We Focus·We Deliver

We Focus· We Deliver

UC520

UC510/UC520
IP Office for SOHO

Firmware Version V1.0.8

Safety Notice

Please read the following safety notices before installing or using this device. They are crucial for safe and reliable operation of the device. Failure to follow the instructions contained in this document may result in damage to your device and void the manufacturer's warranty.

1. Please use the external power supply which is included in the package. Other power supplies may cause damage to the device, affect the performance or induce noise.
2. Before using the external power supply in the package, please check your building power voltage. Connecting to Inaccurate power voltage may cause fire and damage.
3. Please do not damage the power cord. If the power cord or plug is impaired, do not use it. Connecting a damaged power cord may cause fire or electric shock.
4. Ensure the plug-socket combination is accessible even after the device is installed. In order to service this device it will need to be disconnected from the power source.
5. Do not drop, knock or shake the device. Rough handling can break internal circuit boards.
6. Do not install the device in places where there is direct sunlight. Also do not place the device on carpets or cushions. Doing so may cause the device to malfunction or cause a fire.
7. Avoid exposing the device to high temperature (above 40°C), low temperature (below -10°C) or high humidity. Doing so could cause damage and will void the manufacturer warranty.
8. Keep this device far away from water or any liquid which would damage the device.
9. Do not attempt to open it. Non-expert handling to the device could cause damage and will immediately void the manufacturer warranty.
10. Consult your authorized dealer for assistance with any issues or questions you may have.
11. Do not use harsh chemicals, cleaning solvents, or strong detergents to clean the device.
12. Wipe it with soft cloth that has been slightly dampened in a mild soap and water solution.
13. If you suspect your device has been struck by lightning, do not touch the device, power plug or phone line. Call your authorized dealer for assistance to avoid the possibility of electric shock.
14. Ensure the device is installed in a well-ventilated room to avoid overheating and damaging the device.
15. Before you work on any equipment, be aware of any hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. If you are in a situation that could cause bodily injury.

Contents

1. Overview

1.1 Brief Introduction of UC510/UC520

UC510/520 is an all-in-one IP office solution for SOHOs (Small Office and Home Offices). The new solution offers not only a Wi-Fi router supports 4G LTE, VPN Client/Server, but also a fully featured IP PBX that can host up to 10 extensions with 2 analog ports connected, and supports Call Forward, Blind/Attendant Transfer, and many other features. UC510/520 is configured and managed through a single web GUI which significantly reduces the time and effort required to install the product. This simplified management and reduction in hardware costs through merging two products into one makes the UC510/UC520 an amazing and cost effective solution for SOHOs.

Telephony Module: Built-in 2 FXO or 1FXOS; LTE is default on UC520.

Model	FXS	FXO	LTE
UC510	1	1	0
	0	2	0
UC520	1	1	1
	0	2	1

1.2Main Features

PBX Features

SIP/IAX extensions
BLF
Voicemail/Voicemail to Email
Call Transfer
Call Forward
Call Pickup
DID
Dial Plan
IVR/IVR Prompts
Inbound Route
Music On Hold
Outbound Route
Ring Group
SIP/FXO Trunk
Time Rule

Router Features

WAN Mode (PPPoE/4G LTE)
Wi-Fi Security
Wi-Fi Advanced Setup
WPS
DHCP Server
Static Routing
Port Forwarding (NAT)
Firewall
VPN(Server/Client)

1.3Hardware Design

UC510 Front Panel

UC520 Front Panel

UC510Rear Panel

UC520 Rear Panel

- Turbo Button
- Power Interface (DC 12V 2A)
- Five Ethernet Interfaces (10/100Mbps)
- Two Analog Ports (FXO/FXS)
- Two USB Ports
- 802.11 b/g/n wireless LAN

UC510/520 LED Indications:

Label	Function	Status	Indication
PWR	Power Status	On	Power On
		Off	Power Off
WPS	WPS Status	On	WSC Succeeded(Off after300s)
		Off	WPS Ready or Disabled
		200ms Blink	WSC Running, Timeout 120s
		100ms Blink	WSC Failed or Timeout 120s
	WAN Data Status	Blink	Data Transmitting

		Off	Line Disconnected
LAN	LAN(1..2..3..4) Data Status	Blink	Data Transmitting
		Off	Line Disconnected
Wi-Fi	Wireless Status	On	Wi-Fi broadcast on
		Off	Wi-Fi broadcast off
1	FXO	On	Channel Available
		Off	Channel Failure
2	FXS	On	Channel Available
		Off	Channel Failure
*3G/4G	3G/4G Status (UC520)	On	Module Detected
		Blink	Module Loading Succeeded or Data Transmitting
		Off	No Module, No SIM card or Module Failure

Notice: WPS (Wi-Fi Protected Setup), WSC (Wi-Fi Simple Configuration)

1.4Environmental Requirements

- Working Temperature: 0 ℃ ~40 ℃
- Storage Tempreture: -20 ℃ ~ 55 ℃
- Humidity: 5~95% Non-Condensing

1.5Packing List

Item	UC510	UC520
Main Case	1 set	1 set
Antenna	2 pieces	3 pieces
Power Supply	1 piece	1 piece
Ethernet Cable	1 piece	1 piece
Quick Installation Guide	1 piece	1 piece
Warranty Card	1 piece	1 piece

2. Getting Started

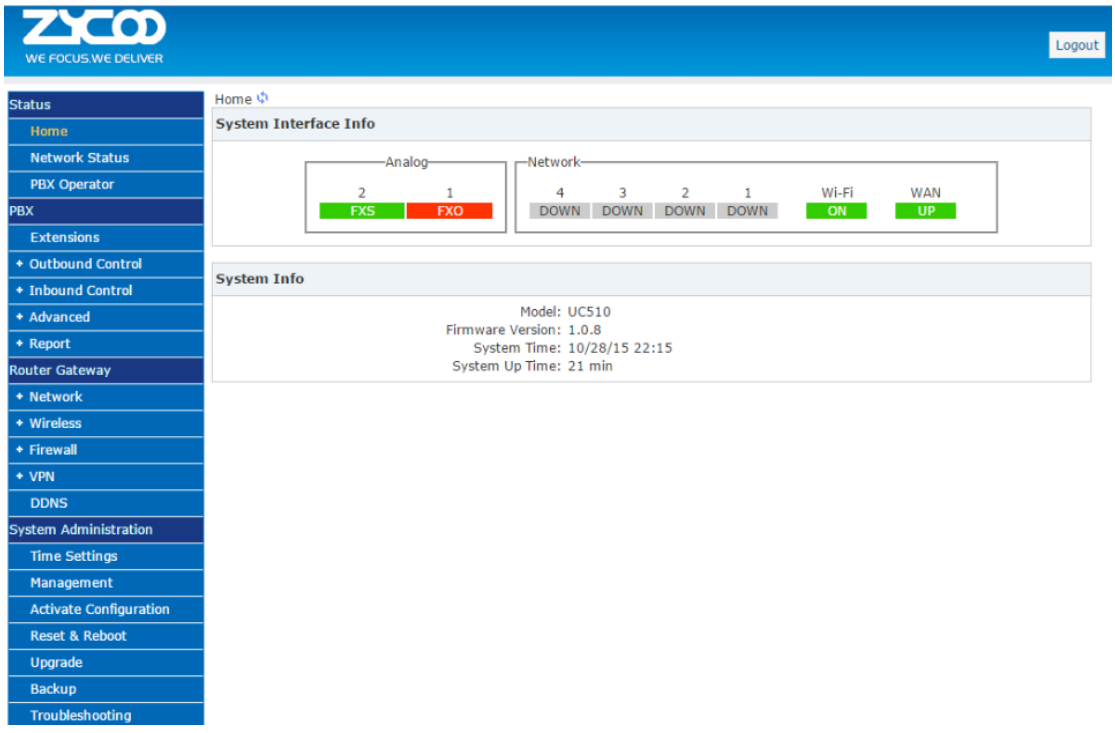
2.1 System Login

Configuration of the UC510 is undertaken through an intuitive Web based GUI. To access this GUI you must first connect a PC directly to one of the UC510 LAN interfaces, or alternatively you can use a laptop to connect to the UC510 Wi-Fi. Default UC510 Wi-Fi SSID is "UC510_AP" and requires no password to connect. Click the  icon on your Windows task bar and click on the wireless network named "UC510_AP"and click "Connect(C)"to connect.

UC510 LAN interfaces are all configured with default IP address of 192.168.1.1, and therefore the default Web GUI login URL is http://192.168.1.1:9999.

The default username is **admin** and password **admin**.

After successful system login, you'll first be asked to change admin password and then subsequently you'll be directed to Status->Home page which provides basic information relating to the UC510 system.



- **System Interface Info**

If an Analog module is installed on the UC510,"FXO" or "FXS" will be displayed at the appropriate position. If no Analogue module is fitted onboard then "N/A" will be displayed.

If a live Ethernet cable is connected on either LAN or WAN,"UP" will be displayed for the relevant port. If no connection is detected on the port then "DOWN" will be displayed.

If Wi-Fi is enabled, "ON" will be displayed and if disabled, "OFF" is displayed.

- **System Info**: displays information relating to device model, system version, system current time and system up time.

2.2 Network Configurations

2.2.1 WAN Configurations

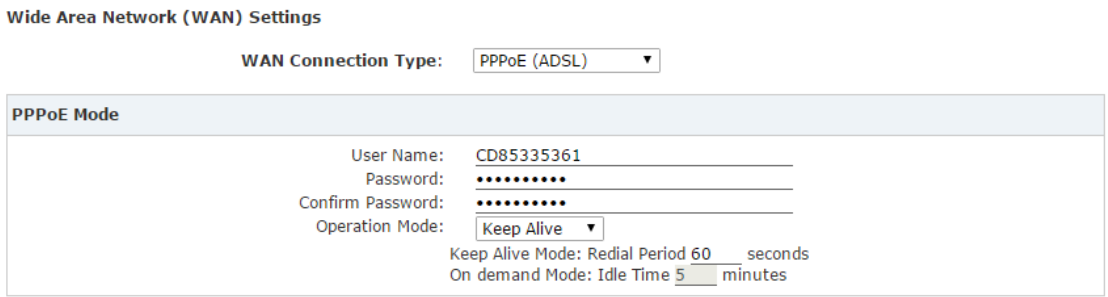
To configure the WAN interface you must navigate to the Web Menu: *Router Gateway->Network->WAN*

UC510 WAN mode can be configured as either Static IP, DHCP, PPPoE or LTE(UC520).

Connection Mode

- STATIC(Fixed IP): If STATIC is selected, a static IP Address must be obtained from your Internet service provider including parameters such as subnet mask, default gateway, DNS.
- DHCP(Auto Config): If DHCP is selected, your Internet connection automatically provides you with a usable IP address.
- PPPoE(ADSL): If PPPoE is selected, the UC510 is connected to the network via ADSL modem by means of Point-to-Point Protocol over Ethernet (PPPoE)dial-up.
- LTE: If LTE is selected, UC520 doesn't require a wired connection for Internet access, it only requires a 4G SIM for 4G wireless connection. (***LTE is only supported by UC520***)

PPPoE



WAN Connection Type please select "PPPoE(ADSL)" and fill in the username and password given by your Internet service provider.

Operation Mode:

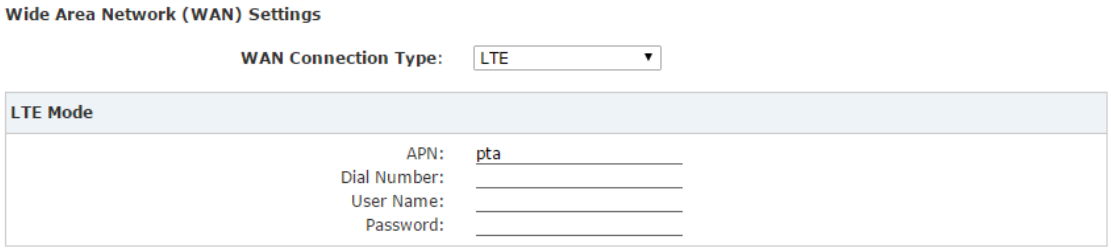
- Keep Alive: While PPPoE is disconnected, system redials every 60 seconds.
- On Demand: If no data transmission through PPPoE on WAN for 5 minutes, PPPoE will be auto disconnected and if data transmission restarts again then the system redials and brings up PPPoE connection automatically.

- Manual: When PPPoE is disconnected, it will remain in this state until you manually reconnect by clicking the "**Save**" button and activate on *System Administration->Activate Configurations* page.

LTE

If your device is UC520, then you can configure 4G LTE as WAN connection for Internet access. First, power off UC520 and insert a 4G SIM card into the SIM slot on the left side of the box and power it on.

Navigate to web menu: *Router Gateway->Network->WAN*



In "WAN Connection Type" field please select LTE. Then provide the necessary information to dial up to your carrier for 4G wireless.

The following information is required to successfully connect to your 4G provider, APN, Dial Number, User name and password.

Each carrier uses its own unique APN Settings to establish connection to their 3G/4G LTE network. For example AT&T requires that you set APN as"phone" or "pta", T-Mobile requires you to set APN to "fast.t-mobile.com". However, username and password may not be always necessary. Most popular carrier settings can be found on Google but if this is not the case then please contact your carrier directly.

After configuration changes are complete, click "Save" button and then any terminals connected to the UC520 will have Internet access through 4G wireless.

Notice: Please make sure the data plan for the 4G SIM is sufficient to meet the demands of the terminals requiring internet access.

MAC Clone

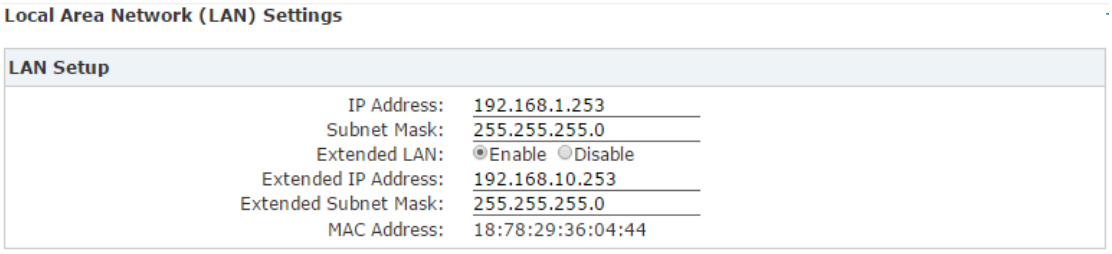
To prevent multiple users from sharing the broadband service, an ISP may need to identify the MAC address of the terminal. UC510can perform MAC address cloning in which the MAC address identified by the ISP can be duplicated to the UC510 WAN interface for network connection and therefore the broadband can be shared with terminals behind UC510.

2.2.2 LAN and DHCP

LAN Configurations

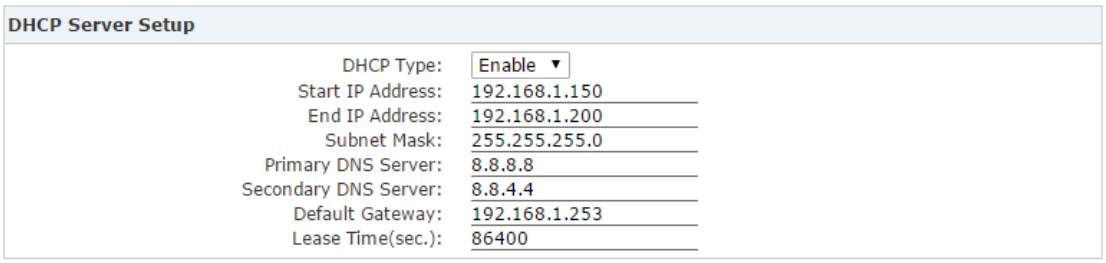
Navigate to Web Menu: *Router Gateway->LAN*

Default LAN IP for UC510/520 is 192.168.1.1, and it can be changed as required.



Notice: If Extended LAN is enabled then a secondary IP can be configured for the LAN interfaces.

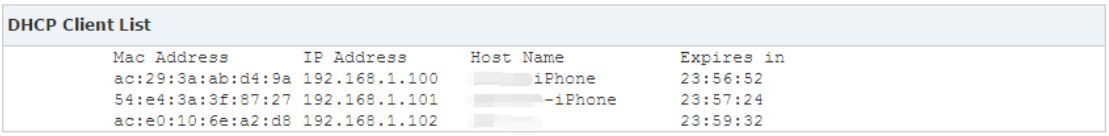
DHCP Configurations



Enable DHCP service if you wish to auto configure IP Addresses for terminals connected with wired and wireless connections. If you want to manually configure fixed IP Address for your terminals then you can disable the DHCP service.

DHCP Client List

Navigate to web menu: *Router Gateway->Network->DHCP Client Info*



This DHCP client page displays a list of all terminals currently connected to UC510 which have obtained IP addresses from DHCP server of UC510.

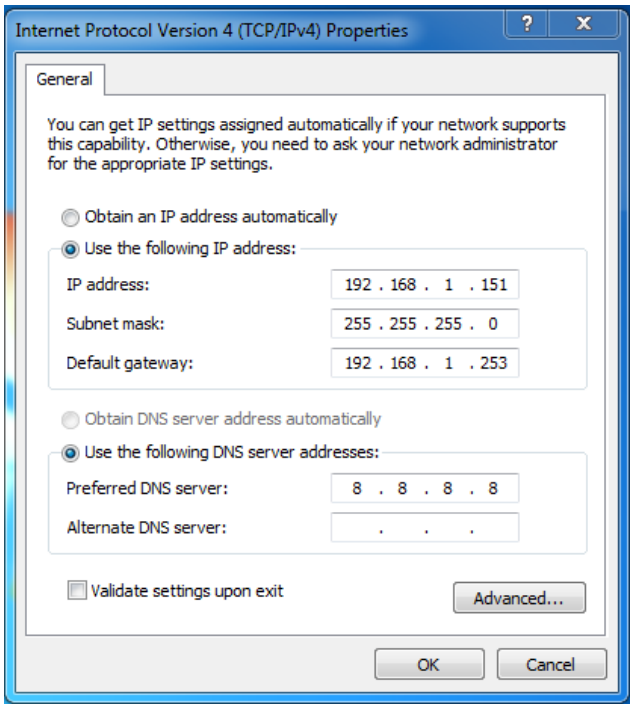
2.2.3 Wired Connections

There are 4 LAN interfaces on UC510 which can be used to connect phones and computers. It is common practice for phones to have their network mode pre-configured as DHCP, and the WAN and LAN interfaces of the phones are often bridged. This enables you to connect the WAN interface of the phone to UC510 LAN port, and LAN port of the phone to a PC. This means with one port you can connect 2 devices and once the network cable is

connected you will have Internet access on your PC. However, if DHCP is not enabled on UC510 LAN interface, then you'll need to manually assign an IP address to the phone and another IP address to the PC.

