

## SmartTAP 360°

### SmartTAP 360° Enterprise Recording Solution

Version 5.6

Smart**TAP 360°** Live



## Notice

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

This document is subject to change without notice.

Date Published: September-24-2024

## WEEE EU Directive

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

## Security Vulnerabilities

All security vulnerabilities should be reported to [vulnerability@audiocodes.com](mailto:vulnerability@audiocodes.com).

## Customer Support

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

## Documentation Feedback

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

## Stay in the Loop with AudioCodes



## Related Documentation

Document Name
SmartTAP 360° Installation Manual
SmartTAP 360° Administrator Guide
SmartTAP 360° for Microsoft Teams Deployment Guide
SmartTAP 360° Genesys Integration Guide

## Document Revision Record

LTRT	Description
27290	Initial document for this release.
27291	Added a note in the specifications regarding SBA integration. In addition the document is now published in the same template as other SmartTAP documentation.
27292	Update to the Server Configurations and the Bot Cluster Specifications.
27293	Update to Server Requirements.
27294	Update for Version 5.5.
27295	Update to the SIPRec specifications.
27296	Update to Sections: Microsoft Teams Bot Cluster Specifications; ; Microsoft Teams Instant Message Service CD-Live Component; SmartTAP 360° for Microsoft Teams Availability; SmartTAP SIPRec Deployment in Azure - Minimum Specifications Added Sections: Deploy Compliance Recording Applications; Microsoft Teams Firewall Requirements
27297	Update to SIPRec specifications.
27298	Added Azure Storage specifications; Microsoft Teams Instant Message Service CD-Live Component; Customer Consent for Azure Active Directory (aad-app); Firewall Rules for Microsoft Azure Removed Section: Active / Standby Resiliency Configuration (Optional)
27299	Correction to figure captions and layout.
27310	Updated Sections: Supported Microsoft Windows OSS (Added support for

LTRT	Description
	Microsoft Windows Server 2022); Supported Microsoft Integrations (Removed Microsoft Lync Server 2013) and SmartTAP 360° Server Specifications (added Windows Server 2022)
27311	Updated Sections: Firewall Rules for Microsoft Azure

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>SmartTAP 360° for Microsoft Teams Requirements</b>	<b>2</b>
	SmartTAP 360° Server Specifications	2
	Database	3
	Supported Storage for Recordings	3
	Bring Your Own Storage (BYOS) on Azure Blob	4
	Microsoft Teams Bot Cluster Specifications	4
	Microsoft Teams Instant Message Service CD-Live Component	7
	Live Monitoring	8
	SmartTAP 360° for Microsoft Teams Availability	8
	Graph API Permissions Requirements	9
	Customer Consent for Calls Recording (calls-app)	9
	Customer Consent for Azure Active Directory (aad-app)	10
	Customer Consent for M365 and Teams Personal App (login-app)	11
	Customer Consent for Instant Messaging (ims-app)	12
	Microsoft Teams Firewall Requirements	12
	Firewall Prerequisites	13
	Firewall Rules for Microsoft Azure	14
	VPN Firewall Rules	16
<b>3</b>	<b>SmartTAP SIPRec Deployment in Azure - Minimum Specifications</b>	<b>18</b>
<b>4</b>	<b>Requirements for Other Integrations</b>	<b>20</b>
	Server Configurations	20
	Supported Virtual Machine (VM) Environments	24
	VMware ESXi	24
	Microsoft Hyper-V	24
	Supported Microsoft Integrations	24
	SBA Integration	24
<b>5</b>	<b>Supported Microsoft Windows OSS</b>	<b>25</b>
<b>6</b>	<b>Application Footprint</b>	<b>26</b>
<b>7</b>	<b>Windows Updates</b>	<b>27</b>
	Installing Windows Updates	27
<b>8</b>	<b>Antivirus Software and Windows Defender</b>	<b>28</b>

# 1 Introduction

This document describes the hardware and software requirements for installing SmartTAP 360° Enterprise Recording Solution including the following:

- [SmartTAP 360° for Microsoft Teams Requirements](#) on page 2
- [SmartTAP SIPRec Deployment in Azure - Minimum Specifications](#) on page 18
- [Requirements for Other Integrations](#) on page 20
- [Application Footprint](#) on page 26
- [Windows Updates](#) on page 27
- [Antivirus Software and Windows Defender](#) on page 28

## 2 SmartTAP 360° for Microsoft Teams Requirements

Microsoft Teams requirements includes the following:

- SmartTAP 360° Server Specifications
- [Microsoft Teams Bot Cluster Specifications](#) on page 4
- [Microsoft Teams Instant Message Service CD-Live Component](#) on page 7
- [SmartTAP 360° for Microsoft Teams Availability](#) on page 8
- [Graph API Permissions Requirements](#) on page 9
- [Microsoft Teams Firewall Requirements](#) on page 12



SmartTAP SIPRec integration is supported when using the Teams SBC for recording PSTN calls. For details, see [SmartTAP SIPRec Deployment in Azure - Minimum Specifications](#) on page 18

### SmartTAP 360° Server Specifications

- **Operating System:** Microsoft Windows Server 2016, Microsoft Windows Server 2019 and Microsoft Windows Server 2022



All Virtual machines are created with 128 GB Operating System disk.

- SmartTAP server with the specifications below can handle up to 500 users and 100 audio-only concurrent recordings:
  - Virtual Machine: Tier=Standard, Instance=DS2 v2 (2 vCPUs, 7 GB RAM, 14 GB Temporary storage)
- SmartTAP server with the specifications below can handle up to 3000 users and 600 audio-only concurrent recordings or up to 500 users and a combination of 100 audio and video concurrent recordings:
  - Virtual Machine: Tier=Standard, Instance=DS3 v2 (4 vCPUs, 14 GB RAM, 28 GB Temporary storage)
- SmartTAP server with the specifications below can handle up to 3000 users and a combination of 600 audio and video concurrent recordings:
  - Virtual Machine: Tier=Standard, Instance=F8s v2 (8 vCPUs, 16 GB RAM, 64 GB Temporary storage)



**Analytics Feature:**

- Enabled for Microsoft Teams integration only.
- The SmartTAP server must be installed on a DS3 v2 machine and higher.

- SmartTAP server with the specifications below can handle up to 100 targeted users and 10 maximum concurrent audio-only call recordings. Post-recording features for the below machine specifications are limited to basic playback and download. In case of maximum recording levels of 10 concurrent audio calls, the playback and download of recordings may be delayed or take a longer time to complete. The Analytics feature is not supported on this server.

- Virtual Machine: B2MS 2 vCPUs, 8 GB RAM

- **Total Available Storage:** Calculation is made according to the following formula:

Audio Licenses + Video Licenses = Free Storage Allocation (1 GB per user) + Purchased Storage Allocation

For example, when a customer has purchased 100 Audio Licenses + 100 Video Licenses, licensing is calculated as follows:

200 GB Free Storage Allocation + Purchased Storage Allocation e.g. 100 GB. In this case, the customer has a Total Available Storage of 300 GB.

