



CooCenter Technical Documentation



PBX Admin User Guide

software version v3.1.0

Software version v3.0.0

Contents

Overview.....	- 1 -
Product Introduction.....	- 1 -
Main Features.....	- 7 -
Environment Requirement.....	- 8 -
Package List.....	- 8 -
System Login.....	- 9 -
Basic.....	- 13 -
Extensions.....	- 13 -
New Extension.....	- 13 -
Other Extension.....	- 15 -
Trunks.....	- 16 -
VoIP Trunks.....	- 16 -
FXO Trunk.....	- 18 -
E1/T1 Trunk.....	- 21 -
BRI Trunk.....	- 22 -
Outbound Routes.....	- 24 -
Dial Plans.....	- 24 -
Dial Rules.....	- 25 -
Operator.....	- 26 -
Inbound Control.....	- 28 -
Inbound Routes.....	- 28 -
General.....	- 28 -
Port DIDs.....	- 28 -
Number DIDs.....	- 29 -
IVR.....	- 29 -
IVR Prompts.....	- 31 -
IVR Prompts.....	- 31 -
Upload IVR Prompts.....	- 31 -
Call Queue.....	- 32 -
Auto Call Settings.....	- 34 -
Ring Groups.....	- 35 -
Black List.....	- 36 -
Time Based Rules.....	- 37 -
Time Settings.....	- 37 -
Holiday Settings.....	- 37 -
Time Based Rules.....	- 38 -
Advanced.....	- 39 -
Options.....	- 39 -
General.....	- 39 -
Analog Settings.....	- 40 -
SIP Settings.....	- 42 -
IAX2 Settings.....	- 45 -

Module Settings.....	- 46 -
E1 PRI Settings.....	- 46 -
T1 PRI Settings.....	- 47 -
BRI Settings.....	- 48 -
MFC/R2 Settings.....	- 49 -
SS7 Settings.....	- 50 -
Voicemail.....	- 51 -
General.....	- 51 -
Email Settings.....	- 52 -
SMTP Settings.....	- 52 -
Conferences.....	- 53 -
Music Settings.....	- 55 -
Call Forward.....	- 56 -
Paging and Intercom.....	- 57 -
PIN Sets.....	- 58 -
Call Recording.....	- 59 -
Feature Codes.....	- 60 -
Phone Provisioning.....	- 67 -
PnP Settings.....	- 67 -
Phone Settings.....	- 68 -
Network Settings.....	- 69 -
Network.....	- 69 -
IPV4 Settings.....	- 69 -
IPV6 Settings.....	- 71 -
VLAN Settings.....	- 72 -
Static Routing.....	- 73 -
Static Routing.....	- 73 -
Routing Table.....	- 73 -
VPN.....	- 74 -
L2TP VPN.....	- 74 -
PPTP VPN.....	- 76 -
OpenVPN.....	- 79 -
IPSec VPN.....	- 81 -
N2N VPN Client.....	- 83 -
DHCP Server.....	- 84 -
DHCP Server.....	- 84 -
DHCP Client List.....	- 86 -
Static MAC.....	- 86 -
DDNS Settings.....	- 87 -
Security.....	- 88 -
Firewall.....	- 88 -
Fail2Ban.....	- 90 -
Fail2Ban.....	- 90 -
Settings.....	- 91 -

Report.....	- 91 -
Register Status.....	- 91 -
SIP Users Status.....	- 91 -
IAX2 Users Status.....	- 92 -
SIP Trunks Status.....	- 93 -
IAX2 Trunks Status.....	- 93 -
Record List.....	- 94 -
Call Recording.....	- 94 -
Conference.....	- 95 -
One Touch Recording.....	- 95 -
Call Recording Playback.....	- 96 -
Call Logs.....	- 96 -
System Logs.....	- 98 -
System.....	- 98 -
Time Settings.....	- 98 -
NTP.....	- 99 -
Manual Time Set.....	- 99 -
Data Storage.....	- 100 -
Data Storage.....	- 100 -
Data Storage Log.....	- 102 -
Management.....	- 103 -
Set System Voice Prompts.....	- 103 -
Backup.....	- 104 -
Take a Backup.....	- 104 -
Upload Backup File.....	- 105 -
Troubleshooting.....	- 106 -
Ping.....	- 106 -
Traceroute.....	- 106 -
Tcpdump.....	- 107 -
Channel Monitor.....	- 108 -
Reset & Reboot.....	- 110 -
Reset.....	- 110 -
Reboot.....	- 110 -
Upgrade.....	- 111 -
WebUpgrade.....	- 111 -
TFTP Upgrade.....	- 112 -

Overview

Product Introduction

- CooCenter-S10+



CooCenter-S10+ Front View



CooCenter-S10+ Back View

CooCenter-S10+ Specifications

Hardware	Ram	1GB DDR3
	Storage	16GB SD Card
	USB (External Storage)	USB2.0 (Max. 1TB mobile HDD with external power supply)
	Ethernet	2x10/100Mbps
	Power	Input: AC 100~240V; Output: DC 12V 1A
System	Call Center Agents	10 (WebRTC or SIP extensions)
	IP PBX Extensions	20
	Simultaneous Calls	10
Capacity		
Telephony Interfaces		4FXO/2FXO+2FXS/4FXS

CooCenter-S10+ LED Indication

The LED indicators on the front panel indicate the interface connection and system activity status of the CooCenter-S10+ system.

LED Label	Function	Status	Indication
PWR	Power Status	On	Power on
		Off	Power off
SYS	System Status	On	System initiating
		Blink	System is functioning
		Off	System failure
WAN	WAN Status	On	Connected but no data transmitting
		Blink	Data transmitting
		Off	Disconnected
LAN	LAN Status	On	Connected but no data transmitting
		Blink	Data transmitting
		Off	Disconnected
1,2,3,4	FXO Status	Red	Channel available
		Blink	Channel ringing
		Off	Channel failure
	FXS Status	Green	Channel available
		Blink	Channel ringing
		Off	Channel failure

- CooCenter-S30



CooCenter-S30 Front View



CooCenter-S30 Back View

CooCenter-S30 Specifications

Hardware	RAM	4GB DDR3L
	Storage	16GB EMMC + 500GB HDD
	USB (External Storage)	2xUSB (Max. 1TB mobile HDD with external power supply)
	Ethernet	2x10/100/1000Mbps
	Power	AC 100~240V
Telephony	Slot1	E1/T1/4FXO/4FXS/4GSM
	Slot2	E1/T1/4BRI/4FXO/4FXS/4GSM
System Capacity	Call Center Agents	60 (WebRTC or SIP extensions)
	IP PBX Extensions	120
	Simultaneous Calls	30

Feasible Module Combinations

For better performance please follow the feasible module combinations in the below table to install you module cards on the CooCenter-S30 call center system. The combinations which have been marked as “No” are not recommended and may cause module cards malfunction.

Slot 1	Slot 2	Feasibility
E1 Module	Vacant	No
4BRI Module		No
FXO/FXS Module		Yes
GSM/WCDMA Module		Yes
Vacant	E1 Module	Yes
	4BRI Module	Yes
	FXO/FXS Module	Yes
	GSM/WCDMA Module	Yes
FXO/FXS Module	E1 Module	Yes
	4BRI Module	Yes
	FXO/FXS Module	Yes
	GSM/WCDMA Module	Yes
GSM/WCDMA	E1 Module	Yes
	4BRI Module	Yes
	FXO/FXS Module	Yes
	GSM/WCDMA Module	Yes
E1 Module	E1 Module	Yes
	4BRI Module	No
	FXO/FXS Module	No
	GSM/WCDMA Module	No
4BRI Module	E1 Module	No
	4BRI Module	No
	FXO/FXS Module	No
	GSM/WCDMA Module	No

CooCenter-S30 LED Indication

The LED indicators on the front panel indicate the interface connection and system activity status of the CooCenter-S30 system.

Identification	Indication	Status		Specification	
PWR	Power States	Green		Power On	
		Off		Power Off	
SYS	System States	Wink		System is Running	
		Off		System Booting or Failed	
WAN/LAN	WAN/LAN Interface States	Wink		Data Transmitting	
		Off		No Data Transmitting	
1-4	Slot1 and Slot2 States	FXS	Green	Channel Loading Succeed	
			Wink	Channel Ringing	
			Off	Channel Loading Failure	
		FXO	Red	Channel Loading Succeed	
			Wink	Channel Ringing	
			Off	Channel Loading Failure	
		GSM/WCDMA	Red	Channel Loading Succeed	
			Wink	Channel Ringing	
			Off	Channel Loading Failure	
		E1/T1 (PRI/R2)	L1	Red	Module Loading Succeed
				Off	Module Loading Failure
			L2/L3	Red/Off	CPE Signaling
				Green/Off	NET Signaling
				Off/Red	SS7 Signaling
				Off/Green	R2 Signaling
			L4	Green	Connected (No Alarm)

(SLOT1/2)				Red	Disconnected (Alarm)
		BRI		Red	TE Mode
				Green	NT Mode
				Off	Module Loading Failure

Main Features

Call Center	Call Popup	Call Queues	Callback Reminder
	Remote Agents	SIP Agents	WebRTC Agents
	ACD	Call Monitoring	Click-to-call
	Auto Dial	Satisfaction Survey	Call Statistics
	Built-in CRM	Questionnaire	Call Barging
	Whisper Coaching	IVR	Voicemail
IP PBX Features	Caller ID	Video Calls	Paging & Intercom
	Voicemail	DID	Voicemail to Email
	IVR	PIN Set	Call Recording
	3-way Calling	Conference Call	Phone Provisioning
	SIP Trunking	Blacklist	BLF
	Feature Codes	Call Transfer	Call Parking
	Call Forward	Call Hold	Call Waiting
	Ring Groups	Call Pickup	MOH
Network Features	Network Protocols	IPv4, IPv6	
	Network Mode	Static IP, DHCP, PPPoE	
	VPN (Server/Client)	L2TP, PPTP, OpenVPN, N2N	
	Transport Protocols	UDP, TCP, TLS	
	Others	DDNS, HTTPS, SSH	
Security		Firewall, IP Blacklist, Auto Defense	
Codecs & Signaling	Audio Codecs	G.711(a,u), G.729, G.722, G.726, GSM, Speex	
	Video Codecs	H.264, H.263+, H.263, H.261	
	Signaling	SIP (RFC3261), IAX	
	DTMF Mode	RFC2833, SIPINFO, In-band	

Environment Requirement

- Operating Temperature: 0 °C ~40 °C
- Storage Temperature: -20 °C ~ 55 °C
- Humidity: 5~95% Non-Condensing

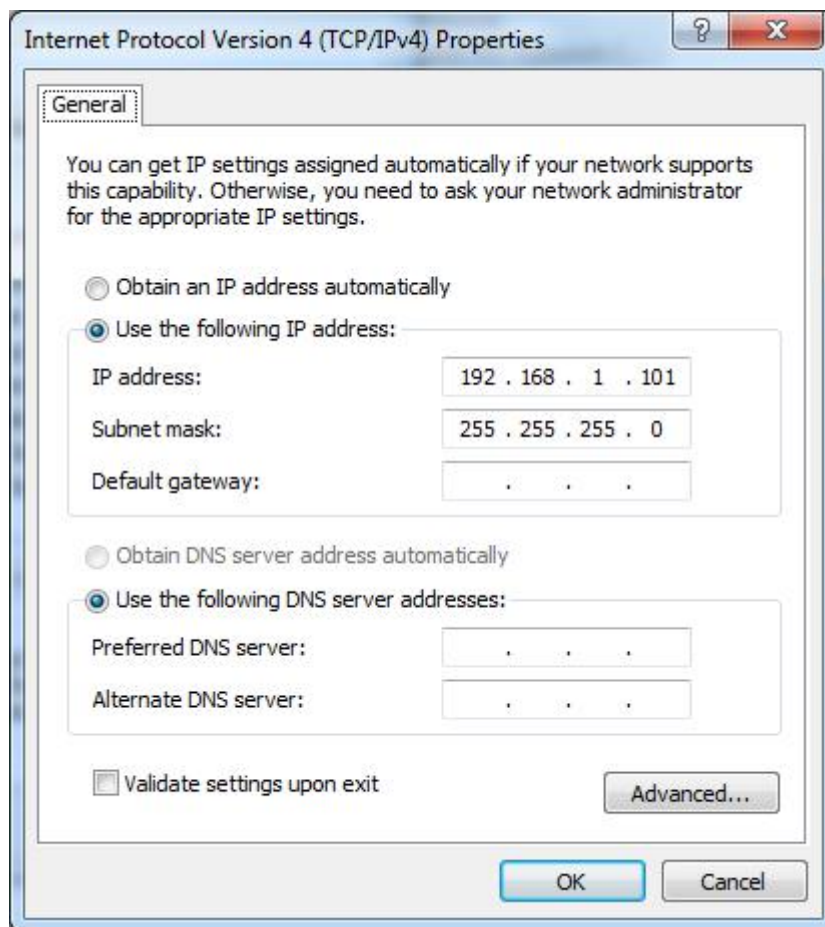
Package List

Items	CooCenter-S10+	CooCenter-S30
Main Case	1	1
Power Adaptor	1	1
Ethernet Cable	1	1
Quick Installation Guide	1	1
Warranty Card	1	1
Module	N/A	According to order

System Login

CooCenter system has been preconfigured with a static IP address of 192.168.1.100 on the devices WAN port (192.168.10.100 on LAN port). If your network is configured with a different IP range to the CooCenter system default address, then you will need to change the IP address to something more appropriate before connecting to your local LAN.

Please connect your PC directly to the WAN interface of the system and change the network profile of the PC to an IP address of 192.168.1.101 and Subnet mask of 255.255.255.0.

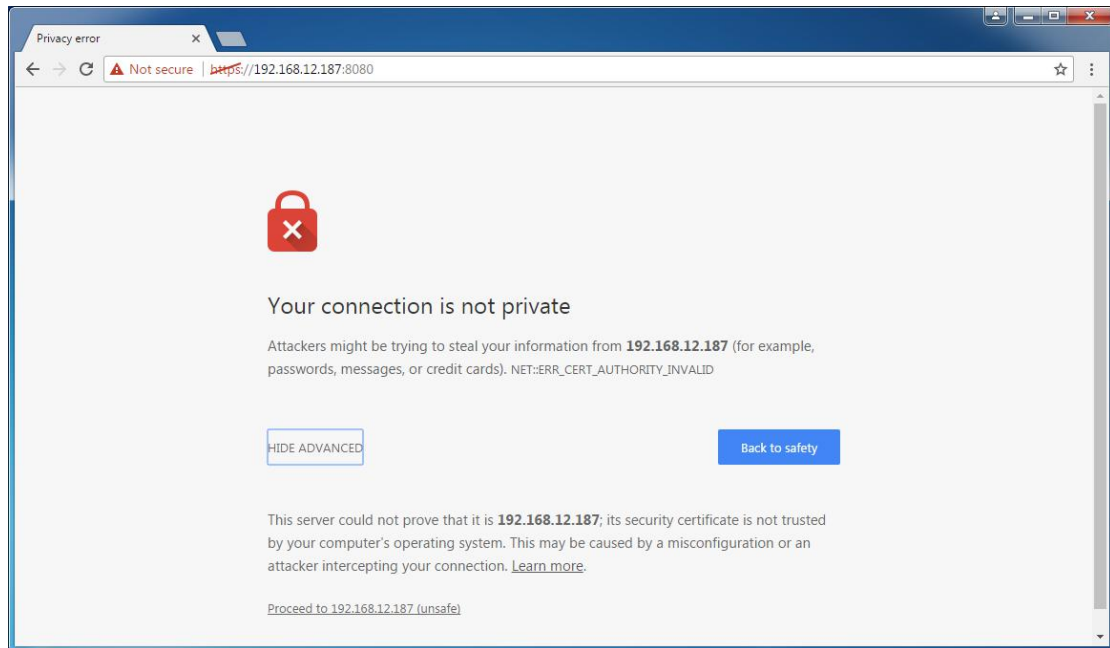


Now you can access the Web interface by typing URL <http://192.168.1.100> into your Internet browser address bar and pressing Enter.

We recommend you using Google Chrome or Opera browser for Web extension (WebRTC) functionality when login as call center agents.

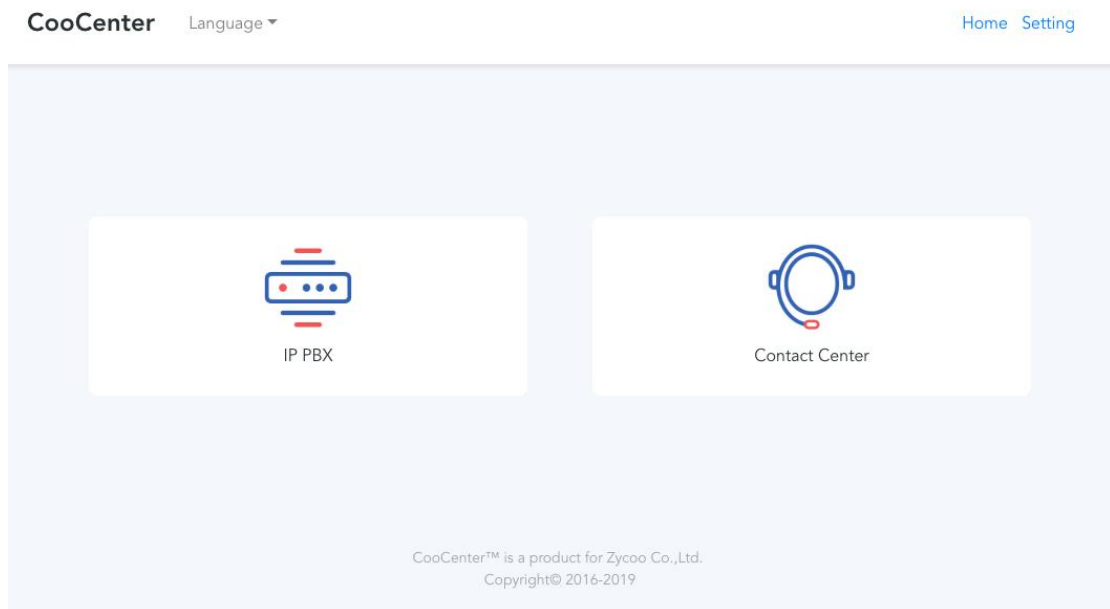


You'll now be presented with a Certificate Error notice as below.



Please click “Advanced” then click on “Proceed to...” and you will be directed to the login page.

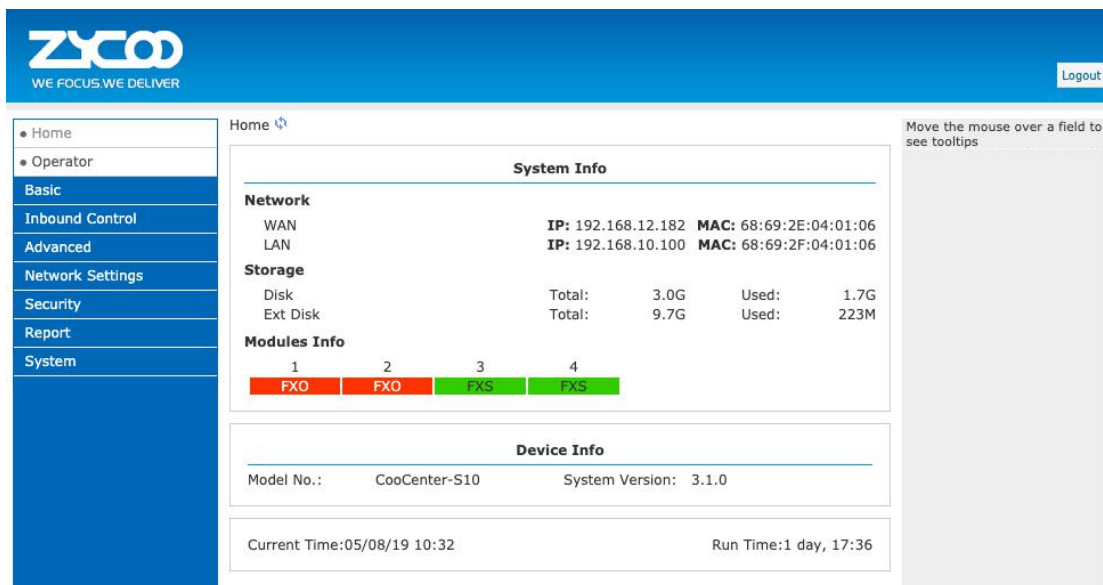
First you'll see the CooCenter Web GUI login screen.



Click the icon 【IP PBX】, Go to IP PBX configuration page



Enter the default username 'admin' and default password 'admin' to login in. After successfully logged in, you will be noticed to change the default admin password. Please follow the instructions within the notice to do this. To ensure the device is secure, the admin password must be complex, so please set a strong password that uses a combination of letters, numbers and also special characters. Every time when you have successfully logged in the IP PBX Web interface, you'll first see the Home page.



On the Home screen, you can check the system status/info.

- **Network:** shows the configurations of WAN and LAN port IP address and MAC address.
- **Disk:** shows the internal system storage usage.
- **Ext Disk:** shows the external storage (USB)usage.

- [Modules Info](#): shows the telephony interface configuration and status.
- [Device Info](#): shows the device model and current software version.

Basic

Extensions

Path: **Basic->extensions**

This page lists all user extensions on CooCenter system IP PBXWeb interface. Here you can add/bulk add, delete/bulk delete user extensions and also edit/bulk edit the user extension properties.

