Voca Conversational Interaction Center

AudioCodes Cloud Security and Architecture Overview

Table of Contents

Background

This document describes the security and connectivity requirements, alongside an infrastructure overview, of AudioCodes Voca Conversational Interaction Center (CIC) solution.

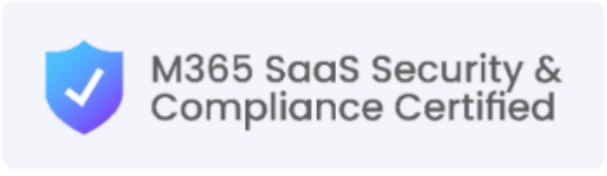
Voca CIC is a SaaS Application Security and Compliance certified solution, tested by Microsoft against SaaS controls derived from leading industry standard frameworks, meeting strong security and compliance practices in place to protect customer data.

Microsoft M365 Application certification is centered around a thorough security audit of the application and its supporting infrastructure. The application is vetted against a series of security controls derived from leading industry standard frameworks such as SOC 2, PCI DSS, and ISO 27001.

Application certification is attained through a qualified analyst's review and approval of a comprehensive assessment centering on an application's security and compliance frameworks, processes, procedures, and annual penetration testing.

For more detailed information on Voca CIC data handling, security, and privacy, please visit:

- Contact center integrations for Microsoft Teams
- SaaS Apps Security and Compliance - All Apps - Microsoft 365 App Certification | Microsoft Learn
- GDPR compliance



FIPS Certification

AudioCodes Voca CIC features a certification for compliance with the Federal Information Processing Standards (FIPS), a set of rigorous security standards established by the U.S. government to ensure robust encryption and data protection. This certification reflects AudioCodes' commitment to delivering secure and reliable solutions that meet the stringent requirements for protecting sensitive information.

With FIPS compliance, Voca CIC is optimized for use in regulated enterprise industries such as government, healthcare, and financial services, where the highest standards of data security are essential.

This certification reinforces AudioCodes' dedication to maintaining the highest levels of enterprise security and compliance standards across its solutions.

AudioCodes Certifications

ISO 9001 Certificate
(LTD)

ISO 9001 Certificate
(INC)

ISO 45001 Certificate
(LTD)

ISO 14001 Certificate
(LTD)

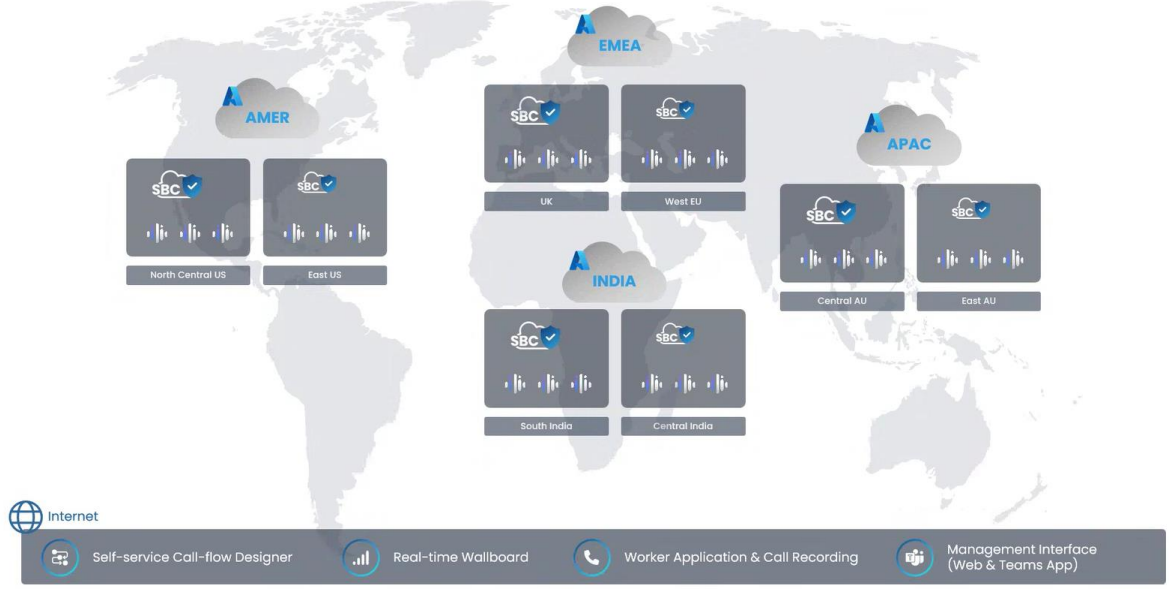
Global Cloud Presence and Availability

Voca CIC is a Contact Center as a Service (CCaaS) solution that is deployed worldwide over multiple regions to serve all AudioCodes multinational customers.

Each cloud is deployed with two key motivations:

- **Geo-redundancy:** With a geo-redundant platform, customers can be sure that even if the entire Azure region is down, call and management access are still available from the backup region, with "zero" downtime.
- **High availability (HA):** Another layer of redundancy is HA, whereby each Voca CIC cloud is deployed with multiple servers to ensure maximum service availability.

Figure 1: Voca CIC - AudioCodes Cloud Microsoft Azure Geo-Redundancy



Azure Region Availability

- **US Cloud:**
  - East US
  - North Central US
- **EMEA Cloud:**
  - UK
  - West EU

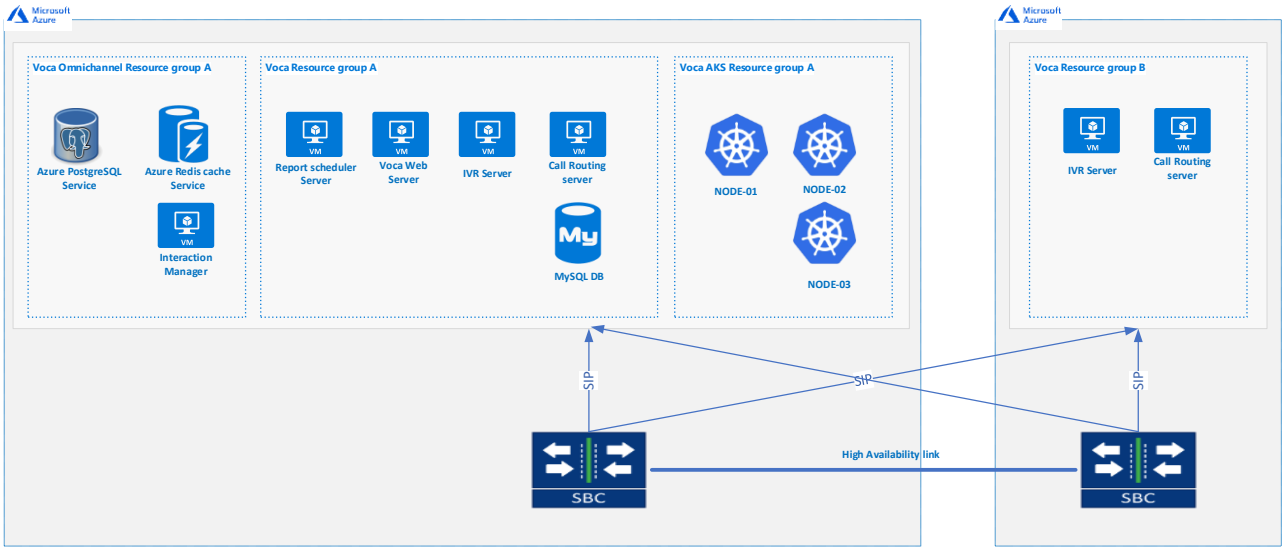
- **APAC Cloud:**
  - East AU
  - Central AU
- **India Cloud:**
  - Central India
  - South India

High-Level Cloud Architecture (e.g., US Cloud)

Each cloud region datacenter contains multiple SBC products that are responsible for inbound and outbound voice communication with the customer's Session Border Controller (SBC)/PSTN providers and the customer's third-party PBX, allowing communication with the contact center platforms.

