

# SCOPCOMM Admin Guide

Last updated for version 1.12, updated February 17, 2021

## Contents

<b>SCOPCOMM Admin Guide</b>	<b>1</b>
Introduction	1
Licences	1
Requirements	1
Security and Encryption	2
SCOPEL Configuration	2
SCOPCOMM Configuration	3
Provisioning	4
Forcing a Provisioning Update	6
Contacts	6
Hidden Extensions	6

## Introduction

SCOPCOMM is a softphone and WebRTC solution offered by SCOPSERV International. This guide explains how to enable SCOPCOMM on SCOPEL and issue provisioning data for user devices. Unless otherwise specified, they are available at <https://download.scopserv.com/software/>.

SCOPEL offers the following SCOPCOMM clients:

- SCOPCOMM for iPhone, available on iOS App Store
- SCOPCOMM for Android, available on Android Google Play
- SCOPCOMM Desktop for Windows
- SCOPCOMM Desktop for MacOS

SCOPEL also offers the following WebRTC solutions:

- SCOPCOMM WebRTC available at <https://rtc.scopserv.com>
- SCOPCOMM WebRTC Windows
- SCOPCOMM WebRTC MacOS

## Licences

To use SCOPCOMM, you must have purchased SCOPCOMM licences. You will need a licence for each device using SCOPCOMM as softphone or WebRTC, and specify how many of each type you want. In SCOPEL you can view your number of allowed SCOPCOM under *Configuration > Server > License*. After updating your licence with you provider, do not forget to update the licence on SCOPEL by clicking the **Download** button.

## Requirements

### **Warning**

SCOPCOMM is an internet service. It requires that your SCOPEL server be reachable at a public IP address.

You must have SCOPEL installed and running with a valid licence. It is also important that in the case you have a firewall between your server and Internet access, it must not block traffic to and from certain addresses (ask your provider). Otherwise, it will not be possible to support provisioning and basic SCOPCOMM services.

If you set up Security (ACL) rules in SCOPEL, make sure you allow the following IP addresses, otherwise WebRTC users will not be able to connect to your PBX:

- 75.98.128.37
- 75.98.128.38

Your installation's firewall must allow the following ports:

- 5060 (UDP)
- 5060 (TCP), or 5061 (TLS) if you need high-level encryption
- 10000 to 20000 (UDP)

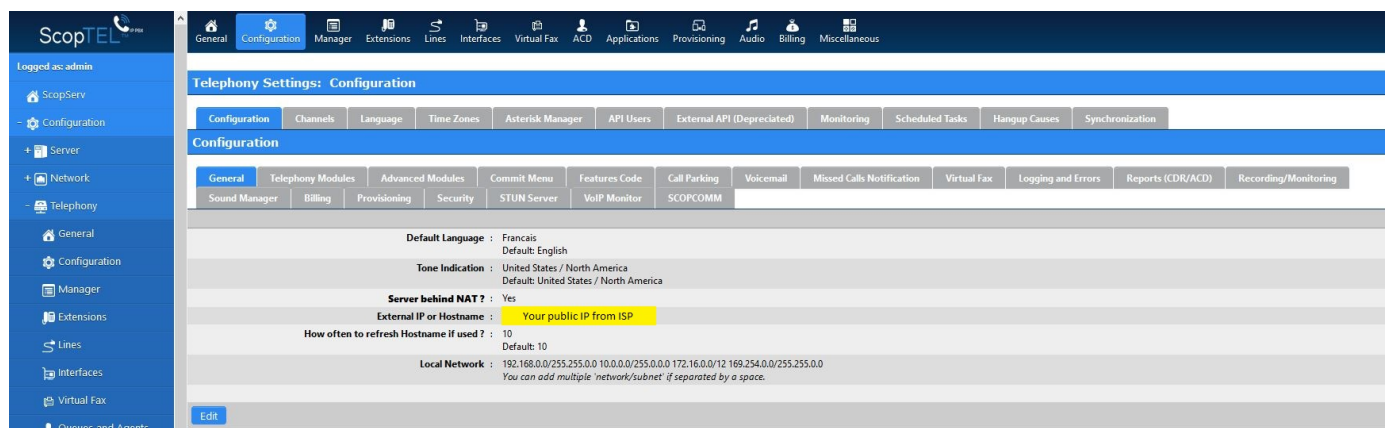
## Warning

Throughout this guide we use these values since they are the default values in SCOPEL, but if they have been set to different values, you must substitute the new port number in every place where a port must be specified.

