

COBA

Authentification multifacteur (AMF)

Résumé du document

Le présent guide donne les détails pour activer et gérer l'authentification multifacteur (AMF) pour les produits COBA : Activités, Finances, RH/Paie, Pédagogie et Collégial.

Version du 16 janvier 2024

CONTACTS

coba.activites@berger-levrault.com
coba.collegial@berger-levrault.com
coba.finance@berger-levrault.com
coba.pedago@berger-levrault.com
coba.rhpaie@berger-levrault.com

Berger-Levrault Canada

2130, boulevard Dagenais Ouest, bureau 200
Laval (Québec) H7L 5X9

514 251-2622 | 1 844 228-2622
ventes.canada@berger-levrault.com

AVERTISSEMENT ET NOTES

Dans le présent document, le genre masculin est utilisé au sens neutre et désigne les femmes autant que les hommes.

Ce document est confidentiel. Il ne peut être copié ou distribué sans l'autorisation de Berger-Levrault Canada Itée

berger-levrault.com

Table des matières

Introduction.....	1
Définir une politique d'authentification multifacteur (V5)	2
Définir une politique d'authentification multifacteur (V6)	4
Communication aux utilisateurs	5
Annoncer une date de l'activation de l'authentification multifacteur	5
Activer une politique d'authentification multifacteur pour une application administrative V6	6
Activer une politique d'authentification multifacteur pour un portail	7
Gérer l'authentification multifacteur pour un utilisateur du portail	8
Activer l'authentification multifacteur	8
Gérer l'authentification multifacteur pour un utilisateur administratif V6.....	10

Introduction

Que ce soit pour les applications et services liés au travail ou personnels, la plupart d'entre nous évitent de créer des mots de passe complexes à moins d'en être obligé et n'avons en moyenne que cinq différents mots de passe pour la multitude d'applications et de services que nous utilisons. Cela facilite l'accès aux malintentionnés. Un pirate informatique peut facilement casser le mot de passe d'un utilisateur et accéder à toutes ses applications et services utilisés. D'où l'importance de l'authentification multifacteur (AMF). Elle ajoute un niveau supplémentaire de sécurité qui empêchent les cybercriminels de pirater les comptes d'utilisateurs.

C'est un outil de sécurité qui permet aux organisations ou aux particuliers d'ajouter des couches supplémentaires de protection lors de la connexion à un site Web ou à une application. Au lieu d'utiliser uniquement un nom d'utilisateur et un mot de passe, les utilisateurs peuvent utiliser AMF pour sécuriser davantage leurs comptes.

L'authentification multifacteur (AMF) ajoute une méthode supplémentaire pour la connexion à un service ou application. Le facteur AMF le plus courant est le code à usage unique (OTP - One Time PIN). Les utilisateurs saisissent leurs noms d'utilisateur et mots de passe. Ils reçoivent ensuite un OTP sur l'un de leurs appareils. Ces codes OTP expirent généralement dans un délai de 60 secondes.

La AMF atténue le risque de vulnérabilité des entreprises ou des utilisateurs privés aux cyberattaques. Il est plus difficile pour un pirate d'accéder au compte d'un utilisateur AMF, car il aurait besoin du mot de passe d'un utilisateur et de l'un de ses appareils (généralement son téléphone mobile).

