



IDENTITY DAYS

7^{ème} édition

@IdentityDays
#identitydays2025

21 octobre 2025 - PARIS



Entra ID, trop de logs tuent le log ?

Jean-Philippe Lesage

AGENDA DE LA CONFÉRENCE

Jean-Philippe Lesage

Etudiant professionnel

Objectifs de la session

Comprendre les différents types de logs Entra ID, Identifier leur usage pour la sécurité, la conformité et le troubleshooting puis savoir exporter et maîtriser les coûts

- La multiplication des logs
- Pour y trouver quoi ?
- Et les ranger où ?
- Quelques pistes pour aller plus loin



La multiplication des logs

Intérêt des logs

Pilier de la sécurité cloud : visibilité et traçabilité

Obligations réglementaires (conformité)

Détection et réponse aux incidents

Support au troubleshooting

Réponses aux questions



Vue d'ensemble

Sign-in logs

Audit logs

Identity Protection (Risky sign-ins, Risky users)

Provisioning logs

- AuditLogs
- SignInLogs
- NonInteractiveUserSignInLogs
- ServicePrincipalSignInLogs
- ManagedIdentitySignInLogs
- ProvisioningLogs
- ADFSSignInLogs
- RiskyUsers
- UserRiskEvents
- NetworkAccessTrafficLogs
- RiskyServicePrincipals
- ServicePrincipalRiskEvents
- EnrichedOffice365AuditLogs
- MicrosoftGraphActivityLogs
- RemoteNetworkHealthLogs
- NetworkAccessAlerts
- NetworkAccessConnectionEvents
- MicrosoftServicePrincipalSignInLogs
- AzureADGraphActivityLogs

Sign-in logs

Réponses aux questions : Qui, Quoi, Quand, Comment ?

Types

- Interactive ([kesako](#)) : utilisateur
- Non interactive ([kesako](#)) : application, système, en délégation
- Service Principal ([kesako](#)) : NHI (application)
- Managed Identity ([kesako](#)) : NHI (ressource azure)

Rôle : Reports reader

ⓘ Note

Entries in the sign-in logs are system generated and can't be changed or deleted.

Audit logs

Réponses aux questions : Quel service, Quand, Quelle [catégorie](#), Quelle activité, Quel statut ?

Rôle : Reports reader

ⓘ Note

Entries in the audit logs are system generated and can't be changed or deleted.

Identity protection

Réponses aux questions

- Utilisateur à risque ([User risk](#))
- Authentification à risque ([Sign-in risk](#))

Rôle : Global reader

Provisioning logs

Réponses aux questions

- Qui
- Origine : source
- Destination : cible
- Action : Create, Update, Delete, Disable, StagedDelete et Other
- Statut : Success, Failure, Skipped et Warning

Rôle : Reports reader

Nécessite un niveau de licence P1

ⓘ Note

Entries in the provisioning logs are system generated and can't be changed or deleted.



Pour y trouver quoi ?

Sign-in logs

Application sign-in Success/Failure

User display name and UPN

Session conditions: location, IP, Date/Time

MFA info: Required, Method, Result

Client conditions: Client App, browser, OS

Conditional Access: Policy, Controls, Result

Correlation ID (basé sur les paramètres transmis par le client)

...

Linkable Identifiers : AADSessionID, UniqueTokenID

User principal name	Conditional access
User	Token issuer type
Application	User type
IP address	Cross tenant access type
Sign-in error code	Through global secure access
Resource	Is CAE token
Resource ID	Flagged for review
Operating system	Incoming token type
Device browser	Authentication protocol
Correlation ID	Client credential type
Home tenant ID	Original transfer method
Home tenant name	Token protection - Sign In Se...
Unique token identifier	Token protection - Sign In ses...
Resource tenant ID	Authentication requirement
Sign-in identifier	Agent type
Session ID	Is Agent
Autonomous system number	
IP address (seen by resource)	
Global secure access IP addre...	
Token issuer name	
Status	
Client app	

