

FOIAXpress

Telemesssage Integration

v11.8.0

September 2024



OPEXUSTECH.COM

© AINS LLC, 2024

FOIAExpress v11.8.0 TeleMessage Integration

Notice of Rights

Copyright © 2024, OPEXUS, 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: OPEXUS, 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 (OPEXUS, 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: OPEXUS, 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 OPEXUS, LLC. This document cannot be released publicly or outside the purchasing agency without prior written permission from OPEXUS, 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 OPEXUS, 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 About TeleMessage Integration 4
- 2 TeleMessage Integration Prerequisites 5
 - 2.1 Upgrade FOIAXpress 5
 - 2.2 Set Up MMA in Azure 5
 - 2.3 Upgrade Application License 13
- 3 TeleMessage Integration Configuration 15



1 About TeleMessage Integration

Users must configure their application settings prior to integrating FOIAXpress with TeleMessage. This manual outlines the requirements and steps for configuring FOIAXpress for TeleMessage integration.



2 TeleMessage Integration Prerequisites

Complete the following steps to ensure your FOIAXpress application is ready to be configured for TeleMessage integration. Once these prerequisites are met, you can set configurations within the application to enable the TeleMessage integration.

2.1 Upgrade FOIAXpress

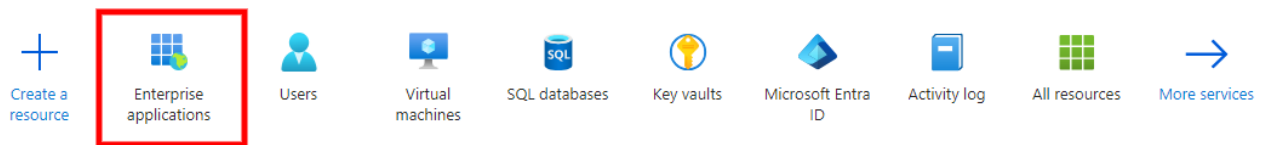
If you are not on FOIAXpress version 11.5.0 or higher, upgrade the application first. Follow the steps in the FOIAXpress Deployment Manual to upgrade your application.

2.2 Set Up MMA in Azure

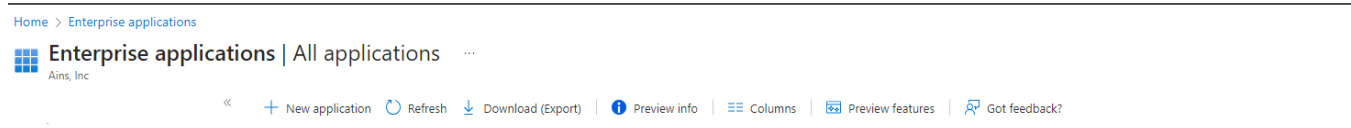
Follow the steps below to set up a Mobile Message Archive in Azure:

1. Select Enterprise application

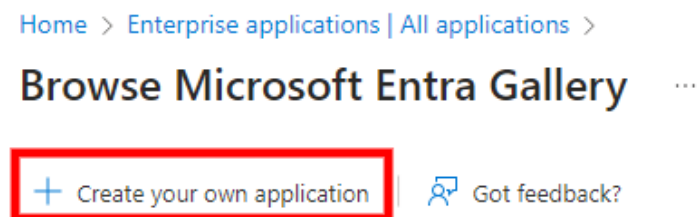
Azure services



2. Click + New application to create a new application




3. Select + Create your own application:



4. Provide a name and select the *Register an application to integrate with Microsoft Entra ID* option (selected in the following example):



Create your own application ✕

 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

MMA_DEMO ✓

What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☒ Register an application to integrate with Microsoft Entra ID (App you're developing)
- ☐ Integrate any other application you don't find in the gallery (Non-gallery)

5. Under *Supported Account Types*, select the **Accounts in this organizational directory only (Single Tenant)** option:

Register an application ...

