SCOPTEL IP PBX Software - Basic Installation Hierarchy for Telephony Server

Contents

Basic Installation Hierarchy for Telephony Server

Therefore the purpose of this document is to provide a visual walkthrough of a very basic but functional installation for one tenant. This tutorial does not include an overview of the overall network configuration but does cover a basic Telephony Firewall Configuration.

Objects like telephony extensions, Class of Service, and Outgoing Lines require that other objects exist before they can be properly and efficiently configured. Configuring these objects in the correct sequence will make first time installation much more efficient and promote a better understanding of each object's intended function. It is best practice not to use Upper Case characters or Special characters when entering object names.

Here is a basic checklist to perform when setting up a new server for the first time.

- Edit Telephony Modules
- Edit Channels
- Edit Feature Codes
- Commit
- Edit Services Startup
- Packages Manager

- Interfaces Card Detect (optional but at least one physical interface must exist)
- Create VoIP Account (optional but at least one physical interface must exist)
- Create Group Interface(s)
- Create Outgoing Line(s)
- Create Class of Service objects
- Security Settings
- Create Extensions
- Create Incoming lines
- Automatic Provisioning Service
- Commit and Services Restart

Provisioning Pre-Requisites

A Provisioning Service must be running on network to provision supported IP Phones. Please refer to https://blog.scopserv.com/2013/07/how-to-use-the-SCOPTEL-automatic-provisioning-system/

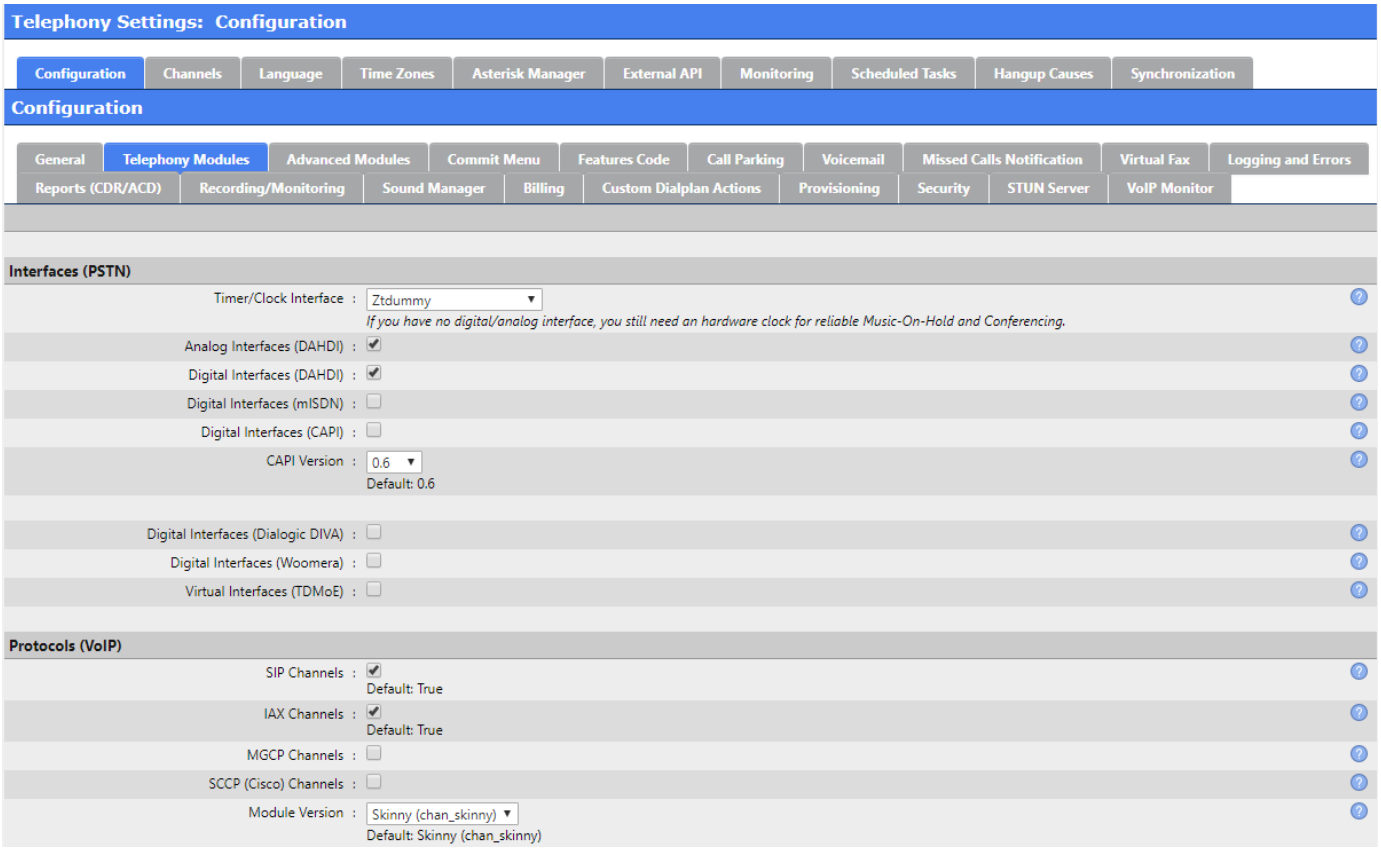
- Make sure that TFTP Service is running on the SCOPTEL server under Server General configuration tab.
- If the SCOPTEL DHCP server is being used then ensure that under Advanced Options tab that TFTP Server name is configured to point DHCP clients to LAN IP address of SCOPTEL server. Also ensure only one DHCP server is servicing that subnet. Restart the DHCP Service if any changes are made to the DHCP Server's configuration.
- If a third party DHCP server is being used on network then ensure that DHCP server on network uses Option 66 (TFTP) and points DHCP clients to LAN IP address of SCOPTEL server. Also ensure only one DHCP server is servicing that subnet.

Reboot any IP Phones connected to the network so they can download their configurations.

- If you are unsure that the phones are downloading their configurations there are two troubleshooting methods to verify configuration downloads are working.
- Navigate to Tools > File Manager > TFTP Directory and inspect each configuration file for proper configuration values. Also put any required firmware update files into this directory if any phones require to have their firmware updated.
- From a root CLI session you can verify provisioning traffic with the following command (omitting all quotation marks) "ngrep -d any host <ipaddress_of_phone> - WBYLINE". If DHCP is properly pointing client TFTP requests to the SCOPTEL server then from this CLI session you can see any file requests being received from the IP Phone during it's boot process. Verify the filename's are correct if you see Provisioning traffic reaching the SCOPTEL server.

Edit Telephony Modules

- It is essential that pre-requisite modules be enabled prior to anything being configured on the server. This is to ensure that only required VoIP protocols and PSTN hardware modules are loaded during startup.
- Edit and save the values for tab Configuration > Telephony > Configuration > Telephony Modules. Check off only the values you require.
- Recommended values are default values and Analog Interfaces (DAHDI), Digital Interfaces (DAHDI), SIP, IAX, Virtual Fax (requires Hylafax, IAXmodem, packages and related dependencies), Emergency Lines, Queues and Agents, Conferences, IVR Report/Logging, Scheduler, Asterisk Manager.

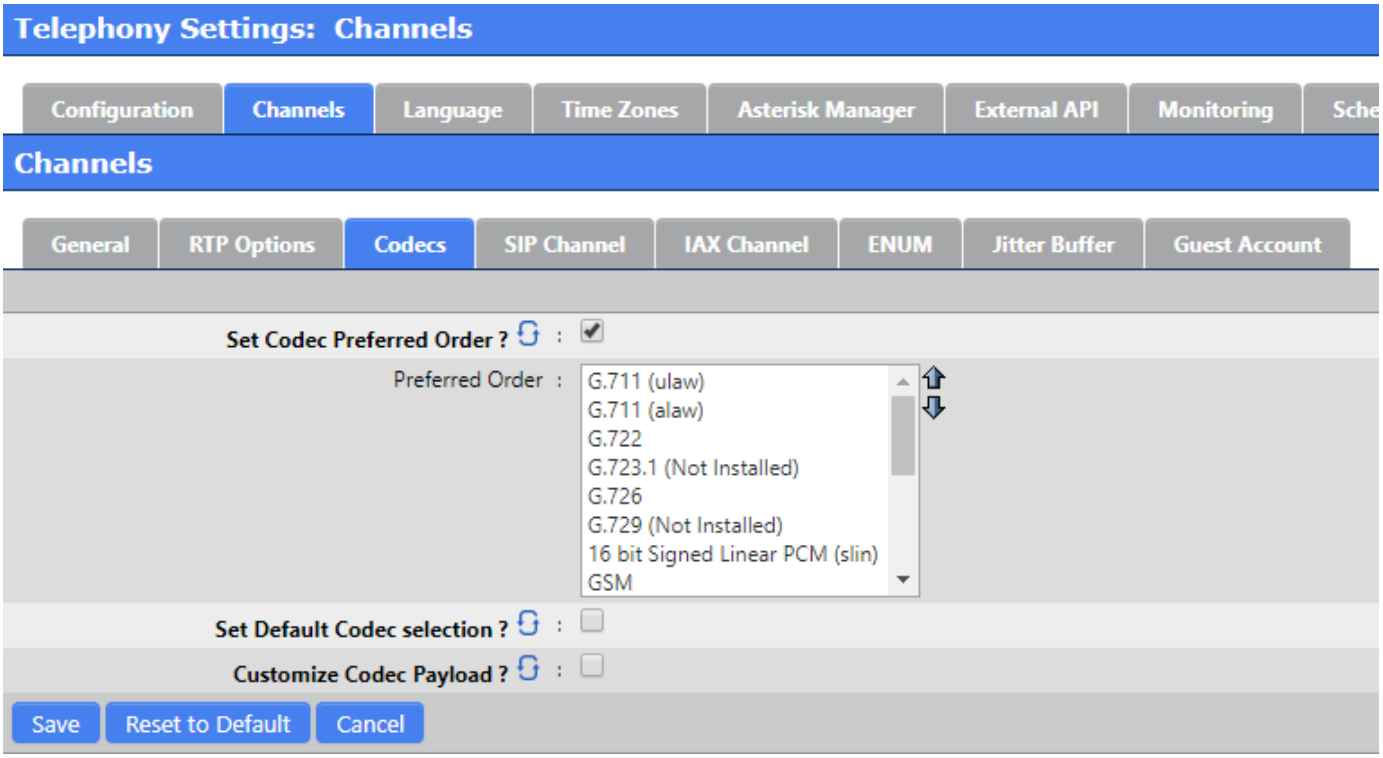


Edit Channels

You must edit your voice channels before you can finish committing your configuration. Configuration > Telephony > Configuration > Channels

This is a good time to configure your preferred CODEC order based on your geographical region. For example in North America the default CODEC used by carriers for T1 and SIP voice channels is G.711 MuLaw. End points normally negotiate CODEC selection with other end points based on the first compatible CODEC listed in the preferred CODEC order.

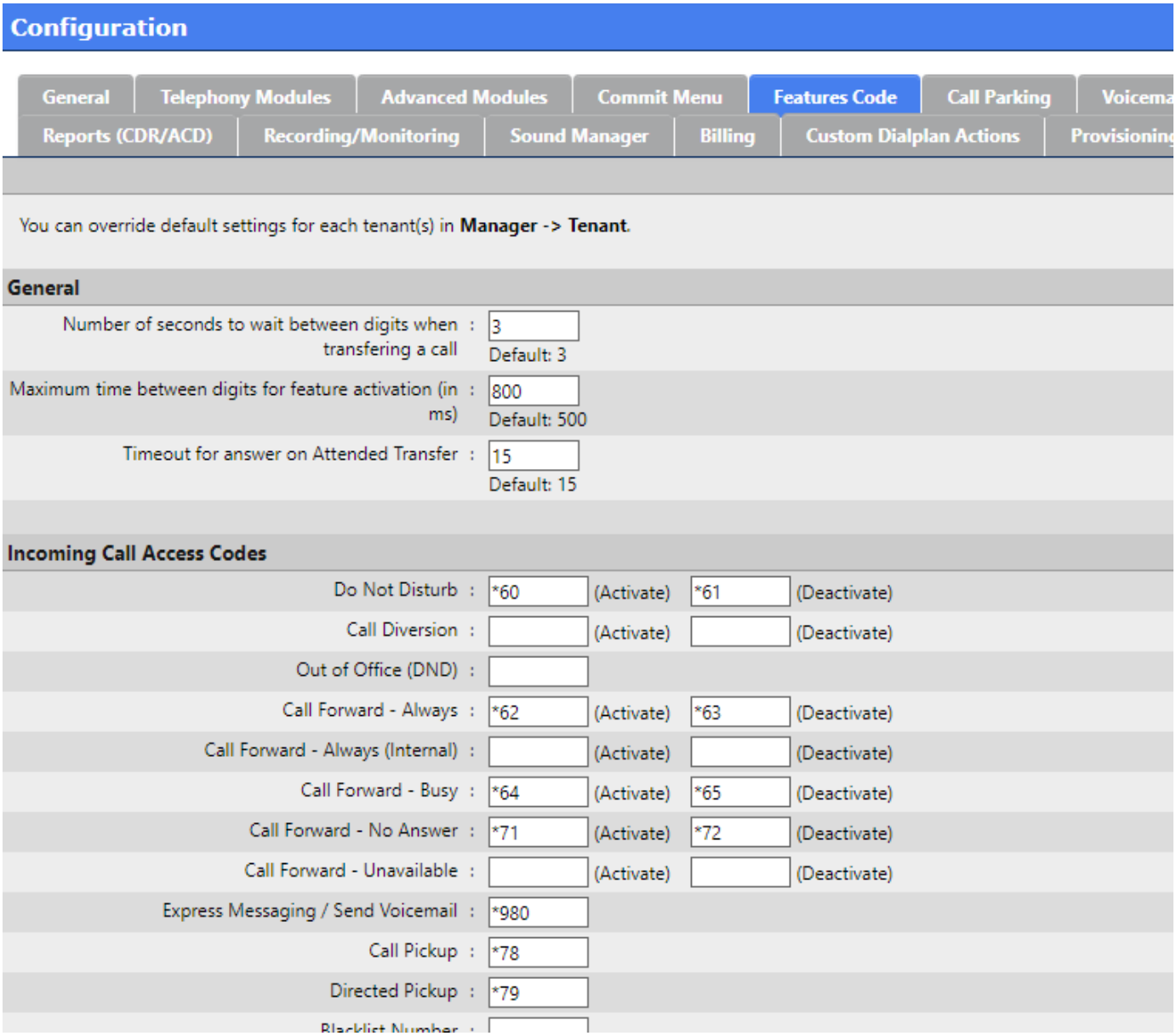
Note that server support for the G.729 CODEC is not possible without appropriate third party G.729 licenses or CODEC transcoding hardware. Transcoding is very CPU heavy therefore hardware transcoding is recommended if necessary since this offloads transcoding from the SCOPTEL CPU. See https://blog.scopserv.com/2012/12/how-to-install-a-sangoma-transcoding-solution-in-SCOPTEL/



Edit Feature Codes

Each feature of the Telephony Server is activated by the user using DTMF feature codes. When the server recognizes DTMF feature codes entered via a user's extension then the server verifies this feature request using the "Class of Service" configured for that extension. If the feature is not listed in the Class of Service configured for that extension the server denies the request and the "Call Fails".

The feature code list is basically a list of DN's (Directory Numbers). This list may be customized but the feature code must not match another Application, Extension, Outgoing Line, Emergency Line, or Special Line. In order to emulate "En Bloc" signalling each phone provisioned by the SCOPTEL's APS (Automated Provisioning System) must include fixed dial plan options/entries for each feature code.

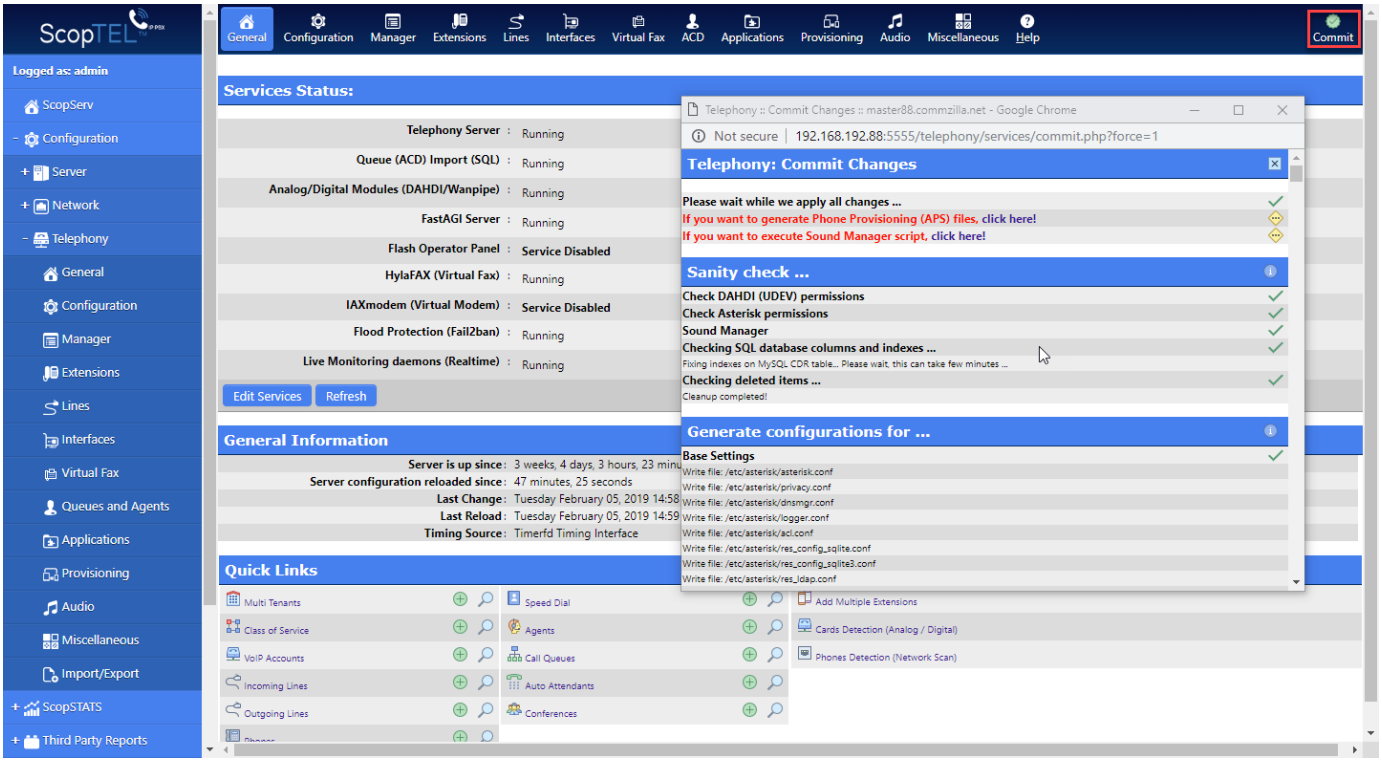


Commit

Once the modules, channels, and feature codes have been edited it is necessary to commit the changes to the server so that the proper service start-up options can be configured and started.

Any time a change in configuration is detected the “Commit” button will be visible at the top right hand corner of the SCOPTEL Telephony GUI module screen. Click this button to reload all configurations after you have saved your required changes. Clicking on this Commit button will only write detected changes to the internal database configurations.

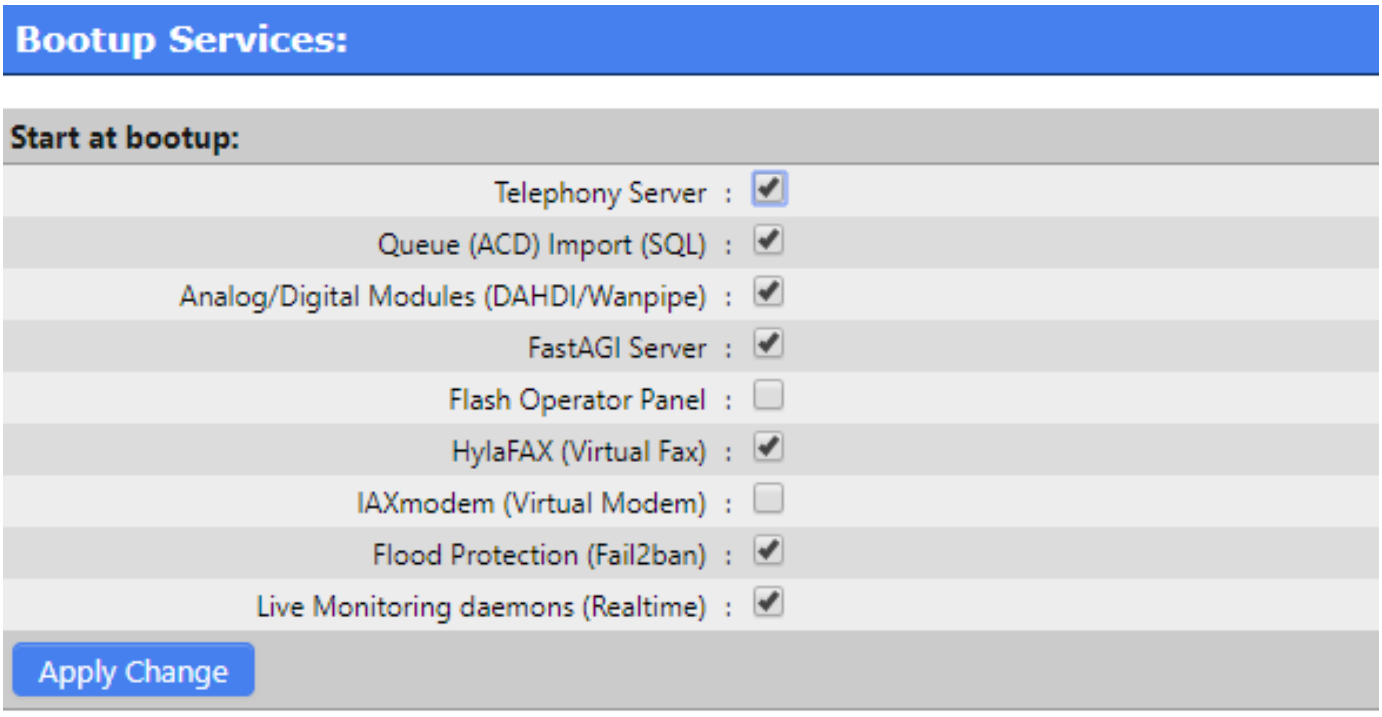
If a full configuration re-write is required then a “Full Commit” can be done from Configuration > telephony > Configuration > General screen. The “Full Commit” is only possible from this screen. Note: This Commit button appears as a normal “Commit” button at the top right corner of the Telephony GUI page. This screenshot displays a “Full Commit” from the “General” tab.



Edit Services Startup

Configuration > Telephony > Configuration > General > Edit Services > Edit

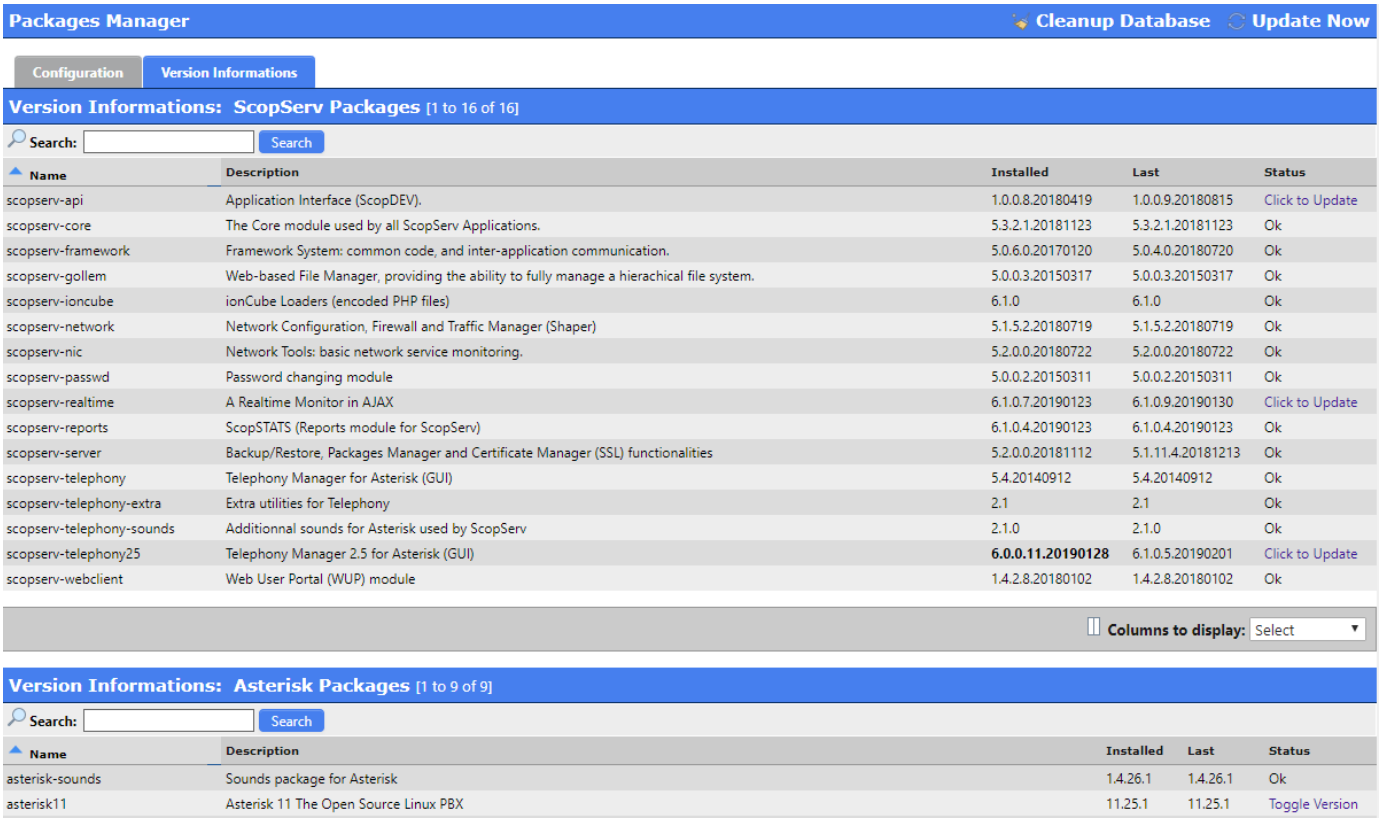
Check off the services required after a server reboot so they start automatically without manual intervention and so that they are loaded in the correct order. Apply Changes when you are done to return to the “General” screen.



