AudioCodes Meeting Solutions for Enterprises

Meeting Insights On-Prem

Installation Manual

Version 2.4

audiocodes

Table of Contents

Notice iv

Security Vulnerabilities iv
WEEE EU Directive iv
Customer Support iv
Stay in the Loop with AudioCodes iv
Related Documentation iv
Document Revision Record v
Documentation Feedback vi

1 Meeting Insights On-Prem Customer Pre-Installation Requirements Guideline 1

1.1 Introduction 1
1.2 Software for Downloading and Execution of Organization Security Procedures 1
1.3 Preparing the Machine 2
1.4 POC Firewall / Port Access Requirements 3
1.5 Software Preparation for Installation 4
1.6 Customer Environment Readiness Validation Scripts 5
1.7 License 5
1.8 Environment Readiness Notification 6

2 Meeting Insights On-Prem Linux Docker Installation 7

2.1 Introduction 7
2.1.1 Goto Installation Directory 7
2.1.2 Extracting the tar.gz Installation Files 7
2.1.3 Running the Installation Script 7
2.1.4 Updating Certificates (if Non Self Signed Certificates Are Provided) 9
2.1.5 Configuring Web Pages Access (Optional) 9
2.1.6 Restarting Meeting Insights On-Prem 10
2.1.7 Exchanging Additional Configuration Needed 10
2.1.8 Installing License File Via Browser 10
2.1.9 Adding Users to Tenant 11
2.1.10 Adding Docx Template 12
2.1.11 Configuring Recording Bot 13
2.2 Basic functionality tests 14
2.2.1 Checking Offline Client 14
2.2.2 Checking Recording Client 14
2.2.3 Checking Dictation Client 15
2.3 Upgrading Procedures 16
2.3.1 Upgrading the Backend Images 16
2.3.2 Upgrading the Clients 17
2.3.3 Upgrading the STT/NLP Factories 18

3 Troubleshooting 19

3.1 Introduction 19

3.2 Issues Found 19

3.2.1 Docker-Load Errors: 19

3.2.2 Keycloak+Maria-DB Issue on Some Linux Distros 19

3.2.3 Nginx responds with “Forbidden” on any request sent to the /html folder, and logs “permission denied” on the error.log file 19

3.2.4 Linux Machine Goes to Sleep or Hibernates 19

A Appendix: Meeting Insights On-Prem Gemalto License Server 21

A.1 Introduction 21

A.2 Getting Started 21

A.3 Installing License Server 21

A.3.1 Installing the License Application on a Dedicated Linux Server 21

A.3.1.1 Prerequisites 21

A.3.1.2 Installation 22

A.3.1.3 Un-Install Procedure 23

A.3.2 Receiving Machine Fingerprint and Uploading Generated License Key 24

A.3.3 Validating Uploaded License Key 24

B Appendix: Meeting Insights On-Prem License 25

B.1 Overview 25

B.2 Installation 25

B.2.1 Prerequisites 25

B.2.2 Installation Steps 25

B.2.2.1 Zip file content 25

B.2.2.2 Linux Installation Steps 26

B.2.3 Uninstallation Steps 27

B.2.4 Configuration File 27

B.3 Get System ID 28

B.4 API Endpoints 28

B.5 Authentication 28

B.6 Available Functions 28

B.6.1 Troubleshooting 30

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: June-11-2025

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Related Documentation

Document Name
Meeting Insights On-Prem Release Notes

Document Revision Record

LTRT	Description
26012	Initial document release (Version 2.0)
26027	Updated to Version 2.2
26028	Updated to Version 2.4

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

1 Meeting Insights On-Prem Customer Pre-Installation Requirements Guideline

1.1 Introduction

This document outlines the steps that must be taken by the Customer before beginning the installation of Meeting Insights On-Prem at a customer site. These steps should be executed following the commercial engagement required to obtain the download link and license key. The instructions and requirements detailed in this document must be completed to ensure a smooth and successful installation at the customer's site.

1.2 Software for Downloading and Execution of Organization Security Procedures

The Meeting Insights On-Prem software must be downloaded using the provided link (see Table 1 and Table 2) and must comply with the organization's security procedures.

Table 1: Linux Installation components

#	Image Name	Contains
1	miaop_setup-2.4.x.zip	Meeting Insights On-Prem installation package

Table 2: License Manager package components

#	Image Name	Contains
1	License Manager Package	■ Gemalto License Server ■ GetMachineNumber ■ MiaOPDecodeLicenseServer ■ Installation manuals

1.3 Preparing the Machine

The Customer must prepare the environment in accordance with the specifications below:

Table 3: HW specification

VM	vCPU	RAM [GB]	HDD [GB]	OS
APP and Cognitive Services	16	72	500	Linux Rocky 9 / RHEL 9 or equivalent

POC terms and conditions:

- **License**:
  - **Period**: 45 days
  - **Max hours of audio**: 1,000
- **Max concurrent sessions**: - 4
  - **Online sessions**: 2
  - **Offline sessions**: 2
- **Processor**: x64 Instruction Set Architecture (ISA), AVX2 support, Min. 2GHz.

Ensure machine time is synchronized across all servers/containers.

Environment pre-installation requirements

Table 4: Pre-installation requirements

#	Requirements	To be prepared	Notes
1	Linux Servers for dockers deployment	Docker CE (community edition) ■ Docker version must be 27.5.0 and above ■ Docker compose version must be 2.32.3 and above To be installed:	During the Linux installation, the following packages must be installed from the customer's own repository using standard Linux tools.
		Use for the installation: ■ **sudo dnf install <package name>** for Rocky ■ **sudo apt install <package name>** for Ubuntu	Use for the installation: ■ **sudo dnf install <package name>** for Rocky ■ **sudo apt install <package name>** for Ubuntu
		Packages required: ■ docker-ce ■ docker-ce-cli ■ containerd.io Docker utility permissions must be available to the Linux user.	Packages required: ■ Openssl (latest) ■ Vim ■ Nano ■ telnet ■ MC ■ Unzip ■ TR ■ Sed ■ Curl ■ Awk ■ Bind-utils (nslookup, dig) ■ dmidecode

