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

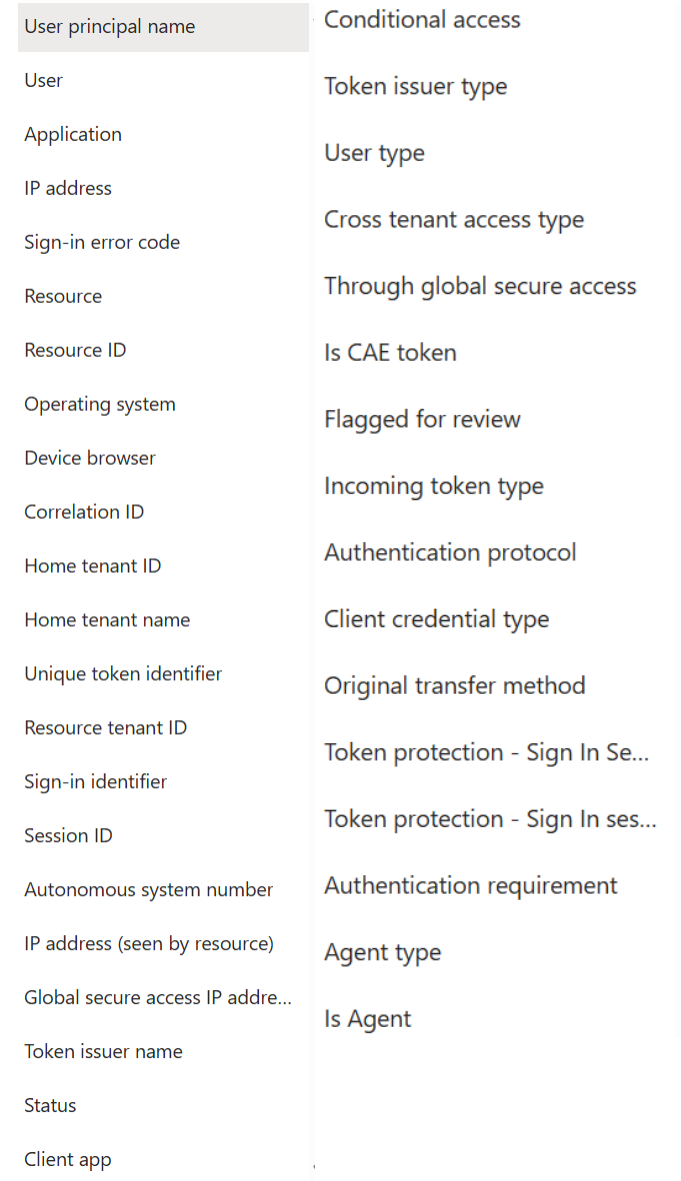
Nécessite un niveau de licence P1

> ⓘ 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



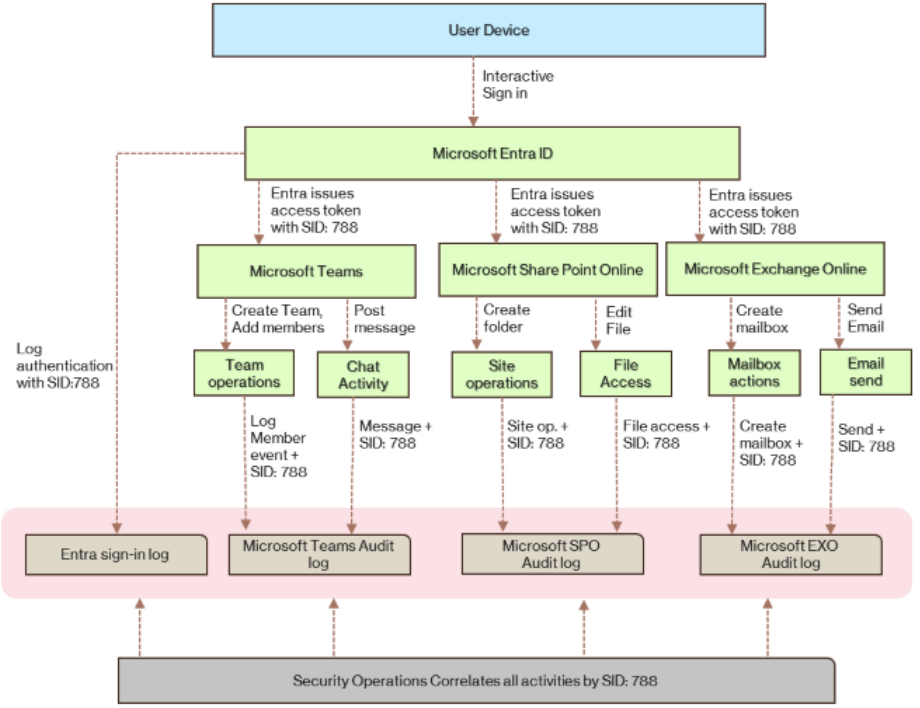
Linkable Identifiers

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

Basé sur la session ou le jeton

Disponibles pour

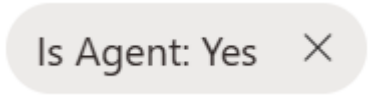
- Microsoft Entra sign-in logs
- Microsoft Exchange Online audit logs
- Microsoft Graph activity logs
- Microsoft SharePoint Online audit logs
- Microsoft Teams audit logs



[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 

[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	
Object ID	64171c5e-cb55-4483-8cec-4648beda9ac2
IP address	
User Principal Name	jplesage@
Additional Details	
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

