



IDENTITY DAYS

28 octobre 2021 - PARIS



@IdentityDays #identitydays2021

Merci à tous nos partenaires !



onelogin



yubico





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

Hervé THIBAULT

Hervé THIBAUT



Chief Technology Officer
@ Metsys

Microsoft Regional
Director depuis 2015



[Rd.microsoft.com/herve.thibault](https://rd.microsoft.com/herve.thibault)

Microsoft Most Valuable
Professional 2007-2014

 @thibherv

AGENDA DE LA CONFÉRENCE

- 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

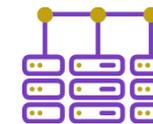
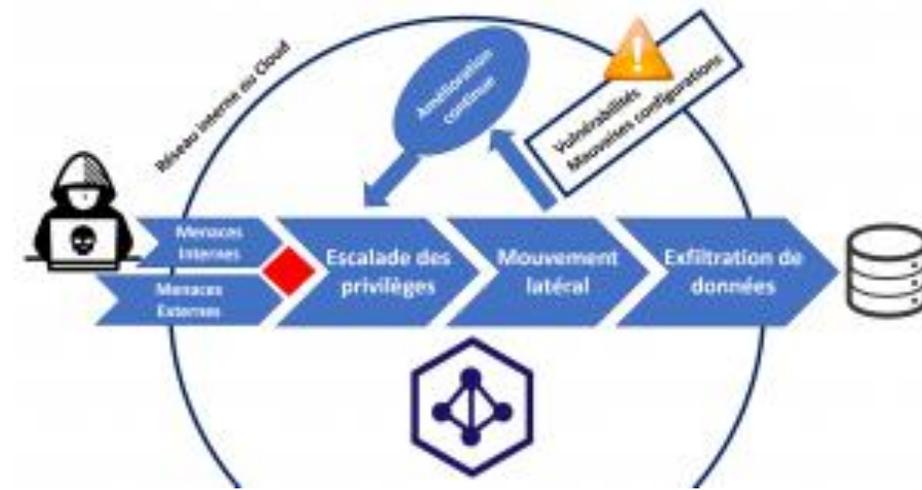


“Legacy” Identity : Active Directory

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 travail & 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)

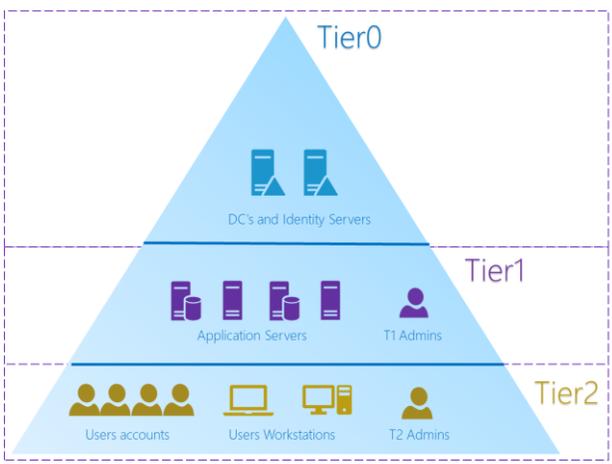
5 Bastion, stations d'administration
sécurisées (PAW)

6 Gestion des identités à privilèges

7 Authentification forte

8 Passwordless

9 Threat Management :
Microsoft Defender
for Identity,
Tenable.ad

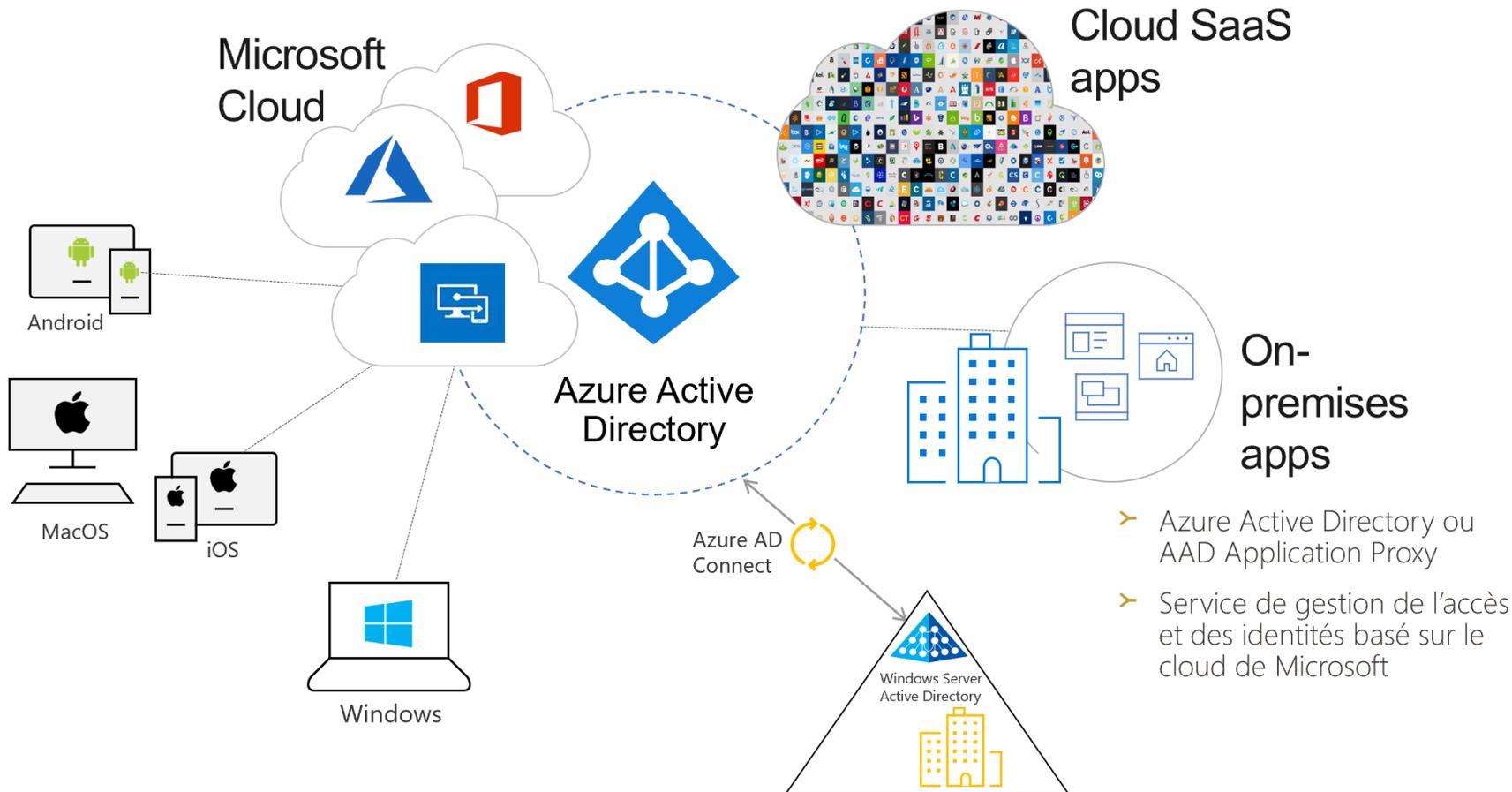




“Modern” Identity : Azure Active Directory

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

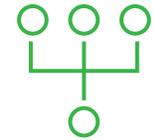

 P2


 O365

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



Identity Protection
 Conditional Access
 MFA
 Secure score
 Password protection



Self-Service
 Password recovery
 My sign-ins
 Bitlocker recovery key



Identity Governance
 Roles
 Administrative Units
 Privileged Identity &
 Access Management

