IDENTITY DAYS

28 octobre 2021 - PARIS

@IdentityDays #identitydays2021

Merci à tous nos partenaires !

zscaler onelogin SailPoint METSYS Auth0 FUSION DIRECTORY

Microsoft Vorteks make IT work, make IT free

tenable yubico ManageEngine WALLIX CYBERSECURITY SIMPLIFIED Exakis Nelite Magellan Partners Alphorm.com

Identité & résistance aux menaces : Et si le Cloud était la solution ?

Hervé THIBAULT

AGENDA DE LA CONFÉRENCE

Hervé THIBAULT

Chief Technology Officer
@ Metsys

Microsoft Regional Director depuis 2015

Rd.microsoft.com/herve.thibault

Microsoft Most Valuable Professional 2007-2014

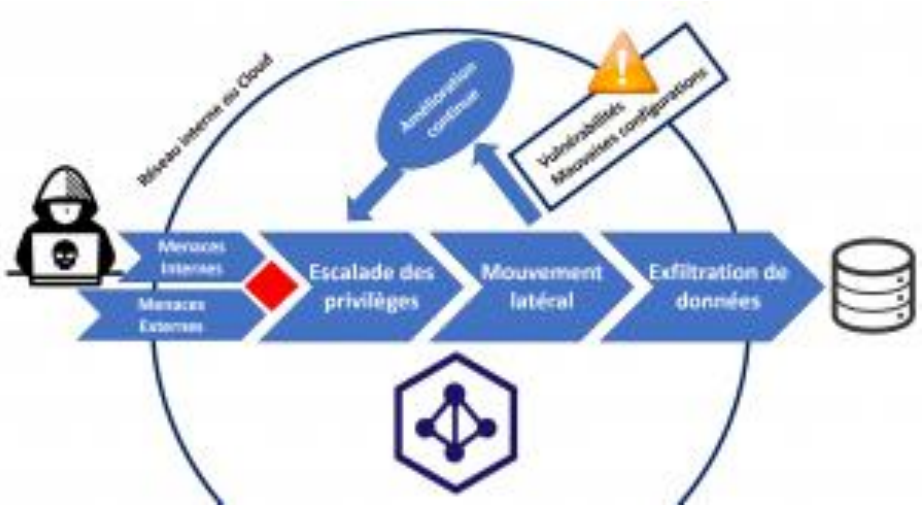
@thibherv

- Etat des menaces sur Active Directory
- Solutions pour la sécurisation AD : Tiering, bastion, Microsoft Defender for Identity, Tenable.ad, …
- Azure AD (premium) pour sécuriser en mode hybride :
  - Identity Protection (Conditional Access, MFA, secure score, password protection, …)
  - Self-Service (SSPR, My sign-ins, Bitlocker Recovery key, …)
  - Modern Authentication (Enterprise Applications & SSO, passwordless …)
  - Identity Governance (Roles, administrative units, PIM, PAM - Accès Packages, …)
- Synthèse : comparaison Azure AD / AD onprem
- Recommandations

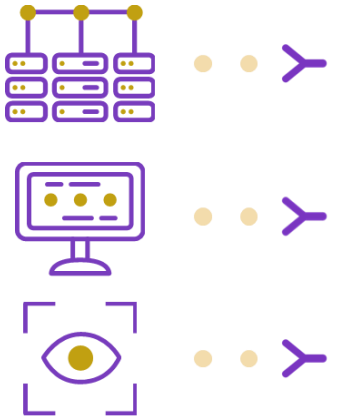
“Legacy” Identity : Active Directory

Active Directory

Etat des menaces



- AD = Composant central de presque tous les SI = Gestion des comptes (à privilèges) et des machines (stratégies systèmes = GPO)
  - Expérience personnelle : + de 90% des demandes de reprise sur incident avaient pour origine une attaque ayant ciblé AD
  - ANSSI: L'analyse des modes opératoires des attaques récentes met en évidence une recrudescence du ciblage des annuaires Active Directory
- L'obtention de privilèges AD élevés (*Domain Admins, Enterprise Admins*), au travers de « mouvements latéraux », permet à l'attaquant de prendre le contrôle de tout l'écosystème postes de travails & serveur Windows, en utilisant bien souvent les mécanismes propres de l'AD (GPO)
- Les données sont ensuite exfiltrées (pour donner une preuve par l'attaquant ou pour exploiter ces données) et chiffrées (pour masquer l'exfiltration et/ou demander une rançon)



Les **serveurs** sont chiffrés (pour demander une rançon)

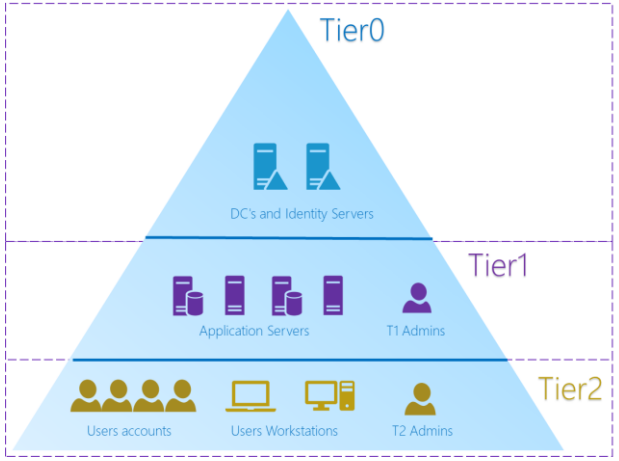
Les **stations** sont chiffrées (pour demander une rançon)

Les **contrôleurs de domaines** sont chiffrés (pour demander une rançon ET pour effacer les traces de l'intrusion)

Active Directory

Résistance aux menaces

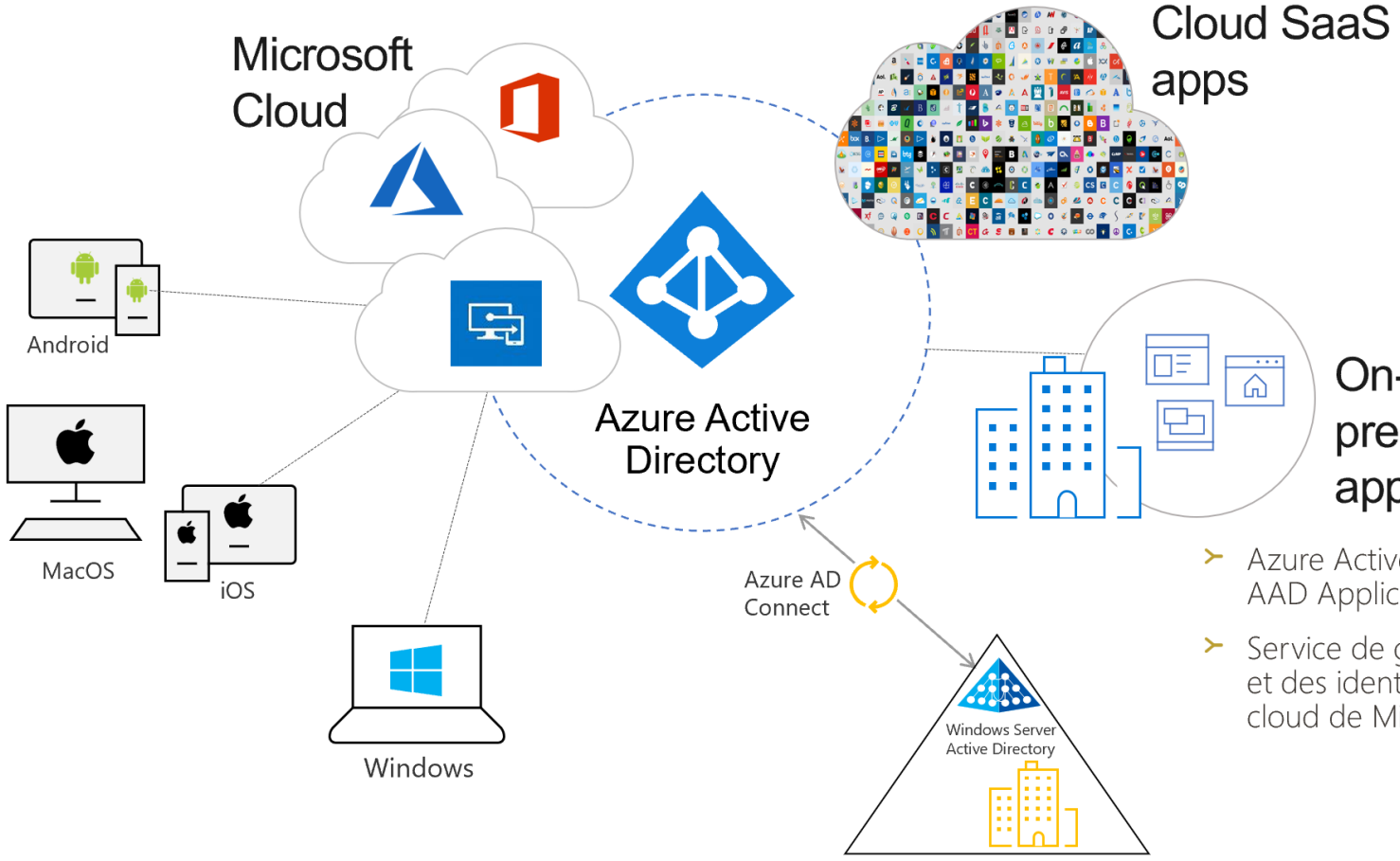
1. Patch Management !!!
2. Hardening Windows (poste de travail, serveurs)
3. EDR / xDR
4. Tiering Model AD (consolidation)
5. Bastion, stations d'administration sécurisées (PAW)
6. Gestion des identités à privilèges
7. Authentification forte
8. Passwordless
9. Threat Management : Microsoft Defender for Identity, Tenable.ad



“Modern” Identity : Azure Active Directory

Azure Active Directory

Introduction



- Azure Active Directory ou AAD Application Proxy
- Service de gestion de l'accès et des identités basé sur le cloud de Microsoft

Figure 1: Magic Quadrant for Access Management

https://www.gartner.com/doc/reprints?id=1-24F36V24&ct=201021&st=sb

Azure Active Directory

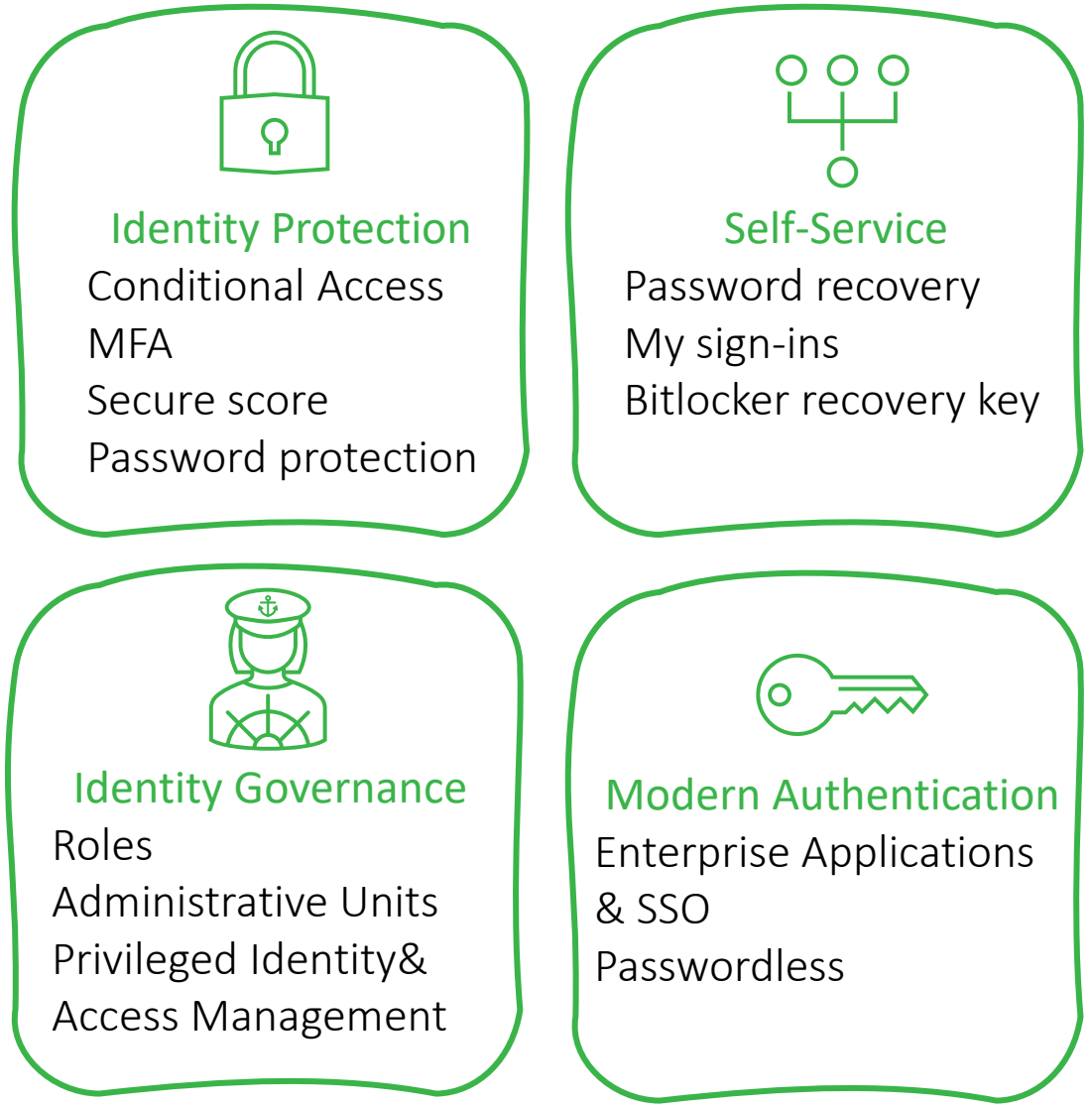
Plus qu'un simple « annuaire »

