SCOPTEL IP PBX Software - Managing Extensions

Contents

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

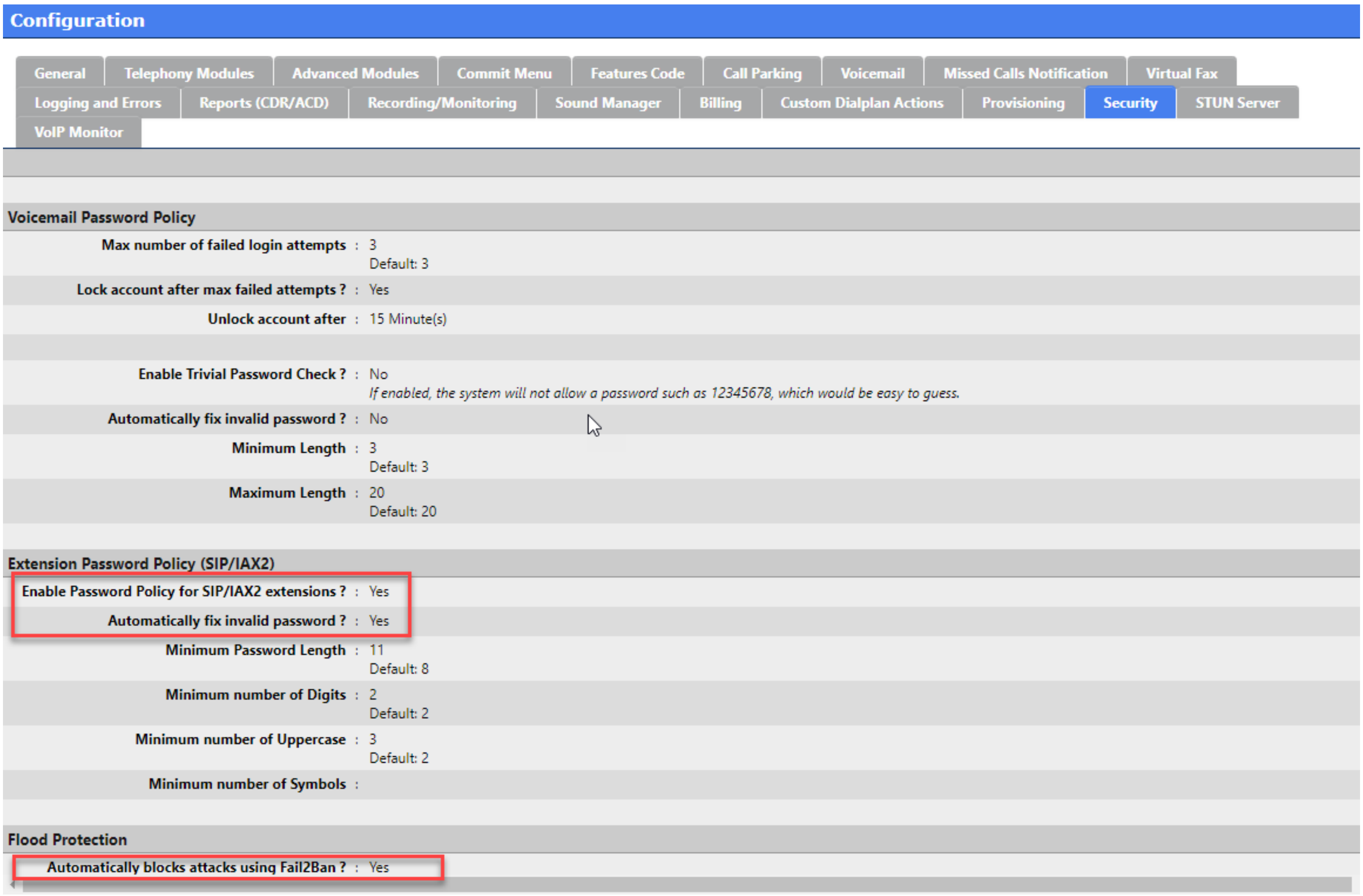
- Minimum password length of 8 alpha numeric characters.
- No Dictionary words
- Minimum 2 Upper Case characters used
- Minimum 2 numerals used
- Passwords should be unique for each extension

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



Voicemail Password Policy

Max number of failed login attempts : 3
Default: 3

Lock account after max failed attempts ? : Yes

Unlock account after : 15 Minute(s)

Enable Trivial Password Check ? : No
If enabled, the system will not allow a password such as 12345678, which would be easy to guess.

Automatically fix invalid password ? : No

Minimum Length : 3
Default: 3

Maximum Length : 20
Default: 20

Extension Password Policy (SIP/IAX2)

Enable Password Policy for SIP/IAX2 extensions ? : Yes

Automatically fix invalid password ? : Yes

Minimum Password Length : 11
Default: 8

Minimum number of Digits : 2
Default: 2

Minimum number of Uppercase : 3
Default: 2

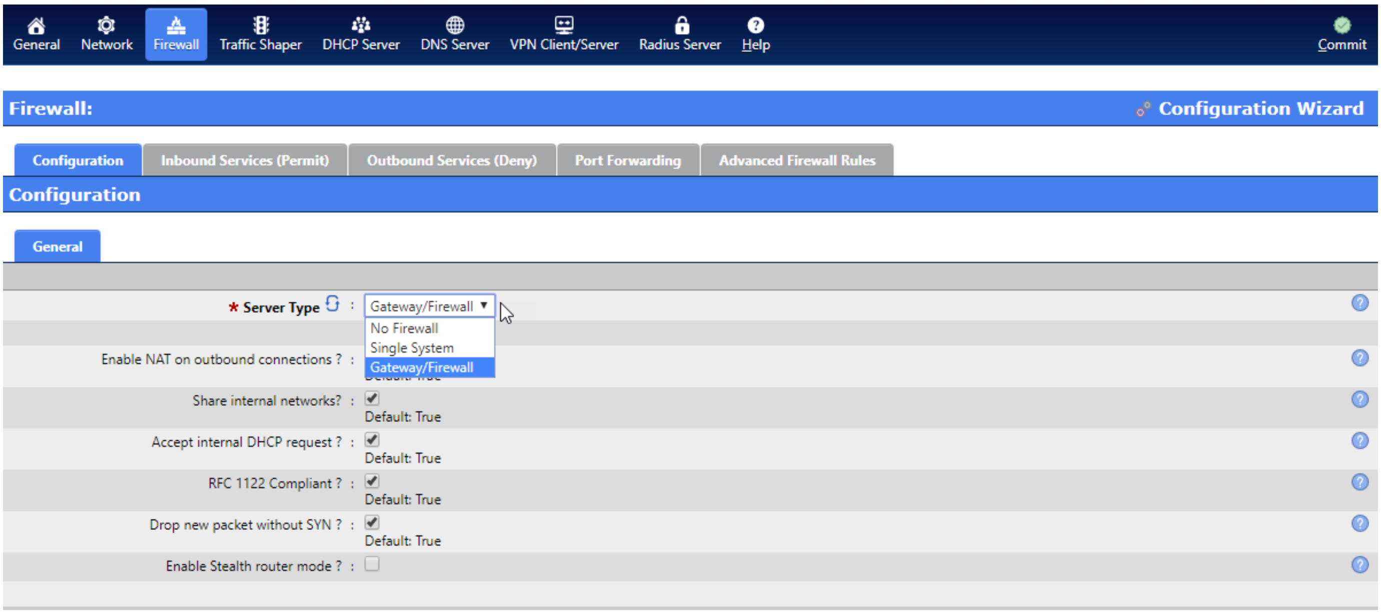
Minimum number of Symbols :

Flood Protection

Automatically blocks attacks using Fail2Ban ? : Yes

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.