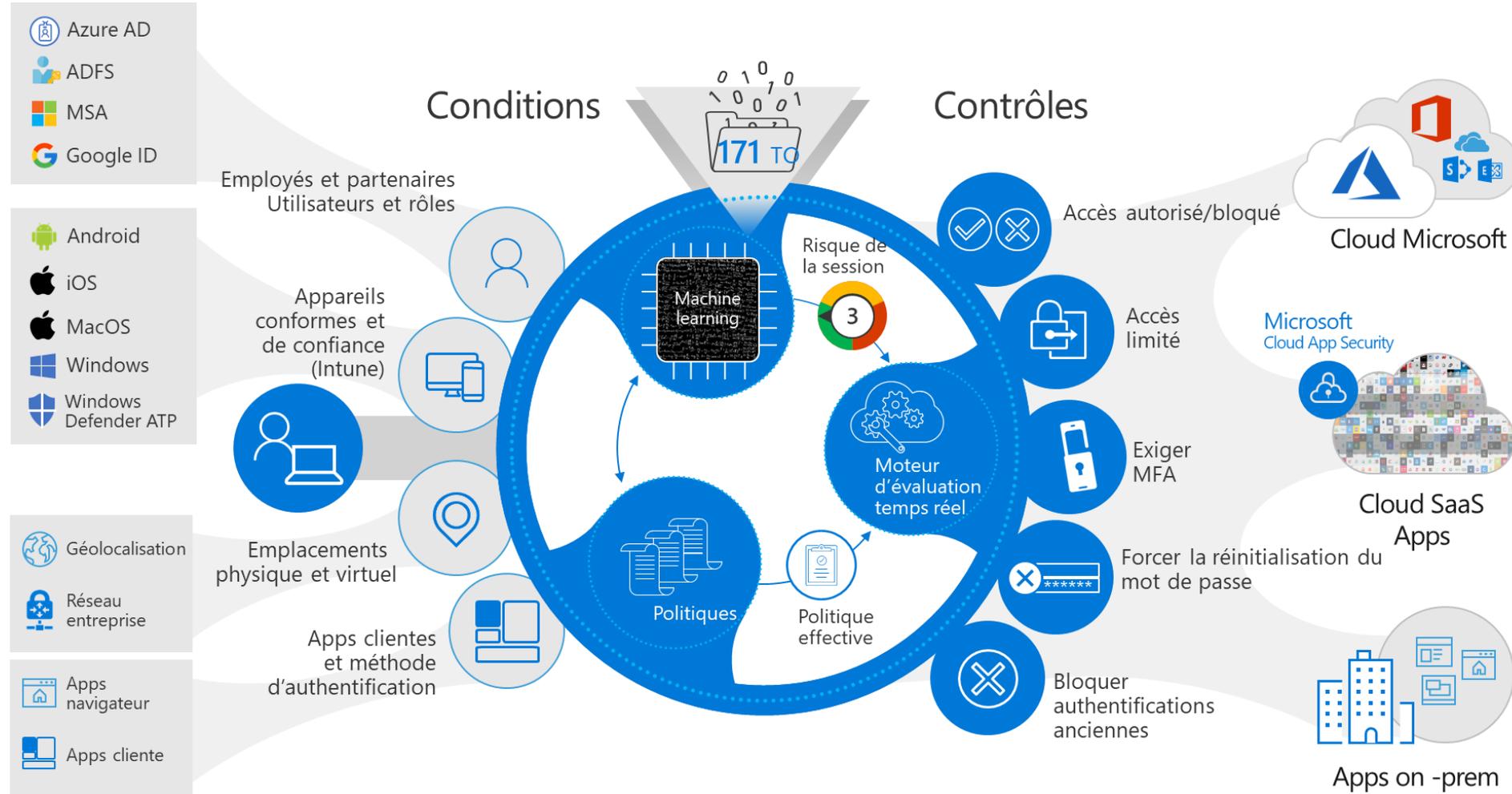


Modern Authentication
 Enterprise Applications
 & SSO
 Passwordless



Azure Active Directory – Identity Protection

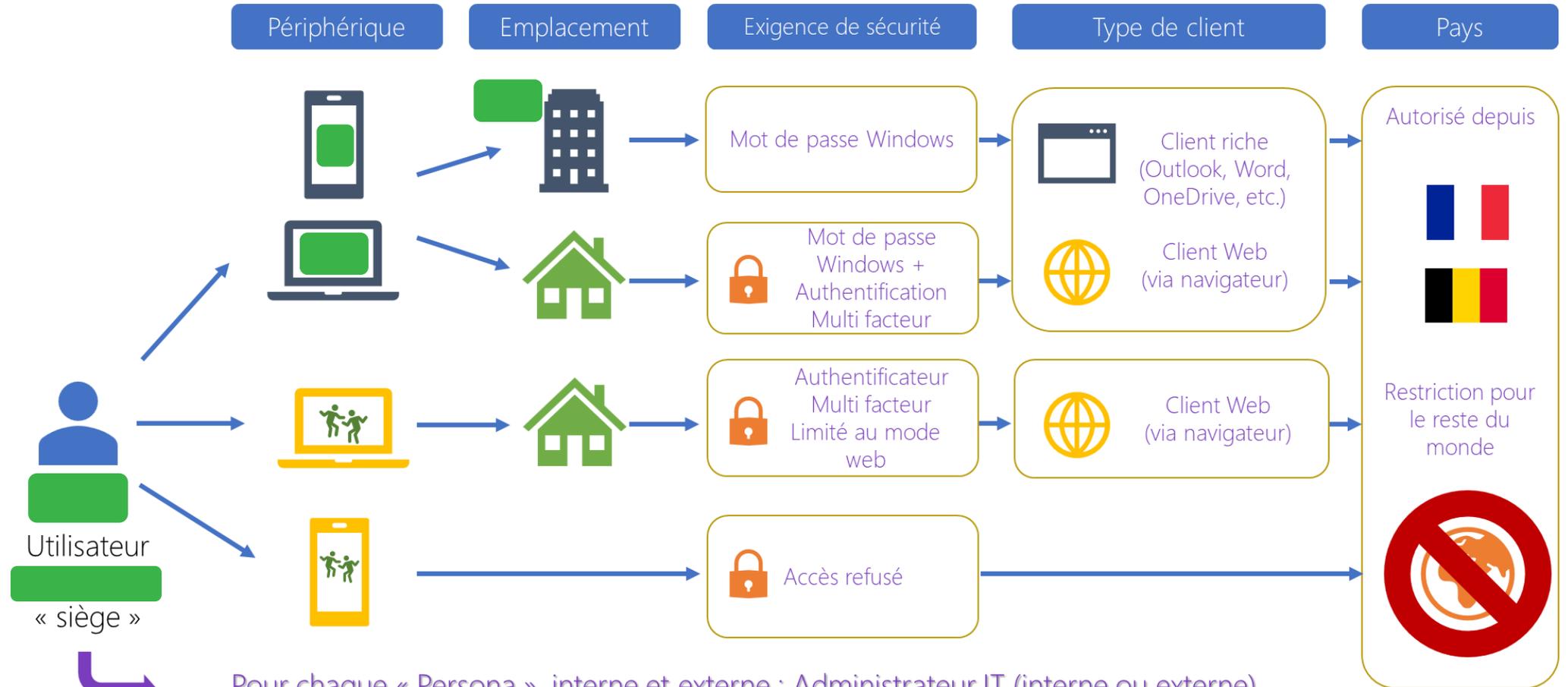
Conditional Access





Azure Active Directory – Identity Protection

Conditional Access



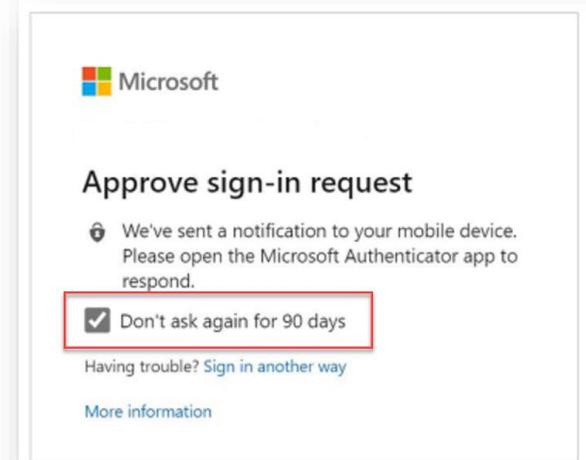
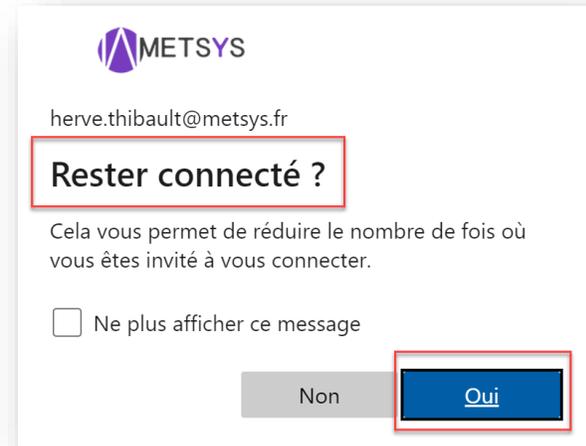
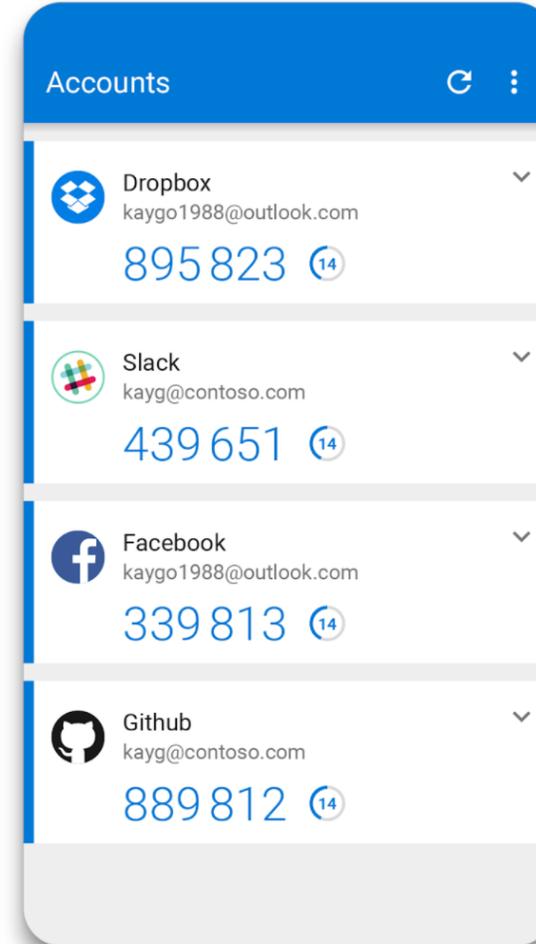
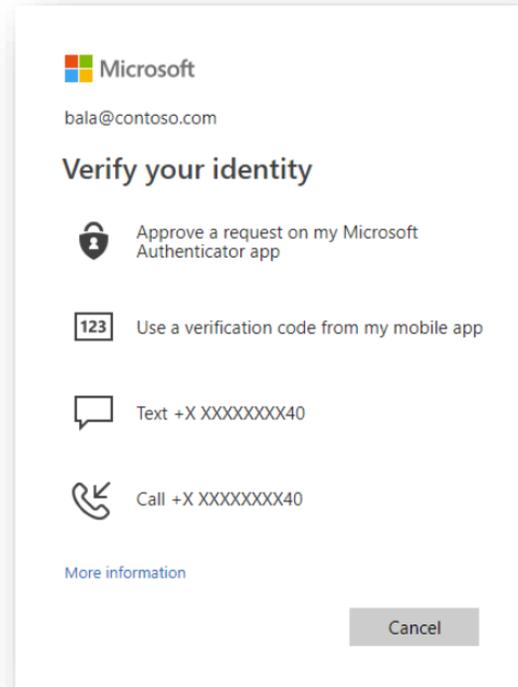
Pour chaque « Persona », interne et externe : Administrateur IT (interne ou externe), collaborateur magasin, patron magasin, prestataire, fournisseur, ...



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





Azure Active Directory – Identity Protection

MFA

<https://aka.ms/MFAsetup>

METSYS

herve.thibault@metsys.fr

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

Is this info up to date?

It's important to keep your security info up to date. This is how you can prove who you are when you sign in or lose your password.

Security info

Default sign-in method: Phone - text

Phone +33

Security key Metsys-HTTP-Yubikey

Ok Edit info

Ajouter une méthode

Quelle méthode voulez-vous ajouter ?

Choisir une méthode

- Application d'authentification
- Numéro de téléphone secondaire
- E-mail
- Mot de passe d'application
- Clé de sécurité
- Téléphone (bureau)

METSYS Mes connexions

- Vue d'ensemble
- Informations de sécurité**
- Organisations
- Appareils
- Confidentialité

Informations de sécurité

Voici les méthodes que vous utilisez pour vous connecter à votre compte ou réinitialiser votre mot de passe.

Méthode de connexion par défaut : Téléphone - envoyer un SMS à +33 [Changer](#)

[+ Ajouter une méthode](#)

Téléphone	+33	Changer	Supprimer
