

# Product Configuration

## User Properties

Every Call Recording user already enabled on the Calling Platform can trigger recordings straight away, providing mandatory fields in relevant Imagicle user, like username and extension number, are filled in.

Moreover, there are a number of Call Recording-related user's parameters that might be entered for additional functionalities:

- **First extension number alias:** PSTN number (DID) corresponding to user's extension number. This is useful to correctly correlate recordings performed through Webex Calling MT, AudioCodes or other SIPREC-enabled Media Gateways.
- **PBX username:** In a Webex Calling MT architecture, this field must be populated with user's account. This is also mapped in Webex Calling [Synch Rules](#).
- **Numeric User ID:** this is a unique ID to be filled while dealing with overlapping users associated to same extension number (CUCM only)
- **Numeric Partition ID:** this is the CUCM partition ID associated to user. It should be filled while dealing with overlapping users associated to same extension number.
- **Group Name:** if set, this field defines the recording group the user belongs to. This field can be used to filter/search recordings and to enable a group superuser (see below).
- **List of additional groups:** This field allows to configure additional recording groups that a group supervisor is granted to, for managing relevant recordings. You can add here multiple groups, separated by semicolon.
- **Send email notifications / Attach recording file to email notifications:** These flags enable email notifications to the user, with or without recording audio file attachment.

IP Telephony			
Partition	<input type="text"/>	First extension number	<input type="text" value="731"/>
First extension number alias	<input type="text" value="0288996731"/>	Device name	<input type="text" value="SEPBC493A48BC5"/>
PBX username	<input type="text" value="john.smith@company.com"/>		

Call Recording			
Numeric User ID	<input type="text"/>	Numeric Partition ID	<input type="text"/>
Group Name	<input type="text" value="Sales"/>	Additional supervised groups (e.g.:Sales;Marketing;Board)	<input type="text" value="Marketing;Support"/>
Send email notifications	<input checked="" type="checkbox"/>	Attach recording file to email notifications	<input checked="" type="checkbox"/>

"First extension number alias", "Group name" and "List of additional groups" fields can be optionally populated during users' synchronization against external sources like AD, LDAP, Webex or CSV. Pls. check [here](#) for further details.

Please remember that both "Group name" and "List of additional groups" fields are relevant if you need to enable multiple "Group Supervisors", with different permissions for different groups of recording users. See next paragraph for further details.

## User Permissions

Each Imagicle user is configured with a specific permission level by application. For Call Recording, three permission levels are available:

- **Record Only:** This profile enables a user to start/stop, pause and resume a recording and prevents him from accessing any recordings (search, listen or download any recordings is forbidden for this user).
- **Base Access:** this is the default access level (simple user) applied to all Application Suite users. This profile can:
  - ◆ Record new conversations
  - ◆ Browse, search, play **own recordings only**
  - ◆ Download and delete own recordings (if globally enabled by administrator)
  - ◆ Tag recordings for a longer retention (if globally enabled by administrator)
  - ◆ Add/edit notes attached to each own recording
- **Group Supervisor:** compared to base access, a user with this profile, with a not blank recording group, can also:

- ◆ Browse, search, play all recordings of the recording group he belongs to
- ◆ Download and delete groups' recordings (if globally enabled by administrator)
- **Administrator:** In addition to supervisor access level, a user with this profile can also:
  - ◆ Browse, search, play, download and delete any recording, of any user
  - ◆ change global settings
  - ◆ start/stop Call Recording service

Moreover, following hierarchical rules apply:

- A user cannot delete a recording preserved by a higher level user
- A user cannot delete or amend a note written by a higher level user

Recordings done by users with a blank recording group can only be seen, played, deleted by the user himself and by the admin profiles (accordingly with the permission settings described below).

Please remember that if you delete an Imagicle user with existing recordings, they are not lost and still accessible by group supervisors and administrators from Call Recording web portal .

## Service Settings

The service settings (*Global Settings*) section is available only to administrative profiles (menu item *Global Settings*).

## Recording Filters

When using the Always-On recording mode, you may need to record only some kind of calls/traffic. For instance, an help desk operator may need to record only incoming calls from the PSTN, not the conversations with other colleagues.

This section allows to define flexible recording filters to decide which type of calls to record or discard. Such filters apply to **all** recording enabled users.

