AudioCodes One Voice for Microsoft® Skype for Business

Cloud SIP Phone Support (cSPS)

Version 0.3





Microsoft Partner

Caudiocodes

Table of Contents

Intro	oduction	
1.1	About cSPS for Skype for Business Online	
Gett	ting Started	
2.1	Downloading Files	
22	Installing cSPS	
23	Installing the Microsoft Infrastructure	
2.0	2.3.1 Installing NET Framework	
	2.3.2 Installing Media Foundation	
	2.3.3 Installing PowerShell	
2.4	Setting up Applications on Azure AD	
	2.4.1 Creating a New Security Group for cSPS Admin	
	2.4.2 Adding cSPS Application	
	2.4.3 Add cSPS Admin Application	
	2.4.4 Granting Permission for Admin application	
2.5	Installing UCMA	
2.6	Creating a Self-signed Certificate	
	2.6.1 Generating a New Certificate if Needed	
2.7	Installing the cSPS Application	
2.8	Installing MongoDB	
	2.8.1 Installing MongoDB as Standalone	
	2.8.2 Installing MongoDB Replica Set (High Availability)	
	2.8.2.1 Configuring MongoDB	
2 0	Configure the oSDS Application	
2.9	Configure the CSPS Application	
	2.9.1 Global and Local Configuration	
	2.9.3 Modifying Configuration	
	2.9.4 Upgrading	
	2.9.5 Access Control	
	2.9.6 Setting the Local Firewall	
~	2.9.7 Firewall	
2.10	Installing Self-Service Web interface	
	2.10.1 General	
	2.10.2 Requirements	
	2.10.3.1 Configuring HTTPS SPS Web API Access	
	2.10.3.2 Azure App Service – Part 1	
	2.10.3.3 Azure Application	
	2.10.3.4 Azure App Service – Part 2	
	2.10.4 SPS Unline Self-Service Hosted on Cloud SPS Server	
	2 10 4 2 Installing NGINX Web Server	
	2.10.4.3 NGINX Configuration	
	2.10.4.4 Configuring HTTPS	
	2.10.4.5 Configuring NGINX to run as Windows Service	
	2.10.5 Using the Self-Service	
Man	naging Users	
3.1	Logging in with Swagger	
3.2	Managing Users Operations	

4	Μοι	nitoring SPS using Swagger	59
	4.1	SipRegistration	59
	4.2	OnlineUsers	59
	4.3	Call Status	60
5	cSF	PS Debugging Tools	61
A	Арр	pendix – Collecting Azure Information	63
В	Арр	pendix – SIP TLS and SRTP Support	65
	B.1	Enabling TLS Support	65
	B.2	Disabling TLS	65
	B.3	SRTP Support	65

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-1-2020

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 Web site at https://www.audiocodes.com/services-support/maintenance-and-support.

Software Revision Record

The following table lists the software versions released in Version 0.3.

Table 1-1:	Software	Revision	Record
------------	----------	----------	--------

Software Version	Date
0.3.0.0	Jul 2019
0.3.3.0	Jan 2020
0.3.4.0	Feb 2020
0.3.6.0	April 2020

Note: The latest software versions can be downloaded from:



3rd Party: <u>https://downloads-</u> audiocodes.s3.amazonaws.com/SPSOnline/SpsOnline3Party.zip

cSPS: <u>https://downloads-</u> audiocodes.s3.amazonaws.com/Download/AC_cSPS_Install.html

Document Revision Record

LTRT	Description
00843	Initial document release for Version 0.3

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 Web site at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This document describes how to install, configure, manage and monitor the cSPS for Skype for Business Online.

1.1 About cSPS for Skype for Business Online

Cloud SIP Phone Support Online (cSPS) is a value-added application that enables third-party SIP IP phones to smoothly connect with Skype for Business Online. cSPS is a software product that can run on a physical server, virtual machine or on an OSN (Open Solution Network) server hosted by the gateway and E-SBC. Both the Mediant 1000 and the Mediant 800 devices support SPS installed on the OSN.

This page is intentionally left blank.

2 Getting Started

The following are the minimum server specifications for 500 users:

- CPU: 4 Physical cores
- Memory: 8GB RAM
- Hard Disk: 80G

The following Operating Systems are supported:

- Windows Server 2019 (Desktop Experience), 64-bit version
- Windows Server 2016, 64-bit version
- Windows Server 2012 R2, 64-bit version



Note: The Operating System should be "clean" with no additional software/applications previously installed. Windows updates must be performed before starting the installation.

The following procedures are required for setting up cSPS:

- 1. Prepare the Windows Server See Section 2.3 on page 10
- 2. Setup Applications on Azure AD See Section 2.4 on page 11
- 3. Install MongoDB See Section 2.8 on page 32
- 4. Install UCMA See Section 2.5 on page 30
- 5. Create a self-signed certificate See Section 2.6 on page 30
- 6. Install the cSPS Application See Section 2.7 on page 31

For now, most of the steps are performed manually without any wizard.

Appendix A includes a form that you can use to save all the information from Azure, that will be used later in the cSPS configuration.

2.1 Downloading Files

There are two links for downloading. Copy both to the cSPS Server and unzip.

3rd party components that are used by the cSPS:

https://downloads-audiocodes.s3.amazonaws.com/SPSOnline/SpsOnline3Party.zip

The cSPS software – this link is used for also downloading the upgrade version. <u>https://downloads-audiocodes.s3.amazonaws.com/Download/AC_cSPS_Install.html</u>

2.2 Installing cSPS

This section describes how to install the cSPS.

2.3 Installing the Microsoft Infrastructure

This section outlines how to install the Microsoft Windows features and components on the cSPS server. This is a prerequisite for and needs to be performed **before** running the cSPS Installation.



Note: cSPS Server can be a member of a workgroup instead of a domain.

2.3.1 Installing .NET Framework

This section describes how to install .NET Framework.

- To install the .Net Framework:
- 1. Open the Server Manager on the SPS server.
- 2. Go to Features > Add Features; the Add Roles and Features Wizard is displayed:

📥 Add Roles and Features Wizard		- 🗆 X
Select features		DESTINATION SERVER MDB3
Before You Begin	Select one or more features to install on the selected server.	
Installation Type	Features	Description
Server Selection	▶ 🗹 .NET Framework 3.5 Features	.NET Framework 3.5 combines the
Server Roles	 NET Framework 4.6 Features (2 of 7 installed) 	power of the .NET Framework 2.0 APIs with new technologies for
Features	ASP.NET 4.6	building applications that offer
Confirmation	▲ WCF Services (1 of 5 installed)	appealing user interfaces, protect
Results	 HTTP Activation Message Queuing (MSMQ) Activation Named Pipe Activation TCP Activation TCP Port Sharing (Installed) ■ Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock BranchCache Client for NFS Containers Data Center Bridging Direct Play Enhanced Storage 	your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
	< <u>P</u> revious <u>N</u> ext	> <u>I</u> nstall Cancel

3. Select the **.NET Framework 3.5 Features** check box, and then click the **Install** button. If you get errors regarding the .Net3.5 installation, try the following command. On drive D:, you should have a mounted Windows Server 2019 iso.

```
DISM /Online /NoRestart /Enable-Feature
/FeatureName:NetFx3ServerFeatures /Source:D:\sources\sxs
```

DISM /Online /NoRestart /Enable-Feature /FeatureName:NetFx3
/Source:D:\sources\sxs

- 4. For Windows 2019, select .Net Framework 4.7 Feature as well.
- 5. For Windows 2016, select .Net Framework 4.6 Feature as well.
- 6. For Windows 2012 R2, select .Net Framework 4.5 Feature as well.
- 7. Install .Net Framework 4.7.2 or higher. You can use the offline installer for .Net Framework (NDP472-KB4054530-x86-x64-AllOS-ENU.exe from the 3rd party ZIP file). http://go.microsoft.com/fwlink/?linkid=863265

2.3.2 Installing Media Foundation

Install Media Foundation by opening the Microsoft Server Manager and navigating to **Add Features**. Enable the Media Foundation feature.

2.3.3 Installing PowerShell

Install Windows PowerShell by opening the Microsoft Server Manager and navigating to **Add Features**. Enable the Windows PowerShell feature.

2.4 Setting up Applications on Azure AD

Three applications must be created in Azure portal <u>https://portal.azure.com</u>



Note: This should be done only for the first cSPS server. All other cSPS servers for the same tenant use the same applications IDs.

2.4.1 Creating a New Security Group for cSPS Admin

The procedure below describes how to create a new security group for cSPS Admin.

- To create a new security group for cSPS Admin:
- 1. On Azure AD, create a new security group. Only users that belong to this group will be able to manage the cSPS and perform administrator operations on it.
- 2. Save the Group ID. We will need it for the cSPS configuration.
- 3. Add this group to the users which will be the administrator of the cSPS.

2.4.2 Adding cSPS Application

The procedure below describes how to add a cSPS application.

- To add a cSPS application:
- 1. In the Azure Active Directory pane, click the **App registrations** menu option, and then select **New registration**.



- 2. In the 'Name' field, enter **SpsOnline**.
- 3. From the 'Redirect URI' drop-down list, select **Web**; enter the Redirect URL "<u>http://localhost:9000".</u>

v

Home > Test_Test_Test_Audiocodes(R&D lab) - App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SpsOnline

Supported account types

Who can use this application or access this API?

	_
Accounts in this organizational directory only (Test_Test_Audiocodes(R&D lab) only - Single tenant)	
Accounts in any organizational directory (Any Azure AD directory - Multitenant)	
Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)	

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

> V http://localhost:9000		http://localhost:9000
---------------------------	--	-----------------------

- 4. Click **Register** to create the new application.
- 5. In the succeeding page, find the **Application ID** value and copy it, as it will be needed later.

🛅 Delete 🌐 Endpoints
O Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? →
Display name : SpsOnlineTest
Application (client) ID : 557fb13b-db7d-4c92-8c25-2c161b6eb621
Directory (tenant) ID : e2fe003e-5130-4f5b-9050-6f1cb7857891
Object ID : af9a1cbe-eaf5-495e-aa3e-db32b005a10c

6. Under the 'Manage' side menu, select Expose an API.

7. Select Application ID URI Set.

Home > Test_Test_Test_Audiocodes(R&D lab) - App registrations > SpsOnlineTest - Expose an API		
SpsOnlineTest - Expose an API		
,© Search (Ctrl+/) «	Application ID URI 😝 Set	
Overview		
📣 Quickstart	Scopes defined by this API	
Manage	Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.	
🚾 Branding	+ Add a scope	
Authentication	SCOPES WHO CAN CONSENT ADMIN CONSENT DISPLAY NAME USER CONSENT DISPLAY NAME STATE	
📍 Certificates & secrets		
API permissions	ivo scopes nave been derimed	
🚳 Expose an API		
👪 Owners	Authorized client applications	

Set the App	URI	
Application ID https://cce.aced	RI cation.info/SpsOnline	
Save	Discard	

- In the Set the App ID URI screen, replace the Application ID URI with the following URI: 'https://<your_tenant_name>/SpsOnline' (replacing <your_tenant_name> with the name of your Azure AD tenant).
- 9. Click Save.
- 10. Click Add a Scope.
- **11.** In the 'Scope name' field, enter "user_impersonation".
- **12.** In the 'Who can consent' field, select **Admin and users**.
- 13. In the 'Admin consent display name' field, enter "Access SpsOnline".
- 14. In the 'Admin consent description' field, enter "Allow the application to access SpsOnline on behalf of the signed-in user."
- 15. In the 'User consent display name' field, enter "Access SpsOnline".
- **16.** In the 'User consent description' field, enter "Allow the application to access SpsOnline on your behalf".

