



Mida Configuration Guide

Mida Teams Compliance Recorder

Document Version: 1.2



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
1.2	02/02/2023	Minor review		

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 BEFORE YOU START	4
1.6 HOW MIDA RECORDER FOR MS TEAM WORKS?.....	4
2. Register the Bot in Azure	6
3. Open the VM ports on Azure.....	7
4. Add a Teams Channel to the Bot Service.....	8
5. Configuring authentication for the bot	10
6. Configuring API permissions for the bot	10
7. Configuring the server	11
8. Setting up Mida Bot.....	11
9. Setting up IIS.....	12
10. Setting up Recording Policy	13
11. Add a collector.....	14
12. Configure Archiving and General Settings.....	17
13. Configure Metadata	18
14. Configure participant metadata	19
15. Playback Station	20
15.1 Playback Station settings.....	21
15.1.1 Change Columns	21
15.2.1 Recorded file status.....	23
16. Recorder Security FAQ.....	25
17. Setup the cleaner.....	26
18. Multi-tenancy	26

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 NONINFRINGEMENT 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

© 2023/2025 Mida Solutions, All rights reserved.

Mida Teams Compliance Recorder

© 2023/2025 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

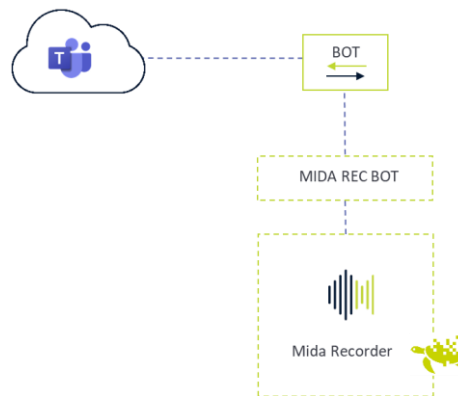


This document highlights, where possible, the main parameters and operations through **bold** or *italics* text and all parts that might be critical during system configuration or use. Critical parts are also marked with the Warning symbol reported here on the left.

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 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, and then call audio files and metadata are made available in Mida Playback Station, from where you manage the recordings.

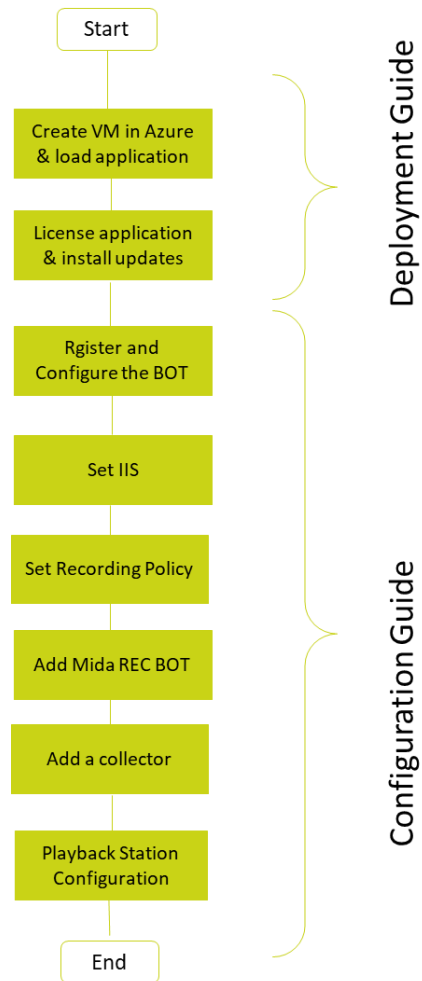


1.6 HOW MIDA RECORDER FOR MS TEAM WORKS?

The bot joins the calls you make-receive in MS Teams (both Teams to Teams, Teams to PSTN, and 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).

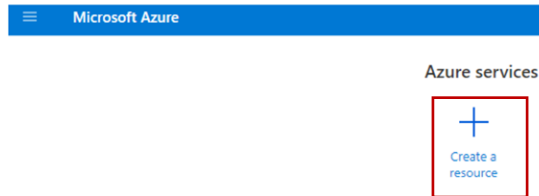
Following our instructions, you must configure a collector within Mida Unified Portal (MUP), allowing the collector to access and copy all the recorded files from the MidaRec.exe folder.

You can set your preferred backup frequency.



2. Register the Bot in Azure

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



- Click on **Create a resource**, look for **Azure Bot**, and create it.

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Bot handle * ⓘ

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Pricing

Select a pricing tier for your Azure Bot resource. You can change your selection later in the Azure portal's resource management. [Learn more about available options](#), or request a pricing quote, by visiting the [Azure Bot Services pricing](#)

Pricing tier * **Standard** [Change plan](#)

Microsoft App ID

A Microsoft App ID is required to create an Azure Bot resource. If your bot app doesn't need to access resources outside of its home tenant and if your bot app will be hosted on an Azure resource that supports Managed Identities, then choose option User-Assigned Managed Identity so that Azure takes care of managing the App credentials for you. Otherwise, depending on whether your bot will be accessing resources only in its home tenant or not, choose either Single tenant or Multi tenant option respectively.