Packages Manager

If a service cannot “Commit” or cannot start because it is not installed then you must install the required packages and dependencies.

A valid software maintenance contract must be in place with SCOPSERV in order to update or install SCOPTEL packages. To install any required packages navigate to Configuration > Server > Packages Manager > Version Information and click on any required links to install any required packages



Packages Manager — Cleanup Database — Update Now

Configuration | Version Informations

Version Informations: ScopServ Packages [1 to 16 of 16]

Search: Search

Name	Description	Installed	Last	Status
scopserv-api	Application Interface (ScopDEV).	1.0.0.8.20180419	1.0.0.9.20180815	Click to Update
scopserv-core	The Core module used by all ScopServ Applications.	5.3.2.1.20181123	5.3.2.1.20181123	Ok
scopserv-framework	Framework System: common code, and inter-application communication.	5.0.6.0.20170120	5.0.4.0.20180720	Ok
scopserv-gollem	Web-based File Manager, providing the ability to fully manage a hierachical file system.	5.0.0.3.20150317	5.0.0.3.20150317	Ok
scopserv-ioncube	ionCube Loaders (encoded PHP files)	6.1.0	6.1.0	Ok
scopserv-network	Network Configuration, Firewall and Traffic Manager (Shaper)	5.1.5.2.20180719	5.1.5.2.20180719	Ok
scopserv-nic	Network Tools: basic network service monitoring.	5.2.0.0.20180722	5.2.0.0.20180722	Ok
scopserv-passwd	Password changing module	5.0.0.2.20150311	5.0.0.2.20150311	Ok
scopserv-realtime	A Realtime Monitor in AJAX	6.1.0.7.20190123	6.1.0.9.20190130	Click to Update
scopserv-reports	ScopSTATS (Reports module for ScopServ)	6.1.0.4.20190123	6.1.0.4.20190123	Ok
scopserv-server	Backup/Restore, Packages Manager and Certificate Manager (SSL) functionalities	5.2.0.0.20181112	5.1.11.4.20181213	Ok
scopserv-telephony	Telephony Manager for Asterisk (GUI)	5.4.20140912	5.4.20140912	Ok
scopserv-telephony-extra	Extra utilities for Telephony	2.1	2.1	Ok
scopserv-telephony-sounds	Additionnal sounds for Asterisk used by ScopServ	2.1.0	2.1.0	Ok
scopserv-telephony25	Telephony Manager 2.5 for Asterisk (GUI)	**6.0.0.11.20190128**	6.1.0.5.20190201	Click to Update
scopserv-webclient	Web User Portal (WUP) module	1.4.2.8.20180102	1.4.2.8.20180102	Ok

Columns to display: Select

Version Informations: Asterisk Packages [1 to 9 of 9]

Search: Search

Name	Description	Installed	Last	Status
asterisk-sounds	Sounds package for Asterisk	1.4.26.1	1.4.26.1	Ok
asterisk11	Asterisk 11 The Open Source Linux PBX	11.25.1	11.25.1	Toggle Version

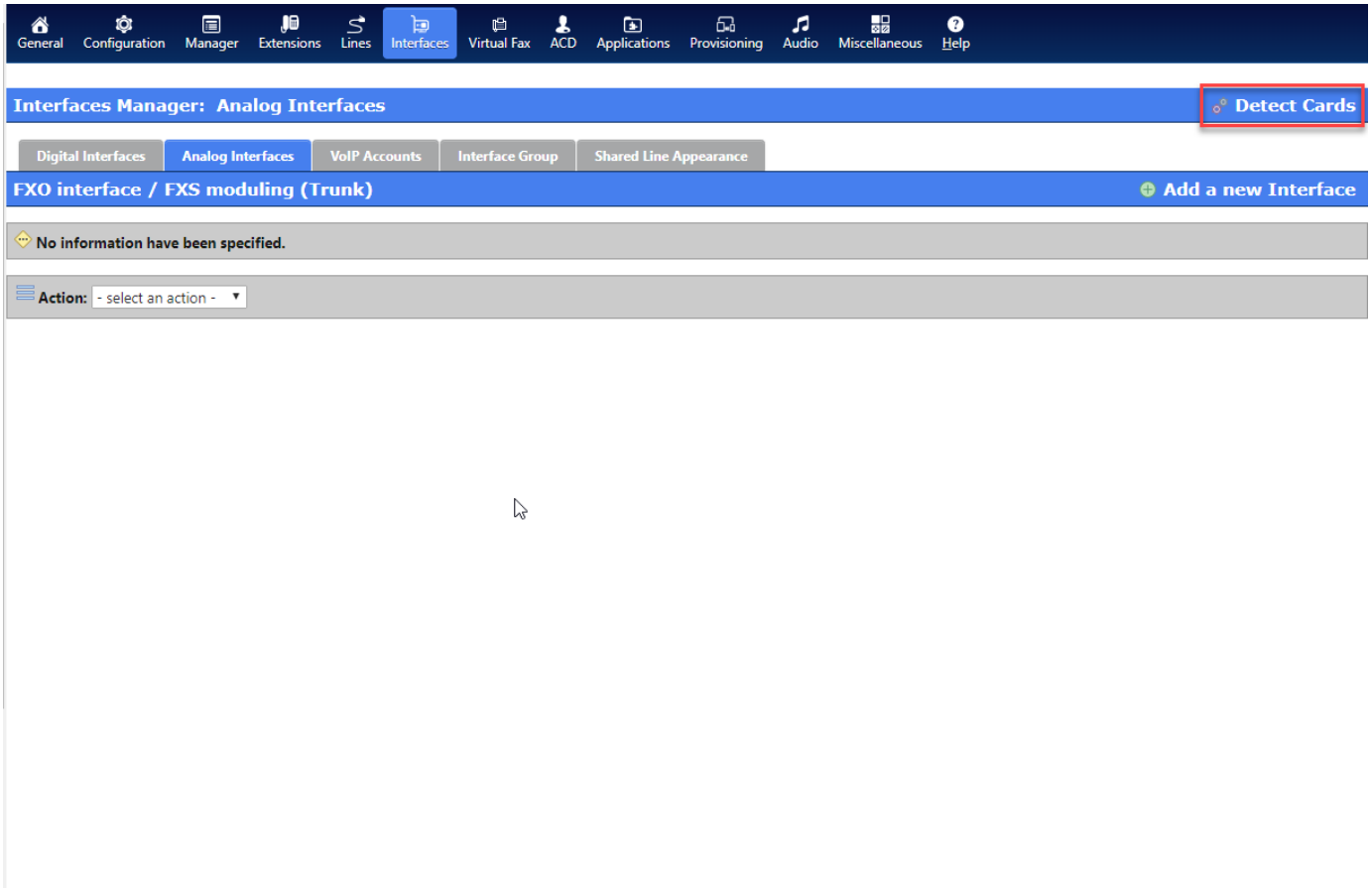
Interfaces Card Detect

If any analog FXO/FXS or T1/E1 or BRI cards are installed then you must do a “Card Detect” to recognize and configure that hardware before the drivers and configurations can be properly loaded. Configuration > Telephony > Interfaces > Detect Cards

Follow the pop-up windows to complete the card detection procedure and be certain to read and follow any instructions that will appear in those pop-up windows. After your PSTN hardware is detected and the required services are running it will be necessary to configure regional properties and gain settings for each of your PSTN cards and ports. If a change is made to any settings on the “Interfaces” tabs it is a good practice to “Commit” those changes and then restart the following services in the correct order. First navigate to the “General” tab…

The correct order to reset services is:

- Stop the “Telephony Server”
- Restart the “Analog/Digital Modules (Zaptel/Wanpipe)
- Start the “Telephony Server”



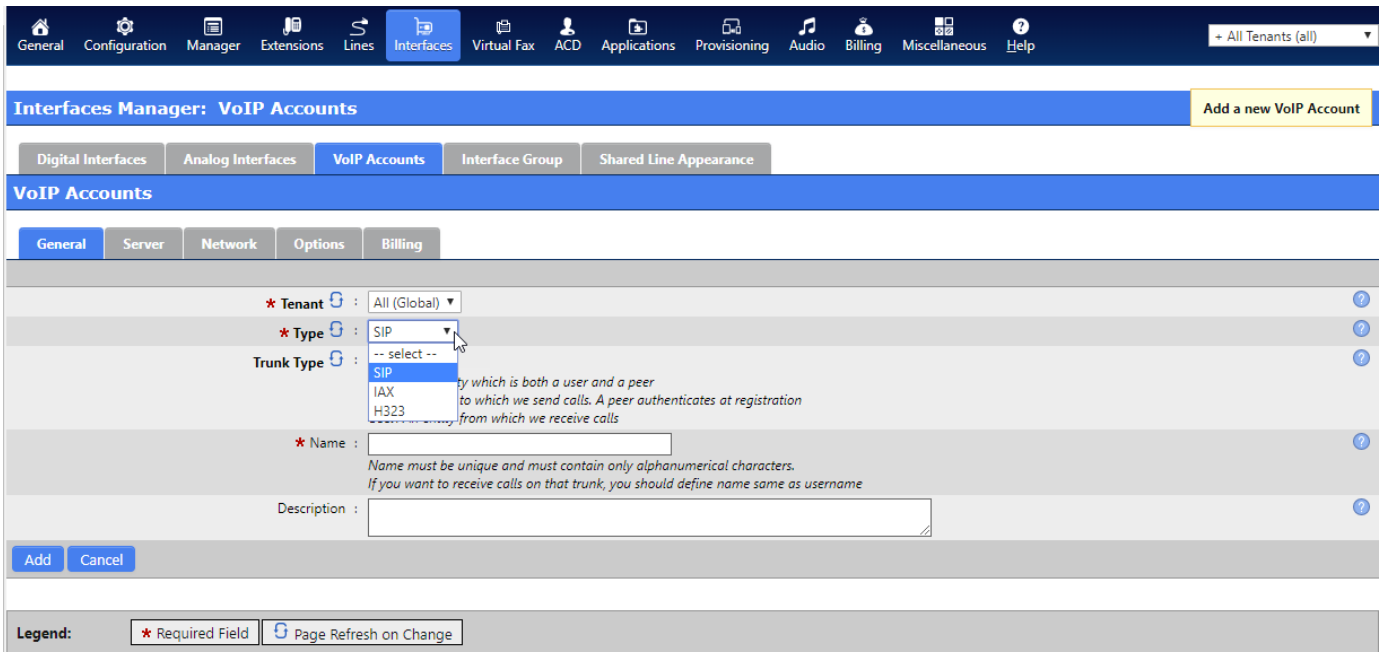
VoIP Accounts

Add a new VoIP Account

A typical VoIP Interface would normally use the industry standard SIP technology. Therefore this example will cover the creation of a CPE side (Customer Provided Equipment) SIP account.

SIP trunks normally require a SIP Registrar for client authentication and a SIP Proxy to handle signaling and media. It is common for the SIP Registrar and SIP Proxy to be the same server but the SIP Registrar and SIP Proxy can reside on different servers.

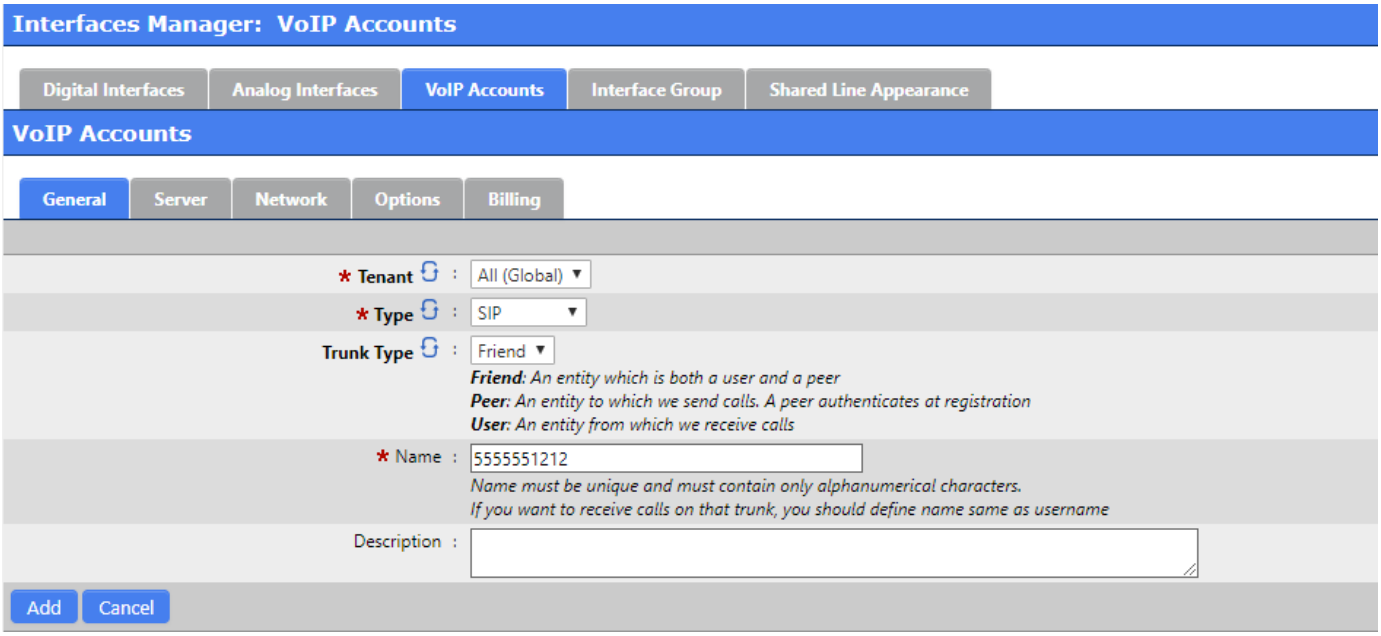
To create a new SIP Interface navigate to Configuration > Telephony > Configuration > Interfaces > VoIP Accounts and Click “Add a New VoIP Account” and choose SIP from the drop down list.



General

The name field is mandatory and it is typical for the name of the SIP trunk to equal the SIP username provided by the SIP ITSP (Internet Telephony Service Provider). A SIP Friend allows both Incoming and Outgoing Calls and is most typical.

In this example the name of our SIP trunk is 5555551212. When the General properties are entered click on the Server tab next to add the authentication properties and the address of the SIP Registrar and Proxy.



Server

Use the Plaintext option to enter username and password into the matching fields (MD5 will be used to encrypt the authentication during transit).

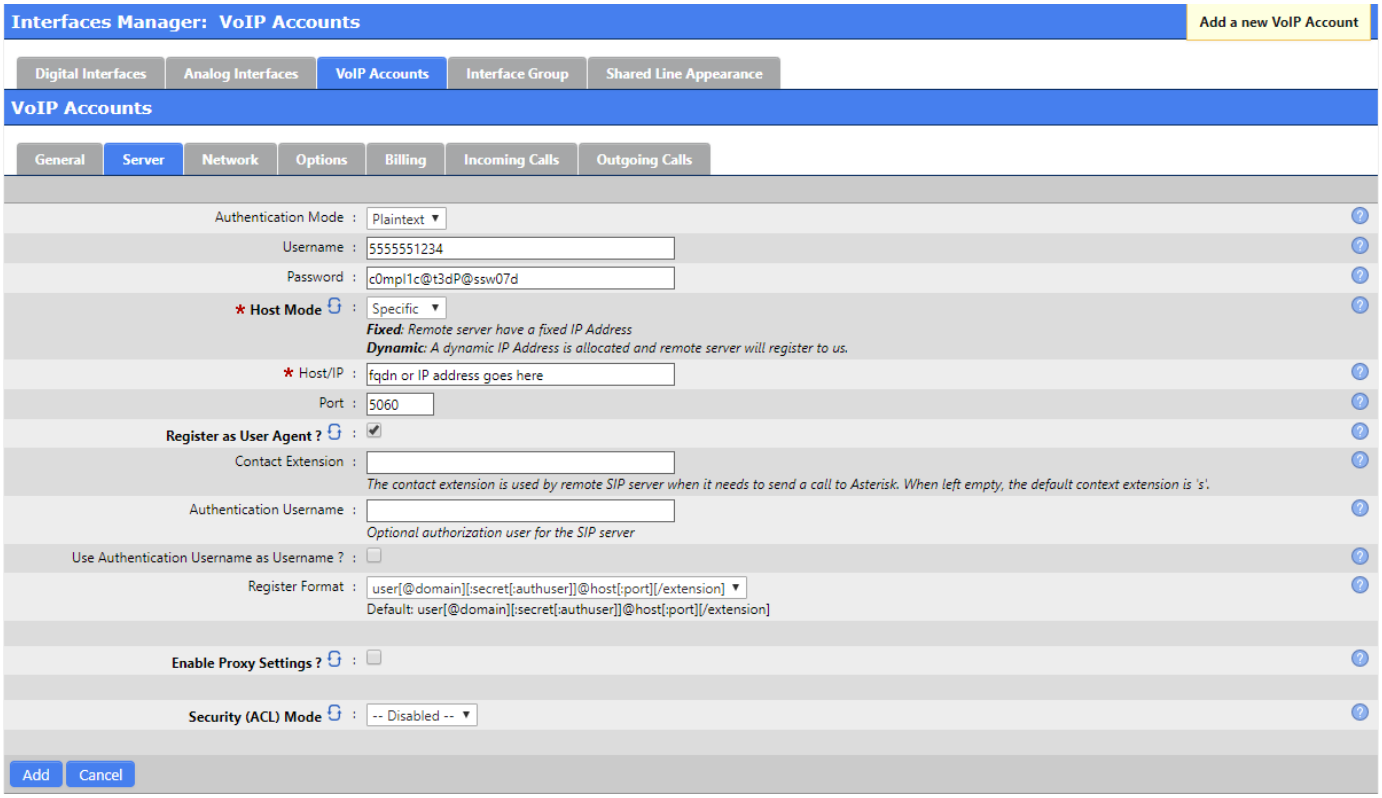
Host Mode Specific is chosen when the server is authenticating to a Dynamic Account like an ITSP in Client Mode.

- Enter either the FQDN or IP address of the remote Dynamic Account

Dynamic Mode is chosen when the remote VoIP Account is authenticating to this VoIP Interface.

In this example we authenticating to a remote account therefore we must choose Host Mode Specific. Registration is required to check the box for Register as User Agent

When finished click on the Network tab



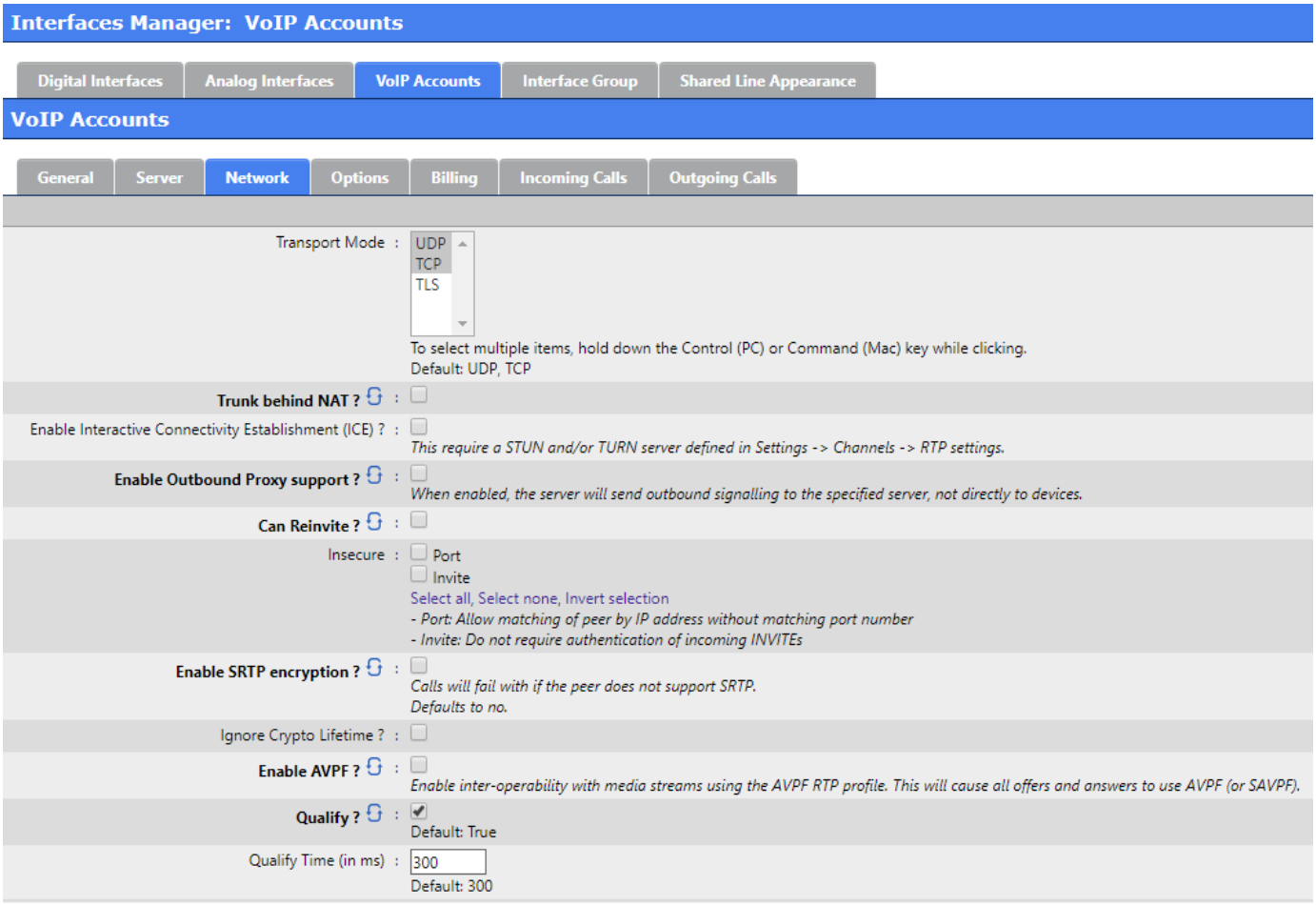
Network

If the server is situated behind a third party NAT Router/Firewall then check off the box for Trunk Behind NAT.

If the server is situated behind a third party NAT Router/Firewall then the third party Firewall rules must port forward the following rules to the LAN IP address of the SCOPTEL server. 5060/udp 10000-20000/udp.

Also a static public IP address and/or FQDN (Fully Qualified Domain Name) is recommended for the SCOPTEL server to help negotiate Firewall related RTP issues. This IP address or FQDN is entered into the text field located at Configuration > Telephony > General > External IP or Hostname and the “Server behind NAT ?[ ]” option be checked [x].

It is common for most SIP ITSP’s to require the Insecure options Port, Invite to be checked. The SIP Qualify Time is defined in seconds (default 300 seconds). The server will send a SIP qualify message to the ITSP every 300 seconds. This allows the ITSP to monitor the status of the SIP registration and latency. When finished here click on the Options tab.



