

# PASSWORDMAKER

ONE PASSWORD TO RULE THEM ALL™



## PasswordMaker Help Manual

### Introduction

Thank you for your interest in **PASSWORDMAKER**. The purpose of **PASSWORDMAKER** is to enable you to securely and easily log in to Internet applications, such as websites, instant messaging, ftp, and others. With the proliferation of online resources, you probably have usernames and passwords for banks, bill pay systems, email accounts, credit card websites, instant messenger, investment accounts, photo sites, blogging tools, and countless others. Most people have a few passwords they use for all of these accounts because it's easier to remember just a few. But this is incredibly risky.

What if you could use passwords unique as fingerprints for each and every one of your accounts, yet not have to remember those fingerprints? **PASSWORDMAKER** does just that. By using complex mathematical formulae, **PASSWORDMAKER** outputs the same unique passwords for you each and every time you provide it with the same input. And these passwords *are unique* across the globe (providing they are of sufficient length).

But only a genius could memorize so many unique passwords. Don't write them down on sticky notes for others to find; no, **PASSWORDMAKER** calculates them for you over and over again -- as needed -- without storing them so they can't be stolen. And if you use more than one computer (for example, one at work and one at home), it's child's play to synchronize them. There's even an [on-line version](#) for times when you are at a public computer and can't install any software.

### The Basics

You provide **PASSWORDMAKER** two pieces of information: a "master password" -- that one, single master password you like -- and the [URL](#) of a website requiring a password (for internet applications without URLs, such as instant messaging, you can make up any URL you like; e.g., aolinstantmessenger.com). Through the magic of [one-way hash algorithms](#), **PASSWORDMAKER** calculates a [message digest](#), also known as a [digital fingerprint](#), which can be used as your password for the website. Although one-way hash algorithms have a number of interesting characteristics, the one capitalized on by **PASSWORDMAKER** is that the resulting fingerprint (password) does "not reveal anything about the input that was used to generate it." <sup>1</sup> In other words, if someone has one or more of your generated passwords, it is *computationally infeasible* for him to derive your master password or to calculate your other passwords. Computationally infeasible means even computers [like this](#) won't help! Other security features,

such as **PASSWORDMAKER**'s ability to paste generated passwords into web sites' password boxes, prevents hackers from using keyboard loggers and trojan horses to determine your passwords. For more details, visit the [FAQ](#).

### Installation and Start

Once you have successfully installed **PASSWORDMAKER**, there are three ways to open it:

- the **PASSWORDMAKER** option in the Tools menu
- the golden ring toolbar icon
- the <ctrl> ' shortcut key



For Mozilla and Netscape users, the toolbar icon is installed by default. For Firefox users, the toolbar icon must be manually added by using the View -> Toolbars -> Customize menu, and then dragging the golden ring icon on to the toolbar.

Once you've opened the extension using one of these methods, you are presented with the [Basic Options screen](#).

## Getting Started

When you go to a site which requires a password, **PASSWORDMAKER**, depending on the settings, will either auto populate the password field, let you right click on the password field and give you the selection **PasswordMaker** in the **context menu**. Then, depending on whether **PASSWORDMAKER** knows your master password, or not, it will prompt you for your master password and populate the password box on the site, or just populate the password box on the site.

Again, depending on your settings, the password populated in to the password field of the site will either be an account specific, or a default password.

After **PASSWORDMAKER** has been installed, you should decide whether you wish to log in to your online account, be it a bank account, a subscription type service, with an account / URL specific password, or a default password. The account specific password will be set up with a URL, so that **PASSWORDMAKER** knows to use those specific settings for the site with the URL set up.

Of course, **PASSWORDMAKER** can not and will not know your site specific password, unless you change the password of the site or service to the password generated by **PASSWORDMAKER**. You do this by logging in to the site in question and select to change the password on that site. Typically, you will supply your old password and then a new password, which you will have to enter again to confirm the new password. The old password, of course, is the one which you are currently using to log in to the site. To enter and to confirm the new password, you'll right click on the new password box and select **PasswordMaker** from the context menu and **PASSWORDMAKER** will paste the new password into these boxes. Then, once you submit the changes, you are ready to start using **PASSWORDMAKER** to log into the site.

