# Simple OTP Login — Guide d’utilisation

Actualités · https://kyzoe.be/fr/docs/simple-otp-login-guide-d-utilisation/

**Version 2.1.0 Des questions ou besoin d’aide ?** N’hésitez pas à nous contacter via hallo@kyzoe.be ou à visiter kyzoe.be.

## 1. Qu’est-ce que Simple OTP Login ?

Simple OTP Login remplace le système classique de mots de passe de WordPress par un **code de connexion à usage unique** envoyé automatiquement par e-mail. OTP signifie *One-Time Password* — un code qui n’est valable qu’une seule fois et qui expire automatiquement après utilisation ou à la fin de sa période de validité.

**Pourquoi est-ce mieux qu’un mot de passe ?**

Un mot de passe est quelque chose que vous retenez — et qui peut être oublié, deviné, volé ou divulgué. Un code à usage unique est créé au moment de la connexion et envoyé à une adresse e-mail à laquelle seul le propriétaire légitime a accès. Pas de mot de passe signifie aussi pas de mot de passe à voler.

**En résumé :**

- Les utilisateurs n’ont plus besoin de mot de passe
- La connexion se fait par e-mail — rapide et familière
- Les codes expirés sont automatiquement inutilisables
- Les attaques par force brute sont activement bloquées
- Entièrement configurable selon les besoins de votre site web

## 2. Comment fonctionne la connexion ?

Le processus de connexion se déroule toujours en deux étapes.

### Étape 1 — Demander un code

Le visiteur se rend sur la page de connexion et saisit son **adresse e-mail ou nom d’utilisateur**. Après avoir cliqué sur *Send login code*, l’extension envoie automatiquement un e-mail contenant un code de connexion à l’adresse correspondante.

### Étape 2 — Saisir le code

Le visiteur saisit le code reçu sur la page de connexion. Si le code est correct et encore valable, l’utilisateur est connecté et redirigé vers le tableau de bord ou la page de redirection configurée.

```
Page de connexion
    |
    ▼
[Saisir l’adresse e-mail ou le nom d’utilisateur]
    |
    ▼
E-mail envoyé avec le code de connexion
    |
    ▼
[Saisir le code sur la page de connexion]
    |
    ▼
Connecté ✓
```

> **Attention :** lorsque le paramètre *Require OTP login* est activé (paramètre par défaut), la connexion par mot de passe est entièrement désactivée pour tous les utilisateurs — administrateur compris.

## 3. Installation

### Via le tableau de bord WordPress (recommandé)

1. Allez dans **Extensions → Ajouter une extension**
2. Cliquez sur **Téléverser une extension**
3. Sélectionnez le fichier `simple-otp-login.zip`
4. Cliquez sur **Installer maintenant**, puis sur **Activer**

L’extension est opérationnelle dès son activation. La connexion par mot de passe est immédiatement désactivée.

### Manuellement via FTP

1. Décompressez le fichier zip sur votre ordinateur
2. Téléversez le dossier `simple-otp-login` dans `/wp-content/plugins/` sur votre serveur
3. Dans le tableau de bord WordPress, allez dans **Extensions** et activez *Simple OTP Login*

> ⚠ **Important avant l’activation**
>
> Assurez-vous que WordPress peut envoyer des e-mails avant d’activer l’extension. Si ce n’est pas le cas, vous ne pourrez plus vous connecter après l’activation, car le code de connexion n’arrivera jamais.
>
> Vous avez un doute ? Installez d’abord une extension SMTP comme *WP Mail SMTP* ou *FluentSMTP* et vérifiez que les e-mails arrivent bien. Vous pourrez ensuite activer Simple OTP Login en toute sécurité.

## 4. Paramètres — aperçu

Vous trouverez tous les paramètres dans le tableau de bord WordPress sous **Réglages → Simple OTP Login**.

La page des paramètres est divisée en quatre onglets :

| Onglet | Ce que vous y configurez |
|---|---|
| **General** | Longueur du code, période de validité, OTP obligatoire ou facultatif |
| **Email Settings** | Objet et contenu de l’e-mail contenant le code de connexion |
| **IP Blocks** | Aperçu des adresses IP bloquées, déblocage |
| **Login Log** | Consulter, filtrer et gérer toutes les tentatives de connexion |

## 5. Onglet : Général

*Réglages → Simple OTP Login → General*

Cet onglet détermine le comportement du code de connexion lui-même.

## Longueur du code

Choisissez le nombre de chiffres du code de connexion : **4**, **6** ou **8** chiffres.

| Choix | Exemple | Utilisation |
|---|---|---|
| 4 chiffres | `4829` | Seuil le plus bas — facile à recopier |
| 6 chiffres | `482971` | Par défaut — bon équilibre |
| 8 chiffres | `48297134` | Sécurité maximale — un peu plus de saisie |

La page de connexion adapte automatiquement les champs de saisie en fonction de la longueur choisie.

