

WMS Start Guide - English

i This step-by-step guide leads you through the process of activation and configuration of the Wildix system.
WMS version: 6.0X / 5.0X
Updated: January 2023
Permalink: <https://wildix.atlassian.net/wiki/x/hhbOAO>


- Introduction
- Connection and HTTP(s) access (Hardware PBX)
 - Connection
 - HTTP(s) access
 - Choosing a network scenario
 - Separated data and voice networks
 - Shared data and voice network
 - Separated data and voice networks with traffic shaper
- PBX Activation and first time WMS access
 - Creation of Per User PBX on WMP
 - First time WMS access
 - WMS access
 - Change admin password
 - Upgrade WMS to the latest stable release
 - PBX Activation (Hardware, Virtual PBXs)
 - Introduction to WMS
- Basic WMS settings
 - Time & date
 - Language & Region
 - Remote Support
 - Activation & Licenses
 - Storage services (Hardware, Virtual PBX)
 - System Backup
 - PBX upgrades
 - DHCP Server (Hardware, Virtual PBXs)
 - SMTP Client
 - Fax server
 - Call & chat history
 - SIP-RTP
 - Dialplan General Settings
- WMS Network
 - Introduction to WMS Network
 - Server and Client configuration
- Adding / importing users and phonebooks
 - Adding users manually
 - Set user passwords
 - User preferences
 - Delete user data
 - Import of users and phonebooks
- Provisioning of devices
 - Provisioning modes supported by Wildix PBX
 - WMP provisioning (Hardware, Virtual, Cloud PBX)
 - Auto-configuration via auto.wildixin.com (Hardware, Virtual PBX)
 - Auto-provisioning - Automatic mode (Hardware, Virtual PBX)

- Remote provisioning - Semi-Automatic mode (Hardware, Virtual, Cloud PBX)
- Devices management
 - Update firmware
- Assign WP4X0 to users
 - Assign from WMS
 - Assign via Feature Code
- Assign analog ports of FXS to users
- Provisioning and login of Vision/ SuperVision
- W-AIR DECT solution
 - Introduction
 - Create a W-AIR network
 - Register and assign W-AIR handsets to users
 - Register and assign W-AIR Headsets to users
 - Assigning W-AIR handsets/ headsets via WMS
- Introduction to Wildix Unified Communication
 - Wildix Collaboration
 - Apps for Android / iOS
 - Call activity analysis & reporting with CDR-View
 - Pricelists
- Configuring SIP trunks and lines
 - SIP Trunk configuration
 - Make a test of SIP trunking between 2 PBXs
 - ISDN lines (BRI/PRI media gateways)
 - GSM network (DaySaver GSM media gateway)
- Call routing strategies: Dialplan
 - Wildix Dialplan: how it works
 - Associating entities to Dialplan procedures
 - Matching called numbers
 - Adding and editing Dialplan procedures
 - Dialplan applications
 - Modify called number
 - Jump to another procedure
 - Included procedures
- Dialplan practical examples
 - Internal Dialplan - users
 - Trunk groups
 - Call through remote PBX
 - Example of users procedure configuration
 - External Dialplan - main
 - Route incoming calls to call agents (call groups)
 - Record and playback audio messages
 - Create a switch
 - Create a timetable
 - Create an IVR tree
 - Incoming faxes management
 - DID & DISA
 - Mobility extension lookup
 - Example of main procedure configuration
- Wildix WebRTC solution
 - Wildix WebRTC Kite
 - WebRTC-based Wizzyconf videoconference
- Debugging and troubleshooting
 - SSH connection

- [Dialplan debug](#)
- [Trace generation](#)
- [Syslog, Reset and recovery of media gateways and phones](#)
- [Other](#)
- [PBX access via RS-232 serial port to reset admin password \(Hardware PBX\)](#)

Introduction

This guide will lead you through the process of PBX installation, starting from PBX installation and activation, and ending with practical Dialplan examples for call routing.

-  Important: this guide does not explain all the features of the system. You can learn more about
- features of the system - in Technical-Commercial Specifications Document: https://drive.google.com/drive/u/0/folders/1XSxqHspyi-G5mmX0s_nhv844d8CwC9Z2

Wildix PBX integrated software consists of two components: WMS (Wildix Management System) for PBX administration and Collaboration user interface. Another important component of the system is WMP (Wildix Management Portal). Below more information on each component.

WMS

PBX admin interface accessible via the browser, allowing you to set up and program the system. WMS provides the access to the following settings:

- All the system settings, general settings, time and date, language settings, system backups, upgrades, system sounds, etc
- Users management, their ACL permissions, preferences; phonebooks
- Provisioning of devices, assigning phones and analog ports to users
- Lines and SIP trunks configuration
- Dialplan configuration: rules for routing incoming and outgoing calls, call groups, IVRs, timetables

Collaboration

User interface for access to UC&C, completely web-based and accessible via the browser; requires at least Essential license. Additionally, you can download mobile apps for iOS/ Android from App store / Google play market.

WMP

Accessible at <https://my.wildix.com/>. Wildix PBXs should connect to the WMP server for:

- Activation and periodic check of Wildix licenses
- Auto-configuration of Wildix devices (auto-provision devices by simply assigning purchased devices to any of your PBXs)
- Remote support (when needed, you can remotely connect to each of your PBXs)
- Statistics and reports

In addition WMP is an important Partner resource for making orders, creating offers, opening support tickets, etc.

Wildix Licensing

Wildix offers three type of PBX appliance:

- Hardware: hardware PBX installed at the client's premises
- Virtual: PBX image installed on server
- Cloud: hosted in our cloud

Wildix currently the following type of licensing:

- Per User licensing (available for Hardware / Virtual / Cloud PBX): add as many users of each profile as you need. Some users may have only basic telephony features, others may have access to UC&C features, and others may have access to advanced features. Pay recurring fees per user / per period of time. Add more users of each type at any time. More information on user profiles: <https://www.wildix.com/licensing/>.

In this guide it will be explained how to activate a Hardware PBX Per User and a Cloud PBX.

More information on Wildix licensing and licenses activation: [PBX Licensing and Activation](#).

Useful links:

- Tech Wizards FB group (please add yourself to the group): <https://www.facebook.com/groups/wildixtechwizards/>
- Official website: www.wildix.com
- WMP (activation, licenses, orders, tickets): <https://my.wildix.com/>
- Tech news: <https://www.wildix.com/new-releases-and-updates/>
- eLearning platform: <https://training.wildix.com/>
- Blog: <https://blog.wildix.com/>
- DOCUMENTATION: <https://wildix.atlassian.net/wiki/spaces/DOC>



Starting from October 1, 2021, Wildix provides partners with a read-only ValuePartnership (former SKit) demo PBX for the training.

The following licenses on 1 year subscription are available within the PBX:

- 10 Premium
- 1 Business
- 1 Essential
- 1 Basic
- 1 Wizzywebinar license for demo purposes

To continue using free licenses on a demo PBX after the grace period, you'll need to sign the yearly Partnership Agreement during the annual Summit in Jan 2023.

Connection and HTTP(s) access (Hardware PBX)

Connection

Access is possible via HTTP(S) / SSH or via RS-232 serial port.

Proceed as follows:

1. Insert the USB Memory Key (WKEY2GB) into the USB port of the PBX
2. Power on the PBX (connect the PBX to the power supply and move the switch situated on the front panel to the "1" position)
3. Connect the PBX to the Switch (use WAN port) or to your PC (use LAN1 port) via RJ-45 network cable

HTTP(s) access

Default settings of Ethernet ports

- LAN1: DHCP – Server, IP – 10.135.0.1/24
- Use the IP address 10.135.0.1

- WAN: DHCP – Client, IP – Dynamic
- Use the IP address released by the DHCP server

Port	1	2	3	4
Type	WAN	LAN1	LAN2	LAN3
DHCP	Client	Server	Disabled	Disabled
IP	Dynamic	10.135.0.1/24	Disabled	Disabled

Access WMS interface

1. Open the browser (recommended: the latest version of Chrome)
2. Type `https://PBX_IP` or `http://PBX_IP` (recommended mode: `https`) into the URL bar, example: `https://10.135.0.1/`
3. Enter the credentials for the first time access:
 - Login: admin
 - Password: wildix

Choosing a network scenario

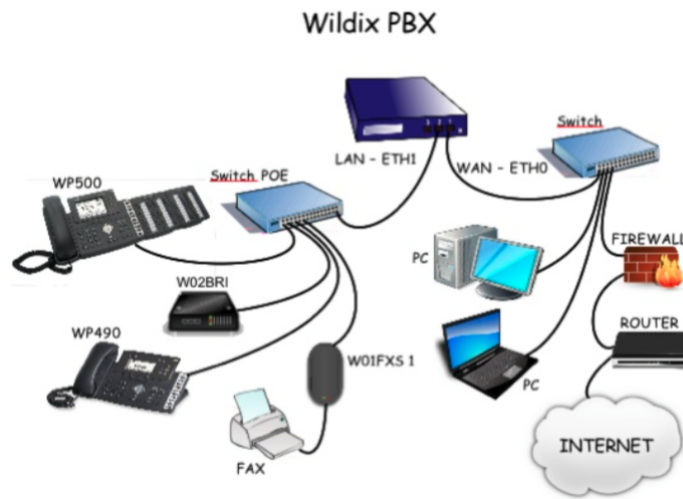
You can set up the network parameters of the PBX based on the selected network scenario:

- Separated data and voice networks (recommended)
- Shared data and voice network

Below the most common network scenarios are described.

Separated data and voice networks

In this scenario the PBX is used as the DHCP server for telephone (voice) network and releases the IP addresses to all the devices (phones, media gateways) belonging to its network; eth0 interface is set up as DHCP client, eth1 must be set up with static IP and as DHCP server. Default settings of ETH1 interface is `10.135.0.1`.



Go to *PBX Settings -> System -> Network*:

1. Select the WAN eth0 interface and make sure the option *Get the address from the DHCP server* is enabled:

Interface	eth0
Get address from DHCP server	<input checked="" type="checkbox"/>
Status	enabled

2. Select the LAN eth1 interface, set the static IP (Default: *10.135.0.1/16*):

Interface	eth1
Get address from DHCP server	<input type="checkbox"/>
Address	10.135.0.1
Netmask	255.255.0.0
Status	enabled

3. Click **Apply the network settings**
4. Check the address of the WAN eth0 interface to know the new IP address of the PBX

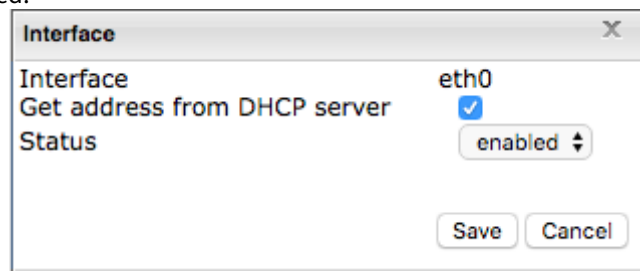
Shared data and voice network

In this scenario telephone and data share the network with the PBX; the single interface used is eth0, the IP address is released by the DHCP server in the network. Check the leases of your DHCP server to know the IP address released to the PBX.



Go to *PBX Settings* -> *System* -> *Network*:

1. Select the WAN eth0 interface and enable the option *Get the address from the DHCP server*. Two other interfaces remain disabled:



2. Click **Apply the network settings**
3. Check the leases of the DHCP server to know the new IP address of the PBX

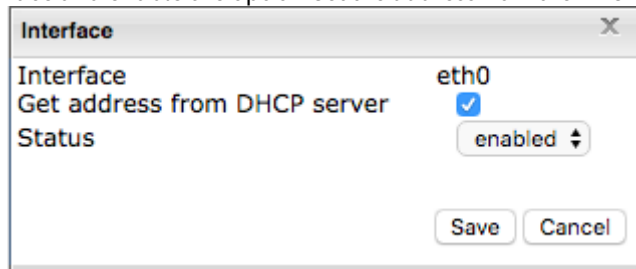
Separated data and voice networks with traffic shaper

In this scenario the PBX is used to keep telephone and data networks separated, making use of the third eth2 interface to create the bridge between eth0 and eth2 interfaces, while the third interface eth1 is reserved for a separate network. It is possible to set up the bandwidth upload and download limits on the WAN eth0 interface - in this way you can control the bandwidth used by WAN eth0 port and allow the PBX to manage intelligently the bandwidth for communication with VoIP operators and remote phones with priority given to the traffic generated on the LAN eth1 port.

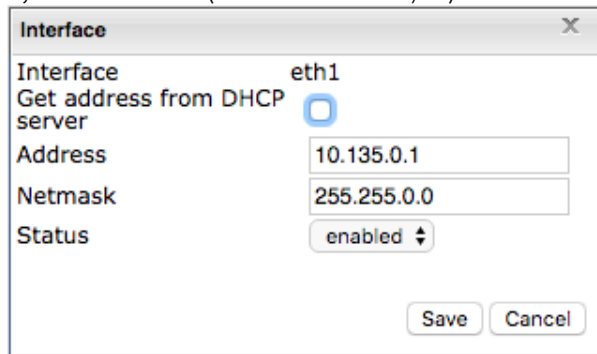


Go to *PBX Settings -> System -> Network*:

1. Connect the second Switch to the LAN2 port of the PBX
2. Select the WAN eth0 interface and enable the option *Get the address from the DHCP server*:



3. Select the LAN eth1 interface, set the static IP (Default: 10.135.0.1/16):



4. Click **Enable traffic shaper eth0-eth2**
5. Click **Apply the network settings**
6. The bridge between WAN eth0 and LAN eth2 interfaces is created, with a dedicated separated network on the LAN eth1 interface
7. The interfaces eth0 and eth2 are no longer present on the page, the interface wbr0 is used as WAN which keeps the same settings of the eth0 interface (either static IP or DHCP client)
8. Select the WAN wbr0 interface and set up the bandwidth limits for *Downlink* and *Uplink*:

Interface ✕

Interface wbr0

Get address from DHCP server

Status enabled ▾

Downlink, kbit/s

Uplink, kbit/s

9. Click **Apply the network settings**
10. Check the address of the WAN wbr0 interface to know the new IP address of the PBX

PBX Activation and first time WMS access

Creation of Per User PBX on WMP

Proceed as follows:

1. Connect to [WMP](#) using your credentials
2. Go to *Customers* tab; to create a new PBX, you first need to add a customer (if it does not exist yet); click **Add**:



3. Create a new customer (company): fill in the fields and click **Save**:

Company name

Price list

VAT IN

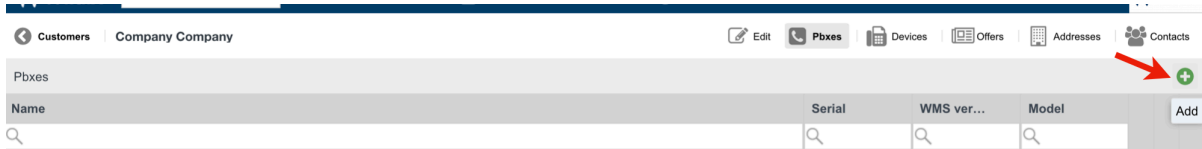
4. You need to create at least one contact: fill in the fields and click **Add**:

Technician
 Sales manager
 Accountant

5. Now you can proceed with adding a new PBX: go to *PBXs* tab:



6. You are now under *PBXs* tab, click + to add a new PBX:



7. Fill in the fields:

- *Model*: select WPBX-CLOUD for Cloud / WPBX-VM/HW for Virtual or Hardware
- *Region* (only for Cloud PBX): select the datacenter region
- *Name*: PBX domain name by which your PBX is accessible via the browser; in the example provided below, the PBX can be accessed by URL <https://elenatest2.wildixin.com>
- *Expire*: select the recurring billing period: monthly / yearly / 5 years / lifetime (lifetime is not available for Cloud PBX)
- *PBX-BASIC / UC-Essential / UC-Business / UC-Premium / UC-Wizyconf Room / UC-Wizywebinar / PBX-Service*: add the number of users of each profile (more about each profile: <https://www.wildix.com/licensing/>)
- Storage size and enable Static IP (only for Cloud PBX): increase Cloud instance storage size. For more details, refer to the chapter: [Increase storage on Cloud PBX](#)

Note: Starting from July 1 2021 onward, all PBXs will get a dynamic IP address by default. If you need to reserve static IP for your Cloud PBX, there are several options:

- Switch to CLASSOUND to provide a more modern service
- Ask your provider to switch from the IP-based authentication to the password/login one
- Buy the storage (If you have previously purchased an extra storage, the IP is reserved)

- *x-caracal*: tick the option to activate x-caracal ACD stats service on this PBX. Important: make sure you add at least 10 Business/ Premium + 1 Premium licenses on this PBX to be able to activate x-caracal. More information on how to activate x-caracal on the WMS side: [x-caracal documentation](#). **Important: x-caracal is supported only on Cloud or Virtual PBXs**, Hardware PBXs are not supported. Make sure you have the min. required WMS version
- *MS-PhoneSystem*: this is an extension of the [teams4Wildix \(integration of Microsoft Teams with Wildix PBX\)](#). It requires the **CLASSOUND** service to be activated on the PBX. **Important:** Make sure you have the min. required WMS version

Model	WPBX-CLOUD		
WMS version	5.03.20210806.2		
Region	EU (Frankfurt)		
Support	Available		
Name	[redacted].wildix.com		
Expire	Monthly		
PBX-BASIC	0	-- +	X EUR = EUR
UC-Essential	8	-- +	X EUR = EUR
UC-Business	11	-- +	X EUR = EUR
UC-Premium	16	-- +	X EUR = EUR
UC-Wizyconf Room	1	-- +	X EUR = EUR
UC-Wizywebinar	2	-- +	X EUR = EUR
PBX-Service	4	-- +	X EUR = EUR
Storage Size (x10Gb) and enable Static IP	0	+	X EUR = EUR
x-caracal	<input type="checkbox"/>		X EUR = EUR
MS-PhoneSystem	<input type="checkbox"/>		X EUR = EUR
			Total: EUR

- Click **Add**; your PBX has been created:

Company Company [Edit] [Pbxes] [CLASSOUND DIDs] [Devices] [Offers] [Addresses] [Contacts]

Name	Serial	WMS ver...	Model
cloud-pbx9	[redacted]	5.01.20200612.2	WPBX-CLOUD

! For Cloud PBX: wait for approximately three minutes before proceeding, your PBX will be activated automatically. Virtual and Hardware PBXs must be activated manually: [PBX Licensing and Activation Guide](#).

WMP Intro Video <https://fast.wistia.com/embed/medias/vpvdep1bwe>

First time WMS access


WMS access

! **For Virtual PBX:** before proceeding, follow the guide to deploy PBX image:

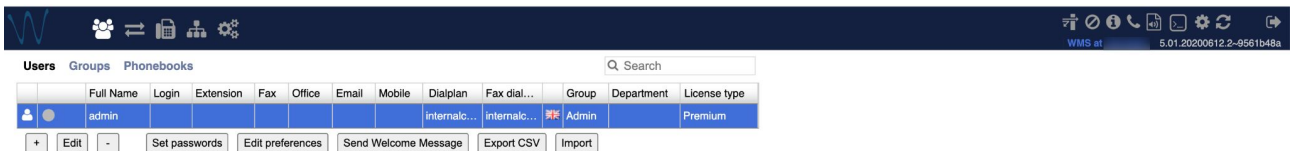
- [Deploying WMS 6.0 on Hardware, Virtual, Cloud PBXs](#)
- [Deploying WMS 5.0 on Hardware, Virtual, Cloud PBXs](#)


Proceed as follows:


1. Open the web browser (recommended browser: Google Chrome updated to the latest version)
2. Type the PBX IP address (https mode is recommended), example: *https://10.135.0.1/* (for LAN1) or PBX name set on WMP (Cloud PBX), example: *https://mycompany.wildixin.com*

 Note: For access by default local IP *10.135.0.1* where your PC is connected to the LAN1 port, your PC must be in the same network segment as the PBX.


3. Enter the credentials for the first time access:
 - user : *admin*
 - password : *wildix*



 Note: To change the language of the WMS interface, double click on the “admin” user and select the language from the list.

 Important! Before proceeding, it is necessary to change the *admin* password. This *admin* user is the “super admin” - the only user with full access to all the levels of the system management.

Change admin password

 Important! On Cloud PBXs, a default admin password is reset after 7 days of uptime. Make sure to change it.
In case you face any issues with reset, contact Wildix Support.

Proceed as follows:

- Select admin user and click **Set passwords**
- Generate or create a new password, click **Ok**
 - *Current password*: enter the current password (*wildix*)
 - *New password*: click **Generate** (green icon) to automatically generate a strong password (click **Show** to view the password generated by the system)
 - *Confirm password*: enter the new password again to confirm it

Dialog box titled "Edit admin" with fields for:

- Current password
- New password
- Confirm password
- SIP/VoIP

Buttons: Cancel, Save

Note: You can also compose your own strong password, consisting of at least 8 symbols, at least 1 uppercase, 1 lowercase, 1 digit, 1 special character.

Note: This password is used by the admin user to access the WMS interface, while SIP/VoIP password is used to register and assign remote devices.

- Enter the email address of the *admin* user to be able to receive email notifications: double click on the *admin* user and fill in the field *Email*:

Dialog box titled "Edit admin" with fields for:

- Role: Admin
- Full Name: admin
- Login: admin
- Extension: 111
- Fax:
- Office:
- Email: tatiana.bieliakova@wildix.com
- Mobile:
- Dialplan: internalcalls (Users dialplan)
- Fax dialplan: internalcalls (Users dialplan)
- Language: En
- Group: Admin
- Department: ?
- License type: Premium

Buttons: Cancel, Save

Upgrade WMS to the latest stable release

Go to *WMS Settings -> Tools and utilities -> Upgrade*.

To upgrade the system, proceed as follows:

- The system checks whether there is a new version available in the selected repository: *rel60 / rel50*:

⚠ Note: Starting from WMS 5.0420220819.1, to be able to upgrade to the next major WMS version in case of WMS Network, e.g. from WMS 5 to WMS 6, WMS Network has to be configured correctly, matching the licences ordered on the Wildix Management Portal.

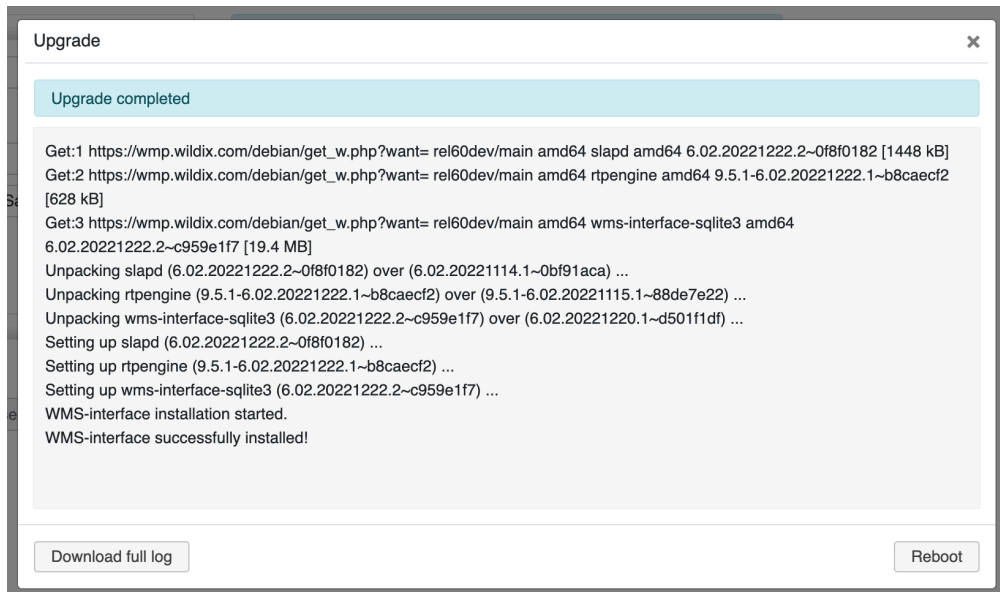
⚠ For Hardware/ Cloud PBXs: you need to first upgrade your PBX to the latest WMS5 version and then update it to WMS6:

1. Enter the following name of the repository into the field *Upgrade repository*: *rel50*
2. Click **Save**
3. Click **Perform upgrade** to update your PBX to the latest WMS5 version
4. Enter the following name of the repository into the field *Upgrade repository*: *rel60*
5. Click **Save**
6. Click **Perform upgrade** to update your PBX to WMS6 version

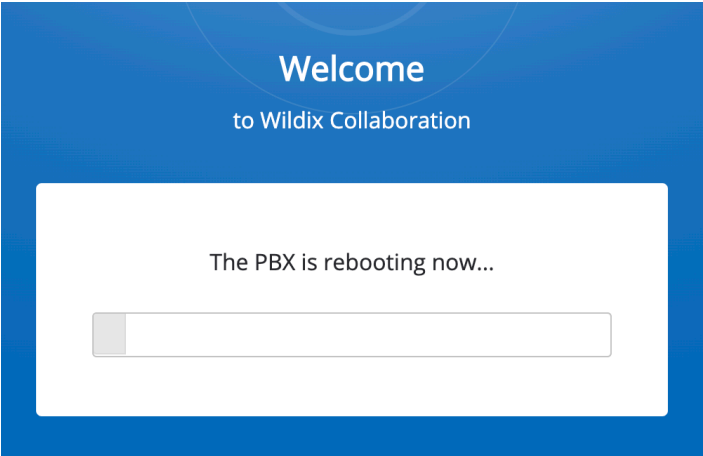
- In case there is a new version available, click **Perform upgrade**
- As a rule, the Upgrade procedure takes several minutes:



- As soon as the update procedure is over, the button **Reboot** is shown:



- Click **Reboot** and wait till the system is being rebooted:



- As soon as the PBX has been rebooted, the login page appears
- Log in to the WMS, the current WMS version is shown in the upper right part of the screen:



PBX Activation (Hardware, Virtual PBXs)

Cloud PBXs are automatically activated after they are created in WMP (see chapter [Creation of Per User PBX on WMP](#)).

