AudioCodes Services

The Voice Experts @ Your Service

Live Platform

Data Flows, Connectivity and Security Measures

Table of Contents

Document Revision Record

Date	Description	Change Owner
16-June-2024	First release	Ofir Nakar
25-June-2024	Update with Customer Portal	Ofir Nakar
18-July-2024	- Add Secure Cloud - Add Voca as Service - Update the Service Location Table	Ofir Nakar
21-July-2024	- Add SOC 2 Type 2 chapter - Update Privacy Regulations chapter	Ofir Nakar
21-Sep-2024	- Add information for Central Syslog Service for on prem SBCs	Ofir Nakar
25-Sep-2024	- Update AI Technology for Meeting Insight Service	Ofir Nakar
24-Nov-2024	- Update Interaction Recording Service name to SmartTap NextGen - Update shared Services location in APAC	Ofir Nakar
25-Nov-2024	- Add Subnets that need to be allowed by the customer for Central Syslog outbound traffic	Ofir Nakar

1 Introduction

The purpose of this document is to present the Connectivity options, Data flows within the framework of AudioCodes Live Platform, and security measures to protect the service and the information.

AudioCodes Ltd. (hereinafter: "Company") designs, develops, and sells advanced Voice-over-IP and converged VoIP and Data networking products and applications to service providers and enterprises.

AudioCodes aspires to be the leading, innovative supplier of converged VoIP and Data solutions for service providers and enterprises globally.

The company headquarters is located in Israel.

AudioCodes is committed to safeguarding the confidentiality, integrity, and availability of all data it holds or processes, including that of its employees, partners, customers, and suppliers. To fulfill this commitment, AudioCodes' management has chosen to adopt and implement the ISO-27001 standards, establishing and maintaining an Information Security Management System (ISMS).

The company is subject to numerous State Information Security and Privacy laws and regulations, and it is the responsibility of every employee in the Company to ensure compliance with these applicable regulations.

Serving some of the world's largest enterprises with stringent security and privacy standards, AudioCodes has earned their trust in handling data and valuable assets over the years. References are available upon request.

1.1 ISO 27001

ISO 27001 is widely recognized for outlining the requirements for an Information Security Management System (ISMS). It encompasses more than a dozen policies and procedures, which AudioCodes utilizes to manage the security of various assets, including customer information, financial data, intellectual property, employee details, and information entrusted by third parties.

IQC
Institute of Quality & Control

CERTIFICATE

NO. 128264

This is to certify that
the Information Security Management System- Cyber Security Techniques of

AudioCodes Ltd.

1 Ha-Yarden St. Lod, Israel

Was audited by IQC and found to be
in compliance with the requirements of the standard:

ISO/IEC 27001:2022 – ISO/IEC 27032:2023

This certificate is valid for
the following scope of activities:

Manufacturing, marketing and sales of voice and unified communications solutions and services

According to statement of applicability Date: 14.08.2023 Version: 2

This certificate is valid until: 15.11.2025
Certification cycle will end on: 15.11.2025
Date of first approval: 15.11.2022

This certificate is subject to the continuing satisfactory operation of the Management System and periodic auditing by IQC

14.11.2023
Issue date

Nir Halpern, CEO

Institute of Quality & Control Ltd.
6 Ravnitzky St., Petah Tikva 4900617, Israel
Tel: 03-9313555, Fax: 03-9044406
E-Mail: info@iqc.co.il, www.iqc.co.il

1.2 Privacy Regulations

Audiocodes is compliant with the following Privacy regulation such as GDPR, CCPA, CPRA, LGPD and others.

All based on the GDPR which encompasses dozens of pages and imposes strict obligations on companies and organizations in virtually every aspect of collecting, processing, handling and storing personal data. At the same time, the GDPR enhances the rights of data subjects to control how their personal data are collected and used. Remedies are also defined in the GDPR language.

To ensure that our data handling practices comply with GDPR (for both our company and our customers), we have been working on GDPR compliance on an ongoing basis. We created a full set of procedures and policies with BDO as our consultant to ensure we are compliant with the GDPR.

The collection of procedures contains and is not limited to the following procedures:

- Privacy policy
- Transfer of Personal Data to Third Countries
- Record-keeping of Personal Data
- Data Retention, Restitution & Deletion
- Disclosure of Personal Information
- Data Subject Rights.

1.3 SOC 2 – Type 2

SOC 2 audits assess service organizations' security, availability, processing integrity, confidentiality controls against the AICPA's (American Institute of Certified Public Accountants) TSC (Trust Services Criteria), in accordance with SSAE 18.

Auditable Product and Service

AudioCodes Live Platform is a service delivery platform delivered from Azure.
The platform includes a range of services for UCaaS and CCaaS environments such as PSTN connectivity, contact center, recording, AI driven meeting insights, device management, user management and additional services to streamline the delivery of voice communication for any size of organization.
The platform is sold by our wire network of partners in more than 100 countries worldwide.

SOC 2 Type-2 will be provided per request after signing NDA agreement


audiocodes

SOC 2 Type II Report

REPORT ON CONTROLS PLACED IN OPERATION AT AUDIOCODES LTD. RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT INCLUDING TESTS PERFORMED AND RESULTS THEREOF.