Microsoft Authenticator	SM-G986B		Supprimer
Clé de sécurité	Metsys-HTTP-Yubikey		Supprimer

[Appareil perdu ? Se déconnecter partout](#)



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 connaître la cause :
 - Niveau d'amélioration de la sécurité
 - Coût d'implémentation / Charge IT
 - Impact utilisateur

Sécurité | Score d'identité sécurisée

Microsoft Secure Score for Identity est une représentation du niveau de sécurité de votre organisation et de votre possibilité de l'améliorer. [En savoir plus.](#)

Secure Score for Identity
29.29%
 Dernière mise à jour : 24/08/2021, 02:00:00
 Consultez votre [Niveau de sécurité Microsoft][1]. [1]: <https://aka.ms/idscorescorefromazureportal>

Historique du score
 7 jours 30 jours 60 jours 90 jours
 29.29%
 0% 50 40 30 20 10 0%
 19 août

Comparaison
 Modern Identity
 Organisation comme la vôtre
 Entreprise classique
 Modifier le secteur d'activité

Actions d'amélioration
 Télécharger Colonnes

Nom	Impact du degré	Impact sur l'utilisateur
Exiger l'authentification multifactor pour les rôles administratifs	17.86 %	Bas
Désignation de plusieurs administrateurs généraux	1.79 %	Bas
Interdiction aux utilisateurs d'accorder des autorisations aux applications non oérées	7.14 %	Modéré
Limitation des rôles d'administrateurs	1.79 %	Bas
Mots de passe sans expiration	14.29 %	Modéré
Activation de la stratégie pour empêcher l'authentification héritée	14.29 %	Modéré
Activation de la stratégie de connexion à risque	12.50 %	Modéré
Activation de la stratégie d'utilisateur à risque	12.50 %	Modéré
S'assurer que tous les utilisateurs peuvent terminer l'authentification multifactor pour un accès sécurisé	16.07 %	Haute
Activation de la réinitialisation du mot de passe libre-service	1.79 %	Modéré

