| Add-on | Input/Action | API | Permissions | Role (IAM) | Default Sourcetype(s) / Sources | Notes |
|---|---|---|---|---|---|---|
| **Splunk Add-on for Microsoft Cloud Services**<br>https://splunkbase.splunk.com/app/3110/<br>https://docs.splunk.com/Documentation/AddOns/released/MSCloudServices/About | Azure Storage Table<br>Azure Storage Blob | N/A | Access key OR<br>Shared Access Signature:<br>- Allowed services: Blob, Table<br>- Allowed resource types: Service, Container, Object<br>- Allowed permissions: Read, List | N/A | mscs:storage:blob<br>mscs:storage:blob:json<br>mscs:storage:blob:xml<br>mscs:storage:table | https://docs.microsoft.com/en-us/rest/api/storageservices/Constructing-an-Account-SAS |
| | Azure Audit | N/A | N/A | (Subscription) Reader | mscs:azure:audit | |
| | Azure Resource | N/A | N/A | (Subscription) Reader | mscs:resource:virtualMachine<br>mscs:resource:networkInterfaceCard<br>mscs:resource:publicIPAddress<br>mscs:resource:virtualNetwork<br>mscs:resource:disk<br>mscs:resource:image<br>mscs:resource:snapshot<br>mscs:resource:resourceGroup<br>mscs:resource:subscriptions<br>mscs:resource:security Group | |
| | Event Hub | N/A | No API permissions are needed, but the Azure AD app registration needs to be assigned to the "Azure Event Hubs Data receiver" role on the Event Hub namespace | (Event Hub) Azure Event Hubs Data receiver | mscs:azure:eventhub (generic event hub events) | https://docs.splunk.com/Documentation/AddOns/released/MSCloudServices/Configureeventhubs |
| | | | | | azure:monitor:aad | Azure Active Directory events - Azure AD sign-ins and Azure AD audit |
| | | | | | azure:monitor:activity | Azure activity log events |
| | | | | | azure:monitor:resource | Azure resources - examples: Cosmos DB, Azure Data Share |
| | Metrics | N/A | | (Subscription) Reader | mscs:metrics<br>mscs:metrics:events | |
| | Azure KQL Log Analytics | Log Analytics API | (Application) Data.Read - Read Log Analytics data | N/A | mscs:kql<br>mscs:kql:stats | |
| | Azure Consumption (Billing) | N/A | | (Subscription) Reader | mscs:consumption:billing<br>mscs:consumption:reservation:recommendation | https://docs.microsoft.com/en-us/rest/api/consumption/usagedetails/list |
| | | | | | | |
| **Splunk Add-on for Microsoft Azure**<br>https://splunkbase.splunk.com/app/3757/<br>https://github.com/splunk/splunk-add-on-microsoft-azure/wiki | Azure Active Directory Sign-ins<br>The REST API this input uses is subject to throttling limits. Refer to the throttling guidance for more information. | Microsoft Graph | (Application) AuditLog.Read.All - Read all audit log data | N/A | azure:aad:signin | An Azure AD Premium P1 or P2 license is required to use this input. https://docs.microsoft.com/en-us/graph/api/resources/signin |
| | | | (Application) Directory.Read.All | N/A | | https://docs.microsoft.com/en-us/graph/known-issues#azure-ad-activity-reports-can-return-an-error |
| | | | | | | Due to throttling limits, it is recommended to send Azure AD sign-in data to an event hub and use the Splunk Add-on for Microsoft Cloud Services or Splunk Data Manager (cloud only) to collect the data. |
| | Azure Active Directory Users | Microsoft Graph | (Application) User.Read.All - Read all users' full profiles | N/A | azure:aad:user | |
| | Azure Active Directory Groups | Microsoft Graph | (Application) Group.Read.All - Read all groups | N/A | azure:aad:group | |
| | Azure Active Directory Audit<br>The REST API this input uses is subject to throttling limits. Refer to the throttling guidance for more information. | Microsoft Graph | (Application) AuditLog.Read.All - Read all audit log data | N/A | azure:aad:audit | |
| | | | (Application) Directory.Read.All | N/A | | https://docs.microsoft.com/en-us/graph/known-issues#azure-ad-activity-reports-can-return-an-error |
