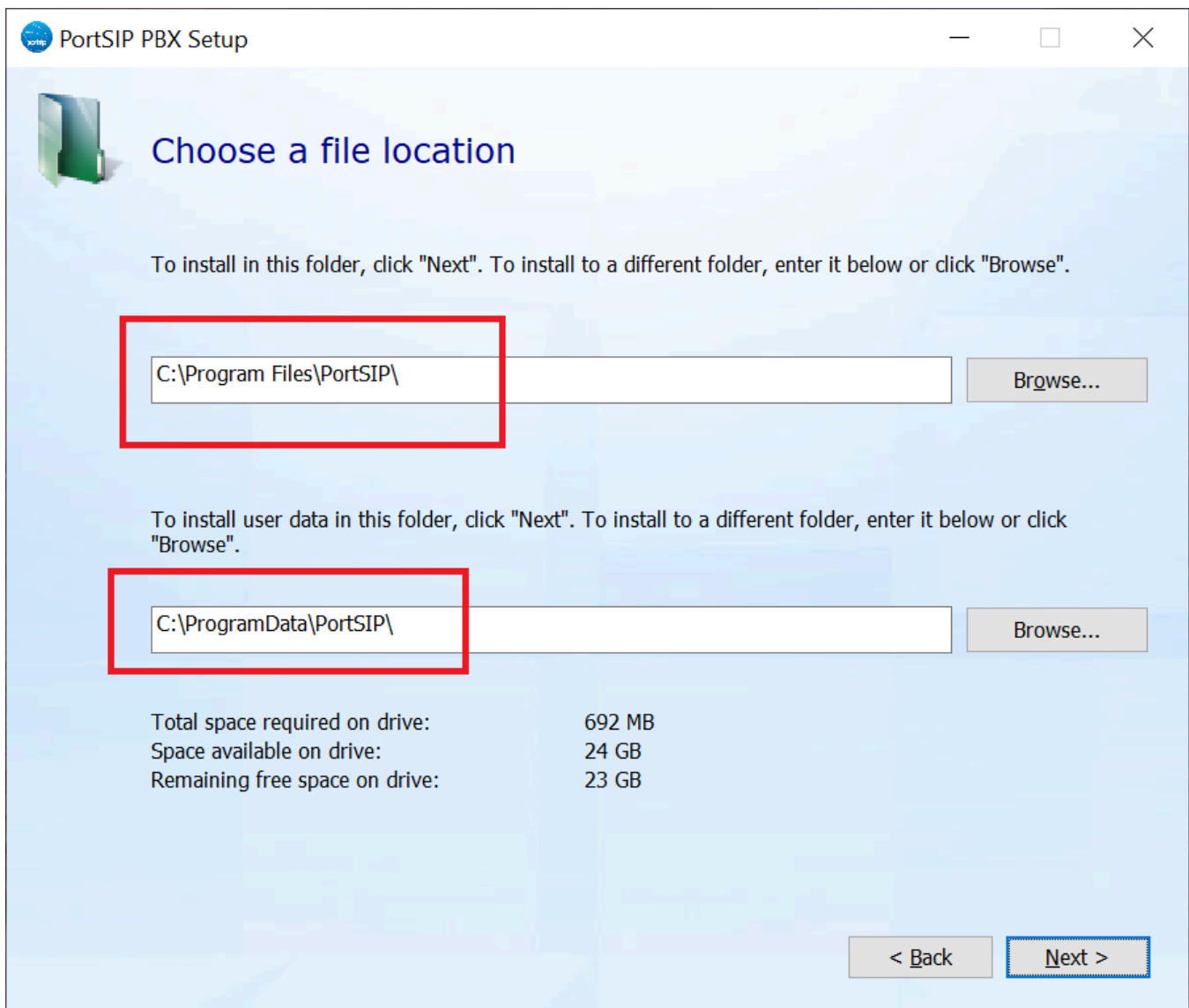
**IMPORTANT:** If you running the PBX on the cloud platform such as AWS, and the cloud platform has the firewall itself, you **MUST** open the ports on the cloud platform firewall too.

## **Installing a fresh PortSIP PBX v12.6.5 for Windows**

To install PortSIP PBX, you only need to double-click the installer, which will guide you through the installation process.

PortSIP PBX services will automatically start after successful installation (and there after every time your computer starts up).

**Important: during installation, when you choose the folders for the PBX, below two folders must not same!!**



## Configuring Windows Firewall Rules

After having successfully installed PortSIP PBX, the PortSIP PBX ports has been opened with Linux firewall.

If your server has a firewall which is blocking the ports, you must open the below ports in order to make the PortSIP PBX working properly.

- UDP ports: **45000– 65000, 25000- 34999**. These ports are used for the RTP sessions.
- TCP: **8899– 8900, 8887-8888, 8881-8885**. These ports are used for the Server control and WebRTC client.
- UDP: **5060**. This is the default UDP transport for SIP communications (to send and receive SIP signaling).

- TCP: **5065**. This is the default WSS transport for SIP communications in browser (to send and receive SIP signaling).

You also need to open the port that you are using for adding new transport:

- Assume you have added a TLS transport on port 5063, you must open TCP port 5063 in your Linux firewall and
- Assume you have added a TCP transport on port 5061, you must open TCP port 5061 in your Linux firewall
- Assume you have added a UDP transport on port 5068, you must open UDP port 5068 in your Linux firewall

**IMPORTANT:** If you running the PBX on the cloud platform such as AWS, and the cloud platform has the firewall itself, you **MUST** open the ports on the cloud platform firewall too.

## 2.4 Upgrade the PortSIP PBX

Please follow this link to upgrade the PortSIP PBX: [Upgrade PortSIP PBX](#)

## 2.6 Avoiding HTTPS Certificate Security Warnings

PortSIP PBX listens on 8888 port for providing HTTP portal to access the PBX Web Portal. Assume your server IP is 172.217.14.16, you should open this URL: <http://172.217.14.16:8888> by your browser. Note: Chrome and Firefox is recommended, please don't use IE.

PortSIP PBX listens on 8887 port for providing HTTPS portal to access the PBX Web Portal.

Assume your server IP is 172.217.14.16, you should open this URL: <https://172.217.14.16:8887> by your browser. Note: Chrome and Firefox is recommended. Please do not use IE.

For HTTPS portal default usage of the self-signed SSL certificate will cause the browser popups SSL certificate security warning.

To avoid SSL certificate warning, you will need to purchase a Signed Certificate (which is an authorized certificate issued by trustworthy certificate authority) to replace the self-signed one. To do this, please:

- Resolve your **PBX web domain** (for example [mypbx.com](http://mypbx.com), if you don't have the

domain you can purchase it from domain provider, such as Godaddy) to the PBX IP in case is 172.217.14.16.

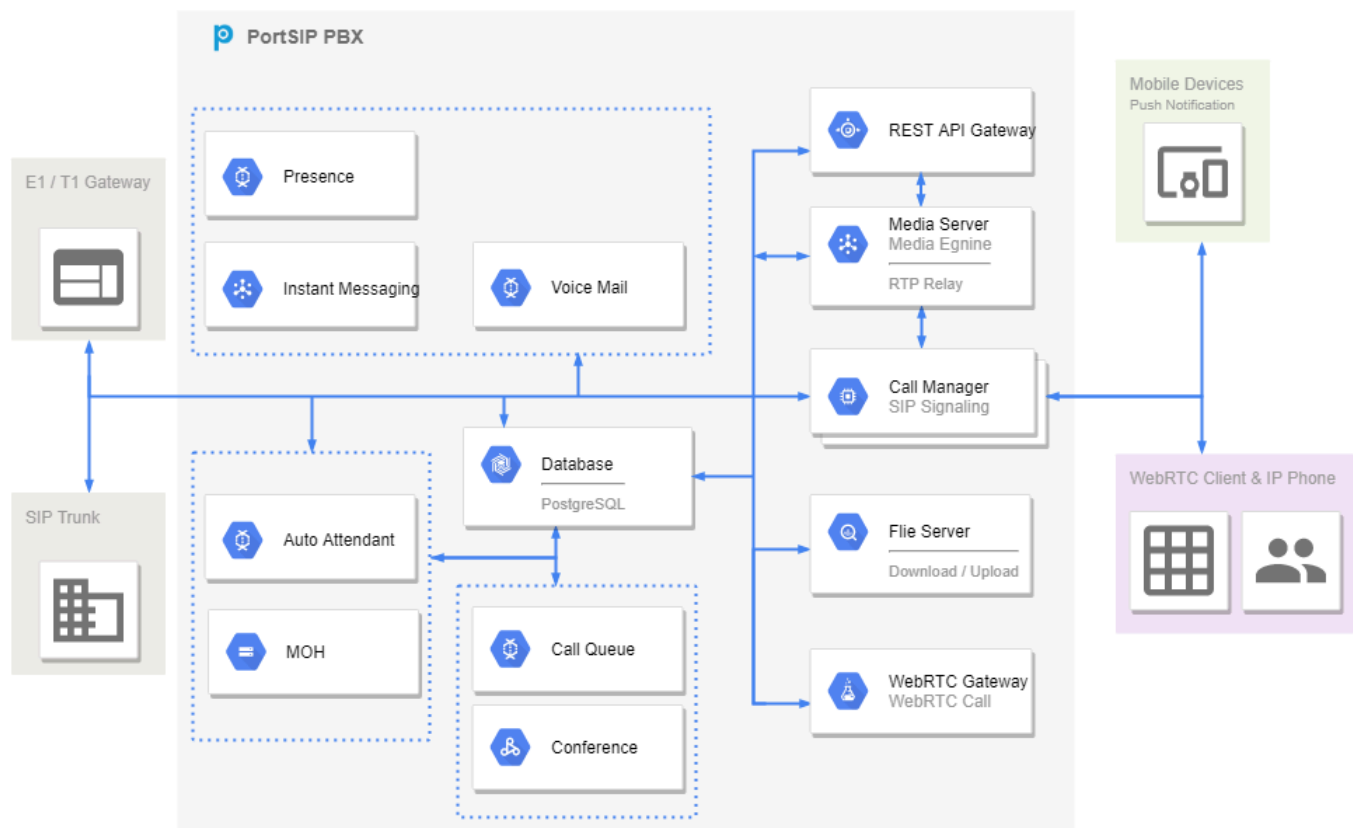
- Go to Thawte or Versign or other certificate providers to purchase a SSL certificate for your PBX Web Domain(in case is [mypbx.com](https://mypbx.com)). Save the private key as **portsip.key**
- After you have obtained the SSL certificate, rename the certificate to **portsip.crt**

Now place the **portsip.crt** and **portsip.key** files in a folder we will use it later.

Note: You may also obtain SSL certificate from [Let's Encrypt](https://letsencrypt.org/) for free.

## Chapter 3. Architecture and deployment of PortSIP® PBX

PortSIP PBX consists of various components, including Call Manager, Media Server, REST API Gateway, File Server, WebRTC Gateway, Database, Call Queue, Conference, Voicemail, MOH, Auto Attendant, Instant Messaging, and Presence Server. Below is a high level architectural diagram about how it works.



PortSIP PBX could be deployed in wide range of scenarios. It is supported in LAN and Internet, as well as popular cloud platforms, such as AZURE, AWS, Digital Ocean and Google Cloud, UCloud, Tencent Cloud, Alibba Cloud.

After successful installation of PortSIP PBX with setup wizard, all you need is a few clicks to make it running.

## Running the PortSIP PBX Configuration Wizard

The PortSIP PBX configuration wizard will guide you through a number of essential tasks to get your system up and running.

PortSIP PBX listens on 8888 port for providing HTTP portal to access the PBX Web Portal, and listens on 8887 port for providing HTTPS portal. More details please read the [2.6 section](#2.6 Avoid HTTPS Certificate Security Warnings).

- Access the PBX Web Portal by visiting <http://172.217.14.16:8888> or <http://mypbx.com:8888> if you resolved your PBX web domain to PBX IP.
- Enter the Username and Password (defaulted as "**admin**" for both) and click the "**Sign in**" button. Note that both the Username and Password are case sensitive. The "**Setup Wizard**" will be displayed which will guide you through the initial configuration step by step

You may change the default Username and Password for "**admin**" by navigating to "**Profile**" > "**General**" in PortSIP PBX Web Portal.

## 3.1 Deploying PortSIP PBX in LAN

Assuming that PortSIP PBX is deployed in LAN with Internet connection, the server/PC has installed the PBX and the private IP is 192.168.0.16. As the PBX is connected to SIP trunk or VoIP provider, users can not only make & receive calls in LAN, but also make & receive external calls with PSTN number and mobile users via services provided by pre-configured SIP trunk or VoIP providers.



1 Configure Network Environment

2 Configure SIP Domain

3 Configure Transport protocol

4 Configure Certificate

5 Configure Mail Server

Web Domain:

Private IPv4:

Public IPv4:

Private IPv6:

Public IPv6:

### Step 1:

If you want to use the **HTTPS** with **PortSIP PBX Web Portal** and **WebRTC client**, you must set up the "**Web Domain**" here, and prepare a SSL certificate for this "**Web Domain**" since the browser requires a trusted certificate otherwise it will block the **HTTPS** and **WebRTC Client**. In case we use the [mypbx.com](https://mypbx.com). You will also need to resolve your Web domain [mypbx.com](https://mypbx.com) to your PBX server IP.

Enter the Public IPv4 if you have a **static public IP** of your LAN. Do not enter the Public IPv4 if your public IP is dynamic.

**Note: the loopback interface (127.0.0.1) is unacceptable.** Only the static IP for LAN where the PBX is located is allowed (do not use DHCP dynamic IP). This private IP must be reachable by your SIP client.

The IP address entered here is the SIP server IP address for PBX. It is required when a SIP client or SIP IP phone registers to PortSIP PBX should be configured as the "**Outbound Proxy Server**".

Configure Network Environment   **2 Configure SIP Domain**   3 Configure Transport protocol   4 Configure Mail Server

SIP Domain:

## Step 2:

You will now need to enter your SIP domain here. The SIP domain is usually a FQDN (Full Qualified Domain Name). You could use IP address instead if you don't have an FQDN. The SIP domain does not have to be resolvable, it's used for PBX authentication purpose only.

After setting up the SIP domain (in this case it is [portsip.io](https://portsip.io)), the extension SIP URI will be [sip:xxx@portsip.io](https://portsip.io). For example, the extension 101 SIP address would be: [sip:101@portsip.io](https://portsip.io). If you don't want to use domain here, enter the private IP (for example: 192.168.0.16) of the Server which has installed the PortSIP PBX instead of the domain (FQDN). In this case the extension 101 SIP address would be: [sip:101@192.168.0.16](https://portsip.io).

Configure Network Environment   Configure SIP Domain   **3 Configure Transport protocol**   4 Configure Mail Server

Transport protocol:

Port:

## Step 3:

You can set transport layer protocol for the SIP signaling here, with the default transport UDP on port 5060.

**Note:** You can add more transports in PortSIP PBX Web Portal after this Wizard.

✓ Configure Network Environment

✓ Configure SIP Domain

✓ Configure Transport protocol

4 Configure Certificate

5 Configure Mail Server

### Upload SSL certificates

In order to use the HTTPS/TLS/WebRTC feature, you must set the "Web Domain" in the first step, and upload the SSL certificates here. By default the PortSIP PBX use self-signed certificate, it will cause browser warning, you can purchase the certificate from a SSL certificate provider or the "Web domain" to avoid the warning. You will also need to resolve your PBX server IP to the "Web domain".

Protocol:

WSS ▼

Port:

5065

Certificate:

portsip.crt ⋮

Private key:

portsip.key ⋮

Previous

Next

#### Step 4:

If you want to use the **HTTPS** with **PortSIP PBX Web Portal** and **WebRTC client**, you **must** upload the SSL certificates file here for **WSS transport**, by default the PBX listens **5065** port for WSS transport which communicates with the WebRTC client.

**Note:** You can use the self-signed certificates here but it will cause browser pop ups the warning when you open the WebRTC client, you can purchase a trusted certificate to avoid the browser blocking and warning. More details please read the [2.6 section](#2.6 Avoid HTTPS Certificate Security Warnings).

#### Step 5:

Setup mail server. You may set up the SMTP mail server in this step for receiving notifications, voicemails, conference invitations and CDR downloads. You can use your SMTP server or Gmail SMTP server.

**Note:** This step is not mandatory. You may choose to setup SMTP server whenever necessary.

By clicking the "**Apply**" button, you have now completed the initial configuration of PortSIP PBX. You will be redirected to Web Portal.

## Step 6

After successfully completed the setup wizard, you have to restart the PortSIP PBX in order to make the SSL certificates work.

### Linux:

```
$ sudo docker exec -it portsip-pbx /bin/bash
$ supervisorctl stop nginx
$ supervisorctl stop gateway
$ supervisorctl start nginx
$ supervisorctl start gateway
```

### Windows:

Restart the Windows Server directly.

After restarted, you can sign in PortSIP PBX Web Portal by URL <https://mypbx.com:8887>

If you don't use trusted certificate files for the WSS transport, you will get the browser warning and blocked when you use WebRTC client.

Please refer to [2.6 Avoid HTTPS Certificate Security Warnings](#2.6 Avoid HTTPS Certificate Security Warnings) to learn how to avoid the browser warning and blocking.

## 3.2 Deploying PortSIP PBX in the cloud

PortSIP PBX can be deployed on popular cloud platforms such as AWS, GCE, AZURE, Digital Ocean.

In this section we will use the AWS as an example, as the other cloud platforms are quite similar to the way how AWS works.

When PortSIP PBX is deployed on AWS, user can make or answer calls through PortSIP PBX with other users through Internet, and make or answer external calls via SIP trunk or VoIP provider.

Please refer to [Creating an AWS account](#) if you do not have an AWS account, and you will need to launch an EC2 instance for installing the PortSIP PBX.

Allocate New Address    Actions ▾

Filter by attributes or search by keyword

<input type="checkbox"/>	Elastic IP	Instance	Private IP Address
<input checked="" type="checkbox"/>	54.183.120.146	i-5290b492 (Windows_PUCS)	172.31.16.207

### Step 1:

On the left bar of AWS EC2 Web Portal, choose “**Elastic IPs**”. As you see the “**Elastic IP**”, please write it down for future use. If the “**Elastic IPs**” does not exist, click “**Allocate New Address**”, and associate the Elastic IP to your instance.

1 Configure Network Environment

2 Configure SIP Domain

3 Configure Transport protocol

4 Configure Mail Server

Web Domain:

Private IPv4:

Public IPv4:

Private IPv6:

Public IPv6:

[Next](#)

### Step 2:

In the Configuration Wizard of PortSIP PBX, enter the private IP of AWS EC2 as “**Private IPv4**”, and enter the “**Elastic IP**” of AWS EC2 as “**Public IPv4**”.

