



ISG50-ISDN **ISG50-PSTN** **Application Note**

Version 2.0
June, 2012



Table of Contents

1. How to Quickly Prepare Communication Infrastructure in a New Small Business?	5
Initial Setup	5
Create Extensions	5
<i>How to configure call forwarding for each extension?</i>	10
<i>How to receive and check the voice mail?</i>	12
Firewall Setting	14
QoS	15
2. How to Manage Extensions as Business Needs Grow?	16
Auto Provision	16
SIP Server/SIP account/Password	17
Phone book	19
Feature Key	20
Firmware Upgrade	22
3. How to Develop a Non-stop Voice Service?	27
WAN failover	27
VoIP survivability	30
DDNS	31
4. How to Expand the Current Networking Infrastructure to Fulfill Multi-site Requirements?	33
Work with ZyWALL USG products	33
Trusted Peer & SIP trunk	43

5. How to Secure the Communication?	55
Site to site IPsec VPN	56
Trusted Peer over IPsec VPN	78
Brute-force Attack Protection	79
6. How to Establish a Seamless Mobile Office with ZyXEL Reach?	82
ZyXEL Reach – Smartphone Application	82
How to avoid missing any call on a certain extension?	88
Mobile Extension	90
7. How to Leverage Enterprise-class Calling Features to Increase Business Productivity?	93
Auto Attendant	93
Hunt Group	100
Three-way Conference	102
How to perform a three-way conference on ZyXEL Reach?	103
How to perform three-way conference on V310?	105
Meet-Me Conference	107
System Sound	108
How to change the language of system sounds from English to a specific language?	108
8. How to Record a Call?	111
Preparation for Call Recording	111
License	111
USB Storage	112
How to record calls on a certain trunk or an extension?	113
Full-time Recording	113

On-demand Recording	114
Query Call Recording Files	115
9. How to Audit Call Usage with Report and Analyzer to Improve Working Efficiency?	117
CDR	117
How to find the call history?	118
How to check QoS of each call in RTCP?	120
Back up CDR file	122
10. How do UC Server and UC Client Work with ISG50?	123
Preparation for TAPI Service	124
TAPI Driver Installation	126
UC Server Installation	129
UC Client Installation	139
Presence	147
Make a call	148
Hang up a call	150
Reject a call	150
Blind Transfer	151
Consultant Transfer	152
Redirect a call	153

1. How to Quickly Prepare Communication Infrastructure in a New Small Business?

Initial Setup

A network administrator plans to deploy an ISG50 for VoIP services in a new small company. First, it is necessary to prepare extension numbers, as well as enable voicemail and call forwarding for the current employees in the Sales and Marketing departments. In order to allow road warriors to register with the ISG50 using their smart phones during business trips, the network administrator needs to define the firewall rules since the ISG50 works as an all-in-one gateway.

Create Extensions

Goal to achieve: Create two authority groups for Marketing department and Sales department, and add 5 extensions in Marketing department.

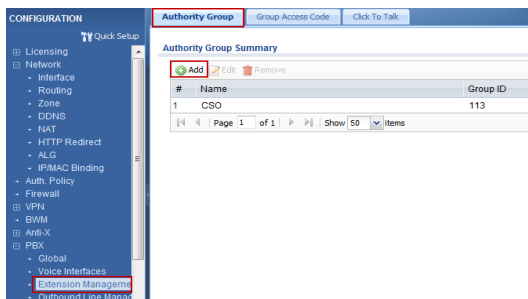
Condition:

Authority Group: Marketing and Sales

Extensions for Marketing: 3100-3104

Pin Code for Marketing: 3100-3104; Password for Marketing: 53100-53104

First, add authority groups for departments.






Create two authority groups and fill in “Marketing” and “Sales” as the authority group names.





The screenshot shows the 'Add Authority Group' dialog box. The title bar says 'Add Authority Group' and '113'. The 'General Settings' section has three fields: 'Authority Group Name' with the value 'Marketing', 'Group ID' with the value '200', and 'Description' which is empty. At the bottom are 'OK' and 'Cancel' buttons.

The screenshot shows the 'Add Authority Group' dialog box. The title bar says 'Add Authority Group' and '113'. The 'General Settings' section has three fields: 'Authority Group Name' with the value 'Sales', 'Group ID' with the value '260', and 'Description' which is empty. At the bottom are 'OK' and 'Cancel' buttons.

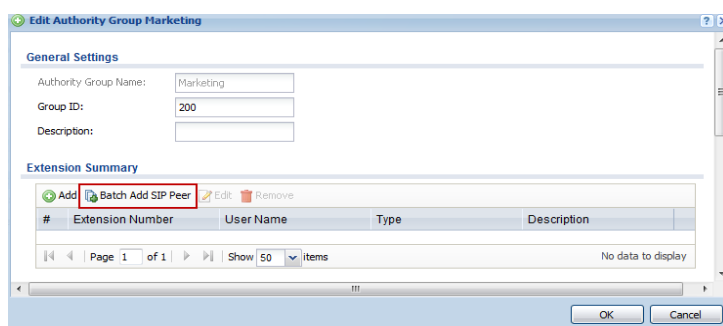
Authority Group	Group Access Code	Click To Talk
-----------------	-------------------	---------------

Authority Group Summary

 Add  Edit  Remove		
#	Name	Group ID
1	CSO	113
2	Marketing	200
3	Sales	260

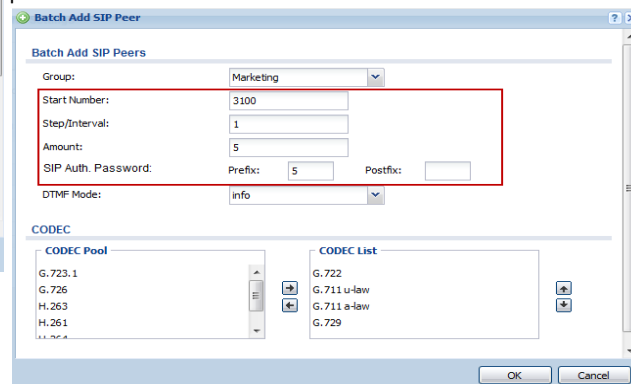


 Page 1 of 1
 

 Show 50 items

You can either add SIP peers one by one or add multiple SIP peers at a time.
Here, we add multiple SIP peers.



Define the start number and the amount of extensions.
Here, we set 3100 as the start number.

The passwords for these SIP peers are the same as the extension numbers. In order to make the password more secure, we add a prefix number to these extensions.



Extensions have been created.
Double click the extension number to check and modify the setting of the extension.

The screenshot shows the 'Edit Authority Group Marketing' window. Under the 'General Settings' tab, the 'Authority Group Name' is 'Marketing' and the 'Group ID' is '200'. The 'Extension Summary' tab shows a table with 5 extensions. Extension 3100 is highlighted.

#	Extension Number	User Name	Type	Description
1	3100		SIP	
2	3101		SIP	
3	3102		SIP	
4	3103		SIP	
5	3104		SIP	

For security reasons, you can modify the Web/VM PIN code and the password for each extension.

The screenshot shows the 'Edit Extension 3100' window. The 'Basic' tab is active. The 'Group' is 'Marketing' and the 'Type' is 'SIP'. The 'Extension Number' is '3100'. The 'Web/VM PIN Code' is '3100'. The 'SIP Auth. User Name' is '3100'. The 'SIP Auth. Password' is '53100'. Other fields like 'Department', 'First Name', 'Last Name', and 'Description' are empty.

How to configure call forwarding for each extension?

Goal to achieve: Configure call forwarding for extension 1006.

Condition:

Extension 1006

Double click the extension in the Authority Group list to configure call forwarding and call blocking rules for this extension.

The screenshot shows the 'Edit Extension 1006' configuration window with the 'Call Forward' tab selected. The 'Office Hour' section has 'Configuration' set to 'Authority Group'. The 'Call Forward' section includes several settings: 'DND(Do Not Disturb):' set to 'Disable', 'Blind Forward:' set to 'Enable', 'Extension Number:' set to '5555', 'Busy Forward:' set to 'Disable', 'No Answer Forward:' set to 'Disable', and 'After Office Hours:' set to 'Disable'. The 'Call Blocking' section has 'Black List:' set to 'Disable' and a checkbox for 'Block the calls without Caller ID' which is unchecked. A red box highlights the 'Call Forward' tab and the 'No Answer Forward:' dropdown menu, which is open showing 'Disable', 'Enable', and 'Voice Mail' options.

Edit Extension 1006

Basic **Call Forward** Voice Mail Advanced

Office Hour:

Configuration: ☒ Authority Group ☐ User Defined

Call Forward:

DND(Do Not Disturb): Disable

Blind Forward: Enable

Extension Number: 5555

Busy Forward: Disable

No Answer Forward: Disable

After Office Hours: Disable

Call Blocking

Black List: Disable

☐ Block the calls without Caller ID

Examples:

DND (Do Not Disturb): When DND is enabled on #1006 and a caller tries to reach this extension, he will hear a voice prompt that the extension is not available. The extensions configured in the “White List” can still reach #1006.

Blind Forward: When Blind Forward is enabled on #1006, every caller who tries to dial #1006 will be redirected to a pre-configured extension or voice mail.

Busy Forward: If a caller dials #1006 while #1006 has a phone call with someone, the caller will be redirected to a pre-configured extension or voice mail when Busy Forward is enabled. The definition of “Busy” is that “Call Waiting” is disabled.

No Answer Forward: A caller dials #1006 but #1006 doesn’t answer the phone. This caller will be redirected to a pre-configured extension or voice mail when the ring time of #1006 exceeds the value of Default Ring Time. The default ring time is 20 seconds. You can change the value of default ring time in CONFIGURATION > PBX > Global > SIP Server > Default Ring Time.

After Office Hours: If the incoming call is not during the office hours, you can allow the incoming call to be forwarded to a specific extension number or voice mail.

Black List: A caller’s number is on the Black List of #1006. When this caller dials #1006, he will hear the disconnect tone.

Block the calls without Caller ID: You can block the incoming calls which are without call ID.

How to receive and check the voice mail?

Goal to achieve: Extension 1006 would like to receive voicemail notification with the voice file in the email box.

Condition: Extension 1006

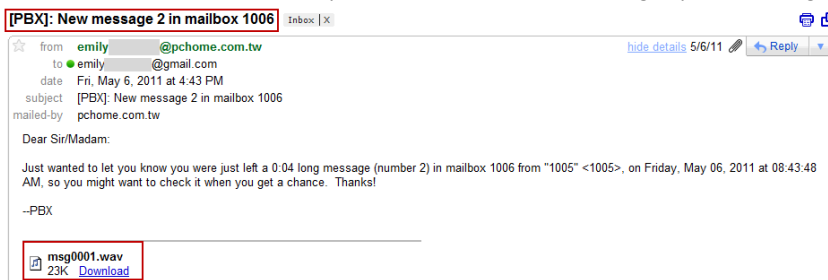
Go to CONFIGURATION > PBX > Global > E-Mail to fill in the mail server information and email account.

The screenshot shows the Asterisk PBX configuration web interface. On the left is a sidebar menu with 'CONFIGURATION' at the top, followed by 'Quick Setup' and a list of configuration categories: HTTP Redirect, ALG, IP/MAC Binding, Auth. Policy, Firewall, VPN, BWM, Anti-X, PBX, and Global. The 'Global' item is highlighted with a red box. The main content area has tabs for 'SIP Server', 'Feature Code', 'E-Mail' (which is selected and highlighted with a red box), 'FakeIP', 'Peer to Peer', and 'QoS'. Under the 'E-Mail' tab, there is a 'General Settings' section with the following fields: 'E-Mail Server' (smtp.pchome.com.tw), 'Sender' (emily@pchome.com.tw), a checked 'SMTP Authentication' checkbox, 'Username' (emily), and 'Password' (masked with dots).

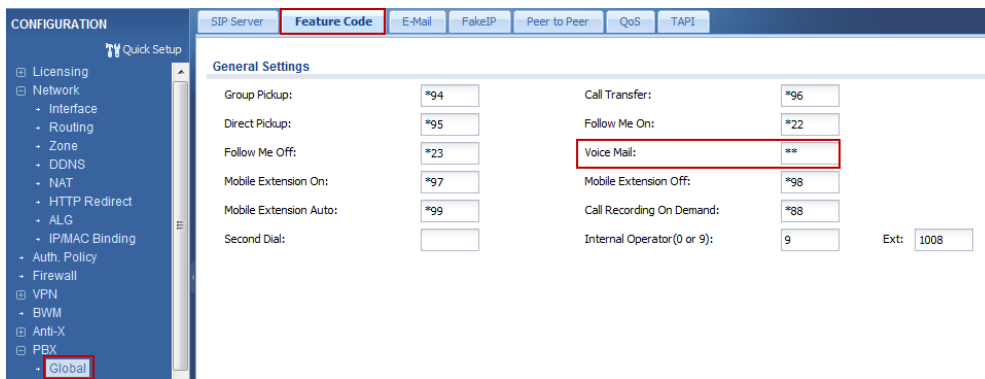
Specify the email address that you want to receive voice mail notifications of your extension.

The screenshot shows the 'Edit Extension 1006' configuration page. It has tabs for 'Basic', 'Call Forward', 'Voice Mail' (which is selected and highlighted with a red box), and 'Advanced'. In the 'Voice Mail' tab, there is a 'Receive E-mail Address' field (highlighted with a red box) containing 'emily@gmail.com'. Below this field are two checked checkboxes: 'Attached Voice File' and 'Delete Voice Message After Mailed'.

If “Attached Voice File” is selected, you can listen to the voice message by downloading the attached file in the notification mail.



If the voice message is not attached in the notification mail, you can dial the feature code and the extension number to hear the voice message. The default feature code is **. In this example, you can dial **1006 to hear the voice mail of extension 1006.



Firewall Setting

Goal to achieve: The administrator allows SIP clients to register from the WAN interface.

Condition:

Activate the firewall rule: PBX_SERVICE

Enable Firewall: checked

By default, ISG50 doesn't allow SIP clients to register from the WAN interface. You have to activate the first firewall rule "PBX_SERVICE" to let SIP clients register from the WAN interface.

FirewallSession Limit

General Settings

☒ Enable Firewall

☐ Allow Asymmetrical Route

Firewall Rule Summary

From Zone: anyTo Zone: anyRefresh

AddEditRemoveActivateInactivateMove

Status	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
1		WAN	Device	none	any	any	any	PBX_SERVICE	allow	no
2		WAN	Device	none	any	any	any	Default_Allow...	allow	no
3		WAN	Device	none	any	any	any	any	deny	log
4		WAN	any (Excluding ...	none	any	any	any	any	deny	log
5		DMZ	Device	none	any	any	any	Default_Allow...	allow	no
6		DMZ	Device	none	any	any	any	any	deny	log
7		DMZ	WAN	none	any	any	any	any	allow	no
8		DMZ	any (Excluding ...	none	any	any	any	any	deny	log

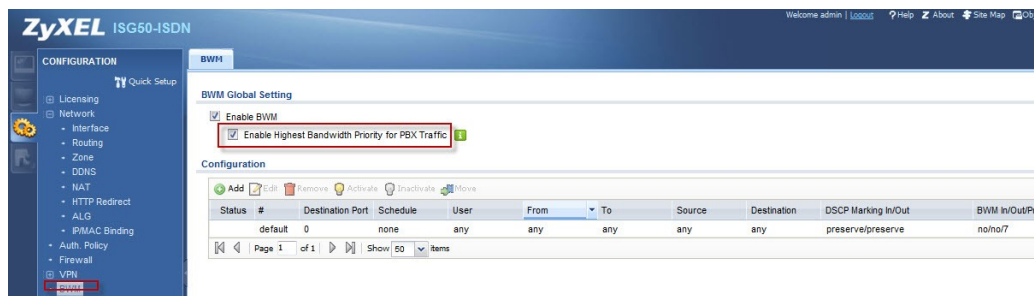
QoS

Goal to achieve: The administrator would like to let VoIP service has the highest priority over other traffic.

Condition:

Enable Highest Bandwidth Priority for PBX Traffic: checked

Check this box to ensure VoIP traffic receives the highest priority.



2. How to Manage Extensions as Business Needs Grow?

The new company recruits more employees in the following weeks and the network administrator would like to quickly deploy phone services for the new employees at their desks. The auto-provisioning feature allows administrators to configure VoIP related settings on the V310/snom SIP clients from a central location. A configuration file associated with the SIP extension on the ISG50 can be configured and maintained. Auto-provisioning allows the V310/snom phones to periodically download the configuration file from the ISG50, such as SIP account authentication, phonebook, feature keys and the phone's firmware URL.

Auto Provision



SIP Server/SIP account/Password

Goal to achieve: Configure SIP accounts on snom and V310 directly from ISG50.

Condition:

V310 **Snom**

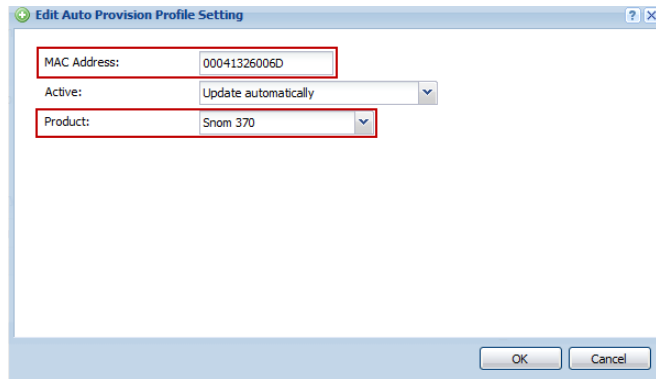
Extension: 1005 Extension: 1007

The screenshot displays the ISG50 configuration web interface. On the left is a navigation menu under the 'CONFIGURATION' header, listing various settings like IP/MAC Binding, Auth. Policy, Firewall, VPN, BWM, Anti-X, PBX, Global, Voice Interfaces, Extension Management, Outbound Line Management, Group Management, Call Service, Call Recording, Meet-me Conference, Paging Group, ACD, Sound File, **Auto Provision** (highlighted with a red box), voice mail, Phonebook, and Office Hour. The main content area has two tabs: 'Auto Provision' (selected and highlighted with a red box) and 'Auto Provision Advanced'. Under 'Auto Provision', there are two sections: 'General Settings' with a checked checkbox for 'Enable Auto Provision' (highlighted with a red box), and 'Batch XML Settings' which includes instructions for uploading a Batch XML file, a 'File Path' field with 'Browse...' and 'Upload' buttons, and an 'XML Download' button with a 'Download' button. Below these is the 'Current SIP Peer Summary' section, which contains a table of SIP peers. Above the table are buttons for 'Edit', 'Remove Config', 'Remove Customized Config', and 'View Config File'. The table has five columns: '#', 'Extension', 'MAC Address', 'Phone Type', and 'Config Exist'. It lists seven peers, with the first three (1005, 1006, 1007) highlighted in blue.

#	Extension	MAC Address	Phone Type	Config Exist
1	1005	000E43D047B8	ZyXEL_V310	yes
2	1006			no
3	1007	00041326006D	snom_370	yes
4	1008			no
5	1009			no
6	1010			no
7	1011			no

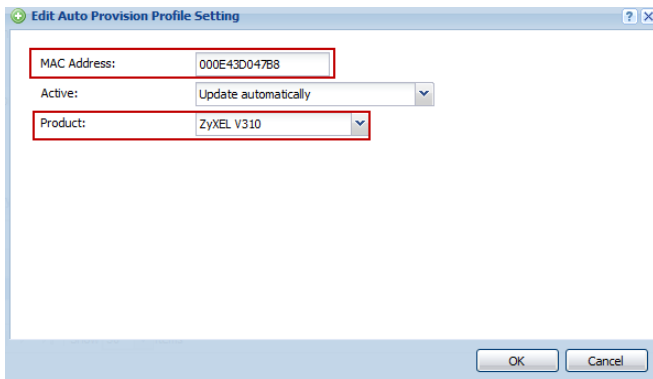
Fill in the MAC address of the IP phone and select the model name from the product list that receives configuration settings from the ISG50 for this extension.

Snom



The screenshot shows a dialog box titled "Edit Auto Provision Profile Setting". It contains three fields: "MAC Address" with the value "00041326006D", "Active" with a dropdown menu set to "Update automatically", and "Product" with a dropdown menu set to "Snom 370". The "MAC Address" and "Product" fields are highlighted with red rectangles. At the bottom right, there are "OK" and "Cancel" buttons.

V310



The screenshot shows a dialog box titled "Edit Auto Provision Profile Setting". It contains three fields: "MAC Address" with the value "000E43D047B8", "Active" with a dropdown menu set to "Update automatically", and "Product" with a dropdown menu set to "ZyXEL V310". The "MAC Address" and "Product" fields are highlighted with red rectangles. At the bottom right, there are "OK" and "Cancel" buttons.

Phone book

Goal to achieve: Download the phonebook on snom and V310 from ISG50.

Condition:

Extension number: 1005-1012; 2000-2001

Snom

The screenshot shows the 'Directory' page of a Snom system. The page has a sidebar with 'Operation' and 'Setup' sections. The 'Directory' section is active, showing a table of contacts. The table has columns for Name, Number, Contact Type, Outgoing Identity, Edit, and Delete. The contacts listed are 1005, 1006, 1007, 1008, 1009, 1010, 1011, 1012, 2001, and 2000. The 'Edit' and 'Delete' columns contain icons for editing and deleting each contact.

Name	Number	Contact Type	Outgoing Identity	Edit	Delete
1005	1005	None	Active		
1006	1006	None	Active		
1007	1007	None	Active		
1008	1008	None	Active		
1009	1009	None	Active		
1010	1010	None	Active		
1011	1011	None	Active		
1012	1012	None	Active		
2001	2001	None	Active		
Emily	2000	None	Active		

V310

The screenshot shows the 'PHONEBOOK' page of a ZyXEL V310 system. The page has a sidebar with 'CONFIGURATION' and 'PHONEBOOK' sections. The 'PHONEBOOK' section is active, showing a table of contacts. The table has columns for #, Name, Number, Domain, and Select. The contacts listed are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10. The 'Select' column contains checkboxes for each contact.

#	Name	Number	Domain	Select
1	1005	1005	192.168.1.1:5060	<input type="checkbox"/>
2	1006	1006	192.168.1.1:5060	<input type="checkbox"/>
3	1007	1007	192.168.1.1:5060	<input type="checkbox"/>
4	1008	1008	192.168.1.1:5060	<input type="checkbox"/>
5	1009	1009	192.168.1.1:5060	<input type="checkbox"/>
6	1010	1010	192.168.1.1:5060	<input type="checkbox"/>
7	1011	1011	192.168.1.1:5060	<input type="checkbox"/>
8	1012	1012	192.168.1.1:5060	<input type="checkbox"/>
9	1013	1013	192.168.1.1:5060	<input type="checkbox"/>
10	1014	1014	192.168.1.1:5060	<input type="checkbox"/>

Feature Key

Goal to achieve: Download the feature keys on snom from ISG50.

Condition:

Feature keys: Agent Login; Agent Pause; Voicemail; Group Pickup; Call Transfer; Mobile Extension On; Mobile Extension Off; Mobile Extension Auto; Call Recording on Demand; Followme On; Followme Off; Line

Configure the feature key settings for the Snom 370 connected to the ISG50. Feature keys cannot be provisioned to V310.

