

Procédure d'inscription à l'expérience combinée

Qu'est-ce que l'authentification multifacteur?

L'authentification multifacteur est un mécanisme dans lequel l'utilisateur est invité pendant le processus de connexion à suivre une forme d'identification supplémentaire, consistant par exemple à entrer un code sur son téléphone portable ou à scanner son empreinte digitale.

L'utilisation d'un mot de passe uniquement ne protège pas complètement des attaques. Si le mot de passe est faible ou s'il a été exposé ailleurs, est-ce vraiment l'utilisateur qui se connecte avec le nom d'utilisateur et le mot de passe, ou s'agit-il d'un attaquant ? Avec une deuxième forme d'authentification, la sécurité est accrue, car ce facteur supplémentaire n'est pas un élément facile à obtenir ou à dupliquer par un attaquant.

L'authentification multifacteur Azure AD impose au minimum deux des méthodes d'authentification suivantes :

- Un élément que vous connaissez, généralement un mot de passe
- Un élément que vous possédez, tel qu'un appareil de confiance qui n'est pas facilement dupliqué, comme un téléphone.
- Un élément biométrique identifiant votre personne, telle qu'une empreinte digitale ou une numérisation du visage.

Qu'est-ce que la réinitialisation de mot de passe en libre-service?

La réinitialisation de mot de passe en libre-service (SSPR) donne aux utilisateurs la possibilité de modifier ou de réinitialiser leur mot de passe, sans implication de l'administrateur ou du service d'assistance. Si le compte d'un utilisateur est verrouillé ou s'il oublie son mot de passe, il peut suivre les invites pour se débloquer et reprendre le travail.

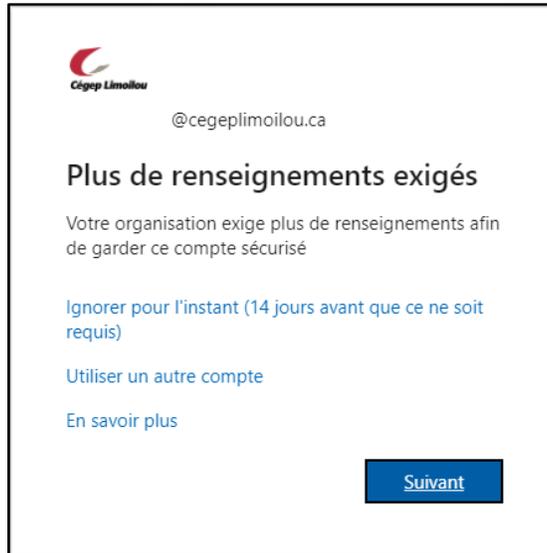
Qu'est-ce que l'inscription combinée?

Avant, les utilisateurs devaient s'inscrire séparément aux méthodes d'authentification multifacteur (MFA) et Réinitialisation de mot de passe en libre-service (SSPR). Désormais, grâce à l'inscription combinée, les utilisateurs n'ont plus besoin de s'inscrire deux fois pour bénéficier des avantages de l'authentification multifacteur et de la réinitialisation SSPR.

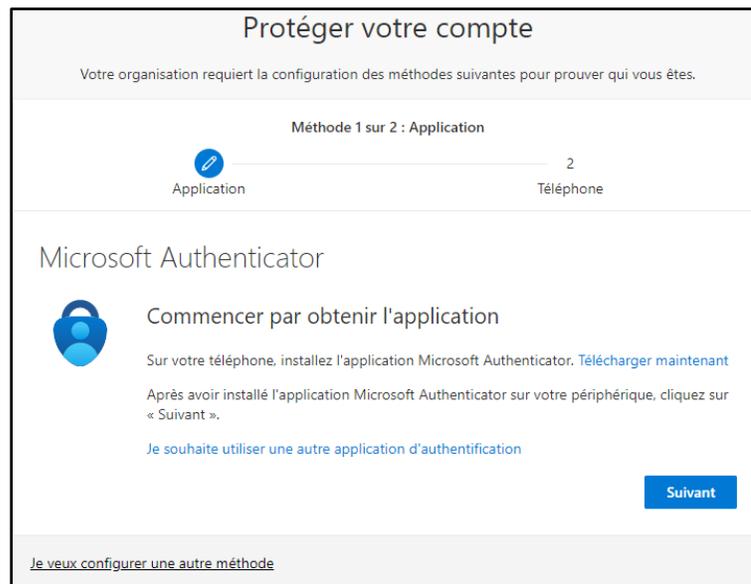
Comment activer l'expérience combinée?

