ClearVote 2.3

ClearDesign Functionality Description

ClearDesign Functionality Description

Clear Ballot Part Number: 100046-10020

Document Type: Technical

Clear Ballot Group
2 Oliver Street, Suite 200
Boston, MA 02109
857-250-4961
clearballot.com

Document history

Date	Description	Version	Author
01/10/2017	Initial submission to EAC	1.0	Joe Srednicki
02/03/2017	Minor typographical and reference-related edits	1.0.1	Joe Srednicki
05/09/2017	Minor update based on feedback from the state of Colorado and Clear Ballot Quality Assurance	1.0.2	Joe Srednicki
06/01/2017	Updated the sections "ClearDesign parts checklist" and "Installation Procedure" (for Installing the DesignServer software). Changed the title of Chapter 2 to "Installing third-party software on the DesignServer."	1.0.3	Joe Srednicki
06/16/2017	Minor updates for vote-by-mail campaign.	1.0.4	Joe Srednicki
06/22/2017	Updated the section "Installation procedure" in Chapter 3.	1.0.5	Joe Srednicki
06/23/2017	Removed Linksys EA2700 N600 Dual-Band Wi-Fi Wireless Router from the section "ClearDesign Parts List."	1.0.6	Joe Srednicki
07/21/2017	Update the version number for Colorado	1.0.7	Joe Srednicki
09/18/2017	Added the section "Retention of audit log data."	1.0.8	Joe Srednicki
01/19/2018	Vote-by-Mail campaign 2	1.0.9	Joni G. McNutt
04/27/2018	Minor updates	1.0.10	Joe Srednicki
08/07/2018	Updated cover page.	1.0.11	Joe Srednicki
04/12/2019	Updated "Logic and controls for accuracy" and "Accurate recording, tabulating, and reporting of votes" to include ClearCast. Updated cover page	1.0.12	Joe Srednicki
11/04/2019	Updated cover page	1.0.13	Joe Srednicki
02/12/2020	Minor edits	1.0.14	Joe Srednicki
11/25/2020	Minor edits	1.0.15	Joe Srednicki
10/22/2021	Updated cover page	1.0.16	Joe Srednicki

Table of contents

Preface

This section defines the purpose of this document.

About this document

This document provides an overview of the features and components of the ClearDesign system. This document corresponds to the requirements for the technical data package (TDP) in the *Voluntary Voting System Guidelines* (VVSG), 2005, Volume 2, Section 2.3 .

Scope of this document

This document contains the following chapters:

- Chapter 1. System overview
- Chapter 2. Security
- Chapter 3. Accuracy
- Chapter 4. Error recovery
- Chapter 5. Integrity
- Chapter 6. System audit
- Chapter 7. Election management system
- Chapter 8. Vote tabulating program
- Chapter 9. Prevoting capabilities
- Chapter 10. Voting capabilities
- Chapter 11. Post-voting capabilities
- Chapter 12. Maintenance, transportation, and storage

Intended audience

The document is for state and federal election officials and their voting system test laboratories. This document is part of the Technical Data Package (TDP) required to certify the ClearVote system for use. Clear Ballot personnel also use this document to support election officials and staff.

Conventions

This section describes conventions used in this document.

References to ClearVote products

A ClearVote® system can comprise the ClearAccess®, ClearCast®, ClearCount®, and ClearDesign® products. Jurisdictions are not required to purchase all products. You can ignore references to any ClearVote products that are not part of your voting system. Also ignore implementation options that are not relevant to your policies and procedures.

BDF and ADF

ClearAccess imports an election definition contained in an accessible definition file (ADF) created by ClearDesign. ClearCount and ClearCast import an election definition contained in a ballot definition file (BDF) created by ClearDesign.

Versions of ClearDesign earlier than 2.0 created unencrypted ADFs and BDFs. ClearDesign 2.0 and later versions produce encrypted ADFs and BDFs. You can distinguish between unencrypted and encrypted ADFs and BDFs by the ending of the filename.

File type	Filename ends in
Unencrypted accessible definition file	adf.zip
Encrypted accessible definition file	adfx.zip
Unencrypted ballot definition file	bdf.zip
Encrypted ballot definition file	bdfx.zip

In this document, the general terms ADF and BDF can refer to both the unencrypted and encrypted versions of these files.

For the specifics of the ADF and BDF file formats, see the following:

- *ClearDesign Accessible Definition File Guide*
- *ClearDesign Ballot Definition File Guide*

Chapter 1. System overview

1.1   Introduction

ClearDesign is an election management system created by Clear Ballot. ClearDesign is a product used to define elections and prepare ballots.