Auto Provision				Auto Provision Advanced	
Feature Key Settings					
P0:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Agent Login
P1:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Agent Pause
P2:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Voicemail
P3:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Group Pickup
P4:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Call Transfer
P5:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Mobile Extension On
P6:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Mobile Extension Off
P7:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Mobile Extension Auto
P8:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Call Recording On Demand
P9:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Followme On
P10:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Followme Off
P11:	Active:	<input checked="" type="radio"/> On	<input type="radio"/> Off	Type:	Line

The setting of feature keys is downloaded from ISG50. Here, key P[k] of ISG50 is mapped to key P[k+1] of Snom phone. (k is from 0 to 11)

snom
VoIP phones
© 2000-2010 [snom AG](#)

RECORD	Key Event	Retrieve
RETRIEVE	Key Event	Redial
REDIAL	Key Event	Help
HELP	Key Event	None
SNOM	Key Event	Conference
CONFERENCE	Key Event	Transfer
TRANSFER	Key Event	Hold
HOLD	Key Event	DND
DND	Key Event	Directory
DIRECTORY	Key Event	None
MENU	Key Event	
P1	Active	Extension
P2	Active	Extension
P3	Active	DTMF
P4	Active	Extension
P5	Active	DTMF
P6	Active	Extension
P7	Active	Extension
P8	Active	Extension
P9	Active	Extension
P10	Active	Extension
P11	Active	Extension
P12	Active	Extension

Firmware Upgrade

Goal to achieve: Get the firmware upgrade through the auto provision from the URL configured in ISG50.

Condition:

Firmware URL:

Snom <http://59.124.163.151/FW/snom370-8.4.32-SIP-f.bin>

V310 http://10.59.1.37/V310_1.00AABT.0B5

Snom

Configure firmware upgrade URLs for the Snom 370.

Visit <http://wiki.snom.com/Firmware> to find the latest firmware version.

You can either fill in the firmware download link (<http://provisioning.snom.com/download/fw/snom370-8.4.32-SIP-f.bin>) or put the firmware on another web server.



snom
VoIP phones

knowledgebase

- » Main Page
- » Search/Suche
- » FAQ
- » Glossary

VoIP Products

- » IP phones
- » DECT phones
- » Conference phones

Firmware/V8/3x0

< Firmware | V8
Languages: English • Deutsch

V8.4

1. Check the **feature list of Version 8.4.32** carefully!
2. Check the **release notes for version 8.4.32** carefully!
3. Check the **change log for firmware branch 8.X** carefully!
4. Perform the **update from V8.X to Version 8.4.32** following the steps below:

❗ Right-click on the following link and choose **Copy shortcut**:

[snom300 8.4.32](#) [snom320 8.4.32](#) [snom360 8.4.32](#) [snom370 8.4.32](#)

Please note that snom phones only support HTTP firmware update, so the URL link must be in the format of **http://IP_address/FW_version.bin**

The screenshot shows the ZyXEL ISG50-ISDN configuration interface. The left sidebar contains a 'CONFIGURATION' menu with options like Auth. Policy, Firewall, VPN, BWM, Anti-X, PBX, Global, Voice Interfaces, Extension Management, Outbound Line Management, Group Management, Call Service, Call Recording, Meet-me Conference, Paging Group, ACD, Sound File, Auto Provision (highlighted), Voice Mail, Phonebook, and Office Hour. The main content area has two tabs: 'Auto Provision' and 'Auto Provision Advanced' (highlighted). Under 'Auto Provision Advanced', there are settings for P8, P9, P10, and P11, each with an 'Active' radio button (set to 'On') and a 'Type' dropdown menu. Below this is the 'Firmware Upgrade File Location Settings' section, which contains a table with columns for device type and URL. The entry for 'snom_370' is highlighted with a red box, showing the URL 'http://59.124.163.151/FW/snom370-8.4.32-SIP-f.bin'.

Device Type	URL
snom_300:	
snom_320:	
snom_360:	
snom_370:	http://59.124.163.151/FW/snom370-8.4.32-SIP-f.bin
snom_820:	
snom_870:	
snom_m3:	
ZyXEL_V311:	

You can log into the GUI of Snom 370 to check if the firmware has been upgraded to target version.

System Information

VERSION 8

Operation

Home

Directory

Setup

Preferences

Speed Dial

Function Keys

Advanced

Certificates

Status

System Information

Log

SIP Trace

DNS Cache

Subscriptions

PCAP Trace

Memory

Manual

System Information:

Phone Type: snom370-SIP

MAC-Address: 00041326006D

IP-Address: 10.5.5.10

Firmware-Version: snom370-SIP 8.4.32

Firmware-URL: <http://59.124.163.151/FW/snom370-8.4.32-SIP-f.bin>

Production Information: Mac:00041326006D;Version:Standard;Hardware:snom370 (MB V33_1159,KB V33_1160);Date:29/01/07;Copyright(C) snom technology AG

Uptime: 0 days, 0 hours, 18 minutes

LCS: 0 days, 0 hours, 18 minutes (0)

Memfree: 13088 K

CPU: 0.05 0.06 0.00 1/10 29

Bootloader-Version: 1.1.3-s

SIP Identity Status:

Identity 1 Status: 1007@10.5.5.1:5060: OK

Identity 2 Status: 100112@zyisg.no-ip.biz:9998: Network Failure

Identity 3 Status: 5566002@10.1.4.83: Network Failure

Identity 4 Status: 100100@zypbx.no-ip.info: Network Failure

Identity 5 Status: 200100@zypbx.no-ip.biz: Network Failure

Identity 6 Status: 200103@zypbx.no-ip.biz: Network Failure

Identity 7 Status: 200104@zypbx.no-ip.biz: Network Failure


Identity 8 Status: 1007@10.5.5.1: OK

Identity 9 Status:

Identity 10 Status:

Identity 11 Status:

Identity 12 Status:



V310

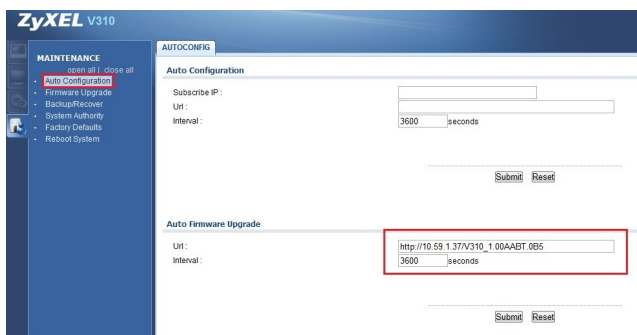
Fill in the firmware download URL.

The screenshot shows the ZyXEL ISG50-PSTN configuration interface. The left sidebar contains a 'CONFIGURATION' menu with options like Licensing, Network, Auth. Policy, Firewall, VPN, BWM, Anti-X, PBX, Global, Voice Interfaces, Extension Management, Outbound Line Management, Group Management, Call Service, Call Recording, Meet-me Conference, Paging Group, ACD, Sound File, Auto Provision, Voice Mail, Phonebook, Office Hour, Object, System, and Log & Report. The 'Auto Provision' tab is selected, and the 'Auto Provision Advanced' sub-tab is active. The main area displays a table of settings for ports P4 through P11, including 'Active' status (On/Off) and 'Type' (Followme Off, Agent Login, Agent Pause, Mobile Extension On, None). Below this, the 'Firmware Upgrade File Location Settings' section contains input fields for various snom_* and ZyXEL_* parameters. The 'ZyXEL_V310:' field is highlighted with a red box and contains the URL 'http://10.59.1.37/V310_1.00AABT.085'. 'Apply' and 'Reset' buttons are at the bottom right.

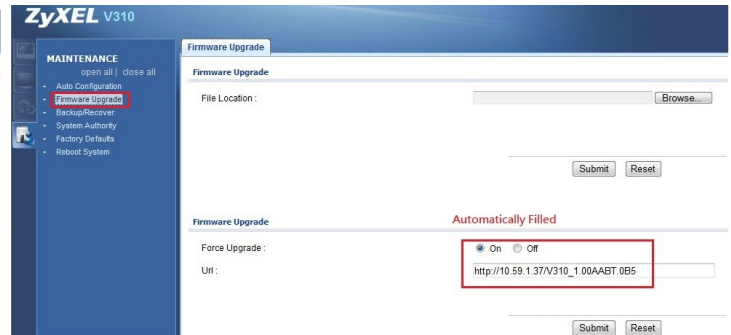
Port	Active	Type
P4:	On	Followme Off
P5:	On	Agent Login
P6:	On	Agent Pause
P7:	On	Mobile Extension On
P8:	Off	None
P9:	Off	None
P10:	Off	None
P11:	Off	None

Parameter	Value
snom_300:	
snom_320:	
snom_360:	
snom_370:	
snom_820:	
snom_870:	
snom_m3:	
ZyXEL_V310:	http://10.59.1.37/V310_1.00AABT.085
ZyXEL_V510:	

V310 will receive the firmware upgrade path through auto provision. Blanks in “Auto Configuration” and “Firmware Upgrade” tabs will be automatically filled with an HTTP IP address.



The image shows the ZyXEL V310 web interface with the 'AUTOCONFIG' tab selected. The 'Auto Configuration' section has fields for 'Subscribe IP' (empty), 'URL' (empty), and 'Interval' (3600 seconds). The 'Auto Firmware Upgrade' section has fields for 'URL' (filled with 'http://10.59.1.37/V310_1.00AABT.0B5') and 'Interval' (3600 seconds). Both sections have 'Submit' and 'Reset' buttons.

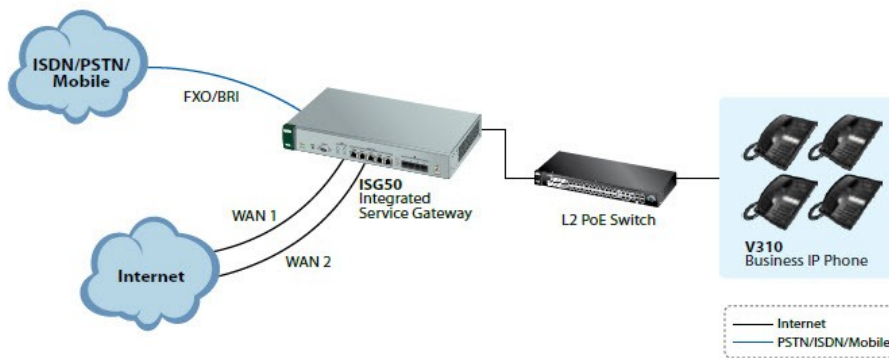


The image shows the ZyXEL V310 web interface with the 'Firmware Upgrade' tab selected. The 'Firmware Upgrade' section has a 'File Location' field (empty) and a 'Browse...' button. The 'Auto Firmware Upgrade' section has a 'Force Upgrade' checkbox (checked) and a 'URL' field (filled with 'http://10.59.1.37/V310_1.00AABT.0B5'). Both sections have 'Submit' and 'Reset' buttons.

3. How to Develop a Non-stop Voice Service?

The interruption of non-stop voice service is often a concern of the employees because interrupted service may cause the company to suffer from business losses and a bad reputation. With the dual WAN design of the ISG50, the company can connect up to two ISPs via Ethernet or PPPoE connections to avoid VoIP service breakdowns. In addition, the ISG50 not only offers voice services through the ITSP by a SIP trunk, but also via a PSTN/ISDN connection to ensure continuous voice services. Furthermore, in case where the WAN IP address is dynamic, the SIP server address can be automatically updated with the DDNS function so that the mobile clients can register with the ISG50 using the domain name.

WAN failover



Goal to achieve:

VoIP traffic goes out primarily through WAN1. In case WAN1 is down, it will go out via WAN2.

Condition:

Primary: WAN1; Backup: WAN2

Add WAN trunk for VoIP traffic - Set WAN1 as Active mode, and set WAN2 as Passive mode.

Configuration > Network > Interface > Trunk > User Configuration > Add

Name: VoIP_Trunk

Load Balancing Algorithm: Least Load First

Load Balancing Index(es): Outbound

#	Member	Mode	Egress Bandwidth
1	wan1	Active	1048576 kbps
2	wan2	Passive	1048576 kbps

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

OK Cancel

Apply this new trunk in **Default Trunk Selection for System Service Traffic**.

Port Role | Ethernet | PPP | Cellular | VLAN | Bridge | **Trunk**

Show Advanced Settings

Configuration

☐ Enable Link Sticking ⓘ
Timeout: (30-600 seconds) ⓘ

☐ Passive Connection Disconnect ⓘ

Default WAN Trunk

Default Trunk Selection for Forwarding Traffic

☒ SYSTEM_DEFAULT_WAN_TRUNK
☐ User Configured Trunk

Default Trunk Selection for System Service Traffic

☐ SYSTEM_DEFAULT_WAN_TRUNK
☒ User Configured Trunk

Use **SYSTEM_DEFAULT_WAN_TRUNK** to do load balancing for data traffic.

System Default

Edit: Object Reference

#	Name	Algorithm
1	SYSTEM_DEFAULT_WAN_TRUNK	lbf

Page 1 of 1 | Show 50 items

VoIP survivability

Goal to achieve: If the connection from ISTP is lost, clients can still make calls through BRI trunk.

Condition:

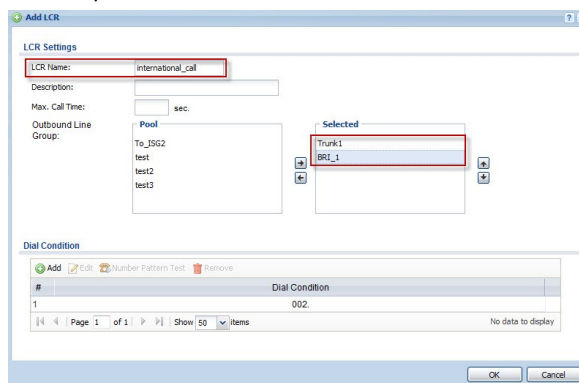
For international calls,

Primary trunk: SIP trunk; Secondary trunk: BRI trunk

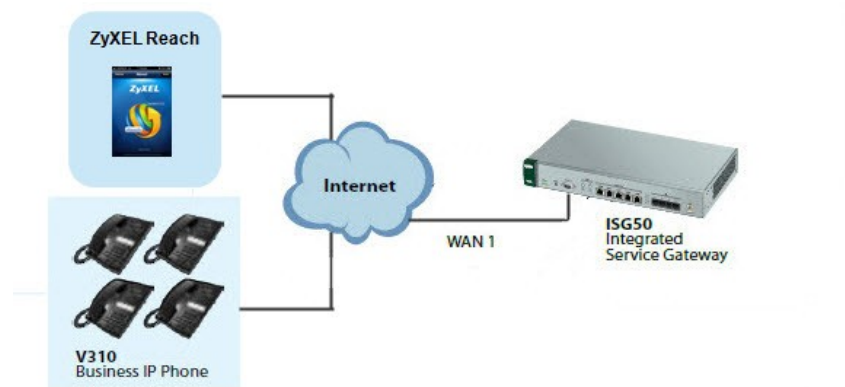
In the LCR, move multiple outbound line groups to the **Selected** column for making calls out.

Use the **Up** and **Down** buttons to specify the priority of the outbound line groups.

In this example, for the LCR “international_call”, select SIP trunk (Trunk1) as the first priority outbound line and BRI trunk (BRI_1) as the secondary outbound line.



DDNS



Goal to achieve: IP Phone and mobile client can register to ISG50 with the domain name in case the IP of WAN1 is dynamic.

Condition:

DDNS service provider: DynDNS

DDNS interface: WAN1

Fill in DDNS account information.

[Edit Profile ISG_DDNS](#)
[Show Advanced Settings](#)

General Settings

☒ Enable DDNS Profile

Profile Name: ISG_DDNS

DDNS Type: DynDNS

DDNS Account

Username: lattepat

Password:

DDNS Settings

Domain name: isgipserver.dyndns.org

Primary Binding Address

Interface: wan1

IP Address: Interface

Backup Binding Address

Interface: none

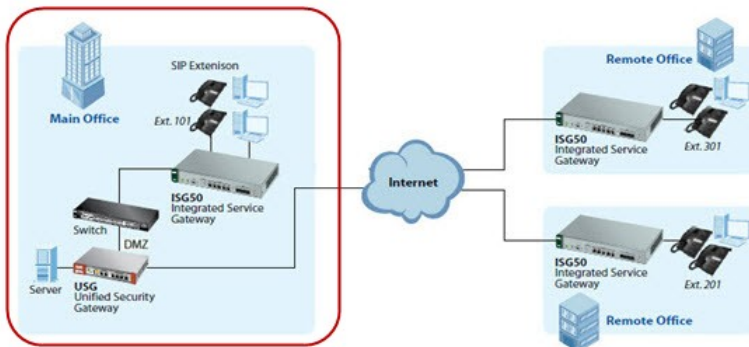
Activate DDNS.

DDNS						
Profile Summary						
Add Edit Remove Activate Inactivate						
#	Status	Profile Name	DDNS Type	Domain Name	Primary Interface/IP	Backup Interface/IP
1		ISG_DDNS	DynDNS	isgipserver.dyndns.org	wan1/from interface	none

4. How to Expand the Current Networking Infrastructure to Fulfill Multi-site Requirements?

Since the company is growing, it is planning to setup two branch offices. The network administrator would like to expand the current networking infrastructure to fulfill the requirements of multiple sites. In order to allow the main office and the branch offices to make calls to each other more easily, the administrator needs to establish a trusted peer between two ISGs located in two offices. Furthermore, to reduce the cost of outbound line deployments in the remote offices, the extensions must make calls out through the BRI trunk of the main office. Moreover, the incoming calls on the BRI trunk can reach the extensions of the remote offices over a trusted peer with LCR and group management settings. The network administrator deploys the ZyWALL USG product to offer robust protection and uses the ISG50 as a pure VoIP service.

Work with ZyWALL USG products



Goal to achieve:

Connect the ISG50 to the DMZ of the ZyWALL. The USG provides security services and the ISG50 acts as a pure IP PBX to provide VoIP services. IP phones from the Internet can register to ISG50 through USG's WAN IP.

Condition:**USG:**

- WAN IP: 59.124.163.156
- SIP server IP (ISG50): 172.16.1.10

ISG50:



- WAN IP: 172.16.1.10

USG:

Step 1. Click **CONFIGURATION > Network > Interface > Ethernet** to assign a WAN IP to USG.

The screenshot shows the 'Edit Ethernet' configuration window. The 'General Settings' section has 'Enable Interface' checked. The 'Interface Properties' section shows 'Interface Type' as 'external', 'Interface Name' as 'wan1', 'Port' as 'P1', and 'Zone' as 'WAN' (highlighted with a red box). The 'IP Address Assignment' section has 'Use Fixed IP Address' selected (highlighted with a red box), with 'IP Address' set to '59.124.163.156', 'Subnet Mask' as '255.255.255.224', and 'Gateway' as '59.124.163.129' (highlighted with a red box). The 'Metric' is set to '0'.

Step 2. Assume ISG50's WAN port is connected to DMZ (port 5) of USG.
Configure an IP for this interface.

General Settings	
<input checked="" type="checkbox"/> Enable Interface	
Interface Properties	
Interface Type:	internal
Interface Name:	dmz
Port:	P5
Zone:	DMZ
MAC Address:	50:67:F0:66:61:B6
Description:	<input type="text"/> (Optional)
IP Address Assignment	
IP Address:	172.16.1.1
Subnet Mask:	255.255.255.0
Interface Parameters	
Egress Bandwidth:	<input type="text" value="1048576"/> Kbps 
DHCP Setting	
DHCP:	<input type="text" value="DHCP Server"/> 
IP Pool Start Address (Optional):	<input type="text" value="172.16.1.5"/> Pool Size: <input type="text" value="200"/>

Step 3. For NAT setting, the user needs to configure the following:

- Rule's name.
- Set Virtual Server type to let USG do packet forwarding.
- Fill in the **Original IP** (WAN IP) address.
- Fill in the **Mapped IP** (ISG's IP) address.
- Configure the **Original Port** and the **Mapped Port**; here we set the SIP signaling port 5060 and RTP port range 10000-20000. Make sure these port settings are the same as those set in ISG50.

The screenshot shows the ZyXEL ZyWALL USG 20W configuration interface. The left sidebar contains the 'CONFIGURATION' menu with options like Licensing, Network, Interface, Routing, Zone, DDNS, NAT (selected), HTTP Redirect, ALG, IP/MAC Binding, Auth. Policy, and Firewall. The main area is titled 'NAT' and 'Configuration'. A note states: 'Note: If you want to configure SNAT, please go to Policy Route.' Below this is a table of NAT rules. Two rules are listed, both highlighted with a red border:

#	Status	Name	Mapping Type	Interface	Original IP	Mapped IP	Protocol	Original Port	Mapped Port
1	On	ISG1	Virtual Server	wan1	59.124.163.156	172.16.1.10	any	5060	5060
2	On	ISG2	Virtual Server	wan1	59.124.163.156	172.16.1.10	any	10000-20000	10000-20000

At the bottom of the table, it says 'Page 1 of 1', 'Show 50 items', and 'Displaying 1 - 2 of 2'.

Step 4. The user can create an address object for ISG50 for further configuration usage. Click **Create new object** for this function.

The screenshot shows the ZyWALL USG 20W configuration interface. The left sidebar contains a navigation menu with options like 'Quick Setup', 'Interface', 'Routing', 'Zone', 'DDNS', 'NAT', 'HTTP Redirect', 'ALG', 'P/MAC Binding', 'Policy', 'Wall', and 'M'. The main content area is titled 'Configuration' and has tabs for 'Address' and 'Address Group'. The 'Address' tab is active, displaying a table of configured address objects. The table has columns for '#', 'Name', 'Type', and 'Address'. The following table represents the data shown in the screenshot:

#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
3	LAN2_SUBNET	INTERFACE SUBNET	lan2-172.16.1.0/24
4	SIPSERVER	HOST	172.16.1.10
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and a 'Show 50 items' dropdown.

Step 5. Click **CONFIGURATION > Network > Firewall** to open the firewall configuration screen.

Click on the Add button to create a firewall rule to enable the VoIP service to pass from the WAN to DMZ.

ZyWALL USG 20W

Welcome admin | [Logout](#) ? Help Z About Site Map Object Reference Console

Firewall Session Limit

General Settings

☒ Enable Firewall

☐ Allow Asymmetrical Route

Firewall Rule Summary

From Zone: any To Zone: any Refresh

Add Edit Remove Activate Inactivate Move

Status	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
	1	WAN	DMZ	none	any	any	SIPSERVER	any	allow	no
	2	any	ZyWALL	none	any	any	any	any	allow	no
	3	any	any (Excluding Z...	none	any	any	any	any	allow	no
	4	WAN	ZyWALL	none	any	any	any	Default_Allow_...	allow	no
	5	WAN	ZyWALL	none	any	any	any	any	deny	log
	6	WAN	any (Excluding Z...	none	any	any	any	any	deny	log
	7	DMZ	ZyWALL	none	any	any	any	Default_Allow_...	allow	no
	8	DMZ	ZyWALL	none	any	any	any	any	deny	log
	9	DMZ	WAN	none	any	any	any	any	allow	no
	10	DMZ	any (Excluding Z...	none	any	any	any	any	deny	log

Step 6. Disable SIP ALG.

The screenshot shows the ZyXEL ZyWALL USG 20W configuration interface. On the left is a 'CONFIGURATION' sidebar with a 'Quick Setup' icon and a tree view containing 'Licensing', 'Network', and 'ALG' (which is selected). The main area is titled 'ALG' and contains 'SIP Settings'. A red rectangle highlights the 'Enable SIP ALG' checkbox, which is currently unchecked. Below this, there are several checked options: 'Enable SIP Transformations' and 'Enable Configure SIP Inactivity Timeout'. Further down are input fields for 'SIP Media Inactivity Timeout' (120 seconds), 'SIP Signaling Inactivity Timeout' (1800 seconds), 'SIP Signaling Port' (5060), and 'Additional SIP Signaling Port(UDP) for Transformations' (empty).

