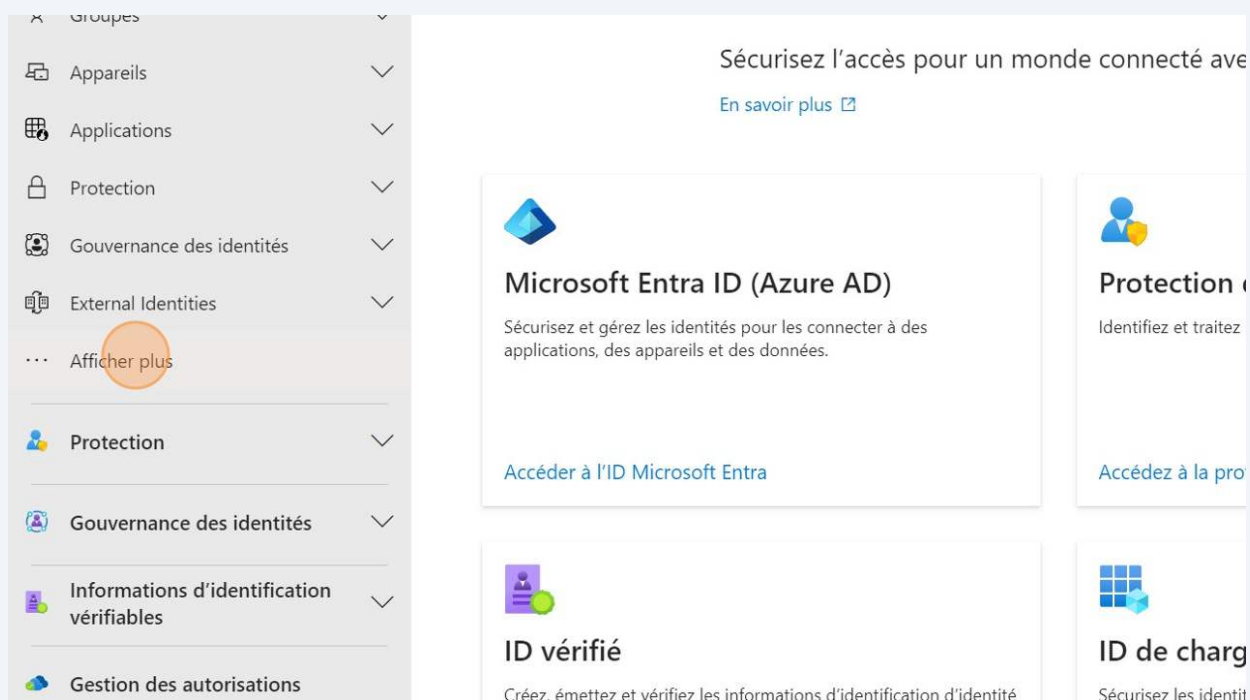


Définir l'authentification multifactorielle avec l'accès conditionnel (M365 A3+)