Options

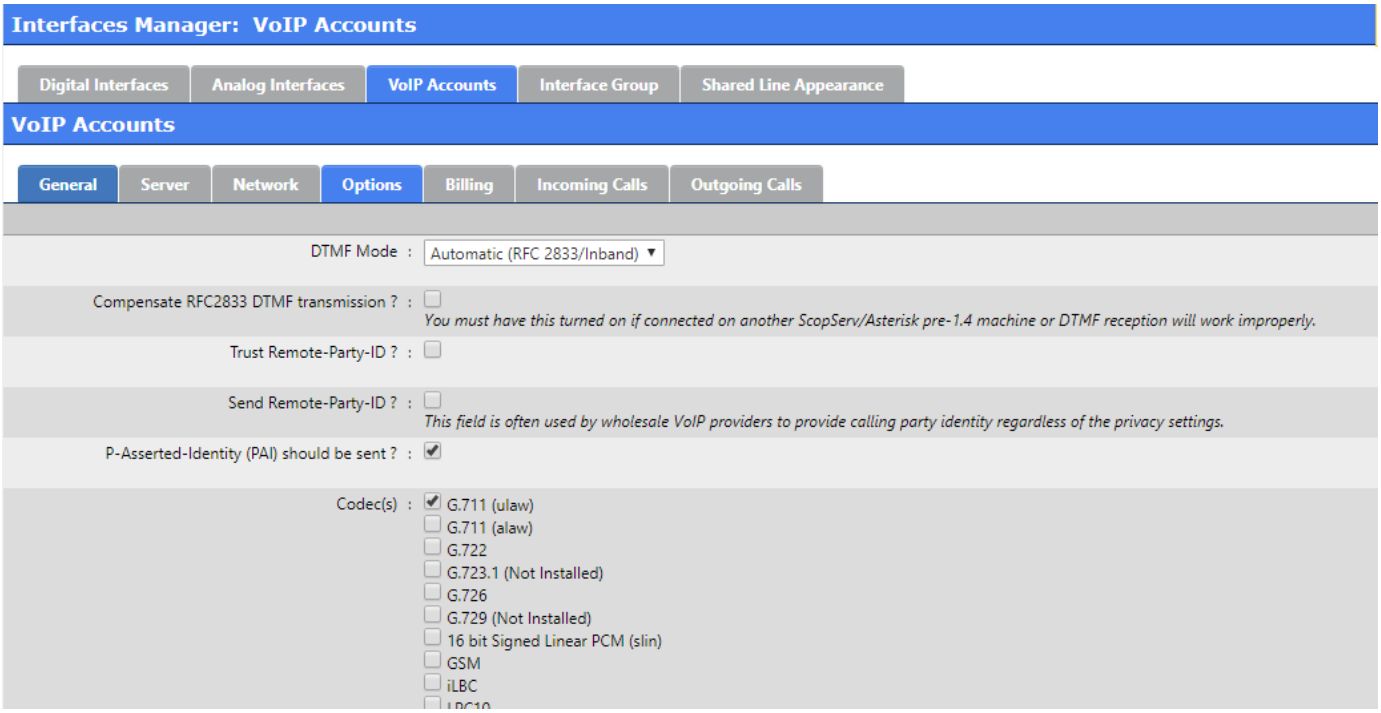
The correct DTMF mode must be selected to match with the requirements of the ITSP. Typically “Automatic RFC-2833/inband” is selected. However most ITSP’s support RFC-2833 because it is more reliable.

The CODEC selection must match the requirements of the ITSP and any supported CODEC’s not checked off will never be negotiated with the ITSP because they have not been allowed. The global Channel options defined in Configuration > Telephony > Configuration > Channels > Codecs will choose the first supported CODEC in the preferred order.

Not all provider support P-Asserted Identity (PAI) but this setting is required for dynamic Caller ID updates such as Connected Party.

Remote Party ID (RPID) is supported by many ITSP’s to support Caller ID Name and Number but RPID is considered a Legacy Protocol.

No other options are required at this time so it is OK to click on the “Add” button.



Interface Groups

Once your PSTN hardware is detected and the required services are running you can set up Interface Groups.

An Interface Group is a “pool” of physical DAHDI interfaces:

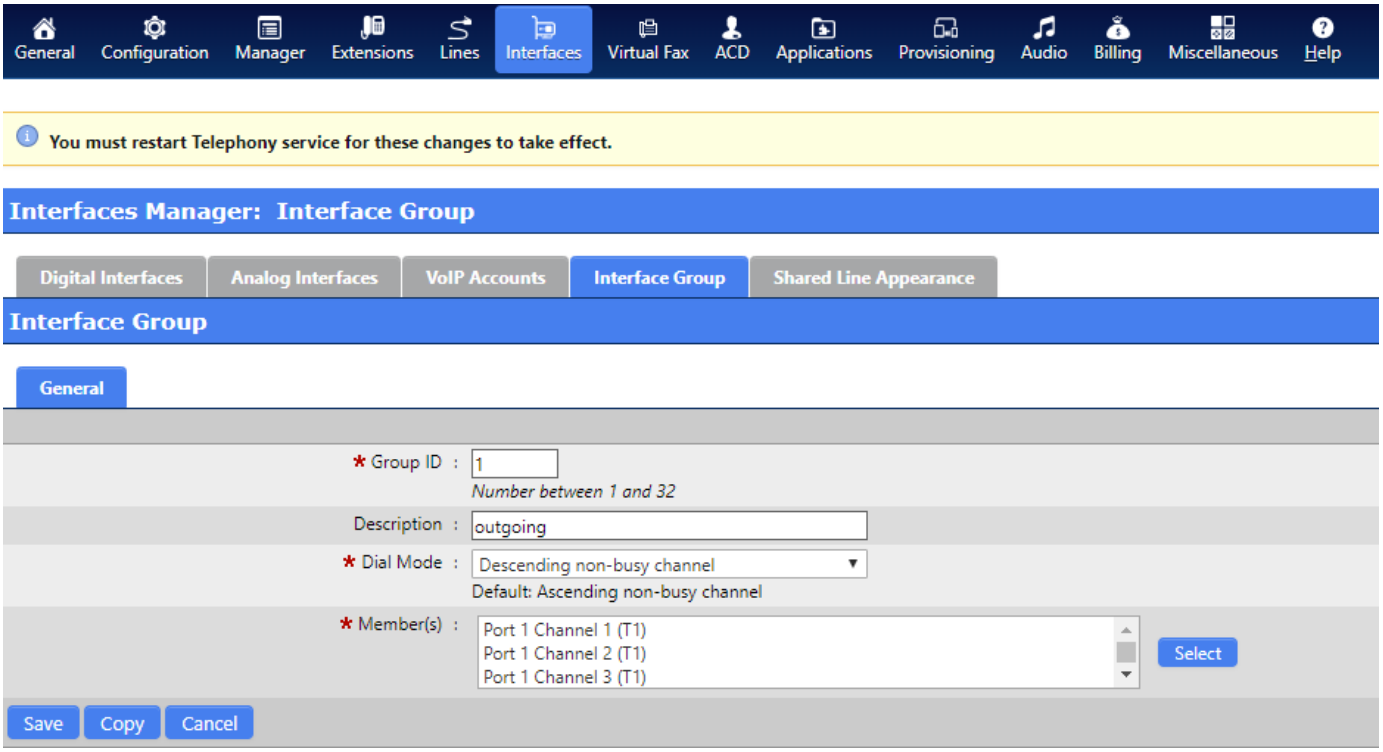
If you are using DADHI hardware

- Navigate to Configuration>Telephony>Configuration>Interfaces>Interface Group>Add a new Group
- The Group Interface can be a collection of DAHDI PRI, FXO, interfaces but it is normally a collection of only one technology.
- The purpose of an Outgoing Line Group is to isolate outgoing physical interfaces to specific Applications, Extensions, Outgoing Lines, Emergency Lines, Special Lines.

For example there are 10 FXO (analog PSTN lines aka POTS lines) ports shared between two companies:

- FXO ports 1-2 belong to Company ABC
- FXO ports 3-4 belong to Company XYZ
- Group 1 is a collection of FXO ports 1-2
- Group 2 is a collection of FXO ports 3-4
- Therefore Group 1 belongs to Company ABC and Group 2 belongs to company XYZ.

In this screenshot a PRI Outbound Group is configured using T1 B channels 1-23 in Descending order 23>1 to prevent network glare.

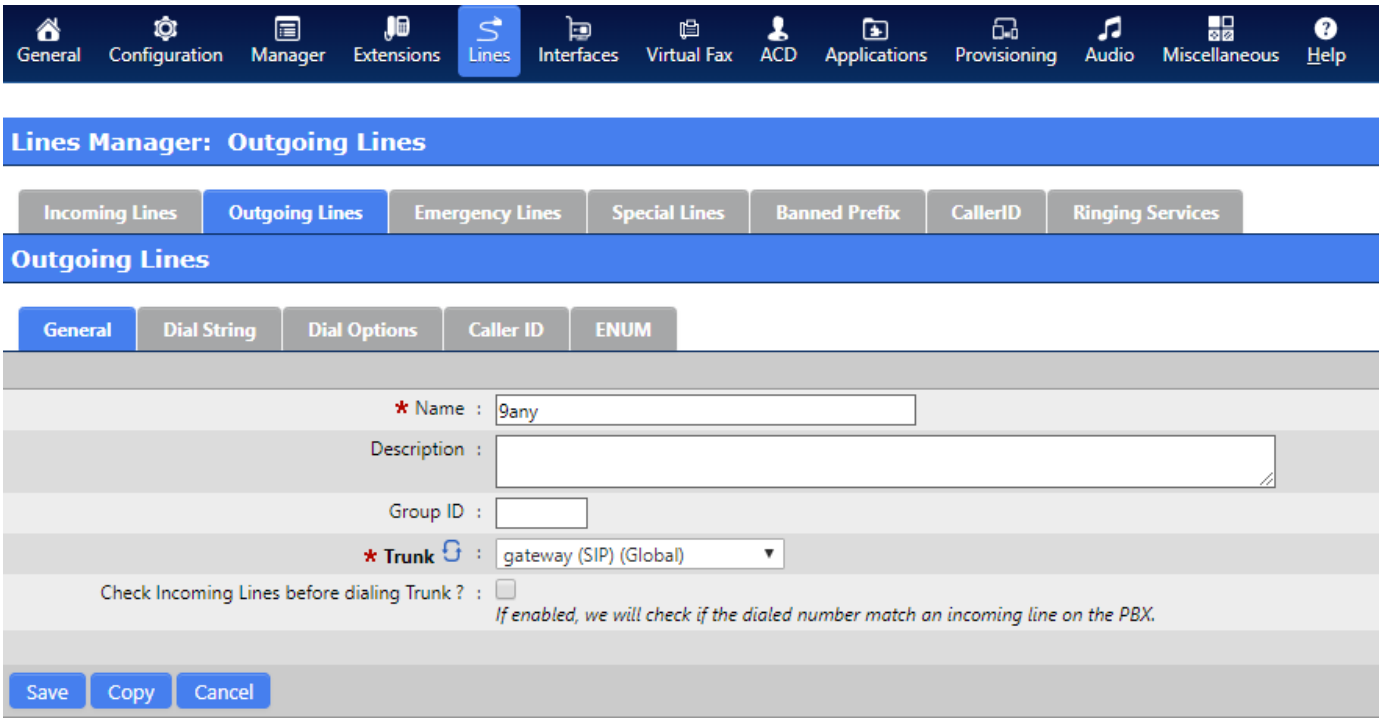


Outgoing Lines

General

Outgoing Lines use dial patterns to select from SCOPTEL Interfaces to place outgoing calls. Recommended interfaces are DAHDI, SIP. Other interface types exist like MGCP, IAX2, SCCP/Skinny, H323 are available but fall into extended or limited support categories. Outgoing calls can be PSTN interfaces or Private TIE trunks. A lot of detailed configuration information can be found on the SCOPTEL knowledgebase at http://blog.scopserv.com

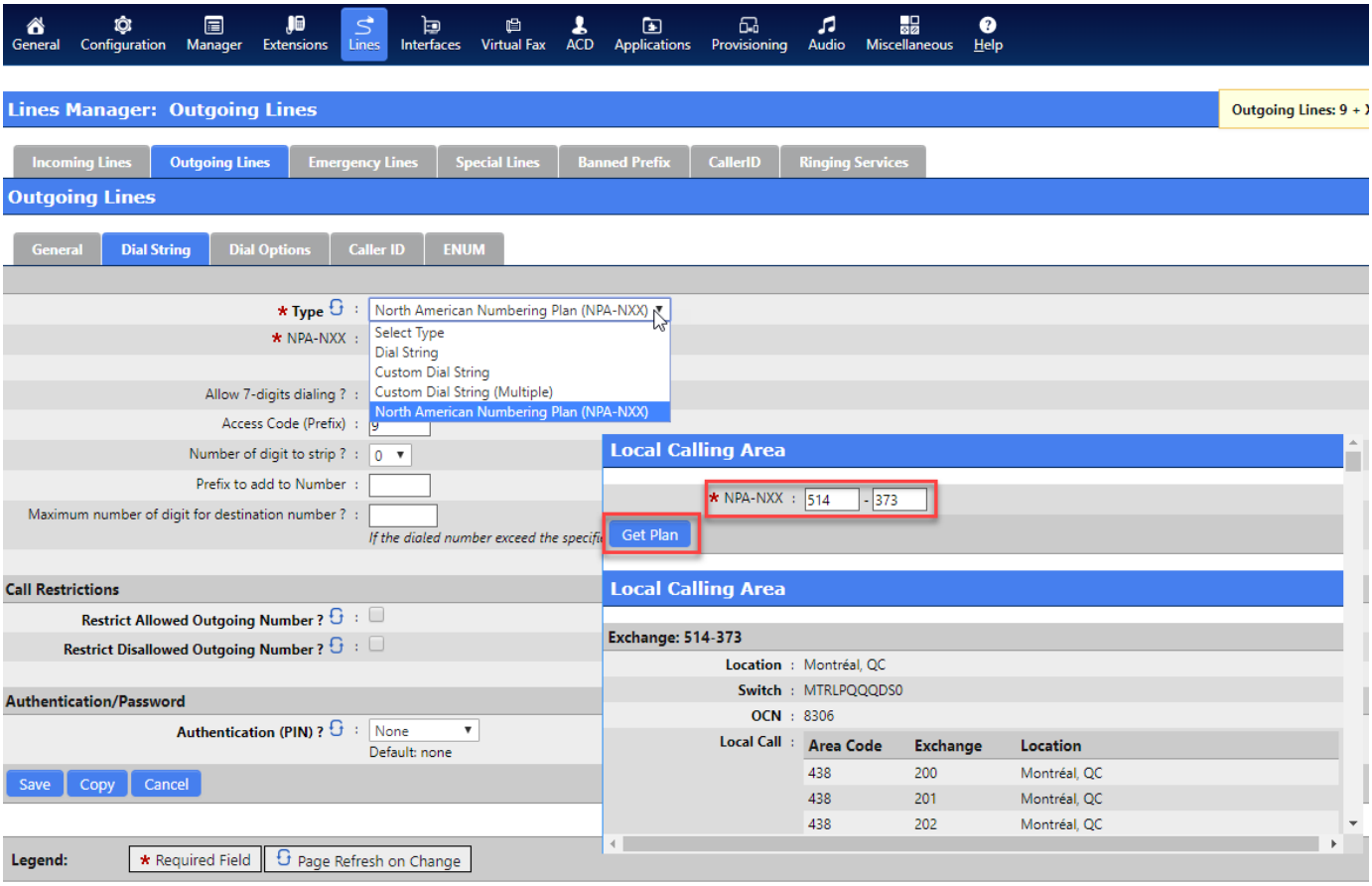
To create an Outgoing Line navigate to Configuration > Telephony > Lines > Outgoing Line then Click “Add a New Outgoing Line”. Enter a unique name for the new Outgoing Line. The name can match the dial pattern used for easier documentation of the configuration. Choose the correct Trunk/Technology for this Outgoing Line. Choose the correct Interface Group if applicable. Click on the Dial String tab



NPA-NXX

One of the most powerful and unique features in the SCOPTEL IP PBX is the ability to download the entire NPA-NXX dial plan for any supported Area Code and Prefix. This greatly simplifies the LCR (Least CoSt Routing) dial plan configuration for the server. Hours and possibly days of configuration are reduced to seconds. However in this tutorial only a simple “Custom Dial String” option will be used.

After clicking on the “Dial String” tab choose “Custom Dial String” and the page will automatically refresh.



Custom Dial Plan Strings

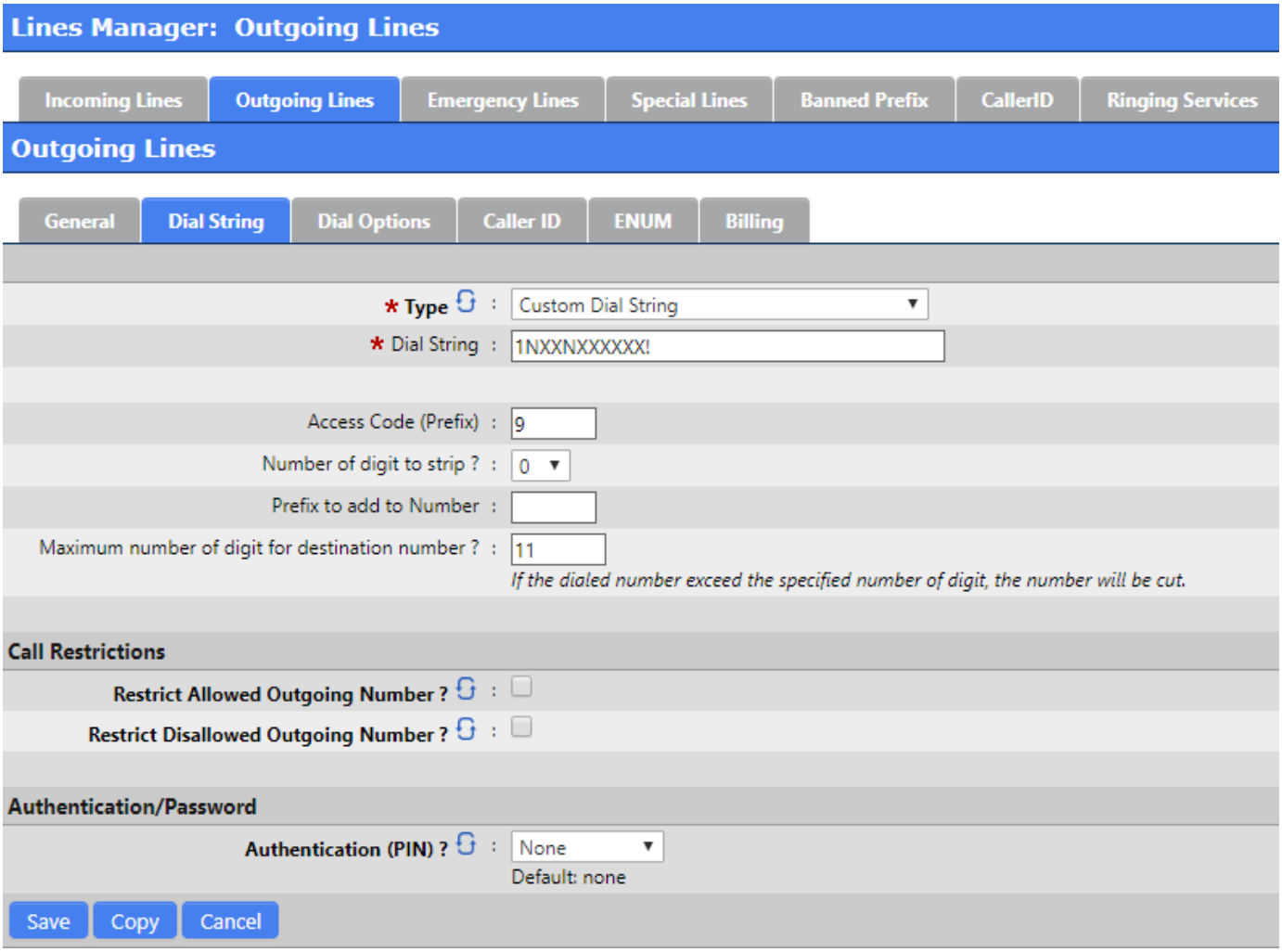
Custom Dial Plan Strings	
X	matches any digit from 0-9
Z	matches any digit form 1-9
N	matches any digit from 2-9
[1237-9]	matches any digit or letter in the brackets (in this example, 1,2,3,7,8,9)
.	wildcard, matches one or more characters
!	wildcard, matches zero or more characters immediately

Examples	
NXXXXXX	matches a normal 7 digit telephone number
1NXXNXXXXX	matches an area code and phone number preceded by a one
9011.	matches any string of at least five characters that starts with 9011, but it does not match the four-character string 9011 itself.

#	matches a single # key press

Dial String

- Type= drop list of possible pre configured or Custom Dial Plan rules
- Dial String= A matching pattern of digits a user can dial from their extension
- Access Code (Prefix)= Optional Outgoing Dial Plan Prefix. This digit is always stripped and never passed to the physical interface. This is most often used by PBX PSTN prefixes like 9 that must be stripped before processing by the PSTN carrier.
- Number of digit to strip = Number of prefixed leading digits stripped from the “Dial String”
- Prefix to add to Number = The digit(s) prefixed to the outgoing call after digits are dialed
- Authentication (PIN) can be used to force user authentication before call is placed.
- Once all fields are completed click on the “Dial Options” tab.

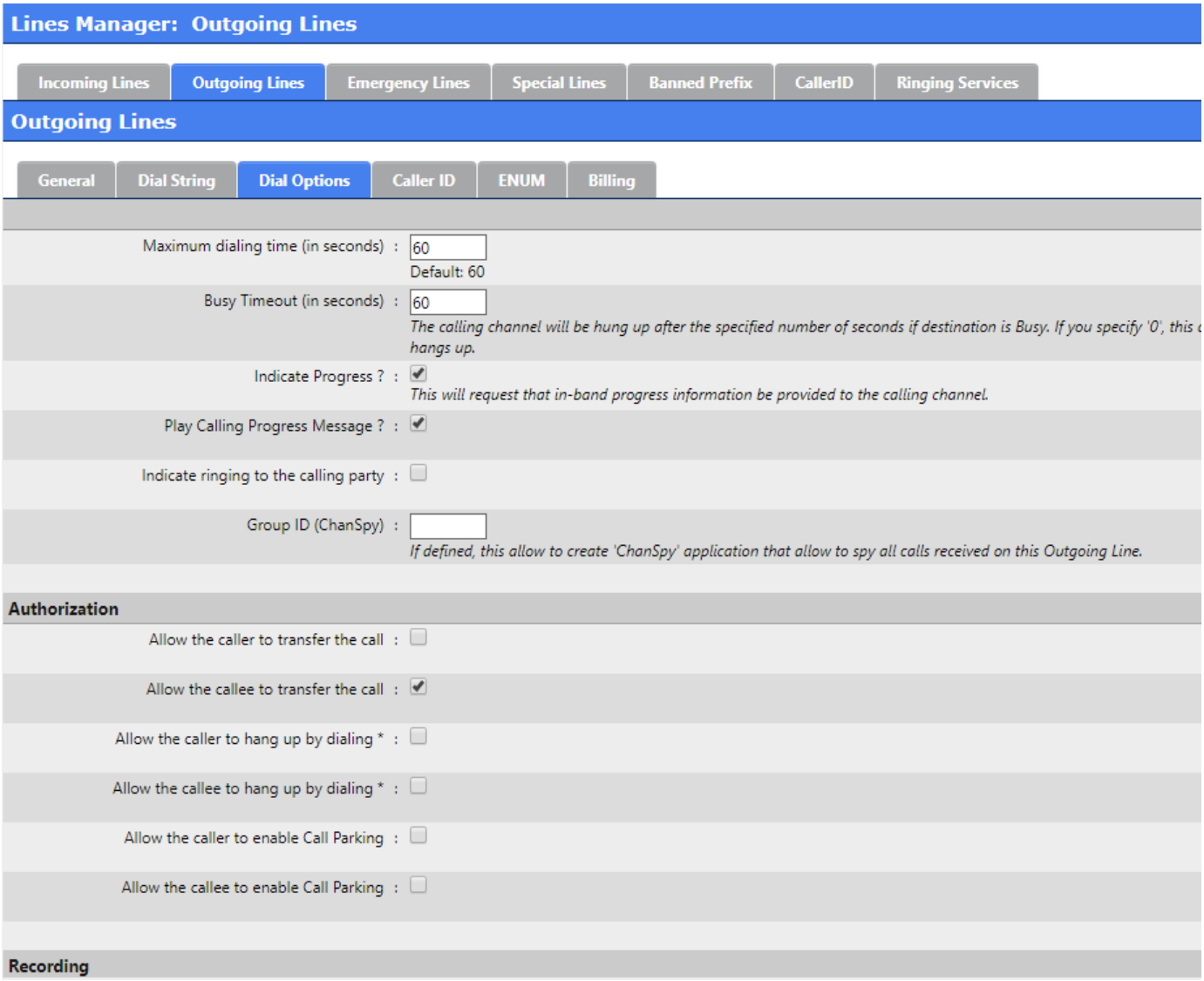


Dial Options

Dial Options must be configured if you wish to provide additional features such as call recording, early media with progress, and T.38 Gateway options

It is often useful to have a unique Music On Hold source for each Outgoing Line if the user places an outgoing call on hold.

