AudioCodes Meeting Solutions for Enterprises

Meeting Insights On-Prem

Installation Manual

Version 2.4.3

Table of Contents

Notice v

Security Vulnerabilities v

WEEE EU Directive v

Customer Support v

Stay in the Loop with AudioCodes v

Related Documentation v

Document Revision Record vi

Documentation Feedback vii

1 Pre-Installation/Upgrade Requirements Guideline 2

1.1 Introduction 2

1.2 Deployment Models 2

1.3 Telephony Sessions Support 3

1.4 Upgrade Process 3

1.5 First-Time Installation Process 3

1.6 Downloading the Required Software 4

1.7 Hardware and Hosts Requirements 4

1.8 Getting Licenses 5

1.8.1 Meeting Insights On-Prem License 5

1.8.2 Gemalto License 6

1.8.3 POC Terms and Conditions 6

2 Installing Multi-Language STT (ML-STT) on Dedicated VM 7

2.1 Prerequisites for ML-STT VM 7

2.2 Security Rules and Network Ports 7

2.3 Installation of GPU and Dockers Support for ML-STT VM 7

2.4 ML-STT Installation 7

3 Installing LLM (AI) on a Dedicated Machine 9

3.1 Prerequisites for LLM VM 9

3.2 Installation of GPU and Dockers Support for LLM VM 9

3.3 LLM (AI) Installation 9

4 Meeting Insights On-Prem Upgrade Process 11

4.1 Upgrade limitations and Notes 11

4.2 Prepare Licenses 11

4.3 Increase storage capacity 11

4.4 Installing ML-STT VM version 2.4.3 13

4.5 Upgrading LLM VM to version 2.4.3 13

4.6 Upgrading VAIC on Separated VM 14

4.7 Upgrading MIA-OP VM 14

4.7.1 Upgrade MIA-OP VM Pre-Requisites 14
4.7.2 Extracting the tar.gz Installation Files 15
4.7.3 Running the Upgrade Script on MIA-OP VM 15
4.8 Update the Gemalto License 15
4.9 Finalizing the VAIC Upgrade 15
5 Meeting Insights On-Prem Linux Docker Installation 19
5.1 Introduction 19
5.2 Environment pre-installation requirements 19
5.3 Firewall / Port Access Requirements 20
5.4 Installation of Gemalto Server 20
5.4.1 Installation of Gemalto Server 20
5.4.2 Requesting Gemalto License 21
5.4.3 Uploading Gemalto License 21
5.5 Software Preparation for Installation 21
5.6 Extracting the tar.gz Installation Files 22
5.7 Running the Installation Script 22
5.8 Running the Setup Script 23
6 Initial Configuration 25
6.1 Configuring Web Pages Access (Optional) 25
6.2 Restarting Meeting Insights On-Prem 25
6.3 Exchanging Additional Configuration Needed 25
6.4 Installing License File Via Browser 26
6.5 Adding Users to a Tenant 26
7 Basic Functionality Tests 28
7.1 Checking Offline Client 28
7.2 Checking Recording Client 28
7.3 Checking Dictation Client 29
8 Maintenance 30
8.1 Changing Deployment Model 30
8.1.1 Increasing Deployment Model from 1.A 30
8.1.2 Increasing Deployment Model from 2.A 31
8.2 Changing Encrypted Environment Variables 32
9 Troubleshooting 33
9.1 Introduction 33
9.2 Issues Found 33
A Appendix: Meeting Insights On-Prem License Server 35
A.1 Introduction 35
A.2 Get System ID 35
A.3 Request a license 35

A.4 API Endpoints 35
A.5 Authentication....35
A.6 Available Functions 36
A.6.1 Troubleshooting 37
B Appendix: Gemalto License Server 38
B.1 Introduction....38
B.2 Getting Started 38
B.3 Installing License Server 38
B.3.1 Installing the License Application on a Dedicated Linux Server 38
B.3.1.1 Prerequisites....38
B.3.1.2 Installation....39
B.3.1.3 Un-Install Procedure....40
B.4 Getting Machine Fingerprint 40
B.5 Uploading Generated License Key and Validating Uploaded License Key 41
C Appendix: Installing Support Environment for LLM / ML-STT VM....42
C.1 Installation on Ubuntu 24.04 42
C.1.1 Preparation....42
C.1.2 Installing Docker Engine (if not already installed)....42
C.1.3 Installing CUDA Toolkit and Driver 44
C.1.4 Installing NVIDIA Container Toolkit....44
C.2 Installation on Rocky Linux....45
C.2.1 Installation of Essential Packages....45
C.2.1.1 Installing Docker Engine (if not already installed)....46
C.2.1.2 Installing CUDA Toolkit and Driver 47
C.2.1.3 Installing NVIDIA Container Toolkit....48
D Appendix: Keycloak Active Directory Integration Guide 50
D.1 Introduction....50
D.2 Prerequisites....50
D.3 Realm Setup 50
D.4 Configure LDAP User Federation....50
D.5 Configure Group Mapper 53
D.6 Configure User Attribute Mapper 55

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: March-08-2026

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
Meeting Insights On-Prem Administrator’ and User’s Manual
Meeting Insights On-Prem Brochure

Document Revision Record

LTRT	Description
26012	Initial document release (Version 2.0)
26027	Updated to Version 2.2
26028	Updated to Version 2.4
26029	Updated to Version 2.4.2
26039	Updated to Version 2.4.3

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 Pre-Installation/Upgrade Requirements Guideline

1.1 Introduction

Meeting Insights On-Prem (MIA-OP) version 2.4.3 supports both First-time Installation and Upgrade from version 2.4.2.

This section outlines the steps that must be taken by the Customer before beginning the installation or upgrade 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 Deployment Models

Meeting Insights On-Prem version 2.4.3 also supports two different STT engines:

- AudioCodes' STT Engine which specialized in Hebrew and English (only).
- Multi-Languages STT supports 50+ languages.

This section summarizes the installation and deployment models which differ in the following parameters:

- The chosen STT engine
- The maximum concurrent sessions (CCS) that the customer wants to achieve.
- AI (LLM) support (enabled/disabled)
- Telephony Support (enabled/disabled)

The user/customer must decide the required deployment model, because it affects the best hardware requirements and software modules for reaching the optimal conditions and best results.

The table below summarizes the 4 options of deployments which are supported:

Table 1: Deployment models

Deployment Model	STT Type	Languages	Maximum Concurrent Sessions	AI (LLM) Option	Telephony Option
1.A	AudioCodes (GPU is not required)	Hebrew/English only	4	Optional (GPU is required)	Optional
1.B			16		
1.C			30		
2.A	Multi-Languages STT (ML-STT) (GPU is required)	50+ Languages	16	Optional (additional GPU is required)	Optional
2.B			30		

1.3 Telephony Sessions Support

All MIA-OP deployment models are supporting Telephony support option.

The telephony sessions support allows MIA-OP to record and transcribe telephony sessions (including meetings) like any other Voice session including AI summary option.

For Telephony support, two modules should be installed:

1. AudioCodes Mediant SBC (session Boarder Controller) version 7.40VA.500.222 – this entity is purchased separately from AudioCodes and it allows routing and processing of SIP phone calls received from Phones, IP Phones, Mobile users, etc. The SBC should be installed on its own dedicated VM (“Mediant VE”) or purchased as an appliance.
2. VAIC (Voice-AI Connect) version 3.24.468 – this module is connecting between the SBC product and MIA-OP. The VAIC software module is installed on the MIA-OP VM itself. During the installation process of MIA-OP VM, the user will be asked whether to install the VAIC module or not.

1.4 Upgrade Process

Users who have already installed Meeting Insights On-Prem version 2.4.2 (2.4.2 rc6) can use the Upgrade procedure to make upgrade to version 2.4.3 and **preserve configuration and data that was already existing**.

The Upgrade procedure supports upgrading to any of the deployment models described in section 1.2.

For upgrading process, follow this order:

1. Make a VM backup of your current MIA-OP VM deployment in case the upgrade fails.
2. Chapter 1 (this chapter): make sure you have all hardware, software and licensing ready.
3. Chapter 2: Install ML-STT VM (only if deployments 2.A or 2.B were chosen).
4. Chapter 3: upgrade LLM (only if AI summary capabilities were already deployed).
5. Chapter 4: upgrade MIA-OP - follow the upgrade process for the main MIA-OP VM.
6. Chapter 6 and Chapter 7: initial configuration, checking basic functionality is working and license update.

1.5 First-Time Installation Process

- Customers who choose to make First-Time Installation will **not** preserve any previous data.
- The Install procedure supports installation of any of the deployment models described in section 1.2.

1. For the installation process, follow this order:
2. Chapter 1 (this chapter): Make sure you have all hardware and software and licensing ready.
3. Chapter 2: Install ML-STT VM (only if deployments 2.A or 2.B were chosen).
4. Chapter 3: Install LLM (only if AI summary capabilities should be deployed).
5. Chapter 5: Installation procedure of MIA-OP VM.
6. Chapter 6 and Chapter 7: initial configuration, checking basic functionality is working and license update.

1.6 Downloading the Required Software

The Meeting Insights On-Prem software must be downloaded from the provided link of **miaop_2.4.3**. This Link includes several folders:

Table 2: Folders containing Linux Installation components

#	Folder Name	Contains
1	Documentation	Installation and User Manuals
2	miaop	■ Meeting Insights On-Prem installation package, including: • Main MIA-OP application packages • VAIC (optional) • Hebrew/English STT (optional)
3	Llm	LLM package (optional)
4	ml_stt	Multi-Language STT package
5	Gemalto	Gemalto License Server
6	SBC	SBC installation files

1.7 Hardware and Hosts Requirements

The Meeting Insights On-Prem solution has multiple deployment models (see section 1.2), which affect the number of machines (virtual-machines) required.

The Customer should choose the requested deployment model and must prepare the environment in accordance with the specifications below:

Table 3: HW specification

VM	Optional/ Required	Deployment Model	CCS	vCPU	RAM [GB]	Storage [GB]	GPU Required
MIA-OP application (including Gemalto Server)	Required	1.A	4	10	24	130	No
		1.B	16	24	64	520	No
		1.C	30	38	120	1000	No
		2.A	16	8	8	520	No
		2.B	30	8	8	1000	No
ML-STT (Multi-Languages) VM	Required only for Deployment 2.A or 2.B	2.A	16	20	34	150	Yes
		2.B	30	34	55	150	Yes
LLM (AI Summary)	Optional	All	Up to 30	2	2	150	Yes
SBC VM	Required only for Telephony support	All	unlimited	2	4	20	No

Supported Operating Systems (for all VMs):

- Linux Rocky 9 / RHEL 9
- Ubuntu 24.04

For other OS, please contact AudioCodes contact manager.

CPU type (for all VMs):

- x64 Instruction Set Architecture (ISA), AVX2 support, Min. at least 4GHz Turbo Speed.

GPU cards supported (for ML-STT VM / LLM VM):

- RTX 6000
- L40S

Ensure machine time is synchronized across all machines and containers.

1.8 Getting Licenses

The system uses two different licenses:

Table 4: Used licenses

	License type	Description	Procedure for Getting a License
1	Meeting Insights On-Prem license	The license specifies: ▪ Number of transcription hours ▪ Expiration date.	**See Appendix A for details:** **Stage 1:** Go to the following directory: `~/miaop_setup/prerequirement_scripts` **Stage 2:** Run the `get_computer_uuid.sh` script **Stage 3:** Send the generated uuid.txt file to your AudioCodes contact manager.
2	Gemalto License	Optimizing the system according to the required Concurrent Session.	**See Appendix B for details:** **Stage 1:** Install the **Gemalto License** server. **Stage 2:** From within the application, generate and send the **xxx.C2V** file to AudioCodes. and specify which deployment model was chosen (see section 1.2).

1.8.1 Meeting Insights On-Prem License

Meeting Insights On-Prem License should be requested according to steps described in Appendix A.

The installation of the MIA-OP license is described in section 6.4.

When upgrading MIA-OP version 2.4.2 to version 2.4.3, a new license is required only if the user would like to change at least one of the following licensing capabilities:

Expiration date

Number of transcription hours

1.8.2 Gemalto License

- For first time installation, the Gemalto server should be installed on the same VM targeted for MIA-OP VM. As described in Appendix B. **Ask for a new Gemalto license before installation.**
- For Upgrading procedure, the existing Gemalto server can be reused. If your system uses AI or if the deployment model or the maximum concurrent sessions were changed, **ask for a new Gemalto license before the upgrade**.

> When a new Gemalto License is requested for installation or upgrading processes, the user should also specify the following information for the proper operation of the application:
>
> - Will AI be deployed or not?
> - The requested deployment model (as described in section 1.2)
> - The required maximum Concurrent Sessions (CCS)
> - The machine fingerprint (see Appendix B.4)

1.8.3 POC Terms and Conditions

The POC License is supported with the following terms:

- Meeting Insights On-Prem License:
  - **Expiration Date:** 45 days
  - **Max hours of audio**: 1,000
- Gemalto License:
  - **Max concurrent sessions**: - 4 (online + offline)

> When making upgrade of POC, new POC licenses should be requested for optimal operation.

2 Installing Multi-Language STT (ML-STT) on Dedicated VM

The installation of ML-STT is required for deployment models B.1 and B.2 as described in section 1.2.

2.1 Prerequisites for ML-STT VM

There are two ML-STT VM deployment models:

Table 5: ML-STT VM deployment models

ML-STT Deployment	Maximum CCS	Number of vCPUs	VM Memory size	Storage size
B.1	16	20	34GB	150GB
B.2	30	34	55GB	150GB

- CPU Architecture: x86_64, preferrable Xeon-SP with turbo speed of 4GHz or more
- GPU attached to the VM using **PCI Passthrough**: RTX 6000 / L40S
- OS supported (on the guest VM):
  - Ubuntu (version 24.04)
  - Rocky Linux (version 9.6)

2.2 Security Rules and Network Ports

For proper operation of MIA-OP application, the following ports and directions should be opened in the organization's firewall:

Table 6: Firewall requirements

Required Port(src -> dest)	Notes
443 (any –> Mia-OP)	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 –> external Mail Server)	Port used by Meeting Insights On-Prem

2.3 Installation of GPU and Dockers Support for ML-STT VM

Follow Appendix C to add GPU and Docker support.