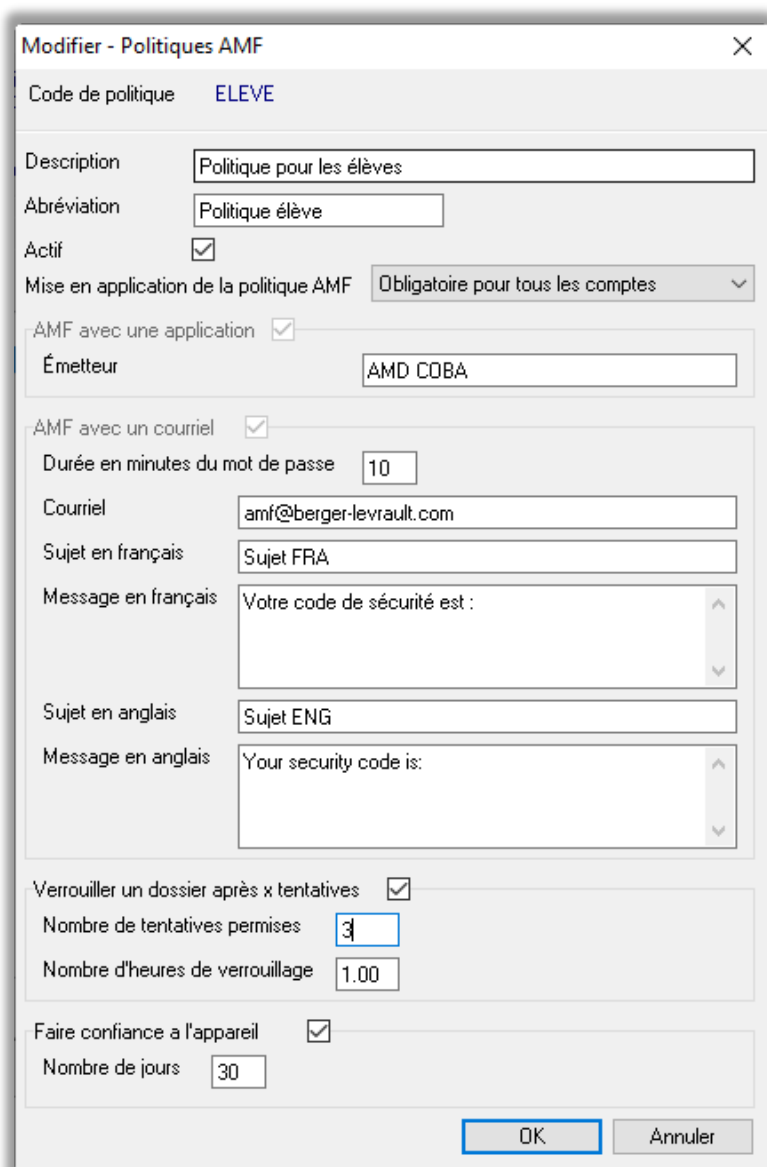
Les utilisateurs doivent toujours utiliser les processus AMF pour accéder à leurs informations et comptes sensibles (dossiers médicaux et bancaires).

Le personnel de Berger Levrault s'efforce de faire tout ce qu'il peut pour protéger les données de ses clients. Il fournit des outils à ses employés pour les aider à protéger l'organisation contre les cyberattaques. La AMF est un moyen de protéger votre entreprise contre les attaques.

Définir une politique d'authentification multifacteur (V5)

Avant de pouvoir déployer l'authentification multifacteur, il faut d'abord suivre les étapes suivantes pour définir une politique d'authentification.

1. Cliquer sur **Système > Configuration > onglet Politiques AMF**.
2. Cliquer sur le bouton **Ajouter** et saisir un code de politique. Vous disposez de 10 caractères alphanumériques.
3. Indiquer une **Description** interne.
4. Indiquer une **Abréviation** interne.
5. La case **Actif** est cochée par défaut, veuillez la décocher si vous souhaitez désactiver la politique.