Type of App

Note: For User-Assigned Managed Identity and Single Tenant app, BotFramework SDK (C# or Javascript) version 4.15.0 or higher is needed for these app types.

An App ID can be automatically created below or you can manually create your own, then return to input your new App ID, secret and tenant ID in the open fields. [Manually create App ID](#)

Creation type ☒ Create new Microsoft App ID ☐ Use existing app registration

- In the left panel, provide a unique name at the **Bot handle** (1)
- Select the **Subscription** based on your requirements
- (If necessary) Create a new **Resource group** for the bot so you can easily see the bill from the Azure portal
- Select the **Pricing tier** based on your requirements
- Select the **Type of App** (Single Tenant / Multi-Tenant / User-Assigned Managed Identity)
- Select the **Creation type** method based on your requirements
- Click on the **Create button**. Creating the Azure Bot may take some seconds. Azure will create an App Registration and a Bot Service assigned to it.

3. Open the VM ports on Azure

- Log in to the Azure portal
- Open the virtual machine and go under the Network tab
- Click on the button on the right in order to create inbound rules for each port reported in the following pictures (add even the Samba port if needed):

<p>Origine ⓘ Any</p> <p>Intervalli di porte di origine * ⓘ *</p> <p>Destinazione ⓘ Any</p> <p>Servizio ⓘ HTTPS</p> <p>Intervalli di porte di destinazione ⓘ 443</p> <p>Protocollo <input type="radio"/> Any <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP </p> <p>Azione <input checked="" type="radio"/> Consenti <input type="radio"/> Nega </p> <p>Priorità * ⓘ 320 ✓</p> <p>Nome HTTPS</p> <p>Descrizione</p>	<p>Origine ⓘ Any</p> <p>Intervalli di porte di origine * ⓘ *</p> <p>Destinazione ⓘ Any</p> <p>Servizio ⓘ Custom</p> <p>Intervalli di porte di destinazione * ⓘ 8445</p> <p>Protocollo <input type="radio"/> Any <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP </p> <p>Azione <input checked="" type="radio"/> Consenti <input type="radio"/> Nega </p> <p>Priorità * ⓘ 330 ✓</p> <p>Nome TeamsMedia</p> <p>Descrizione</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Origine ⓘ
Any

Intervalli di porte di origine * ⓘ
*

Destinazione ⓘ
Any

Servizio ⓘ
HTTP

Intervalli di porte di destinazione ⓘ
80

Protocollo
☐ Any
☒ TCP
☐ UDP
☐ ICMP

Azione
☒ Consenti
☐ Nega

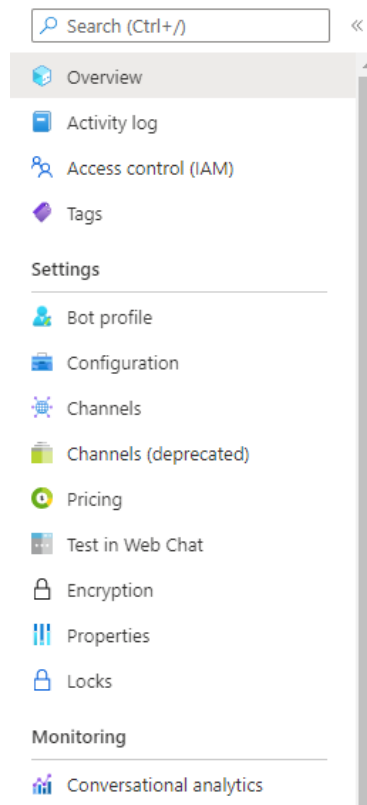
Priorità * ⓘ
340 ✓

Nome
Port_80

Descrizione
Serve per il certificato con letsencrypt


4. Add a Teams Channel to the Bot Service

- Once the Azure Bot is completed, search for it in the search box on the top.
- Under the **Settings** section, click on the **Channels** menu



- Under the **Available Channels** section, select the **Teams** icon (Configure Microsoft Teams channel)
- Select the **Calling** tab, then tick the **Enable calling** checkbox.
- At the **Webhook (for calling) (5)** 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 Bot service. At the domain part, use the domain of the Teams tenant (also specified in the SSL certificate)

Messaging **Calling** Publish

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. 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. [Learn more](#) 

☒ Enable calling

Webhook (for calling)

- Click on the **Apply** button at the bottom of the page.

