USER GUIDE

V 9.4.6 LTS | Sep 18, 2018 | 2998-1202-16

# PortSIP® PBX User Guide

## 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 End User License Agreement for this product.

## Patent Information

The accompanying product may be protected by one or more PRC China and foreign patents and/or pending patent applications held by PortSIP Solutions, Inc.

## 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.

# Contents

# 1.Getting Started with PortSIP® PBX

This PortSIP solutions guide gets you through deployment of PortSIP PBX in Windows® environment. 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**) 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. An IP PBX is also referred to as a VoIP or SIP Server.

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 Trunking, you can connect existing phone lines to the IP 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 Windows infrastructures:

**A popular Linux distribution:**
**Redhat RHEL (64bit), CentOS 7 or higher(64bit), Debian 9 or higher(64bit), Ubuntu 14.04 or higher(64bit).**
**IPv4/IPv6**
**IPtables and Firewalld**

This document assumes that the Linux OS is already deployed and administrators of PortSIP PBX are allocated 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 7/8, Windows 10, Windows Server 2008 R2 with SP1, 2012 R2, 2016 R2)**
**IPv4/IPv6**
**Windows firewall**

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

# 1.3 Hardware and Software Dependencies

## OS Supported by PortSIP PBX includes:

**Linux Server:**

CentOS 7 or higher, 64bit; gcc/g++ 6.4 or higher

Ubuntu 16.04.4 or higher, 64bit; gcc/g++ 6.4 or higher

Debian 9.0 or higher, 64bit; gcc/g++ 6.4 or higher

**Windows Desktop:**

Windows 7, 8 and 10, 64-bit

**Windows Server:**

Windows 2008 R2 SP1, 2012 R2, 2016 R2, 64-bit

**Important: The OS must be up to date.**

## Cloud and Virtualization Environment Supported

To build high-availability communication solution to help clients reduce cost and improve communication performance, PortSIP PBX commits support on cloud services and have confirmed availability on following cloud and virtualization environment:

- VMware ESX 5.X and above.
- Linux HyperV
- Microsoft HyperV 2008 R2 and above
- Amazon AWS
- UCloud
- Alibaba Cloud
- Linode
- Digital Ocean
- Godaddy VPS and Cloud
- Tencent Cloud

## System performance depends on following key factors:

- Maximum simultaneous calls needed for PBX
- Maximum online users needed for PBX
- Recordings for calls
- Record audio only or both of audio, video
- Maximum online users for audio/video conferences on PBX
- Maximum IVR (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 or Internet Explorer
- 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 service.portsip.com on port 6881.
- A constant internet connection to stun.portsip.com and stun1.portsip.com on port 3478.
- A constant internet connection to stun4.l.google.com on port 3478.

## 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 management console for PortSIP PBX
- Easier management of IP phones and clients after IP address change for PBX
- Convenient access to HTTPS when accessing management console

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.

# 1.4 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 to obtain the support.

# 2.Installation of PortSIP® PBX

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

## 2.1 Downloading PortSIP PBX

The latest free version 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 unlimited extensions (users). If you require more simultaneous calls, please refer to License Section for more details.

You will get the installer after download completed.

## 2.2 Installing PortSIP PBX on Linux

### 2.2.1 Preparing the Linux Host Machine for Installation

Tasks that MUST be completed before installing PortSIP PBX.

1. 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.

2. **Install all available updates & service packs before installing PortSIP PBX**.

3. Do not install VPN software on your PortSIP PBX Server

4. Ensure that all power saving options for your System and Network adapters are disabled (by setting the system to High Performance).

5. Do not install TeamViewer VPN Option on the host machine.

6. PortSIP PBX must not be installed on a host which is a DNS or DHCP server.

7. Below ports must be permitted by your firewall:  
   UDP: 33000 – 65000, 5078  
   TCP: 8800 – 8900, 10080,10443  
   TCP: 6459, 5078, 5079

8. Make sure that below ports have not been used by other programs:  
   UDP: 33000 – 65000, 5078  
   TCP: 8800 – 8900, 10080,10443  
   TCP: 6459, 5078, 5079

## 2.2.2 Installing the PortSIP PBX

### Upgrade the PBX

If you already installed the PortSIP PBX 9.4.2 or higher, just use below command to perform the upgrades:

1. For CentOS and RHEL:

   *sudo rpm -Uvh portsip_pbx_xxx.rpm*

   *Note: the xxx is the version number, for example, 9.4.6*

   **IMPORTANT**: on CentOS / RHEL, if you upgraded from currently 9.4.2/9.4.3/9.4.5 to 9.4.6, you must perform below command after successfully upgraded:

   *sudo systemctl enable portsip-pbx.webrtcgw.service*

2. For Ubuntu and Debian:

   *sudo dpkg -i portsip_pbx_xxx.deb*

   *Note: the xxx is the version number, for example, 9.4.6*

### Upgrading from PortSIP PBX 9.4.0

In PortSIP PBX 9.4.0 for Linux, the product name is “portpbx”. From 9.4.2, PortSIP PBX for Linux has been renamed to “portsip-pbx”. Therefore, if you have installed V9.4.0 and need to upgrade to a newer version, please follow below steps:

1. Uninstalling the 9.4.0

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

2. After uninstalled, delete below folders manually:

   *sudo rm -r /var/lib/portpbx*

   *sudo rm -r /opt/portsip/pbx*

3. Now you can install the newer version by following steps as described below.

### Install a fresh PBX

To install PortSIP PBX on Linux, you only need to perform below command, which will guide you through the installation process.

1. For CentOS and RHEL:

   Step1. Ensure your Linux has been installed the uuid, if doesn’t installed yet, perform below command:

   *sudo yum install uuid*

Then start to install PortSIP PBX:

*sudo rpm -ivh   portsip_pbx_xxx.rpm*

2. For Ubuntu and Debian:

*sudo apt-get install uuid*

Then start to install PortSIP PBX:

*sudo dpkg -i portsip_pbx_xxx.deb*

The installer will determine the dependencies of the PortSIP PBX, you have to follow the prompting message to install all required dependencies.

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

If you need to uninstall the PortSIP PBX, for CentOS and RHEL, please perform:

*sudo rpm -e portsip-pbx*

For Debian and Ubuntu:

*sudo dpkg -P portsip-pbx*

In order to fully delete the folders and files, please perform below commands after uninstalled:

*sudo rm -r /var/lib/portpbx*

*sudo rm -r /opt/portsip/pbx*

**Note 1:**

If you got the error like "/usr/lib64/libstdc++.so.6: version `GLIBCXX_3.4.21' not found", this is mean the gcc/g++ version is old, you have to update to newer gcc/g++.

**Note 2:**

If you got the error likes below:

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

Please follow below steps:

1. sudo yum list "compat-libstdc*"

2. I will output:

   ```
   Available Packages
   compat-libstdc++-33.i686

   compat-libstdc++-33.x86_64
   ```

3. Now perform below commands:

   ```
   sudo yum install compat-libstdc++-33.i686
   sudo yum install compat-libstdc++-33.x86_64
   ```

If you got error likes below:

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

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

Please perform below commands:

```
sudo yum install libxml2

sudo yum install libxml2-devel

sudo yum install zlib

sudo yum install zlib-devel
```

### 2.2.3 Configuring Linux Firewall Rules

After successful installation of PortSIP PBX, you must setup the Linux Firewall Rules to enable PortSIP PBX working properly.

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: **33000 - 65000.** These ports are used for the RTP sessions.

TCP: **6459, 5078, 5079, 8800 – 8900, 10080, 10443**. These ports are used for the Server control and WebRTC Gateway transport.

UDP: **5060, 5078.** This is the default UDP transport for SIP communications (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 firewall.

Assume you have added a TCP transport on port 5061, you must open TCP port 5061 in your firewall.

Assume you have added a WS transport on port 5065, you must open TCP port 5065 in your firewall.

Assume you have added a WSS transport on port 5067, you must open TCP port 5067 in your firewall.

Assume you have added a UDP transport on port 5068, you must open UDP port 5068 in your firewall.

# 2.3 Installing PortSIP PBX on Windows

## 2.3.1 Preparing the Windows Host Machine for Installation

Tasks that MUST be completed before installing PortSIP PBX.

1. 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, please assign static IP address for public network.

2. **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.

3. Antivirus Software should not scan the following directories to avoid complications and write access delays: *C:\Program Files\PortSIP*

4. Do not install VPN software on your PortSIP PBX Server

5. Ensure the "Windows Firewall" service has been started.

6. Ensure that all power saving options for your System and Network adapters are disabled (by setting the system to High Performance).

7. Do not install TeamViewer VPN Option on the host machine.

8. Disable Bluetooth adapters if it is a Windows client PC.

9. 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.

10. Below ports must be permitted by your firewall:  
UDP: 33000 – 65000, 5078  
TCP: 8800 – 8900, 10080,10443  
TCP: 6459, 5078, 5079

11. Make sure that below ports have not been used by other programs:  
UDP: 33000 – 65000, 5078  
TCP: 8800 – 8900, 10080,10443  
TCP: 6459, 5078, 5079

12. Ensure your Windows Firewall is enabled

## 2.3.2 Installing the PortSIP PBX

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).

## 2.3.3 Configuring Windows Firewall Rules

After successful installation of PortSIP PBX, you must setup the Windows Firewall Rules to enable PortSIP PBX working properly.

To locate the installation path for PortSIP PBX, click "**Allow another app" -> "Browse".** Below applications for PBX should be permitted in the firewall:

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

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

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

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

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

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

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

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

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

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

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: **33000-65000.** These ports are used for the RTP sessions.

TCP: **6459, 5078, 5079, 8800 – 8900, 10080, 10443**. These ports are used for the Server control and WebRTC Gateway transport.

UDP: **5060, 5078.** This is the default UDP transport for SIP communications (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 firewall.

Assume you have added a TCP transport on port 5061, you must open TCP port 5061 in your firewall.

Assume you have added a WS transport on port 5065, you must open TCP port 5065 in your firewall.

Assume you have added a WSS transport on port 5067, you must open TCP port 5067 in your firewall.

Assume you have added a UDP transport on port 5068, you must open UDP port 5068 in your 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 Avoid HTTPS Certificate Security Warnings

PortSIP PBX listens on 8888 port for providing HTTP portal to access the PBX Management Console.

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 Management Console.

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 don't use IE.

For HTTPS portal default usage of the self-signed SSL certificate will cause the browser popup 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:

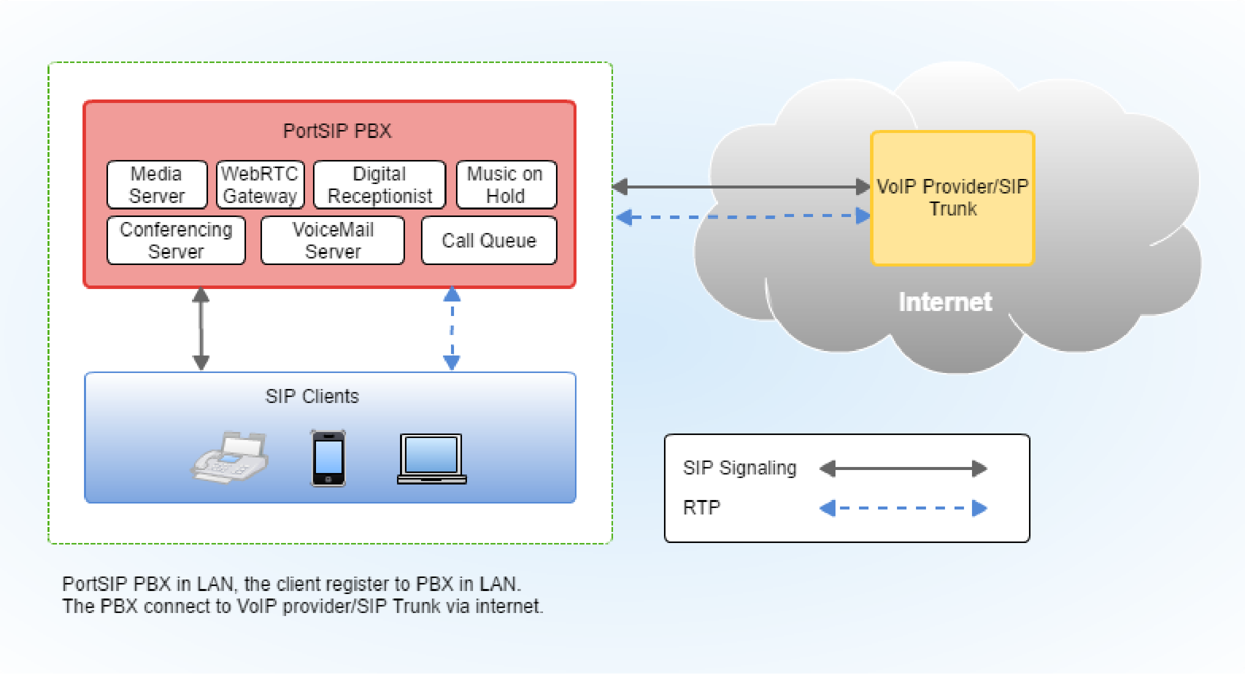
1. Go to Thawte or Versign or other certificate providers to purchase a SSL certificate. Save the private key as **portsip.key**
2. After you have obtained the SSL certificate, rename the certificate to **portsip.crt**
3. On Linux, Copy the **portsip.crt** and **portsip.key** to PortSIP PBX installed path: */opt/portsip/pbx/bin* to replace the existing **portsip.crt** and **portsip.key**.
4. On Windows copy the **portsip.crt** and **portsip.key** to PortSIP PBX installed path: C:/Program Files/PortSIP/PBX/bin to replace the existing **portsip.crt** and **portsip.key**.
5. Now you can sign in PortSIP PBX Management Console by URL https://yourpbx.com:8887

**Note**: You may also obtain SSL certificate from Let's Encrypt for free.

# 3.Deployment of PortSIP® PBX

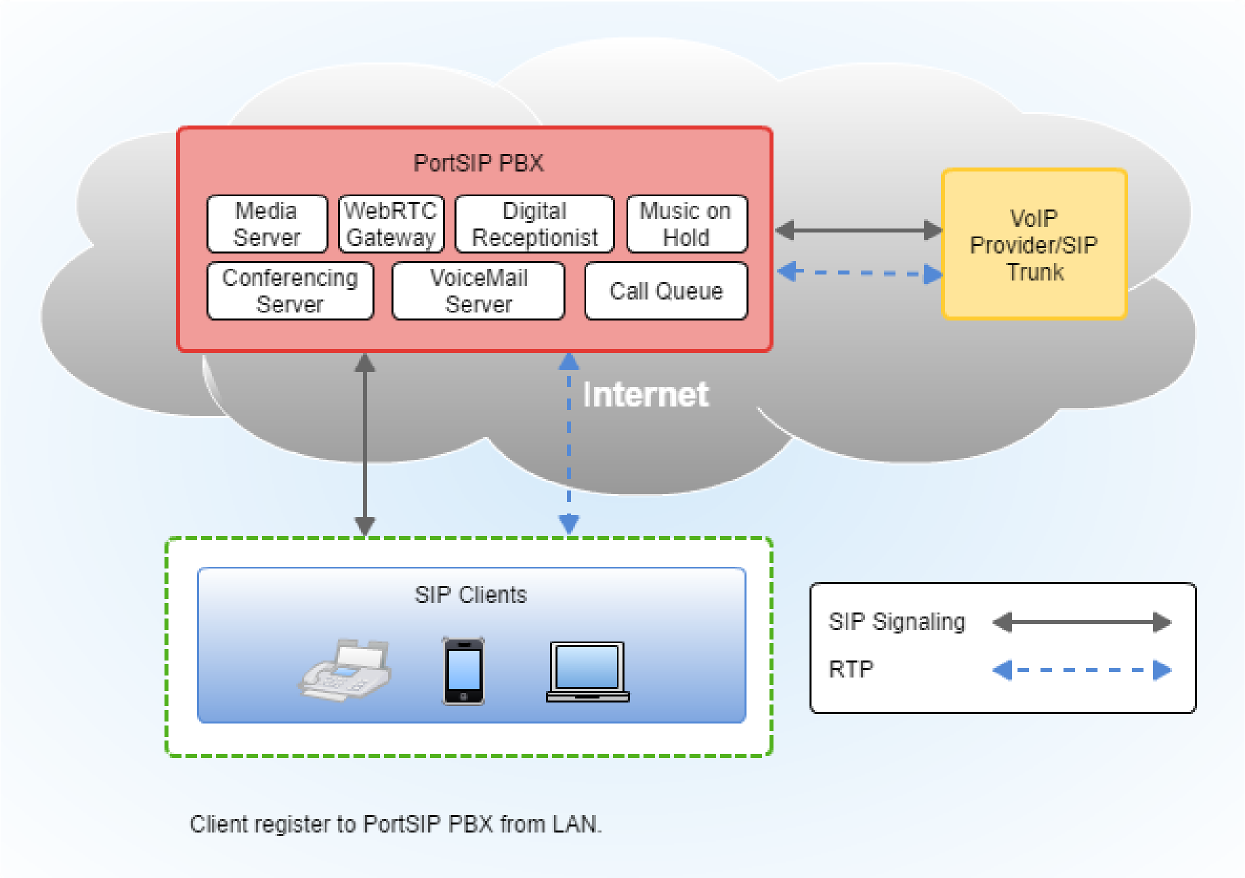
## 3.1 Architecture of PortSIP PBX

**Figure 1: a unified architecture of the PortSIP PBX in LAN**



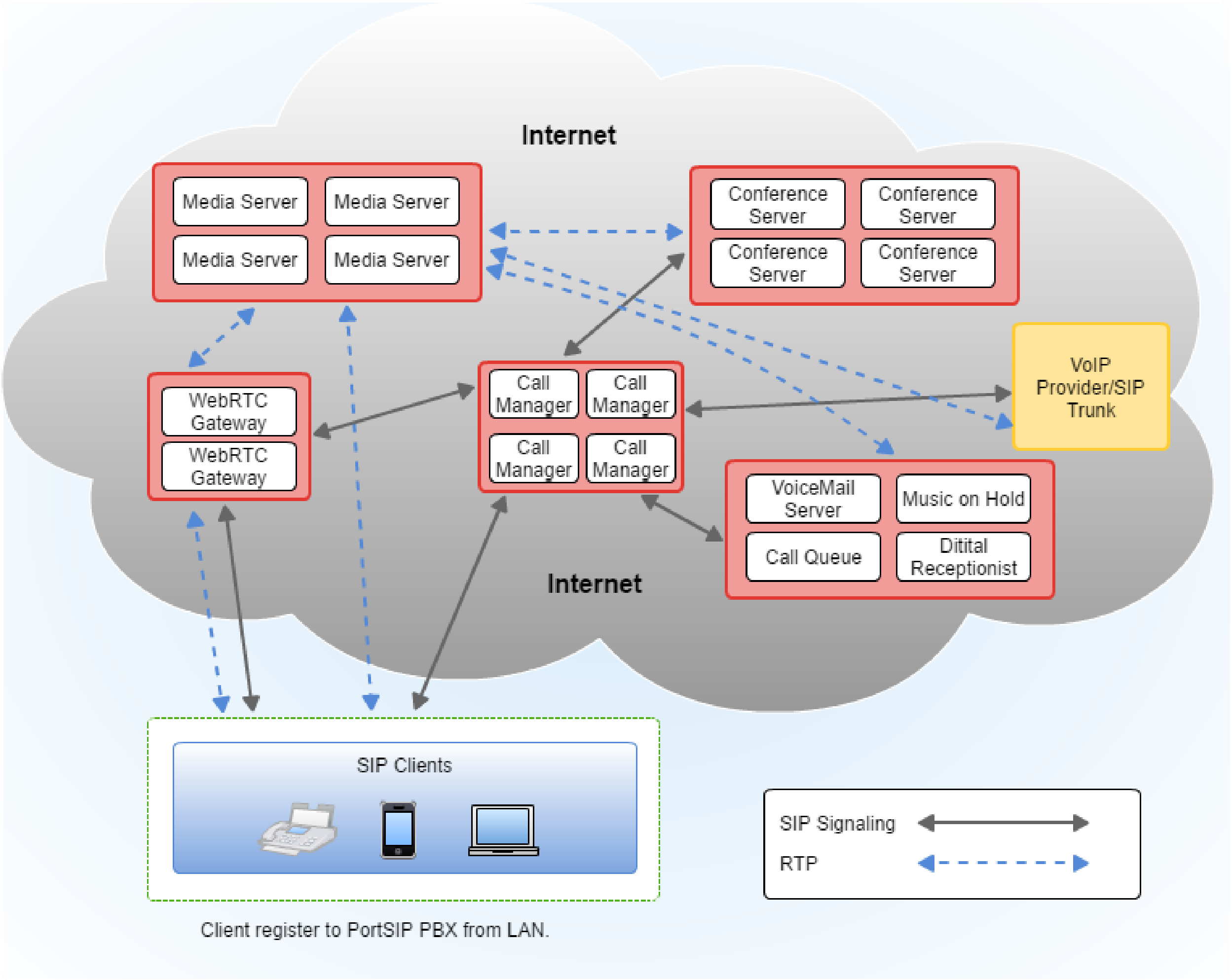
In **Figure 1**, the PBX running in LAN, users (extensions) register to PortSIP PBX in LAN. Users (extensions) who could make & receive calls with other users (extensions) are also able to place and receive calls with PSTN number via VoIP provider/SIP trunk.

**Figure 2: a unified architecture of the PortSIP PBX on Internet**



In **Figure 2**, users (extensions) register to PortSIP PBX (deployed on internet) from LAN. User (extension) who can make and receive calls with other users (extensions) is also able to place and receive calls with PSTN number via VoIP provider/SIP trunk.

**Figure 3: a unified architecture of the PortSIP PBX with Large-Scale deployment**



In **Figure 3**, the Call Manager of PortSIP PBX is deployed on a separate server on Internet; The Media Server, Conference Server, WebRTC Gateway, Voicemail, Virtual Receptionist, Call Queue, WebRTC Gateway and Music on Hold servers are deployed on other separated servers as cluster.

The SIP clients could be registered to the Call Manager of PortSIP PBX, and then make a call. Once the call is established, the RTP will be replayed by separated Media servers.

With Large-Scale deployment, it’s easy for your PortSIP PBX to handle more than 10,000 simultaneous calls. The high scalability also enables to expand simultaneous calls support with increased servers.

# 3.2 Deployment Modes of PortSIP PBX

PortSIP PBX could be deployed in wide range of scenarios. It’s supported in LAN and internet, and to major cloud platforms such as AZURE, AWS, Linode, Digital Ocean and Godaddy Cloud.

After successful installation of the PortSIP PBX with setup wizard, you just need a few clicks to get it works.