2.4 ML-STT Installation

Follow the steps below to install ML-STT (Multi-Languages STT) on a dedicated machine:

1. Log in as a MIA-OP admin user who belongs to the sudoers group.

```
sudo usermod -aG sudo <username> (for Ubuntu)
sudo usermod -aG wheel <username> (for Rocky)
```

2. Add the MIA-OP admin user to the docker group:

```
newgrp docker
sudo usermod -aG docker <username>
```

3. Create a folder for the installation and navigate to that folder:

```
cd ~
cd ml_stt_setup
```

4. Copy the ML-STT installation files to the installation folder:
   - containers_ml_stt_dd.mm.yy.tar.gz
   - setup_ml_stt_dd.mm.yy.tar.gz

5. Extract the two tar.gz installation files

```
tar -xvzf containers_ml_stt*.tar.gz
tar -xvzf setup_ml_stt*.tar.gz
```

6. Go to the installation folder and run the installation script:

```
cd setup_ml_stt/install/
{ sudo -vn || sudo -v; } && (while sudo -n true; do sleep
60; kill -0 "$$" || exit; done &) && ./install_ml_stt.sh
```

7. When prompted, enter the following:

   a. MIAOP_HOME directory: /ac

      Default: `/ac`

      Pressing **Enter** accepts the default.

   b. Enter the URL of keycloak – same as the URL of MIA-OP VM:

      For example: https://miaop-dns.example.com:8443

   c. Enter the Gemalto License server IP.

   d. Run the ***setup_ ml_stt.sh*** script:

   ```
   source ~/.bashrc
   ./setup_ ml_stt.sh
   ```

   e. Enter the URL of keycloak once again.

3 Installing LLM (AI) on a Dedicated Machine

3.1 Prerequisites for LLM VM

The HW requirements for LLM VM are:

Maximum CCS	vCPUs	Memory	Storage
30	2	2GB	150GB

- CPU Architecture: x86_64, preferrable Xeon-SP with turbo speed of 4GHz or more
- GPU attached to the VM using **PCI Passthrough**: RTX 6000 / L40S (for other GPU types please consult with your AudioCodes contact manager)
- OS supported (on the guest VM):
  - Ubuntu (version 24.04)
  - Rocky Linux (version 9.6)

Table 7: 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

3.2 Installation of GPU and Dockers Support for LLM VM

Follow Appendix C to add GPU and Docker support.

3.3 LLM (AI) Installation

Follow the steps below to install LLM (AI summary feature) on a dedicated machine:

1. Create a folder for installation and navigate to that folder:

```
cd ~
cd miaop_setup
```

2. Copy the LLM installation files to the installation folder:
   - containers_ai_dd.mm.yy.tar.gz
   - setup_ai_dd.mm.yy.tar.gz

3. Extract the two tar.gz installation files

```
tar -xvzf containers_ai*.tar.gz
tar -xvzf setup_ai*.tar.gz
```

4. Go to the installation folder and run the installation script:

```
cd setup_ai/install/
./install.sh
```

5. When prompted, enter the following:
   a. MIAOP_HOME directory: /ac

      Default: `/ac`

      Pressing **Enter** accepts the default.
   b. Allow the installer to set up the LLM containers and validate the required AI support drivers.

      If drivers are missing, follow the AI installation guide to install them before proceeding.
   c. Enter the **LLM API key**, ensuring it matches the key provided during the Meeting Insights On-Prem installation on the other machine.
6. Enter the **number of GPU layers** based on available GPU memory:

Available VRAM	N_GPU_LAYERS
Up to 4 GB	5
Up to 16 GB	45
24 GB or more	63

7. At the end of the installation, set the environment variables:

```
source ~/.bashrc
```

4 Meeting Insights On-Prem Upgrade Process

4.1 Upgrade limitations and Notes

Note the following restrictions and limitations of the upgrade procedure:

- **If you are using AI:**
  - Templates that were previously created might no longer be valid due to changes and enhancements in AI summaries. As a result, the System / Tenant admins must create new templates after upgrading to 2.4.3. using the newly supported AI summaries.
  - You should ask for a new Gemalto license with AI enabled.
- **Upgrade is supported only from release 2.4.2 (RC 6).** Users who are using earlier versions should first upgrade to version 2.4.2 rc6 by following the upgrade procedure described in MIA-OP Installation Manual version 2.4.2.
- For users who are using LLM support (for AI summary): In case the default AI prompt/s were modified in version 2.4.2, after upgrading to version 2.4.3 they will be **overwritten** with the default prompt.
- For users who are using Telephony support, the BOT recording users configuration will be deleted. After the upgrade the user’s phone extensions should be updated in the admin UI (Local User List -> Edit User Profile).
- The upgrade procedure allows switching from AudioCodes’ Hebrew/English STT (speech-to-Text) engine to an industrial STT engine which supports multiple languages (ML-STT). Note that the transition to the new STT requires adding additional virtual machine with GPU card as was described in Chapter 1.
- The upgrade procedure supports upgrading LLM or Telephony features, only if those features were already existing in version 2.4.2. In case that LLM or Telephony are requested but weren’t existing in 2.4.2, then need to consult AudioCodes for adding these features.

> **The sections below should be performed one after another, in the same order as the sections are.**

4.2 Prepare Licenses

Before starting the upgrade process, make sure you have the required MIA-OP License and Gemalto License as described in section 1.8.2.

Make sure the license request will fit the requested deployment model, as described in section 1.7.

4.3 Increase storage capacity

In case that storage capacity of the current VM should be increased (according to the Hardware requirements in section 1.7), repeat the steps below to increase the storage size of each VM requires storage increase:

1. Backup the VM before increasing its size.
2. Shut down the VM.
3. Open your VM settings in your Hypervisor.

4. Locate the Hard Disk settings and find the Resize or Expand button.
5. Increase the capacity according to the requirements in section 1.7.
6. Apply changes and start the VM.
7. For VM with Ubuntu:
    a. Install the following packages:

    ```
    sudo apt update
    sudo apt install cloud-guest-utils fdisk lvm2 -y
    ```

    b. Identify your Partition Layout, run the ***lsblk*** command:

    ```
    lsblk
    ```

    c. Look at the mount point for the folder you want to increase (or /myStorage if it is on a separate disk). For MIA-OP VM the folder is defined in the environment parameter MIAOP_DISK.

    For the example below, /acdisk resides on device sdc1:

    ```
    NAME          MAJ:MIN RM   SIZE RO   TYPE MOUNTPOINTS
    sda           8:0      0   512G  0   disk
     ├─sda1       8:1      0    99M  0   part   /boot/efi
     ├─sda2       8:2      0  1000M  0   part   /boot
     ├─sda3       8:3      0     4M  0   part
     ├─sda4       8:4      0     1M  0   part
     └─sda5       8:5      0 510.9G  0   part
       └─rocky-root 253:0    0 510.9G  0   lvm    /
    sdb           8:16     0    64G  0   disk
     └─sdb1       8:17     0    64G  0   part   /mnt
    sdc           8:32     0   500G  0   disk
     └─sdc1       8:33     0   500G  0   part   /acdisk
    ```

    d. In case that TYPE of ***/acdsik*** is 'lvm':
        i. Grow your partition.

        For example, run the following if your disk is ***sdc*** and the LVM partition is ***1***:

        ```
        sudo growpart /dev/sdc 1
        ```

        ii. Resize the Physical Volume:

        ```
        sudo pvresize /dev/sdc1
        ```

        iii. Extend the Logical Volume & Filesystem: suppose you would like to add 500G to your storage on that partition:

        ```
        sudo lvextend -L +500G -r /dev/mapper/ubuntu--vg-ubuntu--lv
        ```

        Note: The LV Path /dev/mapper/ubuntu… can be found using ***sudo lvdisplay.***

    e. In case that TYPE is 'part':
        i. Grow your partition: suppose your disk is ***sdc*** and the LVM partition is ***1***:

        ```
        sudo growpart /dev/sdc 1
        ```

        ii. Resize the Filesystem:

        ```
        sudo resize2fs /dev/sdc1
        ```

8. For VM with Rocky Linux:
    a. Install the following packages:

    ```
    sudo dnf install cloud-utils-growpart lvm2 -y
    ```

    b. Identify your Partition Layout, run ***lsblk*** command:

    ```
    lsblk
    ```

c. Look at the mount point for the folder you want to increase / (or /myStorage if it's on a separate disk). For the example below, **/acdisk** folder reside on device sdc1:

```
NAME        MAJ:MIN RM   SIZE RO    TYPE MOUNTPOINTS
sda          8:0      0   512G  0    disk
 ├─sda1       8:1      0   99M   0    part    /boot/efi
 ├─sda2       8:2      0  1000M  0    part    /boot
 ├─sda3       8:3      0    4M   0    part
 ├─sda4       8:4      0    1M   0    part
 └─sda5      8:5      0 510.9G  0    part
  └─rocky-root 253:0          0 510.9G  0    lvm    /
sdb          8:16     0   64G   0    disk
 └─sdb1      8:17     0   64G   0    part    /mnt
sdc          8:32     0   500G  0    disk
 └─sdc1      8:33     0   500G  0    part    /acdisk
```

d. In case that TYPE of ***/acdsik*** is ‘lvm’:

   i. Resize the Physical Volume:

   ```
   sudo pvresize /dev/sda3
   ```

   ii. Extend the Logical Volume.

   For example, for adding 500G use:

   ```
   sudo lvextend -L +500G -r /dev/mapper/rl-root
   ```

   Note: The LV Path “/dev/mapper/rl-root” can be found using ***sudo lvdisplay.***

e. In case that TYPE is ‘part’ (i.e. XFS filesystem)

   i. Grow the partition

   ```
   sudo growpart /dev/sdc 1
   ```

   ii. Expand the XFS Filesystem

   ```
   sudo xfs_growfs /acdisk
   ```

9. Verify that the extra space was added to the requested folder:

```
df -h /acdisk
```

4.4 Installing ML-STT VM version 2.4.3

In case ML-STT deployment was chosen for version 2.4.3 (deployment models B.1 or B.2 in section 1.2), Need to install the ML-STT VM according to chapter 2.

4.5 Upgrading LLM VM to version 2.4.3

In case that LLM VM was already deployed on 2.4.2, it is required to uninstall the LLM and install version 2.4.3 instead.

See chapter 3 for LLM installation.

4.6 Upgrading VAIC on Separated VM

In case that VAIC (telephony support) on version 2.4.2 was already installed on MIA-OP VM, it will be upgraded as part of MIA-OP VM upgrade on section 4.7.

Otherwise, in case that VAIC (telephony support) on version 2.4.2 was already installed on different VM, need to upgrade this VM as well, as described below:

1. Log in as a MIA-OP admin user and navigate to the **miaop_setup** folder:

```
cd ~
cd miaop_setup/install
```

2. Delete the content of all files in miaop_setup folder and download the installation files for MIA-OP 2.4.3 to this folder.
3. Extract the tar file in the in **miaop_setup** directory:

```
tar -xvzf MiaOP_2.4.3.tar.gz
```

4. There is one installation file which need to extract with the `tar` command:

```
tar -xvzf setup_vaic*.tar.gz
```

5. Navigate to the directory with installation files:

```
cd ~
cd miaop_setup/install
```

6. Run the upgrade script:

```
{ sudo -vn || sudo -v; } && (while sudo -n true; do sleep
60; kill -0 "$$" || exit; done &) && ./upgrade.sh
```

7. Follow the prompts raised by the upgrade script and answer according to the required deployment model.

4.7 Upgrading MIA-OP VM

4.7.1 Upgrade MIA-OP VM Pre-Requisites

> **Important!** Create a backup of the existing MIA-OP VM's (using VM snapshot or other method) before starting the upgrade process.
>
> **This step is essential to protect your data in case that upgrade procedure fails.**

Follow the following preparations for the upgrade procedure:

1. Choose the target deployment model you want to reach and make sure you have prepared the required hardware for the chosen deployment model according to section 1.7. In case that storage size should be increased, follow the instructions on section 4.3.
2. Check if new licenses are required (see section 2.4.2) and get a license from AudioCodes accordingly.
3. Log in as a MIA-OP admin user and navigate to the **miaop_setup** folder:

```
cd ~
cd miaop_setup
```

4. Delete the content of all files in miaop_setup folder and download the installation files for MIA-OP 2.4.3 to this folder.
5. Extract the tar file in the in **miaop_setup** directory:

```
tar -xvzf MiaOP_2.4.3.tar.gz
```

This will extract the following files:

- containers_app_dd.mm.yy.tar.gz
- containers_rcgn_dd.mm.yy.tar.gz
- prerequirement_scripts.tar.gz
- setup_miaop_all_dd.mm.yy.tar.gz
- setup_vaic_dd.mm.yy.tar.gz

4.7.2 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
```

If VAIC (for reaching Telephony support) was also installed on this machine (and not on separated VM), then need also to extract the VAIC setup file by running:

```
tar -xvzf setup_vaic*.tar.gz
```

4.7.3 Running the Upgrade Script on MIA-OP VM

Follow the following steps for upgrading MIA-OP from version 2.4.2:

1. Navigate to the directory with installation files:

```
cd ~
cd setup_miaop_all/install
```

2. Run the upgrade script:

```
{ sudo -vn || sudo -v; } && (while sudo -n true; do sleep
60; kill -0 "$$" || exit; done &) && ./upgrade.sh
```

3. Follow the prompts raised by the upgrade script and answer according to the required deployment.

4.8 Update the Gemalto License

Follow the procedure in Appendix B, section B.5, to update the Gemalto license received from AudioCodes.

4.9 Finalizing the VAIC Upgrade

In case that Telephony support was upgraded, it is required to complete this upgrade manually on the VM on which the VAIC was upgraded.

Follow these steps to configure VAIC for the new version:

1. Execute /ac/update/create_vaic_conf.sh which will create the configuration info you need to update on the VAIC.
2. Display the vaic configuration file in folder /ac/install/original/***vaic.conf***, it will look like this:

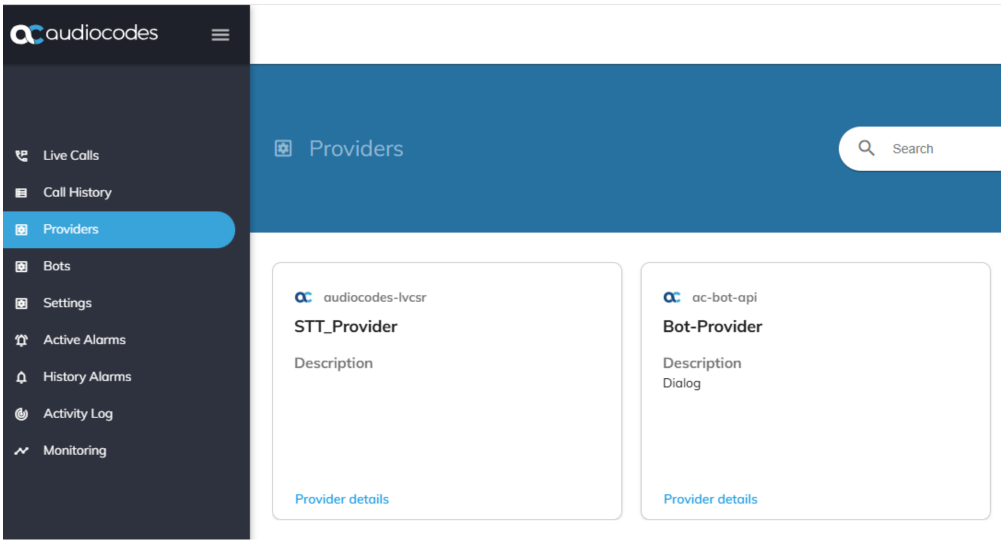
```
BOT_SERVER_HTTP_URL=https://xxx.yyy.audiocodes.com/aabot
STT_SERVER_WS_URL={"he-
il":["wss://xxx.yyy.audiocodes.com/stt"],"*":["wss://xxx.yyy
.audiocodes....}
KEYCLOAK_URL=https://xxx.yyy.audiocodes.com:8443
```

```
KEYCLOAK_REALM=master
KEYCLOAK_CLIENT=service_client
KEYCLOAK_SECRET=0kNoePJRq8IMDecW2ek3AsTxtCLbTian
```

The parameters from this ***vaic.conf*** file will be used for the configuration in the next steps.

3. Login to VAIC Web and choose the Providers setting.

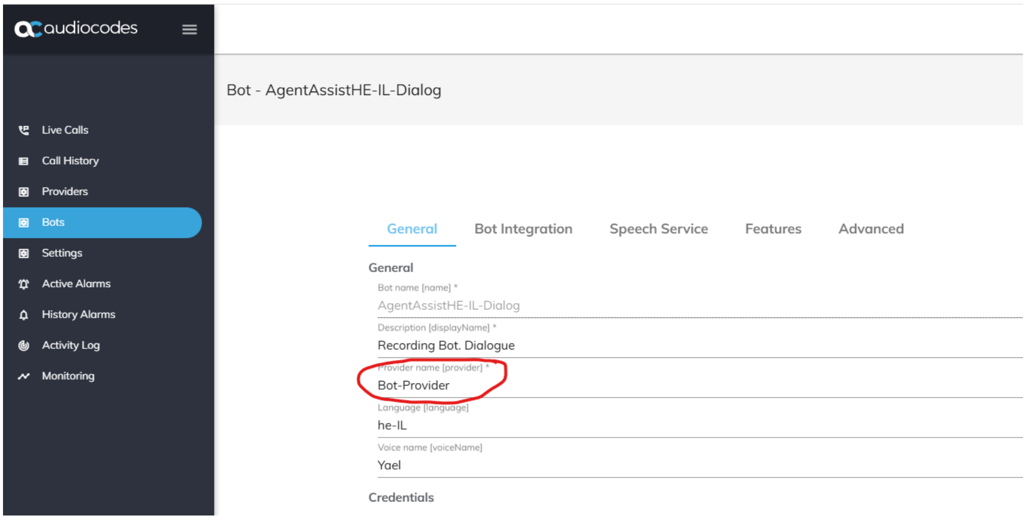
4. Each BOT configuration (mono or dialog) points to two types of providers: Bot framework provider and STT provider. In version 2.4.3, you need to change the configuration of both providers (working with an auth token):



audiocodes-lvcsr
STT_Provider
Description
Provider details

ac-bot-api
Bot-Provider
Description
Dialog
Provider details

5. In the left menu panel, navigate to the **Bots** menu and check which providers (BOT and STT) your bot uses, for BOT and for SST. (In this example we assume they are called "STT_Provider" and "Bot-Provider")



Bot - AgentAssistHE-IL-Dialog

General

Bot name [name] *
AgentAssistHE-IL-Dialog

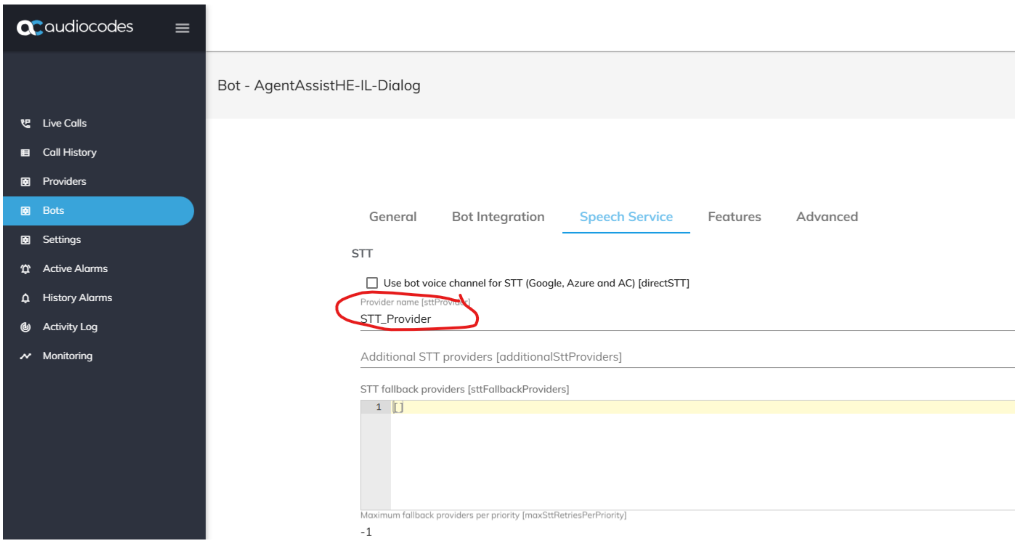
Description [displayName] *
Recording Bot. Dialogue

Provider name [provider] *
Bot-Provider

Language [language]
he-IL

Voice name [voiceName]
Yael

Credentials



Bot - AgentAssistHE-IL-Dialog

STT

□ Use bot voice channel for STT (Google, Azure and AC) [directSTT]

Provider name [sttProvider]
STT_Provider

Additional STT providers [additionalSttProviders]

STT fallback providers [sttFallbackProviders]

```
[]
```

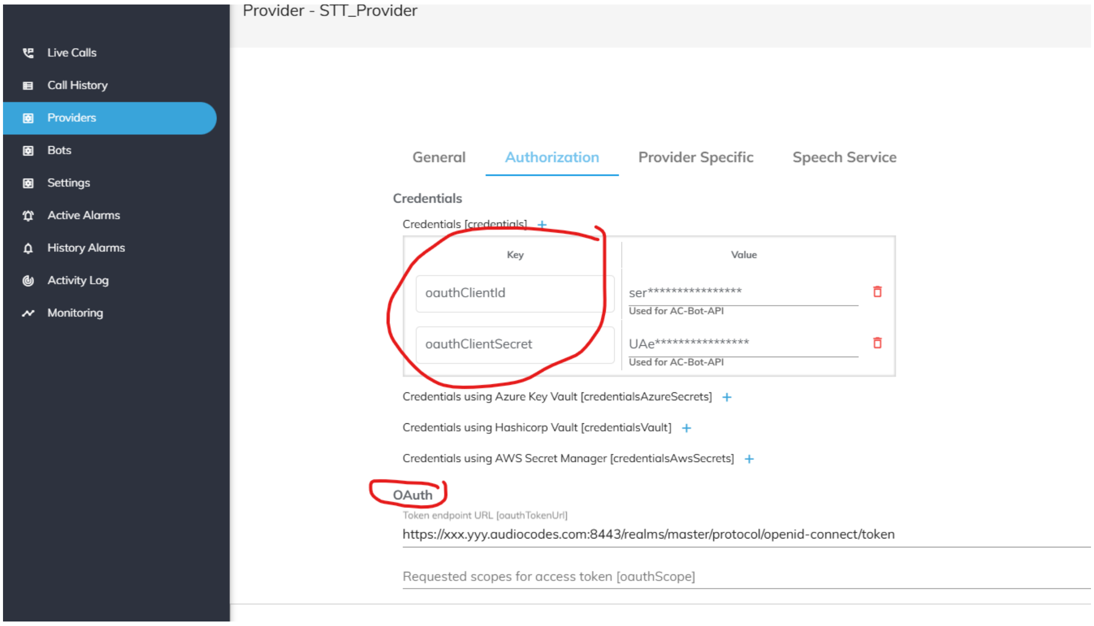
Maximum fallback providers per priority [maxSttRetriesPerPriority]
-1

6. Select "STT_Provider" from the provider list and click the **Authorization** tab.

7. Next to ‘Credentials [credentials]’, click the **+** sign and add two key values:

   - oauthClientId : **service_client** (KEYCLOAK_CLIENT value taken from **vaic.conf**)
   - oauthClientSecret: **0kNoePJRq8IMDecW2ek3AsTxtCLbTian** (KEYCLOAK_SECRET value taken from **vaic.conf**)

8. In the ‘Token endpoint URL’ field under ‘OAuth’ , enter the address of the KEYCLOAK_URL (see vaic.conf above) and concatenate to it "**/realms/master/protocol/openid-connect/token**"(e.g. https://xxxx.yyy.audiocodes.com:8443/realms/master/protocol/openid-connect/token)



Provider - STT_Provider

Credentials

Credentials [credentials] +

Key	Value
oauthClientId	ser**************** Used for AC-Bot-API
oauthClientSecret	UAe**************** Used for AC-Bot-API

Credentials using Azure Key Vault [credentialsAzureSecrets] +

Credentials using Hashicorp Vault [credentialsVault] +

Credentials using AWS Secret Manager [credentialsAwsSecrets] +

OAuth

Token endpoint URL [oauthTokenUrl]
https://xxx.yyy.audiocodes.com:8443/realms/master/protocol/openid-connect/token

Requested scopes for access token [oauthScope]

9. Click the Speech Service tab. In the section ‘*Configuration override [sttOverideConfig]*’, leave only:

```
{
  "save-waveform": 1
}
```

10. Save changes.

11. In the left menu panel, navigate to the **Providers** menu .

12. Select **Bot_Provider** from the provider list and click the **Authorization** tab.

13. Next to ‘Credentials [credentials]’, click the **+** sign and add two key values:
    - oauthClientId : **service_client** (KEYCLOAK_CLIENT value taken from **vaic.conf**)
    - oauthClientSecret: **0kNoePJRq8IMDecW2ek3AsTxtCLbTian** (KEYCLOAK_SECRET value taken from **vaic.conf**)
14. In the ‘Token endpoint URL’ field under ‘OAuth’, enter the address of the KEYCLOAK_URL (see **vaic.conf** above) and concatenate to it "**/realms/master/protocol/openid-connect/token**".
    Example: https://xxx.yyy.audiocodes.com:8443/realms/master/protocol/openid-connect/token
15. Save changes.
16. Complete the configuration of the users accessing the VAIC by mapping between the incoming call to the user or users at a tenant:
    a. Enter the MIA-OP admin WEB UI.
    b. Navigate to Local User List -> Edit User Profile.
    c. Fill in the user’s phone extensions with which the user will call the MIA-OP Bot.
17. Once the configuration is complete, delete the following files to prevent revealing secret keys:

```
rm /ac/update/create_vaic_conf.sh
rm /ac/install/original/vaic.conf
```

5 Meeting Insights On-Prem Linux Docker Installation

5.1 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 on a Linux machine running either **Rocky Linux** or **Ubuntu** distributions.

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

5.2 Environment pre-installation requirements

The following table describes the software support required for installation of MIA-OP VM:

Table 8: Pre-installation requirements

#	Requirements	To be prepared	Notes
1	Docker and docker compose	Docker CE (community edition) ▪ Docker version must be 27.5.0 and above ▪ Docker compose version must be 2.32.3 and above Packages required: ▪ docker-ce ▪ docker-ce-cli ▪ containerd.io Docker utility permissions must be available to the Linux user.	For Ubuntu see: https://docs.docker.com/engine/install/ubuntu/ For Rocky see: https://docs.docker.com/engine/install/rhel/
2	3d parties packages required for flawless installation of the environment	Packages required: ▪ openssl (latest) ▪ vim ▪ nano ▪ telnet ▪ mc ▪ unzip ▪ **coreutils** sed ▪ curl ▪ mawk (Ubuntu) / gawk (Rocky) ▪ dnsutils (Ubuntu) / bind-utils (Rocky) ▪ dmidecode	Use for the installation: ▪ **sudo dnf install <package name>** for Rocky ▪ **sudo apt install <package name>** for Ubuntu
3	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.

#	Requirements	To be prepared	Notes
4	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.
5	Disable SELinux	SELinux must be disabled on the provided Linux machines	Check SELinux on Ubuntu: ■ **sudo apt install** policycoreutils ■ **sestatus** Check SELinux on Rocky Linux: ■ **sudo dnf install** policycoreutils selinux-policy-targeted libselinux-utils ■ **sestatus**

5.3 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 9: 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)
9443 (any – Meeting Insights On-Prem)	internal and external
25/2525 (Meeting Insights On-Prem– mail server)	Port used by Meeting Insights On-Prem

5.4 Installation of Gemalto Server

5.4.1 Installation of Gemalto Server

Follow Appendix B to install the Gemalto License Server on MIA-OP VM.

> If you already have Gemalto License Server installed on different VM, you can reuse that Gemalto Server, but need to update the IP address of that server in the environment parameters as described in section 5.8.

5.4.2 Requesting Gemalto License

Before starting the installation process, make sure you have requested a Gemalto license from AudioCodes as described in section 1.8.2.
Make sure the license request will fit the requested deployment model, as described in section 1.7.

5.4.3 Uploading Gemalto License

Follow the procedure in Appendix B, section B.5, to update the Gemalto license received from AudioCodes.

5.5 Software Preparation for Installation

On the installation Linux machine, perform the following steps:

1. Log in as a MIA-OP admin user who belongs to the **sudoers** group.