#	Requirements	To be prepared	Notes
2	Windows workstation (used for AudioCodes Professional Services personnel and is not a part of the deployment)	**Software** ■ Chrome version 108 and above ■ Wireshark ■ Putty ■ Notepad++ ■ 7zip / Winzip ■ WinSCP **Hardware** ■ Microphone ■ Speakers	The Customer should provide a workspace with a Windows workstation for the AudioCodes installation team to use during deployment and for handling support issues.
3	FQDN Certificates	1. Prepare a valid FQDN for the servers and obtain official certificates (tls.crt, tls.key) from a well-known certificate authority. 2. Generate an authority-signed certificate based on the machine's FQDN. 3. Ensure that all browsers used to connect to Meeting Insights On-Prem have this certificate installed in their trust store. 4. Certificate format: Pem Certificate + private key	**Certificate Requirements:** ■ Format: PEM certificate + private key ■ The FQDN in the certificate must use lowercase characters only ■ The installation package includes a self-signed certificate by default ■ If company policy prohibits the use of self-signed certificates, the Customer must prepare an FQDN and provide an official certificate from a recognized authority ■ A wildcard certificate may be used as an alternative to multiple individual certificates **Note:** It is essential to ensure that the server FQDNs are resolvable by DNS before beginning the installation process.
4	Selinux	Selinux must be disabled on the provided Linux machines	

1.4 POC Firewall / Port Access Requirements

The solution requires dedicated ports to access Meeting Insights On-Prem via the Web/Telephony. The following ports must be configured on the customer premises to allow access to Meeting Insights On-Prem:

Table 5: Firewall requirements

Required Port(src - dest)	Notes
443 (any- Meeting Insights On-Prem)	internal and external
8443 (any – Meeting Insights On-Prem)	internal and external
1947 (any – Meeting Insights On-Prem)	internal and external (Gemalto license)
25/2525 (Meeting Insights On-Prem– mail server)	Port used by Meeting Insights On-Prem

1.5 Software Preparation for Installation

On the Linux machine, perform the following steps:

1. After successfully validating the zip file, copy it to the `/home/<user>/` directory on the installation machine.
2. Log in as a regular user who belongs to the **sudoers** group and does not require a password to elevate privileges.

Meeting Insights On-Prem installation package:

1. Unzip the **miaop_setup** zip file to create a sub-folder named **miaop_setup**.

```
unzip miaop_setup-2.4.x.zip
```

2. Navigate to the directory miaop_setup:

```
cd ~
cd miaop_setup
```

3. Extract the prerequirement tar.gz file.

```
tar -xvzf prerequirement_scripts.tar.gz
```

4. Navigate to the directory prerequirements folder:

```
cd prerequirement_scripts
```

5. Run the script **check_all.sh** (see section 1.6 "Customer Environment Readiness Validation Scripts" for detailed instructions).

```
./check_all.sh
```

6. Review the script output on screen for any error messages marked in red or yellow, and correct the issues as needed.
7. If the check completes without errors, proceed with the installation.
8. If issues remain, consult with AudioCodes support using the generated log file **script.log**.

License Manager Package:

1. Unzip the **License Manager package.zip** file included in the MiaOpInst zip archive.

   This package includes two modules to be installed:

   - Meeting Insights On-Prem License server
   - Gemalto License server
2. Follow the procedures described in the Appendix for both modules.

1.6 Customer Environment Readiness Validation Scripts

This section describes how to use the validation script that checks system prerequisites and verifies the integrity and correctness of the provided installation files.

The script is located in the folder: **/home/<user>/miaop_setup/prerequirement_scripts** It is executed using the master script: **`check_all.sh`**

> The scripts must have execution permissions. If they are not executable, run the following command:
>
> **chmod +x /home/<user>/MiaOpInst/scripts /*.sh**

- **Usage**: execute "sudo check_all.sh"
- **Output**: script.log file and displayed on the screen

Results are displayed on the terminal with color-coded statuses:

- **Pass:** white, black, and green
- **Fail:** yellow and red

A log file named script.log is generated in the same directory. The **script.log** file helps the Customer verify the environment and identify any mismatches that require correction.

Next Steps

1. The Customer is requested to send the script.log file to AudioCodes for review.
2. Installation may proceed once the environment passes validation and AudioCodes confirms readiness for deployment.

1.7 License

The system is licensed with the following license keys:

Table 6: Used licenses

	License type	Installation	Description	Procedure
1	Meeting Insights On-Prem license	Linux Rocky 9 / RHEL 9 or equivalent	Based on the number of transcription hours and expiration date. (see section B.2 "Installation")	**Stage 1:** On the License Server, run the **GetMachineNumber**.sh script provided by AudioCodes. **Stage 2:** Send the generated **FT_DATA.txt** file to AudioCodes. **Stage 3:** Install the **MiaOpDecodeLicenseServer** application.
2	Gemalto License	Linux Rocky 9 / RHEL 9 or equivalent	Based on STT features, number of concurrent connections (see section A.3 "Installing License Server")	**Stage 1:** Install the **Gemalto License** application. **Stage 2:** From within the application, generate and send the **xxx.C2V** file to AudioCodes.

Please refer to the Meeting Insights On-Prem and Gemalto license installation documents for instructions on installing the license applications. Use the installed applications to extract the system files required for license generation and provide these files to AudioCodes. AudioCodes will generate the corresponding licenses and return them for system authorization.

1.8 Environment Readiness Notification

1. Once the environment is fully prepared and all validation tests have passed, the Customer should notify the AudioCodes Project Manager that the system is ready for deployment.
2. The AudioCodes Project Manager prepares the work plan, including the deployment schedule, and coordinates the activity with the assigned AudioCodes Professional Services Engineer.

2 Meeting Insights On-Prem Linux Docker Installation

2.1 Introduction

This section describes the installation procedure for the Meeting Insights On-Prem solution in a Docker environment.

The installation is performed using a command-line script that deploys the entire solution for a POC (Proof of Concept) on a Linux machine running either **Rocky** or **Ubuntu** distributions.

It is assumed that all prerequisites described in the environment preparation document have been met, and the installation files have been delivered to the target machine.

Once installation is complete, refer to the *User Manual* for configuring users and tenants.

2.1.1 Goto Installation Directory

In the Linux user's home directory, the Customer should have created a folder named **miaop_setup** (assuming you are logged in as the Linux User).

Navigate to the directory:

```
cd ~
cd miaop_setup
```

2.1.2 Extracting the tar.gz Installation Files

There are 3 installation files which we need to extract with the tar command.

```
tar -xvzf containers_app*.tar.gz
tar -xvzf containers_rcgn*.tar.gz
tar -xvzf setup_miaop_all_*.tar.gz
```

2.1.3 Running the Installation Script

Goto installation folder and execute the installation script:

```
cd setup_miaop_all/install/
./install.sh
```

Upon execution, the script prompts for the following input:

1. Do you want to install AI LLM on this computer? [y/N]:

   If it is required to install the LLM on the same machine you should answer yes but note that there are some pre-required drivers that should be installed and the installation checks if the required drivers are installed.