The ClearDesign server software resides on unmodified commercial off-the-shelf (COTS) computers that use the Ubuntu Linux operating system. A user interacts with the ClearDesign by using a browser on a Windows desktop computer.

For a detailed summary of the system, see the *ClearDesign System Overview*

1.2   Election workflow

ClearDesign creates the source files that ClearAccess and ClearCount use for:

- Accessible voting
- Vote tabulating
- Ballot counting
- Election reporting

Chapter 2. Security

ClearDesign security consists of programmatic access control, established with passwords and user access levels, and physical security. The ClearDesign system architecture and recommended methodology work together to ensure security.

2.1 Access controls

Users of ClearDesign are assigned a user name, password, and access level. Role-based access control lists (ACLs), stored on the server, protect the client/server interface. These ACLs protect both the web and MySQL database transactions.

Network communication is restricted to a closed Ethernet. There are no connections to computers outside this Ethernet. There are no wireless or Internet connections. Nothing in the product requires a connection to the Internet for maintenance, operation, or administration.

2.2 Process controls

The internal controls of ClearDesign ensure that functions and tasks execute only under intended conditions. For example, when the election state is **Media Created**, ClearDesign prevents any changes that affect the media that has already been created.

2.3 Precondition controls

The internal controls of ClearDesign ensure that functions and tasks execute only after meeting any required preconditions. For example, ClearDesign cannot generate election data for voting devices until ballots are generated.

2.4 Safeguards if a system failure occurs

To protect against tampering during system repairs or interventions in system operations, the ClearDesign data is stored in a MySQL database that requires a username and password. System-repair personnel are not required to know this password.

As a security measure, elections can be backed up and a restored. To back up and restore an election, an authorized user must enter a validation code to ensure the backup has not been tampered with at any time.

2.5 Security provisions

See the *ClearDesign Security Specification*.

2.6 Restrictions

ClearDesign has built-in checks to ensure that no capability is completely restricted from use. A particular user may not have the permissions to execute a given operation. However, the ClearDesign always ensures that someone has access to a given operation or can be assigned access to that operation.

See also "Access controls" on the previous page.

If an election's state restricts an operation, changing the election state can enable the operation. As with all operations, ClearDesign notifies a user of any side effects before executing the operation.

See also "Process controls" on the previous page.

2.7 Administrative procedures

The *ClearDesign Administration Guide* documents all administrative procedures, such as:

* Managing customers, users, and roles
* Viewing the system log
* Managing localization settings

2.8 FIPS 140 cryptographic compliance

Clear Ballot products—ClearDesign, ClearAccess, ClearCast, and ClearCount—are written in the Python language using the standard Python libraries. The standard Python hashing libraries use OpenSSL on the Linux platforms, including Ubuntu and the Windows cryptographic libraries on the Windows platforms. Where native Python support does not exist, a thin wrapper has been created to access the underlying cryptographic libraries.

Clear Ballot products running on Ubuntu build the FIPS-certified version of OpenSSL during the build process. They use the OpenSSL FIPS version that is included as part of the FIPS certificate and build it in conformance with the security policy defined in the certification process. See https://www.openssl.org/docs/fips.html for more information.

Clear Ballot products running on Windows use the cryptographic system provided by the Windows operating system. Versions of Windows used by Clear Ballot products have a FIPS certificate.

When the Clear Ballot products start up, they check that the cryptographic module is operating in FIPS mode. If not, the product displays an error message and will not proceed.

2.9   Browser certificates

To provide security for HTTPS connections to the ClearDesign server, you are required to install browser certificate as part of the overall installation process.

See "Installing the browser certificate for Google Chrome" in the *ClearDesign Installation Guide* for the specific steps.

Chapter 3. Accuracy

This chapter describes the mechanisms that ClearDesign uses to ensure accuracy.

3.1   Record election data accurately

ClearDesign includes several mechanisms to ensure that election data is accurate:

- ClearDesign validates all data entered by the user to ensure conformity to the system requirements and consistency.

  For example, when a user defines a contest, the user interface presents a list of valid districts to associate with the contest. When the user saves the contest, ClearDesign revalidates the district to ensure that it exists within the election.

- ClearDesign supports a variety of formats that allow imports of election definitions from other applications, such as voter registration systems. ClearDesign uses the same logic for validating imported and manually-entered data to ensure integrity and accuracy.

- ClearDesign prompts the user to confirm all operations that affect multiple entities.

  For example, ClearDesign displays a warning when deleting a contest also removes the associated candidates or affects generated ballots.

- ClearDesign uses MySQL as its backend database and SQLAlchemy as its data modeler to ensure data accuracy and integrity.

