



The Security Behind Sticky Password

Technical White Paper

Executive Summary

When it comes to password management tools, concerns over secure data storage of passwords and personal information are often cited as major reasons not to make use of such security products.

Sticky Password utilizes the latest in security and encryption technology to provide users with secure cloud (Amazon server) and local (device only) options for storing their password and other sensitive personal data. This document describes the security of the Sticky Password architecture, so that you can better understand how the software keeps your data secure.

We have also included recommendations on how to use our product to achieve the highest possible protection for your data.

System Architecture

The Sticky Password system architecture follows the standard client/server model, shown in the illustration below:

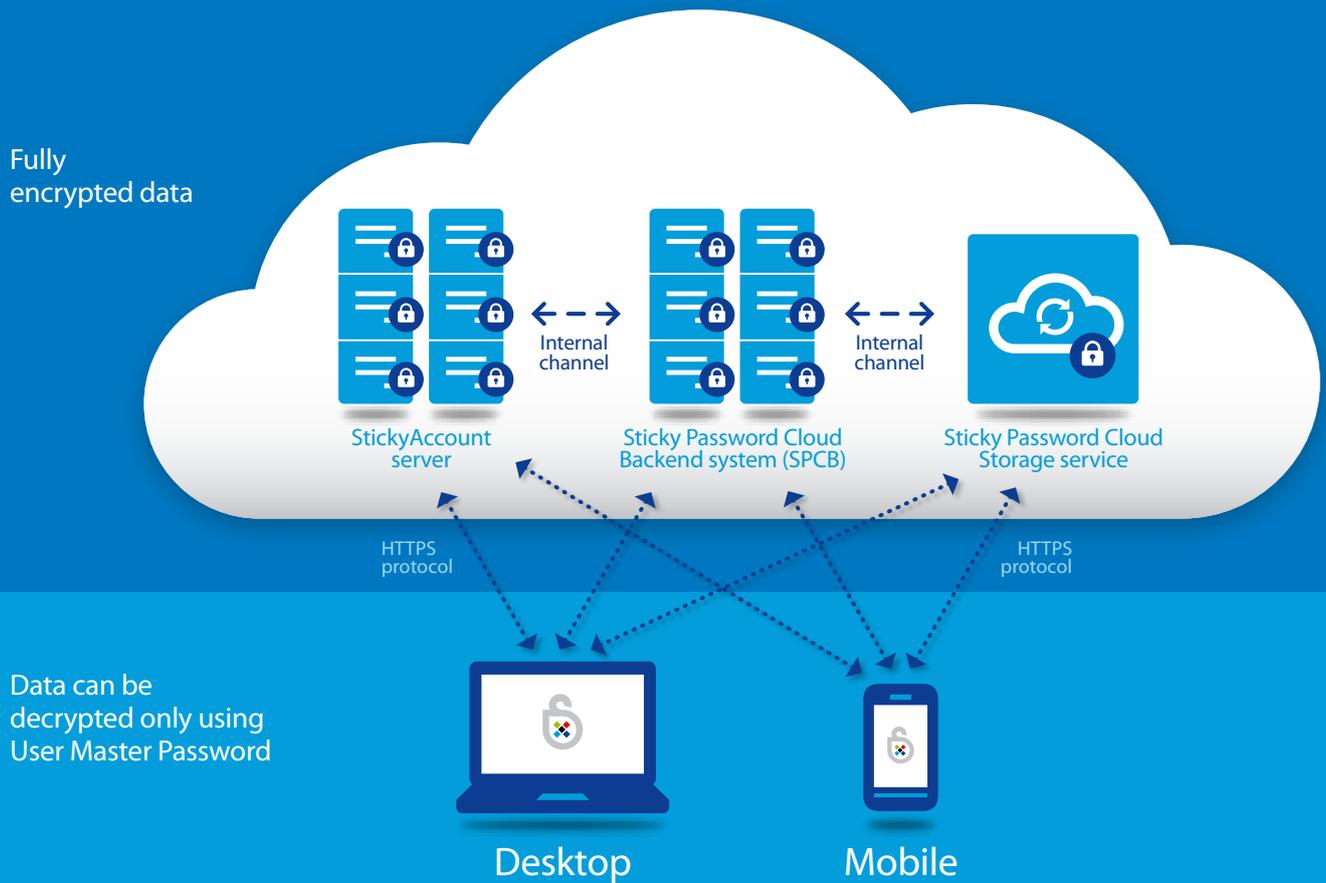


Figure 1: Sticky Password system architecture

The Sticky Password client is a client-side application that runs on various operating systems (the latest list is available on our website). The Sticky Password applications (installed on Windows, Mac OS, iOS, Android) share the same secure and reliable architecture, regardless of the platform on which they are running. As such, all Sticky Password applications are based on identical security principles and use the same strong cryptographic methodologies. The mobile platform (iOS and Android) applications, and the Windows and OS X versions utilize the same secure database architecture, encryption algorithms, and secure cloud synchronization services. Each Sticky Password license (subscription) can be applied to any number of supported physical devices belonging to a single user (NOTE: a user's database is accessible on all of his/her authorized devices). Synchroni-

zation of databases between devices covered by a single license is managed by the Sticky Password Cloud service; alternatively, locally via the local sync option.