| | | | | | | Due to throttling limits, it is recommended to send Azure AD audit data to an event hub and use the Splunk Add-on for Microsoft Cloud Services or Splunk Data Manager (cloud only) to collect the data. |
| | Azure Active Directory Risk Detection | Microsoft Graph | (Application) IdentityRiskEvent.Read.All - Read all identity risk event information<br>(Application) IdentityRiskyUser.Read.All - Read all identity risk user information | N/A | azure:aad:identity_protection:risk_detection<br>azure:aad:identity_protection:risky_user | |
| | Azure Active Directory Devices | Microsoft Graph | (Application) Device.Read.All - Read all devices | N/A | azure:aad:device | |
| | Metrics<br>**This input has been migrated to the supported Splunk Add-on for Microsoft Cloud Services.** | N/A | | (Subscription) Reader | azure:metrics | |
| | Security Center (now called Microsoft Defender for Cloud) | N/A | | (Subscription) Reader | azure:securityCenter:alert<br>azure:securityCenter:task | Security Center has been renamed to Microsoft Defender for Cloud. It is now possible to export these data source to an Event Hub https://learn.microsoft.com/en-us/azure/defender-for-cloud/continuous-export?tabs=azure-portal |
| | Subscriptions<br>**This input has been migrated to the supported Splunk Add-on for Microsoft Cloud Services as part of the "Azure Resource" input.** | N/A | | (Subscription) Reader | azure:subscriptions | |
| | Resource Groups<br>**This input has been migrated to the supported Splunk Add-on for Microsoft Cloud Services as part of the "Azure Resource" input.** | N/A | | (Subscription) Reader | azure:resource:group | |
| | Virtual Networks<br>**This input has been migrated to the supported Splunk Add-on for Microsoft Cloud Services as part of the "Azure Resource" input.** | N/A | | (Subscription) Reader | azure:vnet<br>azure:vnet:nic<br>azure:vnet:nsg<br>azure:vnet:ip:public | |
| | Compute<br>**This input has been migrated to the supported Splunk Add-on for Microsoft Cloud Services as part of the "Azure Resource" input.** | N/A | | (Subscription) Reader | azure:compute:vm<br>azure:compute:disk<br>azure:compute:image<br>azure:compute:snapshot | |

| Add-on | Input/Action | API | Permissions | Role (IAM) | Default Sourcetype(s) / Sources | Notes |
|---|---|---|---|---|---|---|
| | Azure KQL Log Analytics<br>**This input has been migrated to the supported Splunk Add-on for Microsoft Cloud Services.** | Log Analytics API | (Application) Data.Read - Read Log Analytics data | N/A | azure:kql<br>azure:kql:stats | |
| | Azure Billing and Consumption<br>**This input has been migrated to the supported Splunk Add-on for Microsoft Cloud Services.** | N/A | | (Subscription) Reader | azure:billing | https://docs.microsoft.com/en-us/rest/api/consumption/usagedetails/list |
| | Azure Reservation Recommendation<br>**This input has been migrated to the supported Splunk Add-on for Microsoft Cloud Services as part of the "Azure Consumption(Billing)" input.** | N/A | | (Subscription) Reader | azure:reservation:recommendation | |
| | Azure Resource Graph | N/A | | (Subscription) Reader | azure:resourcegraph | |
| | Azure Topology (automatic) | N/A | | (Subscription) Reader | azure:topology | |
| | Azure Topology (manual) | N/A | | (Subscription) Reader | azure:topology | |
| | Add member to Microsoft 365 Group (alert action) | Microsoft Graph | (Application) GroupMember.ReadWrite.All - Read and write all group memberships | N/A | | Adds a member to a group. This can be useful if you need to enable additional policies like MFA based on search results. |
| | Stop Azure VM (alert action) | N/A | | (Subscription) Virtual Machine Contributor | | Stops an Azure Virtual Machine |
| | Dismiss Azure Alert (alert action) | N/A | | (Subscription) Contributor | | https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions |
| | | | | | | |
