IP Desktop Softphone

For Alcatel-Lucent Communication Servers

Version – IPDSP 13.X for Windows
IPDSP 11.X for MacOS

Installation and configuration manual

Alcatel·Lucent Enterprise

Table of Contents

1. Legal notice

2. Document History

Edition	Date	Changes / Comments / Details
1.0	2014-2-11	Creation – Merge all installation guides
2.0	2015-5-19	OXO Compliance for Windows and Mac OS environment
3.0	2018-11-15	Legal disclaimer, end of support for Windows 8
4.0	2018-12-17	Update for version IPDSP 11.1.21
5.0	2019-01-09	Overall review
6.0	2019-03-01	Update for version IPDSP 11.1.27
7.0	2019-03-28	Update for version IPDSP 11.2.0 Add section limitation/advertisement
8.0	2019-04-26	Update for version 11.2.0 Native encryption
9.0	2019-12-12	Update for version IPDSP 11.3.0 - Installation in command line mode - Installation in graphic mode - application monitoring - new theme: Slate Design
10.0	2020-01-08	Update for version 11.3.1 - Masking external call number
11.0	2020-04-15	Update for version 11.4.1 - Add limitations for roaming and offload - Update range of UDP ports for PCX record.
13.0	2020-11-27	Update for version 11.5.2 - Information relative to SRTP options allowed for the FSNE mode
14.0	2021-01-05	Add VPN details and restrictions. MSI option MODEPROACD is replaced by SHAREDNUMBER mode
15.0	2021-03-09	Some IP Desktop Softphone screen messages description
16.0	2021-06-15	VID environment: add new section for VDI
17.0	2021-09-20	- Add trouble shooting to avoid echo in audio using jabra headset - Use silent mode for command line installation - Change for user type: IPTouch 8068s
18.0	2021-11-29	- HTTPS as alternative to TFTP for lanpbx.cfg retrieval
19.0	2022-01-14	Added a limitation in "Troubleshooting": identical headsets on MacOs
20.0	2022-04-14	New IP Desktop Softphone GUI
21.0	2022-05-24	New features: Keyboard shortcuts and Themes
22.0	2022-08-11	TFTP2 remark.
23.0	2022-09-12	Accessibility improvement
24.0	2022-10-17	“Installing certificate in Windows Store” update
25.0	2023-04-06	Ringtone parameters in Audio settings New settings interface Add INTERFACE_DISPLAY msi installation flag
26.0	2023-05-16	Automatic update
27.0	2023-11-16	Automatic update (add details)
28.0	2023-12-14	Headset HID
29.0	2024-01-08	REST API

30.0	2024-01-30	CRM Integration
31.0	2024-03-27	Connector for Teams
32.0	2024-07-15	Add Notes for installation using PowerShell, HID and new Outlook.
33.0	2024-09-19	Enable/disable headset control
34.0	2024-11-05	ConfigFolder updated after repair. Adding RINGTONE_SOUND_OVER setup parameter to enable audio device selection for ringtone.
35.0	2025-02-07	Change the name of the document. Possible combinations of keys on the additional keyboard.
36.0	14-03-2025	Native encryption: Mutual authentication
37.0	23-05-2025	Adding ALE-300 emulation type

3. Terminology

Acronym	Signification
OXE	OmniPCX Enterprise Communication Server
OXO	OXO Connect or OXO Connect Evolution Communication Server
IPDSP	IP Desktop Softphone
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
RTP	Real Time Protocol
RTCP	Real Time Control Protocol
UA	Universal Alcatel
GD	Gateway Driver
GA	Gateway Appliance
VPN	Virtual Private Networking
MDM	Mobile Device Management
AOM	Add-On Module
ToS	Type Of Service (Windows)
QOS	Quality Of Service
CA	Certificate Authority
CTL	Certificate Trust List
TLS	Transport Layer Security

DTLS	Datagram Transport Layer Security
MTLS	Mutual TLS authentication
REST	Representational State Transfer
FNSE	Full Native Software Encryption
NAT	Network Address Translation
PAT	Port Address Translation
VDI	Virtual Desktop Infrastructure
VVX	Virtual Voice eXtension
HID	Human Interface Device
CRM	Customer Relationship Management

4. Introduction

4.1 Purpose of the document

This document presents:

- The required hardware and software environment for the installation of the application
- A description of the application's installation,
- The configuration of the application.

4.2 Audience

This guide is intended for the administrator in charge of the company's telephony.

4.3 Application scope

This guide includes installation and administration of the IP Desktop Softphone application for Windows, MAC OS, and Android.

4.4 Customer Support

Please contact your system administrator or Alcatel-Lucent Enterprise Business Partner for support

4.5 Features: Limitations & Advertisement

IPDSP is an emulation of 8068x terminals. However, it is important to mention that it does not provide same levels of functionality.
New features are developed depending on IPDSP roadmap based on relevancy of use cases.

Following features are not available for all IPDSP platforms.

	Windows	MacOS	Android
REDIRECT	X	X	
ACD Mode (call centre agent feature OXE/OXO) This mode requires extra licence on communication server.	X	X	X
IPDSP Shared Number Mode This mode does not require any extra license.	X		
Desk Sharing DSS/DSU	X	X	X
OXE/OXO redundancy support	X	X	X
PCS mode	X		
NATIVE ENCRYPTION	From IPDSP 11.2.0 and OXE 12.3		
SET REASSIGNMENT	X		
AUDIO SETTINGS - Advanced - Default configuration - Volume Fine tuning	X X X X	X X	

- Custom ring tone	X	X	
INSTALLER FULL OPTIONS	X		
MULTI-LANGUAGES (GUI)	X		
TELURL	X		
SEND My LOGS			X
IPDSP_Collect	X		
WIFI-MESSAGE ALERTS			X
STOP RINGING BUTTON	X	X	
HEADSETS REMOTE CALL CONTROL	X	X (Sennheiser not supported)	
AUTO STARTUP	X		
MULTI-SESSION	X IPDSP will be stopped from session A if session B launched a new IPDSP instance. IPDSP will not be relaunched automatically when switching user session even if auto_startup is set.	X IPDSP is automatically stopped when user session ends.	N/A
Add-On module	X OXE: 10/14/20 keys Up to 3 AOM OXO: 14 keys Limited to 1 AOM	X 14 keys Limited to 1 AOM	X 14 keys Limited to 1 AOM
Accessibility option	X		
SHOW APPLICATION OPTIONS	X		
NETWORK ADAPATER SELECTION	X		
LOCK MENU WITH PASSWORD	X		
RECORDING	X	X	X
Phone identifier (EFA)	X		
URGENT CALL POPUP	X	X	
TOASTER OPTIONS	X	X	
LONG KEY PRESS	X		
ROAMING ETH/WIFI	X ETH/WIFI Automatic restart of application	X ETH/WIFI Automatic restart of application	N/A
OFFLOAD WIFI / 4G	N/A	N/A	Not supported Initial connection mode (Wi-Fi or 4G) must be kept. Set device out of service before changing network to reset connection mode.

5. Windows Environment

This part of the document describes the Windows installations procedures.

5.1 Installation prerequisites

The minimum requirements without which the application cannot function correctly are described below

5.1.1 Hardware

Processor	2 GHz Minimum
RAM	2 GB for Windows
Disk space	80 MB free space
Sound card	Integrated sound card or USB headset

Note:
The above table lists the minimum hardware requirement. With additional hardware, it is possible to establish many types of connections, some of which are discussed in the IP desktop Softphone in different environments.

5.1.2 Operating system

Please refer to the MLE_CrossCompatibility compatibility matrix. Contact your partner.

5.1.3 VPN

The IP Desktop Softphone application requires a direct IP connection with the communication server. If it is used outside the company's LAN, installing a VPN connection may be necessary.

To make IPDSP work, the VPN will have to allow exchanges on all ports listed in sections 5.1.7 to 5.1.9, taking into account the OXE or OXO context.

Caution:
- IPDSP is not compatible with VPNs implementing address (NAT) or port (PAT) translation.

- Any IPDSP version prior to 11.4.2 is not compatible and should not be deployed in a VPN context.

5.1.4 .NET Framework

The IP Desktop Softphone application requires Microsoft .NET Framework 4.6.2.

5.1.5 Visual Studio 2010 Tools for Office Runtime

If the Outlook Add-In is to be installed, please make sure that Visual Studio 2010 Tools for Office Runtime is installed, it is required to run Microsoft Office based solutions built using Microsoft Visual Studio. It is available for download under: https://www.microsoft.com/en-in/download/details.aspx?id=48217.

5.1.6 Pimphony

When the IP Desktop Softphone application is used on a PC, it is forbidden to install and use PIMphony IP Multimedia. To install an IP Desktop Softphone on a PC, PIMphony IP Multimedia, if present on this PC, must be uninstalled first.

5.1.7 UDP ports used (OXE context)

The table below lists the ports that this application uses:

Purpose	Protocol	Device 1	Device 1 port	Device 2	Device 2 port
Phone configuration (file download for configuration data)	TFTP	Softphone	(49152-65535)/udp for Windows (1024-65535)/udp for macOS,iOS and Android	TFTP Server (CS MAIN)	69/udp 10000 to 10499/udp
Outgoing flow	RTP/RTCP	Softphone	32512 to 32515/udp	GD, GA, INT_IP A+B	32512 to 33023/udp
Incoming flow	RTP/RTCP	GD, GA, INT_IP A+B	32512 to 33023/udp	Softphone	32512 to 32515/udp
Incoming flow	RTP/RTCP	Softphone	32512 to 32515/udp	IP Touch	32512 to 32515/udp
Outgoing flow	RTP/RTCP	IP Touch	32512 to 32515/udp	Softphone	32512 to 32515/udp
Incoming flow	RTP/RTCP	Softphone	32512 to 32515/udp	Softphone	32512 to 32515/udp
Outgoing flow	RTP/RTCP	Softphone	32512 to 32515/udp	Softphone	32512 to 32515/udp
Outgoing Signaling flow	UA	Softphone	32512 to 32515/udp	CS (two Physicals)	32640 to 32643/udp
Incoming Signaling flow	UA	CS (two Physicals)	32640 to 32643/udp	Softphone	32512 to 32515/udp
Outgoing flow	RTP/RTCP	Softphone	32516 to 32518/udp	PCX Record	Refer to recorder documentation For Omni-PCX Record: 2000 to 2240/udp (startingPort + 3* number of extensions to record declared) startingPort: 2000 default max umber of records: 80

Incoming flow	RTP/RTCP	Softphone	32512 to 32515/udp	OTMS	28 000 to 39 999/udp
Outgoing flow	RTP/RTCP	OTMS	28 000 to 39 999/udp	Softphone	32512 to 32515/udp

5.1.8 TCP used ports (OXE context)

Purpose	Protocol	Device 1	Device 1 port	Device 2	Device 2 port
Set Reassignment	CMISE	Softphone	2535		

5.1.9 UDP used ports (OXO context)

Purpose	Protocol	Device 1	Device 1 port	Device 2	Device 2 port
Phone configuration (file download for configuration data)	TFTP	Softphone	0-65535/udp for Windows, IOS and Android 1024-65535/udp for macOS	TFTP Server	69/udp 10000-10499/udp
Outgoing flow	RTP	Softphone	32000:32512/udp	GD, GA, INT_IP A+B	32000:32512/udp
Signaling flow	UA	Softphone	7775/udp	GD, GA, INT_IP A+B	5000-5099/udp

5.1.10 Https ports used

Purpose	Protocol	Initiator	Responder	Service port	Authentication
Https Port	HTTPS	IPDSP Update service	Msi server	443	No

This port should be opened to use automatic update feature.

5.1.11 Internal ports used

For information, some components inside the IP Desktop Softphone application communicate between each other locally on a locally internal network. The local network is only used by the containers and all the ports described below are NOT accessible from the outside.
Consequently, none of the ports listed below need to be opened.

Purpose	Protocol	Initiator	Responder	Service port	Authentication
REST Port	HTTPS	Tel protocol, Outlook Addin …	IPDSP	8097	No
VDI Port	HTTPS	IPDSP	VVX module	1443	No
VDI Port	HTTPS	VVX module	VVX service (monitoring)	1444	No
IPDSP Agent Port	HTTPS	IPDSP Agent	IPDSP Update service	1462	No

5.1.12 Networking

Network Interface card	Ethernet card or Wireless LAN

Notes:

- *IPDSP is not compatible with the 802.1Q standard. It supports only TOS*
- *IPDSP supports PBX native encryption. Please refer to chapter 5.3 for more details.*

5.2 Installation and upgrade procedures

Notice that this procedure is valid for both installation and upgrade of the application.

5.2.1 Installation Modes

The installation is done using the MSI file IPDesktopSoftphone_13.X.YY.msi.

You can install this application on two different modes which are:

- Graphic mode by double clicking on the MSI file
- Command line mode from a console.
  The command line mode provides access to a list of installation options.

It is recommended to do installation with one of these two methods so either with command line in silent mode(/qn) or using GUI.

5.2.2 User profile

During the installation, the user profile must be chosen. Two profiles are available:

- Individual Number Mode
- Shared Number Mode (only available in OXE context) This mode is not related to call center. It is a mode local to the computer and IPDSP and does not require any additional Agent nor CCD licenses specific to call center.

Once installed, it is possible to change the existing profile from the settings window. (see Settings: Advanced tab)

Individual Number Mode	Shared Number Mode
One phone number per user = one license per user	One phone number per PC = one license per PC
Users can have their own IP Desktop Softphone application	Users can use the same IP Desktop Softphone application without buying additional licenses
Choosing Individual Number Mode will link the *Softphone ID* to the user (one ID per user account).	Choosing Shared Number Mode will link the *Softphone ID* to the PC (one ID only per PC).
ID & Config data are stored in the USER account	ID & Config data stored for ALL USERS

Limitations:

1. It will not be possible to run two instances of the IP Desktop Softphone application on the same PC at the same time.
2. If you are using Softphone in Shared Number Mode, business users will not be able to have their own phone.

5.2.3 Installation in command line mode

From the command prompt, it is possible to install or update the IPDSP:

```
msiexec /i IPDesktopSoftphone_13.X.YY.msi
       PBXADDR=<server address> BACKUPPBXADDR=<backup server address>
       SHAREDNUMBERMODE=<number> LANGUAGE=<number>
       USEPASSWORD=<number> PASSWORD=<password> SCOPE=<value>
       AUTOSTARTUP=<number>
       SHOWTOASTER=<number> SHOWTASKBAR=<number>
       AUTOMATICHEADSET=<number>
       TRUNKSEIZE=<number> PREFIXINTERNATIONAL=<number>
       PREFIXNATIONAL=<number>
       COUNTRYCODE=<string> MINDIGITS=<number>
       INSTALLDIR=<directory> CONFIGFOLDER=<path>
       SETREASSIGNMENT=<number>
       DEFAULT_DEVICE_MICROPHONE=<name> DEFAULT_DEVICE_SPEAKER=<name>
       SECONDARY_DEVICE_MICROPHONE=<name>
       SECONDARY_DEVICE_SPEAKER=<name> RING_DEVICE_NAME=<name>
       DEACTIVATE_POPUP_URGENT_CALL=<value>
       USE_SYSTEM_VOLUME=<number>
       REDIRECT_FOR_ALLUSERS=<number>
       ADDMBRTOMAC=<value>
       MAC_ID=<value>
       OUTLOOKADDIN=<number>
       MASK_EXTERNAL_CALL_NUMBER=<number>
       REST_SERVER_PORT=<number>
       SUPERVISION=<number>
       RINGING_CADENCE=<value>
       CREATE_DESKTOP_SHORTCUT=<value>
       HTTPS_TFTP_ORDER=<value>
       HTTPS_PORT=<value>
       LANPBX_REMOTE_PATH=<value> INTERFACE_DISPLAY=<value>
       HTTPS_OVERRIDE_HOSTNAME_CHECK=<value> LOCATION_SERVER=<value>
       UPGRADEURL=<value> NO_CERT_CHECK=<value>
       THEME=<value> HEADSET_HID=<number>
       USE_TEAMS_CONNECTOR=<value> RINGTONE_SOUND_OVER=<value>
       DTLS_PKEY_PASSWORD=<value> DTLS_CERT_NAME=<value>
       EMULATION_TYPE=<value>     /qn
```

The command line above displays all the options available.
You don't need to set all the options of the full command given.
Option not explicitly set will be set with the default value.

Component	Description
msiexec	Microsoft command to execute file with 'msi' extension
/i	Optional setting for Status Messages. For more of such options, you can key in the following at command prompt: msiexec /i
IPDesktopSoftphone_13.0.0.msi	Name of file that is to be executed.

Component	Description
PBXADDR=<server address>	IP address or host name of the communication server
BACKUPPBXADDR=<backup server address>	Command indicating that the information following this command is the address of backup PBX server
SHAREDNUMBERMODE=<number> **This parameter replaces the MODEPROACD option which is no longer supported.**	Command indicating that the information following this command is the chosen mode (Individual Number Mode or Shared Number Mode) Possible values: 0 for Individual Number Mode 1 for Shared Number Mode **This parameter must be used carefully with VDI_MODE=1, because, if set to 1, will associate to all VDI users the same extension number**
LANGUAGE =<number>	Command that indicates the language of the application interface. This language will be used in all the interface tabs. Give any of the following integers here. The numbers and their related languages are listed below: 4 – English Generic Alcatel 5 – French 6 – Italian 11 – German 12 – Portuguese 15 – Spanish 18 – Norwegian 22 – Finnish 29 – Dutch 24 – Russian 40 – Chinese 42 – Korean Default – 4: Generic Alcatel English
USEPASSWORD <number>	Indicates whether access to the “Network” and “Call” configuration is password-secured • 0 not secured by password (default value) • 1 access is secure
PASSWORD <password>	Password value (<password> should not be empty, if PASSWORD is not set and USEPASSWORD=1, default value: letacla)

Component	Description
SCOPE <value>	Sets the password protected area. The possible values are: • NET-ADV to protect the Network and Advanced menus. • ALL to protect all menus. If the SCOPE setting is not specified, the default value is NET-ADV
AUTOSTARTUP <number>	Allows the automatic startup of the application at each user login The possible values are: • 0 not enabled (default value) • 1 enabled
SHOWTOASTER <number>	Allows a toaster to be displayed at each incoming call The possible values are: • 0 not enabled • 1 enabled (default value)
SHOWTASKBAR <number>	Allows you to display the application icon in the taskbar The possible values are: • 0 not enabled • 1 enabled (default value)
AUTOMATICHEADSET <number>	Automatic device detection and activation of audio devices. The possible values are: • 0 on demand (default value) • 1 always • 2 never
TRUNKSEIZE	Prefix to make external call. The default value is 0
PREFIXINTERNATIONAL	International call prefix. The default value is 00
PREFIXNATIONAL	First digit used in the country for national calls (06 12 34 56 78). Default value is 0
COUNTRYCODE	The international dialing code of the country. Default value: “France 33”. For all possible values, see for example: https://countrycode.org
MINDIGITS	Minimum number of digits: default value: "9" Any phone number whose number of digits is greater than or equal to the value of this setting will be interpreted as an external number (the professional trunk seize prefix will be added before dialing)

Component	Description
INSTALLDIR <directory>	Specify the installation directory. (Optional) The default value is: C:\Program Files (x86)\Alcatel-Lucent Enterprise\IP Desktop Softphone
CONFIGFOLDER <path>	indicates the path of the configuration files: <username>__MyPhoneIPDesktop.ini, <username>_lanpbx.cfg and <username>_shortCutKeys.cfg. If specified, the chosen path must be writable for all users. **NB: If this parameter was used in installation with specific path, it must be provided also in repair mode (/famv) to keep the same configuration folder. Otherwise, default path will be used.**
SETREASSIGNMENT <number>	Enable the "Set Reassignment" functionality. The possible values are: • 0 not enabled (default value) • 1 enabled
DEFAULT_DEVICE_MICROPHONE <name>	Sets the name of the primary input audio device (mic)
DEFAULT_DEVICE_SPEAKER <name>	Sets the name of the primary output audio device (speaker)
SECONDARY_DEVICE_MICROPHONE <name>	Sets the name of the secondary input audio device (mic)
SECONDARY_DEVICE_SPEAKER <name>	Sets the name of the secondary output audio device (speaker)
RING_DEVICE_NAME <name>	Sets the name of the secondary ringing device
DEACTIVATE_POPUP_URGENT_CALL <value>	Allows activation for launching the popup that tell the user to use a landline or mobile phone in case of emergency call. • 0 enabled (default value) • 1 not enabled
USE_SYSTEM_VOLUME <number>	Allows to use the system volume for the used audio devices, otherwise the application will use its configured volume. • 0 application volume used • 1 system volume used (default value)
REDIRECT_FOR_ALLUSERS <number>	Assign Windows users the same TFTP addresses if a user receives a REDIRECT. This option is only enabled if the PROACD mode is used. Possible values: 0 or 1. Default value: 0
ADDMBRTOMAC <value>	Allows to modify the ID (MAC address sent to PBX as phone identifier) with system specific data. Default value is "1". **Important**: This parameter must be set to 0 in case of use of backuprestoreid.exe script used to import IP Desktop Softphone identifier from PC to another

Component	Description
MAC_ID <value>	Sets the phone ID (MAC address) used to identify IP Desktop Softphone in PBX side. If present, the value must be a valid MAC address (xx:xx:xx:xx:xx:xx) separated with ":" character . The value will be set depending on the Shared Number mode used. If SHAREDNUMBERMODE is 1, then the MAC_ID will be set for all Windows users. If not, it will be set for current user that is launching installation (Individual Number Mode). **NB: When this option is present, it must be used with the option ADDMBRTOMAC=0** **This parameter must be used carefully with VDI_MODE=1, because it will associate to all VDI users the same extension number**
OUTLOOKADDIN <number>	If set to 1, the IP Desktop Softphone Add-In for outlook will be installed. In case the add-in is not to be installed, this option should not be present in the parameters. *NB*: Please make sure that Visual Studio 2010 Tools for Office Runtime is installed before using this option, it is required to run Microsoft Office based solutions built using Microsoft Visual Studio. It is available for download under: https://www.microsoft.com/en-in/download/details.aspx?id=48217 ⚠ IP Desktop Softphone Outlook add-in is not supported in the New Outlook as new version of Outlook that does not support VSTO add-ins.
MASK_EXTERNAL_CALL_NUMBER <number>	Used to hide the call number, an "External Call" string will be displayed instead of the number on the screen as well as all of the application's menus. • 0 not enabled (default value) • 1 enabled
REST_SERVER_PORT <number>	Port number for IP Desktop Softphone REST server. Default value is 8097
SUPERVISION <number>	Activate/Deactivate IP Desktop Softphone application monitoring (see Chapter 5.4.1) • 0 not enabled • 1 enabled (default value)
RINGING_CADENCE <value>	Activate/Deactivate cadence for Ringing • 0 not activated (default value) • 1 activated
CREATE_DESKTOP_SHORTCUT <value>	Allows to create or not the application desktop shortcut, if set to 0 it will not be created otherwise it is created.

Component	Description
	• 0 not created • 1 created (default value)
HTTPS_TFTP_ORDER <value>	Order of HTTPS/TFTP protocols to retrieve lanpbx.cfg file from PBX. Four possible values are available: • 0: TFTP only (default value) • 1: HTTPS only • 2: TFTP then HTTPS • 3: HTTPS then TFTP
HTTPS_PORT <value>	PBX HTTPS port in case of use of HTTPS protocol (used when HTTPS_TFTP_ORDER is set to values 1 or 2 or 3) Default value: 443
LANPBX_REMOTE_PATH <value>	Path of lanpbx.cfg file at PBX side. Default value: /DM/VHE8082/lanpbx.cfg
HTTPS_OVERRIDE_HOSTNAME_CHECK <value>	Bypass the hostname check in HTTPS certificate CN/SAN fields • 0: No bypassing • 1: Bypassing (default value)
LOCATION_SERVER <value>	URL of the VNA server.
INTERFACE_DISPLAY=<value>	Display mode of the application for the user The possible values are: • 0 never ==> the application will not be displayed • 1 on demand ==> the application will be displayed (default value) • 2 always ==> the application will always be displayed in the foreground and topmost.
UPGRADEURL =<value>	If not empty, this field is used to activate IP Desktop Softphone automatic update via https, please refer to chapter (5.11) for more details.
NO_CERT_CHECK =<value>	Set to 1 to bypass certificate check of https requests of automatic update. Default value: 0 please refer to chapter (5.11) for more details
THEME=<value>	Set the theme of the application for the user The possible values are: • 0 ==> DARK mode (default value) • 1 ==> LIGHT mode

Component	Description
HEADSET_HID=<number>	Activate/deactivates the use of HID for on-hook / off-hook and mute / unmute functions from the headset. default value is 0 (not activated) The possible values are: • 0 ==> not activated (default value) • 1 ==> activated for all devices (JABRA, EPOS and POLY) • 2 ==> activated only for JABRA • 3 ==> activated only for EPOS (Sennheiser) • 4 ==> activated only for POLY (Plantronics)  This parameter is used only during the first installation, once the user changes it in audio settings interface, it will have no effect for the next installation/upgrade and repair(/famv), IP Desktop Softphone use the value saved in the current user registry key after.
USE_TEAMS_CONNECTOR=<number>	Indicates whether the application will be used in the Teams context in minimal display (GUI is hidden and without numeric keypad and additional keyboard) • 0 not activated (default value) • 1 activated.
RINGTONE_SOUND_OVER=<value>	Activate or not the choice for the user to choose the ringing tone device. The possible values are: • 0 ==> the user must choose the ringing device in the checkbox "Ringing on incoming call" present in each section of the primary/secondary device (default value) • 1 ==> the user has the choice between a checkbox to select or not the primary device and a list box to choose a second device among the speakers other than that of the primary device.
DTLS_PKEY_PASSWORD=<value>	String value to specify a password. Used in case Mutual Authentication is activated for DTLS handshake (Native encryption) and the certificate private key is installed using a file and protected by a password. Default value: “”
DTLS_CERT_NAME=<value>	String value to specify the CN field of the certificate. Used in case Mutual Authentication is activated for DTLS handshake (Native Encryption) and the certificate is installed in Windows Certificates Store. This parameter must specify the Common Name (CN) field of the certificate. Default value: “”

Component	Description
EMULATION_TYPE=<value>	Sets the ALE phone emulation type The possible values are: • 0 ==> 8068s emulation (default value) • 1 ==> ALE-300 emulation **NB: Please make sure the value is the same as the set type in PABX configuration, mixed values can lead to unexpected behavior.**
/qn	Option to launch the installation using command line in silent mode.

For example:

```
msiexec /i IPdesktopSoftphone_13.4.0.msi
       PBXADDR=155.192.215.150 BACKUPPBXADDR=155.192.215.146
       SHAREDNUMBERMODE=0 LANGUAGE=4 USEPASSWORD=1
       PASSWORD=letacla SCOPE=NET-ADV AUTOSTARTUP=1
       SHOWTOASTER=1 SHOWTASKBAR=1
       AUTOMATICHEADSET=1
       TRUNKSEIZE=0 PREFIXINTERNATIONAL=00 PREFIXNATIONAL=0
       COUNTRYCODE="France 33" MINDIGITS=9
       INSTALLDIR="C:\Program Files (x86)\Alcatel-Lucent
       Enterprise\IP Desktop Softphone"
       CONFIGFOLDER="C:\Users\Public"
       SETREASSIGNMENT=1
       DEFAULT_DEVICE_MICROPHONE="Microphone (2- Sennheiser
       SC260 USB CTRL II)"
       DEFAULT_DEVICE_SPEAKER="Haut-parleurs (2- Sennheiser
       SC260 USB CTRL II)"
       SECONDARY_DEVICE_MICROPHONE="Headset Microphone (2- Jabra
       EVOLVE 65)" SECONDARY_DEVICE_SPEAKER="Headset Earphone
       (2- Jabra EVOLVE 65)" RING_DEVICE_NAME="Loudspeakers /
       Headset Earphones (Realtek Audio)"
       SHORTCUTKEY_ENABLE=0 DEACTIVATE_POPUP_URGENT_CALL=1
       USE_SYSTEM_VOLUME=1
       MAC_ID=12:34:56:ab:cd:ef
       ADDMBRTOMAC=0
       OUTLOOKADDIN=1
       MASK_EXTERNAL_CALL_NUMBER=1
       REST_SERVER_PORT=8099
       SUPERVISION=0 INTERFACE_DISPLAY=1
       RINGING_CADENCE=0 CREATE_DESKTOP_SHORTCUT=0
       LOCATION_SERVER=https://172.25.171.175 THEME=1
       UPGRADEURL=https://155.192.215.150/custom/
       NO_CERT_CHECK=1 HEADSET_HID=1
       USE_TEAMS_CONNECTOR=1 RINGTONE_SOUND_OVER=1 /qn
```

When updating the same version as the installed version (to modify the installation settings for example), execute the command by adding the **/famv** option to force the taking into account of the new values.

```
msiexec /famv IPDesktopSoftphone_13.X.YY.msi
         PBXADDR=<pbxAddr> USEPASSWORD=<New value> /qn
```

In case of upgrade, only parameters which are expressed in command line take a new value. All other parameters are unchanged.

SHAREDNUMBERMODE and MAC_ID are not recommended for use in case of VDI, because they can associate to all VDI users the same extension number.

It is recommended in case of an update using command line to use silent mode(/qn).

After installation/update all the wrong values given for parameters will be replaced with their default values during the first launch of the application (.ini user file will be updated).

When using **msiexec** in Windows **PowerShell**, you will encounter issues with parameters containing spaces. This is because PowerShell handles quotes differently than the command prompt (cmd.exe). To correctly pass arguments with spaces, you need to use the appropriate escaping or quoting techniques.

For example: you will get an error if you execute this command line in **PowerShell**.

> msiexec.exe /i IPDesktopSoftphone_13.8.0.msi COUNTRYCODE="Germany 49"

You should use instead:

1-msiexec.exe /i IPDesktopSoftphone_13.8.0.msi COUNTRYCODE='"Germany 49"'

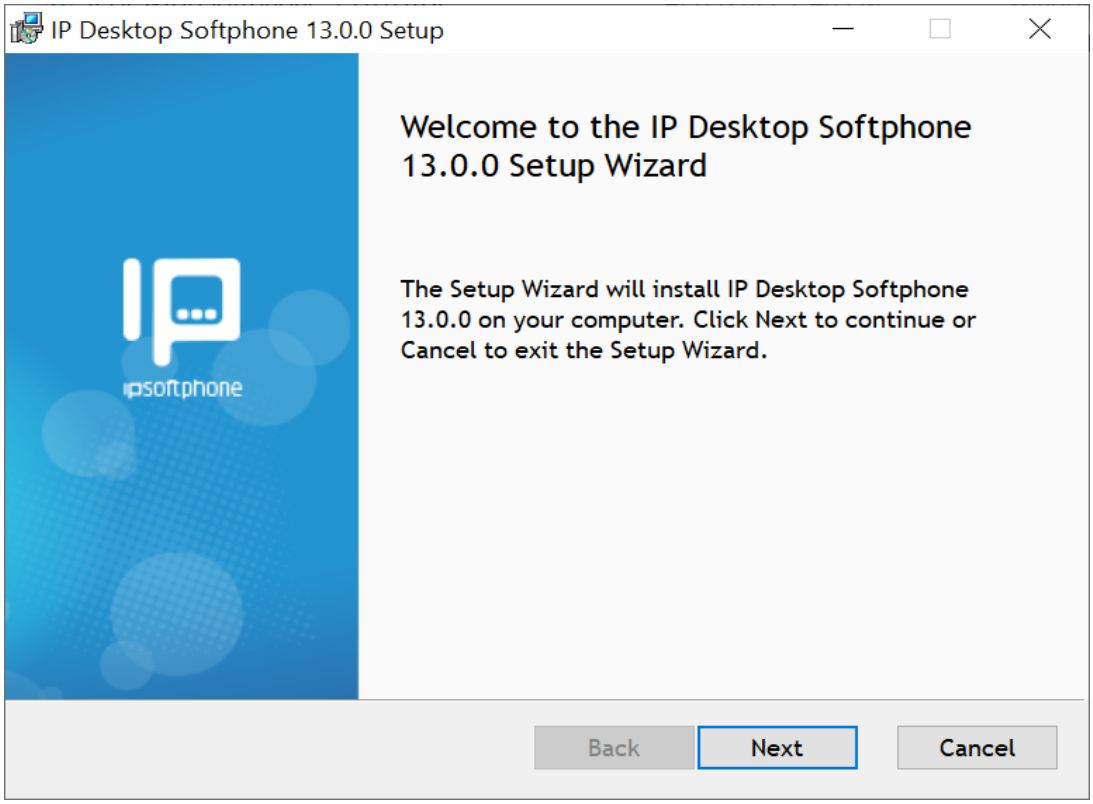
Or

2-cmd /c 'msiexec.exe /i IPDesktopSoftphone_13.8.0.msi COUNTRYCODE="Germany 49"'

5.2.4 Installation in graphic mode

In this mode, you will need to manually configure it the first time you launch the application.

NB: If the Outlook Add-In is to be installed, please make sure that Visual Studio 2010 Tools for Office Runtime is installed, it is required to run Microsoft Office based solutions built using Microsoft Visual Studio. It is available for download under: https://www.microsoft.com/en-in/download/details.aspx?id=48217.



Once the installation is started and the license agreement accepted, you can change the installation path; the default path is:

C:\Program Files (x86)\Alcatel-Lucent Enterprise\IP Desktop Softphone\

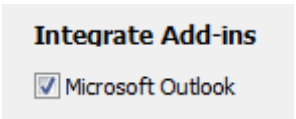
Then You can change the location of the configuration files.

By default, these files are located in:

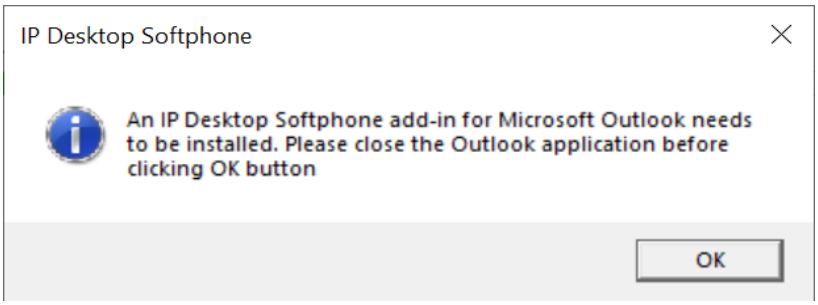
C:\Users\<user name>\AppData\Local\Alcatel-Lucent Enterprise\IP Desktop Softphone\

In the case of restricted write permissions, choose to customize the location of the configuration files.

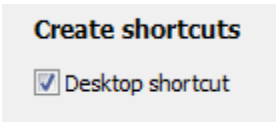
Check the checkbox in the Outlook integration windows if the IP Desktop Softphone Add-in for Outlook is to be installed.