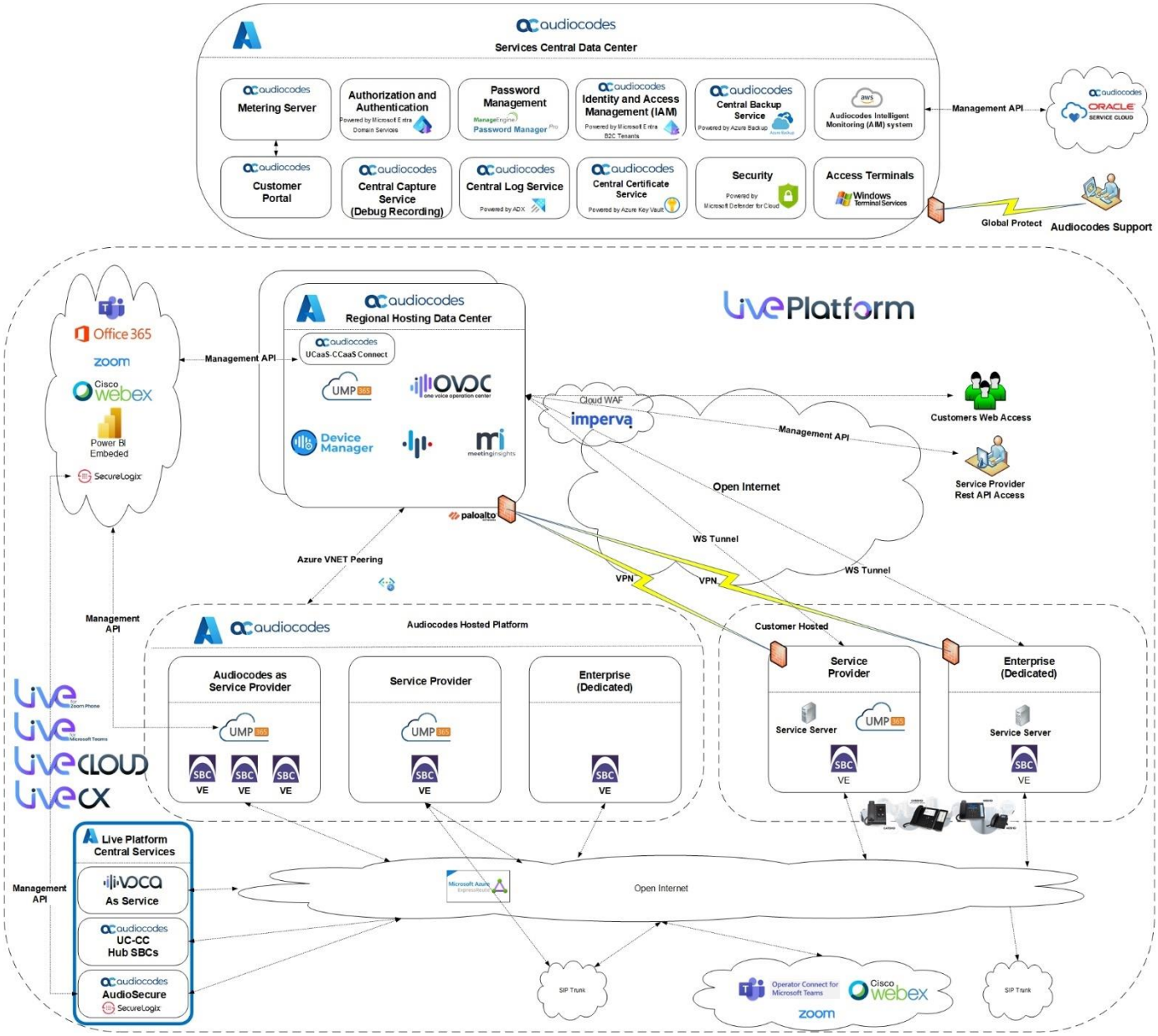
AICPA SOC

CONFIDENTIAL INFORMATION

The information contained in this report is confidential and shall not be duplicated, published, or disclosed in whole or in part, or used for other purposes, without the prior written consent of AudioCodes Ltd.

2 Live Platform Topology

The following diagram illustrates Live Platform Topology



2.1 Key Components

- Mediant Virtual Edition (VE) SBC. can be installed in High Availability mode and/or in Geo redundant mode, depending on the service level.
- UMP 365 - AudioCodes' User Management Pack 365.
- Audiocodes UCaaS-CCaaS Connect.
- Audiocodes Voca as Service.
- Live Platform Portal - One Voice Operations Center (Live OVOC).
- AudioCodes Intelligent Monitoring service (AIM).
- AudioCodes Central Log Service.
- Password Management Pro (PMP).
- AudioCodes Identity and Access Management (IAM).
- Access Terminals – Windows Terminals Server to allow access to AudioCodes Services' personnel.
- Central Certificate Service – AudioCodes' repository to save Live service' certificates.
- Service Server – Local Server for syslog and debug.
- Oracle Service Cloud - AudioCodes Support Ticketing system using Oracle Service Cloud.

2.2 Live Platform and Services Locations

The following chapter describes the global hosting locations for the Live Platform portal on Azure and specifies the services delivered in each region.

For more information about Azure location - Data Residency in Azure | Microsoft Azure

Service		Regional Live Platform Portal (Live OVOC, UCaaS-CCaaS, UMP) Azure region				
		Americas USA (East US)	**Americas Canada** (Central Canada)	**EMEA** (West Europe)	**APAC** (Australia East)	**India** (Central India)
Meeting Insights	Azure region (Service)	West US 2	X	North Europe	X	X
Device Manager		East US	Central Canada	West Europe	Australia East	Central India
SmartTap NextGen		West US 2 West Central US (Double Recording Region)	X	North Europe West Europe (Double Recording Region)	TBD	X
Live CX – HA SBCs (Shared)		Americas [1] East US West US EMEA: Germany West Central APAC [1] Southeast Asia, Korea Central	X	Americas: East US EMEA: West Europe APAC: Southeast Asia	Americas West US APAC East Asia Australia East Australia Southeast	X
Live for Teams -HA SBCs (Shared)		Americas [1] East US West US EMEA: Germany West Central APAC [1] Southeast Asia, Korea Central	X	Americas: East US EMEA: West Europe APAC: Southeast Asia	Americas West US APAC East Asia Australia East	X
Live for Zoom -HA SBCs (Shared)	Azure region (Service)	Americas [1] East US West US EMEA: Germany West Central APAC [1] Southeast Asia, Korea Central	X	Americas: East US EMEA: West Europe APAC: Australia East	Americas West US APAC East Asia Australia East Australia Southeast	X
Live Platform for Channels (Global Service – Provide to all regions)				Americas: West US 2 EMEA: West Europe South Africa North APAC: Australia East		

Live for WebEx Cisco		TBD	TBD	TBD	TBD	TBD
Hybrid Entities		TBD	TBD	TBD	TBD	TBD
Voca as Service [2]		Web and SBC: East US 2 IVRs: East US 2 North Central US	X	Web and SBC: West Europe IVRs: West Europe UK South	Web and SBC: Australia East IVRs: Australia East Australia Central	Web and SBC: Central India IVRs: Central India South India
AudioSecure		East US West US	SIP can be connected via US site	X	X	X
Live Cloud DR (Dedicated)		Per demand [3]	Per demand [3]	Per demand [3]	Per demand [3]	Per demand [3]
Operator Connect (Dedicated)		Per demand [4]	Per demand [4]	Per demand [4]	Per demand [4]	Per demand [4]
Live CX (Dedicated)		Per demand [5]	Per demand [5]	Per demand [5]	Per demand [5]	Per demand [5]
Live Dedicated		Per demand [6]	Per demand [6]	Per demand [6]	Per demand [6]	Per demand [6]

[1] Geo-Redundant option available.

[2] SIP cross connection between regions is allow.

[3] SBC HA (Appliance or SW SBC) and UMP can be hosted on any Customer's Cloud or on Premises

[4] SBCs HA (Appliance or SW SBC) and UMP can be hosted on any Customer's Cloud or on Premises

[5] SBC (Appliance or SW SBC) can be hosted on any Customer's Cloud or on Premises

[6] Some Solution Components can be hosted on any Customer's Cloud or on Premises

3 General Components Connectivity and Security Measures

3.1 General Access Management

The following describes the AudioCodes Services User life cycle, emphasizing that exclusive access to Services and on-premises systems (and their data) is restricted to authorized AudioCodes Service Engineers (only), who may be located world-wide.

- **Onboarding API:** When a new employee starts working at Compony, their details are entered into AudioCodes Oracle HR system. An API then creates a User in the corporate Active Directory without any privileges or Groups.
- **Separate Directories:** AudioCodes Global Services (AudioCodesaaS.com) manages a separate Active Directory from AudioCodes Corporate (AudioCodes.com).
- **Access Control:** Only members of *Services* AudioCodes Corp Active Directory Distribution Groups will gain access to AudioCodesaaS services production tenant. Owners (Regional Managers) of the following AudioCodes Distribution Groups are responsible for adding the desired person as member:
  - ServicesEMEA – for EMEA region
  - ServicesAmericas – for America's region
  - ServicesAPAC – for APAC region
- **User Synchronization:** The API compares all active AudioCodesaaS users with members of the AudioCodes Corp Active Directory *Services* Distribution lists. When a new user is detected in an AudioCodes Distribution Group, the API will create new user on AudioCodesaaS.
- **Termination:** When a termination date is set in Oracle by HR, the API disables the user in the corporate Active Directory
- **Comparison Process:** The API reads from the AudioCodes Corp Active Directory *Services* Distribution Groups to get the list of members in relevant groups and compares them with all users in AudioCodesaaS.
- **User Validation:** For each user found in AudioCodesaaS, the API checks if the user exists in the AudioCodes Corp Active Directory *Services* Distribution lists; if the user is not found, the user will be disabled on AudioCodesaaS.
- **Comparison Process:** The API identifies all disabled users and deletes those who have been disabled for more than 60 days.
- **Immediate Termination:** If a high-level privilege of user's termination is immediate, corporate IT has the authority to disable the user immediately, even before the last day of employment, which disables the user on AudioCodesaaS.
- **Employment Role Change:** If a user moves to another role outside of the AudioCodes Services Organization, Regional Managers must remove the user from the AudioCodes Corp Active Directory Services Distribution Group, which disables the user on AudioCodesaaS.
- **Access to AudioCodes' Services datacenter:** Access to AudioCodes' Services datacenter is facilitated using Client to Server IPSec VPN tunnel with multi-factor authentication (MFA) against AudioCodesaaS Active Directory authentication.

