Table of Contents

1 Introduction .................................................................5
   1.1 System Components ..................................................5
       1.1.1 Repstor Mobile Outlook Add-In ................................5
       1.1.2 Repstor Mobile Web .............................................6
       1.1.3 Repstor Mobile – Filing Engine ................................6
       1.1.4 Repstor Mobile – Maintenance Functions ....................6
   1.2 Configuration Settings for On-Premise Repstor Mobile ..........6
       1.2.1 Mobile Web App ..................................................6
       1.2.2 Filing Engine Function App ......................................6
       1.2.3 Maintenance Function App .......................................7
       1.2.4 Key Vault Configuration Secrets ..............................7
   1.3 Installation requirements ............................................7

2 Azure Install Steps ........................................................9
   2.1 Create a Resource Group in Azure ...................................9
   2.2 Create the Web Application for the Repstor Mobile App .........10
       2.2.1 Create the Web App ..............................................10
       2.2.2 Set Application Insights .........................................11
       2.2.3 Enable Managed Identity .........................................12
       2.2.4 Deploy the App ....................................................12
   2.3 Create the Function Application for Repstor Mobile App .......15
       2.3.1 Create the Function App .........................................15
       2.3.2 Enable Managed Identity .........................................17
       2.3.3 Deploy the App ....................................................18
       2.3.4 Set the Function App URL ........................................20
   2.4 Create the Maintenance Function App for Repstor Mobile .......21
       2.4.1 To Create the Maintenance Function App ....................21
       2.4.2 Enable Managed Identity .........................................23
       2.4.3 Deploy the Maintenance App ....................................24
   2.5 Register the Repstor Mobile App in Azure AD ....................26
       2.5.1 To Create the App Registration ................................26
       2.5.2 Set Permissions for the App .....................................27
       2.5.3 Set the App Keys ..................................................30
       2.5.4 Add Redirect URIs ...............................................31
   2.6 Create SQL Database ..................................................32
       2.6.1 Create the SQL Database ........................................32
       2.6.2 Add your IP address in the firewall setting ...................33
       2.6.3 Connect to the SQL Server DB ...................................33
       2.6.4 Create the Database tables and indexes .......................34
       2.6.5 Insert the Configuration data ....................................34
       2.6.6 Create the Login Account .......................................35
       2.6.7 Configure the Database Connection string ...................35
   2.7 Create the Key Vault Resource .......................................35
2.7.1 Retrieve the Key Vault URL value ........................................................................37
2.8 Create the Sessions Key Vault Resource .....................................................................38
  2.8.1 Retrieve the Key Vault URL value .........................................................................39
2.9 Create the SendGrid API ..........................................................................................40
  2.9.1 Creating the SendGrid API ....................................................................................40
  2.9.2 Create the SendGrid API Key ................................................................................41
  2.9.3 Choose API Key Permissions ................................................................................41
2.10 Configuring the On-Premise Repstor Mobile .............................................................42
  2.10.1 Configure the Web App ......................................................................................42
  2.10.2 Configure the Function App ................................................................................43
  2.10.3 Configure the Maintenance Function App ..........................................................43
  2.10.4 Configure the Key Vault Secrets ........................................................................44
  2.10.5 Summary of Azure Objects ................................................................................44

3 Deployment .................................................................................................................45
  3.1 Granting permissions ...............................................................................................45
  3.2 Applying the App to Exchange ..............................................................................46
Introduction

Repstor Mobile is an Outlook Add-In to save emails to file storage. You can install Repstor Mobile on Azure and deploy mobile e-Filing within Exchange.

Currently Repstor Mobile supports the following file stores:

- SharePoint
- Box
- M-Files

Users can search for and find a location to save an email or attachment. Emails are uploaded as an “.eml” or “.msg” file. Email metadata is applied to the To, From and Subject fields of the uploaded file. Attachments are uploaded in the format that the user receives them.

1.1 System Components

The following image gives an overview of the components and the data flow between them.

1.1.1 Repstor Mobile Outlook Add-In

The Outlook add-in is supported with the following apps:

- Outlook iOS app
- Outlook Android app
- Outlook Web Application
- Outlook 2016 Windows
• Outlook for Mac

The Outlook add-in is a single page application, written in React.js and Office UI Fabric.

