

GUIDE

Integrating GFI Archiver AI with MS365



GFI Software™

Introduction

This guide provides a streamlined process for integrating GFI Archiver AI with Microsoft 365 using modern authentication methods.

Prerequisites Checklist

Before beginning, ensure you have:

- GFI Archiver server version 15.8 installed and configured
- Microsoft 365 subscription with administrative access
- Permissions to register applications in Microsoft Entra ID (formerly Azure AD)
- Network connectivity between your GFI Archiver AI server and Microsoft 365

Method 1 *Direct EWS OAuth Integration*

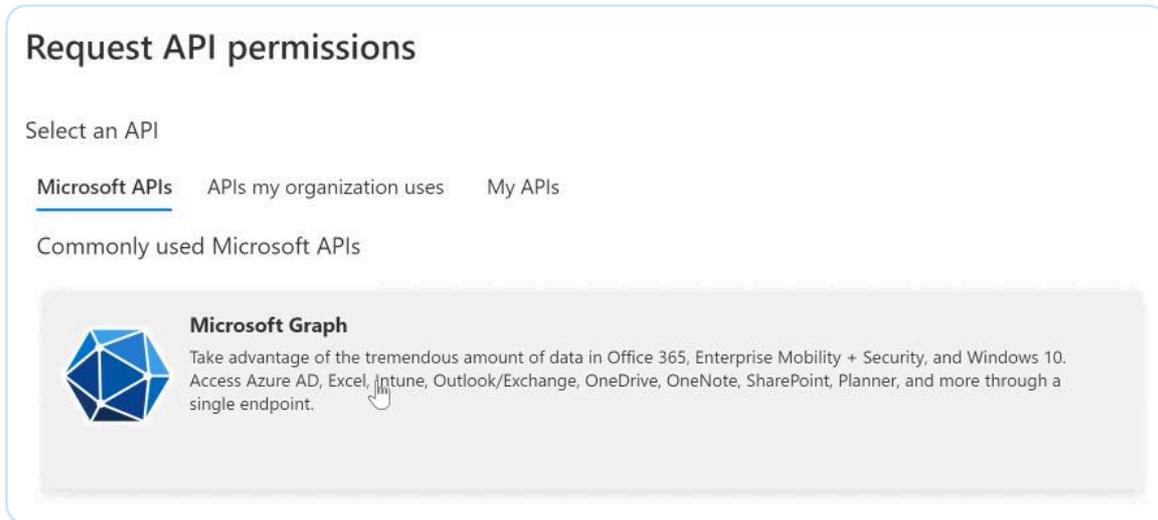
This method is required to directly connect GFI Archiver AI to Microsoft 365. It ensures secure communication by using OAuth authentication.

1 Register GFI Archiver in Microsoft Entra ID

1. **Access Azure Portal:** Log in to the [Azure Portal](#) with administrative credentials.
2. **Navigate to App Registrations:** Go to Microsoft Entra ID > App registrations > New registration.
3. **Register Application:** Name: Enter a descriptive name (e.g., "GFI Archiver")
 - **Supported account types:** Select Accounts in this organizational directory only (Single tenant)
 - **Redirect URI:**
 - Platform: Select Web
 - URI: Enter `https://[YOUR-SERVER-NAME]/Archiver/OAuthRedirect.aspx`
 - Replace [YOUR-SERVER-NAME] with your actual server's FQDN
 - Click Register
4. **Record Credentials:** Note down the Application (client) ID and Directory (tenant) ID displayed.
5. **How the OAuth Flow Works:**
 - During setup, the administrator logs into Microsoft Azure and authenticates from their browser.
 - The authentication response is redirected back to the local GFI Archiver server.
 - Once configured, GFI Archiver uses the acquired tokens to connect to Microsoft 365 services.
 - **Network Requirements:**
 - GFI Archiver server needs outbound connectivity to Microsoft 365 services (primarily over HTTPS/ port 443).
 - No inbound connectivity from the internet to your GFI Archiver AI is required for ongoing operations.

2 Configure API Permissions

1. In your registered app, select API permissions from the left menu.
2. Click Add permission.
3. Select Microsoft Graph > Delegated permissions.



4. Add these permissions:
 - Mail.Read
 - Mail.ReadBasic
 - Mail.ReadBasic.All
 - Mail.ReadWrite
 - offline_access
 - User.Read
5. Click Add permissions.
6. Click Grant admin consent for [Your Organization].

3 Create a Client Secret

1. In your registered app, go to Certificates & secrets in the left menu.
2. Click New client secret.
3. Enter a description and select an expiration period based on your security policies.
4. Click Add.
5. **IMPORTANT:** Immediately copy the client secret value (not the Secret ID) and store it securely. This value cannot be retrieved later.