Extensions

ExtensionWeb Extensions

Extension: Search Show All Import Export

New User Batch Add Edit Selected Delete Selected Delete All

<input type="checkbox"/>	Name	Extension	Port	Protocol	DialPlan	Outbound CID	Options
<input type="checkbox"/>	1 800	800	--	SIP	DialPlan1		Edit
<input type="checkbox"/>	2 801	801	--	SIP	DialPlan1		Edit
<input type="checkbox"/>	3 802	802	--	SIP	DialPlan1		Edit
<input type="checkbox"/>	4 803	803	--	SIP	DialPlan1		Edit
<input type="checkbox"/>	5 804	804	--	SIP	DialPlan1		Edit
<input type="checkbox"/>	6 805	805	--	SIP	DialPlan1		Edit
<input type="checkbox"/>	7 806	806	--	SIP	DialPlan1		Edit
<input type="checkbox"/>	8 807	807	--	SIP	DialPlan1		Edit
<input type="checkbox"/>	9 808	808	--	SIP	DialPlan1		Edit
<input type="checkbox"/>	10 809	809	--	SIP	DialPlan1		Edit

By default, 10 extension numbers within the range of 800 to 809 have been created for you to use.

New Extension

You can add further extensions one by one by clicking the “[New User](#)” button or bulk add extensions by clicking “[Batch Add](#)” button and completing the popup shown below.

Batch Add X

Extension Start: 810 Extension End: 829

DialPlan: DialPlan1 Password: (Random ☒)

Save Cancel

- **Extension Start/Extension End:** These two fields define the new extension range to be generated.
- **DialPlan:** Select a dial plan for the new extensions.

- **Password:** A secure random password consisting of numbers, letters and special characters is the recommended choice and can be selected by selecting the “Random” checkbox. Alternatively, you can specify the same password for all new extensions. If you choose this option then please ensure a secure password is set. Or if you only need to add one new extension, you can click on “New User”.

More details of every parameter please refer to the table below.

- **SIP**、**IAX2**: (Session Initiation Protocol) Check this option if the User or Phone is using SIP or is a SIP device
- **Name**: A character-based name for this user, eg. 'Tom'
- **Extension Number**: The numbered extension, eg. '888', that will be associated with this particular User / Phone.
- **Password**: The password for the user's sip/iax2 account , eg: '12u3b6'
- **Outbound CID**: Overrides the caller id when dialing out with a trunk.
- **DialPlan**: Please choose the Dial Plan for this user, Dial Plan is defined under the "Outbound Routes".
- **AnalogPhone**: If this user is attached to an analog port on the system, please choose the port number here.
- **Enable**: This user will have a voicemail account after choosing this option.
- **Password**: Voicemail Password for this user, eg: "1234".
- **Delete VMail**: Voicemail will not be checkable by phone if you chose this option. Messages will be sent by e-mail only. Note:you must configure SMTP server for this functionality.
- **Email**: The e-mail address for this user, used to receive fax or voicemail(you need

- enable 'fax to email' or 'voicemail' function). eg. 'Tom@gmail.com'
- **Web Manager:** Enable the extension user login the system with extension number and password.
 - **Agent:** Check this option if this User or Phone is an Call Agent.
 - **Call Waiting:** Check this option if the User or Phone should have Call-Waiting capability.
 - **Allow Being Spied:** Check this option if the user allow being spied.
 - **Pickup Group:** Select your pickup group
 - **Mobility Extension:** Enable/Disable Mobility Extension
 - **Mobility Extension Number:** If enable this Setting, while you dial the server with this mobile number, the mobile phone will get the permission of the extension. For example: dialing other extension, playing the voicemail.
 - **NAT:** Check this option if the User or Phone is located behind a NAT (Network Address Translation) enable gateway.
 - **Transfer Protocol:** Please choose the transfer protocol. UDP is by default.
 - **SRTP:** Enable SRTP for the extension.
 - **DTMF Mode:** The Dual-Tone-Multi-Frequency mode to be used is specified here and can be changed if necessary. The default is rfc2833.
 - **Permit IP:** IP address and network restriction. For example: 210.16.1.7/255.255.255.255 or 172.16.0.0/255.255.0.0
 - **Video Call:** Enable/Disable Video call for the extension.
 - **Audio Codecs:** The allowed codecs can be selected. By default only alaw, ulaw and G.729 are allowed.

Other Extension

We have limited the user extension number range in the CooCenter IPPBX Web interface to be between 800 and 899. If you require more extensions or you want extensions in other number ranges then you need to change the extension range before you can add new extensions.

Please navigate to web menu **Advanced->Options->General**.

In the “**Extension Preferences**” section you can change the user extension range.

Extension Preferences		
User Extensions	<u>800</u>	~ <u>869</u>
Web Extensions	<u>870</u>	~ <u>899</u>
Conference Extensions	<u>900</u>	~ <u>909</u>
IVR Extensions	<u>610</u>	~ <u>629</u>
Queue Extensions	<u>630</u>	~ <u>639</u>
Ring Group Extensions	<u>640</u>	~ <u>659</u>
Paging Group Extensions	<u>660</u>	~ <u>679</u>
<input type="button" value="Reset"/>		

In the above example, the user extension range has been changed to be between 100 and 599. If you now go back to the extension page you'll be able to add new extensions within this range.

Trunks

VoIP Trunks

Path: **Basic->Trunks->VoIP Trunks**

Asterisk PBX can register as a SIP user agent to a SIP proxy (provider). If you have subscribed to a VoIP service from an ITSP, then with the account details provided by them you can configure a VoIP trunk on your CooCenter system for the user extensions to share and make outbound phone calls.

Click "[New VoIP Trunk](#)" button and complete the account details provided to setup the trunk as in the example below.

New VoIP Trunk X

Description:

Protocol:

Peer Mode: ☐

Host: :5060

Maximum Channels*:

Prefix:

Outbound CID:

Trunk Outbound CID Preferred: ☐

☐ Without Authentication

Username:

Authuser:

Password:

☒ **Advanced Options**

From Domain: Insecure:

From User: Qualify(sec):

DID Number: Transport:

DTMF Mode: NAT: ☐ SRTP: ☐

Auto Fax Detection: ☐

Context: Language:

Audio Codecs

☒ ulaw ☒ alaw ☐ G.722 ☒ G.729 ☐ G.726 ☐ GSM ☐ Speex ☐ opus

Video Codes

☐ H.261 ☐ H.263 ☐ H.263+ ☐ H.264 ☐ VP8

- **Description:** A name for this trunk.
- **Protocol:** SIP or IAX2 protocol.
- **Peer Mode:** If enabled then Host blank will be hidden. Peer mode requires only that the authorization matches rather than the IP address.
- **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 prefix number you enter here will be added in front of any number you dial via this trunk. This feature is seldom required 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 require a username and password for this account to register to their server then 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:** Your service provider's domain name.
- **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 require this.
- **Qualify(sec):** Asterisk sends a SIP OPTIONS command regularly to check that the device is still online. Default value is 2(sec).

- **DID number:** Self defined, and can be used to setup number DID.
- **Transport:** Default transport type for SIP messages.
- **DTMF Mode:** Used to inform 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. This feature is often required when there is a firewall located between the PBX and the service provider.
- **Context:** Custom dial plan for this trunk, by default it uses the “default” dial plan. Configure only if this trunk is for branch office integration, so calls coming from the other side can dial out from this CooCenter trunk directly. DO NOT change unless you fully understand how this feature works.
- **Language:** You can choose a desired language of the system voice prompts to play to the incoming calls from this trunk. For example, if the call is not answered or the user is busy the CooCenter system will notify the caller to leave a voice message in the language you set.
- **Audio Codecs:** Select the audio codec/codecs the provider can support.
- **Video Codecs:** If the ITSP supports video calls then you can enable compatible video codecs here for video phone calls.

With the exception of configuration options related to your service provider and your account details, please do not change the trunk advanced parameters if you are not familiar with them. After the SIP trunk is successfully added you can see it listed here on this page.

List of Trunks					New VoIP Trunk
	Provider Name	Type	Hostname/IP	Username	Options
1	International	SIP	gw1.sip.us	525274xxxx	Edit Delete

By clicking “[Edit](#)” you can modify the trunk settings and by clicking “[Delete](#)” you can remove this trunk from the CooCenter system.

FXO Trunk

FXO Trunks

On the CooCenter device front panel, red LED indicates the RJ11 interface is FXO. You should attach the telephone wire from your telecom socket to the FXO ports. Once connected you should be able to see the connection status on [Operator](#) page “[FXO/FXS/GSM Ports](#)” section.

FXO/FXS/GSM Ports				
Status	Signal Strength	Type	Port	BLF Label
Connected		FXO	1	Channel1
Connected		FXO	2	Channel2
Connected		FXO	3	Channel3
Connected		FXO	4	Channel4
Disconnected		FXO	5	Channel5
Connected		FXO	6	Channel6
Connected		FXO	7	Channel7
Connected		FXO	8	Channel8

To be able to make calls on your FXO interface you will first need to create a trunk(s). To create a trunk you need to navigate to web menu Basic->Trunks->FXO/GSM Trunks. Click “[New FXO/GSM/WCDMA Trunk](#)” button and you’ll see the available port numbers that can be used.

Edit

X

Description:

port1-8

Lines:

FXO: ☒1 ☒2 ☒3 ☒4 ☒5 ☒6 ☒7 ☒8

Prefix:

Advanced Options

Call Method:

Order

Busy Detection:

Yes

Busy Count:

3

Busy Pattern:

Language:

Default

Input Volume:

60%

Output Volume:

40%

Caller ID Start:

Ring

Caller ID Signaling:

Bell-US

Answer on Polarity Switch:

No

Hangup on Polarity Switch:

No

Auto Fax Detection:

☐

Save

Cancel

- **Description:** A name for this FXO trunk.
- **Lines:** Available FXO and GSM ports.
- **Prefix:** The prefix number you enter here will be added in front of any number you dial via this trunk. This feature is seldom required so please leave this field blank.
- **Call Method:** If in this trunk you have more than 1 FXO/GSM ports selected, then this parameter defines how to use these 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 incoming calls from FXO channel/channels.
- **Output Volume:** The volume of the outgoing calls from FXO channel/channels.
- **Busy Pattern:** If busy detection is enabled, it is also possible to specify the cadence of your busy signal.
- **Language:** You can choose a desired language of the system voice prompts to play to the incoming calls from this trunk. For example, if the call is not answered or the

user is busy the CooCenter system will notify the caller to leave a voice message in the language you set.

- **Answer on Polarity Switch:** When enabled, FXO (FXS signaled) ports watch for a polarity reversal to mark when an outgoing call is answered by the remote party.
- **Hangup on Polarity Switch:** In certain countries, a polarity reversal is used to signal the disconnection of a phone line. If the “hangup on polarity switch” option is selected, the call will be considered "hung up" on a polarity reversal.

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

GSM/WCDMA Trunk

If you have ordered GSM or WCDMA modules for your CooCenter system, the user extensions will be able to make and receive phone calls from the mobile network. You first have to insert SIM cards into the SIM slots of the GSM/WCDMA modules and then install the modules to the CooCenter module slots. Antennas should be properly installed and placed in open space for better signal reception. After completing the above, power on the CooCenter and you'll be able to configure GSM/WCDMA trunks in exactly the same way as you configure FXO trunks.

GSM and WCDMA Specifications

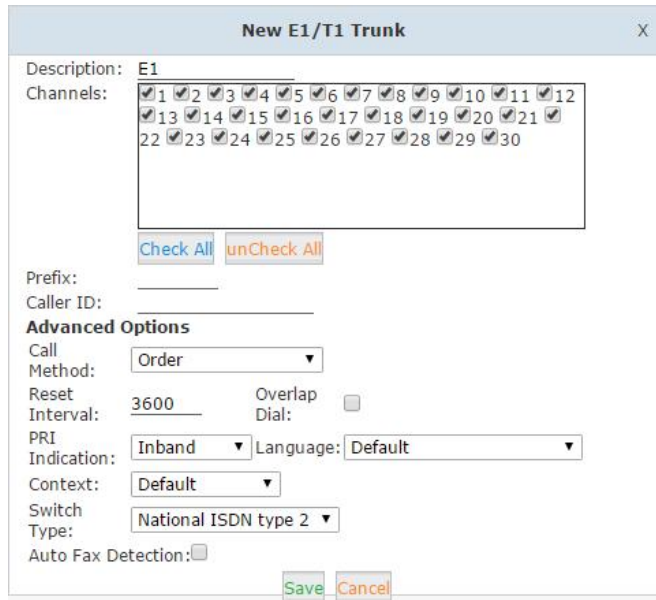
Module	Working Frequencies
2GSM	GSM/GPRS 850/900/1800/1900MHz
4GSM	GSM/GPRS 850/900/1800/1900MHz
2WCDMA	Quad-band: GSM850, EGSM 900, DCS 1800, PCS 1900. SIM5320A: Dual-Band UMTS 850/1900MHz SIM5320E: Dual-Band UMTS 900/2100MHz SIM5320J: Dual-Band UMTS 850(800)/2100MHz
4WCDMA	

Notice

CooCenter-S10+ only support VoIP and FXO trunks, VoIP/FXO/GSM/WCDMA/E1/T1/BRI trunks are supported on CooCenter-S30 system.

E1/T1 Trunk

If you have E1 module installed you'll get a new tab on **Basic-Trunks** page named E1/T1 Trunks. Click on this tab and click on **"New E1/T1 Trunk"** you'll be able to create a new E1/T1 trunk.



E1 connections have 32 channels in total, 30 channels are used as bearer channels (B channels) and 2 channels are used as data channels (D channels). While T1 connections have 24 channels in total, 23 channels are used as B channel and 1 channel is used as D channel.

In the above example, it's an E1 connection so you have 30 available channels to be configured for voice phone calls, if the module is configured to work as T1 then there will be 24 available channels.

Below are the introductions of trunk configuration parameters.

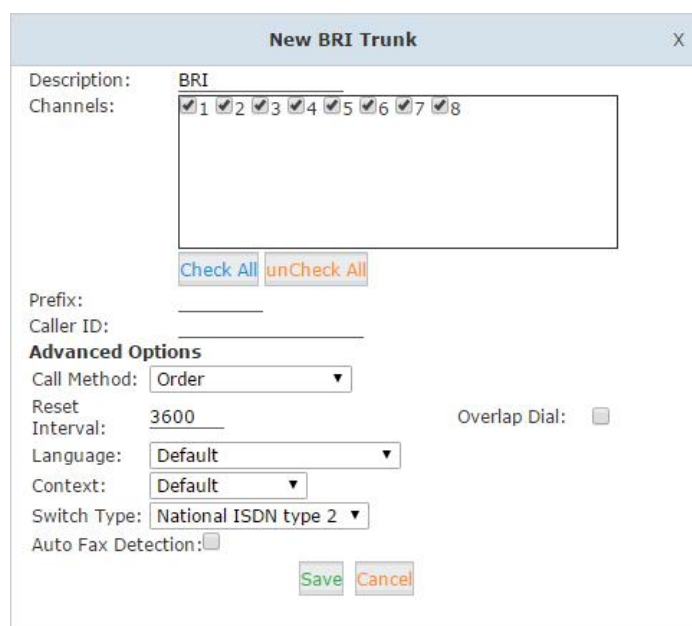
- **Description:** A name to identify this E1 trunk.
- **Channels:** All available B channels of the E1 trunk.
- **Prefix:** The prefix number you enter here will be added in front of any number you dial via this trunk. This feature is seldom required so please leave this field blank.
- **Caller ID:** The number you want to display to the called party.
- **Call Method:** Defines how to use these channels for outbound phone calls.
- **Reset Interval:** Sets the time in seconds between restart of unused B channels.
- **Overlap Dial:** Overlap dialing mode (sending overlap digits).
- **PRI Indication:** Enable this to report Busy and Congestion on a PRI using out-of-band notification.
- **Language:** Custom a system voice prompts language for the callers calling in from this trunk.
- **Context:** Rules of how to handle the inbound calls, default value is "Default" and it's

recommended do not change it or you may not be able to receive inbound calls.

- **Switch Type:** Sets the type of PRI switch being used by the telephony provider.
- **Auto Fax Detection:** Automatically detect inbound faxes and send to specific destination.

BRI Trunk

If you have BRI module installed you'll get a new tab on **Basic->Trunks** page named BRI Trunks. Click on this tab and click on **"New BRI Trunk"** you are able to create a new BRI trunk.



The ISDN BRI configuration provides 2 bearer channels (B channels) and 1 data channel (D channel). There are 2 channels each BRI port that can be used for voice phone calls. ZYCOO 4BRI module has 4 BRI ports equipped, so in total there are 8 channels available for you to configure BRI trunks.

Below are the introductions of trunk configuration parameters.

- **Description:** A name to identify this E1 trunk.
- **Channels:** All available B channels of the E1 trunk.
- **Prefix:** The prefix number you enter here will be added in front of any number you dial via this trunk. This feature is seldom required so please leave this field blank.
- **Caller ID:** The number you want to display to the called party.
- **Call Method:** Defines how to use these channels for outbound phone calls.
- **Reset Interval:** Sets the time in seconds between restart of unused B channels.
- **Language:** Custom a system voice prompts language for the callers calling in from this trunk.
- **Context:** Rules of how to handle the inbound calls, default value is "Default" and it's recommended do not change it or you may not be able to receive inbound calls.

- **Switch Type:** The ISDN switchtype must be set to match the switching equipment being used by the telephony provider.
- **Auto Fax Detection:** Automatically detect inbound faxes and send to specific destination.

Outbound Routes

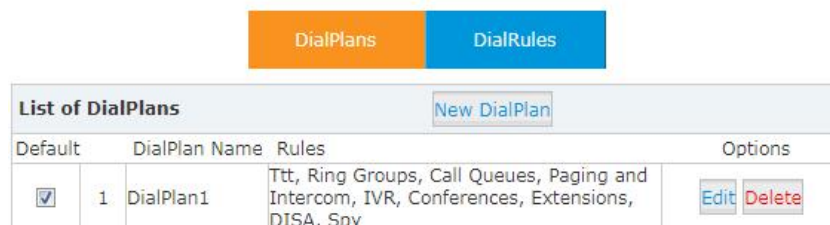
Outbound Routes allow you to define a set of dial rules that tell your CooCenter system which Trunks (phone lines) to use when people dial external telephone numbers. A simple installation will direct CooCenter system to send all calls to a single trunk. However, a complex setup could have for example an outbound route for emergency calls, another outbound route for local calls, another for long distance calls, and perhaps even another for international calls.

With all of the above possibilities, you may have to configure several trunks on your CooCenter system and therefore you will need to configure several dial rules and maybe also several dial plans.

Dial Plans

Path: **Basic->Outbound Routes->Dial Plans**

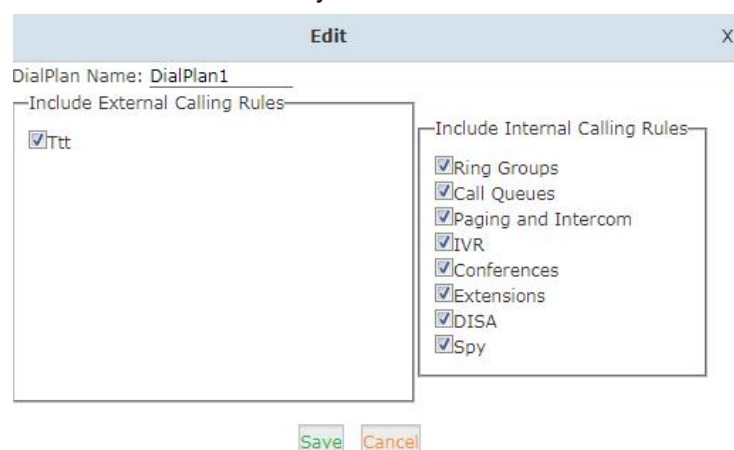
DialPlans



The screenshot shows the 'DialPlans' interface. At the top, there are two buttons: 'DialPlans' (orange) and 'DialRules' (blue). Below them is a table titled 'List of DialPlans' with a 'New DialPlan' button. The table has columns for 'Default', 'DialPlan Name', 'Rules', and 'Options'. There is one row for 'DialPlan1' which is the default plan. The 'Rules' column lists 'Ttt, Ring Groups, Call Queues, Paging and Intercom, IVR, Conferences, Extensions, DISA, Spy'. The 'Options' column has 'Edit' and 'Delete' buttons.

Default	DialPlan Name	Rules	Options
<input checked="" type="checkbox"/>	1 DialPlan1	Ttt, Ring Groups, Call Queues, Paging and Intercom, IVR, Conferences, Extensions, DISA, Spy	Edit Delete

A default dial plan already exists in the CooCenter system. For most installations you just have to click “[Edit](#)” button on the default dial plan “[DialPlan1](#)” and tick on all dial rules to enable them, now extension users will be able to call any destinations using the trunk lines of the CooCenter system.



The screenshot shows the 'Edit' dialog for 'DialPlan1'. It has a title bar 'Edit' with a close button 'X'. Below the title bar, it says 'DialPlan Name: DialPlan1'. There are two main sections: 'Include External Calling Rules' and 'Include Internal Calling Rules'. The 'Include External Calling Rules' section has a checkbox for 'Ttt' which is checked. The 'Include Internal Calling Rules' section has checkboxes for 'Ring Groups', 'Call Queues', 'Paging and Intercom', 'IVR', 'Conferences', 'Extensions', 'DISA', and 'Spy', all of which are checked. At the bottom, there are 'Save' and 'Cancel' buttons.