Type	User
Id	fc74545b-503e-4
Display Name	
User Principal Name	AlexW@

Target

Type	Group
Id	c7c345a6-b672-4
Display Name	
Group Type	unknownFutureValue

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	nationStateIP

What are risk detections? - Microsoft Entra ID Protection

Identity protection : User risk -> riskEventType

Real-Time / Offline

Premium -> P2

Additional risk detected

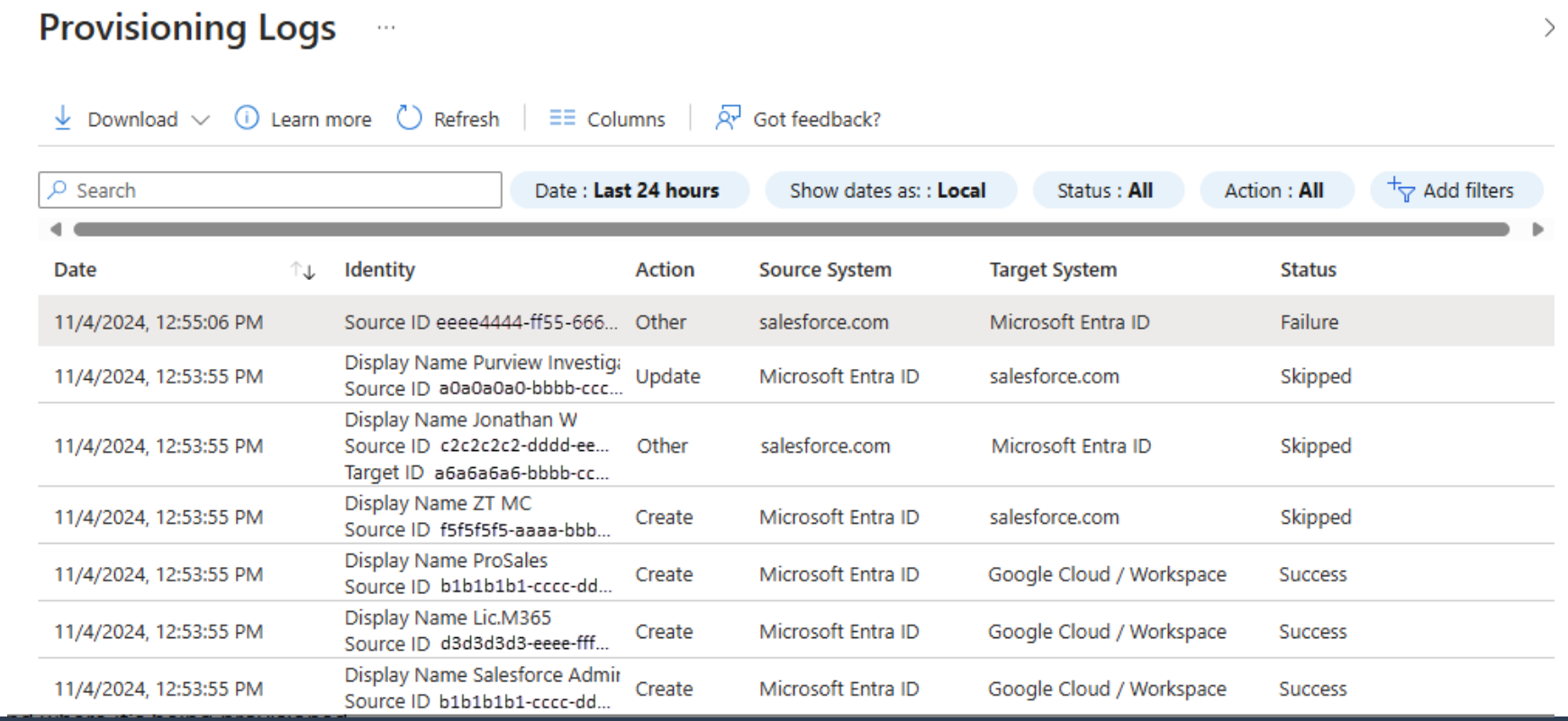
User risk detection	Detection type	Type	riskEventType
Additional risk detected (user)	Real-time or Offline	Nonpremium	generic ^
Anomalous Token (user)	Real-time or Offline	Premium	anomalousToken
Anomalous user activity	Offline	Premium	anomalousUserActivity
Attacker in the Middle	Offline	Premium	attackerinTheMiddle
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]



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

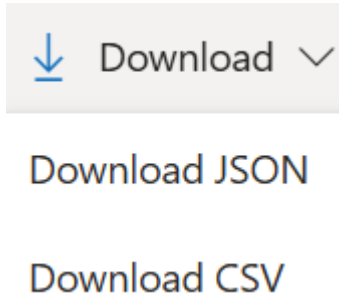
A partir du portail
Des limites :

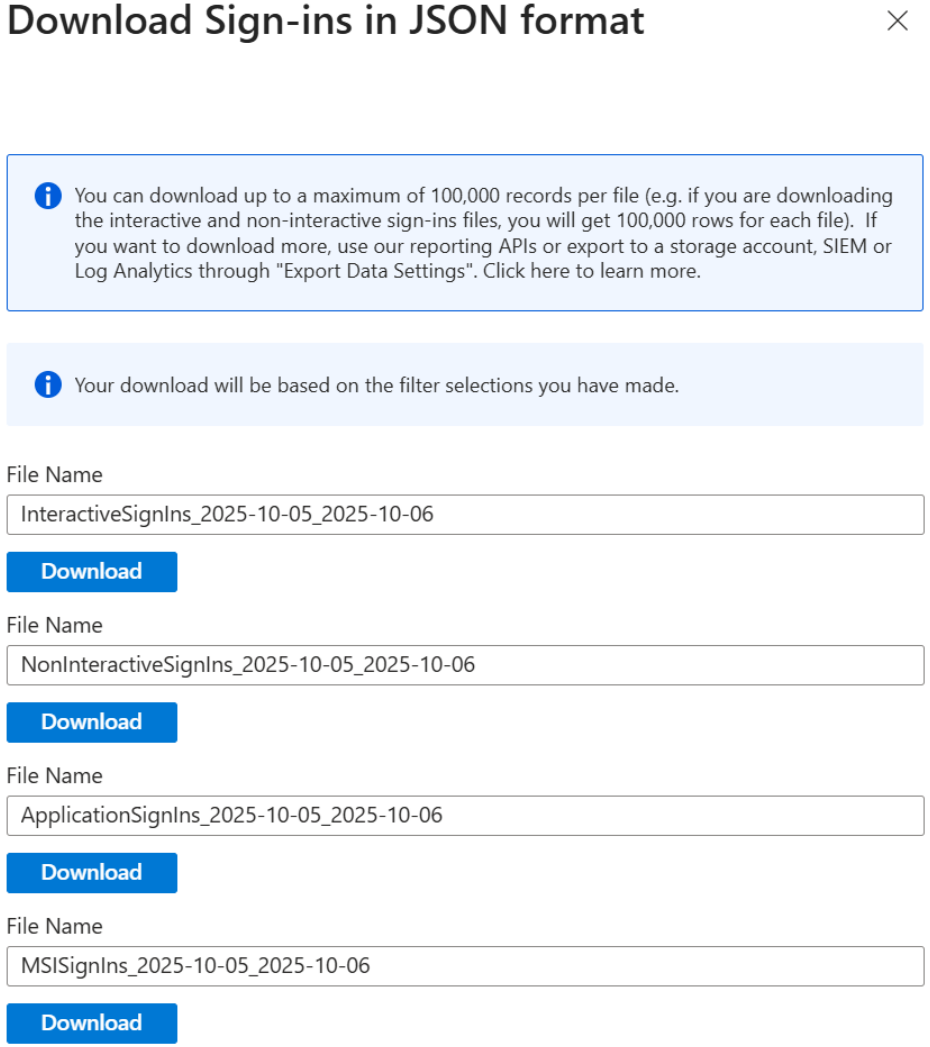
- Audit 250k
- Sign-ins 100k
- Provisionning 100k
- Risky sign-ins 250k
- Risky users 250k

