

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

Objectif : Activer l'authentification à deux facteurs (2FA) sur tous vos comptes importants (email, réseaux sociaux, cloud, banque) et remplacer Google Authenticator par une application libre, open-source et respectueuse de votre vie privée (**Aegis**, **Ente Auth** ou **Proton Authenticator**).

• **Public visé** : Débutant à Intermédiaire

• **Temps estimé** : 30 minutes à 1 heure (selon le nombre de comptes)

• **Niveau de difficulté** : ★★☆☆☆ (Facile)

• **Prérequis** : Avoir déjà un gestionnaire de mots de passe (fiche N°16) – recommandé mais pas obligatoire.

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, phishing, keylogger, mot de passe réutilisé sur plusieurs sites.
Accès à vos comptes	Un pirate qui obtient votre mot de passe peut se connecter à vos comptes depuis n'importe où.
Conséquences	Usurpation d'identité, vidage de compte bancaire, prise de contrôle de vos réseaux sociaux, accès à vos conversations privées.

La solution : 2FA (deuxième facteur)

La 2FA ajoute une deuxième preuve que vous êtes bien vous :

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

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)

Sans le code temporaire généré par votre téléphone, un mot de passe volé ne suffit pas pour se connecter.

Le problème avec Google Authenticator

Problème

Explication

Propriétaire Appartient à Google, closed-source, vous ne savez pas ce qu'il fait avec vos données.

Pas de sauvegarde Si vous perdez votre téléphone, vous perdez tous vos codes 2FA (et vous êtes verrouillé hors de vos comptes).

Pas de synchronisation Difficile d'utiliser le même authenticateur sur plusieurs appareils.

Collecte de données Google collecte potentiellement des métadonnées d'utilisation (quels comptes vous protégez, quand).

Le bénéfice : Une application 2FA open-source, avec sauvegarde chiffrée, synchronisation possible, et zéro collecte de données.

2. Les trois applications recommandées

Application

Open-source

Sauvegarde

Synchronisation

Cloud

Idéal pour

Aegis (Android uniquement)

✓ Oui

✓ Chiffrée
(fichier local)

✓ Manuelle
(fichier à

Non
(fichier

Utilisateurs
Android qui

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

Application	Open-source	Sauvegarde	Synchronisation	Cloud	Idéal pour
			synchroniser)	local)	veulent le contrôle total
				Oui (serveurs	
Ente Auth (Android, iOS, Desktop)	✓ Oui	✓ Chiffrée (automatique)	✓ Native (chiffrée E2EE)	Ente, open-source, audités)	Utilisateurs multi-appareils
Proton Authenticator (Android, iOS, Desktop, Web)	✓ Oui	✓ Chiffrée (automatique)	✓ Native (chiffrée E2EE)	Oui (serveurs Proton, Suisse)	Utilisateurs multi-appareils, déjà dans l'écosystème Proton

Pourquoi Proton Authenticator ?

Proton Authenticator est une application 2FA **gratuite, open-source, et chiffrée de bout en bout**, lancée par Proton en 2025 . Elle présente plusieurs avantages :

- **Multiplateforme complet** : disponible sur iOS, Android, macOS, Windows, Linux, et même en version web .
- **Chiffrement de bout en bout** : même Proton ne peut pas voir vos codes 2FA .
- **Aucun compte Proton requis** : vous pouvez utiliser l'application localement, sans créer de compte .
- **Synchronisation optionnelle** : si vous créez un compte Proton, vos codes se synchronisent entre appareils, protégés par E2EE .
- **Import facile** : depuis Google Authenticator, Aegis, Authy, etc. .
- **Juridiction suisse** : lois de protection de la vie privée solides .
- **Sauvegarde automatique** : activable pour ne jamais perdre vos codes .

Limite : application relativement jeune (lancée en 2025), écosystème en construction .

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

Pourquoi pas Google Authenticator, Microsoft Authenticator ou Authy ?

