



Mida Configuration Guide

Mida Teams Compliance Recorder

Document Version: 1.1

 Solution certified for
Microsoft Teams

Document Information

Revision	Date	Description	Updates	Product Version
1.0	01/09/2021	Initial version		1.0
1.1	26/04/2022	Minor review		1.0.4

Table of Contents

1.	Introduction.....	3
1.1	Legal Statements	3
1.2	Preface.....	3
1.3	Audience	4
1.4	Notations	4
1.5	References	4
	BEFORE YOU START	4
	HOW MIDA RECORDER FOR MS TEAM WORKS?.....	5
2.	Register Mida RecBOT in Azure	6
3.	Add a Teams Channel to Mida RecBOT	7
4.	Configuring authentication for Mida RecBOT	9
5.	Configuring permissions for Mida Rec BOT	9
6.	Configuring the server	10
7.	Setting up Mida Bot.....	10
8.	Setting up IIS.....	11
9.	Setting up Recording Policy	12
10.	Add a collector.....	13
11.	Playback Station	18
11.1	Playback Station settings.....	19
11.1.1	Change Columns	19
11.2.1	Recorded file status.....	21
12.	Recorder Security FAQ.....	23

1. Introduction

1.1 Legal Statements

THE SPECIFICATION AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

ACCESS TO THE SOFTWARE REQUIRES THE PURCHASE OF A VALID LICENSE. Mida Solutions OFFERS SUPPORT AND SOFTWARE BUG FIXES IF THE CUSTOMER IS UNDER A VALID SUPPORT AND MAINTENANCE CONTRACT. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR VENDOR REPRESENTATIVE FOR FURTHER INFORMATION.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. Mida Solutions DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

IN NO EVENT SHALL Mida Solutions OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF Mida Solutions OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All trademarks mentioned in this document are the property of their respective owners.

Any Internet Protocol (IP) address and phone/fax number used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Mida Platform

© 2022/2025 Mida Solutions, All rights reserved.

Mida Teams Compliance Recorder

© 2022/2025 Mida Solutions, All rights reserved.

1.2 Preface

This document is part of the official documentation of Mida Solutions products and details functionalities, user interface, options, and working modes in detail. The system allows the user to configure all system functions using a simple and intuitive WEB interface. Please refer to the reference table for a complete list of documents relevant to system configuration.

1.3 Audience

The present document addresses both end-users and system administrators of the products.

1.4 Notations



This document highlights, where possible, the main parameters and operations through **bold** or *italics* text and all parts that might be critical during system configuration or use. Critical parts are also marked with the Warning symbol reported here on the left.

Therefore, please make sure you have completed the deployment instructions included in [Mida Teams Compliance Recorder - Deployment Guide](#) before proceeding with this guide.

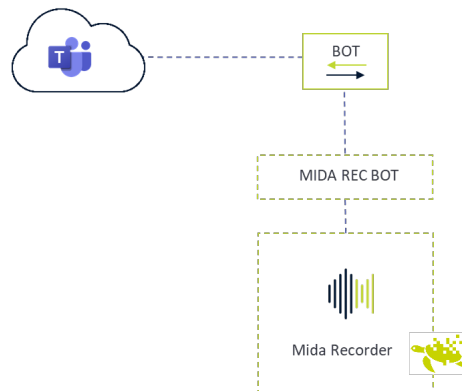
1.5 References

This manual includes references to the following list of documents:

- [1] Mida Unified Portal-Administration & User Manual - This manual is useful to know how to use the MUP by setting customization.
- [2] Mida Recorder – Administration & User Manual - This manual is useful to know how to use the Playback Station.

BEFORE YOU START

Before starting with the configuration, we would like you to acknowledge how Mida Teams Compliance Recorder works. Recordings are made by a bot (hereafter Mida RecBOT), and then call audio files and metadata are made available in Mida Playback Station, from where you manage the recordings.



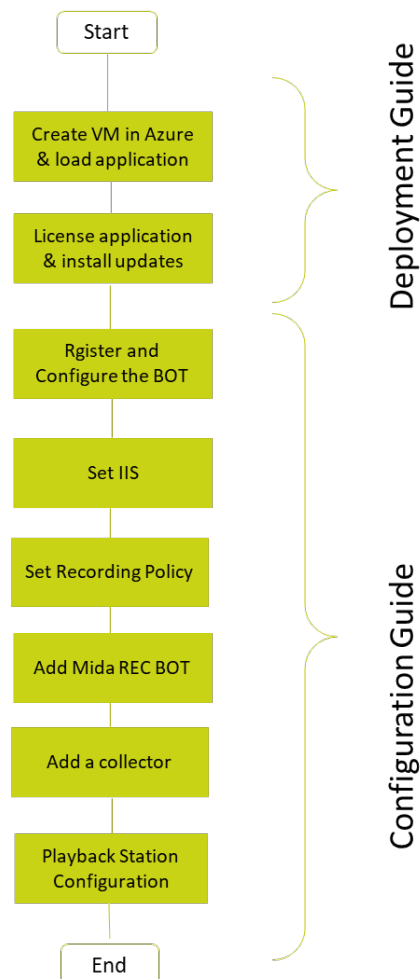
HOW MIDA RECORDER FOR MS TEAM WORKS?

Mida RecBOT joins the calls you make-receive in MS Teams (both Teams to Teams, Teams to PSTN, PSTN to Teams). In the configuration phase, you can set whether it records all users' calls or just some.

Recorded calls are sent to the server where you have installed an executable file (hereafter called MidaRec.exe).

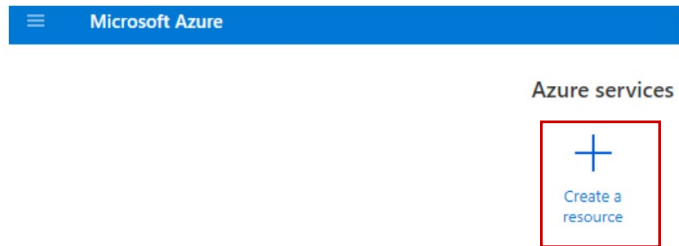
Following our instructions, you must configure a collector within Mida Unified Portal (MUP), allowing the collector to access and copy all the recorded files from the MidaRec.exe folder.

You can set your preferred backup frequency.

