Installation Guide

AudioCodes One Voice for Microsoft® Skype for Business

Cloud SIP Phone Support (cSPS)

Version 0.3

Skype for Business

Microsoft Partner
Gold Communications

audiocodes

Table of Contents

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

cSPS: https://downloads-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.

https://downloads-audiocodes.s3.amazonaws.com/Download/AC_cSPS_Install.html

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.

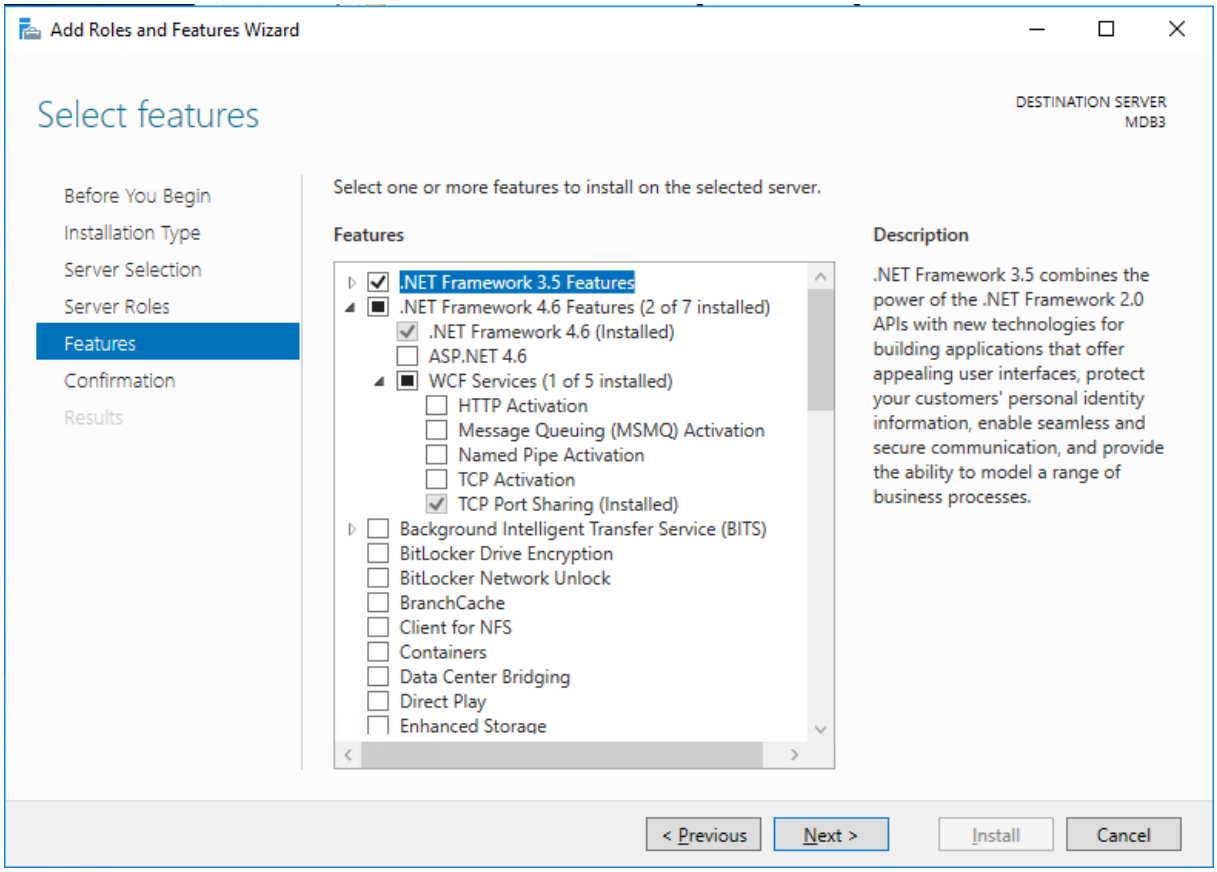
Note: cSPS Server can be a member of a workgroup instead of a domain.

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:



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 https://portal.azure.com

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:**

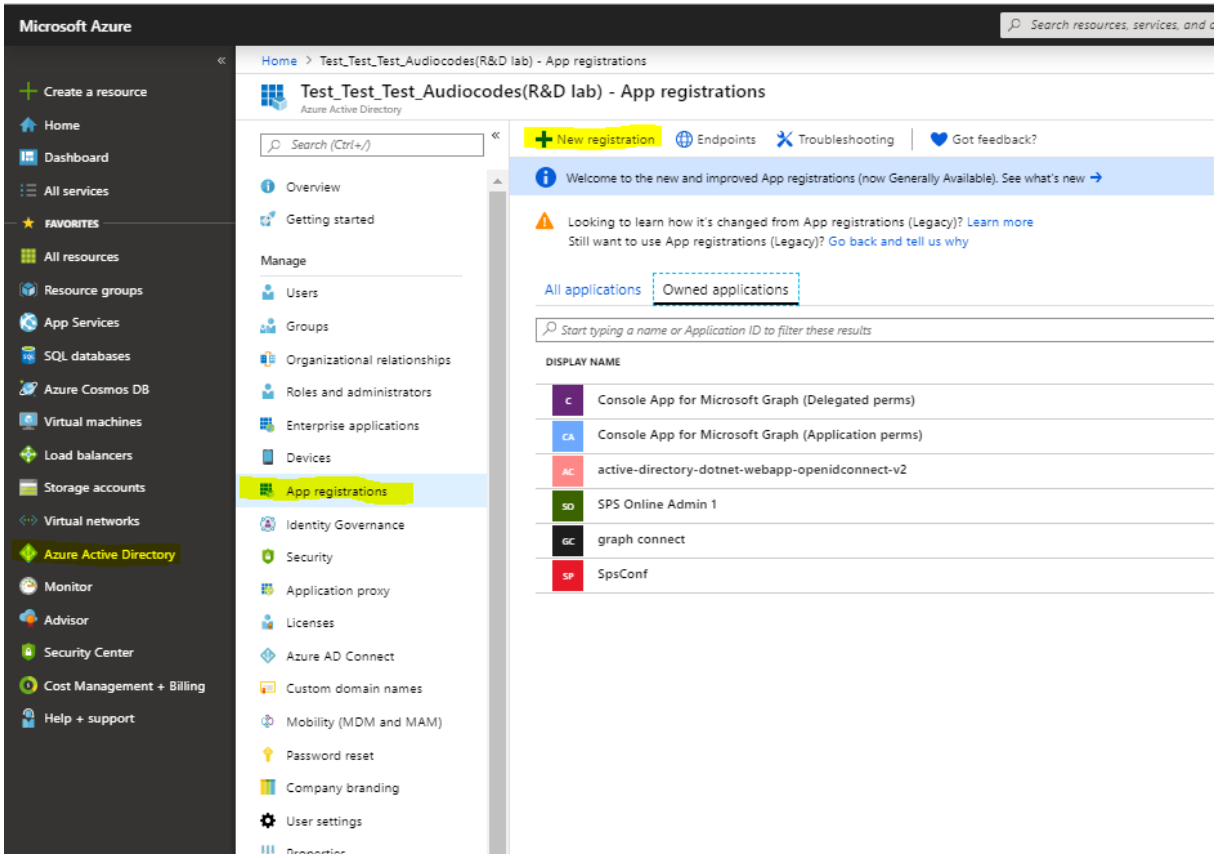
1. On Azure AD, create a new security group. Only users that belong to this group will be able to manage the cSPS and perform administrator operations on it.
2. Save the Group ID. We will need it for the cSPS configuration.
3. Add this group to the users which will be the administrator of the cSPS.

2.4.2 Adding cSPS Application

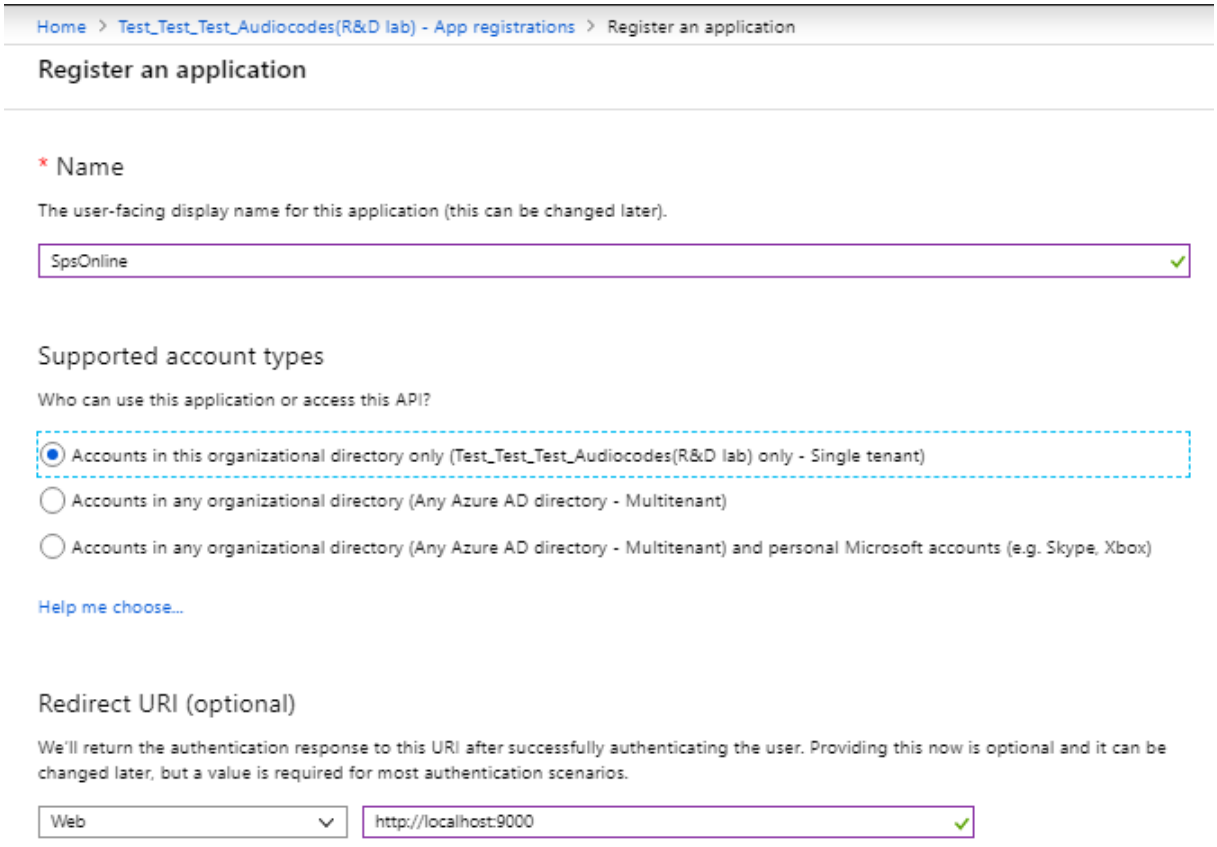
The procedure below describes how to add a cSPS application.

➢ **To add a cSPS application:**

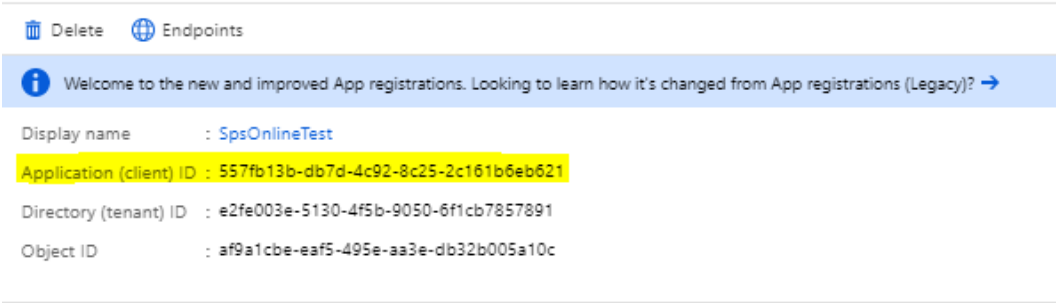
1. In the Azure Active Directory pane, click the **App registrations** menu option, and then select **New registration**.



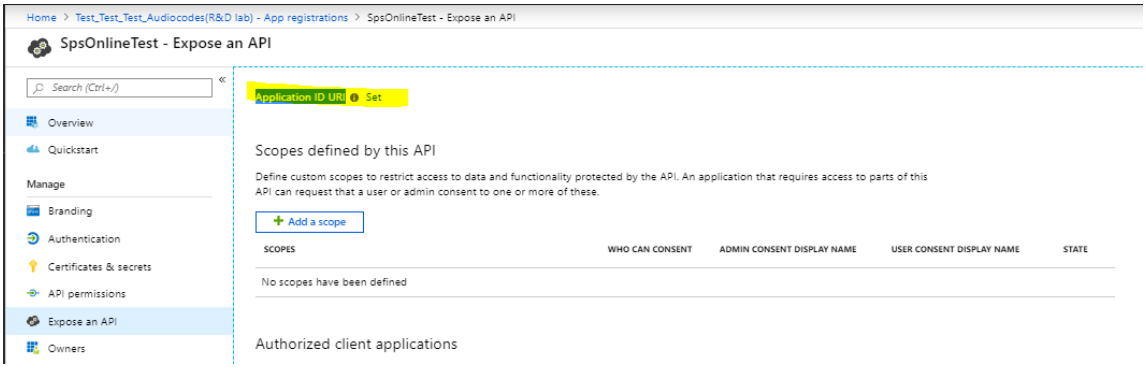
2. In the 'Name' field, enter **SpsOnline**.
3. From the 'Redirect URI' drop-down list, select **Web**; enter the Redirect URL "http://localhost:9000".

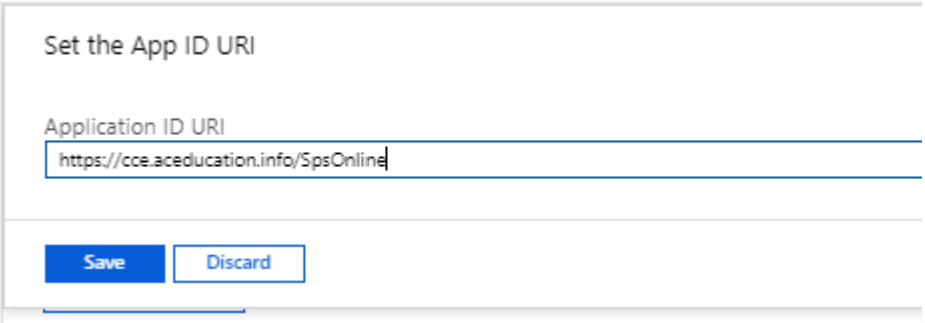


4. Click **Register** to create the new application.
5. In the succeeding page, find the **Application ID** value and copy it, as it will be needed later.

