



# IDENTITY DAYS

27 octobre 2022 - PARIS



@IdentityDays #identitydays2022

Merci à tous nos partenaires !





@IdentityDays #identitydays2022

# IDENTITY DAYS

27 octobre 2022 - PARIS

Où en est-on sur le chemin de la  
modernisation de l'authentification ?

Jeudi 27 octobre 2022 – 16h00 / 16h45



Thibault Joubert  
IDECSI



Julien Rousson  
WAVESTONE



# Où en est on de la modernization de l'authentification ?

Thibault JOUBERT  
Julien ROUSSON

# AGENDA DE LA CONFÉRENCE

## Thibault JOUBERT

Product Manager chez IDECSI, une plateforme de sécurité autour des plateformes de collaboration, dont Office 365, centrée autour des utilisateurs.

MVP Office Apps & Services.

## Julien ROUSSON

Manager chez WAVESTONE  
Expert dans les solutions Digital Workplace, je mène des grands programmes de transformation  
Leader de l'offre M&A / Carveout

- Les enjeux de l'authentification
- Les moyens pour moderniser l'authentification
- Quelle cibles & conseils
- Retour d'expériences

# Les enjeux de l'authentification

## Pourquoi doit on s'authentifier ?



- Identification de l'utilisateur
- Contextualisation de la réponse et des services accédés



- Identification du terminal
- Connaissance du statut du terminal (Managed / UnManaged) et des moyens de protection (eg. conteneurs)
- Accès à des services de manière indépendante de l'utilisateur (eg. VPN machine, SASE ...)



- L'authentification forte repose sur une preuve pérenne (eg. certificats) nécessitant une forte puissance de calcul pour la compromettre
- L'authentification Multifacteurs implique la validation de plusieurs facteurs (eg. 2FA, 3FA...)

## Pourquoi se pose la question de moderniser l'authentification ?

## Enjeux

### Historique

Bien que les **standards** d'authentification **évoluent** de manière conjointe avec les enjeux de sécurité et les évolutions technologiques, les chantiers d'évolutions sont lancés avec du délai dans les entreprises

Dette techno.

### Authentification basique

L'authentification basique est l'un des **vecteurs de compromission** le plus important – 99,9%(1)  
 Son usage est en **perte de vitesse** (dans le domaine de l'entreprise comme pour le grand public). De nombreux fournisseurs (dont Microsoft) sont en train de la **remplacer** par des **mécanismes plus résistants** (OAuth / SAML)  
 Les entreprises se confrontent à deux possibilités : soit elles subissent des **évolutions forcées** par les fournisseurs de services, soit via **l'évolution des standards et des politiques de sécurité**

Sécurité

### Evolution du SI

Conjonction de plusieurs **facteurs majeurs d'évolution** signant la fin du sacro-saint réseau d'entreprise comme un **château fort** (#ZeroTrust):

- Le travail à distance doit proposer le même confort que le travail dans les locaux
- Massification des services Cloud
- Evolution des accès Internet (SASE, Local Break out)

Sécurité

UX

### Usages

La phase d'authentification est perçue comme **non productive** par l'utilisateur qui devient conséquente sur une journée de travail : nombreuses authentification du fait du volume de services car ...  
 ... Le chemin de consolidation des référentiels d'authentification n'est pas encore atteint dans de nombreuses entreprises (#SIRH, #IAM, #AD, #AAD, #IDPTiers, #LocalAuth) et ...  
 ... de nombreux services ne s'intègrent pas à un SSO et de facto le post-it perdure  
**Le MFA n'est qu'une partie de la réponse !**

Securité

UX

## Détails dans les enjeux

### Dette techno.

- Méthode d'authentification non éligible à l'analyse conditionnelle (eg. authentification sur Active Directory)
- Applications & services ne pouvant déléguer l'authentification (eg. base locale d'authentification)
- Authentification SSO transparente via des outils de rejeu de credentials (en particulier pour les clients lourds)



### Sécurité

- « Identity est le nouveau périmètre »
- Trop d'administrateurs n'ont pas de MFA (2)
- Le MFA ne suffit pas (fatigue)
- Configuration de la stratégie d'accès conditionnel (inclusif vs exclusif)
- Sécurisation des authentifications applicatives : 5 à 20 pour 1 (3)