- Copy PBX key from [WMP](#):
- Go to the tab *PBX per user*, select your company, then select the PBX that you have created on *step 1*
- Click **Copy PBX key to clipboard**



- Insert the PBX key on WMS side:
- Go to *WMS Settings -> Tools and utilities -> Activation / Licenses*
- In the *License actions* section, paste the PBX key copied on the previous step into the PBX Key field:

The screenshot shows the Wildix WMS interface. At the top is a dark navigation bar with icons for home, users, call logs, and settings. Below this is the 'System' section, which displays the following information:

Status	Not activated
System name	[Redacted]
SW Serial	[Redacted]
HW Serial	[Redacted]
Processor	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
Memory	7958 Mb
Users	0
Concurrent calls over trunks	0

Below the System section is the 'License usage' section, which displays the following information:

Basic	0 / 0
Essential	0 / 0
Business	0 / 0
Premium	0 / 0
Wizyconf Room	0 / 0
Service	0 / 0
x-bees	No
x-caracal	No
Wizywebinar	No
CLASSOUND	No
Microsoft Phone System	No
WMS network	No

Below the License usage section is the 'License actions' section, which contains several buttons:

- PBX Key** (highlighted with a red box) and **Activate** button
- Refresh via Internet** button
- Download logo** and **Remove logo** buttons
- Renew** button

On the left side of the License actions section, there are labels for 'Gold Partner Logo' and 'SSL Certificate'.

- Click **Activate**:

The screenshot shows the Wildix management interface. At the top, there is a dark blue navigation bar with icons for home, back, forward, and settings. Below this, the 'System' section displays the following information:

Status	Not activated
System name	[Redacted]
SW Serial	[Redacted]
HW Serial	[Redacted]
Processor	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
Memory	7958 Mb
Users	0
Concurrent calls over trunks	0

The 'License usage' section shows the following data:

Basic	0 / 0
Essential	0 / 0
Business	0 / 0
Premium	0 / 0
Wizyconf Room	0 / 0
Service	0 / 0
x-bees	No
x-caracal	No
Wizywebinar	No
CLASSOUND	No
Microsoft Phone System	No
WMS network	No

The 'License actions' section contains several buttons: 'Activate' (highlighted with a red box), 'Refresh via Internet', 'Download logo', 'Remove logo', and 'Renew'. On the left side of this section, there are labels for 'Gold Partner Logo' and 'SSL Certificate'.

Your PBX is now activated:

System

Status: **Activated**

System name: [blurred]

SW Serial: [blurred]

HW Serial: [blurred]

Processor: Intel(R) Xeon(R) CPU E5620 @ 2.40GHz

Memory: 7958 Mb

Users: 41

Concurrent calls over trunks: 220

License usage

Basic	0 / 10
Essential	0 / 10
Business	0 / 10
Premium	0 / 10
Wizyconf Room	0 / 0
Service	0 / 10
x-bees	Yes
x-caracal	No
Wizywebinar	Yes
CLASSOUND	Yes
Microsoft Phone System	No
WMS network	Yes

License valid until: **2023-01-14**

License actions

Deactivate license Refresh via Internet

Gold Partner Logo Download logo Remove logo

SSL Certificate Renew

Introduction to WMS

After you have successfully activated the PBX and changed the admin password, let's take a closer look at the WMS interface.

Users Groups Phonebooks

Q Search

	Full Name	Login	Extension	Fax	Office	Email	Mobile	Dialplan	Fax dial...	Group	Department	License type
admin			111		+3912345678	kzenia.babych@wildix.com		internalc...	internalc...	Admin		Premium

 Edit

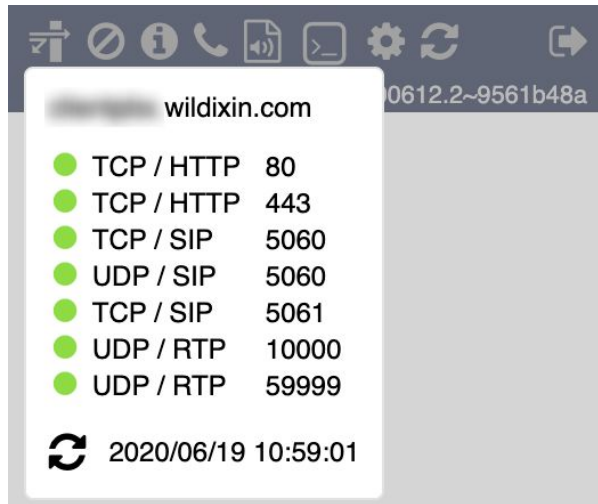
Main menu:

- 1 - *Users*: add users, change preferences and passwords, move users from one PBX to another one in WMS network, set up permissions of ACL groups, import phonebooks
- 2 - *Trunks*: add VoIP trunks, set up parameters of media gateways, create huntgroups (groups of trunks), import pricelists
- 3 - *Devices*: provision devices, assign WP phones and ports of analog devices to users, create W-AIR networks

- 4 - *Dialplan*: set up the strategy for call routing, create timetables, switches, create call groups, create IVRs, set up the general Dialplan parameters
- 5 - *Settings*: system and network configuration

Secondary (top) menu:

- 6 - *Port blocks*: notification (red=error; yellow=warning) in case ports needed for remote trunks / phones are not open (consult the document: [Ports used by Wildix services](#)):



- 7 - *SIP blocks*: click to see the list of temporarily banned IP addresses (in case of unsuccessful login attempt). The icon is visible only in case there are banned devices:



Ability to view the list of blocked IPs and unblock them is limited to the "admin" user

- 8 - *Info* (available only for the admin user!) : click to open monit application that provides the information on the system performance, the current processes, the resources engaged, etc:

Home > Use **M/Monit** to manage all your Monit instances Monit 5.25.1

Monit Service Manager

Monit is running on wildix-gateway and monitoring:

System	Status	Load	CPU	Memory	Swap
wildix-gateway	OK	[0.00] [0.03] [0.00]	0.7%us, 0.3%sy, 0.0%wa	62.2% [292.7 MB]	1.1% [5.8 MB]

Process	Status	Uptime	CPU Total	Memory Total	Read	Write
zabbix_agentd	OK	2h 9m	0.0%	2.1% [9.7 MB]	-	-
xmpp	OK	2h 8m	0.0%	11.2% [52.5 MB]	0 B/s	-
wudpecho1	OK	2h 9m	0.0%	0.1% [692 kB]	0 B/s	-
wudpecho2	OK	2h 9m	0.0%	0.1% [676 kB]	0 B/s	-
whoteld	Initializing	-	-	-	-	-
turnserver	OK	2h 8m	0.0%	2.4% [11.4 MB]	0 B/s	-
iproxyd	OK	2h 8m	0.0%	2.0% [9.6 MB]	0 B/s	-
sipproxy	OK	51m	0.0%	84.5% [397.2 MB]	0 B/s	-
rtengine	OK	2h 8m	0.0%	1.0% [4.7 MB]	0 B/s	-
rsyslog	OK	2h 8m	0.0%	0.5% [2.4 MB]	0 B/s	0 B/s
php-fpm	OK	2h 8m	0.5%	12.2% [57.2 MB]	0 B/s	0 B/s
pbxengine	OK	2h 8m	0.1%	11.8% [55.4 MB]	0 B/s	0 B/s
ntpd	OK	2h 8m	0.0%	0.7% [3.4 MB]	0 B/s	-
nginx	OK	2h 8m	0.0%	3.0% [14.0 MB]	-	-
memcached	OK	2h 8m	0.0%	0.5% [2.2 MB]	0 B/s	-
ldap	OK	51m	0.0%	1.3% [6.2 MB]	0 B/s	0 B/s
fcgiwrap	OK	2h 7m	0.0%	0.5% [2.4 MB]	0 B/s	-
dnsmasq	OK	47m	0.0%	0.1% [468 kB]	0 B/s	-
cron	OK	2h 8m	0.0%	0.6% [2.7 MB]	0 B/s	0 B/s

Program	Status	Output	Last started	Exit value
sipproxy_udpj_wrtun	OK	no output	06 Sep 2019 16:43:28	0

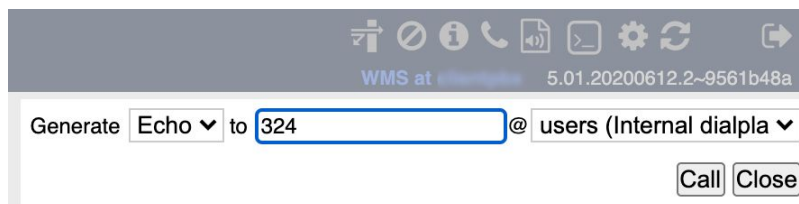
Filesystem	Status	Space usage	Inodes usage	Read	Write
root	OK	27.7% [2.7 GB]	10.1% [66091 objects]	7.9 kB/s	7.4 kB/s

File	Status	Size	Permission	UID	GID
servicelog	OK	282.9 kB	0755	1000	1000
cw_crash	OK	-	-	-	-

Host	Status	Protocol(s)
WmsNetVpnMaster	OK	[DEFAULT] at port 1194
WmsNetVpnMasterip	OK	[DEFAULT] at port 1028

Copyright © 2001-2017 Tiddeslab. All rights reserved. [Monit web site](#) | [Monit Wiki](#) | [M/Monit](#)


- 9 - *Generate call*: click to perform a test call or an echo test using a selected Dialplan procedure (you must specify the extension in the input field and you can select the Dialplan procedure to follow for this call):



- 10 - *Sounds*: via this menu you can upload music on hold and ringtones, record the messages for operator (More information in chapter [Record and playback audio messages](#)); you can generate audio files using TTS (Text-to-Speech), more information: [Wildix Business Intelligence - Artificial Intelligence services](#)
- 11 - *Terminal*: access to the console (enabled only for the admin user)
- 12 - *Debug*: click to view the simple
- log of each call generated on the PBX (More information in chapter [Dialplan debug](#))
- 13 - *Reboot / Power Off*
- 14 - *Logout*

Basic WMS settings

In this chapter we will see the basic settings which you should pay attention to before proceeding with PBX configuration.

 For the basic settings of a PBX residing in the USA, please refer to [Basic PBX Settings USA](#).

Time & date

Go to *WMS Settings -> System -> NTP Server*.

Make sure that the time and the date of the PBX are correct and are synced with the NTP server.

NTP Server	
Primary NTP Server	<input type="text" value="time1.google.com"/>
Secondary NTP server	<input type="text" value="time2.google.com"/>
Time and date of the server 19/06/2020 12:10:15	
<input type="button" value="Save"/>	

Language & Region

Go to *WMS Settings -> PBX -> Language & Region*.

Select your settings for:

- *Language*: (not to be confused with WMS interface language, which can be selected for the current user in *WMS -> Users -> select the user, click **Edit***) select the default language for this PBX, which means by default all the system sounds are pronounced in this language in case there's no sound package installed for the language selected by user (e.g. PBX default language is "Italian", user selected "Dutch", in case Dutch sound package is not installed, all the system sounds are played back in Italian for this user)
- *Default Tone Zone*: select your country / region
- *Country Code*: select your country code
- *Time zone*: select your time zone
- *Sounds packages*: select the sound packages to be installed (maximum three sound packages can be enabled at a time)

Language & region	
Language	Italian
Default Tone Zone	
Country Code	39 Italy
Time zone	Europe Rome

Sounds packages	
German	<input type="checkbox"/>
English	<input checked="" type="checkbox"/>
Spanish	<input type="checkbox"/>
American Spanish	<input type="checkbox"/>
French	<input type="checkbox"/>
Italian	<input checked="" type="checkbox"/>
Dutch	<input type="checkbox"/>
English-US	<input type="checkbox"/>

Click **Save** to apply the changes.

Remote Support

Important: Remote support for Cloud PBXs is removed starting from WMS 4.0X.

Go to *WMS Settings -> Tools and utilities -> Remote support*.

Make sure that the *Server status* is started:

Remote support	
Serial:	
Server status:	started IP:
<input type="button" value="Reload"/> <input type="button" value="Disable"/>	

PBX location	
Last location update:	
Latitude:	50.45
Longitude:	30.5233
Address:	, , Ukraine
Updated at:	14:39:20 2020-01-16
Send the location of the PBX to WMP once a week <input checked="" type="checkbox"/>	
<input type="button" value="Update location"/> <input type="button" value="Save"/>	

The following IP ranges are now used by Remote Support server (make sure they don't collide with your internal network ranges):

- 172.16.0.0/16

- 172.20.0.0/16
- 172.25.0.0/16

For remote support it is necessary to open access to external server *vpn2.wildix.com* on the following ports on our firewall/router:

- outgoing tcp:443
- incoming: tcp:443 or custom secure port

More details on ports used by different Wildix services: [Ports used by Wildix services.](#)

Activation & Licenses

Go to *WMS Settings -> Tools and utilities -> Activation / Licenses.*

Make sure that the PBX and the Additional services are activated:

- *System* section -> Status: *Activated*
- *License usage* section: *Yes* in front of a service

The screenshot displays the 'Activation / Licenses' configuration page. It is divided into several sections:

- System:** A table showing system details. The 'Status' is highlighted with a red box and is 'Activated'. Other details include System name, SW Serial, HW Serial, Processor (Intel(R) Xeon(R) CPU E5620 @ 2.40GHz), Memory (7958 Mb), Users (41), and Concurrent calls over trunks (220).
- License usage:** A table listing various services and their activation status. A red box highlights the following:

x-bees	Yes
x-caracal	No
Wizywebinar	Yes
CLASSOUND	Yes
Microsoft Phone System	No
WMS network	Yes
License valid until	2023-01-14
- License actions:** A section containing several buttons: 'Deactivate license', 'Refresh via Internet', 'Download logo', 'Remove logo', and 'Renew'.



To refresh the licenses you enabled on WMP, click **Refresh via Internet.**

Storage services (Hardware, Virtual PBX)

Go to *WMS Settings* -> *System* -> *Storages*.

The USB key you have inserted into the PBX serves to store such data as Voicemail messages, call recordings, faxes, CDR, CTI data, etc. It is recommended to store the Backups on another USB drive or on a Windows / NFS Share, to be able to restore the system in case of the primary USB drive's failure.

The first section *Storage Device* displays the storage devices mounted at the system startup with the relative table of the partitions and the usage of the specified partition.

Type	Storage Device	Action
HDD	VMware Virtual IDE Hard Drive - Partition 1 Type: ext2	
HDD	Linux File-Stor Gadget - Partition 1 Format: ext2 Size: 1008MB Avail: 955MB Usage: 1%	
	CDR CSV <input type="checkbox"/>	
	CDR SQLite <input type="checkbox"/>	
	Faxes <input type="checkbox"/>	
	Backups <input type="checkbox"/>	
	CTI <input type="checkbox"/>	
	Voicemail <input type="checkbox"/>	
	Call recording <input type="checkbox"/>	

Add NFS/Windows share

Click **Initialize** under *Action* column to start the partition and formatting procedure of the storage device.

Click **+** under *Action* column to add partition for each Service.

It is possible to use a storage server such as Windows Share or NFS Share: click **+** *Add NFS/Windows share* a storage server.

More details: [WMS Settings Menu Guide](#).

System Backup

Each time before proceeding with the system upgrade, it is necessary to create a backup.

Go to *WMS Settings* -> *Tools and utilities* -> *Backup system*.

This menu allows you to create and download the system backup and set up a scheduled system backup.

To create a backup:

- Click **Generate and download backup** to save the backup to your PC
- Otherwise click **Generate backup** to save a backup on the PBX (or on the USB key):

Backup system Scheduled backups

Name	Creation date	Size
_2020.04.17_17.08.36_5.01.20200410.3_22110000326b_wms_b_24681.tar.gz	Apr 17 2020 17:08:39	43.01 KB
_2020.05.19_16.38.37_5.01.20200416.1_22110000326b_wms_b_16a5c.tar.gz	May 19 2020 16:38:41	541.27 KB
_2020.05.25_10.42.56_5.01.20200514.1_22110000326b_wms_b_1c9ac.tar.gz	May 25 2020 10:42:59	544.63 KB
_2020.05.27_10.32.13_5.01.20200522.1_22110000326b_wms_b_d240e.tar.gz	May 27 2020 10:32:16	545.5 KB
_2020.06.10_14.34.18_5.01.20200526.1_22110000326b_wms_b_54a36.tar.gz	Jun 10 2020 14:34:21	551.04 KB
_2020.06.19_10.02.44_5.01.20200605.5_22110000326b_wms_b_5737c.tar.gz	Jun 19 2020 10:02:48	556.53 KB

Showing 1 to 6 of 6 entries Previous 1 Next 20

Upload backup on PBX: No file chosen

Reset WMS interface to factory defaults:

The tab *Scheduled backups* allows you to set up a scheduled system backup (daily / weekly / monthly) to share, FTP or mail. Configuration example:

Backup system Scheduled backups

Backup to share

Perform

Backup to FTP

FTP host

FTP port

FTP login

FTP password

FTP upload directory

Enable passive mode

Perform

Mail

Email

Perform

More details: [WMS Settings Menu Guide](#).

PBX upgrades

Starting from WMS 5.02.20201207.3, weekly automatic upgrade for the Stable repository is enabled by default. You can disable it, but it is re-enabled again after each new upgrade.

Go to *WMS Settings -> Tools and utilities -> Upgrade*.

Note: Each time before performing the upgrade you are prompted to create a backup!

The upgrade procedure is described in chapter [Upgrade WMS to the latest stable release](#).

Available repositories for upgrade:

- rel60 / rel50: stable version, it is recommended to upgrade customers PBXs from this source; changelog: [WMS Stable Changelog rel60](#); [WMS Stable Changelog rel50](#)
- rel60beta / rel50beta: beta version, available for Wildix Partners for tests in the lab before this version becomes stable; changelog: [WMS Beta Changelog rel60beta](#); [WMS Beta Changelog rel50beta](#)

Downgrade is not supported!

DHCP Server (Hardware, Virtual PBXs)

Go to *WMS Settings -> System -> DHCP server*.

If in the chosen network scenario PBX is used as the DHCP server to assign IP addresses to devices, check that the options of the service are enabled with the correct settings:

DHCP server Running on eth0

Enable DHCP server at boot time eth0

Network	10.100.4.0	Netmask	255.255.252.0
Start address: <small>must be more than 10.100.4.1</small>	10.100. 4.2	End address: <small>must be less than 10.100.7.254</small>	10.100. 4.10
Default lease time (mins)	3600	Maximum leases	5
Domain name suffix		Default gateway	10.100.4.1
Primary DNS server		Secondary DNS server	
Primary NTP Server		Secondary NTP server	
Primary WINS Server		Secondary WINS server	

Deny unknown clients

Save changes

Leases

Kind	IP Address	Mac Address	Hostname	Lease expires (local time d/m/y)
No data available in table				

Showing 0 to 0 of 0 entries Previous 1 Next 20

- Edit Purge leases

DHCP server is integrated for auto provisioning of supported devices. It's possible to enable the server for the initial configuration of the devices and successively disable it, otherwise to enable the parameter *Deny unknown clients*.

Parameters:

- *Enable DHCP server at boot time*: enables internal DHCP server and allows you to select the interface on which the server is enabled (normally eth1)
- *must be more than / must be less than*: range of IP addresses that can be assigned to hosts
- *Default lease time (mins)*: minimum time period for lease duration
- *Maximum leases*: maximum number of leases that can be assigned
- *Domain name suffix*: if the hosts are inserted in the network which is managed by the domain controller
- *Default gateway*: IP address of the router or of the PBX (in case of LAN interface)
- *Primary / Secondary DNS server*: addresses of DNS servers
- *Primary / Secondary NTP Server*: addresses of NTP servers
- *Primary / Secondary WINS Server*: addresses of WINS servers
- *Deny unknown clients*: if enabled, IP addresses are not automatically assigned to unknown hosts


All the IP addresses which DHCP server has assigned to devices, appear in the Leases table below.

Detailed information can be found in [WMS Settings Menu Guide](#).

SMTP Client


Go to *WMS Settings* -> *System* -> *SMTP client*.

SMTP client enables the PBX to send email notifications about new voicemails, missed calls, chat requests, call recordings, faxes, etc.

-  For Cloud PBXs, you can use the default server provided by Wildix:
- Check the box *Default settings*
 - Click **Save**

To add a new SMTP profile, proceed as follows:

- Select *Default* and click **Edit**
- Fill in the fields:
- *Email from*: address to be used by PBX to send emails

 Note: Starting from WMS 5.03, in case of using SMTP client w-smtp.wildix.com, the following email is by default used in the "From" field: no-reply@wildix.com

- *SMTP mail server*: server's postal address used by the company
- *Port*: listening port of the SMTP server
- *SMTP authentication method*: choose the authentication method for the SMTP server
- *Timeout*: select the timeout for the SMTP server to send notifications
- *User*: user name to access the server
- *Password*: password to access the server
- *HELO domain*: domain defined for sending emails. Default value is "localhost", change it in case anti-spam filters of the SMTP server block sending the message
- *Enable TLS*: TLS protocol enabled for the security of the connection to the server
- *Enable STARTTLS*: STARTTLS option enabled if provided by SMTP

SMTP client

Default settings

E-mail from

SMTP mail server

Port

SMTP authentication method

Timeout

User

Password

HELO Domain

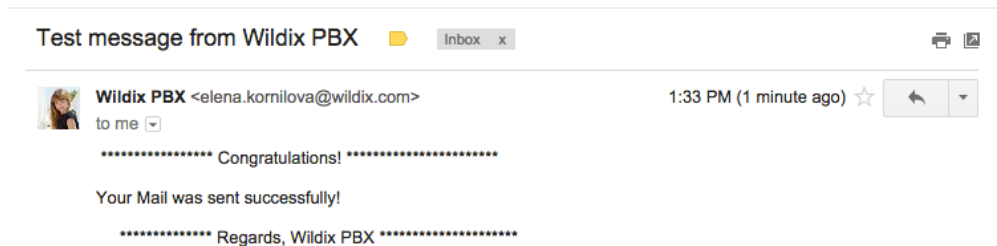
Enable TLS Enable TLS for the secure connection

Enable STARTTLS Enable STARTTLS to start TLS encryption

```

→ Content-Disposition: inline
→ User-Agent: Mutt/1.5.9i
→
→ ***** Congratulations! *****
→
→ Your Mail was sent successfully!
→
→ ***** Regards, Wildix PBX *****
→
← 250 2.0.0 Ok: queued as A7DA66093F
→ QUIT
← 221 2.0.0 Bye
                
```

- Click **Save**
- To make sure that the entered parameters are correct, enter the email address into the field located in the upper right section and click **Test**
- The logs are displayed in the field below and you receive the following email:



Note: in case you are encountering problems while creating an SMTP profile using Gmail client, read the guide: [WMS Settings Menu](#).

Fax server

Go to *WMS Settings* -> *System* -> *FAX/SMS Server*.

Wildix PBXs have the integrated FAX/SMS server. In this menu you can add a Fax Server profile which enables Fax2Mail, Mail2Fax, Mail2SMS services and fax / SMS sending via Wildix Collaboration.

Note: SMS sending is possible either through a third-party provider using CURL SMS sending, or using a W01GSM media gateway. More details: [WMS Settings Menu](#).

To enable FAX/SMS server, proceed as follows:

- Enter the email address into the field Send a copy of sent and received faxes and sent SMS to this e-mail:

FAX/SMS server

Send a copy of sent and received faxes and sent SMS to this e-mail

Standard SMS header

Fax delivery notification

Curl SMS send enabled

Curl SMS send ?

Server profiles

Name	Host	Dialplan procedure
gserver	imap.google.com	users

Showing 1 to 1 of 1 entries 1 row selected

- Click **+** to add a new FAX Server profile
- Fill in the fields:
- **Name**: enter the name (identifier)
- **Protocol**: select the protocol of communication with your email server (POP3 or IMAP)
- **Auth type**: select the preferred authorization type, Basic or OAuth2 (the support of OAuth2 for Fax/SMS Server starts from WMS 6.01.20221019.4). Depending on the chosen type, fill out the following fields:
 - a) In case of Basic Auth type:
 - **Server**: settings of your email server to access incoming messages
 - **User**: email address of user to access to the server
 - **Password**: password to access to email address of user specified in the field above
 - **Use SSL**: enables secure connection to the server (required by some email servers)

Fax/SMS Server
✕

Name

Test

Protocol

POP3 ▼

Auth type

Basic ▼

Server

imap.google.com

User

fax@wildix.com

Password

.....
👁

Use SSL

Dialplan procedure

users (Internal dialplan) ▼

Protection password

.....
↻
👁

Default LOCALSTATION

localhost

Default LOCALHEADER

localhost

Keep e-mails and faxes on server

Save

b) In case of OAuth2 authorization type:

- *Auth provider*: choose auth provider (Google or Office 365) -> click Login and perform the login
- *Dialplan procedure*: select the Dialplan procedure to manage faxes sent by users
- *Protection password*: security password for MAIL2FAX service
- *Default LOCALSTATION*: sender's fax machine ID, appears at the top of each page of outgoing fax, if not specified the default value "Fax Server" is used
- *Default LOCALHEADER*: fax header to identify the sender, appears at the top of each page of outgoing fax, if not specified the default value "Wildix PBX" is used
- *Keep e-mails and faxes on server*: enables storing of messages on the server

Fax/SMS Server ✕

Name

Protocol

Auth type

Auth provider

Dialplan procedure

Protection password

Default LOCALSTATION

Default LOCALHEADER

Keep e-mails and faxes on server

- Click **Save**

The PBX checks the mailbox and once any new email corresponding to Mail2Fax, Mail2SMS or Fax2Mail parameters are found, the system forwards it to the specified destination.