The available options for call filtering are:

- **Call Direction:** setting this option you can decide to record only incoming/outgoing calls (from the IP phone point of view) or both of them.
- **Traffic Type:** setting this option you can decide to record only internal or external (to/from PSTN) calls. Calls are considered internal if the remote party is included in the application suite users list or if the remote party number matches the Internal number patterns defined in the application suite "Numbering Plans Parameters" section.
- **Black List:** this option allows to define a list of remote party numbers/patterns that you don't want to record. You can specify multiple numbers/patterns, one for each row.  
For instance, you can use this option to avoid to record the operator calls towards voicemail systems or conversations with VIP people who cannot be recorded. See the hint on the web page for the available wildcards you can use to build patterns. Some sample patterns:
  - ◆ 7100: avoid to record all calls to the Voicemail pilot 7100.
  - ◆ 72. : avoid to record all conversations from/to numbers 3-digits long, starting with '73'.
  - ◆ 8! : avoid to record all conversations to any number (of any length) starting with '8'.

Hint: include the recorder pilot number (that is the Recording Profile DN configured on CUCM) in the remote party Black-list, to avoid to record calls placed to the recorder itself.

## Permissions

Use this section to decide which access levels can delete or download recordings. Available options are:

- Nobody: useful to prevent accidental deletions, even by service administrators.
- Administrators
- Group Supervisors
- Simple users

# imagicle

This permission is also affecting multiple recordings download feature, available from 2021.Spring.1 release, where you can select multiple recordings from "My Recordings" or "All Recordings" menus and retrieve a zip archive including several MP3 audio files.

For deletion, if you select "Nobody - Irreversible choice", even administrators won't be able to delete the recordings, and nobody will ever be able to change the setting.

## Pilot Numbers

### Automatic user identification

This section allows to enable Call Recording for overlapping extension numbers. Two methods are available:

1. Recognise proper users by using **Numeric User ID**: This field can be populated in Imagicle users' list and, when relevant user triggers the recording, a specific CUCM Recording Profile is used, with a configured pilot number including the "Recording pilot (prefix):" + Numeric User ID. This method is recommended when you have a limited number of overlapping extensions.
2. Recognise proper users by using **Numeric Partition ID**: This field can be populated in Imagicle users' list and, when relevant user triggers the recording, a partition-specific CUCM Recording Profile is used, with a configured pilot number including the "Recording pilot (prefix):" + Numeric Partition ID. This method is recommended when you have several overlapping users, across multiple partitions.

## Live Keep Recording

To use Live Keep Recording, a dedicated service pilot number has to be configured. Follow these suggested steps:

1. choose an UNUSED internal number (like 8500);
2. Insert that number into "Live Keep pilot (prefix)" field and Save;
3. Follow CUCM configuration available [here](#).

## Actions on recordings without assignees (from 2020.Spring.1 release)

This feature, only available to customers with a [channel-based Call Recording license](#), allows to specify an Imagicle "Catch-All" user to whom attribute all those recordings not correlated to a named user. By default this feature is disabled, so all recordings not correlated to Imagicle users are discarded, as it happens with Imagicle versions prior to 2020.Spring.1.

**Note:** Imagicle Call Recording Catch-All user must be ad-hoc created for this purpose. You can't use an existing named user.

## Automated Recording

To implement Automated Dial-In Recording, a dedicated service pilot number has to be configured. Follow these suggested steps:

1. choose an UNUSED internal prefix that identifies an unassigned range of 10000 numbers (like 9000XXXX);
2. Insert that prefix into "CTI controlled pilot nÃ° (prefix)" field and Save;
3. Follow CUCM configuration available [here](#).

## Data Management

### Storage (encrypted) section

#### Storage location

This section allows to choose where to store encrypted audio recording files:

- **Local** - files are stored inside Imagicle server's file system and replicated in all nodes (if HA is in place). Local folder path for recordings is fixed\*.



# imagicle

- After the certificate is uploaded in the Imagicle web interface, browse to Call Recording → Global Setting → Data Management, then scroll down to "Certificates" and click on "Change".
- Select the certificate that you have uploaded previously and click on "OK".

