

# Administrators Guide

---

## Voice alert



Version: 7.5.x

[SUPPORT@TELISCA.COM](mailto:SUPPORT@TELISCA.COM)  
TEL. +331 4645 0512

## HELP

Open a ticket with your logs on <http://support.telisca.com> for a prompt and efficient response!

Server: MENU>Support>Zip Logs

# Table of content

<b>1</b>	<b>VOICE ALERT PRODUCT DESCRIPTION .....</b>	<b>4</b>
1.1	SERVICES AND FEATURES .....	4
1.2	TRIGGERING .....	4
1.3	TARGET LISTS, DISTRIBUTION MODES.....	4
1.4	REPORTING .....	5
<b>2</b>	<b>ARCHITECTURE .....</b>	<b>7</b>
2.1	SCHEMA AND COMPONENTS.....	7
2.2	CALL MS TEAMS DESTINATIONS.....	7
2.3	SEND TEXT MESSAGES .....	7
2.4	FAULT TOLERANCE.....	7
2.5	REQUIREMENTS .....	8
2.6	NETWORK MATRIX.....	8
2.7	NETWORK MATRIX WITH MICROSOFT TEAMS .....	9
<b>3</b>	<b>VOICE ALERT CONFERENCE MODE (INTERPHONIE) .....</b>	<b>10</b>
3.1	SHORT DESCRIPTION.....	10
3.2	ADHOC CONFERENCE REQUIREMENTS.....	10
3.3	ADMINISTRATION.....	10
3.4	CALLS SCENARIOS' DESCRIPTIONS.....	10
3.4.1	<i>Alert triggered and conference created .....</i>	<i>11</i>
3.4.2	<i>One of the participant hangup while conference started.....</i>	<i>11</i>
3.4.3	<i>One of the participant calls the alert CTI Port while the conference is started.....</i>	<i>11</i>
3.4.4	<i>One of the participant of the conference answers another calls .....</i>	<i>11</i>
3.4.5	<i>The initiator hang-ups before any participant has answered.....</i>	<i>11</i>
3.4.6	<i>Participant not authorized to trigger a conference.....</i>	<i>11</i>
<b>4</b>	<b>MS TEAMS AZURE GATEWAY INTEGRATION .....</b>	<b>12</b>
4.1	GATEWAY URL.....	12
4.2	AZURE .....	13
4.2.1	<i>App registration.....</i>	<i>13</i>
4.2.2	<i>Authentication.....</i>	<i>14</i>
4.2.3	<i>Scopes.....</i>	<i>14</i>
4.2.4	<i>Secret.....</i>	<i>15</i>
4.3	MS TEAMS BOT REGISTRATION.....	15
4.3.1	<i>Create the bot.....</i>	<i>15</i>
4.3.2	<i>Call registration .....</i>	<i>16</i>
4.3.3	<i>Miscellaneous.....</i>	<i>17</i>
4.4	MICROSOFT TEAMS ADMIN CENTER .....	18
4.4.1	<i>Publish the bot.....</i>	<i>18</i>
4.4.2	<i>Create a phone number .....</i>	<i>19</i>
4.5	PHONE NUMBER AND POWERSHELL .....	20
4.5.1	<i>Application Instance creation.....</i>	<i>20</i>

4.5.2	<i>Phone license</i> .....	20
4.5.3	<i>Associate the phone number to the bot – Calling Plan</i> .....	21
4.5.4	<i>Associate the phone number to the bot – Direct routing</i> .....	22
4.6	TELISCA ADMINISTRATION .....	22
4.6.1	<i>Global configuration Parameters tab</i> .....	22
4.6.2	<i>Global configuration Azure tenant tab</i> .....	22
<b>5</b>	<b>VOICE ALERT ADMINISTRATION</b> .....	<b>24</b>
5.1	PARAMETERS TAB .....	24
5.2	ENTITIES TAB.....	25
5.3	CONTACTS LISTS.....	27
5.4	CONTACTS .....	27
5.5	BROADCAST LISTS .....	28
5.5.1	<i>CUCM lists</i> .....	28
5.5.2	<i>Global Directory lists</i> .....	29
5.5.3	<i>MS Teams Lists</i> .....	30
5.6	ALERT'S GROUPS.....	30
5.7	ALERTS TAB.....	30
5.7.1	<i>Main parameters to check to create an alert</i> .....	30
5.7.2	<i>Details of parameters</i> .....	31
5.7.3	<i>Audio files definition</i> .....	31
5.7.4	<i>Dry contact input parameters</i> .....	33
5.7.5	<i>Destination lists</i> .....	33
5.7.6	<i>Recycling</i> .....	34
5.8	WEB ALERTS TAB .....	34
5.9	REPORTS .....	37
5.10	DRY CONTACTS/IP PARAMETERS .....	38
5.11	REST API TO TRIGGER AN ALERT.....	41
5.12	SEND SMS.....	42
5.13	SEND FAX .....	42

## 1 Voice Alert Product description

### 1.1 Services and features

Voice Alert is an alert management application based on Cisco Unified Communication Manager and Microsoft Teams. Voice Alert may be used to alert automatically a list of internal or external recipients and play a recorded audio message alert or distribute text messages, with an audible signal and vibration sent to the telephones or MS-Teams users. Voice Alert can also send SMS, emails or Fax and can play audio on IP Speakers.

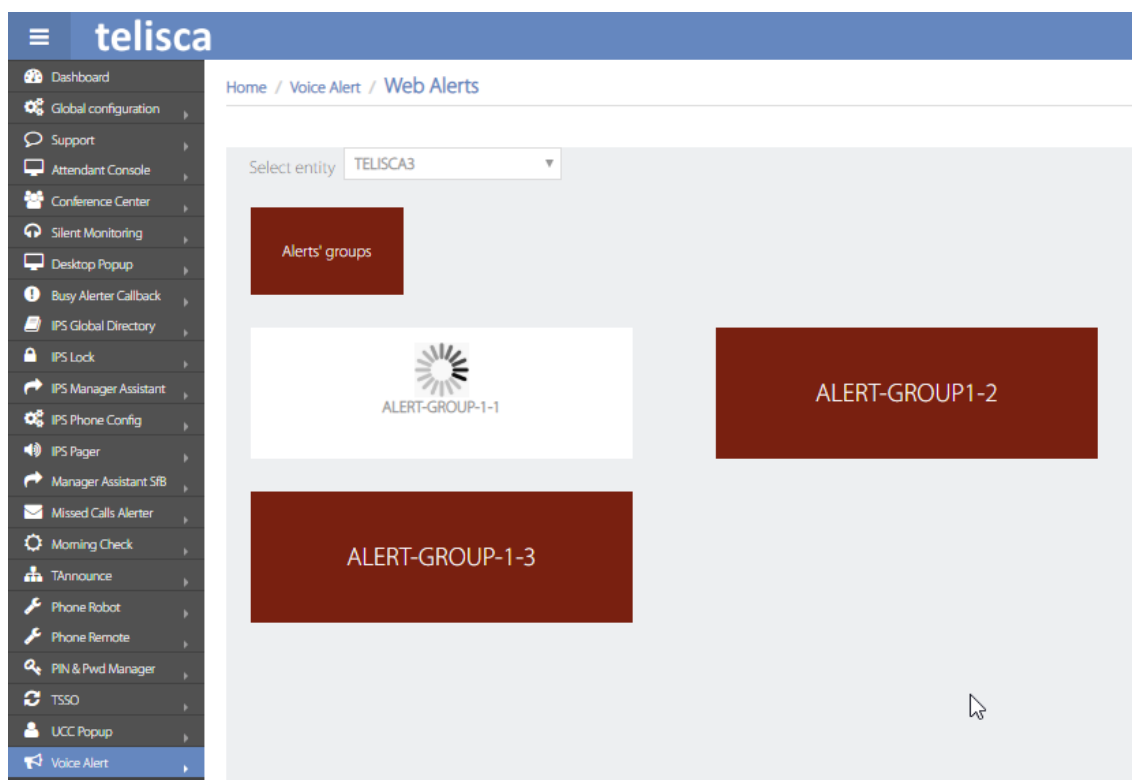
Voice Alert can send broadcast or successive calls/messages and verifies that the call was indeed taken into account.

Voice Alert generates reports that can be sent to supervisors.

### 1.2 Triggering

The alert may be triggered by calling a defined directory number, from an authorized calling number and eventually typing a DTMF code. The alert is selected according to the number dialed (one number per alert), or according to a list of calling numbers. A DTMF code may be required to trigger the transmission.

An authorized user can display a Web Page to start, monitor and stop alerts, organized in alerts' groups.



The alert can also be triggered by a dry contact, such as by pressing a button. The interface is accomplished either by a dry contact/IP converter (ControlByWeb), or by an ATA 186/188/190 unit.

The alert can be triggered by an external application:

- By calling an URL, from an authorized calling IP address.
- By creating a text file.

### 1.3 Target lists, distribution modes

The administration is used to define different alerts with a specific audio message, text message, recipients list, distribution and recycle modes.

The recipient list can be defined as:

- A list of contacts (with several directory numbers)
- A list of directory numbers,
- A list of IP Phones,
- A selection of device pool,
- A selection of Location,
- A selection of Calling Search Space,
- A selection of IP address prefixes
- A list of MS-Teams URI
- A selection of any directory (Voice Alert includes IPS Global Directory sources).

The list is browsed in order to mix the different destinations with different selection criteria (for example to avoid calling all building A, then building B).

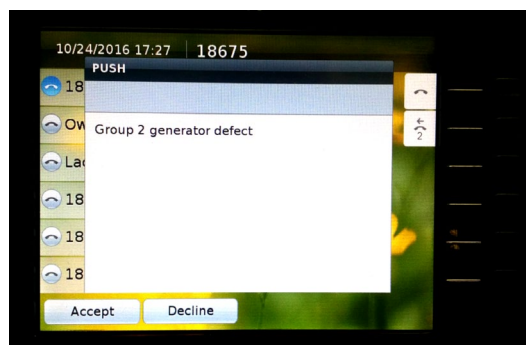
It is possible to associate two list types for example one for internal IP phone and a liste of directory numbers for mobile phones.

Different distribution modes are available:

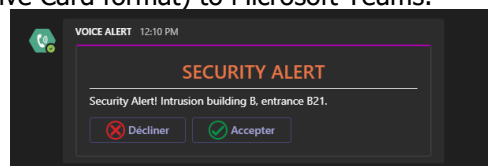
- Broadcast: recipients are called simultaneously,
- Successive: the numbers are called in order. As soon as a number correctly takes the call, the alert is terminated.
- Broadcast on contact, successive on directory numbers per contact.
- Stop on first accepted alert or not.
- If the dialed number is busy, it is possible to interrupt the call in progress in order to send the alert,
- Numbers transferred to external lines are not called.

The alert can be considered as accepted, when:

- The call is answered before a defined response delay,
- The communication duration reaches a minimum length defined,
- The recipient has entered a DTMF validation code.
- The text notification is confirmed via the screen of the IP Phone.



- A text notification (in Adaptive Card format) to Microsoft Teams.



When the call is not answered or not listened 'adequately', the call is recycled several times after a defined delay.

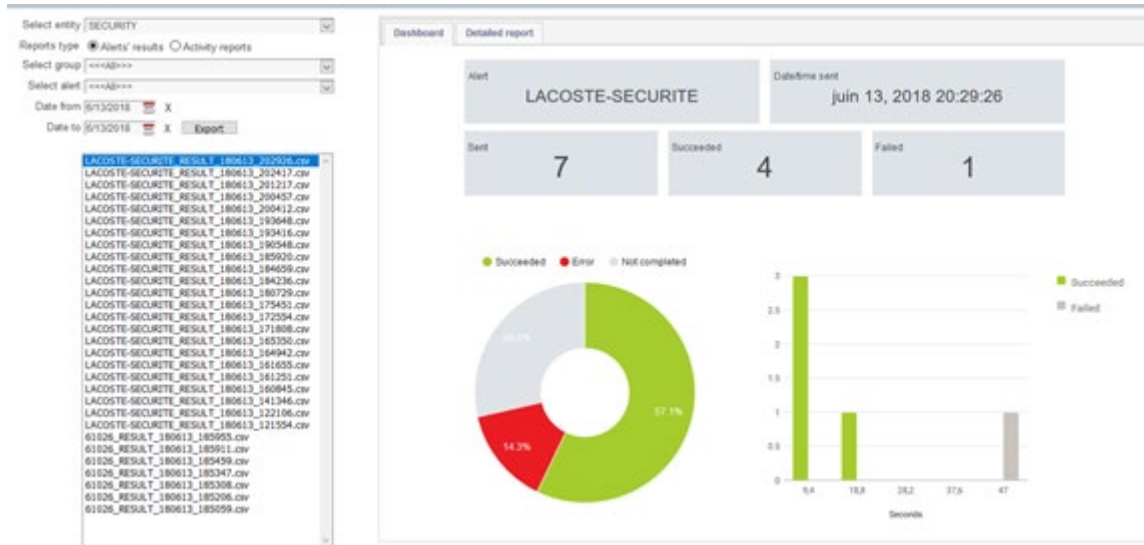
An output dry contact can be closed, during the duration of the alert or when started or when at least one destination user has acknowledged the call.