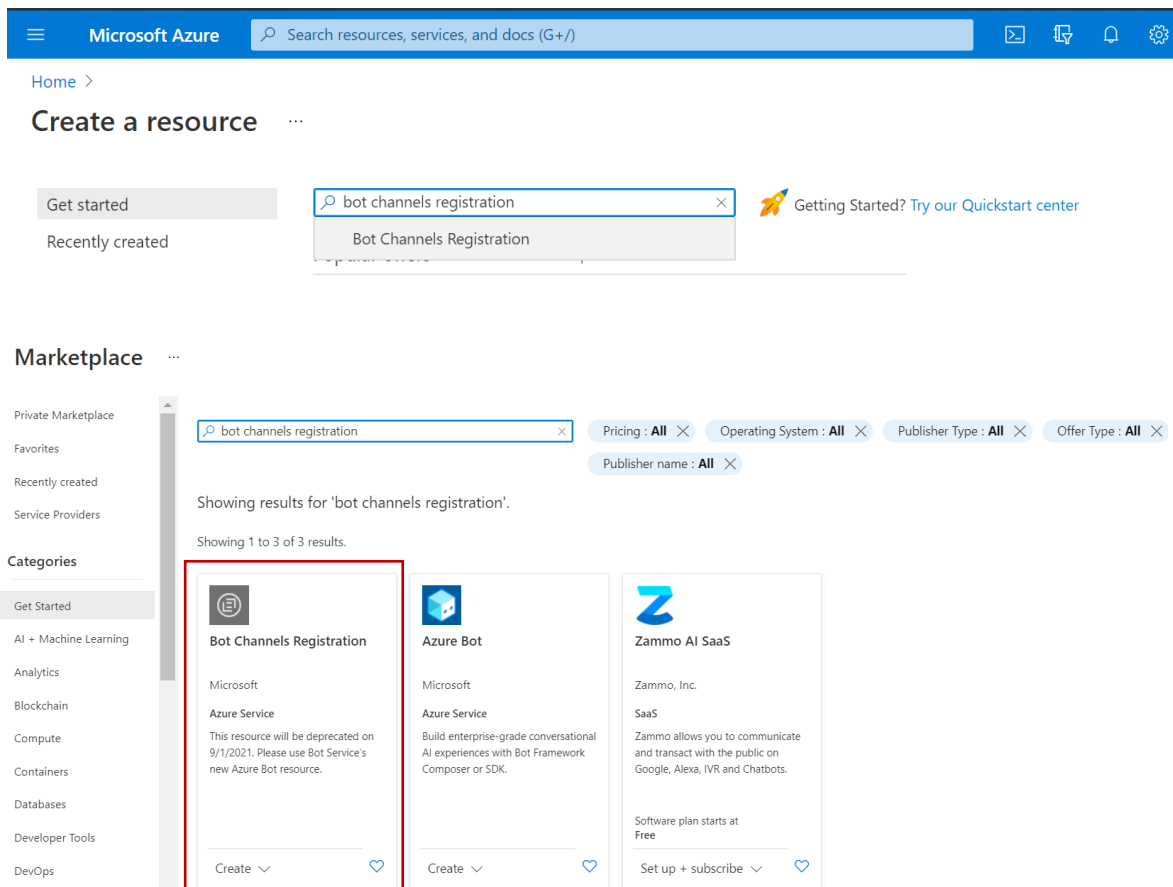


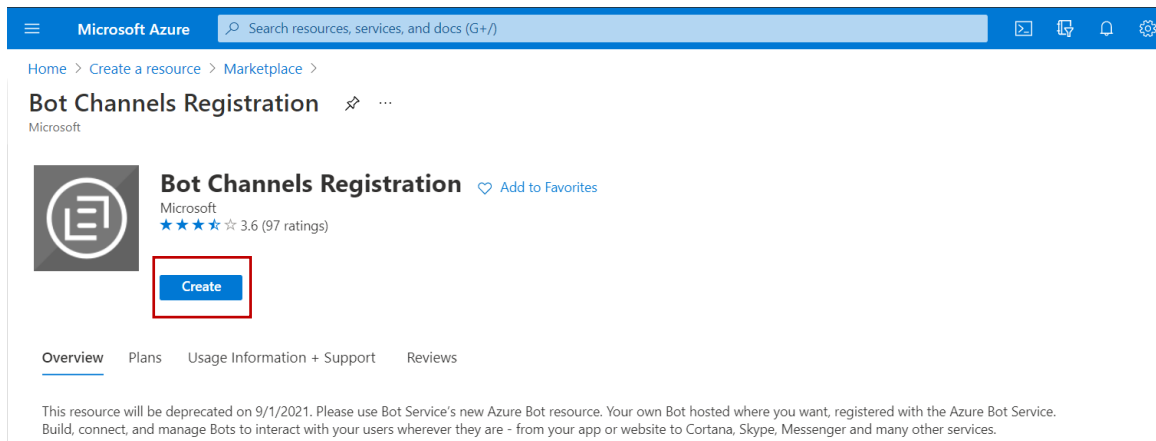
2. Register Mida RecBOT in Azure

- Log in to the [Azure portal](#)



- Click on **Create a resource** and select **Bot Channels Registration** and then click on **Create**





- In the left panel, provide a unique name in the **Bot handle** box
- Select the **Subscription** type based on your requirements
- Create a new **Resource group** for the bot so you can easily see the bill from the Azure portal
- Select the **Location**. It should be the same region you have selected for Mida RecBOT virtual machine
- Select the **Pricing tier** based on your requirements
- **Application Insights** are not mandatory. You can choose to enable or disable it based on your requirements
- Click on the **Create** button. Creating the Bot Channel Registration may take some seconds. Azure will create an App Registration and a Bot Service assigned to it.

Bot handle * ⓘ
Mida_RecordingBot ✓

Subscription *
Pagamento in base al consumo ▼

Resource group *
Teams-Dev ▼
[Create new](#)