Filtre

- Toutes les colonnes mais certaines seront vides

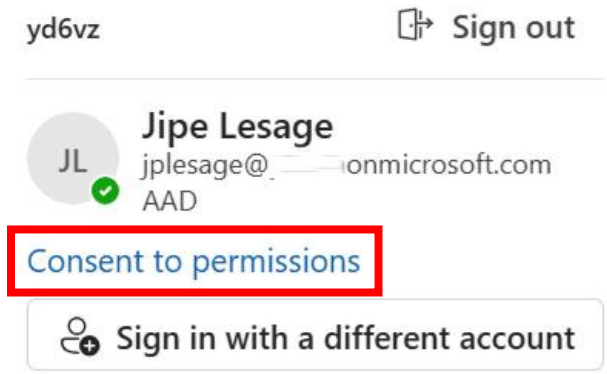
Pas de prérequis de licence lié au téléchargement

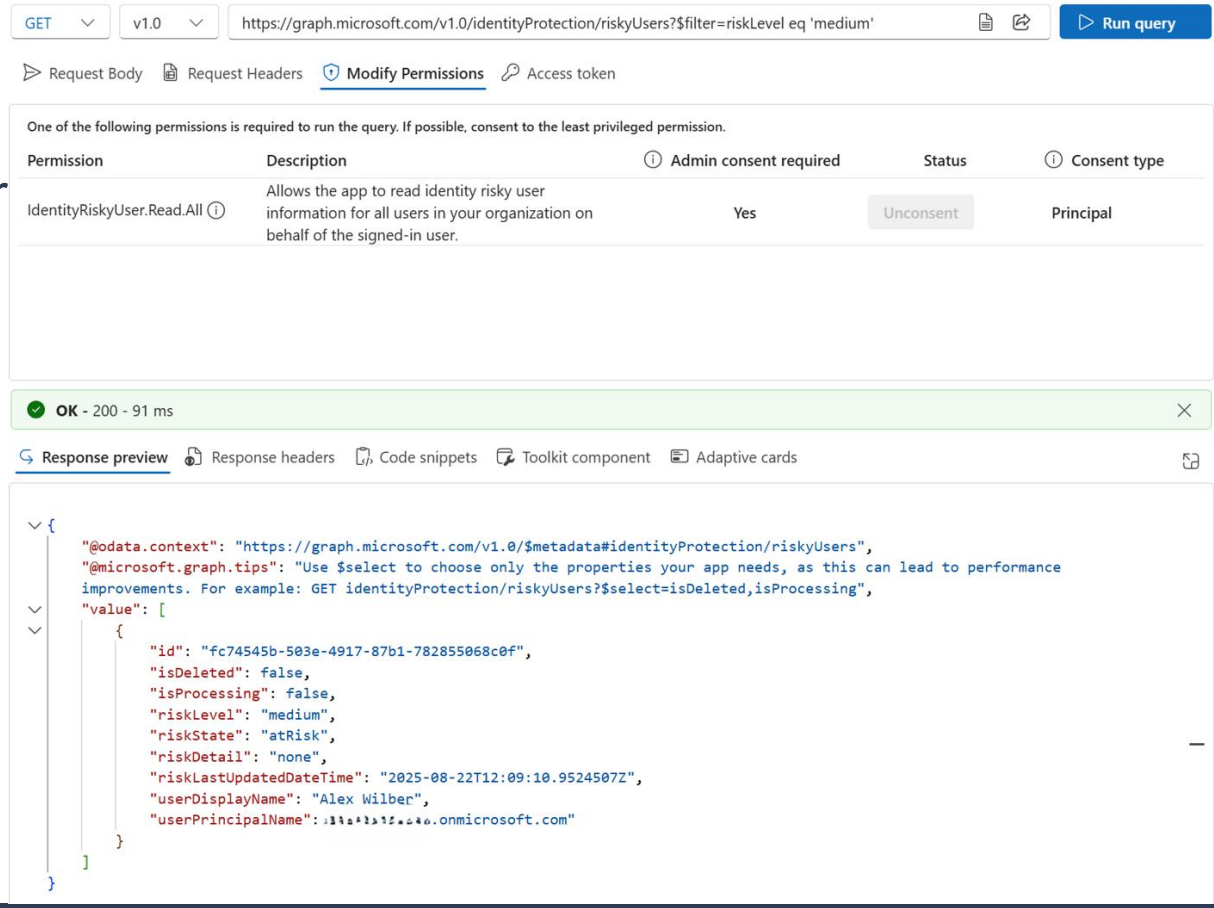




APIs

Nécessite un niveau de licence P1
Tester avec Graph Explorer : https://aka.ms/ge
Autoriser avec le rôle *Privileged Role Administrator*