Please refer to your IP phone user manual for details on how to configure a static IP Address.

To configure a static address on the PC, please click the  icon on your Windows task bar and click "Open Network and Sharing Center" then click "Change adaptor settings", double click on wired or wireless adaptor icon (as appropriate) and click "Properties", and double click "Internet Protocol Version 4(TCP/IPv4)" to manually configure an IP Address as detailed in below example:



In addition to direct connection of devices to UC510, you can also connect a hub or switch to the UC510 LAN interface to expand the number of wired devices that can connect.

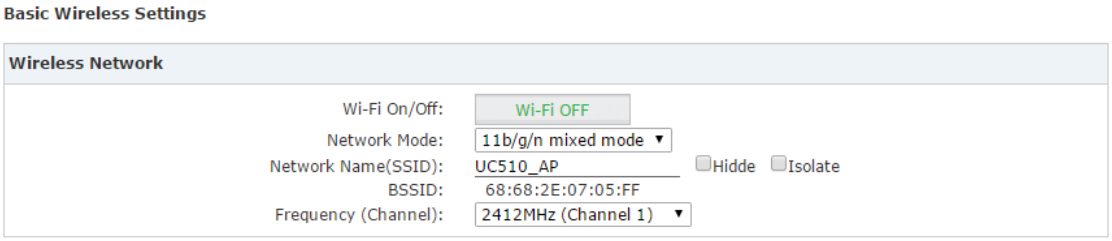
2.3 Wireless

2.3.1 Basic Wireless Network Configurations

Navigate to Web Menu: *Router Gateway->Wireless->Basic*

Wi-Fi broadcast can be turned on or off by clicking "Wi-Fi On" or "Wi-Fi Off" button. If the indicator  on UC510 is on, it means the wireless network is turned on; otherwise, it is

turned off.



Network Mode

- 802.11 b/g mixed mode: The connection of both 802.11b and 802.11g terminals is supported, and the maximum connection rates are 11 Mbps and 54 Mbps respectively.
- 802.11 b only: Only a connection of 802.11b terminal is supported, and the maximum connection rate is 11 Mbps.
- 802.11 g only: Only a connection of 802.11g terminal is supported and the maximum connection rate is 54 Mbps.
- 802.11 b/g/n mixed mode: The connection of 802.11b, 802.11g, and 802.11n terminals are supported, and the maximum connection rates are 11Mbps, 54 Mbps, and 150 or 300 Mbps respectively.
- 802.11 n only: Only a connection of 802.11n terminal is supported, and the maximum connection rate is 150 Mbps or 300 Mbps.

Wi-Fi network modes supported by UC510 include 802.11b/g/n. The mode to be applied depends on the properties of the terminals. By default it is preconfigured to work in 802.11 b/g/n mixed mode.

Network Name(SSID)

SSID is short for service set identifier. It helps Wi-Fi terminals to identify a wireless network to connect to.

- Hide: If selected, the wireless network will be invisible to the Wi-Fi terminals, to connect to UC510 the terminals will have to manually specify the SSID to connect.
- Isolate: If selected, the Wi-Fi terminals will not be able to communicate with each other.

BSSID

BSSID is Basic Service Set Identifier, which is defined as the MAC address of the Wi-Fi router in IEEE 802.11.Its purpose is to define a unique address that identifies the access point/router that creates the wireless network.

Frequency(Channel)

The 2.4GHz Wi-Fi frequency range has been divided into multiple channels with different frequencies by the 802.11 workgroup, the channel list is a set of legally allowed wireless

local area network channels using IEEE 802.11 protocols. Choosing the best Wi-Fi channel on your router can also help reducing interference and improve your Wi-Fi signal.
By default, UC510/520 has been configured to auto select the Wi-Fi channel to be used.

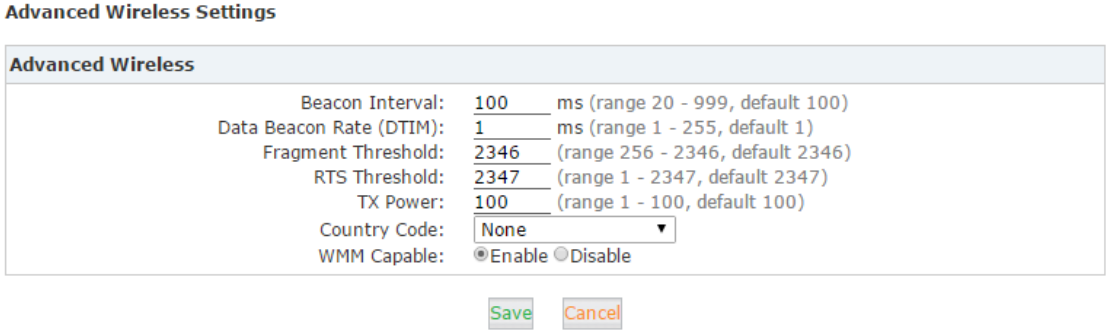
HT Physical Mode

- Channel BandWidth: In 802.11n mode, two 20-MHz channels are bundled into a 40-MHz channel. In reality, the 40-MHz channel can be used as two 20-MHz channels (a primary channel and a secondary channel).Data can be sent and received from the 40-MHz channel or a single 20-MHz channel which doubles the transmission rate and improves the throughput of the wireless network. By default it is configured as 20/40MHz.
- Guard Interval: Is used to ensure that distinct transmissions do not interfere with one another. These transmissions may belong to different users (as in TDMA) or to the same user (as in OFDM).Send interval between the wireless signals; long interval or auto interval is alternative.

2.3.2 Advanced Wi-Fi Options

These advanced Wi-Fi parameters are used to help improve the wireless network performance, if you are not competent with the parameters elaborated below, it is not recommended to change the default values.

Navigate to Web Menu: *Router Gateway->Wireless->Advanced*



Advanced Wireless

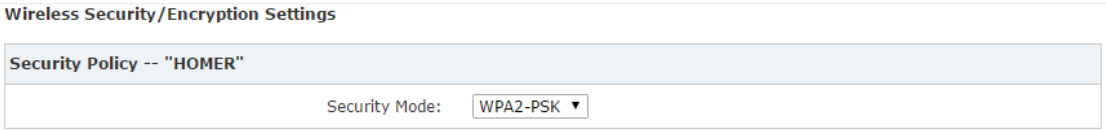
- Beacon Interval: This parameter represents the amount of time between beacon transmissions. The smaller the interval, the faster the access speed of the wireless client. The larger the interval, the higher the data transmission efficiency of the wireless network. The default is 100, and you are not recommended to change the default.
- Data Beacon Rate(DTIM): A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default setting is 1ms.

- Fragment Threshold: Specifies the fragmentation threshold for data packets and when the packet length exceeds fragmentation threshold, it will be divided into several data packets. However, more data packets results in poor performance of the network. The default setting is 2346. It's not recommended to set a lower value.
- RTS Threshold: Specify the RTS threshold for data packets, when the packet length exceeds this value, the router will send the RTS to destination for negotiation, after receiving the RTS frame the wireless site will respond to a CTS (Clear to send) frame in response to the router and the client which confirms there is wireless communication between them.
- TX Power: Defines the distance and range that wireless signals can cover. The default value is 100.
- Country Code: The Wi-Fi allowed channels, maximum regulatory transmit power level, and frequency ranges are regulated on a country by country basis. The listed countries have been approved to operate and fully conform to current country requirements.
- WMM Capable: Wi-Fi multimedia (WMM) is a wireless Quality of Service (QoS) protocol, ensuring the priority of voice and video data transmission. To perform WMM, the wireless client is also required to support WMM. By default, WMM is enabled.

2.3.3 Wireless Security

By default, UC510 does not enable any security mode for authenticating the terminals to connect to its wireless network. After you have connected the Internet for UC510 and with Wi-Fi turned on, it's strongly recommended to enable Wi-Fi security settings.

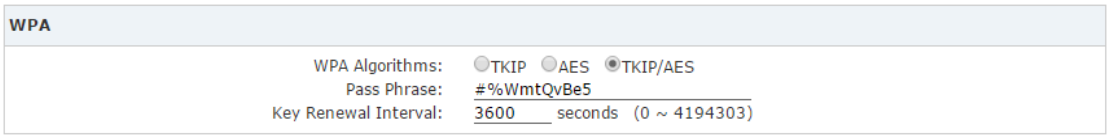
Navigate to Web Menu: *Router Gateway->Wireless->Security*



Security Mode

- WPA-PSK: Wi-Fi Protected Access Pre-shared Key, also referred to WPA-Personal. It is designed for home and small office networks and doesn't require an authentication server.
- WPA2-PSK: is mainly used for enterprise's. Adopt 802.1x for authentication and generating root key for encrypting data, but do not set PSK(pre-shared key) manually. A RADIUS server will replace the single password mechanism in authentication.

WPA



Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

The most common mode is WPA/WPA2-PSKwith the encryption type of TKIP&AES.

WPA Algorithms

- TKIP: TKIP stands for "Temporal Key Integrity Protocol." It was a stopgap encryption protocol introduced with WPA to replace the very-insecure WEP encryption at the time. TKIP is actually quite similar to WEP encryption.
- AES: AES stands for "Advanced Encryption Standard." This is a more secure encryption protocol introduced with WPA2 which replaced the interim WPA standard.
- TKIP/AES: TKIP is an older encryption standard used by the old WPA standard. AES is a newer Wi-Fi encryption solution used by the new-and-secure WPA2 standard.WPA2 uses AES for optimal security, it also has the option to use TKIP for backward compatibility with legacy devices.

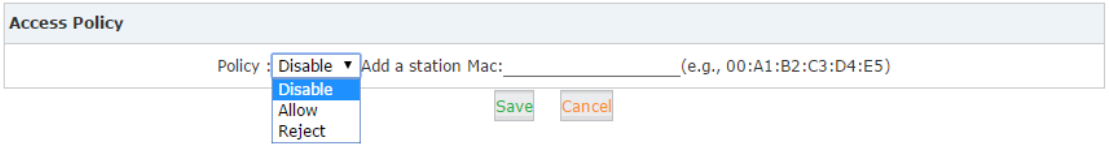
Pass Phrase

A Wi-Fi passphrase is a code required to gain wireless access to your home network. The Wi-Fi password can include numbers, letters or special characters.

Key Renewal Interval

Indicates the interval at which the broadcast and multicast keys are refreshed. Default is 3600 seconds.

Access Policy



By selecting "Allow" or "Reject" and specifying the MAC address will grant or refuse a terminal connection to UC510wireless network.

2.3.4 Connect Wi-Fi

Windows 7

Step 1:

Click the  icon and it will show nearby wireless networks.

Step 2:

Click the wireless network named "UC510_AP" and click "Connect(C)" button.

Step 3:

Enter the password "#%WmtQvBe5", and you will be connected to the device and have access to the internet.

Notice: If DHCP is disabled on *Router Gateway->Network->LAN* page, then you'll need to assign an IP address for your wireless network adaptor. Please refer to chapter 2.2.3.

iPad and iPhone

Step 1:

Tap the 

icon

Step 2:

Tap WLAN menu

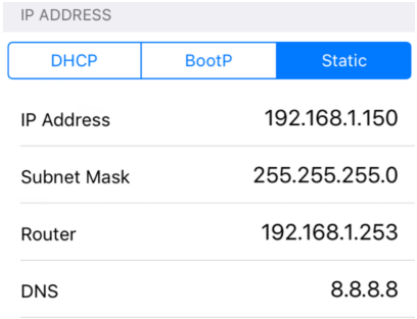
Step 3:

Find wireless network "UC510_AP"

Step 4:

Enter password "#%WmtQvBe5" and you will be connected and have Internet access through UC510 Wi-Fi.

Notice: If DHCP is disabled then you'll need to manually assign an IP address to your iPad or iPhone. In WLAN menu tab  to manually assign an IP address:



- IP Address: Assign an IP Address that is different to the one assigned to the LAN interface of UC510, therefore it cannot be 192.168.1.253.
- Subnet Mask: Defines the network size.

- Router: Gateway, the LAN interface IP, in this example it's 192.168.1.253.
- DNS: The DNS IP Address given by your ISP. This can be found on *Status->Network Status* page. Or other public DNS server, for example Google public DNS server: 8.8.8.8.

Android phones

Step 1:

Open your list of Apps.

Step 2:

Tap 

icon.

Step 3:

Tap 

menu.

Step 4:

Select the wireless network named "UC510_AP" to connect, once connected you have Internet access through UC510 Wi-Fi.

Notice: To apply a manual IP Address on Android phones follow the instructions below.

Step 1:

Tap and hold the network "UC510_AP" until a box appears.

Step 2:

Select Modify Network.

Step 3:

Tap the checkbox next to Show Advanced Options.

Step 4:

Choose Static from the IPv4 settings menu.

Step 5:

Input your static IP Address information.

Step 6:

Tap Save.

2.3.5 Station List

Navigate to Web Menu: *Router Gateway->Wireless->Station List*

The station list page details all devices that are connected using Wi-Fi to UC510.

Station List

Wireless Network			
MAC Address	Connect Time	RX Packets	TX Packets
54:E4:3A:3F:87:27	110	275	442
AC:E0:10:6E:A2:D8	3005	1039385	668051
1C:65:9D:5E:6C:24	2704	12619	9084

2.3.6 WPS

WPS (Wi-Fi Protected Setup) is used to establish encrypted connections between wireless clients and UC510 in a much simpler and quicker way. You are not required to select the encryption type or set a key for WPS. You only need to enter the PIN code or press the WPS button on the back panel of UC510.

Navigate to web menu: *Router Gateway->Wireless->WPS*

Wi-Fi Protected Setup

WPS Config

WPS : Enable

In"WPS Config" section turn on WPS by selecting "Enable".

On UC510 there are three ways to connect Wi-Fi by using WPS facility. Let's take the mobile phone as an example:

1. You can generate a random password from the UC510 GUI, and then you can input the password on your mobile phone to access Wi-Fi.

WPS Summary

WPS Current Status :	Idle
WPS Configured :	Yes
WPS SSID :	UC510_AP
WPS Auth Mode :	WPA2-PSK
WPS Encryption Type :	AES
WPS Key(ASCII):	#%WmtQvBe5
AP PIN :	66400622 Generate

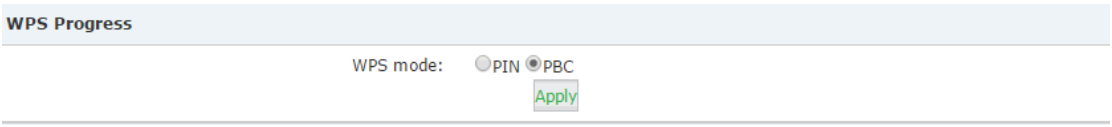
Here in this example you input the password "66400622" on you mobile phone to connect to Wi-Fi.

2. Enter the WPS PIN from the terminal device into your UC510 and click "Apply" button to connect Wi-Fi, as detailed below:

WPS Progress

WPS mode: PIN PBC
PIN: 12345678
Apply

3. If the phone is equipped with a WPS configuration button, please select PBC as the WPS mode and click "Apply"



Once activated, press WPS configuration button on your mobile phoneand UC510 will automatically authorize your phone to access Wi-Fi.

3. Voice

3.1 Extensions

Which devices can you use as an extension on the UC510?

IP extensions

SIP/IAX2 enabled IP phones. For example: Cisco, Grandstream, Yealink, etc.

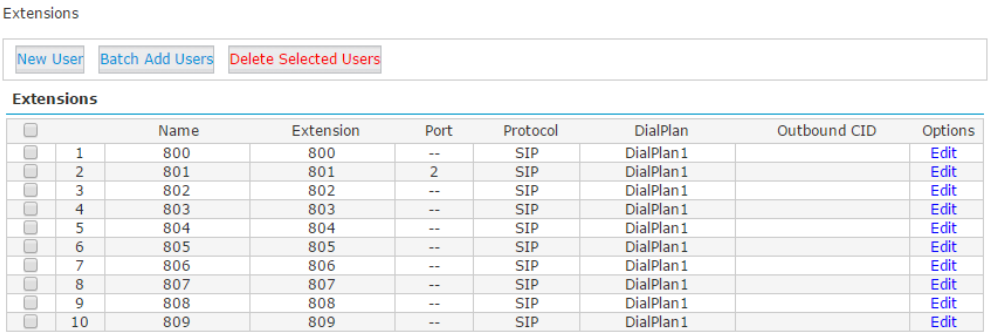
PC, Cell phones, Tablet swith softphone APP installed e.g. 3CX, Bria, Zoiper, etc.

Analog extensions

Ordinary analog phones/Fax Machines.

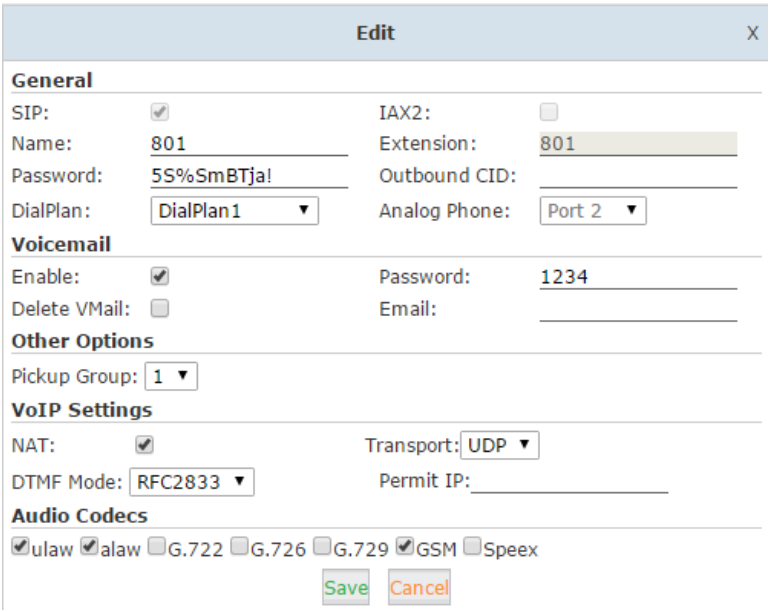
To configure or view an extension, navigate to Web Menu: *PBX->Extensions*

An IP extension can register to UC510 with the existing accounts preconfigured on UC510 system. By default, UC510 supports a maximum of 10 extension numbers.