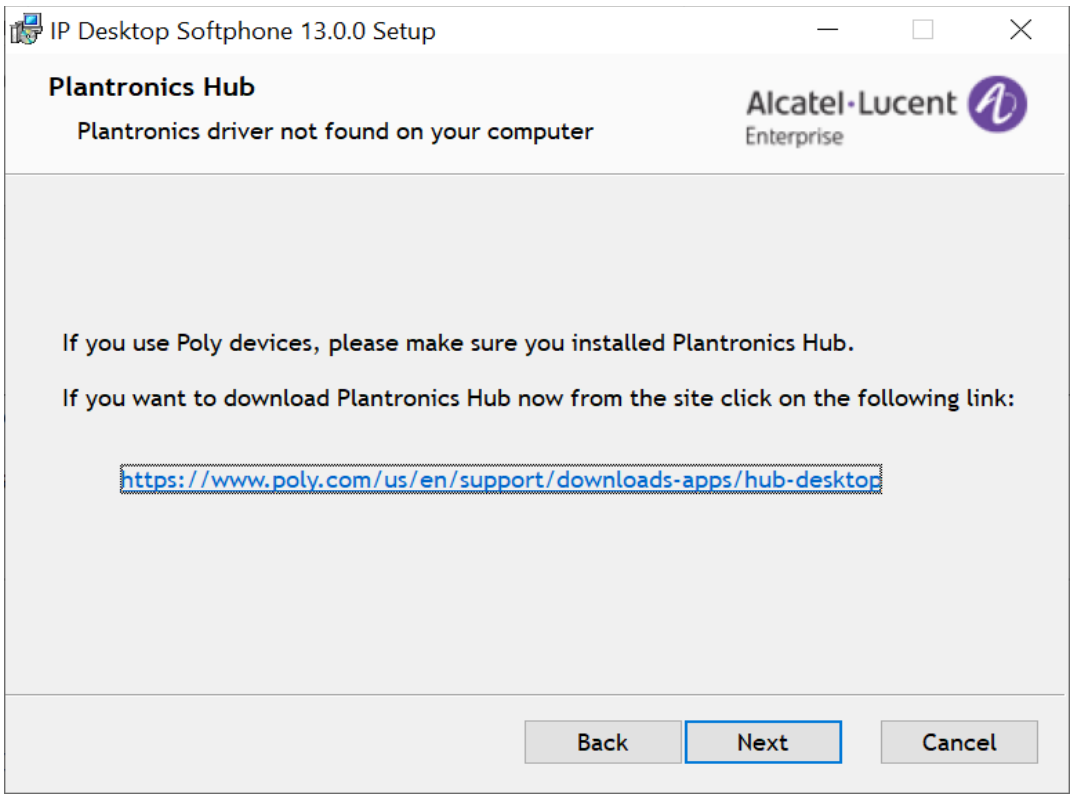
In this case, if the Outlook application is running, a popup window is shown to ask for its termination.



Check the checkbox in the Desktop Shortcut Creation windows to allow the IP Desktop Softphone shortcut to be created in the Windows desktop (by default it is checked), if you uncheck it the shortcut will not be created.



During installation, it will be necessary to install the Plantronics Hub.
Proceed with the installation if you wish to use Plantronics headphones.



5.3 Native encryption

Since IP Desktop Softphone release 11.2.0 and OXE 12.3, native encryption is supported. It enables securing both signaling (UA/NOE) and media (RTP) flows. This solution is designed as a pure software solution and does not require any specific physical encryption.
There are different ways for IP Desktop Softphone to establish secured connection with OXE:

1. Installing necessary certificates on IP Desktop Softphone Windows system store, in that case the connection will be established without prompting any message to user to accept certificates.
2. Accepting certificate during connection establishment, in this case, a message is prompted to user to accept certificates temporarily or permanently.

5.3.1 Installing certificate in Windows Store

In order to accept connection silently (without prompting a message to user), The CA (Certificate Authority) chain provided in the CTL (Certificate Trust List) must be stored in the Trusted Root Certificates Authorities preferably for Local Machine so that it can apply to all windows users' sessions. In case of presence of intermediate CA, it must also be stored in "Personal" store preferably for Local Machine.

5.3.2 Accepting certificate during connection

In case Certificates are not stored in windows store, user will be prompted to accept a server certificate. Please refer to the user's guide for more information for this section.

5.3.3 Mutual authentication

5.3.3.1 IP Desktop Softphone configuration

In case MTLS is required (mutual TLS authentication) during DTLS handshake, IP Desktop Softphone must provide its own certificate. This certificate must be provided by the administrator and installed.
The certificate can be Installed in two different ways:

- Installed in Windows Certificates Store:
  The certificate must have its private key and installed in the Windows Certificates Store under **"Local Computer/Personal"**. The private key of the certificate must also be **exportable** with the **readable access rights** for the users that will use the application.
  During handshake, the application will search in this store for this certificate, the search is based on the **Common Name (CN)** field of the certificate configured during installation of IP Desktop Softphone using the parameter: **DTLS_CERT_NAME** (please refer to section *5.2.3*).

- Using files:
  Certificate files (private key and certificate) must be put under **the installation directory** of the application and named exactly as the following:
  - softphone_pkey.pem for private key.
  - softphone_cert.pem for certificate
    The private key can be protected by password. In this case the password must be configured during Ip Desktop Softphone installation using the parameter: **DTLS_PKEY_PASSWORD** (please refer to section *5.2.3*).

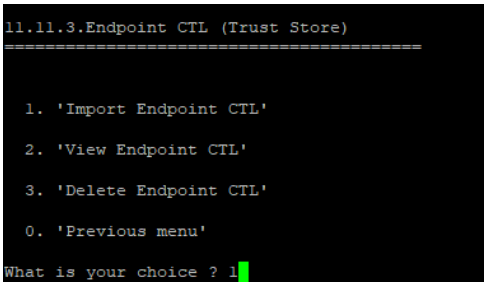
    NB: If the key password was not configured during installation, a tool (**DTLSPkeyPassphrase.exe**) is provided under **serviceability** directory. It can be used to configure the passphrase after installation. The syntax of the command is: **DTLSPkeyPassphrase.exe /set <passphrase>**. The Command must be launched under command line console with administrator rights.
    Example: DTLSPkeyPassphrase.exe /set 12345678

NB: In case of **VDI environment**, the certificate files must be put under **Installation directory of VVX module** under local PC.

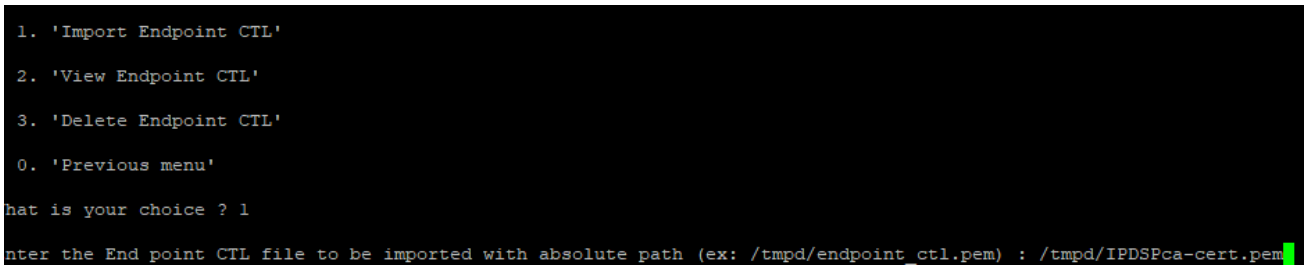
5.3.3.2 OXE configuration

The Certificate Authority (CA) that issued the IP Desktop Softphone certificate must be added into OXE's trust store.

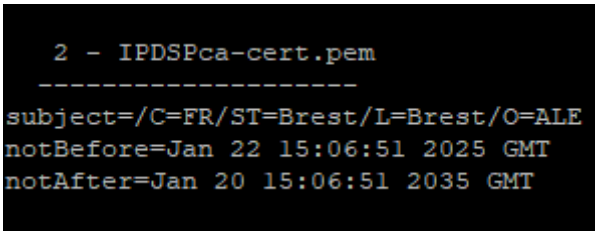
- Use the command "netadmin -m" after being logged to OXE as root.
- Choose the menu: 11. Security -> 11. PKI Management -> 3. 'Endpoint CTL (Trust Store)'
- Choose menu: 1. Import Endpoint CTL:



- Enter the path of CA certificate to be imported then press enter:



- Check that the file has been successfully imported. Use the menu: 2. 'View Endpoint CTL', and check that the newly added terminal CA certificate is inside OXE's trust store.



5.4 TFTP/HTTPS protocols order for lanpbx.cfg file

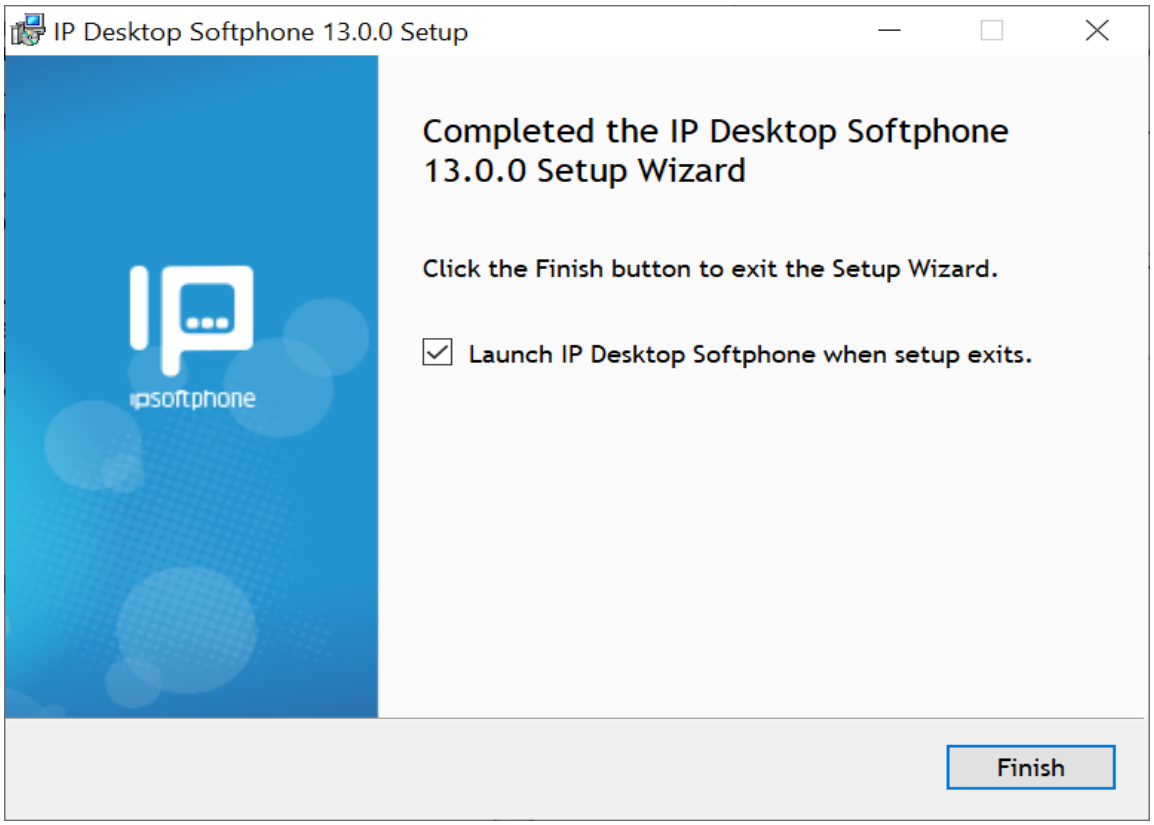
⚠ This feature is only available starting from **OXE Purple R100, N1.291.6.d**.

⚠ HTTPS is only used with OXE using native encryption (DTLS enabled).

In order to comply with security requirements, IP desktop Softphone provides HTTPS protocol as an alternative to TFTP to retrieve the lanpbx.cfg file from OXE.
IPDSP provides the possibility to choose the protocol order used for lanpbx.cfg retrieval (see description of HTTPS_TFTP_ORDER, HTTPS_PORT and LANPBX_REMOTE_PATH parameters in Chapter 5.2.3).
The lanpbx.cfg must be present in OXE in the path defined by the parameter LANPBX_REMOTE_PATH (default value is /DM/VHE8082/lanpbx.cfg). if not present, it must be copied manually.
To complete hostname's validation against certificate's CN/SAN of OXE, the server address (OXE address) must be set to FQDN instead of IP address if available.
(In case the OXE address is configured with IP - please make sure that the OXE certificate contains IP address as well).
By default, IP desktop softphone bypasses the certificate's CN/SAN check, use the parameter HTTPS_OVERRIDE_HOSTNAME_CHECK (see Chapter 5.2.3) during installation with value 0 to activate certificate's CN/SAN check.

5.5 Launching the application

At the end of the installation the user can launch the application by checking the checkbox:



Otherwise to start the softphone, use the shortcut of the application created during the installation

Or access the application from the start menu.

→ Alcatel-Lucent Enterprise → IP Desktop Softphone

In case the application has been installed in graphics mode, it will be necessary to fill in the connection information to the OXE or OXO telephony server.
This information is configurable from the Network tab

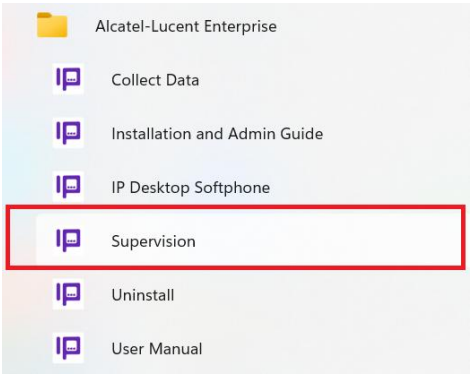
A default audio device must be declared in Windows in order to start the application.

If the application does not come into service, please make sure to add in the Windows Firewall the IpDesktopSoftphone.exe as exclude rule for uncheck.

5.5.1 Application Monitoring

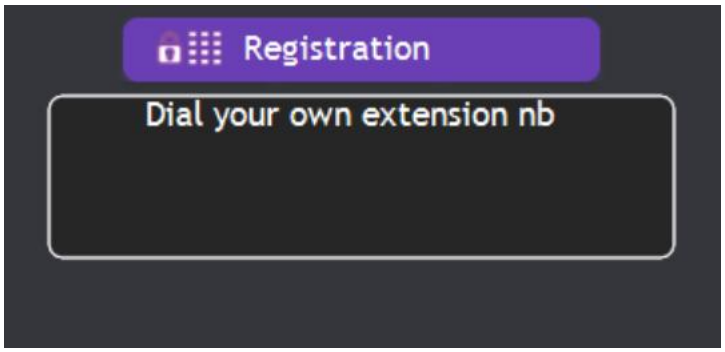
A monitoring system for IP Desktop Softphone is activated when the application starts. This will restart the IP Desktop Softphone automatically if the application freezes or unexpectedly stops.
Supervision is disabled when the IP Desktop Softphone is normally stopped.

In the Windows menu: Alcatel-Lucent Enterprise, the "Supervision" command is used to activate or deactivate supervision.



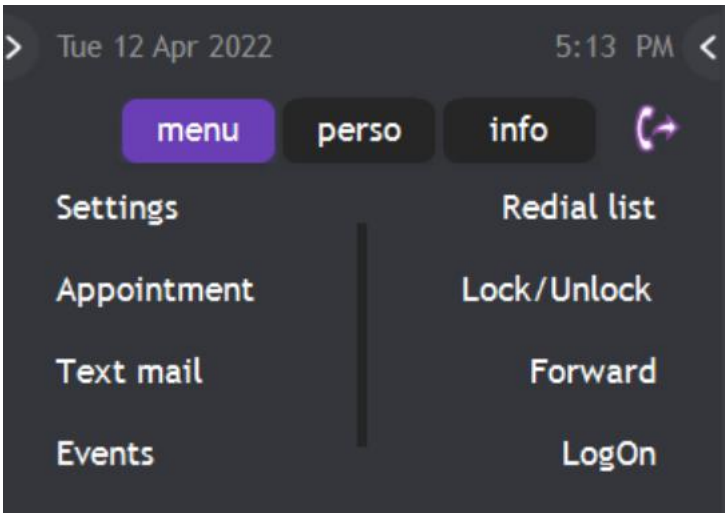
5.5.2 Registration in the OXE context

When starting the IPDSP for the first time, a directory number must be entered.
Creation and OXE user configuration are described in section OXE Configuration



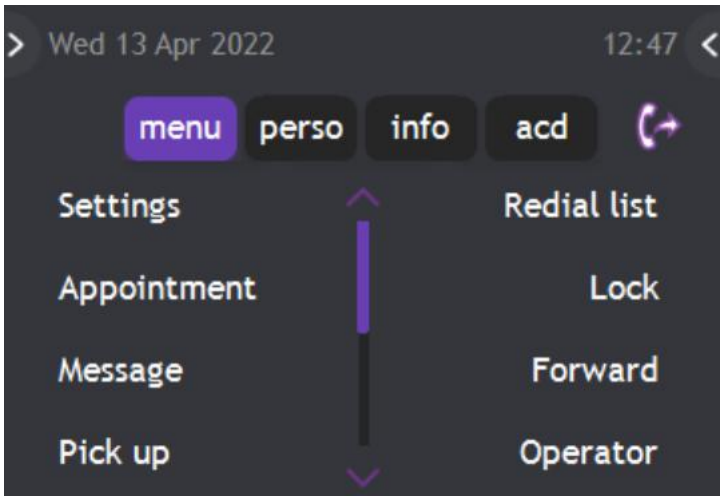
Enter the number, reported in the OXE, that has been assigned to you.

Once the number is entered with your personal code, the application is ready. It can now be used.



5.5.3 Registration in OXO context

Once the connection information to the server is correctly entered, the assignment of the extension number is automatic.



The application is ready. It can now be used.

5.6 Configuration of application

Customize the application to suit your existing environment.

Only the administrator settings are documented in this section.
All settings are detailed in the user manual.

Access configuration options by right-clicking from the application window.
The following menus are available:

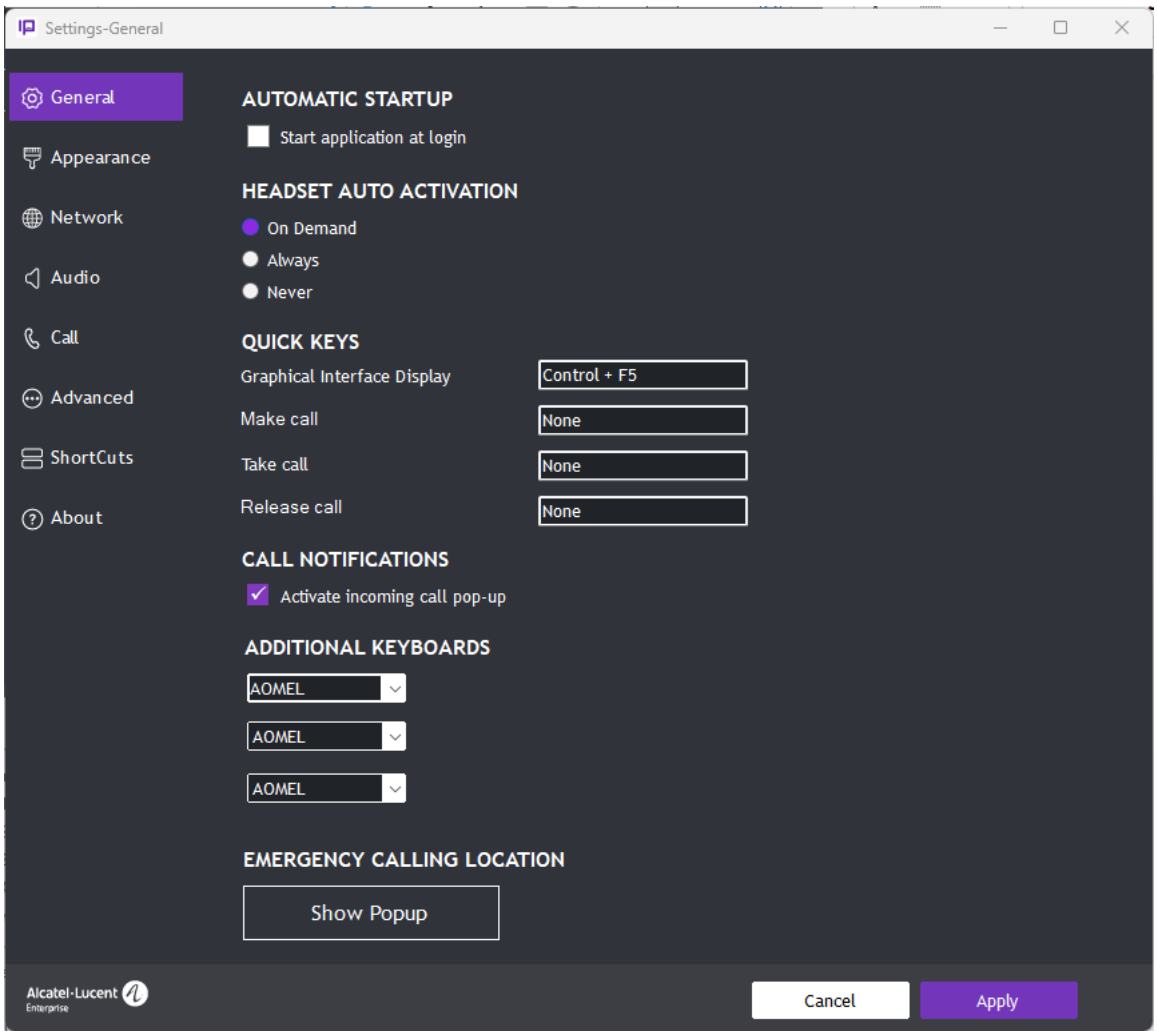
- Settings
- Audio settings

Note that there are two settings display mode depending on the choosen theme: dark or light we will use the dark theme in the screenshots in the rest of the document.

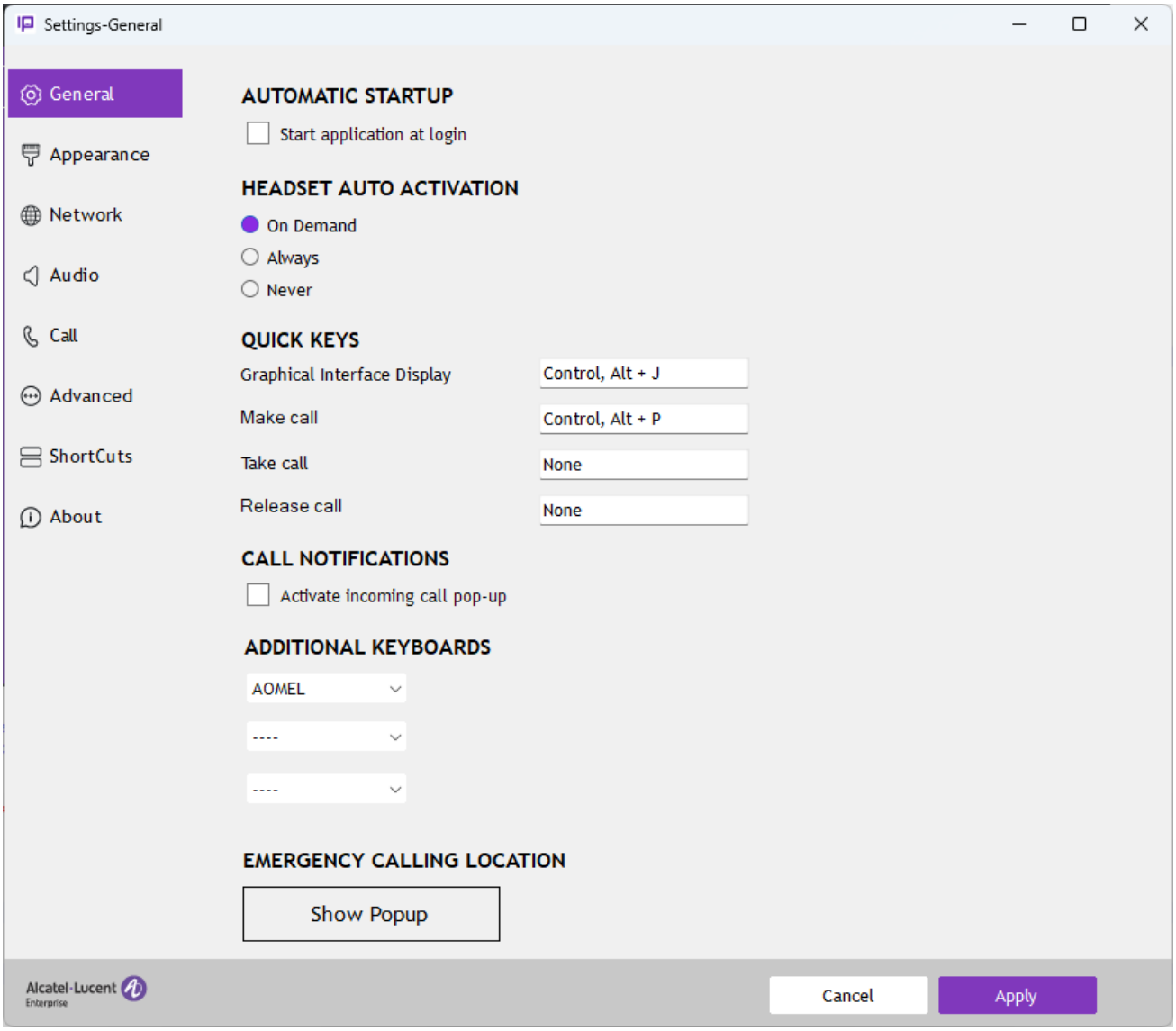
5.6.1 Settings: General tab

By default, the General tab is displayed. If access is secured, a password is requested.

1. Dark Theme:



2. Light Theme:



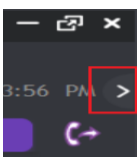
The AOM section references the list of additional keypads available.
In an OXE context, 3 keypads can be configured

- AOMEL
- AOM 10
- AOM 40

In an OXO context, only one keypad can be configured

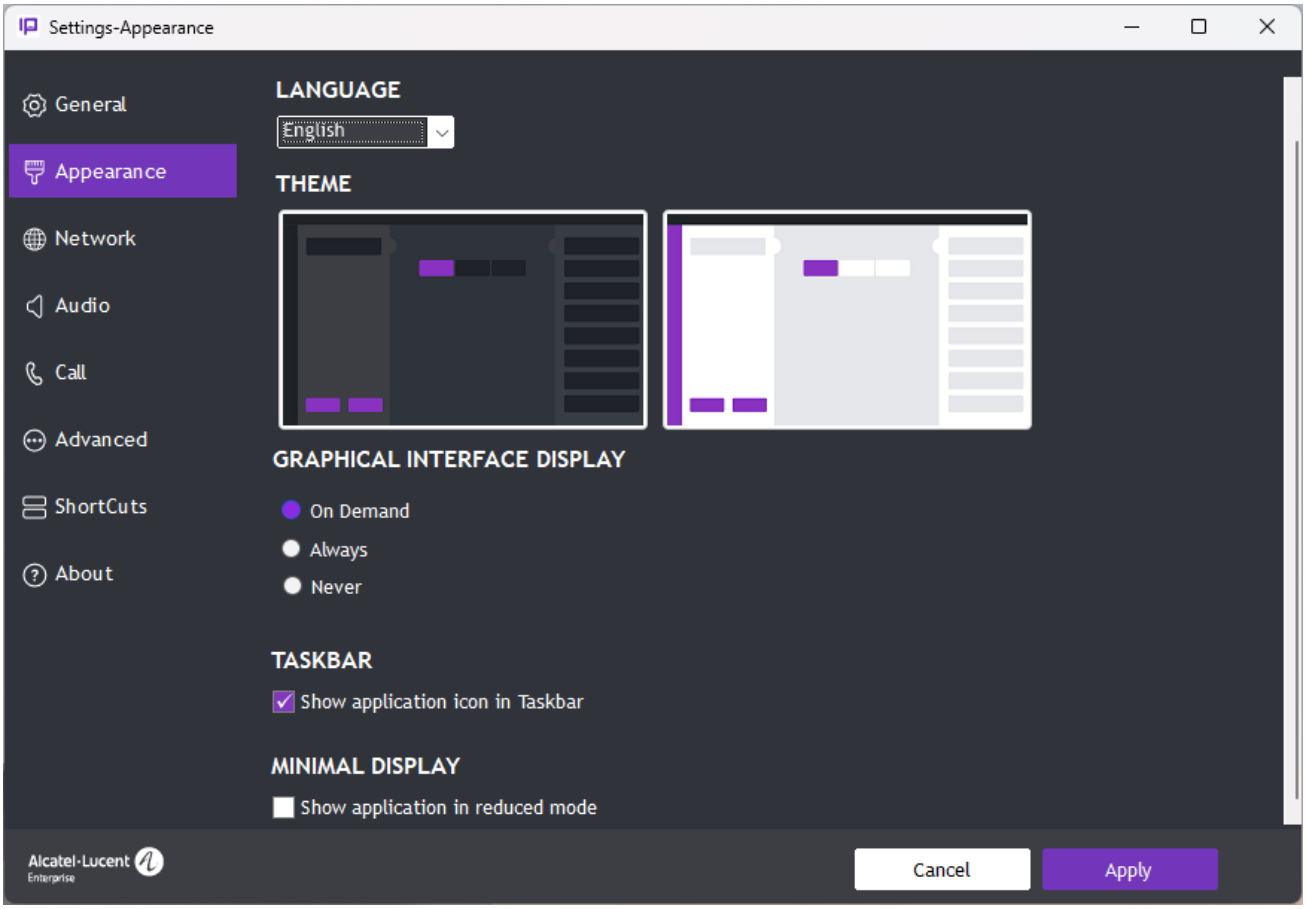
- Smart Display

The additional keypad configuration is detailed in the OXE Configuration, OXO Configuration section.
The additional keypad is accessible from the application window, once configured;



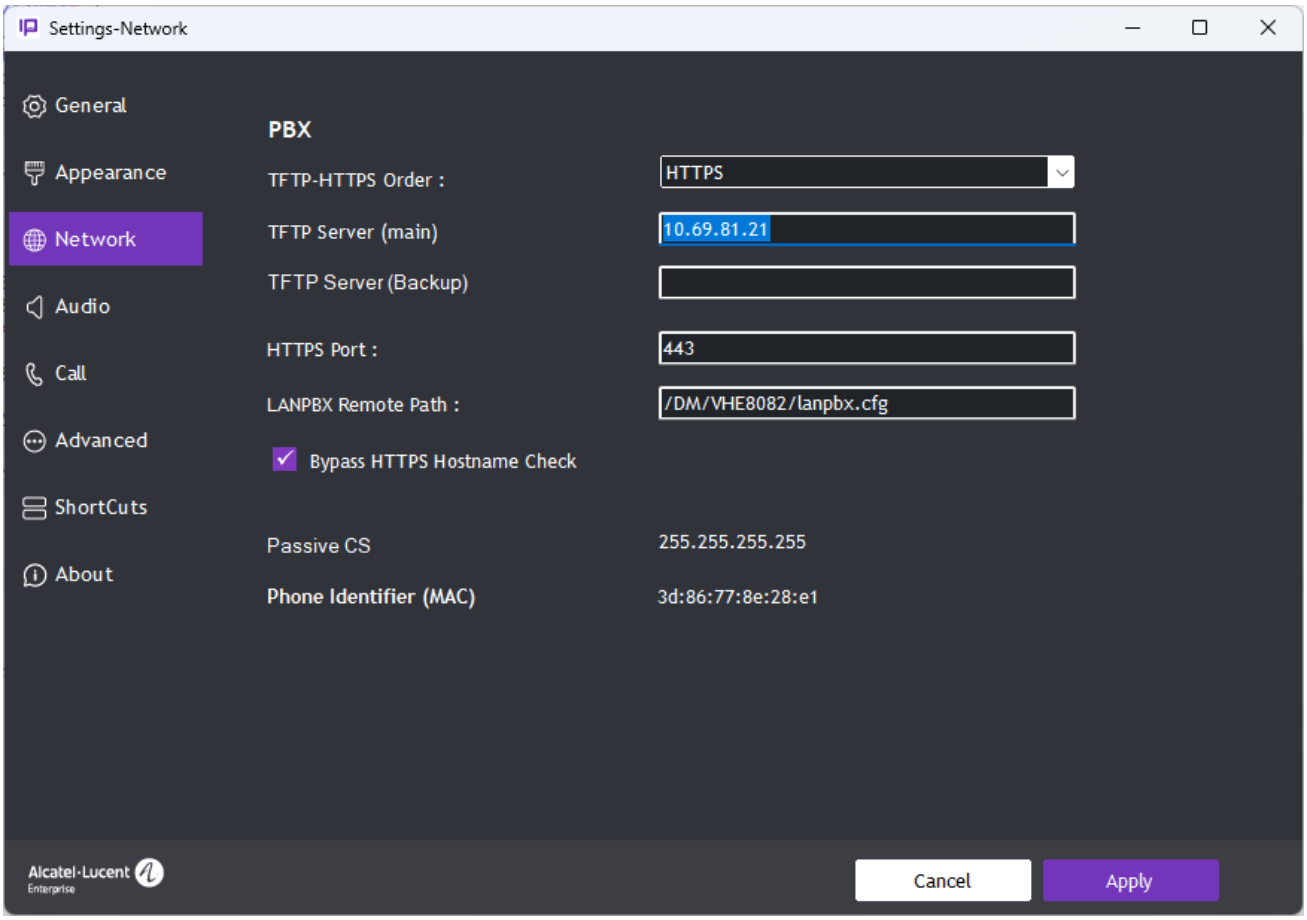
5.6.2 Settings: Appearance tab

If access is secured, a password is requested.



5.6.3 Settings: Network tab

If access is secured, a password is requested.



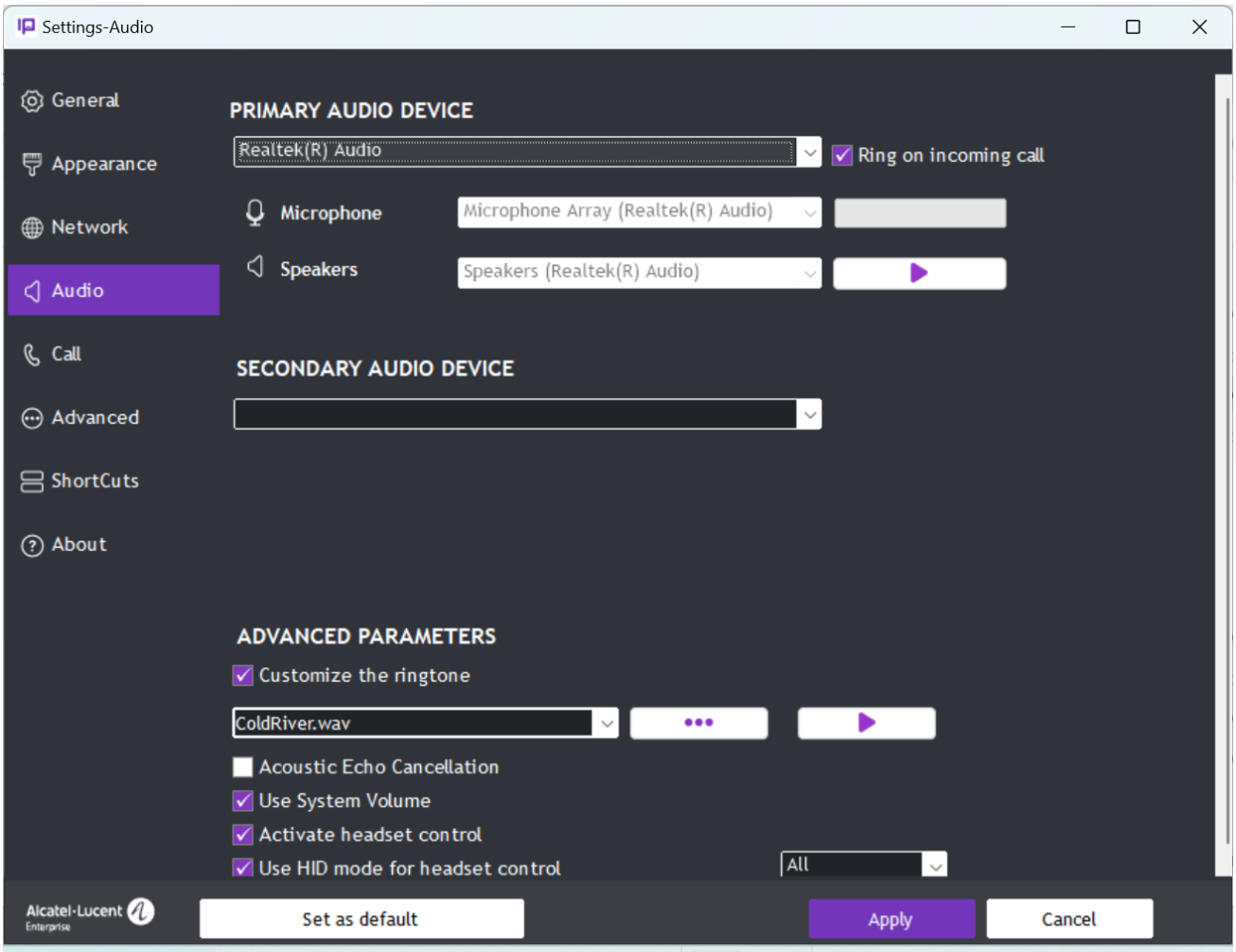
Field Name	Description
TFTP Server (Main)	IP address of your call server. The entry displayed here is the one you had keyed in during the installation process. You can change these data if required. An input error will interrupt the connection. These data are mandatory.
TFTP Server (Backup)	This is the IP address of the 2nd CPU. Enter the 2nd Role MAIN IP address here if spatial redundancy is managed.
PCS	If there is a Passive call server configured, its IP address is displayed here. This value is automatically provided by the NOE protocol and cannot be modified manually.
Phone Identifier	This is the MAC ID for your terminal, which is automatically generated by the application. You cannot change it.

