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?

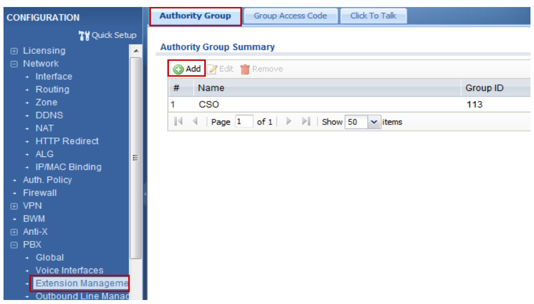
Initial Setup

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.

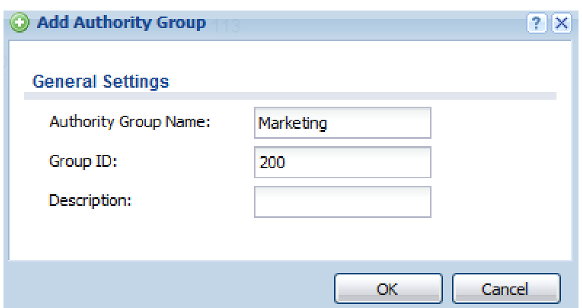
<u>Create Extensions</u>

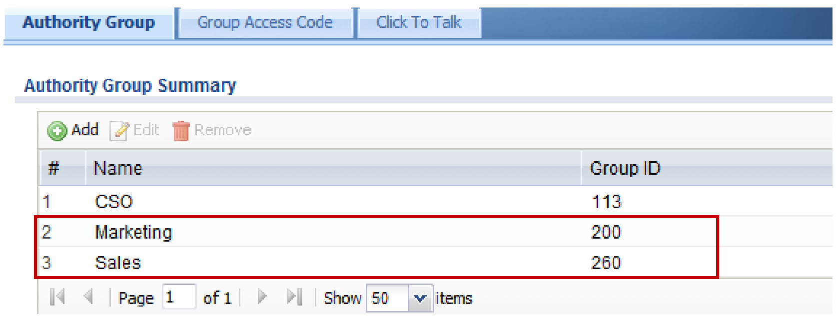
Goal to achieve: Create two authority groups for Marketing department and Sales department, and add 5 extensions in Marketing department.
Condition:
Authority Group: Marketing and Sales
Extensions for Marketing: 3100-3104 Pin Code for Marketing: 3100-3104; Password for Marketing: 53100-53104

First, add authority groups for departments.



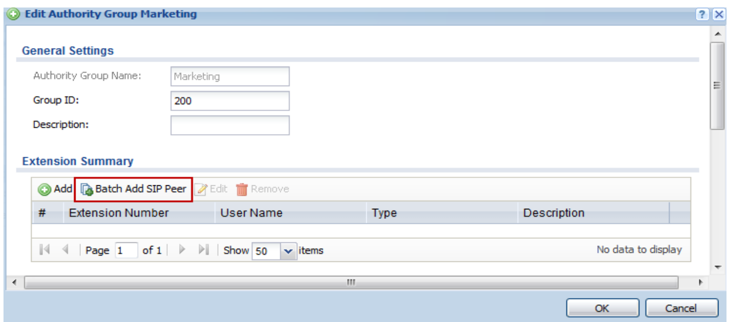
Create two authority groups and fill in “Marketing” and “Sales” as the authority group names.




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.

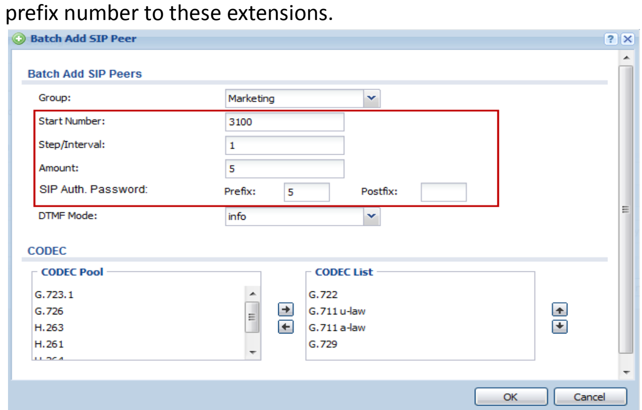
Here, we add multiple SIP peers.



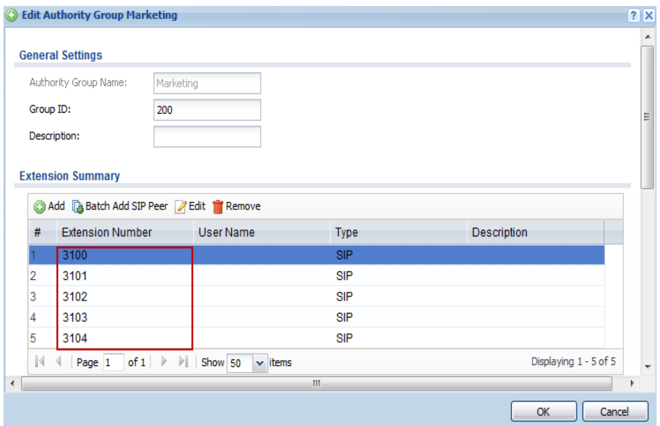
Define the start number and the amount of extensions.

Here, we set 3100 as the start number.

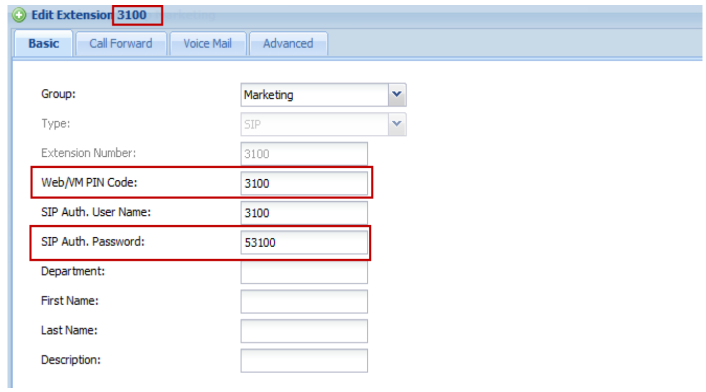
The passwords for these SIP peers are the same as the extension numbers. In order to make the password more secure, we add a prefix number to these extensions.



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



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



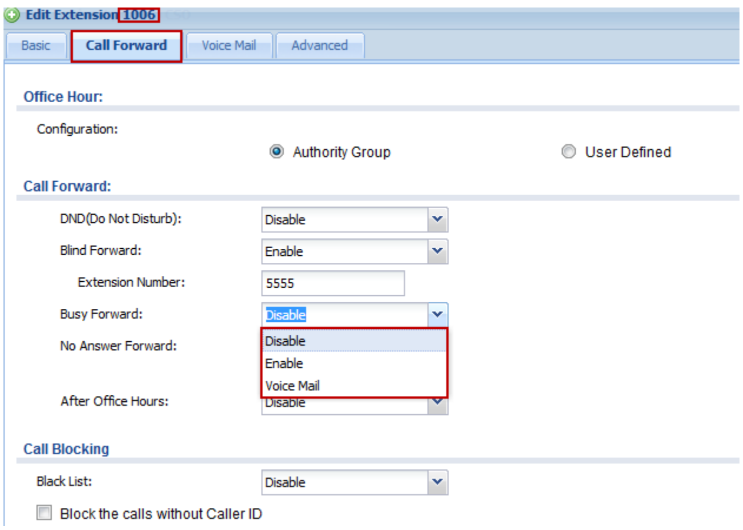
How to configure call forwarding for each extension?

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.



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.

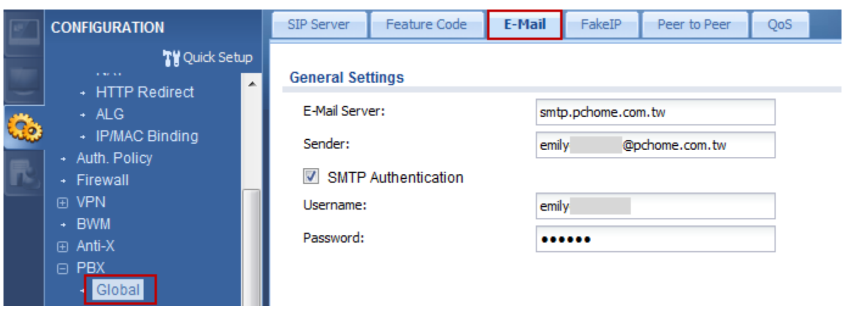
Block the calls without Caller ID: You can block the incoming calls which are without call ID.

How to receive and check the voice mail?

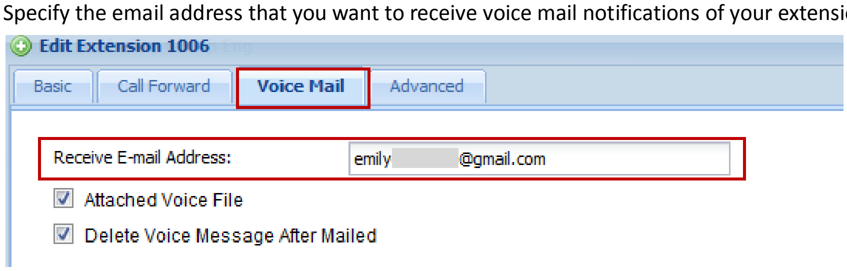
Goal to achieve: Extension 1006 would like to receive voicemail notification with the voice file in the email box.

Condition: Extension 1006

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

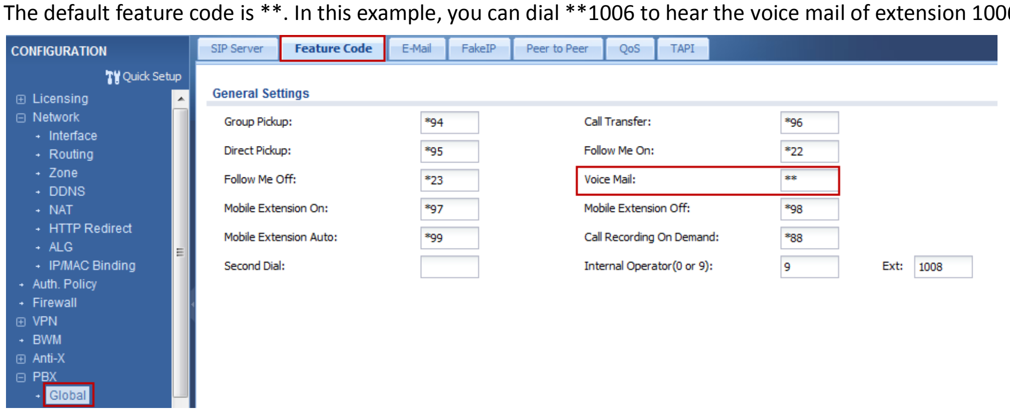


Specify the email address that you want to receive voice mail notifications of your extension.



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

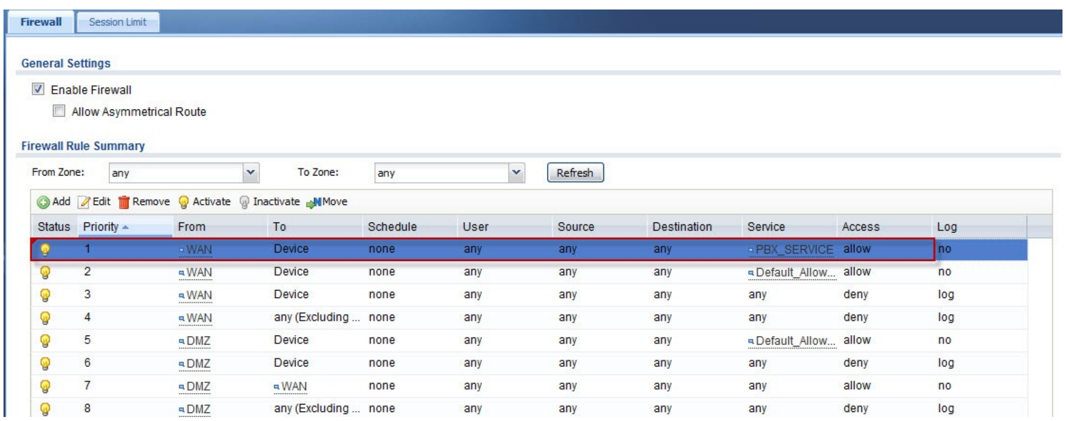
If the voice message is not attached in the notification mail, you can dial the feature code and the extension number to hear the voice message. The default feature code is **. In this example, you can dial **1006 to hear the voice mail of extension 1006.



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

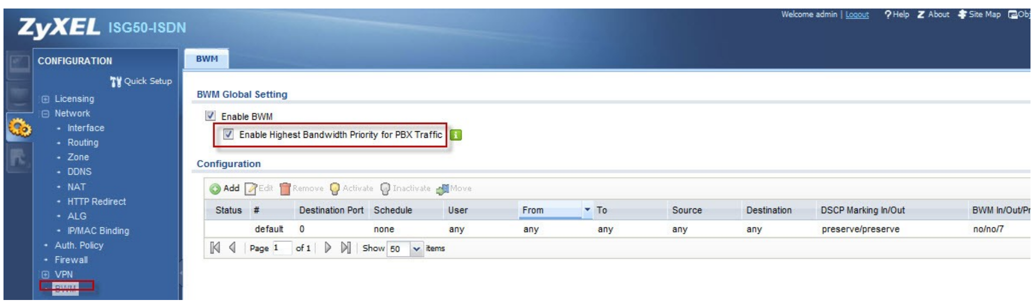
By default, ISG50 doesn't allow SIP clients to register from the WAN interface. You have to activate the first firewall rule “PBX_SERVICE” to let SIP clients register from the WAN interface.



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.

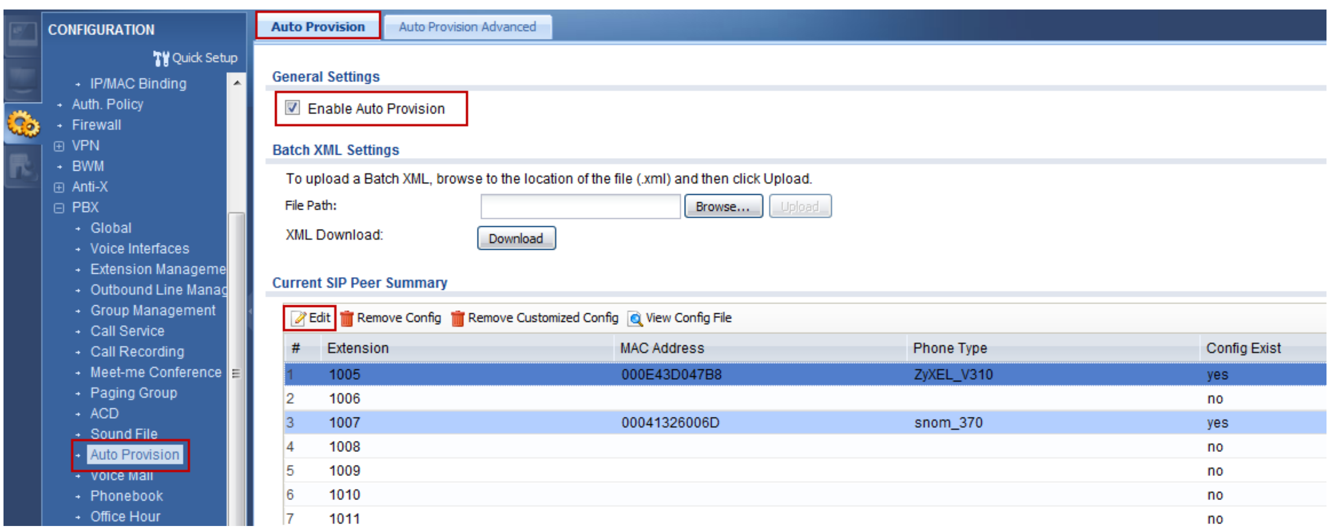
Auto Provision

SIP Server/SIP account/Password

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

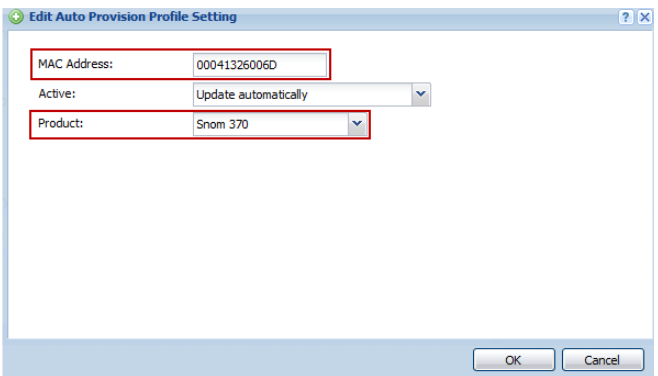
Condition:

V310	***Snom***
Extension: 1005	Extension: 1007

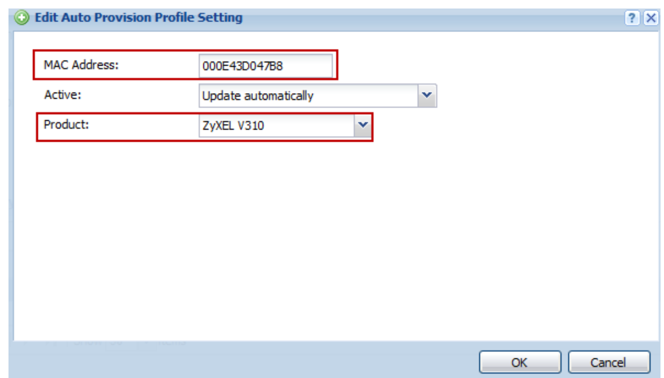


Fill in the MAC address of the IP phone and select the model name from the product list that receives configuration settings from the ISG50 for this extension.

Snom



V310



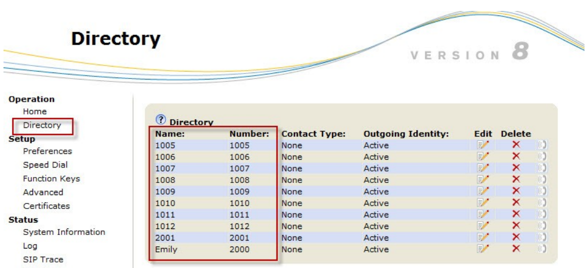
Phone book

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

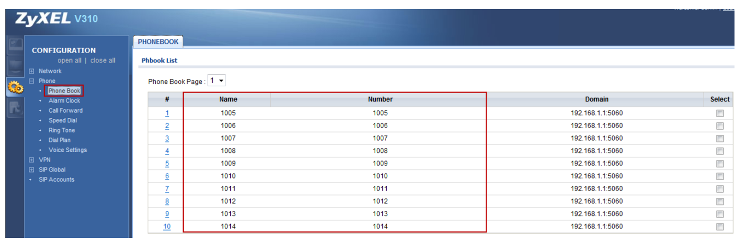
Condition:

Extension number: 1005-1012; 2000-2001

Snom



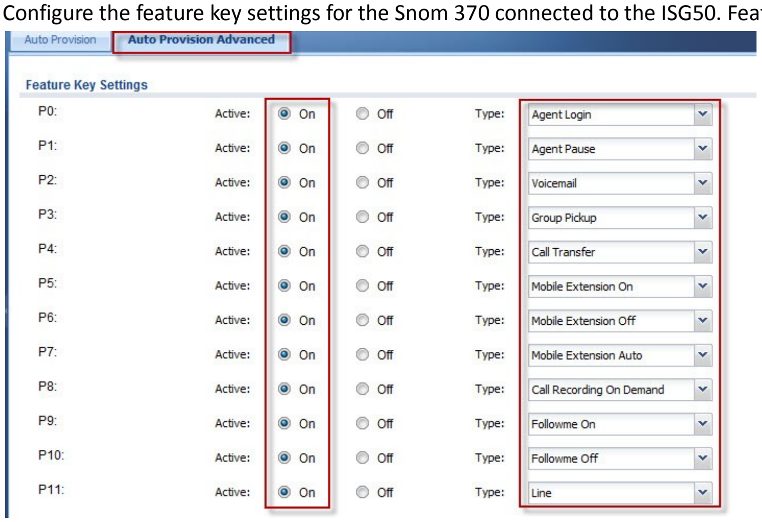
V310



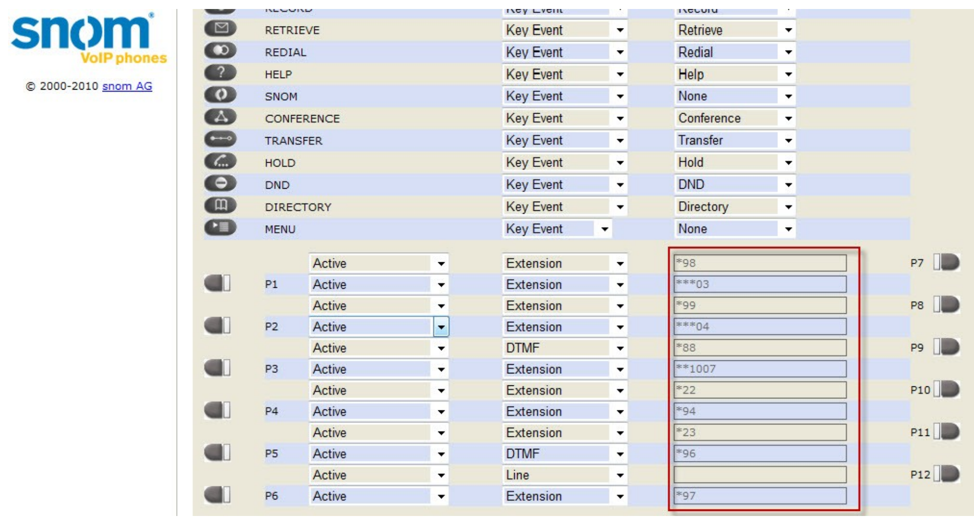
Feature Key

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.



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)



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

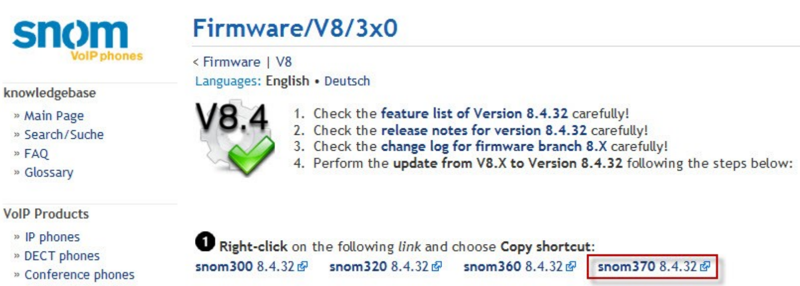
V310 http://10.59.1.37/V310_1.00AABT.0B5

Snom

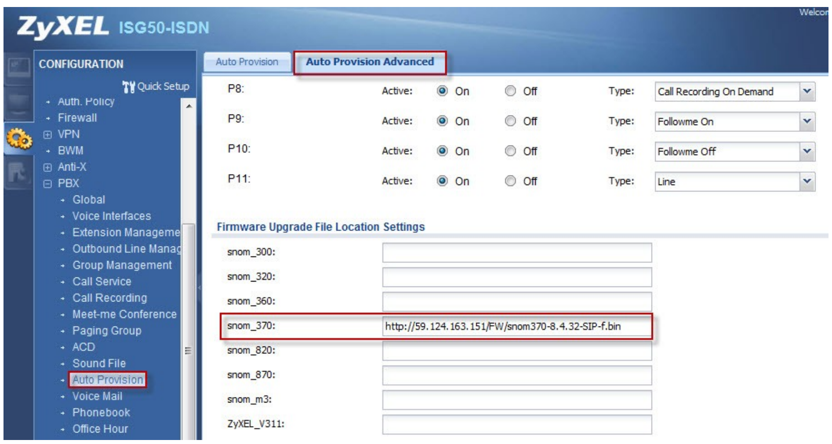
Configure firmware upgrade URLs for the Snom 370.

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

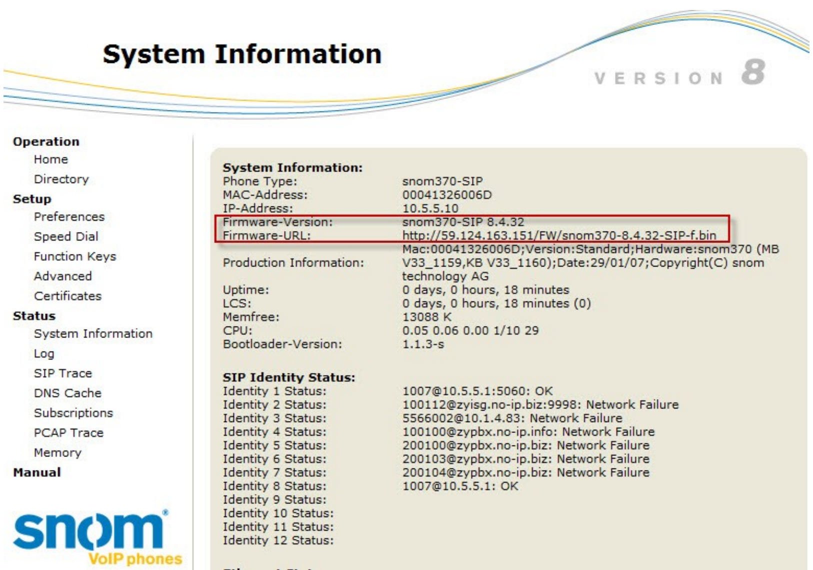
You can either fill in the firmware download link (http://provisioning.snom.com/download/fw/snom370-8.4.32-SIP-f.bin) or put the firmware on another web server.



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

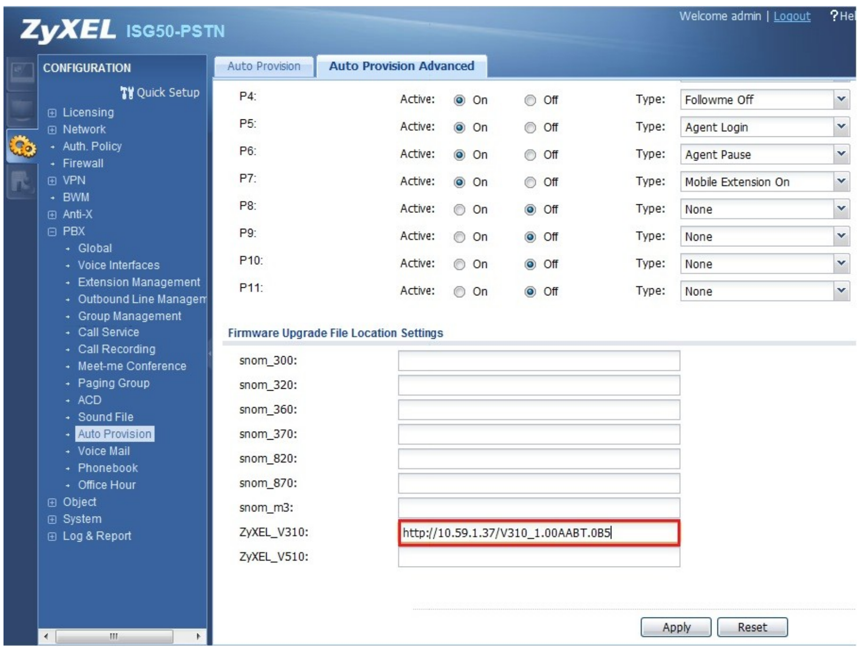


You can log into the GUI of Snom 370 to check if the firmware has been upgraded to target version.