```
sudo usermod -aG sudo <username> (for Ubuntu)
```

```
sudo usermod -aG wheel <username> (for Rocky)
```

2. After successfully downloading and validating the Meeting Insights On-Prem installation package file (MiaOP_2.4.3.tar.gz), create the **/miaop_setup** directory (if it does not already exist) in the /home/<user>/ path, then copy the file into that directory.
3. Extract the installation file in the /miaop_setup directory:

```
tar -xvzf MiaOP_2.4.3.tar.gz
```

This extracts the following files:

- containers_app_dd.mm.yy.tar.gz
- containers_rcgn_dd.mm.yy.tar.gz
- prerequirement_scripts.tar.gz
- setup_miaop_all_dd.mm.yy.tar.gz
- setup_rcgn_dd.mm.yy.tar.gz

4. Navigate to the /miaop_setup directory:

```
cd ~
cd miaop_setup
```

5. Validate the checksum of the files with the below command:

```
sha256sum -c sha256sum.txt
```

6. Extract the prerequirement tar.gz file.

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

7. Add the MIA-OP admin user to the docker group:

```
sudo usermod -aG docker <username>
```

8. For Ubuntu – disable AppArmor:

```
sudo aa-teardown
sudo systemctl stop apparmor
sudo systemctl disable apparmor
```

9. Navigate to the directory prerequirements folder:

```
cd prerequirement_scripts
```

10. Run the script **check_all.sh**.

```
./check_all.sh
```

11. Review the script output on screen for any error messages marked in red or yellow, and correct the issues as needed.

    Note: GPU is not required for deployments 1.A, 1.B and 1.C.

12. If the check is completed without errors, proceed with the installation.
13. If issues remain, consult with AudioCodes support using the generated log file **script.log**.

5.6 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
```

If the VAIC containers for reaching Telephony support are also installed on this machine, extract the VAIC file by running:

```
tar -xvzf setup_vaic*.tar.gz
```

5.7 Running the Installation Script

To run the installation script, go to the installation folder and run it:

```
cd setup_miaop_all/install/
{ sudo -vn || sudo -v; } && (while sudo -n true; do sleep 60;
kill -0 "$$" || exit; done &) &&./install.sh
```

When prompted, provide the following inputs:

1. Which STT type do you want to install?

   ```
   -  Hebrew/English STT (AudioCodes STT)
   -  Multi-Languages STT (ML-STT)
   ```

2. Do you want to install VoiceAI Connect on this computer? [y/n]

   Note: VoiceAI Connect (VAIC) is essential for transcription of telephony sessions.

3. Please enter MIAOP_HOME directory: /ac
   - Default: `/ac`
   - Press **Enter** to accept the default.
4. Please enter MIAOP_DISK directory: /acdisk
   - Default: `/acdisk`

     The MIAOP_DISK is where all database and voice files will be stored for the long term. You must ensure that this folder resides in a partition which has enough free storage so it can increase in size dramatically.
   - Press **Enter** to accept the default.
5. Certificate setup options:
   The script pauses to let you choose between two setup paths:

   a. **Pause installation** – Recommended if using a private or well-known authority certificate.

   b. **Continue without pause** – For self-signed certificate usage.

      If you have certificates from a well-known or private Certificate Authority, copy them to /ac/certs with the following filenames:

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

    - If using a private CA, also include:
        - Root CA: rootCA.crt
        - Intermediate CA: intrCA.crt

6. Certificate Handling:

   If installation was **paused** for certificate setup, copy the required certificates to **/ac/certs** as described in Step 4.

5.8 Running the Setup Script

1. If the Gemalto License server was installed on a different machine than the MIA-OP VM, then you need to update its IP address in the .env file:

   ```
   cd /ac
   vi ./.env
   ```

   Search (or add, if not existing) the GEMALTO_LICENSE_IP parameter, and set the correct IP address of your Gemalto License server. For example:

   GEMALTO_LICENSE_IP=10.3.0.4

2. Resume the setup by running:

   ```
   cd /ac/install/
   { sudo -vn || sudo -v; } && (while sudo -n true; do sleep
   60; kill -0 "$$" || exit; done &) && ./setup.sh
   ```

3. Continue for the next prompts.

   You are prompted to enter the maximum Concurrent Sessions (CCS) and approve your hardware resources accordingly. The CCS is referring to the sum of concurrent offline tasks and online tasks, online tasks also including telephony sessions and meetings. **Note that if you approve continuing installation although your hardware resources are below the recommended size, then the performance might be reduced and as result the requested CCS will not be achieved within a reasonable duration.**

4. You are prompted to enter max number of off-line concurrent sessions. This figure is an upper limit for the concurrent off-line tasks and also allows a place holder reservation for online tasks according to the total CCS minus the offline CCS. Some examples:

   - If all tasks are expected to be offline, the set Offline CCS = CCS.
   - If all tasks are expected to be online, the set Offline CCS = 0.

5. You are prompted to 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

6. Select the type of certificate used, providing 3 options:

   - 1 – Certificate issued by well-known certificate authority
   - 2 – Certificate issued by private certificate authority
   - 3 – Self-signed certificate

   Enter 1 or 2 or 3 based on the type of certificate you prepared in section 4.

7. Enter the **tenant** name or names (comma-separated):

   - Provide one or more tenant names, separated by commas.
   - Example*:* tenant1,tenant2

8. System admin user:

   - Provide the master admin user name to the system (default provided “adm”).

- Example*:* Administrator

9. System admin password:
    - Provide the master admin password to the system (default provided an auto generated password).
    - Example*:* xCf56G6
10. Enter the SMTP server address:
    - Provide the SMTP server address provided by customer.
    - Example*:* SMTP.mail.com

> If not provided, there will be no mail support, and the following three SMTP related prompts are not shown.

11. Enter the SMTP server user:
    - Provide the SMTP server user credentials provided by customer.
12. Enter the SMTP server password:
    - Provide the SMTP server password credentials provided by customer.
13. Enter the email address of the sender:
    - Provide the SMTP server user email address used for sending emails.
    - This value must be supplied by the customer.

The installation process takes approximately 10 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.

> At the end of the installation process, you **must** set the environment variables by running:
>
> source ~/.bashrc

6 Initial Configuration

This chapter explains the initial configuration required after installation.

6.1 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:

```
https://<main-url>/offline_client/
```

1. Hide 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
   ```

2. Access tenants when list is hidden:

   If **EXPOSE_TENANTS_LIST** is set to **false**, the tenant list is not shown on the main page. To access a tenant, enter the tenant name manually in the text field on the login page using a direct URL:

   ```
   https://<main-url>/offline_client?tenant=<tenant-name>
   ```

3. Access the master tenant:

   ```
   https://<main-url>/offline_client?tenanat=master
   ```

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

6.2 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:

   ```
   ./stop.sh
   ./start.sh
   ```

6.3 Exchanging Additional Configuration Needed

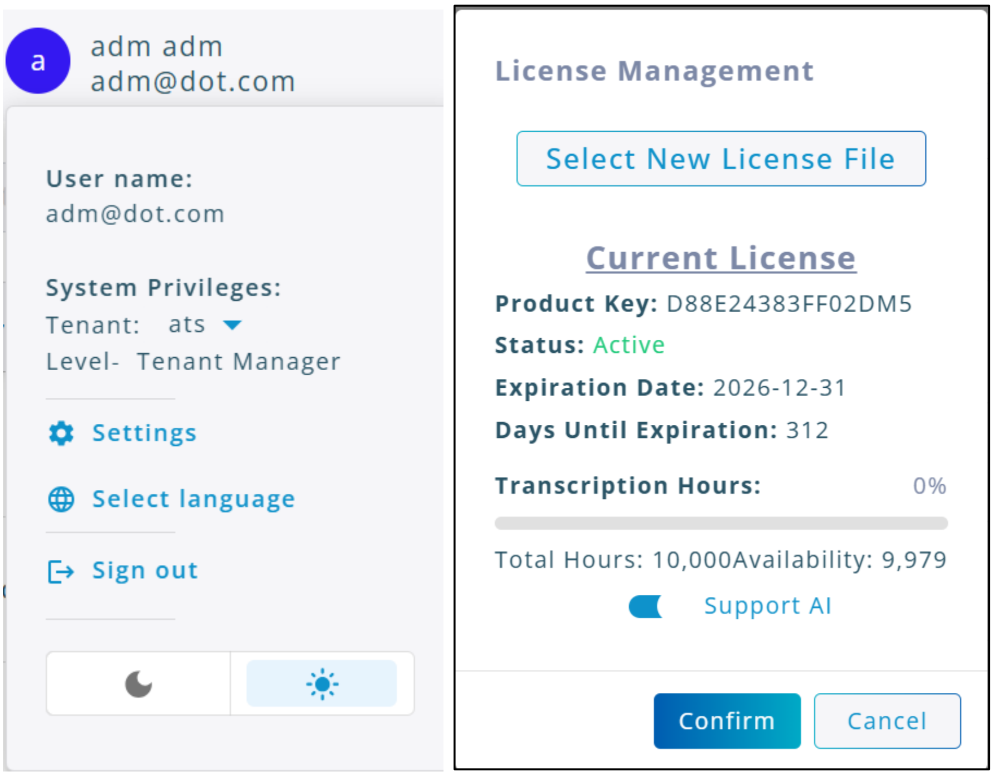
If the Customer uses **Microsoft Exchange** as the mail server for sending emails from the Meeting Insights On-Prem system, the following configuration steps are required:

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.

6.4 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 **License Management**.
5. Click **Select New License** and upload the provided license file.
6. Review the license details and click **Confirm** to complete the installation.



User name: adm@dot.com

System Privileges:
Tenant: ats
Level- Tenant Manager

Product Key: D88E24383FF02DM5

Status: Active

Expiration Date: 2026-12-31

Days Until Expiration: 312

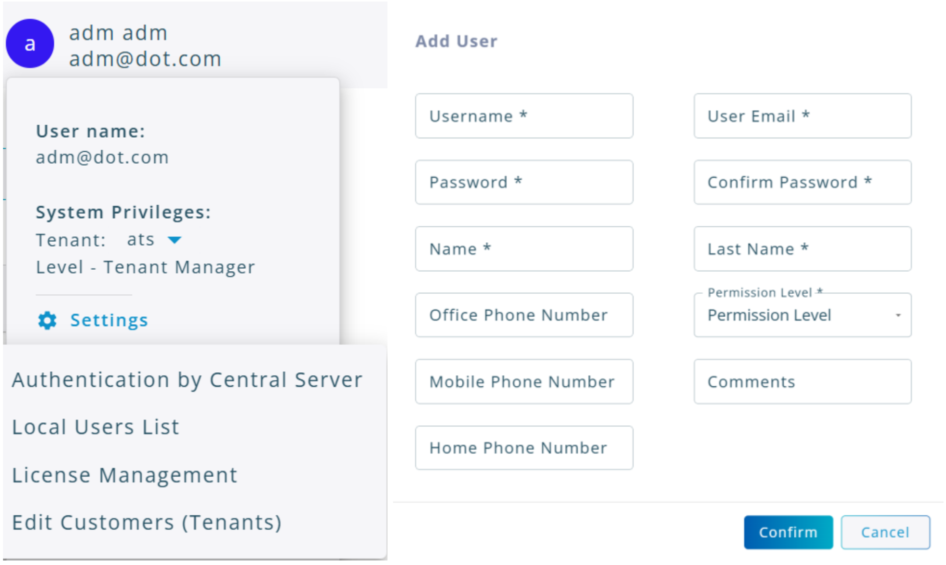
Transcription Hours: 0%

Total Hours: 10,000Availability: 9,979

6.5 Adding Users to a 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.



a adm adm
adm@dot.com

User name:
adm@dot.com

System Privileges:
Tenant: ats
Level - Tenant Manager

Settings

Authentication by Central Server
Local Users List
License Management
Edit Customers (Tenants)

Add User

Username *
User Email *
Password *
Confirm Password *
Name *
Last Name *
Office Phone Number
Permission Level *
Permission Level
Mobile Phone Number
Comments
Home Phone Number

Confirm
Cancel

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

7 Basic Functionality Tests

7.1 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**.

7.2 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.

7.3 Checking Dictation Client

The dictation client is disabled when choosing to work in Deployment models B.1 or B.2.

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.

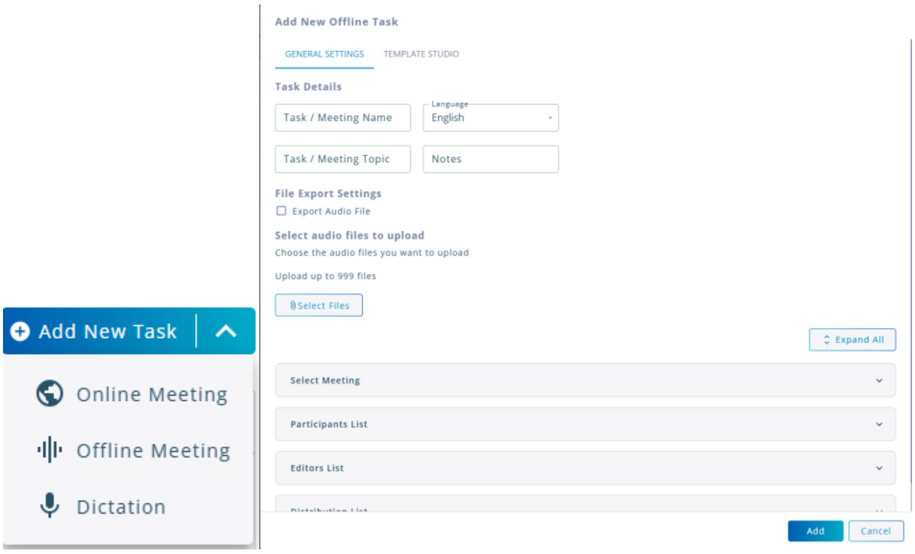
   b. Verify that the alert "Connecting to STT server successfully" appears.

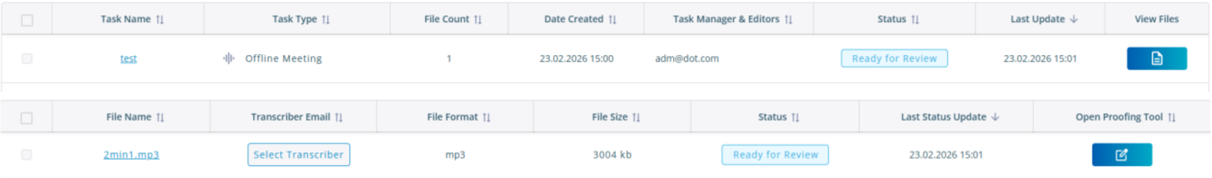
   c. Click Stop Dictation.

   d. Click **Send**.

4. Verify transcription.

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





☐	Task Name	Task Type	File Count	Date Created	Task Manager & Editors	Status	Last Update	View Files
☐	test	Offline Meeting	1	23.02.2026 15:00	adm@dot.com	Ready for Review	23.02.2026 15:01	

☐	File Name	Transcriber Email	File Format	File Size	Status	Last Status Update	Open Proofing Tool
☐	2min1.mp3	Select Transcriber	mp3	3004 kb	Ready for Review	23.02.2026 15:01	

8 Maintenance

8.1 Changing Deployment Model

After the installation is complete, it is possible to increase the deployment model in order to increase the maximum concurrent sessions (CCS):

- Increase deployment model 1.A to 1.B or 1.C (i.e., from 4CCS to 16CCS or 30CCS)
- Increase deployment model 2.A to 2.B (i.e., from 16CCS to 30CCS)

8.1.1 Increasing Deployment Model from 1.A

The following sections describe the steps for increasing deployment model from 1.A to 1.B or 1.C.

To Choose your Target Deployment Model:

Choose your target deployment model (1.B or 1.C) according to section 1.7.

Make sure you have the available vCPUs, memory and storage resources according to Table 3: HW specification.

Requesting a new Gemalto License:

Due to increasing the CCS, a new Gemalto license should be prepared. When asking AudioCodes for a new Gemalto license, please specify:

1. The newly requested deployment model: 1.B or 1.C.
2. Will AI be used: yes / no.
3. Machine Fingerprint – as described in Appendix B, section B.4.

Increasing the MIA-OP VM Size:

Increasing the MIA-OP VM size requires shutting down the MIA-OP service and should be done during a maintenance window, as follows:

1. Backup your MIA-OP VM.
2. Navigate to MIAOP_HOME, for example:

   ```
   cd /ac
   ```

3. Stop the MIA-OP service:

   ```
   ./stop.sh
   ```

4. Shutdown the MIA-OP VM.
5. In VM settings of your hypervisor: Increase the number of vCPUs, the memory size (RAM) and the storage size according to the specification in Table 3: HW specification.
6. Apply the new VM settings and start the MIA-OP VM.
7. Navigate to MIAOP_HOME, and stop the MIA-OP service:

   ```
   cd /ac
   ./stop.sh
   ```

8. Edit the following environment file (*.env*) in file editor and change the following environment parameters:

Parameter Name	Value for 1.B	Value for 1.C
MAX_CONCURRENT_SESSIONS	16	30
WATCH_TRANSCRIBER_TRANSCRIPTION_MAX_WORKERS_ONLINE	Choose 1..16 *	Choose 1..30 *
WATCH_TRANSCRIBER_TRANSCRIPTION_MAX_WORKERS_OFFLINE	Choose 1..16 *	Choose 1..30 *
CPUSET_DB	0-1	0-1
CPUSET_APP	2-5	2-5
CPUSET_DNN	6-21	6-35
CPUS_DB	0	0
CPUS_APP	3.6	3.6
CPUS_DNN	0	0

   ***Note:** The sum of Online workers + Offline workers should not exceed maximum CCS+1.

9. Save the environment file (*.env*) with the new values.
10. Follow the procedure described in section 4.3 to increase the storage size of the MIAOP_DISK folder (usually */acdisk*) in the MIA-OP VM.
11. Apply the new Gemalto license provided from AudioCodes (see Appendix B, section B.5).
12. Reset the MIA-OP VM.
13. Verify that basic functionality is working properly (see chapter 7).

8.1.2 Increasing Deployment Model from 2.A

The following sections describe the steps for increasing deployment model from 2.A to 2.B.

Requesting a new Gemalto License:

Due to increasing the CCS, a new Gemalto license should be prepared. When asking AudioCodes for a new Gemalto license, please specify:

1. The newly requested deployment model: 2.B.
2. Will AI be used: yes / no.
3. Machine Fingerprint – as described in Appendix B, section B.4.

Increasing the MIA-OP VM Size:

Increasing the MIA-OP VM size requires shutting down the MIA-OP service and should be done during maintenance window.

1. Backup your MIA-OP VM.
2. Navigate to MIAOP_HOME, for example:

```
cd /ac
```

3. Stop the MIA-OP service:

```
./stop.sh
```

4. Shutdown the MIA-OP VM.
5. In VM settings of your hypervisor: Increase the storage size according to the specification in Table 3: HW specification for deployment 2.B.

6. Apply the new VM settings and start the MIA-OP VM.
7. Navigate to MIAOP_HOME, and stop the MIA-OP service:

   ```
   cd /ac
   ./stop.sh
   ```

8. Follow the procedure described in section 4.3 to increase the storage size of the MIAOP_DISK folder (usually */acdisk*) in the MIA-OP VM.
9. Apply the new Gemalto license provided from AudioCodes (see Appendix B, section B.5).

Increasing the ML-STT VM Size:

1. Shutdown the ML-STT VM.
2. In ML-STT VM settings of your hypervisor: Increase the number of vCPUs and Memory (RAM) according to the specification in Table 3: HW specification for deployment 2.B.
3. Apply the new VM settings and start the ML-STT VM.

Restarting the MIA-OP service:

1. Reset the MIA-OP VM.
2. Verify that basic functionality is working properly (see Chapter 7).

8.2 Changing Encrypted Environment Variables

Some of the variables configured during installation are encrypted (using passwords, keys and secrets).

To change one of these environment parameters (if required), use the following command line:

```
KEY=ENV_PASS VALUE='ENV_VALUE' && sed -i
"s|^${KEY}=.*|${KEY}=${VALUE}|" "$MIAOP_HOME"/.env &&
"$MIAOP_HOME/update/hide" encrypt "$KEY"
```

For example, to replace the SMTP_PASS parameter’s value with “my-new-password”:

```
KEY=SMTP_PASS VALUE='my-new-password' && sed -i
"s|^${KEY}=.*|${KEY}=${VALUE}|" "$MIAOP_HOME"/.env &&
"$MIAOP_HOME/update/hide" encrypt "$KEY"
```

9 Troubleshooting

9.1 Introduction

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

9.2 Issues Found

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

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
```

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.

Containers can’t communicate with the Keycloak server

- **Possible cause:** DHCP is not configured, and the address is not being resolved. This can also occur if DNS is configured manually in the Linux OS `/etc/hosts` file.
- **Solution:** Add a static hostname resolution entry for all containers in `compose.yaml`.

Example:

```
image: ${REGISTRY}proofingbe:${proofingbe}
extra_hosts:
    - "my.custom.domain.com:192.168.1.100"
```

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. Restart the systemd-logind:

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

A Appendix: Meeting Insights On-Prem License Server

A.1 Introduction

The Meeting Insights On-Prem License Server is keeping the following keys:

- Number of transcription hours that can be use – this will be reduced upon any audio session / meeting, according to its length.
- AI support – Enable / Disable AI support
- Expiration date

A.2 Get System ID

The following steps explain how to retrieve the UUID , i.e., the Universal Unique Identifier (FP_DATA) of the license server.

1. Navigate to the script directory:

   bash

   ```
   cd ~/miaop_setup/prerequirement_scripts
   ```

2. Run the get_computer_uuid.sh script.
3. A new text file named "computer_uuid.txt" is created in the same directory and it contains the System ID.

A.3 Request a license

Send the generated "computer_uuid.txt" file to your AudioCodes contact manager and specify:

- Which deployment model is required (choose from Table 1: Deployment models).
- Does AI (summary) feature is required or not?

A.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.

A.5 Authentication

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

- **Key**: authorization
- **Value**: Bearer 3248954350243754938576458957455

A.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
    - ` Encrypted license content

Example Request Url and headers:

```
POST https://license.miaop.audiocodes.co.uk/ decodeLicense
Content-Type: application/json
authorization: Bearer 32489543502437549385764589 57455
```

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":
"5c806eb9cf8d44e37b6672d620dcc857243878c49e7d67bf525f37d7052f9e5
9"
    },
    "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"
}
```

A.6.1 Troubleshooting

Service Not Starting

If the service doesn't start after installation:

1. Verify that the certificate files (tls.crt and tls.key) are valid.
2. Check the logs folder for error messages.
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.

B Appendix: Gemalto License Server

B.1 Introduction

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

B.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.

B.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.

B.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.

B.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

Actions:

- 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.

B.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
```

Verify that the “aksusbd-9.12.1” folder was created, by executing “ls -ltr”|find aksusbd-9.12.1“. This should find the folder..

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.

B.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:

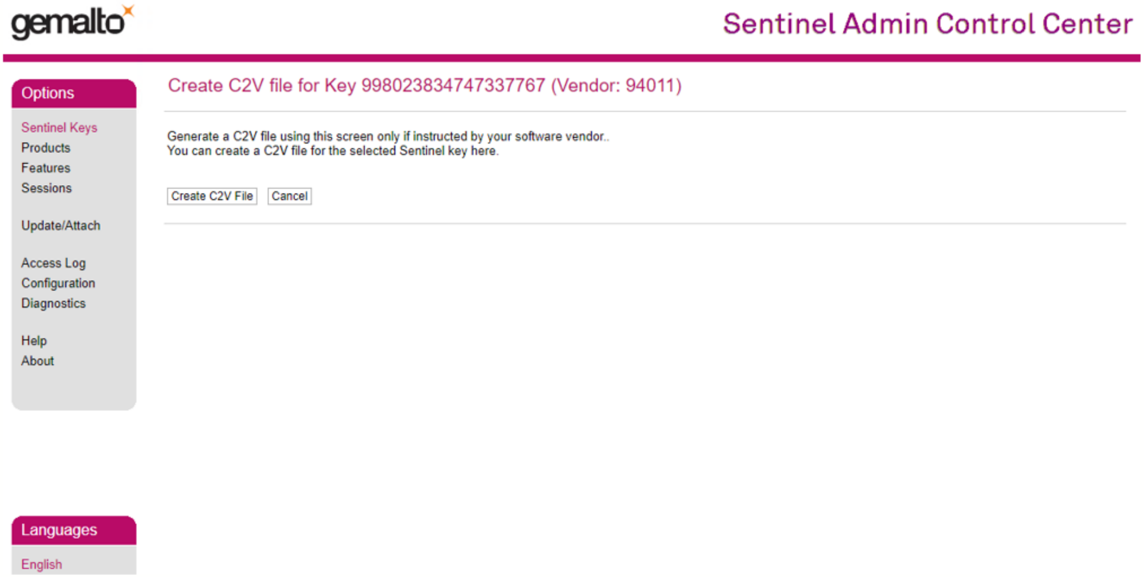
- rm -fr aksusbd-9.12.1
- rm aksusbd_94011-9.12.1.tat.gz
- rm hasplm.ini

B.4 Getting Machine Fingerprint

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

To receive the machine fingerprint:

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.



Create C2V file for Key 998023834747337767 (Vendor: 94011)

Generate a C2V file using this screen only if instructed by your software vendor..
You can create a C2V file for the selected Sentinel key here.

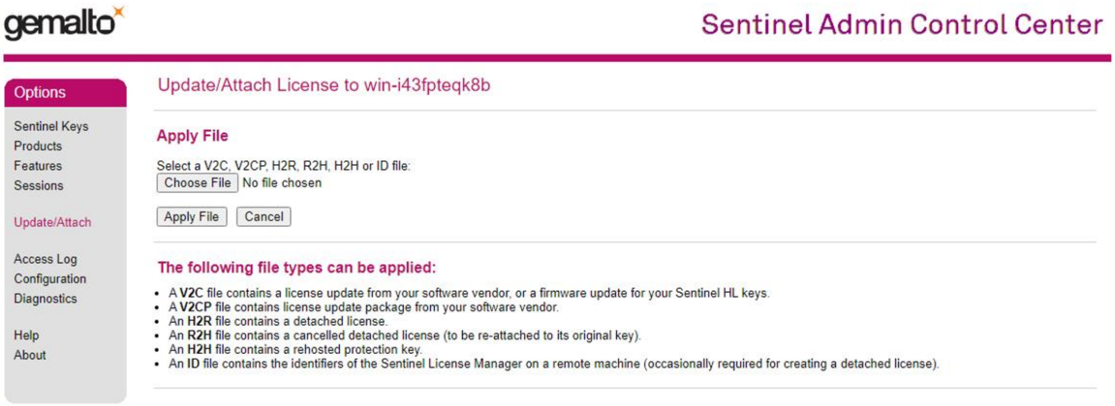
3. Send the created fingerprint (C2V file) to your AudioCodes contact person,and also specify the deployment model. AudioCodes contact person will send back the appropriate license key (V2C file).

B.5 Uploading Generated License Key and Validating Uploaded License Key

The procedure below describes how to upload the License Key and validate the uploaded license key.

To upload the license key:

Receive the V2C file from AudioCodes and then upload it to the server (Update/Attach > Choose File and Apply File).