		Name	Extension	Port	Protocol	DialPlan	Outbound CID	Options
☐	1	800	800	--	SIP	DialPlan1		Edit
☐	2	801	801	2	SIP	DialPlan1		Edit
☐	3	802	802	--	SIP	DialPlan1		Edit
☐	4	803	803	--	SIP	DialPlan1		Edit
☐	5	804	804	--	SIP	DialPlan1		Edit
☐	6	805	805	--	SIP	DialPlan1		Edit
☐	7	806	806	--	SIP	DialPlan1		Edit
☐	8	807	807	--	SIP	DialPlan1		Edit
☐	9	808	808	--	SIP	DialPlan1		Edit
☐	10	809	809	--	SIP	DialPlan1		Edit

Click on "Edit" button and you can check the account info and modify the feature options of this user extension.



Explanations of the configuration options are detailed below:

General

- SIP: Tick the checkbox to activate SIP protocol.
- IAX2: Tick the checkbox to activate IAX2 protocol.
- Name: Alias of this extension, this can be the name of the extension user.
- Extension: Number of this user extension which can be used for phones to subscribe and can be used for others to call this extension.
- Password: The password used on the phones to register.
- Outbound CID: Choose a number to show to the external called party. This feature only works with SIP trunk if the ITSP(Internet Telephony Service Provider) allows this number to be passed.
- DialPlan: Defines which type of numbers the extension can dial.
- Analog Phone: When FXS module installed, the FXS port number, means the analog phone attached to this port will use this extension number.

Voicemail

- Enable: Activate voicemail service for this extension.
- Password: Password for extension user to access the voicemail facilities.
- Delete VMail: Delete the voice messages if system has sent the message to user via email.
- Email: Email address of this extension user.

Other Options

- Pickup Group: Define a pickup group for this extension, extensions in the same pickup group can pickup an incoming call on a ringing extension in the same pickup group using feature code *8.

VoIP Settings

- NAT: Check this option if extension user or the phone is located behind a router.
- Transport: Choose UDP or TCP as the transport protocol for SIP signaling.
- DTMF Mode: Defines how the system will detect the DTMF tones, the default setting is rfc2833, however, it can be changed if necessary.
- Permit IP: Defines which IP address or network address is allowed to register to this extension number, other Addresses will be rejected. It can be private IP or public IP.

Audio Codecs

UC510/UC520 supports audio codecs: ulaw, alaw, G.722, G.726, G.729, GSM and Speex. You can select the one/ones you want to use.

3.1.1 IP Extension Registration

CooFone IP phones

Below is an example of how to configure a Zycoo CooFone to register with UC510

Step 1:

Press the softkey "Status" beneath the phone screen, here you can see the IP phone IP address.

Step 2:

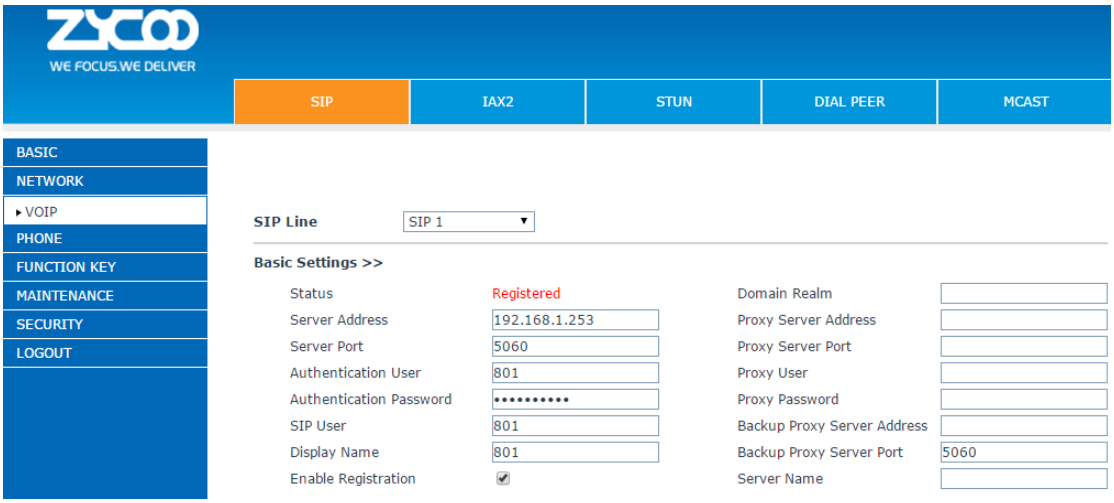
Open the IP phone web interface by entering the phone IP address into the web browser address bar.

Step 3:

Default login credentials are username admin and password admin.

Step 4:

After login, you must navigate to the phone web menu *VOIP->SIP*, and register an extension number as below example.



- Server Address: LAN IP of the UC510.
- Server Port: SIP service port number, by default it's 5060, you are not required to change this as 5060 is standard.
- Authentication User: User extension number from the UC510 user extension page.
- Authentication Password: The password of the extension number.
- SIP User: The same as Authentication user.
- Display Name: Name of the extension user.
- Enable Registration: Once enabled, the phone will register to UC510 as an extension.

Softphone on Windows PC

The softphone 3CX, Bria, Zoiper and many other softphone APPs all work well with UC510. Below is an example of registering Zoiper to UC510 as an extension from your Windows PC.

Step 1:

Download Zoiper from http://www.zoiper.com/

Step 2:

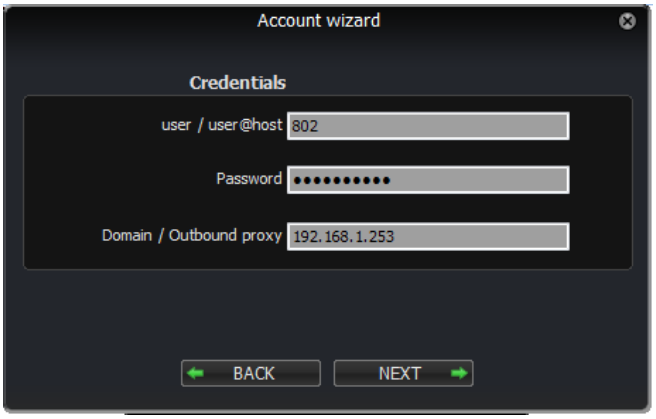
Install and run Zoiper within Windows

Step 3:

Click menu "Settings" and select "Create a new account" and select "SIP" protocol and click Next.

Step 4:

Fill in the register credentials as below



Step 5:

Click Next to complete registration

Softphone on Android phone, iPhone or iPad

Most of the softphones mentioned previously have mobile editions for both Android and iOS platforms. You can download and install them from your mobile phone APP Store. Below is how you register Zoiper softphone to UC510 as an extension from your iPhone:

Step 1:

Run Zoiper on your iPhone and tap Settings menu

Step 2:

Tap Accounts menu

Step 3:

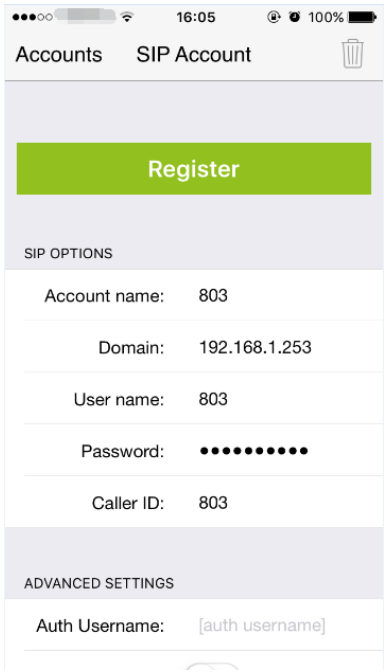
Tap + to create a new account

Step 4:

You will be asked "Do you already have an account(username and password)?" tap "Yes" and then tap "Manual configuration" to continue

Step 5:

Tap SIP account to configure the account as below:



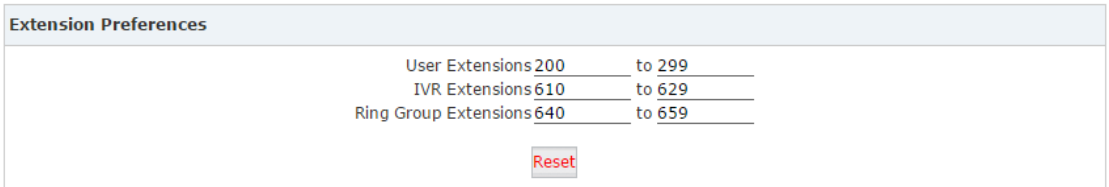
Step 6:

After entering your register credentials next tap Register to register to UC510 as an extension.

3.1.2 What If I Don't Want the Default User Extensions?

Step1:

Navigate to Web menu *PBX->Advanced->Options* page; in "Extension Preferences" section where you can change the user extension range. For example, 200 to 299.



Step2:

Navigate to Web menu *PBX->Extensions* page, select all the existing user extensions and click "Delete Selected Users" button to delete the default extensions.

Step 3:

To create new user extensions, you can click "New User" button to add extensions one by one, or you can click "Batch Add Users" button to add the numbers in bulk. UC510 can only adopt 10 user extensions, if you are adding new users in bulk, please make sure the extension range is within maximum allowance of 10 extensions.

3.2 Outbound Call

3.2.1 Trunks

The UC510 supports FXO trunks and VoIP trunks for outbound phone calls. The FXO trunk refers to the PSTN lines attached to the FXO ports, VoIP trunk(in most cases SIP trunks, but also supports IAX2 trunks) means you can subscribe an account from an ITSP for inexpensive long distance phone calls.

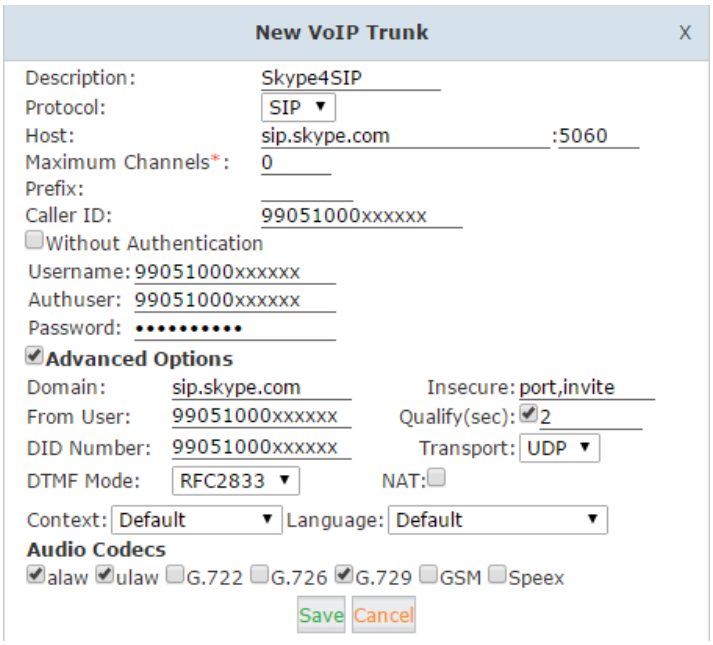
Navigate to Web Menu: *PBX->Outbound Control->Trunks*

Here on this page you can create VoIP trunks and FXO trunks.

VoIP Trunk

UC510 can register as a SIP user agent to a SIP proxy (provider). If you have subscribed to the VoIP service from ITSP, then with the account details given by them you can setup a VoIP trunk on UC510 for the user extensions to share this trunk for making outbound phone calls.

Click "New VoIP Trunk" button and fill in the account details to setup the trunk.



- Description: A name for this trunk.

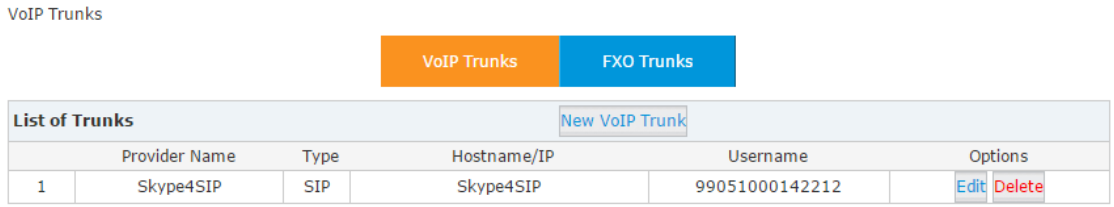
- Protocol: SIP or IAX2 protocol to be chosen.
- Host: The SIP server domain or IP address.
- Maximum Channels: Maximum calls that can be made through this trunk at the same time, 0 means unlimited.
- Prefix: The numbers specified here will be added to the number you dial. Usually you don't need this prefix so please leave this field blank.
- Caller ID: The number you want to display to the called party.
- Without Authentication: If the service provider doesn't need any username and password for this account to register to their server, you can enable this option.
- Username: Username provided by VoIP Provider.
- Authuser: The optional authorization user for the SIP server
- Password: Password provided by VoIP Provider.

Advanced Options

- Domain: The domain is where you register your username.
- Insecure: Default value is "port, invite";"port"--Allow matching of peer by IP address without matching port number; "invite"--Do not require authentication of incoming INVITEs.
- From User: fromuser=yourusername; Many SIP providers requires this.
- Qualify(sec): Asterisk based servers regularly send a SIP OPTIONS command to check that the device is still online. Default value is 2(sec).
- DID number: Self defined, it can be used to setup number DID.
- Transport: Default transport type for SIP messages.
- DTMF Mode: Used to tell the system how to detect the DTMF(Dual Tone Multi Frequency) key press. Choices are inband, rfc2833, or info. By default we use RFC2833.
- NAT: With this option enabled, Asterisk may override the address/port information specified in the SIP/SDP messages, and use the information (sender address) supplied by the network stack instead. Typically needed when behind a firewall router.
- Context: Custom dial plan for this trunk, by default it's using the "default" dial plan. Configure only if this trunk is for branch office integration, so the calls coming from the other side can dial out from this IPPBX trunk directly. DO NOT change it unless you understand how exactly this option works.
- Language: You can choose your language here and the system will interact with the incoming calls from this trunk with the voice prompts you selected.
- Audio Codecs: Select the audio codec/codecs that your provider can support.

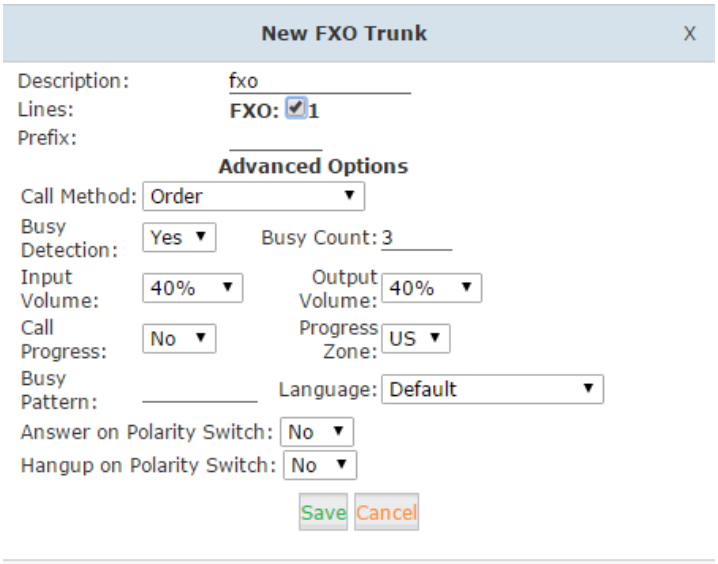
With the exception of configuration options related to the service provider and your account details. Please do not change the trunk advanced parameters unless you are familiar with them. After the SIP trunk is successfully added it will be listed as shown

below.



FXO Trunks

Click the "FXO Trunks" tab and click "New FXO Trunk" to add a FXO trunk. This will allow you to make calls through the PSTN line attached to the UC510 FXO port/ports.



- Description: A name for this FXO trunk.
- Lines: Available FXO port/ports. If you have only one FXO then only one can be selected here, if you have two then there will be 2 ports that can be selected.
- Prefix: The numbers specified here will be added to the number you dial. Usually you don't need this prefix please leave this field blank.
- Call Method: Configurable if you have 2 FXO ports, it defines how to use two ports for outbound phone calls.
- Busy Detection: Enable busy tone detection, it is also possible to specify how many busy tones to wait for before hanging up.
- Busy Count: Specify how many busy tones to wait for before hanging up, configurable only if Busy Detection is enabled.
- Input Volume: The volume of the calls from FXO channel/channels which have been received.
- Output Volume: Controls the volume level of the calls from FXO channel/channels.
- Call Progress: If enabled, call progress attempts to determine answer, busy, and ringing on phone lines. This feature is HIGHLY EXPERIMENTAL and can easily detect false answers and therefore it is not recommend to use this feature as it can produce

unreliable results.

- Progress Zone: Progress zone also affects the pattern used for busy detection, only effective when Call Progress in turned on.
- Busy Pattern: If busy detect is enabled, it is also possible to specify the cadence of your busy signal.
- Language: You can choose your language here and the system will interact with the incoming calls from this trunk with the voice prompts you selected.
- Answer on Polarity Switch: For FXO (FXS signaled) ports, this setting when enabled watches for a polarity reversal to mark when an outgoing call is answered by the remote party.
- Hangup on Polarity Switch: In some countries, a polarity reversal is used to signal the disconnect of a phone line. If the hangup on polarity switch option is selected, the call will be considered "hung up" on a polarity reversal.

While creating a FXO trunk, if you are not competent with the advanced options please do not configure or change the default values.