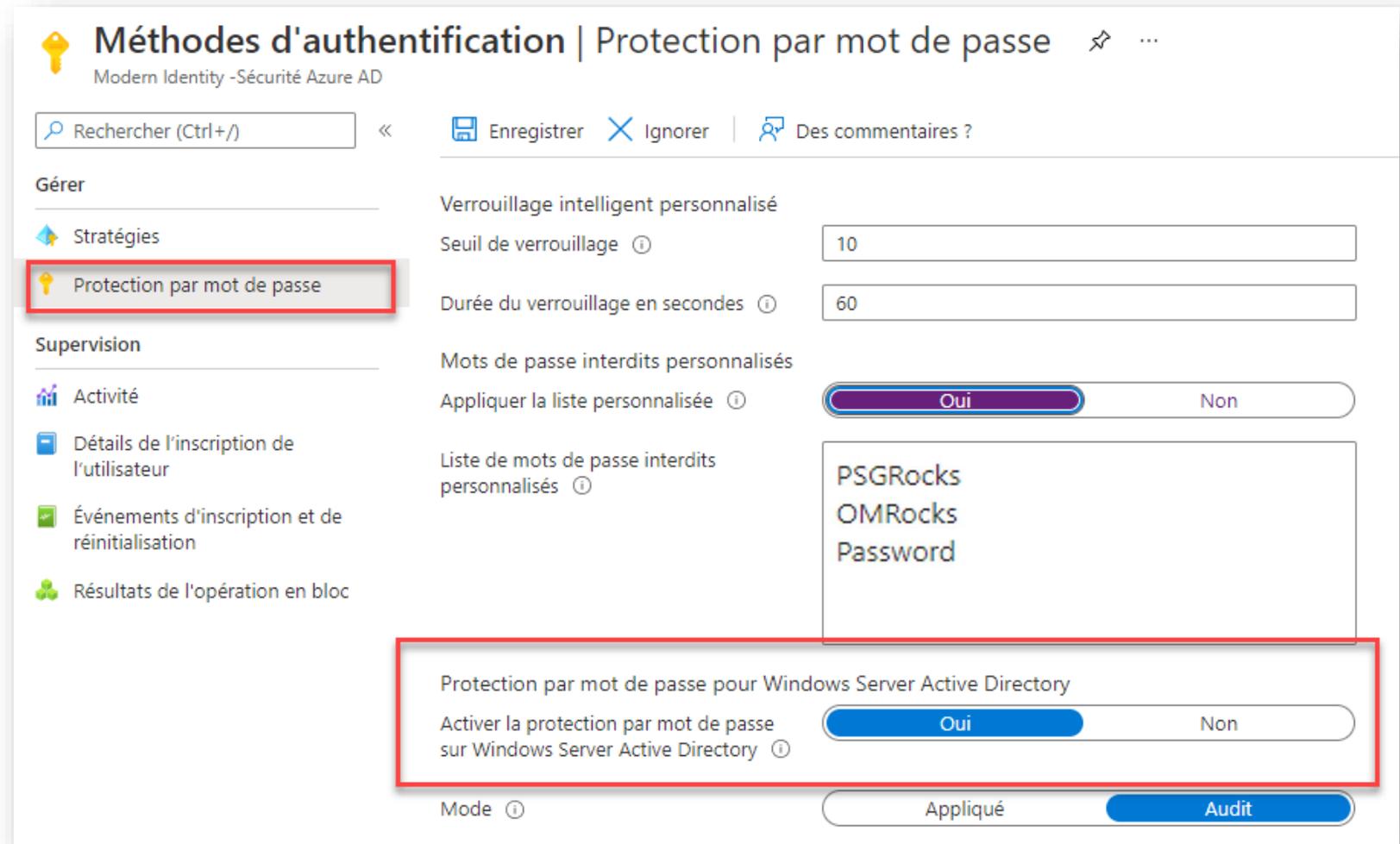
Action d'amélioration
libre-service
 IMPACT DU DEGRÉ +1.79 %
 DEGRÉ ACTUEL 0
 DEGRÉ MAXIMAL 1
STATUT
 Pour traiter
 DESCRIPTION
 Avec la réinitialisation de mot de passe en libre-service dans Azure Active Directory, les utilisateurs n'ont plus besoin de solliciter le support technique pour réinitialiser leur mot de passe. Cette technologie fonctionne bien avec les mots de passe interdits de manière dynamique par Azure AD afin d'empêcher l'utilisation des mots de passe faciles à deviner.
 IMPACT SUR L'UTILISATEUR Modéré
 COÛT D'IMPLÉMENTATION Modéré
 QUE SUIS-JE SUR LE POINT DE CHANGER ?
 Dans le panneau Azure AD Réinitialisation de mot de passe, vous pouvez activer la réinitialisation de mot de passe en libre-service. Sur la page Propriétés, sélectionnez **Tous** ou **Sélectionné** pour choisir les utilisateurs auxquels appliquer votre stratégie. Configurez vos méthodes d'authentification pour permettre aux utilisateurs de réinitialiser leur mot de passe. Sur la page inscription, sélectionnez **Oui** sous Exiger l'inscription des utilisateurs lors de la connexion, et définissez le nombre de jours après lequel les utilisateurs sont invités à reconfirmer leurs informations d'authentification.
 COMMENT CELA VA AFFECTER MES UTILISATEURS ?
 Les utilisateurs pourront réinitialiser leur mot de passe en libre-service dans Azure AD et n'auront plus besoin de contacter le support technique.



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>



Méthodes d'authentification | Protection par mot de passe

Modern Identity - Sécurité Azure AD

Rechercher (Ctrl+/) << Enregistrer Ignorer | Des commentaires ?

Gérer

- Stratégies
- Protection par mot de passe**

Supervision

- Activité
- Détails de l'inscription de l'utilisateur
- Événements d'inscription et de réinitialisation
- Résultats de l'opération en bloc

Verrouillage intelligent personnalisé

Seuil de verrouillage ⓘ 10

Durée du verrouillage en secondes ⓘ 60

Mots de passe interdits personnalisés

Appliquer la liste personnalisée ⓘ **Oui** Non

Liste de mots de passe interdits personnalisés ⓘ

PSGRocks
OMRocks
Password

Protection par mot de passe pour Windows Server Active Directory

Activer la protection par mot de passe sur Windows Server Active Directory ⓘ **Oui** Non

Mode ⓘ Appliqué **Audit**

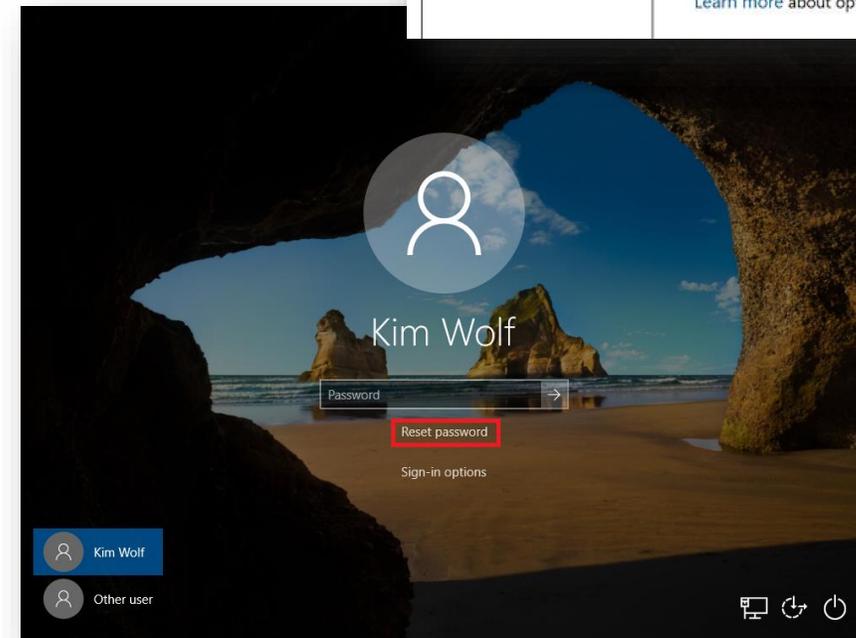
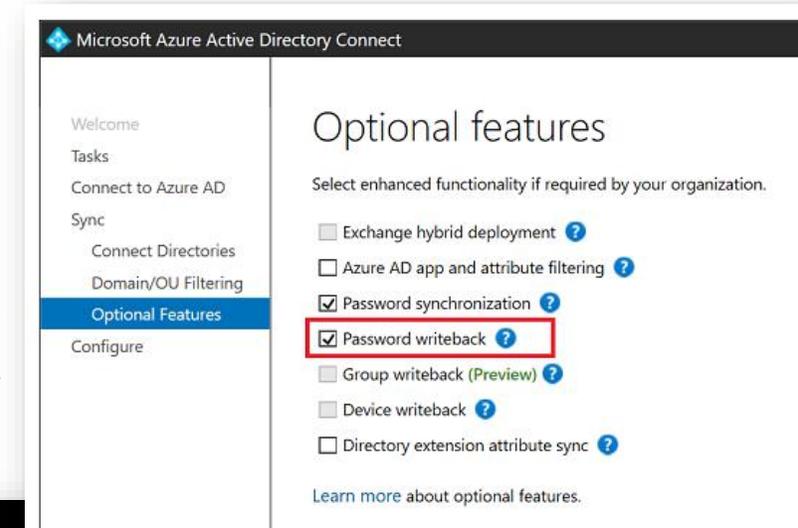


Azure Active Directory – Self-service

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**
- 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/tutorial-enable-sspr-writeback>



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



Azure Active Directory – Self-service

Self-Service Password Recovery (SSPR)

Réinitialisation du mot de passe | Méthodes d'authentification

Modern Identity - Azure Active Directory

Enregistrer Ignorer

Diagnostiquer et résoudre les problèmes

Gérer

- Propriétés
- Méthodes d'authentification
- Inscription
- Notifications
- Personnalisation
- Intégration locale
- Stratégie d'administrateur

Activité

- Journaux d'audit
- Utilisation et insights

Dépannage + support

- Nouvelle demande de support

Nombre de méthodes à réinitialiser

1 2

Méthodes disponibles pour les utilisateurs

- Notification d'application mobile
- Code d'application mobile

Les utilisateurs peuvent inscrire leur application mobile à la page <https://aka.ms/mfasetup> ou expérience d'inscription des informations de sécurité à la page <https://aka.ms/setupsecurityin> l'inscription des informations de sécurité pour votre organisation en suivant les étapes indiquées à <https://aka.ms/securityinfodocs>. Pour une aide supplémentaire sur l'utilisation des méthodes d'Authenticator, visitez <https://aka.ms/uthappsspr>.