**NOTE:** For recording security it is recommended to use a certificate signed by a Certificate Authority (CA), otherwise the system will use the self-signed unsecure one. The signed certificate you are going to use must be saved, backed up and kept outside the Imagicle VM (For security reasons we are not backing it up using the "backup and restore" tool that installs with the Imagicle setup).

**In case a UC Suite backup is restored onto a new one, you must import the certificate manually otherwise you won't be able to playback old recordings.**

- To import the existing certificate, from Windows Start menu run "inetmgr"
- Click on the server name, and on "Server Certificates"
- On the top right, click on "import"
- choose the right certificate and input the password in case required.

After import is complete, follow the above steps to change the certificate to the one uploaded.

## Hardware Requirements

In our [Storage Calculator](#), we also display the amount of **Calls Per Second (CPS)** globally engaged by Call Recording users. CPS is calculated for both channel-based license (ERLANG calculation applied) and user-based license. Please make sure to keep CPS value below 3, to avoid overloading Imagicle recording engine with too many concurrent recording requests. If your calculation returns a CPS value over 3, please contact Imagicle to learn about specific hardware requirements to fulfill your traffic needs.

## Data Export (Unencrypted)

Recordings saved in the application suite server (as encrypted files) can also be exported to a remote storage in MP3, unencrypted file format. This export job can be useful for backup scopes or to realize further processing inside the organization (for instance loading them into a centralized document repository).

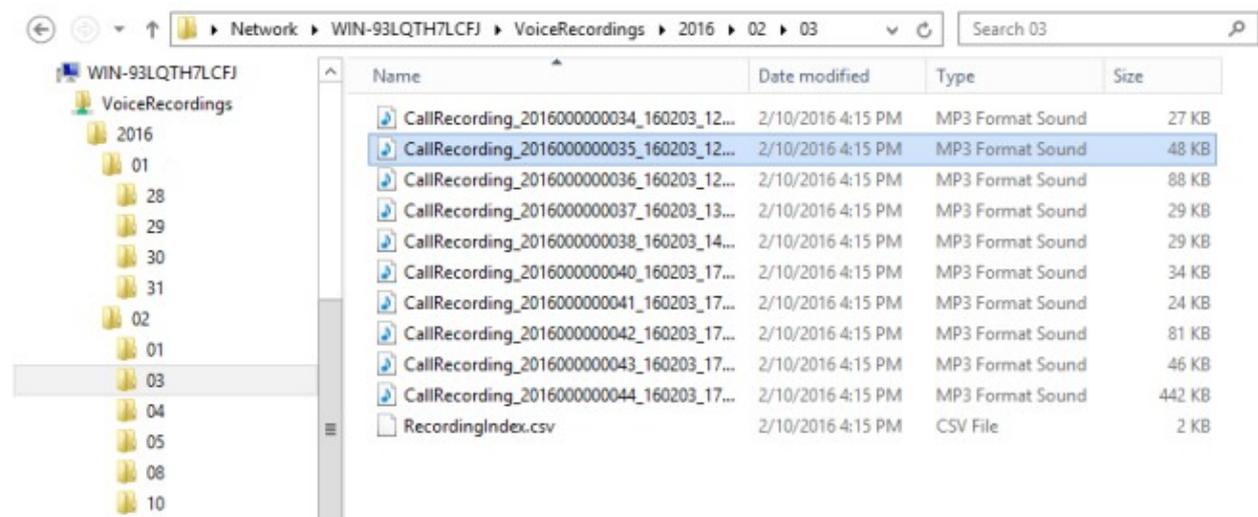
The destination storage must be a network folder shared by Microsoft Sharing protocol (SMB) and accessible by a network path, for instance:

```
\\nas-backup\VoiceRecordings.
```

Such path represent the base folder for data export. Further subfolders will be automatically created by the system in a hierarchical date schema `year\month\day` (one folder per day).