On the application layer, each Voca CIC region datacenter is built with multiple IVR servers that are responsible for caller interaction and communication. In addition, HA architecture includes two database servers to support the replication of information access in case of failover.

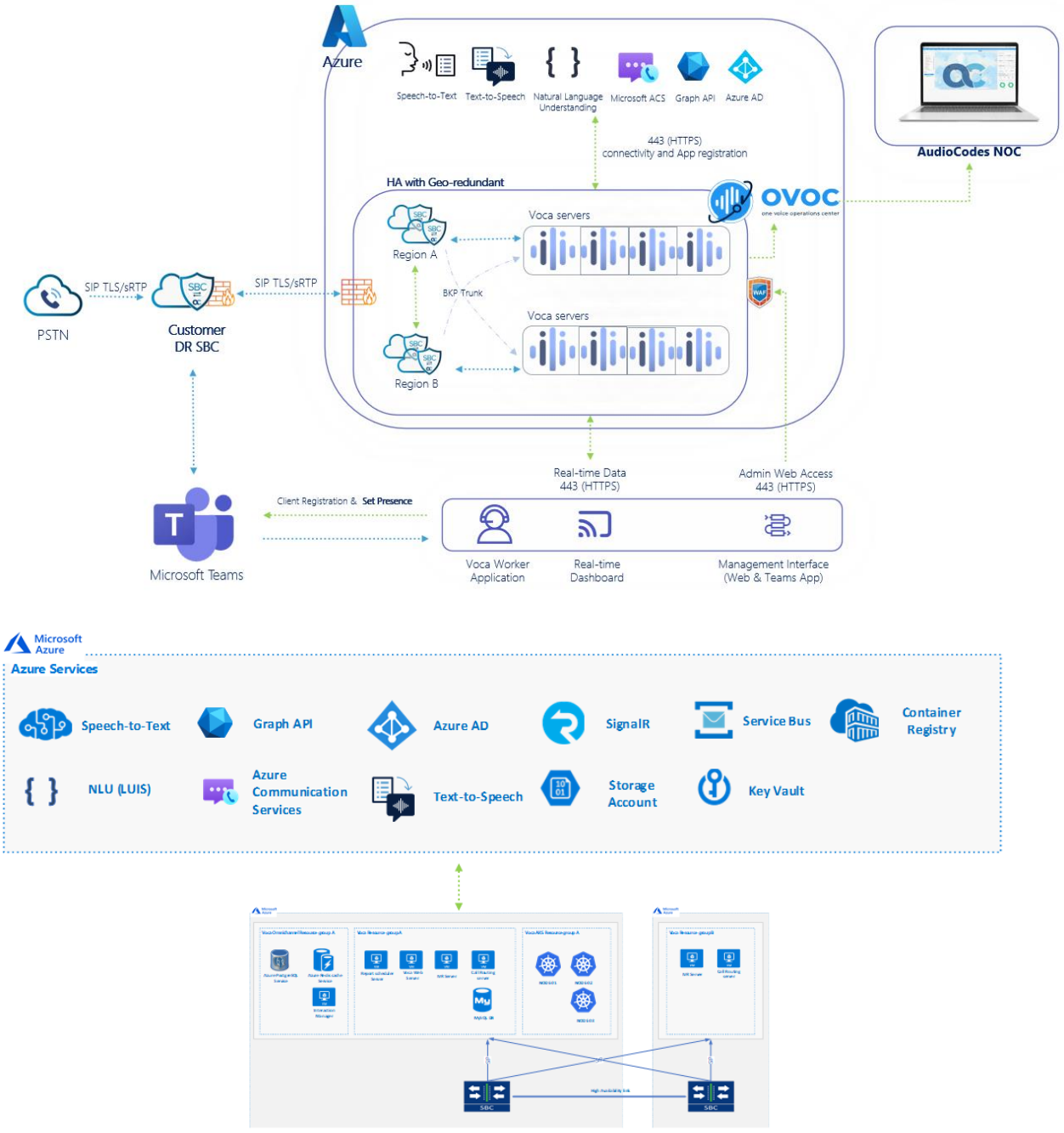
Figure 2: Voca CIC – Azure Region-specific High-Availability View



Solution Security and Topology Overview

The Voca CIC High Level Design and Security is illustrated and described below.

Figure 3: Voca CIC – High level Design and Security Overview



The Voca CIC solution is an Azure-native Contact Center as a Service that can be deployed either on the customer's Azure cloud, or on AudioCodes Azure (delivered as a service).

To integrate Voca CIC with the PSTN/IP PBX/UC layer, AudioCodes offers an SBC as a built-in element to support voice firewall capabilities, such as strict access between source and destination IP addresses, and encryption and security of the SIP trunk between Voca CIC and the customer's internal PBX/external PSTN provider over SRTP and TLS.

AudioCodes allows customers to implement a TLS trunk between the Customer's Direct Routing SBC (DR-SBC) and the Voca CIC Cloud SBC, using the Customer's self-signed certificate to encrypt traffic.

In addition, customers whose organization has strict security policies can also setup SIP connectivity using account registration with username and password for SIP authentication.

Voca CIC cloud includes a cloud firewall application to ensure only defined customer's SIP trunks are allowed to communicate with Voca CIC Cloud SBCs.

Voca CIC also interfaces with Microsoft services using APIs over HTTPS (8443) for the following capabilities:

- **Speech-to-Text (STT)**: Enables voice recognition capabilities and converts caller requests from voice-to-text as part of a Voca CIC conversational IVR flow.
- **Natural Language Understanding (NLU)**: Supports open natural language inputs of caller requests, allowing Voca CIC to extract call flow entities based as part of a Voca CIC conversational IVR flow.
- **Text-to-Speech (TTS)**: Enables reading out dynamic data or any other data that wasn't pre-recorded as part of a Voca CIC conversational IVR flow.
- **Azure Communication Services (ACS):** Used for skill-based routing and an Agent Desktop interface with tight integration with Microsoft Teams.
- **Graph API:** Supports presence-based routing to Microsoft Teams users acting as agents in a Voca CIC call queue.
- **Azure AD:** Effectively builds Auto-Attendant routing entities and destinations using the company's address book (contacts and departments).