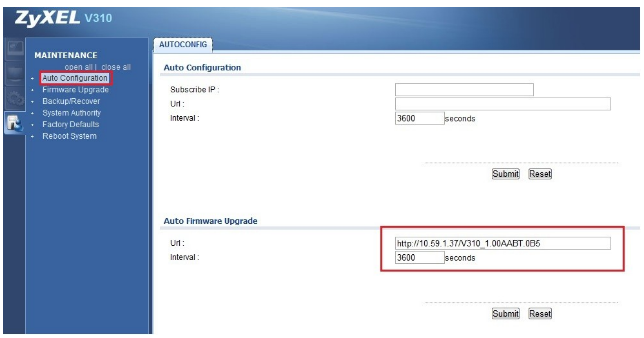


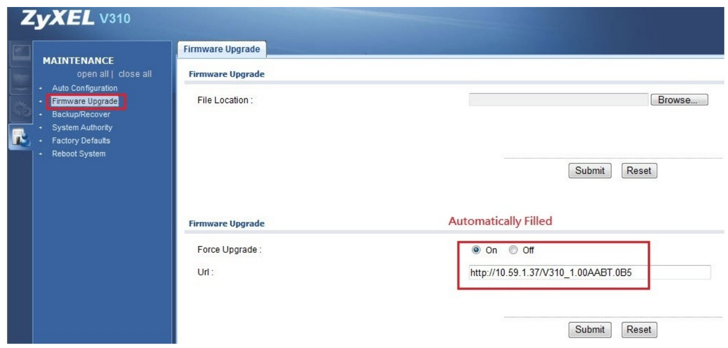
V310

Fill in the firmware download URL.



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.

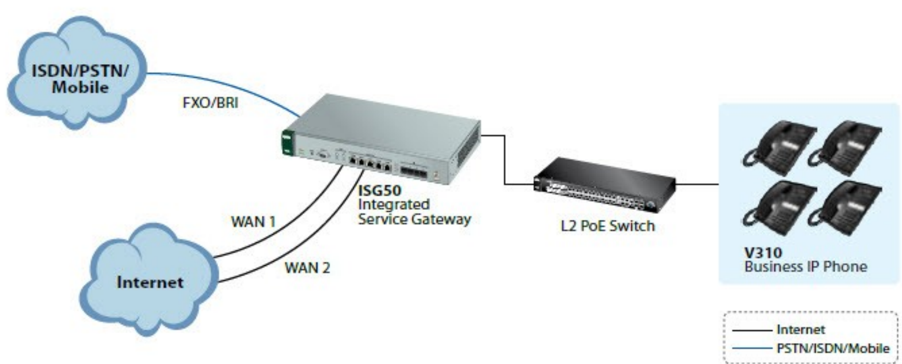




3. How to Develop a Non-stop Voice Service?

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:

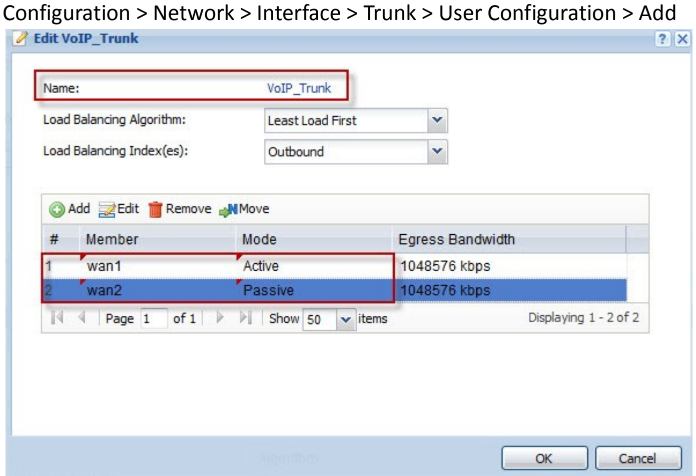
VoIP traffic goes out primarily through WAN1. In case WAN1 is down, it will go out via WAN2.

Condition:

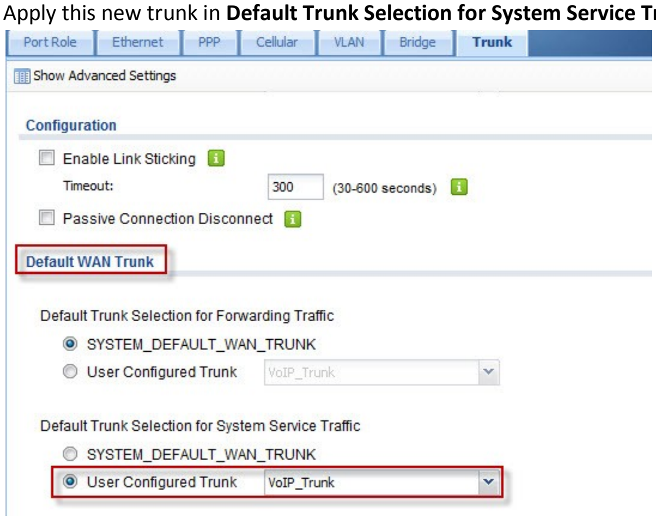
Primary: WAN1; Backup: WAN2

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

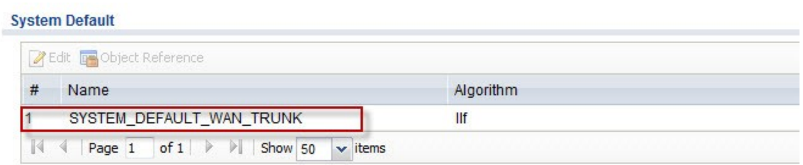
Configuration > Network > Interface > Trunk > User Configuration > Add



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



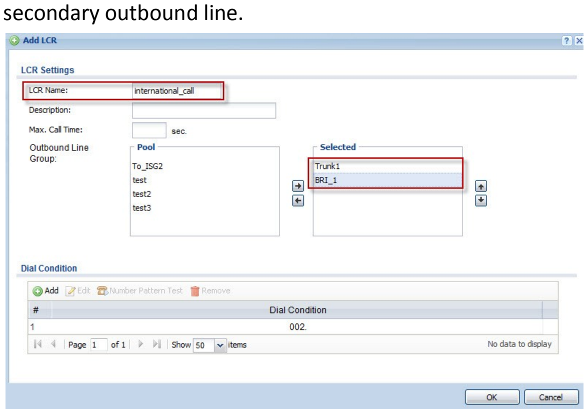
Use **SYSTEM_DEFAULT_WAN_TRUNK** to do load balancing for data traffic.



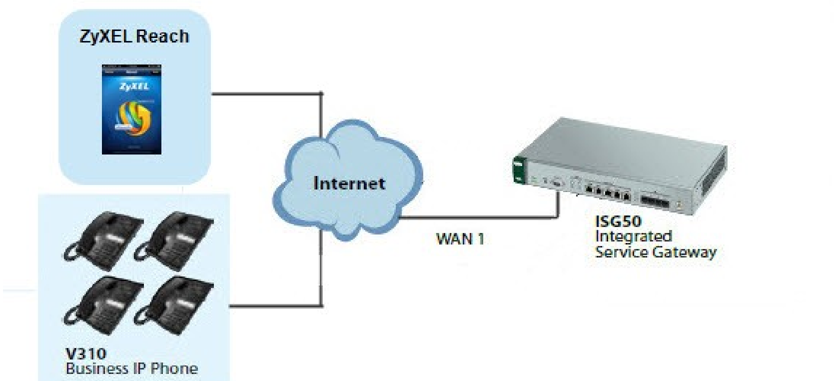
VoIP survivability

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



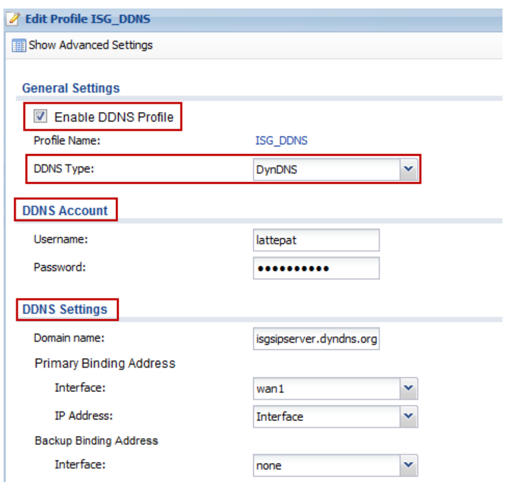
Goal to achieve: IP Phone and mobile client can register to ISG50 with the domain name in case the IP of WAN1 is dynamic.

Condition:

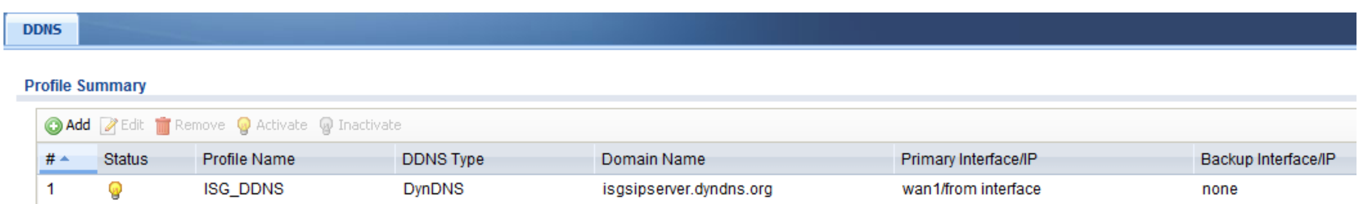
DDNS service provider: DynDNS

DDNS interface: WAN1

Fill in DDNS account information.



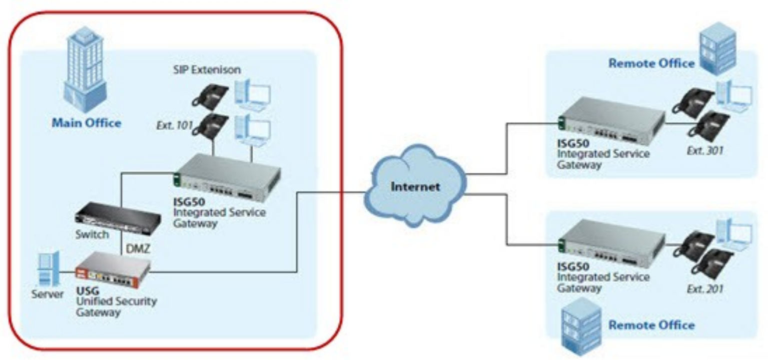
Activate DDNS.



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:

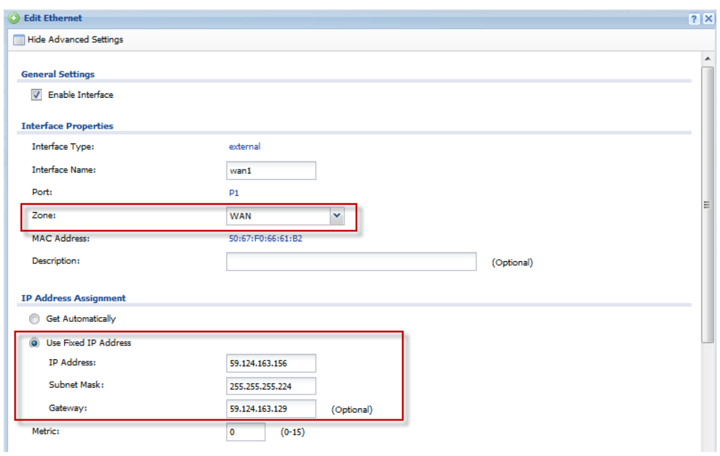
- WAN IP: 59.124.163.156
- SIP server IP (ISG50): 172.16.1.10

ISG50:

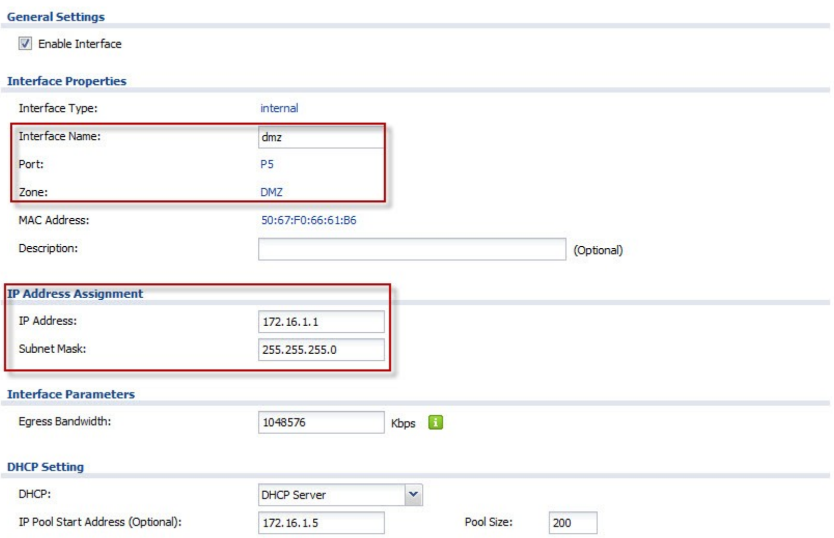
- WAN IP: 172.16.1.10

USG:

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

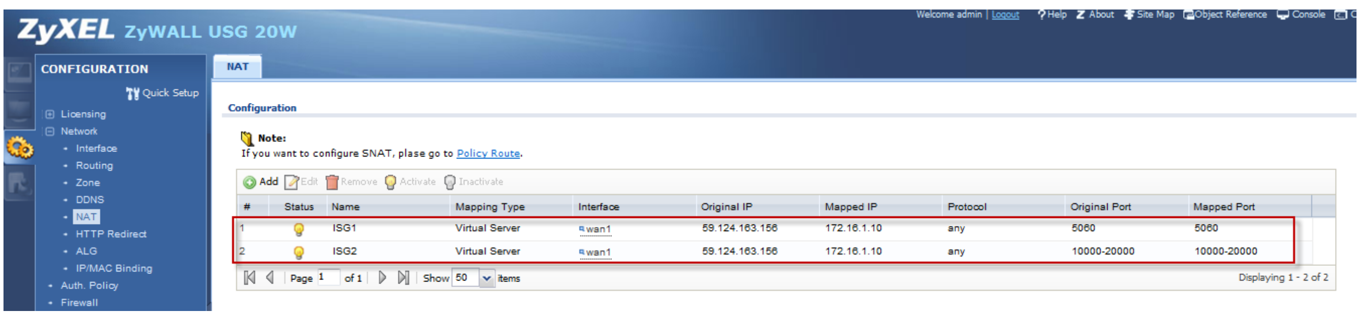


Step 2. Assume ISG50’s WAN port is connected to DMZ (port 5) of USG.
Configure an IP for this interface.

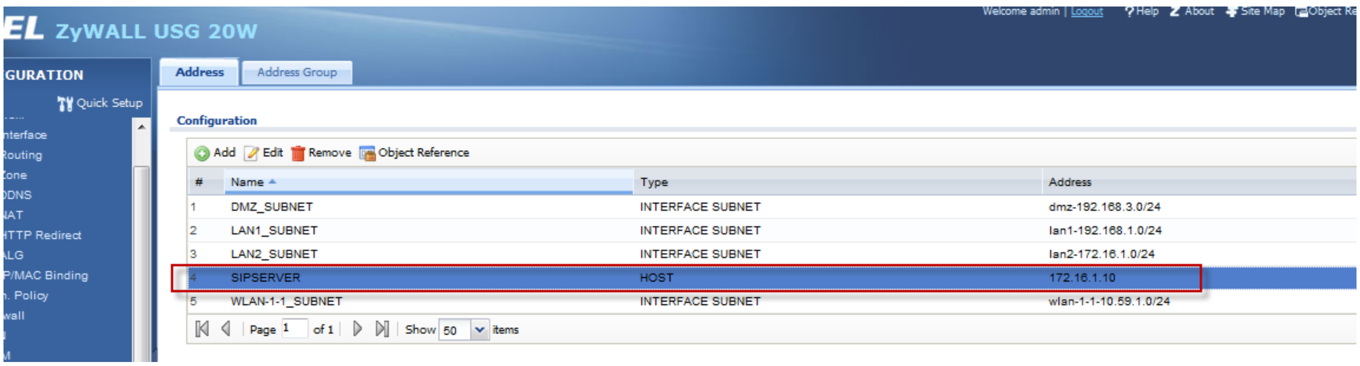


Step 3. For NAT setting, the user needs to configure the following:

- 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.

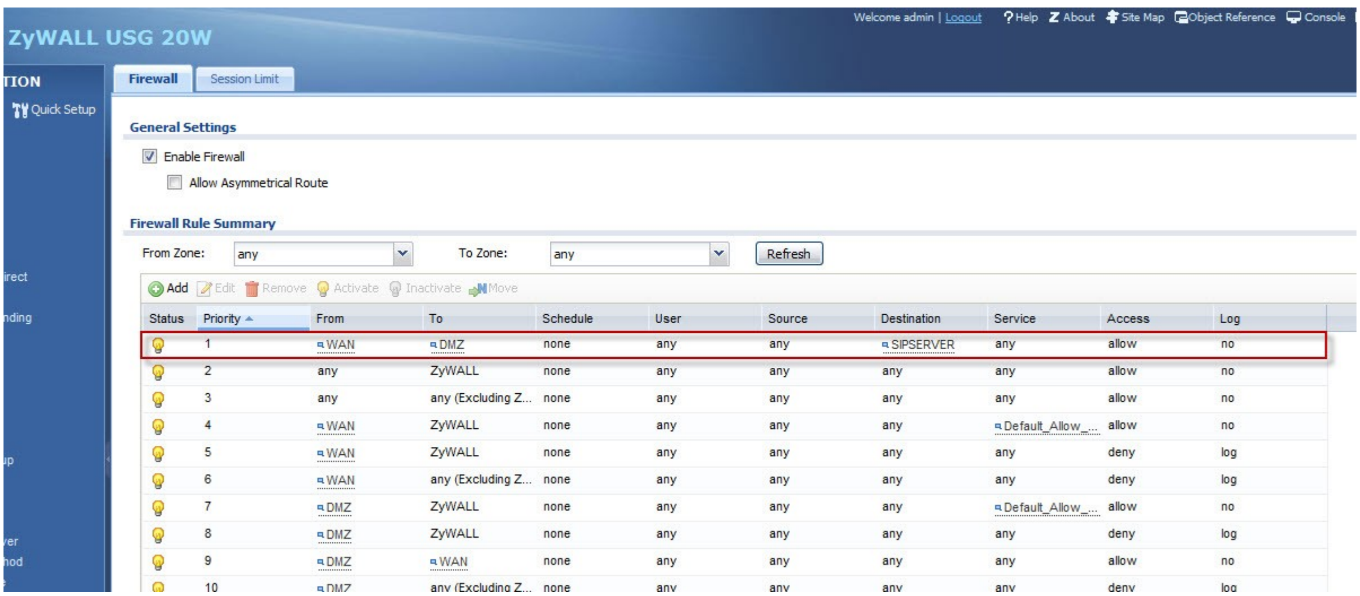


Step 4. The user can create an address object for ISG50 for further configuration usage. Click **Create new object** for this function.

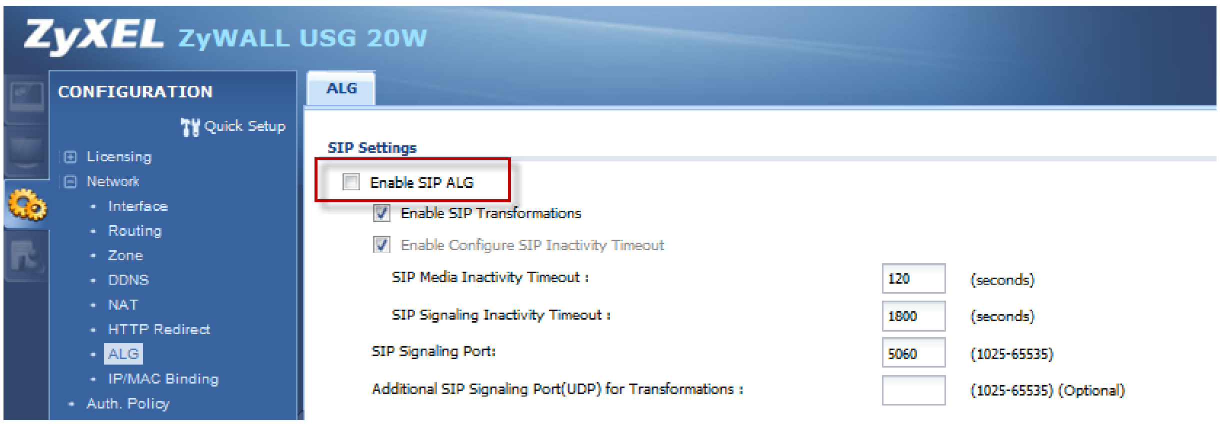


Step 5. Click **CONFIGURATION > Network > Firewall** to open the firewall configuration screen.

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

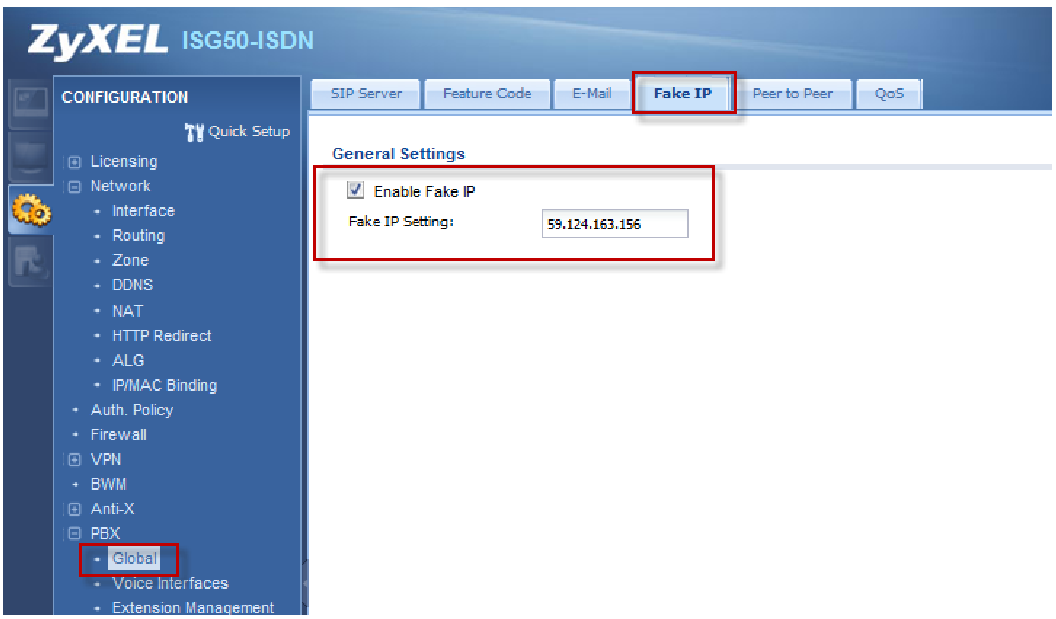


Step 6. Disable SIP ALG.

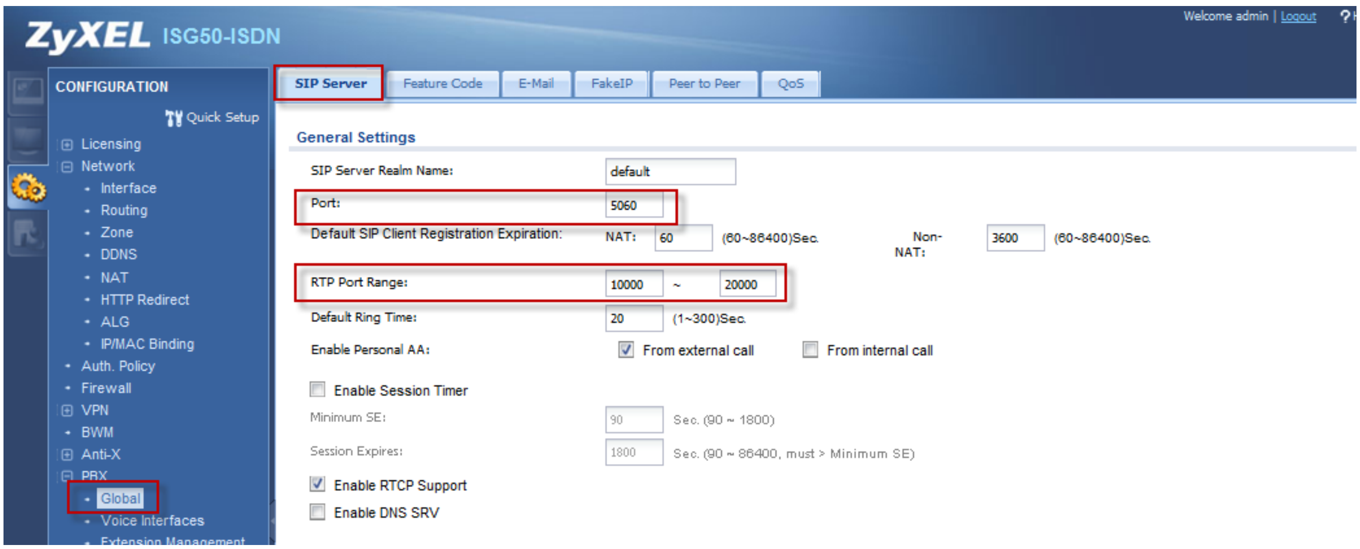


ISG50:

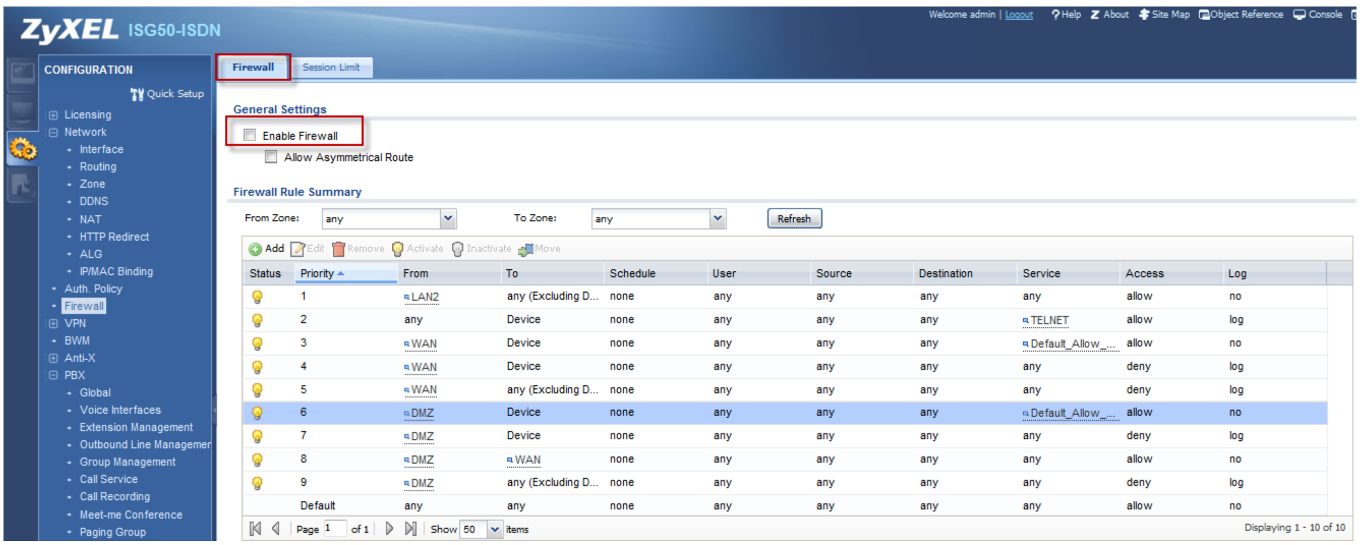
Step 1. Set the WAN IP of USG in the Fake IP field.



