Clear Ballot Event Logging Facts

Clear Ballot's system creates two logs while the system is running: The Election Activity Log and the Web Activity Log. Some overlapping information exists between the two logs. However, each log contains unique information, and together, with the Windows Event Log are considered the audit logs for the ClearCount system. See exhibit A.

The Web Activity Log records information from two additional sources the Election Activity Log does not. See exhibit B-1 and B-2.

One of the events the WAL records that the EAL does not is log-ins and log-outs to the admin account. See exhibit C.

Clear Ballot's system uses three logs for in-process auditing purposes, the Election Activity Log (EAL), the Web Activity Log (WAL), both created by ClearCount, and the Widows Event Logs (WEL) according to the ClearCount Functionality Description manual, section 1.5.3. See exhibit D.

The Election Preparation and Installation Guide clearly states that the WAL must be backed up separately prior to any upgrades, such as the upgrades done by Clear Ballot that deleted the WAL in several counties within Washington state. See exhibit E.

The Election Administration Guide states the EAL **and** the WAL should be checked before resuming the scanning of ballots. Both logs are needed for system operation. See exhibit F.

If someone were trying to gain access to the system, and did not enter the correct password, this would only be logged in the Web Activity Log. See exhibit G.

In the 1.5 version that was used by the counties that deleted the logs, it is the only log that records when the "display vote totals" feature is turned off or on.

Exhibits:

A.

1.3.2.2 Audit logging locations

All ClearCount system and software events, and errors are logged to the following locations:

- The ClearCount web activity log tracks all users' web-based actions for all of the jurisdiction's elections. This includes ScanServer, ScanStation and election administration station logins, logouts, and authentication failures; user access to election reports and card images; ballot card resolution; and administrative changes to elections and users.

- The ClearCount election activity log tracks events in a specific election, including user access to election reports and logs; as well as Tabulator start, processing, and end events; probable target card and scanning error identification; and ScanServer warning and error messages. The election activity log also tracks overall scanning rate and progress across ScanStations.
- The Windows Event Log on each ScanStation and election administration station logs all operating system-specific actions on each respective computer.
- The ScanServer, which is Linux-based, is configured as an appliance. After installation, under normal use, there is no need for any direct access to the ScanServer. Remote access to the ScanServer is logged to the ClearCount web activity log.

For a full description of the functional requirements for the ClearCount activity logs, see Event recording, logging, and tracking. For user documentation on these logs, see "ClearCount log files" in the *ClearCount Election Administration Guide*.

For a list of ClearCount warning and error messages and how to respond to them, see "ClearCount messages" in the *ClearCount Election Administration Guide*.

Clear Ballot Event Logging Facts

B-1.

6.1.1 Election activity log contents

The election activity log contains one row for each event recorded *for the selected election*. The log contains the following columns.

Time

Date and time of the election-specific event

Source

Source of the election-specific event:

- AdminDB—Includes changes made through the Election Administration page (URL equivalent to //*serverName*/admin/db).
- Background—Includes tasks performed through background jobs, such as backing up the named election.
- DeleteBox—Includes deletions of data and images for scanned boxes (so they can be rescanned).

- Resolver—Includes changes made through the Card Resolutions tool (URL equivalent to //*serverName*/remaking).
- Tabulator—Includes Tabulator application activity at ScanStations, such as startup, boxes being scanned, and errors (there is no URL).
- WebServer—Includes all election-specific events not covered by the other sources (for example, most user requests and interactions with reports and logs, and background job cancellations). Also includes the initial entry for any DeleteBox utility action.

B-2.

6.2.1 Web activity log contents

The web activity log contains one row for each event currently recorded in the ClearCount database. The log contains the following columns.

Time

Date and time of the event

Source

Source of the event:

- AdminDB—Includes changes through the Election Administration page (URL equivalent to //*serverName*/admin/db).
- AdminUser—Includes changes made through the User Administration page (URL equivalent to //*serverName*/user/db).

- Background—Includes tasks performed through background jobs, such as system maintenance activities.
- DeleteBox—Includes deletions of data and images for scanned boxes (so they can be rescanned).
- Linux—Includes ScanServer logins, logouts, and authentication failures.
- Resolver—Includes changes made through the Card Resolutions tool (URL equivalent to //*serverName*/remaking)
- Tabulator—Includes Tabulator application activity at ScanStations, such as startup, boxes being scanned, and errors (there is no URL).
- WebServer—Includes all election-specific events not covered by the other sources (for example, most user requests and interactions with reports and logs, and background job cancellations). Also includes the initial entry for any DeleteBox utility action.

C.

3.4 Hardening the ScanServer computer

The ScanServer computer is an Ubuntu Linux server that is configured as an appliance. After the ClearCount software has been installed, there is no need for any direct access to the ScanServer computer (other than during a support call with Clear Ballot). All normal pre-election, election, and postelection access to the ScanServer computer is by remote connection from the ScanStation computers or election administration station computers, all of which are running on authenticated Microsoft Windows workstations.