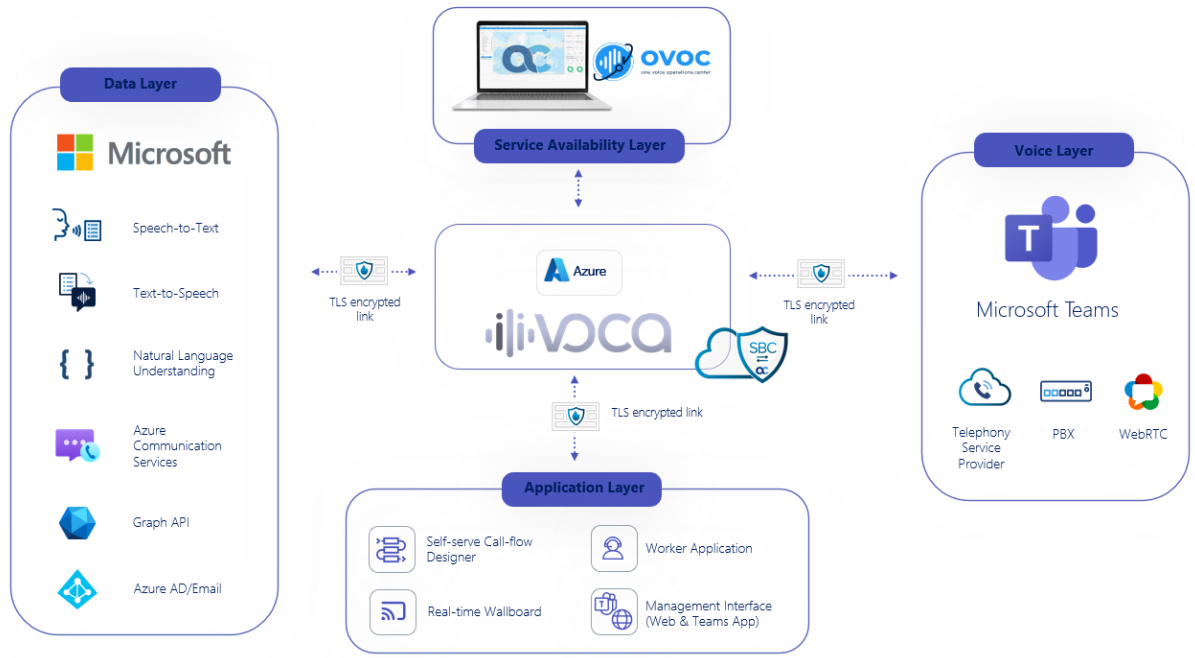
- Voca CIC doesn't correlate caller requests with a specific call or caller; any information exchanged between Voca CIC and Microsoft doesn't contain any information disclosing a specific call, or a specific caller's identity.
- Any information used in the Voca CIC call flow is never stored on the Voca CIC database and is only used in real-time during an active call flow interaction.
- Please read the Voca CIC GDPR and HIPAA-Ready Notice.

Voca CIC also provides web-based interfaces for the Solution administrator, as well as for agents and supervisors:

- **Voca CIC Web Management Interface:** Using this web management interface (over HTTPS and also protected by WAF application to avoid unwanted access to the customer Tenant via the Web portal), the admin can setup and configure Voca CIC tenants, call flows, and view/generate reports.
- **Self-Service Call Flow Designer:** Part of the Voca CIC management user interface, Call Flow Designer operates in low-code/no-code. It can be used to build advanced call flows with access to external API-facing sources.
- **Agent Desktop/Worker Application:** Voca CIC's Worker application provides a centralized interface for supervisors and agents to make and receive calls while receiving any call-related information (e.g., IVR or CRM) during their calls. It also provides basic call controls, availability controls, and wrap-up events. Supervisors enjoy additional real-time queuing data and control over the availability of agents and associated queues.

- **Real-Time Dashboard:** Displays real-time data of call queue activity and caller behavior while queuing.

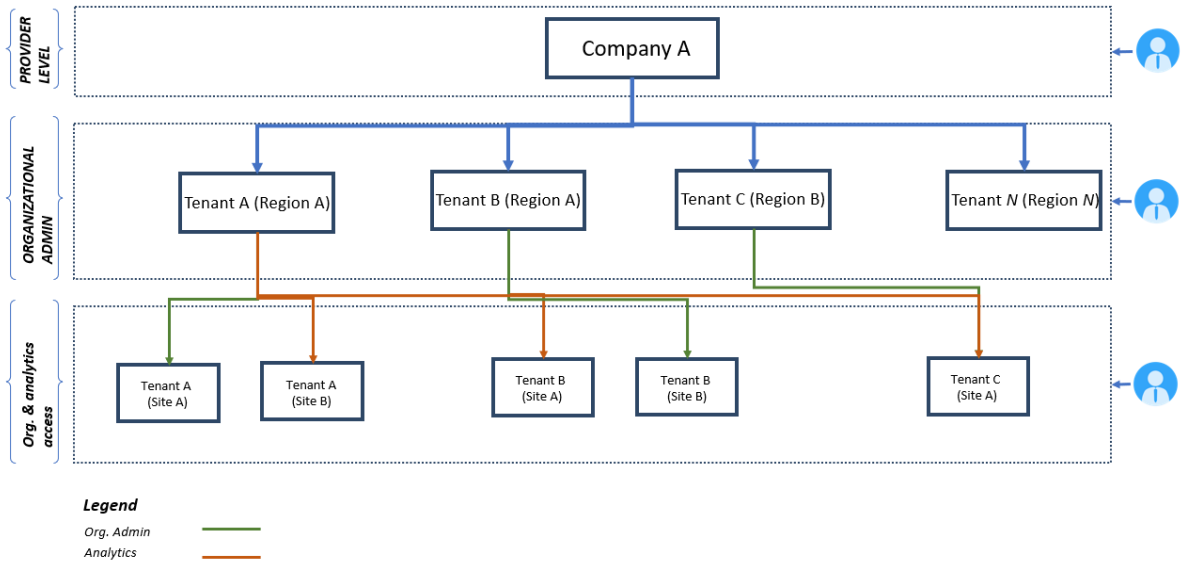
Figure 4: Voca CIC – Architecture Overview



Multi-tenancy

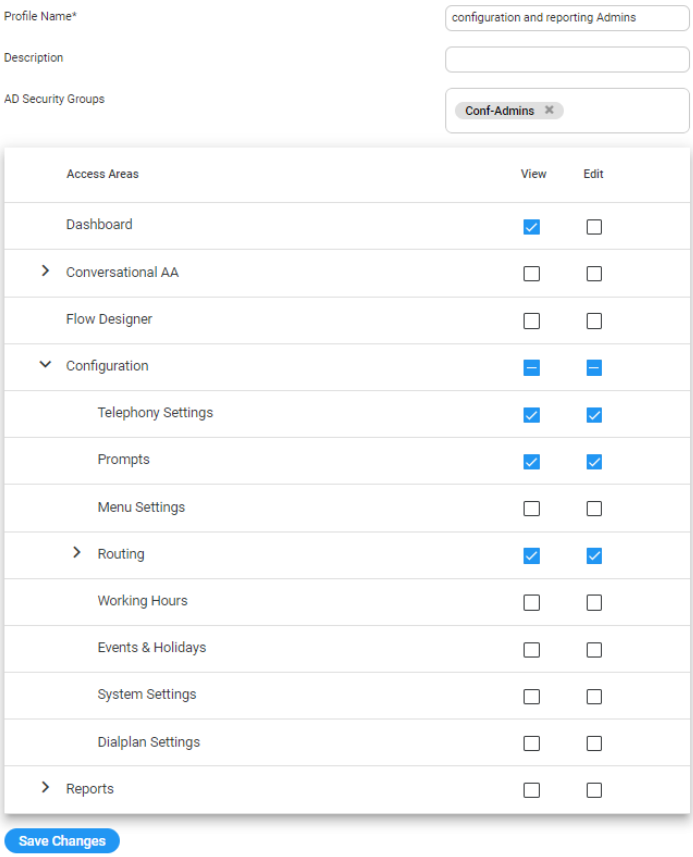
Voca provides a Web-based management interface with multi-tenant support and role-based access (RBAC), allowing Service Providers to build, create, and manage customer tenants/sites under their infrastructure environment.

