Sticky Password

Reviewer Guide - Core Functionality
Revision 1.0
November 17, 2014

Sticky Password is the **password manager** for the entire lifecycle of your passwords.

- *Strong passwords* – the built-in **password generator** prompts you to create strong, unpredictable passwords whenever you need them for registration and other online forms and your new login credentials are stored as new accounts are created.
- *Automatic login to website and applications* – just one click automatically launches your favorite password-protected websites and logs you in. Sticky Password also works with many applications too.
- *Import* – logins and passwords can be imported easily from popular browsers, as well as other password managers.
- *New websites are recognized* – as you login to new web accounts, Sticky Password automatically prompts you to create strong passwords, and then saves your new logins and passwords. No need to manually create records.
- *Security dashboard* – weak passwords are displayed in one place so you always know which accounts need better passwords to increase *your* security.

Sticky Password is the **form filler** that saves time by completing registration forms and online shopping cart data automatically and accurately.

- *Automatic profile creation* – when you fill in a registration form with your name, address, payment and other information, Sticky Password will prompt you to store the data as an **Identity** for future use.
- *One click form-filling* – any time you register or shop online, your saved Identity can be reused to fill the form automatically. Of course, you can save multiple Identities for each of your different roles in life e.g. one for personal use and one for work.

Sticky Password stores all your personal data.

- Sticky Password is more than a password manager and form filler. Your ID data, notes and personal information will be encrypted and safely synchronized within **Secure Memos** and accessible on all your devices.
- **Bookmarks** from your favorite browsers can also be stored and managed in one secure place.

Synchronize data across all your devices

If you're like most people today, you have multiple devices that you use to connect to the Internet – computers, tablets, and smartphones, and you need to have access to your passwords and data on all your devices. With Sticky Password, it's easy to securely backup and synchronize your data using cloud synchronization. Alternatively, if you are wary of cloud storage, you can take advantage of synchronization over your Wi-Fi or local network.

And with Sticky Password – unlike other password managers – **all your data is always encrypted locally and stored on your devices.**

Sticky Password uses AES-256, the leading encryption algorithm in the world to encrypt your data. AES-256 is so secure that it is used by the government and the military.

Basic concepts

Sticky Password supports all popular platforms – Windows, Mac, Android and iOS. Installing Sticky Password is straightforward and fast. The First Run Wizard will guide you through the basic settings, including setting up your StickyAccount and creating your Master Password.

In this guide, we'll highlight key elements of Sticky Password as you would come across them in a typical Windows installation. The concepts and terminology are generally applicable across Sticky Password platforms and key differences will be highlighted at the end of this document.

StickyAccount

You'll create your StickyAccount the first time you install Sticky Password. This is your personal admin account where you'll be able to manage your Sticky Password license and settings like your authorized devices, sync options and more. In other words, ***you will only have one StickyAccount regardless of how many devices you use with Sticky Password***.

StickyID – This is your email address that serves as your login name and will be your unique identifier for everything to do with your StickyAccount.

StickyPass – This is the password that you create to access your StickyAccount. (NOTE: This is not your Master Password that secures your password database.)

Your StickyAccount authentication info (StickyID and StickyPass) is automatically saved in your encrypted Sticky Password database. (Click the My StickyAccount tab in the Settings menu to login to your StickyAccount.)

Synchronization – you decide!

When it comes to synchronizing and backing up your data, Sticky Password allows you to decide whether you'd like to take advantage of our secure cloud to synchronize and back up your encrypted database or if you would prefer to keep your data only on your devices. You'll be prompted to enable or disable synchronization via the cloud during installation. You'll also be able to change your selection from the main Sticky Password interface at any time (for more information, see Synchronization options). If you prefer that your encrypted database never leaves the control of your devices, you can select local synchronization of your devices via your local Wi-Fi or local area network.