Exporter les logs

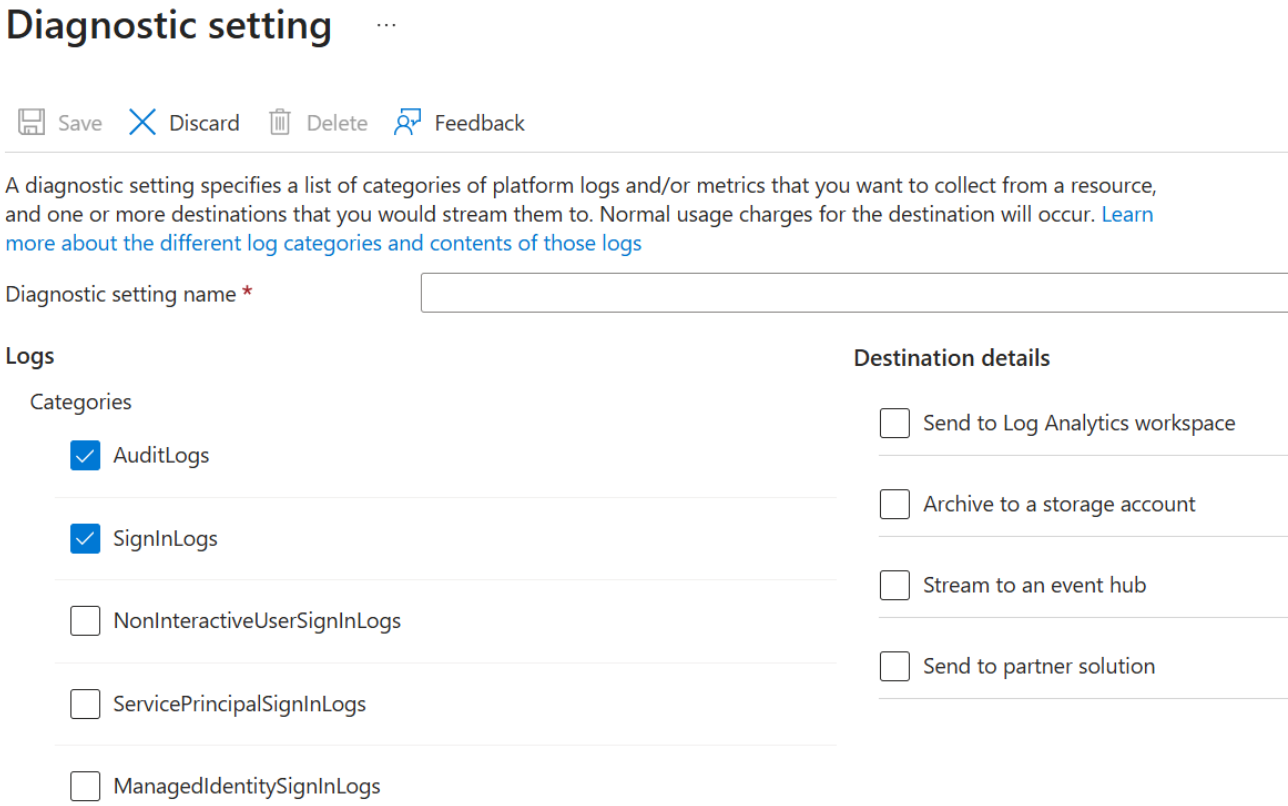
Dans Diagnostic setting

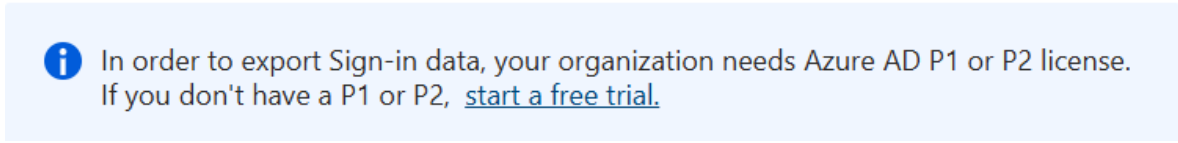
Storage Account

Log Analytics workspace

Event hub

Partner Solution



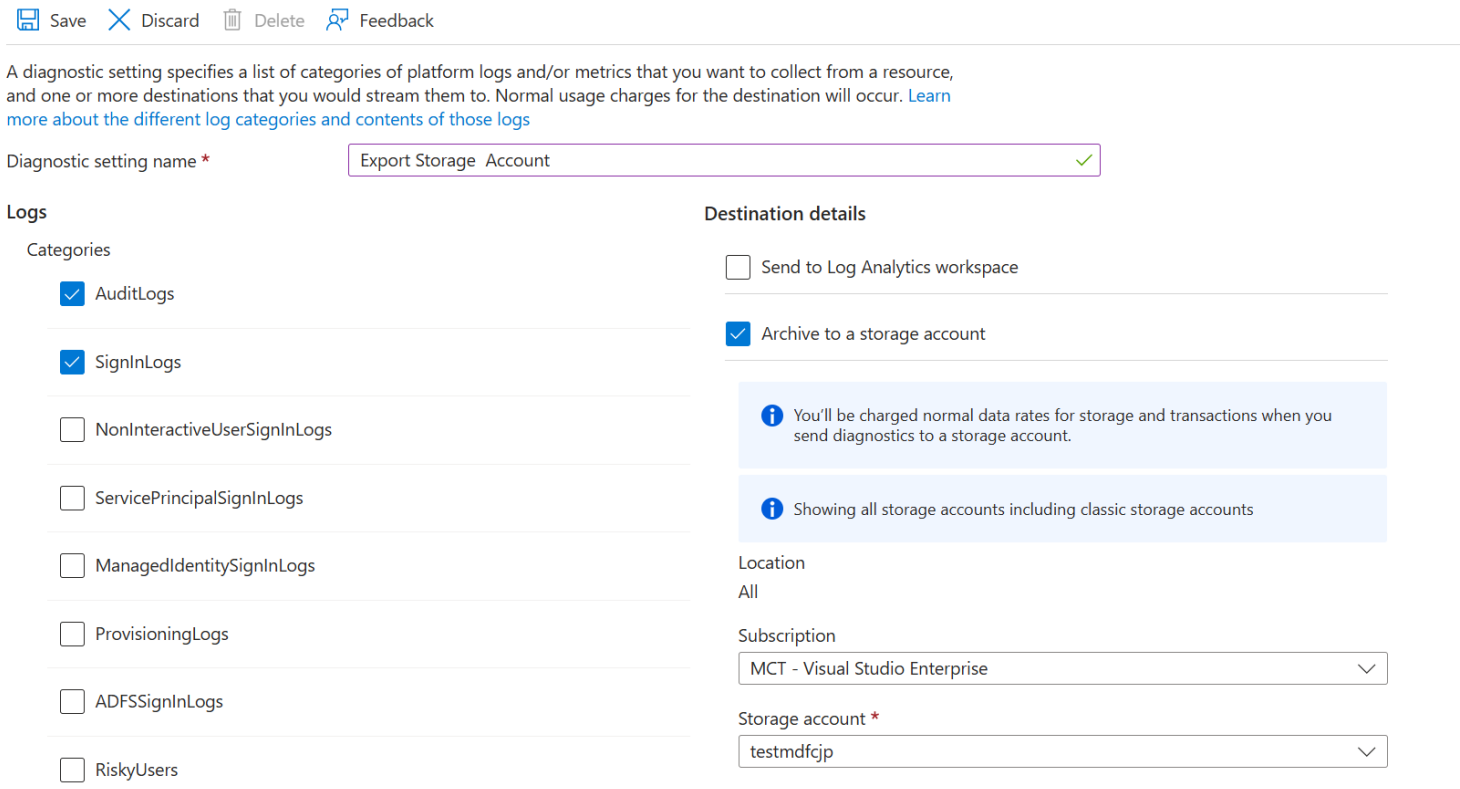


Storage Account

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?

How to archive activity logs to a storage