1.1.2 Repstor Mobile Web

Repstor Web Application is an ASP.NET application hosted on an Azure Application Service. The authenticated web application uses OAuth Flow 2. Repstor Web Application connects with Outlook Rest API, to the end users exchange mailbox, with delegated permissions only. As part of the Web Application, access tokens and other sensitive data are stored in the Azure Key Vault. A SQL Database is necessary to store non-sensitive configuration data.

1.1.3 Repstor Mobile – Filing Engine

The Filing Engine is a .NET application, this Application will run as an Azure Function Application. Functions are triggered by HTTP requests from Repstor Mobile Web. Authentication tokens are included in the inbound request body.

1.1.4 Repstor Mobile – Maintenance Functions

Maintenance Functions is a .NET application, this Application will run as an Azure Function Application. Functions are triggered by HTTP requests from Repstor Mobile Web. Authentication tokens are included in the inbound request body.

1.2 Configuration Settings for On-Premise Repstor Mobile

Note The following configuration settings will be captured and then configured during the installation process. The setting names are case sensitive

1.2.1 Mobile Web App

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td>Must be one of &quot;Production&quot;</td>
<td></td>
</tr>
<tr>
<td>KeyVaultUrl</td>
<td>URL for key vault</td>
<td>Retrieve the Key Vault URL value</td>
</tr>
</tbody>
</table>

1.2.2 Filing Engine Function App

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td>Must be one of &quot;Production&quot;</td>
<td></td>
</tr>
<tr>
<td>KeyVaultUrl</td>
<td>URL for key vault</td>
<td>Retrieve the Key Vault URL value</td>
</tr>
</tbody>
</table>
1.2.3 Maintenance Function App

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td>Must be one of &quot;Production&quot;</td>
<td></td>
</tr>
<tr>
<td>KeyVaultUrl</td>
<td>URL for key vault</td>
<td>Retrieve the Key Vault URL value</td>
</tr>
</tbody>
</table>

1.2.4 Key Vault Configuration Secrets

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppInsightsKey</td>
<td>Application Insights Instrumentation Key</td>
<td></td>
</tr>
<tr>
<td>ErrorEmailFromAddress</td>
<td>From address for error emails. For example, <a href="mailto:donotreply@repstor.com">donotreply@repstor.com</a></td>
<td></td>
</tr>
<tr>
<td>ExchangeAndShaRepointAppClientId</td>
<td>Application ID for Repstor Mobile App Registration</td>
<td>Set the App Keys</td>
</tr>
<tr>
<td>ExchangeAndShaRepointAppSecret</td>
<td>Secret for Repstor Mobile App Registration</td>
<td>Set the App Keys</td>
</tr>
<tr>
<td>FilingNotificationPostRequestUrl</td>
<td>Base URL for maintenance function.</td>
<td>https://[&lt;insert web app service url here&gt;]/api/MailboxSubscriptions/Notification e.g. <a href="https://repstormobilewebapp.azurewebsites.net/api/MailboxSubscriptions/Notification">https://repstormobilewebapp.azurewebsites.net/api/MailboxSubscriptions/Notification</a></td>
</tr>
<tr>
<td>FilingPostRequestBaseUrl</td>
<td>Base URL for filing engine. Will look like. <a href="https://repstormobilefunapp.azurewebsites.net">https://repstormobilefunapp.azurewebsites.net</a>. Can be found in the Function app overview. Set the Function App URL</td>
<td></td>
</tr>
<tr>
<td>SendGridApiKey</td>
<td>SendGrid API Key</td>
<td>Create the SendGrid API Key</td>
</tr>
<tr>
<td>SettingsDb</td>
<td>Connection string to the SQL Database. Configure the Database Connection string:</td>
<td></td>
</tr>
<tr>
<td>SessionsKeyVaultUrl</td>
<td>URL for the sessions key vault.</td>
<td></td>
</tr>
</tbody>
</table>

1.3 Installation requirements

The installation requires the following components:

1. An FTP Client installed to transfer application files to the Azure servers, e.g. Filezilla - https://filezilla-project.org/download.php