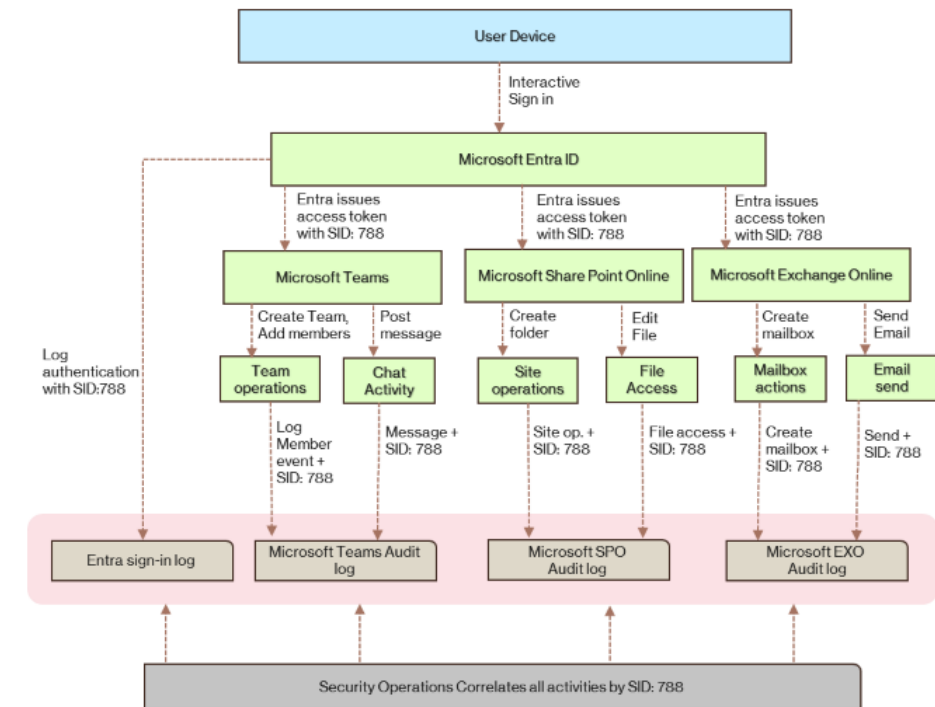
Linkable Identifiers

Objectif : Pouvoir corréler les activités avec un événement d'authentification

Basé sur la session ou le jeton

Disponibles pour

- Microsoft Entra sign-in logs
- Microsoft Exchange Online audit logs
- Microsoft Graph activity logs
- Microsoft SharePoint Online audit logs
- Microsoft Teams audit logs



[Track and investigate identity activities with linkable identifiers in Microsoft Entra](#)

Des agents ?

Les agents créés avec Azure AI Foundry ou Copilot Studio sont identifiés dans Entra ID

Dans les Sign-in logs → Agent ID

Is Agent: Yes ✕

[Microsoft Entra Agent ID: Secure and manage your AI](#)

Audit log

AAD Management UX

Access Reviews

Account Provisioning

Application Proxy

Authentication Methods

Azure AD Recommendations

Azure MFA

Azure RBAC (Elevated Access)

