Cloud SIP Phone Support (cSPS)

Version 0.3.x

Skype for Business

audiocodes

Table of Contents

This page is intentionally left blank.

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: June-7-2020

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Document Revision Record

LTRT	Description
28815	Initial document release for Version 0.2.x
28816	Updates for Version 0.3.x

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.

This page is intentionally left blank

1   Introduction

Cloud SIP Phone Support (cSPS) software allows connectivity of standard SIP devices to Microsoft Skype for Business Online, including DECT and Voice over Wi-Fi (VoWifi) base stations, analog devices (gateways), SIP desk phones and customized SIP devices.
This version supports the following features:

- ■ **Multi-user Device Registration**: Defines the terminating device registration from the SPS.

- ■ **Outgoing Calls**: Users can make outgoing calls.

- ■ **Incoming Calls**: User can receive incoming calls.

- ■ **Hold Un-hold, Switch Between Calls**: Calls may be placed on Hold, Un-hold and users can switch between calls.

- ■ **Swagger GUI:** The current cSPS version supports a simple GUI (Swagger) that only works locally on the server.

- ■ **Transfer Calls:** Users can relocate the call to another phone.

- ■ **End User Self-service GUI:** An SPS Online user must activate their account before it can be used. Activation is performed by the user running a Web API on the server while signed in to their Azure account.

- ■ **User Presence**: The current version supports only Busy (in a call) mode.

- ■ **Conference**: The current version supports Conference Calls.

- ■ **TCP only:** The current version supports TCP only.

This page is intentionally left blank.

2   New Features

This section lists the new features added to the new version.

2.1   Software Update 0.3.4.0

This section describes software update 0.3.4.0.

2.1.1   Get Version REST API

Added Get Version REST API to the app and the UCMA versions to the Swagger.

2.2   Software Update 0.3.3.0

This section describes software update 0.3.3.0.

2.2.1   Member in Too Many Groups

In previous versions, an error occurred with an unauthorized SpsAdmin group member, caused by an administrator being a member in too many groups. As a result, the token was not returning all member groups, if there were four or more groups. The 'hasgroups' value is returned and a graph query is required for the groups. This problem has now been fixed.

> **Note:** A new Azure API permission must be added to the SpsOnline application:
>
> From the Azure Portal, navigate to **Active Directory** > **App Registrations** > **SpsOnline** > **View API Permissions**.
>
> Select **Add a Permission** > **Microsoft Graph** > **Application Permissions** > **Group.**
>
> Select **Group.ReadAll** > **Add Permissions**.
>
> Click **Add admin consent for**.

2.2.2   User Token Refresh Task

A 'user token' refresh task that runs every night, was added This should solve the problem of the refresh token expiring after 90 days.

If the user was inactive for 90 days and then tries to log in, the login will fail and the user will need to re-activate.

2.3   Software Update 0.3.2.0

This section describes software update 0.3.2.0.

2.3.1   Trusted Register IPs

Clients registering from a trusted IP are trusted and the server does not challenge them for authentication. Trusted IPs are configured as one or more IP address ranges in CIDR format.

Specific web APIs were added to be set and delete trusted IP addresses configuration.

2.4 Software Update 0.3.1.0

This section describes software update 0.3.1.0.

2.4.1 Debug Swagger Operation

Added debug swagger test for printing user token claims.

2.5 Software Update 0.3.0.0

This section describes software update 0.3.0.0.

2.5.1 16KHz Audio HD Support

By default, 16KHz audio is supported in both IPP SIP and S4B legs. This greatly improves sound quality.

Previously, due to UCMA limitations, audio was sampled at 8KHz. Even if a 16KHz codec was used, audio was sampled at 8KHz and up-sampled to 16KHz. Therefore, it is not possible to see this change by inspecting the codecs only. This change is best witnessed by comparing previous and new audio quality.

This feature is configurable by the Boolean value 'Data.SipConfig.Use8KHz' (see the configuration below).

2.5.2 Central Database Configuration

The application configuration is now stored in the MongoDB database. This feature enables multiple servers to share the same configuration and easily add new servers.

Previously, all configurations were stored in a local application configuration file. Now, the local application configuration file is used only for storing the database connection string.

2.5.3 Global and Local Configuration

The database includes a global configuration entry and an entry for each server. Entries are created automatically. This enables each server to have a different configuration, if needed.