* Server Type : Gateway/Firewall ▾
No Firewall
Single System
Gateway/Firewall

Enable NAT on outbound connections ? :

Share internal networks? : ☑
Default: True

Accept internal DHCP request ? : ☑
Default: True

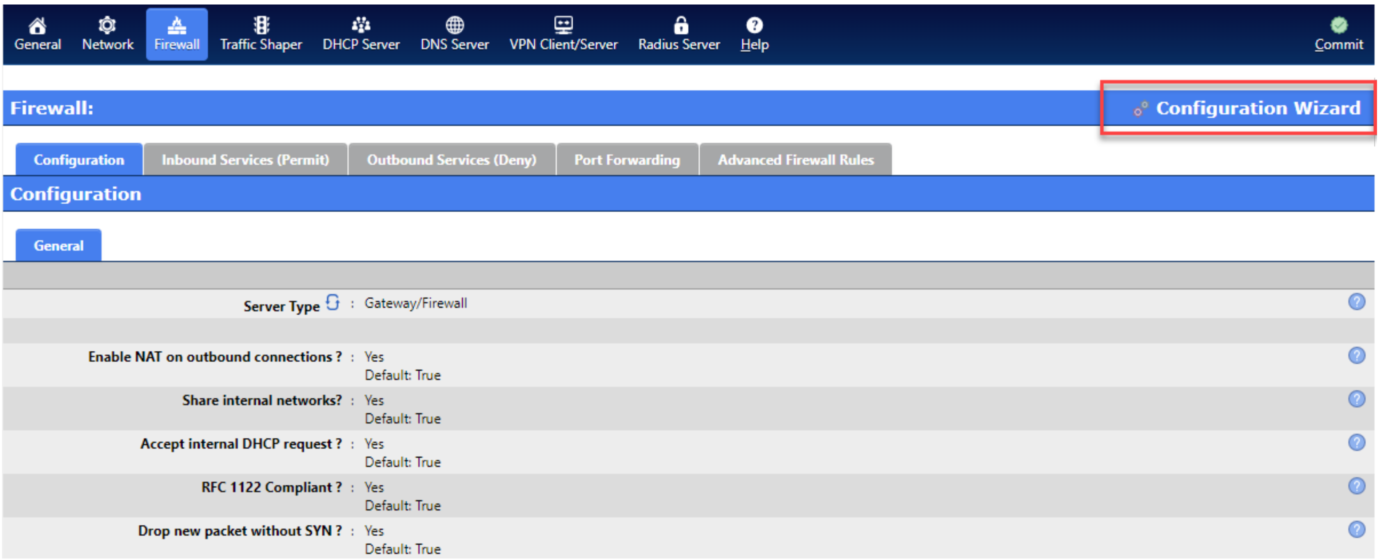
RFC 1122 Compliant ? : ☑
Default: True

Drop new packet without SYN ? : ☑
Default: True

Enable Stealth router mode ? : □

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
- Choose the “Single System” option
- Click “Next”



Server Type : Gateway/Firewall

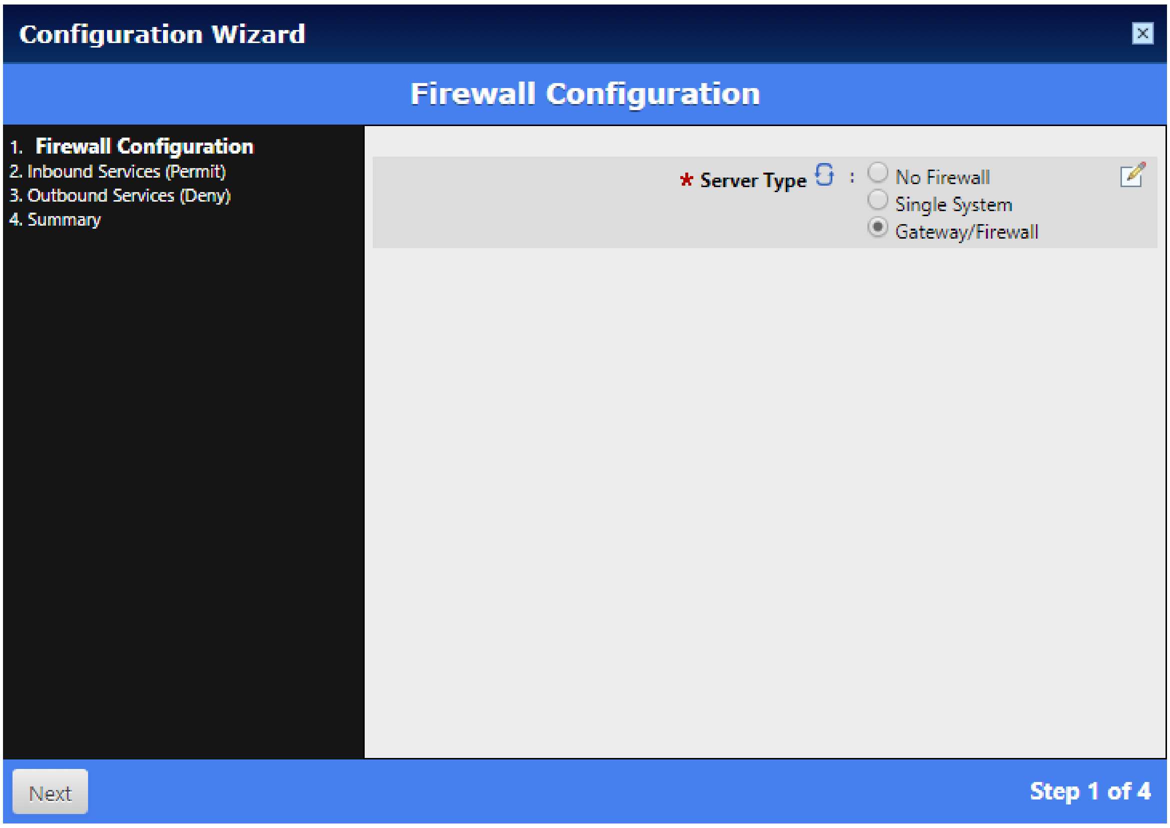
Enable NAT on outbound connections ? : Yes
Default: True

Share internal networks? : Yes
Default: True

Accept internal DHCP request ? : Yes
Default: True

RFC 1122 Compliant ? : Yes
Default: True

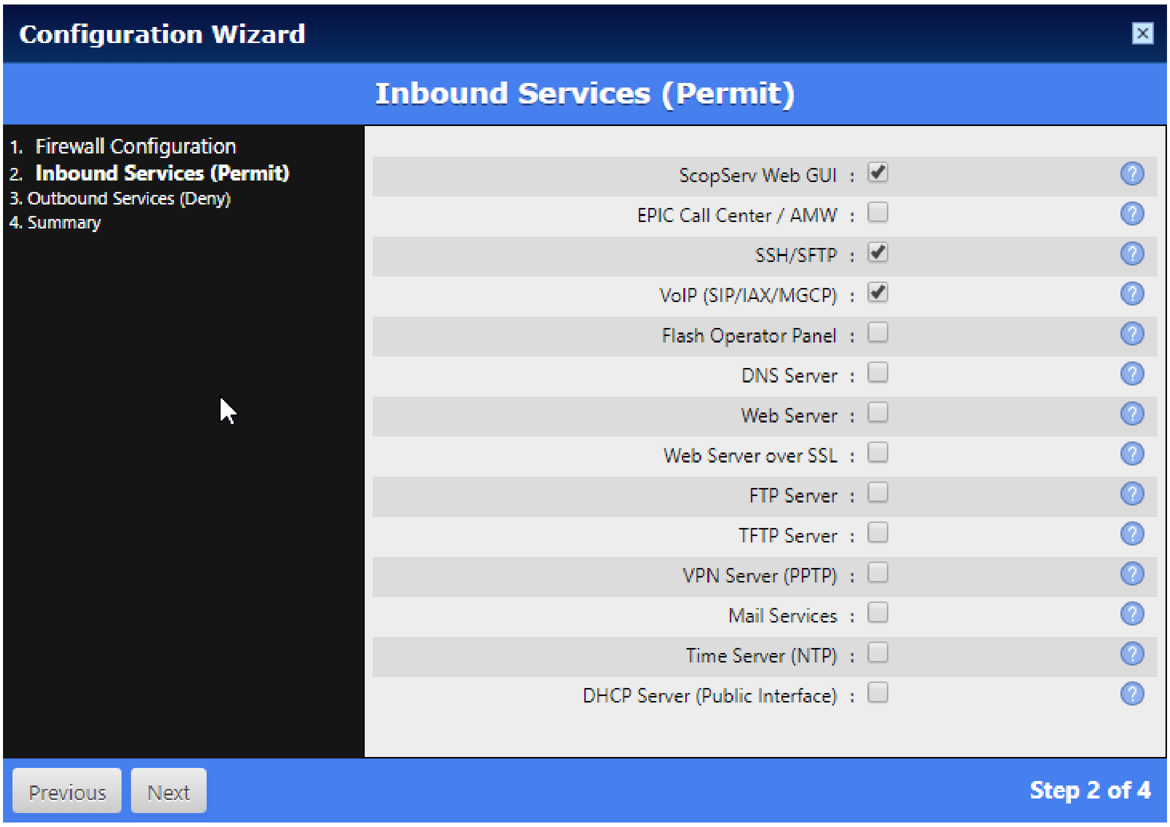
Drop new packet without SYN ? : Yes
Default: True


Configuration Wizard
Firewall Configuration
1. Firewall Configuration
2. Inbound Services (Permit)
3. Outbound Services (Deny)
4. Summary
Next
Step 1 of 4

* Server Type : ○ No Firewall ○ Single System ● Gateway/Firewall

Firewall Inbound Services

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


Configuration Wizard
Inbound Services (Permit)
1. Firewall Configuration
2. Inbound Services (Permit)
3. Outbound Services (Deny)
4. Summary
Previous
Next
Step 2 of 4