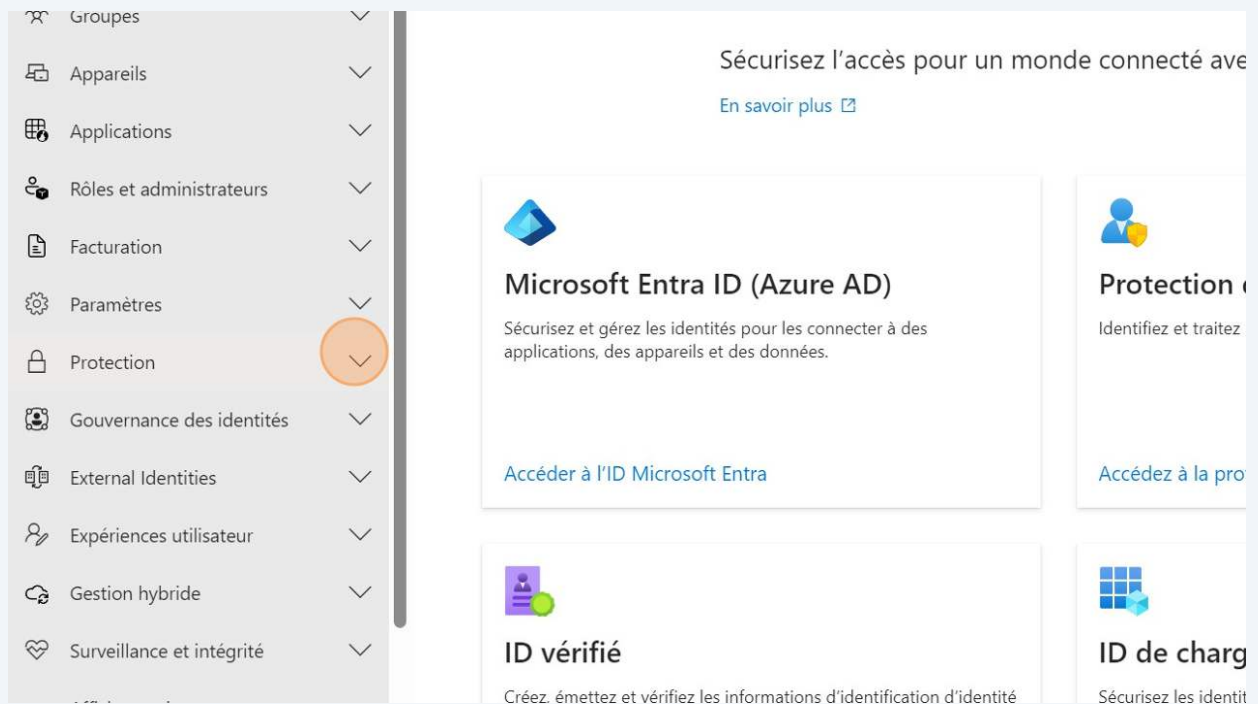
Ce guide contient des instructions pas à pas pour configurer l'authentification multifactorielle avec l'accès conditionnel. Nous utilisons la nouvelle interface Méthode d'authentification ainsi que l'accès conditionnel. De nombreux autres paramètres sont possibles, mais nous nous limitons dans ce guide à l'essentiel pour activer cette politique pour les enseignants.

1 Naviguez vers <http://entra.microsoft.com/>

Dans la barre de menu grise, cliquez sur "Afficher plus"