Location *
North Europe ▼

Pricing tier ([View full pricing details](#))
F0 (10K Premium Messages) ▼

Messaging endpoint
https URL

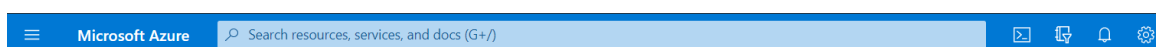
Application Insights ⓘ
☒ On ☐ Off

Application Insights Location * ⓘ
North Europe ▼

Microsoft App ID and password ⓘ
[Auto create App ID and password](#) >

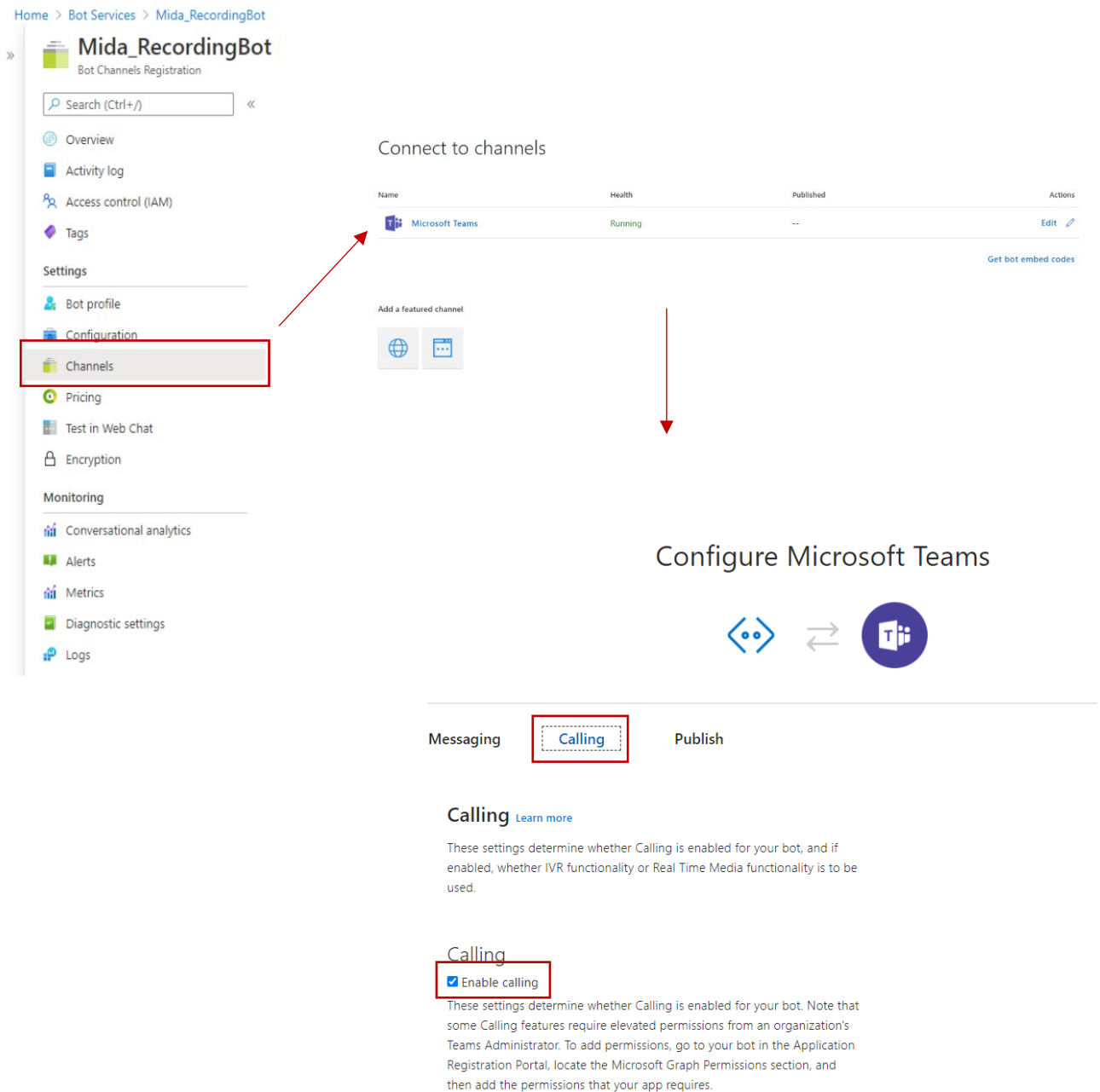
3. Add a Teams Channel to Mida RecBOT

- Once Mida RecBOT Channels Registration is completed, search for **Bot Services** in the search box on the top of the Azure page, then click on your newly created Bot



- Under the Bot management section, click on the Channels menu

- Under the **Add featured channel** section select the **Teams** icon (Configure Microsoft Teams channel)
- Select the **Calling** tab, then tick the **Enable calling** checkbox.



The screenshot shows the Mida RecordingBot Bot Channels Registration portal. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Settings (with sub-items: Bot profile, Configuration, Channels, Pricing, Test in Web Chat, Encryption), and Monitoring (with sub-items: Conversational analytics, Alerts, Metrics, Diagnostic settings, Logs). The 'Channels' option is highlighted with a red box. A red arrow points from this box to the 'Add a featured channel' section, which shows a 'Microsoft Teams' channel listed in a table with columns for Name, Health, Published, and Actions. Another red arrow points from the 'Microsoft Teams' channel to the 'Configure Microsoft Teams' section. This section has tabs for 'Messaging', 'Calling', and 'Publish'. The 'Calling' tab is selected and highlighted with a red box. Below the tabs, the 'Calling' section is titled 'Calling' with a 'Learn more' link. It contains a paragraph explaining that these settings determine whether Calling is enabled for the bot. Below this, the 'Calling' section is repeated, and the 'Enable calling' checkbox is checked and highlighted with a red box. The text below the checkbox explains that these settings determine whether Calling is enabled for the bot and notes that some features require elevated permissions from a Teams Administrator.

- At the **Webhook (for calling)** setting, provide the following URL:
https://mida_bot_vm.domain.com/api/calling
 Replace the *mida_bot_vm* part with the hostname of the Azure virtual machine which will host the

Mida RecBOT. At the domain part, use the domain of the Teams tenant (also specified in the SSL certificate)

- Click on the **Save** button. Agree with the terms of service.

4. Configuring authentication for Mida RecBOT

- Search for **App registrations** in the search box on the top, then click on the **App registrations** link under the **Services** section
- Select the App Registration from the list that was created previously using the name provided during registration
- Take a note of the **Application (client) ID** and the **Directory (tenant) ID**. You will need them later
- Select the **Certificates & secrets** menu in the left panel
- Under the Client secrets section, click on the **New Client Secret** button
- Provide a **Description**, set when the secret **Expires**, then click on the **Add** button
- Take a note of the new **Client secret**. You will need it later

5. Configuring permissions for Mida Rec BOT

- In the left panel, under the **Manage** section, click on the **API permissions** menu
- Click on the **Add a permission** button
- Select Microsoft Graph, then select **Application permissions**
- Select the following permissions:
 - Calls.JoinGroupCall.All
 - Calls.AccessMedia.All
 - Calls.JoinGroupCallAsGuest.All
- Click on the **Add permissions** button
- Grant admin consent for your tenant for the permission added above

6. Configuring the server

- Install the latest version of **VC_redist_x64**
- Create and Install a public **HTTPS** certificate under **Personal** folder
- Get a certificate thumbprint through the following steps:
 - Select **Run** from the **Start** menu, and then enter *mmc*
 - From the **File** menu, select **Add/Remove Snap In**.
 - From the **Available snap-ins** list, choose **Certificates**, then select **Add**.
 - In the **Certificates snap-in** window, select **Computer account**, and then select **Next**
 - In the **Select Computer** window, leave **Local computer** selected, and then select **Finish**
 - In the **Add or Remove Snap-in** window, select **OK**
 - To view your certificates in the MMC snap-in, select **Console Root** in the left pane, then expand **Certificates (Local Computer)**
 - Double click on the https certificate you installed previously and select **Details** tab
 - Scroll through the list of fields and click **Thumbprint**. Take note of this value.
- Install Mida Bot Recorder using the given installer
- Open the **InstancePublicPort** described in the next section in the firewall
- The Microsoft Teams Bot Service is considered a standard Microsoft Teams endpoint and the standard firewall rules can be applied. The following Microsoft documentation contains all the required endpoints and ports which has to be accessible for a Teams endpoint: [Office 365 URLs and IP address ranges](#) (section Skype for Business Online and Microsoft Teams)
In addition, the Microsoft Teams Bot Service uses Microsoft Graph API via the <https://graph.microsoft.com/v1.0> endpoint for sending requests to Microsoft Teams (e.g.: Call answer, Azure AD queries)

7. Setting up Mida Bot

- Once the bot has been installed, go to the installation folder
- Right-click on the “records” folder and select properties. From the “Sharing” tab click on “Advanced Sharing”
- Enable “Share this folder” and save.
- Open “.env” file with a text editor and compile **ONLY** the following fields without spaces after equal operator (=), leaving other fields with default values:
 - AzureSettings__BotName - fill with Azure Bot Handle
 - AzureSettings__AadAppId - fill with Application client ID (2)
 - AzureSettings__AadAppSecret - fill with client secret(3)
 - AzureSettings__ServiceDnsName - fill with DNS:PORT where Mida Bot is installed

