AudioCodes SBC - Unified Deployment & Configuration Guide

KS

13 February 2026

AudioCodes SBC - Unified Deployment & Configuration Guide
Cloud Operations & Voice Engineering Reference Document
Table of Contents
1. Executive Summary
Key Takeaways
Scope
2. Critical Findings
Stack Manager Requirement for Cross-AZ HA
How the Failover Mechanism Works
HA Scope Clarification
API Access Requirements
3. Architecture Overview
Non-Production Environment (Australia Region Only)
Production Environment
PRODUCTION TOTAL: 9 VMs
4. Component Specifications
Mediant Virtual Edition (VE) SBC
Stack Manager Specifications
AudioCodes Routing Manager (ARM) Specifications
AudioCodes One Voice Operations Center (OVOC) Specifications
Compute Requirements Summary (from Design Document)
5. AWS Infrastructure Requirements
VPC Configuration
Subnet Design
Security Groups
External Publishing Patterns
Cloud East-West Firewall
6. Microsoft Entra ID Integration
Overview
Required App Registrations Summary
App Registration 1: OVOC Teams Integration
App Registration 2: ARM Web UI Authentication
App Registration 3: SBC Teams Direct Routing (If Using SBA)
7. Microsoft Graph API Permissions
Complete Permissions Matrix
Graph API Endpoints Used
OVOC Teams Integration Requirements
8. Microsoft Teams Direct Routing Requirements

Certificate Requirements
Approved Certificate Authorities
DNS Requirements
Microsoft SIP Endpoints
Microsoft 365 Admin Roles Required
PowerShell Configuration Requirements
9. SBC Provisioning
9.1 Proxy SBC Provisioning (AWS)
9.2 Downstream SBC Provisioning (Physical)
9.3 High Availability Configuration
9.4 Compute Requirements
10. Security Controls
10.1 Administrative Access Controls
10.2 Role Hierarchy
10.3 Hardening and Default Account Management
10.4 SBC Management Authentication
11. SBC Network Configuration
11.1 Physical Connectivity
11.2 Logical Connectivity
11.3 Ethernet Device Configuration
11.4 IP Interfaces
12. TLS Certificate Configuration
12.1 TLS Context Configuration
12.2 Certificate Signing Request (CSR)
12.3 Deploying Trusted Root Certificates for MTLS
13. Media Configuration
13.1 NTP Server Configuration
13.2 Media Realm Configuration
13.3 Coder Groups
14. SIP Signalling Configuration
14.1 SIP Signalling Interfaces
14.2 Proxy Sets
15. Routing Configuration
15.1 IP Profiles
15.2 IP Groups
15.3 Message Manipulation Rules
15.4 Classification Rules
15.5 IP-to-IP Call Routing Rules
16. Firewall Rules
16.1 Proxy SBC Firewall Rules
16.2 OVOC Firewall Rules
16.3 ARM Firewall Rules
16.4 Downstream SBC Firewall Rules
16.5 SIP Generic Endpoint Firewall Rules
16.6 Teams Endpoints Firewall Rules
17. Break Glass Accounts
Overview
Requirements
Non-Production Environment Accounts
Production Australia Accounts

Production United States Accounts
Password Storage
Access Procedure
Password Rotation Schedule
18. Deployment Methodology
8-Phase Deployment Sequence
Deployment Methods by Component
19. High Availability Considerations
SBC HA Architecture
Prerequisites for HA Deployment
What Happens During SBC Failover
ARM HA Architecture
SIP Trunk Connectivity in HA
Voice Recording Considerations
20. IAM Permissions and Security
Stack Manager IAM Policy
SBC IAM Policy (Required for HA Failover)
IAM Role Creation Steps
21. Cyber Security Considerations
Overview
Security Architecture Summary
Stack Manager Component
Component Classification
Functional Description
IAM Permissions Required
Network Placement
VPC Endpoints (PrivateLink) — Required for AWS API Access
Security Considerations
Compliance Considerations
Risk Assessment Summary
Approval Checklist
22. Licensing Considerations
Mediant VE SBC Licensing
ARM Licensing
OVOC Licensing
22A. OVOC Data Analytics and Reporting
Overview
OVOC Data Analytics API
Available Database Views
Data Retention Constraints
Data Lake Integration Architecture
Power BI Configuration
Cyber Security Considerations
Licensing Prerequisite
23. References and Documentation
23.1 Official AudioCodes Documentation
23.2 Microsoft Documentation
23.3 AudioCodes Product Pages
23.4 AWS Marketplace Links
23.5 Third-Party References

Appendix A: Deployment Checklist
Pre-Deployment
Microsoft Entra ID Configuration
Break Glass Accounts
Component Deployment
Integration Verification
Appendix B: Credentials Reference Template
App Registration Credentials
Break Glass Account Reference
Appendix C: Quick Reference Tables
Port Summary
IP Range Summary (Microsoft Teams)
Instance Type Summary
Appendix D: Network Flow Diagrams
D.1 High-Level Architecture Overview
D.2 SIP Signalling Flows
D.3 Media (RTP/SRTP) Flows
D.4 Management & Monitoring Flows
D.5 Call Flow Examples
D.6 Port Summary Quick Reference
D.7 Microsoft Teams IP Ranges Quick Reference
D.8 Comprehensive Interface Mapping - All Appliances
Document Control

AudioCodes SBC - Unified Deployment & Configuration Guide

Cloud Operations & Voice Engineering Reference Document

Document Version: 2.6 **Date:** 13 February 2026 **Classification:** Public
Related Documents: AudioCodes AWS Deployment Guide v2.0, AudioCodes Detailed Design Document v1.0

Table of Contents

1. Executive Summary
2. Critical Findings
3. Architecture Overview
4. Component Specifications
5. AWS Infrastructure Requirements
6. Microsoft Entra ID Integration
7. Microsoft Graph API Permissions
8. Microsoft Teams Direct Routing Requirements
9. SBC Provisioning

10. Security Controls
11. SBC Network Configuration
12. TLS Certificate Configuration
13. Media Configuration
14. SIP Signalling Configuration
15. Routing Configuration
16. Firewall Rules
17. Break Glass Accounts
18. Deployment Methodology
19. High Availability Considerations
20. IAM Permissions and Security
21. Cyber Security Considerations
22. Licensing Considerations

- 22A. OVOC Data Analytics and Reporting

23. References and Documentation

- Appendix A: Deployment Checklist
- Appendix B: Credentials Reference Template
- Appendix C: Quick Reference Tables
- Appendix D: Network Flow Diagrams

---

1. Executive Summary

This document provides deployment guidance for the AudioCodes voice infrastructure stack on Amazon Web Services (AWS). It covers the deployment of:

- **Mediant Virtual Edition (VE) Session Border Controllers (SBCs)** in High Availability configuration
- **AudioCodes Stack Manager** for initial HA deployment and Day 2 operations
- **AudioCodes Routing Manager (ARM)** for centralized call routing
- **AudioCodes One Voice Operations Center (OVOC)** for management and monitoring

Key Takeaways

1. **Stack Manager for Deployment:** The AudioCodes Stack Manager is a **mandatory component for initial deployment** of Mediant VE SBCs in High Availability across multiple Availability Zones. It deploys the HA stack via CloudFormation but does **not** participate in active failover.

2. **SBCs Handle Failover:** During HA switchover, the **SBCs themselves** call AWS APIs to update route tables and move Virtual IPs. The HA subnet requires connectivity to AWS API endpoints.

3. **Stack Manager Retained for Day 2:** Stack Manager is recommended to be retained (low cost t3.medium) for ongoing management tasks such as software updates, stack healing, and configuration changes. A single instance is deployed per environment in the Australian region, managing all regions (including US) via cross-region AWS API calls.
4. **HA Scope:** High Availability is configured **within a single VPC across two Availability Zones**. This deployment does NOT use cross-VPC HA or AWS Transit Gateway for Virtual IP routing.
5. **Microsoft Integration Required:** All components require integration with Microsoft Entra ID (Azure AD) for authentication and Microsoft Graph API for Teams call quality data and user information.
6. **Break Glass Accounts:** Each workload requires a dedicated local break glass account for emergency access when identity provider integration fails.

Scope

This guide covers: - AWS deployment of AudioCodes virtual appliances - SBC configuration for Microsoft Teams Direct Routing - High Availability design and failover mechanisms - Integration with Microsoft Entra ID and Graph API

---

2. Critical Findings

Stack Manager Requirement for Cross-AZ HA

When deploying AudioCodes Mediant VE SBCs in High Availability across two Availability Zones in AWS, the **Stack Manager is a mandatory separate VM for initial deployment** that performs the following critical functions:

1. **Initial Stack Deployment:** The Stack Manager deploys and configures the SBC HA stack via CloudFormation, including all required network interfaces, security groups, and route table entries.
2. **Virtual IP Address Management:** The Stack Manager allocates and manages Virtual IP addresses (from the `10.x.x.x` range) that are routable within the VPC CIDR during initial deployment.
3. **Cluster Lifecycle Management:** The Stack Manager handles initial deployment, topology updates, and “stack healing” in case of underlying cloud resource corruption.
4. **Day 2 Operations:** While Stack Manager can technically be decommissioned after initial deployment, it is recommended to retain it for ongoing management tasks such as software updates, configuration changes, and stack maintenance.

Important Clarification: The Stack Manager does **not** participate in active HA switchover. During failover, the **SBCs themselves** send AWS API commands to update route tables and move Virtual IPs to the newly active SBC. This is why the HA subnet requires connectivity to AWS API endpoints.

How the Failover Mechanism Works

Key Point: The SBCs themselves handle HA switchover by communicating directly with AWS APIs. The Stack Manager is used for initial deployment only and does not participate in active failover.

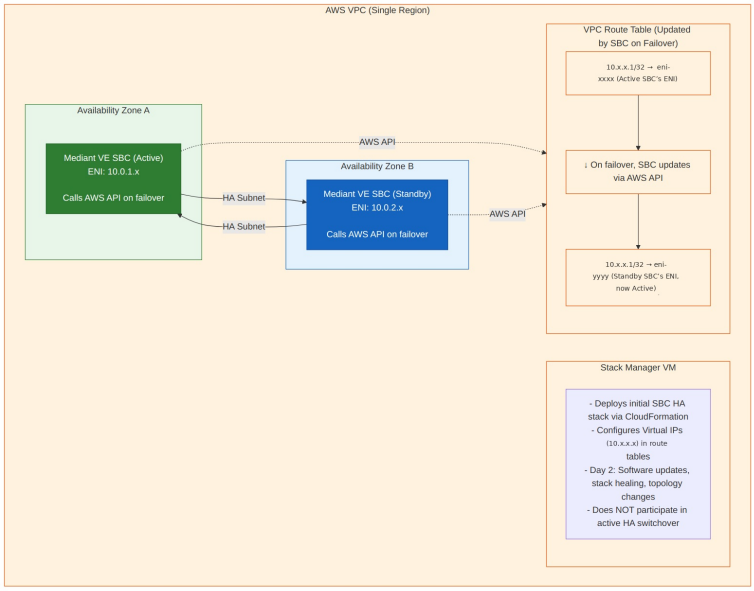


Diagram 1

HA Scope Clarification

Important: This deployment uses HA **within a single VPC across two Availability Zones only**. We are NOT implementing: - Cross-VPC HA - Cross-region HA for SBCs - AWS Transit Gateway for Virtual IP routing between VPCs

The Virtual IP addresses are used for failover routing **within the same VPC**, where the route table is updated to point traffic to the newly active SBC's ENI.

> **Cross-Region SBC-to-SBC Connectivity:** While HA failover VIP routing is scoped to a single VPC, the Virtual IPs assigned to each regional SBC pair **do** need to be routable between the AU and US regions for SBC-to-SBC (proxy-to-proxy) signalling and media. This cross-region reachability is provided by the organisation's existing network backbone (AWS Direct Connect / VPN) and does not require AWS Transit Gateway. The Transit Gateway exclusion above refers specifically to HA failover VIP routing between VPCs, not to general cross-region SBC-to-SBC reachability.

API Access Requirements

Stack Manager API Access

The Stack Manager requires **internet access** (via Internet Gateway or NAT Gateway) to communicate with AWS APIs for initial deployment and Day 2 operations. The Stack Manager is deployed in the Australian region only and manages SBC HA stacks in all regions (including US) via cross-region AWS API calls: - EC2 API (including cross-region endpoints for US region management) - CloudFormation API - IAM API - Elastic Load Balancing API (if using NLB)

SBC API Access (Critical for HA Failover)

The SBCs require **internet access from the HA subnet** to communicate with AWS APIs during failover. The SBCs themselves call AWS APIs to update route tables and move Virtual IPs during switchover: - EC2 API (route table manipulation, ENI management)

Important: The HA subnet must have a route to AWS API endpoints, either via: - NAT Gateway (recommended for private subnets) - VPC Endpoints for EC2 (PrivateLink) - Internet Gateway (if using public IPs on HA interfaces - not recommended)

---

3. Architecture Overview

Non-Production Environment (Australia Region Only)

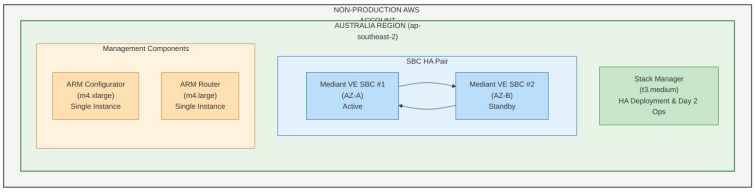


Diagram 2

Total VMs: 5 - 2x SBC (HA pair) - 1x Stack Manager - 1x ARM Configurator - 1x ARM Router

Production Environment

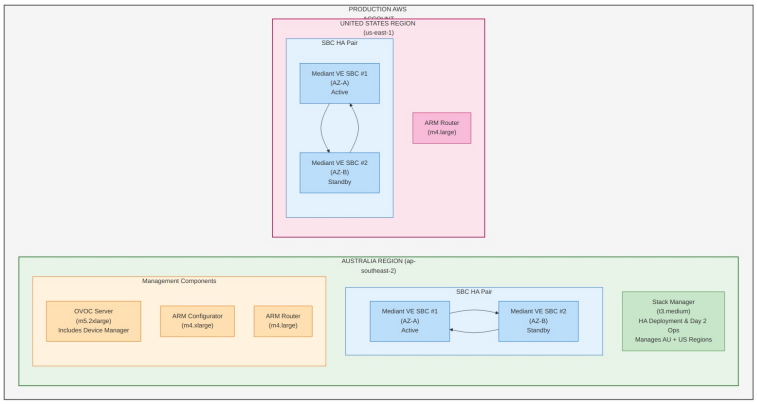


Diagram 3

Total AUS VMs: 6 - 2x SBC (HA pair) - 1x Stack Manager - 1x OVOC (includes Device Manager) - 1x ARM Configurator - 1x ARM Router

Total US VMs: 3 - 2x SBC (HA pair) - 1x ARM Router

> **Note:** The US region does not have a dedicated Stack Manager. The Australian Stack Manager manages US SBC HA stacks remotely via cross-region AWS API calls.

PRODUCTION TOTAL: 9 VMs

4. Component Specifications

Mediant Virtual Edition (VE) SBC

Specification	Details
Purpose	Session Border Controller for SIP trunking, security, media handling
HA Mode	1+1 Active/Standby across Availability Zones (within single VPC)
Minimum Version for Cross-AZ HA	Version 7.4.500
Deployment Method	Via Stack Manager (required for multi-AZ HA)

Recommended EC2 Instance Types

Use Case	Instance Type	vCPUs	Memory	Notes
Without Transcoding	m5.large	2	8 GiB	Basic SIP proxy
				Memory optimized (r4

Without Transcoding (Higher capacity)	r4.large	2	15.25 GiB	is previous-generation; consider r5 or r6i for better price-performance)
With Transcoding	c5.2xlarge	8	16 GiB	Compute optimized for DSP
With Transcoding (High capacity)	c5.9xlarge	36	72 GiB	High session count with transcoding

Network Interfaces Required (per SBC)

Interface	Purpose	Subnet Type
eth0	HA Communication + AWS API Access	HA Subnet (dedicated)
eth1	Management + LAN/Internal (OVOC, ARM, SSH, HTTPS, Downstream/Site SBCs, Third-Party PBX, ATAs)	Internal Subnet
eth2	WAN/External (Microsoft Teams Direct Routing, SIP Providers, Public SIP)	DMZ/External Subnet

> **SIP Connectivity Direction:** All SIP connectivity on eth1 to site SBCs, existing third-party PBX systems (e.g., Cisco CUCM, Avaya Aura, Mitel), and ATAs (Analog Telephone Adapters) is **bidirectional — both inbound and outbound**. The SBC operates as a Back-to-Back User Agent (B2BUA) with paired IP-to-IP Routing Rules configured for each direction. Inbound calls (from these entities toward the Proxy SBC) are classified via Classification Rules and Proxy Set matching; outbound calls (from the Proxy SBC toward these entities) are routed via the destination IP Group's Proxy Set. SIP signalling and RTP media flow in both directions for all connected entity types.

SBC IAM Role Requirements

The SBCs require an IAM role to call AWS APIs during HA failover. The SBC directly manipulates route tables to redirect traffic during switchover.

```
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "AllowDescribeActions",
                    "Effect": "Allow",
                    "Action": [
                        "ec2:DescribeAddresses",
                        "ec2:DescribeNetworkInterfaceAttribute",
                        "ec2:DescribeNetworkInterfaces"
                    ],
                    "Resource": "*"
                },
                {
                    "Sid": "AllowReplaceRoute",
                    "Effect": "Allow",
                    "Action": "ec2:ReplaceRoute",
                    "Resource": "arn:aws:ec2:<REGION>:<ACCOUNT_ID>:route-
table/<ROUTE_TABLE_ID>",
                    "Condition": {
                        "StringEquals": {
                            "aws:ResourceTag/Env": "<NonProd_SBC|Prod_SBC>"
                        }
                    }
                },
                {
                    "Sid": "AllowAssociateAddress",
                    "Effect": "Allow",
                    "Action": "ec2:AssociateAddress",
                    "Resource": "arn:aws:ec2:<REGION>:<ACCOUNT_ID>:elastic-
ip/<EIP_ALLOCATION_ID>",
                    "Condition": {
                        "StringEquals": {
                            "aws:ResourceTag/App": "Voice",
                            "aws:ResourceTag/Env": "<NonProd_SBC|Prod_SBC>"
                        }
                    }
                }
            ]
        }
```

> **Note:** Replace `<REGION>`, `<ACCOUNT_ID>`, `<ROUTE_TABLE_ID>`, and `<EIP_ALLOCATION_ID>` with your environment-specific values. The `Env` tag value should match your environment naming convention (e.g., `NonProd_SBC` or `Prod_SBC`).

Note: The HA subnet must have connectivity to AWS API endpoints (via NAT Gateway or VPC Endpoint) for failover to function correctly.

Stack Manager Specifications

The Stack Manager is a **Linux-based application** that can be installed on a server running a supported operating system. It is not limited to pre-built cloud marketplace images — it can be deployed on any VM or bare-metal server using a two-step process: provision a server with a supported OS,

then install the Stack Manager application. This means it can also run on an organisation's **Standard Operating Environment (SOE)** OS, provided it is one of the supported distributions listed below.

Specification	Details
Purpose	HA cluster deployment, lifecycle management, Day 2 operations
Type	Linux application (Python-based, uses its own virtual environment)
EC2 Instance Type	t3.medium (when deployed on AWS)
Minimum Resources	1 vCPU, 2 GB RAM, 10 GB disk
Storage	8 GiB gp3 (default on AWS)
Deployment	One per environment, hosted in Australian region; manages all regions including US via cross-region AWS API calls
Lifecycle	Retained ongoing for Day 2 operations (low cost)

Supported Operating Systems

The Stack Manager application supports the following Linux distributions:

Distribution	Supported Versions
Ubuntu	18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS
Debian	10 (Buster), 11 (Bullseye), 12 (Bookworm), 13 (Trixie)
Red Hat Enterprise Linux (RHEL)	8, 9
CentOS / CentOS Stream	8, 9
Rocky Linux	8, 9
AlmaLinux	8, 9
Amazon Linux	2, 2023

> **SOE Compatibility:** Organisations running RHEL 8/9, CentOS 8/Stream 9, Rocky Linux 8/9, or AlmaLinux 8/9 as their Standard Operating Environment can install Stack Manager directly on their SOE-compliant servers without requiring a separate appliance image.

Deployment Options

Method	Description
Cloud Marketplace Image	Pre-built images available in AWS AMI, Azure Marketplace, and GCP (recommended for simplicity)
Software Application Install	Install on any VM or server running a supported OS (two-step: provision OS, then install application)
Containerised Mode	Docker/Podman deployment mode for managing Mediant VE/CE as container images on remote hosts via SSH

Critical Requirements

- **Hosted in the Australian region** and manages SBC HA stacks across all regions via cross-region AWS API calls
- **Requires internet access** (via IGW or NAT Gateway) for AWS API calls (including cross-region API endpoints)
- **IAM Role** with EC2, CloudFormation, IAM, and optionally ELB permissions

Operational Notes

- **Does not participate in HA failover** - SBCs handle switchover directly via AWS APIs
- **Can be decommissioned** after initial deployment if Day 2 operations are not required
- **Recommended to retain** - low cost (t3.medium) and useful for software updates, stack healing, and configuration changes
- See Cyber Security Variation section for security details

AudioCodes Routing Manager (ARM) Specifications

Component	Instance Type	vCPUs	Memory	Quantity
Configurator	m4.xlarge	4	16 GiB	1 (single instance)
Router	m4.large	2	8 GiB	1+ per region

> **Note:** m4 is a previous-generation instance family. If AudioCodes AMI compatibility permits, consider m5 or m6i equivalents for better price-performance.

Deployment Requirements

- **All ARM VMs must be in the same VPC and subnet**
- Configurator: Single instance only (centralized in AUS)
- Router: Deploy one per region for local routing decisions

AudioCodes One Voice Operations Center (OVOC) Specifications

Profile	Instance Type	vCPUs	Memory	Storage
Low Profile	m5.2xlarge	8	32 GiB	500 GB GP3 SSD
High Profile	m5.4xlarge	16	64 GiB	2 TB GP3 SSD

Includes

- Device Manager functionality (manages IP phones and SBCs)
- Quality of Experience monitoring
- Network topology management
- **Microsoft Teams Call Quality Dashboard integration**

Compute Requirements Summary (from Design Document)

Application	Resource	Instance Type	Memory	Recommended Disk Space	Proc
VM for Mediant VE Proxy SBC (HA Pair)	AWS	m5n.large	8 GiB	20 GB	2 vCI
VM for Stack Manager	AWS	t3.medium	4 GiB	10 GB	2 vCI
OVOC	AWS	m5.4xlarge	64 GiB	AWS EBS: GP3 SSD 2 TB	16 v(
ARM Configurator	AWS	m4.xlarge	16 GiB	100 GB	4 vCI
ARM Router	AWS	m4.large	8 GiB	80 GB	2 vCI

> **Notes:**
>
> - The Mediant VE Proxy SBC instance type (m5n.large) is selected for its enhanced networking performance, which is critical for real-time voice media processing.
> - The Stack Manager (t3.medium) is a lightweight management component but is mandatory for initial HA deployment and Day 2 operations.
> - OVOC (One Voice Operations Center) requires substantial resources due to its role in centralised monitoring, analytics, and quality-of-experience reporting across all SBC instances.
> - ARM (AudioCodes Routing Manager) consists of two components: the Configurator (management and policy engine) and the Router (real-time call routing decisions). Both must be deployed for full ARM functionality.
> - All AWS instances should be deployed with appropriate EBS volume types and IOPS provisioning based on workload requirements. GP3 SSD is recommended as the baseline storage tier.

5. AWS Infrastructure Requirements

VPC Configuration

Per Region Requirements

Resource	Requirement	Notes
VPC	1 per region	Dedicated or shared
Subnets	Minimum 2 per AZ (Main + HA)	Plus optional additional subnets
Internet Gateway or NAT Gateway	Required	For Stack Manager API access
Route Tables	One per subnet minimum	Stack Manager will modify these

Subnet Design

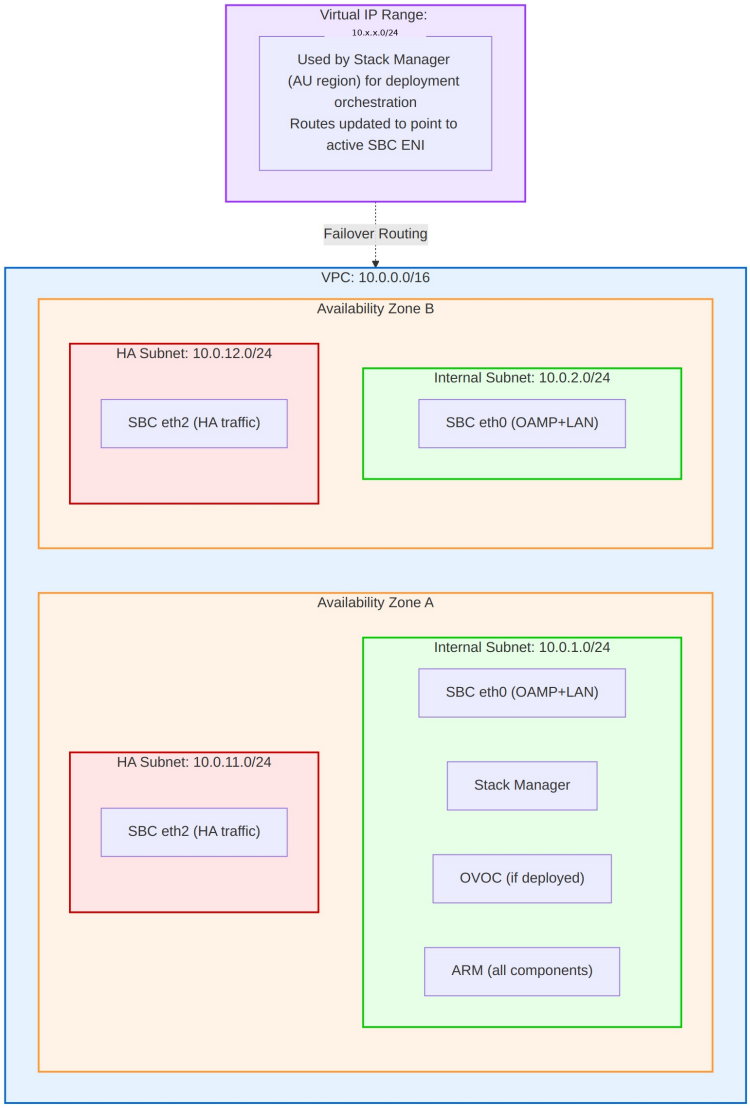


Diagram 4

Security Groups

Stack Manager Security Group

Direction	Protocol	Port	Source/Destination	Purpose
Inbound	TCP	22	Admin CIDR	SSH Management
Inbound	TCP	443	Admin CIDR	HTTPS Management
Outbound	TCP	443	VPC Endpoint SG	AWS API Access (EC2, CloudFormation, CloudWatch, IAM via PrivateLink)

Outbound	TCP	443	S3 Prefix List	S3 Access (CloudFormation templates, firmware storage)
Outbound	All	All	VPC CIDR	SBC Communication

SBC HA Security Group (eth0 — HA ENI)

Direction	Protocol	Port	Source/Destination	Purpose
Inbound	All	All	HA Subnet CIDR	HA Communication (heartbeat & state sync)
Outbound	TCP	443	VPC Endpoint SG	AWS EC2 API (HA failover — route table updates, EIP reassignment via PrivateLink)
Outbound	All	All	HA Subnet CIDR	HA Communication

SBC Internal Security Group (eth1 — Internal/LAN ENI)

Direction	Protocol	Port	Source/Destination	Purpose
Inbound	TCP	22	Admin CIDR	SSH Management
Inbound	TCP	80/443	Admin CIDR	Web Management
Inbound	TCP	443	OVOC CIDR	OVOC Device Management
Inbound	UDP	161	OVOC CIDR	SNMP Polling (OVOC)
Inbound	TCP/UDP	5060/5061	SIP Endpoints	SIP Signalling (internal)
Inbound	UDP	6000-19999	Internal Media Sources	RTP Media (internal, downstream)
Inbound	UDP	30000-39999	Endpoint CIDRs	LMO Media
				Cross-region

Inbound	All	All	Other Region VPC CIDR	SBC-to-SBC and management connectivity
Outbound	TCP/UDP	5060-5061	VPC CIDR	SIP Signalling (downstream SBCs, PBX, proxy-to-proxy)
Outbound	UDP	6000-39999	VPC CIDR	RTP Media (internal, downstream, LMO)
Outbound	TCP	443	OVOC CIDR	OVOC Device Management (REST API, keep-alive)
Outbound	UDP	162	OVOC CIDR	SNMP Traps to OVOC
Outbound	UDP	514	OVOC CIDR	Syslog to OVOC
Outbound	TCP	5001	OVOC CIDR	QoE Reporting to OVOC
Outbound	All	All	Other Region VPC CIDR	Cross-region SBC-to-SBC connectivity

SBC External Security Group (eth2 — External/WAN ENI)

Direction	Protocol	Port	Source/Destination	Purpose
Inbound	TCP	5061	52.112.0.0/14, 52.122.0.0/15	Teams SIP Signalling (TLS)
Inbound	UDP	20000-21999	52.112.0.0/14, 52.120.0.0/14	Teams Media (SRTP)
Inbound	UDP/TCP	5060, 5061	SIP Provider CIDRs	SIP Provider Signalling (inbound)
Inbound	UDP	40000-41999	SIP Provider CIDRs	PSTN Media (inbound from carrier)

Inbound	All	All	Other Region VPC CIDR	Cross-region SBC connectivity
Outbound	TCP	5061	52.112.0.0/14, 52.120.0.0/14	Teams Direct Routing SIP Signalling (TLS)
Outbound	UDP	20000-21999	52.112.0.0/14, 52.120.0.0/14	Teams Media (SRTP)
Outbound	UDP/TCP	5060-5061	SIP Provider CIDRs	SIP Provider Signalling (outbound)
Outbound	UDP	40000-41999	SIP Provider CIDRs	PSTN Media (outbound to carrier)
Outbound	All	All	Other Region VPC CIDR	Cross-region SBC connectivity

ARM Security Group

Direction	Protocol	Port	Source/Destination	Purpose
Inbound	TCP	22	Admin CIDR	SSH
Inbound	TCP	80/443	Enterprise CIDR	HTTP/HTTPS
Inbound	All	All	VPC CIDR	Internal communication
Inbound	All	All	Other Region VPC CIDR	Cross-region SBC and ARM Router connectivity
Outbound	TCP	443	20.20.32.0/19, 20.190.128.0/18, 20.231.128.0/19, 40.126.0.0/18	Microsoft Graph API and Entra ID Authentication (M365 Endpoint ID 56)
Outbound	All	All	VPC CIDR	Internal communication (SBC management, OVOC)
Outbound	All	All	Other Region VPC	Cross-region ARM Router

			CIDR	connectivity

OVOC Security Group

Direction	Protocol	Port	Source/Destination	Purpose
Inbound	TCP	22	Admin CIDR	SSH
Inbound	TCP	443	Admin CIDR	HTTPS Web UI
Inbound	TCP	443	Reverse Proxy CIDR	Graph API Webhooks (via Cloud Firewall + Reverse Proxy)
Inbound	UDP	162	SBC CIDR	SNMP Traps
Inbound	UDP	1161	SBC CIDR	Keep-alive (NAT traversal)
Inbound	UDP	514	SBC CIDR	Device Syslog Ingestion (audit logging)
Inbound	TCP	5001	SBC CIDR	QoE Reporting
Inbound	TCP	5432	ETL Platform CIDR	Analytics API (PostgreSQL)
Outbound	TCP	443	20.20.32.0/19, 20.190.128.0/18, 20.231.128.0/19, 40.126.0.0/18	Microsoft Graph API and Entra ID Authentication (M365 Endpoint ID 56)
Outbound	TCP	514	Syslog/SIEM CIDR	Audit Log Forwarding (syslog to SIEM)
Outbound	UDP	1164-1174	NMS/SIEM CIDR	SNMP Trap Forwarding (audit events to NMS)
Inbound	All	All	Other Region VPC CIDR	Cross-region SBC connectivity
Outbound	All	All	VPC CIDR	Internal traffic

> **Security Group Design Notes:**
>
> - **No 0.0.0.0/0 outbound rules.** All egress is restricted to specific destinations following the principle of least privilege.

> - **AWS API access** (Stack Manager, SBC HA failover) uses **VPC Endpoints (PrivateLink)** for EC2, CloudFormation, CloudWatch, and IAM. This keeps API traffic within the AWS network and eliminates internet egress requirements. See Section 20 for VPC Endpoint setup.
> - **S3 access** uses a **VPC Gateway Endpoint** with prefix list reference in security group rules (no hourly cost).
> - **Microsoft Graph API and Entra ID authentication** (OVOC, ARM) uses published Microsoft 365 Endpoint ID 56 CIDRs: `20.20.32.0/19`, `20.190.128.0/18`, `20.231.128.0/19`, `40.126.0.0/18`. These ranges are published via the Microsoft 365 IP Address and URL web service and should be reviewed monthly for changes. Consider automating updates via Lambda polling the M365 endpoints version API.
> - **Teams Direct Routing** CIDRs (`52.112.0.0/14`, `52.120.0.0/14`) are stable and documented in the Direct Routing planning guide.
> - **SIP Provider CIDRs** must be obtained from each carrier and maintained as provider-specific managed prefix lists or documented CIDRs.