2. SQL Server Management Studio to create the DB schema and update tables.
3. Code files:
   a. FunctionApp.zip – code files for the Filing Engine App
   b. OutlookAddin.zip – code files for the Web App
   c. MaintenanceFunctionApp – code files for the Maintenance Function App
   d. SQL Scripts
      • 1.RepstorMobile-CreateDatabase.sql
      • 2.RepstorMobile-Configuration.sql
      • 3.RepstorMobile-Create Login.sql
      • 4.RepstorMobile-Create User.sql
   e. Addin manifest file
      • Onpremise.RepstorMobile.xml
Azure Install Steps

The following are the steps to install all the components into the Azure environment. The user must be logged on to the Azure portal [https://portal.azure.com](https://portal.azure.com)

### 2.1 Create a Resource Group in Azure

**Note** All the Azure components will run in this Resource Group.

1. In the left navigation menu, click on Resource groups.

2. Click [Add]. The **Create a resource group** pane appears.

3. In the **Basics** tab, enter a name for the **Resource group**. For example, **RepstorMobile**.

4. Select an appropriate **Region**.

5. Click **Review + Create**.

6. In the **Review + Create** tab, click **Create**.
2.2 Create the Web Application for the Repstor Mobile App

2.2.1 Create the Web App

1. In the Microsoft Azure portal, click Create a resource.

2. In the Search the Marketplace type Web App.

3. In the search results, select Web App.

4. In the Web App panel, click Create. The Web App panel appears.

5. In the Web App panel, complete the following:
f. In the Subscription list, click a type.
g. In the Resource Group list, click Use existing and select the resource group created in Create a Resource Group. For example, RepstorMobile.
h. In the Name box, types a name, for example, RepstorMobileWebApp.
i. In Publish, click Code.
j. In Runtime stack, select ASP.NET V4.7.
k. In Operating System, click Windows.
l. In Region, click the appropriate region.
m. In Windows Plan, click a suitable plan.
n. In Sku and size, enter an appropriate size.

6. Click Next Monitoring.

2.2.2 Set Application Insights

1. Select Application Insights. The Application Insights panel appears.

2. In Enable Application Insights, click Yes.

3. In the Application Insights list, click a suitable list item.

4. Create Tags if necessary. If not, click Review and create, and then click Create.

5. On the Web App panel, click Create. It may take a few seconds to complete the creation.

6. To retrieve the Applications Insights Instrumentation Key, click Application Insights – Overview.
7. Copy Instrumentation Key to ApplInsightsKey in the table Key Vault Configuration secrets.

2.2.3 Enable Managed Identity

1. In the left navigation pane, click App Services and select the newly created Web app. For example, RepstorMobileWebApp

2. Click Identity.

3. Change the status to On.

4. Click Save.

2.2.4 Deploy the App

**Note** FTP deployment is described for simplicity. However, deployment can be completed using Azure DevOps/Pipelines if preferred. Configuration of Azure Pipelines is outside the scope of this document.

1. Under Deployment, click on Deployment Center.
2. In the **Deployment Center** pane, select **FTP**, and then click **Dashboard**.

3. The Dashboard panel shows the FTP connection details to the site in order to copy files.
4. Unzip the contents of **OutlookAddln.zip**

5. Use an FTP client, for example, Filezilla, to copy the files to the `\site\wwwroot` on the server using the connection details supplied in the Dashboard panel.

**Note**  Copy the contents of the folder **OutlookAddln**: do not copy the folder itself.
2.3 Create the Function Application for Repstor Mobile App

2.3.1 Create the Function App

1. In the Azure portal, click Create a resource.

2. In the Search the Marketplace box, type Function App.

3. In the search results, select Function App.

4. In the Function App panel, click Create. The Function App panel appears.
5. In the **Function App** panel enter:
   - An **App name**, For example, RepstorMobileFunApp
   - A **Subscription**.
   - In the **Resource Group**, click **Use existing** and select the one created **here** RepstorMobile.
   - In **OS**, click **Windows**
   - A **Hosting plan**.
• A Location.
• In Runtime Stack, click .NET
• In Storage – select Create new and use the default.
• In Application Insights – select Enable