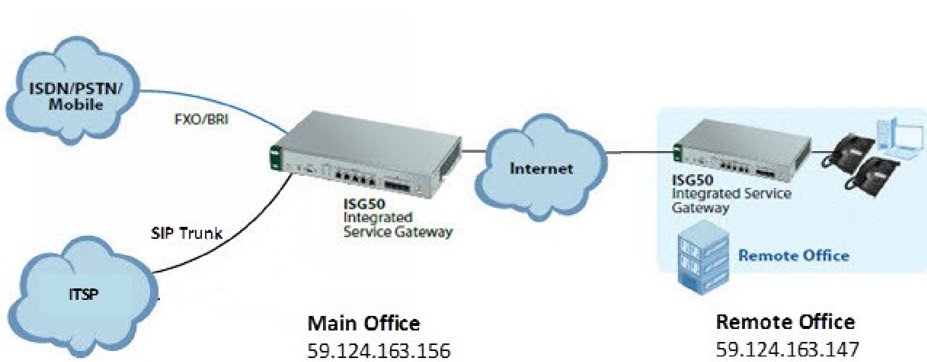
Step 2. Make sure the SIP signaling port and the RTP port range are the same as those you configured in the port forwarding in USG.



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



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):

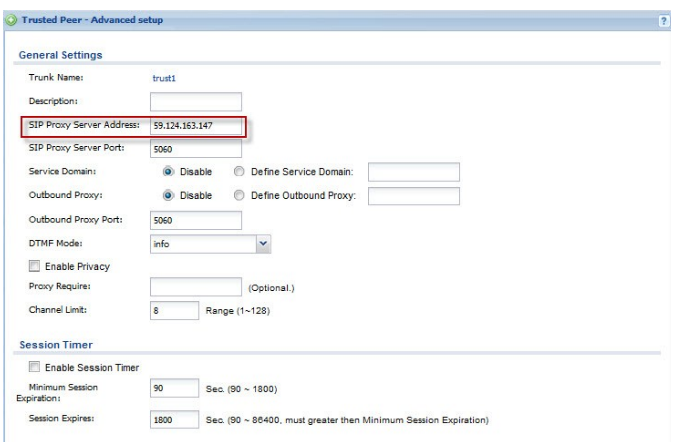
WAN IP: 59.124.163.147

Extension format: 4 digit

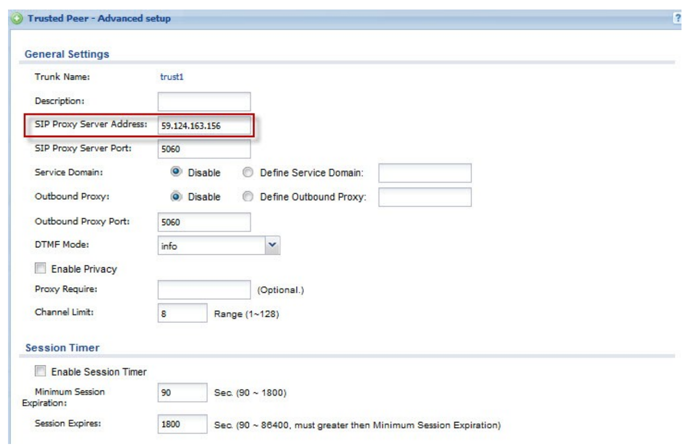
Prefix number before dialing to the main office: 48

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.

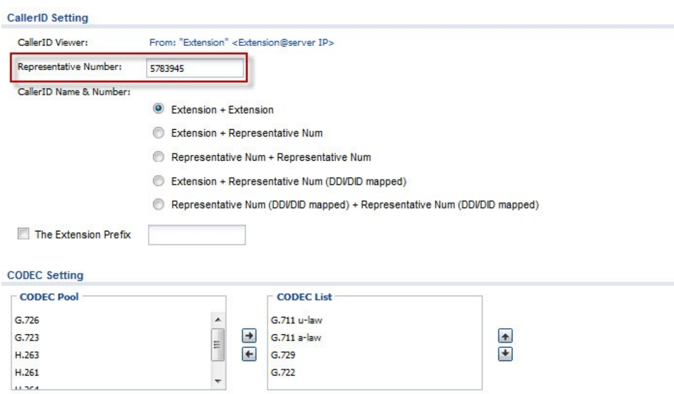
ISG50-1 (Main Office):



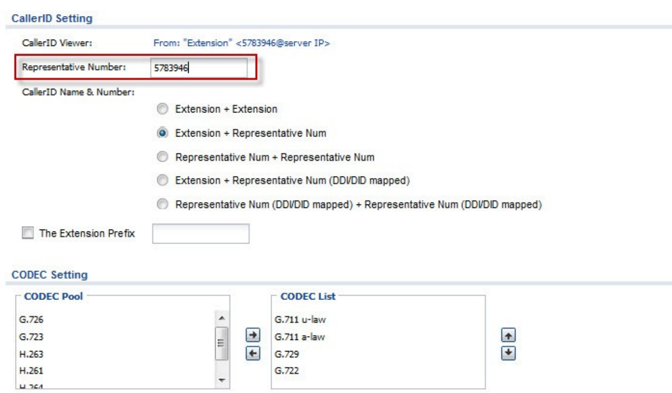
ISG50-2 (Remote Office):



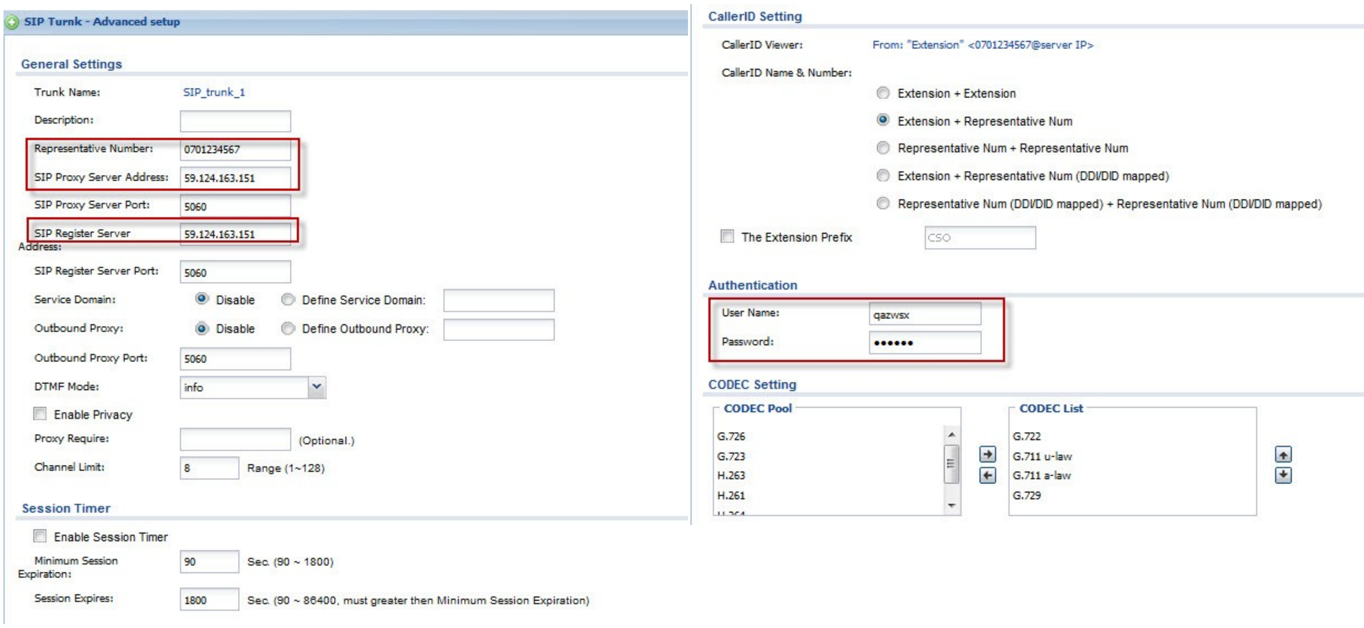
ISG50-1 (Main Office):



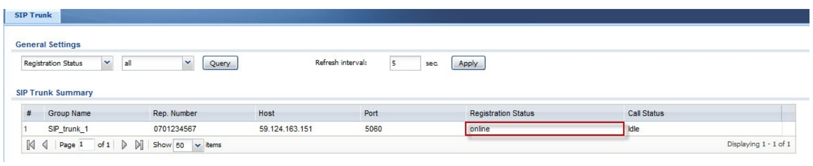
ISG50-2 (Remote Office):



Add a SIP trunk in ISG50-1 (Main Office). The account information is provided by your ITSP.



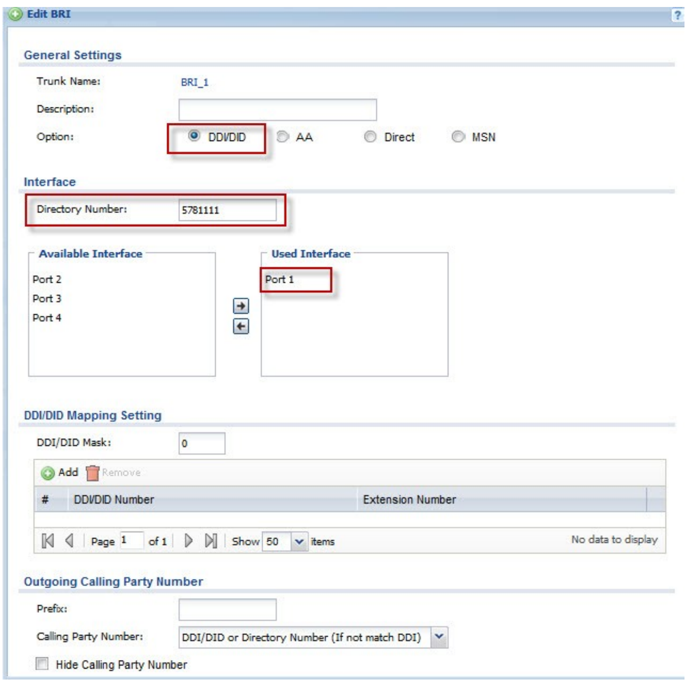
You can check if the registration status is **online** through MONITOR > PBX > SIP Trunk.



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

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

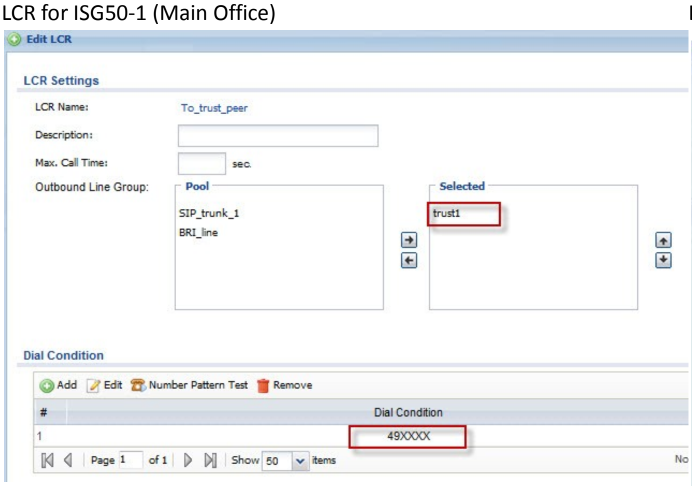
Here, we use DDI/DID as the AA option.



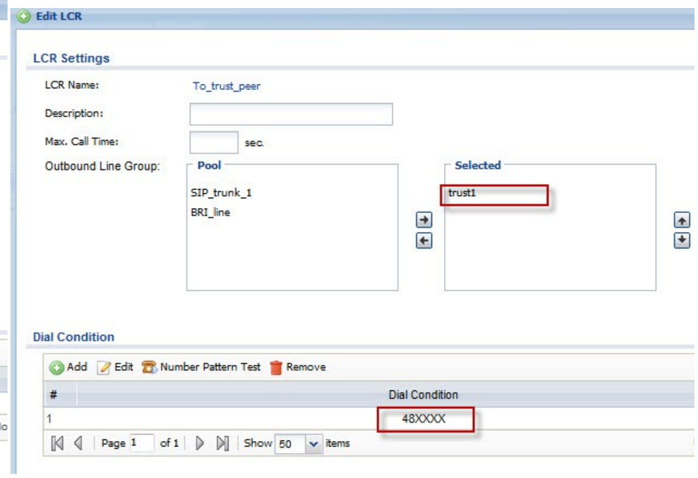
Configure the LCR in both ISG50-1 (Main Office) and ISG50-2 (Remote Office) to let the extensions of ISG50-1 (Main Office) and ISG50-2 (Remote Office) make call to each other over **Trusted Peer**.

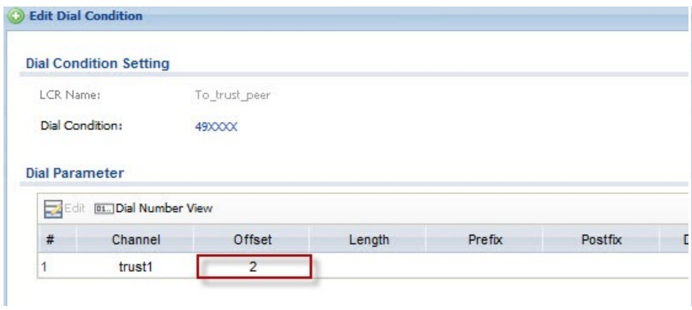
In this example, for extensions in ISG50-1 (Main Office), they need to dial 49XXXX to reach extensions in ISG50-2 (Remote Office). For extensions in ISG50-2 (Remote Office), they need to dial 48XXXX to reach extensions in ISG50-1 (Main Office).

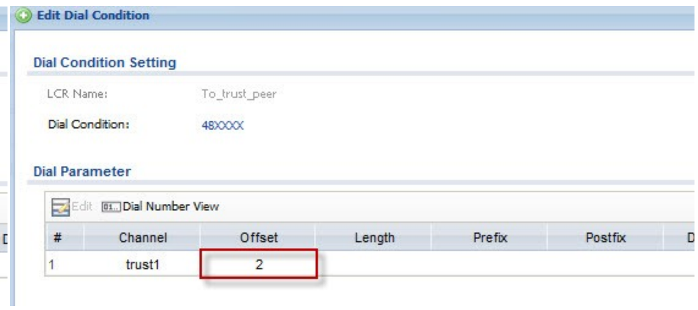
LCR for ISG50-1 (Main Office)



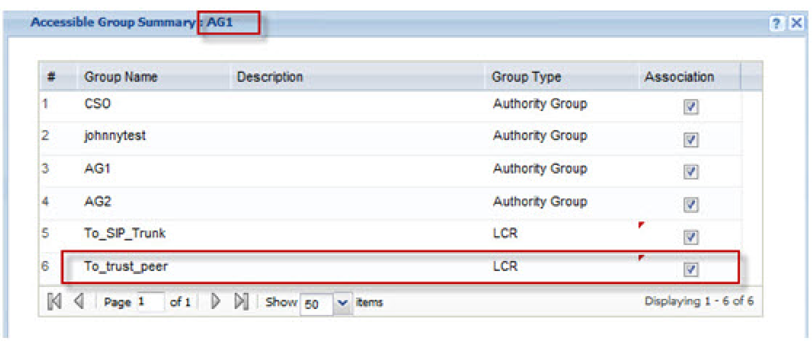
LCR for ISG50-2 (Remote Office)







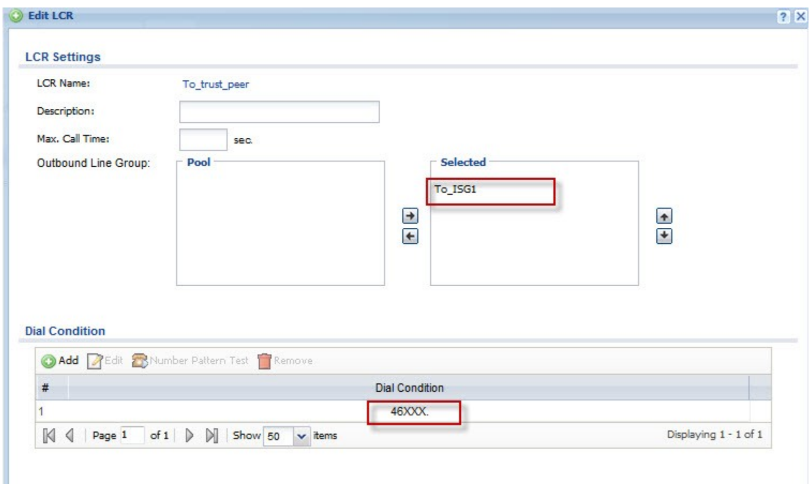
Configure **Group Management** in both ISG50-1 (Main Office) and ISG50-2 (Remote Office).
Associate AGs with LCR.

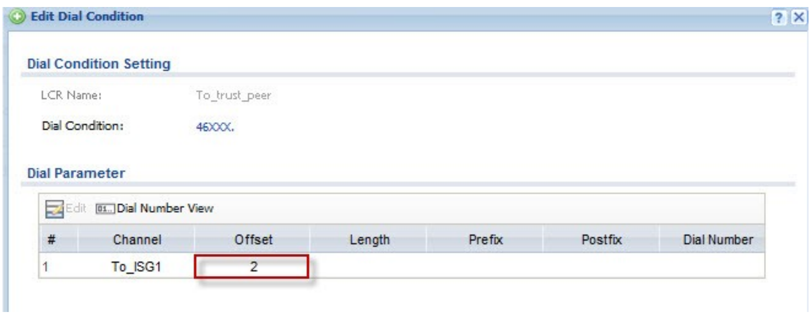


The incoming call on BRI trunk can reach the extension of ISG50-2 (Remote Office) over trusted peer.

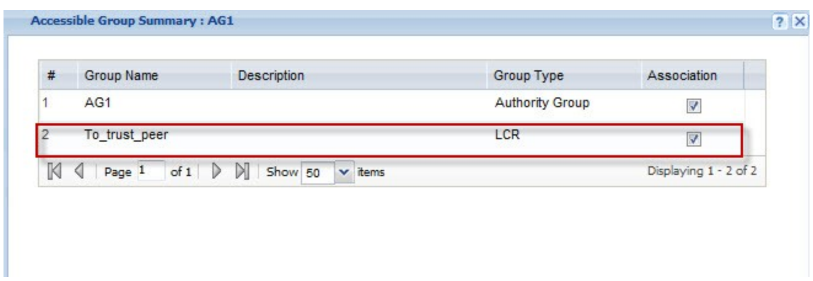
Configure LCR in ISG50-2 (Remote Office).

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”**.

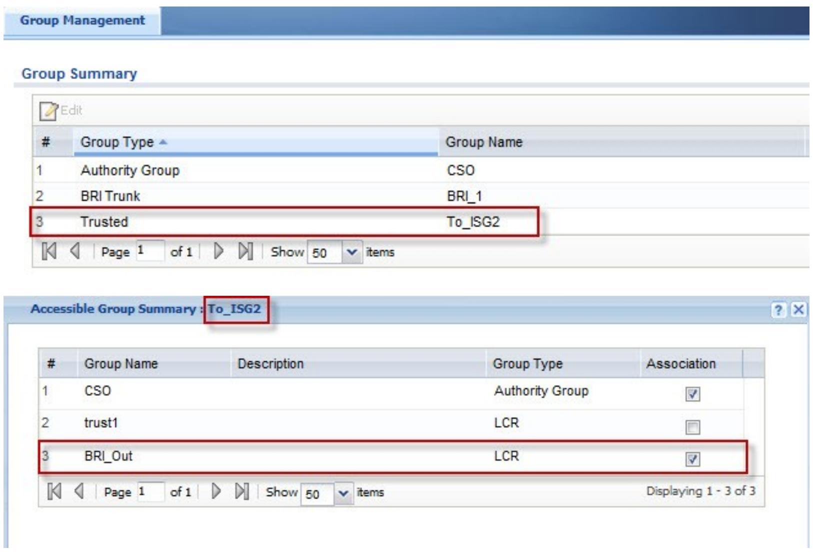




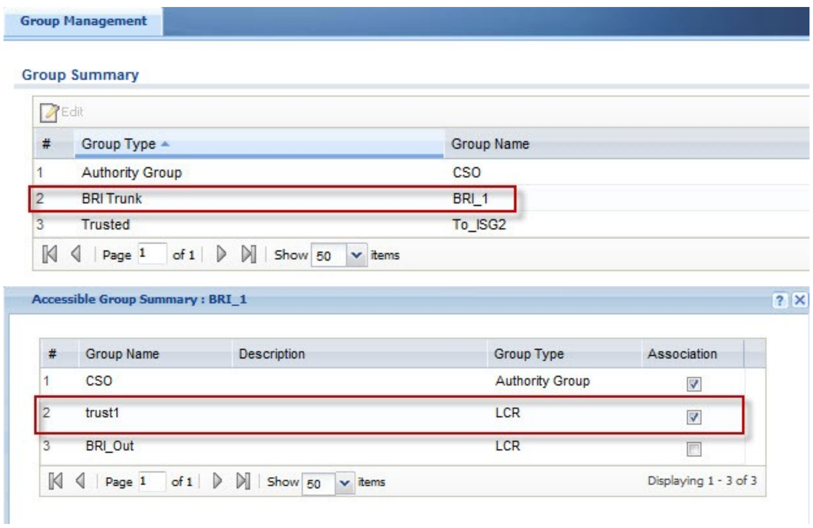
Configure the Group management in ISG50-2 (Remote Office).



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.

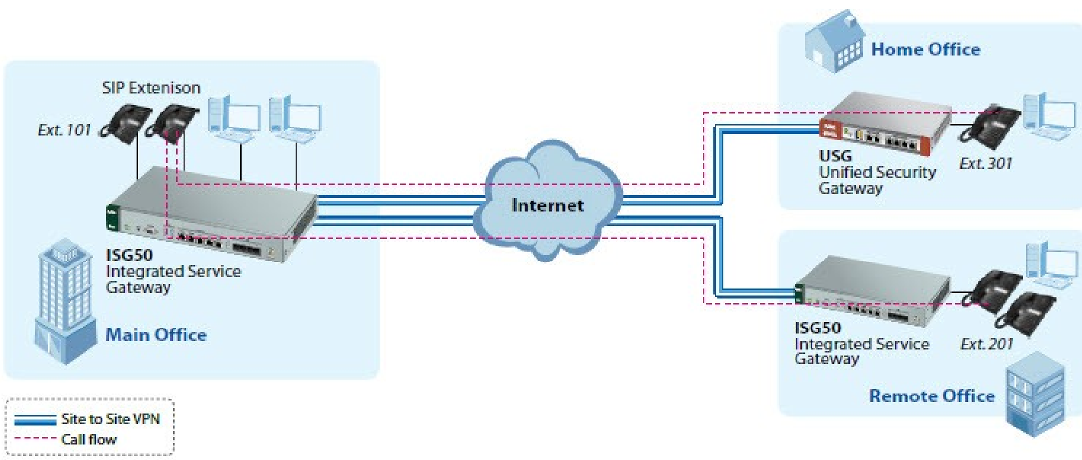


In ISG50-1 (Main Office), to let the incoming call on BRI trunk reach the extension of ISG50-2 (Remote Office) over trusted peer, we need to associate the outbound line (BRI trunk) with the LCR.



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

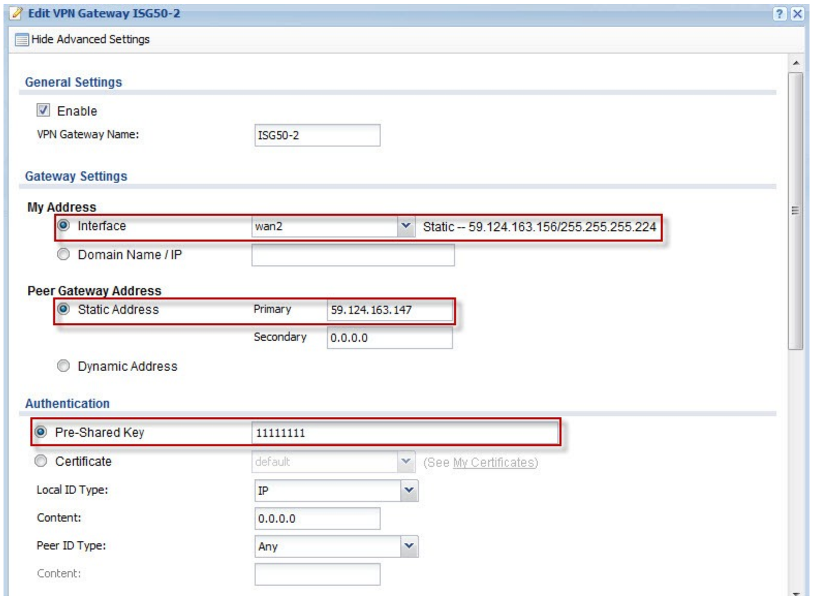
Encryption Algorithm: DES

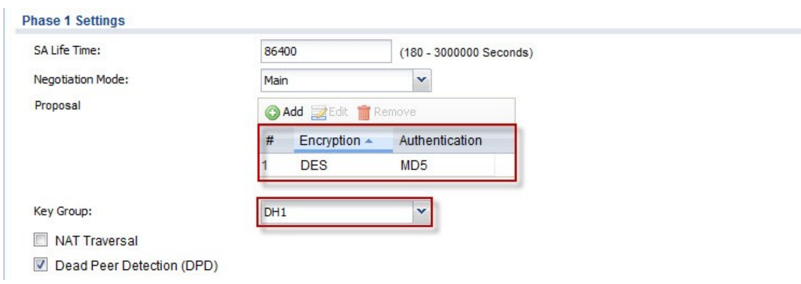
Authentication Algorithm: SHA1

Perfect Forward Secrecy (PFS): None

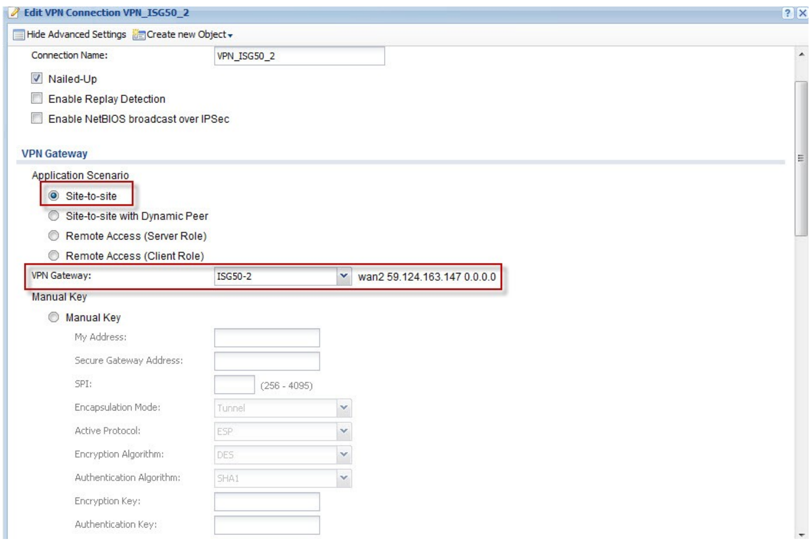
ISG50-1 (Main Office):

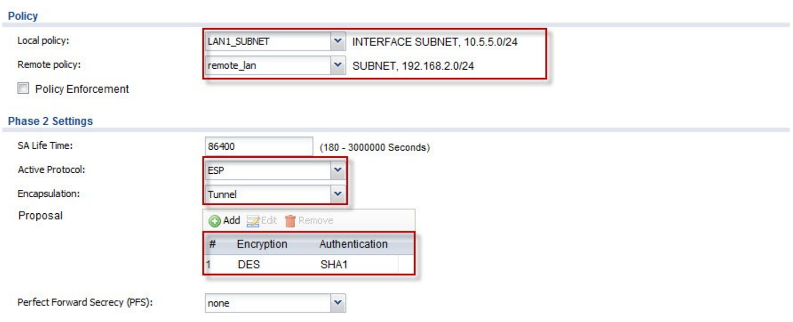
Add a VPN gateway rule.