> **Audit Logging:** OVOC provides two layers of audit logging: OS-level audit logging via Linux **auditd** (STIG-compliant, logs to `/var/log/audit/`) and application-level logging via the **Actions Journal** (tracks configuration changes, user actions, and device operations). Audit logs can be forwarded to an external SIEM (e.g., Splunk, Azure Sentinel) via syslog (TCP 514), SNMP traps (UDP 1164-1174), or the REST API (HTTPS 443). The OVOC Northbound Interface supports Syslog, SNMP (v2/v3), Email, and REST as alarm and journal forwarding destinations. Device syslog ingestion (UDP 514 inbound) allows OVOC to collect syslog messages directly from managed SBCs without requiring a separate syslog server. It is **recommended** to enable auditd and configure syslog forwarding to the organisation's SIEM for centralised audit trail and compliance reporting.

External Publishing Patterns

Two distinct external publishing patterns are used in this architecture, reflecting the different protocol requirements of each component.

Proxy SBC — Bespoke External Publishing (Dedicated EIP + Security Group)

The Proxy SBC uses a bespoke external publishing pattern for public-facing connectivity to Microsoft Teams Direct Routing and PSTN SIP providers. This pattern differs from standard reverse proxy or application gateway approaches commonly used for web applications.

Architecture:

- **Dedicated Elastic IP (EIP):** Each Proxy SBC HA pair is assigned a dedicated Elastic IP address on the External (WAN) ENI. The EIP

provides the public-facing IP address for SIP signalling (TLS 5061) and SRTP media (UDP 20000-21999). During HA failover, the EIP is automatically reassigned to the newly Active instance.
- **AWS Security Group (Layer 4):** Traffic filtering is enforced at the AWS Security Group level using Layer 4 rules (protocol, port, source/destination CIDR). Security Groups act as a stateful firewall controlling inbound and outbound traffic to the External ENI. SIP and media traffic from Microsoft Teams and PSTN providers is permitted based on published IP ranges and port allocations.
- **No Reverse Proxy or Firewall on External Side:** The SBC's WAN ENI is **not** behind a cloud firewall or reverse proxy. SIP/TLS and SRTP/RTP protocols require direct IP connectivity between the SBC and external parties for proper NAT traversal, session persistence, and real-time media delivery. The SBC handles its own TLS termination, SIP message inspection, and media anchoring natively.

Design Rationale:

- SIP signalling requires stateful session tracking that is incompatible with traditional load balancers or reverse proxies.
- SRTP media streams require low-latency, direct UDP connectivity — additional proxy hops introduce jitter and latency.
- Microsoft Teams Direct Routing expects the SBC FQDN to resolve directly to the SBC's public IP (EIP) for TLS certificate validation.
- The SBC's built-in VoIP firewall provides application-layer (Layer 7) SIP message inspection, rate limiting, and classification in addition to the Layer 4 Security Group rules.

OVOC — Traditional Ingress (Cloud Firewall + Reverse Proxy)

OVOC and other management components that require inbound HTTPS connectivity from the internet use the organisation's standard ingress pattern: cloud firewall with reverse proxy.

Architecture:

- **Cloud Firewall:** Inbound traffic from the internet is inspected by the cloud firewall, which provides Layer 7 application inspection, threat prevention, URL filtering, and SSL decryption capabilities.
- **Reverse Proxy:** Behind the cloud firewall, a reverse proxy terminates and forwards HTTPS requests to the internal OVOC instance on the Internal Subnet. The reverse proxy provides an additional layer of access control and decouples the internal service from direct internet exposure.
- **No Direct Public IP on OVOC:** Unlike the SBC, OVOC does not have a dedicated Elastic IP or public-facing ENI. The OVOC instance resides entirely on the Internal Subnet and is reachable from the internet only via the cloud firewall + reverse proxy ingress path.
- **FQDN Resolution:** The OVOC FQDN (e.g., `ovoc.yourdomain.com`) resolves to the public IP of the cloud firewall / reverse proxy ingress, not directly to the OVOC instance.

Applicable Traffic:

Traffic	Source	Destination	Protocol	Path
Graph API Webhooks	Microsoft 365	OVOC	TCP 443	Internet → Cloud Firewall → Reverse Proxy → OVOC
OVOC Web UI	Admin Users	OVOC	TCP 443	Internet → Cloud Firewall → Reverse Proxy → OVOC

Design Rationale:

- OVOC uses standard HTTPS (TCP 443) which is fully compatible with reverse proxy and Layer 7 firewall inspection.
- The cloud firewall provides centralised threat prevention, logging, and compliance enforcement for all inbound HTTPS traffic.
- Microsoft 365 Graph API webhooks are standard HTTPS POST requests that traverse the reverse proxy without protocol compatibility issues.
- This pattern aligns with the organisation's standard security posture for publishing internal services to the internet.

Cloud East-West Firewall

Internal/private-side traffic between the SBC and on-premises infrastructure traverses a cloud east-west firewall for traffic inspection, policy enforcement, and security monitoring. This applies to all traffic on the Internal (OAMP + LAN) subnet.

Inspection Scope:

Traffic Type	Source	Destination	Protocol/Ports	Inspection
SIP Signalling	Proxy SBC	Downstream SBCs	TCP/UDP 5060, 5061	Inspected
RTP Media	Proxy SBC	Downstream SBCs	UDP 6000-19999	Inspected
Management	OVOC/ARM	Proxy SBC	TCP 443, UDP 162	Inspected
Management	Admin	Proxy SBC	TCP 22, TCP 443	Inspected
Analytics ETL	ETL Platform	OVOC	TCP 5432	Inspected

Design Considerations:

- The cloud east-west firewall sits in the traffic path between the AWS VPC and on-premises infrastructure (via AWS Direct Connect / Transit Gateway). All internal traffic traverses this firewall for inspection.
- Firewall rules must permit SIP signalling and RTP media ports as documented in the firewall rules tables (Sections 15-16). Blocking or rate-limiting RTP traffic will cause call quality degradation.
- The firewall must support UDP session tracking for SIP and RTP traffic. Stateless firewalls or firewalls with aggressive UDP timeout values may cause media drops or one-way audio.
- Firewall logging provides visibility into east-west traffic flows for security monitoring, compliance, and troubleshooting.
- The external/public-facing interface (WAN ENI) does **not** traverse the east-west firewall — it is protected by the AWS Security Group and the SBC's native VoIP firewall (see External Publishing Pattern above).

---

6. Microsoft Entra ID Integration

Overview

All AudioCodes components require integration with Microsoft Entra ID (formerly Azure AD) for: - User authentication (OAuth 2.0) - Microsoft Teams Direct Routing - Call quality data retrieval - User directory information

Required App Registrations Summary

App Registration	Used By	Purpose
AudioCodes-OVOC-Teams-Integration	OVOC	Teams QoE data, user information
AudioCodes-ARM-WebUI	ARM	Web UI authentication
AudioCodes-SBC-DirectRouting	SBC	Teams Direct Routing SBA (if applicable)

App Registration 1: OVOC Teams Integration

Purpose: Enables OVOC to retrieve Microsoft Teams call quality data and user information via Microsoft Graph API.

Registration Steps

1. Navigate to **Azure Portal** > **Microsoft Entra ID** > **App registrations** > **New registration**

2. Configure:
   - **Name:** `AudioCodes-OVOC-Teams-Integration`
   - **Supported account types:** Accounts in this organizational directory only (Single tenant)
   - **Redirect URI:** Leave blank (not required for application permissions)
3. Click **Register**

Credentials to Capture

Credential	Location	Usage
Application (Client) ID	Overview blade	OVOC configuration
Directory (Tenant) ID	Overview blade	OVOC configuration
Client Secret	Certificates & secrets blade	OVOC configuration

Client Secret Creation

1. Navigate to **Certificates & secrets** > **Client secrets** > **New client secret**
2. Description: `OVOC-Teams-QoE-Integration`
3. Expiry: Select appropriate expiry (recommend 24 months with calendar reminder)
4. **IMPORTANT:** Copy the secret value immediately - it cannot be retrieved later

API Permissions Required

API	Permission	Type	Purpose
Microsoft Graph	`CallRecords.Read.All`	Application	Read all call records (CDR/QoE)
Microsoft Graph	`User.Read.All`	Application	Read user profiles

Grant Admin Consent

1. Navigate to **API permissions**
2. Click **Grant admin consent for [Tenant Name]**
3. Verify both permissions show green checkmarks under “Status”

OVOC Configuration

Configure in OVOC under **System** > **Administration** > **External Servers** > **Microsoft 365**:

Field	Value
Tenant ID	`<Directory (Tenant) ID>`
Client ID	`<Application (Client) ID>`
Client Secret	`<Secret Value>`

App Registration 2: ARM Web UI Authentication

Purpose: Enables OAuth 2.0 authentication for ARM web interface users.

Registration Steps

1. Navigate to **Azure Portal** > **Microsoft Entra ID** > **App registrations** > **New registration**
2. Configure:
   - **Name:** `AudioCodes-ARM-WebUI`
   - **Supported account types:** Accounts in this organizational directory only
   - **Redirect URI:** `https://<ARM-FQDN>/ARM/armui/login`
3. Click **Register**

Authentication Configuration

1. Navigate to **Authentication**
2. Under **Implicit grant and hybrid flows**, enable:
   ☒ Access tokens
   ☒ ID tokens

API Permissions Required

API	Permission	Type	Purpose
Microsoft Graph	`User.Read`	Delegated	Sign in and read user profile
Microsoft Graph	`User.Read.All`	Application	Read all users' full profiles
Microsoft Graph	`Group.Read.All`	Application	Read all groups
Microsoft Graph	`Application.Read.All`	Application	Read all applications

Create App Roles

Navigate to **App roles** > **Create app role** for each role:

Display Name	Value	Description
Security Administrator	`SecurityAdmin`	Full administrative access
Administrator	`Admin`	Standard administrative access
Monitor	`Monitor`	Read-only monitoring access

Enterprise Application Assignment

1. Navigate to **Enterprise applications** > **AudioCodes-ARM-WebUI**
2. Under **Users and groups**, assign users/groups to appropriate roles

---

App Registration 3: SBC Teams Direct Routing (If Using SBA)

Purpose: Required if using Survivable Branch Appliance (SBA) functionality with Teams Direct Routing.

Registration Steps

1. Navigate to **Azure Portal** > **Microsoft Entra ID** > **App registrations** > **New registration**
2. Configure:
   - **Name:** `AudioCodes-SBC-DirectRouting`
   - **Supported account types:** Accounts in this organizational directory only
   - **Redirect URI:** `https://login.microsoftonline.com/common/oauth2/nativeclient`
3. Click **Register**

Authentication Configuration

1. Navigate to **Authentication**
2. Under **Implicit grant and hybrid flows**, enable:
   ☒ Access tokens
   ☒ ID tokens

API Permissions Required

API	Permission	Type	Purpo
Skype and Teams Tenant Admin API	`application_access_custom_sba_appliance`	Application	SBA appliar access

Note: Admin consent is required for this permission.

---

7. Microsoft Graph API Permissions

Complete Permissions Matrix

Component	API	Permission	T
	Microsoft		

OVOC	Graph	`CallRecords.Read.All`	App
OVOC	Microsoft Graph	`User.Read.All`	App
ARM	Microsoft Graph	`User.Read`	Del
ARM	Microsoft Graph	`User.Read.All`	App
ARM	Microsoft Graph	`Group.Read.All`	App
ARM	Microsoft Graph	`Application.Read.All`	App
SBC	Skype and Teams Tenant Admin	`application_access_custom_sba_appliance`	App

Graph API Endpoints Used

Component	Endpoint
OVOC	`https://graph.microsoft.com/v1.0/communications/callRec`
OVOC	`https://graph.microsoft.com/v1.0/users`
ARM	`https://graph.microsoft.com/v1.0/me`
ARM	`https://graph.microsoft.com/v1.0/users`
ARM	`https://graph.microsoft.com/v1.0/groups`

OVOC Teams Integration Requirements

Prerequisites

1. **OVOC Version:** 8.0 or later (8.0.114+ recommended)
2. **License:** Active “Analytics” license for Teams QoE monitoring
3. **Certificate:** OVOC must have a **valid public CA certificate** (not self-signed)
4. **Network (Outbound):** Outbound HTTPS (443) to Microsoft Graph API endpoints
5. **Network (Inbound):** OVOC must be reachable from Microsoft 365 IPs on TCP 443 for webhook notifications. Inbound traffic is published via

the cloud firewall + reverse proxy ingress path (see Section 5 External Publishing Patterns).

6. **FQDN:** Properly configured FQDN (e.g., `ovoc.yourdomain.com`) resolving to the public IP of the cloud firewall / reverse proxy ingress

Data Retrieved from Microsoft

Data Type	Graph API	Retention
Call Detail Records (CDR)	CallRecords API	Per OVOC retention policy
Call Quality Metrics (QoE)	CallRecords API	Per OVOC retention policy
User Display Names	Users API	Cached
User Principal Names	Users API	Cached

8. Microsoft Teams Direct Routing Requirements

Certificate Requirements

Requirement	Details
Certificate Authority	Must be signed by a CA in the Microsoft Trusted Root Certificate Program
Subject Name (CN) or SAN	Must contain the SBC FQDN (e.g., `sbc.yourdomain.com`)
Extended Key Usage	Must include Client Authentication EKU (enforcement timeline evolving – verify against latest Microsoft Message Center announcements)
TLS Version	TLS 1.2 minimum (TLS 1.3 recommended)
Mutual TLS (mTLS)	Required for SBC-to-Teams connectivity

Approved Certificate Authorities

- DigiCert
- GlobalSign
- Comodo/Sectigo
- Entrust
- GoDaddy

Note: Self-signed certificates are NOT supported.

DNS Requirements

Record Type	Name	Value	Purpose
A	`sbc.yourdomain.com`	`<SBC Public IP>`	SBC endpoint resolution

Domain Registration: The domain used for the SBC FQDN must be registered and verified in your Microsoft 365 tenant.

Microsoft SIP Endpoints

The SBC connects outbound to these Microsoft endpoints (allow in firewall):

FQDN	Port	Protocol	Purpose
`sip.pstnhub.microsoft.com`	5061	TLS	Primary SIP endpoint
`sip2.pstnhub.microsoft.com`	5061	TLS	Secondary SIP endpoint
`sip3.pstnhub.microsoft.com`	5061	TLS	Tertiary SIP endpoint

Microsoft 365 Admin Roles Required

Role	Purpose
Global Administrator	Grant admin consent for app registrations
Teams Administrator	Configure Direct Routing, voice policies
Teams Communications Administrator	Manage calling policies

PowerShell Configuration Requirements

Required Modules

```
        # Install MicrosoftTeams module
        Install-Module -Name MicrosoftTeams -Force -AllowClobber

        # Connect to Teams (interactive)
        Connect-MicrosoftTeams

        # Or connect with service principal (for automation)
        Connect-MicrosoftTeams -TenantId "<TenantId>" -ApplicationId "
<AppId>" -CertificateThumbprint "<Thumbprint>"
```

Key PowerShell Commands

```
        # Register SBC in Teams
        New-CsOnlinePSTNGateway -Fqdn "sbc.yourdomain.com" -SipSignalingPort
```

```
5061 -Enabled $true

        # View registered SBCs
        Get-CsOnlinePSTNGateway

        # Create voice routing policy
        New-CsOnlineVoiceRoutingPolicy -Identity "AU-VoicePolicy" -
OnlinePstnUsages @{Add="AU-Usage"}

        # Enable user for Direct Routing
        Set-CsPhoneNumberAssignment -Identity user@domain.com -PhoneNumber
"+61XXXXXXXXX" -PhoneNumberType DirectRouting
```

---

9. SBC Provisioning

9.1 Proxy SBC Provisioning (AWS)

The Proxy SBC is deployed as an AudioCodes Mediant VE (Virtual Edition) SBC instance within AWS. Prior to provisioning, the following deployment prerequisites must be satisfied.

Deployment Prerequisites

#	Prerequisite	Details	Notes
1	**Public Elastic IP and FQDN**	An Elastic IP (EIP) must be allocated and mapped to the SBC WAN interface. A publicly resolvable FQDN must be configured with a DNS A-record pointing to the EIP.	The FQDN is used by Microsoft Teams Direct Routing for SIP connectivity. The A-record must resolve to the EIP at all times, including after HA failover.
2	**Public TLS Certificate**	A TLS certificate issued by a trusted public Certificate Authority (CA) must be installed on the SBC. The certificate Common Name (CN) or Subject Alternative	Microsoft Teams Direct Routing mandates a trusted CA-issued certificate. Self-signed certificates are not supported. The certificate must include the full chain (root

			Name (SAN) must match the FQDN.	and intermediate CAs).
3	**AWS Networking Readiness**	Security Groups must be configured to permit SIP signalling and RTP media traffic. An Internet Gateway (IGW) or NAT Gateway must be in place to allow outbound and inbound connectivity as required.	Signalling ports (TCP/TLS 5061) and media ports (UDP 6000-49999, as defined by the configured media realm ranges in Section 14.3) must be explicitly allowed. Security Group rules must accommodate both Microsoft Teams media relay ranges and on-premises connectivity.
4	**NTP Server**	A reachable NTP source must be configured and accessible from the SBC.	NTP synchronisation is required for SBC operational stability, accurate logging, certificate validation, and call detail record timestamps. AWS provides an internal NTP service at 169.254.169.123, or an external NTP server may be used.
		The Active SBC instance must be deployed in	This determines the failover sequence. The Active instance processes all signalling and

5	**HA Pair Setup**	Availability Zone A (AZ-A) and the Standby SBC instance in Availability Zone B (AZ-B).	media traffic under normal operation. The Standby instance assumes the Active role upon detection of a failure condition.
6	**VIP and Subnet IPs**	A shared LAN Virtual IP (VIP) must be allocated alongside individual IP addresses for each instance across the HA, Management, Internal (LAN), and External (WAN) subnets.	The VIP is reused post-failover to maintain seamless connectivity for internal-facing services. During failover, the Elastic IP shifts from the Active to the Standby instance to maintain external reachability.
7	**Finalized Certified AudioCodes VE SBC Model**	The deployed SBC must be a certified AudioCodes Mediant VE SBC model that is compatible with both AWS and Microsoft Teams Direct Routing. The minimum required software version is **7.4.500**.	Refer to the AudioCodes and Microsoft compatibility matrices to confirm the selected model and firmware version are certified for Teams Direct Routing. Running a version below 7.4.500 is not supported for this deployment.

9.2 Downstream SBC Provisioning (Physical)

The Downstream SBC is a physical **AudioCodes Mediant 800C** SBC appliance deployed at remote branch sites. The Mediant 800C is a modular branch appliance designed for enterprise edge deployments, providing the

following capabilities:

- **PSTN Interfaces:** Optional dual or single E1/T1 PRI interface modules for legacy PSTN trunk connectivity.
- **Analogue Interfaces:** Optional FXS (Foreign Exchange Station) and FXO (Foreign Exchange Office) analogue modules for connecting analogue endpoints (telephones, fax machines) and analogue PSTN lines.
- **Network Interfaces:** Redundant Gigabit Ethernet (GE) network interfaces for LAN and WAN connectivity, supporting link-level resilience.
- **Power Supply:** Dual AC power supplies for hardware-level power redundancy.

The Mediant 800C supports full SBC and VoIP gateway functionality, enabling:

- **SIP-to-PSTN Interworking:** The appliance acts as a media gateway, converting SIP-based VoIP calls to TDM-based PSTN calls (and vice versa) over the connected E1/T1 PRI or analogue interfaces.
- **Secure Connection to Central Proxy SBC:** The Downstream SBC establishes a secure SIP trunk (TLS/SRTP) back to the centralised Proxy SBC in AWS, ensuring that all branch-originated calls are routed through the controlled, policy-enforced core infrastructure.

9.3 High Availability Configuration

9.3.1 Proxy SBC HA Provisioning

The Proxy SBC is deployed in a **Multi-AZ High Availability (HA)** configuration within a single AWS VPC. The design principles and requirements are as follows:

- **Multi-AZ HA Deployment:** Two SBC instances are deployed in an Active/Standby configuration across two different Availability Zones within the same AWS Region. This provides resilience against single-AZ failures.
- **Subnet Connectivity:** Each SBC instance connects to three distinct subnets:
  - **HA Subnet** – Used for heartbeat communication between the Active and Standby instances.
  - **Internal Subnet** – Used for both SBC administration (SSH, HTTPS, SNMP, QoE) and private/internal-facing SIP signalling and media traffic (e.g., towards on-premises infrastructure via AWS Direct Connect or Transit Gateway). Management (OAMP) and Internal (LAN) functions share a single ENI and subnet.
  - **External (WAN) Subnet** – Used for public-facing SIP signalling and media traffic (e.g., towards Microsoft Teams Direct Routing).
- **Unique IP Addresses:** Every SBC instance uses unique IP addresses for each of its network interfaces. No IP address is shared between the Active and Standby instances at the interface level.
- **Elastic IP Handling:** Elastic IPs are assigned to the Active instance's

WAN interface. During a failover event, the Elastic IP is automatically moved to the Standby instance, which then assumes the Active role. This ensures that the public-facing FQDN continues to resolve to the correct instance without DNS changes.

- **Virtual IP (VIP) Handling:** Virtual IPs are allocated from the **10.x.x.x** range within the VPC CIDR block. These VIPs are used for private VPC connectivity (LAN-side). During a switchover, the VPC routing table entries are updated to point to the newly Active instance, ensuring continued reachability of the VIP.
- **AWS EC2 API Interaction:** The Active instance handles Elastic IP and Virtual IP reassignment by interacting with AWS EC2 APIs over the HA subnet. Appropriate IAM roles and permissions must be configured to allow these API calls.
- **Stack Manager (MANDATORY):** The AudioCodes Stack Manager is a mandatory component. It deploys SBC stacks via AWS CloudFormation and handles initial HA deployment, topology updates, and Day 2 operations (software upgrades, stack maintenance). A single Stack Manager instance is deployed in the Australian region per environment and manages SBC HA stacks across all regions (including US) via cross-region AWS API calls. During failover, the SBCs themselves update VPC route tables by calling AWS EC2 APIs directly to redirect traffic to the newly Active instance. The Stack Manager must be deployed and operational before any SBC HA pair is provisioned.
- **HA Scope:** HA is supported within a **single VPC** across **two Availability Zones only**. Cross-VPC HA and cross-Region HA are **not supported**.

Subnet Requirements

Subnet	Purpose
HA Subnet (one per AZ)	Dedicated subnet for HA heartbeat and synchronisation traffic between the Active and Standby SBC instances. Each AZ has its own HA subnet.
Internal Subnet	Used for both SBC administration access (SSH, HTTPS, SNMP, QoE) and internal SIP signalling/media traffic. Management and LAN functions share this subnet.
Virtual IP Subnet	The Virtual IP must be allocated from a subnet that does not overlap with any existing subnets in the VPC or connected networks. The VIP subnet must be routable within the AWS VPC.

Connectivity

- **AWS Direct Connect** is assumed as the primary connectivity method between on-premises infrastructure and the AWS environment.
- **AWS Transit Gateway** is used for on-premises-to-AWS connectivity and inter-VPC connectivity, providing a centralised routing hub.

AWS Regions

Region Code	Location
ap-southeast-2	Australia (Sydney)
us-east-1	United States (N. Virginia)

Active/Standby Parameter Comparison

The following table summarises the parameter assignments for the Active and Standby SBC instances:

Parameter	Active SBC	Standby SBC
Availability Zone	e.g. ap-southeast-2a	e.g. ap-southeast-2b
Instance Role	Active	Standby
Elastic IP (WAN)	Associated	Moves here on failover
Virtual IP (LAN)	–	Same VIP (used after failover)
HA Subnet IP	X.X.X.X	X.X.X.X
Mgmt Subnet IP	X.X.X.X	X.X.X.X
Internal Subnet IP	X.X.X.X	X.X.X.X
External Subnet IP	X.X.X.X	X.X.X.X

> **Note:** The “X.X.X.X” placeholders must be replaced with the actual IP addresses allocated during the provisioning phase. Each instance must have unique IP addresses for all subnets. The Elastic IP and Virtual IP are shared resources that move between instances during failover.

9.3.2 Proxy SBC HA Configuration

The following HA parameters must be configured on each Proxy SBC instance to enable Active/Standby operation:

Parameter	Value	Description
		When the preferred Active instance recovers from a failure, it will **not** automatically resume

revertive-mode (Pre-empt mode)	Off	the Active role. Instead, the recovered instance remains in Standby until a manual switchover or subsequent failure event. This prevents unnecessary service disruption caused by repeated role changes.
priority	10	Determines the priority for assuming the Active role. A lower numeric value indicates a higher priority. The instance with the lowest priority value will be preferred as the Active instance during initial startup or contention scenarios.
remote-address	<IP Address>	The heartbeat/management IP address of the remote (peer) SBC instance used for HA synchronisation and health monitoring. This must be the HA subnet IP of the peer SBC.
redundant-unit-id-name	<Name>	The logical identifier of the remote (peer) SBC unit. Used to identify the partner SBC in the HA pair for configuration synchronisation and failover coordination.
unit-id-name	<Name>	The logical name of the local SBC unit. Used to uniquely identify this SBC instance within the HA pair.

9.3.3 Downstream SBC HA Provisioning

The Downstream SBC (AudioCodes Mediant 800C) supports High Availability through the deployment of two physical devices at each branch site. The HA provisioning model operates as follows:

- **Maintenance Interface:** The two Mediant 800C devices are connected to each other via a dedicated **Maintenance interface**. This interface is used exclusively for HA heartbeat communication, configuration synchronisation, and software version alignment between the two units.
- **Unique Maintenance IP:** Each device is assigned a unique IP address on the Maintenance interface to enable peer-to-peer HA communication.
- **HA Stand-alone Mode:** When only one device is powered on and operational, it operates in **HA Stand-alone** mode. In this state, the single device handles all signalling, media, and gateway functions independently.
- **HA Redundant State:** When the second device is connected and powered on, it enters the **HA Redundant** state. Upon entering this state, it automatically synchronises its configuration and software version with the Active device to ensure consistency.
- **Interface Behaviour:**
  - **Active Device:** All network interfaces (LAN, WAN, PSTN) are enabled and processing traffic.
  - **Redundant Device:** Only the Maintenance interface is active. All other interfaces remain in a disabled state to prevent traffic duplication or conflicts.
- **Failover Behaviour:** Upon detection of a failure on the Active device (e.g., hardware fault, software crash, interface failure), the Redundant device transitions to the Active state. All interfaces on the formerly Redundant device are enabled, and it assumes full responsibility for call processing and gateway functions.

9.3.4 Downstream SBC HA Configuration

The HA configuration parameters for the Downstream SBC (Mediant 800C) are identical to those defined for the Proxy SBC. The same parameter set applies:

Parameter	Value	Description
revertive-mode (Pre-empt mode)	Off	When the preferred Active instance recovers from a failure, it will **not** automatically resume the Active role. Instead, the recovered instance remains in Standby until a manual switchover or subsequent failure

		event. This prevents unnecessary service disruption caused by repeated role changes.
priority	10	Determines the priority for assuming the Active role. A lower numeric value indicates a higher priority. The instance with the lowest priority value will be preferred as the Active instance during initial startup or contention scenarios.
remote-address	<IP Address>	The heartbeat/management IP address of the remote (peer) SBC instance used for HA synchronisation and health monitoring. This must be the Maintenance interface IP of the peer device.
redundant-unit-id-name	<Name>	The logical identifier of the remote (peer) SBC unit. Used to identify the partner device in the HA pair for configuration synchronisation and failover coordination.
unit-id-name	<Name>	The logical name of the local SBC unit. Used to uniquely identify this device within the HA pair.

> **Note:** While the parameter names and values are consistent between the Proxy and Downstream SBC HA configurations, the underlying transport differs. The Proxy SBC uses the HA subnet in AWS for heartbeat communication, whereas the Downstream SBC uses the dedicated physical Maintenance interface.

9.4 Compute Requirements

The following table details the compute resource requirements for all components in the AudioCodes SBC deployment:

Application	Resource	Instance Type	Memory	Recommended Disk Space	Proc
VM for Mediant VE Proxy SBC (HA Pair)	AWS	m5n.large	8 GiB	20 GB	2 vCI
VM for Stack Manager	AWS	t3.medium	4 GiB	10 GB	2 vCI
OVOC	AWS	m5.4xlarge	64 GiB	AWS EBS: GP3 SSD 2 TB	16 v(
ARM Configurator	AWS	m4.xlarge	16 GiB	100 GB	4 vCI
ARM Router	AWS	m4.large	8 GiB	80 GB	2 vCI

> **Notes:**
>
> - The Mediant VE Proxy SBC instance type (m5n.large) is selected for its enhanced networking performance, which is critical for real-time voice media processing.
> - The Stack Manager (t3.medium) is a lightweight management component but is mandatory for initial HA deployment and Day 2 operations.
> - OVOC (One Voice Operations Center) requires substantial resources due to its role in centralised monitoring, analytics, and quality-of-experience reporting across all SBC instances.
> - ARM (AudioCodes Routing Manager) consists of two components: the Configurator (management and policy engine) and the Router (real-time call routing decisions). Both must be deployed for full ARM functionality.
> - All AWS instances should be deployed with appropriate EBS volume types and IOPS provisioning based on workload requirements. GP3 SSD is recommended as the baseline storage tier.

10. Security Controls

10.1 Administrative Access Controls

- Enforce TLS 1.2+ for all management (HTTPS, SSH) and SIP signalling, using certificates from approved CAs and disabling weak ciphers and protocols.
- Restrict management access (Web/SSH/SNMP) to dedicated admin subnets or jump hosts using firewall policies and SBC management-

access control lists.
- Disable or block all unused services and network ports (e.g., HTTP, TFTP, FTP, Telnet, unused SIP transport) and allow only explicitly required signalling/media ranges.
- Enable SBC VoIP firewall / classification protection features to rate limit malformed SIP, block scans, and protect from DoS/registration attacks.
- Change default Admin/User credentials and, where possible, rename default usernames; enforce password complexity and expiry using the SBC password policy parameters.
- Integrate management authentication with a centralised RADIUS AAA server (recommended: Cisco ISE) so roles are mapped via Vendor-Specific Attributes from directory groups (e.g., NOC Monitor, Voice Admin, Sec Admin). See Section 10.4: SBC Management Authentication for detailed configuration.
- Restrict Security Administrator role to a minimal number of users; use separate named accounts (no shared logins) and enable account lockout on failed login thresholds.
- Limit per-role Web page/CLI permissions so Monitor is strictly read only and day-to-day operations use Admin, reserving Security Admin for security and system-wide changes.

10.2 Role Hierarchy

AudioCodes SBCs implement a built-in role hierarchy for administrative access control:

Role	Description
Security Administrator	Full security and configuration control. Has access to all system functions including security settings, certificate management, and user administration.
Administrator	Configuration and operations access. Can modify SBC configuration, manage routing, and perform operational tasks but cannot modify security settings or user accounts.
Monitor	Read-only access. Can view configuration, status, and logs but cannot make any changes to the system.

10.3 Hardening and Default Account Management

- Immediately change all factory default accounts (Admin/Admin, User/User) and any vendor/maintenance accounts, document new credentials in the organisation’s password vault.
- Enable password complexity enforcement and minimum length;

configure password validity period and inactivity lockout to meet corporate policy.
- Disable or remove any unused local user accounts; if external auth (LDAP/RADIUS) is in place, keep only a single local break glass account stored offline.
- Disable legacy/weak management protocols (Telnet, HTTP, SNMPv1) and use only HTTPS, SSH, and SNMPv3 with strong credentials and, where supported, encryption.
- Keep SBC software at a vendor-supported release; apply security patches per change process and review AudioCodes security/hardening guidelines at each upgrade.

10.4 SBC Management Authentication

This section describes the authentication architecture for SBC management access. All SBCs — both Proxy (AWS) and Downstream (on-premises) — authenticate against a centralised RADIUS AAA server for management access (Web GUI, CLI/SSH).

> **Note on TACACS+:** AudioCodes Mediant SBC products (including Mediant VE, Mediant 800C, Mediant 4000, and Mediant 9000) do **not** support TACACS+ for management authentication. TACACS+ is only available on the AudioCodes Mediant MSBR (Multi-Service Business Router) product line. For SBC deployments, RADIUS is the supported centralised AAA protocol. RADIUS and LDAP cannot be used simultaneously for management login — one must be chosen.

> **SBC Management via OVOC (SSO):** While SBCs authenticate direct management access (SSH, Web GUI) via RADIUS (Cisco ISE), users can also manage SBCs through the OVOC portal. OVOC authenticates users via Microsoft Entra ID (OAuth 2.0 with MFA via Conditional Access), and once authenticated, OVOC connects to the SBC on the user's behalf using its management connection (HTTPS 443). This provides the best of both worlds: SBCs use RADIUS for direct access, while OVOC provides single sign-on (SSO) via Entra ID for centralised SBC management through the OVOC portal.