## Période de validité :

Combien de temps un code envoyé reste-t-il valable ?

| Choix | Explication |
|---|---|
| **5 minutes** | Plus strict — l'utilisateur doit être rapide |
| **10 minutes** | Par défaut — suffisant sans être trop long |
| **15 minutes** | Plus souple — davantage de temps en cas de livraison lente des e-mails |

Une fois la période écoulée, le code est inutilisable. L'utilisateur peut facilement demander un nouveau code via le bouton retour de la page de connexion.

**Recommandation :** utilisez 10 minutes comme paramètre par défaut. Envisagez 15 minutes si vos utilisateurs se plaignent régulièrement de codes expirés — cela peut indiquer une livraison lente des e-mails.

## OTP obligatoire (interrupteur)

Cet interrupteur détermine si la connexion par mot de passe reste possible.

**Activé (par défaut — recommandé)**

Le formulaire de connexion WordPress standard est entièrement masqué. La connexion par mot de passe est bloquée pour tous les utilisateurs. La seule façon de se connecter est d'utiliser le code à usage unique.

**Désactivé**

Le formulaire OTP s’affiche au-dessus du formulaire WordPress standard. Les utilisateurs peuvent choisir : se connecter avec le code ou avec leur mot de passe. Une ligne de séparation claire distingue les deux options sur la page de connexion.

> ⚠ **Avertissement :** lorsque l’interrupteur est désactivé, la connexion par mot de passe reste active. Une bannière d’avertissement jaune apparaît dans l’administration à titre de rappel. Nous recommandons de laisser l’interrupteur activé pour une sécurité maximale.

# 6. Onglet : Paramètres e-mail

*Réglages → Simple OTP Login → Email Settings*

Vous pouvez adapter ici l’e-mail que les utilisateurs reçoivent lorsqu’ils demandent un code de connexion.

## Objet et texte du message

Vous pouvez librement personnaliser l’objet et l’intégralité du texte du message. Le texte prend en charge des **variables** (également appelées *placeholders*) qui sont automatiquement remplacées par les bonnes valeurs au moment de l’envoi.

## Variables disponibles

| Variable | Est remplacée par |
|---|---|
| `{otp}` | Le code de connexion lui-même (p. ex. `482971`) |
| `{name}` | Le nom d’affichage de l’utilisateur |
| `{site}` | Le nom de votre site web |
| `{expires}` | Le nombre de minutes de validité du code |

**Obligatoire :** la variable `{otp}` doit toujours figurer dans le texte du message. Sans cette variable, l’utilisateur ne reçoit pas de code et ne peut pas se connecter.

## Aperçu en direct

Pendant que vous modifiez l’objet ou le texte du message, le panneau à droite (ou en dessous) affiche un **aperçu en direct** de l’e-mail tel que le destinataire le verra. Les variables y sont déjà

remplies avec des valeurs d’exemple.

### Rétablir le texte par défaut

Le bouton **Restore defaults** rétablit l’objet et le texte du message d’origine fournis avec l’extension. Une boîte de dialogue de confirmation s’affiche avant que la modification ne soit appliquée.

### Exemple d’e-mail par défaut

```
Objet : [Mon site web] Your login code

Hello Jan de Vries,

Your one-time login code is:

  482971

This code is valid for 10 minutes.

If you did not attempt to log in, you can safely ignore this email.

— Mon site web
```

> **Astuce :** vous souhaitez un e-mail entièrement en néerlandais ? Remplacez le texte du message par votre propre texte en néerlandais et utilisez les mêmes variables. Le bouton *Save settings* enregistre vos modifications.

## 7. Onglet : Blocages IP

*Réglages → Simple OTP Login → IP Blocks*

Lorsqu’une personne saisit à plusieurs reprises un code erroné, l’extension bloque automatiquement l’adresse IP de ce visiteur. Cet onglet vous donne un aperçu complet et vous permet de lever manuellement les blocages.