Additionally, if your server is in a NAT (network address translation) network, you must configure the server address:

1. In SCOPEL, go to *Configuration > Telephony > Configuration > General*.
2. Make sure that the **Server behind NAT** is active.
3. Write the public IP adresse just below.
4. Press the **Commit** button.

Please note that the public IP address must be static. If this is not the case, contact your Internet service provider to obtain one. For more information on SCOPEL and NAT, please read <https://blog.scopserv.com/2016/09/how-to-use-the-scoptel-certificate-manager-to-enable-tls-encryption/>.



The screenshot shows the SCOPEL web interface. The left sidebar is blue with a navigation menu. The main content area is white with a blue header. The header contains the text 'Telephony Settings: Configuration'. Below the header is a navigation bar with tabs for 'Configuration', 'Channels', 'Language', 'Time Zones', 'Asterisk Manager', 'API Users', 'External API (Deprecated)', 'Monitoring', 'Scheduled Tasks', 'Hangup Causes', and 'Synchronization'. The 'Configuration' tab is selected. Below the navigation bar is a sub-header 'Configuration' with a row of tabs: 'General', 'Telephony Modules', 'Advanced Modules', 'Commit Menu', 'Features Code', 'Call Parking', 'Voicemail', 'Missed Calls Notification', 'Virtual Fax', 'Logging and Errors', 'Reports (CDR/ACD)', and 'Recording/Monitoring'. The 'General' tab is selected. The main content area shows the following settings:

- Default Language : Francais  
Default: English
- Tone Indication : United States / North America  
Default: United States / North America
- Server behind NAT ? : Yes
- External IP or Hostname : Your public IP from ISP
- How often to refresh Hostname if used ? : 10  
Default: 10
- Local Network : 192.168.0.0/255.255.0.0 10.0.0.0/255.0.0.0 172.16.0.0/12 169.254.0.0/255.255.0.0  
You can add multiple 'network/subnet' if separated by a space.

You can use the *yougetsignal* public utility (<https://www.yougetsignal.com/tools/open-ports/>) to check that your system is really reachable from Internet. You should test your server address with ports 5060 and 10000 to quickly check that your firewall rules are correct.

## Security and Encryption

For security purposes, we encourage you to use SSL certificates on your SCOPEL installation. To set this up, please refer to this document: <https://blog.scopserv.com/2016/09/how-to-use-the-scoptel-certificate-manager-to-enable-tls-encryption/>.

## SCOPEL Configuration

SCOPEL must be configured to allow SIP on TCP:

1. In SCOPEL, go to *Configuration > Telephony > Configuration > Channels > SIP Channel*.

2. Make sure that the **Enable Support for SIP TCP** option is active and in the **TCP Port** write *5060* (or your TCP or TLS port setting).

The screenshot shows the Scoptel web interface. The left sidebar contains navigation options: Home, Configuration, Server, Network, Telephony, General, Configuration, Manager, Extensions, Lines, Interfaces, Virtual Fax, Queues and Agents, Applications, Provisioning, Audio, Billing, Miscellaneous, and Import/Export. The main content area is titled 'Telephony Settings: Channels' and has sub-tabs for Configuration, Channels, Language, Time Zones, Asterisk Manager, API Users, External API (Deprecated), Monitoring, Scheduled Tasks, Hangup Causes, and Synchronization. Under the 'Channels' tab, there are sub-tabs for General, RTP Options, Codecs, SIP Channel, IAX Channel, Jitter Buffer, and Guest Account. The 'SIP Channel' sub-tab is active, showing the following configuration:

- Port (UDP) : 5060 (Default: 5060)
- Bind Address (UDP) :
- Enable support for SIP TCP ? : Yes
- Port (TCP) : 5060 (Default: 5060)
- Bind Address (TCP) :
- Enable support for SIP TLS (secure) ? : No
- Enable Outbound Proxy support ? : No (When enabled, the server will send outbound signalling to the specified server, not directly to devices.)

Below these are 'SIP Options':

- Realm for Digest Authentication : scopserv (Default: scopserv)
- User Agent : Asterisk-PBX (ScopServ) (Default: Asterisk-PBX (ScopServ))
- Record SIP History : No
- Auto-create Peers : No
- Enable RTP Auto Framing ? : No (If set, then all calls will try to set the packetization based on the remote endpoint's preferences.)
- Enable DNS SRV lookups on outbound calls : Yes (Default: True)

3. Click **Commit**.
4. Got to *Configuration > Network > Firewall > Advanced Rules*.
5. Find and edit entry **VoIP (SIP/IAX/MGCP)** and add this rule: *5060/tcp* (substitute your TCP or TLS port setting).
6. Click **Commit**.
7. Go to *Configuration > Network*.
8. Click **Restart Service**.