4 éditions : Gratuite, Applications Office 365, Premium (P1 & P2)

- L'édition gratuite est disponible avec tout abonnement Azure
- L'édition « Applications Office 365 » est disponible avec Office 365
- Azure AD Premium est disponible dans Microsoft 365 et Enterprise Mobility + Security :
  - Azure AD Premium P1 = M365 E3 = EMS E3
  - Azure AD Premium P2 = M365 E5 = EMS E5

P1 P2 O365

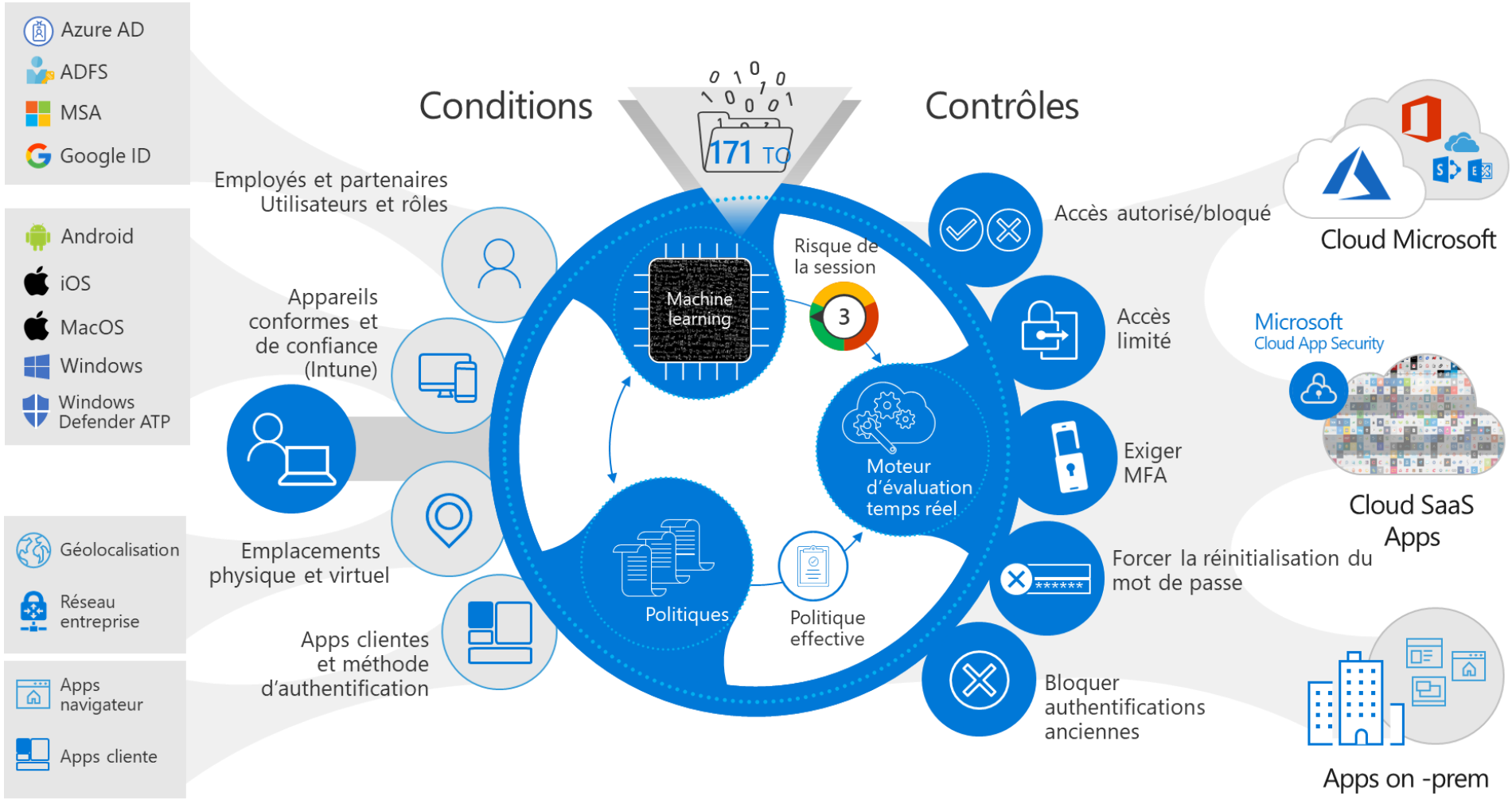
https://azure.microsoft.com/fr-fr/pricing/details/active-directory/



P1

Azure Active Directory – Identity Protection

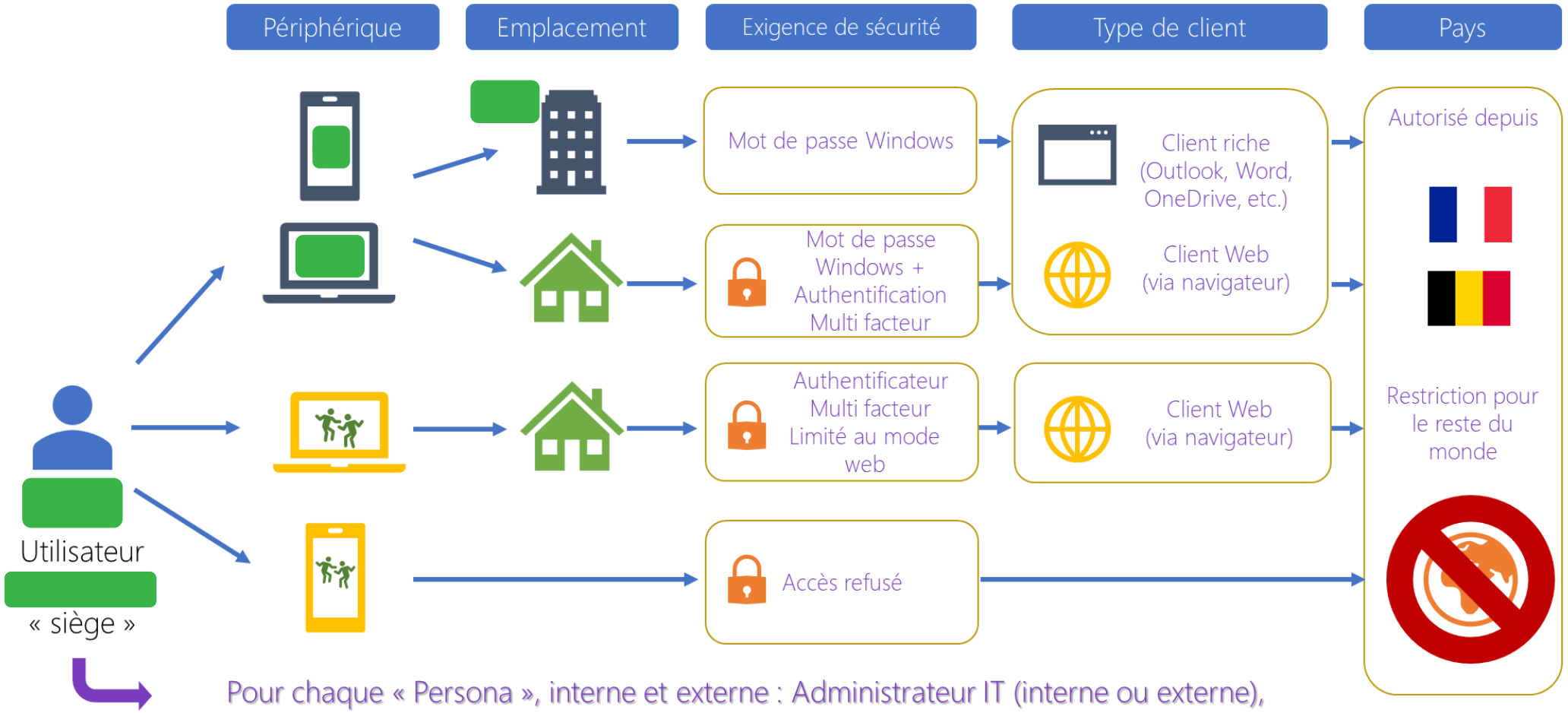
Conditional Access



P1

Azure Active Directory – Identity Protection

Conditional Access

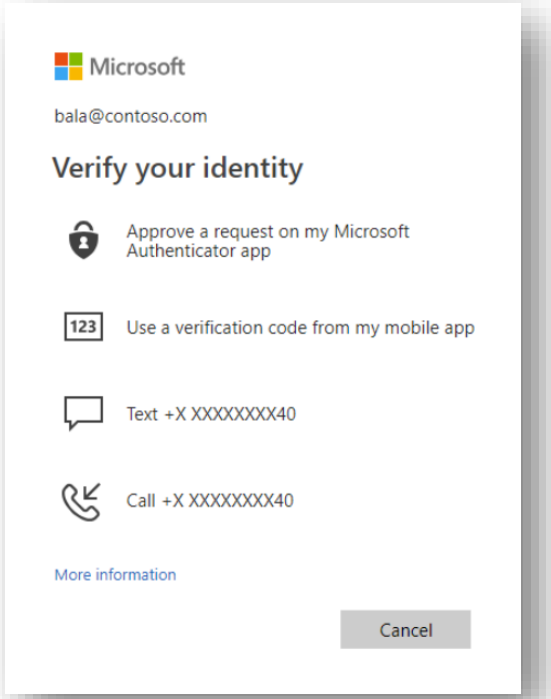


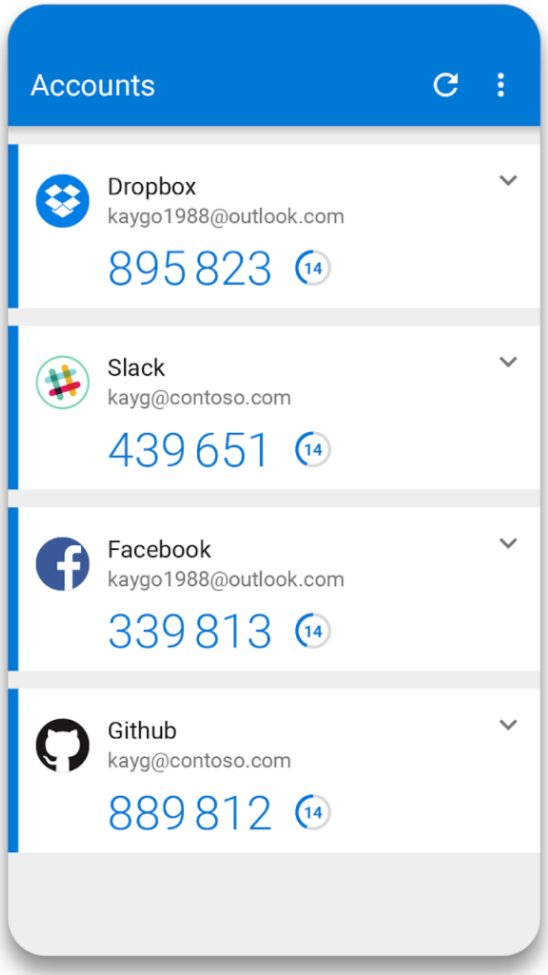
Pour chaque « Persona », interne et externe : Administrateur IT (interne ou externe), collaborateur magasin, patron magasin, prestataire, fournisseur, …

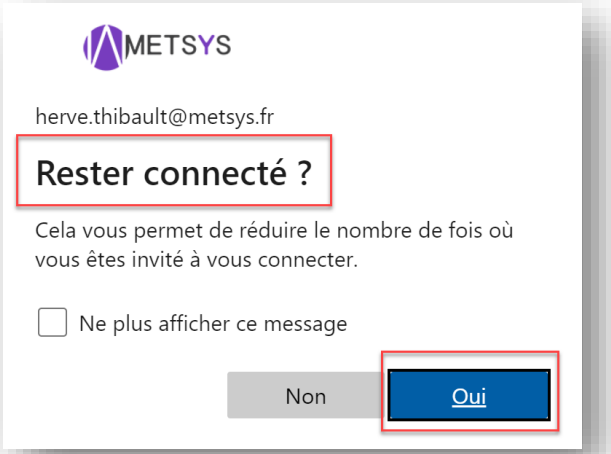
Azure Active Directory – Identity Protection

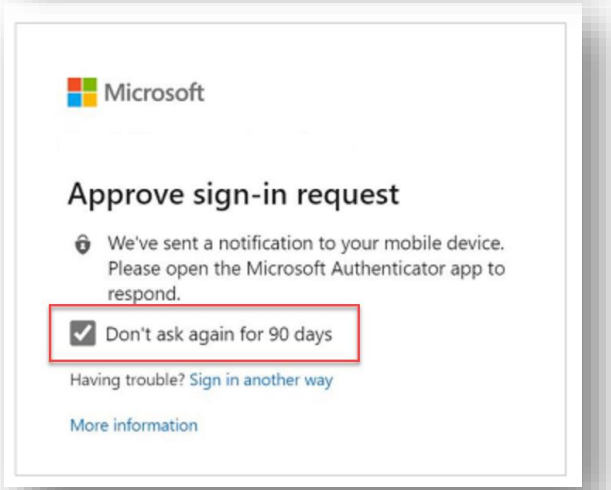
MFA

- Plusieurs méthodes de vérification pour ajouter une couche supplémentaire de sécurité aux connexions des utilisateurs
- Possibilité de définir une « période de grâce » pour le MFA → « confort » des utilisateurs / adoption
- La configuration par défaut d'Azure AD pour la fréquence de connexion utilisateur est une fenêtre dynamique de 90 jours