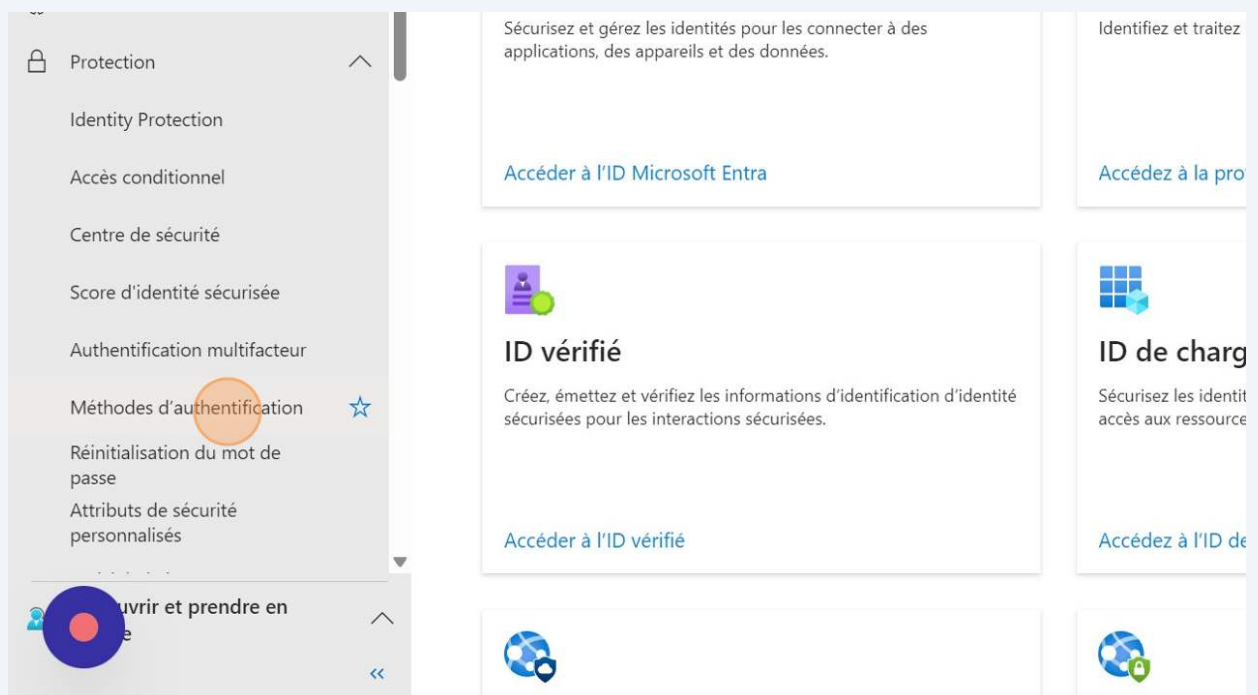


2 Ouvrir le menu "Protection"



The screenshot shows the Microsoft Entra ID dashboard. On the left, a sidebar contains a list of navigation items: Groupes, Appareils, Applications, Rôles et administrateurs, Facturation, Paramètres, Protection (highlighted with an orange circle), Gouvernance des identités, External Identities, Expériences utilisateur, Gestion hybride, and Surveillance et intégrité. The main content area displays a header with the text 'Sécurisez l'accès pour un monde connecté avec' and a link 'En savoir plus'. Below the header, there are four tiles: 'Microsoft Entra ID (Azure AD)' with a description and a link to 'Accéder à l'ID Microsoft Entra'; 'Protection' with a description and a link to 'Accédez à la pro'; 'ID vérifié' with a description and a link to 'Accéder à l'ID vérifié'; and 'ID de charg' with a description and a link to 'Accédez à l'ID de'.

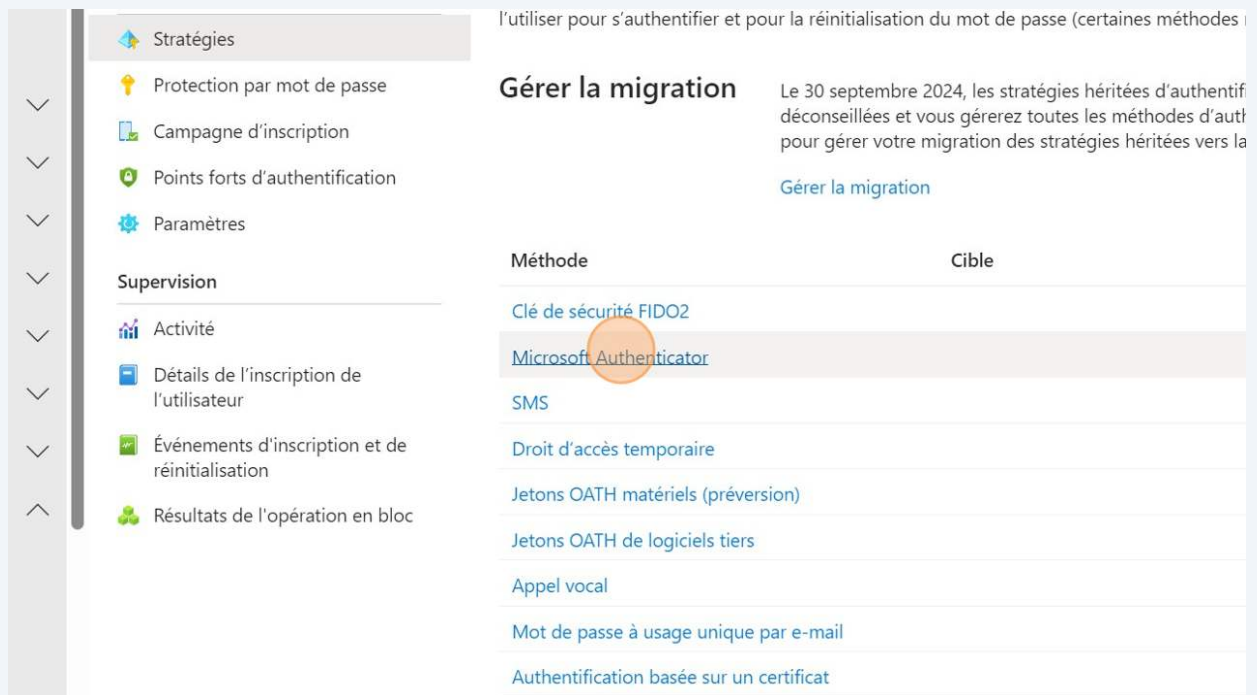
3 Cliquez sur "Méthodes de vérification" pour activer les méthodes de vérification.



