MFA PASSLESS PIZAZZ

MfaPasslessPizazz est conçu pour simplifier et sécuriser le déploiement et la configuration de votre environnement MFA et/ou Passwordless.
L'outil se veut être un facilitateur, réduisant la complexité inhérente à l'implémentation de ces méthodes d'authentification tout en renforçant leur sécurité.

Dans cette optique, MfaPasslessPizazz se concentre sur trois méthodes d'authentification clés, toutes reconnues pour leur accessibilité, leur fiabilité et leur robustesse en termes de sécurité :

1. **Microsoft Authenticator (en mode mdp + Push)** : Cette application mobile de Microsoft offre un moyen rapide, pratique et sécurisé de vérifier son identité lors de la connexion à un compte ou à une application. La double authentification par mot de passe et notification push assure une sécurité renforcée. L'utilisateur reçoit une notification sur son appareil mobile et n'a qu'à approuver la demande d'authentification. Cela offre un niveau de sécurité élevé, tout en rendant l'authentification rapide et facile pour l'utilisateur.
2. **TAP (Droit d'accès temporaire)** : Les TAP offrent un moyen efficace et flexible de donner un accès temporaire à un utilisateur, ce qui est particulièrement utile lors de la configuration initiale d'un compte ou si l'utilisateur a temporairement perdu l'accès à ses méthodes d'authentification habituelles. Le TAP est conçu pour être utilisé une seule fois et expire après une durée définie, ce qui le rend très sûr.
3. **Clé de sécurité FIDO2** : FIDO2 est une norme d'authentification qui vise à éliminer l'utilisation de mots de passe, augmentant ainsi la sécurité. Les clés de sécurité FIDO2 offrent une méthode d'authentification à deux facteurs hautement sécurisée qui est également résistante au phishing. En plus de cela, elles sont faciles à utiliser et portables, ce qui signifie que les utilisateurs peuvent les emporter partout où ils vont.

Cette sélection permet une authentification multi-facteur flexible, sécurisée et conviviale, ainsi qu'une transition vers une authentification sans mot de passe (Passwordless), respectant à la fois les besoins de l'utilisateur et les exigences de l'industrie en matière de sécurité.

MfaPasslessPizazz propose 4 outils :

Update Tool :
Le centre névralgique d'MfaPasslessPizazz.
Update Tool gère les utilisateurs d'une organisation Microsoft, en les triant en fonction de leur configuration d'authentification. Il utilise des contrôles conditionnels pour dispatcher les utilisateurs dans trois groupes distincts : MFA_NotConfigured, MFA_Authenticator+FIDO2 et MFA_FIDO2_Passwordless. Cette distinction permet une gestion efficace de l'authentification multi-facteur (MFA) et de la configuration "Passwordless" (sans mot de passe).
L'outil permet ainsi une gestion complète pour différentes stratégies d'authentification au sein d'un environnement Microsoft (multi-facteur, sans mot de passe ou le combo multi-facteur+ sans mot de passe)

Reset Tool :
C'est un élément essentiel de MfaPasslessPizazz qui facilite une remise à zéro des configurations d'authentification des utilisateurs au sein d'un environnement Microsoft. L'outil scrute et supprime les méthodes d'authentification assignées à chaque utilisateur spécifié, permettant ainsi une réinitialisation totale de l'authentification, incluant l'authentification par email, FIDO2, Microsoft Authenticator, téléphone, Software Oath et TAP. Suite à la réinitialisation, Reset Tool révoque tous les jetons d'authentification actifs, ce qui impose à l'utilisateur de se reconnecter à toutes ses applications.

Passwordless Tool :
Le Passwordless Tool est un composant de MfaPasslessPizazz qui permet de passer un utilisateur en mode d'authentification sans mot de passe, sous condition que celui-ci ait déjà configuré une clé FIDO2. L'outil retire toutes les autres méthodes d'authentification de l'utilisateur et révoque tous les tokens actifs. Cela oblige une reconnexion via le moyen sans mot de passe uniquement, assurant ainsi une transition sécurisée vers une authentification sans mot de passe.

