Office 365 Direct getting started guide

Version 2.0

April 30, 2020

Contents

Overview

This document will provide prerequisites and onboarding steps for Office 365 Direct.

Step 1 — Prerequisites

Enable Office 365 audit logging

The Office 365 audit log records user and admin activity and retains the data for 90 days. **Audit logging is not enabled by default in Office 365 deployments. Enabling audit logging is a hard requirement for Expel to provide detection and investigative value for Office 365.** *Note: If PowerShell is preferred, please skip over to section "Step1 — Option 2: Enable Audit Logging in Office 365 with PowerShell in 3 easy steps!"*

Option 1: Enable audit logging in Office 365 Security and Compliance Center in 5 easy steps!

A. Log to the Office 365 Admin Portal with a global admin user (or at minimum a user with the Organization Management or Compliance Management roles)

B. Navigate to the **Security & Compliance Center** (see Figure 1)

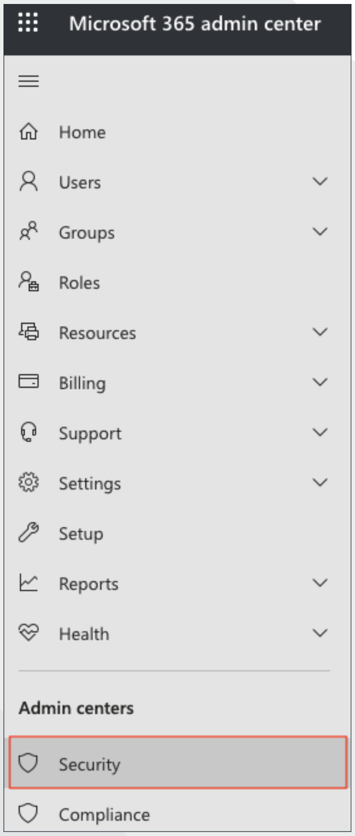


Figure 1

C. Navigate to **Search & investigation** > **Audit log search** (Figure 2)

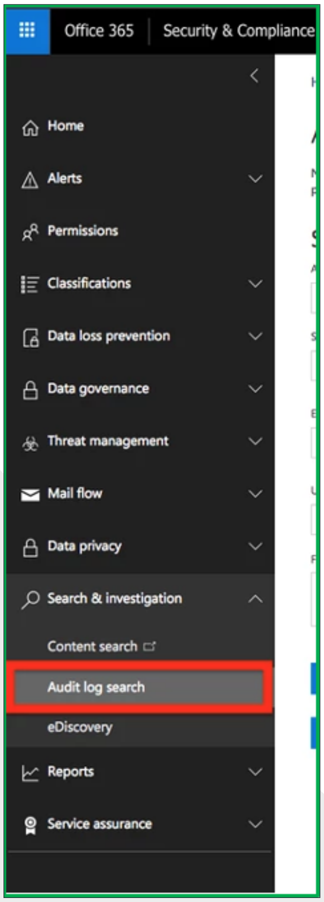
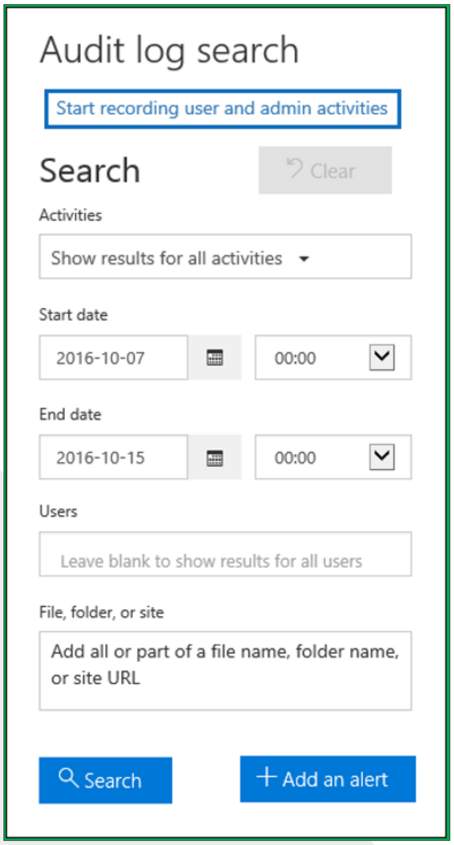


Figure 2

D. Click **Start recording user and admin activities** (Figure 3)



Activities

Show results for all activities

Start date

2016-10-07 00:00

End date

2016-10-15 00:00

Users

Leave blank to show results for all users

File, folder, or site

Add all or part of a file name, folder name, or site URL

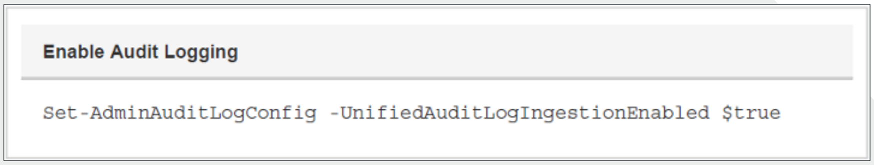
Figure 3

E. That's it! Office 365 will make some changes behind the scenes and begin recording activity in the audit log. **Note: This change can take ~ 24 hours to complete**

Option 2: Enable audit logging in Office 365 with PowerShell in 3 easy steps!