## How to use PASSWORDMAKER

When you visit a site which requires a password, just enter your Username and right click on the password box and select **PasswordMaker**, to fill in your password, which is determined by your settings. Then, when you click on the login button, you will be logged into the site.



Here we describe the textboxes and buttons on the Basic Options dialog.

**At the top left** you will see a menu bar. Click [here](#) to learn about it.

### Master Password

Your ONE "password to rule them all". This password, when combined with a URL, hash algorithm, optional I33t-speak, username, and counter, is used to generate unique, site-specific passwords, as explained in the introduction.

### Master Password Storage Options

There are three options from which to choose:

- **Do not store master password** the master password is not stored anywhere at any time (memory or disk). This is the most secure option, but also the least convenient because you are prompted to enter the master password everytime a password is generated.
- **Store master password in memory (encrypted)** the master password is stored in the browser's memory but not on disk. This option provides a reasonable trade-off between security and convenience. You won't be prompted to enter the master password again until all browser instances have closed (disposing memory contents), and the browser is re-opened. The master password is encrypted in memory so that if it's written to disk by the operating system as part of a swap file/paging file, it can't easily be decrypted.

To erase the master password from memory, select the do not store master password option, or simply clear the master password field.

- **Store master password on disk and in memory (encrypted)** the master password is stored encrypted on the local hard drive and in memory. This option is the least secure but the most convenient. You won't ever be prompted to enter the master password when using this option. Note: although the encryption used to store the master password is strong, the encryption/decryption key is also stored on your local hard drive. This makes decryption of the master password relatively simple. You should not use this option unless either (a) you are the only person with access to the hard drive, or (b) you are comfortable with the master password possibly being decrypted by others.

To erase the master password and encryption key from disk and memory, select the do not store master password option, or simply clear the master password field.

### Using URL

This shows which URL is being used to generate the password.

### Generated Password

Shows the generated password. It'll be shown as plain text, or encrypted depending on your setting.

### Advanced Options

Clicking this button opens the Advanced Options dialog, explained [here](#).

### Help

This button displays the help page.

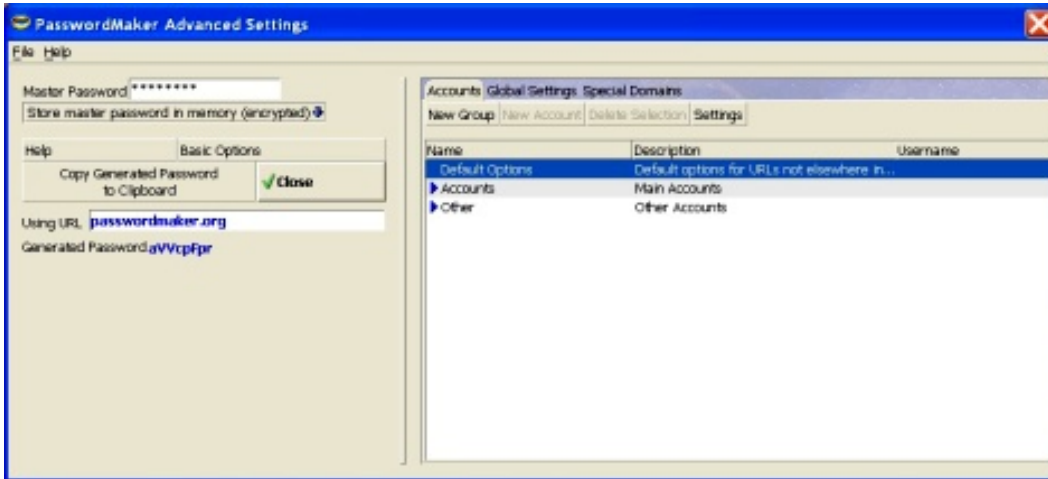
### Copy Generated Password to Clipboard

This button copies the generated password to the clipboard where it remains for the amount of time specified amount in the [Advanced Options](#) dialog (10 seconds by default).

### Close

This button closes the current dialog.