More information on Fax Server: [FAX/ SMS Server Quick Admin Guide](#).

Call & chat history

Go to *WMS Settings* -> *PBX* -> *Call and chat history*.

To be able to store call and chat history, you must enable a CDR backend. You can also enable contact notes and set up different options that allow auto-deleting of old calls, chats, voicemails and recordings after a specified number of months. Detailed information can be found in [WMS Settings Menu Guide](#).

For Cloud PBXs you don't need to specify a backend, just make sure that the box Enabled is checked:

Settings Call and chat history

Enabled

Enable contact notes

Tags

Hide in CDR-View digit(s)


Delete calls after month(s)

Delete chats after month(s)

Delete voicemail after month(s)


Delete recording after month(s)

Save

 Note: Starting from WMS Beta 6.01.20220721.1, it is possible to set up backend for storing chat and call history (CDR) for Cloud PBX.

Wildix PBX supports three CDR storage modes:

- External server Microsoft SQL: MySQL or MSSQL. The server must be previously installed and must be reachable by the PBX
- Internal database: CDR Sqlite. In this case CDR is stored on the PBX (on the backend specified for CDR storage). This backend is recommended for PBXs WGW40 and less
- CSV file

 Important: for PBX with 90 and more users under high load, external server (MySQL or MSSQL) is recommended.

To enable CDR backend, proceed as follows:

- Configure at least one CDR backend: go to one of the tabs *CDR MSSQL*, *CDR MySQL*, *CDR Sqlite* and enable connection to the server; example of MSSQL/MySQL configuration:
 - *Enabled*: Check the box to enable the backend
 - *Hostname*: The name or the IP address of the remote server
 - *Database name*: The existing database where the CDR must be saved
 - *CDR Table name*: The name of the table that the PBX creates on the remote database
 - *User*: The user to access to the server
 - *Password*: The password to access to the server
 - *Port*: specify the port used

Settings **CDR MSSQL** **CDR MySQL** CDR Sqlite CDR CSV

Enabled	<input checked="" type="checkbox"/>
Hostname	<input type="text"/>
Database name	wms_uc_cdr
CDR table name	cdr
User	wms
Password	<input type="password"/>
Timeout	10
Port	3306

Mysql CDR engine enabled
 Connected to , port 3306 using table
 cdr for 2 hours, 35 minutes, 23 seconds.
 Wrote 96 records since last restart and 48 records since last reconnect.

- Click **Save**
- Go to the first tab *CDR Settings* and select the backend used for displaying CDR statistics:
 - *CDR-backend*: select here the CDR backend (more information on other fields can be found here: [WMS Settings Menu Admin Guide](#))

Settings **CDR MSSQL** **CDR MySQL** **CDR Sqlite** CDR CSV

CDR-backend	MySQL ▾
Enable contact notes	<input checked="" type="checkbox"/>
Tags	marked, confirmed
Hide in CDR-View	<input type="text" value="3"/> digit(s)
Delete calls after	<input type="text" value="0"/> month(s)
Delete chats after	<input type="text" value="0"/> month(s)
Delete voicemail after	<input type="text" value="0"/> month(s)
Delete recording after	<input type="text" value="0"/> month(s)

Call Detail Record (CDR) settings

Logging: Enabled
 Mode: Batch
 Log unanswered calls: Yes
 Log congestion: No
 * Batch Mode Settings

Safe shutdown: Enabled
 Threading model: Scheduler plus separate threads
 Current batch size: 0 records
 Maximum batch size: 100 records
 Maximum batch time: 3 seconds
 Next batch processing time: 3 seconds
 * Registered Backends

mysql
 cdr_manager
 cdr-custom
 Count thread batch process: 0

- Click **Save**

For each backend there is a log shown in the right part of the screen, with the actual status and eventual errors. After you have enabled the backend for saving CDR, the PBX can save the calls and chat history. Calls history can be accessed from Collaboration, WP, iOS / Android apps (W-AIR shows only local call history).

Note: It is possible to configure SSL connection for sending CDR data to external MySQL server. See the following guide for instructions: [Custom config parameters List: Enable SSL connection to remote MySQL server](#).

SIP-RTP

Go to *WMS Settings* -> *PBX* -> *SIP-RTP*

The default parameters present on this page are set up in accordance with VoIP protocol.

Check the following parameters:

- *Auto discover external IP address* (Hardware / Virtual PBX): enable to automatically discover the public IP address using DynDNS website url entered into the field below
- *DynDNS website url* (Hardware / Virtual PBX): the URL of the service used to discover the public IP address (<http://checkip.wildix.com/> by default)
- *External secure port* (Default 443) (Hardware / Virtual PBX): this option allows you to enter a different port used for TLS connections
- *Auto add new devices in local networks* (Hardware / Virtual PBX): must be enabled to allow auto-configuration of Wildix devices via auto.wildix.com (the option is enabled for 2 hours after which it is automatically disabled)

Settings SIP-RTP

Auto discover external IP address

DynDNS website url

External IP address

External secure port

Use only https

Random music on hold

Default music on hold

RTP start port

RTP end port

Outgoing registration timeout (seconds)

Jitter buffer : min delay

Jitter buffer : average delay

Jitter buffer : max delay

RTP / T.38 ToS / DSCP

SIP ToS / DSCP

Auto add new devices in local networks (for 2 hours)

Custom Direct RTP Subnets

If you want to enable direct RTP in networks larger than /24, please enter them here
For example:
10.0.0.0/16

TLS Certificate (*.crt) No file chosen

TLS Private Key (*.key) No file chosen
Private key should be decrypted

Click **Save** to apply changes. More information on SIP-RTP settings can be found here: [WMS Settings Menu Admin Guide](#).

Dialplan General Settings

Go to *WMS -> Dialplan -> General Settings*.

This menu allows you to set up the default parameters for calls management. The default parameters present on this page should be changed in case the operator requires it.

Parameters:

- *Park call timeout*: timeout in seconds for return from park orbit. Make sure you define the value for a call to return from Park Orbit; more information about parking feature: [How to implement the Parking feature](#)
- *Prefix for external line*: prefix to get the outside line (0 by default)

- *International Prefix*: prefix to call abroad (00 by default)
- *National Prefix*: prefix to call within your country (0 by default)
- *Internal call default timeout*: timeout after which the call to another user is forwarded (if forwarding is enabled in user preferences) or terminated
- *First digit timeout (secs)*: timeout after which the call is terminated in case there is no input (time countdown starts if the handset is raised)
- *Interdigit timeout (secs)*: timeout in seconds after which the number is dialed automatically unless the user presses the Send call key on the phone
- *Send call key*: it's possible to select #, *, or None as a send key
- *Playback tones while entering number*: if enabled, DTMF tones are played
- *Quality of recorded voicemails / recordings*: choose the optimal quality and file size
- *Send mail notification after the record is complete*: if enabled, users receive notification by email after the record is complete
- *Attach files with records to emails*: if enabled, users receive recording files attached to email notification
- *Convert Voicemails to text and send by email*: if enabled, Voicemails are converted to text and sent to user by email (read the guide [Wildix Business Intelligence - Artificial Intelligence services](#) for more information)
- *Notify by email in case SIP trunk registration status is changed*: if enabled, the PBX admin receives notification about SIP trunks changing their registration status
- *Announce date, time and caller phone number for Voicemail messages*: if disabled, user is invited to press a key in Voicemail IVR menu in order to hear date, time and caller phone number for each Voicemail
- *Set dialplan variables*: this field allows setting Custom Dialplan variables; documentation: [Custom Global Dialplan Variables List](#)
- *Set quick dial patterns*: this field is used only for the first generation of WP phones (pre 2015)!

[Dialplan rules](#)
[Call Groups](#)
[Paging Groups](#)
[Timetable / Switch](#)
[IVR](#)
[Feature codes](#)
[General Settings](#)

Park call timeout	<input type="text" value="60"/>
Prefix for external line	<input type="text" value="0"/>
International Prefix	<input type="text" value="00"/>
National Prefix	<input type="text" value="0"/>
Internal call default timeout	<input type="text" value="65"/>
First digit timeout (secs)	<input type="text" value="600"/>
Interdigit timeout (secs)	<input type="text" value="2"/>
Send call key	<input type="text" value="#"/>
Playback tones while entering number	<input checked="" type="checkbox"/>
Quality of recorded voicemails	<input type="text" value="mp3 - normal quality, normal size of files"/>
Quality of calls recordings	<input type="text" value="wav - the best quality, large size of files"/>
Send mail notification after the record is complete	<input checked="" type="checkbox"/>
Attach files with records to emails	<input checked="" type="checkbox"/>
Convert Voicemails to text and send by email	<input checked="" type="checkbox"/>
Notify by email in case SIP trunk registration status is changed	<input type="checkbox"/>
Announce date, time and caller phone number for Voicemail messages	<input type="checkbox"/>
Set dialplan variables Set custom dialplan variables. For example: VAR1=VALUE1 VAR2=VALUE2 (Do not insert spaces)	<input type="text" value="USER_CAN_PAUSE_RECORDING=no
MULTILOGIN_SUPPORT=yes"/>
Set quick dial patterns Set custom dial patterns For example: 2[0-9][0-9] 3[0-9][0-9] (Do not insert spaces)	<input type="text" value="1[0-9][0-9]
2[0-9][0-9]"/>

WMS Network

Introduction to WMS Network

WMS Network is a secure intra network, which enables the colleagues located in offices to collaborate in one transparent and automatic environment.

WMS Network is normally deployed in these situations:

- **Multisite environment:** you need to enable flawless communication between different offices of the company
- **Failover / redundancy or load sharing:** one PBX is the primary, another PBX is the secondary (backup PBX), which works in idle mode and receives all the updates from the primary PBX; in case of the primary PBX failure, the secondary PBX takes on, ensuring the continuity of the service. In this case all the devices have a double SIP registration (both to the Primary and the Secondary PBX). Read [Failover - Admin Guide](#).

Wildix system supports Hybrid scenarios, where Hardware, Cloud and Virtual PBXs can be connected in the same WMS Network.

Sharing of Wildix licenses is possible in WMS network. More information: [PBX Licensing and Activation - Admin guide](#).

In this guide we will show how to deploy the WMS Network for a multisite scenario.

Key features of WMS Network:

- Presence status of users and internal communication free of charge (pay only for Internet connection)
- Users database resides on a distributed LDAP server; each user added to the system is immediately visible and can be contacted by other users of the system
- Roaming profile: users can move between the sites of the company while keeping the same number and user preferences
- One PBX in the network is assigned as the Server: any change that take place on a Client PBX first is passed to the Server and then from the Server to other Clients
- Auto sync of users, call groups and ACL configuration between the PBXs in the WMS Network allows for significant time savings on configuration and maintenance
- Direct peer-to-peer communication between PBXs, in case direct connection between two Clients is impossible, they can use Server as a proxy
- WMS Survivability: continuity of internal and external calls in case one PBX in the network (including the Server) becomes unavailable
- WMS Auto-recovery: in case of Server failure, another PBX in the WMS Network dynamically takes up all the functions of the Server
- Local survivability: a Client disconnected from the network continues to operate, but without the possibility to receive the users database updates
- Each PBX has its own local lines, users, IVRs and Dialplan procedures, however it's possible to set up the Dialplan to route calls via a different PBX in the WMS Network, thus using its local lines (even in a different country)
- Up to 1000 nodes in WMS 5
- Up to 5000 users on one PBX in WMS 5
- Up to 500 concurrent calls
- Up to 100k users in WMS network



Server and Client configuration

If PBXs are remote and communicate via Internet, it's necessary to allow outgoing traffic on 443 TCP (or custom secure port) and 1194 UDP on firewall / router on the side of the Client PBX towards the Server PBX.

Go to *WMS Settings* -> *PBX* -> *WMS Network*.

Server configuration:

- *PBX mode*: select *Server*
- *MTU*: specify the size of the largest protocol data unit that the can be passed on VPN (MTU = maximum transmission unit)
- *Login*: set up the Login (must be the same on Server and Clients)
- *Password*: set up the Password (must be the same on Server and Clients)

Click **Start** to enable WMS Network:

WMS Network settings

Data Sync Role	Server
Connection status:	ON
Internal IP:	
Serial:	
Sync configuration port:	443
Server VPN port:	1194
MTU:	900
Login:	w77373ed3e20f
Password: Show

[Generate credentials](#) [Update parameters](#)

[Start](#) [Stop](#)

Client configuration:

- *Data sync mode*: select *Client*
- *Server PBX IP*: specify the WAN IP of the Server PBX (or the *.wildixin.com domain name)
- *MTU*: same as on Server PBX
- *Login*: same as on Server PBX
- *Password*: same as on Server PBX

Click **Start** to enable the Client mode on this PBX:

WMS Network settings

Data Sync Role: Client

Server PBX IP: [redacted]

Sync configuration port (def. 443 tcp): 443

Server VPN port (def. 1194 udp): 1194

Client VPN port (def. 1194 udp): 1194

MTU: 900

Login: w77373ed3e20f

Password: Strong [Show](#)

Go to *WMS Users* -> *PBXs*: now you can view all the PBXs in your WMS network and click on the Host name to connect to any of these PBXs.

IP	Serial	Host name	Fallover	WMS version
[redacted]	[redacted]	wildix.com	wildix.com	6.02.20230117.1
[redacted]	[redacted]	wildix.com		6.02.20221221.1
[redacted]	[redacted]	wildix.com		6.02.20221207.1

Showing 3 to 3 of 3 entries Previous 1 Next

- Notes:**
- Enabling Client mode on a PBX that has been previously in use will delete all users and groups from the Client; read how to prevent this from happening: [WMS Settings Menu Guide](#).
 - All the PBXs belonging to the same WMS Network can have only one *admin* user, which is the *admin* user of the Server PBX.
 - Starting from WMS 5.03, Directory sync protocol is routed outside of WMS network. For correct behaviour of WMS Network, first update Server PBX and then Client PBXs.

Adding / importing users and phonebooks

- !** It is required to set licenses per each user! Consult [Assign correct license type to each user](#) for detailed information.
- In case the number of licenses used was exceeded, users do not lose access to any functionality, but the system administrator is informed with the notification:



License usage exceeded.
Basic: 8 / 0
Essential: 16 / 8
Business: 8 / 11
Premium: 16 / 16
Wizyconf room: 0 / 1
Service: 4 / 4
Wizywebinar: 0 / 2
x-caracal: 0 / 1
Classound: 0 / 1

The system administrator can also check the number of licenses bought and used in WMS *Settings* -> *Tools and utilities* -> *Activation / Licenses*.

Users can be added manually or imported from MySQL / MSSQL, LDAP / AD, Google, Office 365, Exchange Server, CSV file, Zoho CRM or other sources.

Adding users manually


Go to *WMS* -> *Users*.

It is possible to add users of different type:

- *Admin*: system administrator with the right to access WMS
- *User*: regular user of the system
- *Fax*: T.38 support for analog phones or faxes connected via W01FXS media gateways
- *Park Orbit*: parking lot, read more about parking feature: [How to implement the Parking feature](#)
- *Room*: hotel room; Wildix PBXs supports hotel features via WebAPI hotel manager (read more: [WebAPI Admin Documentation](#)) and FIAS protocol (read more: <https://www.wildix.com/fias-fidelio/>)

To add a user, click + and enter the parameters into the table:

- *User*: select type User
- *Full Name*: enter the user's full name
- *Login*: this field is used for login with Active Directory credentials (read more: [Import of Contacts and Users Guide/ Active Directory](#))
- *Extension*: the extension number (normally in format 1XX, 2XX)
- *Fax and Office*: DID number for faxes and calls
- *Email*: personal email address for notifications (Voicemail, call recordings)

 Important: user's email should be unique. The same email cannot be used twice.

- *Mobility*: personal mobile number for mobility extension management (mobility feature allows making and receiving calls to mobile number via the company PBX)
- *Dialplan*: dialplan procedure for outgoing calls, by default "users"
- *Fax dialplan*: dialplan procedure for sending faxes from Wildix Collaboration, by default "users"
- *Language*: language of the interface and system sounds
- *Group*: ACL group, by default "default"
- *Department*: in Collaboration web interface, users are by default grouped by their Group (ACL group) in roster; however if Department field is specified, users are grouped by Department field

! Difference between Group and Department fields:

- *Group* field assign user to a certain ACL group; ACL is a set of user permissions; you can change ACL permissions of groups in *WMS -> Users -> Groups*; more information: [ACL rules and Call classes management - Admin Guide](#)
- You can decide to group users in Collaboration -> Colleagues menu either by *Group* or by *Department* field, but *Department* field doesn't affect users ACL permissions
- Starting from WMS Beta 5.04.20211227.3, there is an option to create a multilevel hierarchy of Departments. See the guide [How to configure Departments tree](#) for more details.

- License type: assign a license based on needed functionalities, more information: <https://www.wildix.com/licensing/>

Click **Save** to save a new user:

Form fields and values:

- Role: User
- Full Name: Bill
- Login: user3301
- Extension: 3301
- Fax:
- Office:
- Email:
- Mobile: +38099999000
- Dialplan: users (Internal dialplan)
- Fax dialplan: users (Internal dialplan)
- Language: En
- Group: Default
- Department:
- License type: Premium

Users are displayed in the table:

	Full Name	Login	Extension	Fax	Office	Email	Mobile	Dialplan	Fax dialplan	Group	Department	License type	PBX
1	Bill	user3301	3301					users	users	Default		Premium	

Showing 1 to 1 of 1 entries 1 row selected Previous 1 Next


Toolbar actions: 2 Add, 3 Edit, 4 Delete, 5 Set passwords, 6 Edit preferences, 7 Send Welcome Message, 8 Invite to x-bees, 9 Move users to another PBX, 10 Export CSV, 11 Import

The first column displays an icon representing the user type:

- admin
- user
- fax
- park orbit
- room

The second column displays the user's device SIP registration status, which can be:


- Green: user has a SIP device registered (Collaboration Web Phone, VoIP phone, TAPI, iOS/ Android mobile app in active use)
- Grey: user has no SIP device registered

 Important: SIP registration status indication displayed in *WMS - Users* is not a substitution for Wildix Collaboration user presence status indication.

At the moment the status is grey, because users have no devices registered to their accounts and none of them is connected to Wildix Collaboration.

Description of parameters:

- 1 - **+Add**: add user
- 2 - **Edit**: change the same parameters, which are available upon adding a user
- 3 - **Delete**: delete one or multiple users

 Note: It is possible to remove user's personal data (calls, chats, voicemails, phonebooks, recordings, faxes) when deleting this user. Refer to section [Delete user data](#)

Limitations:

- the feature works for standalone PBXs or for WMS Networks PBXs which share the same MySQL or MSSQL DB
 - if a user to be deleted is an owner of contacts in shared phonebooks, than contacts remains without an owner
 - voicemails left via FC "Voicemail: 81 are not reset (but it is possible to reset them via Terminal, consult [this Article](#))
- 4 - **Set passwords**: change user passwords; for security reasons only the admin user can set passwords for other admins of the system; by default strong passwords are automatically created by the system, read more about changing user passwords in chapter [Set user passwords](#)
 - 5 - **Edit preferences**: manage user preferences and phone features, for details, see chapter [User preferences](#)
 - 6 - **Send Welcome Message**: send a message to newly created users with details of access to Wildix Collaboration (URL, login, password); for security reasons, only the admin user can send welcome messages to other admins of the system
 - 7 - **Move users to another PBX**: in case of WMS Network, you can select one or more users and move them to another PBX in the network
 - 8 - **Export CSV** (available only for the admin user): save a CSV file containing users information in *.csv format to your PC
 - 9 - **Import**: import users from MySQL / MSSQL, LDAP / AD, Google, Office 365, Exchange Server, CSV file, Zoho CRM, other resources; more information in chapter [Import of users and phonebooks](#)
 - 10 - *Search field*
 - 11 - *Select PBX*: in case of WMS Network, you can select to view users of a different PBX in the Network or to view all the users registered to all the PBXs in the WMS Network

Set user passwords

The first time you connect to the WMS, you are required to change the generic admin password.

System automatically generates strong passwords for each new user, and it is not necessary to change them.

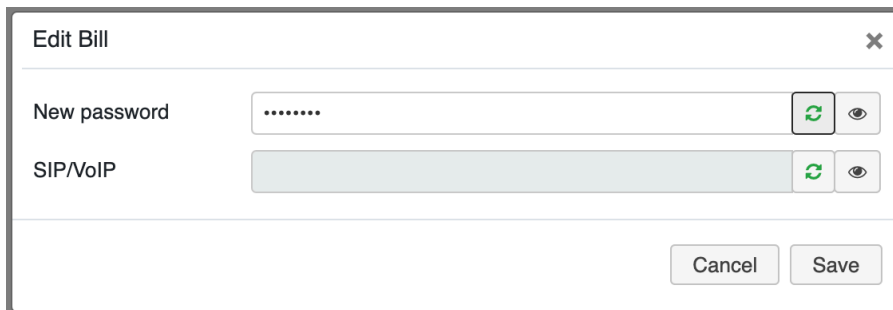
To send access credentials to users, the *admin* user should select the user (users) and click **Send Welcome Message** from *WMS -> Users*.

Users can change their passwords from Collaboration interface (*Collaboration Settings -> Personal*).

Only the *admin* can set passwords for other users with admin rights (users of *admin* type).

To set user passwords, select a user in *WMS -> Users* and click **Set passwords**:

- *New password*: password used to access WMS/Collaboration
- *SIP/VoIP* - password to assign and provision non-Wildix devices




For security reasons, this configuration window allows only setting new passwords, but it doesn't display previously created passwords.

- Click **Generate** (the green icon) to automatically generate a strong password
- Click **Show** (the eye icon) to see the newly generated password


Otherwise enter your own strong password into the fields, consisting of at least 8 symbols, at least 1 uppercase, 1 lowercase, 1 digit.

Click **Ok** to apply the changes.

 **Note:** Starting from WMS 6.01.20221019.4, when admin changes password of a user via WMS (WEB/ SIP password), all active sessions of the user are dropped and user is logged out. In case of changing SIP password, automatic logout is applied for web Collaboration only.

User preferences

To edit user preferences, select a user and click **Edit preferences** from *WMS -> Users*.

 **Note:** Many of the settings present in this menu, can be modified directly by user from *Collaboration -> Settings*; Call features can be also modified from WP and via Feature Codes (more information on system feature codes: [Feature Codes and Pre answer Services Guide](#)).

Features: call features for different call classes

- *Classes*: select the call class before modifying the phone features below; the phone features will be applied only to the selected call class:
 - *Internal / internal DND / internal away*
 - *External / external DND / external away*
 - *Blacklist / blacklist DND / blacklist away*



Call classes can be set for Contacts in *Collaboration* -> *Phonebook*, more information in *Collaboration* user guide (Phonebook chapter): [Collaboration 5.0X](#).

It is also possible to set the call class via Dialplan applications *Set / Jump to if call type is*, more information in Dialplan applications guide: [Dialplan applications Admin Guide](#).

- *Activate the class*: by default, all the settings are applied for Internal call class; to set up call Features for a different call class, first select the needed call classes, then enable the checkbox for the selected call class
- *Call reject*: reject all calls
- *Call Forward Busy / No Answer / All*: you can enable call forwarding in case user is busy / does not answer or unconditional call forwarding; enter the destination number or the VOICEMAIL into the field
- *Call waiting*: enable the option to be able to receive more than one call at a time
- *Call timeout*: if enabled, the call is terminated in case there is no answer within the specified timeout; enter timeout in seconds into the field
- *Mobility extension management*: if enabled, the call is forwarded also to the user mobile phone number (mobile phone number must be specified for this user in WMS -> Users -> Edit) after the specified timeout; enter timeout in seconds into the field
- *Mobility confirmation*: if enabled, the user is notified on who the caller is once he receives the call to mobility extension number, and is invited to enter the digit to accept the call
- *Notify missed calls via email / via sms*: enable missed calls notification to email / via SMS
- *Custom Ring*: enable the option and select the ringtone; ringtones selected here are applied to WP4X0, WelcomeConsole and Collaboration; Custom ringtones can be uploaded via Sounds menu (more information in chapter [Record and playback audio messages](#))

Settings: user personal settings

- *Shared voicemail*: enable this option to subscribe to the Voicemail of another user; enter the extension number to subscribe to; user receives notification to Collaboration / WP about new Voicemails arrived to the mailbox he/she is subscribed for and can listen to it
- *Hotline*: if enabled, the number entered into the field is automatically dialed once the user lifts the handset (supported on WP4X0 2015, FXS gateways 2014-2015); indicate the timeout in seconds in the field
- *Call waiting tone*: if enabled, phone user receives audio notification in case of second incoming call
- *Ring only active device*: read more in Collaboration User Guide -> *Settings* -> *Personal*: [Collaboration 5.0X](#).
- *Notify unread messages via email*: if enabled, user gets notifications about unread messages via email (disabled by default)
- *Two-factor authentication*: read more in Collaboration User Guide -> *Settings* -> *Personal*: [Collaboration 5.0X](#).
- *Phonebooks*: select the Phonebooks which can be accessed by user from Collaboration and WP; move the phonebooks from Available to Selected section
- *Date format / Time format*: date and time format to be displayed in Collaboration (*Messaging*, *History* pages, CDR-View etc) and on Wildix devices except W-AIR Headsets (must be set up on device)

⚠ Note: Wildix devices support 2 date formats: "www dd mmm" and "www dd mmm". Depending on the selected format in Collaboration (European: "dd/mm/yyyy", "dd mmm yyyy", "dd-mm-yyyy", "dd.mm.yyyy" or US: "mmm dd yyyy"/ "mm/dd/yyyy"/ "mm-dd-yyyy"), the date can be displayed as, for example, "Tue 6 Nov" or "Tue Nov 6".