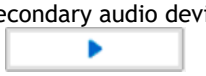
We must manually enter TFTP2 IP if present, because it is not received automatically, so it must in any case be filled in manually at the start of the installation, configuration change/change of node ....

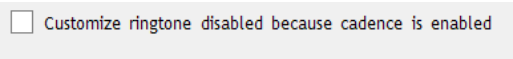
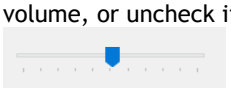
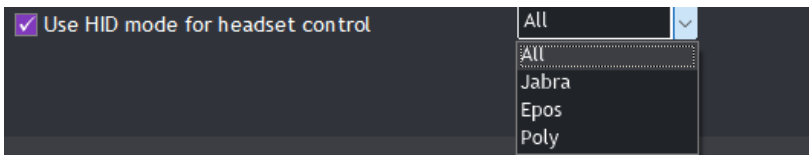
5.6.4 Settings: Audio tab

This section describes the configuration of the different types of audio devices related to the application.

To function properly, the IP Desktop Softphone application requires at least one microphone and one speaker installed on the PC.

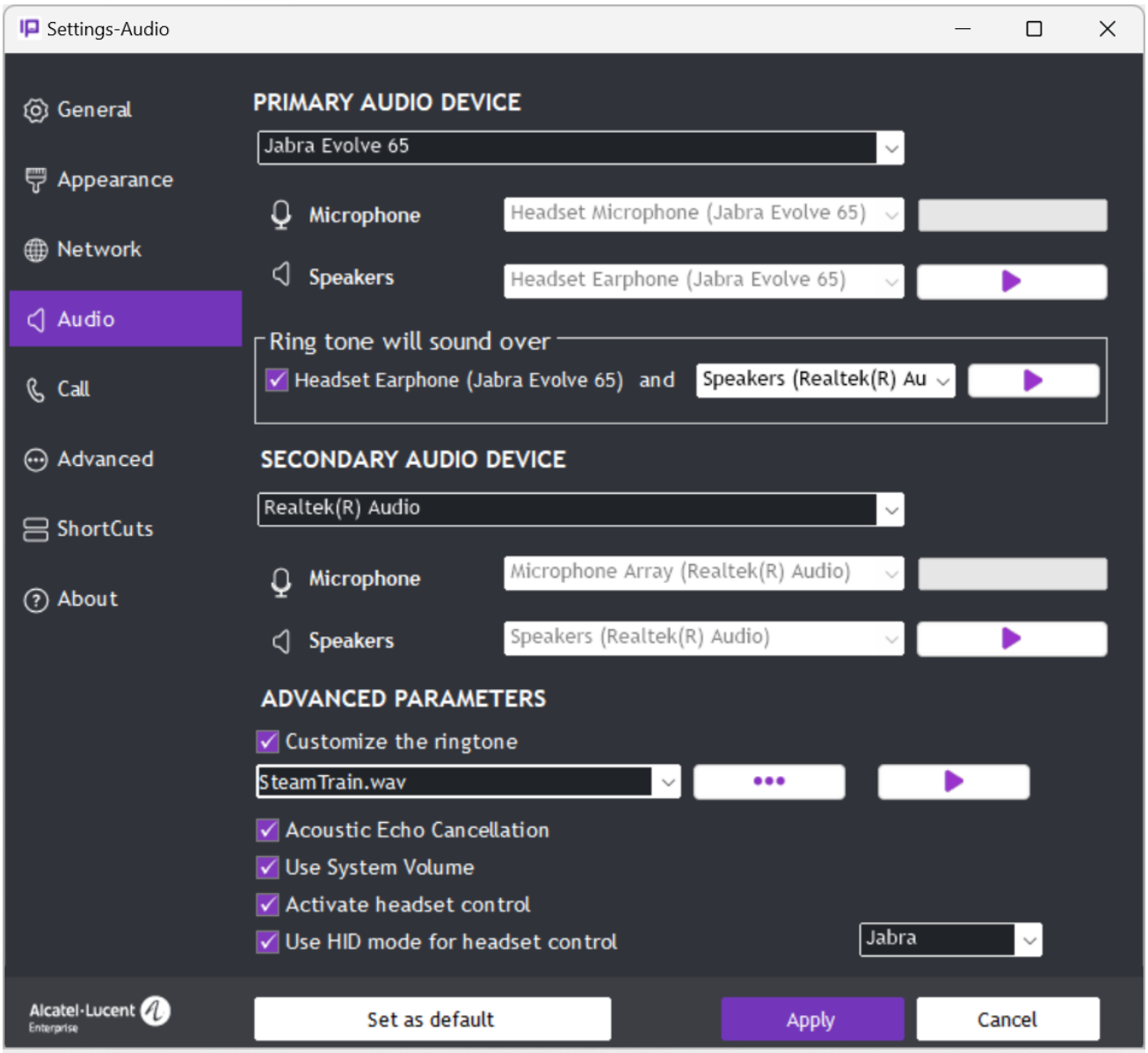


Field Name/Icon	Description
Speakers	In this drop-down list, the audio device that you select will be used for phone's output and audio playback will be heard via the speakers. One is required for the primary audio device and another one is optional for the secondary audio device. You can test them by clicking the button in front of this drop-down list  Use the button  to stop the test.
Microphone	The audio device selected here picks up your speech and sends it to the phone. You can check the maximum level of audio recording in real time in the progress bar located in front of this drop-down list  The Microphone of the secondary audio device is used for hands-free mode.

“Acoustic echo cancellation” check box	This refers to the audibility of your voice in your earpiece. If you select this check box, echo is supported. Do not check this box if you are using a headset. The audio quality of your equipment would be reduced. Select this option only if you are using IP Desktop Softphone in hands-free mode.
“Ring on incoming call” check box	When the box is selected, the selected Speaker device is used for ringing. It is present for both primary and secondary audio device. To have the ringing in a second device, select devices in Secondary audio device parameters, speaker and micro fields must be defined.
“Customize the ringtone” check box	To customize your ringtones, check this box. Otherwise the PABX ringtones will be played. This function will be disabled if the cadence is enabled. 
Ringtones	Click on this button to select a ringtone which will be for both internal and external calls: either in the drop-down list or by clicking the Browse  button, the explorer window will open. Then, select a .wav file. The phone uses this file while testing the audio properties. The file you have selected is displayed next to this button. To have different ringtones for internal and external calls, disable "Customize the ringtone" and choose a different PABX ringtone for these two types of call. For compatibility reasons, when personalized melodies (.wav) are chosen and Call Ringing Cadences are programmed in the PABX system parameters, the ringtone may be altered or not or played.
“Use System Volume” check box	To customize the volume level, you have either to check this box if you want to use system volume, or uncheck it if you want to adjust the used volume level or mute it 
Activate headset control	Check this box to activate Headset control (on-hook, off-hook mute and unmute function) Uncheck it to deactivate headset control. Default: Checked
Use HID mode for headset control	Check this box to use HID for headset control. And choose which headset type it is applied to.  Default: Unchecked

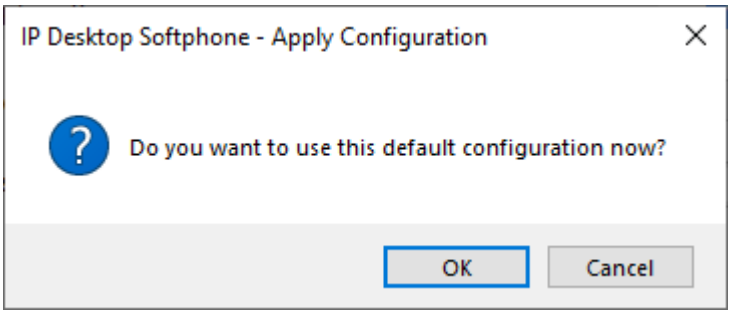
By default, the active volume is that of the audio device used in the audio configuration. You can customize the volume level using the audio setting windows (uncheck the box “Use System Volume”). Also use your audio device or the +/- keys of the application if you want to temporarily change the volume during the conversation.

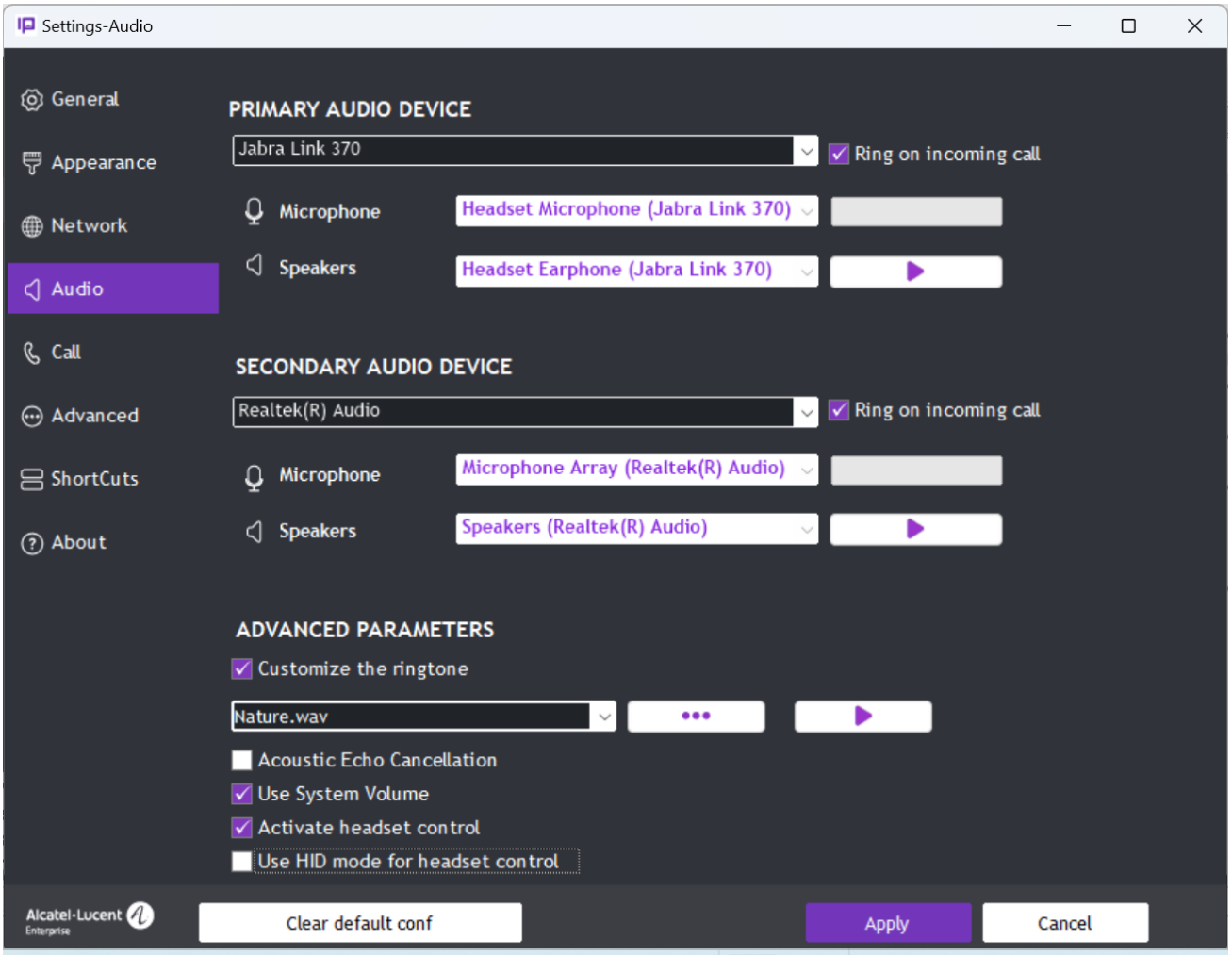
When RINGTONE_SOUND_OVER is activated(set to 1) the user has to choose the ringing tone device either from checkbox to select or not the primary device and from a listbox to choose a second device among the speakers other than that of the primary device(see “Ring tone will sound over” groupbox).



DEFAULT AUDIO CONFIGURATION:

You can choose to set and save your default audio configuration, that will be taken automatically when a default device is plugged.
Default configuration concerns: MICRO/SPEAKER of primary and secondary device and ringer device.
You can also visually see the default devices in the list box by a distinctive display (bold and blue color) when device is detected by the system.
Default configuration is applicable when option "Headset Auto activation" is set to:
- Never
- on demand. (no popup when default device is plugged)
To do this operation, click on the “Set as default” button, you can either use this default configuration now (answer OK), or when a default device is plugged.



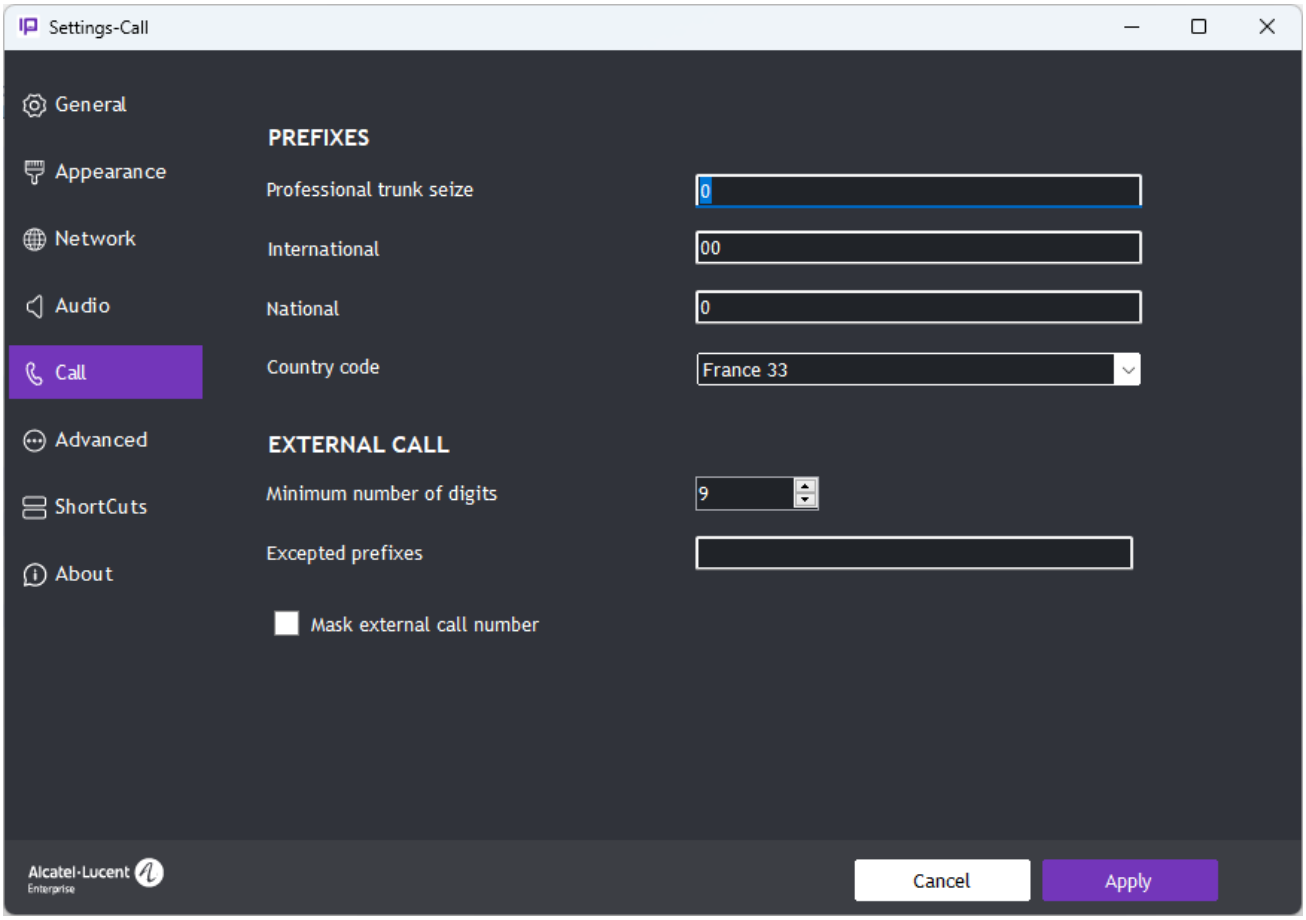


You want to remove the default configuration you set before, click on the button “Clear default conf”.

5.6.5 Settings: Call tab

This window allows you to customize the call settings.

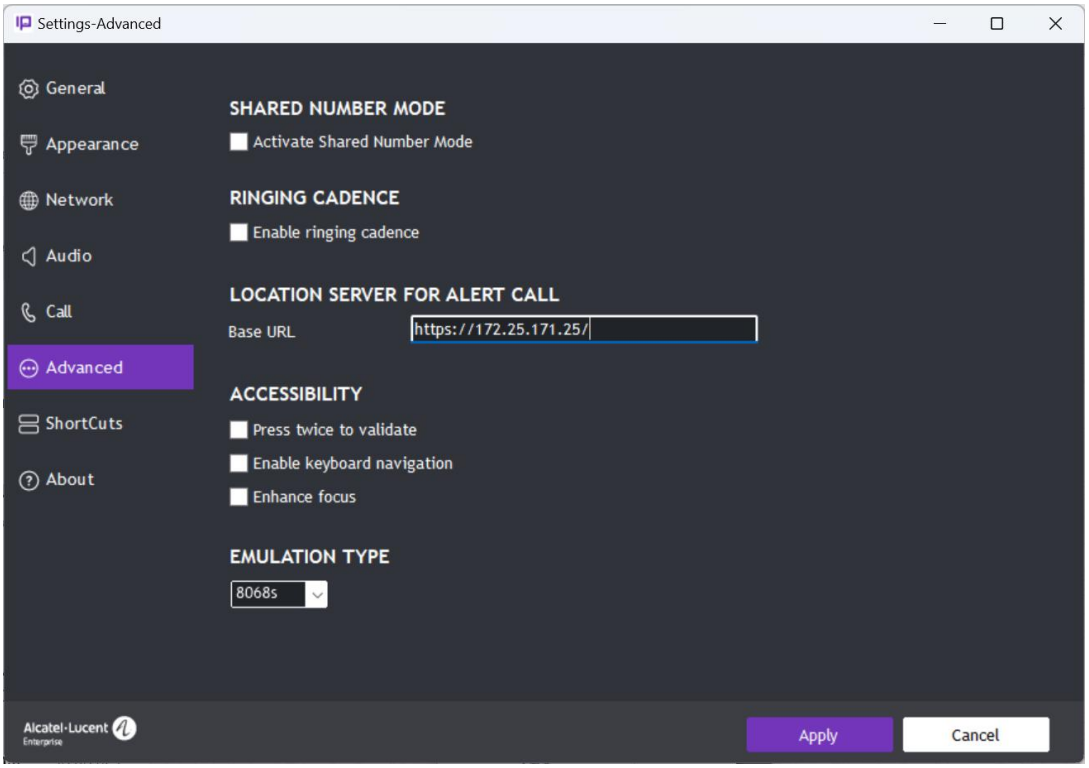
If access is secured, a password is requested.



Field Name	Description
Professional trunk seize	See the description of the "TRUNKSEIZE" field in Chapter 8 (Installation)
International	See the description of the “PREFIXINTERNATIONAL” field in Chapter 8 (Installation)
National	See the description of the “PREFIXNATIONAL” field in Chapter 8 (Installation)
Country code	See the description of the “COUNTRYCODE” field in Chapter 8 (Installation)
Minimum number of digits	See the description of the “MINDIGITS” field in Chapter 8 (Installation)
Excepted prefixes	Exceptions from the previous field separated by spaces
Masking external call number	Used to hide the call number, an "External Call" string will be displayed instead of the number on the screen as well as all of the application's menus.

5.6.6 Settings: Advanced tab

If access is secured, a password is requested.



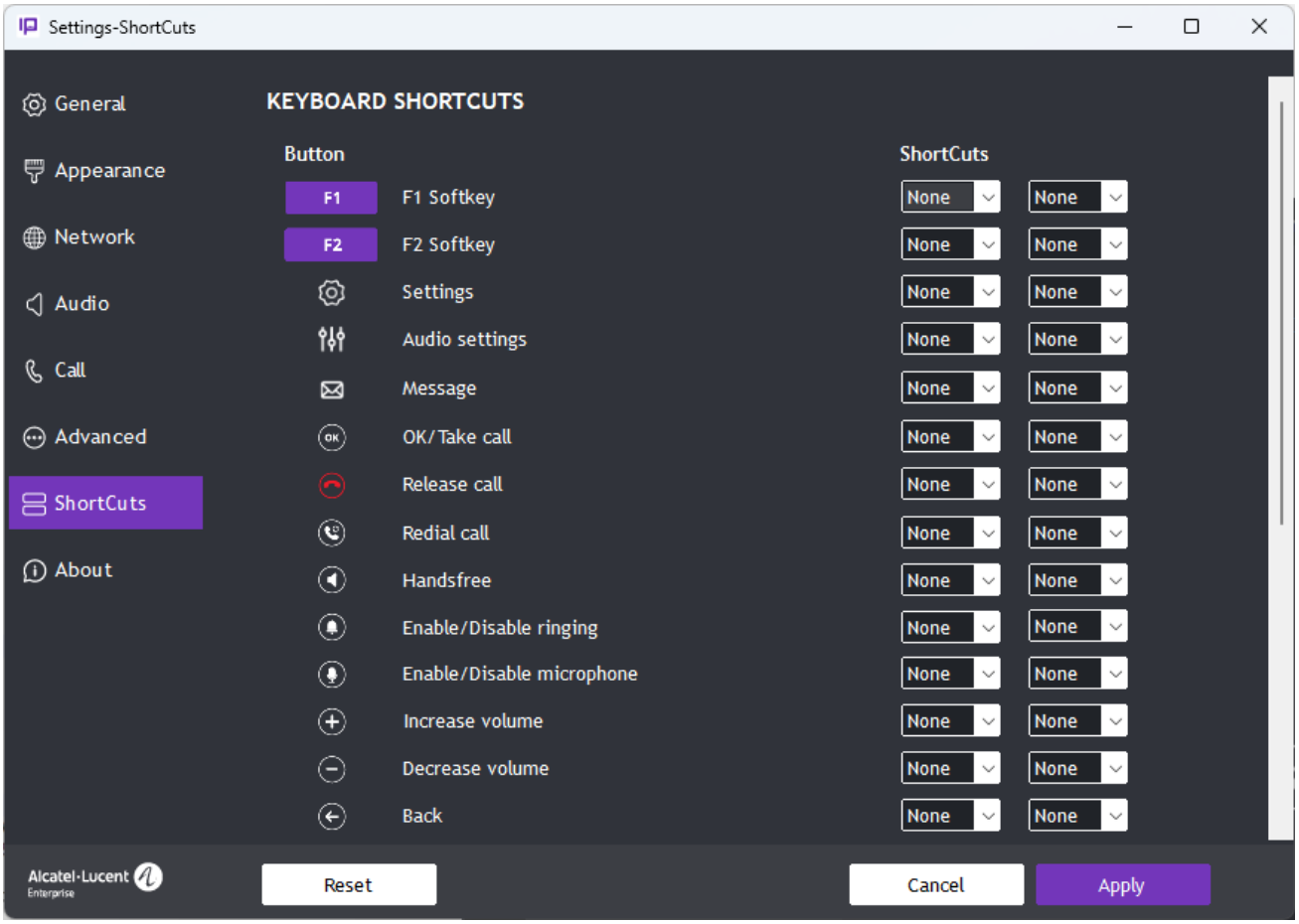
Field Name	Description
Shared Number Mode	Choosing Shared Number Mode will link the Softphone ID to the PC (one ID only per PC).
Ringing cadence	Used to activate or not the cadence for ringing, by default it is not activated.
Location Server for alert call	URL of the VNA server.
Press twice to validate	If checked, the user must press the button twice. The first press is used to know the function of the button. The second press executes the function.
Enable keyboard navigation	This option is only for interface buttons. If checked the keyboard events (like “Enter”) executes the button function. If not, the keyboard event is sent to PBX
Enhance focus	If checked, the focus rectangle is shown for main application screen and buttons like Release, Mute …
Emulation Type	Sets the type of emulation of ALE IP phone. Possible values: • 8068S (default value) • ALE-300 **NB: Please make sure the value is the same as the set type in PABX configuration, mixed values can lead to unexpected behavior.**

5.6.7 Settings: Shortcuts tab

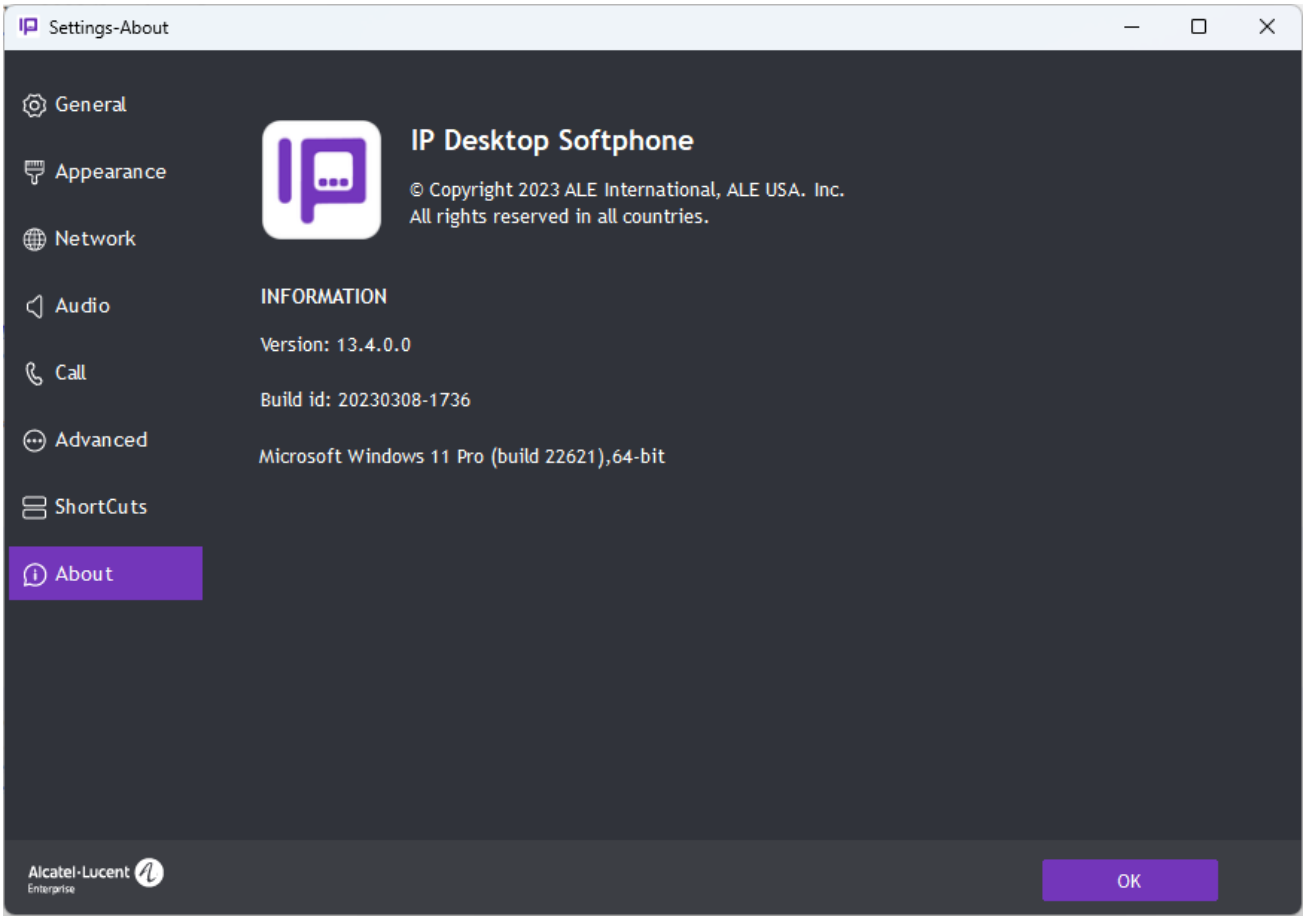
This window allows you to set keyboard shortcuts for different application buttons.

The first choice of shortcut combination is none, Ctrl, Shift or Alt keyboard key. The second part of combination is F1 to F12 keyboard keys.

Examples: F4, Ctrl F4, Shift F4 or Alt F4.



5.6.8 Settings: About tab



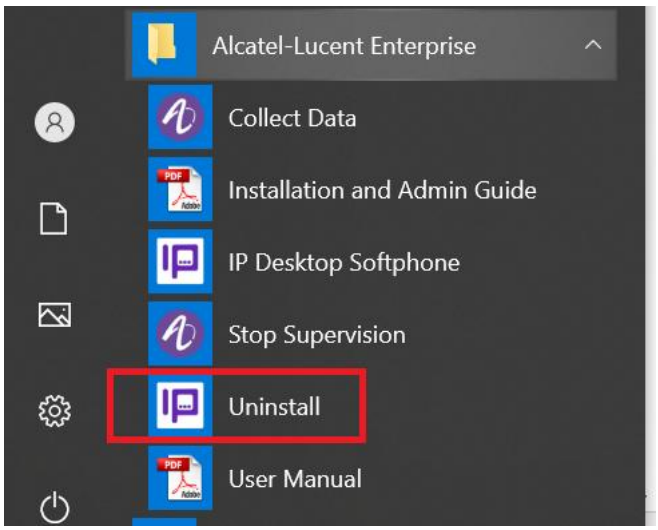
5.7 Uninstalling

Close the application before starting the uninstallation process

5.7.1 Uninstalling Using Windows Shortcut

To uninstall the application from Windows:

Start → All Programs → Alcatel-Lucent Enterprise → Uninstall



5.7.2 Uninstalling Using: .msi File from command prompt

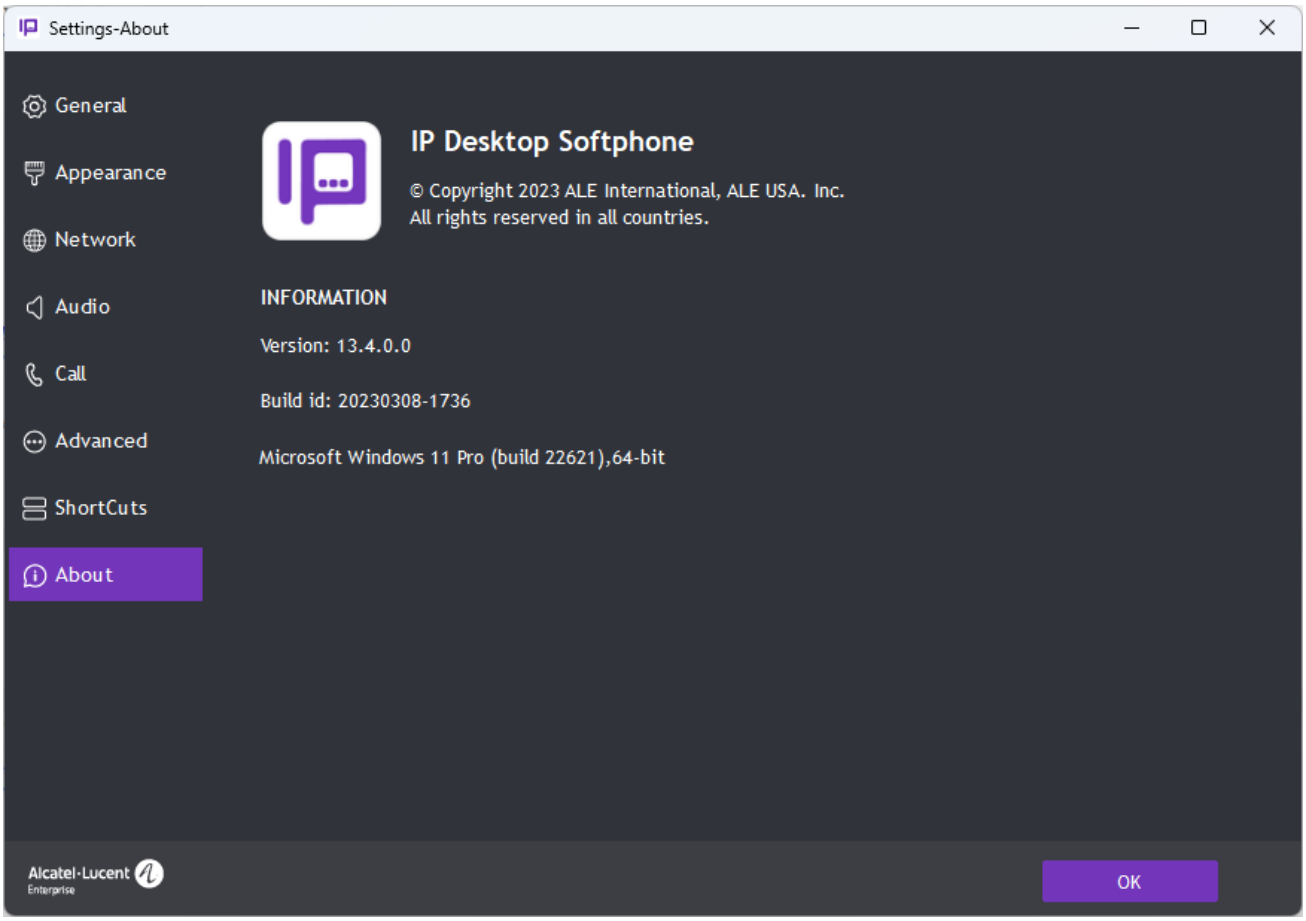
msiexec /x IPDesktopSoftphone_13.X.YY.msi

Component	Description
msiexec	Microsoft command to execute file with 'msi' extension
/x	Setting indicating uninstallation
IPDesktopSoftphone_13.X.YY.msi	Name of the file to be executed.

5.8 RUN mode

5.8.1 Version

Check the installed version with the "?" button



5.8.2 Activating traces

To activate the traces:

1. Edit the file *log4cxx.xml* in the installation directory.
2. Locate the line (normally line 84 to 90)
   - *<level value="OFF" class="org.apache.log4j.xml.Level" />*
3. By default, the value is OFF. Replace the OFF value with INFO.
   - *<level value="INFO" class="org.apache.log4j.xml.Level" />*
4. Save the file
5. Restart the IP Desktop Softphone to take changes into account.

Log files are located under the directory:
C:\Users\<username>\AppData\Local\Temp\Alcatel-Lucent Enterprise\IP Desktop SoftPhone\logs

Where <username> is the current Windows username

5.9 IP Desktop Softphone REST API

The IP Desktop Softphone REST API is based on HTTPS GET and POST requests which makes it easy for developers to write applications that can perform call actions on IP Desktop Softphone (make call, release call and some other audio actions). This service is available only from the localhost (host where IP desktop Softphone is running), it cannot be called from remote host.
To access REST APIs, client must prefix the requests by the domain https://localhost:<REST_SERVER_PORT>/IPDSPAction where <REST_SERVER_PORT> is the REST port number configured during installation (refer to chapter 5.2.3), default value of port number is 8097.
HTTP request header Content-type must be application-json (Content-Type: application/json).

NB: the HTTPS service uses a self-signed certificate.

5.9.1 REST API for Call/Hangup actions

Request type: **POST**.
Url: /Call
The body of the request has the following json format:

```
{
    action: makeCall / hangUp
    data1: <number to call>
    data2:
}
```

action can have two possible values: makeCall (to make a call) or hangUp (to release call).
data1: the number to call. (in case of action = makeCall).
data2 is not used for the moment (for future use).