L'expérience combinée vous sera proposée dès l'ouverture de votre session ou à l'utilisation d'Office 365. Voici la configuration recommandée par la DSTI :

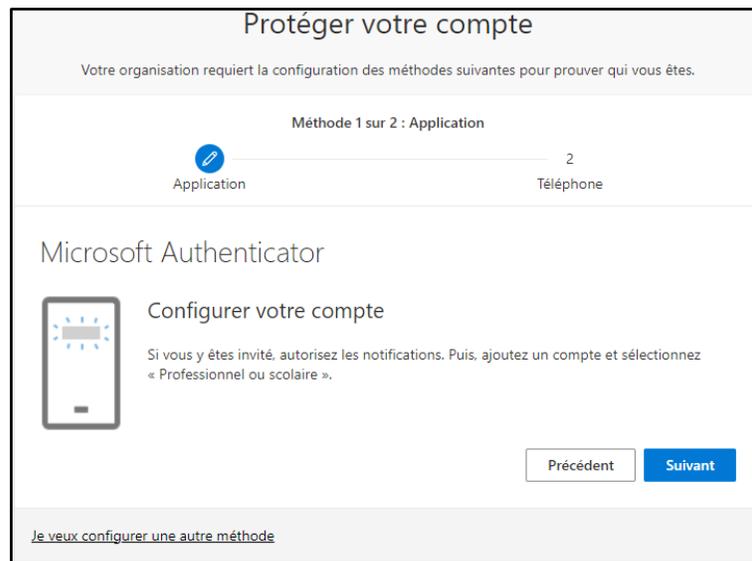
1. Depuis un ordinateur, allez sur <http://www.cegeplimoilou.ca/office> et connectez-vous avec votre compte du cégep
2. Vous aurez la question « **Plus de renseignements exigés** », cliquez sur « **Suivant** » :



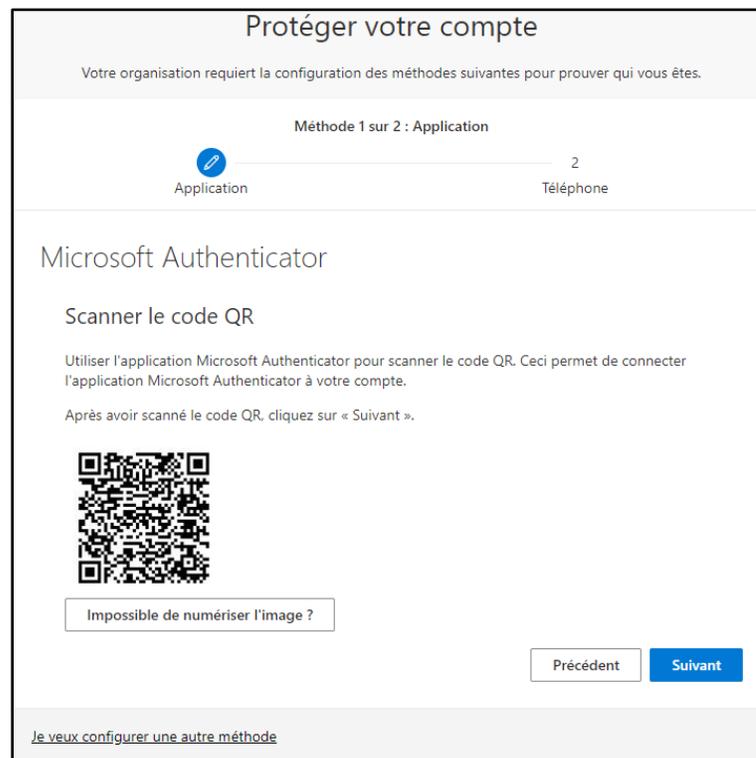
3. Vous devrez télécharger l'application Microsoft Authenticator sur votre téléphone/tablette.
Si vous ne souhaitez pas utiliser l'application, vous pouvez sélectionner : « **Je veux configurer une autre méthode. »



