

Discovery Attender

Version 4.5



Table of Contents

Discovery Attender.....	1
Welcome.....	4
Where to Install.....	5
System Requirements.....	6
Permissions.....	7
Installation Guide.....	8
Running Discovery Attender.....	11
License Key.....	11
Uninstall.....	12
Discovery Attender for SharePoint Component.....	14
Microsoft 365 & EWS.....	15
Modern Authentication.....	15
Create a Self-signed Certification.....	15
Application Registration Process.....	16
Establish OAuth Application Permissions.....	17
Configure Discovery Attender with Modern Authentication (OAuth).....	24
Basic Authentication.....	26
Establish Application Impersonation Rights.....	26
Configuring Discovery Attender for EWS (Microsoft 365) Basic Authentication.....	27
Discovery Attender for SharePoint.....	29
SharePoint REST (EWS).....	30
Modern Authentication.....	30
Basic Authentication.....	31
SharePoint Component.....	32
Permissions.....	32
Where to Install.....	32
Installation Guide.....	33
Configuration Wizard for Discovery Attender for SharePoint.....	33
Where to Begin.....	37
Create Project.....	37
Manage Searches (Main Console).....	38
New Search (Search Wizard).....	40



Manage Results.....	41
Organize Items	41
Exports and Actions.....	41
Preview Pane and Text Viewer	42
Reports.....	42
Contact Information.....	43

Welcome

Thank you for choosing Discovery Attender®. This application is designed to make the searching, collection and management of electronically stored data easy and efficient. Discovery Attender can collect and export email and files from many different data stores including:

- Outlook Personal Folders (PST files)
- Microsoft Exchange Mailboxes, Online Archives and Public Folders
- Microsoft 365 Mailboxes, Online Archives, and Public Folders
- SharePoint Servers
- Lotus Notes NSF files
- MBOX format email files
- Loose email in MSG or EML format
- Hard Drives, File Shares and Network drives

Use this Getting Started document to guide you through the setup of the program and initial scans of your data.

Where to Install

- Discovery Attender can be installed on a desktop, laptop, server, or virtual machine. The more memory and processing power on the machine, the better the performance of the application.
- Never install Discovery Attender on a machine running mission critical applications without testing it first.
- Discovery Attender requires *Local Administrator Rights* to the machine where it is installed.
- Installing Discovery Attender on a production Exchange server is *not recommended* due to potential CPU or I/O constraints.
- Discovery Attender can search across a network. However, a slow connection can cause delays with the processing of files and reduce the efficiency of the product.
- Microsoft Office must be installed on the machine where Discovery Attender is installed.
- Microsoft Outlook must be enabled with at least one profile created to successfully search Exchange based email stores (on-premises Exchange, PST or MSG sources) or export to a PST or MSG,. Outlook provides the MAPI drivers needed for communication with certain mail stores as well as any exports to PST (including from M365). These drivers are not initialized until a profile is created and Outlook opened at least once.
- To search NSF files, a Lotus Notes client version 8.5.1 or above must be installed and configured.
- The Microsoft.Net 4.8 (or above) framework is required on the machine where Discovery Attender is installed.
- The appropriate Microsoft Visual Runtime C++ library (currently 2019) will be installed or updated if not present on the installation machine.
- In certain environments, you may need to install an Access engine redistributable file for Discovery Attender to successfully communicate with its databases. It can be found [here](#). Download the version that matches the bitness of your Microsoft Office installation.
- To search on-prem 2013 SharePoint stores, an additional, separately licensed component needs to be installed on a server in the SharePoint farm along with .Net 4.8 or above.

All other SharePoint searches, including on-prem SharePoint 2016 or above, or online, can use the REST protocol which does **not** require the installation of any additional components.

System Requirements

Discovery Attender runs as a stand-alone application on your desktop, laptop, or server. The following are *minimum* system requirements. However, Discovery Attender speed and efficiency are highly dependent on CPU and memory. The more of each of these you have installed on the machine, the faster searches and exports will complete.

- Windows 10 or higher; Windows 2008 Server, SP 2 or higher
- **Minimum:** 2 GHz or higher CPU (more is recommended)
- For *significantly* better performance, please use 2x or 4x the minimum amount of processing power listed above
- 4 GB of RAM or higher (more is recommended)
- Microsoft Office 2013 or higher installed
- Microsoft Outlook 2013 or higher installed and configured with a profile (if searching mailboxes, online archives, PST files, or other on premise Microsoft Exchange based data stores)

Note: If searching M365 email stores, Office 2016 or above is required.

- Lotus Notes Client 8.5.1 or higher (if searching Lotus Notes NSF files)
- Approximately 100 MB free Hard Drive space for the installation. **Additional** Hard Drive space will be **required** as projects, searches and (optional) indexes are created. We recommend at least 20 GB per active project, and *more* if caching is used.
- **Local administrator rights** are required to run Discovery Attender

Please Note:

- **The above requirements are the minimum needed for running the product. However, to improve the performance of Discovery Attender, Gimmal highly recommends increasing the CPU and the memory.**
- Microsoft .Net 4.8 framework (or above) is required for Discovery Attender to function properly. The framework can be [downloaded](#) from the Microsoft web site.
- The login account that Discovery Attender is running under **requires** local administrator rights to the computer where the application is installed.
- Discovery Attender is available in 32-bit and 64-bit versions. The bitness (32-bit or 64-bit) of Discovery Attender must match the bitness of Microsoft Office, not the bitness of the machine operating system.

Permissions

- Discovery Attender uses the Login credentials (i.e. NT Account) of the user account logged into the machine where the program is installed. This account is used to access file shares and some mail store locations as well as reading and writing to the system registry. Therefore, this account **requires** Local Administrator Rights on the machine where Discovery Attender is installed.
- If you are searching mailboxes on more recent versions of on-premises Exchange servers, and you wish to use the MAPI protocol, an email profile needs to be created. This profile should be linked to an Exchange account with the associated search permissions for the mailboxes, online archives, public folders or recover deleted items that will be scanned. This profile needs to be created with the Control Panel | Mail options, then added to Discovery Attender's Settings.

Starting with Exchange 2016, the EWS protocol can be used as an alternative to MAPI. If you are searching Microsoft 365 mail stores, EWS **must** be used.

- For SharePoint searches, Discovery Attender 4.x can only access files or other data on an on-prem SharePoint 2013 server or above. There are two methods of accessing this data, component or REST. The component requires full permissions and needs to be installed on a server that is part of the SharePoint farm you intend to search.

When searching online SharePoint in Microsoft 365, the REST (EWS) protocol is required. Please see the SharePoint section below for further details.

- The user will need read/write access to Discovery Attender Project storage locations.
- If you are running Discovery Attender on a machine with UAC settings enabled (Windows 8.1 and above), you must select the "Run this program as administrator" privilege level under Properties | Compatibility. You will be prompted every time Discovery Attender is run.
- You will need full access to the mailboxes which need to be searched when connecting to on-premises Exchange data stores using our standard protocols. The reason Gimmal requires an elevated permission level is that our experience has shown that the full access permissions will work in **all** deployments for **all** Discovery Attender functionality. Select customers have been able to deploy with reduced permissions, however Gimmal cannot assist in setting up or supporting those configurations.

Notes for Searching on premises Exchange 2016 and above

Exchange 2016 is best searched using an EWS impersonated account. If searching via MAPI, be aware that not all implementations support MAPI searching of Exchange 2016 accounts. See notes below for 2013.

Notes for Searching Exchange 2010 and 2013

Permissions need to be run through PowerShell to propagate correctly.

Exchange throttling should be disabled for the Discovery Attender account. If throttling is not disabled, connection errors can and will occur.

Installation Guide

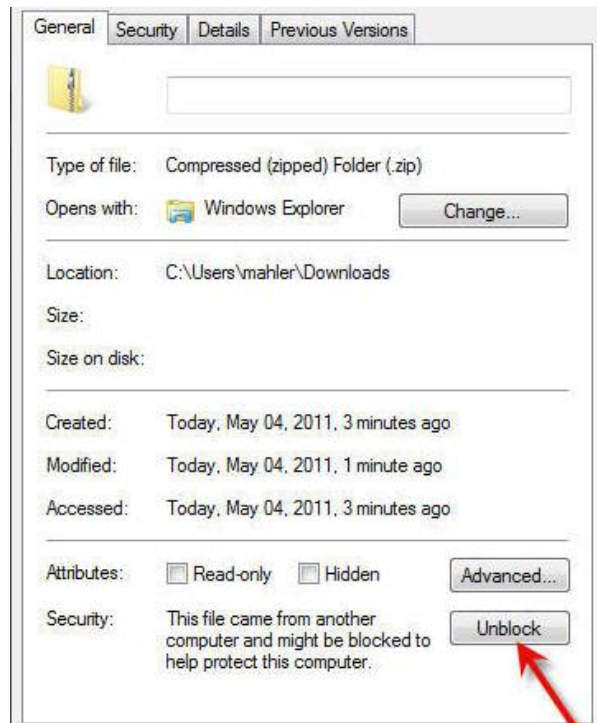
The following are general steps to install Discovery Attender.

1. Choose the server or computer where you wish to install Discovery Attender.
2. Verify that Outlook 2013 or above has been installed and run at least once with at least one profile. Outlook is not completely configured until the first profile has been created.

Outlook does not need to be installed in the following scenarios:

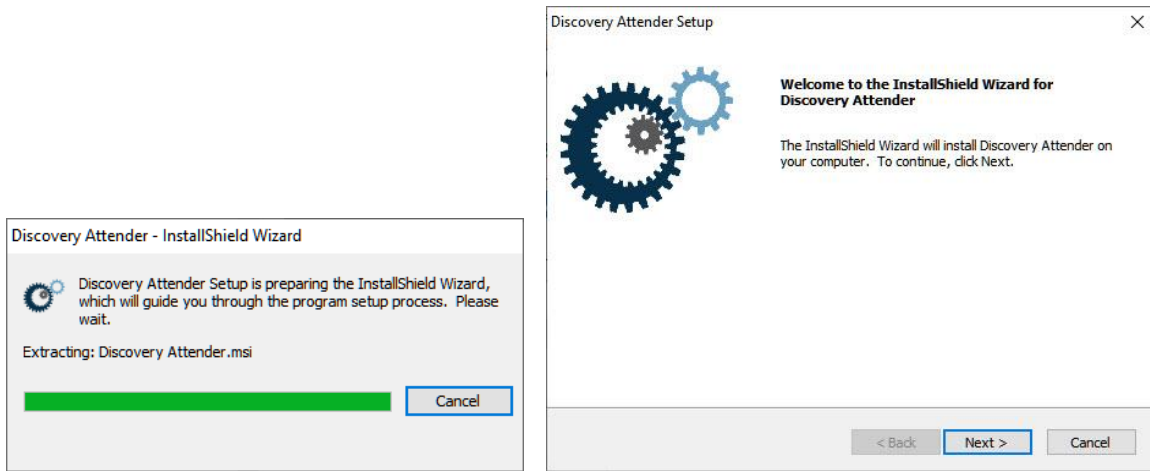
- You are **only** searching files shares for standard files (not PST files).
- You are **only** searching NSF files (see below for additional NSF requirements)
- Exchange Server installation (*not recommended*).

3. Make sure you select the correct setup file for the machine where Discovery Attender is to be installed. The bitness of Discovery Attender is dependent on the **bitness of the version of Office/Outlook** installed on the machine, not the bitness of the operating system.
 - a. If you are using a 64-bit version of Outlook/Office on your machine, then you must use the 64-bit version of the setup (DA_Setup_64.exe).
 - b. If your Outlook/Office is 32-bit you must choose the standard setup (DA_Setup.exe)
4. Verify the setup executable is unblocked. To do so, right-click on the file and select Properties. If there is an Unblock button in the lower, right-hand corner, select it and hit OK.



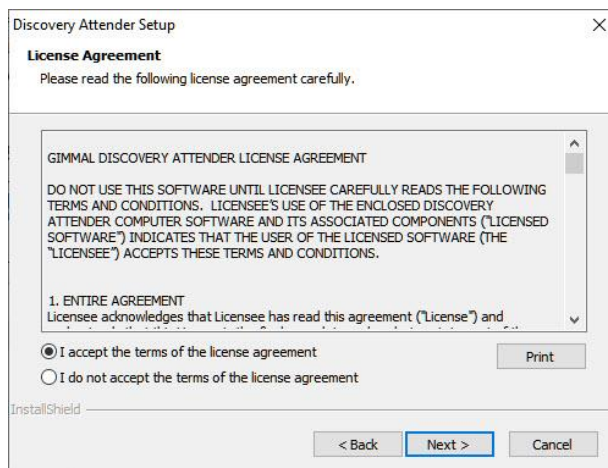
5. Double-Click the setup file to begin the installation of Discovery Attender.

6. The InstallShield™ wizard should automatically launch the setup. Follow the screens as prompted.

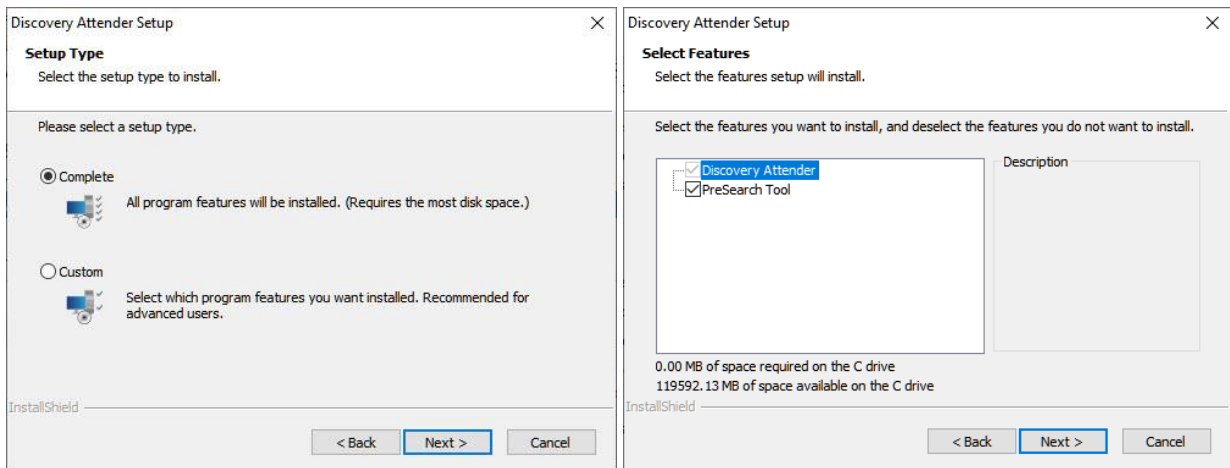


7. Please note: The Microsoft .Net 4.8 framework (or above) is required for proper functioning of Discovery Attender. If it is not installed, you will receive an error message and the setup will not continue.