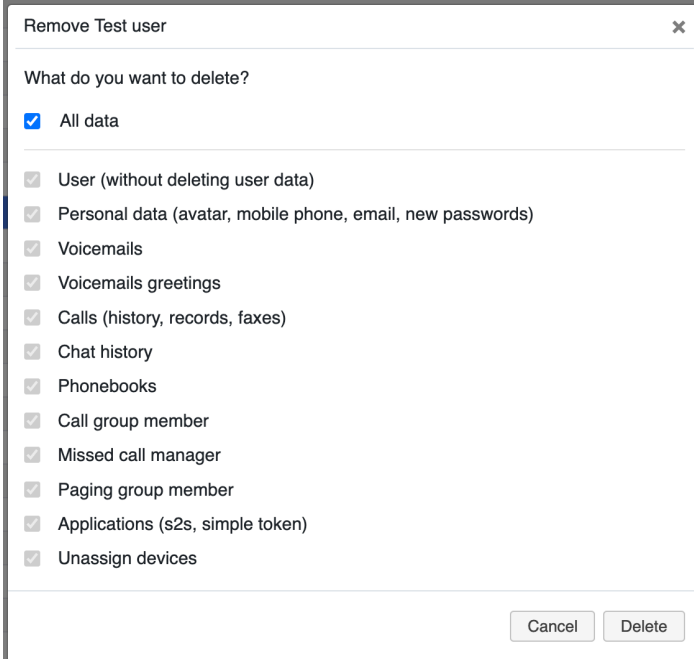
- *Popup URL:* allows specifying the URL to open upon receiving / placing a call; read more in Collaboration User Guide -> *Settings* -> *Personal*: [Collaboration 5.0X](#).
- *Function keys:* set up the BLF keys for WP; read more in Collaboration User Guide -> *Settings* -> *Function keys*: [Collaboration 5.0X](#).
- *Predefined statuses:* temporary user statuses (Do not disturb / Away) defined here can be later on set by user from Collaboration, read more in Collaboration User Guide -> *Settings* -> *Chat / Presence*: [Collaboration 5.0X](#).
- *Limit call groups:* if enabled, call groups to which users can dynamically log into are limited (Contact center feature in Collaboration/ on desk phones and via Feature code), read more in [Dynamically added call group members](#)
- *Contact Center:* if enabled, users are dynamically logged into Call groups; read more in Collaboration User Guide -> *Settings* -> *Personal*: [Collaboration 5.0X](#).
- *Company / Fax machine id / Fax header / Company logo:* Fax cover settings; read more in Collaboration User Guide -> *Settings* -> *Fax Server*: [Collaboration 5.0X](#).
- *Call groups / Pickup groups:* define call and pickup groups to allow users to pick up call group calls: [Call and Pickup Groups](#)
- *Identities:* specify identities of numbers for outgoing calls: [Identities Feature](#)

Roster: select the users which appear in Wildix Collaboration -> *Colleagues*; move users from *Available* to *Selected* section.

Delete user data

Starting from WMS 6.01.20221019.4, there is possibility to choose which user data (personal data, voicemails, etc.) has to be deleted.

1. In *WMS* -> *Users*, choose a user or group of users and click - **Delete**
2. Select the data to be deleted:
 - a. You can either choose *All data*:



Remove Test user

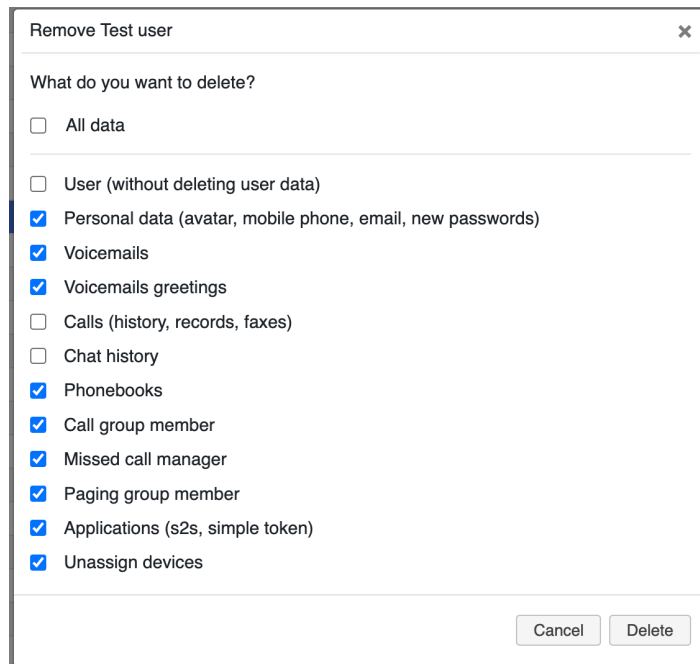
What do you want to delete?

- All data
- User (without deleting user data)
- Personal data (avatar, mobile phone, email, new passwords)
- Voicemails
- Voicemails greetings
- Calls (history, records, faxes)
- Chat history
- Phonebooks
- Call group member
- Missed call manager
- Paging group member
- Applications (s2s, simple token)
- Unassign devices

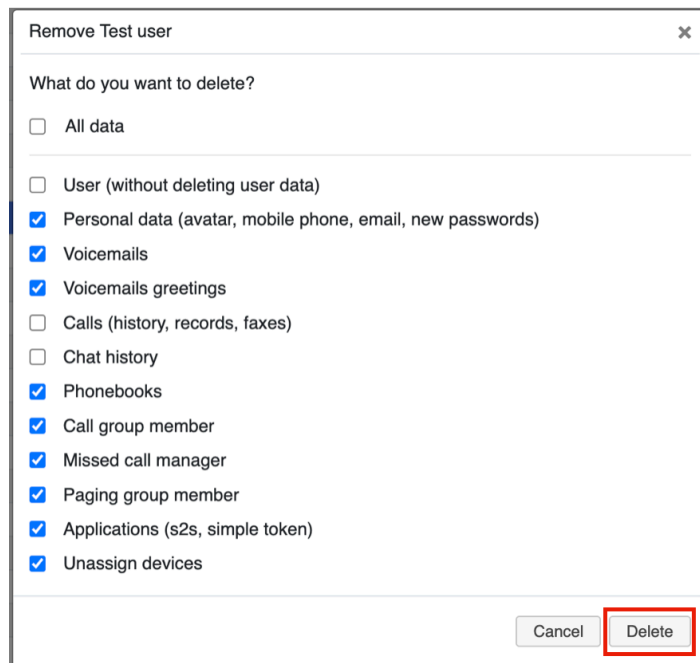
Cancel Delete

b. Or untick All data and choose which data needs to be removed. The list of options you can choose from:

- User (without deleting user data)
- Personal data (avatar, mobile phone, email, new passwords)
- Voicemails
- Voicemail greetings
- Calls (history, records, faxes)
- Chat history
- Phonebooks
- Call group member
- Missed call manager
- Paging group member
- Applications (s2s, simple token)
- Unassign devices



3. Once necessary data is selected, click **Delete**:



Import of users and phonebooks

Wildix system supports import of users and contacts from different resources, to name some of them:

- LDAP
- Active Directory
- MSSQL
- MySQL

- Google
- Infusionsoft
- Exchange Server
- Zoho CRM

Import of users can be done only by the admin user: go to *WMS* -> *Users*, and click **Import**.

To import phonebooks, go to *WMS* -> *Users* -> *Phonebooks*, and click **+** to add a new backend and to import the phonebooks and to set up a scheduled job.

For more information about configuration of each backend read the guide [Import of Contacts and Users](#).

Provisioning of devices

Provisioning modes supported by Wildix PBX

Wildix PBX supports different provisioning modes:

- WMP provisioning: available for Wildix devices purchased via WMP
- Auto-configuration via *auto.wildixin.com*: available for Wildix devices connected to the same network as the PBX (supported by Wildix devices starting from a certain FW version)
- Auto-provisioning: available for Wildix devices connected to the local LAN or remote network via VPN
- Remote provisioning: available for remote/unreachable devices behind NAT/firewall



Note: It is possible to assign unprovisioned devices to users. Available only for devices added via Remote Provisioning (Semi-automatic mode) or WMP. Refer to [this chapter](#) for detailed information about assigning to users.

More information on Wildix provisioning: [Provisioning of Wildix devices Admin Guide](#).

In this chapter we will learn how to provision:

- Wildix gateways (PRI, BRI, DaySaver, FXO, FXS)
- WP4X0, WelcomeConsole, WorkForce
- W-AIR base stations

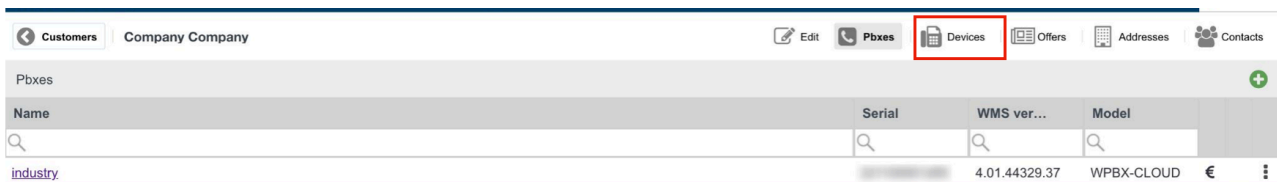
For provisioning of Vision/ SuperVision, see chapter [Provisioning and login of Vision / SuperVision](#).

WMP provisioning (Hardware, Virtual, Cloud PBX)

Thanks to this provisioning mode, Wildix Partners can assign Wildix devices to the PBX directly via the WMP.

After you have ordered the devices and they have been shipped to you, proceed as follows:

- Go to *WMP* -> *PBX per user* -> select the customer -> select the PBX -> click **Devices** icon:



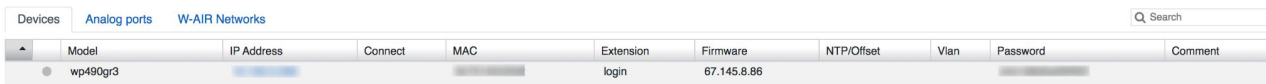
- Click **+**:



- The list of all your available devices is displayed; select only those devices that you want to assign to this PBX and click **Add**:



- Power on / connect devices (WP phones, media gateways, W-AIR bases) to the network
- Go to *WMS* -> *Devices*: the added devices are displayed in the table:



How to understand that devices have been provisioned:

- They have received the IP address (column *IP Address*)
- Device's model is correctly indicated (column *Model*)
- WP display loginX on the screen, which means they are ready to be assigned to users (column *Phone*)

Watch the video tutorial:<https://youtu.be/kAvKgv1Rz3Y>

Auto-configuration via auto.wildixin.com (Hardware, Virtual PBX)

This mode is available for Wildix devices located in the same network as the PBX.

Features:

- Automatically add and provision Wildix devices during new installations
- Automatically add and provision Wildix devices that had been reset

Network configuration requirements:

- If internal DHCP server is used, it must return PBX address as Primary DNS Server address
- If external DNS server is used, you must add the correct DNS record (auto.wildixin.com must be resolved to the PBX IP)
- If external DHCP server is used, you must use PBX address as Primary DNS server
- For auto-configuration of W-AIR base stations (not SB), you must first manually create a W-AIR network via WMS interface

Make sure the option in WMS Settings -> PBX -> SIP-RTP, *Auto add new devices in local networks* is enabled: when it's enabled, devices are added and provisioned automatically in local networks.

For auto-configuration of DaySaver, read the guide [Provisioning of Wildix devices](#).

If all the requirements specified above are respected, proceed as follows:

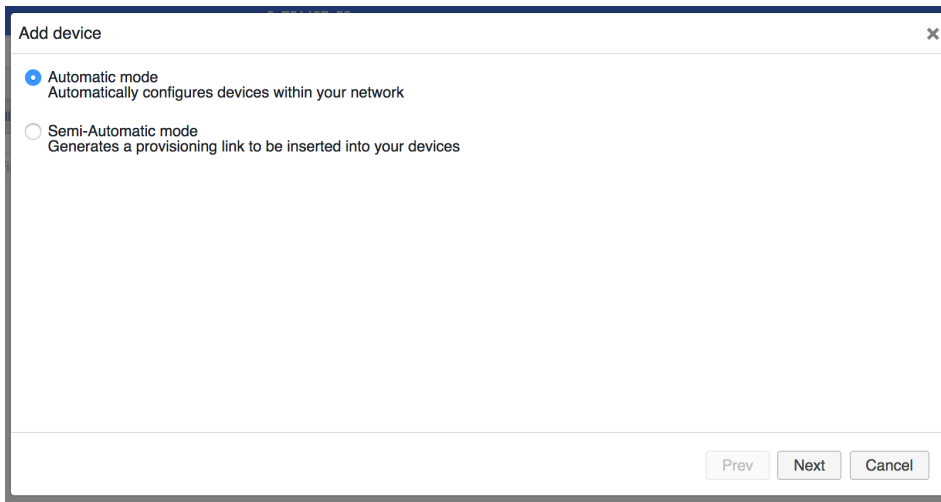
- Power on / connect WP4X0 and media gateways to the network
- Go to *WMS* -> *Devices*; provisioned devices are displayed in the table.

Auto-provisioning - Automatic mode (Hardware, Virtual PBX)

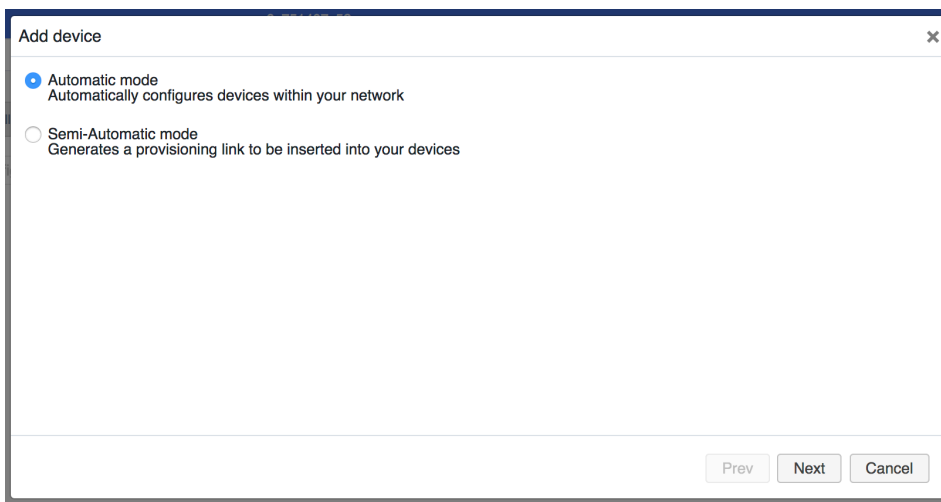
Auto-provisioning mode is available for Wildix devices connected to the local LAN or remote network (VPN).

Proceed as follows:

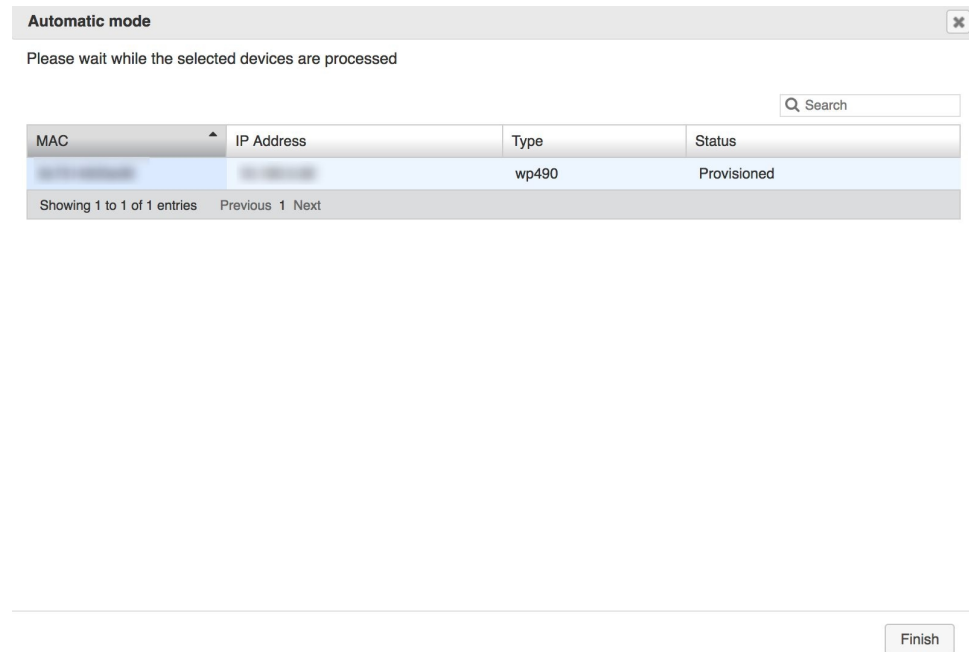
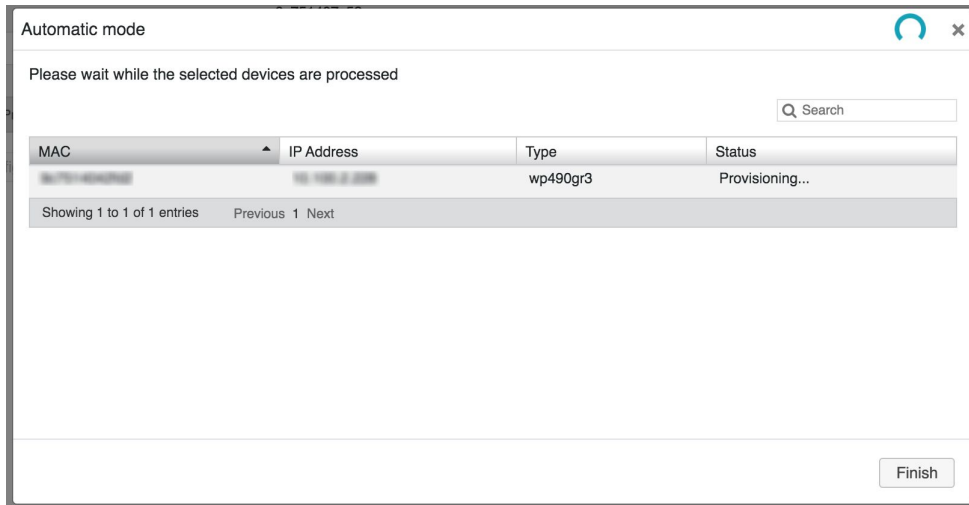
- Power on / connect WP4X0 / media gateways / W-AIR base stations to the network
- Make sure that all the devices have received the IP address from the DHCP server of the network (PBX or external DHCP)
- Go to *WMS Devices* -> *Devices*
- Click **+Add**
- Select *Automatic mode* and click **Next**



- Click **Scan**; you can specify the IP range in the *Search field* located just above the table:



- Select your device(s) on the list and click **Next**
- Wait till device(s) *Status* changes from *Provisioning* to *Provisioned*



- Provisioned devices are displayed in the table

Remote provisioning - Semi-Automatic mode (Hardware, Virtual, Cloud PBX)

Remote provisioning mode is recommended for provisioning of remote / unreachable devices behind NAT/ Firewall.

Proceed as follows:

- Power on / connect WP4X0 Wildix phones media gateways to the network.
- Make sure that all the devices have received the IP address from the DHCP server of the network (PBX or external DHCP).
- Go to *WMS Devices -> Devices*
- Click **+Add** to add a new device
- Select *Semi-Automatic mode* and click **Next:**

Add device

Automatic mode
Automatically configures devices within your network

Semi-Automatic mode
Generates a provisioning link to be inserted into your devices

Prev Next Cancel

- Enter the device's Mac Address (Mac address can be normally found on the backside of each device):

Semi-Automatic mode

Semi-Automatic mode allows you to provision the devices behind the firewall.
Insert Mac addresses of your devices and click "Add device(s)". WMS will generate a provisioning link for each device.

Device MAC: +

-

Prev Next Cancel

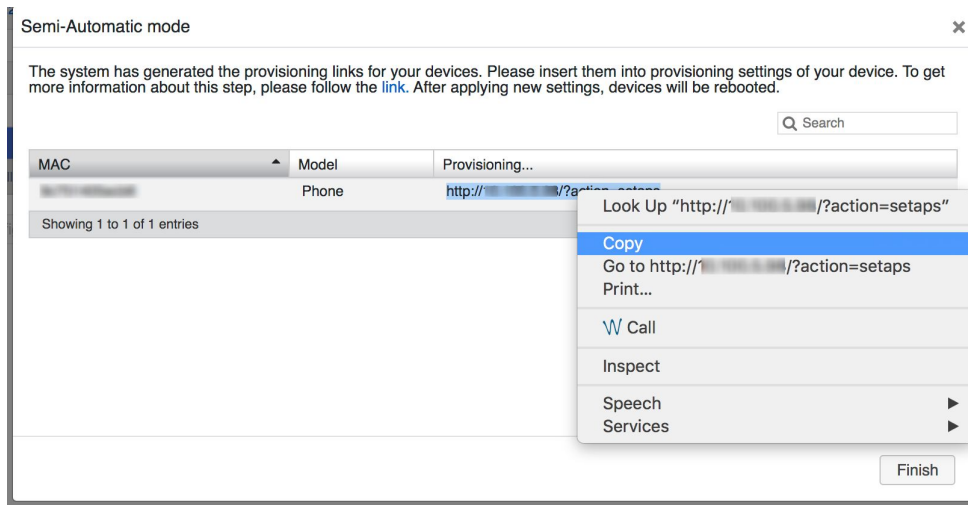
- The provisioning link has been generated:

Copy the link address of the Provisioning URL

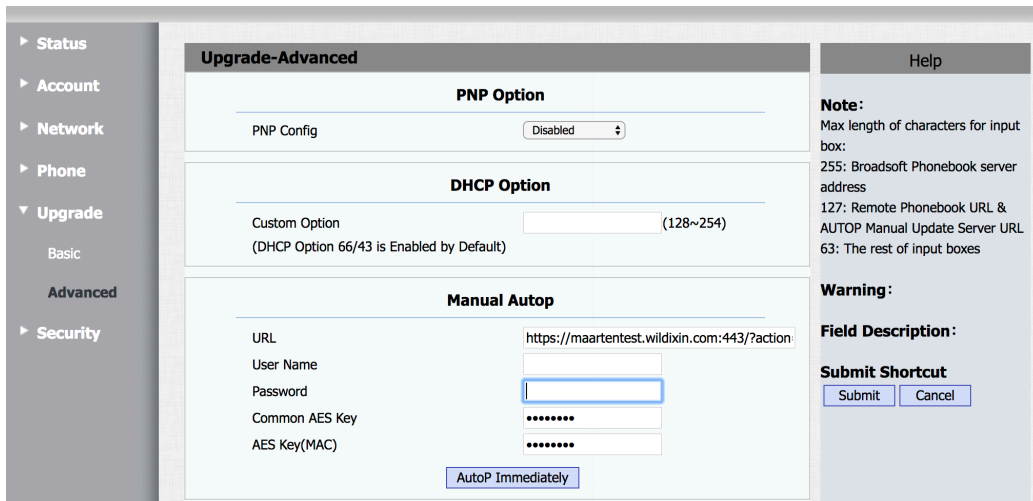
Provisioning link format:

http://[PBX_IP]/?action=setaps&config=xml (W01GSM)

http://[PBX_IP]/?action=setaps (other devices)



- Access the web interface of the device and insert the provisioning link
- In this specific example we are provisioning a WP4X0G phone: enter credentials for the first time access: *admin : admin*
- Go to the menu *Upgrade -> Advanced*:



- Click **AutoP Immediately**
- Device is now rebooting (the phone screen indicates that the device is rebooting)
- After the reboot, date and time, BLF keys and *login0X* are displayed on the screen
- Go to *WMS -> Devices*: provisioned device is now displayed in the table:

Model	IP Address	Connect	MAC	Extension	Firmware	NTP/Offset	Vlan	Password	Comment
wp490gr3				login	67.145.8.86				
wp480gr3				login1	63.145.10.7				

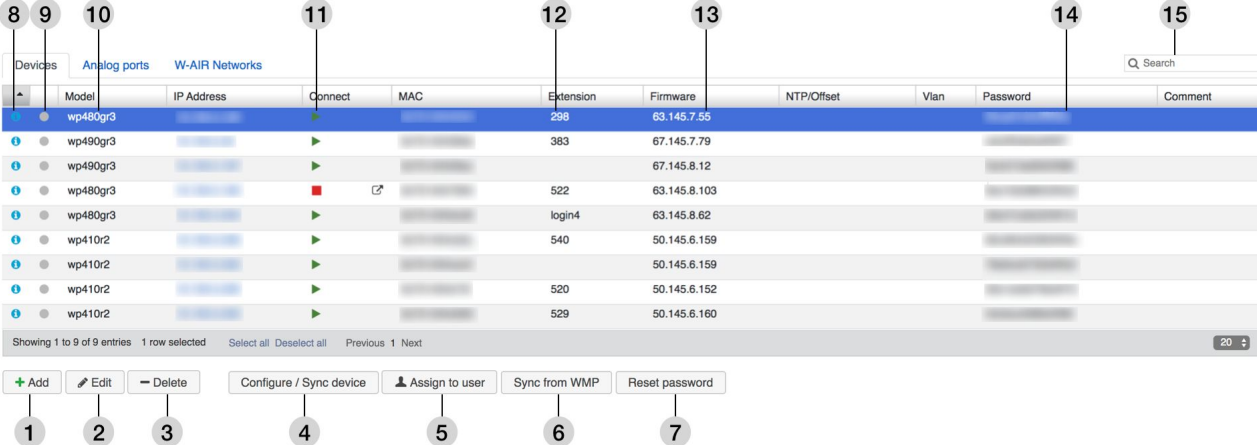
- Credentials to access the device's web interface after it has been provisioned:
 - *login : admin*
 - *password : the value in the column Password*

Consult documentation for remote provisioning of each Wildix device: [Remote Provisioning of Wildix devices](#).