### Statistiques

En haut de l’onglet, vous voyez trois compteurs :

- **Currently blocked** — nombre d’adresses IP actuellement bloquées
- **Failed attempts** — adresses IP ayant des tentatives échouées mais pas encore bloquées
- **Total in log** — nombre total d’adresses IP enregistrées

## Adresses IP actuellement bloquées

Dans le tableau *Currently blocked IP addresses*, vous voyez pour chaque adresse IP :

| Colonne | Explication |
|---|---|
| IP address | L’adresse IP bloquée |
| Attempts | Nombre de tentatives échouées |
| Blocked until | Moment où le blocage expire automatiquement |
| Time remaining | Compte à rebours mis à jour en direct dans le navigateur |
| Last attempt | Moment de la dernière tentative |
| Action | Bouton pour lever immédiatement le blocage |

Le bouton **Unblock** lève le blocage d’une adresse IP spécifique. Le bouton **Unblock all** (en haut à droite du tableau) lève tous les blocages actifs en une fois — une boîte de dialogue de confirmation s’affiche.

## Adresses IP ayant des tentatives échouées (non bloquées)

Vous trouverez ci-dessous les adresses IP qui ont enregistré des tentatives échouées sans avoir encore atteint le seuil de 5 tentatives. Le bouton **Remove from log** permet de retirer une telle adresse de l’aperçu.

## Comment fonctionne le blocage automatique ?

Après **5 tentatives de connexion échouées consécutives** — que ce soit par des codes erronés ou par la demande d’un code pour un compte inexistant — l’extension bloque automatiquement l’adresse IP pendant **15 minutes**.

Une fois la durée de blocage écoulée, l’adresse est automatiquement débloquée. Vous n’avez rien à faire.

# 8. Onglet : Journal des connexions

*Réglages → Simple OTP Login → Login Log*

Le journal des connexions enregistre chaque tentative de connexion effectuée via l'extension — réussie ou échouée. Vous avez ainsi une vue complète de qui se connecte à votre site web et de toute activité suspecte éventuelle.

## Statistiques

En haut de l'onglet figurent quatre compteurs :

| Compteur | Signification |
|---|---|
| **Total attempts** | Toutes les tentatives de connexion du journal |
| **Successful** | Tentatives de connexion réussies |
| **Failed** | Tentatives échouées (code erroné, code expiré) |
| **Blocked** | Tentatives bloquées (l'IP ou le compte était déjà bloqué) |

## Consulter les entrées du journal

Pour chaque tentative de connexion, le tableau affiche les informations suivantes :

| Colonne | Explication |
|---|---|
| **Time** | Date et heure de la tentative |
| **User** | Nom d'utilisateur saisi |
| **IP address** | Adresse IP du visiteur |
| **Status** | Réussie / Échouée / Bloquée (code couleur) |
| **Reason** | Description de l'erreur en cas de tentative échouée |

Les lignes se distinguent visuellement par une bande de couleur à gauche :

- **Vert** — Connexion réussie
- **Orange** — Tentative échouée
- **Rouge** — Tentative bloquée

### Filtrer par statut

Les boutons de filtre au-dessus du tableau vous permettent de limiter l'affichage à un statut spécifique :

- **All** — toutes les tentatives
- **Successful** — uniquement les connexions réussies
- **Failed** — uniquement les tentatives échouées
- **Blocked** — uniquement les tentatives bloquées

### Pagination

Lorsqu'il y a beaucoup d'entrées, les résultats sont répartis en pages de 50 entrées. En bas du tableau, vous trouverez des boutons de navigation pour parcourir les pages.

### Définir la durée de conservation

Par défaut, les entrées du journal sont conservées pendant **30 jours**. Elles sont ensuite supprimées automatiquement. Vous pouvez modifier la durée de conservation entre **1 et 365 jours**.

Modifiez la valeur dans le champ *Keep log entries for* et cliquez sur **Save**.

### Vider le journal

Le bouton **Clear login log** supprime toutes les entrées du journal en une seule fois. Une boîte de dialogue de confirmation s'affiche. Attention : cette action est **irréversible**.

## 9. Formulaire de connexion sur votre propre page

Par défaut, Simple OTP Login affiche le formulaire de connexion sur la page de connexion WordPress standard (`/wp-login.php`). Si vous souhaitez afficher le formulaire sur votre propre page — par exemple une page aux couleurs de votre identité visuelle — vous pouvez utiliser le shortcode suivant :

```
[simple_otp_login_form]
```

Collez ce shortcode dans le contenu de n'importe quelle page WordPress. Le formulaire apparaît automatiquement à cet endroit. Si l'utilisateur est déjà connecté, le shortcode affiche un message indiquant qu'il est déjà connecté.

**Utilisation :**

1. Créez une nouvelle page (p. ex. *Connexion*)
2. Ajoutez le shortcode `[simple_otp_login_form]` dans l'éditeur
3. Publiez la page

> **Astuce :** vous pouvez aussi utiliser le shortcode dans des zones de widgets ou dans des constructeurs de pages comme Elementor ou Divi.

## 10. Sécurité — comment fonctionne la protection ?

Simple OTP Login comprend plusieurs couches de protection contre les abus.