- **Mixed Deployments:** When Microsoft Teams and another integration such as SIPRec are deployed as part of the same SmartTAP solution, the other integration must be deployed on a separate RDD according to the specifications for the relevant integration.

- **Playback performance:** The Web interface may hang when CPU resources are insufficient to execute playback:

- For optimal audio playback performance: The number of concurrent playbacks should not exceed the number of CPU cores - 1.
- For optimal video playback performance: The number of concurrent playbacks should not exceed half the number of CPU cores.

A server with an equivalent or higher spec must be used when the SmartTAP is deployed On-premises or on a cloud platform other than Azure.

- **Concurrent recording:** Specifications should be equal to the maximum simultaneous calls that can be made by the targeted users for recordings; this includes all recording types e.g. Full Time Recording, Record on Demand, Save on Demand.

- **Integrations with third-party applications:** Custom specifications are required.

## Database

An additional managed disk is required for database storage. The estimated size of the required disk can be calculated using the SmartTAP storage calculator. The additional managed disk is not required for POC if the SmartTAP Server's OS disk has sufficient space to hold the database. The disk should be a premium SSD managed disk.

## Supported Storage for Recordings

- AudioCodes hosting:

- Azure Blob Storage in AudioCodes subscription



- BYOS – Bring your own Azure Blob storage
- Customer hosting:
- Azure Blob
  - SMB

## Bring Your Own Storage (BYOS) on Azure Blob

Bring Your Own Storage (BYOS) is supported when SmartTAP is hosted in AudioCodes Azure Subscription and customers need to keep recordings in their Azure Blob Storage. To connect SmartTAP hosted in AudioCodes Azure Cloud to the customer's Azure Blob, customers must create an Azure Blob Storage account and provide AudioCodes with the following storage account credentials:

- Storage Account Name
- Storage Account Key
- Media Container Name

Once SmartTAP is deployed, customers can restrict the access to recorded media to the specific IP address of the SmartTAP application server and Teams Bot IP address in case of Teams recording deployment.

## Microsoft Teams Bot Cluster Specifications

Microsoft Teams Bot can be deployed in the Microsoft Azure Generic Cloud using one of the below options in a **single organizational tenant** setup:

- **Azure Service Fabric Cluster:** Azure Service Fabric Cluster with Silver Durability with a minimum of 5 nodes is required:
  - Virtual Machine: Tier=Standard, Instance=DS2\_v2 (2 vCPUs, 7 GB RAM), OS disk size: 128 GB for voice only recording, 256 GB for audio and video/screen sharing
  - Windows Server 2019 Data Center - with Containers

For more information, refer to [Microsoft Service Fabric Cluster](#).

**Table 2-1: Service Fabric Cluster Concurrent Calls Recordings Table**

Media in a Call	Maximum Total Calls per vCPU
Voice	25
Voice and video (p2p or group calls up to 4 streams)	9 <sup>1</sup>

<sup>1</sup>When a user is enabled for different types of media (audio, video, chat or screen sharing), resources are allocated for audio and video, even if the user is on an audio call only.

Media in a Call	Maximum Total Calls per vCPU
Voice and screen sharing	15 <sup>1</sup>

■ **Azure Standalone Cluster:** Standalone cluster including one of the VM specifications below:

- Virtual Machine: Tier=Standard, Instance= DS2\_v2 (2 vCPUs, 7 GB RAM), OS disk size: 128 GB for voice only recording, 256 GB for audio and video/screen sharing.
- Virtual Machine: Tier=Standard, Instance= DS3\_v2 (4 vCPUs, 14 GB RAM)), OS disk size: 128 GB for voice only recording, 256 GB for voice only with 16khz codec (for STT), and 512 GB for audio and video/screen sharing.
- Virtual Machine: Tier=Standard, Instance= DS4\_v2 (8 vCPUs, 28 GB RAM), , OS disk size: 256 GB for voice only recording, 512 GB for audio and video/screen sharing.

**Table 2-2: Standalone Cluster Concurrent Calls Recordings Table**

Media in a Call	Maximum Total Calls per vCPU
Voice	40
Voice and video (p2p or group calls up to 4 streams)	13 <sup>2</sup>
Voice and screen sharing	25 <sup>3</sup>

■ **Additional mandatory Azure resources:**

- Deployed in Service Fabric Cluster:
  - ◆ Standard Load Balancer for Bot Service Fabric Cluster
  - ◆ Virtual Machine ScaleSet – VMs for Bot Service Fabric Cluster
- Public IP address for the Standard Load Balancer (for Standard Load Balancer in case of SFC)
- Key Vault to store Bot Service Fabric Cluster certificates
- Microsoft Azure Blob Storage
- Microsoft Azure Functions – Consumption Tier (when the Analytics feature is enabled for Teams integration)

<sup>1</sup>When a user is enabled for different types of media (audio, video, chat or screen sharing), resources are allocated for audio and desktop sharing, even if the user is on an audio call only.

<sup>2</sup>Maximum of 70 video concurrent calls on a single server. When a user is enabled for different types of media (audio, video, chat or screen sharing), resources are allocated for audio and video, even if the user is on an audio call only.

<sup>3</sup>When a user is enabled for different types of media (audio, video, chat or screen sharing), resources are allocated for audio and desktop sharing, even if the user is on an audio call only.

- Microsoft Azure App Service – Standard Tier (when the Analytics feature is enabled for Teams integration)

■ **Optional Azure resources:**

- Application Insights to store Bot logs.
- App Configuration to store Bot configuration.

■ **Teams Bot Media Buffering:** The Teams Bot software includes a mechanism to protect against the temporarily loss of the connection to the storage device. When the Teams Bot can't reach the storage device, it temporarily stores the recordings of finished calls locally until it has available local disk space. When connection to the storage device is restored, the Bot transfers the temporarily stored recordings to the storage device.


The required OS disk sizes for the Teams Bot VMs are calculated to provide space for higher loads with full capacity recordings in a Bot (for example, a cluster Bot node can handle 50 audio calls concurrently), calls duration of four hours and at least two additional hours for buffering recording locally in case of temporarily no connectivity to storage (refer to Azure Blob Hot tier [SLA](#)).

For Hybrid deployment when the Teams Bot is deployed in Azure and SmartTAP Server and storage is local, a possible disconnect time between the Bot and storage may depend on the VPN connection and can be longer than two hours. To overcome longer disconnects a large OS disk might be needed. To calculate the needed space please use SmartTAP storage calculator. The Bot VM requires about 60 GB for OS and the software operation.

The table below provides the estimated extra hours of recording in cases of an unreachable storage device.

