

[Pm Wiki](#) possède un système intégré de gestion d'accès par mots de passe à différentes parties du site. Ces mots de passe peuvent être appliqués à des pages individuelles, à des [groupes Wiki](#), ou à l'ensemble du site Wiki. Notez que les mots de passe ne sont qu'une petite partie de l'aspect sécurité d'un site Wiki, pour un aperçu global, consultez [Les Sécurités de PmWiki](#).

Les auteurs peuvent utiliser PmWiki pour ajouter des mots de passe aux pages individuelles et aux [WikiGroupes](#) comme décrit dans [Mots de passe](#). Cependant, [Les administrateurs Wiki](#) peuvent aussi appliquer des mots de passe grâce à des fichiers [de personnalisation](#) comme décrit ci-dessous.

## Les bases des mots de passe

Pm Wiki supporte plusieurs types d'accès aux pages wiki.

`read` est le mot de passe qui autorise la lecture des pages.

`edit` est celui qui autorise l'édition et la modification des pages.

`attr` est celui qui autorise l'initialisation et la modification des mots de passe pour les différents attributs (et potentiellement d'autres attributs futurs).

`upload` autorise la possibilité d'attacher des fichiers (si la fonctionnalité [Fichiers joints](#) est activée).

Enfin, il y a un mot de passe `admin` qui permet à l'administrateur de prendre la main sur tout mot de passe affecté à une page ou un groupe.

Par défaut, Pm Wiki a la configuration de mots de passe suivante:

- Les mots de passe `admin` et `upload` sont bloqués par défaut
- Les groupes Main et Pm Wiki ont un mot de passe `attr` bloqué (dans leurs pages [.Group Attributes?](#) respectives).
- Les pages dans le groupe Site sont bloquées contre l'édition, excepté [Site.Side Bar](#).

Un mot de passe `admin` peut être utilisé pour dépasser les mots de passe bloqués, sinon, aucun mot de passe ne permettra l'accès.

Regarder [Mots de passe](#) pour de l'information au sujet de l'application de mots de passe par page et par groupe. Le reste de cette page décrit l'application des mots de passe pour l'ensemble du site depuis le fichier `local/config.php`.

## Application de mots de passe au site entier

La première chose qu'un administrateur devrait savoir est d'appliquer un mot de passe `admin` au site. Ceci est réalisé par une ligne dans le fichier `local/config.php` comme ce qui suit:

```
$DefaultPasswords['admin'] = crypt('secret_password');
```

Notez que l'appel `crypt()` est requis pour cela -- Pm Wiki stocke et gère tous les mots de passe comme des objets cryptés. Voyez le [crypt section](#) dessous pour des détails sur l'élimination des mots de

passé en clair dans le fichier de configuration.

Pour restreindre l'édition du site entier à ceux qui connaissent le mot de passe "edit", Ajoutez une ligne comme suit au fichier *local/config.php*:

```
$DefaultPasswords['edit'] = crypt('edit_password');
```

De même, vous pouvez activer `$DefaultPasswords['read']`, `$DefaultPasswords['attr']`, et `$DefaultPasswords['upload']` pour contrôler les mots de passe par défaut `read`, `edit`, and `upload` pour le site entier. Les mots de passe par défaut sont utilisés seulement pour les pages qui n'ont pas de mot de passe actifs. De plus, chaque valeur `$DefaultPasswords` peut contenir une rangée de mots de passe:

```
$DefaultPasswords['read'] = array(crypt('alpha'), crypt('beta'));  
$DefaultPasswords['edit'] = crypt('beta');
```

Ces lignes signifient que "alpha" ou bien "beta" peuvent être utilisés pour lire les pages, mais seul le mot de passe "beta" accordera l'autorisation d'éditionner une page. Comme Pm Wiki retient n'importe quel mot de passe entré durant la session en cours, le mot de passe "beta" permettra à la fois la lecture et l'écriture des pages, tandis que le mot de passe "alpha" permet seulement la lecture. Une personne sans aucun mot de passe ne pourra consulter aucune page.

## Connexion avec Identification ( requière un nom d'utilisateur plus un mot de passe [AuthUser](#))

Contrairement à beaucoup de systèmes qui ont une méthode d'identification pour contrôler l'accès aux pages (c'est à dire, avec un *nom d'utilisateur* et un *mot de passe* pour chaque personne), Pm Wiki est par défaut un système à *mot de passe* comme décrit ci-dessus. En général les systèmes de ce type sont souvent plus faciles à maintenir car ils évitent les tâches administratif de création de comptes utilisateur, de récupération des mots de passe perdus et la gestion des droits accordés à chaque utilisateur.

