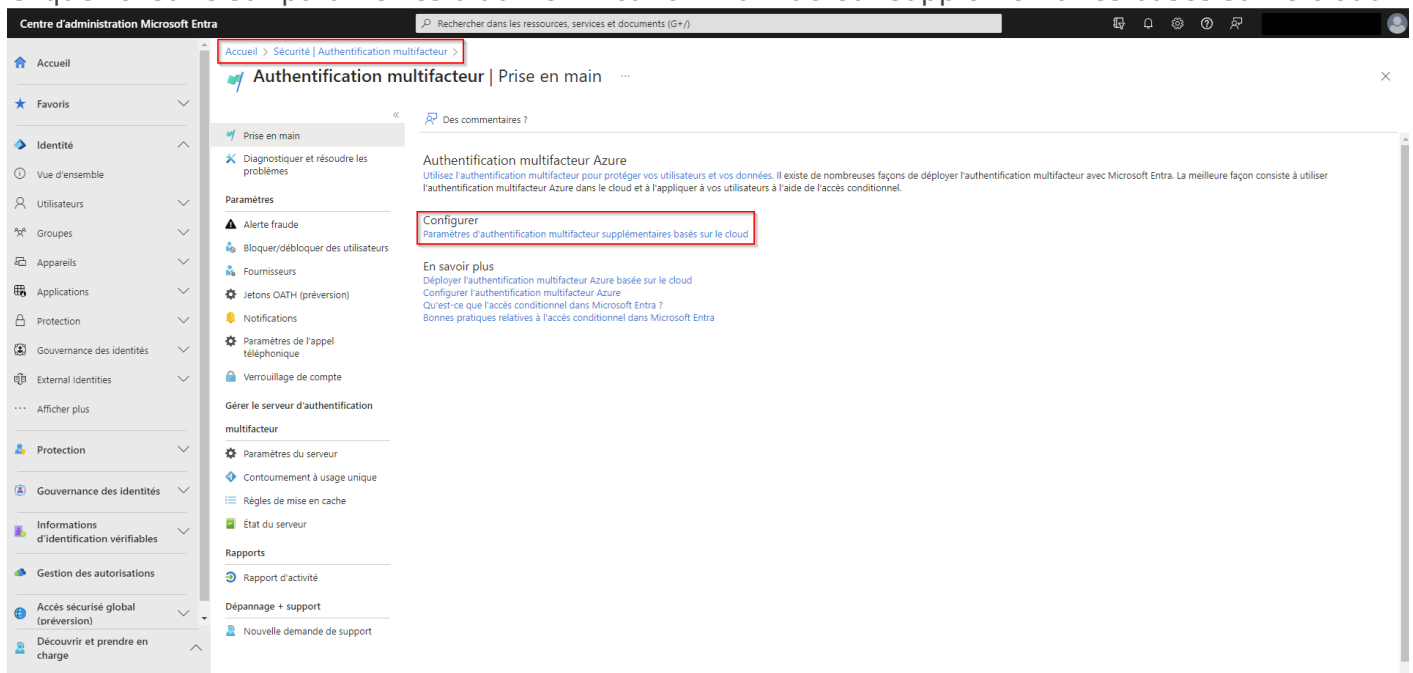


MFA - Désactivation application Authenticator

Microsoft force actuellement les utilisateurs à enregistrer l'application Authenticator comme méthode d'authentification via des campagnes.

Voici les étapes à suivre pour désactiver (temporairement) cette méthode :

Se connecter sur Azure et accéder à la page Accueil > Sécurité | Authentification multifacteur. Cliquer ensuite sur paramètres d'authentification multifacteur supplémentaires basés sur le cloud.



Sur la page qui s'ouvre, décocher la "Notification via l'application mobile" et valider en enregistrant

:

authentification multifacteur

utilisateurs paramètres du service

mots de passe d'application [\(en savoir plus\)](#)

- ☒ Autoriser les utilisateurs à créer des mots de passe d'application pour se connecter à des applications sans navigateur
- ☐ Ne pas autoriser les utilisateurs à créer des mots de passe d'application pour se connecter à des applications sans navigateur

adresses ip de confiance [\(en savoir plus\)](#)

- ☐ Ignorer l'authentification multifacteur pour les demandes issues d'utilisateurs fédérés provenant de mon intranet

Ignorer l'authentification multifacteur pour les demandes provenant d'une plage spécifique d'adresses IP

192.168.1.0/27
192.168.1.0/27
192.168.1.0/27

Input trusted IP list

options de vérification [\(en savoir plus\)](#)

Méthodes disponibles pour les utilisateurs :

- ☒ Appel téléphonique
- ☒ SMS par téléphone
- ☐ Notification via application mobile
- ☒ Code de vérification à partir de l'application mobile ou du jeton matériel

mémoriser multi-factor authentication sur un appareil approuvé [\(en savoir plus\)](#)

- ☐ Permettre aux utilisateurs de mémoriser l'authentification multifacteur sur les appareils auxquels ils font confiance (de 1 à 365 jours)

Nombre de jours pendant lesquels les utilisateurs peuvent faire confiance aux appareils

REMARQUE : pour une expérience utilisateur optimale, nous vous recommandons d'utiliser la fréquence de connexion Accès conditionnel pour étendre les durées de vie des sessions sur les appareils, les emplacements de confiance ou les sessions à faible risque en tant qu'alternative à l'utilisation des paramètres 'Mémoriser MFA sur un appareil de confiance'. Si vous utilisez 'Mémoriser MFA sur un appareil de confiance', assurez-vous d'étendre la durée à 90 jours ou plus. [En savoir plus sur les invites de réauthentification.](#)

enregistrer

Ensuite, se rendre sur la page "Accueil > Méthodes d'authentification" puis cliquer sur "Campagne d'inscription" et modifier.

Changer l'état sur "Désactivée" puis valider.

Centre d'administration Microsoft Entra

Rechercher dans les ressources, services et documents (G+)

Accueil

Favoris

Identité

Vue d'ensemble

Utilisateurs

Groupes

Appareils

Applications

Rôles et administrateurs

Facturation

Paramètres

Protection

Gouvernance des identités

External identities

Expériences utilisateur

Gestion hybride

Surveillance et intégrité

Afficher moins

Accueil > Méthodes d'authentification

Méthodes d'authentification | Campagne d'inscription

COMEXPOSIUM - 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

Paramètres

Modifier

Ignorer

État

Désactivée

Nombre de jours autorisés pour la répétition

1 jour

Nombre limité de répétitions

Activé

Utilisateurs et groupes exclus

Aucun élément sélectionné

Ajouter des utilisateurs et des groupes

Méthode d'authentification

Méthode

Utilisateurs et groupes inclus

Microsoft Authenticator

Tous les utilisateurs

Revision #2

Created 31 October 2024 17:21:43 by Cavallone

Updated 31 October 2024 17:23:57 by Cavallone