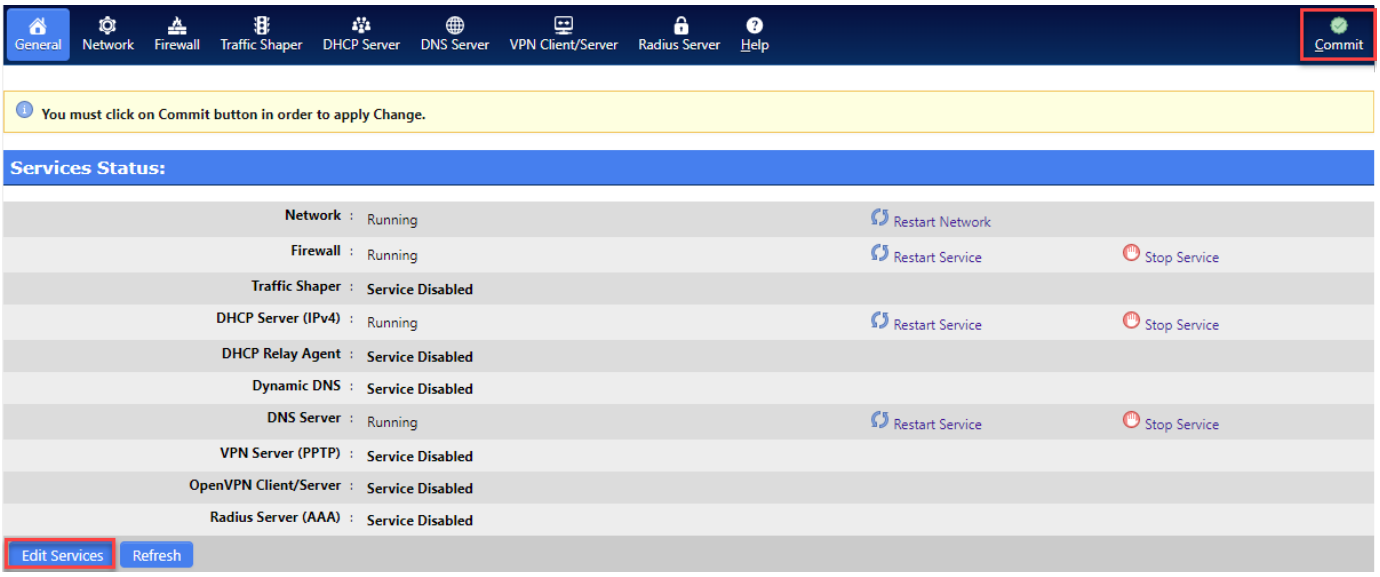
ScopServ Web GUI : ☑
EPIC Call Center / AMW : □
SSH/SFTP : ☑
VoIP (SIP/IAX/MGCP) : ☑
Flash Operator Panel : □
DNS Server : □
Web Server : □
Web Server over SSL : □
FTP Server : □
TFTP Server : □
VPN Server (PPTP) : □
Mail Services : □
Time Server (NTP) : □
DHCP Server (Public Interface) : □

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.



You must click on Commit button in order to apply Change.

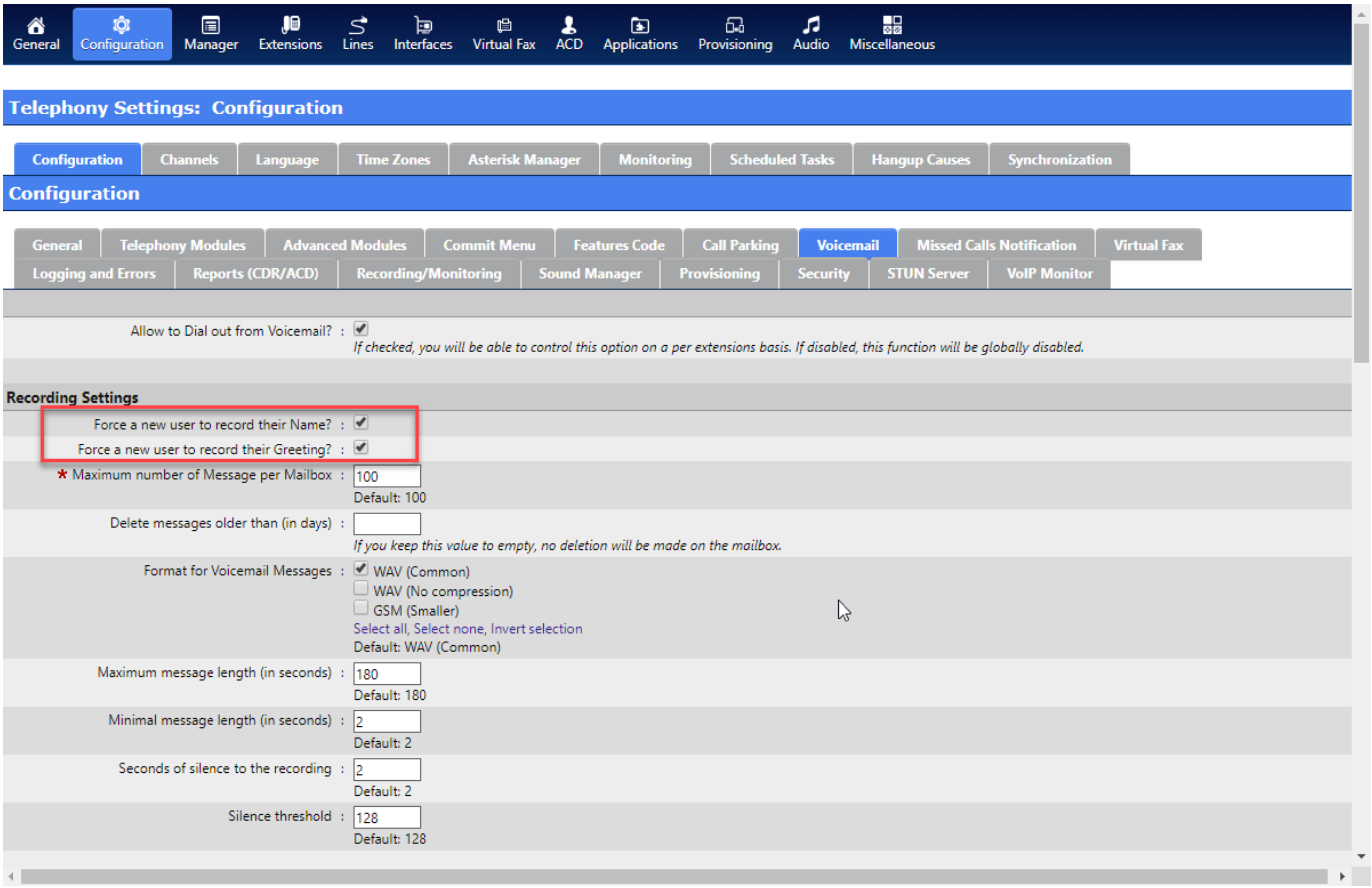
Services Status:

Network :	Running	Restart Network	
Firewall :	Running	Restart Service	Stop Service
Traffic Shaper :	Service Disabled		
DHCP Server (IPv4) :	Running	Restart Service	Stop Service
DHCP Relay Agent :	Service Disabled		
Dynamic DNS :	Service Disabled		
DNS Server :	Running	Restart Service	Stop Service
VPN Server (PPTP) :	Service Disabled		
OpenVPN Client/Server :	Service Disabled		
Radius Server (AAA) :	Service Disabled		

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.



Telephony Settings: Configuration

Configuration

Allow to Dial out from Voicemail? : ☑
If checked, you will be able to control this option on a per extensions basis. If disabled, this function will be globally disabled.

Recording Settings

Force a new user to record their Name? : ☑

Force a new user to record their Greeting? : ☑

* Maximum number of Message per Mailbox : 100
Default: 100

Delete messages older than (in days) :
If you keep this value to empty, no deletion will be made on the mailbox.

Format for Voicemail Messages : ☑ WAV (Common)
☐ WAV (No compression)
☐ GSM (Smaller)
Select all, Select none, Invert selection
Default: WAV (Common)

Maximum message length (in seconds) : 180
Default: 180

Minimal message length (in seconds) : 2
Default: 2

Seconds of silence to the recording : 2
Default: 2

Silence threshold : 128
Default: 128

Types

SIP Extension

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

IAX2 Extension

- **IAX2** Extension (IP Extension using the IAX 2 protocol) is allowed its own voicemail box and therefore requires a User license

Zap Extension

- **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** 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.

