AVAIL™

AVAIL & Azure Active Directory Integration

Reference & Instruction Guide

AVAIL™ & Azure Active Directory Integration

Reference & Instruction Guide

Version: 20220112

Table of Contents

Overview

This document will guide you through the necessary steps for configuring AVAIL with Azure Active Directory for your organization.

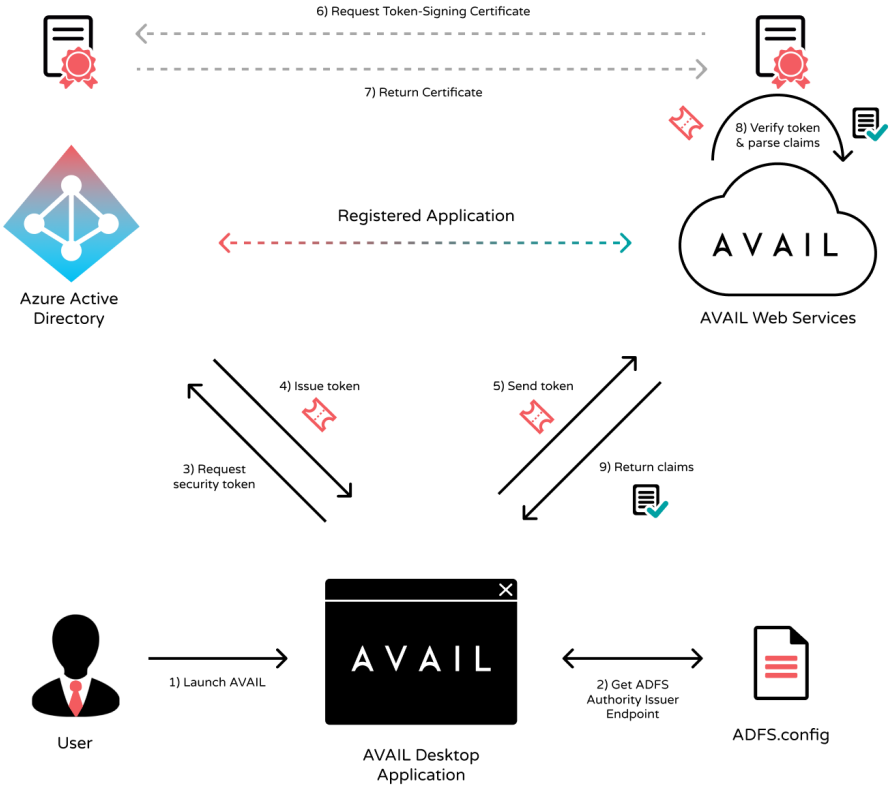
Generally, the document guides through the following tasks:

- How to configure AVAIL as a custom application within your Azure AD.
    - You can assign all users, a subset of users, or an existing group in company Azure AD to this application.
- How to configure a dedicated Publishers group within your Azure AD.
    - You will be assigning users and/or existing groups (e.g. a BIM Managers group) in your Azure AD to this new Publisher group.
    - All users that are assigned to the AVAIL application within your Azure AD are able to sign-in to AVAIL. The Publisher group that is defined in your Azure AD will be translated such that any member of that group will have Publisher privileges within the AVAIL application, such as creating channels, indexing content into channels, and managing and curating tags on content.
    - Any user that is not a member of that Publisher group, but is assigned to the AVAIL application, defaults to a Consumer role.
- How to deploy the AVAIL Desktop software.
    - During the deployment process, you include installer switches that are associated with your Azure AD. When the software is deployed with these switches, it places a special config file on each user's machine that contains info about the AVAIL application that you set up in Azure.
    - When the user launches the AVAIL software, the user is presented with your company's Azure login dialog.

Your Azure Active Directory & AVAIL

Your Azure Active Directory (AD) will establish a trust relationship with AVAIL. Because of this trust relationship, AVAIL is able to accept this token and authenticate the user. Your Azure AD will use a token-signing certificate to digitally sign all security tokens that it produces. Because each security token is digitally signed by your Azure AD federated services, AVAIL can verify that the security token was in fact issued by you and that it was not modified. This helps prevent attackers from forging or modifying security tokens to gain unauthorized access to resources.

(1) When a user launches the AVAIL application on their workstation, (2) AVAIL retrieves the necessary authority issuer endpoint for (3) requesting a security token from your Azure AD. (4) AD provides a token that contains information about the user requesting access to AVAIL then (5) sends the token to the AVAIL web service. (6) AVAIL will request a token-signing certificate upon receiving the token from your federation URI, which is then (7) returned to validate the token. (8) Once the token is verified, AVAIL will parse the claims extracted from the token and determine what actions the user is authorized to perform, and then (9) return those as claims back down to the AVAIL application.

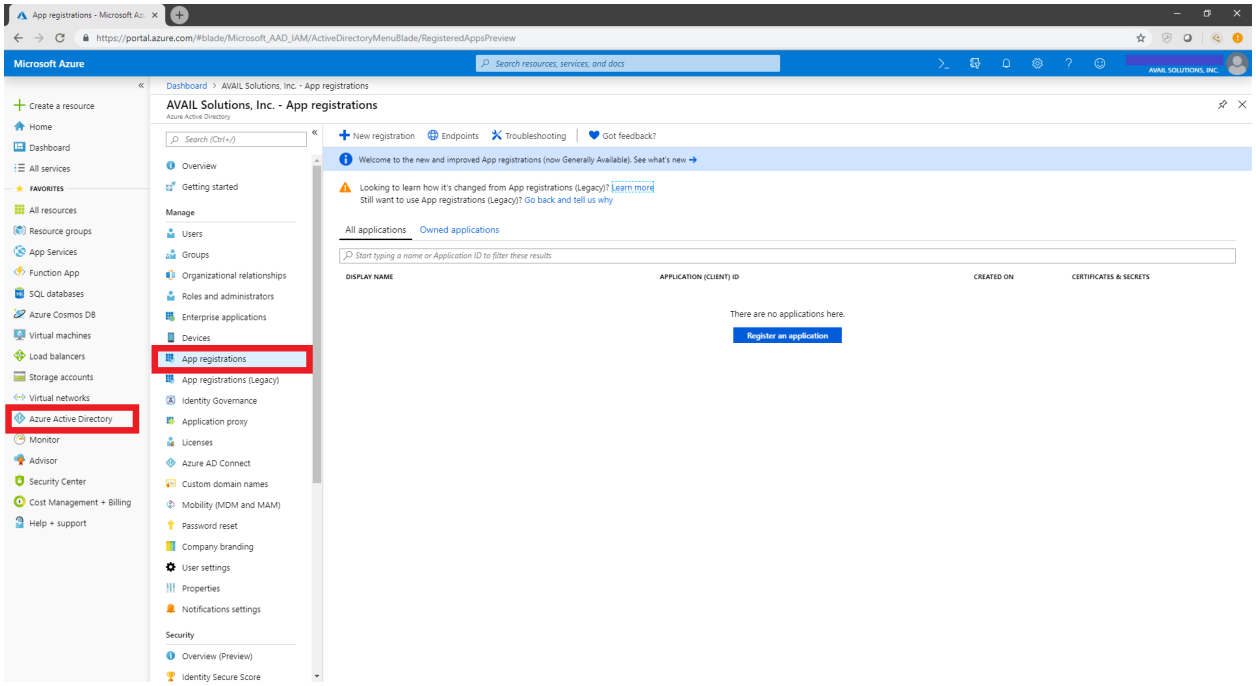


Configuring AVAIL in Azure

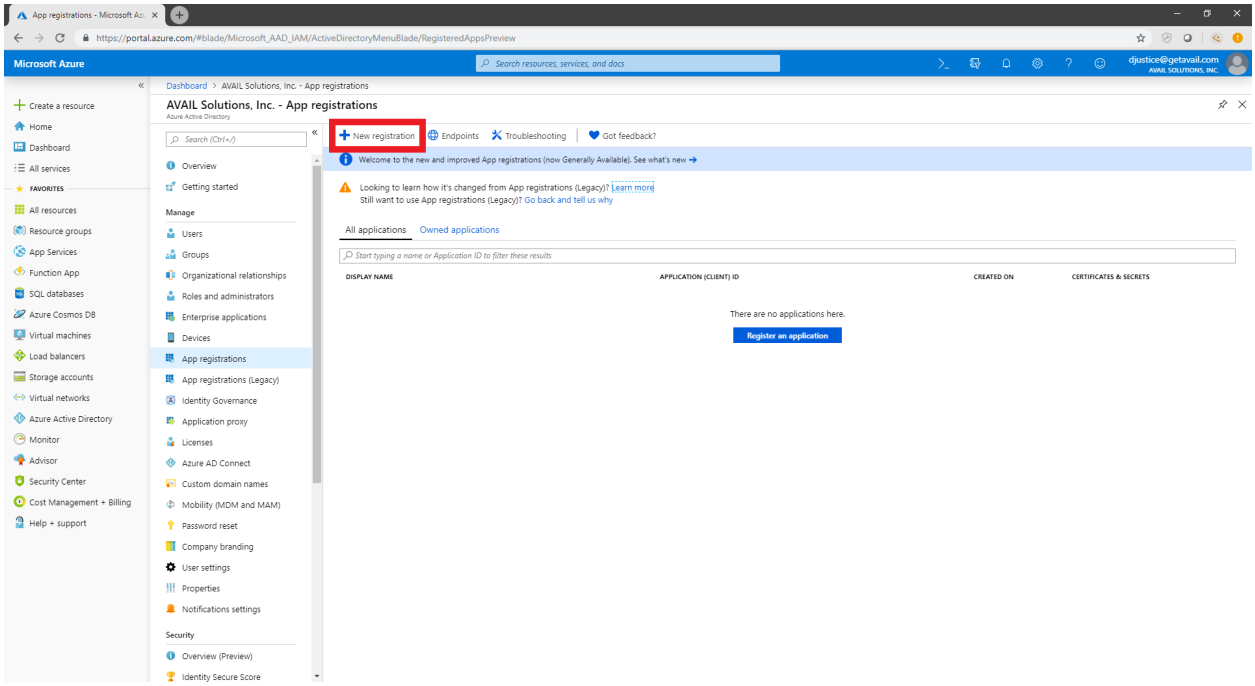
In this section, you will be registering the AVAIL Application, configuring the application with certain permissions, and defining an AVAIL Publishers group all within your Azure Active Directory Portal.