* Scope name 🜒
user_impersonation 🗸
https://cce.aceducation.info/SpsOnline/user_impersonation
Who can consent?
Admins and users Admins only
* Admin consent display name 📵
Access SpsOnline
* Admin consent description
Allow the explication to serve Co-Colling on helpelf of the singer line way
Allow the application to access spschline on behalf of the signed-in user.
User consent display name 👩
Access SosOnline
User consent description ()
Allow the application to access SpsOnline on your behalf.
State 🚯
Enabled Disabled

- 17. Click Add scope.
- 18. Open Certificates & secrets, and then select New client secrets.
 - a. In the 'Description' field, enter a key description of the instance app secret.

- **b.** In the 'Expires' field, select a key duration of either **In 1 year, In 2 years,** or **Never**. When you add this new key, the key value is displayed.
- c. Copy and save the value in a safe location.



Note: You need this key for later. This key value will not be displayed again, nor retrievable by any other means. So record it as soon as it is visible from the Azure portal.

Home > SpsOnlineTest - Certificat	es & secrets			
💡 SpsOnlineTest - Cert	tificates & secrets			
,C Search (Ctrl+/)	Add a client secret			
8 Overview	Description			
📣 Quickstart	Key			
Manage	Expires			
🧰 Branding	In 1 year			
Authentication	Never			
Certificates & secrets				
-> API permissions	Add Cancel			
Expose an API	THUMBPRINT		START DATE	EXPIRES
🛃 Owners				
🧟 Polor and administrators (Dravi				
Home > SpsOnlineTest - Certificates & se	ecrets			
🔶 SpsOnlineTest - Certificat	tes & secrets			
	•			
,O Search (Ctrl+/)	Copy the new client secret value. You won't	t be able to retrieve it after you leave th	s blade.	
🖶 Overview	Credentials enable applications to identify the	emselves to the authentication servic	e when receiving tokens at a web addressable location (usin	g an HTTPS scheme). For a
📣 Quickstart	higher level of assurance, we recommend usi	ng a certificate (instead of a client se	cret) as a credential.	
Manage	Certificates			
m Branding	Certificates can be used as secrets to prove the	he application's identity when reques	ting a token. Also can be referred to as public keys.	
Authentication	Tupload certificate			
Certificates & secrets	No certificates have been added for this appl	lication.		
API permissions				
Expose an API	THUMBPRINT	START DATE	EXPIRES	
Owners				
Roles and administrators (Previ	Client secrets			
Manifest	A secret string that the application uses to pr	ove its identity when requesting a to	ken. Also can be referred to as application password.	
Support + Troubleshooting	+ New client secret			
X Troubleshooting	DESCRIPTION	EXPIRES	VALUE	
New support request	KeyTest	12/31/2299	Rf[0vowzRmDwhG/wijsjbAfMXwAaA260 IP	商
				<u> </u>



19. Under API permissions, select Add a permission.

Home > SpsOnlineTest - API permissions					
SpsOnlineTest - API perm	nissions				
,> Search (Ctrl+/) «	API permissions				
 Overview Quickstart 	Applications are authorized to call APIs all the permissions the application nee	when they are granted ds.	permissions by users/admins as part	of the consent process. The list of configure	ed permissions should include
Manage	+ Add a permission	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED	STATUS
 Branding Authentication 	✓ Microsoft Graph (1)				
📍 Certificates & secrets	User:Read	Delegated	Sign in and read user profile	-	
-D- API permissions	These are the permissions that this app	lication requests statical	Ily. You may also request user consen	t-	
Expose an API	able permissions dynamically through	code. See best practices	for requesting permissions		
Owners					
Roles and administrators (Previ	Grant consent				
Manifest	As an administrator, you can grant con users will not be shown a consent scre	sent on behalf of all use en when using the applic	rs in this directory. Granting admin co cation.	onsent for all users means that end	
Support + Troubleshooting	Grant admin consent for Test_Test_Te	st_Audiocodes(R&D lab)			
★ Troubleshooting					
New support request					

20. Select Microsoft APIs, and then select Microsoft Graph.



Request API permissions	
< All APIs	
MICrosoft Graph https://graph.microsoft.com/ Docs 🖸	
What type of permissions does your application require?	
Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
Select permissions	expand all
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
► AccessReview	
AdministrativeUnit	
Application	

22. Under the Group (1) group, select Group.Read.All.

 > EduRoster	
> ExternalItem	
> Files	
∽Group (1)	
 Group.Create Create groups ①	Yes
 Group.Read.All Read all groups ①	Yes
 Group.ReadWrite.All Read and write all groups ①	Yes
 Group.Selected Access selected groups ①	Yes
 > GroupMember	
 > IdentityProvider	
 > IdentityRiskEvent	

23. Under the User (1) group, select Users.Read.All.

TrustFrameworkKeySet	
UserNotification	
Vser (1)	
User.Export.All Export user's data 🕕	Yes
User.Invite.All Invite guest users to the organization ()	Yes
User.Read All Read all users' full profiles ()	Yes
User.ReadWrite.All Read and write all users' full profiles ()	Yes

24. Click Add permissions.

25. Select Add new permissions.

- 26. Select Microsoft APIs, and then select Microsoft Graph.
- 27. Under 'Delegated permissions', select Profile to view the users' basic profile.

Request API permissions	
All APIs Microsoft Graph https://graph.microsoft.com/ Docs [2]	
What type of permissions does your application require?	
Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
Select permissions	expand all
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
email View users' email address 🕦	
Offline_access Maintain access to data you have given it access to ()	•
□ openid Sign users in ●	
View users' basic profile	-
► AccessReview	
AdministrativeUnit	

28. Click Add permissions.

29. Add a new permission - On the Request API Permissions screen, click **Microsoft APIs**, and then select **Skype for Business**.

Request API permissions		
Select an API		
Microsoft APIs APIs my organization	uses My APIs	
Commonly used Microsoft APIs		
Microsoft Graph Take advantage of the tremendous amount Security, and Windows 10. Access Azure AD OneNote, SharePoint, Planner, and more th	of data in Office 365, Enterprise Mobility + , Excel, Intune, Outlook/Exchange, OneDrive, rough a single endpoint.	
Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	Azure DevOps Integrate with Azure DevOps and Azure DevOps server	Azure Rights Management Services Allow validated users to read and write protected content
Azure Service Management Programmatic access to much of the functionality available through the Azure portal	Data Export Service for Nicrosoft Dynamics 365 Export data from Nicrosoft Dynamics CRM organization to an external destination	Control Dynamics 365 Business Central Programmatic access to data and functionality in Dynamics 365 Business Central
Dynamics CRM Access the capabilities of CRM business software and ERP systems	Flow Service Embed flow templates and manage flows	Programmatic access to intune data
Office 365 Management APIs Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity	OneNote Create and manage notes, lists, pictures, files, and more in OneNote notebooks	Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power Bl
PowerApps Runtime Service Powerful data storage, modeling, security and integration capabilities	SharePoint Interact remotely with SharePoint data	Skype for Business Integrate real-time presence, secure messaging calling, and conference capabilities

Request API permissions		×
All APIs		
Skype for Business https://api.skypeforbusiness.com/ Docs [2]		
What type of permissions does your application require?		
Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.	
Select permissions	collapse	all
Type to search		
PERMISSION	ADMIN CONSENT REQUIRED	
▼ Contacts (1)		
Contacts.ReadWrite Read/write Skype user contacts and groups		
 Conversations (2) 		
Conversations.Initiate Initiate conversations and join meetings	-	
Conversations.Receive Receive conversation invites (preview)	-	
▼ Meetings (1)		
Create Skype Meetings ()		
▼ User (1)		
User.ReadWrite Read/write.Skype user information (preview) 0	-	

30. Under **Delegated permissions**, select <u>all</u> permissions.

31. Select Add permissions.

32. Select Grant admin consent, and then select Yes to confirm it.



33. Under 'Delegated permissions', select all permissions.

34. Edit the application manifest. Change "groupMembershipClaims": null to "groupMembershipClaims": "SecurityGroup".

35. Click Save.

Home 2 spsOnlineTest - Manifest	
SpsOnlineTest - Manifes	t
,C Search (Ctrl+/) «	🕂 Save 🗙 Discard 🚡 Upload 🚽 Download
Sverview	The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: Understanding the Azure Active Directory application manifest.
📣 Quickstart	1 (
Manage	<pre>2 "id": "af9a1cbe-eaf5-495e-aa3e-db32b005a10c", 3 "acceptHappedClaims": null,</pre>
🚾 Branding	4 "accessTokenAcceptedVersion": null,
Authentication	5 "addins": [], 6 "allowPublicClient": null,
💡 Certificates & secrets	/ applu : 5570150-00/0-4522-6125-21161066051 , 8 "apple1es":[],
API permissions	9 "oauth2AllowUrlPathMatching": false, 10 "createdDateTime": "2019-08-11112:58:34Z".
Expose an API	<pre>11 "groupHembershipClaims": "SecurityGroup",</pre>
👪 Owners	12 "identifierUris": [13 "https://cce.aceducation.info/SpsOnlineTest"
Roles and administrators (Previ	14], 15 "informationallicis": /
11 Manifest	16 "termsofservice: null,
Support + Troubleshooting	17 "support": null, 18 "privacy": null,
★ Troubleshooting	19 "marketing": null 20 },
New support request	<pre>21 "keyCredentials": [], 22 "knownClientApplications": [],</pre>
	23 "logourl": null,
	24 "logouturl": hull, 25 "name": "ossonlinetest".
	26 "oauth2AllowIdTokenImplicitFlow": false,
	27 "oauth2AllowImplicitFlow": false, 29 "oauth2Parmissions": fl

36. On the Branding screen, set the home page URL to "http://localhost:9000".

Home > Test_Test_Test_Audiocodes(R&D I	ab) - App registrations 🗧 Sps	Online - Branding	
SpsOnline - Branding			
,> Search (Ctrl+/)	🔒 Save 🗙 Discard		
Overview	* Name 🕦	SpsOnline	
📣 Quickstart	Logo	None provided	
Manage	Upload new logo 🚯	Select a file	
Manual Branding	Home page URL @	http://oralbost9000	
Authentication		http://ecanoscageo	
💡 Certificates & secrets	Terms of Service URL \tag	e.g. https://myapp.com/termsofservice	
-> API permissions	Privacy Statement URL 👩	e.g. https://myapp.com/privacystatement	
Expose an API	Publisher Domain 🚯	▲ Unverified	Configure a domain
Owners		The application's consent screen will show 'Unverified'. Learn more about publisher domain [2]	
Roles and administrators (Previ		· –	

37. On the Authentication screen, select the 'ID tokens' check box, and then click **Save**.



,O Search (Ctrl+/)	Save 🗶 Discard 🎽 Try out the new experience 💙 Got feedback?
Overview Quickstart	Suggested Redirect URIs for public clients (mobile, desktop) If you are using the Microsoft Authentication Library (MSAL) or the Active Directory Authentication Library (ADAL) to build applications for desktop or mobile devices, you may select from the suggested Redirect URIs below or enter a custom redirect URI above. For more information, refer to the library documentation.
Nanage	
Branding	msaisa40c/00-9515-4ac2-D0904c1D9410//autri (MISAL ONIY)
Authentication	https://login.live.com/oauth20_desktop.srf (LiveSDK)
Certificates & secrets	
 API permissions 	Advanced settings
Expose an API	
Owners	Logout URL 🜒 e.g. https://myapp.com/logout
Roles and administrators (Previ	
🔟 Manifest	Implicit grant
upport + Troubleshooting	Allows an application to request a token directly from the authorization endpoint, necommenced only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript.
K Troubleshooting	To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:
New support request	Access tokens
	V ID tokens

2.4.3 Add cSPS Admin Application

The procedure below describes how to add a cSPS Admin Application.