2. Please enter MIAOP_HOME directory: /ac

   /ac is the default installation directory and just pressing enter will install the application on the default directory.

3. Please enter MIAOP_DISK directory: /acdisk

   /acdisk is the default installation directory and just pressing enter will configure the disk application on the default directory.

4. Enter the **Fully Qualified Domain Name** (FQDN) of this machine:

- Must be valid and resolvable by the customer's DNS to the IP address of the installation machine.
- *Example:* miaop.example.com

5. Enter the FQDN (or IP) of LLM machine (or empty string to disable):

   Must be a valid fqdn or I.P address of the LLM server used by the MiaOP.

   Example: 116.171.93.230

6. Enter the **tenant** name(s) (comma-separated):
   - Provide one or more tenant names, separated by commas.
   - *Example:* tenant1,tenant2
7. Keycloak admin user:

   Provide the master admin user name to the system (default provided "adm").

   Example: Administrator

8. Keycloak admin password:

   Provide the master admin password to the system (default provided an auto generated password).

   Example: xCf56G6

9. Enter the SMTP server address:

   Provide the smtp server address provided by customer.

   Example: smtp.mail.com

   note: if not provided there will be no mail support.

10. Enter the SMTP server user:

    Provide the smtp server user credentials provided by customer. (Shown only if smtp address provided)

11. Enter the SMTP server password:

    Provide the smtp server password credentials provided by customer. (Shown only if smtp address provided)

12. Enter the email address of the sender:
    - Provide the smtp server user email that is used for sending mails, also should be provided by customer. (Shown only if smtp address provided)
13. The installation is built from 2 parts:
    - Part 1 executed with the "install.sh" command:

      This part will load the containers images and will make the necessary setup, after this is done and before loading the client containers the installation prompts the user for pause the installation to copy certificate files.
    - Part 2 that is executed with the "setup.sh" command

      This part will install the data containers (factory's and web clients) and will reset the DBs.

      When the installation part 1 is finished it asks the user either to continue automatically to part 2 or hold the installation for certificate replacement (the installation generates self-signed certificates which should be replaced by a known authority certificates provided by customer).

    In this part the user can either pause the installation and copy the certificate files (continue from the same folder with setup.sh command) or ignore this request and select to not pause and continue with the installation.

The user may copy the certificate files after the installation (which will require restart of Meeting Insights On-Prem)

The installation process takes approximately 8 minutes. Upon completion, a confirmation message is displayed.

If any errors occur during installation, a log file named **installation.log** is generated. This file can be used to identify the source of the issue.

14. **Important Note:** At the end of the installation process the user MUST execute the below command to set the environment variables:

```
source ~/.bashrc
```

2.1.4 Updating Certificates (if Non Self Signed Certificates Are Provided)

If the Customer provides officially signed TLS certificates, copy them to the following folder:

```
/ac/certs
```

Ensure the following file naming conventions:

- Certificate file: `tls.crt`
- Private key file: `tls.key`

2.1.5 Configuring Web Pages Access (Optional)

The Meeting Insights On-Prem system can be accessed through a web interface that allows users to log in to different tenants via the main page URL.

1. Main Page URL:
   ```
   https://<main-url>/offline_client/
   ```
2. Hiding the Tenant List:
   If the Customer prefers not to display the tenant list, edit the .env file and set the following parameter:
   ```
   EXPOSE_TENANTS_LIST=false
   ```
3. Accessing Tenants When List Is Hidden:
4. If **EXPOSE_TENANTS_LIST** is set to **false**, the tenant list will not be shown on the main page. Tenants can be accessed by:
   - Entering the tenant name manually in the text field on the login page
   - Using a direct URL:
     ```
     https://<main-url>/offline_client?tenant=<tenant-name>
     ```
5. Accessing the master Tenant:
   ```
   https://<main-url>/offline_client?tenanat=master
   ```

Changes in the .env file require restarting the Meeting Insights On-Prem system.

2.1.6 Restarting Meeting Insights On-Prem

To restart the system, follow these steps:

1. Navigate to the /ac directory:

```
cd /ac
```

2. Stop and restart the Docker containers:

```
docker compose down
docker compose up -d
```

> Alternatively, you can run the provided script that performs the same actions:
> `./restart.sh`

2.1.7 Exchanging Additional Configuration Needed

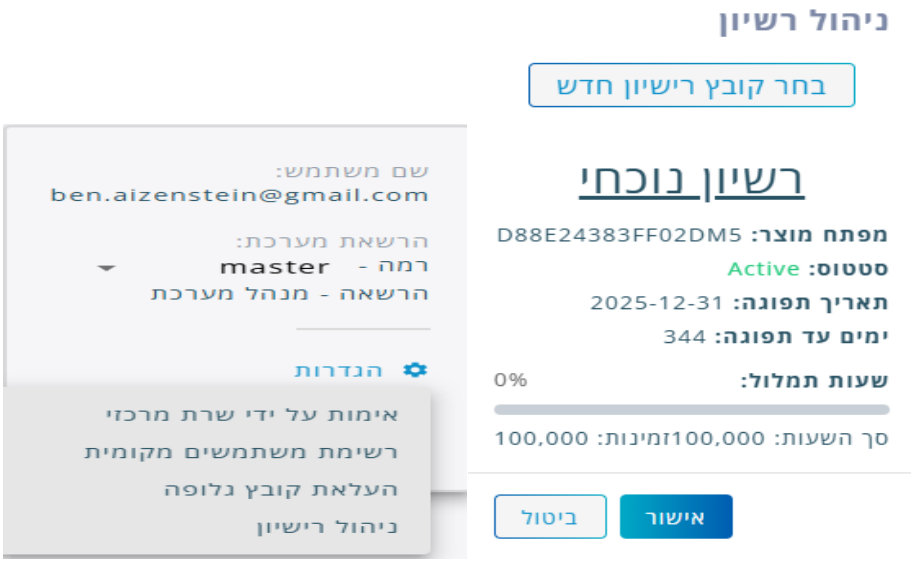
If the Customer uses **Microsoft Exchange** as the mail server for sending emails from the Meeting Insights On-Prem system, the following configuration steps are required:

1. Open the Exchange ECP (Exchange Control Panel).
2. Navigate to the appropriate section for receive connectors or mail flow settings (depending on Exchange version).
3. Add the IP address of the Meeting Insights On-Prem application as an authorized receiving client.