## SCOPCOMM Configuration

You must configure a SCOPCOMM admin e-mail and select the notification destination. This e-mail will be used to issue provisioning information necessary.

If the public address/domain or ports of your network are not the same as that of your installation, this is where you must specify them. For example, if you use a firewall or SBC that has different values, this is where you must specify it. This address and port are the ones visible to devices on the public network.

1. In SCOPTEL, go to *Configuration > Telephony > Configuration > SCOPCOMM*.
2. Click **Edit**.
3. Write the public IP address or domain of your installation.
4. Set an administrator e-mail.

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

## Telephony Settings: Configuration

Configuration	Channels	Language	Time Zones	API Users	Monitoring	Scheduled Tasks	Hangup Causes	Synchronization
<b>Configuration</b>								
General	Telephony Modules	Advanced Modules	Commit Menu	Features Code	Call Parking	Voicemail	Missed Calls Notification	
Provisioning	Security	STUN Server	VoIP Monitor	ScopCOMM				
* Server IP or Hostname : <input type="text" value="10.10.10.10"/>								
* Provisioning email sent to : <input type="text" value="Administrator"/> <small>In case End User is chosen, be sure every end user has an email in Identity tab</small>								
* Administrator Email : <input type="text" value="service@scopserv.com"/>								
Save	Reset to Default	Cancel						

5. Select a destination for provisioning e-mails. The options are:

- Administrator: the admin e-mail configured on this page is the only recipient of provisioning info.
- End user: end users will get the provisioning e-mail at the address configured under their profile.
- Both

6. If your public ports are not the same as your installation's ports, first click "Specify custom public ports" and type in the ports for each protocol (UDP, TCP, TLS).

7. Click **Save**.

## Provisioning

To generate provisioning information for devices using SCOPCOMM:

1. In SCOPTEL, go under *Configuration > Telephony > Extensions*.
2. If you want to add a SCOPCOMM account to an existing extension, click the edit button next to the extension of your choice and go to step 4.
3. To create a new extension with SCOPCOMM, click **Add a new phone**. Under the **General** tab, select the tenant (if you are in a multi-tenant site).
4. Under the **General** tab, select phone type *SIP* and click **Add/Save**.
5. Under the **Authentication** tab, type a username and password.
6. If you want to enable SCOPCOMM for multiple devices or for a device other than the main one, check **Enable Shared SIP support ?**. This will automatically add another SIP device. You can have up to three devices per extension.

7. For each device select if you want activate SCOPCOMM for softphone, desktop, or WebRTC. You may also choose to not activate SCOPCOMM for that device. Just below is indicated the number of each type you have left.

8. Under the **Phone Options** tab, set the following:

- **Transport Mode:** *UDP* and *TCP* (or *TLS* is you have SSL security set up on your system)
- **Phone behind NAT:** selected if you are in a NAT network
- **Codec:** *H.264 Video*

9. Under the **Identity** tab, write the user e-mail. This is where the provisioning e-mails will be sent to.

10. Click **Save**.

11. Click **Send to SCOPCOMM**. A pop-up will display success or errors.

12. If any username, password, or number of shared device has changed, you will also need to click **Commit** to save changes on SCOPEL.

Following this, provisioning e-mails will be sent as per your configurations: each user will receive a provisioning e-mail with their credentials, or the admin may receive these e-mails. E-mails are resent following any update in SCOPTEL, assuming you clicked **Send to SCOPCOMM**.

Be advised that each device will require a licence, so if user has three shared devices and uses SCOPCOMM on two of them, two licences will be used.

## ***Forcing a Provisioning Update***

If a user failed to get their provisioning information, or if for some other reason you need to resend a user's provisioning information:

1. In SCOPTEL, go under *Configuration > Telephony > Extensions*.
2. Click the *edit* button for the extension.
3. Under the **Authentication** tab, click **Resend**.

## **Contacts**

During provisioning, SCOPCOMM also downloads the company directory from SCOPTEL and displays in **Contacts**. If you need to update the SCOPCOMM contact list, you can click **Send to SCOPCOMM** to update the company directory for SCOPCOMM users.

## ***Hidden Extensions***

SCOPTEL can hide extensions from being shared in a company phone directory. This functionality also applies to SCOPCOMM. To hide an extension:

1. In SCOPTEL, go to *Configuration > Telephony > Extensions*.
2. Select an extension to edit.
3. Go under **User Options** tab.
4. Turn on **Hide user from Company Directory?**.