Figure 5: Voca CIC - Multi-tenancy Hierarchy



In addition, Voca also offers an additional layer to create relevant access to users with permission to access Voca to manage Voca tenants or multiple contact center using Role-based access control and create dedicated access profiles.

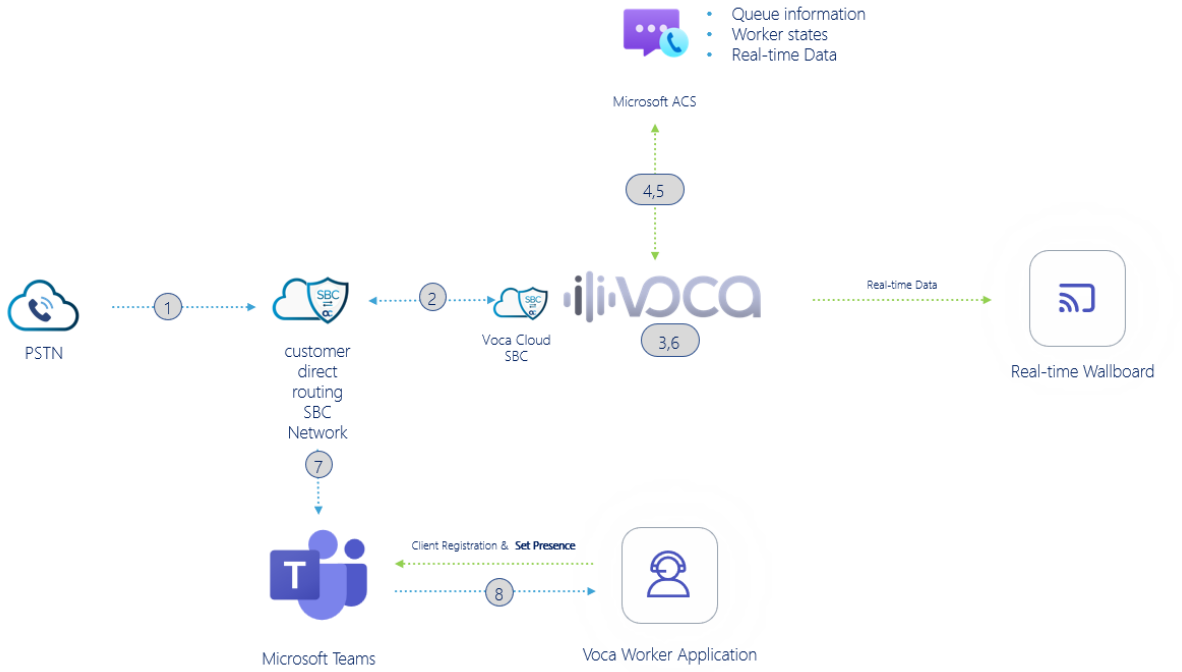
Figure 6: Voca CIC - Creating Custom User Access Profiles



High-Level Call Flow Diagram

The figure below illustrates the High-Level Call Flow.

Figure 7: Voca CIC – High-Level of Call Flow



The flow is as follows:

1. The call is routed from the customers' PSTN provider to the customers' Direct Routing SBC (DR SBC).
2. The customers' DR SBC routes all Contact Center calls to the customer's Voca CIC Cloud tenant.
3. Voca CIC manages the IVR/Business logic and customer interaction.
4. Voca CIC initiates backend interaction with Microsoft Azure Communication Services (ACS) to retrieve information on relevant available agents.
5. Voca CIC receives Agent/Queue information from the Job Router.
6. Voca CIC sends information to the Voca CIC real-time dashboard application.
7. Voca CIC connects the call to the customers' Teams tenant via the customer's DR SBC.

8. Microsoft Teams receives the call and then calls the relevant Voca CIC Worker/Teams user (logged-in registered device such as Teams app/Voca CIC Worker Application based on ACS SDK).
9. Once the Agent answers the Voca CC call, Voca CIC updates the Teams user/identity with the relevant presence status.

- Item #8 represents the connectivity to ACS through the Voca CIC Worker Application, as mentioned in Section 'Consent for Voca CIC Worker Application/Agent Desktop'.
- Item #8 represents the connectivity between the Voca CIC Worker Application and the customers' Teams users' presence status, as mentioned in Section 'Voca CIC Presence-based Routing and Azure AD Synchronization', using "Set Presence" as follows:

Worker Application State	Teams Identity State
Ready	Available
Not Ready	Busy
Talking	In a Call

Proactive and Real-Time Monitoring for Cloud-Based Contact Center

A cutting-edge proactive and real-time monitoring service for Cloud-based contact centers has been designed to make sure AudioCodes' customers have service availability to support their critical business contact center applications and end-customers.

This monitoring layer employs a comprehensive array of monitoring tools that continuously track and analyze various facets of contact center operations, such as call volume, service connectivity and system health, allowing AudioCodes to promptly identify and address potential issues before they escalate.

The proactive nature of the monitoring service ensures swift intervention, minimizing downtime and optimizing customer service delivery.

Customers are part of the managed service solution when it comes to Voca CIC as a cloud solution, with 24x7 NOC and support teams worldwide.

Solution Security and Network Requirements

Customers wishing to use Voca CIC delivered from AudioCodes Cloud should meet the following requirements:

- Customers must have an Active Direct Routing environment that includes the following:
  - Direct Routing SBC (DR SBC) connected to Microsoft Teams tenant.
  - Microsoft Teams users with phone numbers.
- If Media Bypass is enabled on the organization level (i.e., Microsoft Teams tenant and SBC), the organization's administrator must open the following ports and protocols in the organization's firewall:
  - From Microsoft ACS (20.202.0.0/16) to the customer SBC network UDP ports 3478-3481.
  - From Microsoft ACS (20.202.0.0/16) to the customer SBC network UDP ports 6000-10000 (SBC media ports).
  - From Microsoft ACS (20.202.0.0/16) to the customer SBC network UDP ports 9580-9585.
  - From Microsoft ACS (20.202.0.0/16) to the customer SBC network TCP port 443.

Using Voca CIC as a Service using AudioCodes Cloud

For customers who wish to implement Voca CIC as a Service using AudioCodes Cloud, the organization's administrator should allow the following:

- HTTPS connectivity (port 8443) between the agent desktop clients' network and the Voca CIC Cloud *.audiocodesaas.com.

