Connection Magic
Security & Storage

Advantage Software Inc. (ASI) has been a trusted name in the court reporting industry for more than thirty years. Our products have been approved for use throughout the world. We are ever mindful of our customers' information, proactively engaging in the prevention of data loss and unauthorized access.

Connection Magic is a product/service provided by ASI that allows users to share and/or store data. There are multiple methods in which one may interface with or implement Connection Magic. This document provides a summary of the security and data integrity measures employed by ASI products utilizing these mechanisms.

First, and perhaps foremost, one should note that security in Connection Magic and the related family of ASI products is far more robust than the standard practices employed within the court reporting industry. We encourage IT departments to evaluate the procedures followed by their personnel that are beyond the scope of our software.

The preferred manner in which Connection Magic is utilized is for a court reporter to use it in conjunction with Eclipse, our flagship CAT software. Eclipse has the built-in ability to directly communicate with Connection Magic when the user has purchased a "Bridge Broadcaster" license. For users of competing CAT software, a local utility called "Connection Magic Link" is available. Running that alongside the third-party CAT software allows for communication to take place between the disparate systems.

Connection Magic exists in two distinct forms – "remote" and "local." The remote variation is a Cloud-hosted service. One must connect to that in order to share information across the Internet. The other option, "Connection Magic Local," provides a server hosted on a reporter's personal computer. That provides the ability to share information across a local area network (LAN) without connecting to the Internet. It is common for Connection Magic Local users to purchase a "pocket router" from us. With that, they do not even have to involve the common LAN within the physical facility where they are working. Instead, they can provide their own personal LAN for their clients. More details on this are provided later in this document.

The purpose one has in connecting to Connection Magic is to either link to another copy of Eclipse, another third-party CAT program, or to Bridge Mobile clients. Bridge Mobile is used primarily by judges and attorneys. It allows them to view the transcripts produced by court reporters, including via real-time streaming. Bridge Mobile comes in many formats. This includes a cross-browser web-based version, available online for those transmitting over the Internet, or over a LAN where it is hosted on a reporter's personal computer when running Connection Magic Local. The more robust formats for Bridge Mobile, however, are the stand-alone apps that are available for Windows, macOS, Android, and iOS.

Each option for using this system has been made highly secure. The first critical area of potential concern is the protection of authentication information supplied by end users (i.e. email addresses and passwords). As a front line of defense, passwords are protected using "BCrypt" hashing algorithms, inclusive of a unique "salt" (https://en.wikipedia.org/wiki/Bcrypt). BCrypt is not subject to "brute force" cracking by its nature. Such hashing takes place client-side, so a clear text password is never transmitted over a network or stored remotely. Unlike encrypted data, hashed data is not reversible (http://www.differencebetween.info/difference-between-hashing-and-encryption). Therefore, in the event the database were possibly compromised, a hacker would not gain useful information of this nature. The hashed value is not the actual password the user enters to access our system, nor is it of use on any other authentication system. Further, ASI staff can never view any true user passwords. Even the developers could not convert the hash back to clear text.

In addition to password hashing, all data transferred across networks is passed through secure sockets layer (SSL) encryption. This prevents "man in the middle" attacks (https://en.wikipedia.org/wiki/Man-in-the-middle_attack). If a hacker were to intercept the data packets transmitted over a network, they would find such are encrypted. Also, both the ends of these transmissions are bi-directionally authenticated, so neither party will exchange information with an imitator. Our SSL configuration has been closely securitized and designed to use very specific protocols and ciphers. Variations of elliptic curve secondary key-pairs are supported (https://en.wikipedia.org/wiki/Elliptic-curve_cryptography) where compatible.

The quality of this configuration can be directly ascertained by visiting the following URL: https://www.ssllabs.com/ssltest/analyze.html?d=connect.eclipsecat.com&latest. One can see there that this third-party service awards us an "A" rating. Note that it is nearly impossible to get an "A+" and that doing so is likely to negatively impact client compatibility. If you check our competitors, you will typically see ratings of Bs and Cs.