Authentication Architecture Overview

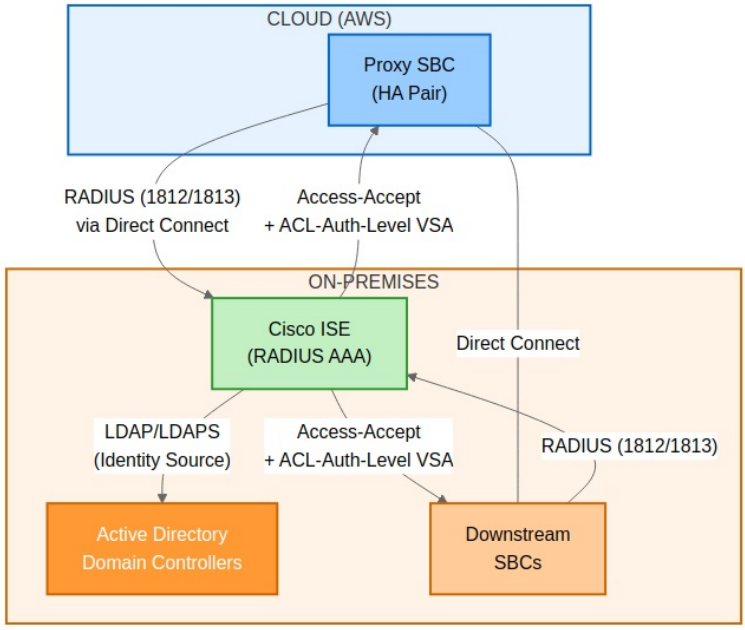


Diagram 5

Rationale for Unified RADIUS Authentication:

Factor	Decision
Consistency	Using the same AAA server and protocol (RADIUS) for all SBCs eliminates authentication model mismatch between Proxy and Downstream SBCs. A single set of RADIUS policies, user groups, and authorisation profiles apply uniformly across the entire SBC fleet.
Role-Based Access Control	RADIUS Vendor-Specific Attributes (VSAs) provide granular role mapping directly in the Access-Accept response, mapping users to Security Administrator, Administrator, or Monitor roles without requiring a separate authorisation lookup.
Centralised Audit Trail	RADIUS accounting (RFC 2866) provides a centralised record of all management access sessions across the SBC fleet, supporting compliance and security audit requirements.
Operational Simplicity	A single authentication model reduces operational complexity — one set of RADIUS policies, one shared secret management process, one authorisation profile pattern across all SBCs.

> **Note on MFA:** RADIUS-based authentication does not natively enforce multi-factor authentication on the SBC management interface. However, the RADIUS AAA server (e.g., Cisco ISE) can be configured to proxy authentication to an identity source that supports MFA (e.g., Microsoft Entra ID via ROPC, or Duo integration). OVOC and ARM continue to use Microsoft Entra ID authentication, which supports MFA via Conditional Access (see Section 6).

Recommended AAA Server: Cisco ISE

Cisco Identity Services Engine (ISE) is recommended as the centralised RADIUS AAA server for all SBC management authentication. Cisco ISE provides:

Capability	Details
RADIUS Server	Full RADIUS server with custom vendor dictionary support
Custom VSA Dictionary	Supports defining the AudioCodes vendor dictionary (Vendor ID 5003) with the `ACL-Auth-Level` attribute for role-based access
Identity Source Integration	Authenticates users against on-premises Active Directory, Microsoft Entra ID (via ROPC), or local ISE identity stores
Policy-Based Authorisation	Maps AD security groups to AudioCodes SBC roles (Security Administrator, Administrator, Monitor) via RADIUS authorisation profiles
Centralised Audit and Accounting	Full RADIUS accounting logs for all management access sessions, exportable to SIEM
Licensing	RADIUS-based device administration requires ISE **Essentials** licenses (one per concurrent RADIUS device admin session); no separate Device Administration license required for RADIUS

> **Note:** Cisco ISE is recommended based on its broad enterprise adoption, mature RADIUS VSA support, and integration with Microsoft Active Directory and Entra ID. Alternatives include Aruba ClearPass, Fortinet FortiAuthenticator, or FreeRADIUS, provided they support custom VSA dictionaries for AudioCodes (Vendor ID 5003).

AudioCodes RADIUS VSA Dictionary for Cisco ISE

Configure the following AudioCodes vendor dictionary in Cisco ISE under **Policy** > **Policy Elements** > **Dictionaries** > **System** > **Radius** > **Radius Vendors**:

Field	Value
Vendor Name	AudioCodes
IANA Vendor ID	5003
Attribute Name	ACL-Auth-Level
Attribute ID	35
Data Type	Integer

Access Level Values (for ISE Authorisation Profiles):

ISE Authorisation Profile	ACL-Auth-Level Value	SBC Role
`AC-SBC-SecurityAdmin`	200	Security Administrator — full access including security settings
`AC-SBC-Admin`	100	Administrator — configuration and operations access
`AC-SBC-Monitor`	50	Monitor — read-only access

Cisco ISE Policy Configuration

Map Active Directory security groups to AudioCodes SBC roles via ISE RADIUS authorisation policies:

AD Security Group	ISE Authorisation Profile	ACL-Auth-Level	SBC Role
`SBC-SecurityAdmin`	AC-SBC-SecurityAdmin	200	Security Administrator

`SBC-Admin`	AC-SBC-Admin	100	Administrator
`SBC-Monitor`	AC-SBC-Monitor	50	Monitor

All SBCs: RADIUS Configuration

All SBCs (Proxy and Downstream) authenticate management users via RADIUS. The SBC sends the user's credentials to the RADIUS server, which authenticates the user and returns an Access-Accept with the `ACL-Auth-Level` VSA to determine the user's role.

Prerequisites

- Cisco ISE (or equivalent RADIUS AAA server) deployed and reachable from all SBC management interfaces
- AudioCodes VSA dictionary configured on the RADIUS server (Vendor ID 5003, ACL-Auth-Level attribute 35)
- RADIUS shared secret configured on both the RADIUS server and each SBC
- Active Directory security groups created for role mapping
- Network connectivity from SBC management interfaces to RADIUS server (UDP 1812/1813 or legacy 1645/1646)

RADIUS Server Configuration

Configure RADIUS on each SBC via **Setup** > **IP Network** > **AAA Servers** > **RADIUS Servers**:

Parameter	Value
RADIUS Server 1 (Primary)	`<ISE PSN 1 IP Address>`
RADIUS Server 2 (Secondary)	`<ISE PSN 2 IP Address>`
Authentication Port	1812 (change from AudioCodes default of 1645)
Accounting Port	1813 (change from AudioCodes default of 1646)
Shared Secret	`<RADIUS Shared Secret>`
Timeout	5 seconds
Retransmission Attempts	3

> **Important:** AudioCodes defaults to legacy RADIUS ports 1645/1646. Change these to the standard ports 1812/1813 to align with Cisco ISE defaults and industry standards.

Enable RADIUS for Management Login

Configure via **Setup** > **Administration** > **Web & CLI** > **Authentication Server**:

Parameter	Value
Authentication Mode	RADIUS
Enable RADIUS for Management Login	Enabled
VSA Vendor ID	5003
VSA Access Level Attribute	35
Behavior upon Authentication Server Timeout	**Verify Access Locally** (enables break glass fallback)
RADIUS Local Cache Timeout	900 seconds (15 minutes)
RADIUS Local Cache Mode	Reset Timer Upon Access

Equivalent CLI configuration:

```
configure system > radius settings > enable
configure system > radius settings > enable-mgmt-login
configure system > radius settings > vsa-vendor-id 5003
configure system > radius settings > vsa-access-level 35
```

RADIUS Message Security

Enable RADIUS Message-Authenticator (Attribute 80) to protect against man-in-the-middle attacks on PAP-based RADIUS packets:

Parameter	Value	CLI
Require Message-Authenticator in Requests	Enabled	`rad-pap-req-msg-auth-tx`
Require Message-Authenticator in Responses	Enabled	`rad-req-msg-auth-rx`

Emergency Access: Break Glass Accounts

Local break glass accounts provide emergency access when the RADIUS AAA server is unavailable. For break glass account configuration and procedures, see Section 17: Break Glass Accounts.

When to use break glass accounts:

- RADIUS AAA server(s) unreachable (all SBCs)
- RADIUS misconfiguration preventing authentication
- Network connectivity issues (e.g., Direct Connect failure for Proxy SBC, WAN failure for Downstream SBC)
- Cisco ISE maintenance or outage

> **Important:** The “Behavior upon Authentication Server Timeout” parameter must be set to **“Verify Access Locally”** to enable local break glass fallback. When the RADIUS server is unreachable (5-second timeout), the SBC will fall back to the Local Users table where the break glass account is stored.

Network and Security Requirements

Firewall Rules

Ensure the following firewall rules are in place (see Section 16: Firewall Rules for complete rule sets):

Source	Destination	Port	Protocol	Purpose
All SBCs (Proxy + Downstream)	Cisco ISE PSNs	1812	UDP	RADIUS Authentication
All SBCs (Proxy + Downstream)	Cisco ISE PSNs	1813	UDP	RADIUS Accounting

RADIUS Network Path Security

Requirement	Details
Transport	RADIUS over UDP with shared secret (RADIUS does not use TLS natively; shared secret provides packet-level authentication via MD5 hash)
Message-Authenticator	Enable Attribute 80 (Message-Authenticator) on both SBC and ISE to protect PAP credentials
Network Segmentation	Management function shares the internal subnet (OAMP + LAN combined interface)
Firewall	Permit only SBC management IPs to ISE RADIUS ports (1812/1813 UDP)
Shared Secret Management	Use unique shared secrets per SBC or per site; store in the organisation's password vault

11. SBC Network Configuration

11.1 Physical Connectivity

SBC Configuration Concept in Teams Direct Routing

In the Teams Direct Routing Enterprise Model, the Proxy SBC connects Microsoft Teams Phone System to the PSTN and downstream SBC infrastructure. The SBC maintains separate network interfaces for internal connectivity (management, signalling, and media toward downstream SBCs, third-party PBX systems) and external (WAN) connectivity toward Microsoft Teams and PSTN providers. Management (OAMP) and Internal (LAN) functions are consolidated onto a single interface and subnet. The HA interface operates on a dedicated subnet for failover coordination.

Proxy SBC Virtual Ports

The following interfaces are enabled on the Proxy SBC:

Interface	Status	Purpose
GE_1	Enabled	Ethernet Group 1 (HA)
GE_2	Enabled	Ethernet Group 2 (OAMP + Internal)
GE_3	Enabled	Ethernet Group 3 (External)
GE_4	Disabled	Unused
GE_5	Enabled	Ethernet Group 1 (HA) - Redundant
GE_6	Enabled	Ethernet Group 2 (OAMP + Internal) - Redundant
GE_7	Enabled	Ethernet Group 3 (External) - Redundant
GE_8	Disabled	Unused

In AWS, AudioCodes physical ports (GE1-GE8) are virtualized and mapped to Elastic Network Interfaces (ENIs). Each ENI connects to a specific VPC subnet, acting like a virtual switch port, receiving its own private IP (with optional Elastic IP for public access). Since ports are grouped into Ethernet Groups for redundancy (GE1+GE5 for HA, GE2+GE6 for OAMP+Internal, GE3+GE7 for External), three ENIs are created - one per Ethernet Group - for logical separation and redundancy at cloud level. Management (OAMP) and Internal (LAN) functions share a single ENI and subnet, reducing the number of required network interfaces. Security Groups and routing tables control traffic flow.

Downstream SBC Physical Ports

The following interfaces are configured on the Downstream SBC:

Interface	Status
GE_1	Enabled
GE_2	Enabled
GE_3	Enabled
GE_4	Enabled

On Mediant 800, front-panel GE/FE ports are mapped to Physical Ports and grouped into Ethernet Groups for redundancy or single-port operation. Groups can be single-port or two-port for L2 redundancy (active/standby or active/active). All ports share the same MAC address - redundant ports should connect to different switches to avoid MAC flaps. For simple setups without VLAN tagging, configure upstream switch ports as access ports.

Downstream SBC with LBO Physical Ports

The physical port configuration for the Downstream SBC with LBO is identical to that described for the Downstream SBC Physical Ports above.

11.2 Logical Connectivity

Ethernet Groups

Ethernet Groups are used to define logical groupings of physical or virtual ports for the purposes of traffic management and routing. By grouping ports together, the SBC can provide link-level redundancy and separate traffic domains (management, signalling, media, HA) across distinct network segments.

Proxy SBC Ethernet Groups

Ethernet Group	Member Ports	Purpose
Group 1	GE_1, GE_5	HA
Group 2	GE_2, GE_6	OAMP + Internal (LAN)
Group 3	GE_3, GE_7	External (WAN)

Downstream SBC Ethernet Groups

Ethernet Group	Member Ports	Purpose
Group 1	GE_1	OAMP + Internal (LAN)
Group 2	GE_2	HA

Downstream SBC with LBO Ethernet Groups

The Ethernet Group configuration for the Downstream SBC with LBO is identical to that described for the Downstream SBC Ethernet Groups above.

11.3 Ethernet Device Configuration

The Ethernet Device table defines the logical network interfaces on the AudioCodes SBC, mapping each to an underlying physical port group and VLAN assignment. Proper separation of management, signalling/media, and high-availability traffic is critical for security, performance, and resilience.

Proxy SBC Ethernet Device Configuration

The Proxy SBC requires three logical Ethernet interfaces: an HA interface for high-availability synchronisation, a combined OAMP + Internal (LAN) interface for management and internal signalling/media, and an External (WAN/DMZ) interface for Microsoft Teams and SIP Providers.

Interface Name	Underlying Interface	VLAN ID
HA (High Availability)	Group_1	VLAN ID1
OAMP + Internal (LAN)	Group_2	VLAN ID1
External (WAN)	Group_3	VLAN ID1

Design Notes:

- Management (OAMP) and Internal (LAN) functions are consolidated onto a single Ethernet Device and ENI. This reduces the number of required network interfaces from four to three while maintaining logical separation through distinct IP interface application types (OAMP vs Media+Control) on the same underlying device.
- External/untrusted traffic destined for or originating from the DMZ (i.e., Microsoft Teams Direct Routing) must traverse a separate physical or logical interface (External/WAN) to enforce security zone boundaries.
- If the internal and external interfaces connect through **different physical switches**, they should be assigned to different physical ports on the SBC, each connected to the appropriate switch and VLAN.
- If the internal and external interfaces connect through the **same physical switch infrastructure**, VLAN segmentation must be used to enforce traffic isolation between the trusted (internal) and untrusted (external/DMZ) zones. Appropriate firewall or ACL policies must be applied at the switch or upstream firewall to control inter-VLAN traffic.
- The HA interface is dedicated to heartbeat and state synchronisation traffic between the active and standby SBC nodes and must not carry any signalling or media traffic.

Downstream SBC Ethernet Device Configuration

The Downstream SBC operates entirely within the trusted internal network and does not require a WAN-facing interface. It connects upstream to the Proxy SBC and downstream to registered endpoints on the LAN. Two logical interfaces are required: a combined OAMP + Internal (LAN) interface and an HA interface.

Interface Name	Underlying Interface	VLAN ID
OAMP + Internal (LAN)	Group_1	VLAN ID1
HA (High Availability)	Group_2	VLAN ID1

Design Notes:

- Management (OAMP) and Internal (LAN) functions are consolidated onto a single Ethernet Device, reducing the required interfaces from three to two.
- All signalling and media traffic between the Downstream SBC and the Proxy SBC traverses the combined OAMP + Internal (LAN) interface.
- The HA interface provides heartbeat and state synchronisation between the active and standby Downstream SBC nodes.

Downstream SBC with LBO Ethernet Device Configuration

The Downstream SBC with Local Breakout (LBO) shares the same Ethernet Device configuration as the standard Downstream SBC. The LBO functionality is achieved through additional SIP interface and routing configuration rather than additional physical or logical Ethernet interfaces.

Interface Name	Underlying Interface	VLAN ID
OAMP + Internal (LAN)	Group_1	VLAN ID1
HA (High Availability)	Group_2	VLAN ID1

Design Notes:

- The PSTN connectivity for Local Breakout is provided via the combined OAMP + Internal (LAN) interface using a dedicated SIP signalling interface and media realm, as detailed in subsequent sections.

11.4 IP Interfaces

The IP Interfaces table defines the Layer 3 addressing and application type for each logical interface on the SBC. Each IP interface is bound to a specific Ethernet Device and serves a designated application role (OAMP, Media + Control, or Maintenance/HA).

Proxy SBC IP Interfaces

The Proxy SBC requires three IP interfaces corresponding to the three Ethernet Devices.

Index	Application Types	Interface Mode	IP Address	Gateway	DNS	Interfac Name
0	OAMP + Media + Control	IPv4 Manual	X.X.X.X	X.X.X.X	X.X.X.X	OAMP + Internal (LAN)
	Media +	IPv4	X.X.X.X	X.X.X.X	As per	Externa

1	Control	Manual	(DMZ IP)	(Router IP)	ISP	(WAN)
2	Maintenance	IPv4 Manual	X.X.X.X	X.X.X.X	X.X.X.X	HA

Design Notes:

- **Index 0 (OAMP + Internal LAN):** Combined interface carrying both SBC management access (Web GUI, CLI, SNMP, syslog) and internal/trusted SIP signalling and RTP media traffic including Downstream SBCs, third-party PBX systems, and PSTN SIP trunk providers. This interface must be reachable from both network management systems and internal SIP endpoints.
- **Index 1 (External WAN - Media + Control):** Carries SIP signalling (TLS) and SRTP media for the Microsoft Teams Direct Routing connection. The IP address is the DMZ-facing address, the gateway is the DMZ router/firewall IP, and the DNS server is provided by the ISP or is the enterprise DNS server capable of resolving Microsoft 365 FQDNs.
- **Index 2 (HA - Maintenance):** Dedicated to HA heartbeat and state synchronisation. The Maintenance application type ensures this interface is used exclusively for HA purposes.

Downstream SBC IP Interfaces

The Downstream SBC requires two IP interfaces. No External (WAN) interface is configured as the Downstream SBC does not connect directly to Microsoft Teams or any external/DMZ network.

Index	Application Types	Interface Mode	IP Address	Gateway	DNS	Interfac Name
0	OAMP + Media + Control	IPv4 Manual	X.X.X.X	X.X.X.X	X.X.X.X	OAMP + Internal (LAN)
1	Maintenance	IPv4 Manual	X.X.X.X	X.X.X.X	X.X.X.X	HA

Design Notes:

- All SIP signalling, RTP media, and management traffic between the Downstream SBC and the Proxy SBC, as well as between the Downstream SBC and registered endpoints, is carried over the combined OAMP + Internal (LAN) interface (Index 0).
- The HA interface (Index 1) supports high-availability synchronisation between the active and standby nodes.

Downstream SBC with LBO IP Interfaces

The Downstream SBC with Local Breakout (LBO) uses the same IP Interface configuration as the standard Downstream SBC. The PSTN local breakout connectivity is achieved by configuring additional SIP signalling interfaces and media realms on the existing combined OAMP + Internal (LAN) IP interface, rather than by adding a separate IP interface.

Index	Application Types	Interface Mode	IP Address	Gateway	DNS	Interfac Name
0	OAMP + Media + Control	IPv4 Manual	X.X.X.X	X.X.X.X	X.X.X.X	OAMP + Internal (LAN)
1	Maintenance	IPv4 Manual	X.X.X.X	X.X.X.X	X.X.X.X	HA

12. TLS Certificate Configuration

This section details the TLS certificate configuration required for secure SIP connectivity between the Proxy SBC and Microsoft Teams Direct Routing. Microsoft Teams requires mutual TLS (MTLS) authentication on the SIP signalling path, which necessitates a trusted TLS certificate on the SBC signed by a publicly trusted Certificate Authority (CA).

> **Note:** TLS certificate configuration for Microsoft Teams Direct Routing is **only applicable to Proxy SBCs**. Downstream SBCs communicate with the Proxy SBC over the internal network using unencrypted SIP (UDP) and do not require TLS certificates for Teams connectivity.

12.1 TLS Context Configuration

A dedicated TLS Context named “Teams” is created on each Proxy SBC to hold the certificate and trust chain used for the Microsoft Teams Direct Routing SIP TLS connection.

Parameters

Parameter	Value
Index	1
Name	Teams
TLS Version	TLSv1.2
TLS Cipher Suite	Default
OCSP Server	Default
OCSP Default Response	Default
Mutual TLS (MTLS)	Default
Session Resumption	Default

Renegotiation	Default

Configuration Steps

1. **Create the TLS Context:**
   - Navigate to **Setup** > **IP Network** > **Security** > **TLS Contexts** on the SBC Web GUI.
   - Click **New** and configure the TLS Context with the parameters defined in the table above.
   - Set the **TLS Version** to **TLSv1.2** (minimum version required by Microsoft Teams).
   - All other parameters should remain at their default values unless specific security policies dictate otherwise.
   - Click **Apply**.
2. **Generate a Certificate Signing Request (CSR):**
   - Within the newly created “Teams” TLS Context, navigate to the **Certificate** section.
   - Click **Generate CSR** and fill in the required fields as detailed in Section 12.2.
3. **Deploy Certificates:**
   - After receiving the signed certificate from the CA, upload the server certificate, intermediate certificate(s), and trusted root certificate(s) as detailed in Sections 12.2 and 12.3.

12.2 Certificate Signing Request (CSR)

The CSR must be generated with the following field values to ensure compatibility with Microsoft Teams Direct Routing and the enterprise PKI infrastructure.

CSR Fields

CSR Field	Required Value
Common Name (CN)	sbc-proxy.domain.com
Subject Alternative Names (SANs)	Primary SBC FQDN + all required aliases (e.g., sbc-proxy-01.domain.com)
Organization (O)	Organization Name
Organizational Unit (OU)	As per organization
Country (C)	Country Code (e.g., AU, US)
State/Province (ST)	As per site location
Locality (L)	As per site location
Key Length	2048-bit RSA

Important: The Common Name (CN) and Subject Alternative Names (SANs) must exactly match the FQDN(s) configured in the Microsoft Teams Direct Routing voice route and PSTN gateway configuration in the Microsoft Teams Admin Center. Any mismatch will cause TLS negotiation failures and call routing failures.

Generation and Deployment Steps

1. **Generate the CSR** on the SBC within the "Teams" TLS Context by navigating to the Certificate section and clicking **Generate CSR**. Populate all fields as specified in the table above.
2. **Download the CSR** file from the SBC by clicking **Download CSR**.
3. **Submit the CSR** to the enterprise Certificate Authority (CA) or Public Key Infrastructure (PKI) team for signing. The CA must be a publicly trusted CA recognised by Microsoft (e.g., DigiCert, GlobalSign, Comodo/Sectigo, etc.). Internal/private CAs are not accepted by Microsoft Teams.
4. **Obtain the signed certificate** from the CA. Ensure you also obtain the full certificate chain including:
   - The signed server certificate (for the SBC FQDN)
   - All intermediate CA certificate(s)
   - The root CA certificate
5. **Upload the signed server certificate** to the SBC: Navigate to the "Teams" TLS Context > Certificate section > Click **Upload Certificate** and upload the signed server certificate file.
6. **Upload the intermediate CA certificate(s):** Navigate to the "Teams" TLS Context > Trusted Root Certificates section > Click **Upload** and upload each intermediate CA certificate.
7. **Upload the root CA certificate:** Upload the root CA certificate to the Trusted Root Certificates section as well.
8. **Verify the certificate chain:** After uploading, verify the certificate status shows as valid and the full chain is trusted by navigating to the TLS Context and reviewing the Certificate Information.

12.3 Deploying Trusted Root Certificates for MTLS

For mutual TLS (MTLS) authentication with Microsoft Teams, the SBC must trust the root CA certificates used by Microsoft to sign its SIP TLS certificates. Microsoft currently uses DigiCert as its certificate provider. The following root certificates must be downloaded and uploaded to the "Teams" TLS Context on each Proxy SBC.

Required Root and Intermediate Certificates

Certificate Name	Purpose
DigiCert Global Root G2	Root CA trust anchor for Microsoft SIP certs
DigiCert Global Root G3	Included as a precautionary measure; DigiCert Global Root G2

	is the confirmed active root CA for Teams SIP
Baltimore CyberTrust Root	Expired May 2025; retain only if required for backward compatibility with older configurations
DigiCert intermediate certificates (as needed)	Intermediate CA certificates in the chain

Deployment Steps

1. **Download** the DigiCert Global Root G2 and DigiCert Global Root G3 root certificates from the DigiCert website (https://www.digicert.com/kb/digicert-root-certificates.htm) in PEM or DER format.
2. **Download** any additional intermediate certificates published by Microsoft for Teams Direct Routing SIP TLS connectivity.
3. **Upload all DigiCert root and intermediate certificates** to the SBC:
   - Navigate to **Setup** > **IP Network** > **Security** > **TLS Contexts**.
   - Select the “Teams” TLS Context.
   - Go to the **Trusted Root Certificates** section.
   - Click **Upload** and upload each root and intermediate certificate file.
4. **Verify** that all uploaded certificates appear in the Trusted Root Certificates list and their validity dates are current.
5. **Test MTLS connectivity** by initiating a test call through Microsoft Teams Direct Routing and verifying that the TLS handshake completes successfully (check the SBC syslog for TLS handshake events).

> **Note:** Microsoft may update its certificate chain periodically. Monitor Microsoft 365 Message Center and Microsoft documentation for any certificate rotation announcements and update the SBC trusted root certificates accordingly.

---

13. Media Configuration

13.1 NTP Server Configuration

Network Time Protocol (NTP) synchronisation is essential for all SBCs to ensure accurate timestamps for call detail records (CDRs), syslog messages, TLS certificate validation, and HA synchronisation. All SBCs (Proxy, Downstream, and Downstream with LBO) must be configured to synchronise with the enterprise NTP server.

Parameter	Value
NTP Server Address	X.X.X.X
NTP Auth Mode	None

Configuration Path: Setup > Administration > Time & Date > NTP Server Address.

> **Note:** Ensure the NTP server is reachable from the SBC Management interface. If the NTP server resides on a different network segment, verify that appropriate routing and firewall rules are in place. A time drift of more than a few seconds can cause TLS certificate validation failures with Microsoft Teams and inconsistencies in CDR and syslog records.

13.2 Media Realm Configuration

Media Realms define the RTP port ranges and interface bindings for media (audio) traffic on the SBC. Each Media Realm is associated with a specific IP interface and allocates a pool of RTP ports for media sessions. Separate Media Realms are configured for internal and external traffic to ensure proper media routing and firewall rule alignment.

Proxy SBC Media Realm

The Proxy SBC requires three Media Realms to handle media for internal trunk traffic, Microsoft Teams (external) traffic, and PSTN carrier traffic respectively.

Index	Name	Interface	RTP Start Port	Number of Media Session Legs	RTP End Port (Calculate
0	Internal_Media_Realm	OAMP + Internal (LAN)	XXXX	1000	XXXX + 199
1	M365_Media_Realm	External (WAN)	XXXX	1000	XXXX + 199
2	PSTN_Media_Realm	External (WAN)	XXXX	500	XXXX + 999

Design Notes:

- **Internal_Media_Realm (Index 0):** Used for RTP media sessions between the Proxy SBC and internal entities such as Downstream SBCs, third-party PBX systems, and registered endpoints. Bound to the OAMP + Internal (LAN) interface.
- **M365_Media_Realm (Index 1):** Dedicated to RTP/SRTP media sessions between the Proxy SBC and Microsoft Teams (via the External/WAN/DMZ interface). This realm is bound to the External (WAN) interface so that media traffic egresses through the DMZ. Firewall rules must permit the configured RTP port range on this interface.

- **PSTN_Media_Realm (Index 2):** Used for RTP media sessions between the Proxy SBC and the PSTN SIP trunk provider. Bound to the External (WAN) interface, as SIP Provider connectivity uses the external/DMZ interface. A separate Media Realm is used (rather than sharing Internal_Media_Realm) to maintain distinct port ranges for troubleshooting and capacity management. Configured with 500 session legs (250 concurrent calls) to align with PSTN trunk capacity requirements.
- **Media Session Legs:** Internal, M365, and LMO Media Realms are configured with 1000 media session legs (approximately 500 concurrent calls each). The PSTN Media Realm is configured with 500 session legs (250 concurrent calls) to match the contracted PSTN trunk capacity. Each call consumes two legs (one for each direction). Adjust these values based on expected call volumes and SBC licensing.
- **RTP Port Range:** The RTP Start Port should be selected to avoid conflicts with other services.

> **Local Media Optimisation (LMO) — Scope and Requirements:** LMO applies to **local users only** — specifically, Teams endpoints (soft clients, IP phones, conference room devices) that reside on subnets directly reachable by the Proxy SBC. For LMO to function, all EUC (End User Computing) and voice subnets must be identified, documented, and configured as trusted network subnets in the Microsoft Teams admin centre. This enables Teams to identify when a user is on the corporate network and route media directly to the SBC (via the LMO Media Realm, UDP 30000-39999) rather than through the Microsoft Teams media relay infrastructure. The Proxy SBC itself is reachable from all locations — LMO eligibility is determined by the **endpoint's** network location, not the SBC's. Remote or external users will continue to use standard Teams media relay paths. **Action Required:** The voice/network engineering team must map out all EUC and voice subnets across all sites and configure these into the Teams admin centre Network Topology settings. Refer to Microsoft documentation for configuring Network Topology and Trusted IP settings.

Each Media Realm requires a contiguous range of ports equal to twice the number of media session legs (e.g., 1000 legs = 2000 ports, 500 legs = 1000 ports). Ensure that the port ranges for all Media Realms on the same interface do not overlap.

Downstream SBC Media Realm

The standard Downstream SBC requires only a single Media Realm for internal media traffic, as it does not connect to external networks or PSTN carriers directly.

Index	Name	Interface	RTP Start Port	Number of Media Session Legs

0	Internal_Media_Realm	OAMP + Internal (LAN)	XXXX	1000

Design Notes:

- All media between the Downstream SBC and the Proxy SBC, as well as between the Downstream SBC and registered endpoints, uses this single Internal Media Realm bound to the combined OAMP + Internal (LAN) interface.

Downstream SBC with LBO Media Realm

The Downstream SBC with Local Breakout requires two Media Realms: one for internal traffic toward the Proxy SBC and registered endpoints, and one for PSTN media traffic via the local SIP trunk.

Index	Name	Interface	RTP Start Port	Number of Media Session Legs
0	Internal_Media_Realm	OAMP + Internal (LAN)	XXXX	1000
1	PSTN_Media_Realm	OAMP + Internal (LAN)	XXXX	500

Design Notes:

- **Internal_Media_Realm (Index 0):** Handles media for calls between the Downstream SBC and the Proxy SBC, as well as registered endpoints. Bound to the combined OAMP + Internal (LAN) interface.
- **PSTN_Media_Realm (Index 1):** Handles media for calls that break out locally to the PSTN via the directly connected SIP trunk provider. A dedicated Media Realm ensures port range separation from internal media traffic. Configured with 500 session legs (250 concurrent calls) to align with PSTN trunk capacity.

13.3 Coder Groups

The default Coder Group (`AudioCodersGroups_0`) is used across all SBC roles and is configured with the following considerations:

Codec Considerations:

- **Preferred Codecs:** The Coder Group should include codecs in order of preference based on audio quality and bandwidth requirements. Typical codec priority order: G.711 A-law, G.711 Mu-law, G.729, Opus (if supported).

SDP Negotiation Notes:

- The SBC performs SDP offer/answer negotiation independently on each call leg. The Coder Group defines the codecs offered by the SBC on each leg, and the SBC selects the best matching codec based on the remote party's capabilities and the configured priority.
- If no common codec can be negotiated between the SBC and a remote party, the call attempt fails with a SIP 488 (Not Acceptable Here) or 606 (Not Acceptable) response. The Coder Group should include a broad enough set of codecs to ensure interoperability with all connected systems while maintaining acceptable audio quality.

Transcoding Notes:

- If the codecs negotiated on the two legs of a call differ (e.g., G.711 on the PSTN leg and Opus on the Teams leg), the SBC performs real-time transcoding between the two codecs. Transcoding consumes additional DSP resources and should be minimized where possible by aligning codec preferences across trunk endpoints.

> **Note:** The specific codec list and priority order within the Coder Group are configured during implementation based on the capabilities of each connected system and the bandwidth available on each network segment. Refer to the implementation worksheet for site-specific codec configurations.

---

14. SIP Signalling Configuration

14.1 SIP Signalling Interfaces

SIP Signalling Interfaces define the listening addresses, ports, and transport protocols for SIP signalling on each SBC. Each SIP Interface is bound to a specific IP interface and Media Realm, and controls how the SBC receives and sends SIP messages on that interface.

Proxy SBC SIP Interfaces

The Proxy SBC requires three SIP Interfaces: one for internal SIP trunk signalling, one for PSTN SIP trunk signalling, and one for Microsoft Teams Direct Routing (external TLS).

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepali
0	Internal (LAN)	Internal (LAN)	SBC	XXXX	0	0	Disable
1	PSTN	Internal (LAN)	SBC	XXXX	0	0	Disable
2	External (WAN)	External (WAN)	SBC	0	0	5061	Enable

Design Notes:

- **Index 0 – Internal (LAN):** Listens on a UDP port for SIP signalling from Downstream SBCs, third-party PBX systems, and other internal trunk endpoints. TCP and TLS are disabled (port 0) as internal signalling uses UDP. Classification Failure Response is set to 500 (Server Internal Error) to reject unclassified calls gracefully.
- **Index 1 – PSTN:** Listens on a separate UDP port on the Internal (LAN) interface for SIP signalling from the PSTN SIP trunk provider. Using a different port from the Internal (LAN) SIP Interface allows the SBC to distinguish PSTN traffic from other internal trunk traffic. Classification Failure Response is set to 500.
- **Index 2 – External (WAN):** Listens on TLS port 5061 for SIP signalling from Microsoft Teams Direct Routing. UDP and TCP are disabled (port 0) as Microsoft Teams requires TLS exclusively. TCP Keepalive is **enabled** to maintain persistent TCP/TLS connections with Microsoft Teams. Classification Failure Response is set to **0** (no response) as a Denial-of-Service (DoS) mitigation measure – unclassified SIP messages from the external interface are silently dropped rather than responded to, preventing reconnaissance and amplification attacks. The TLS Context is set to “Teams” to use the certificate configured in Section 12.