### UX

- L'expérience employée est au centre des préoccupations des employeurs pour conserver leur talents – 13%(1) étant pleinement satisfaits
- Proposer une expérience fluide et transparente pour accéder aux ressources & services quelque soit la situation de travail de l'utilisateur tout restant aligné sur les standards de sécurité du marché

# Les moyens pour moderniser l'authentification

## Reminder : Azure Active Directory vs. Active Directory

### Entra

#### Active Directory :

Annuaire historique de Microsoft disponible depuis les années 2000. Il est traditionnellement hébergé de façon on-premises et/ou en IaaS  
 Les évolutions sont désormais très rares (eg. niveau fonctionnel max 2016)

#### Azure Active Directory :

Annuaire Microsoft apparu avec les services Office 365 & Azure  
 Services accessibles depuis Internet

Contrairement à AD qui n'évolue plus, AAD bénéficie des évolutions au sein de Microsoft Entra

#### Active Directory Cloud / Active Directory Azure :

Terme utilisé pour signifier l'hébergement de l'Active Directory au sein de fournisseur IaaS. Ce terme ne fait pas référence à une technologie mais à une situation d'hébergement

#### Azure Active Directory Domain Services :

Annuaire Active Directory fourni sous la forme d'un service PaaS, provisionné depuis Azure Active Directory et utilisable principalement pour le lift & shift de serveurs sur le IaaS Azure

Azure Active Directory

Entra Permissions Management

Entra Verified ID

Entra Identity Governance

## Reminder : Azure Active Directory vs. Active Directory

Azure Active Directory est une version cloud (PaaS) de l'Active Directory



Azure Active Directory propose toutes les fonctions d'Active Directory



GPOs, Domain Join, OU, ...

Azure Active Directory propose des fonctions inexistantes sur Active Directory



SAMLv2, GraphAPI, GBL, sécurité, etc.