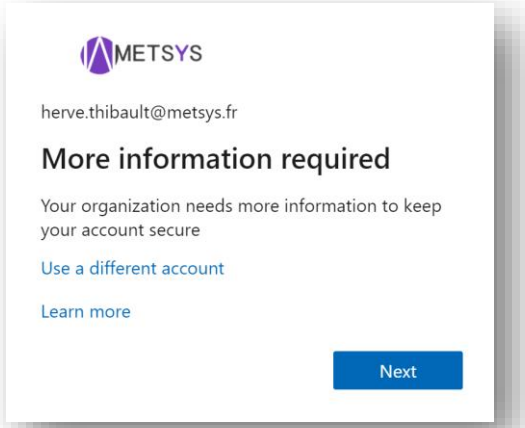


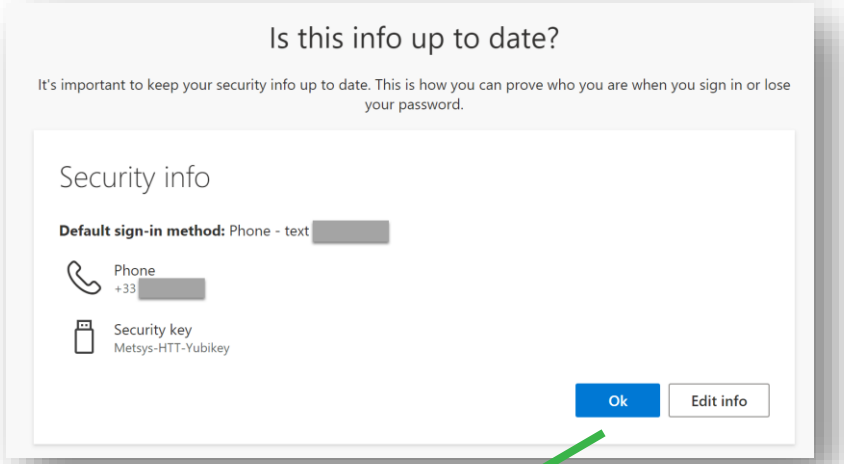
O365

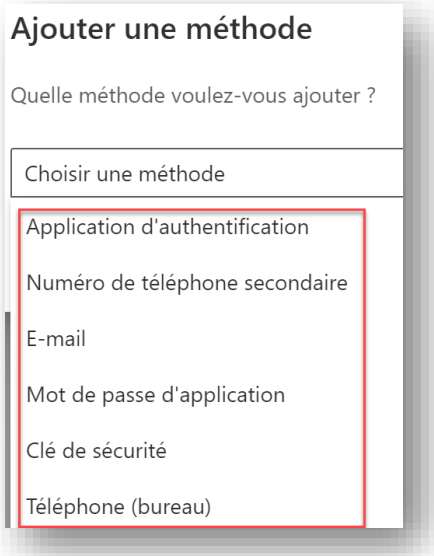
Azure Active Directory – Identity Protection

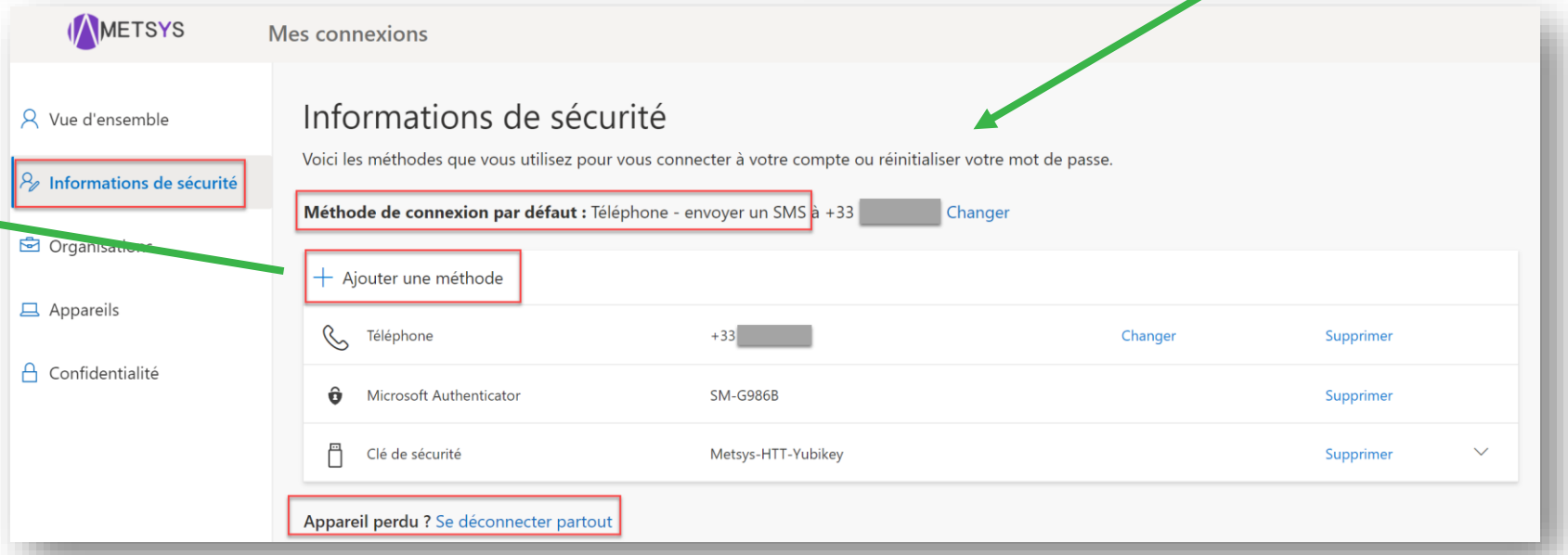
MFA

https://aka.ms/MFAsetup









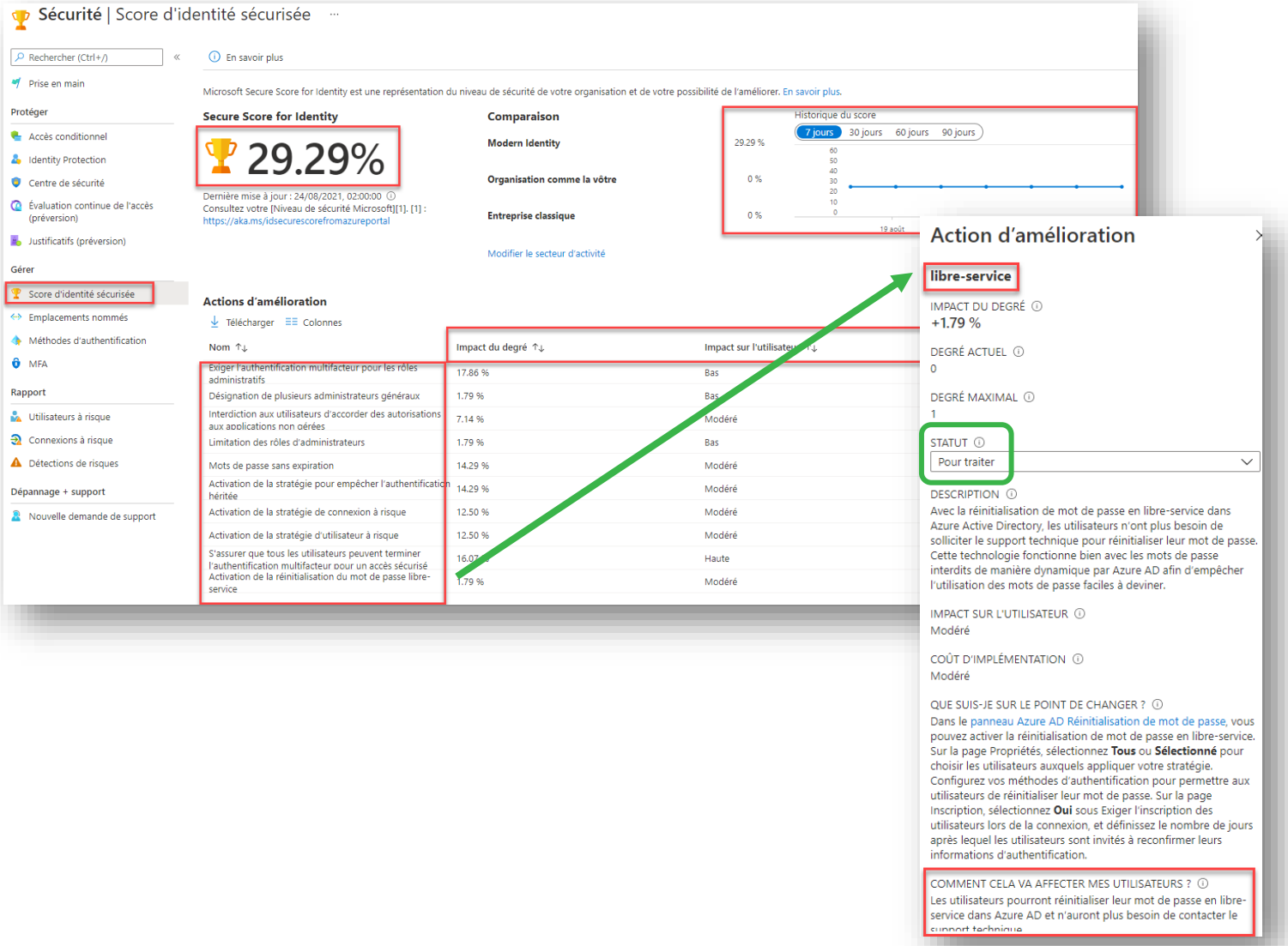
O365

Azure Active Directory – Identity Protection

Identity Secure Score

- Degré de sécurisation Identity Secure Score (pourcentage)
- Graphique de comparaison qui situe le score par rapport aux autres sociétés de tailles similaires et du même secteur d'activité
- Graphique de tendance représentant l'évolution du score au fil du temps

- Liste des améliorations possibles - 3 indicateurs pour les changements, afin de prioriser les modifications en connaissance de cause :
  - Niveau d'amélioration de la sécurité
  - Coût d'implémentation / Charge IT
  - Impact utilisateur

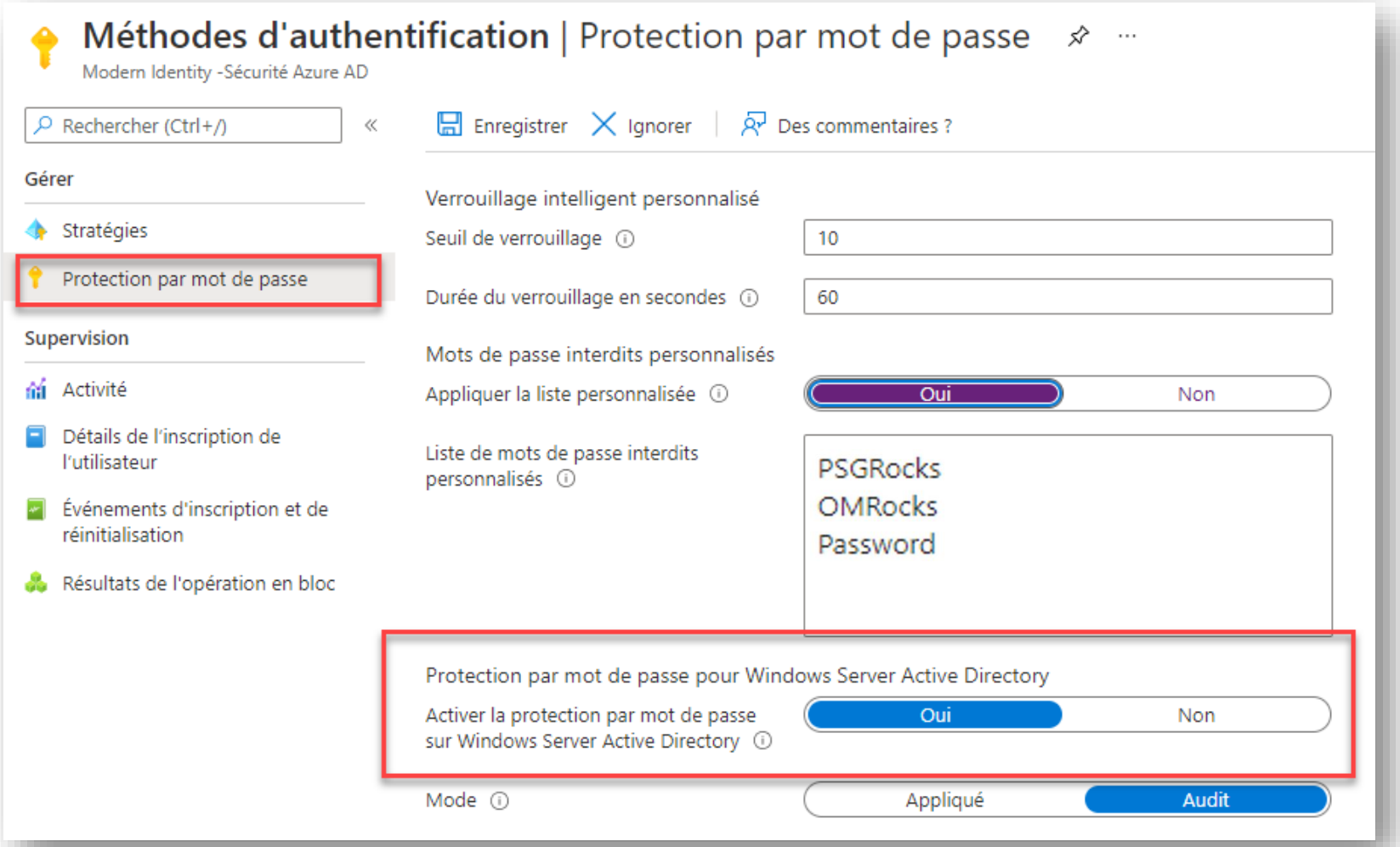


P1 (Liste personnalisée) (on-prem)

