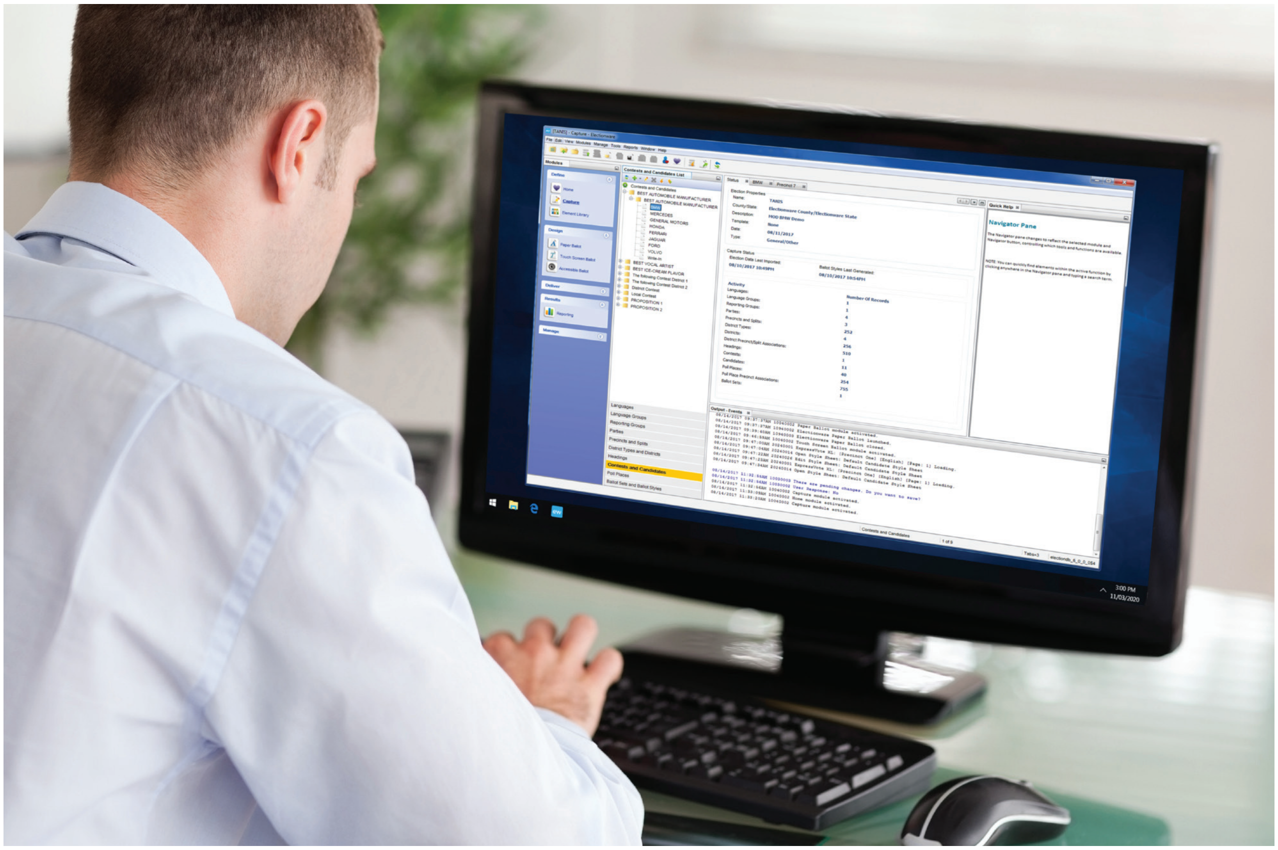
Electionware®



PRODUCT INFORMATION

Electionware election management software allows jurisdictions of all sizes to manage their elections through the software's easy-to-understand, user-friendly interface

Digital media assets, including pictures, videos, security documents and our marketing one-sheets are available for download at:
essvote.com/download-media-assets-electionware

KEY FEATURES & BENEFITS

ROBUST AND FLEXIBLE MANAGEMENT

This agile election management software is the result of our nearly 40 years of election software leadership, designed to accommodate a variety of election needs, including early and overseas voting, ADA compliance, ballot adjudication, and election-night reporting and auditing. With the capability to manage nearly 10,000 ballot styles, support multiple languages, and allow authorized teams to work in Electionware simultaneously, the software is intuitive and easy to use. The database for multiple equipment types provides election-wide uniformity and compliance with less room for human error.