Example:

Url: https://localhost:8097/IPDSPAction/Call

To call number 0123456789:

```
{
    "action": "makeCall",
    "data1": "0123456789",
    "data2": ""
}
```

To release call:

```
{
    "action": "hangup",
    "data1": "",
    "data2": ""
}
```

5.9.2 REST API for audio actions

5.9.2.1 Get mute state

Request type: **GET**.
Url: **/api/getMuteState**
Parameters: **No parameters**
Response: **200 OK**
true (if muted), **false** (if not)

5.9.2.2 Mute capture device

Request type: **POST**.
Url: **/api/muteCaptureDevice**
Parameters: **No parameters**
Response: **200 OK**
true

5.9.2.3 Unmute capture device

Request type: **POST**.
Url: **/api/unmuteCaptureDevice**
Parameters: **No parameters**
Response: **200 OK**
true

5.9.2.4 Get capture devices

Request type: **GET**.
Url: **/api/getCaptureDevices**
Parameters: **No parameters**
Response: **200 OK**

```
[
  {
    "deviceName": "Microphone Array (Realtek(R) Audio)",
    "deviceType": "MIC",
    "isActive": true,
    "primaryStatus": 1,
    "volume": 65535
  },
  {
    "deviceName": "Headset Microphone (Jabra Link 370)",
    "deviceType": "MIC",
    "isActive": false,
    "primaryStatus": 0,
    "volume": 38549
  }
]
```

5.9.2.5 Get render devices

Request type: **GET**.
Url: **/api/getRenderDevices**
Parameters: **No parameters**
Response: **200 OK**

```
[
  {
    "deviceName": "Headset Earphone (Jabra Link 370)",
    "deviceType": "HP",
    "isActive": false,
    "primaryStatus": 0,
    "volume": 65535
  },
  {
    "deviceName": "Speakers (Realtek(R) Audio)",
    "deviceType": "HP",
    "isActive": true,
    "primaryStatus": 1,
```

```
    "volume": 46360
  }
]
```


5.9.2.6 Get current capture device

Request type: **GET**.
Url: **/api/getCurrentCaptureDevice**
Parameters: **No parameters**
Response: **200 OK**


```
{
 "deviceName": "Microphone Array (Realtek(R) Audio)",
 "deviceType": "MIC",
 "isActive": true,
 "primaryStatus": 1,
 "volume": 65535
}
```


5.9.2.7 Get current render device

Request type: **GET**.
Url: **/api/getCurrentRenderDevice**
Parameters: **No parameters**
Response: **200 OK**


```
{
  "deviceName": "Speakers (Realtek(R) Audio)",
  "deviceType": "HP",
  "isActive": true,
  "primaryStatus": 1,
  "volume": 46360
}
```


5.9.2.8 Switch Active device

Request type: **POST**.
Url: **/api/switchActiveDevice**
Parameters: **No parameters**
Response: **200 OK**


```
[
  {
    "deviceName": "Speakers (Realtek(R) Audio)",
    "deviceType": "HP",
    "isActive": true,
    "primaryStatus": 2,
    "volume": 46360
  },
  {
    "deviceName": "Microphone Array (Realtek(R) Audio)",
    "deviceType": "MIC",
    "isActive": true,
    "primaryStatus": 2,
    "volume": 65535
  }
]
```

5.9.2.9 Switch to secondary device

Request type: **POST**.
Url: **/api/switchToSecondary**
Parameters: **No parameters**
Response: **200 OK**


```
[
  {
    "deviceName": "Speakers (Realtek(R) Audio)",
    "deviceType": "HP",
    "isActive": true,
    "primaryStatus": 2,
    "volume": 46360
  },
  {
    "deviceName": "Microphone Array (Realtek(R) Audio)",
    "deviceType": "MIC",
    "isActive": true,
    "primaryStatus": 2,
    "volume": 65535
  }
]
```


5.9.2.10 Switch to primary device

Request type: **POST**.
Url: **/api/switchToPrimary**
Parameters: **No parameters**
Response: **200 OK**


```
[
  {
    "deviceName": "Headset Earphone (Jabra Link 370)",
    "deviceType": "HP",
    "isActive": true,
    "primaryStatus": 1,
    "volume": 65535
  },
  {
    "deviceName": "Headset Microphone (Jabra Link 370)",
    "deviceType": "MIC",
    "isActive": true,
    "primaryStatus": 1,
    "volume": 45746
  }
]
```

5.9.2.11 Decrease current capture device volume

Request type: **POST**.
Url: **/api/decreaseCurrentCaptureDeviceVolume**
Parameters: **No parameters**
Response: **200 OK**


```
{
  "deviceName": "Microphone Array (Realtek(R) Audio)",
  "deviceType": "MIC",
  "isActive": true,
  "primaryStatus": 2,
  "volume": 58981
}
```


5.9.2.12 Decrease current render device volume

Request type: **POST**.
Url: **/api/decreaseCurrentRenderDeviceVolume**
Parameters: **No parameters**
Response: **200 OK**


```
{
  "deviceName": "Speakers (Realtek(R) Audio)",
  "deviceType": "HP",
  "isActive": true,
  "primaryStatus": 2,
  "volume": 39321
}
```


5.9.2.13 Increase current capture device volume

Request type: **POST**.
Url: **/api/increaseCurrentCaptureDeviceVolume**
Parameters: **No parameters**
Response: **200 OK**


```
{
  "deviceName": "Microphone Array (Realtek(R) Audio)",
  "deviceType": "MIC",
  "isActive": true,
  "primaryStatus": 2,
  "volume": 65535
}
```


5.9.2.14 Increase current render device volume

Request type: **POST**.
Url: **/api/increaseCurrentRenderDeviceVolume**
Parameters: **No parameters**
Response: **200 OK**

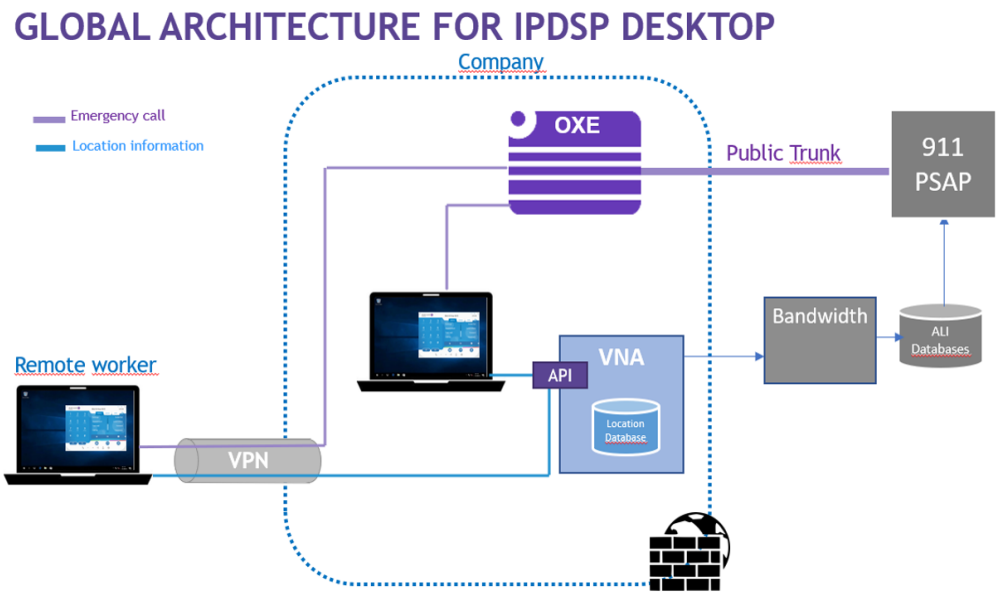

```
{
  "deviceName": "Microphone Array (Realtek(R) Audio)",
  "deviceType": "MIC",
  "isActive": true,
  "primaryStatus": 2,
  "volume": 65535
}
```

5.9.2.15 Schemes

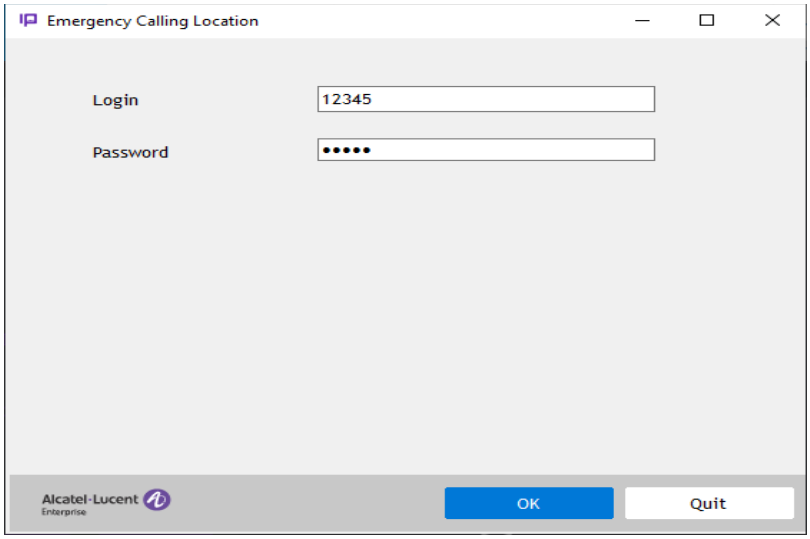
deviceName: string
deviceType: string (“MIC” or “HP”)
isActive: boolean (true if active, false if not)
primaryStatus: integer (0: if device not configured,
1: if configured as primary,
2: if configured as secondary)
Volume: integer (0 to 65535)

5.10 Emergency Calling Location

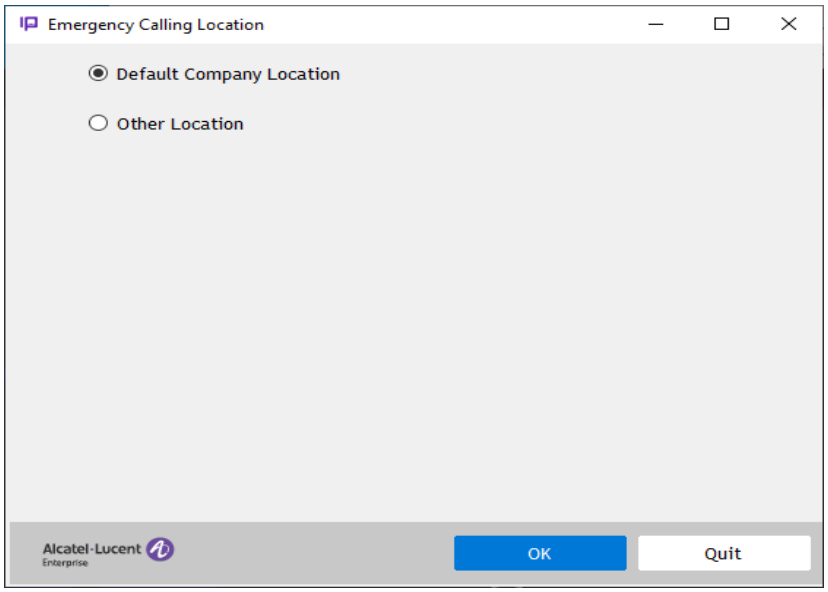
The IPDSP dervice that will play the role of location provider is VNA server. VNA provides an API to all IPDSP device to update the location information for a given phone device.
A default location information is set in VNA as the company location information. That means by default the devices have not to manage the location information.
Ones the phone device moves to company outside, it must manage the new location (for instance home working).



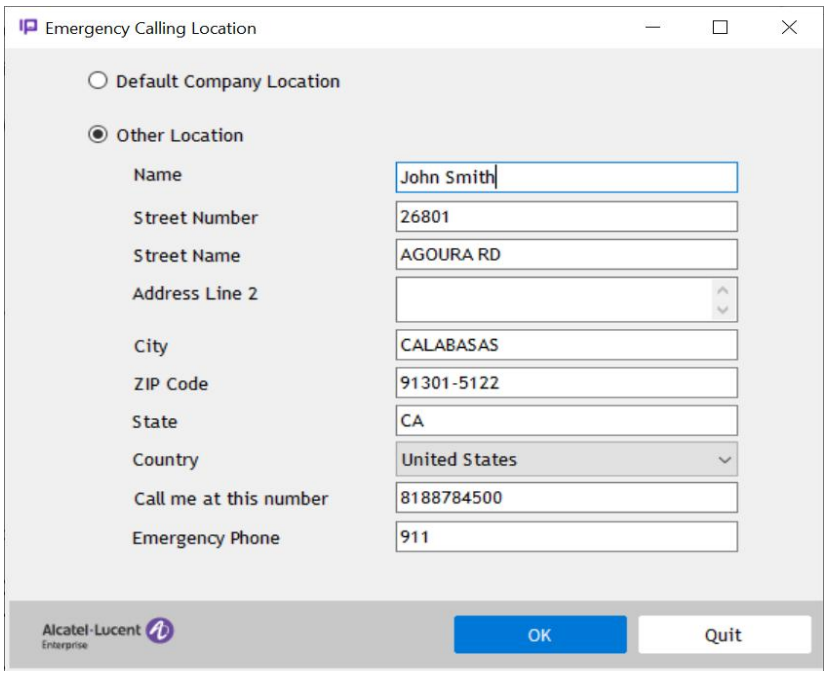
- At First startup, IPDSP will show the pop-up to connect to VNA server:



- After and for each startup, IPDSP will show the pop-up with 2 options:
  - default location that is managed at company level, inside the VNA server
  - other location that asked the end-user to enter the whole address where he is using the IPDSP



- Each time the IPDSP is restarted, the pop-up is displayed.
- The last choice is presented as the preferred choice (example: last choice = Other Location, at the restart the tick choixe is “Other location”)
- The “other location” information is stored with the end-user data and presented again in the pop-up each time it is displayed.
- If Other Location is chosen and address fields are empty, the user is unable to save this choice (OK button not active)



5.11 Automatic Update

This feature consists in offering the possibility for customers to automatically upgrade all the IP Desktop Softphone fleet connected to an OXE.
During installation, the administrator can specify the HTTPS URL of the file “ipdsp.file” that contains the information about the IP Desktop Softphone version that must be installed in end user PC. The parameter UPGRADEURL is used in installation command line as follows: UPGRADEURL=<URL>. If this field is not used or empty, no automatic update check is done.
For example, if ***UPGRADEURL=https://155.192.215.150/custom*** during installation, the application will download the file ipdsp.info using this URL (full download URL will be: ***https://155.192.215.150/custom/ipdsp.info***).
Once the ipdsp.info file is downloaded, IP Desktop Softphone uses it to check if the application must be updated.

⚠ If the IPDSP Agent and IPDSP Update Service does not come into service, please make sure to add in the Windows Firewall the IPDSPAgent.exe and IPDSPUpdateService.exe as exclude rule for uncheck.

A. The auto-upgrade requires a certificate that must be present either:

1- in Windows Store of the PC (as indicated for Native encryption chapter 5.3 .1 Installing certificate in Windows Store).

2- in a directory with the name of the server (can also be pabx) given in the UPGRADEURL installation parameter under %AppData%\Alcatel-Lucent Enterprise\IpDesktopSoftPhone\PBX_CTL\, like root-xxxxxxxxxx.cer.

For example:
UPGRADEURL=https://155.192.215.150/custom
so, the certificate file should be present either in Windows Store or in the directory:
%AppData%\Alcatel-Lucent Enterprise\IpDesktopSoftPhone\PBX_CTL\155.192.215.150

B. in case of FQDN of pabx given in the UPGRADEURL parameter, ipdsp will search the certificate file first in directory FQDN then if not found, it will try also in the equivalent @ip directory of this FQDN.

For example:
FQDN is **hostname.domain.com** and its equivalent @ip is **155.192.215.150**
UPGRADEURL=https://hostname.domain.com/DM/VHE8082/
so ipdsp will search the certificate file first in directory hostname.domain.com under PBX_CTL
then if not found, it will try also in the equivalent @ip directory **155.192.215.150** of this FQDN **hostname.domain.com**.

NB: To avoid checking the certificate, the installer can use the parameter NO_CERT_CHECK set to 1 during installation (refer to chapter 5.2.3).

5.11.1 Ipdsp.info file format

The ipdsp.info has the following format describing the version of Ip Desktop Softphone available at server side and its installation parameters:

```
# ------------------------#
# Upgrade                 #
# ------------------------#
ipdsp.version=13.4.0
ipdsp.download.url=https:/155.192.215.150/custom/IPDesktopSoftphone_13.4.0.msi
ipdsp.maximum.time.before.download=3600
ipdsp.maximum.download.attempts=3

# ------------------------#
# install options         #
# ------------------------#
ipdsp.install.option.PBXADDR= 155.192.215.150
ipdsp.install.option.BACKUPPBXADDR=155.192.215.151
ipdsp.install.option.AUTOSTARTUP=0
ipdsp.install.option.SUPERVISION=0
ipdsp.install.option.UPGRADEURL=https://155.192.215.150/custom/
```

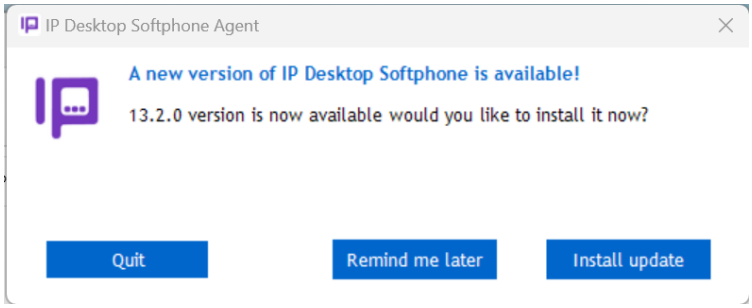
5.11.2 Ipdsp.info file properties description

Property Key	mandatory	default value	description
ipdsp.version	yes	N/A	Target version if the value is less than installed version the application is downgraded, else it is upgraded.
ipdsp.download.url	yes	N/A	download URL of the MSI installation file
ipdsp.maximum.time.before.download	no	0	maximum time (in seconds) before download start (ex: 0 => download immediately, 3600 => download will start 1 hour at most after new version has been detected
ipdsp.maximum.download.attempts	no	3	Maximum attempts number to download MSI file
ipdsp.install.option.PBXADDR=172.25.141.25 ipdsp.install.option.AUTOSTARTUP [… see chapter 5.2.3]	No, for upgrade. Yes, for downgrade		ipdsp.install.option.* must match an existing MSI parameter - if option is not specified IPDSP will keep existing value - if new parameter is introduced in the new version, the new value is applied

5.11.3 Update scenario

If the previous configuration is done by the administrator, the Application IP Desktop Softphone, at startup, downloads the file ipdsp.info from server via https, and compares installed version with parameter *ipdsp.version*. If different, the application will proceed to upgrade or downgrade itself:

- The MSI file of the parameter *ipdsp.download.url* is downloaded.
- If download succeeds, the user is prompted to proceed to update his application. User can choose to update immediately, or he can ask to be reminded later (6 hours by default).



- If the user confirms the action to update his IP Desktop Softphone application, the application is stopped, and the update starts.
- Once the application is updated, it is restarted.

5.11.4 Getnoeversion command

In OXE, the administrator can use the command “getnoeversion” to check the OS and the version of IP Desktop Softphone. The command can be used as follows: getnoeversion d <extension number>.
For example: getnoeversion d 21031
Where 21031 is the extension number to get information about.

```
(101)oxenla> getnoeversion d 21031
getnoeversion started 2023-06-28 at 13:40:16

+-----------------------------------------------------------------------------------------------------------------------------------+
| dir numb | in |  typ term      | dom |  serial number |  hardware version  |   code vers   | data vers  | rom | ram |
+-----------------------------------------------------------------------------------------------------------------------------------+
| 21031    | OK | IPT 8068s      |   0 | IPDSP          | Windows 11 Pro     |     13.4.7.0  | Unknown |   8 |   8 |
|                                                                                                                                   |
|      dotlx tls compatible no                                                                                                      |
|      dotlx certif  type   0                                                                                                       |
|      BOOTLOADER version Unknown                                                                                                   |
|      AOMEL detected                                                                                                               |
|          LOCALIZATION  : File name : jpn-4068              Version :  2.01.00                                                     |
+-----------------------------------------------------------------------------------------------------------------------------------+
getnoeversion ended 2023-06-28 at 13:40:16
(101)oxenla>
```

Or it can be used to get versions of all extensions and save the result to xml or csv file as follows: getnoeversion.

```
(101)oxenla> getnoeversion
getnoeversion started 2023-06-28 at 13:41:32
Begin the inventory of all Alcatel 8&9 Series phones registered on that node ?
Choose between 2 output file types (x for xml, c for csv, q to quit) (x/c/q) c
Getnoeversion Terminal Count starts 2023-06-28 at 13:42:54
Getnoeversion Terminal Count completed 2023-06-28 at 13:42:54
.. 83% achieved ..
 91% achieved ..
getnoeversion ended 2023-06-28 at 13:43:00
getnoeversion ... 5 extensions retrieved out of 6 requested (37 configured in management).
getnoeversion ... inventory file path is /DHS3dyn/mao/getnoeversion.csv.Z
getnoeversion.csv.Z                                                    100% 1028     1.0KB/s   00:00
Copy of inventory file on stand by cpu succeeded.
```

5.12 CRM interaction

This feature allows IP Desktop Softphone to launch an external application or a HTTP request on incoming, answered or released call events. Customer ca use this feature to automatically open a contact card in a web page or an external application (executable file) when receiving calls.

IP Desktop Softphone provides a properties file (ipdsp.manifest) to configure actions to be launched. These actions can be configurable with the caller name and caller number **(${caller.name}** and **${caller.phoneNumber}).**

5.12.1 ipdsp.manifest file

ipdsp.manifest file must be located under %PROGRAMDATA%\Alcatel-lucent Enterprise\IP Desktop Softphone\ folder (c:\programdata\Alcatel-lucent Enterprise\IP Desktop Softphone\).

The file is loaded at IP Desktop Softphone application startup. Restarting the application is necessary to reload ipdsp.manifest file if it is modified.

The format of the file is JSON:

```
{
        on-call-ringing-action: {
            filter: <filter value>
            command: {
                    url: <executable or HTTP URL>
                    params: <parameters of URL or exe file>
            }
        },
        on-call-answered-action: {
            command: {
                    url: <executable or HTTP URL>
                    params: <parameters of URL or exe file>
            }
        },
        on-call-released-action: {
            command: {
                    url: <executable or HTTP URL>
                    params: <parameters of URL or exe file>
            }
        }
}
```

5.12.2 ipdsp.manifest file properties description

Property Key	mandatory	default value	description
filter	no	“” (No filter)	Values can be (case-insensitive): • “” (empty) if no filter to be applied. • “Internal”: action to be applied for internal calls only. • “External”: action to be applied for external calls only
url	yes	N/A	HTTP URL or executable file to be launched. Since it's JSON, you have to consider that directory separators must be “/” or “\\”. Example: C:/Program Files (x86)/MicroCRM/bin/MicroCRM.exe Or C:\\Program Files (x86)\\MicroCRM\\bin\\MicroCRM.exe
params	no	“”	Parameters to add to HTTP request or executable (configurable with (**${caller.name}** and **${caller.phoneNumber}**)

ipdsp.manifest file example:

```
{
        "on-call-ringing-action": {
            "filter": "Internal",
            "command":{
                    "url": "C:/Program Files (x86)/MicroCRM/bin/MicroCRM.exe",
                    "params": "-first ${caller.name} -number ${caller.phoneNumber}"          }
        },
        "on-call-answered-action": {
            "command": {
                    "url": "http://www.linkedin.com/ANSWERED",
                    "params": "type=all&keywords=${caller.name}+${caller.phoneNumber}"
            }
        },
        "on-call-released-action": {
            "command": {
                    "url": "http://www.linkedin.com/RELEASED",
                    "params": "type=all&keywords=${caller.name}+${caller.phoneNumber}""
            }
        }
}
```

Note that this feature works well for a single incoming call, answered or abandoned.
However, there are usage restrictions, particularly for double calls in the case of multi-line extensions, because in some cases you may have either incorrect information or no event triggered.

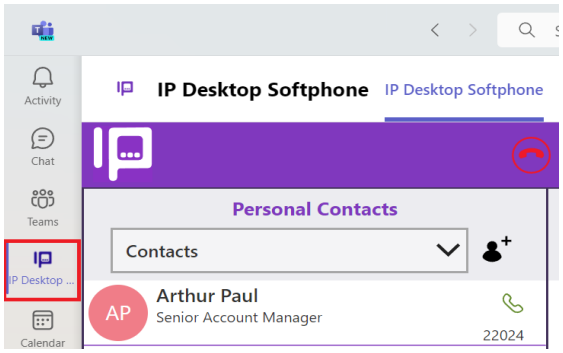
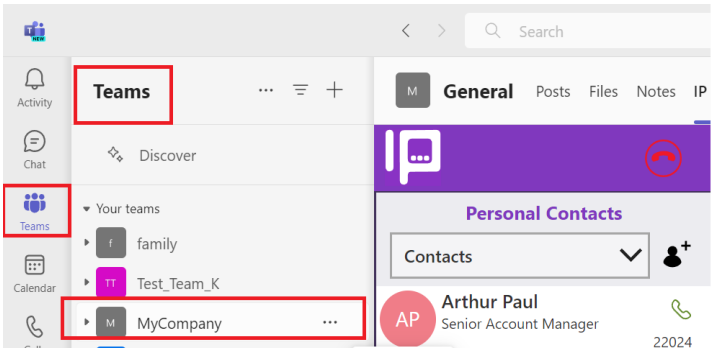
5.13 Microsoft© Teams integration

The IP Desktop Softphone provides an advanced level of services when associated with Teams.
It is recommended to install IP Desktop Softphone for PC with the appropriate option:
“USE_CONNECTOR_TEAMS” set to 1.

IP Desktop Softphone is integrated as Microsoft PowerApps. The administrator should install IP Desktop Softphone PowerApps and manage the IP Desktop Softphone team.

Access to the IP Desktop Softphone depends on how it is installed in the Teams environment.

The application can be installed in two different ways.

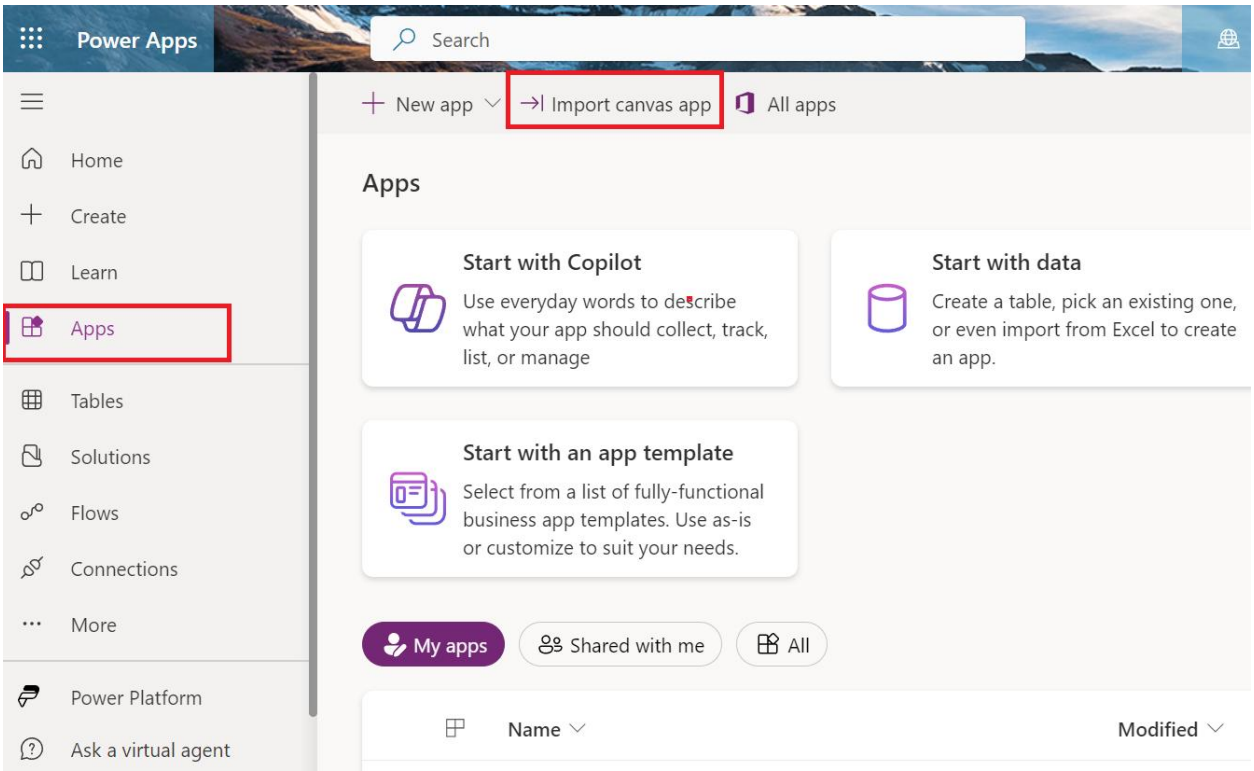
Teams app	Teams PowerApp
Once connected, the IP Desktop Softphone app is displayed in the Teams app area. 1. Select the IP Desktop Softphone app to open it. See paragraph 5.13.5	Once connected, open the team containing the IP Desktop Softphone PowerApp. 1. Open the Teams tab. 2. Select the team containing the IP Desktop Softphone PowerApp. See paragraph 5.13.4
	

This section describes how to set up the IP Desktop Softphone integration into Teams.
Firstly, it is recommended that only administrators should carry out this installation.

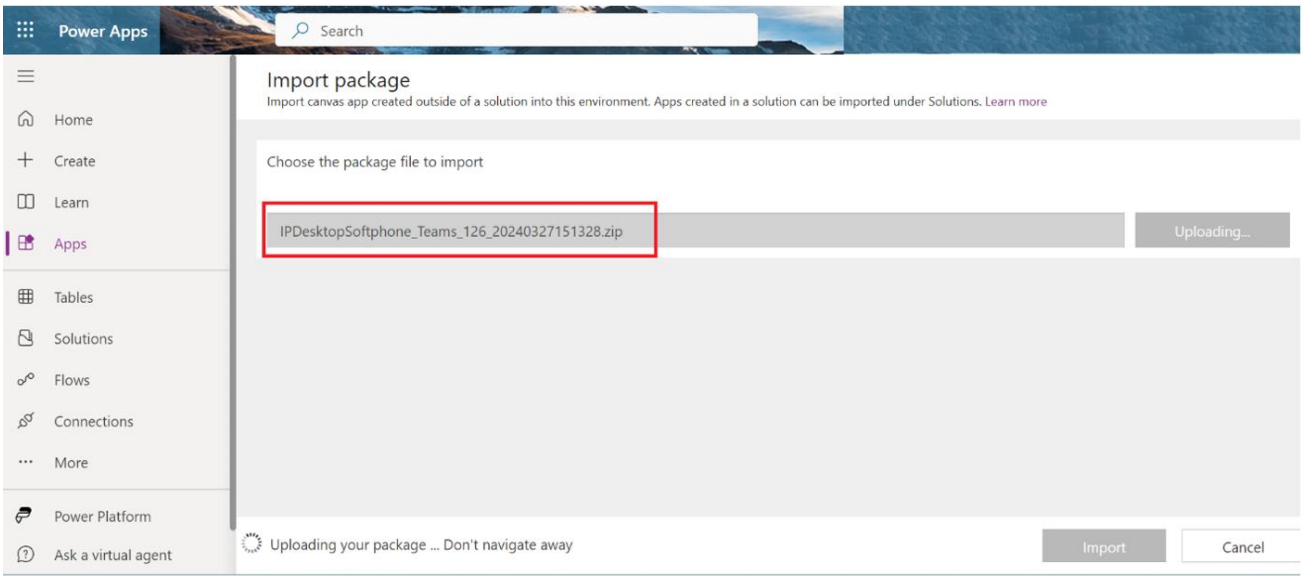
5.13.1 Importing IP Desktop Softphone canvas app package

To import the IP Desktop Softphone canvas app package, please follow the operations described below. (You can find more details in this link from the Microsoft site. https://learn.microsoft.com/en-us/power-apps/maker/canvas-apps/export-import-app)

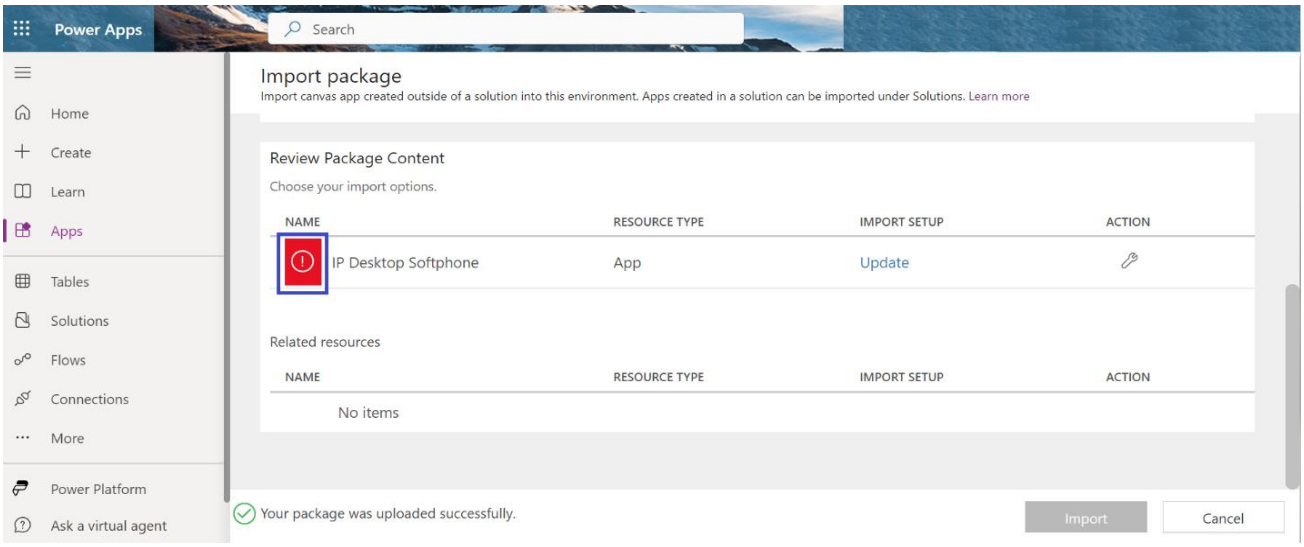
1. Open Power Apps in web browser: https://make.powerapps.com/
2. Click on “Apps” item on the left of the page.
3. Then click in “Import canvas app”.



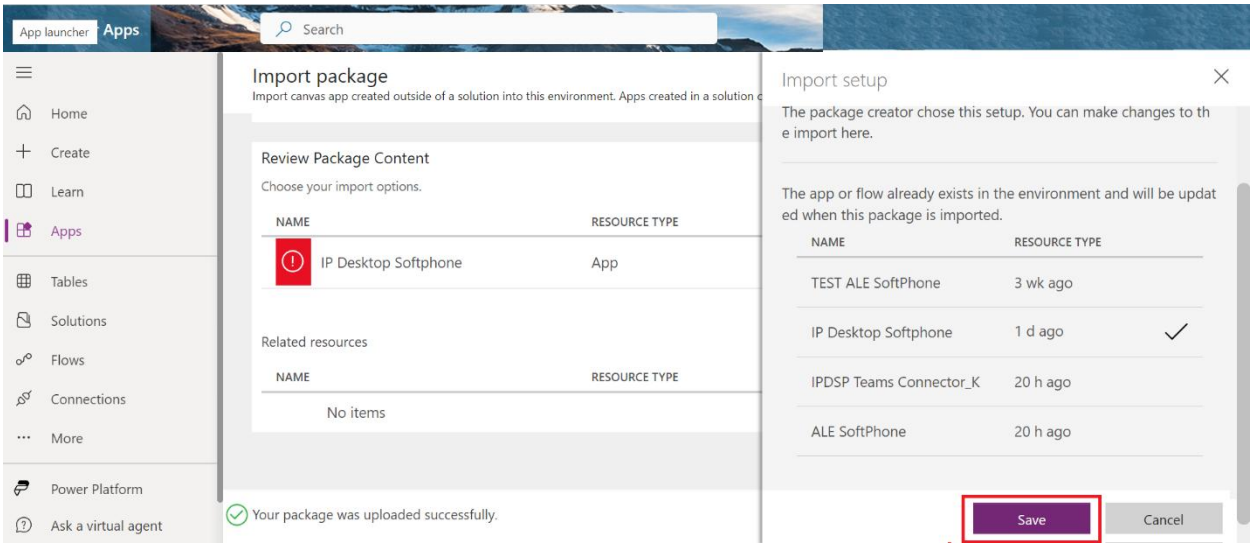
4. Browse the zip package file delivered to be imported.



