CLINTON CONNECT

DATA SECURITY

Clinton Electronics takes the security of your data very seriously. We have designed the Clinton Connect platform from the ground up with security in mind. Be it software or hardware solutions, preventing accidental loss or malicious attacks, we are committed to providing a platform you can trust. This commitment to security is never-ending and continues as we develop new features of the platform.

Security Features

Identity Protection

Access to the Clinton Connect platform requires login by username and password. It is a closed ecosystem in that users may not self-enroll. A user may only be issued account access by a privileged user. We employ a tiered Access Control List based on Roles and Permissions to prevent people from accessing and manipulating sensitive data. Connect users can also enable single sign-on and two-factor authentication for an additional level of identity protection.

Data Storage

Data stored in the Clinton Connect platform is protected against loss. Database backups are made nightly and stored for an extended period. Most data is never deleted immediately, only marked for deletion at a later date. This way, we can quickly restore items "accidentally" deleted by any user. The Web Client and the Connect PVM are both designed as "thin clients," meaning they store very little data locally, and any data can quickly be restored to them from the Server.

Network Communications

All data on the Clinton Connect platform is encrypted while in transit via industry-standard SSL technology (HTTPS). Clinton Connect software and devices only require a connection to our server, push notification service, and our file server. Network admins may easily limit traffic on their network to these three sources. In the case of a high network load or a network-based attack, we employ a load balancer and request rate limits to keep the application running.

3rd Party Pen Tested

Clinton Electronics proactively takes measures to help secure its network and protect customers and their data.

The Clinton Connect platform has undergone rigorous 3rd Party Penetration testing performed by Gotham Digital Science (GDS). GDS used a combination of automated tools and manual penetration testing to search for missing, broken and improperly implemented security controls. The assessment evaluated application/network security best practices and common vulnerabilities, including the OWASP Top Ten (https://www.owasp.org), and other flaws typical of similar applications, networks, and environments.

GOTHAM
DIGITAL • SCIENCE
A STROZ FRIEDBERG COMPANY

Two-Factor Authentication (2FA)

Go beyond the password and protect your account from hackers and account takeovers.

Two-factor Authentication (2FA) is a security process where the user provides two forms of ID to log in to Clinton Connect. 2FA helps to keep your account safe. It's easy to set up and only takes a minute to activate.

Clinton Connect 2FA supports a wide range of authenticator apps such as 1Password, Authy, Microsoft Authenticator, Google Authenticator, and more.

Single Sign-On (SSO) Authentication via SAML 2.0

SAML 2.0 based SSO gives users access to Clinton Connect through an identity provider (IDP) of your choice.

Single sign-on (SSO) allows users of your Clinton Connect account to log in using your existing SAML-enabled identity provider, such as Active Directory, Okta, and more. With SSO, companies can maintain control of who has access to manage their Connect devices, automatically provision new users, and quickly revoke user access all from their existing identity provider.

Interested in learning more about Clinton Connect?

Contact us today for a **free consultation** about how the Connect Platform can **benefit your store or business**.

Schedule A Demo

v.07.02.20