Azure Active Directory est le référentiel d'identité pour Office 365

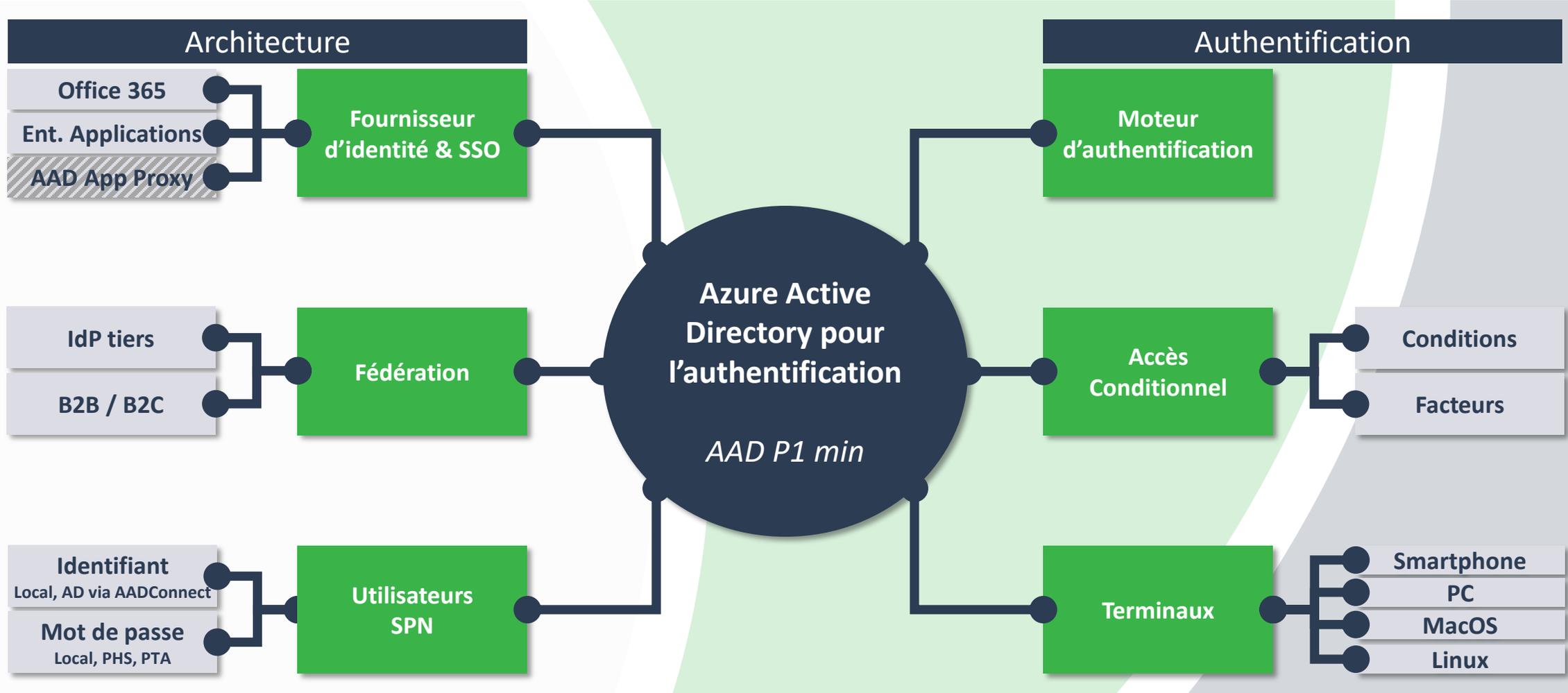


Azure Active Directory est limité aux services Office 365



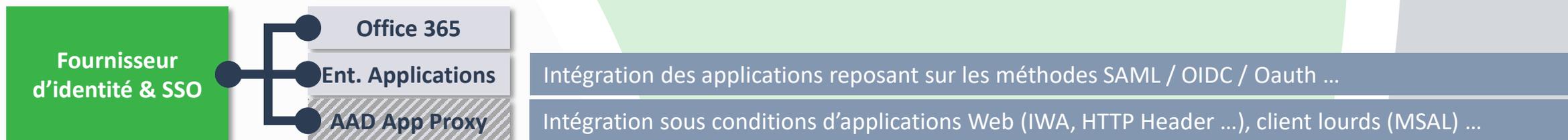
Enterprise Apps

# L'Azure AD un incontournable dès que l'on parle des services Cloud Microsoft

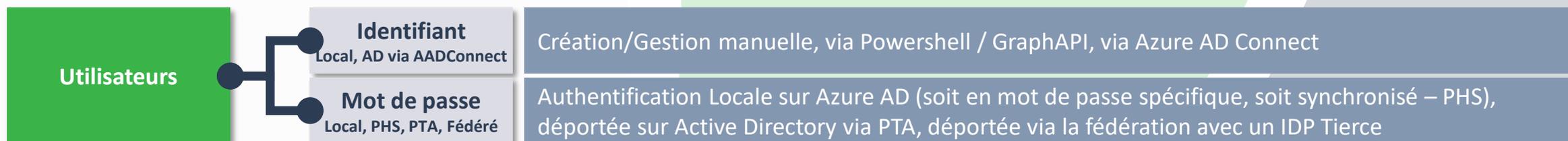


Les services étant nativement exposés sur Internet (à contrario d'Active Directory), l'usage des fonctions d'authentification est grandement facilité et est indépendant du réseau d'accès (#ChateauFort)

## L'Azure AD un incontournable dès que l'on parle des services Cloud Microsoft



 Bien que les moyens pour massifier l'authentification des apps & services sur Azure AD (et bénéficier des fonctions d'authentification moderne), la méconnaissance et l'historique peut être un frein



 Les cumul des fonctionnalités PHS & PTA est possible. Ce couplage permet aux entreprises qui souhaitent conserver l'AD comme référence pour les mots de passe de supporter une défaillance de la chaîne d'authentification de manière sans couture (via le failover en authentification Azure AD sans PTA)

# L'Azure AD un incontournable dès que l'on parle des services Cloud Microsoft

## Moteur d'authentification



Point d'entrée de tous types d'authentification nativement exposé sur Internet

Instancie les briques nécessaires pour dérouler, vérifier, contrôler les authentifications

Permet les authentifications interactives & transparentes



Point d'entrée de la plateforme d'Identity de Microsoft pour fournir l'ensemble des jetons d'accès nécessaires supportant les protocoles standards

## Fédération

Identity Provider Tierce

Permet de déléguer à un Identity Provider Tierce (ADFS, OKTA, Ping ...) l'authentification des utilisateurs joignant des services & applications intégrées à Azure AD

B2B / B2C

B2B : Permet de faire collaborer des organisations sur des ressources communes  
B2C : Permet à des clients des solutions de l'entreprise de s'authentifier



Les connexions directe B2B permettent d'établir des relations d'approbations  
La collaboration Azure AD B2C repose sur la technologie Azure AD mais repose sur une instance ad'hoc