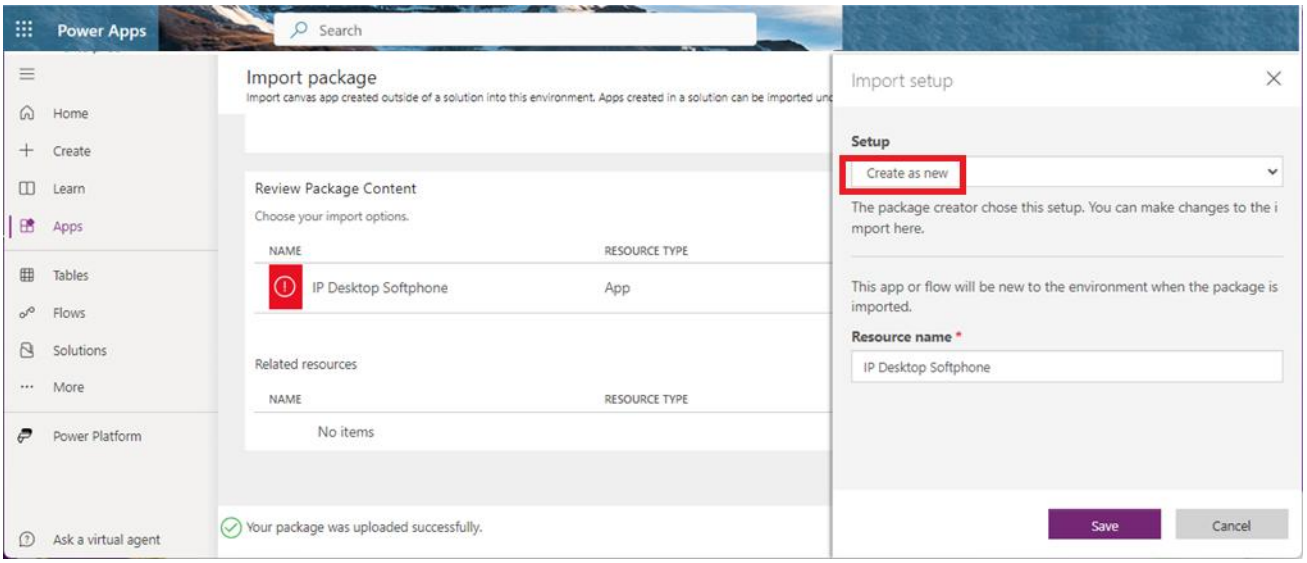
5. Click on the red icon.



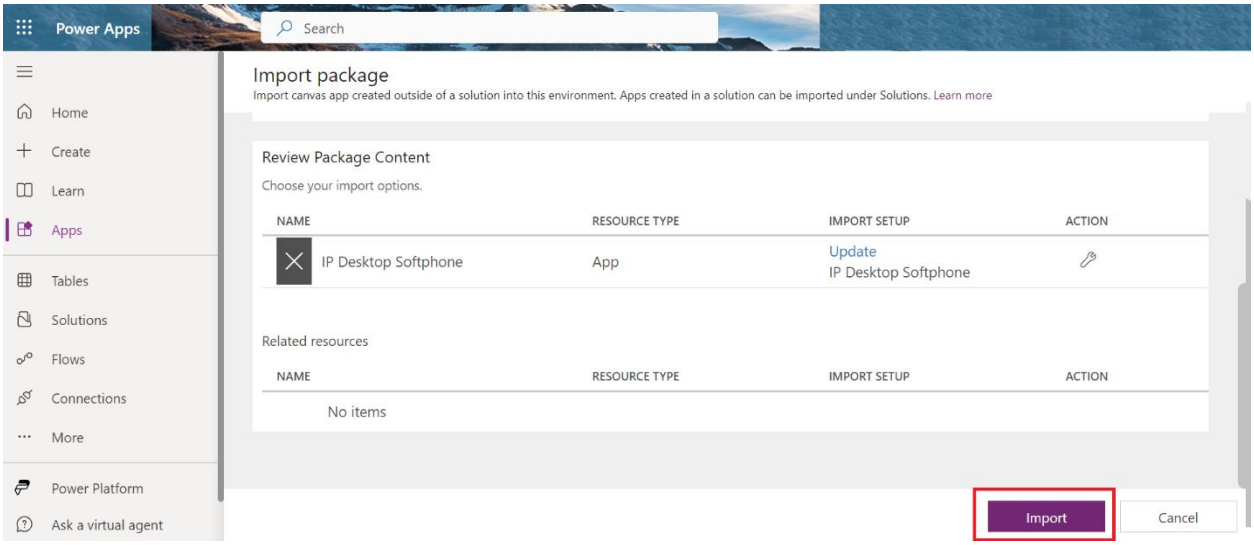
6. Choose the name of the application “IP Desktop Softphone” and click “Save” button.



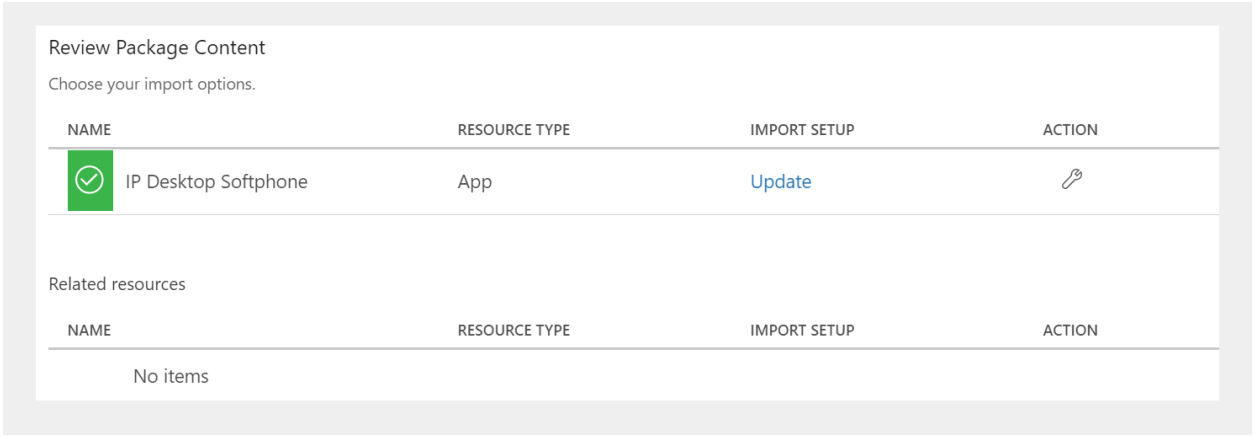
For the first installation, change the import setup from “Update” to “Create as new” and give the name “IP Desktop Softphone” and click “Save” button.



7. Now click on the “import” button.



The package is now well imported.



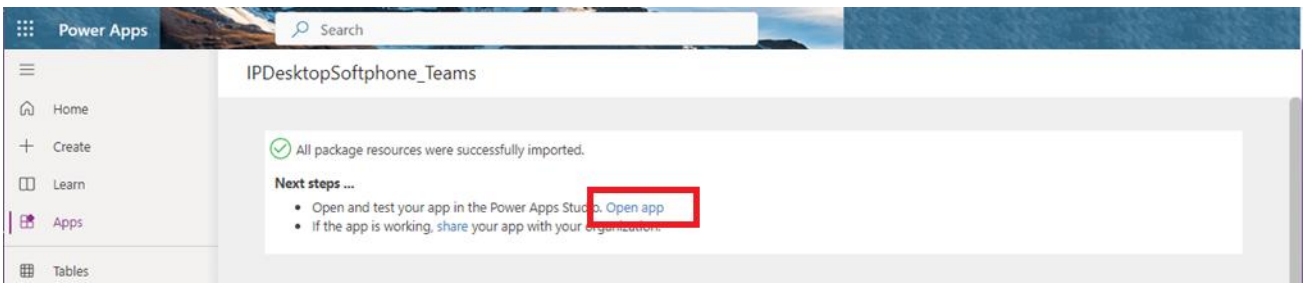
5.13.2 Publishing IP Desktop Softphone canvas app

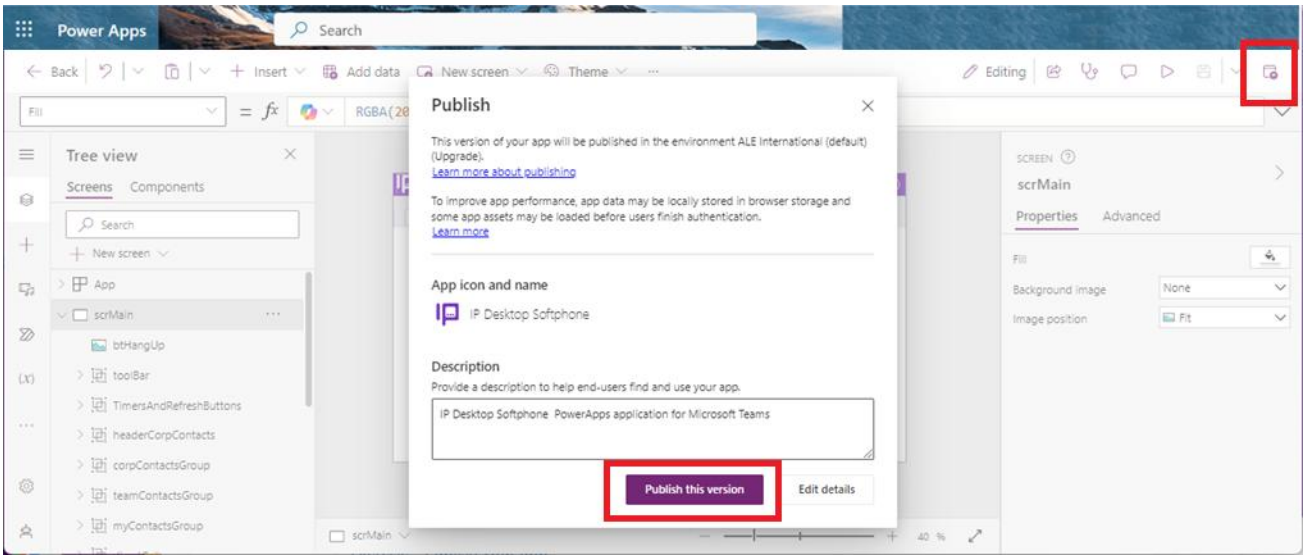
8. The next page is different for a first installation or an update:

For the first installation:
To publish the app: click on “Open app” and in Power Apps Studio click on publish icon.

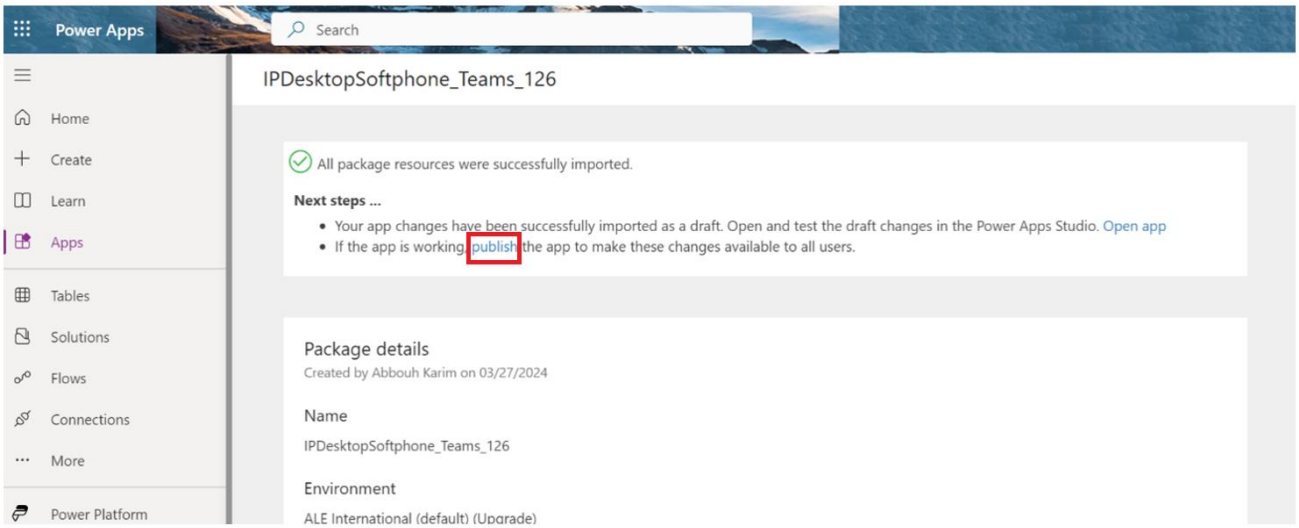
Validate authorizations upon opening.

And publish with the “Publish this version” button.

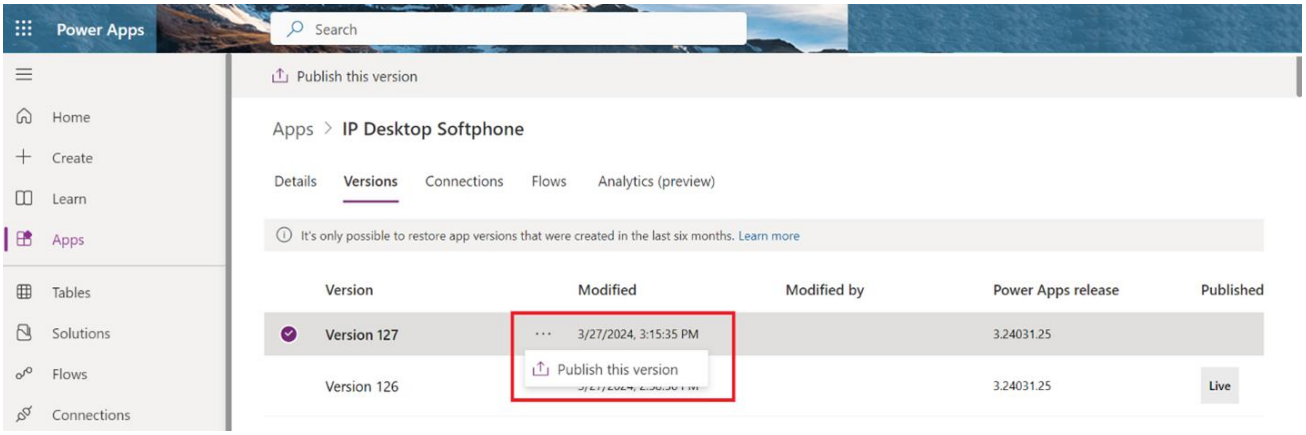




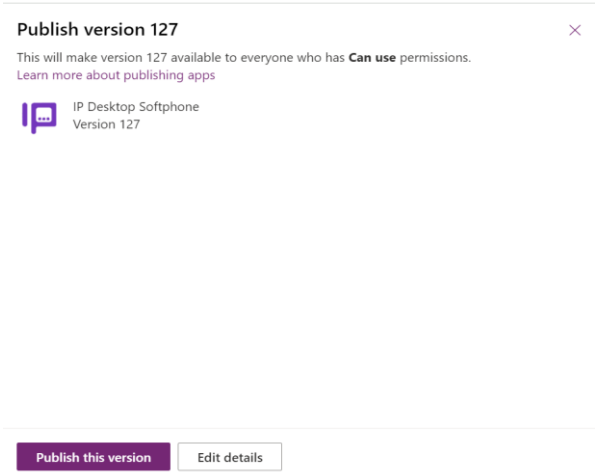
For an update:
Now click on the “Publish” highlighted word in this page.



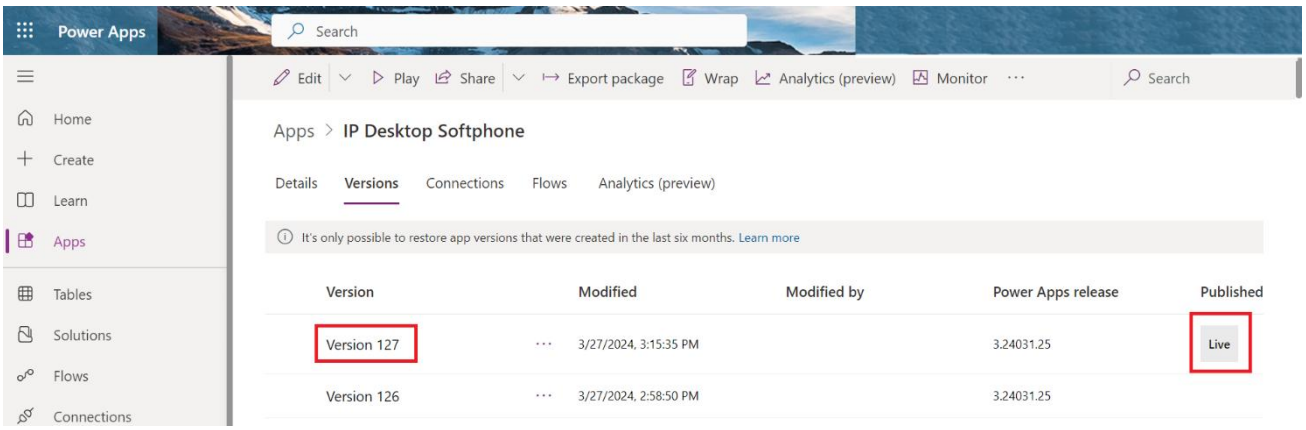
Click on the three points of the last version and press “Publish this version”.



And click on the “Publish this version” button.



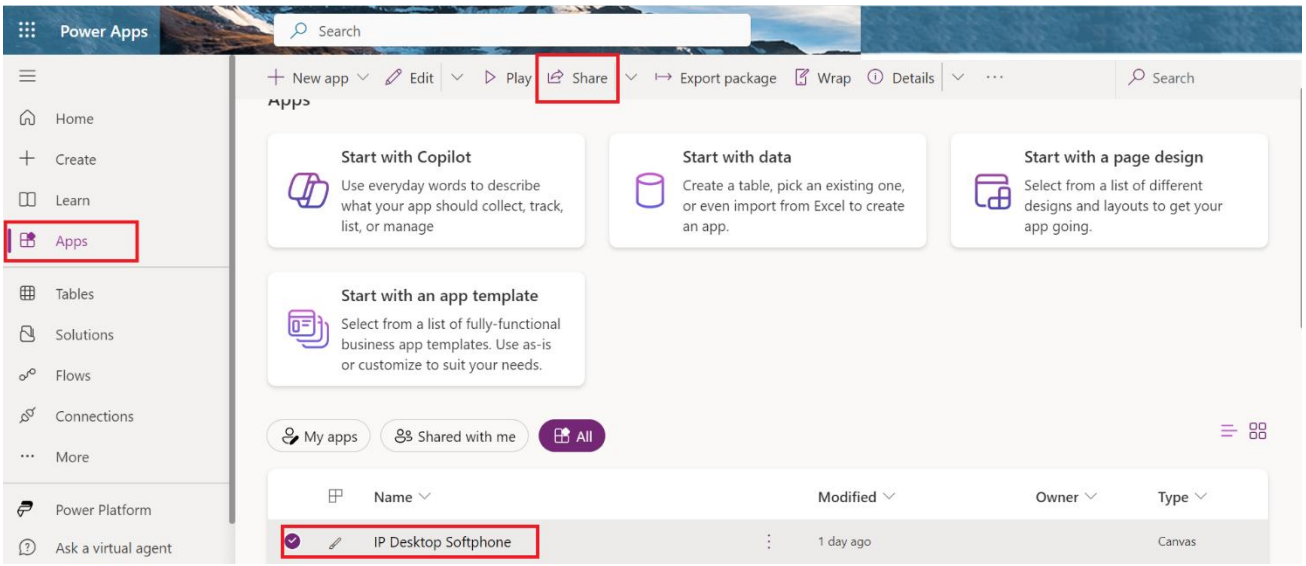
Now you can see that the version published is the one live.



5.13.3 Sharing IP Desktop Softphone canvas app

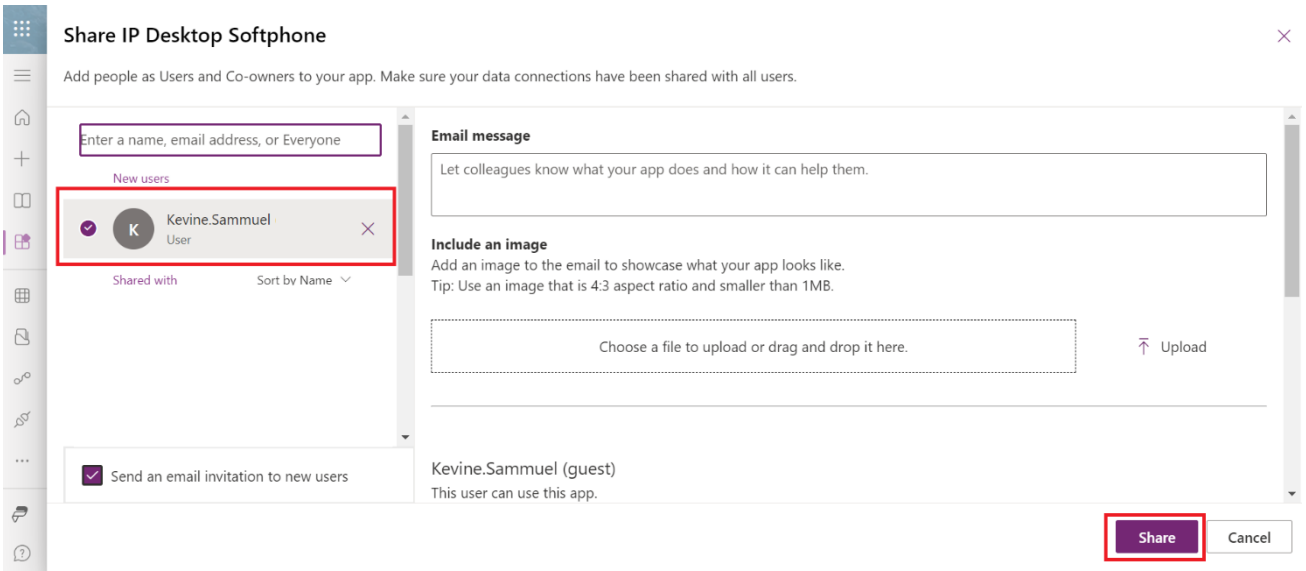
To share the application to other users, follow the operations bellow:
(you can find more descriptions in this link https://learn.microsoft.com/en-us/power-apps/maker/canvas-apps/share-app)

9. Open Power Apps in web browser: https://make.powerapps.com/
10. Click on “Apps” item on the left pane of the page.
11. Choose the IP Desktop Softphone from the list.
12. Click on the Share action in the toolbar.



13. Add people as Users and Co-owners to the application and check them.
    In this example we add “Kevine.Sammuel” user.

14. Click on the “Share” button.



Installation Procedure:

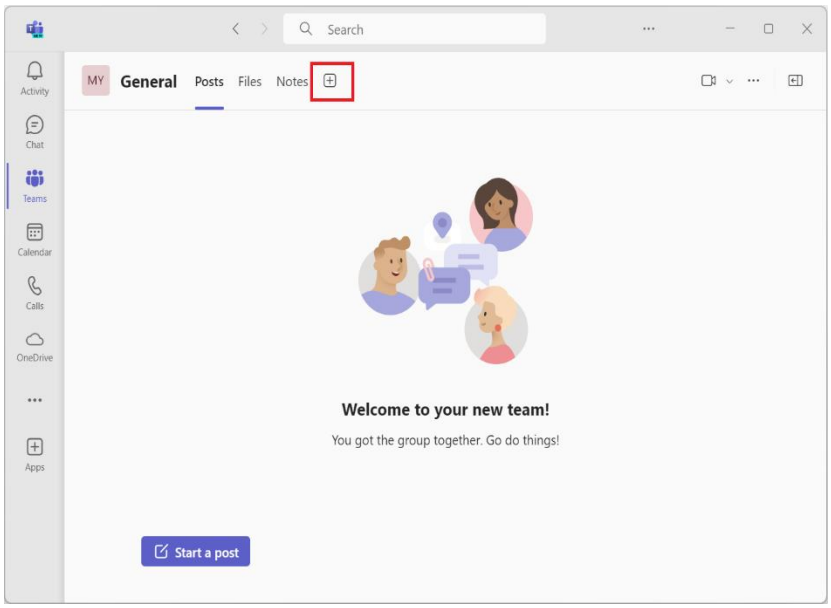
5.13.4 Installation as a Teams PowerApp

A PowerApp is an application that enables the way Teams behaves to be customized.
Installation requires certain rights and permissions.

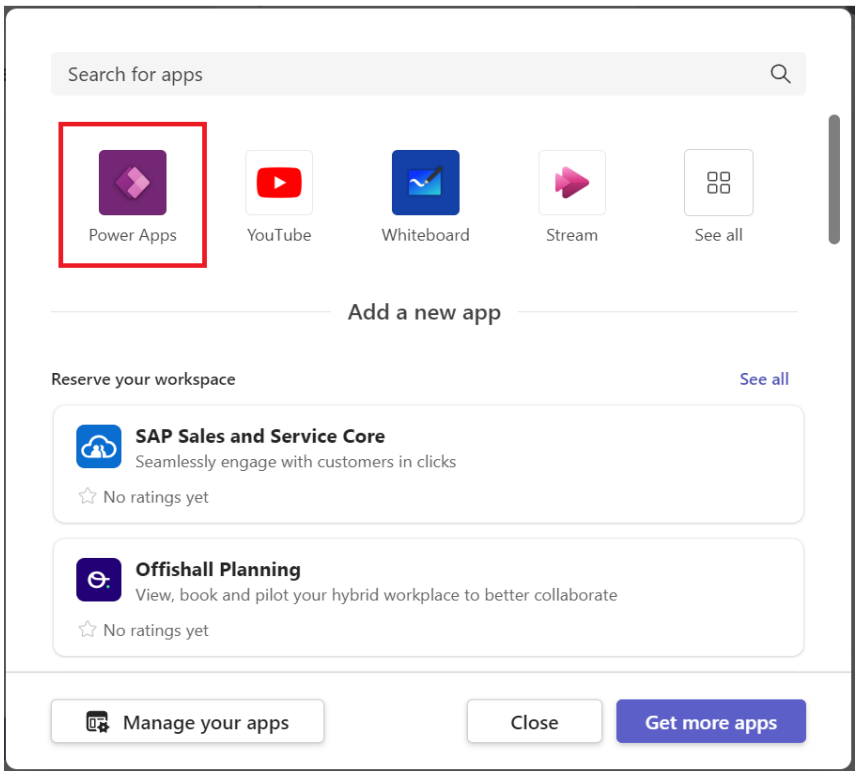
IP Desktop Softphone integration can be added to any number of teams.

Prerequisites: the IP Desktop Softphone PowerApp must be imported by your administrator into the Teams' environment using the PowerApps development tool (see previous paragraph).

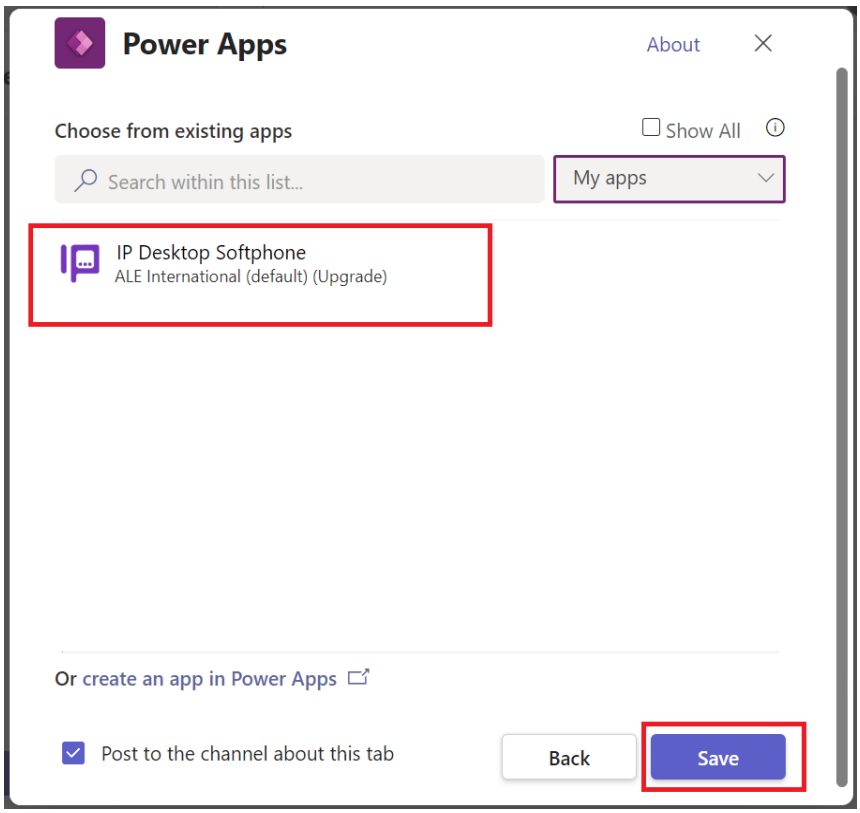
1. Open the team you want to add the IP Desktop Softphone PowerApp to.
2. Add a new tab by selecting this icon ⊞ :

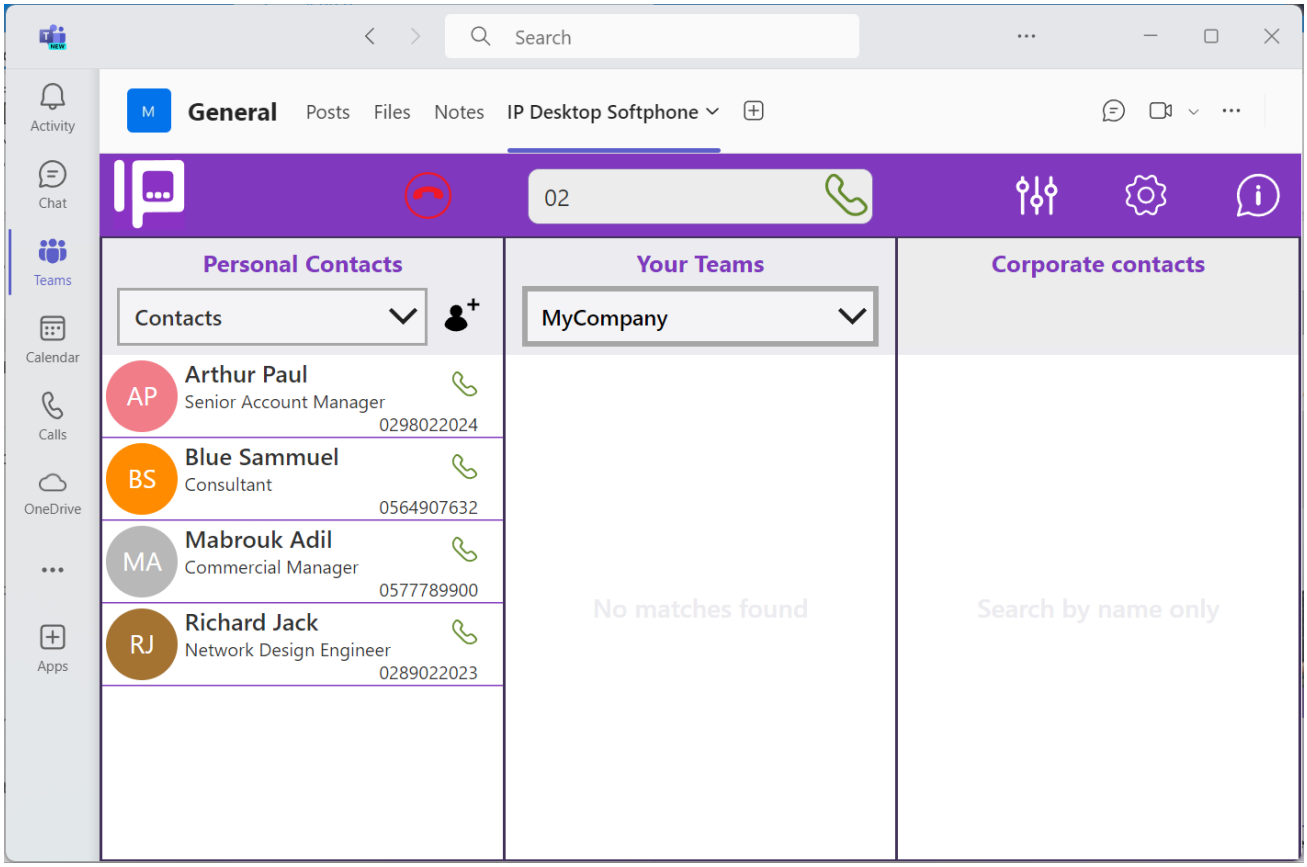


3. Open the PowerApps application
4. Add the IP Desktop Softphone PowerApp:



- Click the 'Add' button.
- Search the IP Desktop Softphone PowerApp.
- Select and save the PowerApp.





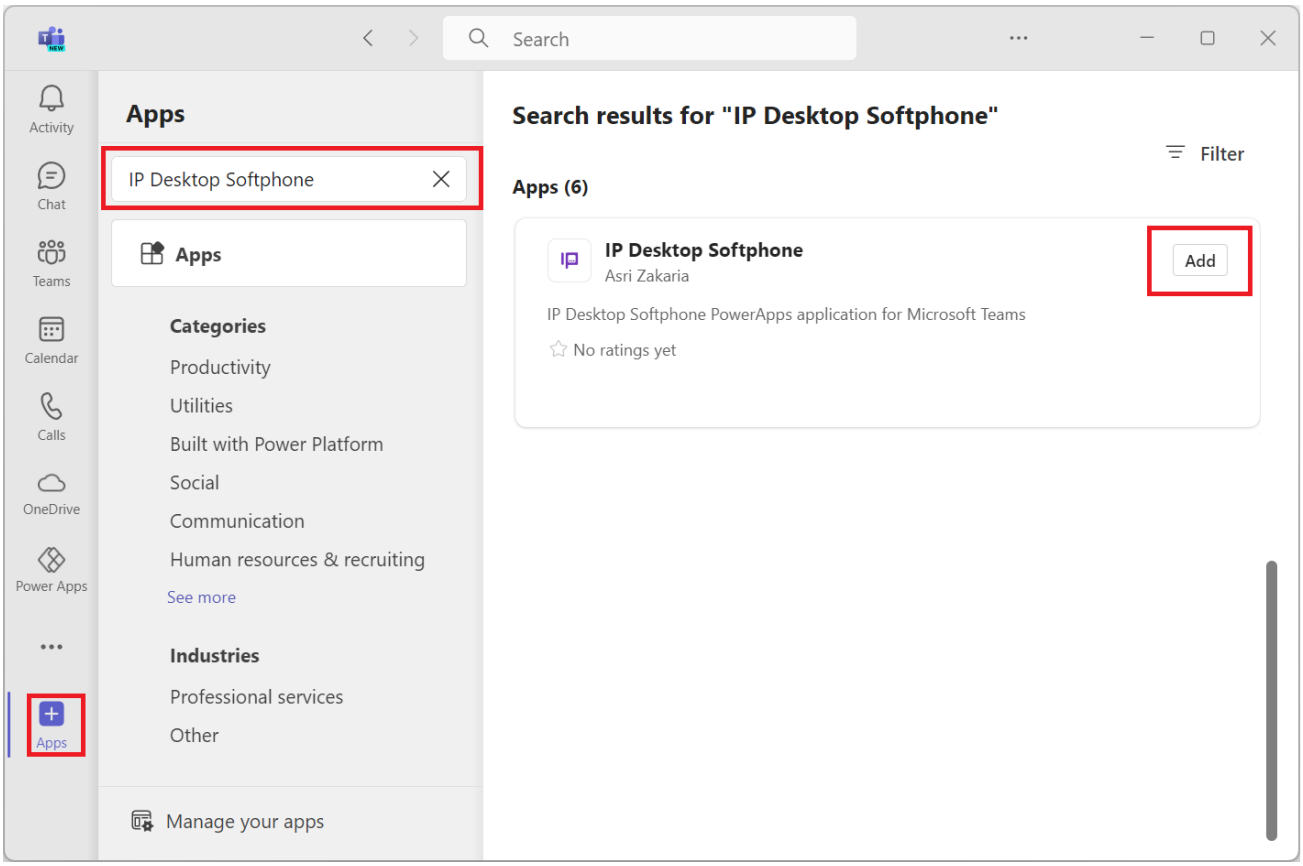
5.13.5 Installation as a Teams app

IP Desktop Softphone integration will be added into the Teams app area.
Prerequisites: the IP Desktop Softphone PowerApp should be provided to all company employees by the administrator.