2.1.8 Installing License File Via Browser

To install a license file through the web interface:

1. Log in to the **Master Tenant** using an administrator account.
2. Click your **email address** located in the top-left corner of the interface.
3. Select **Settings** from the dropdown menu.
4. In the settings menu, click **Management License**.
5. Click **Select New License** and upload the provided license file.
6. Review the license details and click **Confirm** to complete the installation.

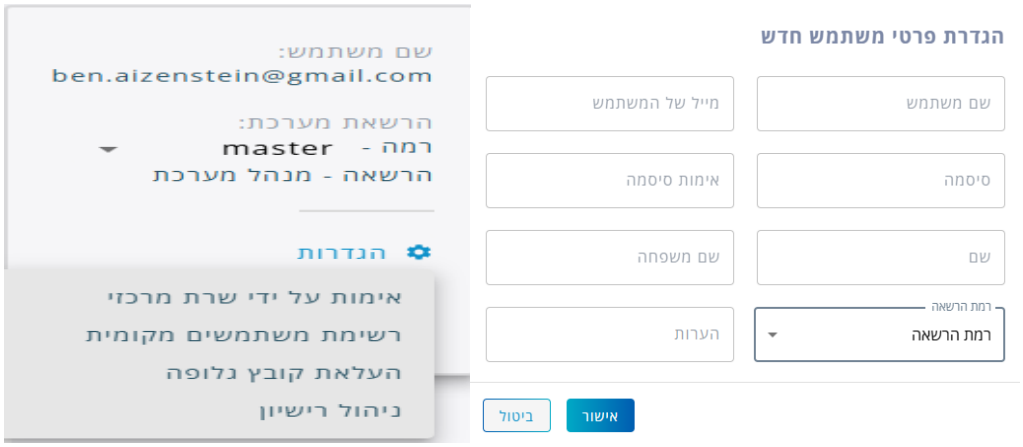


2.1.9 Adding Users to Tenant

At least one user must be added to an existing tenant to enable testing or working with Meeting Insights On-Prem.

To add Users to Realm (Using Offline Client):

1. Log in to the **Master Tenant** with an administrator account.
2. Click your **email address** in the top-left corner of the interface.
3. Select **Settings** from the dropdown menu.
4. In the settings menu, click **Local Users List**.
5. Click **Create New User**.
6. Complete all required fields and click **Confirm** to add the user to the realm.



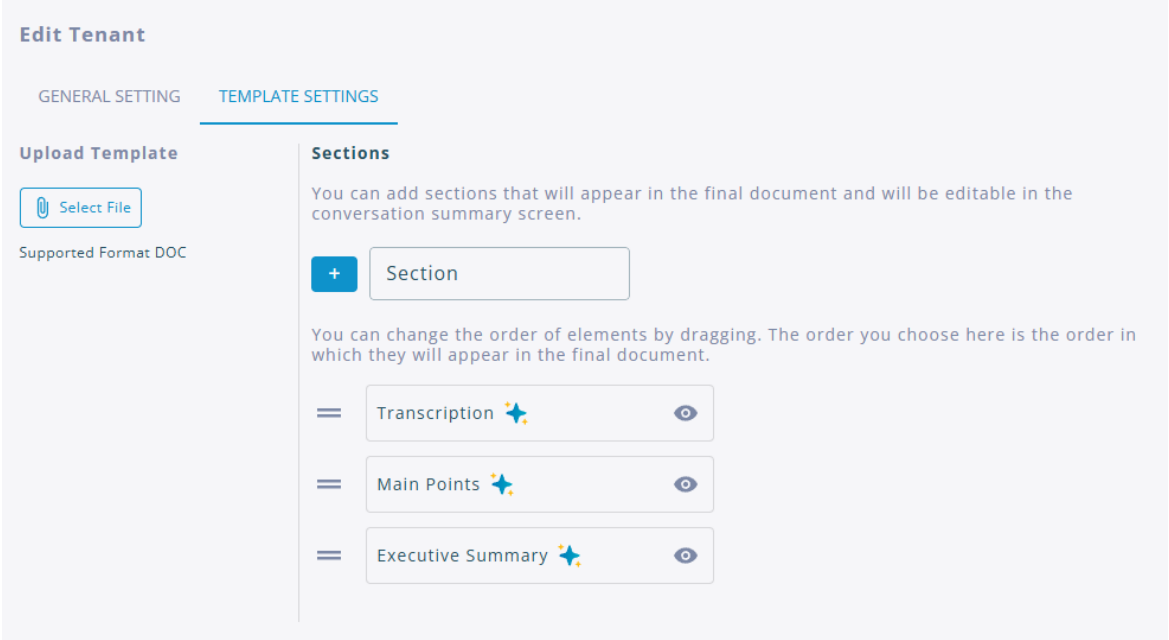
Adding users to the realm can also be performed by a **Tenant Administrator**, not only by the **Master Tenant Administrator.**

2.1.10 Adding Docx Template

A DOCX template must be uploaded per tenant and can be managed by the **Tenant Administrator**.

To upload a DOCX template to your tenant:

1. Log in to your **Tenant** as an administrator.
2. Click your **email address** in the top-left corner of the interface.
3. Select **Settings** from the dropdown menu.
4. In the settings menu, click **Edit customer** again (if not already selected).
5. Select the **Template settings** tab
6. Click the **Select File** button.
7. Choose the desired template file (*a default file is provided for this purpose*) and click **Confirm** to complete the upload.
8. Note: one of the uploaded template files should be set as default by clicking “set as default” near the template name.



2.1.11 Configuring Recording Bot

The recording Bot Allows to add recorded phone call meetings to the Meeting Insights On-Prem environment for transcription/Diarization and AI summarizations.

To link a phone number to Users and tenants in the Meeting Insights On-Prem DB it is required to make this mapping in the ".env" configuration file on the "Recording Bot" folder located at: "/ac/recording_bot".

The value to be added in the .env file is of "TENANT_CALLERS_1" and is in the structure of a json like in the below format:

```
{
<tenanat-
name1>:["<ext1>/<username1>/<email1>","<ext2>/<username2>/<email2>"…..],
<tenanat-
name2>:["<ext3>/<username3>/<email3>","<ext4>/<username4>/<email4>"…..],
.
.
}
```

In this format:

- Calls that arrive from extension "ext1" are assigned to user "username1" in tenant "tenant-name1".
- Calls that arrive from extension "ext2" are assigned to user "username2" in tenant "tenant-name1".
- Calls that arrive from extension "ext3" are assigned to user "username3" in tenant "tenant-name2".
- Calls that arrive from extension "ext4" are assigned to user "username4" in tenant "tenant-name2".