**Table 2-3: Teams Bot Media Buffering Estimations**

Recording Coder Type	Server Specification	Estimated Number of Days/Hours
Voice recording with g729	Standalone Ds2v2, 128 GB OS disk	10 days
	Standalone Ds3v2, 128 GB OS disk	5 days
	Standalone Ds4v2, 256 GB OS disk*	14 days
	Cluster Node, 128 GB OS disk	16 hours
Voice recording with g711	Standalone Ds2v2, 128 GB OS disk	1 day
	Standalone Ds3v2, 128 GB OS disk	11 hours
	Standalone Ds4v2, 256 GB OS disk*	18 hours
	Cluster Node, 128 GB OS disk	1.5 days

Recording Coder Type	Server Specification	Estimated Number of Days/Hours
Voice with 16 kHz for STT codec	Standalone Ds2v2, 128 GB OS disk	3 hours
	Standalone Ds3v2, 256 GB OS disk*	7 hours
	Standalone Ds4v2, 256 GB OS disk*	2 hours
	Cluster Node, 128 GB OS disk	12 hours
Voice and video recording	Standalone Ds2v2, 256 GB OS disk*	3 hours
	Standalone Ds3v2, 512 GB OS disk*	4 hours
	Standalone Ds4v2, 512 GB OS disk*	2 hours
	Cluster Node, 256 GB OS disk*	6 hours
 The default Azure VM is created with an OS disk is 128 GB.		

## Microsoft Teams Instant Message Service CD-Live Component

- Installed as a component of the SmartTAP server on Azure (at least DS3\_V2, 2 vCPUs, 7 GB RAM or higher).
- Installed as a Standalone VM on Azure (B2MS 2 vCPUs, 8 GB RAM).
- SmartTAP servers support up to 165 messages multiplied by the number of users that are enabled for chat (with all included licenses) per day. For example, two users can share 330 messages where one user may have 200 messages and another 130 messages. The maximum number of chat messages supported per day is 495,000.
- Microsoft requires an E5 user license for reading chats of the users by compliance or security applications. The E5 license includes a seeded capacity of 1600 messages per user per month and \$0.00075 per message for additional messages (see MSFT license page: [microsoft graph teams licenses](#))



- CD-Live cannot be installed On-premises.
- Instant messages are stored in the database and not on storage disks.

## Live Monitoring

- Two Live monitoring sessions are included and supported in the deployment. For additional Live Monitoring sessions, CPUs need to be added according to the following:
  - One CPU per four Live Messaging sessions

## SmartTAP 360° for Microsoft Teams Availability

SmartTAP 360° for Microsoft Teams availability is based on Azure Virtual Machines (VM) Service Level Agreement (SLA):

- SmartTAP Server on Azure VM - SLA is 99.9% for one instance and 99.99% can be achieved by deploying the two servers in different Availability Zones (optionally available at extra cost). Refer to [Azure VM SLA](#).
- SmartTAP 360° Teams BOT on Azure VM - SLA 99.9% (99.95% Service Fabric Cluster). Refer to [Azure VM SLA](#).
- SmartTAP Media on Azure BLOB – SLA is 99.9% for Hot tier, and 99% for Cool Tier. Refer to [Azure Blob Storage SLA](#).
- The durability of Azure Blob using Local Redundant Storage (LRS) is 11 nines. Refer to [Azure Blob Storage Durability](#).
- Zone Redundant Storage (ZRS) is required for the deployment of two servers in different Availability Zones for higher SLA on the VMs. The durability of Azure BLOB using ZRS is 12 nines: Refer to [Azure Blob Storage Durability](#).
- Two independent SmartTAP recording solutions can be deployed across Azure Region's Availability Zones or across regions for higher availability. The double solutions are managed separately and record calls in parallel. In case of failure of one of the solutions, the other solution continues recording. There is no synchronization between the solutions and hence after a failure of one of the solutions only the solution that was up and running will possess the recordings of the calls that took place during the failure.

## Graph API Permissions Requirements

The SmartTAP Compliance Recording utilizes Graph APIs to authenticate users, read groups and users from the customer AAD, and to successfully join the calls to be recorded. The Graph APIs are divided into groups of enterprise applications. The applications are deployed in the hosted environment and the Graph APIs permissions under the applications must be consented to by the customer's M365 administrators.

**Figure 2-1: Applications Deployed on the Customer Tenant**

Registration	Description
Recording App (calls-app)	Application for the Bot Recording application to join Teams' tenant calls and to receive the media to be recorded. See <a href="#">Customer Consent for Calls Recording (calls-app)</a> below
AAD App (aad-app)	Application for reading groups and users from the customer tenant's Active Directory. See <a href="#">Customer Consent for Azure Active Directory (aad-app)</a> on the next page
M365 Login App (login-app)	Application for OpenID Connect Login connection for signing into the SmartTAP Web with Microsoft 365 user credentials. See <a href="#">Customer Consent for M365 and Teams Personal App (login-app)</a> on page 11.
Personal App	SmartTAP can be added as a Personal App in the customer's Microsoft Teams admin center with the main tab/page that includes On-demand buttons and an additional tab for access to the full application. See <a href="#">Customer Consent for M365 and Teams Personal App (login-app)</a> on page 11.
SmartTAP CD-Live	SmartTAP Live Configuration for Instant Message Recording (see <a href="#">Customer Consent for Instant Messaging (ims-app)</a> on page 12).

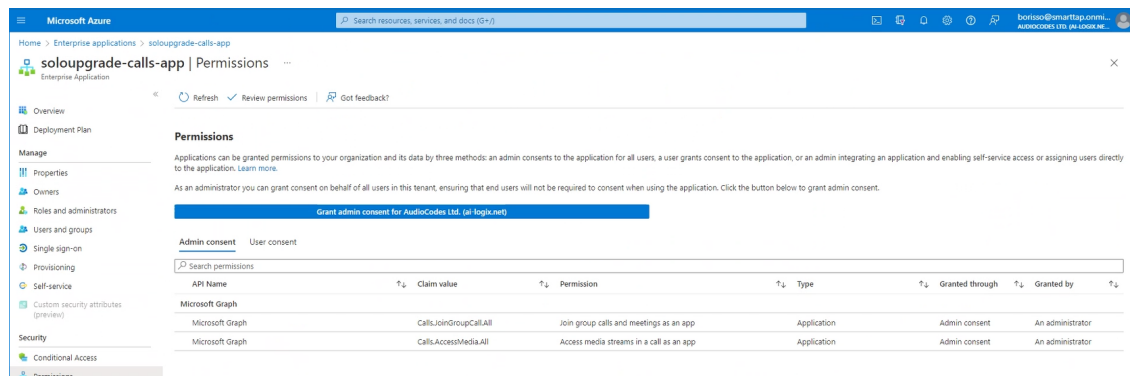
### Customer Consent for Calls Recording (calls-app)