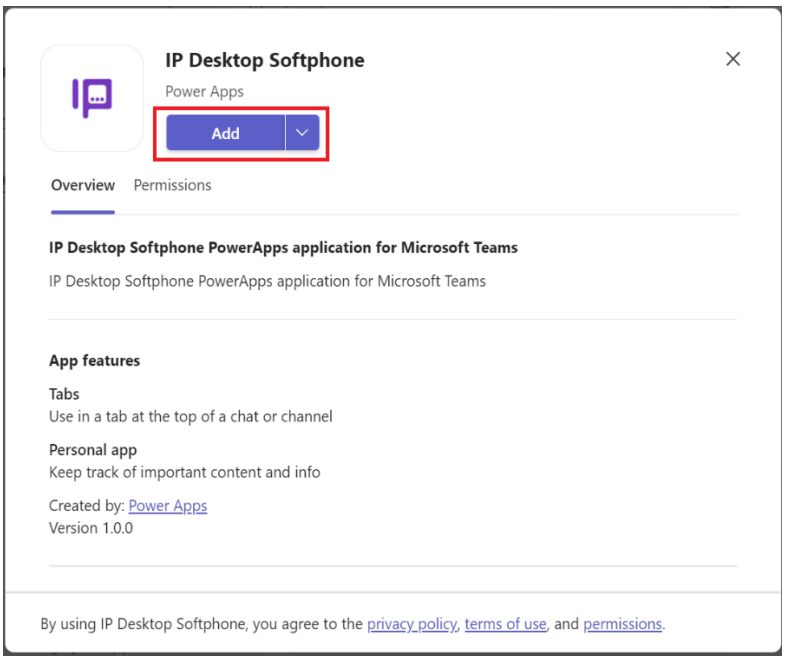
1. Open the Apps in Microsoft Teams to upload a custom app.
   You can choose to upload IP Desktop Softphone for either just you or your teams.

2. Select the IP Desktop Softphone app to upload. click the 'Add' button.

3. IP Desktop Softphone is installed as a Teams app. Do not forget to pin it.

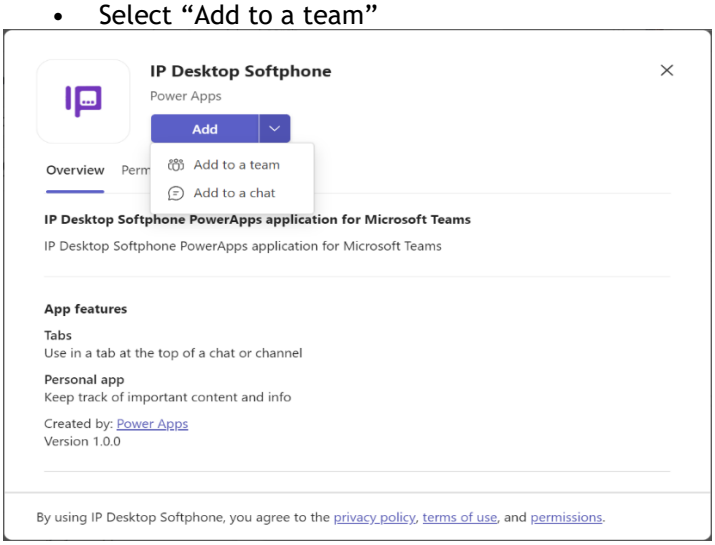


5.13.5.1 Installation as a Teams app for a user

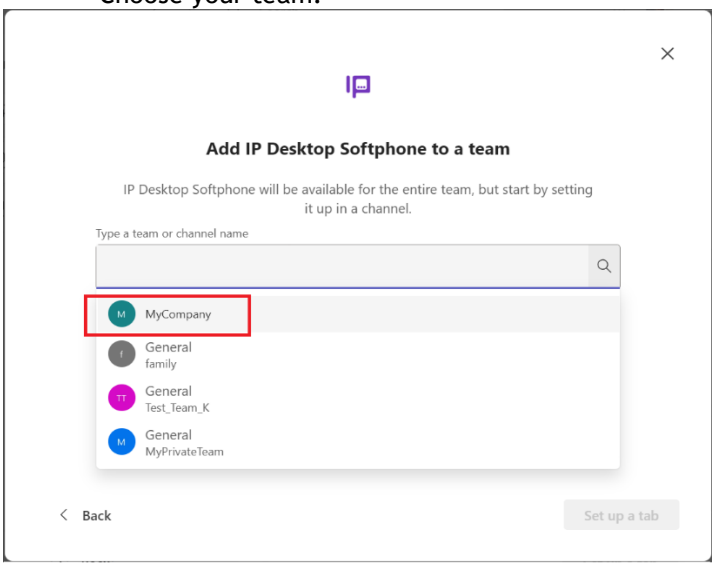


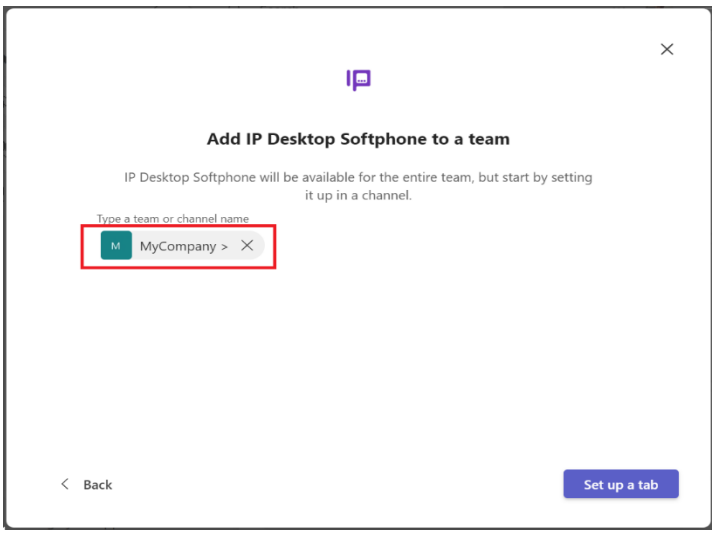
5.13.5.2 Installation as a Teams app for a team

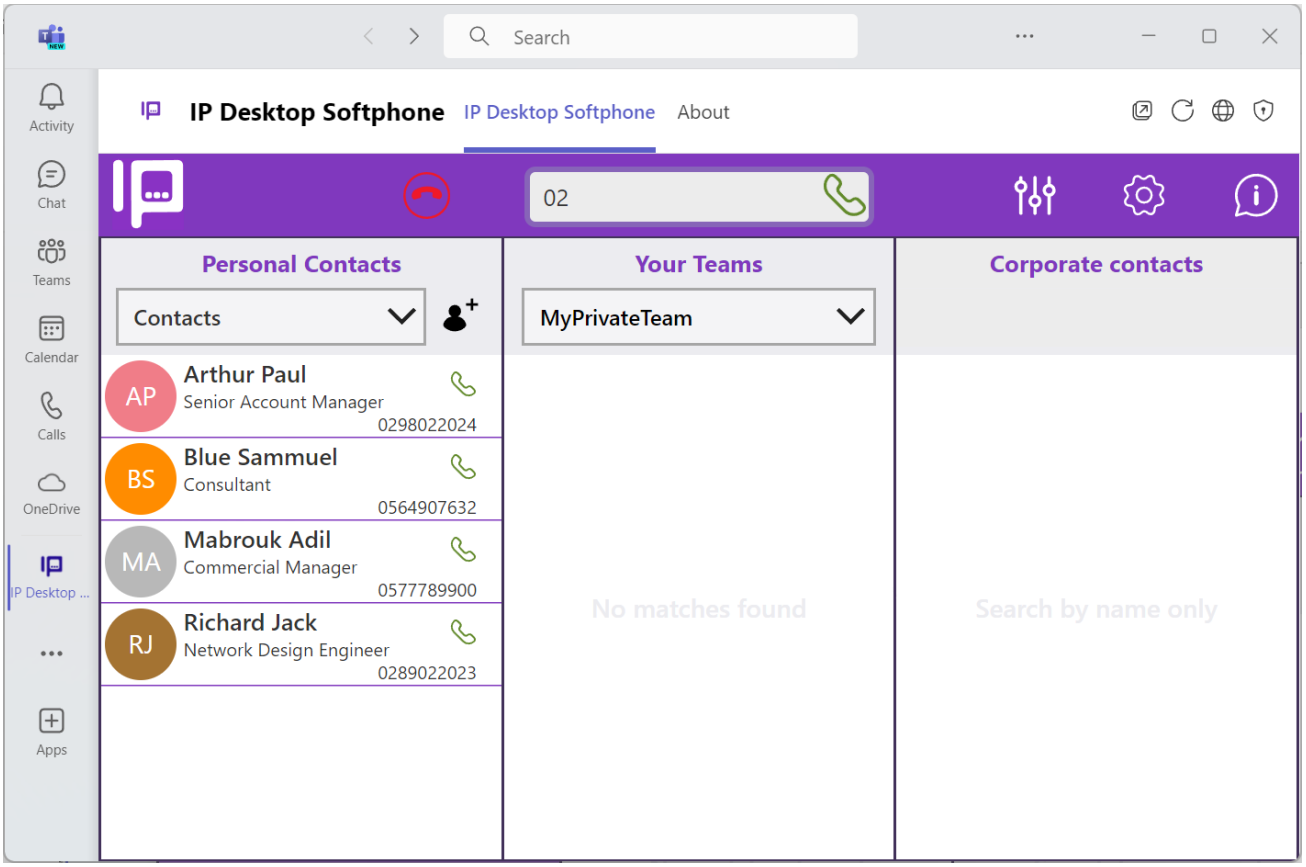
- Select “Add to a team”



- Choose your team.






Search
Activity
Chat
Teams
Calendar
Calls
OneDrive
IP Desktop ...
Apps
IP Desktop Softphone
IP Desktop Softphone
About
02
Personal Contacts
Contacts
Your Teams
MyPrivateTeam
Corporate contacts
AP
Arthur Paul
Senior Account Manager
0298022024
BS
Blue Sammuel
Consultant
0564907632
MA
Mabrouk Adil
Commercial Manager
0577789900
RJ
Richard Jack
Network Design Engineer
0289022023
No matches found
Search by name only

6. VDI Environment

6.1 VDI Feature

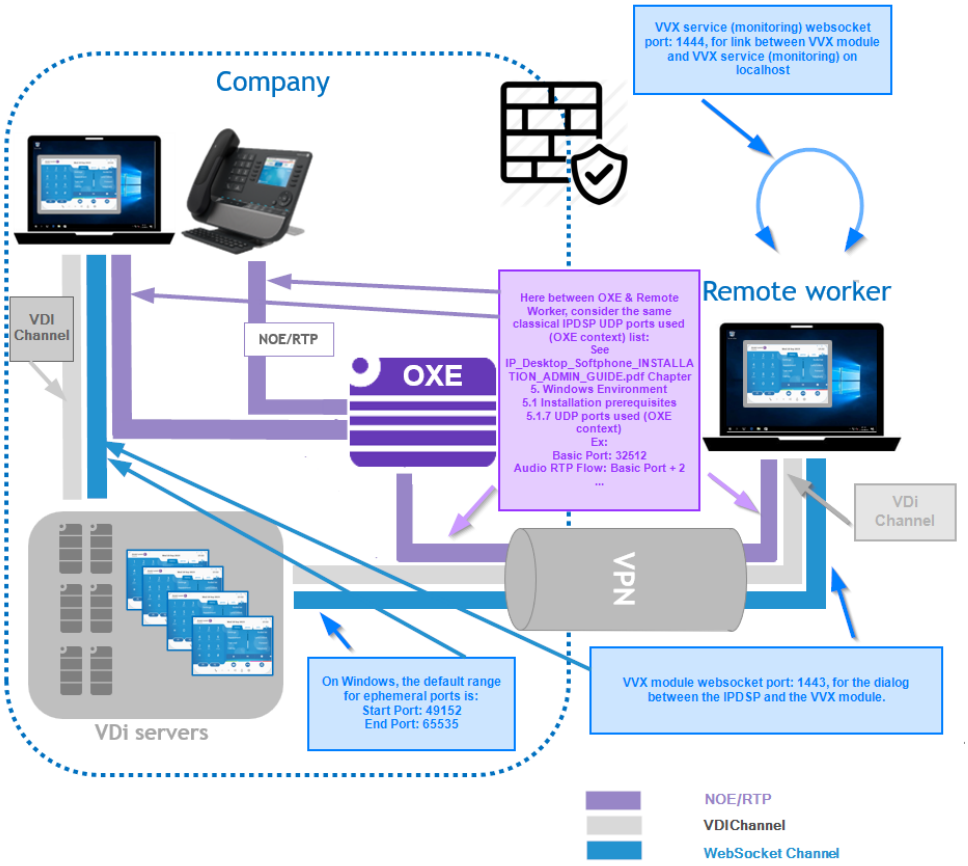
A VDI solution allows to display on a PC, applications or whole desktop running on a remote server. This type of infrastructure offers several advantages (deployment, updates, security, …)
A VDI solution is based on a server/client exchange done through a dedicated connection within which all flows required for applications are compressed and carried.
To summarize, an application runs on remote server and all media are carried to simulate a local application.

As of Release 12.0, IP Desktop softphone supports following VDI solution:

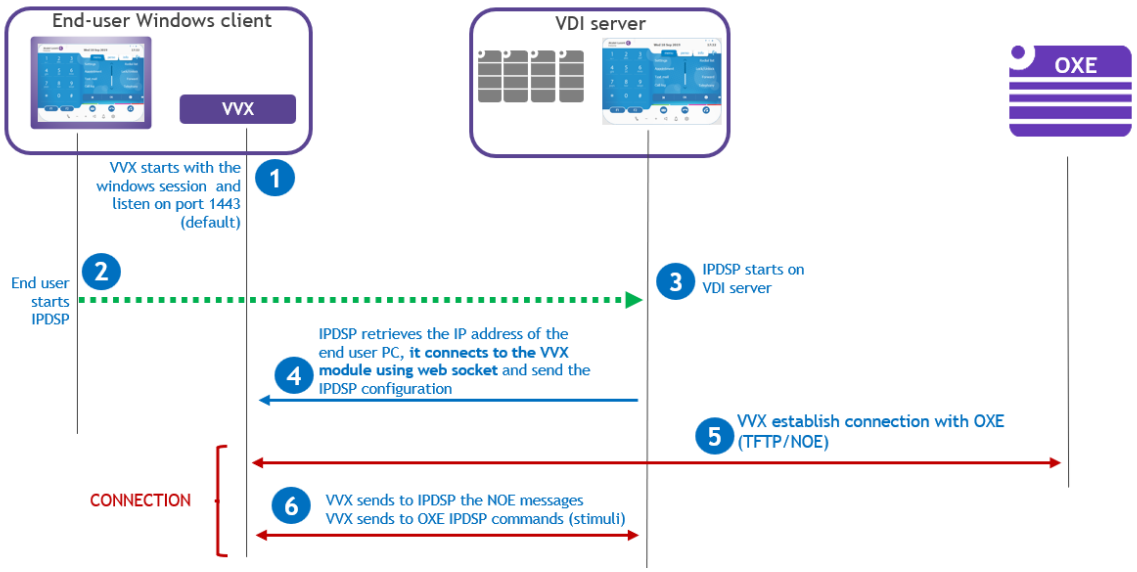
- Citrix Virtual App and Desktop 7

The extension module hosted on the end-user PC and named Virtual Voice eXtension (VVX) manages NOE and RTP protocols, ensuring quality and performance.
The dialog between the IPDSP running on the VDI server and the VVX module is done through an HTTPS link. It is used to send configuration values, manage event from network and USB (headset) …

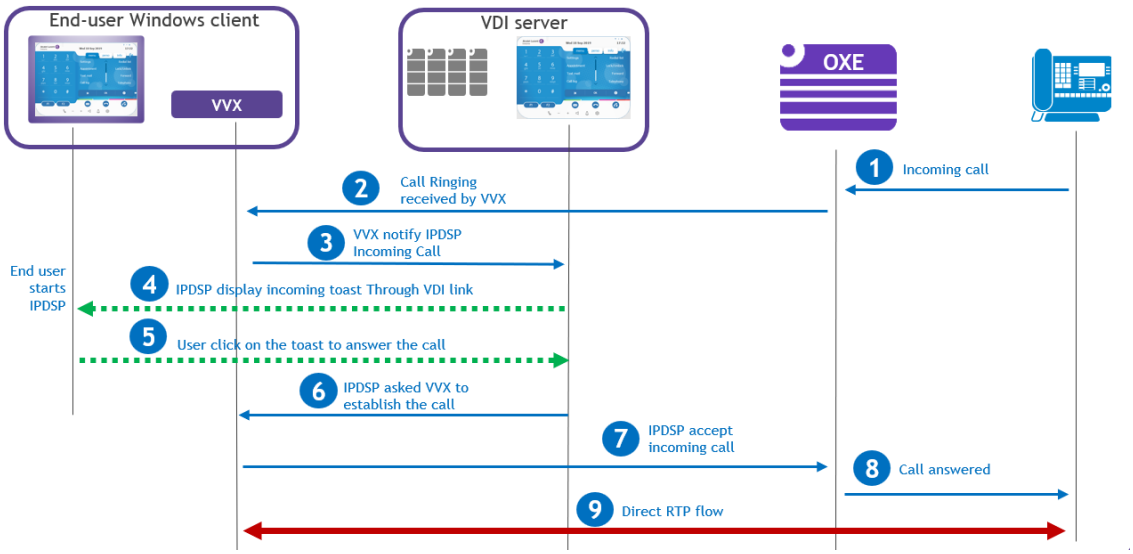
6.1.1 General Architecture



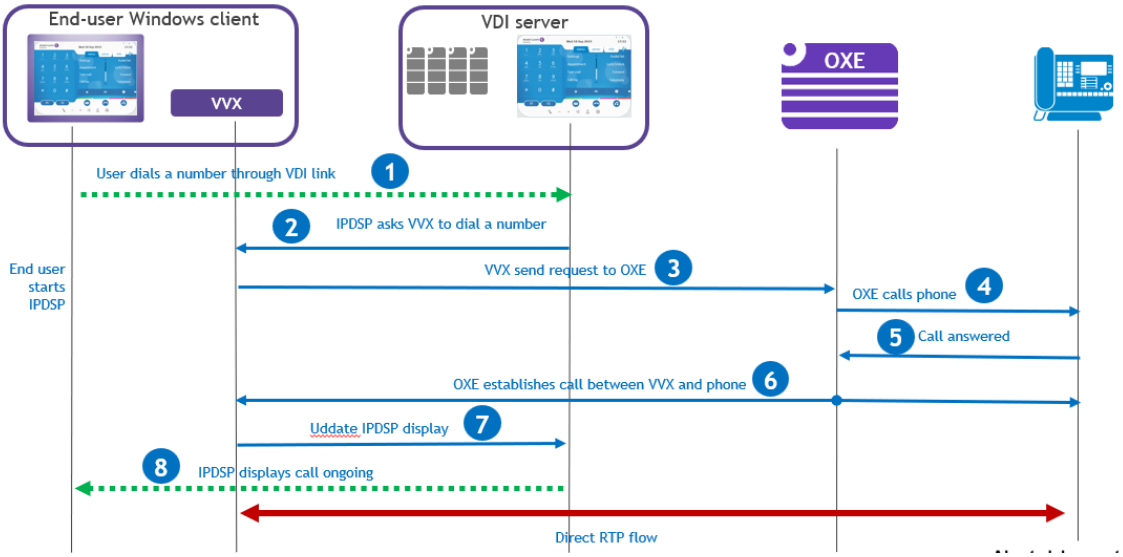
6.1.2 Starting IP Desktop Softphone



6.1.3 Incoming Call



6.1.4 Outgoing call



6.2 Installation prerequisites

The minimum requirements without which the application cannot function correctly are described below.

6.2.1 Hardware

Hardware prerequisite to install VVX module on user PC.

Processor	2 GHz Minimum
RAM	2 GB for Windows
Disk space	80 MB free space
Sound card	Integrated sound card or USB headset

6.2.2 Operating system

Please refer to the MLE_CrossCompatibility compatibility matrix. Contact your partner.

6.2.3 Networking

Network Interface card	Ethernet Card or Wireless LAN Card

6.2.4 VPN

Refer to the Windows section: VPN

6.2.5 .NET Framework

- The IP Desktop Softphone application requires Microsoft .NET Framework 4

To install Microsoft .NET Framework 4 (if not already installed) please visit:
https://www.microsoft.com/en-us/download/details.aspx?id=17851

- The VVX module requires Microsoft .NET Framework 4.6.1

To install Microsoft .NET Framework 4 (if not already installed) please visit:
https://www.microsoft.com/en-us/download/details.aspx?id=49981

6.2.6 Ports

The ports used by the application are identical to Windows and described below:
UDP ports used (OXE context),
TCP used ports (OXE context),
UDP used ports (OXO context)

Supplementary ports for VVX module:

- Websocket port: Default value is 1443, it can be changed.

Used for the dialog between the IPDSP and the VVX module.

- Service Socket port: Default value is 1444, it can be changed.

Socket port for link between VVX module and VVX service (monitoring).

6.3 Installation and upgrade procedures

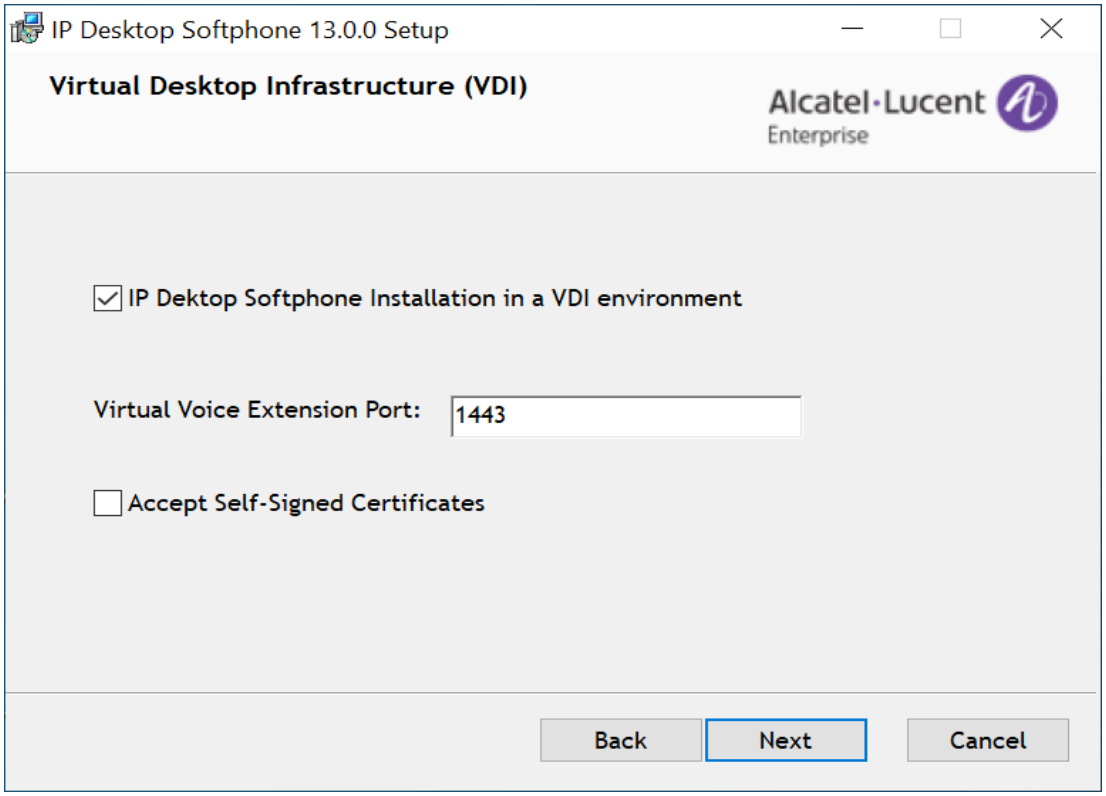
Installation of IP Desktop Softphone for VDI mode involves installing two msi files:

- IPDesktopSoftphone_13.0.x.msi deployed on VDI server
- SetupVVXserver_13.0.x.msi deployed on end-user PCs

6.3.1 Installation on VDI server

The **IPDesktopSoftphone_13.0.x.msi** is the same for installation of IPDSP in VDI mode or normal mode.

- For VDI mode, during installation the parameter “Virtual Server Mode” must be selected
- For the dialog between the IPDSP and the VVX module running on user PC, the “Virtual Server Port” must be set. The Same value is set on VVX module. Default value is 1443
- The check box (Accept-self-Signed certificates) is unchecked by default, it sets the level of security to the value 1, which indicates that IP Desktop Softphone will not accept WebSocket connection to VVX that has self-signed certificate. Check this box if the level of security is 0: Self-signed certificate is accepted to establish connection between IP Desktop Softphone and VVX.



- Installation in command line mode

From the command prompt, it is possible to install the IPDSP:

```
msiexec /i IPDesktopSoftphone_13.X.YY.msi
       VDI_MODE=<number> VDI_PORT=<number> VDI_SECURITY_LEVEL=<number> /qn
```

For the other parameters see the Windows sections: Installation in command line mode

SHAREDNUMBERMODE and MAC_ID are not recommended for use in case of VDI, because they can associate to all VDI users the same extension number.
It is recommended in case of an installation using command line to use silent mode(/qn).

Component	Description
msiexec	Microsoft command to execute file with 'msi' extension
/i	Optional setting for Status Messages. For more of such options, you can key in the following at command prompt: msiexec /i
IPDesktopSoftphone_13.X.YY.msi	Name of file that is to be executed.
VDI_MODE=<number>	Select the VDI mode or Normal mode The possible values are: • 0 Normal mode (default value) • 1 VDI mode

Component	Description
VDI_PORT=<number>	"Virtual Server Port": For the dialog between the IPDSP and the VVX module running on user PC. The Same value must be set on VVX module. Default value is 1443
VDI_SECURITY_LEVEL=<number>	This value indicates the level of security when IP Desktop Softphone establishes WebSocket connection with VVX. The possible values are: • 1: indicates that IP Desktop Softphone will not accept establishing WebSocket connection with VVX that has self-signed certificate. This is the default value. • 0 (low security level): indicates that IP Desktop Softphone will accept establishing WebSocket connection with VVX that has self-signed certificate.
/qn	Option to launch installation using command line in silent mode.

For example:

```
msiexec /i IPDesktopSoftphone_13.4.0.msi PBXADDR=155.192.215.150 VDI_MODE=1
VDI_PORT=1443 VDI_SECURITY_LEVEL=0 /qn
```

When updating the same version as the installed version (to modify the installation settings for example), execute the command by adding the **/famv** option to force the taking into account of the new values.

```
msiexec /famv IPDesktopSoftphone_13.X.YY.msi VDI_PORT=<number> /qn
```

In case of upgrade, only parameters which are expressed in command line take a new value. All other parameters are unchanged.
It is recommended in case of an update using command line to use silent mode(/qn).

By default, the configuration files are located in:

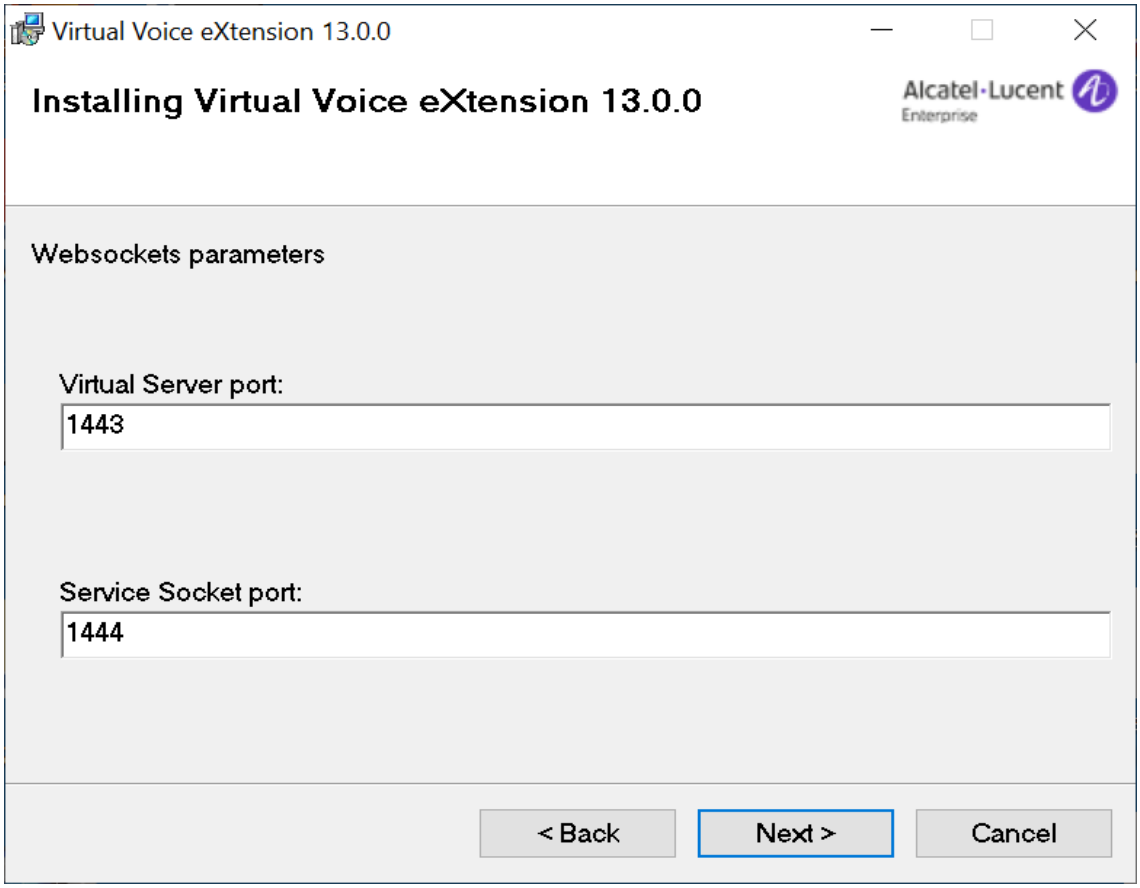
C:\Users\<user name>\AppData\Roaming\Alcatel-Lucent Enterprise\IP Desktop Softphone\config

6.3.2 Installation on User PC

For the first installation, run the file **SetupVVXserver_13.0.x.msi** to install the VVX module on the user PC.

- **Follow the instructions on the screen step by step:**

  1. **Read carefully and accept the license agreement**
  2. **Change the installation location if necessary**
  3. **Change the connection parameters to VDI server if necessary**



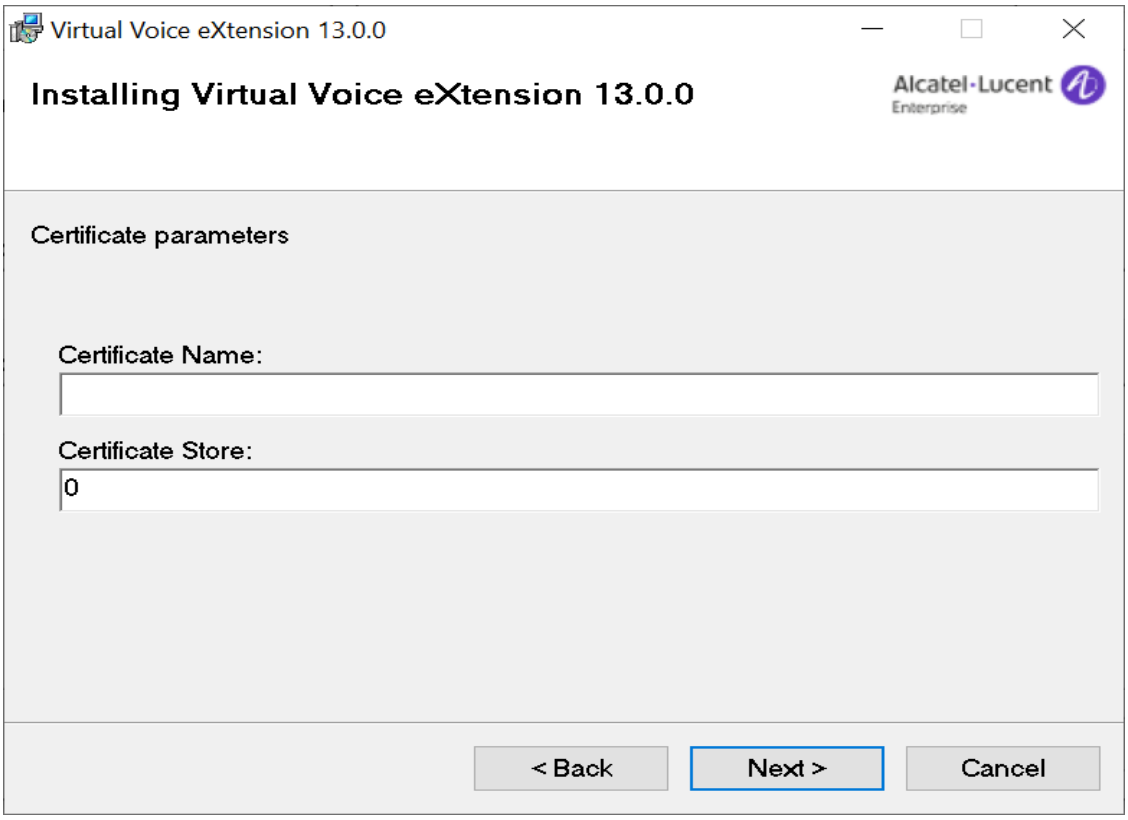
The “Virtual Server port” value must be set to the same value set in VDI server. Default value is 1443.