The screenshot shows the Microsoft Entra ID 'Protection' menu. The left sidebar is expanded, showing a list of sub-items: Identity Protection, Accès conditionnel, Centre de sécurité, Score d'identité sécurisée, Authentification multifacteur, Méthodes d'authentification (highlighted with an orange circle and a blue star), Réinitialisation du mot de passe, and Attributs de sécurité personnalisés. The main content area displays a header with the text 'Sécurisez et gérez les identités pour les connecter à des applications, des appareils et des données.' and a link 'Accéder à l'ID Microsoft Entra'. Below the header, there are four tiles: 'Microsoft Entra ID (Azure AD)' with a description and a link to 'Accéder à l'ID Microsoft Entra'; 'Protection' with a description and a link to 'Accédez à la pro'; 'ID vérifié' with a description and a link to 'Accéder à l'ID vérifié'; and 'ID de charg' with a description and a link to 'Accédez à l'ID de'.

4

Cliquez sur la méthode d'authentification (par exemple Microsoft Authenticator) pour l'activer.



l'utiliser pour s'authentifier et pour la réinitialisation du mot de passe (certaines méthodes)

Gérer la migration

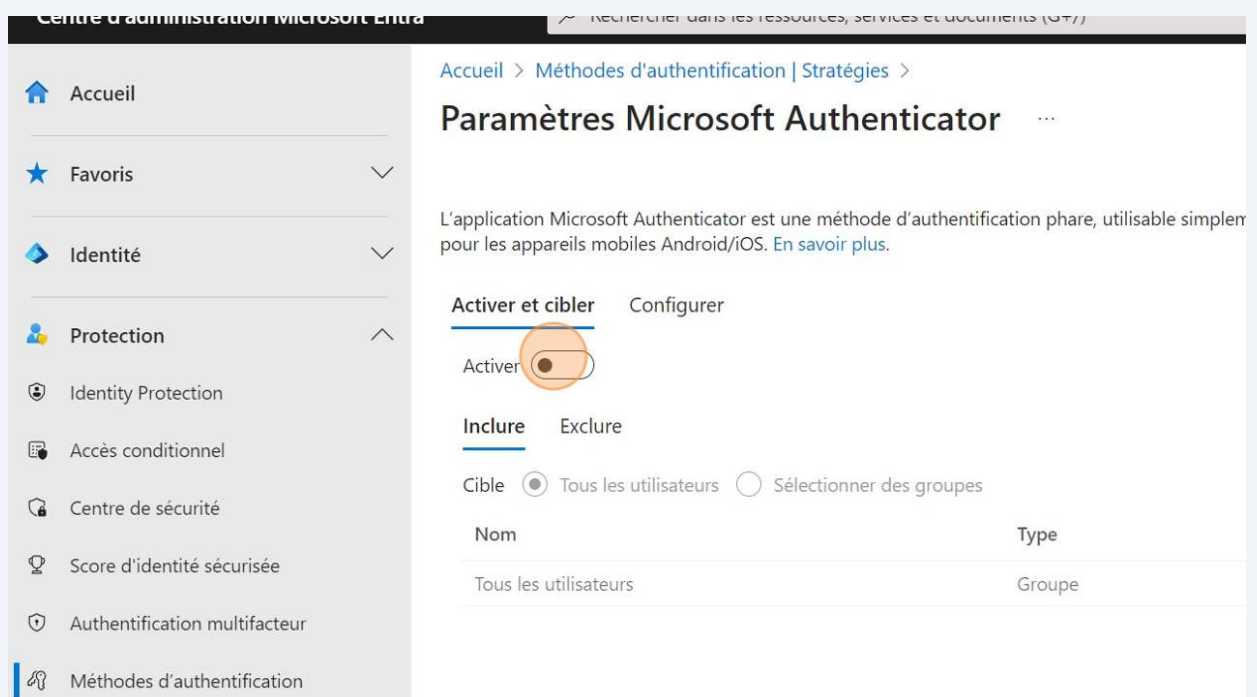
Le 30 septembre 2024, les stratégies héritées d'authentification déconseillées et vous gérerez toutes les méthodes d'authentification pour gérer votre migration des stratégies héritées vers la

[Gérer la migration](#)

Méthode	Cible
Clé de sécurité FIDO2	
Microsoft Authenticator	
SMS	
Droit d'accès temporaire	
Jetons OATH matériels (préversion)	
Jetons OATH de logiciels tiers	
Appel vocal	
Mot de passe à usage unique par e-mail	
Authentification basée sur un certificat	

5

Activez la méthode et choisissez le groupe d'utilisateurs qui peut l'utiliser.