* Name

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

MMA_DEMO ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Ains, Inc only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

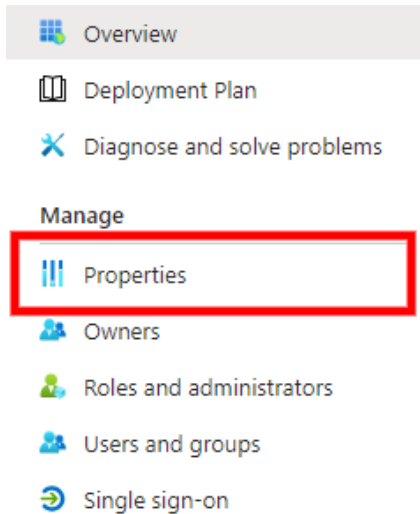
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform ▼ e.g. https://example.com/auth

6. Create the application.
7. After creating the application, click on **Properties**:

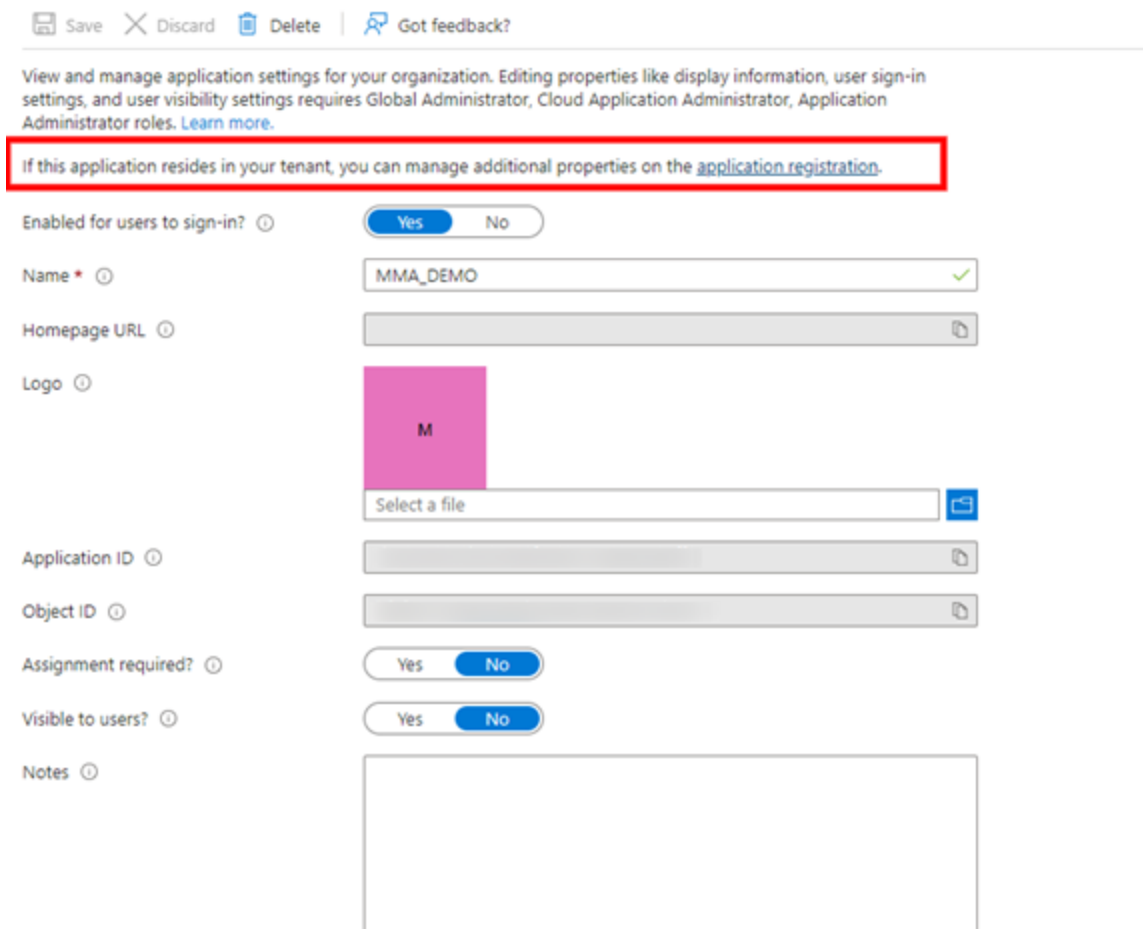


Introduction



- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage**
 - Properties**
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on

8. Click on **Additional Properties**:



Save Discard Delete Got feedback?