Application	Problème
Google Authenticator	Propriétaire, pas de sauvegarde (perte de téléphone = perte des codes)
Microsoft Authenticator	Propriétaire, synchronisation via compte Microsoft (vos données chez Microsoft)
Authy	Propriétaire (Twilio), fermeture annoncée du bureau, cloud propriétaire

3. Comment choisir ? (Selon votre profil)

Si vous êtes...	Choisissez...	Pourquoi
Sur Android uniquement, vous voulez le contrôle total	Aegis	Fichier local chiffré, export manuel, zéro cloud, open-source
Sur plusieurs appareils (Android + iPhone + ordinateur)	Ente Auth ou Proton Authenticator	Synchronisation chiffrée de bout en bout, applications natives
Sur iPhone uniquement	Ente Auth ou Proton Authenticator	Aegis n'existe pas sur iOS
Déjà utilisateur Proton (Mail, Drive, VPN, Pass)	Proton Authenticator	Écosystème intégré, Suisse, pas de compte supplémentaire
Débutant, vous voulez la simplicité avec sauvegarde automatique	Proton Authenticator ou Ente Auth	Interface moderne, sauvegarde automatique chiffrée
Exigeant / paranoïde, zéro cloud même chiffré	Aegis	Fichier local, vous contrôlez la sauvegarde (Nextcloud, Syncthing)

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

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

Pourquoi Aegis ?

- 100 % open-source (code auditable sur GitHub).
- Fichier local chiffré (vos codes ne quittent pas votre téléphone).
- Export chiffré (vous sauvegardez où vous voulez : Nextcloud, Syncthing, clé USB).
- Zéro compte, zéro cloud, zéro collecte.
- Import depuis Google Authenticator (facile).

Comment faire ? (Pas à pas)

Étape 1 : Installez Aegis

- Android : Aurora Store (sans traçage) ou F-Droid → recherchez "Aegis Authenticator".
- (Pas disponible sur iOS)

Étape 2 : Configurez la protection de l'application

1. Lancez Aegis.
2. L'application vous propose de définir un mot de passe pour déverrouiller l'application (optionnel mais recommandé).
3. Activez l'authentification biométrique (empreinte digitale) si vous le souhaitez.

Étape 3 : Importez vos codes existants (depuis Google Authenticator)

Si vous utilisez déjà Google Authenticator :

1. Dans Google Authenticator : menu → Transférer les comptes → Exporter → sélectionnez tous → suivant → afficher le code QR.
2. Dans Aegis : Menu → Importer → Google Authenticator (QR) → scannez le code QR.
3. Supprimez les codes de Google Authenticator une fois l'import terminé.

Étape 4 : Ajoutez un nouveau compte 2FA

1. Sur le site web : activez la 2FA → "Application d'authentification".

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

2. Scannez le code QR avec Aegis.
3. Saisissez le code à 6 chiffres sur le site pour confirmer.

Étape 5 : Sauvegardez votre fichier Aegis

1. Dans Aegis : Menu → Exporter → Chiffré (recommandé).
 2. Choisissez un mot de passe de sauvegarde (différent du mot de passe d'ouverture).
 3. Enregistrez le fichier .aegis dans un endroit sûr (Nextcloud, Cryptpad, clé USB).
-

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

Pourquoi Ente Auth ?

- Open-source avec audits indépendants.
- Synchronisation chiffrée de bout en bout entre tous vos appareils.
- Sauvegarde automatique (plus besoin d'exporter manuellement).
- Interface moderne et très intuitive.
- Import depuis Google Authenticator, Aegis, Authy...

Comment faire ? (Pas à pas)

Étape 1 : Installez Ente Auth

- Android : Aurora Store ou F-Droid → "Ente Auth"
- iPhone : App Store → "Ente Auth"
- Ordinateur : ente.io → téléchargez l'application de bureau

Étape 2 : Créez un compte

1. Lancez Ente Auth.
2. Cliquez sur "Créer un compte".
3. Entrez une adresse email.

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

4. Créez un mot de passe fort (stockez-le dans Bitwarden – fiche N°16).
5. Vérifiez votre email (code de confirmation).

Étape 3 : Importez vos codes existants

- Depuis Google Authenticator : Exporter → QR code → Ente Auth : Importer → QR code
- Depuis Aegis : Exportez fichier .aegis → Ente Auth : Importer → Aegis JSON

Étape 4 : Ajoutez un nouveau compte 2FA

1. Sur le site web : activez la 2FA → "Application d'authentification".
2. Scannez le QR code avec Ente Auth.
3. Saisissez le code sur le site pour confirmer.

