

How to configure Splunk Add-on for Microsoft Office 365 (including Azure / Office 365 app registration)

Disclaimer: The steps mentioned in this document are current as of 14 Apr 2020. The Azure portal, Office 365 portal and Splunk Add-on for Microsoft Office 365 continue to evolve and change, which may render some steps / screenshots invalid.

- 1) Log in to admin.microsoft.com > go to **Azure Active Directory**.
- 2) On the left pane, click **All Services** > search for: "App registrations".
- 3) Click **App registrations** > **New registration**.
- 4) Put any name you like. For the supported account type, select option 2 (Any Azure AD directory - Multitenant). Leave the **Redirect URL** blank. Click **Register**.

Azure Active Directory admin center

All services > App registrations > Register an application

Register an application

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

Supported account types
Who can use this application or access this API?

☐ Accounts in this organizational directory 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

- 5) Once registration is complete, you will see the registration summary. Copy the **Application (client) ID** and **Directory (tenant) ID**. You will need them when configuring Splunk.

All services > App registrations > ingest_to_splunk

ingest_to_splunk

Delete Endpoints

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name	: ingest_to_splunk	Supported account types	: Multiple organizations
Application (client) ID	: [redacted]	Redirect URIs	: Add a Redirect URI
Directory (tenant) ID	: [redacted]	Application ID URI	: Add an Application ID URI
Object ID	: [redacted]	Managed application in ...	: ingest_to_splunk

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)

Documentation

- [Microsoft identity platform](#)
- [Authentication scenarios](#)
- [Authentication libraries](#)
- [Code samples](#)
- [Microsoft Graph](#)
- [Glossary](#)
- [Help and Support](#)

- 6) On the app you just registered, go to **Certificates & secrets** > **New Client Secret** > put a description and expiration period > click **Add**. A client secret value will appear. Copy it. This is needed later when configuring Splunk.

Add a client secret

Description

client secret

Expires

☒ In 1 year

☐ In 2 years

☐ Never

Add Cancel

- 7) Now go to **API Permissions** > click **Add a permission** > select **API my organization uses**. Search for “Office 365” and when the search result is shown, click **Office 365 Management APIs**.

All services > App registrations > ingest_to_splunk | API permissions

ingest_to_splunk | API permissions

Search (Cmd+/) « Refresh

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators (Previ...

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Request API permissions

< All APIs

Office 365 Management APIs
https://manage.office.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.

8) For both **Delegated permissions** and **Application permissions**, assign the same permissions below:

- ActivityFeed > ActivityFeed.Read
- [Optional] ActivityFeed > ActivityFeed.ReadDlp
- Service Health > ServiceHealth.Read

Request API permissions

[All APIs](#)

 **Office 365 Management APIs**
<https://manage.office.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.

Select permissions [expand all](#)

Type to search

Permission	Admin consent required
ActivityFeed (2)	
<input checked="" type="checkbox"/> ActivityFeed.Read Read activity data for your organization ⓘ	Yes
<input checked="" type="checkbox"/> ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data ⓘ	Yes
ActivityReports	
ServiceHealth (1)	
<input checked="" type="checkbox"/> ServiceHealth.Read Read service health information for your organization ⓘ	Yes
ThreatIntelligence	

9) Grant admin consent when requested.

The Azure / Office 365 configuration is now complete. The remaining steps are to be performed on the Splunk side (see next page).

10) Launch your web browser and point to the Splunk node where **Splunk Add-on for Microsoft Office 365** is to be configured.

11) Install the add-on if you have not done so. Note:

- Installation method depends on the Splunk role and whether it is clustered or not.
- Splunk service will need to be restarted after installing this add-on.

12) Go to the **Splunk Add-on for Microsoft Office 365** page and click **Tenant** tab. Add the Tenant information using the **Tenant ID**, **Client ID**, and **Client Secret** noted earlier. Click **Add**.

Add Tenant

Name

office365

Only letters, numbers and underscores are supported

Endpoint

Worldwide

Tenant ID

The Directory ID from Azure Active Directory.

Client ID

The Application ID from the registered application within the Azure Active Directory.

Client Secret

The registered application key for the corresponding application.

Learn More

Cancel

Add

13) If proxy configuration is required, go to the **Settings** tab and configure it.

14) Once **tenant** and **proxy (optional)** are configured, go to the **Input** tab and enable the inputs as required.

Input

Tenant

Settings

>

Splunk Add-on for Microsoft Office 365

Add Input

Management Activity

Service Status

Service Message

Input Name	Input Type	Tenant	Index	Interval (seconds)
------------	------------	--------	-------	--------------------

For example:

Add Management Activity Input ×

Input Name

management_activity

Tenant Name

office365

Content Type

Audit.AzureActiveDirectory

Index

aaa

Interval (seconds)

300







Cancel

Add

15) By default, the data is fetched every 300 seconds. You can adjust the interval as required.