A more direct inspection of our certificate (which can be done through any browser upon visiting https://connect.eclipsecat.com/) also reveals that we took the extra step of procuring an Extended Validation (EV) SSL certificate. That requires a more thorough vetting process than the acquisition of a standard certificate, and thus provides end users more certainty they are communicating with the intended party (https://en.wikipedia.org/wiki/Extended_Validation_Certificate).

If one wishes to use Connection Magic Local, and not involve the Internet at all, SSL is still provided for the LAN transmissions. In fact, the program generates a private certificate on the fly for that specific court reporter. It also creates a unique "ephemeral DH key." (https://tls.mbed.org/kb/cryptography/ephemeral-diffie-hellman). As such, these local broadcasts are particularly secure.

When Connection Magic Local is initialized, it automatically sets up hosting on the IP address made available to it by the LAN. Normally, that IP is dynamically assigned. The SSL certificate it creates is bound to that singular IP. The program displays this IP address. Browser users must input that manually to connect to Bridge Mobile Local. Standalone BM app users, however, do

not have to do so. Behind the scenes, they will receive a broadcast over the LAN via UDP if they have joined the network (i.e. often the pocket WiFi router of the reporter). That broadcast relays this local IP address and then connects to it automatically. To implement SSL, Bridge Mobile then downloads the dynamically generated client key Connection Magic Local has created. That end of the private key pair is installed on the user's device, and the secure connection is established.

Once data has been received by Bridge Mobile, it is quite unlikely to be lost or to be accessed by malicious programs. Closing a document, or the app as whole, results in automatically saving the data and one's markups. On mobile devices especially, the data is made inaccessible to other software by being saved to storage areas inherently private to the app. Especially sensitive information, such as a password, is additionally encrypted as a failsafe.

If users opt to purchase the Bridge Mobile Professional upgrade, among other additional functions, they will be able to use Cloud-based storage. When this is utilized they will have copies of their transcripts backed up to the Cloud as well. That safety net ensures they will not lose their data in the event they lose or break their device on which it was locally stored. This mechanism also makes it easy to retrieve and edit stored documents across devices and platforms.

The Cloud Connection Magic server has a minimal risk of exposure to attacks from the outside world. None of our infrastructure tools accept and execute code or macros, so the system itself does not provide a malware or hacking pathway. Standardized measures are specifically taken to prevent SQL injections from occurring via the processing of dynamic data (https://stackoverflow.com/questions/7929364/python-best-practice-and-securest-to-connect-to-mysql-and-execute-queries).

Administrative access to these servers is extremely minimal, with only a handful of select ASI personnel having authorization parameters. The entire file system has been locked down tightly, with permissions set as restrictively as possible. Likewise, firewalls are maximally employed. The physical server itself is controlled and maintained by Google.

All user data is backed up daily. Multiple weeks of these backups are retained prior to an automatic purging process being run to prevent the server's disk space from being exhausted. Along with permission controls, these backups are each compressed, encrypted, and password-protected. This encryption takes place using the AES-256 methodology (https://en.wikipedia.org/wiki/Advanced_Encryption_Standard).

Such daily backups are securely off-sited via SSH immediately after being generated, utilizing "passwordless" key-pair authentication (https://www.ssh.com/ssh/key/). As previously stated, the backups are securely packaged prior to these transfers taking place. The passwords to decrypt them are unique to the file and are dynamically defined through a proprietary algorithm.

The off-sited data goes to a completely different physical location. It is then pooled into a larger set of data and backed up again as part of that more inclusive collection. Such is handled by a third party specializing in that service.

All of these redundant backups protect against the possibility of data loss. Further, in the event the database is somehow corrupted, we are able to rapidly roll back to a state where it was perfectly intact.

Additional Resources

https://www.eclipsecat.com/sites/default/files/Bridge%20Mobile%20Security.pdf

https://www.eclipsecat.com/sites/default/files/BridgeBroadcasterFAQ.pdf

https://www.eclipsecat.com/sites/default/files/Bridge%20Mobile%20for%20Attorneys.pdf

https://www.eclipsecat.com/content/bridge-mobile

https://www.eclipsecat.com/category/catalog/routers

https://www.eclipsecat.com/catalog/software