## 1.4 Reporting

A report is generated to control the alerts triggered. It provides information on who has raised the alert, who has been called and who has listened/view/accepted the alert. The result of the call for each destination is also available, providing status and failed cause.

The Alert report can be exported or sent by email to supervisors' address list.

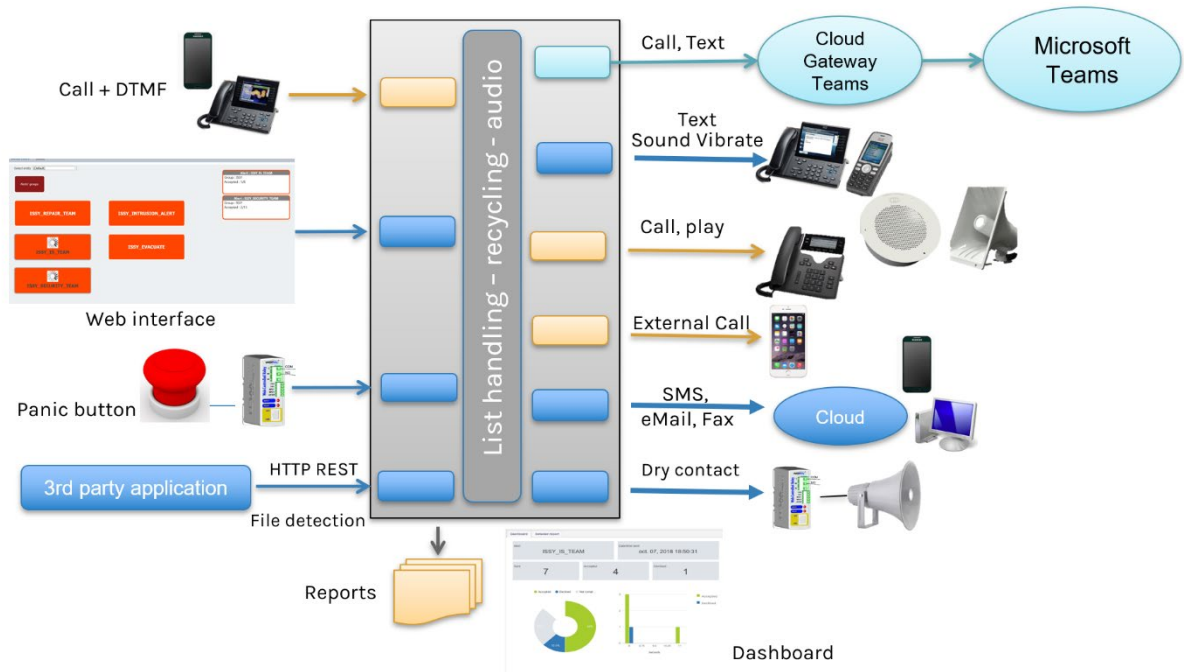
A dynamic Dashboard can be displayed to analyze the reports.



## 2 Architecture

### 2.1 Schema and components

Alerts can be triggered by calling a number + pressing DTMF, via a Web interface, by dry contact or by a secured API...



Voice Alert includes an audio server that can play up to 500 simultaneous audio messages. The audio messages are loaded from audio files (.wav) and converted automatically to the right format. It is also possible to enter a text which is converted to audio by Text to Speech.

Voices:

Speech text:

Audio file:    
 c:\inetpub\wwwroot\IPSCFG\data\audio\audio\_41.wav   
[Download](#)

IPS Administration creates also the adequate number of alert's CTI ports that may be called to trigger the alerts. Depending of the entity, different pools of CTI Ports with different Device Pool, Partition and Calling Search Space can be created.

### 2.2 Call MS Teams destinations

Calls and chat are sent to MS-Teams users through a Cloud base module which also handles recycling and calls reporting. Voice Alert distributing server communicates with the Voice Gateway by HTTPS through a REST API.

Voice Alert sends call requests that are communicated to MS Teams Graph APIs to generate call to the destination. The Gateway can also play the audio messages. The Gateway returns call handling events (connected, DTMF accepted, not answered, error/busy, ...) to Voice Alert which handles the recycling and reporting.

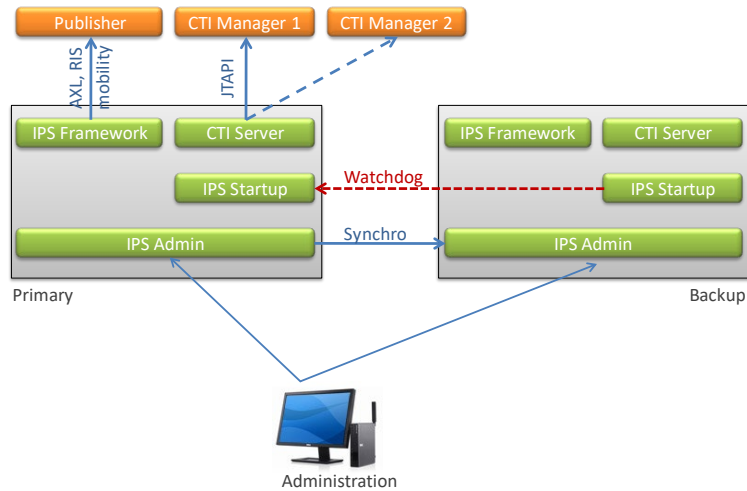
### 2.3 Send text messages

Voice Alert can also push a text message on a Cisco IP phone, vibrate a Wifi IP phone, send an email, a SMS or Fax, send a text message with Adaptive Card to Microsoft Teams.

### 2.4 Fault tolerance

Voice Alert may function in fault tolerance mode. Voice Alert supports an automatic reconnection to a backup CTI Manager and publisher (for AXL read and Serviceability queries).

Voice Alert can also be installed on replicated servers with the additional Hot Standby module. In this case, both configurations are synchronized. The backup server monitors the primary server. If a failure is detected the backup server becomes primary, connects himself to the CTI Manager and registers again the CTI ports used to handle the alerts.



## 2.5 Requirements

Supported Cisco CUCM:

- CUCM version 10.5, 11.5, 12, 12.5, 14

**Available on private cloud company.telisca.cloud**

**On premise installation:**

Windows servers supported:

- Windows Server 2012 R2 Essentials or Standard
- Windows Server 2016 Essentials or Standard
- Windows Server 2019 Essentials or Standard
- Windows Server 2022 Standard

- Minimum configuration: 1 vCPU, 4GB RAM, 70GB disk
- Any virtual machine VMware vSphere, HyperV or Cisco UCS, Microsoft Azure
- Support dry Contact to IP: ControlbyWeb WebRelay (1 port), X-310 (4 ports) or X-332 (16 ports).
- Support Microsoft Teams Graph APIs.
- Calls/Text MS-Teams destinations through a Cloud based Gateway
- Send email by SMTP,
- send SMS by Cloud gateway,
- send fax by Cloud gateway (email with fax destination in email address).

## 2.6 Network matrix

Source	Destination	Protocol	Port
Administration web page	telisca server	HTTPS	443
telisca server	CUCM Publisher	HTTPS	8443
telisca server	CUCM CTI Manager	JTAPI	2748
telisca server	IP Phone, Jabber	RTP	24576 - 32768
Dry Contact-to-IP	telisca server	HTTP	8081
telisca server	eMail Server	SMTP	25, 587
telisca Server (Fault Tolerant)	telisca Server (Fault Tolerant)	HTTPS	443



## 2.7 Network matrix with Microsoft Teams

Source	Destination	Protocol	Port
Administration web page	telisca server	HTTPS	443
Administration web page	telisca server (MS Teams Gateway)	HTTPS	8544
MS Teams Gadget	telisca server	HTTPS	443
telisca server	Microsoft (Graph, Azure, ...)	HTTPS	443
Microsoft Graph	telisca Server	HTTPS	8544
telisca Server (Fault Tolerant)	telisca Server (Fault Tolerant)	HTTPS	443

### 3 Voice Alert conference mode (Interphonie)

#### 3.1 Short description

Voice Alert can be used to create automatically a conference with the destinations of the alert. The destination list should be a list of directory numbers.

To trigger the alert/conference an authorized user calls the Alert CTI Port, for example by pressing a speed dial button on a phone or by clicking on a number in the buddy list of Jabber. If a list of authorized number has been defined, the calling number must be in this list, otherwise all destination numbers set are authorized.

As soon as the participants answer the alert call, from a dial CTI Port, they are redirected to the alert CTI port and added to the conference.

Depending of the option, when the initiator drops the call while in conference, the conference is dropped for all the participants.

#### 3.2 Adhoc conference requirements

The conference is created using ad'hoc conference CUCM resources.

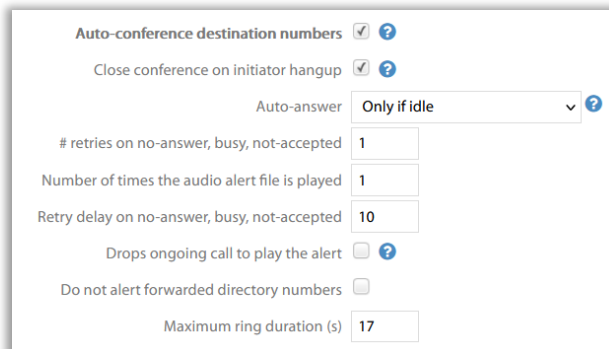
When using Software conference resource, the limitation is 32 participants. As the alert CTI port is part of the conference, only 31 users can be connected together.

When using hardware conference resource, the maximum number of participants is restricted to the hardware used.

The conference resource is defined by the Media resource associated to the device pool defined in telisca Administration for the Alert CTI Ports.

#### 3.3 Administration

The conference mode is defined in the alert definition, 'Recycle & treatments' tab.



Auto-conference destination numbers	<input checked="" type="checkbox"/>	<a href="#">?</a>
Close conference on initiator hangup	<input checked="" type="checkbox"/>	<a href="#">?</a>
Auto-answer	Only if idle <a href="#">?</a>	
# retries on no-answer, busy, not-accepted	1	
Number of times the audio alert file is played	1	
Retry delay on no-answer, busy, not-accepted	10	
Drops ongoing call to play the alert	<input type="checkbox"/>	<a href="#">?</a>
Do not alert forwarded directory numbers	<input type="checkbox"/>	
Maximum ring duration (s)	17	

You can define if the conference closes when the initiator hang-ups. Otherwise, the conference remains open until they are only one participant connected.

You can auto-answer the call from the dial CTI Ports and then create the conference automatically. If the alert is not too urgent, it may be better to avoid the auto-answer if the destination is already online, otherwise the other party is set on hold and if the destination of the alert wants to permute to the other party, he will put the conference on hold.

#### 3.4 Calls scenarios' descriptions

Here are the different calls scenarios supported.

A is the alert CTI Port number.

P1, P2, P3 are call initiator and participants.

P1 is authorized to trigger the alert, P2 & P2 are in the alert's destination list.

### 3.4.1 Alert triggered and conference created

P1 calls A, an 'In progress audio message' is played.  
Dial CTI Ports call P2 and P3.  
P2 answers  
Audio message is stopped  
P2 is redirected to A which answers and creates a conference.  
P3 answers  
P3 is redirected to A which answers and creates a conference.

### 3.4.2 One of the participant hangup while conference started

P2 or P3 hang-ups, the conference continues

P1 hang-ups

If option drop conference on initiator hang-up

Conference is dropped (and alert terminated)

If P1 calls back the Alert CTI Port while the conference is started, he joins again the conference. But it does not trigger an alert again, so the participants which did not answer previously are not called.

If P1 or P2 or P3 hang-ups, and only one participant remains in the conference, the conference is dropped and the alert terminated.

### 3.4.3 One of the participant calls the alert CTI Port while the conference is started

If conference is started and one of the participants, defined in the destination list or authorized triggering list, calls the Alert CTI Port, then he joins immediately the ongoing conference.

*Note: If the initiator has dropped the call but the option to drop the conference on initiator hang-up is not set, when he can come back to the conference by calling again the Alert CTI Port. He will join immediately the remaining participants; however, it will not call other participants in the list.*

### 3.4.4 One of the participant of the conference answers another calls

If the participant of the conference supports two calls, he may receive another call inbound call while in conference. He should not answer the call while in conference otherwise he will put the conference call on hold and other participants to the conference will hear the MOH audio.

Instead, he can hang-up the conference call, answer the urgent incoming call, and call the Alert CTI Port to join the conference again.

*Note: If the participant calls back the dial CTI Port which has called him initially to join the conference, he will not join again the conference.*

### 3.4.5 The initiator hang-ups before any participant has answered

If this case, the alert is stopped, the dial CTI ports will stop ringing the destination list, the alert is terminated.