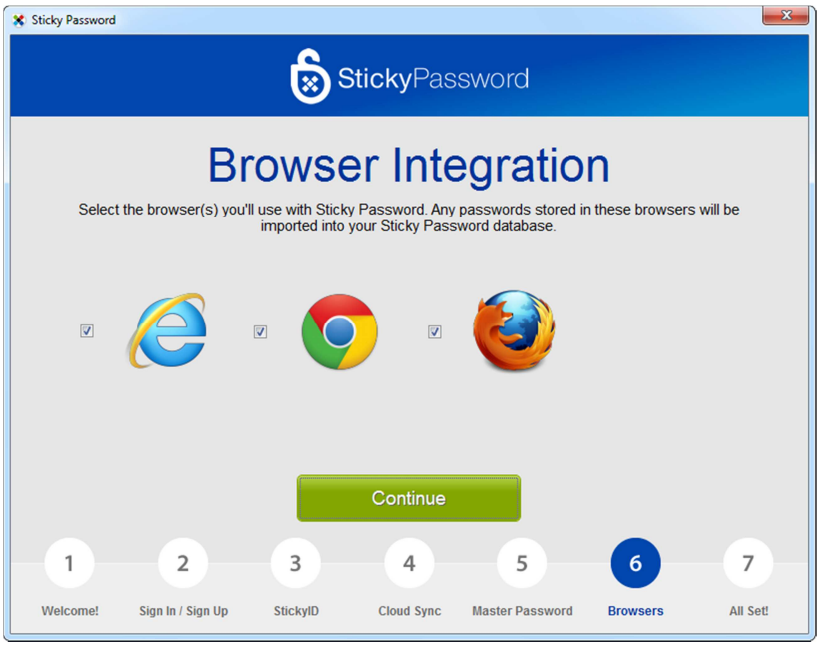
Master Password

Your Master Password is the key to your encrypted database. **Only YOU know your Master Password.** We never save it on our servers or send it over the Internet. If you forget or lose your Master Password, it cannot be resent to you. Be sure to choose a strong password that you will remember.

In general, the longer your Master Password, the better: We recommend that your Master Password should contain no fewer than 8 characters, and consist of a mix of upper and lowercase letters, numbers and special characters.

Browser integration – importing passwords

During the installation, you will be prompted to select the browsers from those identified on your computer that you would like Sticky Password to integrate with. During this step, appropriate plugins will be installed and any passwords and logins from your selected browsers will be imported into the database. If you decide to skip this step of the installation, Sticky Password will not be able to work with your browsers until you have installed the necessary plugins through the Settings menu.



Using Sticky Password

Unlock

To ensure the security of your passwords, Sticky Password won't let you forget to lock your database when you are away from your computer.

A popup dialog will prompt you to enter your Master Password to unlock the encrypted database. You can lock Sticky Password using the Lock or Exit options in the various menus. Sticky Password will also lock automatically when the Autolock inactivity timer expires. Users can set the duration of the timer in the Autolock setting in the Security section of the Settings menu.

When you return to your computer, simply enter your Master Password to unlock Sticky Password and resume using all the features.

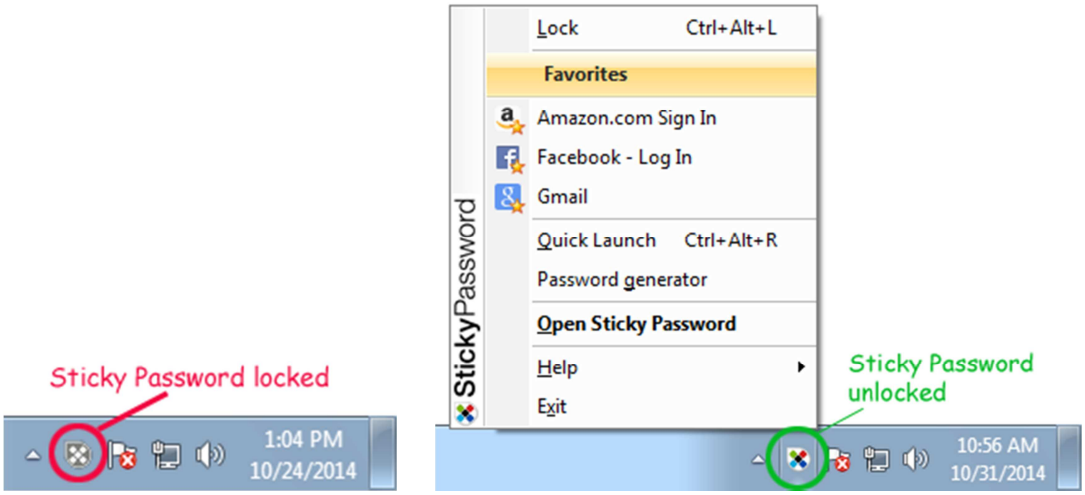
Tutorial

After installing Sticky Password, a short tutorial will appear to show you how to get the most out of your new password manager. You can return to the tutorial at any time by hovering over Help in the notification area menu (right click on the Sticky Password icon in the systray) and then choosing Tutorial.