E-mail

Téléphone mobile (SMS uniquement)

Téléphone (bureau)

Questions de sécurité

Nombre de questions requises pour l'inscription

3 4 5

Nombre de questions requises pour la réinitialisation

3 4 5

Sélectionner les questions de sécurité

3 questions de sécurité sélectionnées

Tableau de bord > Modern Identity > Réinitialisation du mot de passe >

Sélectionner les questions de sécurité

+ Prédéfinies + Personnalisé X Supprimer

Prédéfinies

- Dans quelle ville avez-vous rencontré votre premier(ère) époux/épouse ou compagnon/compagne ?
- Quel était le nom de votre héros d'enfance ?
- Quelle est la personne la plus célèbre que vous ayez jamais rencontrée ?

Personnalisé

- Quel est votre magasin favori ?

Ajouter des questions de sécurité prédéfinies

- Dans quelle ville avez-vous rencontré votre premier(ère) époux/épouse ou compagnon/compagne ?
- Dans quelle ville vos parents se sont-ils rencontrés ?
- Dans quelle ville vit votre frère ou sœur le/la plus proche ?
- Dans quelle ville votre père est-il né ?
- Dans quelle ville était votre premier travail ?
- Dans quelle ville votre mère est-elle née ?
- Dans quelle ville étiez-vous pour le Nouvel an de l'année 2000 ?
- Quel était le nom de votre professeur préféré au lycée ?
- Quel est le nom d'un établissement d'enseignement supérieur auquel vous avez postulé mais auquel vous n'êtes finalement pas allé ?
- Quel est le nom de l'endroit où vous avez organisé la réception de votre premier mariage ?
- Quel est le deuxième prénom de votre père ?
- Quel est votre aliment préféré ?
- Quels sont les nom et prénom de votre grand-mère maternelle ?
- Quel est le deuxième prénom de votre mère ?
- Quel sont le mois et l'année de naissance de votre frère ou sœur aîné ? (par exemple, novembre 1985)
- Quel est le deuxième prénom de votre frère/sœur aîné(e) ?
- Quels sont les nom et prénom de votre grand-père paternel ?
- Quel est le deuxième prénom de votre frère/sœur cadet(te) ?
- Où avez-vous effectué votre dernière année de l'école primaire ?
- Quels étaient les nom et prénom de votre meilleur ami quand vous étiez enfant ?
- Quels étaient les nom et prénom de votre premier(ère) petit(e) ami(e) ?
- Quel était le nom de votre instituteur préféré à l'école primaire ?
- Quels étaient la marque et le modèle de votre première voiture ou moto ?
- Quel était le nom de votre toute première école ?
- Quel était le nom de l'hôpital ou de la clinique où vous êtes né ?



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

METSYS Mes connexions

Date et heure	Localisation	Application	Résultat
Last Thursday at 9:20:30 AM CEST	Hauts-De-Seine, FR	Windows Sign In	✓ Connexion réussie
08/18/2021 3:47:50 PM CEST	Loiret, FR	Windows Sign In	✓ Connexion réussie
08/18/2021 3:19:35 PM CEST	Loiret, FR	Microsoft 365 Support Service	✗ Échec de connexion

Additional details for the failed connection (08/18/2021 3:19:35 PM CEST):

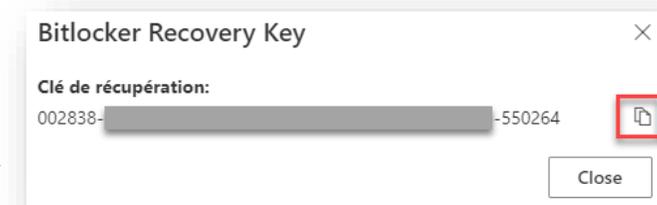
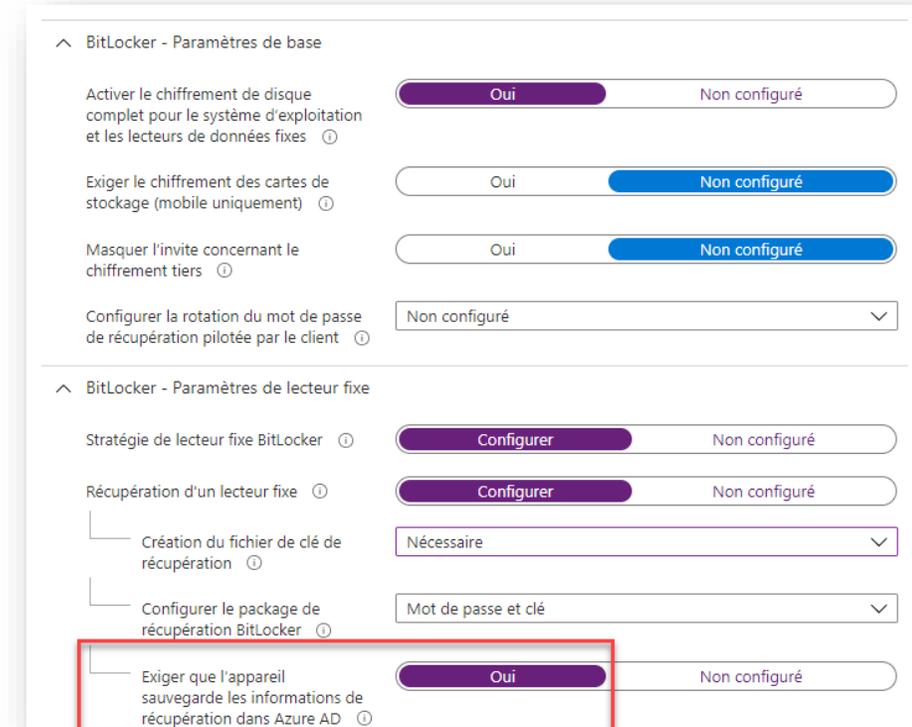
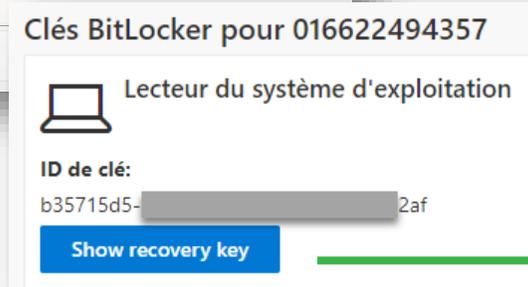
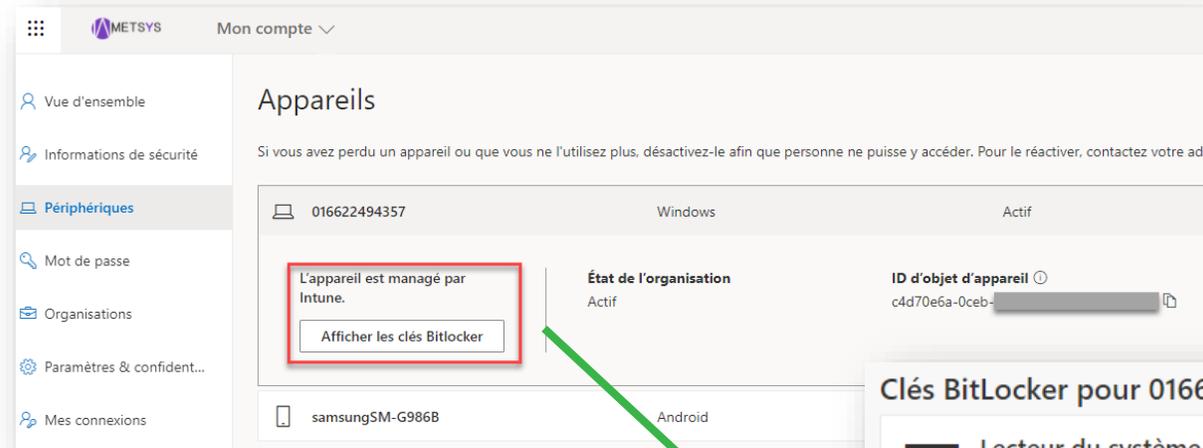
- Emplacement:** Loiret, FR
- Système d'exploitation:** Windows 10
- Navigateur:** Microsoft Edge
- IP:** 90.115.182.113
- Application:** Microsoft 365 Support Service
- Compte:** herve.thibault@metsys.fr