Devices management

Go to *WMS* -> *Devices*.

All the devices connected to the PBX (provisioned or not) are displayed in the table:



Model	IP Address	Connect	MAC	Extension	Firmware	NTP/Offset	Vlan	Password	Comment
wp480gr3				298	63.145.7.55				
wp490gr3				383	67.145.7.79				
wp490gr3					67.145.8.12				
wp480gr3				522	63.145.8.103				
wp480gr3				login4	63.145.8.62				
wp410r2				540	50.145.6.159				
wp410r2					50.145.6.159				
wp410r2				520	50.145.6.152				
wp410r2				529	50.145.6.160				

Showing 1 to 9 of 9 entries 1 row selected Select all Deselect all Previous 1 Next

1 + Add 2 Edit 3 - Delete 4 Configure / Sync device 5 Assign to user 6 Sync from WMP 7 Reset password

- 1 - **+ Add**: add a new device via Auto-provisioning or Semi-provisioning mode
- 2 - **Edit**: edit device settings for one or multiple devices:
 - *Comment*: unique identifier, displayed in the Comment column of Devices table
 - *Default zone / Tone zone (FXS/FXO)*: select the country / the geographical area for the correct tone recognition
 - *DNS Server / Secondary DNS / NTP Server / NTP Zone*: allows setting DNS and NTP settings, which can be useful in some network scenarios, e.g. with remote devices
 - *Use DST*: enables automatic switching to DST
 - *Voice VLAN ID / CoS voice priority / Data VLAN ID / CoS data priority*: allows setting priority for Voice and Data traffic and assign VLAN IDs
 - *Use received IP*: enables static IP
 - *Syslog Server*: you can specify the server IP address to which you would like to send syslog
 - *SNMP Access (BRI, PRI, W-PA, some of WP4X0)*: authorizes SNMP monitoring on devices (it is also possible to authorize SNMP monitoring of the PBX in *WMS Settings* -> *System* -> *SNMP Server*)
 - *Disable SIP Firewall (BRI, PRI, FXO, W-PA, GSM)*: it is necessary to enable this parameter in some complicated network scenarios, where a SIP Firewall is present between the PBX and the connected devices
- 3 - **Delete**: delete one or multiple devices
- 4 - **Configure / Sync device**: send new configuration to one or multiple devices
- 5 - **Assign to user**: assign WP4X0 and W01FXS to users; more information in chapter [Assign WP4X0 to users](#)
- 6 - **Sync from WMP**: sync devices, assigned to this PBX from WMP; more information about WMP provisioning in chapter [WMP Provisioning \(Hardware, Virtual, Cloud PBX\)](#)
- 7 - **Reset password**: in case there is a risk that the provisioning password (displayed in the column *Password*) of one or several devices has been compromised, it's possible to reset it without resetting the device: select one or multiple devices, click Reset password to reset the password, then click **Configure / Sync device** to assign a new password to the device
- 8 - *i*: the blue icon indicates that there is a new firmware version available; more information about firmware upgrade in chapter [Update firmware](#)

- 9 - *Status icon*: displays the device status, hover over it to see additional information (SRC port, transport used):
 - Green: device is registered (connected via SIP)
 - Grey: device is not registered
- 10 - *Model*: for provisioned devices, the model is indicated correctly (e.g. wp480gr3), for not provisioned devices, only the device type is indicated (e.g. phone) in this column
- 11 - **Connect**: enable / disable direct access to device (available for non-Cloud PBXs for devices which are in the same network as the PBX); more information is available in the guide [Provisioning of Wildix devices](#)
- 12 - *Extension*: available for WP4X0 and W01FXS, displays the extension, this device is assigned to; displays loginX in case device is not assigned
- 13 - *Firmware*: the current firmware version
- 14 - *Password*: password to access device's web interface after provisioning; password is displayed only for provisioned devices
- 15 - *Search field*

Update firmware

Go to *WMS* -> *Devices*. In case a new FW version is available, there is a blue *i* icon displayed near this device:



To update the device's firmware to the latest version, proceed as follows:

- Select one or multiple devices
- Click **Configure / Sync device**
- Device is being rebooted
- After the reboot, the device is displayed has been updated to the latest version:



Note: a new FW notification is not indicated for BRI/ PRI media gateways. To update their firmware, upgrade your PBX to the latest version. Within half an hour after the procedure is over, media gateways are automatically updated.

Assign WP4X0 to users

After you have provisioned WP phones, proceed with assigning phones to users.

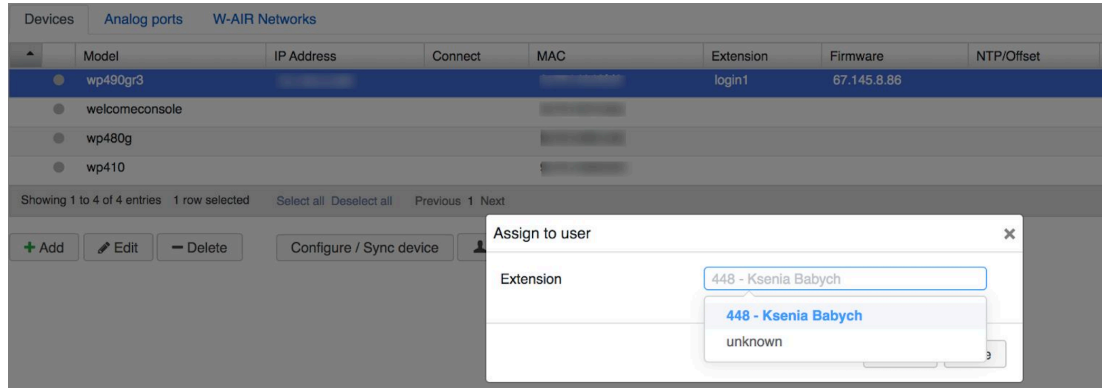
There are several modes of assigning WP phones to users:

- via WMS by system administrators
- via Feature Code, directly from the phone by users or by system administrators

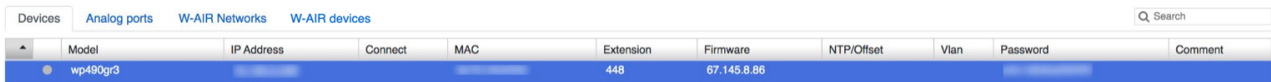
Assign from WMS

To assign WP phone from WMS, proceed as follows:

- Go to *WMS* -> *Devices*
- Select a provisioned WP phone
- Click **Assign to user**
- Select the user from the list (the option Unknown allows you to log out a phone that had been previously assigned):



- After a few seconds, *loginX*, previously displayed under *Extension* column has changed to the extension number of user:



- Extension is displayed on the phone's screen as well; the phone is now assigned and can be used to make and receive calls

Assign via Feature Code

To assign WP phone via Feature Code, proceed as follows:

- Take a provisioned WP phone: *loginX* is displayed on the screen
- Dial 99 from the phone
- Enter the extension number of user, when requested
- Enter the password of user (PIN - it is sufficient to enter first five symbols of user WEB password), when requested;

Logout is performed in the same way, via Feature Code.

Logout via FC 99 on WP phone performs auto logout of all the WP phone phones assigned to you. To change the behavior, use Custom Dialplan variable "MULTILOGIN_SUPPORT=yes", consult [Custom Global Dialplan Variables List](#) for details.

Enter the user password from the phone's dialpad

To enter the user password from the phone's dialpad, take into account the following:

- To enter any lowercase and uppercase letter, press ONCE a corresponding digit

- To enter special characters (% , ^ , & , etc), press the *star* key (*)
- Example: if user password is 4Ag7\$Zl@, then you have to dial 4247*



- Dial *I* to use this phone, when requested
- After a few seconds, extension is displayed on the phone's screen; the phone is now assigned can be used to make and receive calls

Now when you have assigned the phone, you can do a sound test: dial 76 from the phone.

Go to *WMS* -> *Users*: the status of the user to whom the phone has been assigned, has changed to green, the newly assigned device is displayed next to the status:



To change the phone's language, proceed as follows:

- Go to *WMS* -> *Users*
- Double click on the phone user
- Edit the *Language* field
- Click **OK**

For more information on WP phones, consult the User Guide: [Wildix VoIP Phones - User Guide](#).

To connect accessories, such as WHS headsets, WPEHS or WelcomeConsole-EXT, check documentation: [Phones Accessories Quick Start Guide](#).

Assign analog ports of FXS to users

To correctly install FXS media gateways and connect analog devices, read Quick Installation Guides:

- W02FXS 2018: [W02FXS 2018 Quick Installation Guide](#)
- W04FXS 2020: [W04FXS 2020 Quick Installation Guide](#)
- W24FXS 2015: [W24FXS 2015 Quick Installation Guide](#)

After you have provisioned FXS media gateways, proceed with assigning analog ports to users.

To assign analog ports of FXS gateways with 2 and more ports, proceed as follows:

- Go to *WMS* -> *Devices* -> *Analog ports*
- The provisioned FXS is displayed in the table:

Comment	Model	MAC	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	w04fxs																									

Showing 1 to 1 of 1 entries Previous 1 Next

- Double-click on the gateway
- Assign analog ports to users and click **Save**:

Edit Device ✕

Comment

Port 1:

Port 2:

Port 3:

Port 4:

- Assigned ports are displayed in the table:

Comment	Model	MAC	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	w04fxs		448																							

Showing 1 to 1 of 1 entries Previous 1 Next

! Known limitation: It is not recommended to set TCP/ TLS protocols when using W24FXS as the device can not receive more than 3 calls simultaneously. To overcome the limitation, you can set UDP as a transport protocol via the custom provisioning parameter:

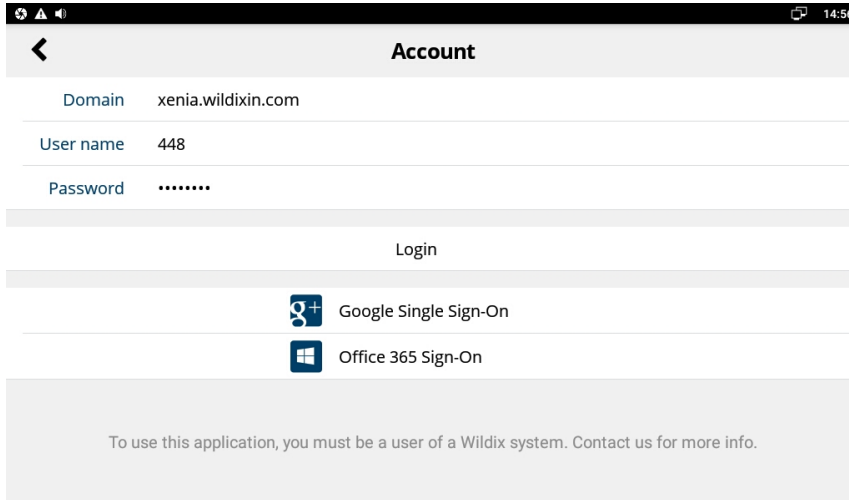
- Add "SIPtransportRemote=UDP" to [wildixfxs2] section. Consult the Guide [Provisioning Custom Settings](#) for detailed information

Provisioning and login of Vision/ SuperVision

Since Vision/ SuperVision is an Android phone, it doesn't need to be provisioned via WMS. To provision Vision/ SuperVision and assign it to user, proceed as follows:

- Connect the phone to the network
- After the phone has booted, *Login page* of the *Wildix Phone* application is displayed
- Enter your credentials:
 - *Domain*: PBX IP address or domain name
 - *User name*: extension number (user name or email address are also accepted)

- *Password*: user's WEB password



- Click the **Login** icon (arrow), situated in the upper right part of the screen
- Go to *Phone application Settings* -> *Advanced* and click **Check for Updates**
- In case there is a new version available, follow the instructions on the screen to perform the update

Video tutorial: <https://wildix.wistia.com/medias/z6n4lheshqn>

User guide: [Vision User Guide](#) / [SuperVision User Guide](#).

W-AIR DECT solution

Introduction

W-AIR is the DECT system developed on the CAT-iq protocol, which supports transferring of data and voice over the radio channel.

Wildix W-AIR architecture consists of the following components:

- Base station: the basic component of the DECT infrastructure
- W-AIR Sync Plus / W-AIR Sync Plus Base Outdoor: multicell, up to 4000 bases, up to 16000 users, up to 8 concurrent calls per base, up to 8 handovers
- W-AIR Small Business (SB): single cell, up to 20 users, up to 10 concurrent calls
- Repeaters: this optional component allows extending the signal coverage of the base station
- Wireless handsets / headset: choose one of the models of handsets W-AIR Basic2 / W-AIR LifeSaver/ W-AIR Med/ W-AIR Office and W-AIR Headset. Detailed documentation: [W-AIR DECT Handset - User Guide](#), [W-AIR Headset User Manual](#)

For more information, refer to W-AIR Datasheet: [W-AIR System Datasheet](#).

Create a W-AIR network

For W-AIR Base Small Business: after you have provisioned the base station, proceed to chapter [Register and assign W-AIR handsets to users](#).

For W-AIR Sync Plus / W-AIR Sync Plus Base Outdoor: after you have provisioned W-AIR base station, proceed as follows:

- Go to *WMS* -> *Devices* -> *W-AIR Networks*
- Click **+Add**
- Enter the name of the network into the field *Name*; do not edit the field *Code* to avoid problems with adding repeaters to the system
- Select the MAC address of the base station from the left section and move the selected item to the right section using the arrow button
- For W-AIR Sync Plus: check off "Sync Plus via Ethernet" option to enable sync over cable

Note: The option can be enabled only for W-AIR Sync Plus Base stations. If you add W-AIR Base Outdoor to the Network, the option is disabled automatically.

- Click **Save**
- W-AIR Network is created:


Devices Analog ports **W-AIR Networks**


Id ^	Title	Gateways
2	WAIR-Trento-SP	0008 (M), 9c7 (S)


Showing 1 to 1 of 1 entries 1 row selected Previous 1 Next

+ Add **Edit** **- Delete**

- Go back to *WMS* -> *Devices*
- Select the same base station and click **Configure / Sync device**

 For CLOUD PBXs, you need to power the base station down and then power it up again (reboot the base station) to apply the new parameters!


 Note: Base station is displayed with grey status in the table of devices, unless you register at least one handset / headset.

 This procedure is valid for the installation of only one W-AIR Base; for multicell installations, it is necessary to carefully plan the installation and do the site survey; for more information refer to the documentation: [W-AIR Network Admin Guide - Sync over the air](#), [W-AIR Network Admin Guide - Sync over LAN](#).

Register and assign W-AIR handsets to users

Proceed as follows:

- Turn on the phone
- Select *Connectivity* -> *Register* in the phone menu
- Enter the code *0000* and select *Ok*

 Note: in case you have several W-AIR bases, hold the handset closer to the base station you are registering it to.

- Wait till *unknownX* is displayed on the screen
- Registered handset(s) are now displayed in *WMS* -> *Devices* -> *W-AIR Networks*, in the column *GW Users*:


ID	Name	Gateways	GW Users
13	W-AIR Network	9c75143400a8(M),9c751433014b(S),9c751433014c(S)	unknown1_1

Showing 1 to 1 of 1 entries (filtered from 8 total entries) 1 row selected Previous 1 Next Show 25 entries

+ Add Edit

- Handset is now ready for login procedure.


To assign W-AIR handset to user, follow procedure of phone login via Feature Code, described in chapter [Assign WP4X0 to users](#).

 Note: Starting from WMS 5.04.20220309.1, it is possible to assign registered W-AIR handsets/ headsets to users via *WMS* -> *Devices* -> *W-AIR Devices*.
See the section: [Assigning W-AIR handsets/ headsets via WMS](#)


Register and assign W-AIR Headsets to users

Register a W-AIR Headset to the base station:

- Put the Headset in the registration mode by pressing Call, Volume+ and Volume- buttons at the same time for more than 5 seconds. The Headset is in subscription mode when the LED indicator blinks with short blue flashes and voice prompt announces “*Registering*”
- The Headset now connects to the Base Station. When the Headset is subscribed, you will hear voice prompt announcing “*Headset subscribed*”

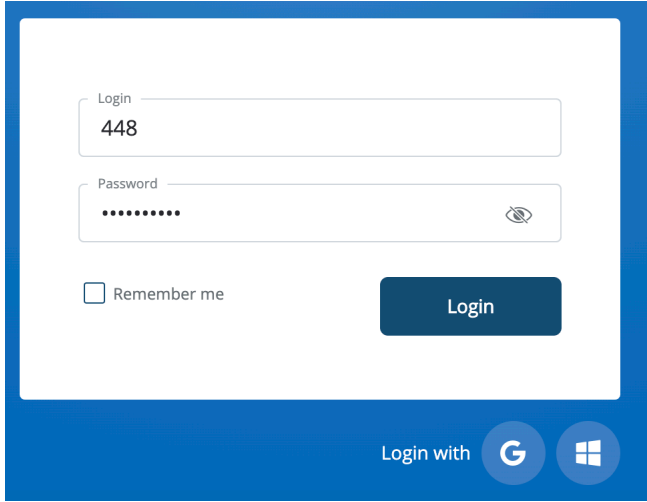
 Note: if the registration fails, the voice prompt will announce “*Headset not subscribed*”. Before trying to register the Headset again, please check if it is within range of W-AIR Base station and voice prompt announces “*Registering*”.

After you registered your Headset to the Base station, you need to assign a user. This must be done by user via Collaboration web interface.

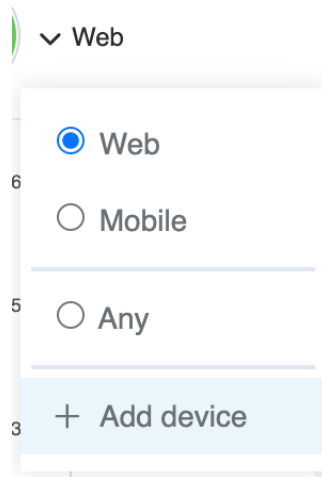
 Note: Starting from WMS 5.04.20220309.1, it is possible to assign registered W-AIR handsets/ headsets to users via WMS -> Devices -> W-AIR Devices.
See the section: [Assigning W-AIR handsets/ headsets via WMS](#).

Assign a W-AIR Headset to user:

- Open the web browser (recommended: Chrome), and access Collaboration by the same URL you used to access WMS, but add */collaboration* in the end of the string, example: *https://mycompany.wildix.com/collaboration* or *https://192.169.1.100/collaboration*
- Enter the user's extension and WEB password into the fields, then click Login icon (arrow), situated in the lower right corner



- Click on **Device selection** in Collaboration top menu to open the drop-down list of devices assigned to this user
- Click **+ Add device**:



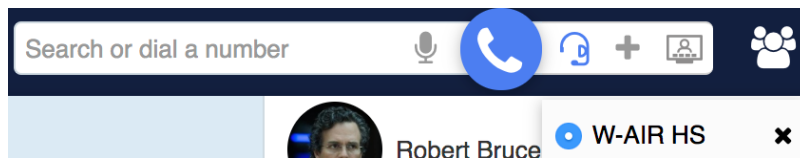
- Press **Call** button on your W-AIR Headset to get the pairing code

Note: a pairing code consists of 4 digits.

- Enter the code into the field *Pairing code*

Note: the code is repeated 3 times. If authentication fails, press **Call** button one more time to get the new code.

- In case the assignment is completed, the voice prompt will announce "Activated, thank you!"
- After the Headset has been assigned to the user, it appears in the list of available devices within a few seconds:



More information on W-AIR headset: [W-AIR Headset User Manual](#).


Assigning W-AIR handsets/ headsets via WMS

Notes:

- The support starts from WMS 5.04.20220309.1.
- W-AIR handset/headset should have DECT registration on the W-AIR base station before it can be assigned to user.

To assign W-AIR headset/ handset:

1. Go to *WMS* -> *Devices* -> *W-AIR devices*
2. Choose the headset/ handset and click **Assign to user**
3. Enter user extension and click **Save**

 Note: To figure out which headset received the assigned extension, you can dial this extension and see which headset rings.

To assign device to a different user:

1. Choose the headset/ handset on the *W-AIR devices* tab -> click **Assign to user**
2. Enter a different extension and click **Save**

To deassign a device:

1. Choose the headset/ handset -> click **Assign to user**
2. Select “unknown” in the *Extension* field and click **Save**

Introduction to Wildix Unified Communication

Wildix Collaboration


Wildix Collaboration is the user interface of Wildix PBX that offers access to Unified Communications features on PC (Mac OS X, Windows, Linux) via the browser (any HTML5 standard browser, however Chrome is recommended, since it fully supports WebRTC).

Basic features:


- Presence status monitoring of colleagues and geolocation
- Personal presence status and geolocation
- Audio / video call
- Chat / File transfer
- Sending of Faxes and SMS, memo messages
- Screen sharing / remote control
- Clientless, accessible via the browser
- PBX shared phonebooks
- Events history
- Create conferences
- Integrated Softphone (Web Phone)
- Attendant Console for call management in high load environment

For the first time access to Wildix Collaboration, proceed as follows:

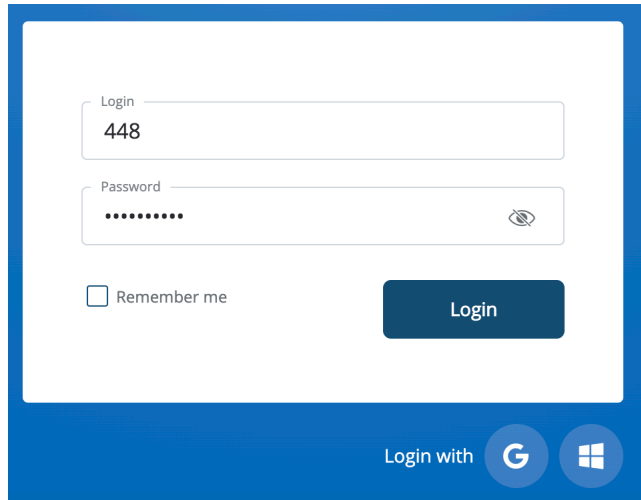
- Open the browser (recommended: Chrome) and enter the IP address or the domain name of the Wildix PBX into the URL

 You can access Collaboration from WMS by adding */collaboration* to the URL, example of the URL to access Collaboration: <https://mycompany.wildixin.com/collaboration>

- Enter the user extension and WEB password into the fields

 Login via user name is no longer supported!

- Click **Login** icon (arrow), situated in the lower right corner:



- Once you access the Collaboration interface, follow the popup notifications inviting you to add colleagues to your roster, enable desktop notifications, geolocation, etc.

Collaboration first time access video: <https://wildix.wistia.com/medias/cnl8s726wi>

Collaboration User Manual: [Collaboration 5.0X](#).

Apps for Android / iOS

Wildix offers free of charge mobile application for iOS / Android.

Basic features:

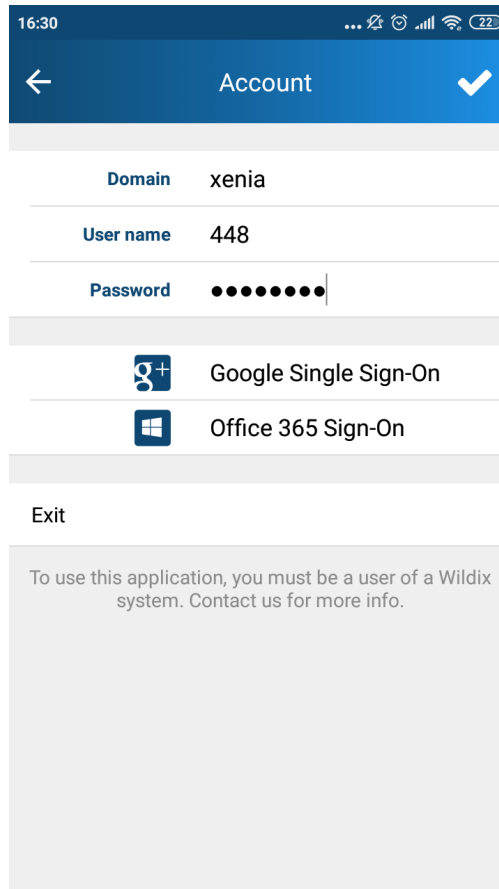
- Calls via VoIP or GSM to all phonebook contacts
- Push notifications
- Video calls to users
- Mobility callback service
- Chat and presence
- Virtual reminders to users
- Call history
- PBX shared phonebooks
- Secure access to the app outside of the company network

Check the ports to open on router / firewall: [Ports used by Wildix services](#).

For the first time access to Wildix Collaboration Mobile application, proceed as follows:

- Search *wildix* in Google play market / *Collaboration* in App store and download the application
- Launch the application
- Enter your credentials or use your Google/ Office 365 credentials for single sign-on:

- *Domain*: PBX IP or domain name of the Wildix PBX
- *User name*: Extension or User name or Email address
- *Password*: WEB password of user



- Tap the **Check** icon situated in the upper right part of the screen

Android User Guide: [Android Collaboration Mobile App Guide](#).

iOS User Guide: [iOS Collaboration Mobile App Guide](#).