## 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.

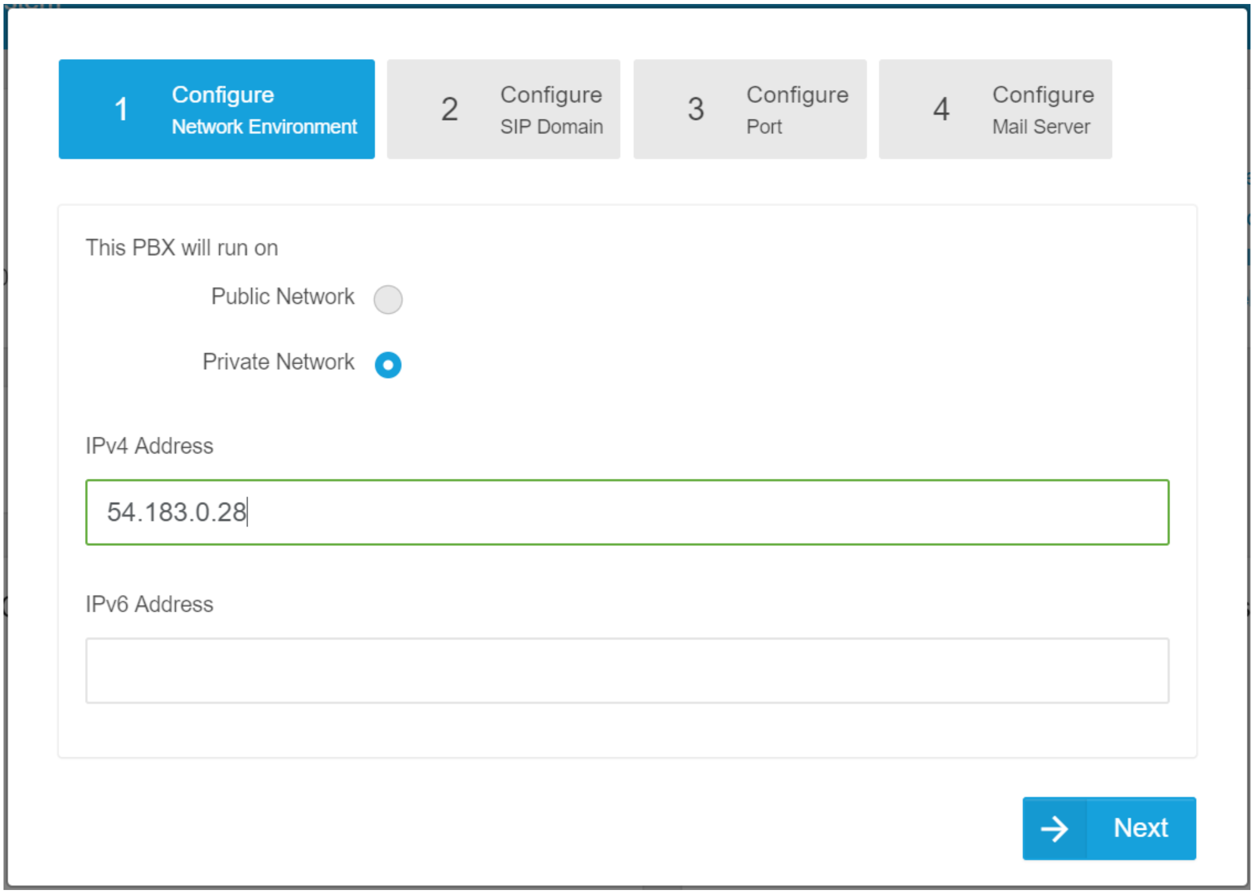
PortSIP PBX listens on 8888 port for providing HTTP portal to access the PBX Management Console, and listens on 8887 port for providing HTTPS portal. More details please read the 2.4 section.

1. Access the PBX Management Console by open http://pbxserverip:8888. IE is not supported.
2. Enter the username and password (defaulted as”**admin**” for both) and click the “**Sign in**” button. Note that the username and password are both case sensitive. The “**Setup Wizard**” will be displayed which will guide you through the initial configuration step by step.

You may change the password for "admin" by selecting the menu **"Profile" >** "**General**" in PortSIP PBX Management Console.

## Mode 1: Deploy PortSIP PBX in LAN

Assume that the PortSIP PBX is deployed in LAN with internet connection, the server/PC has installed the PBX and the private IP is *192.168.0.28.* The PBX is connected to SIP trunk or VoIP provider, and then users not only can make & receive calls in LAN, but also make & receive external calls with PSTN number and mobile users via services provided by preconfigured SIP trunk or VoIP provider.



This PBX will run on

Public Network ○

Private Network ●

IPv4 Address

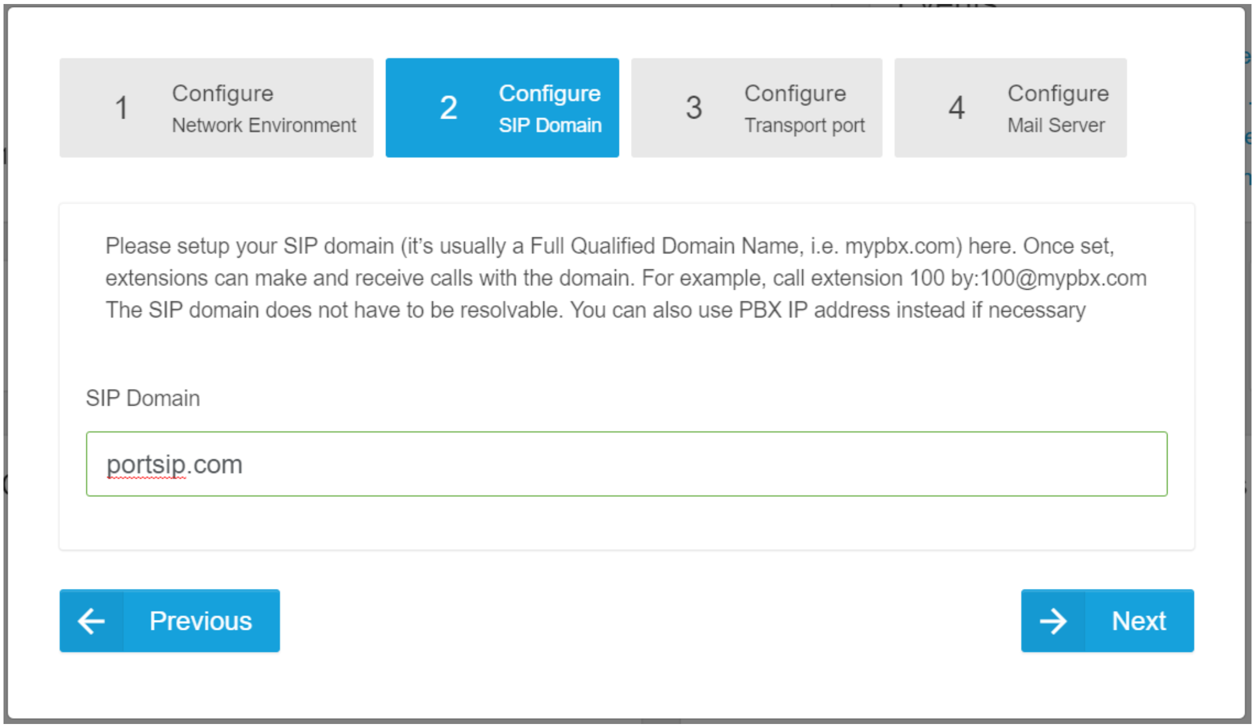
54.183.0.28

IPv6 Address

**Step 1:** In Configuration Wizard, choose “**private network”** for “**This PBX is run on**”**,** and enter the private IP ***192.168.0.28***. Both IPv4 and IPv6 are supported by PBX. In this case, we’ll use IPv4 as example.

**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 address for PBX. It is required when a SIP client or SIP IP phone registers to PortSIP PBX.



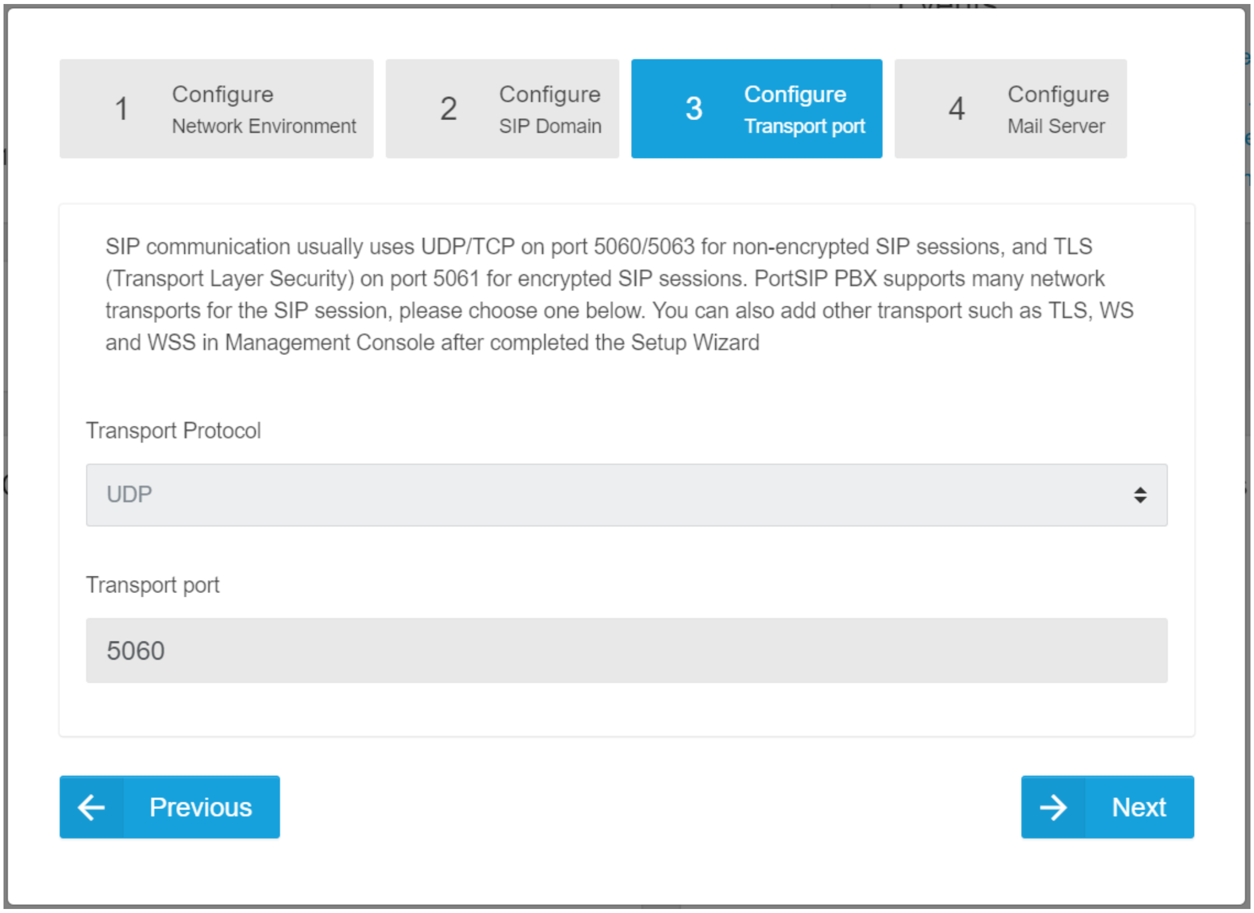
Please setup your SIP domain (it's usually a Full Qualified Domain Name, i.e. mypbx.com) here. Once set, extensions can make and receive calls with the domain. For example, call extension 100 by:100@mypbx.com The SIP domain does not have to be resolvable. You can also use PBX IP address instead if necessary

SIP Domain: portsip.com

**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 for PBX authentication only.**

After set the domain, the extension SIP account will be sip:xxx@domain. Assume we set the domain as ***portsip.com***, the extension 101 SIP address would be: sip:101@ portsip.com.

If you don't want to use domain, enter the private IP (for example: 192.168.0.28) of the PC/Server which has installed the PortSIP PBX instead of the domain(FQDN). In this case the extension 101 SIP address would be: sip:101@192.168.0.28.



SIP communication usually uses UDP/TCP on port 5060/5063 for non-encrypted SIP sessions, and TLS (Transport Layer Security) on port 5061 for encrypted SIP sessions. PortSIP PBX supports many network transports for the SIP session, please choose one below. You can also add other transport such as TLS, WS and WSS in Management Console after completed the Setup Wizard

Transport Protocol: UDP

Transport port: 5060

**Step 3:** You can set transport layer protocol for the SIP here, with the default transport UDP on port 5060.

***Note**: You can add more transports in PortSIP PBX Management Console after this Wizard.*

**Step 4:** Setup mail server. You may setup the 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 when necessary.***

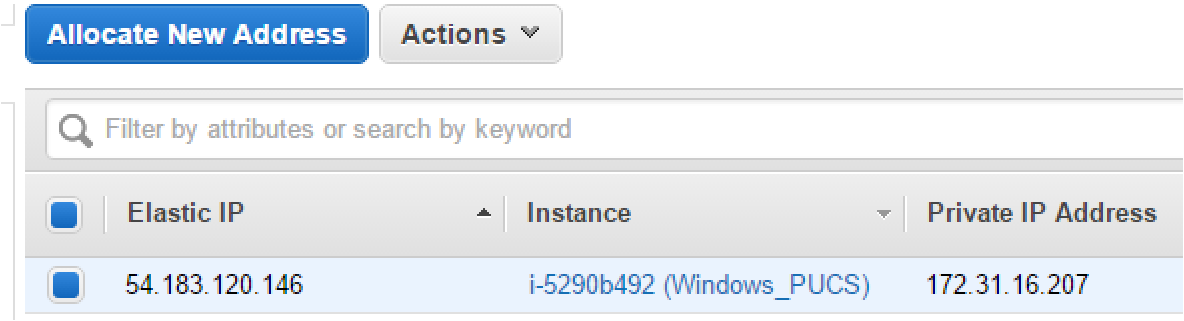
By clicking the “**Finish**” button, you have now completed the initial configuration of PortSIP PBX. You will be redirected to Management Console.

# Mode 2: Deploy PortSIP PBX on AWS

Amazon Web Services (AWS) is a popular cloud services platform that allows you to deploy PortSIP PBX on Cloud.

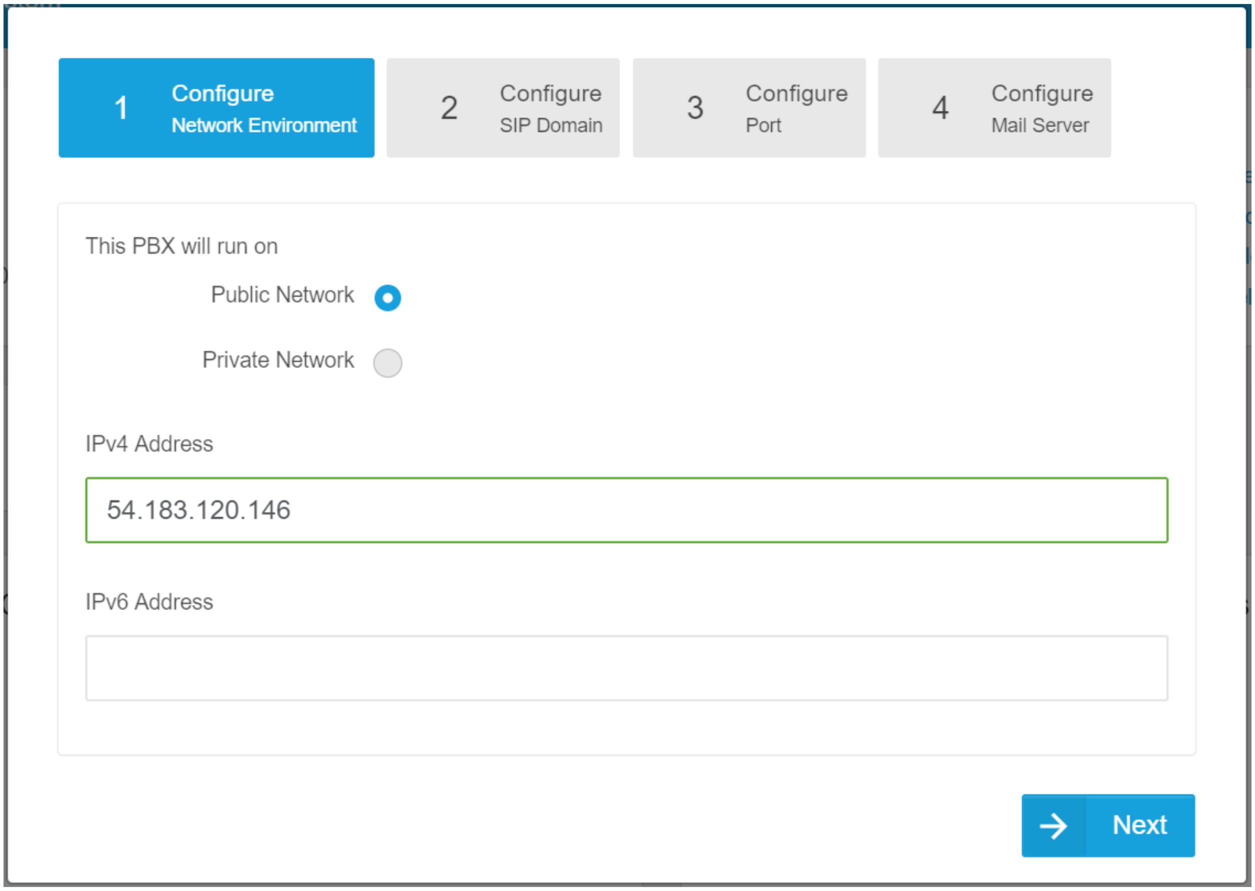
When deploying the PortSIP PBX on AWS, user could make or answer calls through PortSIP PBX with other users through internet, and make or answer external calls via SIP trunk or VoIP provider.

Please refer to Creating an AWS account if you do not have the AWS account.



| Elastic IP | Instance | Private IP Address |
|---|---|---|
| 54.183.120.146 | i-5290b492 (Windows_PUCS) | 172.31.16.207 |

**Step 1:** On the left bar of AWS EC2 Management Console, choose “**Elastic IPs**”, you will see the “**Elastic IP**”, please write it down for future use. If the “**Elastic IPs**” does not exist, you should click “**Allocate New Address**”, and associate the Elastic IP to your instance.



This PBX will run on

Public Network ●

Private Network ○

IPv4 Address

54.183.120.146

IPv6 Address

**Step 2:** In the step 1 of Configuration Wizard in PortSIP PBX, choose "**This PBX run on**" as "**public network**", enter the "**Elastic IP**" that you have in Step 1.

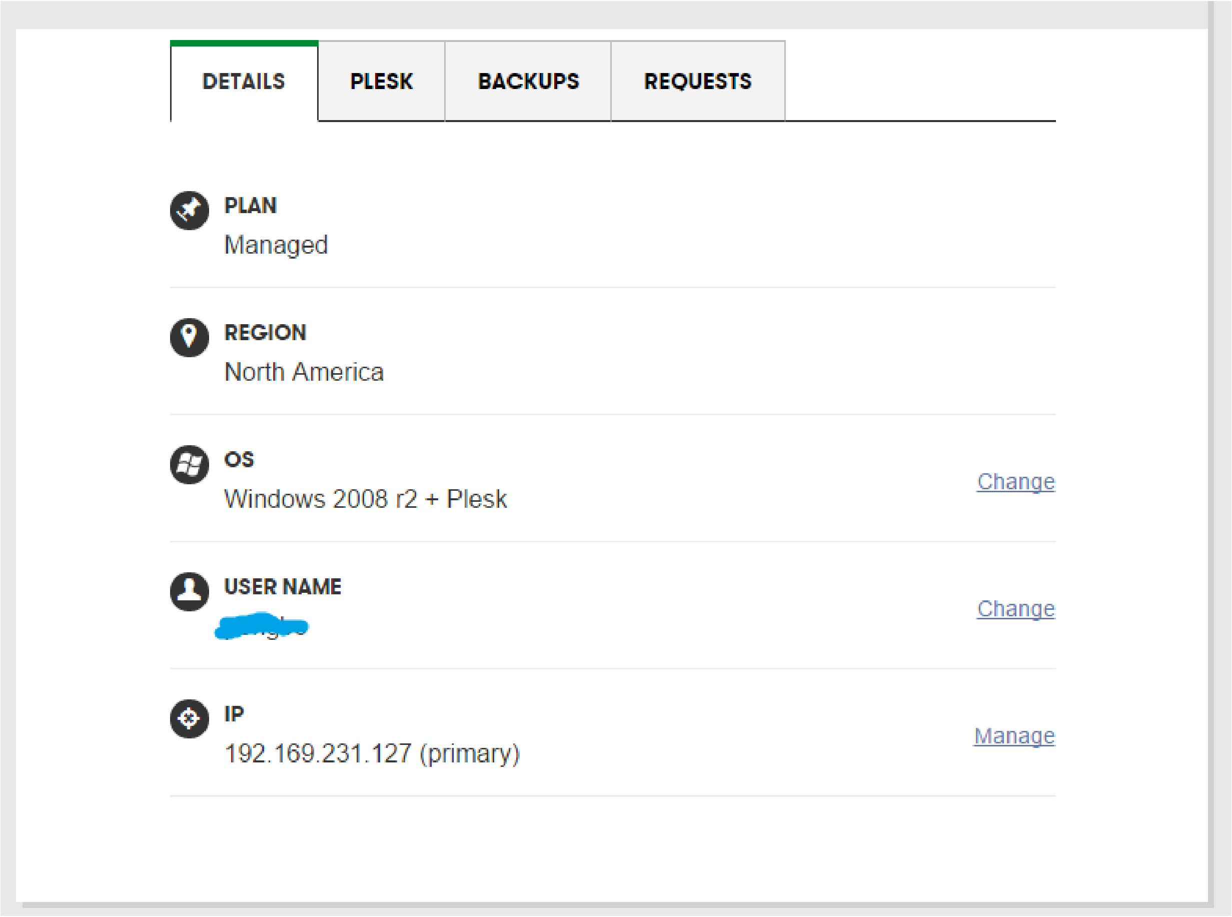
***Now remaining steps are same to the Mode 1.***

## Mode 3: Deploy PortSIP PBX on Virtual Private Server (VPS)

PortSIP PBX can be deployed on popular Virtual Private Server (VPS) and Dedicated Server.

When deploying the PortSIP PBX on VPS or Dedicated Server, user could make or answer calls through PortSIP PBX with other users via internet, and make or answer external calls with SIP trunk or VoIP provider.

We are using Godaddy VPS as an example. Please read this topic if you want to purchase the Godaddy VPS: Sign up Godaddy VPS.