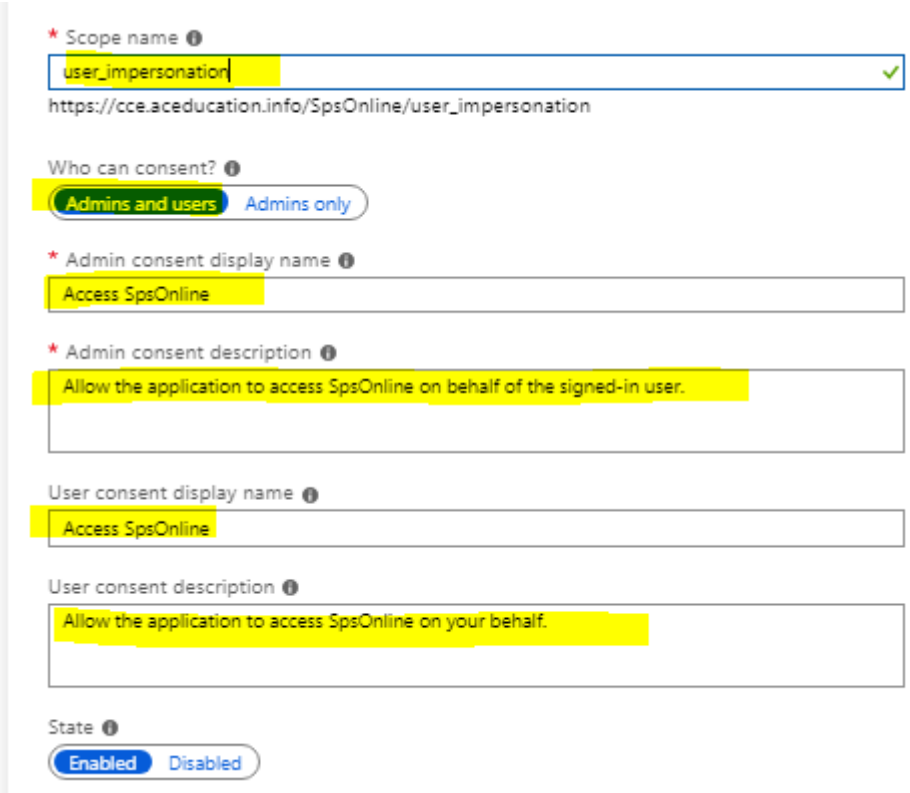


6. Under the 'Manage' side menu, select **Expose an API.**
7. Select **Application ID URI Set**.





8. 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”.

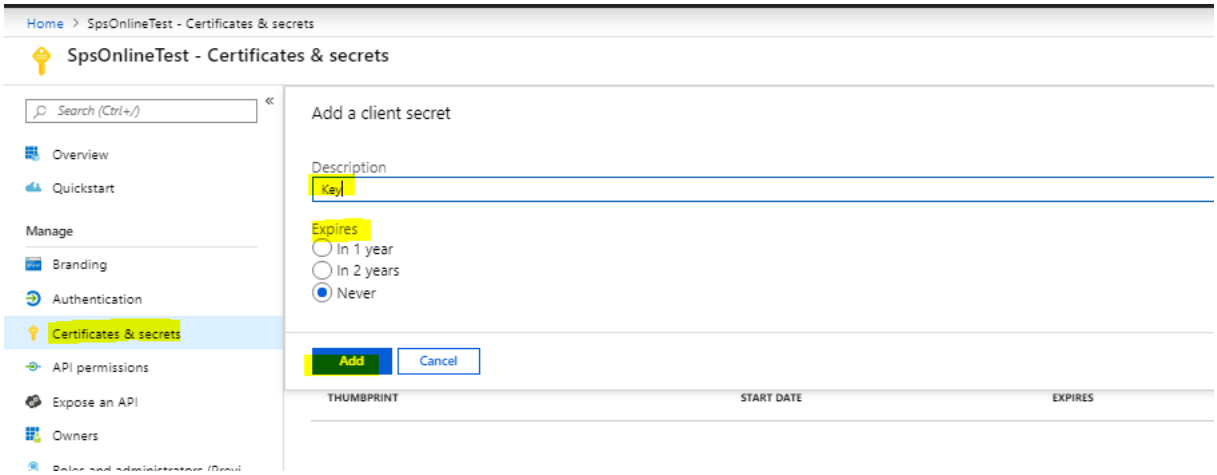


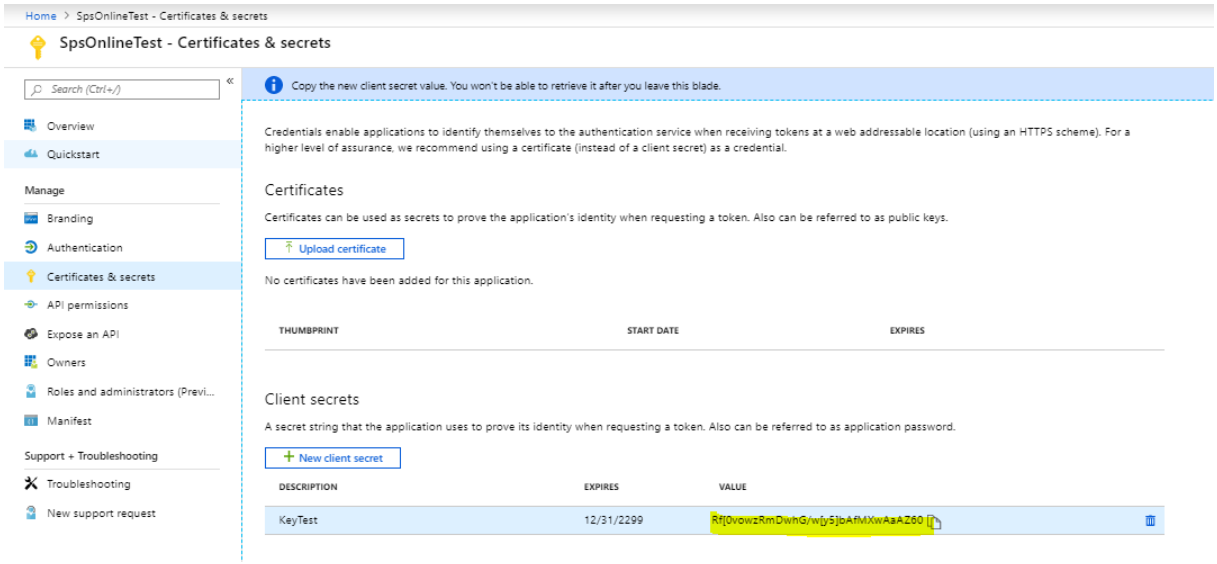
17. Click **Add scope**.
18. Open **Certificates & secrets,** and then select **New client secrets**.
    a. In the 'Description' field, enter a key description of the instance app secret.

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.

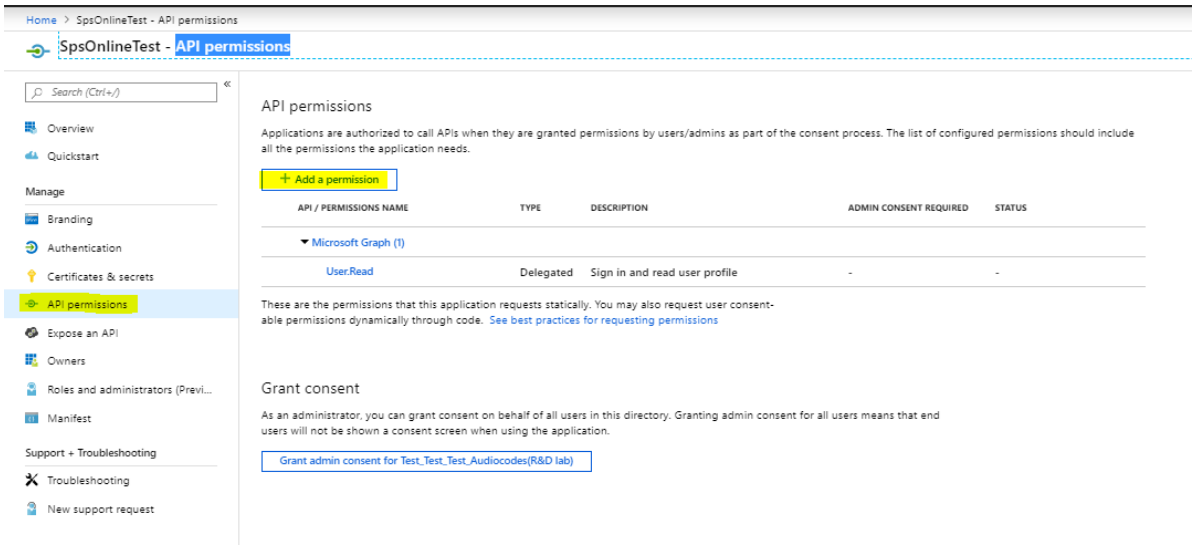
c. Copy and save the value in a safe location.

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.

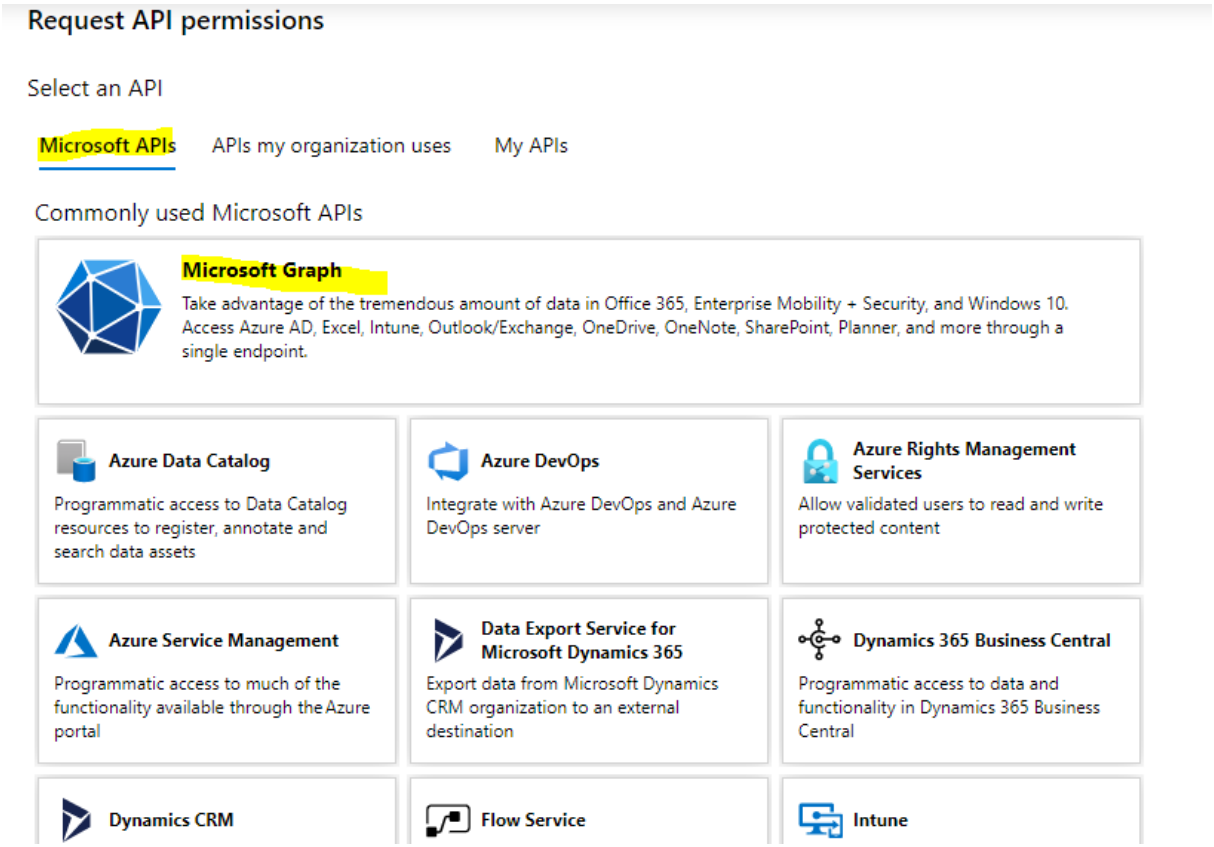




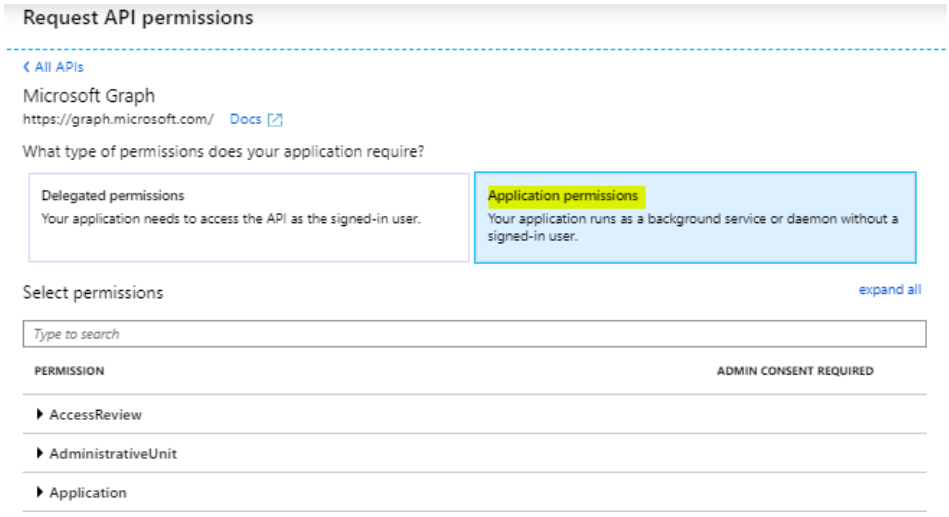
19. Under **API permissions**, select **Add a permission**.



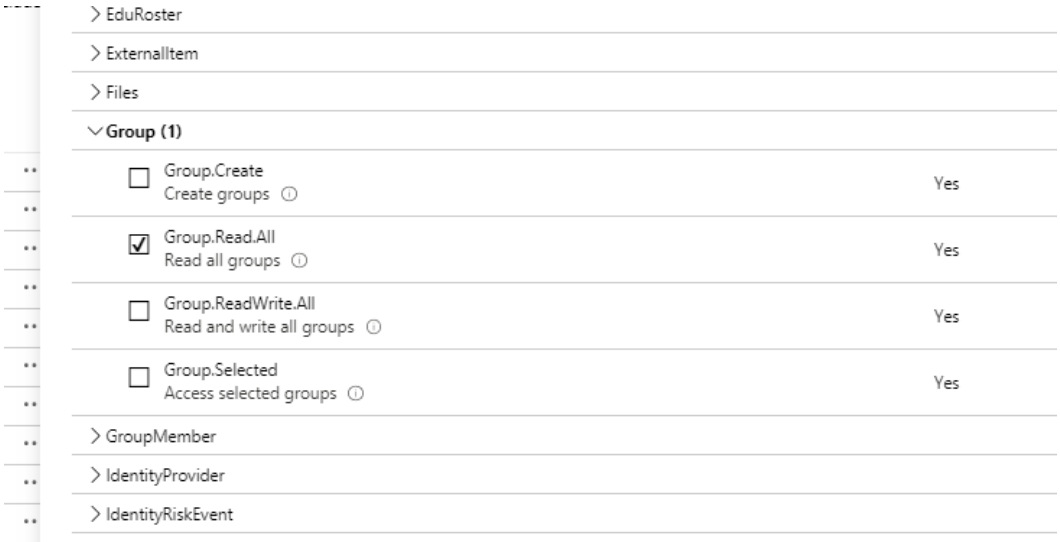
20. Select **Microsoft APIs**, and then select **Microsoft Graph**.