6. Click Create. It may take a few seconds to complete the creation.

### 2.3.2 Enable Managed Identity

1. In the Microsoft Azure portal, click App Services and select the function app. For example, RepstorMobileFunApp.

2. Click Platform features, then Identity.

3. Change the status to On.

4. Click Save.
2.3.3 Deploy the App

1. In the Microsoft Azure portal, click **App Services** and select the function app. For example, RepstorMobileFunApp.

2. Select the **Platform Features** tab and under **Code Deployment** select **Deployment Center**.

---

**Overview**

- **General Settings**
  - Function app settings
  - Application settings
  - Properties
  - Backups
  - All settings
- **Code Deployment**
  - Deployment Center
- **Development tools**
  - Logic Apps
  - Console (CIMD / PowerShell)
  - Advanced tools (Kudu)
  - App Service Editor
  - Resource Explorer
  - Site Extensions

**Platform features**

- **Networking**
  - Networking
  - SSL
  - Custom domains
  - Authentication / Authorization
  - Identity
  - Push notifications
- **Monitoring**
  - Diagnostic logs
  - Log streaming
  - Process explorer
  - Metrics
- **API**
  - API definition
  - CORS
- **App Service plan**
  - Scale up
  - Scale out
- **Quotas**
- **Resource management**
  - Diagnose and solve problems
  - Activity log
  - Access control (IAM)
  - Tags
  - Locks
  - Automation script
3. In the Deployment Center pane, select , and then click Dashboard.

4. The Dashboard panel shows the FTP connection details to the site in order to copy files.

5. Unzip the contents of ServerFilingEngine.zip

6. Use an FTP client, for example, Filezilla, to copy the files to the `site\wwwroot` on the server using the connection details supplied in the Dashboard panel.

   *Note* Copy the contents of the folder **FunctionApp**; do not copy the folder itself.
7. When the transfer is complete, refresh the App to confirm that 3 new functions are added to the App:

2.3.4 Set the Function App URL

1. Retrieve the Function App URL from the Overview tab.
2. Copy the URL to the `FilingPostRequestBaseUrl` value in the table the Key Vault Configuration Secrets.

### 2.4 Create the Maintenance Function App for Repstor Mobile

#### 2.4.1 To Create the Maintenance Function App

1. In the Azure portal, click **Create a resource**.

2. In the **Search the Marketplace** box, type **Function App**.

3. In the search results, select **Function App**.

4. In the **Function App** panel, click **Create**. The **Function App** panel appears.
5. In the **Function App** panel enter:
   - An **AppName**, For example, **RepstorMobileMaintenanceApp**, 
   - A **Subscription**
In Resource Group, select Use existing and select the one created here. For example, RepstorMobile

OS – leave as default Windows.

A Hosting plan

A Location

In Runtime Stack, click .NET

In Storage, click Create new and use the default.

In Application Insights – select Enable

6. Click Create. It may take a few seconds to complete the creation.

2.4.2 Enable Managed Identity

1. In the Microsoft Azure portal, click App Services and select the function app. For example, RepstorMobileMaintenanceApp.

2. Click Platform features, and then, click Identity.

3. Change the status to On.

4. Click Save.
2.4.3 Deploy the Maintenance App

1. In the left navigation pane, click on Function Apps and select the newly created function app. For example, RepstorMobileMaintenanceApp.

2. Select the Platform Features tab and under Code Deployment select Deployment center.

3. In the Deployment Center pane, select , and then click Dashboard.

4. The Dashboard panel shows the FTP connection details to the site in order to copy files.
5. Unzip the contents of MaintenanceFunctionApp.zip
6. Use an FTP client, for exam, Filezilla to copy the files to the \site\wwwroot on the server using the connection details supplied in the Dashboard panel.

**Note** Copy the contents of the folder MaintenanceFunctionAppFiles; do not copy the folder itself.
7. When all the transfer is complete, refresh the App to confirm that 2 new functions are added to the App:

![Function Apps](image)

2.5 Register the Repstor Mobile App in Azure AD

The following are the steps to register the Repstor Mobile in Azure AD. This gives the Repstor Mobile app access to retrieve email content from Office 365 Exchange Online.

2.5.1 To Create the App Registration

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

   ![Register an application](image)

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

   - **Supported account types**: Who can use this application or access this API?
     - Accounts in this organizational directory only (unrestricted)
     - Accounts in any organizational directory
     - Accounts in any organizational directory and personal Microsoft accounts

   - **Redirect URI (optional)**: We'll return the authentication response to this URI after successfully authenticating; it can be changed later, but a value is required for most authentication scenarios.

   ![Web](image)

2. In the Create panel in the Name box, type a name. For example, ReptorMobileApp.
3. In the Supported account types options, click **Accounts in this organizational directory only**.