Phase 1 Settings
SA Life Time:
86400
(180 - 3000000 Seconds)
Negotiation Mode:
Main
Proposal
Add
Edit
Remove
#
Encryption
Authentication
1
DES
MD5
Key Group:
DH1
NAT Traversal
Dead Peer Detection (DPD)

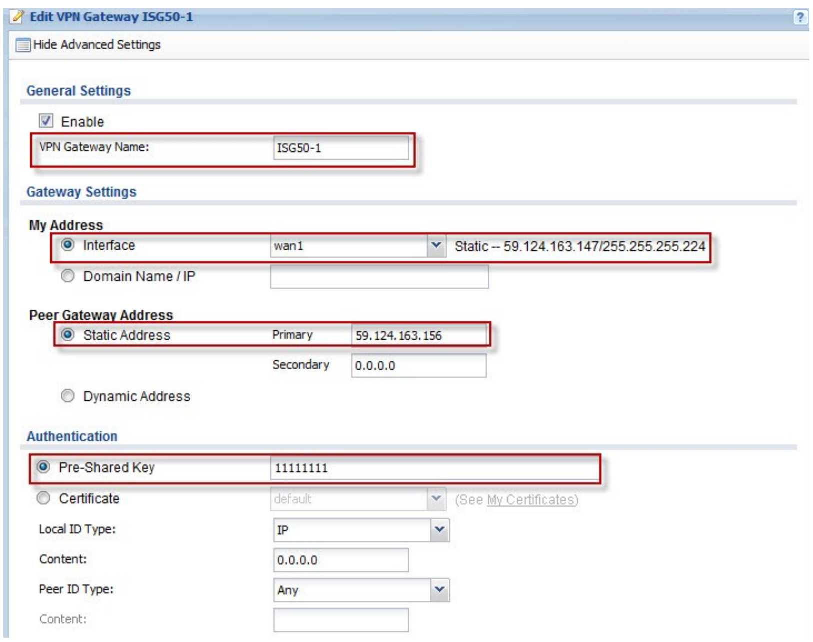
Click **CONFIGURATION > VPN > IPsec VPN > VPN Connection** to configure the phase-2 rule.

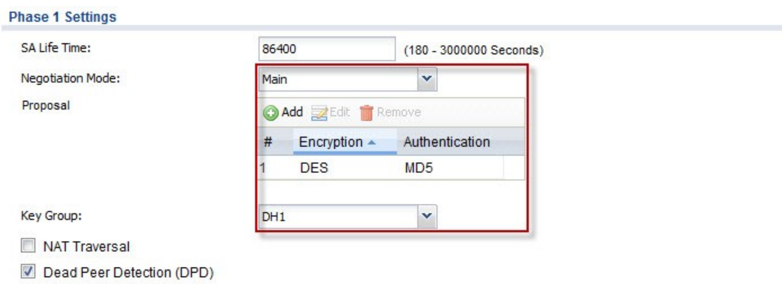



Policy
Local policy:
LAN1_SUBNET
INTERFACE SUBNET, 10.5.5.0/24
Remote policy:
remote_lan
SUBNET, 192.168.2.0/24
Policy Enforcement
Phase 2 Settings
SA Life Time:
86400
(180 - 3000000 Seconds)
Active Protocol:
ESP
Encapsulation:
Tunnel
Proposal
Add
Edit
Remove
Encryption Authentication
1 DES SHA1
Perfect Forward Secrecy (PFS):
none

ISG50-2 (Remote Office):

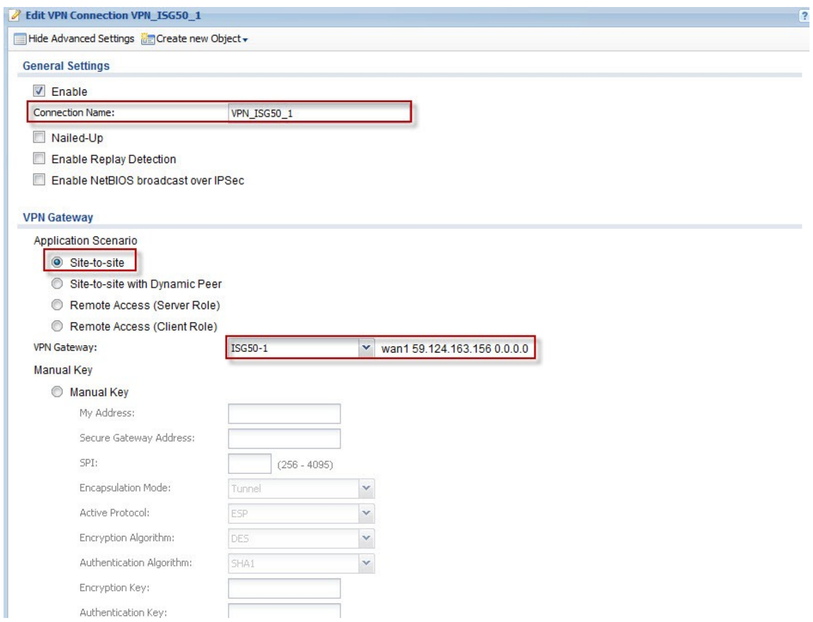
Add a VPN gateway rule.

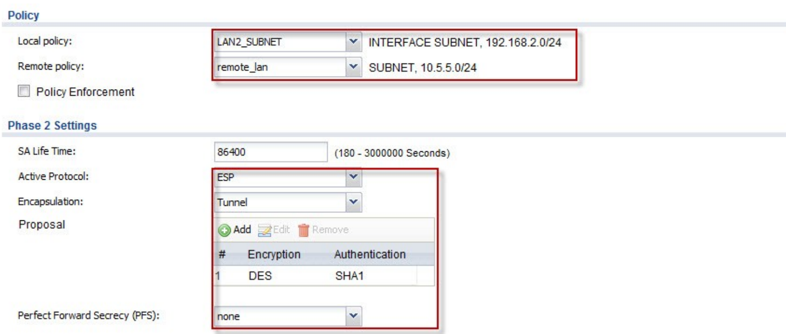




Phase 1 Settings
SA Life Time:
86400
(180 - 3000000 Seconds)
Negotiation Mode:
Main
Proposal
Add
Edit
Remove
#
Encryption
Authentication
1
DES
MD5
Key Group:
DH1
NAT Traversal
Dead Peer Detection (DPD)

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




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
Add
Edit
Remove
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

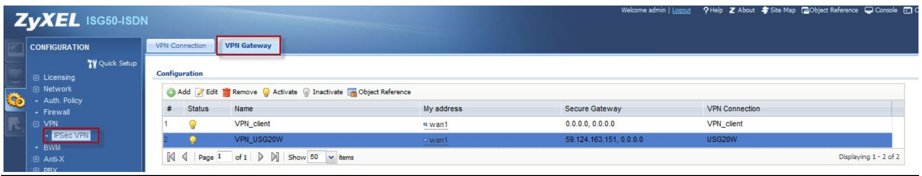
IPSec VPN

Phase 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

<u>ISG50 (Main Office):</u>

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)

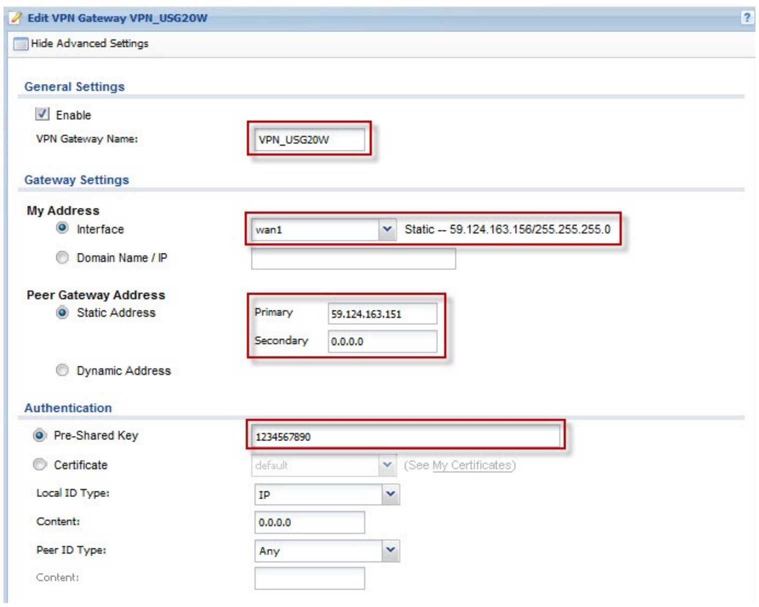
- Phase-1 setting

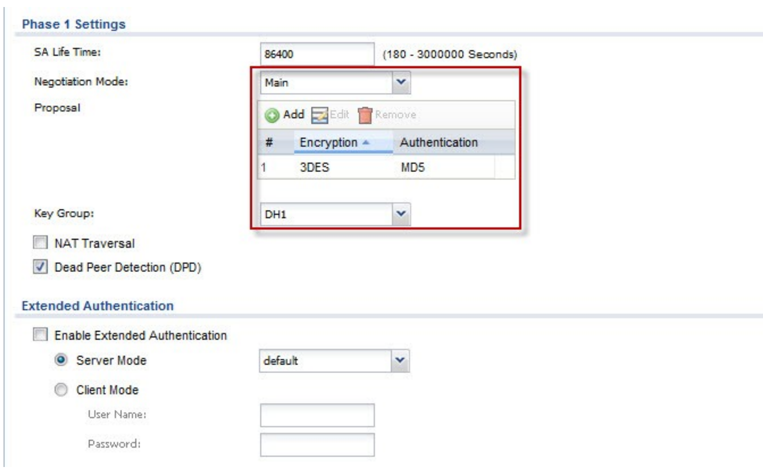
Negotiation mode

Encryption algorithm

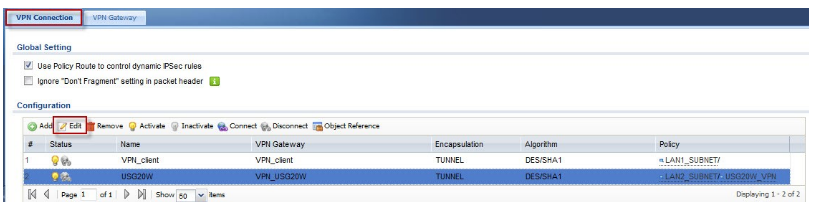
Authentication algorithm

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:

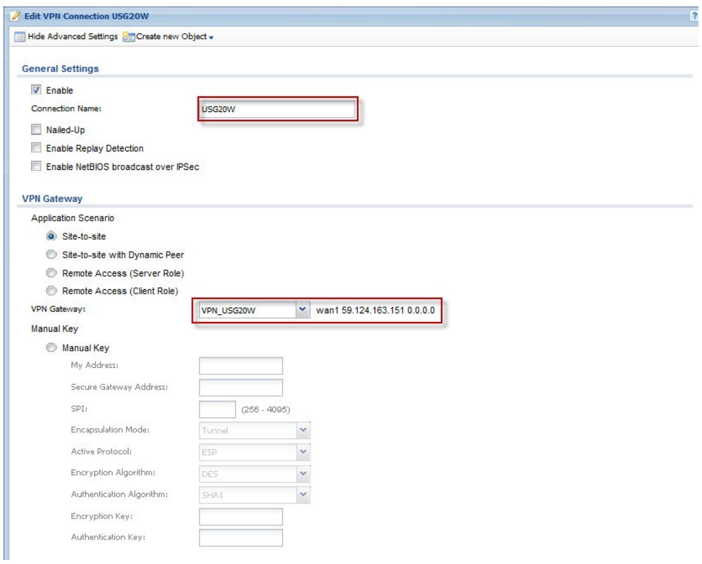

Phase 1 Settings
SA Life Time:
86400
(180 - 3000000 Seconds)
Negotiation Mode:
Main
Proposal
Add
Edit
Remove
#
Encryption
Authentication
1
3DES
MD5
Key Group:
DH1
NAT Traversal
Dead Peer Detection (DPD)
Extended Authentication
Enable Extended Authentication
Server Mode
default
Client Mode
User Name:
Password:

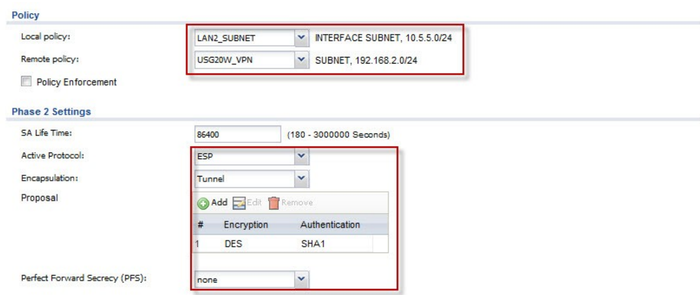
Click **CONFIGURATION > VPN > IPsec VPN > VPN Connection** to configure the phase-2 rule.



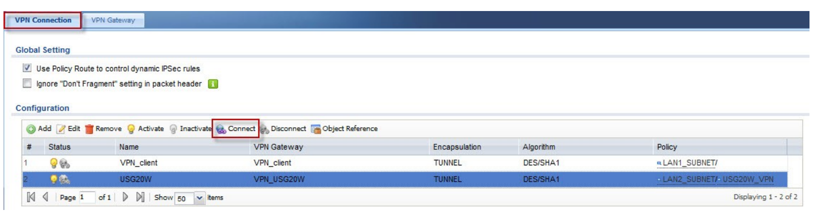
To configure the phase 2 rule, the user needs to fill in the following:

- 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
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:
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:

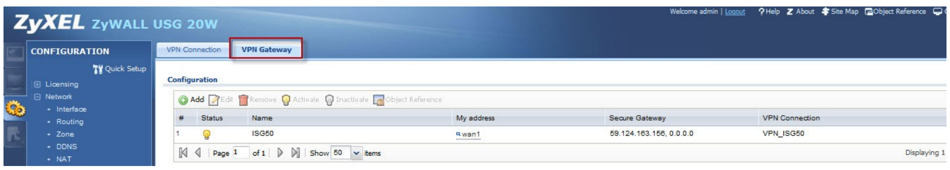


Click the **Connect** button to establish the VPN link. Once the tunnel is established, a **connected** icon will be displayed in front of the rule.



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)

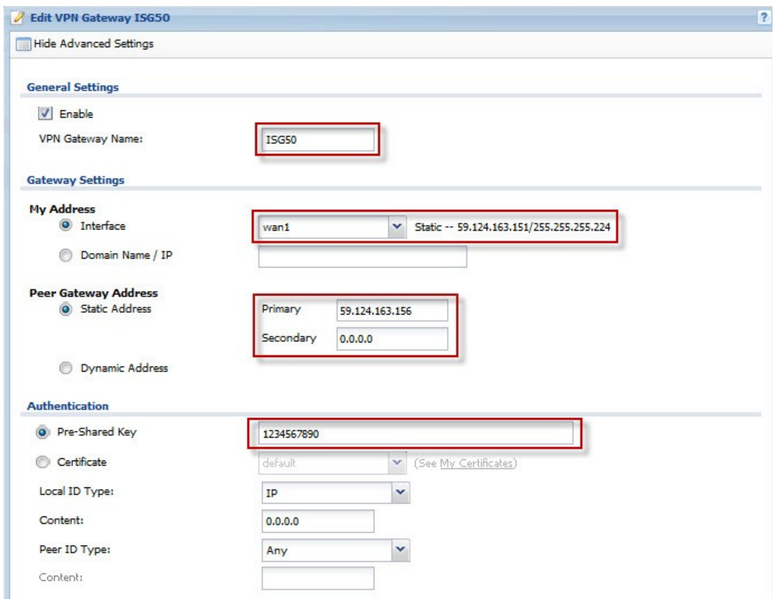
- Phase-1 setting

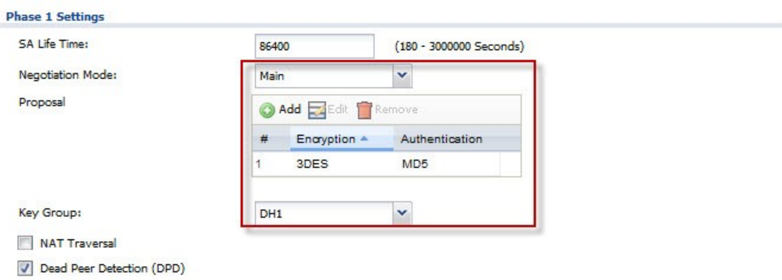
Negotiation mode

Encryption algorithm

Authentication algorithm

Key Group


Edit VPN Gateway ISG50
Hide Advanced Settings
General Settings
Enable
VPN Gateway Name:
ISG50
Gateway Settings
My Address
Interface
wan1
Static -- 59.124.163.151/255.255.255.224
Domain Name / IP
Peer Gateway Address
Static Address
Primary
59.124.163.156
Secondary
0.0.0.0
Dynamic Address
Authentication
Pre-Shared Key
1234567890
Certificate
default
(See My Certificates)
Local ID Type:
IP
Content:
0.0.0.0
Peer ID Type:
Any
Content:

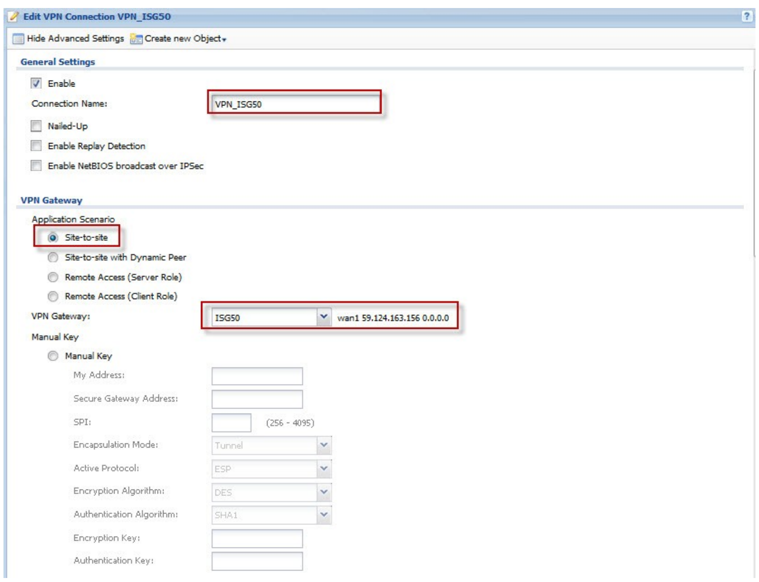


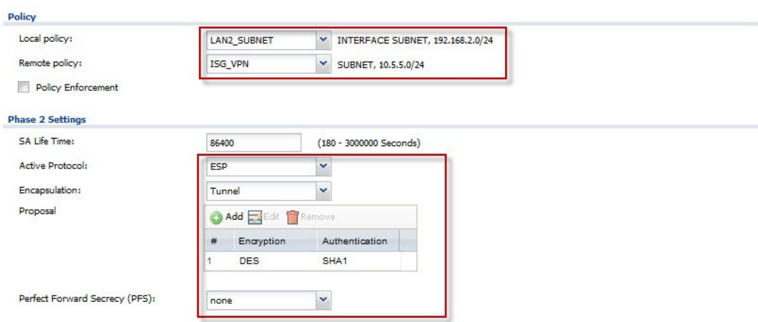
Configure the phase-2 rule.

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

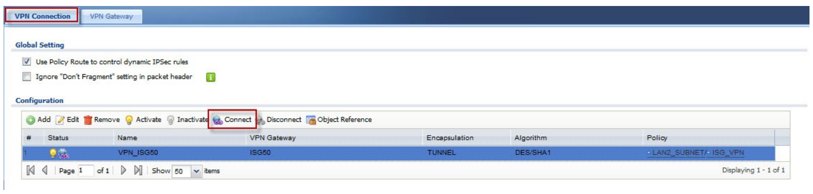
- Active protocol
- Encapsulation mode
- Encryption algorithm
- Authentication algorithm
- Perfect Forward Secrecy





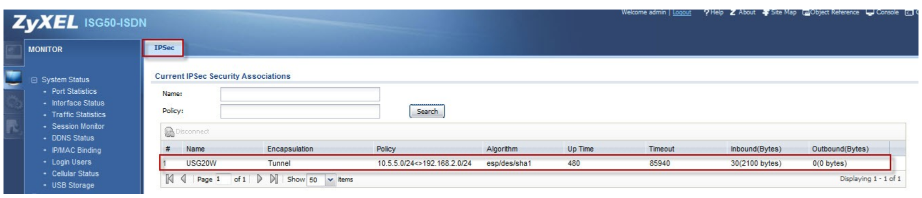
Before configuring Remote Policy, the user can create a specific object for the VPN subnet.

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.

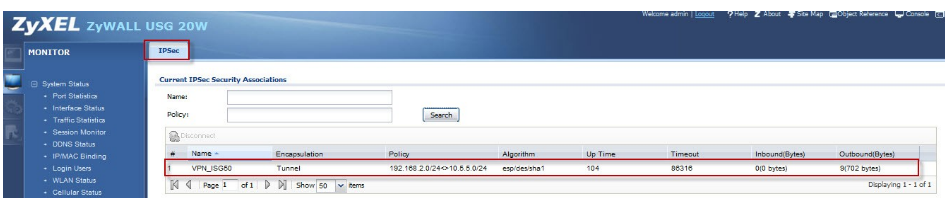


When the VPN tunnel is established, the user can find the SA information on **MONITOR > VPN MONITOR > IPsec**.

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.

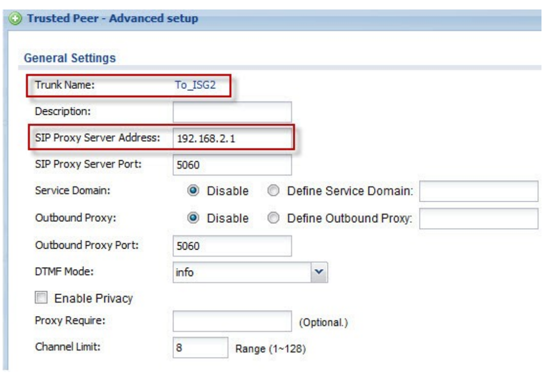
Condition:

ISG50-1 (Main Office):	***ISG50-2 (Remote Office):***
LAN IP: 192.168.2.1	LAN IP: 10.5.5.1

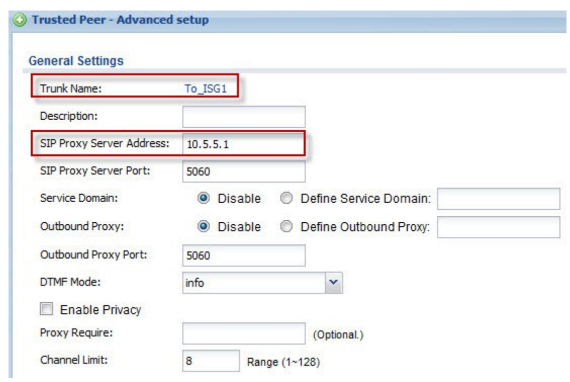
The configuration for IPsec VPN is the same as that in site to site IPsec VPN.

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):



ISG50-2 (Remote Office):



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:

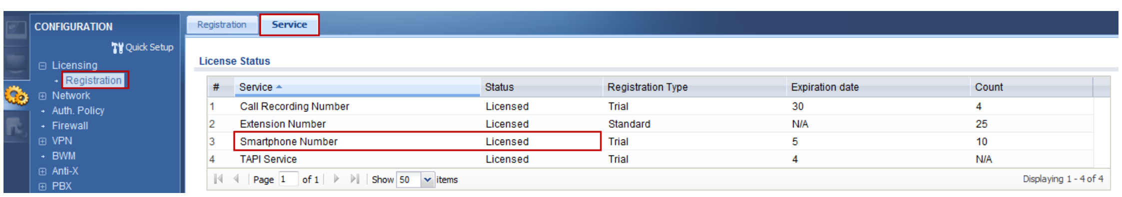
Turn the smartphone into a mobile SIP client with ZyXEL Reach installation and basic configuration.

Condition:

ISG's address: 59.124.163.156

Username: 3002

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



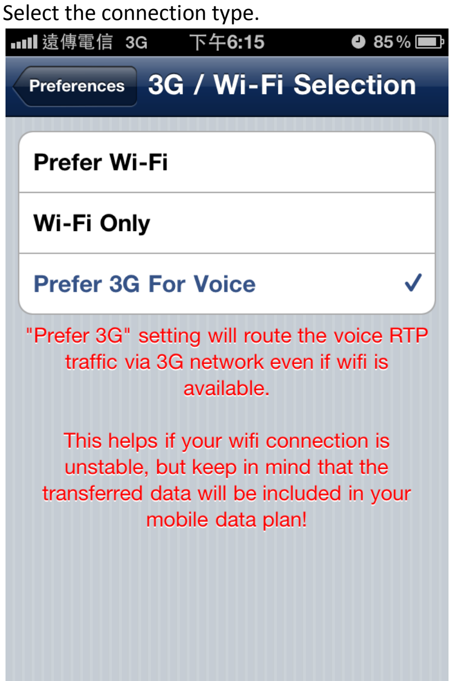
Install the mobile softphone APP, ZyXEL Reach, on your smart phone.
It supports both iPhone and Android platform.