| **Splunk Add-on for Microsoft Office 365**<br>https://splunkbase.splunk.com/app/4055/<br>https://docs.splunk.com/Documentation/AddOns/released/MSO365/About | Management Activity<br>Audit.Azure Active Directory<br>Audit.Exchange<br>Audit.Share Point<br>Audit.General<br>DLP.All | Office 365 Management APIs | (Application) ActivityFeed.Read<br>(Application) ActivityFeed.ReadDlp (if collecting DLP data)<br>(Delegated) ActivityFeed.Read<br>(Delegated) ActivityFeed.ReadDlp (if collecting DLP data) | N/A | o365:management:activity | Click the "Grant permissions" button after creating/updating permissions.<br>DLP is only necessary when using the DLP.All content type found in the Management Activity input.<br>https://learn.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema |
| | Service Health & Communications<br>Service Health<br>Service Update Messages | Microsoft Graph | (Application) ServiceHealth.Read.All<br>(Application) ServiceMessage.Read.All | | o365:service:healthIssue<br>o365:service:updateMessage | https://learn.microsoft.com/graph/api/serviceannouncement-list-issues<br>https://learn.microsoft.com/graph/api/serviceannouncement-list-messages |
| | Mailbox<br>Mailbox Usage Detail<br>Mailbox Usage Mailbox Counts | Microsoft Graph | (Application) Reports.Read.All | | sourcetype=o365:graph:api<br>source=MailboxUsageMailboxCounts<br>source=MailboxUsageDetail | https://learn.microsoft.com/graph/api/reportroot-getmailboxusagemailboxcounts<br>https://learn.microsoft.com/graph/api/reportroot-getmailboxusagedetail |
| | Office 365<br>Office 365 Groups Activity Detail<br>Office 365 Services User Counts | Microsoft Graph | (Application) Reports.Read.All | | sourctype=o365:graph:api<br>source=Office365GroupsActivityDetail<br>source=Office365ServicesUserCounts | https://learn.microsoft.com/graph/api/reportroot-getoffice365groupsactivitydetail<br>https://learn.microsoft.com/graph/api/reportroot-getoffice365servicesusercounts |
| | One Drive<br>One Drive Activity User Counts<br>One Drive Usage Account Detail<br>One Drive Usage Storage | Microsoft Graph | (Application) Reports.Read.All | | sourcetype=o365:graph:api<br>source=OneDriveActivityUserCounts<br>source=OneDriveUsageAccountDetail<br>source=OneDriveUsageStorage | https://learn.microsoft.com/graph/api/reportroot-getonedriveactivityusercounts<br>https://learn.microsoft.com/graph/api/reportroot-getonedriveactivityuserdetail<br>https://learn.microsoft.com/graph/api/reportroot-getonedriveusagestorage |
| | Share Point<br>Share Point Site Usage Detail<br>Share Point Site Usage File Counts | Microsoft Graph | (Application) Reports.Read.All | | sourcetype=o365:graph:api<br>source=SharePointSiteUsageDetail<br>source=SharePointSiteUsageFileCounts | https://learn.microsoft.com/graph/api/reportroot-getsharepointsiteusagedetail<br>https://learn.microsoft.com/graph/api/reportroot-getsharepointsiteusagefilecounts |
| | Teams<br>Teams User Activity Counts<br>Teams User Activity User Detail | Microsoft Graph | (Application) Reports.Read.All | | sourcetype=o365:graph:api<br>source=TeamsUserActivityCounts<br>source=TeamsUserActivityUserDetail | https://learn.microsoft.com/graph/api/reportroot-getteamsuseractivitycounts<br>https://learn.microsoft.com/graph/api/reportroot-getteamsuseractivityuserdetail |
| | Yammer<br>Yammer Groups Activity Detail<br>Yammer Groups Activity Group Counts | Microsoft Graph | (Application) Reports.Read.All | | sourcetype=o365:graph:api<br>source=YammerGroupsActivityDetail<br>source=YammerGroupsActivityGroupCounts | https://learn.microsoft.com/graph/api/reportroot-getyammergroupsactivitydetail |
| | Audit Logs<br>Audit Logs.Sign Ins<br>The REST API this input uses is subject to throttling limits. Refer to the throttling guidance for more information. | Microsoft Graph | (Application) AuditLog.Read.All<br>(Application) Directory.Read.All | | sourcetype=o365:graph:api<br>source=AuditLogs.SignIns | An Azure AD Premium P1 or P2 license is required to use this input. https://docs.microsoft.com/en-us/graph/api/resources/signin<br>Due to throttling limits, it is recommended to send Azure AD sign-in data to an event hub and use the Splunk Add-on for Microsoft Cloud Services or Splunk Data Manager (cloud only) to collect the data. |