Modifier - Politiques AMF

Code de politique: **ELEVE**

Description:

Abréviation:

Actif: ☒

Mise en application de la politique AMF:

AMF avec une application: ☒

Émetteur:

AMF avec un courriel: ☒

Durée en minutes du mot de passe:

Courriel:

Sujet en français:

Message en français:

Sujet en anglais:

Message en anglais:

Verrouiller un dossier après x tentatives: ☒

Nombre de tentatives permises:

Nombre d'heures de verrouillage:

Faire confiance à l'appareil: ☒

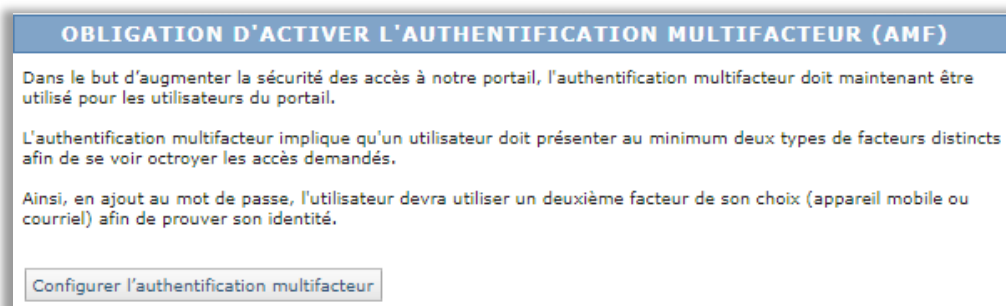
Nombre de jours:

OK **Annuler**

6. Sélectionner une **Mise en application de la politique AMF**. Trois options sont offertes :

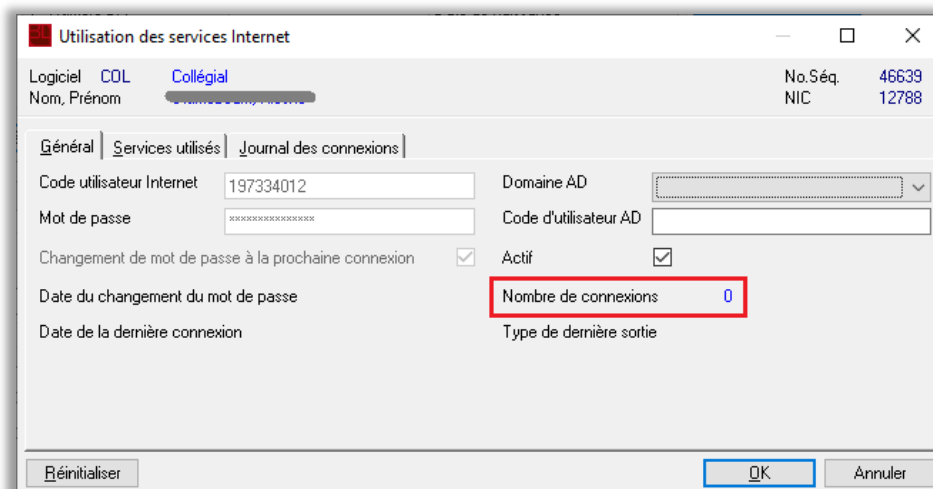
- **Obligatoire pour tous les comptes**

- L'authentification multifacteur est obligatoire pour tous les utilisateurs.
- Si un utilisateur se connecte à un compte sans AMF, l'activation de l'AMF pour son compte sera obligatoire.



- **Obligatoire pour les nouveaux comptes**

- L'authentification multifacteur sera obligatoire pour tous les nouveaux utilisateurs.
- Si un nouvel utilisateur se connecte à un compte sans AMF, l'activation de l'AMF pour son compte sera obligatoire.
 - Un nouvel utilisateur est un utilisateur qui effectue sa première connexion sur le portail donc sans aucune connexion antérieure.



- **Au choix de l'utilisateur**

- L'authentification multifacteur est facultative pour tous utilisateurs.
- Le choix d'activer ou de ne pas activer l'AMF revient à l'utilisateur.

7. Indiquer le nom de votre institution dans le champ **Émetteur** pour l'authentification **AMF avec une application**.

8. Indiquer un nombre dans **Durée en minutes du mot de passe** pour l'option **AMF avec un courriel**. C'est la durée de validité du code envoyé par courriel.