- **Password Requirements:** Passwords for AudioCodes' Services Active Directory must be at least 8 characters long for Engineers and 12 for administrators. They must contain characters from three of the following categories: uppercase characters, lowercase characters, digits (0-9), special characters (e.g.,!, #, $), and Unicode characters. Additionally, the password must not contain more than two characters from the username, and none of the previous 24 passwords can be reused. Users are required to change their password once every 90 days.

3.2 Environment Security

The following describes the security measures taken, concerning exclusive access to Services and on-premises systems (and their data) by authorized AudioCodes Service Engineers (only), who may be located worldwide:

- AudioCodes Service Engineers' authentication to the Access Terminal Server and UMP is done via AudioCodes' Services Active Directory.
- AudioCodes Service Engineers' authentication to the SBCs is done via AudioCodes' Services Active Directory authentication with Secure LDAP.
- AudioCodes Service Engineers authentication to the Live Platform Portal, is based on Azure Entra ID with MFA.
- (Optional) Access to AudioCodes on premise Service Server using RDP from AudioCodes' datacenter's Terminal Server (Windows server 2019) is only via the site-to-site VPN using local or domain user credentials with passwords set to never expire.
- Access to AudioCodes Live Platform Solution Components internal interfaces: RDP (3389), CLI (SSH) is permitted from AudioCodes' datacenter's Access Terminal Server (Windows server 2019) or (optional) from on-premises Service Server only.
- AudioCodes access to Live Platform portal web interface HTTPS (443) is done from public Internet protected by Cloud WAF (Imperva) and requires MFA.
- When service is fully hosted by AudioCodes. for relevant dedicated services, a dedicated Azure subscription is allocated to implement the relevant Solution Components for the Live Customers to create logical separation.
- On shared Services, logical application configuration is done to create logical separation.
- Site to Site IPSec VPN Tunnel with the following default parameters should be in place between AudioCodes' datacenter and Customer's premises:

PHASE	ATTRIBUTE	Default Values
IKE version	**IKEv2**	
Route/Policy based	**Route-based**	
Phase 1: ISAKMP - Main Mode	SA Timeout (seconds)	86400
	Hash Algorithm	SHA-256
	Encryption Algorithm	AES-256
	Diffie-Hellman (DH) Group	Group 5
Phase 2: IPSec - Quick Mode	SA Timeout (seconds)	28800
	Hash Algorithm	SHA-256
	Encryption Algorithm	AES-256
	PFS DH Group	Group 5
	Encrypted Hosts/Subnets	Should include AudioCodes devices, Service Server.

3.3 Password Manager Pro (PMP)

Password Manager Pro is a secure, password manager designed to help users securely vault and manage credentials, secrets, and other digital identities. Trusted by thousands of businesses worldwide, including Fortune 500 companies, Password Manager Pro automates enterprise password management.

PMP is used by AudioCodes Services for storing and managing shared sensitive information, such as local user credentials for all solution components (e.g. SBC, OVOC, UMP).

For more information - ManageEngine - Password Manager Pro

3.4 Microsoft Defender for Cloud

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) designed to protect cloud-based applications from a variety of cyber threats and vulnerabilities.

The Microsoft 365 Defender portal helps security teams investigate attacks across cloud resources, devices, and identities. Microsoft 365 Defender provides an overview of attacks, including suspicious and malicious events that occur in cloud environments. Microsoft 365 Defender accomplishes this goal by correlating all alerts and incidents, including cloud alerts and incidents.

AudioCodes enables Defender for Cloud to perform security assessment and vulnerability scan on Azure Services Platform

For more information - Microsoft Defender for Cloud | Microsoft Learn

3.5 Cloud WAF - Imperva

Imperva Cloud WAF offers the industry's leading web application security firewall, providing enterprise-class protection against the most sophisticated security threats. Imperva Cloud WAF is a key component of Imperva's market-leading, full stack application security solution which brings defense-in-depth to a new level.

As a cloud based WAF, it ensures that Live Platform website interfaces are always protected against any type of application layer hacking attempt. WAF is managed by Audiocodes Services' Core engineers only.

Client signatures are updated from time to time by Imperva as needed. This article lists all the client signatures and last update date:

https://docs.imperva.com/bundle/cloud-application-security/page/settings/client-classification.htm

All Services' Web and Rest API interfaces that are used by Audiocodes Live Platform are utilizing the WAF. For more information - Imperva Web Application Firewall (WAF) | App & API Protection

3.6 Central Log Service

Central Log Service is an internal log system powered by Azure Data Explorer (ADX),

The service stores in a central location Syslog and other log information such as CDR/SDR sent by the SBC (MP1288, Mediant 500/500L/800/1000/2600/3100/4000/90xx/SW-SBC); the information is used for debugging, service analyzing and billing purposes.

The data includes the following information, which may be used to identify a person, and which is based on RFC3261:

- Caller and/or Callee Name
- Caller and/or Callee Phone number
- Caller and/or Callee URI

The service provides central log services for AudioCodes Engineers with the following features set:

- **Data Residency:** The central topology should consist of four separate clusters, distributed across three support regions:
  - Americas: West US 2
  - EMEA: West Europe
  - APAC: Southeast Asia
- Solution Components Log/Syslog messages are transmitted securely over SSL over the Public Network using Kafka protocol over port 9093 to the Regional Azure EventHub using TLSv1.3.
- For SBCs that hosted on customer's premises, the Syslog is transmitted over the internet (securely over SSL utilizing port 9093 to the Regional Azure EventHub).
- Full Role Base Access to the SBC's Syslog is controlled using Row Level Security Access (RLS).
- Access is restricted to personnel within the AudioCodes services organization, and it is protected with Azure MFA.
- Abnormal behavior in the Central Log service is detected.
- Data cannot be deleted or manipulated (Automatic Retention period of 30 days).
- Automatic alerts are triggered in case the SBC stops sending syslog.

Personal Data Type	On Transit	At Rest	View
Personal Data Encryption	Yes	Yes	Full details
Personal Data pseudonymization	No	No	Full details, View Personal Data pseudonymization can be enable on demand

Note: For SBCs that hosted on customer's premises, customer need to allow internet outbound traffic to the following FQDNs on port 9093, which requires estimated bandwidth of 250Kbps per call initiation.