Once these fields are configured click on the Caller ID tab.



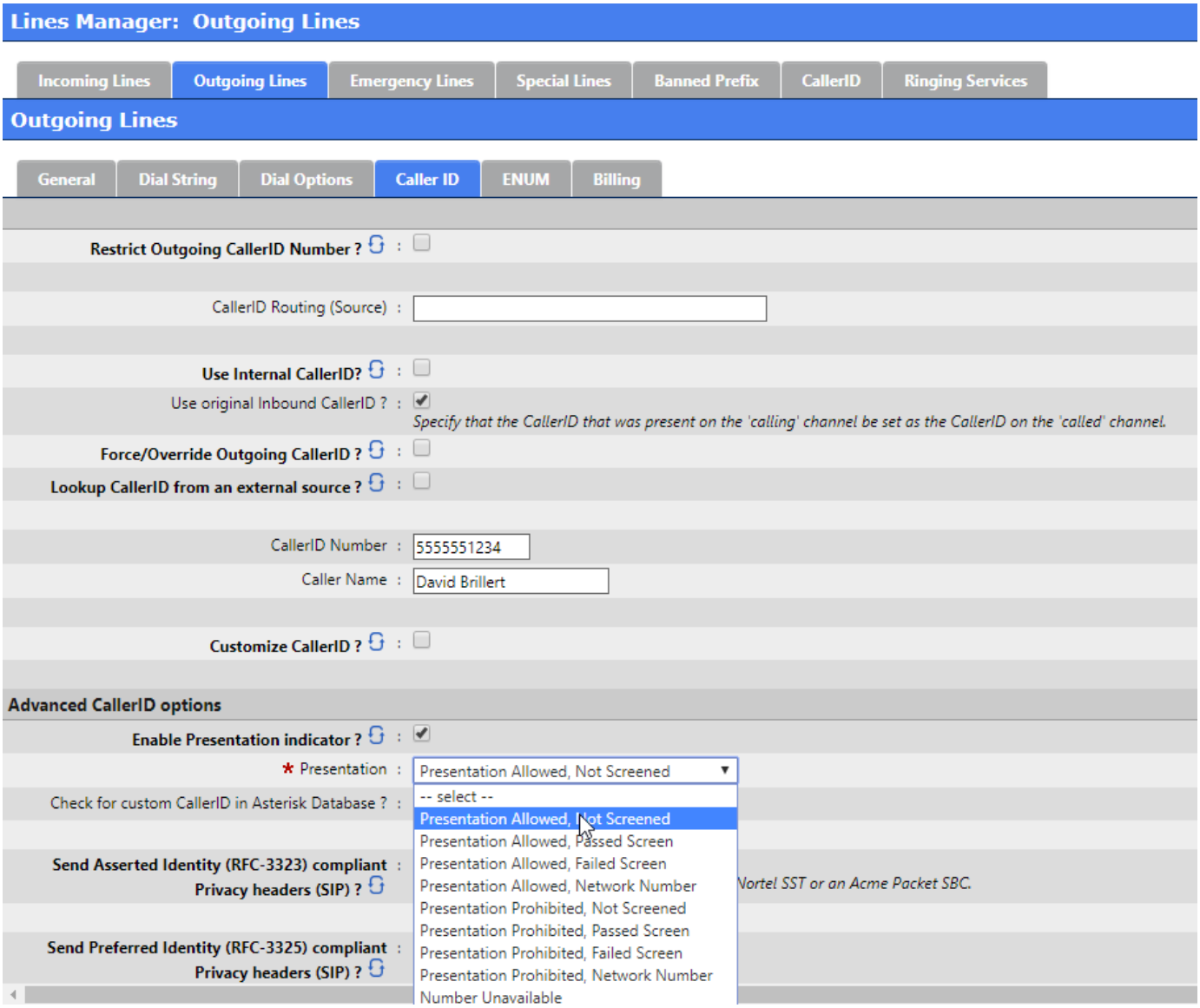
Caller ID

On physical interfaces that support custom ANI to be set on outgoing calls it is useful to define a global Name and Number for outgoing calls. Fill in the custom name and number for outgoing calls here if the Outgoing Line > Trunk supports custom ANI

Note that FXO interfaces do not support custom ANI but in this example the custom “CallerID Number” and “Caller Name” are configured.

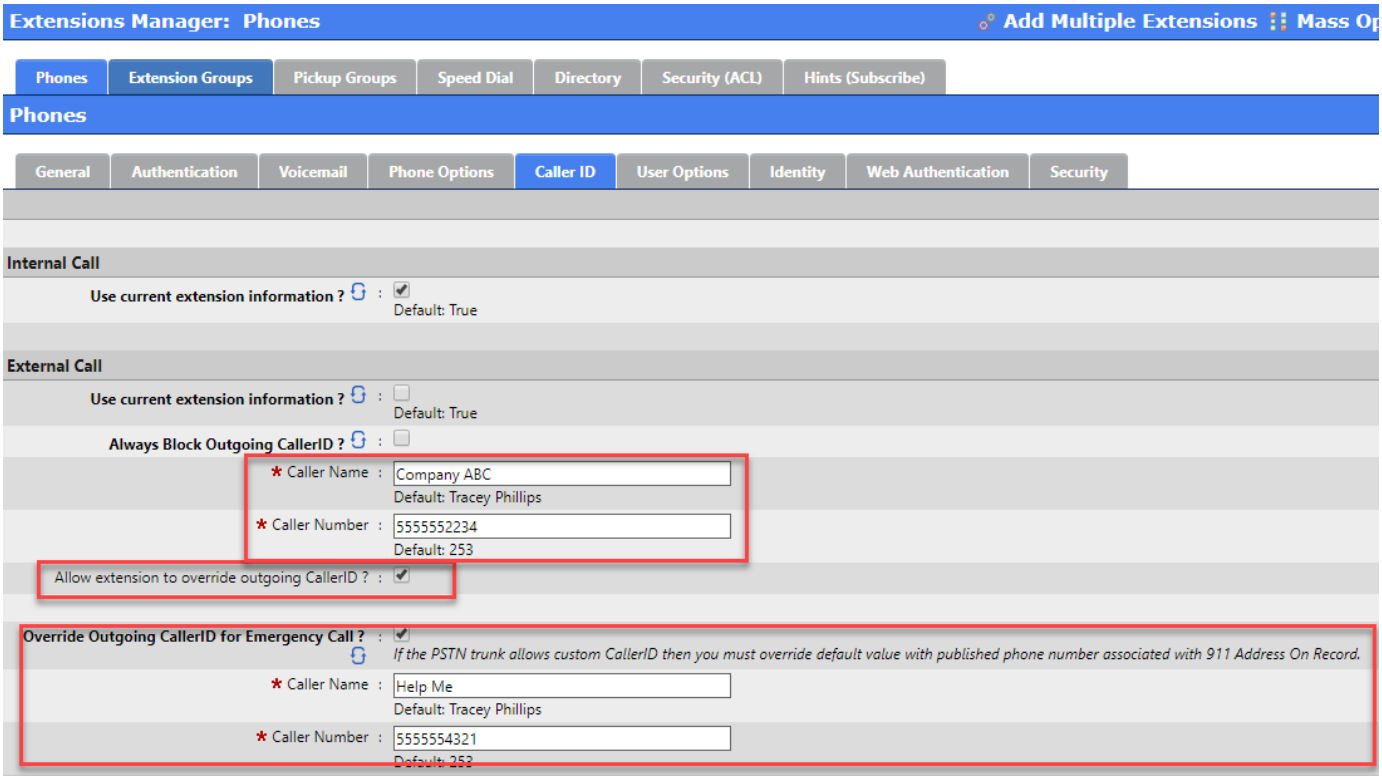
Advanced CallerID options can be selected to comply with https://tools.ietf.org/html/rfc3325

See https://blog.scopserv.com/2018/01/how-to-make-anonymous-calls-from-a-sip-trunk/



Caller ID Extension Overrides

The Outgoing Line custom ANI is always overridden if Extension's>Caller ID>Allow extension to override outgoing CallerID checkbox is enabled and Emergency Calls will also take precedence over the Outgoing Line if configured.



Class of Service (CoS)

Background

The Class of Service Manager is used to create objects with permissions or restrictions to Outgoing Lines, Incoming Lines, Extensions, Feature Codes, or Applications. These CoS objects can then be applied to Extensions, Incoming Lines, Auto Attendants, Outgoing Lines, or Applications The Class of Service Manager can be found by navigating to Configuration>Telephony>Manager>Class of Service.

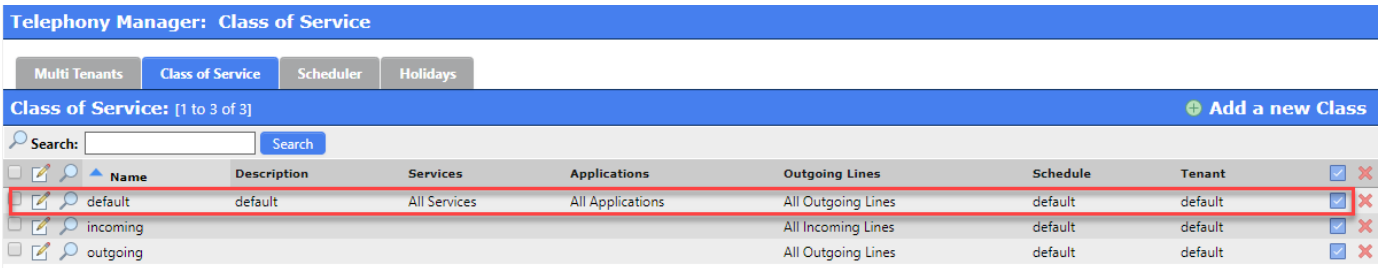
- Class of Service objects also control permissions and restrictions which vary depending on whether or not a Hot Desk Extension, Agent Extension, or Room (Hotel) Restriction Feature code has been invoked. For example an extension can have a Class of Service which restricts long distance Outgoing Lines when no Hotdesk Extension is logged but if a valid Hotdesk Extension logs in then the Outgoing Lines access is allowed.
- There is no limit on the number of Class of Service objects which can be created. Therefore many CoS objects can be added to create granular security rules which can easily be applied to Outgoing Lines, Incoming Lines, Extensions, Feature Codes, or Applications.
- The Class of Service is one of the last objects to be built during a new installation because many pre-requisites are required.
    - Before a new Extension can be added a CoS must be built so that the CoS can be assigned to the new extension.
    - Before a non default Feature Code can be created the matching module must be configured.
    - Before a Feature Code can be included in a CoS the Feature Code must be configured.
    - Before an Application can be assigned to a CoS the Application must exist. It is therefore more efficient to create any required Applications prior to adding any new CoS objects so that the CoS does not have to be edited more than once.
    - Before an Outgoing Line can be included in a CoS object the Outgoing Line must already exist.

NOTE: It is best practice to leave Incoming Lines>Options>Class of Service configured to the default “System Default” setting. This is because the PSTN interface also has a “System Default” CoS value and the Incoming Line CoS and the Interface CoS must use matching values else incoming calls will fail. Unique requirements could dictate non default settings. Also choosing a non System Default CoS on an Incoming Line can have serious security implications if not configured correctly.

default CoS

This example shows the ‘default’ Class of Service automatically assigned to any new Extension

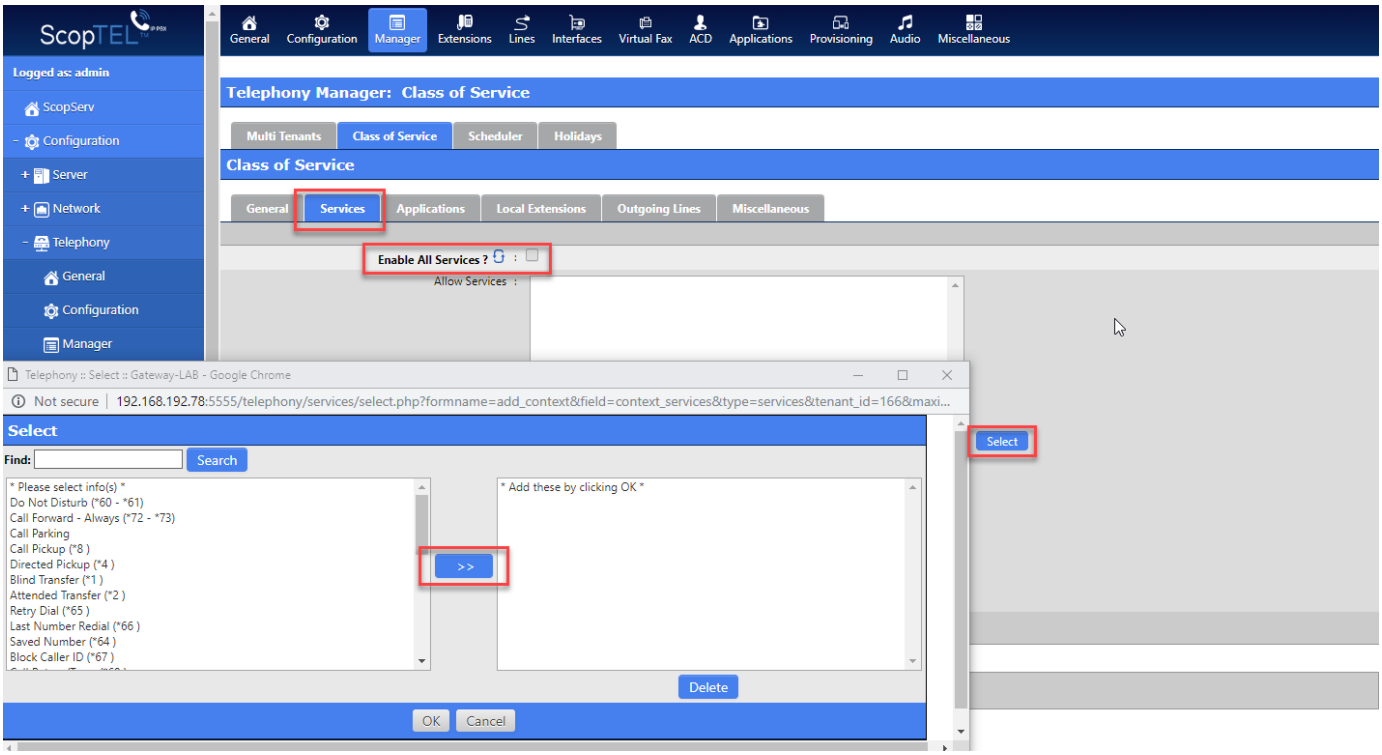
For detailed instructions on Class of Service refer to: https://blog.scopserv.com/2017/10/how-to-configure-class-of-service-objects/



Editing using the Select Tool

The Select tool is visible whenever you edit the Class of Service’s Services, Applications, Local Extensions, Outgoing Lines tabs

From the column on the left showing the available feature codes highlight each feature code required using a mouse and then click >> to assign those codes to the column on the right. Click on the “OK” button to close this window. Feature Codes listed in the right column will be added to the new CoS once the new CoS is saved. Only the objects included in each tab using the Select tool will be allowed wherever this CoS is applied.



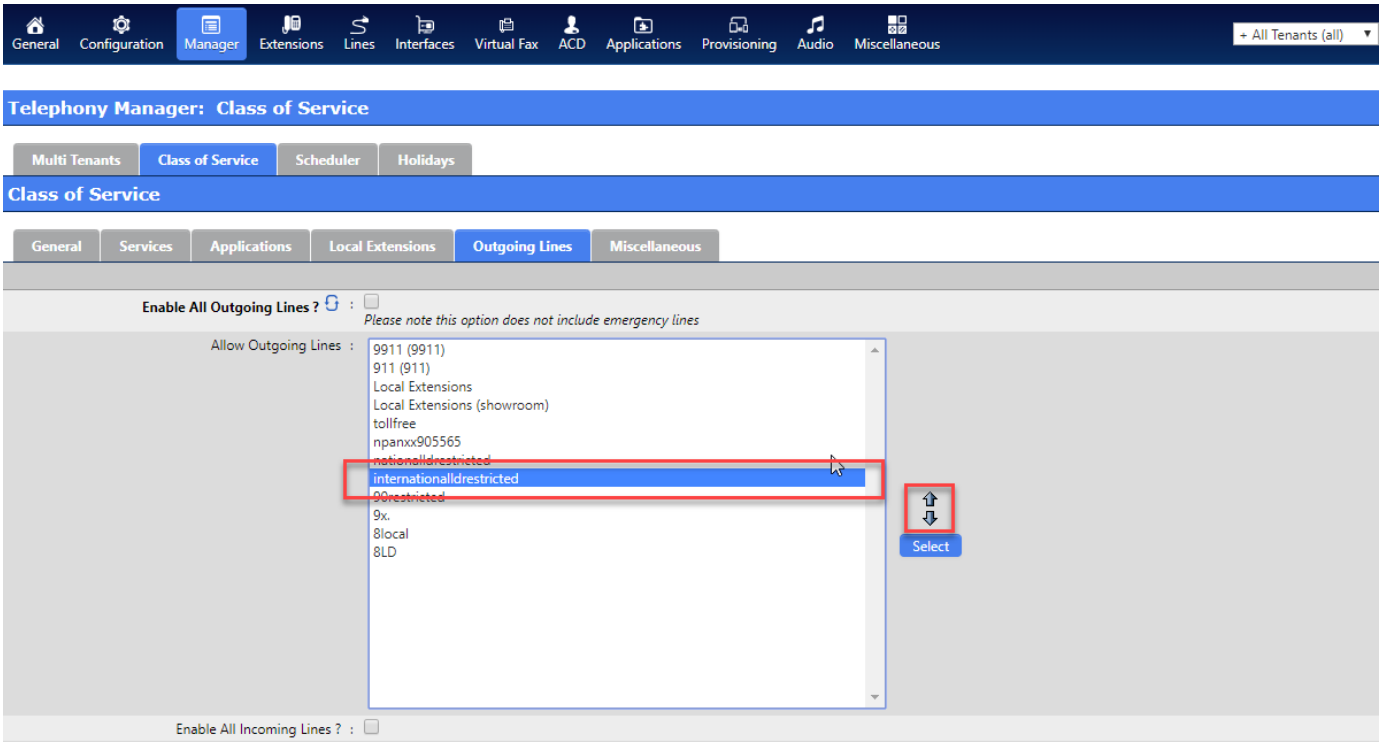
Outgoing Line precedence

After selecting which Outgoing Line objects are allowed it is imperative to select the Outgoing Lines in the correct order of precedence.

Outgoing Lines are matched when dialed according to the precedence defined in the configured CoS object in top to bottom priority. Items at the top if matched will be immediately passed to the dial plan running in memory.

The most specific entry and most important dial plan matches should be placed in the highest priority.

By example a Outgoing Line equal to 1NXXNXXXXXX! should have a lower priority than a dial plan equal to 1800NXXXXXX! Else that rule would be matched and dialed first before querying the next possible match. This can affect which trunk is accessed or LCR rule is used to place the outgoing call.



Security

Background

SIP Phones are SIP User Agents.

For security, SIP User Agents must register to the SIP Registrar via username and password authentication. It is typical for the SIP protocol ports to be open or forwarded to the SCOPTEL server if a third party Firewall is implemented. When the SIP ports are exposed on the Firewall it is common for hackers to attempt brute force attacks on the server. Such attacks systematically request authentication using common dial plan Extensions and trivial passwords.

Examples of such brute force attacks:

- Extension range 100-3000
- Systematic Password attempts using passwords 1000-3000
- Systematic Password attempts using passwords 0000, 1234, 1111, 4321, 123456, 7654321

Therefore if a secure password policy is used it will prevent the overall majority of hackers from registering a SIP Extension or SIP Trunk with the server for fraudulent purposes.

Examples of secure SIP password policy

- Minimum password length of 8 alpha numeric characters.
- No Dictionary words
- Minimum 2 Upper Case characters used
- Minimum 2 numerals used
- Passwords should be unique for each extension

The same policy enforcement should be in effect when configuring Voicemail Passwords except Voicemail Passwords cannot contain Alpha characters and must be numeric.

A poorly implemented Voicemail Password Policy can allow a hacker access to thru dial capabilities from a mailbox configured to allow outdial capabilities. Therefore Voicemail Passwords must be strict regardless of inconvenience caused to end users.

- Voicemail Password should never match the extension number. Example: Extension 100, Voicemail Password 100

- Voicemail Password should never be trivial.

  Examples: 0000, 1234, 1111, 4321, 123456, 7654321

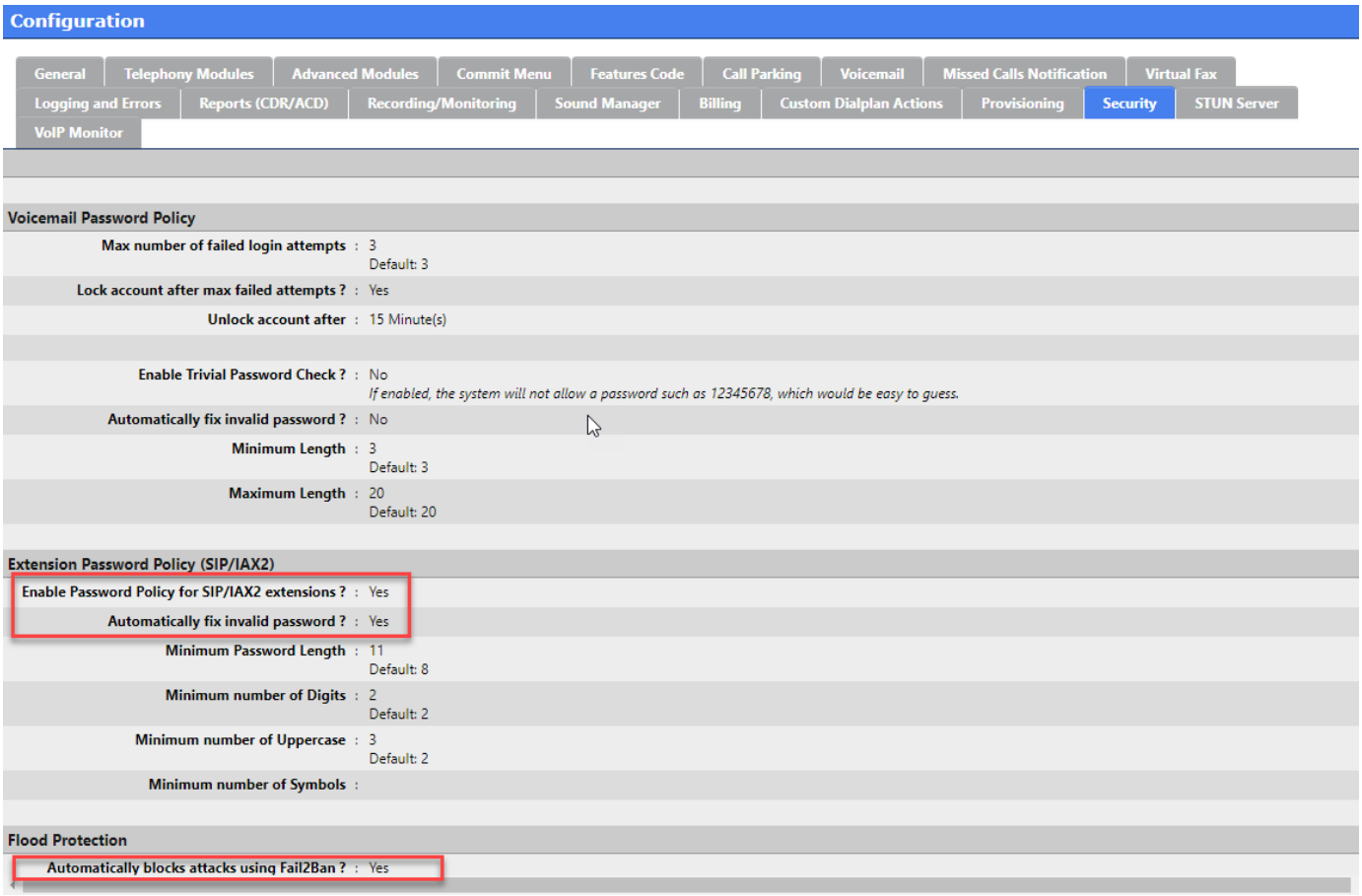
Password Policies and Brute Force protection

To set a Global Password Security Policy navigate to Configuration > Telephony > Configuration > Security

The SIP and IAX2 Password Policy is set independently of the Global Voicemail Password Policy.