- > To add a cSPS Admin Application:
- 1. In the Azure Active Directory pane, click **App registrations**, and then select **New registration**.



- 2. In the 'Name' field, enter "SpsOnlineAdmin" for the application.
- 3. In the Redirect URL' field, select Web, and then enter "http://localhost:9000/swagger".

Register an appli	ication
* Name	
The user-facing display	name for this application (this can be changed later).
SpsOnlineAdmin	
Supported accou	nt types
Who can use this applic	ation or access this API?
 Accounts in this org 	janizational directory only (Test_Test_Audiocodes(R&D lab) only - Single tenant)
O Accounts in any org	janizational directory (Any Azure AD directory - Multitenant)
O Accounts in any org	anizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Help me choose	
Redirect URI (opt	ional)
We'll return the authent	ication response to this URI after successfully authenticating the user. Providing this now is optional and it can be
changed later, but a val	ue is required for most authentication scenarios.
Web	http://localhost:9000/swagger
By proceeding, you agre	ze to the Microsoft Platform Policies [2]
By proceeding, you agre	ee to the Microsoft Platform Policies [2]
By proceeding, you agre	ee to the Microsoft Platform Policies [2]
By proceeding, you agre	te to the Microsoft Platform Policies [2]
By proceeding, you agre	ze to the Microsoft Platform Policies [2]
By proceeding, you agre Register 4. Click	ee to the Microsoft Platform Policies [2]
By proceeding, you agre Register 4. Click 5. On th	ee to the Microsoft Platform Policies [2] Register to create the application.
By proceeding, you agre Register 4. Click 5. On th	ee to the Microsoft Platform Policies [2] Register to create the application. The next page, find the Application ID value and copy it for future use.
By proceeding, you agre Register 4. Click 5. On the ete (1) Endpoints	ee to the Microsoft Platform Policies [2] Register to create the application. the next page, find the Application ID value and copy it for future use.
By proceeding, you agre Register 4. Click 5. On th ete (1) Endpoints elcome to the new and	ee to the Microsoft Platform Policies [2] Register to create the application. the next page, find the Application ID value and copy it for future use. I improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? →
By proceeding, you agre Register 4. Click 5. On the ete (1) Endpoints elcome to the new and name	ee to the Microsoft Platform Policies [2] ■ Register to create the application. The next page, find the Application ID value and copy it for future use. Improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? →
By proceeding, you agree Register 4. Click 5. On the ete (1) Endpoints elcome to the new and name : Spst	ee to the Microsoft Platform Policies [2] Register to create the application. The next page, find the Application ID value and copy it for future use. Improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? OnlineAdminTest
By proceeding, you agre Register 4. Click 5. On the ete (1) Endpoints elcome to the new and name : Spsi tion (client) ID : fcb4	ee to the Microsoft Platform Policies [2] Register to create the application. ne next page, find the Application ID value and copy it for future use. Improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? → OnlineAdminTest te8af-6790-4bf2-88cb-f20b174e4268
By proceeding, you agre Register 4. Click 5. On the ete (1) Endpoints elcome to the new and name : Spsi tion (client) ID : fcb4 ry (tenant) ID : e2fe	ee to the Microsoft Platform Policies [2]

6. Enable the OAuth 2 Implicit Grant by selecting Access tokens and ID tokens on the Authentication screen, under Implicit grant.



- 7. Click Save.
- 8. On the Expose an API screen, select Application ID URI Set.

Home > Test_Test_Audiocodes(R&D lab) - App registrations > SpsOnlineAdminTest - Expose an API						
SpsOnlineAdminTest - Expose an API						
,O Search (Ctrl+/) «	Application ID UR{ 9 Set					
8 Overview						
📣 Quickstart	Scopes defined by this API					
Manage	Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.					
🚾 Branding	+ Add a scope					
Authentication	SCOPES WHO CAN CONSENT ADMIN CONSENT DISPLAY NAME USER CONSENT DISPLAY NAME STATE					
📍 Certificates & secrets						
-> API permissions	No scopes nave been denned					
Expose an API						
🚯 Owners	Authorized client applications					
Roles and administrators (Previ	Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls					

9. Replace the **Application ID URI** with the following URI: 'https://<your_tenant_name>/SpsOnlineAdmin' (replacing <your_tenant_name> with the name of your Azure AD tenant).

Set the App ID URI	
Application ID URI https://cce.aceducation.info/SpsOnlineAdmin	
Save Discard	

- 10. Click Save.
- 11. Click Add a scope and add user name "user_impersonation".
- 12. Select Admin and users for who can consent.
- 13. In the 'Admin consent display name' field, enter "Access SpsOnlineAdmin".
- **14.** In the 'Admin consent description' field, enter "Allow the application to access SpsOnlineAdmin on behalf of the signed-in user.".
- 15. In the 'User consent display name' field, enter "Access SpsOnlineAdmin".
- **16.** In the 'User consent description' field, enter "Allow the application to access SpsOnlineAdmin on your behalf."
- 17. Click Add scope.
- 18. Open Certificates & secrets section and select New client secrets.
 - a. In the 'Description' field, enter a key description of the instance app secret.
 - b. From the 'Expires' field drop-down list, select a key duration of either In 1 year, In 2 years, or Never.
 - **c.** When you add this new key, the key value will be displayed. Copy, and save the value in a safe location.

Add a client secret

Expires	
In 2 years Never	
Add Cancel	

in a safe location. You'll need this key later. This key value will not be displayed again, nor retrievable by any other means. Record it as soon as it is visible from the Azure portal.

💡 SpsOnlineAdminTest - Certificates & secrets							
,O Search (Ctrl+/) «	Copy the new client secret value. You won't be able to retrieve it after you leave this blade.						
 Overview Quickstart 	Credentials enable applications to identify themselves to the authentication senice when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.						
Manage	Certificates						
in Branding	Certificates can be used as secrets to prove the application	n's identity when requestin	g a token. Also can be referred to	as public keys.			
Authentication		→ Upload certificate					
💡 Certificates & secrets	No certificates have been added for this application.	No certificates have been added for this application.					
 API permissions 							
🚱 Expose an API	THUMBPRINT	START DATE		EXPIRES			
Owners							
Roles and administrators (Previ	Client secrets						
0 Manifest	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.						
Support + Troubleshooting	+ New client secret						
★ Troubleshooting	DESCRIPTION	EXPIRES	VALUE				
New support request	KeyAdmin	12/31/2299	S_5Fo5YTklYbCVTMbmpdFak_zv	<mark>«G//р95</mark> [Ъ	Ē		

- **19.** On the API permissions screen, select **Add permission**.
- 20. Select APIs my organization uses, and then select SpsOnline.

ib) - App registrations > SpsOnlineAdminTest - API permissions	Request API permissions
l permissions	Select an API
API permissions Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include	Microsoft APIs APIs my organization uses My APIs Apps In your directory that expose APIs are shown below
all the permissions the application needs.	P sps NAME
API / PERMISSIONS NAME TYPE DESCRIPTION ADMIN CONSENT REQUIRED STATUS	SpsOnline
Microsoft Graph (1)	SpsOnline_Tomer
UserRead Delegated Sign in and read user profile	SpsOnlineAdmin
These are the permissions that this application requests statically. You may also request user consent- able permissions dynamically through code. See best practices for requesting permissions	SpsOnlineAdmin_Tomer
	SpsOnlineAdminErez
Cartering	SpsOnlineErez
Granic consent	SpsOnlineOld
as an administration, you can grant consent on a main of an owner in this directory. Stanting administorisent for an osers means that end users will not be shown a consent screen when using the application.	SpsOnlineSelfService
Grant admin consent for Test, Test, Test, Audiocodes(R&D lab)	SpsTokenCache

21. Click **Delegated Permissions**, and then select the 'user_impersonation' check box.

All APIs	
SpsOnline https://cce.aceducation.info/SpsOnline	
/hat type of permissions does your application require?	
Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
elect permissions	expand
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
user_impersonation	
Access SpsOnline 0	
Access SpyOnline	-

- 22. Click Add Permissions.
- 23. On the API permissions screen, select **Grant admin consent...**, and then select **Yes** to confirm it.

Home > Test_Test_Audiocodes(R&D	lab) - App registrations > SpsOnlineAdminTe	est - API permissions			
ne SpsOnlineAdminTest - AF	PI permissions				
,C Search (Ctrl+/) «	Do you want to grant consent for the	requested permissio	ns for all accounts in Test_Test_Au	udiocodes(R&D lab)? This will update	e any existin
 Overview Quickstart 	No				
Manage	+ Add a permission API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED	STATUS
 Authentication 	 Microsoft Graph (1) 				
📍 Certificates & secrets	User.Read	Delegated	Sign in and read user profile	-	-
API permissions	 SpsOnlineTest (1) 				
Expose an API	user_impersonation	Delegated	Access SpsOnlineTest		
Owners Roles and administrators (Previ Manifest	These are the permissions that this applic able permissions dynamically through co	cation requests statical ide. See best practices	ly. You may also request user consent- for requesting permissions		
Support + Troubleshooting	Grant consent				
 Troubleshooting New support request 	As an administrator, you can grant conse users will not be shown a consent screen Grant admin consent for Test_Test_Test	nt on behalf of all use when using the applic Audiocodes(R&D lab)	rs in this directory. Granting admin conse ation.	nt for all users means that end	



- 24. On the Authentication screen, from the 'TYPE' drop-down list, select Web.
- 25. In the 'REDIRECT URI' field, enter "http://localhost:9000/swagger/ui/o2c-html"