Communication Protocols

Table 1: Voca CIC - Communication Protocols

Destination	Protocol
Microsoft Services	HTTPS
AudioCodes OVOC	WebSocket
Voca CIC Web User Interface	HTTPS
PSTN/Customer SBC	sRTP/TLS

Consent for Voca CIC Web Admin Management Interface

To access the Voca CIC Web Admin Management Interface, users must grant consent for the necessary Microsoft permissions to enable Single Sign-On (SSO) authentication. This ensures a secure and seamless login experience by allowing the system to verify user identities through their Microsoft credentials. By providing consent, users authorize Voca CIC to access basic profile information and necessary directory data in accordance with Microsoft's security and compliance standards.

Your consent will allow AudioCodes the following access:

Table 2: Consent for Voca CIC Web Admin Management Interface

Azure Scope	Permission	Explanation
Microsoft Graph	View users' basic profile	The "**View users' basic profile**" permission is necessary for Voca CIC's functionality, as it allows the system to retrieve the Object ID of users. This Object ID is essential for facilitating internal calls between workers within Microsoft systems.
Microsoft Graph	Sign users in	The "**Sign in user**" permission is necessary because Voca CIC utilizes Microsoft Entra-based single sign-on (SSO) for both administrative and contact center agent logins. To enable this functionality, the application requires sign-in permission to authenticate users and obtain a token that contains information about the authenticated user.
Microsoft Graph	View users' email addresses	The **"View users' email addresses"** Microsoft Graph permission allows an application to access and read the primary email addresses of users in an organization.

Azure Scope	Permission	Explanation
Microsoft Graph	Maintain access to data you have given it access to	The "**Maintain access to data you have given it access to**" permission is necessary because it allows Voca to refresh access tokens as they expire, ensuring uninterrupted access without requiring users to re-authenticate repeatedly.
Microsoft Graph	Sign in and read user profile	The "**Sign in and Read user profile**" permission is necessary because Voca CIC utilizes Microsoft Entra ID-based single sign-on (SSO) for both administrative and contact center agent logins using the Graph API. To enable this functionality, the application requires sign-in and read permissions for the respective users, ensuring secure authentication and access to user-specific data for a seamless login experience.

Consent for Voca CIC Worker Application/Agent Desktop

Voca CIC was designed for seamless integration with Microsoft Teams (also known as the 'Power Model' by Microsoft for a Microsoft-based Contact Center), providing Conversational IVR and Contact Center capabilities to Microsoft Teams Phone.

As part of the application registration and to ensure smooth operation and full functionality, Voca CIC requires consent to access the applicable Azure environment(s). Your consent will allow AudioCodes the following access:

- Read and write user chat messages
- Sign-in and read user profile
- Read all users' full profiles
- Create chats
- Manage calls in Teams

The organization's administrator (Microsoft 365) should grant tenant-wide admin consent to the agent application on behalf of the organization. Use the link below to grant consent, but replace *<Tenant_ID>* with the organization's Azure Tenant ID:

https://login.microsoftonline.com/<Tenant_ID>/adminconsent?client_id=8406a66b-1227-4e07-89f6-bf5ba4210425&redirect_uri=https://vocaus-workerapp.audiocodesaas.com/

Table 3: Consent for Voca CIC Worker Application/Agent Desktop

Azure Scope	Permission	Explanation
Azure Communication Services	Manage calls in Teams	The "**Manage calls in Teams**" permission is necessary because Voca workers operate as Teams users in the backend. To enable seamless integration and functionality with the Azure Communication Services (ACS) SDK, this permission allows managing calls through ACS.
Azure Communication Services	Manage chats in Teams	The "**Manage chats in Teams**" permission is necessary because Voca workers operate as Teams users in the backend. This permission, along with "**Manage calls in Teams**" is required by the Azure Communication Services (ACS) SDK to enable seamless integration and functionality for managing real-time communications.
Microsoft Graph	View users' basic profile	The "**View users' basic profile**" permission is necessary for Voca CIC's functionality, as it allows the system to retrieve the Object ID of users. This Object ID is essential for facilitating internal calls between workers within Microsoft systems.
Microsoft Graph	Read and write user chat messages	The "**Read and write user chat messages**" permission is necessary because Voca agents function as regular Teams users in the backend. Voca CIC uses the Microsoft Azure Communication Services (ACS) SDK to manage agents' real-time communications, and the ACS SDK requires these permissions

Azure Scope	Permission	Explanation
		to effectively facilitate and control chat-related interactions.
Microsoft Graph	Maintain access to data you have given it access to	The "**Maintain access to data you have given it access to**" permission is necessary because it allows Voca to refresh access tokens as they expire, ensuring uninterrupted access without requiring users to re-authenticate repeatedly.
Microsoft Graph	Sign in and Read user profile	The "**Sign in and Read user profile**" permission is necessary because Voca CIC utilizes Microsoft Entra ID-based single sign-on (SSO) for both administrative and contact center agent logins using the Graph API. To enable this functionality, the application requires sign-in and read permissions for the respective users, ensuring secure authentication and access to user-specific data for a seamless login experience.
Microsoft Graph	Sign users in	The "**Sign in user**" permission is necessary because Voca CIC utilizes Microsoft Entra-based single sign-on (SSO) for both administrative and contact center agent logins. To enable this functionality, the application requires sign-in permission to authenticate users and obtain a token that contains information about the authenticated user.
Microsoft Graph	Create Chat	The "**Create chat**" permission is necessary because Voca workers operate as Teams users in the backend. This permission, along with "**Manage chats in Teams**" is required by the Azure Communication Services (ACS) SDK to enable seamless integration and functionality for managing real-time communications.

Voca CIC Presence-Based Routing and Microsoft Entra ID Synchronization

To provide intelligent routing to Microsoft Teams users configured as queue members in Voca CIC call queues, Voca CIC provides routing that is based on presence information of Teams users.

To enable this functionality, Voca CIC requires admin consent (Application registration) from the Customer with the following permissions via the Voca CIC management interface:

Figure 8: Voca CIC – Admin Consent for Routing Based on Teams User Presence

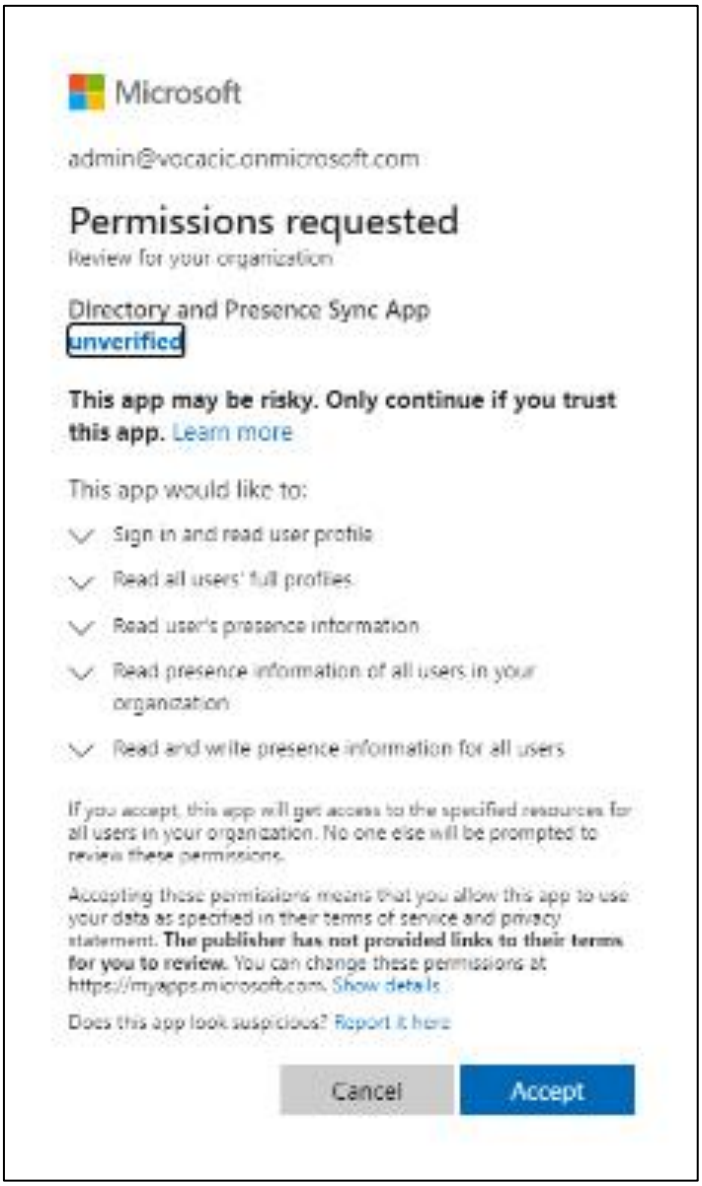


Table 4: Voca CIC - Presence-Based Routing and Microsoft Entra ID Synchronization

Azure Scope	Permission	Explanation
Microsoft Graph	Sign in and read user profile	The "**Sign in and Read user profile**" permission is necessary because Voca CIC utilizes Microsoft Entra ID-based authentication for importing contacts and for retrieving or updating their Azure presence information using the Microsoft Graph API. To enable this functionality, the application requires sign-in and read permissions for the respective users, ensuring access to their profile data and presence information.
Microsoft Graph	Read all users' full profiles	The "**Read all users' full profiles**" permission is necessary because Voca CIC utilizes Microsoft Entra ID-based authentication for importing contacts using the Microsoft Graph API. To enable this functionality, the application requires permission to read all user profiles, allowing it to import the complete information of the contacts into Voca CIC.
Microsoft Graph	Read presence information of all users in your organization	The "**Read presence information of all users in your organization**" permission is necessary because Voca CIC routes calls based on the presence information of contacts imported into the system. This ensures that calls are directed to the appropriate contacts based on their availability. The permission can be revoked manually if routing based on Teams Presence is no longer required.
Microsoft Graph	Read and write presence information for all users	The "**Read and write presence information for all users**" permission is necessary for Voca agents to read and update their presence status when they

Azure Scope	Permission	Explanation
		answer calls in the Worker App. This permission ensures that the presence status is accurately reflected, enabling efficient call management. It can be revoked manually if it is no longer required in the Voca Worker Application.

Voca CIC Email Access (AudioCodes Hosted App)

Table 5: Voca CIC – Email Access (AudioCodes Hosted App)

Azure Scope	Permission	Explanation
Microsoft Graph	Send mail as any user	The "**Send mail as any user**" permission is essential for Voca CIC's functionality, as it enables the system to send emails to customers based on predefined actions within the platform. This permission is restricted to the specific user configured in the system settings, ensuring that all emails are sent exclusively from this user's account, without requiring individual authentication for each action.

Voca CIC Email Access (Self-Hosted App - Application)

Table 6: Voca CIC – Email Access (Self-Hosted App - Application)

Azure Scope	Permission	Explanation
Microsoft Graph	Send mail as a user	The "**Send mail as any user**" permission is essential for Voca CIC's functionality, as it enables the system to send emails to customers based on predefined actions within the platform. This permission is restricted to the specific user configured in the system settings, ensuring that all emails are sent exclusively from this user's account, without requiring individual authentication for each action.

Voca CIC Email Access (Self-Hosted App - Delegated)

Table 7: Voca CIC – Email Access (Self-Hosted App - Delegated)

Azure Scope	Permission	Explanation
Microsoft Graph	Send mail as a user	The "**Send mail as a user**" permission is essential for Voca CIC's functionality, as it enables the system to send emails to customers based on predefined actions within the platform. This permission is limited to a specific user, who must be configured in the system settings using their username and password. Additionally, this user must manually assign the application in Azure to ensure that Voca CIC can only use this designated account for sending emails.

Azure Scope	Permission	Explanation
Microsoft Graph	Sign in and read user profile	The "**Sign in and read user profile**" permission is necessary because Voca CIC relies on Microsoft Entra ID-based authentication to access the Microsoft Graph API. This permission enables the application to authenticate users and retrieve basic profile information required for providing a personalized experience and ensuring secure access.

Voca Omnichannel Email (AudioCodes Hosted App)

Table 8: Voca CIC – Omnichannel Email (AudioCodes Hosted App)

Azure Scope	Permission	Explanation
Microsoft Graph	IMAP.AccessAsApp	The "**IMAP.AccessAsApp**" permission is necessary because Voca CIC uses the IMAP protocol to read emails from inboxes configured within the Voca Interaction Center Emails. This permission enables the application to securely access and process emails to support interaction workflows.
Microsoft Graph	SMTP.SendAsApp	The "**SMTP.SendAsApp**" permission is necessary because Voca CIC uses the SMTP protocol to send emails from inboxes configured within the Voca Interaction Center Emails. This permission enables the application to securely send emails on behalf of configured inboxes, supporting interaction workflows efficiently.

Voca Omnichannel Email (Self-Hosted App - Application)

Table 9: Voca CIC – Omnichannel Email (Self-Hosted App - Application)

Azure Scope	Permission	Explanation
Microsoft Graph	IMAP.AccessAsApp	The "**IMAP.AccessAsApp**" permission is necessary because Voca CIC uses the IMAP protocol to read emails from inboxes configured within the Voca Interaction Center Emails. This permission enables the application to securely access and process emails to support interaction workflows.
Microsoft Graph	SMTP.SendAsApp	The "**SMTP.SendAsApp**" permission is necessary because Voca CIC uses the SMTP protocol to send emails from inboxes configured within the Voca Interaction Center Emails. This permission enables the application to securely send emails on behalf of configured inboxes, supporting interaction workflows efficiently.

Voca Omnichannel Email (Self-Hosted App - Delegated)

Table 10: Voca CIC – Omnichannel Email (Self-Hosted App - Delegated)

Azure Scope	Permission	Explanation
Microsoft Graph	IMAP.AccessAsApp	The "**IMAP.AccessAsApp**" permission is necessary because Voca CIC uses the IMAP protocol to read emails from inboxes configured within the Voca Interaction Center Emails. This permission enables the application to securely access and process emails to support interaction workflows.
Microsoft Graph	SMTP.SendAsApp	The "**SMTP.SendAsApp**" permission is necessary because Voca CIC uses the SMTP protocol to send emails from inboxes configured within the Voca Interaction Center Emails. This permission enables the application to securely send emails on behalf of configured inboxes, supporting interaction workflows efficiently.