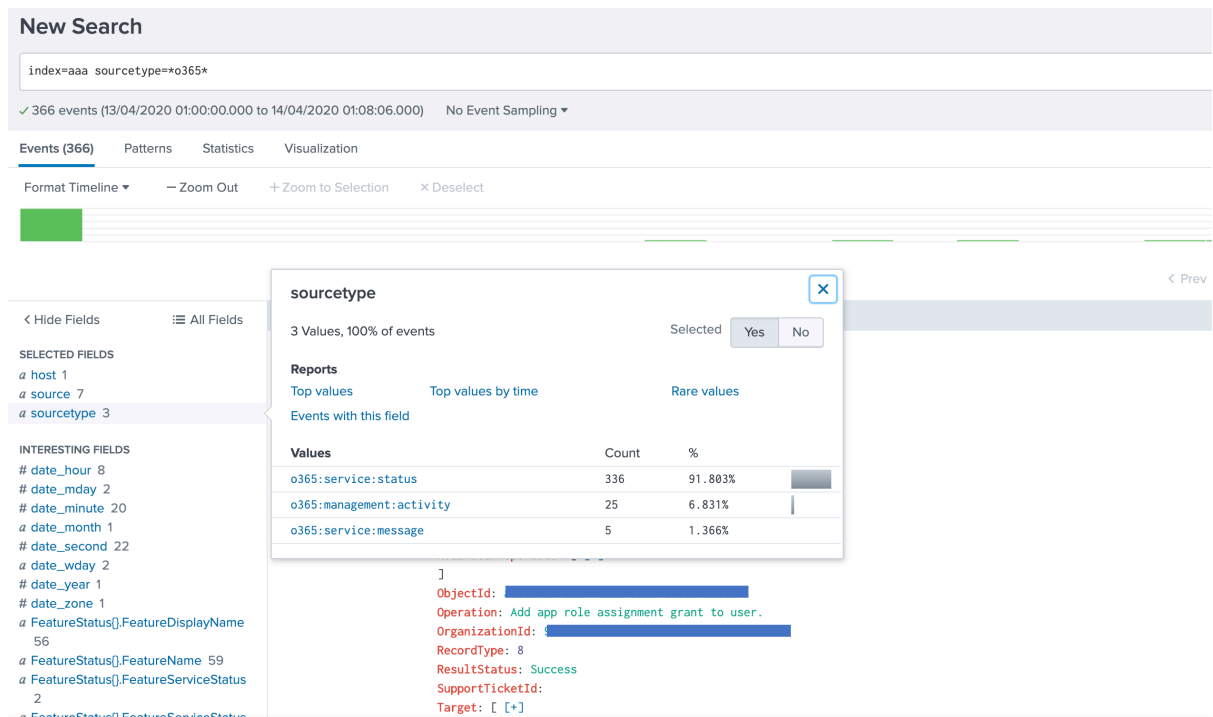
16) Below example shows a couple of enabled inputs:

Add Input ▾

Input Name	Input Type	Tenant	Index	Interval (seconds)	Status	Action
management_activity	Management Activity	office365	aaa	30	 Enabled	<div>EditDelete</div>
audit_exchange	Management Activity	office365	aaa	30	 Enabled	<div>EditDelete</div>
audit_dlp	Management Activity	office365	aaa	30	 Enabled	<div>EditDelete</div>
audit_general	Management Activity	office365	aaa	30	 Enabled	<div>EditDelete</div>
current_status	Service Status	office365	aaa	30	 Enabled	<div>EditDelete</div>
service_message	Service Message	office365	aaa	30	 Enabled	<div>EditDelete</div>

17) Wait for at least the interval period before checking whether the data has been ingested. After that, you can simply search the data to confirm whether it has been indexed successfully.

Using the above example, the data is stored in the index “aaa”. This SPL then shows the data has been indexed successfully: **index=aaa sourcetype=*o365***



New Search

index=aaa sourcetype=*o365*

✓ 366 events (13/04/2020 01:00:00.000 to 14/04/2020 01:08:06.000) No Event Sampling ▼

Events (366) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

< Hide Fields All Fields

SELECTED FIELDS

- host 1
- source 7
- sourcetype 3

INTERESTING FIELDS

- # date_hour 8
- # date_mday 2
- # date_minute 20
- # date_month 1
- # date_second 22
- # date_wday 2
- # date_year 1
- # date_zone 1
- # FeatureStatus().FeatureDisplayName 56
- # FeatureStatus().FeatureName 59
- # FeatureStatus().FeatureServiceStatus 2
- # FeatureStatus().FeatureServiceStatus

sourcetype

3 Values, 100% of events

Selected Yes No

Reports

- Top values
- Top values by time
- Rare values

Events with this field

Values	Count	%
o365:service:status	336	91.803%
o365:management:activity	25	6.831%
o365:service:message	5	1.366%

ObjectID: [REDACTED]
Operation: Add app role assignment grant to user.
OrganizationID: [REDACTED]
RecordType: 8
ResultStatus: Success
SupportTicketId:
Target: [[+]

18) Basic troubleshooting questions:

- Where are the logs located?
/opt/splunk/var/log/splunk. Search for all *o365* files.
- How do I increase the logging detail?
From the Splunk Web UI, go to the Splunk Add-on for Microsoft Office 365 page > **Settings** tab > **Logging** > set the log level to: **DEBUG** > click **Save**.
- Why is Splunk not ingesting my Office 365 audit data?
 - From Splunk side: Check the logs for any errors.
 - From Office 365 side: Ensure Office 365 auditing is enabled. Steps can be found in: <https://support.microsoft.com/en-au/help/4026501/office-auditing-in-office-365-for-admins>
- I have 90 days' worth of audit data, why is Splunk only ingesting data from the past 7 days?
This restriction is imposed by the Office 365 Management API. Reference: <https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-faq>
<https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-reference>
As a workaround, you can export the audit data from the Office 365 Security & Compliance portal (into a CSV file) and ingest the data manually.