A. [Connect to Exchange Online PowerShell]()

B. Run the following PowerShell command to turn on audit log search in Office 365 (Figure 4)



Enable Audit Logging

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

Figure 4

C. That's it! A message will be displayed saying it might take up to 60 minutes for the change to take effect

Reference: [Microsoft: Turn Office 365 audit log search on or off]()

Step 2 — Enable O365 Enterprise Application

In order to integrate O365 Direct with Expel, we need to create secure credentials to the API. There are two options presented below for enabling API access:

- Option 1: Enable the **Expel Office 365 Integration** Enterprise Application within Azure
- Option 2: Create a **custom Azure Active Directory (AD) Application**

In most cases enabling the Enterprise Application (option 1) is the recommended approach. The second option is offered for cases where the absolute minimum permissions are required. In either case, the table (Figure 5) below presents the required items that should be obtained during this step:

Item we need	Description
Azure Directory (tenant) ID	This is a unique identifier for your Azure instance. Expel needs this information to route our API requests to the right place.
Application (client) ID (Option 2 only)	This is a unique identifier for the application you will create that grants Expel the access it needs to your O365 instance.
Application (client) Secret (Option 2 only)	This is the API secret that allows Expel to authenticate as the created application to your O365 instance.

Figure 5

Option 1: Enable Office 365 integration (preferred)

A. As an Administrator, **navigate** to Expel's Admin Consent Page

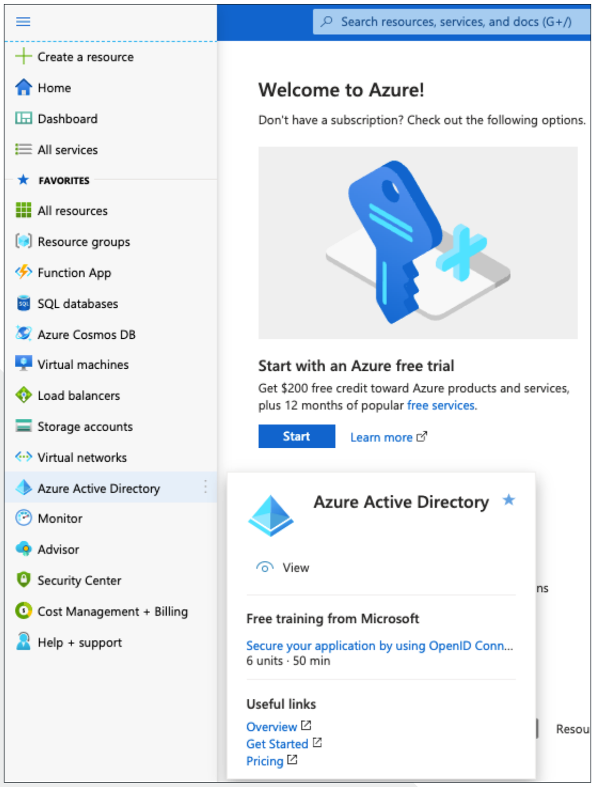
B. **Review** and **accept** requested permissions

C. The **Expel Office 365 Integration** app should now show up under **Enterprise Applications**. Review properties and ensure that all permissions were properly granted

D. **Note** the **Directory (Tenant) ID** when viewing the **Expel Office 365 Integration** application for use in later steps

Option 2: Create Custom Azure AD Application

A. **Log into** your Azure Active directory account (https://portal.azure.com) and open **Azure Active Directory** (Figure 6)



Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Free training from Microsoft