Cloud SaaS App Security Data Flow and Measurement

Secure Web Applications with Imperva WAF

AudioCodes has chosen Imperva WAF as its cloud-based web application firewall solution for several reasons:

- Imperva WAF provides a comprehensive and adaptive security solution that protects web applications from a wide range of attacks, including OWASP Top 10, zero-day, and advanced persistent threats.
- Imperva WAF leverages machine learning and crowdsourced threat intelligence to automatically detect and block malicious traffic, bots, and fraudsters, while allowing legitimate users to access the web applications.
- Imperva WAF offers granular and flexible policies and rules that can be customized to suit the specific needs and preferences of AudioCodes. Imperva WAF also provides real-time alerts and reports that enable AudioCodes to monitor and analyze the security status and performance of its web applications.
- Imperva WAF is a cloud-based solution that can be easily deployed and integrated with AudioCodes' existing infrastructure and platforms, such as AWS and Azure. Imperva WAF also offers a global network of data centers that ensure high availability, reliability, and scalability of the web application security.

Microsoft Azure Defender for Cloud

Azure Defender for Cloud is a comprehensive security solution that provides threat protection and security posture management for Azure resources and hybrid workloads. AudioCodes uses Azure Defender for Cloud to monitor and protect its cloud-based SaaS applications from various threats, such as malware, ransomware, denial of service, and brute force attacks.

Azure Defender for Cloud enables AudioCodes to:

- Gain visibility into the security state of its cloud resources and identify any misconfigurations or vulnerabilities that could expose them to risks.
- Receive alerts and recommendations for remediation actions based on the severity and impact of the detected threats.

- Automate the response and mitigation of threats using Azure logic apps and Azure functions.
- Integrate with Azure sentinel, a cloud native security information and event management (SIEM) solution, to analyze and correlate security data from multiple sources and generate actionable insights.

Microsoft Azure Firewall

Azure Firewall is a cloud native network security service that provides centralized and scalable firewall capabilities for Azure virtual networks. AudioCodes uses Azure Firewall to control and filter the network traffic to and from its cloud-based SaaS applications, and enforce granular policies based on application, protocol, source, and destination.

Azure firewall enables AudioCodes to:

- Protect its cloud-based SaaS applications from unauthorized access and network attacks, such as port scanning, spoofing, and packet fragmentation.
- Enable secure connectivity between its cloud-based SaaS applications and its on-premises network, using Azure VPN Gateway and Azure ExpressRoute.
- Optimize the performance and availability of its cloud-based SaaS applications, using Azure Load Balancer and Azure Traffic Manager.
- Monitor and audit the network activity and firewall logs, using Azure Monitor and Azure Storage.

External Vulnerability Assessments and External Penetration Tests

- **External vulnerability assessments** involve scanning the external network perimeter to identify and evaluate potential security risks.
- **External penetration tests** simulate real-world attacks to assess the exploitability of identified vulnerabilities in the external network perimeter.
- Both assessments are conducted by **certified security professionals** from a **Microsoft-approved penetration testing provider**, using industry-standard tools and methodologies.
- To maintain ongoing security and compliance, these tests are performed quarterly, ensuring that vulnerabilities are promptly identified and addressed.

Third-Party SIEM SOC to Monitor Security Risks

To protect its network and data from cyberattacks, AudioCodes relies on a third-party SIEM SOC (Security Information and Event Management Security Operations Center) service. A SIEM SOC is a centralized platform that collects, analyzes, and correlates security events from various sources, such as firewalls, routers, servers, and applications. A SIEM SOC also provides real-time alerts, incident response, and threat intelligence to help mitigate and prevent security breaches.

This section describes how AudioCodes uses the third-party SIEM SOC service to monitor its security risks, and the benefits and challenges involved in this implementation.

How AudioCodes Uses the Third-Party SIEM SOC Service

AudioCodes has outsourced its SIEM SOC service to a reputable and experienced provider with a team of certified security analysts and engineers. The provider is responsible for deploying, configuring, and maintaining the SIEM SOC platform, as well as providing 24/7 monitoring and support. The provider also delivers regular reports and recommendations to AudioCodes on its security posture and performance.

The SIEM SOC platform collects and analyzes security events from AudioCodes' network devices, servers, and applications, using various data sources, such as logs, flows, packets, and endpoints. The platform uses advanced algorithms and machine learning to detect and prioritize anomalies, patterns, and trends that indicate potential threats or incidents. The platform also integrates with external threat intelligence feeds, such as IP reputation, malware, and phishing databases, to enrich and validate the security events.

When the SIEM SOC platform detects a security event that requires attention, it generates an alert and notifies the provider's security analysts, who then investigate and validate the alert. If the alert is confirmed as a genuine threat or incident, the security analysts escalate it to the provider's security engineers, who then take the appropriate actions to contain and remediate the threat or incident. The security engineers also communicate and coordinate with AudioCodes' IT staff, who are responsible for implementing the recommended actions on their end.

The provider's security analysts and engineers follow a predefined workflow and escalation process, based on the severity and impact of the threat or incident. The provider also maintains a detailed record of all the security events, alerts, and actions, and provides AudioCodes with a dashboard and a report revealing the status and metrics of its security risks and incidents.

General Access Management

The following describes the user life cycle, concerning exclusive access to on-premise systems (and their data) by authorized AudioCodes Service Engineers (only), who may be located worldwide.

- When a new employee starts working at AudioCodes Corporate, the employee's details are entered into AudioCodes Oracle HR system. An API creates a user in the corporate's Active Directory without any privileges or Groups.
- Only members of AudioCodes Corp Active Directory Services* Distribution Groups can gain access to AudioCodes.cloud Active Directory groups.

  Owners (Regional Managers) of the following AudioCodes Distribution Groups should add the desired person as a member:

  - ServicesEMEA – for EMEA region
  - ServicesAmericas – for America region
  - ServicesAPAC – for APAC region

  The API compares all active AudioCodes.cloud users with AudioCodes Corp Active Directory Services* Distribution lists members. When a new user is detected in AudioCodes Distribution Group, the API creates a new user in AudioCodes.cloud Active Directory.
- Termination – in case a termination date is set in Oracle by HR, the API disables the user in the corporate Active Directory.
- The API reads from AudioCodes Corporate Active Directory Services Distribution Groups the list of membered users in relevant groups and compares them with all users in AudioCodes.cloud Active Directory.

  For each user found in AudioCodes.cloud Active Directory, it checks if the user exists in AudioCodes Corporate Active Directory Services* Distribution lists of membered users. If the user doesn't exist, the user is disabled on AudioCodes.cloud Active Directory.
- The API finds all disabled users and deletes all users that have been disabled for more than 60 days.