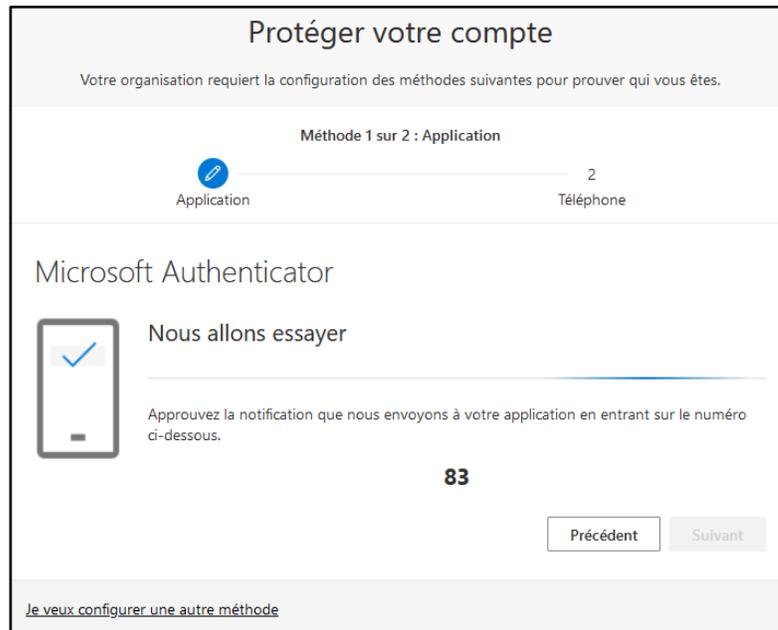
4. Faire « Suivant »



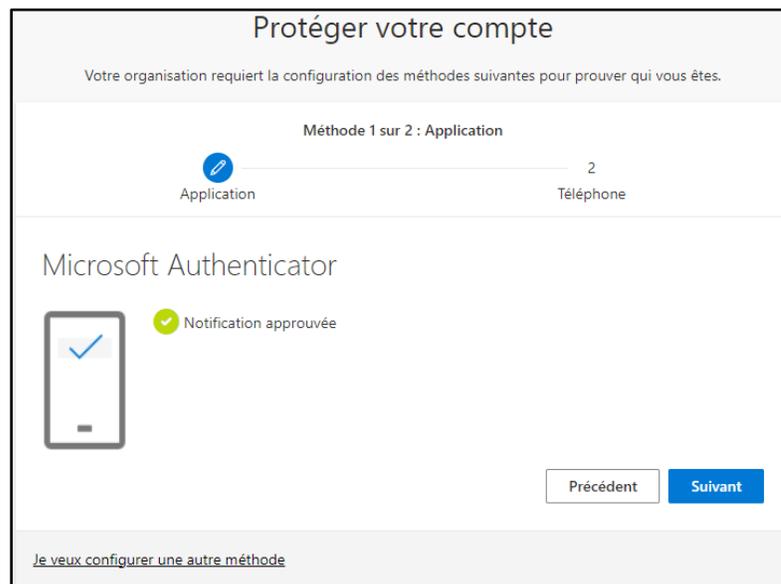
5. Ouvrir l'application mobile Microsoft Authenticator sur votre téléphone/tablette. Ajouter un compte « professionnel ou scolaire » et scanner le Code QR affiché à l'écran de votre ordinateur.