Downstream SBC SIP Interfaces

The Downstream SBC requires a single SIP Interface for internal signalling with the Proxy SBC and registered endpoints.

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepaliv
0	Internal (LAN)	Internal (LAN)	SBC	XXXX	0	0	Disable

Downstream SBC with LBO SIP Interfaces

The Downstream SBC with LBO requires two SIP Interfaces: one for internal signalling (toward the Proxy SBC and registered endpoints) and one for PSTN signalling (toward the local SIP trunk provider).

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepaliv
0	Internal (LAN)	Internal (LAN)	SBC	XXXX	0	0	Disable
1	PSTN	Internal (LAN)	SBC	XXXX	0	0	Disable

(LAN)

14.2 Proxy Sets

Proxy Sets define logical groupings of destination SIP entities (proxy servers, SBCs, PBXs, SIP trunk providers) and their associated connectivity parameters including keep-alive mechanisms, hot-swap failover, and load balancing behavior. Each Proxy Set is associated with a SIP Interface and optionally a TLS Context.

Proxy SBC Proxy Sets

The Proxy SBC maintains Proxy Sets for all trunk destinations in the architecture.

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap	P Bal M
1	Teams Direct Routing	External (WAN)	Teams	Using-OPTIONS	Enable	Ra We
2	Prod_Downstream SBC	Internal (LAN)	–	Using-OPTIONS	Enable	–
3	3rd Party PBX & Radio Systems	Internal (LAN)	–	Using-OPTIONS	Enable	–
4	SIP Provider AU	External (WAN)	–	Using-OPTIONS	Enable	–
5	SIP Provider US	External (WAN)	–	Using-OPTIONS	Enable	–
6	Proxy-to-Proxy	Internal (LAN)	–	Using-OPTIONS	Enable	–

Design Notes:

- **Teams Direct Routing (Index 1):** Uses the External (WAN) SIP Interface and the “Teams” TLS Context for secure SIP connectivity to Microsoft Teams. Load Balancing Method is set to **Random-Weights** to distribute calls across the Microsoft Teams SIP proxies. Proxy Hot Swap is enabled for automatic failover.
- **Prod_Downstream SBC (Index 2):** Routes signalling to the downstream SBC cluster via the Internal (LAN) interface. SIP OPTIONS-based keep-alive monitors the health of each downstream SBC. Hot Swap is enabled for failover between downstream SBC nodes.
- **3rd Party PBX & Radio Systems (Index 3):** Proxy Set for legacy PBX systems and radio/emergency communication systems.
- **SIP Provider AU (Index 4):** Proxy Set for the Australian SIP trunk provider connected to the Australian Proxy SBC. Provides regional PSTN breakout for Australian traffic via the local carrier.

- **SIP Provider US (Index 5):** Proxy Set for the US SIP trunk provider connected to the US Proxy SBC. Provides regional PSTN breakout for US traffic via the local carrier.
- **Proxy-to-Proxy (Index 6):** Enables signalling between the two Proxy SBCs (e.g., AU Proxy to US Proxy) for inter-region call routing and failover.
- **Proxy Keep-Alive (Using-OPTIONS):** All Proxy Sets use SIP OPTIONS messages as keep-alive probes to continuously monitor the availability of each target entity. If an entity fails to respond to OPTIONS, the SBC marks it as unavailable and triggers Hot Swap failover.

Each Proxy Set contains one or more **Proxy Address entries** (not shown in this table) that define the specific IP addresses or FQDNs, ports, and priority/weight of each target entity within the Proxy Set. These are configured in the Proxy Address table associated with each Proxy Set.

Downstream SBC Proxy Sets

The Downstream SBC requires a single Proxy Set pointing to the upstream Proxy SBC.

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap	Proxy Load Balancing Method
1	Proxy_SBC	Internal (LAN)	–	Using-OPTIONS	Enable	–

Downstream SBC with LBO Proxy Sets

The Downstream SBC with LBO requires two Proxy Sets: one for the upstream Proxy SBC and one for the local PSTN SIP trunk provider.

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap	Proxy Load Balancing Method
1	PSTN (Telco)	Internal (LAN)	–	Using-OPTIONS	Enable	–
2	Proxy_SBC	Internal (LAN)	–	Using-OPTIONS	Enable	–

15. Routing Configuration

15.1 IP Profiles

IP Profiles define per-trunk signalling and media behavior, including codec group assignment, media security settings, and handling of SIP REFER, 3xx redirect, and REPLACES methods. Each IP Profile is associated with one or more IP Groups to apply the profile's settings to all calls on that trunk.

Proxy SBC IP Profiles

The Proxy SBC uses multiple IP Profiles to apply trunk-specific signalling and media behavior.

Profile Name	Coders Group	Media Security Behavior
Proxy_Downstream_Internal_Profile	AudioCodersGroups_0	Not Secured
Teams Direct Routing Profile	AudioCodersGroups_0	Secured
PSTN_Profile	AudioCodersGroups_0	Not Secured
3rd Party PBX Profile	AudioCodersGroups_0	Not Secured
Registered Endpoints Profile	AudioCodersGroups_0	Not Secured

Design Notes:

- **Proxy_Downstream_Internal_Profile:** Applied to internal trunks between the Proxy SBC and Downstream SBCs, as well as the Proxy-to-Proxy trunk. Media security is set to "Not Secured" as internal traffic does not require SRTP encryption.
- **Teams Direct Routing Profile:** Applied to the Microsoft Teams Direct Routing trunk. Media Security Behavior is set to **Secured**, which forces the SBC to use SRTP for all media sessions on this trunk. Microsoft Teams requires SRTP for media encryption. The SBC terminates SRTP on the Teams side and bridges to RTP on the internal side (or vice versa).
- **PSTN_Profile:** Applied to PSTN SIP trunk connections. Media is "Not Secured" (standard RTP) as most PSTN carriers do not support SRTP.
- **3rd Party PBX Profile:** Applied to legacy PBX and radio system trunks. Media is "Not Secured".
- **Registered Endpoints Profile:** Applied to locally registered SIP endpoints. Media is "Not Secured".
- **Remote REFER/3XX/REPLACES – Handle Locally:** All IP Profiles are configured to handle REFER, 3xx redirect, and REPLACES messages locally on the SBC. This means the SBC intercepts these messages and performs the call transfer, redirect, or replacement on behalf of the endpoints, rather than forwarding the messages transparently. This ensures consistent behavior regardless of endpoint capabilities and provides the SBC with full visibility and control over call transfers and

redirects.

Downstream SBC IP Profiles

The Downstream SBC uses two IP Profiles: one for the upstream trunk to the Proxy SBC and one for registered endpoints.

Profile Name	Coders Group	Media Security Behavior	Remote REFER Behavior
Proxy_SBC_Internal_Profile	AudioCodersGroups_0	Not Secured	Handle Locally
Registered Endpoints Profile	AudioCodersGroups_0	Not Secured	Handle Locally

Downstream SBC with LBO IP Profiles

The Downstream SBC with LBO requires three IP Profiles: one for the upstream Proxy SBC trunk, one for the local PSTN trunk, and one for registered endpoints.

Profile Name	Coders Group	Media Security Behavior	Remote REFER Behavior
PSTN_Profile	AudioCodersGroups_0	Not Secured	Handle Locally
Proxy_SBC_Internal_Profile	AudioCodersGroups_0	Not Secured	Handle Locally
Registered Endpoints Profile	AudioCodersGroups_0	Not Secured	Handle Locally

15.2 IP Groups

IP Groups are the primary logical entity in the AudioCodes SBC architecture that ties together a Proxy Set, Media Realm, IP Profile, and TLS Context into a cohesive trunk definition. Each IP Group represents a specific trunk or endpoint group and is referenced by routing rules, classification rules, and message manipulation rules.

Proxy SBC IP Groups

The Proxy SBC maintains IP Groups for all trunk destinations in the architecture.

IP-Group Name	Proxy Set Name	Media Realm Name	IP P
Teams			

Direct Routing Trunk	Teams Direct Routing	M365_Media_Realm	Teams Direct I
Downstream SBC Trunk	Prod_Downstream SBC	Internal_Media_Realm	Proxy_Downst
3rd Party PBX Trunk	3rd Party PBX & Radio Systems	Internal_Media_Realm	Proxy_Downst
SIP Provider AU Trunk	SIP Provider AU	PSTN_Media_Realm	PSTN_Profile
SIP Provider US Trunk	SIP Provider US	PSTN_Media_Realm	PSTN_Profile
User	Registered Endpoints	Internal_Media_Realm	Registered End
Proxy-to-Proxy Trunk	Proxy-to-Proxy	Internal_Media_Realm	Proxy_Downst

Design Notes:

- **Teams Direct Routing Trunk:** Uses the M365_Media_Realm (bound to the External/WAN interface), the Teams Direct Routing IP Profile (with SRTP enabled), and the “Teams” TLS Context for secure SIP signalling.
- **Downstream SBC Trunk:** Connects the Proxy SBC to the downstream SBC cluster using internal media and signalling.
- **3rd Party PBX Trunk:** Aggregates connectivity to legacy PBX and radio/emergency systems.
- **SIP Provider AU Trunk:** Uses the dedicated PSTN_Media_Realm and PSTN_Profile for Australian regional PSTN breakout. Configured on the Australian Proxy SBC to route outbound calls to the Australian carrier.
- **SIP Provider US Trunk:** Uses the dedicated PSTN_Media_Realm and PSTN_Profile for US regional PSTN breakout. Configured on the US Proxy SBC to route outbound calls to the US carrier.
- **User:** Represents locally registered SIP endpoints on the Proxy SBC.
- **Proxy-to-Proxy Trunk:** Enables inter-region signalling between the AU and US Proxy SBCs.
- **TLS Context:** Only the Teams Direct Routing Trunk uses a dedicated TLS Context (“Teams”). All other trunks use the “Default” TLS Context (which may have no certificate configured, as they use unencrypted SIP).

Downstream SBC IP Groups

The Downstream SBC maintains two IP Groups: one for the upstream Proxy SBC trunk and one for registered endpoints.

IP-Group Name	Proxy Set Name	Media Realm Name	IP Profile Name
Proxy SBC Trunk	Proxy_SBC	Internal_Media_Realm	Proxy_SBC_Internal_Prof

Registered Endpoints	–	Internal_Media_Realm	Registered Endpoints Profile

Downstream SBC with LBO IP Groups

The Downstream SBC with LBO adds a PSTN (Telco) Trunk IP Group to the standard Downstream SBC configuration.

IP-Group Name	Proxy Set Name	Media Realm Name	IP Profile Name
Proxy SBC Trunk	Proxy_SBC	Internal_Media_Realm	Proxy_SBC_Internal_Prof
Registered Endpoints	–	Internal_Media_Realm	Registered Endpoints Profile
PSTN (Telco) Trunk	PSTN (Telco)	PSTN_Media_Realm	PSTN_Profile

15.3 Message Manipulation Rules

Message Manipulation Rules enable the SBC to modify SIP message headers during call processing. This is required to ensure proper interoperability between Microsoft Teams and other SIP entities, particularly for call transfer (REFER) and redirect (3xx) scenarios where SIP header values must be adjusted.

Manipulation Sets

Manipulation Set Name	Purpose
REFER_Modify PAI	Modifies the P-Asserted-Identity (PAI) header in SIP REFER messages to ensure correct caller identity is presented to the transfer target.
3xx_Modify PAI	Modifies the P-Asserted-Identity (PAI) header in SIP 3xx redirect responses to ensure correct caller identity is maintained during call redirects.

Rule Assignment Notes

- Message Manipulation Rules are assigned to specific IP Groups for inbound and/or outbound message processing.
- The **REFER_Modify PAI** rule set is assigned to the relevant IP Groups (e.g., Teams Direct Routing Trunk, PSTN Trunk) on the **outbound** message manipulation to ensure that REFER messages sent to these trunks contain the correct PAI header.
- The **3xx_Modify PAI** rule set is assigned to the relevant IP Groups on

the **inbound** message manipulation to intercept and modify 3xx responses received from these trunks.
- The specific header manipulation logic (e.g., copying the Referred-By header value to the PAI header, or extracting the redirect target from the Contact header) is defined within each Manipulation Set using the SBC's Message Manipulation scripting syntax.

> **Note:** The detailed Message Manipulation Rule syntax and logic are configured during implementation and may vary based on the specific interoperability requirements discovered during integration testing. The rules documented here represent the baseline configuration; additional rules may be added as needed.

15.4 Classification Rules

Classification Rules allow the SBC to identify and classify incoming SIP messages from external (untrusted) sources and assign them to the correct IP Group. This is critical for security and proper call routing on interfaces that do not have implicit trust (i.e., the External/WAN interface).

> **Note:** Classification Rules are **applicable to Microsoft Teams connectivity from Proxy SBCs only**. Internal SIP interfaces use Proxy Set-based classification (where the source IP is matched against the Proxy Set addresses) and do not require explicit Classification Rules.

Classification Rules for Teams IP Ranges

The following Classification Rules are configured on the Proxy SBC to identify and authorize SIP traffic from Microsoft Teams. Microsoft Teams Direct Routing uses a range of source IP address subnets; all must be classified to the Teams Direct Routing Trunk IP Group.

Index	Name	Source SIP Interface	Source IP Address	Destination Host	Action Type	Sou I Gro
0	Teams_52_112	Teams	52.112..	XXXX	Allow	Tea Dire Rou Tru
1	Teams_52_113	Teams	52.113..	XXXX	Allow	Tea Dire Rou Tru
2	Teams_52_114	Teams	52.114..	XXXX	Allow	Tea Dire Rou Tru
						Tea Dire

3	Teams_52_115	Teams	52.115..	XXXX	Allow	Rou Tru
4	Teams_52_122	Teams	52.122..	XXXX	Allow	Tea Dire Rou Tru
5	Teams_52_123	Teams	52.123..	XXXX	Allow	Tea Dire Rou Tru

Design Notes

- **Source SIP Interface:** All rules reference the "Teams" SIP Interface (External/WAN), meaning they only apply to SIP messages arriving on the external TLS interface.
- **Source IP Address:** The IP address ranges correspond to Microsoft's published IP ranges for Teams media and signalling. These ranges include:
  - 52.112.0.0/14 (covers 52.112.. through 52.115..)
  - 52.122.0.0/15 (covers 52.122.. and 52.123..)
- **Destination Host:** Set to the SBC's external FQDN or the placeholder XXXX to be populated during implementation.
- **Action Type:** "Allow" permits the classified traffic and assigns it to the specified Source IP Group.
- **Source IP Group:** All classified Microsoft Teams traffic is assigned to the "Teams Direct Routing Trunk" IP Group, which applies the Teams-specific IP Profile (with SRTP), Media Realm (External/WAN), and TLS Context.

> **Important:** Microsoft may update its IP address ranges. Always refer to the latest Microsoft 365 URLs and IP address ranges documentation (https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges) and update the Classification Rules accordingly. Consider using broader subnet-based rules rather than individual /16 entries where Microsoft's published ranges permit, to reduce the number of rules and simplify maintenance.

Any SIP message arriving on the External (WAN) SIP Interface that does not match a Classification Rule is rejected based on the Classification Failure Response Type configured on the SIP Interface (set to 0/silent drop for DoS mitigation, as defined in Section 14.1).

15.5 IP-to-IP Call Routing Rules

IP-to-IP Call Routing Rules define the call routing logic on the SBC, determining how incoming calls on one IP Group are routed to the appropriate destination IP Group based on configurable matching criteria such as source IP Group, called number (destination URI), calling number (source URI), and other SIP header fields.

The AudioCodes SBC uses an **Alternative Routing Method (ARM)** that supports sophisticated routing logic including:

- **Primary and alternative route selection** with automatic failover to alternative routes on call failure.
- **Dial plan normalization** to transform called and calling numbers between different numbering formats (e.g., E.164 to local, local to E.164) using Calling and Called Number Manipulation rules.
- **Translation rules** for modifying SIP headers, URIs, and other call attributes during routing.

Supported Routing Scenarios

The ARM routing logic on each SBC role supports the following connectivity scenarios:

Source Entity	Destination Entity	SBC Role
Microsoft Teams	Regional SIP Provider (AU/US)	Proxy SBC
Microsoft Teams	Downstream SBC / Registered Endpoints	Proxy SBC
Microsoft Teams	3rd Party PBX / Radio Systems	Proxy SBC
SIP Provider AU	Microsoft Teams	AU Proxy SBC
SIP Provider US	Microsoft Teams	US Proxy SBC
SIP Provider (AU/US)	Downstream SBC / Registered Endpoints	Proxy SBC
Downstream SBC	Microsoft Teams (via Proxy)	Proxy SBC
Downstream SBC	Regional SIP Provider (via Proxy)	Proxy SBC
3rd Party PBX / Radio Systems	Microsoft Teams	Proxy SBC
3rd Party PBX / Radio Systems	Regional SIP Provider (AU/US)	Proxy SBC
Proxy SBC (AU)	Proxy SBC (US) and vice versa	Proxy SBC
Registered Endpoints	Proxy SBC (upstream)	Downstream
Proxy SBC	Registered Endpoints	Downstream
		Downstream

Registered Endpoints	PSTN (local breakout)	LBO
PSTN (local)	Registered Endpoints	Downstream LBO
Registered Endpoints	Proxy SBC (upstream)	Downstream LBO
Proxy SBC	Registered Endpoints	Downstream LBO

Dial Plan Normalization Notes

- **Calling Number Manipulation:** Applied to outbound calls to transform the calling party number (ANI/CLI) to the format expected by the destination entity (e.g., E.164 format for PSTN, SIP URI format for Teams).
- **Called Number Manipulation:** Applied to transform the called party number (DNIS) to the format expected by the destination entity (e.g., stripping or adding country codes, translating extension numbers to DDI numbers).
- **Translation Rules:** Additional SIP header and URI manipulations applied during routing to ensure interoperability between different SIP implementations (e.g., modifying the Request-URI host part, adjusting SIP headers for specific endpoint requirements).

Routing Logic on ARM:

The routing rules are evaluated in index order (top-down) and the first matching rule is applied. Each rule specifies:

1. **Match Criteria:** Source IP Group, destination number pattern (prefix/regex), source number pattern, SIP header values.
2. **Route Action:** Destination IP Group, call attributes (e.g., alternative route index, cost group).
3. **Manipulation:** Calling/called number manipulation set references for number translation during routing.
4. **Alternative Routes:** Index references to alternative routing rules that are invoked if the primary route fails (e.g., SIP 4xx/5xx response or timeout).

> **Note:** The complete IP-to-IP Call Routing table with all rules, number patterns, manipulation references, and alternative route indices is defined in the site-specific implementation worksheet and is configured during the SBC deployment phase. The routing logic is validated during integration testing with all connected systems (Microsoft Teams, regional SIP providers, PBX, and radio systems) to ensure correct call routing, number presentation, and failover behavior. Each regional Proxy SBC (AU/US) routes PSTN-bound calls to its respective regional SIP provider for local carrier breakout.

16. Firewall Rules

This section details all firewall rules required for the AudioCodes SBC solution components. Rules are organized by device role and integration point.

16.1 Proxy SBC Firewall Rules

Device Administration via OVOC

Service	Direction	Protocol	Source	Src Port	Destination
SNMP (Trap)	SBC → OVOC	UDP	SBC Management Interface IP	161	OVOC IP
SNMP (Trap)	OVOC → SBC	UDP	OVOC IP	1161	SBC Management Interface IP
SNMP (Keep-Alive)	SBC → OVOC	UDP	SBC Management Interface IP	161	OVOC IP
QoE Reporting	SBC → OVOC	TCP (TLS)	SBC Management Interface IP	Any	OVOC IP
Device Management	OVOC → SBC	TCP	OVOC IP	Any	SBC Management Interface IP
Device Management	SBC → OVOC	TCP	SBC Management Interface IP	Any	OVOC IP
NTP	SBC → OVOC	UDP/TCP	SBC Management Interface IP	Any	OVOC IP

Management via Jump Server

Service	Direction	Protocol	Source	Src Port	Destination	D Po
SSH	Jump server → SBC	TCP	Jump server IP / Management Subnet	Any	SBC Management Interface IP	22
HTTPS	Jump server → SBC	TCP	Jump server IP / Management Subnet	Any	SBC Management Interface IP	44

RADIUS Auth	SBC → RADIUS AAA	UDP	SBC Management Interface IP	Any	Cisco ISE PSN	18
RADIUS Acct	SBC → RADIUS AAA	UDP	SBC Management Interface IP	Any	Cisco ISE PSN	18
Debug Recording	SBC → Jump server	UDP	SBC Management Interface IP	Any	Jump server IP / Management Subnet	92
Syslog	SBC → Jump server	UDP	SBC Management Interface IP	Any	Jump server IP / Management Subnet	51
CDR	SBC → CDR server	TCP	SBC Management Interface IP	Any	CDR server	22

Functional

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port
NTP	SBC → NTP Server	UDP/TCP	SBC Management Interface IP	Any	NTP server	123
DNS	SBC → DNS Server	UDP/TCP	SBC Management Interface IP	Any	DNS server	53

Teams Direct Routing

Service	Direction	Protocol	Source	Src Port	Destination	P
Teams Direct Routing	Teams → SBC	TCP	52.112.0.0/14, 52.122.0.0/15	1024-65535	SBC Public IP Address	50
	SBC → Teams	TCP	SBC Public IP Address	1024-65535	52.112.0.0/14, 52.122.0.0/15	50
	Teams → SBC	UDP	52.112.0.0/14, 52.120.0.0/14	3478-3481, 49152-53247	SBC Public IP Address	20 21
	SBC → Teams	UDP	SBC Public IP Address	20000-21999	52.112.0.0/14, 52.120.0.0/14	34 34 49

Integration with SIP Provider AU (Australian Proxy SBC)

Service	Direction	Protocol	Source	Src Port	Destination	Ds Por
Integration with SIP Provider AU	SBC → SIP Provider AU	UDP/TCP	AU Proxy SBC External IP Address	Any	SIP Provider AU IP/s	5060 5061
	SIP Provider AU → SBC	UDP/TCP	SIP Provider AU IP/s	Any	AU Proxy SBC External IP Address	5060 5061
	SBC → SIP Provider AU	UDP	AU Proxy SBC External IP Address	40000-41999	SIP Provider AU IP/s	Any
	SIP Provider AU → SBC	UDP	SIP Provider AU IP/s	Any	AU Proxy SBC External IP Address	4000 4199

> **Note:** Telstra SIP is a REGISTER-type trunk (SBC initiates registration). However, media and SIP signalling flows are **bidirectional** from a network and firewall perspective. Restricting to outbound-only may cause issues with early media, inbound call setup, and call teardown. Firewall rules must permit both directions.

Integration with SIP Provider US (US Proxy SBC)

Service	Direction	Protocol	Source	Src Port	Destination	Ds Por
Integration with SIP Provider US	SBC → SIP Provider US	UDP/TCP	US Proxy SBC External IP Address	Any	SIP Provider US IP/s	5060 5061
	SIP Provider US → SBC	UDP/TCP	SIP Provider US IP/s	Any	US Proxy SBC External IP Address	5060 5061

	SBC → SIP Provider US	UDP	US Proxy SBC External IP Address	40000-41999	SIP Provider US IP/s	Any
	SIP Provider US → SBC	UDP	SIP Provider US IP/s	Any	US Proxy SBC External IP Address	4000 4199

> **Note:** The US carrier may support REGISTER-type SIP trunk configuration. Verify with the carrier whether SIP signalling is SBC-initiated (REGISTER) or carrier-initiated, and whether inbound SIP listening ports (UDP 5060, TCP 5061) are required. Regardless, media flows are bidirectional from a firewall perspective and both directions must be permitted.

Integration with Downstream Devices (SBC, Media Pack, Cisco)

Service	Direction	Protocol	Source	Src Port	Destination
Integration with Downstream Devices	Sites → SBC	TCP/UDP	Downstream Device IPs	Any	SBC Internal IP Address
	SBC → Sites	TCP/UDP	SBC Internal IP Address	Any	Downstream Device IPs
	Sites → SBC	UDP	Downstream Device IPs	Any	SBC Internal IP Address
	SBC → Sites	UDP	SBC Internal IP Address	10000-19999	Downstream Device IPs

> **TLS Between AudioCodes Devices:** TCP 5061 (TLS) is recommended for SIP trunks between AudioCodes devices (Proxy SBC, Downstream SBCs, Media Packs) to encrypt signalling data in transit. Configure a TLS Context on both the Proxy SBC and downstream devices for inter-device SIP connectivity.

Integration with Other Proxy SBC

Service	Direction	Protocol	Source	Src Port	Destination	Dst Por
Integration with Other Proxy SBC	Sites → SBC	TCP	Other Proxy SBC IPs	Any	SBC Internal IP Address	5060 5061

	SBC → Sites	TCP	SBC Internal IP Address	Any	Other Proxy SBC IPs	5060 5061
	Sites → SBC	UDP	Other Proxy SBC IPs	Any	SBC Internal IP Address	1000 1999
	SBC → Sites	UDP	SBC Internal IP Address	10000-19999	Other Proxy SBC IPs	Any

ARM Integration

Service	Direction	Protocol	Source	Src Port	Destination	D P
ARM Integration	ARM → SBC	TCP	ARM Configurator IP, ARM Router IP	Any	SBC IP	4
	SBC → ARM	TCP	SBC IP	Any	ARM Configurator IP, ARM Router IP	4

Teams - LMO Flows

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port
Teams - LMO Flows	Endpoints → Proxy SBC	UDP	Endpoints (Teams soft clients, IP Phones)	3478-3481, 49152-53247	SBC IP	30000 39999
	Proxy SBC → Endpoints	UDP	SBC IP	30000-39999	Endpoints (Teams soft clients, IP Phones)	3478-3481, 49152 53247

Integration with SIP Generic Endpoints

Service	Direction	Protocol	Source	Src Port	Destination	I
SIP	SIP Generic		Downstream		SBC Internal	5

Generic Endpoint	Endpoint → SBC	TCP/UDP	SBC IPs	Any	IP Address	5(
	SBC → SIP Generic Endpoint	TCP/UDP	SBC Internal IP Address	Any	Downstream SBC IPs	5(5(
	SIP Generic Endpoint → SBC	UDP	Downstream SBC IPs	Any	SBC Internal IP Address	3(3!
	SBC → SIP Generic Endpoint	UDP	SBC Internal IP Address	30000-39999	Downstream SBC IPs	A

16.2 OVOC Firewall Rules

Device Administration via OVOC

Service	Direction	Protocol	Source	Src Port	Destination
SNMP (Trap)	SBC → OVOC	UDP	SBC Management Interface IP	161	OVOC IP
SNMP (Trap)	OVOC → SBC	UDP	OVOC IP	1161	SBC Management Interface IP
SNMP (Keep-Alive)	SBC → OVOC	UDP	SBC Management Interface IP	161	OVOC IP
QoE Reporting	SBC → OVOC	TCP (TLS)	SBC Management Interface IP	Any	OVOC IP
Device Management	OVOC → SBC	TCP	OVOC IP	Any	SBC Management Interface IP
Device Management	SBC → OVOC	TCP	SBC Management Interface IP	Any	OVOC IP
NTP	SBC → OVOC	UDP/TCP	SBC Management Interface IP	Any	OVOC IP

Management

Service	Direction	Protocol	Source	Src	Destination	Ds

				Port		Po
SSH	Jump server → OVOC	TCP	Jump server IP / Management Subnet	Any	OVOC IP	22
HTTPS	Jump server → OVOC	TCP	Jump server IP / Management Subnet	Any	OVOC IP	443
LDAP(s)	OVOC → LDAP	TCP	OVOC IP	Any	LDAP server	636
Client PCs	Client PC → OVOC	TCP	Client IP	Any	OVOC IP	22, 443
Syslog	OVOC → Syslog server	UDP/TCP	OVOC IP	Any	Syslog Server / Jump server	514
Debug Recording	OVOC → Syslog server	UDP/TCP	OVOC IP	Any	Syslog Server / Jump server	925

Device Manager Functionality

Service	Direction	Protocol	Source	Src Port	Destination	
HTTPS	Endpoints ↔ OVOC Device Manager	TCP	Endpoints	Any	OVOC IP	
HTTPS	OVOC → AudioCodes ShareFile	TCP	OVOC IP	Any	docs.sharefile.com	

Functional

Service	Direction	Protocol	Source	Src Port	Destination
NTP	OVOC → NTP Server	UDP/TCP	OVOC IP	Any	NTP server
DNS	OVOC → DNS Server	UDP/TCP	OVOC IP	Any	DNS server
Alarm forwarding	OVOC → 3rd party	UDP/TCP	OVOC IP	161	3rd Party SNMP rec
	OVOC →				

Email forwarding	Mail server	TCP	OVOC IP	Any	Mail server
Teams QoE integration	Microsoft Teams → OVOC	TCP	Microsoft 365 IPs (see MS docs)	Any	OVOC IP
	OVOC → Microsoft	TCP	OVOC IP	Any	login.microsoftonli
	OVOC → Microsoft	TCP	OVOC IP	Any	graph.microsoft.cor

Data Analytics API

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port
Analytics API (PostgreSQL)	ETL Platform → OVOC	TCP	ETL Platform IP / CIDR	Any	OVOC IP	5432

16.3 ARM Firewall Rules

Device Administration via OVOC

Service	Direction	Protocol	Source	Src Port	Destination
SNMP (Trap)	ARM → OVOC	UDP	ARM Configurator IP	161	OVOC IP
SNMP (Trap)	OVOC → ARM	UDP	OVOC IP	1161	ARM Configurator IP
SNMP (Keep-Alive)	ARM → OVOC	UDP	ARM Configurator IP	161	OVOC IP
Device Management	OVOC → ARM	TCP	OVOC IP	Any	ARM Configurator IP
Device	ARM →		ARM		

Management	OVOC	TCP	Configurator IP	Any	OVOC IP
NTP	ARM → OVOC	UDP/TCP	ARM Configurator IP	Any	OVOC IP

Management

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port
SSH	Jump server → ARM	TCP	Jump server IP / Management Subnet	Any	ARM Configurator IP, ARM Router IP	22
HTTPS	Jump server → ARM	TCP	Jump server IP / Management Subnet	Any	ARM Configurator IP, ARM Router IP	443
LDAP(s)	ARM → LDAP	TCP	ARM Configurator IP	Any	LDAP server	636
Client PCs	Client PC → ARM	TCP	Client IP	Any	ARM Configurator IP, ARM Router IP	22, 443
Syslog	ARM → Syslog server	UDP/TCP	ARM Configurator IP, ARM Router IP	Any	Syslog Server / Jump server	514

ARM Application

Service	Direction	Protocol	Source	Src Port	Destinat
HTTPS/SSH/JMS	ARM Configurator → ARM Router	TCP	ARM Configurator IP	Any	ARM Rou IP
HTTPS/SSH/JMS	ARM Router → ARM Configurator	TCP	ARM Router IP	Any	ARM Configura IP
HTTPS	ARM Configurator	TCP	ARM Configurator IP, ARM	Any	SBC IP

	→ SBC		Router IP		
HTTPS	SBC → ARM	TCP	SBC IP	Any	ARM Configura IP, ARM Router IP

Functional

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port
NTP	ARM → NTP Server	UDP/TCP	ARM Configurator IP, ARM Router IP	Any	NTP server	123
DNS	ARM → DNS Server	UDP/TCP	ARM Configurator IP, ARM Router IP	Any	DNS server	53

16.4 Downstream SBC Firewall Rules

Device Administration via OVOC

Service	Direction	Protocol	Source	Src Port	Destination
SNMP (Trap)	SBC → OVOC	UDP	SBC Management Interface IP	161	OVOC IP
SNMP (Trap)	OVOC → SBC	UDP	OVOC IP	1161	SBC Management Interface IP
SNMP (Keep-Alive)	SBC → OVOC	UDP	SBC Management Interface IP	161	OVOC IP
QoE Reporting	SBC → OVOC	TCP (TLS)	SBC Management Interface IP	Any	OVOC IP
Device Management	OVOC → SBC	TCP	OVOC IP	Any	SBC Management Interface IP
Device Management	SBC → OVOC	TCP	SBC Management Interface IP	Any	OVOC IP
			SBC		

NTP	SBC → OVOC	UDP/TCP	Management Interface IP	Any	OVOC IP	

Management via Jump Server

Service	Direction	Protocol	Source	Src Port	Destination	D Pc
SSH	Jump server → SBC	TCP	Jump server IP / Management Subnet	Any	SBC Management Interface IP	22
HTTPS	Jump server → SBC	TCP	Jump server IP / Management Subnet	Any	SBC Management Interface IP	44
RADIUS Auth	SBC → RADIUS AAA	UDP	SBC Management Interface IP	Any	Cisco ISE PSN	18
RADIUS Acct	SBC → RADIUS AAA	UDP	SBC Management Interface IP	Any	Cisco ISE PSN	18
Debug Recording	SBC → Jump server	UDP	SBC Management Interface IP	Any	Jump server IP / Management Subnet	92
Syslog	SBC → Jump server	UDP	SBC Management Interface IP	Any	Jump server IP / Management Subnet	51
CDR	SBC → CDR server	TCP	SBC Management Interface IP	Any	CDR server	22

Functional

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port
NTP	SBC → NTP Server	UDP/TCP	SBC Management Interface IP	Any	NTP server	123
DNS	SBC → DNS Server	UDP/TCP	SBC Management Interface IP	Any	DNS server	53

Integration with PSTN SIP Provider (Applicable for SBCs with SIP trunks directly only)