- In case of immediate termination of high-level privilege users, the corporate IT can disable the user immediately, even before the last day of employment. This disables the user on AudioCodes.cloud Active Directory.
- Employment Role change: If users move to another role outside the AudioCodes Services Organization, Regional Managers will remove the user from AudioCodes Corporate Active Directory Services* Distribution Group, which will disable the user on AudioCodes.cloud Active Directory.
- Access to AudioCodes' datacenter using Client-to-Server IPSec VPN tunnel with One Time Password (OTP) and AudioCodes' Services Active Directory authentication.
- AudioCodes' Services Active Directory's passwords must be at least 8 characters long for engineers and 12 for administrators, and must contain characters from three of the following: uppercase characters, lowercase characters, digits (0-9), special characters (e.g., !, #, and $), and Unicode characters. In addition, the password must not contain more than two characters from the username. None of the previous 24 passwords can be reused. Users are required to change their password at least once every 90 days.
- After 5 failed login attempts, the user's account will be locked out for 30 minutes.
- Password Manager Pro is a secure vault that is used by AudioCodes Services for storing and managing shared sensitive information such as local user credentials for all systems (e.g. SBC, OVOC, and Service Server).

Managed Services using Central WebSocket Tunnel OVOC Topology

The following describes Managed Services topology, where AudioCodes OVOC is central and is hosted on the AudioCodes' datacenter.

Key Components

- Managed Device: AudioCodes' SBC(s) only from version 7.20A.258-2, Voca CIC SaaS app.
- Central One Voice Operations Center (OVOC): A 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.
- AIM: AudioCodes Intelligent Monitoring Server.
- Oracle Service Cloud: AudioCodes Support Ticketing system using Oracle Service Cloud.

AudioCodes Intelligent Monitoring (AIM) System

The AIM system analyzes the managed devices' alarms and events and determines how they should be acted upon by AudioCodes Managed Services. It's used by AudioCodes to operate the Managed Services intelligently by analyzing the actual performance of the managed device and by issuing run reports.

As part of the Managed Service, the customer needs to share contact information that will be used by the AudioCodes AIM to communicate with the Customer Help Desk concerning the managed device's alarms or concerning issues with 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 through a web GUI HTTPS (TCP port 443) and is accessible 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 is protected by an Administrator username and password.

Oracle Service Cloud

As part of the managed Service, the customer needs to share contact information that will be used by the AudioCodes TAC to communicate with the Customers' Help Desk regarding managed devices' alarms or issues involving the Site-to-Site VPN.

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

- Organization name/addresses
- Contact details (phone number, email)
- Service Request information:
  - Subject for which the SR was created.
  - Serial Number
  - Correspondence between the Customer and the TAC engineer assigned to the Service Request.
  - Attachments provided by the Customer or by the TAC engineer.
- Delete tickets attachments within a 1-year period. Ticket notes will not be deleted.

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

Debug Information

Syslog and CDR Information

The Managed Device sends syslog and CDR messages over TLS port 514 to the Service Server (on the Customers' premises), which are saved in .txt files in "clear text" mode for a period of 45 days (default period). The syslog contains call-related information from the Managed Device. The call data includes the following information, which may be used to identify a person, and which is based on RFC 3261:

- 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 Service Server (see Chapter 'BitLocker').	Full details
Personal Data Pseudonymization	No	No	Full details

Debug Recording Information

The Managed Device can send debug recording packets to the Service Server (on the Customer's 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.

The debug recording can be done for different types of traffic, such as RTP/RTCP, T.38, ISDN, CAS, and SIP. Debug recording 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 solve voice issues; the Customer needs to make sure that that the recoded voice call doesn't 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

OVOC Information

OVOC collects and stores call-related information from the Managed Device.

The call data includes the following information, which may be used to identify a person. The data is saved for a period of 45 days (default period):

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

The Managed Device sends alarms and/or events to OVOC using the SNMPv3 protocol to secure traps that are generated on the Managed Device. The SNMP connection must be configured on both OVOC and the Managed Device.

OVOC uses a database as part of its operation. The database is embedded in OVOC and can't be accessed directly. It's used only by the OVOC application. The OVOC database access is protected by two layers. Only a root user on the OVOC machine can access the OVOC database. A user must be defined as a root user on the OVOC machine, whereupon database access requires a specific database administrator login and password to access the database content.

Transit/Port/Protocol	On Transit	At Rest	View
Personal Data Encryption	Yes	Yes (AES-256 algorithm)	Not relevant
Personal Data Pseudonymization	No	No	Personal masked for Operators level

Data Flows

The following table describes the data flow between the on-premises Managed Device, Central Log server, and AudioCodes' datacenter components:

Source: Managed Device	Destination: Central Log Server	Protocol	Comments
RFC 3261 information, which includes the following (partial list) information: ▪ Managed Device IP Address ▪ Telecom SIP Trunk IP Address ▪ Third-party SIP Server IP Address ▪ Caller name ▪ Caller phone number ▪ Caller URI ▪ Callee name ▪ Callee phone number ▪ Callee URI ▪ Call Detail Record (CDR) information ▪ Voice Coder Information		▪ Syslog: Over WebSocket Tunnel ▪ CDR: Over WebSocket Tunnel	Syslog is sent and saved per call. CDRs are sent and saved on demand only.

Source: Managed Device	Destination: Central Log Server	Protocol	Comments
AudioCodes Debug Recording (proprietary protocol), which includes the following (partial list) information: ▪ Managed Device IP Address ▪ Telecom SIP Trunk IP Address ▪ Third-party SIP Server IP Address ▪ Caller name ▪ Caller phone number ▪ Caller URI ▪ Callee name ▪ Callee phone number ▪ Callee URI ▪ Call Detail Record (CDR) details ▪ Voice Coder Information ▪ RTP Streams		AudioCodes Debug Recording: Over WebSocket Tunnel	The information is sent and saved on demand.

Source: Managed Device	Destination: Central OVOC	Protocol	Comments
XML-based, TLS secured communication for control, media data reports and SIP call flow messages, which includes the following information (partial list): ▪ Managed Device IP Address ▪ Telecom SIP Trunk IP Address ▪ Third-party SIP Server IP Address ▪ Caller name ▪ Caller phone number ▪ Caller URI ▪ Callee name		AudioCodes QoE: Over WebSocket Tunnel	

Source: Managed Device	Destination: Central OVOC	Protocol	Comments
▪ Callee phone number ▪ Callee URI ▪ SIP Call-ID ▪ Call Details Record (CDR) information ▪ 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.)			
Managed Device sends alarms and/or events to OVOC, and the following information may be included: ▪ Managed Device IP Address ▪ Telecom SIP Trunk IP Address ▪ Third-party SIP Server IP Address ▪ Alarm/Event Information		SNMP: Over WebSocket Tunnel	The information is sent and saved per event.
NTP requests from the Managed Device to OVOC for date synchronization		NTP (UDP port 123): Over WebSocket Tunnel	
HTTP connection for SBC/Gateway to backup transfer files to OVOC		HTTP (TCP port 80): Over WebSocket Tunnel	Trigger after SNMP request from OVOC

Source: AIM System, Oracle Service Cloud	Destination: Customer's Helpdesk	Protocol	Comments
Alarms and/or events sent by email to Customer's Help Desk email address. The following information may be included: ▪ Managed Device IP Address ▪ Telecom SIP Trunk IP Address ▪ Third-party SIP Server IP Address ▪ Alarm/Event Information		SMTP (TCP port 25)	The information is sent per event