ZyXEL ZyWALL USG 20W

CONFIGURATION

- Quick Setup
- Licensing
- Network
 - Interface
 - Routing
 - Zone
 - DDNS
 - NAT
 - HTTP Redirect
 - ALG**
 - IP/MAC Binding
 - Auth. Policy

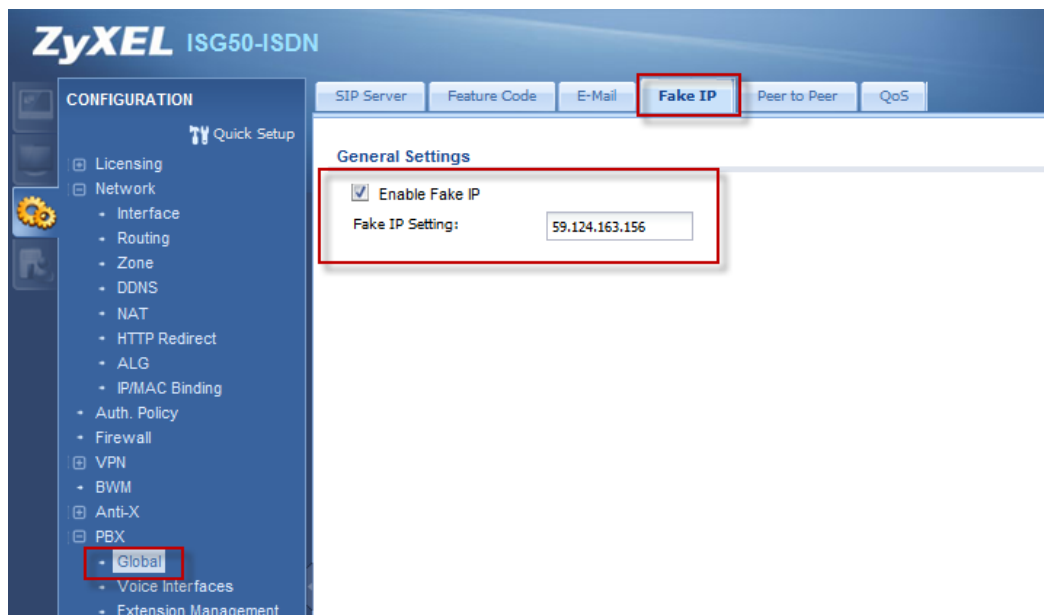
ALG

SIP Settings

- ☐ **Enable SIP ALG**
- ☒ Enable SIP Transformations
- ☒ Enable Configure SIP Inactivity Timeout
- SIP Media Inactivity Timeout : (seconds)
- SIP Signaling Inactivity Timeout : (seconds)
- SIP Signaling Port: (1025-65535)
- Additional SIP Signaling Port(UDP) for Transformations : (1025-65535) (Optional)

ISG50:

Step 1. Set the WAN IP of USG in the Fake IP field.



Step 2. Make sure the SIP signaling port and the RTP port range are the same as those you configured in the port forwarding in USG.

The screenshot displays the ZyXEL ISG50-ISDN configuration interface. The left sidebar shows the 'CONFIGURATION' menu with 'PRX' expanded and 'Global' selected. The main content area is titled 'SIP Server' and contains 'General Settings'. The 'Port' field is set to 5060. The 'RTP Port Range' is set from 10000 to 20000. Other settings include 'SIP Server Realm Name' (default), 'Default SIP Client Registration Expiration' (NAT: 60, Non-NAT: 3600), 'Default Ring Time' (20), 'Enable Personal AA' (checked for external call), 'Enable Session Timer' (unchecked), 'Minimum SE' (90), 'Session Expires' (1800), 'Enable RTCP Support' (checked), and 'Enable DNS SRV' (unchecked).

ZyXEL ISG50-ISDN Welcome admin | [Logout](#) ?

CONFIGURATION **Quick Setup**

- ▢ Licensing
- ▢ Network
 - Interface
 - Routing
 - Zone
 - DDNS
 - NAT
 - HTTP Redirect
 - ALG
 - IP/MAC Binding
- Auth. Policy
- Firewall
- ▢ VPN
- BWM
- ▢ Anti-X
- ▢ PRX
 - **Global**
 - Voice Interfaces
 - Extension Management

SIP Server Feature Code E-Mail FakeIP Peer to Peer QoS

General Settings

SIP Server Realm Name: default

Port: 5060

Default SIP Client Registration Expiration: NAT: 60 (60~86400)Sec. Non-NAT: 3600 (60~86400)Sec.

RTP Port Range: 10000 ~ 20000

Default Ring Time: 20 (1~300)Sec.

Enable Personal AA: ☒ From external call ☐ From internal call

☐ Enable Session Timer

Minimum SE: 90 Sec. (90 ~ 1800)

Session Expires: 1800 Sec. (90 ~ 86400, must > Minimum SE)

☒ Enable RTCP Support

☐ Enable DNS SRV

Step 3. Disable the firewall in ISG50 since USG acts as firewall.

ZyXEL ISG50-1SDN Welcome admin | Logout | ? Help | About | Site Map | Object Reference | Console

CONFIGURATION Quick Setup

- Licensing
- Network
 - Interface
 - Routing
 - Zone
 - DDNS
 - NAT
 - HTTP Redirect
 - ALG
 - IP/MAC Binding
- Auth. Policy
- Firewall**
- VPN
- BWM
- Anti-X
- PBX
 - Global
 - Voice Interfaces
 - Extension Management
 - Outbound Line Management
 - Group Management
 - Call Service
 - Call Recording
 - Meet-me Conference
 - Paging Group

Firewall Session Limit

General Settings

☒ **Enable Firewall**

☐ Allow Asymmetrical Route

Firewall Rule Summary

From Zone: any To Zone: any Refresh

Status	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
1	1	LAN2	any (Excluding D...	none	any	any	any	any	allow	no
2	2	any	Device	none	any	any	any	TELNET	allow	log
3	3	WAN	Device	none	any	any	any	Default_Allow...	allow	no
4	4	WAN	Device	none	any	any	any	any	deny	log
5	5	WAN	any (Excluding D...	none	any	any	any	any	deny	log
6	6	DMZ	Device	none	any	any	any	Default_Allow...	allow	no
7	7	DMZ	Device	none	any	any	any	any	deny	log
8	8	DMZ	WAN	none	any	any	any	any	allow	no
9	9	DMZ	any (Excluding D...	none	any	any	any	any	deny	log
Default		any	any	none	any	any	any	any	allow	no

Page 1 of 1 Show 50 items Displaying 1 - 10 of 10

Trusted Peer & SIP trunk



Goal to achieve:

Add a SIP trunk and a BRI trunk in the main office and establish trusted peer between two ISGs located in the main office and the remote office so that the extensions of two offices can make call to each other.

Furthermore, extensions of remote office can make call out through BRI trunk of the main office.

The incoming call on BRI trunk can be reached to the extension of the remote office over trusted peer.

Condition:

ISG50-1 (Main Office):

WAN IP: 59.124.163.156

Extension format: 4 digit

Prefix number before dialing to the remote office: 49

ISG50-2 (Remote Office):

WAN IP: 59.124.163.147

Extension format: 4 digit

Prefix number before dialing to the main office: 48

In outbound trunk setting, add a new trust peer in each ISG50 and set the remote WAN IP address as the trusted SIP server address.

ISG50-1 (Main Office):

ISG50-2 (Remote Office):

ISG50-1 (Main Office):

CallerID Setting

CallerID Viewers: From: "Extension" <Extension@server IP>

Representative Number: 5783945

CallerID Name & Number:

☒ Extension + Extension

☐ Extension + Representative Num

☐ Representative Num + Representative Num

☐ Extension + Representative Num (DDIVD mapped)

☐ Representative Num (DDIVD mapped) + Representative Num (DDIVD mapped)

☐ The Extension Prefix

CODEC Setting

CODEC Pool	CODEC List
G.726	G.711 u-law
G.723	G.711 a-law
H.263	G.729
H.261	G.722
M.264	

ISG50-2 (Remote Office):

CallerID Setting

CallerID Viewers: From: "Extension" <5783946@server IP>

Representative Number: 5783946

CallerID Name & Number:

☐ Extension + Extension

☒ Extension + Representative Num

☐ Representative Num + Representative Num

☐ Extension + Representative Num (DDIVD mapped)

☐ Representative Num (DDIVD mapped) + Representative Num (DDIVD mapped)

☐ The Extension Prefix

CODEC Setting

CODEC Pool	CODEC List
G.726	G.711 u-law
G.723	G.711 a-law
H.263	G.729
H.261	G.722
M.264	

SIP Trunk - Advanced setup

General Settings

Trunk Name: SIP_trunk_1
Description:
Representative Number: 0701234567
SIP Proxy Server Address: 59.124.163.151
SIP Proxy Server Port: 5060
SIP Register Server Address: 59.124.163.151
SIP Register Server Port: 5060
Service Domain: ☒ Disable ☐ Define Service Domain:
Outbound Proxy: ☒ Disable ☐ Define Outbound Proxy:
Outbound Proxy Port: 5060
DTMF Mode: info
☐ Enable Privacy
Proxy Require: (Optional.)
Channel Limit: 8 Range (1~128)

Session Timer

☐ Enable Session Timer
Minimum Session Expiration: 90 Sec (90 ~ 1800)
Session Expires: 1800 Sec (90 ~ 86400, must greater then Minimum Session Expiration)

CallerID Setting

CallerID Viewer: From: "Extension" <0701234567@server IP>
CallerID Name & Number:

- ☐ Extension + Extension
- ☒ Extension + Representative Num
- ☐ Representative Num + Representative Num
- ☐ Extension + Representative Num (DD/VID mapped)
- ☐ Representative Num (DD/VID mapped) + Representative Num (DD/VID mapped)

☐ The Extension Prefix CSO

Authentication

User Name: qazwsx
Password: *****

CODEC Setting

CODEC Pool

G.726
G.723
H.263
H.261
H.264

☒
☒

CODEC List

G.722
G.711 u-law
G.711 a-law
G.729

☒
☒

You can check if the registration status is **online** through MONITOR > PBX > SIP Trunk.

SIP Trunk

General Settings

Registration Status:

all

Query

 Refresh Interval:

5

 sec

Apply

SIP Trunk Summary

#	Group Name	Reg. Number	Host	Port	Registration Status	Call Status
1	SIP_trunk_1	0701234567	59.124.163.151	5060	online	idle

Page 1 of 1

Show 50 items

Displaying 1 - 1 of 1

Add BRI trunk in ISG50-1 (Main Office).

Go to CONFIGURATION > PBX > Outbound Line Management > Outbound Trunk Group > BRI Settings.

Here, we use DDI/DID as the AA option.

Edit BRI

General Settings

Trunk Name: BRI_1

Description:

Option: ☒ DDI/DID ☐ AA ☐ Direct ☐ MSN

Interface

Directory Number: 5781111

Available Interface

Port 2
Port 3
Port 4

Used Interface

Port 1

DDI/DID Mapping Setting

DDI/DID Mask: 0

Add Remove

#	DDI/DID Number	Extension Number
---	----------------	------------------

Page 1 of 1 Show 50 items No data to display

Outgoing Calling Party Number

Prefix:

Calling Party Number: DDI/DID or Directory Number (if not match DDI)

☐ Hide Calling Party Number

Configure the LCR in both ISG50-1 (Main Office) and ISG50-2 (Remote Office) to let the extensions of ISG50-1 (Main Office) and ISG50-2 (Remote Office) make call to each other over **Trusted Peer**.

In this example, for extensions in ISG50-1 (Main Office), they need to dial 49XXXX to reach extensions in ISG50-2 (Remote Office). For extensions in ISG50-2 (Remote Office), they need to dial 48XXXX to reach extensions in ISG50-1 (Main Office).

LCR for ISG50-1 (Main Office)

LCR Settings

LCR Name: To_trust_peer

Description:

Max. Call Time: sec.

Outbound Line Group: Pool

SIP_trunk_1

BRI_line

Selected

trust1

Dial Condition

#	Dial Condition
1	49XXXX

LCR for ISG50-2 (Remote Office)

LCR Settings

LCR Name: To_trust_peer

Description:

Max. Call Time: sec.

Outbound Line Group: Pool

SIP_trunk_1

BRI_line

Selected

trust1

Dial Condition

#	Dial Condition
1	48XXXX

Edit Dial Condition

Dial Condition Setting

LCR Name: To_trust_peer
Dial Condition: 49XXXX

Dial Parameter

Edit
Dial Number View

#	Channel	Offset	Length	Prefix	Postfix	D
1	trust1	2				

Edit Dial Condition

Dial Condition Setting

LCR Name: To_trust_peer
Dial Condition: 48XXXX

Dial Parameter

Edit
Dial Number View

#	Channel	Offset	Length	Prefix	Postfix	D
1	trust1	2				

Configure **Group Management** in both ISG50-1 (Main Office) and ISG50-2 (Remote Office).
Associate AGs with LCR.

Accessible Group Summary: AG1

#	Group Name	Description	Group Type	Association
1	CSO		Authority Group	<input checked="" type="checkbox"/>
2	johnnytest		Authority Group	<input checked="" type="checkbox"/>
3	AG1		Authority Group	<input checked="" type="checkbox"/>
4	AG2		Authority Group	<input checked="" type="checkbox"/>
5	To_SIP_Trunk		LCR	<input checked="" type="checkbox"/>
6	To_trust_peer		LCR	<input checked="" type="checkbox"/>

Page 1 of 1
Show 50 items
Displaying 1 - 6 of 6

The incoming call on BRI trunk can reach the extension of ISG50-2 (Remote Office) over trusted peer.

Configure LCR in ISG50-2 (Remote Office).

Here, since the call not only reaches the extension of ISG50-1 (Main Office) but also goes out through the BRI trunk, we set **"46XXX."** as the dial condition instead of **"46XXXX"**.

Edit LCR

LCR Settings

LCR Name: To_trust_peer

Description:

Max. Call Time: sec.

Outbound Line Group:

Pool

Selected

To_ISG1

Dial Condition

#	Dial Condition
1	46XXX.

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Configure the Group management in ISG50-2 (Remote Office).

52

In ISG50-1 (Main Office), to let extensions of ISG50-2 (Remote Office) make call out through ISG50-1 (Main Office)'s BRI trunk, we need to associate the outbound line (trusted peer) with the LCR.

Group Management

Group Summary

Edit

#	Group Type	Group Name
1	Authority Group	CSO
2	BRI Trunk	BRI_1
3	Trusted	To_ISG2

Page 1 of 1 | Show 50 items

Accessible Group Summary : To_ISG2


#	Group Name	Description	Group Type	Association
1	CSO		Authority Group	<input checked="" type="checkbox"/>
2	trust1		LCR	<input type="checkbox"/>
3	BRI_Out		LCR	<input checked="" type="checkbox"/>

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

In ISG50-1 (Main Office), to let the incoming call on BRI trunk reach the extension of ISG50-2 (Remote Office) over trusted peer, we need to associate the outbound line (BRI trunk) with the LCR.

Group Management

Group Summary

 Edit

#	Group Type	Group Name
1	Authority Group	CSO
2	BRI Trunk	BRI_1
3	Trusted	To_ISG2

Page 1 of 1 | Show 50 items

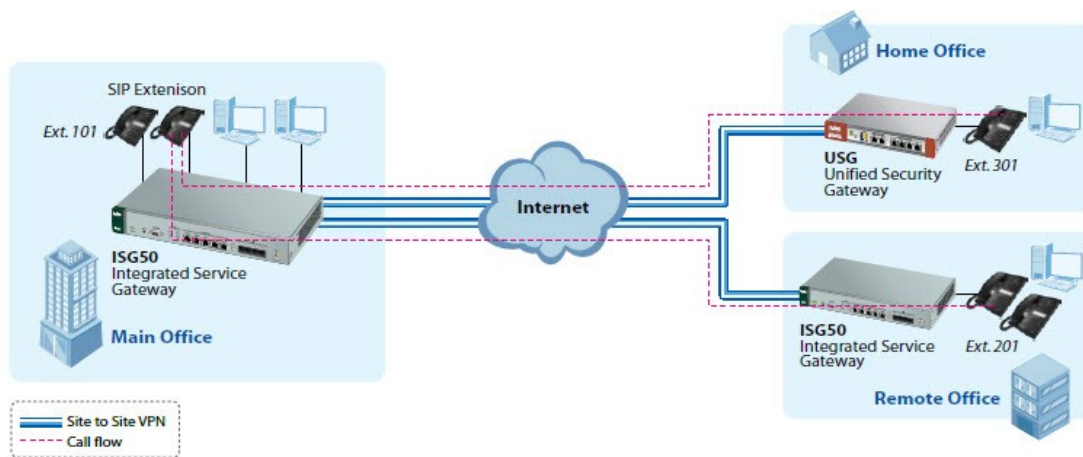
Accessible Group Summary : BRI_1

#	Group Name	Description	Group Type	Association
1	CSO		Authority Group	<input checked="" type="checkbox"/>
2	trust1		LCR	<input checked="" type="checkbox"/>
3	BRI_Out		LCR	<input type="checkbox"/>

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

5. How to Secure the Communication?

The company plans to setup a new branch office and the network administrator would like to secure the communications within the company's network. The ISG50 offers an IPSec VPN feature to establish secure tunnels for data and voice communications across the Internet. This allows employees in the branch offices or home offices to access the company's network in the same secure way as those who work in the main office. To protect against brute-force or password-guessing attacks, the network administrator can enable the brute force protection function to block access to certain accounts for a period of time after multiple consecutive failed login attempts.



Site to site IPsec VPN

Goal to achieve:

Build up the IPsec VPN tunnel between two ISGs located in the main office and the remote office.

Condition:

ISG as a multisite VPN & VoIP connectivity hub

ISG50-1 (Main Office):

WAN IP: 59.124.163.156

LAN IP: 10.5.5.1

Local subnet: 10.5.5.0/24

ISG50-2 (Remote Office):

WAN IP: 59.124.163.147

LAN IP: 192.168.2.1

Local subnet: 192.168.2.0/24

IPsec VPN

Phase 1:

Pre-Shared Key: 11111111

Negotiation mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

Key Group: DH1

Phase 2:

Active Protocol: ESP

Encapsulation Mode: Tunnel

Encryption Algorithm: DES

Authentication Algorithm: SHA1

Perfect Forward Secrecy (PFS): None

ISG50-1 (Main Office):

Add a VPN gateway rule.

Edit VPN Gateway ISG50-2

☐ Hide Advanced Settings

General Settings

☒ Enable

VPN Gateway Name: ISG50-2

Gateway Settings

My Address

☒ Interface: wan2 Static -- 59.124.163.156/255.255.255.224

☐ Domain Name / IP

Peer Gateway Address

☒ Static Address

Primary: 59.124.163.147

Secondary: 0.0.0.0

☐ Dynamic Address

Authentication

☒ Pre-Shared Key: 11111111

☐ Certificate: default (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: Any



Content:

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)

Negotiation Mode:

Proposal

 Add  Edit  Remove

#	Encryption	Authentication
1	DES	MD5

Key Group:

☐ NAT Traversal

☒ Dead Peer Detection (DPD)

Click **CONFIGURATION > VPN > IPsec VPN > VPN Connection** to configure the phase-2 rule.

Edit VPN Connection VPN_ISG50_2

Hide Advanced Settings Create new Object

Connection Name: VPN_ISG50_2

☒ Nailed-Up
☐ Enable Replay Detection
☐ Enable NetBIOS broadcast over IPSec

VPN Gateway

Application Scenario

☒ Site-to-site
☐ Site-to-site with Dynamic Peer
☐ Remote Access (Server Role)
☐ Remote Access (Client Role)

VPN Gateway: ISG50-2 wan2 59.124.147.0.0.0.0

Manual Key

☒ Manual Key

My Address:
Secure Gateway Address:
SPI: (256 - 4095)
Encapsulation Mode: Tunnel
Active Protocol: ESP
Encryption Algorithm: DES
Authentication Algorithm: SHA1
Encryption Key:
Authentication Key:

Policy

Local policy:

LAN1_SUBNET

INTERFACE SUBNET, 10.5.5.0/24

Remote policy:

remote_lan

SUBNET, 192.168.2.0/24

☐ Policy Enforcement

Phase 2 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Active Protocol:

ESP

Encapsulation:

Tunnel

Proposal

Add

Edit

Remove

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS):

none

ISG50-2 (Remote Office):

Add a VPN gateway rule.

Edit VPN Gateway ISG50-1

☐ Hide Advanced Settings

General Settings

☒ Enable

VPN Gateway Name: ISG50-1

Gateway Settings

My Address

☒ Interface wan1 Static -- 59.124.163.147/255.255.255.224

☐ Domain Name / IP

Peer Gateway Address

☒ Static Address Primary 59.124.163.156

Secondary 0.0.0.0

☐ Dynamic Address

Authentication

☒ Pre-Shared Key 11111111

☐ Certificate default (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)

Negotiation Mode:

Proposal

#	Encryption	Authentication
1	DES	MD5

Key Group:

☐ NAT Traversal

☒ Dead Peer Detection (DPD)

Click **CONFIGURATION > VPN > IPsec VPN > VPN Connection** to configure the phase-2 rule.

Edit VPN Connection VPN_ISG50_1

Hide Advanced Settings Create new Object

General Settings

☒ Enable

Connection Name: VPN_ISG50_1

☐ Nailed-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: ISG50-1 wan1 59.124.163.156 0.0.0.0

Manual Key

☐ Manual Key

My Address:

Secure Gateway Address:

SPI: (256 - 4095)

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

Encryption Key:

Authentication Key:

Policy

Local policy: LAN2_SUBNET INTERFACE SUBNET, 192.168.2.0/24

Remote policy: remote_lan SUBNET, 10.5.5.0/24

☐ Policy Enforcement

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

Goal to achieve:

Build up the IPSec VPN tunnel between ISG located in the main office and USG located in the home office.

Condition:***ISG as a Centralized multisite VPN and VoIP connectivity***ISG50 (Main Office):

WAN IP: 59.124.163.156

LAN IP: 10.5.5.1

Local subnet: 10.5.5.0/24

USG (Home Office):

WAN IP: 59.124.163.151

Local subnet: 192.168.2.0/24

IPSec VPNPhase 1:

Authentication: 1234567890

Negotiation mode: Main

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

Key Group: DH1

Phase 2:

Active Protocol: ESP

Encapsulation Mode: Tunnel

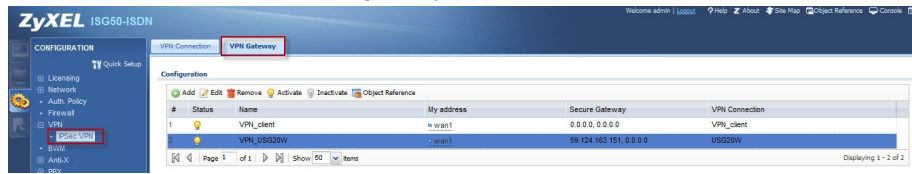
Encryption Algorithm: DES

Authentication Algorithm: SHA1

Perfect Forward Secrecy (PFS): None

ISG50 (Main Office):

Click on the **Add** button to add a VPN gateway rule.



To configure the VPN gateway rule, the user needs to fill in the following information:

- VPN gateway name.
- Gateway address: My Address (ISG50's IP) and Peer Gateway Address (USG's IP).
- Authentication setting.
 - Pre-Shared Key
 - ID Type setting (Local and Peer side)
- Phase-1 setting
- Negotiation mode
- Encryption algorithm
- Authentication algorithm
- Key Group

Edit VPN Gateway VPN_USG20W

☐ Hide Advanced Settings

General Settings

☒ Enable

VPN Gateway Name: VPN_USG20W

Gateway Settings

My Address

☒ Interface wan1 Static -- 59.124.163.156/255.255.255.0

☐ Domain Name / IP

Peer Gateway Address

☒ Static Address

Primary 59.124.163.151

Secondary 0.0.0.0

☐ Dynamic Address

Authentication

☒ Pre-Shared Key 1234567890

☐ Certificate default (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Proposal

#	Encryption	Authentication
1	3DES	MD5

Key Group: DH1

☐ NAT Traversal

☒ Dead Peer Detection (DPD)

Extended Authentication

☐ Enable Extended Authentication

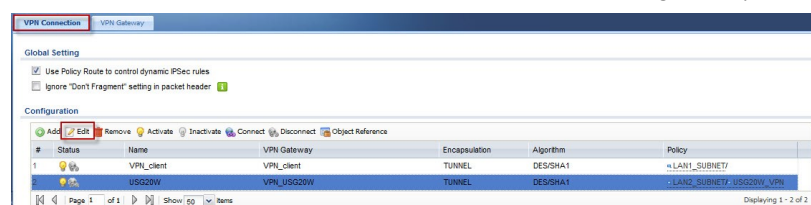
☒ Server Mode default

☐ Client Mode

User Name:

Password:

Click **CONFIGURATION > VPN > IPsec VPN > VPN Connection** to configure the phase-2 rule.