Secure your application by using OpenID Conn...
6 units · 50 min

Useful links

Figure 6

B. Navigate to **App registrations** and create a new app by clicking **+ New registration** (Figure 7)

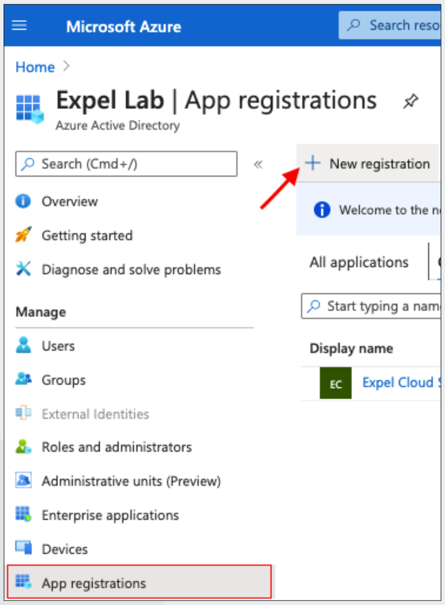
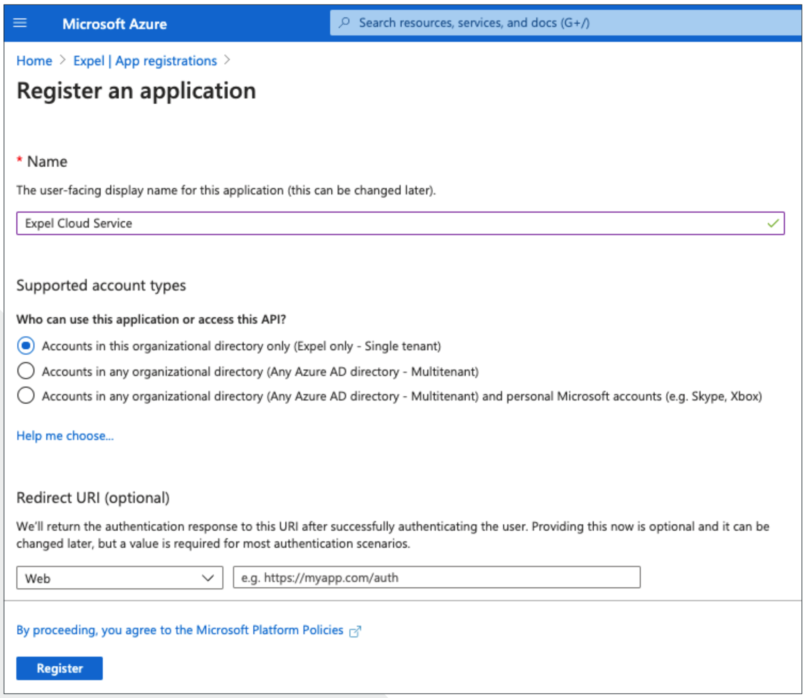


Figure 7

C. Fill in the application details. You can technically fill these in however you want, but we recommend the following: (see Figure 8)

Name: Expel Cloud Service
Supported account types: Accounts in this organizational directory only (first option)



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Expel | App registrations >

Register an application

* Name

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

Expel Cloud Service

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Expel only - Single tenant)
○ 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. Skype, Xbox)

Help me choose...

Redirect URI (optional)

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

Web | e.g. https://myapp.com/auth

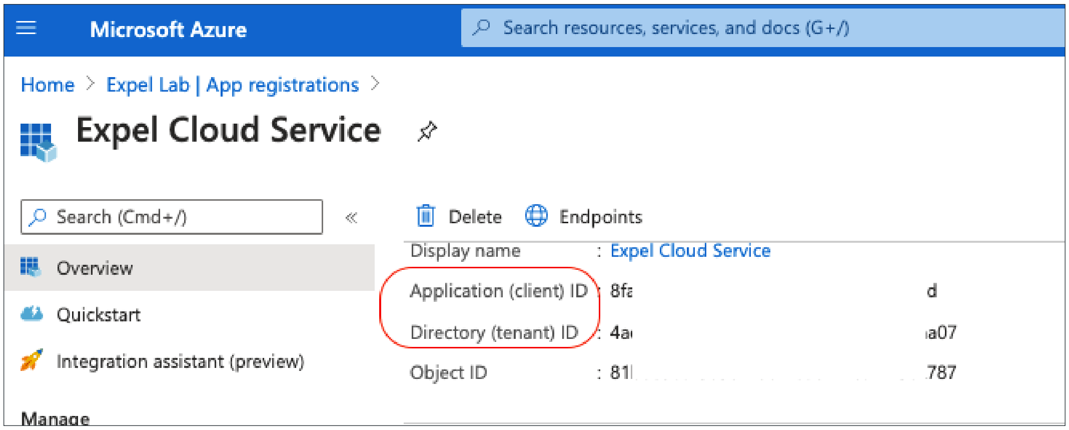
By proceeding, you agree to the Microsoft Platform Policies

Figure 8

D. Once you've filled out the fields, click **Register** to create the new application

E. You should be navigated automatically to the settings page for the **Expel Cloud Service** app you just created. If not, navigate to **Azure Active Directory > App Registrations > View all applications** (if you don't see the new app) **> Expel Cloud Service**

F. Make a note of the **Application (Client) ID** and the **Directory (Tenant) ID**, which will be needed later (See Figure 9)


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Expel Lab | App registrations >
Search (Cmd+/)
Overview
Quickstart
Integration assistant (preview)
Manage
Delete
Endpoints