9. Saisir le **Courriel** de l'expéditeur du courriel envoyé.

10. Indiquer un **Sujet en français**. C'est l'objet du courriel qui sera envoyé.
11. Saisir un **Message en français**. C'est le contenu du courriel qui sera envoyé.
12. Indiquer un **Sujet en anglais**. C'est l'objet du courriel qui sera envoyé si l'utilisateur est connecté sur le portail en anglais.
13. Saisir un **Message en anglais**. C'est le contenu du courriel qui sera envoyé si l'utilisateur est connecté sur le portail en anglais.
14. Cocher la case **Verrouiller un dossier après x tentatives** au besoin.
15. Saisir le **Nombre de tentatives permises** voulu.
16. Saisir le **Nombre d'heures du verrouillage** voulu.
17. Cocher la case **Faire confiance à l'appareil** pour activer cette option.
18. Saisir le **Nombre de jours** que doit durer la confiance. Il s'agit du nombre de jours pour lequel l'application ou le portail doit faire confiance à l'appareil avant d'exiger une nouvelle authentification multifacteur. Le maximum est de 99.
19. Cliquer sur **OK**.

NOTE :

Vous pouvez définir une politique différente pour chaque type d'utilisateur.

Définir une politique d'authentification multifacteur (V6)

Pour définir une politique d'authentification, vous devez accéder à l'option **Configuration > Bases > Politiques AMF**.

Les informations à saisir sont les mêmes que pour la section ci-dessus **Définir une politique d'authentification multifacteur (V5)**.

Communication aux utilisateurs

Avant de déployer l'AMF, il sera important d'envoyer une communication à vos utilisateurs pour les aviser de ce changement. Vous pouvez vous inspirer de l'exemple ci-dessous.

Annoncer une date de l'activation de l'authentification multifacteur

Recommander aux utilisateurs d'activer l'AMF avant cette date.

[Voir dans un navigateur](#)



**S'INVESTIR POUR
UNE MEILLEURE SOCIÉTÉ.**

L'authentification à deux facteurs arrive au Fonds!



Bonjour Sylvain,

Dès les prochaines semaines, la protection de vos renseignements personnels sera bonifiée grâce à l'authentification à deux facteurs qui vous sera demandée lors de la connexion à votre compte en ligne. Lorsque vous vous y connecterez, afin de valider votre identité, un code de sécurité vous sera envoyé par texto ou par courriel.

Facilitez aujourd'hui même vos futures connexions en faisant en sorte que votre compte en ligne contienne une **adresse courriel** et un **numéro de téléphone portable** à jour!

Activer une politique d'authentification multifacteur pour un portail

Pour activer une politique d'authentification multifacteur (AMF) pour un portail, vous devez accéder à la configuration des **Services Internet** du portail.

Selon le profil sélectionné, le bouton AMF sera disponible dans le bas de l'écran afin de permettre de sélectionner un code de politique à appliquer pour les authentifications des utilisateurs de ce profil.

COBA Activités

V5 : **Activités** > **Généralités** > **Outils** > **Configuration du portail Internet** > **Services Internet**

V6 : **Configuration** > **Portail Internet** > **Profil ...- Mon dossier** > **Sommaire** en haut

L'AMF est disponible pour les profils **Participants** et **Moniteurs**.

COBA Collégial

V5 : **Collégial** > **Utilitaires** > **Campus** > **Outils** > **Configuration du portail Internet** > **Services Internet**

V6 : **Configuration** > **Portail Internet** > **Profil ...- Mon dossier** > **Sommaire** en haut

L'AMF est disponible pour les profils **Élèves** et **Enseignants**.

COBA Finances

Finances > **Généralités** > bouton **Internet** > onglet **Profils** > **Client**

L'AMF est disponible pour le profil **Client**.

COBA Pédagogie

Jeune > **Utilitaires** > **École** > **Outils** > **Configuration du portail Internet** > **Services Internet**

L'AMF est disponible pour les profils **Élèves** et **Enseignants**.