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional properties on the [application registration](#).

Enabled for users to sign-in? ☒ Yes ☐ No

Name * MMA_DEMO ✓

Homepage URL

Logo

M

Select a file

Application ID

Object ID

Assignment required? ☐ Yes ☒ No

Visible to users? ☐ Yes ☒ No

Notes

9. Select **Overview**:



Introduction

MMA_DEMO | Branding & properties

Search

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Name * MMA_DEMO

Logo

None provided

Upload new logo

Select a file

Home page URL

e.g. https://example.com

Terms of service URL

e.g. https://example.com/termsofservice

Privacy statement URL

e.g. https://example.com/privacystatement

Service management reference

Internal notes

Add information relevant to the management of this application.

Publisher domain

foiaexpress.com

Update domain

This domain will appear on the application's consent screen. [Learn more about publisher domain](#)

Publisher verification

Associate a verified Microsoft Partner Center (MPN) account with your application. A verified badge will appear in various places, including the application consent screen. [Learn more](#)

MPN ID

[Add MPN ID to verify publisher](#)

Publisher display name

Not provided

Save Discard

10. Record the Client ID and the Tenant ID (these are required during TeleMessage Integration Configuration):

Essentials

Display name : MMA_DEMO

Application (client) ID : [REDACTED]

Object ID : [REDACTED]

Directory (tenant) ID : [REDACTED]

Supported account types : My organization only

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [Add a Redirect URI](#)

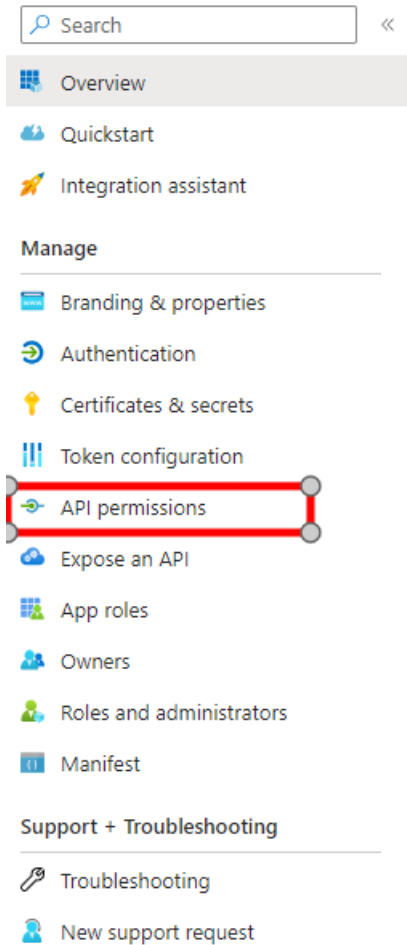
Application ID URI : [Add an Application ID URI](#)

Managed application in l... : MMA_DEMO

11. Go to API Permissions:



Introduction



12. Click **Add a permission**:

⚠ Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#) ×

ℹ The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#) ×

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)


+ Add a permission ✓ Grant admin consent for Ains, Inc

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

13. Search for and select **Microsoft Graph**:





Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

14. Select Application permissions:

[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

15. Under *Mail*, add the **Mail.Read**, and **Mail.ReadBasic.All** permissions:

Permission	Admin consent required
MailboxSettings	
Mail (2)	
<input checked="" type="checkbox"/> Mail.Read ⓘ Read mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadBasic ⓘ Read basic mail in all mailboxes	Yes
<input checked="" type="checkbox"/> Mail.ReadBasic.All ⓘ Read basic mail in all mailboxes	Yes
<input type="checkbox"/> Mail.ReadWrite ⓘ Read and write mail in all mailboxes	Yes
<input type="checkbox"/> Mail.Send ⓘ Send mail as any user	Yes