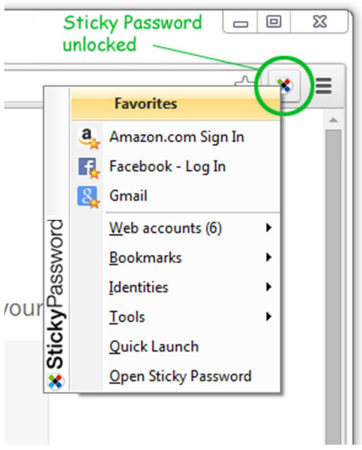
Notification area and Caption Button

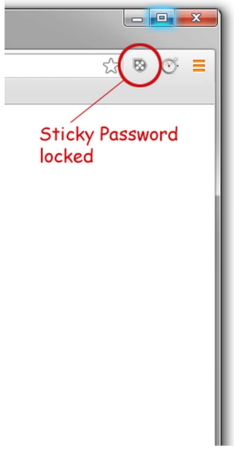
Sticky Password doesn't clutter your browser by installing an extra toolbar. Instead, you'll always have convenient access to Sticky Password in the notification area (AKA the systray) of your desktop, as well as in the caption area in the top right corner of your browser or application.

System Tray Notification Area



The Sticky Password Caption Button

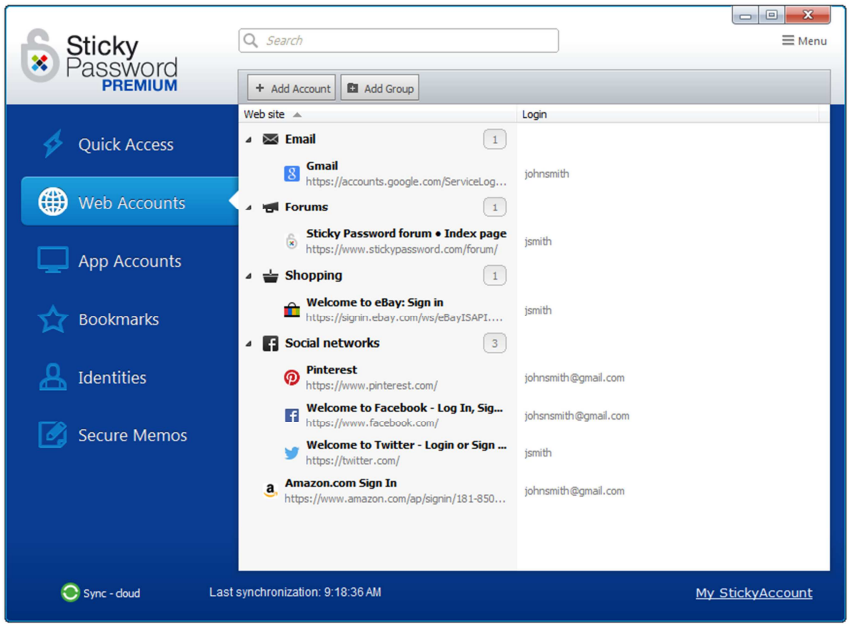




You'll know that Sticky Password is unlocked when the icon in the notification area or caption area appears in full color. Sticky Password is locked when the icon is displayed in gray, in which case, all you have to do to unlock it is to enter your Master Password. For your safety, Sticky Password can be set to be locked automatically after a specified period of inactivity on your computer. To unlock Sticky Password, you'll simply enter your Master Password.

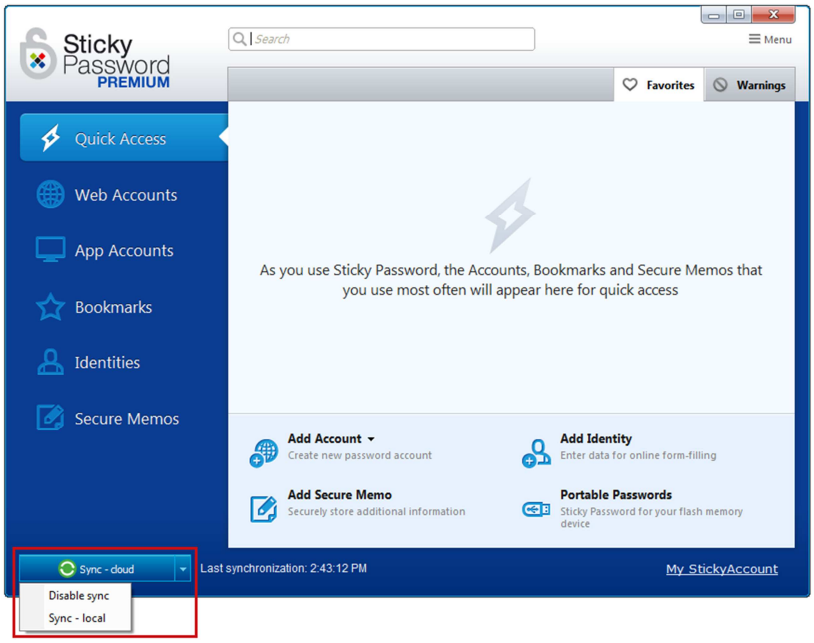
The Main User Interface

All your accounts and data stored in the encrypted database can be managed from the main user interface. Sticky Password integrates so well into your daily workflow and performs so many tasks automatically for you that you won't need to spend much time here at all.