Call activity analysis & reporting with CDR-View

CDR-View allows detailed analysis of call activity of users and groups, costs, usage of trunks, duration and type of all the calls made and received, missed calls.

First time access to CDR-View:

- Open *Collaboration* -> *History* tab
- Click **CDR-View**
- The first time you launch CDR-View, you are prompted to install the *Integration Service*
- Once installed, you can access CDR-View

For more information on CDR-View, refer to <https://www.wildix.com/monitoring/>.

CDR-View User Guide: [CDR-View User Guide](#).

Pricelists

To be able to view and analyze call costs in CDR-View, you must upload the pricelists and associate them to trunks.

Pricelists are the tables that you can import on the PBX in *.csv format to enable the system to calculate call costs.

To add pricelists, go to *WMS -> Trunks -> Pricelists*.

Example of a *.csv file:

dialprefix	destination	rate	min_duration	billing_block	connect_charge	start_day	stop_day	start_time	stop_time
01	Italy Locale	0.02	0	60	0.0	1	7	0	90000
02	Italy Locale	0.02	0	60	0.0	1	7	0	90000
03	Italy Locale	0.02	0	60	0.0	1	7	0	90000
04	Italy Locale	0.02	0	60	0.0	1	7	0	90000
05	Italy Locale	0.02	0	60	0.0	1	7	0	90000

Close

Where

- *dialprefix*: verification prefix (the longest prefix matching criteria applies)
- *destination*: country of the call destination
- *rate*: price per call unit
- *min_duration*: minimum duration of the call without billing in seconds
- *billing_block*: call unit
- *connect_change*: connection fee
- *start_day*: start day of the week (1 = Monday, 7 = Sunday)
- *stop_day*: end day of the week
- *start_time*: start time in seconds from midnight (example: 25200 = 7am; from 0 to 86400)
- *stop_time*: end time in seconds from midnight

Example:

Let's consider 5 different types of calls and the following conditions:

- tariffing from Monday to Sunday
- tariffing from 00:00:00 to 23:59:59
- no connection fee
- duration of connection equaling 60 seconds

CSV file configuration example for 5 different types of calls and the conditions specified above:

- dialprefix,destination,
rate,min_duration,billing_block,connect_charge,start_day,stop_day,start_time,stop_time
- 0461,"Italia TN",0.01,0,60,0.0,1,7,0,86400
- 01,"Italia TO",0.03,0,60,0.0,1,7,0,86400
- 02,"Italia MI",0.03,0,60,0.0,1,7,0,86400
- 3,"Italia mobile",0.298,0,60,0.0,1,7,0,86400
- 0033,"Francia",0.031,0,60,0.0,1,7,0,86400

Download a CSV file example [here](#).



It is recommended to open the file in text editor (TextEdit for macOS, Notepad for Windows). The prefix 0,00 may be removed when the file is opened in Excel or Numbers.

Each trunk can be then associated to a pricelist (the first line in trunk configuration window). Read more about associating pricelists to trunks in the next chapter: [Configuring SIP trunks and lines](#).

Configuring SIP trunks and lines

Wildix PBX supports connection of:

- SIP trunks
- ISDN lines (PRI/BRI media gateways)
- analog lines and analog PBXs (W04FXO media gateway)
- GSM network: (DaySaver GSM gateway)

Connected SIP trunks and ISDN / FXO gateways are displayed in WMS -> Trunks:

Trunk									
SIP									
ID	Login	Dialplan	Host	Port	Country Code	Status outgoing	Status incoming		
1	prova1	1	main	dynamic	no				
+ - Edit									
BRI/PRI									
ID	Port 1 Dialplan	Port 2 Dialplan	Port 3 Dialplan	Port 4 Dialplan	Host	Country Code	Status		
1	ISDN BRI MEDIA GATEWAY 0	main	main	main					
- Edit									
GSM/UMTS									
ID	Host	Country Code	Status						
2	GSM MEDIA GATEWAY 0								
3	GSM MEDIA GATEWAY 1								
4	GSM MEDIA GATEWAY 2								
5	GSM MEDIA GATEWAY 3								
7	GSM MEDIA GATEWAY 4								
- Edit									
FXO									
ID	Port 1 Dialplan	Port 2 Dialplan	Port 3 Dialplan	Port 4 Dialplan	Host	Country Code	Status		
6	FXO MEDIA GATEWAY 0	main	main	main					
8	FXO MEDIA GATEWAY 1	main	main	main					
- Edit									

Note: Wildix offers its own built-in VoIP trunk CLASSOUND:

- Web page: <https://www.wildix.com/classound/>
- [How to configure and use CLASSOUND](#)

Note: SIP trunks must be added manually.
BRI / PRI / GSM / FXO lines are displayed in the corresponding tables once the media gateways have been connected to the system and provisioned as described in chapter [Provisioning of devices](#).

Each trunk is displayed in the corresponding section of the page with the following information:

- Country code
- SIP registration status:
 - Green: trunk is registered
 - Grey: trunk is not registered

Note: SIP trunk registration status can be incoming or outgoing, based on the SIP trunk configuration.

- For GSM trunk, the GSM signal power status is displayed
- For BRI/BRI and GSM trunks, status of Layer 1 and Layer 2 for each port is displayed:

- Green: active
- Red: error (inactive)
- Grey: no event received (inactive)

Each trunk is associated to a Dialplan procedure (*main* by default), more information on Dialplan in chapter [Wildix Dialplan](#).

Each trunk can have an associated *Pricelist*, this allows the system to calculate call costs, which can be later on viewed in CDR-View.

SIP Trunk configuration

- Go to *WMS* -> *Trunks*
- Click **+** under SIP section
- Enter parameters:
 - *Title*: trunk identifier (mandatory field)
 - *Trunk name*: trunk name (optional)
 - *Auth login*: login, provided by the VoIP carrier for authentication (mandatory field)
 - *From user*: forced from Number header and used for invite messages and for registration (if From domain is not empty), usually same as Auth login (optional)
 - *From domain*: forced from Domain header and used in register and invite SIP messages (optional)
 - *Address or host name*:
 - for outgoing registration: address or host name of SIP proxy
 - for incoming registration: select *dynamic*
 - you can specify a custom port in the next field (5060 is used by default)
 - *Password*: password for authentication provided by the VoIP Carrier
 - *Dialplan*: Dialplan procedure used for calls on this trunk (*main* by default)
 - *Tone zone*: select the country/ region
 - *Country Code*: used for number normalization, specify the code of the country where the trunk is used
 - *Keep-Alive*: enables periodic sending of keep alive messages to the trunk
 - *Enable registration*: enable this field for outgoing trunk
 - *Advanced*: other advanced trunk settings, check documentation for more information: [Trunk Settings Admin Guide](#)
- Click **Save**
- After several seconds, SIP trunk status changes to green (outgoing or incoming, depending on configuration); it means that trunk has been successfully registered

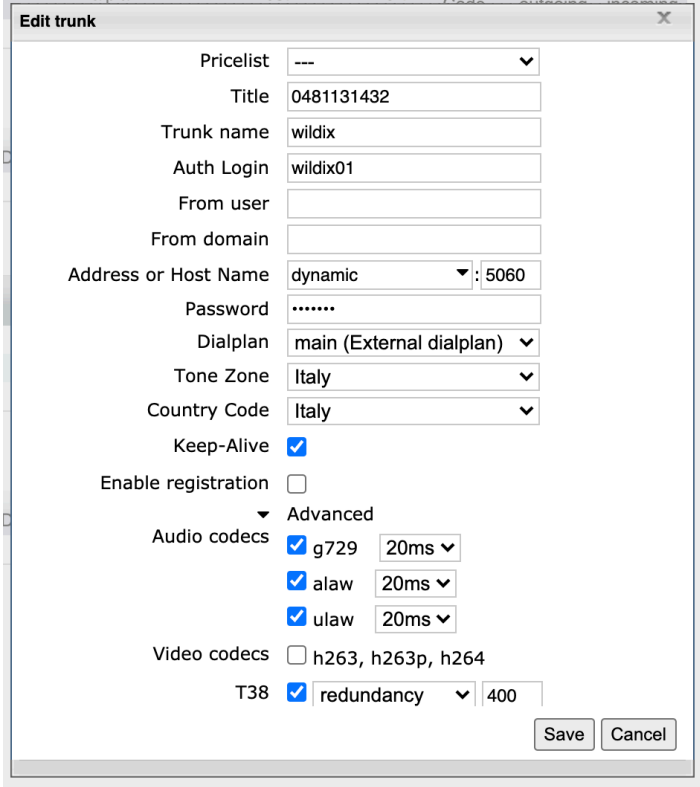
Supported VoIP trunks with configuration examples: [List of Wildix Supported VoIP Operators](#).

Make a test of SIP trunking between 2 PBXs

If you don't have a real SIP trunk, but you have two Wildix PBXs, you can establish SIP interconnection between two PBXs to test calls between them. In this case one PBX is used for outgoing registration, another one - for incoming registration.

Incoming trunk (Server PBX configuration):

- *Address or host name*: *dynamic*



Edit trunk

Pricelist: ---

Title: 0481131432

Trunk name: wildix

Auth Login: wildix01

From user:

From domain:

Address or Host Name: dynamic : 5060

Password:

Dialplan: main (External dialplan)

Tone Zone: Italy

Country Code: Italy

Keep-Alive:

Enable registration:

Advanced

Audio codecs: g729 20ms

alaw 20ms

ulaw 20ms

Video codecs: h263, h263p, h264

T38: redundancy 400

Save Cancel

Outgoing trunk (Client PBX):

- *Address or host name*: IP or domain name of the first PBX
- *Enable registration*: yes
- Make sure password and selected codecs (*Advanced settings*) are the same on both PBXs

Edit trunk ✕

Pricelist: ---

Title: Wildix

Trunk name: wildix

Auth Login: wildix02

From user:

From domain:

Address or Host Name: 192.168.1.69 : 5060

Password:

Dialplan: main (External dialplan)

Tone Zone: Germany

Country Code: Germany

Keep-Alive:

Enable registration:

Advanced

Audio codecs: g729 20ms

alaw 20ms

ulaw 20ms

Video codecs: h263, h263p, h264

T38: redundancy 400

SIP trunk statuses on both PBXs have changed to green, it means that parameters entered for trunk configuration are correct and you can place a call from Client to Server:

Trunks									
SIP									
ID	SIP	Login	Dialplan	Host	Port	Country Code	Status outgoing	Status incoming	
2	aaa	zzz	main	dynamic		it			
3	bbb	yyy	main	dynamic					
4	ccc	xxx	main	dynamic					
10	cloud1	cloud1	main	dynamic					
1	maarten1	maarten1	main	dynamic		it			
9	prova1	prova1	main	dynamic					
7	test	test	main	dynamic					
8	test2	test2	main	dynamic					
6	testmatia	testmatia	main	dynamic					

BRI/PRI									
ID	BRI/PRI	Port 1 Dialplan	Port 2 Dialplan	Port 3 Dialplan	Port 4 Dialplan	Host	Country Code	Status	
8	ISDN BRI MEDIA GATEWAY 0	users	main	main	main	154.41.3.130	ua		
7	ISDN BRI MEDIA GATEWAY 1	users	users			154.41.3.130	it		

GSM/UMTS									
ID	GSM/UMTS	Host	Country Code	Status					
5	GSM MEDIA GATEWAY 0	154.41.3.130							

FXO									
ID	FXO	Port 1 Dialplan	Port 2 Dialplan	Port 3 Dialplan	Port 4 Dialplan	Host	Country Code	Status	
4	FXO MEDIA GATEWAY 0	main	main	main	main	154.41.3.130	it		

ISDN lines (BRI/PRI media gateways)

BRI/ PRI MG are EOL.

Documentation: [Media Gateways Documentation](#).

After you have provisioned a BRI/PRI media gateway, the trunk is displayed in the corresponding section in WMS -> *Trunks* -> *BRI/PRI* table.

- *Status* column -> green light indicates that the trunk SIP registration is active, hover over it for more information (status of connection to the Wildix system)
- *Port X Dialplan* column -> status of Layer 1 and Layer 2 (status of connection to ISDN lines; hover over it for more information)

BRI/PRI	Port 1 Dialplan	Port 2 Dialplan	Port 3 Dialplan	Port 4 Dialplan	Host	Country Code	Status
ISDN BRI MEDIA GATEWAY 0	● ● main				192.168.4.168	de	

To edit the trunk parameters, double-click on the media gateway.

Check the following parameters:

- *Default tone*
- *Country code*

For other trunk parameters, check documentation: [Trunk Settings Admin Guide](#).

GSM network (DaySaver GSM media gateway)

Documentation: [Media Gateways Documentation](#).

To install a DaySaver media gateway, proceed as follows:

- Connect antennas to the rear panel of the gateway
- Insert the SIM card to the slot

Note: Make sure the PIN code of the SIM card is disabled.

- Connect the WAN interface of the gateway to the Wildix Switch
- Provision the gateway as described in chapter [Provisioning of devices](#)
- Once you have provisioned the gateway, a new trunk automatically appears in the corresponding section in WMS > *Trunks* -> *GSM/UMTS* section
- The status is green, which means the media gateway is registered

Important: Status of signal quality is currently not supported!

ID	GSM/UMTS	Host	Country Code	Status
14	GSM MEDIA GATEWAY 0	154.41.3.130		

- Double click on the trunk to edit the trunk parameters:
- *Default Tone*: select the country where the trunk is used
- *Country Code*: select the country where the trunk is used for correct number normalization; select Custom country to manually enter the country code
- *Dialplan (main by default)*: Dialplan procedure used for calls via this trunk
- *Number of SIM*: called number, which should be present in the Dialplan procedure, used for calls via this trunk; more information on Wildix Dialplan to follow, in chapter [Wildix Dialplan](#)
- *Enable SMS receiving*: enable incoming SMS messages to the SIM card; specify the e-mail address in the field below
- *SMS2EMAIL service e-mail*: e-mail address used for new messages notifications

For other trunk parameters, check documentation: [Trunk Settings Admin Guide](#).

For more information on SMS sending, read the guide [FAX/ SMS Server Quick Admin Guide](#).

Call routing strategies: Dialplan

Wildix Dialplan: how it works

Dialplan is a set of rules that determine the strategy of routing incoming and outgoing calls to the right destination. Wildix Dialplan allows you to customize the system to your specific needs, yet is very easy to set up and to manage.

In this guide we will only cover the basic Dialplan scenarios, which are most popular and easy to implement.

Associating entities to Dialplan procedures

In the previous chapters we have seen that each entity that can initiate a call - a user, a VoIP trunk, a media gateway - requires association to a Dialplan procedure.

By default users of the system are assigned to the Dialplan *users* procedure, while VoIP trunks and media gateways are associated to the *main* procedure.

Go to *WMS -> Dialplan*: by default these two Dialplan procedures are already present on your PBX. You can create more Dialplan procedures if needed and then associate them to trunks, to users or, to other Dialplan procedures.

Associating Dialplan procedures to users and trunks:

- Users: go to *WMS -> Users*, double-click on a user and edit the field *Dialplan*
- Trunks: go to *WMS -> Trunks*, double click on a trunk and edit the field *Dialplan*

	Admin ▾
Full Name	Ksenia Babych
Login	Ksenia
Extension	448
Fax	
Office	+3484123455
Email	ksenia.babych@wildix.com
Mobile	
Dialplan	users (Internal dialplan) ▾
Fax dialplan	users (Internal dialplan) ▾
Language	En ▾
Group	Admin ▾
Department	Marketing
License type	Premium ▾

Pricelist	--- ▾
Title	Liberty
Trunk name	Liberty
Auth Login	██████
From user	██████
From domain	
Address or Host Name	dynamic ▾
Password
Dialplan	main (External dialplan) ▾
Tone Zone	Norway ▾
Country Code	Norway ▾
Keep-Alive	<input checked="" type="checkbox"/>
Enable registration	<input type="checkbox"/>
	▶ Advanced

Each time an entity (user, trunk) generates a call, the system checks the Dialplan procedure associated to the entity. For example, a user starts a call, in case the match for this *called number* is found inside the Dialplan procedure associated to this user (*users* by default) the system starts to execute Dialplan applications defined for this *called number* in the specified order.

Matching called numbers

Each Dialplan procedure can contain multiple *called numbers*.

Called numbers inside *main* procedure example: all the company phone numbers can be added as called numbers to the *main* Dialplan procedure. Each time a call arrives from a trunk, the Dialplan checks if the *called number* is present in the Dialplan procedure associated to this trunk.

Called numbers inside *users* procedure example: in a typical implementation it is recommended to cover all the called numbers that can be possibly dialed by users. How to cover all the possible cases? It is possible, because a called number can be either:

- an exact match: e.g. *000380671234567*
- a pattern: a sequence of digits and special characters in order to match all the numbers that correspond to the specified criteria, e.g.: *00038*. any number starting from 00038 and followed by at least one digit. In this way it is possible to route calls based on the country prefix, for example, or depending on whether it is a mobile or a landline phone number
- *default* destination: selecting the word *default* as *called number* allows covering all the cases that have not been covered previously in this Dialplan procedure; in a normal implementation, *default* destination is used in users Dialplan to notify a user that the number he/she dialed is incorrect.

Syntax to use patterns as a called number:

- X (uppercase): any digit from 0 to 9
- . (point): one or more characters from 0 to 9 of any length
- [] (square brackets): any digit from those specified inside the brackets
- Z (uppercase): any digit from 1 to 9
- N (uppercase): any digit from 2 to 9
- ! (exclamation point): zero or more characters

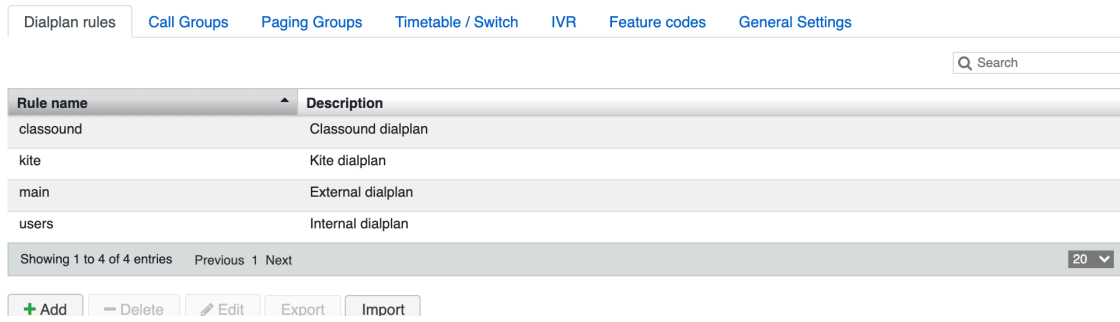
Examples:

- *0*. – the numbers starting with 0 followed by a one digit or a sequence of digits (typically used for direct calls to the public line)
- *1XX* – the numbers starting with 1 followed by two other digits, e.g. 125, 167
- *[37]2X* – the numbers starting with 3 or 7, followed by 2 and by any other digit, e.g. 326, 728
- *X*. – any numbers of any length
- *[1237-9]* – matches 1,2,3,7,8,9
- *XXX!* – all numbers containing three or more characters (while *XXX*. matches all numbers containing at least four characters)

Adding and editing Dialplan procedures

As already said, by default you can find two procedures in *WMS* -> *Dialplan*:

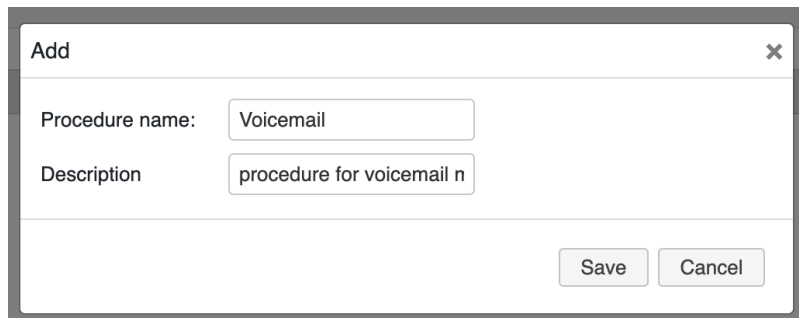
- *main* (associated to media gateways and VoIP trunks)
- *users* (associated to users)
- *kite* (this procedure is dedicated to Kite service, described in chapter [Wildix WebRTC Kite](#))
- *classound* (this procedure is dedicated to CLASSOUND service, described in [How to configure and use CLASSOUND](#))



You can edit these procedures or add new ones and later on associate them to users, to trunks, or to other Dialplan procedures.

To add a new procedure, proceed as follows:

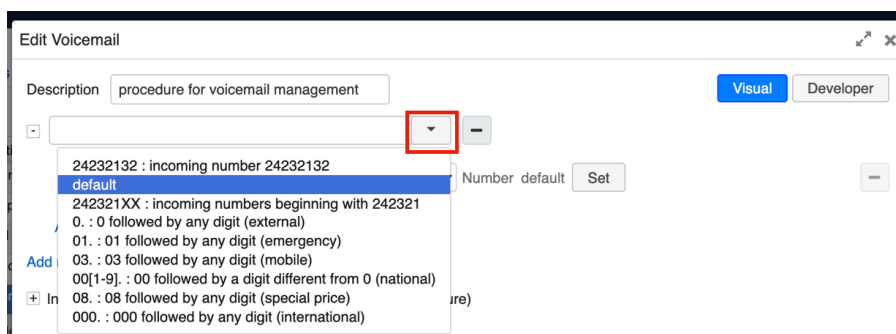
- Click **+**
- Enter *Procedure name* and *Description* (optional)



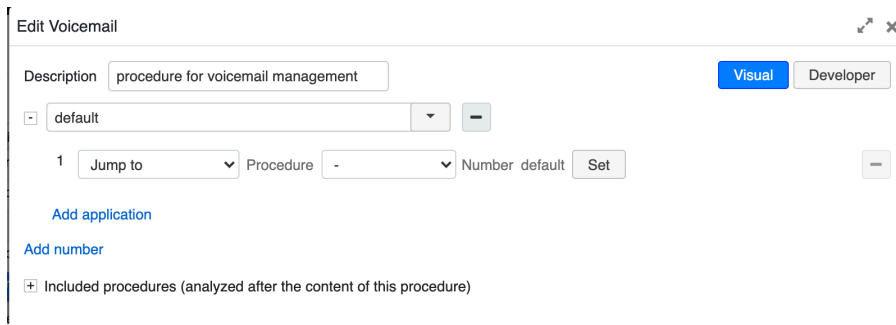
To edit a procedure, double-click on it:

Adding Called numbers:

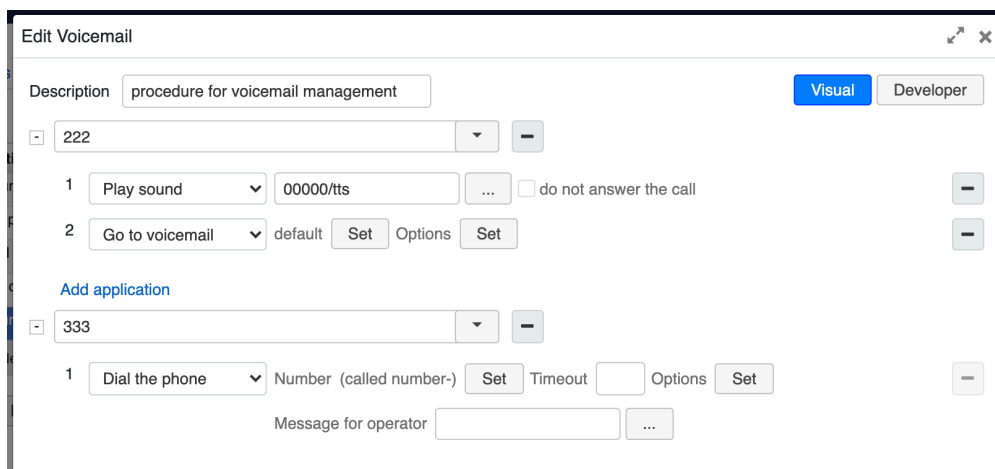
- Click **Add number** to enter manually a called number or click the arrow to open a drop-down list of destinations, including *default*:



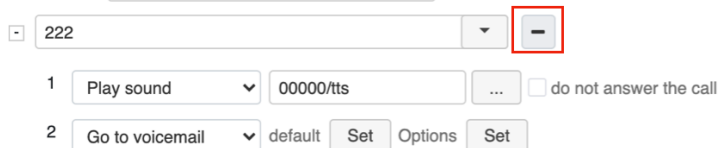
- Enter a *Called number* (which can be a phone number, a pattern or the word *default*):



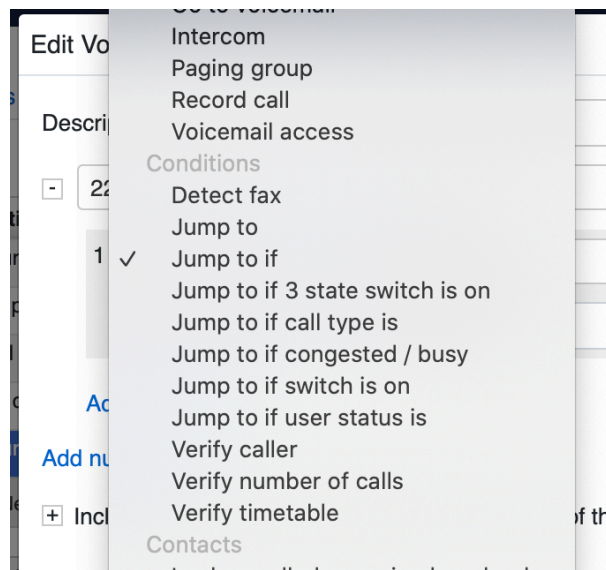
- You can add multiple *Called numbers* to the same Dialplan procedure, click **Add number** again to add more *Called numbers* to the same Dialplan procedure:



- To delete a called number and all the relative Dialplan applications, click - in front of the *Called number*:



- At this point you can start adding Dialplan applications: click **Jump to** to open the drop-down list:



- To add more Dialplan applications, click **Add application**

Dialplan applications

Dialplan applications are the operations which are executed in a sequence defined by the PBX administrator after the match to the called number is found inside the associated Dialplan procedure.