Registering the AVAIL Application

1. From the main navigation bar, select Azure Active Directory, then **App registrations**.

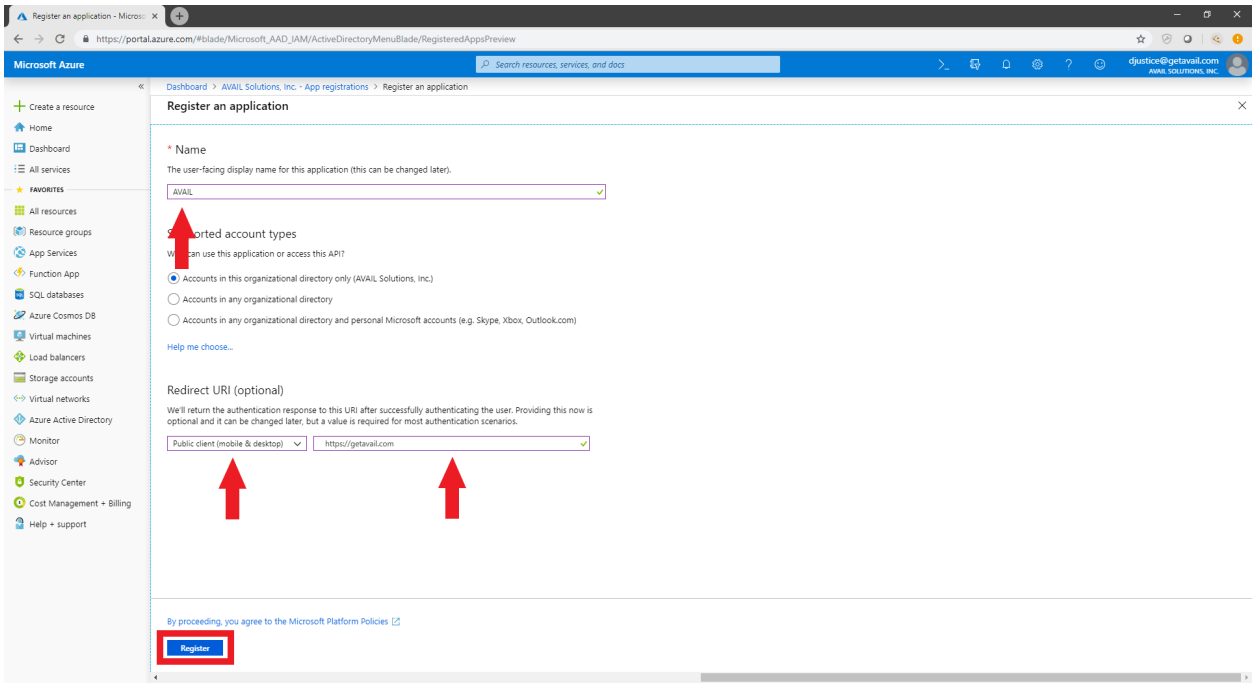


2. Click **+ New application registration.**



3. In the registration form located in the right-hand region, enter in the values shown in the table below. Click **Create** to complete the registration.

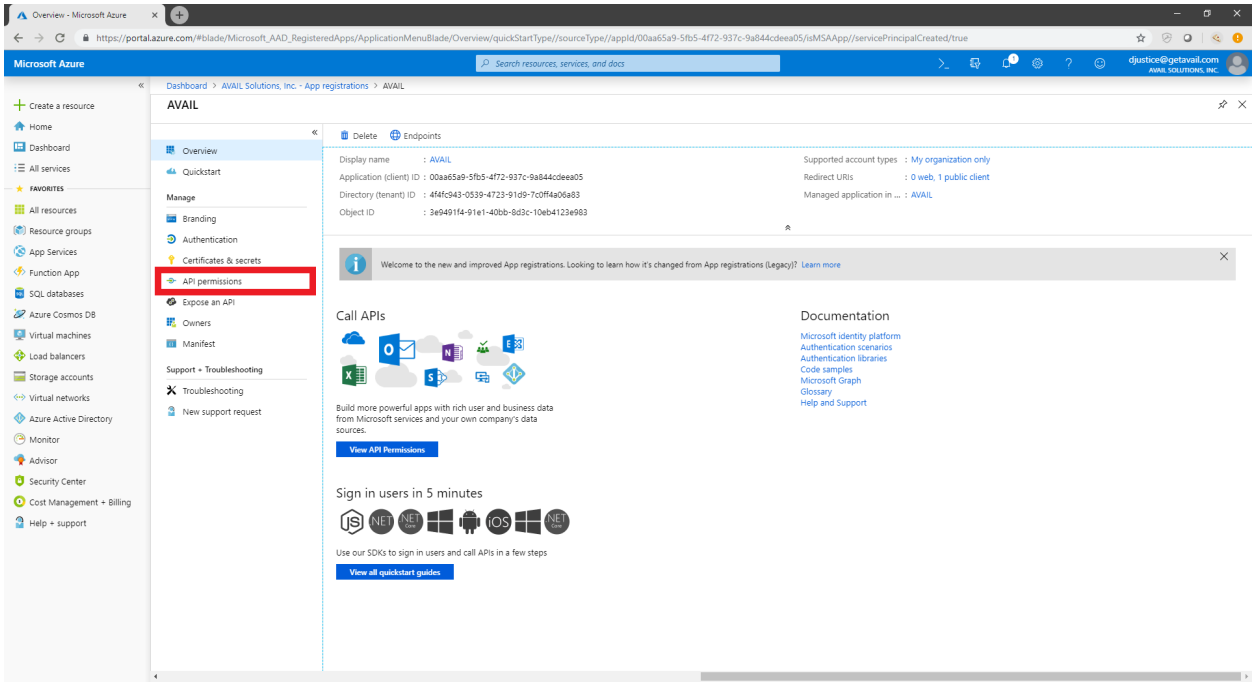
Key	**Value**
Name	AVAIL
Application Type	Public client (mobile & desktop)
Sign-on URL	https://getavail.com



Granting Permissions

Now that the AVAIL Application has been created in Azure, you will next need to grant permission to sign in and read the user's profile.

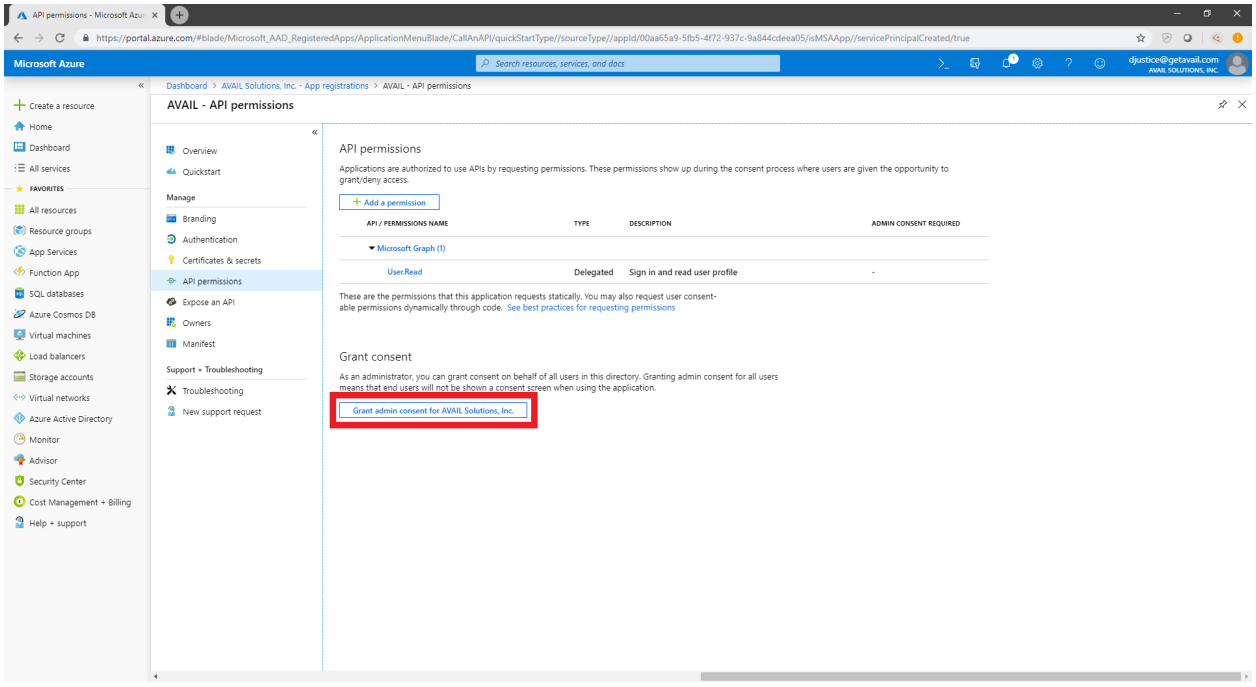
1. In the **AVAIL** application menu**,** select the **API permissions** option.