Update/Attach License to win-i43fpteqk8b

Apply File

Select a V2C, V2CP, H2R, R2H, H2H or ID file:

The following file types can be applied:

- A **V2C** file contains a license update from your software vendor, or a firmware update for your Sentinel HL keys.
- A **V2CP** file contains license update package from your software vendor.
- An **H2R** file contains a detached license.
- An **R2H** file contains a cancelled detached license (to be re-attached to its original key).
- An **H2H** file contains a rehosted protection key.
- An **ID** file contains the identifiers of the Sentinel License Manager on a remote machine (occasionally required for creating a detached license).

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.

C Appendix: Installing Support Environment for LLM / ML-STT VM

C.1 Installation on Ubuntu 24.04

C.1.1 Preparation

Assumed Linux operating system: Ubuntu 24.04.2 LTS, architecture: x86_64 a

1. Update the OS using the package manager:

```
sudo apt-get update
sudo apt-get -y upgrade
```

2. Verify the Nvidia graphic card is recognized by the system:

```
lspci | grep -i nvidia
```

Example output:

```
00:1e.0 3D controller: NVIDIA Corporation GA102GL [A10G]
(rev a1)
```

- If your graphics card is from NVIDIA and it is listed in https://developer.nvidia.com/cuda-gpus, your GPU is CUDA-capable (which is true for 99% of Nvidia's graphic cards).
- If you do not see any output, update the PCI hardware database:

```
sudo update-pciids
```

3. Verify the version of gcc:

```
gcc --version
```

Example output (first line):

```
gcc (GCC) 14.2.1 20250110 (Red Hat 14.2.1-7)
```

- Supported versions of gcc are: 6.x - 14.x
- If you get the following error message:

```
-bash: gcc: command not found
```

It means that gcc is not installed. Install it with:

```
sudo apt-get -y install gcc
```

Then verify that a supported version of gcc was installed.

C.1.2 Installing Docker Engine (if not already installed)

Follow: https://docs.docker.com/engine/install/ubuntu/

1. Set up Docker's apt repository:
2. Add Docker's official GPG key:

```
sudo apt-get update
```

```
sudo apt-get -y install ca-certificates curl
```

```
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL
https://download.docker.com/linux/ubuntu/gpg -o
/etc/apt/keyrings/docker.asc
```

```
sudo chmod a+r /etc/apt/keyrings/docker.asc
```

3. Add the repository to Apt sources:

```
echo "deb [arch=$(dpkg --print-architecture)
signedby=/etc/apt/keyrings/docker.asc]
https://download.docker.com/linux/ubuntu $(. /etc/osrelease
&& echo "${UBUNTU_CODENAME:$VERSION_CODENAME}") stable" |
sudo tee
/etc/apt/sources.list.d/docker.list > /dev/null
```

```
sudo apt-get update
```

4. Install the Docker packages:

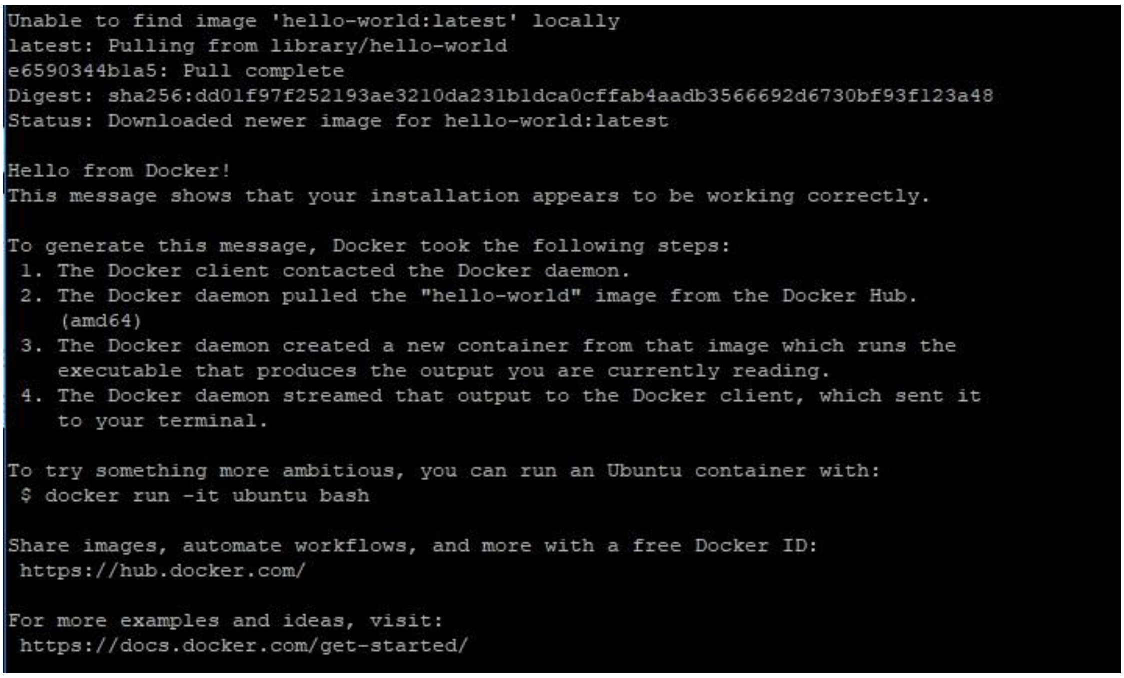
```
sudo apt-get -y install docker-ce docker-ce-cli
containerd.io docker-buildx-plugin docker-composeplugin
```

You *may* need to reboot the machine at this point (sudo reboot).

5. Verify that the installation is successful by running the hello-world image:

```
sudo docker run hello-world
```

This command downloads a test image and runs it in a container. When the container runs, it prints a confirmation message and exits:



```
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
e6590344b1a5: Pull complete
Digest: sha256:dd01f97f252193ae3210da231b1dca0cffab4aadb3566692d6730bf93f123a48
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/
```

C.1.3 Installing CUDA Toolkit and Driver

Follow: https://developer.nvidia.com/cuda-downloads?target_os=Linux&target_arch=x86_64&Distribution=Ubuntu&target_version=24.04&target_type=deb_network

Linux > x86_64 > Ubuntu > 24.04 > deb (network)

1. Install the toolkit:

```
wget
https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/x86_64/cuda-keyring_1.1-1_all.deb
```

```
sudo dpkg -i cuda-keyring_1.1-1_all.deb
```

```
sudo apt-get update
```

```
sudo apt-get -y install cuda-toolkit-12-9
```

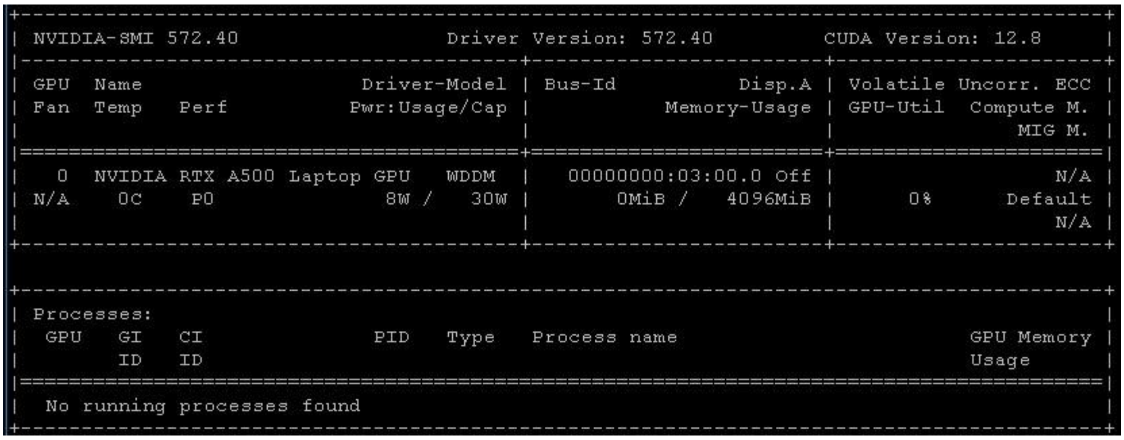
2. Install the driver (proprietary kernel module):

```
sudo apt-get -y install cuda-drivers
```

3. Verify the installation:

```
nvidia-smi
```

You should see a table with the GPU status and various details. Example output:



```
+-----------------------------------------------------------------------------------------+
| NVIDIA-SMI 572.40                 Driver Version: 572.40         CUDA Version: 12.8     |
|-----------------------------------------+------------------------+----------------------+
| GPU  Name                  Driver-Model | Bus-Id          Disp.A | Volatile Uncorr. ECC |
| Fan  Temp   Perf          Pwr:Usage/Cap |           Memory-Usage | GPU-Util  Compute M. |
|                                         |                        |               MIG M. |
|=========================================+========================+======================|
|   0  NVIDIA RTX A500 Laptop GPU   WDDM  |   00000000:03:00.0 Off |                  N/A |
| N/A    0C    P0              8W /   30W |       0MiB /   4096MiB |      0%      Default |
|                                         |                        |                  N/A |
+-----------------------------------------+------------------------+----------------------+

+-----------------------------------------------------------------------------------------+
| Processes:                                                                              |
|  GPU   GI   CI              PID   Type   Process name                        GPU Memory |
|        ID   ID                                                               Usage      |
|=========================================================================================|
|  No running processes found                                                             |
+-----------------------------------------------------------------------------------------+
```

The specific model / driver version / CUDA version may be slightly different than the provided example. The importance is that this monitor screen is shown, and not some error message.

C.1.4 Installing NVIDIA Container Toolkit

1. Install this toolkit with the following command (assuming Ubuntu distribution):

```
sudo apt-get -y install nvidia-container-toolkit
```

2. Then, configure Docker to access the GPU:

```
sudo nvidia-ctk runtime configure --runtime=docker
```

3. Verify the above command: review file `/etc/docker/daemon.json` - it should be:

```
{
    "runtimes": {
        "nvidia": {
            "path": "nvidia-container-runtime",
                "runtimeArgs": []
            }
     } }
```

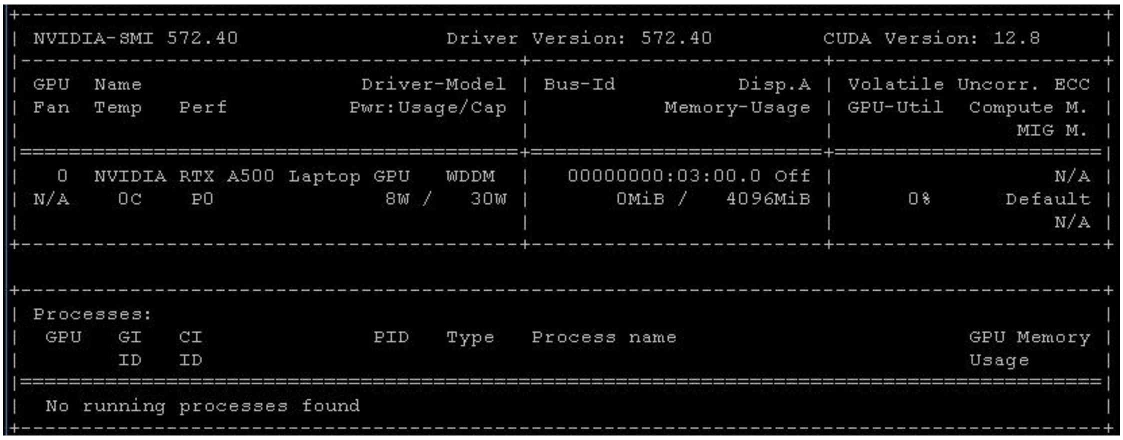
4. Apply the configuration changes by restarting the Docker service:

```
sudo systemctl restart docker
```

5. Verify: Run a Docker container that utilizes the GPU service:

```
sudo docker run --rm --gpus all nvidia/cuda:12.9.0base-
ubuntu24.04 nvidia-smi
```

You should see a table with the GPU status and various details, as output from nvidia-smi command (same as in step 3c). Example output:



```
+-----------------------------------------------------------------------------------------+
| NVIDIA-SMI 572.40                 Driver Version: 572.40         CUDA Version: 12.8     |
|-----------------------------------------+------------------------+----------------------+
| GPU  Name                  Driver-Model | Bus-Id          Disp.A | Volatile Uncorr. ECC |
| Fan  Temp   Perf          Pwr:Usage/Cap |           Memory-Usage | GPU-Util  Compute M. |
|                                         |                        |               MIG M. |
|=========================================+========================+======================|
|   0  NVIDIA RTX A500 Laptop GPU   WDDM  |   00000000:03:00.0 Off |                  N/A |
| N/A   0C    P0              8W /   30W  |       0MiB /   4096MiB |      0%      Default |
|                                         |                        |                  N/A |
+-----------------------------------------+------------------------+----------------------+

+-----------------------------------------------------------------------------------------+
| Processes:                                                                              |
|  GPU   GI   CI              PID   Type   Process name                        GPU Memory |
|        ID   ID                                                               Usage      |
|=========================================================================================|
|  No running processes found                                                             |
+-----------------------------------------------------------------------------------------+
```

The specific model / driver version / CUDA version may be slightly different than the provided example. The importance is that this monitor screen is shown, and not some error message.

C.2 Installation on Rocky Linux

C.2.1 Installation of Essential Packages

Assumed Linux operating system: Rocky 9.6 (Blue Onyx), architecture: x86_64

1. Update the OS using the package manager:

```
sudo dnf check-update
```

```
sudo dnf update -y
```

2. Verify the Nvidia graphic card is recognized by the system:

```
lspci | grep -i nvidia
```

Example output:

```
00:1e.0 3D controller: NVIDIA Corporation GA102GL [A10G]
(rev a1)
```

- If your graphics card is from NVIDIA and it is listed in https://developer.nvidia.com/cuda-gpus, your GPU is CUDA-capable (which is true for 99% of Nvidia's graphic cards).
- If you do not see any output, update the PCI hardware database:

```
sudo update-pciids
```

Then run the above `lspci` command again.