To configure the phase 2 rule, the user needs to fill in the following:

- VPN connection name
- VPN gateway selection
- Policy for
 - Local network side
 - Remote network side
- Phase 2 Settings
 - Active protocol
 - Encapsulation mode
 - Encryption algorithm
 - Authentication algorithm
 - Perfect Forward Secrecy

Edit VPN Connection USG20W

Hide Advanced Settings Create new Object

General Settings

☒ Enable

Connection Name: USG20W

☐ Natted-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: VPN_USG20W wan1 59.124.163.151 0.0.0.0

Manual Key

☒ Manual Key

My Address:

Secure Gateway Address:

SPI: (256 - 4095)

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

Encryption Key:

Authentication Key:

Policy

Local policy: LAN2_SUBNET INTERFACE SUBNET, 10.5.5.0/24

Remote policy: USG20W_VPN SUBNET, 192.168.2.0/24

☐ Policy Enforcement

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

Click the **Connect** button to establish the VPN link. Once the tunnel is established, a **connected** icon will be displayed in front of the rule.

VPN Connection VPN Gateway

Global Setting

☒ Use Policy Route to control dynamic IPsec rules

☐ Ignore "Don't Fragment" setting in packet header

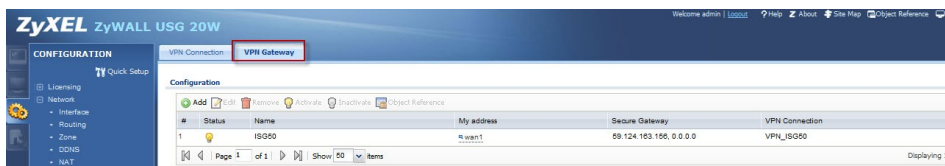
Configuration

#	Status	Name	VPN Gateway	Encapsulation	Algorithm	Policy
1		VPN_client	VPN_client	TUNNEL	DES/SHA1	LAN1_SUBNET/
2		USG20W	VPN_USG20W	TUNNEL	DES/SHA1	LAN2_SUBNET/ USG20W_VPN

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

USG (Home Office):

Add a VPN gateway rule.



To configure the VPN gateway rule, user needs to fill in:

- VPN gateway name
- Gateway address: My Address (USG's IP) and Peer Gateway Address (ISG50's IP)
- Authentication setting
 - Pre-Shared Key
 - ID Type setting (Local and Peer side)
- Phase-1 setting
- Negotiation mode
- Encryption algorithm
- Authentication algorithm
- Key Group

Edit VPN Gateway ISG50

☐ Hide Advanced Settings

General Settings

☒ Enable

VPN Gateway Name:

Gateway Settings

My Address

☒ Interface Static --

☐ Domain Name / IP

Peer Gateway Address

☒ Static Address

Primary

Secondary

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

☐ Certificate (See My Certificates)

Local ID Type:

Content:

Peer ID Type:

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Proposal

#	Encryption	Authentication
1	3DES	MD5

Key Group: DH1

☐ NAT Traversal

☒ Dead Peer Detection (DPD)

Configure the phase-2 rule.

ZyXEL ZyWALL USG 20W

CONFIGURATION

VPN Connection

Global Setting

☒ Use Policy Route to control dynamic IPSec rules

☐ Ignore "Don't Fragment" setting in packet header

Configuration

#	Status	Name	VPN Gateway	Encapsulation	Algorithm	Policy
1		VPN1/IS050	IS050	TUNNEL	DES-SHA1	LAN2_SUBNET=192.168.1.0/24

Page 1 of 1 | Show 50 items | Displaying 1 - 1

To configure the phase 2 rule, user needs to fill in:

- VPN connection name
- VPN gateway selection
- Policy for
 - Local network side
 - Remote network side
- Phase 2 Settings

- ☑ Active protocol
- ☑ Encapsulation mode
- ☑ Encryption algorithm
- ☑ Authentication algorithm
- ☑ Perfect Forward Secrecy

Edit VPN Connection VPN_1SG50

Hide Advanced Settings Create new Object

General Settings

☒ Enable

Connection Name: VPN_1SG50

☐ Nailed-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: 1SG50 wan1 59.124.163.156 0.0.0.0

Manual Key

☐ Manual Key

My Address:

Secure Gateway Address:

SPI: (256 - 4095)

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

Encryption Key:

Authentication Key:

Policy

Local policy: LAN2_SUBNET INTERFACE SUBNET, 192.168.2.0/24

Remote policy: ISG_VPN SUBNET, 10.5.5.0/24

☐ Policy Enforcement

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

Before configuring Remote Policy, the user can create a specific object for the VPN subnet.

Edit Address Rule ISG_VPN

Name: ISG_VPN

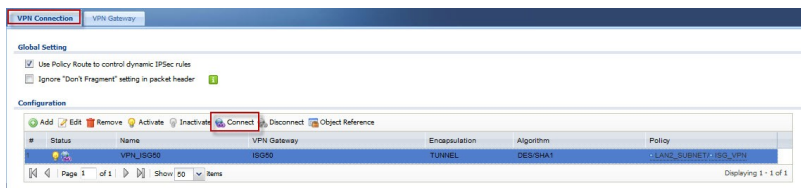
Address Type: SUBNET

Network: 10.5.5.0

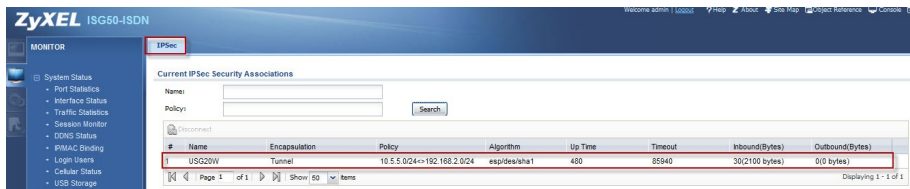
Netmask: 255.255.255.0

OK Cancel

Click on the **Connect** button to establish the VPN link. Once the tunnel is established, a **connected** icon will be displayed in front of the rule.



When the VPN tunnel is established, the user can find the SA information on **MONITOR > VPN MONITOR > IPsec**. **ISG50 (Main Office):**



USG (Home Office):



Clients in the subnet 192.168.2.0/24 of USG can register to ISG50 with the SIP server address 10.5.5.1.

Trusted Peer over IPsec VPN

Goal to achieve: Build up an IPsec VPN tunnel to protect voice traffic over the Trust Peer.

Condition:

ISG50-1 (Main Office):

LAN IP: 192.168.2.1

ISG50-2 (Remote Office):

LAN IP: 10.5.5.1

The configuration for IPsec VPN is the same as that in site to site IPsec VPN.

In outbound trunk setting, add a new trust peer in each ISG50 and set the remote LAN IP address as the trusted SIP server address.

ISG50-1 (Main Office):

The screenshot shows the 'Trusted Peer - Advanced setup' configuration page for ISG50-1 (Main Office). The 'General Settings' section is expanded. The 'Trunk Name' is set to 'To_ISG2'. The 'SIP Proxy Server Address' is set to '192.168.2.1'. The 'SIP Proxy Server Port' is set to '5060'. The 'Service Domain' is set to 'Disable'. The 'Outbound Proxy' is set to 'Disable'. The 'Outbound Proxy Port' is set to '5060'. The 'DTMF Mode' is set to 'info'. The 'Enable Privacy' checkbox is unchecked. The 'Proxy Require' field is empty with '(Optional)' text. The 'Channel Limit' is set to '8' with a range of '(1~128)'.

ISG50-2 (Remote Office):

The screenshot shows the 'Trusted Peer - Advanced setup' configuration page for ISG50-2 (Remote Office). The 'General Settings' section is expanded. The 'Trunk Name' is set to 'To_ISG1'. The 'SIP Proxy Server Address' is set to '10.5.5.1'. The 'SIP Proxy Server Port' is set to '5060'. The 'Service Domain' is set to 'Disable'. The 'Outbound Proxy' is set to 'Disable'. The 'Outbound Proxy Port' is set to '5060'. The 'DTMF Mode' is set to 'info'. The 'Enable Privacy' checkbox is unchecked. The 'Proxy Require' field is empty with '(Optional)' text. The 'Channel Limit' is set to '8' with a range of '(1~128)'.

Brute-force Attack Protection

Goal to achieve:

Check the current protection setting for web-portal and sip and change the block time and retry fail count for web-portal.
Unlock the blocked extension.

Condition:

Brute force attack protection (web-login & SIP) is enabled by default.

Default block time: 60 minutes

Default number of failed access: 3

Blocked extension: 1001

Below are the CLI commands to enable/disable this feature.

Enable:

pbx attack-prevent web-login activate

pbx attack-prevent sip activate

Disable:

no pbx attack-prevent web-login activate

no pbx attack-prevent sip activate

Perform the following CLI commands to check the configuration for attack-prevent status, block time and number of failed access attempts.

show pbx attack-prevent web-login

show pbx attack-prevent sip

Example:

```
Router> show pbx attack-prevent web-login
Web-login attack Prevent: enable
Web-login Block Time: 60
Web-login Fail Access: 3
Router>
```

Below are the CLI commands to change the configuration for block time.

The default value is 60 minutes.

pbx attack-prevent web-login block-time <1-1440 min>

pbx attack-prevent sip block-time <1-1440 min>

Below are the CLI commands to change the configuration for number of failed access attempts.

The default value is 3.

pbx attack-prevent web-login fail-access <1-10>

pbx attack-prevent sip fail-access <1-10>

Check the locked extension list.

show pbx attack-prevent web-login lock-list

show pbx attack-prevent sip lock-list

Unlock a certain blocked extension or all blocked extensions.

pbx attack-prevent web-login unlock {all | NUMBER}

pbx attack-prevent sip unlock {all | NUMBER}

Example:

```
Router>  
Router> configure terminal  
Router(config)# pbx attack-prevent web-login unlock 1001
```

6. How to Establish a Seamless Mobile Office with ZyXEL Reach?

The company would like to allow its employees to be reached easily and not miss any incoming calls when they are out of the office or on business trips. The smartphone application, ZyXEL Reach, turns every smart phone into a mobile SIP client and reduces phone bills by routing all calls to the IP network. In addition, with the mobile extension feature, the ISG50 rings the employee's office extension and his mobile phone number simultaneously.

ZyXEL Reach – Smartphone Application

Goal to achieve:

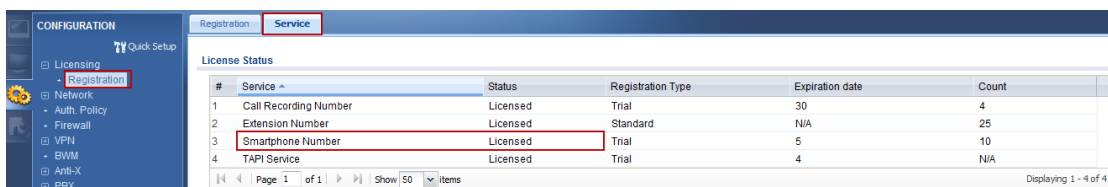
Turn the smartphone into a mobile SIP client with ZyXEL Reach installation and basic configuration.

Condition:

ISG's address: 59.124.163.156

Username: 3002

The smartphone feature is enabled when the license (ISG-SP5) is applied.



CONFIGURATION					
Quick Setup					
Registration Service					
License Status					
#	Service	Status	Registration Type	Expiration date	Count
1	Call Recording Number	Licensed	Trial	30	4
2	Extension Number	Licensed	Standard	N/A	25
3	Smartphone Number	Licensed	Trial	5	10
4	TAPI Service	Licensed	Trial	4	N/A

Page 1 of 1 Show 50 items Displaying 1 - 4 of 4

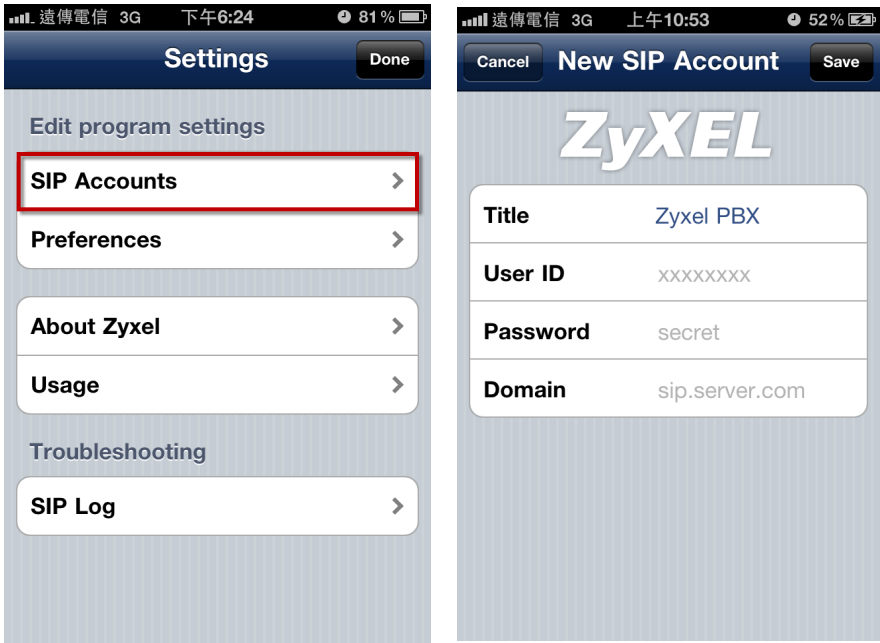
Install the mobile softphone APP, ZyXEL Reach, on your smart phone.
It supports both iPhone and Android platform.



Enter your SIP account, password and the domain of ISG to register an extension on ISG.



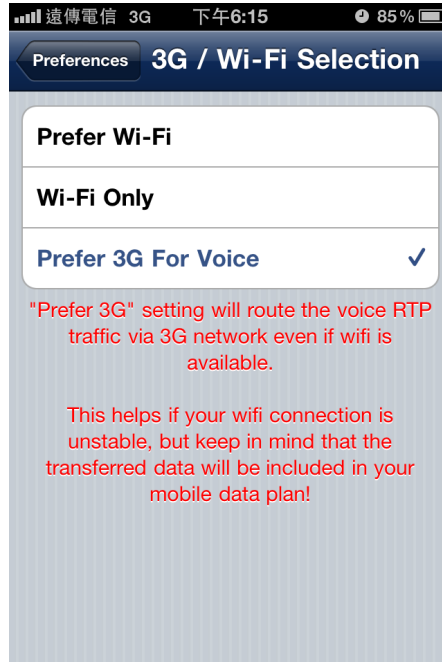
You can also add multiple SIP accounts.



Personal settings.



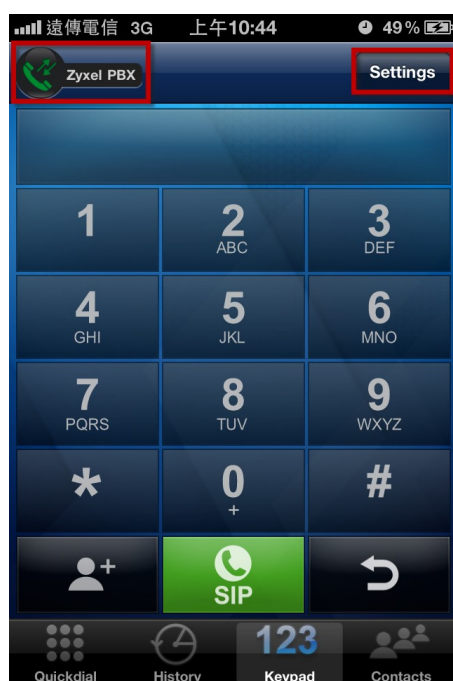
Select the connection type.



Call recording settings.



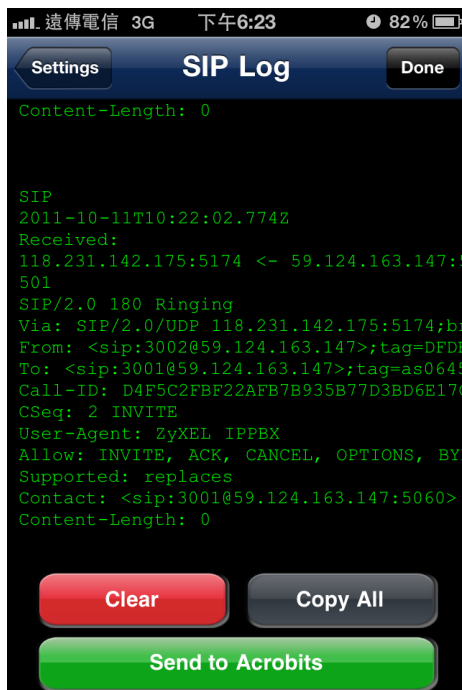
Dial the phone number from the keypad.



Check the call history.



View the packet trace.



How to avoid missing any call on a certain extension?

In this example, an ISG50 rings an office extension #1011 and the corresponding ZyXEL Reach simultaneously with a single number. When the employee is away or out of the office, he can always get calls of his extension. All settings can be done on the ZyXEL Reach by the employee himself, so it is not required to change any configuration on the ISG50.

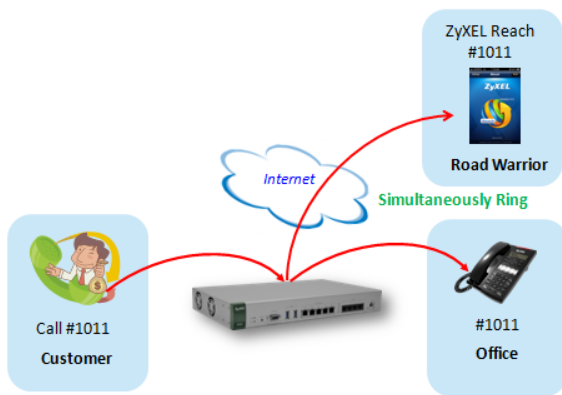
Goal to achieve:

When there is an incoming call on the extension #1011 of the employee, both extensions #1011 on the IP phone in the office and on the ZyXEL Reach can ring at the same time.

Condition:

Authentication on V310 Username: 1011

Authentication on ZyXEL Reach Username: web1011



Use “web + extension” as the username. For extension 1011, set “web1011” as the username.

Then go to Advanced settings to configure the Auth User Name and Caller ID, which are the same as the extension.

Edit SIP Account [Cancel] [Save]

ZyXEL

Title ZyXEL ISG

Username web1011

Password ●●●●

Domain 59.124.163.156

Display Name 1011

Advanced settings >

Delete

Advanced settings

Ringtones >

Auth User Name 1011

Transport Protocol tcp >

STUN Server stun.example.com

Discover Global IP OFF

When empty, the STUN and proxy server is auto-detected

Codecs For WiFi >

Codecs For 3G >

Advanced settings

Registration period. The server may ask to increase this value

Send Keepalives OFF

Keepalive Period 30

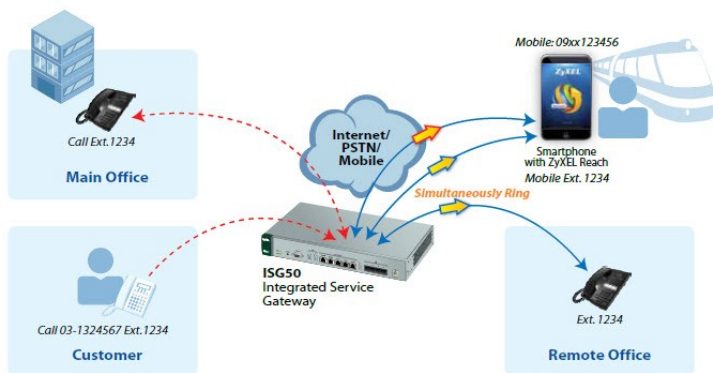
Send keepalive packets to keep the NAT ports open. Set if you have troubles getting incoming calls

Caller ID 1011

Caller Id Method From Username >

Sets the From: header of outgoing INVITE messages. Most VoIP providers will ignore this value though.

Mobile Extension



Goal to achieve:

When there is an incoming call on the extension #1007 of the employee, both of his extension #1007 on the IP phone in the office and his mobile phone 0912345678 can ring at the same time.

Condition:

Extension: 1007

Mobile extension for #1007: 0912345678

Single Number Reach (IP phone & Mobile SIP & GSM Mobile Number)

Go to CONFIGURATION > PBX > Extension Management > Authority Group > [Group Name] > [Extension Number] > Edit > Call Forward to Configure your mobile extension settings.

You can select to “Manually” turn on and off this feature or select “Force Enable” to always turn on this feature.

Fill in a mobile phone number or an extension number and select a dial rule (LCR) from the list.

In this example, ISG50 rings the extension 1007 and the mobile phone number 0912345678 simultaneously with a single number.

The screenshot shows the 'Edit Extension 1007' dialog box with the 'Call Forward' tab selected. The 'Call Forward' section contains five dropdown menus, all set to 'Disable': DND(Do Not Disturb), Blind Forward, Busy Forward, No Answer Forward, and After Office Hours. The 'Call Blocking' section has a 'Black List' dropdown set to 'Disable' and an unchecked checkbox for 'Block the calls without Caller ID'. The 'Mobile Extension' section has three fields: 'Mobile Extension' set to 'Manually', 'Number' set to '0912345678', and 'Dial Rule' set to 'BRI_Out'. The 'OK' and 'Cancel' buttons are at the bottom right.

Section	Field	Value
Call Forward	DND(Do Not Disturb):	Disable
	Blind Forward:	Disable
	Busy Forward:	Disable
	No Answer Forward:	Disable
	After Office Hours:	Disable
Call Blocking	Black List:	Disable
	Block the calls without Caller ID	<input type="checkbox"/>
Mobile Extension	Mobile Extension:	Manually
	Number:	0912345678
	Dial Rule:	BRI_Out

When the “Manually” option is selected, you have to dial the pre-defined feature code to turn this feature on and off.

The screenshot shows a configuration interface with a left sidebar and a main content area. The sidebar, titled 'CONFIGURATION', has a tree view with the following items: Licensing, Network (expanded), Interface, Routing, Zone, DDNS, NAT, HTTP Redirect, ALG, IP/MAC Binding, Auth. Policy, Firewall, VPN, BWM, Anti-X, PBX (expanded), and Voice interfaces. The 'PBX' item is highlighted with a red box, and its sub-item 'Global' is also highlighted with a red box. The main content area has tabs at the top: SIP Server, Feature Code (selected), E-Mail, FakedIP, Peer to Peer, and QoS. Below the tabs is a 'General Settings' section with a table of feature codes. The table has two columns for feature codes and two columns for their descriptions. The following feature codes are highlighted with red boxes: *94, *95, *23, *97, *99, *96, *22, **, *98, and *88.

Feature Code	Description	Feature Code	Description
*94	Group Pickup:	*96	Call Transfer:
*95	Direct Pickup:	*22	Follow Me On:
*23	Follow Me Off:	**	Voice Mail:
*97	Mobile Extension On:	*98	Mobile Extension Off:
*99	Mobile Extension Auto:	*88	Call Recording On Demand:
	Second Dial:		Internal Operator(0 or 9):
			Ext:

7. How to Leverage Enterprise-class Calling Features to Increase Business Productivity?

The company needs an automatic call operator to transfer each incoming call to the specific contact or department. In addition, customer service hotlines are also required for serving customers. Employees often have conference calls with vendors and distributors. The ISG50 has a call distribution system including Auto-Attendant, Hunt Group, Three-way Conference and Meet-me Conference features to increase operating efficiency and reduce the cost of business communications and operations.