- AzureSettings__ServiceCname - fill with Webhook url (4)
 - AzureSettings__CertificateThumbprint - fill with Certificate Thumbprint (5)
 - AzureSettings__InstancePublicPort - fill with TCP public port (default 8445)
 - AzureSettings__CallSignalingPort - fill with call signaling port (default 9442)
 - AzureSettings__InstanceInternalPort - fill with instance internal port (default 8445)
- Save “.env” file
 - Make sure to open the following ports in the firewall
 - InstancePublicPort (e.g. 8445)
 - CallSignalingPort (e.g. 9442)
 - CallSignalingPort+1 (e.g. 9442)
 - InstanceInternalPort (e.g. 8445)

8. Setting up IIS

- Download the latest version of IIS from [here](#) and install it
- Download URL Rewrite the additional package from [here](#) and install it
- Press the Windows Key and type Windows Features, select the first entry “Turn Windows Features On or Off”.
- Make sure the box next to IIS is checked.
- Press the Windows Key and type IIS, select Internet Information Services Manager (IIS)
- In the connection, tab open your server and open “sites” folder
- Select your Web Site (or Default Web Site if it’s the only one)
- Right-click on your Web Site and select “Edit Bindings”
- There should be a default site binding (if not, create it) with the following options:
 - Type: http
 - IP address: All Unassigned
 - Port: 80
- Add a new binding with the following options:
 - Type: https
 - IP address: All Unassigned
 - Port: 443
 - SSL certificate: Select your public HTTPS certificate
- Double click on Url Rewrite
- Right Click on the “Inbound rules that are applied to the requested URL address” and click “Add Rule(s)...”
- It will ask if you want to go to the ARR home page, say **Yes** and Install the **Application Request Routing** extension
- Select Reverse Proxy
- Add new Reverse Proxy with the following options:
 - Inbound rules:
 - IP: 127.0.0.1:9443
 - Enable SSL Offloading
 - Outbound Rules:
 - Rewrite the domain names of the links in HTTP responses
 - From: 127.0.0.1:9443
 - To: your public HTTPS domain

9. Setting up Recording Policy

The following settings must be done by a user with an administrator role in the Azure account

Open **Windows Powershell** from the **Start** menu as administrator and run the following commands (replace the fields in bold with the right values):

- *Install-Module MicrosoftTeams*
- *Import-Module MicrosoftTeams*
\$credential = Get-Credential
Connect-MicrosoftTeams -Credential \$credential
- *New-CsOnlineApplicationInstance -UserPrincipalName **UPN** -DisplayName **DisplayName** -ApplicationId **AppID***

UPN - create an account in your tenant Active Directory

DisplayName -

AppID -

this command returns an **ObjectId (P1)**

- *Sync-CsOnlineApplicationInstance -ObjectId **ObjectId***
ObjectId - (P1)
- *New-CsTeamsComplianceRecordingPolicy -Identity **RecPolicyName** -Enabled \$true -Description "**PolicyDescription**"*
RecPolicyName - choose a name for your Recording Policy (P2)
PolicyDescription - choose a description for your Recording Policy
- *Set-CsTeamsComplianceRecordingPolicy -Identity **RecPolicyName** -ComplianceRecordingApplications @(New-CsTeamsComplianceRecordingApplication -Id **ObjectId** -Parent **RecPolicyName** -RequiredBeforeCallEstablishment \$false -RequiredDuringCall \$false -RequiredBeforeMeetingJoin \$false -RequiredDuringMeeting \$false)*

RecPolicyName - (P2)

ObjectId - (P1)

*Grant-CsTeamsComplianceRecordingPolicy -Identity **TeamsUserEmail** -PolicyName **RecPolicyName***

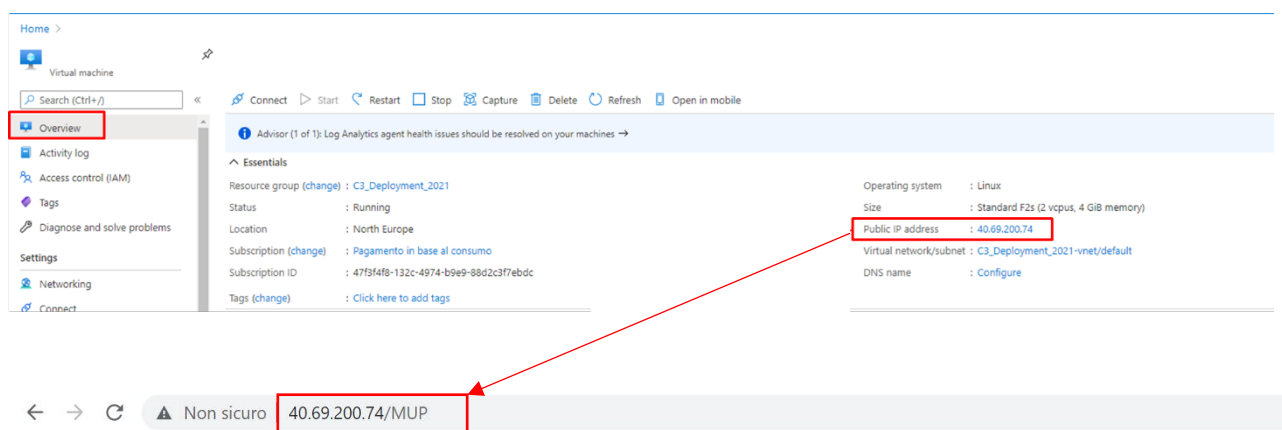
TeamsUserEmail - the email of the user you want to be recorded

RecPolicyName - (P2)

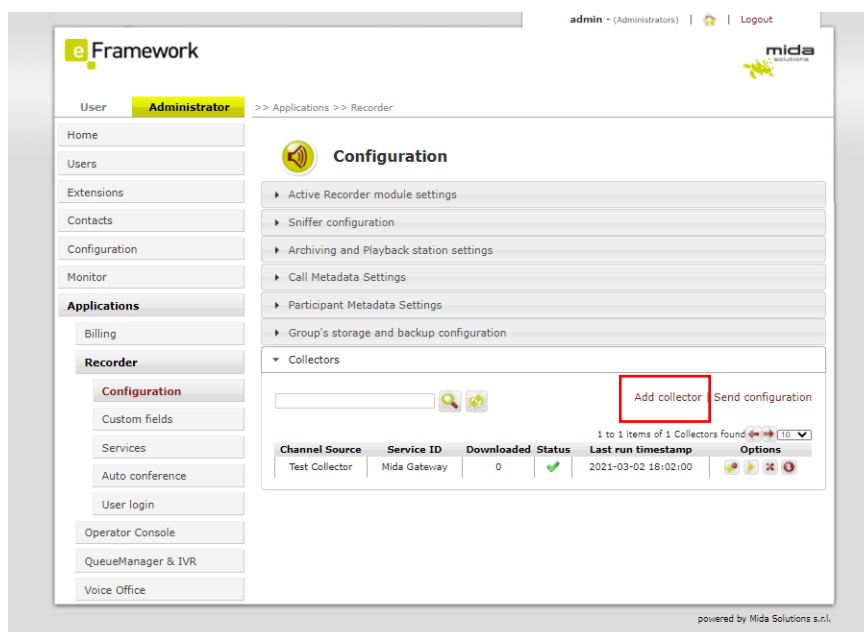
10. Add a collector

To add a collector, you need to enter in Mida Unified Portal (MUP):

