Clear Ballot

ClearVote 2.3

ClearCount Installation Guide

ClearCount Installation Guide

Clear Ballot Part Number: 100006-10020

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

Document Type: Customer

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

Document history

Date	Description	Version	Authors
01/10/2017	Initial submission to EAC	1.0	Joni G. McNutt
02/03/2017	Minor typographical and reference-related edits	1.0.1	Joni G. McNutt
03/30/2017	Minor typographical and reference-related edits based on feedback from the State of Colorado	1.0.2	Joni G. McNutt
04/28/2017	Minor updates based on feedback from the State of Colorado and Clear Ballot Quality Assurance	1.0.3	Joni G. McNutt
05/03/2017	Added RAID 1 and RAID 5 configuration processes to ClearCount installation, minor updates based on feedback from Clear Ballot Quality Assurance	1.0.4	Joni G. McNutt
05/15/17	Added setup process for network switch and static IP addresses, minor updates based on feedback from Clear Ballot Quality Assurance	1.0.5	Joni G. McNutt
06/16/2017	Minor updates for vote-by-mail campaign	1.0.5	Joni G. McNutt
07/21/2017	Added information to the Updating ClearCount section, added information to Backing up an election process, updated the Installing ClearCount process, rearranged the Configuring ScanStations section, updated the Mapping an election administration station section, made edits to Windows procedures for Windows 10 Pro, added a section about Disabling the Edge browser, minor edits	1.1	Joni G. McNutt
10/04/2017	Minor edits	1.1.1	Joni G. McNutt
10/20/2017	Added sections for ScanStation and election administration station hardening, removed obsolete hardening procedures, added sections for verifying operating systems, updated the installation checklist, minor edits	1.2	Joni G. McNutt
01/19/2018	Vote-by-Mail campaign 2, added Installing Windows Drivers section, updated Windows installation procedure, minor edits	1.2.1	Joni G. McNutt

Date	Description	Version	Authors
04/13/2018	Added RAID configurations section, updated the Installing the Windows 10 Pro operating system sections, removed the router information, updated the network switch information, minor edits	1.2.2	Joni G. McNutt
06/15/2018	Revised the Creating a desktop shortcut to the P: drive section, the Running the scanner update script section, the Updating Windows Defender Antivirus sections, and the Mapping the election administration station to the ScanServer section; added the Updating user account access section	1.2.3	Joni G. McNutt
08/03/2018	Added information about encrypted hard drives and USB drives	1.2.4	Joni G. McNutt
08/15/2018	Updated cover, minor edits	1.2.5	Joni G. McNutt
04/12/2019	Updated installation instructions, added information about hardening the network switch, minor edits	1.2.6	Joni G. McNutt
06/21/2019	Removed information about updating BIOS, minor edits	1.2.7	Joni G. McNutt
08/13/2019	Updated the Creating a restore point sections	1.2.8	Joni G. McNutt
11/22/2019	Added process for setting up the Fujitsu fi-7800 and fi-7900 scanners, removed information about Flash and Firefox, minor edits	1.2.9	Joni G. McNutt
12/20/2019	Minor edits	1.2.10	Joni G. McNutt
01/27/2020	Minor edits	1.2.11	Joni G. McNutt
02/12/2020	Minor edits	1.2.12	Joni G. McNutt
12/07/2020	Updated Preface. Reversed two steps in the directions for setting up the Fujitsu fi-7800 and fi-7900 scanners. Changed ScanServer to CountServer. Changed election administration station to CountStation. Reused components. Added "Installing the Windows patch," "Turning off BitLocker," and "Enabling BitLocker (optional)."	1.2.13	Kathleen Gaetz Joe Srednicki

Date	Description	Version	Authors
12/16/2020	Minor edits	1.2.14	George Petta
01/25/2021	Updated "Login credentials and guidelines."	1.2.15	Joe Srednicki
09/30/2021	Updated "Installing the Windows drivers" and minor edits	1.2.16	Joe Srednicki
10/05/2021	Moved chapters containing administrative information to the Election Administration Guide. Updated "Enabling BitLocker" and "Disabling BitLocker." Minor edits.	2.0	Joe Srednicki
03/18/2022	Updated "Installing the Windows 10 Pro operating system."	2.0.1	Joe Srednicki
03/23/2022	Added "Updating the BIOS version on the Dell 5521."	2.0.2	Joe Srednicki
03/23/2023	Updated "Hardware components," "Updating Microsoft Defender Antivirus," and "Installing the CountServer." Added table captions to certain topics. Made minor edits.	2.0.3	Erica Riddle, Kristina Arnold, Douglas McCulloch
04/04/2023	Minor edits	2.0.4	Douglas McCulloch

Table of contents

Preface

This section defines the purpose of this document.

About this document

This document describes how to install and configure ClearCount software and supporting hardware.

For information about election-related tasks, see the *ClearCount Election Administration Guide*.

Scope of this document

This document contains the following sections:

- Chapter 1. High-level system description
- Chapter 2. RAID configurations
- Chapter 3. Installing the CountServer
- Chapter 4. Configuring ScanStations
- Chapter 5. Configuring CountStations
- Chapter 6. Validating and securing the system
- Chapter 7. Removing software
- Appendix A. Login credential rules and guidelines
- Appendix B. Installation checklist

Intended audience

This document is for election officials and election staff who are responsible for operations and maintenance before, during, and after an election. Clear Ballot personnel also use this document to support election officials and election 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*

Contact us

Clear Ballot Group welcomes your feedback on our documentation. Please send comments to Documentation@ClearBallot.com.

If you have questions about using your product, contact your Clear Ballot representative.