Auto Attendant

Goal to achieve:

Record the customized audio file by extension to auto attendant system.

Design a customized auto attendant for office hours and night service. The customer who dials into this auto attendant system during the office hours can follow the option keys to reach the target department, or dial the extension number to reach a certain extension. If the customer dials into the auto attendant after office hours, the call will be served by a hunt group directly.

Condition:

Recorded Peer: 1003

Office Hour: Monday – Friday; 08:00-12:00 and 13:00-17:30

Operator key for office hours: 9; extension number: 9999






Hunt group number for night service: 5555

Configuration for customized Auto Attendant

Outbound Line Group **Auto-Attendant** LCR

Default **Customized**

Auto-Attendant Summary

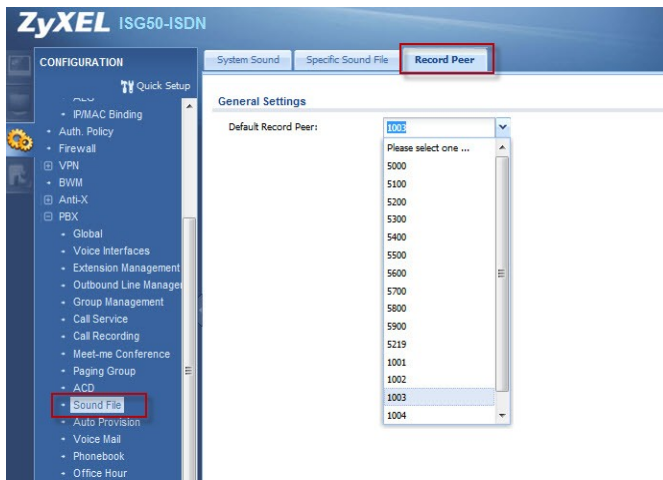
 Add  Edit  Remove  Download  Upload

#	Name	Description
1	AA1	

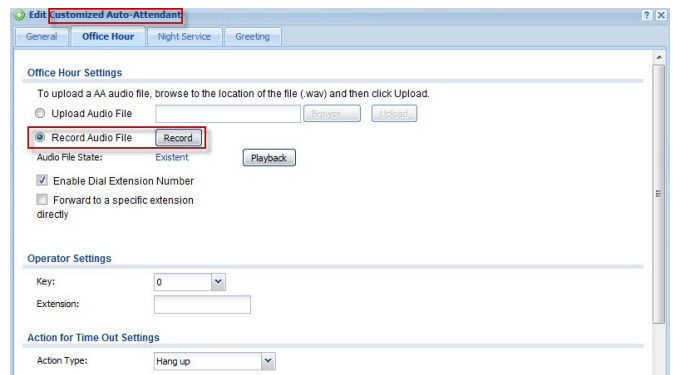
Page 1 of 1 Show 50 items

In addition to uploading an existing audio file to the system, ISG50 provides an easy way for users to record the audio file by extension to Auto Attendant system. When you press the record button, ISG50 will call the record peer. After the extension of the record peer is picked up, you can start recording with this extension.

Set the record peer. For example, we set extension 1003 as the record peer. You will use this extension to record the audio file in the next step.



Select "Record Audio File" and press the record button. ISG50 will call the record peer 1003. Start recording after you pick up the phone of 1003. Hang up the phone or press the # key to finish recording.



Decide if incoming calls are allowed to dial extensions in addition to key codes or bypass the options (key codes) and go straight to the specified extension. In this example, we allow incoming calls to follow the option keys. Besides, the incoming call can also dial the extension number if the user would like to reach a certain extension.

Office Hour Settings

To upload a AA audio file, browse to the location of the file (.wav) and then click Upload.

☐ Upload Audio File

☒ Record Audio File

Audio File State: Existent

☒ Enable Dial Extension Number

☐ Forward to a specific extension directly

Design the customized menu with option keys.

Operator Settings

Key:

Extension:

Action for Time Out Setting:

Action Type:

Options

Key:

Action:

Extension:

Description:

Key	sub-menu	extension	description
1	sub-menu		Sales
1	hunt	7100	sales team 1
2	hunt	7200	sales team 2
2	hunt	3000	customer service
3	acd	5100	
4	extension	1001	
5	repeat		repeat the main menu

Option key 0 and 9 are reserved for the operator and can't be configured as other option keys.
ISG50 supports up to 10 levels of sub menus.
In the sub menu, click the button "Add Child" to edit the options and "Edit" to upload the audio file for the sub menu instruction.

Operator Settings

Key: 9 ← Either 0 or 9

Extension: 9999

Action for Time Out Settings

Action Type: Hang Up

Options

+ Add Option + Add Child ✎ Edit ✖ Remove

Key	Action	Extension	Description
1	sub-menu		Sales
1	hunt	7100	sales team 1
2	hunt	7200	sales team 2
3	return-previous-menu		Back to the main menu
2	hunt	3000	customer service
3	acd	5100	
4	extension	1001	
5	repeat		repeat the main menu

← Main Menu

↓ Sub Menu

Edit Option

Key: 1

Action: Forward to a Sub Menu

Description:

☐ Enable Dial Extension Number

Audio File

Audio File State: Inexistent Playback

☒ Upload Audio File Browse... Upload

☐ Record Audio File Record

OK Cancel

You can also enable “Night Service” to perform different AA directions outside of office hours based on the office hour setting.

Edit Customized Auto-Attendant

General Office Hour **Night Service** Greeting

Night Service Settings

☒ **Enable Night Service**

To upload a AA audio file, browse to the location of the file (.wav) and then click Upload.

☒ Upload Audio File

☐ Record Audio File

Audio File State: Existent

☐ Enable Dial Extension Number

☒ Forward to a specific extension directly Hunt Group 5555/hunt1

☐ Play audio file before forward to a specific extension

Select the working days and specify the time range during these working days.
You can enter up to 6 time ranges. The time must be in 24 hr format with a start time and an end time. Ex: 08:00-12:00, 13:00-17:30

Office Hour

Office Hour Settings

<input type="checkbox"/> Sun						
<input checked="" type="checkbox"/> Mon	08:00-12:00	13:00-17:30				
<input checked="" type="checkbox"/> Tue	08:00-12:00	13:00-17:30				
<input checked="" type="checkbox"/> Wed	08:00-12:00	13:00-17:30				
<input checked="" type="checkbox"/> Thu	08:00-12:00	13:00-17:30				
<input checked="" type="checkbox"/> Fri	08:00-12:00	13:00-17:30				
<input type="checkbox"/> Sat						

You can also set specific days as holidays according to your own country or company policy. Enter a date in mm/dd format.
Incoming calls on these holidays will be treated as “after office hours” and answered by “Night Service AA”.

Holiday Settings

Add

Edit

Remove

#	Date	Description
1	06/06	Dragon Boat Festival
2	09/12	Mid Autumn Festival
3	02/02	Chinese New Year Day

Overwrite Settings

☒ Auto-Attendant

☐ Auto-Attendant + Authority Group

☐ Auto-Attendant + Authority Group + Extension

Hunt Group

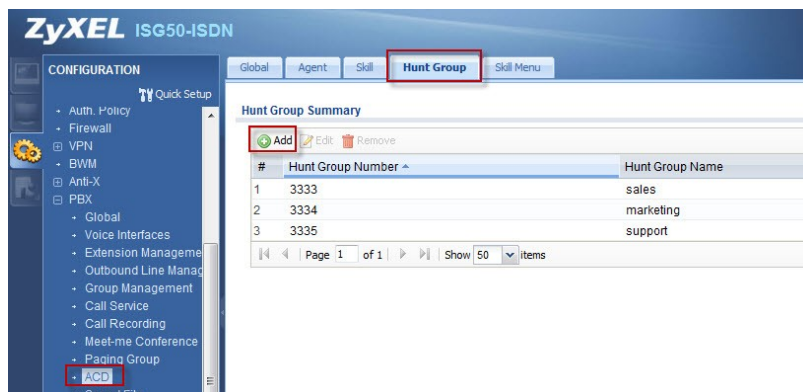
Goal to achieve:

Create a hunt group number 3333 for the sales department.

Condition:

Hunt Group Number: 3333; Members: 1006, 1007 and 1008

Ring Strategy: Random



Associate Hunt Group number with extensions and decide the ring strategy and timeout action. The extensions ring based on pre-configured ringing algorithm.

Assign the priority to each extension. The priority represents which extension the incoming calls are routed to first. 1 is the highest priority while 5 is the lowest priority.

When an incoming call comes in this hunt group, this call will be routed to priority 1 first along with the ring strategy. If no extensions with priority 1 are available, the call will then be routed to extensions with priority 2.

Edit Hunt

Hunt Group Settings

Hunt Group Number:

3333

Hunt Group Name:

sales

Description:

Ring Strategy:

Random

Timeout Action:

Auto Attendant

default

Waiting Music:

No Timeout

Max. Waiting Calls:

Hang Up

Waiting Timeout:

Backup Skill

Ring Member Timeout:

Hunt Group

Auto Attendant

Extension

Voice Mail

Member

Add

Edit

Remove

#	Member	Priority
1	1006	1
2	1007	1
3	1008	2

Page 1 of 1

Show 50 items

Displaying 1 - 3 of 3

OK

Cancel

Three-way Conference

Three-way conference lets you to set up a call with up to two people at the same time.

Goal to achieve:

The extensions 1011, 1010 and 3200 would like to set up a three-way conference call.

Condition:

V310 (#3200) calls ZyXEL Reach (#1010).

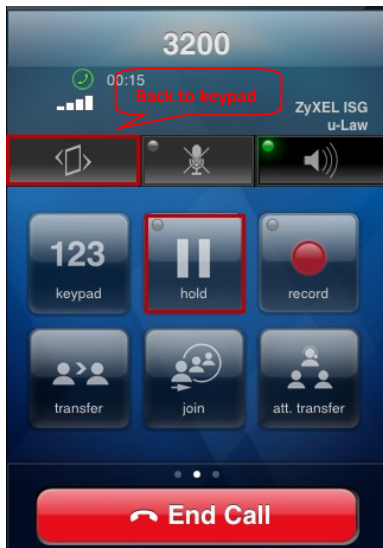
Then ZyXEL Reach (#1010) puts the call with V310 (#3200) on hold, calls another V310 (#1011) and bridges these two calls.



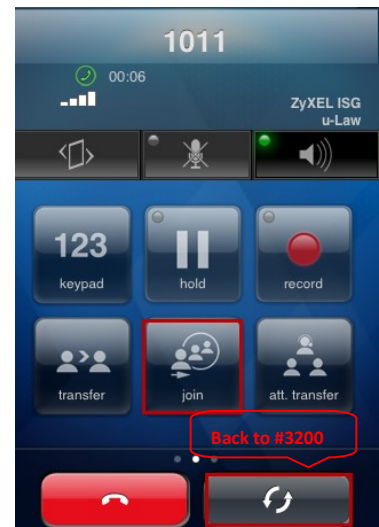
By performing the following steps, these three extensions are having a three-way conference call.

How to perform a three-way conference on ZyXEL Reach?

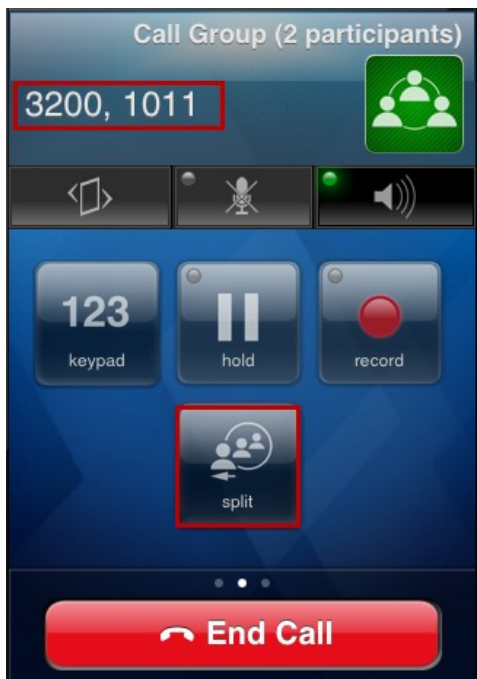
1. ZyXEL Reach (#1010) has a call with V310 (#3200). Before dialing to extension 1011, press the hold key and go back to the keypad.
2. Then dial 1011 and press



3. After the call with 1011 is established, press the join key to set up the three-way conference. Before pressing the join key, you can still press to go back to the call with #3200.

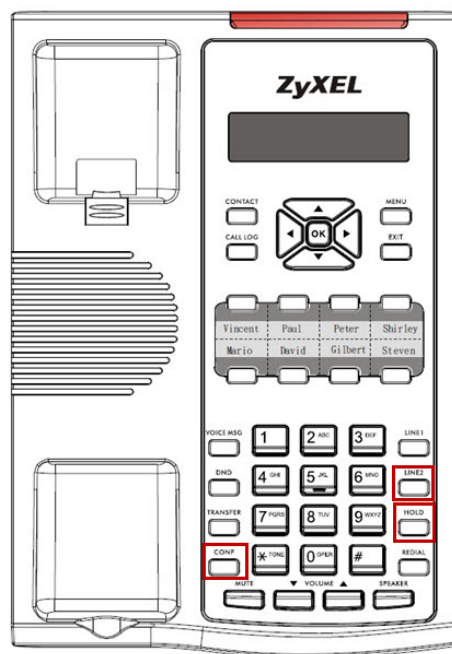


4. Three-way conference has been established. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the split key.



How to perform three-way conference on V310?

1. V310 (#3200) uses LINE 1 to talk with ZyXEL Reach (#1010).
2. Press the HOLD key to put this call on hold and then press LINE 2 to make a call to extension 1011.
3. When the call with extension 1011 is active, press the CONF key to set up the three-way conference.



In order to put a present call on hold and answer a new call, make sure these extensions are selected into the “Enabled Extension” list in “Call Waiting”.

CONFIGURATION

- Quick Setup
- HI IP Redirect
- ALG
- IP/MAC Binding
- Auth. Policy
- Firewall
- VPN
- BWM
- Anti-X
- PBX
 - Global
 - Voice Interfaces
 - Extension Manageme
 - Outbound Line Manag
 - Group Management
 - Call Service**

Call Waiting

General Settings

Enable List

Extension Pool	Enabled Extension
1005	1010
1006	1011
1007	1012
1008	1013
1009	1014

Meet-Me Conference

Goal to achieve:

The employee would like to hold a conference call with customer. All attendees can dial into the conference number 6000 with the PIN code.

Condition:

Conference number: 6000

Add a new conference number.

CONFIGURATION

- Auth. Policy
- Firewall
- VPN
- BWM
- Anti-X
- PBX
 - Global
 - Voice Interfaces
 - Extension Management
 - Outbound Line Management
 - Group Management
 - Call Service
 - Call Recording
 - Meet-me Conference**
 - Paging Group

Meet-me Conference

Conference Room Summary

#	Conference Number	Max. Members	Description
1	6000	5	Conference

Page 1 of 1 | Show 50 items

Edit Conference Number 6000

Conference Number: 6000

Max. Members: 5

PIN Code: (Empty is no authentication)

Confirm PIN Code:

Description: Conference

Configure the conference number, PIN number and the maximum number of attendees.

For users calling from internal extensions, just dial the conference number to access the conference room.

For users calling from outbound trunks, dial the representative number first and then dial the conference number.

If the PIN code is configured, the attendee needs to enter the PIN code before accessing the conference room.

System Sound

How to change the language of system sounds from English to a specific language?

Goal to achieve:

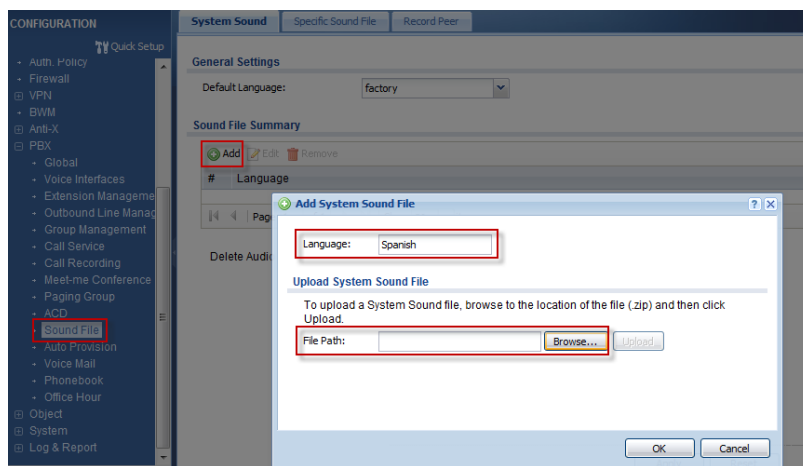
The administrator would like to change the language of system sounds to Spanish.

Condition:

Default Language: Spanish

1. Refer to the script for voice prompts in English.
2. You can refer to the Text (English) column and the filename column.
3. Translate the sentences into the designated language.
4. Record your own voice prompts.
All audio files must follow the **16 kHz, 16-bit, PCM, mono mode** (*.wav) format.
5. Save each sentence as the matching filename.
For example:
filename: goodbye
Text(English): Goodbye.
Text(Designated Language): _____
6. After all the voice prompts are ready, compress them in a single "zip" file per language.

7. Upload the zip file to the system.



8. Select the uploaded language and apply it as the system sounds.

The screenshot shows a configuration interface with a sidebar on the left and a main content area on the right. The sidebar is titled 'CONFIGURATION' and includes a 'Quick Setup' link. It lists various configuration categories: Auth, Policy, Firewall, VPN, BWM, Anti-X, PBX, Global, Voice Interfaces, Extension Management, Outbound Line Management, Group Management, Call Service, Call Recording, Meet-me Conference, Paging Group, ACD, Sound File, Auto Provision, Voice Mail, Phonebook, Office Hour, Object, System, and Log & Report. The 'Sound File' category is highlighted. The main content area has three tabs: 'System Sound', 'Specific Sound File', and 'Record Peer'. The 'System Sound' tab is active. It contains a 'General Settings' section with a 'Default Language' dropdown menu set to 'Spanish'. Below this is a 'Sound File Summary' table with one entry: '1 Spanish'. At the bottom of the main content area, there are 'Apply' and 'Reset' buttons. The 'Apply' button is highlighted with a red box.

CONFIGURATION

Quick Setup

- Auth, Policy
- Firewall
- VPN
- BWM
- Anti-X
- PBX
- Global
- Voice Interfaces
- Extension Management
- Outbound Line Management
- Group Management
- Call Service
- Call Recording
- Meet-me Conference
- Paging Group
- ACD
- Sound File
- Auto Provision
- Voice Mail
- Phonebook
- Office Hour
- Object
- System
- Log & Report

System Sound | Specific Sound File | Record Peer

General Settings

Default Language: Spanish

Sound File Summary

#	Language
1	Spanish

Page 1 of 1 | Show 50 items

Delete Audio Files: Unused All

Apply Reset

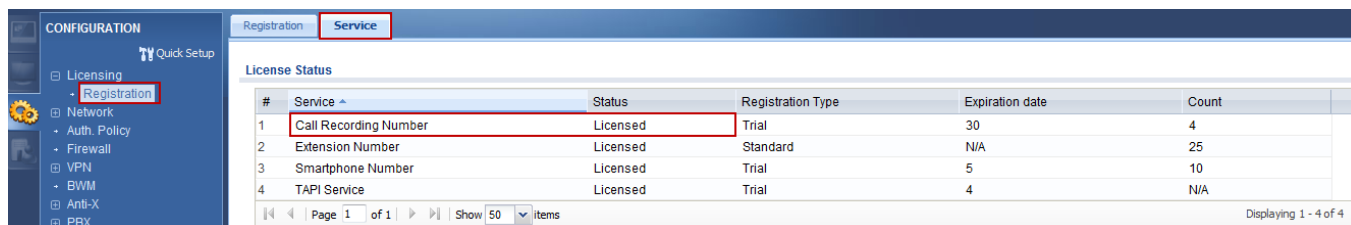
8. How to Record a Call?

The company would like to monitor calls of certain individuals to ensure the incoming calls are being handled professionally and the agents are working efficiently while recording conference calls for writing meeting minutes. The call recording feature allows the network administrator to record conversations to or from specific extensions or trunks, and save them into USB storage devices.

Preparation for Call Recording

License

The call recording feature is enabled when the license (ISG50-CR) is applied.

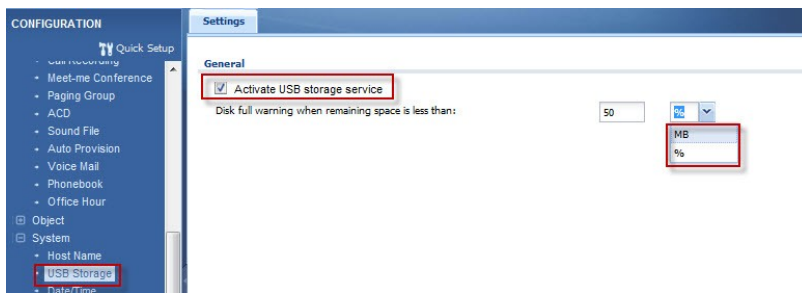


The screenshot shows a configuration interface with a left sidebar and a main content area. The sidebar has a 'CONFIGURATION' header and a 'Quick Setup' icon. Below it, there are several expandable sections: 'Licensing' (which is expanded to show 'Registration'), 'Network', 'Auth. Policy', 'Firewall', 'VPN', 'BWM', 'Anti-X', and 'PBX'. The 'Registration' section is highlighted with a red box. The main content area has a 'Registration' tab and a 'Service' tab, with 'Service' being the active tab. Below the tabs is a 'License Status' table. The table has columns for '#', 'Service', 'Status', 'Registration Type', 'Expiration date', and 'Count'. There are four rows of data. The first row, 'Call Recording Number', is highlighted with a red box. The table also includes pagination controls at the bottom: 'Page 1 of 1', 'Show 50 Items', and 'Displaying 1 - 4 of 4'.

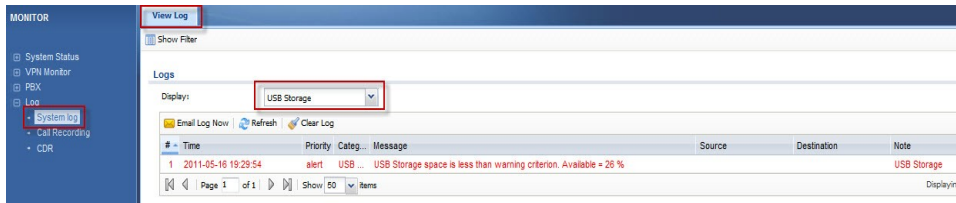
#	Service	Status	Registration Type	Expiration date	Count
1	Call Recording Number	Licensed	Trial	30	4
2	Extension Number	Licensed	Standard	N/A	25
3	Smartphone Number	Licensed	Trial	5	10
4	TAPI Service	Licensed	Trial	4	N/A

USB Storage

You must plug in an external USB storage device and activate USB storage service to store call recordings. USB storage devices with FAT32 or EXT3 file systems are supported for connection to the USB port of ISG50. Also, you have to set a disk full warning limit to stop recording once the storage space is less than this criterion.



When the remaining space of the USB storage is less than this limit, there will be a warning message in the system log to remind the administrator.



How to record calls on a certain trunk or an extension?

Full-time Recording

Goal to achieve:

The administrator would like to record all calls on the FXO trunk and the extensions 1007, 1008 and 1009.

Condition:

Recorded Trunk: Port1_pabx (FXO trunk)

Recorded Peer: 1007, 1008 and 1009

Select from the Trunk Pool and Peer Pool to determine which trunks and/or peers should be recorded.