2. In the **API permissions** page, enable the following API Permissions by click the **+Add a permission** button, under the **Microsoft Graph API**:

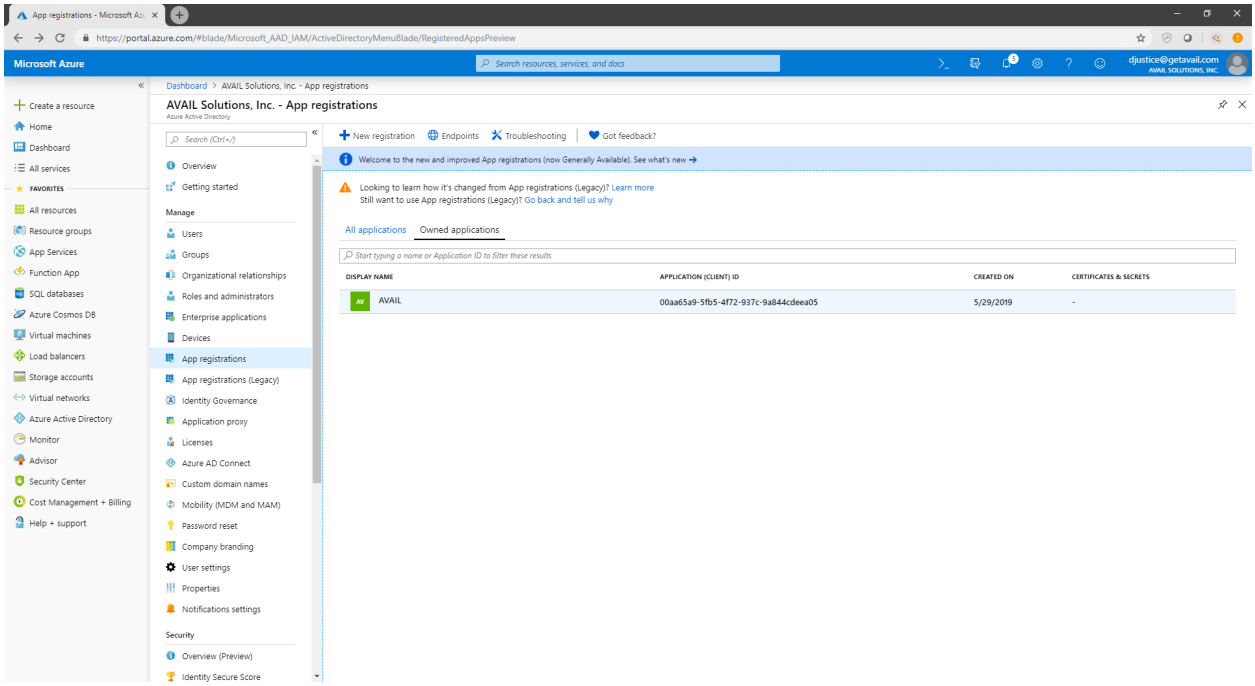
API / Permission name	Type
email	Delegated
offline_access	Delegated
openid	Delegated
profile	Delegated
User.Read	Delegated
Groups.Read.All	Delegated

3. In the **API permissions** page, click **Grant admin consent for AVAIL Solutions, Inc.**
    - If you are prompted “Do you want to grant consent for the requested permissions below for all accounts?”, select **Yes**.