EMEA: Syslog-EMEA-EH.servicebus.windows.net
Americas: Syslog-America-EH.servicebus.windows.net
APAC: Syslog-APAC-EH.servicebus.windows.net

The Subnets in the following files need to be allowed by the customer for outbound traffic

Date source: Download Azure IP Ranges and Service Tags – Public Cloud from Official Microsoft Download Center

3.7 Debug Information

The Managed Device can send debug recording packets to the Central DR Server. When debug recording is activated, the device duplicates all messages sent and/or received by it and then sends them to an external server defined by an IP address.

The debug recording can be done for different types of traffic, such as RTP/RTCP, T.38, ISDN, CAS, and SIP. Debug recording is useful for advanced debugging when analysis of internal messages and signals is required. Additionally, debug recording is useful for recording network traffic in environments where hub or port mirroring is unavailable, as well as for recording internal traffic between two endpoints on the same device.

Debug Recording is disabled by default and can be enabled only for troubleshooting purposes to ensure the quality of the Service. RTP streams are captured only upon customer request in order to address voice issues – the Customer must ensure that recoded Voice calls do not include personal or sensitive information.

Personal Data Type	On Transit	At Rest	View
Personal Data Encryption	No	No	Full details
Personal Data pseudonymization	No	No	Full details

3.8 Central Certificate Service

Central Certificate Service is an internal repository system powered by Azure Key Vault and Azure Web App, designed to manage Live Service's certificate for solution components that require certificates to operate, such as SBC, OVOC, UMP, WAF, etc. The service handles the certificate end-to-end operational process:

- Issue CSR with the necessary parameters.
- Once certificate has been signed by a public certificate authority, create a PFX suite and store it protected with passwords on Key Vault.
- The certificate in the PFX file (protected by password saved on PMP) can be retrieve if needed in cases of restoration or any operational needs.

Central Certificate Service does not save any private information. Central Certificate Service is restricted to personnel within AudioCodes services organization and is protected with Azure MFA.

3.9 Metering Server

AudioCodes Metering Service allows various AudioCodes 'reporting entities" (e.g., SBCs) to report consumption (usage) information to AudioCodes cloud-based metering application;

SBCs report minutes consumption and concurrent sessions usage to AudioCodes metering application. The SBCs send the report using Rest API over HTTPS every minute (even if no sessions occurred during that period).

The Metering Server does not store any Private information, the reported information is used for the following:

- Billing of Customers
- Measuring if Customers have exceeded their ordered capacity.
- Allowing Customers to view their consumption on a portal.

The Metering server is located on the Azure West Europe region and is accessible using the following portal https://metering1.audiocodes.com

3.10 Customer Metering Portal

AudioCodes Metering Service allows various AudioCodes 'reporting entities" (e.g., SBCs) to report Customer Portal is available for VoiceAI Connect and Live CX customers

It provides the following information per Live Project:

From Oracle - the number of sessions/minutes the customer ordered including the dates the subscription is valid

From the metering app – reports on the number of consumed minutes and concurrent sessions their consumption on a portal.

The Customer Metering Portal does not store any calls information, it stores the following Private information of the user that login to the portal:

- User’s Name,
- User’s Email
- User’s Phone Number

3.11 AudioCodes Intelligent Monitoring (AIM) System

The AIM system (located in USA AWS N. Virginia) analyzes and examines alarms and events from managed devices and determines how AudioCodes Managed Services should respond. This system is used by AudioCodes to operate the Service Components intelligently by analyzing the actual performance of the Service Components and by issuing run reports.

As part of the Service Components, the Customer is required to share contact information. This data is used by the AudioCodes AIM to communicate with the Customer Help Desk regarding alarms generated by Managed Devices or issues related to the Site-to-Site VPN.

For this purpose, the AIM system saves the following information in its database:

- NOC / Helpdesk Phone number
- NOC / Helpdesk Email address

Access to the above information is done via web GUI HTTPS (TCP 443) and is permitted only to AudioCodes Managed Services Administrator group.

The AIM System uses Amazon RDS service with MySQL database engine/Instance.

The database is used only by the NOC Service and protected by an Administrator user and password.

4 Service's Components Connectivity and Security Measures

The following section describes the connectivity and security measures that are taken in order to connect and secure the Service.

4.1 Live Platform Portal

Live Platform Cloud Portal - One Voice Operations Center (Live OVOC) - A Multi- Tenant web-based voice network management solution that combines management of voice network devices and quality of experience monitoring into a single, intuitive web-based application that is used by AudioCodes services to manage the service.

Live OVOC collects and stores call-related information from the SBC using Proprietary QoE secure protocol via TLS port 5001.

The call data includes the following information, which may be used to identify a person. The data is saved for a period of up to 1 year depending on the calls volume:

- Caller name
- Caller phone number
- Caller URI
- Callee name
- Callee phone number
- Callee URI
- Full SIP messages call flow.

The solution components send Alarms and/or Events to Live Platform Portal using SNMPv3 (SBC) protocol to secure traps that are generated on solution components (UMP use SNMPv2),

Live Platform Alarms retention policy maintains a maximum of 10 million alarms (for all tenants) or a duration of 1 year, whichever is reached first.

The Live Platform Portal uses Azure PostgreSQL and Cassandra Azure databases as part of its operation. The databases are implemented in a separate virtual network and cannot be accessed directly by any external entity.

Live Platform Portal's utilize single PostgreSQL for all customers, which implemented as schema-based multitenancy architecture (schema per Service Provider / Live Platform Portal's Tenant) which is valid and best practice to create multi-tenancy and segregation between customers in the same database.

Each Service Provider / Live Platform Portal's Tenant uses its own database schema. As such, the tenant identifier is the database schema itself. Since each customer will only be granted access to its own schema, this enables customer data isolation.

Live Platform Portal's PostgreSQL database stores Personal Data, which includes a main database schema that contains non-private data information (such as topology entities, profile tables, configuration tables, etc.) and another database schema per service provider tenant containing private information, such as devices, users, QoE, calls, etc.

When an Administrator needs to access the database content for debugging or bug fixes, two layers of protection are applied. Access to the authorized Access Server is secured by Domain Login and Admin credentials stored encrypted in the Azure Key Vault. Additionally, only a root user on the OVOC machine can access the OVOC database.

Personal Data Type	On Transit	At Rest	View
Personal Data Encryption	Yes	Yes	Full details
Personal Data pseudonymization	No	No	Personal Masked for Operators level

4.2 Mediant Virtual Edition (VE) SBC

Mediant Virtual SBC is a pure-software solution designed to enable connectivity and security between Enterprises' and Service Providers' VoIP networks.

The SBC provides perimeter defense to protect companies from malicious VoIP attacks. It provides voice and signaling mediation and normalization to connection any IP-PBX to any Service Provider and ensures service quality and manageability. The SBC also offers call "survivability", ensuring service continuity to enterprises served by a centralized SIP-based IP-Centrex server or branch offices of distributed enterprises. Survivability functionality enables internal office communication between SIP clients even in the case of disconnection from the centralized SIP IP-Centrex server or IP-PBX. An SBC is utilized for Live Microsoft Teams, Live CX, Live Zoom Phone services and can be Hosted on AudioCodes Hosting platform (Azure) or on the Customer's Cloud or Premises (in that case the SBC can be different SBC models).

As part of the Service, the SBC is configured by default as best practice to utilize secure protocols for VoIP (SIP Over TLS, Secure RTP), other unsecure VoIP protocol (TCP/RTP) are used only if the far end SIP entity does not support secure protocols. For management secure protocols are utilized (HTTPS, SSH, SNMPv3), whereas access is restricted to personnel within the AudioCodes services organization only.