Service	Direction	Protocol	Source	Src Port	Destination	Dst I
SIP Signalling	SBC → Telco Provider	UDP/TCP	SBC IP Address	Any	Telco Provider IP/s	To be confi with
SIP Signalling	Telco Provider → SBC	UDP/TCP	Telco Provider IP/s	Any	SBC IP Address	5060, 5061
Media	SBC → Telco Provider	UDP	SBC IP Address	40000-41999	Telco Provider IP/s	Any
Media	Telco Provider → SBC	UDP	Telco Provider IP/s	Any	SBC IP Address	40000 41999

Integration with Proxy SBC

Service	Direction	Protocol	Source	Src Port	Destination	
SIP Signalling	Sites → Proxy SBC	TCP/UDP	Downstream SBC IPs	Any	Proxy SBC Internal IP Address	5 5
SIP Signalling	Proxy SBC → Sites	TCP/UDP	Proxy SBC Internal IP Address	Any	Downstream SBC IPs	5 5
Media	Sites → Proxy SBC	UDP	Downstream SBC IPs	Any	Proxy SBC Internal IP Address	1 1
Media	Proxy SBC → Sites	UDP	Proxy SBC Internal IP Address	10000-19999	Downstream SBC IPs	A

ARM Integration

Service	Direction	Protocol	Source	Src Port	Destination	D P
ARM Integration	ARM → SBC	TCP	ARM Configurator IP, ARM Router IP	Any	SBC IP	4
	SBC →	TCP	SBC IP	Any	ARM Configurator	4

	ARM				IP, ARM Router IP	

Teams - LMO Flows

Service	Direction	Protocol	Source	Src Port	Destination	D Po
Teams - LMO Flows	Endpoints → Downstream SBC	UDP	Endpoints (Teams soft clients, IP Phones)	3478-3481, 49152-53247	SBC IP	300 399
	Downstream SBC → Endpoints	UDP	SBC IP	30000-39999	Endpoints (Teams soft clients, IP Phones)	347 348 491 532

Integration with SIP Generic Endpoints

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port
SIP Generic Endpoint	SIP Generic Endpoint → SBC	TCP/UDP	SIP Generic Endpoint IPs	Any	SBC Internal IP Address	5060-5069
	SBC → SIP Generic Endpoint	TCP/UDP	SBC Internal IP Address	Any	SIP Generic Endpoint IPs	5060-5069
	SIP Generic Endpoint → SBC	UDP	SIP Generic Endpoint IPs	Any	SBC Internal IP Address	30000 39999
	SBC → SIP Generic Endpoint	UDP	SBC Internal IP Address	30000-39999	SIP Generic Endpoint IPs	Any

16.5 SIP Generic Endpoint Firewall Rules

Device Manager Functionality

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port

HTTPS	Endpoints ↔ OVOC Device Manager	TCP	Endpoints	Any	OVOC IP	443
HTTPS	Jump server → Endpoints	TCP	Jump server IP / Management Subnet	Any	Endpoints	443, 22

Functional

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port	R
NTP	Endpoints → NTP Server	UDP/TCP	Endpoints	Any	NTP server	123	
DNS	Endpoints → DNS Server	UDP/TCP	Endpoints	Any	DNS server	53	
LDAP(s)	Endpoints → LDAP	TCP	Endpoints	Any	LDAP server	636	

Integration with SBC

Service	Direction	Protocol	Source	Src Port	Destination	Ds Por
SIP Signalling	SIP Generic Endpoint → SBC	TCP/UDP	Endpoints	Any	SBC Internal IP Address	5060 5069
SIP Signalling	SBC → SIP Generic Endpoint	TCP/UDP	SBC Internal IP Address	Any	Endpoints	5060 5069
Media	SIP Generic Endpoint → SBC	UDP	Endpoints	Any	SBC Internal IP Address	3000 3999
Media	SBC → SIP Generic Endpoint	UDP	SBC Internal IP Address	30000-39999	Endpoints	Any

16.6 Teams Endpoints Firewall Rules

Device Manager Functionality

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port
HTTPS	Endpoints ↔ OVOC Device Manager	TCP	Endpoints	Any	OVOC IP	443
HTTPS	Jump server → Endpoints	TCP	Jump server IP / Management Subnet	Any	Endpoints	443, 22

Functional

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port	R
NTP	Endpoints → NTP Server	UDP/TCP	Endpoints	Any	NTP server	123	
DNS	Endpoints → DNS Server	UDP/TCP	Endpoints	Any	DNS server	53	

Teams - LMO Flows

Service	Direction	Protocol	Source	Src Port	Destination	Dst Port
Media	Endpoints → SBC	UDP	Endpoints (Teams soft clients, IP Phones)	3478-3481, 49152-53247	SBC IP	30000-39999
Media	SBC → Endpoints	UDP	SBC IP	30000-39999	Endpoints (Teams soft clients, IP Phones)	3478-3481, 49152-53247

Microsoft Services

Service	Direction	Protocol	Source	Src Port	Destination
	Endpoints				Microsoft 365

HTTP/HTTPS	→ Microsoft	TCP	Endpoints	Any	IPs (see MS docs)
STUN/TURN	Endpoints → Microsoft	UDP	Endpoints	Any	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14
Endpoint-to-Endpoint Media	Endpoints ↔ Endpoints	UDP	Endpoints	3478-3481, 49152-53247	Endpoints

17. Break Glass Accounts

Overview

Each AudioCodes workload **must** have a dedicated local break glass account for emergency access when: - Microsoft Entra ID is unavailable - OAuth authentication fails - Identity provider integration is misconfigured - Emergency maintenance is required

Requirements

Requirement	Details
Account Type	Local account on each appliance
Naming Convention	`breakglass-<component>-<environment>`
Password Policy	Minimum 20 characters, complex
Storage	Secure secret repository of your choice
Access	Documented procedure, dual-control access
Audit	All usage must be logged and reviewed

Non-Production Environment Accounts

Component	Username	Purpose
Stack Manager	`breakglass-stackmgr-nonprod`	Emergency Stack Manager access
SBC #1 (AZ-A)	`breakglass-sbc1-nonprod`	Emergency SBC access
SBC #2 (AZ-B)	`breakglass-sbc2-nonprod`	Emergency SBC access
ARM Configurator	`breakglass-armcfg-nonprod`	Emergency ARM Configurator access
	`breakglass-armrtr-`	Emergency ARM

ARM Router	`nonprod`	Router access

Non-Production Total: 5 break glass accounts

Production Australia Accounts

Component	Username	Purpose
Stack Manager	`breakglass-stackmgr-prod-aus`	Emergency Stack Manager access
SBC #1 (AZ-A)	`breakglass-sbc1-prod-aus`	Emergency SBC access
SBC #2 (AZ-B)	`breakglass-sbc2-prod-aus`	Emergency SBC access
OVOC	`breakglass-ovoc-prod`	Emergency OVOC access
ARM Configurator	`breakglass-armcfg-prod`	Emergency ARM Configurator access
ARM Router (AUS)	`breakglass-armrtr-prod-aus`	Emergency ARM Router access

Production AUS Total: 6 break glass accounts

Production United States Accounts

Component	Username	Purpose
SBC #1 (AZ-A)	`breakglass-sbc1-prod-us`	Emergency SBC access
SBC #2 (AZ-B)	`breakglass-sbc2-prod-us`	Emergency SBC access
ARM Router (US)	`breakglass-armrtr-prod-us`	Emergency ARM Router access

Production US Total: 3 break glass accounts

> **Note:** No Stack Manager break glass account is required for the US region. The Australian Stack Manager manages US SBC HA stacks remotely.

Password Storage

Store break glass credentials in a secure, access-controlled secret repository of your choice (e.g., enterprise password vault, secrets manager, or equivalent secure storage solution).

Recommended folder/path structure:

Environment	Path/Folder

Non-Production	`/audiocodes/nonprod/`
Production - Australia	`/audiocodes/prod-aus/`
Production - United States	`/audiocodes/prod-us/`

Access Procedure

1. **Dual Control:** Two authorized personnel required to retrieve credentials
2. **Incident Ticket:** Create incident ticket before retrieval
3. **Time-Limited:** Credentials retrieved for specific maintenance window
4. **Audit Trail:** Log all access to secrets manager
5. **Post-Use:** Rotate password after each use (recommended)

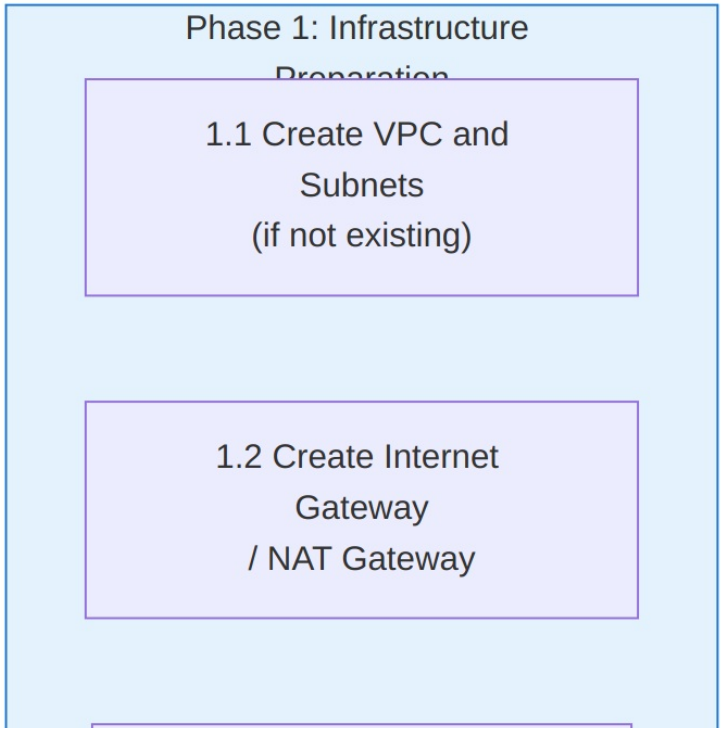
Password Rotation Schedule

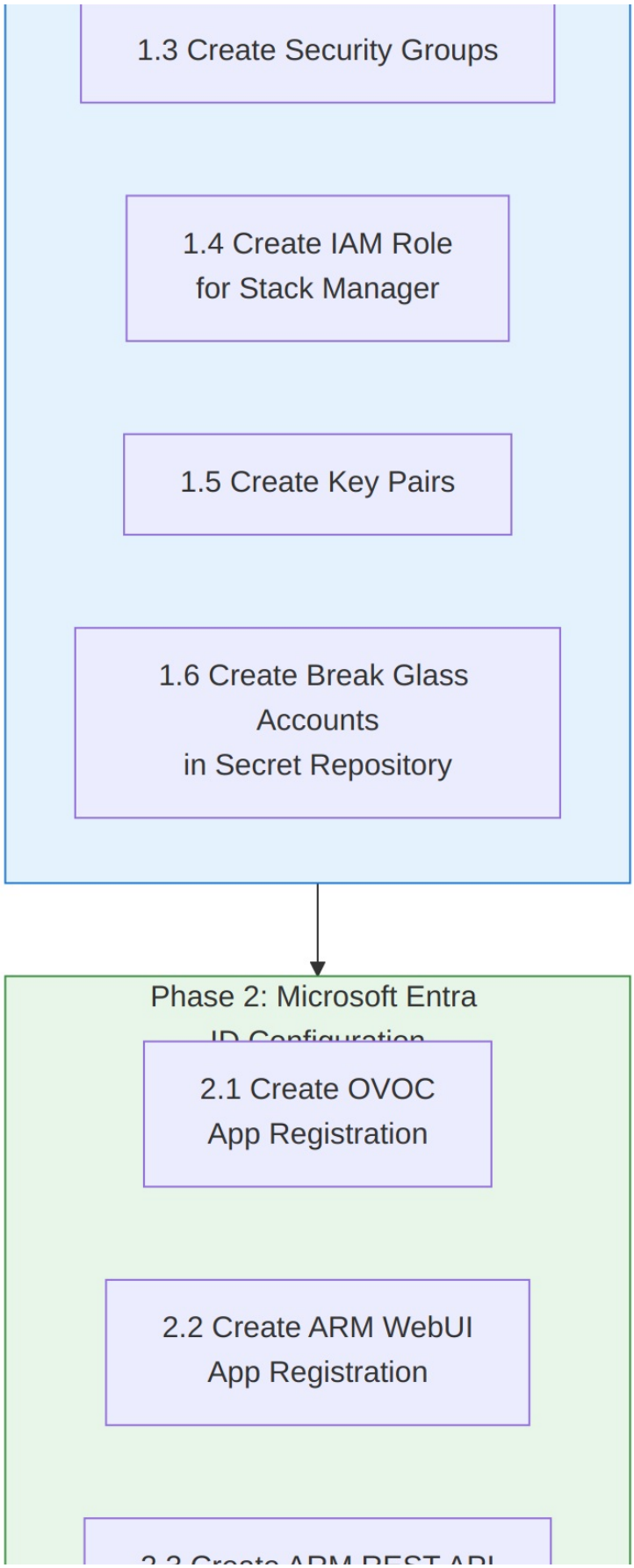
Frequency	Action
Quarterly	Review break glass account status
Semi-Annually	Rotate all break glass passwords
After Each Use	Rotate used account password
Annually	Full break glass procedure test

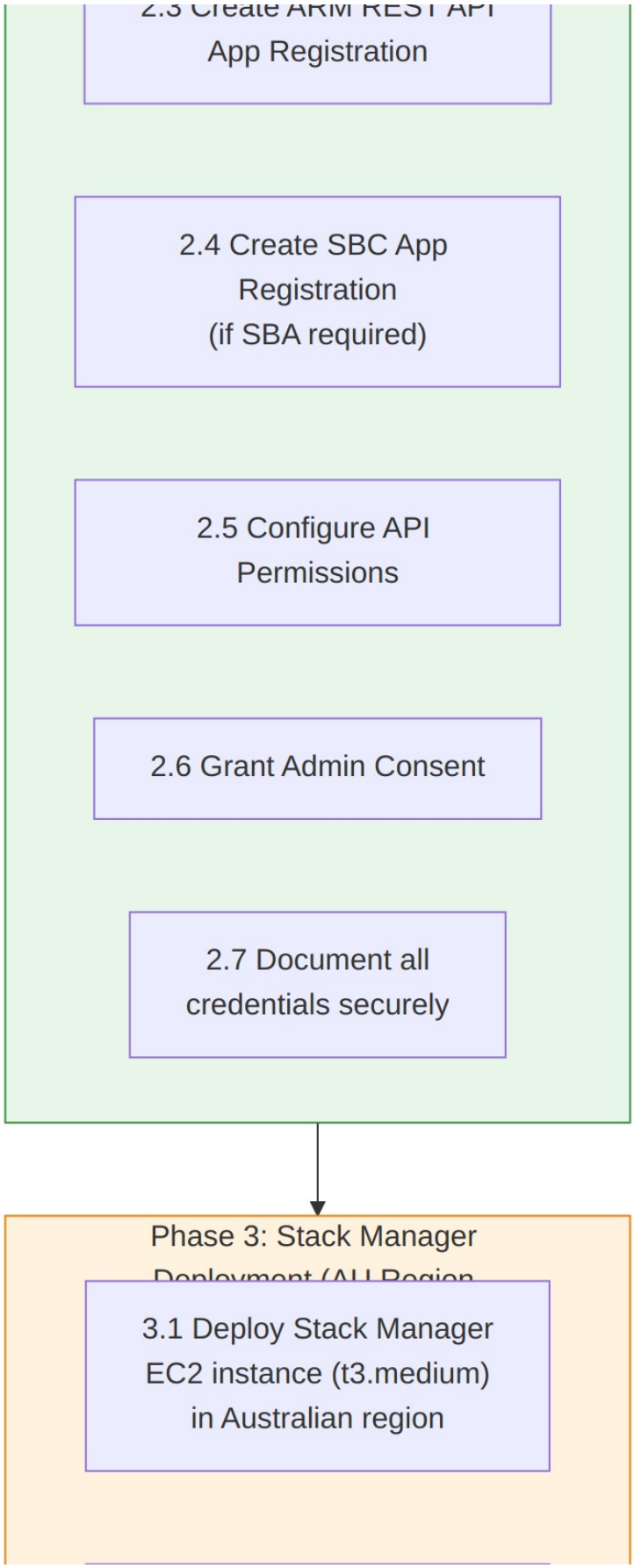
---

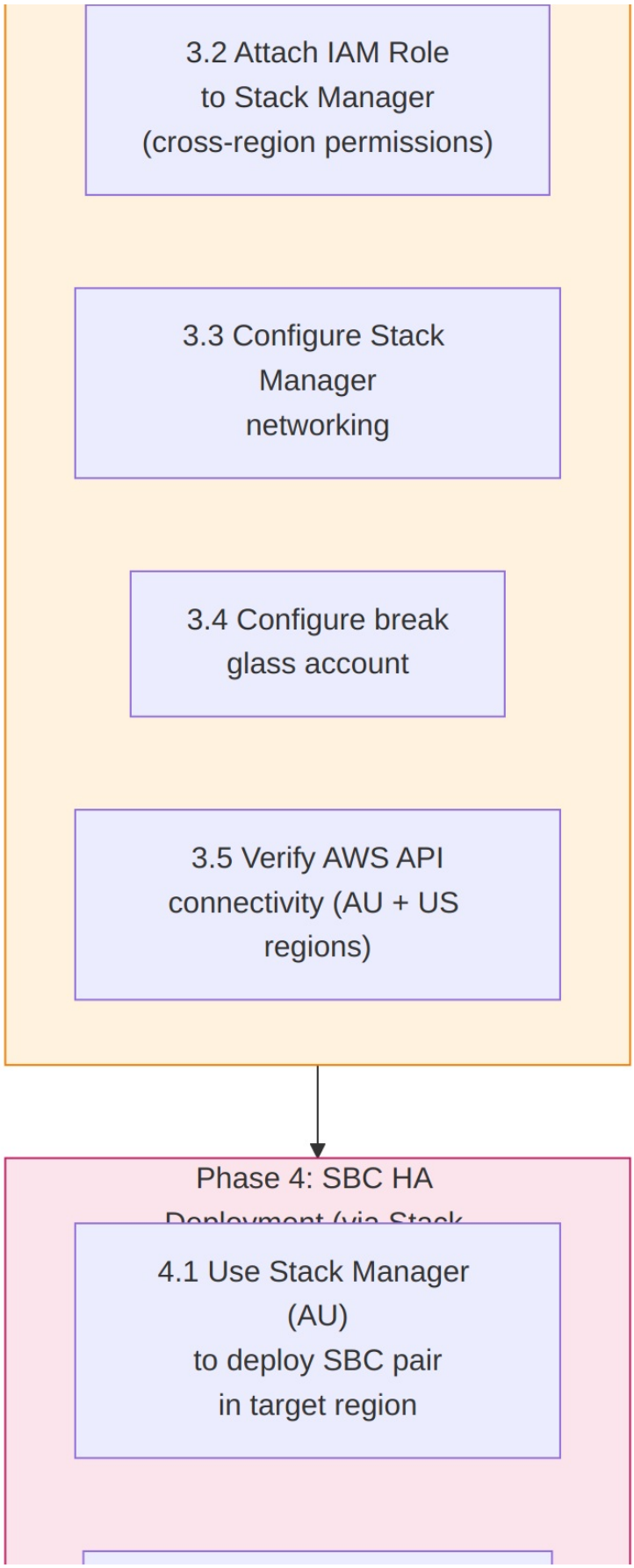
18. Deployment Methodology

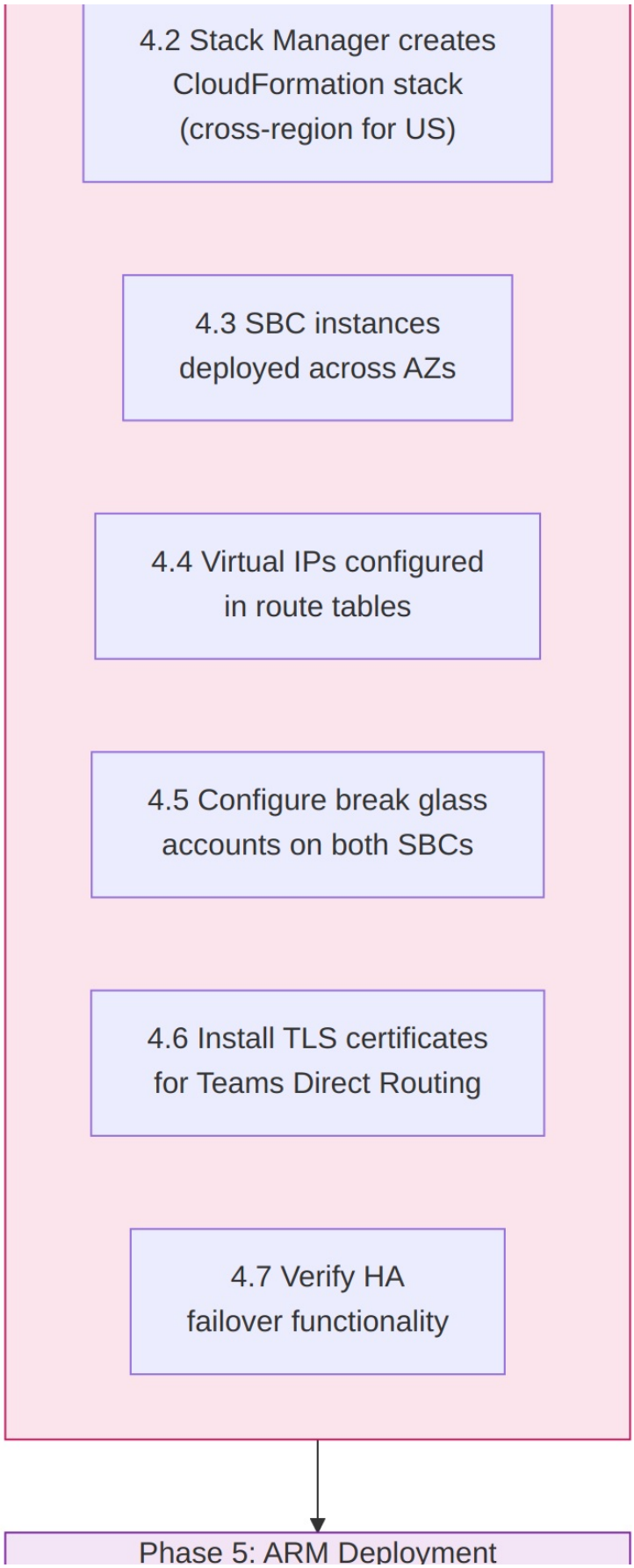
8-Phase Deployment Sequence

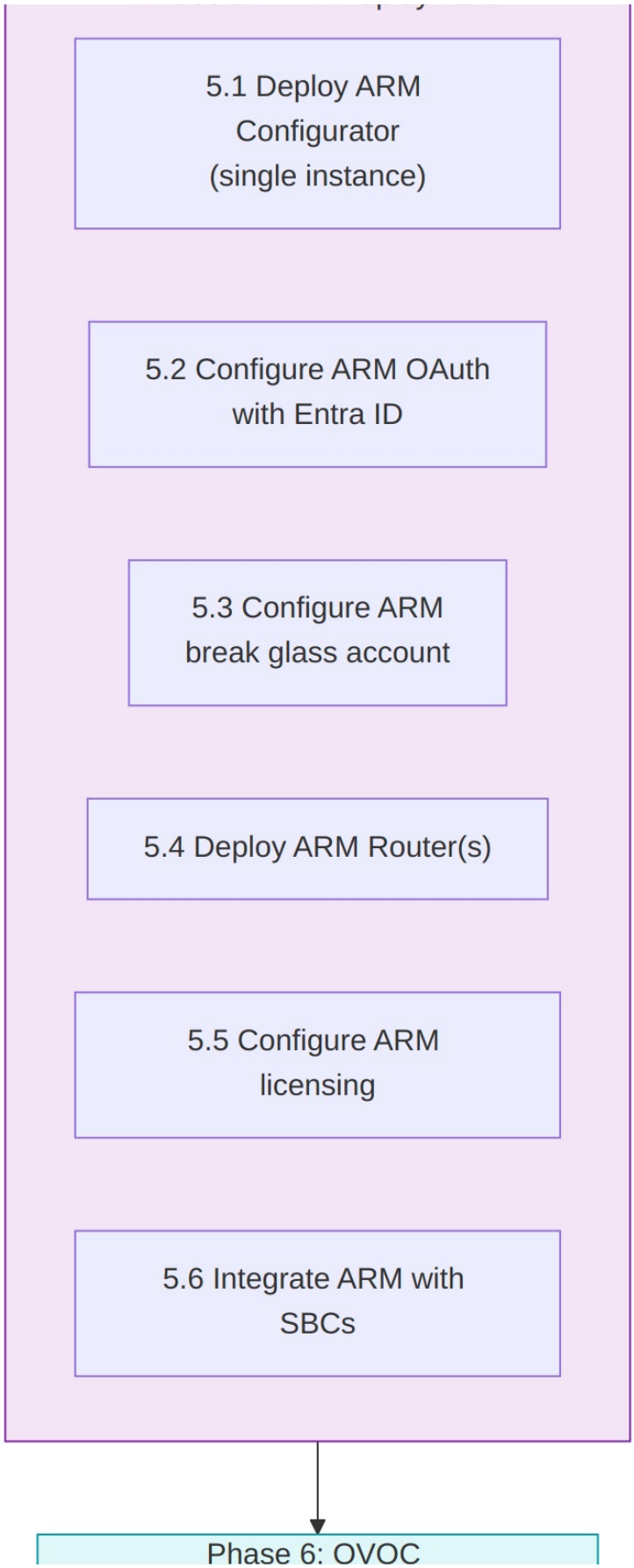


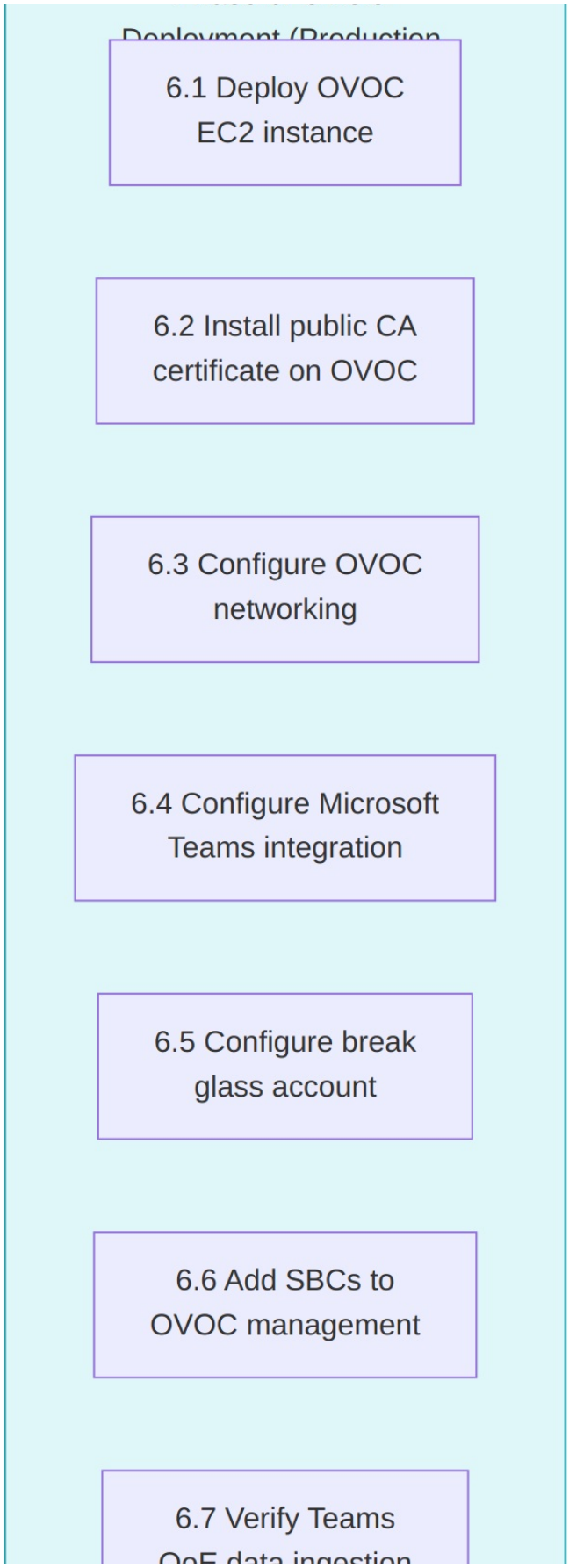

1.3 Create Security Groups
1.4 Create IAM Role for Stack Manager
1.5 Create Key Pairs
1.6 Create Break Glass Accounts in Secret Repository
Phase 2: Microsoft Entra
2.1 Create OVOC App Registration
2.2 Create ARM WebUI App Registration

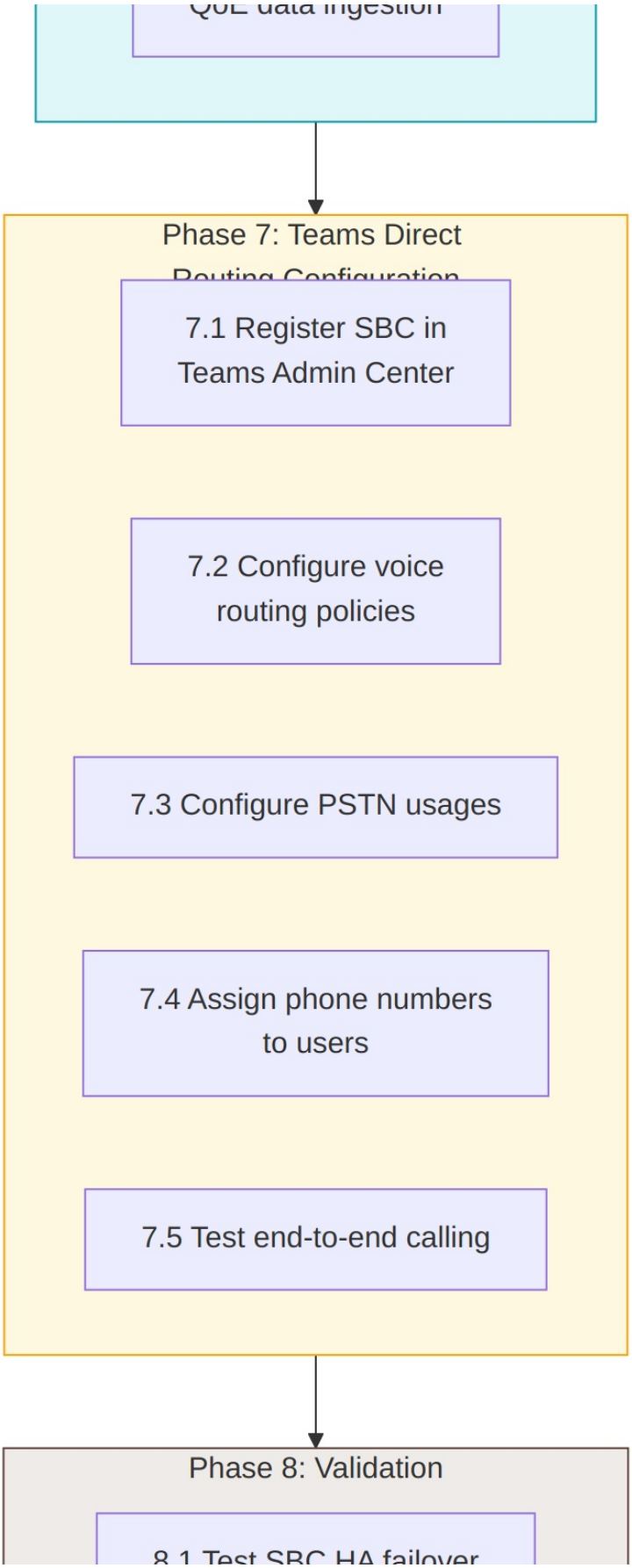

2.3 Create ARM REST API
App Registration
2.4 Create SBC App
Registration
(if SBA required)
2.5 Configure API
Permissions
2.6 Grant Admin Consent
2.7 Document all
credentials securely
Phase 3: Stack Manager
3.1 Deploy Stack Manager
EC2 instance (t3.medium)
in Australian region


3.2 Attach IAM Role to Stack Manager (cross-region permissions)
3.3 Configure Stack Manager networking
3.4 Configure break glass account
3.5 Verify AWS API connectivity (AU + US regions)
Phase 4: SBC HA
4.1 Use Stack Manager (AU) to deploy SBC pair in target region


4.2 Stack Manager creates CloudFormation stack (cross-region for US)
4.3 SBC instances deployed across AZs
4.4 Virtual IPs configured in route tables
4.5 Configure break glass accounts on both SBCs
4.6 Install TLS certificates for Teams Direct Routing
4.7 Verify HA failover functionality
Phase 5: ARM Deployment


5.1 Deploy ARM Configurator (single instance)
5.2 Configure ARM OAuth with Entra ID
5.3 Configure ARM break glass account
5.4 Deploy ARM Router(s)
5.5 Configure ARM licensing
5.6 Integrate ARM with SBCs
Phase 6: OVOC


Deployment (Production
6.1 Deploy OVOC EC2 instance
6.2 Install public CA certificate on OVOC
6.3 Configure OVOC networking
6.4 Configure Microsoft Teams integration
6.5 Configure break glass account
6.6 Add SBCs to OVOC management
6.7 Verify Teams QoE data ingestion


QoE data ingestion
Phase 7: Teams Direct Routing Configuration
7.1 Register SBC in Teams Admin Center
7.2 Configure voice routing policies
7.3 Configure PSTN usages
7.4 Assign phone numbers to users
7.5 Test end-to-end calling
Phase 8: Validation
8.1 Test SBC HA failover