The Sticky Password Cloud, the server side of the Sticky Password client/server configuration, is comprised of several functional blocks:

- A discrete protected storage space for synchronized data
- A back-end system that controls all synchronization operations
- A StickyAccount to enable secure usage of the client-side application

Note: that all password management functionality is accessible only through the client-side application.

The storage space and back-end system reside on secure Amazon AWS services (Amazon S3 and Amazon EC2). All stored data is also backed up to the user's local devices covered by the license.

Local synchronization

The latest version of Sticky Password introduces secure local synchronization of the encrypted database.



Figure 2: Local sync using Sticky Password

This option utilizes the user's Wi-Fi or local network – thereby ensuring that the transferred data (i.e. the encrypted database on each device) is always under the control of the user! Local sync occurs between two devices at a time. In effect, the encrypted database from each of the selected devices is passed to the other device over the local network, where it is then synchronized with the resident database.

Whether you choose the local sync or cloud sync option, whenever transmitting database information, Sticky Password works exclusively with the encrypted databases of the devices involved – never with unprotected data. Synchronization occurs locally at the device level.

Data Protection

Data protection in Sticky Password is based on two critical components:

1. The Master Password

- a. The Master Password is defined by each user, and is used to generate a unique encryption key, which is used to encrypt and decrypt the user's data (i.e. the password database) when accessed via the Sticky Password application. The encryption and decryption process is performed locally in the application only, never on the server side. The Master Password itself is not stored anywhere, either locally or in the cloud, nor is it transmitted over the Internet under any circumstances. For this reason, no-one, including Sticky Password staff, infrastructure administrators, or anyone other than the user has access to the Master Password. Users must take great care to ensure that their Master Password is not lost or forgotten as, without it, they will not be able to access their encrypted protected data.
- b. The industry standard AES-256 encryption algorithm is used for encrypting/decrypting user data (i.e. the password database). An encryption key is derived from the Master Password using the password-based key derivation function PBKDF2, which applies a pseudorandom one-directional function cryptographic hash to the unique Master Password together with a cryptographic salt (random data) in the thousands of cycles (iterations). This approach prevents any unwarranted retrieval of the Master Password.

2. User Account Credentials

A user's account credentials consist of the user's StickyID (user-supplied e-mail address) and StickyPass (user-defined password). These credentials are required for authenticated access to Sticky Password synchronization services for the user's authorized devices, and also to log into the StickyAccount.

These credentials are completely unrelated to the Master Password; they are used to authorize the addition of any new device or browser to the user's license and to authenticate synchronization services. All authorized devices store the user's StickyID and StickyPass credentials in the encrypted database along with other user account data, and the user can access the credentials after entering the Master Password, in the same way as any other protected user data.

For this reason, there is no need to remember these credentials, much less the need to manually enter them when accessing the StickyAccount; the Sticky Password application handles them in the background with no user intervention required. If users forget their credentials, they can retrieve them from the encrypted database - just like any other data. On the server side, the user's StickyID and StickyPass are stored in the database in encrypted form using a similar unidirectional crypto-function as described above and hashed in multiple iterations.

- The Device ID is a unique number generated by each device running the client-side Sticky Pass-

word application and stored on the server in encrypted form. It is used to identify each user device when accessing the synchronization services.

- A one-time unique access token is allocated to each authorized device to permit synchronization services for a limited time - in other words, a per-session authentication of each physical device is performed in the background.

Device Authorization

Before using Sticky Password synchronization, users must first activate their StickyAccount by creating both credentials – the personal StickyID and StickyPass. The Sticky Password application includes a wizard to walk users through this process, which also automatically authorizes the device to access synchronization services. Additional devices must be individually authorized to participate in the synchronization process.

Authorization is a one-time operation: authorized devices are added to the table of so-called Trusted devices on the server side and allowed to perform synchronization operations whenever necessary.

Three authorization modes are available:

- Basic authorization requires proper authentication using only the StickyAccount credentials.
- Extended authorization utilizes two-factor authentication using a one-time PIN (the second factor) sent to the user's StickyID email address in addition to the basic authorization requirements. For security reasons, the PIN must be entered on the target device within 15 minutes.
- Authorization of new devices is disabled is the most secure option and is recommended once all user devices have been authorized.