## Advanced Options



This interface is divided into two sections:

The left section is identical to the **Basic Options** dialog. The right section has the following three tabs:

### - The Accounts Tab

When the Accounts tab is selected, there are four buttons directly beneath the tabs. Initially, the only entry shown in the Name column is the Default Options account. The only two buttons that are activated/clickable are the New Group and the Settings buttons.

#### **New Group**

This button is used to set up a new group -- a container for accounts. When clicked, a dialog is displayed asking for the Folder/Group Name and description. Upon completion of this dialog, the newly-created folder is displayed in the Account Settings dialog along with its description (if one was supplied).

#### **New Account**

When a group is selected, the New Account button is activated/clickable. This button allows you to define custom password-generation settings for specific URLs that should be handled differently than all other ("default") URLs. When the button is pressed, a New Account entry is created and the **Account-Specific Settings** dialog is displayed.

#### **Delete Selection**

As the name indicates, this button delete the selected account or the selected group. Use caution here, however. If a group is deleted, all the accounts within that group are also deleted. You are prompted for confirmation before anything is deleted.

#### **Settings**

When the Settings button is pressed or an account is double-clicked, the PasswordMaker **Account-Specific Settings** dialog is displayed. This dialog allows you to define custom password-generation settings for the selected account; for example, how long the password should be for your email account at gmail.com.

### - The Global Settings Tab

Here you'll settings which apply to all of PasswordMaker. Currently, there are three checkboxes and one drop-down:

- **Mask Generated Password.** When checked, generated passwords are masked with asterisks so that they are not legible to the casual observer.
- **Auto-clear clipboard  $n$  seconds after copying it there.** This security feature prevents you from having to remember to clear the clipboard of generated passwords. If checked, the clipboard is automatically cleared  $n$  seconds after pressing the Copy to Clipboard button, where  $n$  is the value entered in the associated input field. However, before clearing the clipboard, PasswordMaker checks that nothing else has been copied there since the generated password. If something has been copied there since then, the clipboard contents are not cleared. This prevents other data in the clipboard from being overwritten.
- **Hide Master Password Field (number of asterisks)** This option causes the master password box to be completely concealed, thereby disabling the casual observer to determine the password length by counting asterisks.

Finally, there is also a drop-down box which says 'Action to take when **ALT-'** shortcut is pressed'. The four options are:

- Off, which means that pressing this shortcut has no effect.
- Populate all Password Fields, which means that all Password fields will be populated when **ALT-'** is pressed.
- Populate only password fields that are empty, which causes PasswordMaker to populate only empty password fields when **ALT-'** is pressed.
- Clear all password fields, which causes PasswordMaker to clear all the password boxes on a web page when **ALT-'** is pressed.

### - The Special Domains Tab

Some domains mandate the use of subdomains. The most common examples of this are **ccTLDs** (country code top-level domains), such as .uk. A domain in .uk never exists without a **SLD** (second-level domain), such as .co.uk.

Some domains even require third-level domains; for example, government departments in Australia must include a regional subdomain (e.g., .nsw for New South Wales) followed by .gov.au. In other words, government departments in New South Wales, Australia, must be in the .nsw.gov.au domain.

Finally, some countries issue domain names in both their ccTLD *and* in SLDs. Japan is an example: their ccTLD is .jp.

They issue domains in both .jp and .co.jp. (see <http://jprs.jp> and <http://jprs.co.jp>).

With the myriad possibilities for required subdomains, PasswordMaker can't account for them all. It includes some common ones -- the list of which grows from release to release (the *default* list). However, you are free to add/remove your own using the **Special Domains Dialog**. Your customizations to the special domains list are exported when using the **Export Preferences** feature, and imported when using the **Import Preferences** feature (providing the file being imported contains special domains). In this way, you can easily transfer customized lists to other PasswordMaker installations.

## Password Maker Menu

### Menu

#### - File Menu

##### + Import Settings

Reads a file created by Export Settings and applies the settings therein to PasswordMaker. If a master password is contained in the file, it is also applied.

##### + Export Settings

Writes a file containing all accounts, global settings, account-specific settings, special domains and, optionally, the master password. This file can be imported either by PasswordMaker On-Line or by using the Import Settings menu item described above. If you choose to write the master password to the exported file, it is written in encrypted form.

##### + Close

Closes the PasswordMaker dialog.