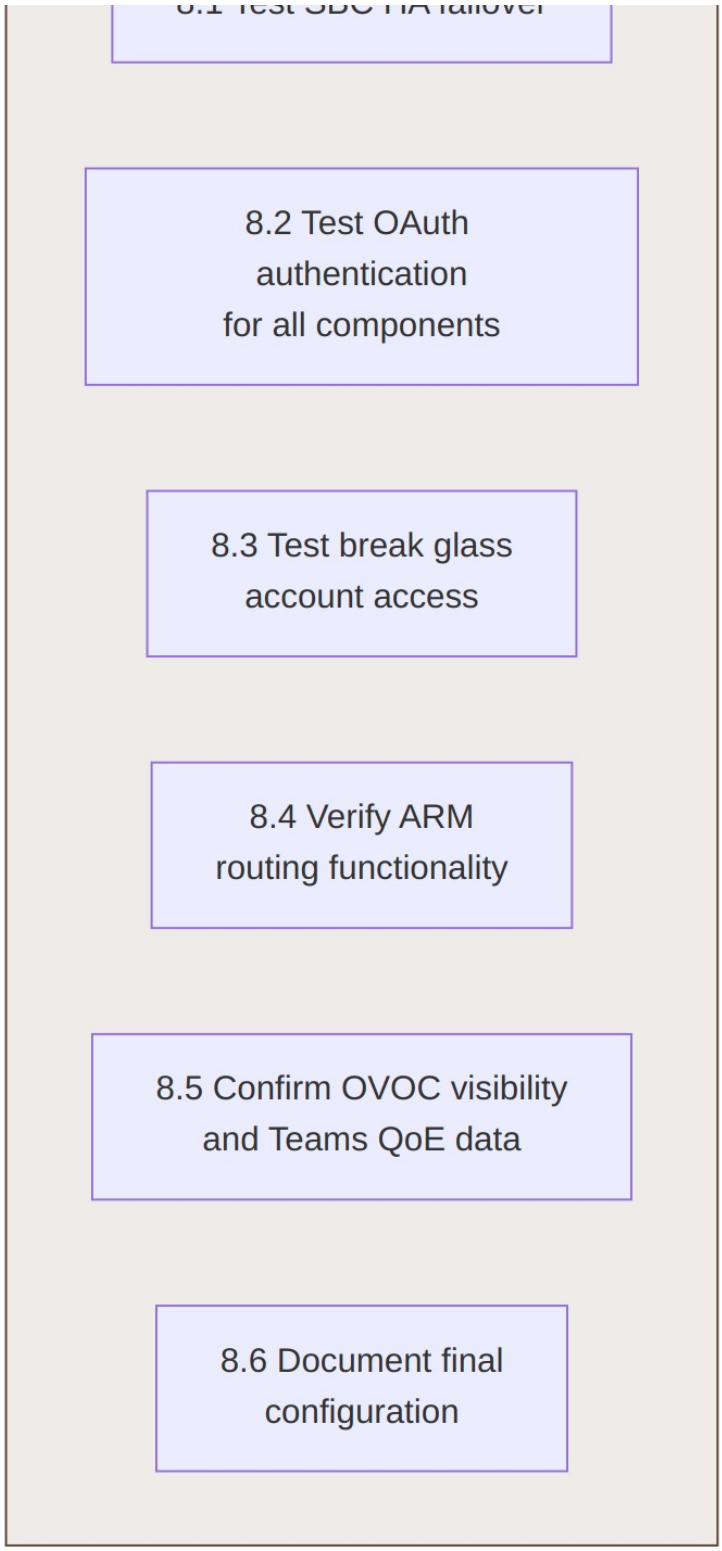

8.1 Test SBC HA failover
8.2 Test OAuth authentication for all components
8.3 Test break glass account access
8.4 Verify ARM routing functionality
8.5 Confirm OVOC visibility and Teams QoE data
8.6 Document final configuration

Diagram 6

Deployment Methods by Component

Component	Deployment Method	Source
Stack Manager	AWS EC2 Console / CLI (AU region only)	AudioCodes AMI from AWS Marketplace
Mediant VE SBC	**Via Stack Manager only** (for HA); Stack Manager in AU manages all regions	Stack Manager orchestrates deployment via cross-region API
ARM Configurator	AWS EC2 Console using AudioCodes AMI	AWS Marketplace Community AMI
ARM Router	AWS EC2 Console using AudioCodes AMI	AWS Marketplace Community AMI
OVOC	AWS EC2 Console using AudioCodes AMI	AudioCodes provided AMI

19. High Availability Considerations

SBC HA Architecture

Aspect	Configuration
Mode	1+1 Active/Standby
Scope	Within single VPC, across two Availability Zones
Failover Trigger	Health check failure, manual trigger
Failover Mechanism	SBC directly updates VPC route tables via AWS API
Call Handling	Active IP calls maintained; PSTN calls dropped
Virtual IP Range	10.x.x.x (within VPC CIDR)
Heartbeat Network	Dedicated HA subnet between SBC instances

> **CRITICAL: SBC IAM Role Required for HA Failover**
>
> SBCs **MUST** have an IAM role attached to call AWS APIs during failover. The SBCs directly manipulate VPC route tables and reassign Elastic IPs to redirect traffic to the newly Active instance. **Without this IAM role, HA failover will NOT work.**
>
> **Required IAM Permissions (least-privilege, per AudioCodes recommendation):** - `ec2:DescribeAddresses` - Query Elastic IP allocation state (`Resource: *`) - `ec2:DescribeNetworkInterfaceAttribute` - Query ENI attributes (`Resource: *`) - `ec2:DescribeNetworkInterfaces` - Query ENI information (`Resource: *`) - `ec2:ReplaceRoute` - Update existing route table entries (scoped to specific route table ARN + `Env` tag) - `ec2:AssociateAddress` - Reassign Elastic IP during failover (scoped to specific EIP ARN + `App`/`Env` tags)
>
> **Network Requirement:** The HA subnet must have connectivity to AWS API endpoints (via NAT Gateway or VPC Endpoint for EC2). Without this connectivity, the SBC cannot call AWS APIs to perform route table updates.
>
> See Section 20: IAM Permissions and Security for the full IAM policy and creation steps.

Prerequisites for HA Deployment

Before deploying an SBC HA pair, ensure all of the following requirements are met:

- ☐ **IAM Role Created** - SBC IAM role with route table manipulation permissions (see Section 20)
- ☐ **IAM Role Attached** - Both SBC EC2 instances have the IAM role attached (typically done via Stack Manager during deployment)
- ☐ **HA Subnet Created** - Dedicated subnet for HA heartbeat communication between SBC instances
- ☐ **AWS API Connectivity** - HA subnet has outbound connectivity to AWS EC2 API endpoints (via NAT Gateway or VPC Endpoint)
- ☐ **Two Availability Zones** - SBC instances deployed in separate AZs within the same VPC
- ☐ **Virtual IP Allocated** - VIP from 10.x.x.x range allocated within VPC CIDR
- ☐ **Route Tables Configured** - VPC route tables prepared for VIP routing
- ☐ **Stack Manager Deployed** - Required for initial HA cluster deployment (see Section 21)

What Happens During SBC Failover

1. **Active SBC fails** (detected via HA subnet heartbeat)
2. **Standby SBC detects failure** via HA heartbeat timeout
3. **Standby SBC calls AWS EC2 API** to update route table (requires IAM

role)
4. **Virtual IP route** changed from failed SBC's ENI to standby SBC's ENI
5. **Elastic IP** (if used) reassigned to standby SBC
6. **Standby becomes Active** and starts serving traffic
7. **Active calls using IP** are maintained during failover
8. **PSTN calls in progress** are dropped and must be re-established

ARM HA Architecture

Aspect	Configuration
Router Mode	Active-Active for Routers
Configurator Mode	Single instance (no HA)
Configurator Failure Handling	Routers continue with last known configuration
Router Failure Handling	Traffic redistributed to remaining routers
Database	Embedded in Configurator

SIP Trunk Connectivity in HA

This section explains how the HA SBC pair connects outbound to regional SIP providers and what happens during failover. Each region (AU/US) has its own SIP provider for local PSTN breakout.

Concept Overview

When configuring SIP trunks with regional SIP providers (e.g., SIP Provider AU for the Australian Proxy SBC, SIP Provider US for the US Proxy SBC), the SBC registers with and initiates outbound connections to the provider. The provider sees traffic originating from a **single Virtual IP (VIP)** address:

- The enterprise SBC initiates registration and maintains the SIP trunk connection to the provider
- Outbound SIP traffic from the SBC originates from the Virtual IP that "floats" between the Active and Standby SBCs
- While the SBC initiates and maintains the SIP registration, **media and SIP signalling flows are bidirectional** from a network and firewall perspective. The provider will send inbound media (RTP/SRTP) and may send inbound SIP requests (e.g., INVITE for incoming calls, BYE, re-INVITE) to the SBC's Virtual IP
- Firewall rules must permit **both** inbound and outbound SIP signalling and media between the SBC and the provider — restricting to outbound only may cause issues with early media, inbound calls, and call teardown
- Failover is transparent to the provider — the new Active SBC re-registers and resumes the connection

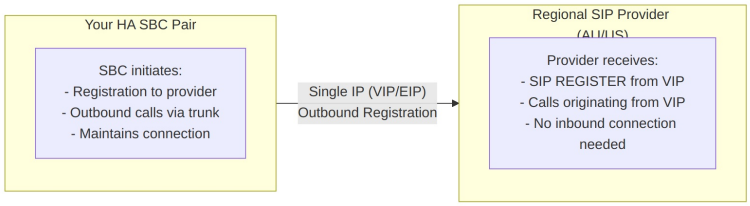


Diagram 7

How the VIP Works

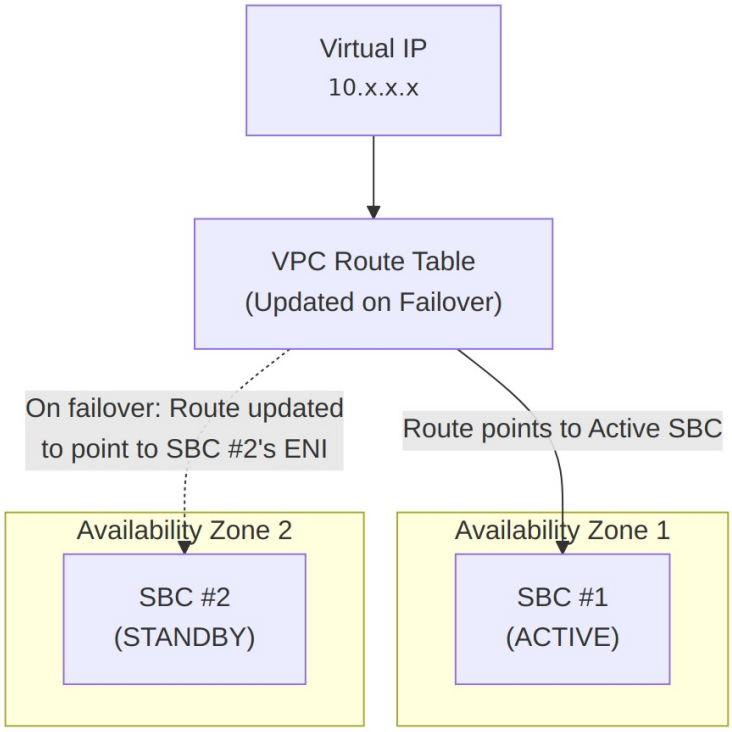


Diagram 8

Traffic Types and Failover Mechanisms

Traffic Type	Direction	Source IP Type	Failover Mechanism	Provider Action Required
External (SBC to Regional SIP Provider)	SBC initiates outbound registration and calls to provider	Virtual IP on External interface	VPC route table updated to point VIP to new Active SBC's ENI; new Active SBC re-registers	None - transparent
External	Microsoft Teams	Elastic IP (public)	Elastic IP reassigned	

(Teams from Internet)	infrastructure from public internet	on External interface	from failed SBC to Standby SBC	None - transparent

Note: Both failover mechanisms are handled automatically by the SBC HA pair calling AWS APIs. The regional SIP provider experiences a brief interruption but does not need to take any action.

Information to Exchange with Your Regional SIP Provider

When onboarding a new SIP trunk with a regional SIP provider (SIP Provider AU or SIP Provider US), exchange the following information. The SBC will register with and initiate connections to the provider:

Information	Value	Notes
SBC Source IP Address	Virtual IP on External interface	Provider should expect SIP REGISTER and calls from this IP
Provider's SIP Server Address	Provided by SIP Provider	The SBC will register to this address
SIP Port	5060 (UDP/TCP) or 5061 (TLS)	Based on your security requirements
Registration Credentials	Username/password from provider	SBC uses these to authenticate with provider
Transport Protocol	UDP, TCP, or TLS	TLS recommended for security
Codec Support	G.711, G.729, etc.	As per your configuration

Important: The SBC initiates SIP registration and maintains the trunk connection. However, from a **network and firewall perspective**, traffic flows are bidirectional — the provider will send inbound SIP requests (for incoming calls) and inbound media (RTP) to the SBC's Virtual IP. Ensure firewall rules permit both directions. Provide the provider with the **Virtual IP** as the expected source/destination address for SIP traffic.

Failover Behavior and Call Impact

Understanding what happens during failover helps set expectations with your regional SIP provider:

Scenario	Behaviour

Active calls in progress (PSTN and Teams)	Calls should **not drop**. Call sessions are synchronised between Active and Standby SBCs via the HA link. As long as the Virtual IP re-assignment completes without issues, ongoing calls remain intact and continue on the newly Active SBC.
New calls during failover	Brief interruption (seconds) while route table updates and VIP re-assignment completes; new calls then succeed
New calls after failover	Route seamlessly via the new Active SBC — no difference from caller perspective
Regional SIP provider reconfiguration	**Not required** — the new Active SBC re-registers with the provider using the same VIP

Key Point: During failover, call sessions are synchronised between Active and Standby SBCs. Ongoing calls should remain intact provided the Virtual IP re-assignment completes successfully. There is no Re-INVITE mechanism in this HA model — call continuity is achieved through session state synchronisation and VIP failover. (Re-INVITE would apply in a Customer Edge SBC model or when using a load balancer instead of Virtual IPs, neither of which applies to this deployment.) Communicate to your regional SIP provider that during rare failover events, there may be a brief interruption lasting a few seconds while the new Active SBC re-registers. The provider does **not** need to take any action — the new Active SBC automatically re-registers and resumes normal operation.

HA Connectivity Architecture Diagram

The following diagram shows how different entities connect to the HA Proxy SBC pair, distinguishing between external (internet-facing) and internal (private network) connectivity. Note that each region (Australia/US) has its own Proxy SBC pair with regional SIP provider connectivity for PSTN breakout:

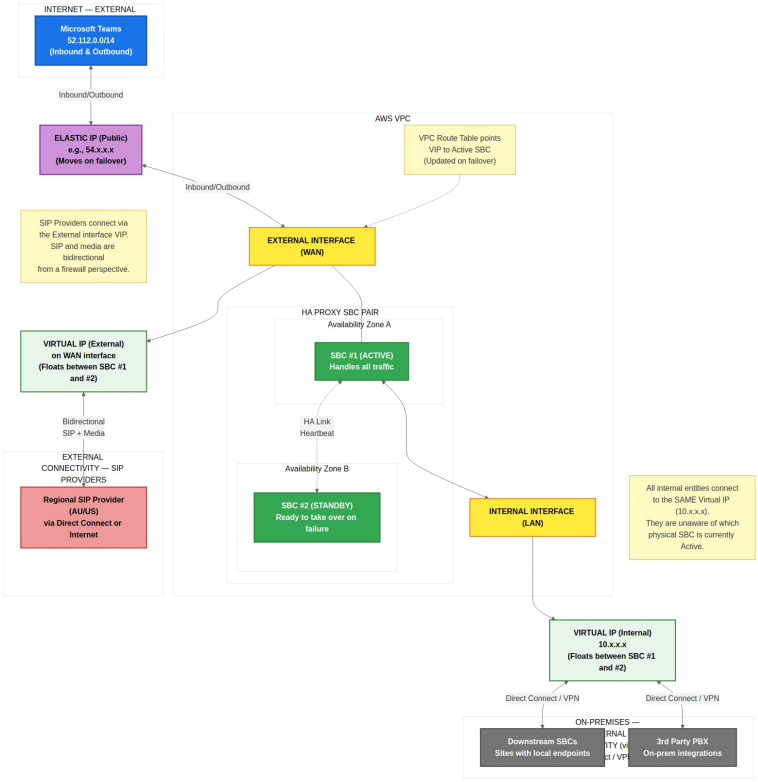


Diagram 9

Connectivity Summary by Entity Type

Entity	Location	Connects To	IP Type	Interface	Failover Impact
Microsoft Teams	Internet	Elastic IP	Public	External (WAN)	EIP moves to new Active SBC
SIP Provider AU	On-premises / Carrier	Virtual IP	Per carrier connectivity	External (WAN)	Route table updated
SIP Provider US	On-premises / Carrier	Virtual IP	Per carrier connectivity	External (WAN)	Route table updated
Downstream SBCs	On-premises	Virtual IP	Private (10.x.x.x)	Internal (LAN)	Route table updated
3rd Party PBX	On-premises	Virtual IP	Private (10.x.x.x)	Internal (LAN)	Route table updated
Registered Endpoints	On-premises	Virtual IP	Private (10.x.x.x)	Internal (LAN)	Route table updated

---

Key Design Points:

1. **External entities** (Teams) connect via the **Elastic IP** on the WAN interface
2. **Internal entities** (downstream SBCs, PBX) connect via the **Virtual IP** on the LAN interface
3. **Regional SIP Providers** connect via the **Virtual IP** on the External (WAN) interface. Although SIP Provider traffic may traverse Direct Connect for private connectivity, the SBC uses the External interface for SIP Provider signalling and media. During failover, the VIP on the External interface is re-assigned to the new Active SBC via route table update
4. **Each region has its own SIP provider** for local PSTN breakout (SIP Provider AU for Australian Proxy SBC, SIP Provider US for US Proxy SBC)
5. **All IP types "float"** - they move to the Active SBC automatically on failover
6. **No entity needs reconfiguration** - the destination IP remains the same regardless of which SBC is Active

Voice Recording Considerations

When deploying SBCs with Microsoft Teams Direct Routing, organisations using existing voice recording solutions must consider the impact of media encryption on their recording infrastructure.

The Challenge

Typical Voice Recorder Setup: - Uses **port mirroring** (SPAN) to capture IP-based RTP traffic - Uses **analog taps** for traditional analog phones - Passively captures traffic - needs to "see" unencrypted media

The Problem: - Teams requires **SRTP** (encrypted media) between Teams and the Proxy SBC - If internal legs are also encrypted, port mirroring captures encrypted data that cannot be decoded - Port mirroring cannot decrypt SRTP without the session keys

The Good News: - Many modern voice recorders support **SIPREC** (e.g., Eventide NexLog DX-Series, Verint, NICE, Red Box, ASC) - SIPREC allows the SBC to send a decrypted media copy directly to the recorder - Full SRTP encryption can be maintained on the network while still recording calls

Media Encryption by Segment

Segment	Encryption	Configurable?	Notes
Teams ↔ Proxy SBC	SRTP (mandatory)	No	Microsoft requirement
Proxy SBC ↔ Downstream	RTP or SRTP	Yes	IP Profile

SBC			setting
Downstream SBC ↔ IP Phones	RTP or SRTP	Yes	IP Profile setting
Proxy SBC ↔ PSTN Provider	Usually RTP	Depends on carrier	Most carriers don't support SRTP

Option 1: Keep Internal Media as RTP (Unencrypted)

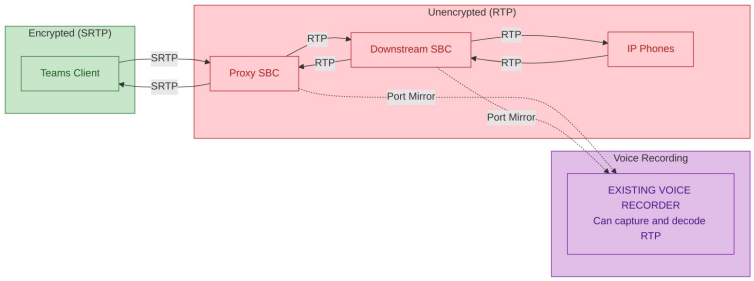


Diagram 10

Pros	Cons
Existing recorder works as-is with port mirroring	No encryption on internal network
Simplest option	Security team will likely object
No additional cost or config changes	Assumes internal network is "trusted"

When this works: If the internal network is segmented, firewalled, and considered a trusted zone.

Option 2: SBC-Based Recording via SIPREC (Recommended)

If the existing voice recorder supports SIPREC (such as Eventide NexLog 740/840, Verint, NICE, Red Box, ASC), this is the recommended approach.

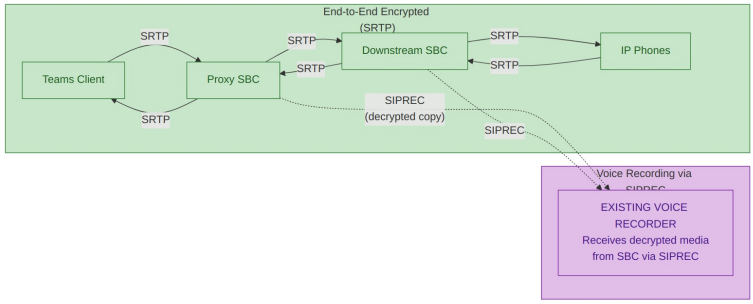


Diagram 11

Pros	Cons
End-to-end SRTP maintained on network	SIPREC licensing may be required on recorder
SBC handles decryption and sends to recorder	Additional SBC configuration
Industry standard approach	Older recorder models may not support SIPREC
Selective recording possible	May need to confirm channel capacity

Prerequisites: 1. Confirm existing voice recorder supports SIPREC 2. Confirm SIPREC is licensed/enabled on recorder 3. Confirm sufficient SIPREC channel capacity 4. Configure AudioCodes SBC as SIPREC client (SRC)

Option 3: Selective Encryption Based on Recording Needs

Use SBC Classification Rules to identify phones needing recording (by IP, User-Agent, number range) and apply RTP profile to those only, while other phones use SRTP.

Pros	Cons
Balance security and compliance	Complex to manage
Only expose what needs recording	Classification rules needed on SBC
Security team gets encryption for most calls	Inconsistent security posture

Option 4: Replace Existing Voice Recorder

If the current voice recorder doesn't support SIPREC, consider replacement with a SIPREC-capable recorder such as Eventide NexLog DX-Series, Verint, NICE, Red Box, or ASC.

Option 5: Microsoft Teams Native Recording + Existing Recorder for Legacy

Use Microsoft Compliance Recording (Purview or third-party policy-based) for Teams calls, while the existing recorder continues to capture PSTN/legacy calls via port mirroring.

Pros	Cons
Uses native Teams compliance	Two recording systems to manage
Existing recorder continues for PSTN/legacy	Data in two places
No changes to existing recorder	Teams recording has data sovereignty considerations

Voice Recording Decision Matrix

Option	Encryption	Existing Recorder Works?	Cost	Complexity	Security Approved?
1. RTP internally	Partial	Yes (port mirror)	None	Low	Unlikely
2. SIPREC	**Full SRTP**	**Yes (if SIPREC-capable)**	**Low-Medium**	**Medium**	**Yes**
3. Selective	Mixed	For selected phones	Low	High	Partially
4. Replace recorder	Full SRTP	N/A (new recorder)	High	High	Yes
5. Teams native + existing	Full SRTP	For non-Teams only	Low	Medium	Yes

Recommendation

If the existing voice recorder supports SIPREC: Option 2 (SIPREC) is recommended - full SRTP encryption on the network while the recorder receives decrypted media via SIPREC from the SBC.

If the existing voice recorder does not support SIPREC: - Option 1 (RTP internally) if security accepts the risk - Option 5 (Teams native + existing recorder for PSTN) as a hybrid approach - Option 4 (Replace/upgrade recorder) for long-term compliance

---

20. IAM Permissions and Security

Stack Manager IAM Policy

> **Note:** The Stack Manager is deployed in the Australian region only and requires cross-region permissions to manage SBC HA stacks in all regions (including US). The `Resource: "*"` scope enables cross-region API calls to us-east-1 and any future regions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudformation:*",
```

```
                "cloudwatch:DeleteAlarms",
                "cloudwatch:PutMetricAlarm",
                "iam:PassRole",
                "iam:ListInstanceProfiles",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note:** AudioCodes confirms these broad permissions (`ec2:*`, `cloudformation:*`) are required for Stack Manager to function — it creates and manages SBC HA stacks via CloudFormation. These permissions cannot be reduced without breaking Stack Manager functionality.

Temporal IAM Elevation Pattern (Recommended)

Because the Stack Manager requires broad permissions but is only actively used during deployment and Day 2 operations, implement a temporal elevation pattern to reduce standing privilege:

Phase	IAM State	When
Normal operations	Detach or disable the Stack Manager IAM policy	Day-to-day — Stack Manager is idle
Deployment / Day 2	Attach the full Stack Manager IAM policy	During initial deployment, software upgrades, stack healing, or topology changes
Post-operation	Detach or disable the policy again	Immediately after the operation completes

Implementation options:

1. **IAM Policy toggle:** Keep the policy created but detach it from the Stack Manager role when not in use. Re-attach via AWS Console or CLI before operations.
2. **AWS SCP (Service Control Policy):** Use an SCP to deny the broad permissions by default; temporarily remove the SCP deny during operations.
3. **Automation:** Use a runbook or pipeline that attaches the policy, performs the Stack Manager operation, and detaches the policy as a post-step.

> **Important:** Ensure the temporal elevation process is documented in the organisation's change management procedures. All attach/detach events are logged in CloudTrail for audit.

SBC IAM Policy (Required for HA Failover)

The SBCs require their own IAM role to perform route table updates and EIP reassignment during HA failover. This policy follows AudioCodes' recommended least-privilege model with resource-scoped permissions and tag-based conditions.

```
        {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "AllowDescribeActions",
                    "Effect": "Allow",
                    "Action": [
                        "ec2:DescribeAddresses",
                        "ec2:DescribeNetworkInterfaceAttribute",
                        "ec2:DescribeNetworkInterfaces"
                    ],
                    "Resource": "*"
                },
                {
                    "Sid": "AllowReplaceRoute",
                    "Effect": "Allow",
                    "Action": "ec2:ReplaceRoute",
                    "Resource": "arn:aws:ec2:<REGION>:<ACCOUNT_ID>:route-
table/<ROUTE_TABLE_ID>",
                    "Condition": {
                        "StringEquals": {
                            "aws:ResourceTag/Env": "<NonProd_SBC|Prod_SBC>"
                        }
                    }
                },
                {
                    "Sid": "AllowAssociateAddress",
                    "Effect": "Allow",
                    "Action": "ec2:AssociateAddress",
                    "Resource": "arn:aws:ec2:<REGION>:<ACCOUNT_ID>:elastic-
ip/<EIP_ALLOCATION_ID>",
                    "Condition": {
                        "StringEquals": {
                            "aws:ResourceTag/App": "Voice",
                            "aws:ResourceTag/Env": "<NonProd_SBC|Prod_SBC>"
                        }
                    }
                }
            ]
        }
```

> **Note:** Replace `<REGION>`, `<ACCOUNT_ID>`, `<ROUTE_TABLE_ID>`, and `<EIP_ALLOCATION_ID>` with your environment-specific values. The `Env` tag value should match your environment naming convention (e.g., `NonProd_SBC` or `Prod_SBC`).

SBC IAM Policy Design Rationale

Statement	Actions	Resource Scope
`AllowDescribeActions`	`DescribeAddresses`, `DescribeNetworkInterfaceAttribute`, `DescribeNetworkInterfaces`	*
`AllowReplaceRoute`	`ReplaceRoute`	Specific route table ARN
`AllowAssociateAddress`	`AssociateAddress`	Specific EIP ARN

IAM Role Creation Steps

Stack Manager Role

1. Navigate to **AWS IAM Console** > **Policies** > **Create Policy**
2. Select **JSON** tab and paste the Stack Manager policy above
3. Name the policy (e.g., `AudioCodes-StackManager-Policy`)
4. Click **Create Policy**
5. Navigate to **Roles** > **Create Role**

6. Select **EC2** as the trusted entity
7. Attach the policy created above
8. Name the role (e.g., `AudioCodes-StackManager-Role`)
9. Click **Create Role**
10. Attach this role to the Stack Manager EC2 instance in the Australian region via **Actions** > **Security** > **Modify IAM Role**

SBC Role

1. Navigate to **AWS IAM Console** > **Policies** > **Create Policy**
2. Select **JSON** tab and paste the SBC policy above
3. Name the policy (e.g., `AudioCodes-SBC-HA-Policy`)
4. Click **Create Policy**
5. Navigate to **Roles** > **Create Role**
6. Select **EC2** as the trusted entity
7. Attach the policy created above
8. Name the role (e.g., `AudioCodes-SBC-Role`)
9. Click **Create Role**
10. Attach this role to both SBC EC2 instances (typically done via Stack Manager during deployment)

---

21. Cyber Security Considerations

Overview

This section consolidates cyber security considerations for the AudioCodes SBC infrastructure on AWS. It covers the overall security architecture, external publishing patterns, authentication model, and component-specific risk assessments required for cyber security approval.

Security Architecture Summary

The solution employs two distinct external publishing patterns and a unified authentication model:

Aspect	SBC (Proxy)	OVOC / ARM	Stack Manager
External Publishing	Bespoke: Dedicated EIP + AWS Security Group L4 (no cloud firewall on external side)	Traditional: Cloud firewall + reverse proxy	None (private subnet only)
Internal Traffic	Cloud east-west firewall inspection on internal subnet	Cloud east-west firewall inspection on internal subnet	Private subnet, NAT Gateway egress

Authentication	RADIUS via Cisco ISE (with on-premises AD as identity source)	Microsoft Entra ID (OAuth 2.0)	Local + SSH key-based
MFA	Not natively supported (RADIUS limitation); ISE can proxy to MFA-capable identity sources	Supported via Entra Conditional Access	N/A

Key Design Decisions:

- **SBC external interface is not firewalled:** The SBC's WAN ENI uses a dedicated Elastic IP with AWS Security Group (L4) rules only. SIP/TLS and SRTP/RTP protocols require direct IP connectivity — reverse proxies and Layer 7 firewalls are incompatible with real-time voice protocols. The SBC provides its own application-layer VoIP firewall for SIP message inspection and rate limiting. See Section 5 External Publishing Patterns for full details.
- **OVOC uses traditional ingress:** OVOC is published via cloud firewall + reverse proxy for inbound Microsoft 365 webhook traffic and admin access. See Section 5 External Publishing Patterns.
- **All SBCs use RADIUS via Cisco ISE:** Both Proxy and Downstream SBCs authenticate against Cisco ISE (RADIUS) with on-premises Active Directory as the identity source. AudioCodes VSA (Vendor ID 5003, ACL-Auth-Level attribute 35) provides role-based access control. TACACS+ is not supported on AudioCodes SBC products. See Section 10.4 for full details.
- **OVOC and ARM use Entra ID:** These components use Microsoft Entra ID (OAuth 2.0) with Conditional Access and MFA support. See Section 6 for app registrations.
- **Cloud east-west firewall:** All internal/private-side traffic traverses a cloud east-west firewall for inspection. The SBC's external WAN interface does not traverse this firewall. See Section 5 Cloud East-West Firewall.
- **OVOC Data Analytics API:** The ETL platform connects to OVOC PostgreSQL (TCP 5432) on the internal subnet for daily data extraction. Traffic traverses the cloud east-west firewall. The `analytics` user is read-only with no write capability. See Section 22A: OVOC Data Analytics and Reporting for full details.

Stack Manager Component

The **AudioCodes Stack Manager** is a new infrastructure component introduced to support High Availability SBC deployments across multiple AWS Availability Zones. A single Stack Manager instance is deployed per

environment in the Australian region (ap-southeast-2), managing SBC HA stacks in both Australian and US regions via cross-region AWS API calls.