<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>

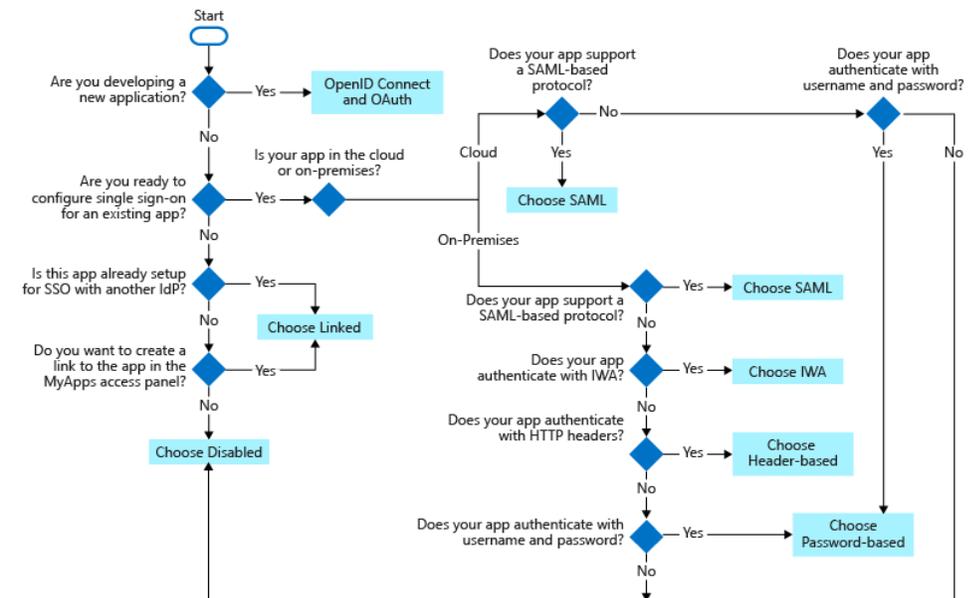
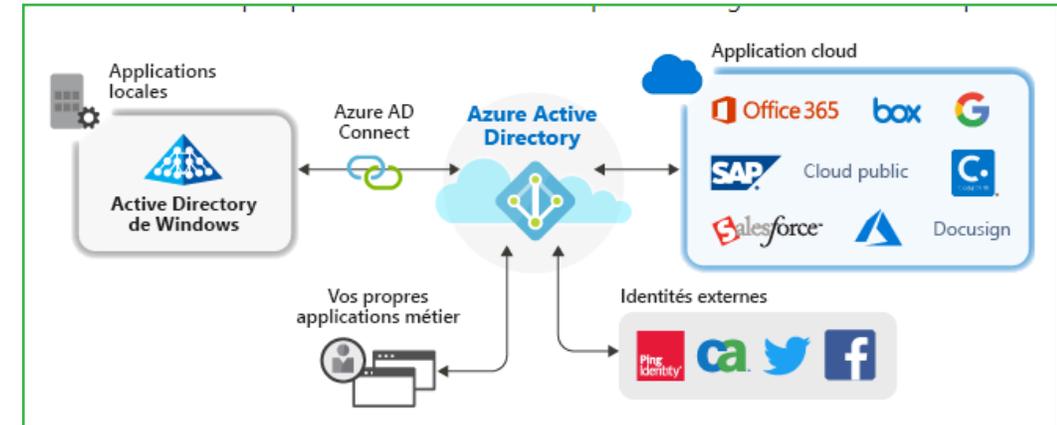


<https://myworkaccount.microsoft.com/>

Azure Active Directory – Modern Authentication

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)



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

Azure Active Directory – Modern Authentication Enterprise Applications & SSO



Accueil > Modern Identity > Applications d'entreprise > Parcourir la galerie Azure AD

+ Créer votre propre application | Demander une nouvelle application de galerie | Des commentaires ?

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

Rechercher dans l'application

Authentification unique : **Tout** | Gestion du compte utilisateur : **All** | Catégories : **Tout**

Plateformes cloud

- Amazon Web Services (AWS)
- Google Cloud Platform
- Oracle
- SAP

Applications locales

Ajouter une application locale

En savoir plus sur

Liens rapides

Logo	Didacticiel d'application pour l'authentification unique	Didacticiel d'application pour l'approvisionnement des utilisateurs
	Atlassian Cloud	Atlassian Cloud - Attribution d'utilisateurs
	ServiceNow	ServiceNow – Attribution d'utilisateurs
	Slack	
	SuccessFactors	
	Workday	

Filterer par titre

Tutoriels relatifs aux applications SaaS

Tutoriels sur l'authentification unique

- > 0 - 9
- > Un
- > B
- > C
- > D - E
- > F - G
- > H - I
- > J - K
- > L - M
- > N - O
- > P
- > Q - R
- > S
- > T - V

Télécharger le PDF

Parcourir la galerie Azure AD

+ Créer votre propre application | Demander une nouvelle application de galerie | Des commentaires ?

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

Rechercher dans l'application

Authentification unique : **Tout** | Gestion du compte utilisateur : **All** | Catégories : **Tout**

SSO fédéré | Approvisionnement

Affichage de 8 sur 8 résultats

- ServiceNow** ServiceNow
- ServiceChannel** ServiceChannel
- UserVoice** UserVoice, Inc.
- Colibri** Visio
- AWS Single Sign-on** Amazon Web Services, Inc.
- AWS ClientVPN** Amazon Web Services (AWS)

Tutoriel : Intégration de l'authentification unique Azure Active Directory à ServiceNow

09/09/2020 • 17 minutes de lecture

Dans ce tutoriel, vous allez apprendre à intégrer ServiceNow à Azure Active Directory (Azure AD). Quand vous intégrez ServiceNow à Azure AD, vous pouvez :

- Contrôler dans Azure AD qui a accès à ServiceNow.
- Permettre à vos utilisateurs de se connecter automatiquement à ServiceNow avec leur compte Azure AD.
- Gérer vos comptes à un emplacement central : le portail Azure.

Prérequis

Pour commencer, vous devez disposer de ce qui suit :

- Un abonnement Azure AD SI vous ne disposez d'aucun abonnement, vous pouvez obtenir un compte gratuit.
- Un abonnement ServiceNow pour lequel l'authentification unique est activée.
- Pour ServiceNow, une instance ou un locataire de ServiceNow prend en charge les versions Calgary, Kingston, London, Madrid, New York, Orlando et Paris ou ultérieures.
- Pour ServiceNow Express, une instance de ServiceNow Express, version Helsinki ou ultérieure.
- Le locataire ServiceNow doit avoir le plug-in d'authentification unique à plusieurs fournisseurs activé.
- Pour la configuration automatique, activez le plug-in multifournisseur pour ServiceNow.
- Pour installer l'application ServiceNow Classic (Mobile), accédez au magasin approprié et recherchez l'application ServiceNow Classic. Ensuite, téléchargez-la.

Application du catalogue

Azure Active Directory – Modern Authentication

Enterprise Applications & SSO



Sélectionner une méthode d'authentification unique [Aidez-moi à choisir](#)

Application d'entreprise | Vue d'ensemble

Propriétés

Nom: [redacted]

ID d'application: 54bfaa1f-c5ce-432d-a274-d... / 54bfaa1f-c5ce-432d-a274-dd0fa3be13e5

ID d'objet: 62695019-a628-4fa7-b816-...