4. Click **Register** to create the App Registration.

### 2.5.2 Set Permissions for the App

1. When the app is created, click **View API Permissions**

2. Click **Add a permission**

3. Under **Supported Legacy APIs**, click

4. Select **Delegated permissions** and expand **User**. Select the **User.Read** check box.
5. Click **Add permissions**.

6. Click **Add a permission**.

7. Under **Supported Legacy APIs**, click.

8. Select **Delegated permissions** and expand **Mail**. Select the **Mail.ReadWrite.Shared** check box.

9. Click **Add permissions**.
10. Click **Add a permission**.

11. Click **Microsoft Graph**.

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

12. Select **Delegated permissions** and expand **Mail**. Check **Mail.ReadWrite.Shared** and **Mail.ReadWrite**.

13. Click **Add permissions**.

14. Click **Add a permission**, click **Add permissions**.

15. Select **Delegated permissions**.
   - Expand **All Sites** and check **AllSites.Write**.
   - Expand **Sites** and check **Sites.SearchAll**.
   - Expand **TermStore** and check **TermStore.ReadWrite.All**.

16. Click **Add permissions**.

17. Under **Microsoft Graph**, click **User.Read**. Click **Remove permission**.

18. The **API permissions** list appears as follows:
2.5.3 Set the App Keys

1. Under Manage, click Certificates & Secrets.

2. Click New client secret.

Client secrets
A secret string that the application uses to prove its identity when referred to as application password.

Add a client secret

Description
Expires
- In 1 year
- In 2 years
- Never

Add | Cancel
3. In the **Add a client Secret** popup:
   - Enter a **Description**, for example, RepMobileAppSecret.
   - Set **Expires** to **Never**.

   **Note** There is an open issue with Secrets that contain characters “+” or “/”. It is necessary to generate a Client Secret that does not contain these characters.

4. Click **Add**.

5. Copy the value generated to **ExchangeAndSharepointAppSecret** under the **Key Vault Configuration Secrets**.

6. Click **Overview**. Copy the **Application (client) ID** from the App description panel to **ExchangeAndSharepointAppClientId** under the **Key vault configuration Secrets**.

### 2.5.4 Add Redirect URIs

1. Click **Overview**. Click **Add a Redirect URI**.

2. Enter

   ```
   https://[<insert web app service url here>]/AzureActiveDirectory/UserAuthorized
   https://[<insert web app service url here>]/AzureActiveDirectory/AADTenantConnected
   ```

   For example

   ```
   https://repstormobilewebapp.azurewebsites.net/AzureActiveDirectory/UserAuthorized
   https://repstormobilewebapp.azurewebsites.net/AzureActiveDirectory/AADTenantConnected
   ```

3. Click **Save**.
2.6 Create SQL Database

You can create a new DB or use an existing DB.

2.6.1 Create the SQL Database

1. In Microsoft Azure, click **Create a resource**.

2. Type **SQL Database**

3. In the search results, select **SQL Database**. In the **SQL Database** panel, click **Create**.

4. In the **Create SQL Database** panel, enter the following:
   a. A **Subscription**.
b. In the **Resource group**, click the resource group created here, for example, **RepstorMobile**

c. In the **Database name**, type a name. For example, **RepstorMobileDB**.

d. **Server** – select an existing Server, or click **Create new** and enter the following:
   - In the **New Server** pane, enter the required fields
   - **Server Name** – a name for the DB server, e.g. **repstomobilesql**
   - Server admin login – the name of the admin login account, e.g. **sqladmin**
   - **Password**
   - **Confirm Password**
   - Location – enter an appropriate location.
   - Ensure **Allow Azure services to access server** is checked.
   - Click **Select**.

e. In **Want to use SQL elastic pool** – select as appropriate.

5. Click **Create + Review**.

6. Click **Create**. It can take a few moments to create the DB.

### 2.6.2 Add your IP address in the firewall setting

In order to access the SQL server from your client machine, you must add your client IP address to the SQL Server Firewall.