For example:

TENANT_CALLERS_1={tenanat1:["5002/dan/dan@audiocodes.com","5005/test/","5006//test@gmail.com","6001/oren/oren@audiocodes.com","6002/michael/"],

tenant2:["5007//ben@gmail.com","5001","5004"],

tenant: ["5003/user103/user103@gmail.com"]}

Note: the username and email fields are optional, if username not entered the user is identified by its email address and if email is also not entered the recording is assigned to the admin of that tenant.

2.2 Basic functionality tests

2.2.1 Checking Offline Client

1. Log In

   Log in to the relevant tenant as an **operator** or **administrator**.

2. Create an Offline Task
   a. Click **Create an Offline Task**.
   b. Upload an **MP3 file** and fill in all required details.
   c. Click **Create** to submit the task.

3. Monitor Task Progress

   Wait a few seconds for the task to appear with the status **Transcription in Progress** in the **Status** column.

4. Review Transcription
   a. In the same row as the task, click **To File List** in the **left column**.
   b. When the file status changes to **Transcription**, click **To Improve Transcription** and check the following:
      - **STT** – Recognized text is available.
      - **SRD** – Text is correctly split by speakers.
      - **NLP** – Text includes punctuation (e.g., **periods, commas**).

5. Verify Completion

   Return to the **File List** page and ensure the status is **Ready**.

2.2.2 Checking Recording Client

1. Log In

   Log in to the relevant tenant as an **operator** or **administrator**.

2. Create an Online Task
   a. Click **Create an Online Task**.
   b. Fill in all required details, then click **Continue**.

3. Start and Stop Recording
   a. Click **Start Recording**, then speak into the microphone.
   b. Click on the **bell icon** and verify that the message **"Connecting to STT server successfully"** appears.
   c. Click **Stop Recording**.

4. Verify Transcription

   Switch to the **Offline Client** and repeat step 3 to check the transcription status.

2.2.3 Checking Dictation Client

1. Log In

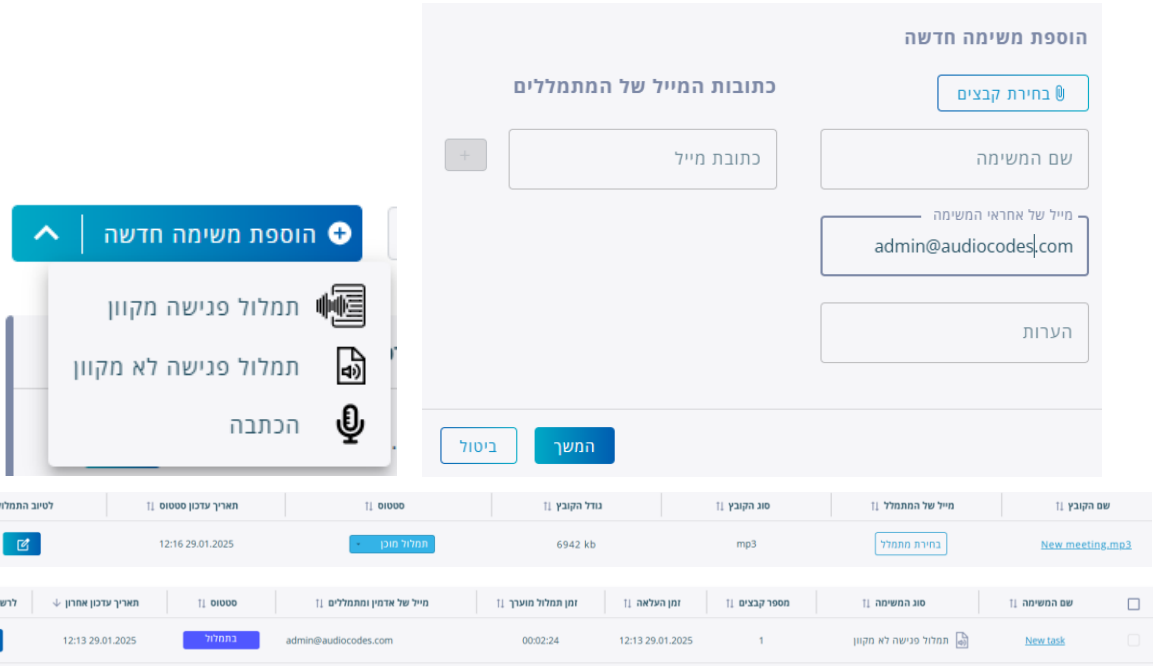
   Log in to the relevant tenant as an **operator** or **administrator**.

2. Create a Dictation Task
   a. Click **Dictation**.
   b. Enter a **Dictation Name**.

3. Start and Stop Dictation
   a. Click **Start Dictation**, then speak into the microphone.
   b. Verify that the alert **"Connecting to STT server successfully"** appears.
   c. Click **Stop Dictation**.
   d. Click **Send**.

4. Verify Transcription

   Switch to the **Offline Client** and repeat steps 3 to check the transcription status.



2.3 Upgrading Procedures

2.3.1 Upgrading the Backend Images

The docker images in this category are:

- Hrec_server
- Calendar_server
- Mailer_server
- Watch-transcriber
- ProofingBE
- AgentAssistBot
- Rls_container
- nlp

To perform the image upgrade, follow these steps:

1. Copy the image to customer server.
2. Upload the image to the local registry.

```
docker load -i <image-name>.tar
```

3. Edit the ".env" file and update the image version to the updated version installed.
4. Restart the system

```
docker compose down
docker compose up -d
```

2.3.2 Upgrading the Clients

The docker images in this category are:

- recording_client
- proofing_client
- offline_client
- keycloak_themes

To perform the clients upgrade, follow these steps:

1. Copy the image to customer server.
2. Upload the image to the local registry.

```
docker load -i <image-name>.tar
```

3. Edit the ".env" file and update the client image version to the updated version installed. (below shown as it appears in the .env file)

```
recording_client=2.1.49
proofing_client=2.1.58
offline_client=2.1.74
keycloak_themes=2.0.9
```