8. You must accept the Discovery Attender License Agreement to continue with the installation.



9. Select if you'd like to perform a Complete or Custom setup.

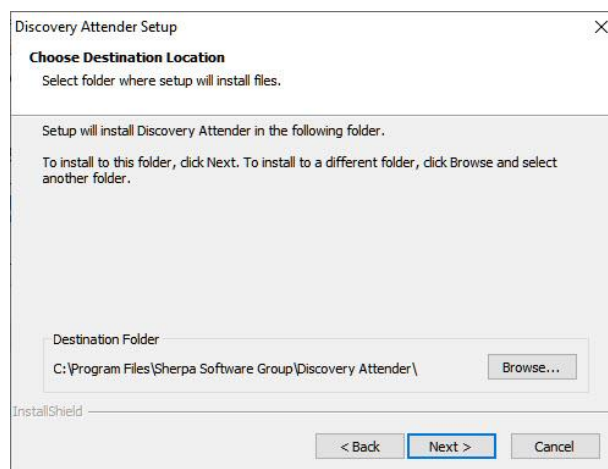


Note: Custom setup allows you to select which the components will be installed.

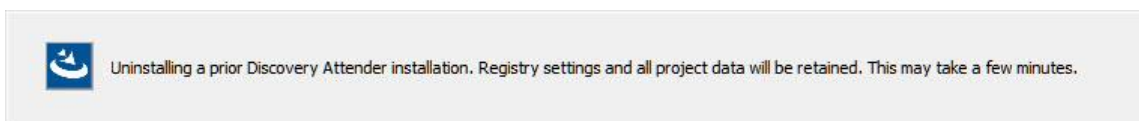
- *Discovery Attender* is the main installation and is not optional
- *PreSearch Tool* is a helpful utility that performs useful tasks such as deduplication, exports, and conversions before a search begins.

10. Select the location where you wish to install Discovery Attender.

- In addition to the program files, this destination will store log files, templates, some settings and the default temporary directory.
- Verify the login account has read/write permission to the chosen destination location.



Please note: If you are upgrading from certain versions of Discovery Attender, you may see the following prompt. Click 'OK' to continue:



11. The setup is now concluded. Discovery Attender will be installed with a new program group created in your start menu. You can access the program from *Start / Programs / Discovery Attender / Start Discovery Attender* to begin. A shortcut will be created onto your desktop.

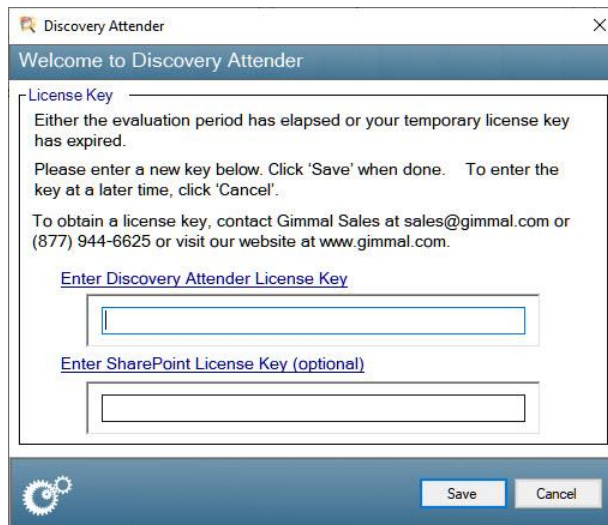
Running Discovery Attender

Note: If the correct version of the Visual C++ runtime or EWS Libraries is not found on the installation machine, they will be installed when Discovery Attender is first started. . This is a silent install and may take a few minutes to validate.

Discovery Attender must run under administrator privileges. To do so, select the "Run this program as administrator" privilege level under *Properties / Compatibility* once the product is installed.

License Key

The License Key setup screen will appear on startup of a new installation. To run the product, just enter your Discovery Attender license key in the box under 'Enter Discovery Attender License Key'. To enable the optional SharePoint searching, enter the separate SharePoint license key in the blocks labeled 'Enter SharePoint License Key (Optional)'.



The screenshot shows a dialog box titled "Discovery Attender" with a close button (X) in the top right corner. The main heading is "Welcome to Discovery Attender". Below this, the text reads: "License Key - Either the evaluation period has elapsed or your temporary license key has expired. Please enter a new key below. Click 'Save' when done. To enter the key at a later time, click 'Cancel'." It then provides contact information: "To obtain a license key, contact Gimmel Sales at sales@gimmel.com or (877) 944-6625 or visit our website at www.gimmel.com." There are two input fields: the first is labeled "Enter Discovery Attender License Key" and the second is labeled "Enter SharePoint License Key (optional)". At the bottom, there are "Save" and "Cancel" buttons.

- This step does not apply to the demo or evaluation versions.
- You can change the license key at any time by using the *Help | License Management* menu option on the main console screen.
- When upgrading from a previous version, Discovery Attender will use the license key from the existing installation.

Upgrading Discovery Attender

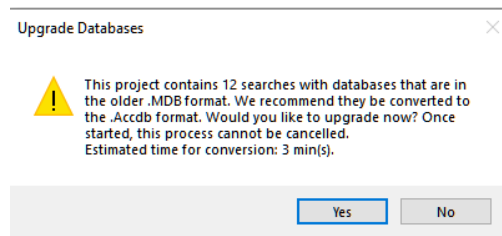
Please note: If you are upgrading Discovery Attender to the 4.5 version, there are several considerations:

Installing

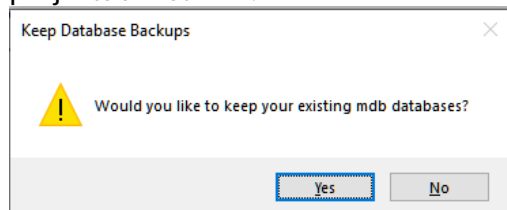
You will need to **uninstall** the previous version of Discovery Attender before you install the 4.5 version. To best maintain all your options, please follow the [steps for upgrading from 4.4 or below](#).

Database Conversion

Discovery Attender uses file based databases for portability and ease of use. Starting with version 4.5, all new searches will use an updated database format (.accdb) that provide stability and performance improvements. For projects stored in the older .mdb format (version 4.4 and below), users will be given the option to upgrade the databases for those affected projects from the older format to the newer ones.



- Choosing 'No' will keep the existing format.
- Choosing 'Yes' will convert the databases to the accdb format.
 - You will also be given the option to keep the existing database in their old .mdb format. When choosing this option, ensure you have sufficient space on the drive where the projects are stored.



Please note: The conversion feature is for **64-bit** versions of Discovery Attender only. 32-bit versions of Discovery Attender are still supported, and will still use the new format for new projects. However, older database formats will not be converted.

Upgrading from 4.4 or Below

Discovery Attender requires an uninstall / reinstall if upgrading from version 4.4 and below. To keep your options and bypass having to reenter your settings and keys, please follow the instructions below.

1. Save application options from the Main Console of Discovery Attender
 - a. Save Settings
 - i. Navigate to Discovery Attender | Settings
 - ii. Click the 'Export' button to save the Settings to a file.
Note: Remember the location of this .xml file, we'll use it later.

- b. Save Project List
Note: This will provide the list of locations for the most recent projects for reference. You will not be able to rehydrate this project list after Discovery Attender is uninstalled.
 - i. Choose the 'Open Project' option in the File Menu to open the 'Open a Project' dialog.
 - ii. Right-Click on the list of projects and select the 'Export to CSV' option to export the list of projects to a CSV file for future reference.
2. Save Management folder to retain configuration and custom exceptions
 - a. Navigate to the Installation directory of Discovery Attender (defaults to C:\Program Files\Sherpa Software Group\Discovery Attender)
 - b. Copy the 'Management' folder to a separate location.
 - c. Make a note of this location. You will need it later.
3. Get System Information
 - a. Navigate to Help | About Discovery Attender
 - b. Note the bitness of Product Version of Discovery Attender on the Components screen.
4. [Uninstall](#) Discovery Attender using the Control Panel
5. Install the application using the setup executable with the appropriate **bitness** as noted in step 3.b above.
6. Restore application options
 - a. Restore Settings
 - i. Open Discovery Attender
 - ii. Cancel the license prompt
 - iii. Choose 'Main Console' from the initial Welcome dialog
 - iv. Navigate to Discovery Attender | Settings
 - v. Click the 'Import' button to import the Settings from the file created in step 1.a.ii above
 - vi. Close Discovery Attender
7. Copy Management Folder
 - a. Locate the Management folder saved in step 2.b above.
 - b. Replace the Management folder in the Installation directory with the one copied earlier.

You should now be ready to use Discovery Attender.

Uninstall

To un-install Discovery Attender, open the Control Panel and choose *Programs and Features*. From the list of programs, select Discovery Attender (which also may be listed as Discovery Attender for Exchange).

In some operating systems, there will be a 'Remove' button to start the installer. In others, double-clicking on the entry will start the installer. From the installer, choose 'Remove' and the installer will proceed to remove all files.

All information stored in the default application directory, as well as any Settings stored in the registry, will be deleted as part of the uninstall process. All existing projects and their associated searches are retained in their original directories.

Discovery Attender for SharePoint Component

If you have installed the optional Discovery Attender for SharePoint component on an on-premises SharePoint server, it can be uninstalled using the Programs and Features options from the Control Panel on the server where the component is installed. Select 'Remove' the setup utility will stop the service and uninstall all the components.

Microsoft 365 & EWS

Discovery Attender can search mailboxes, public folders and online archives via Exchange Web Services (EWS). This includes data stores located in Microsoft 365 or on-premises Exchange 2016 or above.

To access data in these repositories, Discovery Attender supports two protocols, [Basic Authentication](#) and [Modern Authentication](#).

Note: Microsoft has disabled **Basic Authentication** for all *online* tenants. Only Modern Authentication can be used if you are connecting to Microsoft 365. On-premises connectivity should not be affected.

Modern Authentication

oAuth or 'Modern Authentication' is a method of identity management that offers a more secure authentication and authorization for users and applications. It is replacing 'Basic Authentication' as an authentication model for all online tenants and should be seriously considered for on-premises environments or for its security enhancements.

The steps to set up Modern Authentication with Discovery Attender requires several steps:

- 1) [Create or obtain a self-signed certificate](#)
- 2) [Register Discovery Attender with Azure](#)
- 3) [Establish oAuth Application permissions](#)
- 4) [Configure Modern Authentication in Discovery Attender](#)

It is best if an Azure administrator familiar with these steps assists in the process.

Create a Self-signed Certification

A certificate is required as part of the process to register an application for oAuth in Azure. The steps below detail how to create a self-signed certificate.

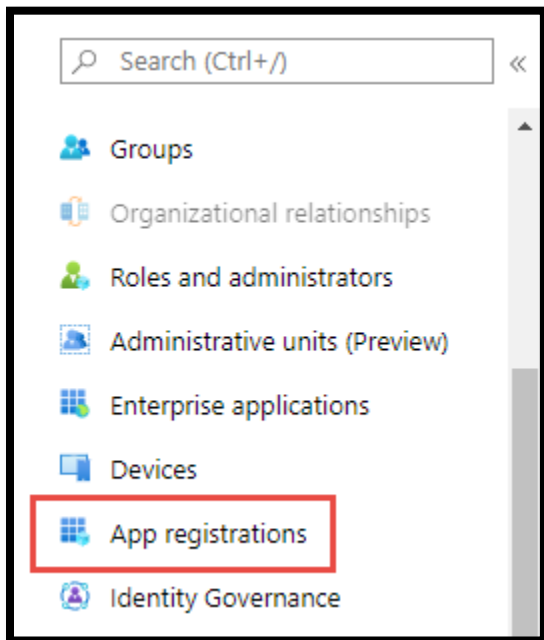
- 1) Contact [Technical Support](#) for a PowerShell script to automate the process.
- 2) Run PowerShell or PowerShell ISE as an Administrator, then navigate and open the provided script file.
- 3) Execute the script:
 - a. The first prompt will be the Common Name (CN) of the certificate. Please give the certificate an easily identifiable name like 'Discovery Attender oAuth'. Click 'Enter' to continue.
 - b. The second prompt will be the Start Date of the Certificate. Please enter the current date and click 'Enter'.
 - c. The third prompt is the End (or expiration) date of the certificate. Please choose this expiration according to your organization's policy, but at least a year or two is advisable. Click 'Enter' to continue.
 - d. The fourth prompt will be a dialog box asking for a password. This password will be used in later steps, please ensure you remember it. Click 'OK' to create the certificate.
 - e. The certificate will be exported to the SYSTEM32 folder of the local machine.
 - f. There are two certificates. They will have the name from step (a). One ends with **.pox**, the other with **.cer**. Copy both certificate files to a safe location. They will be used during the Azure registration process.

Application Registration Process

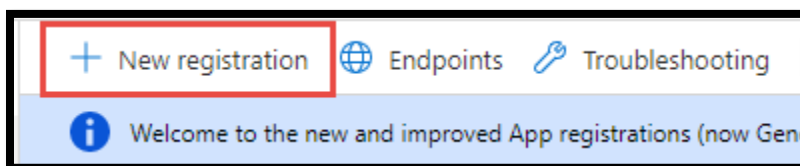
This step is essential for registering Discovery Attender to be able to use Modern Authentication within your organization. You will need your organization's portal credentials before you can continue.

Note: Despite our efforts to keep up to date, Microsoft can and does change the interface for the Azure Portal. The directions below are meant to give a general idea of the process registering an application in Azure.

- 1) Log into the Azure portal (<https://portal.azure.com/>).
- 2) Select 'Azure Active Directory'
- 3) Navigate to the App Registrations node.