Calling rules in the left column are for external calls and calling rules in the right column are for internal calling. If you want to restrict some users from calling out through specific trunk lines or you don't want them to be able to call certain internal destinations, you can create a new dial plan by clicking the “[New DialPlan](#)” button.

New DialPlan
X

DialPlan Name:

Include External Calling Rules

☒ Ttt

Include Internal Calling Rules

☒ Ring Groups
☒ Call Queues
☒ Paging and Intercom
☒ IVR
☒ Conferences
☒ Extensions
☒ DISA
☒ Spy

In the new dial plan you should disable the rules you don't want others to use and save. After this, go to the extension configuration page and give the extension a different dial plan which ensures the restrictions you made take effect.

Dial Rules

Path: **Basic->Outbound Routes->Dial Rules**

List of DialRules
[New DialRule](#)

Rule Name	Dial Pattern	Call Using	Options
1 ttt	XXX	test	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

You can see there is one dial rule on the list. If needed, you should click “[New DialRule](#)” button to add a new dial rule.

New DialRule
X

Rule Name:

PIN Set: ☒

Record in CDR: ☒

Call Duration Limit: seconds

Time Rule: ☐

Place this call through:

Available Trunks

fxo(FXO/GSM)

Selected Trunks

Custom Pattern:

Z Any digit from 1 to 9
N Any digit from 2 to 9
X Any digit from 0 to 9
. Any number of additional digits

Delete digits prefix from the front and auto-add digit before dialing

- 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**.

ringing, in use and also on hold.

VoIP Trunks

You can check the status of all VoIP trunks configured on your CooCenter system via the Operator page “[VoIP Trunks](#)” section.

VoIP Trunks					
Status	Trunk Name	Type	Username	Hostname/IP/Port	Reachability
Registered	test	SIP	841	192.168.18.252:5060	OK (4 ms)

On the above picture, there is one VoIP trunks registered. Status, Trunks Name, Username, Hostname/Port and Reachability are listed in the table. If you want to create a new VoIP Trunks, please refer to [VoIP Trunks](#) page.

FXO/FXS Ports

On the CooCenter device front panel, red LED indicates the RJ11 interface is FXO. You should attach the telephone wire from your telecom socket to the FXO ports. Once connected you should be able to see the connection status on this page.

FXO/FXS Ports				
Status	Signal Strength	Type	Port	BLF Label
Disconnected		FXO	1	Channel1
Disconnected		FXO	2	Channel2
OK		FXS	3	
OK		FXS	4	

Inbound Control

The Inbound Control section is where you define how CooCenter system handles incoming calls. Typically, you determine the phone number that outside callers have called (DID Number) and then indicate which extension, Ring Group, Voicemail, or other destination to which the call should be directed.

Inbound Routes

General

Path: **Inbound Control->Inbound Routes->General**

For both FXO channels and 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 extension, then you can use a time rule to handle the inbound calls.

The screenshot shows the 'General' settings for inbound routes, divided into two sections: 'From FXO/GSM Channels' and 'From VoIP Channels'. Each section has a 'Distinctive Ring Tone' field and a 'Destination' dropdown menu. The 'From FXO/GSM Channels' section has a ring tone of ';info=domestic' and a destination of 'Goto Time Rule'. The 'From VoIP Channels' section has a ring tone of ';info=international' and a destination of 'Goto Time Rule'. Below the sections are 'Save' and 'Cancel' buttons.

From FXO/GSM Channels
Distinctive Ring Tone: ;info=domestic
Destination: Goto Time Rule

From VoIP Channels
Distinctive Ring Tone: ;info=international
Destination: Goto Time Rule

Save Cancel

Port DIDs

Path: **Inbound Control->Inbound Routes->Port DIDs**

If some of the FXO/GSM ports are dedicated to a specific calling service and you want them handling differently to your general inbound settings then you can configure “[Port DIDs](#)” here.

The screenshot shows the 'New Port DID' form. It has a 'Port' dropdown menu set to 'FXO Port 1', a 'Label' text field with 'VIP', and a 'Destination' dropdown menu set to 'Goto Extension'. Below the form are 'Save' and 'Cancel' buttons.

New Port DID	
Port: FXO Port 1	Label: VIP
Destination: Goto Extension	401(401)

Save Cancel

For the above example, all inbound calls from FXO port 1 will be directed to extension number 401. General inbound control will still work with other ports which have not been


configured with port DIDs.

Number DIDs

Path: **Inbound Control->Inbound Routes->Number DIDs**

Number DID is only for inbound control of VoIP/E1/T1/BRI channels but not FXO channels. If you have a VoIP/E1/T1/BRI trunk for outbound and inbound phone calls, then your service provider will issue you with a DID number with which people can call you on.

Click “[Number DIDs](#)” tab and click “[New Number DID](#)” button to add a number DID rule:



New Number DID		X
DID Number:	51097214	Label: Inquiry
Destination:	Goto Extension ▼	410(410) ▼
Save		Cancel

In this example, if the caller calls your DID number 51097214 the call will go directly to extension 410, general inbound control will not work with this DID number. If you experience problems setting inbound DID then please check with your service provider to confirm the exact DID number that the service provider is passing to the CooCenter system.

IVR

Path: **Inbound Control->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 for example: "press 1 for sales, press 2 for marketing, press 0 to speak to the operator".

Click “[New IVR](#)” button to add an IVR menu.

IVR Settings

Name: Extension:

Welcome Message

Please Select: [Custom Prompts](#)

Repeat Loops:

Timeout:

Dial other Extensions: ☐ [\(Custom\)](#)

Keypress Events

Key	Action
0	Goto Extension ▼ 401(401) ▼
1	Goto Ring Group ▼ sales ▼
2	Goto Ring Group ▼ marketing ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼
7	Disabled ▼
8	Disabled ▼
9	Disabled ▼
*	Disabled ▼
#	Disabled ▼
t	Goto Extension ▼ 401(401) ▼
i	Goto Extension ▼ 401(401) ▼

Let's look at the above example where your IVR message says "Press 1 for sales, press 2 for marketing, press 0 for operator". If the caller is on the IVR menu, and after they hear the voice prompts they press 1 then the sales ring group will ring, if 2 is pressed then the Marketing ring group will ring, if 0 is pressed then will the IVR 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 to navigate to Inbound Control->IVR Prompts page for new voice prompts.
- **Repeat Loops:** Define how many times to play the IVR menu to the caller.
- **Timeout:** Timeout for key pressing of each IVR loop.
- **Dial other Extensions:** If enabled, the caller can dial extension numbers directly when in the IVR.
- **Custom:** By clicking "Custom" you can set a dial plan for this IVR menu and the callers on the IVR will be able to dial other destinations that the dial plan allows.(Not recommended)
- **Key Press Events:** Define which destination to go by pressing a key on the phone keypad. If undefined keys are pressed then they will be handled by the "i" parameter, "i" which means invalid. And "t" stands for timeout, after all IVR loops are completed without the caller pressing any key then the incoming call will be handled by "t"

parameter.

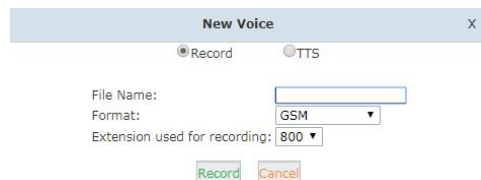
IVR Prompts

IVR Prompts

Path: **Inbound->IVR Prompts-> IVR Prompts**

To configure an IVR menu on CooCenter system you'll first need to record your IVR prompts, these IVR prompts will communicate to the callers the menu options that they have e.g. press one for sales.

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 speak to record your message. Once recording is complete your voice prompts will be listed on this page.

Upload IVR Prompts

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



Here you can select a pre-recorded voice prompts file from your operating system to upload and once complete your file will be listed on Voice Prompts page. Now you can use your file to setup your personalized IVR menu.

Call Queue

Path: **Inbound->Call Queues->Call Queues**

A call queue places incoming calls in line to be answered while extension users are busy with other calls. The queued calls are distributed to the next available extension user in the order received. Once a call queue has been created, it can be assigned to specific extensions and configured to feature greetings, messages, and hold music.

The call queues to be used on the call center system are managed here on the IP PBX system Web UI.

Call Queues

		Call Queues	Auto Call Settings
		Call Queues	
		New Queue	
Queue Number	Name	Label	Options
1	630	630	Edit Delete
2	631	631	Edit Delete
3	632	632	Edit Delete

There are 3 existing call queues pre-configured and all you have to do is click on “[Edit](#)” button to configure them. If you require more call queues then click on “[New Call Queue](#)”. Or if you want to delete a queue, please click on “[Delete](#)”.

Click on “[Edit](#)” button, and then you can be customized the call queue info on the following picture.

Edit

X

Call Queue Reference:

Queue Number: 630Name: 630

Ring Strategy: RoundRobinLabel:

Queue Options:

Announcements:

Agent TimeOut(sec): 15

Auto Pause:

Wrap-Up-Time(sec): 0

Max Wait Time(sec):

Max Callers: 8

Join Empty:

Leave When Empty:

Auto Fill:

Report Hold Time:

Play Recording

Reminder:

Caller Position Announcements

Frequency(sec): 30

Announce Hold Time: Yes

Periodic Announcements

Repeat Frequency(sec): 30

Announcements Prompt: all-busy

If not answered

Destination: Hangup

Save

Cancel

- **Queue Number:** This option defines the extension number that may be dialed to reach this Queue.
- **Ring Strategy:** This option sets the Ringing Strategy for this Queue. The options are:
RingAll -- Ring All available Agents until one answers(default).
RoundRobin -- Take turns ringing each available Agent.

LeastRecent -- Ring the Agent which was least recently called.

FewestCalls -- Ring the Agent with the fewest completed calls.

Random -- Ring a Random Agent.

RRmemory -- RoundRobin with Memory, Remembers where it left off in the last ring pass.

- **Name:** Define the queue name.
- **Label:** Defines a label for the queue. Show the Label when you receive incoming calls from the queue
- **Agent TimeOut (sec):** This option defines the time in seconds that an Agent's phone rings before the next Agent is rung, eg. "15"
- **Auto Pause:** Pauses an Agent if they fail to answer a call.
- **Wrap-Up-Time (sec):** After a successful call, how many seconds to wait before sending a potentially free agent another call(0 to No Delay).
- **Max Wait Time (sec):** The maximum number of seconds a caller can wait in a queue before being pulled out(empty for unlimited).
- **Max Caller:** Set the maximum number of callers that may wait in a Queue(0 to Unlimited). 8 callers are by default.
- **Join Empty:** Defining this option allows callers to enter the Queue when no Agents are available. If this option is not defined, callers will not be able to enter Queues with no available agents.
- **Leave When Empty:** Defining this option forces all callers to exit the Queue if New Callers are also not able to enter the queue. This option and "Join Empty" option can't be used at the same time.
- **Auto Fill:**Defining this option causes the Queue, when multiple calls are in it at the same time, to push them to Agents simultaneously. Thus, instead of completing one call to an Agent at a time, the Queue will complete as many calls simultaneously to the available Agents. It enable by default.
- **Report Hold Time:** CooCenter system will report the customer waiting time when this incoming call is answered.
- **Play Recording Reminder:** Before the agent answer, announce the voice prompts that CooCentersystem will record this conversation between agent and customer. Forexample: for better service, we will record to this conversation, please wait to connect customer service representative.
- **Frequency (sec):** How often to announce queue position and estimated holdtime(0 to Disable Announcements).It is 30s by default.
- **Announce Hold Time:** Announce the customer hold time. Either yes,no,or only once, but hold time will not be announced if <1 minute.The default option is "No".
- **Repeat Frequency (sec):** How often to announce a voice menu to the caller(0 to

Disable Announcements).

- **Announcements Prompt:** Select the 'Announcements Prompt' from IVR Prompts. The default voice prompts is “ all the service representatives are busy, please press 1 to keep waiting, or hang up to exit”
- **Destination:** Set the call destination If the queue not answered. Goto an extension, voicemail, etc.

Auto Call Settings

Path: **Inbound Control->Call Queues->Auto Call Settings**

Auto Call Settings determine how the CooCenter system processes the auto outbound dial tasks created by the call center supervisor users.

Auto Call Settings

Auto Call Settings	
Total Channels:	6
Ratio Of Valid Agents:	1
Interval Time(s):	8
Waiting Time(s):	60
Place this call through:	
<div>Save Cancel</div>	

- **TotalChannels:** You can set up maximum number of outbound calls for auto outbound dial.
- **RatioOfValidAgents:** Set the ratio of auto outbound calls with the valid agent. For example, if its value is set to 2, when there are 3 agents idle, and at this moment the auto outbound dial task starts, 6 calls will be made to the targeted customers.
- **InternalTime:** Set the internal time for each auto dialed outbound call.
- **WaitingTime:** Set the maximum waiting time for each call. If customer doesn't answer during the waiting time, this call will be stopped.
- **Placethiscallthrough:** Set the trunks for auto dialed.

Ring Groups

Path: **Inbound Control->Ring Groups**

In a ring group, an incoming call will ring the phones of everyone in the group at the same time.

Click “**New Ring Group**” button to add a ring group.

The screenshot shows a window titled "Edit - sales" with a close button (X). Inside, there are two main columns: "Ring Group Members" on the left and "Available Channels" on the right. The "Name" field is set to "sales" and the "Strategy" dropdown is set to "RingAll". The "Ring Group Members" list contains: 403(SIP) 403, 404(SIP) 404, 405(SIP) 405, and 406(SIP) 406. The "Available Channels" list contains: 401(SIP) 401, 402(SIP) 402, 407(SIP) 407, 408(SIP) 408, 409(SIP) 409, 410(SIP) 410, 411(SIP) 411, and 412(SIP) 412. Between the columns are four arrow buttons: a double left arrow, a single left arrow, a single right arrow, and a double right arrow. Below the columns, there is a "Label:" field, an "Extension for this ring group:" field with the value "640", and a "Ring (each/all) for lasting time(sec):" field with the value "20". Under the heading "If not answered", there are five radio button options: "Goto Extension", "Goto Voicemail", "Goto Ring Group", "Goto IVR", and "Hangup" (which is selected). At the bottom are "Save" and "Cancel" buttons.

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:** Defines how to ring the group members; selecting “**RingAll**” will ring all the member extensions at the same time, selecting “**Ring In Order**” will ring the member extensions one by one.
- **Ring Group Members:** The extensions selected to be the members of the ring group.
- **Available Channels:** All available extensions/channels can be added to the ring group.
- **Label:** Extensions can be members of multiple ring groups and therefore 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 will know which ring group the call is coming from.
- **Extension for this ring group:** Reach the ring group member by calling this extension.
- **Ring (each/all) for lasting time(sec):** Ring duration of the group members.
- **If not answered:** Defines a destination to redirect incoming calls to if no one answers from within the ring group.

Black List

Path: **Inbound Control->Black List**

Black list feature allows you to create a list of numbers that are not allowed to call in to the CooCenter system.

The Blacklist page shows all the blacklist numbers. You can delete one, and then this number will be allowed to call in to the system. Or if you want to delete more numbers at a time, check the numbers and click on “Delete Selected” button.

Black List

Black List			New Blacklist	Delete Selected
<input type="checkbox"/>	Blacklist Number		Options	
<input type="checkbox"/>	1	8001	Delete	

Click on “New Blacklist” to add a new blacklist.

New Blacklist

X

Blacklist Number: 84363473

Save

Cancel

Please input one blacklist number and click on “Save”. This number will add into black list. This is the first method to add a blacklist.

The second method is that dial feature codes from the phones. (You can refer to [Feature Codes](#))

Any extension user can dial *75 and follow the voice prompts to add the numbers to the CooCenter system blacklist.

To remove numbers from black list, you can dial *075.

Time Based Rules

Time Settings

Path: **Inbound Control->Time Based Rules**

Click on the “[Time Settings](#)” tab, you may create a new time rule or edit the example one, just specify the business hours during the weekdays.

Edit X

Rule Name: office time

Time Settings

Day	Start Time	End Time	Active Times
Sun:	00 : 00	00 : 00	
Mon:	00 : 00	00 : 00	09:00-12:00 14:00-18:00
Tue:	00 : 00	00 : 00	09:00-12:00 14:00-18:00
Wed:	00 : 00	00 : 00	09:00-12:00 14:00-18:00
Thu:	00 : 00	00 : 00	09:00-12:00 14:00-18:00
Fri:	00 : 00	00 : 00	09:00-12:00 14:00-18:00
Sat:	00 : 00	00 : 00	09:00-12:00

Save Cancel

After the business hours have been specified, you may also want to specify the holidays of the company, on which the company will be closed for holidays

Holiday Settings

Many businesses have fixed working hours where they know for example that they are only open Monday to Friday between 9am and 6pm and will be closed for business at all other times. Time conditions in CooCenter system allows you to control what happens to inbound calls both during and outside normal business hours.

Please click on the “[Holiday Settings](#)” tab, and click on the “[New Time Rule](#)” button to specify all the holidays on which the office will be closed.

You may add your holidays one by one by specifying the start date and time and the end date and time of the holidays.

Time Based Rules

Once the business hours and holidays all have been configured, you need to define the inbound rules according to the time conditions that you have configured. Please click on the “[Time Based Rules](#)” tab. And click on “[Edit](#)” button of the existing time rule.

In the “[Time Rule](#)” dropdown list select the time rule you have defined for business hours. And in the “[Destination](#)” section specify where to route the inbound calls during and out of the business hours you have defined.

If you also defined the holidays of the company, you may select the holiday set in the “[Holidays](#)” dropdown list and set a destination for the inbound calls on holidays.

Once done, you will need to direct all inbound calls to the time rule instead of any other destinations, please go to [Inbound Control->Inbound Routes](#) page, set the inbound call destination as “Goto Time Rule” and then select the exact time rule that you have defined, then all inbound calls will be routed according to the time conditions you have configured.

Advanced

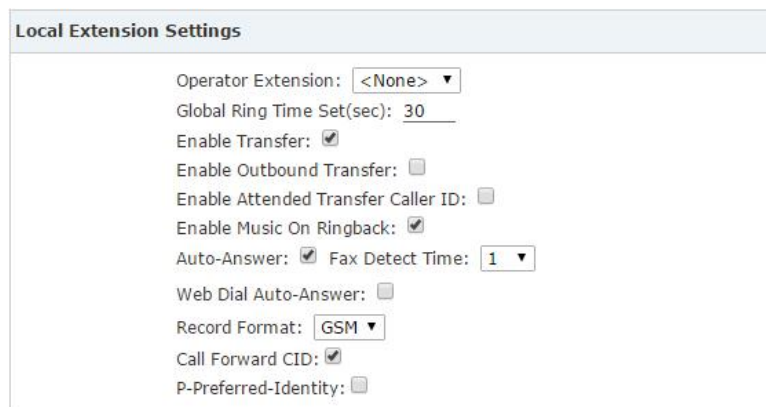
Options

General

Path: **Advanced->Options->General**

Here on this page you can configure some global options for all user extensions. In the “Local Extension Settings” section you can view the below options that can be configured.

Local Extension Settings



The screenshot shows the 'Local Extension Settings' configuration page. It contains the following settings:

- Operator Extension: <None> (dropdown menu)
- Global Ring Time Set(sec): 30 (text input)
- Enable Transfer: ☒
- Enable Outbound Transfer: ☐
- Enable Attended Transfer Caller ID: ☐
- Enable Music On Ringback: ☒
- Auto-Answer: ☒ Fax Detect Time: 1 (dropdown menu)
- Web Dial Auto-Answer: ☐
- Record Format: GSM (dropdown menu)
- Call Forward CID: ☒
- P-Preferred-Identity: ☐

- **Operator Extension:** Choose an extension to be operator extension. When an incoming call has been directed to voicemail, then by pressing ‘0’ the caller will be put through to the operator extension.
- **Global Ring Time Set(sec):** If not specifically configured, an incoming call will ring the extension for the time given here.
- **Enable Transfer:** If enabled, the extension users will be able to perform call transfers.
- **Enable Outbound Transfer:** If enabled, the outbound calls will be able to be transferred.
- **Enable Attended Transfer Caller ID:** Normally if you use feature code *2(This will be introduced in [Feature Codes](#)) to transfer a call to another extension, the extension user only sees your extension number as caller ID but not the actual caller ID, by enabling this option the real caller ID will be passed to the user extension.
- **Enable Music On Ringback:** If enabled, callers will hear music instead of ringback tone when calling other extensions.
- **Auto-Answer:** Auto-answer enables the CooCenter to automatically answer the

inbound calls from analog ports.

- **Fax Detect Time:** If auto-answer enabled, you are able to configure the fax auto detection time here.
- **Web Dial Auto-Answer:** Enable/disable auto answer of the extension numbers while dialing from Web GUI.
- **Record Format:** Choose GSM or WAV as the call recording format.
- **Call Forward CID:** Allow passing the real caller ID to the forwarded number.
- **P-Preferred-Identity:** The P-Preferred-Identity header is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication.