6. Sur votre téléphone/tablette, entrez le numéro indiqué et cliquez « Oui ».



7. Faire « Suivant ».



8. Vous devez choisir votre pays et entrer votre numéro de cellulaire. Un SMS avec un code vous sera envoyé.

****Si vous n'avez pas de téléphone, vous pouvez faire : « Je veux configurer une autre méthode. »**

The screenshot shows a web interface titled "Protéger votre compte". At the top, it says "Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes." Below this, a progress bar indicates "Méthode 2 sur 2 : Téléphone". The "Application" step is marked with a green checkmark, and the "Téléphone" step is marked with a blue pencil icon. The main content area is titled "Téléphone" and contains the text: "Vous pouvez prouver qui vous êtes en envoyant un code par SMS à votre téléphone." Below this is the question "Quel numéro de téléphone voulez-vous utiliser ?". There is a dropdown menu showing "United States (+1)" and an input field labeled "Entrez un numéro de téléphone". A radio button is selected for "M'envoyer un code par SMS". Below this, there is a disclaimer: "Des frais relatifs aux messages et aux données peuvent s'appliquer. Si vous choisissez Suivant, cela signifie que vous acceptez Conditions d'utilisation du service et Déclaration sur la confidentialité et les cookies." A "Suivant" button is visible at the bottom right. At the bottom left, there is a link: "Je veux configurer une autre méthode".

9. Une fois le code entré, vous pourrez faire « **Suivant** ».

The screenshot shows the same "Protéger votre compte" interface. The progress bar still shows "Méthode 2 sur 2 : Téléphone". The "Application" step is marked with a green checkmark, and the "Téléphone" step is now marked with a green checkmark. The main content area is titled "Téléphone" and contains the text: "Vérfifié par SMS. Votre téléphone a été enregistré avec succès." A blue "Suivant" button is now active and visible at the bottom right.

10. Votre compte sera maintenant protégé par le MFA et le service de récupération de mot est maintenant actif.

Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Méthode 2 sur 2 : Terminé

Application Téléphone

Opération réussie

Bravo ! Vous avez correctement configuré vos informations de sécurité. Cliquez sur « Terminé » pour poursuivre la connexion.

Méthode de connexion par défaut :

-  Téléphone
+1 999 9999999
-  Microsoft Authenticator

[Terminé](#)

J'ai un problème avec l'expérience combiné

Contactez-nous par le Centre de services si vous rencontrez un problème ou si vous ne possédez pas de cellulaire.

Pour ce faire, cliquez sur l'icône « Centre de services » présente sur le bureau de votre ordinateur.

1. Sélectionnez « DSTI-SOSInformatique » dans le champ **Service**
2. Sélectionnez « J'ai un problème de... » puis « Accès » dans les deux champs **Type**
3. Décrivez-nous le plus précisément possible le problème rencontré ainsi que l'étape de la procédure en problème (ex : je ne possède pas de cellulaire pour pouvoir mettre en place le MFA, j'ai un problème pour m'authentifier, etc.)
4. Cliquez sur « Soumettre » pour envoyer votre demande.

The screenshot shows a web form titled "Nouvelle requête" (New request). The form fields are as follows:

- Demandeur:** Labolle, Jessica
- Service*:** A dropdown menu with "DSTI-SOSInformatique" selected. A red circle with the number "1" is next to it.
- Type*:** Two stacked dropdown menus. The first has "J'ai un problème de..." selected, and the second has "Accès" selected. A red circle with the number "2" is next to the first dropdown.
- Utilisateur:** Labolle, Jessica, with a "CHANGER" button below it.
- Description*:** A text area with the prompt "Veillez décrire avec le plus d'informations possible votre problème d'accès: message d'erreur, imprime-écran etc." and a sub-prompt "Description du problème:". A red circle with the number "3" is next to the text area.
- Fichier joint:** A "Sélectionner..." button.
- Buttons:** "SOUMETTRE" (highlighted with a red circle and number "4") and "ANNULER".

Vous serez contacté par un technicien dans les plus brefs délais et un rendez-vous pourrait vous être proposé afin de résoudre votre problématique.

Si vous ne pouvez accéder au Centre de services, merci de nous contacter par téléphone (ci-dessous) ou via le [formulaire de demande de service](#)

Direction des systèmes et des technologies de l'information – DSTI
 Centre de Services : DSTI-SOSInformatique <http://centredeservices.cegeplimoilou.ca>
 Courriel : sosinfo@cegeplimoilou.ca
 Téléphone : 418 647-6600, 6533 (Québec et Charlesbourg)
 Avant d'imprimer, pensez à l'environnement!