- If you get the following error message:

  ```
  -bash: lspci: command not found
  ```

  It means that package pciutils is not installed. Install it with:

  ```
  sudo dnf -y install pciutils
  ```

  Then run the above `lspci` command again.

3. Install gcc and other dependencies:

   ```
    sudo dnf -y install tar bzip2 make automake gcc gcc-c++
   elfutils-libelf-devel libglvnd-opengl libglvnd-glx libglvnd-
   devel acpid pkgconf
   ```

4. Then, verify that a supported version of gcc was installed:

   ```
   gcc --version
   ```

   Example output (first line):

   ```
   gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-5)
   ```

   Supported versions of gcc are: 6.x - 14.x

C.2.1.1 Installing Docker Engine (if not already installed)

Follow: https://docs.docker.com/engine/install/rhel/

1. Set up Docker's rpm repository:

   ```
    sudo dnf -y install dnf-plugins-core
   ```

   ```
   sudo dnf config-manager --add-repo
   https://download.docker.com/linux/rhel/docker-ce.repo
   ```

2. Install the Docker packages:

   ```
   sudo dnf -y install docker-ce docker-ce-cli containerd.io
   docker-buildx-plugin docker-composeplugin
   ```

3. Start the Docker daemon: Reboot:

   ```
   sudo reboot
   ```

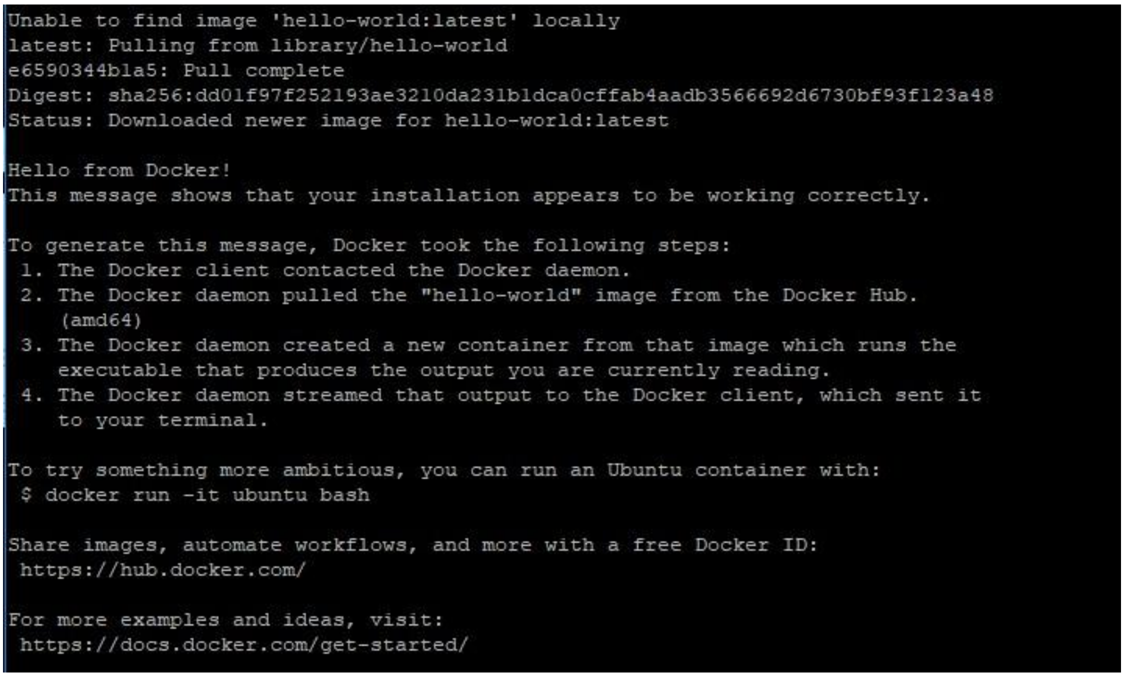
4. Then start the Docker daemon:

   ```
    sudo systemctl enable --now docker
   ```

5. Verify that the installation is successful by running the hello-world image:

   ```
   sudo docker run hello-world
   ```

This command downloads a test image and runs it in a container. When the container runs, it prints a confirmation message and exits:



```
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
e6590344b1a5: Pull complete
Digest: sha256:dd01f97f252193ae3210da231b1dca0cffab4aadb3566692d6730bf93f123a48
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/
```

C.2.1.2 Installing CUDA Toolkit and Driver

Follow: https://developer.nvidia.com/cuda-downloads?target_os=Linux&target_arch=x86_64&Distribution=Rocky&target_version=9&target_type=rpm_network

Linux > x86_64 > Rocky > 9 > rpm (network)

1. Install the toolkit:

```
sudo dnf config-manager --set-enabled crb
```

```
sudo dnf config-manager --add-repo
https://developer.download.nvidia.com/compute/cuda/repos
/rhel9/x86_64/cuda-rhel9.repo
```

```
sudo dnf clean all
```

```
sudo dnf -y install cuda-toolkit-12-9
```

2. Install the driver (proprietary kernel module):

```
 sudo dnf -y install epel-release
```

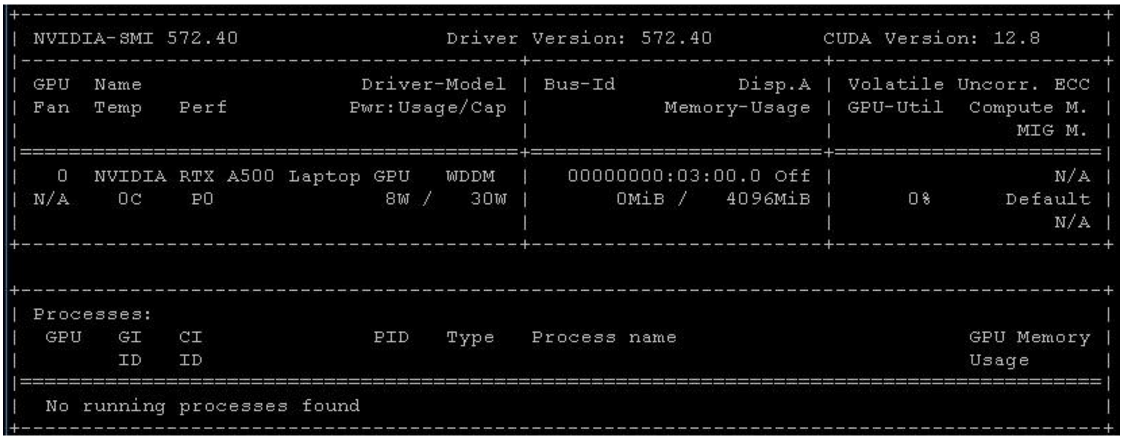
```
sudo dnf -y install kernel-devel kernel-headers perl
```

```
sudo dnf -y module install nvidia-driver:latest-dkms
```

3. Verify the installation:

```
nvidia-smi
```

You should see a table with the GPU status and various details. Example output:



```
+-----------------------------------------------------------------------------------------+
| NVIDIA-SMI 572.40                 Driver Version: 572.40         CUDA Version: 12.8     |
|-----------------------------------------+------------------------+----------------------+
| GPU  Name                  Driver-Model | Bus-Id          Disp.A | Volatile Uncorr. ECC |
| Fan  Temp   Perf          Pwr:Usage/Cap |           Memory-Usage | GPU-Util  Compute M. |
|                                         |                        |               MIG M. |
|=========================================+========================+======================|
|   0  NVIDIA RTX A500 Laptop GPU   WDDM  |   00000000:03:00.0 Off |                  N/A |
| N/A    0C    P0              8W /   30W |       0MiB /   4096MiB |      0%      Default |
|                                         |                        |                  N/A |
+-----------------------------------------+------------------------+----------------------+

+-----------------------------------------------------------------------------------------+
| Processes:                                                                              |
|  GPU   GI   CI              PID   Type   Process name                        GPU Memory |
|        ID   ID                                                               Usage      |
|=========================================================================================|
|  No running processes found                                                             |
+-----------------------------------------------------------------------------------------+
```

The specific model / driver version / CUDA version may be slightly different than the provided example. The importance is that this monitor screen is shown, and not some error message.

C.2.1.3 Installing NVIDIA Container Toolkit

1. This toolkit can be installed with (assuming Rocky distribution):

   ```
   sudo dnf -y install nvidia-container-toolkit
   ```

2. Then, configure Docker to access the GPU:

   ```
   sudo nvidia-ctk runtime configure --runtime=docker
   ```

3. Verify the above command: review file /etc/docker/daemon.json - it should be:

   ```
   {
       "runtimes": {
           "nvidia": {
               "path": "nvidia-container-runtime",
               "runtimeArgs": []
           }
       } }
   ```

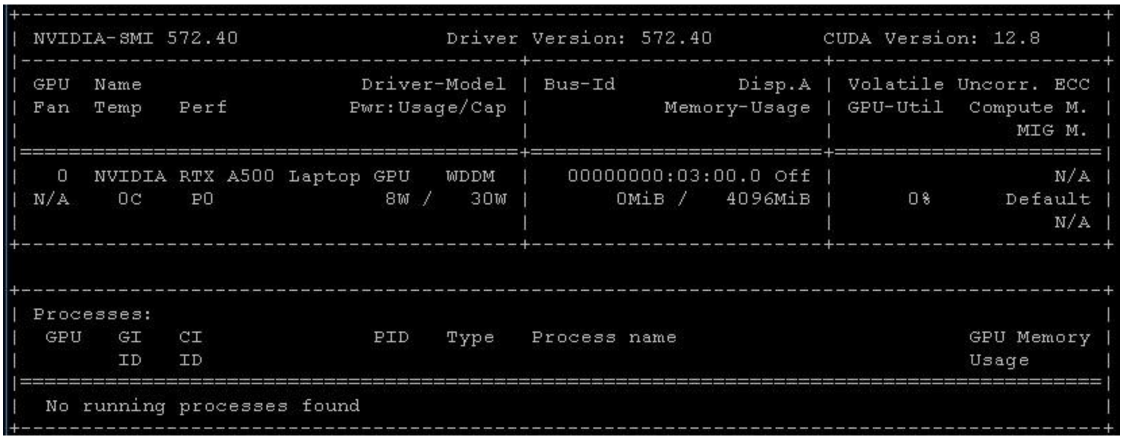
4. Apply the configuration changes by restarting the Docker service:

   ```
   sudo systemctl restart docker
   ```

5. Verify: Run a Docker container that utilizes the GPU service:

   ```
   sudo docker run --rm --gpus all nvidia/cuda:12.9.0base-
   ubuntu24.04 nvidia-smi
   ```

You should see a table with the GPU status and various details, as output from nvidia-smi command (same as in step 3c). Example output:



```
+----------------------------------------------------------------------------------------+
| NVIDIA-SMI 572.40                Driver Version: 572.40        CUDA Version: 12.8      |
|----------------------------------------+------------------------+----------------------+
| GPU  Name                 Driver-Model | Bus-Id          Disp.A | Volatile Uncorr. ECC |
| Fan  Temp   Perf         Pwr:Usage/Cap |           Memory-Usage | GPU-Util  Compute M. |
|                                        |                        |               MIG M. |
|========================================+========================+======================|
|   0  NVIDIA RTX A500 Laptop GPU   WDDM |   00000000:03:00.0 Off |                  N/A |
| N/A   0C    P0              8W /   30W |       0MiB /   4096MiB |     0%       Default |
|                                        |                        |                  N/A |
+----------------------------------------+------------------------+----------------------+

+----------------------------------------------------------------------------------------+
| Processes:                                                                             |
|  GPU   GI   CI              PID   Type   Process name                        GPU Memory |
|        ID   ID                                                               Usage      |
|========================================================================================|
|  No running processes found                                                            |
+----------------------------------------------------------------------------------------+
```

The specific model / driver version / CUDA version may be slightly different than the provided example. The importance is that this monitor screen is shown, and not some error message.

D Appendix: Keycloak Active Directory Integration Guide

D.1 Introduction

This section provides step-by-step instructions for connecting your service to Active Directory (AD) through Keycloak using LDAP user federation.

D.2 Prerequisites

- Access to Keycloak admin console.
- Active Directory credentials and connection details.
- Permission to modify environment variables and restart services.

D.3 Realm Setup

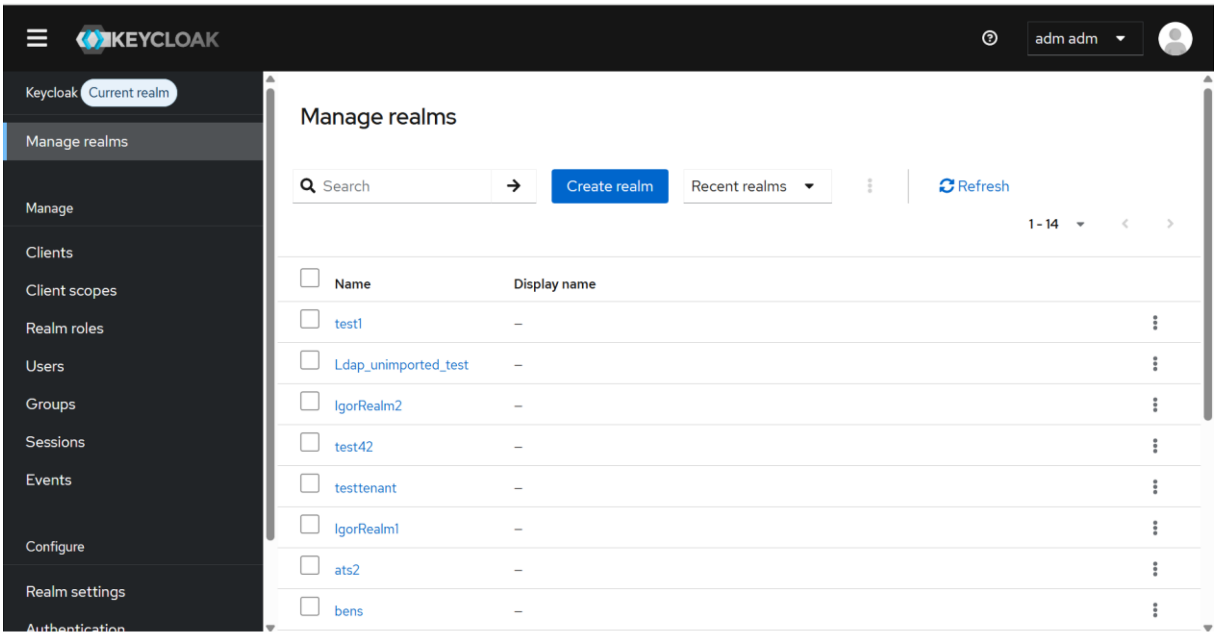
If you already have a realm, you can skip the realm creation steps above and proceed directly to D.4.