- ClearDesign has a variety of reports for validating and proofing the election definition to ensure that it is correct.

3.2   Record options for casting and recording votes

ClearDesign allows the user to define the various options required for accurate vote casting and records. Examples are:

- The number to vote for in a contest
- The office associated with a contest
- The parties associated with a candidate
- The district associated with a contest

3.3   Record votes accurately

ClearDesign is not a vote recording system. ClearCount is the ClearVote vote-recording component. See "Recording votes accurately" in the *ClearCount Functionality Description*.

3.4   Logic and controls for accuracy

ClearDesign is not a vote recording system. ClearCount and ClearCast are the ClearVote vote-recording components. See the following:

- "ClearCount logic and accuracy testing" in the *ClearCount Installation Guide*

- "Security risks addressed" and "Attempt to cast unauthorized ballots" in the *ClearCast Security Specification*

3.5   Monitor overall data quality

ClearDesign validates all data entry for accuracy and quality. ClearDesign validates both manually entered data and import files.

If manually entered data fails validation, ClearDesign does the following:

- Displays a message

- Requires the user to correct the data before adding it to the election database

3.6   Accurate recording, tabulating, and reporting of votes

ClearDesign is not a vote recording system. ClearCount and ClearCast are the ClearVote vote-recording components. See the following:

- "Accuracy" in the *ClearCount Functionality Description*

- "Security risks addressed" and "Attempts to cast unauthorized ballots" in the *ClearCast Security Specification*

For each election, ClearDesign generates a ballot definition file. Both ClearCount and ClearCast use the same ballot definition file. The ballot definition file is imported into the CountServer at a CountStation when an election is created in ClearCount. The ballot definition file is imported directly into ClearCast when an election is opened.

A ballot definition file created by ClearDesign can be unencrypted or encrypted:

- Versions of ClearDesign earlier than 2.0 produce an unencrypted ballot definition file referred to as an BDF.

- ClearDesign version 2.0 and later versions produce an encrypted accessible definition file referred to as an BDFx.

For details on the BDF and BDFx files, see the *ClearDesign Ballot Definition File Guide*.

Chapter 4. Error recovery

ClearDesign includes several features that aid in error recovery. The system is constructed to ensure that errors are not introduced into the system because of problems with hardware, power, or connections to the secure Ethernet. ClearDesign stores all data in appropriate, protected databases to prevent data corruption.

4.1   System and software errors

Before updating the system, the ClearDesign software validates all data and informs the user of any error or inconsistency. This safeguard enables a user to correct any errors or inconsistencies before updates occur.

Furthermore, ClearDesign uses transactions to ensure that either all or none of the data is committed and that the data is always consistent.

4.2   Database backup and recovery

ClearDesign has validated backup and restore facilities to enable a complete restoration of the system to a given state, even in the event of failure of a memory component, including the central processing unit.

A user with backup permissions can back up the election data to a local computer. When backing up an election, the user is prompted to enter a validation code. This code is used to validate the data during a restore operation to ensure the data has not been modified since the backup was created.

A user with restore permissions can restore the election data using the validation code entered when the election was backed up. The restoring of an election does not overwrite any election; restoring an election adds the restored election to the system.

4.3   Web application errors

The ClearDesign system uses a closed, wired Ethernet network. There are no Internet connections in the system.

If a user clicks a link or enters a URL and does not reach the expected location, the user has encountered a defect in the ClearDesign software. ClearDesign displays an error message and records the error in the election activity log. Contact Clear Ballot Technical Support if you find a defect.

4.4   Error message requirements

ClearDesign error messages include:

- Date and time stamps
- The source of the error
- The severity
- A description

Chapter 5. Integrity

ClearDesign software is not a vote-recording and counting system. Therefore, this section does not apply.

However, the following features in ClearDesign ensure data integrity and data protection:

- All access to the data requires login using a valid username and password.

- All data inputs are validated before they are accepted.

- Data is stored in a transactional database, which ensures that the data is always valid.

- The ClearDesign system uses COTS hardware that has been developed and tested to protect against physical threats such as interruption of electrical power, generated or induced electromagnetic radiation, and fluctuations in ambient temperature and humidity.

Chapter 6. System audit

This section describes the audit logging functions and error messages of the ClearDesign system.

6.1   Audit logs

The ClearDesign system has two types of logs:

- Election log—a log associated with a specific election.

    See "Viewing a log for an individual election" in the *ClearDesign User Guide*.

- System log—a log that records system activity that is not associated with a specific election.

    See "System log" in the *ClearDesign Administration Guide*.

To ensure the integrity of the data, ClearDesign stores both types of logs in a transactional database.