#### - Help Menu

##### + Help Contents

Displays this help manual.

##### + On-Line Version

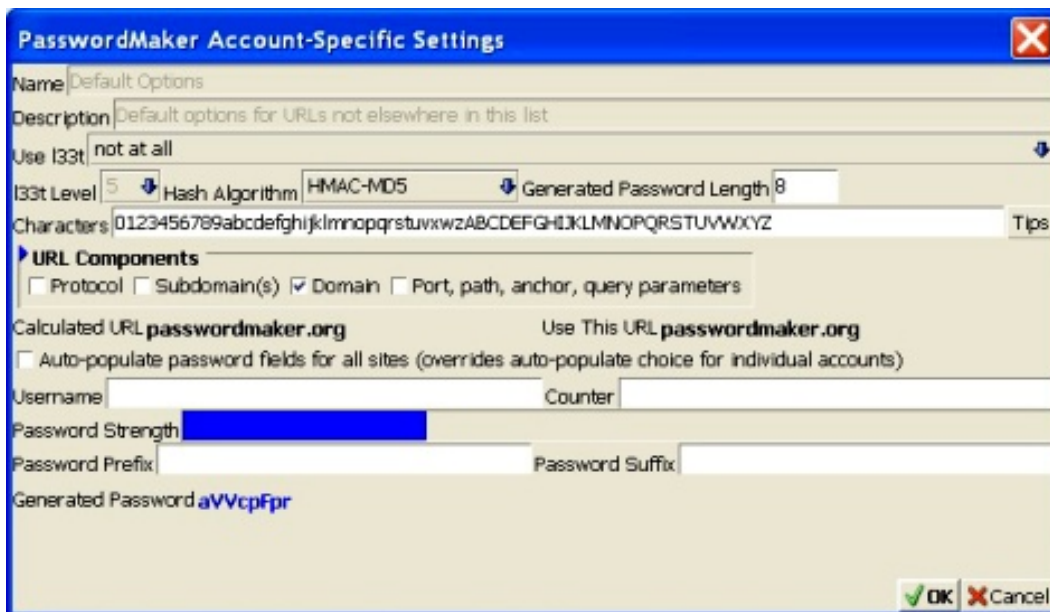
Opens the [on-line version](#) of PasswordMaker in a new browser tab. [PASSWORDMAKER Online](#) is an HTML- and javascript-only webpage duplicating most of the features in the PasswordMaker Mozilla/Firefox Extension. You can synchronize [PASSWORDMAKER Online](#) with settings from the PASSWORDMAKER Mozilla/Firefox Extension by using the Export Settings option (described above) and the Import Settings option found at [PASSWORDMAKER Online](#).

##### + About

Displays credits, attributions, and other information about PasswordMaker.

This is the place where all the important information is set up. We'll go through each one of those text- and dropdown-boxes.

## Default Settings



### Use I33t

Specifies when to apply **I33t** (also known as leetspeak), if at all. I33t can be applied not at all, to the unencrypted master password and URL only (i.e., *before* the hashing function has been applied), to the generated password only (i.e., *after* the hashing function has been applied), or to both the unencrypted master password and URL as well as the generated password (i.e., *before and after* applying the hashing function).

### Select I33t level

The complexity of I33t (also known as leetspeak) applied after the encrypted password has been generated. A side-effect of using I33t (in this version of PasswordMaker) is that all upper-case characters are converted to lower-case.

### Hash Algorithm

From this list, the encryption method used to generate passwords can be selected. All algorithms are **one-**

**way hash functions**, also known as message digests and fingerprints.

### **Generated Password Length**

The length, in characters, of the generated password. Be aware that some web sites specify a range for the allowed password length. Please note that the longer you make the password, the greater the security will be.

### **Characters**

The character set allowed in the generated password, even special characters may be specified. Again, be aware that some web sites disallow certain characters for the password.

### **URL Components**

This is where you specify the portion of the default site's URL you wish to use. We recommend that you just use the URL, but certain sites may require different components.

### **Calculated URL**

This is the URL, which PASSWORDMAKER calculated based upon your settings.

### **Use this URL**

This is the URL, which PASSWORDMAKER will use to combine with your master password to generate the site specific password.