Synchronization Options

During the installation, you were able to choose between enabling/disabling synchronization and backup via the secure cloud solution. You can change your selection at any time through the synchronization selector at the bottom left of the main user interface. Simply click on the green sync icon to reveal the drop down menu.



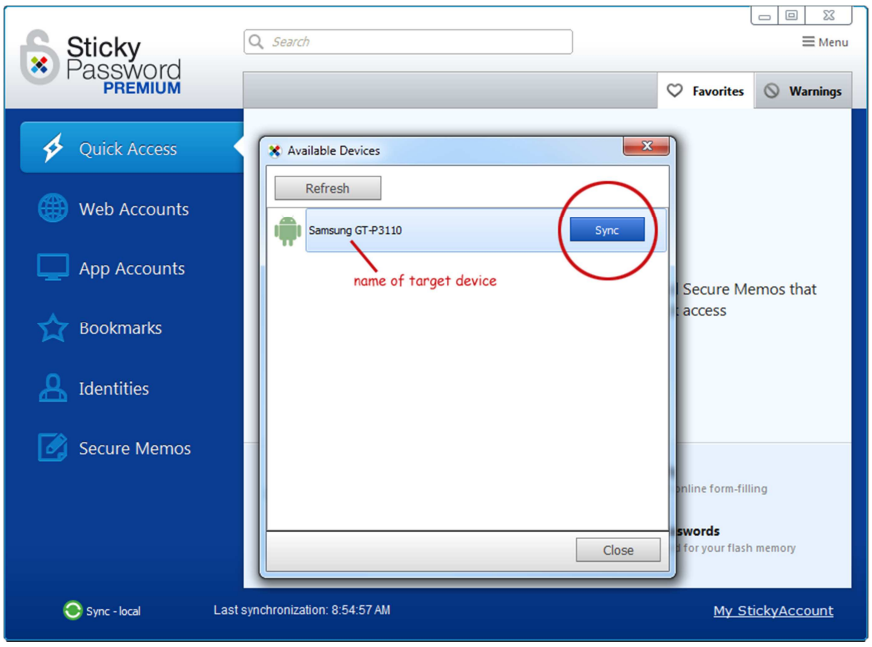
Choosing Sync-cloud allows you to take full advantage of backing up your encrypted database in the cloud, as well as synchronizing your passwords and data across your devices. Syncing via the cloud is the most convenient way to keep your passwords up-to-date on all your devices.

As the name suggests, Disable sync disables syncing with the cloud. No synchronization will take place and your encrypted database will be stored only on your local device.

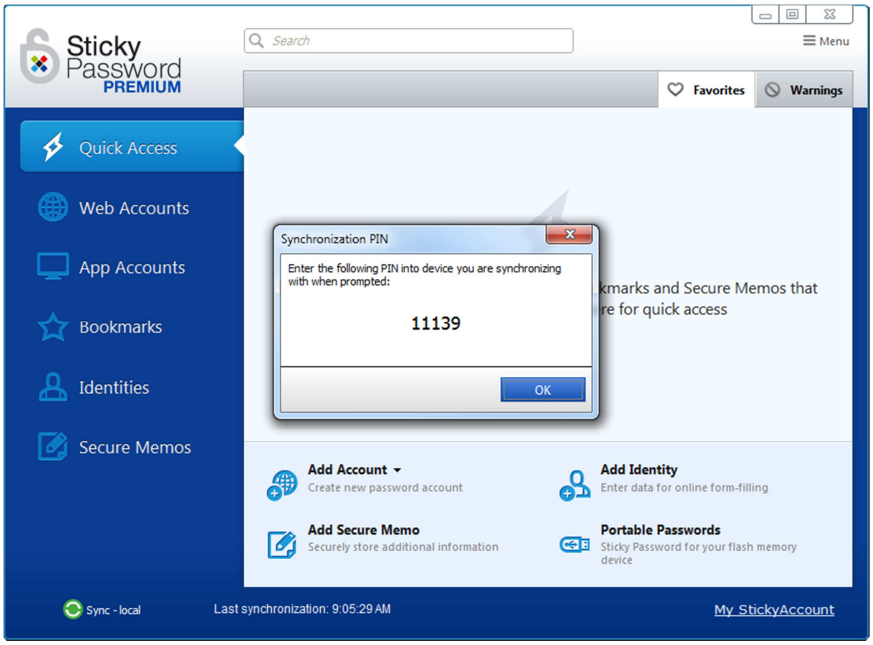
Sync-local is a unique new feature available on Sticky Password. Selecting this option allows you to sync your devices over your Wi-Fi or local area network: your encrypted database never leaves your devices.