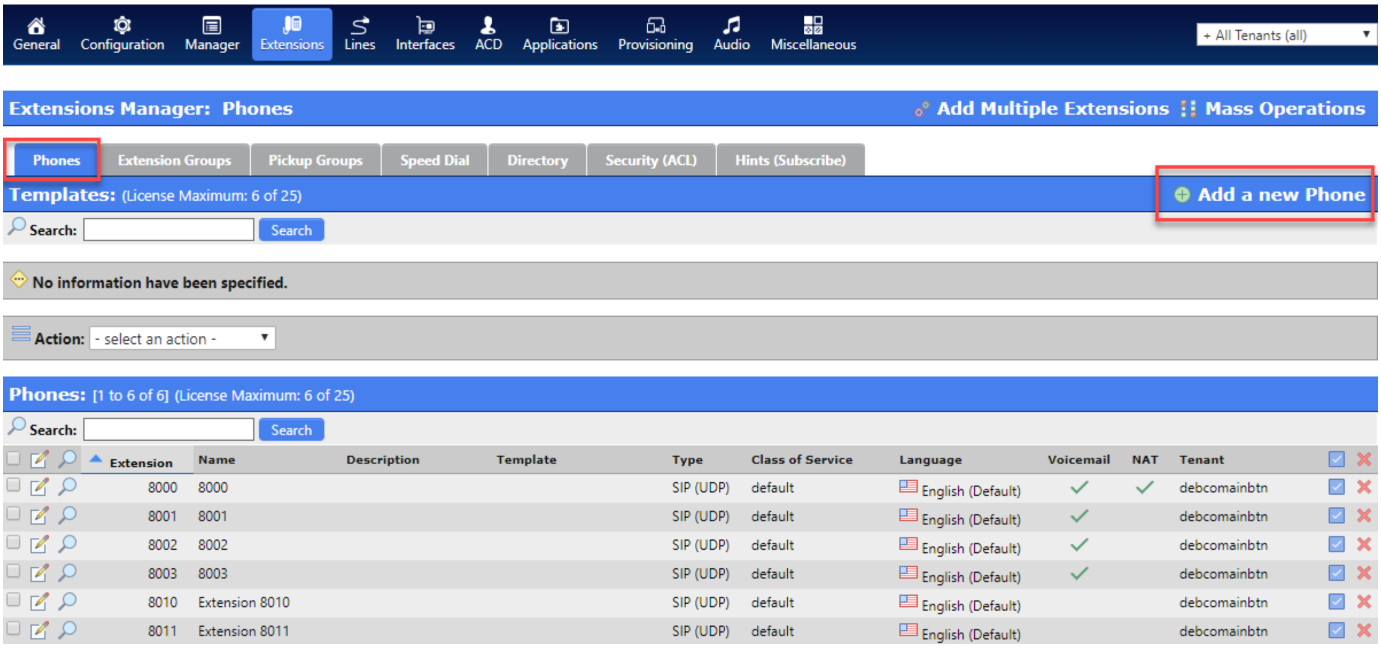
Shared Device Extension

- 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.

Extension

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



Extensions Manager: Phones

Templates: (License Maximum: 6 of 25)

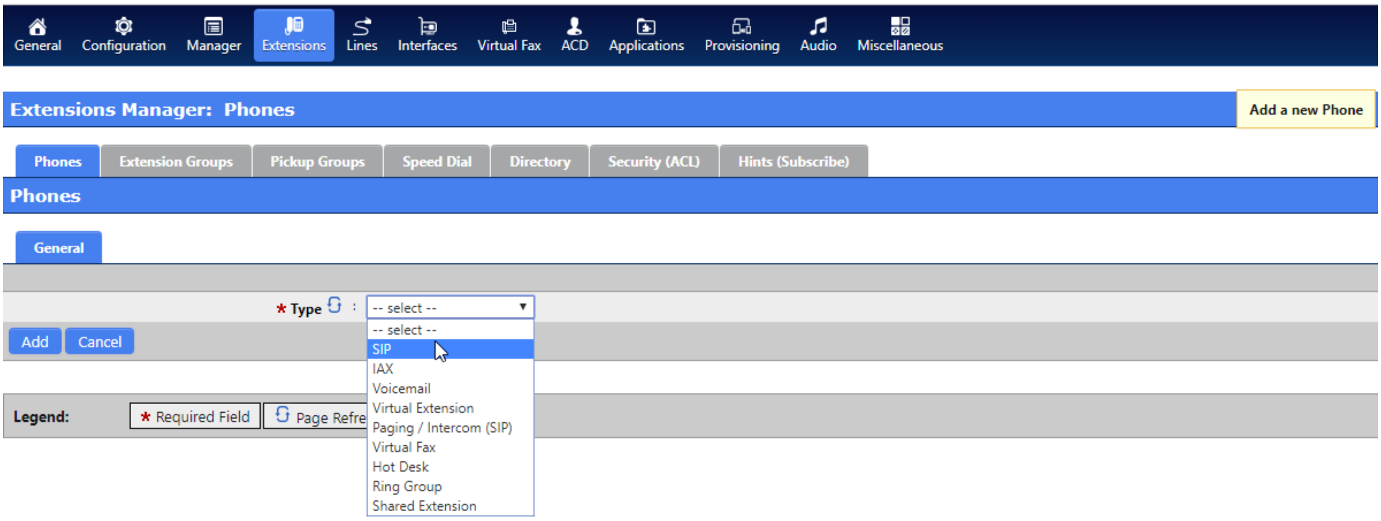
No information have been specified.

Phones: [1 to 6 of 6] (License Maximum: 6 of 25)

Extension	Name	Description	Template	Type	Class of Service	Language	Voicemail	NAT	Tenant
8000	8000			SIP (UDP)	default	English (Default)	✓	✓	debcomainbtn
8001	8001			SIP (UDP)	default	English (Default)	✓		debcomainbtn
8002	8002			SIP (UDP)	default	English (Default)	✓		debcomainbtn
8003	8003			SIP (UDP)	default	English (Default)	✓		debcomainbtn
8010	Extension 8010			SIP (UDP)	default	English (Default)			debcomainbtn
8011	Extension 8011			SIP (UDP)	default	English (Default)			debcomainbtn