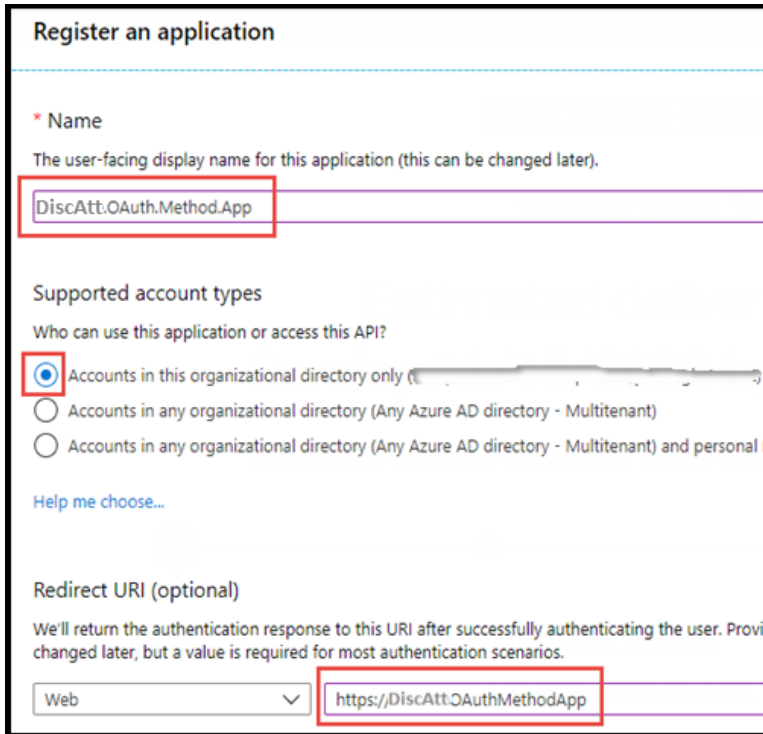


- 4) Click on the 'New registration' button:



- 5) In the 'Register an application' form, enter the following information.
 - a. *Name*: This is a user facing name. We recommend something like **DiscoveryAttender.oAuth.App** to easily identify the program.
 - b. *Supported Account Types*: Choose the appropriate value (most likely '*Accounts in this organizational directory only*').
 - c. *Redirect URI*: NOTE: This URI is ***not*** optional for our registration process
 - i. From the first drop-down, make sure 'Web' is selected.
 - ii. In the text box, enter the URI if not already auto-generated.

- d. Click 'Register' to complete. You will now set up the permissions for the applications.



Register an application

*** Name**
The user-facing display name for this application (this can be changed later).
DiscAtt.OAuth.Method.App

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Tenant ID: [redacted])
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Outlook.com, Hotmail.com, Gmail.com)
[Help me choose...](#)

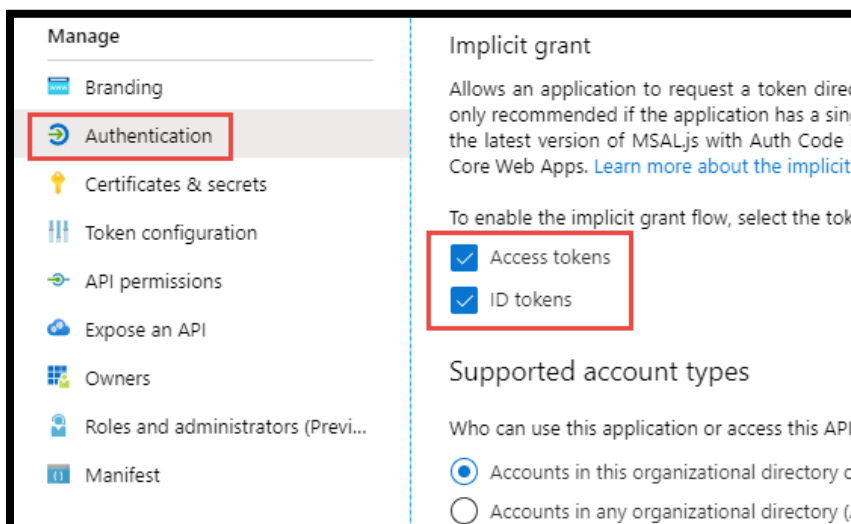
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Provide a value here, or change it later. A value is required for most authentication scenarios.
Web

Note: Please make sure to make note of the 'Application (client) ID' and 'Directory (tenant) ID'. These values will be needed in the application setup.

Establish oAuth Application Permissions

The section details the steps that must be taken in the Azure Active Directory administration portal to register the oAuth service, make it available, and assign the appropriate application permissions.

- 1) Select 'Authentication'.
- 2) Enable both the 'Access tokens' and 'ID token' option under the **Implicit grant** section:



Manage

- Branding
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators (Previous version)
- Manifest

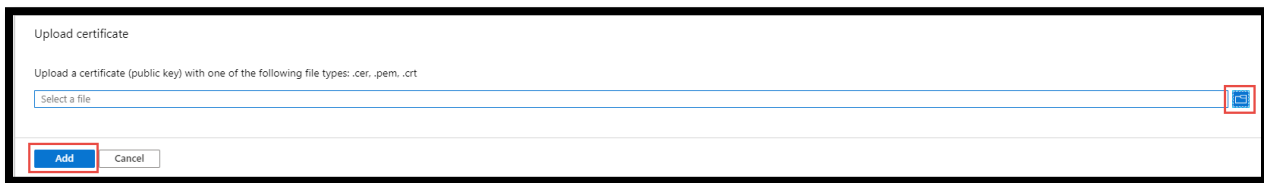
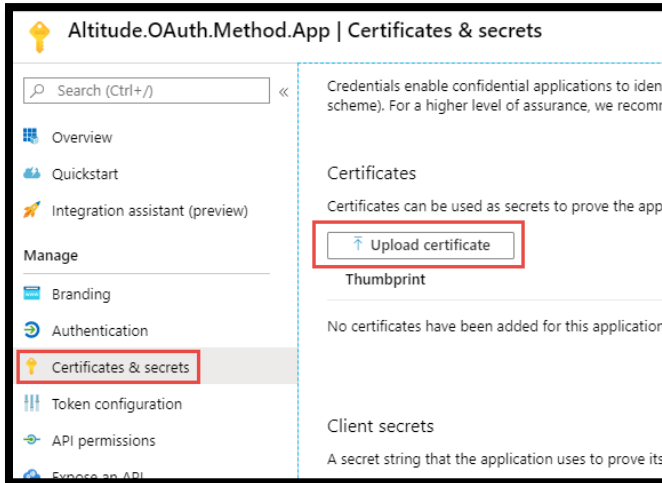
Implicit grant
Allows an application to request a token directly from the identity provider. This is only recommended if the application has a single user and is using the latest version of MSAL.js with Auth Code Flow for Desktop or Core Web Apps. [Learn more about the implicit grant flow.](#)

To enable the implicit grant flow, select the tokens you want to issue:

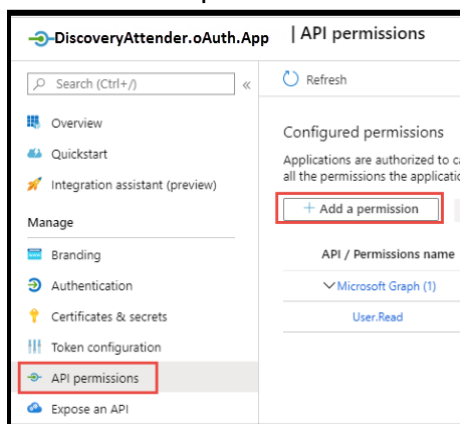
- Access tokens
- ID tokens

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Tenant ID: [redacted])
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)

- 3) Select the **Certificates & secrets** node.
- 4) Click 'Upload certificate'.
- 5) Navigate to the folder path where the certificate you created in the [earlier step](#) is stored. Choose the file with the extension of (.cer). Click the **Add** button to continue.



- 6) Add Permissions to the registered application:
 - a. Select 'API Permissions'
 - b. Click on 'Add a permission'



- c. 'Click on 'APIs my organization uses'.
- d. Type 'Office 365' in search bar and hit enter.

- e. Click on the 'Office 365 Exchange Online' option

Request API permissions ×

Select an API

Microsoft APIs **APIs my organization uses** My APIs


Apps in your directory that expose APIs are shown below

Name	Application (client) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f3f02c9-5679-4a5c-a605-0de55b07d135
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2
Office 365 Search Service	66a88757-258c-4c72-893c-3e8bed4d6899
Office 365 SharePoint Online	00000003-0000-0ff1-ce00-000000000000

- f. Select the 'Application permissions' option.
- g. Enable the 'full_access_as_app' check box.
- h. Check 'Exchange.ManageAsApp' checkboxes.

Request API permissions ×

[< All APIs](#)

 Office 365 Exchange Online
<https://ps.outlook.com>

What type of permissions does your application require?

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

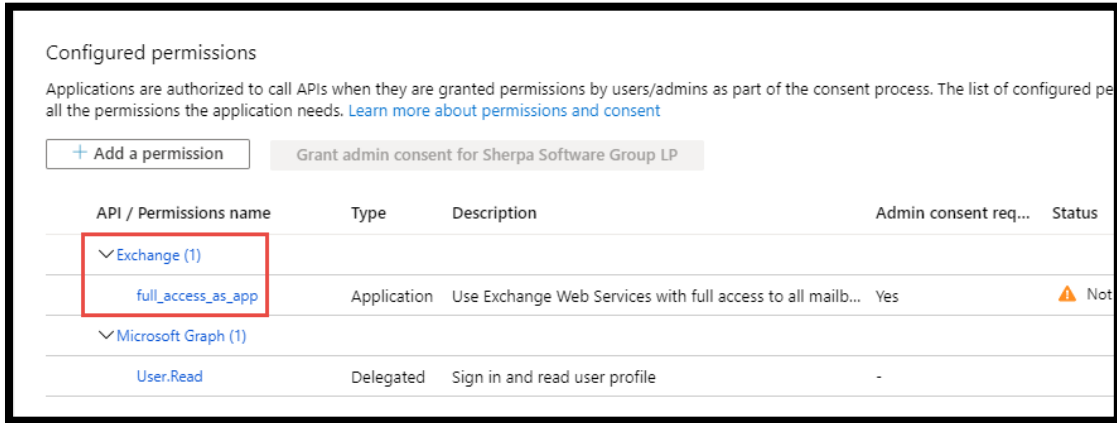
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Permission	Admin consent required
Other permissions (1)	
<input checked="" type="checkbox"/> full_access_as_app ⓘ Use Exchange Web Services with full access to all mailboxes	Yes
Exchange (1)	
<input checked="" type="checkbox"/> Exchange.ManageAsApp ⓘ Manage Exchange As Application	Yes

- i. Click 'Add Permissions' button

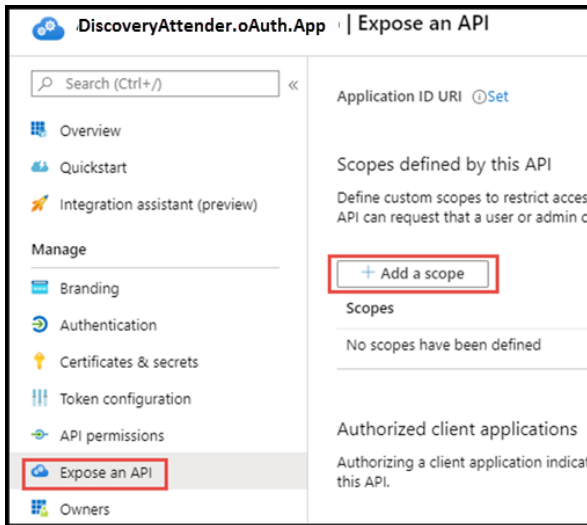
j. The Exchange configured permissions should resemble this form:



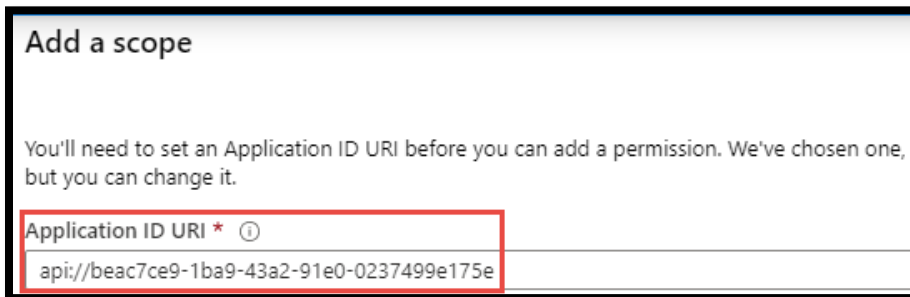
- k. Click the 'Grant admin consent for [your company]' (to the right of the 'Add a permission' box).
- l. Confirm the status of both API permissions. It should now show a green checkmark indicating that admin consent has been granted.

7) Add the scope to expose the API for the registered application

a. Select 'Expose an API' from the registered app options screen



b. Choose 'Add a Scope'

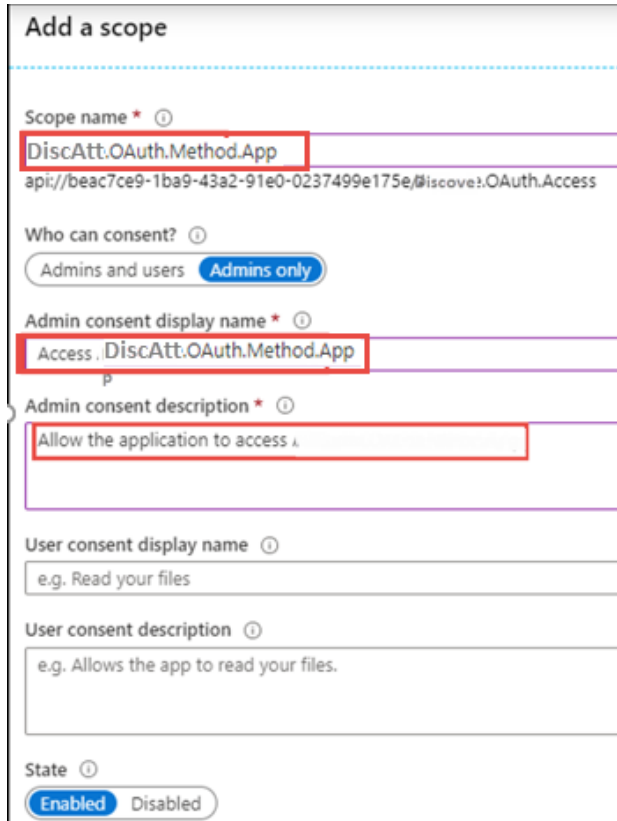


c. The 'Application ID URI' window will pre-fill with the application id. This value is needed to configure Discovery Attender's 'Client ID' value. Store this id for future use.