COBA RH/Paie

RH/Paie > **Généralités** > bouton **Internet** > onglet **Profils** > **Employés**

L'AMF est disponible pour le profil **Employés**.

IMPORTANT :

Avant d'activer l'authentification multifacteur pour un profil, vous **devez vous assurer** que le service internet **Options est actif** pour le profil sélectionné.

Gérer l'authentification multifacteur pour un utilisateur du portail

Activer l'authentification multifacteur

1. Se connecter sur le portail
2. Accéder au service Options > section Authentification multifacteur (AMF)

AUTHENTIFICATION MULTIFACTEUR (AMF)

Activer l'authentification multifacteur
Cette option permet d'activer l'authentification multifacteur (appareil mobile ou courriel) à votre compte.

3. Cliquer sur Ajouter l'authentification multifacteur

ACTIVATION DE L'AUTHENTIFICATION MULTIFACTEUR (AMF)

Dans le but d'augmenter la sécurité des accès à notre portail, l'authentification multifacteur peut maintenant être utilisé pour les utilisateurs du portail.

L'authentification multifacteur implique qu'un utilisateur doit présenter au minimum deux types de facteurs distincts afin de se voir octroyer les accès demandés.

Ainsi, en ajout au mot de passe, l'utilisateur devra utiliser un deuxième facteur de son choix (appareil mobile ou courriel) afin de prouver son identité.

[Configurer l'authentification multifacteur](#)
[Retour](#)

4. Cliquer sur le bouton Configurer l'authentification multifacteur
5. Sélectionner le type d'authentification à configurer
 - a. Avec une application

CONFIGURER L'AUTHENTIFICATION MULTIFACTEUR

Type d'authentification [Avec une application](#)

Le type d'authentification "Avec une application" permet de configurer une application (ex. Microsoft Authenticator ou Google Authenticator) sur un cellulaire ou une tablette afin de recevoir un code à 6 chiffres à utiliser lors de la connexion sur le portail.

Pour ajouter votre compte du portail dans une application, vous devez ouvrir votre application d'authentification, scanner le code QR ou entrer manuellement le code ci-dessous :



TYG7 43OF AR4D QAYA [Copier le code dans le presse-papier](#)

[Valider le code affiché par l'application pour activer l'authentification multifacteur](#)

- b. Par courriel

CONFIGURER L'AUTHENTIFICATION MULTIFACTEUR

Type d'authentification [Par courriel](#)

Le type d'authentification "Par courriel" utilise le courriel à votre dossier pour vous envoyer un code à 6 chiffres à utiliser lors de la connexion sur le portail

Le code qui sera envoyé par courriel sera valide pour les 10 prochaines minutes

[Valider le code envoyé par courriel](#)

6. Valider le code à 6 chiffres affiché dans l'application ou reçu par courriel.



NOTE :

L'option **Activer l'authentification multifacteur** est disponible seulement lorsque la politique AFM du profil de l'utilisateur est **Au choix de l'utilisateur**.

Lorsque l'authentification multifacteur est obligatoire, l'utilisateur est automatiquement dirigé vers le processus d'activation après sa connexion sur le portail.

Une fois l'authentification multifacteur activée, l'utilisateur peut retourner dans le service Options du portail afin d'avoir accès à des options supplémentaires pour gérer l'authentification multifacteurs.

Les options qui seront disponibles sont affichées en fonction de la configuration de l'authentification multifacteur et de l'état du dossier de l'utilisateur.

NOTE :

Pour effectuer une authentification multifacteur avec une application, vous devez installer l'application Microsoft Authenticator ou Google Authenticator à partir Google Play pour les appareils Android ou de l'App store pour les appareils iOS (Apple)

Gérer l'authentification multifacteur pour un utilisateur administratif V6

NOTE :

L'authentification multifacteur pour les utilisateurs administratifs V6 sera disponible avec la révision de la 24.2 prévue pour le mois de mai 2024.