Each server uses its own entry. The global entry is used as a 'template' for creating a server specific entry.

2.5.4 Hierarchical Configuration

The configuration is now organized into four groups:

- System
- SpsAzureApp
- AdminAzureApp
- SipConfig

Within each group, there are multiple leaf values. Each value has a unique key - for example:

```
"Data.System.MinRtpPort": 1025,
"Data.SpsAzureApp.Tenant": "audiocode.biz",
```

2.5.4.1 Modifying Configuration

Several REST APIs, accessible by Swagger, enable modifying configuration.

Most APIs require a server parameter that is either '*' for the global entry, or the case sensitive server name (There is also an API to list available servers).

The APIs enable setting all configurations at once (not recommended), or setting a specific leaf value, for example, setting the value of 'Data.SipConfig.DefaultSipDomain'.

The paths to all leaves are also available in the API.

Modifying a global value ('*') modifies the global entry and all server specific entries.

Modifying a server specific value only modifies that server value.

In addition to the general APIs, there are specific helper APIs to simplify specific configuration tasks, such as setting/modifying/deleting trusted IPs, getting and setting Azure applications configuration, etc.

2.5.4.2 Upgrade

The upgrade of existing configurations is done automatically the first time the new version is run. The upgrade procedure copies local values to the database (if entry doesn't exist) and clears the local configuration file, except for the connection string.

2.5.4.3 Access Control

All REST APIs require an authenticated user that belongs to a specific administrators group.

However, authentication configuration is also stored in the database. Therefore, configuration APIs require special access to initially configure a server.

The solution is to allow unauthenticated access to configuration APIs from the **localhost server** and regular authenticated access from anywhere. Unauthenticated remote access is denied. Access to all other APIs remain the same.

2.5.5 Central SIP Registrations (SIP High Availability)

SIP registrations were always stored in the database. However, since the new version enables the multiple servers to share the same database, an additional column was added for the registrations table to specify the host server.

Upon SIP registration, the SPS server adds/updates the registration with its host name.

Whenever an SPS server starts, it only uses its own SIP registrations. Registrations by other servers are ignored. This feature enables SIP high availability by configuring SIP phones with a primary and backup registrar.

Notes:

- When a phone changes registration to another SPS, the existing registration is modified. A new entry is NOT created.
- The SPS never deletes a SIP registration. It is deleted automatically by MongoDB according to the SIP registration expiry time.

2.5.6 SIP TLS and SRTP Support

This new version supports the SIP leg using TLS and SRTP. **By default, they are both disabled.**

> **Note:** The S4B leg always uses HTTPS and SRTP

2.5.7   Enabling TLS Support

- A server certificate to the Local Computer/Personal/Certificate store issued to the SPS server FQDN, was added. The certificate must be trusted.
- SPS is configured to use this certificate by setting the 'Data.SipConfig.CertificateThumbPrint' value to the certificate thumbprint.
- Restart
- Now you should also configure phones to use TLS. This requires installing a certificate for the phones.
- Note that all certificates, in SPS and phones, must all be trusted.

2.5.8   Disabling TLS

Configure the 'Data.SipConfig.CertificateThumbPrint' value to its default value (disabled).

2.5.9   SRTP Support

SPS supports three SRTP modes, all configured by the 'Data.SipConfig.Srtp' key:

- **Disabled:** By default, SPS does not use SRTP.
- **Supported:** SPS offers and accepts SRTP but does not require the other side to use SRTP.
- **Required:** SPS offers and requires SRTP to/from other side.

3 Known Constraints

The table below shows the known constraints.

Table 3-1: Known Constraints

Incident	Discovered Version	Resolved Version	Description
APPSPSO-53	0.2.0.15	0.3.0.0	Reject a call, when a call to voicemail disconnects immediately.
-	0.2.0.15	-	Up to 500 Registrations and 80 concurrent calls were tested.
APPSPS-5	0.2.0.15	-	cSPS can't be used as a Common Area phone.
-	0.2.0.15	-	cSPS does not play Music-on-Hold; this action should be performed by end user clients (Skype client or IP Phone/DECT).
APPSPSO-50	0.2.0.15	-	Setting Call Forward Unconditional (CFU) via the IP Phone does not work; setting CFU via a PC client does work.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

200 Cottontail Lane

Suite A101E

Somerset NJ 08873

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

Website: https://www.audiocodes.com/

![audiocodes logo]