Now remaining steps are same to the "[3.1 Deploy PortSIP PBX in LAN](#3.1 Deploy PortSIP PBX in LAN)"

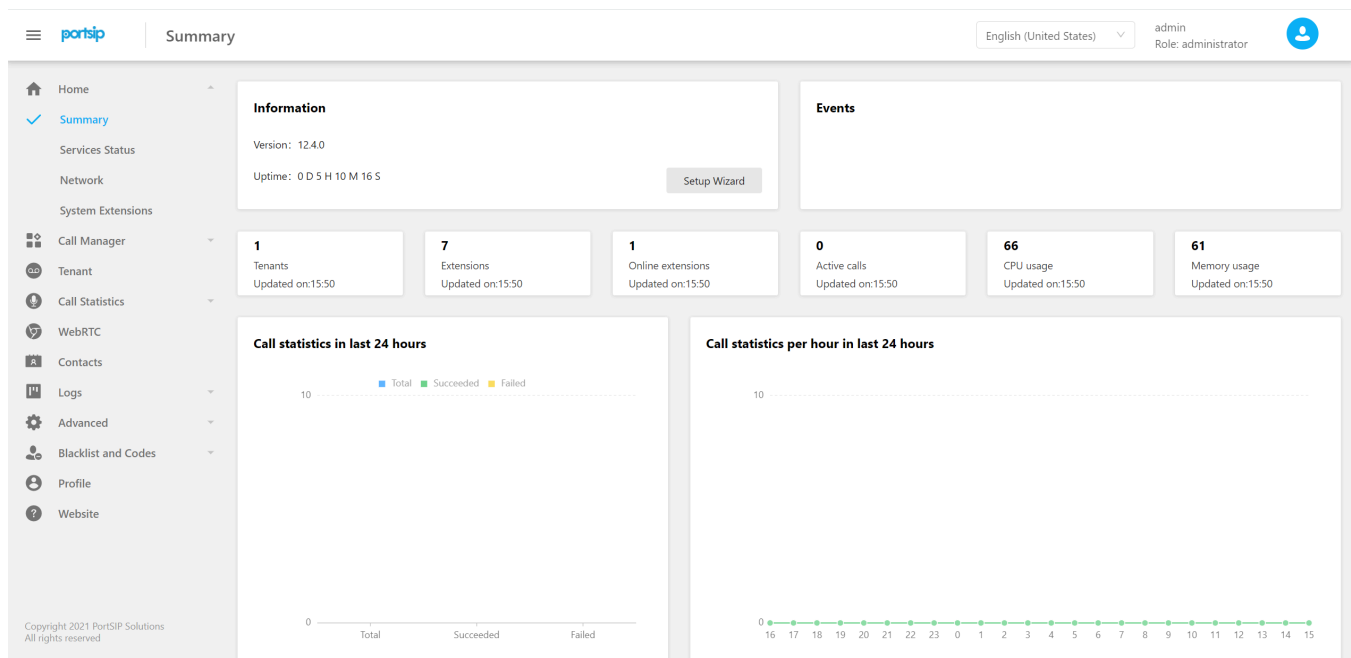
## 3.3 Deploying PortSIP PBX in other scenarios

If you would like to deploy PortSIP PBX in other scenarios which are not mentioned above, you will need to get the server IP address (public IP and private IP) and enter in the PBX setup wizard and follow the Configuration Wizard for deployment.

**Note:** if the server only has public IP but no private IP, **please enter the public IP for both Private IPv4 and Public IPv4.**

# Chapter 4. PBX Overview

## 4.1 Summary



In this page we can have an overview of the PBX statistics:

- Version
- Uptime
- Events
- Extensions
- Tenants
- Active Calls
- CPU and memory usage

- Call statistics for the past 24 hours

## 4.2 Services Status

services

You may navigate to “**Home > Service Status**” menu in the PortSIP PBX System Web Portal to quickly view if all PortSIP PBX system services are working correctly.

## 4.3 Network

This section provides an overview of the general network configurations of PBX, including DNS Server, PBX IP, SIP domain, transports. These settings are useful for SIP clients to register to PBX.

## 4.4 System extensions

PortSIP PBX defines services such as Virtual Receptionist (auto attendant), Conferencing, Ring Group, Call Queue, voicemail and Music on Hold as system extensions, which could be used by PBX only. To check if the system services are correctly registered to PBX, please go to “**Home > System Extensions**” menu in the PortSIP PBX System Web Portal.

# Chapter 5. Call Manager

After completing the Configuration Wizard, you may manage PortSIP PBX in the Web Portal.

## 5.1 Domain and Transport

The SIP domain is used during client registration and calling, and it should match the domain part of your own SIP address on your phone - i.e. if other people are going to call your phone, they must use that domain name as part of the SIP address they use to reach you. The domain can be a FQDN or the IP address, for example “[portsip.io](https://portsip.io)” or “**192.168.0.16**”.

The SIP domain is configured within “**Setup Wizard**” when you sign into Web Portal for the first time. To modify a SIP domain, go to “**Call Manager > Domain and Transport**”, and click “**Edit**” button to enter new SIP domain and save.

## SIP Domain

portsip.io

Edit

## Transports

Add

Refresh

Protocol	Port	Status	
UDP	5060	Active	⋮
WSS	5065	Active	⋮

PortSIP PBX supports a wide range of transports, including UDP, TCP, TLS, WSS (WebSocket Security) for SIP message. You need to configure the transport, and set the ports to use when listening for SIP messages.

The default transport has been configured with “**Setup Wizard**”. To make changes, you need to select the “**Call Manager > Domain and Transport**” menu, and click “**Add**” button in “**Transports**” section. The domain must be added before you add a new transport.

**Note:** only administrator are allowed to create or delete SIP transport. When deleting, at least one transport must be left around.

## Add UDP/TCP/WS transport

To add UDP/TCP/WS transport:

- Click the “**Add**” button, choose the UDP/TCP/WS in “**Transport protocol**” box.



The default Transport Port for UDP/TCP/WS is 5060/5063/5062. You may specify another port as you like, but the port must not be in use by other applications

- Click the “**Apply**” button to add the transport

## Add TLS/WSS transport

In order to use the WebRTC Client, we must add the TLS/WSS transport with self-signed certificate.

If you already uploaded the SSL certificate files in the **step 4** of "**Section 3.1**", then the WSS transport is already added.

First of all, prepare the certificate files.

- You have to generate the certificate files by yourself if you have not purchased trusted certificates from a trusted third-party certificate provider(for example, versign, thawte, digicert). Please download the certificate file tool from [PortSIP website](#) (or run *PortCertMaker.exe* in the installation path of PBX), enter your "**PBX Web domain**" which you entered in the step 1 of "**Setup Wizard**". Once clicked “**Generate**” button, certificate files will be generated automatically.
- The certificates include three files (assume your "Web Domain" is [mypbx.com](#)):  
domain\_key\_mypbx.com.pem  
domain\_cert\_mypbx.com.pem  
root\_cert\_mypbx.com.pem
- Rename **domain\_key\_mypbx.com.pem** to **portsip.key**, rename **domain\_cert\_mypbx.com.pem** to **portsip.crt**

You can also follow below steps if you would like to purchase certificate files from a trusted third-party provider (assume purchased certificate for [mypbx.com](#)):

- Generate the CSR file and private key file according to provider’s guide, and keep the files. If you have set the password when generating the private key file, remember it for future use;
  - Rename the private key file as **portsip.key**
  - Submit the CRS file to provider, and download the certificate files after your certificates approved. This step will end up with two files:  
**Intermediate CA certificate** and **SSL certificate**
  - Use a plain text editor for example Windows Notepad (do not use **MS**

**Word**) to open the Intermediate CA file and SSL certificate file, copy the Intermediate CA contents to append to the SSL certificate file, and rename SSL certificate file as **portsip.crt**.

- Click “**Add**” button and choose the TLS or WSS in “**Transport protocol**” box. The default Transport Port for TLS/WSS 5063/5065. You may specify another port as you like, but the port must not be in use by other applications
- Click the Upload button to choose the certificate files that you have generated for uploading, “**portsip.crt**” for the “**Certificate file**”, “**portsip.key**” for the “**Private key file**”.
- Click the “**Apply**” button to add the transport

**Important: after added TLS/WSS transport, please perform below commands to restart server.**

### Linux:

```
$ sudo docker exec -it portsip-pbx /bin/bash
$ supervisorctl stop nginx
$ supervisorctl stop gateway
$ supervisorctl start nginx
$ supervisorctl start gateway
```

### Windows:

Restart the Windows Server directly.

After restarted, you can sign in PortSIP PBX Web Portal by URL <https://mypbx.com:8887>

If you don't use trusted certificate files for the WSS transport, you will get the browser warning and blocked when you use WebRTC client.

Please refer to [2.6 Avoid HTTPS Certificate Security Warnings](#2.6 Avoid HTTPS Certificate Security Warnings) to learn how to avoid the browser warning and blocking.

### Firewall for new added transports

You have to edit your firewall rules to permit the port that you specified for the transports. For example, you have added below transports in PortSIP PBX:

UDP: 5060

TCP: 5061

TLS: 5063

WS: 5064

WSS: 5065

Then you must add below firewall rules for your PortSIP PBX:

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)

## 5.2 Phones

### Phone Auto Provisioning

Once PortSIP PBX is installed, you can configure your IP phones and assign an extension to each phone.

Phones can be configured one by one manually using their web interface, which is time consuming and leads to many errors; Or by using phone provisioning feature offered by PortSIP PBX, which makes it possible to manage phones centrally and remotely and without having to login to the phone's web interface one by one. Using this method you instruct the phone to retrieve its configuration from PortSIP PBX.

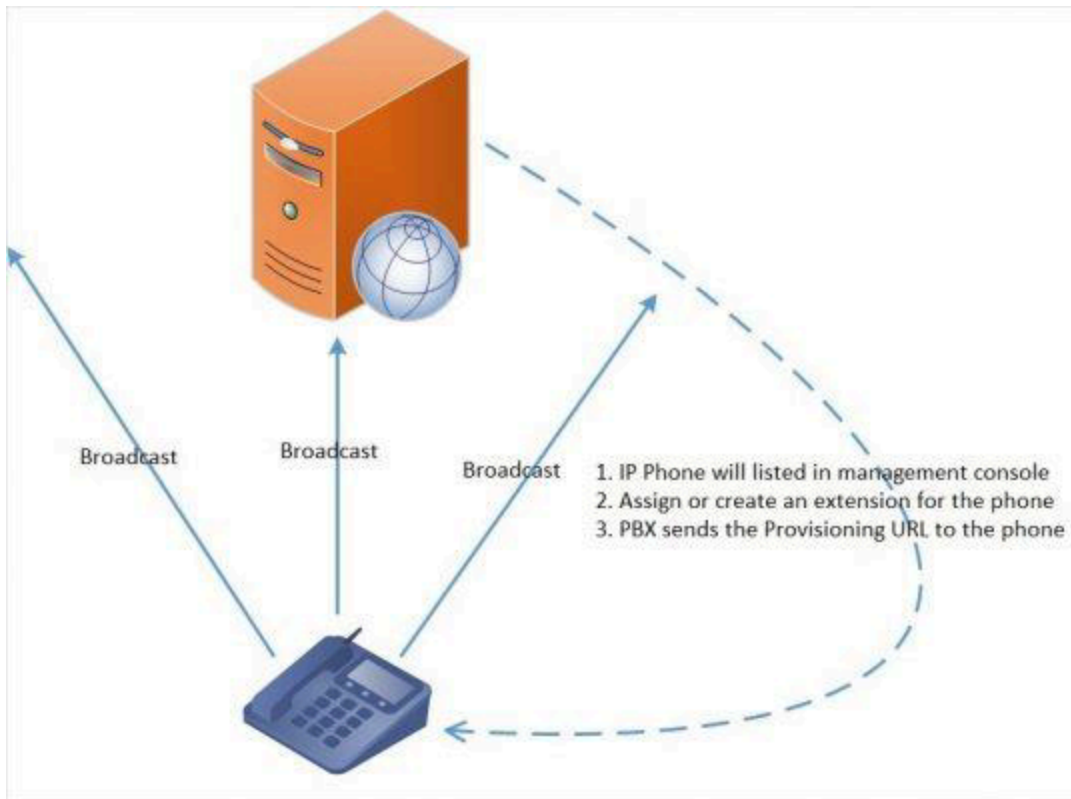
Phone provisioning greatly eases day to day management of IP phones. It makes it easy to change extension passwords, BLF lights and so on because you can do it centrally for all phones from the PortSIP PBX Web Portal and then push the changes to the phone. The following provisioning methods are supported:

- Plug and Play - Supported IP phones can be provisioned automatically using plug and play (Applicable for phones on the local LAN)
- Via RPS - For the Yealink, Fanvil, Htek IP Phones, they can be provisioned by the RPS
- Via Manual Provisioning URL - Supported IP phones can be provisioned by entering the provisioning URL into the phone's web interface (Applicable for local, remote and SBC extensions)

- Via DHCP Option 66 - Legacy phones (from a previous PBX installation, e.g. Polycom, Cisco or Aastra) can be provisioned via DHCP for use in the local LAN only. Some limitations apply

You can find a list of supported and legacy phones here. Additional half an hour to provision the phones saves more hours from future efforts!

## Provisioning phones by using Plug and Play (for local LAN)



**Note:** PnP provisioning requires that the PortSIP PBX runs on the default sip port 5060 and that the IP phones reside on the same local LAN subnet as PortSIP PBX.

To auto provision phones using Plug and Play:

1. Plug the phone into the network
2. The phone will send a multicast message across the LAN, this will be picked up by PortSIP PBX
3. The phone will show up in the “**Call Manager > Phones**” menu in the PortSIP PBX Web Portal as a new phone
4. Assign the phone to an existing extension or create a new one for the phone
5. Go to the extension’s “**Phone Provisioning**” tab and specify other configuration

settings for the phone

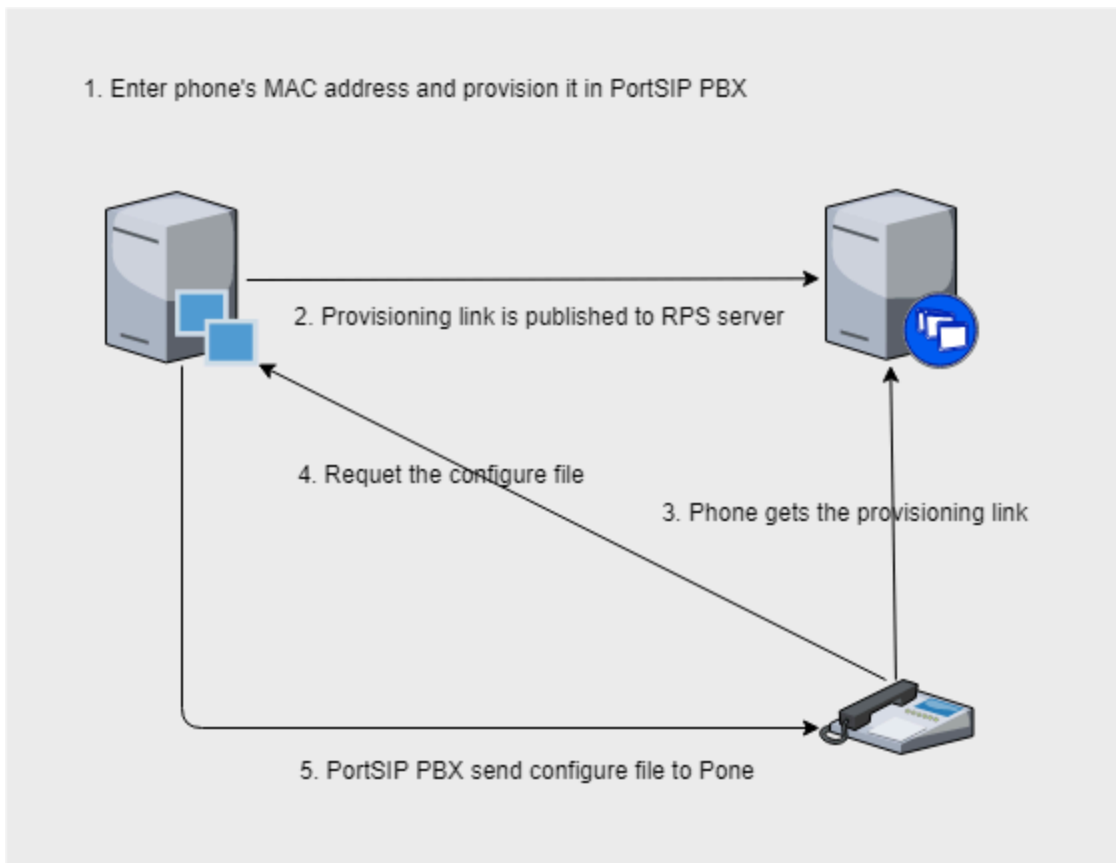
6. Enter the password for access IP Phone web UI
7. Select “**Phone Display Language**” and “**Timezone**” for the phone
8. Click “**OK**”
9. The PBX send the configuration file URL to IP Phone, IP phone will download the configuration file
10. The phone will apply the settings and connect to PortSIP PBX. The IP phone will be manageable from within the PortSIP PBX Web Portal

## Provisioning Phones using provisioning link manually

Remote phones that are not in same LAN with PortSIP PBX, it must be configured manually by the provisioning link. To provision a remote phone:

1. From the “**Call Manager > Phones**” menu in the PortSIP PBX Web Portal, select “**Add Phone**”.
2. Select the extension that the phone uses.
3. Enter the MAC address of the phone (which can be found at the bottom of the phone).
4. Select the appropriate phone model from the drop down menu.
5. Select “**Phone Display Language**” and “**Timezone**” for the phone.
6. Enter the password for access IP Phone web UI
7. Click “**Apply**” button and then edit this extension.
8. Copy the provisioning link.
9. Insert the provisioning link manually into the phones. You can find it in “**Phone Provisioning**” tab of extension configuration.

## Provisioning remote Phones by RPS

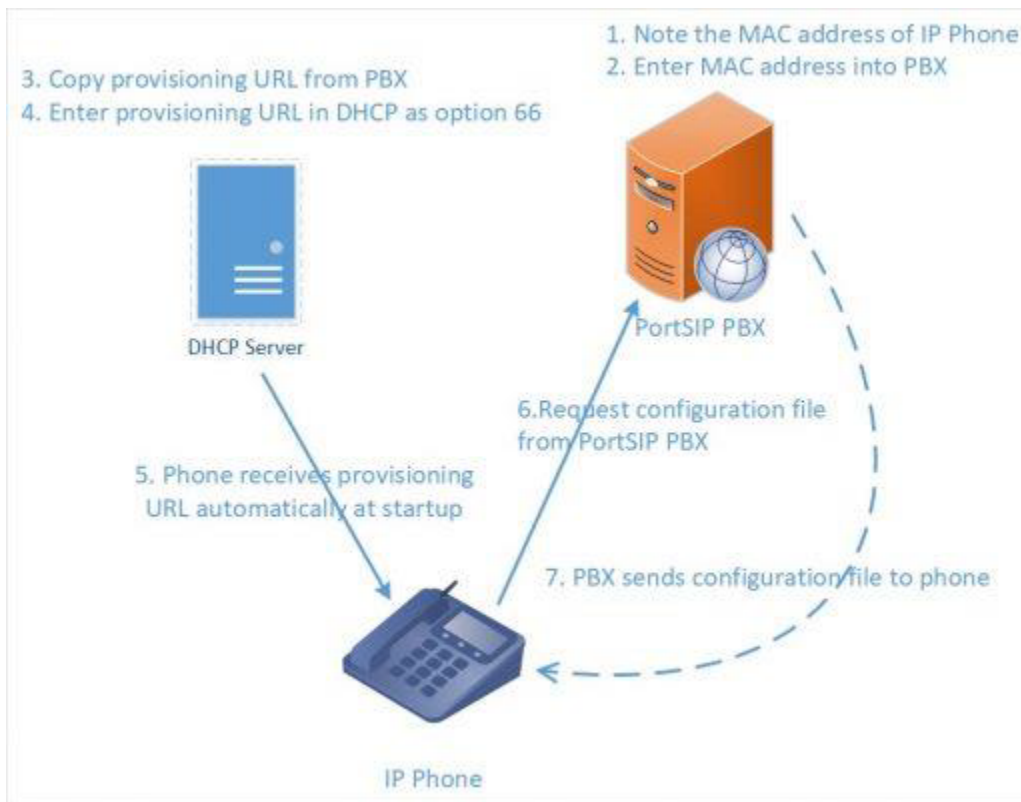


In the case PortSIP PBX locates in cloud, IP Phones can be auto provisioned via RPS (RPS is a service provided by IP Phone vendors). PortSIP PBX supports for Yealink, Htek, and Fanvil RPS. If you are using the IP Phone from one of the providers above, you may configure your IP Phone in a very easy way, without the need to manually copy the auto provisioning link (in this scenario the PnP mode is unavailable).

1. From the **"Call Manager > Phones"** menu in the PortSIP PBX Web Portal, select **"Add Phone"**.
2. Select the extension that the phone uses.
3. Enter the MAC address of the phone (which can be found at the bottom of the phone).
4. Select the appropriate phone model from the drop down menu.
5. Select **"Phone Display Language"** and **"Timezone"** for the phone.
6. Enter the password for access IP Phone web UI
7. Click **"Apply"** button, the PortSIP PBX will writes the provisioning link to the IP Phone's RPS. Once the IP Phone is started, it will query the provisioning link with

its MAC address to complete the auto provisioning.