### 3.4.6 Participant not authorized to trigger a conference

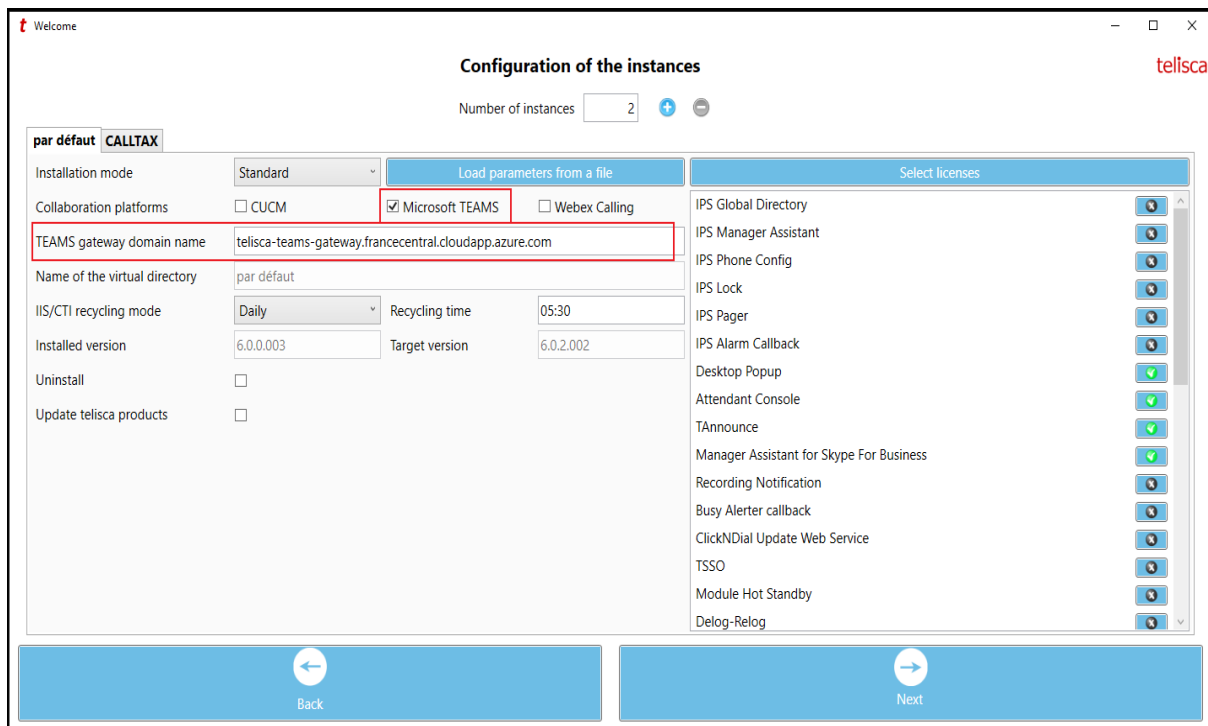
When the user calling the alert CTI Port is not in the authorized number list, the 'Not authorized' audio message is played.

If a conference has already started, and a user not authorized to trigger the alert, but is in the destination list, calls the alert CTI Port, then he joins immediately the conference.

If a conference has already started, and a user not authorized to trigger the alert and not in the destination list, calls the alert CTI Port, then the CTI Port does not answer.

## 4 MS Teams Azure Gateway integration

### 4.1 Gateway URL



The gateway is installed by the telisca setup. During the installation of an instance if you choose the Microsoft TEAMS collaboration platform, the TEAMS gateway domain is prompted. This is the domain name of the server on which you install the setup. You will need a valid certificate for this domain name.

Depending on the instance, two ports will be provided to the gateway service. A public port, used to communicate with the cloud Microsoft. A private port, used to communicate with other telisca modules.

Here is the ports' list:

	PUBLIC HTTPS port	PRIVATE HTTPS port
Tenant 1	8544	8644
Tenant 2	8545	8645
Tenant 3	8546	8646
Tenant 4	8547	8647
Tenant 5	8548	8648
Tenant 6	8549	8649
Tenant 7	8550	8650
Tenant 8	8551	8651
Tenant 9	8552	8652
Tenant 10	8553	8653
Tenant 11	8554	8654
Tenant 12	8555	8655
Tenant 13	8556	8656
Tenant 14	8557	8657

Tenant 15	8558	8658
Tenant 16	8559	8659
Tenant 17	8560	8660
Tenant 18	8561	8661

Finally, the public gateway URL will be: <https://<TEAMS gateway domain name>:<TEAMS gateway HTTPS public port>>

On the other hand, the private gateway URL will be <https://<TEAMS gateway domain name>:<TEAMS gateway HTTPS private port>>

## 4.2 Azure

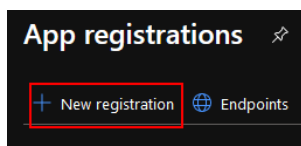
Here is the description of the process to integrate Voice Alert MS Teams gateway with Microsoft Azure.

### 4.2.1 App registration

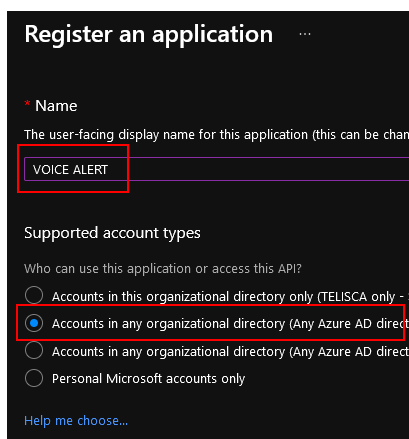
Go to app registrations, on the azure portal

[https://portal.azure.com/#blade/Microsoft\\_AAD\\_RegisteredApps/ApplicationsListBlade](https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade) and login with your Microsoft credentials.

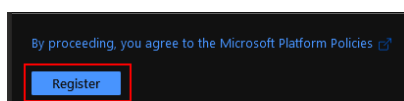
Click on the "New registration" button.

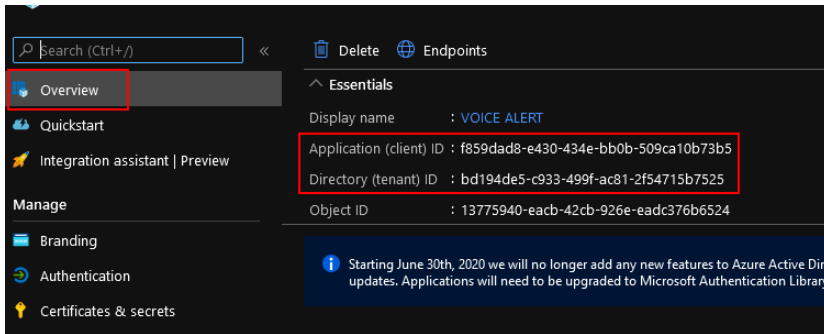


Then fill in the fields as follows.



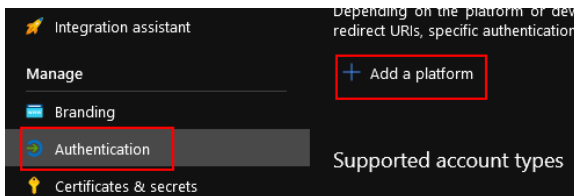
Click on the "Register" button at the bottom of the page and save the "**Application (client) ID**" for later. Do the same with the "**Directory (tenant) ID**".



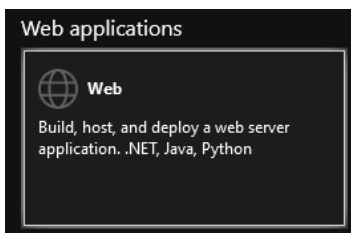


## 4.2.2 Authentication

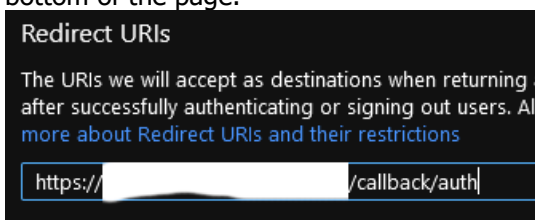
Go to "Authentication" and then to "Add a platform".



Select "Web".

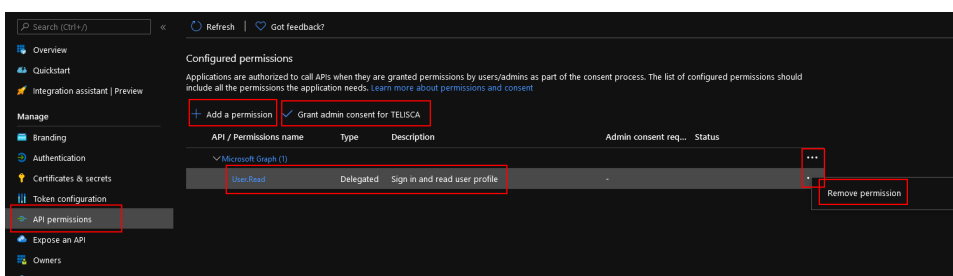


In the redirection url, concatenate the private gateway url with /callback/auth, then click on "Configure" at the bottom of the page.



## 4.2.3 Scopes

On "API permissions" tab, remove the User.Read scope.



Click on the "Add a permission" button then select "Microsoft Graph", then "Application permissions".

Depending on the kind of alert you want to perform (calling and/or messaging alert) select the following permissions:

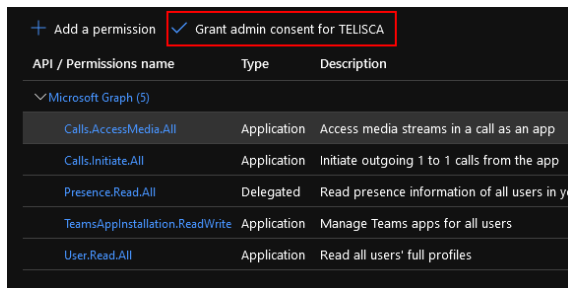
- Calls.Initiate.All [CALLING]
- Calls.AccessMedia.All [CALLING]
- TeamsAppInstallation.ReadWriteForUser.All [MESSAGING]
- User.Read.All [BOTH]

Then, click on the "Add permissions" button.

Click again on the "Add a permission" button then select "Microsoft Graph", then "Delegated permissions". Select this time :

- Presence.Read.All [CALLING]

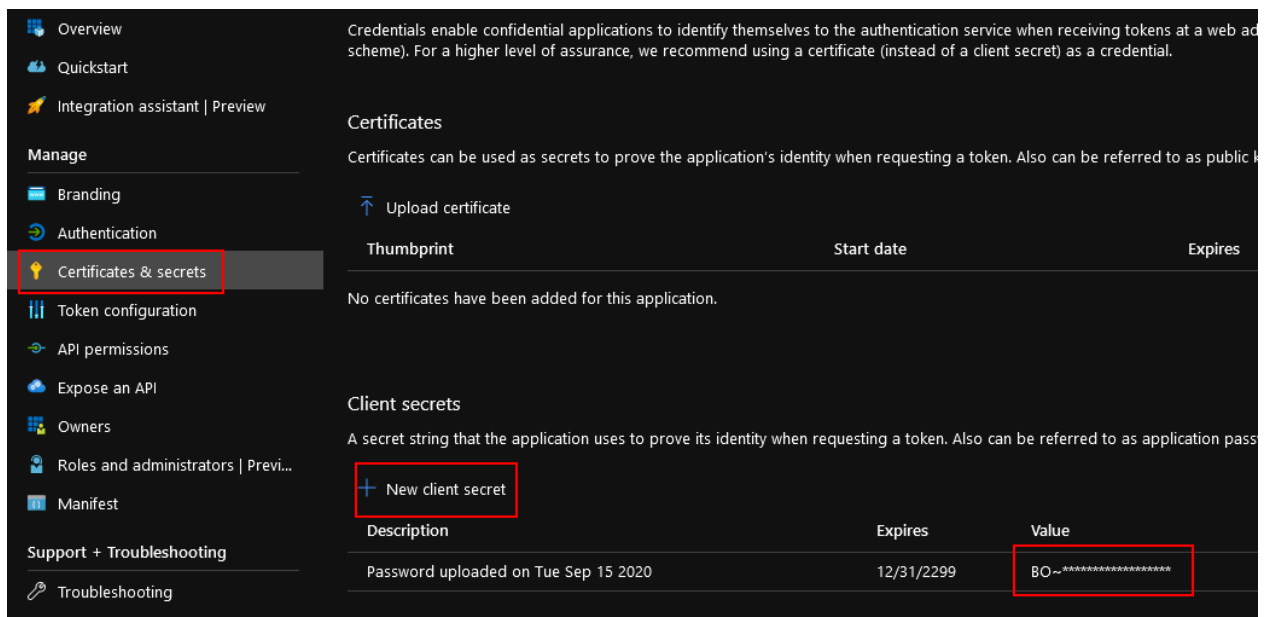
Then click on the "Add permissions" button. Finally, grant the admin consent.



#### 4.2.4 Secret

On "Certificates and secrets" tab, click on 'New client secret' and choose an expiration delay.

Save the value of the secret ("Application password") for later.



### 4.3 MS Teams Bot registration

Voice Alert uses an MS Teams Bot to call the destination.