Here is a complete list of Dialplan applications with detailed descriptions and practical examples: [Dialplan applications Admin Guide](#).

Some Dialplan applications allow modification of the original called number and jumping to a different Dialplan procedure.



Note: Starting from WMS v. 5.01.20200522.1, it is possible to edit Dialplan applications via **Developer** option (JSON editor):



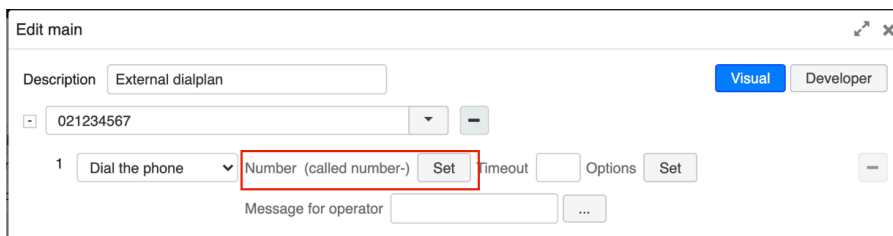
Modify called number

Here is an example of the Dialplan application *Dial the phone* which routes the call to the specified destination.

Expected scenario: an incoming call to the number 021234567 must be routed to user 100.

Implementation:

- add called number 021234567 in *main* Dialplan procedure
- add the Dialplan application *Dial the phone* and click **Set** near *Number (called number)* to edit the *Called number*



The following menu opens allowing you to change the called number:

- *Custom*: tick the field and enter your phone number (in our example, 100)

021234567

1 Dial the phone Number 100 Set Timeout Options Set

Message for operator

Here is another example of the Dialplan application Dial the phone with DID (Direct Inward Dialing).

Expected scenario: call coming to the number 021234533 must be routed to the user 133, call coming to 021234532 must be routed to the user 132, etc.

Implementation:

- add called number 0212345XX in main Dialplan procedure (XX means any two digits)
- add the Dialplan application *Dial the phone* and click **Set** near *Number (called number)* to edit the *Called number*
 - *Remove*: allows removing a number of digits (specified in the input field) from the beginning of the called number; in our example 7 ditis are removed, called number is modified: 0212345XX -> XX
 - *Prepend digits*: allows prepending digits to the called number; in our example the digit 1 is prepended, called number is modified XX -> 1XX

0212345XX

1 Dial the phone Number 1(called number-7) Set Timeout Options Set

Message for operator

As a result an incoming call to number 0212345XX is routed to number 1XX: for example incoming to 021234532 is routed to user 132.

Jump to another procedure

Some Dialplan applications allow under certain conditions jumping to a different Dialplan procedure.

Example scenario: incoming calls must be routed to Voicemail during the hours when the offices are closed.

Implementation:

- create a new timetable in *WMS -> Dialplan -> Timetable / Switch*, and set up the state *check time* (it means that each time this Timetable is verified by the Dialplan, the system checks if your offices are closed at the moment, according to this timetable)
- create a new procedure in *WMS -> Dialplan*, add *default* as *Called number* and add Dialplan application *Go to Voicemail*

In the chapter [Create a timetable](#) it is explained how to create a Timetable and to work with it.

- edit the *main* procedure and add the application *Verify Timetable* for your office phone number and add a jump to another procedure created at the previous step (*Offices_closed*) in our example:

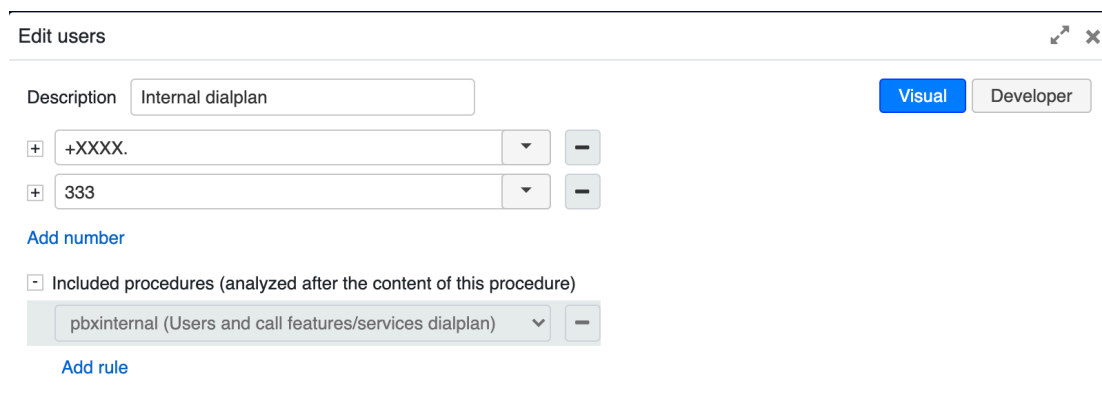
In case your offices are closed, the Dialplan routes the call to another procedure called “Offices_closed”. You must separately create this Dialplan procedure in which, for example, you enable the system to play the audio message to the caller and send the call to Voicemail.

Included procedures

The section *Included procedures* allows you to add the called numbers that must be analysed after the content of the current procedure.

In this way you can create the correct order of operations’ execution in case several patterns (called number prefixes, for instance) come into conflict within the same Dialplan procedure.

Open *users* procedure, go down to *Included procedures* and click to extend it: *pbxinternal (Users and call features/ services dialplan)* is already present there, which by default enables the users to call each other and to use the Feature Codes of the system and which is analyzed only after the content of the Dialplan procedure:



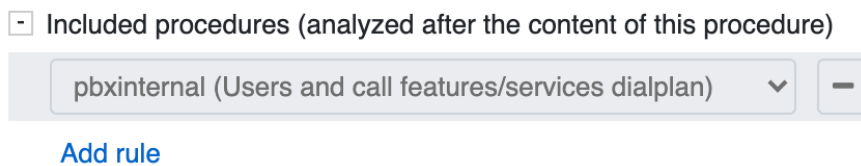
This is just one of the cases where *Included procedures* are used.

Dialplan practical examples

In this part we will learn how to use the most popular Dialplan applications for managing outgoing and incoming calls.

Internal Dialplan - users

As mentioned previously, users are by default enabled to call each other and to call feature codes of the system, since *pbxinternal* procedure is present under *Included procedures* section:



However, *users* procedure must cover all the destinations called by users of the system (national, international, mobile calls etc), and this is why it is recommended to use patterns, described in chapter: [Matching called numbers](#).

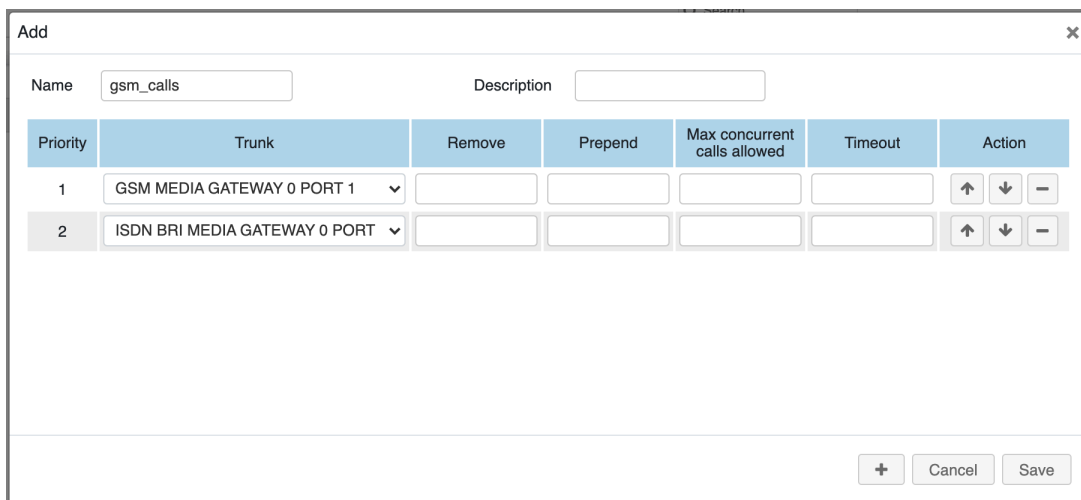
The most common Dialplan applications used in *users* procedure are Dial the trunk / Trunk group. Dial the trunk allows you to select the trunk which is used to place a call.

Trunk groups

Go to *WMS* -> *Trunks* -> *Trunk groups*.

In case you have configured several trunks and you would like to set up a certain priority in which trunks must be tried one after another, you can create Trunk groups.

Example: you would like to route the calls to mobile numbers via GSM trunk, however you would like to have the opportunity to place a call via a different trunk, in case GSM trunk is occupied:



In this case call is routed via GSM trunk, if it's busy, call is routed via the ISDN trunk.

It is possible to remove or prepend digits to called number, set up the maximum concurrent calls on each trunk and define the timeout after which the system tries to place a call via the next trunk in the trunk group.

After you have configured a trunk group on this page, you can use it in the Dialplan (application *Trunk group*).

Call through remote PBX

This Dialplan application is useful in a multisite environment, where the same company has offices and PBXs located in different countries.

Example: a company has its headquarters in Germany and a branch office in France. They would like to route the calls to French phone numbers through their remote PBX installed in France and using local French lines.

German PBX, *users* procedure:

Add the French prefix as a called number and add the Dialplan Application "Call through remote PBX" ("client.wildixin.com" in our example is the name of the French PBX, "users" is the name of the procedure present on the French PBX):

the call is routed through the French PBX, so inside the indicated "users" procedure on French PBX, the match for the indicated called number "00033." must be present.

French PBX, *users* procedure:

Add the same called number 00033. and click **Set** to modify this called number:

Here is the result that we get: the call is routed to the French PBX, before dialling the trunk *local - 22* the system removes the first 5 digits from the called number (the number is normalized), so the number dialled in the international format (for example, 000331234567890), becomes a local French number (1234567890):

1 Number (called number-5) Class

Timeout max calls Options

In the same way many other Dialplan applications allow modifying the called number or require association to another Dialplan procedure present on the same PBX (or on another PBX as in the previous example).

Example of *users* procedure configuration

An example of Dialplan configuration for outgoing calls:

Edit users Visual Developer

Description

1 Procedure

[Add application](#)

1 Procedure Number default Timeout Options

[Add application](#)

1 Number (called number-) Class Timeout max calls Options

[Add application](#)

1 Number (called number-) Class Strategy

[Add application](#)

[Add number](#)

Included procedures (analyzed after the content of this procedure)

- **+XXXX.** : Check if the called number is an international phone number (e.g. +39.). In this case “0” is added as the default prefix for the outgoing line selection
- **00039.** : Check if the called number is an Italian phone number. In our example, the enterprise has an office in Italy and one of the PBXs in the WMS Network is installed in Italy. In this case, it is possible to take advantage of the trunks present on the remote PBX: the call is routed via the remote PBX installed in Italy, following the *users* procedure present in the Dialplan on that PBX.
- **0X.** : Check if the called number is the landline number (any number starting with any digit). In this case the call is routed via the trunk *classound*. The first digit (0 for the external line selection) is removed from the called number
- **01[567].** : Check if the called number a mobile number (any number starting with 15, 16 or 17 for Germany, check the guide [ACL rules and Call classes management](#) for your country). In this case the call is routed via the trunk group *gsm_calls*. The first digit (0 for the external line selection) is removed from the called number

External Dialplan - main

External Dialplan procedure *main* normally should contain all the phone numbers of the company and the rules of routing an incoming call to each of these phone numbers.

Route incoming calls to call agents (call groups)

To create call groups, go to *WMS -> Dialplan -> Call groups*:

- Click on **+** to add a new Call group
- Enter the *Name* of the call group into the field
- Select the agents from the box on the left and move them to the box on the right
- Click **Save**

[Dialplan rules](#) | [Call Groups](#) | [Paging Groups](#) | [Timetable / Switch](#) | [IVR](#) | [Feature codes](#) | [General Settings](#)

Search

ID	Name
1	assistance_tech
2	sales

Showing 1 to 2 of 2 entries 1 row selected Previous 1 Next 20

[+ Add](#) | [- Delete](#) | [Edit](#) | [Edit strategy](#)

! You can add the same call agents to different groups. You can add users from all your PBXs in WMS Network to call groups.

Select the group and click on **Edit strategy** to modify the strategy of call distribution. Read more on Call groups strategies: [Call distribution in Call groups](#).

Now you can edit the *main* procedure to enable the Dialplan to route the incoming calls to your tech support phone number to the call group *assistance_tech*.

Example:

04611715112

1 Call group assistance_tec Message for operator

Timeout 180 Music on hold class class1

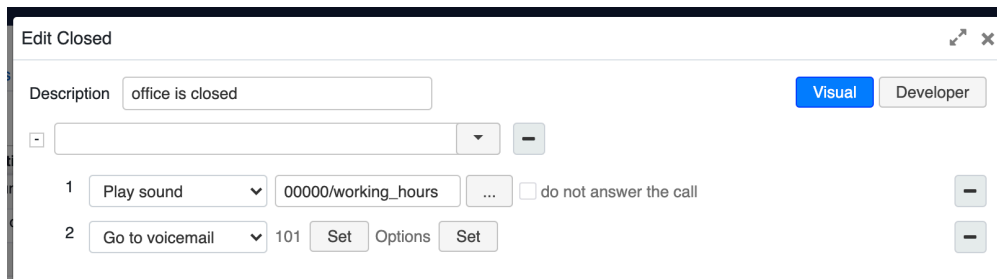
You can:

- set the *Timeout*, after which next Dialplan application is executed
- select the *Message for the operator* providing more information about the call (example of an audio message that the operator who is present in different call groups, hears: “technical support call”)
- select the Music on hold class

Record and playback audio messages

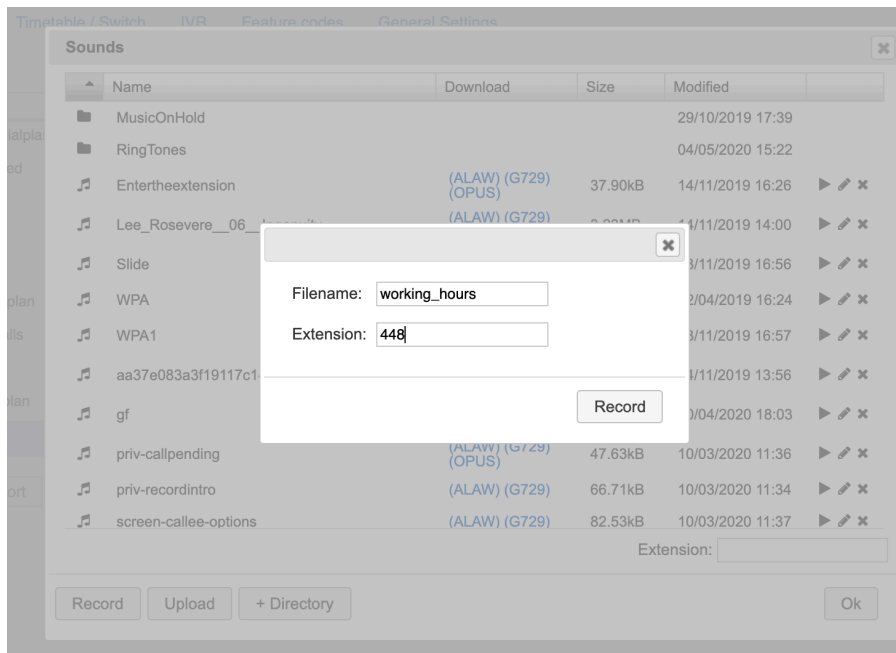
You can record the message for the operator or an audio message to be played back to the caller directly from the Dialplan or from Sounds menu.

Example: you have set up the Dialplan to check the timetable and to route the incoming calls to another Dialplan procedure in case the offices are closed. In this case you can enable the system to playback the audio file to the caller and then to route the calls to Voicemail:

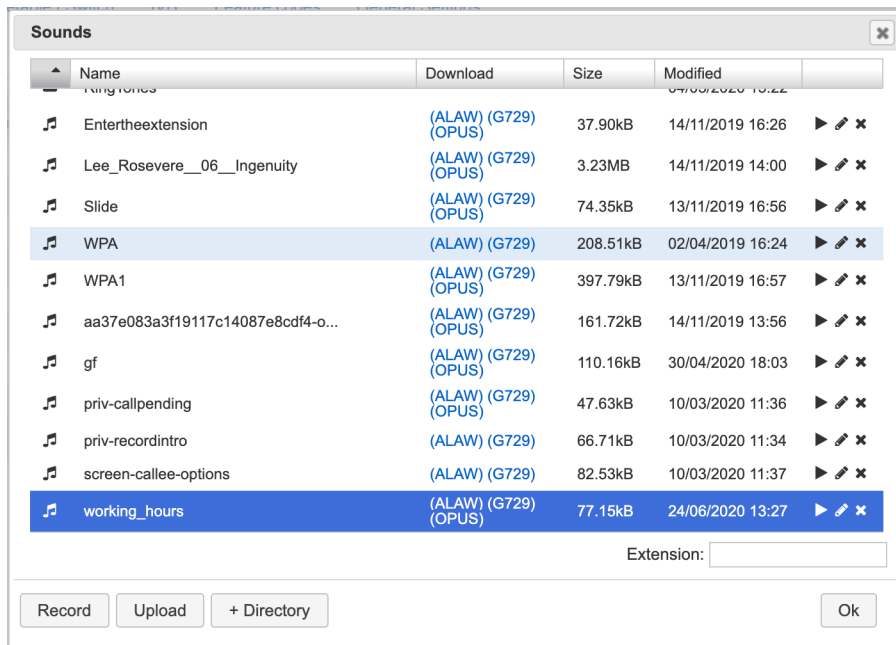


To record the sound to be played to the caller, click the ... button to open *Sounds* menu and then click **Record** button:

- Enter the name for your message into the field *Filename* and your extension number into the field *Extension*:




- Click **Record** button: the call arrives to Collaboration/ the device registered to your account (e.g. a Wildix phone)
- Answer the call and pronounce your message (e.g. “Our offices are closed. Your call will be forwarded to Voicemail”)
- Hang up to save your message:



Via this menu it is possible to upload and play audio files:

- Click **Upload**
- Select the file on your PC that you wish to upload
- Click **Open**

WMS supports all the common audio formats: mp3, wav, alaw.


 Note: All uploaded files are also converted into Opus (HD codec) audio format. To guarantee the high-definition quality, make sure that you upload high quality source files.

Playing the audio files back:.

- Files in opus format can be played directly in browser
- For other formats, specify an extension number in *Extension* field -> the playback call is placed to the extension, answer it to play the file

You can also use TTS (Text-to-speech) in this menu to create audio messages by transforming text into speech (restricted by license, read more: [Wildix Business Intelligence - Artificial Intelligence services](#)); watch the video: <https://www.youtube.com/watch?v=ljHQPyi2bSs>

Create a switch

 Note: Starting from WMS 5.02, there is no limit in the number of created switches and timetables. Prior to this version, you can create no more than 255.

You can create switches to enable the system to change the strategy of incoming calls routing depending on the actual Switch status.

Examples:

- Director / Secretary service - director can enable the switch in order not to be disturbed by calls. When the switch is enabled, all the calls are routed to the secretary; this configuration is normally applied to “users” procedure in order to forbid employees to call the director and to forward all the calls to the secretary or to the group of secretaries. Check documentation: [How to configure a Director-Secretary Switch](#)
- Voicemail switch - enable the switch in case you would like to temporarily route all the incoming calls to Voicemail.
- Three state switch - this switch has three states (on / off / extra) and allows you to route the calls to different Dialplan procedures in each case.

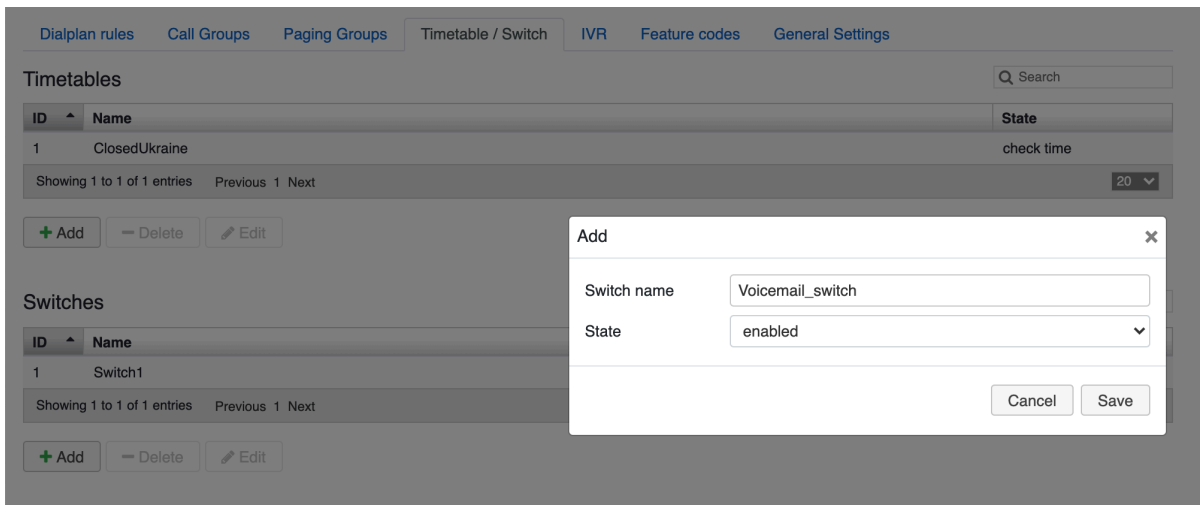
Go to *WMS Dialplan -> Timetables / Switches*.

Click **+** under Switch table to add a new switch (click **+** under *3 states switch* to add a new three states switch).

Example:

Step 1. Create a switch to forward calls to Voicemail:

- Click **+** in the *Switches* section
- Enter the name for the switch and select the State *enabled* (you can change the state of the switch from the phone or by calling a feature code)



Step 2. Create a Dialplan procedure to be executed if the switch is on:



Step 3. Modify the *main* procedure to check the status of the switch before routing the call:

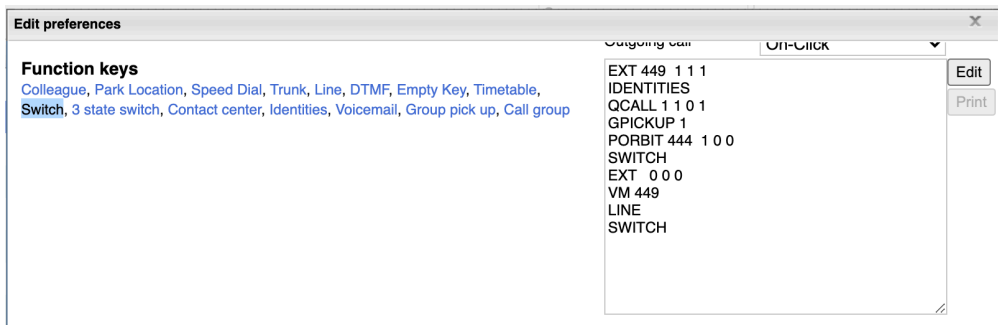


Change the state of the switch

- Via a Feature code: dial the Feature code 93 from your WP phones and follow the audio instructions
- From the phone: press the function key (BLF key) that you have previously configured (explained below)

Configure a function key from *WMS -> Users* (the same operation can be done via *Collaboration Settings -> Function keys*):

- Select the user and click **Edit preferences**
- Go to the section *Settings -> Function keys* and click on **Switch** to add Switch to the list of function keys
- Type the ID number of the Switch (Switch ID can be checked in *WMS -> Dialplan -> Timetables / Switches*)
- Click **Save**

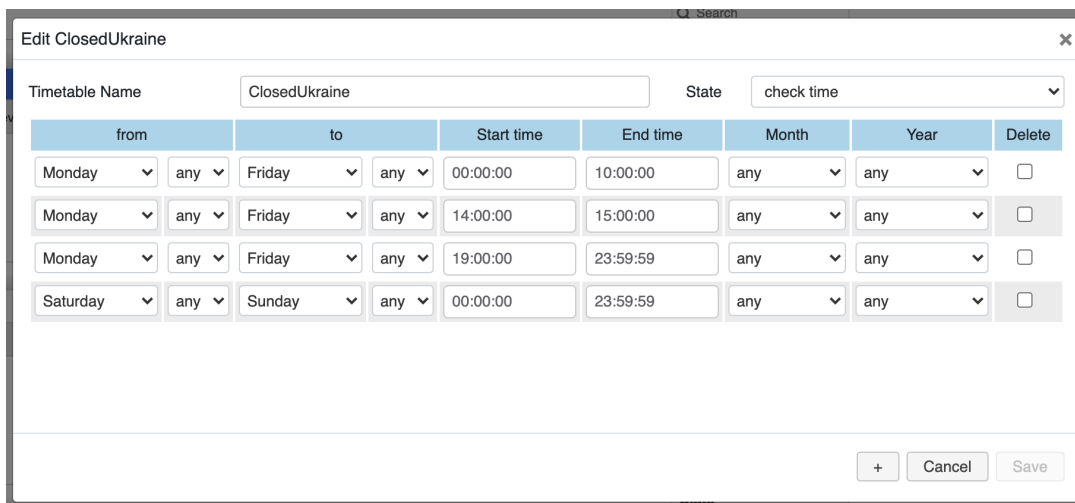


In the same way you can configure 3 state switch or Timetable function key.