Regardless of synchronization option you choose, all your data is always AES-256 encrypted whether stored in the cloud or locally. The storage and back-end systems utilize Amazon Web Services. Find out more about Sticky Password's cloud security in our White Paper.

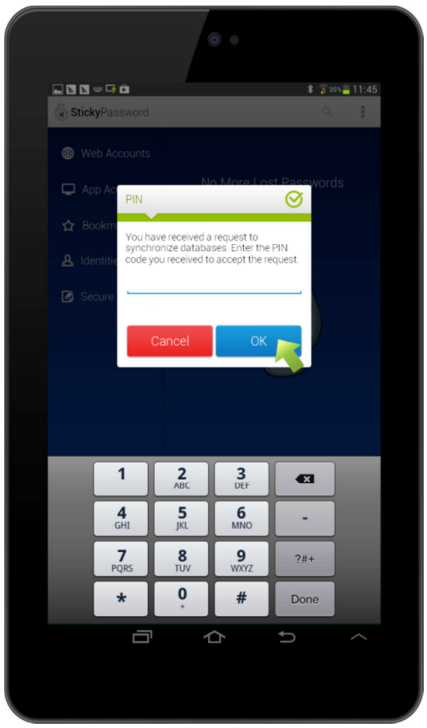
When selecting the Sync-local option to synchronize passwords via your local area network, all the devices that you would like to synchronize must be connected to the Wi-Fi or LAN. Begin by selecting Sync – local on all of the devices that you would like to sync. As you do this on additional devices, you will see the devices available for syncing – a pop-up window will appear showing all available devices.



Select the target device that you'd like to pair with in order to synchronize data and click Sync. Sticky Password will display a Synchronization PIN that you'll need to enter into the target device.



Entering this PIN when prompted in the target device will enable synchronization via Wi-Fi or your local network.

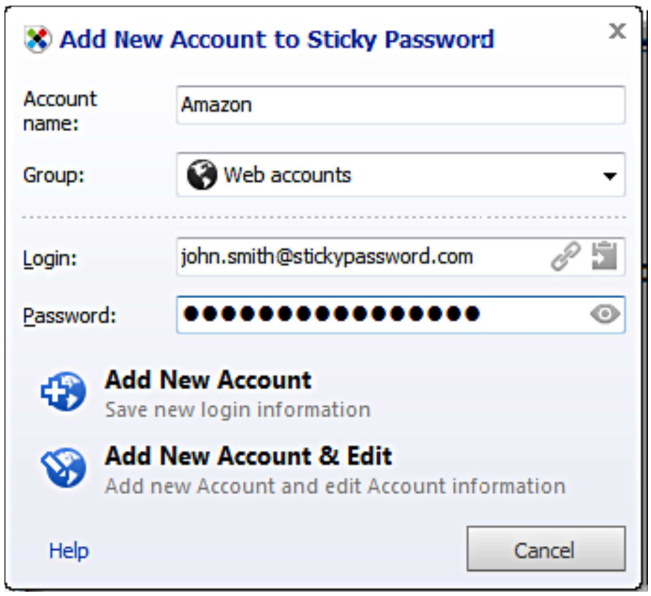


Your Accounts

New Web Accounts and Automated Login

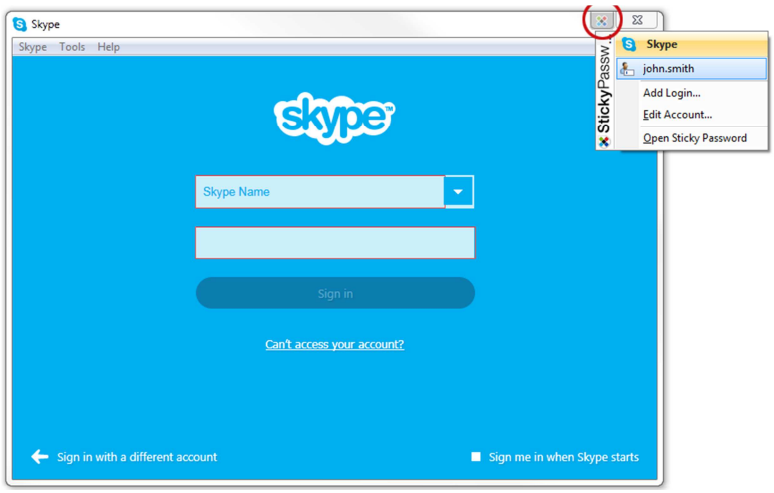
Adding new Web Accounts is easy. Just login to the website as you normally would by entering your username (login) and password (Sticky Password will offer to create a strong password in the password generator) and proceed to login. If the website or the specific login isn't already stored in the database, Sticky Password will prompt you to save the login credentials you just entered.