#### 4.3.1 Create the bot

Go to the following URL <https://portal.azure.com/#create/Microsoft.BotServiceConnectivityGalleryPackage>.

Define a handle, it should be as "VCEALERT\_HANDLE\_NAME\_OF\_YOUR\_COMPANY".  
 In messaging endpoint, only if you want to send messaging alerts, put the public url of the gateway ([as shown here](#)), concatenated with "/callback/message".  
 Turn Application Insights off.  
 Fill-in the remaining fields.

Then, link this bot registration to the azure application created previously by clicking on the "Microsoft App ID and password" button followed by the "Create New" button.

Fill in the fields with the [application ID](#) and the [application secret](#). Click on the "OK" button then on the "Create" button, both at the bottom of the page.

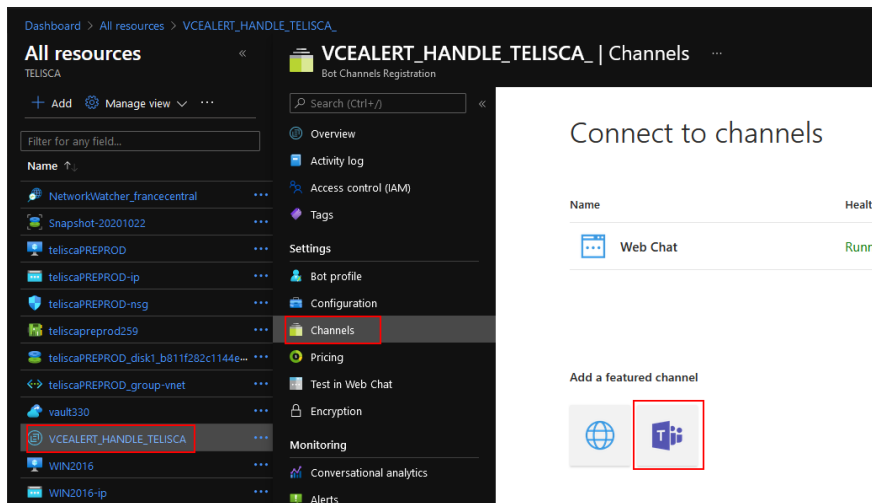
## 4.3.2 Call registration

*This step is required only if you want to perform calling alerts.*

After a while (one or two minutes) go to the "All resources" page (<https://portal.azure.com/#blade/HubsExtension/BrowseAll>) and find the freshly created bot handle.



Go to the 'Channels' tab then clicks on the Microsoft Teams icon.



Go to the calling tab, check the "Enable calling" checkbox.

### Calling [Learn more](#)

These settings determine whether Calling is enabled for your bot, and if enabled, whether IVR functionality or Real Time Media functionality is to be used.

#### Calling

Enable calling

These settings determine whether Calling is enabled for your bot. Note that some Calling features require elevated permissions from an organization's Teams Administrator. To add permissions, go to your bot in the Application Registration Portal, locate the Microsoft Graph Permissions section, and then add the permissions that your app requires.

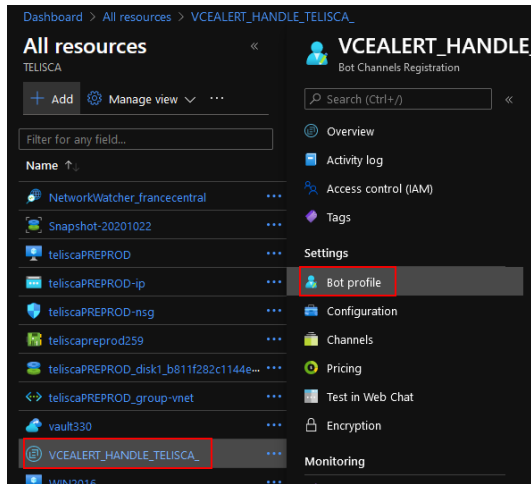
Webhook (for calling)

Then enter the following webhook: the public url of the gateway ([as shown here](#)), concatenated with "/callback/call".

Click on the "Save" button and accept the terms of agreement.

### 4.3.3 Miscellaneous

Go to the bot profile tab.



Upload a custom icon, or the one provided with the [telisca manifest](#). This icon will be displayed in the call popup presented to an alerted user.

Put a DisplayName like "VOICE ALERT".

Click on the "Apply" button at the bottom of the page.

## 4.4 Microsoft Teams admin center

### 4.4.1 Publish the bot

*This step is required only if you want to perform messaging alerts.*

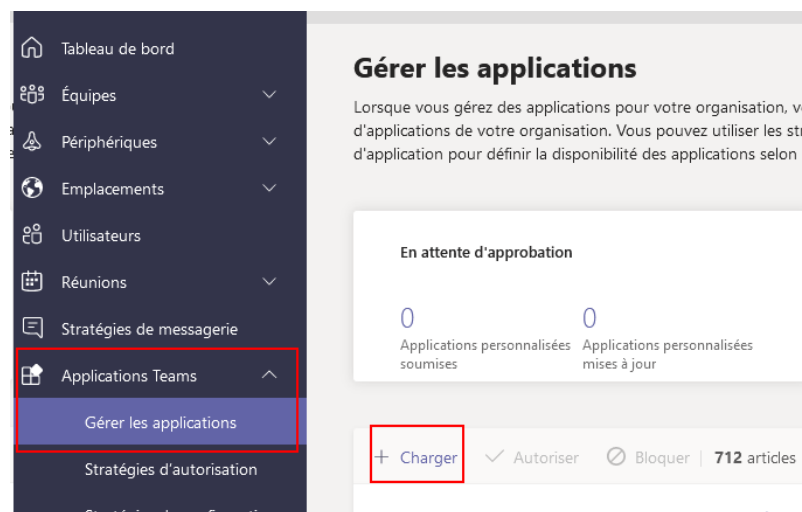
Unzip the package manifest.zip provided by telisca.

Change the manifest.json file by replacing the "id" and "bot-id" properties with the "Application (client) ID" you saved previously.

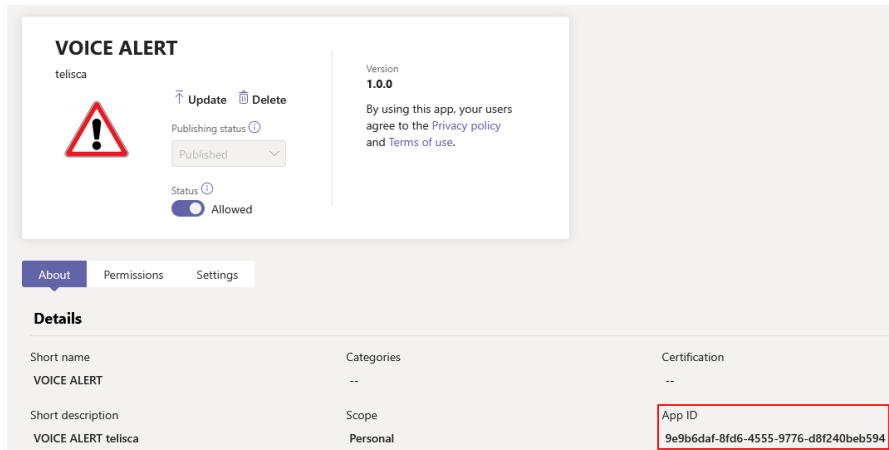
Zip the manifest.json and the two icons (or two other icons of your choice) into a new manifest.zip file.

Go to the following url <https://admin.teams.microsoft.com/policies/manage-apps>.

Click on the "Upload" button and upload the archive.



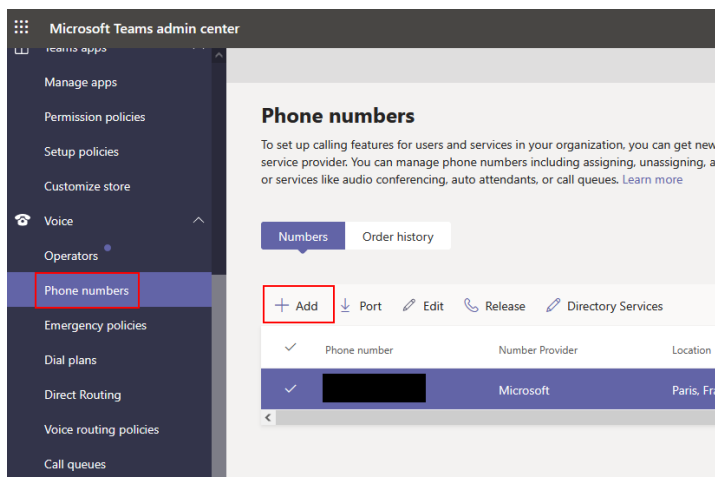
Search for the app "VOICE ALERT" and click on it. This will give you the "Application id (catalog)" and keep it for the next steps.



## 4.4.2 Create a phone number

*This step is required if you want to perform calling alert on PSTN numbers, with a calling plan.*

Go to the following url <https://admin.teams.microsoft.com/phone-numbers>. Then Click on the "Add" button.



Fill in the fields. Be sure to put "Call queue" on the "Number type" field. Then click "Next".

**VOICE\_ALERT\_ORDER**

Used for VOICE ALERT bot in order to make PSTN cal

**Location and quantity**

Country or region  
France

Number type  
Call queue (Toll)

Quantity  
1

City  
Paris

Area code  
188

Then, follow the instructions to confirm the creation of the new phone number.

## 4.5 Phone number and Powershell

*This step is required if you want to perform calling alert on phone numbers (opposed to alert on UPN).*  
Here are the additional steps to associate a phone number to the bot.

### 4.5.1 Application Instance creation

Open a new powershell command prompt window.  
Import the module MS-TEAMS

```
Import-Module MicrosoftTeams
```

Connect to your azure tenant as an administrator

```
$cred = Get-Credential  
Connect-MicrosoftTeams -Credential $cred
```

Create an application instance, where <APPLICATION\_CLIENT\_ID> has to be replaced by the "**Application (client) ID**" you saved [here](#)

```
New-CsOnlineApplicationInstance -UserPrincipalName voicealert@telisca.com -ApplicationId  
<APPLICATION_CLIENT_ID> -DisplayName "VOICE ALERT"
```

Save the ObjectId of the application instance created. (Application instance ID)

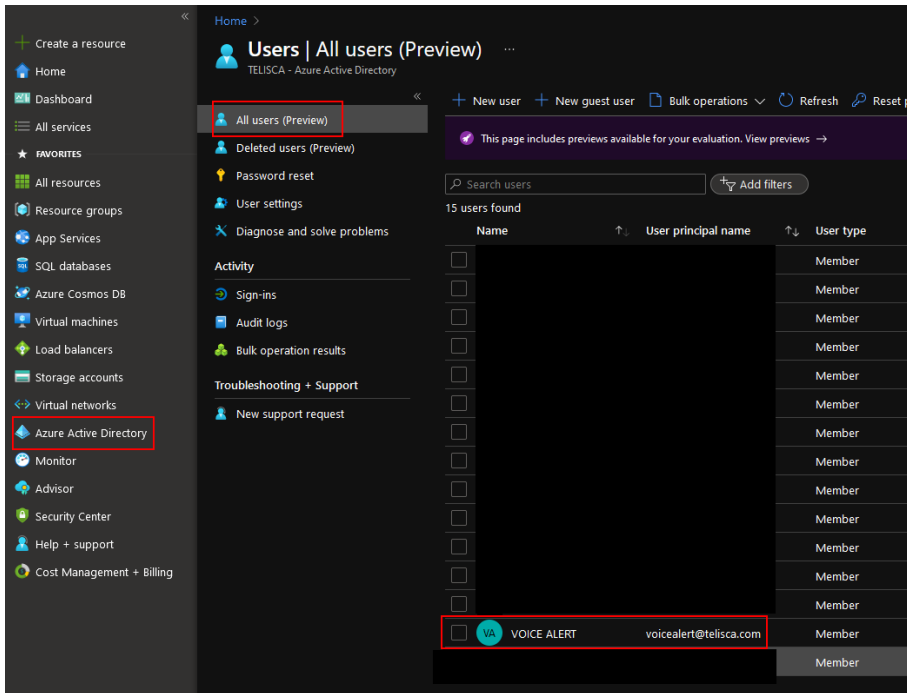
```
RunspaceId :  
ObjectId :  
TenantId :  
UserPrincipalName :  
ApplicationId :  
DisplayName : VOICE ALERT  
PhoneNumber :
```

Now, synchronize it.