26. Click Save.

Home > Test_Test_Test_Audiocodes(R&D lab) - App registrations > SpsOnlineAdminTest - Authentication					
∋ SpsOnlineAdminTest - Au	Ithentication				
,O Search (Ctrl+/) «	R Save X Discard K Try out the new experience G Got feedback?				
Overview	Redirect URIs				
Guickstant	The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. Learn more about adding using for use housile and desting includes 10 and 10 and 10 and 10 and 10 and 10 and 10				
Manage					
m Branding	ТҮРЕ	REDIRECT URI			
Authentication	Web	http://localhost:9000/swagger			
📍 Certificates & secrets	Web	http://localhost:9000/swagger/ui/o2c-html			
API permissions	Web 🗸 🗸	e.g. https://myapp.com/auth			
🚳 Expose an API					
n Owners	Suggested Redirect URIs for public clients (mobile, desktop)				
Roles and administrators (Previ	If you are using the Microsoft Authentication Library (MSAL) or the Active Directory Authentication Library (ADAL) to build app	olications for			
🔲 Manifest	desktop or mobile devices, you may select nom the suggested redirect only below or enter a custom redirect on above. For information, refer to the library documentation.	more			
Support + Troubleshooting	msalfcb4e8af-6790-4bf2-88cb-f20b174e4268://auth (MSAL only)				
X Troubleshooting	https://login.microsoftonline.com/common/oauth2/nativeclient				
New support request	https://login.live.com/oauth20_desktop.srf (LiveSDK) [["				
	Advanced settings				
	-				
	Logout URL 🕘 e.g. https://myapp.com/logout				
	Implicit grant	cipale page			
	anows an application to request a toten directly from the authorization endpoint, necommended only if the application has a architecture (SPA), has no backend components, or invokes a Web API via JavaScript.	single page			
	To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:				
	Access tokens				
	e te tenterte				

27. On the Branding screen, in the 'Home page URL' field, enter "<u>http://localhost:9000/swagger</u>".

Save X Discard		
* Name 🜒	SpsOnlineAdmin	
Logo	None provided	
Upload new logo 🚯	Select a file	
Home page URL 🚯	http://localhost:9000/swagger	
Terms of Service URL 🚯	e.g. https://myapp.com/termsofservice	
Privacy Statement URL 🕚	e.g. https://myapp.com/privacystatement	
Publisher Domain 🚯	▲ Unverified	Configure a domain
	The application's consent screen will show 'Unverified'. Learn more about publisher domain [2]	

28. Click Save.

2.4.4 Granting Permission for Admin application

- 1. Copy the **Application ID** of the **SpsOnlineAdmin** application.
- 2. Edit the manifest of the **SpsOnline** application.
- 3. In the manifest, locate the **knownClientApplications** array property, and add the Application ID of the **SpsOnlineAdmin** as an element. Your code should look like the following:

"knownClientApplications": ["94da0930-763f-45c7-8d26-04d5938baab2"]

4. Save the manifest.

ne 🖈
s 🧨 Manifest 🏛 Delete
e Application ID S846776-9351-4522-00a-bd904t1be4fd Vpre Object ID 2559c175-bes2-4ed-ad13-ed471fd3e47 Managed application in local directory SptOnline A

2.5 Installing UCMA

The procedure below describes how to install UCMA. cSPS uses Microsoft UCMA 5.0 for the SIP leg.

- To install UCMA:
- 1. Download UCMA 5.0 from https://www.microsoft.com/en-us/download/confirmation.aspx?id=47345.
- 2. After this installation, install a Skype 2015 CU to upgrade the Skype and UCMA components (SkypeServerUpdateInstaller.exe from the 3rd party ZIP file).

2.6 Creating a Self-signed Certificate

A self-signed certificate with a default subject name "localhost" must be installed. See the Certificate directory for a sample 10 year "localhost" certificate, with a private key and certificate public key.

- The private key password for installation is 'password'.
- The certificate with a private key must be installed to the local computer\Personal folder.
- The certificate public key must be installed to local computer\trusted root certificates folder.

We recommended you use these certificates instead of creating new ones. Install them according to the above locations and skip the next section.

2.6.1 Generating a New Certificate if Needed

It can be quite tricky to get a self-signed certificate to work without any problems.



Note: Do not use New-SelfSignedCertificate for creating the certificate - .Net will fail access of the private key with "invalid provider specified".

A solution that worked for us was to use an online service <u>http://www.getacert.com/index.html</u> to create a self-signed certificate with subject name "localhost".

2.7 Installing the cSPS Application

The procedure below describes how to install the cSPS Application.

- > To install the cSPS Application
- **1.** Run the cSPS installation file.
- 2. Validate that you have cSPS configuration file under: C:\Program Files\Audiocodes\SpsOnline\Config\System.config

(If the file does not exist, copy System.config.DIST and rename it to System.config)

2.8 Installing MongoDB

cSPS uses Mongo DB as its database. For SPS High Availability (HA) you have two options:

- Use the Data Center HA capabilities Install the database on a separate server that is set to HA on the Data Center. All cSPS Servers will work with it instead of the local database. In this case, the installation is similar to a standalone server but you need to install the MongoDB on the Data Center server.
- Use MongoDB Replica Set Install an odd number of MongoDB nodes (can run locally on the cSPS Server too). This way, one server is the primary server and the others are secondary. Data is synchronized between all nodes. A minimum number of three nodes is required.



Note: A majority of the members must be running and communicating with each other to provide service. (An arbiter node can be used as well, instead of a full database, as less resources are needed).

We support MongoDB Version 4.0.x (Mongo DB community Windows x64 msi) (mongodb-win32-x86_64-2008plus-ssl-4.0.x-signed.msi from the 3rd party ZIP file).

2.8.1 Installing MongoDB as Standalone

Run the MSI installer choosing default values. It should install the server and configure it to run as service.

For locally installed MongoDB (running on same server as cSPS), no further configuration on MongoDB or cSPS is required.

For remote MongoDB servers:

- 1. Add an inbound rule for TCP port 27017 on the local Firewall of the server that runs DB node that allows access from all the cSPS Servers.
- 2. Change MongoDB bind IP address.
- **3.** On the Mongo DB config file (C:\Program Files\MongoDB\Server\4.0\bin\mongod.cfg) do the following:
 - a. Under bindlp add the server local IP

```
net:
    port: 27017
bindIp: 127.0.0.1, <ServerIP>
<ServerIP> replace with the MongoDB server IP
```

- b. Save the file
- 4. Create User/Password for Database Authorization:
 - a. Run CMD.
 - b. Go to C:\Program Files\MongoDB\Server\4.0\bin\.
 - c. Run mongo.
 - d. Enter "use admin".
 - e. Replace **myUserAdmi**n and **abc123** with the user/password that you wish to use):

```
db.createUser(
{
    user: "myUserAdmin",
    pwd: "abc123",
```

```
roles:[{ role: "userAdminAnyDatabase", db: "admin" },
"readWriteAnyDatabase" ]
}
```

5. Remove Users from Database -if you need to delete a user:

```
use admin
db.runCommand( {
dropUser: "myUserAdmin",
writeConcern: { w: "majority", wtimeout: 5000 }
})
```

- 6. Enable database authorization:
 - a. Edit C:\Program Files\MongoDB\Server\4.0\bin\mongod.cfg



Note: The indentation in this file is critical. White spaces before the text must consist of spaces only. Using the Tab key is forbidden.

```
security:
   authorization: "enabled"
```

- b. Save the file
- 7. Configure the cSPS configuration file to the MongoDB address. For example:

<add key="MongoDbConnectionString" value="mongodb:// user:password@<ServerIP>/?connectTimeoutMS=10000" />

The user and password must be replaced with the user/password you defined above for the DB access, <**ServerIP**> the ip address used as the MongoDB bindip.

8. Save the file.

2.8.2 Installing MongoDB Replica Set (High Availability)

For more information on MongoDB replication go to: <u>https://docs.mongodb.com/manual/replication/</u>

Install the odd number of MongoDB instances. It's recommended that from the beginning, all the database members will be defined, although it is possible to start with a standalone SPS server and convert it to HA after the installation

2.8.2.1 Configuring MongoDB

The procedure below describes how to configure the MongoDB in a replica set for HA.

- To set the MongoDB:
- 1. Install MongoDB on cSPS servers (odd number minimum 3) and stop the MongoDB service.
- 2. If one of the servers is running in standalone mode and should be part of the HA, take a backup of the database and stop the MongoDB service.
- **3.** Follow the instructions above for standalone remote server to set the local firewall, and change MongoDB bind IP address.

- 4. Add the SPS server's FQDN to the host file or use the DNS to locate them via FQDN.
- 5. On the MongoDB configuration file, do the following:
- 6. Under Replication add the ReplicaSet name

```
replication:
    replSetName: "rsSps"
```

- 7. Start the MongoDB service on all DB servers.
- 8. If one of the servers is converted to HA and already has data, log in to it. If all servers are new, you can select to which one you wish to log in. It is recommended to select the one that hosts the database and cSPS, and not only the database.
- 9. Run CMD and go to C:\Program Files\MongoDB\Server\4.0\bin directory.
- **10.** Run **mongo.exe** and the MongoDB shell starts.
- **11.** Call to rs.initiate(). It initiates a replica set and will add only the server that runs the command on it.
- 12. Add the other members. It can be done from the Primary MongoDB only!
- 13. Validate that the server is the primary by calling to db.isMaster().
- **14.** To add a member to the replica, call to:

```
rs.add( { host: "<host FQDN>:27017", priority: 0, votes: 0 } )
```

- **15.** Add all the members to the replica set.
- **16.** Ensure that the new members have reached SECONDARY state. To check the state of the replica set members, run rs.status()

```
use rs.reconfig() to update the newly added
member's priority and votes
var cfg = rs.conf() (for 3 nodes you will have to fill-up 0-2)
cfg.members[0].priority = 1
cfg.members[1].priority = 1
cfg.members[2].priority = 1
cfg.members[0].votes = 1
cfg.members[1].votes = 1
cfg.members[2].votes = 1
rs.reconfig(cfg)
```

Priority: Defines a number between 0 and 1000 for primary/secondary; 0 for arbiters. **Default:** 1 for primary/secondary; 0 for arbiters.

A number indicates the relative eligibility of a member to become a primary.

Specify higher values to make a member more eligible to become primary, and lower values to make the member less eligible. A member with a members[n].priority of 0 is ineligible to become primary.

- **17.** Use rs.conf() to display the replica set configuration object.
- 18. Ensure that the replica set has a primary.
- **19.** Use rs.status() to identify the primary in the replica set.
- 20. Create User/Password for Database Authorization.
 - **a.** Open CMD on the first primary DB server (see the command below to know which database is primary)
 - b. Go to C:\Program Files\MongoDB\Server\4.0\bin\.
 - c. Run mongo.
 - d. Enter "use admin".
 - e. Replace "myUserAdmin" and "abc123" with user/password that you wish to use.

```
db.createUser(
{
user: "myUserAdmin",
pwd: "abc123",
roles:[{ role: "userAdminAnyDatabase", db: "admin" },
"readWriteAnyDatabase" ]
}
)
```

f. To remove a user from the database – if you need to delete user:

```
use admin
db.runCommand( {
dropUser: "myUserAdmin",
writeConcern: { w: "majority", wtimeout: 5000 }
} )
```

g. To enable database authorization. **This must be done on all servers**. Edit C:\Program Files\MongoDB\Server\4.0\bin\mongod.cfg.