PLAN
Managed

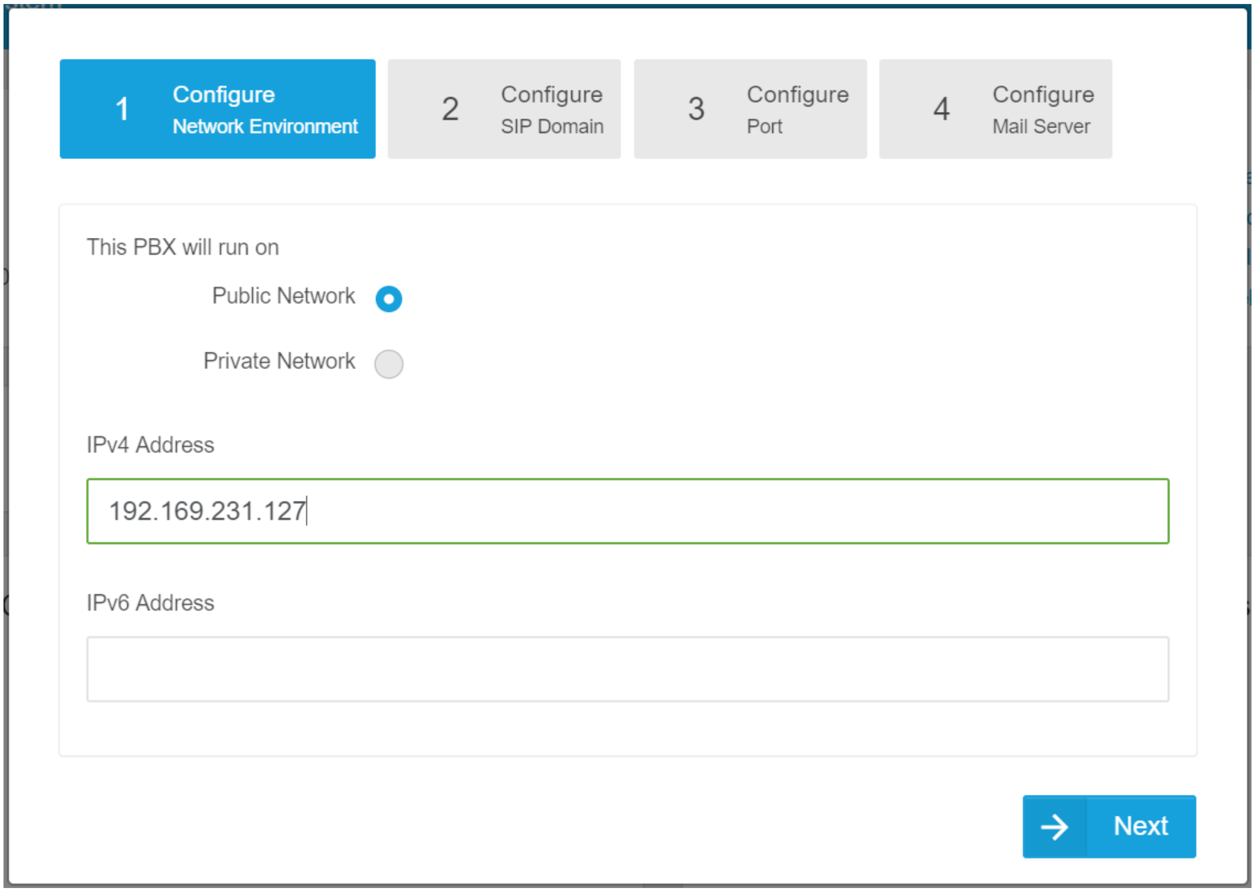
REGION
North America

OS
Windows 2008 r2 + Plesk

USER NAME
[redacted]

IP
192.169.231.127 (primary)

**Step 1:** In Godaddy VPS Management Console, click the “**Details**” tab, you will see the “**IP**” of VPS. Log it for future use.



This PBX will run on

Public Network ●

Private Network ○

IPv4 Address

192.169.231.127

IPv6 Address

**Step 2:** In the step 1 of Configuration Wizard in PortSIP PBX, choose “**This PBX will run on**” as “**public network**”, and then enter the “**IP**” that you have got in Step 1.

***Now remaining steps are same to the Mode 1.***

# Deploy PortSIP PBX in other scenarios

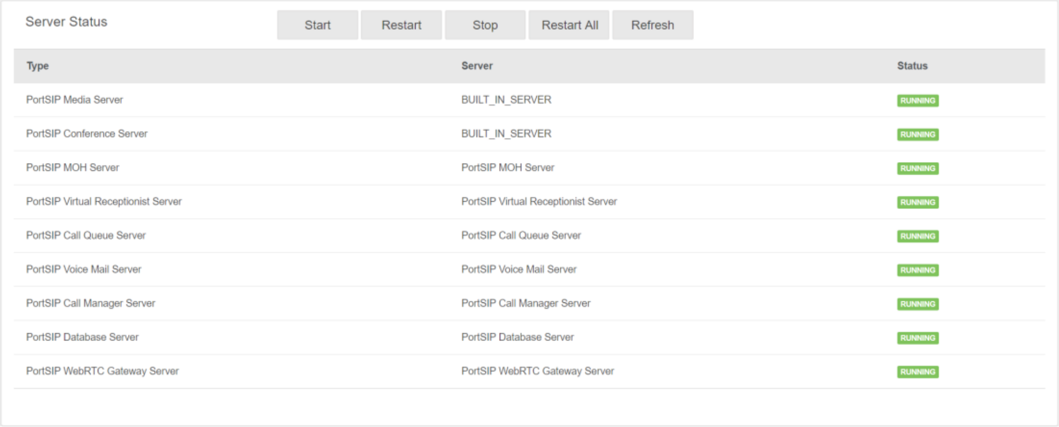
If you would like to deploy the PortSIP PBX in other scenarios which are not mentioned above, you will need to get the server IP address, and choose it run on internet or in LAN and follow the Configuration Wizard for deployment.

# 4. Administration of PortSIP PBX

After completing the Configuration Wizard, now you could manage the PortSIP PBX in the Management Console.

## 4.1 Service Status

### Service Status



| Type | Server | Status |
|---|---|---|
| PortSIP Media Server | BUILT_IN_SERVER | RUNNING |
| PortSIP Conference Server | BUILT_IN_SERVER | RUNNING |
| PortSIP MOH Server | PortSIP MOH Server | RUNNING |
| PortSIP Virtual Receptionist Server | PortSIP Virtual Receptionist Server | RUNNING |
| PortSIP Call Queue Server | PortSIP Call Queue Server | RUNNING |
| PortSIP Voice Mail Server | PortSIP Voice Mail Server | RUNNING |
| PortSIP Call Manager Server | PortSIP Call Manager Server | RUNNING |
| PortSIP Database Server | PortSIP Database Server | RUNNING |
| PortSIP WebRTC Gateway Server | PortSIP WebRTC Gateway Server | RUNNING |

You can go to “**Summary -> Service Status**” menu in the PortSIP PBX System Management Console to quickly view if all PortSIP PBX system services are working correctly.

You could use **Start**/**Stop** button to start/stop a stopped/running service.

A stopped service could be started by clicking “**Start**” button; or a running service could be restarted by clicking “**Restart**” button.

When there are multiple running services, you could click “**Restart all**” to restart all the services.

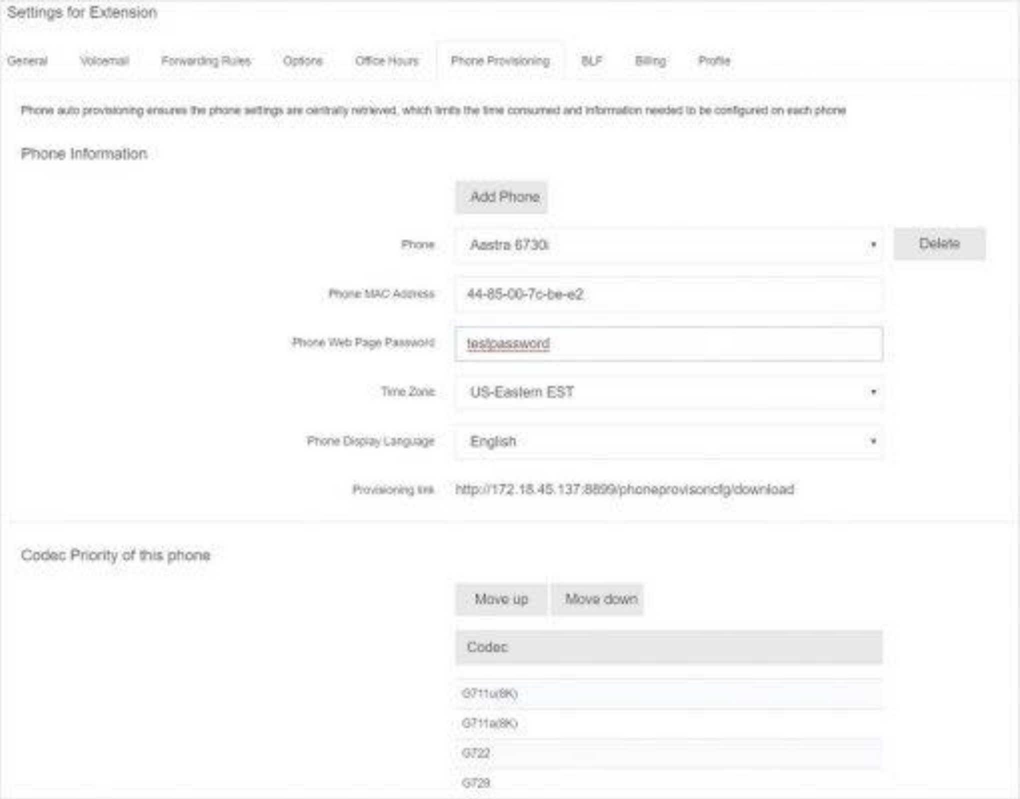
There may be delay for service status displayed on screen. You could click “**Refresh**” button to check for the latest status of service.

### System Extensions

PortSIP PBX defines services such as Virtual Receptionist (auto attendant), Conferencing, Fax, Call Queue, 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 “**Summary -> System Extensions**” menu in the PortSIP PBX System Management Console.

# 4.2 Phone Provisioning

## Phone Auto Provisioning Introduction



Settings for Extension

Phone auto provisioning ensures the phone settings are centrally retrieved, which limits the time consumed and information needed to be configured on each phone

Phone Information

Phone: Aastra 6730i

Phone MAC Address: 44-85-00-7c-be-e2

Phone Web Page Password: testpassword

Time Zone: US-Eastern EST

Phone Display Language: English

Provisioning link: http://172.18.45.137:8899/phoneprovisoncfg/download

Codec Priority of this phone

| Codec |
|---|
| G711u(8K) |
| G711a(8K) |
| G722 |
| G729 |

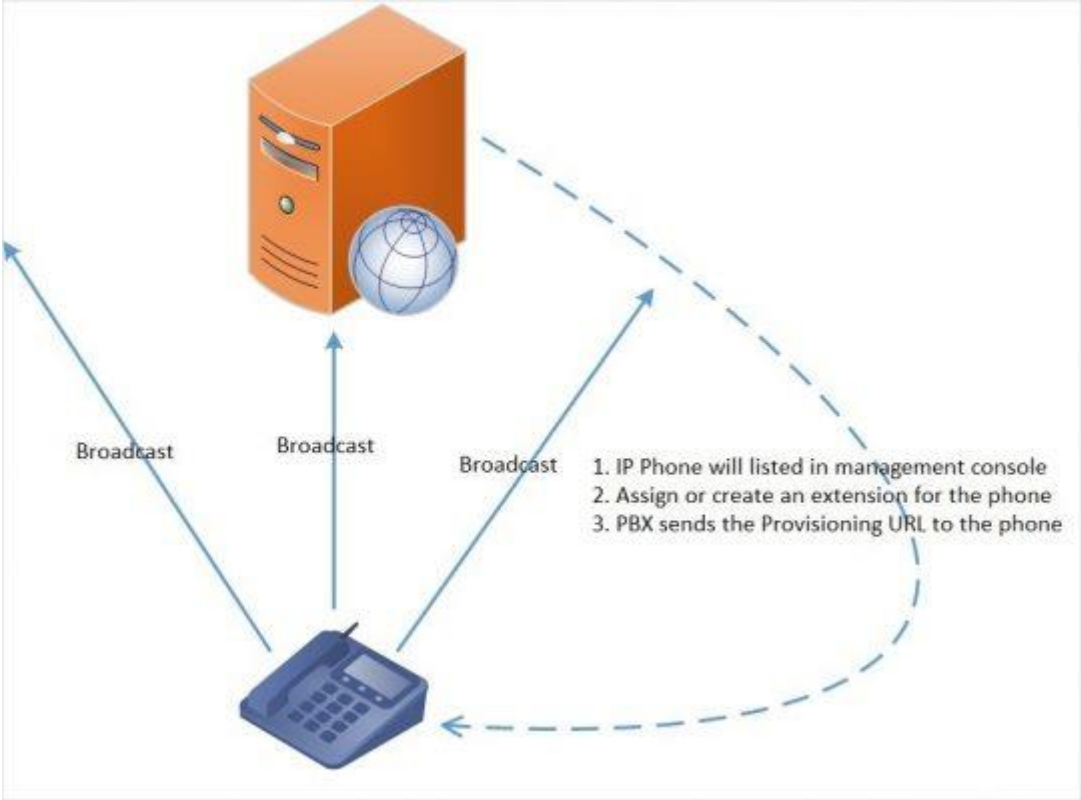
Once PortSIP PBX is installed, you can configure your IP phones and assign an extension to each phone. Phones can be configured one by one manually using their web interface, which is time consuming and leads to many errors; Or by using phone provisioning feature offered by PortSIP PBX, which makes it 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 Management Console 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 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 using Plug and Play (for local LAN)


Broadcast
Broadcast
Broadcast
1. IP Phone will listed in management console
2. Assign or create an extension for the phone
3. PBX sends the Provisioning URL to the phone

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

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 "**Phones**" tab in the PortSIP PBX Management Console as a new phone.
4. Assign the phone to an existing extension or create a new one.
5. Go to the extension's "**Phone Provisioning**" tab and specify other configuration settings for the phone.
6. Select "**Phone Display Language**" and "**Timezone**" for the phone.
7. Click "**OK**".
8. The phone will send a link to the configuration file with the settings you specified and configure itself.
9. The phone will apply the settings and connect to PortSIP PBX. The IP phone will be manageable from within the PortSIP PBX Management Console.

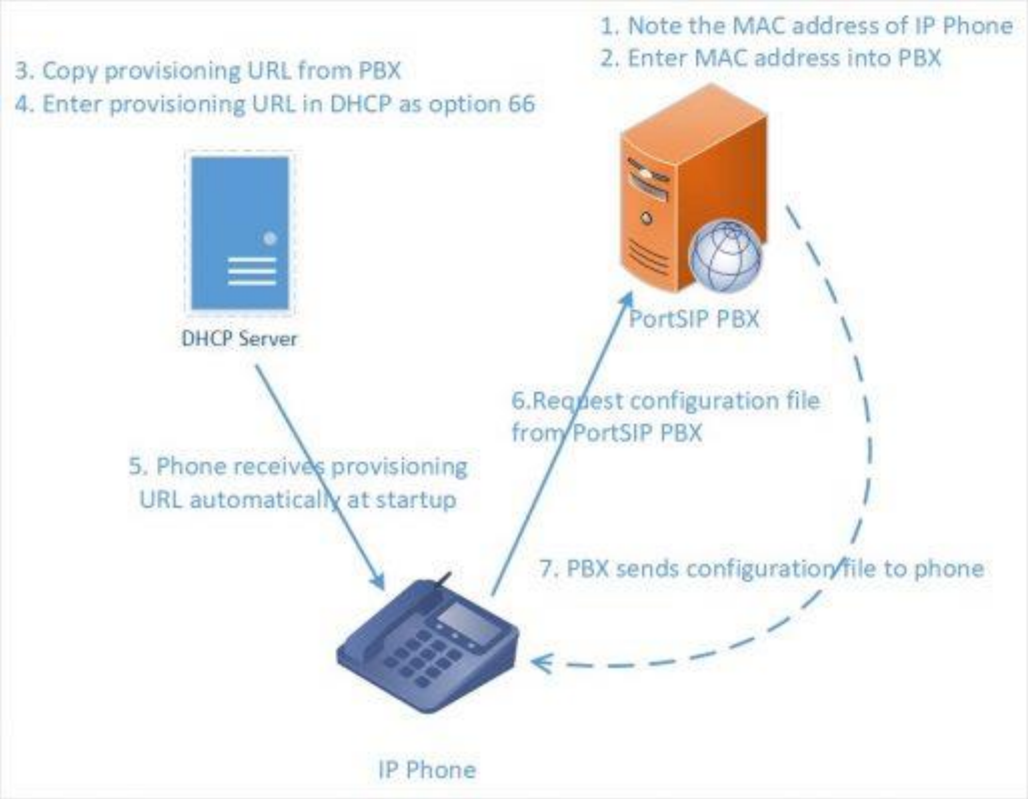
# Provisioning Phones using provisioning link manually

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 "**Phones**" tab in the PortSIP PBX Management Console, select "**Add Phone**."
2. Select the extension for which this phone is.
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. Copy the provisioning link.

7. Insert the provisioning link manually into the phones. You can find it in "**Phone Provisioning**" tab of extension configuration.

# Provisioning Legacy phones: Cisco, Polycom & Aastra


1. Note the MAC address of IP Phone
2. Enter MAC address into PBX
3. Copy provisioning URL from PBX
4. Enter provisioning URL in DHCP as option 66
DHCP Server
PortSIP PBX
6.Request configuration file from PortSIP PBX
5. Phone receives provisioning URL automatically at startup
7. PBX sends configuration file to phone
IP Phone

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. Leave "Phone Web Page Password" default.
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.

# 4.3 Managing Phones

PortSIP PBX provides an easy way to monitor and manage your phones and softphones throughout your network. The "**Phones**" tab in the PortSIP PBX Management Console 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

## 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.

## Provision Remote extensions

If you are adding phones that are installed remotely, i.e. on a remote network, you must:

1. Click “**Add Phone**” button from the “**Phones**” tab.
2. Select extension this phone will be used for.
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. Copy the provisioning link and insert to your IP phone manually.

## 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 will be used for.
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.

# 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:

1. 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. There is no need to reboot again afterwards.

# 4.4 Extensions management

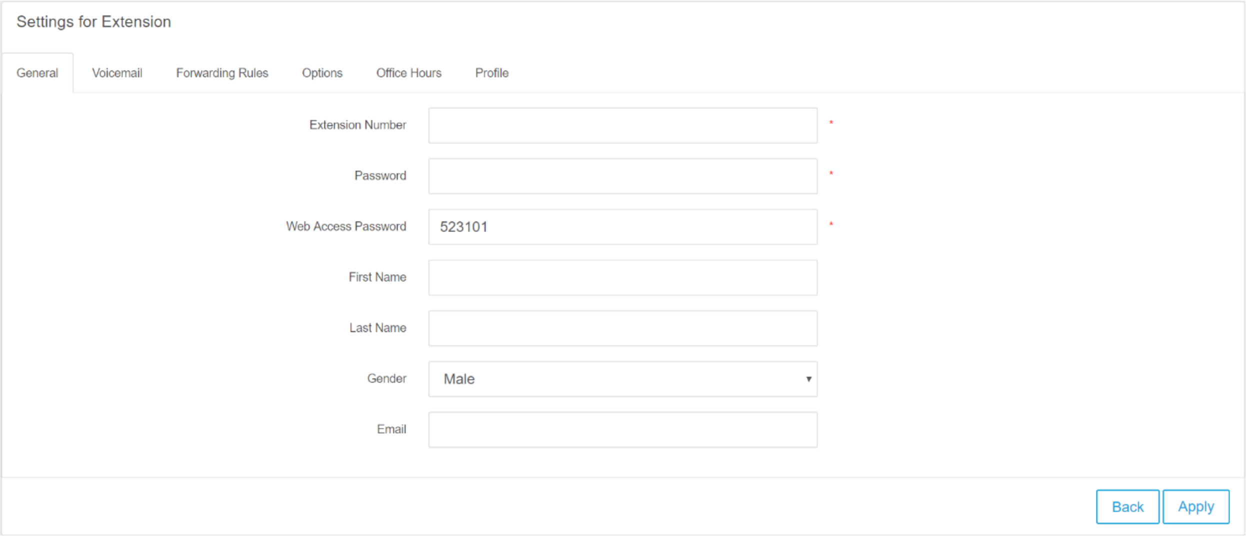
This section explains how to create and configure extensions in PortSIP PBX. There are multiple methods to create an extension.

● 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


Settings for Extension

Extension Number *

Password *

Web Access Password: 523101 *

First Name

Last Name

Gender: Male

Email

To configure an extension, click on "**Call Manager -> Extensions**" in the PortSIP PBX Management Console. 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 management pagel.

## 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 Management Console.

## 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; if the status is set to "Out of Office", you could forward it to their mobile. 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:

● Record audio calls – If this selection is checked, all calls for this extension will be recorded as wav file.

● Record video calls – If this selection is checked, all video calls for this extension will be recorded as AVI file.

●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 4.7.

● Enabled – If this selection is un-checked, the extension will be disabled.

●Allow Paging/Intercom – If this selection is checked, the extension will be allowed to make Paging/Intercom calls.

● Allow External Calls – If this selection is checked, the extension will be allowed to make call to external number via configured VoIP Provider/SIP Trunk.

● Allow Management Console Access – If this selection is checked, the extension will have the access to PBX Management Console.

## 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 13.1), the call 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.

# 4.5 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 default.

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 Management Console, select **Call Manager** > **Extension Groups**, and click **Add**. 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 **OK** button to complete the creation of group.

Once an extension group is granted the permission "**Allow Access to Management Console**", all users in this group could sign in PortSIP PBX Management Console. Assume the password for extension 101 is 101, the SIP domain name set in PBX system is portsip.com, and the extension 101 belongs to default group which has been granted with login permission to the system Management Console, extension 101 could login with below info:

Username: 101@portsip.com

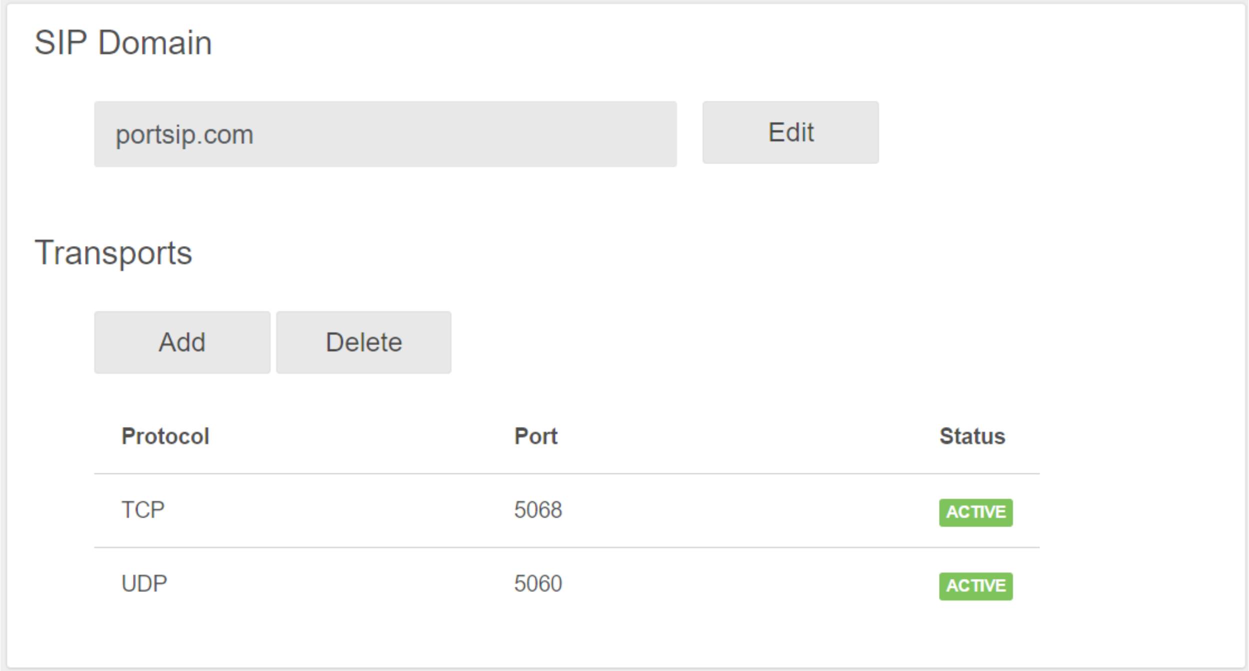
Password: the **web password** of extension 101

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

# 4.6 SIP Domain and Transport Management

## SIP Domain Management

The SIP domain is used during registration, 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.com**” or “**192.168.0.28**”.