Azure Active Directory – Identity Protection

Password Protection

- Détecte et bloque les mots de passe faibles connus et leurs variantes, mais peut aussi bloquer d'autres termes propres à votre organisation
- Fonctionne également on-prem !!! (Agent & proxy)
  - https://docs.microsoft.com/fr-fr/azure/active-directory/authentication/concept-password-ban-bad-on-premises



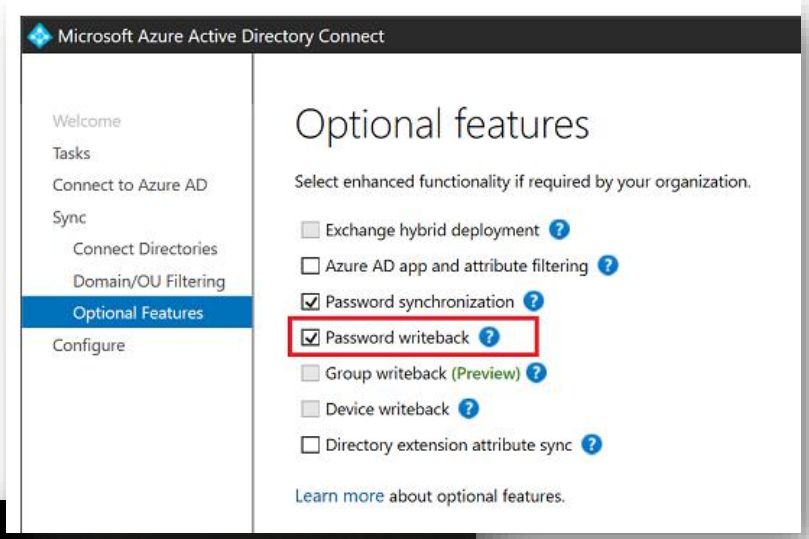
P1 (Write-back)

Azure Active Directory – Self-service

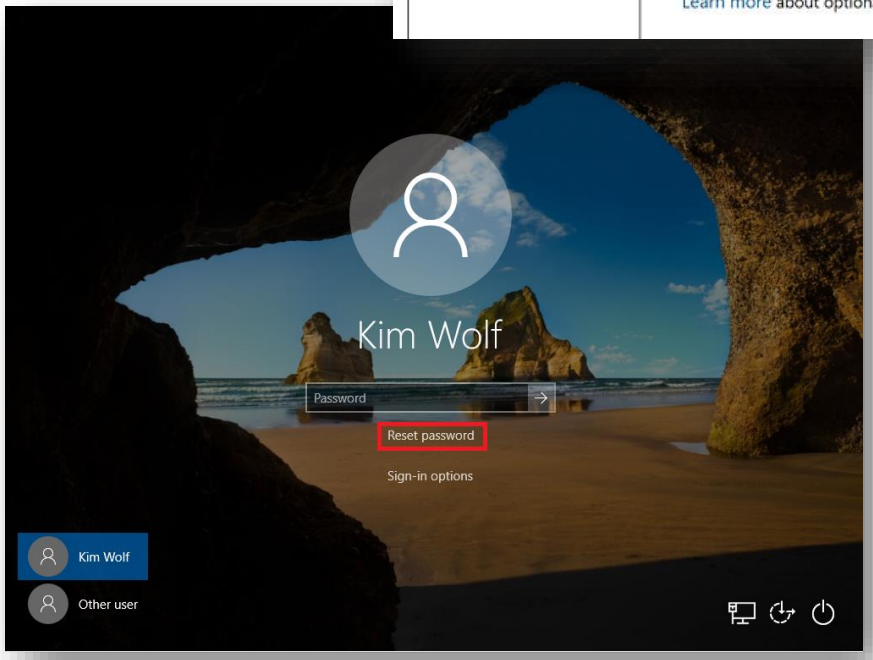
Self-Service Password Recovery (SSPR)

- Offre aux utilisateurs la possibilité de réinitialiser leur mot de passe, sans intervention de l'administrateur, quand et où ils en ont besoin, en utilisant un navigateur web ou directement via la « mire » de connexion Windows 10

https://docs.microsoft.com/fr-fr/azure/active-directory/authentication/tutorial-enable-sspr-writeback



- Options de réinitialisation de mot de passe en libre-service :
  - Modification de mot de passe : je connais mon mot de passe mais je souhaite le remplacer.
  - Réinitialisation de mot de passe : je ne parviens pas à me connecter et je souhaite réinitialiser mon mot de passe à l'aide d'une ou de plusieurs méthodes d'authentification approuvées.
  - Déverrouillage de compte : je ne parviens pas à me connecter, car mon compte est verrouillé, et je souhaite le déverrouiller à l'aide d'une ou de plusieurs méthodes d'authentification approuvées.



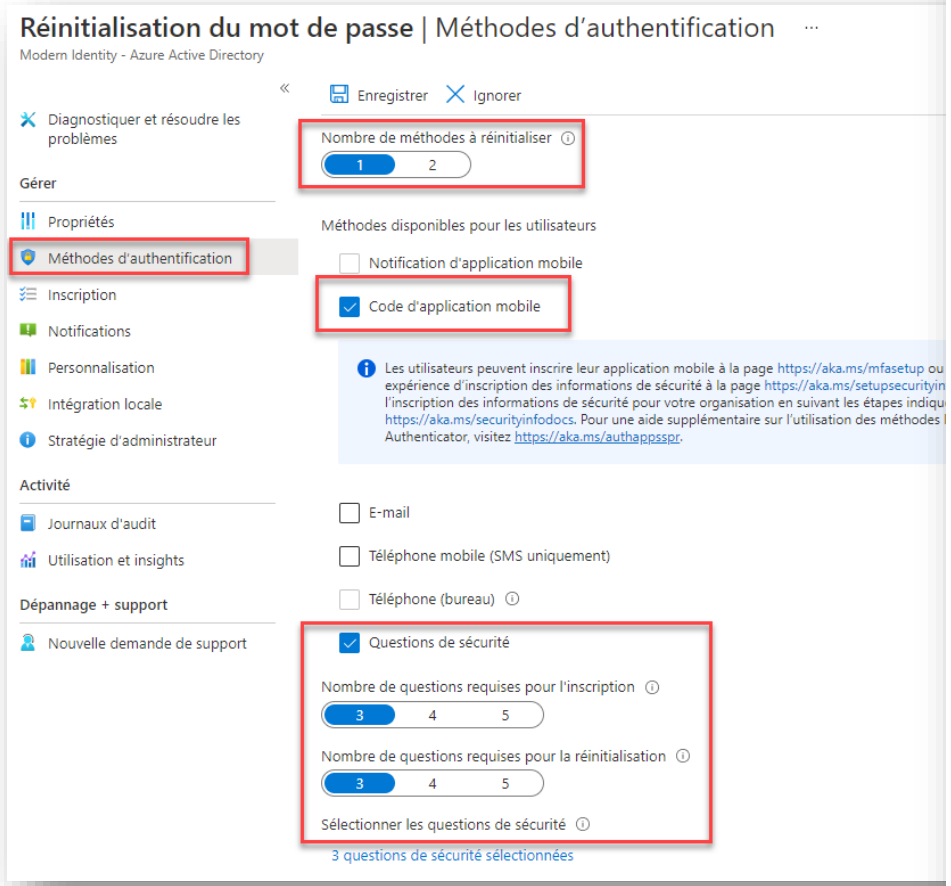
- Azure AD Connect fournit un mécanisme sécurisé qui renvoie ces changements de mot de passe à un annuaire local existant à partir d'Azure AD : La réécriture du mot de passe - Password Write-Back

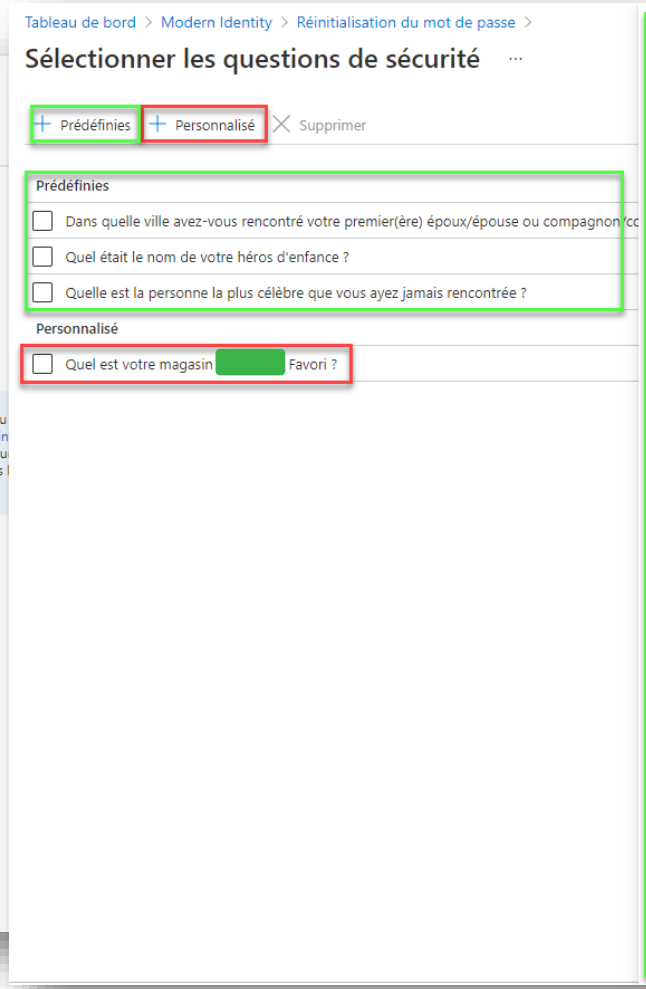
https://docs.microsoft.com/fr-fr/azure/active-directory/authentication/howto-sspr-windows

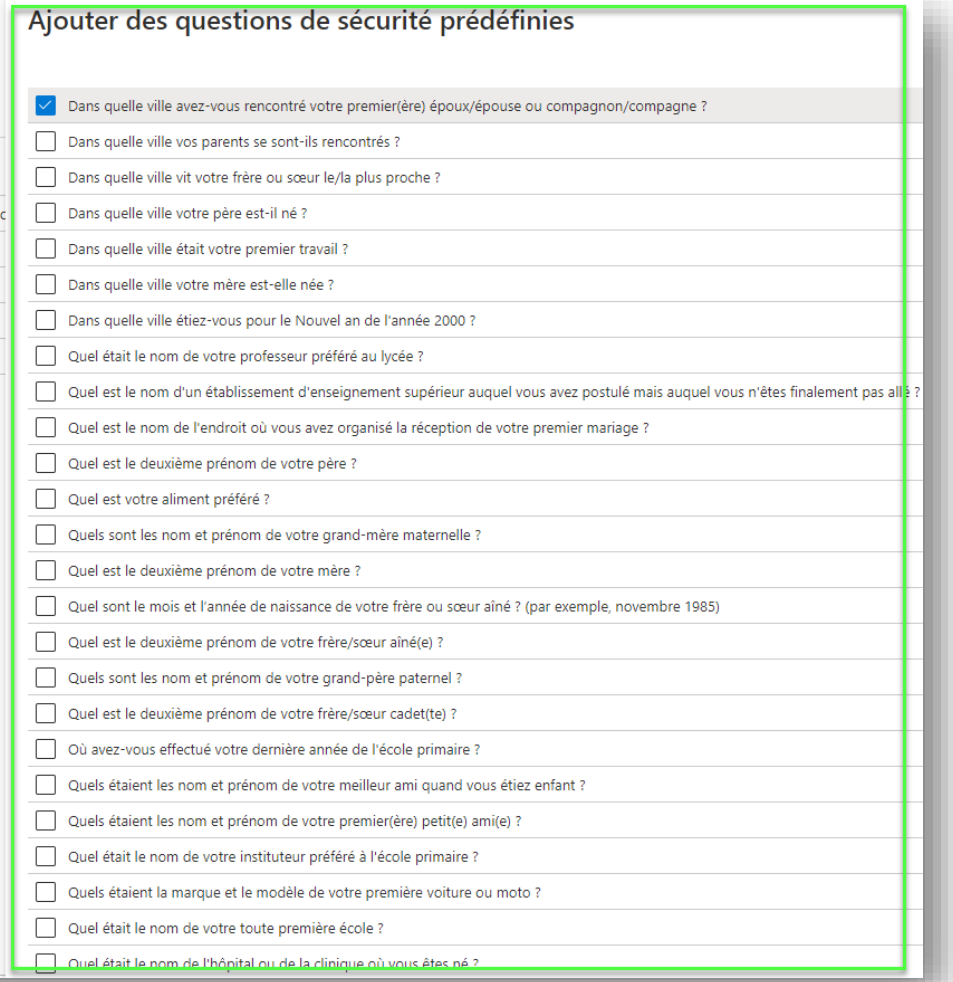
P1 (Write-back)