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

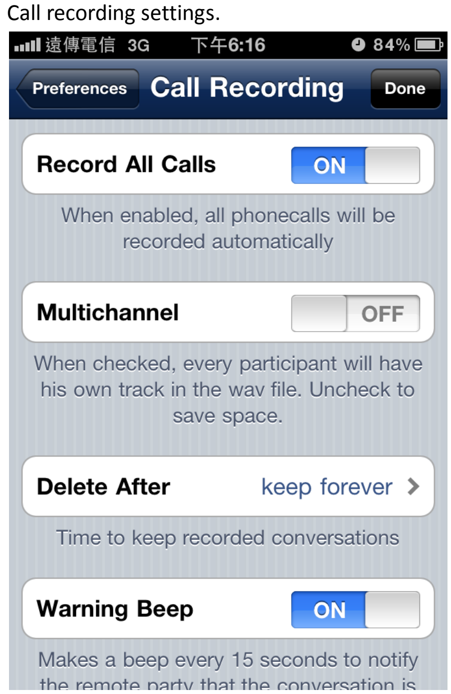
You can also add multiple SIP accounts.

Personal settings.

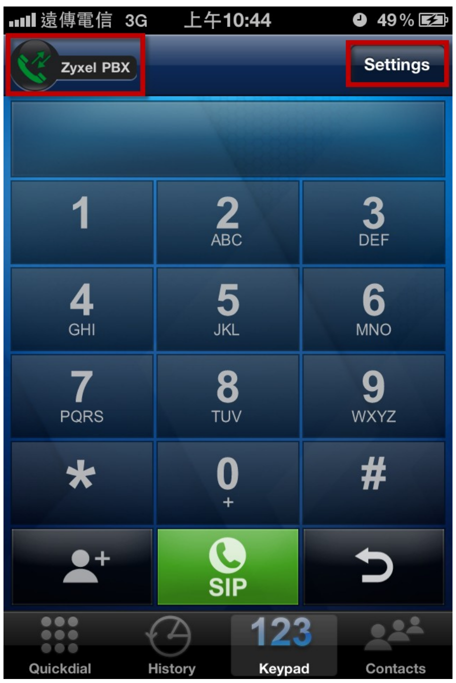
Select the connection type.



Call recording settings.

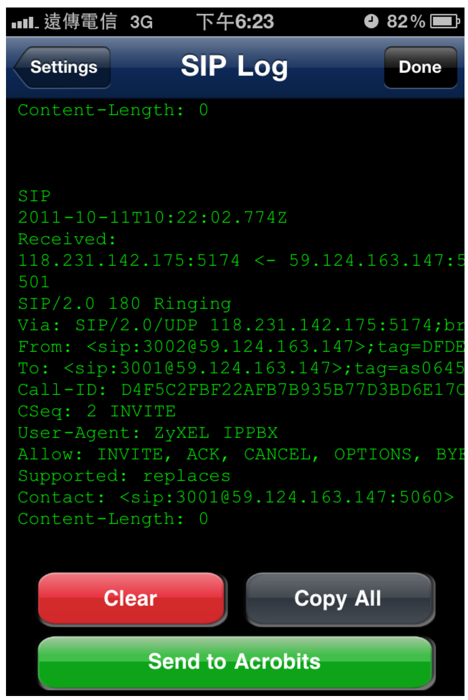


Dial the phone number from the keypad.



Check the call history.

View the packet trace.



How to avoid missing any call on a certain extension?

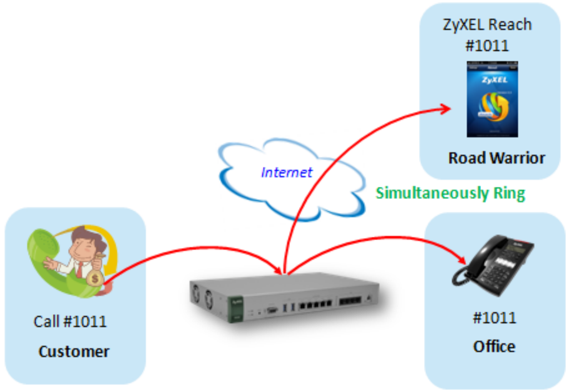
In this example, an ISG50 rings an office extension #1011 and the corresponding ZyXEL Reach simultaneously with a single number. When the employee is away or out of the office, he can always get calls of his extension. All settings can be done on the ZyXEL Reach by the employee himself, so it is not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

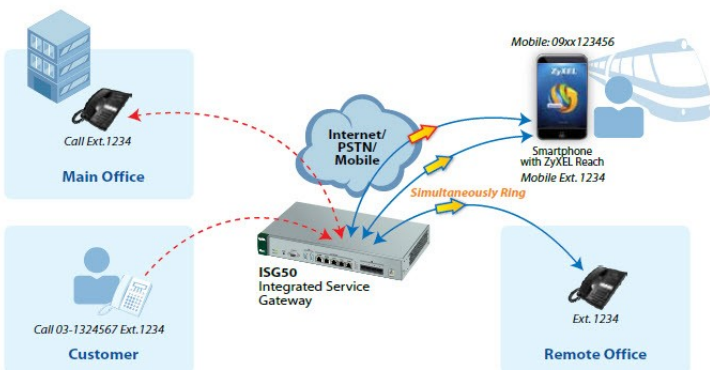
Authentication on V310 Username: 1011 ***Authentication on ZyXEL Reach*** Username: web1011



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.

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

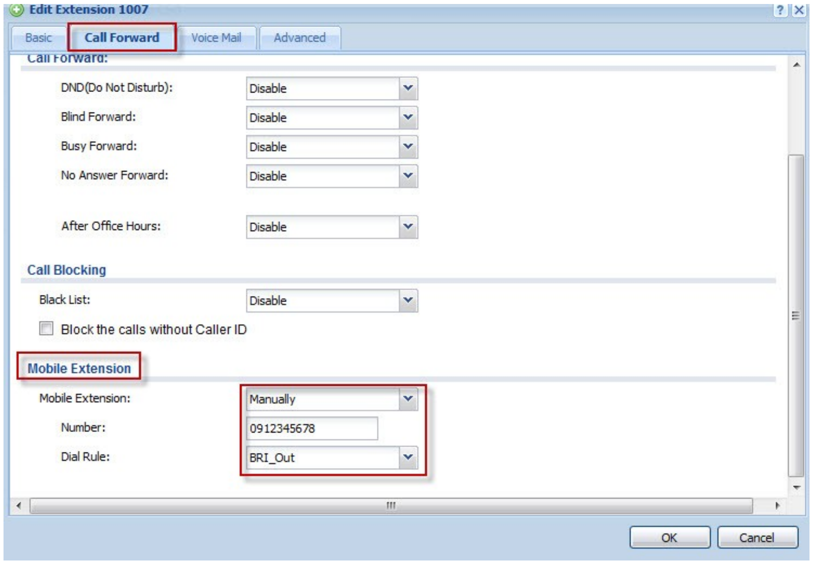
Single Number Reach (IP phone & Mobile SIP & GSM Mobile Number)

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

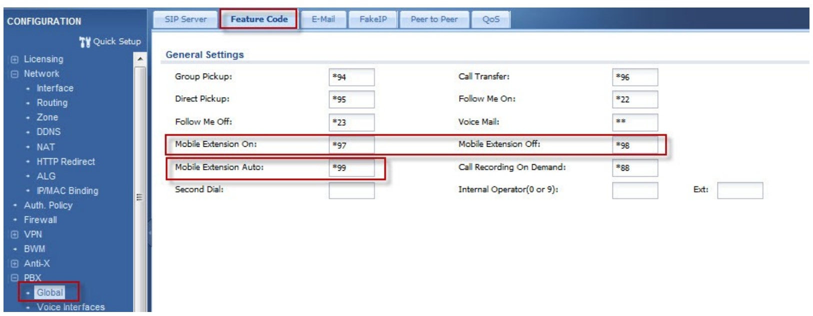
You can select to “Manually” turn on and off this feature or select “Force Enable” to always turn on this feature.

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.



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



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

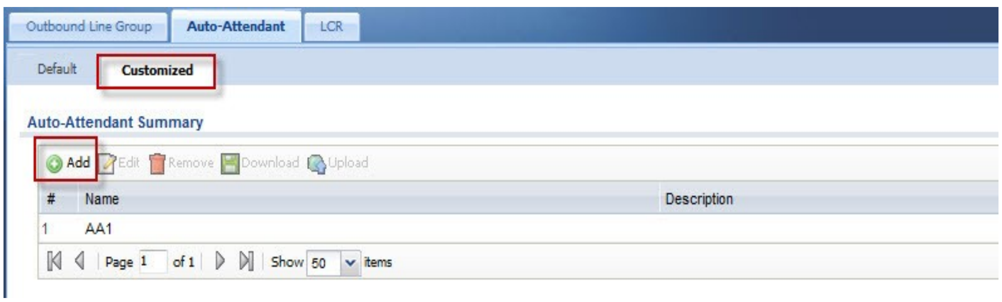
The company needs an automatic call operator to transfer each incoming call to the specific contact or department. In addition, customer service hotlines are also required for serving customers. Employees often have conference calls with vendors and distributors. The ISG50 has a call distribution system 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.

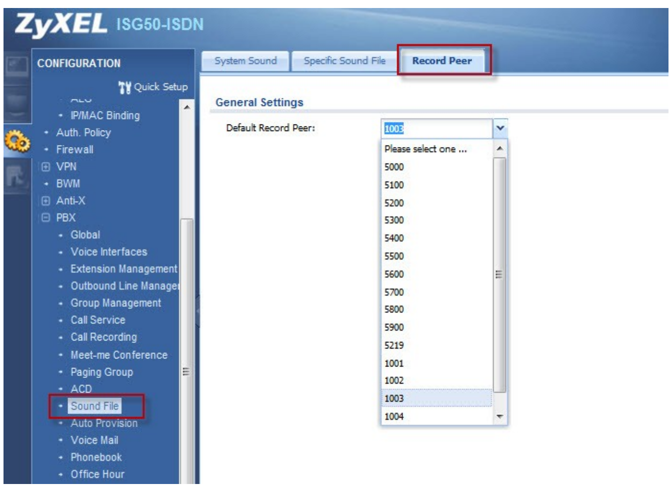
Condition:
Recorded Peer: 1003
Office Hour: Monday – Friday; 08:00-12:00 and 13:00-17:30
Operator key for office hours: 9; extension number: 9999
Hunt group number for night service: 5555

Configuration for customized Auto Attendant

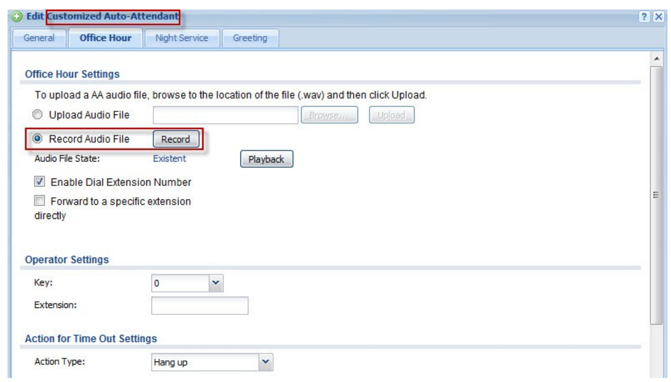


In addition to uploading an existing audio file to the system, ISG50 provides an easy way for users to record the audio file by extension to Auto Attendant system. When you press the record button, ISG50 will call the record peer. After the extension of the record peer is picked up, you can start recording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

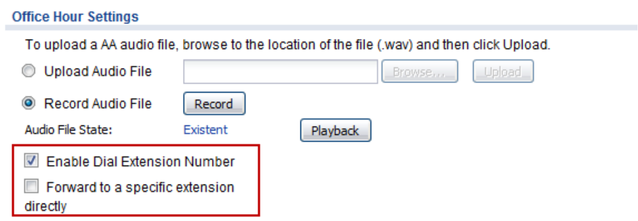
Set the record peer. For example, we set extension 1003 as the record peer. You will use this extension to record the audio file in the next step.



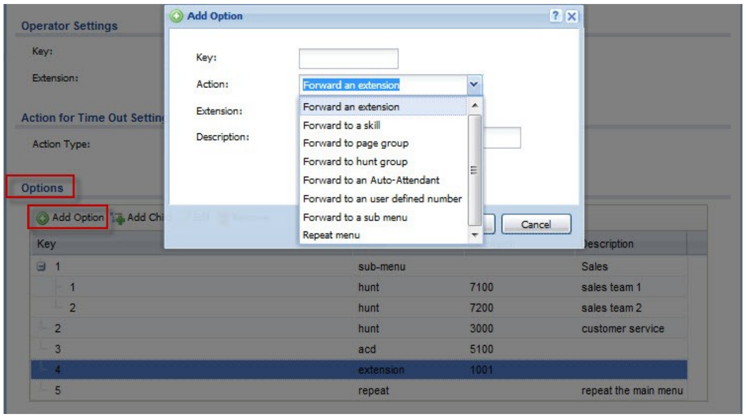
Select "Record Audio File" and press the record button. ISG50 will call the record peer 1003. Start recording after you pick up the phone of 1003. Hang up the phone or press the # key to finish recording.



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.



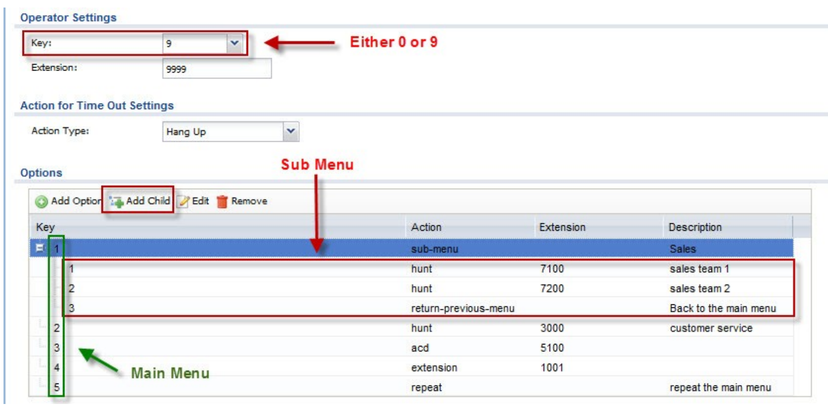
Design the customized menu with option keys.

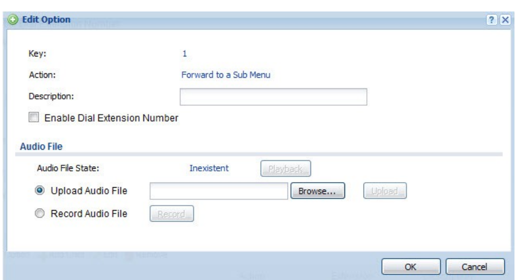


Option key 0 and 9 are reserved for the operator and can't be configured as other option keys.

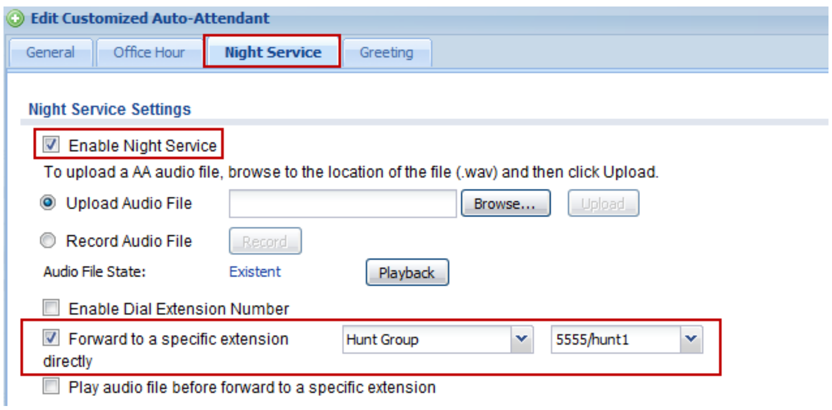
ISG50 supports up to 10 levels of sub menus.

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.

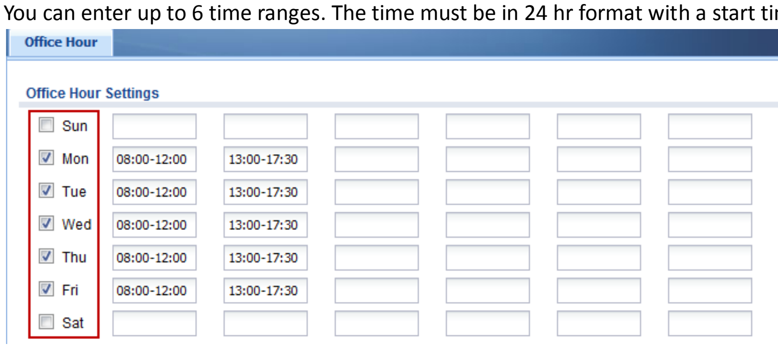




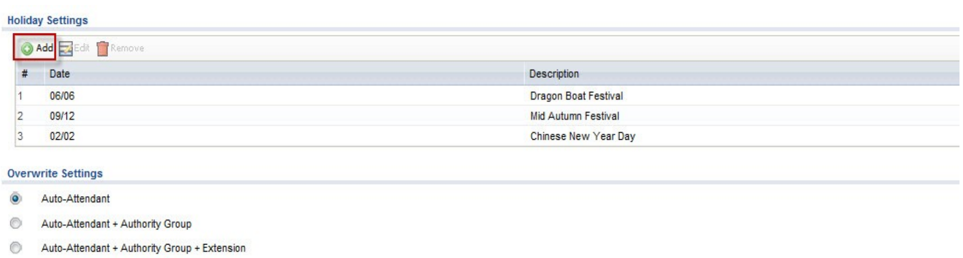
You can also enable “Night Service” to perform different AA directions outside of office hours based on the office hour setting.



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



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”.



Hunt Group

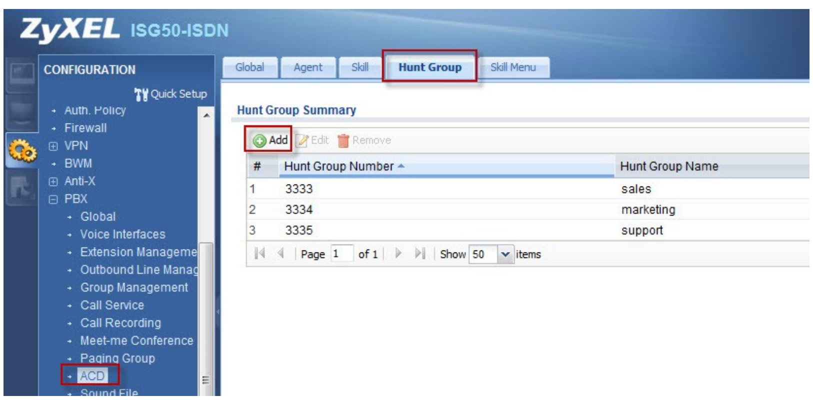
Goal to achieve:

Create a hunt group number 3333 for the sales department.

Condition:

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

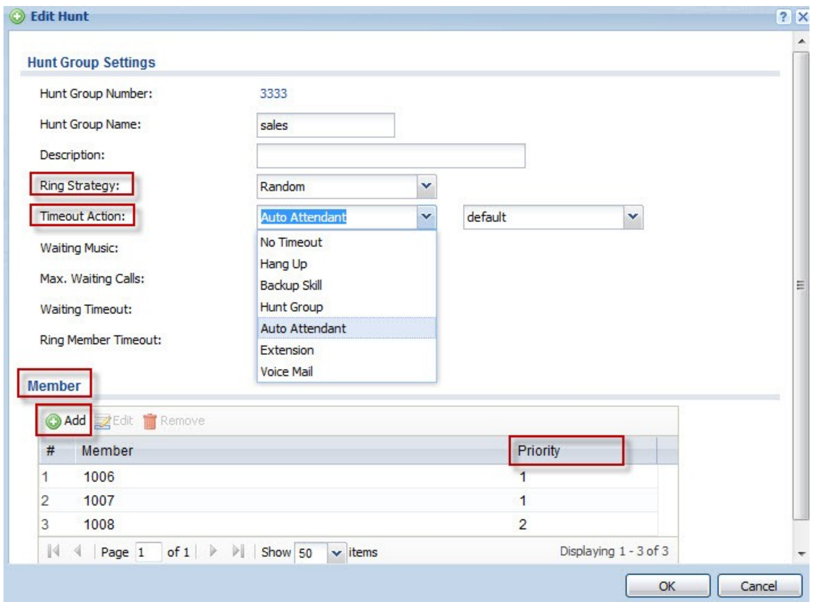
Ring Strategy: Random



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.



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:

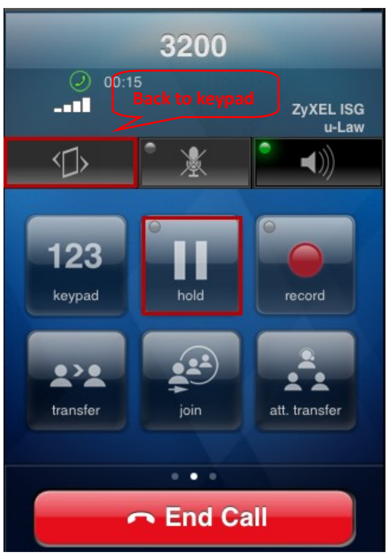
V310 (#3200) calls ZyXEL Reach (#1010).

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

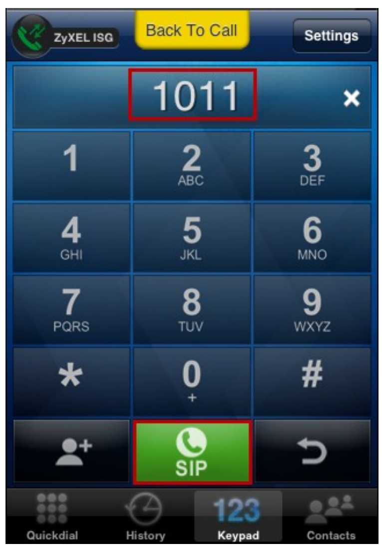
By performing the following steps, these three extensions are having a three-way conference call.

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

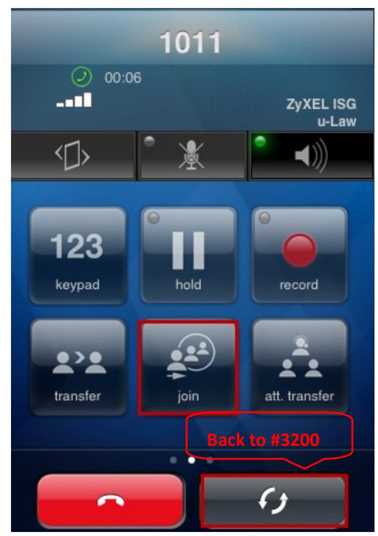
1. ZyXEL Reach (#1010) has a call with V310 (#3200). Before dialing to extension 1011, press the hold key and go back to the keypad.



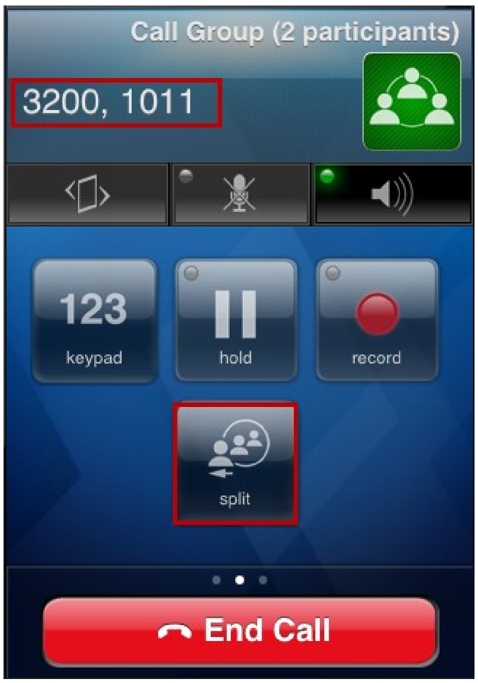
2. Then dial 1011 and press 



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.

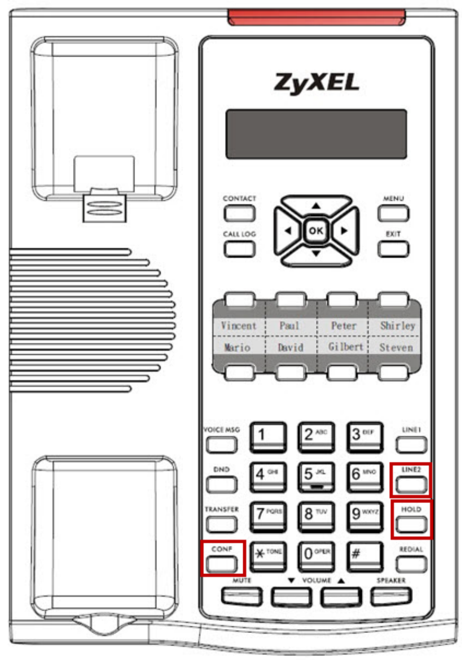


4. Three-way conference has been established. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the split key.

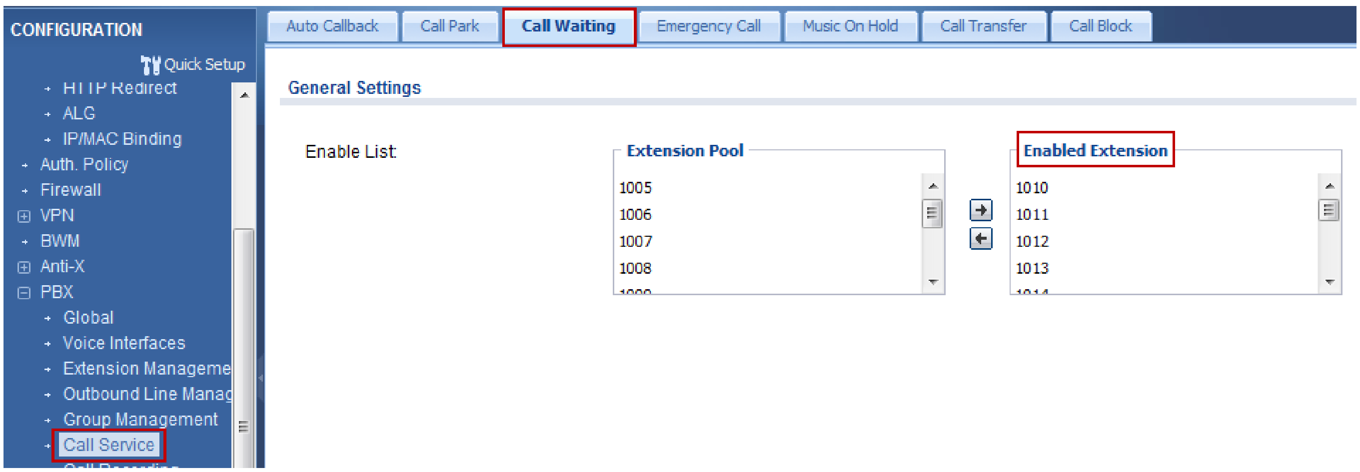


How to perform three-way conference on V310?