### **Username**

This is an optional username field, where you can put a username.

### **Counter**

This is a place where you can put a character(s) for sites, which require you to change passwords periodically. When you enter a number / character here, it'll modify your password without you having to change any of the other settings.

### **Password Strength**

This indicator gives a visual representation of the password strength.

### **Password Prefix**

The letter(s) specified in this field will be put in front of the generated password.

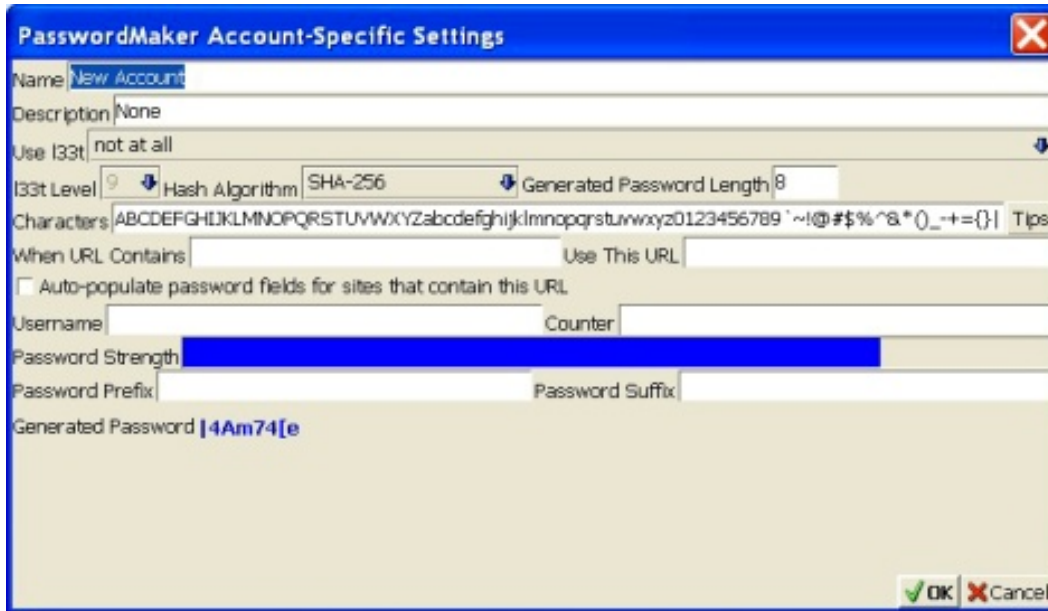
### **Password Suffix**

The letter(s) specified in this field will be put at the end of the generated password.

### **Generated Password**

This field displays the generated password. Optionally, this password can be masked by checking this option in the **Global Settings** tab, as explained earlier.

# Account Specific Settings



The screenshot shows a dialog box titled "PasswordMaker Account-Specific Settings". It contains several fields and options:

- Name: New Account
- Description: None
- Use I33t: not at all
- I33t Level: [dropdown]
- Hash Algorithm: SHA-256
- Generated Password Length: 8
- Characters: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789 `~!@#\$%^&\*()\_+={}| Tips
- When URL Contains: [text field] Use This URL: [text field]
- Auto-populate password fields for sites that contain this URL
- Username: [text field] Counter: [text field]
- Password Strength: [progress bar]
- Password Prefix: [text field] Password Suffix: [text field]
- Generated Password: |4Am74[e
- Buttons: OK, Cancel

## Name

This is a place for the name of this account.

## Description

Here is where the description of the account goes.

## Use I33t

Specifies when to apply **I33t** (also known as leetspeak), if at all. I33t can be applied not at all, to the unencrypted master password and URL only (i.e., *before* the hashing function has been applied), to the generated password only (i.e., *after* the hashing function has been applied), or to both the unencrypted master password and URL as well as the generated password (i.e., *before and after* applying the hashing function).

## Select I33t level

The complexity of I33t (also known as leetspeak) applied after the encrypted password has been generated. A side-effect of using I33t (in this version of PasswordMaker) is that all upper-case characters are converted to lower-case.

## Hash Algorithm

From this list, the encryption method used to generate passwords can be selected. All algorithms are **one-way hash functions**, also known as message digests and fingerprints.