4. Fill the Certificate parameters

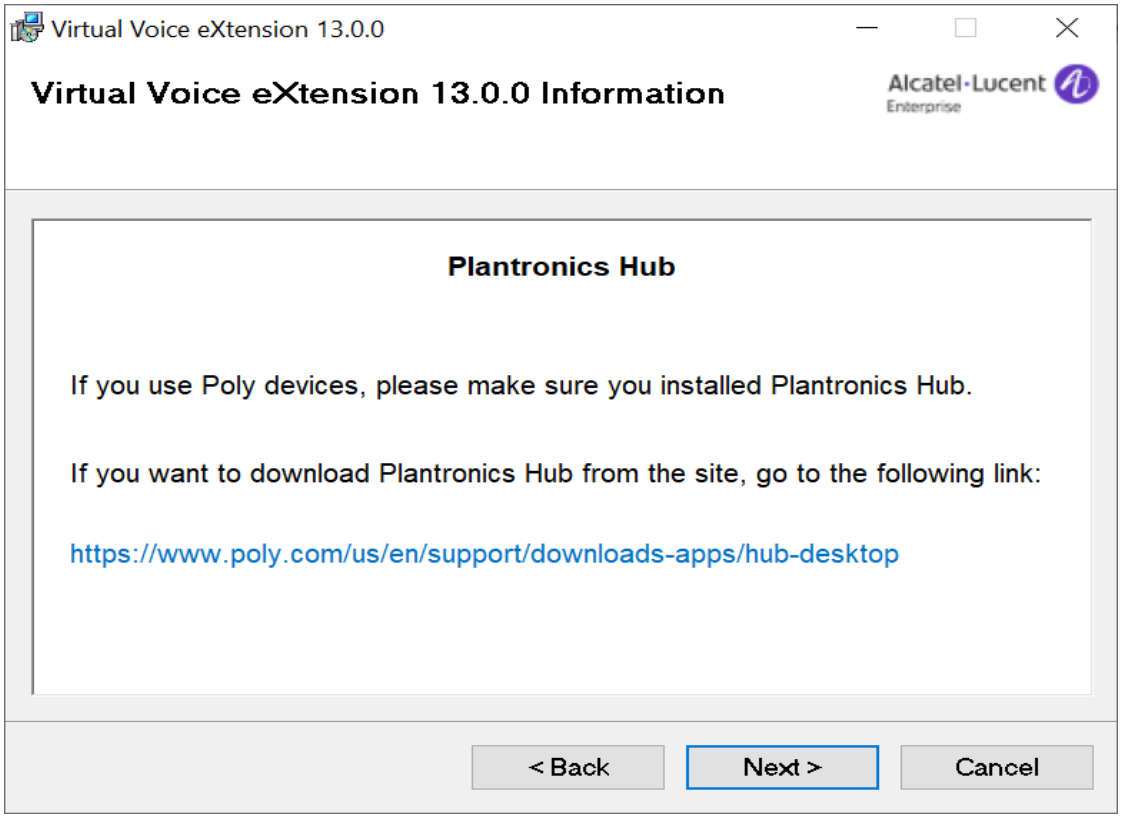
Fill in the "Certificate name". (CN value in the certificate subject field). If this field is kept empty or filled with a value that is not present in the store, the VVX will create a self-signed certificate for the WebSocket.
The "Certificate Store (Web Socket)" parameter must be filled with the value corresponding to the store used:

- Value 0 for the "Personal" store.
- Value 1 for the "Trusted Root Certificate Authorities" store.
- Value 2 for the "Trusted Publishers" store.

NB: The stores used are the Computer account stores, and not User account ones.

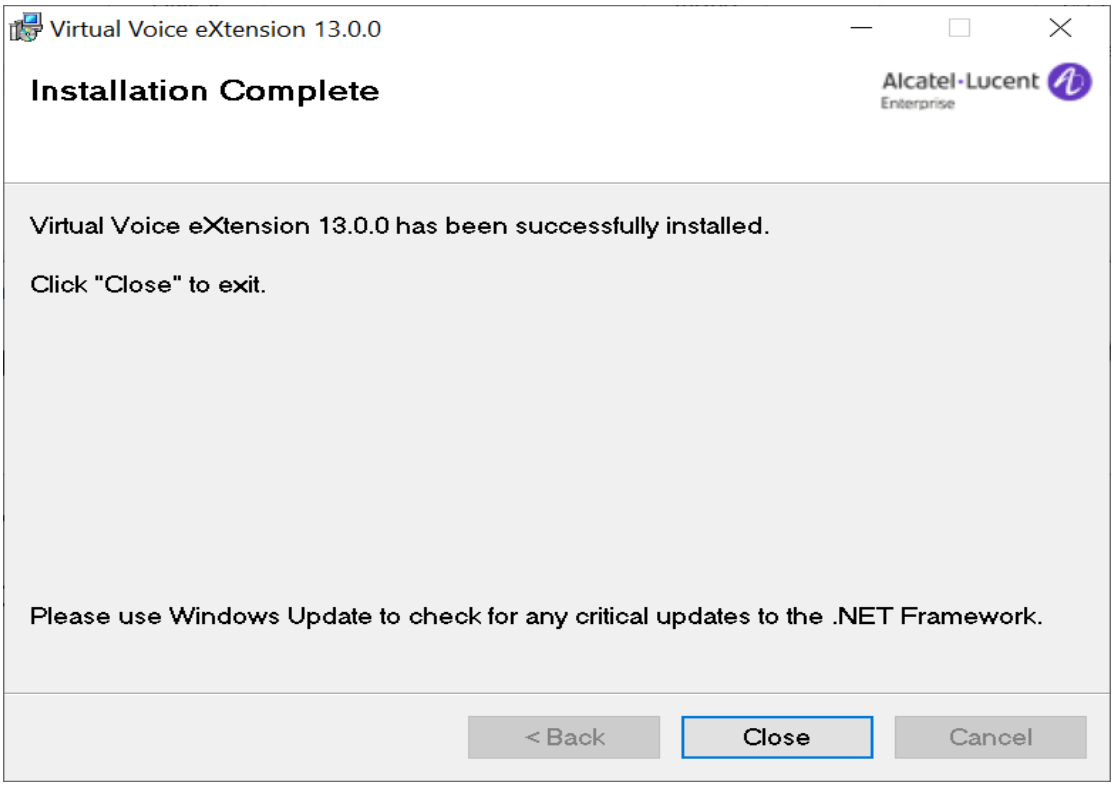


5. **Notice for Plantronics Hub**



6. **You can install Plantronics hub now or after the end of installation**
7. **Click Next to install VVX module**
8. **Click Close to exit,**

The VVX module is installed and is started automatically by the VVX service (named VVXService)



Field Name	Description
Virtual Server port	“Virtual Server port” is a Websocket for the dialog between the IPDSP and the VVX module. The Same value must be set on the two parts. Default value is 1443.
Service Socket port	Value of socket port for link between VVX module and VVX service (monitoring). Default value is 1444.
Certificate Name	Certificate name for secure connection. (CN value in certificate subject field) If empty, the VVX will create a self-signed certificate.
Certificate Store	The "Certificate Store" (Web Socket) parameter must be filled with the value corresponding to the store used (Computer account): • Value 0 for the "Personal" store. • Value 1 for the "Trusted Root Certificate Authorities" store. • Value 2 for the "Trusted Publishers" store.

- Installation in command line mode

From the command prompt, it is possible to install the VVX module:

```
msiexec /i SetupVVXserver_13.X.YY.msi
       LOCAL_WS_PORT=<number>
       SERVICE_PORT=<number>
       CERT_NAME=<name> CERT_STORE=<store> /qn
```

Component	Description
msiexec	Microsoft command to execute file with 'msi' extension
/i	Optional setting for Status Messages. For more of such options, you can key in the following at command prompt: msiexec /i
SetupVVXserver_13.X.YY.msi	Name of file that is to be executed.
LOCAL_WS_PORT=<number>	"Virtual Server Port" (Websocket port): For the dialog between the IPDSP and the VVX module running on user PC. The Same value must be set on VVX module. Default value is 1443
SERVICE_PORT=<number>	Value of socket port for link between VVX module and VVX service (monitoring). Default value is 1444.
CERT_NAME=<name>	Certificate name for secure connection. (CN value in certificate subject field). If this field is not present, VVX will create a self-signed certificate.
CERT_STORE=<store>	The "Certificate Store" (Web Socket) parameter must be filled with the value corresponding to the store used (Computer account): • Value 0 for the "Personal" store. • Value 1 for the "Trusted Root Certificate Authorities" store. Value 2 for the "Trusted Publishers" store.
/qn	Option to launch installation using command line in silent mode.

When updating the same version as the installed version (to modify the installation settings for example), execute the command by adding the **/famv** option to force the taking into account of the new values.

```
msiexec /famv SetupVVXserver_13.X.YY.msi LOCAL_WS_PORT=<number> /qn
```

In case of upgrade, only parameters which are expressed in command line take a new value. All other parameters are unchanged.

It is recommended in case of an update using command line to use silent mode(/qn).

6.4 Launching the application

To start the softphone, use the shortcut of the application created during the installation on the VDI server (used as application or in whole desktop)

Or access the application from the start menu.

Upon first startup, it is necessary to fill in the connection information to the OXE or OXO telephony server. This information is configurable from Settings: Network tab

6.4.1 Application Monitoring

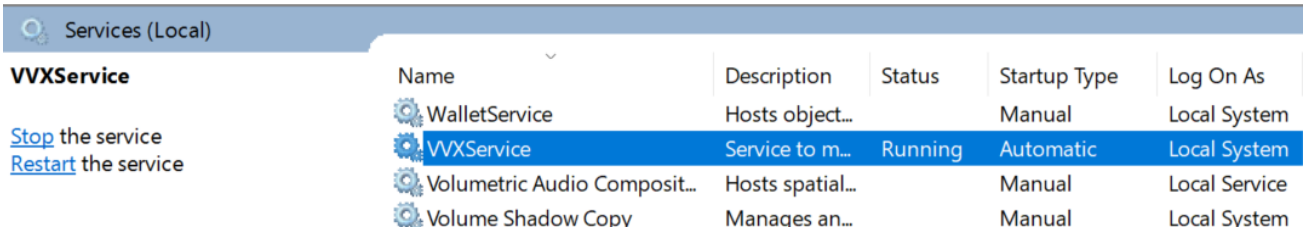
- **Monitoring for IP Desktop Softphone on VDI server:**

A monitoring system for IP Desktop Softphone is activated when the application starts. This will restart the IP Desktop Softphone automatically if the application freezes or unexpectedly stops.
Supervision is disabled when the IP Desktop Softphone is normally stopped.

- **Monitoring for VVX module on User PC:**

A service process 'VVXService' is in charge of monitoring the VVX, it is started at the installation of the VVX module. It launches the VVX automatically.
VVX module is always 'Running', VVXService will restart VVX automatically if it freezes or unexpectedly stops.

To stop VVX module, go to Windows "Service application" and stop "VVXService"



6.4.2 Registration

The registration procedures are identical to those described in the Windows sections:

- Registration in OXE context

- Registration in OXO context

6.5 Configuration of Application

Customize the application to suit your existing environment.

Only the administrator settings are documented in this section.
All settings are detailed in the user manual.

The configuration is identical to those described in the Windows sections: Configuration of application

6.6 Upgrade procedure

Only the IPDesktopSoftphone must be upgraded on VDI server.

if required, VVX is automatically updated on next connection.

6.7 Uninstalling

6.7.1 Uninstalling of IPDesktopSoftphone on VDI server

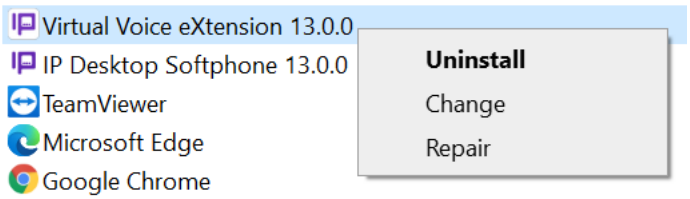
Close the application before starting the uninstallation process.

The process is identical to those described in the Windows sections: Uninstalling

6.7.2 Uninstalling of VVX module on User PC

To uninstall the application from Windows:

Open Control Panel: Control Panel\Programs\Programs and Features, select “Virtual Voice eXtension X.Y.Z” and click “Uninstall”.



6.7.3 Uninstalling Using: .msi File from command prompt

msiexec /x IPDesktopSoftphone_13.X.YY.msi

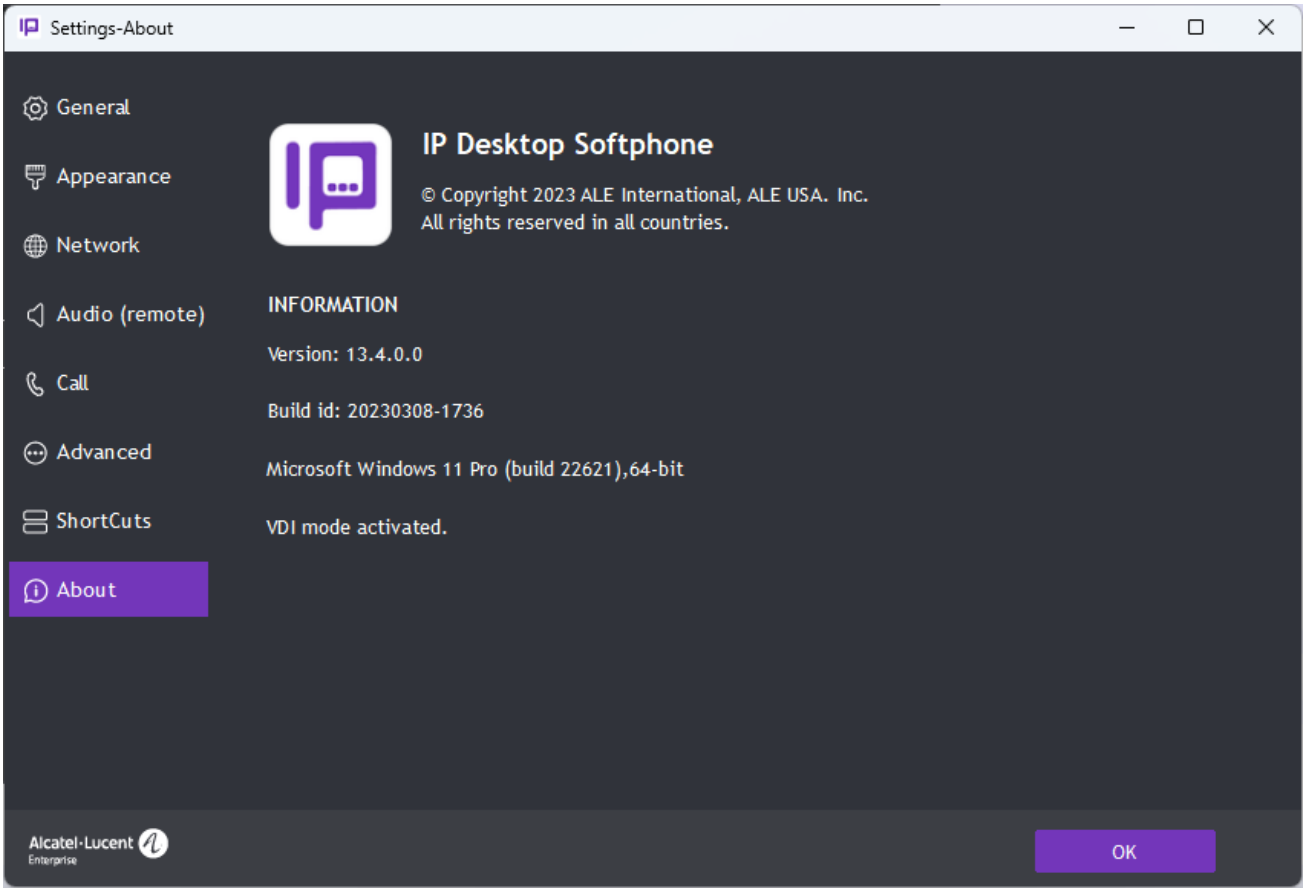
msiexec /x SetupVVXserver_13.X.YY.msi

Component	Description
msiexec	Microsoft command to execute file with ‘msi’ extension
/x	Setting indicating uninstallation
SetupVVXserver_13.X.YY.msi	Name of the file to be executed.

6.8 RUN mode

6.8.1 Version

Check the installed version with the "?" button on IP Desktop Softphone
For VDI use, “VDI mode activated” is mentioned.



Check the installed version of VVX module by Right click on VVX icon on user PC systray, select “About”

If necessary, VVX module can be restarted by selecting “Reset” on VVX icon.

6.8.2 Activating traces

To activate the traces:

1. Edit the file *log4cxx.xml* in the installation directory.
2. Locate the line (normally line 84 to 90)
   - *<level value="OFF" class="org.apache.log4j.xml.Level" />*
3. By default, the value is OFF. Replace the OFF value with INFO.
   - *<level value="INFO" class="org.apache.log4j.xml.Level" />*
4. Save the file
5. Restart the IP Desktop Softphone to take changes into account.

- **For IPDSP on VDI server,** log files are located under the directory:

C:\Users\<username>\AppData\Roaming\Alcatel-Lucent Enterprise\IP Desktop Softphone\logs

Where <username> is the VDI session username.

- **For VVX module on user PC,** log files are located under the directory:

C:\Users\<username>\AppData\Local\Temp\Alcatel-Lucent Enterprise\VVX\logs

Where <username> is the current Windows username.

6.9 Restrictions:

Feature	Description
Customize ringtone	The feature “Customize ringtone” in Audio settings is not available for VDI mode
Multi-session	IP Desktop Softphone cannot be launched in **Desktop** and **Application Modes** simultaneously
API Rest	The API Rest for take call / make call are not available
Missed calls notification badge	**Application Mode:** There is no notification badge on IPDSP icon in Taskbar to indicates the total number of missed calls or messages
TEL protocol	Available only with browser in VDI application mode also or in VDI desktop.
Outlook Addin	Available only with Outlook in VDI application mode also or in VDI desktop.
Call selected number Quick key	Available if the number is selected and copied and IPDSP or VDI desktop have the focus
Maximize Quick key	**Application Mode:** Not available **Desktop mode:** Available only if VDI desktop have the focus
Click to call	Available if the number is selected and copied
OXO Server	IPDSP in VDI mode is not supported on OXO server

7. Mac OS Environment

7.1 Installation prerequisites

The minimum requirements without which the application cannot function correctly are described below.

7.1.1 Hardware

Processor	Intel 1.6 GHz Minimum
RAM	512 Mo Minimum
Disk space	50 MB free space
Sound card	Integrated sound card or USB headset

7.1.2 Operating system

Please refer to the MLE_CrossCompatibility compatibility matrix. Contact your partner.

7.1.3 Networking

Network Interface card	Ethernet Card or Wireless LAN Card

7.1.4 VPN

Refer to the Windows section: VPN

7.1.5 Ports

Only TFTP ports are operating system dependent, macOS in the case of MAC installation.

For the rest, the ports used by the application are identical to Windows and described above:

UDP ports used (OXE context),
TCP used ports (OXE context),
UDP used ports (OXO context)

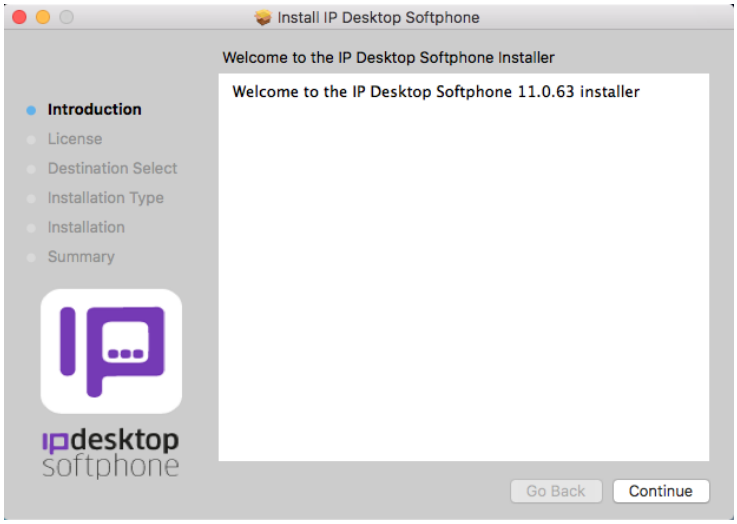
7.2 Installation and upgrade procedures

Note that this procedure is valid for both installation and upgrade of the application.

7.2.1 Installation Mode

Installation of IP Desktop Softphone for Mac OS involves installing IpDesktopSoftphone_11.x.pkg.

7.2.2 Installation in graphic mode

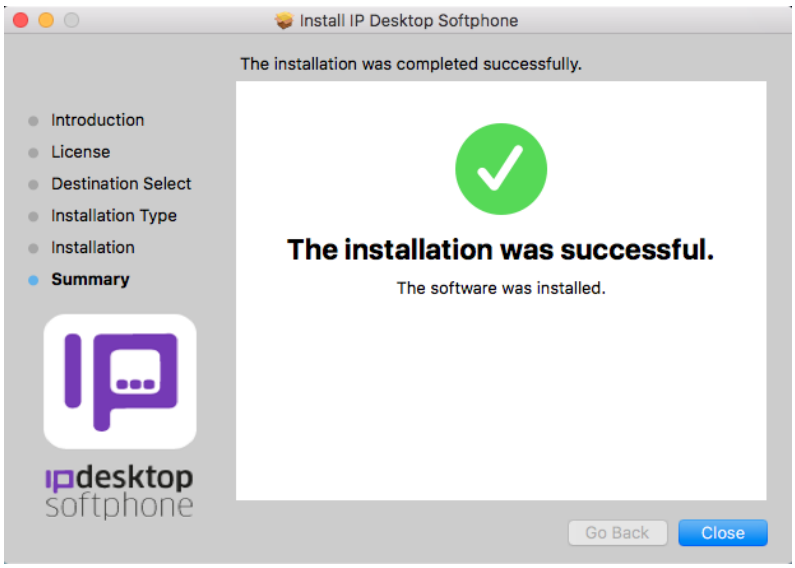


Follow the steps below to install this package:

- **Log in to the system with the credentials of a user with installation rights**
- **Run the file IPdesktopSoftphone_11_x.pkg.**
- **Follow the instructions on the screen step by step:**

  1. **Read carefully and accept the license agreement**
  2. **Select the destination disk**
  3. Change the installation location if necessary
  4. Enter

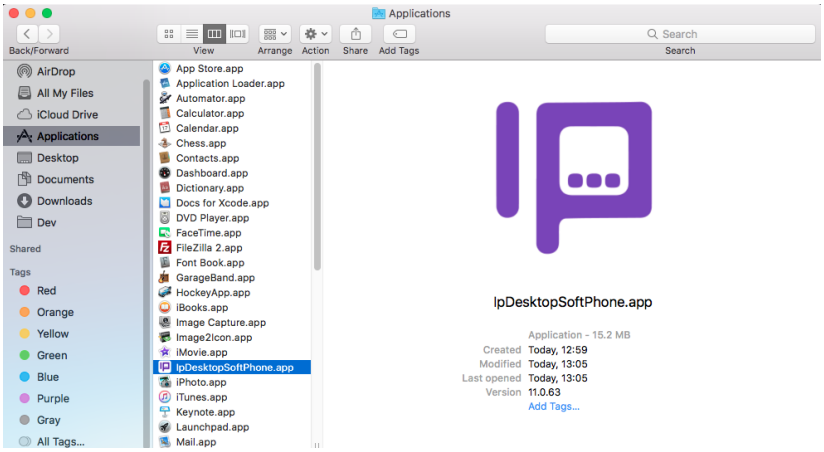
- **Before starting the installation, enter the username and password**
- **Once completed, a message will inform you that the installation is running smoothly**



7.3 Launching the application

To start the softphone, go to the Applications menu:

Finder — Applications — IP Desktop Softphone — Open



Upon first startup, it is necessary to fill in the connection information to the OXE or OXO telephony server. This information is configurable from Settings: Network tab

7.3.1 Registration

The registration procedures are identical to those described in the Windows sections:

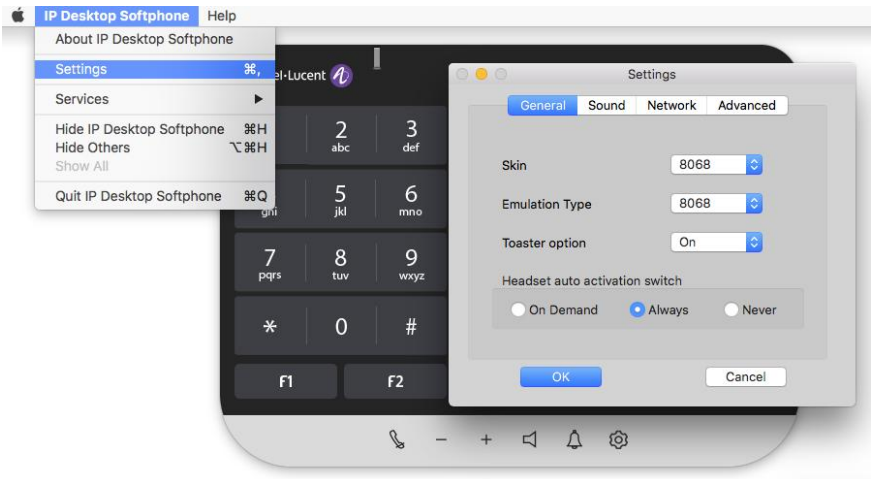
- Registration in OXE context
- Registration in OXO context

7.4 Configuration of Application

Customize the application to suit your existing environment.

Only the administrator settings are documented in this section.
All settings are detailed in the user manual.

Access the configuration options as shown below:



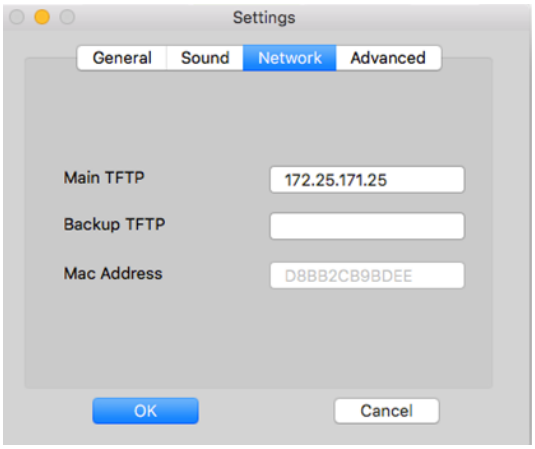
7.4.1 Settings: General tab

Refer to the user manual

7.4.2 Settings: Sound tab

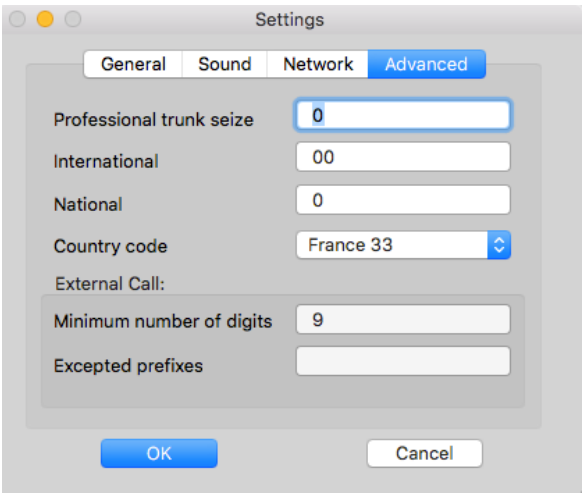
Refer to the user manual

7.4.3 Settings: Network tab



Field	Description
Main TFTP	This field is mandatory, it allows connection of the phone. If you do not enter an address or if the address is incorrect, you will not be connected and receive the following error message: CONNECTION LOST
Backup TFTP	This field is optional. Enter the secondary TFTP server address if applicable
MAC Address	This field is not configurable. The value displayed is the MAC address of your system. It is read by the application

7.4.4 Settings: Advanced tab



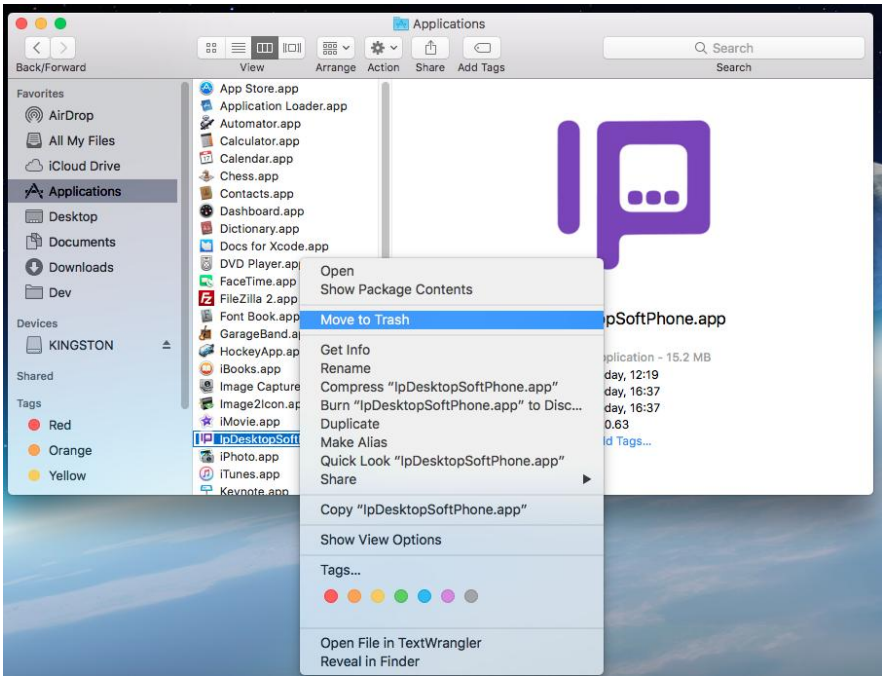
This page is for customizing call settings.

Field	Description
Professional trunk seize	Prefix to make external call. The default value is "0"
International	International call prefix. The default value is "00"
National	First digit used in the country for national calls (06 12 34 56 78). Default value is 0
Country code	The international dialing code of the country. Default value: “France 33”. The associated values are listed in a list.
Minimum number of digits	Minimum number of digits: default value: "9" Any phone number whose number of digits is greater than or equal to the value of this setting will be interpreted as an external number (the professional trunk seize prefix will be added before dialling)
Excepted prefixes	Exceptions from the previous field separated by spaces.

7.5 Uninstalling

To uninstall the IP Desktop Softphone application, follow the steps below:

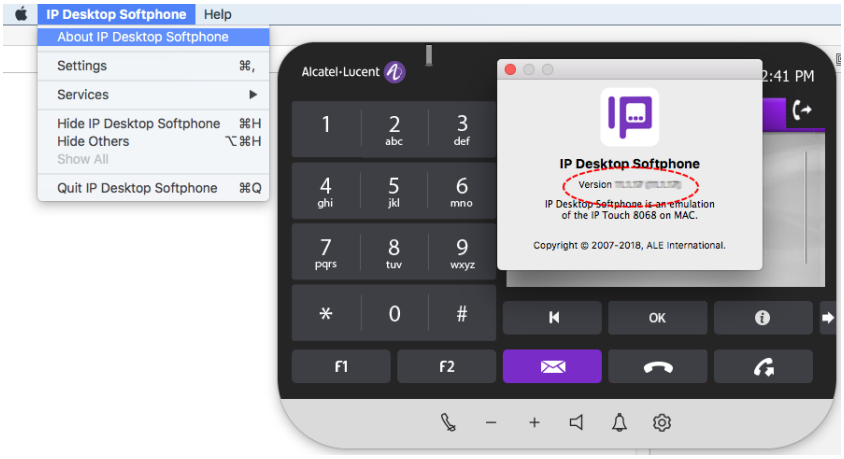
1. Open the Finder
2. Click on the Applications folder.
3. In the list on the right, look for: IPDesktopSoftphone.
4. Right click on it. A new menu is displayed.
5. Click on Move to Trash.
6. This operation starts the uninstallation of the IP Desktop Softphone application.
7. The following screen opens:



7.6 RUN mode

7.6.1 Version

To check the version number, click the "About IP Desktop Softphone" menu



7.6.2 Activating traces

To activate the traces:

1. Edit the *pcmm.cfg* file in the home directory of the current user (/ Users / <user name>).
2. Enter the name of the log file in the "output" setting.
   For example: output= *pcmm.log*.

3. Set the trace levels for **tftp**, **ua**, **pcmm** and **abers**. For **crypto, nomadic, MMC, cnx** and **soap** entries, keep 0.
   Levels of traces:
   0: No traces
   1: Error and main trace
   2: Warning and secondary trace
   3: Detailed data to be transmitted to ALE
   4: Troubleshooting traces

   In the following example, the trace level is set to 3 (detailed data to be sent to R&D)

```
tftp=3
ua=3
pcmm=3
abers=3
crypto=0
nomadic=0
soap=0
MMC=0
cnx=0
```

4. Save the file
5. Restart the IP Desktop Softphone application to take changes into account.
6. When traces are activated, two files are generated: *pcmm.log* (as configured below) and *abers.log*.
   - The Pcmm.log contains the traces of the **tftp**, **ua** and **pcmm**
   - The abers.log file includes traces of the **abers** module.

Note:
Traces should only be activated in the event of a malfunction and are disabled during standard operation of the IP Desktop Softphone application. The aim is to avoid reducing the performance of the software, especially as the size of the log files increases.

8. Android Environment

This part of the document describes the Android installation procedure.

8.1 Installation prerequisites

The minimum requirements without which the application cannot function correctly are described below

8.1.1 Hardware and Operating system supported

Please refer to the MLE_CrossCompatibility compatibility matrix. Contact your partner.

8.1.2 VPN

Refer to the Windows section: VPN

8.2 Installation Procedure

8.2.1 OXE Pre Requisites

After installing the software, you will need to configure the application in order to associate a phone from OXE to the application. To do this, perform the OXE configuration as described in the sectionOXE Configuration.

8.2.2 Installing from the Play Store

As the application's installation is performed by the end user directly from the “Play Store”, it is described in the user manual.

8.2.1 MDM installation

It is possible to deploy applications using MDM type tools.
Contact your partner to get the application in APK format, then refer to the documentation of the deployment tool used.

8.3 Launching the application

Upon first startup, it is necessary to fill in the connection information to the telephony server. This information is configurable from the application options.

8.3.1 Registration

The registration procedures are identical to those described in the Windows sections:

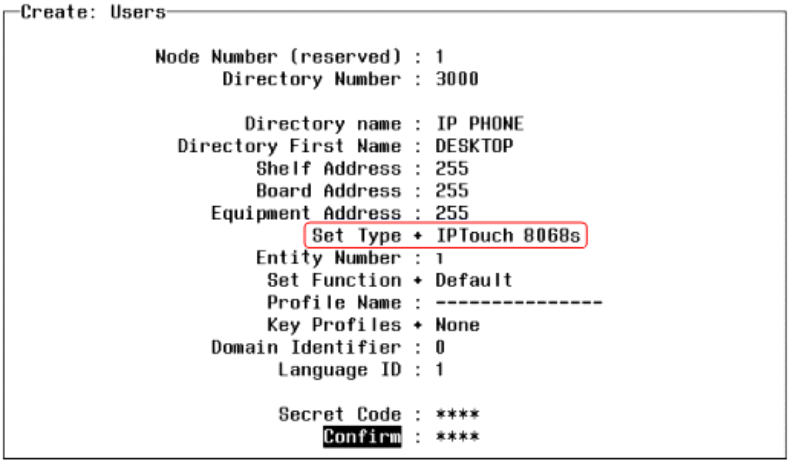
- Registration in OXE context
- Registration in OXO context

9. OXE Configuration

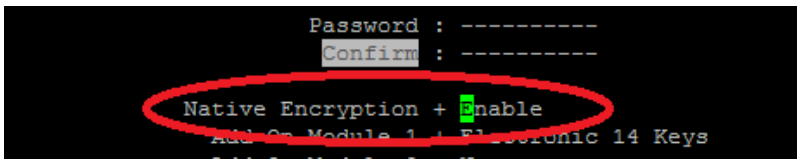
This section describes the OXE configuration.
The OXE configuration is independent of the IP Desktop Softphone installation environment.

9.1 User configuration

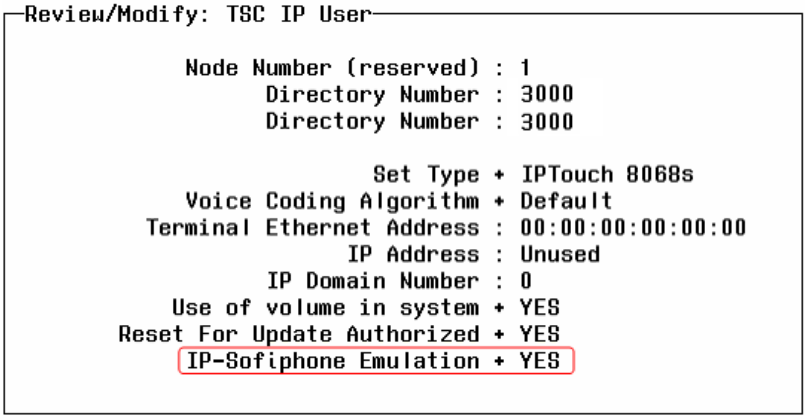
In the telephony server, create a user type IPTouch 8068s.