Note: The indentation in this file is critical. White spaces before the text must consist of spaces only. Using the Tab key is forbidden.

```
security:
   authorization: "enabled"
```

- 21. Save the file.
- **22.** Configure the cSPS configuration file to work with the replica set. You need to do this on all cSPS servers. For example:

```
<add key="MongoDbConnectionString" value="mongodb://
user:password@<MongoDB1 FQDN>,<MongoDB2 FQDN>, <MongoDB3
FQDN>/?replicaSet=rsSps" />
```

- **23.** The user and password must be replaced with the user/password you defined above for the database access.
- 24. <*MongoDB# FQDN>* refers to the FQDN of the database servers. (Remove the "<>" and use DNS or host filse to resolve.)
- **25.** Reset all SPS servers.
- **26.** Here are some useful commands to manage the MongoDB:
 - db.isMaster(): Returns a document that reports the state of the replica set.
 - **db.shutdownServer():** Shuts down the current MongoDB or mongos process cleanly and safely.
 - **db.stats():** Returns a document that reports on the state of the current database.

2.8.2.2 Using TLS for MongoDB sessions

To make the session to the MongoDB encrypted, you need to enable the TLS (SSL). You will need to provide a certificate and private key to every MongoDB to be able to support TLS.

- 1. Edit C:\Program Files\MongoDB\Server\4.0\bin\mongod.cfg.
- 2. Add SSL support in the #interwork interface section under 'bindlp':

```
ssl:
    mode: requireSSL
    PEMKeyFile: C:\Program
Files\MongoDB\Server\4.0\bin\Key.pem
```



Note: The indentation in this file is critical. White spaces before the text must consist of spaces only. Using the Tab key is forbidden.

- **3.** PEMKeyFile is the database side certificate file Include certificate + private key. Save the file.
- 4. Open the services and restart the 'MongoDB Server' service.
- 5. SSL Connection: To the connection string add the following:

....:27017?ssl=true&ssl_ca_certs=key.pem"

- 6. *Key.pem* is the path of the certificate for the database client side. Include certificate and private key. This should be done on the cSPS configuration file.
- 7. Restart the cSPS servers.

2.9 Configure the cSPS Application

The procedure below describes how to configure the cSPS Application. This section describes only the mandatory settings of the global configuration.

Multiple servers share the same configuration, and easily add new servers. Previously (before version 0.3.0.0), all configuration was stored in a local application configuration file.

Currently the local application configuration file is used only for storing the database connection string.

2.9.1 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.

2.9.2 Hierarchical Configuration

The configuration is now organized into four groups:

- System
- SpsAzureApp
- AdminAzureApp
- SipConfig

In each group, there are multiple leaf values. Each value has a unique key. For example:

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

2.9.3 Modifying Configuration

Several REST APIs accessible by Swagger, enable modifying the 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 configuration 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 an API.

Modifying a global value ('*') will modify the global entry AND all server specific entries.

Modifying a server specific value will only modify 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.

2.9.4 Upgrading

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

2.9.5 Access Control

All REST APIs require an authenticated user that belongs to a specific admin group. However, authentication configuration is also stored in 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.

- > To configure the cSPS Application:
- 1. Install Chrome on the SPS before you start working with it.
- 2. Run RDP to the SPS Server, and then open Chrome.
- 3. Open http://localhost:9000/swagger.
- **4.** Open the AppConfig section.
- 5. Open POST /api/config/server/{server}/spsAzureApp
- 6. Click the yellow box on the right, under **Example Value**.

PUT	/api/co	nfig/server/{server}/flat/default/{path}			Set default to a single configuration value
GET	/api/co	nfig/server/{server}/spsAzureApp		Retu	ums all SPS Azure configuration parameters
POST	/api/co	nfig/server/{server}/spsAzureApp			Set all SPS Azure configuration parameters
Param	eters				0
Parame	eter	Value	Description	Parameter Type	Data Type
server	•	(required)	server or '*' for default server	path	string
spsAzu	ыгеАрр	(required) Parameter content type: application/joon		body	<pre>Model Example Value { Tresant": "string", "addsece": "string", "clientDD": "string", "Apprey": "string", " }</pre>
Respo	nse Mes	sages			
204 Try it o	Status Coo	le Reason Response N No Content	lodel		Headers
GET	/api/coi	nfig/server/{server}/adminAzureApp		Return	ns all Admin Azure configuration parameters
POST	/api/cor	nfig/server/{server}/adminAzureApp		s	et all Admin Azure configuration parameters

7. After clicking it, the example values will be copied to the left.

POST /api/config/	server/{server}/spsAzureAp	op			Set all SPS Azure configuration parameters
Parameters					0
Parameter Valu	ie		Description	Parameter Type	Data Type
server)		server or '*' for default server	path	string
spsAzureApp {	'Tenant": "string", 'Audience": "string", 'ClientID": "string", AppKey": "string", 'ADDInstance": "string" ameler content lype: Dication/son	•		body	Model Example Value { Trenant": "string", "Audience": "string", "App(sey": string", "App(sey": string", "AAVInstence": "string")
Response Messag	es				
HTTP Status Code	Reason	Response Model			Headers
204	No Content				
Try it out!					

8. Enter "*" in the server edit box, for performing these settings at the global level.

- **9.** Set the following parameters; assume Tenant name is **cce.aceducation.info**. Change it to your tenant accordingly:
 - Tenant: "cce.aceducation.info"
 - Audience: "https://cce.aceducation.info/SpsOnline"
 - Copy from SPSOnline Expose an API section Application ID URI.
 - ClientID: "7f1c7354-0c07-437d-be55-e2f6908XXXXX" Copy from SPSOnline
 Application ID.
 - AppKey: "mJtbob7R+VL7g7myp07cuzZuyErb9Xw634beoMDXXXXX" Copy from SPSOnline Application saved key.
- Click Try it out! and confirm that the procedure was successful. Open POST /api/config/server/{server}/adminAzureApp



Note: Click on the yellow box on the right, under Example Value.

- **11.** Do the same as in <u>Paragraph 9</u> in Section 2.9.5, using the following parameters:
 - Admin-ClientID: "efa90dbf-36cf-4d49-96c6-3db2df2XXXXX"
 Copy from SPSOnline Admin Application ID.
 - Admin-AppKey: "4zwseWymDclDpyhfGpwWVD7UYrAlhzElhGmR8uDXXXXX" Copy from SPSOnline Application Admin saved key.
 - Admin-ReplyUrl: "http://localhost:9000/swagger/ui/o2c-html" Copy from SPSOnline Application Admin Reply URL.
 - UserAdminsGroupId: "4f6d498d-531c-4d1a-8a72-bc56776XXXXX" Copy from cSPS Azure AD security group.
- **12.** Click **Try it out!** and confirm that the procedure was successful.
- **13.** Reset the cSPS service.

2.9.6 Setting the Local Firewall

Add an inbound rule to allow C:\Program Files\Audiocodes\SpsOnline\SpsOnline.exe to access all ports.

If you are using an external database or using a Replica set, you need to add an inbound rule for TCP Port 27017 on the servers that run database nodes that allow access from the cSPS Server and other database node IPs.

2.9.7 Firewall



Note: Skype for Business Online IP addresses and FQDNs can be found in the <u>Office</u> <u>365 URLs and IP address ranges</u>.

Source IP	Destination IP	Source Port	Destination Port
cSPS	Skype for Business Online	Any	 TCP 443 UDP 3478, 3479, 3480, 3481 Optional: UDP/TCP 50,000-59,999
cSPS	SIP Devices (e.g. SIP IPP, DECT System)	Any	 TCP 5060 (SIP Port used by remote side) UDP – According to Media port range defined on remote devices
SIP Devices (e.g. SIP IPP, DECT System)	cSPS	Any	 TCP 5080 UDP 1025-65535 (this range can be change in the configuration file)

Source IP	Destination IP	Source Port	Destination Port
cSPS	Skype for Business Online	Any	 TCP 443 UDP 3478, 3479, 3480, 3481 Optional: UDP/TCP 50,000-59,999
cSPS	SBC	Any	 TCP 5060 (SIP Port used by SBC) UDP – According to Media port range defined on SBC
SBC	cSPS	Any	 TCP 5080 UDP 1025-65535 (this range can be change in the configuration file)
SIP Devices (e.g. SIP IPP, DECT System)	SBC	Any	 UDP/TCP 5060 (SIP Port used by SBC) UDP – According to Media port range defined on SBC
SBC	SIP Devices (e.g. SIP IPP, DECT System)	Any	 TCP 5060 (SIP Port used by remote side) UDP – According to Media port range defined on remote devices

If the SBC is put between the cSPS and SIP devices:

2.10 Installing Self-Service Web interface

The following describes how to install a self-service Web interface. There are two options for the self-service Web interface:

- SPS Online Self Service Hosted in Azure
- SPS Online Self Service Hosted on the **Cloud SPS server**

The first option **Hosted in Azure** is the recommended option.

2.10.1 General

A cSPS user must activate their account before using it. Activation is performed by running a Web API on the server by the user **while signed in to their Azure account**. This Web API signs in to the user SfB Online account, and stores the user SIP URI in its database.

It also caches the user token and uses it for future logins.

For testing purposes, activation can be run using the Swagger GUI. However, for production this method cannot be used because Swagger is limited for localhost access only, and is insecure, and not user friendly.

This document describes the procedure for setting up a secure, user friendly and remote accessible web site for users self-service.

2.10.2 Requirements

The cSPS server must be accessible for all users on default HTTPS port (443) (port 80 can be used too if needed).

The cSPS server must have a resolvable DNS name for all users required to activate.



Note: The IP address cannot be used. Only a DNS name can be used. The name can be internal for the company.

2.10.3 SPS Online Self Service Hosted in Azure

2.10.3.1 Configuring HTTPS SPS Web API Access

The SPS Web API and Swagger must support HTTPS because the self-service application, which must run over HTTPS, uses SPS Web APIs, and mixed calls from HTTPS to HTTP are not allowed.



Note: HTTPS SPS Web API Access requires SpsOnline Version 0.3.5.0 or higher.

A trusted certificate should be installed and used by the SPS server. For this purpose, a CSR (Certificate Signing Request) should be created for the SPS server and signed a CA (Certificate Authority) that is trusted by the users' browsers.

This certificate cannot be a self-signed certificate (otherwise all users would have to trust it). It is recommended to sign this certificate by the <u>corporate CA</u>.

2.10.3.1.1 Create Corporate Signed Certificate



Note: CSR must include SPS FQDN in SAN (Subject Alternative Name), in addition to the Subject Name. Otherwise, the Chrome browser will reject the certificate.

> To create a Corporate Signed Certificate:

- 1. Navigate to Cmd > MMC > Add snapin > Certificates > Computer Account
- 2. Right-click Certificates > Personal > Certificates.
- 3. Click Request > All tasks > Request new certificate.
- 4. Select Web server 2048 bits.
- 5. Select More information.
- 6. For 'Subject name' select 'common name', enter the server FQDN, and then click Add.
- 7. For 'Alternative name' select 'DNS name', enter the server FQDN, and then click **Add**.
- 8. Click Enroll.
- 9. The certificate should be in the Personal folder. Open it and verify that it's OK.

