Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.1

7 nov, 2026 · @Gabriel

Objectif : *Activer l'authentification à deux facteurs (2FA) sur vos comptes importants (e-mail, gestionnaire de mots de passe, cloud, banque) et remplacer Google Authenticator par une application libre et open source :* ***Aegis***, ***Ente Auth*** *ou* ***Proton Authenticator***.

- ***Public visé :*** *Débutant à Intermédiaire*
- ***Temps estimé :*** *30 minutes à 1 heure (selon le nombre de comptes)*
- ***Difficulté :*** *★★☆☆☆ (Facile)*
- ***Prérequis :*** *avoir un gestionnaire de mots de passe (fiche N°16) – recommandé mais pas obligatoire*
- ***Fiches associées :*** *N°16 (mots de passe), N°15 (messageries)*

1. Pourquoi activer la 2FA ? (Le problème)

Le problème du mot de passe seul

Risque	Explication
Mot de passe volé	Fuite de base de données, hameçonnage, logiciel espion, mot de passe réutilisé.
Accès à vos comptes	Avec votre mot de passe, un pirate peut se connecter depuis n'importe où.
Conséquences	Usurpation d'identité, fraude bancaire, prise de contrôle de vos réseaux sociaux.

La solution : un deuxième facteur

Facteur	Exemple
Quelque chose que vous savez	Votre mot de passe
Quelque chose que vous possédez	Votre téléphone (qui génère un code à 6 chiffres) ou une clé de sécurité

Sans le code temporaire, un mot de passe volé ne suffit plus.

Le problème avec Google Authenticator

Problème	Explication
Propriétaire	Code fermé : impossible de vérifier ce que fait l'application.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.1

Problème	Explication
Synchronisation liée au compte Google	Depuis avril 2023, la sauvegarde passe par votre compte Google ; au lancement, elle n'était pas chiffrée de bout en bout (Google a annoncé l'ajouter plus tard). Sans compte Google, aucune sauvegarde.
Dépendance	Vos codes 2FA dépendent d'un compte big tech.

Le bénéfice : une application 2FA open source, avec sauvegarde chiffrée sous votre contrôle.

2. Les trois applications recommandées

Application	Open source	Sauvegarde	Synchronisation	Compte requis	Idéal pour
Aegis (Android uniquement)	✅	Fichier chiffré (manuel ou automatique vers un dossier)	Manuelle	Non	Contrôle total sur Android
Ente Auth (Android, iOS, ordinateur)	✅	Chiffrée de bout en bout, automatique	✅ Native	Non (mode « sans sauvegarde ») / oui pour synchroniser	Plusieurs appareils
Proton Authenticator (Android, iOS, Windows, macOS, Linux)	✅	Chiffrée (compte Proton, ou iCloud sur iPhone)	✅ Native avec compte Proton	**Non** (compte seulement pour synchroniser)	Plusieurs appareils, écosystème Proton

Pourquoi Proton Authenticator ?

Application 2FA **gratuite**, **open source**, lancée par Proton fin juillet 2025.

- **Multiplateforme :** iOS, Android, macOS, Windows, Linux.
- **Aucun compte Proton requis :** utilisation locale possible.
- **Synchronisation optionnelle :** avec un compte Proton, chiffrée de bout en bout.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.1

- **Import facile :** depuis Google Authenticator, Aegis, 2FAS, Ente Auth, Bitwarden Authenticator, LastPass Authenticator.
- **Juridiction suisse.**

Limite : application récente.

Pourquoi pas Google Authenticator, Microsoft Authenticator ou Authy ?