The calls-app permissions (shown below) are required for the SmartTAP Teams Bot application to join your Teams' tenant calls and to receive the media to be recorded. Deployment of SmartTAP generates the application and consent link to the application:

- Calls.JoinGroupCall.All - Join group calls and meetings as an app (Application)
- Calls.AccessMedia.All - Access media streams in a call as an app (Application)

The following role is required to run the consent link:

- Your Tenant's Office 365 administrator

**Figure 2-2: calls app permissions**

## Customer Consent for Azure Active Directory (aad-app)

The aad-app requires permissions for the following:

- Read users and groups of your AAD and map them to users and associated SmartTAP policies and profiles.
- Authenticate between the SmartTAP server, Bot and Remote Transfer Service (RTS) using the OpenID Token mechanism. The following permissions are required:
  - GroupMember.Read.All – Read all group memberships (Application)
  - User.Read.All – Read all users' full profiles
- Role-based access control for retrieving Azure Blob Storage statistics. The following roles are required:
  - Teams Bot
  - Remote Transfer Service
  - Call Delivery Live

The following role is required to run the consent link:

- Your Tenant's Office 365 administrator

**Figure 2-3: aad-app Permissions**

The screenshot shows the 'API permissions' page for the application '562c1b-aad-app'. The left sidebar contains navigation links for Overview, Quickstart, Integration assistant, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area shows a warning about the November 9th, 2020 deadline for verified publishers. Below this, a section titled 'Configured permissions' explains that applications are authorized to call APIs when permissions are granted by users/admins. A table lists the configured permissions:

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (2)				
GroupMember.Read.All	Application	Read all group memberships	Yes	Not granted for AUDCA...
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for AUDCA...

At the bottom, a note states: 'To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).'

## Customer Consent for M365 and Teams Personal App (login-app)

The login-app permissions (shown below) are required for the SmartTAP application to authenticate users utilizing your tenant AAD authentication, and Microsoft Open ID Connect (OAuth 2) authentication. The permissions enable SmartTAP to reroute users accessing the SmartTAP application either from a browser or from the SmartTAP's Teams application to be authenticated according to your organizational M365 policy:

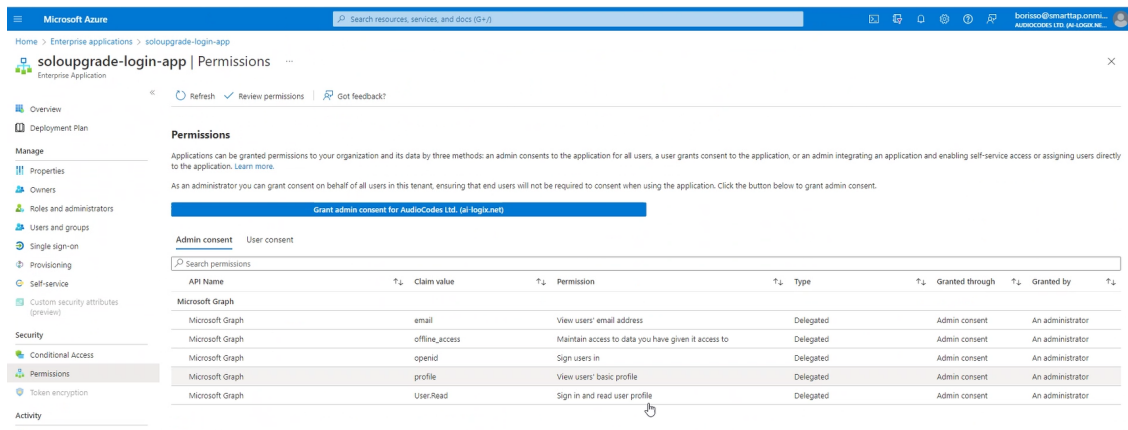
- email – View users; email address (Delegated)
- offline\_access – Maintain access to data you have given it access to (Delegated)
- openid – Sign users in (Delegated)
- profile – View users' basic profile (Delegated)
- User.Read – Sign in and read user profile (Delegated)

The following role is required to run the consent link:

- Your Tenant's Office 365 administrator



Figure 2-4: Login-app permissions



## Customer Consent for Instant Messaging (ims-app)

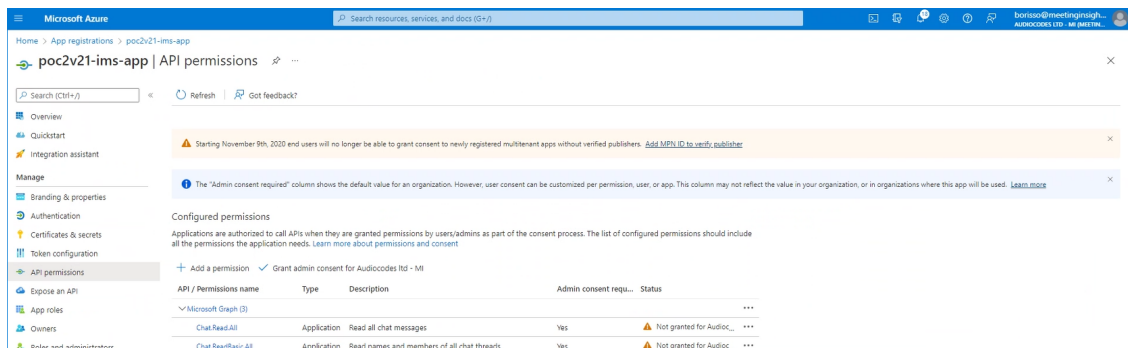
The following ims-app permissions are required to enable the SmartTAP application to read and record user chat messages only:

- Chat.Read.All – Read all chat messages (Application permission)
- Chat.ReadBasic.All – Read names and members of all chat threads (Application permission)

Required Role to run the consent link:

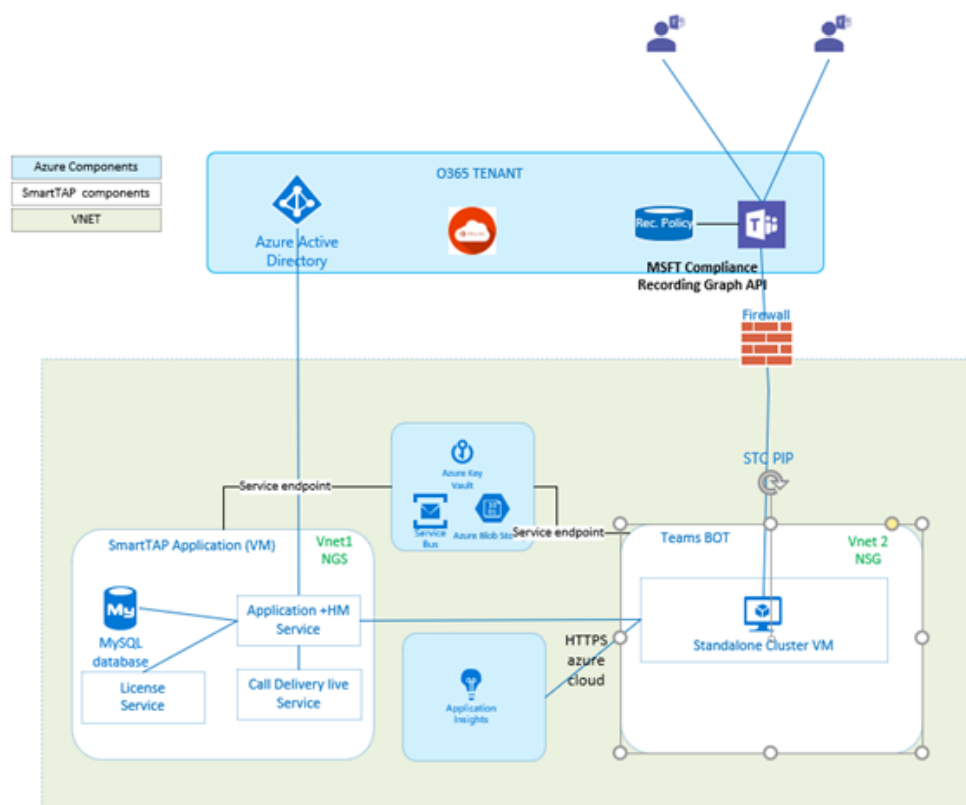
- Your Tenant's Office 365 administrator

Figure 2-5: Instant Messaging Permissions



## Microsoft Teams Firewall Requirements

This custom environment is aimed at customers using Azure Firewall or third-party Firewall (Checkpoint and other proprietary firewalls). In the environment shown in the figure below, all components have internal private IP addresses or endpoint and the only facing network IP address is the public firewall IP address. The SmartTAP Microsoft Teams environment diagram is displayed below:

**Figure 2-6: Standalone Firewall Rules**

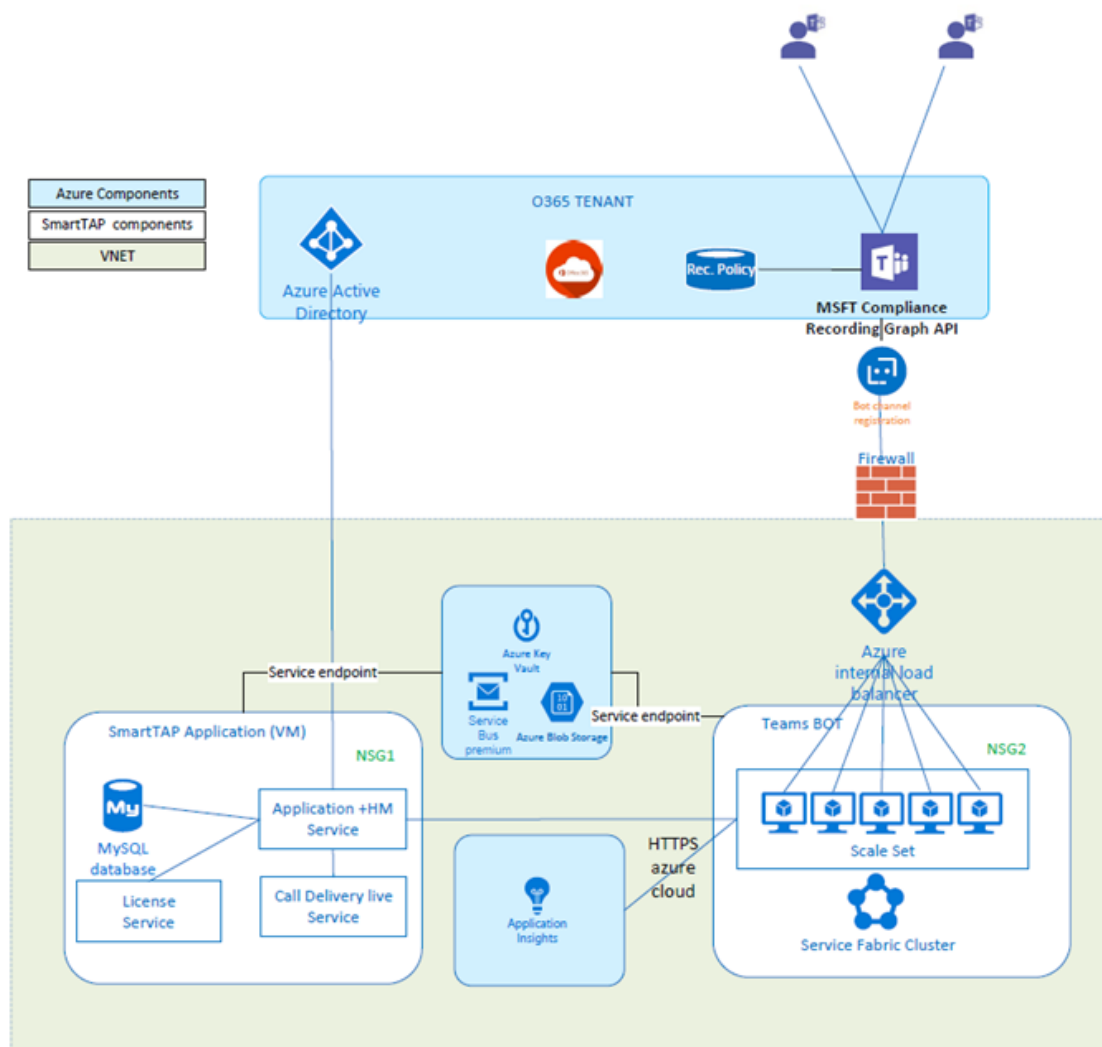
## Firewall Prerequisites

- **Required Roles:** The deployment of SmartTAP requires the creation of VM machines, deployment of SFC, create applications, users, secret keys, configuring virtual networks, given permissions and more. Consequently, it is required to have customer's engineer(s) with the appropriate privileges during the installation meeting such as:
  - A staff member with 'Domain Admin' and Azure administration privileges to required subscription.
  - A staff member with 'Teams Admin' privileges
  - A staff member with Global DNS/Firewall/Networking permissions
  - A staff member with Active Directory Global Administrator Role.
  - A staff member with Subscription Owner Role
- **Create a Resource Group:** Create a new Resource Group dedicated to the solution. For the eDouble Recording (Active – Active) setup two Resource Groups need to be create
- **Create Virtual Network/s:** Create a new (or identify existing -in the same Region as the new RG) Vnet and subnet. For the Active Active setup separate Vnets need to be created for each instance.

## Firewall Rules for Microsoft Azure

Create a new firewall on Microsoft Azure according to the tables below or use rules according to customer recommendations.