2.10.3.1.2Configuring SPS to Use Certificates

- > To configure SPS to Use Certificates:
- 1. Open a new certificate and navigate to **Details** > **Thumbprint**. Save the value (without spaces if any).
- 2. Generate a GUID (e.g., from https://www.guidgenerator.com/). Guid should be something like {e9569b7d-4bde-4b8f-b960-8b94a8299552}.
- Open CMD as administrator and run: netsh http add sslcert ipport=0.0.0.9001 certhash=<thumbprint> appid=<guid>
- Verify that swagger is now available via HTTPS using FQDN on port 9001: <u>https://SPS-FQDN:9001/swagger</u>



Note: The default HTTPS port is 9001. It can be changed with the configuration key Data.System.HtppsListenUrl.

2.10.3.2 Azure App Service – Part 1

- To use the Azure App Service Part 1:
- **1.** Log in to the Azure portal.
- 2. Create a new Web APP resource.
- 3. Select an instance name (e.g., spsonlineselfservice).
- 4. Create a new resource group (recommended).
- 5. In the 'Runtime stack' field, select a Node version.
- 6. In the 'Operating system' field, select Windows.
- 7. Create a new service plan.
- 8. In the 'Size' field, select **Free**.
- 9. Create and open a new Web App resource.
- **10.** We'll get back to the App Service later.

2.10.3.3 Azure Application

An Azure Web application must be configured.



Note: This is the third application, in addition to 'SpsOnline' and 'SpsOnlineAdmin' applications.

> To use the Azure Application:

- **1.** Log in to the Azure portal.
- 2. In the Azure Active Directory pane, click App registrations, and then choose New registration.
- 3. In the 'Name' field, enter "SpsOnlineSelfService".
- **4.** Select accounts in this directory only.

- 5. In the 'Redirect URI' field, select **Web**, and then enter the URL of the <u>Azure App Service</u> created above.
- 6. Click Register.
- 7. In the succeeding page, find the *Application ID* value and copy it to the clipboard. You'll need it later.
- 8. Enable the **OAuth 2 implicit grant** for your application by choosing **Manifest** at the top of the application's page.
- 9. Open the inline Manifest editor. Search for the *oauth2AllowImplicitFlow* property. You will find that it is set to "false"; change it to **true** and click on **Save** to save the manifest.
- **10.** Select **Authentication > Implicit Grant > Enable ID tokens > Save** (Verify both ID tokens and access tokens are enabled).
- **11.** Select **API Permissions > Add a permission**.
- 12. Select APIs my organization uses.
- **13.** Select **SpsOnline > user_impersonation > Add**.
- 14. Select Grant Admin Consent.

2.10.3.4 Azure App Service – Part 2

- To use the Azure App Service Part 2
- 1. Return to the App service created above.
- 2. Select Advanced Tools > Go; the Kudu screen appears.
- 3. From the top menu, select **Debug Console** > **CMD**.
- 4. Select site > wwwroot.
- 5. Delete hostingstart.html.
- 6. Copy the SpsOnlineSelfService folder to the Web App by dragging it to wwwroot.
- 7. From the Kudu screen, select **SpsOnlineSelfService** > **assets** > **Edit appConfig.json**.
- 8. Replace the following:
 - a. "spsServer" with "https://<YOUR-SPS-SERVER-FQDN>:9001",



Note: HTTPS and not HTTP. For example: <u>https://il-rona-pc.corp.audiocodes.com:9001</u>

- **b.** "tenant" with "YOUR-TENANT", (example: "audiocode.biz")
- **c.** "clientId" with "YOUR-SpsOnlineSelfService-APPLICATION-ID" (the application ID saved above)
- **d.** "appUrl" with "YOUR-SpsOnline-APPLICATION-URL" (for example: <u>https://audiocode.biz/spsOnline</u>.



Note: This is the App URL of the SPS Azure application. Find it in **Portal Active Directory > App Registrations > SpsOnline > Overview > Application ID URI**.

9. Click Save.

10. On your PC, create a file named web.config with the following content:

- 11. Drag the web.config to the wwwroot/SpsOnlineSelfService folder.
- **12.** Return to **App Service** > **Configuration**.
- **13.** Select Path Mappings.
- 14. Edit '/' path and modify value 'site\wwwroot' with site\wwwroot\SpsOnlineSelfService.
- 15. Click OK.
- 16. Save settings.

At this point, the Azure self-service site should work. For any problems, enable the debug in Chrome browser (F12).

2.10.4 SPS Online Self-Service Hosted on Cloud SPS Server

The following describes SPS online self-service hosted on the Cloud SPS Server.

2.10.4.1 Adding an Azure Application

An Azure Web application must be configured for the self-service.

- To add an Azure application:
- 1. Define the FQDN for the SPS Server, and then add it to the DNS so it will resolvable for all relevant users for example cSPS.<*your Domain*>.
- 2. Login to the Azure portal.
- 3. In the 'Azure Active Directory' pane, click **App registrations**, and then click **New registration**.
- 4. In the 'Name' field, enter **SpsOnlineSelfService**.

Н	Home > Test_Test_Audiocodes(R&D lab) - App registrations > Register an application
F	Register an application
,	Name
Т	'he user-facing display name for this application (this can be changed later).
[SpsOnlineSelfService 🗸
Ş	Supported account types
v	Who can use this application or access this API?
(Accounts in this organizational directory only (Test_Test_Audiocodes(R&D lab) only - Single tenant)
(Accounts in any organizational directory (Any Azure AD directory - Multitenant)
(Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
H	felp me choose
F	Redirect URI (optional)
V c	We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be hanged later, but a value is required for most authentication scenarios.
Г	Web v ea https://mwanp.com/auth

- 5. Click **Create** to create the new application.
- 6. In the succeeding page, find the *Application ID* value and copy it to the clipboard. You'll need it later.

• Vercome to the new and improved App registrations. Cooking to real now it's changed norm App registrations (cegacy).	
Display name : SpsOnlineSelfServiceTest I⊡ Application (client) ID : 42019295-5030-4976-b3d9-b8c19690ef5e Directory (tenant) ID : e2fe003e-5130-4f5b-9050-6f1cb7857891 Object ID : 58ff985e-04a3-44f9-b554-29346ba78cfd	

7. Enable the OAuth 2 implicit grant open the Authentication section for your application and check Access Token and ID Token under implicit grant.

Home > Test_Test_Test_Audiocodes(R&D	lab) - App registrations > SpsOnlineSelfService - Authentication					
SpsOnlineSelfService - Au	uthentication					
	Save 🗶 Discard 🛛 🐐 Try out the new experience 🛛 🖤 Got feedback?					
Sverview	Redirect URIs					
📣 Quickstart	The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating learn more about adding support for web mobile and desiron clients [2]	users. Also referred to as reply URLs.				
Manage						
🚾 Branding	ТҮРЕ	REDIRECT URI				
Authentication	Web	http://spsonline.cloudbond365b.com				
📍 Certificates & secrets	Web V	e.g. https://myapp.com/auth				
 API permissions 						
Expose an API	Suggested Redirect URIs for public clients (mobile, desktop)					
📴 Owners	If you are using the Microsoft Authentication Library (MSAL) or the Active Directory Authentication Library (ADAL) to build app	olications for				
Roles and administrators (Previ	desktop or mobile devices, you may select from the suggested Redirect URIs below or enter a custom redirect URI above. For information, refer to the library documentation.	more				
(I Manifest	msal741bc95d-c368-4890-b58c-7f041a967456://auth (MSAL only)					
Support + Troubleshooting	https://login.microsoftonline.com/common/oauth2/nativeclient lb https://login.live.com/oauth20_desktop.srf (LiveSDK)	https://login.microsoftonline.com/common/aauth2/nativeclient https://login.microsoftonline.com/common/aauth2/nativeclient https://login.live.com/cauth20_detitop.stf (LiveSD)()				
X Troubleshooting						
New support request						
	Advanced settings					
	Looput URL e.a. https://myapp.com/logout					
	Implicit grant					
	Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a	single page				
	architecture (SPA), has no backend components, or invokes a Web API via JavaScript.					
	To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:					
	Access tokens					
	D tokens					

8. Click Save.

9. On the Expose an API screen, click Application ID URI Set.

SpsOnlineSelfServiceTest	- Expose an API			
	Application ID URI 👩 Set			
🐺 Overview				
📣 Quickstart	Scopes defined by this A	API		
Manage	Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.			
🚾 Branding	+ Add a scope			
Authentication	SCOPES	WHO CAN CONSE	NT ADMIN CONSENT DISPLAY NAME	USER CONSENT DISPLAY N
📍 Certificates & secrets				
 API permissions 	No scopes have been defined			
🚱 Expose an API				
Owners	Authorized client applica	ations		
Roles and administrators (Previ	Authorizing a client application in this API.	dicates that this API trusts the application and users s	hould not be asked to consent when t	he client calls
🚥 Manifest	+ Add a client application			
Support + Troubleshooting	CLIENT ID	SCOPES		
X Troubleshooting	No client applications have been	authorized		
New support request				

Set the App ID URI				
Application ID URI https://audiocodesipprnd.onmicrosoft.com/SpsOnlineSelfSen/i <mark>c</mark> e				
Save Discard				
SCOPES	WHO CAN CONSENT	ADMIN CONSENT DISPLAY NAME	USER CONSENT DISPLAY NAME	STATE

- Replace the Application ID URI with the following URI: 'https://<your_tenant_name>/SpsOnlineSelfService ' (replacing <your_tenant_name> with the name of your Azure AD tenant).
- 11. Click Save.
- 12. Click Add a scope and add user name "user_impersonation".
- **13.** Select Admin and users for who can consent. In the 'Admin consent display name' field, enter "Access SpsOnlineAdmin".