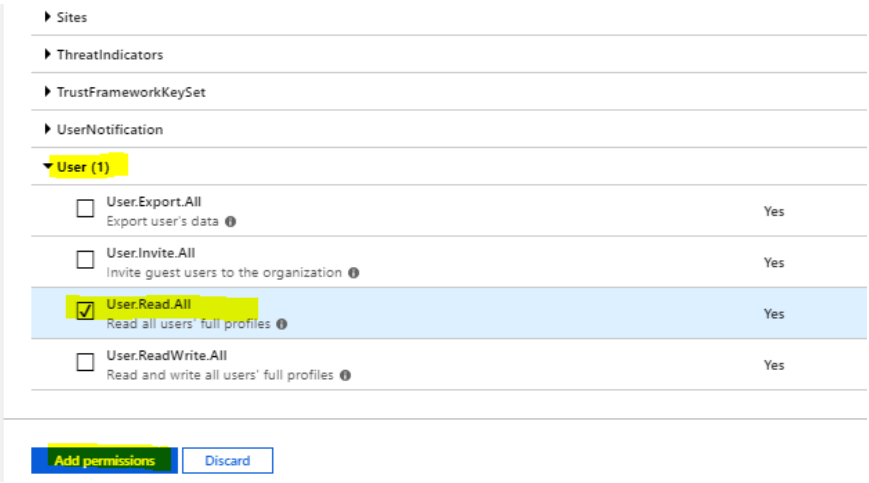
21. On the **Request API permissions** screen, select **Application Permissions.**



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

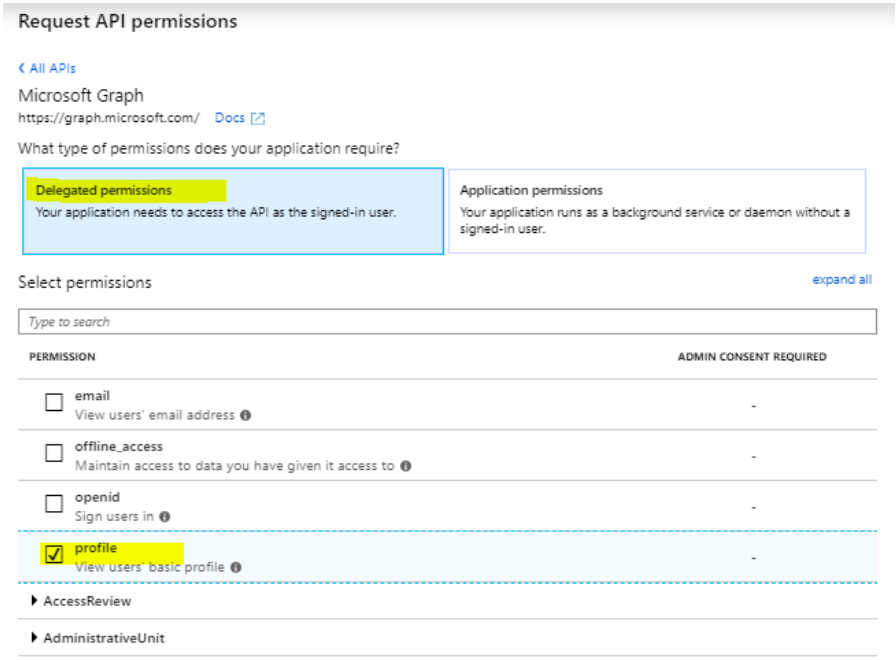


23. Under the **User (1)** group, select **Users.Read.All**.



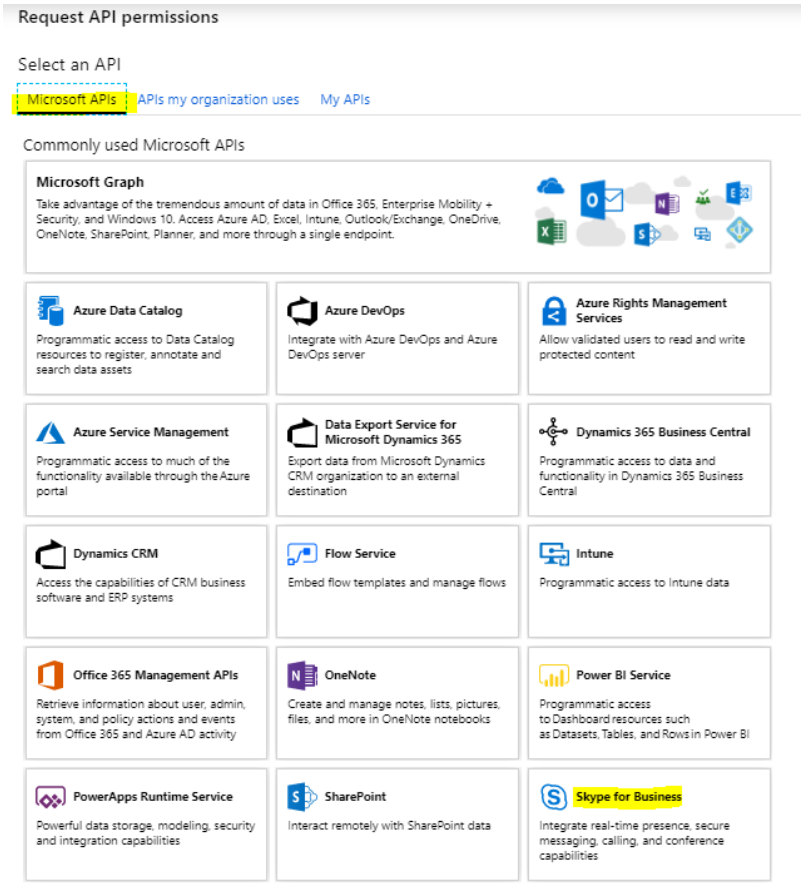
24. Click **Add permissions**.
25. Select **Add new permissions**.