If the Options to automatically fix invalid password?[ ] is checked then non-compliant passwords will be made compliant after a commit.

Here are some recommended Settings



Firewall Background

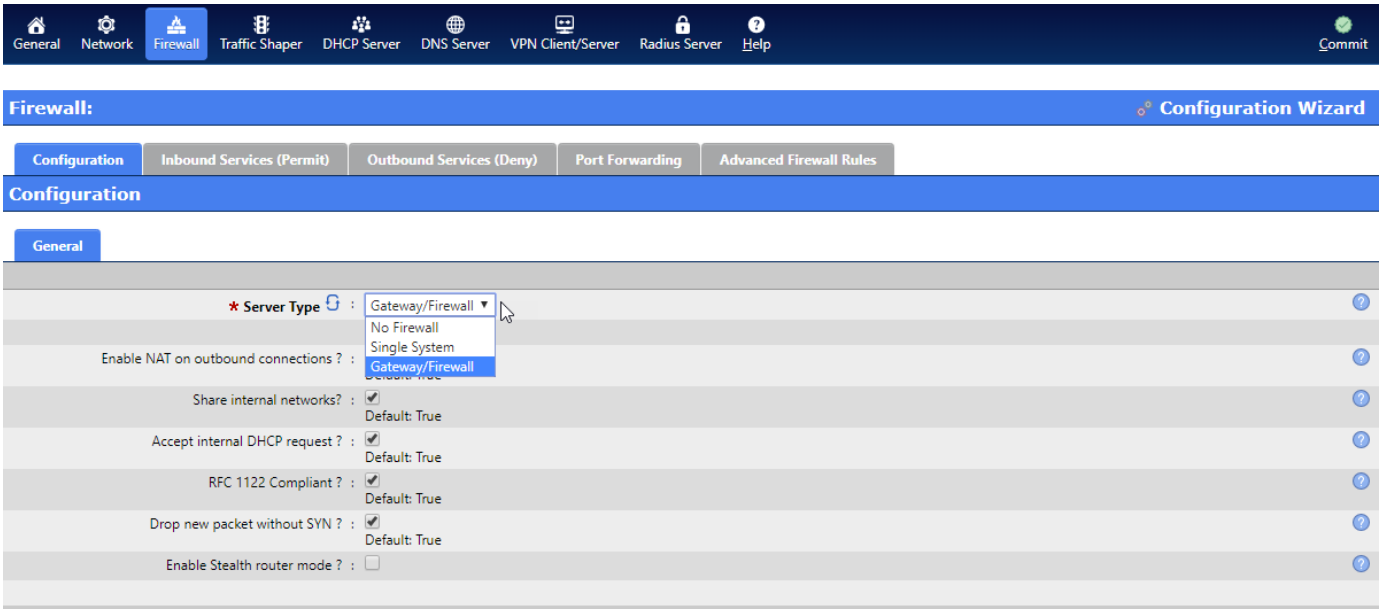
It is common for SIP Extensions to exist for Remote Extensions (Nomadic users). It is highly recommended that the server be protected from malicious attacks by enabling the Firewall.

Configuration>Network>Firewall>General>Server Type

- Server type is default with “No Firewall”. Firewall types are “Single System, Gateway/Firewall”
- If only one Network Interface exists then only “Single System” or “No Firewall” is possible. If two Network Interfaces exist then the server can be configured as a “Gateway/Firewall” which will enable outgoing NAT (Network Address Translation) and Firewall the configured WAN Interface.

In this screenshot the “Server Type” is configured as a “Single System” (Firewall is enabled). It is also recommended to set the “Server Type” and “Inbound Services (Permit)” options using the Configuration Wizard.

NOTE: Firewall rules only apply to Network Interfaces designated as WAN interfaces. LAN interfaces are never policed by the Firewall.

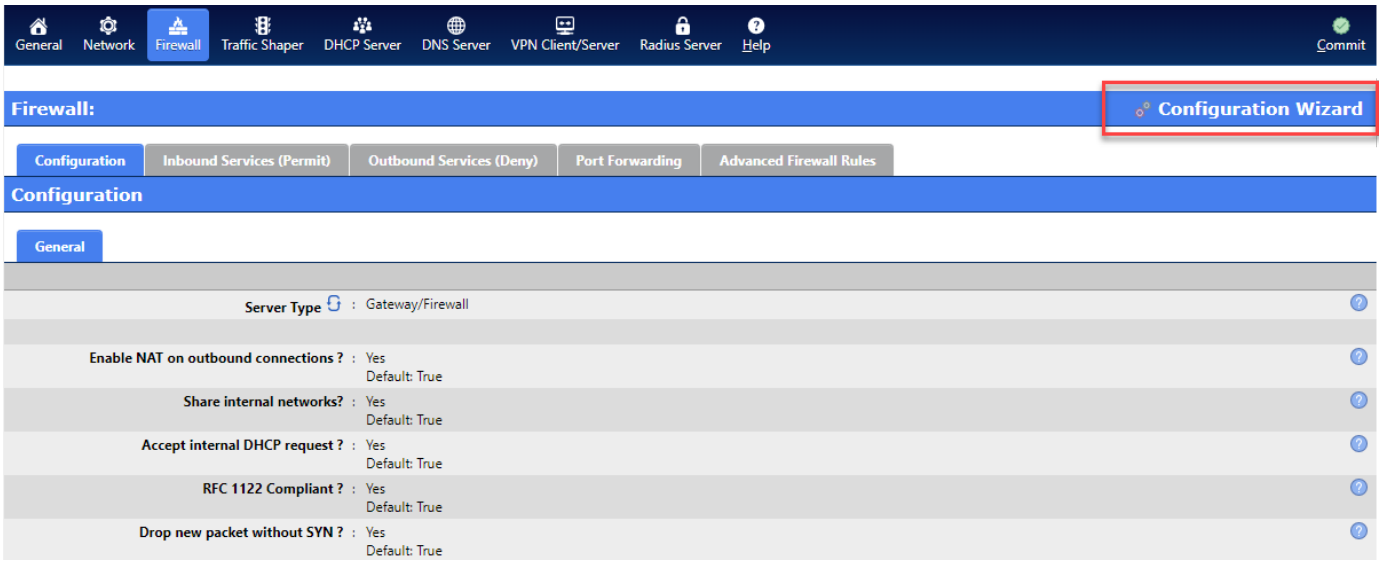


Firewall Configuration Wizard

In this example the Firewall Configuration Wizard will be used to set the recommended Firewall Configurations.

From Configuration > Network > Firewall > General

Click on the “Configuration Wizard” button

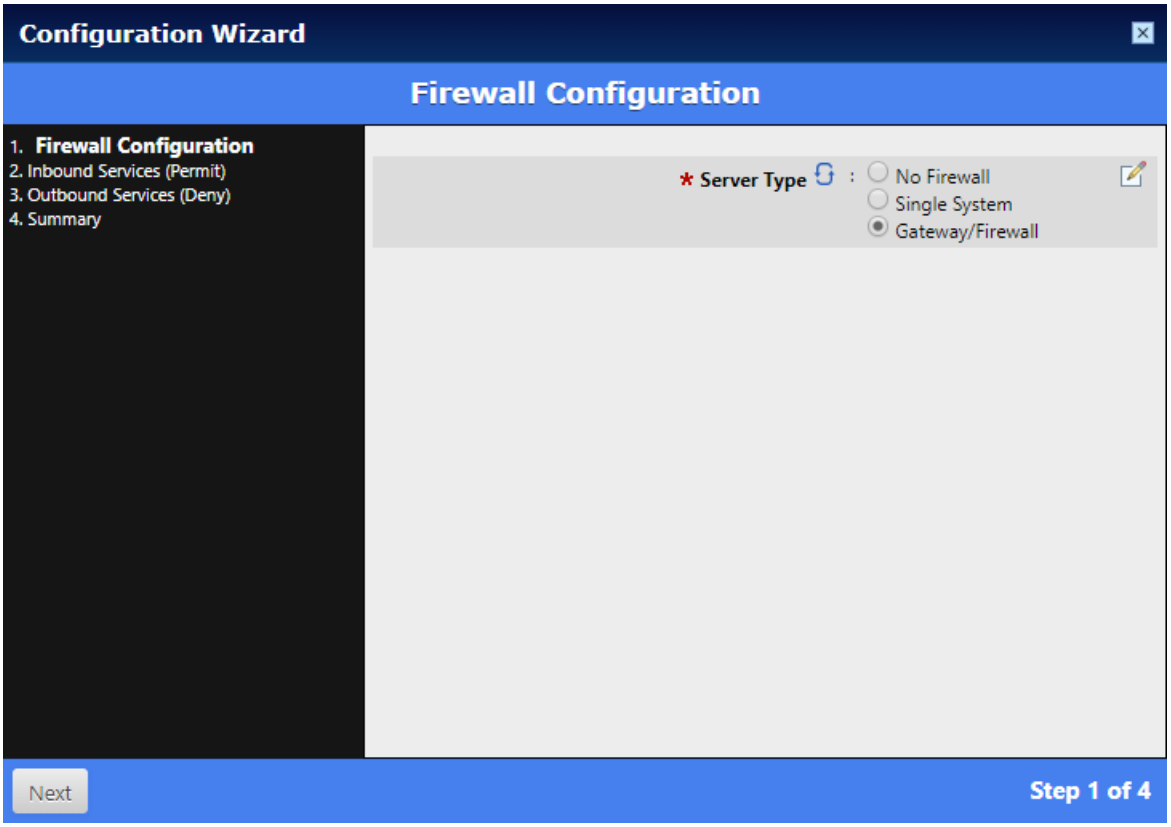


Firewall Wizard

In this example the Firewall Configuration Wizard will be used to set the recommended Firewall Configurations.

From Configuration>Network>Firewall>General

- Click on the “Configuration Wizard” button
- Choose the “Single System” option
- Click “Next”



Firewall Inbound Services

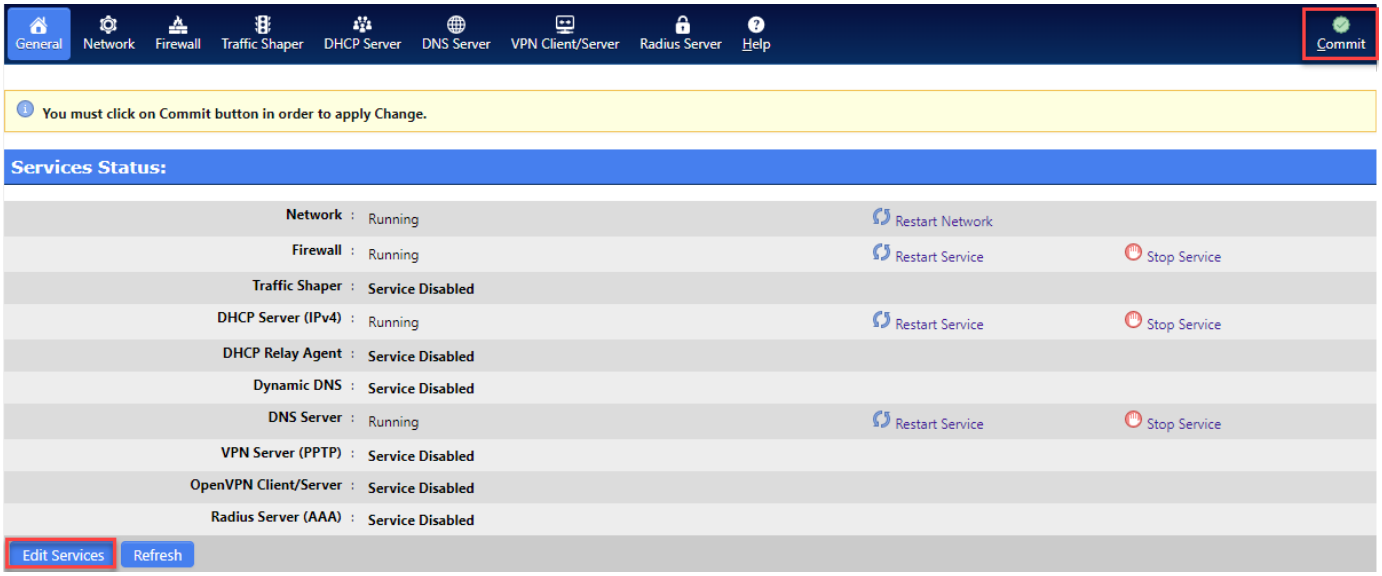
Which services will be allowed is dependent on network configurations and administrative security policies.

Network Services Manager

From Configuration > Network > General Click on “Edit Services”

- Click on Commit to write your changes to the relevant configuration files.

- Any service which has had its configuration modified must be restarted after a commit to reload configuration into memory.
- Choose which Services need to run when the OS reboots.
- Network is mandatory.
- Apply changes after editing services and start or restart the service if required.

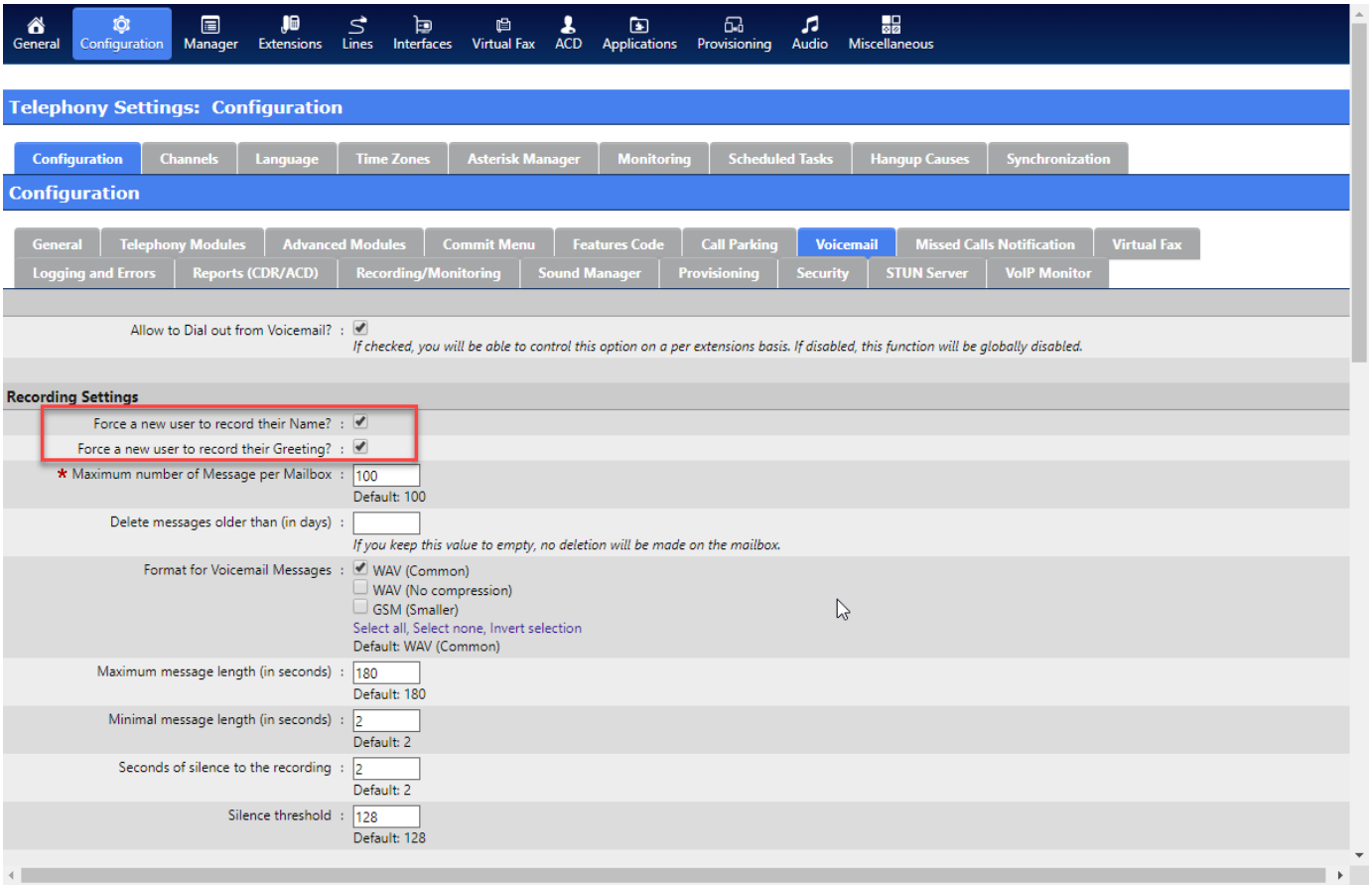


Voicemail

It is recommended to Enable:

- Force a new user to record their Name
- Force a new user to record their Greeting

  This will force the user of a new mailbox to change their password and record each of their greetings before the mailbox can be managed. If the password is not changed all changes to the mailbox are lost.



Extensions

Types

SIP Extension (IP Extension using the SIP protocol) is allowed its own voicemail box and therefore requires a User license

IAX2 Extension (IP Extension using the IAX2 protocol) is allowed its own voicemail box and therefore requires a User license

Zap Extension (analog FXS extension using Sangoma or Digium cards. Sangoma and Digium cards should not co-exist in the same server)

Voicemail Extension (Voicemail box only) is allowed its own voicemail box and therefore requires a User license

Hotdesk Extension

- A Hotdesk Extension is an Extension that logs into a physical Extension using the Hotdesk Feature Code, HotDesk Extension number and required password.
- By logging into a physical Extension the HotDesk Extension can make and receive calls from any extension which allows the HotDesk Feature Code in its assigned Class of Service. Caller ID incoming and outgoing will be automatically manipulated to display HotDesk user information.
- Is allowed its own voicemail box and therefore requires a User license

Virtual Extension

- A Virtual Extension is a very advanced Extension type which allows a user to login to the SCOPTEL GUI and use the Realtime Monitor and customize Call Detail Reports and other types of reports.
- A Virtual Extension is allowed its own voicemail box and therefore requires a User license
- Advanced options can be configured to ring multiple destinations and automatically forward copies of voicemail messages to multiple extensions
- User Options for Virtual Extensions include Follow Me, Camp-On, Personal IVR destinations
- Custom Forwarding Rules can be defined for:
    - Call Forward Immediate
    - Call Forward Busy
    - Call Forward No Answer
    - Call Forward Unavailable (forward when physical extension is offline)
    - It is possible to Immediate Forward a Virtual Extension to make an Application available within an IVR context for inbound PSTN callers.

Ring Group Extension

A Ring Group Extension automatically Immediately Forward it’s calls to configured Follow Me destinations. Advanced options can be configured to ring multiple destinations and automatically forward copies of voicemail messages to multiple extensions. Is not allowed its own voicemail box and therefore does not require a User license User Options for Virtual Extensions include Follow Me, Camp-On, Personal IVR destinations. Custom Forwarding Rules can be defined for:

- Call Forward Immediate
- Call Forward Busy
- Call Forward No Answer
- Call Forward Unavailable (forward when physical extension is offline)
- It is possible to Immediate Forward a Virtual Extension to make an Application available within an IVR context for inbound PSTN callers.

Shared Device Extension

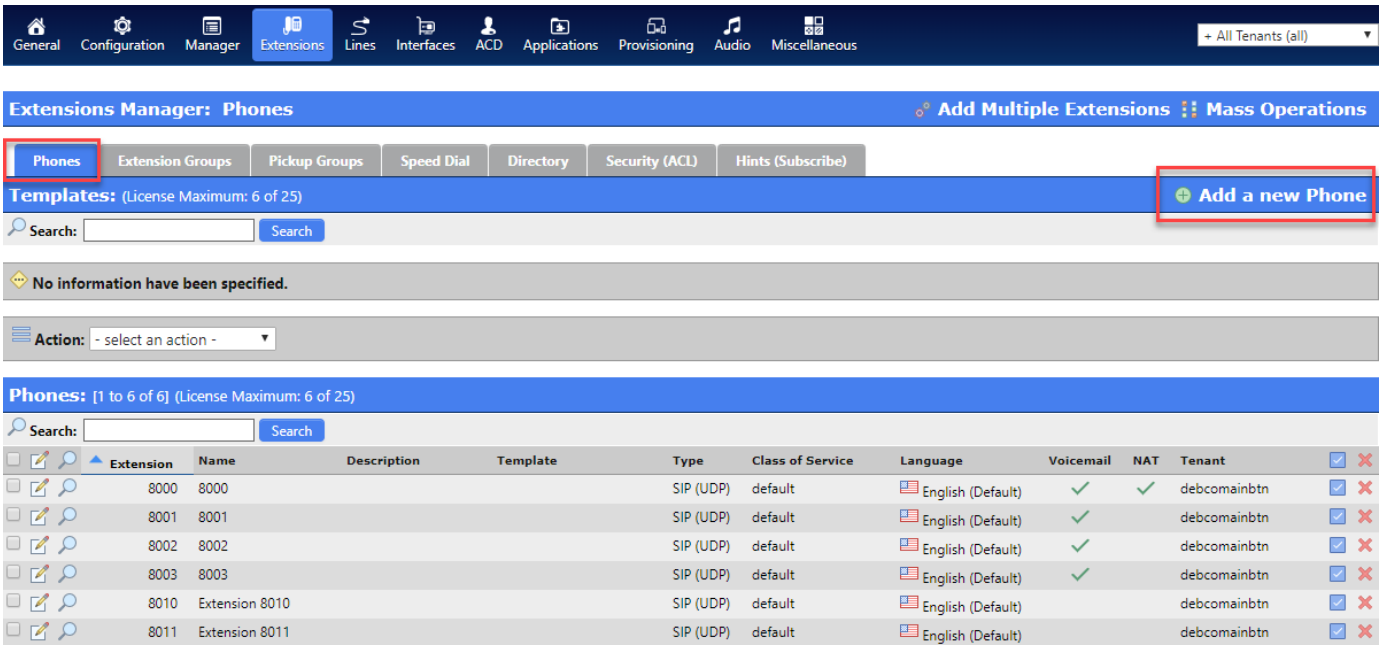
A Shared Extension can be configured so that multiple extensions can ring when the pilot DN is dialed but depending on the busy status of the extension(s) one or more extensions can ring but the busy extension will not ring.

Each Shared Extension requires its own Shared Device license.