If native encryption is used, enable Native Encryption parameter

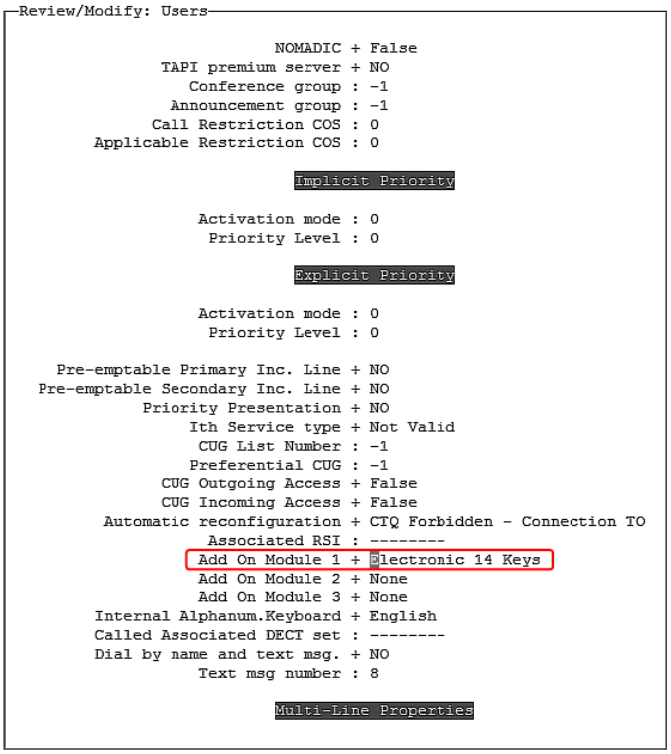


In TSC IP settings, the value of the IP Softphone emulation field must be YES



9.2 Add-on module /AOM configuration

To activate an additional keypad, it is necessary to declare the keypad at the OXE user level



Once completed, and the option confirmed in OXE, the phone offers the option of extended keypad to 14 keys.

You can choose up to 3 additional keypads for Windows:

- **AOM10**: The keypad contains 10 buttons.
- **AOM40**: The keypad contains 40 keys for each tab (two tabs available)
- **AOMEL:** The keypad contains 14 buttons for each tab (three tabs available)

For IPDSP MacOS and Android, only one 14-keys AOM can be configured.

Here are the possible combinations supported by the ipdsp Windows:

- **10-keys**
- **40-keys**
- **40-keys * 40-keys**
- **14-keys**
- **14-keys * 14-keys**
- **14-keys * 14-keys * 14-keys**

9.3 Licensing

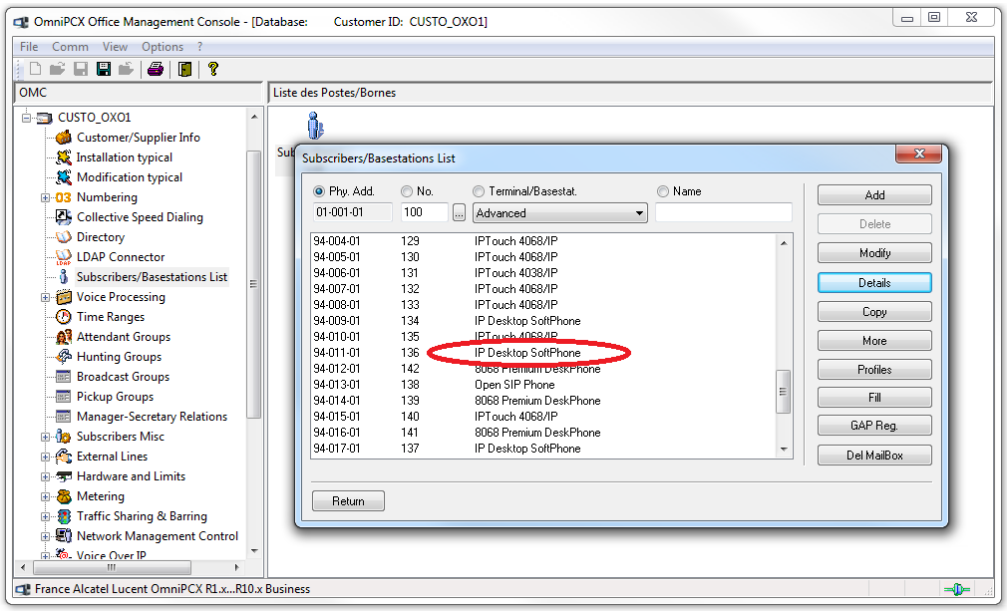
The use of the application requires an IP Desktop Softphone license and an IP license for each user on the OmniPCX Enterprise server.

10. OXO Configuration

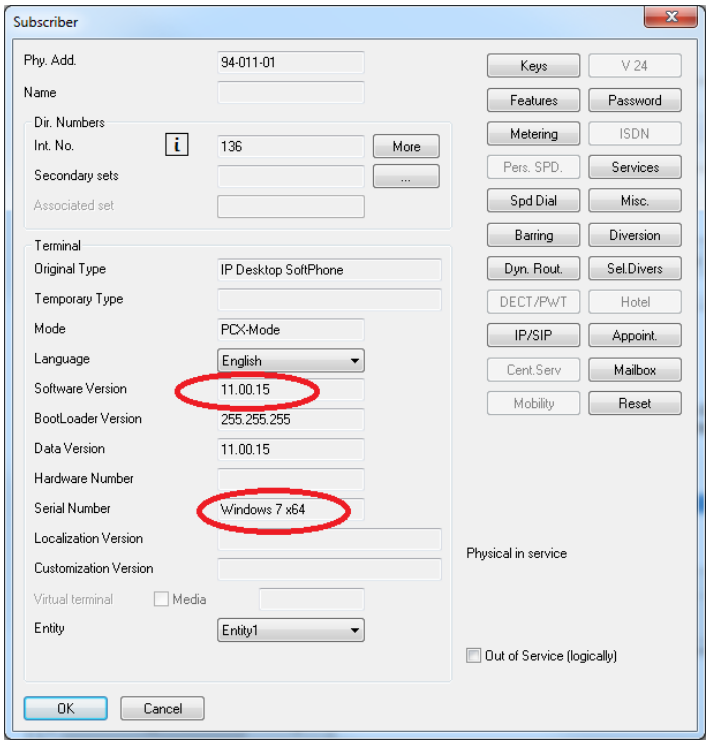
This section describes the OXO configuration.
The OXO configuration is independent of the IP Desktop Softphone installation environment.

10.1 User configuration

In the call server, the user is created with the “IP Desktop Softphone” device type.



To view or edit the user configuration, click the “Details” button.



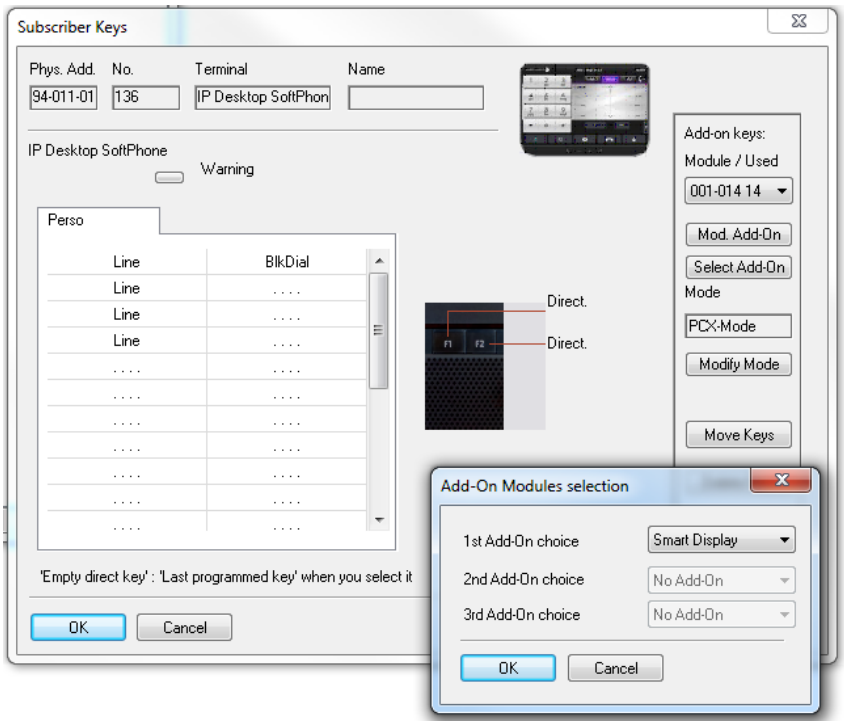
The IPSDP version is displayed in Software Version field.

The operating system version of the installation environment is displayed in the “Serial Number” field.

10.2 Add-On module / AOM configuration

AOM: The 14-key extended keypad is created automatically.
When you click on the Select Add-On button, the Smart Display indication will appear
You can change the settings to remove AOM.

Only one 14-keys AOM can be configured for IPDSP.



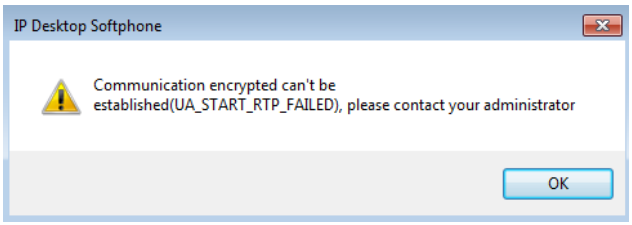
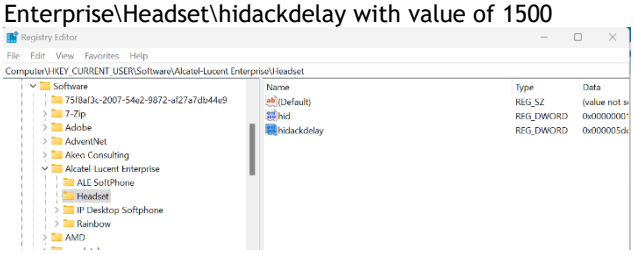
10.3 Licensing

Use of the application requires an IP Desktop Softphone license and one IP license per user on the OXO Server.

11. Trouble Shooting

The table below lists some of the problems you could face, along with their remedial measures:

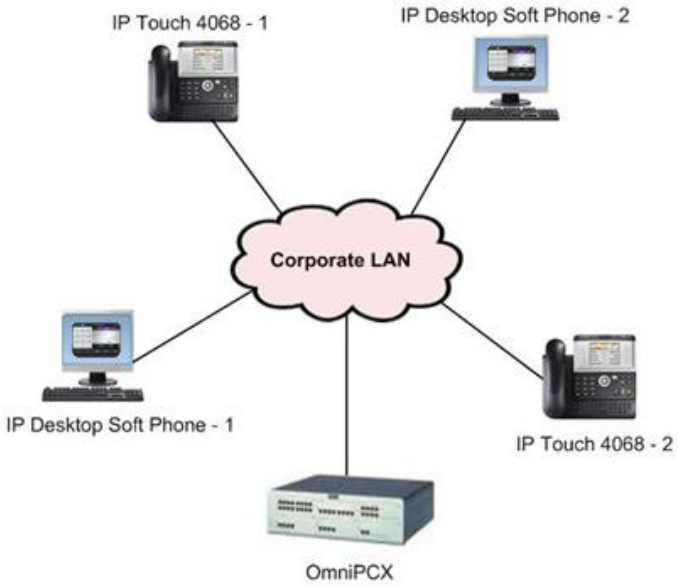
Problem	Solution
Connection establishment fails	○ Check if your network connection is enabled. ○ Check that tftp address is correct and make sure you reach it by a “ping” ○ You may be using an unsuitable network adapter. In the Network tab, check the adapter by clicking the Options → Application menu.
“Set is out of service” message is shown on IP Desktop Softphone screen	If this message is displayed during installation, the “IP-Softphone Emulation” option may not be enabled in the PABX. Ask your administrator to activate this. ***mgr → Users → Descend Hierarchy → TSC IP Users → Review and Modify → Directory Number (Enter terminal number) → Ctrl+V →*** Select the setting ***IP Softphone Emulation →***. ***Click*** to change the setting from ***NO*** to ***YES*** on the PABX side.
When the agent is logged-in, if the Softphone program is closed or if the PC's connection of the PC is lost, the Softphone does not work. When it is opened, it displays the following message on the Softphone’s screen: “Set not registered”. To solve this problem, we need to force disconnect the agent and re-open the Softphone program.	This is normal behavior. However, to solve this problem, set the following settings: ***mgr → Users → Descend Hierarchy → TSC IP Users → Review and Modify → Directory Number (Enter the number of the terminal) → Ctrl+V*** **>Select the setting *IP Softphone Emulation* → Click *Enter* to change the setting from *NO* to *YES*.**
When the user is logged in as IP Softphone agent, Softphone frequently disconnects with the follwowing message: “Set not registered”.	In the Users menu - Descend Hierarchy, change the value of the IP Softphone Emulation setting to No. To do this, connect to the OXE call server. Follow the path: Users → Descend Hierarchy → TSC IP Users → Review and Modify → Directory Number (Enter the terminal number) → Press Ctrl+V. In the list displayed, change the value of the **Reset for update authorized** from True to False.
VPN UAIP user is unable to communicate with another UAIP user on LAN environment.	Check the Firewall or the Access lists. Verify that the ports used by the Softphone are open (see "5.1.7 UDP ports used (OXE context) and 5.1.9 UDP used ports (OXO context)" for more information).
Noise during conversation	To handle this problem, the operation must be done on the PBX side: ***System → Down Hierarchy → Other system param → Down Hierarchy → Compression Param → Review Modify → Voice Activity Detection: False***.
The application does not initialize in laptops connected to LAN through VPN	This is due to a problem in the LAN. Please contact your Administrator in this respect. May be due to network settings (firewall etc)
The application does not start with the system boot	Copy either the .exe file of the application, or its shortcut and paste it in the following directory: C:\Documents and Settings\user\ Start Menu\Programs\Startup

Problem	Solution
No audio in a context FNSE (Full Native Encryption Software). White communication.	Check following OXE configuration: System > other System Parameters > Native Encryption Parameter > Authentication for SRTP Authorised values are : • Authenticated • Authentication tag emis. w/o ctrl The option “Unauthenticated” must not be set in a FNSE context. The user has not to set unauthenticated for "authentication for SRTP", otherwise a message will be displayed to indicate to the user that communication cannot be established with the error code (UA_START_RTP_FAILED) and that he must contact his administrator. 
If the user hears the echo in audio using a headset (Jabra for example) on a new PC Windows 10.	Press “Windows Key” + “R” then press "Enter" Or type "mmsys.cpl 2" in the Search Windows Tab, press "Enter" From "Recording" Tab select the adhoc Jabra Device and double Clic on it (or Right Clic + "Properties" button) The Transmit Properties window appears. Then on "Listen" Tab, uncheck, if not done,the Option "Listen to this device".
On PC MacOs, user does not have the audio in the right headset when using two identical headsets.	Disconnect the two headsets and reconnect the headset you want to use. For some headsets, when a second headset is connected, identical to the first one connected, the detection is not done correctly. The audio is still sent to the first headset. Headset detection is not guaranteed when two identical headsets are connected at the same time.
Call control may fail (HID mode) for some audio headsets, especially EPOS headsets. The issue may be due to the message from headsets is sent way later after communication is over.	Open regedit and add the following registry key (DWORD (32-bit)): Computer\HKEY_CURRENT_USER\Software\Alcatel-Lucent Enterprise\Headset\hidackdelay with value of 1500 

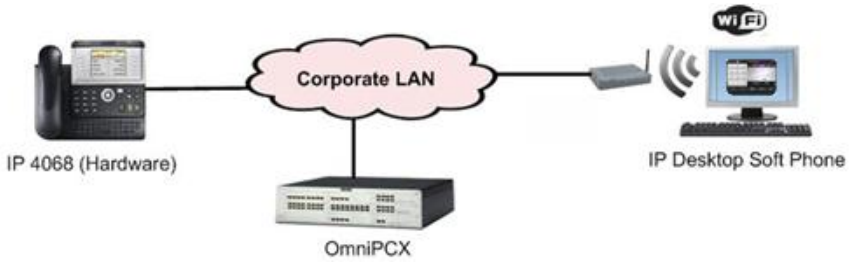
12. Appendixes

12.1 IP desktop Softphone in different environments

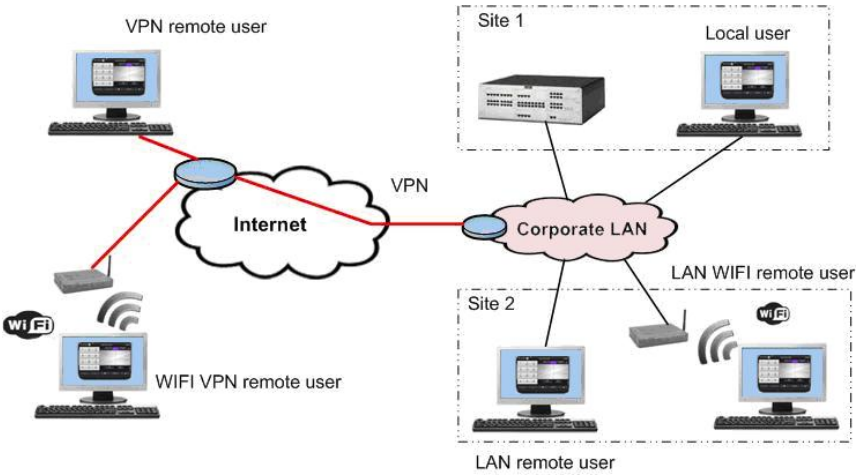
12.1.1 Standard LAN environment



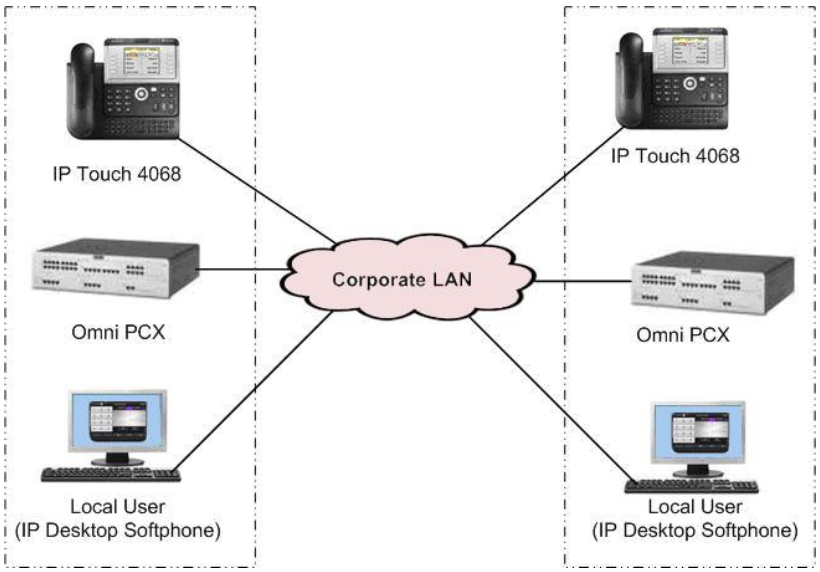
12.1.2 WiFi environment



12.1.3 IP desktop Softphone in a VPN Environment:



12.1.4 IP desktop Softphone in a Dual Call Server environment:



12.2 Qos Management

The ToS field could specify a datagram's priority and request a route for low-delay, high-throughput, or highly-reliable service. The ToS field can specify a datagram priority and request a path to ensure the following performances: short delay, high throughput and service reliability.

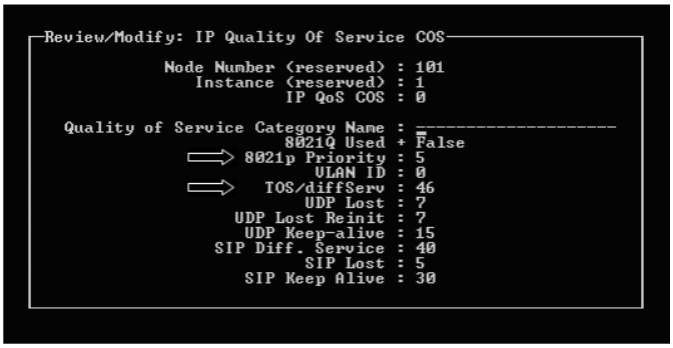
Based on these ToS values, a packet would be placed in a prioritized outgoing queue or take a route with appropriate latency, throughput, or reliability. IP Desktop Softphone can specify the value of this field either in UA messages or RTP flow.
For UA signalization the value of this field is sent from PBX in the connection message: field 06H : QOS_IP_TOS, or in the message : SET_PARAM_REQ field : 00h: QOS_IP_TOS
For RTP flow, the value of the TOS/diffserv is sent from PBX in the Start_RTP message : field 03h: TOS (Type Of Service/Diffserv)
The value of this field must be configured in PBX.

The TOS/DiffServ value is incorrectly entered in Windows Vista, Windows 7 and later when UAC (User Account Control) is enabled.

For Windows to set the value correctly in the header of IP packets, UAC must be disabled.
Please refer to the following link to change UAC settings: https://support.microsoft.com/en-us/kb/975787.

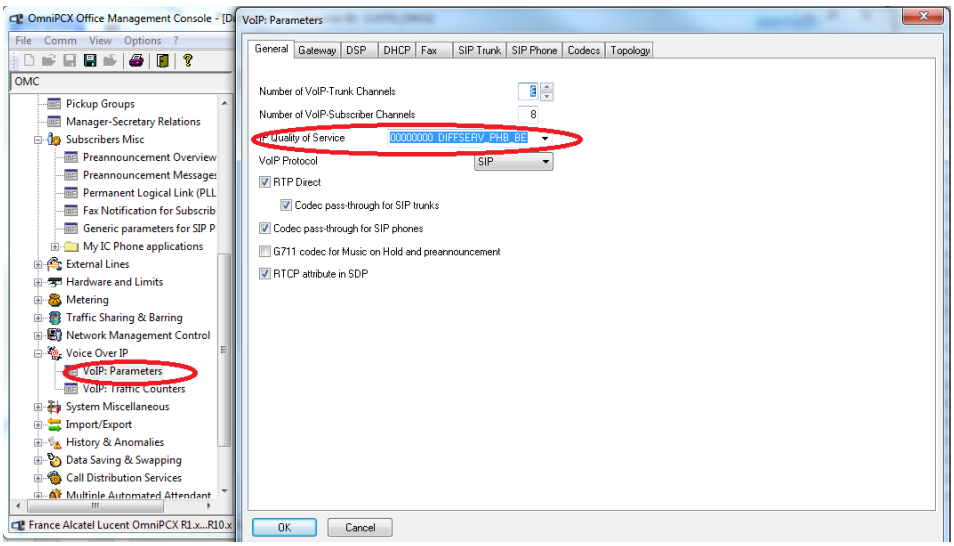
12.2.1 OXE Context

For OXE, TOS / Diffserv is managed in MGR: Mgr -> IP ->Descend hierarchy -> IP Quality of Service COS -> Review/modify



12.2.2 OXO Context

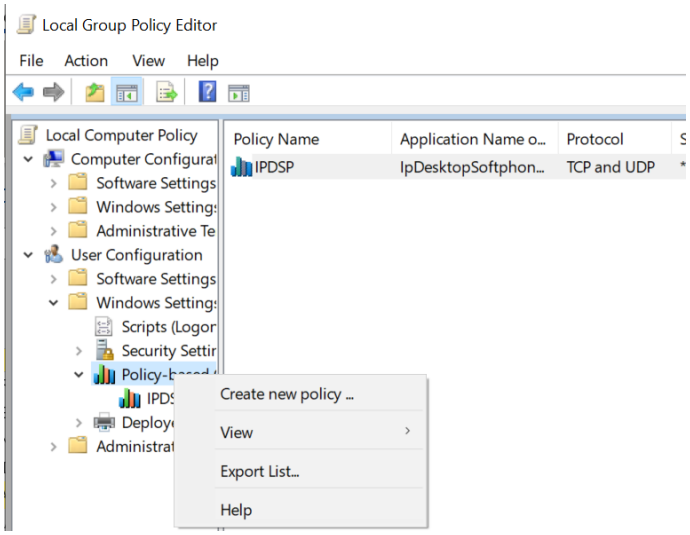
For OXO, launch OMC. Access the following menu: VoIP: settings -> Quality of Service.



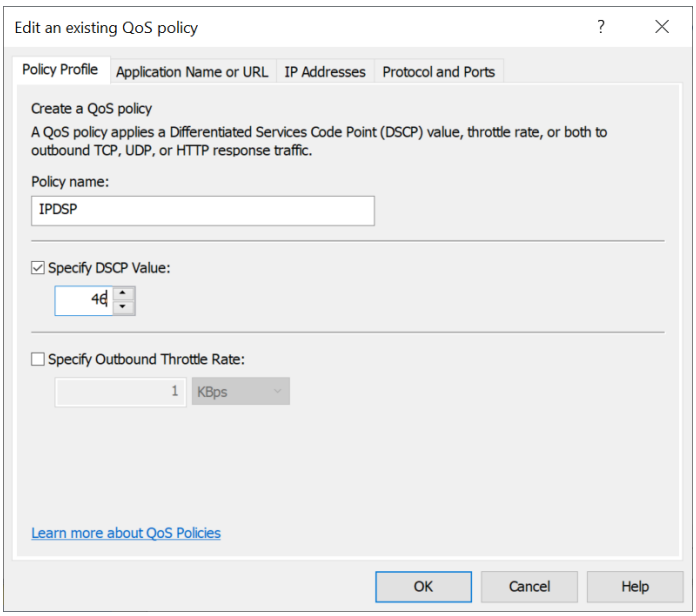
12.2.3 Workaround

To enable QOS on your softphone in Windows, and to circumvent the fact that Windows does not take into account the value set by the IPDSP on outgoing packets, you must add a policy which can be deployed unitarily or massively by the administrator.

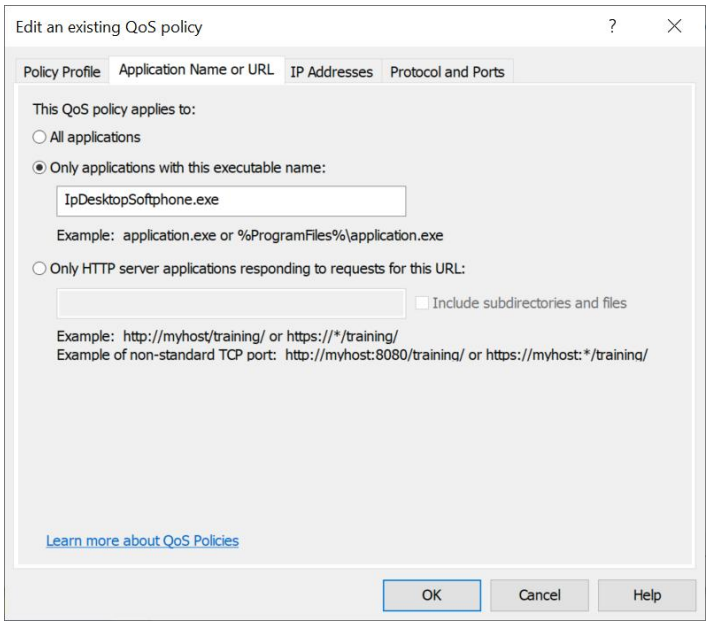
- From the menu “Start”, execute the command: gpedit.msc
- Go to the menu Computer Configuration->Windows Settings->policy based QoS
- Right click and launch “Create new policy…”



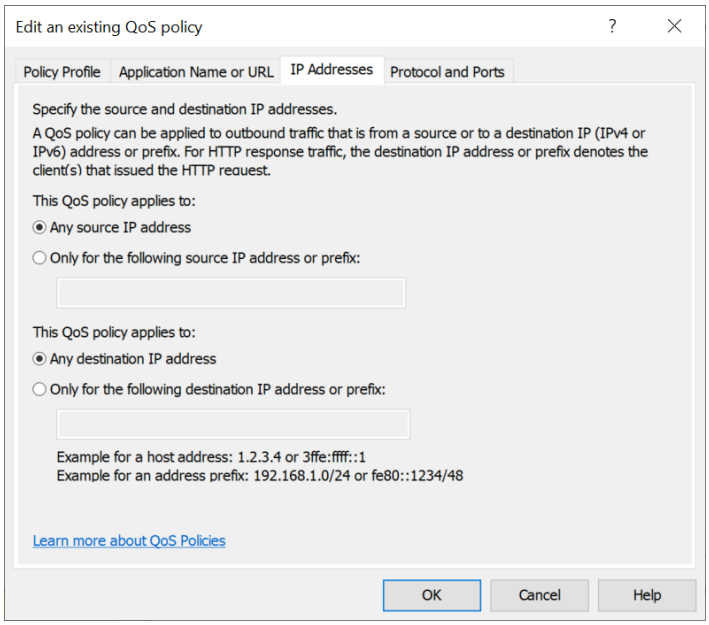
- Enter the policy name, for example “IPDSP”.
- Specify DSCP value to "46", then click “Next”



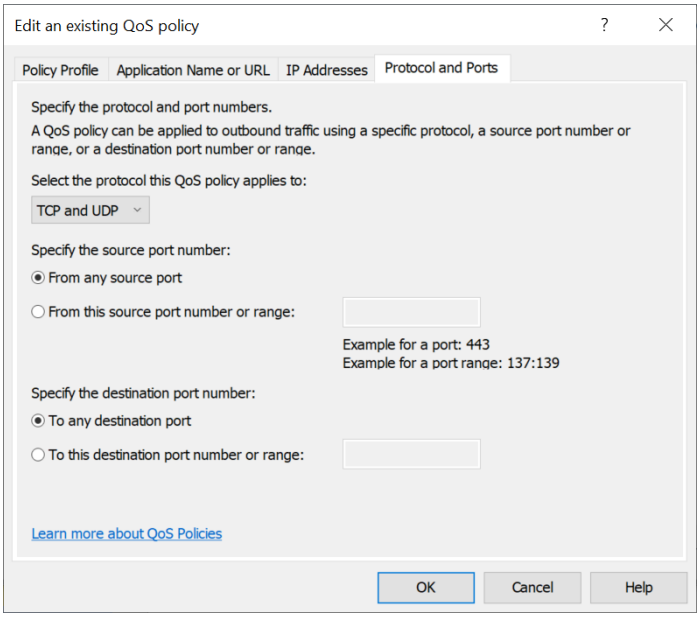
- Enter the name of the executable with " **IpDesktopSoftphone.exe**" and click on "Next"



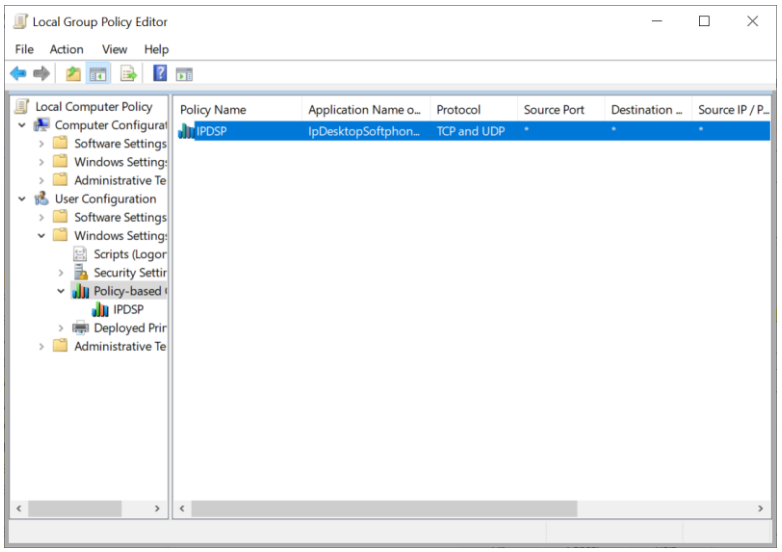
- In the following window leave the default values (“Any source IP address” , “Any destination IP address”) then click “Next”



- Select the protocol to which this "**TCP and UDP**" policy applies and then click "Finish"

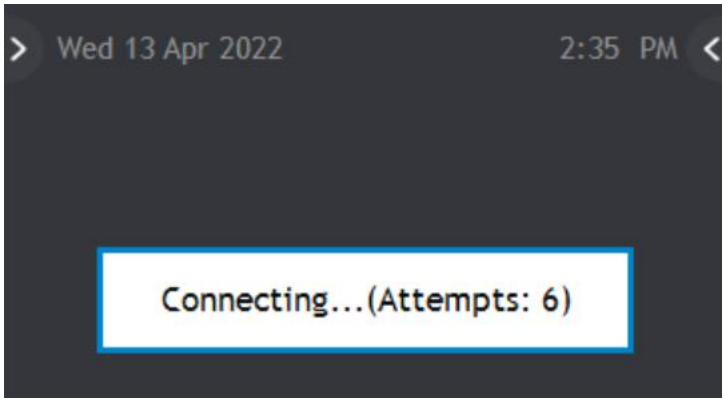


- The QoS policy is now created

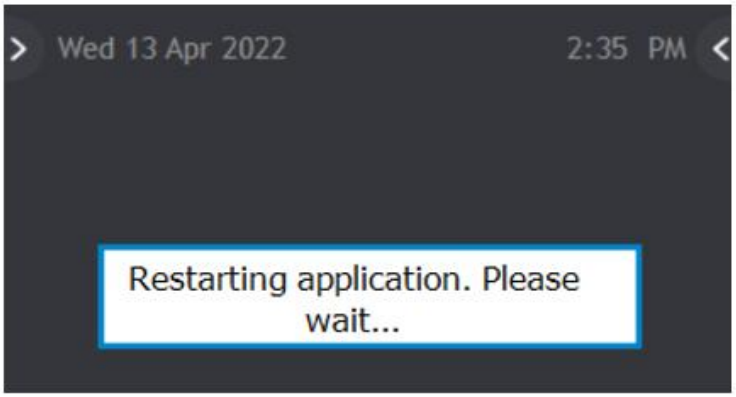


12.3 Some screen messages description

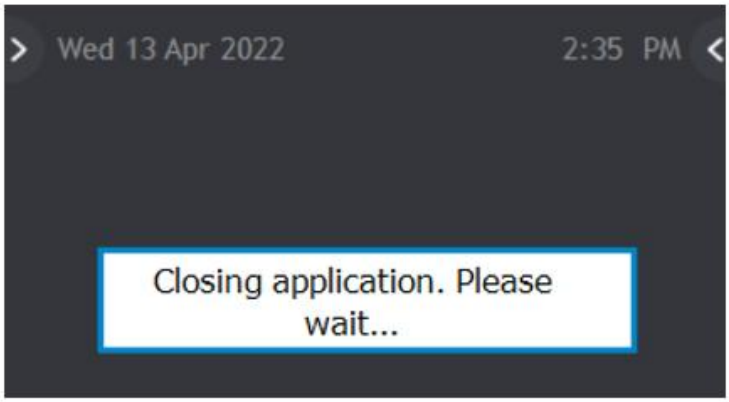
- IP Desktop Softphone is trying to connect to PABX: shows also the number of attempts made to connect.



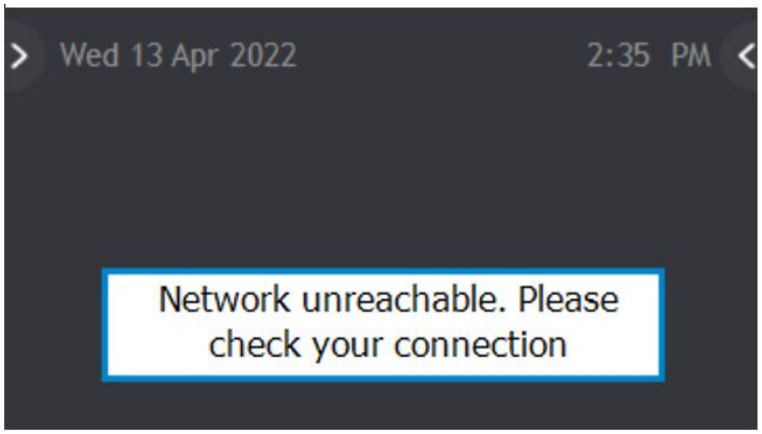
- IP Desktop Softphone is restarting: in some cases, the application may need to restart after some configurations changes (TFTP addresses …)



- IP Desktop Softphone is closing:



- IP Desktop Softphone detects no active network interface card:



END OF DOCUMENT