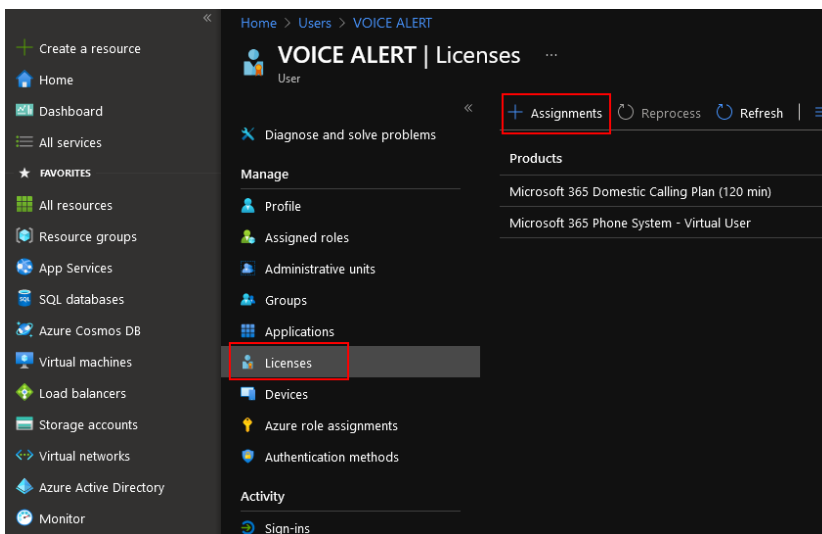
```
Sync-CsOnlineApplicationInstance -ObjectId <OBJECT_ID>
```

### 4.5.2 Phone license

Go back to the azure portal at the following url  
[https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/UsersManagementMenuBlade/MsGraphUsers](https://portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/MsGraphUsers) and select the user newly created.



Go to "Licences", then click on "Assignments".



Finally, add a virtual user license. Add a calling plan license if you are not in "Direct Routing".

### 4.5.3 Associate the phone number to the bot – Calling Plan

*This step is only for "Calling plan" users.*

Go back to the powershell command prompt.

Associate the phone number created previously to the bot.

```
Set-CsOnlineVoiceApplicationInstance -Identity voicealert@telisca.com -TelephoneNumber <PHONE_NUMBER>
```

Finally, synchronize again the application instance.

```
Sync-CsOnlineApplicationInstance -ObjectId <OBJECT_ID>
```

#### 4.5.4 Associate the phone number to the bot – Direct routing

*This step is only for "Direct routing" users.*

Go back to the powershell command prompt.

Associate the phone number created previously to the bot.

```
Set-CsOnlineApplicationInstance -Identity voicealert@telisca.com -OnpremPhoneNumber <PHONE_NUMBER>
```

Finally, synchronize again the application instance.

```
Sync-CsOnlineApplicationInstance -ObjectId <OBJECT_ID>
```

## 4.6 telisca administration

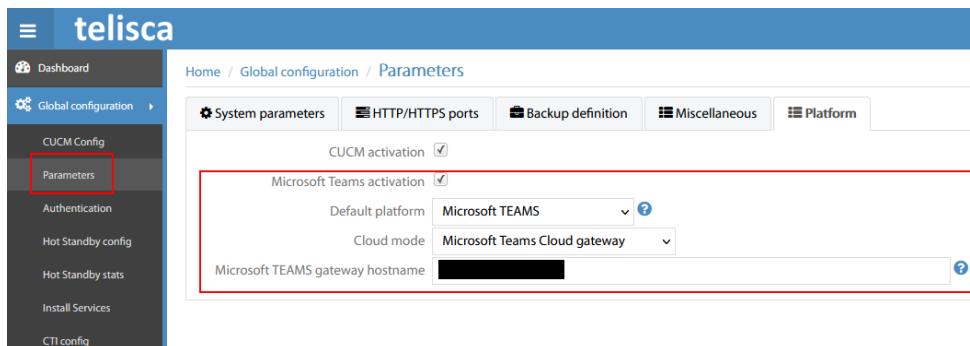
Here are the additional parameters settings for MS Teams Gateway in Voice Alert Administration.

### 4.6.1 Global configuration Parameters tab

Check the "Microsoft TEAMS activation" checkbox.

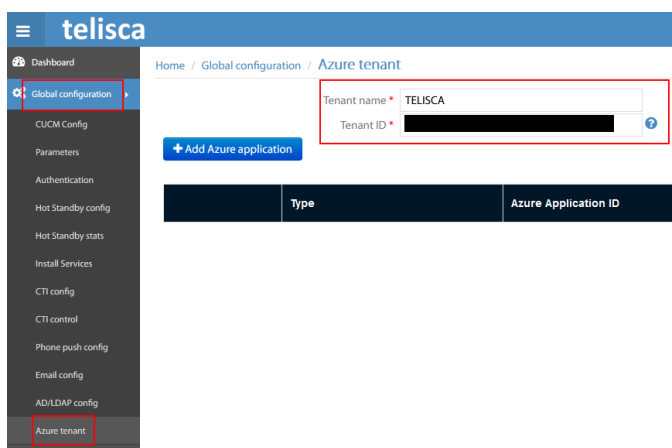
If you have a hybrid configuration (both CUCM and MS TEAMS for instance), the default platform indicates which platform to use by default when there is uncertainty.

Fill in the "Microsoft TEAMS gateway hostname", as soon as the administration web site and the gateway are on separate VM.



### 4.6.2 Global configuration Azure tenant tab

A telisca instance is single tenant. Here is how to set up your Azure tenant.



First of all, fill in the Tenant id field you saved [here](#). Define the name of your tenant also. Then click on "Add Azure application".

Be sure to select VOICE\_ALERT as an application type.

Fill all values you saved previously :  
 The Azure Application ID was saved [here](#)  
 The Application password was saved [here](#)  
 The Catalog application ID was saved [here](#)  
 The Application instance ID was saved [here](#)

Then, click on the "Add" button.

You can add several VOICE ALERT applications. These applications will form a pool for load sharing.

Don't forget to click on the "Save" button at top right of the page when you have finished.

Now click on the "Create application" button. It will create the application on the gateway, and start getting token from microsoft endpoint.

	Type	Azure Application ID	Action	Placeholder user
<a href="#">Edit</a> <a href="#">Delete</a>	VOICE_ALERT	f859dad8-e430-434e-bb0b-509ca10b73b5	<a href="#">+ Create application</a>	
<a href="#">Edit</a> <a href="#">Delete</a>	VOICE_ALERT	9b9cee36-840b-43b8-9b90-c9c30d0be9fa	<a href="#">+ Create application</a>	

Finally, connect a placeholder user to the application. This user will be used to get presence status of other users. It will prompt a Microsoft login popup to connect the user.

	Type	Azure Application ID	Action	Placeholder user
<a href="#">Edit</a> <a href="#">Delete</a>	VOICE_ALERT	f859dad8-e430-434e-bb0b-509ca10b73b5	<a href="#">Update application</a> <a href="#">Remove application</a>	<a href="#">Connect</a>
<a href="#">Edit</a> <a href="#">Delete</a>	VOICE_ALERT	9b9cee36-840b-43b8-9b90-c9c30d0be9fa	<a href="#">Update application</a> <a href="#">Remove application</a>	<a href="#">Connect</a>

A successful connection will result in "OK" button displayed instead of "Connect".

	Type	Azure Application ID	Action	Placeholder user
<a href="#">Edit</a> <a href="#">Delete</a>	VOICE_ALERT	f859dad8-e430-434e-bb0b-509ca10b73b5	<a href="#">Update application</a> <a href="#">Remove application</a>	<a href="#">OK</a>
<a href="#">Edit</a> <a href="#">Delete</a>	VOICE_ALERT	9b9cee36-840b-43b8-9b90-c9c30d0be9fa	<a href="#">Update application</a> <a href="#">Remove application</a>	<a href="#">OK</a>

## 5 Voice Alert Administration

The administration interface is accessible from a web browser at this URL:

Short URL: `http://IP_SERVEUR`  
Full URL: `http://IP_SERVEUR/IPSCFG/admin`

Access by https is also supported.

### 5.1 Parameters Tab

Parameters page from Voice Alert Menu, Parameters item.

Home / Voice Alert / Parameters Cancel Save

Activation
  Trigger modes
  Various
  Advanced

Activate Voice Alert   
 Enable contacts' lists   
 Use Global Directory lists  ?  
 Restrictive access in manager's mode  ?

From this page, you can enable Voice Alert and some of the different modules.

- Activate Voice Alert: Enable Voice Alert (to allow triggering alerts)
- Enable Contacts' lists: If enabled two more tabs CTI Ports are available in Voice alert menu to define Contacts and Contacts' lists.
- Enable IPS Global Directory source lists.

Home / Voice Alert / Parameters Cancel Save

Activation
  Trigger modes
  Various
  Advanced

Trigger alerts by dry contact  ?  
 Trigger alerts by API  ?  
 Trigger alerts on file creation  ?

- Audio trigger by calling a CTI Port: When creating an alert, creates a CTI Port. When calling the CTI Port an audio message is played. It is possible to trigger and alert by entering an optional DTMF code.
- Trigger alerts by dry contact: AN alert can be triggered by closing or opening a dry contact thanks to ControlByWeb dry-contact to IP devices.
- Trigger alerts by API: Alerts can be triggered by calling an http https Get URL.
- Trigger alerts on file creation: Voice Alert detects the creation of a new file and trigger the alert.

Home / Voice Alert / Parameters Cancel Save

Activation
  Trigger modes
  Various
  Advanced

Administrators' email addresses (separated by ,) to send reports  ?  
 Web Alert page's background logo  Aucun fichier choisi ?  
 Fax gateway domain name  ?  
 # columns in 'Launch Alerts' screen  ?

- Set a global administrators' email addresses (separated by commas) that will receive reports. It will be possible also to define supervisors email addresses by entity. SMTP parameters need to be configured in Global Config menu, Email Config tab. See in install and configuration guide IPSCFG\_ADMIN\_EN.pdf.
- It is possible to add a Company Logo to the Web Alert page used by agent to trigger alerts.
- When sending alerts to contacts' list it is possible to enter a fax number for the contacts. Voice Alert can send faxes to contacts, during alerts, using an email to fax gateway. If the contact's fax number is +33146452157, Voice Alert will send an email to the fax number +33146450527@fax-gateway.com, where fax-gateway is the domain name defined here.



Activation
  Trigger modes
  Various
  Advanced

Maximum number of calls per second	30
Input dry contact polling period (ms)	250
Dry contact request timeout (ms)	150
Send RTP stream only on Established	<input checked="" type="checkbox"/>
Reports purge delay	92
Export column's separator	:

- You can define approximately the number of calls per second that will be initiated when starting the alert. This number may be limited by the CUCM cluster performance. When all CTI Ports have been used to dial destinations, the system will then wait for available CTI Ports to dial again.
- Dry contacts can be configured to send an http request on a contact event or can be polled by Voice Alert. You can define here the polling period. Minimum period is 250ms, 500ms is better for ControlByWeb X-332
- When dry contacts are polled you can define the timeout when requesting the timers.
- Voice Alert can push Text notifications to Cisco Phones instead of dialing. Usually the push is executed using CTI API. However, it is possible also to push by HTTP. This request that Cisco Phone Web access is enabled. The authentication URL must be set to query telisca Authentication proxy. Secure on-time password mode should be set (see Push Config page, in Global Config menu, as described in IPSCFG\_ADMIN\_EN.pdf)
- You must then set Push Config parameters, in Global Config menu.
- Force display on: send a command to the phones to light on the screen when pushing notification
- Push first Text, then sound, vibrate, display. In order to provide a workaround, when pushing to the phone the URL to display the notification is an issue, it is possible to push directly the text notification on the phone, then the sound and vibrate command. In this case the message length is limited to 90 characters. This mode can be used to solve issues with some phone's models. They are some limitations:
  - There is no decline SoftKey
  - Text message is limited to 80 characters on some phones,
  - The message cannot clear by itself,
  - It cannot detect the language of the phone.
- Voice Alert will keep the report the number of days defined here
- Export column separator needs to be the one used by you Excel in order to open Excel when double Clicking on the CSV attached to the administrators' email.

## 5.2 Entities tab

Voice Alert support several entities which are used to separate the supervision of Voice Alert for different groups of users using different groups of alerts and different lists.

By default, a '(Default)' entity is created, you can rename it and add some other entities.

	Entity's name	Authorization mode	AD or local Security group	Administrators' Email addresses (separated by ,)	# CTI Ports
<a href="#">Edit</a> <a href="#">Delete</a>	(Default)	Logins' list		jmlacoste@telisca.com	6
<a href="#">Edit</a> <a href="#">Delete</a>	BRIGHTON	Logins' list			5
<a href="#">Edit</a> <a href="#">Delete</a>	ISSY	Logins' list			0
<a href="#">Edit</a> <a href="#">Delete</a>	BRUSSELS	Logins' list			0

After selecting the entity or addin the entity, click on the Edit hyperlink.

- It is possible to define PC Security IP addresses that will be allowed to open the Web Alert page (<http://host/IPSCFG/admin/WebAlert.aspx>) without authentication. This is advised if the security PC needs to have the Web Alert page always opened and ready to send an alert even after an application restart.
- It is possible to define authorized supervisor's login by entity, either by been a member of a Windows or AD Security Group or by entering a list of authorized logins. These can be domain Active Directory logins, if Voice Alert server is part of an Active Directory domain or if the AD query has been defined in Global Config / Parameters and Global Config / AD/LDAP config. It is also possible to define local Login and password separated by a | character.
- Enter a list of supervisor's email addresses that will receive the alerts reports.
- You can define a list of directory numbers that will be alerted event if forwarded.
- It is possible to define a list of directory numbers that will not receive alerts. It can be the security phones' number that should remain available.
- You can define a specific email sender per entity.