Application	Problème
Google Authenticator	Propriétaire ; sauvegarde dépendante du compte Google
Microsoft Authenticator	Propriétaire ; sauvegarde via compte Microsoft
Authy (Twilio)	Propriétaire ; applications de bureau arrêtées en août 2024 ; pas d'export des codes

3. Comment choisir ? (Selon votre profil)

Si vous êtes…	Choisissez…	Pourquoi
Sur Android, vous voulez le contrôle total	**Aegis**	Fichier local chiffré, zéro cloud
Sur plusieurs appareils (Android + iPhone + ordinateur)	**Ente Auth** ou **Proton Authenticator**	Synchronisation chiffrée de bout en bout
Sur iPhone	**Ente Auth** ou **Proton Authenticator**	Aegis n'existe pas sur iOS
Déjà utilisateur Proton	**Proton Authenticator**	Même compte, Suisse
Débutant, vous voulez une sauvegarde automatique	**Proton Authenticator** ou **Ente Auth**	Sauvegarde chiffrée automatique
Exigeant, zéro cloud	**Aegis**	Vous gérez vous-même la sauvegarde

4. Méthode A : Aegis (Android, contrôle total)

Pourquoi Aegis ?

- Open source.
- Coffre local chiffré : vos codes ne quittent pas votre téléphone.
- Export chiffré vers l'emplacement de votre choix (Nextcloud, Syncthing, clé USB).
- Zéro compte, zéro cloud.
- Import depuis Google Authenticator.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.1

Comment faire ? (Pas à pas)

1. **Installez Aegis** : F-Droid ou Aurora Store → « Aegis Authenticator » (pas de version iPhone).
    - Vous devez voir : l'assistant de première configuration.
2. **Protégez le coffre** : choisissez un mot de passe (et, si vous le souhaitez, le déverrouillage biométrique).
    - Vous devez voir : le coffre vide.
3. **Importez vos codes depuis Google Authenticator** :
    - Dans Google Authenticator : **menu › Transférer des comptes › Exporter des comptes** → sélectionnez les comptes → un QR code s'affiche.
    - Dans Aegis : **Réglages › Importer et exporter › Importer** → Google Authenticator → scannez le QR code.
    - Vous devez voir : vos comptes dans Aegis. Supprimez-les ensuite de Google Authenticator.
4. **Ajoutez un nouveau compte** : sur le site, activez la 2FA → « application d'authentification » → scannez le QR code avec Aegis → saisissez le code à 6 chiffres.
5. **Sauvegardez** : **Réglages › Sauvegardes** → activez les sauvegardes automatiques chiffrées vers un dossier, ou exportez manuellement un fichier chiffré.
    - Vous devez voir : un fichier de sauvegarde à copier hors du téléphone (ordinateur, clé USB).

5. Méthode B : Ente Auth (Android, iOS, ordinateur – synchronisation)

Pourquoi Ente Auth ?

- Open source, audité (Cure53, audit du serveur publié en 2025).
- Synchronisation chiffrée de bout en bout entre vos appareils.
- Sauvegarde automatique.
- Utilisable **sans compte** (mode sans sauvegarde), avec un compte pour synchroniser.
- Serveur auto-hébergeable.

Comment faire ? (Pas à pas)

1. **Installez Ente Auth** :
    - Android : F-Droid ou Aurora Store → « Ente Auth ».
    - iPhone : App Store → « Ente Auth ».
    - Ordinateur : **ente.io** → application de bureau.
2. **Créez un compte** (e-mail + mot de passe fort rangé dans votre gestionnaire, fiche N°16) **ou** choisissez l'utilisation sans sauvegarde.
    - Vous devez voir : l'écran (vide) de vos codes.
3. **Importez vos codes** : depuis Google Authenticator (QR code d'export) ou depuis un export Aegis.
4. **Ajoutez un nouveau compte** : scannez le QR code du site, saisissez le code pour confirmer.

gabriel.ananda@mailo.com
CC BY SA

5. **Vérifiez la synchronisation** : ouvrez Ente Auth sur un autre appareil connecté au même compte.
    - Vous devez voir : le même code apparaître.

6. Méthode C : Proton Authenticator (écosystème Proton)

Comment faire ? (Pas à pas)

Étape 1 : Installez Proton Authenticator

Appareil	Action
Android	Aurora Store → « Proton Authenticator » (ou Play Store en dernier recours)
iPhone	App Store → « Proton Authenticator »
Ordinateur	proton.me/authenticator → application de bureau (Windows, macOS, Linux)

Étape 2 : Configurez l'application

1. Lancez Proton Authenticator.
2. Utilisez-la **sans compte Proton** (mode local), ou connectez-vous pour synchroniser.
3. Activez la protection biométrique ou par code.
    - Vous devez voir : l'écran (vide) de vos codes.