# Comment s'authentifier auprès d'Azure AD ?

Utilisateurs

**Bad:** Password

123456  
qwerty  
password  
iloveyou  
Password1

Long password

**Good:** Password and...

SMS  
Voice

**Better:** Password and...

Authenticator (Push Notifications)  
Software Tokens OTP  
Hardware Tokens OTP (Preview)

**Best:** Passwordless

Authenticator (Phone Sign-in)  
Window Hello  
FIDO2 security key  
Certificates

← Phishing resistant

Service Principals

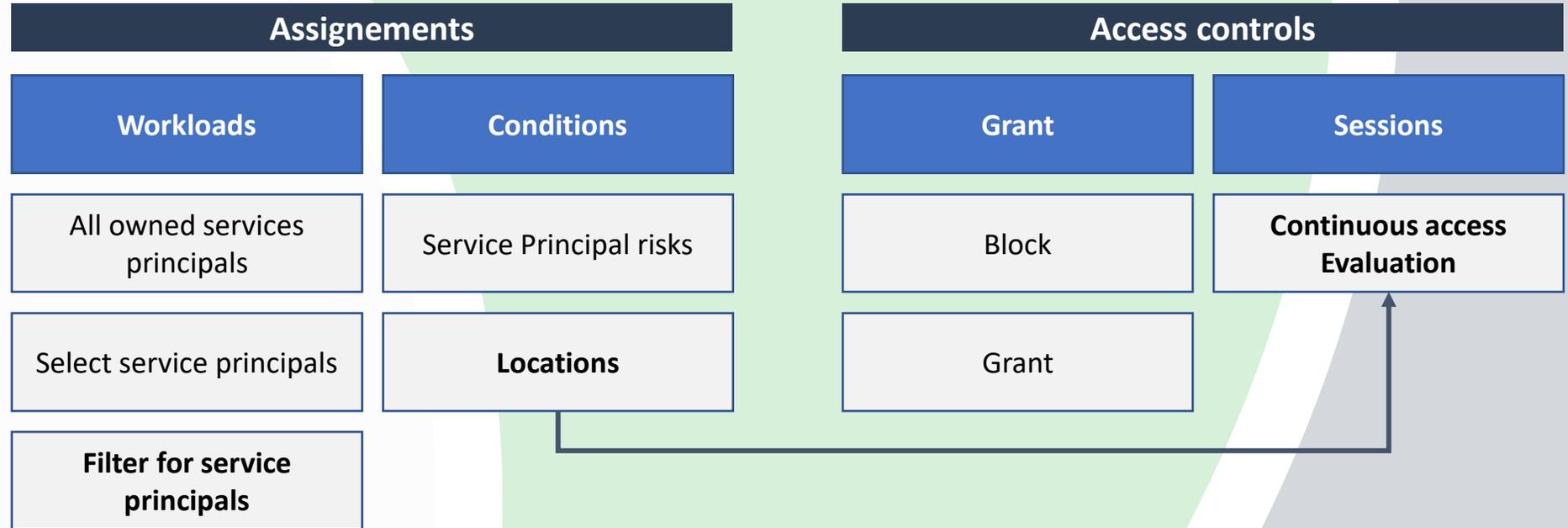
Long client secrets

Certificates

# Accès conditionnel : La pierre angulaire de l'authentification pour les utilisateurs

Assignements			Access controls	
Utilisateurs	Cloud apps or actions	Conditions	Grant	Sessions
All users	Cloud apps <b>All / Filters for apps</b>	User risk	Block access	App enforced restrictions
<b>Select All guests and externals users</b>	Authentication context	Sign-in risk	Grant access – MFA / Authn strenghts	Conditional Access App Control
<b>Select Directory roles</b>	User actions	Locations	Grant access – Device compliant / HAADH	<b>Persistent Browser session</b>
Select users and groups		Client apps	Grant access – Approved app client	<b>Continuous Access Evaluation</b>
		Filter for devices	Grant access – App protection policy	<b>Resilience defaults</b>
			Grant access – Password change	

## Accès conditionnel : ... mais aussi pour les applications



## Focus Azure AD Authentication Strengths (1/2)

Octobre 2022 : Public preview des authentication strengths

Objectif : permettre de limiter les facteurs disponibles pour l'authentification via l'accès conditionnel