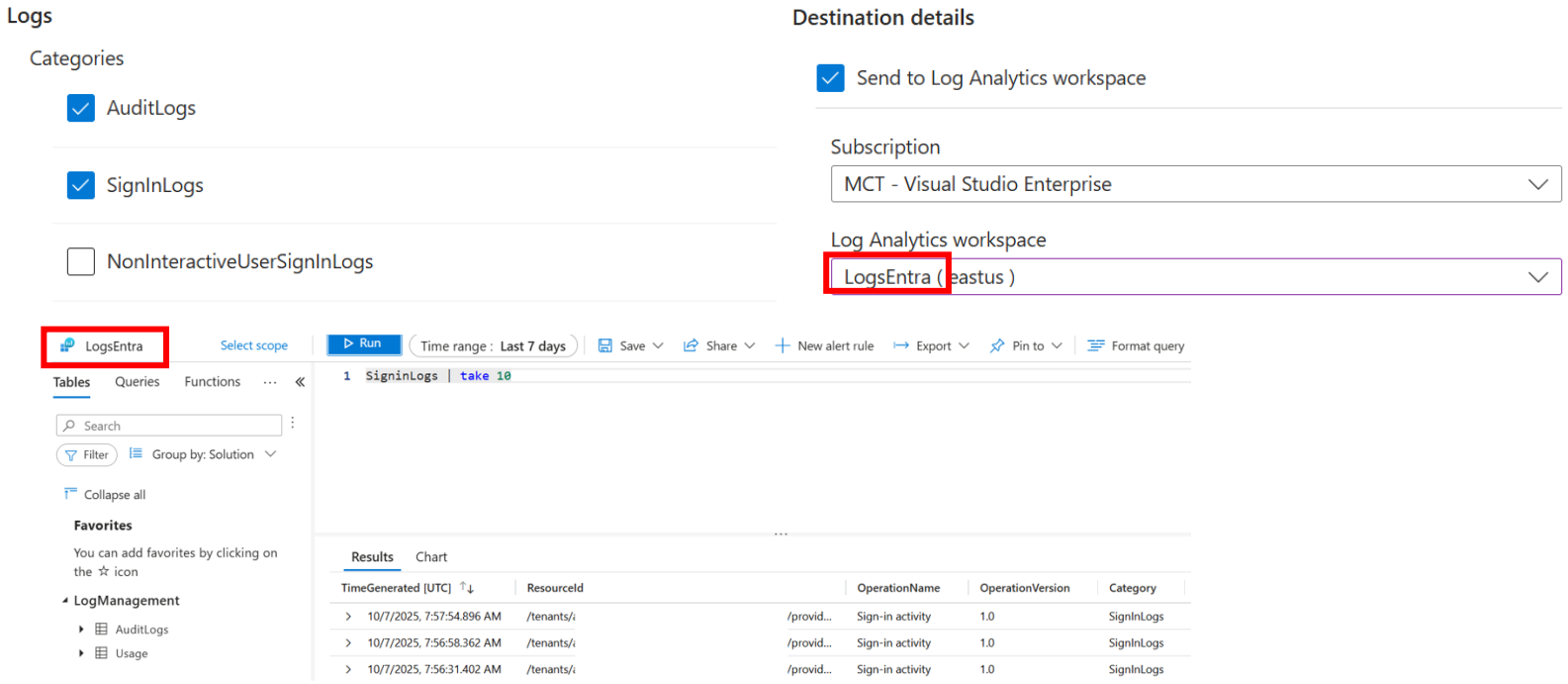
Log Analytics workspace

Avoir un workspace à disposition

Rôles

- Log Analytics Reader
- Reports Reader (pour KQL)

KQL



[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.

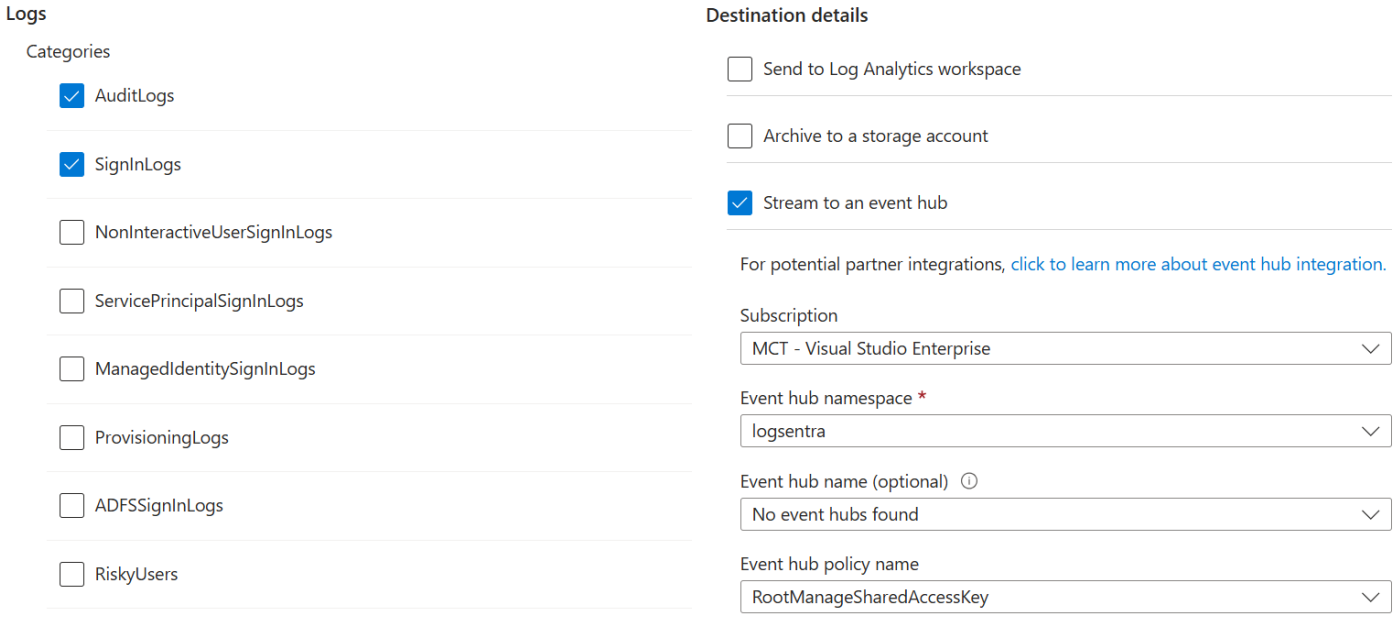
Bien utiliser *CreatedDateTime* pour avoir la date de l'événement d'authentification.