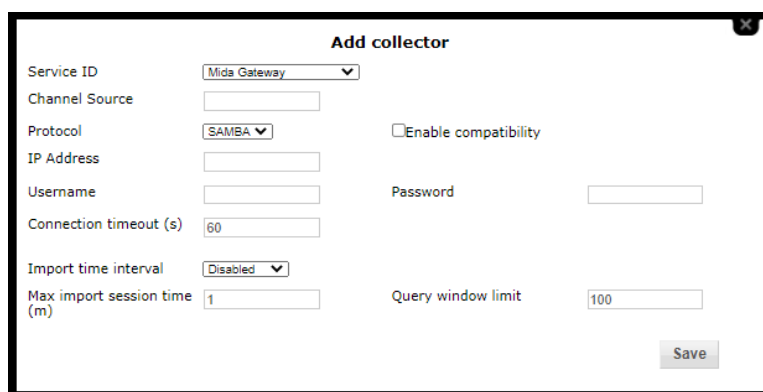
- The Virtual Machine has a Public IP address. You can find it in the overview panel as shown in the Deployment Guide. Copy and paste it into a web browser, adding “/MUP/” at the end.



- Within the MUP, click on the **Administrator** panel, click on **Recorder**, and **Configuration** and then click on **add collector**



Now you need to create and configure a Collector by clicking on the Collectors tab.



Compile the fields as shown in the picture:

- Select **Mida Gateway** on Service ID
- Select **SAMBA** on Protocol and then put the IP Address of the VM where you have just installed the Mida RecBOT, username, and password

Please, remember that the folder where the recordings will be stored must be accessible publicly.

**Notes:**

- **Channel Source:** this is a free string; you can choose what you prefer
- **Import time interval:** use one of the values proposed in the drop-down list (here 60 seconds). This is a very important field as it determines how often the collector synchronizes the recordings, uploading them to the Playback Station. Later in this guide, we will show you how to configure the Playback Station. We recommend you do NOT leave it disabled, otherwise, you will not see any recordings in the Playback Station.
- **Max import session time:** should be set proportionally to the expected number of calls to be periodically uploaded from SIPREC.

After configuring all the required fields, click on save.

11. Configure Archiving and General Settings

Go to **Applications > Recorder > Configuration** and click on the **Archiving and Playback station settings** tab.

Archiving and Playback station settings

Audio files retention period (Hours)

8760

Call logs retention period (days)

366

Delete files only if backup occurred

☐

Volume gain

1

Enable audio file compression

☐

Enable audio file encryption

☐

System encryption key

☐

Backup time interval

Disabled

Backup mode

All

Enable shared folder cleaning

☐

Share Folder

No network shares found

Backup audio file format (sniffer only)

Native audio file format

Timezone

UTC

Backup folder name

<YYYY>/<MM>/<DD>

Backup audio file name

rec_<CHSRC>_<SERVID>_<YYYY>_<MM>_<DD>_<HH>_<mm>_<ss>

Help

Advanced call filter

Show all calls by default

☐

Allow audio files download

☒

Display Convert native or encrypted audio files

☒

Encrypted audio file play mode

Require decryption key

Show timezone selector

☒

Enable waveform player

☒

Save

As a minimum, set the following two parameters:

- **Audio files retention period:** this is the time (in hours) audio files will be kept on the Archiver's storage before being deleted.
- **Call logs retention period:** this is the time (in days) information about audio files (also called metadata) are kept in the Archiver's DB before being deleted.

Other parameters you may be interested to set up are:

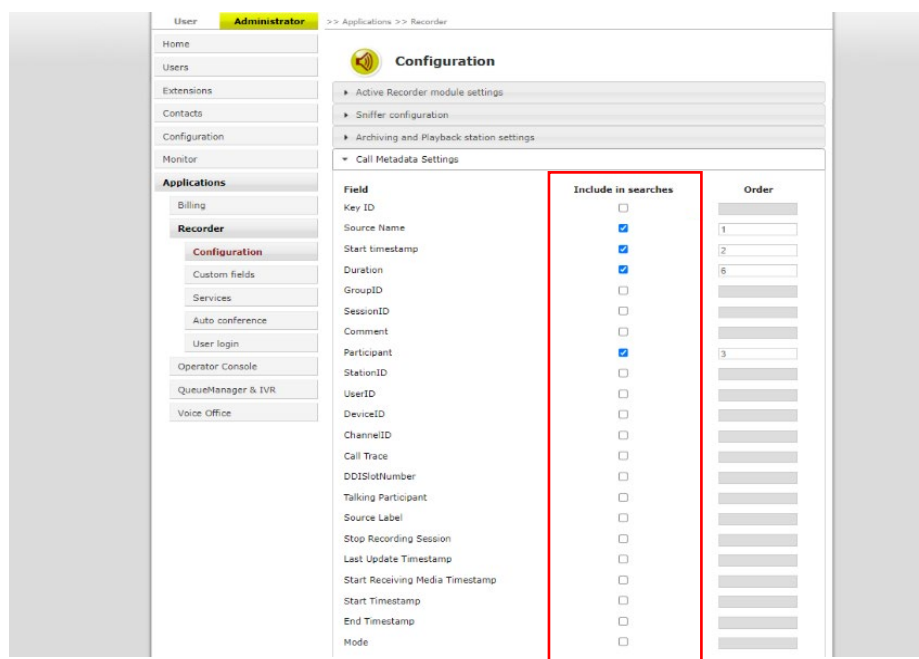
- Enable audio file encryption
- Backup parameters
- General set-up parameters for the Playback station.

For information about these parameters, and in general about this tab, please refer to Mida Recorder – Administration & User Manual.

12. Configure Metadata

Metadata is information about the call that can be extracted from the call signaling. It is possible to define at the system level which such data must be used for searching calls and which one must be displayed in the user GUI (also known as Playback Station). To do this, follow these steps:

1. Go to **Applications > Recorder > Configuration** and click on the **Call Metadata Settings** tab:



Field	Include in searches	Order
Key ID	<input type="checkbox"/>	
Source Name	<input checked="" type="checkbox"/>	1
Start timestamp	<input checked="" type="checkbox"/>	2
Duration	<input checked="" type="checkbox"/>	6
GroupID	<input type="checkbox"/>	
SessionID	<input type="checkbox"/>	
Comment	<input type="checkbox"/>	
Participant	<input checked="" type="checkbox"/>	3
StationID	<input type="checkbox"/>	
UserID	<input type="checkbox"/>	
DeviceID	<input type="checkbox"/>	
ChannelID	<input type="checkbox"/>	
Call Trace	<input type="checkbox"/>	
DDISlotNumber	<input type="checkbox"/>	
Talking Participant	<input type="checkbox"/>	
Source Label	<input type="checkbox"/>	
Stop Recording Session	<input type="checkbox"/>	
Last Update Timestamp	<input type="checkbox"/>	
Start Receiving Media Timestamp	<input type="checkbox"/>	
Start Timestamp	<input type="checkbox"/>	
End Timestamp	<input type="checkbox"/>	
Mode	<input type="checkbox"/>	



Note: the actual window is bigger, here only the upper part is shown for simplicity.