Default Settings for New User

Default Settings for New User			
SIP: <input checked="" type="checkbox"/>	IAX2: <input type="checkbox"/>	Web Manager: <input type="checkbox"/>	Call Waiting: <input checked="" type="checkbox"/>
Agent: <input type="checkbox"/>	Voicemail: <input checked="" type="checkbox"/>	Delete VMail: <input type="checkbox"/>	VM Password: <input type="text" value="1234"/>
NAT: <input type="checkbox"/>	Transport: <input type="text" value="UDP+TCP"/>	SRTP: <input type="checkbox"/>	
Audio Codecs			
<input checked="" type="checkbox"/> ulaw	<input checked="" type="checkbox"/> alaw	<input type="checkbox"/> G.722	<input checked="" type="checkbox"/> G.729
<input type="checkbox"/> G.726	<input type="checkbox"/> GSM	<input type="checkbox"/> Speex	<input type="checkbox"/> Opus

In this section, options are defined for the creation of new extensions. If you have one of the options enabled, then so will any newly created extensions.

Extension Preferences

Extension Preferences	
User Extensions <input type="text" value="401"/>	to <input type="text" value="499"/>
Conference Extensions <input type="text" value="900"/>	to <input type="text" value="909"/>
IVR Extensions <input type="text" value="610"/>	to <input type="text" value="629"/>
Queue Extensions <input type="text" value="630"/>	to <input type="text" value="639"/>
Ring Group Extensions <input type="text" value="640"/>	to <input type="text" value="659"/>
Paging Group Extensions <input type="text" value="660"/>	to <input type="text" value="679"/>
Web Extensions <input type="text" value="680"/>	to <input type="text" value="699"/>
<input type="button" value="Reset"/>	

The user extension number and system extension number ranges are defined here to avoid any conflicts within the CooCenter system. You can modify these number ranges according to your requirements.

Analog Settings

Path: **Advanced->Options->Analog Settings**

Global Analog Settings are used for configuring the CooCenter system to seamlessly work with the telephone lines from your telecommunications provider.

Caller ID Detect

Caller ID Detect	
Caller ID Detection:	<input checked="" type="checkbox"/>
Caller Name:	<input type="checkbox"/>
Caller ID Signaling:	Bell-US ▼
Caller ID Start:	Ring ▼
CID Buffer Length:	2500 ▼
Ring Debounce:	64 ▼
DTMF Hits Begin:	2 ▼
DTMF Misses End:	3 ▼
Detect Caller ID After:	1 ▼

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

- **Caller ID Detection:** Enable/Disable Caller ID Detection.
- **Caller Name:** In some countries/regions caller name can be passed through the PSTN lines, by enabling this option the caller name will be received by the CooCenter system along with the caller ID.
- **Caller ID Signaling:** The signaling type applied on the PSTN lines to pass caller ID.
 Bell-US—Also known as Bellcore FSK. 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:** Defines when the caller ID starts.
 Ring—Caller ID starts when a ring is 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 ID info.
- **Ring Debounce:** Sets the minimum time in milliseconds to debounce extraneous ring events.
- **DTMF Hits Begin:** Sampling matching value of DTMF caller ID digits, you can choose 1 to 5 digits been matched then to consider it as part of the Caller ID.
- **DTMF Miss End:** Sample matching value of DTMF caller ID digits, you can choose 1 to 5 digits been mismatched then to consider it's not part of the caller ID.
- **Detect Caller ID After:** Sets the CooCenter to detect Caller ID after how many rings been detected.

General

General

Opermode:

Tone Zone:

Ring Timeout(s):

Relax DTMF: ☐

Send Caller ID After:

Echo Cancel: ☒

Denoise: ☐

Echo Training: (yes/no/number)

- **Opermode:** Set the Opermode for FXO Ports.
- **ToneZone:** Select the tone zone of your country.
- **Ring Timeout(s):** FXO (FXS signaled) devices must have a timeout to determine if it should hang up before the line is answered. This value can be tweaked to shorten how long it takes before DAHDI considers a non-ringing line to have hung-up.
- **Relax DTMF:** Helps DTMF signal detection.
- **Send Caller ID After:** Certain countries (UK) have ring tones with different ring tones (ring-ring), which means the caller ID needs to be set later on, and not just after the first ring, as per the default (1).
- **Echo Cancel:** Enable/Disable software Echo Cancel algorithm.
- **Denoise:** The denoise parameter will help on noise reduction of the noisy analog lines, especially when gains have been increased on the lines.
- **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.

SIP Settings

Path: **Advanced->Options->SIP Settings**

Global SIP settings allow you to configure some general and advanced options for the IP-PBX system global SIP preferences. Navigate to web menu **Advanced->Options->SIP Settings**.

General

General	
<input type="checkbox"/> Enable	UDP Port: 5060
<input type="checkbox"/> Enable	TCP Port: 5060
<input type="checkbox"/> Enable	TLS Port: 5061
	Start RTP Port: 10001
	End RTP Port: 10500
	DTMF Mode: Auto
	Allow Guest: <input type="checkbox"/>
	Max Registration/Subscription Time(sec): 3600
	Min Registration/Subscription Time(sec): 60
	Default Incoming/Outgoing Registration Time(sec): 60

- **UDP Port:** SIP over UDP service port. By default ZYCOOCooCenter system uses UDP as SIP transmission protocol. Port number can be changed here if required.
- **TCP Port:** By ticking the “Enable” checkbox you can enable global SIP TCP support. To register a SIP extension over TCP protocol, you’ll have to select TCP transport on the extension configure page, please refer to [Extension](#).
- **TLS Port:** By ticking the “Enable” checkbox you can enable global SIP TLS support. To register a SIP extension over TLS protocol, you’ll have to select TLS transport on the extension configuration page, please refer to [Extension](#).
- **Start RTP Port/End RTP Port:** The UDP ports used by CooCenter system to carry RTP voice stream. Do not change the port numbers or you may encounter audio issue with phone calls.
- **DTMF Mode:** The DTMF mode specifies how touch tones will be transmitted to the other side of the call. Possible values for this field are rfc2833, inband, info, and auto.
- **Allow Guest:** This setting determines if anonymous callers are permitted to place calls to the CooCenter system. For security precautions please do not enable this option.
- **Max Registration/Subscription Time(sec):** Maximum allowed time of incoming registrations and subscriptions (seconds).
- **Min Registration/Subscription Time(sec):** Minimum length of registrations/subscriptions.
- **Default Incoming/Outgoing Registration Time(sec):** Default length of incoming/outgoing registration.

NAT Support

When the CooCenter system is behind a NAT device and needs to communicate to the outside. It needs to know whether it is talking to someone "inside" or "outside" of the NATted network. For example, if you are going to deploy remote extensions you have to tell the CooCenter system which network address/addresses are from inside and which are from outside. Below is an example configuration.

NAT Support	
External IP:	117.176.159.157
External Host:	117.176.159.157
External TCP Port:	
External TLS Port:	
External Refresh(sec):	10
Local Network Address:	192.168.1.0/24
Local Network Address:	
Local Network Address:	

- **External IP:** Your static public IP address or domain name.
- **External Host:** This is similar to “External IP” except that the hostname is looked up every "External Refresh" seconds(default 10's).
- **External TCP Port:**Port number of SIP signaling with TCP transport protocol on the public network.
- **External TLS Port:** Port number of SIP signaling with TLS transport protocol on the public network.
- **External Refresh(sec):** The refresh interval of the “External Host”.
- **Local Network Address:** Your local network address/addresses.

Notice:

If you have one-way audio or no audio issue on the remote extensions then this most probably means that NAT support is not properly configured. Please check your configurations here.

T.38 Fax Pass Through Support

T.38 Fax Pass Through Support
T.38 Fax (UDPTL) Pass Through: <input checked="" type="checkbox"/>

Enable T.38 fax (UDPTL) passthrough on SIP to SIP calls.

Notice:

This is suitfor professional operation.If you have some questions, please connect with our technician.

Type of Service

Asterisk supports different QoS settings at the application level for various protocols on both signaling and media. The Type of Service (TOS) byte can be set on outgoing IP packets for various protocols. The TOS byte is used by the network to provide some level of Quality of Service (QoS) even if the network is congested with other traffic.

Type of Service	
TOS for Signaling packets:	CS3 ▼
TOS for RTP audio packets:	ef ▼
TOS for RTP video packets:	AF41 ▼
COS Priority for Signaling packets:	3 ▼
COS Priority for RTP audio packets:	5 ▼
COS Priority for RTP video packets:	4 ▼
DNS SRV Look Up:	<input type="checkbox"/>
Relax DTMF:	<input checked="" type="checkbox"/>
RTP TimeOut(sec):	
RTP Hold TimeOut(sec):	
Add 'user=phone' to URI:	<input type="checkbox"/>
UserAgent:	VOIP

- **TOS for Signaling Packets:** Sets TOS for SIP packets.
- **TOS for RTP audio packets:** Sets TOS for RTP audio packets.
- **TOS for RTP video packets:** Sets TOS for RTP video packets.
- **COS Priority for Signaling packets:** Sets 802.1p priority for SIP packets.
- **COS Priority for RTP audio packets:** Sets 802.1p priority for RTP audio packets.
- **COS Priority for RTP video packets:** Sets 802.1p priority for RTP video packets.
- **DNS SRV Look Up:** Enable DNS SRV lookups on outbound calls.
- **Relax DTMF:** Relax DTMF handling.
- **RTP TimeOut(sec):** Terminate call if there is 60 seconds of no RTP or RTCP activity on the audio channel when we're not on hold. This feature enables the ability to hangup a call in the case of a phone disappearing from the network, for instance if the phone loses power.
- **RTP Hold TimeOut(sec):** Terminate call if 300 seconds of no RTP or RTCP activity on the audio channel when on hold.
- **Add 'user=phone' to URI:** Enable this option if the SIP provider requires ";user=phone" on URI.
- **UserAgent:** Allows you to change the user agent string. The default user agent string also contains the Asterisk version. If you don't want to expose this, change the user agent string here.

Outbound SIP Registrations

The “Outbound SIP Registrations” configures the register behaviors of CooCenter system when registering as a client to the other SIP servers.

Outbound SIP Registrations
Register TimeOut(sec): <input type="text" value="30"/> Register Attempts: <input type="text" value="10"/>

- **Register TimeOut(sec):** Retry registration every 30 seconds (default).
- **Register Attempts:** Number of registration attempts before the CooCenter system give up. Default is 10 and 0 means continue forever.

IAX2 Settings

Path: **Advanced->Options->IAX2 Settings**

General
UDP Port: <input type="text" value="4569"/> Bandwidth: <input type="text" value="low"/> ▼ Max Registration/Subscription Time(sec): <input type="text" value="1200"/> Min Registration/Subscription Time(sec): <input type="text" value="60"/>

- **UDP Port:** IAX2 signaling and media port, the default is 4569.

- **Bandwidth:** Specify bandwidth of low, medium, or high to control which codecs to be used.
- **Max Registration/Subscription Time(sec):** Maximum amount of time that IAX peers can request as a registration expiration interval (in seconds).
- **Min Registration/Subscription Time(sec):** Minimum amount of time that IAX peers can request as a registration expiration interval (in seconds).

Notice:

This is suit for professional operation. If you have some questions, please connect with our technician.

Module Settings

CooCenter-S30 system needs proper module settings to load correct drivers and configure files to drive the E1 and BRI telephony modules.

Default module settings are with module types FXS/FXO/GSM/WCDMA on both telephony module slots. So if you don't have E1 and BRI modules installed then you don't have to configure module settings.

E1 PRI Settings

To configure module settings please navigate to **System->Module Settings** page.

SLOT 1	
Module Type:	E1/T1 ▼
E1/T1 Settings:	
Mode:	E1 ▼
Signaling:	CPE ▼
Framing:	CCS ▼
Coding:	HDB3 ▼
CRC4:	<input checked="" type="checkbox"/>

E1 module can be installed on both Slot1 and Slot2. To ensure CooCenter system can detect and drive E1 module in the Module Type field you should choose "E1/T1".

E1/T1 Setting parameters description:

- **Mode:** Sets the module to work as E1 or T1 mode.
- **Signaling:** Sets the module to work with PRI CPE or NET, R2 and SS7 signaling.
- **Framing:** CPE, NET and SS7 use CSS (Common Channel Signaling). R2 signaling uses CAS.
- **Coding:** PRI CPE, PRI NET, R2 and SS7 all use HDB3.
- **CRC4:** A method of checking for errors in transmitted data on E-1 trunk lines. Enable it only if the telephony provider requires CRC4.

These configuration parameters should be given by the telephony provider, please

configure these parameters correctly according to what they give to match the switching equipment being used by the telephony provider.

Once the configurations had been done save and reboot the CooCenter system. In the meantime you attach the E1 line to the E1 interface. After rebooting you should get LED indications with L1 red, L2 red, L3 off and L4 green of a successful PRI CPE connection. For PRI NET, R2 and SS7 connection LED indications please check chapter [1.5.2 LED Indication](#). Now you open web GUI and navigate to **Operator** page you'll see E1/T1 module connection status as connected and UP.

E1/T1 module			
Port	Type	Status	Alarm
1	E1	Connected	UP
2	E1	Connected	UP

The above example has 2 E1 lines connected and ready for phone calls. If in your deployment you got some else connection status you should check with the telephony provider to confirm the configuration parameters. Or check with them if the line had been activated by them and ready for phone calls. If you need any help from ZYCOO, please contact ZYCOO [Support](#) for help.

T1 PRI Settings

To configure ZYCOO E1 telephony module to work in T1 mode, please choose “T1” in the “Mode” dropdown list. And then configure T1 related parameters given by the telephony provider.

SLOT 1

Module Type: E1/T1

E1/T1 Settings:

Mode: T1

Signaling: CPE

Framing: ESF

Coding: B8ZS

CRC4: ☐

T1 runs on same signaling types as E1 mode except R2. And T1 uses different Framing and Coding methods, configure these parameters according to the details provided by the telephony provider.

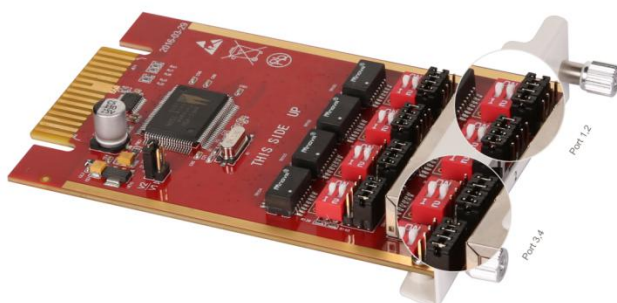
In most cases CRC4 is not needed for T1 circuit. Enable it only when the provider requires it. After configurations been done save and reboot the CooCenter system. In the meantime you attach the T1 line to the T1 interface. After rebooting you should get LED indication with L1 red, L2 red, L3 off, L4 green to indication PRI CPE signaling. For PRI NET and SS7 signaling LED indications please check chapter [1.5.2 LED Indication](#). Now you open web GUI and navigate to **Operator** page you'll E1/T1 module connection status connected and UP.

E1/T1 module			
Port	Type	Status	Alarm
1	T1	Connected	UP
2	T1	Connected	UP

BRI Settings

BRI module can only be installed on Slot2 of the CooCenter-S30 system.

The jumpers shown in the picture below are for crossover cables and straight cables to connect a BRI connection.



The jumpers for Port 1, 2 and Port 3, 4 are on different position. Attach the BRI lines to these ports and then configure BRI parameters on [System->Module Settings](#) page.

SLOT 2

Module Type: ISDN BRI ▼

BRI Settings:

Type of Port 1: NT_PTP ▼

Type of Port 2: NT_PTP ▼

Type of Port 3: TE_PTP ▼

Type of Port 4: TE_PTP ▼

In the Module Type field you should select ISDN BRI.

Below are the BRI protocols supported by CooCenter-S30:

- **NT_PTP**: BRI PTP Point to Point signaling (Network side)
- **NT_PTMP**:BRI PTMP Point to Multi-Point signaling (Network side)
- **TE_PTP**:BRI PTP Point to Point signaling (CPE side)
- **TE_PTMP**:BRI PTMP Point to Multi-Point signaling (CPE side)

Configure the protocols according to the telephony provider gave. Save and reboot the CooCenter system, after rebooting you get red LED to indicate a successful BRI CPE connection, and green LED to indicate a successful BRI NET connection.

On the web GUI [Operator](#)page you will see BRI connection status like below, by now all connected.

BRI module			
Port	Type	Status	Alarm
1	NT	Connected	UP
2	NT	Connected	UP
3	TE	Connected	UP
4	TE	Connected	UP

Please note which ports are not connected and then power off the CooCenter system and unplug the module to adjust the jumpers for the BRI ports according to the well-working ones.

MFC/R2 Settings

In the E1 settings section and Signaling field by selecting R2 you are able to configure E1 R2 signaling.

SLOT 1

Module Type: E1/T1 ▼
E1/T1 Settings:
Mode: E1 ▼
Signaling: R2 ▼
Framing: CAS ▼
Coding: HDB3 ▼
CRC4: ☒
R2 Settings:
Variant: Argentina ▼
Max ANI: 20
Max DNIS: 4
Get ANI First: ☐
Advanced Protocol File: ☐
Category: National Subscriber ▼

R2 parameter descriptions:

- **Variant:** Protocol variant setting depends on country and carries.
- **Max ANI:** The maximum expected number of ANI digits.
- **Max DNIS:** The expected number of dialed digits.
- **Get ANI First:** The usual behavior for incoming calls is to get the calling party category and the ANI as soon as possible, and to get the DNIS afterwards. This doesn't work on all systems, so the option to reverse this behavior is provided.
- **Advanced Protocol File:** Additional configurations for R2 signaling.
- **Category:** Send calling party's category. Usually National Subscriber works just fine, you can set other options if needed in real application.

SS7 Settings

Signaling System No. 7 (SS7) is a set of telephony protocols can be delivered via E1 and T1. In the E1 settings section and Signaling field by selecting R2 you are able to configure E1 SS7 signaling.

SLOT 1

Module Type:

E1/T1 ▼

E1/T1 Settings:

Mode:

E1 ▼

Signaling:

SS7 ▼

Framing:

CCS ▼

Coding:

HDB3 ▼

CRC4:

☒

SS7 Settings:

Variant:

ITU ▼

Point Code:

20

Point Code of Node Adjacent:

4

Network Indicator:

national ▼

Please configure these parameters according to the instructions of the service provider or ask for advice from our support team. Otherwise please do not change these settings without professional guidance.

Voicemail

Voice mail allows callers to leave messages for subscribers (user extensions) of the CooCenter system when they are unable to answer the incoming calls.

General

Path: **Advanced->Voicemail->General**

VoiceMail Reference

VoiceMail Reference	
Max Greeting Time(sec):	<input type="text" value="30"/>
Dial "0" for Operator:	<input checked="" type="checkbox"/>

- **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

Voice Message Options	
Message Format:	<input type="text" value="WAV (16-bit)"/>
Maximum Messages:	<input type="text" value="100"/>
Max Message Time(min):	<input type="text" value="2"/>
Min Message Time(sec):	<input type="text" value="2"/>

- **Message Format:** The audio file format to be used for the recording.
- **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 2 seconds, which means voice messages which are less than 2seconds will be ignored by the CooCenter system.

Playback Options

Playback Options	
<input checked="" type="checkbox"/>	Say Message CallerID
<input checked="" type="checkbox"/>	Say Message Duration
<input type="checkbox"/>	Play Envelope
<input type="checkbox"/>	Allow Users to Review

These 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 enabled, this option will allow users to review the voice

message.

Email Settings

Path: **Advanced->Voicemail->Email Settings**

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

Email Settings

General **Email Settings**

Template for Voicemail Emails

☒ Attach voicemail to email

Sender Name

From

Subject

Message

Template Variables:
\${VM_NAME} : Recipient's first name and last name
\${VM_DUR} : The duration of the voicemail message
\${VM_MAILBOX} : The recipient's extension
\${VM_CALLERID} : The Caller ID of the person who left the message
\${VM_MSGNUM} : The message number in your mailbox
\${VM_DATE} : The date and time the message was left

- **Attach voicemail to email:** If enabled, the system will send any voice message files received to the extension users' email box.
- **Sender Name:** Alias for the SMTP email account.
- **From:** The email account from SMTP settings.
- **Subject:** The subject of the email sent by CooCenter system.
- **Message:** The content 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 then be used in the message field to compose the email content.

SMTP Settings

Path: **Advanced->SMTP Settings**

Define an email account to be used by the system which will send emails with voicemail messages attached to the extension users' email

SMTP Settings

SMTP Settings:

SMTP Server:

Port:

SSL/TLS: ☒

☒ Enable SMTP Authentication

Username:

Password:

boxes.

- **SMTP Server:** SMTP server domain, for example: smtp.gmail.com, smtp.tom.com.
- **Port:** Default SMTP service port is 25, but if you are using SSL/TLS then please use port 465.
- **SSL/TLS:** Encrypts a communication channel between the CooCenter system and the SMTP server.
- **Enable SMTP Authentication:** If your SMTP server requires authentication then 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. If it is working then you’ll receive an email sent by the CooCenter system.

Conferences

Path: **Advanced->Conference**

Conferences allow two or more callers to be joined together so that all parties on the call can hear one another. Conferences are also referred as Conference Bridges or Conference Rooms.

On CooCenter system, you can create up to 20 conference rooms. There are 3 default conference rooms preconfigured for you.

You can click “New Conference” button to add a new conference room or click “Edit” button on the existing conference room to change the properties.