For debugging purposes only, the SBC send the following information to Syslog server, based on the SIP protocol (RFC3261), which can be used to identify a person:

- Caller and/or Callee Name
- Caller and/or Callee Phone number
- Caller and/or Callee URI

Personal Data Type	On Transit	At Rest	View
Personal Data Encryption	Yes	Yes	Full details
Personal Data pseudonymization	Optional	Optional	Full details

4.3 User Management Pack (UMP)

UMP - AudioCodes' User Management Pack (UMP) is a software application that simplifies Microsoft 365 Tenants onboarding automation, as well as the users MACD (Move, Add, Change, Delete) and lifecycle management of Microsoft Teams policies for Microsoft Teams Direct Routing and Operator Connect capabilities.

Live Platform Rest API that isexposed by UMP, allow developer partners to integrate Microsoft Direct Routing and Operator Connect services into their solution as well as operator who wish to perform management and configuration tasks.

UMP is utilized for Live Microsoft Teams services. The UMP can be hosted on AudioCodes hosting platform (Azure) or on the Customer's Cloud or premises.

UMP synchronizes the customer's data from Microsoft Teams (Rest API over HTTPS) into a dedicated SQL database (Per Tenant)

The UMP updates Live Platform Portal with the relevant information utilizing Rest API over HTTPS

This information contains personal information such as:

- User Name
- User Phone Number
- User Email Address
- Etc.

This information is used for life cycle management and saved for the whole lifetime of the service (until the customer is retired or the user is removed from the customer tenant).

Transit/Port/Protocol	On Transit	At Rest	View
Personal Data Encryption	Yes	Yes (Disk Level)	Full details
Personal Data pseudonymization	No	No	Full details

4.4 AudioSecure Cloud

SecureLogix and AudioCodes have partnered to deliver AudioSecure Cloud to provide holistic call authentication and fraud detection for enterprises and contact centers. AudioSecure Cloud Service Leverages Live Platform. Implementing these solutions AudioCodes will connect customers to the AudioSecure Cloud Service. The customers call behavior needs to be reviewed, but by default the call profile will not change.

AudioSecure Cloud Service offers to get the score according to the call direction, for incoming calls the score is for the source number and for outgoing calls the score is for the destination number.

As part of the Service, Audiocodes SBC is utilized, the SBC is configured to utilize secure protocols for VoIP (SIP Over TLS, Secure RTP), other unsecure VoIP protocols are not in use.

The connection to SecureLogix's data centers is done via Rest API utilize HTTPS.

Management access is restricted to personnel within the AudioCodes services organization only.

For debugging purposes only, the SBC send the following information to Syslog server, based on the SIP protocol (RFC3261), which can be used to identify a person:

- Caller and/or Callee Name
- Caller and/or Callee Phone number
- Caller and/or Callee URI

Personal Data Type	On Transit	At Rest	View
Personal Data Encryption	Yes	Yes	Full details
Personal Data pseudonymization	Optional	Optional	Full details

4.5 Voca as Service

Live Voca as Service is a cloud-based contact center that provides an innovative, next-generation service experience for callers interacting with companies. It uses modern Behavioral Routing and Conversational AI technologies to tie together Workers, Agents and internal business lines under service workflows.

Voca as Service's Web interface is protected by WAF, Currently the access to the Web GUI is don directly and not via Live Platform Portal.

As part of the Service, Audiocodes SBC is utilized, the SBC is configured by default as best practice to utilize secure protocols for VoIP (SIP Over TLS, Secure RTP), other unsecure VoIP protocol (TCP/RTP) are used only if the far end SIP entity does not support secure protocols. For management secure protocols are utilized (HTTPS, SSH, SNMPv3), whereas access is restricted to personnel within the AudioCodes services organization only.

For debugging purposes only, the SBC send the following information to Syslog server, based on the SIP protocol (RFC3261), which can be used to identify a person:

- Caller and/or Callee Name
- Caller and/or Callee Phone number
- Caller and/or Callee URI

Voca as service might have internal logs that save the above information and automatically deleted after 21 days

User Information:

The Voca as Service can be configured to connect to the Customer' Azure Entra over HTTPS using Graph-API to retrieve the organization's contacts information, into the Voca's Azure MySQL database. This information is collected in accordance with the service and customer needs and may vary depending on the activity. The organization contacts' data may include the following information:

- First and last name
- Job title
- Phone numbers
- Mobile Phone number
- Email addresses
- Department

Call Information

Call information is stored Azure MySQL server for a specific time range. Once this time range elapses, call information is deleted automatically. The retention time a call remains in the Voca database is configurable by the Voca Customer Tenant administrator. The Call data may include the following information:

- Caller phone number
- Called phone number

This information is used by Voca saved for the whole lifetime of the service (either until the customer is retired or the user is removed from the customer tenant)

To erase the imported personal user information, the Voca Customer Tenant administrator can terminate the connection with the Active Directory and manually delete all the users and their personal data from the Voca Web Management Interface on demand.

Personal Data Type	On Transit	At Rest	View
Personal Data Encryption	Yes	Yes	Full details

4.6 Device Manager

Live Device Manager is a device management application module accessible through the Live Platform's user interface.

The module facilitates device management as Software as a Service (SaaS) directly from Microsoft Azure, ensuring uninterrupted, high-quality phone and meeting room experiences within the enterprise IP network. It also supports a wide range of devices.

Device Manager utilizes the Live Platform Portal's PostgreSQL database, which includes a main database schema containing non-private data information (such as topology entities, profile tables, configuration tables, etc.) and another database schema per service provider tenant containing devices (IPPs), users, QoE, calls, etc. of private information.

The information contains personal information, which are part of the devices, such as:

- User Name
- User Phone Number
- User Email Address
- Etc.

This information is used for life cycle management and saved for the whole lifetime of the service (either until the customer is retired or the user is removed from the customer tenant)

Personal Data Type	On Transit	At Rest	View
Personal Data Encryption	Yes	Yes	Full details
Personal Data pseudonymization	No	No	Full details

The following table represents firewall requirements setting for the Devices to access the public internet on top of Teams access requirements.

Transit/Port/Protocol	AudioCodes Device Manager (Cloud)-> Device (IP Phone)	Device (IP Phone) -> AudioCodes Device Manager (Cloud)
TCP 443 (HTTPS)		X

4.7 Meeting Insights Service Information

AudioCodes Meeting Insights is an AI-powered enterprise solution that allows users to record meeting-generated content (audio and screen sharing), and automatically generate meeting minutes for Microsoft Teams meetings.

Meeting Insights records, transcribes, and organizes all aspects of online meetings. It provides a centralized company platform for all meetings, webinars, and conference calls, making them easily shareable across the organization. It shifts the focus from individual access to meeting content, to a company-wide approach, aiding informed decision-making.

Meeting Insights Service is comprised of the following logical layers:

- Meeting Insights Application layer
  - **Virtual Assistant/Teams Bot**

    The Virtual Assistant joins the meetings, records the content, takes notes, records action items, and more.
  - **Business logic**

    Processing, recording, analyzing and providing a user interface.
- Meeting Insights Data layer
  - **Media Storage Space**

    Azure Blob Storage per customer is used for recording media (audio, desktop sharing, images, etc.). the Azure Blob Storage is located on a separate Azure Subscription.