On subsequent visits to the website, Sticky Password will fill in your username and password and log you in automatically. Alternatively, if there are multiple logins saved for a particular website, you can choose one as the *automatic login*, or you can have Sticky Password prompt you to choose which login you'd like to use for that visit.



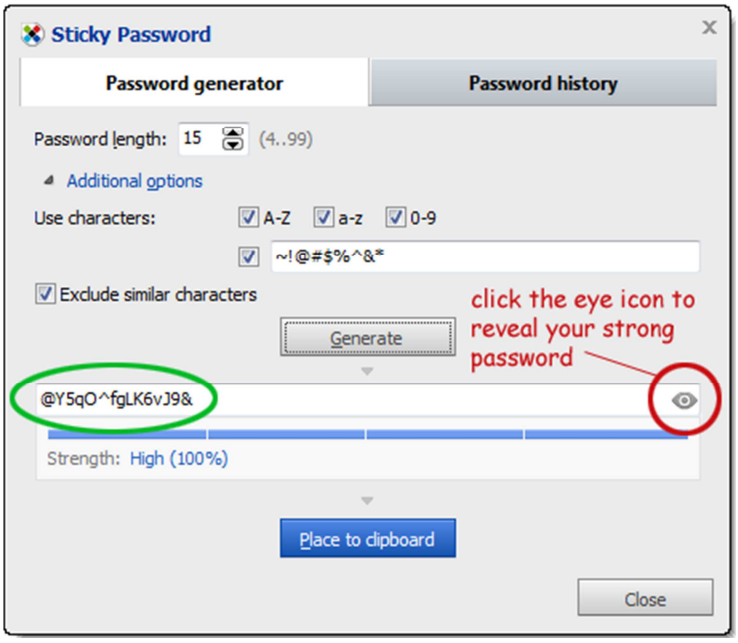
App Accounts

Sticky Password also works with popular applications. Launch the app you want to save in Sticky Password and click the Sticky Password Button in the app's caption area – select Add Account. Enter your login and password in the Sticky Password dialogue. Review the information and click Add New Account. The next time you launch the app, Sticky Password will automatically log you in.



Password Generator

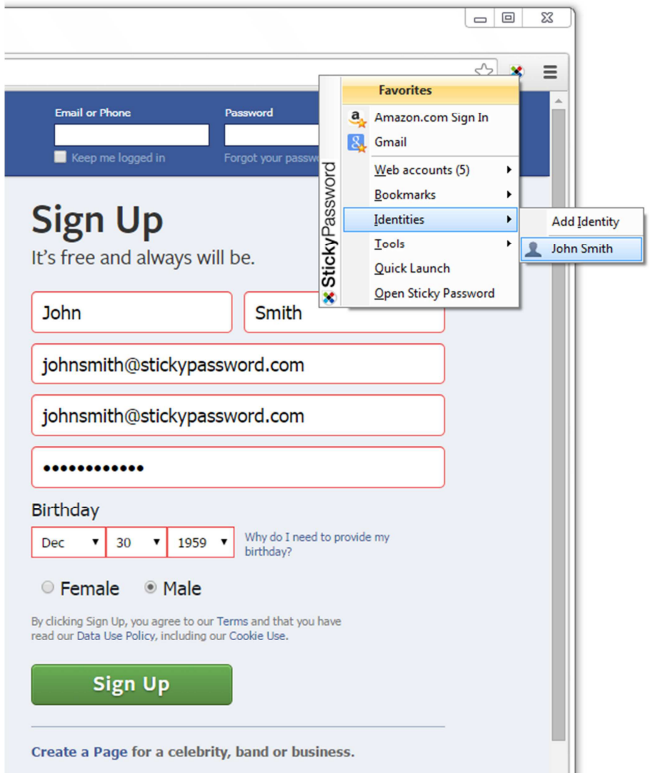
Whenever you create a new password or want to change an existing one, the password generator will generate a strong, hard-to-guess password – long and complex, combining letters, numbers, special characters and more – that can be saved in the target account within Sticky Password.