5. Configuring authentication for the bot

- 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 (**bot handle**) provided during registration
- Take note of the **Application (client) ID (2)** and the **Directory (tenant) ID (4)**. They will be needed 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 note of the **new Client's secret (3)**. It will be needed later

6. Configuring API permissions for the bot

- Go to **API permissions** under **App registrations** > your bot handle > **Manage** section.
- 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
 - User.Read.All
- Click on the **Add permissions** button
- The administrator will now have to grant the added permissions for your tenant by clicking on the **Grand admin consent for your tenant**

7. Configuring the server

- Install the latest version of [VC redist x64](#)
- Create and Install a public **HTTPS** certificate under the **Personal** folder and install IIS (Setting up IIS chapter)
- Get the 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 **the Details** tab
 - Scroll through the list of fields and click **Thumbprint (6)**. Take note of this value
- Install Mida Bot Recorder using the given installer
- **Turn off the firewall (Windows Key > Windows Defender Firewall > Turn Windows Defender Firewall on or off > Turn off both private and public Windows Defender Firewall)**

Optional:

- 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)

8. 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 the “.env” file with a text editor and compile **ONLY** the following fields without spaces after the equal operator (=), leaving other fields with default values:
 - AzureSettings__BotName - fill with Azure Bot Handle (1)
 - AzureSettings__AadAppId - fill with Application client ID (2)
 - AzureSettings__AadAppSecret - fill with client secret(3)
 - AzureSettings__TenantId - fill with the Azure Tenant ID of the bot (4)
 - AzureSettings__ServiceDnsName - fill with DNS:443 where Mida Bot is installed

- AzureSettings__ServiceCname - fill with Webhook URL (5)
- AzureSettings__CertificateThumbprint - fill with Certificate Thumbprint (6)
- 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)
- AzureSettings__MaxSecondsOfSilence - fill with max seconds of silence before stopping recording the call (30)
- AzureSettings__SplittingSeconds - fill with max seconds before splitting the call (16000)
- AzureSettings__MaxEntriesParticipantDictionary - fill with the max entries of participant you want to save (default 1000)
- Save the “.env” file
- Make sure to open the following ports in the firewall
 - InstancePublicPort (e.g. 8445)
 - CallSignalingPort+1 (e.g. 9442)

9. Setting up IIS

- Download the latest version of IIS from [here](#) and install it
- Press the Windows Key and type Windows Features, and select the first entry “Turn Windows Features On or Off”.
- Make sure the box next to Web Server (IIS) is checked and complete the “Add Roles and Features” wizard.
- Download the URL Rewrite the additional package from [here](#) and install it
- Press the Windows Key and type IIS, select Internet Information Services Manager (IIS)
- In the connection, tab open your server and open the “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
 - Hostname: DnsName
- Download and open (as admin) wacs.exe from [here](#) and select the following options:
 - N (create certificate)
 - 1 (default website)
 - A (pick *all* bindings)
 - The DnsName will be shown. Press y (Continue with this selection)
 - Press y again (Open in default application)
 - The terms of the app will open. Close them and press y again (agree with the terms)
 - Enter the email that will be contacted once the certificate expires.
The certificate will be created
 - Press the Windows key and type *Manage computer certificates*.
 - Look for *teamsrecordersandbox2.onmidasolutions.com* certificate under Web Hosting>Certificate and move it (drag and drop it) under Personal>Certificate (if it’s already under Personal>Certificate, skip this step)

- Open again IIS, right-click on your Web Site, and select “Edit Bindings”
- If it’s not present, add a new binding with the following options:
 - Type: https
 - IP address: All Unassigned
 - Port: 443
 - Host name: DnsName
 - SSL certificate: Select your public HTTPS certificate
- If it’s present, edit the https binding, selecting your public HTTPS certificate as an SSL 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)...”
- Select Reverse Proxy
- It will ask if you want to go to the ARR home page, say **Yes** and Install the **Application Request Routing** extension (if not working, try visiting [Application Request Routing: The Official Microsoft IIS Site](#))
- Add a 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

10. Setting up Recording Policy

The following commands must be done by an Azure administrator

- 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 (<bot-name>@<customer-domain>)

DisplayName - (1)

AppID - (2)

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***

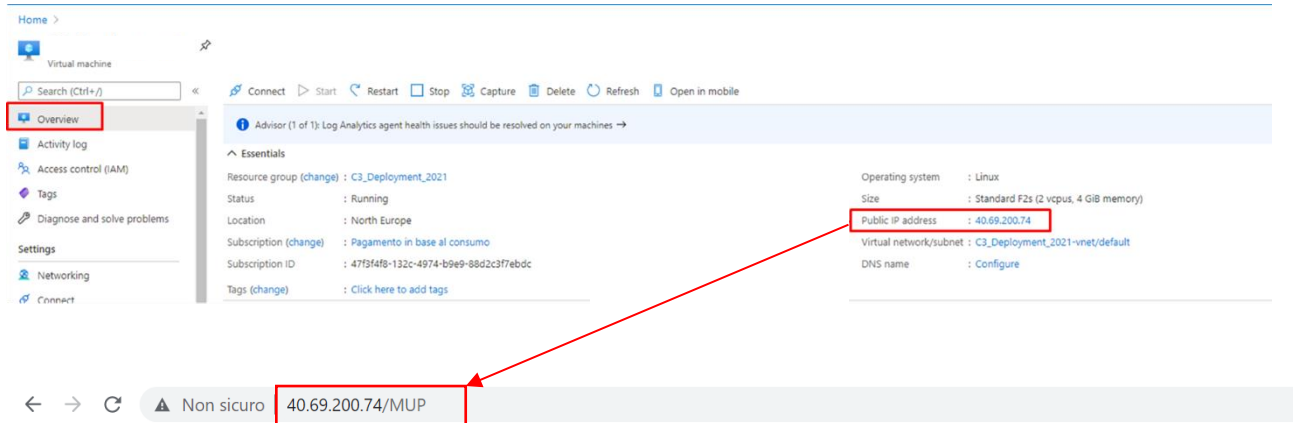
TeamsUserEmail - the email of the user you want to be recorded