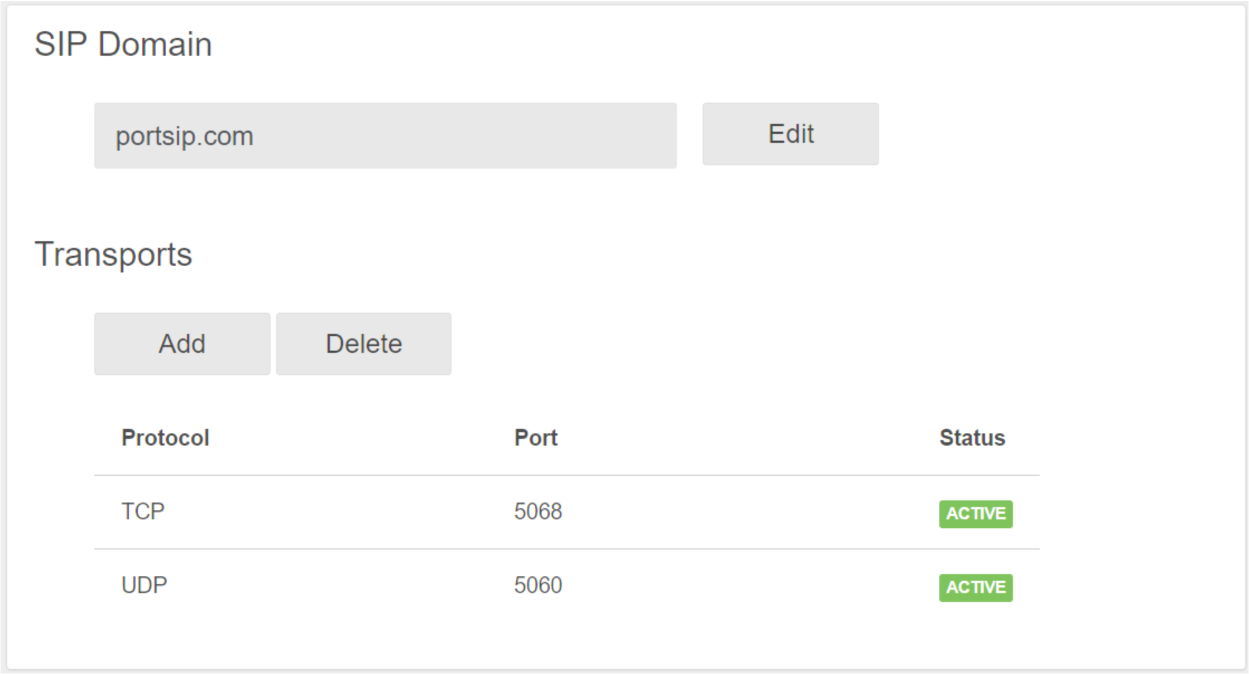
SIP Domain: portsip.com

| Protocol | Port | Status |
|---|---|---|
| TCP | 5068 | ACTIVE |
| UDP | 5060 | ACTIVE |

The SIP domain is configured within “**Setup Wizard**” when you first sign in Management Console. To modify a SIP domain, go to “**Call Manager > Domains and transports**”, and click “**Edit**” button to enter new SIP domain and save.

## SIP Transport Management

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



SIP Domain

portsip.com

Transports

| Protocol | Port | Status |
|---|---|---|
| TCP | 5068 | ACTIVE |
| UDP | 5060 | ACTIVE |

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

Note: only administrators 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:

1. 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.

2. Click the "**Apply**" button to add the transport.

## Add TLS/WSS transport

To add the TLS/WSS transport with self-signed certificate:

First of all, prepare the certificate files.

1. You have to generate the certificate files by yourself if you have not purchased certificates from a third-party certificate provider (or run **PortCertMaker.exe** in the installation path of PBX). Please download the certificate file tool from PortSIP website, enter your SIP domain. Once clicked "**Generate**" button, certificate files will be generated automatically.

2. The certificates include three files (assume your SIP domain is portsip.com):

   *domain_key_portsip.com.pem*

   *domain_cert_portsip.com.pem*

   *root_cert_portsip.com.pem*

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

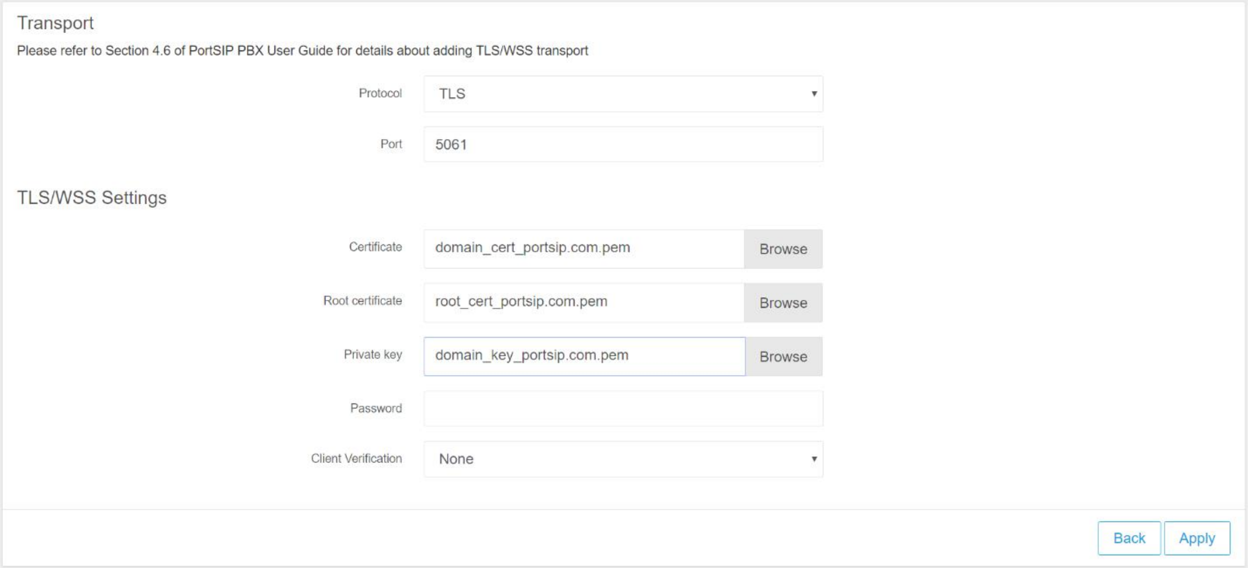
a. Generate the CSR file and private key file according to provider’s guide, and keep the files. If you have set the password when generating the private key file, remember it for future use;

b. Rename the private key file as *domain_key_portsip.com.pem*;

c. 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;

d. 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 *domain_cert_portsip.com.pem*;

e. Download the root certificate from your SSL provider and rename it as *root_cert_portsip.com.pem*;



Transport

Please refer to Section 4.6 of PortSIP PBX User Guide for details about adding TLS/WSS transport

Protocol: TLS

Port: 5061

TLS/WSS Settings

Certificate: domain_cert_portsip.com.pem

Root certificate: root_cert_portsip.com.pem

Private key: domain_key_portsip.com.pem

Password:

Client Verification: None

**3** 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.

**4** Click the **Upload** button to choose the certificate files that you have generated for uploading, “**domain_cert_portsip.com.pem**” for the “**Certificate file**”, “**domain_key_portsip.com.pem**” for the “**Private key file**”, and “**root_cert_portsip.com.pem**” for the “**Root certificate file**”.

**5** Enter the “**Certificate Private Key Password**”. This password is the one that you entered when generating the certificate files in previous steps. Leave it blank if you don’t have it.

**6** Click the “**Apply**” button to add the transport.

## 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)

# 4.7 Configuring VoIP provider and SIP Trunk

VoIP providers "**host**" phone lines and replace the traditional telco lines. VoIP providers 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 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.

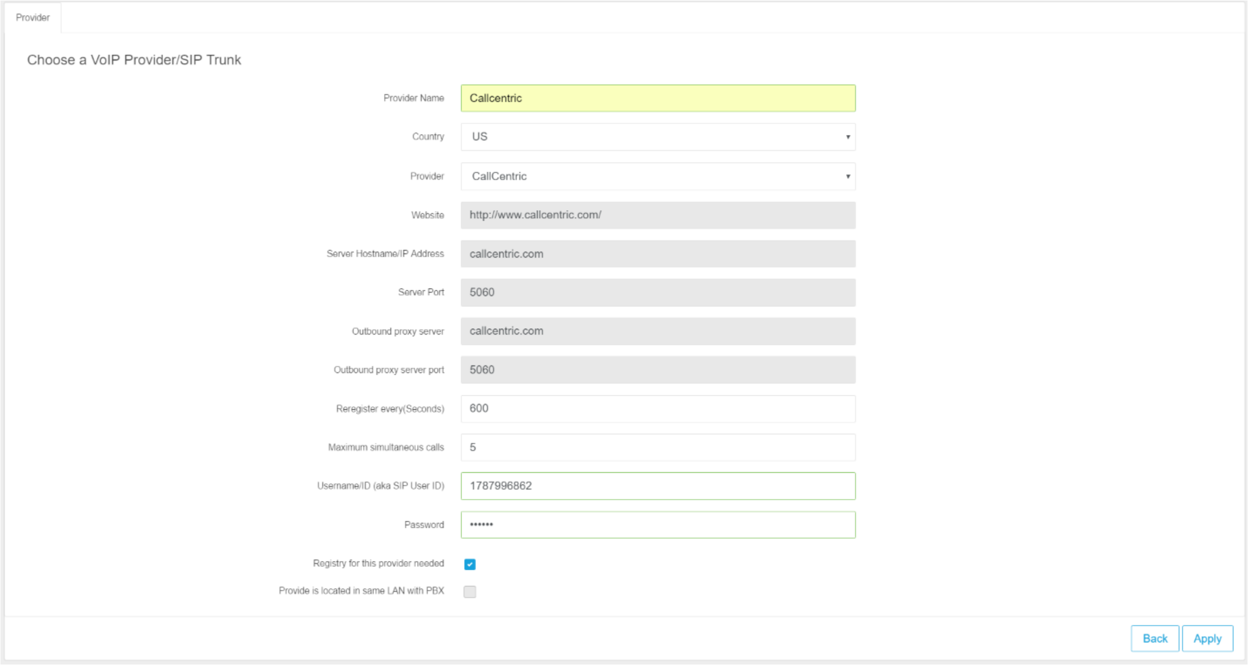
PortSIP PBX supports two types of VoIP providers:

● 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.

## Configuring VoIP Provider / SIP Trunk

**Step 1:** 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 preconfigured templates for these VoIP providers.



Choose a VoIP Provider/SIP Trunk

| | |
|---|---|
| Provider Name | Callcentric |
| Country | US |
| Provider | CallCentric |
| Website | http://www.callcentric.com/ |
| Server Hostname/IP Address | callcentric.com |
| Server Port | 5060 |
| Outbound proxy server | callcentric.com |
| Outbound proxy server port | 5060 |
| Reregister every(Seconds) | 600 |
| Maximum simultaneous calls | 5 |
| Username/ID (aka SIP User ID) | 1787996862 |
| Password | •••••• |
| Registry for this provider needed | ☑ |
| Provide is located in same LAN with PBX | ☐ |

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

**1** In the PortSIP PBX Management Console menu, select "**Call Manager**" > "**VoIP Providers/Trunks**" > "**Add**".

**2** Enter a friendly name for this VoIP provider account.

**3** Select the Country for the VoIP provider. If the provider country is not listed, please choose "**Generic**".

**4** Select your VoIP provider from the Provider drop-down list. If your provider is not in the list, select "**Generic**".

**5** The hostname of SIP server or IP may be prefilled. Compare these with the details that you have received from your VoIP provider and check if all info 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. Click "**Next**" to continue.

**Note: For generic providers, you need to fill in relevant parameters for server by yourself. Please consult your provide for more details.**

**6** If your provider is verified on IP address and does not require registration, please do not check "**Registry for this provider needed**".

**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 "**Provide is located in same LAN with PBX**".

**8** If you would like to allow all tenants using this provider/trunk, please check the "**Available for all tenants**".

**9** Enter the VoIP provider account details. Enter the Authentication ID/username and password of your VoIP provider account. Specify the maximum number of simultaneous calls your provider allows. Click "**Apply**" to complete configuration.

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

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

● In “**Outbound Parameter**” 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**” for “**to**” field 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 4.4**.

● In “**Inbound Parameter**” 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. Configuration requires knowledge on SIP, as wrong configuration may cause PBX to malfunction.

# 4.8 Configuring Inbound/Outbound Rules

Outbound and inbound rules dictate 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 create 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 Trunking before adding the inbound rules. To add Inbound Rule:

1 From the PortSIP PBX Management Console, select "**Call Manager**” **>** "**Inbound Rules**" **>** "**Add**".

2 Enter a friendly name for the rule. Under the new "I**nbound rule**", the "**Type**" allows you to choose between a DID/DDI or (CID) caller ID number mask.

3 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, starting from the last part of the received string. You can use numbers or a wildcard. For example, if your DID number is 2345, the below number mask will be matched to your DID:

*2345*

*

*345 or *45 or *5

2* or 23* or 234*

*2* or *23* or *234*

*1-2346 (Since 2345 is included in the range of 1-2346)*

4 If you chose “**CID**” for "**Type**" in **Step 2**, PortSIP PBX will match the SIP “**from**” header where there is an incoming call.

5 Select which provider/SIP Trunks you wish to be associated with this DID. A DID number can be associated with multiple providers.

6 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*

*Forward call to external number*

7 You can specify that an incoming call should be forwarded differently if it is received outside office hours.

## 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 Management Console.

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 Management Console.

2. Click on the “**Call Manager**” > “**Inbound Rules**” > “**Import**” button.

3. Browse to the file that you want to import, select it and click“**Open**”.

4. The rules will be imported in 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:**

1 From the PortSIP PBX Management Console menu, click "**Call Manager**” **>** "**Outbound Rules**" **>** "**Add** ", and enter a name for the new rule.

2 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.

3 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.

4 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 on the gateway or provider if it is not required. In the example above, you would specify to remove two digits, in order to remove the prefix “**00**” 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.

# 4.9 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:**

1 In the PortSIP PBX Management Console, select **"Call Manager" > "Ring Groups" > "Add "**.

2 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.

**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).

**3** 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.

**4** 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 Management Console, select “**Settings**” > “**Advanced**” tab, 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:

a. Assume you’ve 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 heard 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.

b. 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**”.

# 4.10 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 you 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:**

**1** In the PortSIP PBX Management Console menu, click “**Call Manager**” > "**Virtual Receptionist**" > "**Add** ".

**2** Specify the name and extension number for the digital receptionist.

**3** 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, 8 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**”. English and Simplified Chinese are currently available.

4 Specify the 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.

5 **User Input**: this setting 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:

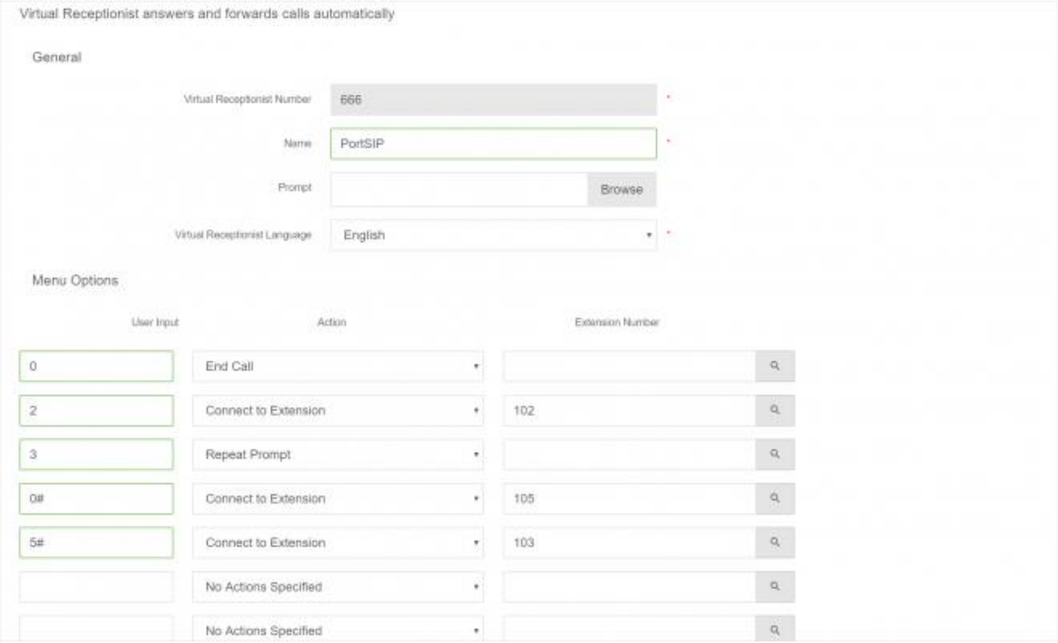
- When Extension Matches: The auto attendant will wait until the caller’s digit sequence matches an existing account. Once the auto attendant finds a match, it will call that extension. This mechanism is useful when accounts of varying name length are used; however, it might be annoying to callers who 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.

6 **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.

7 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

General

| | |
|---|---|
| Virtual Receptionist Number | 666 * |
| Name | PortSIP * |
| Prompt | |
| Virtual Receptionist Language | English * |

Menu Options

| User Input | Action | Extension Number |
|---|---|---|
| 0 | End Call | |
| 2 | Connect to Extension | 102 |
| 3 | Repeat Prompt | |
| 0# | Connect to Extension | 105 |
| 5# | Connect to Extension | 103 |
| | No Actions Specified | |
| | No Actions Specified | |

When configuring straightforward, 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 1, the call will be connected to extension 555.

By placing a pound sign after the direct destination (e.g., “1#”), 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.

- **Input number:** 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.

## Sending HTTP Request to 3rd Server Depending on User’s Input

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 comma-separated list of numbers at one time, e.g. “101,102,103”. The entered number must be unique and must not be duplicated.

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 mandaroty), 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

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.

## 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”.

# 4.11 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, in the PortSIP PBX Management Console, select “**Call Manager**” > “**Call Queues**” > “**Add**”. Now enter the necessary fields:

1. **Queue Number** – Specify the queue number here. It should not be an existing extension number.

2. **Queue Name** – Enter a friendly name for the Queue.

3. **Ring Time** – How long the caller would be queued.

4. **Music on hold** – The music that would be played when the caller is queued.

5. **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

You can configure advanced queue options such as add/remove queue members(agents), and the action taken if no answer, maximum queue calls is reached or maximum queue waiting time is reached.

1. 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

2. 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. You can also decide whether you wish to announce a caller’s position in the queue and the maximum wait time.

3. **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 organisation 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 “Member” tab, you can select the agents for the call queue.

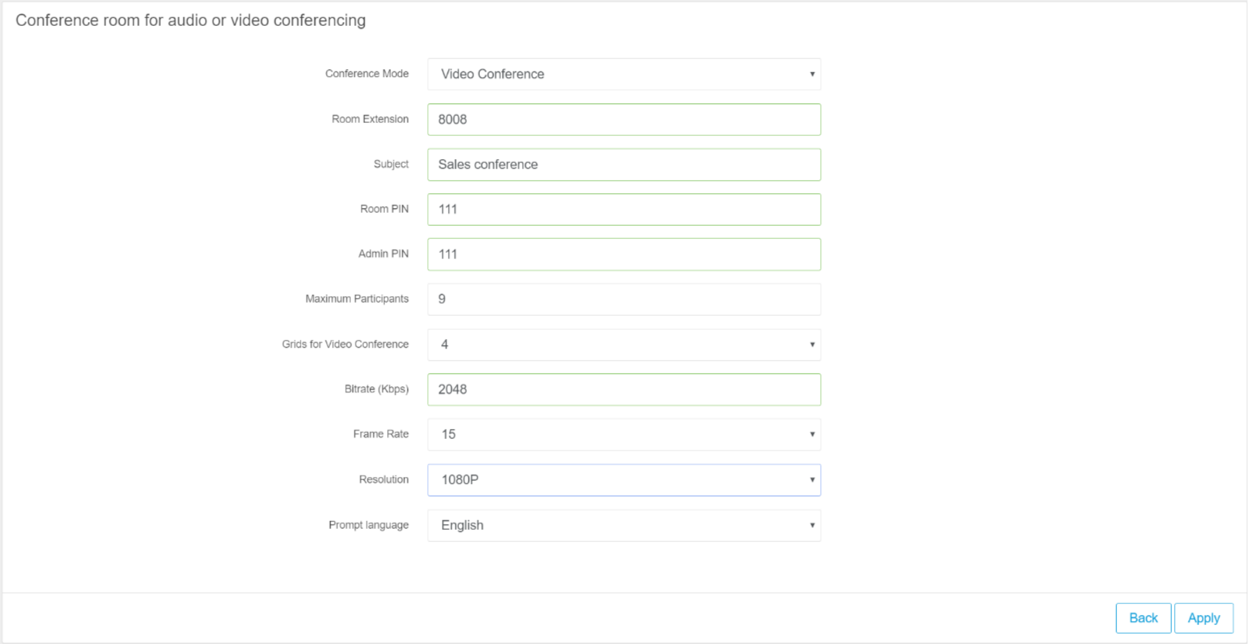
# Notifications

You select 1 or more extension as the queue manager to receive the email notifications if the call is reached SLA time or lost.

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

# 4.12 Configuring Conference

When the PortSIP 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 | 8008 |
| Subject | Sales conference |
| Room PIN | 111 |
| Admin PIN | 111 |
| Maximum Participants | 9 |
| Grids for Video Conference | 4 ▾ |
| Bitrate (Kbps) | 2048 |
| Frame Rate | 15 ▾ |
| Resolution | 1080P ▾ |
| Prompt language | English ▾ |

**To create a conference:**

**1** Select the menu "**Call Manager**" > "**Conference**", and click "**Add**" button.

**2** Select your conference mode from the "**Conference Mode**" drop-down list.

**3** 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.

**4** Enter the suitable **Subject** for the conference to remind participant the content to be discussed.

**5** Enter the **PIN** of the "**Conference Room"** if necessary. If the PIN was set, the Participants must enter the PIN when joining the conference.