B2B Auth

Conditional Access

Core Directory

Device Registration Service

Entitlement Management

Entra Health Monitoring

Global Secure Access

Hybrid Authentication

Identity Protection

Invited Users

Lifecycle Workflows

Global Secure Access

Hybrid Authentication

Identity Protection

Invited Users

Lifecycle Workflows

MIM Service

Mobility Management

MyApps

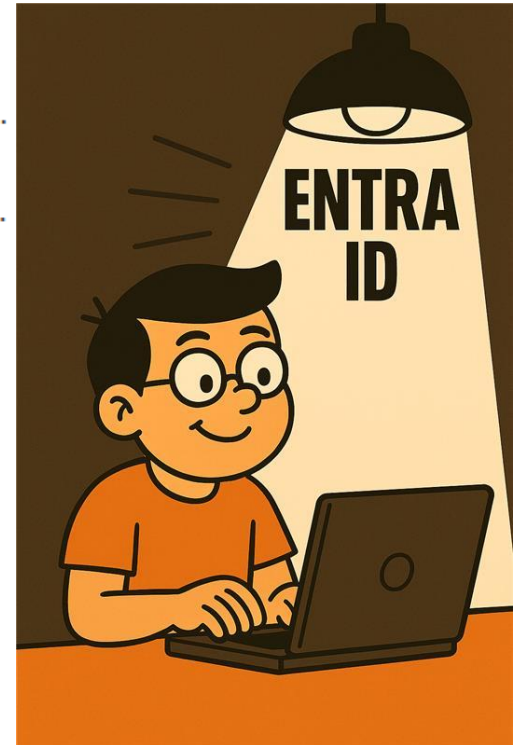
PIM

Self-service Group Managem...

Self-service Password Manag...

Terms Of Use

Verified ID



Audit log

Activity	Target(s)	Modified Properties
Activity		
Date	10/6/2025, 10:07 AM	
Activity Type	Add member to group	
Correlation ID	041135a5-ee87-47d7-b36d-63693f937f18	
Category	GroupManagement	
Status	success	
Status reason		
User Agent		
Initiated by (actor)		
Type	User	
Display Name		
User Principal Name	AlexW@	
Target		
Type	Group	
Id	c7c345a6-b672-4f	
Display Name		
Group Type	unknownFutureValue	
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 Edg/140.0.0.0	

Activity	Target(s)	Modified Properties	
Target	Property Name	Old Value	New Value
AlexW@y...	Group.ObjectID		"c7c345a6-b672-4097-96d8-ba0c63838c28"
AlexW@y...	Group.DisplayN...		"Identity days"

Identity protection : Sign-in risk -> riskEventType

Real-Time / Offline

Premium -> P2 (sinon Additional risk detected)

Defender for Cloud Apps

Sign-in risk detection	Detection type	Type	riskEventType
Activity from anonymous IP address	Offline	Premium	riskyIPAddress
Additional risk detected (sign-in)	Real-time or Offline	Nonpremium	generic ^
Admin confirmed user compromised	Offline	Nonpremium	adminConfirmedUserCompromised
Anomalous Token (sign-in)	Real-time or Offline	Premium	anomalousToken
Anonymous IP address	Real-time	Nonpremium	anonymizedIPAddress
Atypical travel	Offline	Premium	unlikelyTravel
Impossible travel	Offline	Premium	mcasImpossibleTravel
Malicious IP address	Offline	Premium	maliciousIPAddress
Mass Access to Sensitive Files	Offline	Premium	mcasFinSuspiciousFileAccess
Microsoft Entra threat intelligence (sign-in)	Real-time or Offline	Nonpremium	investigationsThreatIntelligence
New country	Offline	Premium	newCountry
Password spray	Real-time or Offline	Premium	passwordSpray
Suspicious browser	Offline	Premium	suspiciousBrowser
Suspicious inbox forwarding	Offline	Premium	suspiciousInboxForwarding
Suspicious inbox manipulation rules	Offline	Premium	mcasSuspiciousInboxManipulationRules
Token issuer anomaly	Offline	Premium	tokenIssuerAnomaly
Unfamiliar sign-in properties	Real-time	Premium	unfamiliarFeatures
Verified threat actor IP	Real-time	Premium	nationStatelP

[What are risk detections? - Microsoft Entra ID Protection](#)

Identity protection : User risk -> riskEventType

Real-Time / Offline

Premium -> P2

Additional risk detected

User risk detection	Detection type	Type	riskEventType
Additional risk detected (user)	Real-time or Offline	Nonpremium	generic ^
Anomalous Token (user)	Real-time or Offline	Premium	anomalousToken
Anomalous user activity	Offline	Premium	anomalousUserActivity
Attacker in the Middle	Offline	Premium	attackerinTheMiddle
Leaked credentials	Offline	Nonpremium	leakedCredentials
Microsoft Entra threat intelligence (user)	Real-time or Offline	Nonpremium	investigationsThreatIntelligence
Possible attempt to access Primary Refresh Token (PRT)	Offline	Premium	attemptedPrtAccess
Suspicious API Traffic	Offline	Premium	suspiciousAPITraffic
Suspicious sending patterns	Offline	Premium	suspiciousSendingPatterns
User reported suspicious activity	Offline	Premium	userReportedSuspiciousActivity

[What are risk detections? - Microsoft Entra ID Protection](#)

Provisioning logs

Inbound ou Outbound provisioning

[Codes d'erreur](#)

Provisioning Logs ...