Expel Cloud Service

Display name : Expel Cloud Service

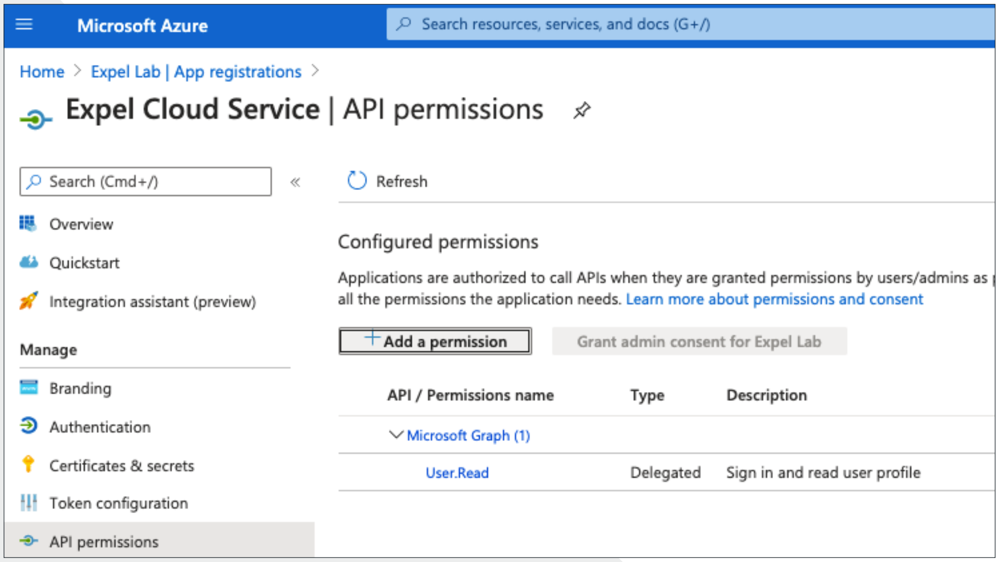
Application (client) ID : 8fa d

Directory (tenant) ID : 4a a07

Object ID : 81 787

Figure 9

G. Navigate to **API permissions** and click on **Add a permission** (see Figure 10)



Expel Cloud Service | API permissions

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Figure 10

H. The below permissions need to be added for the Expel App. Directions for adding these are in *Steps I-K*

a. Microsoft Graph API

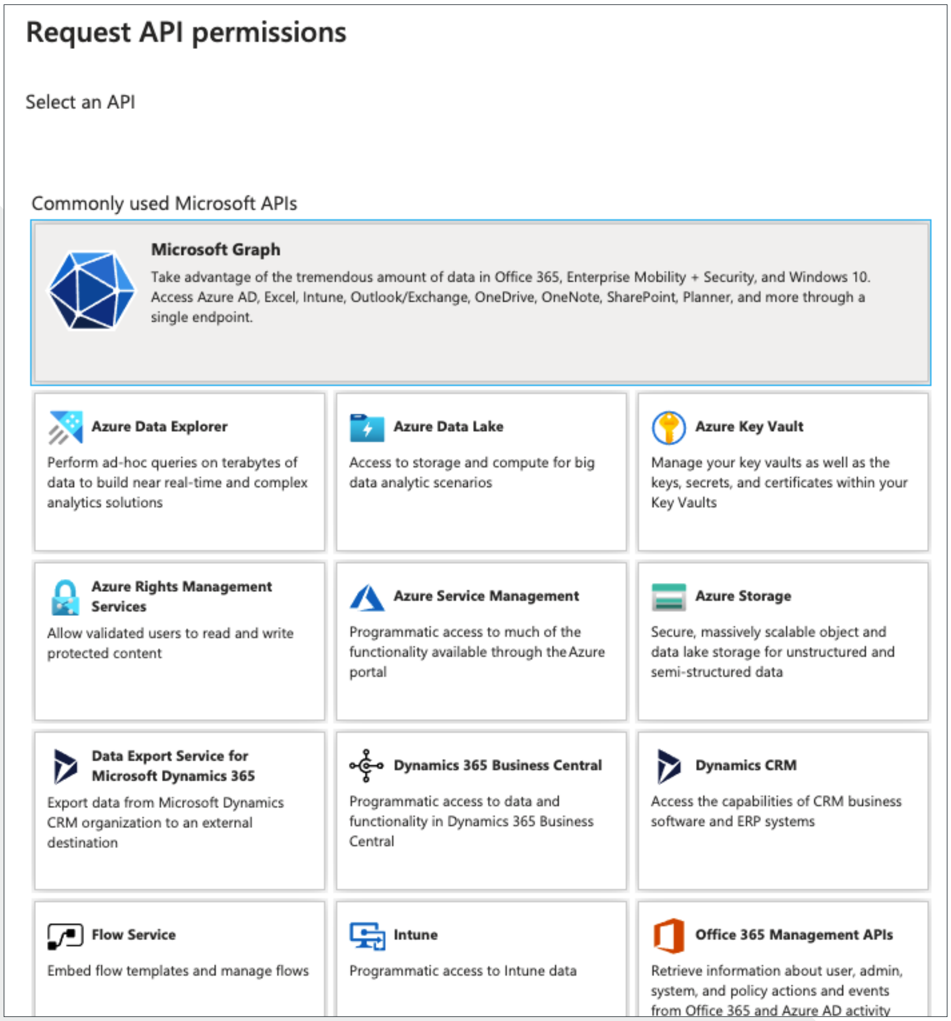
i. AuditLog.Read.All
ii. User.Read.All
iii. Group.Read.All
iv. IdentifyRiskEvent.Read.All
v. SecurityEvents.Read.All
vi. Directory.Read.All