None of the log entries created by ClearDesign contain any voter-specific information or any information about voted ballots.

All log entries contain the information listed in Table 6-1.

Table 6-1. Contents of log entries

Log entry	Description
systemId	Name of the jurisdiction
timestamp	When the event occurred
messageId	Identifies the type of event
userId	Identifies the user associated with the event. There is no user for failed login attempts
message	Describes the event

When you back up and export an election, ClearDesign applies the same access-control mechanisms to log data as used for all other operations. When you restore an election, ClearDesign also restores the log associated with that specific election. As part of the restoration process, ClearDesign performs validity and integrity checks.

You can also back up the system log so that you can review it when needed.

6.2   Retention of audit log data

According to VVSG VI, 2.1.10, all systems must maintain integrity of voting and audit date during an election and for at least 22 months thereafter.

ClearDesign meets this requirement for system logs and election logs. System logs exist as long as the ClearDesign system is installed. The same is true of election logs. The election logs exist as long as corresponding elections are installed on a ClearDesign system.

6.3   Error messages

The ClearDesign system is an interactive system that detects and generates any errors found in real time and presents the error messages to the user as they occur.

The messages are displayed in plain text and do not use any form of numerical code that the user is required to interpret.

Chapter 7. Election management system

ClearDesign is the system that is used to prepare ballots and to generate the data for the ClearAccess and ClearCount systems that are used to vote and tabulate the ballots and tabulate the results.

In ClearDesign, each election is stored as a separate database where the data can be entered manually and imported from a third-party system.

7.1   Define political subdivision boundaries and multiple election districts

The ClearDesign system supports the creation of multiple District Categories, such as State Representative and City, that are used to group districts.

Each District Category can contain multiple districts, such as State Representative District 12, State Representative District 14, and so on. When these categories are established, the precinct, precinct portions or splits, and contests can then be linked to the district. The ClearDesign system uses these relationships to define ballots for the voters.

7.2   Identify contests, candidates, and issues

The ClearDesign system allows for the creation of contests and their associated candidates, as well as referendum issues or questions.

Associated with each contest are the various options, such as district and party, that define who is allowed to vote on the contest, and voting rules, such as the number to vote for, that define how the contest is counted.

The ClearDesign system also allows voterGroups (parties) to be associated with contests for use in primary elections.

Candidates can be associated with one or more (in the case of cross-endorsed candidates) voter groups (parties).

7.3   Define ballot formats and voting options

The ClearDesign system offers great flexibility in defining the ballot formats to optimize the layout and clarity of the information.

Users can view individual ballot layouts both in PDF and HTML formats without having to lay out all of the ballots. Any adjustments to the layout can be identified and implemented early in the process, making election setup more efficient.

7.4   Generate ballots and election-specific programs for voting equipment

The ClearDesign system also generates ballots and election-specific programs for voting equipment:

- Generated ballots can be exported as PDF files and sent to the ballot printer.

- HTML Anywhere Ballots can be generated and exported as part of the ADFx, which can be loaded into the ClearAccess system.

- The ClearDesign system creates a ballot definition file that the ClearCount system uses for tabulating the ballots.

7.5   Count and tabulate the ballots

ClearCount is the ClearDesign vote-counting and tabulating component. See "Vote tabulating program" and "Ballot counter" in the *ClearCount Functionality Description*.

Chapter 8. Vote tabulating program

ClearCount is the ClearVote vote-tabulating component. See "Vote tabulating program" in the *ClearCount Functionality Description*.

Chapter 9. Prevoting capabilities

This section defines the capabilities of the ClearDesign system to prepare the election data for voting.

9.1   Ballot preparation

This section covers the defining of the specific contests, question, and related instructions to be contained in ballots, and to produce all permissible ballot layouts.

9.1.1 General capabilities

The ClearDesign system allows a user to define the entities listed in Table 9-1.

Table 9-1. Entities

Entity	Description
BallotSets	The BallotSet is used to filter contests, such as for "federal only" ballots, and to define whether separate ballots are to be generated for each voter group (party), as in a "closed primary."
Candidates	A person contending in a contest for office. A candidate can be presented as one of the choices on the ballot or can be a write-in candidate. Each candidate is associated with a single contest and one or more voterGroups (parties). Each candidate has a name that is used for reporting purposes, and "ballot text" that is placed on the ballot.
Contests	A single decision within an election, such as a presidential race or a bond issue. A contest has a list of candidates or choices and may include a write-in choice. Each contest is associated with a single district and a single voterGroup (party). Each contest has a name that is used for reporting purposes, and "ballot text" that is placed on the ballot.
District	Districts are used to define the geographical division of voters. Each district belongs to one district category and has one or more splits associated with it. Districts also have contests associated with them.
District categories	District categories are used to group districts so that each split can only belong to one district of a district category.