[Download](#)
[Learn more](#)
[Refresh](#)
[Columns](#)
[Got feedback?](#)

Search

Date : **Last 24 hours**

Show dates as : **Local**

Status : **All**

Action : **All**

[Add filters](#)

Date	Identity	Action	Source System	Target System	Status
11/4/2024, 12:55:06 PM	Source ID eeee4444-ff55-666...	Other	salesforce.com	Microsoft Entra ID	Failure
11/4/2024, 12:53:55 PM	Display Name Purview Investi Source ID a0a0a0a0-bbbb-ccc...	Update	Microsoft Entra ID	salesforce.com	Skipped
11/4/2024, 12:53:55 PM	Display Name Jonathan W Source ID c2c2c2c2-dddd-ee... Target ID a6a6a6a6-bbbb-cc...	Other	salesforce.com	Microsoft Entra ID	Skipped
11/4/2024, 12:53:55 PM	Display Name ZT MC Source ID f5f5f5f5-aaaa-bbb...	Create	Microsoft Entra ID	salesforce.com	Skipped
11/4/2024, 12:53:55 PM	Display Name ProSales Source ID b1b1b1b1-cccc-dd...	Create	Microsoft Entra ID	Google Cloud / Workspace	Success
11/4/2024, 12:53:55 PM	Display Name Lic.M365 Source ID d3d3d3d3-eeee-fff...	Create	Microsoft Entra ID	Google Cloud / Workspace	Success
11/4/2024, 12:53:55 PM	Display Name Salesforce Admir Source ID b1b1b1b1-cccc-dd...	Create	Microsoft Entra ID	Google Cloud / Workspace	Success



Et les ranger où ?

Rétention

Type de log	Free	P1	P2
Sign-ins	7 jours	30 jours	30 jours
Audit	7 jours	30 jours	30 jours
Risky users	Pas de limite	Pas de limite	Pas de limite
Risky Sign-ins	7 jours	30 jours	90 jours

Question : je dois diagnostiquer un risque interne datant de 8 jours sur une version free et je veux passer en P1 pour avoir accès aux données qui m'intéressent

[Microsoft Entra data retention](#)

Téléchargement

A partir du portail

Des limites :

- Audit 250k
- Sign-ins 100k
- Provisionning 100k
- Risky sign-ins 250k
- Risky users 250k

Filtre

- Toutes les colonnes mais certaines seront vides

Pas de prérequis de licence lié au téléchargement



Download JSON

Download CSV



Download Sign-ins in JSON format



i You can download up to a maximum of 100,000 records per file (e.g. if you are downloading the interactive and non-interactive sign-ins files, you will get 100,000 rows for each file). If you want to download more, use our reporting APIs or export to a storage account, SIEM or Log Analytics through "Export Data Settings". Click here to learn more.

i Your download will be based on the filter selections you have made.

File Name

Download

File Name

Download

File Name

Download

File Name

Download

APIs

Nécessite un niveau de licence P1

Tester avec Graph Explorer : <https://aka.ms/ge>

Autoriser avec le rôle *Privileged Role Administrator*

yd6vz

Sign out

JL

Jipe Lesage

jplesage@onmicrosoft.com

AAD

Consent to permissions

Sign in with a different account



GET
v1.0
https://graph.microsoft.com/v1.0/identityProtection/riskyUsers?\$filter=riskLevel eq 'medium'
Run query

Request Body
Request Headers
Modify Permissions
Access token

One of the following permissions is required to run the query. If possible, consent to the least privileged permission.