Azure Active Directory – Self-service

Self-Service Password Recovery (SSPR)



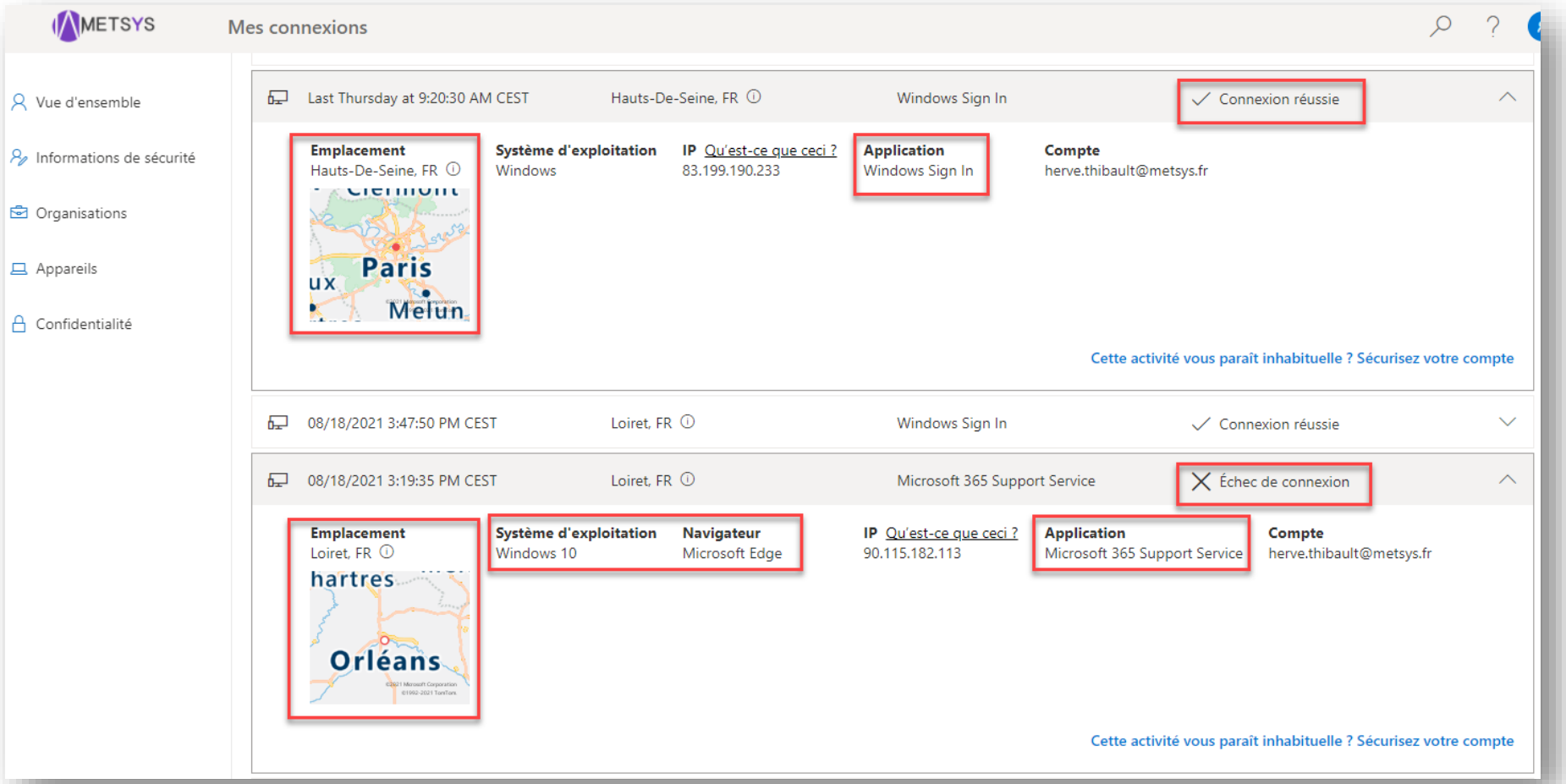




Azure Active Directory – Self-service

My Sign-Ins

- Pour surveiller soi-même ses évènements de connexions (login, application, portail, …) … et prendre les mesures nécessaires le cas échéant

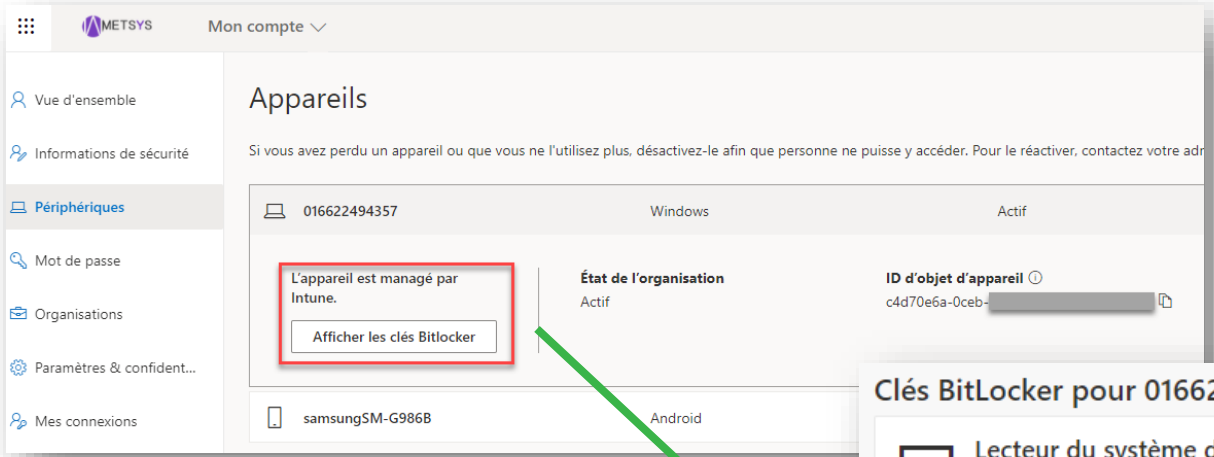


https://myaccount.microsoft.com/

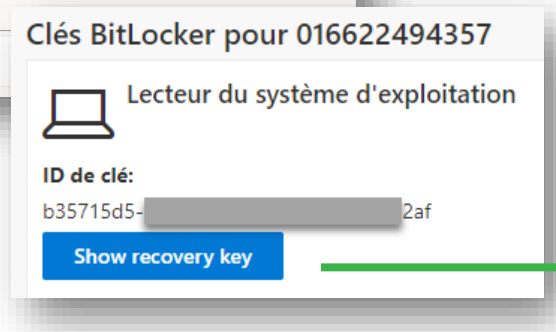
Azure Active Directory – Self-service

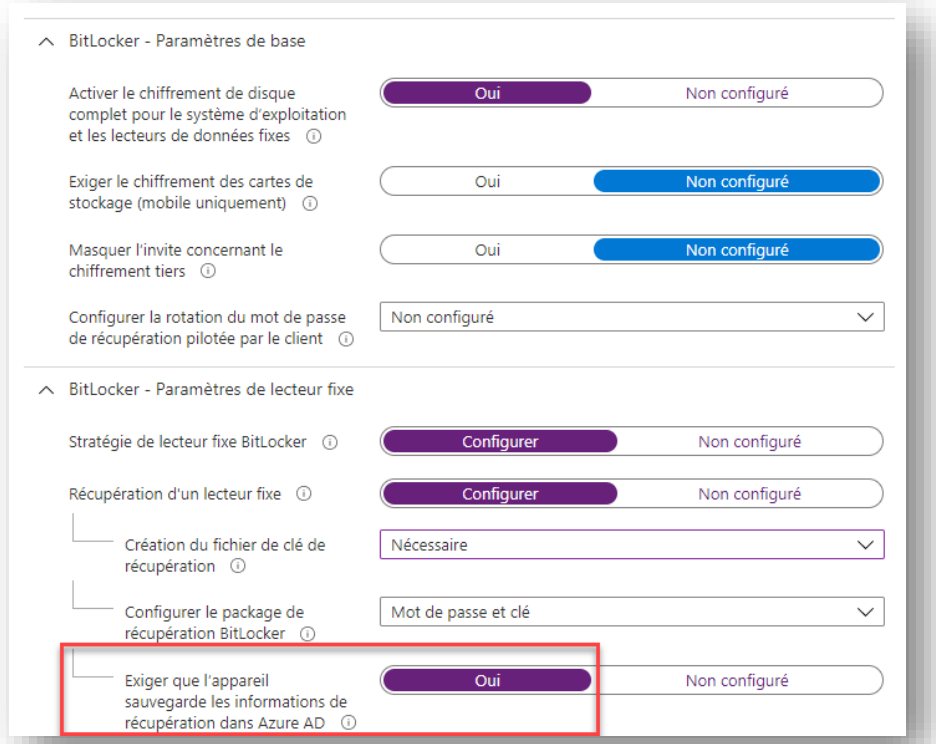
BitLocker Recovery Key

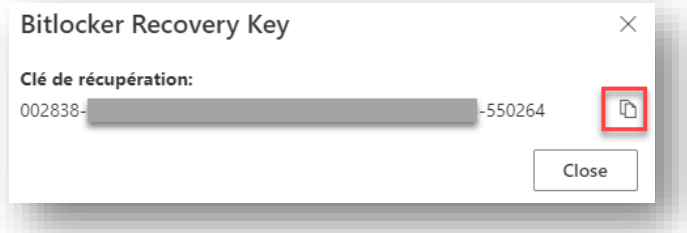
- La clé de récupération BitLocker peut être stockée dans Azure AD et être récupérée en mode self-service par l'utilisateur
- Configurable via stratégie Intune
  - https://docs.microsoft.com/fr-fr/mem/intune/protect/encrypt-devices



https://myworkaccount.microsoft.com/







Azure Active Directory – Modern Authentication

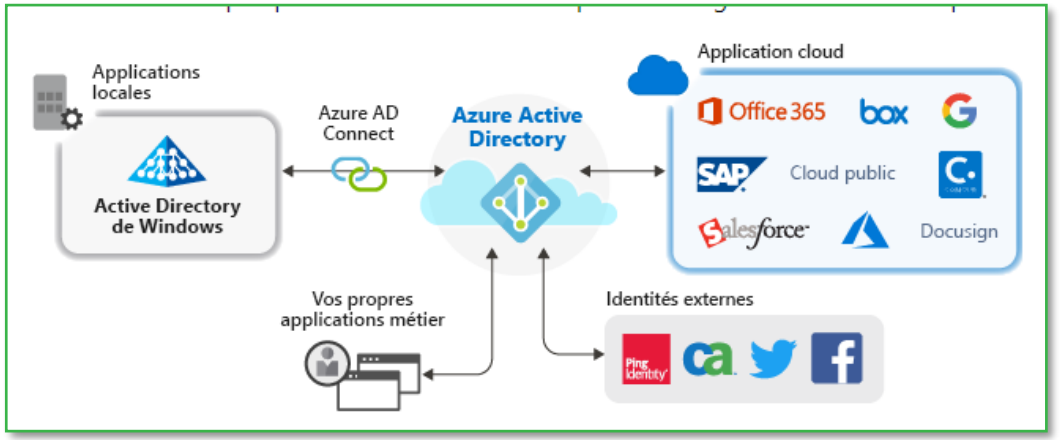
P1

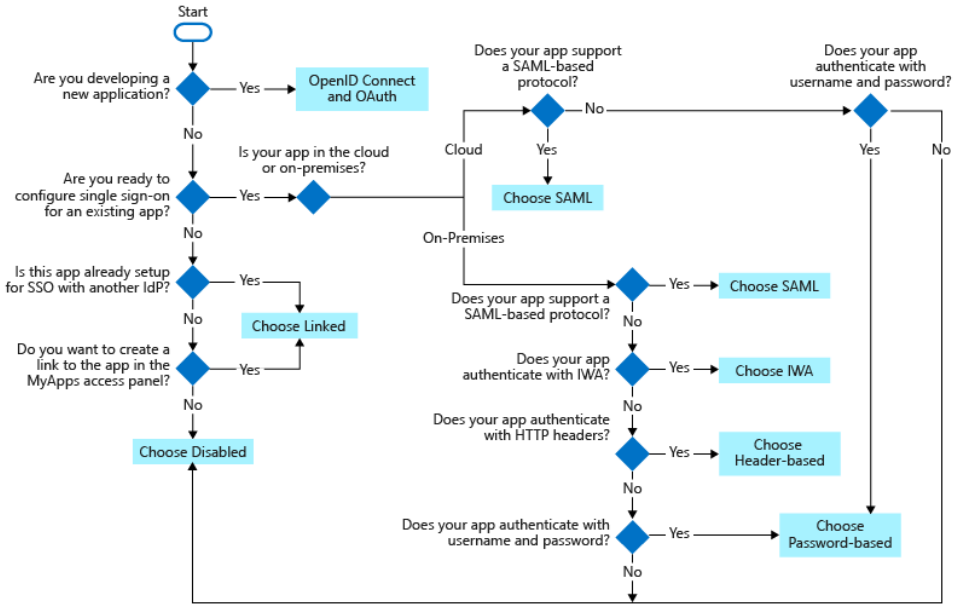
Enterprise Applications & SSO

- Azure AD peut être utilisé comme système d'identité pour quasiment n'importe quelle application