Note : les facteurs tiers ne sont pas (encore ?) supportés

Authentication method combination	MFA strength	Passwordless MFA strength	Phishing-resistant MFA strength
FIDO2 security key	✓	✓	✓
Windows Hello for Business	✓	✓	✓
Certificate-based authentication (Multi-Factor)	✓	✓	✓
Microsoft Authenticator (Phone Sign-in)	✓	✓	
Temporary Access Pass (One-time use AND Multi-use)	✓		
Password + something you have <sup>1</sup>	✓		
Federated single-factor + something you have <sup>1</sup>	✓		
Federated Multi-Factor	✓		
Certificate-based authentication (single-factor)			
SMS sign-in			
Password			
Federated single-factor			

Quelques scenarios:

- Interdire le mot de passe
- Limiter le SMS a des populations très spécifiques
- Exiger un niveau minimum d'authentification pour les internes comme pour les externes
- Exiger un niveau d'authentification élevé pour les administrateurs

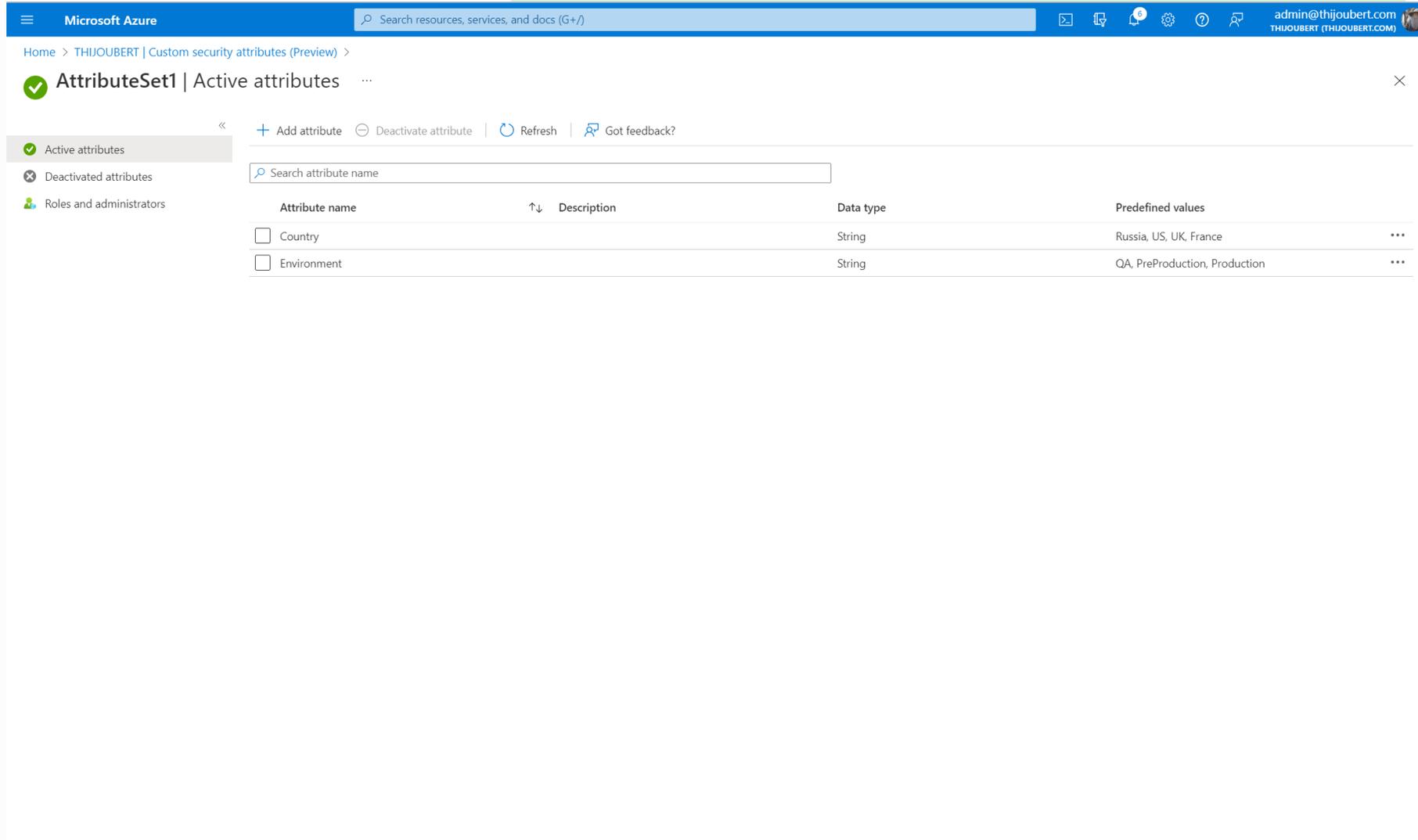
## Focus Azure AD Authentication Strengths (2/2)

Pour les externes (Azure AD B2B Guests), il est possible de définir des politiques d'authentication strengths.