Component Classification

Attribute	Value
Component Type	Management/Orchestration VM
Vendor	AudioCodes
Deployment	AWS EC2 (t3.medium)
Network Zone	Management Subnet (Australian region)
Data Classification	Infrastructure Management
New Component	Yes - Required for multi-AZ SBC HA deployment
Deployment Model	One per environment in Australian region; manages all regions via cross-region API

Functional Description

The Stack Manager is a dedicated virtual machine deployed in the Australian region (one per environment) that manages SBC HA stacks across all regions. It performs the following functions:

Primary Functions (Initial Deployment)

1. **CloudFormation Orchestration:** Creates and manages AWS CloudFormation stacks for SBC HA deployment
2. **Network Configuration:** Configures ENIs, security groups, and route table entries for Virtual IPs
3. **Virtual IP Allocation:** Allocates Virtual IPs from the 10.x.x.x range for HA routing
4. **Instance Provisioning:** Deploys SBC EC2 instances with correct IAM roles and network attachments

Day 2 Operations (Ongoing Management)

1. **Software Updates:** Facilitates SBC software upgrades across the HA pair
2. **Stack Healing:** Repairs corrupted cloud resources or misconfigurations
3. **Topology Changes:** Manages changes to SBC cluster topology
4. **Configuration Backup:** Supports configuration backup and recovery operations

What Stack Manager Does NOT Do

- **Does NOT participate in active HA failover** - SBCs handle this directly via AWS API calls
- Does NOT process voice traffic or signalling
- Does NOT store call records or user data
- Does NOT require persistent connections to SBCs during normal operation

IAM Permissions Required

The Stack Manager requires an IAM role with the following permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudformation:*",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:PutMetricAlarm",
                "iam:PassRole",
                "iam:ListInstanceProfiles",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        }
    ]
}
```

Permission Justification

Permission	Justification	Risk Level
`ec2:*`	Required to create/modify EC2 instances, ENIs, security groups, and route tables for SBC deployment. Cannot be reduced (AudioCodes confirmed). Mitigate via temporal IAM elevation.	Medium
`cloudformation:*`	Required to create and manage CloudFormation stacks for infrastructure-as-code deployment. Cannot be reduced. Mitigate via temporal	Medium

	IAM elevation.	
`cloudwatch:DeleteAlarms`, `cloudwatch:PutMetricAlarm`	Required to configure monitoring alarms for SBC health	Low
`iam:PassRole`	Required to assign IAM roles to SBC instances during deployment	Medium
`iam:ListInstanceProfiles`	Required to enumerate available instance profiles for SBC assignment	Low
`iam:CreateServiceLinkedRole`	Required to create service-linked roles for AWS services (e.g., ELB)	Low

Scope Limitation Recommendations

AudioCodes confirms that the broad `ec2:*` and `cloudformation:*` permissions cannot be reduced without breaking Stack Manager functionality. However, the following mitigations are recommended:

1. Temporal IAM Elevation (Primary recommendation)

Detach the Stack Manager IAM policy when not actively performing deployment or Day 2 operations. See Section 20: Temporal IAM Elevation Pattern for the full procedure.

2. Tag-based condition (Additional layer)

For enhanced security posture, consider adding a tag condition to restrict the scope of `ec2:*` to resources tagged with the AudioCodes project:

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "ec2:ResourceTag/Project": "AudioCodes-Voice"
        }
    }
}
```

> **Caveat:** Not all EC2 actions support tag-based conditions. Test thoroughly in non-production before applying to production. CloudFormation stack creation may fail if tag conditions block required actions on untagged resources.

Network Placement

- **Recommended:** Place in internal subnet with VPC Endpoints for AWS API access (no NAT Gateway required)
- **Not Recommended:** Direct internet exposure via public IP
- **Alternative:** NAT Gateway egress if VPC Endpoints are not deployed

> **Note:** For Stack Manager Security Group rules, see Section 5.3 Security Groups.

VPC Endpoints (PrivateLink) — Required for AWS API Access

The following VPC Endpoints eliminate the need for 0.0.0.0/0 outbound rules and keep AWS API traffic within the AWS network. Deploy in each region where SBC infrastructure exists.

Required VPC Endpoints

Service	Endpoint Type	Service Name	Used By
EC2	Interface	`com.amazonaws.<region>.ec2`	SBC HA failover, Stack Manager
S3	Gateway	`com.amazonaws.<region>.s3`	Stack Manager (CloudFormation templates), SBC (firmware, backups)
CloudFormation	Interface	`com.amazonaws.<region>.cloudformation`	Stack Manager
CloudWatch	Interface	`com.amazonaws.<region>.monitoring`	Stack Manager (alarm management)
STS	Interface	`com.amazonaws.<region>.sts`	SBC (IAM role assumption for HA), Stack Manager

Optional VPC Endpoints

Service	Endpoint Type	Service Name	Used By
SSM	Interface	`com.amazonaws.<region>.ssm`	EC2 management

SSM Messages	Interface	`com.amazonaws.<region>.ssmmessages`	Session Manager
CloudWatch Logs	Interface	`com.amazonaws.<region>.logs`	Centralised logging
ELB	Interface	`com.amazonaws.<region>.elasticloadbalancing`	Stack Manager (multi-zone NLB)

VPC Endpoint Security Group

Create a dedicated security group for all Interface VPC Endpoints:

Direction	Protocol	Port	Source/Destination	Purpose
Inbound	TCP	443	SBC HA Subnet CIDR	SBC HA failover API calls
Inbound	TCP	443	Stack Manager SG	Stack Manager API calls
Inbound	TCP	443	VPC CIDR	All VPC instances needing AWS API access

Configuration Notes

1. **Enable Private DNS** on all Interface Endpoints (default). This ensures SDK/CLI calls automatically resolve service hostnames to private endpoint IPs — no application changes required.
2. **Place EC2 endpoint ENI in the HA subnet** to ensure failover API calls do not traverse NAT Gateway.
3. **S3 Gateway Endpoint** is free and adds a prefix list (`pl-xxxxxxxx`) to route tables. Reference this prefix list ID in security group outbound rules.
4. **Cost estimate:** Interface endpoints cost ~$0.01/hour/AZ (~$7.30/month/AZ). With 5 required endpoints across 2 AZs: ~$73/month per region.

Security Considerations

Attack Surface Analysis

Vector	Risk	Mitigation
Web Management Interface	Medium	Restrict to admin CIDR, use strong authentication
SSH Access	Medium	Key-based auth only, restrict to bastion/admin CIDR
IAM Role Compromise	High	Use least-privilege, enable CloudTrail logging
Network Exposure	Low	Private subnet, no public IP, security group restrictions

Data Handling

Data Type	Handled	Storage	Sensitivity
AWS API Credentials	Yes (via IAM Role)	None (instance metadata)	High
SBC Configuration	Yes (during deployment)	Temporary	Medium
Voice/Call Data	No	N/A	N/A
User PII	No	N/A	N/A

Logging and Monitoring

Log Type	Source	Retention Recommendation
AWS API Calls	CloudTrail	90 days minimum
Stack Manager System Logs	EC2 instance	30 days
CloudFormation Events	CloudFormation	90 days

Compliance Considerations

SOC 2 Relevance

- Stack Manager has elevated AWS permissions - ensure access is restricted and logged
- Include in quarterly access reviews
- Document change management procedures for Stack Manager operations

PCI-DSS Relevance

- Stack Manager does not process, store, or transmit cardholder data
- Included in scope as supporting infrastructure if voice system handles

payment card information

Risk Assessment Summary

Risk Category	Rating	Notes
Confidentiality	Low	Does not handle sensitive user/call data
Integrity	Medium	Has ability to modify infrastructure; changes are logged
Availability	Low	Not in critical path for call processing; SBCs handle failover independently
Overall Risk	Medium	Elevated AWS permissions require appropriate access controls

Approval Checklist

- ☐ IAM role created with documented permissions
- ☐ Security group restricts access to admin CIDR only
- ☐ CloudTrail logging enabled for AWS API calls
- ☐ Break glass account configured and documented
- ☐ Placed in private subnet with NAT Gateway egress
- ☐ Access restricted to authorized personnel only
- ☐ Included in vulnerability scanning scope
- ☐ Change management process documented

---

22. Licensing Considerations

Mediant VE SBC Licensing

Model	Description	Procurement	Notes
BYOL	Bring Your Own License	Purchase from AudioCodes, request via BYOL form	License file applied to SBC

PAYG	Pay-As-You-Go	Consumed via AWS Marketplace billing	Hourly billing through AWS
Capacity	Session-based licensing	Based on concurrent sessions	Scale license with capacity needs

ARM Licensing

- Obtained directly from AudioCodes
- Configured via ARM Configurator web interface
- License types include:
  - **Base license:** Required for all deployments
  - **Router license:** Per-router licensing
  - **Advanced features:** Additional licensing for premium features

OVOC Licensing

- Obtained directly from AudioCodes
- Based on number of managed devices
- License tiers:
  - **Device count:** Number of SBCs and endpoints managed
  - **Analytics license: Required for Teams QoE integration**
  - **Data Analytics API license: Required for direct PostgreSQL access to OVOC analytics views** (SW/OVOC/ANALYTICS — “Analytic API Voice Quality”)
  - **Advanced reporting:** Optional enhanced reporting features

---

22A. OVOC Data Analytics and Reporting

Overview

OVOC stores Quality of Experience (QoE), Call Detail Record (CDR), alarm, and topology data in a local PostgreSQL database (`dbems`). By default, the analytics data views retain only the **last 24 hours** of data. This section documents how to extract that data daily to a corporate data lake and surface it via Power BI for historical reporting and trend analysis.

OVOC Data Analytics API

The OVOC Data Analytics API is **not a REST API** — it provides direct read-only PostgreSQL (SQL) access to pre-defined database views.

Attribute	Detail

Protocol	PostgreSQL wire protocol
Port	TCP 5432
Database	`dbems`
User	`analytics` (read-only, SELECT only)
Access type	SQL queries against pre-defined views
License required	"Analytic API Voice Quality" (SW/OVOC/ANALYTICS) — see Section 22

Available Database Views

View	Category	Description
`NODES_VIEW`	Topology	Device and node details (SBCs, gateways, IP phones)
`LINKS_VIEW`	Topology	Network link information between nodes
`CALLS_VIEW`	QoE	Individual call records with quality metrics (MOS, jitter, packet loss)
`ALARMS_VIEW`	Alarms	Active and historical alarm data
`NODES_SUMMARY_VIEW`	QoE	Aggregated node-level quality statistics
`LINKS_SUMMARY_VIEW`	QoE	Aggregated link-level quality statistics

In addition to the 6 primary views above, OVOC provides **28 enumeration/lookup views** for decoding integer codes (e.g., alarm severity levels, codec types, call termination reasons) into human-readable values.

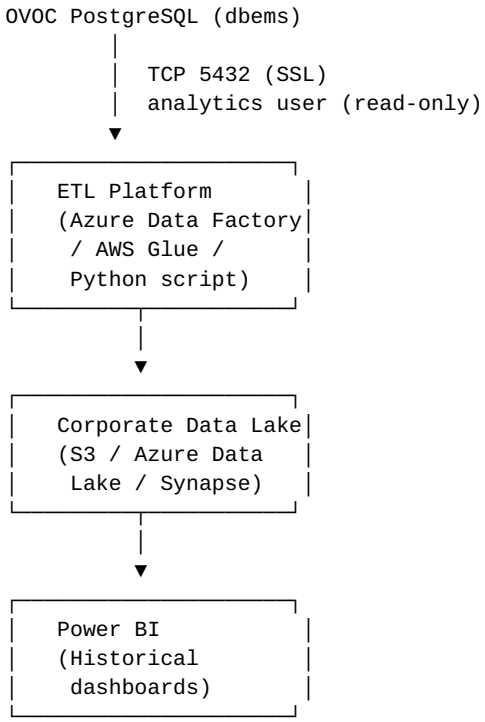
Data Retention Constraints

Constraint	Detail
Default analytics window	Last 24 hours
Access mode	Read-only (SELECT only)
Change tracking	None — no CDC, no cursors, no change data capture
Multitenancy	Not supported — all data visible to the `analytics` user

> **CRITICAL:** The analytics views expose a rolling 24-hour window. If a daily extraction is missed, that day's data is **permanently lost** and cannot be recovered from OVOC. ETL job monitoring and alerting is essential.

Data Lake Integration Architecture

The recommended architecture extracts data daily from OVOC and loads it into a corporate data lake for long-term retention and reporting:



ETL Pipeline Steps:

1. **Schedule:** Daily extraction, timed to run within the 24-hour analytics window (e.g., 02:00 AEST)
2. **Connect:** ETL platform connects to OVOC PostgreSQL on port 5432 via the `analytics` user with SSL
3. **Extract:** Query all 6 primary views plus required enumeration views (full 24-hour window)
4. **Transform:** Decode integer codes using enumeration views, add extraction timestamp, de-duplicate if needed
5. **Load:** Write to corporate data lake in partitioned format (e.g., by date)
6. **Validate:** Confirm row counts and data completeness; alert on zero-row extractions

Power BI Configuration

Aspect	Recommendation
Data source	Corporate data lake (not OVOC directly)

Refresh schedule	Daily, after ETL completes
Direct OVOC connection	Not recommended for production — 24-hour window only, no historical data
Dashboard examples	Call quality trends (MOS over time), alarm frequency, top talkers, codec distribution

Cyber Security Considerations

Network Access

- Port 5432 must be opened from the ETL platform to OVOC on the internal subnet
- Traffic should traverse the cloud east-west firewall (internal subnet) for inspection and logging
- PostgreSQL connections must use SSL encryption (`sslmode=require` in the connection string)

Credential Management

- The `analytics` user password is managed via the OVOC Application Maintenance CLI
- Store the password in the organisation's secrets manager (e.g., AWS Secrets Manager, Azure Key Vault)
- Rotate the password per the organisation's credential rotation policy
- Do not embed credentials in ETL scripts or source code

Access Control

- The `analytics` user has **read-only (SELECT only)** access — no write, update, delete, or DDL capability
- Access is limited to pre-defined views only — the user cannot access underlying database tables
- No multitenancy filtering — all data across all managed devices is visible to the `analytics` user

Data Classification

- CDR data contains call metadata: source/destination numbers, timestamps, duration, codec
- QoE data contains voice quality metrics: MOS scores, jitter, packet loss, round-trip time
- Alarm data contains infrastructure event details
- Classify as per organisation policy — likely **Internal/Confidential**
- Ensure the data lake storage tier, encryption, and access controls meet the classification requirements

Logging and Monitoring

Log Source	What to Monitor

OVOC PostgreSQL connection logs	Successful/failed connection attempts from ETL platform
ETL job execution logs	Job success/failure, row counts, extraction duration
Data lake access logs	Who accesses the extracted data
Power BI audit logs	Dashboard access and data refresh events

> **CRITICAL:** Monitor for failed ETL extractions. A missed extraction means that day's data is permanently lost. Configure alerting on ETL job failures with escalation to the operations team.

CDR Access Auditing — Who Accessed What

A key compliance question is: **can the organisation log and audit who has accessed CDR data through the Analytics API?**

OVOC does not natively log individual SQL queries made through the Analytics API. The OVOC application-level audit trail (Actions Journal) covers GUI-based operator actions but does not extend to raw SQL sessions initiated via the PostgreSQL direct-access interface (port 5432). This means that if someone connects with the `analytics` user and runs SELECT queries against CDR views, OVOC itself does not record the query content.

However, a layered auditing approach can be implemented to achieve compliance-grade CDR access logging:

Layer 1: PostgreSQL Native Logging

PostgreSQL's built-in logging can be configured on the OVOC server to capture all connections and SQL statements. The following `postgresql.conf` parameters are relevant:

Parameter	Recommended Value	Purpose
`log_connections`	`on`	Logs every connection attempt including username, database, and source IP
`log_disconnections`	`on`	Logs session end with duration
`log_statement`	`'all'`	Logs all SQL statements including SELECTs against CDR

		views
`log_duration`	`on`	Logs how long each statement took
`log_line_prefix`	`'%t [%p]: user=%u,db=%d,app=%a,client=%h '`	Includes timestamp, user, database, application name, and client IP in every log line

> **Appliance Caveat:** Since OVOC is a managed appliance, direct modification of `postgresql.conf` may not be officially supported by AudioCodes and could be overwritten during upgrades. Contact AudioCodes support to confirm supportability before modifying the embedded PostgreSQL configuration.

Layer 2: pgAudit Extension (If Supportable)

The **pgAudit** PostgreSQL extension provides granular, object-level audit logging that can target specific CDR views rather than logging all database activity. With pgAudit, audit entries are generated when any user runs a SELECT against a designated view (e.g., `CALLS_VIEW`), including the full SQL statement and bind parameters.

pgAudit is supported natively on AWS RDS PostgreSQL and can be installed on self-hosted PostgreSQL instances. However, installing pgAudit on the OVOC embedded PostgreSQL instance would require root access and is not officially documented by AudioCodes. If the organisation replicates CDR data to an external PostgreSQL instance (e.g., in the data lake), pgAudit can be deployed there without modifying the OVOC appliance.

Layer 3: Network-Level Logging

Network-level controls provide an independent audit trail of who connected to the Analytics API:

Control	What It Captures
AWS VPC Flow Logs	Source IP, destination IP (OVOC), port 5432, connection timestamps, accept/reject
Cloud East-West Firewall Logs	Connection metadata for traffic traversing the internal firewall to OVOC
OVOC Linux auditd	OS-level socket activity on port 5432 (when auditd is enabled via OVOC Server Manager)

Layer 4: Data Lake Access Auditing

Since CDR data is extracted daily to the corporate data lake, the data lake tier provides a more controllable audit point:

Platform	Audit Capability
AWS S3 + Athena	S3 access logging, CloudTrail data events, Athena query execution logs
Azure Data Lake + Synapse	Azure Monitor diagnostic logs, Synapse SQL audit logs
Power BI	Power BI audit logs capture dashboard access, report views, and data refresh events per user

For most compliance scenarios, auditing at the **data lake tier** (Layer 4) is more practical and controllable than auditing at the OVOC PostgreSQL tier (Layer 1), because the data lake supports individual user accounts, role-based access, and native audit logging — whereas OVOC provides only a single shared `analytics` account.

Shared Account Limitation

A significant limitation is that OVOC provides a **single shared `analytics` user** for all external database access. PostgreSQL logs will show `user=analytics` for every connection, making it impossible to distinguish between different human analysts or ETL service accounts at the database level alone.

Mitigations:

Approach	How It Works
IP-based attribution	If each connecting system has a known IP, `log_connections` captures the `client` field to differentiate sources
Application name tagging	Configure each connecting tool (ETL platform, Power BI, ad-hoc clients) to set a unique `application_name` in its PostgreSQL connection string — this appears in `log_line_prefix` with `%a`
Restrict to ETL only	Limit port 5432 access via firewall rules to the ETL platform IP only — no ad-hoc analyst access to OVOC directly. All analyst access goes through the data lake where individual user accounts and audit logging are available
Database proxy	Deploy a PostgreSQL proxy (e.g., PgBouncer) that maps individual user credentials to the shared `analytics` backend user, logging the actual user identity at the proxy layer

Compliance Summary

Compliance Question	How to Answer It
Who accessed CDR data on OVOC?	PostgreSQL `log_connections` (source IP + timestamp) combined with VPC Flow Logs and firewall logs
What CDR queries were executed?	PostgreSQL `log_statement='all'` or pgAudit with `pgaudit.log='read'` — captures full SQL text
When was CDR data accessed?	`log_line_prefix` with `%t` timestamp, VPC Flow Log timestamps
What data was extracted to the data lake?	ETL job execution logs with row counts and extraction timestamps
Who accessed CDR data in the data lake?	Data lake native audit logs (S3 access logs, Athena query logs, Synapse audit logs)
Who viewed CDR dashboards?	Power BI audit logs per user per report
Is the audit trail tamper-proof?	Ship logs in real-time to an immutable store (e.g., S3 with Object Lock, Azure Immutable Blob Storage) separate from the OVOC appliance

> **Recommendation:** For most organisations, the practical approach is to (1) restrict OVOC Analytics API access to the ETL platform only via firewall rules, (2) enable PostgreSQL `log_connections` on OVOC for basic connection auditing, (3) implement comprehensive audit logging at the data lake tier where individual user accounts and native audit capabilities are available, and (4) forward all logs to the organisation's SIEM for centralised audit trail and alerting.

CDR Viewing via the OVOC Web GUI — Audit Limitation

There is no native capability within OVOC to log or audit which operator viewed specific CDR records, call quality data, or QoE reports through the web GUI. This is a platform limitation that cannot be addressed without considerable modification to the underlying operating system and web server stack.

The OVOC **Actions Journal** tracks operator *actions* (configuration changes, device updates, operator management, security level changes) but does **not** track operator *page views* or *data reads*. When an operator browses CDR

search results, views call quality reports, or accesses QoE dashboards through the OVOC web interface, no audit record is generated. The Journal is fundamentally a change log, not an access log.

This means the organisation **cannot** answer the question *"Which operator viewed CDR data for call X on date Y?"* using OVOC's built-in features.

Why This Limitation Exists

This is a common gap across enterprise management platforms — not specific to AudioCodes. Most web applications log write operations (which are transactional and infrequent) but not read operations (which are high-volume and generate significant storage and performance overhead). OVOC's architecture uses a shared application service account for database queries, decoupling the web user session from the underlying data retrieval.

What Cannot Be Achieved Without OS-Level Modification

Audit Question	Native OVOC Capability
Which operator viewed a specific CDR record?	**Not available**
When did an operator access call quality reports?	**Not available**
How many CDR records did an operator view in a session?	**Not available**
Did an operator search for a specific phone number?	**Not available**
Which operator exported CDR data from the GUI?	**Not available**

Mitigations

The following compensating controls can reduce the risk associated with this limitation:

1. Role-Based Access Control (Preventive)

OVOC's built-in operator security levels (Admin, Operator, Monitor) and tenant-scoped access control who *can* view CDR data. While this does not log who *did* view it, it limits the population of users with access and provides a defensible answer to auditors about who *could have* accessed the data.

2. GDPR Phone Number Masking (Data Minimisation)

OVOC supports **Privacy Mode** which masks phone numbers in CDRs, call details, and QoE reports displayed in the GUI. When enabled, standard operators see masked numbers (e.g., `+61 2 9876 ****`) and cannot identify individuals from the displayed data. This reduces the classification of viewed data and makes the "who viewed what" question less critical — if users only see masked data, they have not accessed identifiable personal information.

3. Web Server Access Log Enhancement (Requires OS Modification)

OVOC runs on Apache and Tomcat. Configuring Apache access logs and Tomcat's `AccessLogValve` to capture authenticated usernames and request URLs can provide a partial audit trail showing which operators accessed CDR-related pages. However, this requires root-level modification to the OVOC server, is not officially supported by AudioCodes, and may be overwritten during OVOC upgrades.

Limitations of this approach: - Access logs show URLs requested but not which records were in the response - POST-based search forms do not appear in standard access logs - OVOC's SPA (single-page application) architecture uses generic REST API endpoints, making URL-based analysis difficult (e.g., a CDR query may appear as `POST /api/v1/calls/search` rather than a descriptive URL) - No correlation between the web user and the underlying database query without significant custom engineering

4. Linux auditd (Requires OS Modification)

Enabling auditd via the OVOC Server Manager (Security > Auditd Options) captures OS-level activity including network socket connections and file access. Custom auditd rules can be written to monitor CDR-related database files or API socket connections. However, auditd operates at the kernel/syscall level and cannot correlate database queries with specific OVOC GUI user sessions without significant custom engineering.

5. Network-Level Monitoring (No OS Modification Required)

Monitoring connections to the OVOC HTTPS interface via VPC Flow Logs and cloud east-west firewall logs provides an independent record of which source IPs accessed the OVOC web GUI and when. Combined with OVOC's authentication logs (login/logout events), this can establish which operators had active sessions during a given time window — though it cannot determine what data they viewed within those sessions.

6. Reverse Proxy with Enhanced Logging (No OVOC Modification Required)

Deploying a reverse proxy (e.g., Nginx, HAProxy) in front of the OVOC web interface — separate from the OVOC appliance — can log all authenticated requests including URLs, query parameters, and authenticated usernames without modifying the OVOC server itself. This is the least invasive approach but is still subject to the SPA/REST API URL limitations described above.

7. Data Lake as the Controlled Access Point

For compliance-sensitive environments, the most practical approach is to direct all analyst and reporting access to the **data lake** (where individual user accounts, query logging, and native audit capabilities are available) rather than granting operators direct access to CDR data through the OVOC GUI. OVOC GUI access can be restricted to operational monitoring only, with phone number masking enabled for all standard operators.

Risk Acceptance

If the mitigations above are insufficient for the organisation's compliance requirements, this limitation should be documented in the risk register:

> *"The OVOC platform does not provide application-level audit logging of CDR data viewing events through the web GUI. Compensating controls including role-based access control, phone number masking, network-level monitoring, and data lake access auditing reduce the residual risk. This is accepted by [Risk Owner] and will be reviewed annually or upon OVOC version upgrade."*

Licensing Prerequisite

The OVOC Data Analytics API requires the **"Analytic API Voice Quality"** license (SW/OVOC/ANALYTICS). This is separate from the base OVOC license and the Teams QoE Analytics license. See Section 22: Licensing Considerations.

---

23. References and Documentation

23.1 Official AudioCodes Documentation

Document	Version	URL
Mediant VE SBC for AWS Installation Manual	7.4	PDF
Mediant VE SBC for AWS Installation Manual	7.6	PDF
Stack Manager User's Manual	7.4	PDF
Stack Manager User's Manual	7.6	PDF
ARM Installation Manual	10.0	PDF
ARM User's Manual	9.8	Web
ARM Azure AD Configuration	10.0	Web
OVOC IOM Manual	8.2	PDF
OVOC Server Requirements	8.4	Web

Configure Microsoft Graph API	-	Web
SBC Teams Direct Routing Config	-	PDF

23.2 Microsoft Documentation

Document	URL
Plan Direct Routing	Microsoft Learn
Connect SBC to Direct Routing	Microsoft Learn
Configure Direct Routing	Microsoft Learn
Direct Routing SIP Protocol	Microsoft Learn
Enable Users for Direct Routing	Microsoft Learn
Teams Administrator Roles	Microsoft Learn
Microsoft Graph CallRecords API	Microsoft Learn
Microsoft Trusted Root Certificate Program	Microsoft Learn

23.3 AudioCodes Product Pages

Product	URL
Mediant VE SBC	Product Page
ARM	Product Page
OVOC	Product Page
Device Manager	Product Page

23.4 AWS Marketplace Links

Product	URL
Mediant VE SBC (BYOL)	AWS Marketplace
Mediant VE SBC (PAYG)	AWS Marketplace
Stack Manager	AWS Marketplace
ARM	AWS Marketplace

23.5 Third-Party References

Source	Description	URL
Shawn Harry Blog	Enabling Teams QoE in OVOC	Link
CanUCThis	Installing OVOC Guide	Link
Erik365 Blog	Teams Direct Routing Certificate Changes (2026)	Link
AudioCodes		

Community	AudioCodes Technical Forums	Link

Appendix A: Deployment Checklist

Pre-Deployment

- ☐ AWS Account access confirmed
- ☐ VPC and subnet design finalized
- ☐ Security groups designed and documented
- ☐ IAM policy and role created for Stack Manager (AU region, with cross-region permissions)
- ☐ Key pairs created
- ☐ AudioCodes licensing obtained (or PAYG decision made)
- ☐ Public CA certificates procured for SBCs and OVOC
- ☐ Domain registered and verified in Microsoft 365 tenant
- ☐ DNS records planned

Microsoft Entra ID Configuration

- ☐ OVOC App Registration created
- ☐ ARM WebUI App Registration created
- ☐ SBC App Registration created (if SBA required)
- ☐ All API permissions configured
- ☐ Admin consent granted for all app registrations
- ☐ All credentials documented securely
- ☐ Client secret expiry dates calendared

Break Glass Accounts

- ☐ Secret repository structure created
- ☐ All break glass accounts created on appliances
- ☐ All passwords stored securely in secret repository
- ☐ Access procedures documented
- ☐ Dual-control access configured
- ☐ Break glass account testing scheduled

Component Deployment

- ☐ Stack Manager deployed in Australian region and verified
- ☐ Stack Manager IAM role attached (cross-region permissions for AU + US)
- ☐ SBC HA pair deployed via Stack Manager (AU region; US region via cross-region API)
- ☐ TLS certificates installed on SBCs
- ☐ SBC HA failover tested
- ☐ ARM Configurator deployed
- ☐ ARM Configurator OAuth configured

- [ ] ARM Router(s) deployed
- [ ] ARM licensing applied
- [ ] OVOC deployed (production only)
- [ ] OVOC public certificate installed
- [ ] All break glass accounts tested

Integration Verification

- [ ] OAuth authentication working for all components
- [ ] OVOC receiving Teams QoE data
- [ ] SBCs registered in Teams Admin Center
- [ ] Voice routing policies configured
- [ ] PSTN usages configured
- [ ] Test users enabled for Direct Routing
- [ ] End-to-end calling tested
- [ ] HA failover tested and documented
- [ ] Monitoring and alerting configured

Appendix B: Credentials Reference Template

App Registration Credentials

App Registration	Tenant ID	Client ID	Secret Expiry	Notes
AudioCodes-OVOC-Teams-Integration	_____	_____	_____	OVOC Teams QoE
AudioCodes-ARM-WebUI	_____	_____	_____	ARM Web Interface
AudioCodes-SBC-DirectRouting	_____	_____	_____	SBA Functionality

Break Glass Account Reference

Component	Environment	Username	Secret Path
Stack Manager	Non-Prod	`breakglass-stackmgr-nonprod`	`/audiocodes/nonprod/breakgl stackmgr-nonprod`
SBC #1	Non-Prod	`breakglass-sbc1-nonprod`	`/audiocodes/nonprod/breakgl sbc1-nonprod`
SBC #2	Non-Prod	`breakglass-sbc2-nonprod`	`/audiocodes/nonprod/breakgl sbc2-nonprod`

ARM Configurator	Non-Prod	`breakglass-armcfg-nonprod`	`/audiocodes/nonprod/breakgl armcfg-nonprod`
ARM Router	Non-Prod	`breakglass-armrtr-nonprod`	`/audiocodes/nonprod/breakgl armrtr-nonprod`
Stack Manager	Prod AUS	`breakglass-stackmgr-prod-aus`	`/audiocodes/prod-aus/breakglass-stackmgr-prc aus`
SBC #1	Prod AUS	`breakglass-sbc1-prod-aus`	`/audiocodes/prod-aus/breakglass-sbc1-prod-au`
SBC #2	Prod AUS	`breakglass-sbc2-prod-aus`	`/audiocodes/prod-aus/breakglass-sbc2-prod-au`
OVOC	Prod	`breakglass-ovoc-prod`	`/audiocodes/prod-aus/breakglass-ovoc-prod`
ARM Configurator	Prod	`breakglass-armcfg-prod`	`/audiocodes/prod-aus/breakglass-armcfg-prod`
ARM Router	Prod AUS	`breakglass-armrtr-prod-aus`	`/audiocodes/prod-aus/breakglass-armrtr-prod-`
SBC #1	Prod US	`breakglass-sbc1-prod-us`	`/audiocodes/prod-us/breakgl sbc1-prod-us`
SBC #2	Prod US	`breakglass-sbc2-prod-us`	`/audiocodes/prod-us/breakgl sbc2-prod-us`
ARM Router	Prod US	`breakglass-armrtr-prod-us`	`/audiocodes/prod-us/breakgl armrtr-prod-us`

Note: Never store actual credentials in this document. Use the secret repository paths to retrieve credentials when needed.

Appendix C: Quick Reference Tables

Port Summary

Signalling Ports

Component	Protocol	Port	Direction	Purpose
SBC	TCP/TLS	5061	Inbound/Outbound	SIP Signalling (Teams

				Direct Routing)
SBC	TCP/UDP	5060	Inbound	SIP Signalling (Unencrypted - Internal)
SBC	TCP	443	Inbound	HTTPS Management
SBC	TCP	22	Inbound	SSH Management
ARM	TCP	443	Inbound	HTTPS Web UI / REST API
ARM	TCP	22	Inbound	SSH Management
OVOC	TCP	443	Inbound	HTTPS Web UI
OVOC	UDP	162	Inbound	SNMP Traps from SBCs
OVOC	TCP	5001	Inbound	QoE Reporting from SBCs
OVOC	TCP	5432	Inbound	Analytics API (PostgreSQL) from ETL Platform
Stack Manager	TCP	443	Inbound	HTTPS Management
Stack Manager	TCP	22	Inbound	SSH Management
Stack Manager	TCP	443	Outbound	AWS API Access

Media Ports

Component	Protocol	Port Range	Direction	Purpose
SBC	UDP	6000-19999	Inbound/Outbound	RTP Media (Internal/Downstre
SBC	UDP	20000-21999	Inbound/Outbound	SRTP Media (Teams Direct Routing)
SBC	UDP	30000-39999	Inbound/Outbound	RTP Media (LMO)
SBC	UDP	40000-41999	Inbound/Outbound	RTP Media (PSTN)
SBC	UDP	49152-53247	Outbound	Microsoft Teams Media

IP Range Summary (Microsoft Teams)

Purpose	IP Ranges	Protocol	Ports
Teams Media	52.112.0.0/14	UDP	49152-53247
Teams Media	52.120.0.0/14	UDP	49152-53247
Teams Signalling	sip.pstnhub.microsoft.com	TCP/TLS	5061
Teams Signalling	sip2.pstnhub.microsoft.com	TCP/TLS	5061
Teams Signalling	sip3.pstnhub.microsoft.com	TCP/TLS	5061
Microsoft Graph API	graph.microsoft.com	TCP/HTTPS	443
Azure AD Authentication	login.microsoftonline.com	TCP/HTTPS	443

Instance Type Summary

Component	Environment	Instance Type	vCPUs	Memory	Storage
Stack Manager	All (hosted in AU region)	t3.medium	2	4 GiB	8 GiB gp3
Mediant VE SBC (No Transcoding)	All	m5n.large	2	8 GiB	20 GiB gp3
Mediant VE SBC (With Transcoding)	All	c5.2xlarge	8	16 GiB	20 GiB gp3
ARM Configurator	All	m4.xlarge	4	16 GiB	100 GB gp3
ARM Router	All	m4.large	2	8 GiB	80 GB gp3
OVOC (Low Profile)	Production	m5.2xlarge	8	32 GiB	500 GiB gp3
OVOC (High Profile)	Production	m5.4xlarge	16	64 GiB	2 TiB gp3

Appendix D: Network Flow Diagrams

This appendix provides visual representations of all network flows in the AudioCodes SBC architecture.