Étape 5 : Vérifiez la synchronisation

- Ajoutez un code sur votre téléphone.
- Ouvrez Ente Auth sur votre ordinateur ou votre autre téléphone.
- Le code doit apparaître automatiquement.

6. Méthode C : Proton Authenticator (Android, iOS, Desktop, Web – écosystème Proton)

Pourquoi Proton Authenticator ?

- **Open-source** : code auditable, transparent .
- **Chiffrement de bout en bout** : même Proton ne peut pas voir vos codes .
- **Multiplateforme complet** : iOS, Android, macOS, Windows, Linux, et web .
- **Aucun compte Proton requis** : utilisation locale possible .
- **Synchronisation optionnelle** : via compte Proton, protégée par E2EE .
- **Import facile** : depuis Google Authenticator, Aegis, Authy, etc. .
- **Juridiction suisse** : lois de protection de la vie privée solides .

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

•**Sauvegarde automatique** : activable .

Limite : application jeune (lancée en 2025), écosystème en construction .

Comment faire ? (Pas à pas)

Étape 1 : Installez Proton Authenticator

Appareil	Action
Android	Aurora Store ou F-Droid → "Proton Authenticator" (ou Play Store en dernier recours)
iPhone	App Store → "Proton Authenticator"
Ordinateur	proton.me/authenticator → téléchargez l'application de bureau (Windows/Mac/Linux)

Étape 2 : Configurez l'application

1.Lancez Proton Authenticator.

2.Vous pouvez utiliser l'application **sans compte Proton** (mode local).

3.Pour la synchronisation, connectez-vous à votre compte Proton (ou créez-en un).

4.Activez la protection biométrique ou par code PIN.

Étape 3 : Importez vos codes existants

•Depuis Google Authenticator : Exporter → QR code → Proton Authenticator : Importer → QR code

•Depuis Aegis : Exportez fichier .aegis → Proton Authenticator : Importer → Aegis JSON

•Depuis Authy : pas d'import direct → désactivez puis réactivez la 2FA sur chaque compte

Étape 4 : Ajoutez un nouveau compte 2FA

1.Sur le site web : activez la 2FA → "Application d'authentification".

2.Scannez le QR code avec Proton Authenticator.

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

3.Saisissez le code sur le site pour confirmer.

Étape 5 : Activez la synchronisation (optionnel)

- Connectez-vous à votre compte Proton.
- Vos codes se synchronisent automatiquement entre tous vos appareils.
- Le chiffrement est de bout en bout : Proton ne peut pas voir vos codes .

Étape 6 : Activez la sauvegarde automatique (recommandé)

- Menu → Paramètres → Activer les sauvegardes automatiques.
 - Vos codes sont sauvegardés sur les serveurs Proton, chiffrés de bout en bout .
-

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

Priorité	Type de compte	Exemples
Critique (à faire en premier)	Email principal	Proton Mail, Tuta Mail, Gmail (si vous le gardez), Outlook
Critique	Gestionnaire de mots de passe	Bitwarden, Proton Pass
Élevée	Cloud / Drive	Nextcloud, Cryptpad, pCloud
Élevée	Réseaux sociaux	Mastodon, Twitter (si vous l'utilisez), Reddit
Élevée	Banque / Finances	Comptes bancaires en ligne, PayPal
Moyenne	Messageries	Signal (optionnel), Element (via Matrix)
Moyenne	Comptes techniques	GitHub, GitLab, AWS, Google Developer
Basse	Forums, sites d'actualités (si vous y tenez)	

Règle d'or : Tout compte qui a accès à votre email ou à votre argent doit avoir la 2FA activée.

