Activer DKIM

E-mail · https://kyzoe.be/fr/docs/activer-dkim/

Qu’est-ce que DKIM ?

DKIM (DomainKeys Identified Mail) ajoute une signature numérique à chaque e-mail envoyé depuis votre nom de domaine. Les serveurs de messagerie destinataires utilisent cette signature pour vérifier que l’e-mail provient réellement de votre nom de domaine et n’a pas été modifié en cours de route. Sans DKIM, votre e-mail risque beaucoup plus d’atterrir dans le dossier spam ou d’être refusé par Gmail, Outlook et Microsoft 365.

Conditions préalables

- Un compte d’hébergement actif chez Kyzoe avec accès à cp.vcloudhosting.eu
- Un service e-mail actif pour le nom de domaine
- Accès à la gestion DNS du nom de domaine (chez Kyzoe ou chez un registrar/fournisseur DNS externe)

Étape 1 — Connexion

1. Rendez-vous sur https://cp.vcloudhosting.eu
2. Connectez-vous avec votre adresse e-mail et votre mot de passe.
3. Dans le menu de gauche, cliquez sur **Websites** et sélectionnez le site web/le nom de domaine pour lequel vous souhaitez activer DKIM.

Étape 2 — Accéder aux paramètres e-mail

1. Dans le menu du site web sélectionné, cliquez sur **Email**.
2. Ouvrez l’onglet **Settings** (ou **Paramètres**).
3. Vous y voyez la configuration e-mail du nom de domaine, y compris la section **DKIM**.

Étape 3 — Activer DKIM

1. Réglez l’interrupteur **Enable DKIM** sur **activé**.
2. Enhance génère automatiquement une paire de clés et affiche l’enregistrement DNS correspondant.
3. Cliquez sur **Save** / **Enregistrer**.

Étape 4 — Ajouter l’enregistrement DNS

Enhance affiche maintenant un enregistrement TXT avec la structure suivante :

- **Type :** TXT
- **Nom / Hôte :** `default._domainkey` (ou le sélecteur affiché par Enhance, p. ex. `x._domainkey`)
- **Valeur :** `v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A...` (clé longue)
- **TTL :** 3600 (ou par défaut)

Situation A — Le DNS est géré dans le panneau de contrôle

Si la zone DNS de votre nom de domaine est hébergée chez Kyzoe/Enhance, l’enregistrement est dans la plupart des cas **créé automatiquement**. Vérifiez-le via **Websites → votre nom de domaine → DNS** et recherchez l’enregistrement `_domainkey`. S’il n’est pas présent, ajoutez-le manuellement avec les données ci-dessus.

Situation B — Le DNS est géré en externe (p. ex. Cloudflare ou registrar)

Copiez la valeur complète depuis le panneau de contrôle et créez l’enregistrement TXT manuellement chez votre fournisseur DNS.

Attention :

- Copiez la **totalité** de la clé, sans ajouter d’espaces ni de retours à la ligne.
- Certains panneaux DNS exigent que vous saisissiez uniquement `default._domainkey`, d’autres le nom complet `default._domainkey.uwdomein.be`. N’ajoutez pas le nom de domaine deux fois.
- Chez Cloudflare, l’enregistrement doit être réglé sur **DNS only** (nuage gris) — le proxy ne s’applique pas aux enregistrements TXT.

Étape 5 — Vérifier

Les modifications DNS peuvent prendre jusqu'à 24 heures pour se propager dans le monde entier, mais en pratique, cela prend généralement 5 à 30 minutes.

Vérifiez ensuite :

1. Via la ligne de commande :

```
dig TXT default._domainkey.uwdomein.be +short
```

2. Ou via un outil en ligne comme mxtoolbox.com/dkim.aspx (saisissez le nom de domaine et le sélecteur `default`).
3. Envoyez un e-mail de test à une adresse Gmail, ouvrez-le, puis cliquez sur les trois points → **Afficher l'original**. Pour **DKIM**, la mention `PASS` doit apparaître.

Recommandé : combinez avec SPF et DMARC

DKIM seul ne suffit pas. Pour une bonne délivrabilité, nous vous recommandons de configurer correctement les trois enregistrements :

- **SPF** (TXT sur `@`) : `v=spf1 include:spf.uwmailserver.be ~all`
- **DKIM** (TXT sur `default._domainkey`) : comme ci-dessus
- **DMARC** (TXT sur `_dmarc`) : `v=DMARC1; p=none; rua=mailto:dmarc@uwdomein.be`

Commencez avec DMARC sur `p=none` pour collecter des rapports, puis renforcez la politique ultérieurement vers `quarantine` ou `reject`.

Problèmes fréquents

- **DKIM reste sur "fail"**
  L'enregistrement DNS ne s'est pas (correctement) propagé, ou une ancienne clé se trouve encore dans la zone. Supprimez les enregistrements `_domainkey` obsolètes et vérifiez l'absence de fautes de frappe.
- **La clé est tronquée ou trop longue**
  Certains panneaux DNS tronquent les valeurs TXT longues. Dans ce cas, divisez la valeur en parties de 255 caractères maximum entre guillemets, ou utilisez un fournisseur DNS qui gère cela automatiquement (comme Cloudflare).

- **DKIM fonctionne pour le site web, mais pas pour les e-mails d’une plateforme externe**
  Si vous envoyez des e-mails via un service externe (Amazon SES, Mailchimp, un CRM …), ce service possède son propre sélecteur DKIM et son propre enregistrement. Ajoutez-le séparément — plusieurs enregistrements DKIM peuvent parfaitement coexister tant que les sélecteurs sont différents.
- **Les e-mails arrivent toujours dans les spams**
  Vérifiez que votre adresse IP ou votre nom de domaine ne figure pas sur une liste de blocage. Testez-le via mxtoolbox.com/blacklists.aspx.

Besoin d’aide ?

Contactez le support Kyzoe via support@kyzoe.be. Indiquez le nom de domaine et, si possible, les en-têtes complets d’un e-mail de test.