2. Locate the data you want to use for searching, and flag the **Include in searches** checkbox.
3. Locate the data you want to be displayed in the Playback Station, and flag the **Show** checkbox. By filling the **Order** textbox, you can also specify the order in which the chosen data must be displayed.
4. Once finished, click on **Save**.



Note that, even though the **Call Metadata Settings** tab displays a lot of fields, not all of them may apply to your deployment. You may want to discuss with your company's network expert to determine which ones can be used.



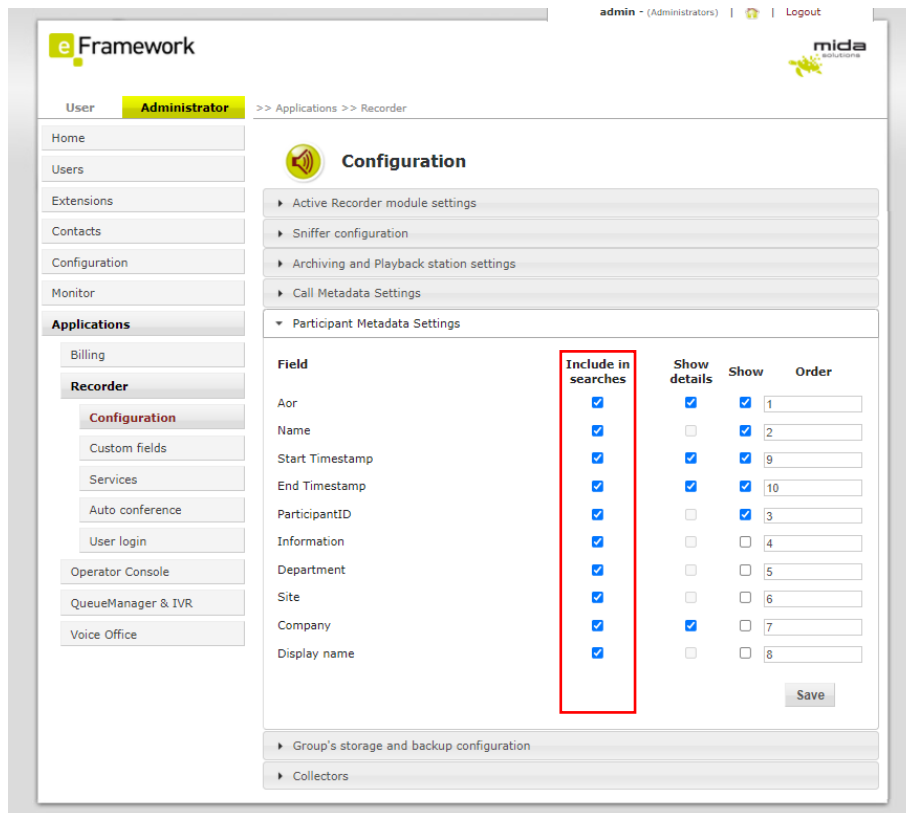
Please note that when you insert a query in the search box of the Playback Station, only the metadata flagged in the section below can be searchable.

13. Configure participant metadata

It is possible to define what information about calls' participants will be displayed on the Playback Station and used for searching calls. To do this, follow these steps:

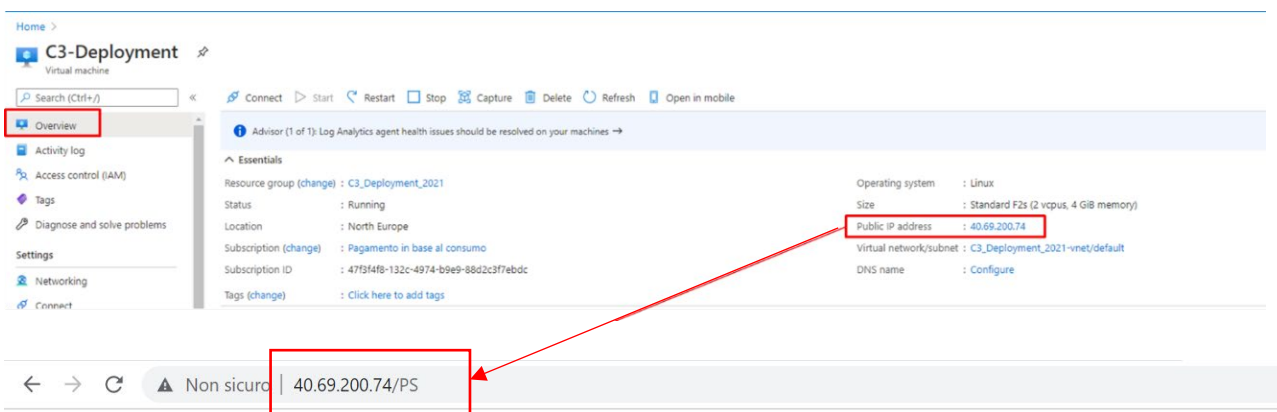
Go to **Applications > Recorder > Configuration** and click on the Participant Metadata Settings tab.

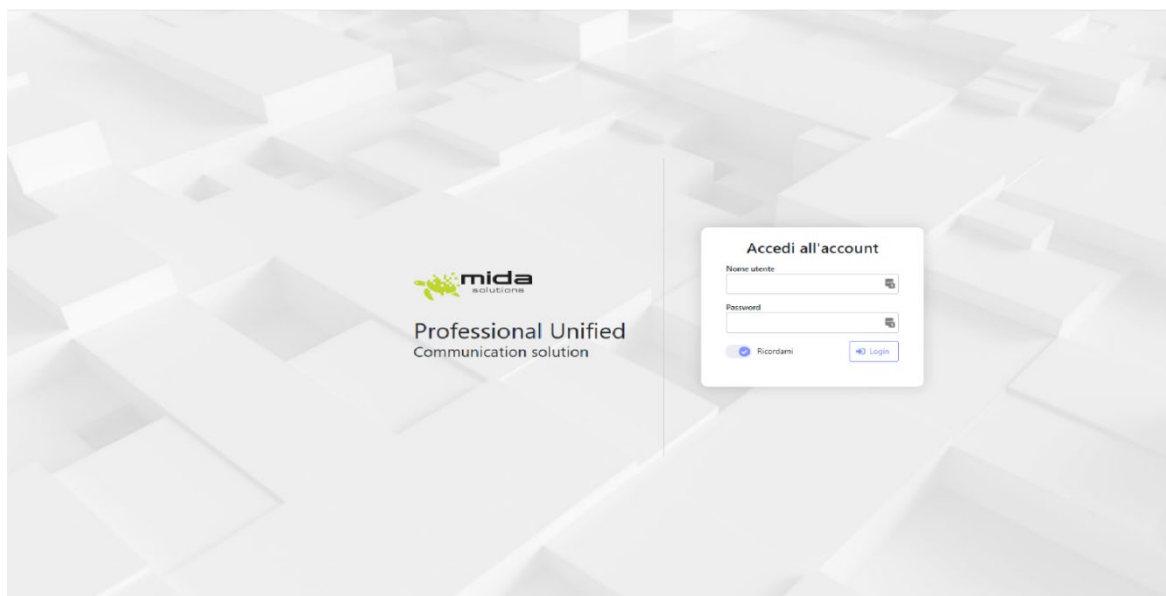
1. Locate the data you want to use for searching, and flag the **Include in searches** checkbox.
2. Locate the data you want to be displayed in the Playback Station, and flag the **Show** checkbox. By filling the **Order** textbox, you can also specify the order in which the chosen data must be displayed.
3. Once finished, click on **Save**.