RecPolicyName - (P2)

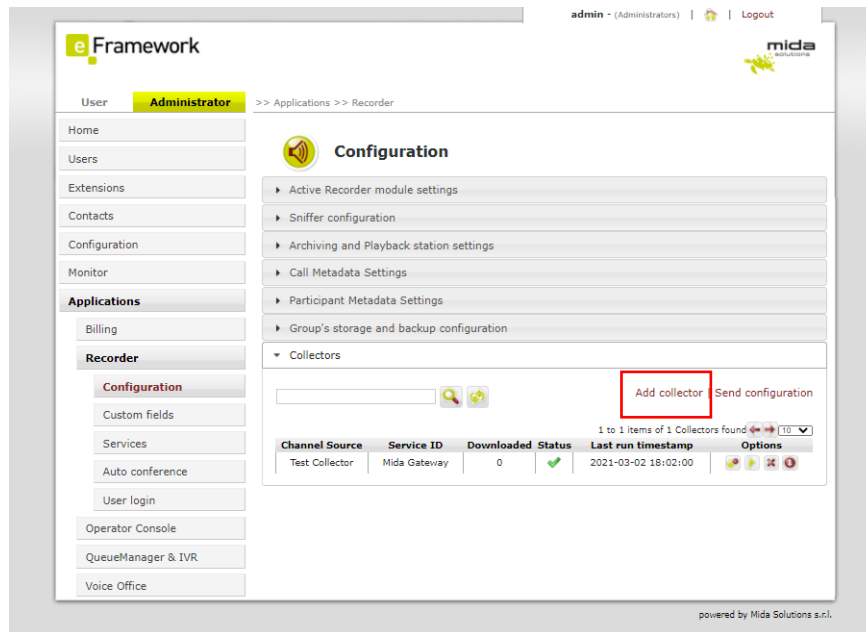
11. Add a collector

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

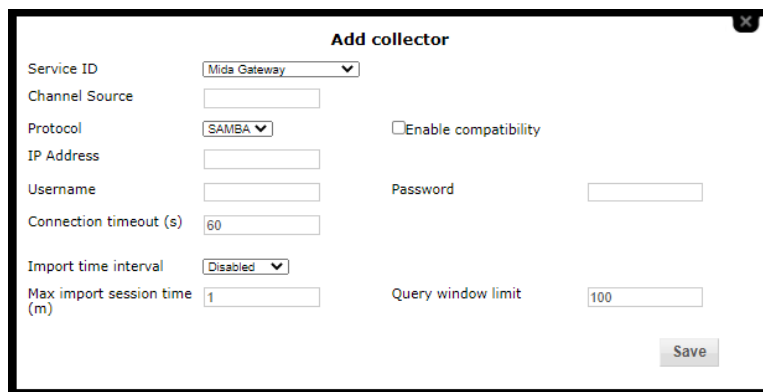
- The Virtual Machine has a Public IP address. You can find it in the overview panel as shown in the Deployment Guide. Copy and paste it into a web browser, adding “/MUP/” at the end.



- 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.

12. 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>

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

☒

Help

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) is kept in the Archiver's DB before being deleted.

Other parameters you may be interested to set up are:

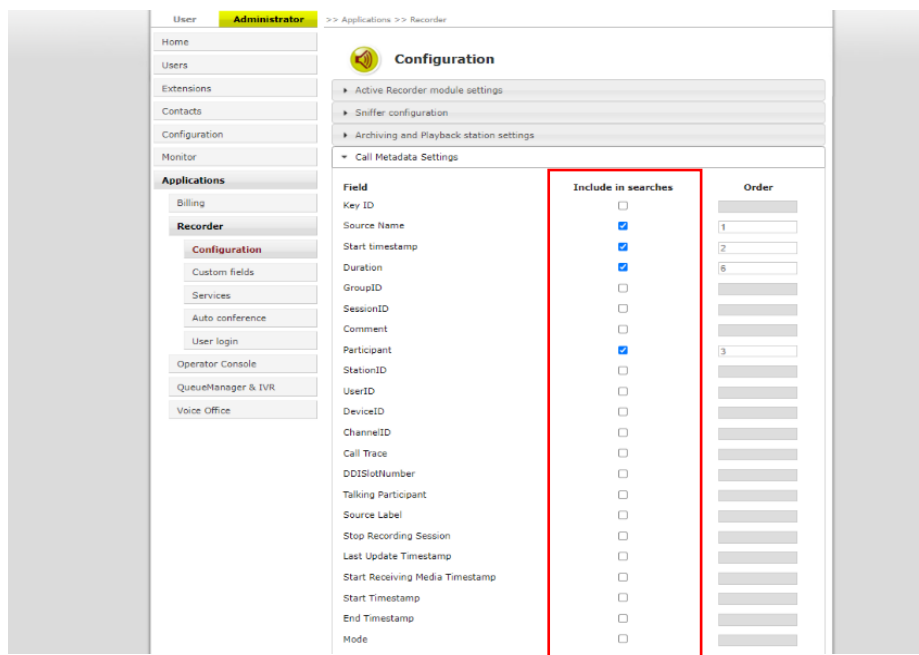
- Enable audio file encryption
- Backup parameters
- General set-up parameters for the Playback station.