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'event hub doit être sur un abonnement lié au tenant

Splunk, SumoLogic et ArcSight

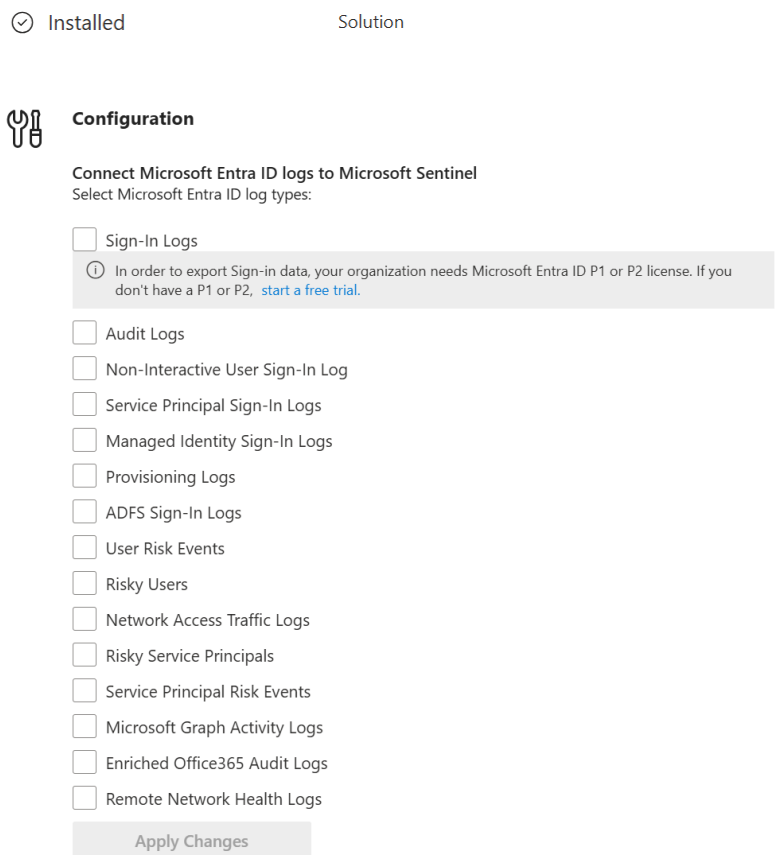


[Stream Microsoft Entra logs to an event hub]

Microsoft Sentinel

Content hub -> Solution Microsoft Entra ID

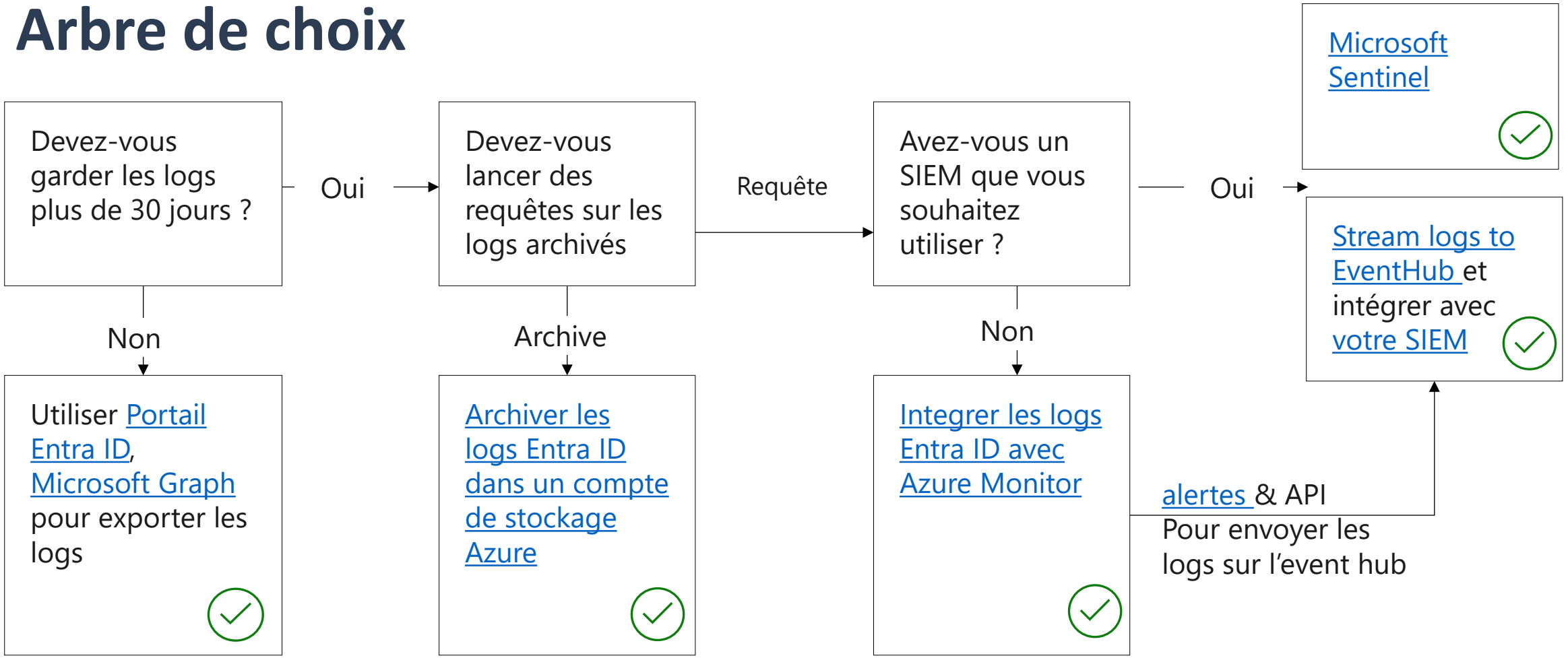
- Connecteur Entra ID
- 73 analytics rule
  - Comptes, CA, modifications…
- 11 playbooks
  - Block, reset, revoke…
- 2 workbooks
  - Sign-in et Audit



