

# First Steps after Installation Guide

---

## Index

- [1. Login to your IVR](#)
- [2. License activation](#)
- [3. Security Recommendations](#)
- [4. Configure your first extension or SIP device](#)
- [5. Configure your first SIP trunk](#)
- [6. Configure your first VoiceXML application](#)

---

## About us

Interactive Powers, SL (EUR)  
Calle Magallanes, 13 5º Izq  
28015 Madrid (Spain)

Interactive Powers, LLC (USA)  
2320 Ponce de Leon Blvd.  
Coral Gables, FL 33134 (United States of America)

Website:

<http://www.ivrpowers.com>

Contact us:

[info@ivrpowers.com](mailto:info@ivrpowers.com)

# 1. Login to your IVR

Using another machine on your same network, open a web browser and enter the IP address of your server.

If you don't know the IP address of your server, go to the Linux console/command prompt. Login to the Linux console using the username "root" without quotes, and the root password you selected during installation. You will then be shown your IP address (your-ip-address).

Open your web browser and go to the localhost URL:

`http://your-ip-adress`

Login with the username and password you just created.

Administrator User: admin / admin2015!

Test User: user / user2015!

Demo User: demo / demo

## 2. License activation

Once installed, your platform can work with only one evaluation port. You can test all features but your IVR will only manage one simultaneous call. The evaluation period is not limited, you can contact IVRPOWERS at anytime to activate your platform once you have make all tests and you require to deploy your own services.

### **Register and license activation**

To order a Commercial License for increase the maximum number of sessions (voicexml ports) supported ,you need to send us your server identification <code> (Settings > VoiceXML Settings > Licence). Once the code is displayed, copy the code and send it by email to support. Please also include information about your reference installation, such as a purchase order number or the context of the installation.

Contact with us at:

Website:

<http://www.ivrpowers.com>

Email:

[info@ivrpowers.com](mailto:info@ivrpowers.com)

After payment has been received for the product, the support will send you the license key as soon as possible. Information on how to set up your license will be emailed to you, along with your license key.

To set your activation <key> you must update the key field in the License section:

## **Apply Changes and Restart Interpreter**

Remember to "Apply Changes" and "Restart Interpreter". These two actions will stop all calls in progress and will reset your platform processes in order to apply your license.

## **3. Security Recommendations**

The bundle already comes with some security measures by using Fail2Ban. Despite these default security rules, we advise you to follow the following recommendations to make an even stronger platform.

### **Passwords**

Use Long passwords (30+ characters) for the root password, the GUI web interface, all trunks, and all extensions.

### **Web Passwords**

In Admin -> Administrators, create a new user with a name other than "admin" with full privileges. Delete "admin" user. This will protect you against robots that are scanning port 80 for server installations and hacking the "admin" user. If you forget your admin password, you can disable the use of passwords temporarily by issuing the following command from the command prompt:

```
# amportal admin auth_none
```

Then access the web interface and change the admin password

When you're ready to start using passwords again, type this at the command prompt:

```
# amportal admin auth_database
```

### **Root Password**

Change your root password from command prompt, type "passwd" without the quotes while logged in as root.

## Port Forwarding

Port forwarding is generally not necessary and substantially increases security risks. If you need remote access to web interface or via SSH, configure a VPN. You can install OpenVPN and many routers include PPTP and L2TP.

## Restrict SSH

Create another user on the Linux machine with a long, unusual name and a long password. Disable root access via SSH. Use su command for root access when SSH. Consider changing SSH Port. <http://wiki.centos.org/HowTos/Network/SecuringSSH>

## Change SIP Signalling Port

Settings -> Asterisk SIP Settings -> Bind Port: Change to something other than 5060. If done, all devices must be updated to register to new port.

## Configure IPTables

Configure IPTables to restrict inbound traffic to allow only UDP Port 5060 (or whatever you changed it to, above).

## 4. Configure the watchdog

A watchdog is a system that checks the proper functioning of the platform and if something happens, relaunches all the necessary components. By default we are setting the checking rate to 30 minutes. If you think this is not enough for your platform, please refer to our configuration guide ([Configuration Guide](#)) to check how to modify it.

## 5. Configure your first extension or SIP device

### Add an Extension

Menu: Applications -> Extensions

This option is not recommended for non-expert FreePBX / Asterisk users.

Connecting a SIP extension is not part of an IVR and will require to add security to your hosted platform.

## 6. Configure your first SIP trunk

Your IVR requires to be connected to a trunk in order to receive or make calls. The platform is based on FreePBX trunk configuration. You will have to contact us or your local operator to set properly the SIP trunk. This section provide a short example from Voztelecom (IP Operator).

Peer example:

```
username = 3400003942
type = peer
secret = XXXXX
host =voztele.com
fromuser = 3400003942
registry string = 3400003942:XXXXX@voztele.com/917713000
telephone number = 917713000
```

Note:

The secret field is a alpha-numeric (5).

### Add an Inbound Trunk

Menu: Connectivity -> Add Trunk

Mandatory fields are:

General Settings:

- **Trunk Name:** VozTelecom IN
- **Continue if Busy:** check the box

Outgoing Settings:

- **Trunk Name:** voztele-in
- **PEER Details:**

```
username=3400003942
type=peer
host=voztele.com
fromuser=3400003942
```

Registration:

- Register String: 3400003942:XXXXX@voztele.com/917713000

## **Add an Outbound Trunk**

Menu: Connectivity -> Add Trunk

Mandatory fields are:

General Settings:

- **Trunk Name:** VozTelecom OUT

Outgoing Settings:

- **Trunk Name:** voztele-out

- **PEER Details:**

```
username=3400003942
type=peer
secret=XXXXX
host=voztele.com
fromuser=3400003942
```

Registration:

- Registrar String:

## **Apply Changes**

The last step will be to press the button "Apply Changes" in the menu bar.

## **7. Configure your first VoiceXML application**

To connect a VoiceXML service to your platform you have to:

### **Add a new VoiceXML Application**

Menu: Connectivity -> VoiceXML

Local VoiceXML scripts (editor directory) stored inside your platform will start with:  
http://localhost/vxml/

Mandatory fields are:

- **Name:** Helloworld
- **URL:** http://localhost/vxml/helloworld.vxml

More:

- **Max Sessions:** [1.. n] set the number of sessions (simultaneous call for this application

Note:

By default, your application will run with the total number of ports purchased for your platform.

## Add a Misc Application

Menu: Applications -> Misc Application

Mandatory sections and fields are:

- **Description:** My First Misc Application
- **Feature Code:** 917713000
- **Feature Status:** Enabled
- **Destination:** VoiceXML Application > HelloWorld

Note:

DID Number must be assigned to an existing registered SIP trunk.

## Add a Number

Menu: Connectivity -> Numbers

Mandatory sections and fields are:

Add Incoming Number:

- **Description:** My First Number
- **DID Number:** 917713000

Set Destination:

- VoiceXML Application > HelloWorld

Note:

DID Number must be assigned to an existing registered SIP trunk.

## **Apply Changes**

The last step will be to press the button “Apply Changes” in the menu bar.