3.2.2 Outbound Routes

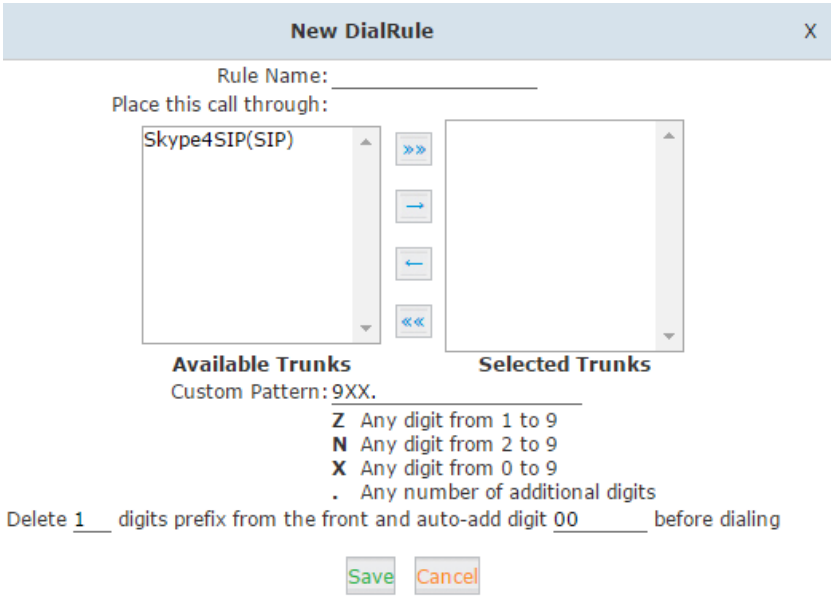
Outbound Routes are a collection of outbound dial rules and dial plans for the IPPBX system to allocate outbound dialing permissions to extensions.

Dial Rules

First you'll need to create dial rules.

Navigate to Web Menu: *PBX->Outbound Control->Outbound Routes->Dial Rules*

Click New "DialRule" button to create a new dial rule.



In "Rule Name" field, specify a name for this dial rule and select an available trunk or alternatively select more than one trunk to the "Selected Trunks" column. Then define a custom pattern for this dial rule which defines what pattern of numbers the system expects to see before passing the call over the selected trunk. Dial patterns act like a filter for matching numbers dialed with trunks. The various patterns you can enter are similar to Asterisk's definition of them:

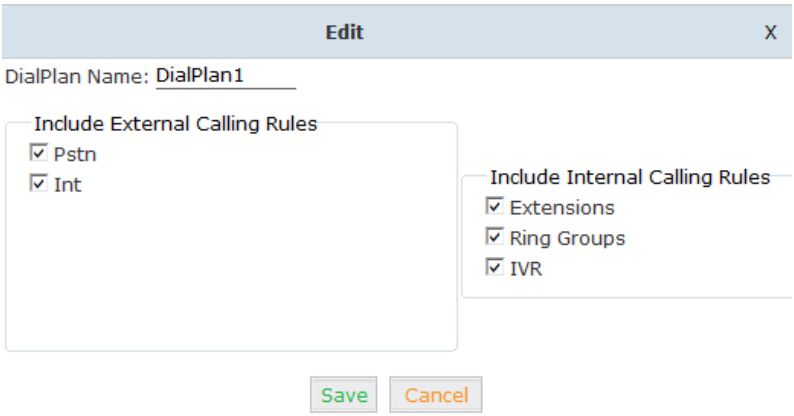
- X — Refers to any digit between 0 and 9
- N — Refers to any digit between 2 and 9
- Z — Any digit that is not zero. (E.g. 1 to 9)
- . — Wildcard. Match any number of anything. Must match *something*.

"Delete ____ digits prefix from the front and auto-add _____ digit before dialing". The first blank allows you to strip some digit/digits before dialing out, here if required, you need to complete the number of digits to delete. The second blank is to prepend some digit/digits before dialing out, here you need to fill in the exact number of digits to be added in front of the dialed number.

For example a user dialing 912345678 using the dial rule introduced above, the prefix 9 at the first digit will be removed, and 00 will be added, so eventually the number called will actually be 0012345678.

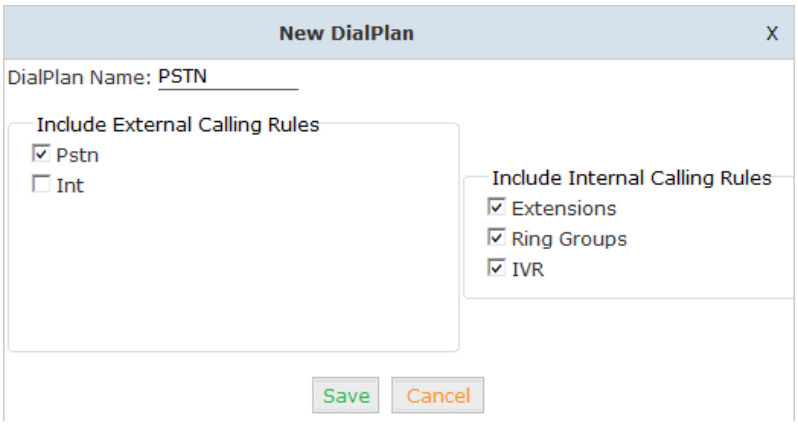
Dial Plans

Usually the default dial plan "DialPlan1" is applied for all the user extensions, you just have to click the "Edit" button and enable the dial rules you created, then users will be able to make outbound calls according to the dial rules included in this dial plan.

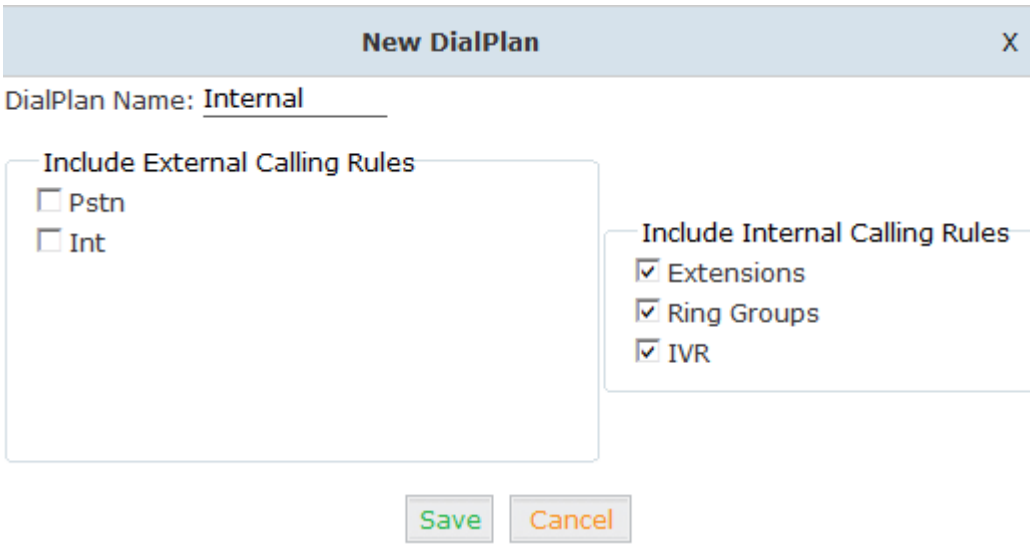


If you want to restrict user access so they are unable to make calls through one of the trunk or some of the trunks, you can click "New DialPlan" button to add a new dial plan for them, in this new dial plan you enable the dial rule/dial rules you want them to be able to use for making outbound calls.

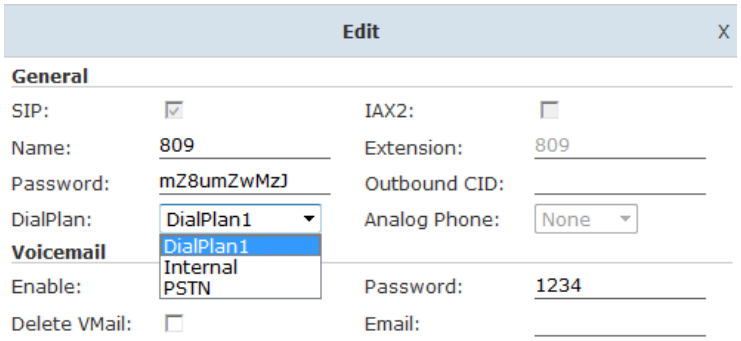
Below is the example of the new dial plan:



If you want to restrict outbound calls altogether for certain users but still allow internal extension to extension calls, you can create a new dial plan without enabling any outbound dial rules.



After creating the new DialPlan, navigate to web menu: *PBX->Extensions*, click "Edit" button and select the appropriate dial plan for the extensions as below:



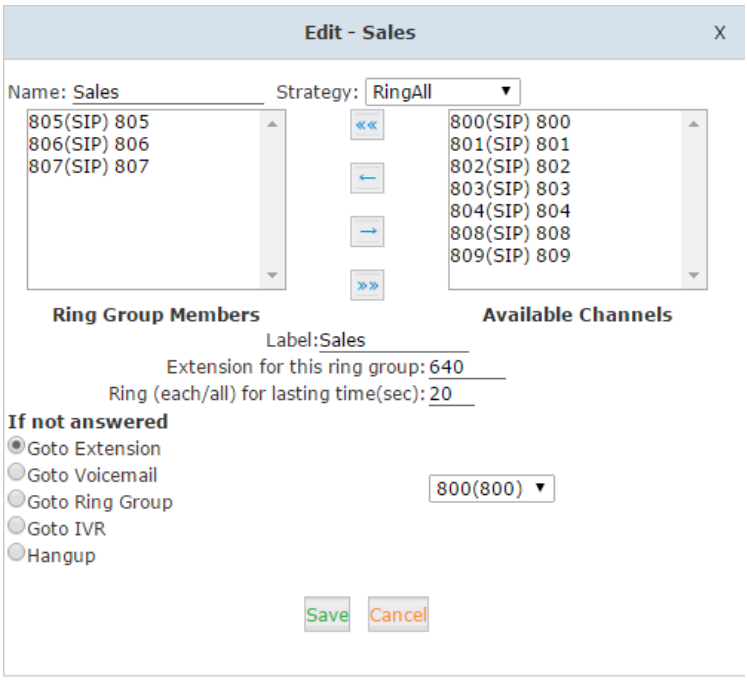
After the above configurations, then user extensions will be able/unable to make external phone calls based on the dialplan set on their extension.

3.3 Inbound Control

3.3.1 Ring Groups

In a ring group, an incoming call will ring the phones of everyone in the group at the same time. To configure a ring group please navigate to web menu: *PBX->Inbound Control->Ring Group*

Click "New Ring Group" button to add a ring group.



The extensions in the "Available Channels" column can be added to the ring group as a ring group member.

- Name: Name for this ring group.
- Strategy: Define how to ring the group members; select "RingAll" will ring all the member extensions at the same time, select "Ring In Order" will ring the member extensions one by one.
- Ring Group Members: The extensions selected will be members of the ring group.
- Available Channels: All available extensions/channels can be added to the ring group.
- Label: The extensions can be members of multiple ring groups, by giving each ring group a different label, if an incoming call rings a ring group the label will be displayed on the phone screen along with the caller ID. Therefore a ring group member can tell from which ring group the call is coming in.
- Extension for this ring group: By calling this extension internal users can reach the ring group members.
- Ring(each/all) for lasting time(sec): Ring duration of the group members.
- If not answered: Setup a destination to redirect the incoming calls to if no one answers.

3.3.2 IVR

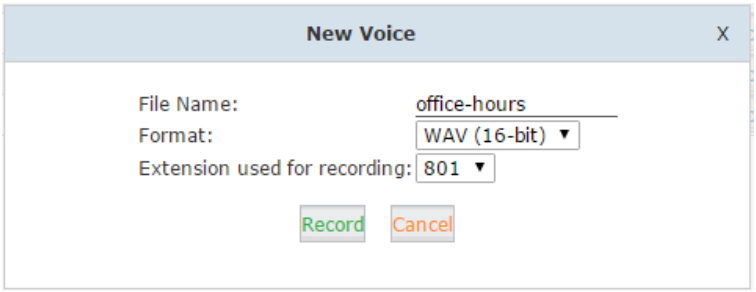
IVR, or interactive voice response, is responsible for the menus people hear and respond to when they call up a company or business and hear the words: "press 1 for sales, press 2 for marketing, press 0 to speak to the operator," for example.

IVR Prompts

To configure IVR menu on UC510 system you'll first need to record your IVR prompts, the IVR prompts will inform the callers of the options they have such as press 1 for sales etc.

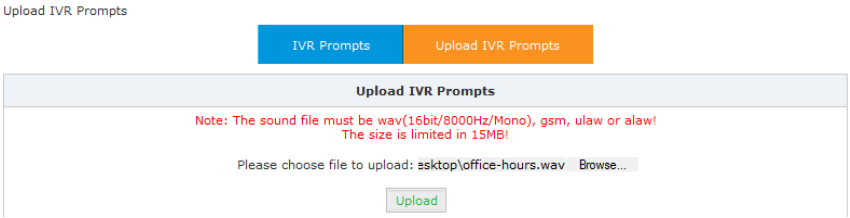
Navigate to web menu: *PBX->Inbound Control->IVR Prompts*

On this page you can delete the default voice prompts and click "New Voice" button to record a new voice prompts from a designated extension.



Click "Record" button and the extension will ring, pickup the extension and start talking to record your message. After recording is complete, your voice prompts will be listed on this page.

There is an alternative way to add voice prompts to the system, click "Upload Voice Prompts" tab.

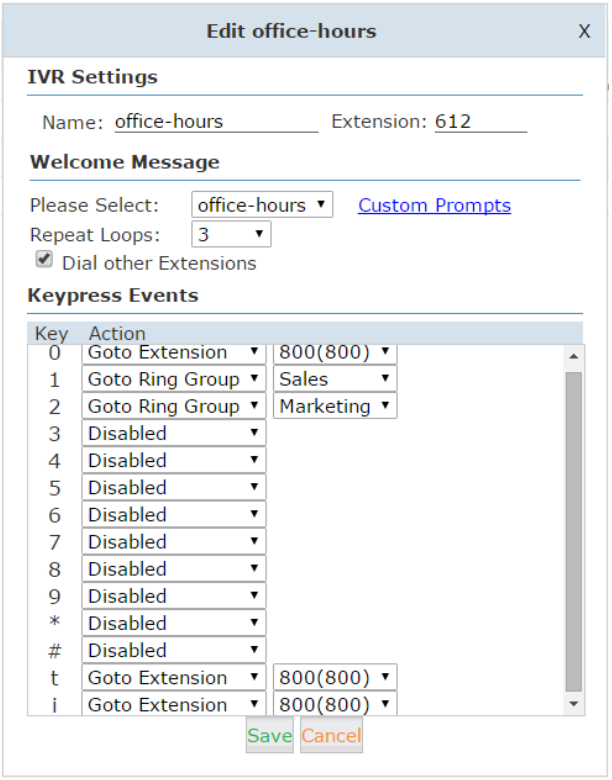


First browse to your pre-recorded voice prompt file and upload. This file will now be listed on *Voice Prompts* page and can be used to setup IVR menu.

IVR menu

Navigate to web menu: *PBX->Inbound Control->IVR*

Click "New IVR" button to add an IVR menu.



Suppose the IVR message says "Press 1 for sales, press 2 for marketing, press 0 for operator", if the caller is on IVR menu, and after they hear the voice prompts and presses 1 the sales ring group will ring, if 2 is pressed then the Marketing ring group will ring, if 0 is pressed then will ring the operator extension.

IVR Settings

- Name: Name for this IVR menu.
- Extension: Extension number for the IVR, by calling this number you can access the IVR menu.

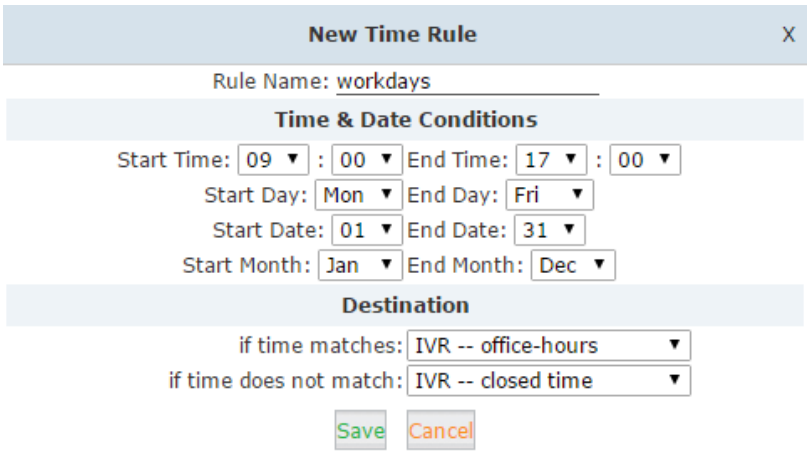
Welcome Message

- Please Select: Select a voice prompts for this IVR menu.
- Custom Prompts: Click this button will navigate to *PBX->Inbound Control->IVR Prompts* page for new voice prompts.
- Repeat Loops: Define how many times to play the IVR menu to the caller.
- Dial other Extensions: If enabled, the caller can dial extension number directly on IVR.
- Key Press Events: Define which destination to go by pressing a key on the phone keypad. If the undefined keys were pressed then it will be handled by the "i" parameter, "i" means invalid. And "t" stands for timeout, after all IVR loops played completely without pressing any key the incoming call will be handled by"t" parameter.

3.3.3 Time Conditions

Time Conditions allow businesses to define their working and non-working hours and use these rules to route calls accordingly. For example, a business may want to route calls to voicemail at weekends. To set time conditions navigate to the web menu: *PBX->Inbound Control->Time Based Rules*

Click "New Time Rule" to add a time condition for the system:



The time rule allows you to setup the time and date of your business hours. If time matches then direct the inbound calls to "office-hours" IVR menu. If not then direct to "closed time" IVR menu.