**6** 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.

**7** Enter the maximum number of "**Maximum Participants**" field that limits the count of members who join this conference.

**8** Specify the count of videos in "**Grids for Video Conference**". Value 1, 2, 3, 4, 6, 9 supported.

**9** Set the bandwidth used during video conference in "**Video Conference Bitrate**". The value rages 128 kbps – 2048 Kbps. The higher the value is, the better the video experience would be.

**10** Choose "**Video Conference Frame Rate**" with the rage 5 – 30. Higher value will guarantee fluent video experience.

**11** Choose "**Video Conference Resolution**" from range of QCIF to 1080P. Higher resolution leads to larger load to bandwidth.

12 Choose the **Prompt Language** for the vocal notices which will be used when user entering the conference.

13 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.

# 4.13 Managing Conference

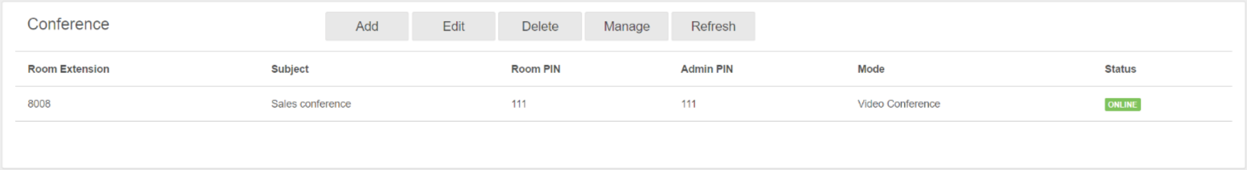
## Joining Conference

After the conference room has been created, inform the participants the conference number ("**Room Extension**"). Assume that the user set **Room Extension** 8008 as the conference number, the user can join the conference by dialing 8008 from any SIP client.

## Invite participants into conference room

You can also invite an extension or the mobile phone/landline phone join the conferencing, please see below section.

## Manage the conference room



| Room Extension | Subject | Room PIN | Admin PIN | Mode | Status |
|---|---|---|---|---|---|
| 8008 | Sales conference | 111 | 111 | Video Conference | ONLINE |

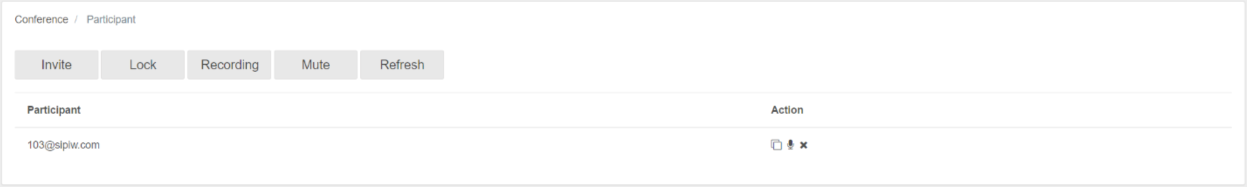
After the conference room has been created, select the menu "**Call Manager**" > "**Conference**" to list available conference rooms. You can either edit the conference room or delete it.

**Manage:** Click the "**Manage**" button to manage the conference room and participants, see next section.

**Edit:** Click the "**Edit**" button 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 |
|---|---|
| 103@sipiw.com | ⧉ 🎤 ✖ |

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. PortSIP 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.

**Lock:** Once the conference is locked, other users cannot dial into the conference room.

**Record:** Start or stop the conference recording. The recorded file will be saved to "*data\mcu\record"* folder of the installation path.

**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 participant:** 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.Configuring Tenant

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.

## 5.1 Creating tenant

To create a new tenant, in the PortSIP PBX Management Console, select the left menu “**Tenant**” and click the “**Add**”.

When creating the 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 in the Management Console.

You can also limit the resource the tenant is using 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.

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

**Recordings:** Specify the space quota for storing recoding files. Default value 0 means unlimited.

**Voice Mails:** Specify the space quota for storing voice mail files. Default value 0 means unlimited.

**Call Reports:** Specify the space quota for storing call report. Default value 0 means unlimited.

To set up the maximum days for keeping recording files, voice mails and call report files, enter the number of days that they will be kept before being deleted and click “**Save**”.

## 5.2 Deactivating tenant

To deactivate an existing tenant, in the PortSIP PBX Management Console, select the left menu “**Tenant**”, and all tenants will be listed. Click the “**Edit**” icon right from the tenant that you want to deactivate, un-check 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.

## 5.3 Deleting tenant

To delete a tenant, in the PortSIP PBX Management Console, select the left menu “**Tenant**”, and all tenants will be listed. Click the “**Delete**” icon button right from the tenant that you want to delete. The tenant and his extensions will be deleted.

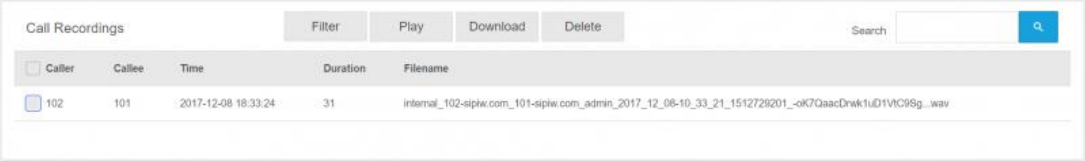
## 5.4 Managing tenant

PortSIP allows administrator to manage tenant and its settings including extension users. To do this, please go to Management Console, navigate to “**Tenant**” section, select a tenant to be managed and click “**Manage**” button on the top of the page. Now user may setup or modify the settings for the tenant and manage its extensions.

Once completed, user may click the “**Switch to Administrator**” menu of the left to switch back to administrator account, without the need to logout of tenant account and relogin to administrator account.

# 6. Call Recording

By using **“Call Recording”** menu in the PortSIP PBX Management Console, you can quickly list all the recorded calls and details on PortSIP PBX.



| □ Caller | Callee | Time | Duration | Filename |
|---|---|---|---|---|
| □ 102 | 101 | 2017-12-08 18:33:24 | 31 | internal_102-sipiw.com_101-sipiw.com_admin_2017_12_08-10_33_21_1512729201_-oK7QaacDrwk1uD1VtC9Sg...wav |

The naming convention for call recording file is: direction_caller-domain_calle-domain_tenant_date_callid.wav. For example:

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

Above recording file name indicates that is a call between two extensions (internal): the caller is sip:101@sipiw.com, callee is sip:102@sipiw.com, their tenant is admin, the call date is Dec 8, 2018, time is 10:33:21 AM, the call ID is **-oK7QaacDrwk1uD1VtC9Sg..**. This call ID is also referred to as the call-id header of SIP message.

You can select the call recording to play it with “**Play**” button, or download or delete it.

# 7.WebRTC

PortSIP PBX integrates WebRTC Gateway by default from V9.0.

After you signed in the Management Console and completed setup wizard, WebRTC is configured by default. You can use the WebRTC Client to make & receive calls directly by clicking “**WebRTC**” > “**HTTP client**” or “**WebRTC**” > “**HTTPS client**“, and WebRTC client will be open in browser.

*Important: Some browsers require HTTPS and do not work with HTTP client, so that we recommend you to use the HTTPS Client.*

## Setup WebRTC

By clicking the “**WebRTC**” > “**Settings**” menu, you would be able to change the WebRTC settings.

**Listen WS**: Default WS port for WebRTC Gateway to be listened. The WS transport is 10080.

**Enable WebRTC service on WSS (Web Socket Security) transport**: You can enable/disable the WebRTC Gateway listens on WSS port. Google Chrome requires WSS to access the camera and microphone. You must select this option to use Google Chrome.

Once “**Listen WSS**” is selected, you should also fill in below fields:

- **Listen WSS on port**: Set a port for the WSS, for example 10443.
- **Gateway Domain Name**: Your WebRTC Gateway domain name, which must be resolvable. If you don’t know it, enter the PortSIP PBX IP. Note: by default the domain is already configured, which does not require modification.
- **Certificate File**: For WSS, you must upload the certificate file. You can generate an SSL certificate file by yourself, or purchase a certificate from provider such as Thawte or Digicert. The certificate must match with the WebRTC Gateway domain (i.e. the previous “Gateway Domain Name”).
- **Private key file**: It will be generated with certificate together.
- **Password of Private key**: The password of private key file is the one you entered when you generated the certificate file. If there is not one, please leave it blank.

*Important: The WSS certificate files were configured by default, which does not require to upload it. The default certificate files are **“Self-signed”**, and thus it will pop up security warnings if you use the browser to open WebRTC client. You can purchase certificate from a third-party certificate provider in order to avoid security warning. For more details, please refer to the next section “Setup WebRTC with the Authorized certificates”.*

### Setup WebRTC with Authorized certificates

You can purchase an official certificate from the certificate provider such as Thawte or Digicert to avoid security alerts and the necessity of adding security exceptions manually.
When purchasing the certificate, you should generate the private key and CSR by yourself – please read the certificate provider’s instructions or ask the provider for support. We recommend you not to set the password for private key file, and you must keep the private key file by yourself.

Assume you have purchased a certificate from Thawte (in this case we use the Thawte SSL123 certificate as example) for your WebRTC Domain example.com. After download the certificate .zip file, you need to extract it and will get two files: IntermediateCA.crt and ssl_certificate.crt. You need to use a plain text editor (for example Windows Notepad; do not use MS Word) to combine your two certs into one file by copying all text from IntermediateCA.crt and appending to ssl_certificate.crt, with the ssl_certificate.crt at the top and IntermediateCA.crt at the bottom.

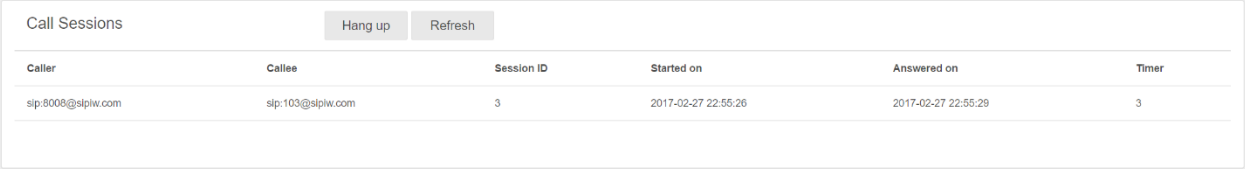
1. Ensure the domain examplertc.com has been resolved correctly to the IP of server where PortSIP PBX is installed.

2. Sign in PortSIP PBX Management Console, click menu **"WebRTC" > "Settings"**, check "**Enable WebRTC service on WSS (Web Socket Security) transport**", enter the "**exmaple.com"** for "**Gateway Domain Name**", and click the "**Browse**" button to upload your ssl_certificate.crt and private key file. Once finished, click "**Apply**" button to save the settings.

Now you can click the "**HTTPS client**" from the "**WebRTC**" menu to open the WebRTC Client, enter your extension number and password, and the SIP domain (this is the SIP domain of extension, not Gateway domain name"), press "**Login**" button to sign in the WebRTC Client to make & receive calls.

# 8.Call Sessions

By using **"Call Sessions"** menu in the PortSIP PBX Management Console, you can quickly monitor all the current calls and details on PortSIP PBX.



| Caller | Callee | Session ID | Started on | Answered on | Timer |
|---|---|---|---|---|---|
| sip:8008@sipiw.com | sip:103@sipiw.com | 3 | 2017-02-27 22:55:26 | 2017-02-27 22:55:29 | 3 |

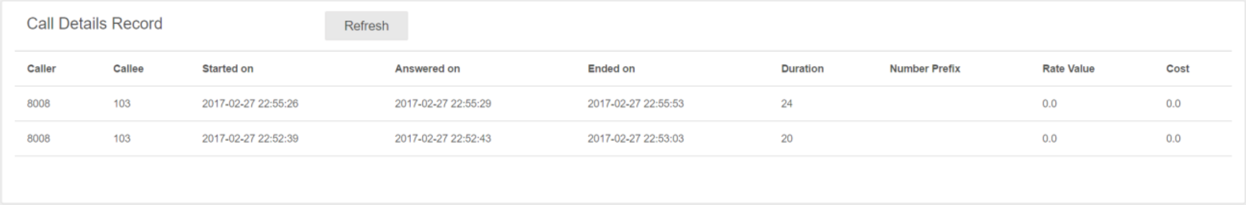
Hang up an established call by clicking "**Hung up**" button from a call session. Click the "**Refresh**" button to update the calls status.

# 9.Call Details & Call Reports

The Call Reports feature allows you to view the call logs 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.

## 9.1 View Call Details

In the PortSIP PBX Management Console, select the left menu “**Call Details**”. All call logs will be listed. Click the “**Next**” button to see more.



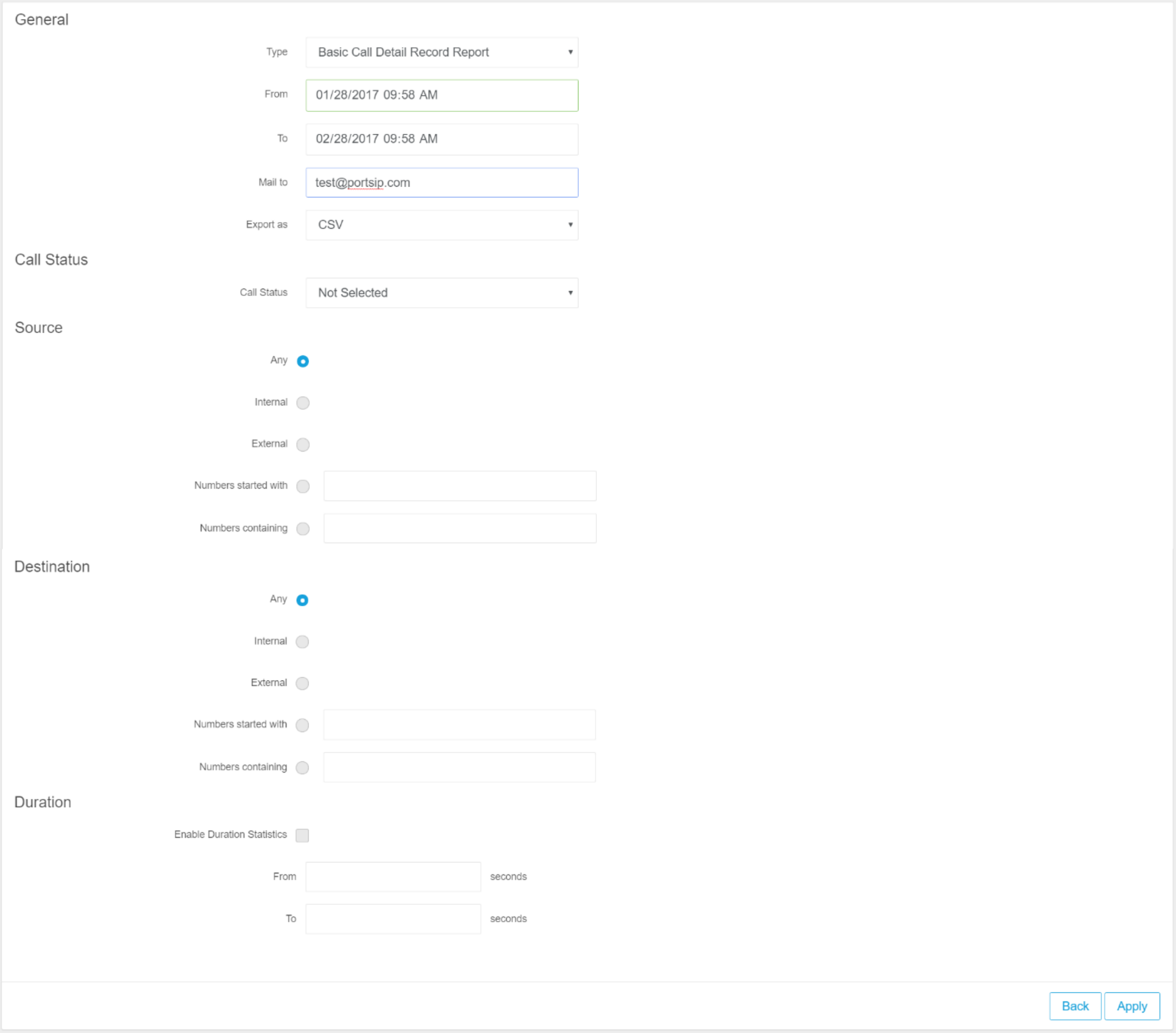
| Caller | Callee | Started on | Answered on | Ended on | Duration | Number Prefix | Rate Value | Cost |
|---|---|---|---|---|---|---|---|---|
| 8008 | 103 | 2017-02-27 22:55:26 | 2017-02-27 22:55:29 | 2017-02-27 22:55:53 | 24 |  | 0.0 | 0.0 |
| 8008 | 103 | 2017-02-27 22:52:39 | 2017-02-27 22:52:43 | 2017-02-27 22:53:03 | 20 |  | 0.0 | 0.0 |

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

## 9.2 Creating 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: 01/28/2017 09:58 AM

To: 02/28/2017 09:58 AM

Mail to: test@portsip.com

Export as: CSV

Call Status

Call Status: Not Selected

Source

● Any

○ Internal

○ External

○ Numbers started with

○ Numbers containing

Destination

● Any

○ Internal

○ External

○ Numbers started with

○ Numbers containing

Duration

Enable Duration Statistics □

From seconds

To seconds

- Select the "**Call Reports**" menu from PortSIP PBX Management Console 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 the caller number. You can specify whole number matched, or only match the number prefix, or filter the caller numbers that include certain numbers.

- Select the filtering criteria by the callee number. You can specify whole number matched, or only match the number prefix, or filter the callee numbers that include certain numbers.

- Select the filtering criteria by call status. Selecting the "**All**" 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.

# 10. Billing

PortSIP PBX allows administrators to define customized calling rate. To do this, please go to Management Console and click “**Billing**”.

## 10.1 Adding Billing Rate

To add rate rule, go to Management Console > “**Billing”** and click “**Add**”, and fill in the fields below:

**Name**: Enter a user-friendly name for the rate.

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

**Rate in**: Rate for incoming calls. The value must be numeric greater than or equal to 0

**Rate out**: Rate for outgoing calls. The value must be numeric greater than or equal to 0.

**Chronon for Rate**: The timing unit used for billing rate.

## 10.2 Editing/Deleting Billing Rate

Once the rate is created successfully, user may view a full list of all rates in “**Billing**” page, and click “**Edit**” or “**Delete**” button on the top of the Billing page to edit or delete the selected rate.

Note: Once the rate created, the value for “**Number Prefix**” cannot be modified.

## 10.3 Importing/Exporting Rate

PortSIP PBX allows to import rates in batch by using “**Import**” button on “**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.

# 11. Settings

After successful installation, the PortSIP PBX Configuration Wizard will guide through the user a series of settings that elicit basic configuration data. After completing basic configuration with the Configuration Wizard, you can perform detailed configuration by using "**Setting**" menu in Management Console 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 General

You can change the general settings by selecting "**Setting"** in PortSIP PBX Management Console.

Note: Usually we do NOT suggest 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 "**portpbx.log**". Set the log level as "**None**" will make large improvement to PBX performance.
- **Enable IPv6:** This option could be used to enable or disable support on IPv6.
- **Disable DIGEST authentication:** If DIGEST challenges disabled, the authorization will be disabled as well. Recommend not to check this option (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.
- **Presence mode:** PortSIP PBX support presence in two modes:

| *Presence Mode* | *Description* |
|---|---|
| Peer to Peer | The Presence state will be relayed via PortSIP PBX, but the PBX will not handle any presence state. |

| | |
|---|---|
| Presence Server | The PortSIP PBX will use internal Presence Server to handle the extension’s presence states. This mode requires the client’s UA supports PUBLISH SIP method. |

**Warning: If the presence mode is changed, PBX will be restarted automatically!**

- **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.

## 11.2 Advanced

You can change the advanced settings by selecting "**Setting" > "Advanced**" in PortSIP PBX Management Console.

**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 “**Ringing Call Prefix**” and “**Held Call Prefix**” respectively to enable Busy Lamp Field feature for calls. Default value for “**Ringing 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.

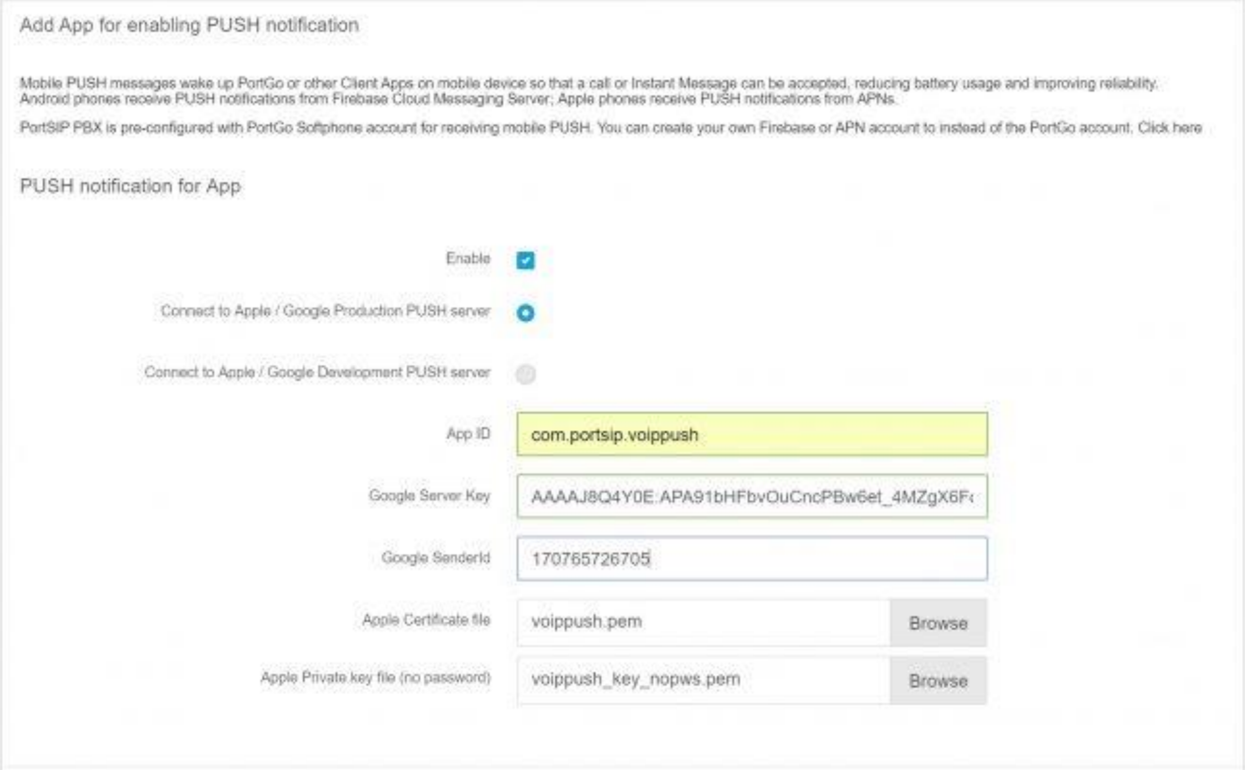
If the boss' extension is 101:

1. The assistant could use his/her IP phone to dial **101 to pick up the boss' incoming call.
2. The assistant could dial ##101 on his/her own IP phone to pick up the call which held by boss.