1. **Configure the realm name** - add your desired realm name to the environment variable: KEYCLOAK_REALMS
2. **Run the setup script** - execute the Keycloak setup script: ./update/kc_setup.sh
3. **Restart the service** - restart Keycloak to apply the changes.

D.4 Configure LDAP User Federation

Step 1: Access Keycloak Admin Console

1. Log in to the Keycloak admin console.
2. Navigate to your realm from the **Manage realms** in the left sidebar.

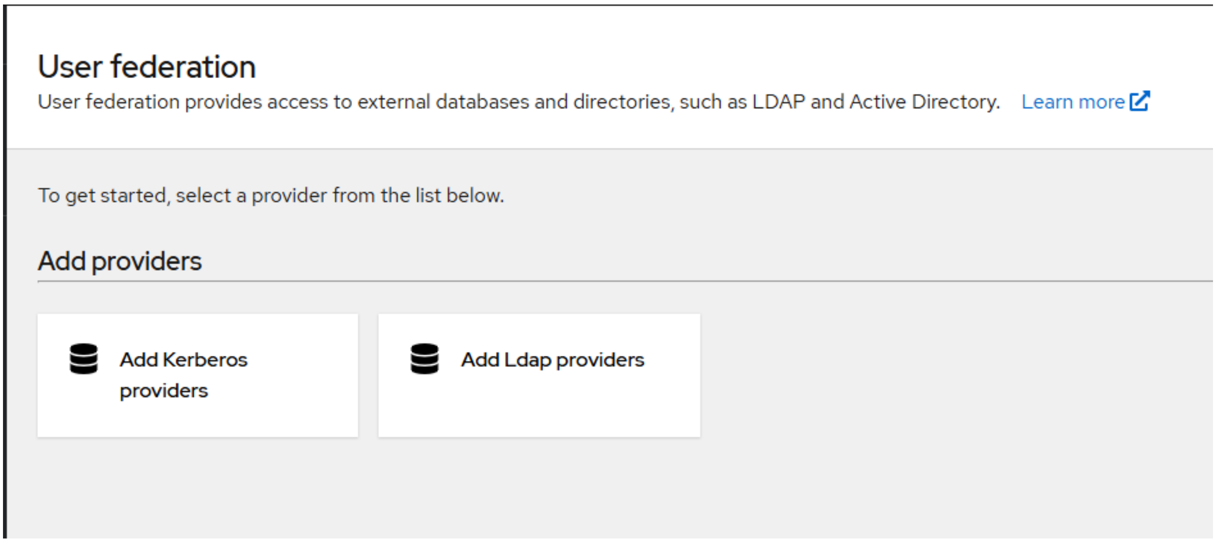


Manage realms

Name	Display name
test1	–
Ldap_unimported_test	–
IgorRealm2	–
test42	–
testtenant	–
IgorRealm1	–
ats2	–
bens	–

Step 2: Navigate to User Federation

1. In the left sidebar, click on **User Federation.**
2. Click the **Add Ldap Provider** button.



User federation

User federation provides access to external databases and directories, such as LDAP and Active Directory. Learn more

To get started, select a provider from the list below.

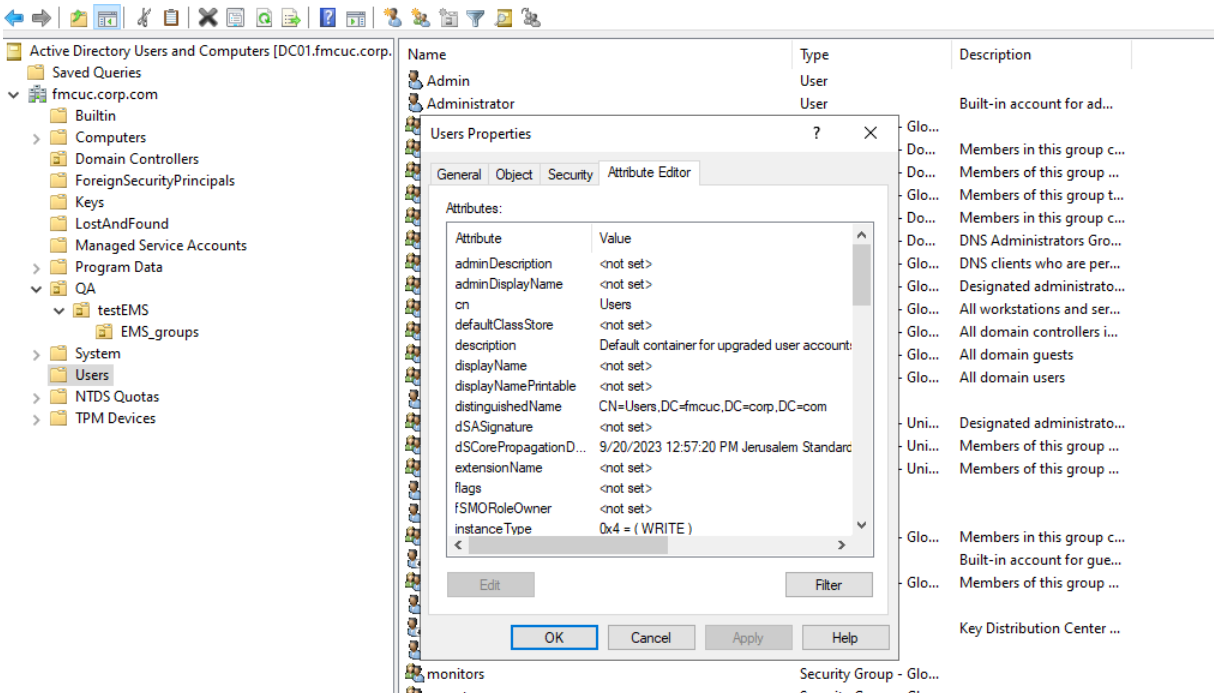
Add providers

Step 3: Configure LDAP connection settings

Fill in the following required fields:

Category	Field	Value to enter
General Settings	UI Display Name	Enter a descriptive name (e.g., "Company AD").
	Vendor	Select Active Directory.
Connection Settings	Connection URL	`ldap://<AD-server-hostname-or-ip>:389` or `ldaps://<AD-server-hostname-or-ip>:636` (for SSL)
	Enable start TLS	Off
	Use Truststore SPI	Always
	Connection pooling	Off
	Connection timeout	(Should be empty)
	Test the connection: Click Test Connection to verify Keycloak can reach your AD server.	
Authentication Settings	Bind Type	Select **simple**.
	Bind DN	Enter the Distinguished Name for the bind user.
	Bind Credentials	Enter the password for the bind user.
	Test the authentication: Click Test authentication to verify the bind credentials are correct.	
LDAP Searching and Updating	Edit Mode	Choose based on your needs: ■ **READ_ONLY**: Users cannot be modified in Keycloak. (Recommended for us). ■ **WRITABLE**: Changes in Keycloak sync to AD. ■ **UNSYNCED**: Changes stay in Keycloak only.

Category	Field	Value to enter
	Users DN	Base DN where users are located – distinguishedName. Example: `CN=Users,DC=fmcuc,DC=corp,DC=com`)
	Relative user creation DN	(Should be empty)
	Username LDAP attribute	**CN** This is the attribute name for username usage.
	RDN LDAP attribute	**CN** This is the field used to identify the user in LDAP.
	UUID LDAP attribute	**objectGUID** This is the unique ID of the user in LDAP.
	User Object Classes	**person**, **organizationalPerson**, **user** These are LDAP object types that define a user.
	User LDAP filter	(Should be empty) This is the filter that selects which LDAP entries are treated as users.
	Search scope	One level This defines how deep Keycloak searches for users in LDAP One level / subtree.
	ReadTimeout	(Should be empty)
	Pagination	Off
	Referral	(Should be empty)


Active Directory Users and Computers [DC01.fmcuc.corp.
Saved Queries
fmcuc.corp.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
QA
testEMS
EMS_groups
System
Users
NTDS Quotas
TPM Devices
Name
Type
Description
Admin
User
Administrator
User
Built-in account for ad...
Glo...
Do... Members in this group c...
Do... Members of this group ...
Glo... Members of this group t...
Do... Members in this group c...
Do... DNS Administrators Gro...
Glo... DNS clients who are per...
Glo... Designated administrato...
Glo... All workstations and ser...
Glo... All domain controllers i...
Glo... All domain guests
Glo... All domain users
Uni... Designated administrato...
Uni... Members of this group ...
Uni... Members of this group ...
Glo... Members in this group c...
Built-in account for gue...
Glo... Members of this group ...
Key Distribution Center ...
monitors
Security Group - Glo...
Users Properties
?
General
Object
Security
Attribute Editor
Attributes:
Edit
Filter
OK
Cancel
Apply
Help

Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
cn	Users
defaultClassStore	<not set>
description	Default container for upgraded user account:
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	CN=Users,DC=fmcuc,DC=corp,DC=com
dSASignature	<not set>
dSCorePropagationD...	9/20/2023 12:57:20 PM Jerusalem Standard
extensionName	<not set>
flags	<not set>
fSMORoleOwner	<not set>
instanceType	0x4 = (WRITE)

Category	Field	Value to enter
Synchronization Settings	Import users	Off
	Sync Registrations	Off
	Batch size	(Should be empty)
	Periodic full sync	Off
	Periodic changed users sync	Off
	Remove invalid users during searches	On
Kerberos Integration	Allow Kerberos authentication	Off
	Use Kerberos for password authentication	Off
Cache Settings	Cache policy	Default
Advanced Settings	Enable the LDAPv3 password modify extended operation	Off
	Validate password policy	Off
	Trust Email	Off
	Connection trace	Off

Step 4: Save and Synchronize

Click **Save** to store the configuration.

Step 5: Verify AD access via keycloak

1. Navigate to Users in the left sidebar.
2. Search for user or search * to get full user list.
3. Verify that AD users appear in the user list.

D.5 Configure Group Mapper

Group mappers allow you to import AD groups into Keycloak and automatically assign users to the predefined roles: admin, operator, and monitor.

> **This mapping must be created 3 times one for each group: admin, operator, monitor.**

Step 1: Access Mappers

1. In the LDAP provider configuration page, navigate to the **Mappers** tab.
2. Click Add Mapper.

Step 2: Configure Group Mapper

Fill in the following fields:

Category	Field	Value to enter
Basic Settings	Name	Enter a descriptive name. Example: “Admin Mapper”, “AdminMapper”
	Mapper Type	Select **group-ldap-mapper**.
LDAP Group Settings	LDAP Groups DN	Base DN where groups are located - distinguishedName Example: OU=Groups,DC=company,DC=com
	Relative creation DN	(Should be empty)

Category	Field	Value to enter
	Group Name LDAP Attribute	**CN** This is the common name of the group.
	Group Object Classes	Group (for Active Directory)
	Preserve Group Inheritance	**On** This option is to save the hierarchical AD groups and depends on the AD structure.
	Ignore Missing Groups	Off
	Membership LDAP Attribute	Member
	Membership Attribute Type	DN
	Membership User LDAP Attribute	**CN** (the user ID attribute)
	LDAP Filter	(&(objectClass=group)(cn=<group name>))
	Mode	Choose based on your needs: ■ **READ_ONLY**: Groups are imported but cannot be modified in Keycloak ■ **LDAP_ONLY**: Groups are stored only in LDAP
	User Groups Retrieve Strategy	Select **LOAD_GROUPS_BY_MEMBER_ATTRIBUTE** (recommended for Active Directory).
	Member-Of LDAP Attribute	memberOf
	Mapped Group Attributes	(Should be empty) This defines which LDAP group attributes are copied into Keycloak group attributes.
	Drop non-existing groups during sync	**Off** If turned on, this option deletes Keycloak groups that no longer exist in LDAP during sync.
	Groups Path	Define the Keycloak group path under which LDAP groups are created (/monitor/operator/admin).

Step 3: Save and Synchronize

1. Click **Save** to store the configuration.
2. Enter to the created mapper.
3. Click Action.
4. Sync Ldap groups to keycloak.

Step 4: Verify AD Groups access via keycloak

1. Navigate to **Groups** in the left sidebar.
2. Search group name <group name>.
3. Click on the selected group.
4. Navigate to Members tab to verify the group’s users display.

Step 5: Repeat this part for operator and monitor groups.

D.6 Configure User Attribute Mapper

User attribute mappers allow you to map user attributes from AD into Keycloak. In our setup, this is used to create three mappings for phone number attributes.

> **This mapping must be created 3 times one for each extension numbers: office, home, and mobile.**

Step 1: Access Mappers

1. In the LDAP provider configuration page, navigate to the **Mappers** tab
2. Click Add Mapper.

Step 2: Configure Group Mapper

Fill in the following fields:

Category	Field	Value to enter
Basic Settings	Name	Enter a descriptive name. Example: “ExtensionNumber-home”
	Mapper Type	Select **user-attribute-ldap-mapper**.
	User Model Attribute	The user property in Keycloak where the LDAP attribute will be mapped (miaop_extension.office, miaop_extension.mobile, miaop_extension.home)
	LDAP attribute	Name of mapped attribute on LDAP object. Example: homePhone
	READ ONLY	On
	Is Mandatory in Ldap	Off
	Attribute default value	(Should be empty)
	Force a default value	On
	Is Binary Attribute	Off

Step 3: Save

Click **Save** to store the configuration.

Step 4: Verify AD Attribute users synchronize in keycloak

1. Navigate to Users in the left sidebar.
2. Search for user or search * to get full user list.
3. Select user with value in extension number.
4. Check for value of extension number.

Step 5: Repeat this section for other extension numbers.

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-26039