3.3.4 Inbound Routes

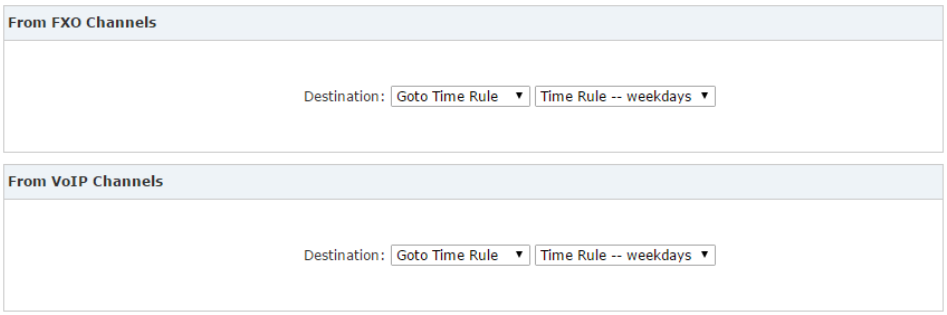
Inbound Routes are used for the system to direct the inbound calls to any destinations of the IPPBX system. The destinations can be time rules, IVR menus, ring groups or even direct ring a specific extension.

Navigate to web menu: *PBX->Inbound Control->Inbound Routes*

Here on this page you have 4 methods to route inbound calls.

General

For both FXO channels and the VoIP channels you can define default inbound destinations. If you don't want the inbound calls to always go to an IVR menu, ring group or extensions, then you can use a time rule to handle the inbound calls.

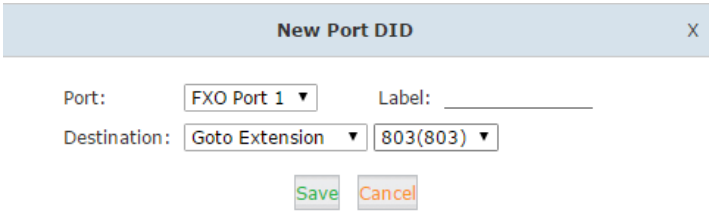


You can of course configure other destinations according to your real world requirements for the phone systems, except when using time rules to handle the calls by time conditions as these will override any settings made here.

Port DIDs

If your UC510 is only equipped with one FXO then you may not need to configure "Port DIDs", and "General" inbound control will be sufficient.

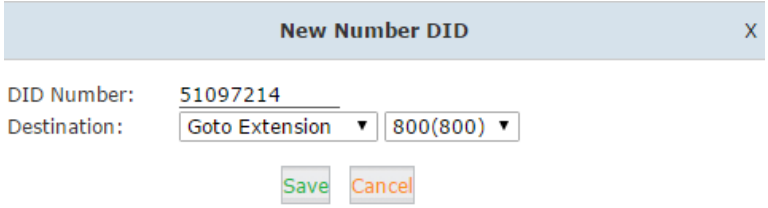
However, if your UC510 is equipped with two FXO ports, and one of the ports is dedicated to for example some kind of calling service, you can configure "Port DIDs" here for different destinations for the two ports.



Number DIDs

Number DID is only for inbound control of the VoIP channels and not FXO channels. If you have a VoIP trunk for outbound and inbound phone calls, for inbound the service provider needs to give you DID numbers so others can call you.

Click "Number DIDs" tab and click "New Number DID" button to add a number DID rule:



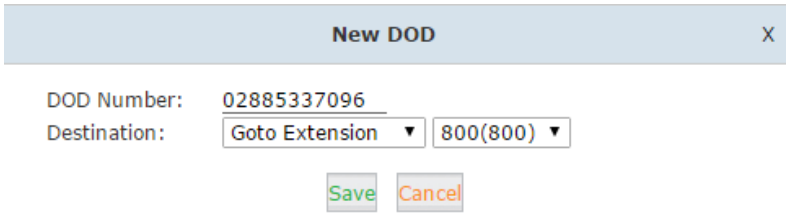
In this example, if the callers are calling 51097214, the call will go directly to extension 800 as this takes priority and general inbound control will not work for this DID number.

DOD Settings

DOD is also known as direct outward dialing, by specifying the number of an external caller

in the UC510 system, when this caller calls in, the call will be directed to a destination directly without restriction of time rule or IVR.

Click DOD Settings tab and click New DOD to add a record.



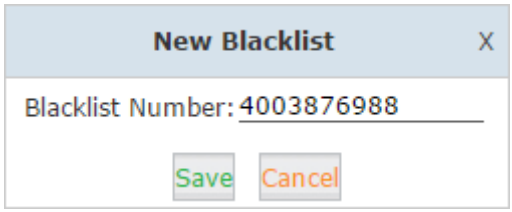
For this example, if caller 02885337096 calls the office number then it will go directly to extension 800.

3.3.5 Black List

Occasionally you may receive annoying advertising phone calls (cold calls), if you want to prevent these numbers calling again then you can use the blacklist feature of the IPPBX system to block these numbers from calling in.

Navigate to web menu: *PBX->Inbound Control->Black List*

Click New Blacklist to add these numbers to your black list.



If you accidently added some ordinary numbers, by selecting the items and clicking Delete button, you can delete the blacklisted numbers and they will be able to call in again.

There's also an alternate way to add the numbers to black list—by feature code.

Navigate to web menu: PBX->Advanced->Feature Codes, here on this page you can see the black list feature code:

Blacklist a number: *75

Remove a number from the blacklist: *075

Dial *75 and follow the voice prompts to enter the number you want to add to blacklist and this number will now be unable to call you anymore. If you want to remove a number from the black list then dial *075 and follow the voice prompts to enter the number you want to remove.

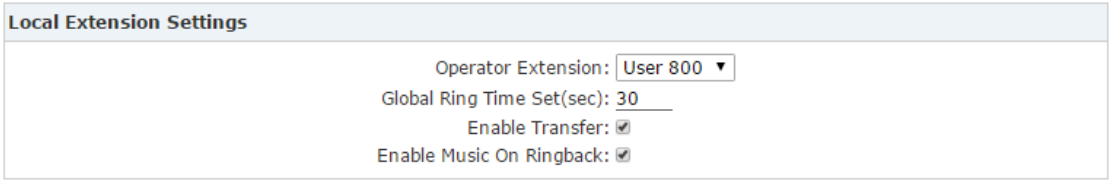
4. Advanced Settings

4.1 PBX Advanced Options

4.1.1 General

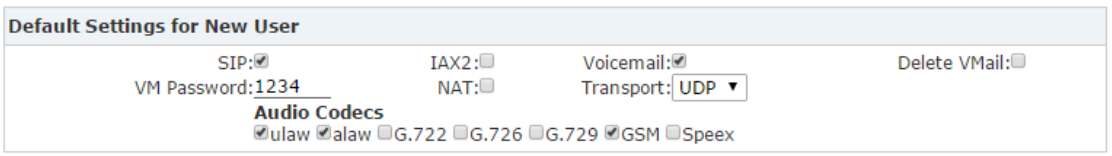
Web Menu: *PBX->Advanced->Options->General*

Local Extension Settings



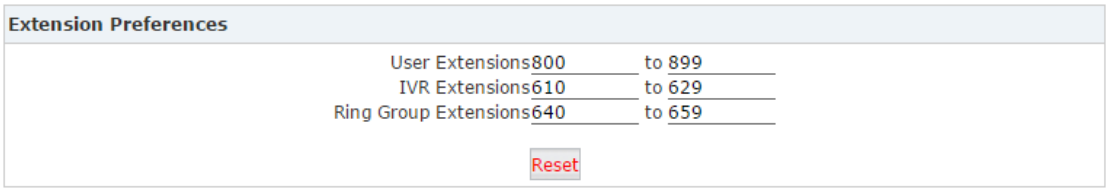
- Operator Extension: Choose an extension to be operator, while a caller is directed to voicemail by pressing '0' the call can go to operator extension.
- Global Ring Time Set(sec): If not specifically configured, the incoming call will ring the extension for the time specified here.
- Enable Transfer: If enabled, the extension users will be able to perform call transfer.
- Enable Music On Ringback: If enabled, callers will hear music instead of ringback tone while calling other extensions.

Default Settings for New User



These options are for new extensions, if you have one of the options enabled then new extensions created will have this option enabled by default.

Extension Preferences

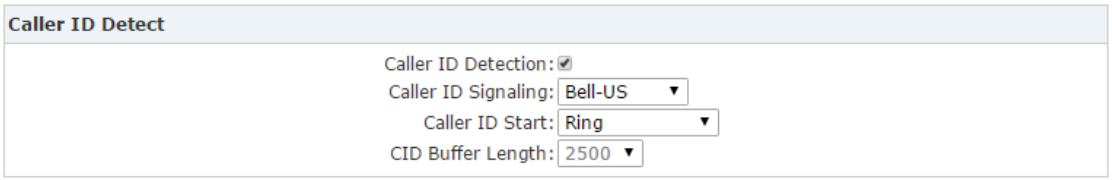


The user extension number, IVR extension number, and ring group extension number ranges are defined here to avoid any conflicts.

4.1.2 Global Analog Settings

Web Menu: *PBX->Advance->Options->Global Analog Settings*

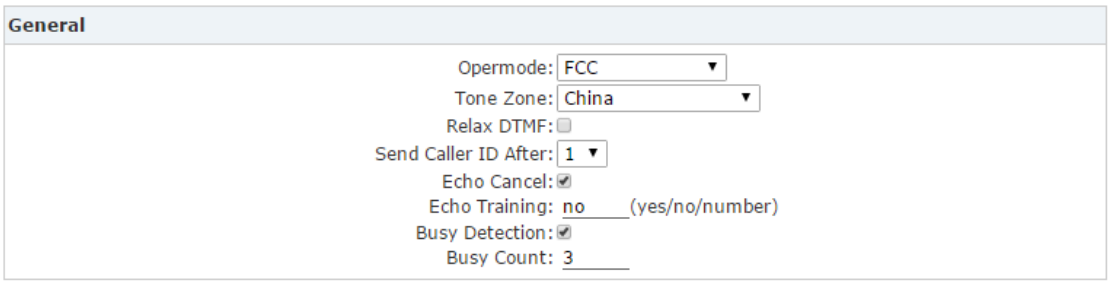
Caller ID Detect



These options are used to teach the UC510 how to detect caller identity(caller ID) from the PSTN lines on FXO ports.

- Caller ID Detection: Enable/Disable Caller ID Detection
- Caller ID Signaling: The signaling type applied on the PSTN lines to pass caller ID.
  Bell-US—Also known as BellcoreFSK. Used in the Canada, China, Hong Kong and US.
  DTMF—Dual Tone Multi-Frequency. Used in Denmark, Finland and Sweden.
  V23—Mostly used in UK.
  V23-Japan—Mostly used in Japan.
- Caller ID Start: When the caller ID starts.
  Ring—Caller ID starts when a ring received.
  Polarity—Caller ID starts when polarity reversal starts.
  Polarity(India)—Can be used in India.
  Before Ring—Caller ID starts before a ring received.
- CID Buffer Length: The buffer length can be used to store caller IDinfo.

General



- Opermode: Defines the Opermode for FXO Ports.
- ToneZone: Select the tone zone of your country.
- Relax DTMF: Helps DTMF signal detection.
- Echo Cancel: Enable/Disable software Echo Cancel algorithm.
- Echo Training: Enabling echo training will cause the PBX system to mute the channel, send an impulse, and use the impulse response to pre-train the echo canceller so it can start out with a much closer idea of the actual echo. Value may be "yes", "no", or

a number of milliseconds to delay before training (default = 400). This option does not apply to hardware echo cancellers.

- Busy Detection: Enable/Disable Busy tone Detection.
- Busy Count: Busy tone counts. This will be active when Busy Detection enabled.

4.1.3 Global SIP Settings

Web Menu: *PBX->Advanced->Options->Global SIP Settings*

Notice: Global SIP Settings are appropriate for advanced administrators only. Please contact our technical support department before modifying anything in this section.

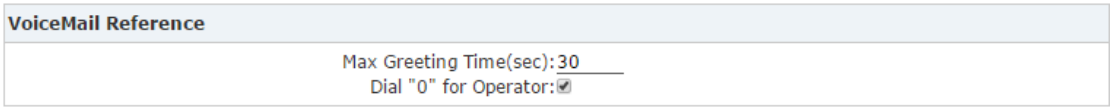
4.2 Voicemail

4.2.1 General Voicemail Options

Web Menu: *PBX->Advanced->Voicemail*

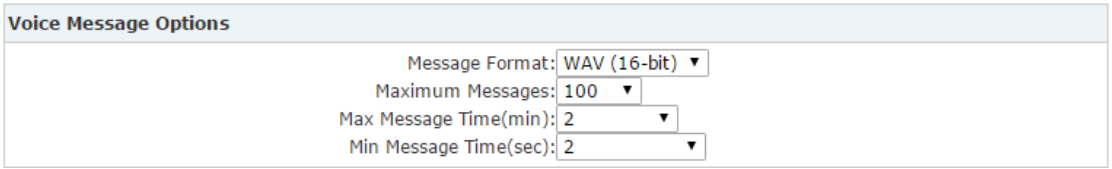
In this section you can configure some general basic options for the user extensions' voicemail box.

Voicemail Reference



- Max Greeting Time(sec): Maximum voicemail box greeting message duration.
- Dial "0" for Operator: If this option is enabled then callers will be able to dial "0" to transfer out of voicemail to the Operator.

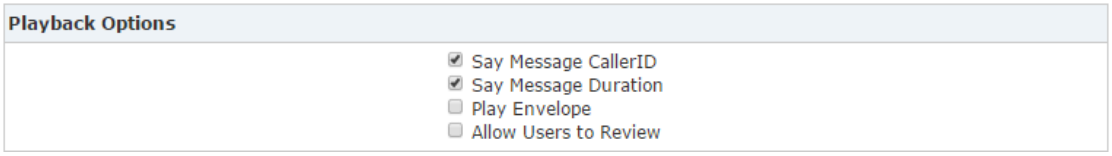
Voice Message Options



- Message Format: The audio file format to be recorded.
- Maximum Messages: The maximum amount of voice messages for each extension.
- Max Message Time(min): The maximum time duration of an individual voicemail message.
- Min Message Time(sec): The minimum time duration of an individual voicemail

message. Default minimum duration is 2s, which means voice messages which are less than 2s will be ignored by the IPPBX system.

Playback Options



The following options are for voicemail message playback.

- Say Message CallerID: Announce the Caller ID of the caller who left this message before playing the voice message.
- Say Message Duration: Announce the message duration before playing the voice message.
- Play Envelope: Announce the date, time and caller ID for the voicemail message.
- Allow Users to Review: If this option is enabled, it will allow users to review the voice message.

4.2.2 Playback Voicemail on the phone

Navigate to Web Menu: *PBX->Advanced->Feature Codes*

On this page, you'll find two feature codes that can be used for checking voicemail.

Voicemail Main Menu: *60

Check Extension Voicemail: *61

Dial *60 and you will enter the main menu of voicemail feature, by specifying the extension number and voicemail password of that extension you can check its voicemail on any extension by following the system voice guidance.

By dialing *61 on one extension and entering the voicemail password of this extension you can follow the voice guidance to check the voicemail from your own extension. Alternatively, you can configure some advanced options for your voicemail box.

4.2.3 Voicemail to Email

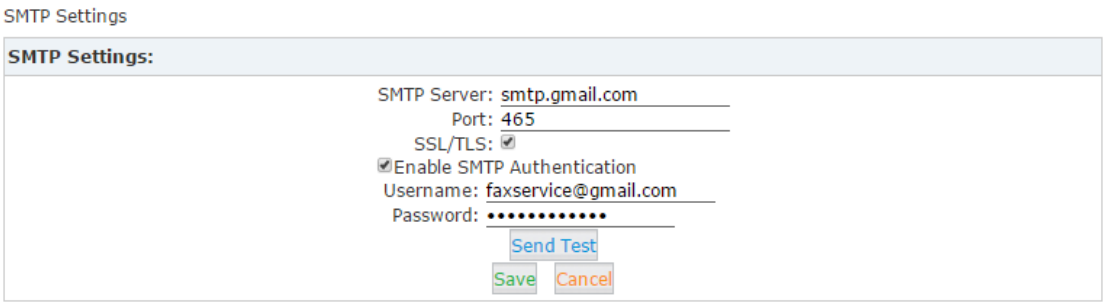
To send voicemail messages that have been received direct to the users' email box, you need to configure SMTP support, email format and also specify email addresses of the extension users.

Step1:

SMTP Settings

Navigate to Web Menu: *PBX->Advanced->SMTP Settings*

Enter an email account to be used by the system and to send emails with voicemail messages attached to the extension users' email boxes.



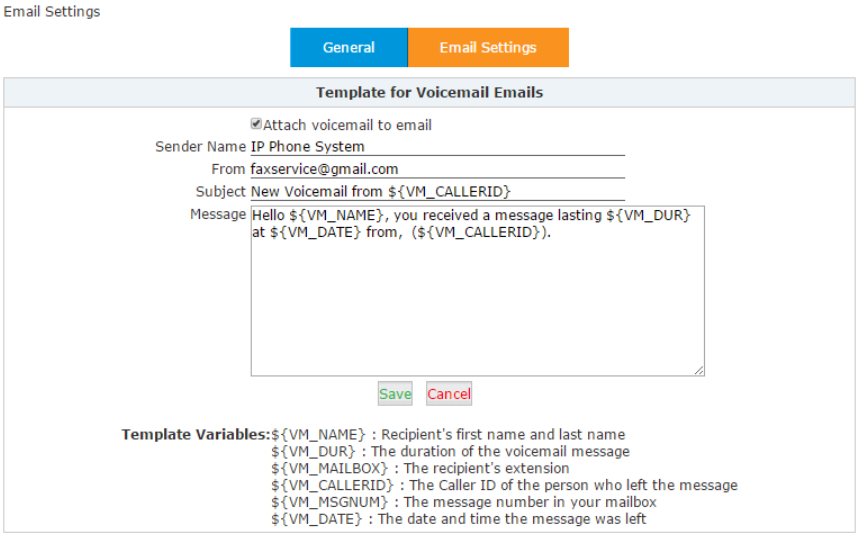
- SMTP Server: SMTP server domain, for example: smtp.gmail.com, smtp.tom.com.
- Port: Default SMTP service port is 25, but if SSL/TLS enabled it will use port 465.
- SSL/TLS: Encrypts a communication channel between the UC510 system and the SMTP server.
- Enable SMTP Authentication: If your SMTP server needs authentication, please enable this option, and configure the following.
- Username: The email account.
- Password: The password for this email account.
- Send Test: Click "Send Test" to send a test email to see if SMTP is working correctly or not.