Form-filling with Identities

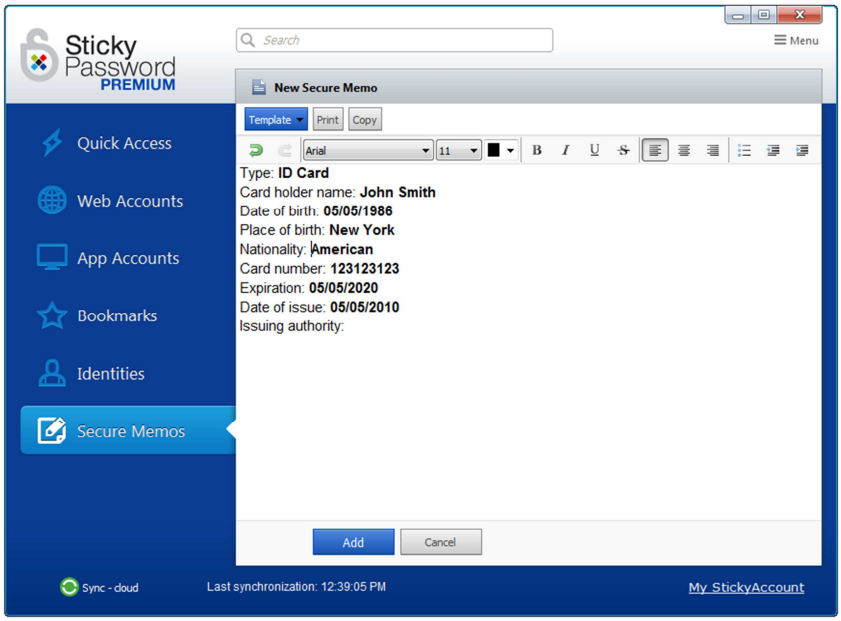
Adding Identities helps you automatically fill out long online forms. The next time you fill in an online form with your name, address, credit card and other personal information, Sticky Password will prompt you to save the data as an Identity. After that, this information will be used by Sticky Password to populate online forms for you. Sticky Password also allows you to store multiple form-filling Identities, so you can have one with your home address, a different one with your work information, and so on. If you prefer, you can enter your personal data directly into Sticky Password – just click on the Identities tab in the main user interface and then Add Identity to get started.

You'll be able to select the desired Identity to use the next time you're shopping online or when you need to complete an online form.



Secure Memos

If you are like most people, in addition to logins and passwords, and Identity data used for online form-filling, you have other data that would benefit from being stored securely on your devices. Examples are insurance policy numbers and details, passport numbers, and other ID and official document data that you'd like to have securely stored and with you on your device when the need arises. Sticky Password has a dedicated section called Secure Memos where you can store a wide variety of sensitive data that is easily accessible and securely stored on your device.



To find out about more Sticky Password features and how they can help you be more secure online, check out our video tutorials at http://www.stickypassword.com/help/tutorials.

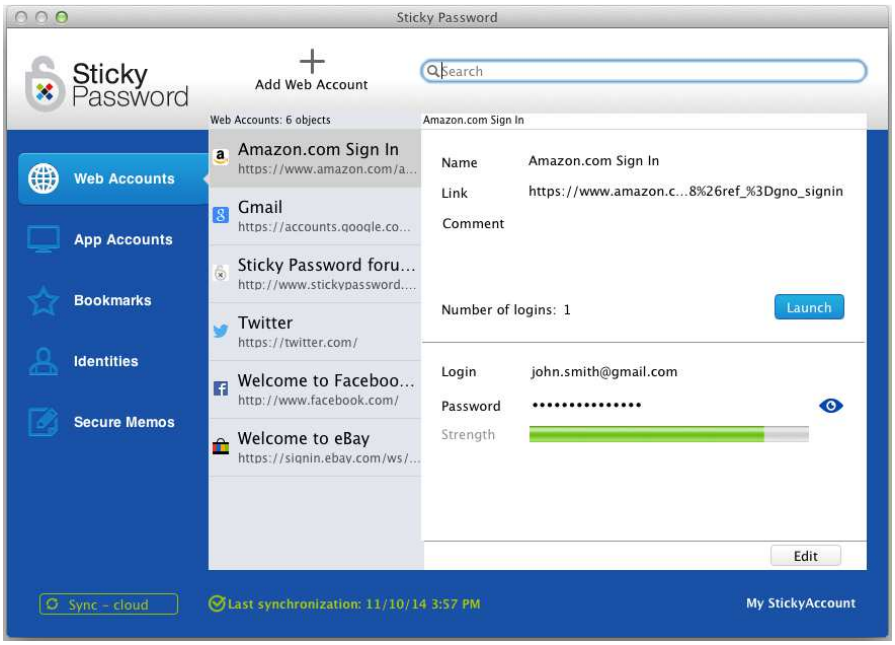
Apple Mac

In response to high customer demand, we've added support for Mac OS X to Sticky Password. Many customers have indicated their need to synchronize passwords and data across mixed Windows and Apple environments (not to mention iOS and Android – which are already supported).

The main graphical user interface (GUI) for Sticky Password for Mac closely mimics the Windows GUI. Sticky Password for Mac allows you to synchronize your password data with Apple's iCloud Keychain password management system by importing passwords stored in the Keychain and securely storing the data in the encrypted Sticky Password database. You'll be able to use Sticky Password to sync your Keychain passwords with your other devices (iOS, Windows or Android).