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

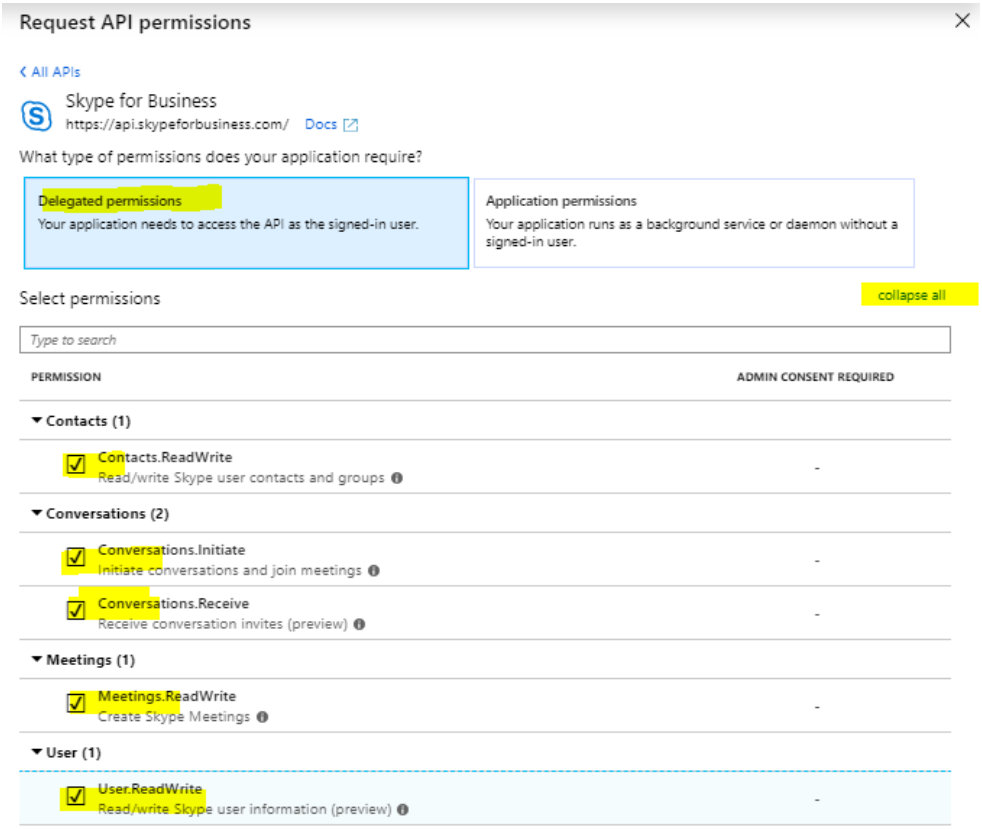


28. Click **Add permissions**.

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

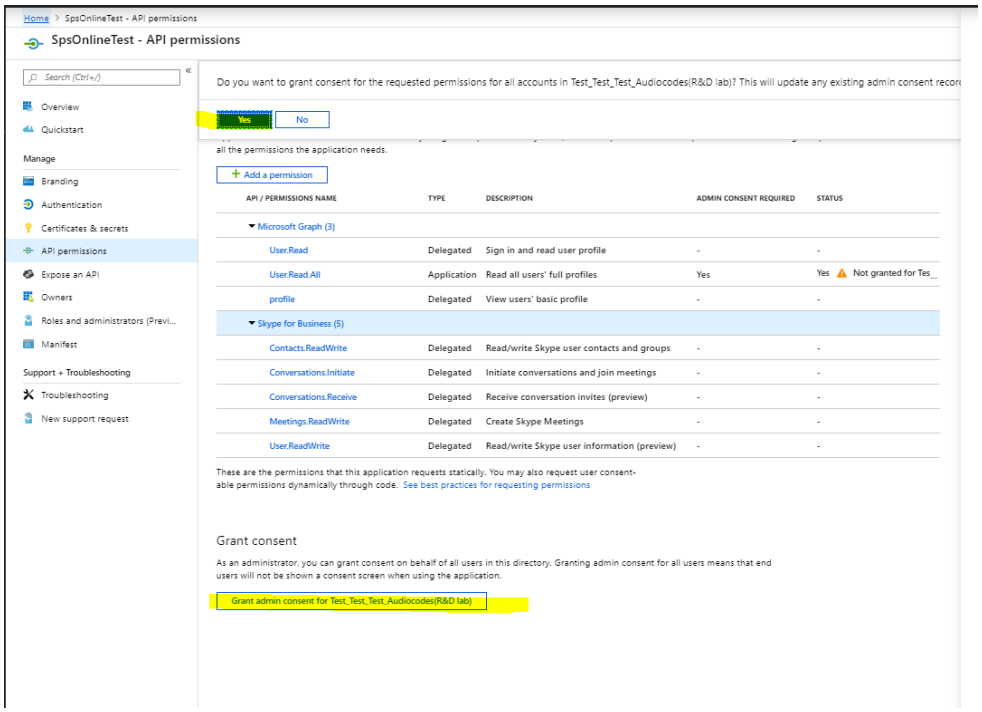


30. Under **Delegated permissions**, select all permissions.



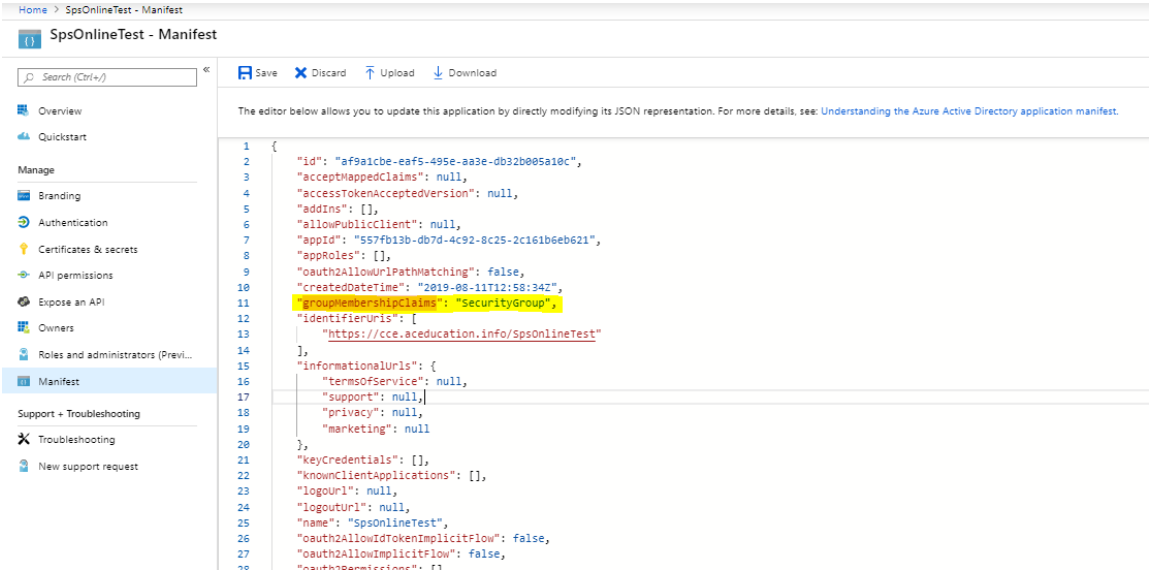
31. Select **Add permissions.**

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

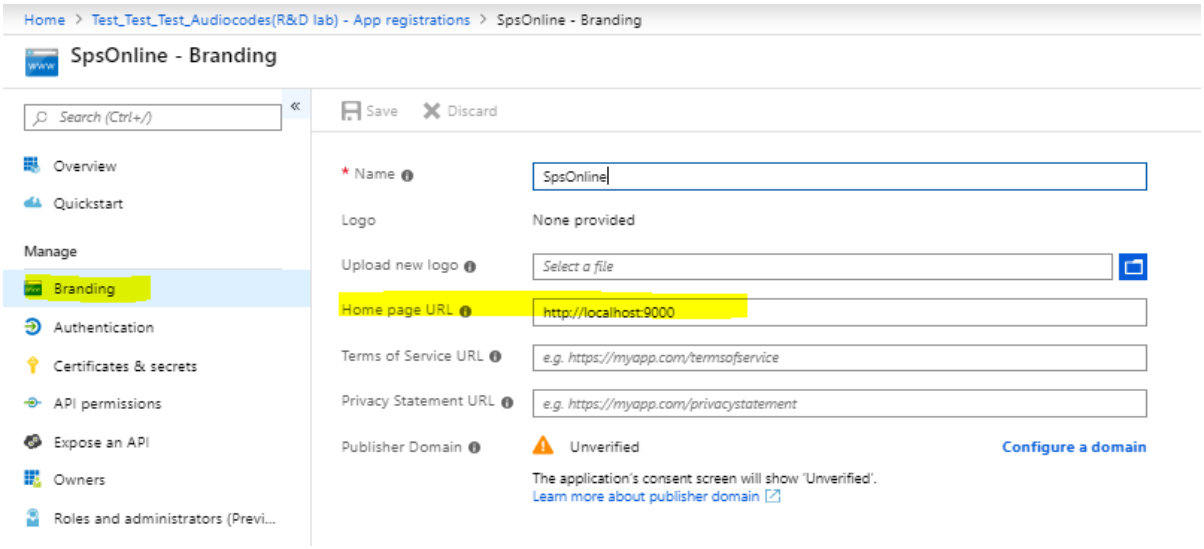


33. Under 'Delegated permissions', select all permissions.

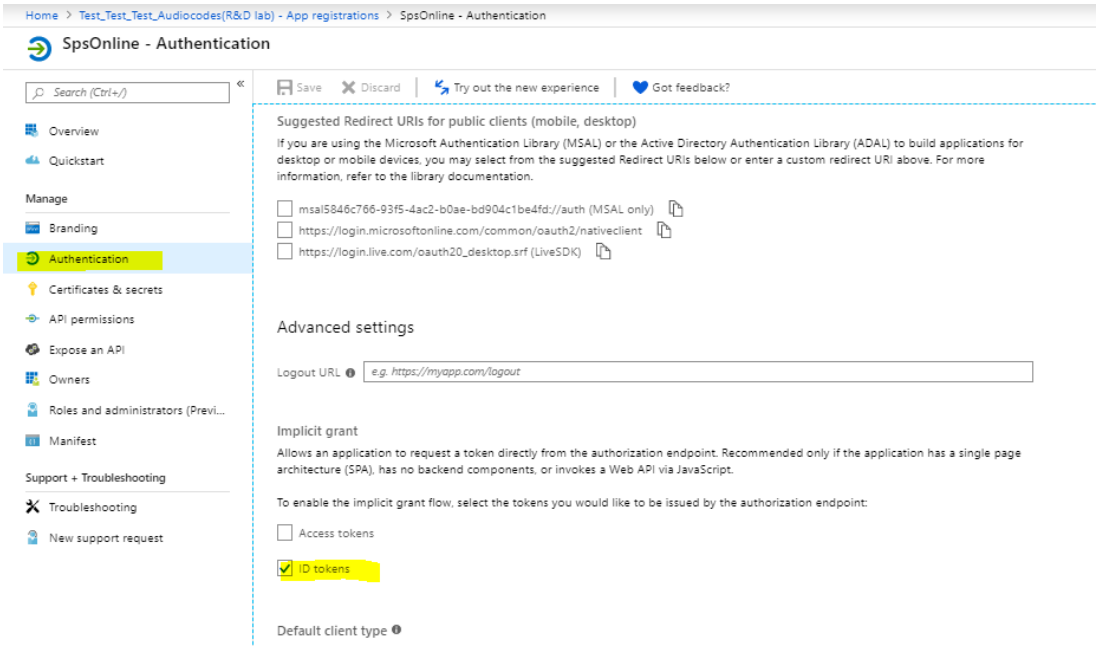
34. Edit the application manifest. Change "groupMembershipClaims": null to "groupMembershipClaims": "SecurityGroup".
35. Click **Save**.



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



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

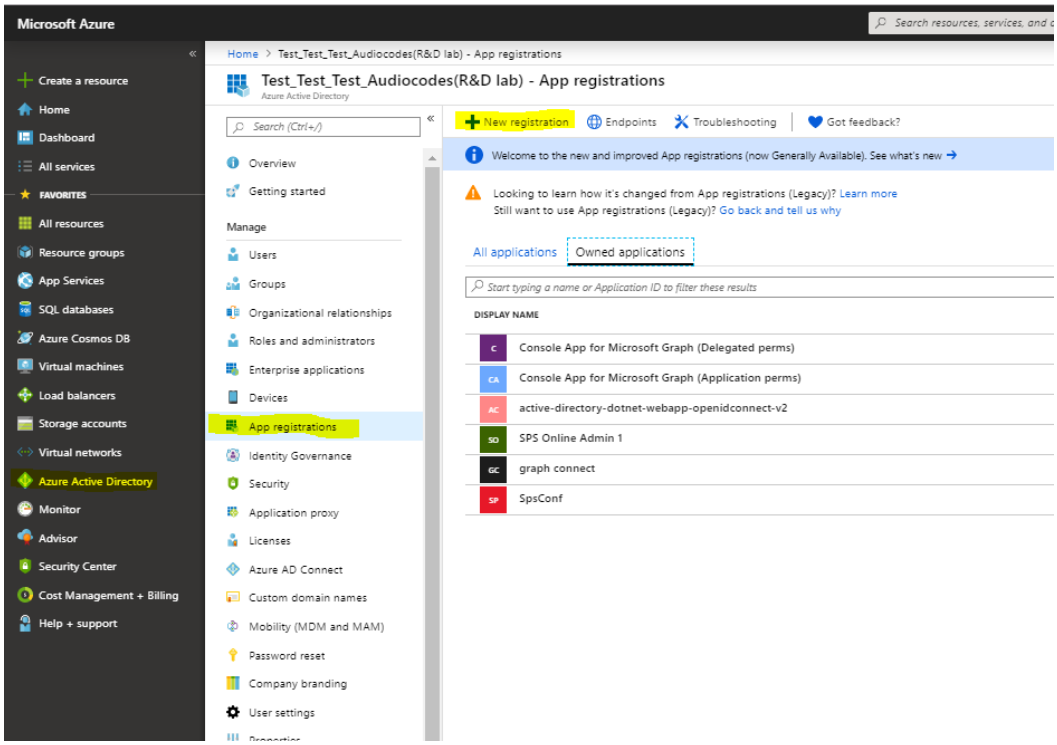

Home > Test_Test_Test_Audiocodes(R&D lab) - App registrations > SpsOnline - Authentication
SpsOnline - Authentication
Search (Ctrl+/)
Overview
Quickstart
Manage
Branding
Authentication
Certificates & secrets
API permissions
Expose an API
Owners
Roles and administrators (Previ...
Manifest
Support + Troubleshooting
Troubleshooting
New support request
Save
Discard
Try out the new experience
Got feedback?
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.
msal5846c766-93f5-4ac2-b0ae-bd904c1be4fd://auth (MSAL only)
https://login.microsoftonline.com/common/oauth2/nativeclient
https://login.live.com/oauth20_desktop.srf (LiveSDK)
Advanced settings
Logout URL
e.g. 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
ID tokens
Default client type

2.4.3 Add cSPS Admin Application

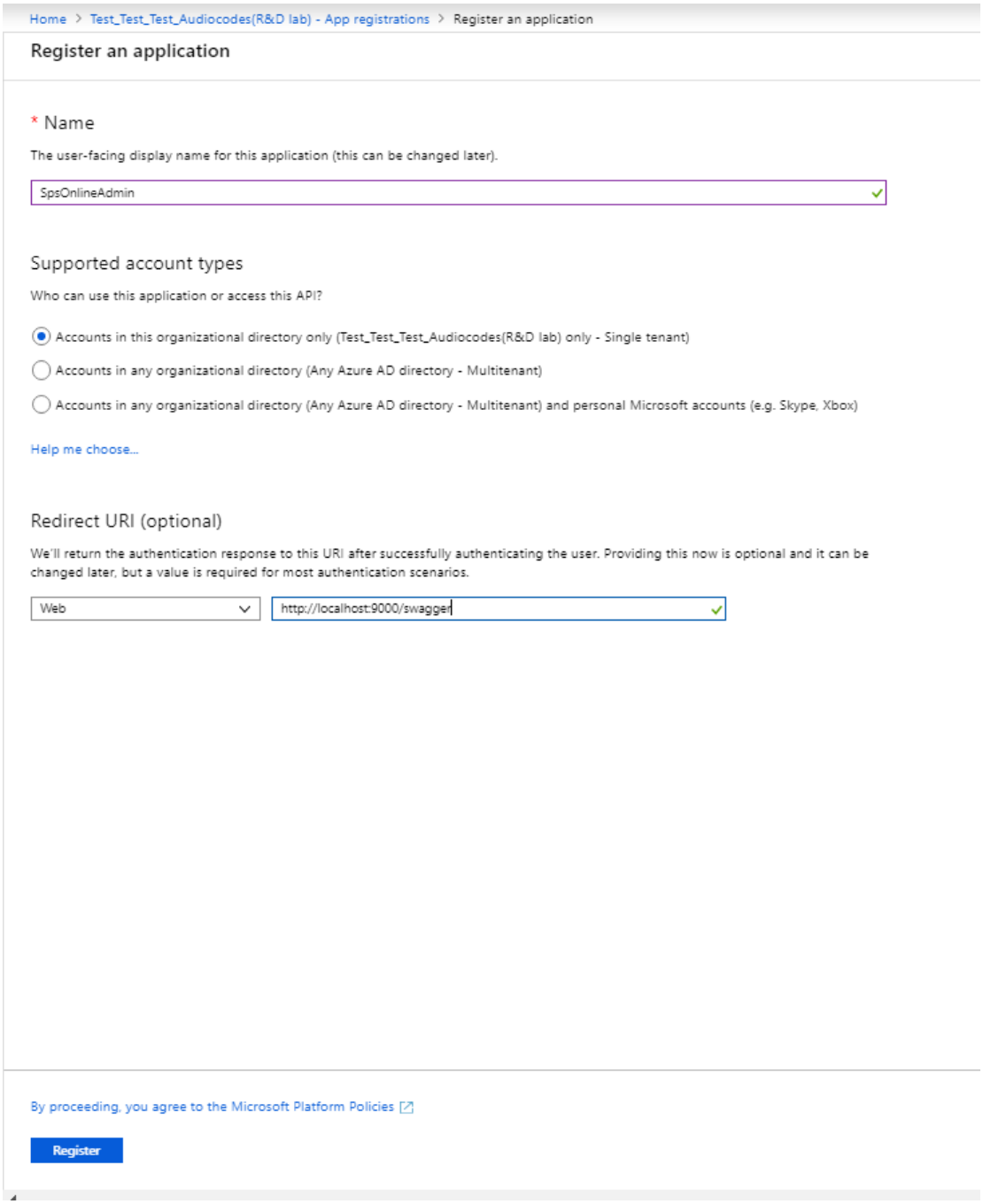
The procedure below describes how to add a cSPS Admin Application.

➢ To add a cSPS Admin Application:

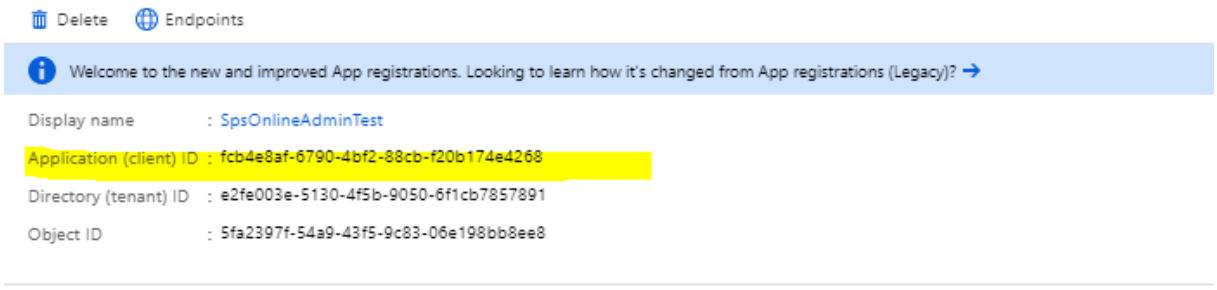
1. In the Azure Active Directory pane, click **App registrations**, and then select **New registration**.



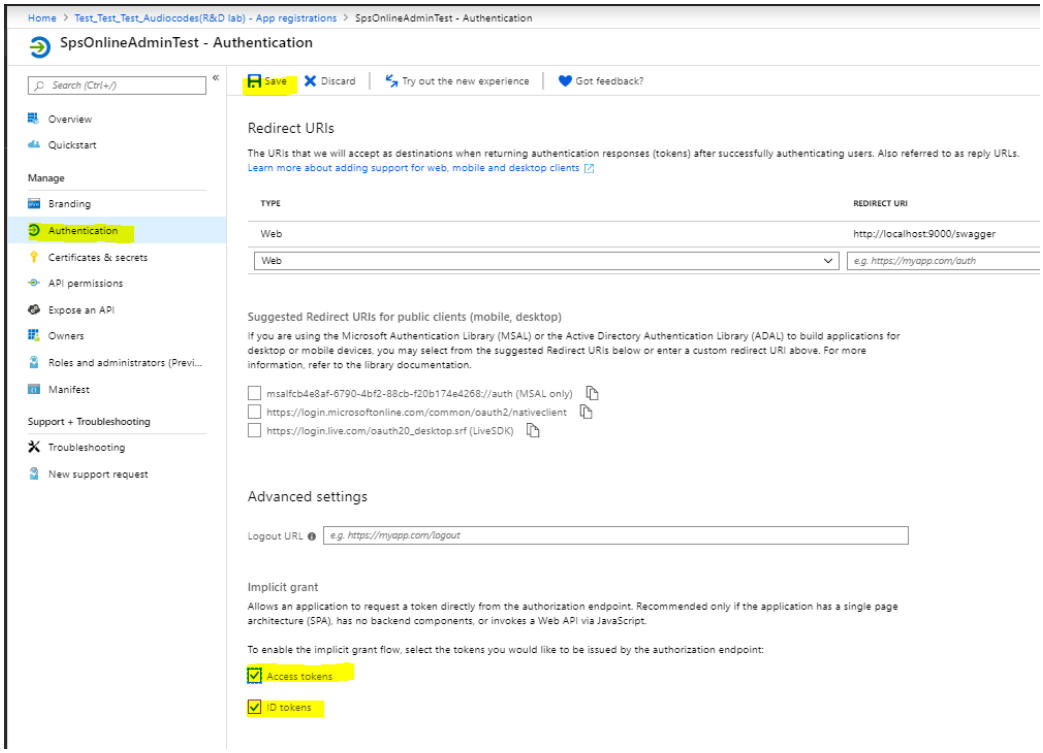
2. In the 'Name' field, enter "SpsOnlineAdmin" for the application.
3. In the Redirect URL' field, select **Web**, and then enter "http://localhost:9000/swagger".