Getting Started

- 1. Attribuer des utilisateurs et des groupes**
Fournir à des utilisateurs et groupes spécifiques un accès aux applications.
[Attribuer des utilisateurs et des groupes](#)
- 2. Configurer l'authentification unique**
Autoriser les utilisateurs à se connecter à leur application à l'aide de leurs informations d'identification Azure AD.
[Prise en main](#)
- 3. Provisionner des comptes d'utilisateurs**
Créer et supprimer automatiquement des comptes d'utilisateurs dans l'application.
[Prise en main](#)
- 4. Accès conditionnel**
Sécurisez l'accès à cette application avec une stratégie d'accès personnalisable.
[Créer une stratégie](#)
- 5. Libre-service**
Permettre aux utilisateurs de demander l'accès à l'application à l'aide de leurs informations d'identification Azure AD.
[Prise en main](#)

Sélectionner une méthode d'authentification unique

- Désactivé**
L'authentification unique n'est pas activée. L'utilisateur ne pourra pas lancer l'application à partir de Mes applications.
- SAML**
Authentification enrichie et sécurisée aux applications à l'aide du protocole SAML (Security Assertion Markup Language).
- Authentification par mot de passe**
Relecture et stockage de mot de passe à l'aide d'une extension de navigateur web ou d'une application mobile.
- Lié**
Link to and/or

Présentation des différentes ...

SAML
L'authentification unique SAML permet une authentification riche et sécurisée auprès d'applications en utilisant le protocole SAML.

Authentification par mot de passe
L'authentification unique basée sur un mot de passe permet le stockage et la relecture sécurisés de mot de passe d'application à l'aide d'une extension de navigateur web ou d'une application mobile. Elle tire parti du processus de connexion existant fourni par l'application, mais permet à un administrateur de gérer les mots de passe.

Lié
Linked sign-on allows you to add a link to an application in My Apps and/or Office 365 application launcher for selected users. This option does not add single sign-on to the application, however the application may already have single sign-on implemented using another service such as Active Directory Federation Services.

Authentification intégrée de Windows
L'authentification Windows intégrée (IWA) fournit une expérience d'authentification unique en donnant l'autorisation aux connecteurs de proxy d'application dans Active Directory d'emprunter l'identité des utilisateurs auprès de l'application publiée, à l'aide de la délégation Kerberos contrainte.

Basé sur l'en-tête
Donnez aux utilisateurs l'accès et l'authentification unique aux applications qui utilisent des en-têtes pour l'authentification.

Désactivé
Le mode Désactivé signifie que l'authentification unique n'est pas utilisée pour l'application. Cela signifie que l'utilisateur ne pourra pas se connecter à partir de Mes applications à moins qu'il ne soit attribué à l'application. Notez que si vous avez configuré l'authentification unique basée sur SAML exécutée par le SP et que vous changez le mode SSO en Désactivé, cela n'empêche pas les utilisateurs de se connecter à l'application en dehors du portail Mes applications. Pour ce faire, vous devez **désactiver la possibilité pour les utilisateurs de se connecter** et supprimer les affectations d'utilisateur et de groupe à l'application.

Configurer l'authentification unique avec SAML

Lire le guide de configuration pour l'intégration de [redacted]

- 1. Configuration SAML de base**

Identificateur (ID d'entité): **Obligatoire**

URL de réponse (URL Assertion Consumer Service): **Obligatoire**

URL de connexion: *Facultatif*

État de relais: *Facultatif*

URL de déconnexion: *Facultatif*
- 2. Attributs et revendications de l'utilisateur**

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Identificateur unique de l'utilisateur	user.userprincipalname
- 3. Certificat de signature SAML**

Statut: Actif

Empreinte numérique: 9CEA37643ACE0D710AD632968578251D1FCA5C48

Expiration: 20/12/2025, 21:50:17

E-mail de notification: herve.thibault@modernidentity.onmicrosoft.com

URL des métadonnées de fédération d'application: <https://login.microsoftonline.com/9a50f382-27a2-...>

Certificat (en base64): [Télécharger](#)

Certificat (brut): [Télécharger](#)

XML de métadonnées de fédération: [Télécharger](#)
- 4. Configurer [redacted]**

Vous devrez configurer l'application pour la lier à Azure AD.

URL de connexion: <https://login.microsoftonline.com/9a50f382-27a2-...>

Identificateur Azure AD: <https://sts.windows.net/9a50f382-27a2-4a6c-9bf4-...>

URL de déconnexion: <https://login.microsoftonline.com/9a50f382-27a2-...>

[Afficher les instructions détaillées](#)
- 5. Test authentification unique avec [redacted]**

Test pour voir si l'authentification unique fonctionne. Les utilisateurs devront être ajoutés à Utilisateurs et groupes avant de pouvoir se connecter.

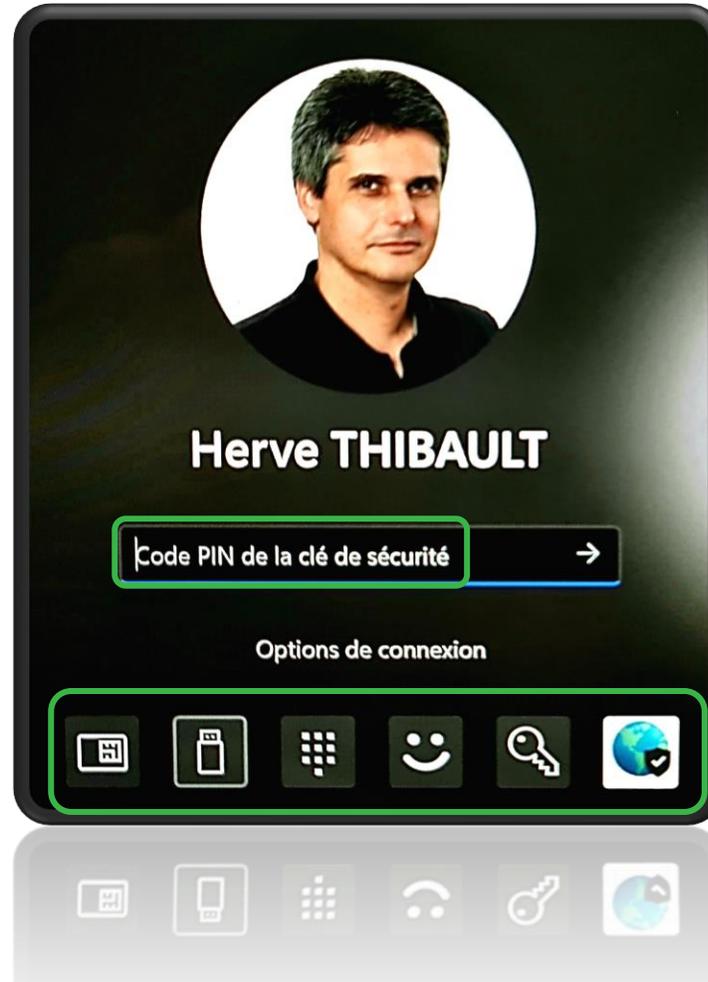
[Test](#)

Application non référencée

Azure Active Directory – Modern Authentication

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

Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456	SMS	Authenticator (Push Notifications)	Windows Hello
qwerty	Voice	Software Tokens OTP	Authenticator (Phone Sign-in)
password		Hardware Tokens OTP (Preview)	FIDO2 security key
iloveyou			
Password1			



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

Modern Identity | Rôles et administrateurs

Nouveau rôle personnalisé

Tous les rôles

Des commentaires ?

De base Autorisations Vérifier + créer

Les rôles créés ici seront disponibles pour l'attribution sur d'autres ressources également. [En savoir plus](#)