## Provisioning Legacy phones: Cisco, Polycom & Aastra



Cisco, Polycom and Aastra phones do not support plug and play nor secure HTTPS provisioning with a Let's encrypt Root CA or self-signed CA. They can only be used on the local LAN and must be provisioned as follows:

1. Download the firmware that has been tested by PortSIP with the legacy phones.
2. Factory reset your phones to ensure that there are no old settings that might conflict with the new configuration. Find out how here for Aastra, Cisco, Cisco SPA and Polycom SoundPoint / SoundStation.
3. Now add the phone to an extension. You can do this from the phones page or you can go straight to the extension, provisioning tab. Click **"Add Phone"**.
4. Select your phone model
5. Enter the MAC address of the phone. You will be taken to the provisioning page
6. Select **"Phone Display Language"** and **"Timezone"** for the phone
7. Enter the password for access IP Phone web UI
8. Click **"Apply"** to add the phone to the extension
9. IMPORTANT: Please take note of the provisioning link shown on **"Auto**

**Provisioning**” tab.

Now configure the phone to retrieve the configuration from the PortSIP provisioning folder. Use DHCP option 66 or configure the phones manually via their web interface with the PortSIP provisioning link. Cisco 7940/7960 phones must be provisioned using TFTP and DHCP option 66.

## **Detailed Step by Step guides for legacy phones:**

[Provisioning Polycom IP Phones](#)

[Provisioning Cisco 7940/ 7941/ 7960 /7961 phones](#)

[Provisioning Cisco SPA 302, 303,501G, 502G, 504G, 508G, 509G, 525G/G2](#)

[Provisioning Aastra 6730i, 6731i, 6739i, 6751i, 6753i, 6755i, 6757i](#)

## **See Also**

Remote phones? Read our guide on [Provisioning a Remote Extension](#).

Using [Provisioning IP Phone via DHCP 66](#) to configure the provisioning URL for legacy phones.

See the list of [Supported IP Phones](#) by PortSIP PBX.

[Setting up a TFTP server](#) for firmware updates.

[Factory resetting](#) Aastra, Cisco, Cisco SPA, Gigaset, Panasonic, Polycom SoundPoint, Polycom Soundstation, Yealink.

[PnP auto provision IP Phone Multicast Debug](#)

## **5.3 Managing Phones**

PortSIP PBX provides an easy way to monitor and manage your phones and softphones throughout your network. The “**Call manager > Phones**” menu in the PortSIP PBX Web Portal allows you to:

- View all the phones in the network, including IP and MAC.
- View all PortSIP Clients connected in softphone mode.



- Check the firmware version that the phone is running.
- Remotely reboot one or all of the phones.
- Re-provision the phones.
- Launch the admin interface of the phone.
- Monitor security of extension password and PIN. Weak extension passwords and PINs are the most common cause of security breaches.

## Adding Phones

You can add phones to PortSIP PBX in the following ways:

- Plug and Play - Plug in the phone in the local LAN
- By MAC - for legacy phones
- By RPS - for remote phones

### Plug and Play (LAN & SBC)

If you are connecting a supported phone that is on the same LAN as PortSIP PBX, you will see the phone appear on the phones page, with its entry in BOLD. This means PortSIP PBX has detected a new phone on the network that you need to process.

Select the phone and decide to:

1. Assign the phone to an existing extension. Click “**Assign Ext**” You will be prompted for the extension number.
2. Create a new extension for the phone. Click the “**Add Ext**” button. You will be taken to the create extension page and prompted for Extension name and number. Click “**OK**” to create the extension.
3. Reject the phone. If the phone does not look familiar to you, or it has not been authorized for use with PortSIP PBX, you can “**Reject**” to delete the provisioning request.

### By MAC - for legacy phones

You can add new legacy phones that do not support plug and play, as follows:

1. Click “**Add Phone**” from the “**Phones**” tab.
2. Select extension this phone uses.
3. Now select the phone model.

4. Enter the MAC address of the device and click “**OK**”.
5. You will be taken to the provisioning page of that extension.
6. You can optionally configure other settings for the phone.
7. When done, click “**Save**” to add the phone to the extension.
8. Configure the DHCP server to serve the configuration URL, or configure it from the phone web interface.

## Provision Remote extensions by RPS

If you are adding phones that are installed remotely, i.e. PBX in cloud, you must:

1. Click “**Add Phone**” button from the “**Phones**” tab.
2. Select extension this phone uses.
3. Select the phone model.
4. Enter the MAC address of the device and click “**OK**”.
5. You can optionally configure other settings for the phone.
6. When done, click “**OK**” to add the phone to the extension.
7. Now the PortSIP PBX will write the provision link to the IP Phone RPS. Once the IP phone starts, it will obtain the link from the RPS to download the profile from PortSIP PBX. **Note: currently PortSIP PBX only support the PRS for Yealink, Fanvil, Htek.** If your IP Phone is not provided by one of them, please follow the step 8.
8. Copy the provisioning link and insert to your IP phone manually.

## Accessing the Phone UI

PortSIP PBX allows you to easily access the password protected web interface of your configured phones. PortSIP PBX will provision them with a username and unique password and manage the credentials for you. To access the Phone UI:

- Select the phone and click on “**Phone UI**”.
- For most phones, you will be taken straight to the phone UI page.
- For some older phones you might be asked to enter the password for the phone. In this case, click the “**Password**” button, for the password to be shown, and copy paste the password configured for the phone in the phone authentication page.

## Changing Phone Settings

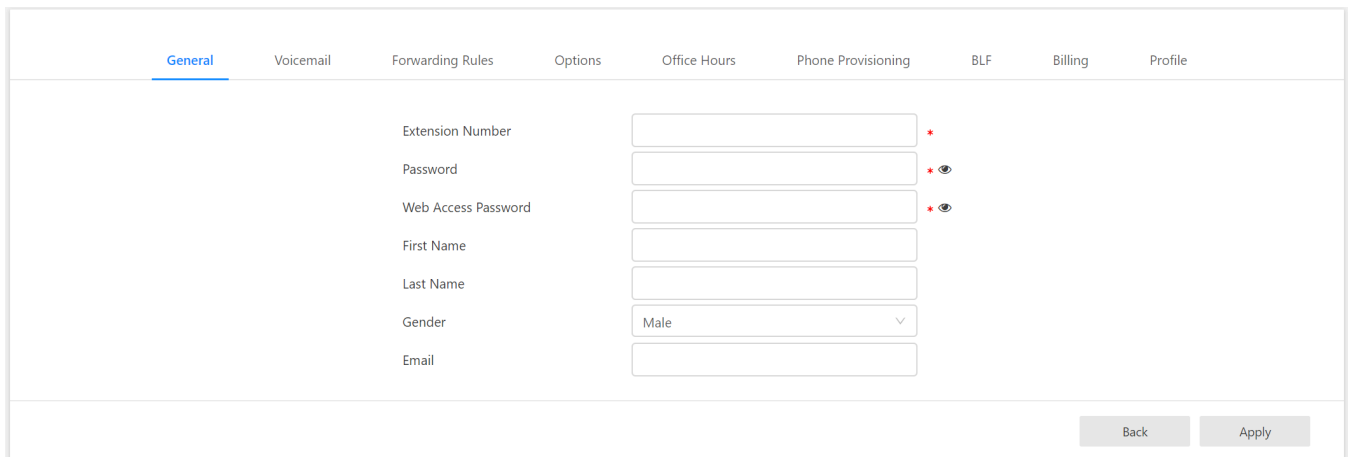
Changes made to the phone configuration from the “**General**” tab of the “**Extensions**” section or within the “**Phone Provisioning**” tab of the “**Settings**” section for certain extension, will take effect within 24 hours. You can re-provision the phones to force them to pick up the new configuration immediately. If you need to re-provision the phones, for example after you have made configuration changes:

1. Select the phones that you wish to re-provision.
2. Click “**Reprovision**”.
3. If the phone needs a reboot, it will be done automatically.

## 5.4 Extension Management

This section explains how to create and configure extensions in PortSIP PBX. There are multiple methods to create an extension.

- When provisioning a new phone, you could choose to create a new extension.
- Extensions can be manually created from the “**Extensions**”.
- Extensions can be imported from a .csv file.
- Create the extension by calling REST API.



The screenshot displays the 'General' configuration page for an extension in the PortSIP PBX web portal. The page features a navigation bar with tabs: General (selected), Voicemail, Forwarding Rules, Options, Office Hours, Phone Provisioning, BLF, Billing, and Profile. The main content area contains a form with the following fields:

Extension Number	<input type="text"/>	*
Password	<input type="password"/>	*
Web Access Password	<input type="password"/>	*
First Name	<input type="text"/>	
Last Name	<input type="text"/>	
Gender	<input type="text" value="Male"/>	▼
Email	<input type="text"/>	

At the bottom right of the form, there are two buttons: 'Back' and 'Apply'.

To configure an extension, click on “**Call Manager > Extensions**” in the PortSIP PBX Web Portal. Click on “**Add**” to create a new one, or select an existing extension and click the **Edit** button to configure or manage the existing extension users. “**Web Access Password**” is used by extension users to log into Web Portal.

## General

In the section of “**General**”, you can enter the extension number, password, first name, last name and the email address of the user. The extension number can be numerals or letters; the extension number and password are required. A welcome email with information on the extension created, as well as voicemail and missed call notifications (configurable) will be sent to the specified email address.

The field “**Web Access Password**” is used for the extension to sign in Web Portal.

If the SMTP server is configured, once an extension is successfully created and the its email is set, PortSIP PBX will send an email to the extension's email which includes the extension information and PBX parameters such as PBX SIP Domain, PBX IP, and the QR code. User can use the PortSIP UC App to scan the QR code to login to PBX without enter the details.

There is a QR code for this extension, you can use PortSIP App to scan the QR code to sign in the PBX rather than entering the information manually.

In the “**Direct Inbound Dialing (DID)**” section, you can select a DID for the extension instead of creating an inbound rule separately.

“**Exceptions**” - create exceptions by entering the “**Caller ID**”, selecting the time frame in “**Received During**” and chose the action in “**Action**” to bypass the extension forward rules.

**Note:** The email that you entered should be unique, duplicated email is not allowed since PortSIP PBX v12, user can use extension's email to sign in the PortSIP PBX Web Portal.

## Voicemail

The “**Voicemail**” tab allows you to configure the extension’s voice mail preferences (including the voicemail PIN number for authentication), enable/disable PIN Authentication, play Caller ID, and enable PortSIP PBX to read out the Caller ID and the Date/Time on which the message was received.

After the extensions created successfully, the “**Greetings for Voice Mail**” section allows you to configure your voicemail greetings.

Click the “**Browse**” button to upload the new greeting file, and click the “**Lock**” icon to specify it as greeting file.

## Forwarding Rules

Each extension can have a set of call forwarding rules that define what PortSIP PBX should do when the extension user is unable to answer an incoming call. This can be configured on the basis of following:

- The user's status
- The time

Each status requires a call-forwarding rule. For example, if the user is unable to take a call whilst their status is "**Available**", you can forward the call to voicemail (The voicemail must be enabled in the "**voicemail**" tab) or to the mobile phone number.

**Note: forwarding the call to certain mobile number requires the VoIP provider and outbound rule configured.**

## Options

The "**Options**" tab allows you to configure options, restrictions and access for the extension:

- Outbound Caller ID – Outbound Caller ID could be entered here for extension, so that when the extension starts external calling via certain provider/SIP trunks, an outbound caller ID could be a replacement for certain SIP field. For more details, please refer to Section [5.6](#Configuring VoIP Provider / SIP Trunk).
- Caller ID for External Emergency Call – It could be entered here for extension, so that when the extension starts emergency external calling via certain provider/SIP trunks, this ID could be used as a replacement of certain SIP field. For more details, please refer to Section [5.6](#Configuring VoIP Provider / SIP Trunk).
- Record audio calls – If checked, all calls for this extension will be recorded as wav file.
- Record video calls – If checked, all video calls for this extension will be recorded as AVI file.
- Enabled – If un-checked, the extension will be disabled.
- Allow Paging/Intercom – If checked, the extension will be allowed to make Paging/Intercom calls. This options can't be changed since it is inherited from the "**Extension Groups**".
- Allow External Calls – If checked, the extension will be allowed to make call to external number via configured VoIP Provider/SIP Trunk. This options can't be

changed since it is inherited from the "**Extension Groups**".

- Allow Web Portal Access – If checked, the extension will have the access to PBX Web Portal. This options can't be changed since it is inherited from the "**Extension Groups**".
- Belonged groups - It indicates the extension groups that this extension belongs with.

## Office Hours

The Office Hours Scheduling feature allows a user's status to be changed on the base of global office hours or specific office hours.

Select if the extension would follow the Global Office Hours, or use Specific Office Hours. To specify Specific Office Hours, enable the option and choose the time for a week, and click left or right arrow to apply in use.

## Phone Provisioning

The "**Phone Provisioning**" tab allows you to add or edit settings of phones linked to this extension. The management of IP phone settings is discussed in "**Phone Provisioning**".

## BLF

You can configure the BLF lights on an IP Phone in this tab.

Match a BLF button with an extension, so that this button will show the status of that extension. The number of available BLF buttons varies per phone.

The following options are available for BLFs:

- BLF – shows presence of another extension.
- Speed Dial – link to a phone number for easy calling
- Custom Speed Dial
- Change status

## Billing

The admin/tenant can set the balance for extension. When billing is enabled and the balance is not enough (see section [5.13](#5.13 Billing)), the call will fails.

## Profile

You can configure the extensions profile here. The company name and company website cannot be modified. These fields are inherited from administrator's profile when the administrator creates extensions.

## 5.5 Extension Groups

Extensions and administrators could be managed under "**Extension Group**" of Call Manager.

Extension groups are used to determine what and to whom the information is shown. The defaulted extension group "**DEFAULT**" cannot be deleted or modified.

Note: that an extension has to be a part of at least one group. When a new extension is created, it will be grouped into "**DEFAULT**" by automatically.

Users can be assigned permission to view details about other members in their group, and managers can be assigned elevated rights over users in their group. Rights are assigned on the basis of Group membership, which means that a manager will be able to see call details of any member of their group, regardless of the call destination or origin.

### Creating Extension Groups

On the left menu of Web Portal, select "**Call Manager > Extension Groups**", and click **Add** button. Fill in the Group Name and Group Description in Group Information, and choose the Group Member Rights to be set.

By clicking "**Group Members**" tab, you could add existing extension users into the group. Once finished, click the **Apply** button to complete the creation of group.

Once an extension group is granted the permission "**Allow Access to Web Portal**", all extensions in this group could sign in PortSIP PBX Web Portal. Assume the "**web access password**" for extension 101 is 111111, the SIP domain set in PBX system is [portsip.io](http://portsip.io), and the extension 101 belongs to default group which has been granted with login permission to the system Web Portal, extension 101 could login with below info:

- Choose "**Sign in with Extension Number**"
- Extension number: 101
- Extension web password: the web password of extension 101, in this case it is

111111

- SIP Domain: [portsip.io](https://portsip.io)

An extension may be assigned to various group simultaneously, and owns a collection of the permission for these groups.

## Monitor

The extension group contains a "**Monitor**" tab, which is used for setting the monitor permissions for the extensions. In this tab, you can choose multiple extensions to assign them the "**Monitor**" permissions. The monitor members can silence monitor other extensions' calls, whisper, barge-in, and barge-break the extensions calls. It is commonly used for CTI purpose. For more details please see [CTI](#11.3 CTI) section.

## 5.6 Providers / Trunks

VoIP providers/trunks "**host**" phone lines and replace the traditional telco lines. VoIP providers/trunks can assign local numbers in one or more cities or countries and route these to your. In most cases they also support number porting.

VoIP providers/Trunks are able to offer better call rates because they may have an international network or have negotiated better rates. Therefore, using VoIP providers can reduce call costs.

We recommend to use supported VoIP providers as all of our supported VoIP providers have been tested for interoperability with PortSIP PBX, and are retested with each new build. The configuration wizard allows you to quickly and easily add them.

PortSIP PBX supports two types of VoIP providers:

- Registration Based – These VoIP providers require the PBX to register with the provider by using an authentication ID and password. Most of the VoIP providers are predefined in PortSIP
- IP Based - IP Based VoIP Providers / SIP Trunks do not generally require the PBX to register with the provider. The IP address of the PBX needs to be configured with the provider, so that it knows where calls to your number should be routed

Only the admin can add/edit/update the provider/trunk. Once the admin adds a provider/trunk,



and the admin can specify the it available to one or more tenants.

The tenants can only see the trunks/providers which assigned to him by admin, and create the inbound/outbound rule on its base.

## **Configuring VoIP Provider / SIP Trunk**

First, you need to have an account with a VoIP service provider. PortSIP PBX supports most of the popular SIP-based VoIP service providers/SIP Trunk, and we recommend to use one that has been tested and approved by PortSIP as PortSIP PBX includes pre-configured templates for these VoIP providers.

### Choose a VoIP Provider/SIP Trunk

Provider Name	<input type="text"/>	*
Country	Generic <span>▼</span>	
Provider brand	Generic <span>▼</span>	
Website	<input type="text"/>	
Host	<input type="text"/>	*
Port	5060	
Outbound proxy server	<input type="text"/>	
Outbound proxy server port	0	
Transport	UDP <span>▼</span>	
Reregister every (Seconds)	600	
Authentication Mode	Register based <span>▼</span>	
<input type="checkbox"/> Provider is located in same LAN with PBX		
<input checked="" type="checkbox"/> This provider is only accept single Via SIP header		
Username	<input type="text"/>	
Authorization Name	<input type="text"/>	*
Password	<input type="text"/>	*
Associated IPs of Provider	<input type="text"/>	

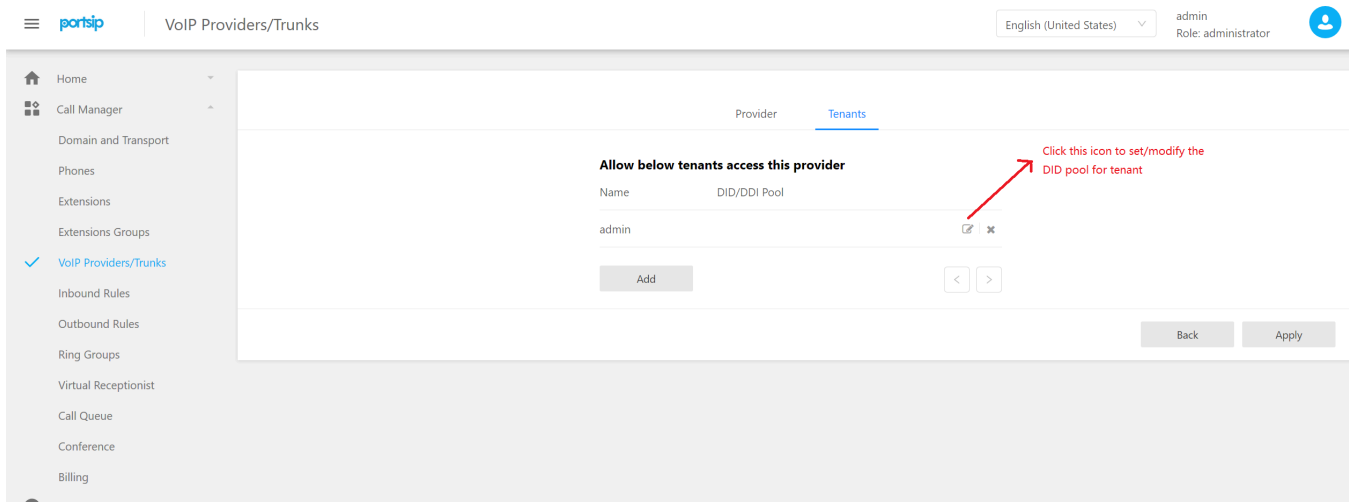
After you have created the VoIP provider account, you will need to configure the account in PortSIP PBX. To do this:

1. Select "**Call Manager > VoIP Providers/Trunks > Add**". Enter a friendly name for this VoIP provider
2. Select the Country for the VoIP provider. If the country that the providers locates is not listed, please choose "**Generic**"
3. Select your VoIP provider from the Provider drop-down list. If your provider is not listed, select "**Generic**".

