# CCASE Pexus

## Office 365 OAuth Configuration



## eCASE 11.2.0 Office 365 OAuth Configuration

#### Notice of Rights

Copyright © 2023, AINS, LLC d/b/a OPEXUS. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publisher: AINS, LLC. For information on obtaining permission for reprints and excerpts, contact info@opexustech.com.

Additionally, all copyrights, confidential information, patents, design rights and all other intellectual property rights of whatsoever nature contained herein are, and shall remain, the sole and exclusive property of the publisher.

### Notice of Liability

The information in this publication is believed to be accurate and reliable. However, the information is distributed by the publisher (AINS, LLC.) on an "As Is" basis without warranty for its use, or for any infringements of patents or other rights of third parties resulting from its use.

While every precaution has been taken in the preparation of this publication, neither the author (or authors) nor the publisher will have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused, directly or indirectly, by the information contained in this publication or by the computer software and hardware products described in it.

### Notice of Trademarks

The publisher's company name, company logo, company patents, and company proprietary products are trademarks or registered trademarks of the publisher: AINS, LLC. All other trademarks or registered trademarks are the property of their respective owners.

#### Non-Disclosure Statement

This document's contents are confidential and proprietary to AINS, LLC. This document cannot be released publicly or outside the purchasing agency without prior written permission from AINS, LLC.

Images in this manual are used as examples and may contain data and versioning that may not be consistent with your version of the application or information in your environment.

#### Additional Notice

Information in this documentation is subject to change without notice and does not represent a commitment on the part of AINS, LLC.

Notwithstanding any of the foregoing, if this document was produced as a Deliverable or other work for hire under a contract on behalf of a U.S. Government end user, the terms and conditions of that contract shall apply in the event of a conflict.

## Contents

1	Ab	out Office 365 OAuth Configuration	.4
	1.1	In This Manual	.4
	1.2	Prerequisites	.4
2	Re	gister Application	. 5
3	Cre	eate Client Secret	. 7
4	AP	I Permissions	. 9

## 1 About Office 365 OAuth Configuration

## 1.1 In This Manual

This manual contains steps to configure eCASE to integrate with OAuth for sending emails from a system account. The steps to complete this configuration take place in three parts:

- Register Application: Register your application through the Azure Portal.
- Create Client Secret: Using the Azure Portal, create a Client Secret you will use for OAuth configuration.
- API Permissions: Add appropriate API permissions to permit sending emails.

## 1.2 Prerequisites

The following are prerequisites for completing OAuth configuration:

- OAuth configuration should be completed by a system administrator with the appropriate knowledge and access to complete all required steps.
- Before beginning the configuration, you must create an Exchange mailbox in Office 365 (ex. noreply@opexustech.com). This email appears as the sender for all system messages from eCASE and is used to complete the configuration.

## 2 Register Application

The first step in OAuth configuration is to register your app. Follow the steps below to register the app in Azure:

- 1. Log in to portal.azure.com using the Exchange mailbox created as the eCASE system account.
- 2. Click **App Registrations > New Registration**. The Register an application screen appears:



- 3. Enter a (A) Name for the app in the field provided.
- 4. Under **(B)** Supported account types, the top option is selected by default. You may need to make a different selection depending on your organization's needs.
- 5. Under **(C)** Redirect URL, enter "<Application Admin URL>/connectors/SMTP.aspx" where <Application URL> is replaced with your application's admin URL.
- 6. Click **Register** to register the app.
- 7. The app is registered. The screen displays the **(A) Application (client) ID and (B) Directory (tenant) ID.** Copy both to your clipboard or otherwise save for later reference:

Home > App registrations > OAUTH Application	\$ <sup>2</sup> ····		×
₽ Search (Ctrl+/) «	🗐 Delete 🜐 Endpoints 💀 Preview features		
Overview	Got a second? We would love your feedback on Microsoft identity	y platform (previously Azure AD for developer). $ ightarrow$	
🗳 Quickstart			A
💉 Integration assistant	↑ Essentials		
Manage	Display name OAUTH Application	Client credentials Add a certificate or secret	
Branding & properties	Application (client) ID 94206c5b-35dc-48d4-980e-a14db1eafb45	Redirect URIs 1.web, 0.spa, 0. public client	
Authentication     Certificates & secrets	Object ID edf2ca10-7fff-4fde-a520-21fb070e7100	Application ID URI Add an Application ID URI	
Token configuration	Directory (tenant) ID 2e6c73c6-1977-4164-8037-33ca7fa29664	Managed application in local directory OAUTH Application	
API permissions     Expose an API	Supported account types My organization only		_

8. Access eCASE Administration (eCASE > Settings > Connectors > eMail (SMTP)). The configuration screen appears as shown below:

<mark>J S</mark> ave   <mark>◎ C</mark> lose		Note: * fields are mandatory when enabled
Enable/Disable:		
Authentication Mode: *	OAuth 🗸	
User Name: *		
OAuth Client ID: *		
Public Key (secret):		
Tenant ID:		
Use SSL:	No V	
Recipient Limit:	0	

- 9. Under (A) OAuth Client ID, enter the Application (client) ID from step 7.
- 10. Under (B) Tenant ID, enter the Directory (tenant) ID from step 7.
- 11. In the *User Name* field, enter the email address being used as the system account for this configuration (ex. noreply@ains.com).
- 12. Click **Save** to save the changes.