Once successfully authorized, devices use the Sticky Password synchronization services based on proper authentication using the StickyAccount credentials. This authentication is based on the user's StickyAccount credentials and processes running in the background and does not require any user intervention.

The device authorization modes can be set in the StickyAccount, where the user can also manage the user profile and other product security settings. In their StickyAccount, users are able to access a list of their authorized devices, disable (de-authorize) any or all devices in case of loss or theft of a device, see a history of device activity, delete all user data from the cloud storage, and change access credentials as well as the registered e-mail address. Access to the StickyAccount portal requires the same authorization process for each browser as for the authorization of new devices.

Communication and back-end security

Any data transmission channels over the Internet (between the physical device, the browser, and the server side) are secured by HTTPS using protocol TLS 1.1 and above, 256 bit encryption. Server side transmissions are verified by High Assurance SSL GeoTrust certificates.

Besides the encrypted communication channel, all protected user data sent via the Internet and stored on Sticky Password servers is in encrypted form, in this way protected data is doubly encrypted when being sent via the Internet.

The Sticky Password server side is hosted on [the Amazon AWS Infrastructure-as-a-Service \(IAAS\) platform](#). All measures taken by Amazon for both physical and platform security are described in the Amazon document "[Overview of security processes](#)".

The back-end system runs on the secure Amazon EC2/Virtual Private Cloud platform. In addition to the Amazon AWS physical and platform security, we have added our own application security layer, consisting of separate internal functional blocks protected by robust firewalls, internal communication channels secured by SSL, and other measures.

The Sticky Password server side uses high-availability architecture and avoids any single point of failure. In the unlikely event that there is a synchronization service outage, users can still access all protected data on their local devices; however, deploying newly entered data/accounts/passwords to other synchronized devices will not be possible for the duration of the outage.

Recommended Sticky Password Best Practices

The Master Password is the sole key to all protected user data. If lost or forgotten, users will be unable to access their database and all data will be lost. It should therefore be memorable for the user, but as hard as possible to guess by others, and also should not be stored anywhere. Here are some hints and tips on developing a complex password that is easily remembered but not easy for others to guess:

Do:

- Mix numbers, upper and lower case letters, and symbols.
- Make it convenient enough to type quickly to prevent others from seeing what you typed.
- Create it from a method that makes it easy to remember. Consider choosing a line from a favorite song or poem and using the first letter of each word in that line to generate the password. For example, "r-e-s-p-e-c-t, **F**ind **O**ut **w**hat it **m**eans **t**o **m**e" can be transformed into "rFOwim2m=". Add numbers or symbols to this to make it even harder to guess.
- Use two unrelated words and separate them with a punctuation mark, symbol or numbers; you could also reverse one or both of the words. For example "surf dent" would become fruS10*tned.

Don't:

- Use your StickyID in any form (reversed, capitalized, and certainly not as-is)
- Use your first, middle or last name, or your pet's, parent's, sweetheart's, or child's name

- Use a common dictionary word

Your StickyID and StickyPass are the keys to accessing your synchronization services. Your StickyID is your email address. Your StickyPass should follow the rules listed above for password complexity, but you do not need to remember this one – it is stored in your protected database within Sticky Password, and you can retrieve it using any of your authorized devices.

To prevent others from adding devices to your list of authorized devices, make sure you set the authorization mode in your StickyAccount Settings tab to “One-time PIN” and, after successfully authorizing your own devices, set the mode to “No new devices”.

When you replace or upgrade any device covered by your Sticky Password license, be sure to remove the old device from the list of authorized (Trusted) devices so it can't be used to access your account. Check your device list periodically for any unauthorized devices and take the following actions immediately if you find anything suspicious:

1. Change your StickyPass in the online Sticky Portal to prevent unauthorized synchronization
2. Disable the unknown device(s) in the Sticky Portal to exclude it from the synchronization process
3. Change the StickyPass in the application GUI on each device to reactivate the synchronization process.
4. Change the Master Password in the application GUI .
5. Perform manual synchronization on all other devices to encrypt the password database with the new Master Password

You should also follow this procedure if you suspect that your Master Password has been compromised. To be absolutely sure you've covered everything, you can purge and restore all encrypted data in the cloud:

1. Log into StickyAccount and select “Delete all cloud data” under the ‘Settings’ tab – this will remove all data from your Sticky Password cloud database, including older records encrypted by the older (and potentially compromised) Master Password.
2. Restore the Sticky Password cloud database from any local Sticky Password application. Bear in mind that this last step removes access to older user data encrypted by the previous Master Password.

Summary

As you can see, we have taken a great deal of care to ensure that your Sticky Password database is as secure in the cloud as it is on your local devices. If you have any additional questions or concerns about the information provided in this document, please contact us at support@stickypass-word.com.

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.