    The access to customer data is restricted and can be obtained only with customer approval and AudioCodes Services' management approval.
  - **Data Storage**

    Mongo DB is a service is used to store the data (user information, recording metadata, etc.). Each customer's data is either physically or logically segregated.

4.7.1 Meeting Insights' Metadata

Meeting Insights manages, collects, and stores the following information:

- **Meeting recording:** Meeting Insights records and stores meeting-related information and meeting media obtained from Microsoft Teams. Meeting recordings may include the following information which may be used to identify a person:
  - Meeting organizer's User Principal Name (UPN)/Login-ID and name
  - Participant's UPN/Login-ID and name
  - Meeting recording Viewer's UPN/Login-ID and name
  - External Participant's name or number.
  - Meeting media (audio, content sharing, pictures)
  - Meeting recaps such as summaries, notes, decisions, and action items
- **User information:** Meeting Insights integrates with Microsoft Azure Entra to access user information and store it into the Meeting Insights database. This information is used by Meeting Insights to correlate between the meeting data and the actual usernames and to authenticate users. The users' personal data includes the following information which may be used to identify a person:

- First and last name
- Account UPN
- Email
- Voiceprint – the system creates a digital presentation of the user's voice, which is stored encrypted and separated from the username.

- **Logs:** Meeting Insights log messages stored on the Meeting Insights servers may contain CDRs and private information such as usernames and emails of meeting participants.

  AudioCodes Support engineers, who manage the Azure Hosting resources as part of the Meeting Insights as Service have access to this information.

- **AI Technology**: Meeting Insights uses AI technology such as Speech to Text, Speaker Identification, and Generative AI to improve productivity, enhance meeting experiences, and foster collaboration by generating automatic AI-insights such as meeting summaries, lists of action items, meeting outlines, and more. The Meeting Insights AI process includes converting the audio into text, transcribing it, and then analyzing the transcription to generate the AI insights. Meeting Insights utilizes Microsoft Azure Cognitive services, Speech, and Azure OpenAI Services (different to OpenAI services) or Amazon Bedrock Anthropic models. The Microsoft Azure OpenAI Service is integrated with enabled abuse monitoring and content filtering. AWS Bedrock implements automatic abuse detection. Your data is NOT available to other customers or to Azure OpenAI, Anthropic. It is NOT used to improve Azure OpenAI models, Anthropic models or AudioCodes models, or to improve any Microsoft or other third-party products or services.

4.7.2 View Information via GUI

The above information contains personal details and is accessible by the customer according to the role-based user access.

Personal Data Type	In Transit	At Rest	View via GUI
Personal Data Encryption	Yes	Yes (AES-256 algorithm)	See above
Personal Data pseudonymization	No	No	See above

4.7.3 Meeting Insights' Meetings Recording Files

The Meeting Insights server stores the Meetings' Recording files in an Azure Storage account (e.g., Blob storage per customer. By default, the files on the Azure Storage account are encrypted at rest (on Azure level).

The recorded meetings' files are accessible to the customer an contain personal details according to the User role in meeting or Administrator role. The Administrator role can be set through the UI; the administrator will have access to all of the meeting recordings.

The access to customer data is restricted and can be obtained only with customer approval and AudioCodes Services' management approval.

Personal Data Type	On Transit	At Rest
Personal Data Encryption	Yes	Yes

Personal Data Type	On Transit	At Rest
Personal Data pseudonymization	No	No

4.7.4 Meeting Insights Teams Bot

The Meeting Insights Teams Bot connects to the customer's Teams subscription and enables the recording of Teams® communications by joining the enabled users' meetings for recording user meetings. The Meeting Insights Teams Bot receives the meeting data and media through Microsoft Media Communication SDK and Graph APIs, and then uploads the metadata to the Meeting Insights application. After the meeting ends, it uploads the recorded media to the customer's Azure Storage.

During recording and until the transfer to the application or storage, the metadata and recording files are temporarily stored on the Meeting Insights Teams Bot. The Bot disks are encrypted.

Personal Data Type	On Transit	At Rest
Personal Data Encryption	Yes	Yes
Personal Data pseudonymization	No	No

4.8 SmartTap NextGen Service Information

AudioCodes Live SmartTap NextGen is an enterprise-grade recording service for Microsoft Teams, allowing enterprises to capture and index calls with customers or internal calls for compliance, quality control, and more. It is highly available service that is suitable for businesses of all sizes. With easy-to-use search, playback, and download features, users can easily record calls, then access and play back the recordings, based on call types and date ranges.

SmartTap NextGen Service is built up from the following logical layers:

- SmartTap NextGen Application Lyer
  - **Teams Compliance Recording Bot**

    The Bot is pulled in by MSFT for the targeted user calls to be recorded and records the call.
  - **Business Logic**

    The application handles business logic of the application, including processing, recording, and providing the user interface.
- SmartTap NextGen Data layer.
  - **Media Storage Space**

    Azure Blob Storage per customer is used for recordings media such as audio of the calls is located on a separate Azure Subscription

    The access to customer data is restricted and can be obtained only with customer approval and AudioCodes Services' management approval.
  - **Data Storage**

    Mongo DB is a service used to store the data (users, recording metadata, etc.). All customers' specific data is physically or logically segregated.
- Office 365 Tenant: Customer's Office 365 tenant that provide the Teams. The SmartTap NextGen Bot joins when the Teams user calls and records its audio.

4.8.1 SmartTap NextGen' Metadata

SmartTap NextGen manages, collects, and stores the following information in the MongoDB as a service:

- **Call Recording**: SmartTap NextGen records and stores call-related information. Call Metadata includes the following information:
  - Caller name
  - Caller phone number
  - Caller URI
  - Callee name
  - Callee phone number
  - Callee URI
  - Answered party name.
  - Answered party number.

- Answered party URI.
- Redirected by party name.
- Redirected to party name.

- **User Information:** SmartTap NextGen can be configured to connect to Azure Entra to retrieve users' information into the SmartTap NextGen database. This information is used in SmartTap NextGen to correlate between the call data and the actual usernames. The users' personal data includes the following:
  - First and Last names
  - Alias
  - Email
  - Additional fields defined by your organization, such as phone number, MSFT SIP URI or Tel URI to identify the user for recording.
- **Logs:** SmartTap NextGen log messages stored on the SmartTap NextGen servers and Azzure Application Insights may contain CDR private information such as usernames and emails of meeting participants.

  AudioCodes service personnel, who manage the Azure Hosting resources as part of the SmartTap NextGen as Service have access to this information.

4.8.2 View Information via GUI

The above information contains personal details and is accessible by the customer according to the role-based user access.

Personal Data Type	In Transit	At Rest	View via GUI
Personal Data Encryption	Yes	Yes (AES-256 algorithm)	See above
Personal Data pseudonymization	No	No	See above

4.8.3 SmartTap NextGen Call Recording Files

The SmartTap NextGen server saves the Calls Recording files in the Azure Storage account (e.g., Blob storage. By default, the files on the Azure Storage account are encrypted at rest (on the Azure level).

The recorded call files contain personal details and are accessible by the customer according to the Security Profile defined by the customer via the SmartTap NextGen Web GUI. The AudioCodes personnel account should be set with a security profile that blocks any access to recordings on the SmartTap NextGen as Service.