# 11.3 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 PortGo 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.

PortSIP PBX is pre-configured with PortGo Softphone account for receiving mobile PUSH. You can create your own Firebase or APN account to instead of the PortGo account. Click here

PUSH notification for App

Enable ☑

Connect to Apple / Google Production PUSH server ●

Connect to Apple / Google Development PUSH server ○

App ID: com.portsip.voippush

Google Server Key: AAAAJ8Q4Y0E:APA91bHFbvOuCncPBw6et_4MZgX6F‹

Google SenderId: 170765726705

Apple Certificate file: voippush.pem

Apple Private key file (no password): voippush_key_nopws.pem

PortSIP softphone 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 Management console.
2. Navigate to "**Settings**" > "**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.

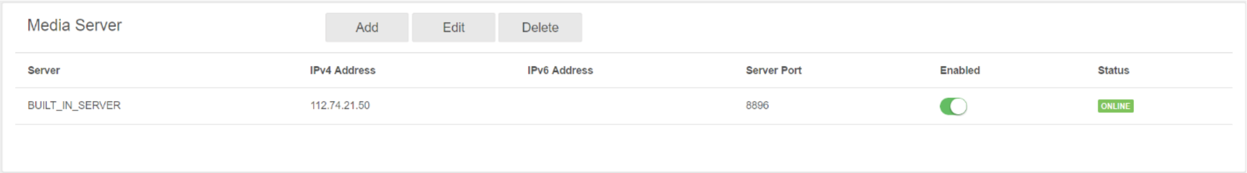
The step by step guide for make the Mobile PUSH notifications works with your app and PortSIP PBX, please refer to below topics:

1. Implement the PUSH notifications in Native iOS App with PortSIP PBX
2. Implement the PUSH notifications in Android App with PortSIP PBX

# 11.4 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.

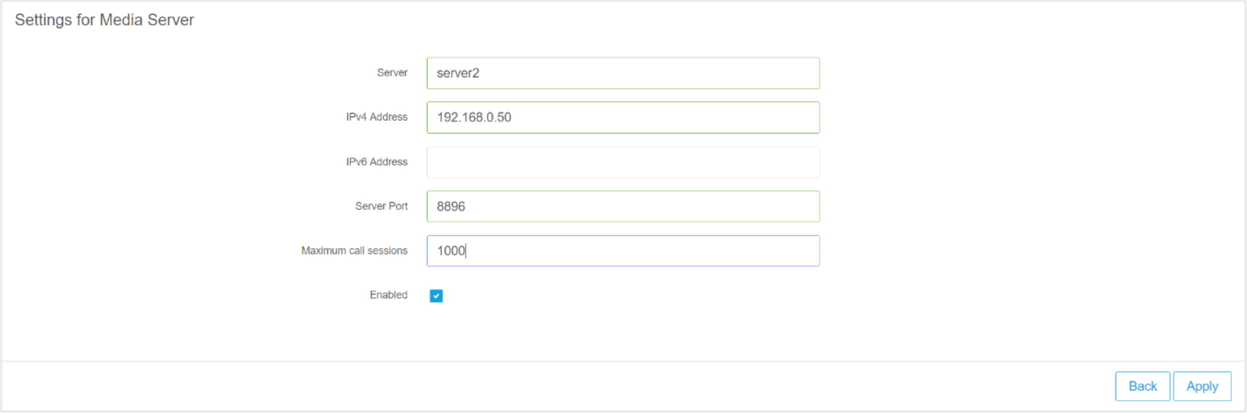


| Server | IPv4 Address | IPv6 Address | Server Port | Enabled | Status |
|---|---|---|---|---|---|
| BUILT_IN_SERVER | 112.74.21.50 |  | 8896 | ● | ONLINE |

## 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: server2

IPv4 Address: 192.168.0.50

IPv6 Address:

Server Port: 8896

Maximum call sessions: 1000

Enabled: ☑

Select the **"Settings" > "Media Server"** menu in PortSIP PBX Management Console, 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 “**Settings**” > “**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 “**Edit**” icon.

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 **"Settings" > "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 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.

# 11.5 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 “**Settings**” > “**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 200MB. You can also enter the number of days that they will be kept before they’re deleted automatically.

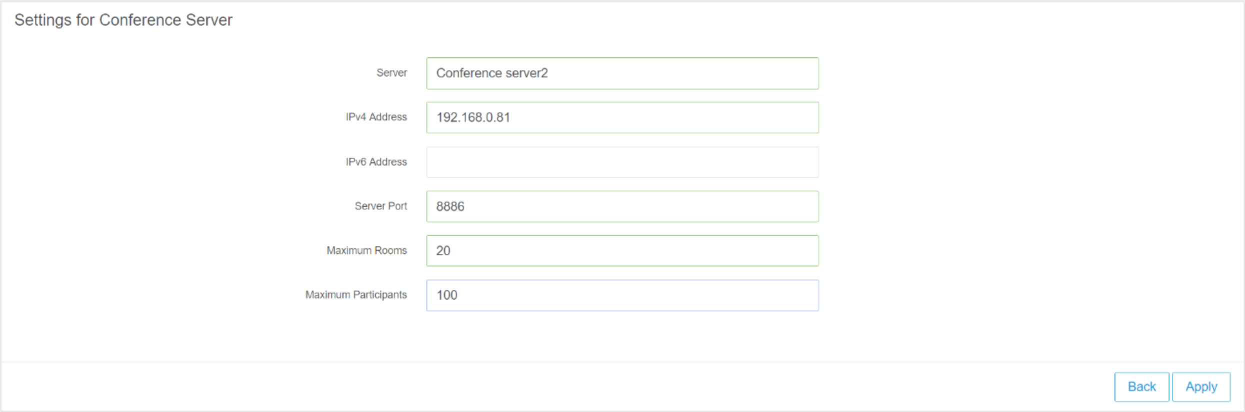
# 11.6 Managing Conference Server

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: Conference server2

IPv4 Address: 192.168.0.81

IPv6 Address:

Server Port: 8886

Maximum Rooms: 20

Maximum Participants: 100

In PortSIP PBX Management Console, select the **"Settings" > "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 "**Settings**" > "**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.

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 **"Settings" > "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.

# 11.7 Backup and Restore

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

# Common Backup

To backup system settings, please:

1. Visit Management Console, go to “**Settings**” > “**Backup**”, 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 to view the backup file. User now may click to select one item of the list and click “**Download**” button on top of the page to download it to local, or click “**Restore**” button to restore PBX to previous settings.

# Migrate PBX to another Machine

To migrate the PortSIP PBX from one machine to another:

1. Visit Management Console, go to “**Settings**” > “**Backup**”, 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. Refresh the page, download and save the backup file.

**Now there has a way to restore the PBX:**

After the PortSIP PBX installed on the new machine without the “**Advanced**” mode, sign in Management Console, click “**Settings**” > “**Backup**” menu, click “**Import**” button to upload your backup file. Once the backup file imported successfully, selected it and click “**Restore**” button. After the restoration progress completed, PBX will be restored to previous settings. **Note: this method is recommended for smaller backup task.**

# Backup Schedule

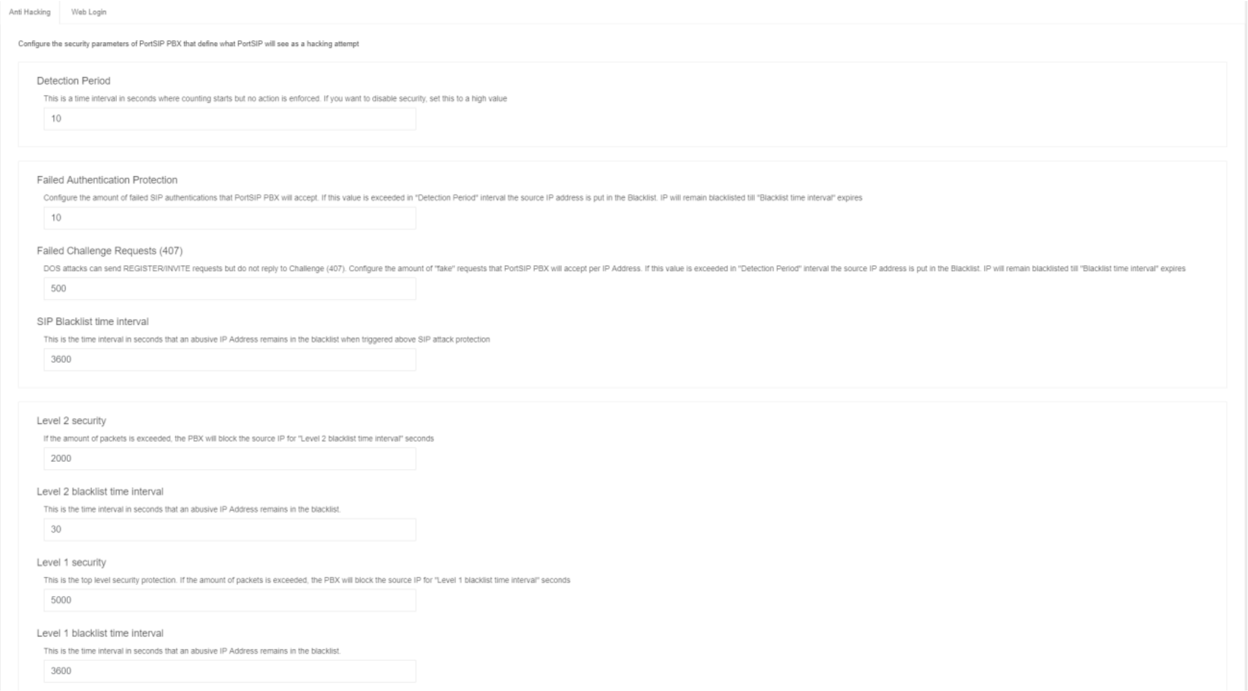
In addition to common single backup, user may also setup “**Backup Schedule**” to backup PBX settings and data regularly.

To do this, please visit Management Console, go to “**Settings**” > “**Backup**”, click “**Backup Schedule**” button on top of the page, and fill in below fields if necessary:

> **Disable 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 but not limited to “**PBX Core Data**”, “**System Prompts**”, and “**Voicemails**” etc. A selected item indicates the file type to be included in backup.
>
> **Backup timing**: Backup could be scheduled to execute daily or weekly by checking the radio at the end of each selection. Once selected, user may specify the hour for staring backup. For weekly backup, the weekday for running backup is also necessary.

# 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.



Configure the security parameters of PortSIP PBX that define what PortSIP will see as a hacking attempt

Detection Period

This is a time interval in seconds where counting starts but no action is enforced. If you want to disable security, set this to a high value

10

Failed Authentication Protection

Configure the amount of failed SIP authentications that PortSIP PBX will accept. If this value is exceeded in "Detection Period" interval the source IP address is put in the Blacklist. IP will remain blacklisted till "Blacklist time interval" expires

10

Failed Challenge Requests (407)

DOS 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 "Blacklist time interval" expires

500

SIP Blacklist time interval

This is the time interval in seconds that an abusive IP Address remains in the blacklist when triggered above SIP attack protection

3600

Level 2 security

If the amount of packets is exceeded, the PBX will block the source IP for "Level 2 blacklist time interval" seconds

2000

Level 2 blacklist time interval

This is the time interval in seconds that an abusive IP Address remains in the blacklist.

30

Level 1 security

This is the top level security protection. If the amount of packets is exceeded, the PBX will block the source IP for "Level 1 blacklist time interval" seconds

5000

Level 1 blacklist time interval

This is the time interval in seconds that an abusive IP Address remains in the blacklist.

3600

The above screenshot shows the main interface of the PortSIP PBX Anti Hacking configuration page. This is accessible by clicking on the menu "**Settings**" > "**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)

DOS 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.

# 12. Blacklist and Codes

## 12.1 Codes and E164

PortSIP PBX allows 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.

## 12.2 Number Blacklist

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

To add the number into blacklist:

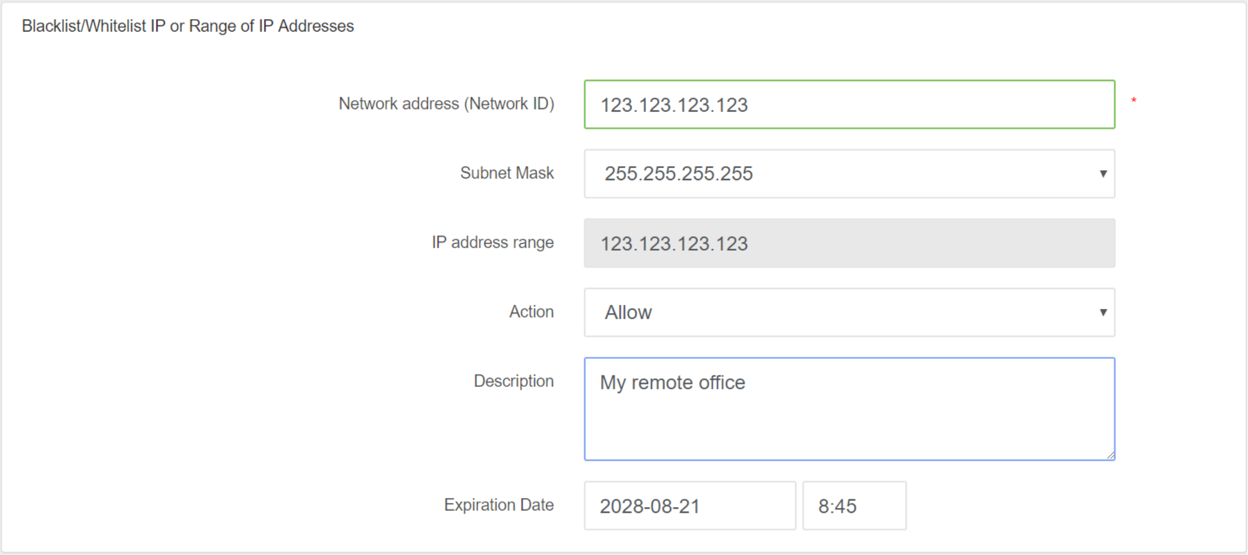
1. Login to the PortSIP PBX Management Console.
2. Click on “**Blacklist**” from the left menu.
3. Click “**Add**” to add a new entry.
4. Enter the number that you want to block and enter the description.

## 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:



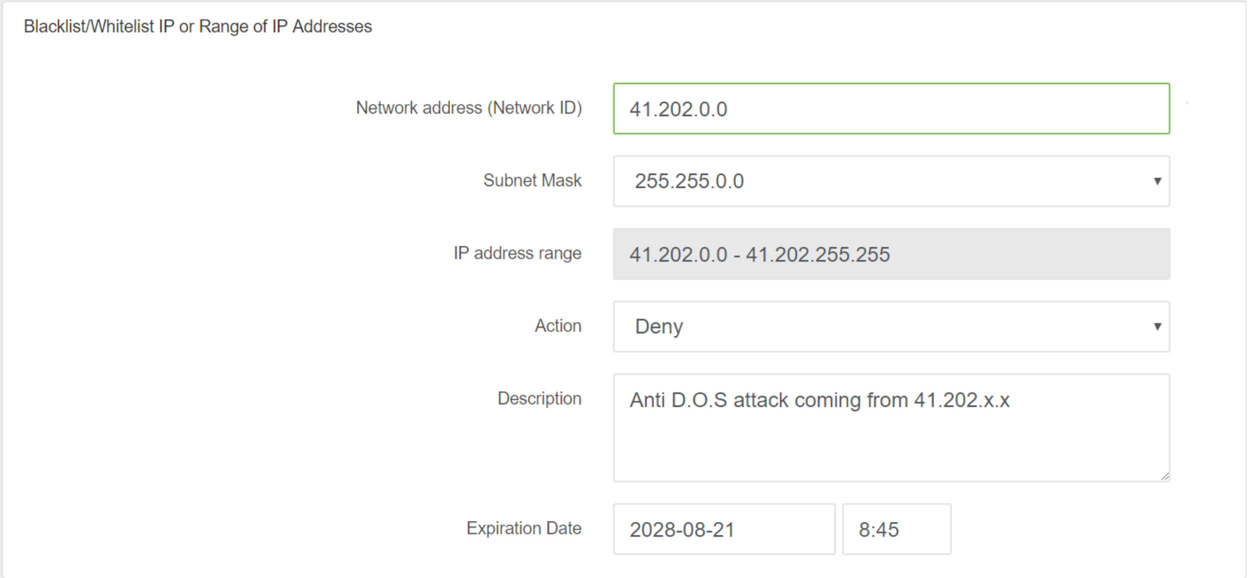
Blacklist/Whitelist IP or Range of IP Addresses

| | |
|---|---|
| Network address (Network ID) | 123.123.123.123 * |
| Subnet Mask | 255.255.255.255 |
| IP address range | 123.123.123.123 |
| Action | Allow |
| Description | My remote office |
| Expiration Date | 2028-08-21 8:45 |

1. Login to the PortSIP PBX Management Console.
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.



Blacklist/Whitelist IP or Range of IP Addresses

| | |
|---|---|
| Network address (Network ID) | 41.202.0.0 |
| Subnet Mask | 255.255.0.0 |
| IP address range | 41.202.0.0 - 41.202.255.255 |
| Action | Deny |
| Description | Anti D.O.S attack coming from 41.202.x.x |
| Expiration Date | 2028-08-21 8:45 |

1. Login to the PortSIP PBX Management Console.
2. Click on “**Blacklist and Codes**” > “**IP Blacklist**”.
3. Click “**Add**” to add an entry.
4. In the “**Network 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 “**Deny**“.
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 Deny entry will be created in the IP Blacklist page. All traffic coming from this IP address will be checked, anti-hacking algorithms will come into effect and all packets from this IP Address 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.

# 13. Profile

The admin and tenant user can manage their profile by selecting the "**Profile**" menu from the PortSIP PBX Management Console.

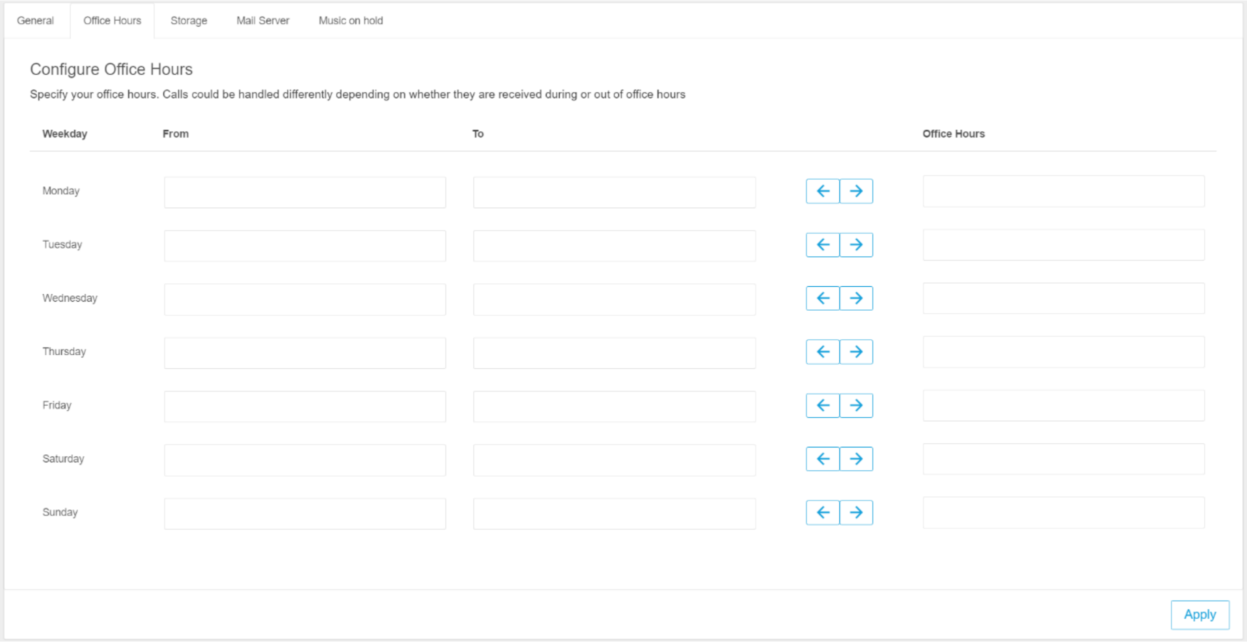
## 13.1 General

The admin user or tenant user can modify their profile details in the "**General**" tab:

- **Username:** The username for the admin or tenant user.
- **Password:** If the password was modified, the admin or tenant user must use new password to login to management console.
- **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.
- **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 un-selected, the extension can't modify his SIP password.
- **Enable extension audio recording:** If this option is selected, the extension calls will be recorded as wav file
- **Enable extension video recording:** If this option is selected, the extension video calls will be recorded as AVI video file.

## 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.



Configure Office Hours

Specify your office hours. Calls could be handled differently depending on whether they are received during or out of office hours

| Weekday | From | To | | Office Hours |
|---|---|---|---|---|
| Monday | | | ← → | |
| Tuesday | | | ← → | |
| Wednesday | | | ← → | |
| Thursday | | | ← → | |
| Friday | | | ← → | |
| Saturday | | | ← → | |
| Sunday | | | ← → | |

Select the "**Profile" >** "**Office Hour**" in PortSIP PBX Management Console. You can configure the office hours for each day by clicking "**Add**" or "**Remove**" buttons.

## 13.3 Storage

By clicking the “**Storage**” tab, you will see the store quota and used quota.

**Recording**: Specify the maximum storage for recordings. Default value 0 indicates unlimited.

**Voicemails**: Specify the maximum storage for voicemails. Default value 0 indicates unlimited.

**Call Reports:** Specify the maximum storage for call reports. Default value 0 indicates unlimited.

To set up the maximum days for keeping recording files, voice mails and call report files, enter the number of days that they will be kept before being deleted and click “**Apply**”.

## 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 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:

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 “**Browse**” 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. The CDR is formatted in JSON.

To setup, please go to “**Profile**” > “**Event URL**” of Management Console.

## CDR Events

To send the CDR event 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.

**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:

```
{“

        call_answered_time”: 1489482637,

        “call_cost”: “0.0001”,

        “call_direction”: “outbound”,

        “call_ended_reason”: “CALLED_DISCONNECT”,
        “call_ended_time”: 1489482652,

        “call_fail_code”: 0,

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

        “call_id”: “irZ8nUlnUuPM3NFVcwL32g..”,

        “call_prefix”: “188”,

        “call_rate”: “0.0001”,

        “call_start_time”: 1489482609,

        “call_status”: “ANSWERED”,

        “call_talk_time”: 15,

        “call_targets”: [{“

                target_add_time”: 1489482609,

                “target_answered_time”: 1489482637,

                “target_end_reason”: “DISCONNECT”,

                “target_number”: “008618817182298”,

                “target_domain”: “callcentric.com”,

                “target_ended_time”: 1489482652,

                “target_fail_code”: 0,

                “target_status”: “ANSWERED”,

                “target_ring_duration”: 10,

                “target_talk_time”: 15

        }],

        “call_trunk_name”: “callcentric”,

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

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

        “caller_display_name”: “”,

        “cost_duration_unit”: 60,

        “caller_display_name”: “James”,

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

}
```

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.