Type

Choose “SIP” from the list of available Extension types



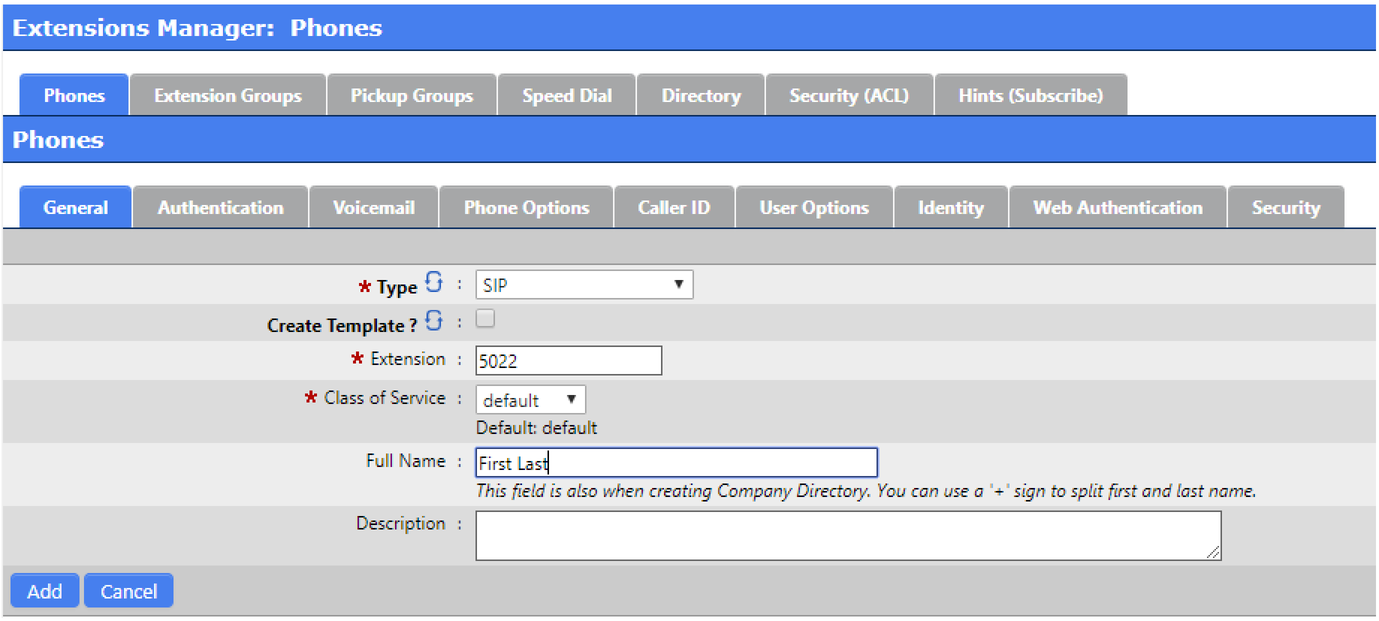
Extensions Manager: Phones

Phones

* Type : -- select --

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



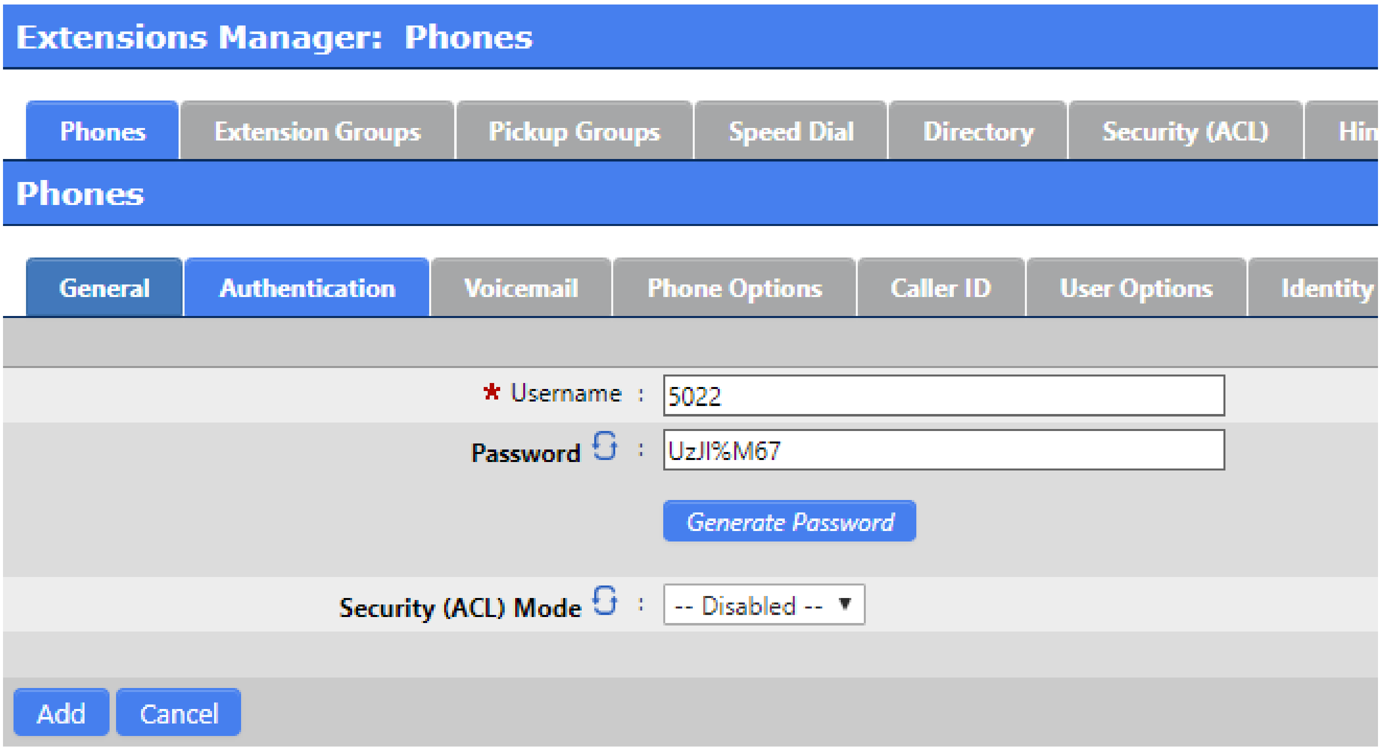
Extensions Manager: Phones

Phones

* Type :	SIP
Create Template ? :	□
* Extension :	5022
* Class of Service :	default Default: default
Full Name :	First Last *This field is also when creating Company Directory. You can use a '+' sign to split first and last name.*
Description :	

Authentication

- The Username should match the numeric value of this Extension number
- Since the Security Policy enforces a strict SIP/IAX 2 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.



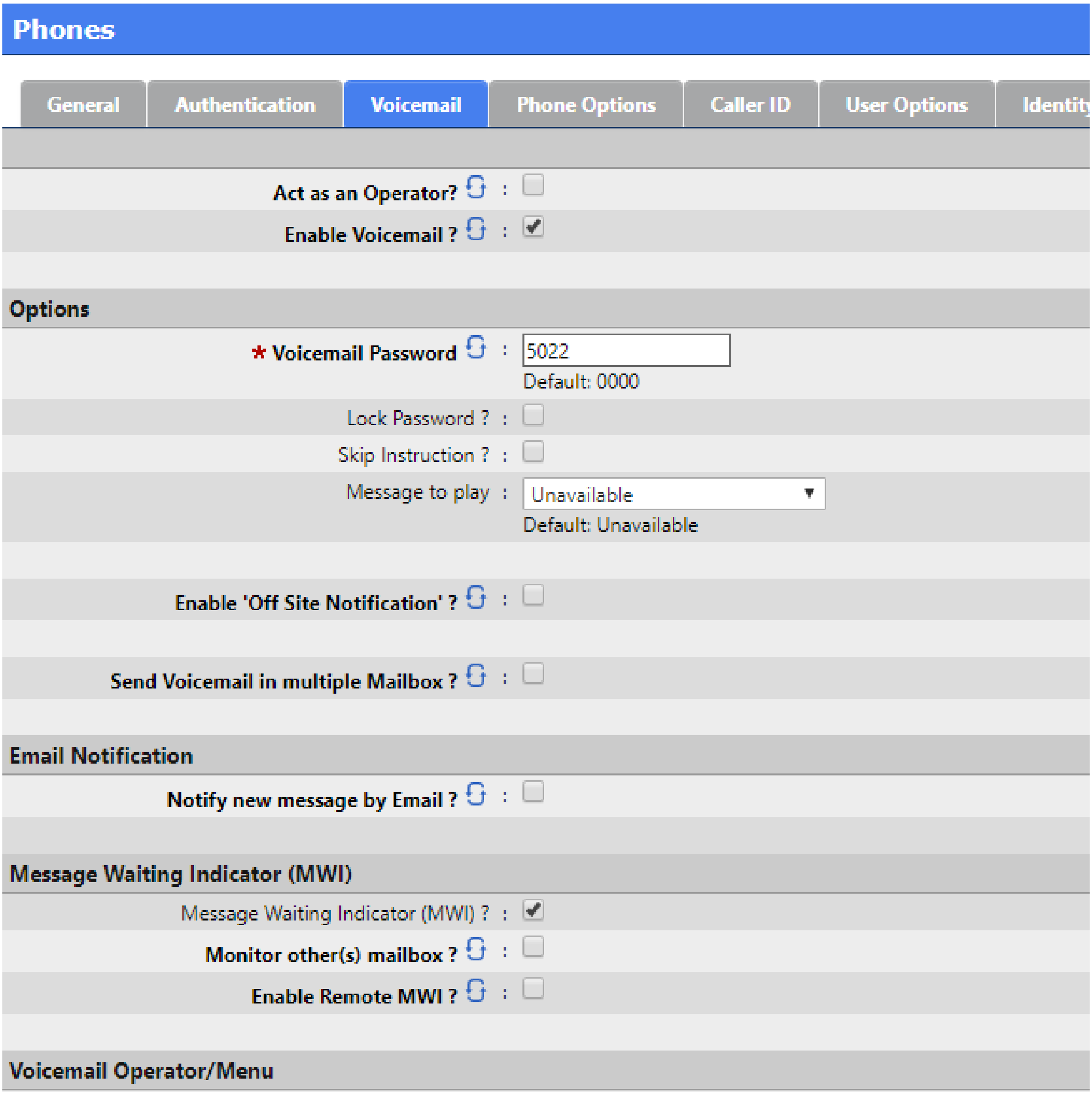
* Username : 5022

Password : UzJI%M67

Security (ACL) Mode : -- Disabled --

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



Act as an Operator? : □

Enable Voicemail ? : ☑

Options

* Voicemail Password : 5022
Default: 0000

Lock Password ? : □

Skip Instruction ? : □

Message to play : Unavailable
Default: Unavailable

Enable 'Off Site Notification' ? : □

Send Voicemail in multiple Mailbox ? : □

Email Notification

Notify new message by Email ? : □

Message Waiting Indicator (MWI)