16. Under *User*, select the **User.Read.All** and **User.ReadBasic.All** permissions as shown below:



Introduction

User (2)		
<input type="checkbox"/>	User.EnableDisableAccount.All ⓘ Enable and disable user accounts	Yes
<input type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage all users' identities	Yes
<input checked="" type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input checked="" type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	Yes
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

17. Click on **Grant admin consent for your account**:

Configured permissions

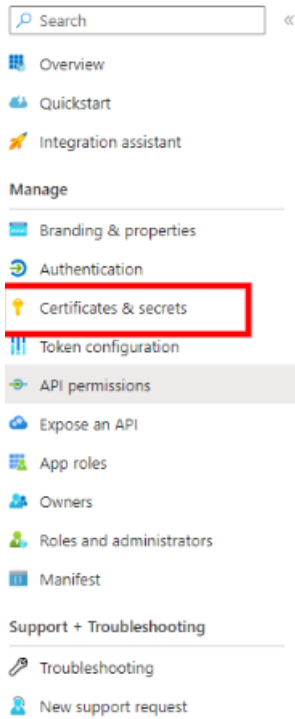
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission		<input checked="" type="checkbox"/> Grant admin consent for Ains, Inc		
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (4) ***				
Mail.Read	Application	Read mail in all mailboxes	Yes	⚠ Not granted for Ains, Inc ***
Mail.ReadBasic.All	Application	Read basic mail in all mailboxes	Yes	⚠ Not granted for Ains, Inc ***
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Ains, Inc ***
User.ReadBasic.All	Application	Read all users' basic profiles	Yes	⚠ Not granted for Ains, Inc ***

18. Click on **Certificates & secrets**:



Introduction



19. Click + New client secret to create a new secret:

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value	Secret ID
-------------	---------	-------	-----------

No client secrets have been created for this application.

20. Add a *Description* and set an *Expires* duration:

Add a client secret

Description	<input type="text" value="TOKEN"/>
Expires	<input type="text" value="Recommended: 180 days (6 months)"/>



21. Copy the *Value* and store it securely.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
TOKEN	10/13/2024	[Redacted]	[Redacted]

With the information gathered from this list, go to the FOIA Application and provide the saved values.