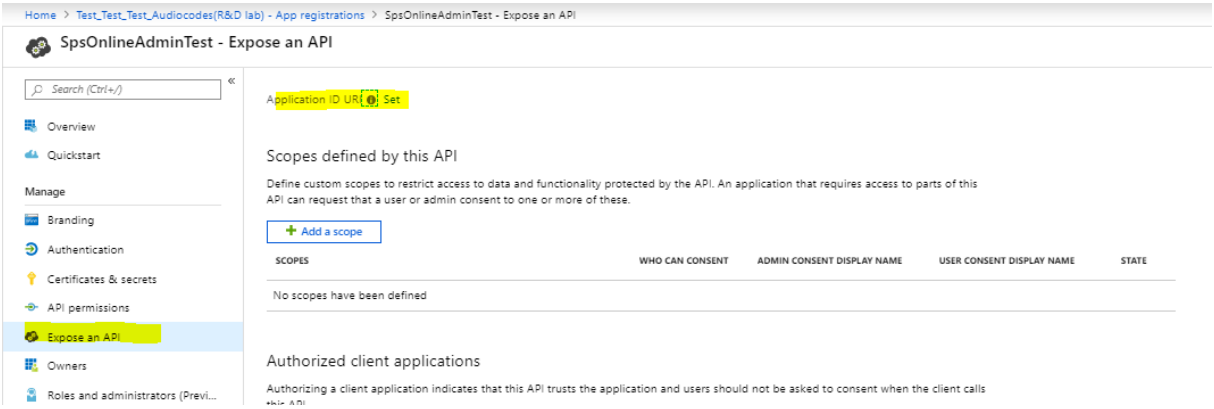
4. Click **Register** to create the application.
5. On the next page, find the **Application ID** value and copy it for future use.



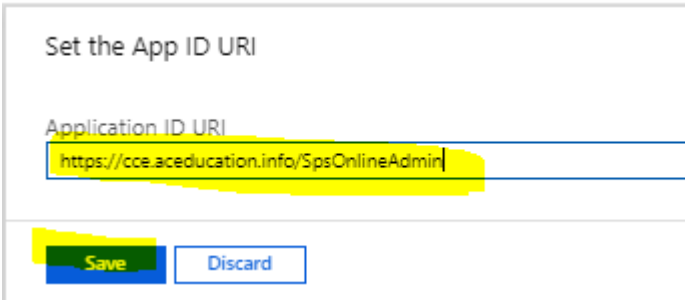
6. Enable the **OAuth 2 Implicit Grant** by selecting **Access tokens** and **ID tokens** on the Authentication screen, under **Implicit grant**.



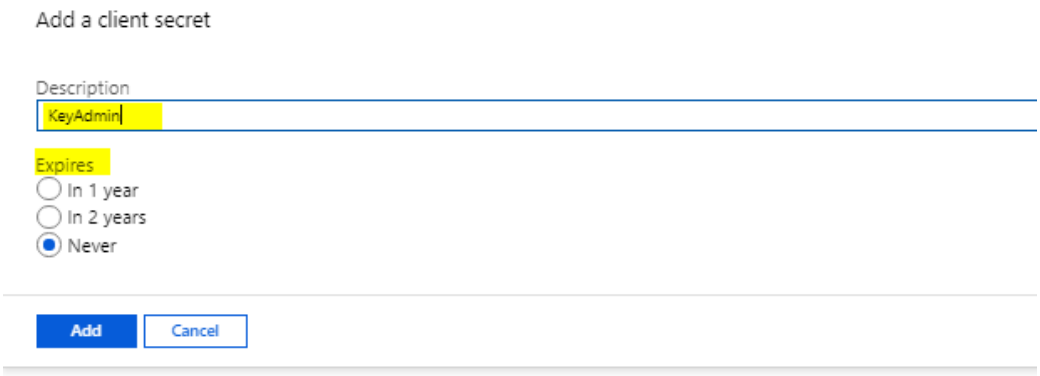
7. Click **Save**.
8. On the Expose an API screen, select **Application ID URI Set**.



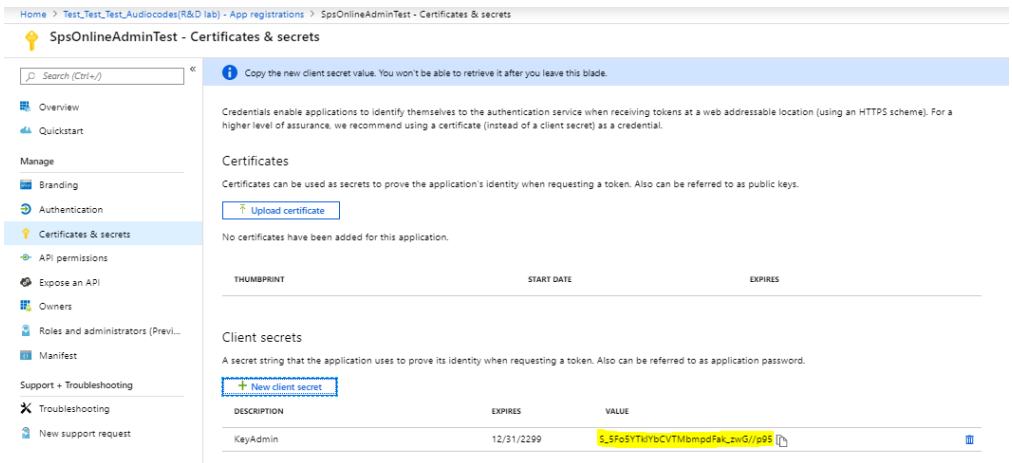
9. Replace the **Application ID URI** with the following URI: 'https://<your_tenant_name>/SpsOnlineAdmin' (replacing <your_tenant_name> with the name of your Azure AD tenant).



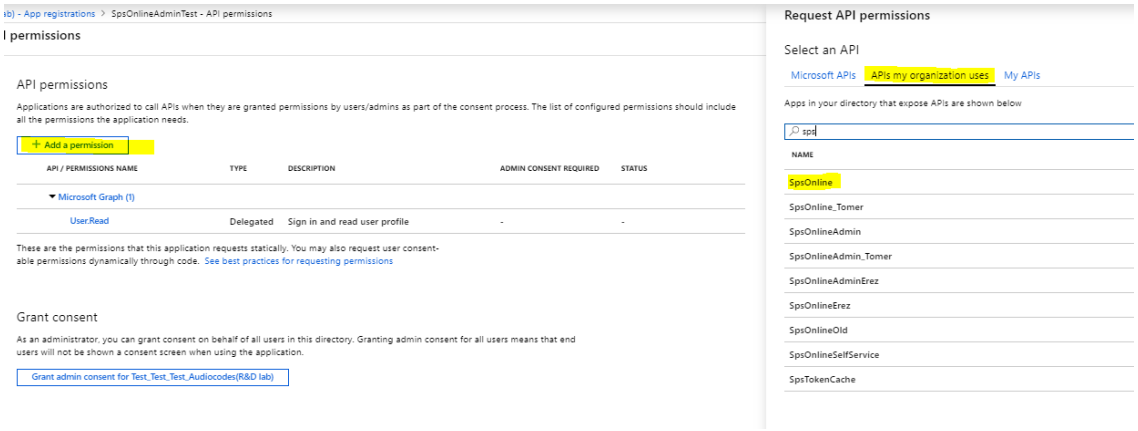
10. Click **Save**.
11. Click **Add a scope** and add user name “user_impersonation”.
12. Select Admin and users for who can consent.
13. In the 'Admin consent display name' field, enter “Access SpsOnlineAdmin”.
14. In the 'Admin consent description' field, enter “Allow the application to access SpsOnlineAdmin 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.



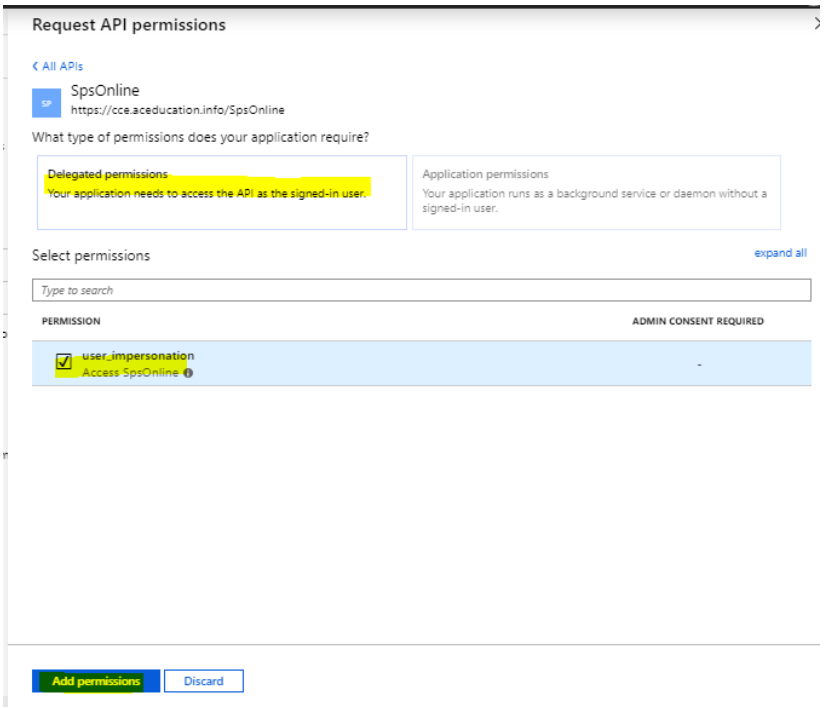
Note: When you save this page, the key value is displayed. Copy and save the value in a safe location. You'll need this key later. This key value will not be displayed again, nor retrievable by any other means. Record it as soon as it is visible from the Azure portal.



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

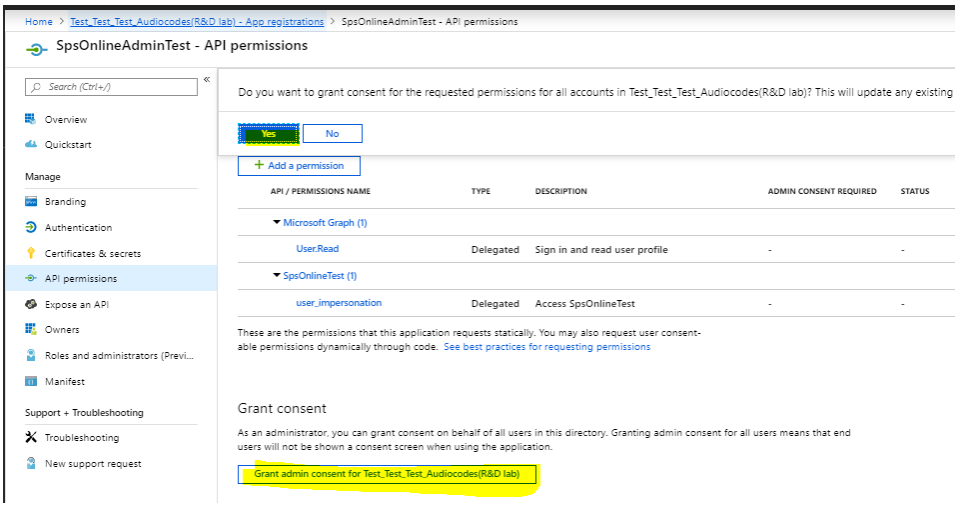


21. Click **Delegated Permissions**, and then select the 'user_impersonation' check box.

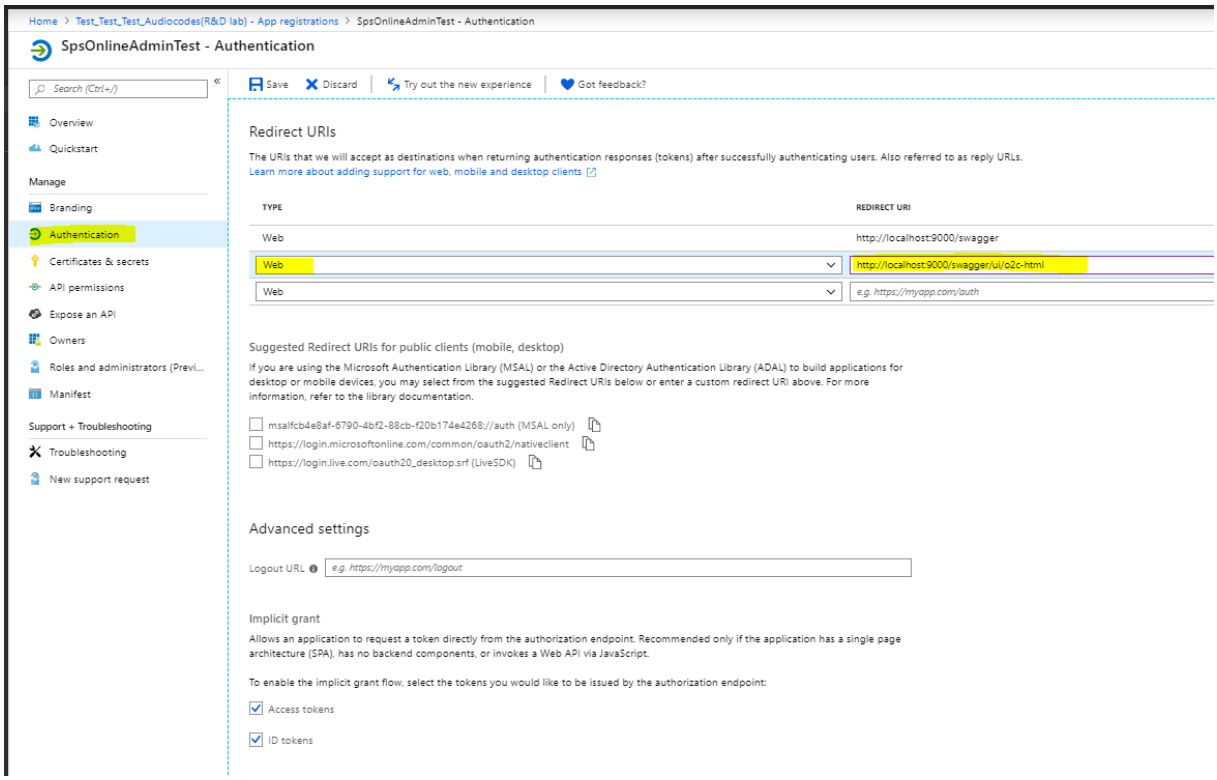


22. Click **Add Permissions**.

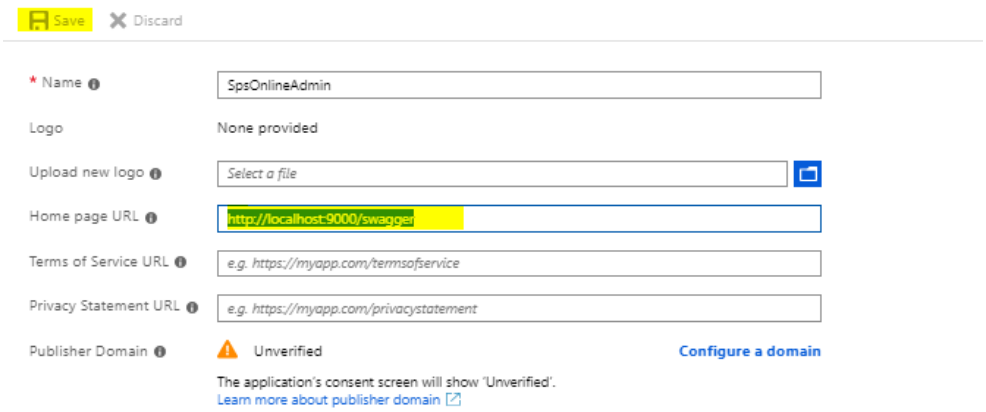
23. On the API permissions screen, select **Grant admin consent...**, and then select **Yes** to confirm it.