**Figure 2-7: Custom-secured Firewall for SFC**



**Table 2-4: Teams Bot Connectivity to Microsoft Azure**

Name	Protocol	Source	Destination Address	Destination Ports	Translated Address	Translated Port	Description
Firewall Dnat Rules (Inbound)							
interanl- lb-health	TCP	Azure Cloud	FW Public IP	9441	ILB Private IP	9441	Call invite from Teams HTTPS health probe for Azure Traffic Manager and Application Gateway.
msgraph- to-bot-signal- node0	TCP	Azure Cloud	FW Public IP	9444	ILB Private IP	9444	Call control port for Teams.
msgraph- bot-	TCP	Azure	FW Public IP	8445	ILB	8445	Media control

Name	Protocol	Source	Destination Address	Destination Ports	Translated Address	Translated Port	Description
media- node0		Cloud			Private IP		port for Teams
Outbound Firewall Rules							
https	TCP	Subnet	Azure Cloud	443			Used for HTTPS-based web access.
udp	UDP	Subnet	<ul style="list-style-type: none"> <li>13.107.64.0/18</li> <li>52.112.0.0/14</li> <li>52.120.0.0/14</li> <li>52.122.0.0/15</li> </ul>	3478-3481			Media relay ports.
Media	TCP		<ul style="list-style-type: none"> <li>13.107.64.0/18</li> <li>52.112.0.0/14</li> <li>52.122.0.0/15</li> <li>52.238.119.141/32</li> <li>52.244.160.207/32</li> </ul>	80, 443			Media control ports.

Figure 2-8: Standalone cluster

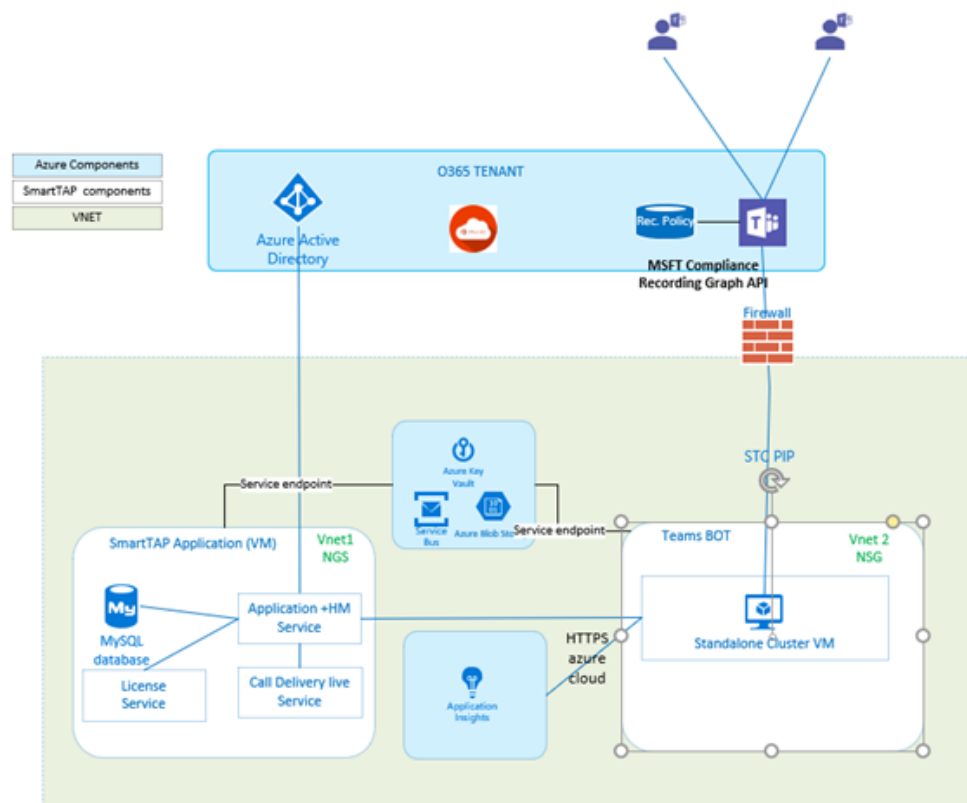


Table 2-5: Microsoft Azure Firewall Rules for Standalone Cluster

Name	Protocol	Source	Destination Address	Destination Ports	Translated Address	Translated Port	Description
Firewall Dnat Rules (Inbound)							
Stand alone cluster VM-	TCP	Azure Cloud	FW Public IP	9441	STC Private IP	9441	Call invite from Teams HTTPS

Name	Protocol	Source	Destination Address	Destination Ports	Translated Address	Translated Port	Description
health							health probe for Azure Traffic Manager and Application Gateway.
msgraph-to-bot-signal- STC	TCP	Azure Cloud	FW Public IP	9444	STC Private IP	9444	Call control port for Teams.
msgraph-bot- media- STC	TCP	Azure Cloud	FW Public IP	8445	STC Private IP	8445	Media control port for Teams.
Outbound Firewall Rules							
https	TCP	Subnet	Azure Cloud	443			Used for HTTPS-based web access.
udp	UDP	Subnet	<ul style="list-style-type: none"> <li>13.107.64.0/18</li> <li>52.112.0.0/14</li> <li>52.120.0.0/14</li> </ul>	3478-3481			Media relay ports.
Media	TCP		<ul style="list-style-type: none"> <li>13.107.64.0/18</li> <li>52.112.0.0/14</li> <li>52.122.0.0/15</li> <li>52.238.119.141/32</li> </ul>	80,443			Media control ports.



- Microsoft Azure IP ranges: [Microsoft Azure IP Ranges](#)
- Microsoft Teams IP ranges: [Microsoft Teams IP Ranges](#)
- Firewall configuration for Teams recording deployments: [Ranges for Teams Recording Deployments](#)

- Add Internal Routing Inbound and Outbound connections to the public IP address.

Table 2-6: Internal Routing

Address prefix	Next hop
0.0.0.0/0	Firewall Private IP address

## VPN Firewall Rules

The following firewall rules are set on the On-Premises Firewall/VPN device for the VPN tunnel.

Table 2-7: VPN Firewall Rules

Protocol	Ports	Connection	Port Flow	Description
TCP	443	Azure VNet ⇔	Send-only	HTTP/S between sites. This port is

Protocol	Ports	Connection	Port Flow	Description
		On-Premises site		used for SmartTAP inter-components communication and communication with Azure resources.
TCP+UDP	53	Azure VNet ⇔ On-Premises site	Bi-directional	For SmartTAP Servers DNS resolution.
TCP	445	Azure VNet ⇒ On-premises site	Send-only	CIFS (SMB) Access: Teams Bot transfers recordings to On-premises SMB storage through the connection.
TCP	8861	Teams Bot(s) VMS (client agents) ⇒ SmartTAP Server(main agent)	Send-only	Connection for alarms transmission between OVOC agent in Teams Bot and the Main agent on the SmartTAP Server.
TCP	8863	SmartTAP Server(Main Agent) ⇒ Teams Bot(s) (Client agents)	Send-only	Connection for Keep alive checks between the OVOC Main agent on SmartTAP Server and OVOC agent in the Teams Bot.