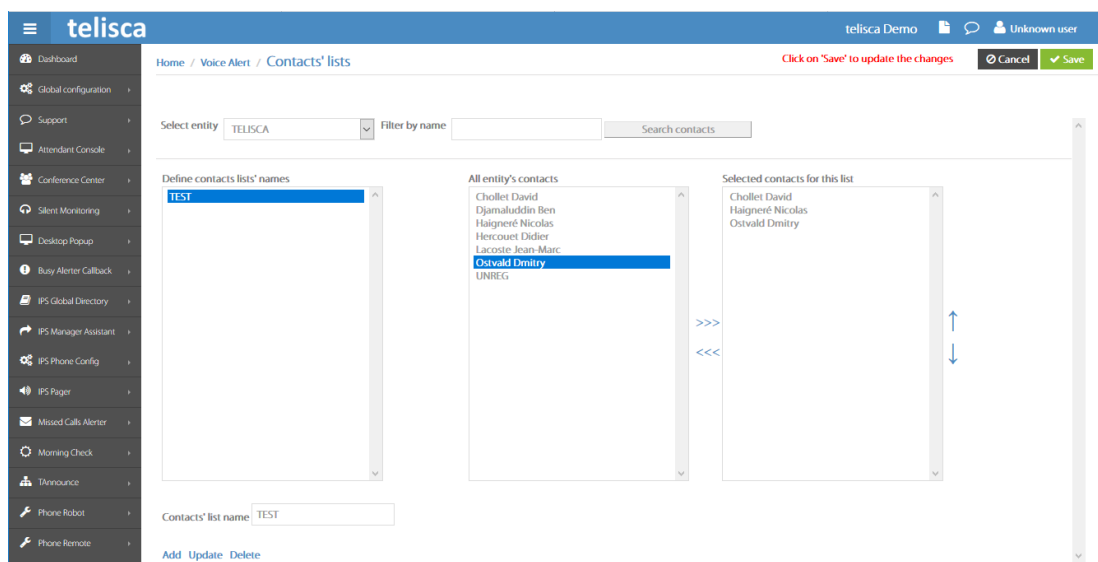
When the entity has been defined two buttons are available to list or create the dial CTI Ports.

- List: To list Dial CTI Ports already created on CUCM.
- Create CTI ports pool to dial destination: To create a pool of CTI Ports on CUCM that will be used to dial destination numbers when triggering an alert.

- Alert CTI ports names prefix: Prefix used to create alert CTI Port
- Base CTI ports directory number: First DN used to create Alert CTI port associated with an alert. This DN is automatically incremented when alerts are created, so a range of DN following this DN must be reserved according to alert numbers. If alert detection mode is "By calling DN", reserved range is not needed.
- The display name is important as it will be the first thing that the user will see when receiving an alert. And it may urge them to answer the call.
- CTI ports Device Pool: Device Pool used to configure Alert CTI ports.
- CTI ports partition: Partition used to configure Alert CTI ports.
- Calling Search Space of the line which should be authorized to call external numbers if required.

## 5.3 Contacts lists

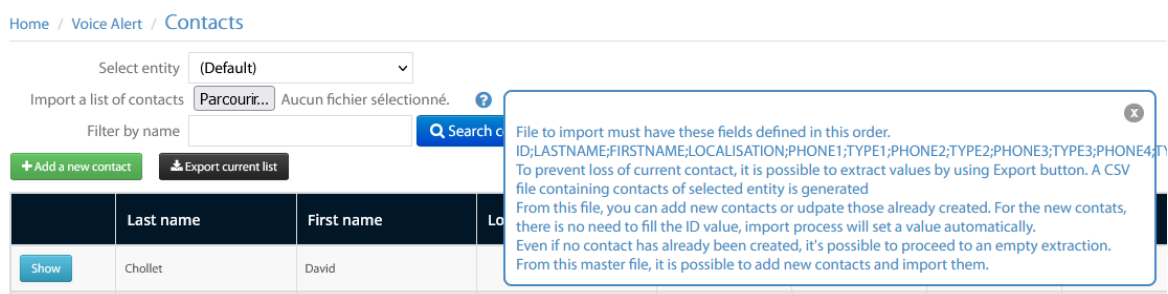
It's possible to define contacts lists grouping persons to contact depending of the kind of alert. This list will be browsed during alert raising. The message will be sent depending of distribution mode to phone numbers of contacts list.



For each entity, several contacts lists can be defined. A list can be imported or exported.

## 5.4 Contacts

Contacts can be defined one by one or imported from a text file using the format described in the hint.



You can define for each contact information as name and also the working hours so that no alert is sent outside of the working hours.

Home / Voice Alert / Contacts Cancel Save

Select entity (Default)   
 Import a list of contacts [Parcourir...](#) Aucun fichier sélectionné.   
 Filter by name  [Search contacts](#)   
 + Add a new contact Export current list 8 filtered contacts

	Last name	First name	Location	Phone #1	Phone #2	Phone #3	Phone #4	Enabled	Start	Stopped
Show	Chollet	David		105016				True	00:00	24:00
Show	Djameluddin	Ben	Brighton	105090	+44798545569			True	00:00	24:00
Show	Haigneré	Nicolas	Issy les Mouligneaux	105099				True	00:00	24:00
Show	Hercouet	Didier	Issy les Mouligneaux	105061				True	00:00	24:00
Show	Lacoste	Jean-Marc	Issy les Mouligneaux	105007				True	00:00	24:00
Show	Ostwald	Dmitry	Moscou	+76549824561				True	00:00	24:00
Show	TEST			105005	105016			True	00:00	24:00

Edit Delete

Active contact

Last name  First name

Location  Email address

Phone #1  Phone #2

Phone #3  Phone #4

Office hour begin  Office hour end

Each contact may have several phone numbers (internal CUCM or externals), SMS, Fax and MS-Teams URIs. See chapters Send Fax and Send SMS for the configuration requirements.

Depending of Alert settings in destination list tab, the numbers/URI are called in top down order or simultaneously.

Identifier Audio trigger mode Trigger audio files Trigger by API Trigger by file Trigger by dry contact input Destination list

Destination list 1 type    
 Contacts lists    
 Destination list 2 type    
 Call distribution mode    
 Contact's numbers distribution    
[Generate IPPhone list relative to this selection](#)

## 5.5 Broadcast lists

From the broadcast lists tab, you can define list of phones or directory numbers that will be used by alerts.

Home / Voice Alert / Broadcast lists Cancel Save

Select entity (Default)

Name	Destination type
IP	IP_ADDRESS_PREFIX
LIST_BY_DN	DN
DP	DEVICE_POOL
GDIR-CONTACTS	GDIR

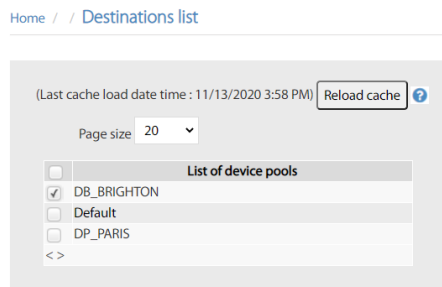
List name    
 Destination list 1 type    
 Source directory    
 Phone/URI column    
 Display name column

Click on Add or an existing list, then on the Edit Hyperlink.

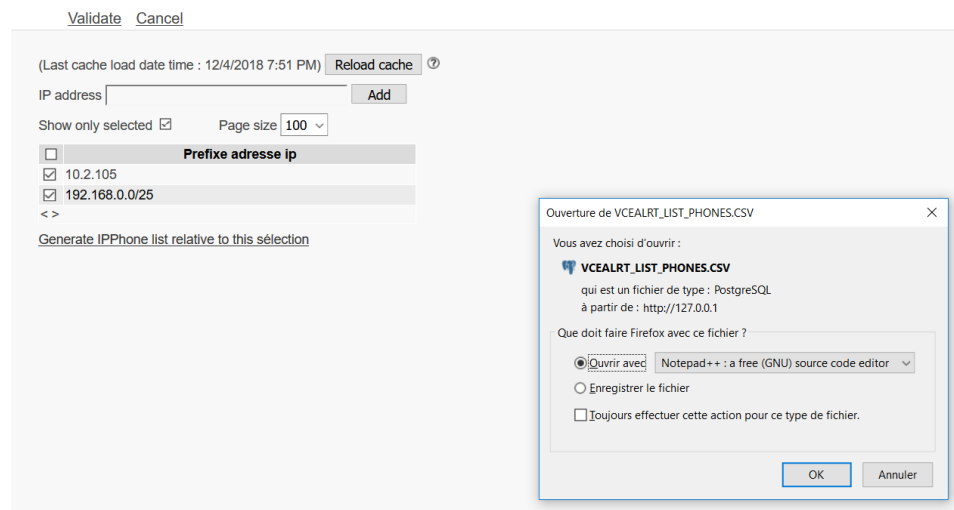
### 5.5.1 CUCM lists

You can define list of directory numbers that can be entered in the multiline text box separated by commas.

You can select all phones, a list of device (phones) or lists by Device pool, Calling Search Space, Location or IP addresses prefixes and subnet.



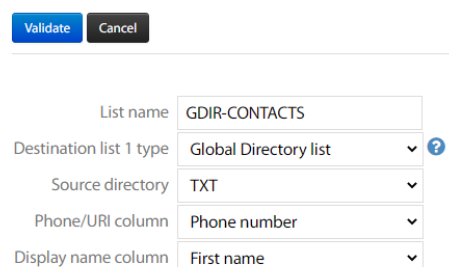
If selecting a list by IP address ranges, you check a IP address prefix from the list or enter a IP address subnet (format y.y.z.t/nn) that will limit to a part of the range depending of the /nn suffix (for example /25 for 126 addresses).



It is possible to generate the list of selected phones, lines and description in a text file and download it to view the selected destinations.

## 5.5.2 Global Directory lists

It is possible to use an IPS Global Directory source as a Voice Alert list. This source directory can be based on Active Directory, LDAP, any database, any file, .... It is possible to apply include and exclude filtering.



You will select the column of IPS Global directory used as a directory number or Microsoft Teams URI.

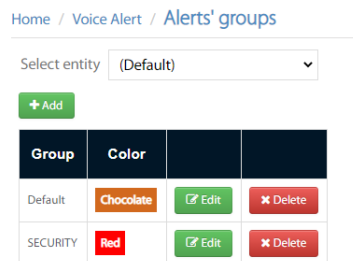
You can also select a field which will contain the name of the contact to ease the reports analysis.

### 5.5.3 MS Teams Lists

For MS Teams, Alerts can be sent to a list of Microsoft Teams URIs separated by commas.

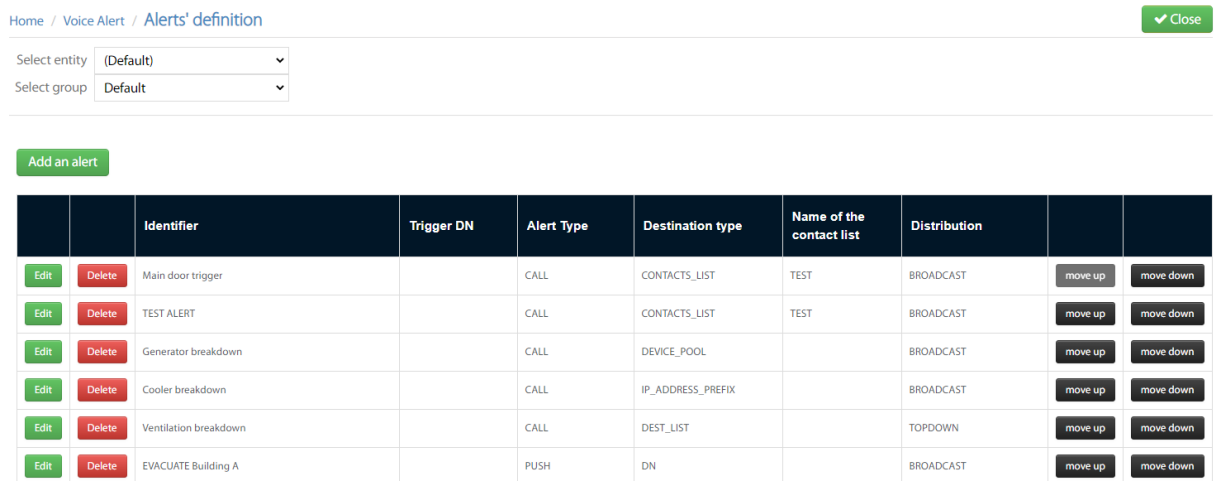
## 5.6 Alert's groups

Different groups of alerts can be created to organize the alerts in the Web Alert page.



## 5.7 Alerts tab

This table displays all alerts of an entity and a group. From here it is possible to add a new one.