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".



Meet-Me Conference

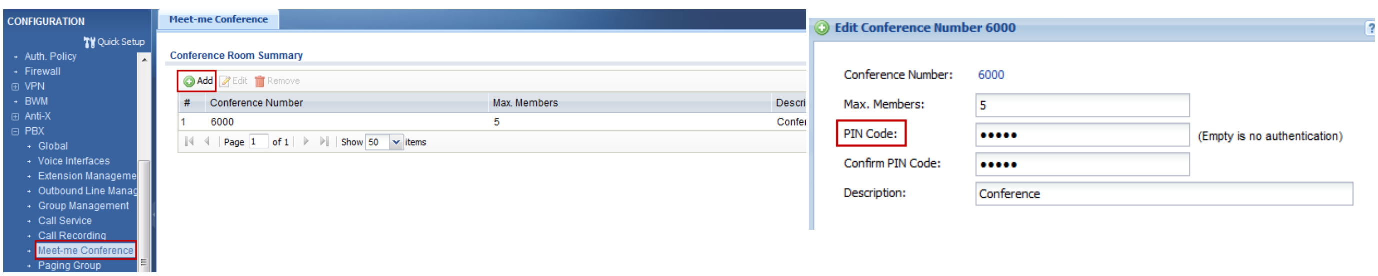
Goal to achieve:

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.



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

<u>How to change the language of system sounds from English to a specific language?</u>

Goal to achieve:

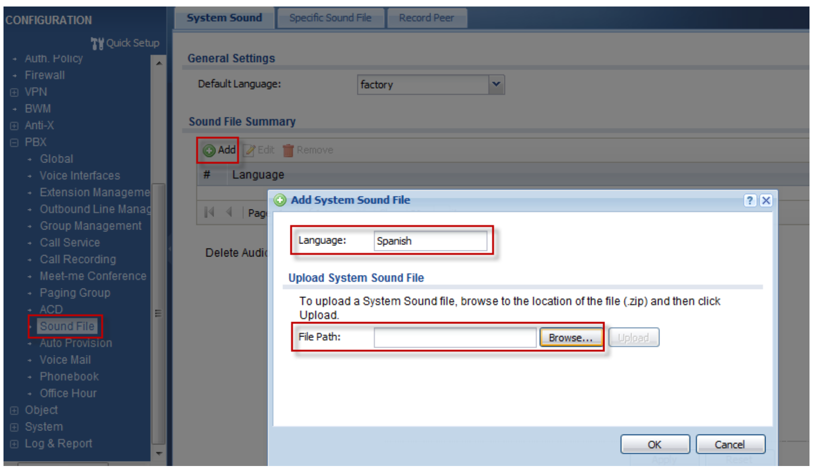
The administrator would like to change the language of system sounds to Spanish.

Condition:

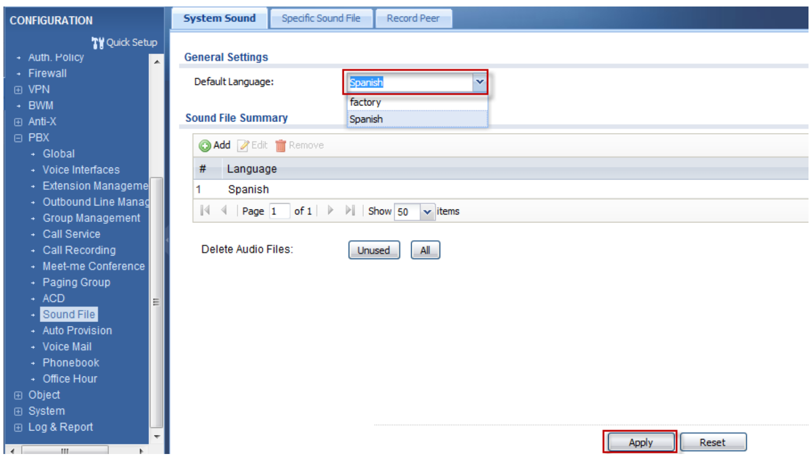
Default Language: Spanish

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.



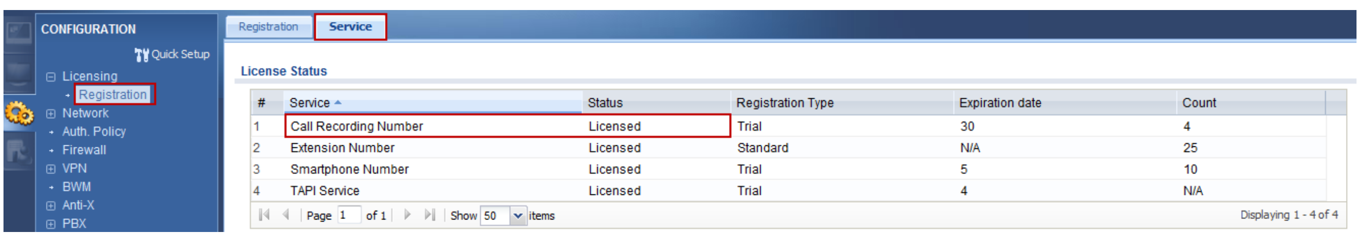
8. How to Record a Call?

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

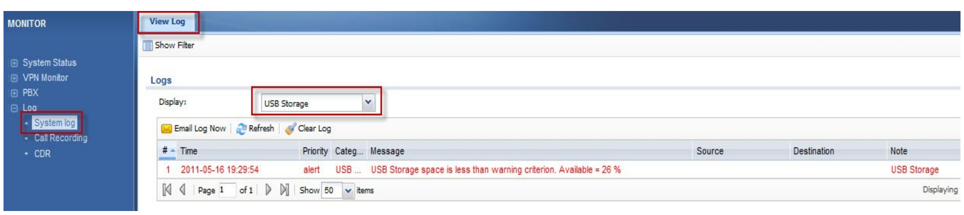
The call recording feature is enabled when the license (ISG50-CR) is applied.



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:

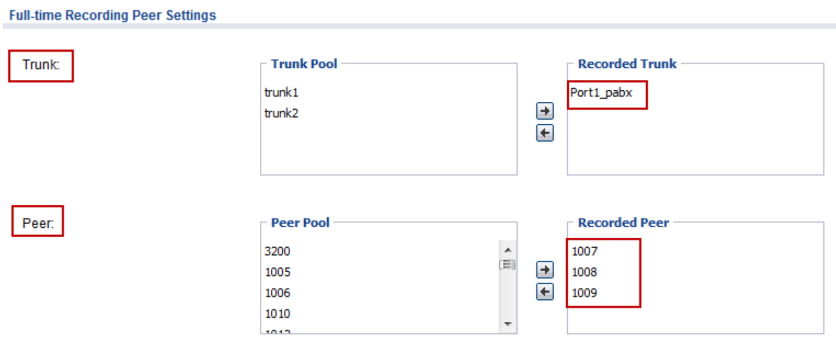
The administrator would like to record all calls on the FXO trunk and the extensions 1007, 1008 and 1009.

Condition:

Recorded Trunk: Port1_pabx (FXO trunk)

Recorded Peer: 1007, 1008 and 1009

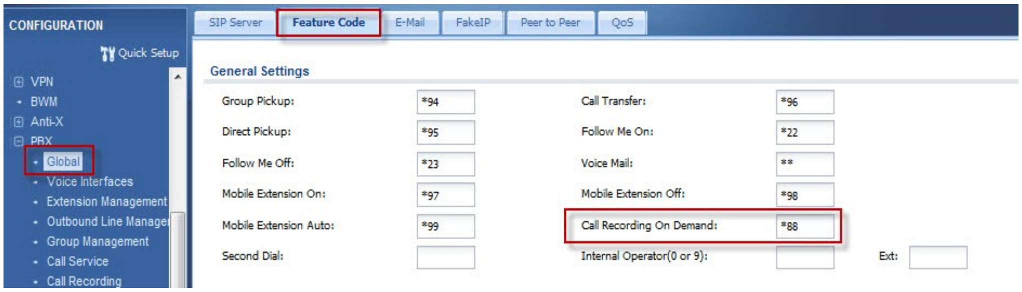
Select from the Trunk Pool and Peer Pool to determine which trunks and/or peers should be recorded.



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.



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.

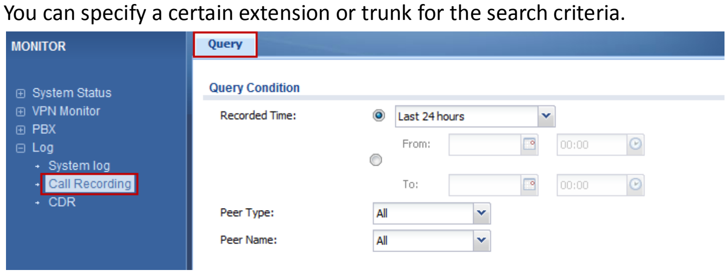
Condition:

Recorded Time: Last 24 hours

Peer Type: All

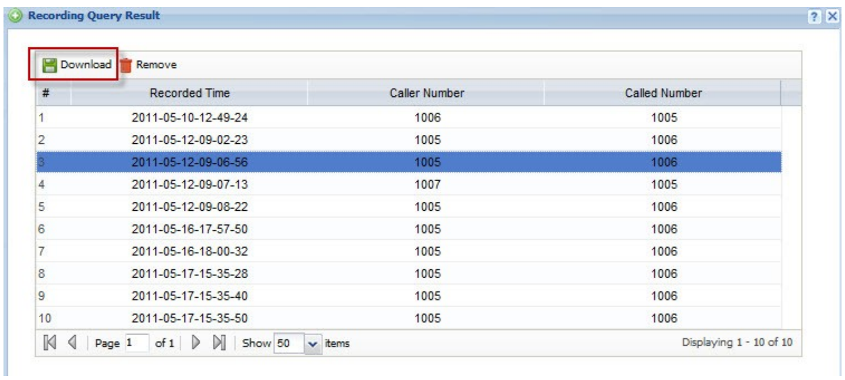
Peer Name: All

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.

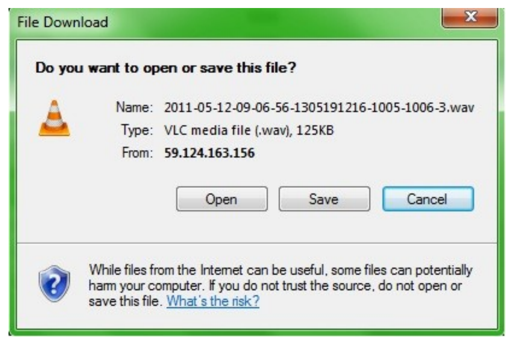


This screen lists the call recordings that matched the specified criteria.

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



#	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.

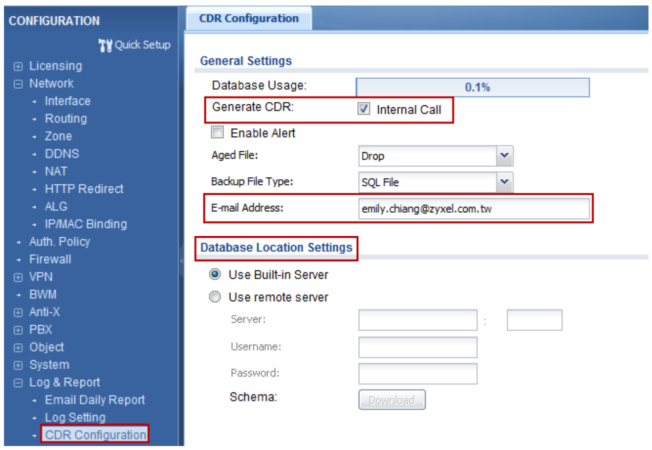
Condition:

Search period: Last 24 hours

Direction: all directions

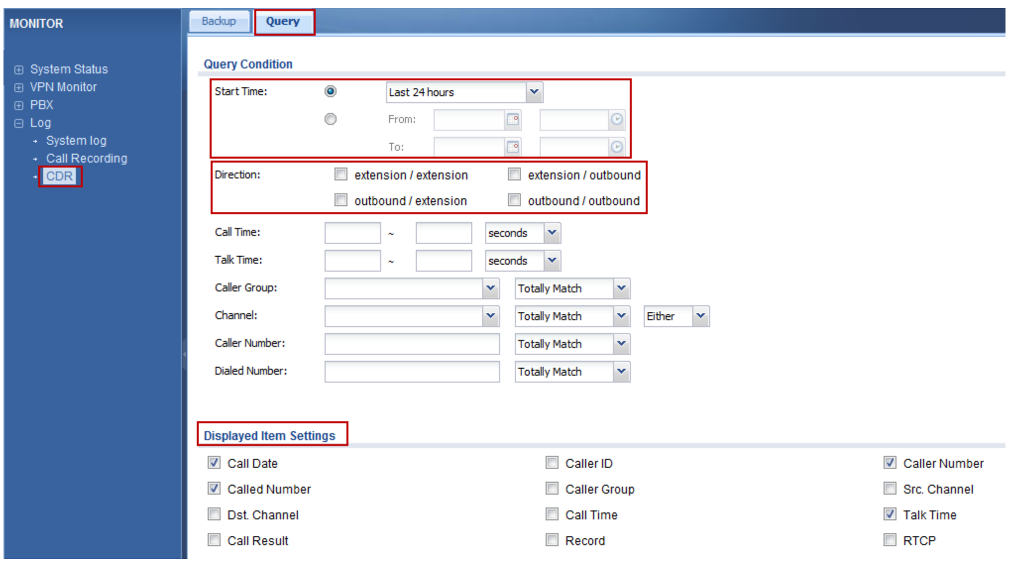
The ISG50 has a built in CDR database that automatically stores calls made to or from its extensions. The administrator can decide if internal calls are logged in the CDR record.

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.

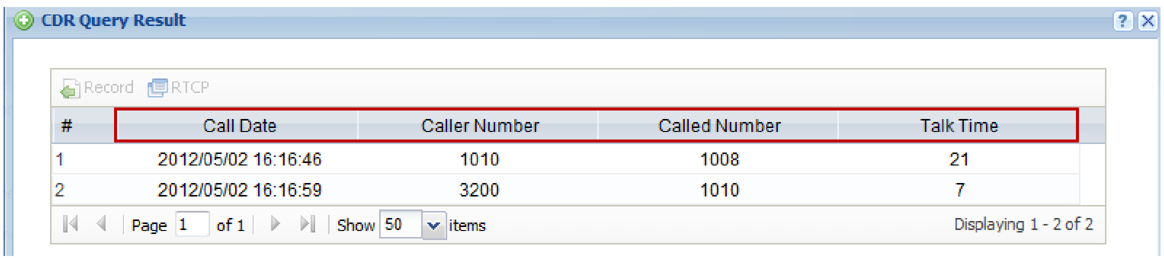


How to find the call history?

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.



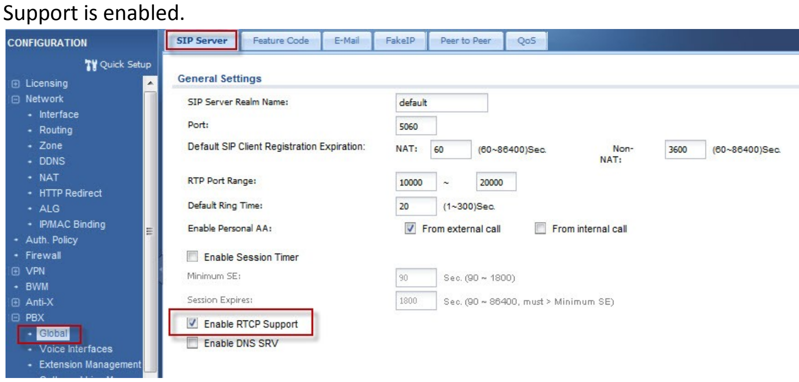
After configuring query conditions and displayed items, click the “Search” button to view your CDR query result.



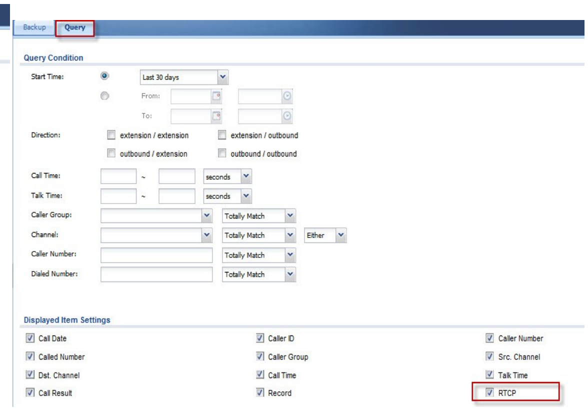
#	Call Date	Caller Number	Called Number	Talk Time
1	2012/05/02 16:16:46	1010	1008	21
2	2012/05/02 16:16:59	3200	1010	7

<u>How to check QoS of each call in RTCP?</u>

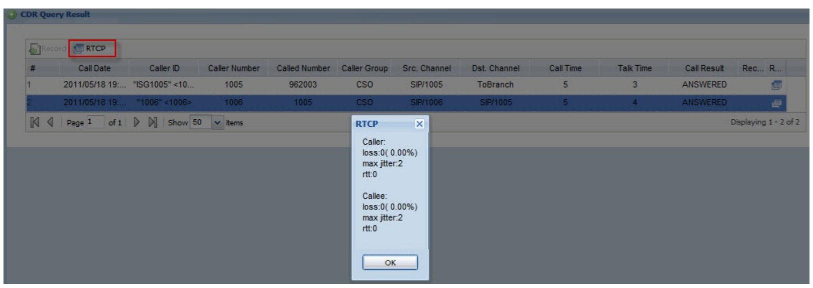
To view the RTCP information, select “Enable RTCP Support”. By default, RTCP Support is enabled.



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



Click the button to view RTCP information for each call.



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

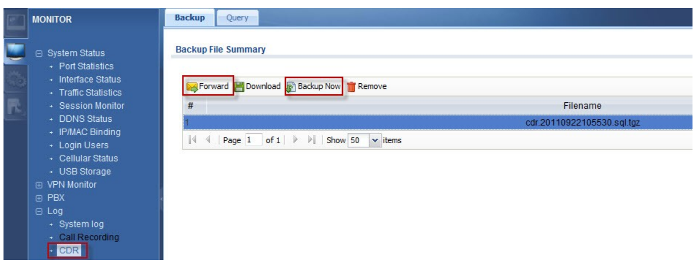
Goal to achieve: Backup call records to administrator's email.

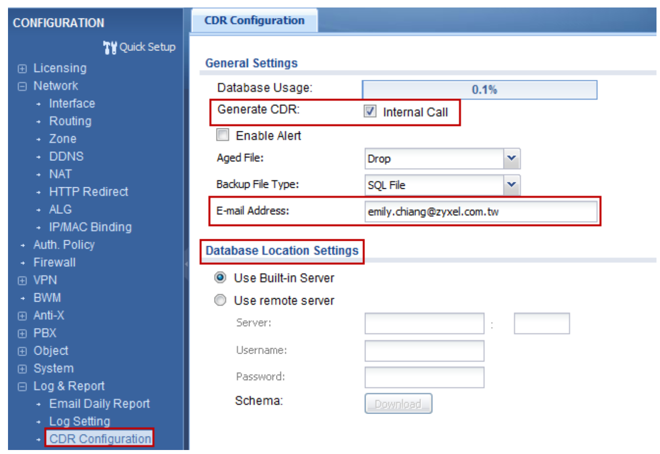
Condition:

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

Click the "Backup Now" button to back up the CDR file.

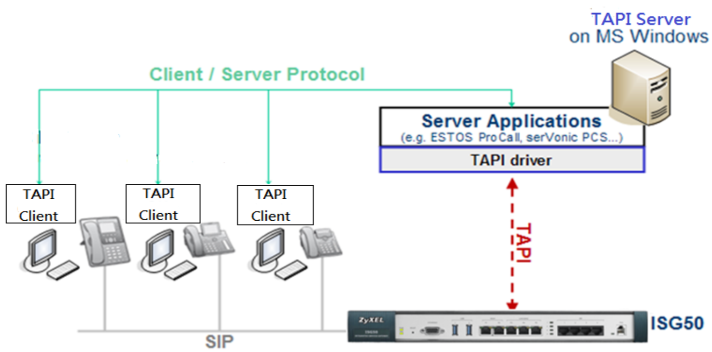
You can also send the backup file to the administrator by clicking the "Forward" button.





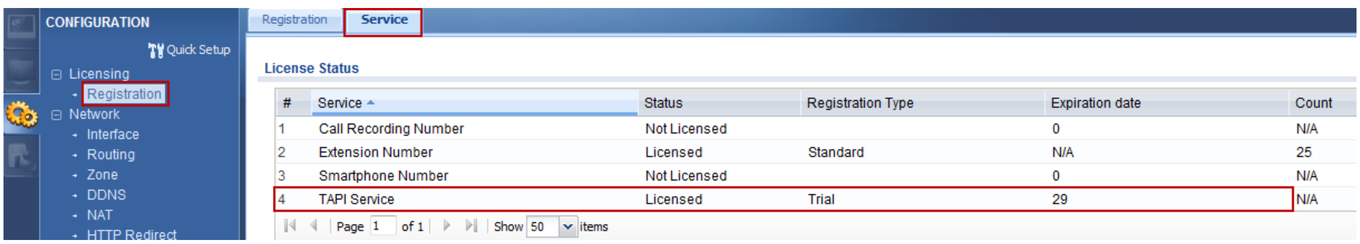
10. How do UC Server and UC Client Work with ISG50?

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.

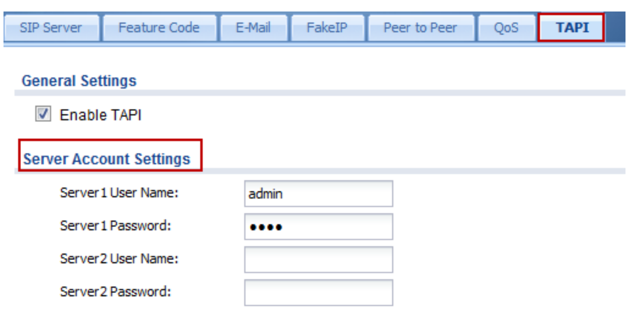


Preparation for TAPI Service

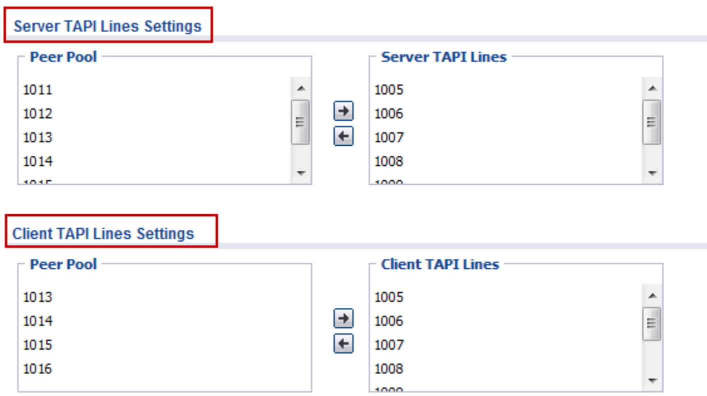
The TAPI feature is enabled when the license “ISG50-CTI” is applied.



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.



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



TAPI Driver Installation

Goal to achieve: Install TAPI driver on the PC.

Condition:

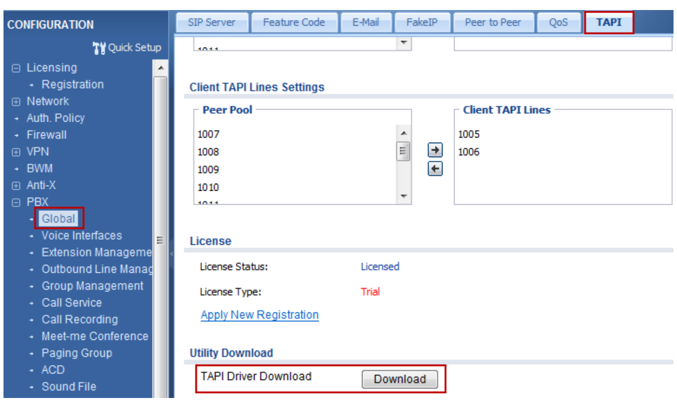
ISG server IP address: 59.124.163.156

TAPI Server user name: admin

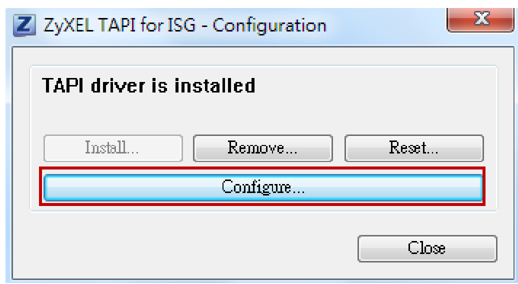
TAPI line: 1005-1016

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

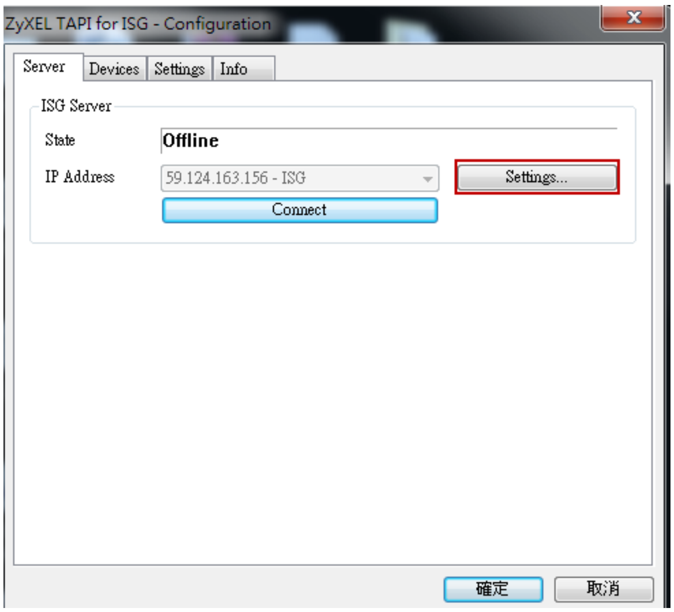
Download TAPI driver from the ISG50.