4. The hostname of SIP server or IP may be prefilled. Compare these information with the details that you have received from your VoIP provider and check if they are correct. Depending on the VoIP provider that you are using, some fields will be disabled, which means you do not need to change them  
**Note:** For generic providers, you need to fill in relevant parameters for server by yourself. Please consult your provide for more details
5. Transport. The transport which used for the PBX communicates with your provider / trunk, you should consult your provider and choose appropriate transport, currently support UDP and TCP. The transport must added in PBX before add the provider / trunk. For example, if your provider requires the TCP, you should add the TCP transport in PBX, please refer to section [5.1](#5.1 Domain and Transport)
6. If your provider is verified on IP address and does not require registration, please choose "**IP Based**" for "**Authentication Mode**"
7. If you have customized a provider such as the E1 gateway and it is located in the same LAN with PBX, or other PBX/SIP servers, please check "**Provider is located in same LAN with PBX**"
8. This provider only accepts single via SIP header. Usually the providers/trunks only accept single via SIP header. It is selected by default
9. Enter the VoIP provider account details. Enter the Authentication ID/username and password of your VoIP provider account. If your provider/trunk is IP based, no need to enter them.
10. Associated IPs of Provider. For some providers/trunks, it maybe sends the INVITE message to PBX from multiple IPs rather than from the host only. You need to enter each IP here and click the "**Add**" button to add them
11. Click the "**Tenants**" tab, choose one or more tenants to allow them access this trunk/provider.
12. Once a tenant is assigned with the trunk/provider, admin can also set the DID pool for this tenant. When tenant creates the inbound rule based on this assigned trunk/provider, he can only use the DID number from the DID pool.
13. Admin can leave the DID pool empty for a tenant, so that the tenant cannot create the inbound rule based on this trunk/provider, but no matter to create the outbound rule based on this trunk/provider.
14. The DID Pool format: allows to set the wildcard \*. If a tenant is assigned with the trunk/provider, and the DID pool is set as "\*". When we assign this trunk/provider to other tenants, we cannot set any DID pool for them (the DID pool can be left as

empty) since the "\*" is already assigned to the first tenant.

15. The DID pool allows to set a numerical prefix and wildcard \*. For example, setting the DID pool as 44\*\*\*\*\* means all numbers started with 44 and a total length of 8. Once the inbound rule is created, any number started with 44 and a total length of 8 can be set as DID number for this rule.
16. The DID pool allows to set a number range like 12000-18000, or 22000-22800. Setting the number range requires the start number and end number use a same prefix: 12000-22000 is not allowed. The numbers must has same amount of digits: 12000-180000 is not allowed. The start number must be less than end number: 18000-12000 is not allowed.
17. DID pool allows to set a semicolon-separated list of multiple ranges, for example: 123;1100-1200;44\*\*\*\*\*



The PortSIP PBX will display all added providers/trunks status by clicking **"Call Manager > VoIP Providers/Trunks"** menu.

## Configure E1/T1 Gateway register to PortSIP PBX

Consider we deployed the PortSIP PBX on a cloud platform such as AWS, AZURE, GCE, and wish to configure the E1/T1 gateway which located in local LAN as a trunk for the PortSIP PBX, but the E1/T1 without static public IP, we can't configure the **Authentication mode** to **"IP Based"** and **"Register Based"**.

For this scenario, we can configure that E1/T1 is registering to the cloud PortSIP PBX from local LAN, then the E1/T1 can act as the VoIP Provider / SIP Trunk works with PortSIP PBX for make & receive calls.

Please follow the below steps to config the E1/T1 register to the cloud PortSIP PBX.

1. Select "**Call Manager > VoIP Providers/Trunks > Add**". Enter a friendly name for this VoIP provider.
2. Choose "**Generic**" for both provider country and provider brand.
3. Enter a domain for the "**Host**" filed, this domain doesn't require to exist, you can enter any domain here, for example, [portspitrunk1.io](http://portspitrunk1.io).  
**Important:** ensure this domain does not equal to any tenant's SIP domain.
4. Please choose "**Accept Register**" for "**Authentication Mode**".
5. For the "**Authorization Name**" , you can enter any number here, for example **123456**, the E1/T1 gateway will use this for the authorization when it registers to PortSIP PBX.
6. For the password, you can enter any password here, the E1/T1 gateway will use this for the authorization when it registers to PortSIP PBX.
7. Other settings are the same as the previous section for confining the "**IP based**" and "**Register based**" VoIP provider/Trunk.
8. After applied the settings, now you can configure the E1/T1 gateway to let it register to the cloud PortSIP PBX. In the E1/T1 settings, set up the step3 "**Host**" as "**SIP Domain/SIP Server**", for example [portsiptrunk1.io](http://portsiptrunk1.io), set up the cloud PBX public static IP as "**Outbound Proxy Server**", set up the PortSIP PBX transport port as the "**Outbound Proxy Server port**", set up the step 5, 6 **Authorization name** and **Password** as the **username** and **password**, then the E1/T1 gateway can register to cloud PortSIP PBX.
9. You can sign in to the PortSIP PBX Web Portal to create the inbound & outbound rule base on this E1/T1 gateway trunk.

## Outbound parameters and Inbound parameters

After completing the setup for providers, you could also go to "**Call Manager > VoIP Providers/SIP Trunks**" and click "... " button to choose "**Edit**" the Inbound/Outbound Parameters for providers:

- In "**Outbound Parameters**" tab, you could set some rules to make changes for headers of INVITE messages to be sent to VoIP providers/SIP trunks. For example, "**user**" of "**to**" SIP header could be set to "**Outbound Caller ID**" of the extension who starts the call. You can setup the "**Outbound caller ID**" of extension in the "**Options**" tab of extension, see section [5.4](#).

- In “**Inbound Parameters**” tab, user could set rules to make changes to field values of SIP messages for incoming calls.

**NOTE:** Both inbound and outbound parameters are advanced options. It's recommended to use default values.

## 5.7 Configuring Inbound/Outbound Rules

Outbound and inbound rules determines how PortSIP PBX routes calls on the base of certain criteria. You can configure rules to control through which provider/Trunk a call will be placed, for example, to route the calls through your VoIP provider on the basis of least cost routing.

You can also set DID (Direct Inward Dialing) numbers to allow to bypass the receptionist or IVR and place calls directly to a user's extension.

### Creating Inbound Rules

Many companies provide users and/or departments with “**Direct or DID numbers**”, which allow their contacts to bypass the receptionist and make calls directly. DID numbers is also referred to as DDI numbers in the United Kingdom and MSN numbers in Germany.

Even if you make use of a virtual receptionist, a direct line/number is often preferable because it's more convenient for the caller.

Direct dial numbers are easily implemented by using “**Inbound Rules**”. DID numbers is provided by your VoIP provider or Phone Company and are virtual numbers assigned to your physical lines. Usually you are assigned a range of numbers. Please ask your Phone Company or VoIP provider for more information about DID numbers.

You have to configure one VoIP provider/SIP Trunk before adding the inbound rules.

To add Inbound Rule:

- From the PortSIP PBX Web Portal, select “**Call Manager > Inbound Rules > Add**”
- Enter a friendly name for the rule
- **CID number mask:** you can enter the CID number mask here, which the PBX will use to identify the caller. You can add the number in it's entirety, identifying a single caller, or use the \* as a wildcard. For example 0044\*\*\*\*\* will identify a

UK Caller and 004420\*\*\*\*\* will identify a caller from London. Note: the \* digits must match number actually digits. If the number is 3 digits, then should use \*\*\*

The CID number mask also allow set a number range, for example:

00442012345670-00442012345680.

The CID number mask can be empty.

- In the "**DID/DDI number/mask**" field, enter the DID number as it will appear in the SIP "**to**" header (The number your provider has been applied as your main, or first, DID number). PortSIP PBX will match the number inserted into this field with the "**to**" header, you can use a single \* to match any DID number, or use a single number likes 00442012345678;

The number range is disallow, and **prefix and \*** is disallow - for example: 004420\*

- Select which provider/SIP Trunk you wish to be associated with this DID and inbound rule, only allow assign one provider with an inbound rule.
- Specify how you wish to forward incoming calls according to this inbound rule:
  - *End Call*
  - *Connect to Extension*
  - *Connect to Ring Group*
  - *Connect to Virtual Receptionist*
  - *Connect to Voice Mail of an extension*
  - *Connect to Call Queue*
  - *Forward call to external number*
- You can specify that an incoming call should be forwarded differently if it is received outside office hours

**Note:** you can create multiple inbound rules based on a same DID number, but all these inbound rules should set the CID number mask, and the CID number mask must not be conflicted.

**Example:** You have a DID number 442012345670. Now create two inbound rules: the CID for the first rule is set to 0044\*\*\*\*\*, the DID number mask set to 00442012345670, and the call is set to route to the call queue 8000; the CID for the second rule is set to 0033\*\*\*\*\*, the DID number mask set to 00442012345670, and the call is set to route to the call queue 9000.

Now let all English-speaking employees to be agent of call queue 8000, let all French-speaking employees to be agent of call queue 9000. When the caller calls to 00442012345670, callers

from UK will be routed to the call queue 8000 to talk with English agent, and callers from France will be routed to the call queue 9000 to talk with French agent.

## Office hours for Inbound Rules

In the "**Office Hours**" tab, you can set the office hours for the inbound rule so that the incoming calls will be routed to different destinations on the basis of the current hour.

If "**Use default Global Office Hours**" is selected, the PBX will use the office hours specified by admin/tenant;

If "**Use specific Office Hours**" is selected, customized office hours rules apply instead.

## Exporting and Importing Inbound Rules

If you need to export your Inbound Rules to a .CSV file either for backup or to make any updates, follow these steps:

1. Sign in the PortSIP PBX Web Portal
2. Click on the "**Call Manager > Inbound Rules**"
3. Click on the "**Export**" button to start exporting your inbound rules
4. Select a location and a file name for your exported inbound rule file and click "**Save**". Your rules will be exported and saved in the .CSV file

To create multiple inbound rules, insert necessary fields on a CSV file by using correct format, and then import them back into PortSIP PBX by using the import function.

To import your inbound rules into PortSIP PBX from a CSV file:

1. Sign in the PortSIP PBX Web Portal.
2. Click on the "**Call Manager > Inbound Rules**", click the "**Import**"
3. Browse to the file that you want to import, select it and click "**Open**"
4. The rules will be imported into PortSIP PBX

## Creating Outbound Rules

An outbound rule decides through which VoIP provider/Trunk an outbound call would be placed.

The rule is decided by the user/extension who is making the call, the number that is being dialed or the length of the number, or the extension group to which the caller belong.



To add outbound rules:

- From the PortSIP PBX Web Portal menu, navigate to "**Call Manager > Outbound Rules**" and click "**Add**" button. Enter a name for the new rule in the prompted box.
- Specify the criteria that should be matched for this outbound rule to be triggered with. In the "**Apply this rule to below calls**" section, specify any of the following options:
  - **Calls to numbers started with prefix** – Apply this rule to all calls started with the number you specify. For example, enter "**00**" to specify that all calls with numbers started with 00 should trigger this rule. Callers should dial "**00123456**" to trigger this rule. You can specify more than one prefixes, separated by ";". For example, "**00;123;88**" specifies prefixes 00 and 123 and 88. If the called number matches one of these prefixes, this rule will be triggered.
  - **Calls from extension(s)** – Select this option to define a particular extension or extension range for which this rule applies. Specify one or more extensions separated by semicolons, or specify a range by using a "-". For example 100-120.
  - **Calls to number with certain digits** – Select this option to apply the rule to numbers with a particular digit length, for example 8 digits. By this method, you can capture calls to local area numbers or national numbers without requiring a prefix.
  - **Calls from extension group(s)** – Rather than specifying individual extensions, you can select an extension group.
- Now specify how to match outbound calls with the criteria. In the "**Make outbound calls on**" section, select up to three routes for the call. Each defined provider/trunk will be listed as a possible route. If the first route is not available or busy, PortSIP PBX will automatically try the second route.
- You can transform the number that matches the outbound rule before the call is routed to the selected gateway or provider by using the "**Strip Digits**" and "**Prepend**" fields:
  - **Strip digits** – Allows you to remove one or more digits from the called number. Use this option to remove the prefix before a call is dialed to the gateway or provider if it is not required. For example the extension make call to 002345, if you specify to remove two digits, the prefix "**00**"

will be removed before it is routed

- **Prepend** – Allows you to add one or more digits at the beginning of the number if this is required by the provider or gateway. For example, the extension make call to 002345, we specify 2 in the “**Strip digits**” field and set “**Prepend**” to “**+44**”, the final called number which PBX forward to VoIP provider/SIP Trunk will be +442345

## Office hours for Outbound Rules

In the "**Office Hours**" tab, you can set the office hours for the outbound rule so that the outgoing call will be routed to trunks or not depending on the current hour.

For example, if currently time is out of the specified office hours, the call fails even the outbound rule is successfully matched.

If selected "**Use default Global Office Hours**", the PBX will use the office hours which set by admin/tenant;

If selected "**Use specific Office Hours**" this outbound rule will use the customized office hours.

## 5.8 Configuring Ring Groups / Paging / Intercom

The Ring Group feature adds powerful capabilities to your PortSIP PBX. Ring groups will help you not to miss any important calls, whilst the Paging/Intercom feature allows you to make announcements to groups of people rather like a PA system.

A ring group allows you to direct calls to a group of extensions. For example, you could define a group of three sales, and have the general sales number "**DID**" ring on all three extensions at the same time or one after the other. When you create a ring group, you assign it with a virtual extension number. This will be the number used by the PortSIP PBX to "**Address**" to the ring group.

To add a Ring Group:

- In the PortSIP PBX Web Portal, select "**Call Manager > Ring Groups**" and click the "**Add**" button
- Now enter the ring group fields:

- **Ring Group Number** – This number identifies the ring group from other extensions. Specify a new one as needed. Do not specify an existing extension number
- **Ring Group Name** – Enter a friendly name for the ring group
- **Outbound Caller ID** - Once the outbound caller ID for the ring group is set, when no members answer the call and forward the call to external number on a provider / trunk, this outbound caller ID could be a replacement for certain SIP field. For more details, please refer to Section [5.6](#Outbound parameters and Inbound parameters).
- Ring Time – Specify how long the extension should ring for.
- Ring strategy – Select the appropriate ring strategy for this ring group:
  - **Ring Simultaneously**: All Ring Group members will ring at the same time.
  - **Prioritized Hunt**: Ring each available member of the group by specific order.
  - **Cyclic Hunt**: Ring each available member of the group by the sequence the members are added into the group. The member who has not been rang from a call would take the priority.
  - **Least Worked Hunt**: Ring each available member of the group by the order the members are added into the group. The member who has not answered a call from this group would take the priority.
  - **Paging/Intercom**: This is a Paging or Intercom group (see the next section for more details).
- In the section "**Group Members**", specify the extensions that should be part of this ring group. Simply click on the extensions to add them to the ring group, and click again to remove them from the group.
- In the section "**Destination if no answer**", you can define what should happen if the call is not answered by the ring group

## Paging

When creating the ring group, selecting the "**Ring Strategy**" with "**Paging/intercom**" would allow someone to ring a group of extensions and make an announcement via the phone speaker. The called party will not need to pick up the handset as the audio will be played via

the phones speaker. The person who's paging will not hear any audio back from the people being paged.

## Intercom

When creating the ring group, selecting the "**Ring Strategy**" with "**Paging/intercom**" would allow someone to ring a group of extensions and make an announcement via the phone speaker. The called party will not need to pick up the handset as the audio will be played via the phone speaker. The person paging will not hear any audio back from the people being paged.

If the extension user wants to talk with the caller, he/she should press the "\*" **button to start talking, and stop by pressing "#**" button.

## Important

Before using the Paging or Intercom feature, make sure you have specified the paging/intercom prefix number by:

1. From the PortSIP PBX Web Portal, select "**Advanced > Settings**" menu, click "**Advanced**" tab to add the paging prefix in the "**Dial code**" field (\*11 for example)
2. Make sure that the user who is trying to page/intercom a group has the permission to do so. If a certain extension user would like to start paging/intercom, select "**Call Manager > Extension Groups**", edit the group to which the extension belongs, click "**Group Member Rights**" table, and check the "**Allow Paging/Intercom**" option

There are two ways to commit Paging and Intercom:

1. Assume that you have created a ring group for which the group number 9000, and selected the "**Ring Strategy**" with "**Paging/intercom**". When dialing 9000, all members of ring group 9000 will answer the call automatically and can hear from caller but caller cannot hear back from members. If someone of the members wish to talk with the caller, just press the "\*", and stop talking by press "# key.
2. If extension 100 want to intercom with extension 101, just dial "**\*\*11101**", and extension user 101 will answer the call automatically and talk with caller 100. In this example, **\*11** is the value of "**Dial Code**".

## 5.9 Configuring Virtual Receptionist/Auto-Attendant

The virtual receptionist feature allows PortSIP PBX to answer phone calls automatically. When a call comes into the PortSIP, the caller is presented with a list of options. The caller can choose the appropriate option by using the numbers on their phone keypad. You can implement a menu by using this feature. A virtual receptionist is also known as an **Auto Attendant**.

For example, "**For sales, press 1. For support, press 2 or wait on the line to be transferred to the operator**".

You can configure various virtual receptionists, each of which owns a unique extension number. Depending on your preferences, you may configure to answer calls on the base of which line the call comes in and from, as well on whether the call is received inside or outside office hours. For example, you can have a different prompt for outside office hours that does not include the options to be transferred to groups/queues since there are not agents available to take the calls.

### Recording a Menu Prompt

Before create your virtual receptionist, you must decide the menu options you wish to offer the caller and record the announcement. A sample would be, "**Welcome to XYZ. For sales, press 1. For support, press 2 or stay on the line for an operator**".

**Note:** It is recommended to put the number the user should press after the option, i.e. "**For sales, press 1**", rather than "**press 1 for sales**". This is because the user will wait for the desired option and then "**register**" what number to press.

### Creating a Virtual Receptionist

You can create multiple digital receptionists and link them to a particular line.

To create a virtual receptionist:

- In the Web Portal menu, click "**Call Manager > Virtual Receptionist**", click "**Add** "
- Specify the name and extension number for the digital receptionist.
- By default, PBX uses the system-defined "**Default.WAV**" for prompt. Click on the "**Browse**" button to select a file that you previously recorded for prompt menu. You must save the file in WAV format in PCM, 16kHz/32kHz/48 kHz, 16 bit, Mono

format. (In Windows Sound Recorder you must use the "**Save as**" option to save this format). Besides, user may also choose prompt language for virtual receptionist in "**Virtual Receptionist Language**"

- The prompt when call is transferring - The prompt file which will be played when the call is transferring after caller pressed DTMF.
- Virtual Receptionist Language - The language for the prompt files
- Menu options. Specify actions and the extension number or System extension number for each of numeric keys. Default value is "**No Actions Specified**", referring that no specific actions will be taken in response to the key. If the action is directed to specific extension, ring group, call queue or another virtual receptionist, please also select the target extension number you desired
- User Input: this option allows you to determine when the auto attendant will begin the search for an extension that matches the user's input. The available options are detailed below:
  - When Extension Matches: The auto attendant will wait until the caller's digit sequence matches an existing account. Once the auto attendant finds a match, it will call that extension. This mechanism is useful when accounts of varying name length are used; however, it might be annoying to callers who enter a non-existing number since the auto attendant will never begin the search
  - After 1/2/3/4/5 Digit Input: The auto attendant will wait until the correct number of digits has been entered before it will begin looking for an account that matches. If the account does not exist, the system will play an announcement indicating that the extension does not exist.
  - User Must Hit Pound: The auto attendant will wait until the user hits the # sign before searching for an extension. This mode is useful in variable-length scenarios
- Timeout allows you to specify how long the system should wait for an input. If it receives no input, it will automatically perform this action. This is for callers who do not understand the menu or who do not have a DTMF capable phone. When ready, click "**Apply**" to save the virtual receptionist.
- If extension user enters a DTMF value or key that is not defined in step 4, the action fails. User may define how the call should be handled in such case in "Calling failed" section, and the extension number (if necessary)

## Direct Destinations

The Direct Destinations feature is somewhat like a built-in version of the IVR system.

To direct inbound calls to specified extensions, you can use the pre-configured destination fields and link them to pre-recorded announcements and user input options.

Using the sample shown below, the auto attendant's welcome message will be as follows: **“For Sales, press 1. For Support, press 2. For Accounting, press 3. For all other inquiries, press 0.”** (The user input options are linked to extensions 555, 518, 511, and 570.)