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**.



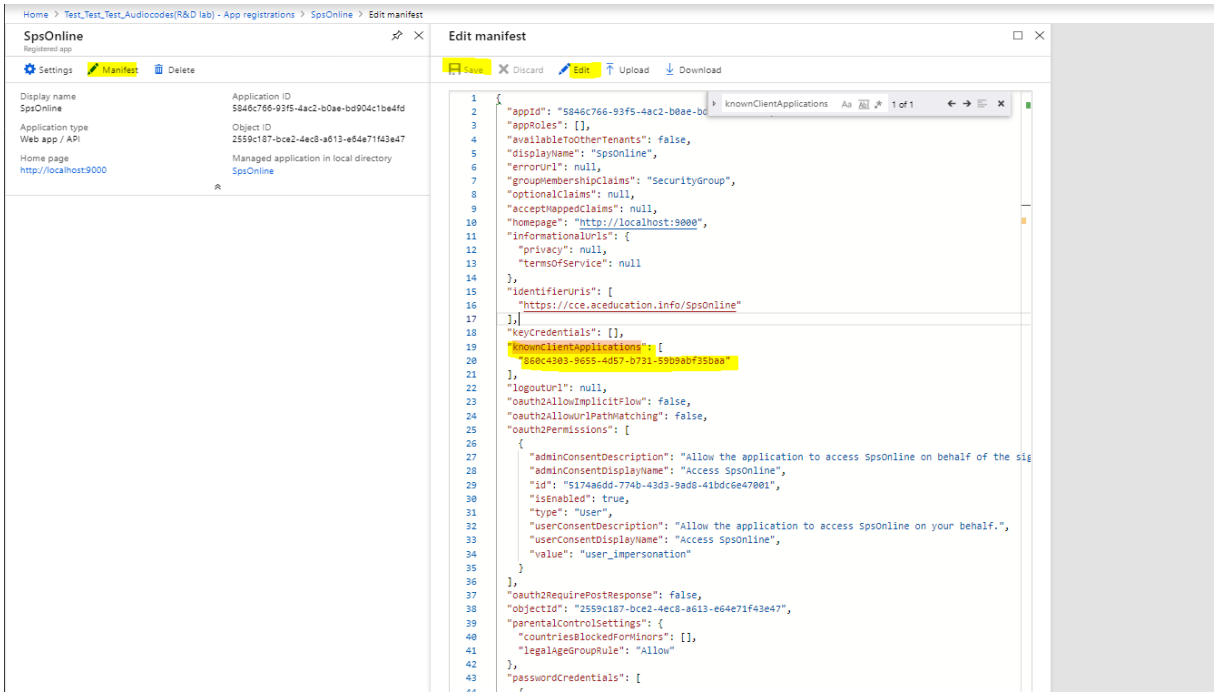
27. On the Branding screen, in the 'Home page URL' field, enter "http://localhost:9000/swagger".



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.



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 http://www.getacert.com/index.html 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 bindIp 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:
https://docs.mongodb.com/manual/replication/

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 'bindIp':

```
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&amp;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.

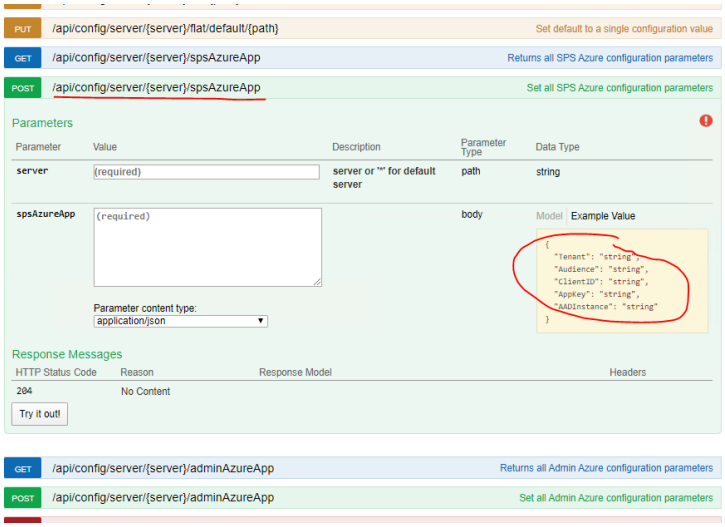
2.9.5 Access Control

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.

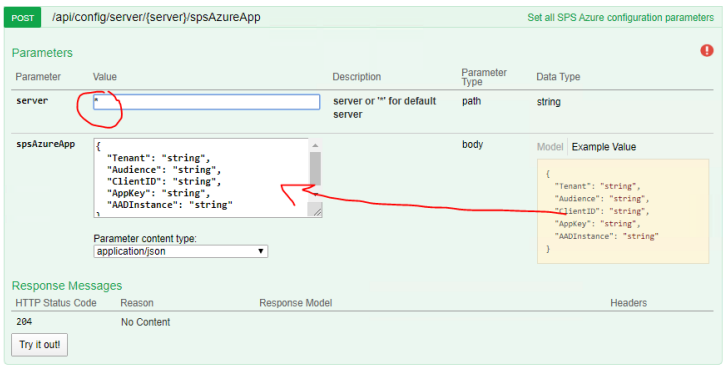
The solution is to allow unauthenticated access to configuration APIs from the **localhost server** and regular authenticated access from anywhere. Unauthenticated remote access is denied. Access to all other APIs remain the same.

➢ 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**.



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



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.
10. 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 Paragraph 9 in Section 2.9.5, using the following parameters:
    - **Admin-ClientID:** "efa90dbf-36cf-4d49-96c6-3db2df2XXXXX"
      Copy from SPSOnline **Admin** Application ID.
    - **Admin-AppKey:** "4zwseWymDcIDpyhfGpwWVD7UYrAlhzEIhGmR8uDXXXXX"
      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 Office 365 URLs and IP address ranges.

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)

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

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

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 **corporate CA**.

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.

2.10.3.1.2 Configuring 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}.
3. Open CMD as administrator and run:

   netsh http add sslcert ipport=0.0.0.0:9001 certhash=<thumbprint> appid=<guid>
4. Verify that swagger is now available via HTTPS using FQDN on port 9001:

   https://SPS-FQDN:9001/swagger

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 Azure App Service 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: https://il-rona-pc.corp.audiocodes.com:9001

   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: https://audiocode.biz/spsOnline .

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:

```
<?xml version="1.0" encoding="UTF-8"?>
  <configuration>
    <system.webServer>
      <staticContent>
        <mimeMap fileExtension=".json"
mimeType="application/json" />
      </staticContent>
    </system.webServer>
  </configuration>
```

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

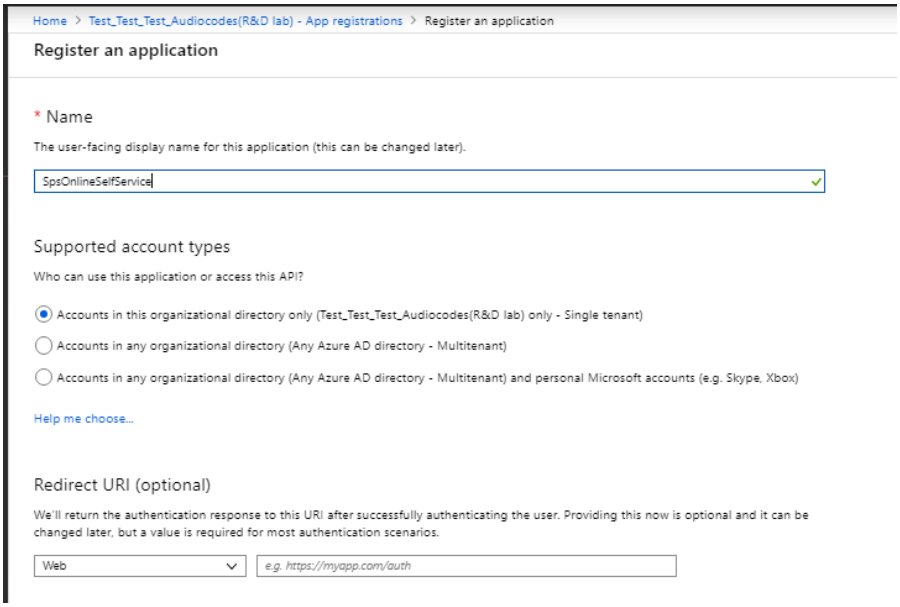
The following describes SPS online self-service hosted on the Cloud SPS Server.

2.10.4.1 Adding an Azure Application

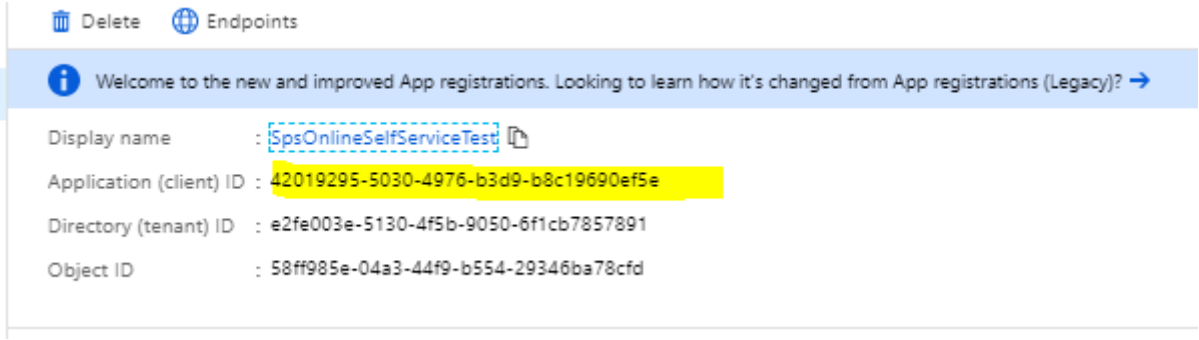
An Azure Web application must be configured for the self-service.

➢ **To add an Azure application:**

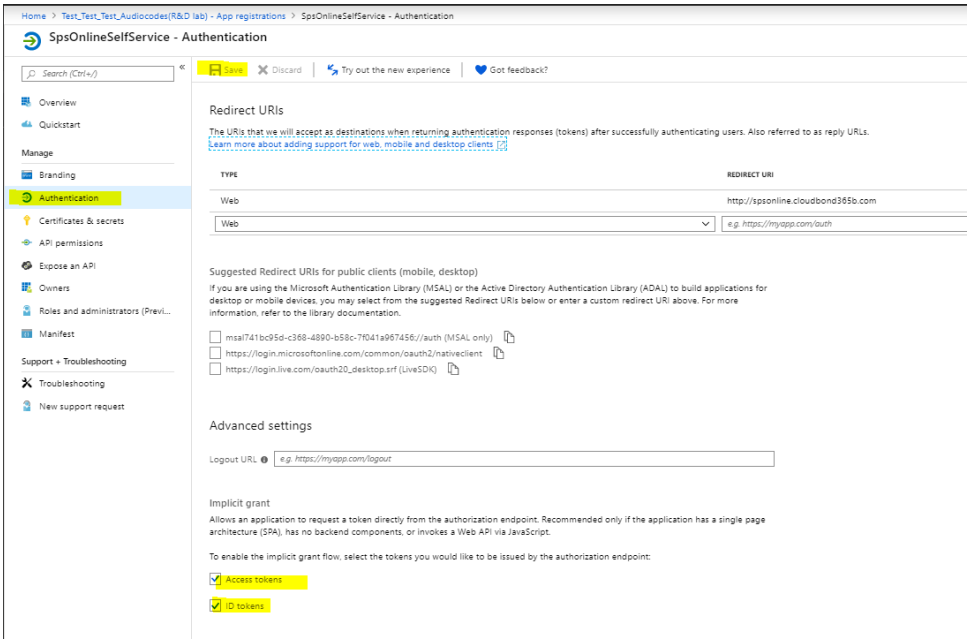
1. Define the FQDN for the SPS Server, and then add it to the DNS so it will resolvable for all relevant users – for example cSPS.<*your Domain*>.
2. Login to the Azure portal.
3. In the 'Azure Active Directory' pane, click **App registrations**, and then click **New registration**.
4. In the 'Name'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



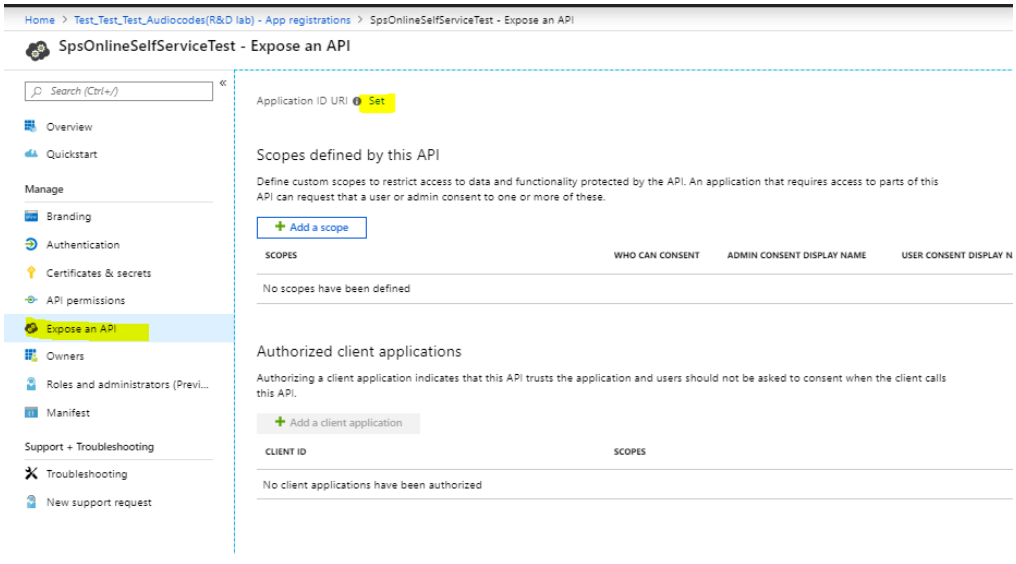
5. Click **Create** to create the new application.
6. In the succeeding page, find the *Application ID* value and copy it to the clipboard. You'll need it later.

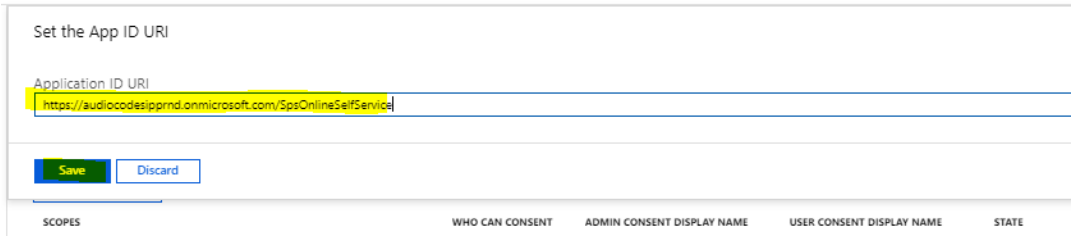


7. Enable the OAuth 2 implicit grant open the Authentication section for your application and check Access Token and ID Token under implicit grant.



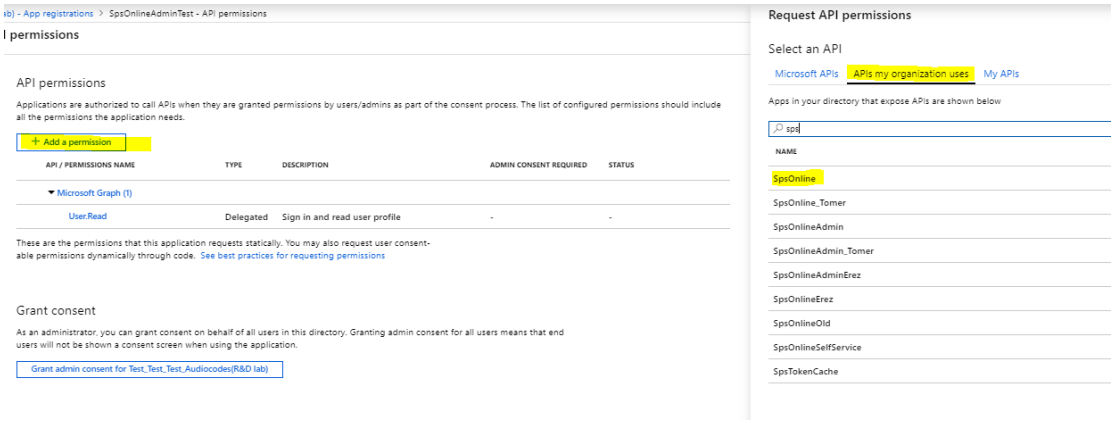
8. Click **Save**.
9. On the **Expose an API** screen, click **Application ID URI Set**.



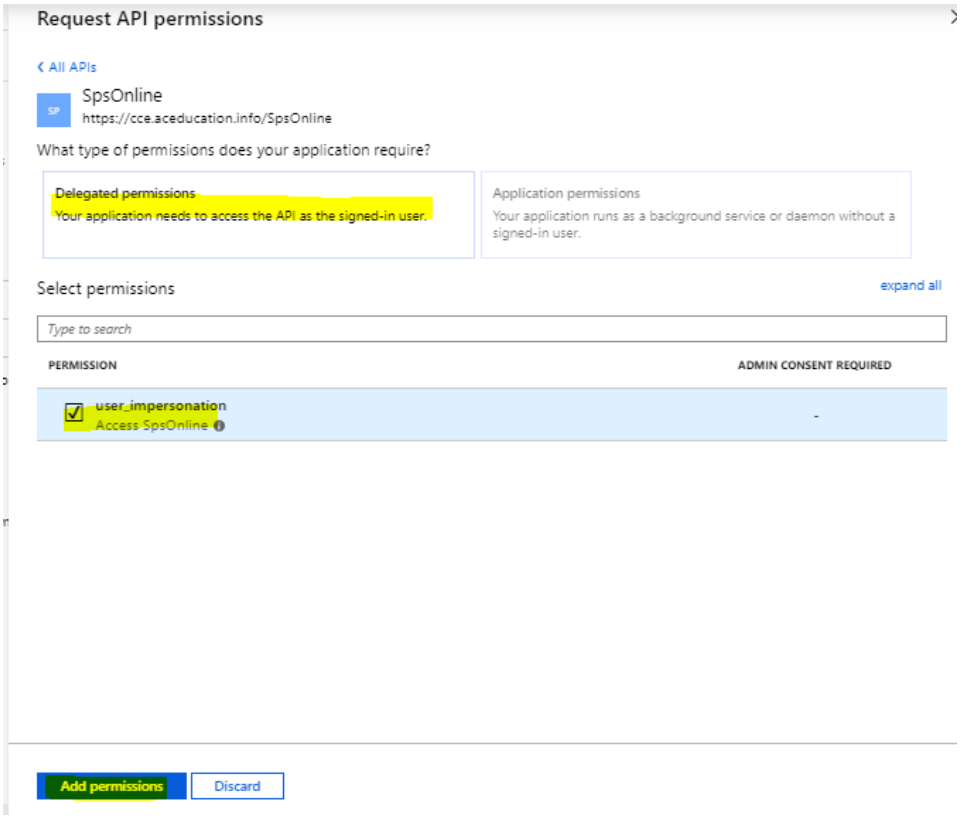


10. Replace the Application ID URI with the following URI: 'https://<your_tenant_name>/**SpsOnlineSelfService** ' (replacing <your_tenant_name> with the name of your Azure AD tenant).
11. Click **Save**.
12. Click **Add a scope** and add user name “user_impersonation”.
13. Select Admin and users for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

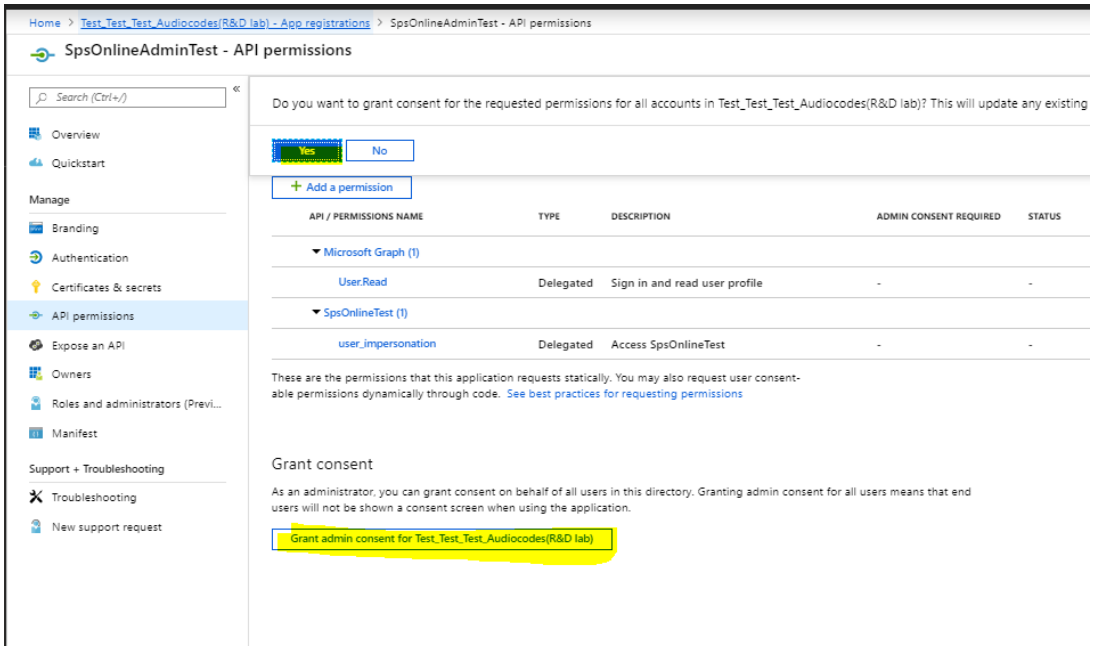
14. In the 'Admin consent description' field, enter “Allow the application to access SpsOnlineAdmin on behalf of the signed-in user.”.
15. In the 'User consent display name' field, enter “Access SpsOnlineAdmin”.
16. In the 'User consent description' field, enter “Allow the application to access SpsOnlineAdmin 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**.



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



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



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 http://localhost/ and verify that the NGINX Welcome page is displayed.
5. Open a Web browser from an external server to http://YOUR-SPS-FQDN/ 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 http://YOUR-SPS-FQDN/ (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 http://YOUR-SPS-FQDN/ 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 **corporate CA**.

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 https://certificatetools.com/.

➢ **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.

2.10.4.4.2 Sign 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 **corporate CA**.

➢ **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;
```

```
        }

        # 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;
        }
    }
```

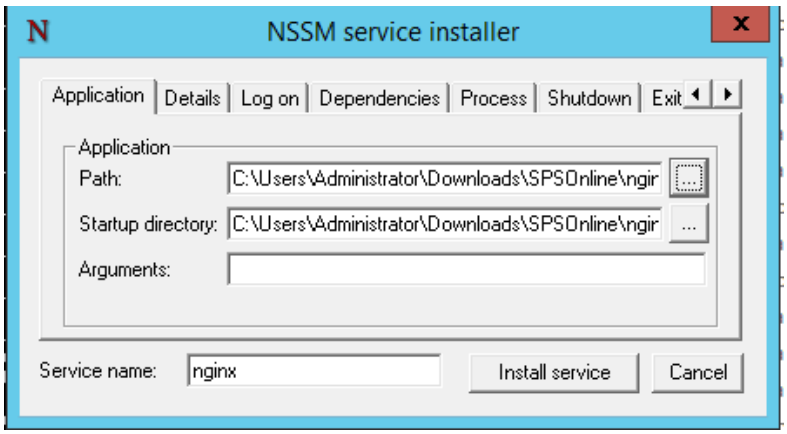
2. Edit the *SpsOnlineSelfService\assets\appConfig.json* file and change "spsServer" to https:
   - "spsServer": "https://YOUR-SPS-SERVER-FQDN", (For example: "spsServer": "https://il-rona-pc.corp.audiocodes.com",)
3. Run **nginx -s reload**.
4. Verify that the SpsOnline server is running.
5. Open a Web browser to https://YOUR-SPS-FQDN/ (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 https://YOUR-SPS-FQDN/ 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**.



6. Open the services and start the NGINX service.

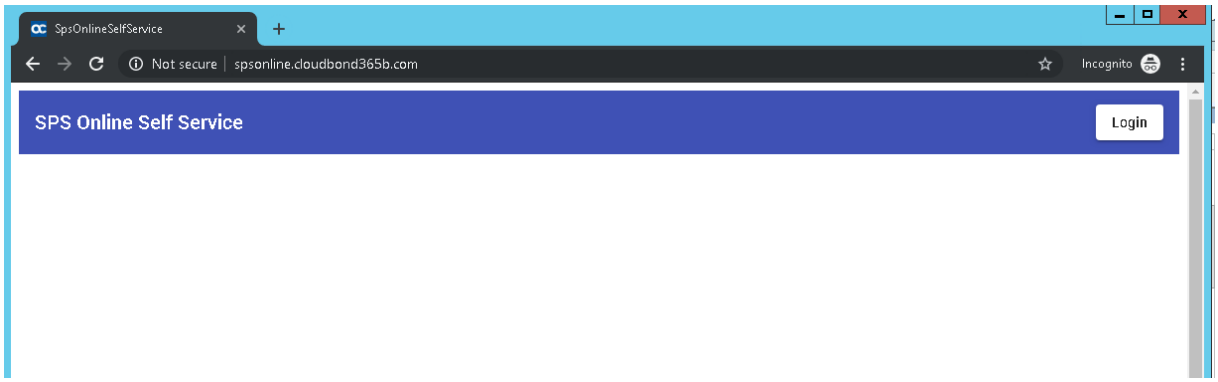
2.10.5 Using the Self-Service

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

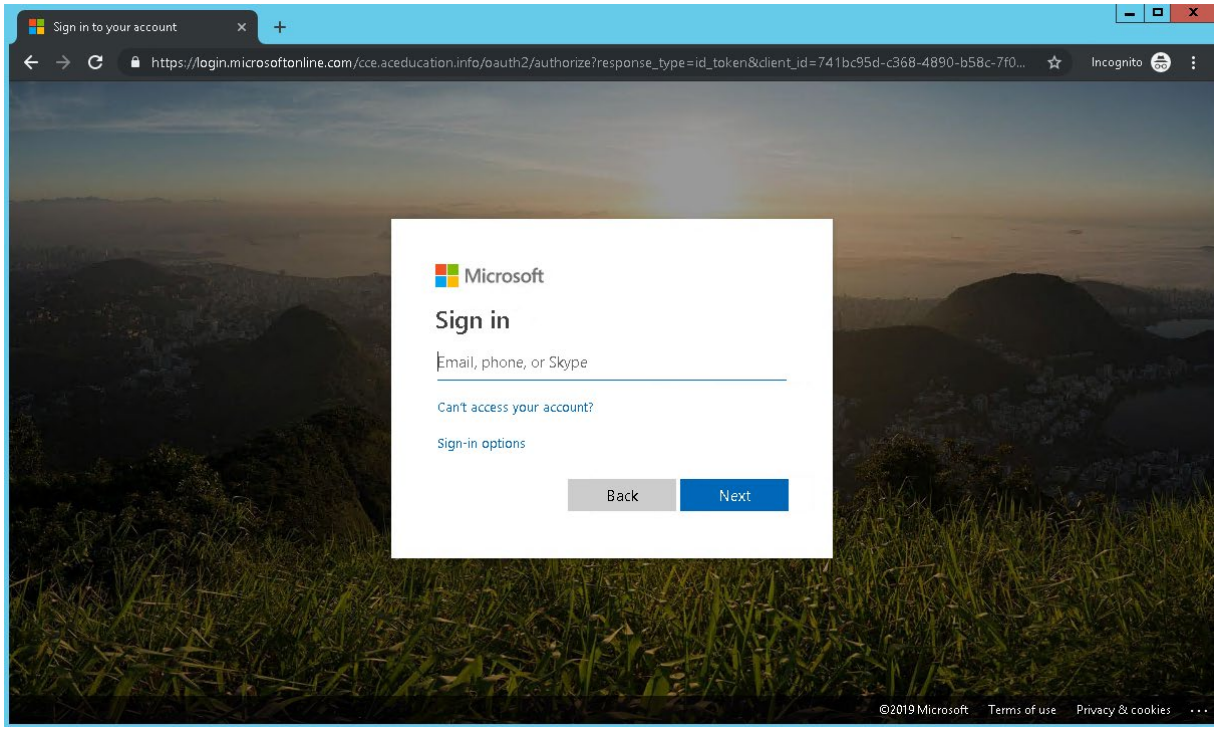
Note: You first need to add the users to the cSPS. The cSPS does not save the password. Only a token is used to authenticate for log in to Skype Online.