Étape 3 : Importez vos codes existants

- Depuis Google Authenticator, Aegis, 2FAS, Ente Auth, Bitwarden Authenticator ou LastPass Authenticator.
- Depuis Authy : pas d'export possible → désactivez puis réactivez la 2FA sur chaque compte avec la nouvelle application.

Étape 4 : Ajoutez un nouveau compte 2FA

1. Sur le site : activez la 2FA → « application d'authentification ».
2. Scannez le QR code avec Proton Authenticator.
3. Saisissez le code pour confirmer.

Étape 5 : Sauvegarde et synchronisation

- Avec un compte Proton : synchronisation et sauvegarde chiffrées de bout en bout.
- Sans compte : sauvegarde chiffrée possible sur iPhone (iCloud) ou **export** de vos codes vers un endroit sûr.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.1

7. Activer la 2FA sur vos comptes : quels comptes en priorité ?

Priorité	Type de compte	Exemples
Critique (en premier)	E-mail principal	Proton Mail, Tuta Mail, Gmail, Outlook
Critique	Gestionnaire de mots de passe	Bitwarden, Proton Pass
Élevée	Cloud / stockage	Nextcloud, kDrive, pCloud
Élevée	Réseaux sociaux	Mastodon, X, Reddit
Élevée	Banque / paiement	Banque en ligne, PayPal
Moyenne	Messageries	Element (Matrix) ; Signal : activez le **verrouillage d'inscription** (code PIN)
Moyenne	Comptes techniques	GitHub, GitLab
Basse	Forums, sites d'actualité	Si vous y tenez

Règle d'or : tout compte qui donne accès à votre e-mail ou à votre argent doit avoir la 2FA.

Comment activer la 2FA sur un site (méthode générale)

1. Ouvrez les paramètres de sécurité du compte.
2. Cherchez « Authentification à deux facteurs », « 2FA », « Validation en deux étapes » ou « MFA ».
3. Choisissez « Application d'authentification » (plutôt que SMS ou e-mail).
4. Scannez le QR code avec Aegis, Ente Auth ou Proton Authenticator.
5. Saisissez le code à 6 chiffres pour confirmer.
6. **Notez les codes de récupération** : rangez-les dans votre gestionnaire de mots de passe **et** sur papier.

Le site 2fa.directory (anciennement twofactorauth.org) liste les sites qui proposent la 2FA et les méthodes acceptées.

8. Codes de récupération – à ne pas négliger

À l'activation de la 2FA, le site fournit en général une série de codes à usage unique.

Action	Explication
Rangez-les dans votre gestionnaire (fiche N°16)	Sécurisé, accessible depuis vos appareils
Imprimez-les	Rangez la feuille en lieu sûr
Ne les gardez pas uniquement sur le téléphone qui génère les codes	Sinon, vous perdez tout en même temps

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.1

Sans codes de récupération ni sauvegarde de votre application, la perte du téléphone peut vous bloquer définitivement hors de vos comptes.

9. Tableau récapitulatif : Aegis, Ente Auth, Proton Authenticator

Critère	Aegis	Ente Auth	Proton Authenticator
Open source	✅	✅	✅
Sans compte	✅	✅ (sans sauvegarde)	✅
Sauvegarde automatique	✅ (fichier chiffré local)	✅ (chiffrée)	✅ (avec compte, ou iCloud sur iPhone)
Synchronisation multi-appareils	❌	✅	✅
Application de bureau	❌	✅	✅ (Windows, macOS, Linux)
iPhone	❌	✅	✅
Import depuis Google Authenticator	✅	✅	✅
Export	✅ (chiffré)	✅	✅
Idéal pour	Contrôle total	Multi-appareils, simplicité	Écosystème Proton