/!\ il sera nécessaire d'activer le *Trust* entre les deux organisations afin de bénéficier de la meilleure expérience utilisateur possible

Authentication method	Home tenant	Resource tenant
SMS as second factor	✓	✓
Voice call	✓	✓
Microsoft Authenticator push notification	✓	✓
Microsoft Authenticator phone sign-in	✓	✓
OATH software token	✓	✓
OATH hardware token	✓	
FIDO2 security key	✓	
Windows Hello for Business	✓	

# Accès conditionnel : ... mais aussi pour les applications



Microsoft Azure | Search resources, services, and docs (G+)

admin@thijoubert.com  
THIJOUBERT (THIJOUBERT.COM)

Home > THIJOUBERT | Custom security attributes (Preview) >

AttributeSet1 | Active attributes

+ Add attribute | - Deactivate attribute | Refresh | Got feedback?

Search attribute name

Attribute name	Description	Data type	Predefined values
<input type="checkbox"/> Country		String	Russia, US, UK, France
<input type="checkbox"/> Environment		String	QA, PreProduction, Production

# Accès conditionnel : ... mais aussi pour les applications

Microsoft Azure

admin@thijoubert.com  
THIJOUBERT (THIJOUBERT.COM)

Home > Conditional Access | Policies >

**New** ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

803 - France Production Applications ✓

Assignments

Users or workload identities ⓘ

Specific service principals included

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only On Off

Create

## Edit filter (Preview) ✕

Configure ⓘ

Yes  No

Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. [Learn more](#)

And/Or	Attribute	Operator	Value	
	AttributeSet1_Environment	Equals	Production	🗑️
And	AttributeSet1_Country	Equals	France	🗑️

[+ Add expression](#)

Rule syntax ⓘ [Edit](#)

```
CustomSecurityAttribute.AttributeSet1_Environment -eq "Production" -and CustomSecurityAttribute.AttributeSet1_Country -eq "France"
```

Done

Control access based on who the policy apply to, such as users and groups, workload identities, directory roles, or external groups. [Learn more](#)

What does this policy apply to?

Workload identities (preview)

**Include** Exclude

None

All owned service principals

Select service principals

Edit filter (Preview)