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

13. 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 data must be used for searching calls and which 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"/>	<input type="text"/>
Source Name	<input checked="" type="checkbox"/>	1
Start timestamp	<input checked="" type="checkbox"/>	2
Duration	<input checked="" type="checkbox"/>	5
GroupID	<input type="checkbox"/>	<input type="text"/>
SessionID	<input type="checkbox"/>	<input type="text"/>
Comment	<input type="checkbox"/>	<input type="text"/>
Participant	<input checked="" type="checkbox"/>	3
StationID	<input type="checkbox"/>	<input type="text"/>
UserID	<input type="checkbox"/>	<input type="text"/>
DeviceID	<input type="checkbox"/>	<input type="text"/>
ChannelID	<input type="checkbox"/>	<input type="text"/>
Call Trace	<input type="checkbox"/>	<input type="text"/>
DDISlotNumber	<input type="checkbox"/>	<input type="text"/>
Talking Participant	<input type="checkbox"/>	<input type="text"/>
Source Label	<input type="checkbox"/>	<input type="text"/>
Stop Recording Session	<input type="checkbox"/>	<input type="text"/>
Last Update Timestamp	<input type="checkbox"/>	<input type="text"/>
Start Receiving Media Timestamp	<input type="checkbox"/>	<input type="text"/>
Start Timestamp	<input type="checkbox"/>	<input type="text"/>
End Timestamp	<input type="checkbox"/>	<input type="text"/>
Mode	<input type="checkbox"/>	<input type="text"/>



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 in 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.



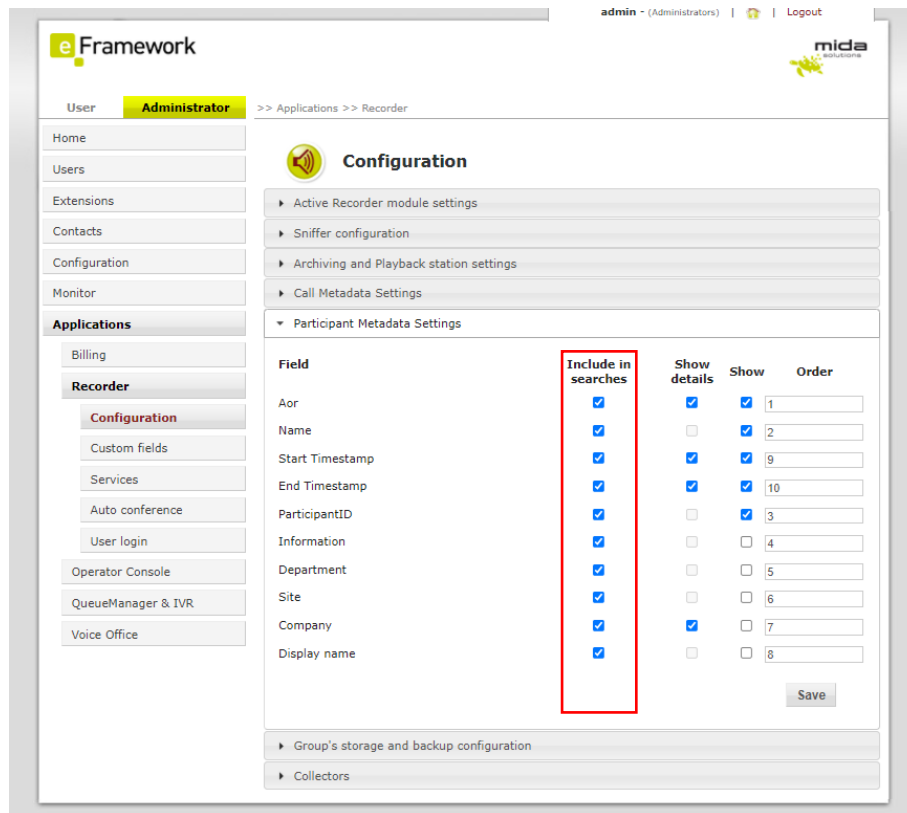
Please note that when you insert a query in the search box of the Playback Station, only the metadata flagged in the section below can be searchable.