14. Playback Station

To enter the Playback Station, copy the Virtual Machine Public IP address and paste it into a web browser, adding **"/PS/"** at the end of the URL, and enter your username and password.



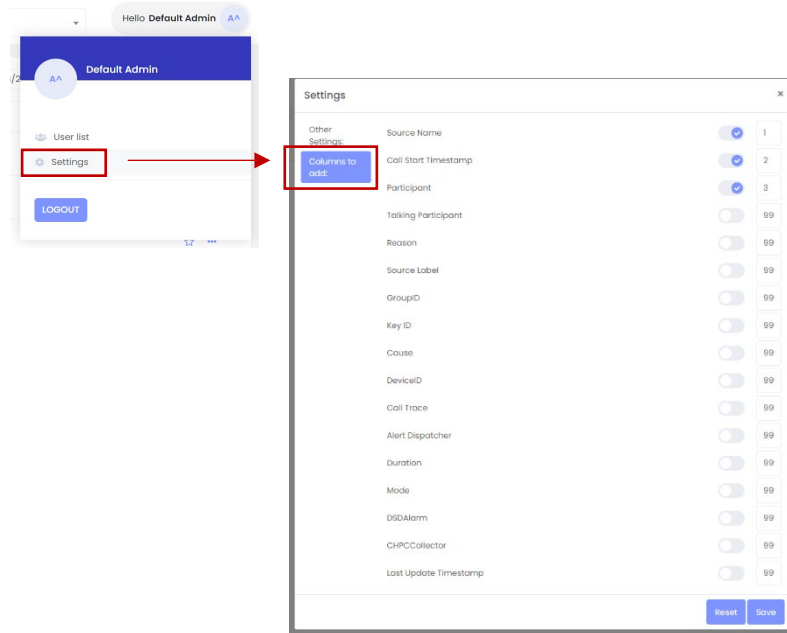


14.1 Playback Station settings

You can customize the appearance of the Playback Station homepage from **Settings**, as shown below.

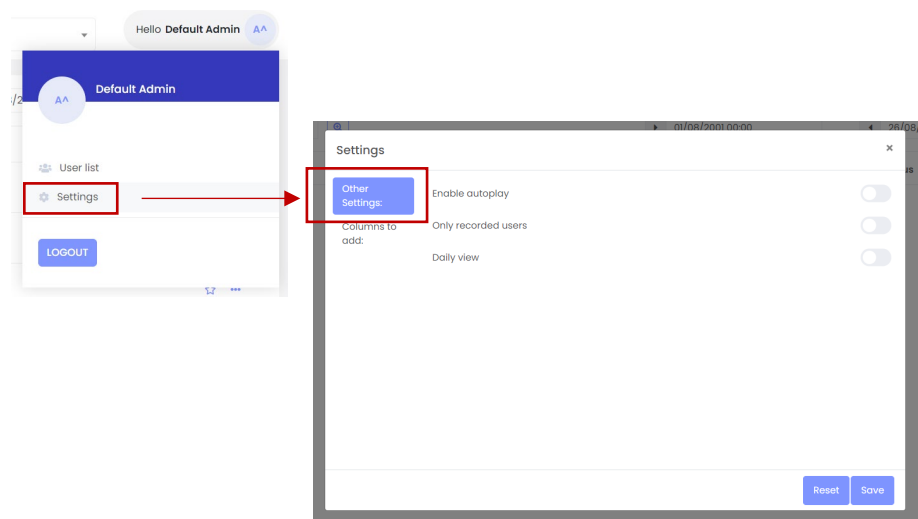
14.1.1 Change Columns

To change the columns shown on the Playback Station homepage, from **Settings > Columns to add** you can choose which column to prioritize on the Playback Station. Remember that the Actions column is fixed and you add a maximum of 5 additional columns as shown in the picture below.



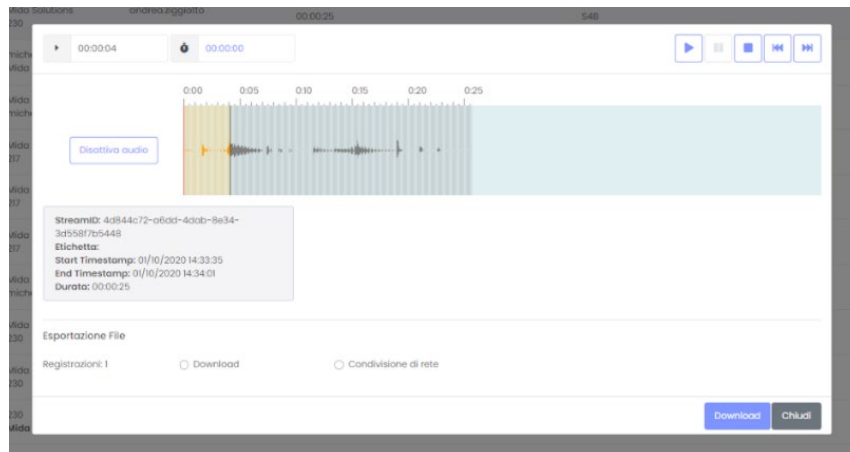
14.2 Additional settings

To customize the appearance of the Playback Station homepage, click on **Settings > Other Settings**, as shown below.



In this settings tab you can select or deselect the following options:

- **Enable autoplay**
 - if selected, when you open an audio file, it will automatically play
 - if disabled, you must click on play to listen to the file



