

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

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 ou Ente Auth).

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 (email, banque, réseaux sociaux) 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) V1.0

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 (Ente Auth), et zéro collecte de données.

2. Les deux applications recommandées

Application	Open-source	Sauvegarde	Synchronisation	Cloud	Idéal pour
Aegis (Android uniquement)	✓ Oui	✓ Chiffrée (fichier local)	✗ Manuelle (fichier à synchroniser)	Non (fichier local)	Utilisateurs Android qui veulent le contrôle total
Ente Auth (Android, iOS, Linux, Windows, macOS)	✓ Oui	✓ Chiffrée (automatique)	✓ Native (chiffrée E2EE)	Oui (serveurs chiffrés)	Utilisateurs multi-appareils

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

Application	Open-source	Sauvegarde	Synchronisation	Cloud	Idéal pour
iOS, Desktop)				Ente, open-source, audits)	(iPhone + Android + ordinateur)

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	Synchronisation chiffrée de bout en bout, applications natives
Sur iPhone uniquement	Ente Auth	Aegis n'existe pas sur iOS
Débutant, vous voulez la simplicité avec sauvegarde automatique	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) V1.0

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** (écran suivant).
2. Dans Aegis : Menu → Importer → Google Authenticator (QR) → scannez le code QR affiché sur l'autre téléphone (ou la même capture d'écran).
3. **Supprimez les codes de Google Authenticator** une fois l'import terminé (vous ne l'utiliserez plus).

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

 **Attention** : Si vous ne faites que scanner le code, les codes restent dans Google Authenticator. Pensez à les supprimer ensuite.

Étape 4 (plus tard) : Ajoutez un nouveau compte 2FA


1. Sur le site web (ex: Google, Proton, GitHub) : activez la 2FA → choisissez "Application d'authentification".
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

C'est **l'étape la plus importante**. Si vous perdez votre téléphone sans sauvegarde, vous perdez tous vos codes.

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` (ou `.json` chiffré) dans un endroit sûr :

- **Option locale** : sur votre ordinateur (via USB ou transfert).
- **Option cloud chiffré** : dans un dossier Nextcloud (voir fiche N°7) ou Cryptpad Drive.
- **Option hors ligne** : sur une clé USB conservée dans un endroit sûr.

 **Astuce** : Programmez un rappel mensuel pour exporter votre fichier Aegis vers votre ordinateur.

Étape 6 (optionnel) : Synchronisez avec d'autres appareils

Aegis n'a pas de synchronisation native. Pour utiliser les mêmes codes sur plusieurs appareils :

- **Méthode simple** : Exportez le fichier `.aegis` vers votre autre téléphone (manuellement).
- **Méthode avancée** : Utilisez Syncthing (voir fiche N°7) pour synchroniser le dossier Aegis.

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

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 (Android, iPhone, ordinateur).
- **Sauvegarde automatique** (plus besoin d'exporter manuellement).
- **Interface moderne** et très intuitive.
- **Import depuis Google Authenticator, Aegis, Authy...**
- **Serveurs open-source** : vous pouvez même auto-héberger votre instance Ente.

Comment faire ? (Pas à pas)

Étape 1 : Installez Ente Auth

Appareil	Action
Android	Aurora Store ou F-Droid → "Ente Auth" (ou Play Store en dernier recours)
iPhone	App Store → "Ente Auth"
Ordinateur	ente.io → téléchargez l'application de bureau (Windows/Mac/Linux)

Étape 2 : Créez un compte

1. Lancez Ente Auth.
2. Cliquez sur "Créer un compte".
3. **Entrez une adresse email** (votre email habituel ou un email dédié aux comptes sensibles).
4. **Créez un mot de passe fort** (stockez-le dans Bitwarden – fiche N°16).
5. Vérifiez votre email (code de confirmation).



Note de sécurité : Le mot de passe est chiffré en local avant d'être envoyé. Ente ne peut pas voir vos codes 2FA.

Étape 3 : Importez vos codes existants

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

Source	Méthode
Google Authenticator	Dans GA : Exporter → afficher code QR → Ente Auth : Importer → QR code
Aegis	Exportez fichier .aegis → Ente Auth : Importer → Aegis JSON
Authy	Pas d'import direct (bloqué) – voir solution ci-dessous

Cas Authy : Si vous venez d'Authy (propriétaire), vous devrez **désactiver puis réactiver** la 2FA sur chaque compte pour générer un nouveau QR code.

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 (quelques secondes de latence max).

Étape 6 (optionnel) : Activez la sauvegarde chiffrée

Par défaut, Ente Auth synchronise vos codes sur ses serveurs (chiffrés de bout en bout). Si vous voulez **une couche de sauvegarde supplémentaire** :

- Menu → Paramètres → Exporter → Sauvegarde locale (fichier chiffré).
- Conservez ce fichier dans un endroit sûr (Nextcloud, Cryptpad Drive, clé USB).

Étape 7 (optionnel) : Auto-hébergement d'Ente (avancé)

Si vous ne voulez pas utiliser les serveurs Ente :

```
git clone https://github.com/ente-io/ente
cd ente
docker-compose up -d
```

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

Pointez votre application Ente Auth vers votre propre serveur. Ceci est pour des utilisateurs avancés.

6. 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.

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 ou Ente Auth.
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.

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

7. 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 Auth), vous êtes définitivement verrouillé hors de vos comptes.

8. Tableau récapitulatif Aegis vs Ente Auth

Critère	Aegis	Ente Auth
Open-source	✓	✓
Sans compte	✓ (zéro cloud)	✗ (compte requis, mais chiffré E2EE)
Sauvegarde automatique	✗ (manuelle)	✓ (chiffrée)
Synchronisation multi-appareils	✗ (manuelle)	✓ (native)
Application bureau	✗	✓ (Windows/Mac/Linux)
iOS	✗ (Android seulement)	✓

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

Critère	Aegis	Ente Auth
Import depuis Google Authenticator	✓	✓
Export chiffré	✓ (.aegis)	✓ (fichier JSON chiffré)
Idéal pour	Contrôle total, zéro cloud	Multi-appareils, simplicité

9. À savoir avant de se lancer

Crainte fréquente	La réalité
"C'est trop compliqué, je vais me verrouiller hors de mes comptes."	C'est la peur principale. Avec des codes de récupération sauvegardés (Bitwarden + papier), vous êtes protégé. 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, 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 (disponible 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.

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

10. 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 ou Ente Auth) 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).

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) ou Ente (synchronisation), vous ne redoutez plus la perte de votre téléphone.

11. 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 (application bureau) ou KeePassXC (intégré aux mots de passe)

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

Si vous avez besoin de...	Essayez plutôt...
Vérifier que la 2FA est activée sur vos comptes	twofactorauth.org (annuaire des sites supportant 2FA)

12. 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
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
iPhone uniquement	Ente Auth
Débutant, voulez de la simplicité	Ente Auth (synchronisation automatique)

Fiche Pratique N°18 : Activez l'authentification à deux facteurs (2FA) V1.0

Si vous êtes...	Choisissez...
Exigeant / paranoïde, zéro cloud	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 et Ente Auth sont **meilleurs et plus respectueux**.
- **Commencez petit** : un seul compte (email). Une fois que le réflexe est pris, passez aux autres.

Test final :

- 1.Installez **Aegis** ou **Ente Auth**.
- 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** ✓