ClearAccess 1.0
Security Specification

Abstract: This document provides the security specifications of the ClearAccess system.
© 2012–2015 Clear Ballot Group
ClearAcess Security Specification
ClearAccess Part Number: 100050-10001

Copyright © 2012–2015, Clear Ballot Group
All rights reserved.

This document contains proprietary and confidential information, consisting of trade secrets of a technical and/or commercial nature. The recipient may not share, copy, or reproduce its contents without express written permission from Clear Ballot Group.


ScandAll PRO and PaperStream are trademarks of FUJITSU LIMITED. All rights reserved.

Other product and company names mentioned herein are the property of their respective owners.

Clear Ballot Group
7 Water Street, Suite 700
Boston, MA 02109
(857) 250–4957
http://www.clearballot.com

**Document history**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Version</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/18/15</td>
<td>Initial creation date</td>
<td>1.0.0</td>
<td>Talbot Iredale</td>
</tr>
<tr>
<td>7/8/15</td>
<td>Update poll place security</td>
<td>1.0.1</td>
<td>Talbot Iredale</td>
</tr>
</tbody>
</table>
Table of Contents

1. Abstract .................................................................................................................. 4
   1.1 About this document............................................................................................ 4
   1.2 Scope of this document......................................................................................... 4
   1.3 Intended audience ............................................................................................... 4
2. Product description .................................................................................................. 5
   2.1 ClearAccess artifacts .......................................................................................... 5
   2.2 Data access........................................................................................................... 5
3. Access control .......................................................................................................... 6
   3.1 General access control......................................................................................... 6
   3.2 Access control identification .............................................................................. 6
   3.3 Access control authentication ............................................................................ 7
   3.4 Access control authorization ............................................................................. 7
4. Physical security measures ....................................................................................... 8
   4.1 Polling place security ........................................................................................ 8
   4.2 Central count location security ......................................................................... 8
5. Software security ..................................................................................................... 9
   5.1 Software and firmware installation ................................................................... 9
   5.2 Protection against malicious software ............................................................... 9
   5.3 Software distribution and setup validation ....................................................... 9
   5.4 Software distribution ......................................................................................... 9
   5.5 Software reference information ....................................................................... 9
   5.6 Software setup validation ................................................................................. 10
6. Telecommunications and data transmission .......................................................... 11
7. Use of public communications networks ............................................................... 11
8. Wireless communications ...................................................................................... 11
9. Independent verification systems ........................................................................... 11
10. Voter Verifiable Paper Audit Trail requirements .................................................. 11
1. Abstract

This section defines the purpose of this document. It contains the following sections:

- About this document
- Scope of this document
- Intended audience

1.1 About this document


1.2 Scope of this document

This section provides summary information about the following aspects of the ClearAccess system:

- User roles and permissions
- Access control mechanism
- Data access

1.3 Intended audience

This document is intended for state election officials and their delegated Voting Systems Test Laboratory, as part of the technical data package required to certify the ClearAccess election definition system for use in their state.
2. System overview

2. Product description

ClearAccess is an accessible ballot-marking device created by the Clear Ballot Group (Clear Ballot). The ClearAccess software runs on unmodified commercial off-the-shelf (COTS) computers that run the Microsoft Windows operating system.

2.1 ClearAccess artifacts
Several artifacts are stored and managed on the ClearAccess device.

- config.txt—This file contains machine configuration information.
- state.txt—This file contains information about the currently loaded election and what election state it is in.
- system.log—The system log records all non-election specific activity. A log record is appended whenever users log in or log out, fail to log in, or any other change is made to the system.
- election.log—The election-specific log is created when the election is loaded; records are appended whenever there is any election-related activity.

2.2 Data access
The ClearAccess system uses role-based access controls in which each login contains the role letter followed by the role password or code.
3. Access control
The ClearAccess system uses roles and permissions to control the access to specific functions. The permissions are based on the state of the election and the role.

3.1 General access control
a. The ClearAccess system requires all users to log in with a role code prior to being able to access the system.
b. The ClearAccess system operates on a hardened Windows 8.1 system that controls access to any of the systems software and files.
c. The ClearAccess system creates roles and associated permissions for the following roles:
   - **Maintenance**—Can access system setup and logs only to help diagnose any issues. Cannot access election data.
   - **Administrator**—Can access system setup, logs, and load and unload elections, but cannot access election data.
   - **Election Administrator**—Can access election data, view the logs, do pre-election testing, and prepare the system for voting.
   - **Poll worker**—Can open and close polls, and view the logs.
   - **Voter**—Can vote a ballot only.
d. ClearAccess checks the permissions on all operations based on the permissions granted to the role of the user who is logged in, thereby preventing a restricted user from being able to access or modify anything that is not explicitly permitted by their own permissions.
e. Access control for the ClearAccess system requires explicit permissions to access any operation, privileged or other.
f. Valid user credentials, including passwords, are required to be able to upgrade the software.

3.2 Access control identification
Every access to the ClearAccess system requires the user to enter a valid access code that identifies the role of the user.

a. The process and data access granted to a user and role is identified by the permissions assigned to that user and role.
b. The ClearAccess permissions system is a role-based permission system
   - **Role**—A collective identity with associated permissions that is defined by the system and to which a user belongs
   - **Entities**—The data elements the system controls access to
   - **Actions**—The operations that can be performed on the entities
ClearAccess Installation Guide for more information.

5.6 Software setup validation

This topic is covered in the user documentation. See the Software setup validation section of the Hardening, validating, and securing the system chapter of ClearAccess Installation Guide.
6. Telecommunications and data transmission
ClearAccess does not use public communications networks. Therefore, the only requirements that apply are access control and prevention of data interception:
- Access control is addressed in section 3, “Access control.”
- ClearAccess does not use any network communications.

7. Use of public communications networks
ClearAccess does not use public communication networks.

8. Wireless communications
ClearAccess does not use wireless communication.

9. Independent verification systems
ClearAccess is not a vote-casting or vote-tabulating system; therefore, this section does not apply.

10. Voter Verifiable Paper Audit Trail requirements
ClearAccess is not a DRE system; therefore, this section does not apply.