1. In the left navigation pane, click **All Resources** and select the SQL server on which the newly created SQL Database is running, e.g. “repstomobilesql”

2. In server panel, under **Security**, click on **Firewalls and virtual networks**.

![Security](image)

3. Click on **Add client IP**

4. Click **Save**.

### 2.6.3 Connect to the SQL Server DB

1. Using SQL Server Management studio, connect to the Database in Azure using the SQL Admin credentials.

2. Provide SQL Admin credentials with Azure as Username and password.

**Note**  [Additional information](#) on connecting to an Azure SQL Database.
2.6.4 Create the Database tables and indexes

1. Open the file 1. RepstorMobile-CreateDatabase.sql
2. Update the first line of the file: USE [{DatabaseName}]. For example, USE [RepstorMobileDB]
3. Click Execute. The message Commands completed successfully. appears in the message pane.

2.6.5 Insert the Configuration data

1. Open the file 2. RepstorMobile-Configuration.sql
2. Update the highlighted text accordingly:

```
INSERT INTO [dbo].[Settings] ([Id], [StorageType], [IncludeAttachmentsInCategorization], [EnableSuggestions], [FiledCategory], [FiledInfoText], [UseMillisecondsInFingerprint], [ConvertToMsg], [BoxMetadataEmailTemplate], [BoxMetadataFingerprintTemplate], [AadApp]) VALUES ('unarep.onmicrosoft.com' - domain, 'sharepoint', 0, 0, 'Filed by Repstor', 'Filed to {path}', 1, 1, null, null, 'exchangeandsharepoint')
```
2.6.6 Create the Login Account

1. Open the file 2. Repstor Mobile - Create Login.sql. Ensure this script is run against the master database.

2. Update the highlighted text.

```sql
CREATE LOGIN [mobile_filing_webservice]
WITH PASSWORD=N'Password123'
```


4. Update the highlighted text.

```sql
```

2.6.7 Configure the Database Connection string:

1. Configure the Database Connection string as below:

   ```
   Server=tcp:{server_domain_name},1433;Initial Catalog={database_name};Persist Security Info=False;UserID={your_username};Password={your_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;
   ```

   E.g.

   ```
   Server=tcp:repstormobilesql.database.windows.net,1433;Initial Catalog=RepstorMobileDB;Persist Security Info=False;UserID=mobile_filing_webservice@repstormobilesql;Password=Password123;MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;
   ```

2. Copy the DB connection string to SettingsDB in the table under Key Vault configuration secrets.

2.7 Create the Key Vault Resource

1. In Microsoft Azure, click Create a resource. In the Search the Marketplace box type key vault.

2. Click Create.
3. In the **Create key vault** panel, complete the required fields. Enter:
   - A name, for example, **RepstorMobileKV**.
   - A subscription
   - In **Resource Group**, click **Use existing** and select the one created [here](#). For example, **RepstorMobile**
   - A location

4. Click **Access policies** and then click **Add new**.
5. Click **Select Principal** and search for the principal representing the App Service identity created earlier. For example, RepstorMobileApp.

6. Select **Key Permissions** and grant the following: **Get, List**.

7. Select **Secret Permissions** and grant the following: **Get, List**.

8. Repeat the above 4 steps to grant the same permissions to the following principals:
   a. Function App Service identity, For example, RepstorMobileFunApp.
   b. Web App Service identity, For example, RepstorMobileWebApp.
   c. Maintenance App identity, For example, RepstorMobileMaintenanceApp.

9. Click **OK** to confirm the access policies.

10. Click **Create** to complete the creation of the key vault.

### 2.7.1 Retrieve the Key Vault URL value

- Copy the following values to the Mobile Web App, Filing Engine Function App and the Maintenance Function App tables under the Configuration Settings for On-Premise Repstor Mobile:
**KeyVaultUrl** – the URL obtained from All resources, click on the Key Vault resource. For example, **RepstorMobileKV**.

### 2.8 Create the Sessions Key Vault Resource

**Note** A separate Key Vault is created to store user sessions. The steps are the same as the previous key vault except Write permissions are granted.

1. In Microsoft Azure, click **Create a resource**. In the **Search the Marketplace** box type key vault.

2. Click **Create**.

3. In the **Create key vault** panel, complete the required fields. Enter:
   a. A name, for example, **RepstorMobileSessionsKV**
   b. A Subscription
   c. In the **Resource Group**, click **Use existing** and select the one created [here](#). For example, **RepstorMobile**
d. **Location** – Enter an appropriate location

4. **Click Access policies** and then click **Add new**.