14. 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:

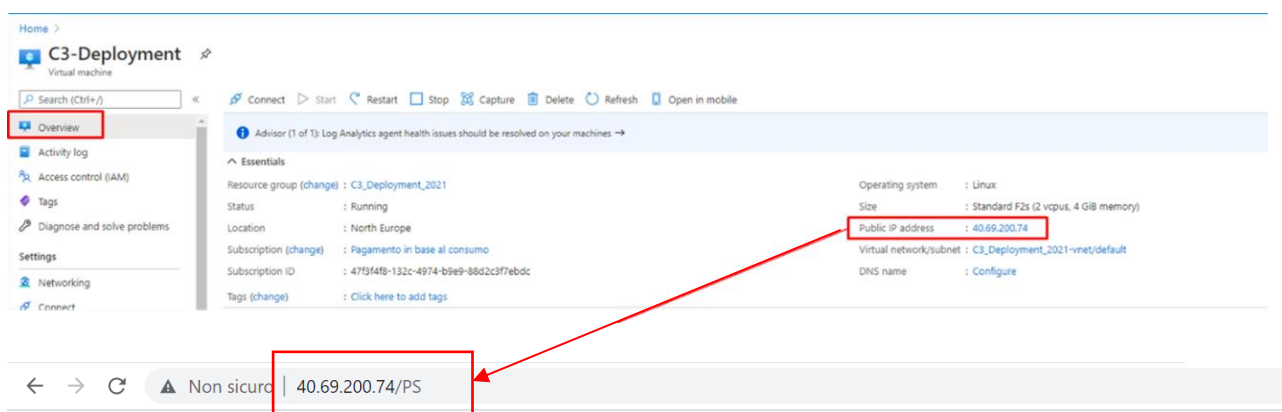
Go to **Applications > Recorder > Configuration** and click on the Participant Metadata Settings tab.

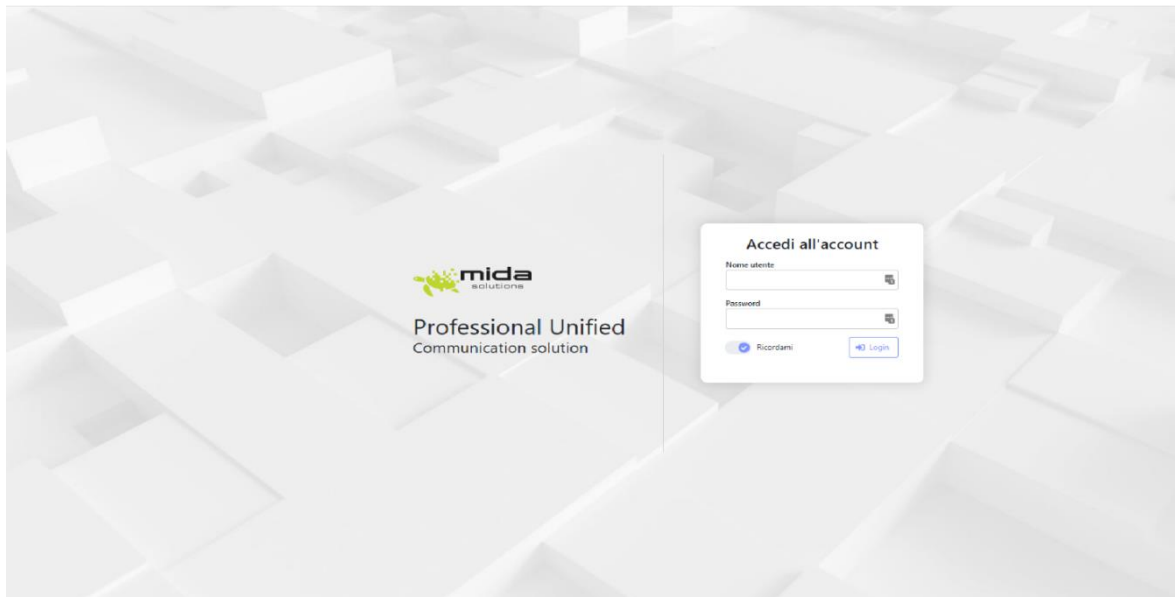
1. Locate the data you want to use for searching, and flag the **Include in searches** checkbox.
2. Locate the data you want to be displayed in the Playback Station, and flag the **Show** checkbox. By filling in the **Order** textbox, you can also specify the order in which the chosen data must be displayed.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



15. 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.