2.3 Upgrade Application License

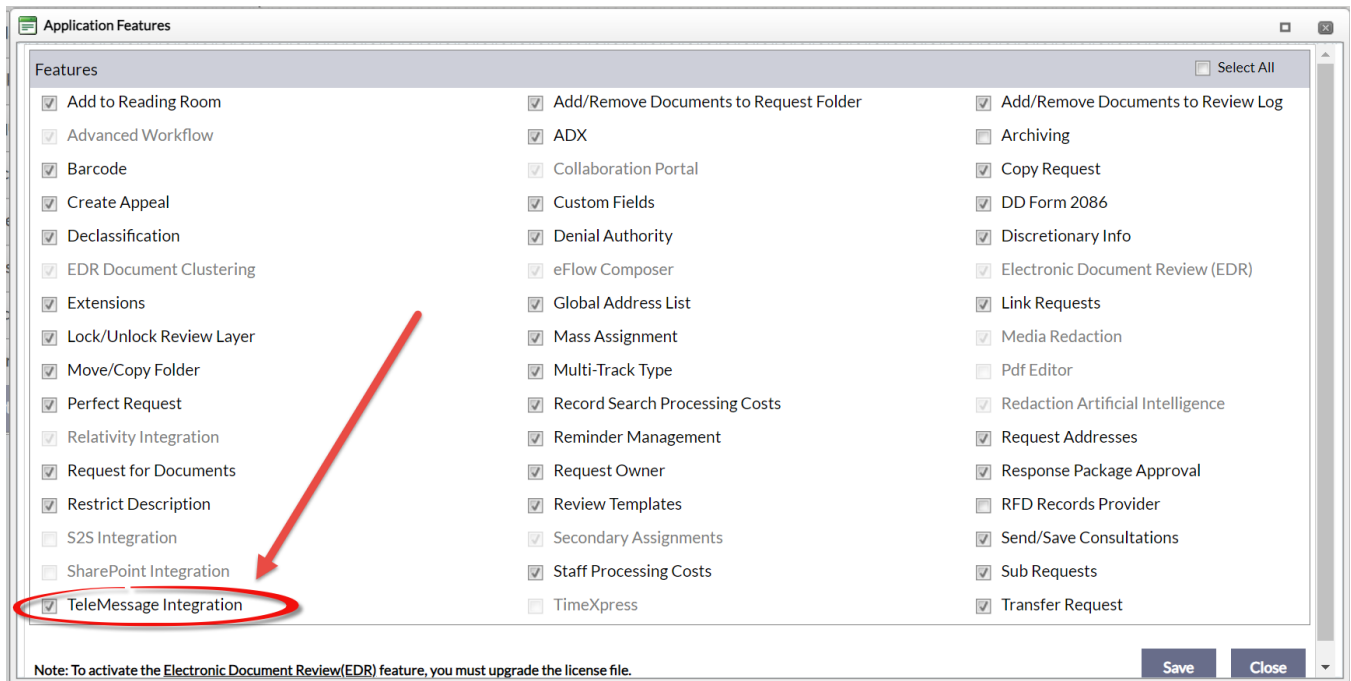
1. Upgrade the application license in the *Administration* settings.

Note: The TeleMessage feature is tied to your application license, and the feature is automatically enabled with the appropriate license. Please upgrade your license to include the TeleMessage integration.

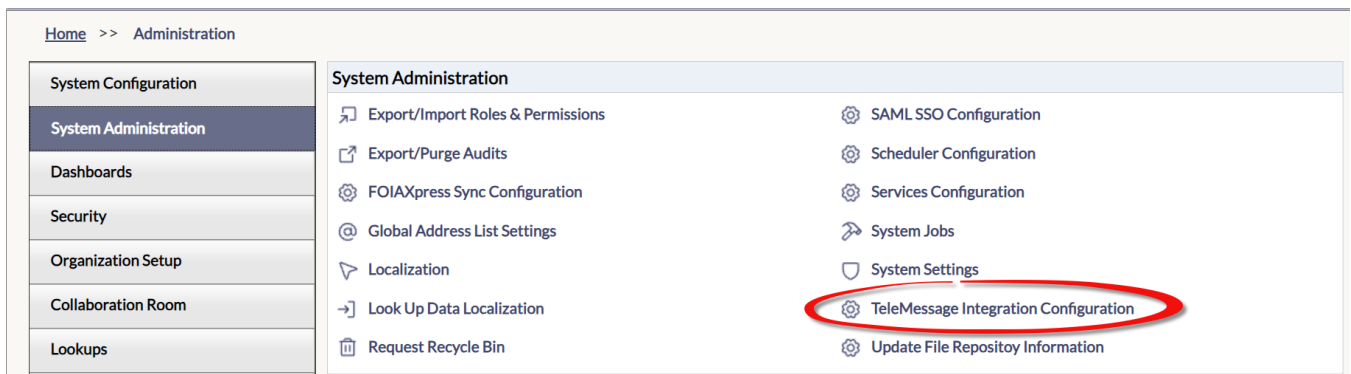
2. Ensure that the TeleMessage integration is enabled in the *Application Features* menu (**Administration > Features and Licenses > Application Features**). It should be enabled automatically after upgrading your license. If not enabled after upgrading your license, select the **TeleMessage Integration** checkbox and save the configuration:



Introduction



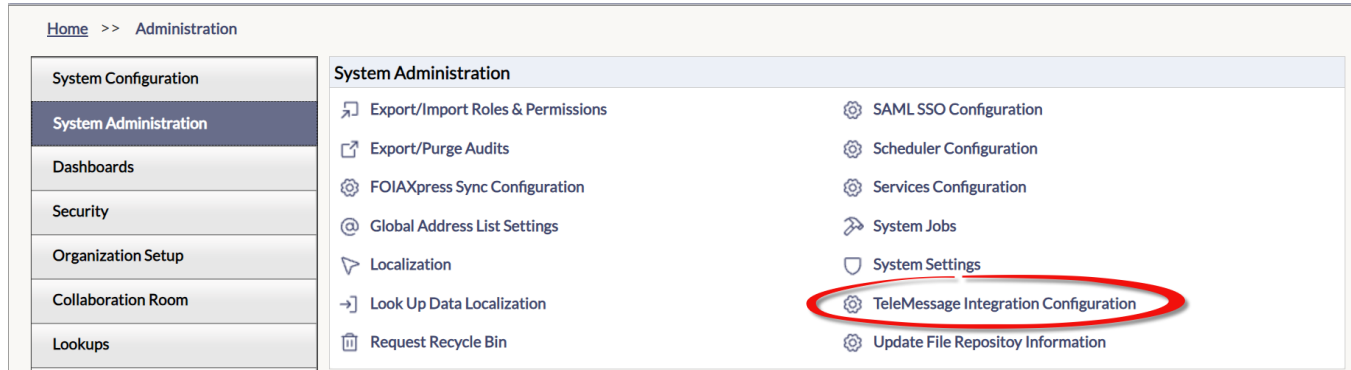
3. The *TeleMessage Integration Configuration* menu should be visible when accessing **Administration > System Administration**. If the menu is not visible, log out of the application and log back in.



3 TeleMessage Integration Configuration

Follow the steps below to configure the TeleMessage integration:

1. Navigate to the *TeleMessage Integration Configuration* menu (**Administration > System Configuration > TeleMessage Integration Configuration**):



2. The *TeleMessage Integration Configuration* screen appears as shown below. Use these fields to configure the integration. They are described in the following table.

(!!) Note: Please consult with OPEXUS support to obtain the correct values for these fields, based on your specific environment and integration.

A screenshot of a web form titled 'TeleMessage Integration Configuration'. The form has a header 'Azure App Configuration' and contains five input fields: 'Client Id', 'Secret Key Value', 'Email', 'Tenant Id', and 'MailBox'. The 'MailBox' field has the value 'Inbox' entered. At the bottom right of the form are two buttons: 'Save' and 'Cancel'.

Field	Description
Client Id	<p>The Client Id (or Application ID) represents the application's identity in the directory. When the application interacts with Azure services or APIs, it presents this ID as part of the authentication process to prove its identity.</p> <p>This value is recorded at step 10 of section 2.2, <i>Set Up MMA in Azure</i>.</p>
Secret Key Value	<p>A credential, often a string value, generated for an application to authenticate itself against Azure services. This key is paired with the Client ID to authenticate the application. It's like a password and is used as part of the authentication flow to ensure that only the application with the correct credentials can access protected resources.</p> <p>This value is recorded at step 21 of section 2.2, <i>Set Up MMA in Azure</i>.</p>
Email	Represents a Microsoft Entra user account used for this integration.
Tenant Id	<p>The identifier of the Azure AD tenant where the application and its related resources (like users, groups, and applications) are registered. Azure AD tenants are unique environments created by organizations to manage and secure access to their resources. The Tenant Id is used to specify which Azure AD tenant the application is associated with.</p> <p>This value is recorded at step 10 of section 2.2, <i>Set Up MMA in Azure</i>.</p>
MailBox	The location where your emails, contacts, calendar events, tasks, and other personal information are stored.

- After configuring these fields, click **Save** to save the settings.
- Once your integration is configured, your users will be able to search the TeleMessage Mobile Message Archive using the **Add Documents drop down** and selecting **Mobile Message Archive**.