- **14.** In the 'Admin consent description' field, enter "Allow the application to access SpsOnlineAdmin on behalf of the signed-in user.".
- 15. In the 'User consent display name' field, enter "Access SpsOnlineAdmin".
- **16.** In the 'User consent description' field, enter "Allow the application to access SpsOnlineAdmin on your behalf".
- 17. Click Add scope.
- 18. On the API permissions screen, select Add a permission.
- 19. Select APIs my organization uses, and then select SpsOnline.

 b) - App registrations > SpsOnlineAdminTe 	st - API permissions				Request API permissions
permissions					Select an API
API permissions Applications are authorized to call APIs w all the permissions the application needs.	hen they are granted	permissions by users/admir	is as part of the consent process. The list of con	figured permissions should include	Microsoft APIs APIs my organization uses My APIs Apps in your directory that expose APIs are shown below
API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIR	ED STATUS	SncOnline
 Microsoft Graph (1) 					SpsOnline Tomer
User.Read	Delegated	Sign in and read user pr	ofile -		SecOnline Admin
These are the permissions that this applic able permissions dynamically through cou	ation requests statica de. See best practice	ally. You may also request us s for requesting permissions	er consent-		SpsOnlineAdmin_Tomer
					SpsOnlineAdminErez
Grant concent					SpsOnlineErez
	a an inclusif of all	en in this dimeters. Granting	adation and the all states and the and		SpsOnlineOld
As an administrator, you can grant consent on behalf of all users in this directory. Granting administorator all users means that end users will not be shown a consent screen when using the application.					SpsOnlineSelfService
Grant admin consent for Test_Test_Test_	Audiocodes(R&D lab)				SpsTokenCache

20. Click **Select Delegated Permissions**, and then select **user_impersonation**.

Request API permissions	
All APIs	
SpsOnline	
⁵² https://cce.aceducation.info/SpsOnline	
Vhat type of permissions does your application require?	
Delegated permissions	Application permissions
Your application needs to access the API as the signed-in user.	Your application runs as a background service or daemon without a signed-in user.
elect permissions	expa
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
user_impersonation Access SpsOnline 0	
vser_impersonation Access SpsOnline	-
Access SpsOnline	
Access SpsOnline	
Access SpsOnline (
Access SpsOnline (
Access SpeOnline	

22. Select Grant admin consent, and then click Yes to confirm it.

 SnsOnlineAdminTest - API nermissions 	Home > Test_Test_Audiocodes(R&D lab) - App registrations > SpsOnlineAdminTest - API permissions							
ے۔ SpsOnlineAdminTest - API permissions								
C Search (Ctr(+/) C Search (Ct	cisting							
Overview Quickstart No								
Manage + Add a permission								
E Branding API / PERMISSIONS NAME TYPE DESCRIPTION ADMIN CONSENT REQUIRED STATUS	.s							
Authentication ▼ Microsoft Graph (1)								
Y Certificates & secrets User.Read Delegated Sign in and read user profile								
Sexpose an API user_impersonation Delegated Access SpsOnlineTest								
Owners These are the permissions that this application requests statically. You may also request user consent-								
able permissions dynamically through code. See best practices for requesting permissions								
Manifest								
Support + Troubleshooting Grant consent								
As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end Troubleshooting								
Image: Series with not be shown a consent for Test, Test, Audiocodes(R&D lab) Image: Series with not be shown a consent for Test, Test, Audiocodes(R&D lab)	users will not be shown a consent screen when using the application. Grant admin consent for Test_Test_Test_Audiocodes(R&D lab)							

2.10.4.2 Installing NGINX Web Server

The SPS self-service site is an Angular application. Since it is a set of static Web pages, any static Web server can be used. We'll use **NGINX**.

- > To install the NGINX Web server:
- 1. Download the NGINX Web server from https://nginx.org/en/download.html.
- 2. Extract the zip file to anywhere on the SPS server.
- **3.** Open a CMD prompt in the NGINX directory and run "**start nginx**"; verify that two NGINX processes are running in the Task Viewer.
- 4. Open a Web browser in <u>http://localhost/</u> and verify that the NGINX Welcome page is displayed.
- 5. Open a Web browser from <u>an external server</u> to <u>http://YOUR-SPS-FQDN/</u> and verify that the NGINX Welcome page is displayed.
- 6. Validate that the firewall is open for Port 80,443 on the SPS server.

2.10.4.3 NGINX Configuration

You now need to configure NGINX to run self-service Web site.

- To configure NGINX to run self-service Web site
- 1. Copy the SpsOnlineSelfService directory to the NGINX folder.
- 2. Edit the 'SpsOnlineSelfService\assets\appConfig.json' file:
 - **a.** In the 'spsServer' field, enter "http://YOUR-SPS-SERVER-FQDN", (for example: "spsServer": "http://il-rona-pc.corp.audiocodes.com",).
 - **b.** In the 'tenant' field, enter "YOUR-TENANT", (for example: "tenant": "audiocode.biz",).
 - c. In the 'clientId' field, enter "YOUR-SpsOnlineSelfService-APPLICATION-ID", (for example: "clientId": "c04bfa22-c2a8-43f2-974c-813c31d8e6ff",).
 - **d.** In the 'appUrl' field, enter "YOUR-SpsOnlineSelfService-APPLICATION-URL" (for example: "appUrl": "https://audiocode.biz/SpsOnline".



Note: The value is the app ID Url of the SpsOnline application, not this application.

3. Edit the **conf\nginx.conf** file. Comment out all server {} sections (should be only one) and add the following:

```
proxy connect timeout
                             5;
proxy send timeout
                             5;
proxy read timeout
                             5:
server {
      listen
                   80;
      server name
                           YOUR-SPS-FQDN;
      location / {
            root /YOUR/PATH/SpsOnlineSelfService;
            try files $uri $uri/ /index.html;
      }
      # proxy /api/userSelfService/ web API requests to SPS
server
      location /api/userSelfService/ {
            # Proxy only to 127.0.0.1, otherwise it will also
try IPv6 and error time will be doubled
            proxy_pass
http://127.0.0.1:9000/api/userSelfService/;
            proxy set header Host localhost;
      }
    }
```

- 4. Run 'nginx -s reload'.
- 5. Verify that the **SpsOnline** service is running.
- 6. Open a Web browser to <u>http://YOUR-SPS-FQDN/</u> (Not localhost). If all is running correctly, the self-service application should open and you should be able to log in, activate and enable/disable a user.
- 7. Verify that <u>http://YOUR-SPS-FQDN/</u> also works from a remote browser.

2.10.4.4 Configuring HTTPS

The self-service Web site should run over secure HTTPS because users log in and pass their token to the self-service site.

A trusted certificate should be installed and used by the NGINX Web server. For this purpose, a Certificate Signing Request (CSR) should be created for the SPS server and signed a Certificate Authority (CA) that is trusted by the users' browsers.

This certificate cannot be a self-signed certificate (otherwise all users would have to trust it). It is recommended to sign this certificate by the <u>corporate CA</u>.

2.10.4.4.1 Creating CSR and Private Key

The procedure below describes how to create CSR and Private keys.



Note: The CSR must have SPS FQDN in the Subject Alternative Name (SAN), in addition to the Subject Name. Otherwise the Chrome browser rejects the certificate!

You can use any method you want to create CSR and private keys. For example, you can use an online service such as <u>https://certificatetools.com/</u>.

- To create CSR and Private keys:
- 1. Set SPS FQDN in common name (subject).
- 2. Set SPS FQDN in SAN (Subject Alternative Name) as DNS entry.
- 3. Set organization and other attributes.
- 4. Set key size to 2048 bits.
- 5. Generate CSR and private key.
- 6. Save private key, including -----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY----- parts to **spsOnlineSelfService.key** in Nginx/conf directory.

2.10.4.4.2Sign CSR

The CSR must be signed by a CA that is trusted by the users' browsers. It is recommended to sign this certificate by the **<u>corporate CA</u>**.

- To sign the CSR:
- 1. Find the corporate CA by running 'certutil' in cmd taking the 'server' line output.
- 2. Open a browser to http://YOUR-CA/certsrv.
- 3. Select Request a certificate.
- 4. Select Advanced certificate request.
- 5. Select the Web server 2048 bit template.
- 6. Paste the CSR.
- 7. Submit the CSR.
- 8. Select 'Base 64 encoded'.
- 9. Download the certificate.
- **10.** Copy the certificate to **spsOnlineSelfService.cert** in the NGINX/conf directory.

2.10.4.4.3 Modifying NGINX

1. Modify nginx.conf:

```
server {
    listen 443 ssl;
    server_name YOUR-SPS-FQDN;
    ssl_certificate spsOnlineSelfService.cert;
    ssl_certificate_key spsOnlineSelfService.key;
    location / {
        root /YOUR/PATH/SpsOnlineSelfService;
        try_files $uri $uri/ /index.html;
    }
}
```

- 2. Edit the SpsOnlineSelfService\assets\appConfig.json file and change "spsServer" to https:
 - "spsServer": "https://YOUR-SPS-SERVER-FQDN", (For example: "spsServer": "https://il-rona-pc.corp.audiocodes.com",)
- 3. Run nginx -s reload.
- 4. Verify that the SpsOnline server is running.
- Open a Web browser to <u>https://YOUR-SPS-FQDN/</u> (Not localhost). If all is running correctly, the self-service application should open and you should be able to log in, activate and enable/disable a user.
- 6. Verify that <u>https://YOUR-SPS-FQDN/</u> also works from a remote browser.

2.10.4.5 Configuring NGINX to run as Windows Service

You need to configure NGINX to run as a Windows service. An external application is needed to run it as a service.

- > To configure NGINX to run as a Windows service:
- 1. Stop NGINX by running "**nginx -s stop**" in the NGINX directory. Verify that no NGINX task is running.
- 2. Download NSSM from http://nssm.cc/.
- 3. Extract anywhere and open a cmd as administrator in Win64 directory.
- 4. In the cmd, run nssm install nginx.
- 5. Enter the information according to the path used to copy the NGINX files, and then click **Install service**.

N NSSM service installer	x
Application Details Log on Dependencies Process Shutdown Ex	•••
_ Application	
Path: C:\Users\Administrator\Downloads\SPSOnline\ngir	
Startup directory: C:\Users\Administrator\Downloads\SPSOnline\ngir	
Arguments:	
Service name: nginx Install service (Cancel

6. Open the services and start the NGINX service.

2.10.5 Using the Self-Service

The end user will have activated their account before they can use the cSPS.



Note: You first need to add the users to the cSPS. The cSPS does not save the password. Only a token is used to authenticate for log in to Skype Online.

To use the self-service:

1. Open a Web browser to the URL you defined before; the following page is displayed.

🚾 SpsOnlineSelfService × +		
← → C ③ Not secure spsonline.doudbond365b.com	☆	Incognito 🗂 🗄
SPS Online Self Service		Login

2. Click Login to sign in to Microsoft online.

Sign in to your account × +		_ D X
← → C ≜ https://login.microsoftonline.com/cce.aceducation.int	fo/oauth2/authorize?response_type=id_token&client_id=741bc95d-c368-4890-b58c-7f0 😽	Incognito ⊜ :
Section and the section of the secti		
	Microsoft	
Sig	n in	
Emai	I, phone, or Skype	
Cant	access your account?	
Sign-	in options	
	Back	
	THE REPORT OF A DECEMPTION OF A	
Telle Little Antherite	行为这些方法的。 第二章 11章 14章 14章 14章 14章 14章 14章 14章 14章 14	CAR Stall
CALLER AND DO		
	©2019 Microsoft Terms of use	Privacy & cookies

3. Validate that **Enabled** is set, and then click **Activate**.



SPS Online Self Service ron@cce.aceducation.info Logout	← → C ③ Not secure spsonline.doudbond365b.com		☆ 0	:	
ron@cce.aceducation.info Activation Activ	SPS Online Self Service		ron@cce.aceducation.info	Logout	Î
getUserSelfService success		ron@cce.aceducation.info Activation \checkmark Enabled \checkmark	Activate		
	getUserSelfService success			×	

3 Managing Users

For now the cSPS has a simple GUI (Swagger) that works only locally on the server. A version with a full Web GUI will be added in the future. The Swagger GUI works best with Chrome.

- > To manage users:
- 1. Install Chrome on the SPS before you start working with it.
- 2. Run RDP to the SPS Server, and then open Chrome.
- 3. Open http://localhost:9000/swagger.