b. Azure Active Directory Graph

i. Directory.Read.All

c. **Office 365 Management APIs**
   i. ActivityFeed.Read
   ii. ActivityFeed.ReadDlp
   iii. ActivityReports.Read (select both)
   iv. ServiceHealth.Read
   v. ThreatIntelligence.Read (select both)

l. Select the appropriate **API Category** (for example, Microsoft Graph — See Figure 11)



Request API permissions

Select an API

Commonly used Microsoft APIs

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.

Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

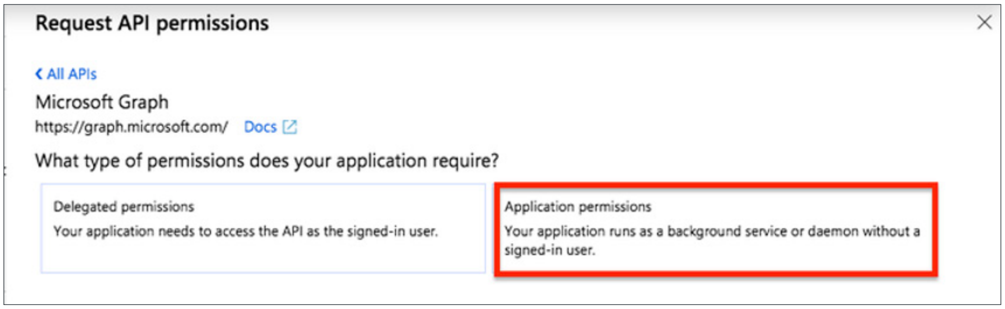
Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

Figure 11

J. Then select **Application Permissions** (see Figure 12)



Request API permissions

‹ All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions

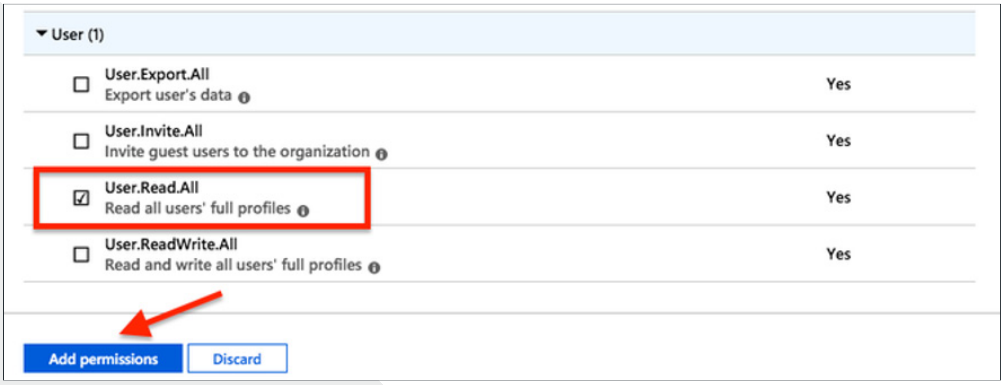
Your application needs to access the API as the signed-in user.

Application permissions

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

Figure 12

K. Select the appropriate permission(s) and click **Add Permissions** (see Figure 13)



▾ User (1)

□	User.Export.All Export user's data	Yes
□	User.Invite.All Invite guest users to the organization	Yes
☑	User.Read.All Read all users' full profiles	Yes
□	User.ReadWrite.All Read and write all users' full profiles	Yes