- « Cloud »
  - Nombreuses applications déjà préconfigurées (Office 365, Intune, …) - Publiées dans la galerie d'applications Azure AD
  - Didacticiel pour intégrer les applications du catalogue : https://docs.microsoft.com/fr-fr/azure/active-directory/saas-apps/tutorial-list
  - Configuration manuelle de la plupart des applications pour l'authentification unique si elles ne se trouvent pas dans la galerie – Protocoles d'authentification : OpenID, OAuth, SAML, mot de passe

- Et pour les applications « locales » (AD) ?
  - Azure AD Application Proxy
  - Fonctionnalité d'Azure AD qui permet aux utilisateurs d'accéder à des applications web locales à partir d'un client distant
  - Accès à distance aux applications locales – Proxy d'application Azure Active Directory | Microsoft Docs



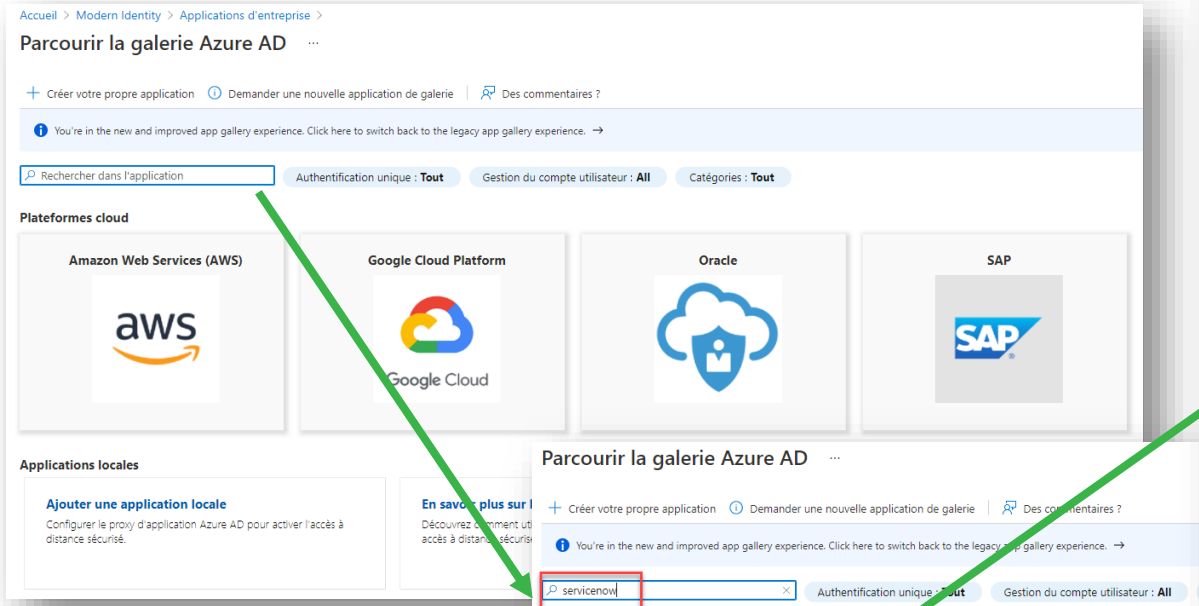


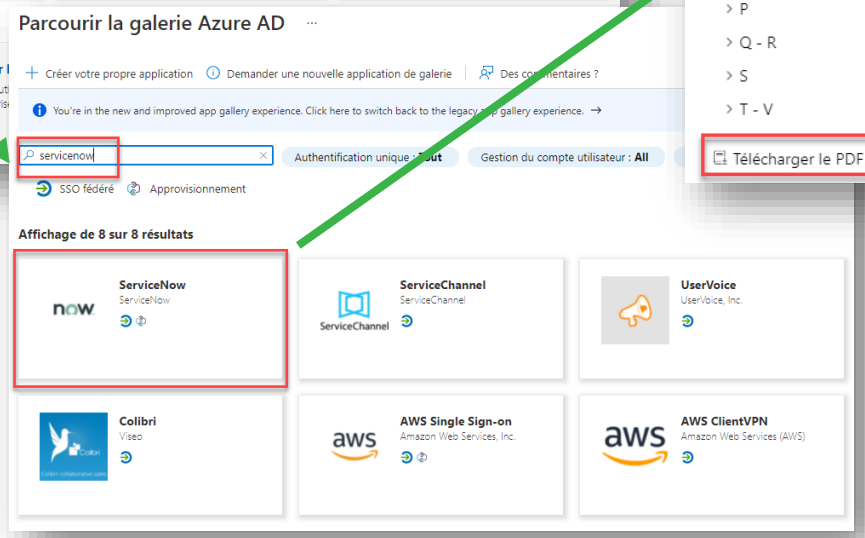
https://docs.microsoft.com/fr-fr/azure/active-directory/manage-apps/sso-options

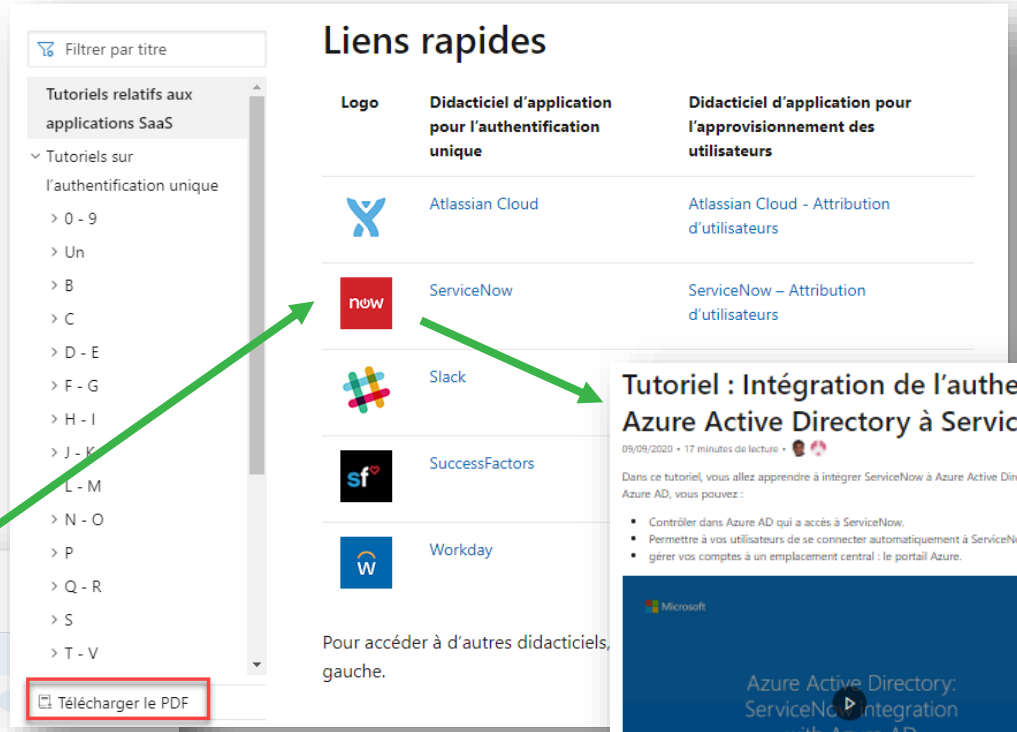
Azure Active Directory – Modern Authentication

