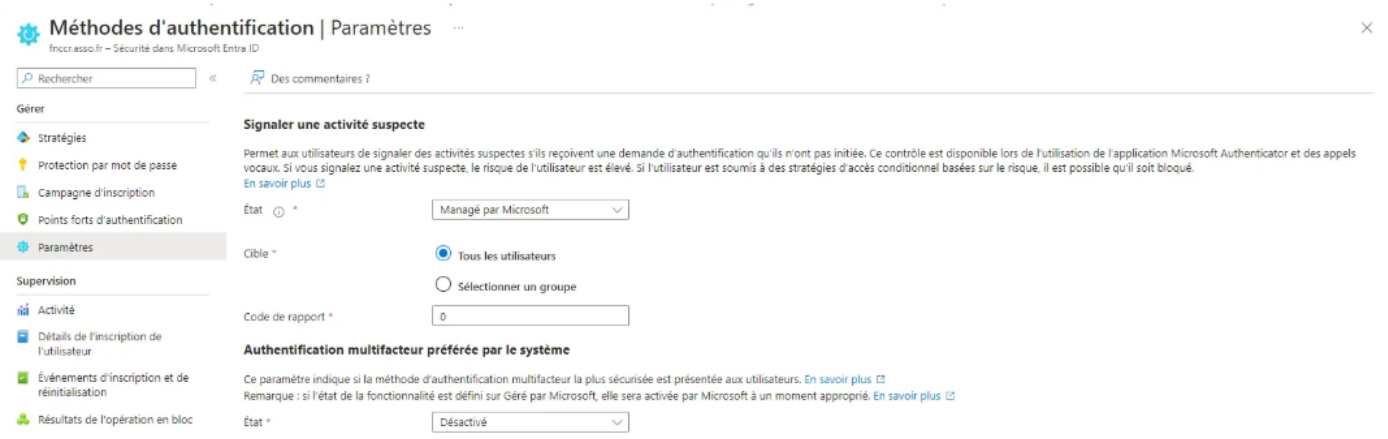
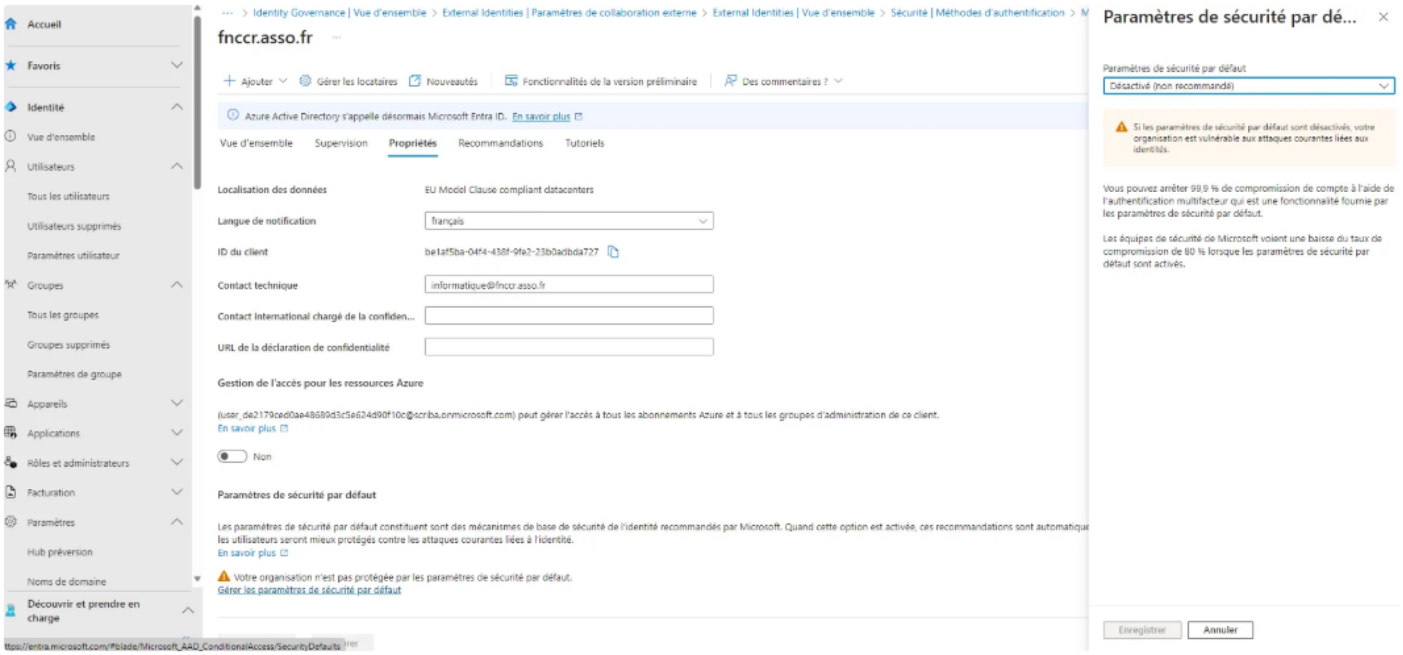
MFA

ENTRA

Méthode MFA préférée par le système



Dans vue d’ensemble



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 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