## **3** Create Client Secret

Next, you'll follow the steps below to create a new Client Secret:

- 1. Within the Azure Portal, access your application, then access the *Certificates* & *Secrets* screen.
- 2. Click New Client Secret:

Home > App registrations > OAUTH Ap	plication				
💡 OAUTH Application	Certificates & secrets	¢			×
$\red{rescale}$ cer $ imes$ «	🖗 Got feedback?				
Manage	Credentials enable confidential applications to	o identify themselve	s to the authentication service when receivi	ng tokens at a web addressable location (us	sina
📍 Certificates & secrets	an HTTPS scheme). For a higher level of assur	ance, we recommen	d using a certificate (instead of a client secr	et) as a credential.	
					× Ising
	Application registration certificates, secret	ts and federated crede	entials can be found in the tabs below.		×
	Certificates (0) Client secrets (0) F	ederated credentia	ls (0)		
	A secret string that the application uses to p	prove its identity whe	n requesting a token. Also can be referred	o as application password.	
<	+ New client secret				
	Description	Expires	Value 🛈	Secret ID	
	No client secrets have been created for this	application.			

3. The *Add a client secret* screen appears. First enter a *Description* in the field provided. This is an internal description that is visible only to Admin users:

Add a client secret		$\times$
Description	Enter a description for this client secret	
Expires	Recommended: 6 months	$\sim$
Add Cancel		

4. Use the *Expires* field to determine an expiration date based on your organization's preference (with a 24-month maximum).

(!!) Note: Take a note of this expiration date, as this Client Secret will need to be renewed prior to the expiration for continuous operation.

- 5. Click **Add** to generate the Client Secret.
- 6. The Client Secret is successfully generated, and the secret appears as shown in the example below:

#### Create Client Secret

Application registration certificates, secrets and	federated credentials o	an be found in the tabs below.		>	¢
Certificates (0) Client secrets (1) Federa A secret string that the application uses to prove i	ted credentials (0) ts identity when requ	esting a token. Also can be referred to as applica	tion password.		
+ New client secret					
Description	Expires	Value 🛈	Secret ID		
New client secret	2/18/2023	hoZ8Q~tKQUtNjHsFMsUp4GX0.uK~Odz 🗈	f627ab0e-4bb8-4894-92df-92f09f168577	D [	Ì

(!!) Note: Save the "Value" as this cannot be retrieved. You will need this to complete the configuration.

- 7. Copy the *Value* field to your clipboard.
- 8. Access eCASE Administration (eCASE > Settings > Connectors > eMail (SMTP)).
- 9. Copy the value obtained in step 7 into the Public Key (secret) field:

🛃 <u>S</u> ave   🙆 <u>C</u> lose		Note: * fields are mandatory when enabled
Enable/Disable:		
Authentication Mode: *	OAuth 🗸	
User Name: *		
OAuth Client ID: *		
Public Key (secret):		
Tenant ID:		
Use SSL:	No V	
Recipient Limit:	0	

10. Click **Save** to save the changes.

## 4 API Permissions

The final step to enable OAuth is configuring API permissions:

1. Open the Azure Portal and access your application page, then click API permissions:



- 2. From the API Permissions screen click Add a Permission.
- 3. The Request API Permissions screen appears. Click Microsoft Graph:

#### **Request API permissions**



4. Next click Application Permissions.

0	Σ	Ŗ	Q		?	<u>কি</u>	QAOffice365@ainsinc.o AINS, INC (FOIAEXPRESS.COM)
Request API permissions							×
<ul> <li>✓ All APIs</li> <li>Microsoft Graph https://graph.microsoft.com/ Docs ♂<sup>3</sup></li> <li>What type of permissions does your application require?</li> </ul>							
Delegated permissions Your application needs to access the API as the signed-in user.		Applic Your a signed	ation p pplicati I-in use	ermissi on runs r.	ons as a ba	ckground	d service or daemon without a

- 5. In the Select Permissions field, type "mail".
- 6. Locate and expand the Mail permissions, then select Mail.Send:

		agree moren	
lect	permissions		expand all
ma	il		×
P	ermission	Admin consent requ	ired
> м	lailboxSettings		
/ M	lail (1)		
	Mail.Read ① Read mail in all mailboxes	Ves	
	Mail.ReadBasic ① Read basic mail in all mailboxes	Ves	
	Mail.ReadBasic.All ① Read basic mail in all mailboxes	Yes	
	Mail.ReadWrite ① Read and write mail in all mailboxes	Yes	
/	Mail.Send ① Send mail as any user	Ves	

- 7. Click Add Permissions to apply the selected permission.
- 8. The Administrator must grant these permissions. The Admin receives a notification to grant the requested permission and, once this permission is granted, the mailbox can send mail from the system account.

Add permissions Discard