- d. Click Save and Continue to proceed.



- e. Fill out the highlighted fields in the 'Add a Scope' window.



Add a scope

Scope name * ⓘ
DiscAtt.OAuth.Method.App
api://beac7ce9-1ba9-43a2-91e0-0237499e175e/#scope!.OAuth.Access

Who can consent? ⓘ
Admins and users Admins only

Admin consent display name * ⓘ
Access . DiscAtt.OAuth.Method.App

Admin consent description * ⓘ
Allow the application to access .

User consent display name ⓘ
e.g. Read your files

User consent description ⓘ
e.g. Allows the app to read your files.

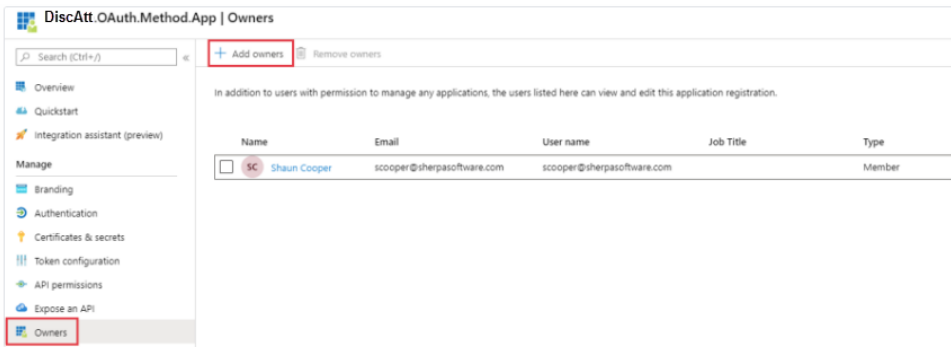
State ⓘ
Enabled Disabled

- f. Click the 'Add Scope' button to proceed.



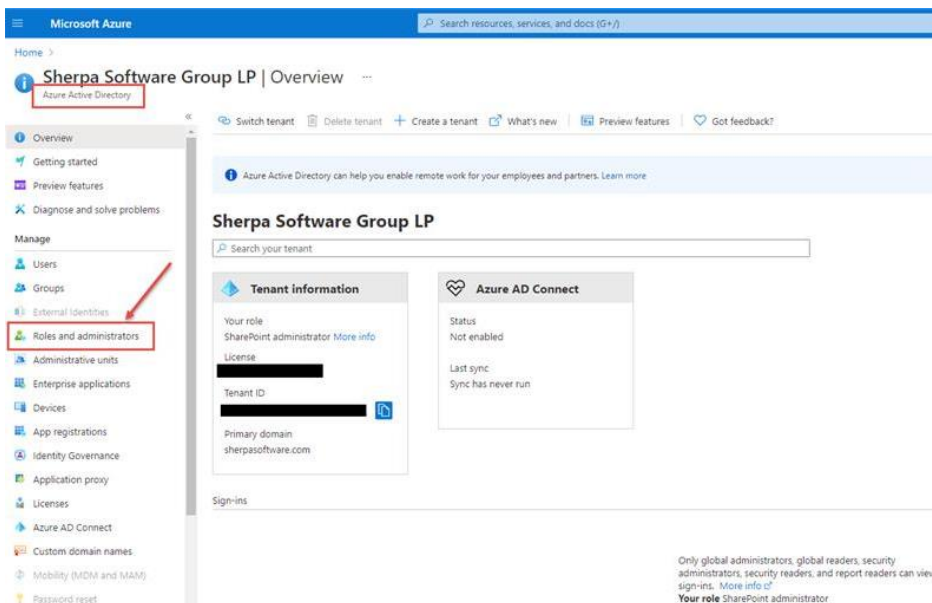
- 8) Assign owners to the application if additional users need to have access to manage the application or edit the application registration. This step is optional.
 - a. Choose the 'Owners' node
 - b. Click the 'Add Owners' option.

c. Select and Add any additional owners

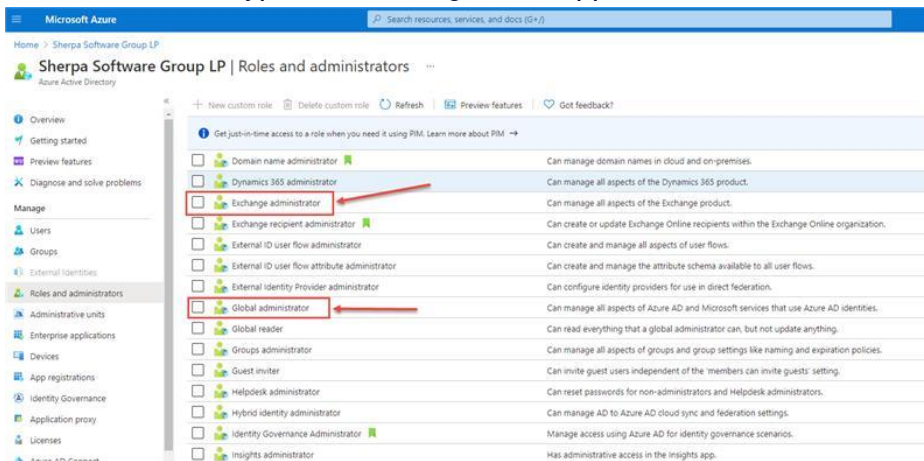


9) Configure Roles and Administrators for the registered application.

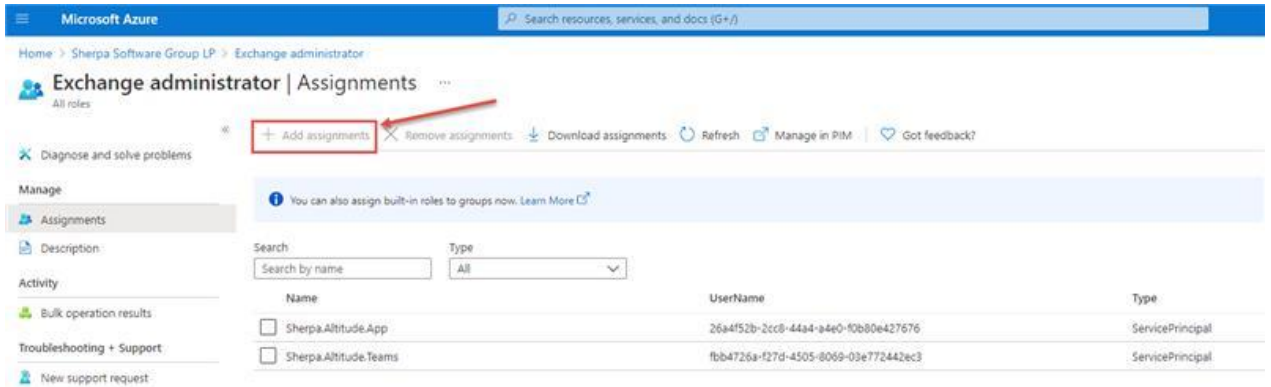
- a. For this step you will need to return to the main Azure dashboard. Once there, click on link for "Roles and Administrators".



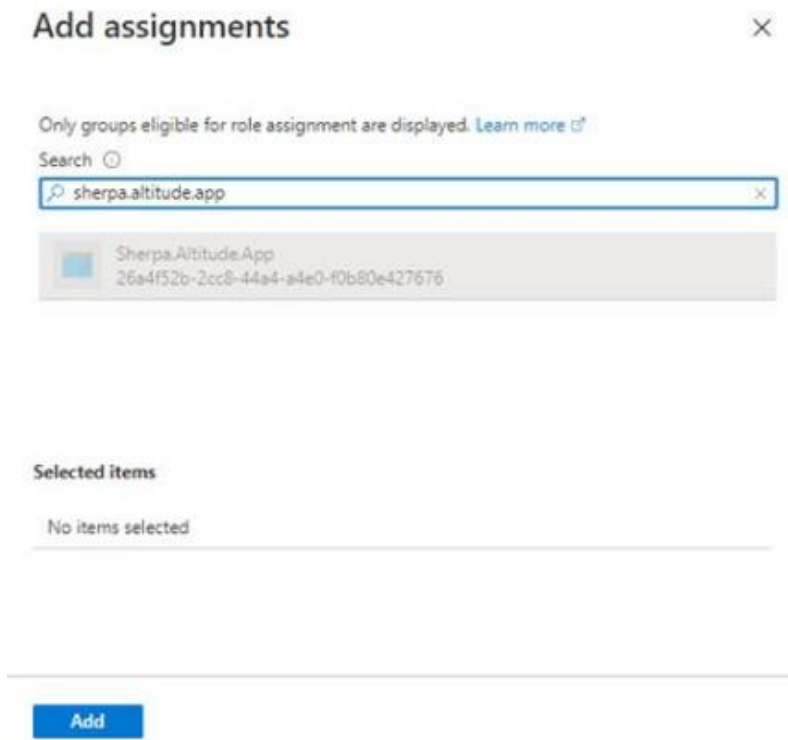
- b. Select 'Exchange administrator' or 'Global administrator'. Either role will work, but Exchange Administrators is typical for the registered app to use.



- c. After selecting a role, click Assignments then select 'Add Assignments' and search for the registered app:



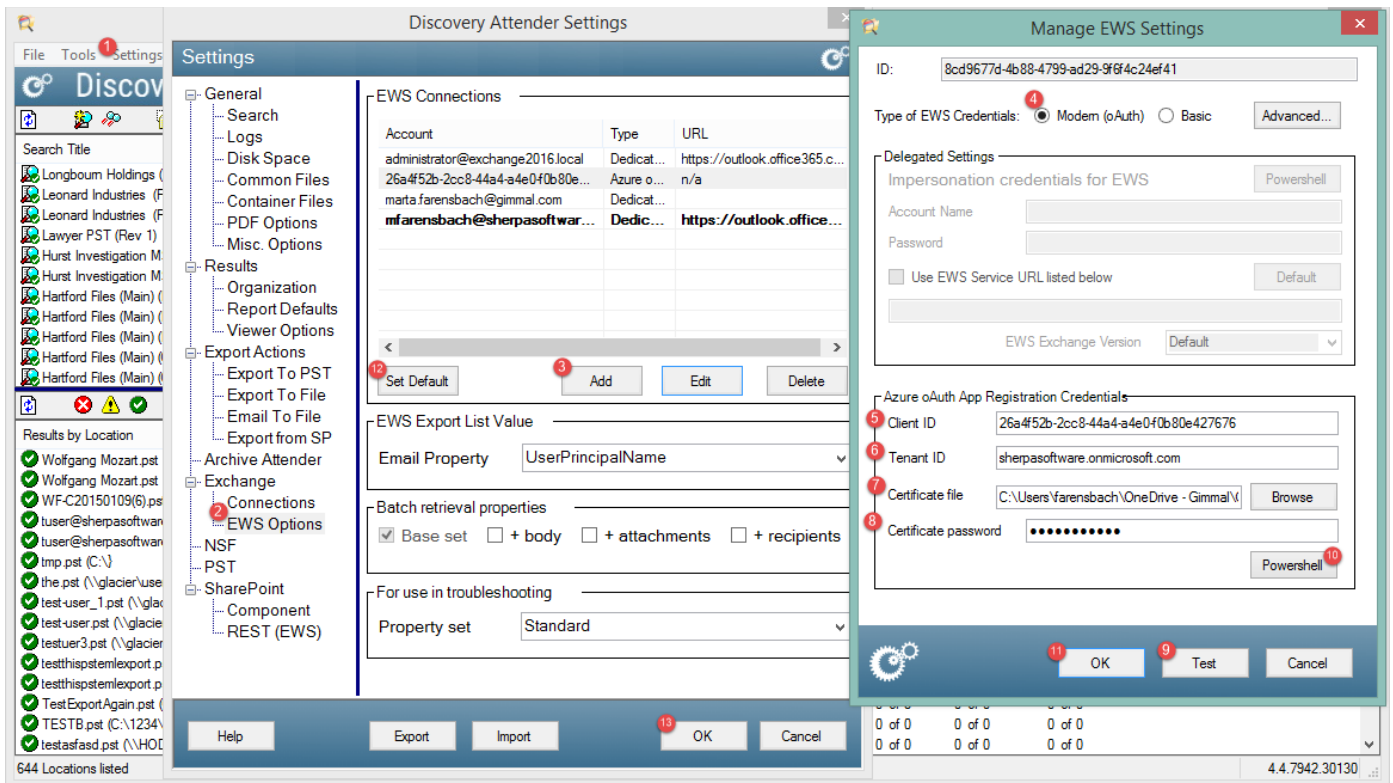
- d. Type the name of the registered app and click the 'Add' button at the bottom



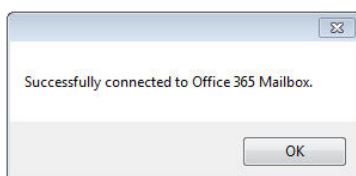
- e. For more information on modern authentication role permissions, please refer to this Microsoft post:
<https://docs.microsoft.com/en-us/powershell/exchange/app-only-auth-powershell-v2?view=exchange-ps#step-5-assign-azure-ad-roles-to-the-application>

Configure Discovery Attender with Modern Authentication (oAuth)

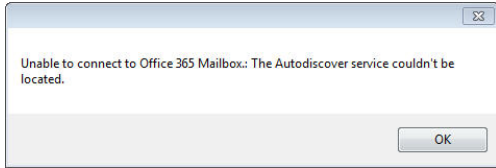
Once the steps for registering the application have been completed, Discovery Attender will need to be configured with the credentials you (or your Azure administrator) have established in the steps above.