The access to customer Calls Recording is restricted and can be obtained only with customer approval and AudioCodes Services' management approval

Personal Data Type	On Transit	At Rest
Personal Data Encryption	Yes	Yes
Personal Data pseudonymization	No	No

4.8.4 SmartTap NextGen Teams Bot

The SmartTap NextGen Teams Bot connects to the customer's Teams subscription and enables recording of Teams® communications by joining the user calls enabled for recording. The SmartTap NextGen Teams Bot receives the call data and media through Microsoft Compliance Recording and Graph APIs and uploads the metadata to the SmartTap NextGen server. It uploads the recorded media at the end of the call to the media storage (e.g., Blob).

During recording and until it transfers to the SmartTap NextGen database or storage, the metadata and recording file will be temporarily stored on the SmartTap NextGen Bot. If there is a communication issue due to SmartTap NextGen or due to the storage, it can be preserved for a maximum of 24 hours or until the communication has been restored.

Personal Data Type	On Transit	At Rest
Personal Data Encryption	Yes	Yes
Personal Data pseudonymization	No	No

4.9 UCaaS-CCaaS Connect

AudioCodes UCaaS-CCaaS Connect is regional web app that is used to manage UC and CC services within the Live Platform (e.g., Zoom Phone System, Genesys SIP Connection, etc.).

UCaaS Connect communicates with the UC applications using Rest API over HTTPS to setup and manage the life cycle of the Service.

CCaaS Connect create trunks to Contact Centers and manages the routing and features of the Service.

For this purpose, UCaaS-CCaaS Connect stores the following information in its database which is not Personal data:

- Company name.
- Company Contact name.
- Company Contact email.
- Company Contact phone.

4.10 Oracle Service Cloud

As part of the managed Service, the customer will need to share contact information to be used by the AudioCodes TAC for communicating with the customer regarding managed device alarms or site-to-site VPN issues.

For this purpose, the Oracle Service Cloud stores the following information on the AIM system's database:

- Organization name/Addresses
- Contact details (Phone number, Email)
- Service Request information:
  - Subject of the service request
  - Serial Number
  - Correspondence between the customer and TAC engineer assigned to the Service Request.
  - Attachments provided by the customer or TAC engineer.
- Attachments to tickets are deleted within a one Year period. Ticket notes are not deleted.

Oracle offers appropriate data transfer safeguards to all Oracle Cloud, Consulting, Advanced Customer Support, and Technical Support customers, including Oracle's Binding Corporate Rules for Processors (BCR-p) or the EU Standard Contractual Clause.

5 Personal Data Flows

The following table illustrates the Personal Data flow between internal Solution components in the Live Platform services:

Personal Data	Source	Destination	Protocol	Comments
RFC3261 information that include the following (partial list) information, ■ Managed Device IP Address ■ Telecom SIP Trunk IP Address ■ 3rd party SIP Server IP Address ■ Caller name ■ Caller phone number ■ Caller URI ■ Callee name ■ Callee phone number ■ Callee URI ■ Call/Session Detail Record (CDR/SDR) details. ■ Voice Coder Information	SBC	Central Log Service (Over the Internet)	Syslog (SSL 9093)	Syslog is sent and saved per Call.
AudioCodes Debug Recording, proprietary protocol that includes the following (partial list) information: ■ Managed Device IP Address ■ Telecom SIP Trunk IP Address ■ 3rd party SIP Server IP Address ■ Caller name ■ Caller phone number ■ Caller URI ■ Callee name ■ Callee phone number ■ Callee URI ■ Call/Session Detail Record (CDR/SDR) details. ■ Voice Coder Information ■ RTP Streams	SBC	Central DR Service	AudioCodes Debug Recording (UDP 925)	The information is sent and saved on demand

Personal Data	Source	Destination	Protocol	Comments
XML-based, TLS secured communication for control, media data reports and SIP call flow messages that include the following information (partial list): ■ Managed Device IP Address ■ Telecom SIP Trunk IP Address ■ 3rd party SIP Server IP Address ■ Caller name ■ Caller phone number ■ Caller URI ■ Callee name ■ Callee phone number ■ Callee URI ■ SIP's Call-ID ■ Call/Session Detail Record (CDR/SDR) details. ■ Voice Coder Information ■ Voice Call Quality information (Successful/Failed Streams, Max Concurrent Streams, Streams Quality Utilization Distribution, Avg Call Duration (ACD), MOS, Packet Loss, Jitter, Delay and Echo, etc.)	SBC	Live Platform Portal	AudioCodes QoE (TLS 5001)	The information is sent and saved per Call. Applicable for AudioCodes SBC only.
User information collected from Teams. ■ User Name ■ User Phone Number ■ User Email Address ■ Etc.	UMP	Live Platform Portal	HTTPS	
Alarms and/or Events information may be included: ■ Managed Device IP Address ■ Telecom SIP Trunk IP Address ■ 3rd party SIP Server IP Address ■ Alarm/Event Information	SBC UMP	Live Platform Portal	SNMP (UDP 162)	The information is sent and saved per event.
Alarms and/or Events information may be included: ■ Managed Device IP Address ■ Telecom SIP Trunk IP Address ■ 3rd party SIP Server IP Address ■ Alarm/Event Information	OVOC	AIM System	SNMP (UDP 162)	The information is sent and saved per event.
Alarms and/or Events information may be included: ■ Managed Device IP Address ■ Telecom SIP Trunk IP Address ■ 3rd party SIP Server IP Address Alarm/Event Information	AIM System	AIM System	Rest API HTTPS (443)	The information is sent per event
Alarms and/or Events information may be included: ■ Managed Device IP Address ■ Telecom SIP Trunk IP Address ■ 3rd party SIP Server IP Address ■ Alarm/Event Information	AIM System Oracle Service Cloud	Customer's Helpdesk	SMTP (TCP 25)	The information is sent per event

The following table illustrates the Personal Data flow between the on-premises SBC and the local Service Server in Live Platform services:

Personal Data	Source	Destination	Protocol	Comments
RFC3261 information that include the following (partial list) information, ■ Managed Device IP Address ■ Telecom SIP Trunk IP Address ■ 3rd party SIP Server IP Address ■ Caller name ■ Caller phone number ■ Caller URI ■ Callee name ■ Callee phone number ■ Callee URI ■ Call/Session Detail Record (CDR/SDR) details. ■ Voice Coder Information	SBC	On Prem Service Server	Syslog (TLS 514) CDR (UDP 514)	Syslog is sent and saved per Call. CDR is sent and saved on demand
AudioCodes Debug Recording, proprietary protocol that includes the following (partial list) information: ■ Managed Device IP Address ■ Telecom SIP Trunk IP Address ■ 3rd party SIP Server IP Address ■ Caller name ■ Caller phone number ■ Caller URI ■ Callee name ■ Callee phone number ■ Callee URI ■ Call/Session Detail Record (CDR/SDR) details. ■ Voice Coder Information ■ RTP Streams	SBC	On Prem Service Server	AudioCodes Debug Recording (UDP 925)	The information is sent and saved on demand

6 Backup and Restore

The following table describes the way data is backed up.

Entity	Frequency and Method	Where
Central DC Components	Daily VM Backup	Domain Controller, AIM, PMP services backed up on daily base with retention of 14 days on the same cloud site that they installed and remote cloud site. the backups are encrypted.
Regional DC Components	Daily VM Backup	Live Platform Portal (AKS) – PostgreSQL database is set with daily Geo-Redundant backup with 7 retention period. Cassandra database is set with daily backup with 2 retention period. UMP as VM - Daily Azure Backup. Retain backup taken every day for 14 days. Retain instant recovery snapshot for 2 days. Meeting Insight – MongoDB is snapshot every 6 hours with 2 days retention. SmartTap NextGen – MongoDB is snapshot every 6 hours with 2 days retention.
SBC	Configuration Package, OVOC's Backup Manager.	The OVOC configured to automatically (daily) backup SBC configurations (ini, conf or cli script files). The backup files are managed by the Backup Manager that save 5 (five) latest backup files to be stored for each Managed Device.