Add a new Phone

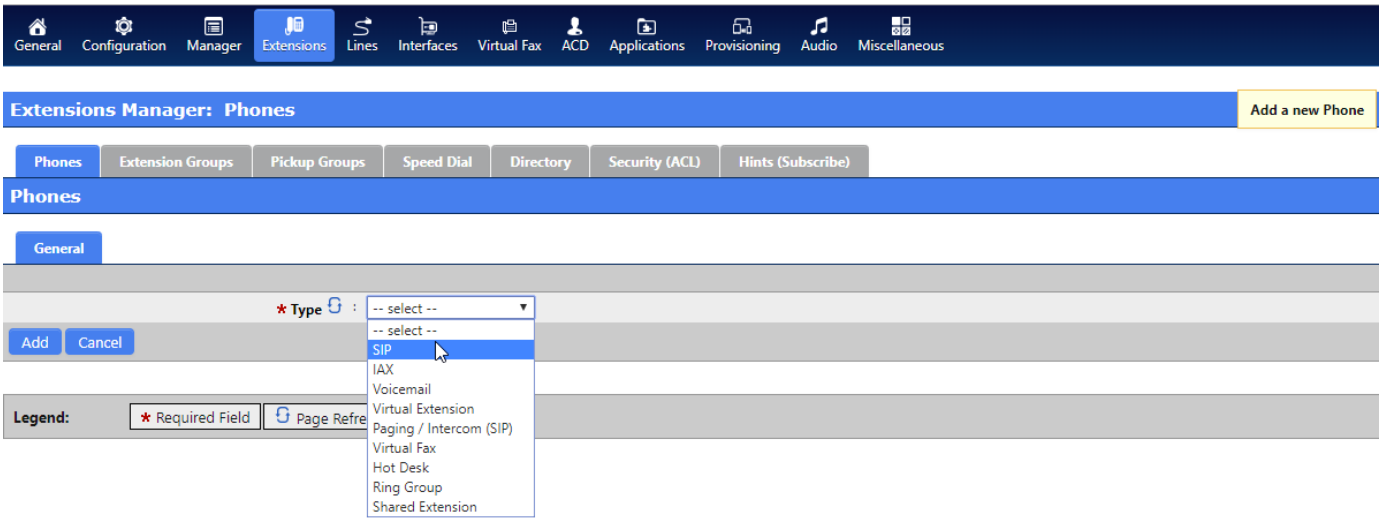
To create a SIP Extension navigate to Configuration > Telephony > Extensions

- Click on “Add a New Phone”
- You can also use the Add Multiple Extensions Wizard to add many Extensions



Type

Choose “SIP” from the list of available Extension types



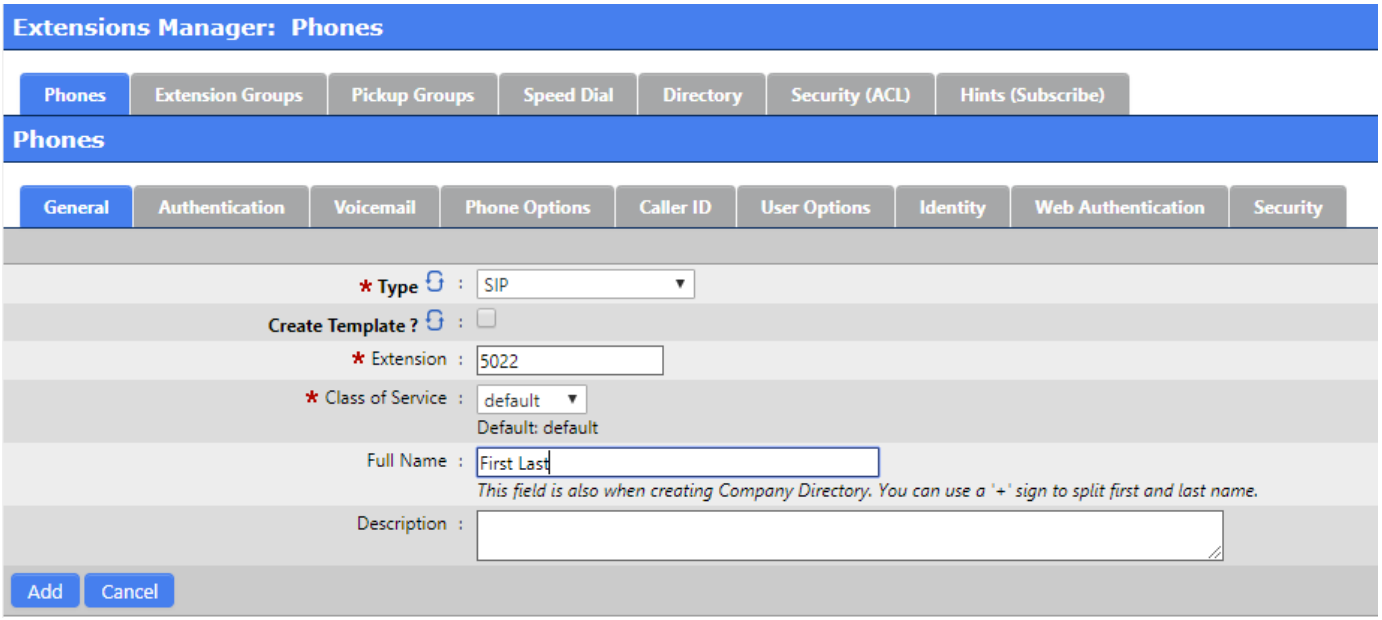
Extension Number and Name

Assign an unused Extension number

Enter a Full Name for this user <First Last> with no special characters and only one space

Select the desired Class of Service to apply to this user from the drop list

Click on the Authentication tab



Authentication

The Username should match the numeric value of this Extension number

Since the Security Policy enforces a strict SIP/IAX2 Password Policy the first pre-requisite is to enter a compliant alpha numeric password into the text box or use the Generate Password button to generate a random compliant password. Click on the Voicemail tab once the Authentication text is entered.

Voicemail

Enable Voicemail if required

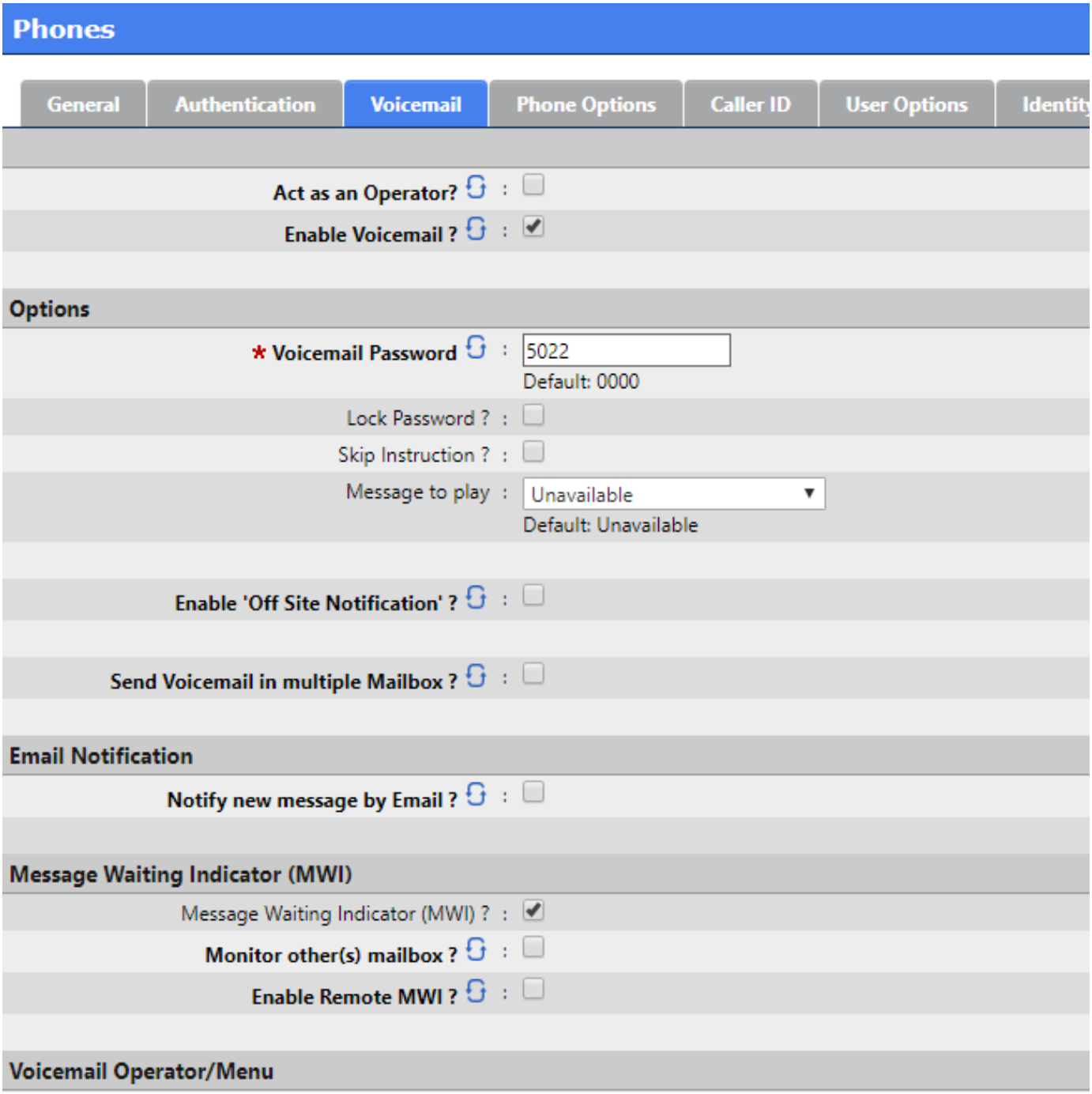
To force a new mailbox owner to initialize their mailbox use the extension number in the password field (pre-requisite enable Force a new user to record their Name [x], Force a new user to record their Greeting [x] in the Voicemail Manager template).

Enable Message Waiting Indicator (MWI) to light the Voicemail light on the matching SIP hardware or softphone

Enable Email Notification if you want to enable voicemail to email (normally requires a pre-requisite SMTP Smart Relay configuration in the Server Manager)

Configure additional security options in the Advanced Settings section.

Click on Phone Options tab



Phone Options

Host Mode should be left default and the IP address field should be ignored because this is an advanced field used for problematic Remote Extensions behind a NAT Router

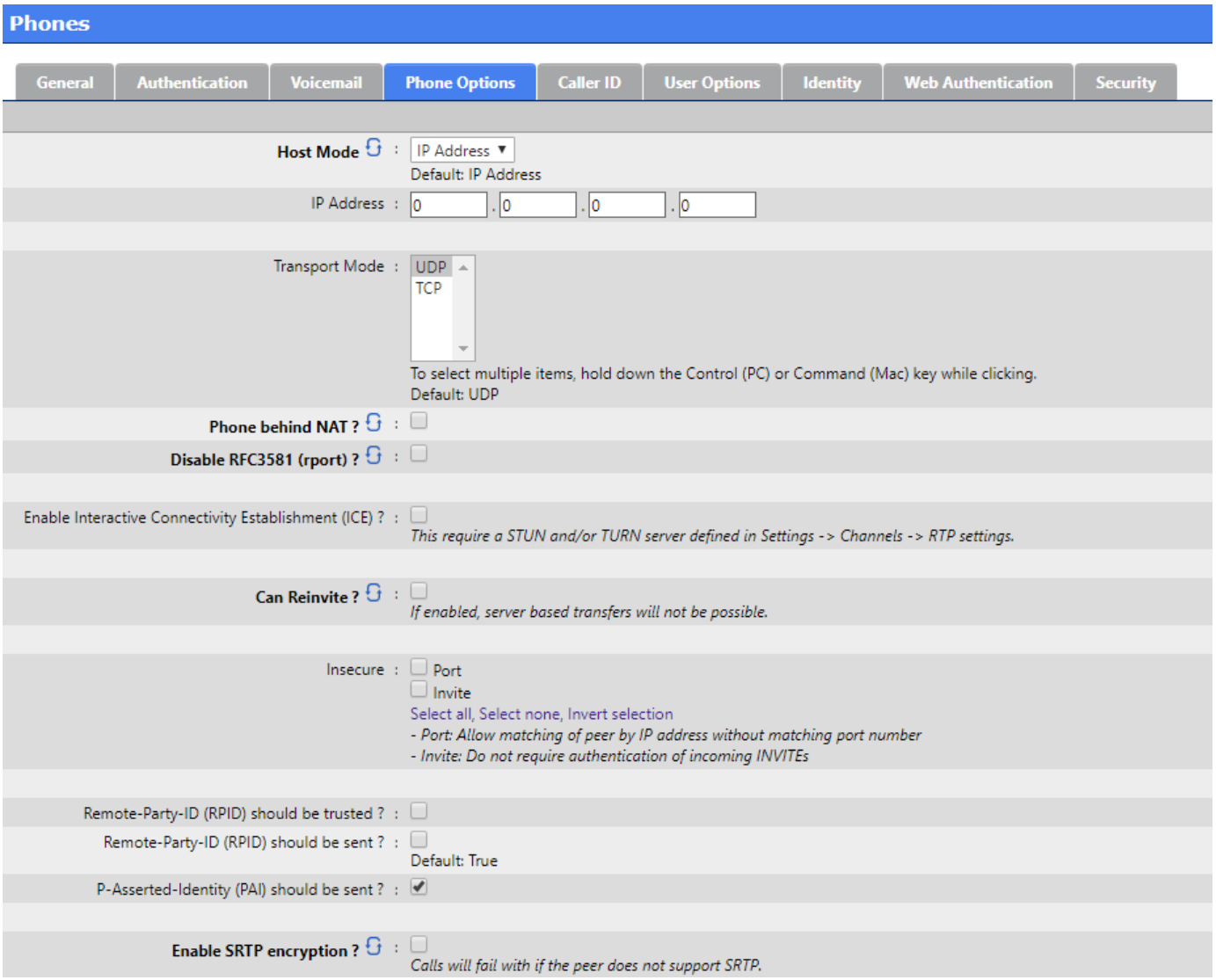
If the SIP device is to be used on the LAN then the “Phone behind NAT” option should not be checked.

Transport Mode(s) are vendor specific but the majority of SIP User Agents support UDP. Allowing both modes will allow the server and user agent to negotiate the compatible mode in the SDP messages. UDP should be considered a pre-requisite

If the SIP device is to be used as a Remote Extension located behind a NAT router then the “Phone behind NAT” option should be checked. Checking this option is normally sufficient to ensure that the Remote Extension can register with the server and two way speech paths are possible (assuming that the Firewall is and global NAT options are configured correctly).

P-Asserted is highly recommended over the default RPID mode which has become a legacy method. PAI is required for connected line updates. You cannot enable both settings, only one option is allowed.

If you wish to activate TLS Transport Mode and Enable SRTP encryption then refer to: https://blog.scopserv.com/2016/09/how-to-use-the-SCOPTEL-certificate-manager-to-enable-tls-encryption/



Qualify is enabled by default and allows the server to monitor the Extension for Registration status and packet latency using OPTIONS messages. But not all SIP peers support OPTIONS so this might have to be unchecked depending on the device (Cyberdata devices do not support OPTIONS)

DTMF mode is normally Automatic (RFC 2833/Inband)

Only CODEC's supported by the SIP end point should be enabled.

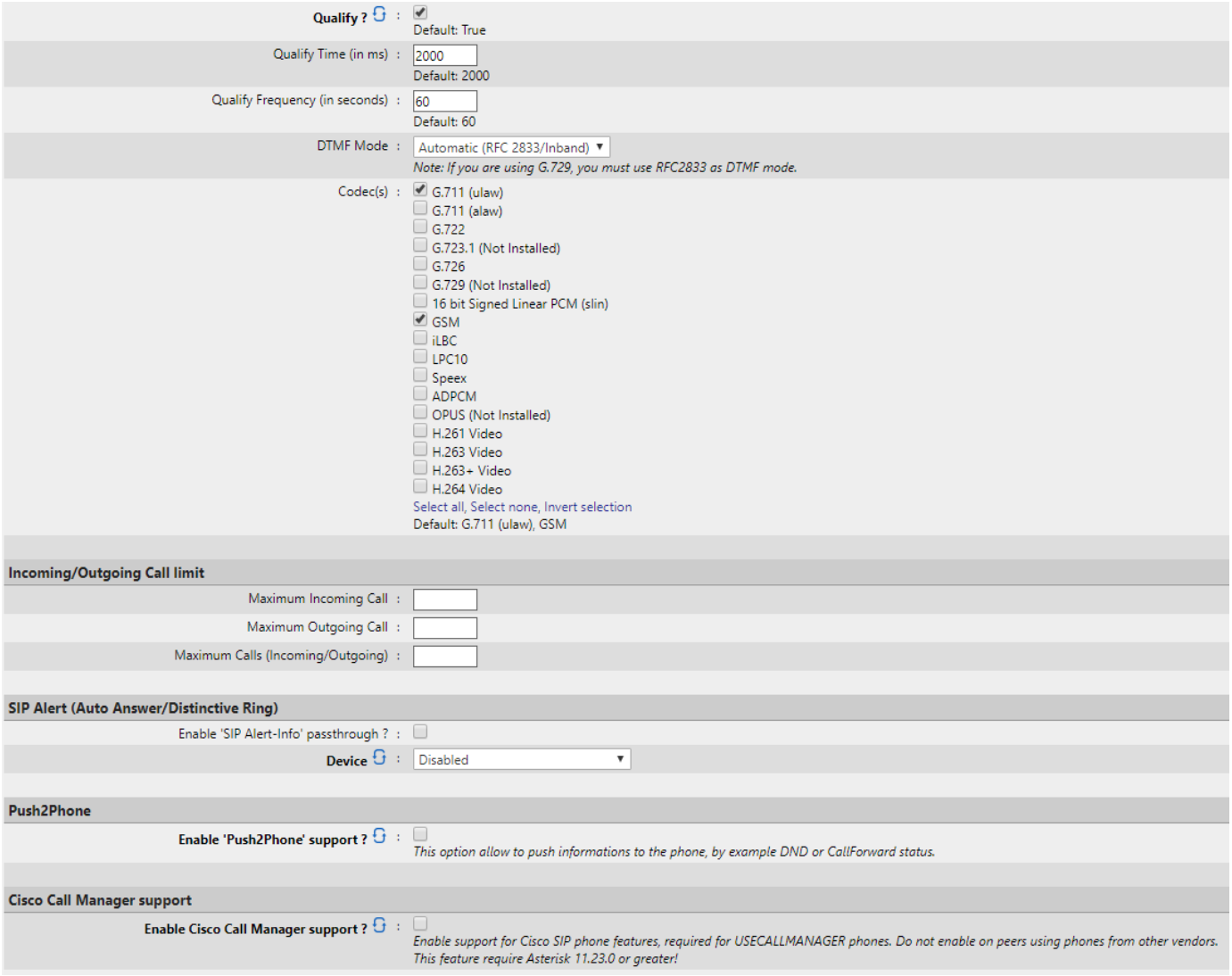
Incoming/Outgoing Call Limit can restrict the number of simultaneous calls supported by this Extension (default 8).

"SIP Alert (Auto Answer/Distinctive Ring)" is used to configure this SIP end point to receive an internal page if the SIP end point is a supported device.

For Cisco support refer to:

https://blog.scopserv.com/2017/07/SCOPTEL-cisco-sip-phone-integration/

When done Click on the Caller ID tab



Caller ID

All Caller ID fields can be modified.

Default values will set the local and outgoing PSTN Caller ID to match the configured Extension Number and Name.

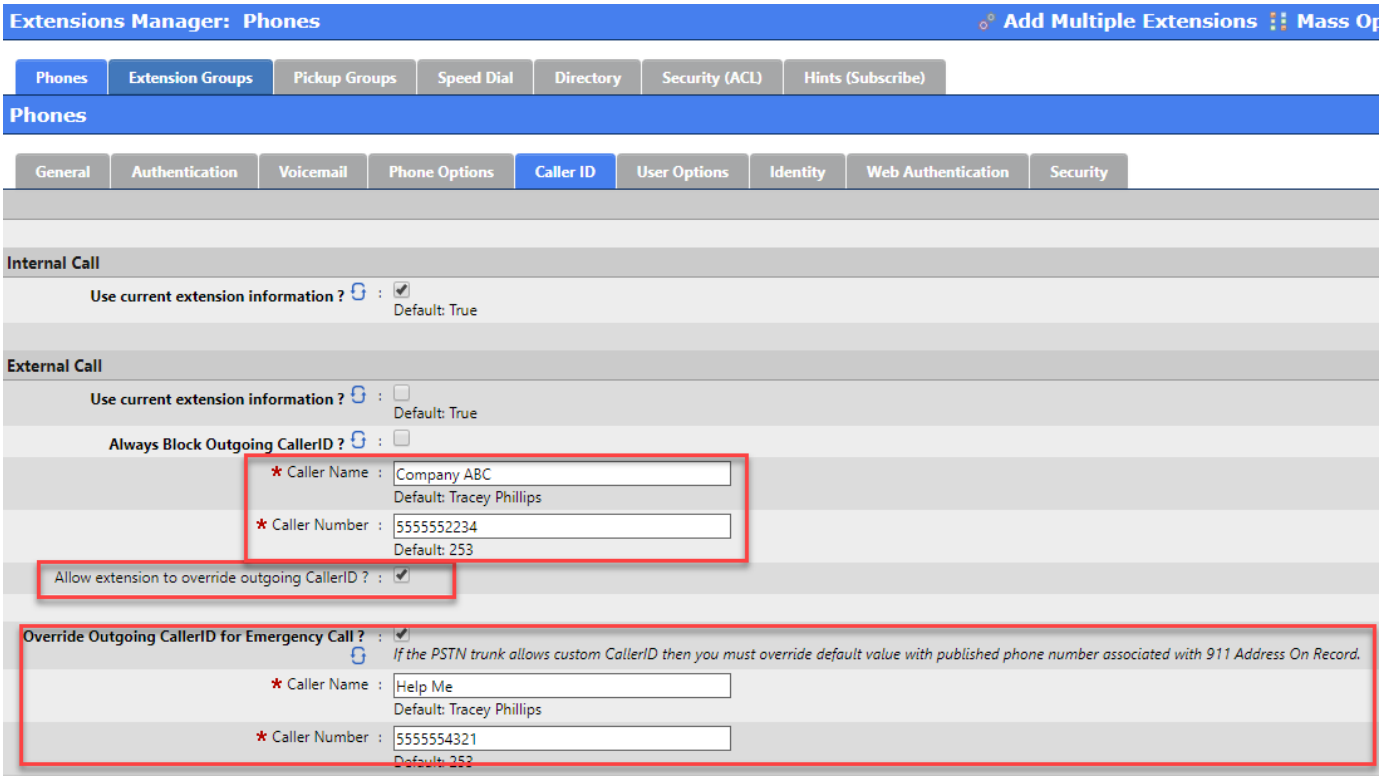
Un-checking either “Internal Call” or “External Call” checkboxes will allow the Caller ID configuration to be modified.

Note that “External Call” and “Emergency Call” Caller ID cannot be customized if the ITSP or PSTN provider’s trunks do not allow the Caller ID (ANI) to be re-written.

It is highly recommended that the “External Call“ and “Emergency Call” be modified to show either the published “BTN” of the customer or “DID” of the user. Failure to modify the defaults will result in only the Name and Extension number appearing on any outgoing external and emergency calls.

The Outgoing Line custom ANI is always overridden if Extension’s>Caller ID>Allow extension to override outgoing CallerID checkbox is enabled and Emergency Calls will also take precedence over the Outgoing Line if configured.

When done click on the User Options tab



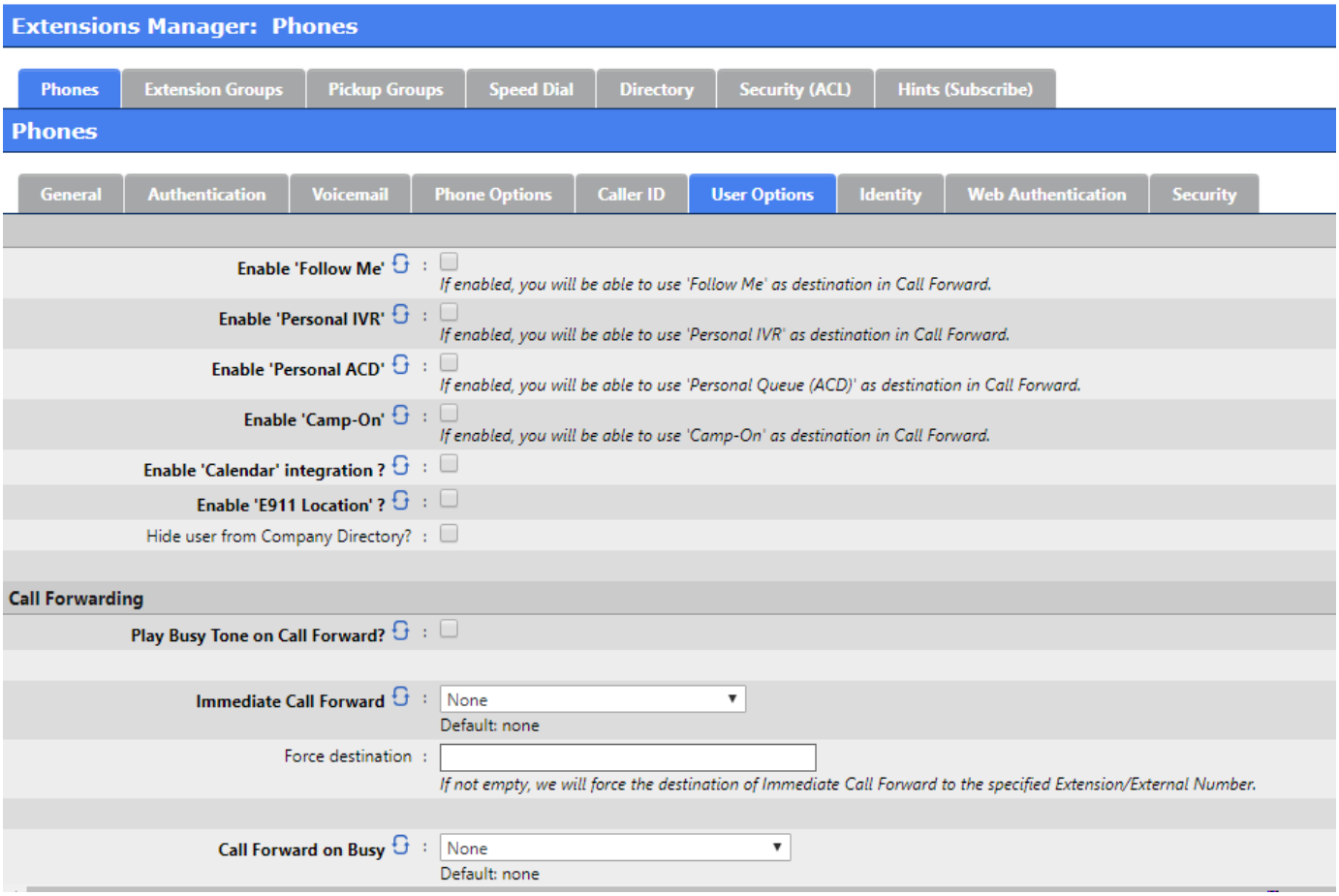
User Options

User Options define call forwarding rules, language, Music On Hold source file directory, default ring time, Call Recording options, Fax Detection, etc…

Enabling any advanced options such as “Follow Me”, “Personal IVR”, “Camp-On”, “E911 Location” will add new tabs and options to this extension’s GUI interface and allow additional configurations.