1. From the Discovery Attender console, select *Settings*.
 2. Navigate to the *Exchange / EWS Options* node.
 3. Click the 'Add' button.
 4. Choose the 'Modern (oAuth)' option.
 5. Enter the *Client ID*. This is the 'Application (Client) ID' value from the [Register an App](#) step above.
 6. Enter the *Tenant ID*. This is the 'Directory (Tenant) ID' value from the [Register an App](#) step above.
 7. Navigate and select the certificate file generated in the [certificate creation step](#) above.
- Note: this cert file has an extension of (.pfx), NOT (.cer).
8. Enter the *Certificate password* which was used in the [certificate creation step](#) above.
 9. Use the *Test* button to verify permissions and connectivity:

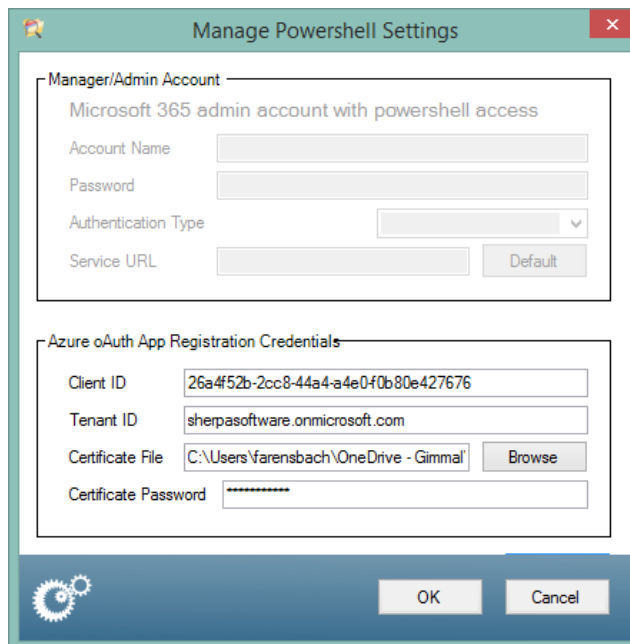


If the test fails, a pop up will display the reason:



If the connectivity issues are not obvious, please contact [Technical Support](#) for additional assistance.

10. The optional 'PowerShell' button accesses a feature to create a list of mailboxes to choose from when creating a search. The *Manager/Admin Account* section uses an account to create a list of EWS data stores via PowerShell. This output is used in conjunction with the 'List' options in the wizard selection pages to populate the list of mailboxes or online archives.

A dialog box titled "Manage Powershell Settings" with a close button. It contains two sections: "Manager/Admin Account" and "Azure oAuth App Registration Credentials". The "Manager/Admin Account" section has fields for "Account Name", "Password", "Authentication Type" (a dropdown menu), and "Service URL" (with a "Default" button). The "Azure oAuth App Registration Credentials" section has fields for "Client ID" (containing "26a4f52b-2cc8-44a4-a4e0f0b80e427676"), "Tenant ID" (containing "sherpasoftware.onmicrosoft.com"), "Certificate File" (containing "C:\Users\Yarensbach\OneDrive - Gimmel" with a "Browse" button), and "Certificate Password" (with a masked password field). At the bottom are "OK" and "Cancel" buttons.

- In most situations, the 'Azure oAuth App Registration Credentials' to run PowerShell scripts should match the Modern Authentication credentials from the previous screen.
- Click the 'Export' button to start generation of the list.
- Be aware that it can take a significant amount of time for the list to generate in larger environments.
- Please establish connectivity to mailboxes first, before trying this feature.

11. Click 'OK' on the *Manage EWS Settings* screen to save the values established above.

12. If this account is the only one you will be using, or if the account is the *primary* account you will be using, highlight the account and select 'Set Default'. This will save many steps when setting up searches in the future.

13. If you have a hybrid environment or need to use multiple accounts, add each one individually. When finished, click the 'OK' button.

Don't hesitate to contact [Technical Support](#) with any questions for working with M365 and EWS.

Basic Authentication

To access data using Basic Authentication (aka Delegated or Impersonated access), two steps need to be taken.

First, the [appropriate application impersonation rights](#) need to be established within the Exchange environment. This grants permission to search the desired data stores.

Second, the correct credentials and connectivity need to be [configured in the Discovery Attender console](#). Gimmel recommends selecting an administrative account (mailbox) that has been granted application impersonation rights to access the user mailboxes that need to be searched.

Note: Microsoft has [announced](#) they are disabling Basic Authentication for all online tenants by October 2022. You **must** use [Modern Authentication](#) if you are connecting to Microsoft 365 and it is strongly advised for on-premises authentication.

Establish Application Impersonation Rights

There are several ways to establish application impersonation rights, including the [Exchange Management Console](#) and [Exchange Management Shell \(PowerShell\)](#).

Exchange Management Console

Note: Despite our efforts to keep up to date, Microsoft can and does change the interface for the Exchange Management Console. The directions below are meant to give a general idea of the process of assigning application impersonation rights to a specified account or group.

1. Log into the Microsoft portal as an administrator (<http://portal.microsoftonline.com>)
2. Choose 'Exchange' to open the 'Exchange admin center'
3. Select the 'Permissions' node, choose 'Admin Roles'
4. Under roles, select '*DiscoveryManagement*' (a predefined role).
Note: Alternately, you can create a new role group.
5. Under the 'Roles' section of your role group, click the plus (+) sign and select '*ApplicationImpersonation*'
6. Under the 'Members' section of the role group, select the account or group that will be used for searching and add it as a member of the '*ApplicationImpersonation*' role.
7. After these steps, your account or group should have requisite impersonation rights to run searches in Discovery Attender. Continue to Configure Discovery Attender section below.

Exchange Management Shell (PowerShell)

Please follow the steps outlined below to configure the administrative mailbox with application impersonation rights. If you are not familiar with running PowerShell, please use the 'Console' option (above).

Note: These directions assume that you are assigning the application impersonation permissions to a pre-defined role. If you are assigning them to a group or individual, please use the 'Console' option.



Discovery Attender 4.x

1. Launch Windows PowerShell and execute the following command to supply the credentials to open a session to EWS or Microsoft 365:

```
$LiveCred = Get-Credential
```

When prompted, enter the credentials for the account that will have administrative application impersonation privileges in Microsoft 365 / EWS.

2. Execute the following command to open a new session:

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri  
https://ps.outlook.com/powershell/ -Credential $LiveCred -Authentication Basic -  
AllowRedirection
```

3. Import the session to retrieve the PowerShell commands by running the following script:

```
Import-PSSession $Session
```

4. Next, to grant this administrative account impersonation rights over all of the users' mailboxes run the following command:

```
New-ManagementRoleAssignment -Name "[My Role Name]" -Role "ApplicationImpersonation" -  
User [Administrative account]
```

where [My Role Name] is the name you assign this role and [Administrative Account] is the email address of the administrative account that will be used to access the user mailboxes.

Here is an example: *New-ManagementRoleAssignment -Name "MA-Impersonation" -Role "ApplicationImpersonation" -User administrator@gimmalsoftwaresample.com*

For more information on application impersonation in Exchange, please refer to these Microsoft technical notes:

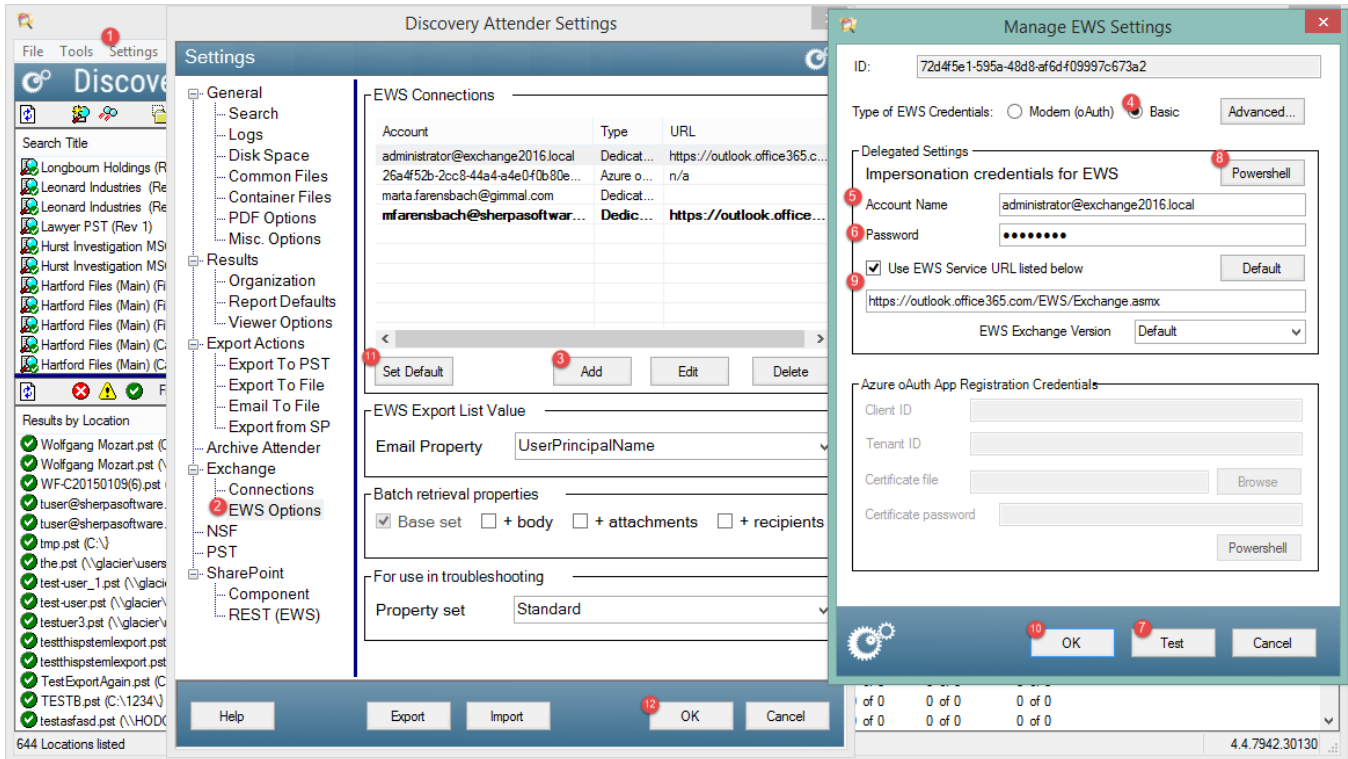
<https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-configure-impersonation>

<https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/impersonation-and-ews-in-exchange>

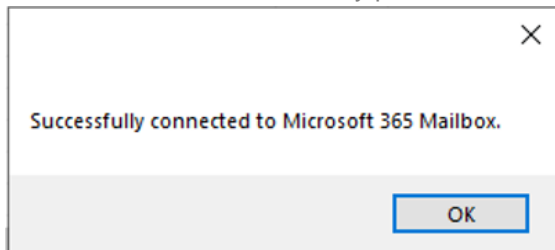
Configuring Discovery Attender for EWS (Microsoft 365) Basic Authentication

Once the impersonation account has been established and permissions granted in Exchange, the credentials need to be entered into Discovery Attender's settings after the program has been installed.

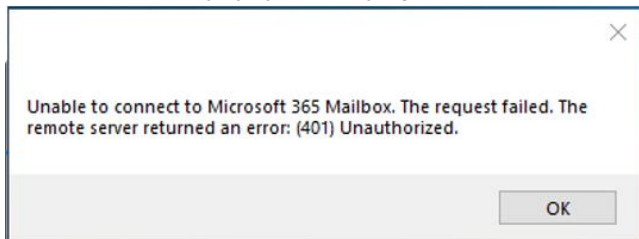
1. From the Discovery Attender console, select *Settings*.
2. Navigate to the *Exchange | EWS Options* node.
3. Click the 'Add' button.
4. Choose the 'Basic' option.



5. Enter the *Account Name*. This should be the account which was granted *ApplicationImpersonation* privileges in the [steps above](#).
6. Enter the password associated with the *Account Name*.
7. Use the *Test* button to verify permissions and connectivity:

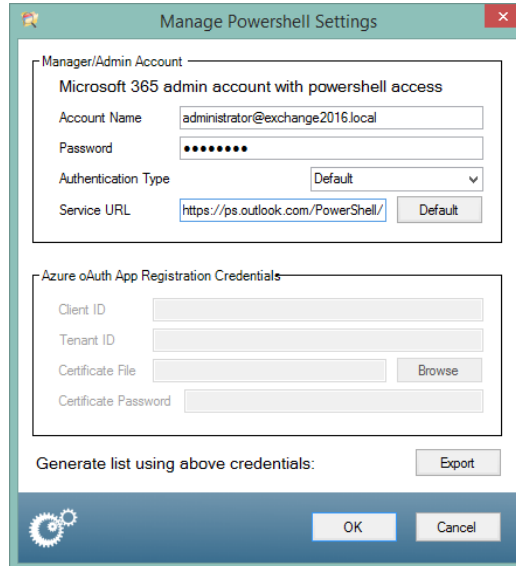


If the test fails, a popup will display the reason:



If the connectivity issues are not obvious, please contact [Technical Support](#) for additional assistance.

8. The optional 'PowerShell' button accesses a feature to create a list of mailboxes to choose from when creating a search. The *Manager/Admin Account* section uses an account to create a list of EWS data stores via PowerShell. This output is used in conjunction with the '*List*' options in the wizard selection pages to populate the list of mailboxes or online archives.



- The *Account Name* entered in this section must have permissions and connectivity to local PowerShell *and* M365 Exchange PowerShell to run effectively.
- Click the 'Export' button to start generation of the list.
- Be aware that it can take a significant amount of time for the list to generate in larger environments.
- Do **not** change the *Email Property*, *Authentication Type* or *Service URL* properties unless directed to do so by [Technical Support](#).
- Please establish connectivity to mailboxes first, before trying this feature.

9. Note: If you are having trouble establishing connectivity, it is possible that the EWS Service URL in your current environment differs from the default values. This can be the case in a number of situations, including hybrid environments. For further assistance, please contact [Technical Support](#).

10. Click 'OK' on the *Manage EWS Settings* screen to save the values established above.

11. If this account is the only account you will be using, or if the account is the *primary* account you will be using, highlight the account and select 'Set Default'. This will save many steps in the future.

12. If you have a hybrid environment or need to use multiple accounts, add each one individually. When finished, click the 'OK' button.

Discovery Attender for SharePoint

SharePoint searching is a separately licensed, optional module used to search data stored in SharePoint sites. There are two methods for searching SharePoint:

- Rest protocol which can search all versions of SharePoint from 2016 and above, on-premises or cloud. This is the preferred protocol and can be run with basic or modern authentication.
- A component which runs as a service directly installed in the SharePoint Farm. This is for on-prem SharePoint 2013 or 2016 only. This should only be used if Rest is not available.

SharePoint REST (EWS)

The REST (EWS) protocol allows for the direct searching of sites and lists. Permissions will still need to be established.

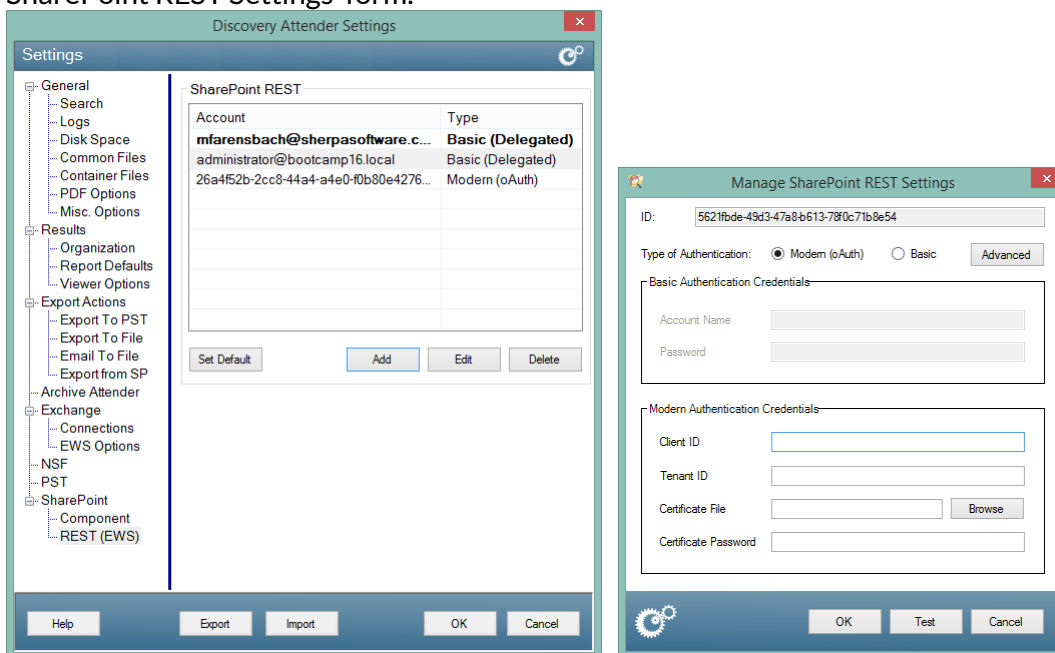
Discovery Attender supports both Basic and Modern Authentication to search SharePoint, however there are limitations. For on-prem services, only Basic (delegated) Authentication is supported. Discovery Attender prefers Modern Authentication for searching online SharePoint.

Modern Authentication

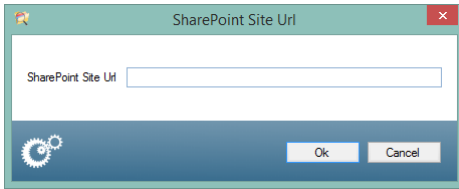
Only online SharePoint data stores can be searched with Modern Authentication. Please see the section for '[Modern Authentication](#)' above for important notes and information for establishing permissions. Once you have established permissions, use the following steps to configure Discovery Attender.

Note: Discovery Attender cannot use Modern Authentication to search on-premises SharePoint servers.

1. Navigate to the Settings | SharePoint | REST (EWS) node and select 'Add' to open the 'Manage SharePoint REST Settings' form.



2. Choose the 'Modern (oAuth)' option.
3. Enter the *Client ID*. This is the 'Application (Client) ID' value from the [Register an App](#) step above.
4. Enter the *Tenant ID*. This is the 'Directory (Tenant) ID' value from the [Register an App](#) step above.
5. Navigate and select the certificate file generated in the [certificate creation step](#) above. Note: this cert file has an extension of (.pfx), NOT (.cer).
6. Enter the *Certificate password* which was used in the [certificate creation step](#) above.
7. Use the *Test* button to verify permissions and connectivity by entering a value in the 'SharePoint Site URL' that you wish to search and then clicking 'OK'



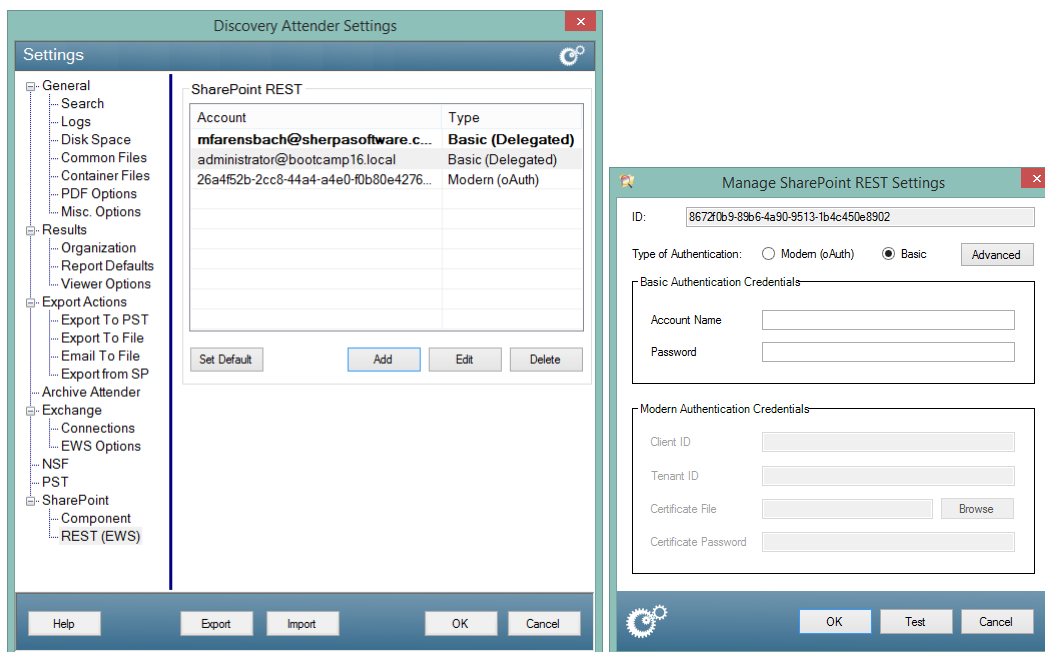
A message will appear to verify the connection or inform you of a failure to connect.

8. Click 'OK' on the *Manage SharePoint REST Settings* screen to save the values established above.
9. If this account is the only one you will be using, or if the account is the *primary* account you will be using, highlight the account and select 'Set Default'. This will save many steps when setting up searches in the future.

Basic Authentication

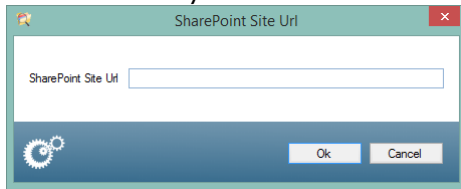
Delegated or 'Impersonated' permissions use an established account which has access to the SharePoint sites you need to search. In Discovery Attender, it can only be used to connect to on-premises SharePoint data sources. Use the account given to you by the SharePoint administrator to populate the requisite fields.