Edit		X
Conference Number		
Room Extension:	900	
Conference Password		
Guest Password:	1234	
Administrator Password:	2345	
Conference Options		
Conference DialPlan	Internal ▼	
<input type="checkbox"/>	Play hold music for first caller	
<input type="checkbox"/>	Enable caller menu	
<input type="checkbox"/>	Announce callers	
<input type="checkbox"/>	Record conference	
<input type="checkbox"/>	Quiet Mode	
<input type="checkbox"/>	Close the conference when last administrator exits	
<input type="checkbox"/>	Leader Wait	
Save		Cancel

Conference number

- **Room Extension:** Call this extension number to enter the conference room.

Conference Password

- **Guest Password:** If callers use this password to enter the conference then they are ordinary participants.
- **Administrator Password:** If callers use this password to enter the conference then they are administrators and have advanced conference menu features such as inviting people to participate in the conference.

Conference Options

- **Conference DialPlan:** Conference admin can use this dialplan to invite other participants.
- **Play hold music for first caller:** Plays the hold music for the first participant in the conference until another participant enters the conference.
- **Enable caller menu:** Check this option to allow the conference admin to access the conference menu by pressing “*” on the phone.
- **Announce Callers:** Announce all the participants in the room when a new participant enters the conference room.
- **Record Conference:** Record this conference(Recording format is wav). The recorded conference can be searched within Report->Record List->Conference page.
- **Quiet Mode:** If this option is checked then the system will not give any announcement when participants enter or leave the conference.
- **Close the conference when last administrator exits:** If this option is checked then the conference will be terminated when the last administrator exits.
- **Leader Wait:** Wait until the conference leader(administrator) enters the conference

before starting the conference.

Music Settings

Path: **Advanced-> Music Settings**

Music Settings, or Music On Hold(MOH) as it is more commonly known on an CooCenter system allows audio files (such as WAV or MP3 files) to be uploaded to the CooCenter system and played back when a caller is placed on hold or is waiting in a queue.

Enter in the music settings page according to the path we give.

Music Settings

Music Settings

Music Management

Music On Hold Reference

Music: Music 1 ▼

Music On Ringback Reference

Music: Music 2 ▼

Music On Queue Reference

Music: Music 3 ▼

Save Cancel

- **Music On Hold Reference:** Audio files in this selected folder will play to the party which is on hold.
- **Music OnRingback Reference:** Audio files in this folder will be played instead of playing ringback tone to the caller.
- **Music On Queue Reference:** Audio files in this folder will be played when the caller is waiting in a call queue.

There are 10 folders for music files, by default the first 3 folders are preloaded with music files which you may wish to choose. However, if you want to upload your own audio files please click “**Music Management**” tab.

Music Management

Music Settings

Music Management

Music Management

Select Music Directory: Music 1 ▼ Load

Files: ▼ Delete

Upload Music File

Select Music Directory: Music 1 ▼

Note: The sound file must be mp3, wav(16bit/8000Hz/Mono), gsm, ulaw or alaw!
The size is limited in 15MB!

Please choose file to upload: Choose File No file chosen

Upload

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 your preferred audio file and click “Upload” button to upload the audio file. If there are more than one audio file in the same music folder, they will be played at random.

Notice:

CooCenter system can adopt MP3, wav(16bit, 8000Hz, mono), gsm, ulaw and alaw audio file format.

Call Forward

Path: **Advanced-> Call Forward**

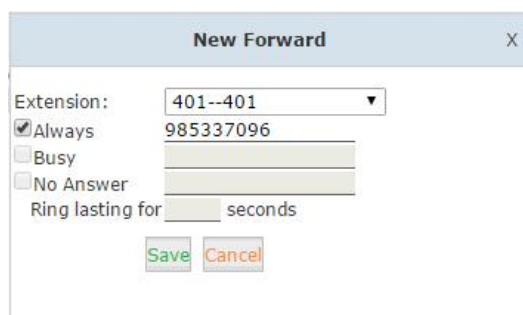
This feature allows calls to an extension to be automatically forwarded to a specific internal extension or external phone number.

Before configuring call forward you can enable the CooCenter system to play a voice prompt before the call is forwarded. This voice prompts can be recorded or uploaded from the Inbound Control->IVR Prompts page.

Once the voice prompt file is ready you can navigate to web menu **Advanced->Call Forward** and enable the system to play back the voice prompt before the incoming call is forwarded.



After the voice prompt is set, 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.
- **Ring lasting for ____ seconds:** Only configurable for “No Answer” option. It defines how long to ring the extension before forwarding if the extension didn't answer.

This feature also can be set on the phone with feature codes. Please refer to [Feature Codes](#).

Notice:

1. If you are forwarding a call to an external phone number then please ensure that you add a prefix in front of the number if your system requires a prefix to dial out.
2. The forward condition “[Always](#)” is mutually exclusive to “[Busy](#)” and “[No Answer](#)”.

Paging and Intercom

Path: **Advanced->Paging and Intercom**

The Paging and Intercom feature allows you to use your phone system as an intercom system, provided that your endpoints (phone devices) support this functionality. The Paging and Intercom feature allows you to define a number (just like an extension or Ring Group number) that will simultaneously page a group of devices. For example, in a small office, you might define a paging group that allows any user to dial 699, allowing them to page the entire office. You can also use the feature code *50/*51 to page/intercom a single extension, by dialing *50/*51 followed by the extension number.

Click “[New Paging Group](#)” button to add a new paging group.

' checkbox. At the bottom right are 'Save' and 'Cancel' buttons."/>

New [X]

Paging Extension: 660
Description: managers

Paging Group Members	Device List
401(SIP) 401	406(SIP) 406
402(SIP) 402	407(SIP) 407
403(SIP) 402	408(SIP) 408
404(SIP) 404	409(SIP) 409
405(SIP) 405	410(SIP) 410
	411(SIP) 411
	412(SIP) 412
	412(IAX2) 412

Duplex: ☒

Save Cancel

- **Paging Extension:** The extension number for this paging group, by calling this extension number you can reach the group members.
- **Description:** Description of this paging group.
- **Duplex:** If enabled, the group members can talk back to the caller.

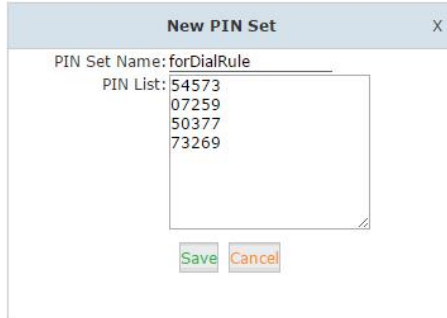
By calling the paging extension number, all group member phones will auto answer in speaker mode (requires that the IP phones support auto answer feature), the caller can now make a brief announcement to the group members.

PIN Sets

Path: **Advanced->PIN Sets**

Pin sets can be used to secure your CooCenter system phone services and in particular for outbound dial rules and DISA.

Click on “[New PIN Set](#)” button to create a collection of PIN codes.



The screenshot shows a 'New PIN Set' dialog box. It has a title bar with the text 'New PIN Set' and a close button 'X'. The main area contains a text field labeled 'PIN Set Name:' with the value 'forDialRule'. Below this is a text area labeled 'PIN List:' containing the following PIN codes: 54573, 07259, 50377, and 73269. At the bottom of the dialog are two buttons: 'Save' and 'Cancel'.

Each line is a PIN code, press Enter to add the next PIN code without any symbols.

Call Recording

Path: **Advanced->Call Recording**

Navigate to web menu Advanced->Call Recording. Click “[New Call Recording](#)” to activate call recording for the extensions you want calls to be recorded.

New Call Recording X

Extension:

☒ 401 (401) ☒ 402 (402) ☒ 403 (403) ☐ 404 (404) ☐ 405 (405) ☐ 406 (406) ☐ 407 (407) ☐ 408 (408) ☐ 409 (409) ☐ 410 (410) ☐ 411 (411)

Call Recording Time

Always Recording: ☒

Start Time: : End Time: :

Start Day: End Day:

Call Recording Settings

Inbound Record: ☒ Outbound Record: ☒

- **Extension:** Select the extensions which you want their calls to be recorded.
- **Always Recording:** If enabled, all calls from the above selected extensions will be recorded regardless when the calls were made and received.
- **Start Time, End Time, Start Day, End Day:** If Always Recording is unnecessary then you can specify which time durations in a week to record all calls from the above selected extensions.
- **Inbound Record:** Enable to record all inbound calls.
- **Outbound Record:** Enable to record all outbound calls.

The recordings can be searched on Report->Record List->Call Recording page. Please see [Call Recording](#).

Another recording method is “One Touch Recording” which is also known as Record on Demand. It allows users to record phone calls selectively. Please see [One Touch Recording](#). The one touch recordings can be searched from Report->Record List->One Touch Recording page.

Feature Codes

Path: **Advanced->Feature Codes**

Feature codes allow you to set the special codes that users can dial to access various features.

Call Parking

Call Parking

Extension to Dial for Parking Calls: 700
Extension Range to Park Calls: 701-720
Call Parking Time(sec): 45
Enable Call Park BLF notification: ☒

A Parking Lot 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). Anyone else on your CooCenter system can now dial 701 to pick-up the parked call.

A call can be parked for a maximum of 45 seconds as per the definition of “[Call Parking Time](#)”, if nobody picks this call up then it will go back to the extension which parked it. The “[Enable Call Park BLF Notification](#)” enables the parked extensions 701-720 to be monitored by BLF keys, so if there’s a call that is parked, the extension user will be able to see it from the BLF panel.

Pickup Call

Pickup Call

Pickup Extension: *8
Pickup Specified Extension: **

Pickup call option allows users to pick up calls that are not directed to them by dialing a feature code *8 or **.

“[Pickup Extension: *8](#)” has already been introduced in the [Extension](#) page, as it’s related to the pickup group option of the extension settings. Set Pickup Extension.Dial the feature code will pickup the same pickup group ringing extension.

While “[Pickup Specified Extension: **](#)” can help pickup a call on any ringing extension. Dial ** followed by the extension number and you can pickup a call on a ringing extension if it is in the same pickup group as your extension or not.

Transfer

Call Transfer is used to transfer a call in progress to some other destination. There are two types of call transfer.

Transfer

Blind Transfer: #
Blind Transfer Callback: ☐
Attended Transfer: *2
Disconnect Call: *
Timeout for answer on attended transfer(sec): 15

- **Blind Transfer:** In a live call, an extension user can press # key and the CooCenter system prompts “Transfer”, you then enter the number to transfer to, this call will be transferred instantly and the user can hangup. If the transferred number doesn’t answer this call then it will ring back to the extension user.
- **Blind Transfer Callback:** Determines whether the transferred call should call back to the user who transferred it or not. If enabled and the transferred call was unanswered it will call back to the user who transferred it, if disabled and the transferred call was unanswered it will go to voicemail box of the transferred extension.
- **Attended Transfer:** In a live call, extension user can press *2 and the CooCenter system prompts “Transfer”, you then enter the number to transfer to, after someone answers your call, you can introduce this call and hangup at which point the call is transferred.
- **Disconnect Call:** In an attended transfer if the other side doesn’t want to take the call to be transferred, you can press * to disconnect with them and get back to the caller.
- **Timeout for answer on attended transfer(sec):** In an attended transfer, if the third party rang for 15 seconds without answering, the extension user will go back to the caller and the transfer is terminated.

One Touch Recording

One Touch Recording is also known as Record on Demand. It allows users to record phone calls selectively. In a live call conversation, an extension user can use feature code *1 to record this call. With this feature, you don’t have to configure recording all calls for the extensions which may cause heavy system resource use if some call recordings are not required.



The One Touch Recording Logs can be found on Report-> Record List->One Touch Recording page.

Call Forward

You’ll see feature codes for call forward as follows:



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

For example, a CooCenter 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.

Do Not Disturb

Do Not Disturb

Enable Do Not Disturb: *74
Disable Do Not Disturb: *074

With the Do Not Disturb(DND) feature enabled, an extension can make outbound phone calls but inbound calls to the extension cannot be made.

If an extension user of the CooCenter system dials *74 from their phone, the system will play a beep sound to indicate DND has been activated.

To disable DND, simply dial *074, another beep sound will play and DND has been deactivated.

Spy

Spy

Normal Spy: *90
Whisper Spy: *91
Barge Spy: *92

Call Spy allows users to dial the spy feature codes followed by an extension number to listen to the call conversation in real-time.

- **Normal Spy:** For example, extension 410 is talking to someone on the phone, you can dial *90410 to listen to their conversation, however, neither speaker will be able to hear you.
- **Whisper Spy:** Whisper spy is also known as coaching. For example, a new employee is talking to the customer on the phone, their supervisor can dial *91 followed by the employee's extension number to listen to their conversation. The supervisor can talk to the new employee only without the customer hearing the conversation.
- **Barge Spy:** Barge spy is similar to an instant 3-way conference call. While an extension user is talking to someone else on the phone, you can dial *92 followed by their extension number to talk to both of the speakers.

Notice:

Before call spy can be used, you have to make sure the extensions to be spied, have the "Allow Being Spied" option enabled on extension settings page.

Black List

Black List

Blacklist a number: *75

Remove a number from the blacklist: *075

Black list feature allows you to create a list of numbers that are not allowed to call in to the CooCenter system.

Any extension user can dial *75 and follow the voice prompts to add the numbers to the CooCenter system black list.

To remove numbers from black list, you can dial *075.

Voicemail

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

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 the required extension then you can check its voicemail and you can do this for any extension by following the system voice guidance.

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

Conference

CooCenter system allows you to press a key sequence (feature code) to create a conference during a live call.

Conferences

Invite Participant:	0
Create Conference:	*0
Return to conference with participant:	**
Return to conference without participant:	*#

- **Invite Participant:** When in a static conference room or a dynamic conference room, if the conference administrator presses 0 they will get a dial tone to invite others to participate in this conference.
- **Create Conference:** During a live call the extension user can press *0 to create a dynamic conference room. The other side will automatically enter the conference as an ordinary participant while the extension user who created this conference will be requested to enter the conference password to enter.
- **Return to conference with participant:** While using the conference menu to invite other people, you can dial ** to return to the conference with invited party.
- **Return to conference without participant:** If the invited party doesn't want to participate in the conference you can press *# to return to the conference without the invited party.

Notice:

After a dynamic conference is created, in reality you have entered a static conference room (by default 900 is the first available conference room). You are able to use conference admin menu to invite others to the conference also others can dial 900 to enter this conference.

Call Queues

Call Queues

Pause Queue Member Extension:	*95
Unpause Queue Member Extension:	*095

Call queue agents can dial *95 to suspend their extension temporarily, new calls will not

be distributed to their extensions, until they dial *095 to resume.

Wakeup

Wakeup

Wakeup Advance: *55
Wakeup Add: *55*
Wakeup Delete: *055

- **Wakeup Advanced:**Advanced wakeup call menu for adding, viewing andcanceling wakeup calls.
- **Wakeup Add:**Add a wakeup call directly by dialing this feature code followed by a specific date and time in 8-digit numberformat, for example, feature code is *55*, you can dial *55*08010730 to add a wakeup call of 7:30am on August 1st.
- **Wakeup Delete:**By dialing this code to cancel all requested wakeup calls.

Others

Others

Intercom: *50
Paging: *51
Directory: *3
Check WAN Port IP: **11
Check LAN Port IP: **12
Listen to Account Number: **13

- **Intercom:** The intercom feature code allows you to intercom one extension only. You don't have to create a "Paging and Intercom" group for only one extension if you intend to intercom with only that extension.
- **Paging:** The paging feature code allows you to page one extension only. It's the same as the intercom feature code, the only difference between paging feature code and intercom feature code is by using intercom feature code both sides can talk to each other but using paging feature code, only the caller can talk to the called party.
- **Directory:** Directory is also known as dial by name. Extension users can dial *3 and follow the voice prompts to enter the first 3 letters of another extension user's first or last name and then make a call to an extension number without knowing its extension number.
- **Check WAN Port IP:**By dialing this code you'll hear the system announce the IP address of the CooCenter WAN interface. It can be dialed on a registered IP phone or an analog phone connected to the FXS port, whether the analog phone has been assigned with extension number or not.
- **Check LAN Port IP:**By dialing this code you'll hear the system announce the IP address of the CooCenterLAN interface. It can be dialed on a registered IP phone or an analog phone connected to the FXS port, whether the analog phone has been assigned with extension number or not.
- **Listen to Account Number:**By dialing this code you can check the extension number

of your phone, either it's an IP phone or analog phone.

Phone Provisioning

PnP Settings

Path: **Advanced->Phone Provisioning->PnP Settings**

Here on this page you can see the term “PnP”, which refers to Plug and Play. By using this technique you don’t have to undertake any configurations directly on the IP phones, but instead only some minimized configurations on the CooCenter system. After this configuration is complete you can plug the phones to your LAN and once they start up, they are ready for phone calls through the CooCenter system.

Click on “[PnP Settings](#)” tab.

Plug and Play(PnP) Settings

Phones Settings

PnP Settings

Plug and Play(PnP) Settings

Enable:

☒

Interface:

WAN ▾

☐ Custom URL:

Multicasting Address:

224.0.1.75

Port:

5060

Save

Cancel

On this page, tick “[Enable](#)” to enable PnP feature.

- **Interface:** Select WAN or LAN depending on which interface you have connected the CooCenter to your local LAN.
- **Custom URL:** Custom URL tells the IP phones where to obtain the configuration files for auto provisioning. You should read your IP phone user manual to determine which kind of files it requires for auto provisioning. Then you create/upload these files to a FTP/TFTP/HTTP server for the phones to download. The URL can be IP address or domain name with subdirectory.

For example: [http://192.168.1.2/phones/\\${MAC}.conf](http://192.168.1.2/phones/${MAC}.conf). With “[Custom URL](#)” configured, you don’t have to add phones from the “[Phone Settings](#)” tab.

- **Multicasting Address:** IP phones which support PnP can use multicast discovery of SIP Registrar. Multicast registrations are addressed to the well-known “all SIP servers” multicast address “sip.mcast.net” (224.0.1.75 for IPv4).
- **Port:** SIP signaling port, default is 5060.

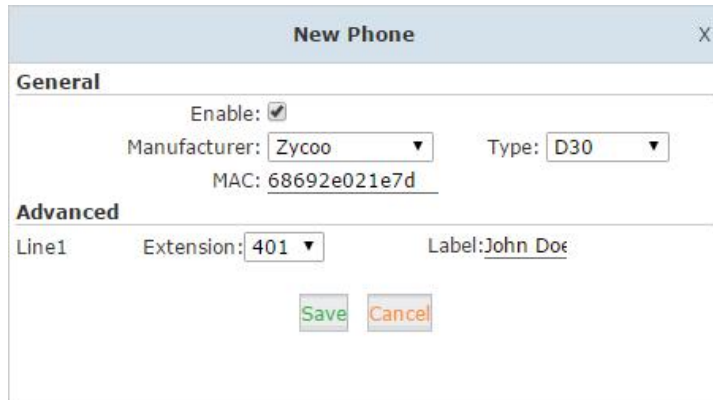
Notice:

Phone provisioning only works for IP phones that are in the same LAN where the CooCenter is deployed.

Phone Settings

Path: **Advanced->Phone Provisioning->Phone Settings**

After enabling PnP feature, click on “[Phone Settings](#)” tab and click “[New Phones](#)” to generate the configuration files for the phones to be added to the CooCenter system.



- **Manufacturer:** Manufacturer of the IP phone, currently, CooCenter supports phone provisioning phones from the following manufacturers: Zycoo, Grandstream, Yealink, Escene, AkuVox, Htek, Cisco, MOCET and Fanvil.
- **Model:** You must specify the exact model number of the phone, even if the phone is from the same manufacturer. This is because different models require different configuration files.
- **MAC:** CooCenter uses the MAC address of the phone to identify it on the local LAN as part of the provisioning process and it essential that you enter the correct MAC address for your IP Phone
- **Extension:** The extension number selected here will be auto configured to the phone with the MAC address given above.
- **Label:** Specify the user name of the phone.

Once you have added your new IP Phone(s) as described above, configuration files will be generated in the background of the CooCenter system. You can now connect the phone(s) to your LAN and once the phone(s) have booted up they will download configuration files from the CooCenter system and complete auto configuration with the extension numbers you provided.

Network Settings

Network

IPv4 Settings

Path: **Network Settings->Network->IPv4 Settings**

CooCenter system supports static IP, DHCP and PPPoE for WAN connection, while on LAN port only static IP is supported. If you are configuring your WAN connection as static IP or DHCP, ensure WAN and LAN IP addresses are not in the same network.

Static

Navigate to web menu Network Settings->Network->IPv4 Setting.

Network

IPv4 Settings	IPv6 Settings	VLAN Settings
WAN Port Setup		
IP Assign: Static ▼		
IP Address: <input type="text" value="192.168.1.254"/>		
Subnet Mask: <input type="text" value="255.255.255.0"/>		
Gateway: <input type="text" value="192.168.1.1"/>		
Primary DNS: <input type="text" value="8.8.8.8"/>		
Alternative DNS: <input type="text" value="4.4.4.4"/>		
LAN Port Setup		
IP Address: <input type="text" value="192.168.10.254"/>		
Subnet Mask: <input type="text" value="255.255.255.0"/>		
<input checked="" type="checkbox"/> IP AddressV1: <input type="text" value="192.168.5.254"/>		
Subnet MaskV1: <input type="text" value="255.255.255.0"/>		
<input type="checkbox"/> IP AddressV2: <input type="text"/>		
Subnet MaskV2: <input type="text"/>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

By default, CooCenter has been preconfigured with a static IP address of 192.168.1.100 and 192.168.10.100 on WAN and LAN interfaces respectively. If you want to use a static IP then configure required address here and include the address, netmask, gateway and DNS given by your ISP or network administrator.