- **Only recorded users**

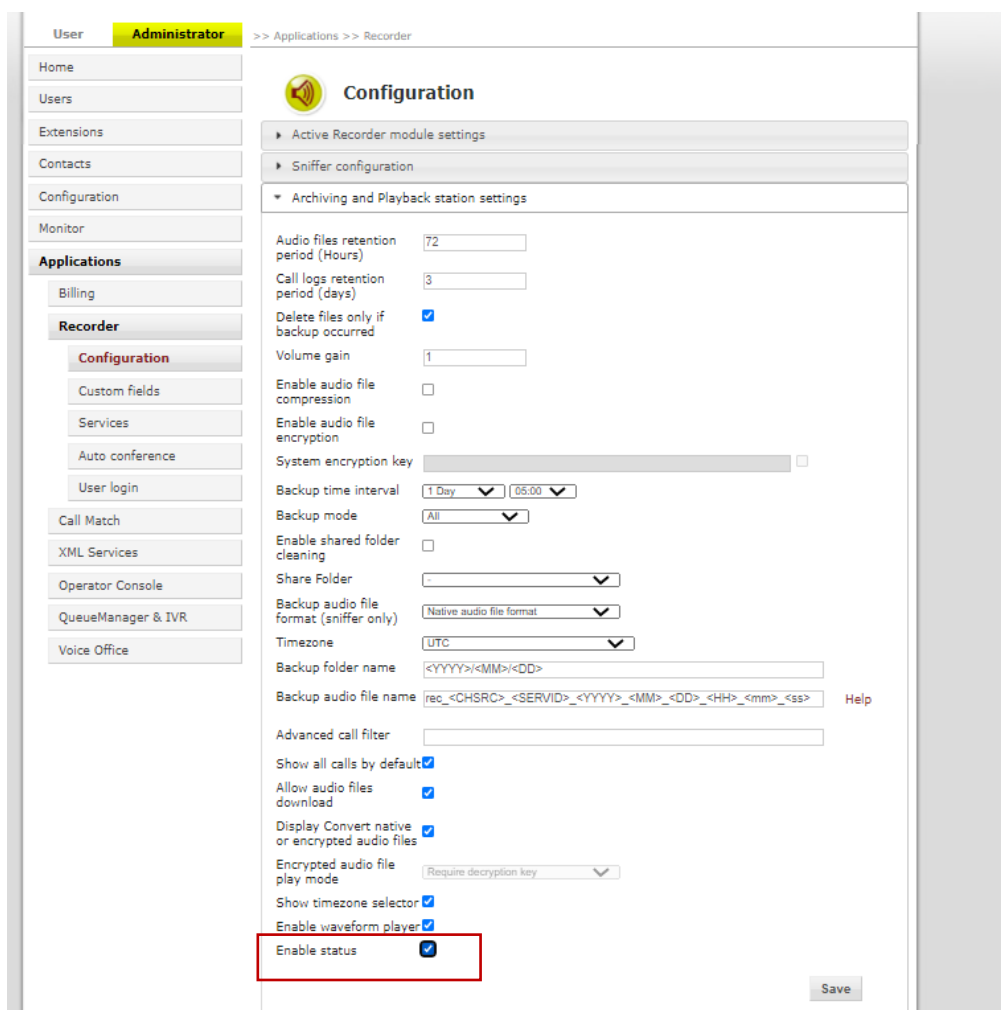
You can decide to flag as “recorded” some users (to do this see paragraph 4.1.4.5 in the Mida Unified Portal – Administration & User Manual). If selected this option allows the supervisor and administrator to view recorded users and their files.

- **Daily view**

- if disabled the Playback Station shows you the recorded calls from day 1 to the last day of the current month
- if selected the Playback Station shows you the recorded calls from the current day until the end of the month

14.2.1 Recorded file status

To view additional information about the recordings you must enable the option in the Mida Unified Portal. Login to the MUP with an administrator account and click **Application > Recorder > Configuration > Archiving and Playback Station settings** and enable “Enable Status”.



User: **Administrator** >> Applications >> Recorder
















Configuration

- Active Recorder module settings
- Sniffer configuration
- Archiving and Playback station settings
 - Audio files retention period (Hours): 72
 - Call logs retention period (days): 3
 - Delete files only if backup occurred: ☒
 - Volume gain: 1
 - Enable audio file compression: ☐
 - Enable audio file encryption: ☐
 - System encryption key:
 - Backup time interval: 1 Day 05:00
 - Backup mode: All
 - Enable shared folder cleaning: ☐
 - Share Folder:
 - Backup audio file format (sniffer only): Native audio file format
 - Timezone: UTC
 - Backup folder name: <YYYY><MM><DD>
 - Backup audio file name: rec_<CHSRC>_<SERVID>_<YYYY>_<MM>_<DD>_<HH>_<mm>_<ss> [Help](#)
 - Advanced call filter:
 - Show all calls by default: ☒
 - Allow audio files download: ☒
 - Display Convert native or encrypted audio files: ☒
 - Encrypted audio file play mode: Require decryption key
 - Show timezone selector: ☒
 - Enable waveform player: ☒
 - Enable status: ☒**

[Save](#)

Once log again into the Playback Station in the actions column you can see on the left some icons:

- Green microphone: the audio file is available
- Red microphone: the audio file is missing o Dark
- Grey microphone: the audio file has been backed up
- Green envelope: the text message is available
- Grey envelope: the text message has been backed up

Source Name	Call Start Timestamp	Participant	Actions
S4B	02/12/2020 18:52:12	maun 7b2d2b3-ee6f-46b3-93b1-e1748495a7222 160693032294 1606930348732 260 1c8c640f-c6c4-40cb-bc47-7d35632b507c 160693032294 1606930348732	  
S4B	02/12/2020 18:49:27	260 17587d2b-cdab-4105-c7ac-oad2e2d73af 1606930387222 160693037522 E202 5dd4fb7-e8b0-439b-8526-577c4263a409 1606930387222 160693037522	  
S4B	02/12/2020 18:49:01	mauro 5a688280-8837-457b-be49-5da254885 160693034925 160693034925 260 2f5d3952-900f-488b-842b-9c58982b29fd 160693034925 160693034925	  
S4B	02/12/2020 18:39:12	260 df3d899-d562-40e4-937f-8c0ac21c8f6 1606930752464 1606930766992 E202 139f542f-0032-4602-9449-7ff4334ac40 1606930752464 1606930766992	  
S4B	02/12/2020 18:38:49	mauro 1462e0d1-8f61-4a28-af28-783039583545 1606930729288 1606930743601 260 7f63863d-8a00-44a2-8a4d-685d0df02c1 1606930729288 1606930743601	  

15. Recorder Security FAQ

- **How's the authentication between Microsoft's bot and the customer's recording server done?**
The authentication is made using the JSONWebToken
- **To manage Microsoft's bot settings, what permissions are required in the tenant?**
To edit BOT configurations, the user must be registered as the owner of the resource in Azure, but after the creation, there is no need to access the configuration page
- **Is the recording media landed on the customer's recording server encrypted? If yes, how is the encryption managed?**
When recordings are saved in the recorder, the recording files are not encrypted
- **Do the Microsoft Bot services have a dedicated public IP range (to be used as source IP in our internet FW)? If yes, do we know if it's shared with other Microsoft services?**
It is not possible to have a list of IPs associated with the BOT Service because it is hosted on Azure and the IP addresses are constantly changed.
- **As we need to mention the customer's URL in the bot configuration, what happens if another office 365 client configures the customer URL in his tenant?**
The URL is configured in the BOT settings, the authentication bot uses the BOT identifier and if the token is not correct, the bot is not authenticated
- **For audit trail purposes does the recorder produce needed logs for the soc and security team?**
At the operative system level, you could use the event viewer to monitor all the operations made in the recorder machine.
We can integrate it with a database where all the calls received by the Teams recorder are stored
- **How is the connection between the archiver and the recorder securely done? Is there any authentication level?**
For this type of recorder, we support all the SAMBA version
- **Could we freely install our EDR product on the internet exposed recorder?**
It is possible to install it if it doesn't impact the behavior of the recorder