**Virtual Receptionist answers and forwards calls automatically**

[Virtual Receptionist](#)    Action URL

---

**General**

Virtual Receptionist Number:  \*

Name:  \*

Prompt:

The prompt when call is transferring:

Virtual Receptionist Language:  \*

Gap time between DTMF digits (seconds):  \*

**Menu Options**

User Input	Action	Destination extension
<input type="text" value="0"/>	<input type="text" value="End Call"/>	<input type="text" value=""/>
<input type="text" value="2"/>	<input type="text" value="Connect to Extension"/>	<input type="text" value="101"/>
<input type="text" value="3"/>	<input type="text" value="Repeat Prompt"/>	<input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value="No Actions Specified"/>	<input type="text" value=""/>

When configuring straight forward, uncomplicated auto attendants, direct destination is a great solution. However, when configuring auto attendants that require advanced IVR development and functionality, the IVR node is recommended.

Once the direct destination links have been established, the system will call the destination number whenever a caller enters the number that is associated with it. In the sample shown above, when the caller presses 2, the call will be connected to extension 101.

By placing a pound sign after the direct destination (e.g., “2#”), the system will wait 3 seconds before dialing the direct destination. This is useful if you have extension numbers in the 100 range (101, 102, etc.). The 3-second delay ensures that the caller's complete input (e.g., 101) will be processed rather than just the first digit.

- **User Input:** This number can be one or multiple digits; however, the system dials direct destinations immediately after a user has provided keypad input, so overlapping between a direct destination and an extension number can be a problem. For example, extensions starting with “1” would conflict with a direct destination of “1” because the system would be unable to dial the extension number. The best way to avoid this situation is to choose extension numbers that do not overlap with either direct destinations or mailbox and outbound call prefixes. The extension range 4xx through 7xx meets these criteria. Wild cards can also be used in this field.
  - If circumstances render it difficult to change the extension assignments (e.g., business cards with extension numbers already in circulation), a timeout mechanism can be used. By placing a pound sign after the direct destination (e.g., “1#”), the system will wait for 3 seconds before dialing the destination.
  - To redirect fax messages to a specific destination, you can use the direct destination “F”. The CNG tone that announces a fax tone is recognized by the system and is translated into the “F” key.
- **Destination:** This number can be either an internal number (e.g., an extension or conference room) or an external number (must configure appropriate VoIP provider and outbound rules)

## Allowing Callers to Dial a Known Extension Directly

Whilst a digital receptionist prompt is playing, a caller can enter the extension number directly to be connected to an extension immediately. This allows callers who know their party’s extension to avoid going through a receptionist. This option is enabled by default. If you wish to make use of this feature, simply instruct your callers by explaining this in the voice prompt.

For example, *“Welcome to Company XYZ. If you know your party’s extension number, you may enter it now, otherwise, for sales press 1. For support press 2”.*

## Sending HTTP Request to 3rd Server Depending on User’s Input(Web Hook)

When creating virtual receptionist, there are two tabs available for user: **Virtual Receptionist** and **Action URL**. User may setup common Virtual Receptionist in “**Virtual Receptionist**” tab, and define HTTP request and relevant actions in “**Action URL**”.



Action URL is applied as in below scenario:

When users call the Virtual Receptionist and dials the pre-configured DTMF key, Virtual Receptionist will send a HTTP request as defined to the URL of a third-party server, and parse the target extension number in respond message from the third-party server to forward the call to the target extension.

- **Name:** Enter a user-friendly name for the HTTP request. This field is mandatory.
- **Action Type:** Choose the method to trigger Action URL. PortSIP PBX allows to trigger the rule with user inputted DTMF key or caller number. Depending on his request, user may choose “**DTMF**” or “**Caller Number**”. Once “**DTMF**” is chosen, if the DTMF entered is replica to DTMF specified in “**Virtual Receptionist**” tab, system will always invalidate settings in “**Virtual Receptionist**” and handle the call as defined in “**Action URL**”.

- **DTMF match list/ Caller number match list:** Depending on the selection in “**Action Type**”, user may specify the “**DTMF match number**” or “**Caller number match list**”. User may enter a semicolon-separated list of numbers at one time, e.g. “101;102;103”. The entered number must be unique and must not be duplicated.

The match list also can specify to a numbers range, for example: 860000-880000, it's used for below scenario: someone calls to virtual receptionist and enters his bank card number. If the number fall in the matched DTMF range, the virtual receptionist will call the action URL to return some values to indicates the next actions.

Once an item of the Action URL is triggered, an HTTP request will be sent to the third-party server. User may specify the username and password for authentication in “**Credentials for HTTP Basic authentication with 3rd server**” section (not mandatory), and choose the method for sending HTTP request from POST or GET. Fields “**Connection timeout**” and “**Timeout for waiting response**” are filled to setup the timeout value for communication between Virtual Receptionist and third-party server.

- **Action (URL or number):** Action to be executed will be entered here when the preset action is triggered. If HTTP URL is entered here, Virtual Receptionist will send an HTTP request to the third-party server and forward the call depending on the returned value of HTTP request. If a DTMF number is entered here, Virtual

Receptionist will forward the call to the designated number

## HTTP Request Message

PortSIP has defined below parameters to form up the HTTP request message to third-party server in JSON format.

- "from": "var\_caller\_number" - Caller's number, i.e. the caller number who's calling to Virtual Receptionist
- "to": "var\_callee\_number" - Callee's number, i.e. the extension number for Virtual Receptionist
- "input": "var\_input\_dtmf" - DTMF inputted by user
- "from\_name": "var\_caller\_display\_name" - Display name of caller. It will be left empty if no value provided
- "account\_name": "var\_account\_name" - Name of the Virtual Receptionist

Assuming that we had create a Virtual Receptionist with number 888 and named as Sales. And its Action URL is defined as follows:

- Name: Action1
- Action Type: DTMF
- DTMF match list: 22, 33
- HTTP method: GET
- Action (URL or Number): <http://www.appserver.com/dest.php> (If a DTMF number is filled here other than URL, Virtual Receptionist will forward the call to the extension specified other than sending request to third-party server.)

When extension 101 (display name Jason) calls 888, Virtual Receptionist 888 will auto-answer the call and play prompt to the caller. As extension 101 dials 22 or 33, Virtual Receptionist will send below HTTP request in GET method: [http://www.appserver.com/dest.php?from=101&to=888&input=22&from\\_name=Jason&account\\_name=Sales](http://www.appserver.com/dest.php?from=101&to=888&input=22&from_name=Jason&account_name=Sales)

If POST is chosen for HTTP method, Virtual Receptionist will send below HTTP request in JSON format by means of POST:

```
{  
"from" : "101",
```

```
“to” : “888”,  
“input”: “22”,  
  
“from_name” : “Jason”,  
  
“account_name” : “Sales”  
  
}
```

## HTTP Response Message

PortSIP PBX has defined response to HTTP request sent by Virtual Receptionist as follows:

- "status\_code": 200 or other possible status code, of which 200 represents successful request and other refers to failure.
- “action”: Values including “call”, “hangup” and “repeat” indicates the action to be taken by Virtual Receptionist.
  - call – To forward the call to number as defined in “destination”
  - hangup – To hang up the call directly
  - repeat – To repeat the prompt message
- “destination”: The target callee number. It’s valid only if value for “action” is set as “call”; otherwise it will be ignored.

```
{  
  
“status_code” : 200,  
  
“action” : “call”,  
  
“destination” : “222”  
  
}
```

Once Virtual Receptionist has received response as above, it will forward the call to extension 222.

## 5.10 Configuring Call Queue

Call Queue allows calls to be queued whilst agents (members of a call queue) answering calls. Calls do not go unanswered but wait in a queue until an agent is available to take the call.

To add a Call Queue, select menu “**Call Manager > Call Queue**” and click “**Add**”. Now fill in the necessary fields:

- **Queue Number** – Specify the queue number here. It should not be an existing extension number
- **Queue Name** – Enter a friendly name for the Queue
- **Outbound Caller ID** - Once the outbound caller ID for the call queue is set, when no members answer the call and forward the call to external number on a provider / trunk, this outbound caller ID could be a replacement for certain SIP field. For more details, please refer to Section [5.6](#Outbound parameters and Inbound parameters).
- **Ring Duration** – How long the caller would be queued
- **Music on hold** – The music that would be played when the caller is queued
- **Skip member(s) who's calling** - If this option was checked, the queue will don't distribute calls to the agent who is on call
- **Keep waiting if there is no members online** - If this option was checked, even there no any agent online, the queue will still keep the caller in the queue until reached the maximum wait time
- **Set the member ready to accept call automatically** - If this option was checked, once a queue agent(member) is registered to PBX, his status will be set to "**sign in the queue**" automatically, then the queue will distribute calls to that agent, after the agent was ringing or completed a call, the agent status will be set to "**sign in the queue**" automatically.

If this option was unchecked, once the queue agent is registered to PBX, his status will be set to "**sign out the queue**" automatically, the agent must use REST API or dial a code to sign in the queue in order to let queue distribute the calls to him. After the agent was ringing or completed a call, his status will be set to "**sign out the queue**" automatically.

- **Polling strategy** – This option allows you to choose how calls should be distributed to agents:
  - **Ring Simultaneous**: All Ring Group members will be rang at the same time.
  - **Prioritized Hunt**: Ring each available member of the group in configured order
  - **Cyclic Hunt**: Ring each available member of the group by the order the member was added. The member who has not been rang

previously will take the priority

- **Least worked Hunt:** Ring each available member of the group by the order the member was added to the group. The member that hasn't answered a call from this group takes priority

## Configuring Queue Options

- In the “**Destination if no answer**” section, you can define what should happen if the call does not get answered by an agent. If no agent logged into the queue, this option would be triggered immediately
- In the “**Other options**” section, you can specify a custom introduction prompt and a custom music on hold file. You can now choose whether to play the full intro prompt before the system starts to call queue agents
- **Maximum Queue Wait Time.** Once the caller stayed in the call queue longer than this duration, it will be hangup by PBX.
- **SLA time.** SLA refers to service level agreement. Once it's set, you will get a notification every time when a call stays in the queue longer than the specified SLA time.

SLA is used to make sure that your callers are queuing no longer than the time you have specified.

For example you declare that all calls within your organization are answered within 3 minutes, you need to set the SLA in the queue to 180 seconds. Once that time is reached the queue manager will receive an alert notifying that a call has breached the SLA.

## Configuring Queue Agents (members)

By clicking the “**Members**” tab, you can select the agents for the call queue, the queue manager will never receive calls from the queue.

## Notifications

You can set one or more extensions as the queue manager(s) to receive the email notifications if the call exceeds SLA time or is lost.

If an extension is set as queue manager, PBX will not assign the call to him/her, which means the queue manager will not receive the call even he is a member of the call queue.

**Note:** The SMTP server and the email of queue manager must be set up in order to receive the notifications.

## Lost calls

You can query the lost calls of the queue in this tab, for example, if the agents are busy and the caller hang up the call, then the call will be listed here.

## Set agent status to ready or not ready by REST API

When an agent is registered to PBX, by default his status is ready, that mean the he is available to receive calls. If agent away, he can use the REST API to set his status to "**Not ready**" then queue will don't send call to him.

You can find the REST API details here: [https://www.portsip.com/pbx-rest-api/v12.2/call\\_queue.html#member\\_state\\_update](https://www.portsip.com/pbx-rest-api/v12.2/call_queue.html#member_state_update)

The REST API POST request body likes below:

```
{
  "extension_number" : "8000",
  "status" : false,
  "extension_id" : 244385281237716992
}
```

The **extension\_id** is the id of extension which be the queue agents(members).

The **extension\_number** is the queue number.

## Set agent status to ready or not ready by dial code

The queue agent can dial a code to set his status to ready or not ready.

For example, extension 102 is the member of queue 8000, 102 can dial \*51\*8000 to set his status to **ready(sign in the queue)** and use \*52\*8000 to set the status to **Not ready(sign out the queue)**.

If extension 102 wants to set the status to **ready(sign in the queue)** for all queues, just dial \*51\*, set the status to **Not ready(sign out the queue)** for all queues, dial \*52\*.

## 5.11 Configuring Conference

When the PBX is successfully installed, you can create a conference room by selecting the menu “**Call Manager > Conference**” and click the “**Add**” button.

**Conference room for audio or video conferencing**

Conference Mode	Video Conference	*
Room Extension	9000	*
Subject	Test	*
Room PIN	123456	
Admin PIN	123456	
Outbound Caller ID		
Maximum Participants	9	
Grids for Video Conference	9	
Bitrate (Kbps)	1024	
Frame Rate	15	
Resolution	720P	
Prompt language	English	

Do not play prompt when joining the conference

Back Apply

To create a conference:

- Select the menu “**Call Manager > Conference**”, and click “**Add**” button.
- Select your conference mode from the “**Conference Mode**” drop-down list.
- Enter a conference Room Extension number which will be dialed by the conference Participants to join the conference. It should not be an existing extension number.
- Enter the suitable Subject for the conference to remind participant the topic to be discussed.
- Enter the PIN of the “**Conference Room**” if necessary. If the PIN was set, the Participants must enter the PIN when joining the conference.
- Enter the Admin PIN for the host. When a user enters this PIN, he/she will be identified as the conference admin to host the conference.
- Outbound Caller ID - Once the outbound caller ID for the conference room is set, when inviting an external number to the conference, PBX will place the call to external number on a provider / trunk, and this outbound caller ID could be a replacement for certain SIP field. For more details, please refer to Section [5.6](#Outbound parameters and Inbound parameters).

- Enter the maximum number of "**Maximum Participants**" field that limits the count of members who join this conference.
- Specify the count of videos in "**Grids for Video Conference**". Value 1, 2, 3, 4, 6, 9 supported.
- Set the bandwidth used during video conference in "**Video Conference Bitrate**". The value ranges 128 kbps – 2048 Kbps. The higher the value is, the better the video experience would be.
- Choose "**Video Conference Frame Rate**" with the range 5 – 30. Higher value will guarantee fluent video experience.
- Choose "**Video Conference Resolution**" from range of QCIF to 1080P. Higher resolution leads to larger load to bandwidth.
- Choose the Prompt Language for the vocal notices which will be used when user entering the conference.
- Click "**Apply**" button to confirm creating the conference room.

Each conference room supports up to 200 participants. It may vary dependent on the server CPU, memory and bandwidth.

## 5.12 Managing Conference

### Joining Conference

Once the conference room is created, inform the participants the conference number ("**Room Extension**"). Assume that the user sets Room Extension 8008 as the conference number, the user can join the conference by dialing 8008 from any SIP clients.

### Inviting participants into conference room

You can also invite an extension or the mobile phone/landline phone user to join the conference. Please see below section for more details.

### Managing the conference room





<input checked="" type="checkbox"/> Room Extension	Subject	Room PIN	Admin PIN	Mode	Status	
<input checked="" type="checkbox"/> 9000	Sales conference	123456	123456	Video Conference	Online	<a href="#">Manage</a> <a href="#">Edit</a> <a href="#">Delete</a>



Once the conference room is created, select the menu “**Call Manager > Conference**” to list available conference rooms. You can either edit the conference room or delete it by click the “...” icon to expand the menu.

- **Manage:** select the “**Manage**” menu to manage the conference room and participants, see next section.
- **Edit:** select the “**Edit**” menu to change the conference room settings, such as the **Room PIN, Admin PIN, Maximum Participants**.
- **Delete:** End and remove the Conference.

## Managing the conference participants

Participant	Action
101@portsip.io	   

Check a conference room in the conference list, and click the “**Manage**” icon to manage the conference room participants.

- **Invite participant:** Click the “**Invite**” button to select an extension from extension list, or enter the extension number directly. PBX will start a call to the specified extension.  
Once the call has been answered, the invited extension will be joint into the conference automatically.  
Mobile number or PSTN number could also be entered here to be invited into the conference but must configured the appropriate trunk and outbound rules.
- **Lock:** Once the conference is locked, other users cannot dial into the conference room.
- **Record:** Start or stop the conference recording
- **Mute:** When the room has been muted, all participants can't hear from each other.
- **Refresh:** Refresh the conference room information.
- **Recording files:** List recording files of the conference room. They could be downloaded and saved in local.
- **Mute:** Click the “**Mute**” button by the end of a listed extension to mute the selected participant.
- **Set as main:** Set the participant video as the main screen of video conference.
- **Hang up:** Kick out a participant from the conference room.

## 5.13 Billing

PortSIP PBX allows administrators/tenants to define customized calling rate. To do this, please go to "**Call Manager > Billing**".

### Parameters of billing rules

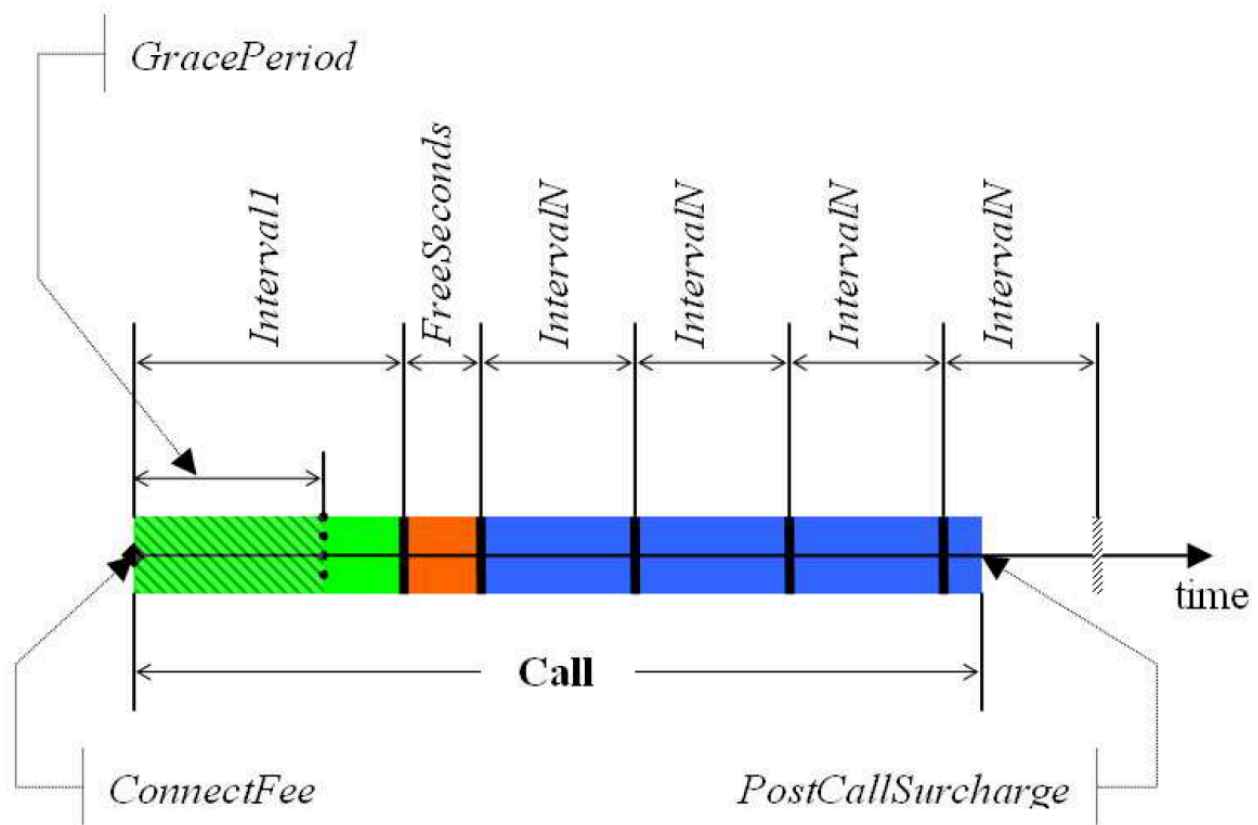
There are few parameters need to be entered when create the billing rule:

- FreeSeconds - in seconds
- ConnectFee - in monetary units
- PostCallSurcharge - in percents (0.01 means 1%)
- GracePeriod - in seconds
- Price' - in monetary units per minute
- PriceN - in monetary units per minute
- Interval' - in seconds
- IntervalN - in seconds

The simplest parameters are *ConnectFee*, which is fixed amount of money charged for each successful call regardless of its duration; and *PostCallSurcharge* which is additional charge applied. It is calculated on the percentage of the amount charged, that is if the call costs 1 dollar and the *PostCallSurcharge* is 0.01, the actual amount charged will be 1.01 dollar.