For instance, referring the path mentioned above, recordings started on April 21st, 2016 will be exported to:

```
\\nas-backup\VoiceRecordings\2016\04\21.
```



# imagicle

Inside each folder the service will place :

- All recordings files (started in such date), in plain MP3 format. The destination filename includes:
  - ◆ The unique (sequential) RecordID
  - ◆ A timestamp yyyyMMdd\_hhmmss
  - ◆ The recording user (username)
  - ◆ The call direction (IN/OUT/DIALIN)
  - ◆ The recorded extension number
  - ◆ The remote party number
  - ◆ The group name (if any)
- A CSV text file (UTF-8 encoding) containing all the relevant data of the exported recordings. This file can be easily opened with a spreadsheet application or used for indexing purposes by third party systems. The CSV fields include:
  - ◆ Recording agent name
  - ◆ Recorded extension number
  - ◆ Remote party number,
  - ◆ Start time
  - ◆ Call duration
  - ◆ Group Name

The destination folder must be accessible for writing to a local or domain user. The service will use the credentials of such user to create files and folders on the destination folder.

The export job runs at regular time intervals (about 1 minute).

Exported files are never deleted by Imagicle Call Recording on the remote storage. The customer is in charge of the retention policies for such files.

## Configuration

**Data Export (Unencrypted)**

The service can AUTOMATICALLY export a copy of the recordings into a network shared folder (accessible for writing). Use this section to enable and configure it. Recordings will be saved in MP3, unencrypted, format. A text file (CSV) containing the relevant call data will be created in the same folder, for indexing purposes. The exported recordings are not part of Call Recording lifecycle and not retrievable through Search and Play UI.

Save a copy of recordings on an external storage area ⚠ Any change to these settings will apply to new recordings only.

Destination folder (base path):  ⓘ

Use this username (domain\user):

Use this password:

In this form enter:

- The network path of the destination folder. For instance: `\\nas-backup\VoiceRecordings`
- The username used to access the destination folder. This can be either a domain user (for instance `IMAGICLE\backupuser`) or a local user defined in the remote machine. This user must be enabled for writing in the specified folder.
- The password of the user specified above.

**Note:** you cannot specify a local path as export destination folder, only network paths are admitted. This is because local paths would be problematic for high-availability configurations.



Use the 'Test access' button to verify if the destination folder is accessible to the service with provided credentials: if successful, a small test file will be created on the destination folder.

Only new recordings will be exported to the specified path.

In the case the remote storage is temporarily unavailable or unreachable (for example because of a network outage), the missing recordings will be automatically exported as soon as it comes back available.

## Notifications

### Email notifications

Users may receive an email notification whenever their calls have been recorded. You choose which users receive the email by ticking the "Send email notifications" flag in the users profile properties, Call Recording section. If you also enable "Attach recording file to email notifications", an **unencrypted copy** of the recorded message will be attached to the email message, in plain .mp3 format.

On the Email notifications setting page, you can set the size limit for the attachment. If the limit is overcome, the email is sent anyway. The minimum size limit is 1 MByte. Unchecking the flag, no limit will be applied.

You can also set the email notification sender name. You can set other SMTP properties through Admin, System Parameters, SMTP parameters.

How to edit the Email notification template

To change the email body contents for all the users, locate this folder:

```
<installation dir>\StonevoiceAS\Apps\Recorder\Locale\XX\
```

Where XX is the language code for the users language. Eg. en, it, fr..

Copy User.Notification.Template.txt as User.Notification.Template.txt.user. Edit User.Notification.Template.txt.user.

The template can be customized with the following tags, which will be replaced with the actual data when the email is sent:

```
[RecordingID] - Recording unique identifier
[Username] - Recording owner's user name
[UserExtension] - Recording owner's extension number
[UserFirstName] - Recording owner's first name
[UserLastName] - Recording owner's last name
[UserNumericUserID] - Recording owner's numeric identifier
[RemotePhoneNumber] - Recording's remote phone number
[RecordingStartDate] - The date the recording started
[RecordingStartTime] - The moment the recording started (hh:mm:ss)
[RecordingDuration] - The recording duration (hh:mm:ss)
[RecordingGroupName] - Recording owner's group name
[PBXCallID] - Recording identifier assigned by PBX
[CallDirection] - The call direction
[RecordingPilotNumber] - The recorder pilot number
[AttachmentFileSize] - The size of sent attachment in KBytes (0 when no attachment has been sent)
[MaxAttachmentSize] - The maximum size allowed for attachment (in MBytes)
```

To change the template for the users who belong to a specific department, follow the same procedure in this folder:

```
StonevoiceAS\Settings\Departments\<department>\MailNotificationTemplates\CallRecording
```

Where <department> must match the content of the Department field in the user profile.