Full-time Recording Peer Settings

The screenshot displays the 'Full-time Recording Peer Settings' configuration page. It features two main sections: 'Trunk' and 'Peer'. Each section has a source pool on the left and a 'Recorded' list on the right, connected by arrow buttons.

Trunk Section:

- Trunk:** A label with a red box.
- Trunk Pool:** A list containing 'trunk1' and 'trunk2'.
- Recorded Trunk:** A list containing 'Port1_pabx' (highlighted with a red box).

Peer Section:

- Peer:** A label with a red box.
- Peer Pool:** A list containing '3200', '1005', '1006', '1010', and '1012'.
- Recorded Peer:** A list containing '1007', '1008', and '1009' (all three are highlighted with a red box).

On-demand Recording

Goal to achieve:

The internal extensions can enable and disable the call recording by dialing the feature code.

Condition:

Feature code for Call Recording On demand: *88

On-demand recording is only used by internal extensions. Dial the feature code to enable/disable on-demand recording.

The default feature code is *88.

However, for trunks and peers which are already configured in the full-time recording list, peers can't dial this feature code to enable/disable recording.

The screenshot shows the Asterisk Manager GUI. The left sidebar has a 'CONFIGURATION' section with a 'Quick Setup' icon and a list of options: VPN, BWM, Anti-X, PRX, Global (selected), Voice Interfaces, Extension Management, Outbound Line Manager, Group Management, Call Service, and Call Recording. The main area has tabs for SIP Server, Feature Code (selected), E-Mail, FaxesIP, Peer to Peer, and QoS. Under the 'Feature Code' tab, there is a 'General Settings' section with a table of feature codes. The 'Call Recording On Demand' feature code is highlighted with a red box and is set to *88.

General Settings	
Group Pickup:	*94
Direct Pickup:	*95
Follow Me Off:	*23
Mobile Extension On:	*97
Mobile Extension Auto:	*99
Second Dial:	
Call Transfer:	*96
Follow Me On:	*22
Voice Mail:	**
Mobile Extension Off:	*98
Call Recording On Demand:	*88
Internal Operator(0 or 9):	

Ext:

Query Call Recording Files

Search for the recorded files by recorded time, peer type and peer name.

Goal to achieve:

The administrator would like to search for and download call recording files in the past 24 hours.

Condition:

Recorded Time: Last 24 hours

Peer Type: All

Peer Name: All

In Recorded Time, you can search for call recordings from the past day, week, or month.

Furthermore, you can also specify an exact time period for which to find call recordings.

In Peer Type, select "All" to search for all recordings including extensions and trunks.

You can specify a certain extension or trunk for the search criteria.

MONITOR

- System Status
- VPN Monitor
- PBX
- Log
- System log
- Call Recording**
- CDR

Query

Query Condition

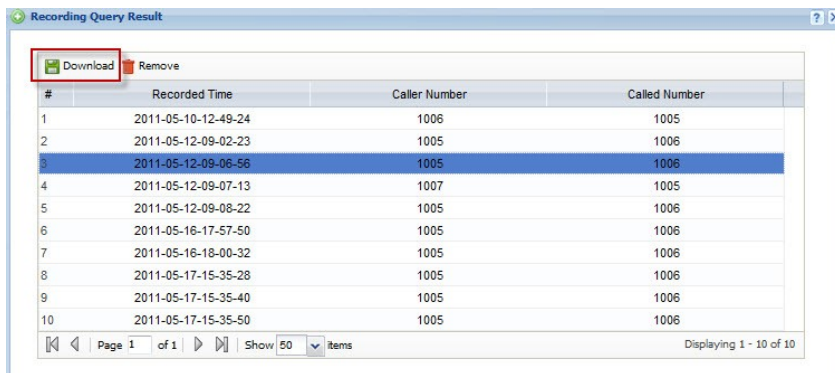
Recorded Time: ☒ Last 24 hours ☐ From: 00:00 To: 00:00

Peer Type:

Peer Name:

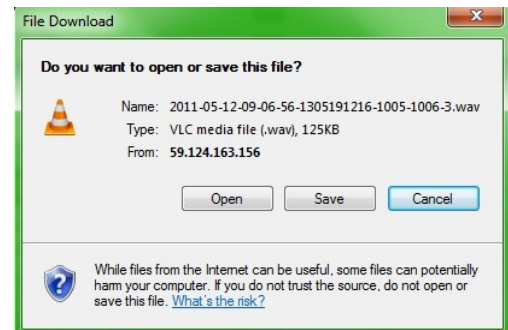
This screen lists the call recordings that matched the specified criteria.

You can download individual call recordings and play back the files with any audio software which supports WAV format.



The screenshot shows a window titled "Recording Query Result". At the top left, there are two buttons: "Download" (highlighted with a red box) and "Remove". Below these buttons is a table with four columns: "#", "Recorded Time", "Caller Number", and "Called Number". The table contains 10 rows of data. The third row is highlighted in blue. At the bottom of the window, there is a pagination bar showing "Page 1 of 1", "Show 50 items", and "Displaying 1 - 10 of 10".

#	Recorded Time	Caller Number	Called Number
1	2011-05-10-12-49-24	1006	1005
2	2011-05-12-09-02-23	1005	1006
3	2011-05-12-09-06-56	1005	1006
4	2011-05-12-09-07-13	1007	1005
5	2011-05-12-09-08-22	1005	1006
6	2011-05-16-17-57-50	1005	1006
7	2011-05-16-18-00-32	1005	1006
8	2011-05-17-15-35-28	1005	1006
9	2011-05-17-15-35-40	1005	1006
10	2011-05-17-15-35-50	1005	1006



9. How to Audit Call Usage with Report and Analyzer to Improve Working Efficiency?

The company wants auditing and reporting of the communications to evaluate if the call usage is effective and efficient. The ISG50 has a built-in CDR database that automatically stores call activities and includes phone records with details. The network administrator can use the CDR database to search for abnormal activities in order to improve working efficiency.

CDR

Goal to achieve: Search for the call history for any calls including internal calls and external calls in the past 24 hours.

Condition:

Search period: Last 24 hours

Direction: all directions

The ISG50 has a built in CDR database that automatically stores calls made to or from its extensions. The administrator can decide if internal calls are logged in the CDR record.

When the local database is full, the ISG50 removes all the CDRs from the local database and creates an “Aged File” and sends the Aged CDR records to the specified E-mail address. The E-mail address is also used for receiving alerts indicating that the CDR file is half full when the “Enable Alert” is selected.

CONFIGURATION Quick Setup

- ▢ Licensing
- ▢ Network
 - Interface
 - Routing
 - Zone
 - DDNS
 - NAT
 - HTTP Redirect
 - ALG
 - IP/MAC Binding
- Auth. Policy
- Firewall
- ▢ VPN
 - BWM
- ▢ Anti-X
- ▢ PBX
- ▢ Object
- ▢ System
- ▢ Log & Report
 - Email Daily Report
 - Log Setting
 - CDR Configuration

CDR Configuration

General Settings

Database Usage: 0.1%

Generate CDR: ☒ Internal Call

Enable Alert: ☐

Aged File: Drop

Backup File Type: SQL File

E-mail Address: emily.chiang@zyxel.com.tw

Database Location Settings

☒ Use Built-in Server

☐ Use remote server

Server: :

Username:

Password:

Schema: Download

How to find the call history?

You can use the query conditions plus the other items to generate your own CDR report.

For example, you can select the time period for your query. ISG50 provides time range.

Start time: specify the time period for your query.

Direction: Specify the types of calls you want to view based on the source and destination of the calls.

The screenshot shows the 'MONITOR' interface with a sidebar on the left containing a tree view with the following items: System Status, VPN Monitor, PBX, Log, System log, Call Recording, and CDR (highlighted with a red box). The main area has two tabs: 'Backup' and 'Query' (highlighted with a red box). Below the tabs is the 'Query Condition' section, which includes: 'Start Time' with radio buttons for 'Last 24 hours' (selected) and 'From: To:'; 'Direction' with four checkboxes: 'extension / extension', 'extension / outbound', 'outbound / extension', and 'outbound / outbound'; 'Call Time' and 'Talk Time' with input fields and 'seconds' dropdowns; 'Caller Group', 'Channel', 'Caller Number', and 'Dialed Number' with dropdown menus and 'Totally Match' buttons. Below this is the 'Displayed Item Settings' section (highlighted with a red box) containing a grid of checkboxes: Call Date, Called Number, Dst. Channel, Call Result, Caller ID, Caller Group, Call Time, Record, Caller Number, Src. Channel, Talk Time, and RTP. The 'Call Date', 'Called Number', 'Caller Number', and 'Talk Time' checkboxes are checked.

After configuring query conditions and displayed items, click the “Search” button to view your CDR query result.

CDR Query Result

Record

RTCP

#	Call Date	Caller Number	Called Number	Talk Time
1	2012/05/02 16:16:46	1010	1008	21
2	2012/05/02 16:16:59	3200	1010	7

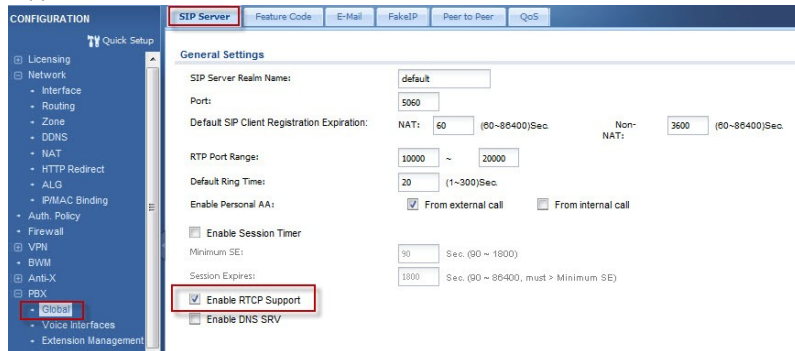
Page 1 of 1

Show 50 items

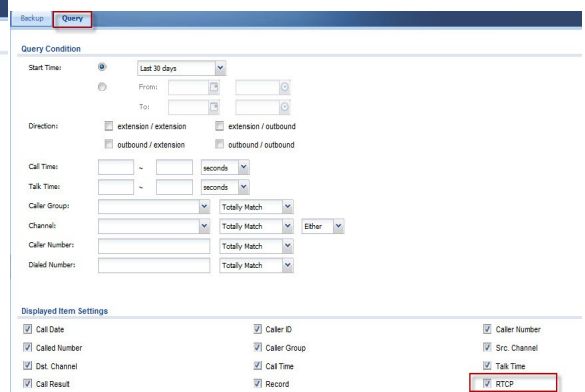
Displaying 1 - 2 of 2

How to check QoS of each call in RTCP?

To view the RTCP information, select “Enable RTCP Support”. By default, RTCP Support is enabled.



You can select “RTCP” to display the RTCP information in the CDR report.



Click the button to view RTCP information for each call.

The top screenshot shows a 'CDR Query Result' window with a table containing the following data:

#	Call Date	Caller ID	Caller Number	Called Number	Caller Group	Src. Channel	Dst. Channel	Call Time	Talk Time	Call Result	Record RTCP
1	2011/05/17 19:23:36	"SG1005" <1005>	1005	962003	CSO	SP11005	ToBranch	19	8	ANSWERED	[Record RTCP]
2	2011/05/17 19:33:36	"SG1005" <1005>	1005	962003	CSO	SP11005	ToBranch	19	16	ANSWERED	[Record RTCP]

The bottom screenshot shows the same window with a context menu open over the 'Record RTCP' button for the first row. The menu displays the following RTCP statistics:

```

RTCP
Caller:
loss:0( 0.00%)
max jitter:2
rtt:0
Callee:
loss:0( 0.00%)
max jitter:2
rtt:0
OK
  
```

Recommended value of RTCP for good quality:

loss < 1% (If packet loss > 3%, call quality will degrade audibly.)

Jitter < 10 ms. (The meaning of the jitter value depends greatly on the jitter buffers involved.)

rtt < 150 ms (RTT = delays of both directions added)

Back up CDR file

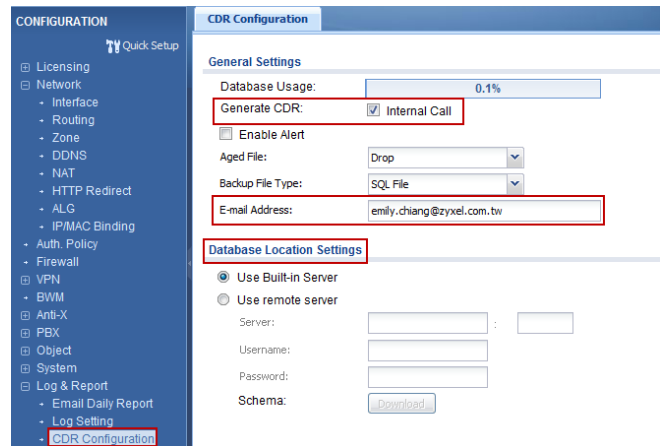
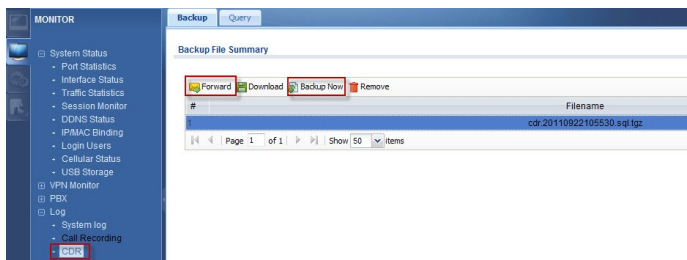
Goal to achieve: Backup call records to administrator's email.

Condition:

Backup email: emily.chiang@zyxel.com.tw

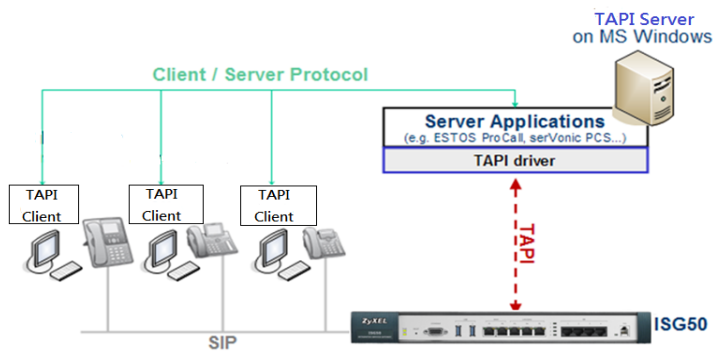
Click the “Backup Now” button to back up the CDR file.

You can also send the backup file to the administrator by clicking the “Forward” button.



10. How do UC Server and UC Client Work with ISG50?

The company would like a simple way to use computers to manage telephone calls. The employees can use the UC client to make, terminate, reject, transfer and redirect calls by one simple click on the UC client. In addition, using the presence feature, employees can be aware of the availability status of their colleagues. Finally, with the TAPI service, employees may communicate more efficiently.



Preparation for TAPI Service

The TAPI feature is enabled when the license “ISG50-CTI” is applied.

The screenshot shows the 'CONFIGURATION' window with the 'Service' tab selected. The 'License Status' table is displayed below the navigation pane.

#	Service	Status	Registration Type	Expiration date	Count
1	Call Recording Number	Not Licensed		0	N/A
2	Extension Number	Licensed	Standard	N/A	25
3	Smartphone Number	Not Licensed		0	N/A
4	TAPI Service	Licensed	Trial	29	N/A

Navigation: Page 1 of 1 | Show 50 items

In the configuration, set the username and password for the administrator. ISG50 can support up to 2 administrator accounts for TAPI service. The account will be used for TAPI driver login later.

The screenshot shows the 'TAPI' configuration page. The 'General Settings' section has the 'Enable TAPI' checkbox checked. The 'Server Account Settings' section contains fields for 'Server 1 User Name' (admin), 'Server 1 Password' (masked), 'Server 2 User Name', and 'Server 2 Password'.

Select the extensions that administrator can control and determine which extensions can use the TAPI service.

Server TAPI Lines Settings

Peer Pool

1011
1012
1013
1014
1015

Server TAPI Lines

1005
1006
1007
1008
1009

Client TAPI Lines Settings

Peer Pool

1013
1014
1015
1016

Client TAPI Lines

1005
1006
1007
1008
1009

TAPI Driver Installation

Goal to achieve: Install TAPI driver on the PC.

Condition:

ISG server IP address: 59.124.163.156

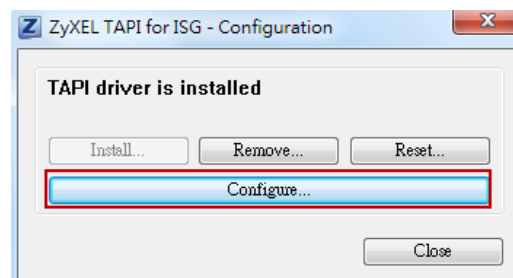
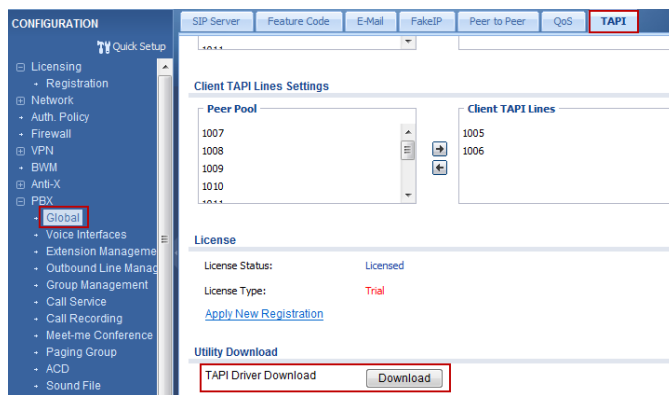
TAPI Server user name: admin

TAPI line: 1005-1016

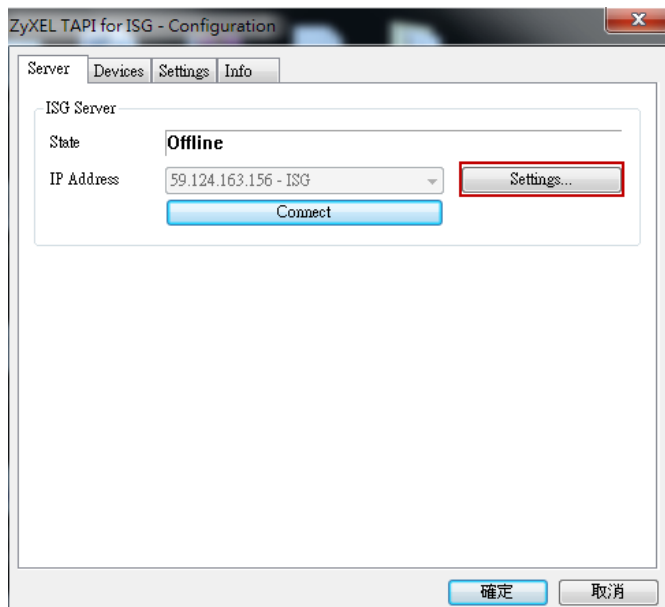
The TAPI driver must be installed on the same PC as the UC server installed.

Download TAPI driver from the ISG50.

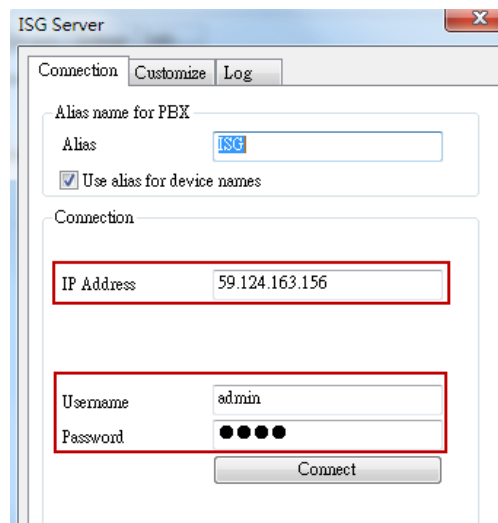
Install it in the PC.



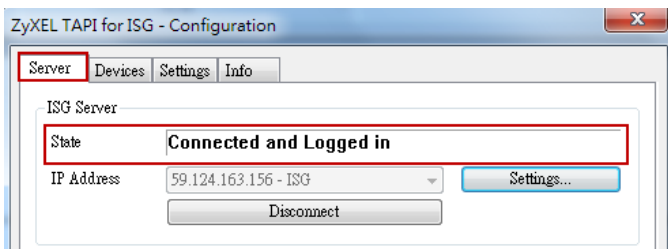
Configure the ISG server.



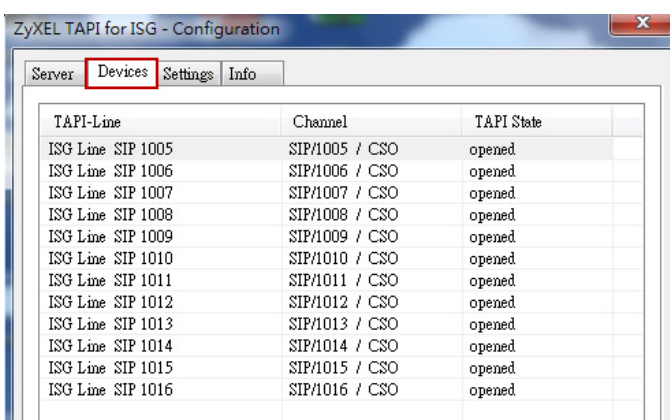
Fill in the IP address of ISG and log in with the administrator account.
Then click the "Connect" button.



Check if the state is connected.



TAPI lines that administrator can control.



UC Server Installation

Goal to achieve:

Install UC server on the PC.

Create users on UC server and assign an extension number from the server TAPI lines in ISG50 for each user.

Condition:

Administrator's account for access UC server: ucisg

Download the trial version of UC server from the website of ESTOS.

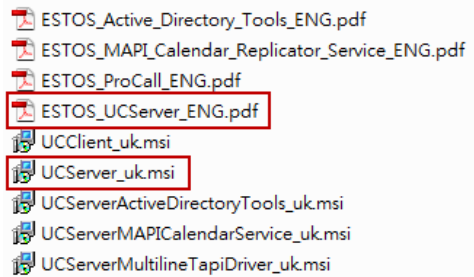
<http://www.estos.com/products/unified-communications-classic-cti/procall-40-enterprise.html>

The screenshot shows the ESTOS website with the following layout:

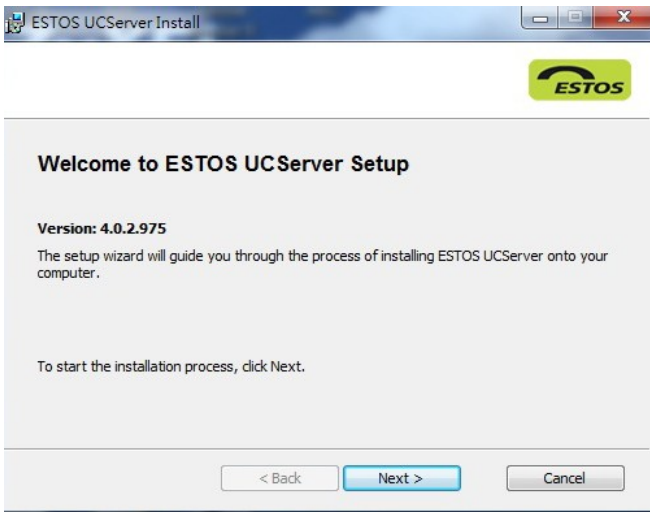
- Header:** ESTOS logo (Communication Solutions), navigation links (Products, Solutions, Service & Support, About us, Contact), and a search bar.
- Breadcrumbs:** estos.com // Products // Unified Communications & Classic CTI // ProCall 4.0 Enterprise
- Left Sidebar:**
 - Unified Communications & Classic CTI
 - ProCall 4.0 Enterprise (highlighted)
 - ProCall One
 - PhoneTools for Lync
 - Database & Directory Services
 - MetaDirectory 3.0 Professional
 - Drivers & Middleware
 - ECSTA Series
 - CallControlGateway 3.0
 - TaniServer ? ?
- Main Content Area:**
 - ProCall 4.0 Enterprise** (Section Header)
 - ProCall 4.0 Enterprise** (Product Description): ProCall 4.0 Enterprise is a Unified Communications Solution with CTI, Presence-Management and Instant Messaging to improve company-wide cooperation, and via Federation, beyond company borders. In addition to all comfort CTI benefits (e.g. dial assistance, hotkey dialing, call journal, busy-lamp-field and reverse look-up) the software is equipped with a person-centric presence management system with telephony and calendar integration.
 - Image:** A screenshot of the ProCall software interface showing a status bar with "Claude Rozier" and "Available".
 - The Federation functionality** has been designed for corporate use and is an Internet communication concept founded on the social networking principles. Based on...
- Right Sidebar:**
 - Quicklinks:** Functions, Topology
 - Download:** ProCall 4.0.2.1101 uk (highlighted), ProCall 4.0.2.1101 uk (Client only, for Outlook 2010 x64), ProCall 4.0.2.1101 SDK, ProCall 4.0 Enterprise Brochure

Install ProCall4.0 UC Server “UCServer_uk.msi” on the PC.