## Generated Password Length

The length, in characters, of the generated password. Be aware that some web sites specify a range for the allowed password length. Please note that the longer you make the password, the greater the security will be.

## Characters

The character set allowed in the generated password, even special characters may be specified.

Again, be aware that some web sites disallow certain characters for the password.

## When URL contains

When the URL of the site being visited contains this portion, such as chase.com, PASSWORDMAKER knows these settings, this account.

## Use this URL

Tells PASSWORDMAKER to hash URL into the password.

## Auto-populate username and password

When checked, PasswordMaker prefills input boxes for you when a page loads. For example: say you have this option checked for an account you've created (not Default Settings...we'll get to that in a moment) where URL contains "yahoo.com". You then navigate to <http://mail.yahoo.com>.

PasswordMaker automagically fills in the "Username:" and "Password:" fields for you (based on what you've entered for that account). All you have to do is click submit.

If you select "Auto-populate username & password" in Accounts Tab->Defaults->Settings, then PasswordMaker uses whatever the default settings are to automatically fill username and password fields on **every page loaded EXCEPT those which match custom accounts you've defined** (i. e., "default overrides", like the custom account for "yahoo.com" discussed in the previous paragraph).

If more than one custom account matches the current URL, you're prompted for which to use.

Some people confuse *auto-populate* and *auto-complete*. Auto-complete, described [here](#), is when the browser offers to finish what you're typing with a list of previously entered information.

## Username

This field is optional, but when specified, it will also be hashed into the password.

## Counter

This is a place where you can put a character(s) for sites, which require you to change passwords periodically. When you enter a number / character here, it'll modify your password without you having

to change any of the other settings.

### **Password Strength**

This indicator gives a visual representation of the password strength.

### **Password Prefix**

The letter(s) specified in this field will be put in front of the generated password.

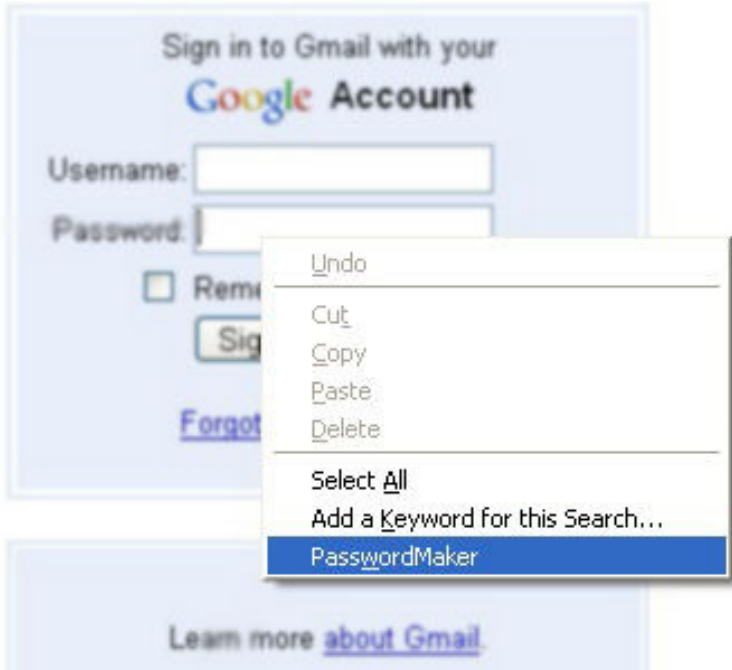
### **Password Suffix**

The letter(s) specified in this field will be put at the end of the generated password.

### **Generated Password**

This field displays the generated password. Optionally, this password can be masked by checking this option in the [Global Settings](#) tab, as explained earlier.

## Context Menu



### PasswordMaker

When the context menu is opened with focus on a password box and the *PasswordMaker* option is clicked, the appropriate password is generated and pasted into the password box. The "appropriate password" is determined by examining the **Default Account Settings** combined with any **Account-Specific Settings**.

Note: If you haven't saved your master password to memory or disk, **PASSWORMAKER** prompts you for the master password before populating the password box. It also gives you the option of storing the master password to memory or disk so you're not prompted again.