Table 9-1. Entities (continued)

Entity	Description
Headers	The instructional information that is placed on the ballots. Headers can be "card" headers that are associated with ballots independent of any contest, or "contest" headers that are associated with a ballot only if their associated contest is on the ballot. Each header has a name that is used for reporting purposes, and "ballot text" that is placed on the ballot.
Precincts	The geographical division of voters for the purpose of organizing them for an election. Precincts have one or more splits associated with them.
Splits	Splits are the geographical area within a precinct that is not split by any district. Each split is associated with a single precinct and only one district of each district category.
voterGroups (parties)	voterGroups (or parties) allow contests to be filtered according to a nongeographical division of voters for the purpose of determining which contests a voter is allowed to vote on. When contests are associated with voterGroups other than the nonpartisan voterGroup, the election is considered to be a primary or partisan election.

The ClearDesign system performs the ballot layout process in two phases:

1. In the ballot-generation phase, all contests that each voter can vote on are grouped on the basis of the split that the voter resides in and the voterGroup that the voter is associated with. This phase produces a set of ballot styles and ballots. If the contest uses candidate rotation, the ballots are the versions of the ballot style in which candidates are rotated within the contests.

2. In the card layout phase, all headers and contests are placed onto individual cards. The layout of the card conforms to the layout rules defined in the headers and to the card template defined in the ballot set for the card.

Each card that is defined by the system has a unique identifier that is placed at the bottom of the card and is read by the ClearCount system to determine where each vote response field is located.

After the cards are laid out, the user can generate a PDF file of each card to be sent to the printer. The generated PDF file includes the timing marks (the card identifier marks and the precinct identifier marks), and all of the contest, candidate, and instruction information.

9.1.2 Ballot formatting

The ClearDesign system allows an authorized user to create a new election. The new election can be one that is restored from a previously backed-up template election, one that is created using an imported file of a supported format, or an empty election.

The ClearDesign system allows the user to enter any new election information that is required and modify any existing election data. All data that is entered into the system is validated before it is saved to ensure an error-free definition.

When the voterGroups (parties), district categories, districts, precincts/splits, contests, candidates, headers, and ballot sets are defined, the user can generate and layout the ballots.

The ClearDesign system's ballot layout ensures that all candidate voting positions are of the same size for a given contest and supports candidate rotation to ensure equal positioning of candidates in a contest.

As with all aspects of the ClearDesign system, modifications to ballot layouts or ballot formats can be made only by authorized users and can be locked out after the ballot layout has been completed.

9.1.3 Ballot production

The ClearDesign system allows the user to produce ballot PDF files for sending to the printer for ballot production. See the *ClearVote Ballot Stock and Printing Specification* for the ballot-printing specification.

The ClearDesign system also allows the user to create the ballot definition file that is used by the ClearCount system to count and tally the ballots.

If jurisdictions require ballots in other languages, the ClearDesign system allows these languages to be defined and the ballots produced.

9.2 Election programming

ClearDesign associates each contest with voting attributes. These attributes determine the following:

- Who is allowed to vote on the contest
- How many selections a voter can make
- The district and voterGroups with which the contest is associated

ClearDesign uses the following attributes to exclude contests that a voter is ineligible to vote on:

- Districts
- voterGroups (parties)
- Precincts/splits
- The contest filter of the ballot set
- The separate ballot option of the ballot set

 ClearDesign generates a single ballot definition file that includes the definition for the entire election.

9.3   Ballot and program installation and control

See "Ballot and program installation and control" in the *ClearCount Functionality Description*.

9.4   Readiness testing

To ensure system readiness, code a small election and take it all the way through to PDF, ADFx, and BDF or BDFx creation.

9.5   Verification at the polling place

ClearDesign is not a vote counting system. ClearCount is a central counting system that does not include a polling-place component. See "Verification at the central location" in the *ClearCount Functionality Description*.

9.6   Verification at the central location

See "Verification at the central location" in the *ClearCount Functionality Description*.

Chapter 10. Voting capabilities

ClearDesign is not a vote-counting system. See "Voting capabilities" in the *ClearCount Functionality Description* for this information.

Chapter 11. Post-voting capabilities

ClearDesign is not a vote-counting system. See "Postvoting capabilities" in the *ClearCount Functionality Description* for this information.

Chapter 12. Maintenance, transportation, and storage

ClearDesign is not a vote-counting system. For maintenance information, see the *ClearDesign Maintenance Guide*.