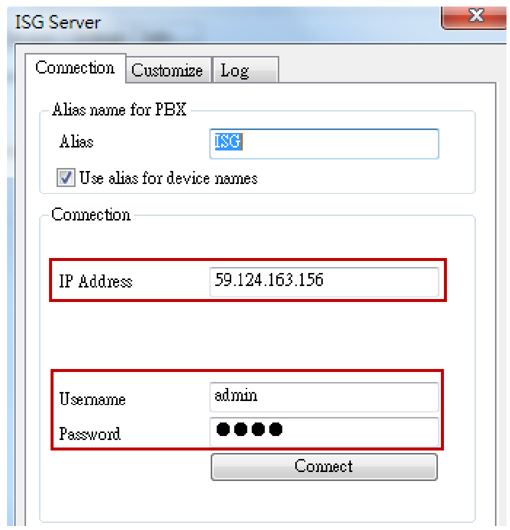
Install it in the PC.



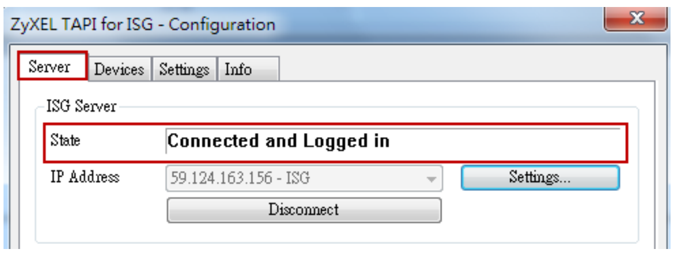
Configure the ISG server.



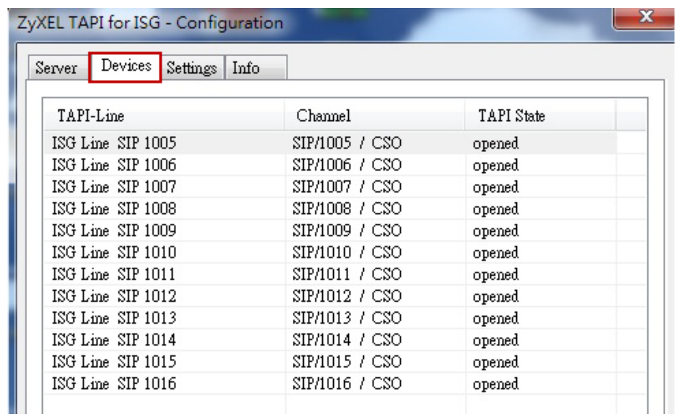
Fill in the IP address of ISG and log in with the administrator account. Then click the “Connect” button.



Check if the state is connected.



TAPI lines that administrator can control.



UC Server Installation

Goal to achieve:

Install UC server on the PC.

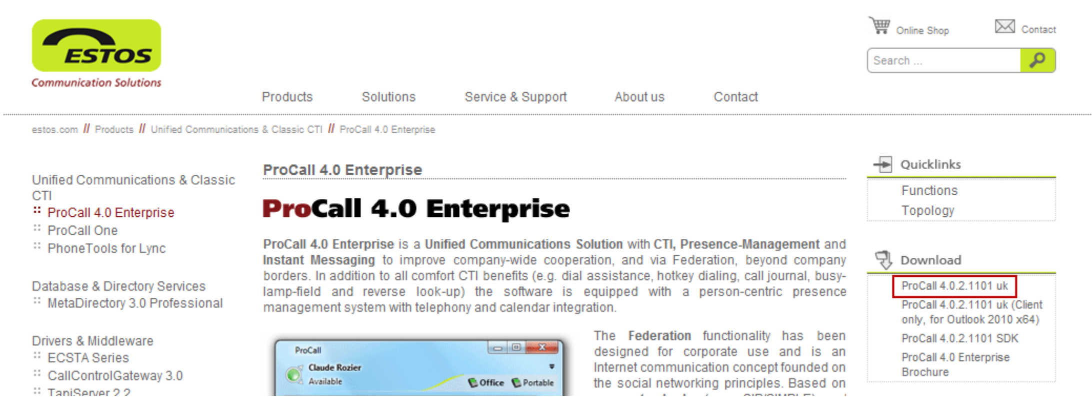
Create users on UC server and assign an extension number from the server TAPI lines in ISG50 for each user.

Condition:

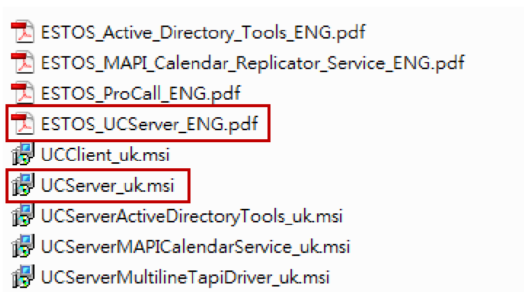
Administrator's account for access UC server: ucisg

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

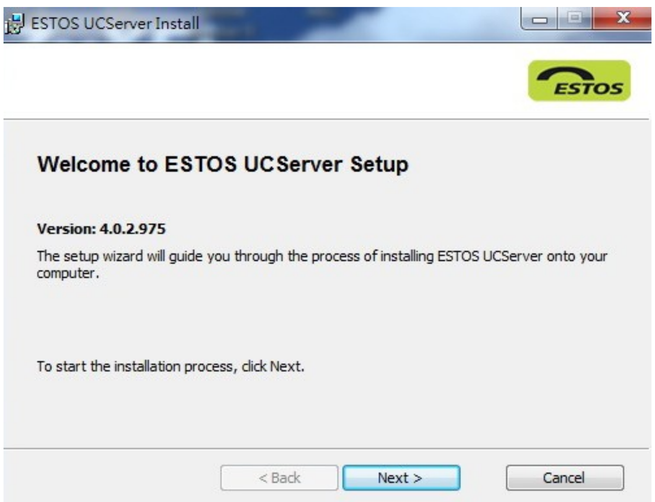
http://www.estos.com/products/unified-communications-classic-cti/procall-40-enterprise.html



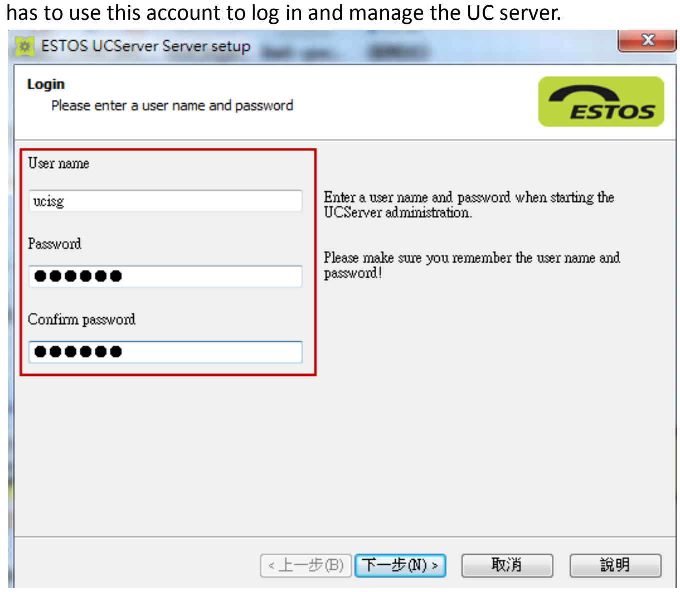
Install ProCall4.0 UC Server “UCServer_uk.msi” on the PC.
For detailed of configuration of the UC server, please refer to the document “ESTOS_UCServer_ENG.pdf”.



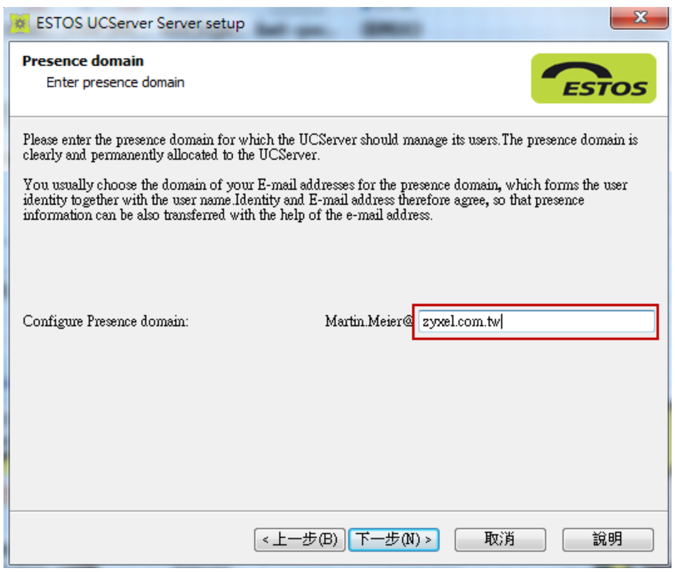
Start to install ESTOS UC server. Keep on pressing "Next" to finish the installation.



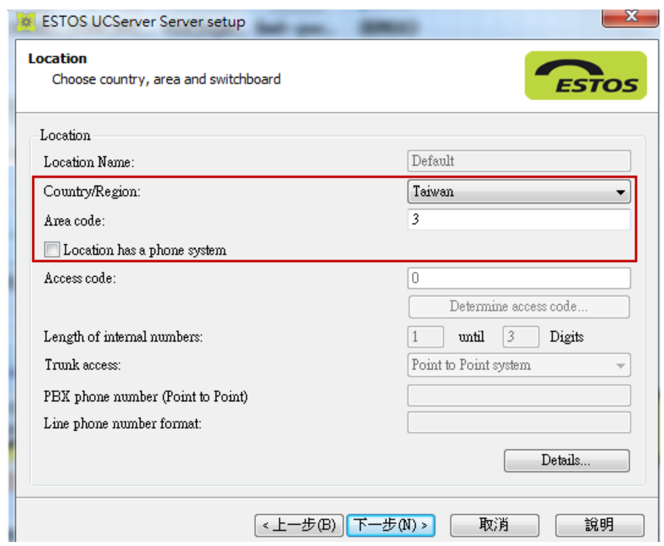
Create a username and password for the UC server. The administrator has to use this account to log in and manage the UC server.



Configure the presence domain.
For example, we fill “zyxel.com.tw” in this field.

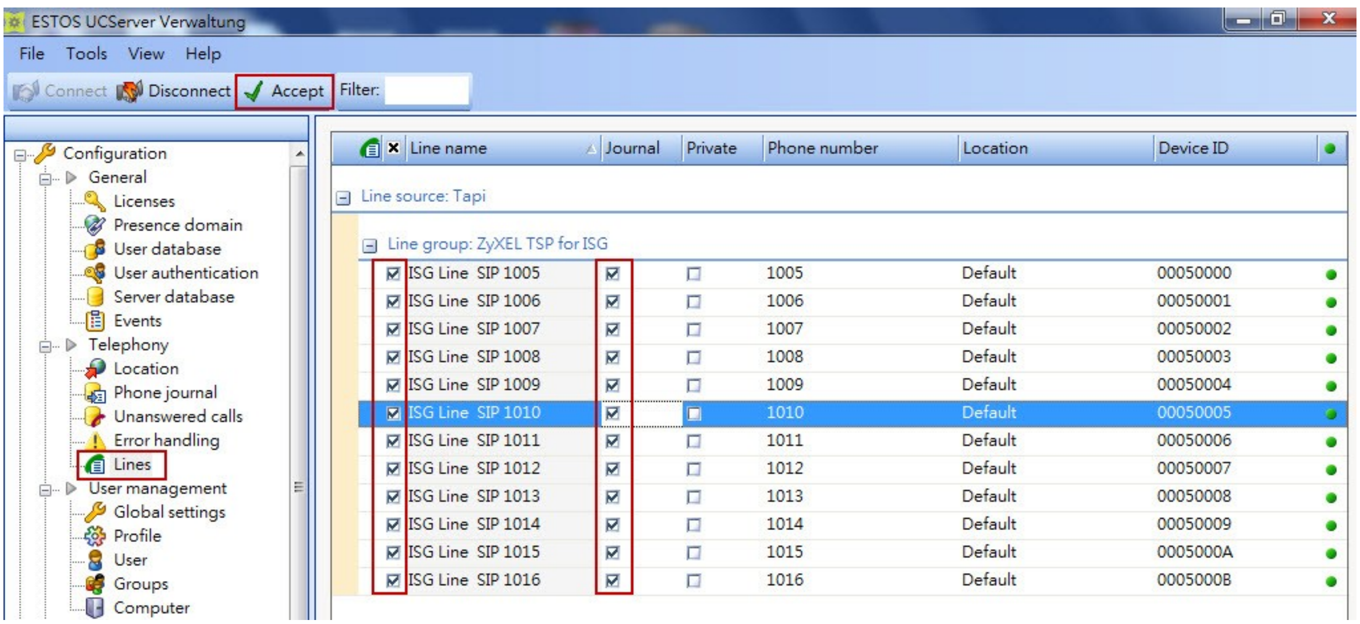


In one of the installation steps, set the country and the area code.
For example, we select “Taiwan” as the country/region and set “3” as the area code.
If “Location has a phone system” is unchecked, all dialed digits will be treated as “internal”.
If this box is checked, the country code and the area code will be added before the dialed numbers if more than 3 digits are entered.

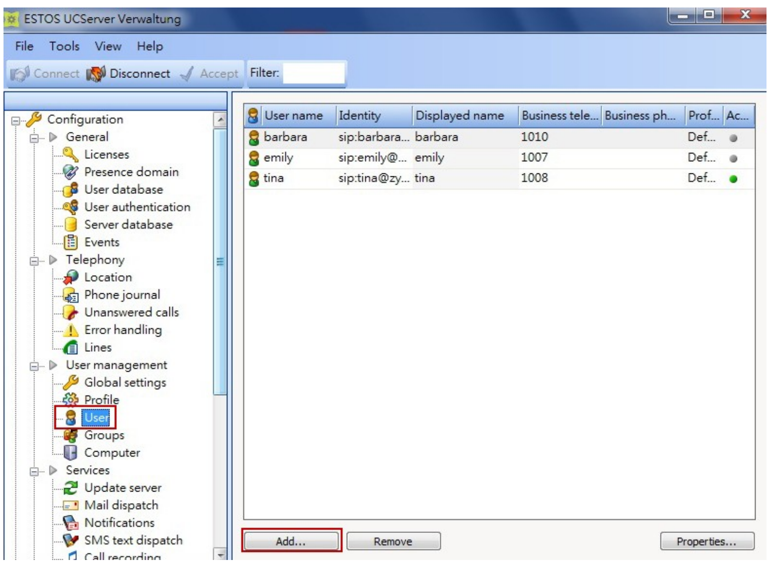


These are the extensions which are configured in the "Server TAPI Lines" in ISG50.

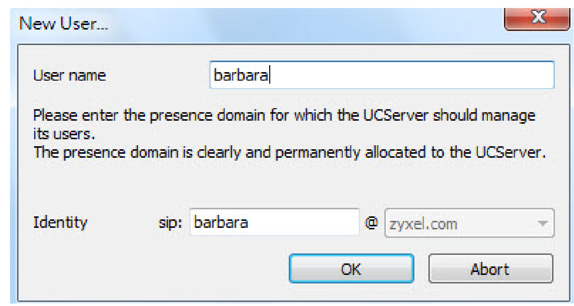
Click on "Accept" to apply the new settings on the server.



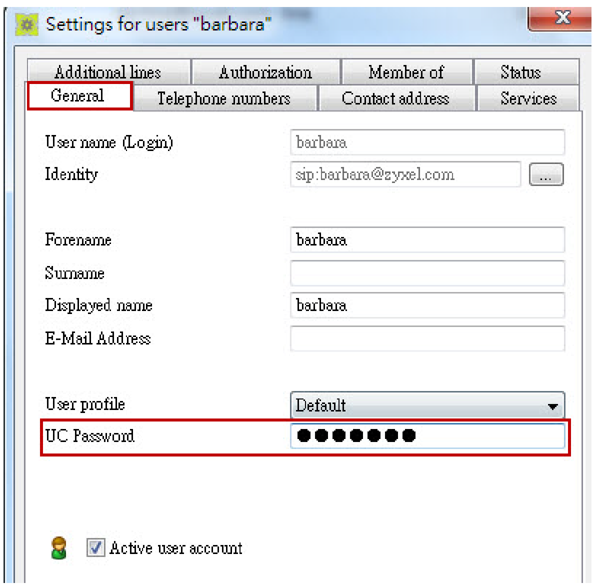
Create new users on the UC server.



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

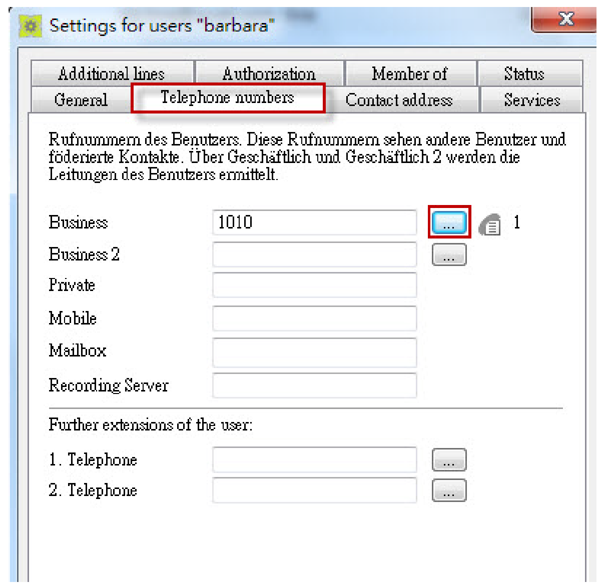


Configure the password for this new user.

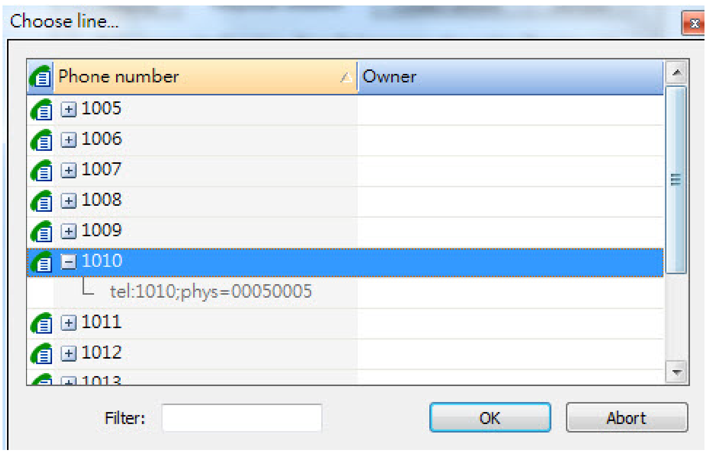


Assign an extension number for this user.

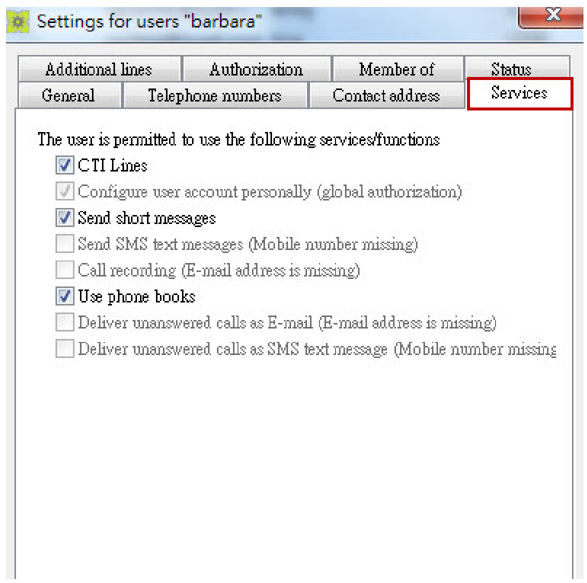
You can click the button to choose from the "Server TAPI Lines".



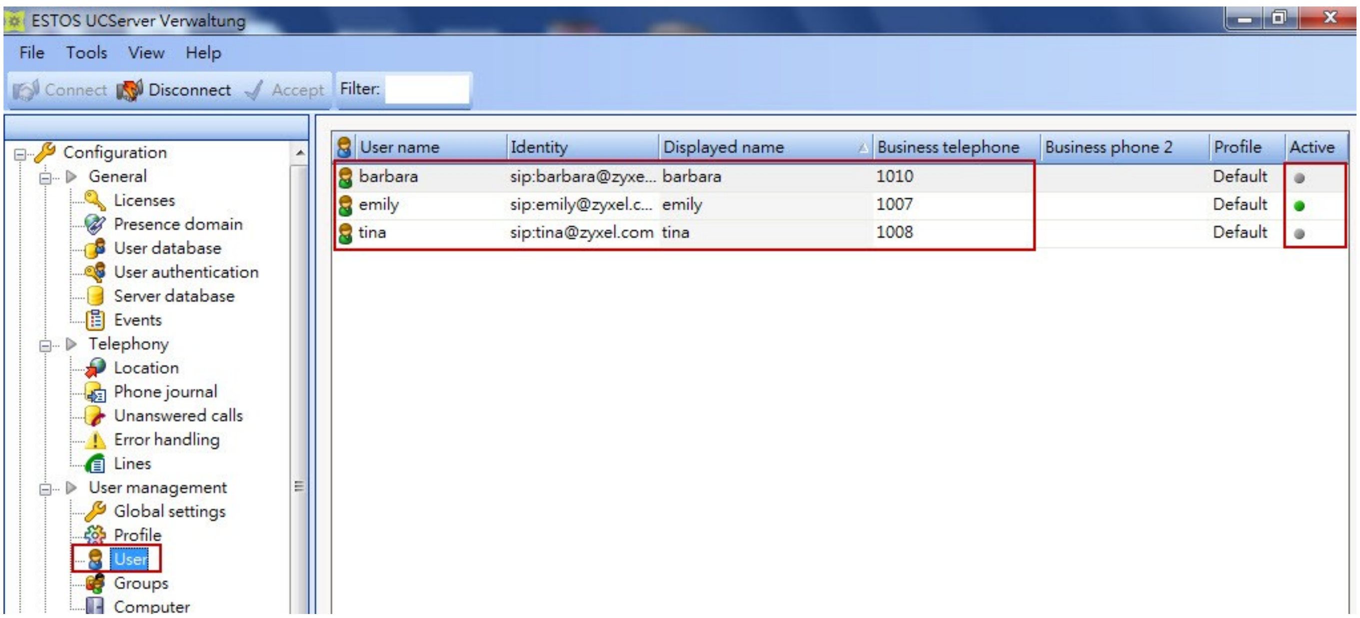
Select an extension number for the new user from the “Server TAPI Lines”.



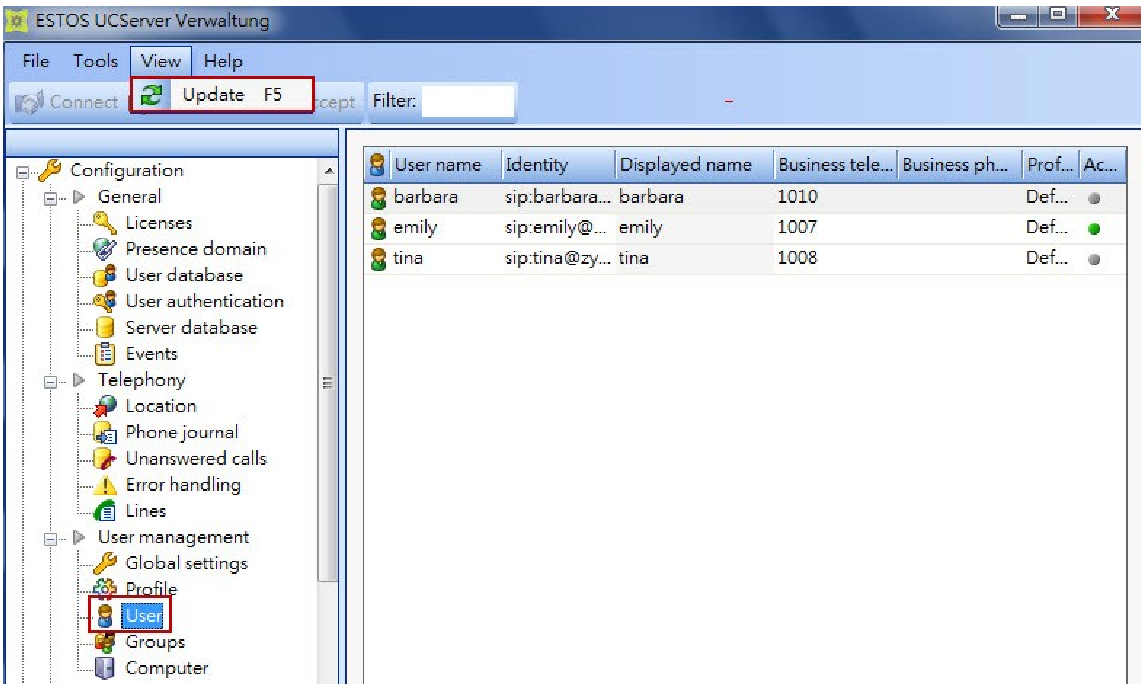
Select the services for this user.



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



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



UC Client Installation

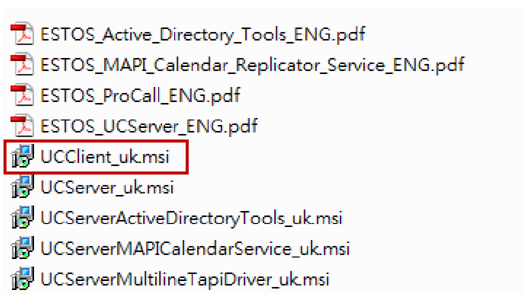
Goal to achieve: Use the UC client to make a call, hang up a call, reject a call, transfer a call, redirect a call and check the status of other extensions.

Condition:

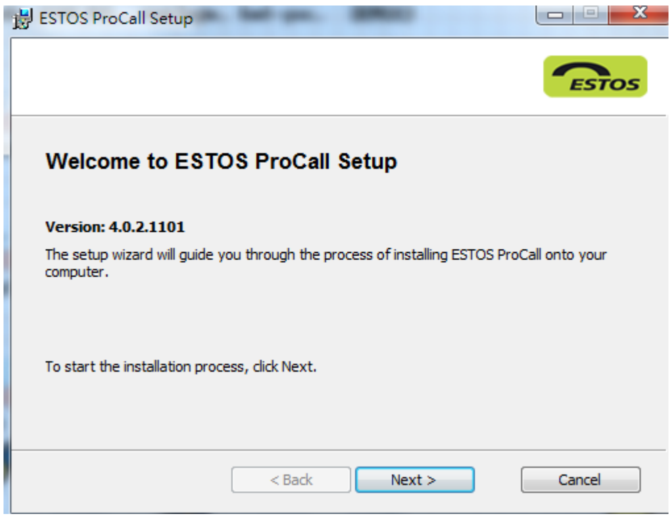
UC Server User & corresponding extension:

barbara	1010
emily	1007
tina	1008

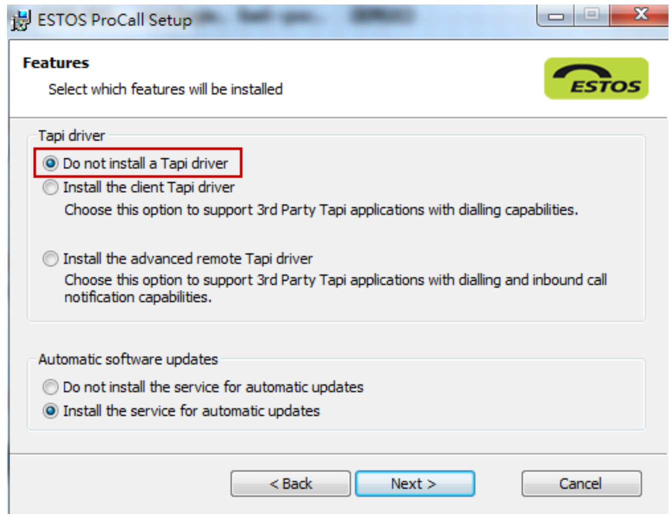
Install UC Client on the laptop.