The following picture illustrates how the calls are charged. The process starts with comparing value of the *GracePeriod* parameter with the duration of the call. The *GracePeriod* parameter determines the minimum duration of the call that will be subject of charge. Calls with durations of less than this value are not charged at all. *GracePeriod* value of 0 second and 1 second provide almost the same behavior except that when the *GracePeriod* is 1 second, connected calls with zero duration won't be charged with connection fee.

A *ConnectFee* is charged immediately upon connection, and all calls shorter than Interval' will be rounded to *Interval1* seconds. *FreeSeconds* are granted after the *Interval1*, so this part of the call is not charged, and calls shorter than (*Interval1* + *FreeSeconds*) will be rounded to *Interval1* seconds. If call is longer than (*Interval1* + *FreeSeconds*) remaining portion will be rounded up to multiple *IntervalN* seconds. After that, the *PostCallSurcharge* is applied to the total amount charged.



The call illustrated in the figure will be charged using the following formula:

$$AmountCharged = \left( ConnectFee + \frac{Interval1 \times Price1}{60} + \frac{4 \times IntervalN \times PriceN}{60} \right) \times (1 + PostCallSurcharge)$$

- Connect fee - monetary units
- Price 1 - monetary units
- Price N - monetary units
- Interval 1 - seconds
- Interval N - seconds
- Post call surcharge - fractional based on the setting in the Tariff/Destination Set (E.g. for 10% fractional = 0.1)

## Adding Billing Rate

To add billing rate, go to “**Call Manager > Billing**” and click “**Add**”, and fill in the fields below:

- **Number Prefix:** Enter the specific number prefix. Once specified, all calls related to numbers started with this number will be applied with this rule.

- **Type:** Specify this rule for inbound or outbound calls.

Other fields are described in previous [section](#Parameters of billing rules).

## Importing/Exporting Rate

PortSIP PBX allows to import rates in batch by using “**Import**” button on “**Call Manager > Billing**” page. Once imported, all the imported rates will be listed on “**Billing**” page. If the rate to be imported is replica to an existing rate on PBX, the import process will fail.

Besides, all rate info online could be exported by using “**Export**” button on “**Billing**” page. Once completed, user will have a downloaded CSV file with all rates inclusive.

**Note:** Only CSV supported for both import and export features.

# Chapter 6: Tenant Management

PortSIP PBX is designed as Multi-Tenant, which means one PortSIP PBX installation can work for multiple enterprise (companies) by creating more than one tenants, and each tenant will be able to have their own PBX system.

## 6.1 Creating tenant

To create a new tenant, select the left menu “**Tenant**” and click the “**Add**”.

When creating a tenant, you can specify the tenant profile details such as username, password, sip domain and office hours. A tenant can modify his profile after signing into the Web Portal.

You can also limit the resource the tenant uses by clicking the “**Options**” tab. The “**Capability**” section under this tab allows you to set the maximum extensions, maximum concurrent calls, maximum ring groups etc.

In the “**General**” tab allows to set below parameters:

- **Username** - The tenant username that is used to sign in the Web Portal. It should be unique.
- **Domain** - The SIP domain for this tenant. It should be unique.

- **Extension is not allowed to delete recordings** - If it's selected, the extension can't delete the recording files even if he signs in the PBX Web Portal.
- **Enable this Tenant** - If this option is deselected, this tenant will be disabled, and all extensions of this tenant will no longer be valid.
- **Allow concurrent logins** - If this option is selected, the tenant can sign in Web Portal from multiple devices. If deselected, once tenant signs in, the login in another PC/mobile phone will be invalid.
- **Allow display extension password in local** - If selected, when editing extension in the "**Call Manager > Extension > General**", the extension password will be displayed.
- **Allow extension to create temporary meeting** - If selected, the extensions of this tenant will be able to create temporary meetings via REST API.

In the "**Options**" tab, set below parameters:

- **Country** - The country for the tenant
- **Timezone** - The timezone for the tenant
- **Currency** - The currency for the tenant
- **Enable extension to modify personal SIP password** - If selected, the extension will be able to modify his SIP password
- **Enable extension audio recording** - If selected, audio calls of all extensions will be recorded
- **Enable extension video recording** - If selected, video call of all extensions will be recorded
- **Capability** - Used to set the capabilities for the tenant

The "**Storage**" tab allows to adjust the storage quota for Recording files, Voice Mails and the Call Reports:

- **Disk quota (MB)** - The maximum disk quota allowed for this tenant
- **Recordings** - Current disk usage of recordings for this tenant
- **Voice Mails** - Current disk usage of voice mails for this tenant

You can set the way of deleting old recording files and voice mails in "**Auto cleaning**" section.

## 6.2 Deactivating tenant

To deactivate an existing tenant, select the left menu **“Tenant”**, and all tenants will be listed. Click the **“...”** button to expand the menu and choose **“Edit”** menu from the tenant that you want to deactivate, uncheck the **“Enable this tenant”** box and click **“Apply”** button. The tenant will be deactivated and all the extensions belongs to it would be deactivated as well.

If you want enable it again, check the **“Enable this tenant”** box.

## 6.3 Deleting tenant

To delete an existing tenant, select the left menu **“Tenant”**, and all tenants will be listed. Click the **“...”** button to expand the menu and choose **“Delete”** menu from the tenant that you want to delete.

**Note:** Once the tenant is deleted, all extensions of this tenant will be deleted as well.

## 6.4 Managing tenant

PortSIP allows administrator to manage tenant and its settings including extension users. To do this, please go to Web Portal, navigate to **“Tenant”** menu, select a tenant to be managed and click **“...”** button and choose **“Manage”**. Now user may setup or modify the settings for the tenant and manage its extensions.

Once completed, user may click avatar on the top right of page to display the menu and choose **“Switch to Administrator”** to switch back to administrator account, without the need to logout of tenant account and re-login to administrator account.

# Chapter 7. Call Statistics

The Call Statistics feature allows you to view the call log, current active sessions, call recordings and can be configured to send an email containing specific report statistics about calls to and from PortSIP PBX. You can also receive these reports with .CSV format.

## 7.1 Call Sessions

By using **“ Call Statistics > Call Sessions”** menu, you can quickly monitor all the current calls and details on PortSIP PBX.

<input type="checkbox"/> Caller	Callee	Session ID	Started on	Answered on	Talk Duration (Seconds)
<input type="checkbox"/> 101	102	6576733138179850242	2019-09-09 16:00	2019-09-09 16:00	14

< >

Hang up an established call by clicking "**Hung up**" button from a call session. Click the "**Refresh**" button to update the calls status.

## 7.2 Call Recording

By using "**Call Statistics > Call Recording**" menu, you can quickly list all the recorded calls and details on PortSIP PBX.

<input type="checkbox"/> Caller	Callee	Session ID	Started on	Answered on	Talk Duration (Seconds)
<input type="checkbox"/> 101	102	6576733138179850242	2019-09-09 16:00	2019-09-09 16:00	14

< >

You can select the call recording and click the "... " button to expand the menu to play , or download or delete it.

## 7.3 View Call Details

Select the left menu "**Call Statistics > Call Details**". All call logs will be listed. Click the "**Next**" button to see more.

<input type="checkbox"/> Caller	Callee	Started on	Answered on	Ended on	Duration	Outbound Caller...	DID/CID	Call Cost
<input type="checkbox"/> 101	102	2019-09-09 16:00	2019-09-09 16:00	2019-09-09 16:03	222			0.000000
<input type="checkbox"/> 101	102	2019-09-09 15:52	2019-09-09 15:53	2019-09-09 15:53	4			0.000000
<input type="checkbox"/> 101	102	2019-09-09 15:49	2019-09-09 15:49	2019-09-09 15:52	203			0.000000

< >

Note: You can view more call details by double clicking the CDR.

## 7.4 Call Reports

Reports are generated and sent automatically via emails, so that report creation can be executed with a low priority and will not interfere with the PortSIP PBX.

Note: To receive the exported call report, please make sure you have correctly configured SMTP mail server. To setup, please go to the Step 4 of Setup Wizard or go to "**Profile > Mail Server**".

**General**

Type: Basic Call Detail Record Report \*

From: 2019-09-09 16:12 \*

To: 2019-09-09 16:12 \*

Name: My\_CDR \*

Mail to: admin@portsip.com \*

Export as: CSV \*

**Call Status**

Answered

**Source**

Internal

**Destination**

Any

**Duration**

Enable Duration Statistics

From: 5 Seconds To: 30 Seconds

Back Apply

Select the "**Call Statistics > Call Reports**" menu and click "**Generate**" to create a new call report.

- Select the date range for call histories.
- Enter the email address the report will be sent to.
- Choose your preferred Report Format from the drop-down list. Default is .CSV.
- Select the filtering criteria by call status. Selecting the "Any" option will include both answered or unanswered calls, whilst selecting the "**Answered**" will include the answered calls only.
- Select the filtering criteria by call duration, then enter the call duration range (in seconds). For example, enter 10 to "From", and 20 to "End", so that the call report will include all call histories with the call duration between 10 and 20 seconds.

Click the "**Apply**" button, the call report will be sent to the specified email.

## Chapter 8. WebRTC

PortSIP PBX has inbuilt WebRTC client which allows you make & receive calls in the browser, support send IM, file, picture, picture clip, audio and video message, support conferencing and



sharing screen.

Before starting to use WebRTC Client, please ensure you have been read these sections carefully:

- The [2.6 Avoid HTTPS Certificate Security Warnings](#2.6 Avoid HTTPS Certificate Security Warnings).
- The [3.1 Deploying PortSIP PBX in LAN](#3.1 Deploying PortSIP PBX in LAN).
- The [5.1 Add TLS/WSS transport](#5.1 Add TLS/WSS transport).
- The [17.3 Solve the self-signed certificates warning](#17.3 Solve the self-signed certificates warning).

If you used a trusted SSL certificates, please click left menu node "**WebRTC**", the browser will opens WebRTC client in a new browser tab (Note: Chrome, new Edge, Firefox are recommended), you will just need to enter the extension number and password to sign in.

Note: Chrome, new Edge, Firefox are recommended, and up to date.

**If you used the self-signed SSL certificates, please follow below steps:**

**step 1:** open <https://192.168.0.16:5065/> in a browser, the browser will warning the connection is unsafe, see below screenshot, please just click the "**Proceed to 192.168.0.16(unsafe)**".

(Note: the 5065 port is the WSS transport that you added in the PortSIP PBX, if you used another port for the WSS transport, you should change the port here:

<https://192.168.0.16:wssport/> )



## Your connection is not private

Attackers might be trying to steal your information from **192.168.0.16** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

💡 To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced

Back to safety

This server could not prove that it is **192.168.0.16**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.0.16 (unsafe)

**Step 2:** please click left menu node "**WebRTC**", the browser will opens WebRTC client in a new browser tab, the browser will raises warning again, please just click the "**Proceed to 192.168.0.16(unsafe)**". then you will just need to enter the extension number and password to sign in.

After signed in, you can use the WebRTC client to make & receive calls.

## Chapter 9. Contacts

PortSIP includes Contacts (Phone Book) feature to manage contacts. It enables to import and export contacts to the CSV file.

Contacts not only allows easy dialing of contacts, but also enables to match incoming call to customer names, so that caller is shown with its customer name instead of the caller ID.

The Contacts is synchronized with the PortSIP UC client apps and connected IP phones.

<input checked="" type="checkbox"/> Name	Member count	Description
<input type="checkbox"/> PublicPhonebook	0	
<input checked="" type="checkbox"/> SalesPhonebook	0	

Manage  
 Edit  
 Delete

By clicking "**Contacts**" menu, all the contacts in the phone book will be listed. You can click the "..." button to expand the menu beside a certain contact:

- **Manage** - To add the contacts into the phone book
- **Edit** - To change the phone book settings
- **Delete** - To delete the phone book

## Creating a new Phone book

By navigating to "**Contacts**" menu, and clicking the "**Add**" button, you can create a new Phone book and assign it to the specified extension group, so that the extensions of the extension group will be able to access this Phone book.

**Manage Contacts**

Name  \*

Description

**Extension groups**

Allow below extension groups access this contacts

Sales Department

Support Department

\_\_DEFAULT\_\_

## Importing & Exporting Phonebook Entries

You can import contact entries from a CSV file with the column headers on the first line, and each contact entry on a single line with fields separated by a comma. You may find the [example CSV file at PortSIP Website](#).

After you have downloaded that sample CSV file, you can fill in it with your contact entries. To import the company contact entries into the PortSIP PBX, sign in the Web Portal:

1. Navigate to "**Contacts**" menu and click "**Import**" button.

2. Browse your saved CSV file, select it and click “**Open**” to import your contact entries into the phonebook.

To export entries from the PortSIP Contacts to a CSV file:

1. Navigate to the “**Contacts**” menu and select a phone book, and click “**Export**” button.
2. Enter the target CSV file and click “**Save**” to export your phonebook entries.

When an IP Phone is successfully provisioned, the phone books which assigned to this extension will be Synchronized to IP Phone automatically as “**Remote Phone Book**” for IP Phone.

## Chapter 10. Logs

The PBX Logs is an important troubleshooting tool that may help you identify the cause of simple (and possibly complicated) issues.

### 10.1 Event Log

The Event Log will display the information when an event occurs, for example, the media server is connected or disconnected, an transport is created.

### 10.2 Activity Log

The Activity Log will display the information for an operation which is completed or failed, for example, a conference room is successfully created.

### 10.3 Log Files

You can download the log files of the PBX and analyze it locally.

## Chapter 11. Advanced

After successful installation, the PortSIP PBX Configuration Wizard will guide the user go through a series of settings that elicit basic configuration data. After completing basic

configuration with the Configuration Wizard, you can commit detailed configuration by using "**Advanced**" menu in Web Portal of PortSIP PBX.

**Important Note:** only the administrator is allowed to access the "**Settings**" menu to change the settings. Neither the tenant nor extension could change the settings.

## 11.1 Settings

### General

You can change the general settings by selecting "**Advanced > Setting**" in PortSIP PBX Web Portal.

Note: Usually we recommend NOT to change the default settings.

- **Log Level:** To output all SIP messages (sent and/or received) to log file in an easy-to-read manner. The log file is named as "*callmanager\_log*". Set the log level as "**None**" will make significant improvement to PBX performance.
- **Enable IPv6:** This option could be used to enable or disable support on IPv6.
- **Disable DIGEST authentication:** If DIGEST authentication is disabled, the authorization will be disabled as well. This option is deprecated (do not disable DIGEST challenges).
- **Disable auth-int DIGEST authentication:** Once this option is checked, auth-int quality of protection will be disabled.
- **Disable authentication of mid-dialog requests:** The PBX will not require authentication of all requests in dialogs if this option is selected.
- **Send 403 if a client sends a bad nonce:** Send 403 if a client sends a bad nonce in their credentials with this option selected. A new challenge will be sent if this options is un-selected.
- **Allow "to" tag in Registrations:** Allow "to" tag in REGISTER message.
- **Statistics Log Interval:** Specify the interval for writes of the stack statistics to the log files. The default value is 600 seconds.
- **Enable Congestion Management:** Use this option to enable/disable the congestion management.
- **Congestion Management Metric:** The recommend value is **WAIT\_TIME**. This value is dependent on the expected wait time for each FIFO; this is calculated by multiplying the size with the average service time.

- **Congestion Management Tolerance:** Congestion Management Tolerance for the given metric. This determines when the Rejection Behavior changes. The default value is 80.

Value	Description
80	Percentage of max tolerance -> NORMAL (Not rejecting any request);
80 - 100	Percentage of max tolerance -> REJECTING_NEW_WORK (Refuses new work, not continuation of old work.);
> 100	Percentage of max tolerance -> REJECTING_NON_ESSENTIAL (Rejecting all work that is non-essential to the system (i.e. if dropping something is liable to cause a leak, instability, or state-bloat, don't drop it. Otherwise, reject it.).

- **Automatically create the extension when a non-existent extension tries to register:** If this option is selected, when a non-existent extension registers to PBX, the PBX will create this extension automatically. The default password for this new extension is "portsip".
- **Enable PRACK (Reliability of Provisional Responses):** If this option is selected, the Reliability of Provisional Responses (RFC3262) will be enabled.
- **Enable Flow Routing:** To enable RFC5626.
- **Close the session if no RTP packet received within specified period:** The PortSIP PBX tracks idle time for each of existing sessions (i.e. the time within which there were no packets received), and automatically cleans up a session whose idle time exceeded the value specified at compile time (120 seconds by default).
- **Enable the session timer (RFC4028):** Enable the session timer (RFC4028) to detect if the caller and callee are online. If this option is selected, the PBX will send repeated INVITE requests to both caller and callee. The call will be hung up by PBX if the INVITE is not correctly responded.
- **Session timer duration:** Specify the session timer duration during which the PBX will send INVITE message to caller and callee. Default value is 120 seconds, and the minimize value is 90 seconds.
- **DNS Server:** Specify the DNS server here, which overrides default OS detected

DNS server list. If it is left blank, the PortSIP PBX will use default DNS server for system.

## Port Range

You can change the Media server RTP range by selecting "**Advanced > Port Range**" in PortSIP PBX Web Portal.

## Advanced

You can change the advanced settings by selecting "Advanced > Settings" in PortSIP PBX Web Portal.

- **Dial code:** Specify the prefix for making the Paging/Intercom call. With this prefix specified, when the calling number is prefixed with dial code, the PBX will process the call as Paging/Intercom. For more information, please see Section "**Paging**" and "**Intercom**".
- **Alert-Info header for Auto Answer:** Choose the "**Alert-Info**" header's value, which will be inserted into the SIP INVITE message when making Paging/Intercom call.  
For example, if "**alert-autoanswer**" is chosen, the below header will be inserted into SIP INVITE message: "**Alert-Info:info=alert-autoanswer**"  
Once the extension IP Phone detected "Alert-Info", it will answer the call automatically and turn on the speaker.
- **Enable Call-Info header for Auto answer:** Insert the "**Call-Info**" header into the SIP INVITE message when making Paging/Intercom call.  
For example, if this option is selected, the below header will be inserted into SIP INVITE message:  
**"Call-Info: sip:portsip.com;answer-after=0"**  
Once the extension IP Phone detected "**Call-Info**", it will answer the call automatically and turn on the speaker.
- **Require Answer Mode (RFC5373):** Insert the "AnswerMode" into the SIP INVITE message when making Paging/Intercom call.  
For example, if this option is selected, the below header will be inserted into SIP INVITE message:  
**"AnswerMode: auto"**  
Once the extension IP Phone detected "**AutoAnswer**" as "**auto**", it will answer the

call automatically and turn on the speaker.

Different IP phones support different auto answer modes. Please refer to your IP Phone manual to choose the correct mode.

- **Busy Lamp Field:** In this section, you could check “**Enable Dialog State Agent**” and enter value for “**Ringling Call Prefix**” and “**Held Call Prefix**” respectively to enable Busy Lamp Field feature for calls. Default value for “**Ringling Call Prefix**” is , and ## for “**Held Call Prefix**”.

For example, an administrative assistant can see the status of their supervisor's line so he or she knows when their boss is on the phone. Speed Dial is also available, which means the assistant can pick up the phone, press the line configured to their supervisor's line, and their supervisor's extension will ring.

If the boss' extension is 101:

1. The assistant could use his/her IP phone to dial \*\*101 to pick up the boss' incoming call, if there no available incoming call, PBX will try to pickup the held call
2. The assistant could dial ##101 on his/her own IP phone to pick up the call which held by boss

## 11.2 CTI

The PortSIP PBX support advanced CTI features, for example, silence monitoring, whisper, barge-in, barge-break.

### CTI Features

Silent call monitoring allows a supervisor to eavesdrop on a call conversation. The most common scenario is in a call center where a call agent is speaking with a customer. Call centers need to be able to guarantee the quality of customer service that an agent in a call center provides. With silent monitoring, the supervisor can hear both call participants, but neither of the call participants can hear the supervisor.

Silent monitoring is call based. When a supervisor invokes a silent monitoring session, the following occurs:

- The supervisor selects a specific extension call to be monitored.
- The agent and customer voice will be sent to supervisor call automatically. The monitoring call does not get presented to the agent and customer.