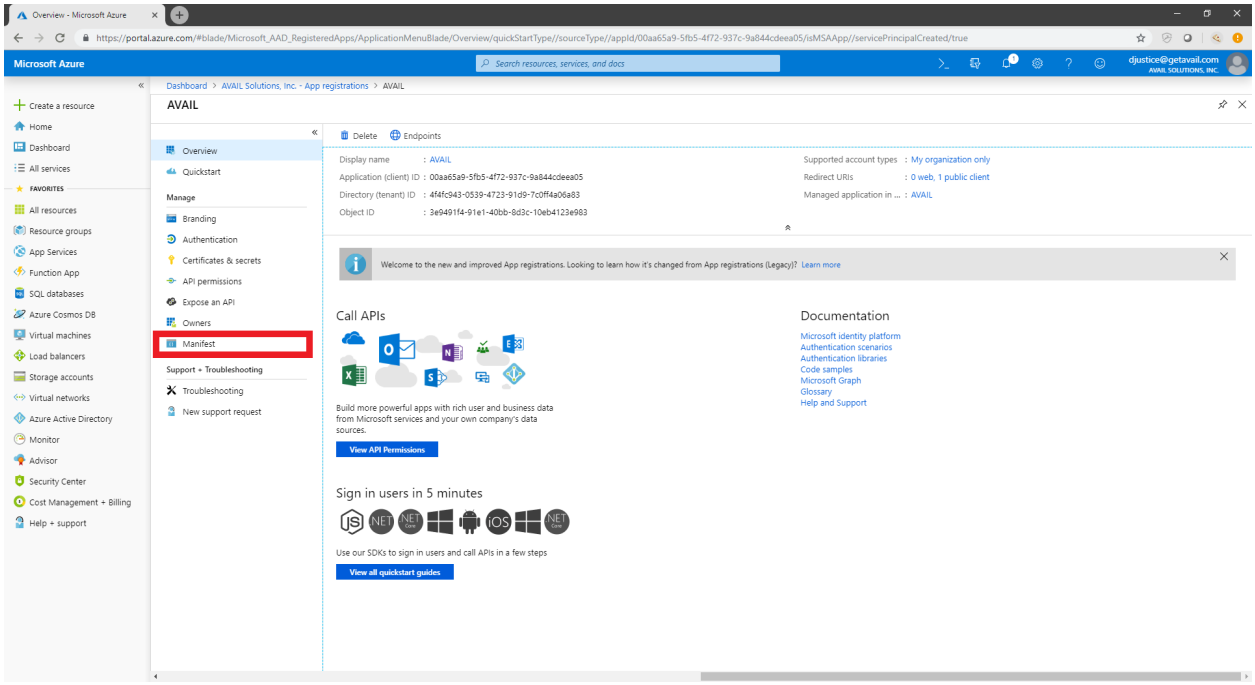


Configuring the Manifest

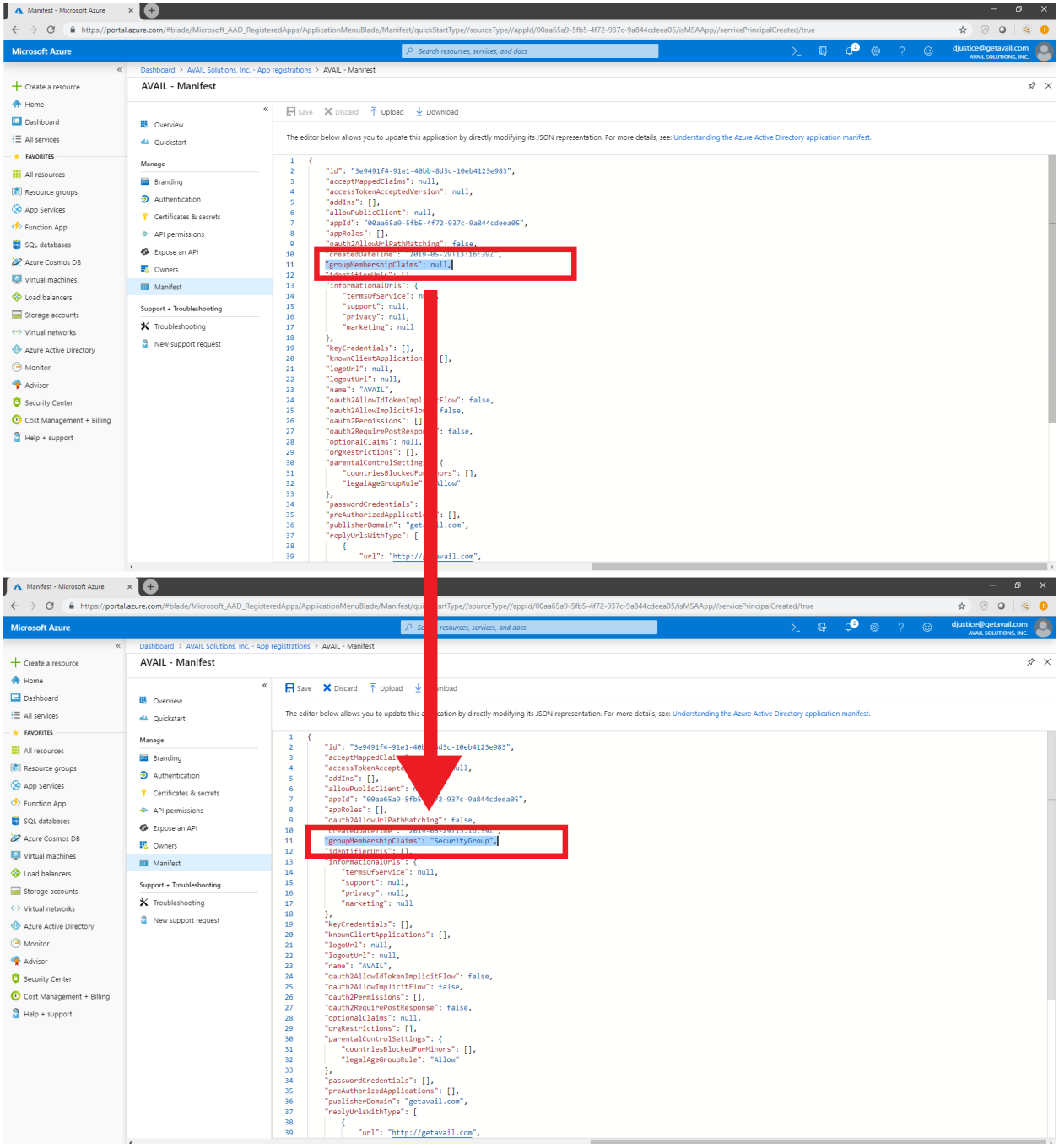
1. Navigate back to the **App Registrations** section and click on the **AVAIL** application.



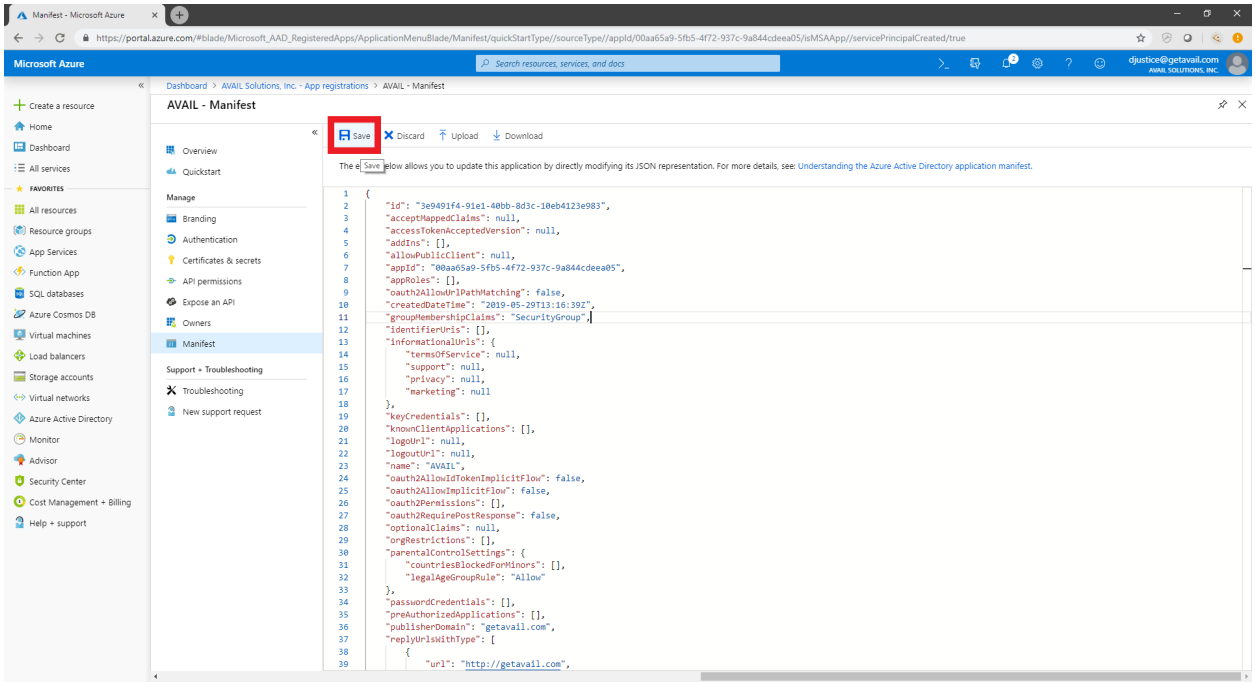
2. In the AVAIL Application area, click **Manifest**.



3. In the **Edit manifest** area in the JSON listed, you should see an item called **“groupMembershipClaims”**. Change the value from **null** to **“SecurityGroup”**.



4. Click **Save** at the top of the **Edit manifest** section.



Creating the Publisher Role Group

Overview

AVAIL supports two primary application roles: Publisher and Consumer. Publishers are generally those who manage content on your network, such as your BIM Managers. Publishers have the ability to create channels, index content into those channels, and share the channels with others within their plan. Consumers on the other hand can only consume the channels that have been shared with them.

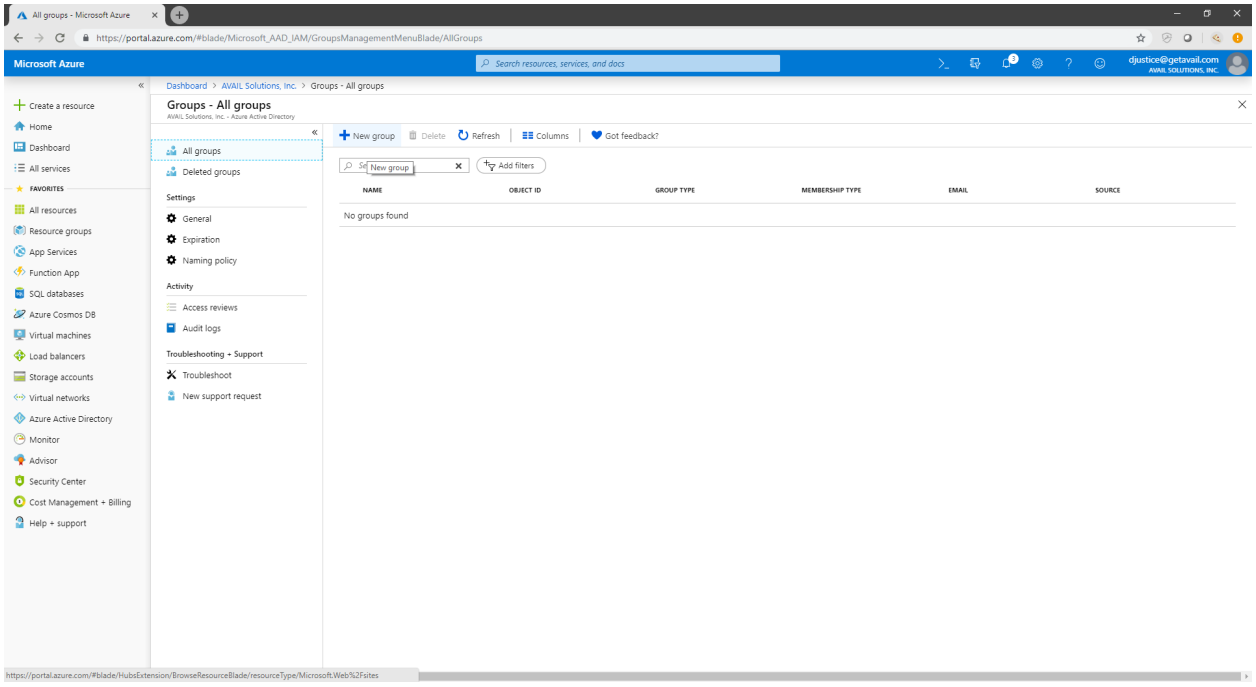
In the Configuring the Manifest section, you configured the AVAIL Application to be able to read a user's Active Directory group memberships. When AVAIL receives, verifies and parses the group memberships from the token, it will check to see if that user is a member of a group that you will specify as representing the AVAIL Publisher Role. Upon detecting the user is a member of that group, AVAIL will determine that user is a Publisher in your plan and provide specific claims back to the AVAIL desktop application. If the user is not a member of this AVAIL Publisher AD group, they will default to the Consumer role in AVAIL.

We recommend creating a dedicated "AVAIL Publishers" group, but it is absolutely acceptable if you already have an existing AD group in mind (such as a "BIM Managers" group). Every organization is just a little bit different, and we're happy to talk through an appropriate configuration for your company.