4. Execute the shell script (each client has its own script) in folder "./update_data" to deploy the image client to nginx/html folder.
   - For updating the recording client execute the command
     `/ac/update_data/recording_client.sh`
   - For updating the offline client execute the command
     `/ac/update_data/offline_client.sh`
   - For updating the proofing client execute the command
     `/ac/update_data/proofing_client.sh`
   - For updating the keycloak_themes client execute the command
     `/ac/update_data/keycloak_themes.sh`
5. Restart the system

```
docker compose down
docker compose up -d
```

2.3.3 Upgrading the STT/NLP Factories

The docker images in this category are:

- speech-service-factory
- nlp-service-factory

To perform the factories upgrade, follow these steps:

1. Copy the image to customer server.
2. Upload the image to the local registry.

```
docker load -i <image-name>.tar
```

3. Edit the ".env" file and update the client image version to the updated version installed. (below shown as it appears in the .env file)

```
speech_service_factory=F20.20.00
nlp_service_factory=N50.00.03
```

4. Execute the shell script (each factory has its own script) in folder "./update_data" to deploy the image client to nginx/html folder.
   - For updating the speech-service-factory execute the command

     ```
     /ac/update_data/stt_factory.sh
     ```

   - For updating the nlp--service-factory execute the command

     ```
     /ac/update_data/nlp_factory.sh
     ```

5. Restart the system

```
docker compose down
docker compose up -d
```

3 Troubleshooting

3.1 Introduction

This section describes possible errors encountered during installation and possible solutions.

3.2 Issues Found

3.2.1 Docker-Load Errors:

- **Description:** During installation scripts, sometimes docker-load command fails on the docker daemon.
- **Solution 1:** manual: Restart the docker daemon service on the OS (might depend on the Linux distribution. Example: sudo service docker restart)
- **Solution 2:** on installation script: error-recovery of failed commands with some limited retries

3.2.2 Keycloak+Maria-DB Issue on Some Linux Distros

- **Description:** Keycloak failed and crashes on startup and keeps restarting, showing error messages from MariaDB.

  The key to this problem is a warning message that MariaDB attempted to allocate some memory size to multicast socket buffer, but the OS only allows a small part of it.
- **Example:** "WARN: the send buffer of socket MulticastSocket was set to 20MB, but the OS only allocated 212.99KB"
- **Solution:** To ensure MariaDB operates properly, the following command needs to run:

```
RUN sysctl -w net.core.rmem_max=25600000 && sysctl -w
net.core.wmem_max=1024000
```

3.2.3 Nginx responds with "Forbidden" on any request sent to the /html folder, and logs "permission denied" on the error.log file

- **Possible cause:** access on the /html folder might not be allowed.
- **Solution:** run chown -R on the nginx folder to recursively change access permissions for read / write.

3.2.4 Linux Machine Goes to Sleep or Hibernates

- **Possible cause:** Usually happens when a AI server is installed on a laptop and goes to sleep due to lid closing or saving power reasons
- **Solution:**
  1. Disable the sleep / hibernate with the below commands (relevant for Ubuntu and Linux)

     ```
     sudo systemctl mask sleep.target suspend.target
     hibernate.target hybrid-sleep.target
     ```
  2. Edit the file /etc/system/logind.conf and set the below parameters

     ```
     HandleLidSwitch=ignore
     HandleLidSwitchDocked=ignore
     HandleSuspendKey=ignore
     HandleHibernateKey=ignore
     ```

3. After that restart the systemd-logind:

```
sudo systemctl restart systemd-logind
```

A Appendix: Meeting Insights On-Prem Gemalto License Server

A.1 Introduction

This section provides an overview of the installation and configuration of the **Gemalto License Server** for the **AudioCodes STT (Speech-to-Text)** engine. It also outlines the steps required to request and activate a license key.

A.2 Getting Started

The License Server must be deployed in an environment where an **STT server is already installed and configured** to obtain its license from this License Server.

> The STT application runs as a Docker container on a Linux machine and cannot function without access to a valid license key from the License Server.

A.3 Installing License Server

The Gemalto License Server must be installed on a **dedicated Linux machine** (see system requirements) and be **accessible on port 1947** from the STT application.

A.3.1 Installing the License Application on a Dedicated Linux Server

The procedure below describes how to install the License Application on a Dedicated Linux Server.

A.3.1.1 Prerequisites

The LM installation files include:

- Gemalto LM installer tar.gz file, namely **aksusbd_94011-9.12.1.tar.gz**
- Configuration INI file, namely **hasplm.ini**
- This document file

Target Instance \ VM \ Server

Operating system must be one of the following:

- Ubuntu 18.04, 20.04, 22.04, 24.04
- Rocky Linux 8, 9
- RHEL 8, 9
- CentOS 8
- Verify Operating System key found by executing “hostnamectl” on a bash terminal to the target.
- Ensure the Operating System includes **tar** utility (check with “tar –version” on a bash terminal to the target)
- The Gemalto LM must be installed using **sudo** or **root** user.

A.3.1.2 Installation

Step 1: Copy Files to Target Machine

Copy following files into the user's home folder (e.g. /home/ubuntu for ubuntu user, /root for root user, etc. all according to operating system type and target available users):

- aksusbd_94011-9.12.1.tar.gz
- haslm.ini

Step 2: Extract the Driver Installer

From the previous step folder run to extract installer by executing from bash terminal to the target:

- tar -xvzf aksusbd_94011-9.12.1.tar.gz

  check "aksusbd-9.12.1" folder created (by executing "ls -ltr"|find aksusbd-9.12.1" and folder should be found).

Step 3: Install the Driver

From the previous step folder run following to install by executing from bash terminal to the target:

- cd aksusbd-9.12.1
- sudo ./dinst
- cd ..
- sudo cp hasplm.ini /etc/hasplm/

Step 4: Restart the Driver

From the previous step folder run following to restart driver by executing from bash terminal to the target:

- sudo systemctl restart aksusbd

Step 5: Post-Installation Check

From remote computer, using the browser direct to the Gemalto LM web portal (http://<target IP>:1947) to operate standard licensing procedure of vendor to customer and vice versa to gain fingerprint and apply license.

Step 6: Cleanup

The following copied and extracted folder may be deleted from the target:

- rm -fr aksusbd-9.12.1
- rm aksusbd_94011-9.12.1.tat.gz
- rm hasplm.ini

Please note that to uninstall, the folder **aksusbd-9.12.1** must remain and should not be deleted.