If you want someone (for example, the call queue manager) do silence monitor, you will follow below steps:

1. Click the menu "**Call manager > Extension groups**", Selected an extension group and click the "..." icon to pops up the menu, then choose "**Edit**", click the "**Monitor**" tab, choose the extensions who you would like to grant the monitor permission to him and checked the "**Allow Monitor**" the click "**Apply**" button.
2. Click the menu "**Advanced > CTI**", checked "**Enable Monitor**" option, by default, the silence monitor service number(Monitor Number) is **888**, you can change it if you like.

## Example:

We would like to let the extension 101 and 102 to silence monitor other extension's calls.

1. Click the menu "**Call manager > Extension groups**", create a new group which named "**Queue Manager**"
2. Selected this extension group and click the "..." button, choose "**Edit**" menu, click the "**Monitor**" tab
3. In "**Monitor**" tab, add the 101 and 102 into the monitor members
4. Checked the "**Allow monitor**" option and click the "**Apply**" button
5. Click the menu "**Advanced > CTI**", checked "**Enable Monitor**" option, and click the "**Apply**" button.
6. Now if the extension 103 has a call, then 101 or 102 can silence monitor 103 by dial "**888\*103**"
7. During silence monitoring, the 101 or 102 can press DTMF 2 to whisper, press 3 to barge-in, and press 4 to barge-break the 103's call
8. The 101 or 102 can dial "**888\*103\*1**" or "**888\*103**" directly to silence monitoring; By dial "**888\*103\*2**" to whisper 103, dial "**888\*103\*3**" directly to barge-in, and dial "**888\*103\*4**" directly to barge-break the 103's call.

## Exclusive Agent

In some scenarios, for the special industry callers of contact center, we will need the special agents who have rich special industry knowledges and skills to serve them.

PortSIP PBX provides the "**Exclusive Agent**" feature allow set up one or more agents from the queue as "**Exclusive Agent**" for the special callers, once the call comes from these

callers, the queue will distribute the call to the **exclusive agent** give highest priority if the agent is idle, of course if all exclusive agents are busy / sign out, the call will be distributed to other agents.

- Click the menu "**CTI > Exclusive Agent**", click the "**Add**" button
- **Description:** A descriptive name for the exclusive agent being entered. For example, enter "**XXX Bank**" as the description for the bank caller.
- **\*\*Caller number:\*\*** enter the caller number who will be assigned the exclusive agents. Once the call comes from this caller, the call will be distributed to the exclusive agent with highest priority.  
You can add more caller numbers by click the "**Add**" button.
- **Call Queue:** choose the queue member from the queues to set up as exclusive agent

**Note: if the call is not comes from the specified caller numbers, the exclusive agent works as the normal agent.**

## VIP List

PortSIP PBX provides the VIP Caller feature, make VIP customers feel special when trying to connect PortSIP PBX contact center. When the VIP call was determined, the queue always give the top priority to the caller and pushed on top of the queue.

- Click the menu "**CTI > VIP List**", click the "**Add**" button
- Enter the VIP customer phone number
- **Description:** A descriptive name for the VIP Caller being entered. For example, enter "**Microsoft team**" as the description for the VIP caller
- Set up how long of the the VIP number validity
- **Enabled:** turn on/off

**Note: the VIP list is global validity for all queues**

## Harass Numbers

Spam calls are the plague of all businesses, especially call centers, PortSIP PBX provide three ways for anti the spam calls.

1. A global "**Number Blacklist**", it will rejected the call silently if the caller is in the

number blacklist. You can find the details at section [12.2 Number Blacklist](#12.2 Number Blacklist).

2. **Harass Number:** PortSIP PBX also provides the "**Harass Number**" features for anti the spam calls only for the Call Queue. The harass number is defined as two levels, if a caller is determined in the "**Level 1**", the preset prompt file will be played to alert the caller, and if caller press **1** the call will be hang-up, press **2** the call is continue; If a caller is determined in the "**Level 2**", the preset prompt file will be played to alert the caller, and the call will be hang-up automatically after play finished.

**Note: both of the two levels of the "Harass Number" only for the call which reached to the queues, and its validity to all queues.**

## 11.3 Managing Media Server

The media server is used for handling NAT scenarios and acts as a relay gateway for RTP sessions of calls.

With the PortSIP PBX successfully installed, a built-in media server has been enabled by default. The RTP packet from VoIP Endpoint A will be routed to Endpoint B with both IP and Port translation during each call established.

<input type="checkbox"/> Server Name	Private IPv4	Public IPv4	Private IPv6	Public IPv6	Port	Enabled	Status
<input type="checkbox"/> _DEFAULT_	192.168.0.16	192.168.0.16			8896	<input checked="" type="checkbox"/>	Online

< >

### Adding External Media Server

The PortSIP PBX uses default media server to relay RTP packets for calls. A large amount of simultaneous calls will lead to high loads of CPU, network bandwidth, memory overload, voice latency, unavailability for new calls, etc...

You can add more media servers to handle the RTP packets relay in order to reduce the PortSIP PBX IP loads and decrease network latency.

**Settings for Media Server**

Server Name	<input style="width: 95%;" type="text" value="MediaServer2"/>	*
Private IPv4	<input style="width: 95%;" type="text" value="192.168.0.18"/>	
Public IPv4	<input style="width: 95%;" type="text"/>	
Private IPv6	<input style="width: 95%;" type="text"/>	
Public IPv6	<input style="width: 95%;" type="text"/>	
Server Port	<input style="width: 95%;" type="text" value="8896"/>	*
Maximum call sessions	<input style="width: 95%;" type="text" value="2000"/>	*
<input checked="" type="checkbox"/> Enabled		

Select the "**Advanced > Media Server**" menu in PortSIP PBX Web Portal, click "**Add**" and enter a friendly name for the new Media server, and the IP of new Media Server (it could be IPv4 or IPv6), and port number (default is 8896). Also please specify the maximum of call sessions the media server could support on RTP data transportation.

## Editing Media Server

You can view all the added media servers by clicking the menu "**Advanced > Media Server**". In the media server list, you can check the state for each server, such as enabled or disabled, connected to PBX or disconnected. You may also configure the media server settings by clicking "... " icon to popups the menu and choose the "**Edit**".

In the "**Maximum call sessions**" filed, you can specify the maximum call sessions the media server could handle.

You can also disable a media server by turning off the "**Enabled**" switch button in the media server list.

## Removing Media Server

You can view the media servers by clicking "**Advanced > Media Server**". To remove a media server, please click to select the server, and click the "**Delete**" button on the top of web page. After a media server is removed, the PortSIP PBX will no longer use it to relay the RTP packets.

**Note:** The Built-in(default) Media Server cannot be removed, but you can disable it by clicking the "**Enabled**" button to disable it.

Be careful about the Built-in Media server. If you disabled it and did not add any other media servers, the RTP packet will be sent directly between SIP endpoints during the calls, and if the PortSIP PBX is running on internet, it may cause no audio and video transmit in the call.

## 11.4 Managing Conference Server

PortSIP PBX System provides multi-user conference features. Once the PBX successfully installed, a built-in conference server is enabled by default. You can create as many conferences as you like, as long as there still are free system resources (i.e. memory, CPU, bandwidth) left.

### Adding External Conference Server

PortSIP PBX uses conference server to handle the conference. The large amount of simultaneous calls or a lot of conference servers will lead PBX server to high loads of CPU, network bandwidth and memory, which eventually cause voice latency, and unavailability to handle new calls.

You can add more conference servers to handle the conference in order to reduce the PBX Server loads and decrease network latency.

**Settings for Conference Server**

Server Name	<input type="text" value="ConferenceServer2"/>	*
IPv4 Address	<input type="text" value="192.168.0.20"/>	
IPv6 Address	<input type="text"/>	
Server Port	<input type="text" value="8886"/>	*
Maximum Rooms	<input type="text" value="200"/>	*
Maximum Participants	<input type="text" value="10"/>	*

In PortSIP PBX Web Portal, select the "**Advanced > Conference Server**" menu, click "**Add**" button, and enter a friendly name for the new Conference Server, the IP of new Conference Server (could be IPv4 or IPv6), and conference server port 8886. Also please enter the maximum conference rooms and maximum participants, and click "**Apply**" button.

### Editing Conference Server

You can view all the added conference servers by clicking "**Advanced > Conference Server**". In the conference server list, you can check the state for each server, such as enabled or disabled, connected to PBX or disconnected. You may also configure the conference server settings by clicking "**Edit**" icon button to popups the menu and choose "**Edit**".

In the "**Maximum Rooms**" filed, you can specify the maximum conference rooms for this conference server that you can handle.

You can also disable a conference server by turning off the “**Enabled**” switch in the conference server list.

## Removing Conference Server

You can view all the Conference Servers by clicking "**Advanced > Conference Server**". To remove a conference server, click to select the server to be removed and "Delete" button from the top of webpage. Once the Conference Server is removed, the PortSIP PBX will no longer use this Conference Server to handle conference.

**Note:** The Built-in Conference Server cannot be removed, but you can disable it by clicking the "**Enabled**" switch.

Be careful about the Built-in Conference server. If you disabled it and did not add other conference server, the conference feature will not be enabled.

## 11.6 Configuring Mobile PUSH

PortSIP PBX uses PUSH technology to wake up the smartphone when a call is received on client. Mobile PUSH messages wake up PortSIP Softphone or other Client Apps on mobile device so that a call or Instant Message can be accepted, reducing battery usage and improving reliability.

Android phones receive PUSH notifications from Firebase Cloud Messaging Server; Apple phones receive PUSH notifications from APNs.

**Add App for enabling PUSH notification**

Mobile PUSH messages wake up PortSIP Softphone or other Client Apps on mobile device so that a call or Instant Message can be accepted, reducing battery usage and improving reliability  
Android devices receive PUSH notifications from Firebase Cloud Messaging Server; iOS devices receive PUSH notifications from APNs  
PortSIP PBX is pre-configured with PortSIP Softphone account for receiving mobile PUSH. You can create your own Firebase or APN account to instead of the PortSIP account. [Click here](#)

**PUSH notification for App**

Enabled

Connect to Apple / Google Production PUSH server

Connect to Apple / Google Development PUSH server

App Name  \*

Google Server Key

Google Senderid

Apple Certificate file  ...

Apple Private key file (no password)  ...

PortSIP UC Client app has built-in push service enabled by default in PortSIP PBX. If you wish to enable another app, you can create your own Firebase or APN account to support the push notifications for your apps.

### Configure PortSIP PBX for Mobile PUSH Notifications

1. Login to the PortSIP PBX Web Portal.
2. Navigate to “**Advanced > Mobile PUSH > Add new APP**” for setting up a new app for receiving PUSH notifications.
3. Check “**Enable**” to enable PUSH notification.
4. Enter the App ID.
5. If necessary, enter Google Server Key and Google SenderID for Android clients, and upload Apple Certificate File and Apple Private Key file for Apple clients.
6. Click “**Apply**” to apply the settings and restart all clients so they re-provision and take the latest settings. The step by step guide for make the Mobile PUSH notifications works with your app and PortSIP PBX, please refer to below topics:
  1. [Implement the PUSH notifications in Native iOS App with PortSIP PBX](#)
  2. [Implement the PUSH notifications in Android App with PortSIP PBX](#)

## 11.7 Configuring Voicemail

### Set the extension number of voicemail

When the PortSIP PBX is successfully installed, the Voicemail service would be enabled by default. You can specify the voicemail service extension number by clicking “**Advanced > Voice Mail**” node in left menu.

Users could dial to read his voice mails. The default voice mail number is 999.

### Set voice mail quota

PortSIP PBX allows you specify the disk quota to store the voice mails. The default value is unlimited. You can also enter the number of days that they will be kept before they're deleted automatically.

## 11.8 Security

PortSIP PBX provides security features with main purpose to block any malicious attacks

targeted to the PortSIP PBX in case the admin has not taken necessary precautions at firewall level. It works by detecting and blocking packet floods / DoS attacks or brute force dictionary attacks within the scope of identifying and cracking the extension number and the password.

The Anti Hacking configuration page is accessible by clicking on the menu "**Advanced > Security**".

## **Detection Period**

This is a time interval in seconds when counting starts but no action is enforced. To disable security, set it to a higher value.

## **Failed Authentication Protection**

This is the protection in case the attacker tries to use a dictionary attack to guess the password set for a particular extension. To do this the attacker has to send numerous invites and after the server sends a "Proxy authentication Required message" the attacker will send an invite with authentication. With this feature, the attacker can only send 25 requests in an attempt to crack the password. If an IP Address spams PortSIP with 10 wrong Authentication attempts in "Detection Period", that IP address will be blocked and put in the blacklist for the time specified in the "SIP Blacklist time interval" parameter, by default 1 hour.

## **Failed Challenge Requests (407)**

D.O.S attacks can send REGISTER/INVITE requests but do not reply to Challenge (407). Configure the amount of "**fake**" requests that PortSIP PBX will accept per IP Address. If this value is exceeded in "**Detection Period**" interval the source IP address is put in the Blacklist. IP will remain blacklisted till "**SIP Blacklist time interval**" expires, by default 1 hour.

## **Level 2 security**

This is the 2nd layer of protection. Here you can specify how many packets can be sent from a unique source IP address. The default value is 2000 packets per second. If an IP Address is sending more than 2000 packets per second, it means that there is something wrong. At this point the attacker IP will be blocked until "Level 2 blacklist time interval" expires.

## **Level 1 security**

This is the 1st layer in packets per second. If an IP sends more packets than the amount



specified per second, it will get blacklisted for the "**Level 1 blacklist time interval**". Default value is 5000 packets per second. At this layer, once that packet rate exceeds this layer, the blacklist is enforced.

Once an IP address was blocked due to above rules, it will display in the 12.3 section, from which you can add it into "**Whitelist**" manually.

## 11.9 Backup and Restore

PortSIP PBX has provided backup and restore feature to backup system settings and data, which enables to easily restore system and data when necessary, or migrate the system from one machine to another.

### Backup

To backup the PBX, please:

1. Go to "**Advanced > Backup**" menu, and click "**Backup**" button on top of the page.
2. Enter the filename for the backup in "**Backup File Name**", and choose the files to be included in the backup.
3. Click "**Apply**" to commit the backup.
4. It will take a while to complete the backup. Once completed, please refresh the page to view the backup file. User now may click to select one item of the list and click "... " icon button to popups the menu and choose "**download**" to download it to local, or click "**Restore**" button to restore PBX from backup file.

### Migrate PBX to another Machine on Windows

To migrate the PortSIP PBX from one machine to another:

1. Backup the PBX as described in [above steps](#), and download the backup file to local.
2. In the new machine which has the PortSIP PBX installed, copy that downloaded backup file to the **c:\ProgramData\PortSIP\backups** folder of new PBX server (The **c:\ProgramData** is hidden folder)
3. Sign in Web Portal of PortSIP PBX Click menu "**Advanced > Backup**", you will see that backup file.
4. Click the "... " button of this back file to expand the menu, choose "**Restore**"

5. Once the restoration is completed, you will be redirected to the Sign-in page. Sign in again (If you fail to sign in, please wait a while as the restoration is not completed yet)

## Migrate PBX to another Machine on Linux

To migrate the PortSIP PBX from one machine to another:

1. Backup the PBX as described in [above steps](#), and download the backup file to local.
2. In the new machine which has the PortSIP PBX installed, copy that downloaded backup file to the **/var/lib/portsip/backups** folder of new PBX server
3. Perform this command to change the owner of the backup file:

```
sudo chown 888:888 /var/lib/portsip/backups/backupfile.ar
```

4. Sign in Web Portal of PortSIP PBX, click the menu "**Advanced > Backup**", you will see that backup file.
5. Click the "..." button of this back file to expand the menu, choose "**Restore**"
6. Once the restoration is completed, you will be redirected to the Sign-in page. Sign in again (If you fail to sign in, please wait a while as the restoration is not completed yet)

## Backup Schedule

In addition to common single backup, user may also setup "**Backup Schedule**" to backup PBX settings and data regularly.

To do this, please go to "**Advanced > Backup**" menu, click "**Backup Schedule**" button on top of the page, and fill in below fields if necessary:

- **Enable backup schedule:** Please check this selection to enable "**Backup Schedule**".
- **Choose items to be included in backup:** This sections lists all the files available for backup, including a few items which can be backup. A selected item indicates the file type to be included in backup.
- **Backup timing:** Backup could be scheduled to execute daily or weekly by selecting the list time. Once selected, user may specify the hour for stating backup. For weekly backup, the weekday for running backup is also necessary.

## 11.10 License

Without a license, PortSIP PBX could work for up to 3 simultaneous calls and 10 extension registrations. If you require more, you will need to purchase a license.

Feel free to contact [sales@portsip.com](mailto:sales@portsip.com) to purchase the license.

Once you have received the license key, please click the menu "**Advanced > License**", and enter the key received.

PortSIP PBX requires Internet connection to verify the license key periodically. Please ensure that your PBX server could be connected to Internet smoothly. If the license key verifications fails, the PBX will be downgraded to free version which only allow maximum of 3 simultaneous calls.

Do not let others know your license key. If PortSIP PBX detects a second user, it will be forced into invalid and will downgrades to free version which only allow maximum of 3 simultaneous calls and 10 extensions registrations.

Please contact PortSIP Support or reseller if you encountered any license key related issue.

## Chapter 12. Blacklist and Codes

### 12.1 Codes and E164

PortSIP PBX allows to set the allowed country code and disallowed code in order to stop extension dialing a specific country.

To allow or disallow the country code, please click the "**Blacklist and Codes > Codes and E164 > Allowed Country Codes**", you can select or de-select one of more than one country.

#### Disallowed Codes

User may use this feature to block the calls made on the trunks by specified prefix.

Go to "**Blacklist and Codes > Codes and E164**" menu, select the "**Disallowed Codes**" tab, you can add the disallowed number prefix by click the "**Add**" button.

## Number Processing

**Select country:** Pretty straight forward. Select the country you are in so the system knows your country code. For our examples lets use US as our country.

**Remove if same country:** When this option is selected and you try calling the same country using the E164 format the country code will be removed from the called number.

Example: Number dialed as +12345678910 will be converted to 2345678910.

**International Dial Code:** If you call a different country using the E164 format then the number will be converted and the international dial code will be added. If you are in the US for example this will be 011. This will enable you to make international calls without the "+".

Example: Number dialed as +44123456789 will be converted to 01144123456789.

**Area Code:** Here you can add your area code so if you are making calls within your area and the area code is not required then you can strip it if the "Remove if same Area Code" is selected.

Example: Our area code is set to 813. Number dialed as +181345678910 will be converted to 45678910.

**National Code:** If you need to add a national code to make calls then you can add a national code here and it will be prepended to the number during the processing.

Example: National code set to 8. Number dialed as +12345678910 will be converted to 82345678910.

**Add Prefix:** A prefix can be added in case it is needed or if you want to use it to select an outbound rule. E164 rules are processed before the outbound rules.

Example: Prefix is set to 2. Number dialed as +12345678910 will be converted to 22345678910.

## 12.2 Number Blacklist

PortSIP PBX allows you to block certain number. All requests associated with blacklist will be blocked immediately.

To add the number into blacklist:

1. Sign in the PortSIP PBX Web Portal
2. Click on "**Blacklist and Codes > Number Blacklist**" from the left menu

3. Click **“Add”** to add a new entry
4. Enter the number that you want to block and enter the description

## 12.3 IP Blacklist

PortSIP PBX allows you to whitelist and blacklist IP addresses. All traffic originated from whitelisted IP addresses will be allowed through unchecked by the anti-hacking features. All traffic originating from blacklisted IP addresses will be dropped immediately.