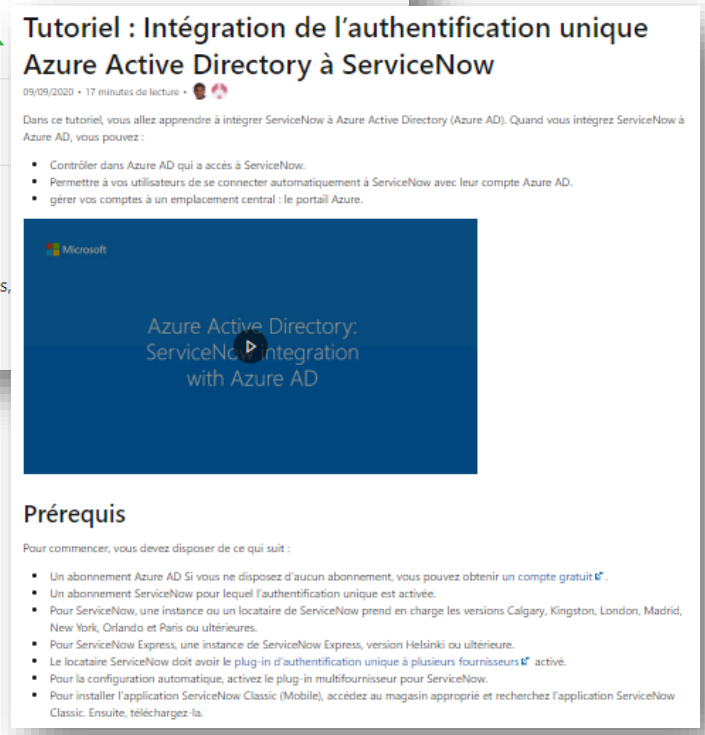
P1

Enterprise Applications & SSO







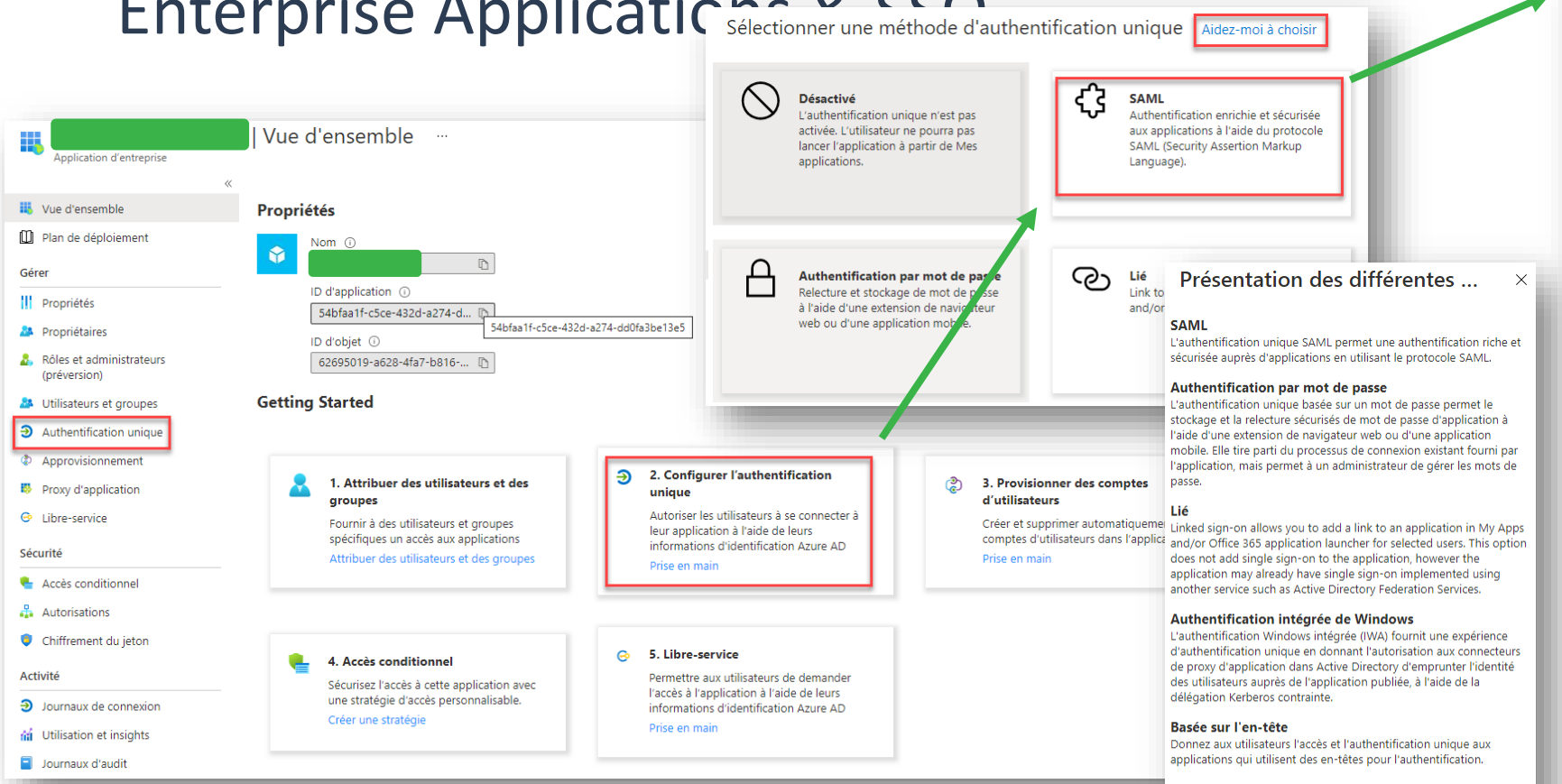


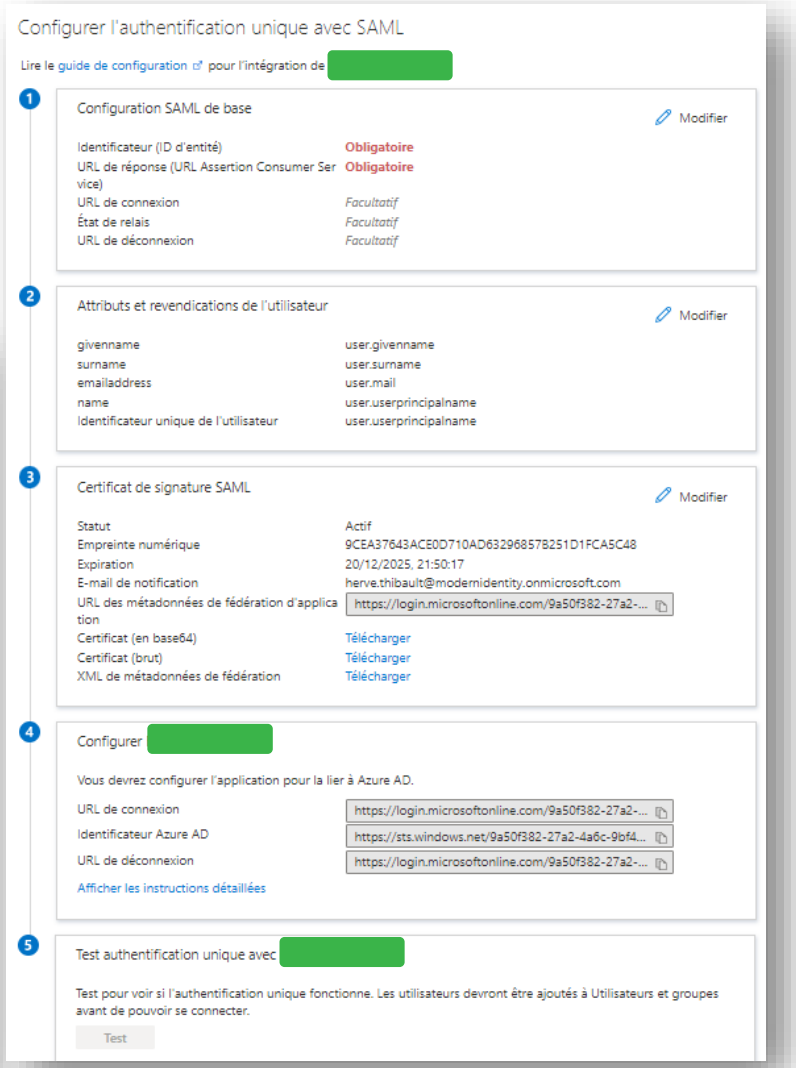
Application du catalogue

Azure Active Directory – Modern Authentication

P1

Enterprise Applications & SSO





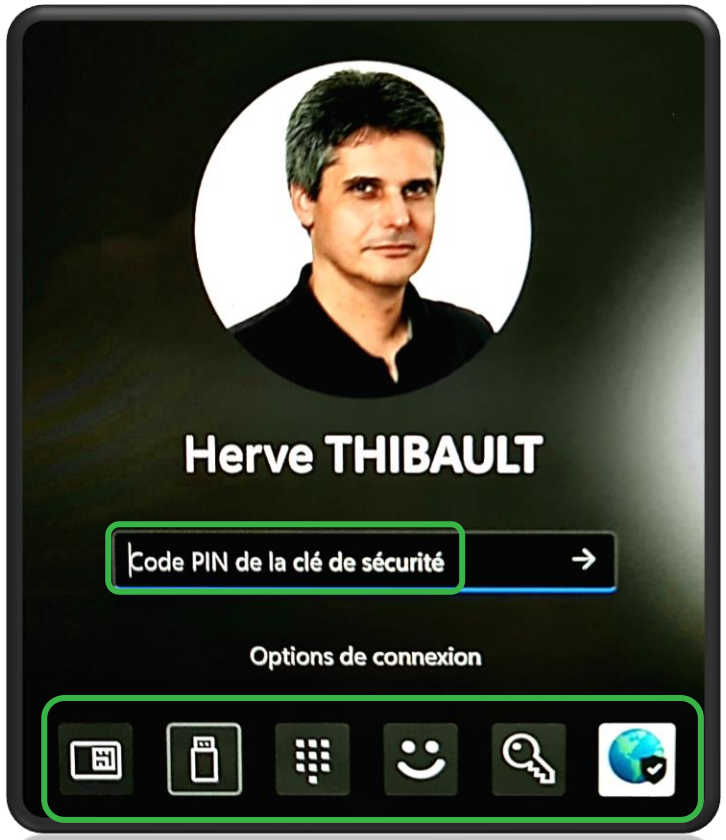
Application non référencée

Azure Active Directory – Modern Authentication

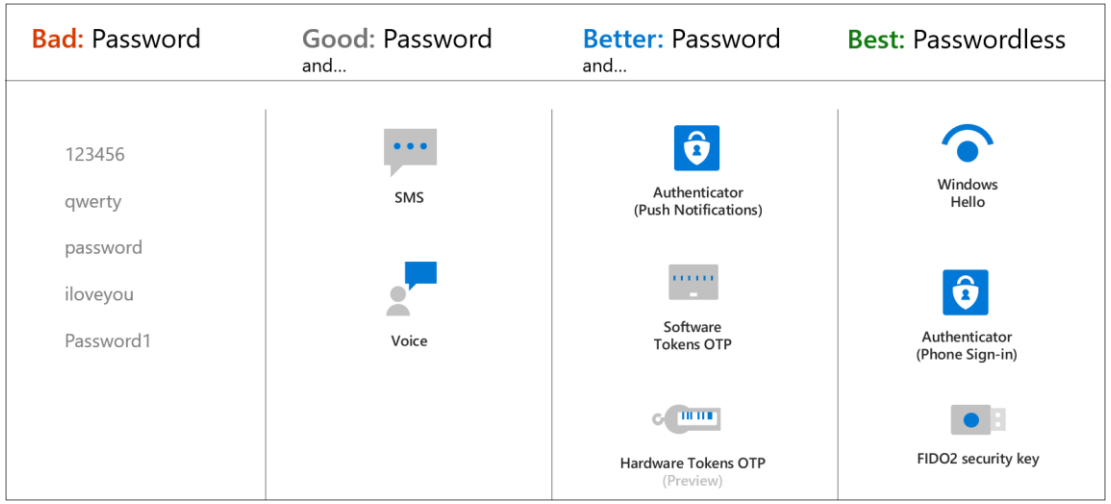
P1

Passwordless

- Passwordless ou comment simplifier l'accès aux ressources d'entreprise sans sacrifier la sécurité
- Introduction : http://aka.ms/gopasswordless
- Windows Hello for Business : https://aka.ms/whfb
- FIDO2 Documentation : http://aka.ms/fido2docs



Méthode d'authentification	Sécurité	Facilité d'utilisation	Disponibilité
Windows Hello Entreprise	Élevée	Élevée	Élevée
Application Microsoft Authenticator	Élevée	Élevée	Élevée
Clé de sécurité FIDO2	Élevée	Élevée	Élevée
SMS	Moyenne	Élevée	Moyenne
Voix	Moyenne	Moyenne	Moyenne
Mot de passe	Faible	Élevée	Élevée

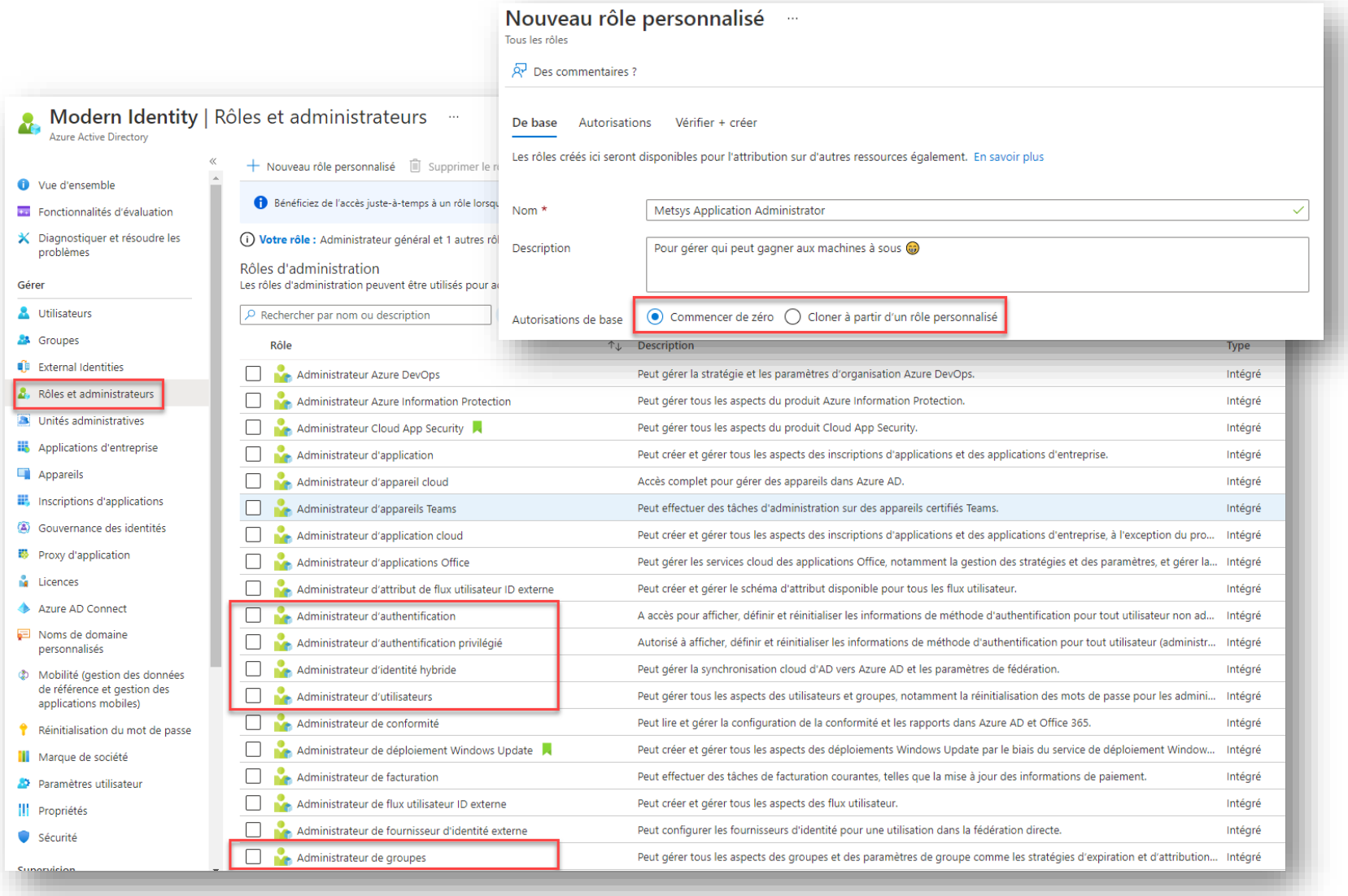


O365

Azure Active Directory – Identity Governance

Roles & Custom Roles

- Un rôle est défini comme une collection d'actions
- Plus de 60 rôles pré-intégrés dans Azure Active Directory :
  - Certains associés à des services : Exchange Online, Intune, Teams, …
  - Beaucoup associés à des « rôles opérationnels » Azure AD
  - Ces définitions de rôles ne peuvent pas être modifiées
- Pour compléter les rôles intégrés, Azure AD prend également en charge des rôles personnalisés (custom roles), à utiliser pour définir des autorisations de rôle spécifiques



P2

Azure Active Directory – Identity Governance

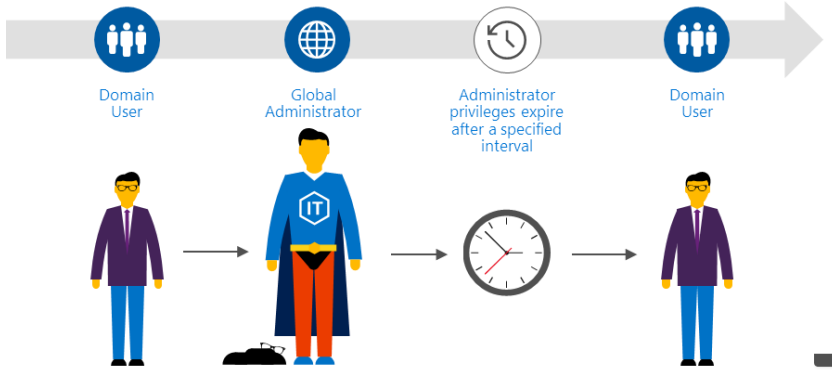
Privileged Identity Management

Les organisations doivent limiter le nombre de personnes qui ont accès aux informations et aux ressources sécurisées, afin de réduire le risque qu'un acteur malveillant accède à ces données, ou qu'une ressource sensible soit accidentellement impactée par un utilisateur autorisé

Cependant, certains utilisateurs doivent pouvoir continuer à effectuer des opérations privilégiées dans les applications Azure AD, Azure, Microsoft 365 ou SaaS

Le juste équilibre !