Message Waiting Indicator (MWI) ? : ☑

Monitor other(s) mailbox ? : □

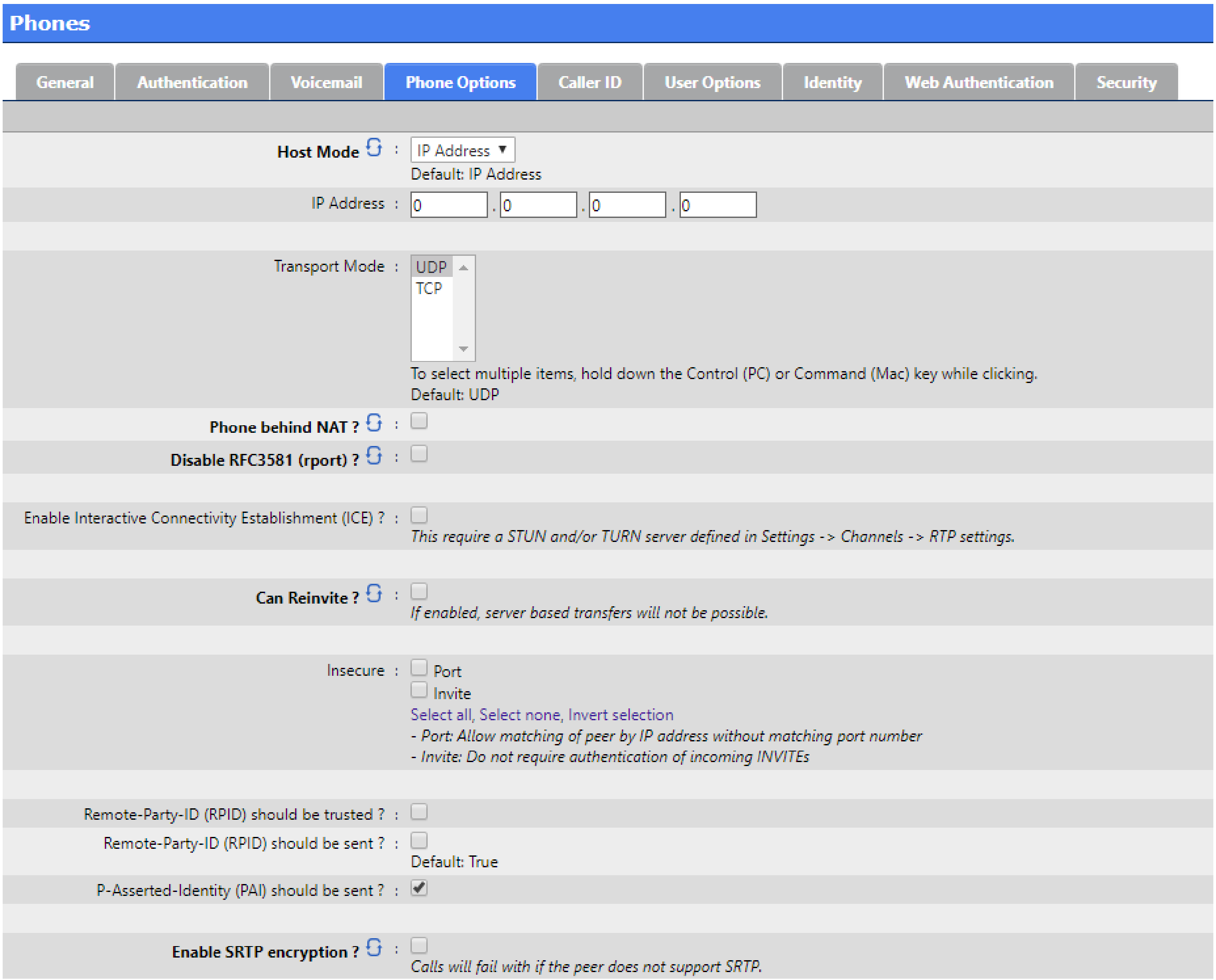
Enable Remote MWI ? : □

Voicemail Operator/Menu

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/



Host Mode : IP Address ▼
Default: IP Address

IP Address : 0 . 0 . 0 . 0

Transport Mode : UDP
TCP
To select multiple items, hold down the Control (PC) or Command (Mac) key while clicking.
Default: UDP

Phone behind NAT ? : □

Disable RFC3581 (rport) ? : □

Enable Interactive Connectivity Establishment (ICE) ? : □
This require a STUN and/or TURN server defined in Settings -> Channels -> RTP settings.

Can Reinvite ? : □
If enabled, server based transfers will not be possible.

Insecure : □ Port
□ Invite
Select all, Select none, Invert selection
- *Port: Allow matching of peer by IP address without matching port number*
- *Invite: Do not require authentication of incoming INVITEs*

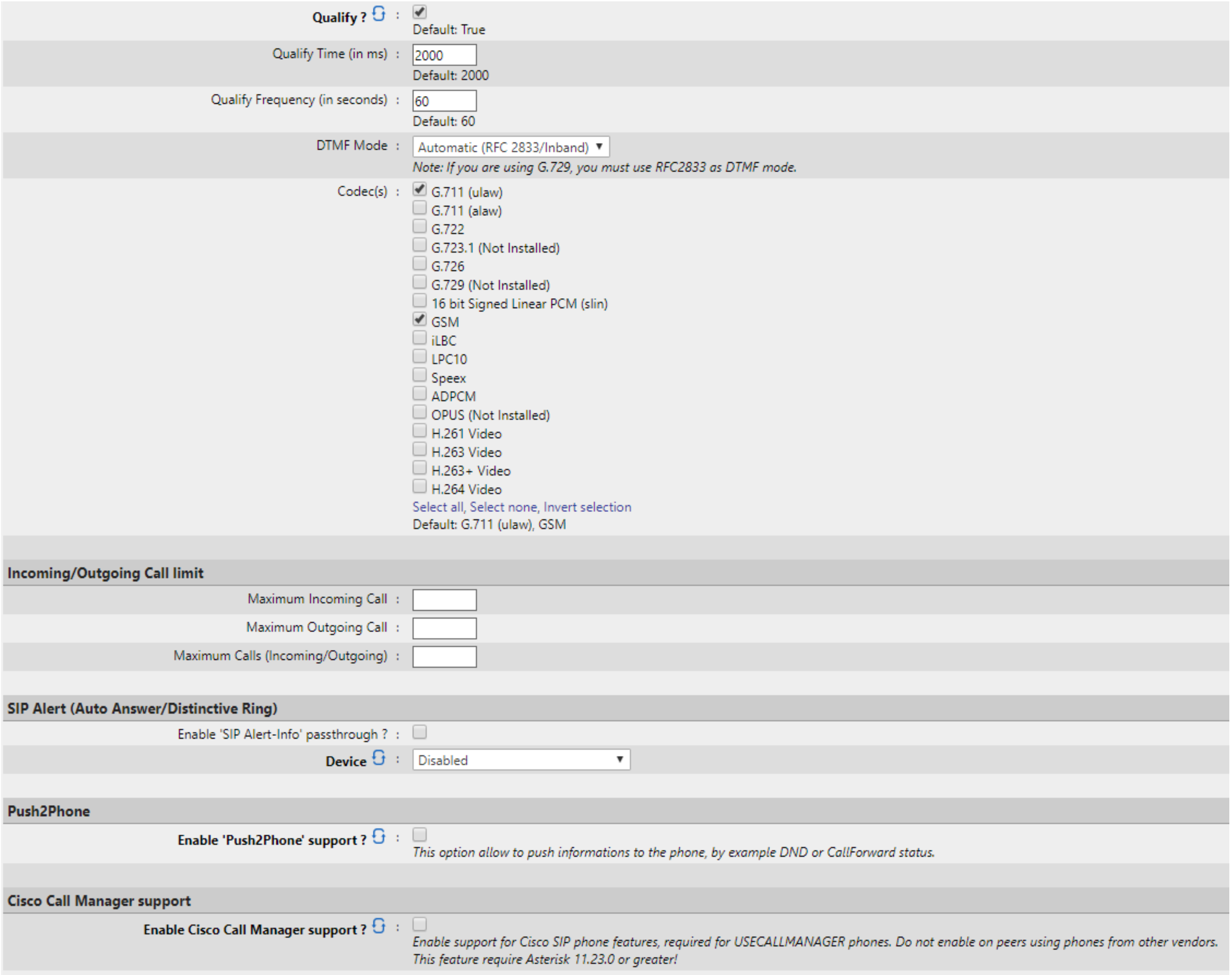
Remote-Party-ID (RPID) should be trusted ? : □

Remote-Party-ID (RPID) should be sent ? : □
Default: True

P-Asserted-Identity (PAI) should be sent ? : ☑

Enable SRTP encryption ? : □
Calls will fail with if the peer does not support SRTP.

- 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



Qualify ? : ☑
Default: True

Qualify Time (in ms) : 2000
Default: 2000

Qualify Frequency (in seconds) : 60
Default: 60

DTMF Mode : Automatic (RFC 2833/Inband) ▼
Note: If you are using G.729, you must use RFC2833 as DTMF mode.