Figure 13

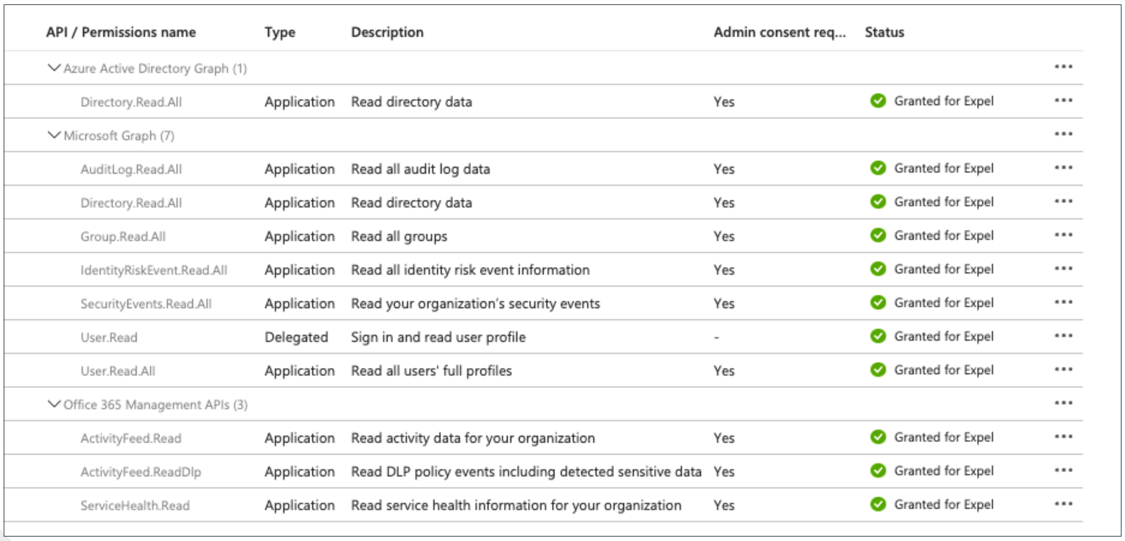
L. Repeat *Steps I-K* for each permission needed (as listed in *Step H*). Verify that:

   a. All permissions have been added as Application permissions and NOT Delegated Permissions

   b. All Permissions have been assigned

   c. Consent has been granted for the permissions by the AAD admin

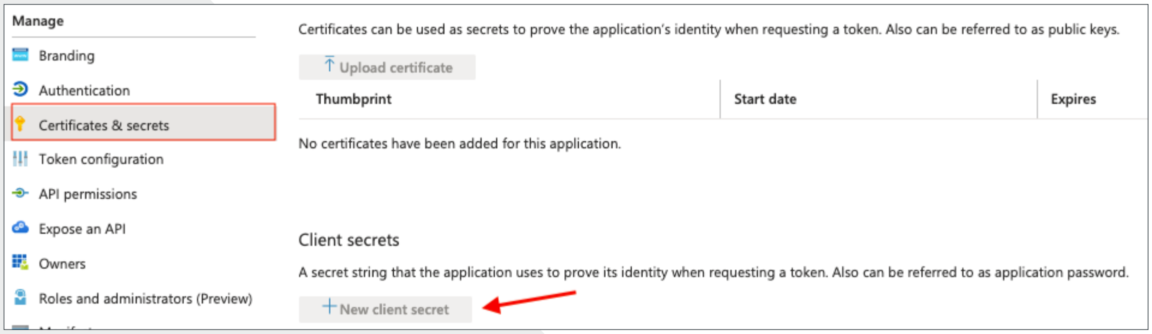
M. Once permissions have been assigned, click **Grant admin consent** and **Yes** on the confirmation popup (see Figure 14)



API / Permissions name	Type	Description	Admin consent req...	Status	
Azure Active Directory Graph (1)					•••
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Expel	•••
Microsoft Graph (7)					•••
AuditLog.Read.All	Application	Read all audit log data	Yes	✓ Granted for Expel	•••
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Expel	•••
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Expel	•••
IdentityRiskEvent.Read.All	Application	Read all identity risk event information	Yes	✓ Granted for Expel	•••
SecurityEvents.Read.All	Application	Read your organization's security events	Yes	✓ Granted for Expel	•••
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for Expel	•••
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Expel	•••
Office 365 Management APIs (3)					•••
ActivityFeed.Read	Application	Read activity data for your organization	Yes	✓ Granted for Expel	•••
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data	Yes	✓ Granted for Expel	•••
ServiceHealth.Read	Application	Read service health information for your organization	Yes	✓ Granted for Expel	•••

Figure 14

N. Navigate to **Expel Cloud Service>Certificates & secrets** to begin creating an API key (aka client secret). To create a new key, click on **+New client secret** (see Figure 15)



Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires

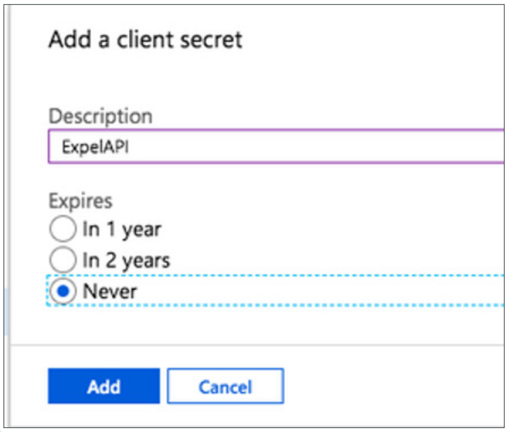
No certificates have been added for this application.