- Just In Time Administration (JITA)
- Just Enough Administration (JEA)

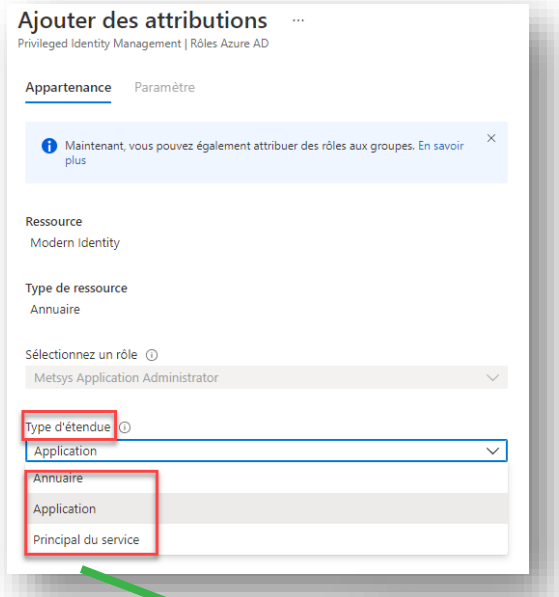


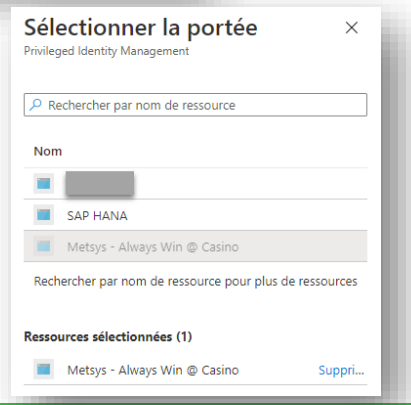
- Les organisations peuvent donner aux utilisateurs un accès privilégié, juste le temps nécessaire et sur le périmètre nécessaire, aux ressources Azure et à Azure AD
- Elles doivent alors pouvoir surveiller ce que ces utilisateurs font avec leurs privilèges d'administrateur

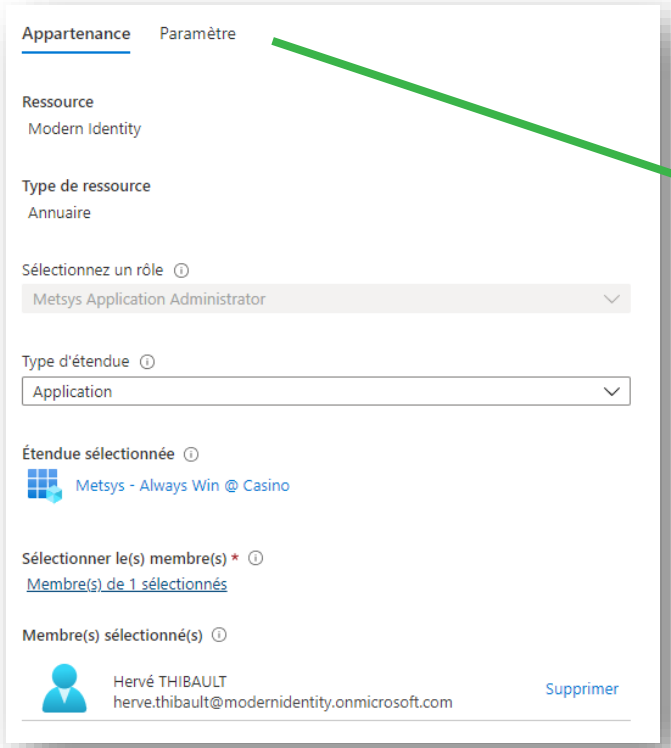
P2

Azure Active Directory – Identity Governance

Privileged Identity Management







Gérer l'accès

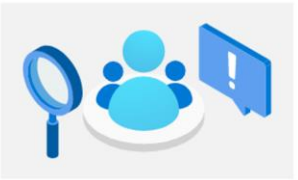
Les utilisateurs disposant d'un accès excessif sont vulnérables en cas de compromission d'un compte. Assurez-vous que votre organisation gère le moindre privilège en examinant, en renouvelant ou en étendant l'accès aux ressources.

Gérer

Activer juste-à-temps

Réduisez le risque de mouvement latéral en cas de compromission d'un compte en éliminant l'accès permanent aux rôles et ressources privilégiés. Appliquez l'accès juste-à-temps aux rôles critiques avec PIM.

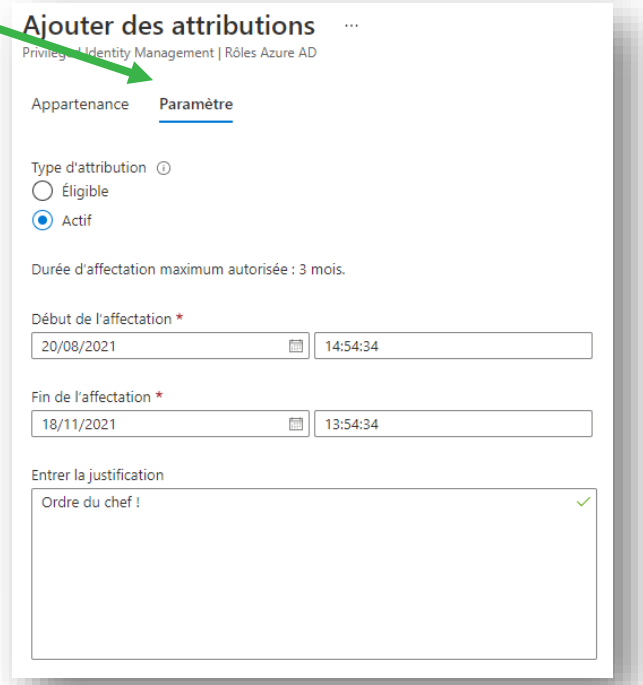
Activer



Découvrir et surveiller

Il est courant que l'accès aux ressources critiques ne soit pas détecté. Vérifiez que vous savez qui a accès à quoi et recevez des notifications lorsque de nouvelles attributions sont accordées aux comptes de votre organisation.

Détecter

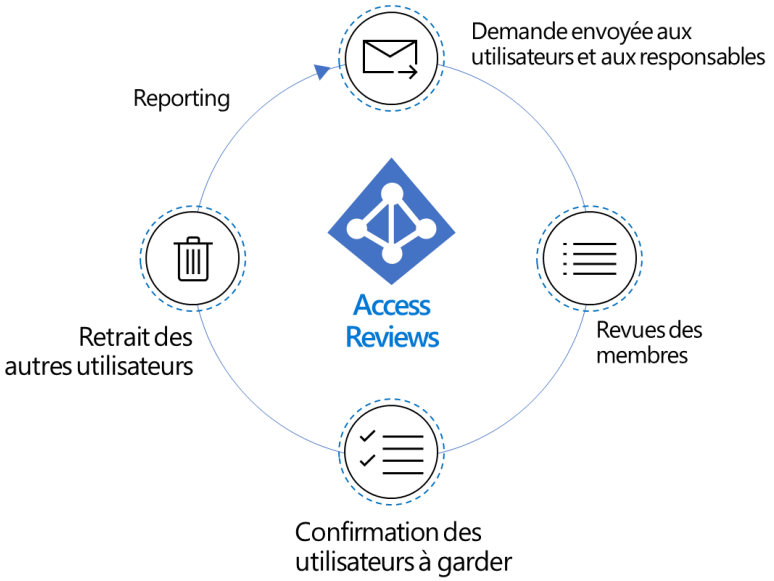


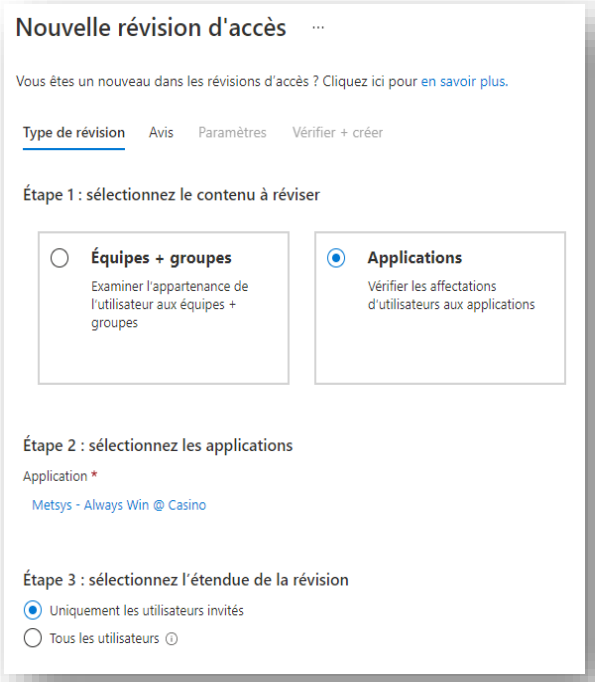
Azure Active Directory – Identity Governance

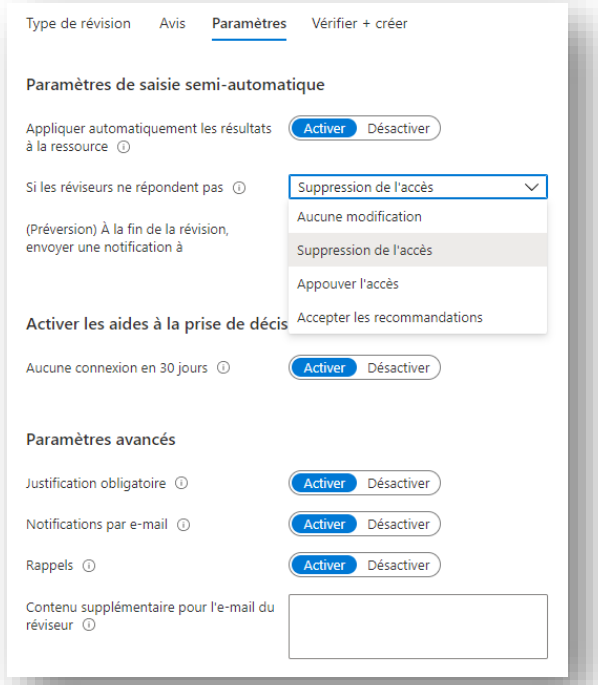
Access Review

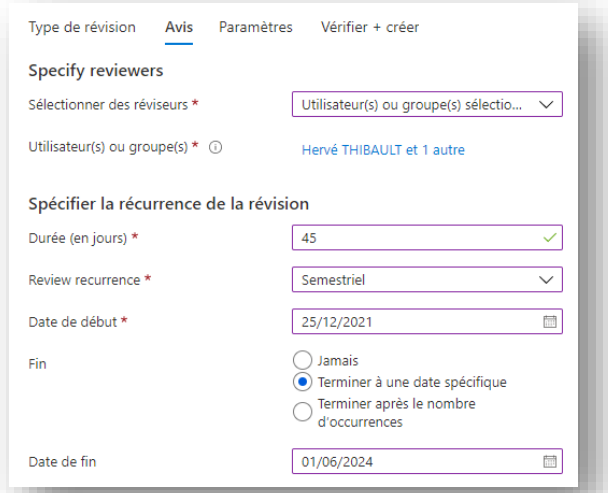
P2

- Gérer efficacement les appartenances à des groupes, les accès aux applications d'entreprise et les attributions de rôles
- L'accès des utilisateurs peut être passé en revue régulièrement pour vérifier que seules les personnes appropriées continuent de bénéficier d'un accès









“Legacy” Identity : Active Directory

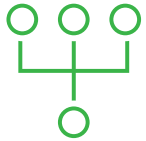
“Modern” Identity : Azure Active Directory

Active Directory vs Azure Active Directory

	Active Directory	Azure AD (premium)
Infrastructure & Authentication	• Forêts, domaines, DCs, OUs, GPOs … • Protocoles : Kerberos, NTLM, … • Users, groups, applications, Windows Wks & Srv • Pas de solution intégrée de SSO	• Microsoft-managed (zero infra) • Internet-friendly / Modern protocols (oAuth, …) • Users, groups, applications, devices (iOS, Android, …) • Pas de GPOs dans Azure AD … Mais Intune est là pour çà ! • Pas d'OUs … Mais voir du côté des Administrative Units pour les aspects délégation • Seamless SSO / Enterprise Applications
Access Management & Identity Governance	• Des tonnes de groups (statiques) pour gérer les accès aux ressources (files/print) • Pas de PIM/ PAM	• Dynamic Groups • Roles / RBAC / Custom Roles • Access Review • Protected Identity Management • Entilement Management – Access packages & strategies
Identity Protection & Self-Service	• Logs AD, réputés pour être explicites et faciles à analyser ☺ • Add-on Microsoft Defender for Identity ou Tenable.ad pour resistance aux menaces • Pas de solution native de MFA • Pas de suivi de ses propres connexions, pas d'alerting • Pas de self-service mot de passe • Clé Bitlocker dans AD mais pas de self-service natif (MBAM)	• MFA / Conditional Access • Users at risk • My sign-ins • Self Service Password Reset • Identity Secure Score • SSPR • Self-Service Bitlocker Recovery Key

Azure Active Directory, la solution miracle ?

- Azure AD n'est pas une solution miracle qui résout tous les problèmes en un clin d'œil …
- … Mais elle permet d'améliorer sensiblement, facilement et rapidement, sa posture de sécurité sur l'identité
  - Quick Wins : MFA, Passwordless
  - Intermédiaire : Conditional Access (mais le jeu en vaut généralement largement la chandelle)
  - Plus exigeant car demandant notamment un niveau de maturité élevé (process) : Identity Governance (PIM/PAM), …
- Et sinon, pour des occasions particulières :
  - Carve-out (ou au contraire intégration de nouvelle structure)
  - Reprise sur incident (ransomware) – Alternative pour remonter rapidement un SI (Infra lite)

Merci à tous nos partenaires !

zscaler onelogin SailPoint METSYS Auth0 FUSION DIRECTORY

Microsoft Vorteks make IT work, make IT free

tenable yubico ManageEngine WALLIX CYBERSECURITY SIMPLIFIED Exakis Nelite Magellan Partners Alphorm.com