Create a timetable

Create the working hours timetable for your office:

- Click **+** in the section *Timetable*
- Enter the *Timetable Name* and select *State check time* (*Check time state* means that the PBX determines whether the timetable is active, based on the PBX time at the moment of the Dialplan execution)
- Select the timetable and click **Edit** and specify the working hours:




In the same way as we did for the Switch, you must create a separate procedure to be executed in case the office is closed according to this timetable.

You can then enable the Dialplan to jump to another procedure in case the offices are closed:



Create an IVR tree

IVR (Interactive Voice Responder) is a technology that allows humans interact with telephone system by entering DTMF tones. An example of IVR is when a caller hears “Press 1 for English, press 2 for German” and call is routed to a different destination based on the choice made by the caller.

 **Note:** It is possible to use Automatic Speech Recognition in Dialplan for creating IVRs with voice control. More information: [How to configure IVR via ASR with Directory in Dialplan.](#)

Wildix graphical IVR tree can be multilevel and is easy to manage. You can define each node (each level) of an IVR tree as an action or as a submenu:

- *Submenu* is an intermediate node which brings the caller to the next level of IVR. You can set up the system to playback an audio file inviting the caller to make a new choice.
- *Action* ends the IVR execution and routes the call to the specified Dialplan procedure with the possibility to modify the caller number.

Example: create an IVR of three levels.

Level 1: Audio file inviting to press 1 for English, 2 for German

Level 2, caller pressed 1: audio file inviting to press 1 for tech support, 2 for sales

Level 3, caller pressed 1: call is routed to the English speaking operator of the tech support

Level 3, caller pressed 2: call is routed to the English speaking sales assistant

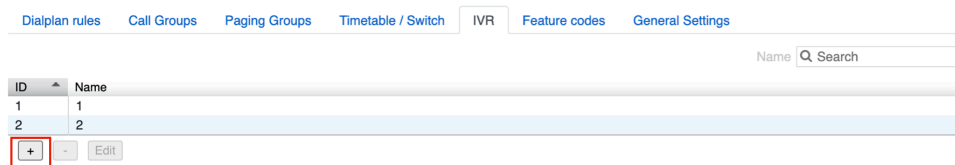
Level 2, caller pressed 2: audio file inviting to press 1 for tech support, 2 for sales, in German

Level 3, caller pressed 1: call is routed to German speaking Tech_support group

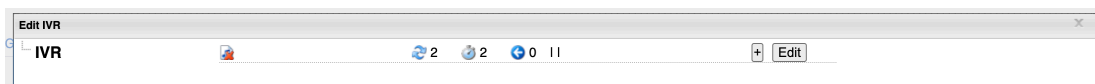
Level 3, caller pressed 2: call is routed to German speaking Sales group

Go to WMS -> Dialplan -> IVR

- Click **+** to create a new IVR tree and give it a name. Click **Save:**



- Double click the IVR to edit it:



At this step we can create levels (nodes) of our IVR tree.

Node of the first level

(Audio file inviting to press 1 for English, 2 for German)

Click **Edit**:

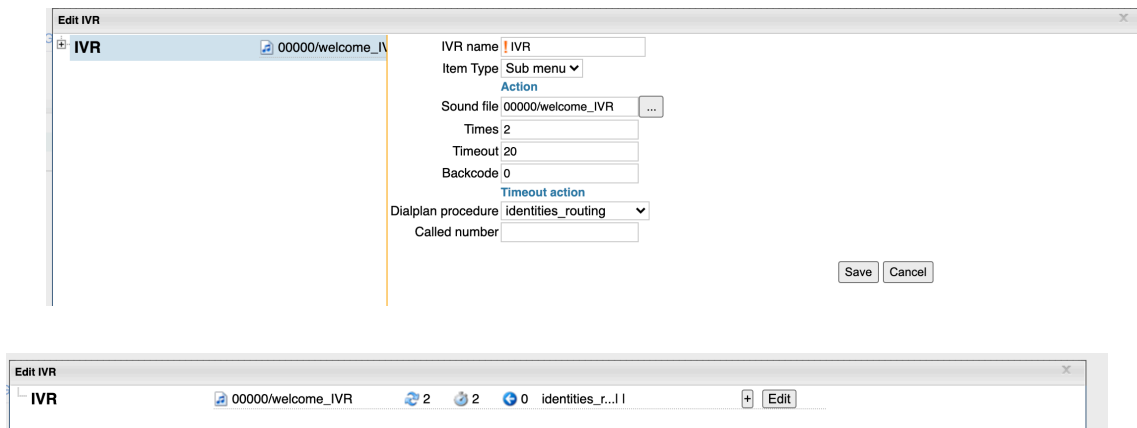
- *Item time: Sub menu* (an intermediate node)

Action:

- *Sound file*: select the audio file (or record it)
- *Times*: number of times the audio file is played back to the caller
- *Timeout*: after this timeout in seconds, the Timeout action is performed
- *Backcode*: code to come back to the previous menu

Timeout action:

- *Dialplan procedure*: set up to route the call to a different Dialplan procedure in case caller pressed nothing within the specified timeout
- *Called number*: this option allows you to modify the caller number (match must be found in the specified Dialplan procedure)

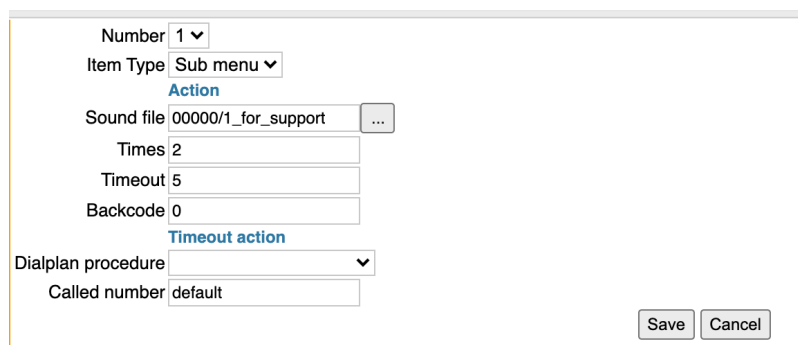


Nodes of the second level

(Audio file inviting to press 1 for tech support, 2 for sales (in English in case caller entered 1, in German, in case caller entered 2))

Press + in front of the first level node to add a new level.

- *Number*: the number that the caller must enter in order to arrive to this node



Number ▾

Item Type ▾

Action

Sound file ...

Times

Timeout

Backcode

Timeout action

Dialplan procedure ▾

Called number

Nodes of the third level

(Routes the call to the final destination (user or group))

Click + in front of the corresponding second level node, to add a new level, for example:



All of these nodes terminate the execution of the IVR tree:

- *Item type: Action*

Action:

- *Called number: extension number*

Number ▾

Item Type ▾

Action

Dialplan procedure ▾

Called number

Number ▾

Item Type ▾

Action

Dialplan procedure ▾

Called number

Where 123 and 224 are English speaking operators (tech support and sales)



Where 111 and 222 are the called numbers present in the procedure IVR that we must create separately.

Number	1
Item Type	Action
Dialplan procedure	IVR
Called number	111

Number	2
Item Type	Action
Dialplan procedure	IVR
Called number	222

According to this procedure, incoming calls to 111 are routed to tech support call group, incoming calls to 222 are routed to sales call group:

Edit IVR Visual Developer

Description

▾ 111 ▾ -

1 Call group ▾ Tech_Support ▾ Message for operator ... ▾

Timeout 20 Music on hold class default ▾

2 Jump to ▾ Procedure Voicemail (Voic) ▾ Number default Set ▾

Add application

▾ 222 ▾ -

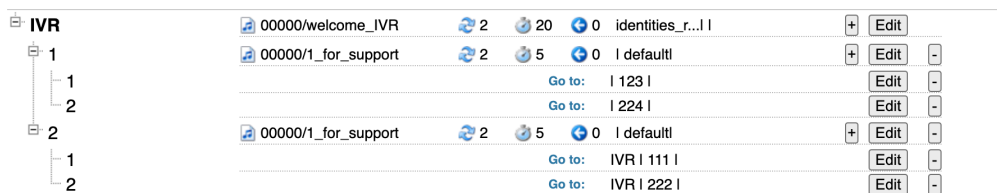
1 Call group ▾ Sales ▾ Message for operator ... ▾

Timeout 20 Music on hold class default ▾

2 Jump to ▾ Procedure Voicemail (Voic) ▾ Number default Set ▾

- Called number 111: call is routed to Tech_Support call group (in case of no response within 20 seconds, call is routed to Voicemail)
- Called number 222: call is routed to Sales call group

Here is the ready IVR tree:



Now we can use it inside our main procedure:

▾ 04611715110 ▾ -

1 IVR ▾ IVR ▾ ▾

Incoming faxes management

Wildix systems integrate Fax server by default. All the services for managing incoming and outgoing faxes are enabled on all Wildix PBXs.

Make sure SMTP client is defined in *WMS Settings -> System -> SMTP client* (see the chapter [SMTP Client](#)).

Fax to e-mail

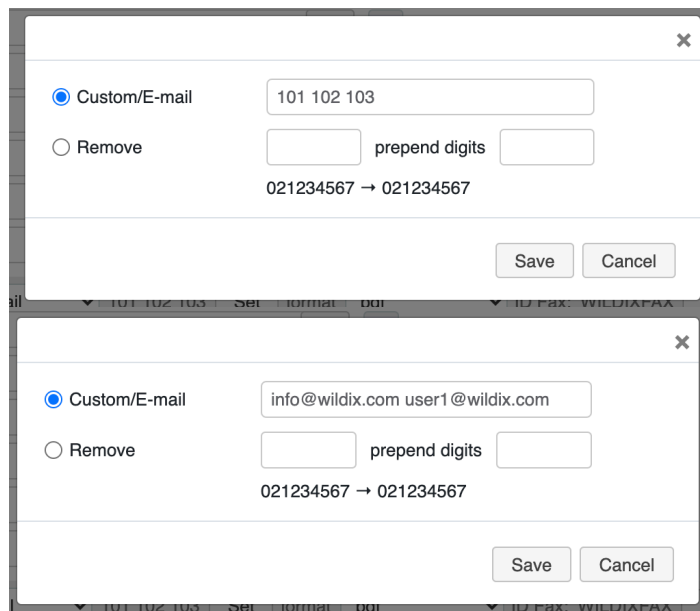
Answers an incoming call using FAX Server and forwards fax to one or multiple fax numbers / users:

021234567

1 Fax to e-mail 101 102 103 format pdf ID Fax: WILDIXFAX

If you indicate an extension number (e.g. 101), a copy of fax is sent to the user email address, and a link to fax download appears in *Wildix Collaboration* → *History* menu and in CDR-View.

You can enter several extension numbers / email addresses into the field, separated by spaces, in this case the copy of received faxes is sent to multiple destinations:



All received and sent faxes are permanently saved on the storage device defined in *WMS Settings* -> *System* -> *Storages*.

Detect fax

Note: especially helpful when the same number is used for incoming calls and faxes.

Answers the call and within a timeout specified in *fax detect time* waits for the tones of a remote fax (in the meantime the system to continue the Dialplan execution).

- *Fax detect time*: enter the timeout for fax detection in seconds (usually 3 seconds are enough)
- *Continue the execution*: if enabled, the Dialplan execution continues without waiting for the number of seconds specified in *fax detect time* field before the fax is detected (to avoid silence while the fax is being detected)
- *Procedure*: select the procedure to route the call in case the fax is detected
- *Set Number*: modify called number (the match must be present in the specified Dialplan procedure)

021234567

1 Detect fax fax detect time 4 (seconds). Continue the execution

Procedure main (External) Number default Set

2 Call group test Message for operator ...

Timeout 40 Music on hold class default

[Add application](#)

fax

1 Fax to e-mail info@wildix.com Set format pdf ID Fax: WILDIXFAX Set

In our example in case within 4 seconds fax is detected, the system stops the execution of the application *Call group* and the call is forwarded to the called number *fax* (present inside the same Dialplan procedure *main*), in which the fax is being sent to email.

Incoming fax from trunk to FXS user (fax machine)

Add Dialplan application *Detect fax* in case phone number is used both for faxes and calls, otherwise you can use *Jump to*.

Select the procedure *pbxfeatures* or *pbxservices* and edit the called number (click **Set** near *Number*)

- Tick *custom* and enter the string *90*101* (where *101* is fxs user extension number), example:

04611715111

1 Detect fax fax detect time 4 (seconds). Continue the execution

Procedure pbxfeatures (F) Number 90*101 Set

Where

- *pbxfeatures* / *pbxservices* are procedures that are present by default on Wildix PBX for recognition of PBX services and features (including feature codes)
- *90* is the feature code *Fax relay*; *101* is the fxs user extension number (read more about Feature codes: [Feature Codes and Pre answer Services Guide](#))

DID & DISA

DID and DISA services enable the caller to reach PBX users directly by dialing their extension numbers.

Example of DID (Direct Inward Dial) configuration:

046117151XX

1 Dial the phone Number (called number-8) Set Timeout Options Set

Message for operator

First 8 digits are removed from the called number. Depending on the last two digits of the called number (*1XX*) incoming call is routed to the extension, examples:

- Incoming call to 04611715111 is routed to extension 111
- Incoming call to 04611715112 is routed to extension 112
- Incoming call to 04611715122 is routed to extension 122

Example of DISA configuration:

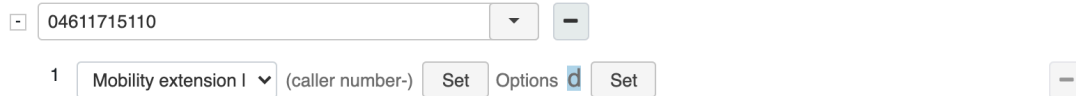
- Called number *default*:
 - The message is played inviting the caller to enter the extension number
 - The system waits for digits for 5 seconds
 - In case of no input within the specified timeout, call is routed to call group
- Called number *XXX*:
 - In case caller entered extension number, call is routed to the corresponding user

Mobility extension lookup

It is possible to enable the system to recognize PBX users when they call the office phone number from their mobile phone numbers. Note that user mobile phone number must be present in WMS.

Thanks to this feature PBX, mobile calls of employees become an extension of Wildix PBX and calls can be treated in the same way, as the ones done from the office phone.

If the caller number corresponds to the mobile number of one of PBX users, Dialplan jumps to the procedure predefined for the outgoing calls of this user.



04611715110

1 Mobility extension I (caller number-) Set Options Set

- *Set - caller number*: allows you to modify the caller number to match the one present in the procedure for the outgoing calls for this user, e.g. *users*
- *Set - Options - d*: hangs up a call and makes a call back to the user (in this way call is free of charge for the user)

Example of *main* procedure configuration

In our example, the enterprise has three phone numbers:

- +49 0461 1715110 – general company phone number
- +49 0461 1715111 – technical support
- +49 0461 1715112 – sales assistance

In case of incoming call to +4904611715110, the following operations are executed:

1. Mobility extension lookup. In case the phone number from which the call arrives is present in the field *Mobility* of one of the users of the system, the call is hanged up and the system makes an automatic callback to the caller
2. Check the timetable *Working_hours*, in case the call has arrived at the time when the office is closed, another Dialplan procedure *Working_hours* is executed
3. Check the switch *Voicemail*, in case the switch status is enabled, another Dialplan procedure *Voicemail* is executed
4. The call is routed to IVR

In case of incoming call to +4904611715111, the following operations are executed:

1. Check the timetable *Working_hours*, in case the call has arrived at the time when the office is closed, another Dialplan procedure *Working_hours* is executed
2. Check the switch *Voicemail*, in case the switch status is *enabled*, another Dialplan procedure *Voicemail* is executed
3. The call is routed to the call group *Tech_support*
4. In case no one responds within 20 seconds, another Dialplan procedure, *Voicemail* is executed

In case of incoming call to +4904611715112, the following operations are executed:

1. Check the timetable *Working_hours*, in case the call has arrived at the time when the office is closed, another Dialplan procedure *Working_hours* is executed
2. Check the switch *Voicemail*, in case the switch status is *enabled*, another
3. Dialplan procedure *Voicemail* is executed
4. The call is routed to the call group *Sales*
5. In case no one responds within 20 seconds, another Dialplan procedure, *Voicemail* is executed

Edit main Visual Developer

Description External dialplan

04611715110

- 1 Mobility extension I default Set Options Set
- 2 Verify timetable if matched Closed Procedure Closed (office i) Number default Set
- 3 Jump to if switch is Voicemail_swit Procedure Voicemail (Voic) Number default Set
- 4 IVR IVR

Add application

04611715111

- 1 Verify timetable if matched Closed Procedure Closed (office i) Number default Set
- 2 Jump to if switch is messagerie Procedure Voicemail (Voic) Number default Set
- 3 Call group Tech_Support Message for operator Timeout 20 Music on hold class default
- 4 Jump to Procedure Voicemail (Voic) Number default Set

Add application

04611715112

- 1 Verify timetable if matched Closed Procedure Closed (office i) Number default Set
- 2 Jump to if switch is Voicemail_swit Procedure Closed (office i) Number default Set
- 3 Call group Tech_Support Message for operator Timeout 20 Music on hold class default
- 4 Call group Sales Message for operator Timeout 20 Music on hold class default
- 5 Jump to Procedure Voicemail (Voic) Number default Set

Add application

Add number

Included procedures (analyzed after the content of this procedure)

Save Cancel

Wildix WebRTC solution

Wildix WebRTC Kite

Wildix Kite is a professional solution for business communication based on the WebRTC technology that brings Unified Communications to the corporate website.

Features supported:

- Chat / file transfer
- Audio call
- Video streaming
- Desktop sharing

Wildix Kite service allows each PBX user to have a personal Kite link by which he or she can be contacted on the Internet via the browser.

Examples of Kite implementation:

- Contact button on the website (simple HTML template)
- Widget (embedded into the website or into a separate web page)
- HTML email signature with contact button (simple HTML template)

An example of Kite implementation can be found here: www.wildix.com/contacts.

One of the advantages of Kite is that it's fully integrated into the Wildix telephony system:

- Chat requests are managed by PBX users via Wildix Collaboration interface

- Audio calls can be answered from any Wildix devices (WP, W-AIR, mobile apps, Collaboration)
- Wildix Kite uses a separate Dialplan which makes it easy to customize the service
- Chat requests and calls from Kite service can be routed to separate call agents or to call groups

Check Documentation: [Wildix WebRTC Kite Admin Guide](#).

WebRTC-based Wizyconf videoconference

Wildix Videoconference is based on WebRTC technology and Kite solution and allows access for PBX users and external users via a link or a phone call.

Features supported:

- Access for internal and external users via invitation by email, via link, audio call
- Multi user chat, audio and video conference
- Screen sharing
- Document sharing / application sharing / link sharing
- Recording
- Conference scheduling
- Mute/unmute participants
- Dynamic video allocation


Documentation: [Wizyconf Videoconference](#).

Debugging and troubleshooting

Wildix systems offer logging, debugging and troubleshooting possibilities on different levels. In this chapter we will only see the basics.


SSH connection

If your PBX is accessible in the network at the default IP (LAN port) or at the IP released by your DHCP server (WAN port), you can access your PBX using some SSH client to view the logs of the callweaver and to analyse the basic problems with PBX activation, trunk registration, Dialplan operations, impossibility to place calls, ACL permissions etc.

 The admin user can access the Terminal directly from WMS, see chapter [Introduction to WMS \(Terminal\)](#).

To connect via SSH you can connect to the PBX via console (on Windows you can use “putty” or other SSH clients) or click on “terminal” icon in WMS upper menu (“admin” user)

- To analyze call logs: select the entry 1 (Connect to PBX engine)
- To analyze the syslog: select the entry 5 (Open Syslog)
- To start recovery procedure: select the entry 9 (Recover System)

 Important: possibility to run Recovery procedure on Virtual / Cloud systems has been blocked!

- For other advanced operations: select the entry 11 (Shell)

Example:

```

Enter an option (default 11): 1
CallWeaver 5.01.20200604.2-5dd1d5d3 GIT-stable_5_01-5dd1d5d3 - The True Open Source PBX
=====
Running as user 'wms'
Running under group 'wms'
Connected to Callweaver GIT-stable_5_01-5dd1d5d3 currently running on ██████████ (pid = 1670)
== Using SIP VIDEO CoS mark 6
== Using SIP RTP CoS mark 5
-- Executing [500@users:1] NoOp("SIP/448-00000037", "Dialing from 448 to number 500 ")
-- Executing [500@users:1] NoOp("SIP/448-00000037", "Set call class to 'internal'(1)")
-- Executing [500@users:1] NoOp("SIP/448-00000037", "Calltype 'internal'")
-- Executing [500@users:1] NoOp("SIP/448-00000037", "Dst features for active calltype/status - internal/default:
-- MEXT:0 BCF:1(VOICEMAIL) UCF:1(VOICEMAIL) SMSMCN:0 REJECT:0 EMAILMCN:1 FCF:0 TOUT:0 CW:1 MOBCONFIRMATION:0 RING:1(Ring1) ROAD:0")
-- Executing [500@users:1] NoOp("SIP/448-00000037", "Device state for 'SIP/500' is NOT_INUSE")
-- Executing [500@users:1] Dial("SIP/448-00000037", "SIP/500,65,zb(predial^internalcall^1(, <http://127.0.0.1/Ring1.wav;info=internal>,1,,1
710019,false))")
== Using SIP VIDEO CoS mark 6
== Using SIP RTP CoS mark 5
    
```

Dialplan debug

Note: Dialplan debug is always active by default.

Click **Debug** icon in the upper menu of WMS.

Now you can see the basic log of ongoing (section *Active Calls*) or terminated (section *History*) calls, click on a call to view details (in the right part of the screen):

Debug dialplan

Search

Active Calls

Date	From	To
23/06/2020 12:51:26	500	448

Showing 1 to 1 of 1 entries

History

Date	From	To
No data available in table		

Showing 0 to 0 of 0 entries

```

-- Executing [448@users:1] NoOp("SIP/500-00000033", "Dialing from 500 to number 448 ")
-- Executing [448@users:1] NoOp("SIP/500-00000033", "Set call class to 'internal'(1)")
-- Executing [448@users:1] NoOp("SIP/500-00000033", "Calltype 'internal'")
-- Executing [448@users:1] NoOp("SIP/500-00000033", "Dst features for active calltype/status -
internal/default:
MEXT:0 BCF:1(VOICEMAIL) UCF:1(VOICEMAIL) SMSMCN:0 REJECT:0 EMAILMCN:1 FCF:0
TOUT:0 CW:1 MOBCONFIRMATION:0 RING:1(Ring1) ROAD:0")
-- Executing [448@users:1] NoOp("SIP/500-00000033", "Device state for 'SIP/448' is
NOT_INUSE")
-- Executing [448@users:1] Dial("SIP/500-00000033",
"SIP/448,65,zb(predial^internalcall^1(,1,,8553220,false))")
    
```

Trace generation

- Go to *WMS Settings -> Tools and utilities -> Generate trace*

This tool allows generation of a *pcap trace that helps you to debug and analyze eventual problems with VoIP traffic on the PBX or on separate interfaces.

More information: [WMS Settings Menu Admin Guide](#).

Syslog, Reset and recovery of media gateways and phones

VoIP phones reset and recovery: Press the central button of the Navigation keys and hold it for several seconds. For more details read the guide: [How to perform reset and recovery of Start, WorkForce, WelcomeConsole, WP4X0 new generation](#).

Enable remote syslog on Wildix devices: *WMS* -> *Devices*, double click on a provisioned device to edit it and select "Syslog Server" (enter the address of the remote server; it is also possible to enable Remote Syslog without installation of a remote server). Refer to [Remote Syslog Guide](#) for detailed information.

For the information on how to collect syslog from Wildix devices without Remote syslog server, read the guide: [Collecting Syslog from Wildix Devices](#).

ISDN gateways:

1. Connect to the media gateway via SSH (on Windows you can use "putty" or other SSH clients) using the same credentials you used for access to web interface
2. Type "logs on" (at the end of the session, type "logs off")
3. Make a test call

The logs help you to understand eventual issues, here is what happens when a user places an outgoing call to a trunk:

1. PBX receives a request from the user and forwards it to the BRI/PRI gateway
2. The gateway forwards the call to the operator
3. The operator responds to the gateway with the status "Call Proceeding" to confirm the reception of the request
4. The operator responds with the status "Call Progress" to indicate that the call has been routed to the destination
5. The operator responds with the status "Alerting" to indicate that the destination is available
6. The operator responds with the status "Setup Confirm" to indicate that the call has been responded

In case the call could not be connected or the call was hang up by the operator, the media gateway receives the following message: "Unicast RECV Disconnect"

Check the field indicating the reason of the call disconnection, for example: "Cause: Normal call clearing (16)". Check the codes of disconnection reasons: https://en.wikipedia.org/wiki/ISDN_User_Part#Cause_codes

More information on troubleshooting of Wildix Media gateways: [Debugging and troubleshooting of Media Gateways](#).

Other

- *Upper menu* -> *info*: Monit service allows you to check the performance of the system services, CPU, memory usage
- *Upper menu* -> *ports block*: check if any ports needed for remote trunks and calls are not open

PBX access via RS-232 serial port to reset admin password (Hardware PBX)

- Use the RS-232 cable to connect your PC to the serial port of the PBX
- Open the RS-232 terminal (such as PuTTY for Windows or ZetaTerm for Mac) and set up the baud rate to 19200