Client secrets

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

Figure 15

O. Add a description for the secret (like **ExpelAPI**) and select **Never** for expiration. Click **Add** to create the secret (see Figure 16)



Add a client secret

Description

ExpelAPI

Expires

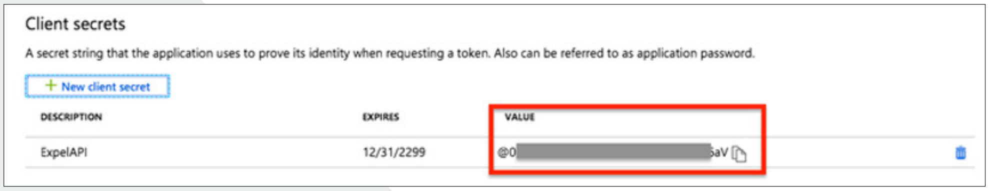
○ In 1 year

○ In 2 years

● Never

Figure 16

P. You will see a new **client secret** (API Key) appear under Client secrets. **Copy the value and save it for later**. It will disappear when you navigate away from this screen (see Figure 17)



Client secrets

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

DESCRIPTION	EXPIRES	VALUE
ExpelAPI	12/31/2299	@0[redacted]aV

Figure 17

Q. That's it! Now you're ready to onboard Office 365 with Expel!

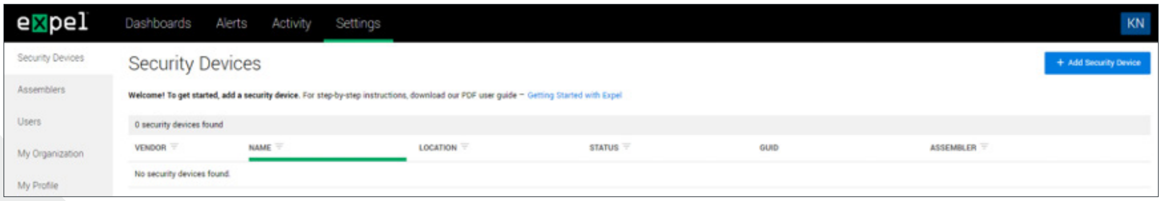
Step 3 — Configure Office 365 Direct in Expel Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate Office 365 Direct with Expel Workbench.

A. In a new browser tab, log into https://workbench.expel.io

B. On the console page, navigate to **Settings** and click **Security Devices**

C. At the top right of the page, select **Add Security Device** (Figure 18)



Security Devices

Welcome! To get started, add a security device. For step-by-step instructions, download our PDF user guide – Getting Started with Expel

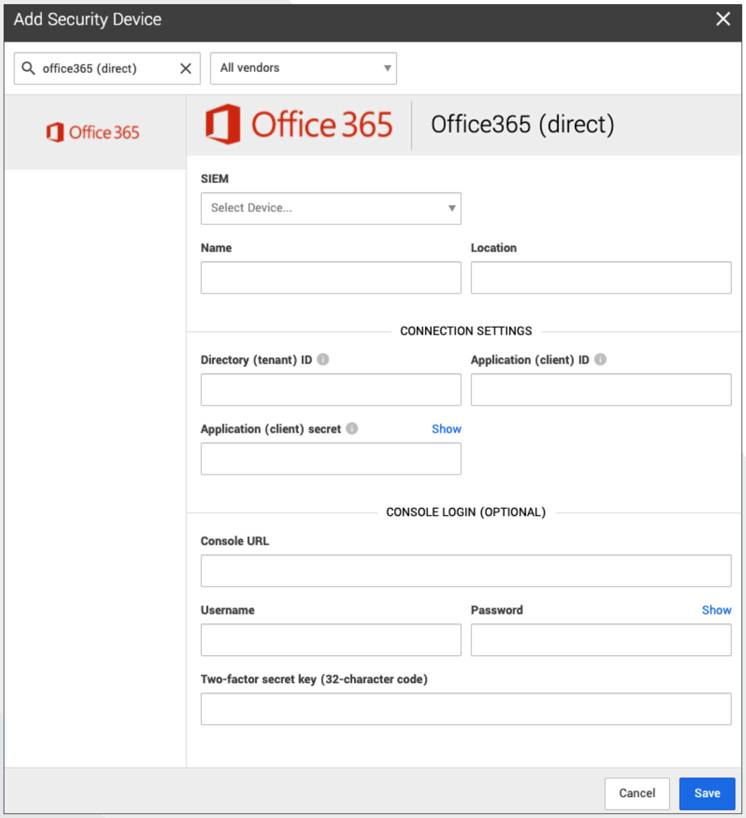
0 security devices found

VENDOR	NAME	LOCATION	STATUS	GUID	ASSEMBLER
No security devices found.					