Microsoft 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

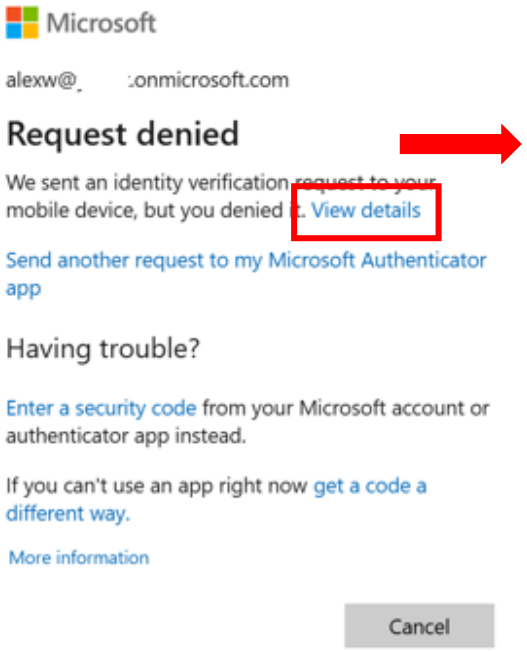
Estimation des coûts

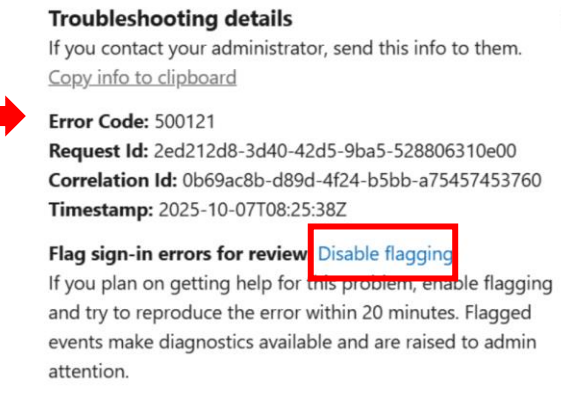
Quelques pistes pour aller plus loin

Flag Sign-in

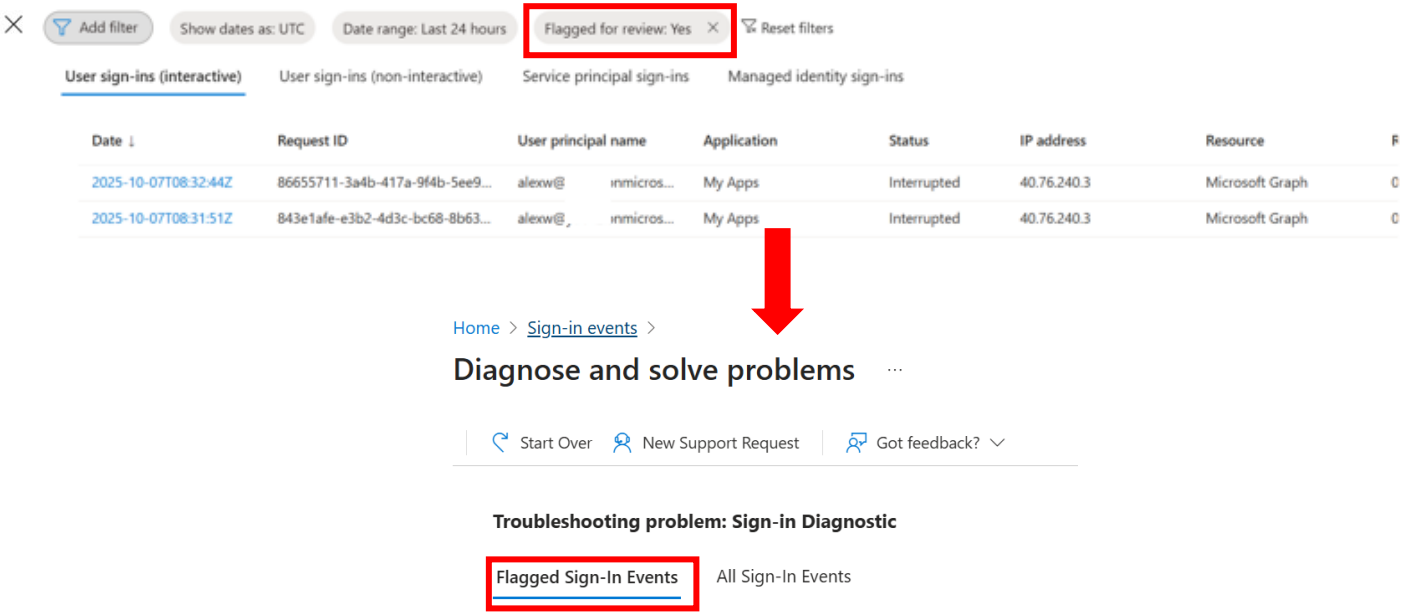
Pour le troubleshooting, l'utilisateur peut valider le Flag Sign-in pour une durée de 20 mns