### 3 SmartTAP SIPRec Deployment in Azure - Minimum Specifications

SmartTAP SIPRec recording deployment can be used to record Teams PSTN calls that the SBC or gateway handles.



For deployments other than Azure, see [Requirements for Other Integrations](#) on page 20.

#### SmartTAP SIPRec server:

- **Low-profile:** DS2\_v2, 2 vCPUs, 7-GB RAM, SmartTAP for up to 3,000 users and 50 concurrent audio recordings. Post recording features for this machine specification are limited to basic playback and download. In case of maximum recording levels of 50 concurrent audio calls, the playback and download of recordings may be delayed or take a longer time to complete.
- **Middle-profile:** One of the following:
  - DS3\_v2, 4 vCPUs, 14 GB RAM with SmartTAP for up to 3,000 users and 250 concurrent audio recordings.
  - F8s\_v2, 8 vCPUs, 16 GB RAM with SmartTAP for up to 3,000 users and 250 concurrent audio recordings.
- **High-profile:** DS4\_v2, 8 vCPUs, 28 GB RAM with SmartTAP for up to 3,000 users and 600 concurrent audio recordings.
- **Distributed deployment:** One Ds3 v2 for SmartTAP Server (FE, DB, BE) and two DS4 v2 each handling 500 ccs can be deployed for up to 3,000 users and 1000 concurrent audio recordings.
- Two additional managed disks are required for database storage and for temporarily storing media. The estimated size of the required disks can be calculated using the SmartTAP storage calculator.
  - The disks should be premium SSD managed disks.
  - SmartTAP DB disk cannot be changed after the installation.
  - SmartTAP media storage configuration can be changed after the installation.
  - The additional managed disks are not required for POC if the SmartTAP Server's OS disk has sufficient space.
  - The size of the media disk should be calculated (using the SmartTAP storage calculator) with the provision of sufficient space for the ongoing recordings and in the case of Azure Blob storage, for recordings that might need to be buffered when there is a temporary disconnection with Azure.

- The additional media disk is not required for lower loads of up to 50 concurrent audio recordings, however it's recommended.
- **SmartTAP SIPRec availability:** SmartTAP SIPRec availability is based on Azure Virtual Machines (VM) Service Level Agreement (SLA):
- SmartTAP Server on Azure VM - SLA is 99.9% for one instance and 99.99% can be achieved by deploying the two servers in different Availability Zones (optionally available at extra cost). Refer to [Azure VM SLA](#).
- **SmartTAP SIPRec Backup/Restore:** Azure Virtual Machines (VM) backup/restore procedures are highly recommended.



- Playback performance depends on CPU availability; slowness of the Web interface may be experienced when there are insufficient CPU resources to execute playback: For optimal audio playback performance, the number of concurrent playbacks should not exceed the number of CPU cores - 1.
- Concurrent recording specifications should be equal to the maximum simultaneous calls that can be made by the targeted users for recordings; this includes all recording types e.g. Full Time Recording, Record on Demand, Save on Demand.



## 4 Requirements for Other Integrations

This section describes requirements for other integrations including Skype for Business including:

- [Server Configurations](#) below
- [Supported Virtual Machine \(VM\) Environments](#) on page 24
- [Supported Microsoft Integrations](#) on page 24
- [SBA Integration](#) on page 24

### Server Configurations

The following table lists the maximum available resources for three different SmartTAP 360° server profiles and for the Media Proxy and Announcement servers.



- Resources refers to Audio, Video, Announcement and Screen Sharing licenses.
- When SmartTAP 360° server is deployed on Microsoft Azure, see Microsoft Teams Deployment Specifications.

Figure 4-1: SmartTAP 360° Server

Server	Specification	Available Resources
SmartTAP 360° server (Low Profile)	<ul style="list-style-type: none"> <li>■ 2 Core 2.5 GHz</li> <li>■ 6 GB Memory</li> <li>■ 2 SATA 7200 RPM HDD/SSD*</li> <li>■ PCIe slots FL / FH2**</li> </ul>	50 resources (audio only)
		25 resources when Media Proxy Service is installed on the same server (audio only)
SmartTAP 360° server (Medium Profile)	<ul style="list-style-type: none"> <li>■ 6 Cores 2 GHz****</li> <li>■ 8 GB Memory</li> <li>■ 2 SATA 7200 RPM HDD/SSD*</li> <li>■ PCIe slots FL / FH2**</li> </ul>	150 resources
		50 resources when Media Proxy Service is installed on the same server (audio only)
SmartTAP 360° server*** (High Profile)	<ul style="list-style-type: none"> <li>■ 12 Core 2 GHz****</li> <li>■ 14 GB Memory</li> <li>■ 2 SATA 7200 RPM HDD/SSD*</li> <li>■ PCIe slots FL / FH2**</li> </ul>	300 resources 500 audio resources
Media Proxy server***	<ul style="list-style-type: none"> <li>■ Quad Core 2 GHz (300 resources)</li> </ul>	300 resources 500 audio resources

Server	Specification	Available Resources
	<ul style="list-style-type: none"> <li>8 Core 2 GHz (500 audio resources)</li> <li>8 GB Memory</li> <li>SATA 7200 RPM HDD/SSD*</li> </ul>	
Announcement server***	<ul style="list-style-type: none"> <li>Quad Core 2 GHz</li> <li>8 GB Memory</li> <li>SATA 7200 RPM HDD/SSD*</li> </ul>	300 resources (assuming the announcement length does not exceed 20% of an average call length)

\*SmartTAP 360° server requires two dedicated HDDs/SSDs - one disk for the Windows OS, SmartTAP 360° application software and DB. Another disk is required for the recorded media. The application disk size should be large enough to hold the OS (refer to Microsoft documentation for the disk space requirements) minimum application space and the DB space. Use the SmartTAP storage calculator for DB size estimation. The size of the media disk should be large enough to hold the media; the estimated size of the media can be calculated using the SmartTAP storage calculator. The media disk is required for both local or remote media storage, in case of the temporarily media, make sure the media disk has enough capacity to hold recordings' media over a time that external storage may not be accessible. When running the SmartTAP 360° Server in a virtual environment, the HDDs/SSDs has to be dedicated and mapped to SmartTAP 360° server VM.

\*\* PCIe Full Length / Full Height slots. The number of slots required is determined by the number of Analog Stations required to record. Each card can record 24 channels (i.e., 56 Phones will require three PCIe card slots).

\*\*\* A group of these servers can be deployed when more than the supported recording capacity in one server is required. An additional high-end server is required to be deployed for the Application Server and Database.

\*\*\*\* Higher CPU speed (higher than 2.0 GHz) is recommended to accelerate download and playback for Video or Screen Sharing recorded calls.