The Ubuntu Linux operating system requires at least one administrator account. Clear Ballot conforms to this requirement by allowing jurisdictions to create an administrator account with a password of their own choosing. Clear Ballot requires that the password that is created during installation be secured. The administrator account is *never* used, except as needed by Clear Ballot to diagnose a problem or reinstall the software. (Reinstallation completely replaces the software. All accounts initialized by the installation procedure must be recreated.) To verify compliance with this no-use policy, logins and logouts to the Linux server, if any, are recorded to the web activity log.

Clear Ballot recommends that you institute a policy of recording all logins to the ScanServer computer using the ScanServer Access Log located in the *ClearCount Election Administration Guide*. If any unexpected logins to the ScanServer computer appear in the web activity log, the system might be compromised. Alert the appropriate authorities for your jurisdiction and investigate the nature of these unexpected logins.

To completely harden the ScanServer computer, you must restrict access to the BIOS.

D.

1.5.3 In-process audit records

The ClearCountsystem logs system and user operations during the scanning and tallying of cards. The first message that is written to the web activity log shows the initial user logging in to the Linux ScanServer. Subsequently, the web activity log captures election and user creation and user login, logout, and use of the ClearCount web applications.

The ClearCount system generates event, error, and exception messages for its software components, as follows:

- The Tabulator application writes messages to its terminal screen, as well as to the election activity log for the election. The initiation and termination of each ScanStation's instance of the Tabulator application and its associated scanner are logged to the election activity log. For explanations of Tabulator error messages and suggested responses, see "ClearCount messages" in the *ClearCount Election Administration Guide*.
- The User Administration and Election Administration pages and election reports write messages to the web activity log. For explanations of error messages and suggested responses, see "ClearCount messages" in the *ClearCount Election Administration Guide*.
- The ScanStation logs messages in the following ways:
  - When a ScanStation is started or stopped, the action is logged to the Windows log.
  - Scanner and scanner software errors are logged to the election activity log. Documentation covering scanner error and exception information can be found in the manufacturer's documentation, which is included with the TDP submission.
  - In the event of a power failure, an unexpected restart is written to the Windows Event Log.

  - ScanServer session opening and closing are logged to the web activity log.
  - Transmission errors, memory errors, or problems saving files are written to the web activity log. For example, if a user rescanned a previously scanned box, the system writes an alert to the web activity log.

E.

3.3 Updating ClearCount

Updated ClearCount software is installed over the previous version. You do not need to uninstall the previous version.

Security updates should be made to the ClearCount system on a periodic basis, but must be in the form of new software versions issued by Clear Ballot and approved/certified by the jurisdiction's state election governance office.

Installing ClearCount erases any election databases currently residing on the ScanServer. Before installing an upgrade, back up all elections, export the web activity log, export the Windows logs, and export your user accounts. See "Backing up an election," "Web activity log," "Exporting Windows logs," and "Exporting user accounts" in the *ClearCount Election Administration Guide* for instructions.

Before updating

- Back up all elections.
- Export the web activity log.
- Export the Windows logs.
- Export your user accounts.
- Ensure that you have the router's IP address.
- Print the "Installation checklist" on page 131.
- Install the updated software following the process described in Installing ClearCount.

F.

3.2 Resuming scanning

To restart the ClearCount system:

1. Reactivate or restart any of the hardware (scanners, computers, or network switches) that you shut down.
2. Log in to an election administration station as an administrator.
3. Check the election activity log and the web activity log to ensure nothing unexpected (such as unauthorized logins) occurred since the system was shut down.
4. Restart the Tabulator application on each ScanStation as explained in Task 1: Start the Tabulator application. The scanning supervisor must enter the password to start the Tabulator application.
5. On the election administration station, check the Statement of Cards Cast with Precincts and the Statement of Votes Cast reports that you generated when shutting down the system the previous day against the live version to make sure that they match.
6. In the Phase column for the election, click the phase to open the Change Election Phase dialog, click the **Status** drop-down list, select **Scanning**, and then click **Save**.
7. Initialize the ScanStations and resume scanning. See Checklist 2: Initializing ScanStations.

For details about system breakdown and storage, see the *ClearCount Election Preparation and Installation Guide*.

G.

1.4.4 Protection against attempts at improper data entry or retrieval

Improper data entry and retrieval are prohibited through numerous mechanisms.

When a user is created in the system, he or she is assigned a user name and a password. Access to the system requires logging in with the user name and password. The ClearCount system times out user login sessions after 24 hours of inactivity or when the ScanServer is restarted, whichever occurs first. All user actions, including viewing election reports, are logged by user name and machine name.

A user who tries to log in with an incorrect password receives a *login failed* message and is not allowed to access the system. A warning message detailing the failed login attempt is logged to the web activity log. (Because it is not associated with a particular election, it is not logged to the election activity log.)