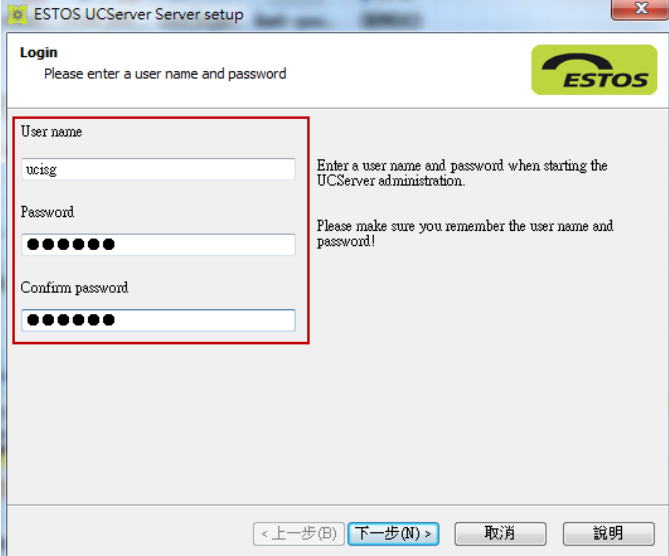
For detailed of configuration of the UC server, please refer to the document “ESTOS_UCServer_ENG.pdf”.



Start to install ESTOS UC server. Keep on pressing “Next” to finish the installation.

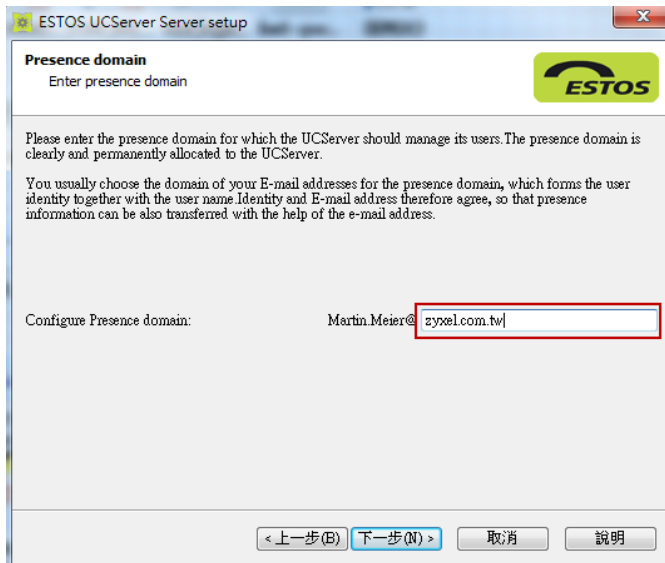


Create a username and password for the UC server. The administrator has to use this account to log in and manage the UC server.



Configure the presence domain.

For example, we fill "zyxel.com.tw" in this field.



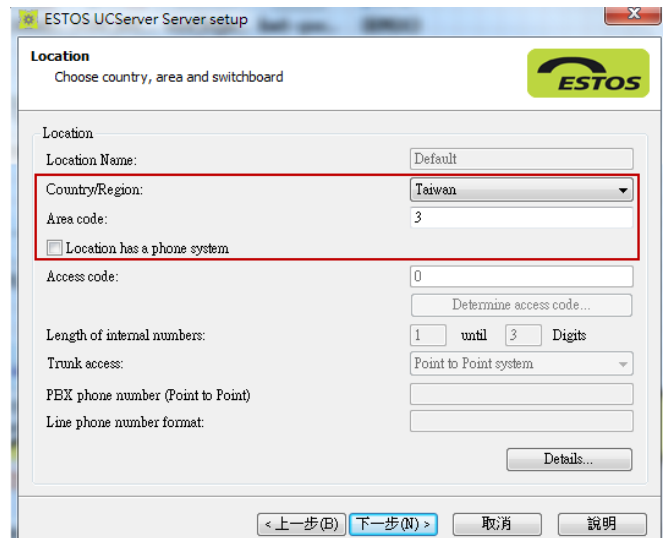
The screenshot shows the 'Presence domain' configuration window. The title bar reads 'ESTOS UCServer Server setup'. The main heading is 'Presence domain' with the instruction 'Enter presence domain'. Below this, a paragraph explains that the presence domain is for user management and is linked to email addresses. A text input field labeled 'Configure Presence domain:' contains the text 'Martin Meier@zyxel.com.tw', with 'zyxel.com.tw' highlighted by a red rectangle. At the bottom are buttons for '< 上一步(B)', '下一步(N) >', '取消', and '說明'.

In one of the installation steps, set the country and the area code.

For example, we select "Taiwan" as the country/region and set "3" as the area code.

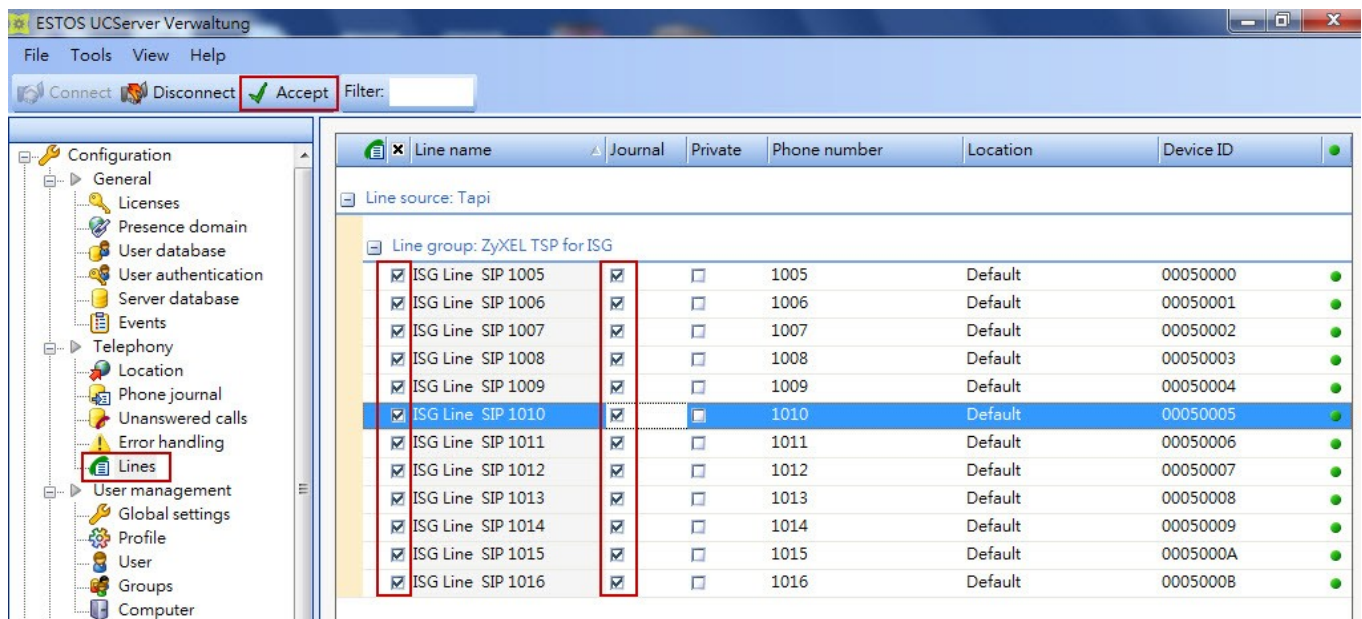
If "Location has a phone system" is unchecked, all dialed digits will be treated as "internal".

If this box is checked, the country code and the area code will be added before the dialed numbers if more than 3 digits are entered.

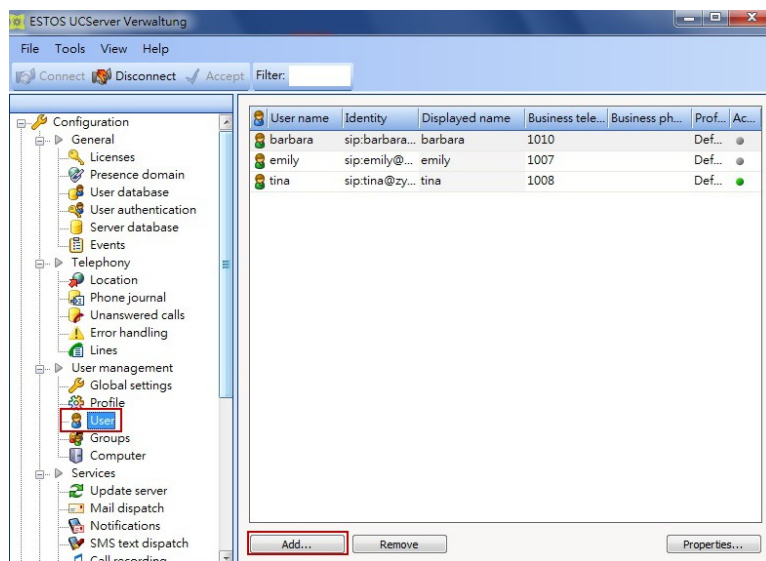


The screenshot shows the 'Location' configuration window. The title bar reads 'ESTOS UCServer Server setup'. The main heading is 'Location' with the instruction 'Choose country, area and switchboard'. The 'Country/Region' dropdown is set to 'Taiwan' and the 'Area code' is set to '3', both highlighted by a red rectangle. Below these, there is an unchecked checkbox labeled 'Location has a phone system'. Other fields include 'Access code' (0), 'Length of internal numbers' (1 until 3 Digits), 'Trunk access' (Point to Point system), 'PBX phone number (Point to Point)', and 'Line phone number format'. A 'Details...' button is at the bottom right. Navigation buttons at the bottom are '< 上一步(B)', '下一步(N) >', '取消', and '說明'.

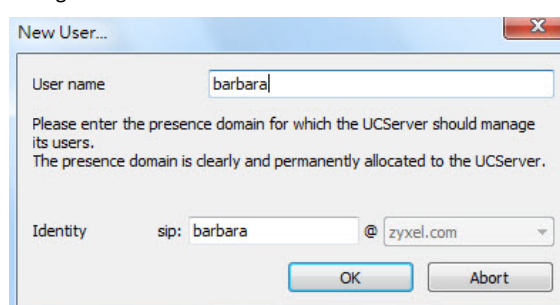
These are the extensions which are configured in the “Server TAPI Lines” in ISG50.
Click on “Accept” to apply the new settings on the server.



Create new users on the UC server.



Configure the user name for the new account on UC server.



Configure the password for this new user.

The screenshot shows the 'Settings for users "barbara"' window with the 'General' tab selected. The 'UC Password' field is highlighted with a red box. The 'Active user account' checkbox is checked.

Additional lines	Authorization	Member of	Status
General	Telephone numbers	Contact address	Services

User name (Login): barbara
 Identity: sip:barbara@zyxel.com
 Forename: barbara
 Surname:
 Displayed name: barbara
 E-Mail Address:
 User profile: Default
 UC Password: [Redacted]
☒ Active user account

Assign an extension number for this user.

You can click the button to choose from the "Server TAPI Lines".

The screenshot shows the 'Settings for users "barbara"' window with the 'Telephone numbers' tab selected. The 'Business' field and its selection button are highlighted with a red box. The 'Further extensions of the user' section is also visible.

Additional lines	Authorization	Member of	Status
General	Telephone numbers	Contact address	Services

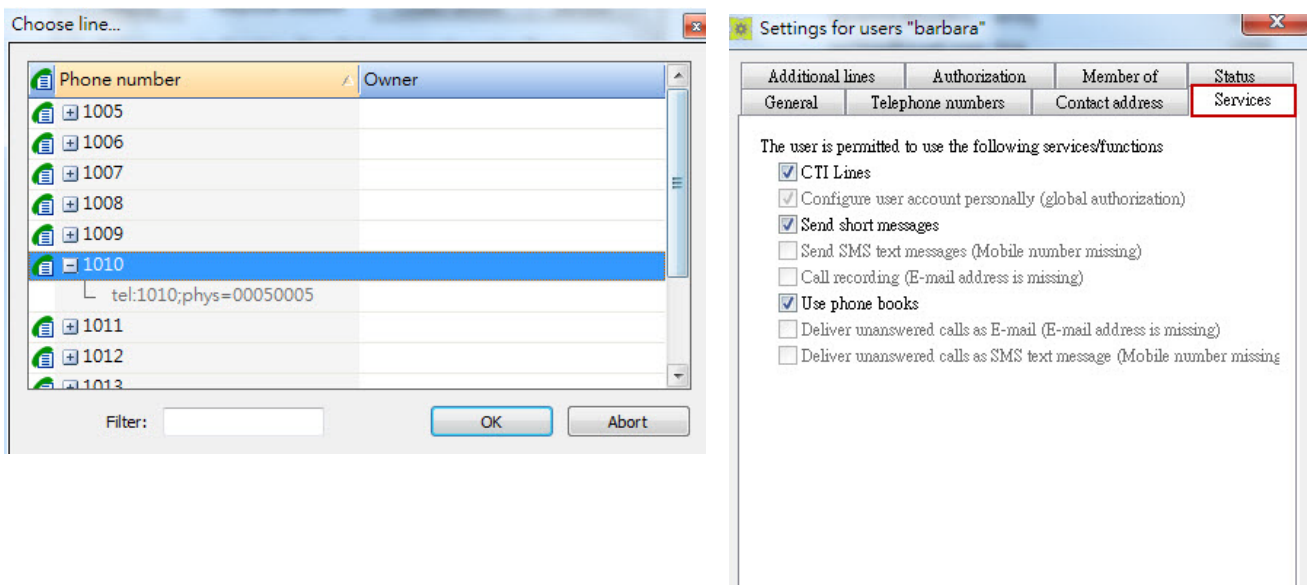
Rufnummern des Benutzers. Diese Rufnummern sehen andere Benutzer und föderierte Kontakte. Über Geschäftlich und Geschäftlich 2 werden die Leitungen des Benutzers ermittelt.

Business: 1010 [Selection button] 1
 Business 2: [Selection button]
 Private:
 Mobile:
 Mailbox:
 Recording Server:

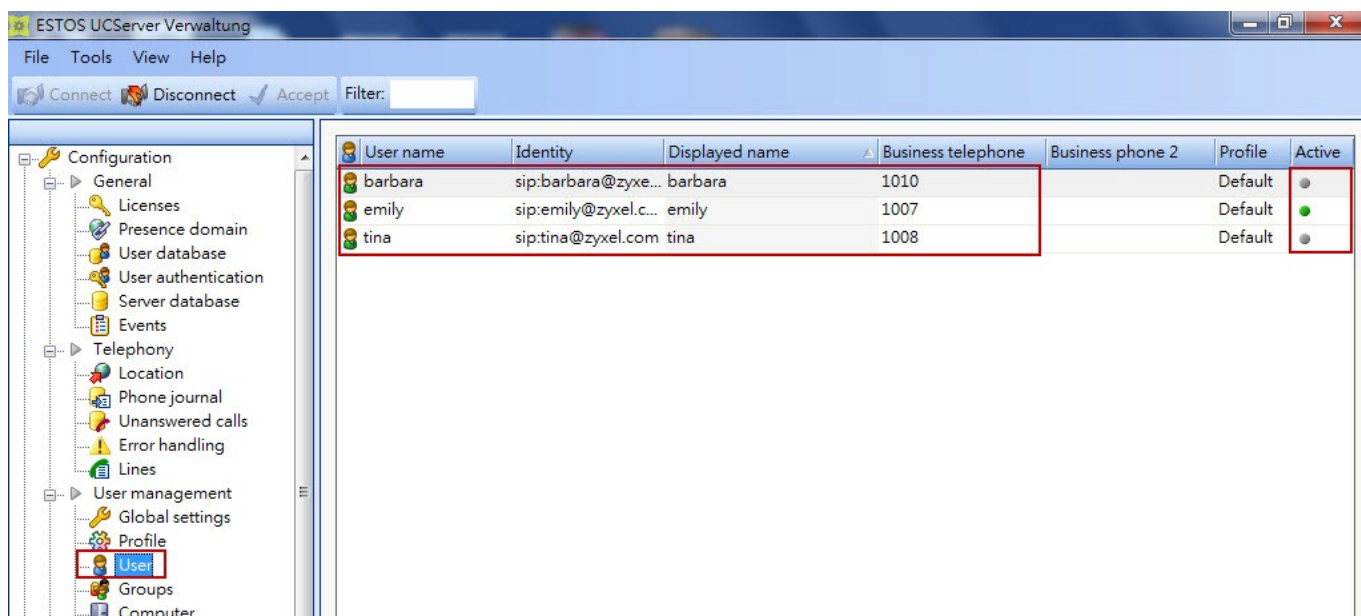
Further extensions of the user:

1. Telephone: [Selection button]
 2. Telephone: [Selection button]

Select an extension number for the new user from the "Server TAPI Lines". Select the services for this user.



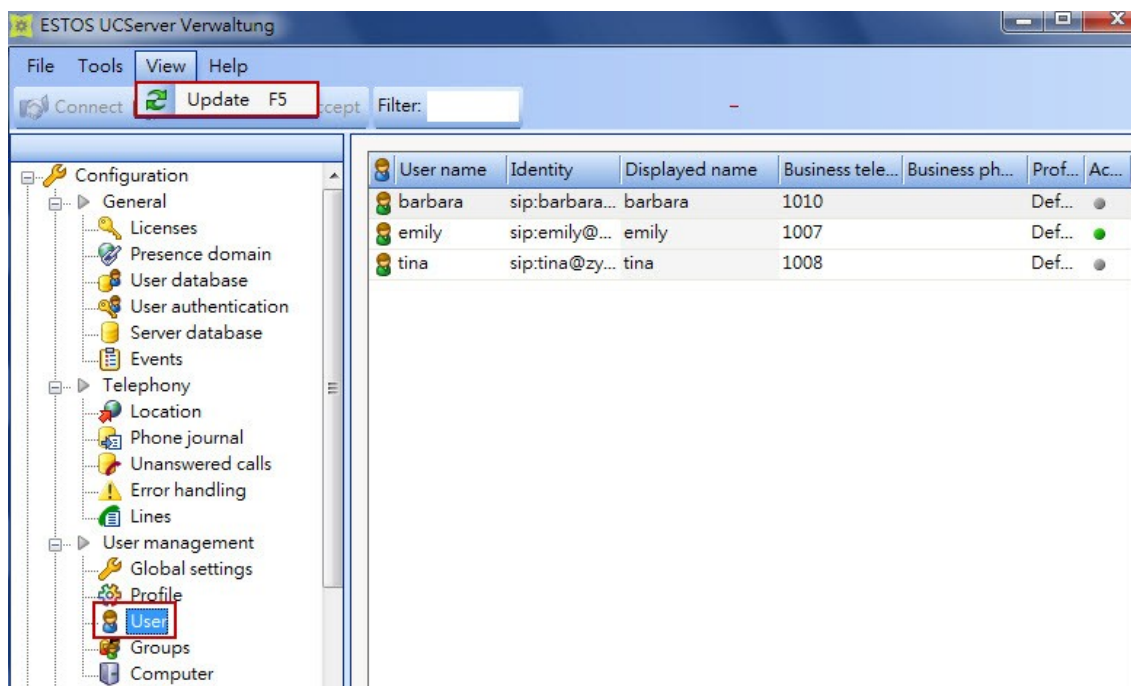
After the users are created, the administrator can monitor if the user is online or offline.



The screenshot shows the ESTOS UCServer Verwaltung application window. The left sidebar contains a tree view with categories like Configuration, Telephony, and User management. The 'User' option under 'User management' is selected and highlighted with a red box. The main area displays a table of users with columns for User name, Identity, Displayed name, Business telephone, Business phone 2, Profile, and Active. Three users are listed: barbara, emily, and tina. The 'Active' column shows a green dot for emily and grey dots for barbara and tina. A red box highlights the first three columns and the 'Active' column for all three users.

User name	Identity	Displayed name	Business telephone	Business phone 2	Profile	Active
barbara	sip:barbara@zyxe...	barbara	1010		Default	●
emily	sip:emily@zyxel.c...	emily	1007		Default	●
tina	sip:tina@zyxel.com	tina	1008		Default	●

The administrator can press “F5” to get the most updated status of all users.



UC Client Installation

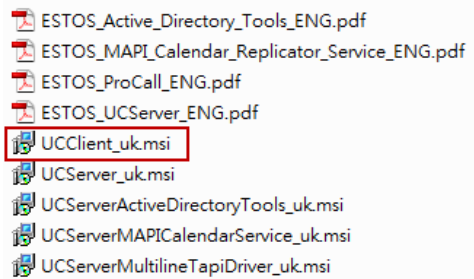
Goal to achieve: Use the UC client to make a call, hang up a call, reject a call, transfer a call, redirect a call and check the status of other extensions.

Condition:

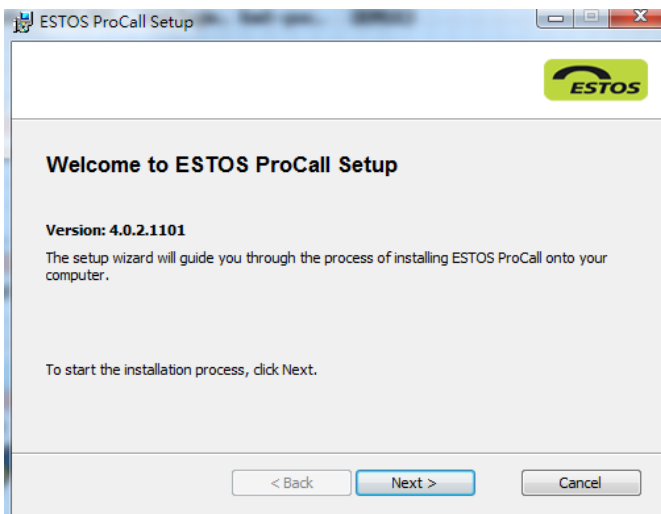
UC Server User & corresponding extension:

barbara	1010
emily	1007
tina	1008

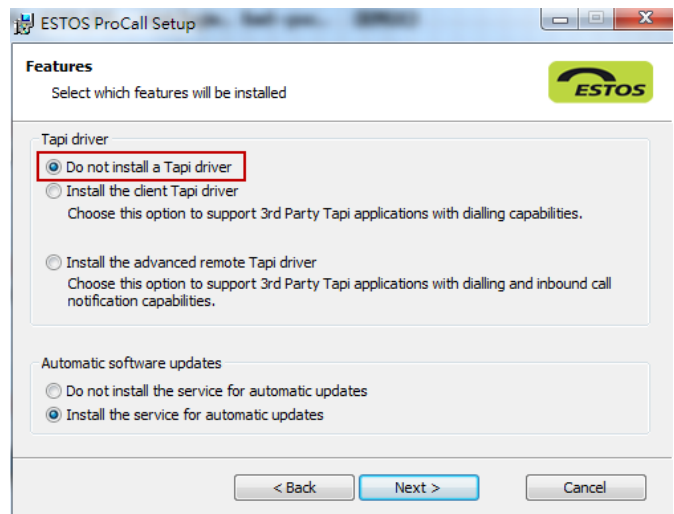
Install UC Client on the laptop.