### Adding a Whitelist Entry to PortSIP PBX

Assume that you have a remote office connected to your PortSIP PBX. Your remote office has a public IP address of 123.123.123.123. Traffic from this IP address is trusted. To add this IP address into whitelist, you'll need to follow below steps:

Blacklist/Whitelist IP or Range of IP Addresses	
IP Address	<input type="text" value="123.123.123.123"/>
Subnet Mask	<input type="text" value="255.255.255.255"/>
IP address range	<input type="text" value="123.123.123.123"/>
Action	<input type="text" value="Allow"/>
Description	<input type="text" value="My remote office"/>
Expiration Date	<input type="text" value="2019-09-27 14:42"/>

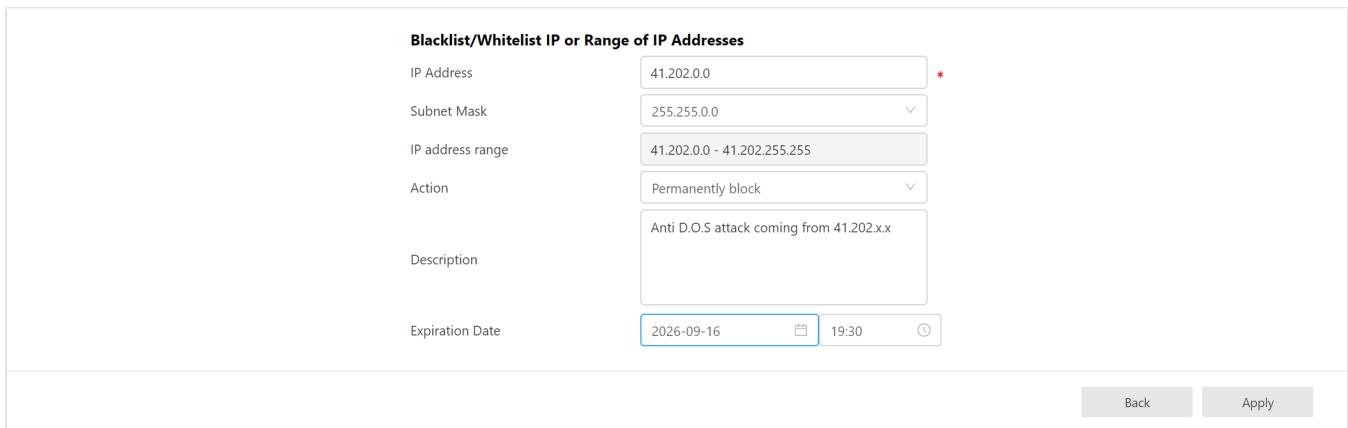
Back Apply

1. Sign in the PortSIP PBX Web Portal.
2. Click on **“Blacklist and Codes”** > **“IP Blacklist”**.
3. Click **“Add”** to add an entry.
4. Enter the IP address that you want to allow – in this example it should be 123.123.123.123 (you can also enter the IP 123.123.123.0 and choose a Subnet Mask to allow an IP range).
5. Choose **“Allow”** for **“Action”** field.
6. Add a description for the IP address, for example **“My Remote office”**.
7. Click **“Apply”**. An allow entry will be created in the IP Blacklist page for the whitelisted IP address. All traffic originated from this IP address will not be checked and the anti-hacking algorithms will not come into effect.

## Blocking an IP Address or a range of IP Addresses

Let us look at another scenario. Assume that there is a distributed attack coming from the following IP addresses – 41.202.160.2 and 41.202.191.5. These two IP addresses have already been blacklisted by PortSIP PBX’s anti-hacking auto-detection mechanisms.

You would, however, want to blacklist all the range, since you are sure that you will never get any traffic from these IP addresses. In this case, we will blacklist the whole range from 41.202.0.0 to 41.202.255.255, i.e. all the IP addresses that started with 41.202.



The screenshot shows a web form titled "Blacklist/Whitelist IP or Range of IP Addresses". The form contains the following fields and values:

Field	Value
IP Address	41.202.0.0 *
Subnet Mask	255.255.0.0
IP address range	41.202.0.0 - 41.202.255.255
Action	Permanently block
Description	Anti D.O.S attack coming from 41.202.x.x
Expiration Date	2026-09-16 19:30

At the bottom right of the form, there are two buttons: "Back" and "Apply".

1. Sign in the PortSIP PBX Web Portal
2. Click on “**Blacklist and Codes > IP Blacklist**”
3. Click “**Add**” to add an entry
4. In the “**IP address**” enter the first address of the network range you want to block. For this example we will enter 41.202.0.0
5. Since we want to block all IP addresses started with 41.202, we will select a Subnet Mask of 255.255.0.0. The range of IP addresses contained in this mask will be displayed below
6. Set Action to “**Permanently block**”.
7. Enter a Description for this entry to help you remember why you added this entry, for example “Anti D.O.S attack coming from 41.202.x.x”.
8. Click “**Apply**”. A block entry will be created in the IP Blacklist page. All traffic coming from this IP address range will be checked, anti-hacking algorithms will come into effect and all packets from this IP Address range will be completely dropped and ignored
9. The PortSIP Blacklist / Whitelist mechanism does not conform a replacement of firewall. It merely provides a defense mechanism to help differentiate traffic

trustable, and traffic not trustworthy. If, for example, you want to block all traffic to your network and allow only your VoIP Provider IP address, you need to set this up on your firewall.

When configuring a range of IP addresses in the Blacklist, you should also ensure that the range does not include the IP address of which the PBX is installed.

## Chapter 13. Profile

The admin and tenant user can manage their profile by selecting the “**Profile**” menu from the PortSIP PBX Web Portal.

### 13.1 General

The admin user(admin also is a tenant) or tenant user can modify their profile details in the “**General**” tab:

Username: The username for the admin or tenant user.

#### General Information

- **Username:** You can change the username (used for signing into Web Portal)
- **Password:** If the password was modified, the admin or tenant user must use new password to login to Web Portal.
- **Domain:** The SIP domain for the tenant.
- **Company name and company website:** The company name and company website for the admin or tenant user. The extension’s company name and company website is inherited from the admin/tenant user who created the extension.
- **Email:** The email for admin or tenant user, which is used for receiving notification from PBX.

#### Capability

This section will display the capability of the admin/tenant. The tenant cannot modify the capability for himself.

- Maximum Extensions

- Maximum simultaneous calls
- Maximum Ring Groups
- Maximum Call Queues
- Maximum Conference Rooms
- Maximum Virtual Receptionists

## Options

- **Country:** The country of the tenant
- **Time zone and Currency:** The time zone and currency for the admin or tenant. This setting will affect all extensions created by the admin or tenant.
- **Billing for all outbound calls:** If this option is selected, when the extension make outbound call via trunk/VoIP provider, and the extension balance is not enough, the call fails. And if the outbound call is established, but after a while, the extension balance is not enough to make long call, the call will be hung up automatically.
- **Billing for all inbound calls:** If this option is selected, when the extension receives inbound call from trunk/VoIP provider, and the extension balance is not enough, the call fails. And if the outbound call is established, but after a while, the extension balance is not enough to make long call, the call will be hung up automatically.
- **Enable extension to modify personal SIP password:** If this option is unselected, the extension can't modify his SIP password.
- **Enable extension audio recording:** If selected, the extension calls will be recorded as wav file
- **Enable extension video recording:** If selected, the extension video calls will be recorded as AVI video file
- **Record the call as dual tracks:** If selected, the PBX will record the caller and callee voice into dual tracks in the audio file, one track store the caller voice, another track store the callee ovice.
- **Extension is not allowed to delete recordings:** If selected, the extension cannot delete the recording files
- **Allow concurrent logins:** If this option is selected, the tenant can sign in Web Portal from multiple devices. If deselected, once tenant signs in, the login in another PC/mobile phone will be invalid
- **Allow display extension password in local:** If selected, when editing extension



in the "**Call Manager > Extension > General**", the extension password will be displayed

- **Allow extension to create temporary meeting:** If selected, the extensions of this tenant will be able to create temporary meetings via REST API

## 13.2 Office Hours

PortSIP PBX allows you to specify your office hours, after which the calls can be configured to be routed on the base of the office hours. For example, in the office hours, calls will be routed to your extension, and to voice mail when outside the office hours.

The screenshot shows a configuration page with tabs: General, Office Hours (selected), Storage, Mail Server, Music on hold, Event URL, and SMS. The Office Hours section includes a description: "Specify your office hours. Calls could be handled differently depending on whether they are received during or out of office hours". Below this are seven columns for days of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Each column has a "Configure" link. The Holidays section includes a description: "System will be switched to Out Of Office hours mode on these days and times". There is an "Add" button and a table with columns: Name, Date, Time, and Every Year. Below the table are navigation arrows (< and >). An "Apply" button is located at the bottom right of the page.

You can click "**Configure**" to set up the office hours for every weekday.

## Holidays

You can also set up the holidays by clicking the "**Add**" button in "**Holidays**" Section. When a call is made or received during the holiday, it will be treated according to the "**Out of office hours**" rule.

## 13.3 Storage

The "**Storage**" tab allows to adjust the storage quota for Recording files, Voice Mails and the Call Reports:

- **Disk quota (MB)** - The maximum disk quota allowed for this tenant

- **Recordings** - Current disk usage of recordings for this tenant
- **Voice Mails** - Current disk usage of voice mails for this tenant

## 13.4 Mail Server

To enable email notifications with PortSIP PBX, the SMTP details must be configured by going to "**Profile > Mail Server**".

If you are using the Google SMTP server, please make sure that you have "**less secure**" enabled for your Gmail account. Please refer to below links for more details:

[Less secure apps & your Google Account](#)

You also need to select SSL or TLS security protocol if you're using Google SMTP Server.

## 13.5 Music on Hold

"**Music on Hold**" could be leveraged to set the music on hold and the rules for playing.

- **Enable**: This box could be checked to enable "**Music on Hold**" so that when a call is on hold, music will be played to the hold caller. To enable this feature, at least one piece of music file must be specified.
- **Personalized Music on Hold**: Once this option is selected, music will be played for the hold caller in random. Default playing mode is "**Random music per day**".
- **Random music per call**: When Personalized Music on Hold is checked, user could specify check this option so that music on hold for each call may differ.
- **Random music per day**: Default playing mode for Personalized Music on Hold.
- **Music on Hold**: Music could be uploaded here by clicking "..." button to navigate the desired music files. To enable "Music on Hold" feature, this field is mandatory. Only .WAV files supported currently.
  - **Music 1**:
  - .....
  - **Music 9**: More music files could be uploaded by using these fields to support on random music feature.

## 13.6 Event URL

### Event URL

By setting up Event URL, PortSIP PBX is able to send CDR (Call Detail Report) and Extension activity details to 3rd server by of HTTP request in POST method(Web Hook). The CDR is formatted in JSON. To setup, please go to “**Profile > Event URL**” of Web Portal.

### CDR Events

To send the CDR event to a 3rd server, below options should be provided:

**Authentication method:** The authentication method used when sending request to third-party server. Both HTTP Basic Authentication and HTTP Digest Authentication are supported by PortSIP PBX. If authentication is not necessary, please choose “None”.

- **Username:** Username used for authentication.
- **Password:** Password used for authentication.
- **CDR URL:** URL used for sending CDR to third-party server, e.g. <http://www.cdrserver.com/add.php>.

Once set, CDR will be sent as below:

```
{  
  
"answered_time":"1569567973",  
  
"call_id":"b3dKobNICwlOsjwylqD4A..",  
  
"call_status":"ANSWERED",  
  
"callee":"102",  
  
"callee_domain":"portsip.io",  
  
"caller":"101",  
  
"caller_display_name": "",  
  
"caller_domain":"portsip.io",
```

```
"did_cid":"","  
"direction":"ext",  
"ended_reason":"caller hangup",  
"ended_time":"1569567981",  
"fail_code":"0",  
"final_dest":"sip:102@192.168.0.16:7059",  
"outbound_caller_id":"","  
"related_callid1":"","  
"related_callid2":"","  
"ring_duration":"5",  
"ring_time":"1569567968",  
"start_time":"1569567968",  
"talk_duration":"8",  
"tenant_id":"229806676134465536",  
"tenant_name":"admin"}
```

Of the CDR messages sent, *call\_start\_time*, *call\_answered\_time*, *call\_ended\_time*, *target\_add\_time*, *target\_answered\_time* and *target\_ended\_time* are all formatted in UNIX time, which is a system for describing instants in time, defined as the number of seconds that have elapsed since 00:00:00 Coordinated Universal Time (UTC), Thursday, 1 January 1970. User needs to count the actual time with the timezone information.

## Extension Events

To send the Extension events to 3rd server, below options should be provided:

**Authentication method:** The authentication method used when sending request to third-party server. Both HTTP Basic Authentication and HTTP Digest Authentication are supported by

PortSIP PBX. If authentication is not necessary, please choose "**None**".

**Username:** Username used for authentication.

**Password:** Password used for authentication.

**Event URL:** URL used for sending events to third-party server, e.g.

<http://www.eventsserver.com/add.php>.

Once set, the extension events will be sent as below:

```
{  
  "event_type": "extension_registered",  
  "tenant_id": "admin",  
  "extension_number": "101",  
  "source_ip": "192.168.0.98",  
  "time": 1489482652,  
  "domain": "sip.portsip.net"  
}
```

## 13.8 Rebranding

The PortSIP PBX allows you customize and rebrand it.

Click the menu "**Profile**" and choose the "**Rebranding**" tab, in this page, it will allows you enter the brand name, company name and upload logo file, you can simply have your own PBX.

Each Tenant can customize the PBX with his own brand name, logo.

If the tenant wish to display his own brand information, should open the Web Portal as this way:

<http://192.168.0.16:8888/login?tenantname=test>

In above link, the 192.168.0.16 is the PBX IP, the parameter tenantname is use for specify the

tenant name, in case is for "test" tenant.

## Chapter 14. REST API

PortSIP PBX offers the rich REST APIs. It allows you to implement your own web management for the PBX rather than the PBX itself, and enables you to easily integrate the PortSIP PBX with other system.

You can access the [REST API user guide](#) to learn more.

**Note:** The PortSIP PBX Web Portal is built based on REST APIs.

### Calls related REST API

**/api/extensions/hold** - Allows use the REST API to hold a existing call by given extension number or by given extension number and call session ID.

**/api/extensions/refer** - Allows use the REST API to refer the existing call by give extension number or by given extension number and call session ID.

**/api/extensions/attended\_refer** - Allows use the REST API to attended refer the existing call by give extension number or by given extension number and call session ID.

**/api/extensions/sessions** - Allows use REST API to obtain all existing calls information by given extension number.

**/api/call\_sessions/create** - Initialize a call by given caller and callee number, the caller and callee will receive the incoming call, after answered, the call will be connected.

### Rewrite outbound caller ID

The outbound caller ID also known as CLI (Calling Line Identification), represents the phone number of the calling (A) party in a phone call. It can be the full phone number or just a partial representation (say, the last 4 digits) depending on the carrier, country and frame of mind of the switch jockey.

PortSIP PBX allows set the outbound caller ID when make outbound call - just add a SIP header into the INVITE message.

## Example

If added X-Outbound-Cli SIP header to the INVITE message and make call to PBX, once the PBX received call from client app, the PBX will rewrite INVITE message before send it to the trunk.

```
X-Outbound-Cli: rewrite-from=123
```

Above header will cause the PBX rewrite the username of the From header to 123 when sending INVITE to the trunk.

```
X-Outbound-Cli: rewrite-pai=456
```

Above header will cause the PBX add "**P-Asserted-Identity**" SIP header and set the username to 456 when sending INVITE to the trunk.

```
X-Outbound-Cli: rewrite-rpi=789
```

Above header will cause the PBX add "**Remote-Party-ID**" SIP header and set the username to 789 when sending INVITE to the trunk.

If you would like to rewrite above headers only on specify trunk, you can also add below parameter.

```
X-Outbound-Cli: rewrite-from=123;trunk-name:abc
```

Above header will cause the PBX rewrite the from header if the call is send to the trunk which named "**abc**"; If no "**trunk-name**" parameter, the PBX will rewrite INVITE message on all trunks.

## Chapter 15. WebSocket Publisher

PortSIP PBX provides the Pub/Sub mechanism which bases on the WebSocket, the user is able to create the WebSocket in any programming languages to subscribe to the PBX events, once the subscribed events occur, PortSIP PBX will push the event message to subscriber automatically, the message is in the JSON format.

PortSIP PBX provides below topics and keys for the Pub/Sub.

## extension\_events

All extension related event message will be published by **extension\_events** topic, it includes below message keys.

```
extension_register: extension registered to PBX or un-register from the PBX.
call_hold: call was held.
call_unhold: call has been resumed from held.
call_start: call starting.
call_established: the call was answered and successfully connected.
call_ended: call is ended.
call_noanswer: call is no answer.
call_reroute: the call was re-routed to another target.
call_fail: call is failed.
target_add: start call to a target. For example, extension 101 is registered to PBX from an IP Phone and an App, when the call is made to extension 101, the call will be routed to the App.
target_ringing: the called target is ringing.
target_noanswer: there no answer from the called target.
target_fail: call failed from the called target. For example, the App / IP Phone rejected the call.
target_ended: call is ended from the called target. For example, the App / IP Phone hangs up the call.
```

## cdr\_events

Once a call is ended, the CDR of this call will be push to the subscribers, the message topic is: **cdr\_events**, the message key is below.

```
call_cdr: once a call is ended, the CDR will be packed in JSON format and push to subscriber.
```

## queue\_events

Once the queue status is changed, for example, the caller who in the queue was hangup the call, or the caller who is in the queue is answered by an agent.... the related status information will be pushed to the subscribers. The message topic is **queue\_events**, includes below message key.

```
queue_status: if the queue status changed, the information will be packed into JSON message and push to subscriber.
```

## trunk\_events

Once a trunk state is changed, for example, the PBX successfully registered to a Trunk, or register to the Trunk is fails, or the registration is lost from a trunk, connection timeout, PortSIP



PBX will push the message information to the subscribers, the message topic is **trunk\_events**, the key is below.

```
trunk_connected  
  
trunk_disconnected
```

More details of the WebSocket Pub/Sb, please read this link [Going Real-Time with PortSIP PBX Pub/Sub](#).

## Chapter 16. Help

Skype ID: portsip, the name is "PortSIP PBX"

Email: [support@portsip.com](mailto:support@portsip.com)

## Chapter 17. Best Practices for Deployment

Sometimes a bad production deployment can ruin all the efforts you invested in a development process. This chapter aims to help you better understand how to deal with deployments in your scenario and provide some best practices for deployments.

### 17.1 Deploying PortSIP PBX in LAN

This is a simple but typical deployment mode, in which scenario the PortSIP PBX is deployed in LAN. Extensions from the same LAN will register to PBX and make calls to each other. With default settings, the SIP signaling and RTP streams (RTP packet for audio and video) are relayed by PBX.

In this deployment, when running the "**Setup Wizard**", in the step 1 you will need to enter the "**Private IPv4**" only.

### 17.2 Deploying PortSIP PBX in LAN and registering to public trunk

When the PBX is deployed in LAN, and yet it registers to a trunk that is located on Internet, the

caller can make call from landline/mobile phone to the extension of PBX, and the extension can make call to a landline/mobile phone number.

This scenario requires the PBX server has a public static IP. When running the "**Setup Wizard**", in the step 1 enter the "**Private IPv4**" and "**Public IPv4**". The public IPv4 is the static public IP of the PBX server.

## 17.3 Solve the self-signed certificates warning

After you completed the PBX setting up, if get the self-signed certificates warning in browser when you access PBX Web Portal by HTTPS or access the WebRTC client, please follow up below steps to solve it.

1. Purchase a Domain from the domain provider for your PBX, for example Godaddy.
2. Add the an A record in the Domain DNS zone, resolve the Domain to your PBX IP.
3. Purchase a certificate from the trust certificate provider, for example Digicert, Thawte, GeoTrust, usually you will have two files, one is certificate, another one is private key. **Note**, please check the certificates for Nginx.
4. Sign in the PortSIP PBX Web Portal.
5. Click left menu "**Home > Summary**", then click the "**Setup Wizard**", in the step 1, enter your domain for the "**Web Domain**", click **Next** button to complete the wizard.
6. Click the left menu "**Home > Call Manager > Domain and Transport**", if there has the TLS, WSS transport added, just delete the TLS and WSS transport.
7. Add the WSS and TLS transport with upload the purchased certificate files.
8. For Windows installation, restart the Windows Server directly.
9. For Linux installation, perform the below commands:

```
$ sudo docker exec -it portsip-pbx /bin/bash
$ supervisorctl stop nginx
$ supervisorctl stop gateway
$ supervisorctl start nginx
$ supervisorctl start gateway
```

After restarted, you can sign in PortSIP PBX Web Portal by URL <https://yourdomain.com:8887>

If you don't use trusted certificate files for the WSS transport, you will get the browser warning and blocked when you use WebRTC client.