Nom * Metsys Application Administrator ✓

Description Pour gérer qui peut gagner aux machines à sous 🎰

Autorisations de base Commencer de zéro Cloner à partir d'un rôle personnalisé

Rôle	Description	Type
<input type="checkbox"/> Administrateur Azure DevOps	Peut gérer la stratégie et les paramètres d'organisation Azure DevOps.	Intégré
<input type="checkbox"/> Administrateur Azure Information Protection	Peut gérer tous les aspects du produit Azure Information Protection.	Intégré
<input type="checkbox"/> Administrateur Cloud App Security	Peut gérer tous les aspects du produit Cloud App Security.	Intégré
<input type="checkbox"/> Administrateur d'application	Peut créer et gérer tous les aspects des inscriptions d'applications et des applications d'entreprise.	Intégré
<input type="checkbox"/> Administrateur d'appareil cloud	Accès complet pour gérer des appareils dans Azure AD.	Intégré
<input type="checkbox"/> Administrateur d'appareils Teams	Peut effectuer des tâches d'administration sur des appareils certifiés Teams.	Intégré
<input type="checkbox"/> Administrateur d'application cloud	Peut créer et gérer tous les aspects des inscriptions d'applications et des applications d'entreprise, à l'exception du pro...	Intégré
<input type="checkbox"/> Administrateur d'applications Office	Peut gérer les services cloud des applications Office, notamment la gestion des stratégies et des paramètres, et gérer la...	Intégré
<input type="checkbox"/> Administrateur d'attribut de flux utilisateur ID externe	Peut créer et gérer le schéma d'attribut disponible pour tous les flux utilisateur.	Intégré
<input type="checkbox"/> Administrateur d'authentification	A accès pour afficher, définir et réinitialiser les informations de méthode d'authentification pour tout utilisateur non ad...	Intégré
<input type="checkbox"/> Administrateur d'authentification privilégié	Autorisé à afficher, définir et réinitialiser les informations de méthode d'authentification pour tout utilisateur (administr...	Intégré
<input type="checkbox"/> Administrateur d'identité hybride	Peut gérer la synchronisation cloud d'AD vers Azure AD et les paramètres de fédération.	Intégré
<input type="checkbox"/> Administrateur d'utilisateurs	Peut gérer tous les aspects des utilisateurs et groupes, notamment la réinitialisation des mots de passe pour les admini...	Intégré
<input type="checkbox"/> Administrateur de conformité	Peut lire et gérer la configuration de la conformité et les rapports dans Azure AD et Office 365.	Intégré
<input type="checkbox"/> Administrateur de déploiement Windows Update	Peut créer et gérer tous les aspects des déploiements Windows Update par le biais du service de déploiement Window...	Intégré
<input type="checkbox"/> Administrateur de facturation	Peut effectuer des tâches de facturation courantes, telles que la mise à jour des informations de paiement.	Intégré
<input type="checkbox"/> Administrateur de flux utilisateur ID externe	Peut créer et gérer tous les aspects des flux utilisateur.	Intégré
<input type="checkbox"/> Administrateur de fournisseur d'identité externe	Peut configurer les fournisseurs d'identité pour une utilisation dans la fédération directe.	Intégré
<input type="checkbox"/> Administrateur de groupes	Peut gérer tous les aspects des groupes et des paramètres de groupe comme les stratégies d'expiration et d'attribution...	Intégré



Azure Active Directory – Identity Governance

Privileged Identity Management

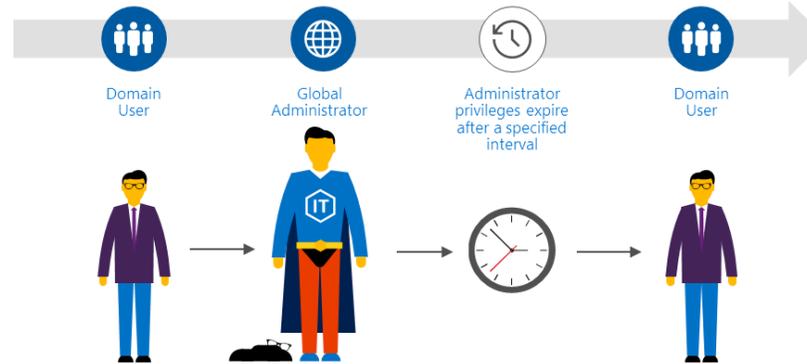
Les organisations doivent limiter le nombre de personnes qui ont accès aux informations et aux ressources sécurisées, afin de réduire le risque qu'un acteur malveillant accède à ces données, ou qu'une ressource sensible soit accidentellement impactée par un utilisateur autorisé

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**



Azure Active Directory – Identity Governance

Privileged Identity Management

Ajouter des attributions ...
Privileged Identity Management | Rôles Azure AD

Appartenance Paramètre

Maintenant, vous pouvez également attribuer des rôles aux groupes. En savoir plus

Ressource
Modern Identity

Type de ressource
Annuaire

Sélectionnez un rôle ⓘ
Metsys Application Administrator

Type d'étendue ⓘ
Application

Annuaire

Application

Principal du service

Sélectionner la portée ...
Privileged Identity Management

Rechercher par nom de ressource

Nom

SAP HANA

Metsys - Always Win @ Casino

Rechercher par nom de ressource pour plus de ressources

Ressources sélectionnées (1)

Metsys - Always Win @ Casino

Appartenance Paramètre

Ressource
Modern Identity

Type de ressource
Annuaire

Sélectionnez un rôle ⓘ
Metsys Application Administrator

Type d'étendue ⓘ
Application

Étendue sélectionnée ⓘ
Metsys - Always Win @ Casino

Sélectionner le(s) membre(s) * ⓘ
Membre(s) de 1 sélectionné

Membre(s) sélectionné(s) ⓘ
Hervé THIBAUT
herve.thibault@modernidentity.onmicrosoft.com



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

Ajouter des attributions ...
Privileged Identity Management | Rôles Azure AD

Appartenance Paramètre

Type d'attribution ⓘ
Éligible

Actif

Durée d'affectation maximum autorisée : 3 mois.

Début de l'affectation *
20/08/2021 14:54:34

Fin de l'affectation *
18/11/2021 13:54:34

Entrer la justification
Ordre du chef !



Azure Active Directory – Identity Governance

Access Review

- 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



Nouvelle révision d'accès

Vous êtes un nouveau dans les révisions d'accès ? Cliquez ici pour [en savoir plus](#).

Type de révision Avis Paramètres Vérifier + créer

Étape 1 : sélectionnez le contenu à réviser

Équipes + groupes

Examiner l'appartenance de l'utilisateur aux équipes + groupes

Applications

Vérifier les affectations d'utilisateurs aux applications

Étape 2 : sélectionnez les applications

Application *

Metsys - Always Win @ Casino

Étape 3 : sélectionnez l'étendue de la révision

Uniquement les utilisateurs invités

Tous les utilisateurs

Type de révision Avis Paramètres Vérifier + créer

Paramètres de saisie semi-automatique

Appliquer automatiquement les résultats à la ressource Activer Désactiver

Si les réviseurs ne répondent pas Suppression de l'accès

(Préversion) À la fin de la révision, envoyer une notification à

Aucune connexion en 30 jours Activer Désactiver

Paramètres avancés

Justification obligatoire Activer Désactiver

Notifications par e-mail Activer Désactiver

Rappels Activer Désactiver

Contenu supplémentaire pour l'e-mail du réviseur

Type de révision Avis Paramètres Vérifier + créer

Specify reviewers

Sélectionner des réviseurs *

Utilisateur(s) ou groupe(s) sélectionné(s)

Utilisateur(s) ou groupe(s) * Hervé THIBAUT et 1 autre

Spécifier la récurrence de la révision

Durée (en jours) * 45

Review recurrence * Semestriel

Date de début * 25/12/2021

Fin

Jamais

Terminer à une date spécifique

Terminer après le nombre d'occurrences

Date de fin 01/06/2024

“Legacy” Identity : Active Directory



“Modern” Identity : Azure Active Directory

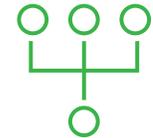


Active Directory vs Azure Active Directory

	Active Directory	Azure AD (premium)
Infrastructure & Authentication	<ul style="list-style-type: none"> • Forêts, domaines, DCs, OUs, GPOs ... • Protocoles : Kerberos, NTLM, ... • Users, groups, applications, Windows Wks & Srv • Pas de solution intégrée de SSO 	<ul style="list-style-type: none"> • 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 ça ! • Pas d'OUs ... Mais voir du côté des Administrative Units pour les aspects délégation • Seamless SSO / Enterprise Applications
Access Management & Identity Governance	<ul style="list-style-type: none"> • Des tonnes de groupes (statiques) pour gérer les accès aux ressources (files/print) • Pas de PIM/ PAM 	<ul style="list-style-type: none"> • Dynamic Groups • Roles / RBAC / Custom Roles • Access Review • Protected Identity Management • Entitlement Management – Access packages & strategies
Identity Protection & Self-Service	<ul style="list-style-type: none"> • Logs AD, réputés pour être explicites et faciles à analyser ☺ • Add-on Microsoft Defender for Identity ou Tenable.ad pour résistance 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) 	<ul style="list-style-type: none"> • 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)





ii IDENTITY DAYS

28 octobre 2021 - PARIS



@IdentityDays #identitydays2021

Merci à tous nos partenaires !



onelogin



yubico