10. À savoir avant de se lancer

Crainte fréquente	La réalité
« Je vais me bloquer hors de mes comptes. »	Avec les codes de récupération (gestionnaire + papier), vous êtes protégé. Commencez par un compte peu important pour vous entraîner.
« Si je perds mon téléphone, je perds tout. »	Non, si vous avez vos codes de récupération et une sauvegarde (export Aegis, Ente Auth, Proton Authenticator).
« Dois-je activer la 2FA partout ? »	Commencez par l'e-mail, le gestionnaire de mots de passe et la banque, puis le reste progressivement.
« Aegis n'est pas sur iPhone. »	Utilisez Ente Auth ou Proton Authenticator.
« Ente ou Proton stockent mes codes : est-ce sûr ? »	Ils sont chiffrés de bout en bout : le service ne peut pas les lire. Les deux s'utilisent aussi sans compte.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.1

11. Challenge 7 jours

Challenge : pendant 7 jours, activez la 2FA sur trois comptes critiques.

- **Jour 1-2 :** choisissez et installez votre application.
- **Jour 3 :** activez la 2FA sur votre e-mail principal.
- **Jour 4 :** activez-la sur votre gestionnaire de mots de passe.
- **Jour 5 :** activez-la sur votre stockage en ligne.
- **Jour 6 :** rangez tous vos codes de récupération (gestionnaire + papier).
- **Jour 7 :** déconnectez-vous et reconnectez-vous avec la 2FA.

Vous allez constater :

- La 2FA ajoute quelques secondes par connexion.
- Un mot de passe volé ne suffit plus à entrer dans vos comptes.
- Avec une sauvegarde, la perte du téléphone n'est plus une catastrophe.

12. Alternatives et approfondissements

Si vous avez besoin de…	Essayez plutôt…
Une clé physique (sans téléphone)	Clé de sécurité FIDO2 / passkeys (YubiKey, Nitrokey…)
2FA sur vos comptes Proton	Application d'authentification ou clé de sécurité
Une solution auto-hébergée	Ente Auth (serveur auto-hébergeable) ou Aegis + Syncthing
Codes 2FA sur l'ordinateur	Ente Auth, Proton Authenticator ou KeePassXC
Savoir quels sites acceptent la 2FA	2fa.directory

13. En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Utiliser Aegis (Android)	2FA open source, zéro cloud	§ 4
Utiliser Ente Auth	2FA synchronisée et chiffrée	§ 5
Utiliser Proton Authenticator	2FA open source, Suisse, avec ou sans compte	§ 6
Quitter Google Authenticator	Vos codes ne dépendent plus d'un compte Google	§ 1
Activer la 2FA sur votre e-mail	Boîte protégée même si le mot de passe fuit	§ 7

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.1

Action	Gagné	Renvoi
Ranger vos codes de récupération	Vous pouvez récupérer vos comptes sans téléphone	§ 8

À retenir absolument

- La 2FA transforme un compte vulnérable en compte robuste : il faut aussi votre téléphone (ou votre clé).
- **Les codes de récupération sont aussi importants que le mot de passe** : gestionnaire + papier.
- **Aegis**, **Ente Auth** et **Proton Authenticator** sont open source et vous laissent maîtres de vos sauvegardes.
- Commencez petit : un seul compte (l'e-mail), puis les autres.

Test final :

1. Installez Aegis, Ente Auth ou Proton Authenticator.
2. Activez la 2FA sur votre e-mail.
3. Rangez les codes de récupération dans votre gestionnaire et sur papier.
4. Déconnectez-vous, puis reconnectez-vous avec le code 2FA.
5. Si vous réussissez : **vos comptes sont bien mieux protégés** ✅

Références

- Proton Authenticator – page officielle
- MacRumors – Lancement de Proton Authenticator (31 juillet 2025)
- Ente – Mode hors ligne d'Ente Auth
- Ente – Audit Cure53 sponsorisé par le CERN
- The Hacker News – Google Authenticator synchronise via le compte Google (avril 2023)
- AlternativeTo – Arrêt des applications de bureau Authy (août 2024)
- 2fa.directory – Annuaire des sites proposant la 2FA
- 2factorauth – changement de domaine vers 2fa.directory

gabriel.ananda@mailo.com
CC BY SA