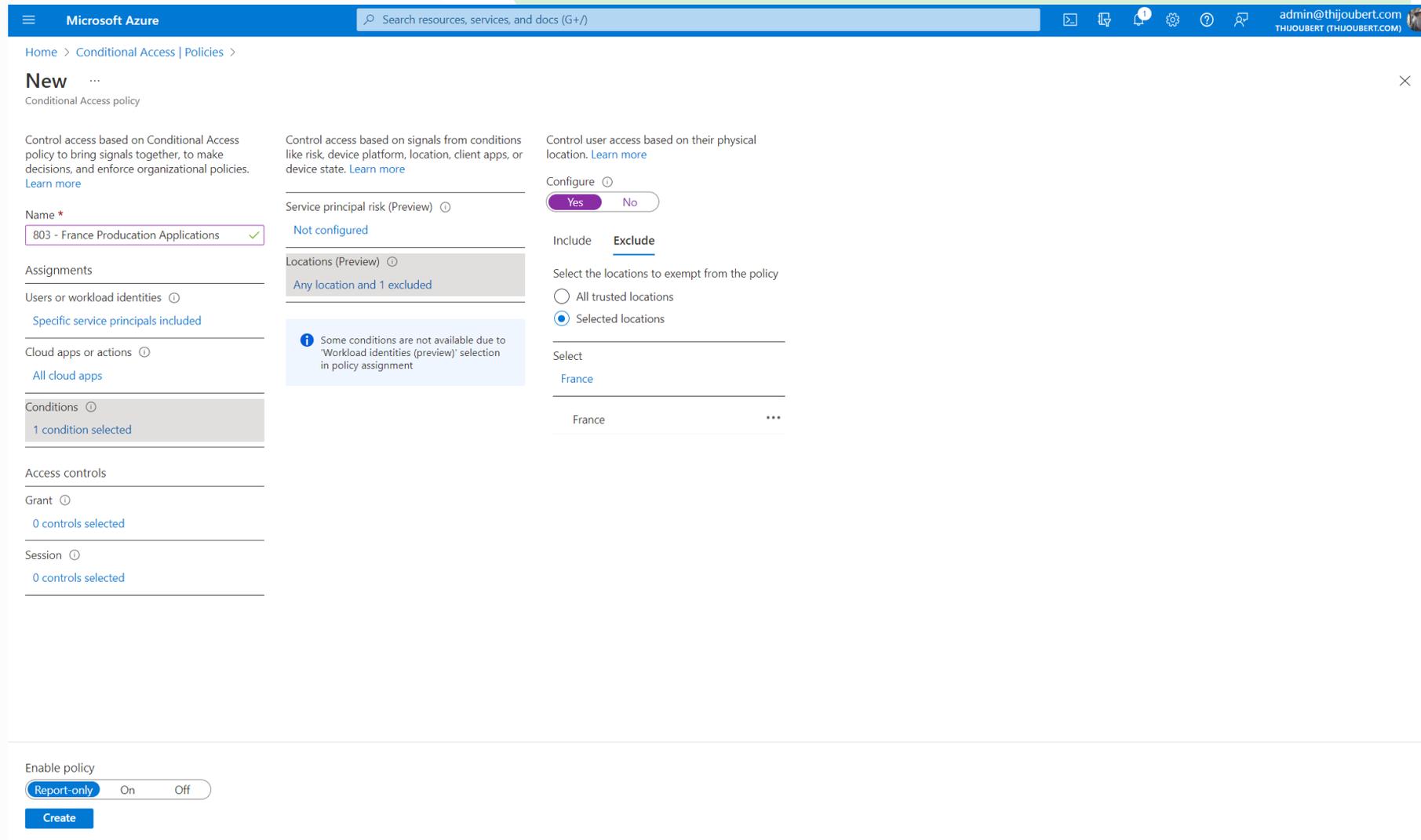
Configured

Select

None

**i** Policy only applies to single tenant service principals owned by your organization. [Click here to learn more](#)

# Accès conditionnel : ... mais aussi pour les applications



The screenshot shows the Microsoft Azure portal interface for configuring a new Conditional Access policy. The page is titled "New" and "Conditional Access policy".

**Policy Name:** B03 - France Production Applications ✓

**Assignments:** Specific service principals included

**Cloud apps or actions:** All cloud apps

**Conditions:** 1 condition selected

**Access controls:** Grant: 0 controls selected; Session: 0 controls selected

**Enable policy:** Report-only (selected), On, Off

**Configuration details:**

- Service principal risk (Preview):** Not configured
- Locations (Preview):** Any location and 1 excluded
- Control user access based on their physical location:** Configure: Yes (selected), No
- Include/Exclude:** Exclude (selected)
- Select the locations to exempt from the policy:** Selected locations (selected)
- Select:** France

**Warning:** Some conditions are not available due to "Workload identities (preview)" selection in policy assignment

**Buttons:** Create

## Nouveautés récentes sur l'authentification dans Azure AD

Microsoft Entra Identity Governance: Conditionnal Access & Identity Protection	GA November 2022
Conditional Access authentication strengths	PPreview Octobre 2022
Certificate-based authentication	GA Octobre 2022
Public Preview Authenticator (Numbers matching and Authenticator notifications)	GA Octobre 2022
Accès conditionnel & Linux	GA September 2022
Multiple Passwordless Phone sign-in Accounts for iOS devices	July 2022
Cross-tenant access settings for B2B collaboration	July 2022
Temporary Access Pass is now available	June 2022
Continuous Access Evaluation	January 2022

# Quelles cibles et conseils

# Conseils pour déployer une politique d'authentification moderne

## Dette techno.

En cas d'authentification avec Active Directory, privilégier les modes de fonctionnement PHS / PTA proposés par Azure AD Connect (*no more ADFS*)

Globaliser la politique d'authentification autour d'une unique Identity Provider afin de permettre des contrôles homogènes entre les applications (intégration dans les cahiers des charges en particulier, bascule par opportunisme)

## Sécurité

Limitier le MFA interactif aux accès vraiment nécessaire (contextes critiques et/ou données sensibles). Pour les autres cas, le MFA transparent (tel que Windows Hello For Business) reste suffisant

## UX

Sécuriser l'enrôlement des machines et des seconds facteurs afin de disposer de méthodes d'authentification sûres de bout en bout et supprimer les méthodes faibles (eg. SMS)

Massifier des méthodes d'authentification robustes proposant une expérience utilisateurs à l'état de l'art (FIDO2, Passwordless ...)