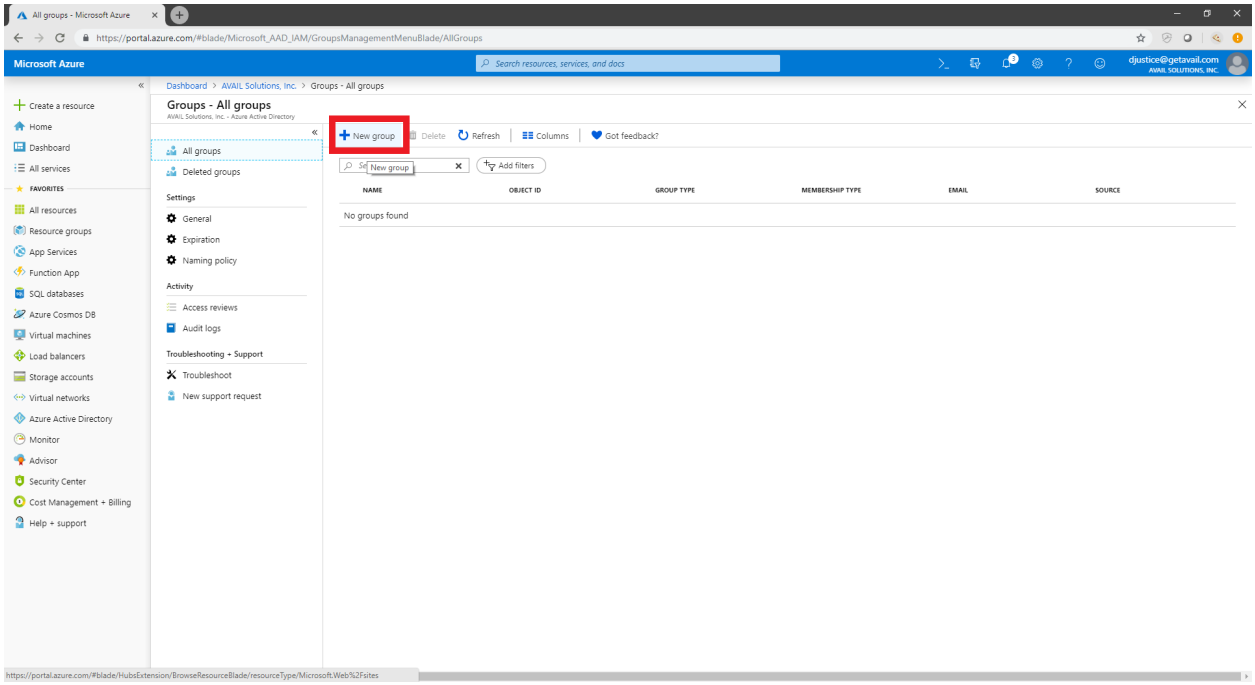
Creating the AVAIL Publishers Group

To view or add the groups within your Azure Active Directory Portal:

1. Select the **Azure Active Directory** menu option in the left navigation menu, then select the **Groups** option in the second column.



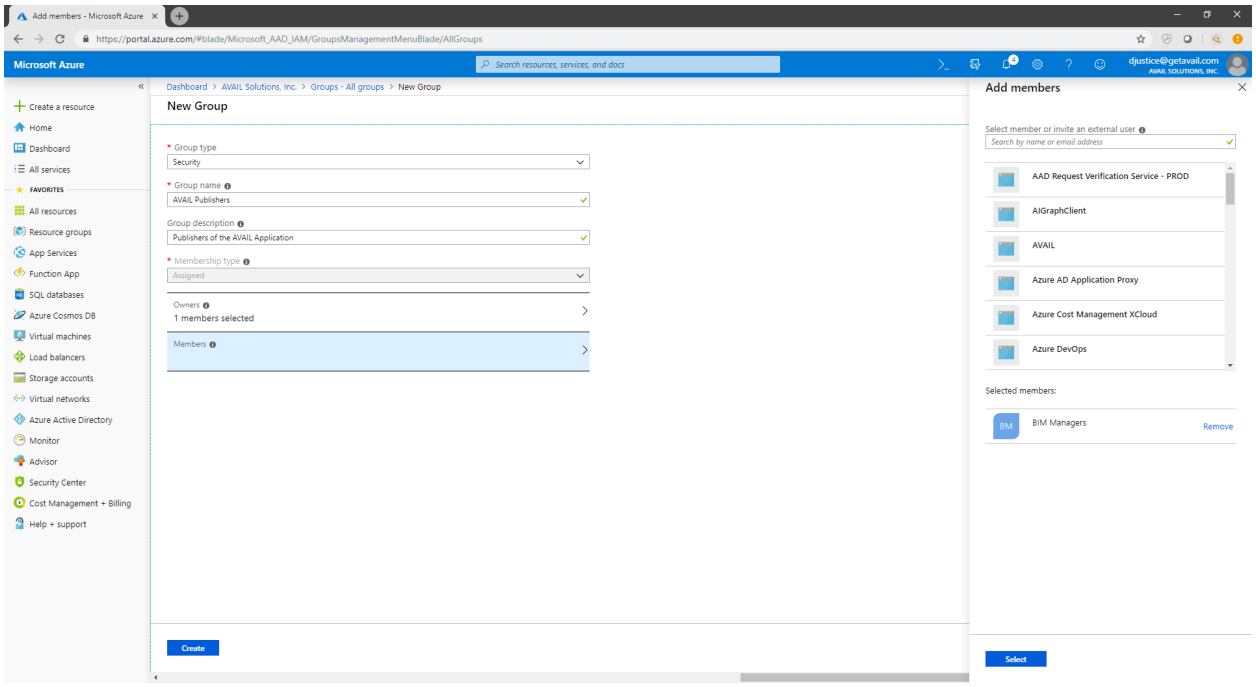
2. Click the **+ New group** option.



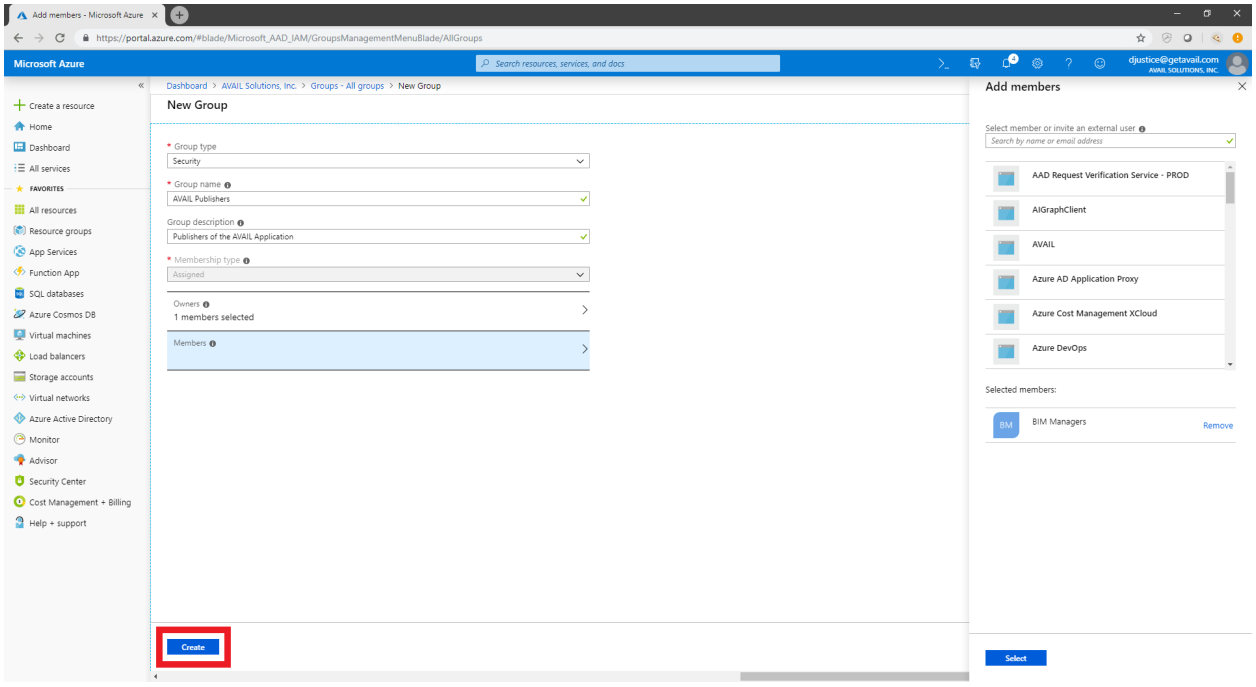
3. In the **New Group** form, enter in the following values:

Group type	Security
Group name	AVAIL Publishers
Group description	“Publishers of the AVAIL Application”
Membership type	Assigned

To add existing users and/or groups to the AVAIL Publishers group, select the **Members** option in the form. Once added, click the **Select** button.



4. Click the blue **Create** button to finish creating the group.



Submit Information to AVAIL

You have completed all the necessary steps for the registration of the AVAIL application in your Azure Active Directory Portal. In this section, you will need to share some information with AVAIL regarding the application registration that you have just completed.

There are five values associated with your Azure Active Directory and the AVAIL registered application that you will need to submit: Tenant ID, Application ID, Object ID, SAML-P Sign-On Endpoint and the Publisher Group Object ID. If you need assistance in locating these values, the sections in this chapter will guide you.