Néanmoins, le script *authuser.php* de Pm Wiki ajoute au système à mot de passe un contrôle par couple nom d'utilisateur et mot de passe. Consultez [AuthUser](#) pour plus de détails sur la gestion des accès aux pages basées sur les identités d'utilisateurs.

## Trous de sécurité ...

Les administrateurs doivent planifier soigneusement comment sont utilisés les mots de passe afin d'éviter d'ouvrir accidentellement des trous de sécurité. Si votre Wiki est ouvert (quiconque peut lire et écrire), ceci ne semble pas un problème, **sauf**, un utilisateur malveillant ou maladroit pourrait créer un mot de passe de lecture à un groupe et ainsi rendre le groupe complètement inaccessible à tous. Au minimum, même un wiki ouvert doit posséder un mot de passe "administrateur" et "attr" (mots de passe) global au site définis dans le fichier *config.php*. Le fichier exemple *sample-config.php* distribué avec Pm Wiki indique que les groupes Pm Wiki et Main ont la fonction "attr" verrouillée par défaut, mais si quelqu'un crée un nouveau groupe, "attr" est déverrouillé. Un administrateur doit dans ce cas se rappeler qu'il faut définir des mots de passe "attr" pour chaque nouveau groupe (si souhaité). Une solution plus simple est d'inclure ces lignes dans le fichier

*config.php* :

```
$DefaultPasswords['admin'] = crypt('votremotdepasseadmin');  
$DefaultPasswords['attr'] = crypt('votremotdepasseattr');
```

Un des problèmes lié au fait d'utiliser la fonction `crypt()` pour coder les mots de passe dans *config.php* est que tous ceux qui peuvent lire ce fichier vont voir le mot de passe non crypté. Par exemple, si *config.php* contient

```
$DefaultPasswords['admin'] = crypt('monsecret');
```

alors le mot de passe "monsecret" est visible en clair pour d'autres. Cependant, un administrateur wiki peut obtenir et utiliser une forme cryptée d'un mot de passe directement en utilisant `?action=crypt` sur n'importe quelle adresse url de Pm Wiki url (ou simplement en allant sur [PasswordsAdmin?action=crypt](#)). Cette action présente un formulaire qui génère des versions cryptées des mots de passe à utiliser dans le fichier *config.php*. Par exemple, quand `?action=crypt` reçoit le mot de passe "monsecret", Pm Wiki renverra une chaîne du genre

```
$1$hMMhCdfT$mZSch.BJOidMRn4SOUUSi1
```

La chaîne renvoyée par `?action=crypt` peut alors être placée directement dans *config.php*, comme ceci:

```
$DefaultPasswords['admin'] = '$1$hMMhCdfT$mZSch.BJOidMRn4SOUUSi1';
```

Notez que la fonction *crypt* et les parenthèses sont supprimées, puisque le mot de passe est déjà crypté. Le mot de passe doit être entre apostrophes simples. Dans cet exemple le mot de passe est toujours "monsecret", mais quelqu'un ayant accès à *config.php* ne pourra pas le connaître en lisant le fichier. *Crypt* peut vous proposer des formes différentes pour un même mot de passe --ceci est normal (et augmente la difficulté à découvrir le mot de passe original).

## Supprimer un mot de passe

Pour supprimer totalement un mot de passe de site, comme le mot de passe pour les envois de fichiers, créer une variable vide:

```
$DefaultPasswords['upload'] = '';
```

Vous pouvez aussi utiliser le mot de passe spécial "nopass" (défini dans la variable `$AllowPassword`) via `?action=attr` pour avoir une page non protégée par mot de passe à l'intérieur d'un groupe protégé par mot de passe, ou un groupe non protégé par mot de passe avec un site doté d'un mot de passe global.

La suppression d'un mot de passe peut être faite dans la page `?action=attr` par le rajout :

@nopass

Ou pour seulement effacer des mots de passe spécifiques qui avaient été rajoutés au groupe :

clear

## Révocation ou invalidation d'un mot de passe

Si un mot de passe a été découvert et que l'administrateur veut annuler rapidement tous les usages de ce mot de passe sur un site, une solution rapide est d'écrire dans le fichier *local/config.php*:

```
$ForbiddenPasswords = array('secret', 'tanstaaf1'); if  
(in_array(@$_POST['authpw'], $ForbiddenPasswords)) unset($_POST['authpw']);
```

Ceci empêche "secret" et "tanstaaf1" d'être accepté comme un mot de passe d'autorisation valide, Quelque soit la page qui l'utilise.

## Voir aussi

- Le tableau \$HandleAuth, qui définit le niveau d'authentification requis pour effectuer une action.

<< [Per Group Customizations](#) | [Index doc admin](#) | [Authentification utilisateur](#) >>