Codec(s) :
☑ G.711 (ulaw)
□ G.711 (alaw)
□ G.722
□ G.723.1 (Not Installed)
□ G.726
□ G.729 (Not Installed)
□ 16 bit Signed Linear PCM (slin)
☑ GSM
□ iLBC
□ LPC10
□ Speex
□ ADPCM
□ OPUS (Not Installed)
□ H.261 Video
□ H.263 Video
□ H.263+ Video
□ H.264 Video
Select all, Select none, Invert selection
Default: G.711 (ulaw), GSM

Incoming/Outgoing Call limit

Maximum Incoming Call :

Maximum Outgoing Call :

Maximum Calls (Incoming/Outgoing) :

SIP Alert (Auto Answer/Distinctive Ring)

Enable 'SIP Alert-Info' passthrough ? : □

Device : Disabled ▼

Push2Phone

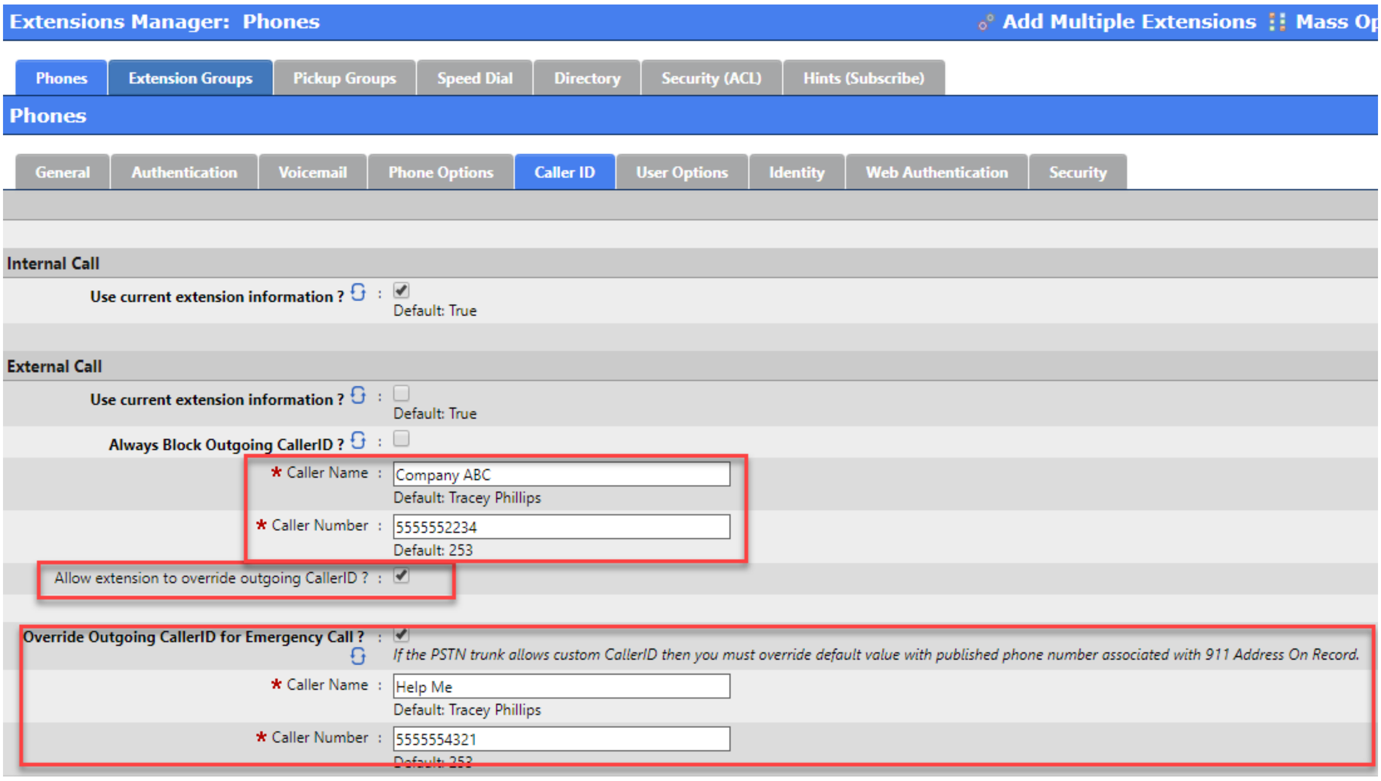
Enable 'Push2Phone' support ? : □
This option allow to push informations to the phone, by example DND or CallForward status.

Cisco Call Manager support

Enable Cisco Call Manager support ? : □
Enable support for Cisco SIP phone features, required for USECALLMANAGER phones. Do not enable on peers using phones from other vendors. This feature require Asterisk 11.23.0 or greater!

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



Internal Call

Use current extension information ? : ☑ Default: True

External Call

Use current extension information ? : ☐ Default: True

Always Block Outgoing CallerID ? : ☐

* Caller Name : Company ABC Default: Tracey Phillips

* Caller Number : 5555552234 Default: 253

Allow extension to override outgoing CallerID ? : ☑

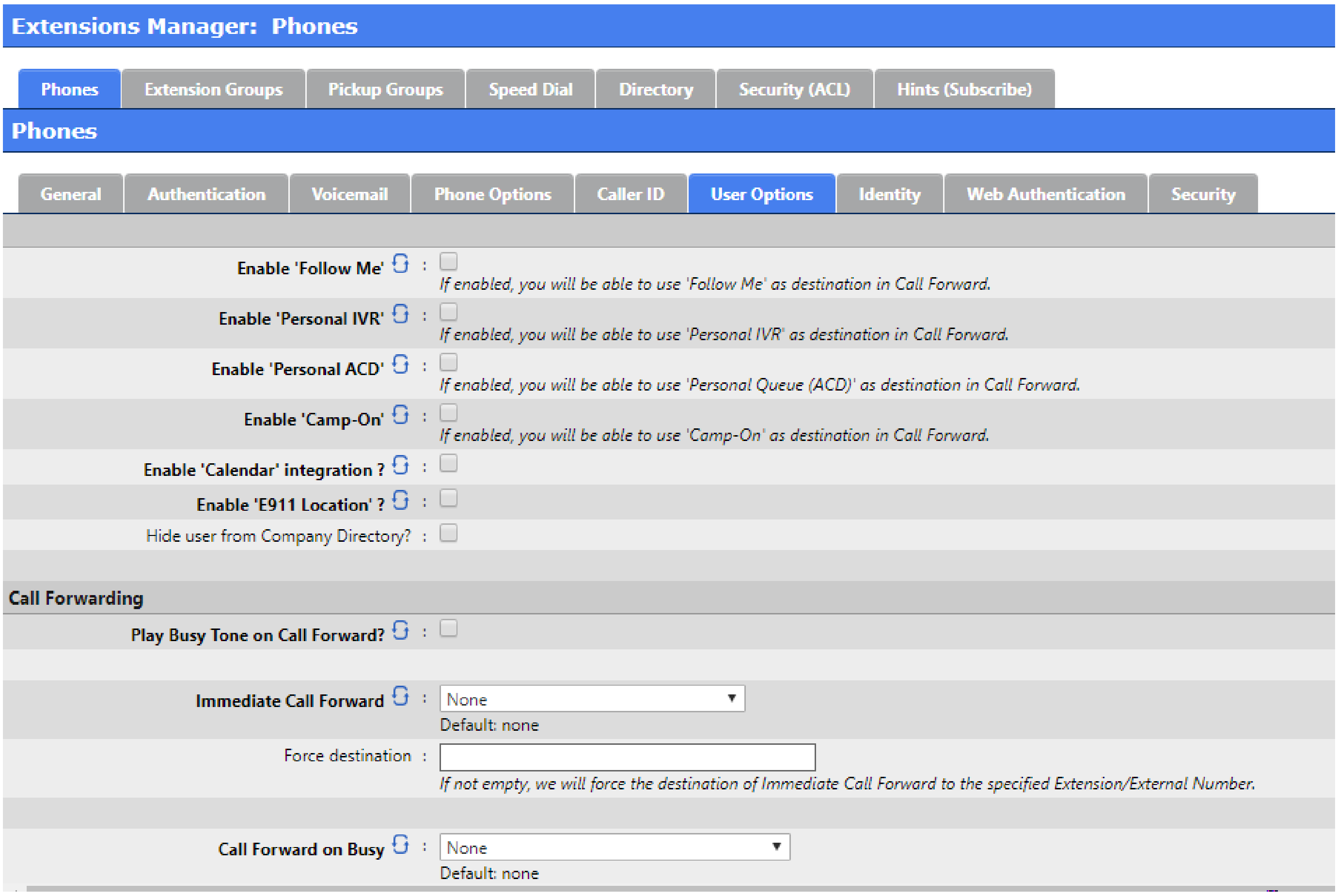
Override Outgoing CallerID for Emergency Call ? : ☑ *If the PSTN trunk allows custom CallerID then you must override default value with published phone number associated with 911 Address On Record.*

* Caller Name : Help Me Default: Tracey Phillips

* Caller Number : 5555554321 Default: 253

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



Extensions Manager: Phones

Phones

Enable 'Follow Me' : □
If enabled, you will be able to use 'Follow Me' as destination in Call Forward.

Enable 'Personal IVR' : □
If enabled, you will be able to use 'Personal IVR' as destination in Call Forward.

Enable 'Personal ACD' : □
If enabled, you will be able to use 'Personal Queue (ACD)' as destination in Call Forward.

Enable 'Camp-On' : □
If enabled, you will be able to use 'Camp-On' as destination in Call Forward.