NOTE: to activate an advanced rule like Follow Me, you must choose a call forwarding option and use the drop list to select it from the destination drop list.

When done click on Web Authentication

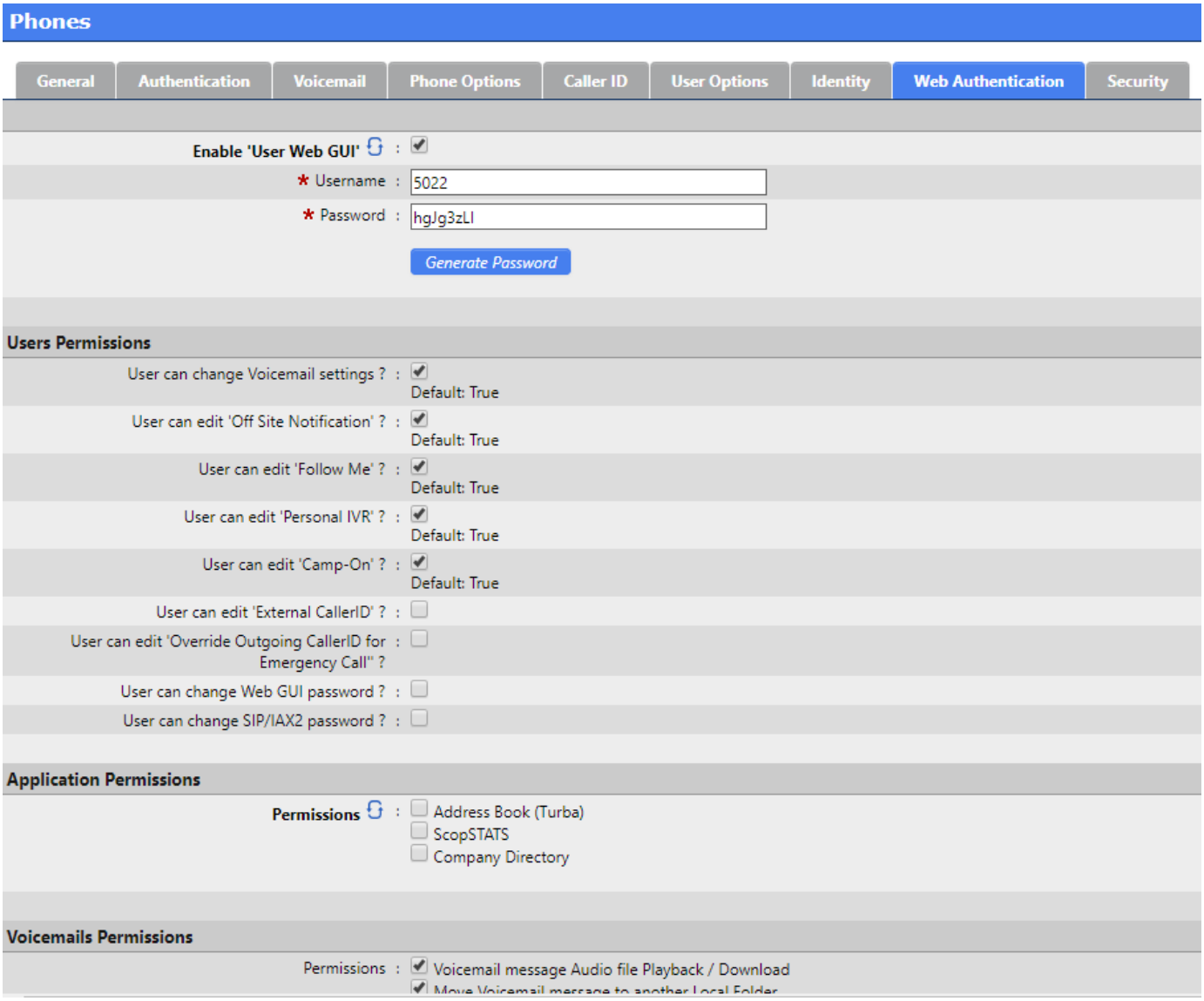


Web Authentication

The “Web Authentication” option allows the owner of an Extension to login to the SCOPTEL GUI and access several unique features including Voicemail playback and management. And its an optional feature and not mandatory to configure.

To access those features a unique login is created by checking the “Enable User Web GUI” and assigning a unique Username and Password for this Extension. The user logs into the same IP address and management port as the administrator but uses this login to access their personal GUI login.

Click on the “Security” tab when finished with this configuration.

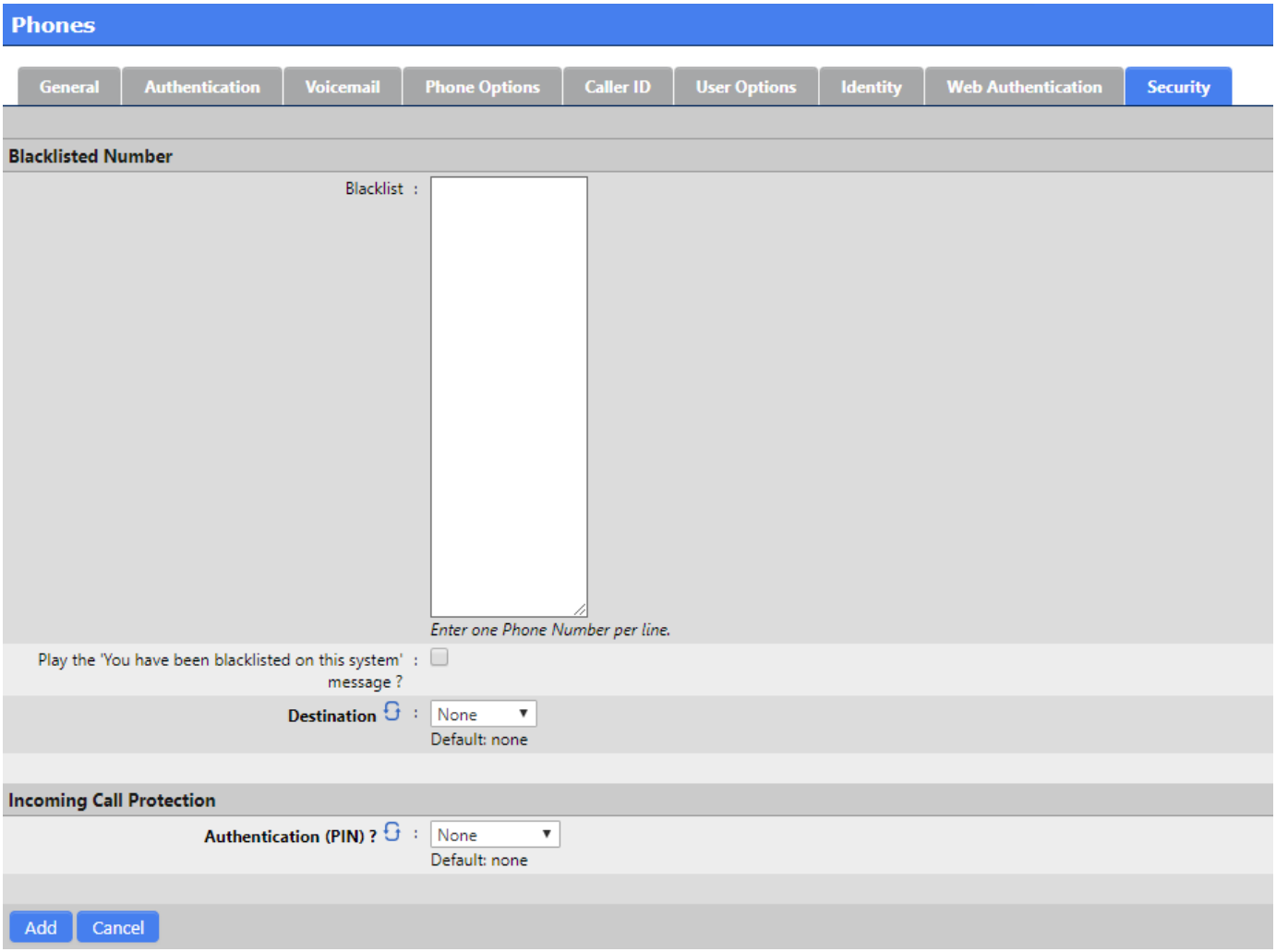


Security

Blacklisted numbers can be added to the text field and a password can be enforced when another extension or PSTN channel attempts to call this extension. If the password is not entered correctly then the Extension cannot be called.

This setting is optional and rarely used.

Click “Add” when finished to complete adding this extension to the server.



Incoming Lines

Background Information

Incoming Lines types are typically:

- "Extension (DNIS)" which are received numbers from SIP/IAX2 or PRI trunks. "Block" (a configured list of DNIS numbers).

  DNIS (Dialed Number Information Service). The service is provided by the TELCO and refers to the Called Party Number.

  - On ISDN PRI trunks the number is received in the Q.931 SETUP on the D channel.

    PRI Span: 1 < Message Type: SETUP (5) PRI Span: 1 < Called Party Number (len= 7) [Ext: 1 TON: Subscriber Number (4) NPI: ISDN/Telephony Numbering Plan (E.164/E.163) (1) '0312'] Executing [0312@zap-incoming:5] Set("DAHDI/i1/5796301651-d0f0", "__INCOMING_DNIS=0312") in new stack

  - On SIP trunks the DNIS is derived by default from the SIP INVITE and in some fringe cases To Header routing must be enabled.

    INVITE sip:211@192.168.192.88;user=phone SIP/2.0 Via: SIP/2.0/UDP 192.168.192.78:5060;branch=z9hG4bK6d5aafcc Max-Forwards: 70 From: "Extension 8010" <sip:5555558011@192.168.192.78>;tag=as1ce199ae To: sip:211@192.168.192.88;user=phone Executing [211@all-gateway-incoming:5] Set("SIP/gateway-00000086", "__INCOMING_DNIS=211") in new stack

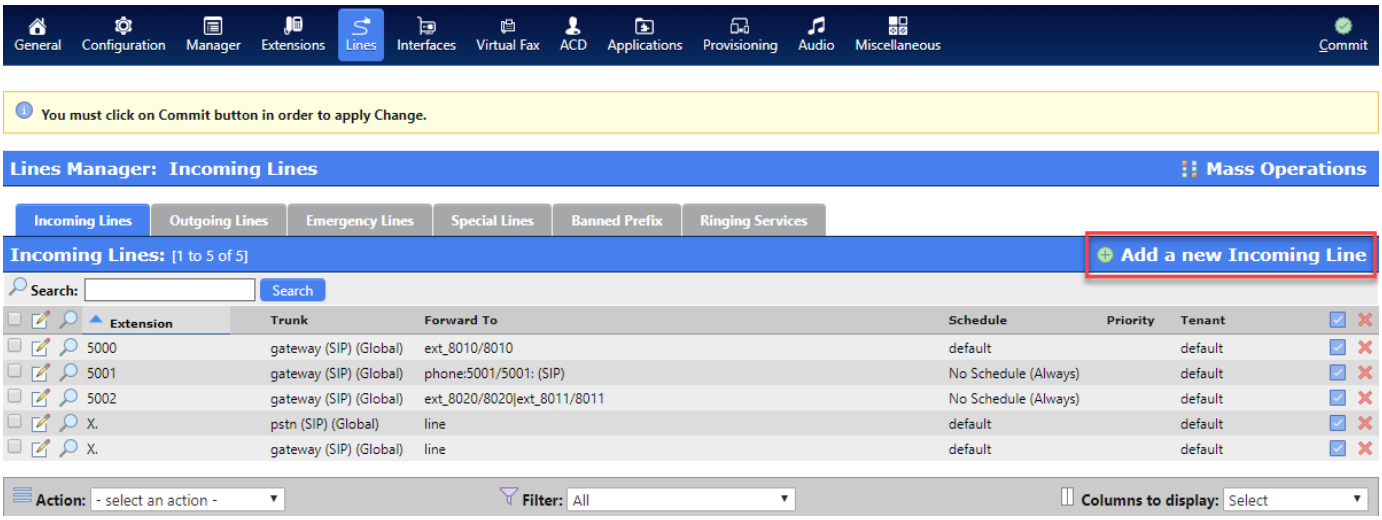
- "Port (TDM)" which are analog FXO ports supported by Sangoma or Digium cards.

Add a new Incoming Line

Incoming Lines must be created to Route incoming calls to required destinations.

From Configuration > Telephony > Lines > Incoming Lines.

Click on “Add a new Incoming Line”.



General

This is an example of SIP trunk DNIS configuration

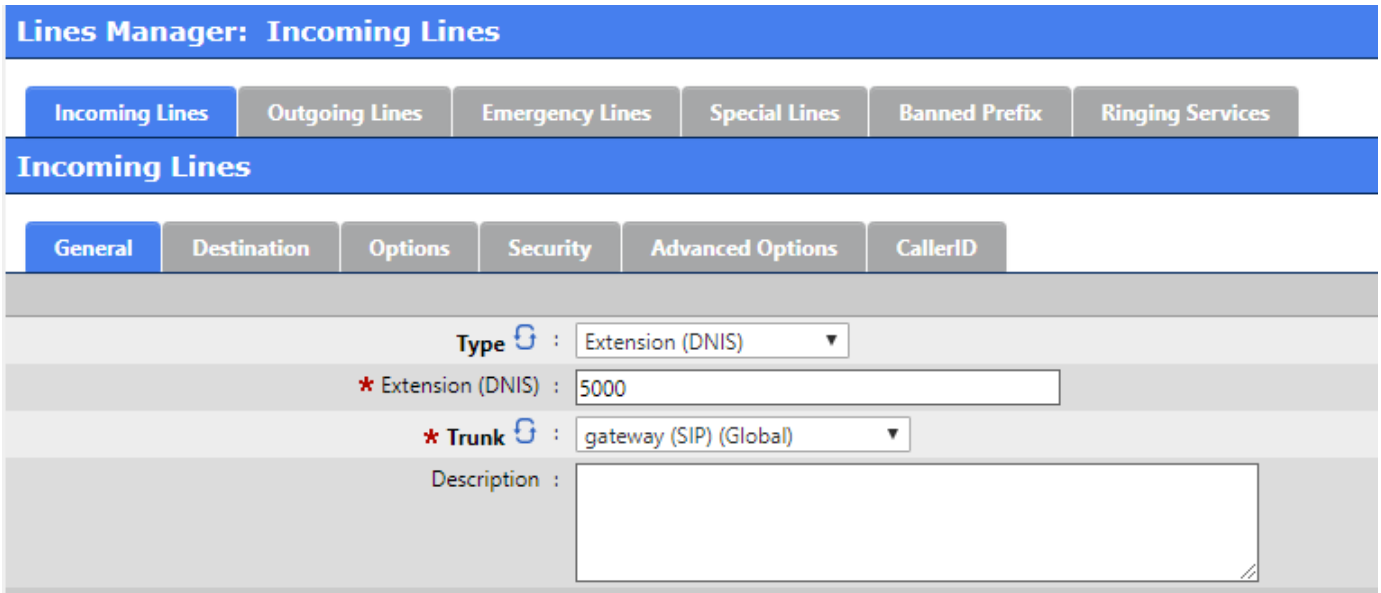
The Extension (DNIS) field is configured to match 5000 patterns are also supported like: 5XXX

There is fixed length requirement to the DNIS field, DNIS matches are matched from right to left

Outgoing Lines, Extensions, Applications, Incoming Lines are unique objects so there is no conflict when there are matching prefix patterns. Example: if an extension’s leading digit is a 9 and the Outgoing Line assigned in the CoS leading digit is a 9 and the DNIS leading digit is also a 9 there is no dial plan conflict.

The trunk is selected from the drop list, in this example ‘gateway (SIP) (Global)’

Once the DNIS and Trunk(s) are configured click on the Destination tab



Destination

Use the drop list to select a Destination type in this example Extension(s)

Use the Select button to choose one or more Extensions from using the Select tool.

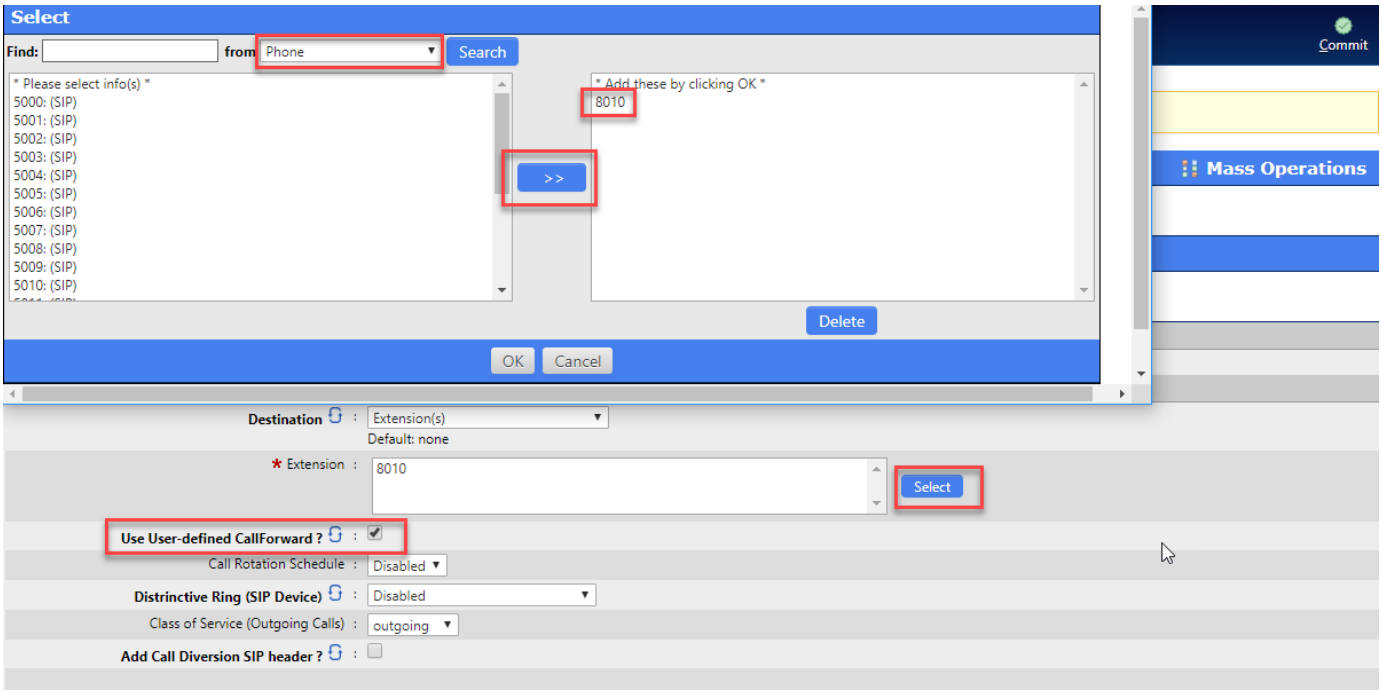
To choose Internal Extensions Use the Phone drop list selector and to enter an External Number choose that option from the drop list

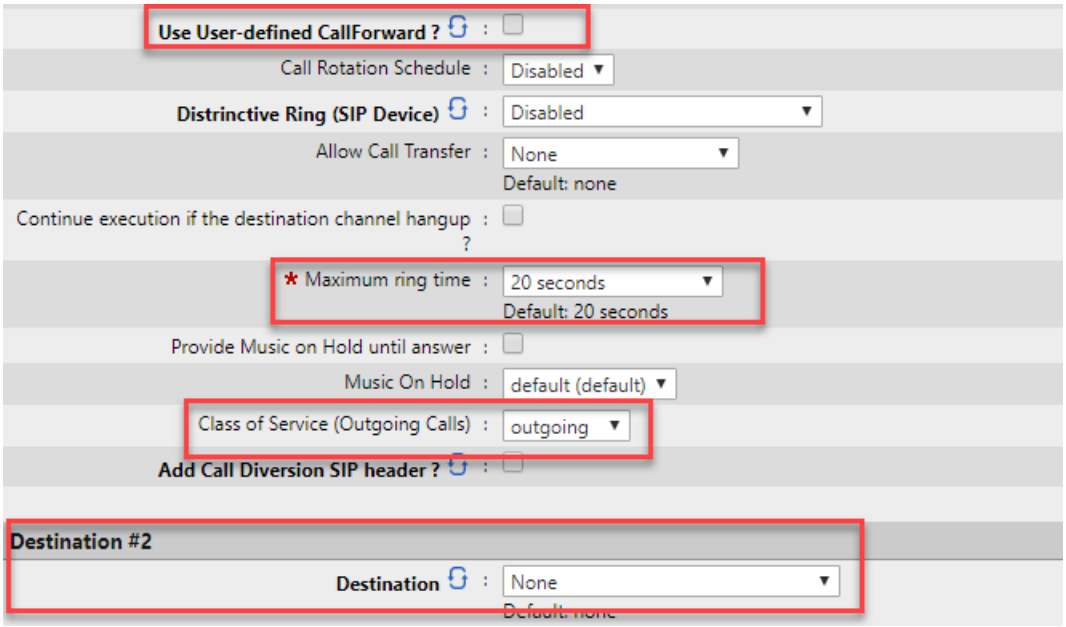
In this example Phone is selected and Extension 8010 is added from the left column to the right

The ‘Use User-defined CallForward’ option is enabled in this example because we want the User Options in Extension 8010 to be applied to this Incoming Line. If special considerations are required then do not enable this option.

If the ‘Use User-defined CallForward’ option is disabled you must configure additional CoS details and configure Destination 2 which is invoked after the ‘Maximum ring time’ value in Destination 1. If Destination 2 is not defined the Maximum ring time will terminate with a hangup.

Click on the Options tab when done





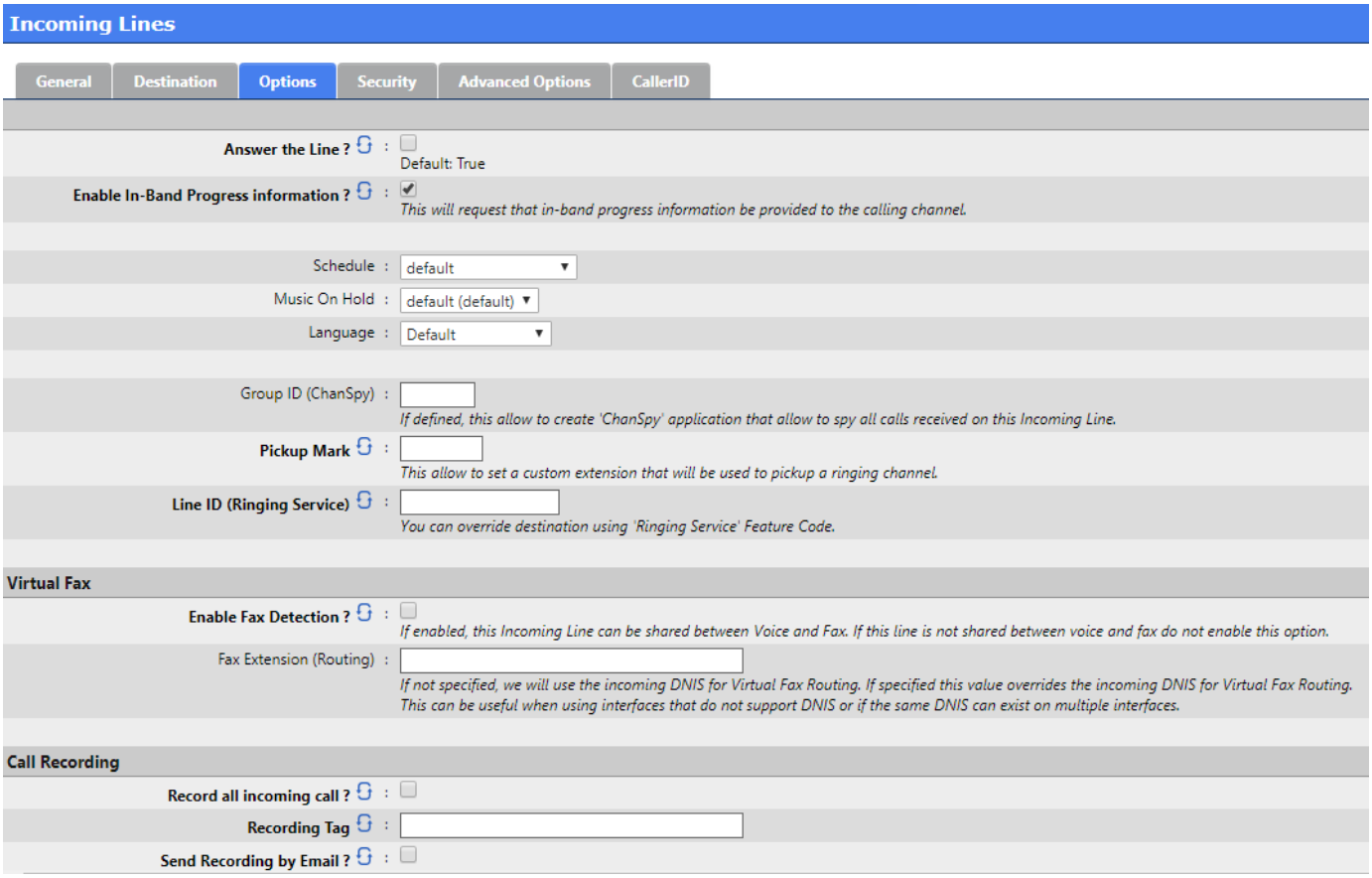
Options

There are many Incoming Line options and advanced usage is dependent on the Carrier and Trunk type.