Step2:

Email Settings

Navigate to Web Menu: *PBX->Advanced->Voicemail->Email Settings*

On this page you can define the email context which will be sent to the extension users' email boxes.

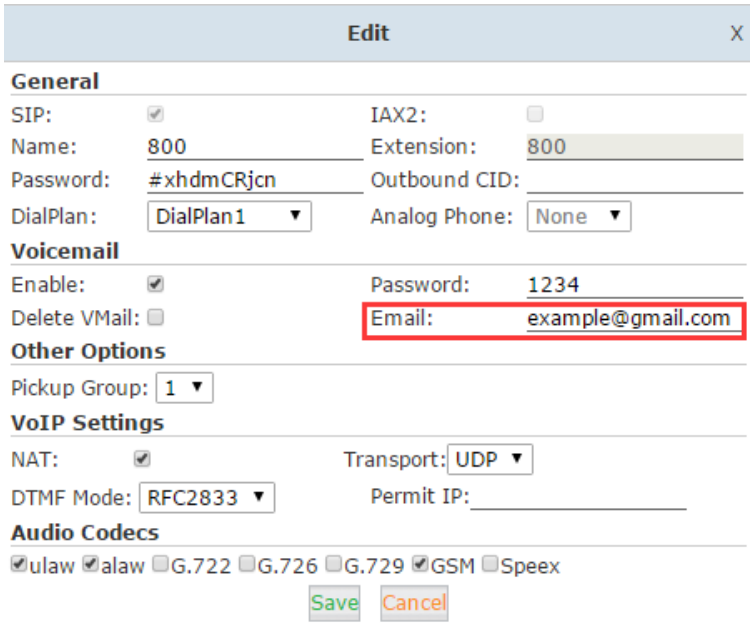


- Attach voicemail to email: If enabled, the system will send the received voice message files to the extension users' email boxes.
- Sender Name: Alias for the SMTP email account.
- From: The email account from SMTP settings.
- Subject: The subject of the emails sent by UC510 system.
- Message: The context of the email describes the details of the voicemail message received.
- Template Variables: These variables can be used to acquire details of the voicemail messages which can be used in the message field to compose the email context.

Step3:

Email Address

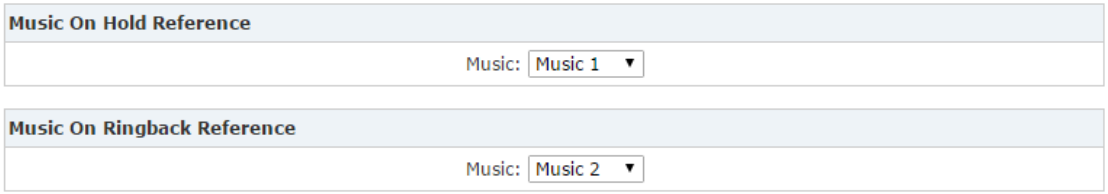
On the user extension you must specify the email addresses that you want to receive voicemails



After completing these 3 configuration steps, if as in this example, a user extension 800 gets a new voicemail message, UC510 will send this voicemail message to example@gmail.com.

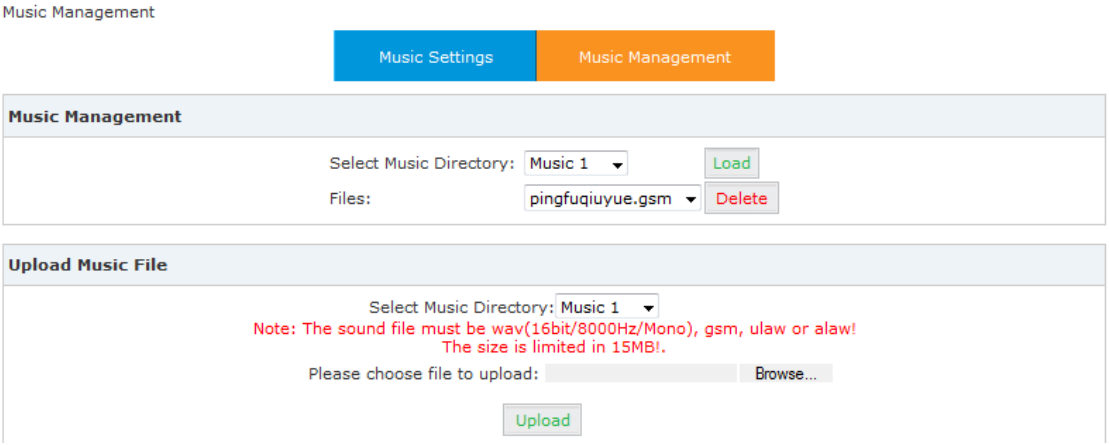
4.3 Music Settings

Web Menu: *PBX->Advanced->Music Settings*



- Music On Hold Reference: Audio files inside this selected folder will play to the party which has been put on hold.
- Music On Ringback Reference: Audio files inside this music folder will be played instead of playing ringback tone to the caller.

There are 10 folders for music files, by default the first 3 folders had been uploaded with some music files. You can choose an appropriate music file among these 3 folders. If you want to upload your own audio files please click "Music Management" tab.



In the Music Management section, you can select a music folder and click "Load" button to check which audio files are inside this folder. By clicking "Delete" button you can delete the existing audio files.

In the Upload Music File section, you can select a music folder and browse your PC file system to select an audio file and click "Upload" button to upload the required audio file. If there are more than one audio files in the same music folder, they will be played randomly.

Notice: UC510 system can utilize wav(16bit, 8000Hz, mono), gsm, ulaw and alaw audio file format.

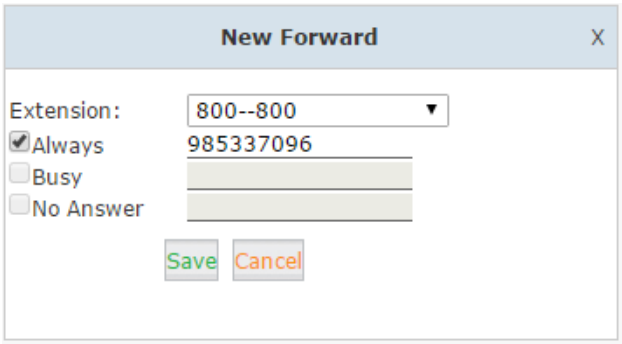
4.4 Call Forward

4.4.1 Configure from Web GUI

This feature allows calls to an extension to be automatically forwarded to a specific internal extension or external phone number.

Web Menu: *PBX->Advanced->Call Forward*

Click "New Forward" button to set call forward for an extension.



- Always: Unconditionally forward the incoming calls.
- Busy: Forward the incoming calls only if the extension is busy.
- No Answer: Forward the incoming call only if the extension didn't answer.

Notice:

1. If you forward a call to an external phone number please make sure to add a prefix in front of the number if your system requires prefix to dial out.
2. The forward condition "Always" is mutually exclusive to "Busy" and "No Answer".

4.4.2 Configure Call Forward from a phone

Navigate to Web Menu: *PBX->Advanced->Feature Codes*

You'll see feature codes listed for call forward as follows:

Enable Forward All Calls: *71

Disable Forward All Calls: *071

Enable Forward on Busy: *72

Disable Forward on Busy: *072

Enable Forward on No Answer: *73

Disable Forward on No Answer: *073

With these feature codes, you can activate or deactivate call forward directly from your phones without the need to configure on the Web GUI.

For example, if UC510 requires prefix 9 to call outbound, and the number you want to forward the calls to is 85337096.

Activate always call forward: Dial *71985337096, press 1 to confirm.

Deactivate always call forward: Dial *071.

Activate call forward on busy: Dial *72985337096, press 1 to confirm.

Deactivate call forward on busy: Dial *072.

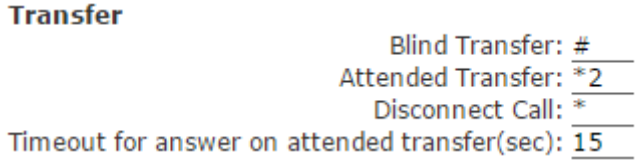
Activate call forward no answer: Dial *73985337096, press 1 to confirm.

Deactivate call forward no answer: Dial *073.

4.5 Call Transfer

When talking to someone on your extension, you can transfer this call to another extension using the transfer feature codes.

Navigate to web menu: *PBX->Advanced->Feature Codes*



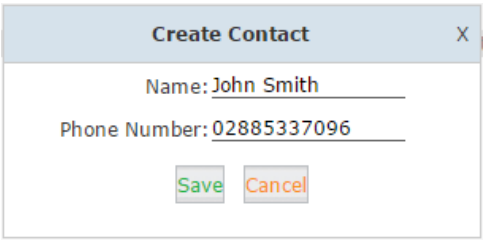
Here in this section you can see there are two feature codes that can be used to transfer a call.

- Blind Transfer: Using the # key you(transferor) can transfer a call to another extension or external number(transferee) directly. During a live call, you press # and system says "Transfer", then you enter the transferee number and end with another # key, this call is transferred. If the call is not answered by the transferee this call will go back to your extension.
- Attended Transfer: Using the key sequence *2 you can transfer a call as well, however, before the call is transferred, you can talk to the transferee to introduce this call. During a live call, you press *2 and the system will say "Transfer", then enter the third party number, the caller will be put on hold, and after the transferee answered your call you can introduce this call to them, if they wish to take this call you just hang up and the caller and the transferee will now be connected. If they don't want to take the call then press * to disconnect this conversation and go back to the caller.
- Disconnect Call: Used to disconnect with the transferee if they don't want to take the call.
- Timeout for answer on attended transfer(sec): The number of seconds to be considered as timeout before the transferee answering the transferor.

4.6 Phonebook

Contacts can be added to the UC510 system, so should one of the contacts call the office number, the person receiving the call will see the caller ID and also the caller name on their phone screen.

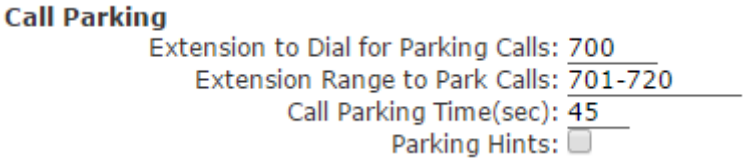
Click "Create Contact" button to add a contact to the UC510 system as shown below:



4.7Call Parking

Call Parking allows anyone who has received a call to park the call on an extension, allowing any other user to access the parked call. Typically, you receive the call, transfer it to extension 700, and then listen as the system tells you where you can pick up the call (usually extension 701). Any user extension on UC510 can now dial 701 to pick-up the parked call.

Navigate to web menu: *PBX->Advanced->Feature Codes*

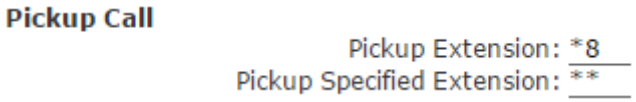


- Extension to Dial for Parking Calls: If you want to park a call just transfer it to extension 700, both transfer with # and *2 will work.
- Extension Range to Park Calls: While parking a call, system will say on which extension the call is being parked. Usually it will be parked on 701, if at the same time another call is going to be parked then it will be on 702. Just dial 701 or 702 on another user extension to resume the call.
- Call Parking Time(sec): Parking time duration. If not answered within this time limit it will go back to the extension which parked this call.
- Parking Hints: If this option is enabled then the parking lot numbers can be monitored by BLF indicators.

4.8 Call Pickup

With call pickup feature, extension users can help pick up an incoming call which is ringing on another extension.

Navigate to web menu: *PBX->Advanced->Feature Codes*



Here in this section you can see there are two types of feature codes which can be used to pickup a ringing extension.

- Pickup Extension: Dial *8 directly and you can pickup a ringing extension which is in the same pickup group as your extension. This feature code and pickup group is introduced in chapter 3.
- Pickup Specified Extension: Dial ** followed by a specific extension number which is ringing allows you to pickup the call from the extension whether in the same pickup group as your extension or not.

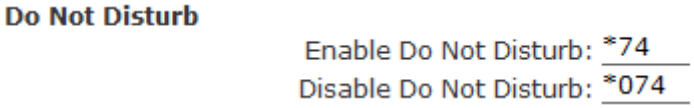
4.9 DND(Do Not Disturb)

DND(Do Not Disturb) functionality is the ability of a phone or client to ignore any incoming calls. This can be implemented in several ways. One way is to implement it from the IP phone menu. The other way is to implement it on the IPPBX system.

For the IP phones, please read the phone user manual about how to implement this feature.

For UC510, you can use the feature code to implement this feature.

Navigate to web menu: *PBX->Advanced->Feature Codes*



In this section you can see that by dialing feature code *74, DND will be enabled on your extension and any calls to your extension will be redirected straight to voicemail. To disable DND, simply dial *074 and you will be able to receive calls again.

4.10 Set System Voice Prompts Language

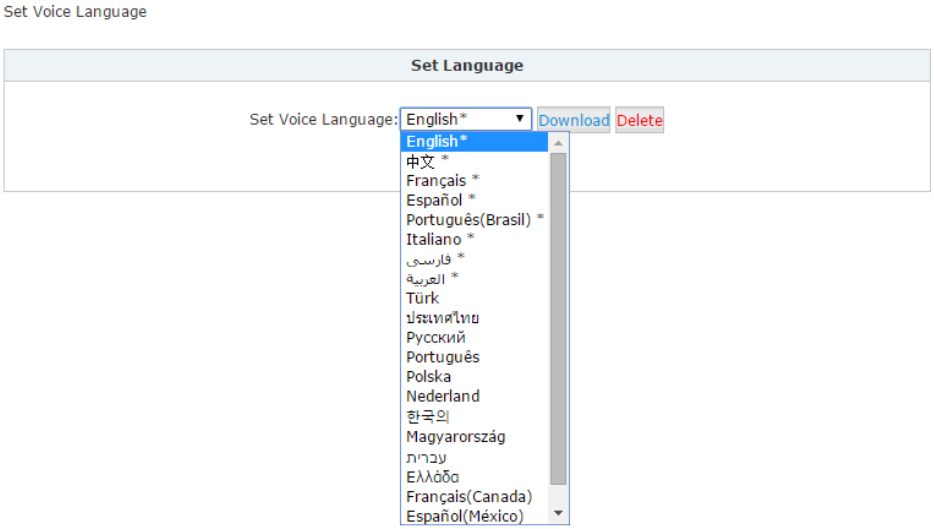
What are system voice prompts?

System voice prompts guide the callers on how to place a call or how to use the IPPBX system functionalities. For example, while checking your voicemail, the system voice

prompts guides you to enter voicemail password. Another example is when you call someone and they do not answer the call, a system voice prompt will ask you to leave a message.

Navigate to Web Menu: *PBX->Advanced->Set Voice Language*

At this time, UC510(v1.0.8) support 21 languages for system voice prompts.



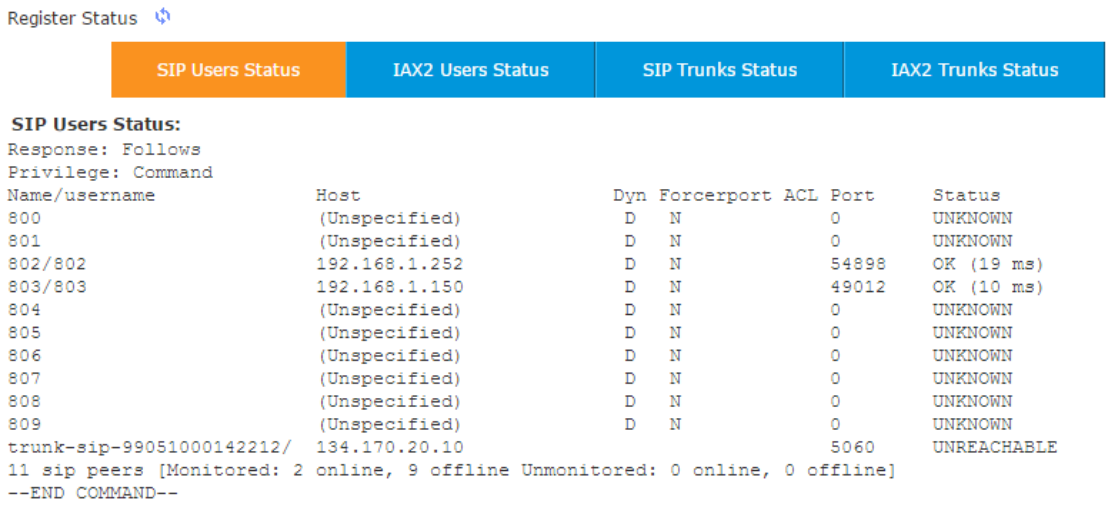
The items with * means these languages already exist locally in the system while other languages need to be downloaded by clicking "Download" button.

4.11 Reports

4.11.1 Register Status

The PBX Operator page provides basic information on extension and trunk status, However, if you require more detailed information on SIP/IAX2 extensions and trunks then this is available here on the Register Status page.

Navigate to Web Menu: *PBX->Report->Register Status*

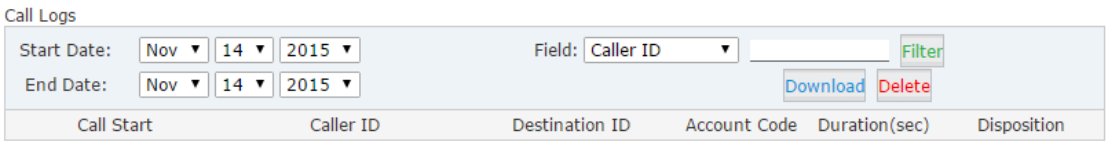


The register status page displays the register status of extensions and trunks, specified by the end points' IP addresses, port number and reachability, etc.

4.11.2 Call Logs

Call log is also known as CDR(Call Detailed Records), on this page you can check any call records made through the IPPBX system.

Navigate to Web Menu: *PBX->Report->Call Logs*



On this page you can define the query criteria by time intervals, caller ID, destination ID and also account code.