TAP Management :
L'outil TAP Management (Temporary Access Pass) de MfaPasslessPizazz est un système d'authentification temporaire qui génère des mots de passe à usage unique pour les utilisateurs. Ces mots de passe temporaires peuvent être utilisés lorsque les utilisateurs n'ont pas accès à leur méthode d'authentification habituelle ou lors de la configuration initiale pour les utilisateurs membres de MFA_NotConfigured.
Cet outil offre la possibilité de choisir la durée de validité du mot de passe temporaire, qui peut varier de 10 minutes à 30 jours. Le TAP est généré pour un ou plusieurs utilisateurs spécifiés et les détails sont exportés exclusivement dans un fichier CSV local pour référence.
L'outil permet également de supprimer les TAP existants pour un ou plusieurs utilisateurs. Ceci est utile pour révoquer les accès temporaires s'ils ne sont plus nécessaires.

Comportement et interaction utilisateur en fonction des groupes de sécurité :

Groupe MFA_NotConfigured

Un utilisateur sera automatiquement affecté au groupe MFA_NotConfigured dans les cas suivants :

- L'utilisateur n'a configuré aucune méthode d'authentification.
- L'utilisateur a été traité par l'outil Reset Tool, qui réinitialise les configurations d'authentification.

Si un utilisateur se trouve dans le groupe MFA_NotConfigured sans TAP, lors de sa prochaine connexion, une fenêtre d'information s'affiche avec le message suivant : "Plus d'informations requises : votre organisation a besoin de plus d'informations pour préserver la sécurité du compte". L'utilisateur est alors invité à suivre les étapes suivantes :

- Installer Microsoft Authenticator sur son smartphone.
- Ajouter un compte professionnel à l'aide du QR code qui apparaît à l'écran.
- Valider son inscription et son appareil en acceptant la connexion test.

Dans le cas où l'utilisateur n'aurait pas de smartphone ou si vous souhaitez lui proposer directement une solution Passwordless, vous pouvez générer un TAP à l'utilisateur et lui fournir une clé FIDO2.
Lors de sa prochaine connexion, l'utilisateur sera alors invité à "Entrer le droit d'accès temporaire".
Une fois connecté, l'utilisateur devra ajouter sa clé FIDO2 et/ou Microsoft Authenticator pour compléter son processus d'authentification et ainsi profité d'une solution hybride avec le combo MFA/Passwordless.
Cette approche permet de fournir aux utilisateurs différentes options pour sécuriser leur compte et d'adapter les méthodes d'authentification en fonction de leurs besoins et de leurs équipements *(Procdure_MFA_PASSWORLDESS incluse avec l'outil)*.

Groupe MFA_Authenticator+FIDO2

Si un utilisateur qui était précédemment dans le groupe MFA_NotConfigured a configuré son Microsoft Authenticator ou le combo FIDO2+Microsoft Authenticator, il est automatiquement transféré dans le groupe MFA_Authenticator+FIDO2.

Dans ce groupe, la sécurité est légèrement allégée pour assurer une meilleure expérience utilisateur.
Lorsque l'utilisateur se trouve dans le groupe MFA_Authenticator+FIDO2, il est autorisé à contourner les méthodes d'authentification supplémentaires s'il tente de se connecter depuis des emplacements définis comme "de confiance".
Ces emplacements de confiance sont déterminés par une liste d'adresses IP publiques spécifiées dans les Emplacements nommés.

Cette approche permet à l'utilisateur de bénéficier d'une expérience plus fluide et d'un accès plus rapide aux services et applications, tout en maintenant un niveau de sécurité adéquat.

Groupe MFA_FIDO2_Passwordless
L'utilisateur peut se retrouver dans le groupe MFA_FIDO2_Passwordless dans deux cas de figure :

- Si l'utilisateur est initialement dans le groupe MFA_NotConfigured, qu'un TAP lui a été généré et qu'il n'a ajouté que sa clé FIDO2.
- Si l'utilisateur est initialement dans le groupe MFA_Authenticator+FIDO2 et qu'il passe par l'outil "Passwordless Tool", qui supprime toutes les méthodes d'authentification de l'utilisateur sauf FIDO2.