In this example In-Band Progress messages are enabled on the SIP trunk which is very common among SIP ITSP’s. Before this option can function there are SIP Channel pre-requisites to configure

Virtual Fax and Call Recording Options can be configured if needed.

Click on the Security tab

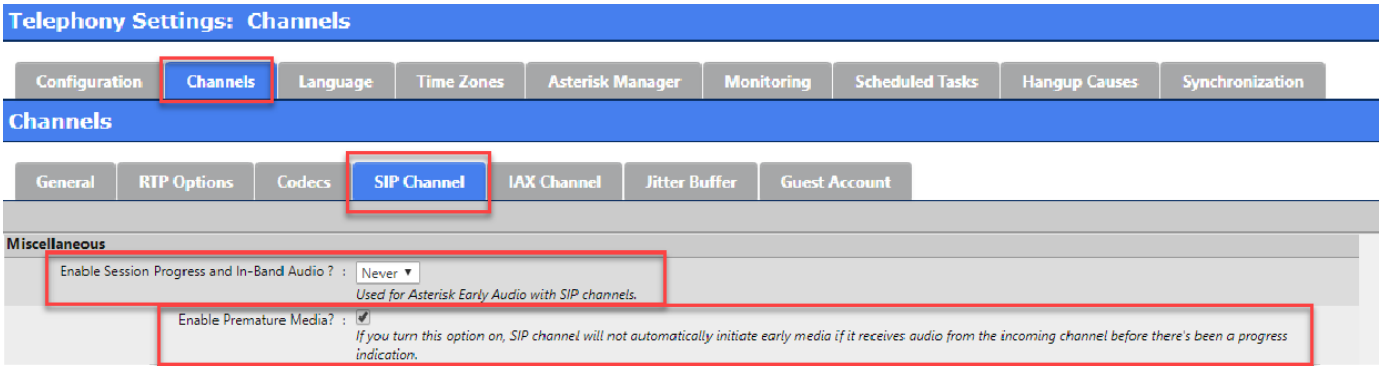


SIP In-Band Progress Pre-requisites

Enable Session Progress and In-Band Audio must be set to Never

Enable Premature Media must be enabled

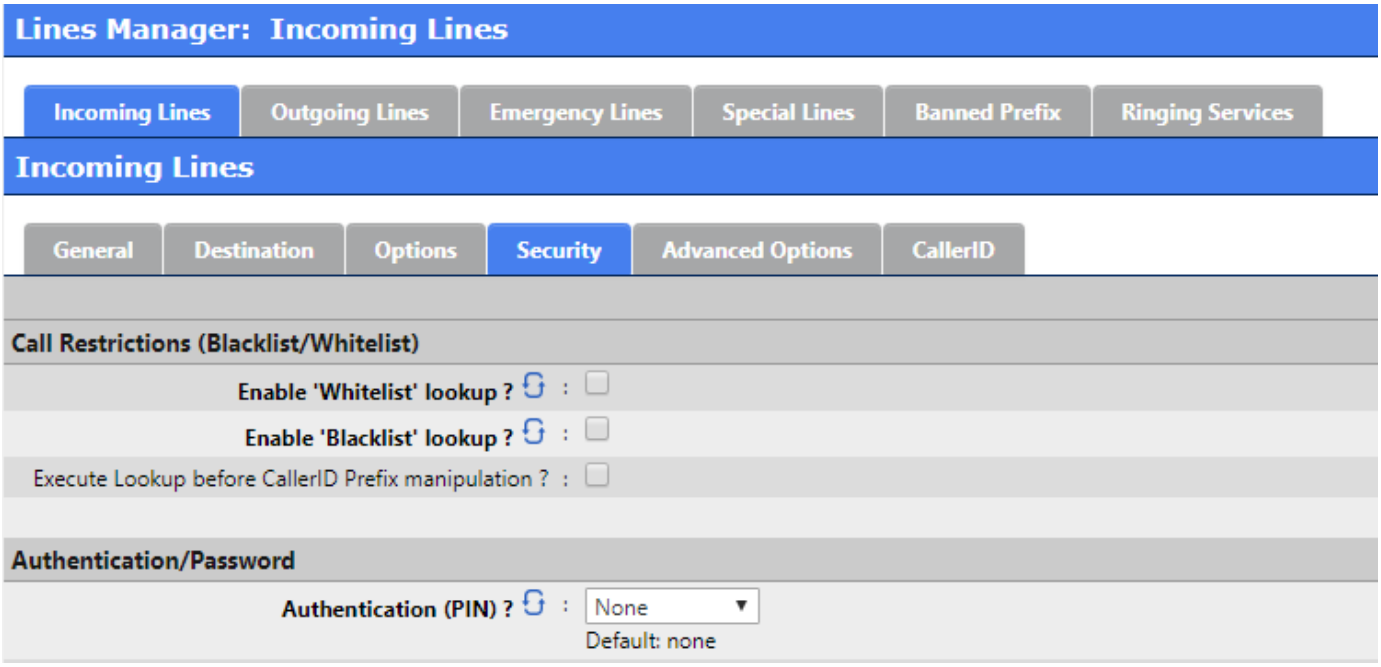
These are Global options and will effect all SIP VoIP Interfaces.



Security

Advanced Security options may be optional configured

Click on Advanced Options

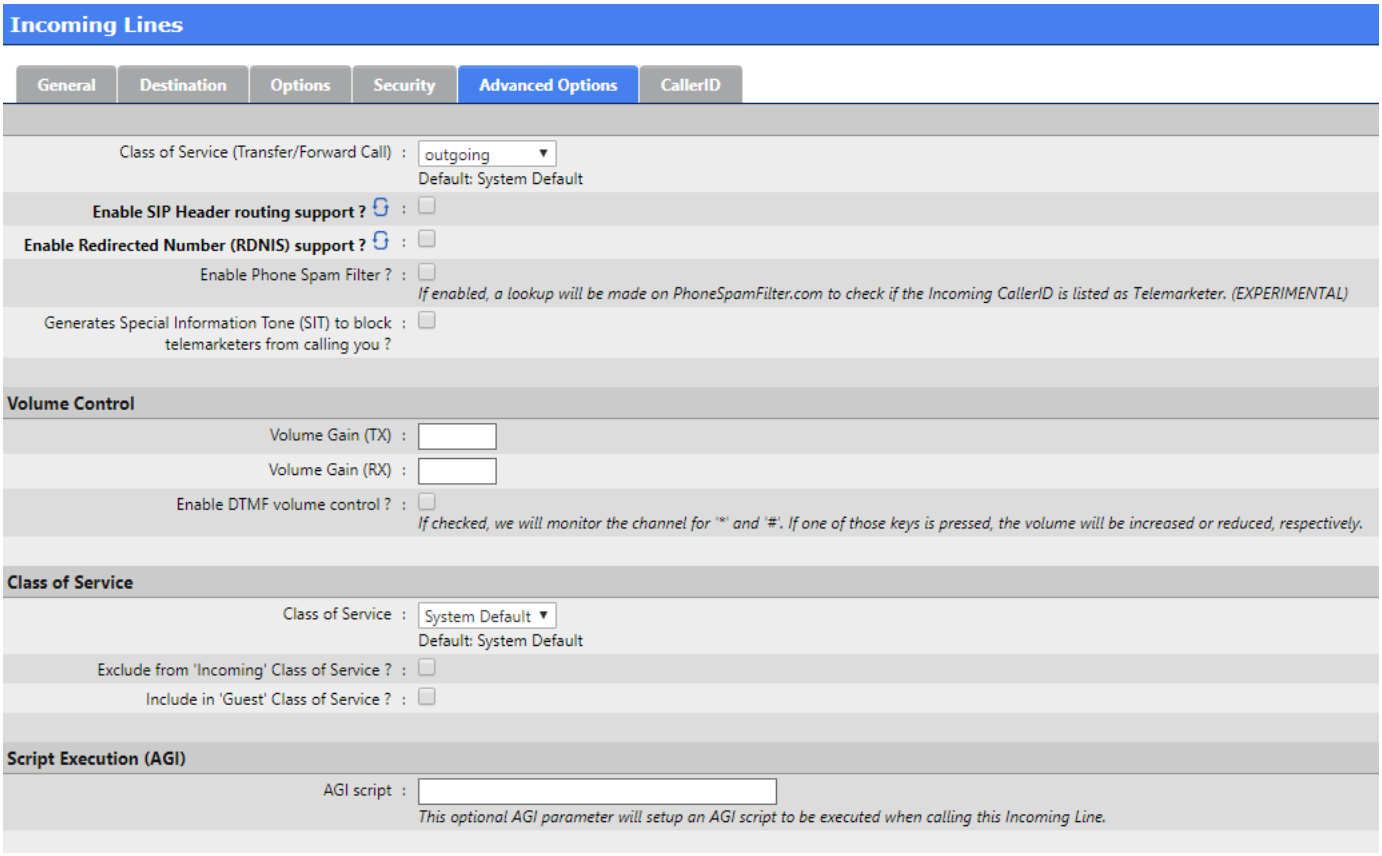


Advanced Options

Class of Service (Transfer/Forward Call) will apply specific Class of Service security considerations to any call which is transferred or forwarded by an Extension or Auto Attendant after being answered by this Incoming Line

Class of Service selection should be normally be left on System Default which does not expose the Incoming Line to any advanced Feature Codes or Outgoing Lines assigned to another Class of Service. The System Default matches the Source Interface's CoS only with assigned Incoming Lines and any Incoming Call will be rejected if there is no matching Incoming Line object. Using another Class of Service should only be considered in rare use cases.

Click on CallerID when done



CallerID

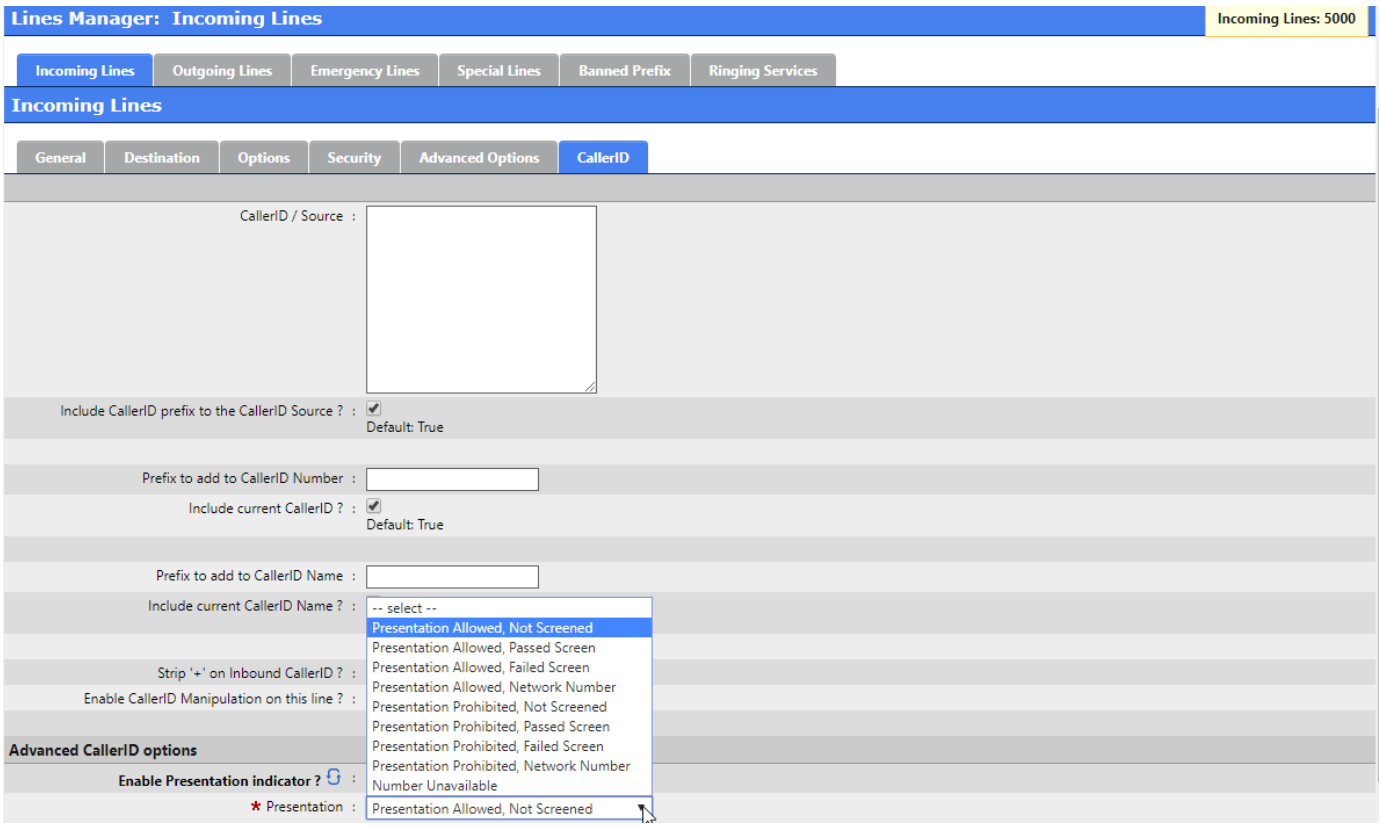
CallerID/Source text box allows multiple CallerID filters to be associated with this Incoming Line which can be used for specialized routing.

A numeric prefix can be added to the incoming call display which will be passed to the ringing phone. This can be useful if some additional dialing prefix is required to initiate an Outgoing call from the phone's CallerID history

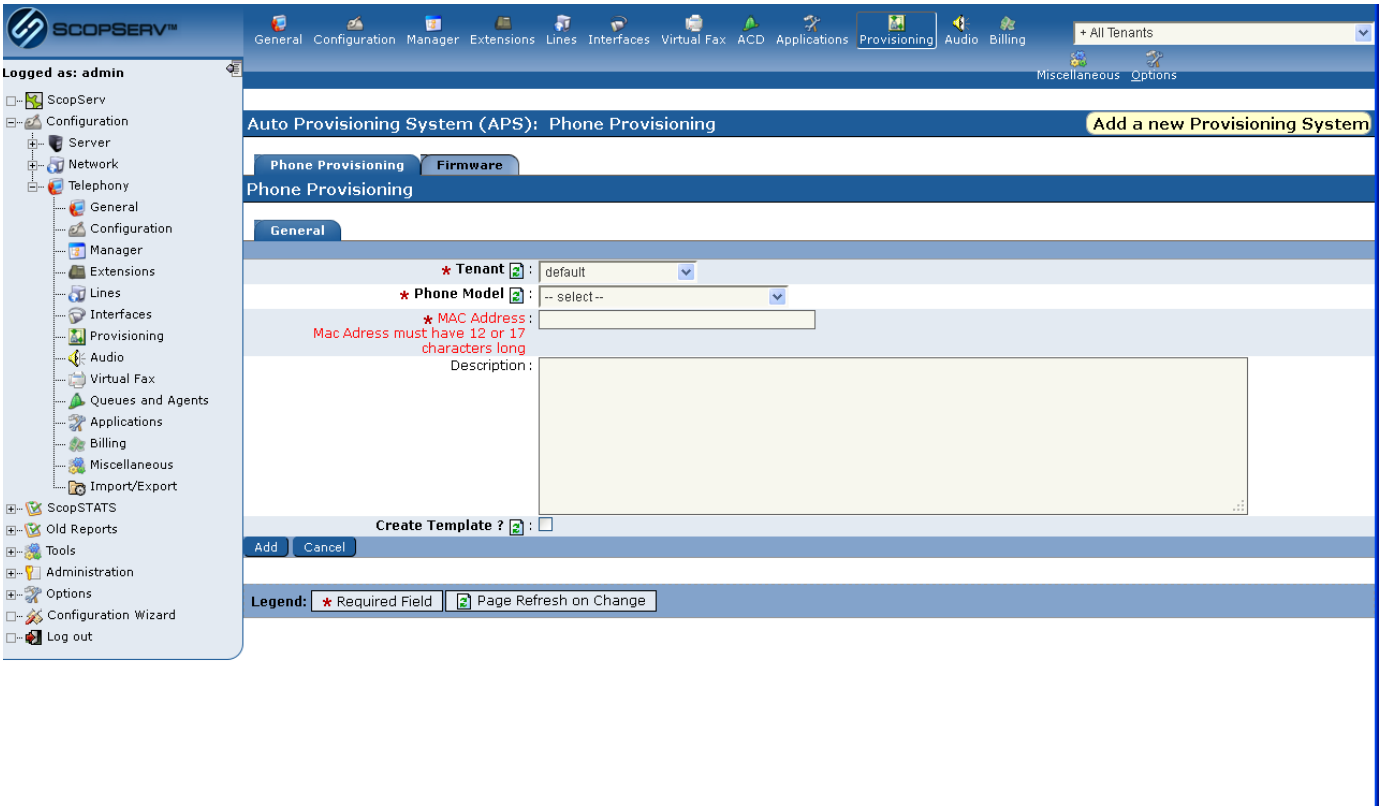
A Name prefix can be added to the incoming call display of the ringing phone. This can be useful to distinguish inbound calls for each customer and answer the phone with the correct greeting response.

Advanced CallerID options can be selected to comply with https://tools.ietf.org/html/rfc3325

Click on Add when done



Automatic Provisioning Service



The APS (Automatic Provisioning Service) is used to create the required configuration files needed for many SIP end points to work correctly.

The APS assigns SIP usernames and passwords, network options, time settings, QoS settings, dial plan options, firmware upgrade policies, soft key programming, DSS/BLF programming, security settings, DTMF modes, LDAP settings.

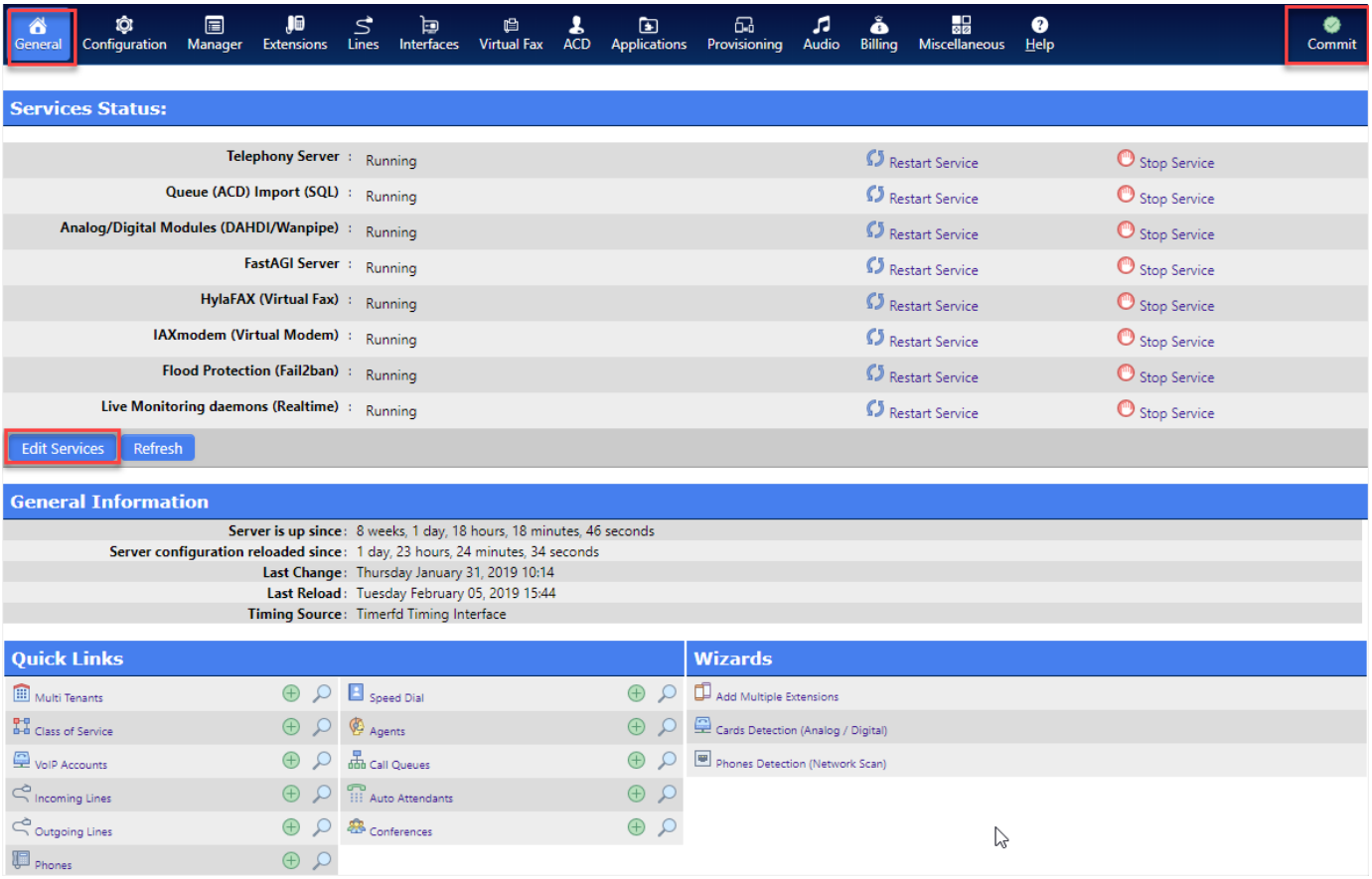
Templates can be configured to simplify tedious configuration settings for as many supported SIP end points as required.

Please refer to detailed documentation at: https://blog.scopserv.com/2013/07/how-to-use-the-SCOPTEL-automatic-provisioning-system/

Commit and Telephony Services Manager

From Configuration > Telephony >General

- Edit the Serices Manager to enable and missing modules which need to be added to automatic boot services
- When all is configured then all changes must be Committed in order to reload the configurations into memory. Click the “Commit” button.
- If you have any Digum or Sangoma hardware installed then the Analog/Digital Modules (DAHDI/Wanpipe) services must be restarted to properly reload Analog/Digital Modules (DAHDI/Wanpipe) kernel drivers.
- The correct order to reset Analog/Digital Modules (DAHDI/Wanpipe) services is:
- Stop the “Telephony Server”
- Restart the Analog/Digital Modules (DAHDI/Wanpipe) Service
- Start the “Telephony Server”


General
Configuration
Manager
Extensions
Lines
Interfaces
Virtual Fax
ACD
Applications
Provisioning
Audio
Billing
Miscellaneous
Help
Commit
Services Status:
Telephony Server : Running
Queue (ACD) Import (SQL) : Running
Analog/Digital Modules (DAHDI/Wanpipe) : Running
FastAGI Server : Running
HylaFAX (Virtual Fax) : Running
IAXmodem (Virtual Modem) : Running
Flood Protection (Fail2ban) : Running
Live Monitoring daemons (Realtime) : Running
Restart Service
Stop Service
Edit Services
Refresh
General Information
Server is up since: 8 weeks, 1 day, 18 hours, 18 minutes, 46 seconds
Server configuration reloaded since: 1 day, 23 hours, 24 minutes, 34 seconds
Last Change: Thursday January 31, 2019 10:14
Last Reload: Tuesday February 05, 2019 15:44
Timing Source: Timerfd Timing Interface
Quick Links
Multi Tenants
Class of Service
VoIP Accounts
Incoming Lines
Outgoing Lines
Phones
Speed Dial
Agents
Call Queues
Auto Attendants
Conferences
Wizards
Add Multiple Extensions
Cards Detection (Analog / Digital)
Phones Detection (Network Scan)