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

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

1. Allez dans les paramètres de sécurité du compte.
 2. Cherchez "Authentification à deux facteurs" / "2FA" / "MFA" / "Authenticator app".
 3. Sélectionnez "Application d'authentification" (pas SMS, pas email).
 4. Scannez le code QR avec Aegis, Ente Auth ou Proton Authenticator.
 5. Saisissez le code à 6 chiffres généré pour confirmer.
 6. **Notez les codes de récupération** (backup codes) : stockez-les dans votre gestionnaire de mots de passe (fiche N°16) ou sur un papier dans un coffre. Sans ces codes, si vous perdez votre téléphone, vous ne pourrez plus accéder à votre compte.
-

8. Codes de récupération (backup codes) – À ne pas négliger

Lorsque vous activez la 2FA sur un site, le site vous fournit des codes de récupération (généralement 8 à 10 codes à usage unique).

Que faire de ces codes ?

Action	Explication
Stockez-les dans Bitwarden (fiche N°16)	Sécurisé, accessible depuis tous vos appareils.
Imprimez-les (sur papier)	Conservez dans un endroit sûr (coffre, enveloppe scellée).
Ne les stockez pas dans le même appareil que votre 2FA	Sinon, vous perdez tout en même temps.

Sans codes de récupération : si vous perdez votre téléphone (Aegis/Ente/Proton), vous êtes définitivement verrouillé hors de vos comptes.

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

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

Critère	Aegis	Ente Auth	Proton Authenticator
Open-source	✓	✓	✓
Sans compte	✓ (zéro cloud)	× (compte requis, chiffré E2EE)	✓ (optionnel)
Sauvegarde automatique	× (manuelle)	✓ (chiffrée)	✓ (chiffrée)
Synchronisation multi-appareils	× (manuelle)	✓ (native)	✓ (native)
Application bureau	×	✓ (Windows/Mac/Linux)	✓ (Windows/Mac/Linux)
Version web	×	✓	✓
iOS	× (Android seulement)	✓	✓
Import depuis Google Authenticator	✓	✓	✓
Export chiffré	✓ (.aegis)	✓ (fichier JSON chiffré)	✓
Juridiction	UE (open-source)	UE (open-source)	Suisse
Idéal pour	Contrôle total, zéro cloud	Multi-appareils, simplicité	Écosystème Proton, multi-appareils

10. À savoir avant de se lancer

Crainte fréquente

"C'est trop compliqué, je vais me verrouiller hors de mes

La réalité

C'est la peur principale. Avec des codes de récupération sauvegardés (Bitwarden + papier), vous êtes protégé.

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

Crainte fréquente

La réalité

comptes."

Commencez par un compte non critique (ex: forum) pour tester.

"Si je perds mon téléphone, je perds tout."

Non : si vous avez sauvegardé vos codes de récupération et/ou exporté Aegis / utilisé Ente Auth / Proton Authenticator, vous pouvez récupérer vos comptes.

"Est-ce que je dois activer la 2FA sur tous mes comptes ?"

Commencez par les comptes critiques (email, gestionnaire de mots de passe, banque). Ensuite, progressivement, sur les autres.

"Aegis n'est pas sur iPhone, que faire ?"

Utilisez Ente Auth ou Proton Authenticator (disponibles sur iOS).

"Ente Auth stocke mes codes sur leurs serveurs, est-ce sûr ?"

Oui, le chiffrement est de bout en bout. Ente ne peut pas voir vos codes. Et vous pouvez auto-héberger si vous ne faites pas confiance.

"Proton Authenticator stocke mes codes sur leurs serveurs, est-ce sûr ?"

Oui, le chiffrement est de bout en bout. Proton ne peut pas voir vos codes . Et vous pouvez utiliser l'application sans compte Proton, en local .

11. Challenge 7 jours

Challenge : Pendant 7 jours, activez la 2FA sur trois comptes critiques (email, gestionnaire de mots de passe, et un autre service important).

Jour 1-2 : Choisissez votre application (Aegis, Ente Auth ou Proton Authenticator) et installez-la.

Jour 3 : Activez la 2FA sur votre email principal.

Jour 4 : Activez la 2FA sur votre gestionnaire de mots de passe (Bitwarden / Proton Pass).