Note: Microsoft has disabled Basic Authentication for all online tenants. Please use Modern Authentication if you are connecting to Microsoft 365.



1. Navigate to the Settings | SharePoint | REST (EWS) node and select 'Add' to open the 'Manage SharePoint REST Settings' form.
2. Select 'Basic'.
3. Enter the 'Account Name' and 'Password' provided by your SharePoint administrator.

4. Use the *Test* button to verify permissions and connectivity by entering a value in the 'SharePoint Site URL' that you wish to search and then clicking 'OK'



A message will appear to verify the connection or inform you of a failure to connect.

5. Click 'OK' on the *Manage SharePoint REST Settings* screen to save the values established above.
6. If this account is the only one you will be using, or if the account is the *primary* account you will be using, highlight the account and select 'Set Default'. This will save many steps when setting up searches in the future.

SharePoint Component

The Discovery Attender for SharePoint service which is used by the component only runs with on-premises SharePoint 2013 and above. See the notes and directions below regarding this component *only*. If using the Rest protocol, please consult the included help document.

- Never install the *Discovery Attender for SharePoint* service on a machine running mission critical applications without testing it first. The component is very CPU intensive and can negatively affect the processing of other programs.
- SharePoint searches are created using the search wizard in the main Discovery Attender console. However, the actual search processing is done via the SharePoint service.
- The SharePoint service is managed through the main Discovery Attender installation under *Tools | Settings | SharePoint*.
- Pending results are stored on the server where the SharePoint component is installed. Once these results are transferred and saved to the main Discovery Attender installation, they are deleted from the SharePoint server.
- Results are stored, managed and exported using the main Discovery Attender console.
- The main Discovery Attender installation should not be installed on a SharePoint server.

Permissions

Full permission to the sites included in the searches is required for the SharePoint service to run effectively. Please contact your SharePoint administrator with any questions on creating an account with proper access on the specified SharePoint farms.

Where to Install

- The *Discovery Attender for SharePoint Service* must be installed on a SharePoint server that is a member of the SharePoint farm that is being searched.
- Processing of data is done through the service installed on the SharePoint server. Pending results are stored on the server while before and during processing. Therefore, the machine where this service component is installed should have sufficient bandwidth, CPU, hard drive space and memory to conduct searches.
- Only SharePoint 2013 or above can be searched. Older versions of SharePoint are not supported.

- To search data located in SharePoint stores, the .Net 4.8 (or above) framework is required to be present on the same machine where the component is installed. The .Net 4.8 version can be found [here](#).

Installation Guide

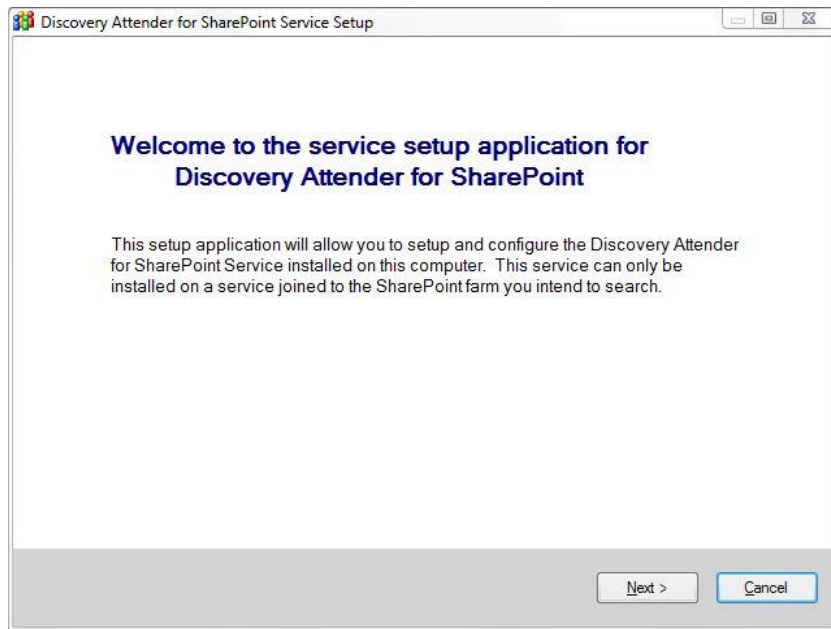
The following are steps to install the SharePoint component.

1. Choose the server where you wish to install the Discovery Attender SharePoint Service.
 2. Double-click the setup file to begin the installation of the Discovery Attender for SharePoint Service.
- Please note: The proper version of the .Net framework is required for the SharePoint service to function correctly. If it is not installed, you will receive an error message.
3. Follow the screens as prompted. You must accept the Discovery Attender License Agreement to continue with the installation.
 4. Select the Complete Install, (the Custom only gives the SharePoint service component option), then choose the destination folder to install the component files.
 5. The setup will execute, installing the required components in the chosen directory.
 6. Once the setup is complete, the Discovery Attender for SharePoint Service configuration wizard will begin.

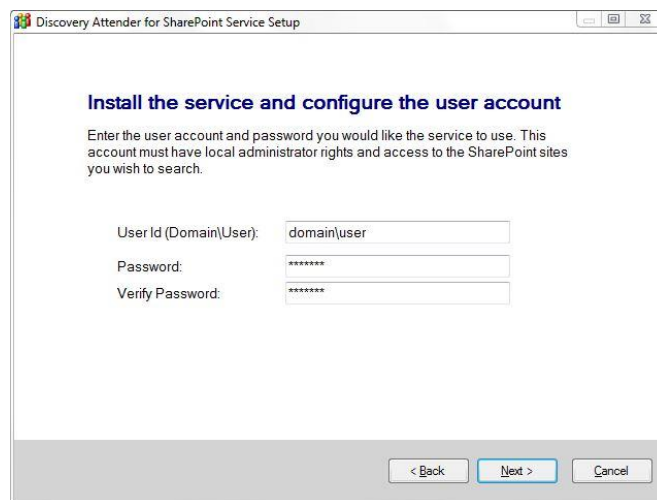


Configuration Wizard for Discovery Attender for SharePoint

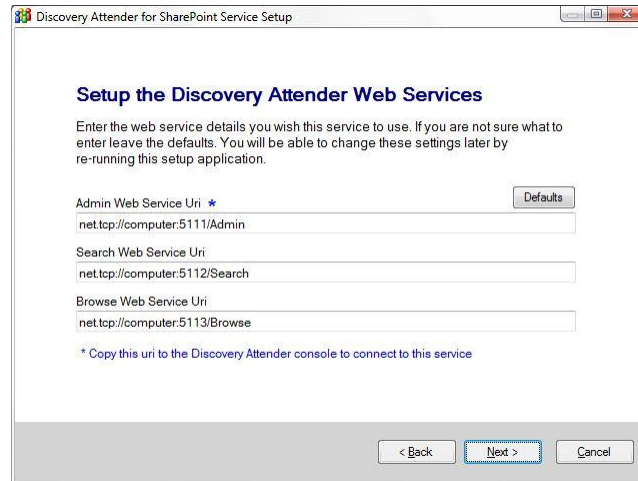
1. Once the installation is complete, the Discovery Attender for SharePoint Service configuration wizard will begin.



2. Enter the user account details that will be used by the Discovery Attender for SharePoint Service. Please verify this account has the proper permissions to the sites that need to be searched.

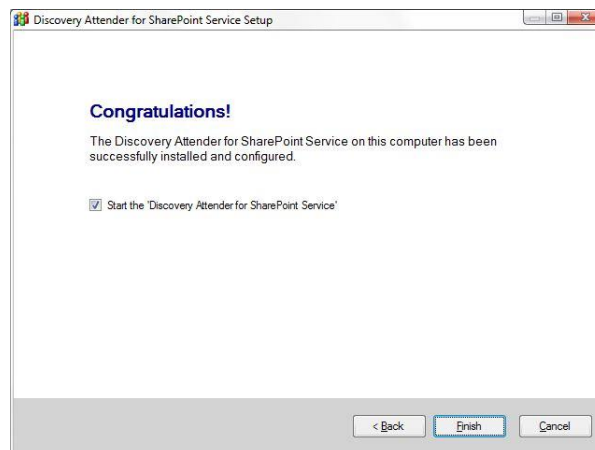


3. Enter the web service URI (Uniform Resource Identifier) for this service to use to communicate with Discovery Attender. In most situations, the default values will be used. If unsure about the options, leave the defaults.



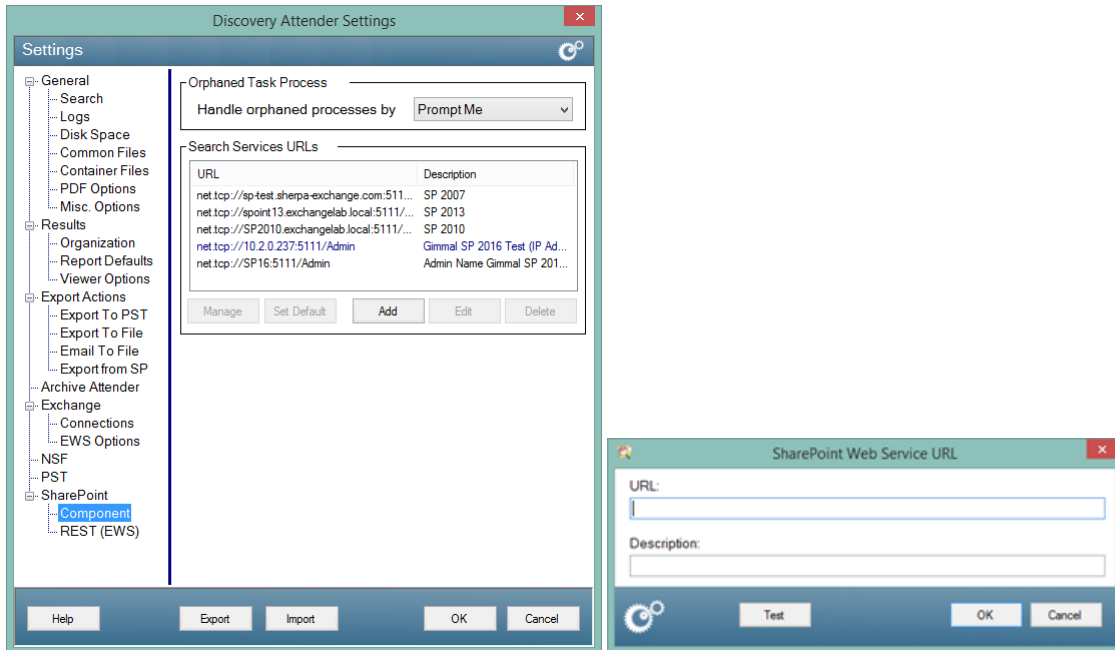
Note: Store the Admin Web Service URI details for future use as this data needs to be entered into the Discovery Attender *Main Console* (see below) for successful processing of SharePoint files.

4. Once the URI details are entered, setup is complete and the service can be started by clicking 'Finish'.



The *Discovery Attender for SharePoint* component installation is now complete on the SharePoint server. However, Settings need to be enabled in the main console before searching can commence.

1. Open Discovery Attender on the machine where it is installed (i.e. *not* the SharePoint server).
2. Enter the SharePoint license key (see *License Key* section below). A valid SharePoint license key will enable the SharePoint options in the settings and wizard screen screens.
3. Open the *Settings* screen. This can be reached from *Tools | Settings* in the Main Console.
4. Navigate to the SharePoint node and verify the 'Wizard Show Options' is enabled.
5. Choose the 'Components' node and click 'Add' to enter a new 'Search Service URL'.

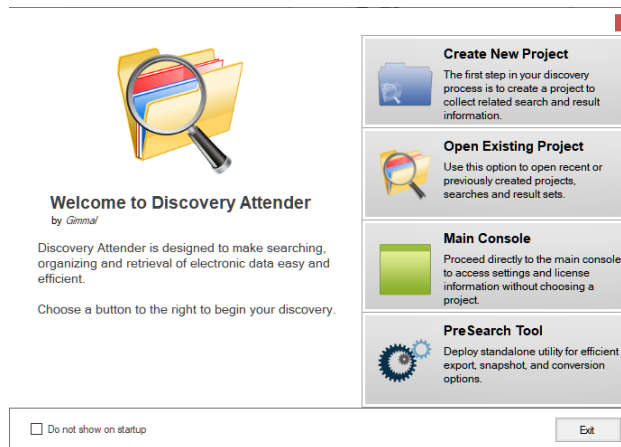


6. The correct '*Admin Web Service Uri*' address chosen in the *Discovery Attender or SharePoint Service* configuration wizard (*Step 3* of the configuration wizard setup [above](#)) needs to be entered into SharePoint WebService URL before SharePoint can be searched successfully.

Be sure to use the 'Test' button to verify you have access and connectivity to the SharePoint server. If the connection cannot be opened, please recheck the address to ensure it has been entered correctly. If you still are experiencing issues, verify the service is running on the SharePoint server.