### Codes à usage unique

Chaque code ne fonctionne qu'une seule fois. Après une saisie réussie, le code est immédiatement invalidé. Une personne qui intercepte ce même code ne peut rien en faire.

### Expiration automatique

Chaque code a une période de validité limitée (configurable : 5, 10 ou 15 minutes). Les codes expirés sont refusés — il est impossible de réutiliser un code expiré.

### Blocage du compte après des tentatives échouées

Après **5 codes erronés consécutifs**, le compte utilisateur est automatiquement verrouillé pendant **15 minutes**. Pendant ce verrouillage, aucun nouveau code ne peut être demandé ni saisi pour ce compte.

### Blocage IP

En plus du blocage du compte, l'adresse IP du visiteur est également bloquée après 5 tentatives échouées. Cela empêche quelqu'un de réessayer avec un nouveau compte.

### Confidentialité pour les comptes inconnus

Lorsque quelqu'un demande un code pour une adresse e-mail ou un nom d'utilisateur inexistant, l'extension affiche toujours le même message neutre : "*Si ce compte existe, vous recevrez un e-mail.*" Cela empêche les attaquants de découvrir quels comptes existent réellement sur votre site

web.

### Comparaison à temps constant (timing-safe)

Pour vérifier le code saisi, l'extension utilise une méthode spéciale (`hash_equals`) qui prend toujours le même temps, que le code soit correct ou non. Cela protège contre les *timing attacks* — des attaques qui tentent de deviner si un code est correct à partir du temps de réponse.

### Protection CSRF

Tous les formulaires sont protégés par un *nonce* WordPress — un jeton de sécurité à usage unique qui empêche des sites malveillants de soumettre des formulaires au nom de vos visiteurs.

## 11. Questions fréquentes

**Les utilisateurs peuvent-ils encore se connecter avec leur mot de passe ?**
Non, pas lorsque le paramètre *Require OTP login* est activé (par défaut). La connexion par mot de passe est alors entièrement bloquée. Vous pouvez modifier ce comportement dans l'onglet *General*.

**Que faire si je suis moi-même déconnecté par erreur et que je ne reçois pas d'e-mail ?**
Vérifiez d'abord votre dossier spam ou courrier indésirable. Si les e-mails n'arrivent jamais, demandez à votre hébergeur ou à Kyzoe de désactiver temporairement l'extension via FTP ou l'environnement d'hébergement, afin que vous puissiez vous connecter avec votre mot de passe et résoudre le problème d'e-mail.

**Que faire si un utilisateur n'a plus accès à son adresse e-mail ?**
En tant qu'administrateur, vous pouvez modifier l'adresse e-mail d'un utilisateur via **Comptes → Tous les comptes** dans le tableau de bord WordPress. L'utilisateur pourra ensuite se connecter avec la nouvelle adresse.

**Cela fonctionne-t-il aussi avec WooCommerce ou d'autres formulaires de connexion ?**
L'extension fonctionne sur la page de connexion WordPress standard. Pour les formulaires de connexion de WooCommerce ou d'autres extensions, nous recommandons d'utiliser le shortcode `[simple_otp_login_form]` sur une page distincte.

**Plusieurs utilisateurs peuvent-ils avoir la même adresse IP ?**
Oui, c'est possible dans des environnements de bureau ou sur des réseaux partagés. Si un utilisateur provoque le blocage d'un compte, l'adresse IP peut être temporairement bloquée pour

tous les utilisateurs de ce réseau. Vous pouvez débloquer manuellement l'adresse IP via l'onglet *IP Blocks*.

**Combien de temps les tentatives de connexion sont-elles conservées ?**
30 jours par défaut. Vous pouvez modifier cette durée dans l'onglet *Login Log* (de 1 à 365 jours).

**L'extension est-elle disponible en néerlandais ?**
L'interface d'administration est rédigée en anglais en vue de sa publication dans le répertoire WordPress.org. Vous pouvez entièrement rédiger en néerlandais l'e-mail que reçoivent les utilisateurs via l'onglet *Email Settings*.

**L'extension fonctionne-t-elle sur tout hébergement WordPress ?**
Oui, tant que WordPress version 5.8 ou supérieure est installé et que PHP version 7.4 ou supérieure est disponible. L'extension n'utilise aucun service externe — tout fonctionne sur votre propre serveur.

**Que se passe-t-il lorsque l'extension est supprimée ?**
Lors de la suppression via le tableau de bord WordPress, tous les paramètres de l'extension, le journal des connexions et la table de base de données sont automatiquement supprimés. Rien ne reste dans votre base de données.

*Simple OTP Login est développé et maintenu par Kyzoe.*