5. **Click Select Principal** and search for the principal representing the App Service identity created earlier.

6. Select **Key Permissions** and grant the following: **Get, List, Update, Create, Delete**

7. Select **Secret Permissions** and grant the following: **Get, List, Set, Delete**

8. Repeat the above 4 steps to grant the same permissions to the following apps:
   - Function App Service identity. For example, RepstorMobileFunApp.
   - Web App Service identity. For example, RepstorMobileWebApp.
   - Maintenance App identity. For example, RepstorMobileMaintenanceApp.

9. Click **OK** to confirm the access policies.

10. Click **Create** to complete the creation of the key vault.

**2.8.1 Retrieve the Key Vault URL value**

- Copy the following values to the table under the **Key Vault Configuration Secrets** settings:

  **SessionsKeyVaultUrl** – the URL obtained from All resources, click on the Key Vault resource. For example, **RepstorMobileSessionsKV**.
2.9 Create the SendGrid API

In the event of email filing failures, Repstor Mobile app will send a notification email. SendGrid is used to achieve this.

2.9.1 Creating the SendGrid API

1. In Microsoft Azure, click **Create a resource**. Azure will automatically create a SendGrid account per tenant.

2. Type **SendGrid**.

3. In the **Select a software plan drop down**, ensure **Free 25,000 emails per month** is selected.

4. Click **Create**.
5. In the **Create a New SendGrid** panel, complete the required fields. Enter:
   a. A name. For example, RepstorMobileSG
   b. A password and re-enter it to confirm it.
   c. A Subscription
   d. In **Resource Group**, click **Use existing** and select the one created here. For example, RepstorMobile
   e. In **Pricing Tier** – select F1 Free and click **Select**.
   f. In **Contact Information**, type a name and email address. Click **OK**.
   g. In **Legal terms**, click **Create**.

6. Click **Create**.

### 2.9.2 Create the SendGrid API Key

1. From the left navigation, click on **All resources**, and locate the Send Grid app created in the previous step, For example RepstorMobileSG.

2. Click ![Manage](image) this will redirect to the 3rd Party SendGrid web site.

3. When on the Sendgrid API page click **Settings** then **API Keys**.

   ![Settings](image)
   - Account Details
   - Alert Settings
   - API Keys
   - Inbound Parse
   - IP Access Management
   - IP Addresses
   - Mail Settings

4. Select **Create API Key**.

![Create API Key](image)

### 2.9.3 Choose API Key Permissions

1. Give your API key a name, RepstorMobileSGAPIKey.

2. Select Restricted Access and under Access Details, select Mail Send.
3. Click **Create and View**.

4. Copy the API Key that was generated to the SendGridApiKey setting in the table under the **Key Vault configuration secrets** settings.

### 2.10 Configuring the On-Premise Repstor Mobile

This section will use the settings captured during the installation that were recorded to the configuration settings tables in **Configuration for the on-Premise Repstor Mobile**.

#### 2.10.1 Configure the Web App

1. In the left navigation, click **App Services**. Click the Web App that was created [here](#). For example, **RepstorMobileWebApp**.

2. Under **Settings**, click **Configuration**.

3. In this page go to **Application Settings**.

4. Add each of the Web application settings in the table in the Mobile Web App service section:
2.10.2 Configure the Function App

1. In the left navigation, click **App Services**. Click the Function App that was created in Create the Function Application for Repstor Mobile App section. For example, RepstorMobileFunApp.

2. Under **Configured features**, click **Application settings**.

3. Add each of the Web application settings in the table detailed at the start of this document.

4. Update `FUNCTIONS_EXTENSION_VERSION` to be `~1`.

5. Click **Save**.

2.10.3 Configure the Maintenance Function App

1. In the left navigation, click **App Services**. Click the Maintenance Function App that was created in Create the Maintenance Function Application for Repstor Mobile App section. For example, RepstorMobileMaintenanceApp.
2. Under **Configured features**, click **Configuration**.

3. In this page go to **Application Settings**.

4. Add each of the application settings in the table detailed at the start of this document.

5. Update `FUNCTIONS_EXTENSION_VERSION` to be ~1

6. Click **Save**.

### 2.10.4 Configure the Key Vault Secrets

1. Under **All Resources**, click the Repstor Mobile Key Vault that was created in [Create the Key Vault Resource section](#).