- Start Date: Query the records after this timeline.
- End Date: Query the records before this timeline.
- Field: Criteria that can be used to query the call logs.

  Caller ID: Searching by Caller ID.

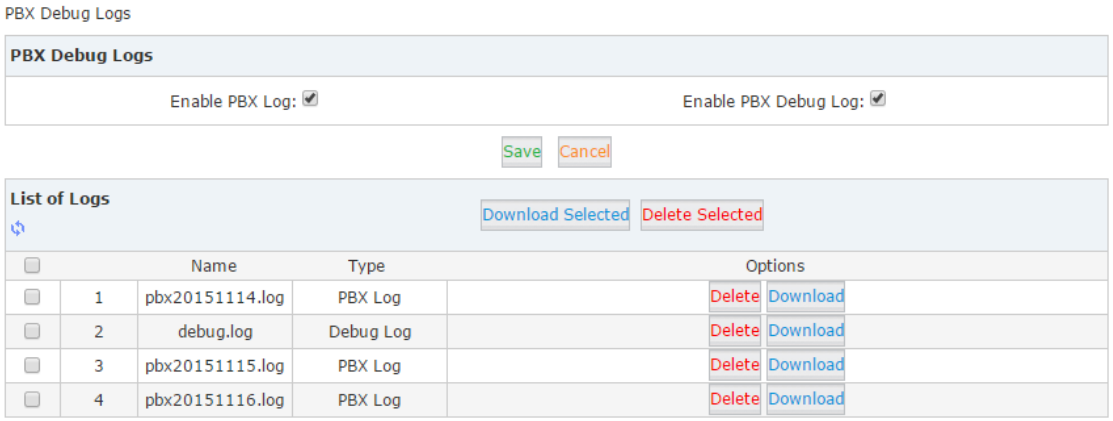
  Destination: Searching by destination ID.

  Account: The pin code been used for making the outbound phone calls.
- Filter: Click this button to search for records based on search criteria specified.
- Download: Click this button to download your search results and it will be saved as a CSV file which can be opened by excel.
- Delete: Click this button to delete the searching results from the IPPBX system.
- Call Start: The precise time when the call began.
- Caller ID: The number of the call originator.

- Destination ID: The number of the called party.
- Account Code: Pin code been used to place this outbound phone call.
- Duration(sec): The time the phone call lasted displayed in seconds.
- Disposition: Indicates how the phone calls been handled.

4.12 PBX Debug Logs

Web Menu: *PBX->Report->PBX Debug Logs*



These logs are IPPBX journals which store all system activities. They can be used for debug purpose if you are troubleshooting a system problem.

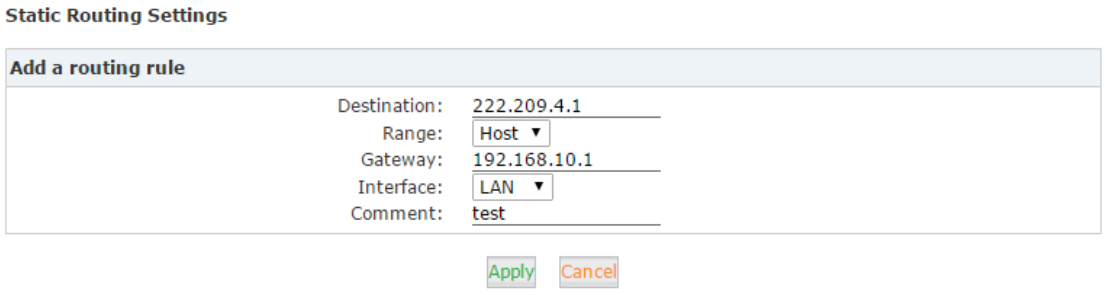
Please do not enable these logs if the system is functioning properly as they generate a lot of information which will take up storage space on the UC510.

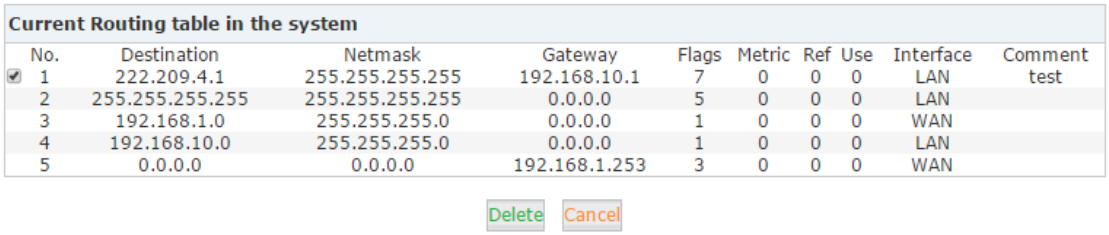
4.13 Network Advanced

4.13.1 Static Routing

Static Routing is a form of routing that occurs when a router uses a manually-configured routing entry rather than information from a dynamic routing protocol to forward traffic.

Web Menu: *Router Gateway->Network->Static Routing*





Current Routing table in the system

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	222.209.4.1	255.255.255.255	192.168.10.1	7	0	0	0	LAN	test
2	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN	
3	192.168.1.0	255.255.255.0	0.0.0.0	1	0	0	0	WAN	
4	192.168.10.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN	
5	0.0.0.0	0.0.0.0	192.168.1.253	3	0	0	0	WAN	

Delete Cancel

- Destination: Set the IP address of destination host or network address.
  E.g. 222.209.4.1, 192.168.10.0.
- Range: Select the routing mode: Host or Net. When "Net" is selected, you need to configure the netmask, e.g. 255.255.255.0.
- Gateway: Set the gateway address.
- Interface: Select the interface WAN or LAN.
- Comment: Name for this rule.
- Current Routing table in the system: Routing table list. The manually configured static routing records can be deleted, but default routing cannot.

4.13.2 VPN

VPN(Virtual Private Network) is mainly used for setting up long-distance and/or secured network connections. When used on UC510, all the phone calls you make and receive are encrypted so it secures your remote offices/extensions' phone services. Built-in VPN Server on UC510 is an easy way to set up such secured connectivity between other UC510 or IP phones. You don't require a dedicated VPN server or need to buy a VPN router. This is also a workaround to avoid a firewall issue when configuring remote VoIP client as SIP protocol is notoriously difficult to pass through a firewall due to the random numbers required to establish connection.

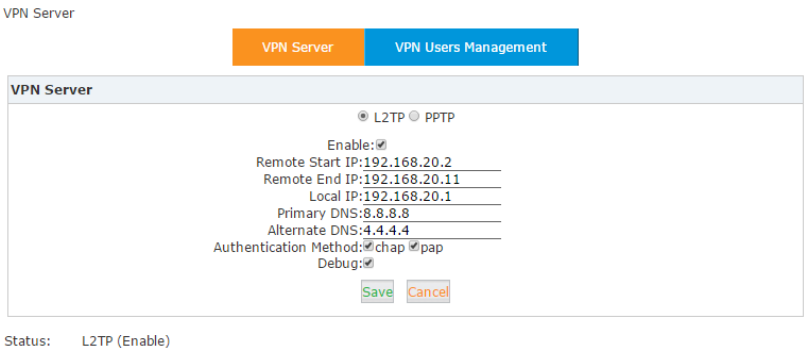
With UC510 you can build L2TP/PPTP VPN server for other terminals to connect. In addition to another UC510 and IP phones, you also can connect PC or mobiles phones as VPN clients.

A maximum of 10 VPN clients can be connected.

VPN server

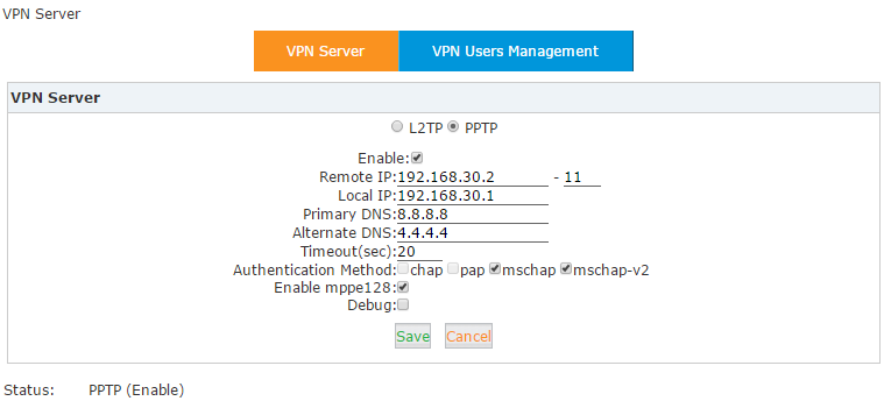
Navigate to Web Menu: *Router Gateway->VPN->VPN Server*

Choose L2TP to configure a L2TP VPN server:



- Remote Start IP: Defines the remote L2TP VPN client start IP. This can be any private IP but not one that is in the same network address range as UC510.
- Remote End IP: Defines the remote L2TP VPN client end IP. UC510 supports a maximum of 10 VPN clients, so please give a proper end IP according to the given start IP.
- Local IP: Set the local IP of L2TP server, so the VPN clients can communicate with server with this given IP address.
- Primary DNS: Set the primary DNS of L2TP server.
- Alternate DNS: Set the alternate DNS of L2TP server.
- Authentication Method: Select the authentication method: chap or pap.
- Debug: Enable/ Disable debug.

Choose PPTP to configure a PPTP VPN server:

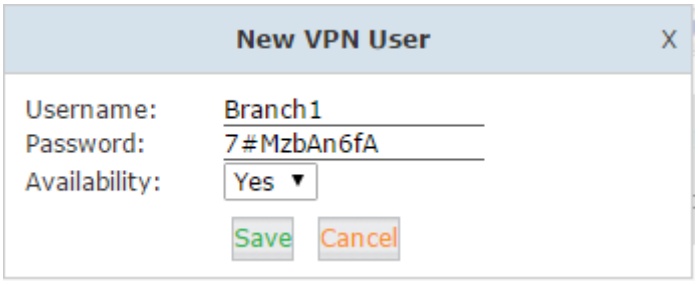


- Remote IP: Defines the remote PPTP VPN client start IP and end IP, this can be any private IP but not one in the same network address range as UC510. UC510 supports a maximum of 10 VPN clients, so please give a proper end IP according to the given start IP.
- Local IP: Set the local IP of PPTP VPN server, so the VPN clients can communicate with server with this given IP address.
- Primary DNS: Set the primary DNS of PPTP server.
- Alternate DNS: Set the alternate DNS of PPTP server.

- Timeout(sec): Timeout for disconnection of PPTP.
- Authentication Method: Select the authentication method: chap/pap/mschap/ maschap-v2.
- Enable mppe128: Enable/ Disable mppe128 encryption.
- Debug: Enable/ Disable debug of the VPN connection process.

VPN user management

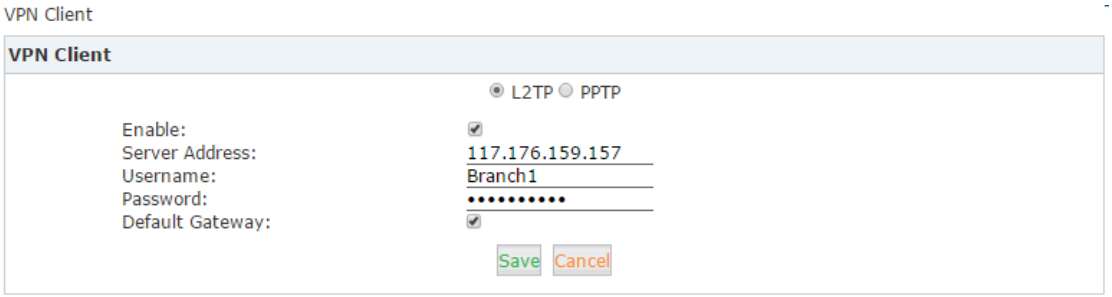
After VPN Server configurations, you need to define username and password for VPN clients to connect to VPN server. Both L2TP and PPTP are the same.



VPN Clients

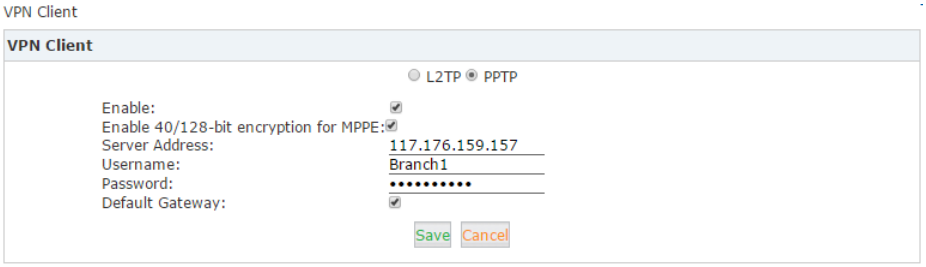
Navigate to Web menu: *Router Gateway->VPN->VPN Client*

Choose L2TP VPN Client to connect to L2TP VPN Server:



- Server Address: The fixed public IP of UC510 WAN interface.
- Username: The username defined on VPN server.
- Password: The password defined on VPN Server.
- Default Gateway: All traffic goes through the L2TP VPN connection.

Choose PPTP VPN client to connect PPTP VPN server:



- Enable 40/128-bit encryption for MPPE: Select to enable MPPE encryption.
- Server Address: The fixed public IP on UC510 WAN interface.
- Username: The username defined on VPN server.
- Password: The password defined on VPN server.
- Default Gateway: All traffic goes through the PPTP VPN connection.

4.13.3 DDNS

DDNS is a useful feature for businesses that don't have a static IP Address provided by their internet service provider but need to be able to provide an address for external users to connect to. By signing up with a Dynamic DNS provider in combination with the built-in DDNS feature on UC510means you can provide a DNS name to these external users that always points to the correct IP Address for yourUC510.

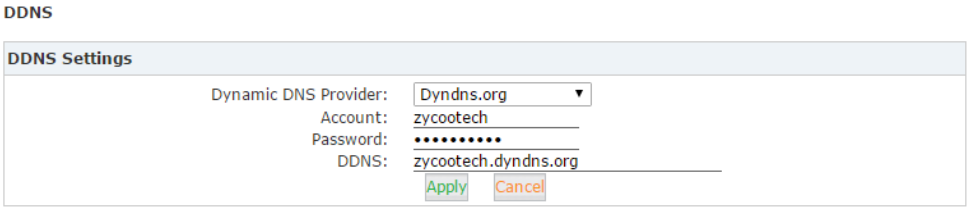
UC510 can support DDNS service providers listed below:

- http://dyn.com/
- http://freedns.afraid.org/
- http://www.zoneedit.com/
- http://www.noip.com/

Sign up with one of those DDNS service providers' website and subscribe a dynamic domain name.

Navigate to Web menu: *Router Gateway->DDNS*

Choose the DDNS service provider you have subscribed to. Then fill in the username and password you have signed up on their website along with the dynamic domain name.



After this please refer to chapter 5.1.3 to configure port forwarding then you'll be able to access internal services from internet using this dynamic domain. For example you can port forwarded port number 9999, then you'll be able to access UC510 web interface using URL: http://zycootech.dyndns.org:9999.

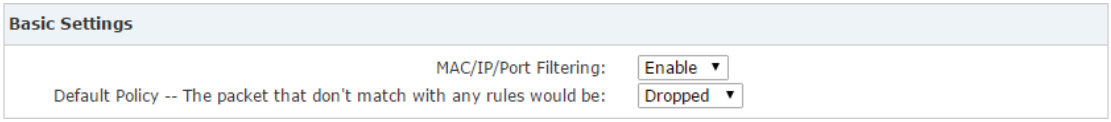
5. System Administration

5.1 Security

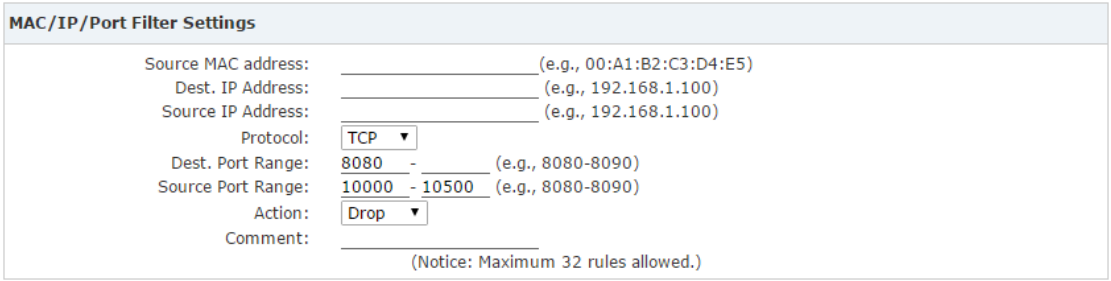
5.1.1 Mac/IP/Port Filter

Any connection request from terminals can be controlled by the filter feature according to the defined rule parameters. Filtering based on MAC, source IP and source port can prevent a terminal from obtaining an unauthorized network connection.

Navigate to Web Menu: *Router Gateway->Firewall->Mac/IP/Port Filter*

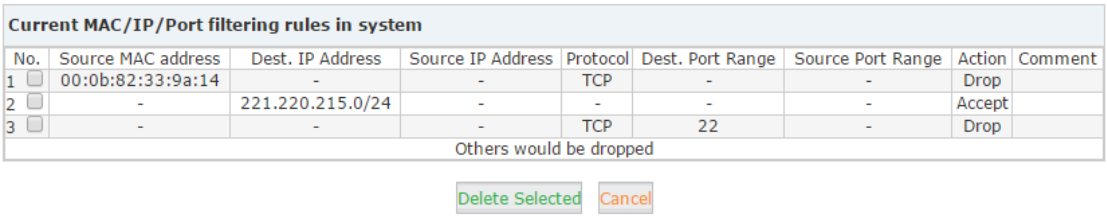


- MAC/IP/Port Filter: Enable or Disable the system to implement the filter rules.
- Default Policy: The default strategy, configure to receive or discard the specified packets from an unauthorized Mac address, IP address or port number.



In this section, you can create up to 32 customized grant or reject rules according to MAC addresses, IP addresses and also port numbers. By specifying only one of these factors the rule is valid.