Centre d'administration Microsoft Entra

Accueil > Méthodes d'authentification | Stratégies >

Paramètres Microsoft Authenticator

L'application Microsoft Authenticator est une méthode d'authentification phare, utilisable simplement pour les appareils mobiles Android/iOS. [En savoir plus.](#)

Activer et cibler Configurer

Activer ☒

Inclure Exclure

Cible ☒ Tous les utilisateurs ☐ Sélectionner des groupes

Nom	Type
Tous les utilisateurs	Groupe

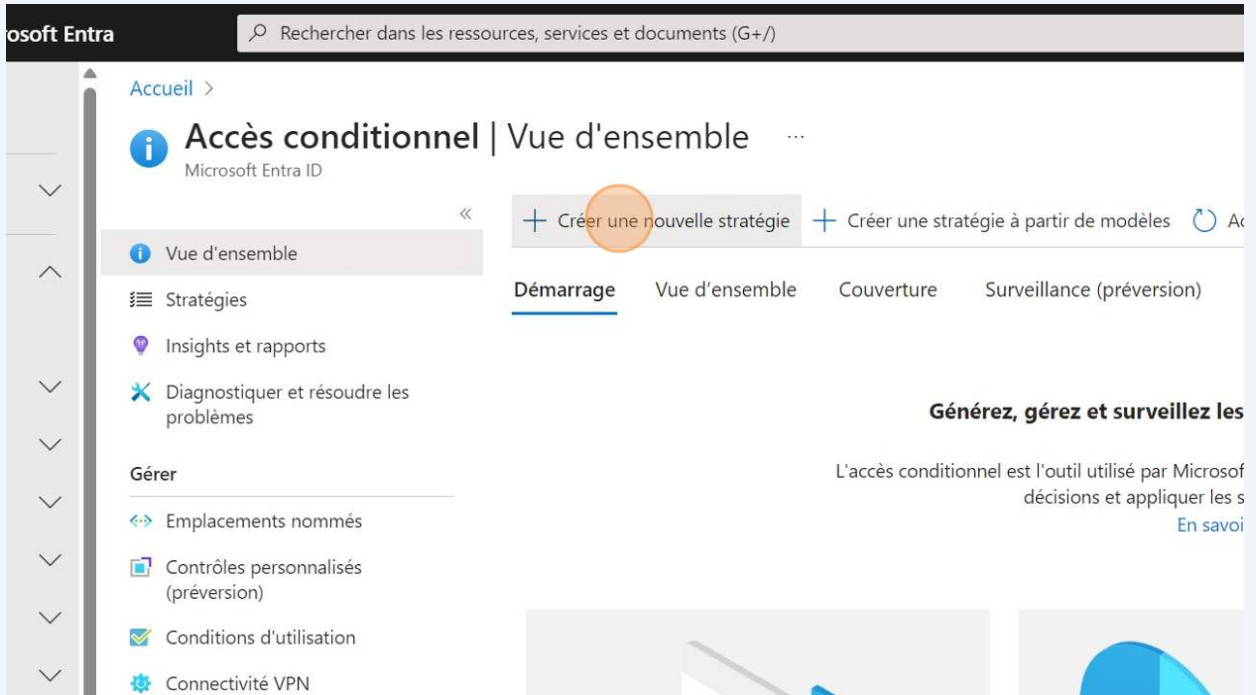
6 Confirmez cette configuration en cliquant sur "Enregistrer"

The screenshot shows the Microsoft Entra ID configuration page. On the left, there is a grey sidebar menu with the following items: Réinitialisation du mot de passe, Attributs de sécurité personnalisés, Activités à risque, Afficher moins, Gouvernance des identités, Informations d'identification vérifiables, Gestion des autorisations, Accès sécurisé global (préversion), and Ouvrir et prendre en charge. The 'Enregistrer' button is highlighted with an orange circle. The 'Ignorer' button is also visible.