**talk_time** indicates the seconds of duration consumed in the calling.

## 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”

}

# 13.7 SMS

## SMS

By setting up SMS, PortSIP PBX will be able to send SMS message when it receives a text message from extension. To setup, go to “**Profile**” > “**SMS**” of Management Console.

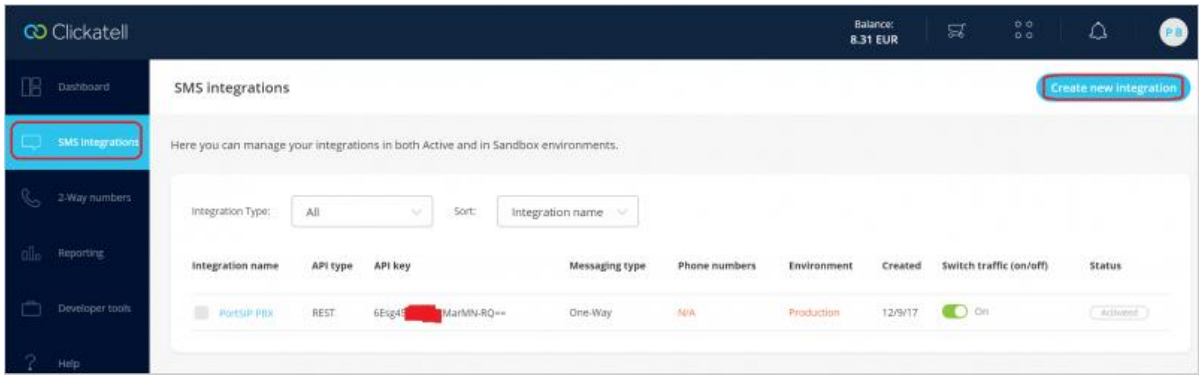
To enable the SMS feature, below options should be provided:

**Enable:** By checking/unchecking this option, you are allowed to enable or disable the SMS feature.

**SMS Provider:** SMS providers supported by PortSIP PBX, currently including Twilio, Clickatell, Nexmo, SMSAPI. You can signup an account from one of these providers.

## Setup with Clickatell

Clickatell is a SMS provider. You can visit https://www.clickatell.com to register an account and sign in.



Here you can manage your integrations in both Active and in Sandbox environments.

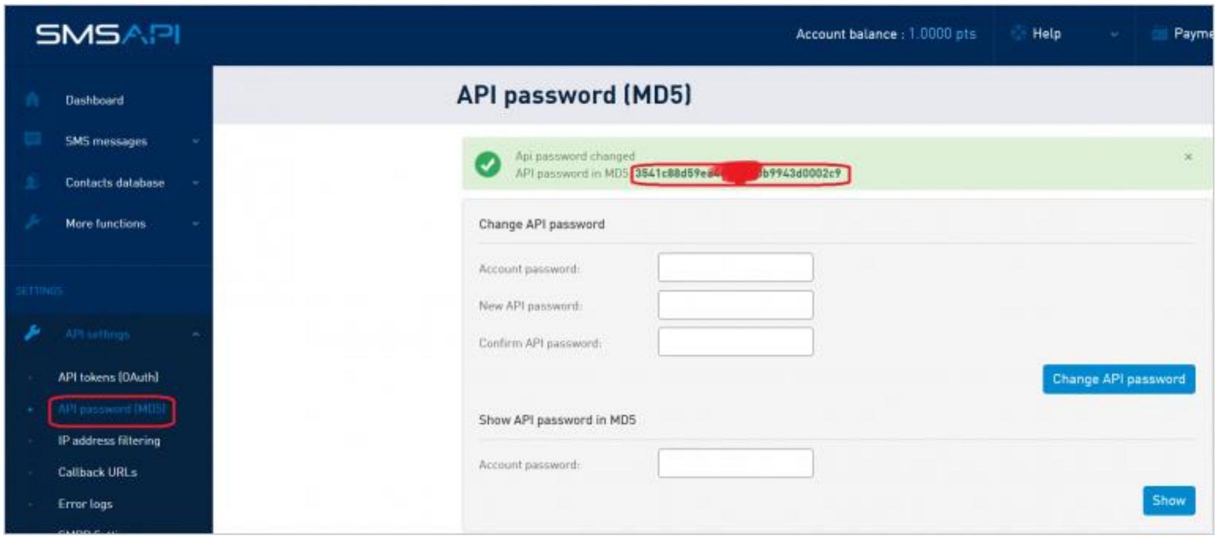
| Integration name | API type | API key | Messaging type | Phone numbers | Environment | Created | Switch traffic (on/off) | Status |
|---|---|---|---|---|---|---|---|---|
| PortSIP PBX | REST | 6Esg4[redacted]MarMN-RQ== | One-Way | N/A | Production | 12/9/17 | On | Activated |

Click the “**SMS integrations**” on the left menu, and the “**Create new integration**” in the top right corner. Follow the wizard to create and copy API key once integration created. Note: You should choose “**REST**” as the API type.

Now in PortSIP PBX, choose the SMS provider “**Clickatell**“, paste the copied API key into “**API key/Token**“.

# SMSAPI

SMSAPI is a SMS provider. You can visit https://www.smsapi.com to register an account and sign in.



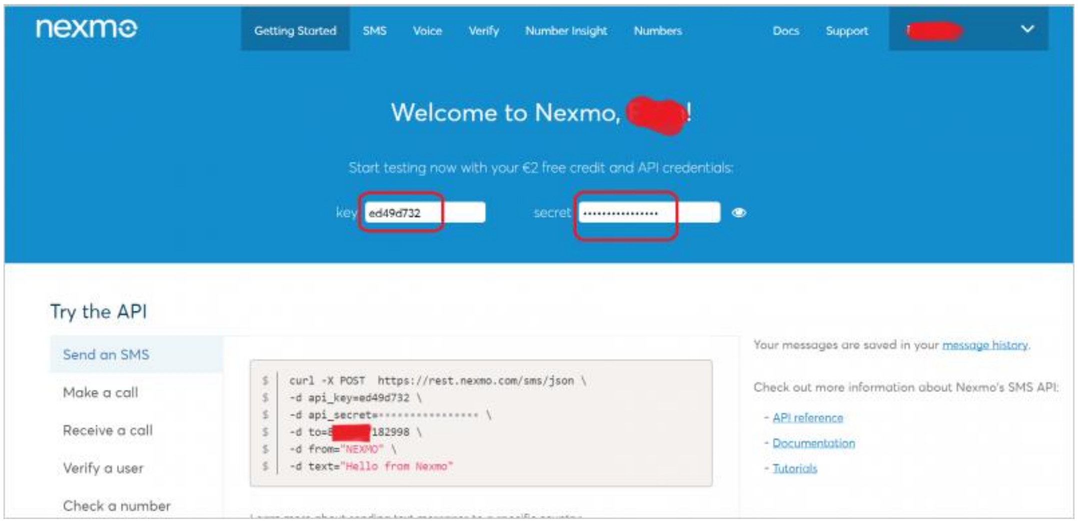
Api password changed
API password in MD5 3541c88d59e[redacted]b9943d0002c9

Click the “**API password (MD5)**” on the left menu. In the “**Change API Password**” section displayed, enter your account password and new API password, click “**Change API password**“. In this page the “**API password in MD5**” will show up, please copy the MD5 string.

Now in PortSIP PBX, choose the SMS provider “**SMSAPI**“, paste the copied API MD5 string to “**Password**“, enter your SMSAPI account as the “**Username**“, and enter a name for “**From**” filed if you want to specify the SMS sender.

# Nextmo

Nextmo is a SMS provider. You can visit https://www.nextmo.com to register an Account and sign in.



[redacted]

Welcome to Nexmo, [redacted]!

Start testing now with your €2 free credit and API credentials:

key ed49d732 secret ••••••••••••••••

```
$ curl -X POST  https://rest.nexmo.com/sms/json \
$ -d api_key=ed49d732 \
$ -d api_secret=•••••••••••••••• \
$ -d to=[redacted]182998 \
$ -d from="NEXMO" \
$ -d text="Hello from Nexmo"
```

Your messages are saved in your message history.

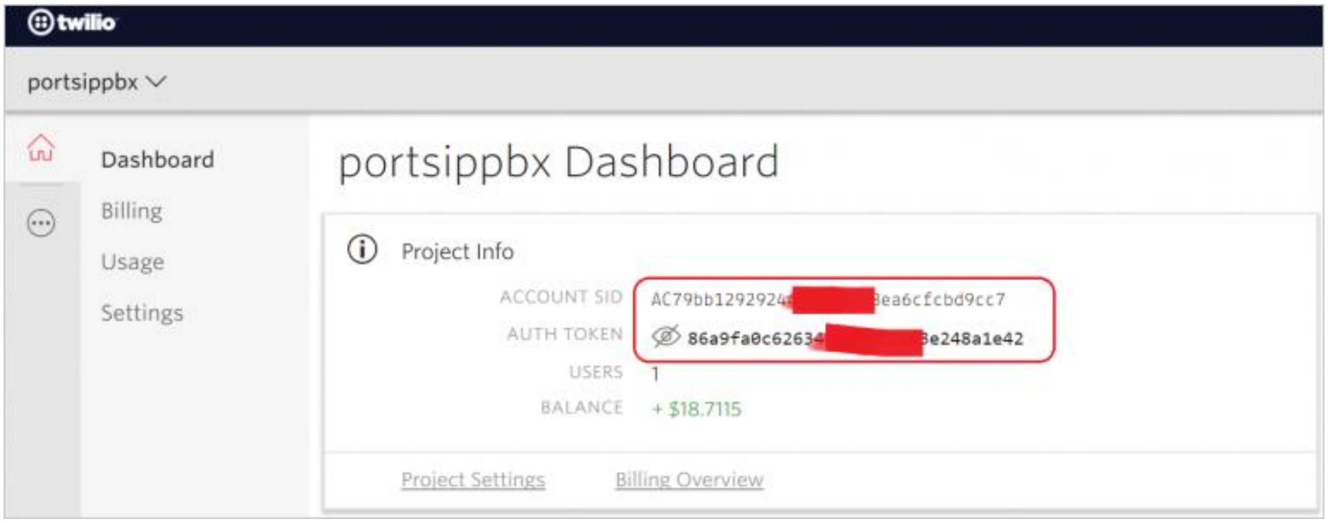
Check out more information about Nexmo's SMS API:

- API reference
- Documentation
- Tutorials

Now in PortSIP PBX, choose the SMS provider as “**Nexmo**“, copy the “**key**” from Nexmo and paste to “**Username**” filed in PortSIP PBX, copy the “**secret**” from Nexmo and paste to “**Password**” filed in PortSIP PBX. Enter a name for “**From**” filed if you want to specify the SMS sender.

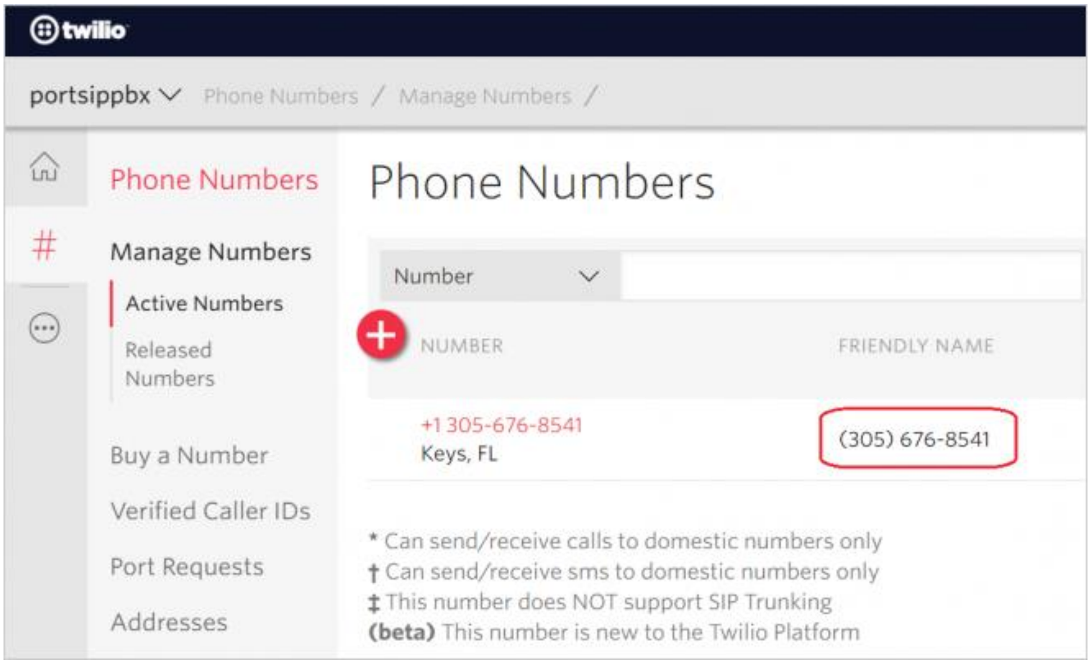
# Twilio

Twilio is a SMS provider. You can visit https://www.twilio.com to register an account and sign in.



| | |
|---|---|
| ACCOUNT SID | AC79bb1292924[redacted]ea6cfcbd9cc7 |
| AUTH TOKEN | 86a9fa0c62634[redacted]e248a1e42 |
| USERS | 1 |
| BALANCE | + $18.7115 |

To work with Twilio, you should also buy a number in order to send the SMS. To do so, click the Manage Numbers in "**Phone Numbers**" section and follow the instructions to buy a number.



| NUMBER | FRIENDLY NAME |
|---|---|
| +1 305-676-8541<br>Keys, FL | (305) 676-8541 |

* Can send/receive calls to domestic numbers only
† Can send/receive sms to domestic numbers only
‡ This number does NOT support SIP Trunking
**(beta)** This number is new to the Twilio Platform

Now in PortSIP PBX, choose the SMS provider "**Twilio**", copy the "**ACCOUNT SID**" from Twilio Console Dashboard to "**Username**" field in PortSIP PBX, copy the "**AUTH TOKEN**" from Twilio Console Dashboard to "**Password**" field in PortSIP PBX, and copy the phone number to "**From**" field in PortSIP PBX.

Note, you should remove the "(", "-", and blank space from the phone number before pasting to PortSIP PBX. For example, the (305) 676-8541 should be 3056768541.

*Important: Before you fill the SMS provider information into PortSIP PBX, we recommend you to send some test SMS messages in your SMS provider management console/panel to make sure SMS works well.*

**Example:**

If you have setup the SMS provider, now an extension sends a pager message to PortSIP PBX, and indicates that pager message is a SMS message:

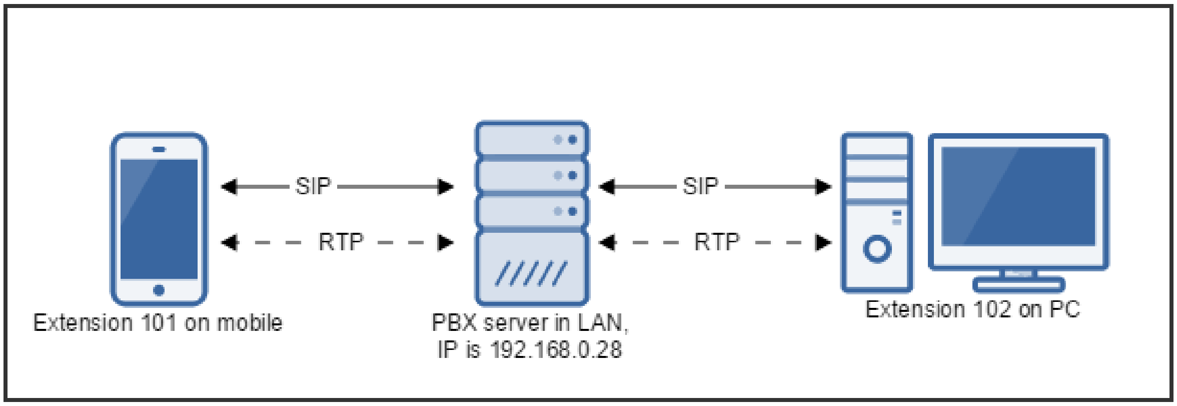
*To: <sip:102@sipiw.com>;messagetype=SMS*

If the parameter “messagetype” is presented in the “**To**” header, and the value is “**SMS**”, PBX will relay this pager to the configured SMS provider.

# 14. Deployment Practices

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.

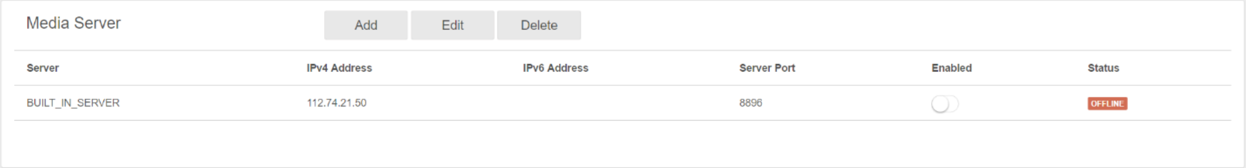
## 14.1 Deploy PortSIP PBX in LAN



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.

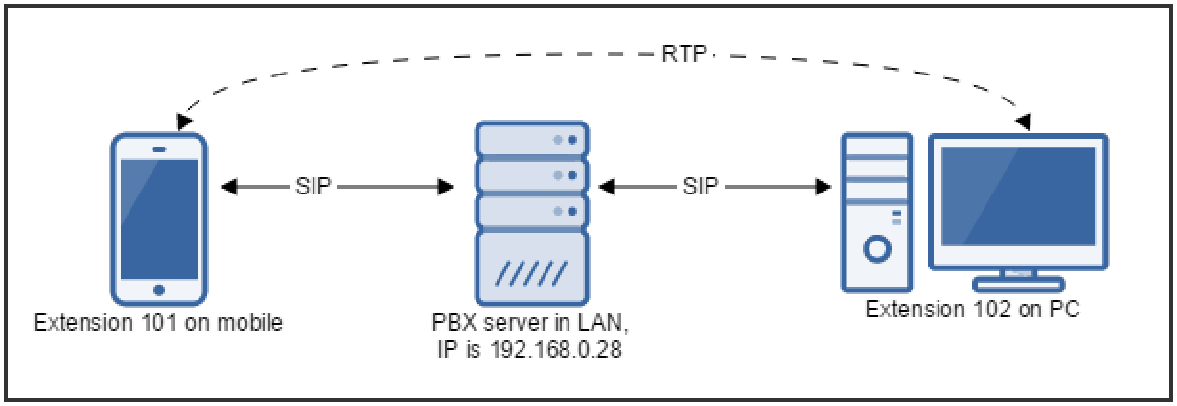
## 14.2 Large-Scale Deployment in LAN

In **12.1 scenario**, if there are a lot of simultaneous calls, the PortSIP PBX will get high loads since all RTP streams pass through the PortSIP IP. In order to reduce PortSIP IP server loads we can disable the RTP relay feature, thus the RTP packages will be sent and received directly between the caller and callee.



| Server | IPv4 Address | IPv6 Address | Server Port | Enabled | Status |
|---|---|---|---|---|---|
| BUILT_IN_SERVER | 112.74.21.50 | | 8896 | ○ | OFFLINE |

Sign in the PortSIP PBX Management Console, select “**Settings**” > “**Media Server**” from left menu, and all media servers will display. Click the “**Enabled**” button to disable all the media servers, and then click “**Apply**” button.



Once set, the media streams (RTP packets for audio and video) from the caller is sent directly to the callee and vice versa. The signaling (SIP) for both caller and callee still passes through PBX, but the media is point-to-point. See above figure.

**Note:** *Do not disable the media server when you deploy the PortSIP PBX on internet, which will cause no audio* and video transmit in call.

## 14.3 Large-Scale Deployment in LAN for Handling 10K+ Concurrent Calls

This section provides complete information about how to customize and administer large-scale deployments of PortSIP PBX. For example, how to handle 10K+concurrent calls.

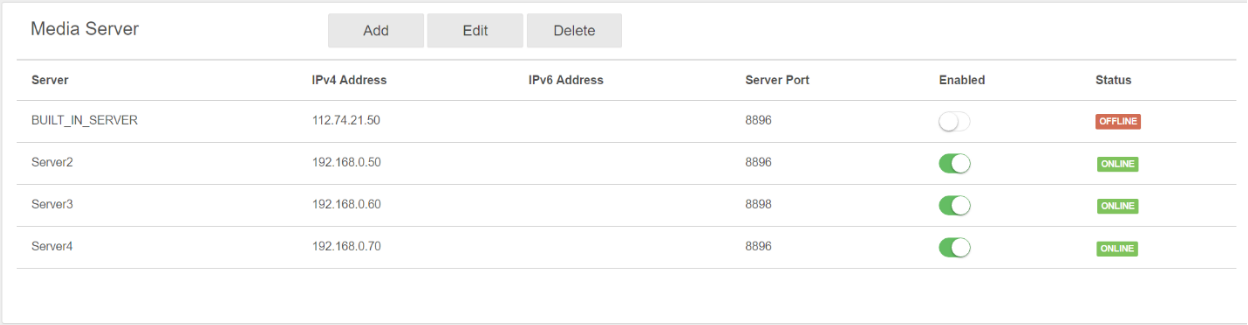
### Scale Deployment for Media Server

If order to reduce the server loads, we can enable the load-balancing in case of large numbers of concurrent calls on PortSIP PBX.

**Step 1:** Download the standalone PortSIP Media Server installer at PortSIP Website.

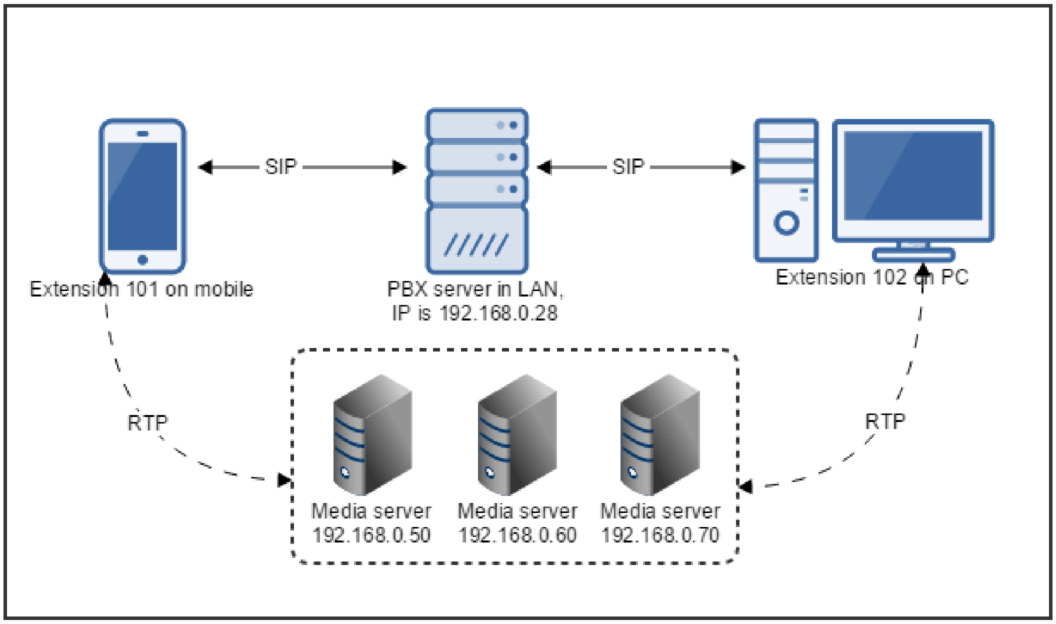
**Step 2:** Select “**Settings**” > “**Media server**” in PortSIP PBX Management Console, and the media servers will be displayed. Click the “**Enabled**” button from the "**Built-in Server"** to disable the default media server. Click "**Apply**" button.