- Source MAC Address: Specify the MAC address of the device from where the packets originate.
- Dest. IP Address: Specify the destination IP address packets are sending to.
- Source IP Address: Specify the IP address from which the packets originate.
- Protocol: Select a protocol type, if TCP or UDP then you need to specify an IP address or port number/port number range.
- Dest. Port Range: Specify the destination port/ports the sent packets.
- Source Port Range: Specify the source port/ports the packets originated.
- Action: Grant or reject the packets transmission.
- Comment: Alias for this rule.



As in the above diagram, you will find a list of the customized rules. By checking the checkbox and clicking "Delete Selected" button you can delete items from this list.

5.1.2 System Firewall

Navigate to Web Menu: *Router Gateway->Firewall->System Firewall*

The following options are used to configure certain specific services in the UC510 system, these options allow you to strengthen the security of the system and protect connected endpoint devices and the PBX from malicious attacks.

System Security Settings

- Remote management: Allow or Deny remote access to web GUI and SSH through WAN port. The default is Deny.
- Ping from WAN Filter: Allow or Disallow ping request on WAN interface.
- Block Port Scan: By default this feature is enabled as this can help to avoid port scan attacks.
- Block SYN Flood: SYN flooding is an attack vector for conducting a denial-of-service (DoS) attack, by enable this option the system can prevent DoS attack.
- Stateful Packet Inspection (SPI): Stateful packet inspection, also known as dynamic packet filtering is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.
- SIP register decline: If this option is enabled then remote extensions will not be able to register to UC510 through WAN interface. By default it is disabled. If you only require internal extensions then you can enable this setting.

5.1.3 Port Forward

Port forward allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN).

Navigate to web menu: *Router Gateway->Firewall->Port Forward*

Port Forward Settings

Port Forward

Private IP Address:	192.168.1.253
Public Port Range:	9999 -
Private Port Range:	9999 -
Protocol:	TCP&UDP
Comment:	web

(Notice: Maximum 32 rules allowed.)

On this page you can define your rules such as forward a single port or a port range for example 9999 and 10000-10500.

After the rules had been configured and they will be listed as below:

Current Port Forward in System

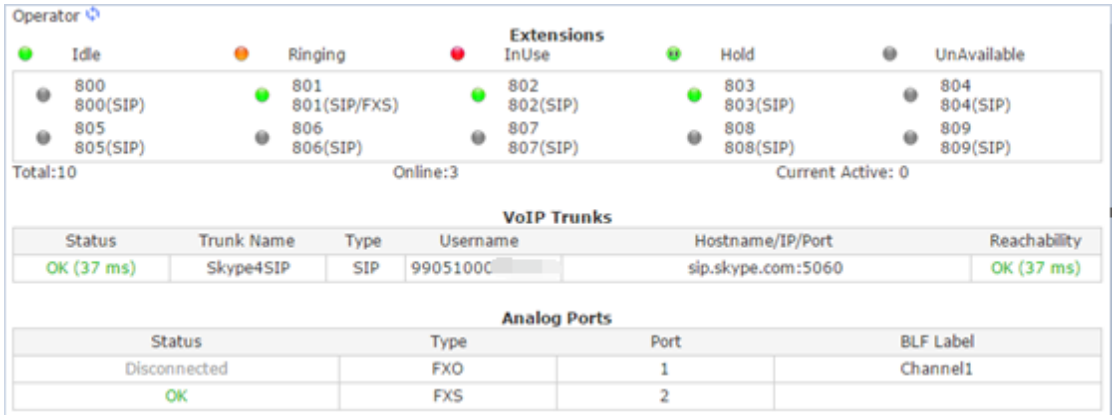
No.	Private IP Address	Public Port Range	Private Port Range	Protocol	Comment
1	192.168.1.253	9999	9999	UDP	web
2	192.168.1.253	10000 - 10500	10000 - 10500	UDP	rtp
3	192.168.1.253	5060	5060	TCP + UDP	SIP

32 port forwarding rules is the maximum supported by the UC510 system.

5.2 Status Monitor(Operator)

Navigate to web menu: *Status->PBX Operator*

The status monitor page displays real-time status of all the extensions, VoIP trunks and also FXO trunk status.



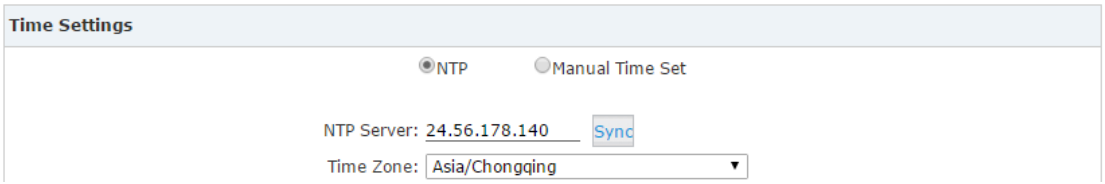
In the analog ports section, the BLF Label is used for BLF monitor of the FXO channel.

5.3 Time Settings

System time is very important for an IPPBX system, especially if the UC510 system handles inbound phone calls using time rules as the time must be correct for calls to be handled properly, additionally, call logs and debug logs need the correct time to record system events accurately.

Navigate to web menu: *System Administration->Time Settings*

Time Settings

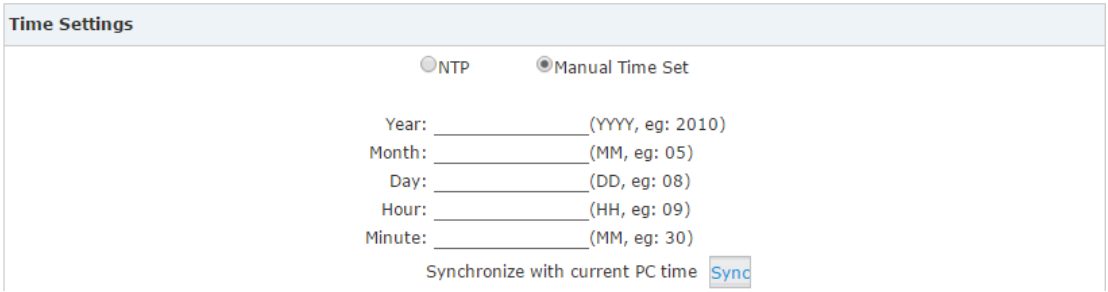


On the time setting page you can configure the system to obtain time online from the public NTP server or you can manually set the system time.

If you are setting the system to obtain time from online NTP server, you need to specify a proper NTP server and select the correct time zone.

If you are manually setting the system time, then select "Manual Time Set":

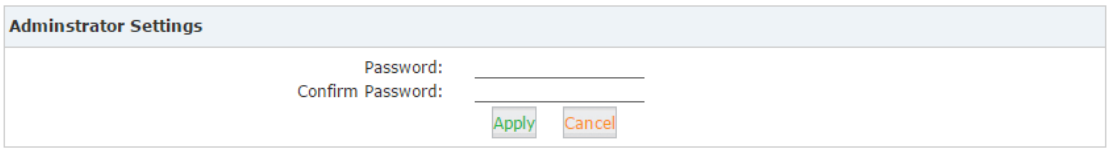
Time Settings



To configure time manually, fill in the current date and time details then click "Save" button for your changes to take effect or you can click the "Sync" button to synchronize the current time from your operating system.

5.4 Management

Navigate to web menu: *System Administration->management*

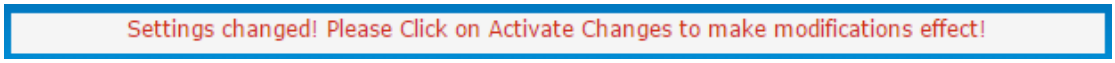


To change your Web Admin password, enter new password in the "Password" field and repeat the new password again in the "Confirm Password" field and click "Apply" button. After "Apply" is clicked, then 3 seconds later the Web GUI will reload and redirect you to the login page, you need to use username admin and the new password to login in.

5.5 Activate Configuration

5.5.1 Activate Configurations of the IPPBX system

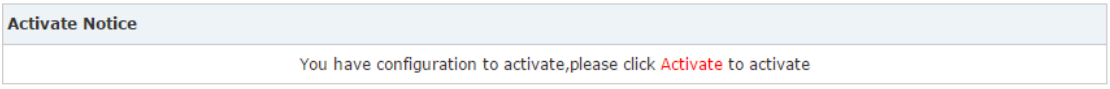
After you have made changes to the IPPBX system there will be a notice at the top of the web page:



And also a button  will appear on the top left corner of the web page. Click either the notice message or the button to activate the changes made to the IPPBX system.

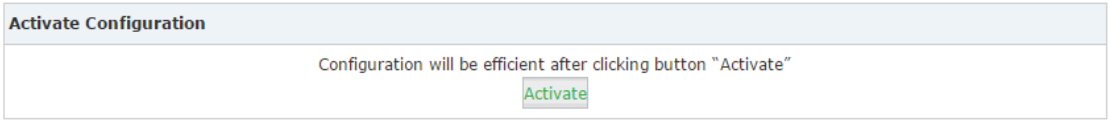
5.5.2 Activate Configurations of the Router Gateway system

If you make configuration changes to the router gateway system then a notice will appear at the bottom of the web page.



By clicking Activate button it will redirect you to *System Administration->Activate Configuration* page for you to activate the changes made, click "Activate" button then the router gateway system will restart the services to make sure the configurations takes effect. This process will take around 50 seconds.

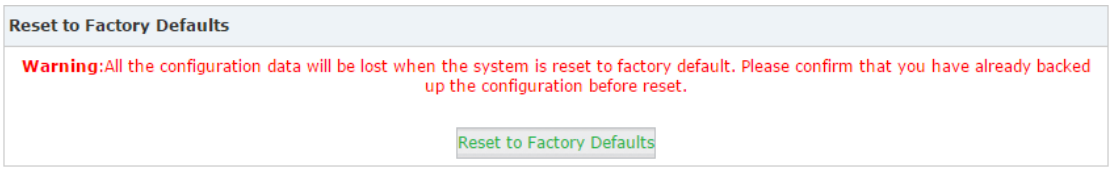
You can also navigate to the *System Administration->Activate Configuration* page to activate the new configurations.



5.6 Reset &Reboot

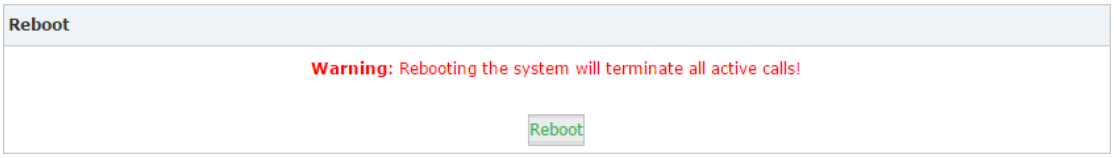
5.6.1 Reset

Navigate to web menu: *System Administration->Reset & Reboot*



If you click the "Reset to Factory Defaults" button then you will reset the configurations of the UC510 system back to factory default settings.

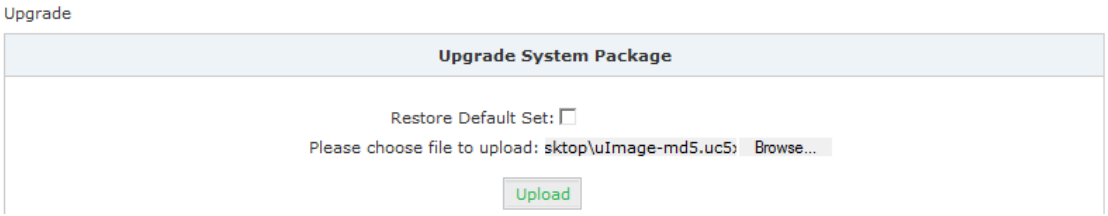
5.6.2 Reboot



By clicking the "Reboot" button the system will restart, the whole process will take around 3 mins.

5.7 Upgrade

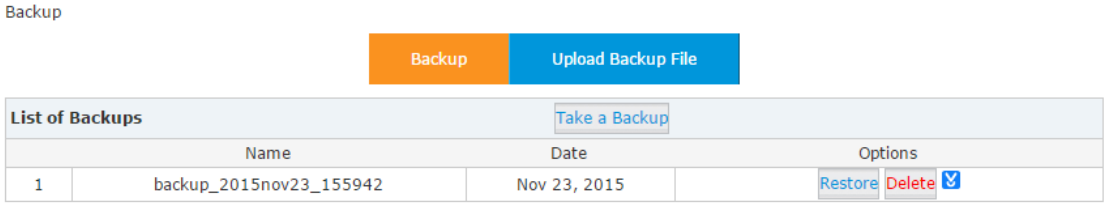
You can check new firmware release for UC510 for bug fix or new features from our office website: www.zycoo.com.
After downloading the firmware package(it will come as a zip file please extract it with winrar), please upload the uImage-md5.uc5xxx file to upgrade the UC510 firmware.
Navigate to web menu: *System Administration->Upgrade*



Click "Browse" button to select the firmware package and click upload to start upgrading the firmware. If you enable "Restore Default Set" then after upgrading the system will also be reset to factory default settings.

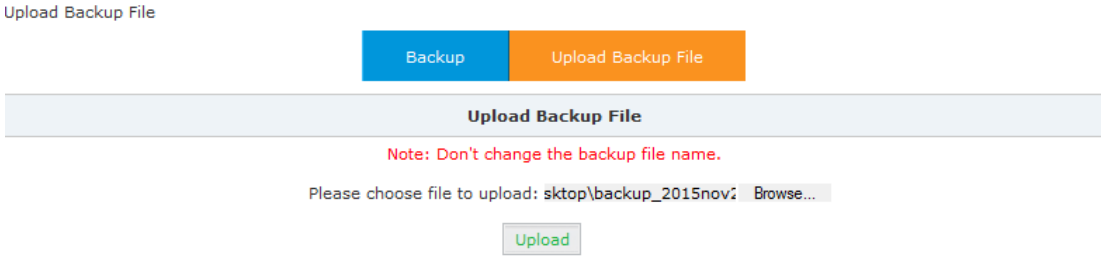
5.8 Backup

Taking backup of the UC510 system is important, especially after you have spent time configuring the system to meet your requirements. A backup can then be used at a later date to easily recover the system to a known good state.
Navigate to web menu: *System Administration->Backup*
Click "Take a Backup" button to backup the currect configurations of the UC510 system.



After taking this backup the backup file will be listed on this page, and the file name including the time of exactly when this backup was taken. By clicking "Restore" button you can restore the system and the configuration to the exact date and time of the backup file.

Also you can delete this backup from the system or you can download it to your operating system.
Click the "Upload Backup File" tab, you can choose a backup file from your local file system and restore to the UC510 system.



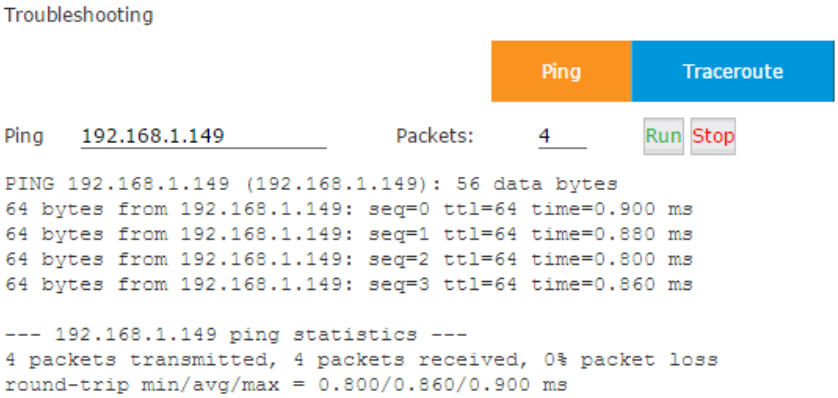
5.9 Troubleshooting

Troubleshooting includes two tools for you to check the network reachability, ping and traceroute. With these tools you'll get an outside view of your network response time and network topology, which allows you to track down possible errors more easily.

5.9.1 Ping

The ping command is a very common method for troubleshooting the accessibility of devices. It uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine:

- Whether a remote host is active or inactive.
- The round-trip delay in communicating with the host.
- Packet loss.

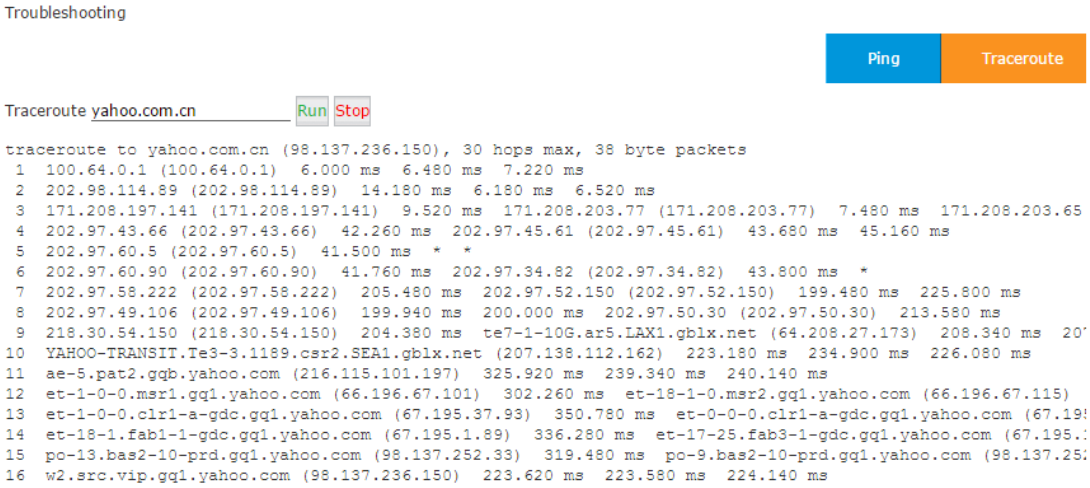


To use ping, simply specify the domain or IP of the host and how many packets you want to send and click "Run" button to start the process. The results will be listed below.

5.9.2 Traceroute

The traceroute command is used to discover the routes that packets actually take when traveling to their destination.

Click "Traceroute" tab and specify the domain or IP address you want to lookup then click "Run" button to start the process.



After the process system will notice "Trace Complete" and you can see which routes the packets taken before reaching the final destination.