For the LAN interface, you can specify 2 additional virtual IP addresses. These can be used to access other networks from the LAN port.

DHCP

If your Internet connection automatically provides you with a usable IP address, you can select “DHCP” on the WAN interface.

Network

IPv4 Settings
IPv6 Settings
VLAN Settings

WAN Port Setup

IP Assign: **DHCP**

IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
Primary DNS: 8.8.8.8
Alternative DNS: 4.4.4.4

LAN Port Setup

IP Address: 192.168.10.100
Subnet Mask: 255.255.255.0

☐ IP AddressV1:
Subnet MaskV1:

☐ IP AddressV2:
Subnet MaskV2:

Save
Cancel

If DHCP is selected then the WAN interface will not be configurable as it obtains all its network parameters from the DHCP server. DHCP should be used cautiously as all IP extensions register to the CooCenter system through the WAN interface and as DHCP addresses can change and IP extensions need to know the address of the CooCenter at all times. It is best practice to configure WAN address with a Static IP.

PPPoE

CooCenter can be connected to the network via ADSL modem by means of Point-to-Point Protocol over Ethernet (PPPoE)dial-up. In such a situation, extensions will subscribe to the CooCenter system through the LAN port, while WAN port can be used for remote extensions.

Network

IPv4 Settings
IPv6 Settings
VLAN Settings

WAN Port Setup

IP Assign: **PPPoE**

Username: CD85335361
Password:

IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
Primary DNS: 8.8.8.8
Alternative DNS: 4.4.4.4

LAN Port Setup

IP Address: 192.168.10.100
Subnet Mask: 255.255.255.0

☐ IP AddressV1:
Subnet MaskV1:

☐ IP AddressV2:
Subnet MaskV2:

Save
Cancel

If PPPoE is set, you have to specify the username and password given by your ISP and the CooCenter system will dial-up to the ISP and once successfully connected, you will have Internet access on the WAN interface.

LAN port connects to your local network for internal IP extensions to register. If

necessary, you can change LAN IP to suit your local network.

IPv6 Settings

Path: **Network Settings->Network->IPv6 Settings**

IPv6(Internet Protocol Version 6) has been in development for nearly two decades. Now the next-generation protocol is ready to replace IPv4 and assume its place as the back of the Internet.

Today, major Internet service providers (ISPs), home networking equipment manufacturers, and web companies around the world are permanently enabling IPv6 for their products and services. Many organizations, institutions and universities have deployed their own networks on IPv6.

To be able to deliver VoIP calls over IPv6(SIP over IPv6), you can configure CooCenter system with IPv6 addresses to be able to deploy it in your IPv6 network infrastructure.

To do this, navigate to web menu Network Settings->Network->IPv6 Settings.

Network

IPv4 Settings IPv6 Settings VLAN Settings

WAN Port Setup

Enable:	<input checked="" type="checkbox"/>
IPv6 Address:	<u>2001:db8:4005:80a::200e</u>
Prefix Length:	<u>64</u>
Gateway:	<u>2001:db8:4005:80a::1</u>
Primary DNS:	<u>2001:da8:8000:1:202:120:2:1</u>
Alternative DNS:	<u></u>

Save Cancel

Specify your IPv6 network profile here and you will be able to connect CooCenter to your IPv6 network infrastructure.

VLAN Settings

Path: **Network Settings->Network->VLAN Settings**

With a layer-3 switch you can configure VLAN on CooCenter system to divide the VoIP and data traffic. Voice VLAN can ensure that phones remain working even when the data network is congested.

To set VLAN, navigate to web menu **Network Settings->Network->VLAN**. As you can see here on this page, you are able to configure 4 VLANs, 2 each for WAN or LAN port.

Network

IPv4 Settings	IPv6 Settings	VLAN Settings
---------------	---------------	---------------

WAN VLAN 1
Enable: <input checked="" type="checkbox"/>
VLAN ID: <u>2</u>
VLAN IP Address: <u>172.16.10.2</u>
Subnet Mask: <u>255.255.255.0</u>
WAN VLAN 2
Enable: <input checked="" type="checkbox"/>
VLAN ID: <u>3</u>
VLAN IP Address: <u>172.16.20.2</u>
Subnet Mask: <u>255.255.255.0</u>
LAN VLAN 1
Enable: <input checked="" type="checkbox"/>
VLAN ID: <u>4</u>
VLAN IP Address: <u>172.16.30.2</u>
Subnet Mask: <u>255.255.255.0</u>
LAN VLAN 2
Enable: <input checked="" type="checkbox"/>
VLAN ID: <u>5</u>
VLAN IP Address: <u>172.16.40.2</u>
Subnet Mask: <u>255.255.255.0</u>

Ensure VLAN IPs for VLAN1 and VLAN2 of WAN and LAN interfaces are in several different network segments.

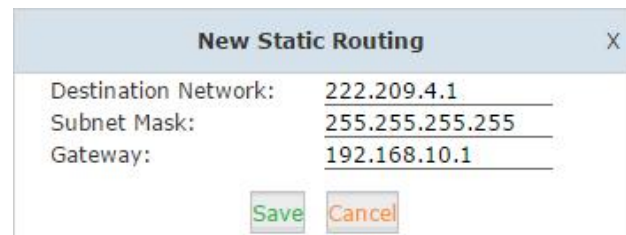
Static Routing

Static Routing

Path: **Advanced->Static Routing->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.

Click “New Static Routing” to add a new routing record to the system.



The dialog box titled "New Static Routing" contains three input fields: "Destination Network:" with the value "222.209.4.1", "Subnet Mask:" with the value "255.255.255.255", and "Gateway:" with the value "192.168.10.1". At the bottom are "Save" and "Cancel" buttons.

- **Destination:** Set the IP address of destination host or network address.
E.g.222.209.4.1, 192.168.10.0.
- **Gateway:** Set the gateway address.

After the new record has been manually created you can see it listed here on this page.

List of Static Routing				New Static Routing
	Destination Network	Subnet Mask	Gateway	Options
1	222.209.4.1	255.255.255.255	192.168.10.1	Edit Delete

You can click “[Edit](#)” button to edit one of the items, or you can delete the item by clicking the “[Delete](#)” button.

Routing Table

Path: **Static->Static Routing->Routing Table**

Click the “Routing Table” tab and you’ll see a detailed list of all the system routing rules, including default and custom ones.

Routing Table

Static Routing

Routing Table

Routing Table:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.10.1	0.0.0.0	UG	0	0	0	WAN
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	LAN
192.168.7.0	0.0.0.0	255.255.255.0	U	0	0	0	LAN
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	0	WAN
222.209.4.1	192.168.10.1	255.255.255.255	UGH	0	0	0	WAN

VPN

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

CooCenter system supports four varieties of VPN, they are L2TP, PPTP, OpenVPN and IPSec.

L2TP VPN

L2TP VPN Server

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy. Here on the CooCenter system we use IPSec to do the encryption.

To configure your L2TP server, navigate to web menu [Network Settings->VPN Server](#). Check the radio button of L2TP to configure L2TP VPN server.

VPN Server

VPN Server OpenVPN Certificate Download

VPN Server

☒ L2TP ☐ PPTP ☐ OpenVPN ☐ IPSec

Enable:	<input checked="" type="checkbox"/>
Remote Start IP:	172.16.0.2
Remote End IP:	172.16.0.9
Local IP:	172.16.0.1
Primary DNS:	8.8.8.8
Alternative DNS:	4.4.4.4
Authentication Method:	<input checked="" type="checkbox"/> chap <input checked="" type="checkbox"/> pap
Debug:	<input checked="" type="checkbox"/>
IPSec:	<input checked="" type="checkbox"/>
IPSec Local IP:	117.176.159.163 ▼
IPSec Password:	hPC2he@Q

Save Cancel

- **Enable:** Tick the checkbox to enable L2TP VPN server.
- **Remote Start IP, Remote End IP:** L2TP VPN remote network IP range, between start IP and end IP there must be less than 10 available IP addresses.

- **Local IP:** L2TP VPN local server IP address.
- **Primary DNS:** Primary DNS for VPN connection.
- **Alternate DNS:** Alternative DNS for VPN connection.
- **Authentication Method** : Select the authentication method: chap or pap.
pap: Password Authenticate Protocol, PAP works like a standard login procedure; it uses static user name and password to authenticate the remote system.
chap: Challenge Handshake Authentication Protocol
 CHAP takes a more sophisticated and secure approach to authentication by creating a unique challenge phrase (a randomly generated string) for each authentication.
- **Debug:** Tick to enable debug for L2TP VPN connection, debug info will be written into system logs.
- **IPSec:** Enable IPSec encryption for L2TP VPN server.
- **IPSec Local IP:** CooCenter system WAN IP which can access Internet.
- **IPSec Password:** Define a password for IPSec VPN client to authenticate.

Notice:

If the CooCenter system is behind NAT, you need to open ports 500, 4500 and 1701 on the router/firewall.

For the VPN client to connect you'll need to create a VPN user account.

Click "**VPN User Management**" tab and click "**New VPN User**" button to add a VPN user account.



New VPN User	
Username:	BranchB
Password:	u%UnBa-F
Availability:	Yes ▼
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Now the L2TP VPN client can connect to the L2TP VPN server.

L2TP VPN Client

For example, in the branch office you are going to connect another CooCenter system to the head office using L2TP VPN.

Navigate to the web menu **Network Settings->VPN Client**. Check the radio button of L2TP to configure L2TP VPN client.

VPN Client

VPN Client

☒ L2TP
 ☐ PPTP
 ☐ OpenVPN
 ☐ N2N
 ☐ IPSec

Enable: ☒

Server Address:

Username:

Password:

IPSec: ☒

IPSec Local IP:

IPSec Password:

Default Gateway: ☒

- **Enable:** Tick to enable L2TP VPN client.
- **Server Address:** L2TP server public IP.
- **Username:** L2TP VPN user name given by the VPN server.
- **Password:** L2TP VPN user password given by the VPN server.
- **IPSec:** Enable IPSec support.
- **IPSec Local IP:** Coocenter WAN IP Address that can access the Internet.
- **IPSec Password:** Set according to the password specified on the server.
- **Default Gateway:** All traffic goes through the L2TP VPN connection.

Notice:

If connection is successfully established, the system will display as follows:

Status: L2TP client VPN remote IP address 172.16.0.1

L2TP client VPN local IP address 172.16.0.x (An IP address between 172.16.0.2 and 172.16.0.9)

PPTP VPN

The Point-to-Point Tunneling Protocol (PPTP) uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

PPTP VPN Server

To configure your PPTP Server, navigate to web menu **Network Settings->VPN Server**. Check the radio button of PPTP to configure PPTP VPN server.

- **Enable:** Tick the checkbox to enable PPTP VPN server.
- **Remote IP:** PPTP VPN remote network IP range, there must be 10 or less available IP addresses between start IP and end IP.
- **Local IP:** PPTP VPN local server IP address.
- **Primary DNS:** Primary DNS for VPN connection.
- **Alternative DNS:** Secondary DNS for VPN connection.
- **Timeout(sec):** Session timeout for PPTP tunnels.
- **Authentication Method:** Choose method/methods for the authentication of the VPN clients.

chap: Challenge Handshake Authentication Protocol

CHAP takes a more sophisticated and secure approach to authentication by creating a unique challenge phrase (a randomly generated string) for each authentication.

pap: Password Authenticate Protocol PAP works like a standard login procedure; it uses static user name and password to authenticate the remote system.

mschap: MS-CHAP is the Microsoft version of the Challenge-Handshake Authentication Protocol.

mschap-v2: Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), this provides stronger security for remote access connections.

- **Enable mppe128:** Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections with 128-bit key.
- **Debug:** Tick to enable debug for PPTP VPN connection, debug information will be written into system logs.

You will need to create a VPN user account for a VPN client to be able to connect to the VPN Server.

To create an account, click “[VPN User Management](#)” tab and click “[New VPN User](#)” button to add a VPN user account.



New VPN User [X]

Username:

Password:

Availability: ▼

Now the PPTP VPN client will be able to connect to the PPTP VPN server.

Notice:

If the CooCenter system is behind NAT, you will need to open ports 1723 on the router/firewall.

PPTP VPN Client

To create your VPN client at the branch office site, open the CooCenter web GUI and navigate to web menu **Network Settings->VPN Client**. Check the radio button of PPTP to configure PPTP VPN client.

VPN Client



VPN Client

☐ L2TP ☒ PPTP ☐ OpenVPN ☐ N2N ☐ IPSec

Enable: ☒

Enable 40/128-bit encryption for MPPE: ☒

Server Address:

Username:

Password:

Default Gateway: ☒

- **Enable:** Tick to enable PPTP VPN client.
- **Enable 40/148-bit encryption for MPPE:** Tick to enable 40-bit key (standard) or 128-bit key (strong) MPPE encryption schemes.
- **Server Address:** PPTP VPN server public IP.
- **Username:** PPTP VPN user name given by the VPN server.
- **Password:** PPTP VPN user password given by the VPN server.
- **Default Gateway:** All traffic goes through the L2TP VPN connection.

Notice:

If connection is successfully established the system will display:

Status: Local IP address 172.16.0.x (An IP address between 172.16.0.2 and 172.16.0.9)

Remote IP address 172.16.0.1

OpenVPN

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls. It was written by James Yonan and is published under the GNU General Public License (GPL).

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

OpenVPN Server

To create your OpenVPN Server, navigate to web menu **Network Settings->VPN Server**. Check the radio button of OpenVPN to configure your OpenVPN server.

The screenshot shows the 'VPN Server' configuration window. At the top, there are four radio buttons: L2TP, PPTP, OpenVPN (selected), and IPSec. Below this, there are several configuration options with checkboxes and input fields. The 'Enable' checkbox is checked. The 'Stealth' checkbox is checked. The 'Certificate' field shows 'Done' with 'Create' and 'Delete' buttons. The 'Port' field is set to '1194'. The 'Stealth Port' field is set to '443'. The 'Protocol' dropdown is set to 'TCP'. The 'Device Node' dropdown is set to 'TUN'. The 'Cipher' dropdown is set to 'Default'. The 'Compress Lzo' checkbox is checked. The 'TLS-Server' checkbox is checked. The 'Remote Network' field is set to '172.16.0.0 / 255.255.255.0'. The 'Route' field is set to '172.16.0.0 / 255.255.255.0'. The 'Client-to-Client' checkbox is checked. At the bottom, there are 'Save' and 'Cancel' buttons.

- **Enable:** Tick to enable OpenVPN server.
- **Stealth:** Certain deep packet inspection firewalls might not allow OpenVPN traffic, stealth SSL tunneling can disguise your OpenVPN traffic under the HTTPS traffic which is often seen as HTTPS traffic by the DPI.
- **Certificate:** Certificate is one of the client authentication methods available in OpenVPN.
- **Port:** OpenVPN service port, the default is 1194.
- **Stealth Port:** Stealth service port, the default is 443.
- **Protocol:** You can choose either UDP or TCP. Stealth requires TCP only so if you have stealth enabled then this option is not configurable and the Server will use TCP by default.

- **Device Node:** TUN or TAP; A TAP device is a virtual Ethernet adapter, while a TUN device is a virtual point-to-point IP link.
- **Cipher:** Cipher (or cypher) is an algorithm for performing encryption or decryption.
- **Compress Lzo:** LZO is an efficient data compression library which is suitable for data de-compression in real-time.
- **TLS-Server:** TLS is an excellent choice for authentication and key exchange mechanism of OpenVPN.
- **Remote Network:** OpenVPN remote network.
- **Route:** The route entries adjust the local routing table, telling it which network to route over the VPN.
- **Client-to-Client:** Client-to-Client can enable intercommunication between clients.

IPSec VPN

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

IPSec can be configured to operate in two different modes, Tunnel and Transport mode. Use of each mode depends on the requirements and implementation of IPSec.

IPSec VPN Server (Tunnel mode)

Tunnel mode is used to encrypt all traffic between secure IPSec Gateways, for example if you have two CooCenter systems and each acts as an IPSec Gateway for the hosts/IP phones behind it. The WAN ports will be used to connect both CooCenter systems to establish IPSec VPN connection, now all PCs or IP phones on the LAN ports can communicate with each other on both sides via a secure IPSec tunnel.

Navigate to web menu **Network Settings->VPN Server**. Check the IPSec radio button to configure IPSec VPN server.

VPN Server

VPN Server OpenVPN Certificate Download

VPN Server

☐ L2TP ☐ PPTP ☐ OpenVPN ☒ IPSec

Enable: ☒

Type: Tunnel

IPSec Local IP: 117.176.159.163

IPSec Password: hPC2he@Q

IPSec Remote IP 1: 192.168.1.252

IPSec Remote Network 1: 192.168.200.0 / 255.255.255.0

IPSec Remote IP 2: _____

IPSec Remote Network 2: _____ / _____

IPSec Remote IP 3: _____

IPSec Remote Network 3: _____ / _____

Save Cancel

- **Enable:** Tick the checkbox to enable IPSec VPN server.
- **Type:** Defaults to Tunnel mode.
- **IPSec Local IP:** CooCenter WAN IP, which can be used to connect to the client network.
- **IPSec Password:** Define a password for authentication of the IPSec client.
- **IPSec Remote IP:** IPSec VPN client IP. The client uses this IP to connect to IPSec server.
- **IPSec Remote Network:** Specify the IPSec VPN client LAN network address.

Notice:

1. If the CooCenter is behind NAT, port 500 and 4500 must be open on the router/firewall.
2. If the CooCenter is connected to the Internet via PPPoE, then IPSec Local IP needs to be the IP

address assigned by PPPoE.

3. IPSec VPN server can connect 3 IPSec clients.

IPSec VPN Client (Tunnel mode)

On the remote site, open the web GUI of another CooCenter system and navigate to web menu to configure the VPN Client **Network Settings->VPN Client**.

On the VPN Client page choose IPSec and tick “Enable” option to enable IPSec client.

VPN Client

VPN Client

☐ L2TP ☐ PPTP ☐ OpenVPN ☐ N2N ☒ IPSec

Enable:

☒

Type:

Tunnel

IPSec Local IP:

192.168.1.252

Server Address:

117.176.159.163

IPSec Password:

hPC2he@Q

IPSec Remote Network:

192.168.10.0 / 255.255.255.0

Save

Cancel

- **Enable:** Tick the checkbox to enable IPSec client.
- **Type:** Ensure this is the same as the IPSec server.
- **IPSec Local IP:** WAN port IP which can connect to the IPSec server.
- **Server Address:** Specify the IPSec server IP.
- **IPSec Password:** Specify the IPSec VPN password defined previously on the server.
- **IPSec Remote Network:** The IPSec VPN server LAN network address.

Notice:

1. After saving the configuration, the client will try to connect to the server using the details provided.
2. If connection is successfully established then the system will display “Status: 1 tunnel has been established!!!”
3. If connection fails then the system will display “Status: There’s no tunnel! Reconnecting...”

IPSec VPN server (Transport mode)

IPSec Transport mode is used for end-to-end communications, NAT traversal is not supported with the transport mode. So if two CooCenter systems are connected via IPSec transport mode, IPSec only encrypts the communication service ports, unlike Tunnel mode which encrypts the whole LAN subnet.

Navigate to web menu **Network Settings->VPN Server**. Check the IPSec radio button.

- **Enable:** Tick the checkbox to enable IPsec VPN server.
- **Type:** Select Transport mode.
- **IPsec Local IP:** CooCenter WAN IP.(This is the same as configuring in Tunnel mode)
- **IPsec Password:** Define a password for authentication of the IPsec client.

IPsec VPN Client(Transport mode)

On the remote site, open the client CooCenter web GUI and navigate to web menu Network Settings->VPN Client. Check the radio button of IPsec.

- **Enable:** Tick the checkbox to enable IPsec VPN client.
- **Type:** Ensure this is the same as the IPsec VPN server.
- **IPsec Local IP:** CooCenter WAN IP which can connect to the IPsec server.
- **Server Address:** IPsec VPN server IP.
- **IPsec Password:** Specify the IPsec VPN password defined previously on the server.

Notice:

If a successful connection is established, then the system will display "Status: 2 tunnels have been established!!!". Because the CooCenter system encrypts all service ports over UDP and TCP protocols, this means there will be 2 tunnels established.

N2N VPN Client

N2N is an open source Layer 2 over Layer 3 VPN application which utilizes a peer-to-peer architecture for network membership and routing.

On CooCenter system we support N2N VPN client, to configure the N2N VPN client, please navigate to web menu Network Settings->VPN Client. Check the radio button of N2N VPN and configure the client info.



VPN Client

☐ L2TP
 ☐ PPTP
 ☐ OpenVPN
 ☒ N2N
 ☐ IPSec

Enable: ☒
 Server Address: 88.86.108.50
 Port: 82
 Local IP: 192.168.20.101
 Subnet Mask: 255.255.255.0
 Local Port: 30256
 Username: user1
 Password: *****

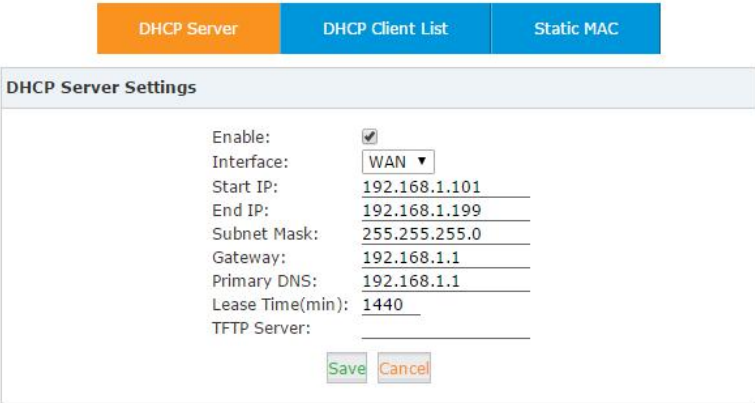
- **Enable:** Tick this checkbox to enable N2N VPN client.
- **Server Address:** N2N server(supernode) IP address.
- **Port:** N2N service port number. This is 82 by default.
- **Local IP:** VPN local IP.
- **Subnet Mask:** Netmask of the VPN network.
- **Local Port:** N2N local service port.
- **Username/Password:** Used for the N2N server to authorize the connection.