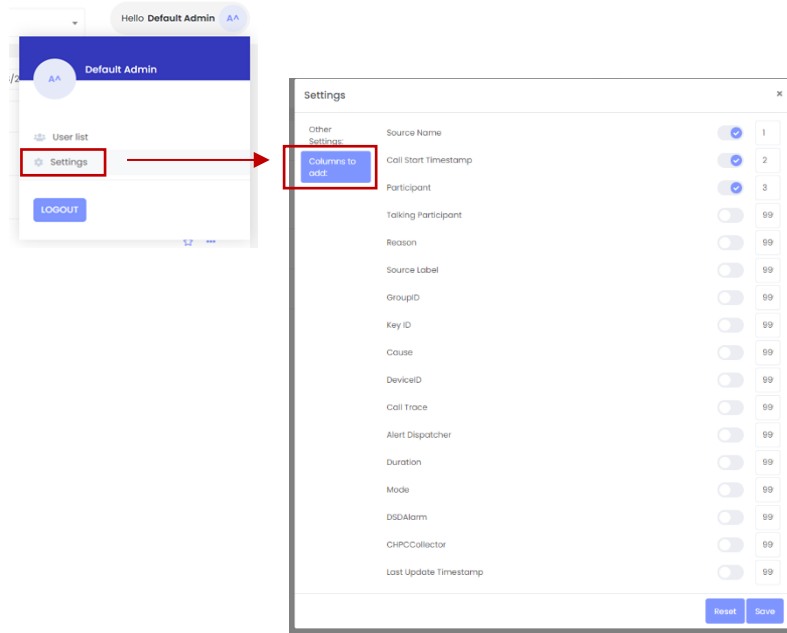


15.1 Playback Station settings

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

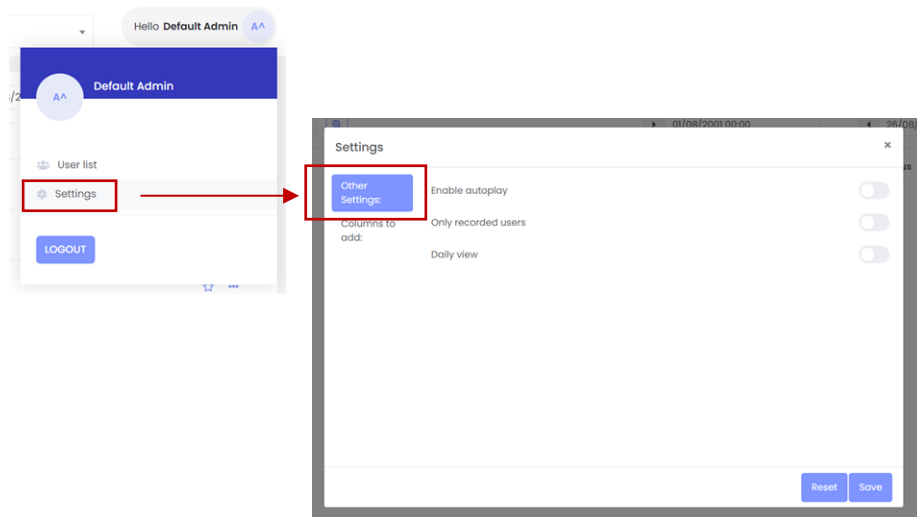
15.1.1 Change Columns

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.