D.1 High-Level Architecture Overview

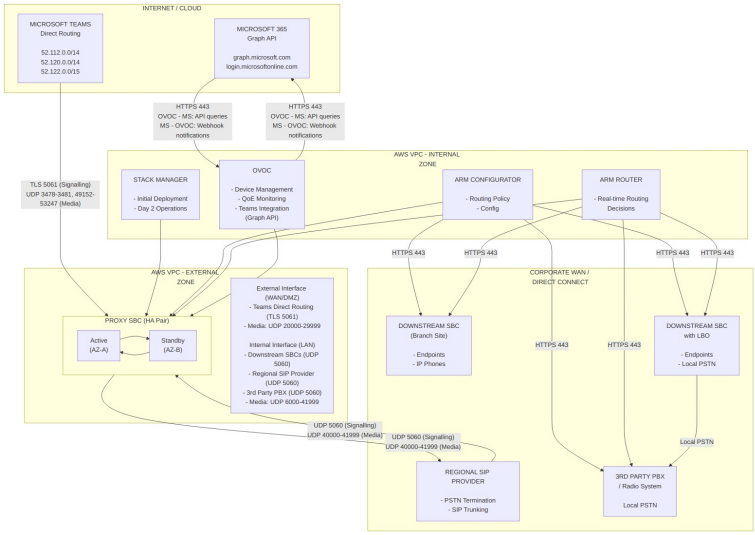


Diagram 12

D.2 SIP Signalling Flows

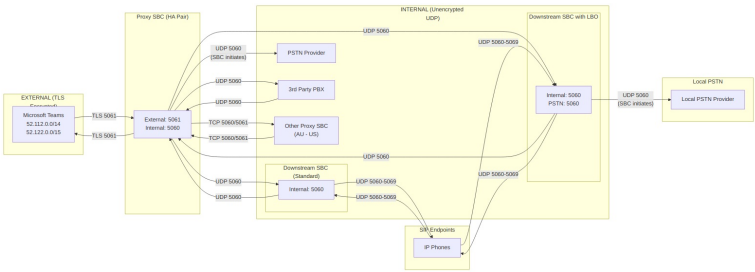


Diagram 13

D.3 Media (RTP/SRTP) Flows

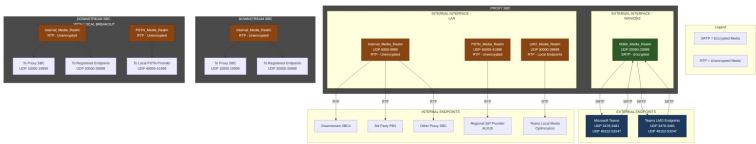


Diagram 14

D.4 Management & Monitoring Flows

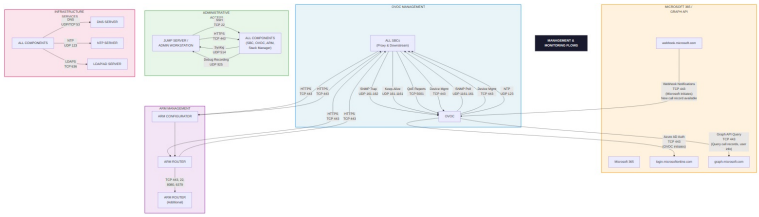


Diagram 15

> **IMPORTANT:** OVOC must be reachable from Microsoft 365 IPs on TCP 443 for webhooks

---

D.5 Call Flow Examples

Example 1: Teams User to PSTN (via Proxy SBC)

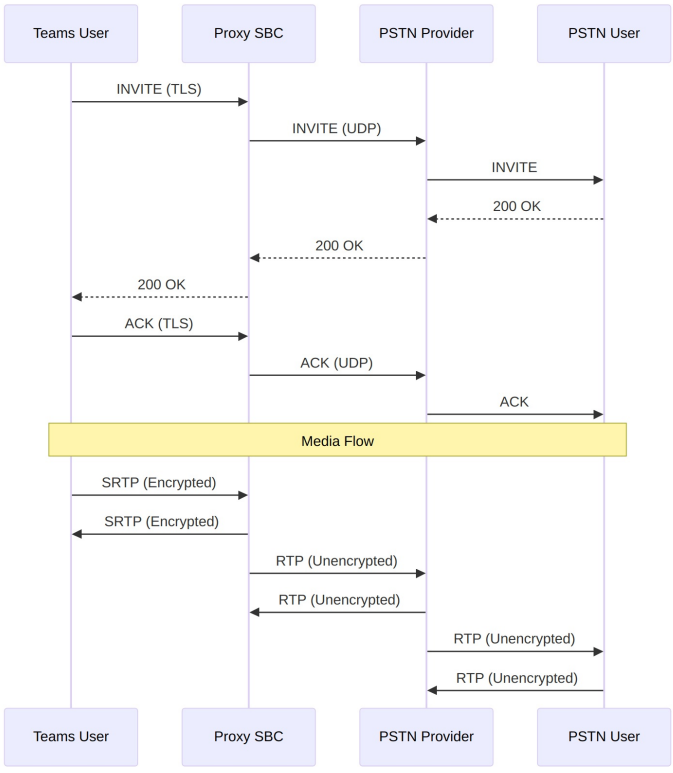


Diagram 16

Example 2: PSTN to Downstream SBC Endpoint

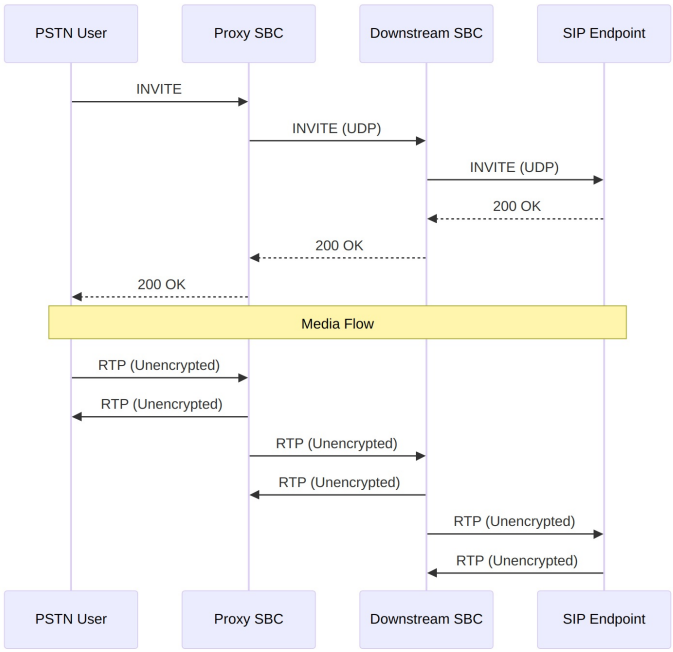


Diagram 17

D.6 Port Summary Quick Reference

Flow Type	Source	Destination	Protocol	Ports	Encrypti
Signalling					
Teams → Proxy SBC	Microsoft 365	Proxy SBC (WAN)	TCP	5061	TLS
Proxy SBC → Teams	Proxy SBC (WAN)	Microsoft 365	TCP	5061	TLS
Internal SIP	Any Internal	Proxy SBC (LAN)	TCP/UDP	5060, 5061	None/TLS
Endpoint SIP	Endpoints	Downstream SBC	UDP	5060-5069	None
Media					
Teams Media	Microsoft 365	Proxy SBC (WAN)	UDP	20000-21999	SRTP
LMO Media	Teams Endpoints	SBC	UDP	30000-39999	RTP
Internal Media	Downstream SBC	Proxy SBC	UDP	10000-19999	RTP
PSTN Media	SBC / PSTN Provider	PSTN Provider / SBC	UDP	40000-41999	RTP
3rd Party PBX Media	Internal Systems	Proxy SBC	UDP	6000-9999	RTP
Management					

SNMP Traps	SBC	OVOC	UDP	162	None
QoE Reports	SBC	OVOC	TCP	5001	TLS
Device Mgmt	OVOC/ARM	SBC	TCP	443	HTTPS
SSH	Admin	All Components	TCP	22	SSH
Graph API (queries)	OVOC	Microsoft	TCP	443	HTTPS
Graph API (webhooks)	Microsoft	OVOC	TCP	443	HTTPS

> **Note:** Graph API traffic is bidirectional. OVOC initiates outbound queries to graph.microsoft.com, while Microsoft sends inbound webhook notifications to OVOC when new call records are available. OVOC must be reachable from Microsoft 365 IPs.

D.7 Microsoft Teams IP Ranges Quick Reference

Range	CIDR	Purpose
52.112.0.0/14	52.112.0.0 - 52.115.255.255	Teams Signalling & Media
52.120.0.0/14	52.120.0.0 - 52.123.255.255	Teams Media Relays
52.122.0.0/15	52.122.0.0 - 52.123.255.255	Teams Signalling
13.107.64.0/18	13.107.64.0 - 13.107.127.255	Teams STUN/TURN

> **Note:** Always verify current IP ranges at: https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges

---

D.8 Comprehensive Interface Mapping - All Appliances

This section provides detailed low-level interface mappings for all AudioCodes appliances in the solution, showing physical ports, ethernet groups, IP interfaces, media realms, and SIP interface bindings.

D.8.1 Proxy SBC (AWS) - Complete Interface Architecture

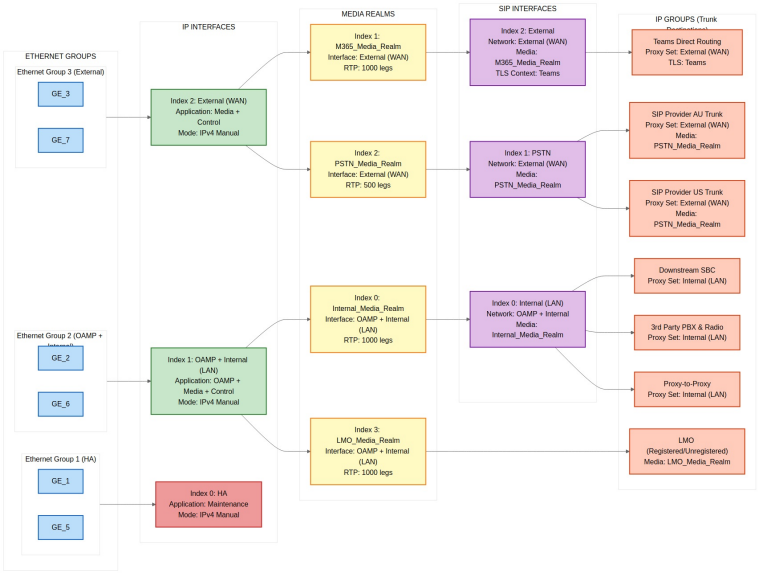


Diagram 18

D.8.2 Downstream SBC (On-Premises Mediant 800) - Complete Interface Architecture

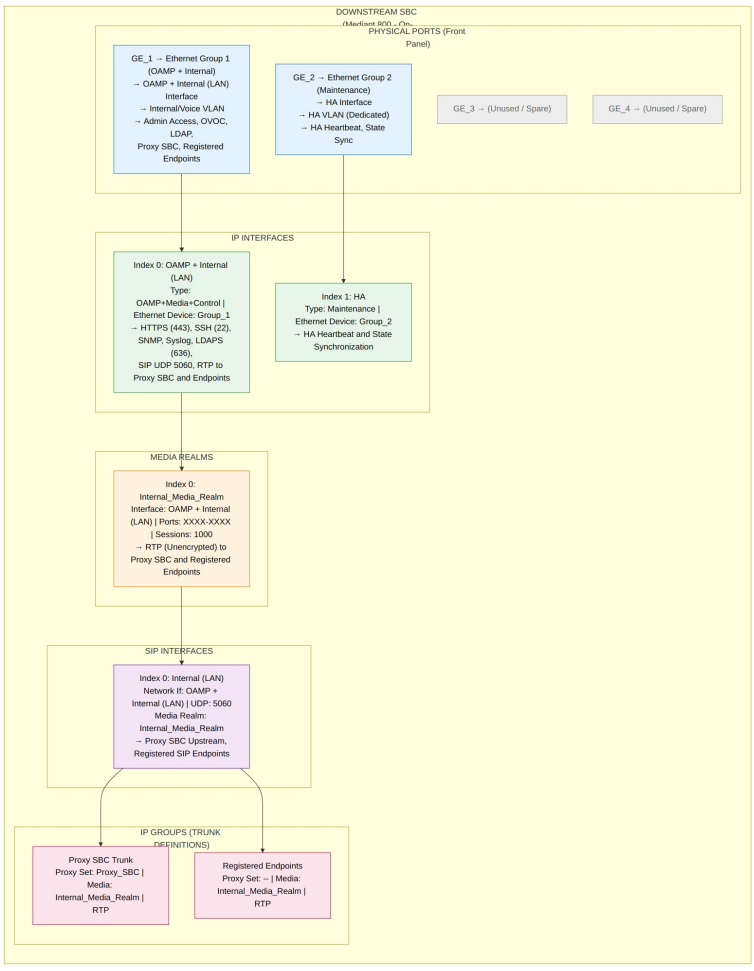


Diagram 19

D.8.3 Downstream SBC with Local Breakout (LBO) - Complete Interface Architecture

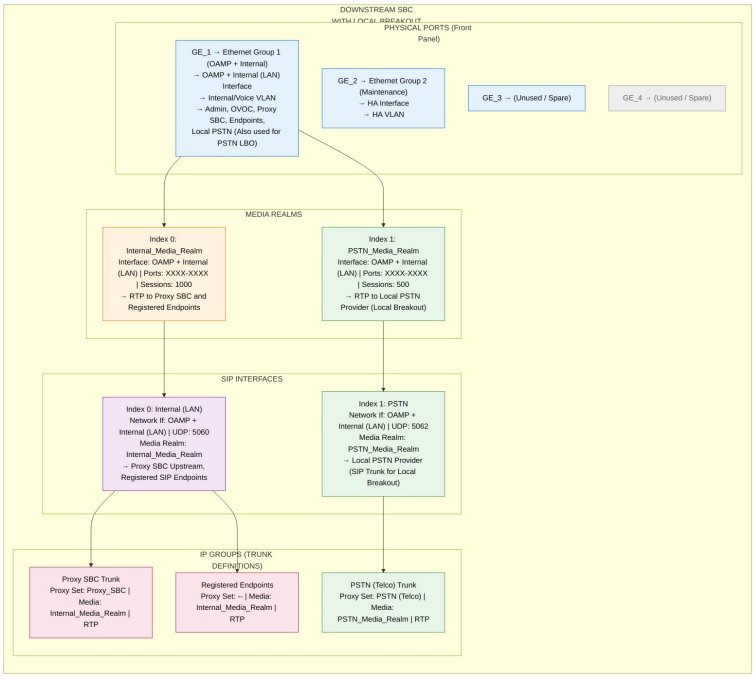


Diagram 20

D.8.4 OVOC - Interface Architecture

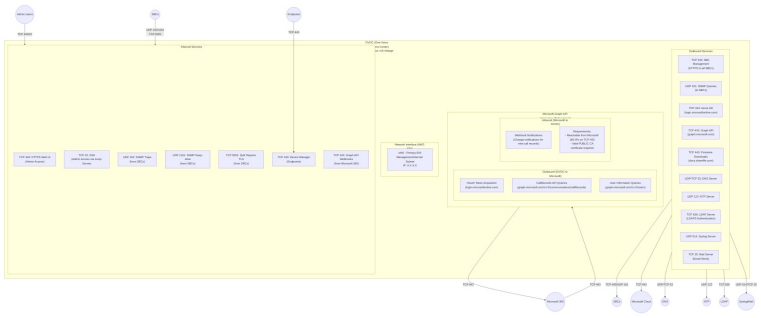


Diagram 21

D.8.5 ARM (AudioCodes Routing Manager) - Interface Architecture

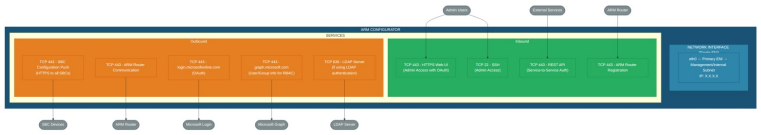


Diagram 22

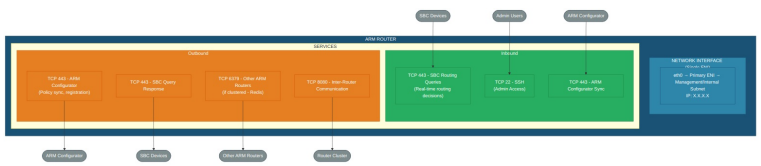


Diagram 23

D.8.6 Stack Manager - Interface Architecture

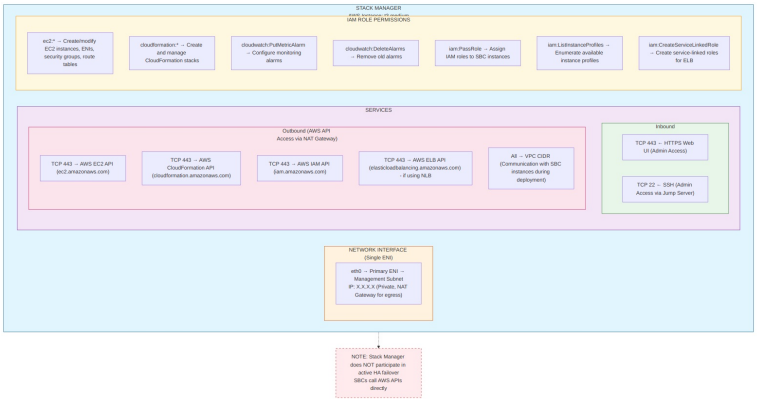


Diagram 24

D.8.7 Complete Solution - End-to-End Connectivity Map

How Traffic Flows Through the SBC

The diagram below shows the SBC as a “gateway” device. Think of it like a security checkpoint at an airport - calls enter on one side, get inspected and processed, then exit on the other side to reach their destination.

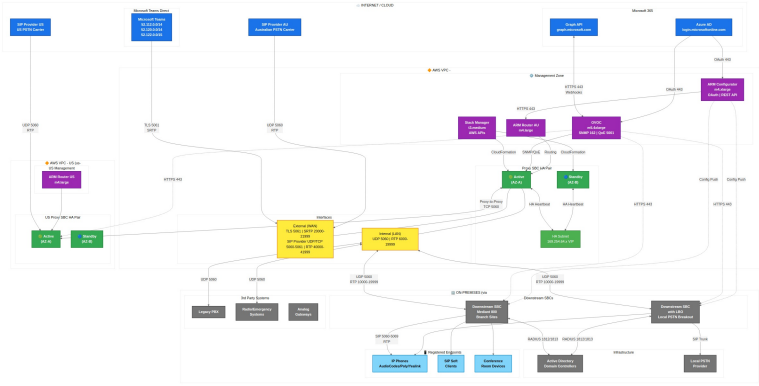


Diagram 25

Interface Summary (from D.8.8 Matrix):

Interface	Port	IP Interface	SIP Interface(s)	Media Realm(s)	Connects To
eth0	GE_1	HA	N/A	N/A	Standby SBC (heartbeat & state sync)
eth1	GE_2	OAMP + LAN	Internal	Internal, LMO	OVOC, Stack Manager, Downstream SBCs, IP Phones

eth2	GE_3	WAN	External	M365, PSTN	Teams (bidirectional), SIP Provider AU/US

Key Concepts: - **eth0 (HA)** - Dedicated HA communication link to keep the Standby SBC synchronised, plus AWS API access for HA failover route table updates - **eth1 (OAMP + LAN)** - Combined management and internal interface carrying admin access (HTTPS, SSH, SNMP) and internal SIP signalling/media for branch offices and phones - **eth2 (WAN)** - The external interface handles TWO types of traffic: - **Microsoft Teams**: Bidirectional (Teams calls in, your calls out to Teams) - **SIP Provider**: SBC initiates registration; media and SIP signalling flows are **bidirectional** from a firewall perspective

---

Detailed Technical View: AWS Infrastructure & HA Failover

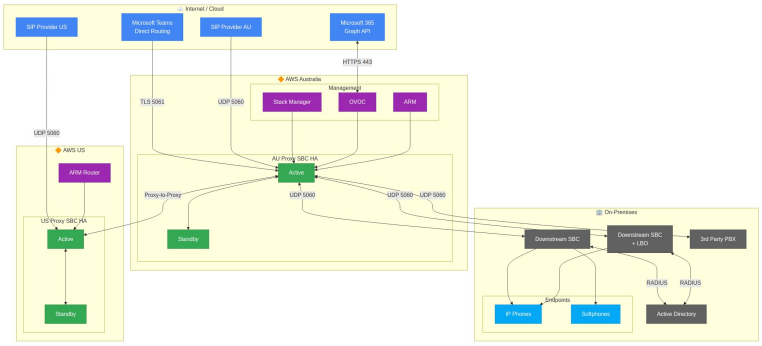


Diagram 26

How HA Failover Works: 1. Both SBCs share a **Virtual IP (VIP)** address on the HA subnet 2. The **AWS Route Table** has a route pointing the VIP to the Active SBC's network interface 3. If the Active SBC fails, the Standby SBC calls the **AWS EC2 API** to update the route table 4. Traffic now flows to the Standby (which becomes the new Active) - no IP changes needed for external parties

D.8.8 Interface Summary Matrix

Appliance	Physical Ports	Ethernet Groups	IP Interfaces	Media Realms	In
Proxy SBC (AWS)	GE_1-GE_8 (Virtual)	3 (HA, OAMP+Internal, External)	3 (HA, OAMP+LAN, WAN)	4 (Internal, M365, PSTN, LMO)	3 (Ir PS Ex
Downstream SBC	GE_1-GE_4	2 (OAMP+Internal, HA)	2 (OAMP+LAN, HA)	1 (Internal)	1 (Ir
		2	2	2	2

Downstream SBC (LBO)	GE_1-GE_4	(OAMP+Internal, HA)	(OAMP+LAN, HA)	(Internal, PSTN)	(Ir PS
OVOC	eth0 (ENI)	1	1	N/A	N/
ARM Configurator	eth0 (ENI)	1	1	N/A	N/
ARM Router	eth0 (ENI)	1	1	N/A	N/
Stack Manager	eth0 (ENI)	1	1	N/A	N/

> **Note:** Stack Manager is deployed in the Australian region only (one per environment) and manages SBC HA stacks across all regions via cross-region AWS API calls.

Document Control

Version	Date	Author	Changes
1.0	5 February 2026	KS	Initial release - Unified deployment guide consolidating AWS deployment and SBC configuration documentation
1.1	9 February 2026	KS	Clarified Stack Manager role (deployment only, not active failover); Added SBC IAM requirements for HA failover; Added Cyber Security Variation section; Updated failover mechanism documentation; Stack Manager retained for Day 2 operations
1.2	9 February 2026	KS	Added Section 10.4 SBC Management Authentication documenting split identity model: Proxy SBC uses Microsoft Entra ID (OAuth 2.0), Downstream SBCs use on-premises Active Directory (LDAPS); Added SBC Management app registration to Section 6; Added cross-references from Section

			10.1
1.3	9 February 2026	KS	Added Section 19.1 SIP Trunk Connectivity in HA documenting how PSTN/ISP SIP trunks connect to the HA Proxy SBC pair via Virtual IP; explained failover behavior for external parties; added HA connectivity architecture diagram showing internal vs external entity connections
1.4	9 February 2026	KS	Updated Appendix D diagrams to clarify bidirectional Graph API traffic: OVOC initiates outbound queries to Microsoft, Microsoft sends inbound webhook notifications to OVOC for call records; added note in quick reference table
1.5	9 February 2026	KS	Added Voice Recording Considerations subsection to Section 19 documenting SRTP encryption impact on existing voice recorders; covered SIPREC integration option, selective encryption, and decision matrix for recording solutions
1.6	9 February 2026	KS	Removed Cisco Webex DI references; Added regional SIP providers (SIP Provider AU, SIP Provider US) for PSTN breakout per region; Enhanced SBC IAM role documentation with CRITICAL callout and Prerequisites checklist in Section 19; Updated firewall rules for regional SIP providers
1.7	10 February 2026	KS	Added comprehensive interface mapping diagrams (Appendix D.8) showing all physical ports, ethernet groups, IP interfaces, media realms, SIP interfaces, and IP groups for all appliances: Proxy SBC (AWS), Downstream SBC, Downstream SBC with LBO, OVOC, ARM Configurator, ARM Router, and Stack Manager; Added end-to-end connectivity map showing complete solution architecture across AU and US regions
			Comprehensive review and correction pass: Fixed 4 broken mermaid diagrams (D.1 arrow directions, D.2 orphaned nodes, D.5 invalid bidirectional arrows, D.8.5 duplicate

			node IDs); Resolved Stack Manager role contradiction across 7 locations (does not manage active HA failover); Fixed QoE port inconsistency (5000→5001); Corrected network interface mapping from 2-ENI to 4-ENI; Standardised TLS Context name to “Teams”; Fixed firewall protocol TCP→UDP for internal SIP signalling; Updated OVOC storage from GP2 to GP3; Added SIP Provider node to D.1 diagram; Updated certificate notes (Baltimore CyberTrust Root expiry, DigiCert G3 clarification, EKU enforcement timeline); Added previous-generation instance notes for r4/m4 families; Fixed revertive-mode description; Standardised spelling to British/Australian English; Aligned Appendix C storage sizes with main document; Fixed formatting inconsistencies
1.8	10 February 2026	KS	
1.9	11 February 2026	KS	Consolidated Stack Manager deployment to Australian region only: Removed Stack Manager from US region (us-east-1); Australian Stack Manager now manages all regions via cross-region AWS API calls; Updated production VM count from 10 to 9; Removed US Stack Manager break glass account; Updated D.3 production diagram, D.4 subnet diagram, deployment phases, IAM policy notes, Section 9/18/20/21, Appendix A/B/C; Updated all tables, checklists, and credentials references to reflect single-region Stack Manager model
2.0	11 February 2026	KS	Major network architecture revision: Consolidated Management (OAMP) and Internal (LAN) interfaces onto a single ENI and subnet, reducing Proxy SBC from 4-ENI to 3-ENI model and Downstream SBC from 3 to 2 Ethernet Groups; Reduced PSTN_Media_Realm from 1000 to 500 session legs (250 concurrent calls, UDP 40000-41999) to match contracted PSTN trunk capacity; Added dual External Publishing Patterns: SBC uses bespoke dedicated EIP + Security Group L4 (no firewall),

			OVOC uses traditional cloud firewall + reverse proxy ingress; Added Cloud East-West Firewall section for internal traffic inspection; Updated OVOC Security Group and prerequisites for reverse proxy ingress; Updated all interface tables, Ethernet Groups, IP Interfaces, Media Realms, SIP Interfaces across Sections 4, 5, 9, 11, 13 and Appendix D diagrams (D.1, D.3, D.4, D.6, D.8.1, D.8.2, D.8.3, D.8.7, D.8.8)
2.1	11 February 2026	KS	Unified SBC authentication to on-premises Active Directory (LDAPS) for all SBCs: Removed split identity model where Proxy SBC used Microsoft Entra ID (OAuth 2.0); All SBCs now use on-prem AD for consistency, WAN resilience, and operational simplicity; Documented MFA limitation as accepted trade-off; Removed AudioCodes-SBC-Management app registration; OVOC and ARM retain Entra ID authentication with MFA support; Broadened Section 21 from Stack Manager-only to comprehensive Cyber Security Considerations with security architecture summary, publishing patterns, and authentication model overview; Removed duplicate network security requirements from Section 21 (consolidated to Section 5.3)
2.2	11 February 2026	KS	Added Section 22A OVOC Data Analytics and Reporting: Documented OVOC Data Analytics API (direct PostgreSQL read-only access to analytics views), 24-hour data retention constraint, daily ETL pipeline to corporate data lake, Power BI integration, and comprehensive cyber security considerations (network access, credential management, access control, data classification, logging); Tightened SBC HA IAM policy per AudioCodes recommendation: Replaced 6-action Resource:* policy with least-privilege multi-statement policy using resource-scoped ARNs and tag-based conditions (ec2:AssociateAddress, ec2:DescribeAddresses, ec2:DescribeNetworkInterfaceAttribute,

			ec2:DescribeNetworkInterfaces, ec2:ReplaceRoute); Added temporal IAM elevation pattern for Stack Manager (detach broad permissions when not in active use); Updated OVOC Security Group (TCP 5432), Cloud East-West Firewall table, Section 16 OVOC Firewall Rules, Appendix C Port Summary, and Section 21 Security Architecture Summary for Analytics API; Added Data Analytics API license to OVOC Licensing section
2.3	12 February 2026	KS	Replaced SBC management authentication from LDAPS to RADIUS with Cisco ISE as recommended AAA server; Documented AudioCodes VSA dictionary (Vendor ID 5003, ACL-Auth-Level attribute 35) with role mapping (Security Administrator=200, Administrator=100, Monitor=50); Noted TACACS+ is not supported on AudioCodes SBC products (MSBR only); Added OVOC audit logging requirements to OVOC Security Group (syslog UDP 514 inbound, TCP 514 outbound, SNMP trap forwarding UDP 1164-1174); Documented OVOC dual-layer audit logging (OS-level auditd + application-level Actions Journal) with SIEM integration paths; Updated SBC firewall rules from LDAPS (TCP 636) to RADIUS (UDP 1812/1813); Updated Section 21 security architecture summary; Added Stack Manager supported OS list and SOE compatibility; Clarified bidirectional SIP connectivity for site SBCs, third-party PBX, and ATAs
			Added CDR access auditing guidance to Section 22A: Documented that OVOC does not natively log individual SQL queries via the Analytics API; Added 4-layer auditing approach for Analytics API (PostgreSQL native logging, pgAudit extension, network-level logging, data lake audit); Documented shared analytics account limitation and mitigations (IP attribution, application_name tagging, ETL-only

			restriction, database proxy); Added compliance summary table mapping audit questions to solutions; Documented OVOC GUI CDR viewing audit limitation — no native capability to log which operator viewed specific CDR records through the web GUI without considerable OS-level modification; Added 7 mitigations for GUI audit gap (RBAC, GDPR phone number masking, web server access log enhancement, Linux auditd, network-level monitoring, reverse proxy with enhanced logging, data lake as controlled access point); Included risk acceptance template for compliance documentation
2.4	12 February 2026	KS	
2.6	13 February 2026	KS	Replaced all 0.0.0.0/0 security group outbound rules with specific destinations following least-privilege egress: Stack Manager and SBC HA now use VPC Endpoints (PrivateLink) for AWS API access (EC2, CloudFormation, CloudWatch, STS); SBC Internal egress scoped to VPC CIDR for SIP/RTP/OVOC traffic; SBC External egress scoped to Teams Direct Routing CIDRs (52.112.0.0/14, 52.120.0.0/14) and SIP Provider CIDRs; ARM and OVOC egress scoped to Microsoft Graph/Entra ID CIDRs (M365 Endpoint ID 56: 20.20.32.0/19, 20.190.128.0/18, 20.231.128.0/19, 40.126.0.0/18); Added VPC Endpoints (PrivateLink) subsection to Section 20 with required/optional endpoint tables, VPC Endpoint Security Group, and configuration notes; Added Security Group Design Notes explaining egress architecture; Added S3 Gateway Endpoint with prefix list for CloudFormation template and firmware storage
			Network interface remapping and security architecture update addressing 10 items of stakeholder feedback: (1) Remapped SBC network interfaces — eth0=HA, eth1=OAMP+LAN, eth2=WAN (previously eth0=OAMP+LAN, eth1=WAN, eth2=HA); updated all

2.5	12 February 2026	KS	interface tables, Key Concepts, and D.8.8 Matrix; (2) Clarified HA scope — Transit Gateway exclusion applies to HA failover VIP routing only; Virtual IPs must be routable cross-region for SBC-to-SBC connectivity via organisation's existing network backbone; (3) Added cross-region VPC CIDR inbound rules to SBC, ARM, and OVOC Security Groups for US-AU management and SBC connectivity; (4) Split single SBC Security Group into three per-interface groups (HA, Internal, External) assigned to respective ENIs; added SNMP 161 and HTTPS 443 inbound from OVOC to Internal SG; narrowed Teams media to 20000-21999, PSTN media 40000-41999 on External interface; (5) Added Local Media Optimisation (LMO) scope clarification — applies to local users only, requires EUC/voice subnet mapping in Teams admin centre; (6) Removed App Registration 3 (ARM REST API Authentication) and all references (summary table, checklist, credentials template); renumbered App Registration 4 to 3; (7) Updated Section 16 firewall rules — Teams media 20000-21999; added bidirectional SIP signalling and media rules for SIP Provider AU (Telstra REGISTER-type) and US; added inbound SIP listening ports for carriers; renamed Downstream SBC to Downstream Devices (SBC, Media Pack, Cisco); added TCP 5061 (TLS) for inter-device SIP trunks; (8) Updated failover behaviour — ongoing calls should not drop during HA switchover; call sessions synchronised between Active/Standby; no Re-INVITE in VIP-based HA model; (9) Updated SIP trunk flow direction — clarified media and SIP signalling are bidirectional from firewall perspective for all SIP Providers; restricting to outbound-only may cause early media issues; (10) Clarified authentication model — SBCs use RADIUS (Cisco ISE) for direct access, OVOC/ARM use Azure

	Entra ID; OVOC provides SSO for centralised SBC management via Entra ID; moved SIP Provider connectivity from Internal to External interface; updated PSTN_Media_Realm binding, Proxy Set SIP Interfaces, Cloud East-West Firewall scope; updated Appendix C/D port summaries; updated Mermaid diagrams (d8-7 complete solution and simplified); fixed pre-existing inconsistencies (LDAPS→RADIUS in diagrams, US Stack Manager removal from simplified diagram); Cascaded interface remapping through Section 11 SBC configuration tables (Virtual Ports, Ethernet Groups, Ethernet Device Config — Group 1=HA, Group 2=OAMP+Internal, Group 3=External) and Section 19 HA/failover SIP Provider interface references (Internal→External)

End of Document