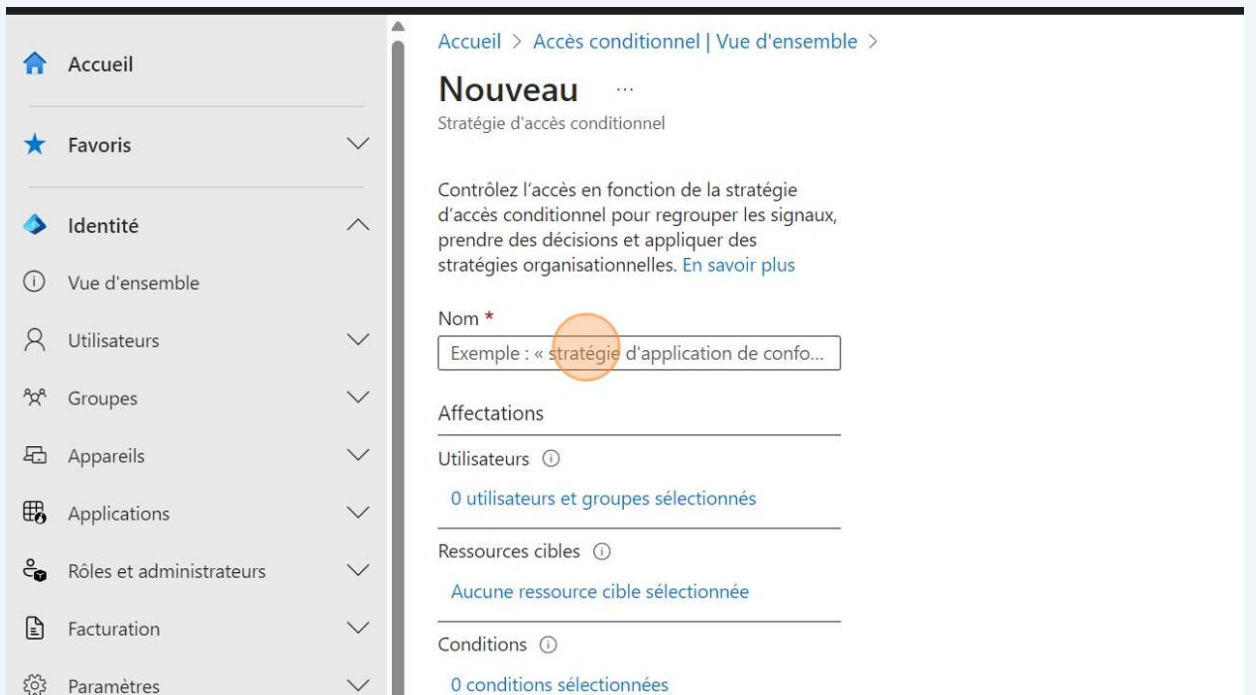
7 Dans le menu gris, sous Protection, cliquez sur "Accès conditionnel"

The screenshot shows the Microsoft Entra ID configuration page. On the left, there is a grey sidebar menu with the following items: Applications, Rôles et administrateurs, Facturation, Paramètres, Protection, Identity Protection, Accès conditionnel, Centre de sécurité, Score d'identité sécurisée, Authentification multifacteur, Méthodes d'authentification, Réinitialisation du mot de passe, and Attributs de sécurité. The 'Accès conditionnel' option is highlighted with an orange circle. On the right, there is a 'Supervision' section with the following items: Clé de sécurité FIDO2, Microsoft Authenticator, SMS, Droit d'accès temporaire, Jetons OATH matériels (préversion), Jetons OATH de logiciels tiers, Appel vocal, Mot de passe à usage unique par e-mail, and Authentification basée sur un certificat.

8



9



10

Cliquez sur le texte bleu sous utilisateurs pour choisir le groupe d'utilisateurs auquel cette politique sera appliquée.

Contrôlez l'accès en fonction de la stratégie d'accès conditionnel pour regrouper les signaux, prendre des décisions et appliquer des stratégies organisationnelles. [En savoir plus](#)

Nom *

MFA Enseignants ✓

Affectations

Utilisateurs ⓘ

0 utilisateurs et groupes sélectionnés

Ressources cibles ⓘ

Aucune ressource cible sélectionnée

Conditions ⓘ

0 conditions sélectionnées

Contrôles d'accès

Octroyer ⓘ

11

Vous pouvez "inclure" des groupes mais aussi exclure des utilisateurs au sein de ces groupes via "exclure". Cela vous permet d'exempter temporairement un groupe d'utilisateurs de cette politique en cas de problème.