| | Cloud Application Security<br>Policies<br>Alerts<br>Cloud Discovery<br>Entities<br>Files | | | | o365:cas:api | O365 Cloud Application Security uses a token generated from the portal.<br>https://portal.cloudappsecurity.com/<br>Once logged in, go to Settings > Security extensions > Add token<br>https://learn.microsoft.com/defender-cloud-apps/api-introduction#what-actions-are-supported |
| | Message Trace | APIs my organization uses => Office 365 Exchange Online | (Application) ReportingWebService.Read.All | Global Reader | o365:reporting:messagetrace | Updated Microsoft documentation:<br>https://docs.microsoft.com/en-us/previous-versions/office/developer/o365-enterprise-developers/jj984325(v=office.15) |
| | | | | | | |
| **Microsoft O365 Email Add-on for Splunk**<br>https://splunkbase.splunk.com/app/5365/ | O365 Email | Microsoft Graph | (Application) Mail.ReadWrite | N/A | ms:o365:email | Click the "Grant permissions" button after creating/updating permissions. |
| | O365 Email Groups | Microsoft Graph | (Application) Group.Read.All<br>(Application) GroupMember.Read.All<br>(Application) Directory.Read.All | | ms:o365:groups | |
| | | | | | | |
| **Microsoft Teams Add-on for Splunk**<br>https://splunkbase.splunk.com/app/4994/ | Teams User Report | Microsoft Graph | (Application) Reports.Read.All<br>(Delegated) Reports.Read.All | N/A | m365:teams:user:report | https://lantern.splunk.com/Data_Descriptors/Microsoft/Getting_started_with_Microsoft_Teams_call_record_data |
| | Teams Subscription | Microsoft Graph | (Delegated) Subscriptions.Read.All | | m365:subscription | |
| | Teams Call Record | Microsoft Graph | (Application) CallRecords.Read.All | | m365:teams:callRecord | |
| | Teams Webhook | N/A | N/A | | m365:webhook | |
| | | | | | | |
| **Splunk Add-on for Microsoft Security**<br>https://splunkbase.splunk.com/app/6207/ | Microsoft 365 Defender Incidents (input) | Microsoft Threat Protection | (Application) Incident.Read.All | N/A | m365:defender:incident<br>m365:defender:incident:alerts | https://docs.microsoft.com/en-us/microsoft-365/security/defender/api-hello-world?view=o365-worldwide |
| | Defender Advanced Hunting (action) | Microsoft Threat Protection | (Application) AdvancedHunting.Read.All | N/A | m365:defender:incident:advanced_hunting | https://docs.microsoft.com/en-us/microsoft-365/security/defender/api-advanced-hunting?view=o365-worldwide |

| Add-on | Input/Action | API | Permissions | Role (IAM) | Default Sourcetype(s) / Sources | Notes |
|---|---|---|---|---|---|---|
|  | Defender Update Incident (action) | Microsoft Threat Protection | (Application) Incident.ReadWrite.All | N/A | N/A | https://docs.microsoft.com/en-us/microsoft-365/security/defender/api-update-incidents?view=o365-worldwide |
|  | Microsoft Defender for Endpoint Alerts (input) | WindowsDefenderATP | (Application) Alert.Read.All | N/A | ms:defender:atp:alerts | https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/api-hello-world?view=o365-worldwide |
|  |  |  |  |  |  |  |
| **Microsoft Graph Security API Add-on for Splunk**<br>https://splunkbase.splunk.com/app/4564/ | Microsoft Graph Security | Microsoft Graph | (Application) SecurityEvents.Read.All | N/A | mscs:resource:virtualMachine<br>mscs:resource:networkInterfaceCard<br>mscs:resource:publicIPAddress<br>mscs:resource:virtualNetwork<br>mscs:resource:disk<br>mscs:resoure:image<br>mscs:resoure:snapshot<br>mscs:resoure:resourceGroup<br>mscs:resoure:subscriptions<br>mscs:resoure:securityGroup | https://docs.microsoft.com/en-us/graph/security-concept-overview |