Permission	Description	Admin consent required	Status	Consent type
IdentityRiskyUser.Read.All	Allows the app to read identity risky user information for all users in your organization on behalf of the signed-in user.	Yes	Unconsent	Principal

OK - 200 - 91 ms

Response preview
Response headers
Code snippets
Toolkit component
Adaptive cards

```

{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#identityProtection/riskyUsers",
  "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For example: GET identityProtection/riskyUsers?$select=isDeleted,isProcessing",
  "value": [
    {
      "id": "fc74545b-503e-4917-87b1-782855068c0f",
      "isDeleted": false,
      "isProcessing": false,
      "riskLevel": "medium",
      "riskState": "atRisk",
      "riskDetail": "none",
      "riskLastUpdatedDateTime": "2025-08-22T12:09:10.9524507Z",
      "userDisplayName": "Alex Wilber",
      "userPrincipalName": "jlesage@onmicrosoft.com"
    }
  ]
}

```

Exporter les logs

Dans Diagnostic setting

Storage Account

Log Analytics workspace

Event hub

Partner Solution

Diagnostic setting ...

 Save
  Discard
  Delete
  Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

Logs

Categories

☒ AuditLogs

☒ SignInLogs

☐ NonInteractiveUserSignInLogs

☐ ServicePrincipalSignInLogs

☐ ManagedIdentitySignInLogs

Destination details

☐ Send to Log Analytics workspace

☐ Archive to a storage account

☐ Stream to an event hub

☐ Send to partner solution



 In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

Storage Account

Rôle Security administrator

Lifecycle Management du Storage Account pour la rétention

- Jouer sur les règles



 Storage retention via diagnostic settings is being deprecated and new rules can no longer be configured. To maintain your existing retention rules please migrate to Azure Storage Lifecycle Management by September 30th 2025. [What do I need to do?](#)

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name * Export Storage Account ✓

Logs

Categories

- ☒ AuditLogs
- ☒ SignInLogs
- ☐ NonInteractiveUserSignInLogs
- ☐ ServicePrincipalSignInLogs
- ☐ ManagedIdentitySignInLogs
- ☐ ProvisioningLogs
- ☐ ADFSSignInLogs
- ☐ RiskyUsers

Destination details

☐ Send to Log Analytics workspace

☒ Archive to a storage account

 You'll be charged normal data rates for storage and transactions when you send diagnostics to a storage account.

 Showing all storage accounts including classic storage accounts

Location

All

Subscription

MCT - Visual Studio Enterprise

Storage account *

testmdfcjp

[How to archive activity logs to a storage](#)

Log Analytics workspace

Avoir un workspace à disposition

Rôles

- Log Analytics Reader
- Reports Reader (pour KQL)

KQL

Logs

Categories

- ☒ AuditLogs
- ☒ SignInLogs
- ☐ NonInteractiveUserSignInLogs

Destination details

☒ Send to Log Analytics workspace

Subscription

MCT - Visual Studio Enterprise

Log Analytics workspace

LogsEntra (eastus)

LogsEntra

Select scope

Run

Time range : Last 7 days

Save

Share

New alert rule

Export

Pin to

Format query

1 SignInLogs | take 10

Results

TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category
> 10/7/2025, 7:57:54.896 AM	/tenants/i	/provid... Sign-in activity	1.0	SignInLogs
> 10/7/2025, 7:56:58.362 AM	/tenants/i	/provid... Sign-in activity	1.0	SignInLogs
> 10/7/2025, 7:56:31.402 AM	/tenants/i	/provid... Sign-in activity	1.0	SignInLogs

[Configure a Log Analytics workspace and a custom workbook - Microsoft Entra ID](#)

TimeGenerated avec Azure Monitor



TimeGenerated devient le moment où il est reçu et publié par Log Analytics.

Bien utiliser *CreatedDateTime* pour avoir la date de l'événement d'authentification.

Pour le Sign-in Risk c'est équivalent mais il faut alors utiliser le *CorrelationId* pour faire le rapprochement avec l'événement dans le Sign-in log.