DHCP Server

DHCP Server

Path: **Advanced->DHCP Server->DHCP Server**

Navigate to web menu **Network Settings->DHCP Server**.



DHCP Server Settings

Enable: ☒
 Interface: WAN
 Start IP: 192.168.1.101
 End IP: 192.168.1.199
 Subnet Mask: 255.255.255.0
 Gateway: 192.168.1.1
 Primary DNS: 192.168.1.1
 Lease Time(min): 1440
 TFTP Server:

- **Enable:** Enable DHCP service.
- **Interface:** Choose the network port to implement DHCP service.
- **Start IP, End IP:** Specify the DHCP IP address pool.
- **Subnet Mask:** Netmask to be assigned to client devices.
- **Gateway:** Gateway address to be assigned to client devices.
- **Primary DNS:** DNS to be assigned to client devices.
- **Lease Time(min):** Duration for DHCP server to lease an address to a new device.

When the lease expires, the DHCP server might assign the IP address to a different device. Default value is 1440 minutes.

- **TFTP Server:** Input the TFTP server address if required which may be used to auto provision your IP phones.

DHCP Client List

Path: **Advanced->DHCP Server->DHCP Client List**

Navigate to Network Settings->DHCP Server->DHCP Client List and you will see a list of all devices receiving their IP address from the CooCenter system.

DHCP Client List 

<div>DHCP ServerDHCP Client ListStatic MAC</div>			
DHCP Client List:			
Mac Address	IP Address	Host Name	Expires in
00:0b:82:71:b3:17	192.168.1.157		23:08:17

Static MAC

Path: **Advanced->DHCP Server->Static MAC**

Static MAC is a useful feature which ensures the DHCP service on CooCenter always assigns the same IP address to a specific computer or IP phone on your LAN. To be more specific, the DHCP service assigns this static IP to a unique MAC address assigned to each NIC on your LAN.

To create a static Mac, navigate to web menu Network Settings->DHCP Server->Static MAC. Click “[New Static MAC](#)” to add a record to the CooCenter system.

New Static MAC

X

MAC Address: 192.168.1.123

IP Address: 6e72c3d4e5f6

SaveCancel

In this example, the IP address 192.168.1.123 will always be assigned to the device with MAC address 6E:72:C3:D4:E5:F6, lease time will not apply to this IP Address.

DDNS Settings

Path: **Networking Settings->DDNS Settings**

Unlike DNS that only works with static IP addresses, DDNS (Dynamic Domain Name Server) is designed to also support dynamic IP addresses, such as those assigned by a DHCP server.

Built-in DDNS feature on CooCenter system only requires you to sign up with a Dynamic DNS provider, then with the domain name they provide which maps your IP address on the Internet, you can access CooCenter and also other services within your LAN via the domain name without needing to know your Dynamic public IP Address.

After setting DDNS, CooCenter phone services can be accessed from remote site via the domain name which your DDNS provider supplied you. Also remote management is possible, even without a static public IP.

CooCenter system supports the following DDNS service providers:

- <http://dyn.com/>
- <http://www.noip.com/>
- <http://www.zoneedit.com/>
- <http://www.oray.com/>
- <http://www.3322.net>
- <http://freedns.afraid.org/>

Sign up to one of these DDNS service providers' website and subscribe a dynamic domain name. Once you have your account details, navigate to web menu **Network Settings ->DDNS Settings**.

DDNS Settings



Enable:	<input checked="" type="checkbox"/>
DDNS Server:	dyndns.org
Username:	zycootech
Password:
Domain:	zycootech.dyndns.org
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- **Enable:** Tick to enable DDNS service.
- **DDNS Server:** Select the DDNS service provider which you have subscribed to.
- **Username:** Username you subscribed to the service provider.
- **Password:** Password you used to sign up to the service provider.
- **Domain:** Your domain name.

After completing the above, please configure port forwarding on your router/firewall, then you'll be able to remote access CooCenter services from the internet using this dynamic domain. For example, you can port forward port number 8080 and then you can access

the CooCenter web interface using the URL: <https://zycootech.dyndns.org>.

Security

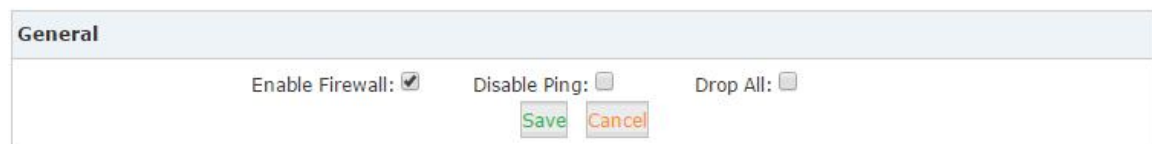
Firewall

Path:**Security->Firewall**

CooCenter system has been preconfigured with a built-in firewall which prevents your IP phone system from unauthorized access, phone calls and certain other attacks.

To manage the firewall, navigate to web menu Security->Firewall.

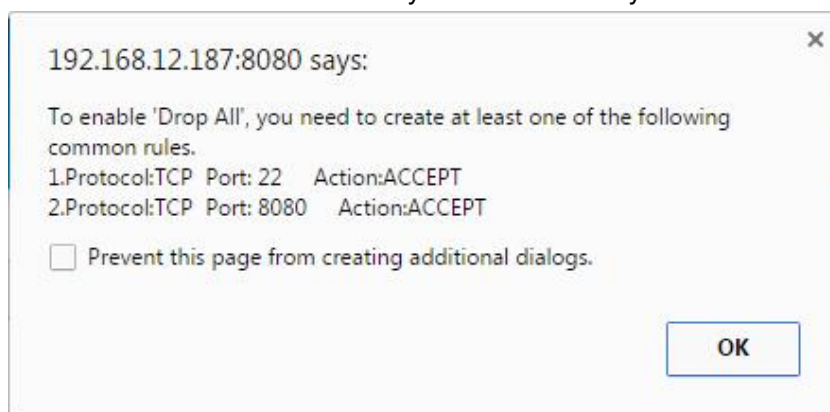
General



General

Enable Firewall: ☒ Disable Ping: ☐ Drop All: ☐

- **Enable Firewall:** By default, the firewall is enabled. You may disable the built-in firewall by unchecking “Enable Firewall” checkbox. Only consider disabling your firewall if your CooCenter is behind a router/firewall without any port forwarding from the Internet.
- **Disable Ping:** Ignore ping request. If enabled, you cannot ping the CooCenter system.
- **Drop All:** Drop all packets sent to the CooCenter system, this will cause CooCenter system to block all communication with the outside world. Because of this, the system will prompt to add at least one grant rule on port 22(SSH) or 8080(Web) to make sure the CooCenter system is not totally unreachable.



192.168.12.187:8080 says:

To enable 'Drop All', you need to create at least one of the following common rules.

1.Protocol:TCP Port: 22 Action:ACCEPT
2.Protocol:TCP Port: 8080 Action:ACCEPT

☐ Prevent this page from creating additional dialogs.

The rule/rules can be created in the “Common Rules” section.

Common Rules

In Common Rules section, you can configure the firewall to grant or deny an IP address or a network from communicating with the CooCenter system. Even the service port number can be specified so it can grant or deny a specific IP or network to access a specific service.

By clicking “[Add Rule](#)” button you can add a custom rule for rejecting or accepting an IP address or network address.

- **Name:** A name for this rule.
- **Description:** Optional, you may describe why this rule has been created.
- **Protocol:** Transmission protocol, UDP, TCP or UDP with TCP.
- **Port:** Service port number.
- **IP:** Can be an IP address or a network address.
- **MAC:** Action to be taken according to the Mac address of a device instead of its IP Address. This only works with devices within the same local network because Mac address are not routable.
- **Action:** Select “[Drop](#)” to block and “[Accept](#)” to grant.

Auto Defense

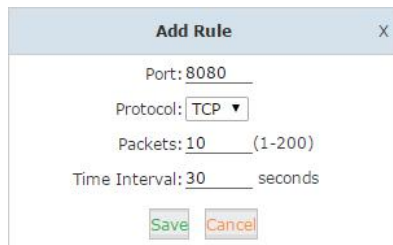
CooCenter system uses Fail2Ban to perform intrusion detection, iptables is used for blocking any attack attempts.

Fail2Ban is an intrusion prevention framework written in the Python programming language. It works by reading Asterisk logs and some other logs in the Coocenter system, and uses iptables profiles to block brute-force attempts.

In the Auto Defense section you can define some custom rules to help the Coocenter system determine brute-force attempts.

Auto Defense			Add Rule
Port	Protocol	Rate	Options
5060	UDP	40/2s	Edit Delete
5061	TCP	80/2s	Edit Delete

Click “[Add Rule](#)” button to add a new custom rule.



Add Rule X

Port: 8080

Protocol: TCP ▼

Packets: 10 (1-200)

Time Interval: 30 seconds

Save Cancel

In this example, it will block an IP Address that sends more than 10 packets to the port 8080 within 30 seconds, this rule will prevent brute-force attempts on the web GUI login.

Rejected IP

Any IP address that is banned will be shown in the table of “Rejected IP”. The table will show the IP address of the banned host, as well as what kind of service intrusion was detected.

Rejected IP		
Type	IP	Options
VOIP	212.83.154.178	Delete
VOIP	173.249.158.227	Delete
VOIP	5.189.154.148	Delete

If a host appears incorrectly in the list of rejected IP, you can click on the "Delete" button to remove it from the list.

Fail2Ban

Fail2Ban

Path: **Security->Fail2Ban->Fail2Ban**

Allowed address allows you to add IP addresses and network addresses to the CooCenter system as a whitelist. The IPs in the whitelist will always be treated as trusted IP's and will not be filtered by the firewall rules.

Navigate to web menu Security->Allowed Address. Click “Add New IP” button and you can add a trusted IP or network to the system IP whitelist.



Add Allowed IP X

Description: all

Protocol: ☒ SIP ☒ IAX2 ☒ HTTPS ☒ SSH

Allowed IP: 117.176.159.157

Subnet Mask: 255.255.255.255

Availability: Yes ▼

Save Cancel

- **Description:** A name for this entry.
- **Protocol:** Select protocols this IP/network can access.
- **Allowed IP:** IP address or network to be trusted.
- **Subnet Mask:** Netmask for this IP or network.
- **Availability:** Choose “Yes” to activate this entry, choose “No” to deactivate.

Settings

Path: **Security->Fail2Ban->Settings**

Allowed Address

Allowed Address	Settings
SIP	
Max Retry: <input type="text" value="10"/>	
Find Time: <input type="text" value="600"/> seconds	
Ban Time: <input type="text" value="3600"/> seconds	
IAX2	
Max Retry: <input type="text" value="10"/>	
Find Time: <input type="text" value="600"/> seconds	
Ban Time: <input type="text" value="3600"/> seconds	
HTTPS	
Max Retry: <input type="text" value="5"/>	
Find Time: <input type="text" value="600"/> seconds	
Ban Time: <input type="text" value="600"/> seconds	
SSH	
Max Retry: <input type="text" value="5"/>	
Find Time: <input type="text" value="600"/> seconds	
Ban Time: <input type="text" value="600"/> seconds	

These options are actually for Fail2Ban, the “**Max Retry**” limits the authentication attempts. “**Find Time**” defines the time duration from the first attempt to the last attempt which reaches the “**Max Retry**” limitation. “**Ban Time**” is the time in seconds the CooCenter system will block the IP which exceeds max retry. These settings don’t take effect on any allowed addresses.

Report


Register Status

On the register status page you are able to check the extension and SIP/IAX2 trunk status intuitively. You can view from which IP an extension is registered and you can also see the connection state, for example how much delay there is between the CooCenter system and the end point.

SIP Users Status

Path: **Report->Resister Status->SIP Users Status**

Navigate to web menu Report->Register Status->SIP User Status.

Register Status 

SIP Users Status		IAX2 Users Status		SIP Trunks Status		IAX2 Trunks Status	
SIP Users Status							
Name	Extension	IP	NAT	ACL	Port	Status	
401	401	N/A	No	No	N/A	Unregistered	
402	402	192.168.7.32	No	No	5060	Registered (4 ms)	
403	403	192.168.7.147	No	No	45290	Registered (5 ms)	
404	404	N/A	No	No	N/A	Unregistered	
405	405	N/A	No	No	N/A	Unregistered	
406	406	N/A	No	No	N/A	Unregistered	
407	407	N/A	No	No	N/A	Unregistered	
408	408	N/A	No	No	N/A	Unregistered	
409	409	192.168.7.147	No	No	39480	Registered (4 ms)	
410	410	N/A	No	No	N/A	Unregistered	
411	411	N/A	No	No	N/A	Unregistered	
John Doe	682	N/A	Yes	No	N/A	Unregistered	

Here on this page you can see the SIP/IAX2 extensions, web extensions and also the register status of trunk users. Only a trunk that is configured as peer mode will be listed here.


Status and Description

- **Registered:** Registration success.
- **Unregistered:** Registration failure or unapplied.
- **Unreachable:** Network issue.
- **Timeout:** Register request timeout.

IAX2 Users Status

Path: **Report->Resister Status->IAX2 Users Status**

To view IAX2 user status, navigate to web menu **Report->Register Status->IAX2 Users Status**.

Register Status 

SIP Users Status		IAX2 Users Status		SIP Trunks Status		IAX2 Trunks Status	
IAX2 Users Status							
Name		Extension	IP		Port	Reachability	
412		412	192.168.7.32		4569	Registered (2 ms)	
413		413	N/A		N/A	Unregistered	


Status and Description

- **Registered:** Registration success.
- **Unregistered:** Registration failure or unapplied.
- **Unreachable:** Network issue.
- **Timeout:** Register request timeout.

SIP Trunks Status

Path: **Report->Resister Status->SIP Trunks Status**

To view SIP trunk status, navigate to web menu Report->Register Status->SIP Trunk Status.

Register Status 

SIP Users Status	IAX2 Users Status	SIP Trunks Status	IAX2 Trunks Status
SIP Trunks Status			
Username	Hostname/IP	Status	
5252742452	gw1.sip.us:5060	Registered	
61921248	183.62.205.209:5060	Registered	

Here you can see all your outbound SIP trunks' status.


Status and Description

- **Registered:** Successfully registered to the service provider and ready for phone calls.
- **Request Sent:** In this status, it's most probable that the network is totally unreachable to the SIP server. Please make sure network setting on the CooCenter system are correct.
- **Waiting for Authentication:** If "Waiting for Authentication" then most probably the register request has already been received by the server side but cannot authenticate the register request due to incorrect credentials. Please double check your credentials.
- **Failed:** After trying to register within a certain time period without success, you get "Failed" on the trunk status.

IAX2 Trunks Status

Path: **Report->Resister Status->IAX2 Trunks Status**

To view IAX2 trunk status, navigate to web menu Report->Register Status->IAX2 Trunk Status.

Register Status 

SIP Users Status	IAX2 Users Status	SIP Trunks Status	IAX2 Trunks Status
IAX2 Trunks Status			
Username	Hostname/IP	Status	
asterisk	192.168.7.146:4569	Registered	

Here you can see all of your outbound IAX2 trunks' status.

Status and Description

- **Registered:** Successfully registered to the service provider and ready for phone

calls.

- **Request Sent:** If in this status, it's most probable that the network is totally unreachable to the service provider. Please make sure network setting on the CooCenter system are correct.
- **Waiting for Authentication:** If "Waiting for Authentication" then most probably the register request has already been received by the server side but cannot authenticate the register request due to incorrect credentials. Please double check the credentials again.
- **Failed:** After unsuccessfully trying to register within a certain time period, you will see "Failed" on the trunk status.

Record List

Call Recording

Path: **Report->Record List->Call Recording**

On the web page Report ->Record List. You are able to search all recorded call conversations if you have configured the extension to be always recorded.

Call Recording

Call Recording			Conferences	One Touch Recording	
Caller ID: <input type="text"/>	Destination ID: <input type="text"/>	Duration(sec): <input type="text" value="Less"/>			
Start Date: <input type="text" value="Dec"/> <input type="text" value="17"/> <input type="text" value="2018"/>	End Date: <input type="text" value="Dec"/> <input type="text" value="17"/> <input type="text" value="2018"/>	<input type="button" value="Filter"/>			
List of Recording Files			<input type="button" value="Delete Selected"/>		
<input type="checkbox"/>	Caller ID	Destination ID	Date	Duration(sec)	Options

- **Extension:** Select an extension number to search the recordings of this extension.
- **Delete:** Delete all recordings from the selected extension number.
- **Field:** Filter the recordings by specifying caller ID or destination ID. For example, if you select "Caller ID" and specify number 401, you will get back the recordings of the calls made by extension 401; if you select "Destination ID" and specify number 401, you get back the recordings of the calls which called extension 401.
- **Start Date/End Date:** Search recordings made during this time period.
- **Delete Selected:** Delete the select recording items.
- **Caller ID:** Caller ID of this recorded call.
- **Destination ID:** The number that was called.
- **Date:** Exact time when this call recording began.
- **Duration(sec):** Duration of the recording.
- **Options:** Playback, delete and download options for the recorded files.
- **Play:** You can playback the recordings directly on the web page or playback on a

specific phone.

Conference

Path: **Report->Record List->Conference**

All recorded conferences can be found here on Report->Record List->Conference page.

Conferences

Call Recording		Conferences		One Touch Recording	
Start Date: Dec ▼ 21 ▼ 2015 ▼		End Date: Dec ▼ 21 ▼ 2015 ▼		Filter	
List of Conference Record Files				Delete Selected	
Conference Room		Date		Options	
<input type="checkbox"/>	1 900	2015/12/21 14:52:39		<input type="checkbox"/>	Play Delete

- **Start Date/End Date:** Specify a time duration to search the recorded conferences.
- **Delete Selected:** Delete the selected searched results.
- **Delete All:** Delete all searched results.
- **Conference Room:** The number of the recorded conference.
- **Date:** Exact time when the conference began.
- **Options:** Playback, delete or download the recording file.
- **Play:** Playback the recordings directly on the web page or playback on a specific phone.
- **Delete:** Delete the recorded audio file.

One Touch Recording

Path: **Report->Record List->One Touch Recording**

Call recordings recorded by one touch recording feature code *1 and can be found on Report-> Record List->One Touch Recording page.

One Touch Recording

Call Recording		Conferences		One Touch Recording	
Extension: 402 ▼		Delete			
Start Date: Dec ▼ 21 ▼ 2015 ▼		End Date: Dec ▼ 21 ▼ 2015 ▼		Filter	
List of Recording Files				Delete Selected	
Caller ID		Destination ID		Date	
<input type="checkbox"/>	1 402	403		2015/12/21 14:49:15	
				Options	
<input type="checkbox"/>				Play Delete	

- **Extension:** Extensions that used one touch recording to record calls will be listed here.

- **Delete:** Delete all recordings for the selected extension number.
- **Start Date/End Date:** Search the recordings during this time period.
- **Delete Selected:** Delete the select recording items.
- **Caller ID:** Caller ID of this recorded call.
- **Destination ID:** The number the caller called.
- **Date:** The exact time when this call began.
- **Play:** Playback, delete and download options of the recording files.
- **Delete:** Delete the recorded audio file.

Call Recording Playback


Path: **Report->Record List**

On CooCenter system, there are two ways to playback recordings.

- Playback on the web interface
- Playback on a specific phone

By clicking the “**Play**” button on a call recording file you’ll see a dialog box like below:



With “**Type 1**”, you can click the  button you can playback the recording directly on the web interface.

With “**Type 2**”, you can specify an extension number and click on “**Play**” and then the extension will ring and you can pickup the call and the recording will play on the phone.

Call Logs

Path: **Report->Call Logs**

Call logs are also known as CDR(Call Detailed Records), on the call logs page you can check records for any call that went through the CooCenter system.

Navigate to web menu **Report->Call Logs** and by specifying the time duration and/or Caller ID/Destination ID/Account you can find the call records that you require.