Please fill in the information located in the form linked below. Once you have submitted the form, await confirmation from a member of the AVAIL Support team before continuing to the Installing AVAIL chapter of this instruction document.

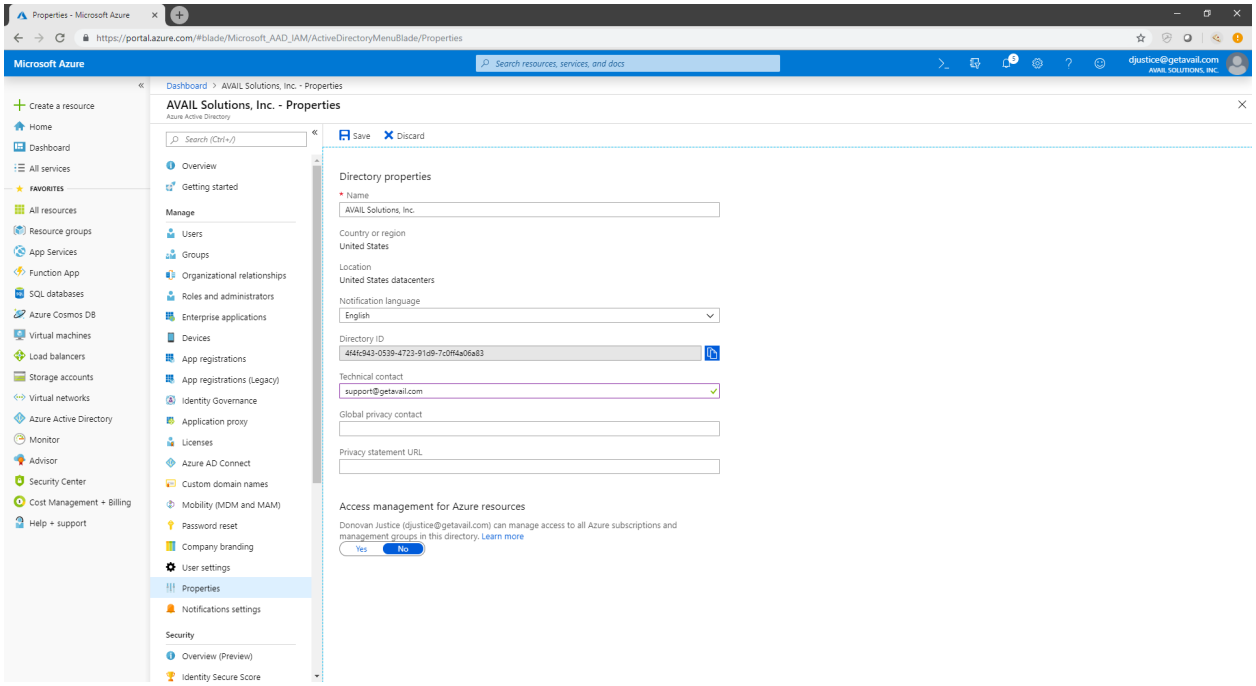
Azure Active Directory Information Form

Tenant ID

To locate the **Tenant ID** of your Active Directory:

1. Select **Azure Active Directory** from the main navigation menu
2. Select the **Properties** option from the menu in the second column.
3. In the Properties area, copy the **Tenant ID** that is listed by clicking the blue copy button and paste it into the form.

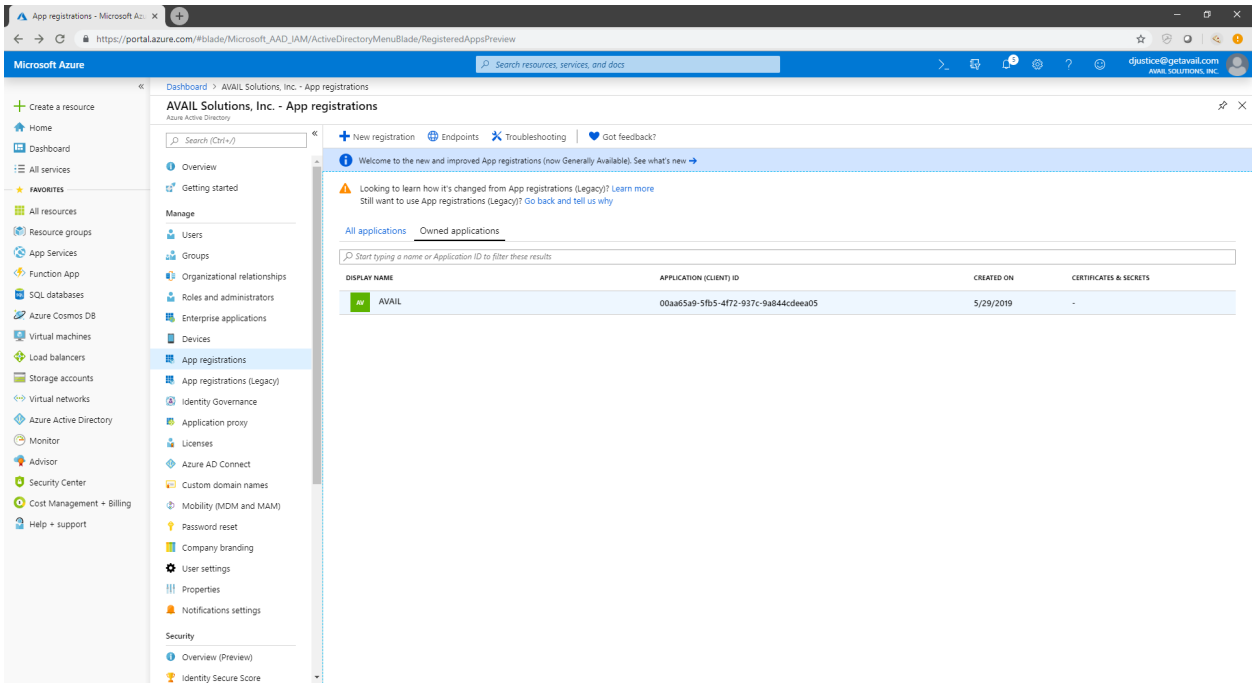
   Note: Directory ID (pictured below) is now called Tenant ID



Application ID

To locate the **Application ID** of the AVAIL application:

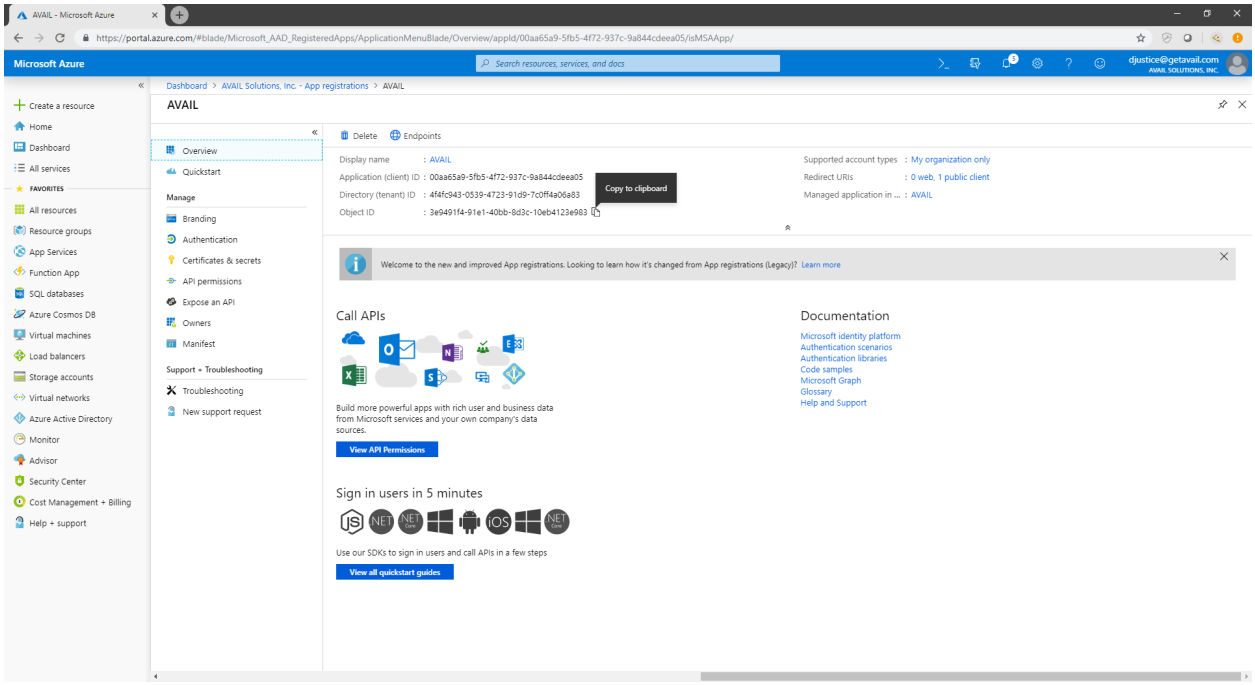
1. Select **App Registrations** in the left navigation menu
2. Select the **AVAIL** application row to display the properties slideout region on the right.
3. In the application slide out region, copy the value of the Application ID listed and paste it into the form.
    - Note: Remain in this view for the Object ID.