Jour 5 : Activez la 2FA sur votre cloud (Nextcloud, Cryptpad, ou autre).

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

Jour 6 : Sauvegardez vos codes de récupération dans Bitwarden.

Jour 7 : Vérifiez que tout fonctionne (déconnectez-vous, reconnectez-vous avec 2FA).

Vous allez constater :

- La 2FA n'ajoute que 5 à 10 secondes par connexion.
 - Votre sécurité est multipliée par un facteur énorme.
 - Avec Aegis (fichier local), Ente Auth ou Proton Authenticator (synchronisation), vous ne redoutez plus la perte de votre téléphone.
-

12. Alternatives et approfondissements

Si vous avez besoin de...	Essayez plutôt...
Une clé physique (sans téléphone)	YubiKey (hardware token, plus coûteux mais plus sécurisé)
2FA sur vos comptes Proton	Proton Mail, Drive, VPN, Pass supportent la 2FA via application ou clé
Une solution open-source auto-hébergée	Ente Auth (auto-hébergement possible) ou Aegis + Syncthing
Codes 2FA sur votre ordinateur uniquement	Ente Auth ou Proton Authenticator (application bureau) ou KeePassXC (intégré aux mots de passe)
Vérifier que la 2FA est activée sur vos comptes	twofactorauth.org (annuaire des sites supportant 2FA)

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

13. En résumé (ce que vous gagnez)

Action	Bénéfice
Utiliser Aegis (Android)	2FA open-source, fichier local chiffré, zéro cloud, contrôle total
Utiliser Ente Auth (Android/iOS/Desktop)	2FA synchronisée, sauvegarde automatique chiffrée, interfaces modernes
Utiliser Proton Authenticator (Android/iOS/Desktop/Web)	2FA open-source, E2EE, multiplateforme, Suisse, écosystème Proton
Quitter Google Authenticator	Plus de code closed-source, plus de risque de perte (sauvegarde ou synchronisation)
Activer la 2FA sur votre email	Votre boîte aux lettres protégée même si mot de passe volé
Activer la 2FA sur votre gestionnaire de mots de passe	Tous vos mots de passe protégés par un second facteur
Sauvegarder vos codes de récupération	Sécurité ultime : vous pouvez récupérer vos comptes même sans téléphone

Conclusion générale

Si vous êtes...	Choisissez...
Android uniquement, contrôle total	Aegis
Multi-appareils (Android + iPhone + ordinateur)	Ente Auth ou Proton Authenticator
iPhone uniquement	Ente Auth ou Proton Authenticator
Déjà utilisateur Proton (Mail, Drive, VPN, Pass)	Proton Authenticator

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V2.0

Si vous êtes...

Débutant, voulez de la simplicité

Exigeant / paranoïde, zéro cloud

Choisissez...

Proton Authenticator ou **Ente Auth**
(synchronisation automatique)

Aegis avec sauvegardes manuelles

À retenir absolument

- La 2FA transforme un compte vulnérable en compte robuste. Sans 2FA, votre mot de passe suffit à un pirate. Avec 2FA, il lui faut aussi votre téléphone.
 - **Les codes de récupération sont aussi importants que votre mot de passe.** Stockez-les dans Bitwarden (fiche N°16) et sur papier.
 - **Google Authenticator est à éviter** (pas de sauvegarde, closed-source). **Aegis, Ente Auth** et **Proton Authenticator** sont meilleurs et plus respectueux.
 - **Proton Authenticator** est une option récente mais solide : open-source, E2EE, multiplateforme, Suisse, et utilisable sans compte Proton .
 - **Commencez petit** : un seul compte (email). Une fois que le réflexe est pris, passez aux autres.
-

Test final

1. Installez Aegis, Ente Auth ou Proton Authenticator.
2. Activez la 2FA sur votre compte email (Proton Mail, Gmail, Outlook, etc.).
3. Sauvegardez les codes de récupération dans Bitwarden.
4. Déconnectez-vous, reconnectez-vous avec le code 2FA.
5. Si vous réussissez : félicitations, vos comptes sont désormais bien plus sécurisés.