Event hub

L'évent hub doit être sur un abonnement lié au tenant

Splunk, SumoLogic et ArcSight

Logs

Categories

- ☒ AuditLogs
- ☒ SignInLogs
- ☐ NonInteractiveUserSignInLogs
- ☐ ServicePrincipalSignInLogs
- ☐ ManagedIdentitySignInLogs
- ☐ ProvisioningLogs
- ☐ ADFSSignInLogs
- ☐ RiskyUsers

Destination details

- ☐ Send to Log Analytics workspace
- ☐ Archive to a storage account

- ☒ Stream to an event hub

For potential partner integrations, [click to learn more about event hub integration](#).

Subscription

MCT - Visual Studio Enterprise

Event hub namespace *

logsentra

Event hub name (optional) ⓘ

No event hubs found

Event hub policy name

RootManageSharedAccessKey

[Stream Microsoft Entra logs to an event hub](#)

Microsoft Sentinel

Content hub -> Solution Microsoft Entra ID

- Connecteur Entra ID
- 73 analytics rule
 - Comptes, CA, modifications...
- 11 playbooks
 - Block, reset, revoke...
- 2 workbooks
 - Sign-in et Audit



Microsoft Entra ID **FEATURED**

Installed

Solution



Configuration

Connect Microsoft Entra ID logs to Microsoft Sentinel
Select Microsoft Entra ID log types:

☐ Sign-In Logs

① In order to export Sign-in data, your organization needs Microsoft Entra ID P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

☐ Audit Logs

☐ Non-Interactive User Sign-In Log

☐ Service Principal Sign-In Logs

☐ Managed Identity Sign-In Logs

☐ Provisioning Logs

☐ ADFS Sign-In Logs

☐ User Risk Events

☐ Risky Users

☐ Network Access Traffic Logs

☐ Risky Service Principals

☐ Service Principal Risk Events

☐ Microsoft Graph Activity Logs

☐ Enriched Office365 Audit Logs

☐ Remote Network Health Logs

Apply Changes

Microsoft 365 E5, A5, F5, and G5, and Microsoft 365 E5, A5, F5, and G5 Security customers can receive a data grant of up to 5MB per user per day to ingest Microsoft 365 data. This offer includes the following data sources:

- Microsoft Entra ID (formerly Azure AD) sign-in and audit logs

Arbre de choix



Estimation des coûts

Une entrée Sign-ins log : 11,5 ko en moyenne

Une entrée audit log : 2 ko en moyenne

Un tenant de 100k utilisateurs : 1,5 M événements par jour

Prendre un échantillon de log

- Attention aux pics dans la journée
- Attention à la répartition géographique

Utiliser le service Cost Analysis d'Azure

[Estimation des coûts](#)



Quelques pistes pour
aller plus loin

Flag Sign-in

Pour le troubleshooting, l'utilisateur peut valider le Flag Sign-in pour une durée de 20 mns

Utilisateur

 Microsoft

alexw@...onmicrosoft.com

Request denied

We sent an identity verification request to your mobile device, but you denied it. [View details](#)

[Send another request to my Microsoft Authenticator app](#)

Having trouble?

Enter a [security code](#) from your Microsoft account or authenticator app instead.

If you can't use an app right now [get a code a different way](#).

[More information](#)

Troubleshooting details

If you contact your administrator, send this info to them.
[Copy info to clipboard](#)

Error Code: 500121
Request Id: 2ed212d8-3d40-42d5-9ba5-528806310e00
Correlation Id: 0b69ac8b-d89d-4f24-b5bb-a75457453760
Timestamp: 2025-10-07T08:25:38Z

Flag sign-in errors for review [Disable flagging](#)

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

Cancel

Analyste

×

Add filter

Show dates as: UTC

Date range: Last 24 hours

Flagged for review: Yes ×

Reset filters

User sign-ins (interactive)

User sign-ins (non-interactive)

Service principal sign-ins

Managed identity sign-ins

Date ↓	Request ID	User principal name	Application	Status	IP address	Resource	F	
2025-10-07T08:32:44Z	86655711-3a4b-417a-9f4b-5ee9...	alexw@...	inmicros...	My Apps	Interrupted	40.76.240.3	Microsoft Graph	0
2025-10-07T08:31:51Z	843e1afe-e3b2-4d3c-bc68-8b63...	alexw@...	inmicros...	My Apps	Interrupted	40.76.240.3	Microsoft Graph	0

Home > [Sign-in events](#) >

Diagnose and solve problems ...