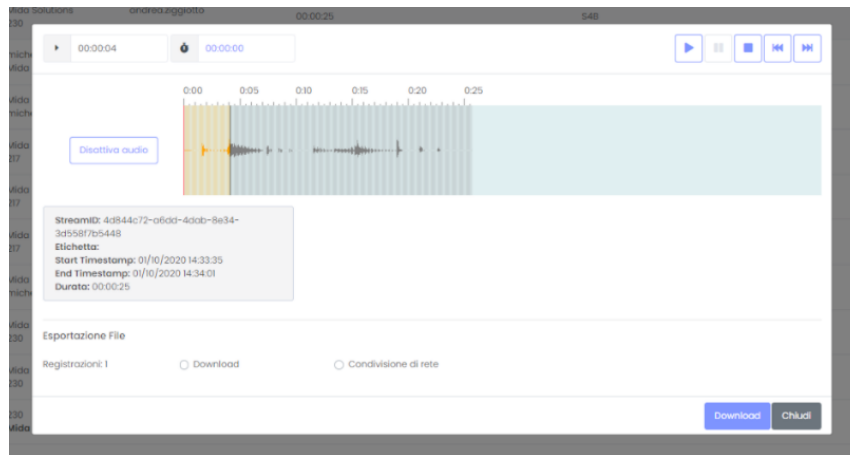
15.2 Additional settings

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**

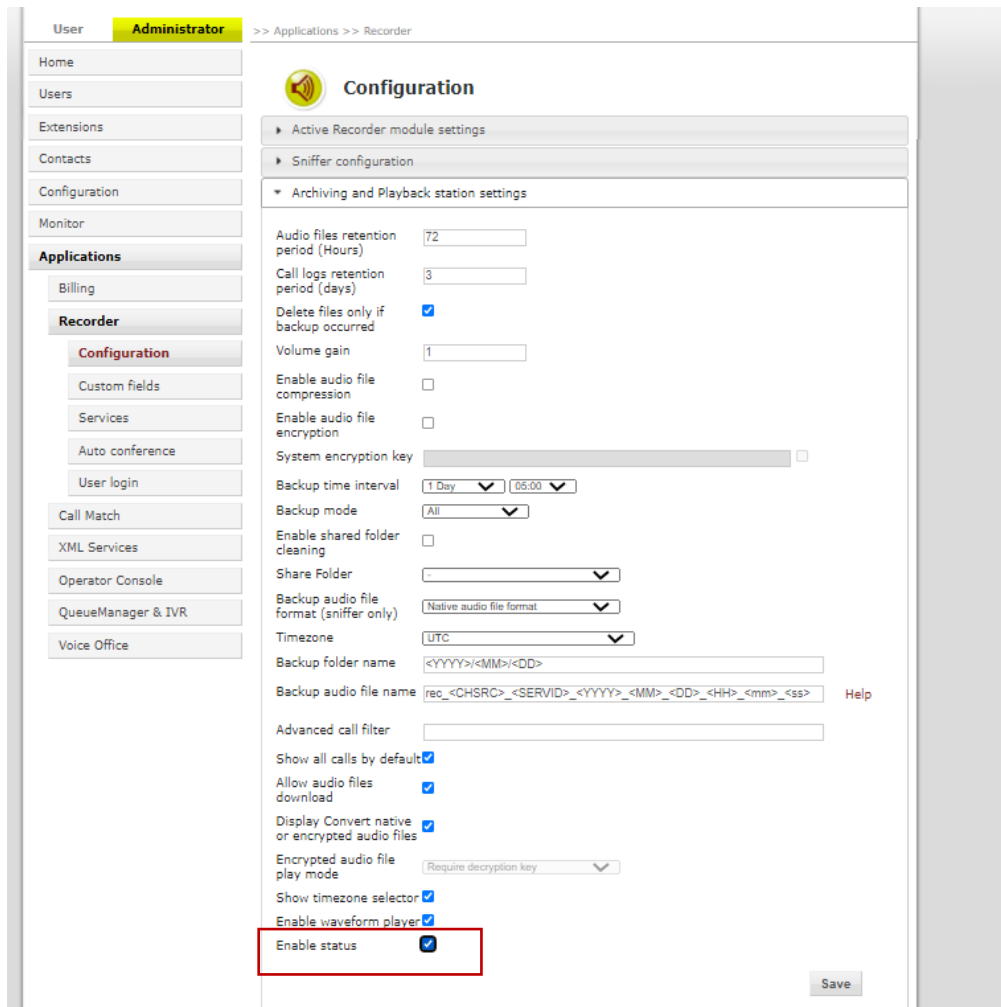
You can flag some users as “recorded” (to do this, see paragraph 4.1.4.5 in the Mida Unified Portal – Administration & User Manual). If selected this option allows the supervisor and administrator to view recorded users and their files.

- **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

15.2.1 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 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	moun 7b2d9b3-ee0f-46b3-93b1-e748495a7222 160693032294 1606930348732 260 1c6ca40f-cac4-40cb-bc47-7d39632d507c 160693032294 1606930348732	  
S4B	02/12/2020 18:49:27	260 1758702b-c8db-40b5-a7ac-0ad2a2d73af 1606930367222 1606930375022 8202 5dd4fb7-e80c-439b-8526-577c4283a409 1606930367222 1606930375022	  
S4B	02/12/2020 18:49:01	moun1 5a68838d-8837-457b-ba49-5dd254885 1606930349025 1606930349025 260 2f9d3952-300f-488b-842b-9c0b982b279d 1606930349025 1606930349025	  
S4B	02/12/2020 18:39:12	260 d73d899-d562-40a4-937f-8cc0c21c8f8 1606930752464 1606930768992 8202 139542f-0032-4602-949f-7ff4334ac40 1606930752464 1606930768992	  
S4B	02/12/2020 18:38:49	moun1 1482ee0f-8f04-4a28-0a28-78303953545 1606930729288 1606930743001 260 7b38633d-8a00-44c2-8a4d-685d0d702c1 1606930729288 1606930743001	  

16. Recorder Security FAQ

- **How's the authentication done between Microsoft's bot and the customer's recording server?**
 - The authentication is made using the JSONWebToken
- **To manage Microsoft's bot settings, what are the needed permissions for 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

17. Setup the cleaner

- **Obtain batch job right for the user:**
 - Click START and type `secpol.msc` then press Enter
 - Expand Security Settings > Local Policies > User Rights Assignment node
 - Double click `Log on as a batch job`
 - Click the Add User or Group button and add your service account user
 - Click OK
- **Open PowerShell as administrator and type:**
 - `Set-ExecutionPolicy RemoteSigned`
- Type `"taskschd.msc"` in Execute to open Task Scheduler
- Click on "Create a task" and insert "Mida Cleaning folder routine" in the name field
- Check "Run whether the user is logged on or not"
- Open the trigger section and create a new trigger
- Select the day and the time, an out-of-work time
- Open the action section and create a new action
- Select run program and enter `"Powershell.exe"`. In the optional parameter add `[PATH_ROUTINE]`

18. Multi-tenancy

To set up the multi-tenancy feature for your recorder, you will need to:

- open a web browser and log in with your Microsoft account in the Azure portal with an admin account of the tenant you want to authorize.
- build the following URL:
`https://login.microsoftonline.com/{tenant_id}/adminconsent?client_id={microsoft_app_id}&state=12345&redirect_uri={redirect_uri}`
where *tenant_id* is the Directory (tenant) ID of the account you signed in to, and *microsoft_app_id* is the Application (client) ID. Both of these IDs can be found in the Registration tab of your bot in the Azure portal. The *redirect_uri* could be any website and it's just the URL of where you will be redirected after a login (ex. ...&redirect_uri=<https://www.midasolutions.com>).

This procedure must be done for every tenant you want to authorize for the recording.