A.3.1.3 Un-Install Procedure

Uninstall driver

From the install folder run following to uninstall by executing from bash terminal to the target:

- cd aksusbd-9.12.1
- sudo ./dunst

Cleanup

The following copied and extracted folder may be deleted from the target as well:

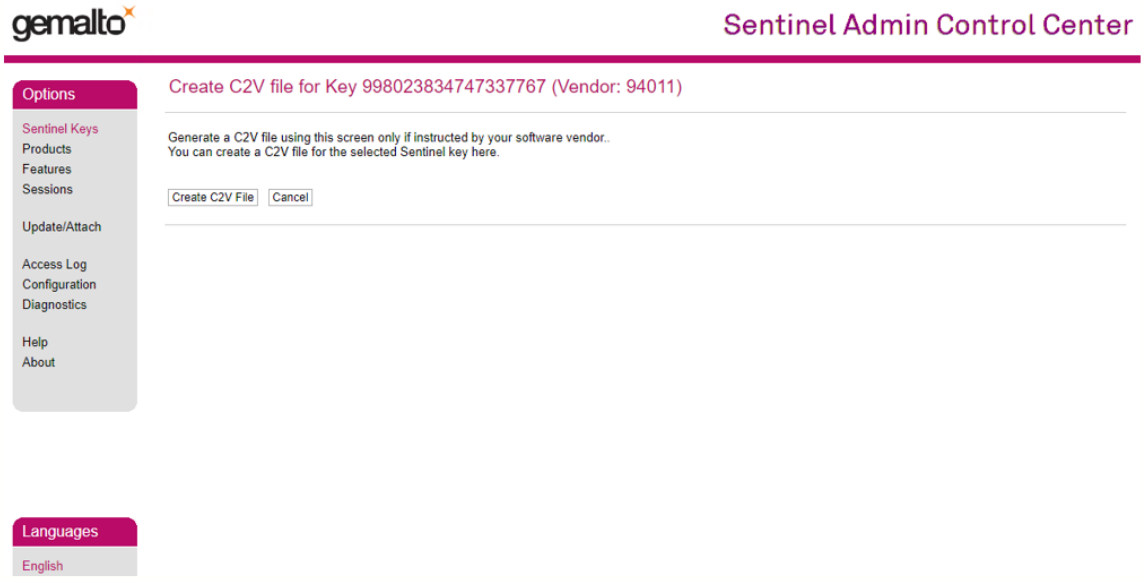
- rm -fr aksusbd-9.12.1
- rm aksusbd_94011-9.12.1.tat.gz
- rm hasplm.ini

A.3.2 Receiving Machine Fingerprint and Uploading Generated License Key

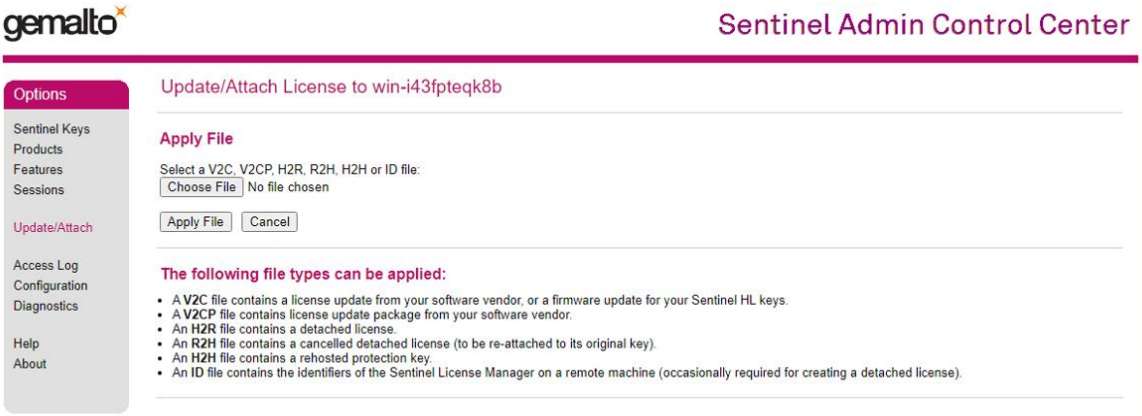
The procedure below describes how to receive the machine fingerprint and upload the generated license key.

To receive the machine fingerprint and upload the generated license key

1. Open Google Chrome browser and type: <gemalto machine ip>:1947.
2. Create the C2V file on the license server; the file created provides a fingerprint of the server.



1. Send the created fingerprint (C2V file) to AudioCodes to generate the license key (V2C file).
2. Receive the V2C file and then upload it to the server (update/attach > choose file and apply file).



A.3.3 Validating Uploaded License Key

The procedure below describes how to validate the uploaded license key.

To validate the uploaded license key:

1. Access <gemalto machine ip>:1947 > Products to see the product is shown correctly
2. Access <gemalto machine ip>:1947 > Features
3. Check the **Features** page to see that the license was uploaded successfully.

B Appendix: Meeting Insights On-Prem License

B.1 Overview

The **Meeting Insights On-Prem License Decoder API** is a REST-based service used to decode and manage licenses for AudioCodes Meeting Insights On-Prem applications. It is typically used in conjunction with the license server to validate and activate product licenses.

This section provides installation instructions and usage guidelines for deploying the API on a **Linux platform**.

B.2 Installation

B.2.1 Prerequisites

1. Linux operating system
2. Administrative privileges
3. HTTPS certificates (tls.crt and tls.key files)

B.2.2 Installation Steps

B.2.2.1 Zip file content

```
MiaopDecodeLicenseServer/
├─ cert/
│    └─ tls.crt
│    └─ tls.key
├─ GetMachineNumber/
│    └─ linux
│       └─ GetMachineNumber.sh
├─ installation/
│    └─ linux
│       └─ install.sh
│       └─ uninstall.sh
├─ nssm-2.24/
│    └─ src
│    └─ win32
│    └─ win64
│       └─ nssm.exe
├─.env
├─ install.bat
├─ uninstall.bat
└─ main-linux
└─ main-win.exe
└─ License Management REST API Manual Documentation.pdf
```

The installation folder name is MiaOpDecodeLicenseServer-x.x.x.zip (where x.x.x is the version number), and should contains the following files and directories:

B.2.2.2 Linux Installation Steps

1. Create folder /ac

   bash
   ```
   sudo mkdir /ac/
   ```
2. Copy MiaOpDecodeLicenseServer-x.x.x.zip into folder /ac/ and extract it:

   bash
   ```
   sudo cp MiaOpDecodeLicenseServer-x.x.x.zip /ac/
   cd /ac/
   sudo unzip MiaOpDecodeLicenseServer-x.x.x.zip
   ```
3. Go to the created folder /ac/MiaOpDecodeLicenseServer:

   bash
   ```
   cd /ac/MiaOpDecodeLicenseServer
   ```
4. Make the service file executable:

   bash
   ```
   sudo chmod +x main-linux
   ```
5. Update the certificate files in the cert folder:
   - Replace *tls.crt* and *tls.key* with your own certificate files.
   - **Important**: Keep the filenames as *tls.crt* and *tls.key*.
6. Navigate to the installation directory:

   bash
   ```
   cd /ac/MiaOpDecodeLicenseServer/installation/linux
   ```
7. Make the installation script executable:

   bash
   ```
   sudo chmod +x install.sh
   ```
8. Run the installation process:

   bash
   ```
   sudo ./install.sh
   ```
9. Verify the installation:

   Check the service status:

   bash
   ```
   sudo systemctl status MiaOpDecodeLicenseService
   ```
   a. Confirm that the Active line shows "active (running) since..."

   b. Open a browser outside the server and navigate to: *https://127.0.0.1:3003* or by send through bash command inside the server "*curl -k https://127.0.0.1:3003*"

   c. Confirm you receive the response: *{"type":"ac-lic-api","success":true}*

   d. Check that a logs folder was created in the root directory containing log files in the format *log-yyyy-mm-dd.log*

B.2.3 Uninstallation Steps

1. Navigate to the installation directory:

   bash
   ```
   cd /ac/MiaOpDecodeLicenseServer/installation/linux
   ```
2. Make the uninstallation script executable:

   bash
   ```
   sudo chmod +x uninstall.sh
   ```
3. Run the uninstallation process:

   bash
   ```
   sudo ./uninstall.sh
   ```
4. Verify the uninstallation:

   Check the service status:

   bash
   ```
   sudo systemctl status MiaOpDecodeLicenseService
   ```
   Confirm you received the message: "Unit MiaOpDecodeLicenseService.service could not be found."

B.2.4 Configuration File

The .env configuration file include the next properties:

- LOG – log folder location and name (ex: LOG="./logs")
- LOGLEVEL – log level specification (Possible values: error, warn, info, verbose, debug, silly)
- PORT – port number for access the server (ex: PORT=8083)
- ACCESS_TOKEN - authorization header: value to include as described in authentication Section. (ex: ACCESS_TOKEN=32489543502437549385764589574 55)
- CERT_KEY_FILE_PATH – authorization key file location and name (ex: CERT_KEY_FILE_PATH="./cert/tls.key")
- CERT_CRT_FILE_PATH - authorization crt file location and name (ex: CERT_CRT_FILE_PATH="./cert/tls.crt")
- IS_SECURE - Choosing between creating secure server (https) or insecure server (http) (“Yes” for https. Any other value for http)

B.3 Get System ID

Retrieves the UUID - Universal Unique Identifier (FP_DATA) of the license server.

Get Linux System ID

1. Navigate to the script directory:

   bash
   ```
   cd /ac/MiaOpDecodeLicenseServer/GetMachineNumber/linux
   ```
2. Make the script executable:

   bash
   ```
   sudo chmod +x GetMachineNumber.sh
   ```
3. Run the process:

   bash
   ```
   sudo ./GetMachineNumber.sh
   ```
4. A new text file named “FP_DATA.txt” is created in the same directory and will contains the System ID.

B.4 API Endpoints

The API service is accessible at this base Url: *license.miaop.audiocodes.co.uk*

All requests use the HTTPS protocol with authentication.

B.5 Authentication

All requests to the API must include the following authorization header:

Key: authorization

Value: Bearer 32489543502437549385764589574 55

B.6 Available Functions

DecodeLicense

Decodes an existing license file.

- **Method**: POST
- **Endpoint**: `/decodeLicense`
- **Request Body**: JSON object containing license information
  - *iv*: Initialization vector for decryption
  - *license*: Encrypted license content

Example Request Url and headers:

```
POST https://license.miaop.audiocodes.co.uk/ decodeLicense
Content-Type: application/json
authorization: Bearer 32489543502437549385764589574 55
```

Example Request Body:

json

```
{
    "iv": "2hRwPCpnhQwiJU2vl0IHsw==",
    "license":
"im8236Vac068Ngabh8lEITNGDj4bLa/K4AnAusFI/QlwOxFbWno817AwGil5oV/y.
.."
}
```

Successful Response (200 OK):

json

```
{
    "success": true,
    "license": {
        "APPLICATION_NAME": "MIAOP",
        "PRODUCT_KEY": "D88E24383FF02DM5",
        "Options": {
            "Tbr": "1",
            "Qbr": "1",
            "TestRoute": "1",
            "NumberOfRoutingRules": "9999",
            "NetworkPlanner": "1",
            "PolicyStudio": "1",
            "ExpirationDate": "2026-01-03",
            "NumOfHours": "15000",
            "MiaNumberOfUsers": "999999",
            "NumberPortability": "1",
            "MiaOPRouteRegistrations": "99999",
            "MiaOPNumberOfSession": "999999",
            "MonthlySTSecurityQueries": "99999",
            "numberADVSecurityQueryMon": "99999",
            "MiaOPAnalytics": "1"
        },
        "issueDate": "2025-01-03T06:33:00.695Z",
        "licenseId":
"5c806eb9cf8d44e37b6672d620dcc857243878c49e7d67bf525f37d7052f9e59"
    },
    "message": "License decoded successfully"
}
```

Unsuccessful Response (Status Code: 403 Forbidden):

json

```
{
    "success": false,
    "error": "SyntaxError: Unexpected token ' ', \"
\"APPLICAT\"... is not valid JSON Invalid or corrupted license
file"
}
```

B.6.1 Troubleshooting

Service Not Starting

If the service doesn't start after installation:

1. Check the logs folder for error messages
2. Verify that the certificate files (tls.crt and tls.key) are valid
3. Ensure you have administrative privileges
4. Verify port is not already in use (3003 Linux)

Authentication Errors

If you receive a 401 Unauthorized response:

1. Verify that you're including the correct authorization header
2. Check for any typos in the Bearer token

API Connection Issues

If you cannot connect to the API:

1. Verify the service is running.
2. Check that the hostname is resolved correctly to the server IP
3. Ensure port 443 is open on the server firewall
4. Validate the SSL/TLS certificates are trusted by your client

International Headquarters
Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com

Document #: LTRT-26028