Décliner les concepts du Zero Trust sur les authentifications et moderniser la politique de sécurité de l'entreprise

- La sécurité ne se résume plus au sanctuaire du SI de l'entreprise et aux terminaux managés
- Définissez le niveau de sécurité minimal qui doit être appliqué dans telle ou telle conditions (et non pas : no BYOD)
- Contrôler afin de détecter les nouveaux usages et statuer sur leur légitimité / illégitimité
- Effectuer un suivi mensuel de l'évolution des conditions et des critères possibles sur l'Azure AD Conditional Access
- Le sujet va delà d'Office 365 et requiert une vision transverse
- La constitution d'un écosystème intégré de sécurité et de gestion des identités et terminaux est un accélérateur

La critères et conditions du Conditionnal Access ne cessant d'évoluer, une approche de définition des règles de manière inclusive (plusieurs règles s'appliquent) est à privilégier

## Exemple de règles d'authentification selon des profils types

Utilisateurs internes (ou assimilés) à l'entreprise	Utilisateurs internes (ou assimilés) à l'entreprise sur un tenant tierce	Utilisateurs partenaire à l'entreprise	Administrateurs
<p>Sur des terminaux non managés</p> <ul style="list-style-type: none"> <li>▪ Accès via client Web uniquement</li> <li>▪ MFA interactif</li> <li>▪ Sessions à durée limitée / sans persistance</li> </ul> <p>Sur des terminaux managés</p> <ul style="list-style-type: none"> <li>▪ Accès via client lourd et web</li> <li>▪ MFA transparent par défaut</li> <li>▪ MFA interactif pour les données sensibles</li> <li>▪ Sessions longues</li> </ul>	<p>Alignement des règles au travers d'une relation d'approbation B2B Direct</p>	<p>MFA interactif porté par l'entreprise sur les comptes Guests</p> <p>Interdiction d'accès aux contextes sensibles</p> <p>Durée de session de l'ordre de la semaine</p>	<p>MFA interactif forcé pour chaque nouvelle session</p> <p>Durée de session courtes (de l'ordre de la journée)</p> <p>Accès possible uniquement depuis des terminaux managés, vérifiant les critères de conformité et restreints aux sites de l'entreprise</p>
Interdictions des facteurs faibles sauf cas particulier			FIDO2 / WHfB uniquement
Access uniquement depuis les clients approuvés des les terminaux iOS / Android			
Usage du <i>Continuous Access Evaluation</i>			



# Retours d'expérience

## Bonnes pratiques issues de retours d'expériences

- 1 L'usage des « Trusted Locations » va à l'encontre des concepts du Zero Trust (aka. Château Fort) et doit être utilisé en dernier recours ou des besoins très spécifiques
- 2 Le critère Hybrid Azure AD Join, reste limitatif et ne doit pas être assimilé à un critère de conformité (et il ne couvre pas les machines en Azure AD Join et AD Join). Et par conséquent génère des effets de bords pour les accès depuis les serveurs (eg. RDS Farm).
- 3 Affiner les politiques d'authentification selon les critères de conformité des terminaux et abandonner le concept du BYOD au profit du statut managé / non managé
- 4 Réaliser des tests exhaustifs des règles de conditional access au préalable de leur généralisation (merci le WhatIf)
- 5 Intégrer les contraintes de vérifications de conditions :
  - Plug-in conditionnal access pour Chrome
  - Limite des données utilisées en mode InPrivate / Incognito
- 6 La condition « Device State » étant dépréciée, reporter les conditions en « Filters for devices »
 

L'usage du « Filter for devices » doit être fait en connaissance de son comportement qui peut varier selon le statut de la machine

  - Certains filtres ne sont pas évaluables lorsque le terminal est non enregistré sur Azure AD
  - Certains filtres sont évaluables uniquement lorsque le terminal est managé par Intune
  - Certains filtres sont évaluables selon le type d'opérateurs utilisés (positif / négatif)
- 8 Déployer de manière progressive les règles en termes de populations ciblées et complexité

**T H A N K**  
**Y O U**



# IDENTITY DAYS

27 octobre 2022 - PARIS



@IdentityDays #identitydays2022

Merci à tous nos partenaires !