The restoration of each component is executed according to the internal procedure of each service.

7 On Premises Hosting (Optional)

7.1 Service Server

The Service server is a Microsoft Windows Server which is used as a local repository on customer's premises. The server collects Syslog files 24x7which assist AudioCodes services personnel to triage and analyze the Enhanced reports. Additionally, Configuration information of the SBC/Gateway is backed up daily to the server's hard disk and can be used if restoration of the service is needed.

The Service Server's applications (NXlog Syslog Service, Wireshark, AC INI editor, AC Syslog Viewer, WinSCP, Windows IIS Service, Notepad++, etc.) are provided by AudioCodes. The Customer needs to grant AudioCodes Administrator permission for that server with a password that never expires. We recommend that the server be standalone and not be part of the Customer's domain.

7.1.1 Syslog Information

The Managed Device sends Syslog messages over TLS port 514 to the Service Server (on Customer Premises), where they are saved in txt files in "clear text" mode for a period of 30 days. The syslog contains call-related information from the Managed Device, including the following details, which may be used to identify a person (based on RFC3261):

- Caller and/or Callee Name
- Caller and/or Callee Phone number
- Caller and/or Callee URI

Transit/Port/Protocol	On Transit	At Rest	View
Personal Data Encryption	Yes	Yes - Under Customer's responsibility to implement and maintain it on the on prem Service Server, see BitLocker Chapter.	Full details
Personal Data pseudonymization	No	No	Full details

7.1.2 Debug Recording Information

The Managed Device can send Debug Recording packets to the Service Server (on Customer premises).

When the Debug Recording is activated, the device duplicates all messages that are sent and/or received by it and then sends them to an external server defined by an IP address.

Debug Recording can be done for different types of traffic, such as RTP/RTCP, T.38, ISDN, CAS, and SIP. It is used for advanced debugging when analysis of internal messages and signals is required. Debug Recording is also useful for recording network traffic in environments where hub or port mirroring is unavailable, as well as for recording internal traffic between two endpoints on the same device.

Debug Recording is disabled by default and can be enabled only for troubleshooting purposes to ensure the quality of the Service. RTP streams are captured upon Customer request only in order

to resolve Voice issues – The Customer needs to ensure that the recoded voice call does not include personal or sensitive information.

Transit/Port/Protocol	On Transit	At Rest	View
Personal Data Encryption	No	No	Full details
Personal Data pseudonymization	No	No	Full details

7.1.3 BitLocker Overview

BitLocker Drive Encryption is a data protection feature that integrates with the operating system to safeguard against data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides the highest level of protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component often included in many newer computer by computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline.

For computers that do not have TPM version 1.2 or later, you can still use BitLocker to encrypt the Windows operating system drive. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation. Starting with Windows 8, you can use an operating system volume password to protect the operating system volume on a computer without TPM. Both options do not provide the pre-startup system integrity verification offered by BitLocker with a TPM.

In addition to the TPM, BitLocker offers the option to lock the normal startup process until the user supplies a personal identification number (PIN) or inserts a removable device, such as a USB flash drive, containing a startup key. These additional security measures provide multifactor authentication and assurance that the computer will not start or resume from hibernation until the correct PIN or startup key is provided.

The following link is for the Customer's IT professional. It explains how to deploy BitLocker on Windows Server 2012 and later. It is the Customer's responsibility to implement and maintain.

https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server

For all Windows Server editions, BitLocker can be installed using Server Manager or Windows PowerShell cmdlets. BitLocker requires administrator privileges on the server to install.

7.2 Firewall Requirements

The following table outlines the connectivity matrix, including protocols, ports, and directions required to be implemented on the IPSec site to Site VPN between AudioCodes' Datacenter and Customer's Cloud or Premises. These firewall configurations allow AudioCodes Services to manage the Solution Components hosted by the Customer.

Transit/Port/Protocol	AudioCodes DC -> SBC	SBC-> AudioCodes DC
TLS 5001 (Secure QoE)		X
TCP 22 (SSH)	X	
UDP 161 (SNMPv3)	X	
UDP 162 (SNMPv3)		X
TCP 443 (HTTPS)	X	
NTP 123 (UDP)		X
TCP 636 (LDAPs)		X

Transit/Port/Protocol	AudioCodes DC -> UMP	UMP-> AudioCodes
TCP 80 (http)	X	X
TCP 3389 (RDP)	X	
UDP 161 (SNMPv2)	X	
UDP 162 (SNMPv2)		X
UDP 1161 (KeepAlive)		X
TCP 443 (HTTPS)	X	
UMP require "basic" direct internet access without a proxy server.		

Transit/Port/Protocol	AudioCodes DC -> Service Server	Service server-> AudioCodes DC
TCP 3389 (RDP)	X	
TCP 636 (LDAPs) - Optional		X

The following tables represent firewall requirements for defining access to the public internet.

Transit/Port/Protocol	Metering Server (Cloud)-> SBC	SBC-> Metering Server (Cloud)
TCP 443 (HTTPS)		X

When utilize Audiocodes' Central Syslog service, the following port need to be open for outbound traffic to the public internet.

Transit/Port/Protocol	Live Platform -> Service Components	Service Components -> Live Platform
TCP 9093 (SSL Kafka)		X

When WebSocket connectivity is used, the following table outlines the connectivity matrix with the protocols, ports and directions that must be implemented between AudioCodes' datacenter and Customer premises.

The WebSocket connectivity encapsulate all the management protocols (SNMP, HTTPS, NTP, QoE, etc.) inside the WebSocket tunnel

The following Public IPs needs to be allowed to initiate TCP/Https outbound traffic - Allow listing Imperva IP addresses & Setting IP restriction rules.

Transit/Port/Protocol	Live Platform -> Service Components	Service Components -> Live Platform
TCP 443 (HTTPS – WS Tunnel)		X

7.3 Backup and Restore

The following table describes the data backed process.

The restoration of managed devices should be according to the best practice of each service component.

Entity	Recommended Frequency and Method	For how long	Where
SBC	Backup Done by the Live Platform	5 last files	The OVOC configured to automatically (daily) backup Managed Devices configurations (ini, conf or cli script files). The backup files are managed by the Backup Manager that save the 5 latest (five) backup files to be stored for each Managed Device.
UMP	Daily	14 days	UMP backup is under Customer's responsibility to backup and restore.
Service Server	Daily	5 Days	Service Server backup is under Customer's responsibility to backup and restore.

About AudioCodes

AudioCodes is a global company with an enduring commitment to the foundation of all human communications - voice.
We design, manufacture and sell advanced Voice over IP and converged VoIP and data networking products, applications and professional services to global enterprises, medium and small business, as well as to service providers globally.
Our extensive product range includes IP phones, session border controllers (SBCs), media gateways, mobile VoIP clients, multi-service business routers (MSBRs), routing applications, call recording, voice dialing, and more.

International Headquarters
Naimi Park
6 Ofra Haza Street
Or Yehuda, 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