2. Under **Settings**, click on **Secrets**.

3. For each of the Key Vault configuration secrets table:
   a. Click **Generate/Import** .
   b. In the **Create a secret**, enter the **Name** and **Value**. Click **Create**.


### 2.10.5 Summary of Azure Objects

The objects created by this installation:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>RepstorMobileFunApp</td>
<td>App Service</td>
</tr>
<tr>
<td>RepstorMobileWebApp</td>
<td>App Service</td>
</tr>
<tr>
<td>repstormobilemaintenanceapp</td>
<td>App Service</td>
</tr>
<tr>
<td>ASP-RepstorMobile-b545</td>
<td>App Service plan</td>
</tr>
<tr>
<td>WestEuropePlan</td>
<td>App Service plan</td>
</tr>
<tr>
<td>RepstorMobileFunApp</td>
<td>Application Insights</td>
</tr>
<tr>
<td>RepstorMobileMaintenanceApp</td>
<td>Application Insights</td>
</tr>
<tr>
<td>RepstorMobileWebApp</td>
<td>Application Insights</td>
</tr>
<tr>
<td>RepstorMobileKV</td>
<td>Key vault</td>
</tr>
<tr>
<td>RepstorMobileSessionsDV</td>
<td>Key vault</td>
</tr>
<tr>
<td>RepstorMobileSG</td>
<td>SendGrid Account</td>
</tr>
<tr>
<td>RepstorMobileDB</td>
<td>SQL database</td>
</tr>
<tr>
<td>repstormobilesql</td>
<td>SQL server</td>
</tr>
<tr>
<td>repstormobilefu9caf</td>
<td>Storage account</td>
</tr>
<tr>
<td>repstormobilema9762</td>
<td>Storage account</td>
</tr>
<tr>
<td>sqlvanwadiqv4viff2</td>
<td>Storage account</td>
</tr>
</tbody>
</table>
Deployment

3.1 Granting permissions

To make Repstor Mobile available as an outlook add-in for users, the app must first be able to make Office 365 requests on behalf of the users. To do this you must grant consent for the application to make requests to your Azure Active Directory (AAD). The Repstor Azure Active Directory App is registered with delegated permissions only. This means that the app can only make requests on behalf of your users, and therefore have the same permissions as your users. To Grant Consent to the Repstor Mobile AAD App.

1. In the following URL, replace the “<customerdomain.com>” with your domain name and browse to the URL

https://<webappurl>/AzureActiveDirectory/AppAdminConsent?emailOrDomain=<customerdomain.com>&appName=exchangeandsharepoint

For example,
https://repstormobilewebapp.azurewebsites.net/AzureActiveDirectory/AppAdminConsent?emailOrDomain=unarep.onmicrosoft.com&appName=exchangeandsharepoint

The Permissions requested Accept for your organization dialog box appears.

![Microsoft Permissions Request](image)
2. Click **Accept**. The Repstor Mobile AAD App now has the listed permissions on behalf of any user that authenticates with Repstor Mobile.

### 3.2 Applying the App to Exchange

1. Open and edit the file “Onpremise.RepstorMobile.xml”
   a. Ensure that all web URL occurrences are set to the web URL of the Web App installed [here](https://repstornobilewebapp.azurewebsites.net/). For example,

   ```xml
   <IconUrl DefaultValue="https://repstornobilewebapp.azurewebsites.net/Content/Icons/assistant-64x64.png" />
   ```
   b. Ensure you have a unique GUID for the Add-In, by replacing the GUID below

   ```xml
   <Id>5eaf461f-3b77-4d0e-88ee-645050c017db</Id>
   ```
   
   IMPORTANT! Id must be unique for your add-in, if you reuse this manifest ensure that you change this id to a new GUID. -->

2. As an admin user, navigate to [https://admin.microsoft.com/adminportal](https://admin.microsoft.com/adminportal)

3. Under **Settings - Services & add-ins**, click **+Deploy Add in**.

4. Under **Centralized Deployment**, click **Next**.

5. Click **I have the manifest file (.xml) on this device** and browse to the “Onpremise.RepstorMobile.xml” file and click **Next**.
6. Select who should have access to this add-in and click **Deploy Now**. It may take up to 12 hours for the Add-in to be available to the targeted users.