Object ID

To locate the **Object ID** of the AVAIL application:

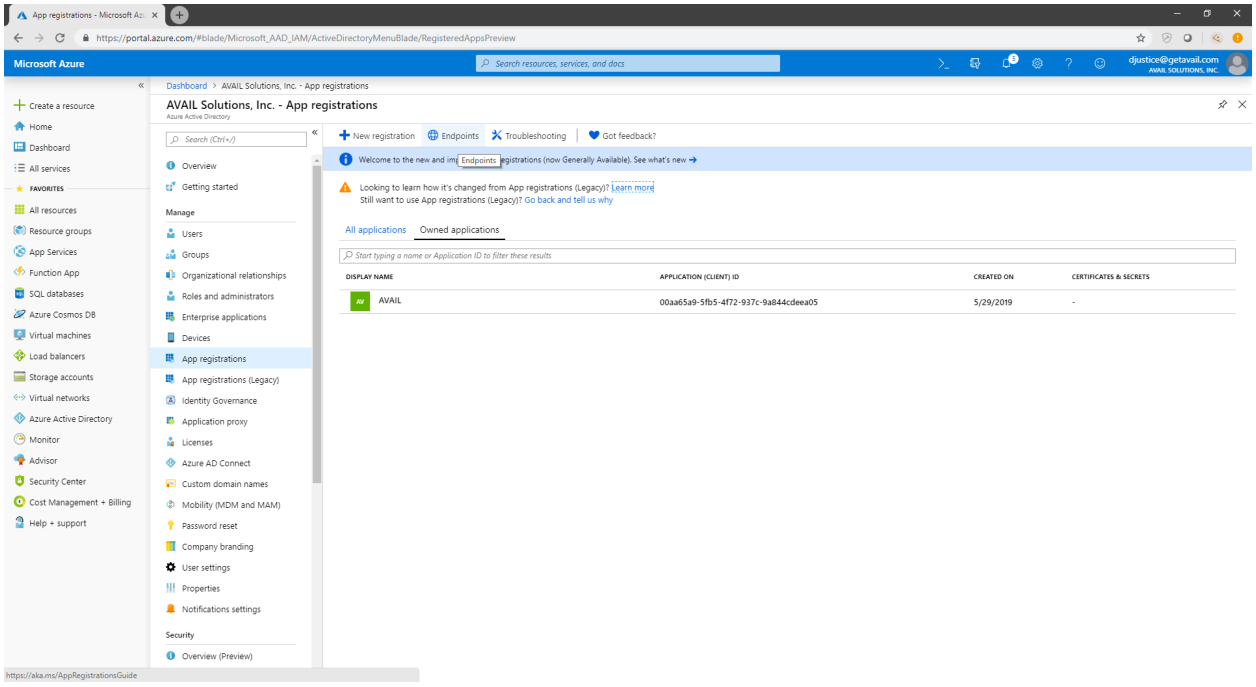
1. Select **App Registrations** in the left navigation menu.
2. Select the **AVAIL** application row to display the properties slideout region on the right.
3. In the application slide out region, copy the value of the Application ID listed and paste it into the form.



SAML-P Sign-On Endpoint

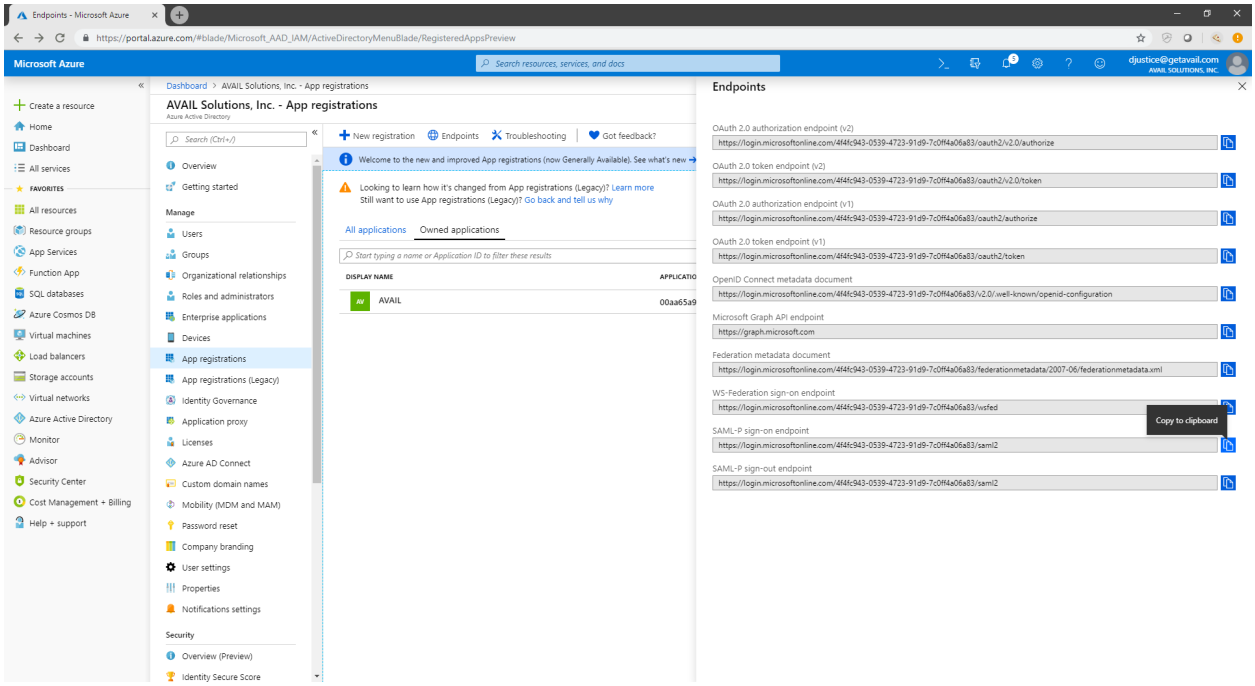
To locate the **SAML-P Sign-On Endpoint**:

1. Select **App Registrations** in the left navigation menu.
2. Select the **Endpoints** button located at the top of the application list. A slideout region will display on the right listing available endpoints.



(continued on next page)

3. Click the blue copy button to copy the **SAML-P SIGN-ON ENDPOINT** value and paste it into the [form].

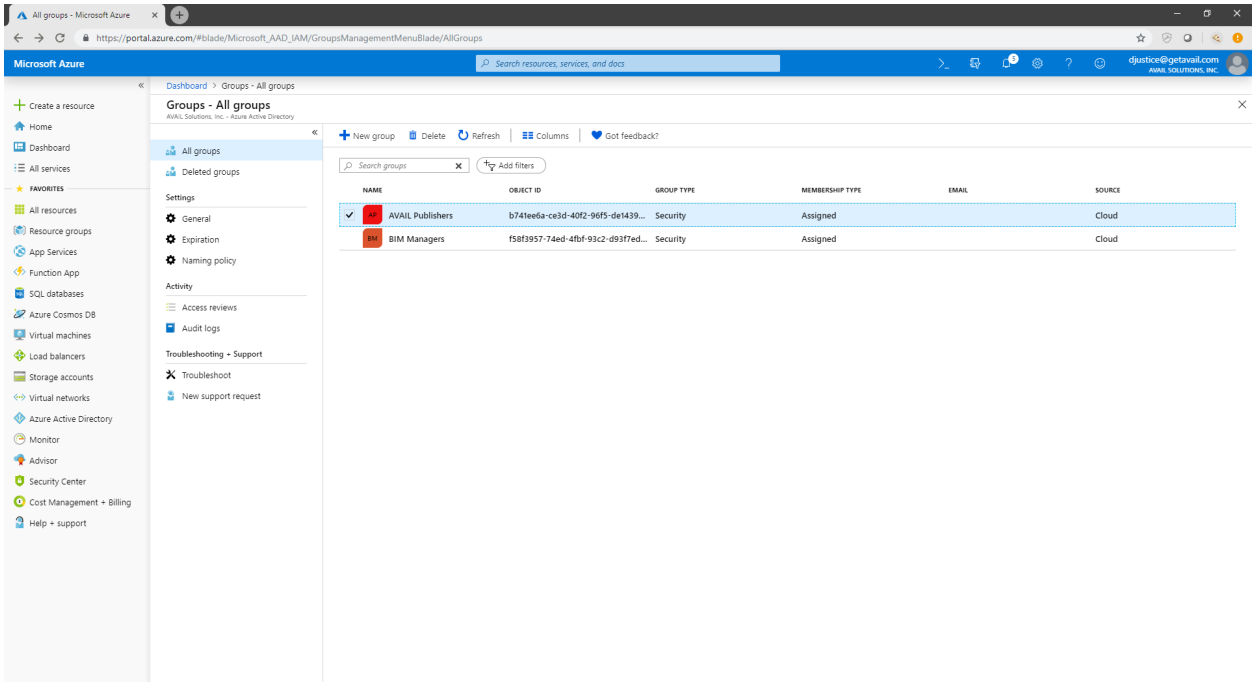


Publisher Group Object ID

The **Publisher Group Object ID** is the identifier of the Active Directory group that will be used by AVAIL's web services to determine if a user within your plan has publishing privileges. If you have not created or determined what group will be the AVAIL Publisher group, please read the AD Group Memberships & the AVAIL Publisher Role section in this document.