- When running in a virtual environment, all specification resources in the table above must be reserved for all servers of SmartTAP 360°.
- Dual GB NIC interfaces are required for VoIP Port Mirroring Integration Configuration (this is not relevant for Skype for Business and SIP Recording).
- Playback performance depends on CPU availability; slowness of the Web interface may be experienced when there are insufficient CPU resources to execute playback:
  - ✓ For optimal audio playback performance, the number of concurrent playbacks should not exceed the number of CPU cores - 1
  - ✓ For optimal video playback performance, the number of concurrent playbacks should not exceed the half the number of CPU cores
- Concurrent recording specifications should be equal to the maximum simultaneous calls that can be made by the targeted users for recordings; this includes all recording types e.g. Full Time Recording, Record on Demand, Save on Demand.
- Maximum capacity of 3000 users and 1000 concurrent recordings. A single server can handle up to 500 audio recordings. When more than a single server capacity is required (server cluster deployment), one high end SmartTAP server for management purposes including an Application Server and DB should be deployed together with a number of RDDs for recordings. For example, when 1000 audio concurrent recordings are required, three high end servers need to be deployed: a SmartTAP server together with two RDDs each handling 500 concurrent recordings.

To determine the server specification, calculate the required available resources. The calculation of the required resources is based on the number of licenses multiplied by one of the factors specified in the table below.

**Figure 4-2: License Factors**

License Type	Factor
Audio Recorder License	1
Video Recorder License	10
Announcement License	1
Screen Sharing License	5

- Calculate the required number of resources on the SmartTAP 360° server and the Media Proxy server according to the following formula:

**Required Number of Resources = (Number of Audio Recorder Licenses)\*(Audio Recorder License Factor) + (Number of Video Recorder Licenses)\*(Video Recorder License Factor) + (Number of Screen Sharing Recorder Licenses)\*(Screen Sharing Factor)**

Choose the SmartTAP 360° server and Media Proxy server with the number of available resources equal or higher than the required recording resources.

- Calculate the required number of resources on the Announcement server according to the following formula:

Required Number of Resources = (Number of Announcement Licenses)\*(Announcement License Factor)

**Example 1:** 100 Audio Recorder Licenses

- Required Number of Resources = (100 Audio Recorder Licenses)\*(1 Audio Recorder License Factor) = 100
- Choose Medium Profile SmartTAP 360° server and one Media Proxy server

**Example 2:** 30 Video Recorder Licenses

- Required Number of Resources = (30 Video Recorder Licenses)\*(10 Video Recorder License Factor) = 300
- Choose High Profile SmartTAP 360° server and one Media Proxy server

**Example 3:** 50 Audio Recorder Licenses and 20 Video Recorder Licenses

- Required Number of Resources = (50 Audio Recorder Licenses)\*(1 Audio Recorder License Factor) + (20 Video Recorder Licenses)\*(10 Video Recorder License Factor) = 50 + 200 = 250
- Choose High Profile SmartTAP 360° server and one Media Proxy server

**Example 4:** 40 Audio Recorder Licenses

- Required Number of Resources = (40 Audio Recorder Licenses)\*(1 Audio Recorder License Factor) = 40
- Choose either of the following:
  - Medium Profile SmartTAP 360° server with Media Proxy service installed on the SmartTAP 360° server
  - Low Profile SmartTAP 360° server and separate Media Proxy server

**Example 5:** 200 Audio Recorder Licenses with Announcement

- For SmartTAP 360° server and Media Proxy servers:
  - Required Number of Resources = (200 Audio Recorder Licenses)\*(1 Audio Recorder License Factor) = 200
  - Choose High Profile SmartTAP 360° server and one Media Proxy server
- For Announcement server:
  - Required Number of Resources = (200 Announcement Licenses)\*(1 Announcement License Factor) = 200
  - Choose one Announcement server

**Example 6:** 50 Audio Recorder Licenses and 50 Screen Sharing Recorder Licenses

- For SmartTAP 360° server and Media Proxy servers:

- Required Number of Resources = (50 Audio Recorder Licenses)\*(1 Audio Recorder License Factor) + (50 Screen Sharing Recorder Licenses)\*(5 Screen Sharing Recorder License Factor) = 300
- Choose High Profile SmartTAP 360° server and one Media Proxy server

## Supported Virtual Machine (VM) Environments

### VMware ESXi

- Version 4.1 and higher (IP-based integrations only)
- See Enabling Promiscuous Mode on VMWare ESXi for instructions on how to enable promiscuous mode required for a SmartTAP 360° system that is monitoring (tapping) the network.

### Microsoft Hyper-V

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 64bit



Hyper-V does not support promiscuous mode. Do not use in Passive integration environments.

## Supported Microsoft Integrations

- Skype for Business 2015
- Skype for Business 2019
- Microsoft Teams

## SBA Integration

The SmartTAP 360 server with low-profile can be deployed on AudioCodes Mediant 1000B with OSN Server (Mediant 1000B OSN4B 256 GB SSD) together with the Survivable Branch Appliance (SBA) where the SBA is configured with up to 250 users and 8 trunks per branch.

## 5 Supported Microsoft Windows OSS

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2

## 6 Application Footprint

The estimated application footprint for all integration types is 25 GB with a default logging configuration.

## 7 Windows Updates

- It is recommended to disable Automatic Windows Updates to prevent unknown side effects.
- AudioCodes only certifies major version Service Pack updates.



Before applying Windows updates, ensure that a system backup is performed.

### Installing Windows Updates

- Schedule a maintenance window. SmartTAP does not record during this timeframe.
- Download and install Windows updates.
- Reboot the server, even if Windows does not ask you to reboot to finish installing updates.
- Windows may continue installing updates after the system restart which may cause instability within SmartTAP.
- Once the Windows updates are complete, reboot the server again.



## 8 Antivirus Software and Windows Defender

- No virus software is included with SmartTAP
- No specific virus software is tested or certified
- If installed, do not scan the following SmartTAP folders and contents to prevent performance impact:
  - Media path: (i.e., Local D:\Media, SAN or NAS)
  - ...\\Ai-Logix\\
  - ...\\AudioCodes\\
  - ...\\MySQL\\
- If installed, do not scan the following Teams BOT folders and contents to prevent performance impact:
  - C:\Program Files\Microsoft Service Fabric
  - D:\SvcFab
  - C:\ProgramData\SF
  - C:\MiMedia
  - C:\Program Files (86)\AudioCodes
- For **Windows Defender** disable scanning the same file types and folders.

**This page is intentionally left blank.**

**International Headquarters**

6 Ofra Haza Street

Naimi Park

Or Yehuda, 6032303, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

**AudioCodes Inc.**

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

**Contact us:** <https://www.audiocodes.com/corporate/offices-worldwide>

**Website:** <https://www.audiocodes.com/>

**Documentation Feedback:** <https://online.audiocodes.com/documentation-feedback>

©2024 AudioCodes Ltd.. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-27311

