FaxMaker

OAuth support for POP3 / SMTP

Overview

The introduction of OAuth support for POP3 and SMTP in GFI FaxMaker marks a significant advancement in ensuring compatibility with modern email authentication protocols. With Microsoft enforcing OAuth as the standard for accessing Office 365 email services, this update resolves the critical limitation posed by FaxMaker's reliance on Basic Authentication.

By enabling OAuth integration, organizations can now seamlessly connect FaxMaker to Microsoft 365 email services, ensuring secure and uninterrupted faxing capabilities through email clients and web interfaces. This enhancement not only aligns FaxMaker with industry authentication standards but also provides users with a more secure and future-proof solution for managing electronic fax communications.

Prerequisites:

1. **Azure Business Account:** A registered organizational account within Microsoft Azure to enable integration with Microsoft 365 services.
2. **Admin access to the Azure portal:** Administrative permissions to configure app registrations, manage API permissions, and set up OAuth credentials.
3. **Exchange Online Plan for users:** A valid subscription plan providing email services via Microsoft 365 for users needing access to FaxMaker's email-based faxing.

Application registration process

To enable OAuth authentication for FaxMaker, follow these step-by-step instructions to configure the necessary settings in the Azure portal and Microsoft 365 environment. This process includes registering an application in Azure, setting up appropriate permissions, configuring authentication details, and creating user accounts tailored for POP and SMTP access. By completing these steps, you'll ensure seamless and secure integration of FaxMaker with Microsoft 365 email services.

1 Initial Setup in Azure Portal

1. Log in to portal.azure.com as an admin
2. Navigate to App Registration
3. Click on "+ New Registration"
4. Configure the application:
    a. Set a name for the new application
    b. Set the account type : “Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
    c. Click on register
5. Once the App is created, note down the Application (client) ID which will be required for the FaxMaker configuration.

2 Permission Configuration

1. Go to API permissions
2. Click on “+Add a permission”
3. Add Microsoft Graph > Delegated Permissions:
    a. POP access permissions
    b. SMTP permissions
    c. Offline access permissions
4. Click on “Add permissions”
5. Click on “Grant admin consent”.

3 Authentication Setup

1. Go to Authentication
2. Click on “+ Add platform” > “Mobile and desktop applications”
3. Configure redirect URI:
    a. http://localhost:5000/callback
    b. **Note down this callback URI which will be required** for the GFI FaxMaker configuration.
4. Scroll down to Advanced Settings and toggle the “Allow public client flows” to Yes
5. Click on Save.

4 User configuration

To prevent loopback, create two separate users: one designated for POP access and the other for SMTP.

1. Go to your admin portal admin.microsoft.com.
2. Go to the “Mail” setting on each user
    a. Click on “Manage email apps”
    b. Enable all mail management checkboxes (Remember to do this for each user)
3. For POP users - also under “Mail” > Mailbox as permissions
    a. Under “Send as permissions” and “Send on behalf of permissions” add the other user (The user for SMTP)
4. For the pop user also login to its inbox (outlook.office.com) and go to “Settings”
    a. Go to Email > Sync Email
    b. Make sure POP and IMAP settings are enabled.

GFI FaxMaker configuration

To enable OAuth authentication for FaxMaker, follow these step-by-step instructions to configure the necessary settings in the Azure portal and Microsoft 365 environment.

This process includes registering an application in Azure, setting up appropriate permissions, configuring authentication details, and creating user accounts tailored for POP and SMTP access.

By completing these steps, you’ll ensure seamless and secure integration of FaxMaker with Microsoft 365 email services.

Prerequisites:

- Application (client) ID.
- Callback URI.

These values should be retrieved from the Azure configuration. For more details refer to the Application registration section.

SMTP Connector:

1. Go to the FaxMaker server > GFI FaxMaker Configuration
2. Go to Email2FaxGateway and click on Properties
3. Under SMTP Connector click on the “Office 365 Authentication” option and set the following information:
   a. Mail server name / IP: smtp.office365.com
   b. Port: 587
   c. Mailbox account: <The user created in the previous section for SMTP>
   d. Authorization redirect URL: <the callback URI set up previously>
   e. Timeout (in minutes): <minimum value 1>
   f. Client ID: <The application (client) ID configured in the previous section>
4. Click on “Authenticate” and you will be redirected to a web browser to authenticate the user. Once you enter the password the web browser window can be closed.
5. A test can be performed by sending a test email.

POP3 Downloader:

1. Go to the FaxMaker server > GFI FaxMaker Configuration
2. Go to Email2FaxGateway and click on Properties
3. Under POP3 Downloader > Enable POP3 downloader
4. Click on the “Office 365 Authentication” option and set the following information:
   a. Mail server name / IP: outlook.office365.com
   b. Port: 995
   c. Mailbox account: <The user created in the previous section for POP3>
   d. Authorization redirect URL: <the callback URI set up previously>
   e. Client ID: <The application (client) ID configured in the previous section>
   f. Timeout (in minutes): <minimum value 1>
5. Click on “Authenticate” and you will be redirected to a web browser to authenticate the user. Once you enter the password the web browser window can be closed.
6. Go back to the FaxMaker configuration and click on OK.

Note: The same options can be configured by using the GFI FaxMaker configuration wizard