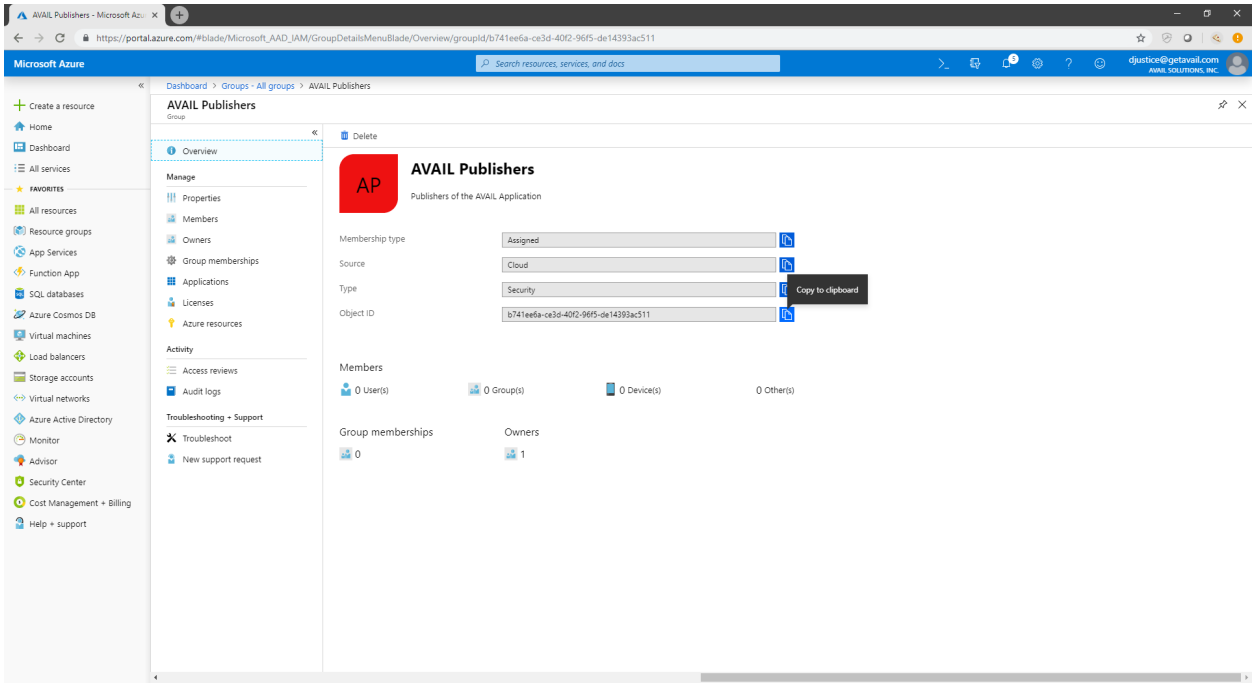
To access the **Object ID** of the Publisher Group:

1. Click the **Azure Active Directory** menu option in the left navigation menu
2. Select the **Groups** option in the second column. A list of groups will be listed in the main region of the portal.
3. Select the **AVAIL Publishers** group in the list to view the group's properties.



(continued on next page)

4. Highlight the **Object ID** of this group, then copy and paste it into the form.



Installing AVAIL

NOTE: Before continuing this section, you must provide AVAIL with the necessary values prior to deploying the AVAIL application across your organization. Please fill in the values in the form located in the Submit Information to AVAIL section.

Once you have completed the form, please wait for confirmation from the AVAIL Support team before continuing this instruction document.

Overview

Once you have supplied the necessary values to AVAIL and have received confirmation, you will need to inform your assigned AVAIL Support team member your preferred method of installation: .msi (MSI Installation) or .exe (EXE Installation). Prior to installing AVAIL on your user's workstations, you will need to configure your software deployment process to include specific installer switches.

During installation, the switches defined in the sections of this chapter will create a special configuration file titled **ADFS.config** on each workstation. This file is critical for providing the AVAIL desktop application with special values for authenticating users through your Active Directory. You will need the values for the **Application ID** and the **SAML-P Sign-On Endpoint** that you found earlier in the Submit Information to AVAIL chapter.

It is highly recommended that you first perform a test installation with the defined installer switches prior to deploying AVAIL. In the sections below, there are examples provided which will show you how to install via command line.

EXE Installation

AVAILInstaller.exe

This file packages the AVAIL Desktop application, the AVAIL Sync Service and SQL LocalDB into a single installer. The switches below are the values written in the ADFS.config file upon installing AVAIL.

Switches

- DisableUpdates=1
- ActiveDirectory=1
- ActiveDirectoryVersion="ADFS3"
- ActiveDirectoryAuthority="**[Your SAML-P Sign-On Endpoint]**"
- ActiveDirectoryRealm=”**[Application ID]**”
- ActiveDirectoryClientId=”**[Application ID]**”
- ActiveDirectoryRedirectUri="https://getavail.com"

Example

```
C:\>"C:\AvailInstaller.exe" /i /quiet /norestart DisableUpdates=1 ActiveDirectory=1
ActiveDirectoryVersion="ADFS3"
ActiveDirectoryAuthority="https://login.microsoftonline.com/4c5bf2ea-7b9d-4fff-ab3a
-5182900cab07/saml2" ActiveDirectoryRealm="42fc3910-509f-4b8f-b023-b417a855c526"
ActiveDirectoryClientId="42fc3910-509f-4b8f-b023-b417a855c526"
ActiveDirectoryRedirectUri="https://getavail.com"
```

MSI Installation

In order to properly install the AVAIL application via MSI installation, you will need to deploy one .exe installer and two .msi installers in the following order:

1. *vc_redist.x64.exe (optional, see below)*
2. *AvailSyncService.msi*
3. *Avail.msi*

1. vc_redist.x64.exe

The *vc_redist.x64.exe* file is the Microsoft Visual C++ 2015 Redistributable (x64) and installs run-time components of Visual C++ libraries. These components are required to run C++ applications that are developed using Visual Studio 2015 Update 3 RC and link dynamically to Visual C++ libraries.

Note that many modern applications, such as Autodesk Revit® 2018 (or greater), also require the Microsoft Visual C++ Redistributable package and a supported newer version may already be installed.

Switches

- `/i /quiet /norestart`

Example

```
C:\>"C:\vc_redist.x64.exe" /i /quiet /norestart
```

2. AvailSyncService.msi

The *AvailSyncService.msi* file installs a background service that manages syncing the content that is indexed into AVAIL.

Example

```
C:\>msiexec.exe /i "C:\AvailSyncService.msi" /qn
```

Continued on next page...

3. AVAIL.msi

The *Avail.msi* is the installer for the AVAIL Desktop application. The switches below are the values written in the ADFS.config file upon installing AVAIL.

Switches

- DISABLEUPDATES=1
- ACTIVEDIRECTORY=1
- AD_VERSION="ADFS3"
- AD_AUTHORITY="**[Your SAML-P Sign-On Endpoint]**"
- AD_REALM="**[Your Application ID]**"
- AD_CLIENT_ID="**[Your Application ID]**"
- AD_REDIRECT_URI="https://getavail.com"

Example

```
C:\>msiexec.exe /i "C:\Avail.msi" /quiet /norestart DISABLEUPDATES=1
ACTIVEDIRECTORY=1 AD_VERSION="ADFS3"
AD_AUTHORITY="https://login.microsoftonline.com/4c5bf2ea-7b9d-4fff-ab3a-5182900cab0
7/saml2" AD_REALM="42fc3910-509f-4b8f-b023-b417a855c526"
AD_CLIENT_ID="42fc3910-509f-4b8f-b023-b417a855c526"
AD_REDIRECT_URI="https://getavail.com"
```

The ADFS.config file

After installing with the switches defined (either msi or exe), a special configuration file titled **ADFS.config** will be created on each workstation. This file is located in the same install location as the AVAIL.exe application (`C:\Program Files\AVAIL`). This file is a crucial component for providing the AVAIL desktop application with special values for authenticating users via your Active Directory.

Example

A proper, Azure-based ADFS.config file should look something like this:

```
<adfsSettings>
    <add key="ActiveDirectoryVersion" value="ADFS3"/>
    <add key="ActiveDirectoryAuthority" value="[Your SAML-P Sign-on Endpoint]"/>
    <add key="ActiveDirectoryRealm" value="[Your Application ID]"/>
    <add key="ActiveDirectoryClientId" value="[Your Application ID]"/>
    <add key="ActiveDirectoryRedirectUri" value="https://getavail.com"/>
</adfsSettings>
```

Support

Have a question?
Email us at support@getavail.com
or call us at +1 859-963-1616

AVAIL Solutions, Inc.
163 East Main Street
3rd Floor
Lexington, KY 40507
USA

Website: www.getavail.com
Phone: +1 859-963-1616
Email: support@getavail.com