Utilisateur



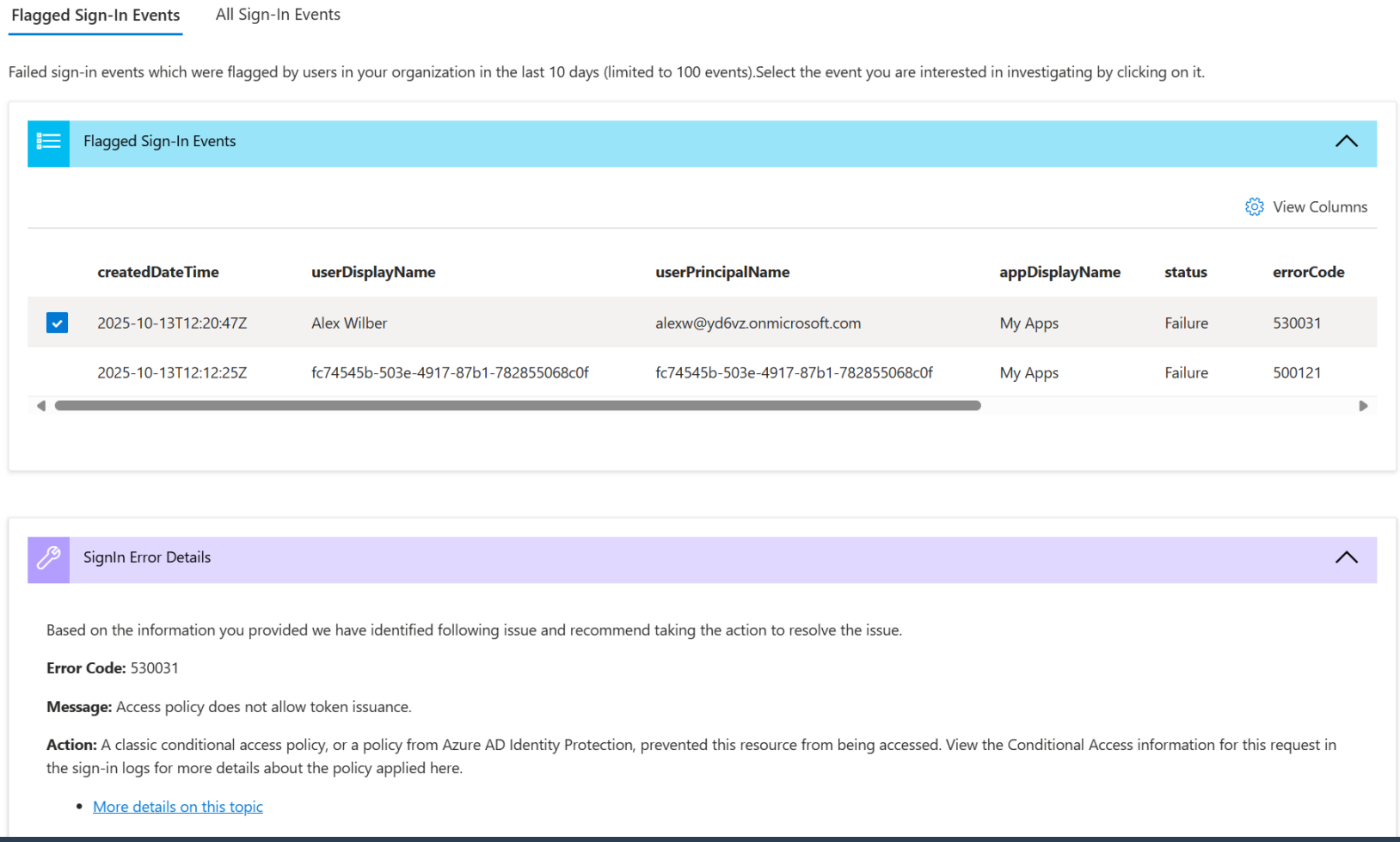


Analyste



Flag Sign-in -> Diagnose

Utilisation de Tor



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-111bbbbb000
Correlation ID	cccc2222-dd33-4444-55ee-666666ffffff
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.
Troubleshoot Event	Follow these steps: 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)

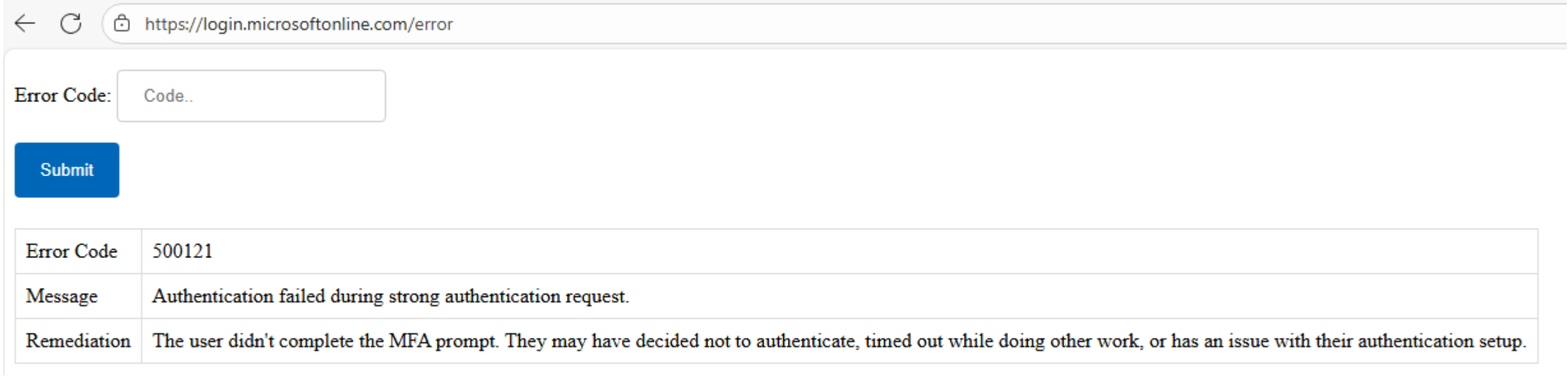
Dans la partie *Conditional Access Policy details*
Authentification mais demande d'accès à plusieurs ressources
Quid si une règle d'accès conditionnel cible Sharepoint online ?

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



Microsoft Entra authentication & authorization error codes

IDENTITY DAYS

21 octobre 2025 - PARIS

21 octobre 2025 - PARIS

IDENTITY DAYS

@IdentityDays
#identitydays2025