Contrôlez l'accès en fonction de la stratégie d'accès conditionnel pour regrouper les signaux, prendre des décisions et appliquer des stratégies organisationnelles. [En savoir plus](#)

Nom *

MFA Enseignants ✓

Affectations

Utilisateurs ⓘ

0 utilisateurs et groupes sélectionnés

Ressources cibles ⓘ

Aucune ressource cible sélectionnée

Conditions ⓘ

0 conditions sélectionnées

Contrôles d'accès

Octroyer ⓘ

Contrôlez l'accès en fonction des personnes auxquelles la stratégie s'applique, telles que des utilisateurs et des groupes, des identités de charge de travail, des rôles d'annuaire ou des invités externes. [En savoir plus](#)

Inclure Exclure

☒ Aucun

☐ Tous les utilisateurs

☐ Sélectionner des utilisateurs et des groupes

12 Sous "Ressources cibles", sélectionnez "Toutes les applications cloud".

Contrôlez l'accès en fonction de la stratégie d'accès conditionnel pour regrouper les signaux, prendre des décisions et appliquer des stratégies organisationnelles. [En savoir plus](#)

Nom *

MFA Enseignants ✓

Affectations

Utilisateurs ⓘ

[Utilisateurs spécifiques inclus](#)

Ressources cibles ⓘ

Aucune ressource cible sélectionnée

Conditions ⓘ

0 conditions sélectionnées

Contrôles d'accès

Octroyer ⓘ

Contrôlez l'accès en fonction du trafic d'accès réseau, des applications cloud ou des actions spécifiques. [En savoir plus](#)

Sélectionner ce à quoi cette stratégie s'applique

Applications cloud ▼

Inclure Exclure

☒ Aucun

☒ Toutes les applications cloud

☐ Sélectionner les applications

13 Cliquez sur le texte bleu sous " Octroyer ".

Applications ▼

Rôles et administrateurs ▼

Facturation ▼

Paramètres ▼

Protection ▲

Identity Protection

Accès conditionnel

Centre de sécurité

Score d'identité sécurisée

Authentification multifacteur

Méthodes d'authentification

Réinitialisation du mot de passe

[Utilisateurs spécifiques inclus](#)

Ressources cibles ⓘ

[Toutes les applications cloud](#)

Conditions ⓘ

0 conditions sélectionnées

Contrôles d'accès

Octroyer ⓘ

0 contrôles sélectionnés

Session ⓘ

0 contrôles sélectionnés

☐ Sélectionner les applications

⚠ Ne bloquez pas votre accès ! Cette stratégie a un impact sur le portail Azure. Avant de continuer, assurez-vous que vous ou quelqu'un d'autre sera en mesure de revenir au portail. Ignorez cet avertissement si vous configurez une stratégie de session de navigateur persistante qui ne fonctionne correctement que si l'option « Toutes les applications cloud » est sélectionnée. [En savoir plus](#)

14

Choisissez d'"accorder l'accès" mais en exigeant une "authentification multifacteur".

Vous pouvez également laisser l'intelligence artificielle de Microsoft déterminer cela elle-même en utilisant des modèles avancés via " Exiger la force d'authentification ".

Octroyer

Contrôlez l'application de l'accès pour bloquer ou accorder l'accès. [En savoir plus](#)

☐ Bloquer l'accès
☒ **Accorder l'accès**

☐ Exiger une authentification multifacteur ⓘ
☐ Exiger la force de l'authentification ⓘ
☐ Exiger que l'appareil soit marqué comme conforme ⓘ
☐ Exiger un appareil avec jointure Microsoft Entra hybride ⓘ
☐ Demander une application cliente approuvée ⓘ

15

Activez la stratégie et confirmez en cliquant sur "Créer".

Contrôles d'accès

Octroyer ⓘ

1 contrôle sélectionné

Session ⓘ

0 contrôles sélectionnés

Activer une stratégie

Rapport uniquement Activé Désactivé

Créer