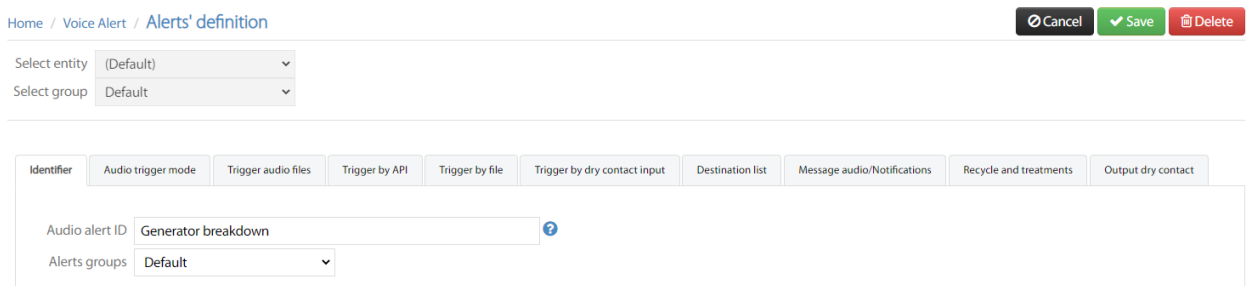


### 5.7.1 Main parameters to check to create an alert

Before create an alert, an entity and a group must be selected. It is possible after to attribute this alert to another group by updating it.

Once alert name has been defined, it is not possible de change it.

Depending of the setting in the parameters tab, several tabs will be available to define the alert.



A **cti port to dial number** is automatically proposed. It is possible to change it but however, it's better to let cti number like this.

**Destination list type:** Contacts list, list of extensions, All phones ...

**Contacts list** need to be selected if destination type is Contacts list.

**Call distribution mode** is the behaviour of alerts sending management: Broadcast, Top Down or broadcast on speakers

**Contact's numbers distribution** is the behaviour of distribution inside list of phones number for a contact, top down or broadcast.

One of the main parameters is **audio alert file**: It is possible to import an already made audio file or to generate in Text to Speech mode.

## 5.7.2 Details of parameters

### 5.7.2.1 Audio alert ID

ID/Name of alert.

### 5.7.2.2 Trigger Mode

- List of authorized calling DN: List of calling authorized to raise alert. If alert detection mode is "by calling DN", this list of calling DN is used to identify alert to raise.
- Can be called only from an internal number: To raise alert only from an internal number configured in CUCM.
- Enable alert by URL: to raise alert from and url.
- URL to raise the alert: URL automatically generated. Each alert have a specific URL.
- List of authorized sending IP addresses: IP addresses authorized to raise alert by URL.
- Dry contact input parameters: Parameters to allow specific dry contact equipment to raise alert.
- Audio files: Audio files used by alert when user try to raise it.
- DTMF code to raise the alert: DTMF code used to raise alert when user call alert CTI port.

### 5.7.2.3 Destination List

- Destination list type: Type of destination list used to define phones called by dial CTI ports when alert is raised.
- Call distribution mode: Mode of call distribution.
- Alert audio file: audio file spread, to phones called by dial CTI port, when alert is raised.

### 5.7.2.4 Treatments, recycle

Parameters used by alert for calls treatments.

### 5.7.2.5 Dry contact input parameters

Define interface with Dry Contact to IP devices.

## 5.7.3 Audio files definition

This section allows to generate text to speech audio files for 3 conditions in addition to the main audio file.

- For authorized calling party
- For unauthorized number

- When announce is currently played



Home / Voice Alert / Alerts' definition

Cancel Save Delete

Select entity (Default) Select group Default

Identifier Audio trigger mode Trigger audio files Trigger by API Trigger by file Trigger by dry contact input Destination list Message audio/Notifications Recycle and treatments Output dry contact

Alert Type **Call & play audio message**

Audio Alert file

Concatenate languages 2 languages

Voices Microsoft Server Speech Text to Speech Voice (fr-FR, Hortense)

Text to speech Le générateur G21 bâtiment B est en panne. Merci de confirmer la prise en compte de l'alert en tapant 1. Play

Voices Microsoft Server Speech Text to Speech Voice (en-GB, Hazel)

Text to speech G21 generator in building B is breakdown. Please confirm you take care of this incident by typing 1.

Or upload audio file Browse...

Ending audio silence duration (s) 0

c:\inetpub\wwwroot\IPSCFG\data\AUDIO\audio\_96.wav

## 5.7.4 Dry contact input parameters

This section allows to control parameters for dry contact.

### [Hide dry contact input parameters](#)

Dry contact IP input type ControlByWeb WebRelay

Detection mode REQUEST

Confirm action by pulsing relay

Dry contact IP address 1

Dry contact IP port 1

Dry contact index 1

## 5.7.5 Destination lists

You can select one or two destination lists. You can mix phones' lists and directory numbers lists. However, you cannot mix contacts' lists with other type of lists.

Home / Voice Alert / Alerts' definition

Cancel Save Delete

Select entity (Default) Select group Default

Identifier Audio trigger mode Trigger audio files Trigger by API Trigger by file Trigger by dry contact input Destination list Message audio/Notifications Recycle and treatments Output dry contact

Destination list 1 type Broadcast list

Selected items list GDIR-CONTACTS

Destination list 2 type

Call distribution mode Broadcast

[Generate IPPhone list relative to this selection](#)

You also select the call distribution mode:

- Broadcast: call in parallel as many destinations as possible
- Broadcast on speaker: call in parallel and answer the call (only for Cisco IP Phones that can be CTI Monitored)
- Top down: call the first destination, then the second, etc. Generally, this mode is used for a limited list of contacts and the alert stops when one of them has accepted the alert.

## 5.7.6 Recycling

From this tab, you will define how the alert is managed and recycled.

Home / Voice Alert / Alerts' definition Cancel Save Delete

Select entity (Default)   
 Select group Default

Identifier	Audio trigger mode	Trigger audio files	Trigger by API	Trigger by file	Trigger by dry contact input	Destination list	Message audio/Notifications	Recycle and treatments	Output dry contact
<p>Stop alert on first accepted <input type="checkbox"/> ?</p> <p>Sort list by phone's location <input type="checkbox"/> ?</p> <p># retries on no-answer, busy, not-accepted <input type="text" value="1"/></p> <p>Retry delay on no-answer, busy, not-accepted <input type="text" value="30"/></p> <p>Drop ongoing call to play the alert <input type="checkbox"/> ?</p> <p>Do not alert forwarded directory numbers <input type="checkbox"/></p> <p>Maximum ring duration (s) <input type="text" value="17"/></p> <p>Minimum message listen duration (s) <input type="text" value="5"/> ?</p> <p>DTMF code to acknowledge the alert <input type="text" value="1"/> ?</p> <p>DTMF code to decline alert <input type="text" value="0"/> ?</p>									

When Voice Alert is used to alert a small security team, whenever one of the contacts has accepted the alert can be stopped.

When using Voice Alert in auto-answer mode it is important to alert the phones located in the same open space as quickly as possible to avoid echo. In other case, we may prefer to alert as quickly as possible some phones in each location.

You can choose to call again a destination on no answer or busy several seconds after a delay.

For critical alert it is possible to drop an ongoing call and play the audio notification instead.

When the line is forwarded, the alert can be omitted to avoid alerting somebody in the wrong location.

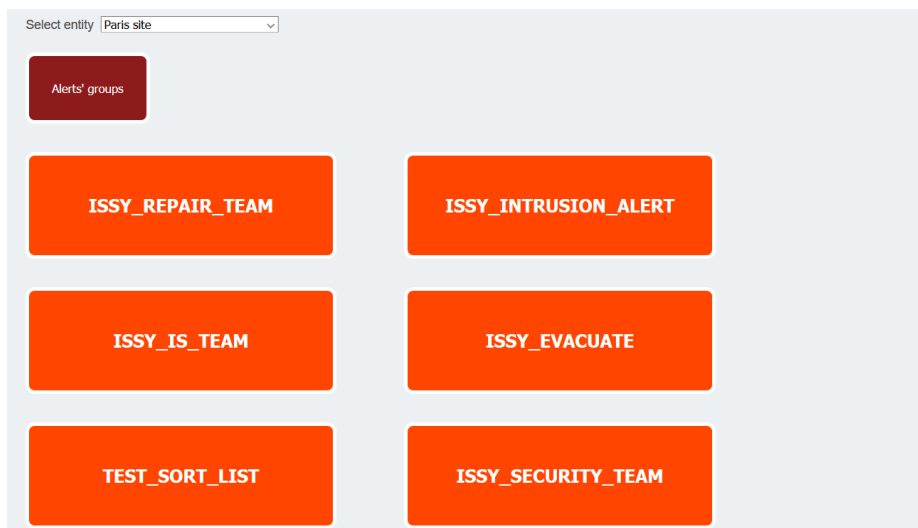
You can define the delay after which the ringing call will be considered as not answered. It is important that this delay is smaller than the delay set to forward on no answer to the Voice Mail (generally 20 seconds) otherwise the notification will be recorded in the voice mail.

To check that the notification has been listen you can define a minimum call duration and also ask the user to press a DTMF key. You can also define the decline DTMF code. In this case the call is not recycled and considered as declined.

## 5.8 Web Alerts tab

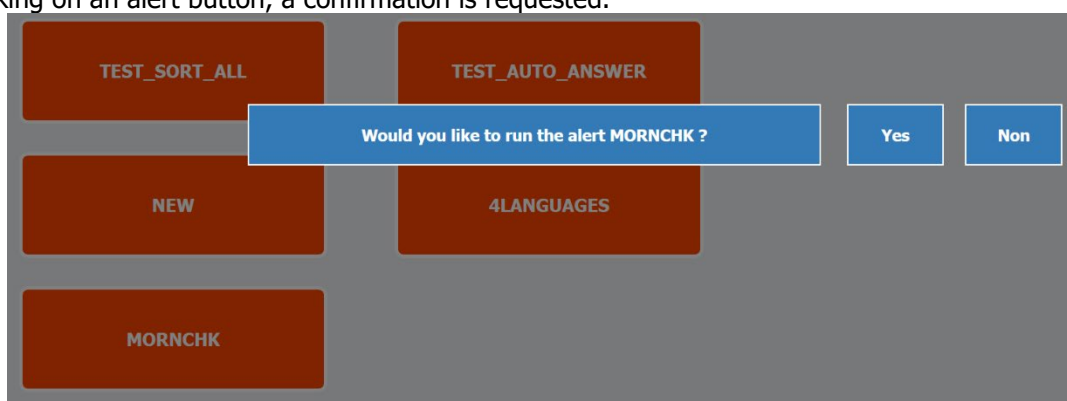
The Web Alert scen is used to trigger alerts. It can be accessed by administrators and entity's supervisor. It can be also opened without authentication from an authorized IP address (see entity definition).

It is possible to create groups of alerts according to different criteria. You can navigate between the alerts' group.

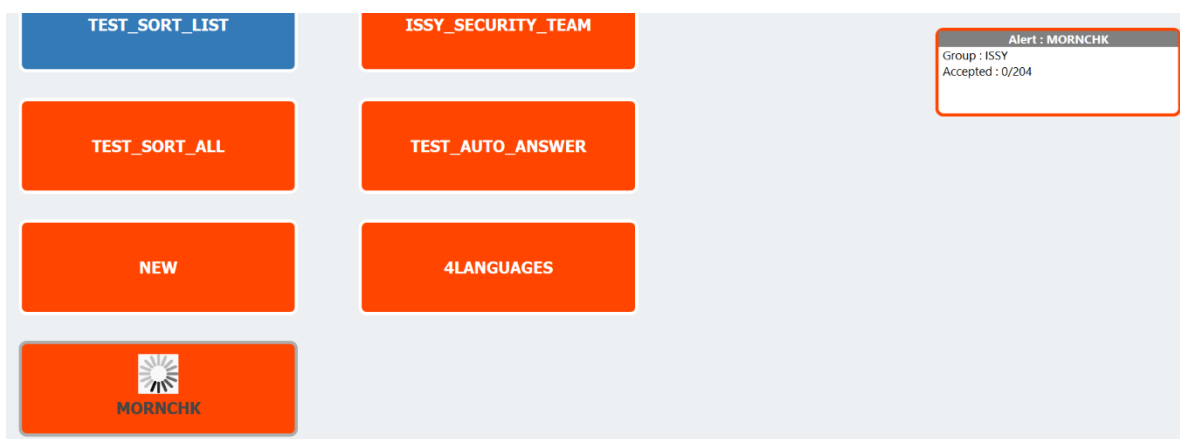


Once a group has been selected, the list of alerts of this group is displayed like this. It is possible to go back to previous screen by using Alert's groups button.

When clicking on an alert button, a confirmation is requested.



When the alert is starting an icon is displayed on the button and a small Window is displayed with the alert's name and number of destinations.