Synchronization between your various devices is performed either via the secure Sticky Password cloud or locally via your local Wi-Fi. (NOTE: Local sync on the Mac will be available at the time of the public release.)

The initial release of Sticky Password for Mac supports the Safari browser's native autofill capability that is integrated with the iCloud Keychain (other browsers may also include support for iCloud Keychain in the future). Native autofill support (using 'extensions') for additional browsers will be added in future releases of Sticky Password.



Installation on the Mac is very similar to installing Sticky Password on your Windows computer. You'll be prompted to sign into an existing StickyAccount, or to create a new one. As indicated earlier, your StickyAccount is the online administrative account that allows you to manage your devices that are authorized to access your encrypted database.

After choosing your preferred sync method (Enable cloud sync or Disable cloud sync), and creating your Master Password, you will be prompted to allow Sticky Password to sync data with your Keychain. The data from your Mac will be added to the Sticky Password database. After syncing with your encrypted database in the cloud, any passwords stored there will be imported to the Keychain. In this way, your database will always be comprehensive on all your devices. While surfing on the Internet, Safari will automatically fill in your logins and passwords via your Keychain.

Mobile devices

Sticky Password for mobile devices brings the password management experience onto the Android and iOS mobile operating systems. Sticky Password can be used as a standalone password management application on your mobile phone or tablet, or as a complementary utility on all your devices, giving you the ability to manage and access sensitive data whenever and wherever you need them.

We strive to keep the user experience as similar as possible across all our supported platforms. Still there are some differences due to the specificity of mobile device environments and associated limitations when compared to desktop computers. Following are the main functionality differences that are specific to mobile devices:

- Sticky Password for mobile includes an embedded Sticky Password browser for auto-fill of logins and passwords. Browser integration has not been a standard policy of mobile operating systems. Support for individual browsers will be added as these policies change.
- On Android only – the Sticky Password Floating Window allows you to easily fill in your logins and passwords into third-party browsers and applications.

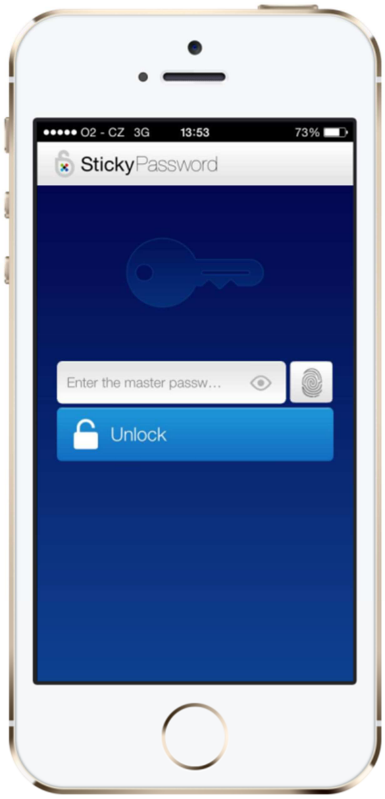
- In addition to the standard synchronization options described earlier, Sticky Password for mobile devices has additional settings for syncing including allowing Sticky Password to sync only when a Wi-Fi network is available. You can also elect to sync each time you launch Sticky Password or set it for manual synchronization.
- On mobile devices, we've added a PIN code option, as well as biometric options for even more convenient access when alternating between Sticky Password and other apps.

Biometric Authentication

Fingerprint Scanning

Sticky Password now supports biometric authentication on mobile devices equipped with fingerprint scanning capability. The Samsung S5 and the iPhone 5s, and higher versions of Android and iOS phones and tablets support fingerprint scanning. (Be sure to check with your phone or tablet manufacturer to see if your phone supports fingerprint scanning.)

To use the fingerprint scanning feature, unlock Sticky Password with your Master Password and go to Settings, choose App protection settings and enable Fingerprint Protection. You'll be able to set the time of the Alternate app protection duration. During the period of time you set, you'll be able to unlock Sticky Password simply with the swipe of your finger. It's fast, convenient and secure.



About Sticky Password

Sticky Password, founded in 2001, is a software utility that creates and organizes passwords to simplify a user's online life without compromising security. Sticky Password provides automatic login, one-click form filling, storage for personal data, and basic collaboration functionality for small groups. It brings "set and forget" password management technology to the world. Security leaders like Kaspersky Lab, among others, have selected Sticky Password to power elements of their own product solutions. Sticky Password is available at stickypassword.com and at major US retailers including Office Depot, Office Max, Sam's Club, Fry's, MicroCenter and Amazon.