➢ **To use the self-service:**

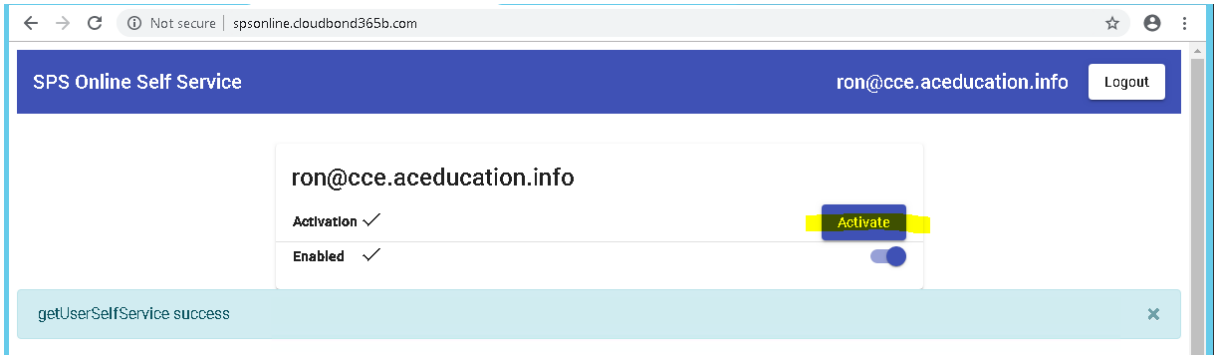
1. Open a Web browser to the URL you defined before; the following page is displayed.



2. Click **Login** to sign in to Microsoft online.



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


Not secure | spsonline.cloudbond365b.com
SPS Online Self Service
ron@cce.aceducation.info
Logout
ron@cce.aceducation.info
Activation
Activate
Enabled
getUserSelfService success

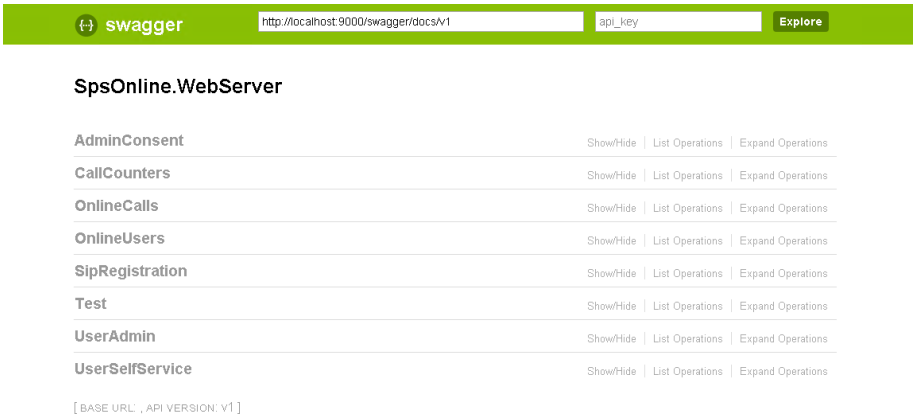
3 Managing Users

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.

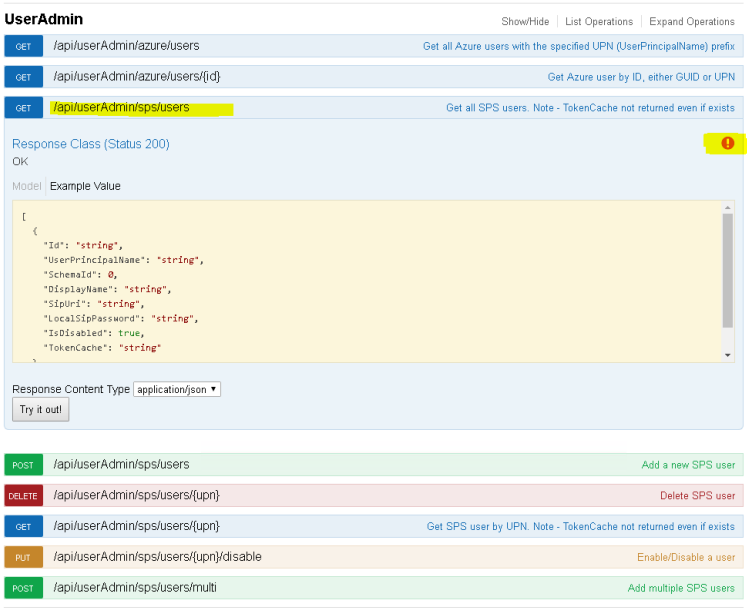


3.1 Logging in with Swagger

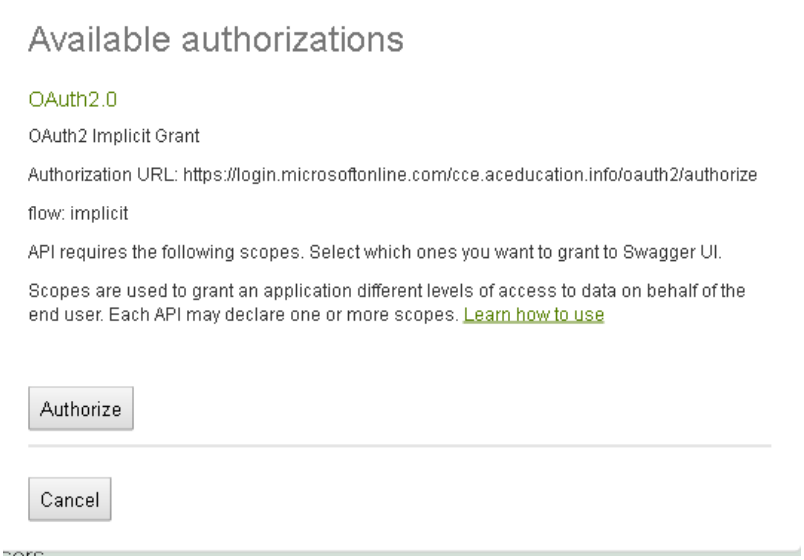
The procedure below describes how to log in using Swagger.

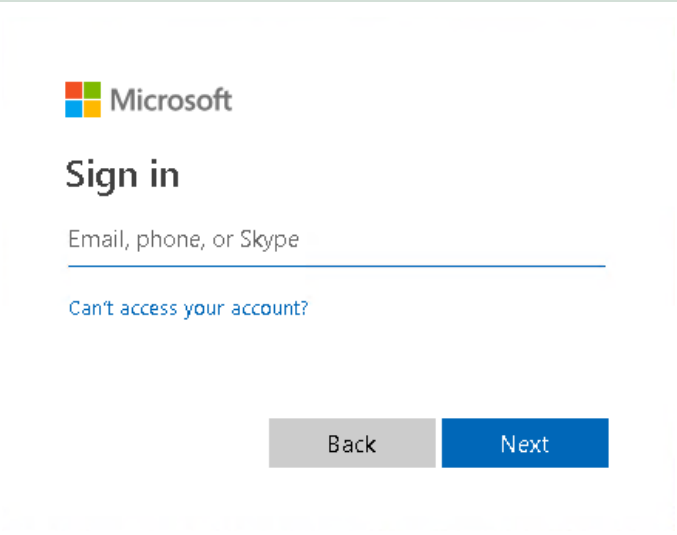
➢ **To log in using Swagger:**

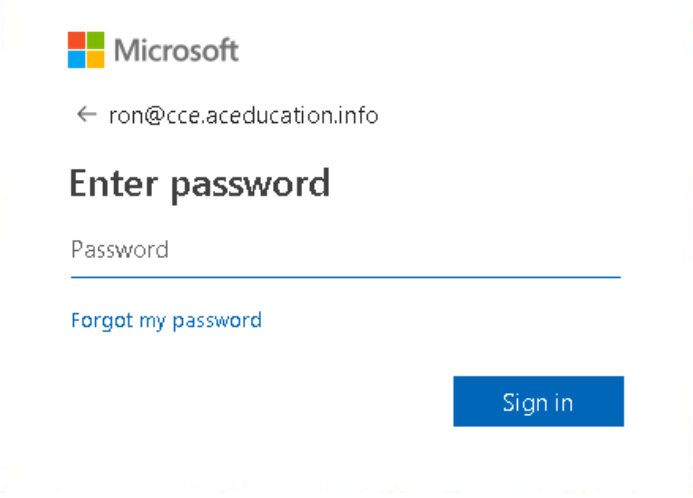
1. To perform operations using the Swagger, first log in with the user that belongs to the security group that you defined earlier on Azure AD.
2. Open one of the operations in the Swagger – for example, */api/user/Admin/sps/users*, and then press the red icon .



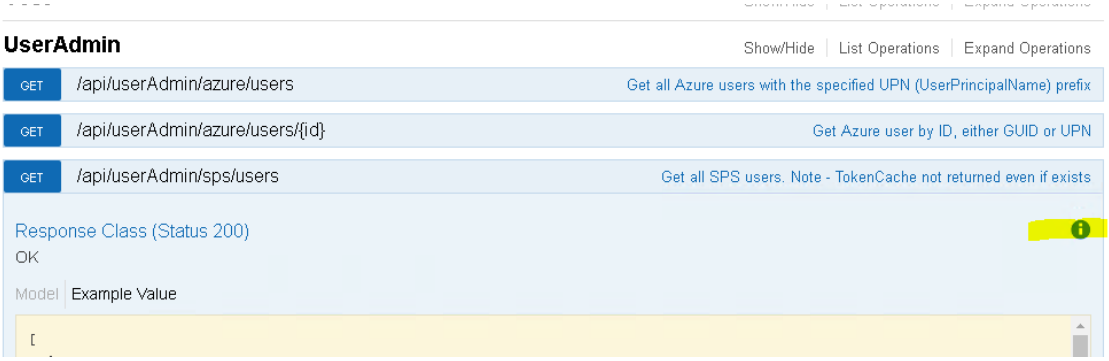
3. Click **Authorize;** a new tab opens to log in.







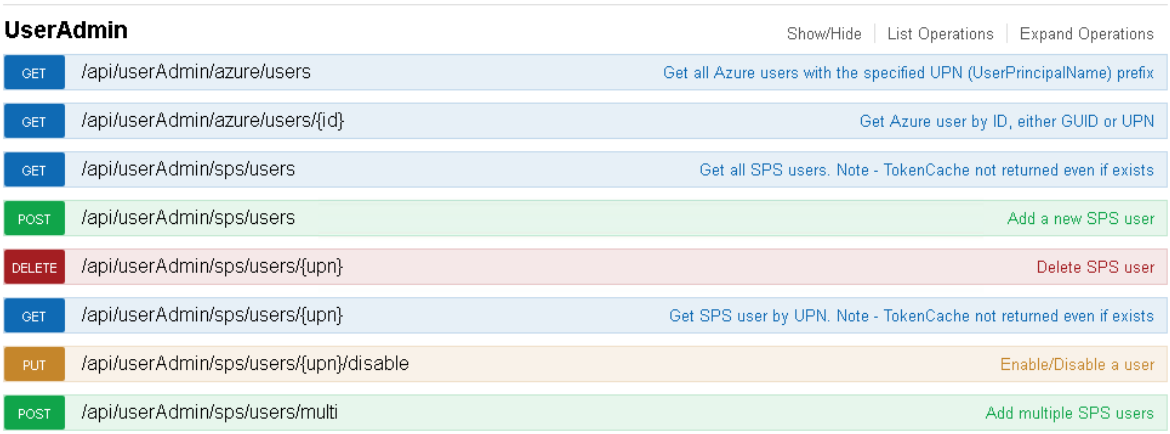
4. If the login is successful, you will see a blue i[icon].



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!**.



- **/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",
  - "SchemaId": 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.

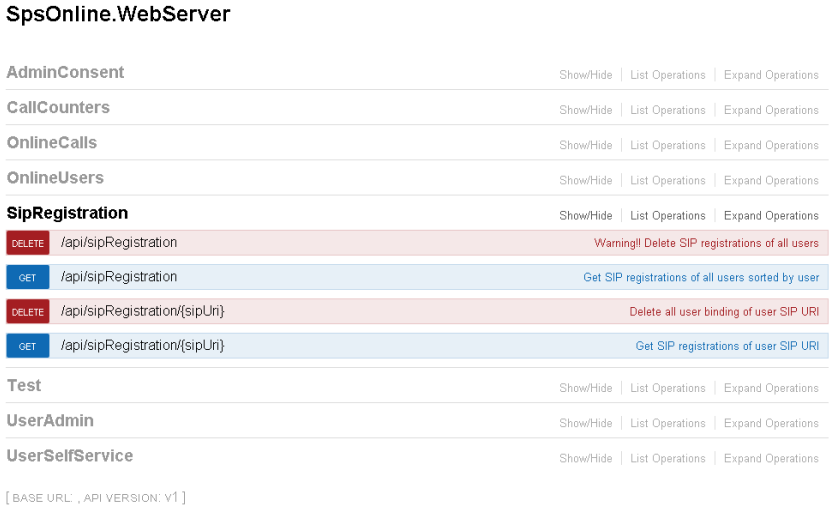
Note: After adding a user and after a user changes the AD password, they must log in to self-service Web that runs on the SPS server and activates the user. (It provides privileges to the SPS to log in to the cSPS as the user). The login is with the AD user/password.

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.

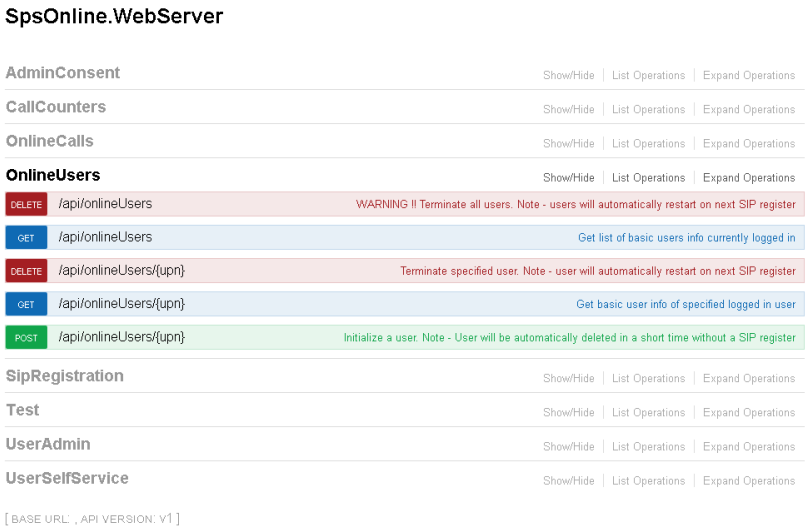


For every user that is registered, the following data is displayed :

```
"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.



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.

A Appendix – Collecting Azure Information

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

cSPS Azure AD security group:
ID:

cSPS Application
ID:
Key Value:

cSPS Admin Application
ID:
Key Value:

SpsOnlineSelfService
ID:

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.
2. 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: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com/

Document #: LTRT-00843