**Step 3:** Deploy several servers in LAN, for example: 192.168.0.50, 192.168.0.60, 192.168.0.70; and install Media Server on these servers.



| Server | IPv4 Address | IPv6 Address | Server Port | Enabled | Status |
|---|---|---|---|---|---|
| BUILT_IN_SERVER | 112.74.21.50 | | 8896 | ○ | OFFLINE |
| Server2 | 192.168.0.50 | | 8896 | ● | ONLINE |
| Server3 | 192.168.0.60 | | 8898 | ● | ONLINE |
| Server4 | 192.168.0.70 | | 8896 | ● | ONLINE |

**Step 4:** Select the menu "**Settings" > "Media Server",** click **"Add Server"** in PortSIP PBX Management Console. Enter a friendly name, IP and port for each new Media Server that you deployed on 192.168.0.50, 192.168.0.60, 192.168.0.70.



Once set, the media streams (RTP packets for audio and video) will be relayed by one of the Media Servers on the base of the media server loads. The signaling (SIP) for both caller and callee still passes through PortSIP IP PBX System, but the media streams handled by separate media servers will not pass through PortSIP PBX server. See above figure.

By following the above method, you can add more media servers into the PortSIP PBX for handling more concurrent calls.

## Scale Deployment for Conference Server

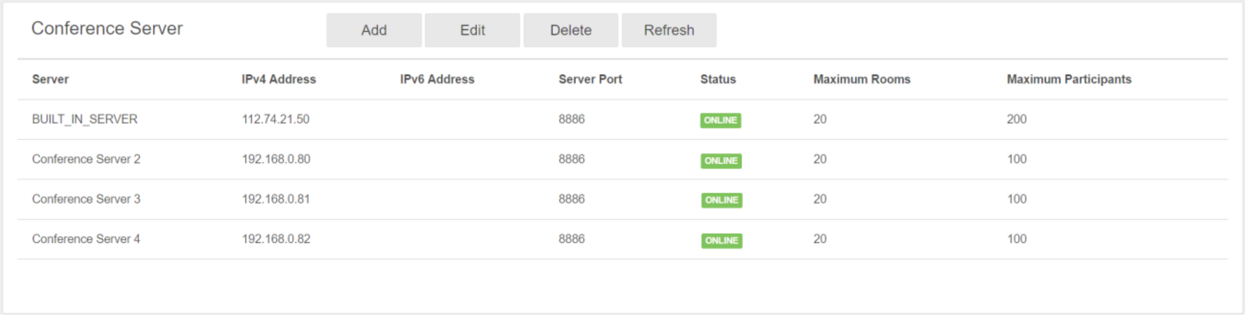
We can use similar method to deploy Conference Server likes Media Server to reduce the PortSIP PBX IP server loads.

**Step 1:** Download the standalone PortSIP Conference Server installer at PortSIP Website.

**Step 2:** Select menu “**Settings**” > “**Conference server**” in PortSIP PBX Management Console, and the conference servers will display. Click the “**Enabled**” button from the **"Built-in Server"** to disable the default conference server. Click "**Apply**" button.

**Step 3:** Deploy several servers in LAN, for example: 192.168.0.80, 192.168.0.81, 192.168.0.82; and install Conference Server on these servers.

**Step 4:** Select the menu "**Settings" > “Conference Server”,** click "**Add Server**" in PortSIP PBX Management Console. Enter a friendly name, IP and port for each new Conference Server that you deployed on 192.168.0.80, 192.168.0.81, 192.168.0.82.



| Server | IPv4 Address | IPv6 Address | Server Port | Status | Maximum Rooms | Maximum Participants |
|---|---|---|---|---|---|---|
| BUILT_IN_SERVER | 112.74.21.50 | | 8886 | ONLINE | 20 | 200 |
| Conference Server 2 | 192.168.0.80 | | 8886 | ONLINE | 20 | 100 |
| Conference Server 3 | 192.168.0.81 | | 8886 | ONLINE | 20 | 100 |
| Conference Server 4 | 192.168.0.82 | | 8886 | ONLINE | 20 | 100 |

Once set, you can create many conference rooms on the Conference Servers. PortSIP PBX will allocate conferences to the available conference servers to reduce the server loads for PortSIP PBX.

By following above method, you can add more conference servers into the PortSIP PBX for handling more conferences.

# 14.4 Deploy PortSIP PBX on AWS

This section provides complete information about how to deploy PortSIP PBX on the AWS cloud platform to provide calling service to users, and how the users can login to PBX from internet, make calls to other users and to PSTN via VoIP provider/SIP Trunk.

## Sign up for AWS Account

Please skip this step if you already have an AWS account (Amazon account).

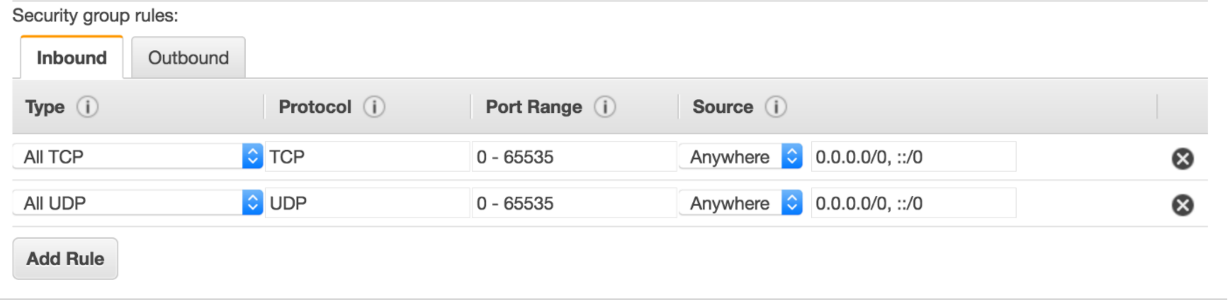
Go to AWS website, and sign up by following the instructions. Part of the sign-up procedures involve receiving a phone call and entering a PIN by using the phone keypad.

## Launch an EC2 Windows Instance

**Step 1:** After successfully created an account, sign in to the AWS Management Console, and follow this guide. Please pay attention to below items:

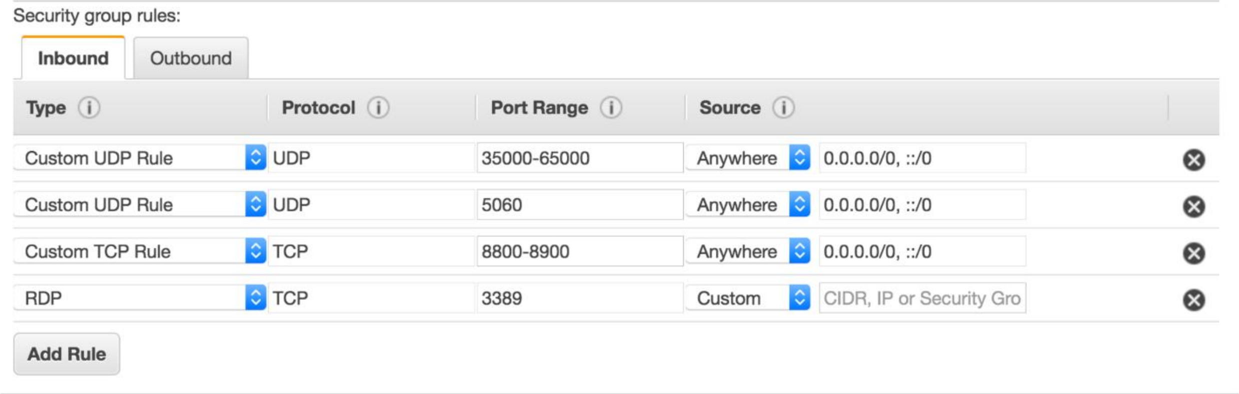
- **Choose an Amazon Machine Image:** The Windows Server 2008 R2 Base 64bit or Windows Server 2012 Base 64bit instance is recommended.

- **Configure Instance Details > Auto-assign Public IP:** Ensure this option is checked.
- **Configure Security Group:** You can simply allow all UDP and TCP ports with below rules:



| Type | Protocol | Port Range | Source | |
|---|---|---|---|---|
| All TCP | TCP | 0 - 65535 | Anywhere | 0.0.0.0/0, ::/0 |
| All UDP | UDP | 0 - 65535 | Anywhere | 0.0.0.0/0, ::/0 |

If you want to control the ports more precisely, you must configure the Security Group as below in order to get the PortSIP PBX works.



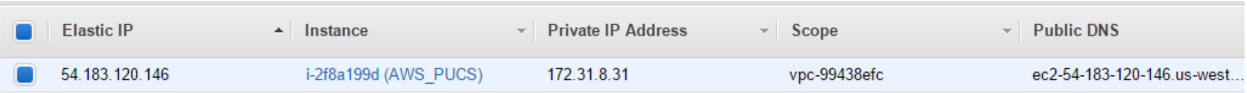
| Type | Protocol | Port Range | Source | |
|---|---|---|---|---|
| Custom UDP Rule | UDP | 35000-65000 | Anywhere | 0.0.0.0/0, ::/0 |
| Custom UDP Rule | UDP | 5060 | Anywhere | 0.0.0.0/0, ::/0 |
| Custom TCP Rule | TCP | 8800-8900 | Anywhere | 0.0.0.0/0, ::/0 |
| RDP | TCP | 3389 | Custom | CIDR, IP or Security Gro |

The UDP rule on 35000 – 65000 ports is used for RTP media relay; The TCP rule on 8800-8900 ports is used for server controls; The RDP rule on port 3389 is used for Windows Remote Desktop; The UDP rule on 5060 port is used for SIP message when your clients register to the PortSIP PBX.

**Note: If you add another transport in PortSIP PBX, for example, to add a TCP/TLS/WS/WSS transport in PortSIP PBX on port 5068, you MUST add a new rule: TCP – 5068;**

- **Create Key Pair:** In the selection of an existing key pair or creation of a new key pair dialog box, you can create a new key pair. Select/Create a new key pair, enter a name for the key pair, and choose **Download Key Pair** to save the key on your PC.

**Step 2:** In the EC2 dashboard, click "**Elastic IPs**", right-click the instance that you created, and choose "**Associate Address**" for it. In the new window, choose the instance and then click "**Associate**" button.



| | Elastic IP | Instance | Private IP Address | Scope | Public DNS |
|---|---|---|---|---|---|
| ■ | 54.183.120.146 | i-2f8a199d (AWS_PUCS) | 172.31.8.31 | vpc-99438efc | ec2-54-183-120-146.us-west... |

Now your **Elastic IP (public IP)** is associated to your instance. Unless you terminate this instance, it will not be released even you stop the instance.

## Install and Setup PortSIP PBX

**Step 1:** Before you use the "**Remote Desktop Connection**" to connect to your AWS Windows server, you should get the default administrator password. Please refer to "**To connect to your Windows instance using an RDP client**" section of Getting Started with Amazon EC2 Windows Instances.

**Step 2:** Use "**Remote Desktop Connection**" to login to your AWS Windows. Please download the PortSIP PBX installer from PortSIP website to your AWS Windows, and double-click it to install. Click **"PortSIP PBX Management Console"** from **"Start"** menu, and enter the default username and password: admin/admin.

**Step 3:** In the step 1 of Setup Wizard, choose “Public Network” for PBX since the AWS is running on internet. Enter the Elastic IP (in this case it’s 54.183.120.146) for " **Public IP**. Click "**Next**" button.

**Note: Do choose the right network type (public network or private network), otherwise the PBX will not be able to work properly.**

**Step 4:** In the step 2 of Setup Wizard, enter SIP domain that you would like to use. You can use the IP address you entered in step 1 as SIP domain, or a FQDN for SIP domain. The SIP domain is used for PBX only, which does not have to be resolvable.

**Step 5:** In the step 3 of Setup Wizard, you’re recommended to use the default transport settings (UDP on 5060). Click "**Apply**" button to complete the Configuration Wizard.

**Step 6:** In the step 4 of Setup Wizard, enter the settings for mail server if necessary. This step is not mandatory.

**Step 7:** In the PortSIP Management Console, choose "**Call Manager**" **>** "**Extensions**" to create the extensions. For example, 101 and 102.

Now you can use any SIP client/SIP IP Phone to register to your PortSIP PBX with extensions that you created.

## Use SIP client to login to PortSIP PBX

**1** Download and install PortGo from PortSIP Website, App Store, or Google play. In the login window, enter below information:

**Username** – The extension number. In this case, it’s 101.

**Password** – The password for extension 101.

**SIP Server** – The PortSIP PBX public IP. In this case, it’s 54.183.120.146, and server port is 5060.

**SIP Domain** – The domain that you set in the step 2 of Configuration Wizard.

**Transport** – Default as UDP.

**2** You can download and install other SIP softphone such as Counterpath XLite/Bria, or Yealink, GrandStream, Snom, Polycom, Cisco IP Phone to register to PortSIP PBX.

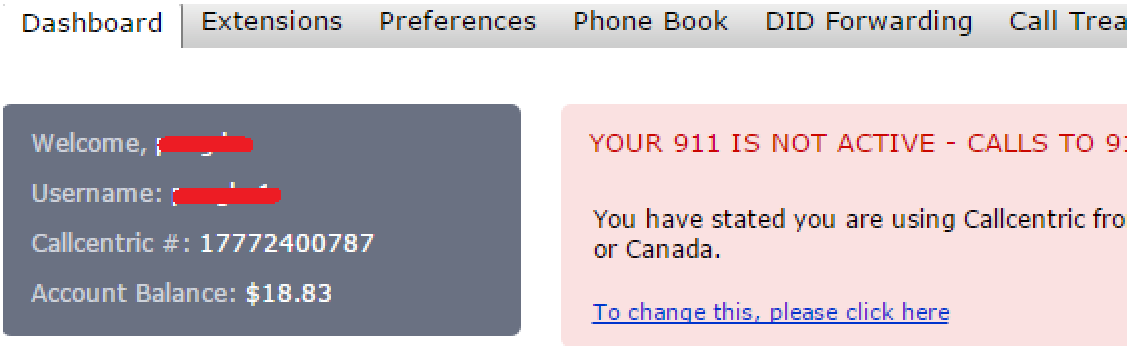
## Sign up for VoIP Provider/SIP Trunk Account

In order to make and receive the PSTN phone calls, we need to sign up for an account from a provider/SIP Truck. In this case we will use Callcentric as an example.

Callcentric provides Voice over Internet Protocol (VoIP) phone service to residential and business customers worldwide. Please follow Sign up Callcentric account instructions.

After you sign up the Callcentric account, you should purchase a phone plan and phone number (DID) for making and receiving the PSTN phone calls. More details please ask Callcentric support. Below is an example.

After you sign in Callcentric Dashboard, please remember your **Callcentric #.** In this case it’s **17772400787**, and we assume the phone number (DID) as **15169261408** for our next step.



Welcome, [redacted]

Username: [redacted]

Callcentric #: 17772400787

Account Balance: $18.83

YOUR 911 IS NOT ACTIVE - CALLS TO 9

You have stated you are using Callcentric fro or Canada.

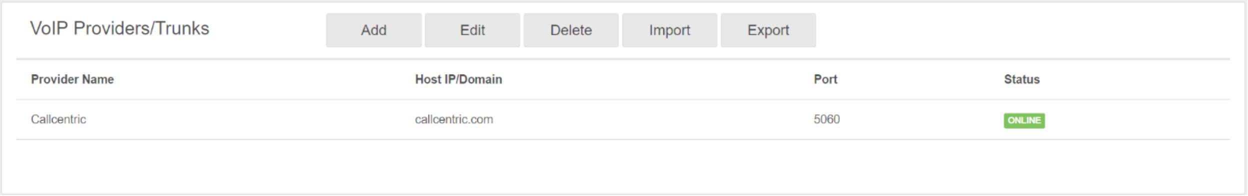
To change this, please click here

## Configuring VoIP provider/SIP Trunk

1 Select the **"Call Manager" > "VoIP Providers/SIP Trunks" > "Add ".**

2 Enter a friendly name for "Provider name" filed, choose "US" for "**Country**" filed and "Callcentric" for "**Provider**" filed. Enter Callcentric# 17772400787 in "UserName ID" filed and password of 17772400787, and keep other settings as default. Click "**Apply**" button to complete the process.

Click "**Call Manager" > "VoIP Providers/SIP Trunks"**, and the added VoIP Providers and SIP Trunks will be displayed. The VoIP provider status will be updated to Registered if it is successfully registered to Callcentric.



| Provider Name | Host IP/Domain | Port | Status |
|---|---|---|---|
| Callcentric | callcentric.com | 5060 | ONLINE |

## Configuring Inbound Rules

Select the "**Call Manager" > "Inbound Rules" > "Add Inbound Rule"**, and fill in below fields:

- **Name:** Enter a friendly name for it.
- **Type:** Choose "DID ".
- **DID/DDI number mask:** Enter DID number **15169261408**.

- **Apply rule to these VoIP Providers/SIP Trunks:** Choose the provider/SIP trunk this inbound rule will be applied to. In this case choose “Test_CallCentric” that we added before.

- **Office Hours:** Choose where the incoming call will be routed to in office hours. In this case, please choose extension 101 for "**Connect to Extension**".

- **Outside of Office Hours:** Choose where the incoming calls will be routed to when outside of office hours. In this case, please choose "**End call"**.

Click "**Apply "** button to save the inbound rule.

The Callcentric will forward the call to PortSIP PBX if someone makes call to the DID **15169261408**. PBX will check the inbound rule when receiving calls from Callcentric: If the rule is matched and current time is in the office hours or the office hours is not set, the call will be forwarded to extension 101, the extension 101 can answer this call from an SIP client (softphone/IP Phone). If current time is outside the office hours, the call will be ended by PBX.

## Configuring Outbound Rule

When the PortSIP PBX receive calls from extension, if below rules matched, the call will be route to Callcentric provider:

1 The dialed number is start with "00".

2 The call comes from extension 101, 102 or 110-120;

Now select "**Call Manager" > "Outbound Rules" > "Add "**, and enter below information:

- **Name:** Enter a friendly name for it.

- **Calls to numbers started with prefix:** Enter 00.

- **Calls from extension(s):** Enter **101,102,110-120**.

- **Make outbound calls on:** In the Route 1, choose the added Callcentric provider. If you want the PortSIP PBX to remove the prefix "00" from the dialed number, select "**2**" for "**Strip Digits**".

Click "**Apply "** button to save outbound rule.

Now if a call which comes from extension 101 or 102, or one of 110-120, is dialed to 00017688902, it will be routed to the Callcentric provider, and the dialed number will be modified to 017688902 (the prefix 00 is removed).

## Multiple Transports

With the default settings of PortSIP PBX, there will be only one UDP transport enabled, you can add more transports to the PBX, such as TCP and TLS.

**To add the TCP transport:**

1 Select "**Call Manager" > "Domains and Transports" > “Transports” > "Add "** in PortSIP PBX Management Console.

2 Choose TCP from "**Protocol**" drop-down list.

3 The default port is 5063 for TCP.

Click the "**Apply"** button to save the TCP transport.

You can use a SIP client/IP Phone to register to PortSIP PBX over TCP transport.

**To add the TLS transport:**

Please read 4.6 section for information about adding the TLS transport .

## Large-Scale deployment on AWS

This section provides full information about how to customize and manage large-scale deployments of PortSIP PBX on AWS, e.g. how to handle more than 10,000 concurrent calls.

## Mode 1: Use "Auto-Scaling"

Since the AWS is cloud platform, it offers the **"Auto-Scaling"** feature, which you can simply use the **"Auto-Scaling"** in the EC2 Management Console to enable: For more information, refer to Getting Started with Auto Scaling.

## Mode 2: Scaling Media Server and Conference Server

We can also scale the PortSIP PBX on AWS EC2 as similar to Section 12.3.

### To scale the Media Server:

**Step 1:** Download the standalone PortSIP Media Server installer at PortSIP Website.

**Step 2:** Select “**Settings**” > “**Media server**” in PortSIP PBX Management Console, and the media servers will be displayed. Click the “**Enabled**” switch from **"Built-in Server"** to disable the default media server. Click "**Apply**" button.

**Step 3:** Launch a new AWS EC2 instance and have it associated with the Elastic IP. Remember the Elastic IP. Install the standalone Media Server on the new instance. Do remember to enable UDP ports 45000 – 65000 and TCP port 8896 in the firewall settings.

**Step 4:** Click "**Settings" > “Media Server” > "Add Server"** in PortSIP PBX Management Console, and enter a friendly name, IP and port 8896 for the new AWS instance that you installed the Media Server.

**Step 5:** By repeating Step 3 and Step 4 you can add more media servers.

Once set, the media streams (RTP packets for audio and video) will be relayed by one of the Media Servers with media servers loads. The signaling (SIP) for both caller and callee still goes through PortSIP PBX, but the media streams handled by separate media servers will not go through PortSIP PBX server.

### To scale the Conference Server:

**Step 1:** Download the standalone PortSIP Conference Server installer at PortSIP Website.

**Step 2:** Select “**Settings**” > “**Conference server**” in PortSIP PBX Management Console, and the Conference servers will be displayed. Click the “**Enabled**” switch from the **"Built-in Server"** to disable the default Conference server. Click "**Apply**" button.

**Step 3:** Launch a new AWS EC2 instance with the Elastic IP associated. Remember the Elastic IP for future use. Install standalone Conference Server on the new instance. Do remember to enable the UDP ports 43000 – 44999, 8828 - 8833 and TCP ports 8886 in the firewall settings.

**Step 4:** Click "**Settings" > “Conference Server” > "Add Server"** in PortSIP PBX Management Console, and enter a friendly name, IP address and port 8886 of the new AWS instance that you installed on the Conference Server.

**Step 5:** By repeating Step 3 and Step 4 you can add more Conference Servers.

# Activating your License

Without a license, PortSIP PBX could work for up to 3 simultaneous calls. If you require more, you will need to activate a license.

Feel free to contact sales@portsip.com to purchase the license.

Once you have received the license key, please go to PBX Management Console, click the menu “Settings”->”License”, and enter the key received.

PortSIP PBX requires internet connection with http://service.portsip.com:6881 to verify the license key periodically. Please ensure that your PBX server could be connected to http://service.portsip.com:6881 smoothly. If the license key verifications fails, the PBX will be downgraded to free version which only allow maximum 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.

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