\varTheta swagger	http://iocalhost:9000/swagger/docs/v1	api_key	Explore
SpsOnline.Web	Server		
AdminConsent		Show/Hide List Operations	Expand Operations
CallCounters		Show/Hide List Operations	Expand Operations
OnlineCalls		Show/Hide List Operations	Expand Operations
OnlineUsers		Show/Hide List Operations	Expand Operations
SipRegistration		Show/Hide List Operations	Expand Operations
Test		Show/Hide List Operations	Expand Operations
UserAdmin		Show/Hide List Operations	Expand Operations
UserSelfService		Show/Hide List Operations	Expand Operations

[BASE URL: , API VERSION: V1]

3.1 Logging in with Swagger

The procedure below describes how to log in using Swagger.

- To log in using Swagger:
- 1. To perform operations using the Swagger, first log in with the user that belongs to the security group that you defined earlier on Azure AD.
- 2. Open one of the operations in the Swagger for example, */api/user/Admin/sps/users*, and then press the red icon 9.

Jser/	Admin	Show/Hide List Operations Expand Operations
GET	/api/userAdmin/azure/users	Get all Azure users with the specified UPN (UserPrincipalName) prefix
GET	/api/userAdmin/azure/users/{id}	Get Azure user by ID, either GUID or UPN
GET	/api/userAdmin/sps/users	Get all SPS users. Note - TokenCache not returned even if exists
Respo OK	onse Class (Status 200)	0
Model	Example Value	
C (Respo	<pre>'UserPrincipalHame': "string", 'UserPrincipalHame': "string", 'DisplayHame': "string", 'Sighui': "string", 'LocalSippessword': "string", 'LocalSippessword': "string" 'Tobfaaled': true, 'Tobfaaled': "string" nse Content Type [application/son * out]</pre>	
POST	/api/userAdmin/sps/users	Add a new SPS user
DELETE	/api/userAdmin/sps/users/{upn}	Delete SPS user
GET	/api/userAdmin/sps/users/{upn}	Get SPS user by UPN. Note - TokenCache not returned even if exists
PUT	/api/userAdmin/sps/users/{upn}/disable	Enable/Disable a user
POST	/api/userAdmin/sps/users/multi	Add multiple SPS users

3. Click Authorize; a new tab opens to log in.

Available authorizations

OAuth2.0

OAuth2 Implicit Grant

Authorization URL: https://login.microsoftonline.com/cce.aceducation.info/oauth2/authorize flow: implicit

API requires the following scopes. Select which ones you want to grant to Swagger UI.

Scopes are used to grant an application different levels of access to data on behalf of the end user. Each API may declare one or more scopes. <u>Learn how to use</u>

J		
Microsoft		
Sign in		
Email, phone, or Sky	/pe	
Can't access your acco	ount?	

	Microsoft	
	← ron@cce.aceducation.info	
	Enter password	
	Password	
	Forgot my password	
	Sign in	
4.	If the login is successful, you will see a blue i	no T Eskano okoiano
nin	Show/Hide List Operatio	ns Expand Operatio

UserAdmin	Show/Hide List Operations Expand Operations
GET /api/userAdmin/azure/users	Get all Azure users with the specified UPN (UserPrincipalName) prefix
оет /api/userAdmin/azure/users/{id}	Get Azure user by ID, either GUID or UPN
оет /api/userAdmin/sps/users	Get all SPS users. Note - TokenCache not returned even if exists
Response Class (Status 200) OK Model Example Value	— 0
t .	A



Note: If you perform an action and get an error similar to *"Authorization has been denied for this request"*, you will need to log out and re-log in. To log out, click the blue icon and select **Logout**.

3.2 Managing Users Operations

Under the **UserAdmin** section, you have the operations to manage the users. For every operation, you need to fill the mandatory data and click **Try it out!**.

UserA	dmin	Show/Hide List Operations Expand Operations
GET	/api/userAdmin/azure/users	Get all Azure users with the specified UPN (UserPrincipalName) prefix
GET	/api/userAdmin/azure/users/{id}	Get Azure user by ID, either GUID or UPN
GET	/api/userAdmin/sps/users	Get all SPS users. Note - TokenCache not returned even if exists
POST	/api/userAdmin/sps/users	Add a new SPS user
DELETE	/api/userAdmin/sps/users/{upn}	Delete SPS user
GET	/api/userAdmin/sps/users/{upn}	Get SPS user by UPN. Note - TokenCache not returned even if exists
PUT	/api/userAdmin/sps/users/{upn}/disable	Enable/Disable a user
POST	/api/userAdmin/sps/users/multi	Add multiple SPS users

- /api/userAdmin/azure/users: Get all Azure users with a specific UPN prefix you can use it to get the full UPN for a user to be used when adding the user to SPS.
- /api/userAdmin/azure/users/{id}: Get azure user by ID (GUID or UPN)
- GET /api/userAdmin/sps/users: Get all the users that were added to the SPS: For every user you will get the following data:
 - "Id": "5c07559b383d6311f82ac018",
 - "UserPrincipalName": "Erez@cce.aceducation.info",
 - "Schemald": 2,
 - "DisplayName": "Erez",
 - "SipUri": "Erez@audiocodesipprnd.onmicrosoft.com",
 - "LocalSipPassword": "123456",
 - "IsDisabled": false,
 - "TokenCache": null

The SIP password is the password that need to use on the SIP phone to register to the SPS.

- POST /api/userAdmin/sps/users: Adds a user. When performing this operation, you need to enter the user UPN and the SIP password that is used on the SIP phone.
- DELETE /api/userAdmin/sps/users{UPN}: Deletes a user.
- GET /api/userAdmin/sps/users{UPN}: Gets one SPS user according to UPN. Only users that were added to the SPS will be returned.
- PUT /api/userAdmin/sps/users{UPN}/disable: Enables/Disables users in the SPS. Can also be used instead of deleting users.
- **POST /api/userAdmin/sps/users/multi:** Adds multiple users in JSON format.



Note: After adding a user and after a user changes the AD password, they must log in to self-service Web that runs on the SPS server and activates the user. (It provides privileges to the SPS to log in to the cSPS as the user). The login is with the AD user/password.

SPS Online Self Service

Login

4 Monitoring SPS using Swagger

The procedure below describes how to monitor SPS using Swagger.

4.1 SipRegistration

Using the SipRegistration section, you can see which phones are registered on the SIP side. You can delete the registration for specific user or for all.

SpsOnline.WebServer

dminConsent Show/Hide List Operations Expand Operation		
CallCounters	Show/Hide List Operations Expand Operations	
OnlineCalls	Show/Hide List Operations Expand Operations	
OnlineUsers Show/Hide List Operations Expand Op		
SipRegistration	Show/Hide List Operations Expand Operations	
DELETE /api/sipRegistration	Warning!! Delete SIP registrations of all users	
GET /api/sipRegistration	Get SIP registrations of all users sorted by user	
DELETE /api/sipRegistration/{sipUri}	Delete all user binding of user SIP URI	
cer /api/sipRegistration/{sipUri}	Get SIP registrations of user SIP URI	
est Show/Hide List Operations Expand Operation		
JserAdmin Show/Hide List Operations Expand Opera		
UserSelfService Show/Hide List Operations Expand		

[BASE URL: , API VERSION: V1]

For every user that is registered, the following data is displayed :

```
"Owner": "sip:julia@cce.aceducation.info",
"ContactAddress": "sip:Julia@10.21.2.25:5050;transport=tcp",
"CallId": "801a803f-f4c0280f9c84c43e9087080023f0b97f@10.21.2.25",
"CSeq": 1198,
"UserAgent": "Panasonic_KX-TGP500B01/22.90 (080023f0b97f)",
"ExpireUtc": "2019-03-25T17:34:45.019Z"
```

4.2 OnlineUsers

Using the OnlineUsers section, you can see the status of the Skype online side, which users are registered.

SpsOnline.WebServer

Admir	nConsent	Show/Hide List Operations Expand Operations
CallCounters Show/Hide List Operations Expand Op		Show/Hide List Operations Expand Operations
Onlin	eCalls	Show/Hide List Operations Expand Operations
OnlineUsers Show/Hide List Operations Expand		Show/Hide List Operations Expand Operations
DELETE	/api/onlineUsers	WARNING II Terminate all users. Note - users will automatically restart on next SIP register
GET	/api/onlineUsers	Get list of basic users info currently logged in
DELETE	/api/onlineUsers/{upn}	Terminate specified user. Note - user will automatically restart on next SIP register
GET	/api/onlineUsers/{upn}	Get basic user info of specified logged in user
POST	/api/onlineUsers/{upn}	Initialize a user. Note - User will be automatically deleted in a short time without a SIP register
SipRe	gistration	Show/Hide List Operations Expand Operations
Test	Fest Show/Hide List Operations Expand Operations	
UserAdmin Show/Hide List Operations Expand Oper		Show/Hide List Operations Expand Operations
UserSelfService Show/Hide List Operations Expand Operations		Show/Hide List Operations Expand Operations

[BASE URL: , API VERSION: V1]

The following data is applicable to all users:

```
"Upn": "sps2103@cce.aceducation.info",
"UserSipUri": "sip:sps2103@cce.aceducation.info",
"StartTime": "2019-03-24T15:17:18.6760994+02:00",
"StartDuration": "1.03:55:45.9296983"
```

4.3 Call Status

By using the callsCount and onlineCalls sections, you can get counters and information regarding calls. The information is for current calls and total counters from the start of the SPS application.

5 cSPS Debugging Tools

The SPS provides the following debugging tools:

- cSPS Logs
- SPS Swagger web interface
- MongoDB console and GUI Application
- WireShark

This page is intentionally left blank.

Α

Appendix – Collecting Azure Information

This information helps you setup the cSPS, keeps the Azure data and configures the cSPS.

<u>cSPS Azure AD security group:</u> ID:

<u>cSPS Application</u> ID: Key Value:

<u>cSPS Admin Application</u> ID: Key Value:

SpsOnlineSelfService



This page is intentionally left blank.

B

Appendix – SIP TLS and SRTP Support

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



Note: The S4B leg always uses HTTPS and SRTP.

B.1 Enabling TLS Support

To enable TLS Support:

- 1. Add a server certificate to the *Local Computer/Personal/Certificate* store issued to the SPS server FQDN. The certificate must be trusted.
- Configure SPS to use this certificate by setting the Data.SipConfig.CertificateThumbPrint value to the certificate thumbprint.
- 3. Restart the server.
- **4.** Now you should also configure phones to use TLS. This requires installing a certificate for the phones.
- 5. Note that all certificates, in SPS and phones, must all be trusted.

B.2 Disabling TLS

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

B.3 SRTP Support

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

- **Disabled:** Default value SPS does not use SRTP.
- Supported: SPS offers and accepts SRTP but does not require other side to use SRTP.
- **Required:** SPS offers and requires SRTP to/from other side.

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: <u>https://www.audiocodes.com/corporate/offices-worldwide</u> Website: <u>https://www.audiocodes.com/</u>

©2020 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, AudioCodes Room Experience and CloudBond 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-00843