Figure 18

D. Search for and select **Office 365 (direct)**

E. Refer to the table in Figure 20 to complete the fields in Figure 19



Office365 (direct)

SIEM
Select Device...

Name

Location

CONNECTION SETTINGS

Directory (tenant) ID

Application (client) ID

Application (client) secret Show

CONSOLE LOGIN (OPTIONAL)

Console URL

Username

Password Show

Two-factor secret key (32-character code)

Figure 19

Field Name	What to put in it
SIEM	Select the name of a previously onboarded Expel Cloud device from the drop down
Name	What you want to name the security device
Location	Microsoft Cloud
Tenant ID	Azure Directory (tenant) ID from *Step 2, Letter D* (Option 1) or *Step 2, Letter F* (Option 2)
Client ID (Option 2 only)	The Azure Application (client) ID that we saved in *Step 2, Option 2, Letter F*
Client Secret (Option 2 only)	The Application (client) Secret that we saved in *Step 2, Option 2, Letter P*

Figure 20

F. Select **Save**

G. After a few minutes, refresh the **Security Devices** page and you should see your device status reporting as *Healthy*, or if there is an issue, it will provide more details of what the issue may be

H. To check and see if alerts are coming through, navigate to **Alerts** on the console page. Click the icon in the upper right to switch to grid view, then check the list for Office 365 Direct alerts

Step 4 — Configure Azure AD Identity Protection in Expel Workbench (Premium P2 license required)

Now that we have all the correct access configured and have noted the credentials, we can integrate Azure AD Identity Protection with Expel Workbench.

A. In a new browser tab, login to https://workbench.expel.io

B. On the console page, navigate to **Settings** and click **Security Devices**

C. At the top right of the page, select **Add Security Device** (Figure 18, above)

D. Search for and select **Azure AD Identity Protection**

E. Refer to the table in Figure 20 to complete the fields in Figure 21

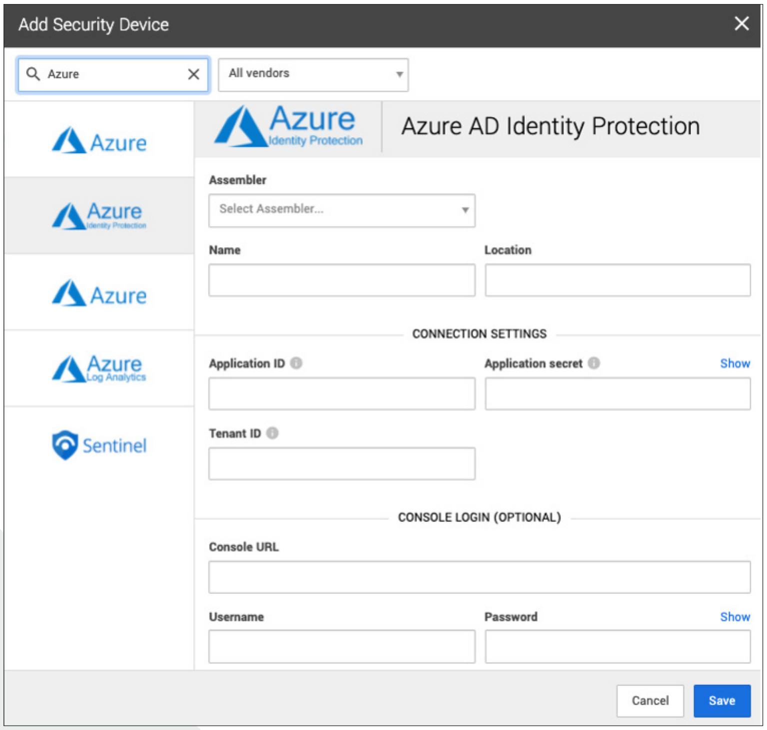


Figure 21

F. Select **Save**

G. After a few minutes, refresh the **Security Devices** page and you should see your device status reporting as *Healthy*, or if there is an issue, it will provide more details of what the issue may be

H. To check and see if alerts are coming through, navigate to **Alerts** on the console page. Click the icon in the upper right to switch to grid view, then check the list for Azure AD Identity Protection alerts

That's it! Give yourself a pat on the back — you're done!

If you have any issues, concerns, questions or feedback,
please don't hesitate to contact Expel at devicehealth@expel.io.