USE AND CONFIGURATION

The Electionware election management software is used by election officials to create an election information database, format ballots, program voting and ballot-scanning equipment, consolidate tabulator results, generate election night reports, and review ballot images. The 5 software groups contain 11 modules: tools to make elections management more intuitive, auditable and secure, and the configuration of each group is set up to meet equipment and election requirements.

EFFICIENT RESULTS REPORTING

Among the features are an innovative results reporting module and a state of the art application that allows administrators to electronically adjudicate ballots. This function masterfully handles the management of write-in votes. The interface displays key ballot information including precinct, ballot style, poll type, machine serial number, and polling location as well as color-coded identification of undervotes and counted votes, which can be exported as individual PDF files.

In addition, Electionware improves the post-election audit process by allowing election officials more flexibility to effectively and efficiently conduct a wide range of post-election audits. The easy-to-read, side-by-side comparison of the unaltered ballot image and its corresponding cast vote record make it possible to audit any election in a fraction of the time.

Electionware® Security Facts

PHYSICAL SECURITY & USER AUTHENTICATION

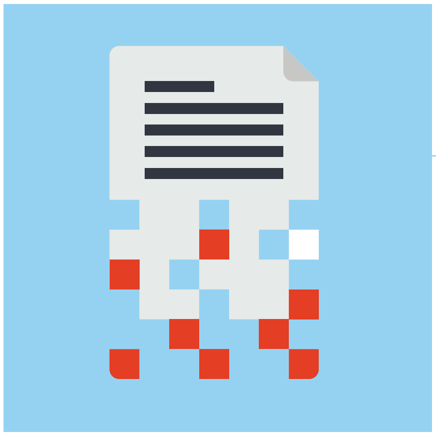
» The Electionware PC is stored in a secure, controlled environment that limits physical access to the system and adheres to jurisdictional security requirements. While in storage, transport, preparation and operation, tamper-evident seals alert election officials of unauthorized access. ES&S supplies a variety of tamper-evident devices (wire seals, plastic pin seals, etc.) imprinted with identification numbers for securing the unit. These physical locks and seals are a first line of defense, and minimize the effect of any unauthorized access to an Electionware PC.

» The operating software provides security access controls to limit and detect access to critical system components during equipment preparation, testing and operation, guarding against system integrity loss and availability. All failed login attempts are logged, alerting election officials if an attempt to access the system has been made. These safeguards cannot be bypassed or deactivated during system installation or operation, maintaining the integrity of the election data and audit record. Username and password information is encrypted.

» Security levels are configurable to the levels required by the jurisdiction.

SYSTEM SECURITY

» The Electionware PC is a hardened device which has been configured to include only the services, applications, utilities and settings required to successfully operate the system. The hardening process turns the PC into a single-use device, dedicated solely to creating and operating elections.



ENCRYPTION & DATA INTEGRITY VALIDATION

- All data in motion, including data on election USB flash drives, is encrypted using FIPS-compliant, signed data keys. Electionware will only recognize these certified and approved data keys.
- As data is transferred to election devices, additional hash validations ensure data integrity remains intact. Each election device also generates a signed data key, ensuring that should unauthorized access of a device occur, no other devices can be affected through data transfer. All election data is encrypted and digitally signed before it is transferred from an election device for reporting results and auditing.

VERIFICATION

- Electionware maintains a detailed audit log of all actions and events that have occurred on the unit. This includes a record of all user actions, with username and timestamp to the system audit log. This audit log can be filtered by date and type of event, printed or saved in a variety of file formats, including .pdf, .rtf, .html, .xls and .csv. The log operates during all processes including results processing.
- Audit records created during the election definition and ballot preparation include records for the finalization of ballot layout and modifications to that finalization. These records incorporate a date/time stamp, include a description of the action and the module the action occurred in and can be filtered by date, event type, and sorted by ascending or descending timestamps.