

MFA

ENTRA

Méthode MFA préférée par le système

Méthodes d'authentification | Paramètres

fnccr.asso.fr – Sécurité dans Microsoft Entra ID

Rechercher

Des commentaires ?

Gérer

- Stratégies
- Protection par mot de passe
- Campagne d'inscription
- Points forts d'authentification
- Paramètres**

Supervision

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

Signaler une activité suspecte

Permet aux utilisateurs de signaler des activités suspectes s'ils reçoivent une demande d'authentification qu'ils n'ont pas initiée. Ce contrôle est disponible lors de l'utilisation de l'application Microsoft Authenticator et des appels vocaux. Si vous signalez une activité suspecte, le risque de l'utilisateur est élevé. Si l'utilisateur est soumis à des stratégies d'accès conditionnel basées sur le risque, il est possible qu'il soit bloqué.

En savoir plus

État ^{*} Managé par Microsoft

Cible ^{*} Tous les utilisateurs

☐ Sélectionner un groupe

Code de rapport ^{*} 0

Authentification multifactorielle préférée par le système

Ce paramètre indique si la méthode d'authentification multifactorielle la plus sécurisée est présentée aux utilisateurs. En savoir plus

Remarque : si l'état de la fonctionnalité est défini sur Géré par Microsoft, elle sera activée par Microsoft à un moment approprié. En savoir plus

État ^{*} Désactivé

Dans vue d'ensemble

Identity Governance | Vue d'ensemble | External Identities | Paramètres de collaboration externe | External Identities | Vue d'ensemble | Sécurité | Méthodes d'authentification

fnccr.asso.fr

+ Ajouter ^{*} Gérer les locataires Nouveautés Fonctionnalités de la version préliminaire Des commentaires ?

Azure Active Directory s'appelle désormais Microsoft Entra ID. En savoir plus

Vue d'ensemble Supervision **Propriétés** Recommandations Tutoriels

Localisation des données EU Model Clause compliant datacenters

Langue de notification français

ID du client be1af5ba-04f4-436f-9fa2-23b0ac1bda727

Contact technique informatique@fnccr.asso.fr

Contact international chargé de la confiden...

URL de la déclaration de confidentialité

Gestion de l'accès pour les ressources Azure

(user_de2179ced0ae4869d3c5e624d90f10c@scriba.onmicrosoft.com) peut gérer l'accès à tous les abonnements Azure et à tous les groupes d'administration de ce client.

En savoir plus

☐ Non

Paramètres de sécurité par défaut

Les paramètres de sécurité par défaut constituent sont des mécanismes de base de sécurité de l'identité recommandés par Microsoft. Quand cette option est activée, ces recommandations sont automatiquement appliquées à tous les utilisateurs de votre organisation.

En savoir plus

⚠ Votre organisation n'est pas protégée par les paramètres de sécurité par défaut. [Gérer les paramètres de sécurité par défaut](#)

Paramètres de sécurité par défaut

Désactivé (non recommandé)

Si les paramètres de sécurité par défaut sont désactivés, votre organisation est vulnérable aux attaques courantes liées aux identités.

Vous pouvez réduire 99,9 % de compromission de compte à l'aide de l'authentification multifactorielle qui est une fonctionnalité fournie par les paramètres de sécurité par défaut.

Les équipes de sécurité de Microsoft voient une baisse du taux de compromission de 80 % lorsque les paramètres de sécurité par défaut sont activés.

Enregistrer Annuler

https://entra.microsoft.com/#blade/Microsoft_AAD_ConditionalAccess/SecurityDefault1ref

Mail type pour explication :

Bonjour Laura,

Ce mail fait suite à ma tentative infructueuse de contact.

Microsoft vous a adressé cette notification, car Microsoft va déployer sur votre tenant, des presets de sécurité par défaut pour améliorer la sécurité des comptes de votre organisation.

Ces presets vont occasionner :

- La désactivation des protocoles de connexion non sécurisés
- L'obligation, pour vos utilisateurs, de valider leurs connexions aux services 365 avec une méthode supplémentaire d'authentification. (MFA : Multi Facteur Authentification)

Pour valider leur identité lors de leurs connexions, vos utilisateurs pourront valider une notification sur une application à installer sur le mobile (Microsoft Authenticator, disponible gratuitement sur IOS et Android) ou entrer un code de sécurité qu'ils auront reçu par SMS.