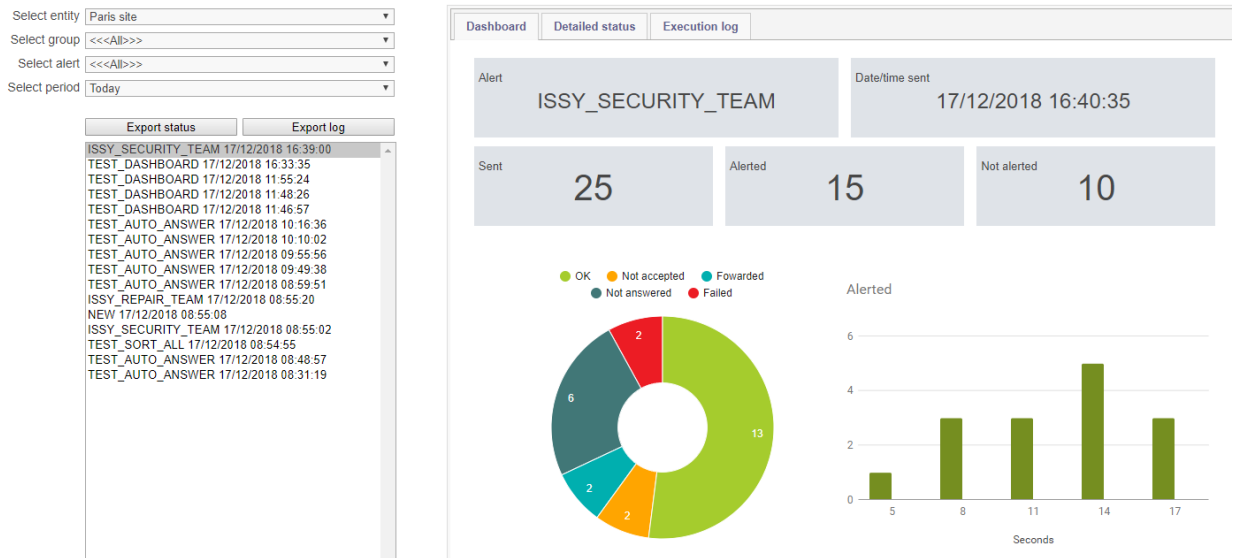
You can stop the alert by clicking again on the button. A confirmation is requested.

The screenshot displays a web interface with a grid of buttons. A central blue dialog box asks, "Would you like to stop the alert MORNCHK?". To the right, a grey alert box shows "Alert : MORNCHK", "Group : ISSY", and "Accepted : 0/204". Below the dialog are "Yes" and "Non" buttons. The interface buttons include "TEST\_SORT\_LIST", "ISSY\_SECURITY\_TEAM", "TEST\_SORT\_ALL", "TEST\_AUTO\_ANSWER", "NEW", "4LANGUAGES", and a "MORNCHK" button with a sun icon.

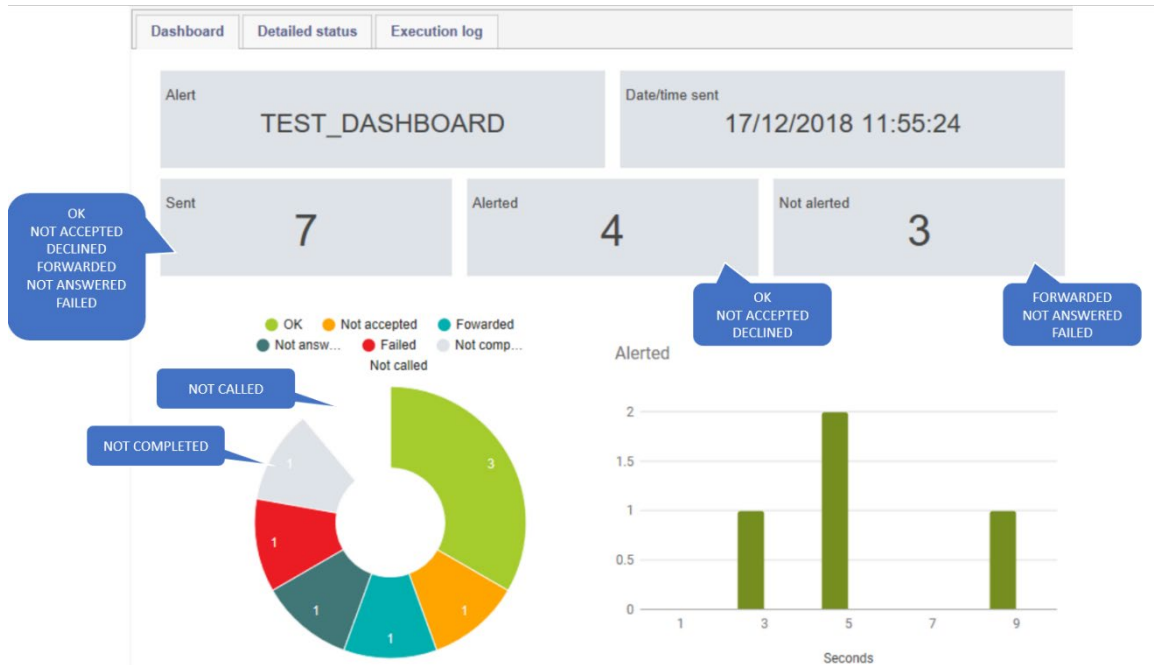
## 5.9 Reports

In reports tab, it is possible to consult historic of alert management. A report is created to check the proper functioning of alerts. An other report displays final state alerts receipt. The report can be exported. The reports are sent to the administrator's email addresses.

By default the last report of the day is selected. You can select another report by filtering by entity (only for the administrator), Alert's group, Alert and period.



Here is detail of the Dashboard count:



Sent = Alerted + Not Alerted.

Sent does not include 'NOT COMPLETED' and 'NOT ALERTED'.

The screenshot shows the telisca interface with the following elements:

- Filter options:
  - Select entity: Paris site
  - Select group: <<<All>>
  - Select alert: <<<All>>
  - Select period: Today
- Buttons: Export status, Export log
- Execution log window:
  - Dashboard | Detailed status | Execution log
  - ISSY\_SECURITY\_TEAM;17/12/2018 16:40:35
  - ORIGIN WEB;127.0.0.1
  - SUCCEEDED;1
  - NOT ACCEPTED;1
  - FAILED;1
  - NOT ANSWERED;2
  - FORWARDED;1
  - CALL\_TIME;PHONE\_NAME;DIR\_NUM;STATUS;CAUSE
  - 16:40:40;;105010;OK
  - 16:40:35;;105007;NOT ANSWERED
  - 16:40:35;;105005;FORWARDED
  - 16:40:42;;105034;NOT ACCEPTED
  - 16:40:35;;105006;NOT ANSWERED

Here is the explanation for the different status you can find in the "Detailed status" (for calling mode):

- **OK:** The user has answered, listen the audio message the minimum required duration and (if requested) entered the DTMF key,
- **NOT ACCEPTED:** The user has answered but not listen the minimum duration or not entered the DTMF key (if requested).
- **DECLINED:** The user has answered but entered the declined DTMF (if required).
- **FORWARDED:** The line is forwarded and the alert has been configured to skip forwarded lines.
- **NOT ANSWERED:** The user has not answered even after the defined retries
- **FAILED:Reason :** The line could not be dialled or was busy after each defined retries
- **NOT COMPLETED:** The line has not answered and the recycling is not completed
- **NOT ALERTED:** The line has not been dialled yet.

The execution log gives more detail on the different steps trying to reach the destination. So for each destination they are several lines. The different information logged can be:

- **FORWARDED; NOT DIALED:** The destination number is forwarded, depending of the parameters of the alert he may not be dialled
- **Dial Succeeded:** The destination has been dialled
- **Dial Failed:** The destination is busy, not registered, incorrect or the CTI Ports does not have the right level of Calling Search Space to dial it
- **No Answer;Retry:** The destination has not answered in the delay defined for this alert. The destination will be dialled again.
- **No Answer;FAILED:** The destination has not answered in the delay defined for this alert. The maximum number of attempts is reached. The destination will not be called again.
- **Playing audio alert:** The destination has answered and the audio server is playing the audio message
- **Played less than n sec.;Retry:** The audio message has been played but the destination has hang up before the minimum duration defined for this alert, to be considered as successful. The destination will be dialled again.
- **Play;SUCCEEDED:** The audio message has been played for the minimum required duration before the destination has hangup. The alert notification has succeeded.
- **LAST TRY => FAILED:** All attempts was unsuccessful; the destination will not be called again.

## 5.10 Dry contacts/IP parameters

Parameters used by alert to open/close a dry contact equipment for ControlByWeb devices.

Example of settings of ControlByWeb Web Relay, default Admin Web Server setting.



Two modes can be used for input dry contacts:

- Polling: Voice Alert send an http get request to the dry contact to the specified IP address and port and analyse the status return to see if a digital input has been pressed.
- Request: The dry contact must be configured to send a socket connection to Voice Alert Server on port 2018 (for instance 1, 2028 for instance 2, ...). The IP address of the dry contact must be defined because it is used to identify the dry contact and the alert. So it will not work if the dry contact call the Voice Alert Server through a VIP address, because the Dry Contact IP address will be lost.

In Polling mode, no other dry Contact/IP setting is mandatory.

Example of setting with WebRelay in Request mode



Example of setting with ControlByWeb X-332 in Request mode

**CONTROL by WEB™**  
www.ControlByWeb.com

Information Network **Adv. Network** Passwords Date/Time Logging Events Basic Script Control Page Setup

**MODBUS**  
Enable Modbus Features.

Modbus Enabled:  Yes  No  
 Port:   
 Endianness: Big Endian

**Remote Services**  
Connect to remote services server.

Enabled:  Yes  No  
 Server Name/IP Address:   
 Server Port:   
 Connection String:   
 Connection Interval:  Minutes

General Settings  
I/O Setup  
Monitor and Control

Example of settings with ControlByWeb X-310 in Request Mode

Information Network **Adv. Network** Passwords Date/Time Logging Events Basic Script Control Page Setup

**MODBUS**  
Enable Modbus Features.

Modbus Enabled:  Yes  No  
 Port:   
 Endianness: Big Endian

**Remote Services**  
Connect to remote services server.

Enabled:  Yes  No  
 Server Name/IP Address:   
 Server Port:   
 Connection String:   
 Connection Interval:  Minutes

Voice Alert Administration, Dry contact X-332, set in Request mode, on input 2.

[Masquer paramètres contacts sec entrant](#)

Type interface contact sec -> IP

Mode de détection

Confirme prise en compte par impulsion sur relais

Login contact sec

Password contact sec

Adresse IP contact sec 1

Port IP contact sec 1

Index entrée contact sec 1



Input digital 2 is set, 'Sent State Msg/Trap on I/O change is checked.

## 5.11 REST API to trigger an alert

It is possible to trigger an alert using an HTTPS GET request.

This mechanism needs first to be enabled in Voice Alert / Parameters page / Activation tab.

Then when creating an alert, check 'Enable alert by URL'.

Use the URL to raise the alert by replacing 127.0.0.1 by Voice Alert's server IP or FQDN.

You should also restrict the usage of the API to specific calling servers' IP addresses, by entering a list separated by commas.

The API may return: 'SEND ALERT' or 'ID NOT FOUND' or 'CALLING IP NOT AUTHORIZED' or 'ERROR'.

## 5.12 Send SMS

If the alert is based on contacts lists, it is possible to send an SMS to alert the contact. Then select the type SMS in front of the contact's number.

Edit
Delete

Active contact

Last name  First name

Location  Email address

Phone #1  Phone  Phone #2  SMS

Phone #3  FAX  Phone #4  Phone

Office hour begin  Office hour end

Currently SMS are sent using <https://esendex.com> cloud service which provides API to send massive number of SMS. You need to have a subscription to use this Cloud Service.

The first step is to configure you esendex ID, login and password in telisca Global Configuration / SMS Gateway page:

[Home](#) / [Global configuration](#) / [SMS Gateway](#)

### SMS Gateway settings

Send SMS enabled

Send SMS method

Account ref

Username  ?

Password  ?

In the Alert definition, Audio message/Notification tab, you can enter the content of the SMS to send.

Enable SMS/Fax  ?

SMS/Fax content

## 5.13 Send Fax

If the alert is based on contacts lists, it is possible to send a Fax to alert the contact. Then select the type FAX in front of the contact's number.

Edit
Delete

Active contact

Last name  First name

Location  Email address

Phone #1  Phone  Phone #2  SMS

Phone #3  FAX  Phone #4  Phone

Office hour begin  Office hour end

To send Fax you need to subscribe to an Email to Fax Cloud service. Then enter the domain name of this fax service in Voice Alert / Parameters / Various tab.

Activation Trigger modes **Various** Advanced

Administrators' email addresses (separated by ,) to send reports

Fax gateway domain name gofax.com

Voice Alert will send an email to an email address built with the destination mobile number and the domain name like [+33608181226@gofax.com](mailto:+33608181226@gofax.com) .

In the Alert definition, Audio message/Notification tab, you can enter the content of the FAX to send.

Enable SMS/Fax  ⓘ

SMS/Fax content

URGENT: ENGINE B3 BREAKDOWN AT ISSY LOCATION.  
PLEASE CALL +33165428744