↶ Start Over

👤 New Support Request

🗣️ Got feedback? ▾

Troubleshooting problem: Sign-in Diagnostic

Flagged Sign-In Events

All Sign-In Events

Flag Sign-in -> Diagnose

Utilisation de Tor

[Flagged Sign-In Events](#)
[All Sign-In Events](#)

Failed sign-in events which were flagged by users in your organization in the last 10 days (limited to 100 events). Select the event you are interested in investigating by clicking on it.

Flagged Sign-In Events						
	createdDateTime	userDisplayName	userPrincipalName	appDisplayName	status	errorCode
☒	2025-10-13T12:20:47Z	Alex Wilber	alexw@yd6vz.onmicrosoft.com	My Apps	Failure	530031
	2025-10-13T12:12:25Z	fc74545b-503e-4917-87b1-782855068c0f	fc74545b-503e-4917-87b1-782855068c0f	My Apps	Failure	500121



SignIn Error Details

Based on the information you provided we have identified following issue and recommend taking the action to resolve the issue.

Error Code: 530031

Message: Access policy does not allow token issuance.

Action: A classic conditional access policy, or a policy from Azure AD Identity Protection, prevented this resource from being accessed. View the Conditional Access information for this request in the sign-in logs for more details about the policy applied here.

- [More details on this topic](#)

Troubleshooting Sign-in

Activity Details: Sign-ins

Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only
Date	8/18/2023, 7:46:06 AM				
Request ID	1111aaa-000011-aabb-111bbbb000				
Correlation ID	cccc2222-dd33-4444-55ee-666666fffff				
Authentication requirement	Multifactor authentication				
Status	Failure				
Continuous access evaluation	No				
Sign-in error code	500121				
Failure reason	Authentication failed during strong authentication request.				
Additional Details	The user didn't complete the MFA prompt. They may have decided not to authenticate, timed out while doing other work, or has an issue with their authentication setup. Follow these steps:				
Troubleshoot Event	Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.				
User	Semyon Maslov				
Username	semaslov@woodgrovegroceries.com				
User ID	44ee44ee-ff55-aa66-bb77-88cc88cc88cc				

Activity Details: Sign-ins

Basic info	Location	Device info	Authentication details	Conditional access	Report only
Location	Palaiseau, Essonne, FR				
IP address	Mon @IP				
Through global secure access	No				
Autonomous system number	15557 → SFR (MS = 8075)				
Named location type	Location name				
Basic info	Location	Device info	Authentication details	Conditional access	Report only
Device ID	716dd72b-e46d-45f7-a82a-c26b583f00e4				
Device browser	Edge 140.0.0				
Operating system	Windows10				
Compliant	No				
Managed	No				
Join Type	Azure AD registered				

Troubleshooting Sign-in (audience)

Dans la partie *Conditional Access Policy details*

Authentification mais demande d'accès à plusieurs ressources

Quid si une règle d'accès conditionnel cible Sharepoint online ?

Audience ⓘ	Application Id
Microsoft Teams Services	cc15fd57-2c6c-4117-a88c-83b1d56b4bbe
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 SharePoint Online	00000003-0000-0ff1-ce00-000000000000
Skype for Business Online	00000004-0000-0ff1-ce00-000000000000

Code d'erreur

Net helpmsg ?

<https://login.microsoftonline.com/error> ou <https://login.microsoftonline.com/error?code=500121>

←

↺

🔒

https://login.microsoftonline.com/error

Error Code:

Code..

Submit

Error Code	500121
Message	Authentication failed during strong authentication request.
Remediation	The user didn't complete the MFA prompt. They may have decided not to authenticate, timed out while doing other work, or has an issue with their authentication setup.

[Microsoft Entra authentication & authorization error codes](#)



21 octobre 2025 - PARIS



IDENTITY DAYS



@IdentityDays
#identitydays2025