Enable 'Calendar' integration ? : □

Enable 'E911 Location' ? : □

Hide user from Company Directory? : □

Call Forwarding

Play Busy Tone on Call Forward? : □

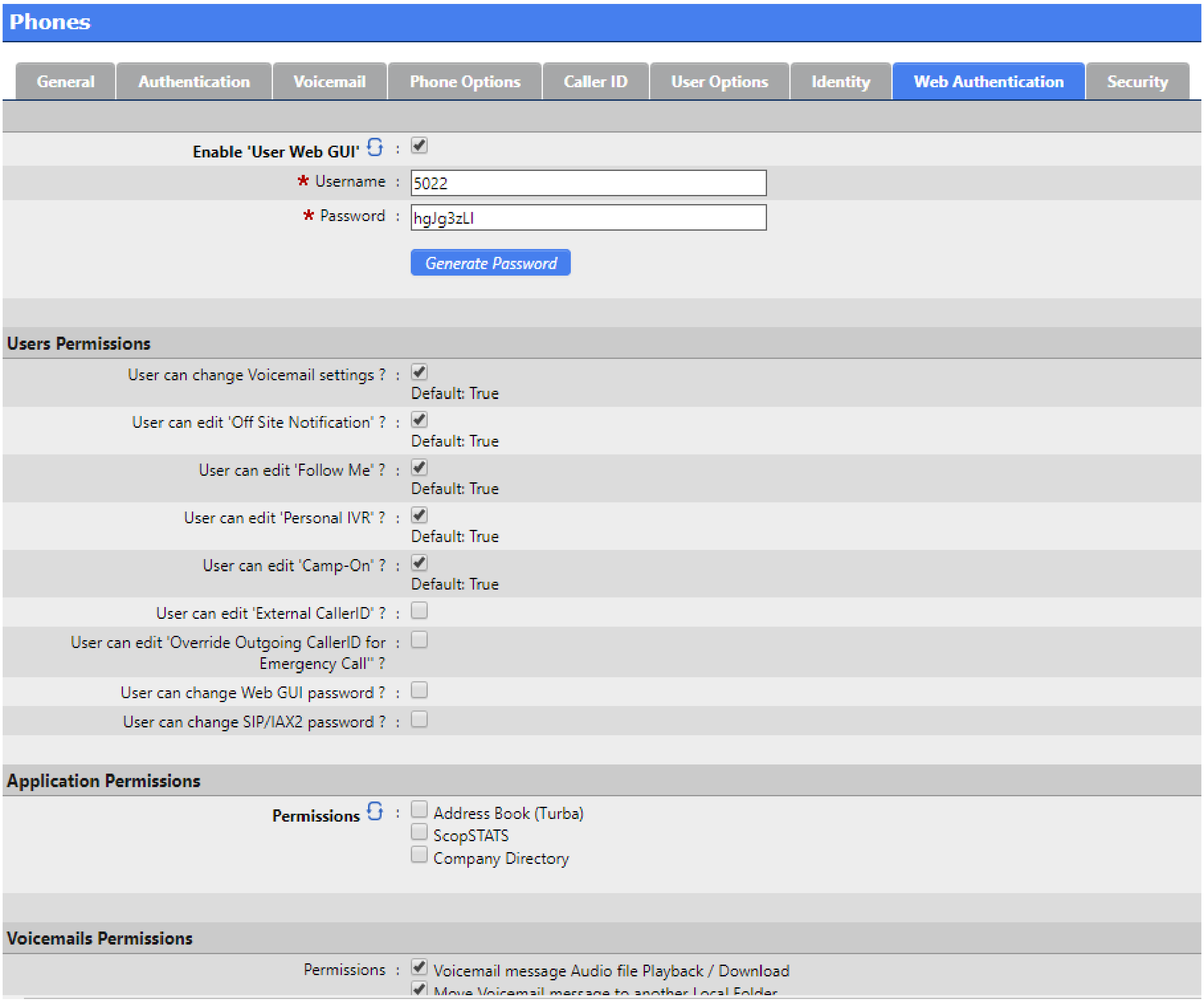
Immediate Call Forward : None ▾
Default: none

Force destination :
If not empty, we will force the destination of Immediate Call Forward to the specified Extension/External Number.

Call Forward on Busy : None ▾
Default: none

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.



Phones

Enable 'User Web GUI' : ☑

* Username : 5022

* Password : hgJg3zLI

Users Permissions

User can change Voicemail settings ? : ☑ Default: True

User can edit 'Off Site Notification' ? : ☑ Default: True

User can edit 'Follow Me' ? : ☑ Default: True

User can edit 'Personal IVR' ? : ☑ Default: True

User can edit 'Camp-On' ? : ☑ Default: True

User can edit 'External CallerID' ? : □

User can edit 'Override Outgoing CallerID for Emergency Call'' ? : □

User can change Web GUI password ? : □

User can change SIP/IAX2 password ? : □

Application Permissions

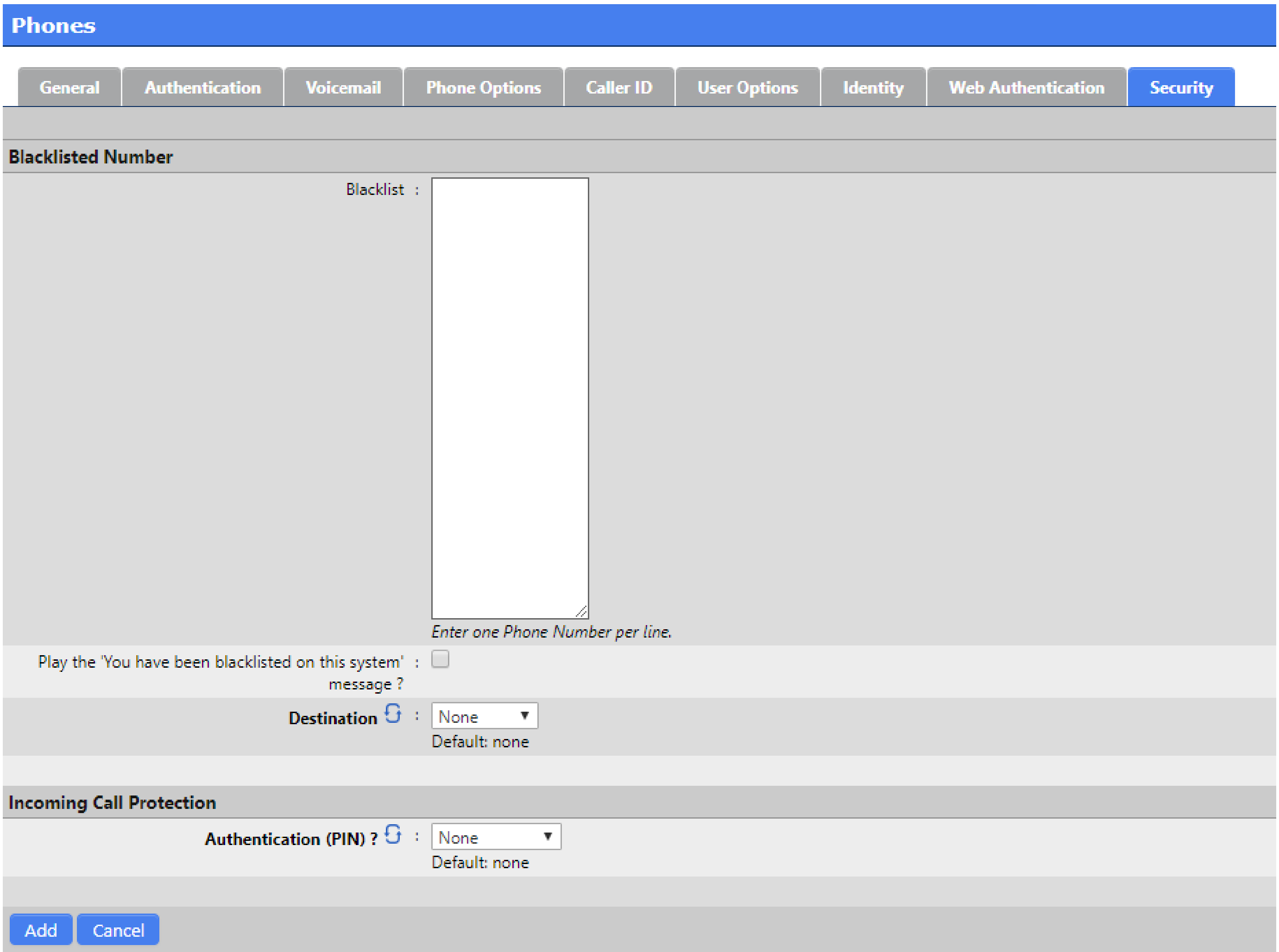
Permissions : □ Address Book (Turba)
□ ScopSTATS
□ Company Directory

Voicemails Permissions

Permissions : ☑ Voicemail message Audio file Playback / Download
☑ Move Voicemail message to another Local Folder

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.



Blacklisted Number

Blacklist :

Enter one Phone Number per line.

Play the 'You have been blacklisted on this system' message ? : □

Destination : None ▾

Default: none

Incoming Call Protection

Authentication (PIN) ? : None ▾

Default: none