Call Logs

Start Date:	Dec ▾	21 ▾	2015 ▾	Field: Caller ID ▾	<input type="text"/>	Filter
End Date:	Dec ▾	21 ▾	2015 ▾		Download	Delete
Call Start	Caller ID	Destination ID	Account Code	Duration(sec)	Disposition	
2015-12-21 16:35:56	402 <402>	013880424687	50377	240	Answered	
2015-12-21 16:33:41	402 <402>	013880424687		43	Answered	
2015-12-21 16:08:49	402 <402>	785756211		252	Answered	
2015-12-21 16:06:00	85337096 <85337096>	402		55	Answered	
2015-12-21 14:52:35	404 <404>	conference		2031	Answered	
2015-12-21 14:52:49	402 <402>	conference		2014	Answered	
2015-12-21 14:53:07	402 <402>	conference		56	Answered	
2015-12-21 14:50:02	404 <404>	conference		42	Answered	
2015-12-21 14:50:28	402 <402>	conference		12	Answered	
2015-12-21 14:49:15	402 <402>	402		22	Answered	
2015-12-21 12:00:21	402 <402>	402		40	Answered	
2015-12-21 11:46:40	402 <402>	402		7	Answered	
2015-12-21 11:46:33	402 <402>	403		2	Answered	

Total:13 35 ▾ Per Page Pages:<< 1 ▾ >>

- **Start Date/End Date:** Define the searching time period by “Start Date” and “End Date”.
- **Field:** Search criteria.
Caller ID: Search by the caller number.
Destination ID: Search by the called number.
Account Code: Search within the pin code which was used for outbound dialing.
- **Download:** Download the search results.
- **Delete:** Delete the search results.
- **Call Start:** The exact time when this call began.
- **Caller ID:** The number of the caller.(By clicking on the number you can add this number to the CooCenter system phone book.)
- **Destination ID:** The number which has been called.(By clicking on the number you can add this number to the CooCenter system phone book.)
- **Account Code:** The pin code that was used for outbound dialing.
- **Duration:** The duration of this phone call.
- **Disposition:** How the calls have been handled. Either answered, no answer or failed.

System Logs

Path: **Report->System Logs**

These logs are CooCenter journals which store all system activities. They can be used for debug purpose if the system is running into exception. Please do not enable these logs if the system is functioning properly as debug information creates large log files which consume space and also utilize system resources.

In the CooCenter system, there are 4 kinds of log files.

- [System Log](#): System Logs store all system events.
- [PBX Log](#): PBX Logs store all Asterisk events.
- [PBX Debug Log](#): Asterisk debug logs.
- [Access Log](#): Web and SSH access logs.

To enable these logs for the CooCenter system, please navigate to web menu Report->System Logs. And enable the logs by ticking the corresponding checkboxes.

System Logs

Enable System Log:	<input checked="" type="checkbox"/>	Enable PBX Log:	<input checked="" type="checkbox"/>
Enable PBX Debug Log:	<input checked="" type="checkbox"/>	Enable Access Log:	<input checked="" type="checkbox"/>

[Save](#) [Cancel](#)

After checking the checkboxes please click “[Save](#)” and the log files will be generated.

List of Logs ↕

Download Selected

Delete Selected

<input type="checkbox"/>	Name	Type	Options	
<input type="checkbox"/>	1 debug20151221.log	Debug Log	<div>Delete</div>	<div>Download</div>
<input type="checkbox"/>	2 login201512.log	Login Log	<div>Delete</div>	<div>Download</div>
<input type="checkbox"/>	3 pbx20151221.log	PBX Log	<div>Delete</div>	<div>Download</div>
<input type="checkbox"/>	4 sys20151221.log	System Log	<div>Delete</div>	<div>Download</div>

Each day there will be a new log file generated for each of the log types. Enable them only if you are familiar with these logs for troubleshooting purposes.

System

Time Settings

System time is very important for the CooCenter system, especially if the CooCenter system handles inbound phone calls using time rules, then only if the system time is correct will calls be handled properly. Also, call logs and debug logs recorded to the

system events use system time.

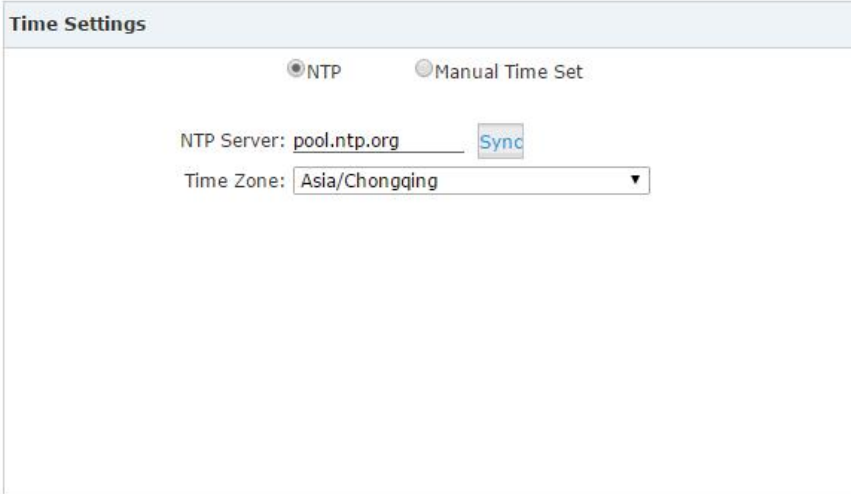
CooCenter system supports NTP (Network Time Protocol) and manual time set.

NTP

Path: **System->Time Settings->NTP**

By default, CooCenter system use NTP to obtain time from Internet time servers. To configure, simply inform the CooCenter system where to find the server by specifying its domain or IP address. Also, please remember to select the correct time zone.

Time Settings



☒ NTP ☐ Manual Time Set

NTP Server:

Time Zone:

Once complete, click “Sync” button and the CooCenter system will attempt to synchronize the current time from the Internet. It might take a while depending on your network conditions.

After the process is complete, you’ll receive a notice saying either “Sync Failed!” or “Sync Success!”. If failed, then please check if the CooCenter can access the Internet or please change to another NTP server and try again.

Manual Time Set

System->Time Settings->Manual Time Set

If you want to manually set the time for the CooCenter system or for some special reason the CooCenter cannot access the Internet. You can choose to manually set the system time by checking “Manual Time Set” radio button.

Time Settings

Time Settings

☐ NTP ☒ Manual Time Set

Year: (YYYY, eg: 2010)

Month: (MM, eg: 05)

Day: (DD, eg: 08)

Hour: (HH, eg: 09)

Minute: (MM, eg: 30)

Synchronize with current PC time [Sync](#)

[Save](#) [Cancel](#)

There are two ways to manually set a time on the system.

1. Manually input the time and date info and click “[Save](#)”.
2. Synchronize the CooCenter system time with your PC time by clicking “[Sync](#)” button and then click on “[Save](#)” button.

Once “[Save](#)” is clicked the time is manually written or synchronized from the PC and will be stored into the hardware clock chip on the CooCenter motherboard.

Data Storage

Path: **System->Data Storage->Data Storage**

Data storage allows you to upload your recording files, log files and voicemail messages to an FTP server through the Ethernet. If a USB drive is attached to the USB interface then the call recordings will be saved automatically to the USB drive instead of internal storage of the CooCenter system.

Data Storage

USB Data Storage

Plug the USB disk to the USB interface of CooCenterdevice. Navigate to [Home](#) page. You’ll see the USB storage info like below snapshot.

Home 

System Info			
Network			
WAN	IP: 192.168.1.7	MAC: 68:69:2E:04:18:1A	
LAN	IP: 192.168.10.100	MAC: 68:69:2E:FF:18:1A	
Storage			
Disk	Total:	5.3G	Used: 2.1G
Ext Disk	Total:	7.5G	Used: 129M
Slot Info			
SLOT 1		SLOT 2	
1	2	3	4
FXO	FXO	FXS	FXS
1	2	3	4
GSM	GSM	N/A	N/A

Call recordings will be saved into USB drive without additional configurations. And the files can be accessed from CooCenter system Web GUI.

Important Notice:

1. If you are using a mobile HDD please use external power supply to power the mobile HDD.
2. You can plug in the USB drive with COOCENTER system in production, but please DO NOT unplug it without cut off the power.

FTP Data Storage

Utilizing your existing FTP server, you can configure the CooCenter to upload call recordings, voicemails and call log files to your FTP server. If you don't have one you can even use your Windows PC to setup an FTP server for the CooCenter system to connect to. You must however ensure that your PC is always turned on or at least available at the times when your CooCenter is going to upload files.

Data Storage

Data Storage

Data Storage Log

Data Storage

Enable: ☒

Server Address: 192.168.1.149

Username: U50

Password:

Directory: /uploading

Automatically upload frequency(day): 7

Time of automatically upload: 13 : 01

Forcibly upload when the flash storage is over: 60%

Call Recording: ☒ Voicemail: ☒ Call Logs: ☒

Save Cancel

Status: Disabled Upload Now

After each upload you'll have a new folder created on your FTP server directory named by the date and time of this upload.

<< Local Disk (C:) > ftp > uploading > 2015_12_22_13_30 > <input type="text" value="Search 2015_"/>			
Include in library > Share with > New folder			
	Name	Date modified	Type
ites			
ktop	cdr-custom	12/22/2015 1:30 PM	File folder
wnloads	monitor	12/22/2015 1:30 PM	File folder
ent Places	voicemail	12/22/2015 1:30 PM	File folder

Notice:

After each upload, with the exception of call logs(Master.csv inside cdr-custom folder) all other files will be removed from the CooCenter system, including call recordings(files inside monitor folder) and voice messages(files inside voicemail folder). So after each upload you will only have newly generated audio files.

Data Storage Log

Path: **System->Data Storage->Data Storage Log**

On this page, you can view all the data storage recordings.

Data Storage Log



Refresh: click on this button, this page will be loaded again, and then you will obtain the newest data.

Clear: this button is used to delete some useless data.

Management

Path: **System->Management**

Set System Voice Prompts

What are system voice prompts?

System voice prompts guide callers on for example how to place a call or how to use the CooCenter system functionality. One example is while checking voicemail the system voice prompts informs the user to enter voicemail password and in another example if you call someone and they don't answer then the system voice will ask that you should leave a message.

In the “[Set Language](#)” section you can decide in which language the system uses for the callers.



Set Language	
Set Voice Language:	English * ▼ Download Delete
Save	

At this time, CooCenter system(firmware version 3.0) supports 22 different languages as the system voice prompts. They are English, English (Australia), Chinese, French, French (Canada), Spanish, Spanish (Mexico), Portuguese, Portuguese (Brazil), Italian, Persian, Arabic, Turkish, Thai, Russian, Polish, Dutch, Korea, Hungary, Vietnamese, Hebrew, Greek and Germany.

The items with * means these languages already exist on the system while others can be downloaded here by clicking the “[Download](#)” button.

Backup

Take a Backup

Path: **System->Backup->Backup**

Taking a backup on CooCentersystem is the same as when you create a recovery point on your Windows system. By restoring the backup you can recover the CooCenter system configurations to the time point when it was still functioning well.

Normally the first backup should be taken when you have finished configuring the CooCenter to work for the very first time. Also, when you have applied new changes to your configuration is always a good time to take another backup.

Navigate to web menu System->Backup. Click “Take a Backup” button to create a backup file which will contain all current system configurations.

Backup


Backup

Upload Backup File

List of Backups

Take a Backup

	Name	Date	Options
1	backup_2015dec14_174001	Dec 14, 2015	<div>RestoreDelete</div> <div>Download</div>

Once complete, you will see the backup file listed on this page. The file is stored in the file system. At any time, by clicking “Restore” button you can restore your configurations. By clicking “Delete” button you can delete this backup. You can also download the backup to your computer hard disk drive by clicking the  button.

Notice:

If you are downloading the backup to your computer hard drive, please keep this file confidential, because this file contains web admin password, user extension password and many other sensitive information which may compromise your CooCentersystem.

Upload Backup File

Path: **System->Backup->Upload Backup File**

Click on “[Upload Backup File](#)” tab and you are able to upload a backup file from your computer hard drive.

Upload Backup File

Backup

Upload Backup File

Upload Backup File

Note: Don't change the backup file name.

Please choose file to upload: backup_2015d...015dec22.tar

Upload

Notice:

If you are uploading a backup from another CooCenter system, please ensure they have the same hardware configurations. It is not recommended to upload backup files to different CooCenter systems, unless you are pretty comprehensive with Zycoo CooCenter systems.

Troubleshooting

Path: **System->Troubleshooting**

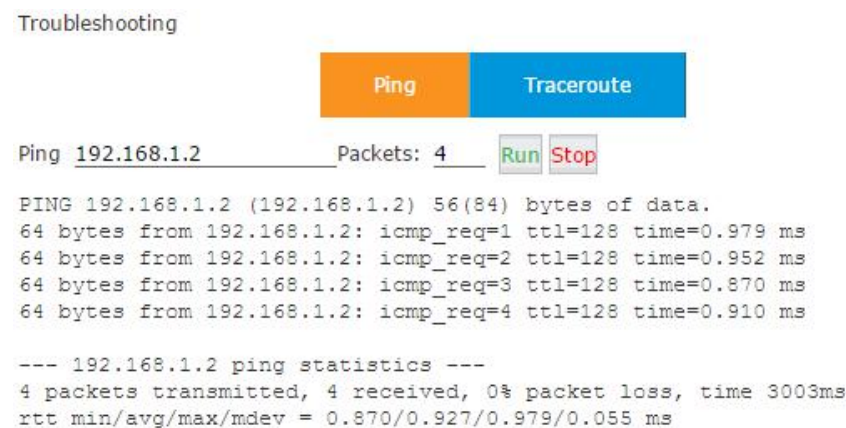
We have included two tools for troubleshooting network problems and they allow you to check the network reachability, ping and traceroute. With these tools you'll get an outside view of your network response time and network topology, which allows you to track down possible errors more easily.

Ping

Path: **System->Troubleshooting->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.



First specify the domain or IP of the host you want to contact and then define how many packets are to be sent, finally click the “Run” button and the command begins to process. You will receive results output from the system indicating the reachability of the destination.

Traceroute

Path: **System->Troubleshooting->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 that you want to lookup and then click the “Run” button to start the process.

Troubleshooting

Ping

Traceroute

Traceroute 8.8.8.8 Run Stop

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
 1  192.168.1.253 (192.168.1.253)  9.090 ms  2.339 ms  1.364 ms
 2  117.176.159.129 (117.176.159.129)  2.953 ms  3.768 ms  3.141 ms
 3  221.182.42.129 (221.182.42.129)  7.828 ms  3.642 ms  3.220 ms
 4  * * *
 5  *  221.183.19.45 (221.183.19.45)  3.036 ms  2.875 ms
 6  221.176.20.137 (221.176.20.137)  42.682 ms  42.717 ms  42.592 ms
 7  221.176.24.2 (221.176.24.2)  89.873 ms  38.681 ms  38.080 ms
 8  221.183.15.14 (221.183.15.14)  202.732 ms  202.97.15.9 (202.97.15.9)
 9  202.97.60.134 (202.97.60.134)  209.421 ms  210.220 ms  207.741 ms
10  * * *
11  *  202.97.60.82 (202.97.60.82)  210.967 ms  210.754 ms
12  202.97.61.118 (202.97.61.118)  209.741 ms  209.814 ms  212.201 ms
13  202.97.62.214 (202.97.62.214)  47.344 ms  43.307 ms  44.187 ms
14  209.85.241.56 (209.85.241.56)  43.452 ms  209.85.241.58 (209.85.241.58)
15  216.239.40.13 (216.239.40.13)  45.787 ms  209.85.142.185 (209.85.142.185)
16  216.239.57.239 (216.239.57.239)  77.555 ms  209.85.253.89 (209.85.253.89)
17  64.233.175.205 (64.233.175.205)  109.890 ms  72.14.237.171 (72.14.237.171)
18  * * *
19  google-public-dns-a.google.com (8.8.8.8)  75.043 ms  86.514 ms  72.941 ms
```

After the process has completed the system will notify you that “Trace Complete” and you can view which routes the packets have taken before reaching their final destination.

Tcpdump

Path: **System->Troubleshooting->Tcpdump**

TCPDUMP is a common packet analyzer allows users to capture TCP/IP and other packets being transmitted or received over a network to which the CooCentersystem is attached. The captured packets can be downloaded from the CooCenter system and been analyzed on your Windows PC to display the SIP traffic details. It can be used to debug a VoIP call problem.

On **System->Troubleshooting->Tcpdump** page you can do a capture on one of the CooCenterEthernet interface.

Tcpdump

[Ping](#)
[Traceroute](#)
[Tcpdump](#)
[Channel Monitor](#)

Tcpdump

Capture Trace on Adapter:

Duration(seconds): (1-300)

[Start](#)

List of Files [Delete Selected](#)

	Name	Options
<input type="checkbox"/>	1 20160506033404.pcap	Delete Download

Select an interface and specify the duration of this capture then click on “Start”, the process will begin and now you can make a call to recur the problem.

Once time is up the captured packets will be displayed in the “List of Files” section. You can download it to analyze the SIP packets for troubleshooting purpose.

Channel Monitor

Path: **System->Troubleshooting->Channel Monitor**

Channel Monitor, technically DAHDI Monitor allows you to monitor signal level on analog channel and record the output to a file. Recorded audio files are by default raw signed linear PCM. You can play it to the speaker to listen to the phone call signaling on the analog channel. Or you can use a sounds editor to visual display the audio level at both the Rx (audio Received by Asterisk) and Tx (audio Transmitted by Asterisk).

Usually Channel Monitor can be used to capture the caller ID signaling of an FXO channel. If you are experiencing caller ID problem you can perform channel monitor on the FXO port and then analyze the captured packets. If needed, you can send this file to [ZYCOO support](#) for help.

Channel Monitor

[Ping](#)
[Traceroute](#)
[Tcpdump](#)
[Channel Monitor](#)

Channel Monitor

Monitor on channel:

Duration(seconds): (1-300)

[Start](#)

List of Files [Delete Selected](#)

	Name	Options
No Files		

In the “Monitor on channel” field you should select a channel to be monitored. And then you have to specify the duration to monitor. Then click on “Start” the capture will begin. Now you should make a call in from this channel (port).

After the capture is done you'll get the file listed in the "List of Files" section.

Reset & Reboot

Path: **System->Reset & Reboot**

Reset & Reboot

Factory Defaults
<p>Warning: All the configuration data will be lost when the system is reset to factory default. Please confirm that you have already backed up the configuration before reset.</p> <p><input type="checkbox"/> Keep the current network settings</p> <p>Factory Defaults</p>
Reboot
<p>Warning: Rebooting the system will terminate all active calls!</p> <p>Reboot</p>

As you can see here on this page, you are able to reset and reboot the CooCenter system directly via web GUI.

Reset

By clicking “[Factory Defaults](#)” button you can reset all configurations for the CooCenter system. In addition to the configurations to be reset, recording files, voicemail messages and call logs will also be erased. So please ensure you have backed up the files you need before resetting.

The whole resetting process will be completed in 2 minutes. If you have chosen to reset network settings also, then you need to login with the default URL <https://192.168.1.100:8080>. Username and password will all be reset to “admin”.

Reboot

By clicking “[Reboot](#)” you can restart the CooCenter system, the whole process will be completed in 2 minutes.

Upgrade

Zycoo will update the CooCenter firmware at regular intervals for new features and bug fixes. You can visit our official website www.zycoo.com to check the updates for your CooCenter system.

The downloaded firmware package should be in .rar or .zip format, please extract the package first and upgrade with the ulmage-md5.xxx file to upgrade your CooCenter system.

Navigate to web menu **System->Upgrade**. You can see there are two methods you can upgrade the CooCenter firmware, they are web upgrade and TFTP upgrade.

WebUpgrade

Path: **System->Upgrade->WEB Upgrade**

Upgrade



Check “**WEB Upgrade**” radio button and click “**Browse**” button to locate the new firmware in your PC hard drive. Click “**Upload**” and you will be asked to confirm a restart of the CooCenter system to complete the upgrade process. You can click “**Yes**” to continue upgrading.

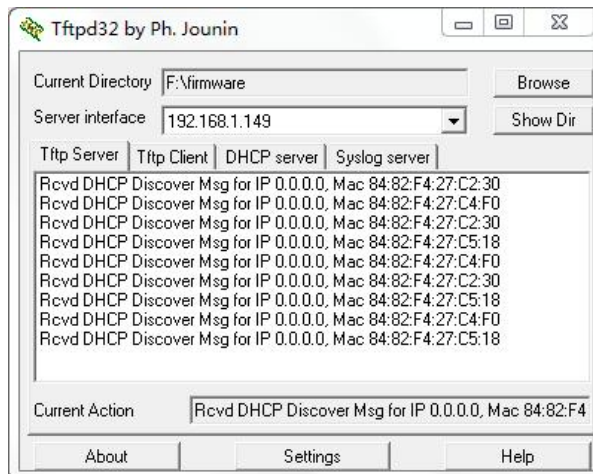
Notice:

The “**Restore Default Set**” option is used to reset the CooCenter system configurations while upgrading, You don’t have to enable this option to reset the CooCenter system and only do so if you do wish to reset to default settings as it will reset all system configurations including the network profiles.

TFTP Upgrade

Path: **System->Upgrade->TFTP Upgrade**

If you don't have a TFTP server, you can Google tftpd32 and download this application to setup a lightweight TFTP server on your Windows.



Please click “Browse” on the TFTP application window to locate the new firmware. In the “Server Interface” dropdown list is a list of your PC network interfaces. Please select a correct interface(in the same network) which can access the CooCenter system.

On the CooCenter web GUI please check the “[TFTP Upgrade](#)” radio button, and specify the exact firmware file name in the “Enter The Package Name” blank, and in the “TFTP Server IP address” blank please specify the IP address displayed on the TFTP application window.

Upgrade

Upgrade System Package

☐ WEB Upgrade ☒ **TFTP Upgrade**

Restore Default Set: ☐

Enter The Package Name: uImage-md5.s30

TFTP Server IP address: _____

Please double check the file name and TFTP server IP address then click “[Apply](#)” you will be able to upgrade the firmware just like web upgrade.