Dans le groupe MFA_FIDO2_Passwordless, l'utilisateur bénéficie d'une expérience d'authentification sans mot de passe, où seule sa clé de sécurité FIDO2 est requise pour accéder aux services et applications.
Cela simplifie grandement le processus d'authentification tout en maintenant un niveau élevé de sécurité.

Toutefois, il est important de noter que toutes les applications utilisées par l'utilisateur doivent prendre en charge l'authentification sans mot de passe (Passwordless).
Certaines applications spécifiques, telles que certains client VPN utilisant la connexion Radius, peuvent ne pas être compatible Passwordless et nécessiter une méthode d'authentification supplémentaire, telle qu'une notification push.
Il est donc recommandé de vérifier la compatibilité des applications avec l'authentification sans mot de passe avant de basculer vers le groupe MFA_FIDO2_Passwordless.
Cela afin de garantir une expérience d'authentification fluide et sécurisée pour l'utilisateur, en tenant compte des exigences spécifiques de chaque application.

Paramétrage et Prérequis
MfaPasslessPizazz est développé autour de PowerShell, Microsoft Azure et Microsoft Graph.
C'est en combinant Paramètre des Méthodes d'authentification, Stratégies de Méthodes d'authentification, Points forts d'authentification, Détails de l'inscription de l'utilisateur, Stratégies d'Accès conditionnel, Emplacements nommés et Groupes de Sécurité que MfaPasslessPizazz conditionne les actions de ses Scripts.
À ce titre, certaines configurations préalables sont requises.
Pour cela, MfaPasslessPizazz dispose d'un module d'**AutoConf** qui préparera votre environnement en 1 clic ! (La seule et unique interaction attendue sera, si vous le souhaitez, la saisie de votre liste d'@IP Safe).
Enfin, sachez qu'avant de pouvoir exécuter les outils d'MfaPasslessPizazz, En guise de mesure préemptive, il vous faudra **obligatoirement** renseigner une liste d'utilisateur à exclure des différents traitements.

Le Mot de la Fin

MfaPasslessPizazz a été conçu pour simplifier et sécuriser les déploiements d'authentification MFA et Passwordless dans les environnements Azure AD. En réponse à la confusion fréquente entre MFA et Passwordless, ainsi qu'au manque de maîtrise de l'environnement Azure AD qui peut décourager certaines organisations, j'ai voulu rendre l'adoption de ces méthodes d'authentification robustes plus accessible.

L'objectif principal de MfaPasslessPizazz est de faciliter et de renforcer la sécurité des déploiements d'authentification. Pour cela, j'ai pris en compte les défis spécifiques auxquels les administrateurs sont confrontés en fournissant une solution allant de l'autoconfiguration aux procédures d'inscription simplifiées prêtes à être partagées avec les utilisateurs finaux. Vous disposez ainsi d'un ensemble complet d'outils qui simplifient non seulement la configuration technique, mais aussi l'expérience des utilisateurs finaux lors de leur inscription.

De plus, je souhaite que cet outil donne la confiance nécessaire à d'autres administrateurs pour se lancer dans l'aventure de l'authentification Azure AD et de l'API Graph. J'ai pris le temps d'écrire un script propre, aéré et documenté pour aider les administrateurs aventuriers à personnaliser l'outil en fonction de leurs besoins spécifiques.

Amis administrateurs, n'hésitez pas à explorer les possibilités infinies offertes par l'authentification Azure AD et l'API Graph. Avec MfaPasslessPizazz entre vos mains, vous disposez d'un outil puissant pour déployer des méthodes d'authentification robustes et sécurisées dans votre environnement Azure AD.
Je vous souhaite un bon déploiement et que votre aventure d'authentification soit couronnée de succès !