7. Click 'OK' to include the *Admin Web Service URI* address in the *SharePoint Web Service URL* list. The *Description* is to help you identify the server if you have multiple entries.
8. Once the connection is established and tested, you will be able to search your SharePoint data stores with a variety of wizard and result options.

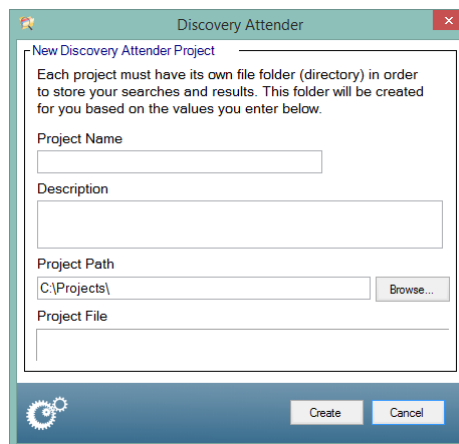
Where to Begin



The Discovery Attender interface is designed to be intuitive and user friendly. The Welcome Screen (above) serves as the gateway to the product. From here you can [create a project](#) to start searching . A project serves as a repository for a collection - related searches and associated result sets. Once a new project is created, the [Main Console](#) acts as the central hub to allow you to control the creation, processing, and organization of searches. From the Main Console, you can access [the Search Wizard](#) which guides you through the step-by-step process of creating a new search. The Main Console also provides access to the [Result Management](#) features to view, organize, export and report on the messages, attachments and files that are found during your searches.

Create Project

Discovery Attender organizes related searches and results in containers called Projects. When you first open Discovery Attender, you can choose to create a new project or select one from a list of existing projects.



Creating a new project performs several tasks. First, a new project directory is created using the project name. Housed under this directory is all the project related information including searches, databases, results, logs and more. Make sure the location you select has sufficient space to store this data.

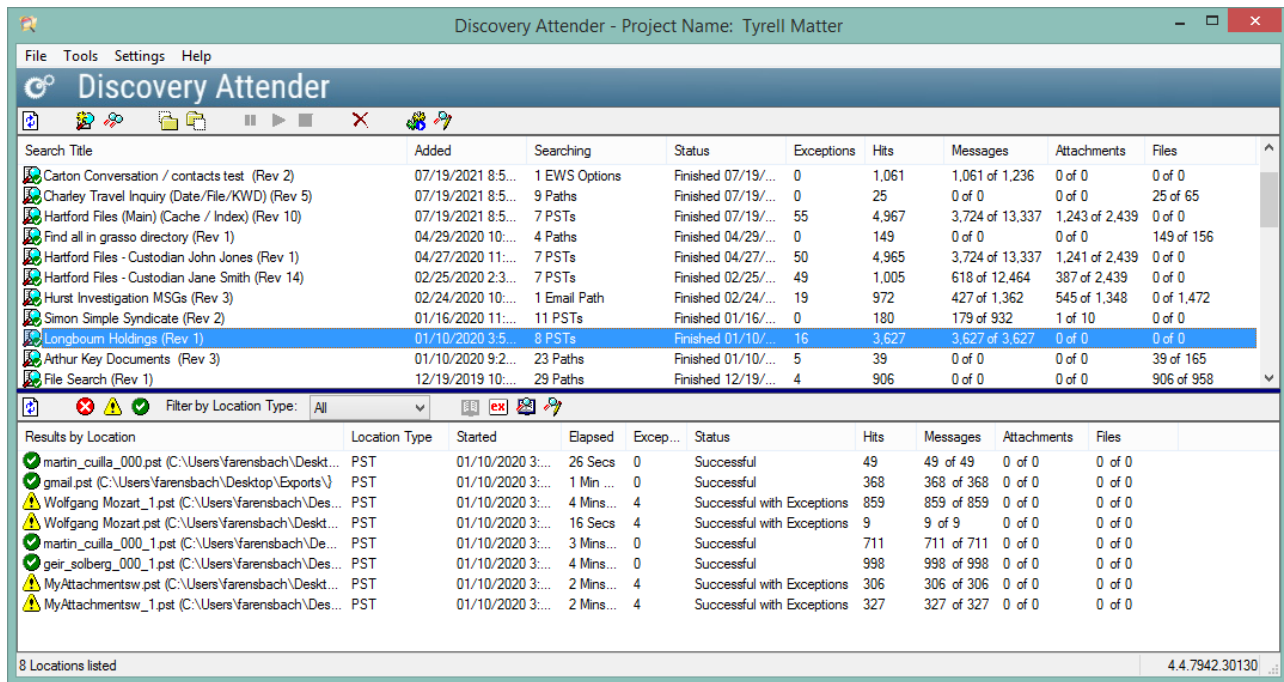
To create a project, choose a location to store the project under Project Path, and then select a Project Name. The default location is *C:\Projects*. However, you may want to store your projects in an alternate

location that is more convenient or has more storage capacity. Please ensure the length of the project path does not exceed 100 characters.

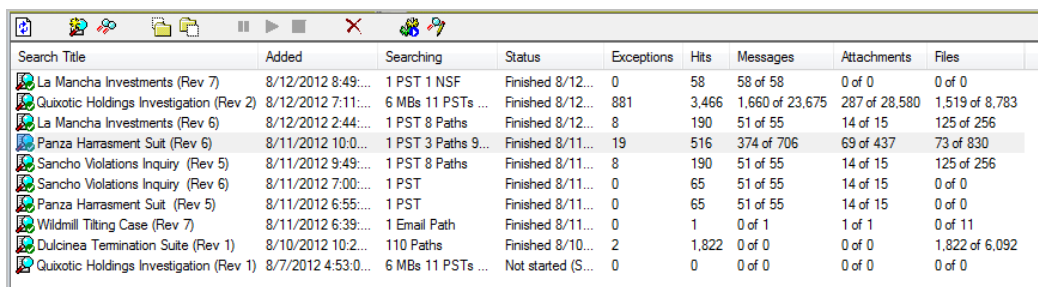
Click the **Create** button to create the project file, project folder and the default folder path structure for the project. Click **Cancel** if you do not want to create a project at this time. Please note, you cannot create or run searches without a project container.

Manage Searches (Main Console)

The main console allows you to create and manage your searches. It contains a summary of your searches and serves as the gateway for most Discovery Attender functionality. You can start new searches, modify existing searches, cancel searches, or view the result summary.

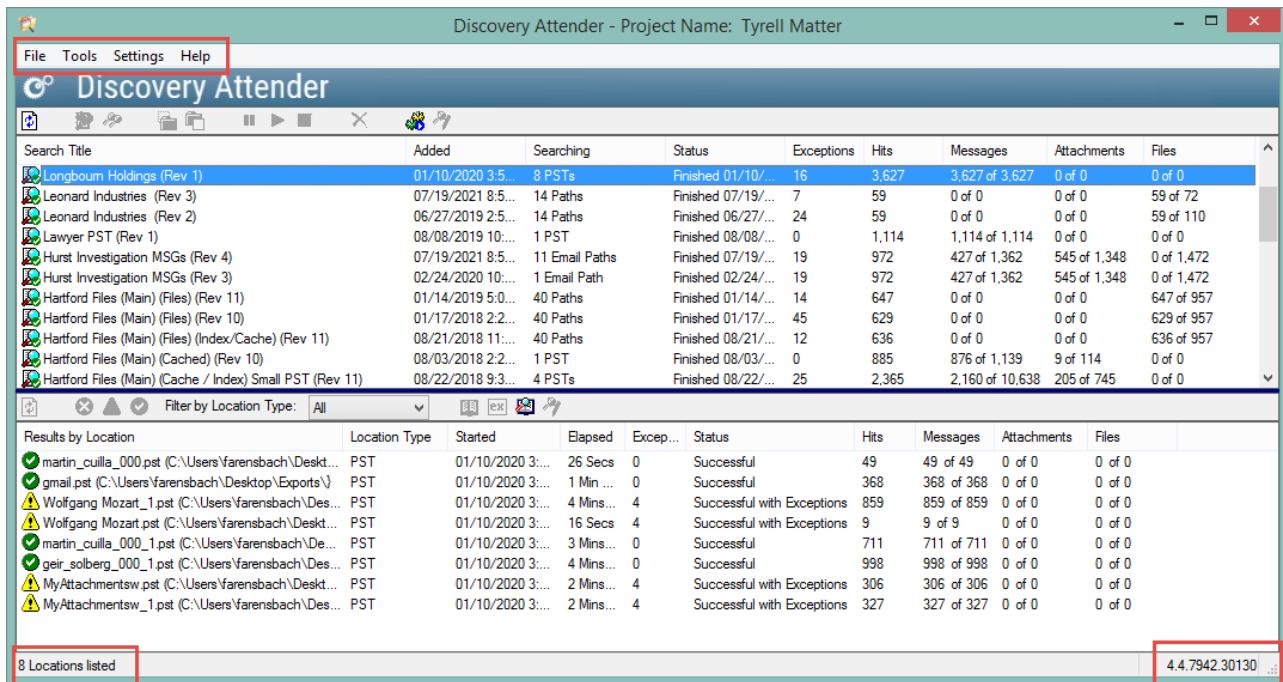


The top portion of the console is used for **Search Management**. This area shows a list of searches with a brief statistical summary. Double-clicking on a search will open the **Result Management** window.

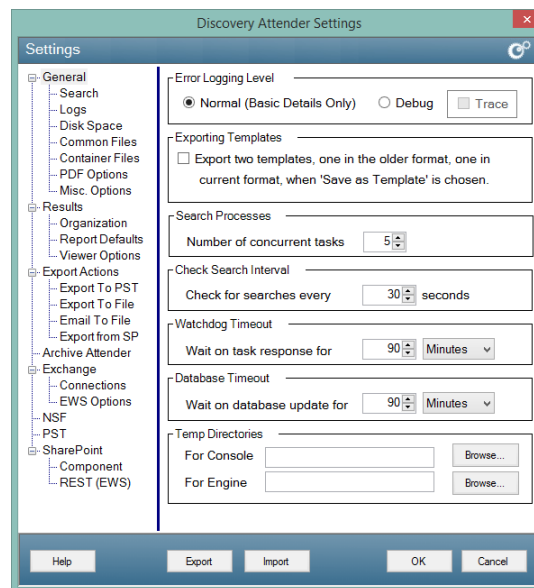


The bottom portion of the console provides the **Results by Location** for each data store included in the search selected in the Search Management section. Options available in this section include summary by task, log file and exception lists.

The Application Menu and Status Bar round out the console screen. These menus allow you to manage projects, control application settings and learn more about Discovery Attender.

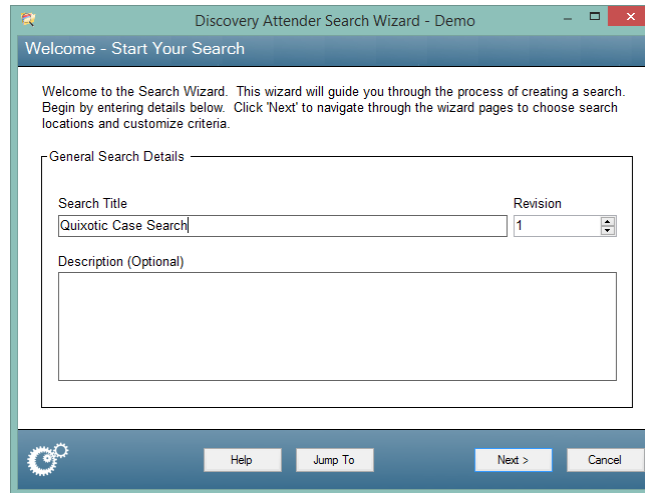


A number of application features can be customized using the Discovery Attender *Settings*. To set these options, navigate from the main console using the *Settings* file menu option.



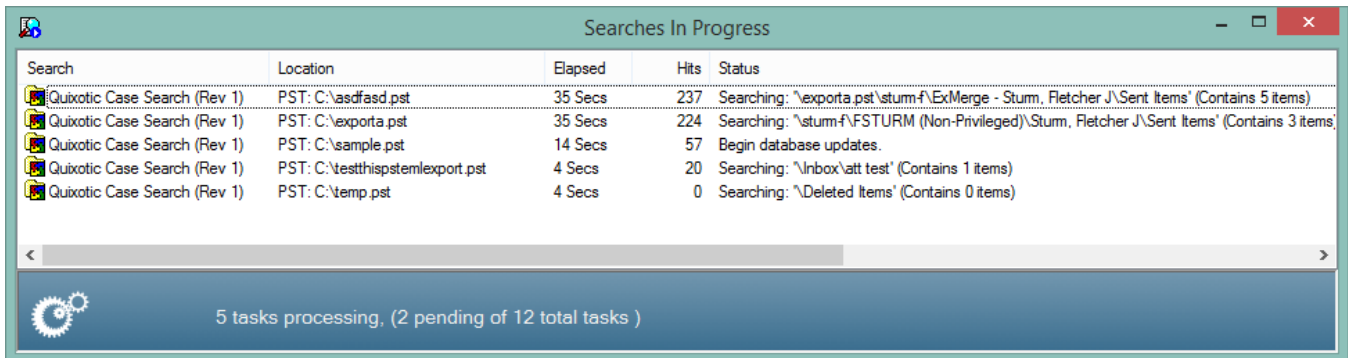
New Search (Search Wizard)

The Search Wizard guides the user in creating a search. Each screen has choices that will define the criteria, search conditions, options and data stores that will be searched. Once the wizard setup is complete, you can begin your search process.



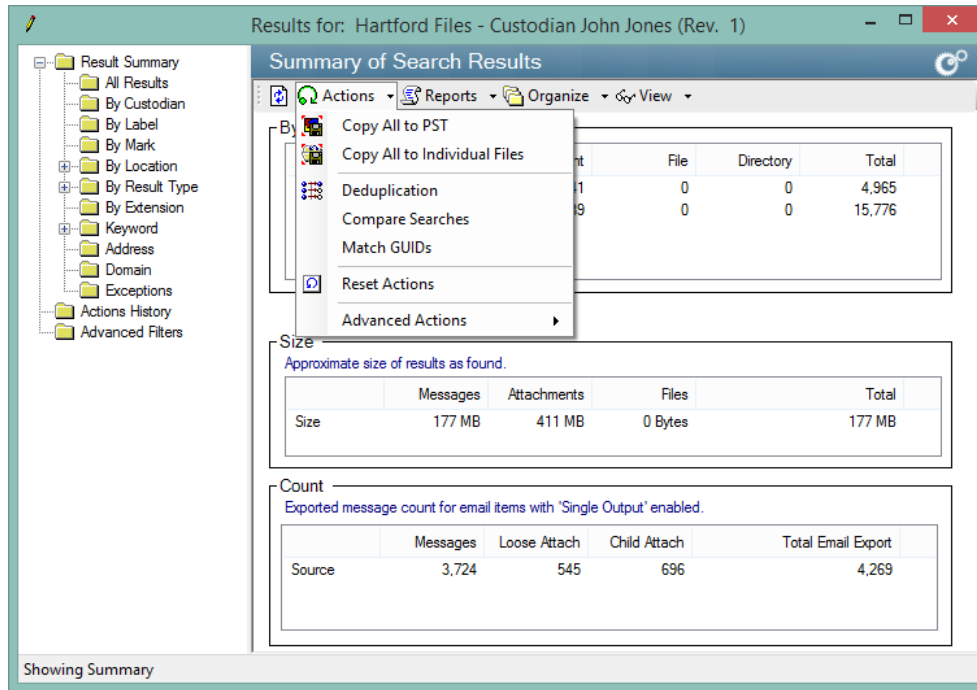
The Search Wizard is accessed from the Main Console. Use the toolbar or context menu to begin a New Search or Search Again. You can also base a new search on a template by selecting the option to Load a Template.

Use the navigation buttons to guide you through the search. Click the 'Help' button to access context specific help about the option on each available screen. Once completed, your search will begin running, with each data store searched a separate task process.



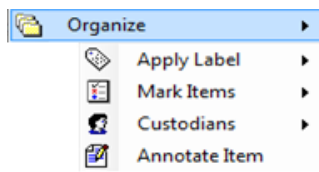
Manage Results

Once your search has completed, the Result Management views provide the functionality to view, organize, deduplicate, report, and export your results. A tree view on the left side of the screen helps you navigate through the different aspects of your result data. These views include options for showing result tallies by keywords or file type as well as address and domain reports for email. Each view has robust functionality accessed via the toolbar and menu options.



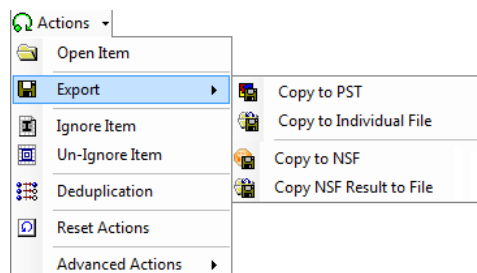
Organize Items

Discovery Attender has a number of options which allow a user to label, mark and annotate their result set. These options are fully customizable using the *Settings* menu.



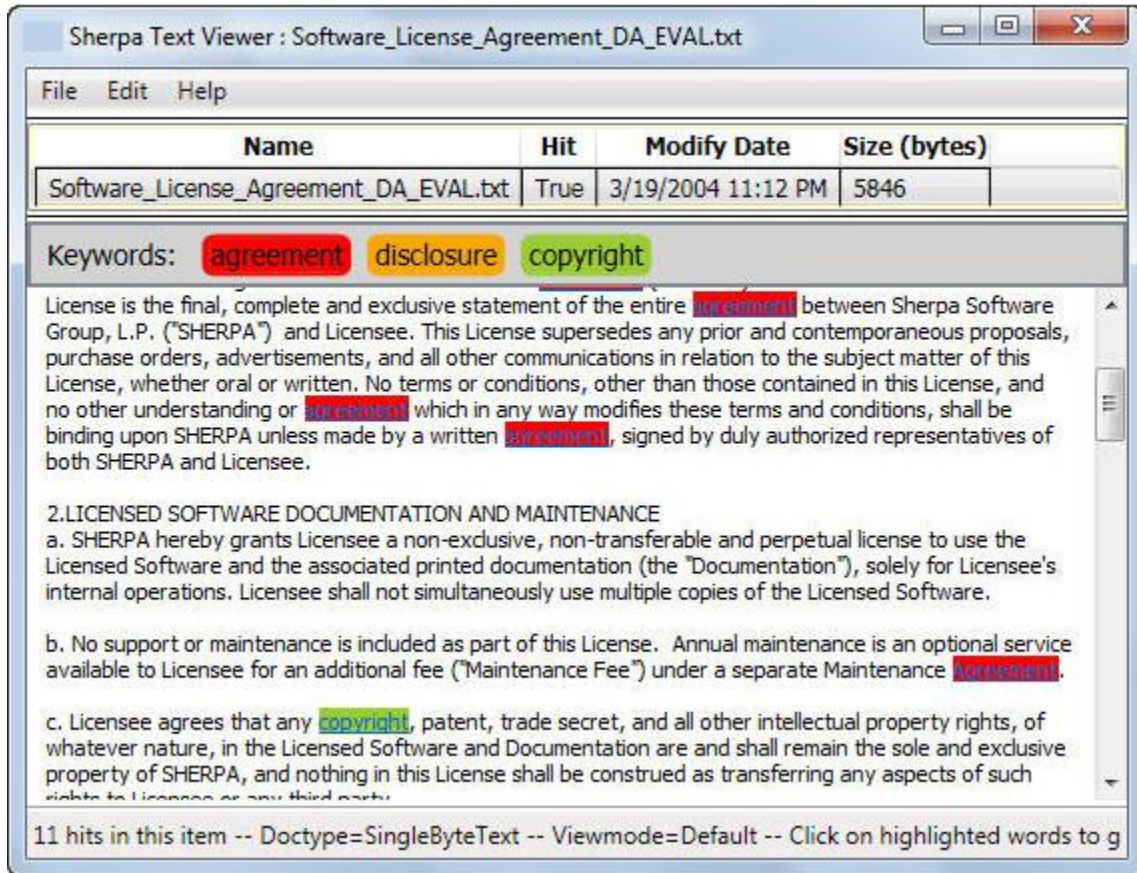
Exports and Actions

Via the *Actions* menu, a user can export items to a number of formats. Additionally, a user can run a deduplication process to eliminate all duplicates from the result set.



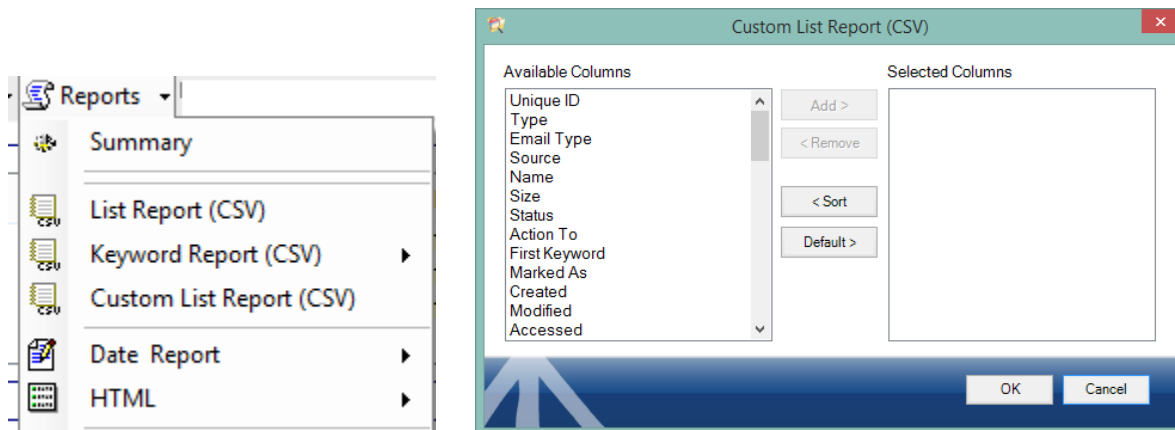
Preview Pane and Text Viewer

The Preview Pane and Text viewer will open result items without a native application. In addition, all keywords found in the result are highlighted for easy view. Simply double click on a result item to open it in the Gimmel Text Viewer.



Reports

Discovery Attender contains a number of standard reports to help you produce information about your result sets. A helpful CSV report builder is included with Discovery Attender. In addition, most list views within Discovery Attender can be exported to a CSV file, which can be opened in any spreadsheet program (e.g. Microsoft Excel).



Contact Information

For additional information regarding Discovery Attender, visit our web site <http://www.gimmel.com> or contact us using the information below.

Gimmel, LLC

24 Greenway Plaza - Suite 1000
Houston TX, 77046

Phone: 877.944.6625
Information: info@gimmel.com
Support: support@gimmel.com
Website: www.gimmel.com