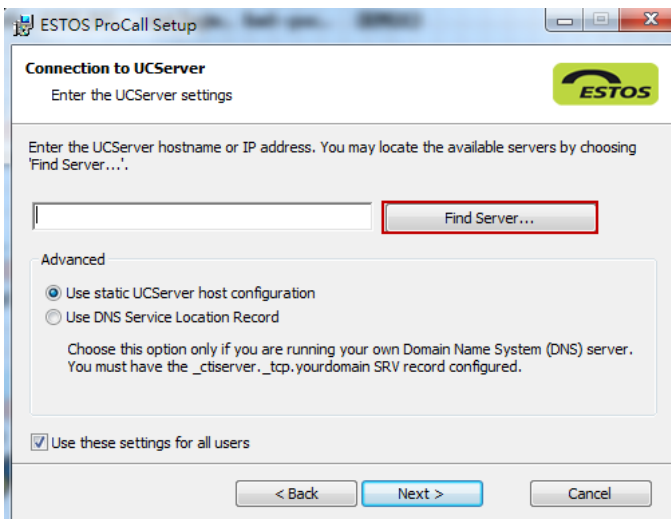
Start to install ESTOS UC client “ProCall”. Keep on pressing “Next” to finish the installation.



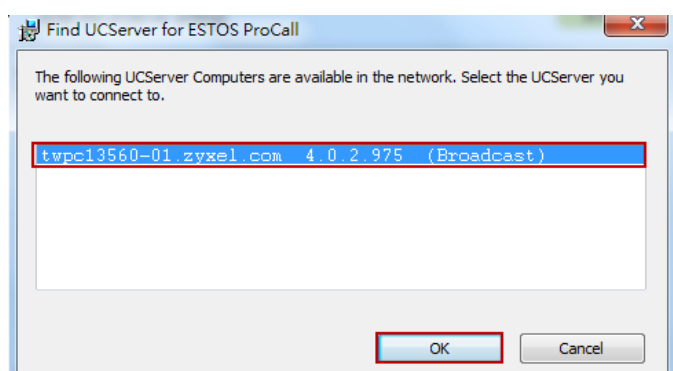
In this scenario, the ISG TAPI driver is installed on the UC server. Hence, select “Do not install a Tapi driver” in this step.



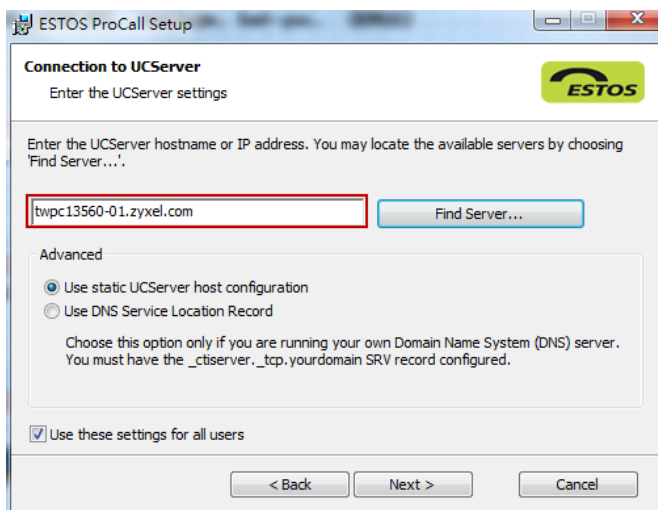
Click on "Find Server..." to select the UC Server you are connecting to.



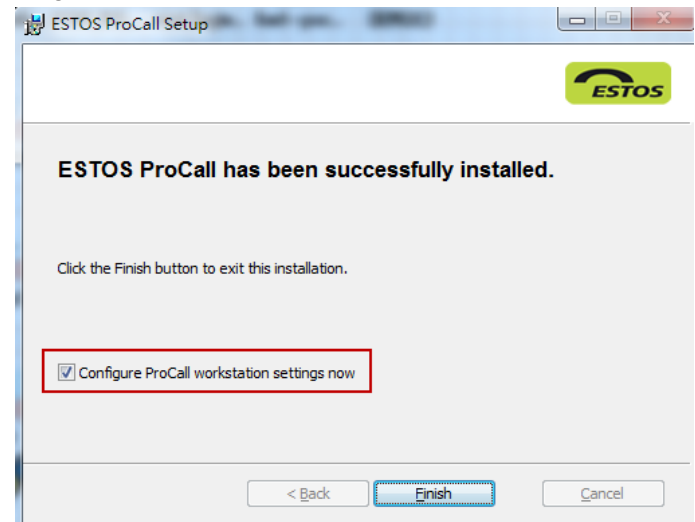
Find your UC Server and click "OK" to confirm.



Click “Next” to proceed to the next step.



ESTOS UC client has been successfully installed. Check the box to configure ProCall workstation.



Configure the username and the password. This is one of the accounts configured in the “User” list on UC server.

ProCall Workstation settings

User login
Please enter the login data for the user

User login

Specify the UC Server user login

☐ Use Windows user name [Emily] as login
☒ Use individual login

User name
barbara

Password
●●●●●●●●

Example: someone@ctide
Emily

Fill in the user’s personal information.

ProCall Workstation settings

User settings (barbara)
Additional settings for this user

General user information

Please enter the general user information.

User name (login) barbara

Identity sip:barbara@zyxel.com

First name barbara

Last name

Display name barbara

E-Mail address

Password ●●●●●●●●

Repeat password ●●●●●●●●

Fill in detailed information of this user.

ProCall Workstation settings

User settings (barbara)
Additional settings for this user

Contact details

Please enter your contact details and add a photo.

Company: ZyXEL

Job title: Support Engineer

Room number:

Street and number: No.2 Gongye E 9th Rd. Science Park

Post code and city: 300 Hsinchu

State:

Country: Taiwan

Website:

Click the “Select” button to associate a phone number to this user.

ProCall Workstation settings

User settings (barbara)
Additional settings for this user

Telephone numbers

Please enter the phone numbers of the user:

Work phone: [Select...]

Work phone 2: [Select...]

Private phone:

Mobile phone:

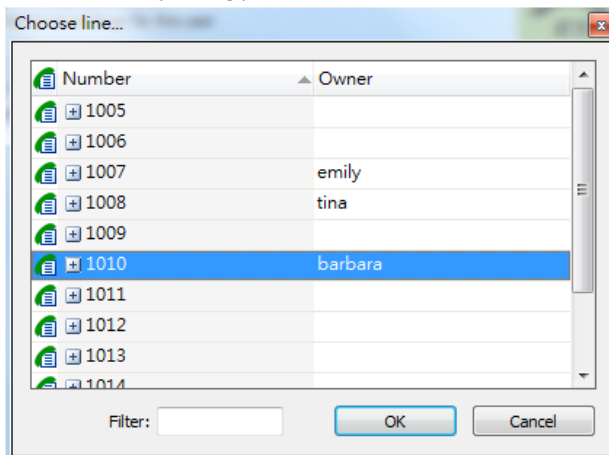
Voicemail:

Recording server:

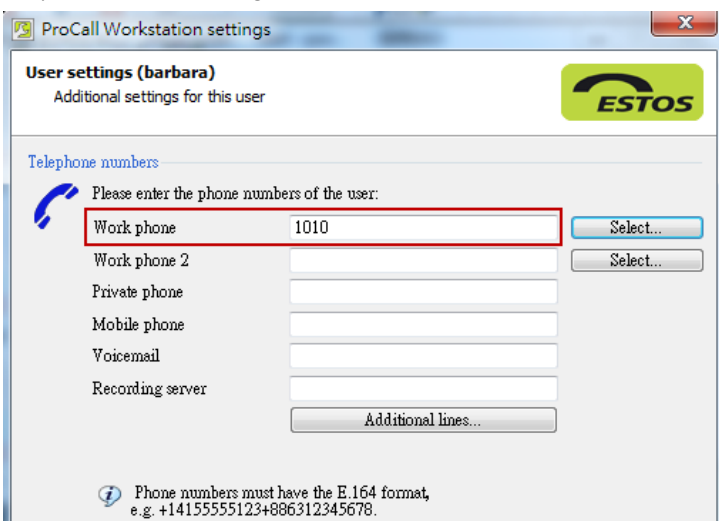
Additional lines...

Phone numbers must have the E.164 format,
e.g. +14155555123+886312345678.

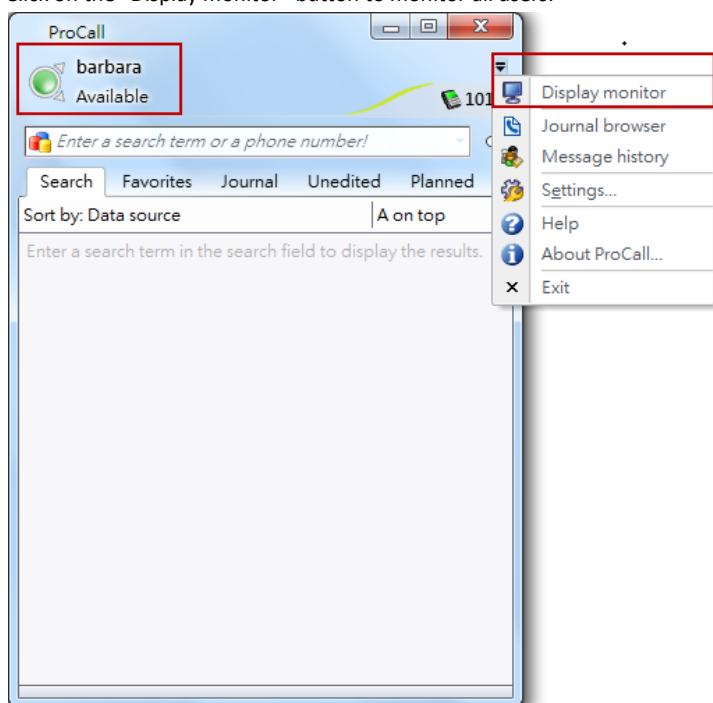
Select the corresponding phone number for this user.



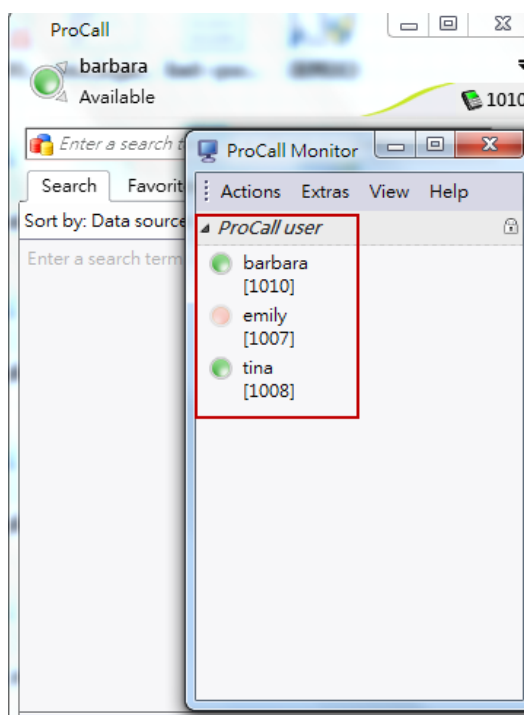
The phone number is configured.



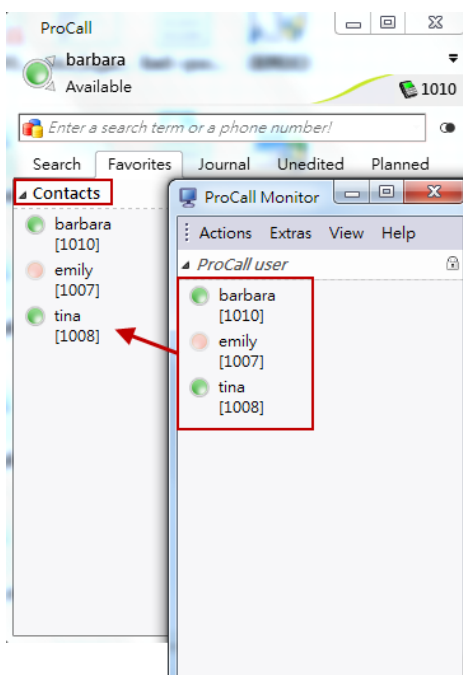
Launch the ESTOS ProCall application. Log in with the username and password.
Click on the "Display monitor" button to monitor all users.



Here is the list of all users

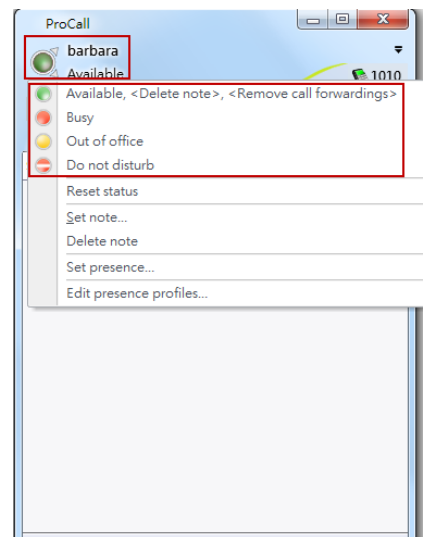


You can drag all ProCall users into “Contacts”.



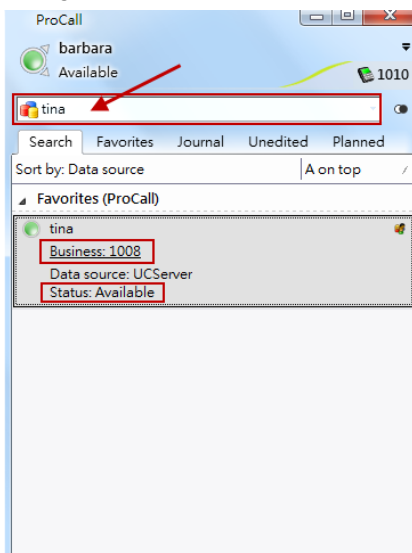
Presence

The status button shows the status of the user. In “Contacts”, you can check the status of each user. The presence can let you know if the user you’d like to call is available at that moment.

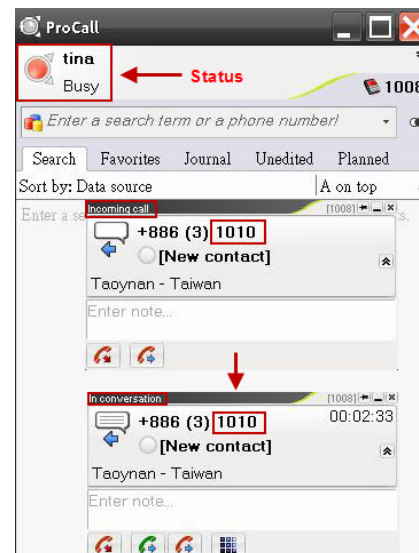


Make a call

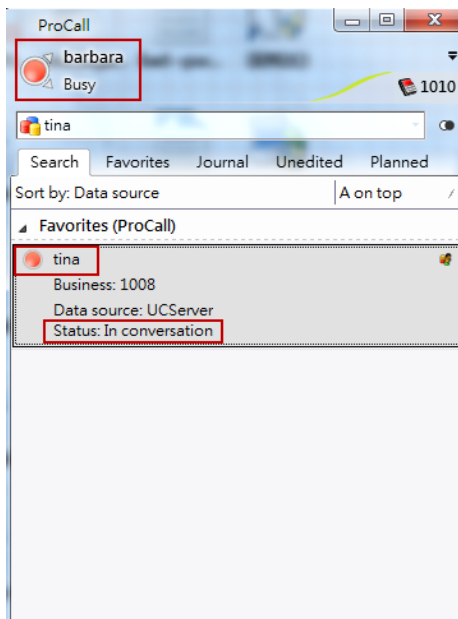
You can make a call by directly clicking on the user in the “Contacts” or by typing a phone number in the blank. In this example, barbara is making a call to tina.



When tina gets the incoming call, a notification window will pop up and the status button will flash. When tina picks up the phone, the notification window will become “In conversation”.

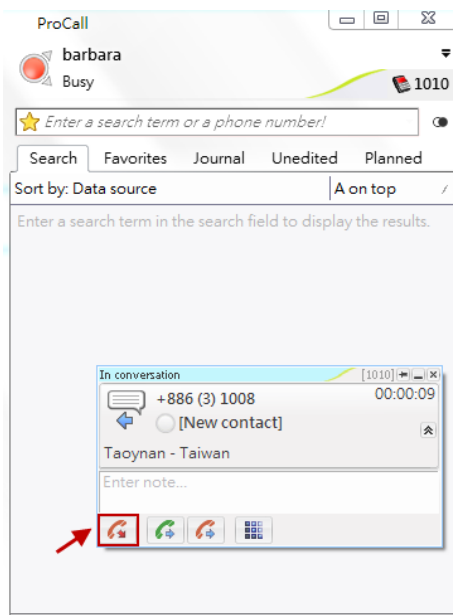


When barbara is taking with tina on the phone, the presence is “Busy” and the status of tina is “In conversation”.



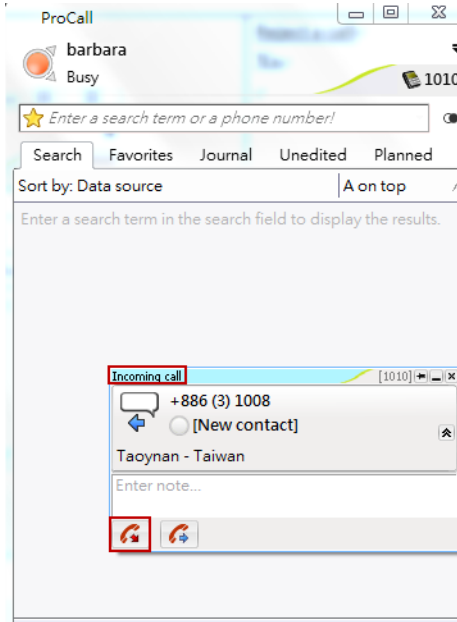
Hang up a call

Click on the button to hang up the call.



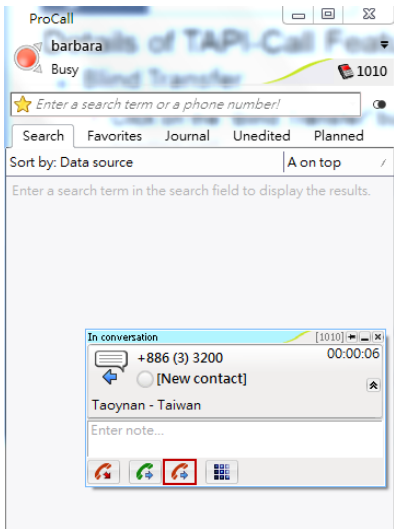
Reject a call

Click on the "Reject" button to reject a call.

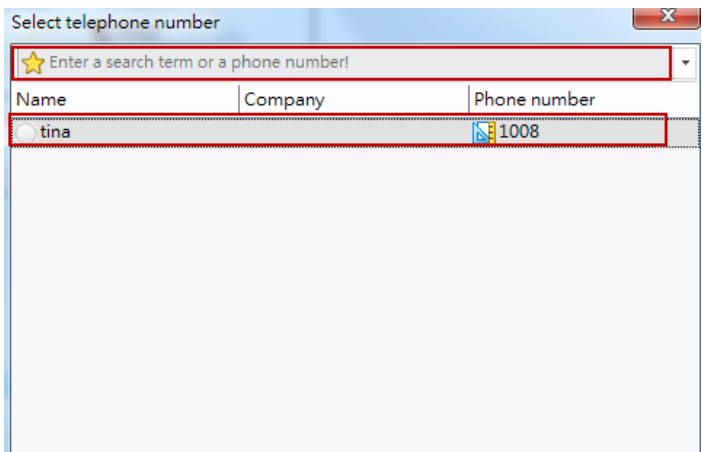


Blind Transfer

Click on the “Blind Transfer” button (Ctrl+W) to transfer an existing call.

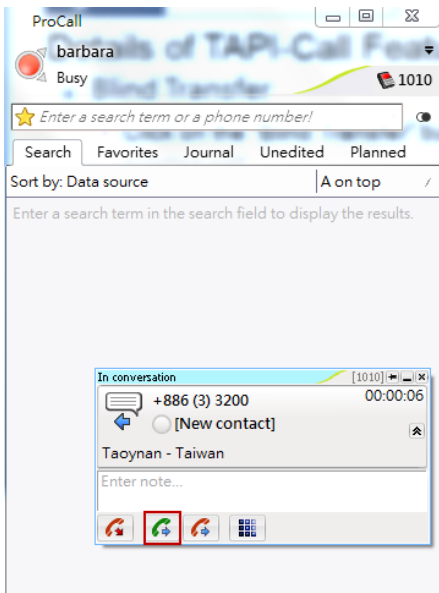


Type a phone number in the blank or click on the phone number in the list to blind transfer the call to this number. In this example, barbara gets a call from extension 3200 and then blind transfers this call to tina.

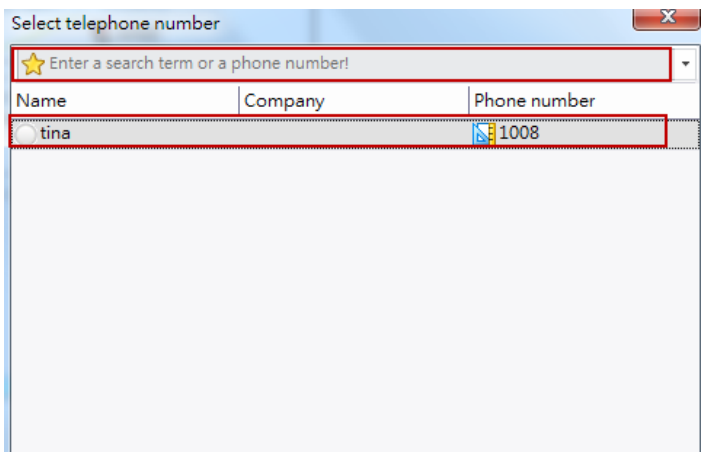


Consultant Transfer

Click on the “Consultant Transfer” button (Ctrl+R) to transfer an existing call.

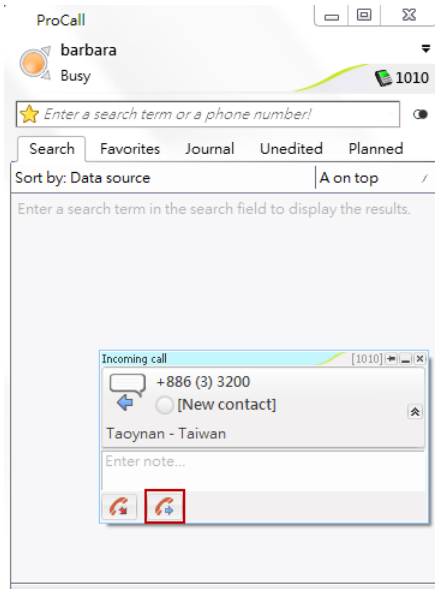


Type a phone number in the blank or click on the phone number in the list to consultant transfer the call to this number. In this example, barbara gets a call from extension 3200 and then consultant transfers this call to tina.



Redirect a call

Before you answer the call, you have an option to redirect the incoming call to another extension.



Type a phone number in the blank or click on the phone number in the list to consultant transfer the call to this number. In this example, barbara gets a call from extension 3200 and then redirects this call to tina.