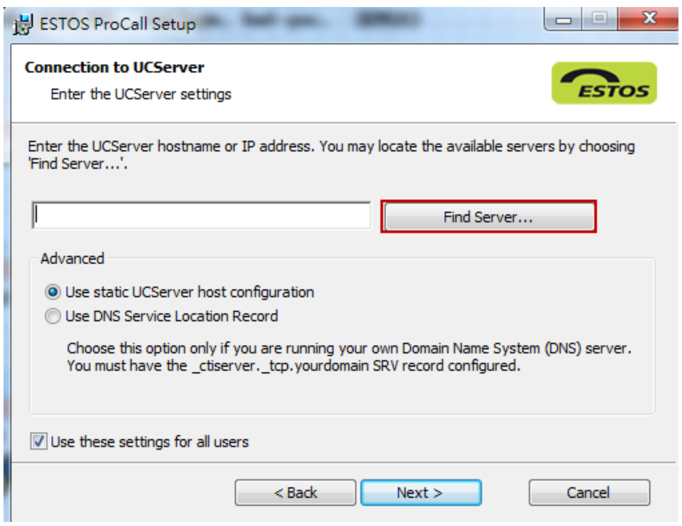
Start to install ESTOS UC client "ProCall". Keep on pressing "Next" to finish the installation.



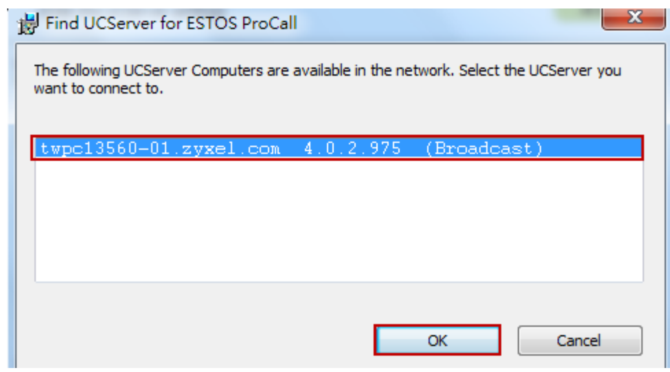
In this scenario, the ISG TAPI driver is installed on the UC server. Hence, select "Do not install a Tapi driver" in this step.



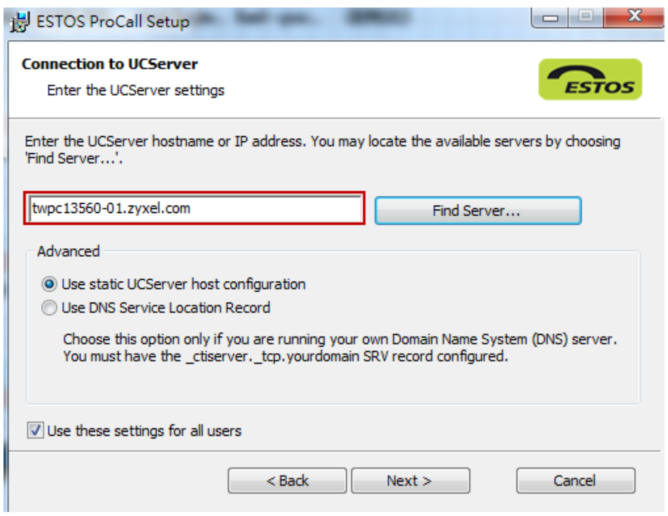
Click on “Find Server…” to select the UC Server you are connecting to.



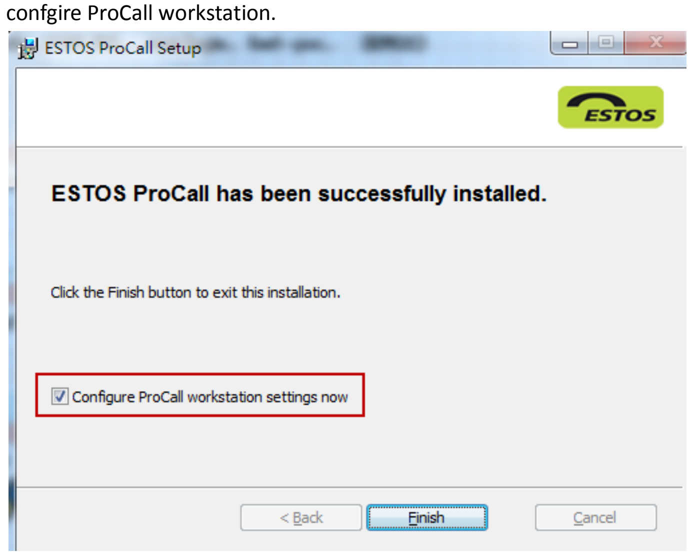
Find your UC Server and click “OK” to confirm.



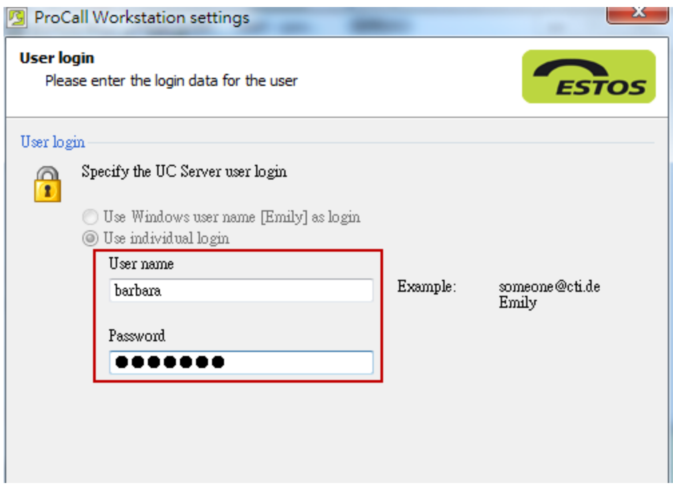
Click “Next” to proceed to the next step.



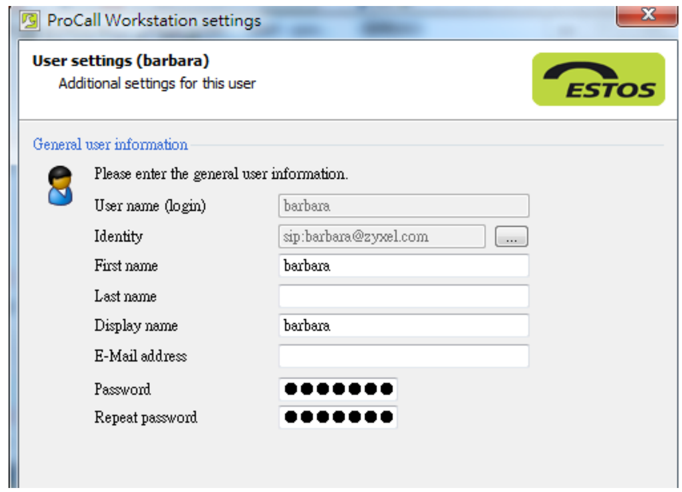
ESTOS UC client has been successfully installed. Check the box to confgire ProCall workstation.



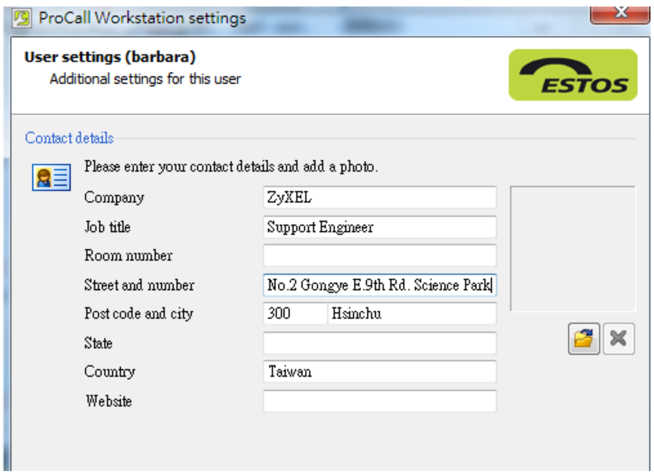
Configure the username and the password. This is one of the accounts configured in the "User" list on UC server.



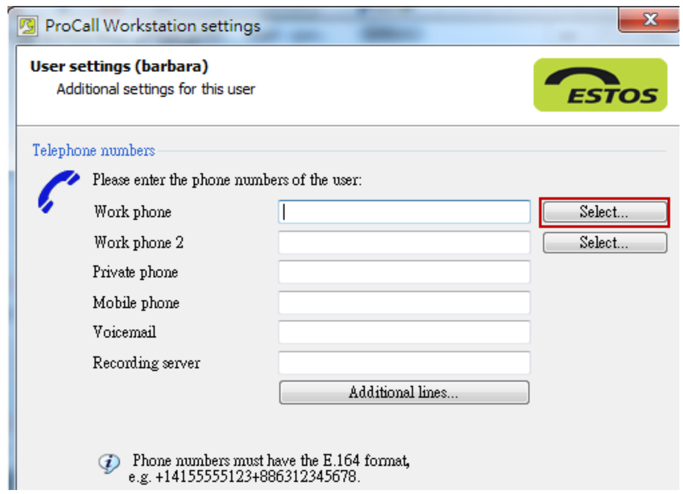
Fill in the user's personal information.



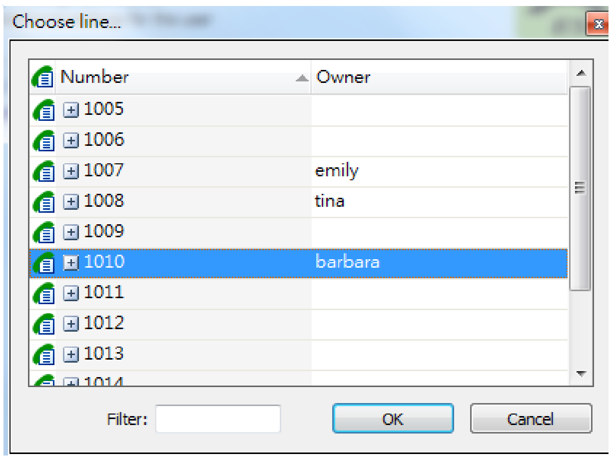
Fill in detailed information of this user.



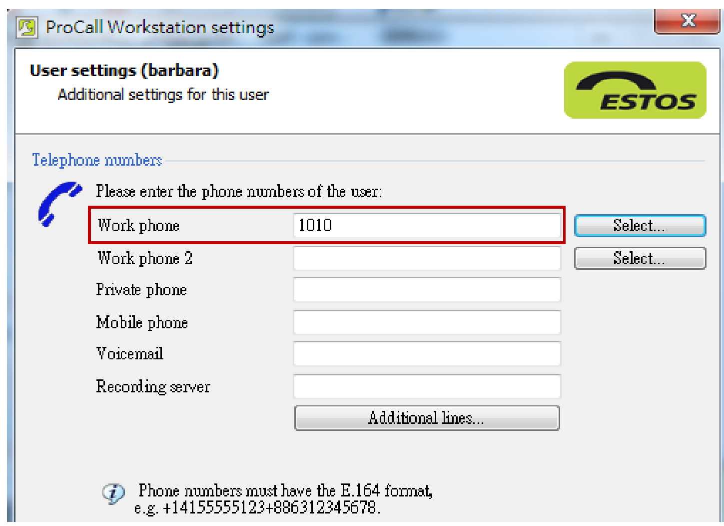
Click the “Select” button to associate a phone number to this user.



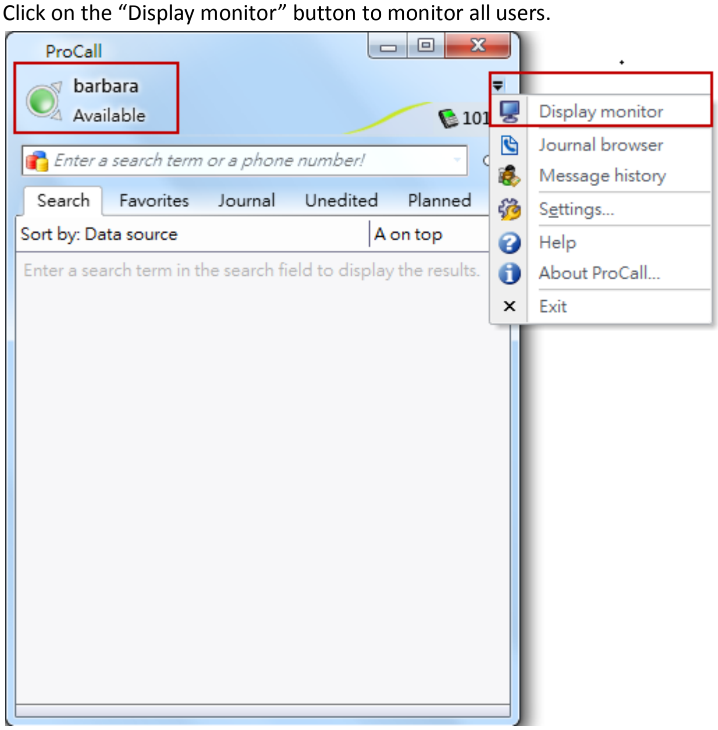
Select the corresponding phone number for this user.



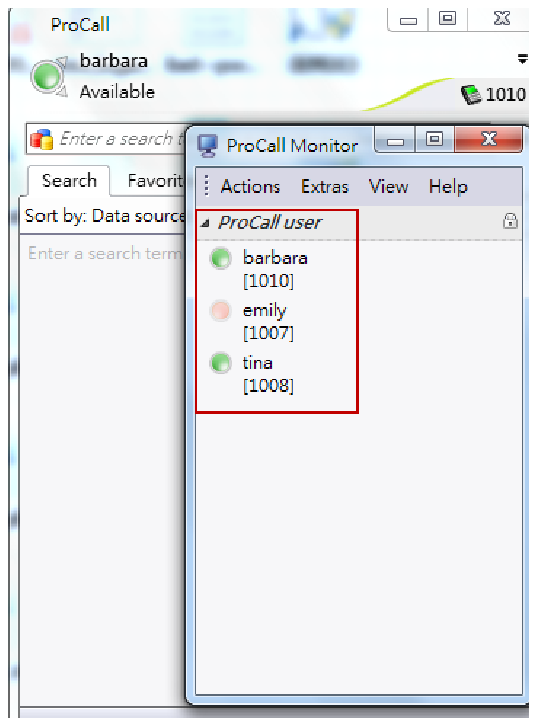
The phone number is configured.



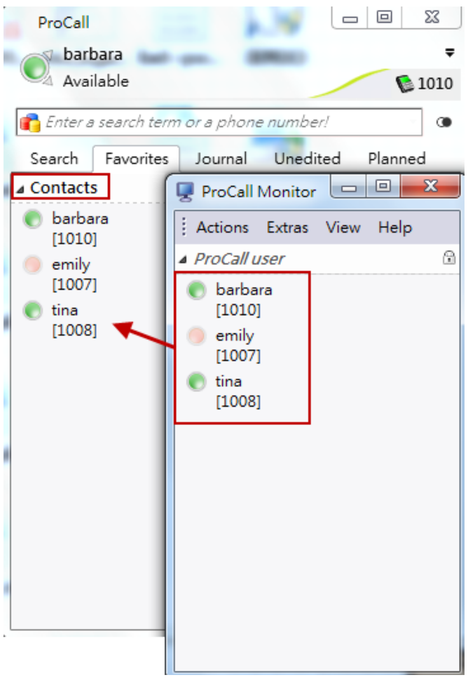
Launch the ESTOS ProCall application. Log in with the username and password.
Click on the “Display monitor” button to monitor all users.



Here is the list of all users

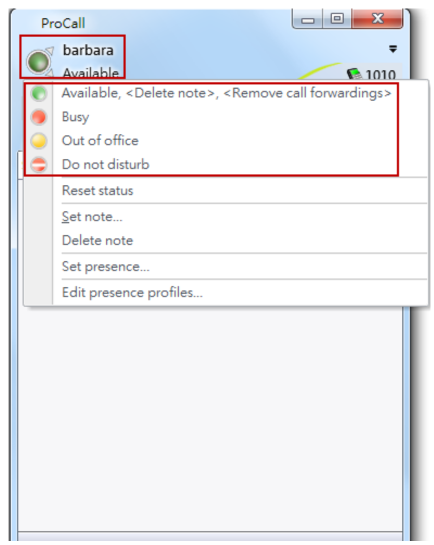


You can drag all ProCall users into “Contacts”.



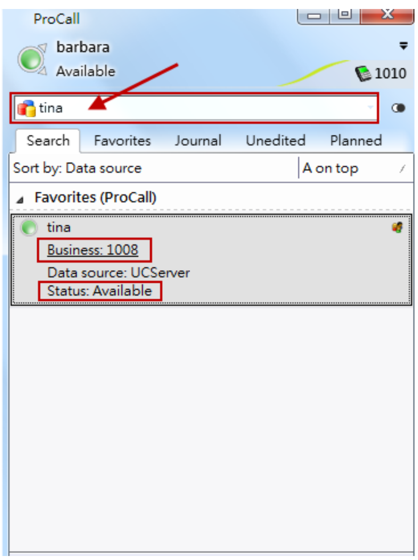
Presence

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.

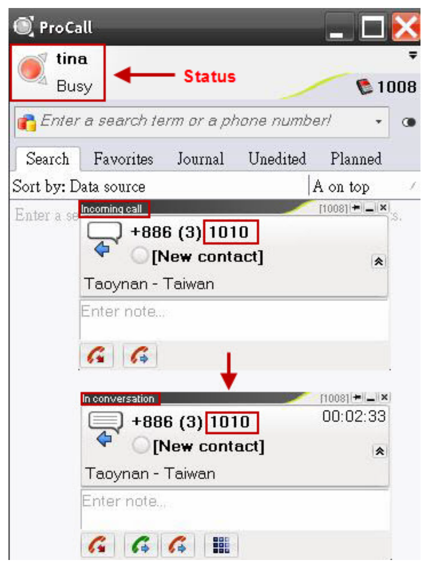


Make a call

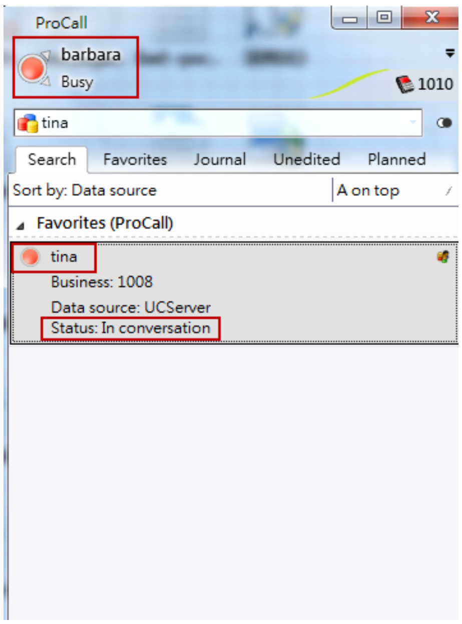
You can make a call by directly clicking on the user in the "Contacts" or by typing a phone number in the blank. In this example, barbara is making a call to tina.



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".

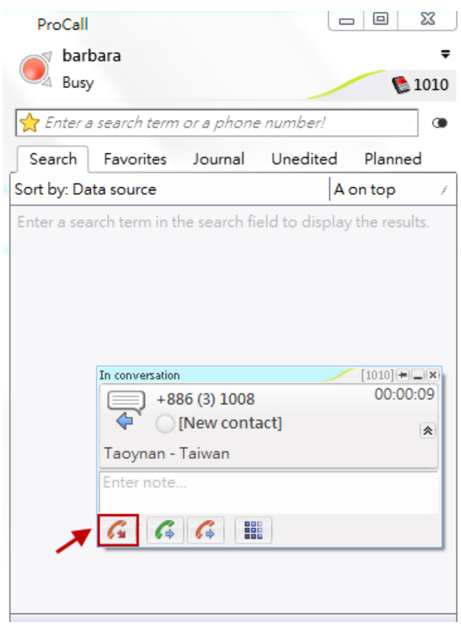


When barbara is taking with tina on the phone, the presence is "Busy" and the status of tina is "In conversation".



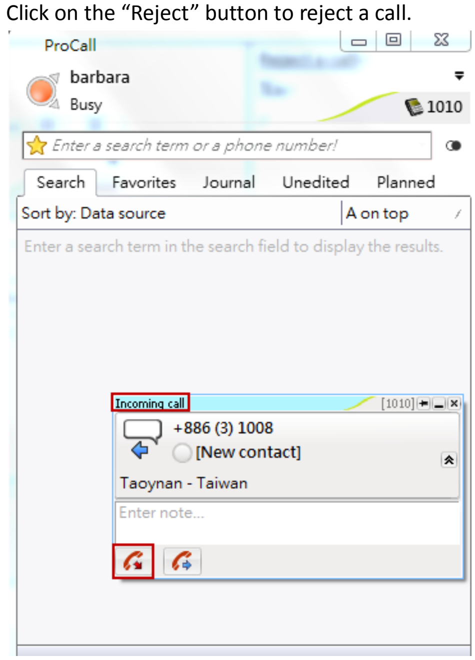
Hang up a call

Click on the button to hang up the call.



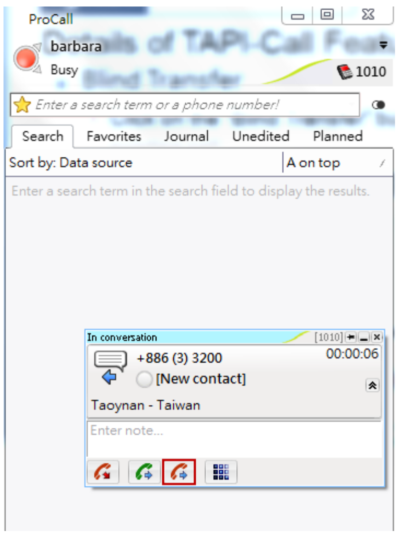
Reject a call

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

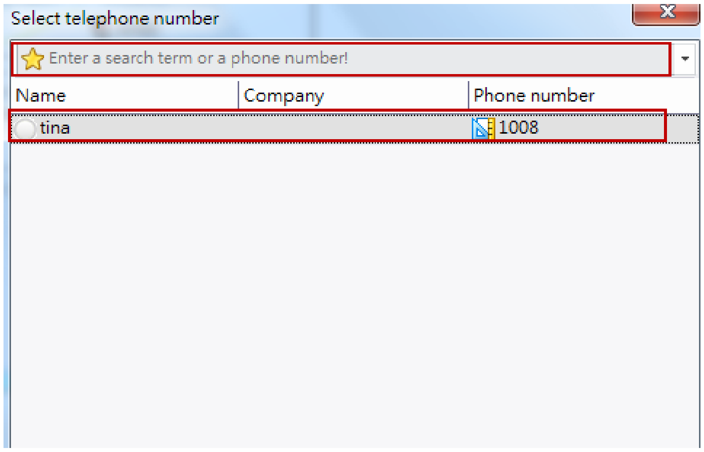


Blind Transfer

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

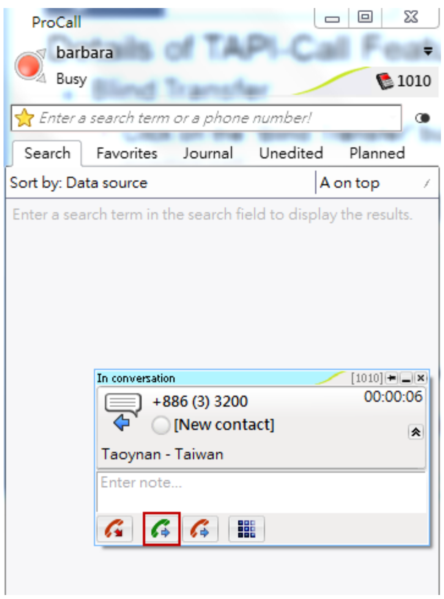


Type a phone number in the blank or click on the phone number in the list to blind transfer the call to this number. In this example, barbara gets a call from extension 3200 and then blind transfers this call to tina.

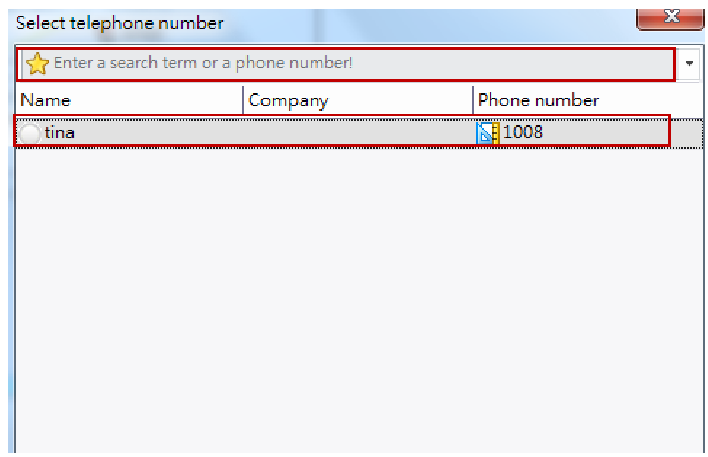


Consultant Transfer

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

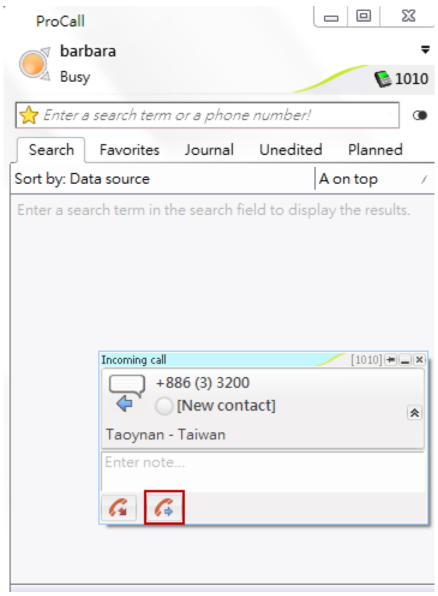


Type a phone number in the blank or click on the phone number in the list to consultant transfer the call to this number. In this example, barbara gets a call from extension 3200 and then consultant transfers this call to tina.



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.