Ces prochains jours, vos collaborateurs seront invités à configurer cette méthode MFA en se connectant en web sur <https://office.com>

A l'issue de la campagne d'inscription, toute connexion n'utilisant pas le MFA sera bloquée.

Actuellement, 58 utilisateurs sur 153 au total sont déjà prêts pour utiliser le MFA, leurs méthodes sont déjà configurées activées. Je vous invite à demander à vos collaborateurs de se connecter sur [Office.com](https://office.com) pour vérifier que tout est en ordre.

Quelles sont vos disponibilités pour échanger sur ce sujet ?

Vous pouvez me recontacter au 05 57 92 87 99 et en répondant à ce mail.

Dans l'attente de votre retour, je vous souhaite une excellente journée.

Par suite des réceptions de mails frauduleux et tentatives d'intrusions sur vos comptes Microsoft, il est impératif que seuls vos collaborateurs puissent accéder aux données 365 de votre entreprise.

L'authentification multi-facteurs, ou authentification forte, est principalement réputée pour constituer une défense supplémentaire et rendre plus difficile l'accès d'une personne non autorisée à un réseau ou à une base de données. La mise en place d'une solution MFA robuste permet de sécuriser instantanément les données et les ressources informatiques contre le vol d'identité, l'usurpation de compte et le phishing.

Les entreprises recourent donc au MFA pour contrôler l'accès à leurs systèmes et solutions informatiques internes.

Selon Microsoft, le MFA bloque plus de 99,9 % des attaques de compromission de compte. Vous entendrez souvent dire que le MFA est une composante essentielle de la sécurité. En effet, alors qu'il est relativement facile d'obtenir les informations d'identification d'un utilisateur par des attaques telles que le phishing ou credential stuffing, l'authentification forte multi-facteurs rend

quasiment impossible pour les hackers d'obtenir le second facteur d'authentification

L'authentification multifacteur (MFA) ajoute une couche de protection au processus de connexion. Pour accéder à leurs comptes ou à des applications, les utilisateurs doivent confirmer leur identité, par exemple en scannant leur empreinte ou en entrant un code reçu par téléphone. Elle ne demande pas de modifications sur les licences actuelles, pour les méthodes de base.

Nous pouvons configurer / activer le MFA (Authentification Multi Factorielle) sur vos comptes et faire en sorte qu'une connexion inhabituelle demande la saisie d'un code reçu par SMS par exemple.

<https://support.microsoft.com/fr-fr/office/configurer-votre-connexion-microsoft-365-pour-l-authentification-multifacteur-ace1d096-61e5-449b-a875-58eb3d74de14>

Vos utilisateurs peuvent dès à présent se connecter sur le portail Web <https://aka.ms/mfasetup>

Et configurer par eux-mêmes la méthode de confirmation qu'ils souhaitent. Nous pouvons également le faire à leur place, si nous disposons des numéros de mobile.

Les Méthodes disponibles :

- Utilisation du numéro de mobile pour recevoir par SMS un code à usage unique
- Installation de l'application Authenticator, disponible gratuitement sur Google Play Store ou Apple IOS Store , qui, une fois liée au compte 365, permettra de valider ou non une connexion au compte Microsoft 365. Cette Méthode permet de ne pas communiquer son numéro de mobile à Microsoft.
- Clé de sécurité FIDO2
- Windows Hello Entreprise

Une fois ce système configuré et activé, les services Microsoft demanderont de confirmer à la première connexion l'identité de l'utilisateur. Cette confirmation est à renouveler tous les 90 jours par défaut.

Je me tiens à votre disposition au 05 57 92 87 99 et en réponse à ce mail.

Dans l'attente de votre retour, je vous souhaite une excellente journée.

On peut mettre en place la MFA pour chaque connexion ou à la première connexion (définir la durée pendant laquelle la confiance est accordée).

On peut mettre en place des stratégies d'accès conditionnel

Il faut des business premium pour bénéficier d'INTUNE

On peut mettre une notification lorsque des mails viennent de l'extérieur alors qu'ils ne devraient pas (en Shell)

[Office 365 - Ajouter un préfixe à l'objet et un disclaimer aux e-mails externes | IT-Connect](#)

[How To Warn users for Email Impersonation Phishing mail — LazyAdmin](#)

[Microsoft Authenticator App Not Working: 15 Tips to Fix It](#)

Revision #1

Created 25 November 2024 12:50:34 by Johann

Updated 25 November 2024 12:51:33 by Johann