4 Configure TLS on GFI Archiver AI Server (If Needed)

1. Ensure your GFI Archiver AI server is running the latest version of TLS.
2. Configure required TLS settings according to Microsoft 365 requirements.
 - To change TLS settings in GFI Archiver:
 - Open a PowerShell prompt as administrator on the GFI Archiver AI server.
 - Run the following commands to enable strong cryptography and TLS 1.2:

```
``powershell

New-ItemProperty -path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -name
'SchUseStrongCrypto' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:
\SOFTWARE\WOW6432Node\Microsoft\.NetFramework\v4.0.30319' -name 'SchUseStrongCrypto'
-value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -name
'SystemDefaultTlsVersions' -value '1' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:
\SOFTWARE\WOW6432Node\Microsoft\.NetFramework\v4.0.30319' -name
'SystemDefaultTlsVersions' -value '1' -PropertyType 'DWord' -Force | Out-Null.
```

3. Restart the server after making any changes.
 - [Configuring EWS OAuth Authentication with GFI Archiver AI](#)

5 Configure GFI Archiver AI for Microsoft 365 Integration

1. Access GFI Archiver: Log in to your GFI Archiver AI web interface as an administrator.
2. Add New Mail Server: Navigate to Configuration > Mail Servers to Archive > Add.
3. Configure Mail Server:
 - Select Microsoft 365 as the mail server type
 - Enter a descriptive name for the connection
 - Select OAuth as the authentication method
 - Enter the following details:
 - Application (client) ID: Paste the ID from Step 1
 - Directory (tenant) ID: Paste the ID from Step 1
 - Client secret: Paste the secret value from Step 3
 - Redirect URI: Verify it matches the URI entered in Azure
 - Click Next

4. Complete OAuth Authentication:

- You'll be redirected to Microsoft login
- Sign in with your Microsoft 365 admin account and grant permissions
- Upon successful authentication, you'll be redirected back to GFI Archiver AI

5. Configure Journaling Settings:

- Enter the email address of the journaling mailbox
- Set email checking frequency (recommended: 5 minutes)
- Configure additional settings as needed
- Complete the setup wizard

[🔗 Archiver Integration with Microsoft 365](#)

Method 2 *Optional Journaling Mailbox Method (Alternative)*

This method is useful if direct EWS access is impractical or if additional compliance measures require an alternative approach.

1 Set Up Mail Flow in Microsoft 365

If using a journaling mailbox with mail flow rules instead of direct EWS access:

1. Log into Microsoft 365 admin center.
2. Navigate to Exchange admin center > Mail flow > Rules.
3. Click Add a rule > Create a new rule.
4. Name the rule (e.g., "Archive all emails").
5. Under conditions, select Apply to all messages.
6. Under actions, select BCC the message to...
7. Select the journaling mailbox configured in GFI Archiver AI.
8. Save the rule.

2 Testing and Validation

1. Test Connection:

- In GFI Archiver AI, go to Configuration > Mail Servers to Archive
- Select your Microsoft 365 connection
- Click Test Connection to verify connectivity

2. Send Test Emails:

- Send a few test emails between users in your organization
- Check GFI Archiver AI to verify emails are being archived

3. Verify Search Functionality:

- Use GFI Archiver's search features to locate the test emails
- Confirm that content and attachments are properly indexed

Troubleshooting

OAuth Authentication Errors

Incorrect Redirect URI:

- Ensure the Redirect URI is exactly the same in both Azure and GFI Archiver AI
- Even minor differences can cause authentication failures

Missing Permissions:

- Verify all required API permissions are granted in Azure
- Confirm admin consent has been provided

Expired Client Secret:

- If the client secret expires, generate a new one in Azure
- Update the client secret in GFI Archiver AI

Connection Issues

Firewall Restrictions:

- Ensure your firewall allows outbound connections to Microsoft 365 services
- Default port is 443 (HTTPS)

TLS Version Compatibility:

- Microsoft 365 requires modern TLS versions
- Verify your server supports TLS 1.2 or later

Multi-Factor Authentication:

- For journaling mailboxes, MFA may need to be disabled
- Use app passwords or service accounts where appropriate

Emails Not Being Archived

Mail Flow Rules:

- Verify mail flow rules are active in Exchange admin center
- Check that the correct journaling mailbox is configured

Journaling Mailbox Configuration:

- Ensure the journaling mailbox exists and is accessible
- Check that GFI Archiver AI has the correct permissions

GFI Archiver AI Services:

- Verify all GFI Archiver AI services are running
- Check logs for any errors or warnings

[🔗 Archiver not consuming emails from the journal mailbox on Exchange Online](#)

Best Practices

- **Regular Monitoring:** Implement periodic checks to ensure the archiving process is working correctly.
- **Security Updates:** Keep both GFI Archiver AI and your Microsoft 365 environment updated.
- **Backup Configuration:** Document your configuration settings and maintain backups.
- **Permission Reviews:** Periodically review permissions to ensure they remain appropriate.
- **Log Monitoring:** Regularly review GFI Archiver AI logs for any warnings or errors.

Support

If you encounter persistent issues after following this guide, collect the following information before contacting GFI Support:

- GFI Archiver AI version and build number
- Detailed error messages
- Troubleshooter logs from the GFI Archiver AI server
- Screenshots of your configuration settings

Additional Resources:

- [Archiver Integration with Microsoft 365](#)
- [Registering Archiver in Azure Portal](#)
- [Configuring EWS OAuth Authentication with GFI Archiver](#)
- [GFI Archiver and Office 365 Deployment Guide](#)
- [Gathering Troubleshooter Logs for Archiver](#)

This guide was created based on GFI Archiver AI version 15.8 and Microsoft 365 as of February 2025.

Features and interfaces may change in future updates.