Chapter 1. High-level system description

ClearCount is a central-count optical-scan system. ClearCount uses unmodified commercial off-the-shelf (COTS) computers that run the Ubuntu Linux and Microsoft Windows operating systems and support specific scanner models.

ClearCount aggregates precinct results but is not intended for direct voter interaction.

1.1 Hardware components

The ClearCount system contains the hardware components listed in Table 1-1. All these components are COTS hardware and are connected over a closed, wired Ethernet.

Table 1-1. Hardware components

Component	Description
CountServer	A computer running the ClearCount software and hosting the election database and the web server that serves the election reports. The CountServer computer uses the Ubuntu Linux operating system. A configured version of Ubuntu Linux is installed with the ClearCount software.
ScanStations	One or more Microsoft Windows computers linked by a closed, wired Ethernet connection to the CountServer computer through the network switch. Each ScanStation computer is paired to an individual scanner. The computer and scanner pairs are used to scan and adjudicate ballots.
Scanners	Each scanner is connected to a single ScanStation computer with a USB cable.
CountStations	One or more Microsoft Windows computers installed with browser software, linked by a wired Ethernet connection to the CountServer computer by the network switch. Election officials use this computer to create election reports. The election administrator also uses this computer to monitor the system, upload ClearCast results, and manage databases and users.
Network switch	Connects the ScanStation and CountStation computers to the CountServer computer over a wired, closed Ethernet.
Uninterruptible power supply (UPS)	Used to ensure that the CountServer computer or other desktop computer is available if a power outage occurs.
External hard drive	Used to back up and restore elections. The external hard drive connects to the CountServer computer.

The minimum configuration of hardware contains one CountServer, one ScanStation computer, and one CountStation connected by Ethernet cables to a single network switch. It is also possible to expand the closed network to include multiple ScanStations and CountStations with a single CountServer computer.

All connections between devices in the system are closed and wired. The system does not use wireless connectivity. Wireless capabilities present on any hardware used with the system must be disabled.

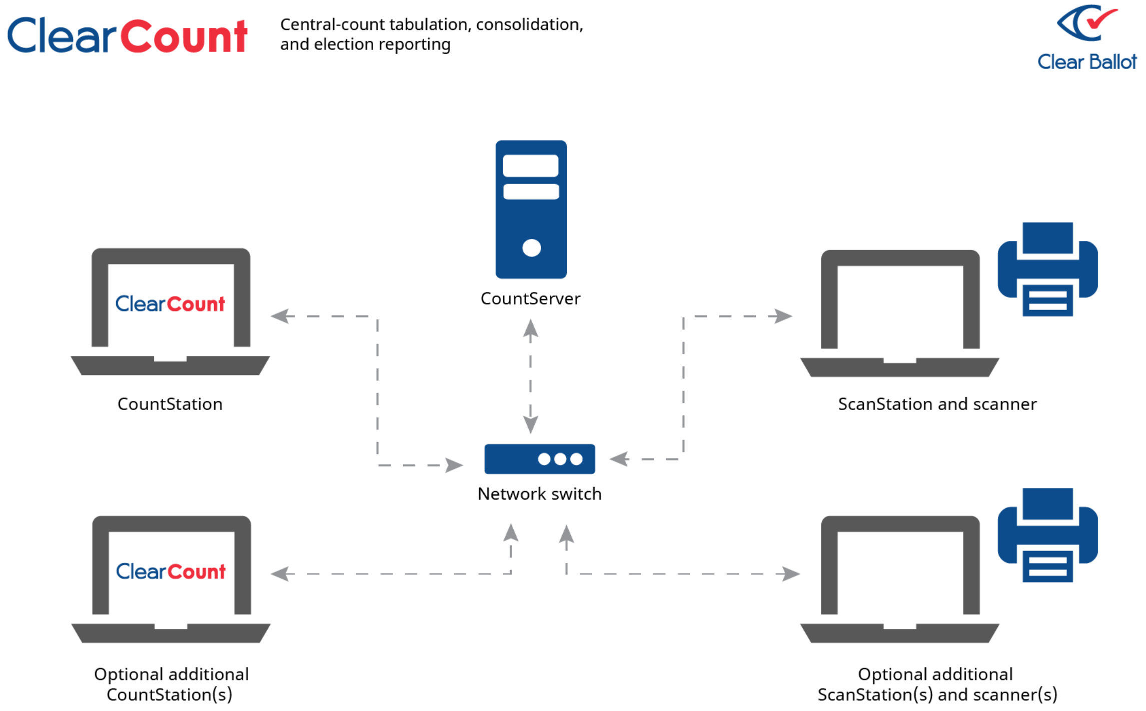

ClearCount
Central-count tabulation, consolidation, and election reporting
Clear Ballot
CountServer
ClearCount
CountStation
ScanStation and scanner
Network switch
ClearCount
Optional additional CountStation(s)
Optional additional ScanStation(s) and scanner(s)

Figure 1-1. ClearCount hardware configuration

1.2 Software components

The ClearCount software contains the components listed in 1.2.

Table 1-2. Software components

Component	Description
Tabulator application	The Tabulator software is stored on the CountServer and an instance of the Tabulator application runs on each ScanStation computer to handle the ballots it scans. The Tabulator application analyzes the incoming images and transfers them to the local output folder named *CBGBallotImages*, from where the CountServer computer retrieves them. The Tabulator application is accessible from a CountStation.
ResultsUploader application	The ResultsUploader application transfers ClearCast results from a USB drive to a CountStation. An instance of the ResultsUploader runs on each CountStation. When the ResultsUploader is in an uploading state, the application does the following: • Monitors the CountStation for a newly inserted USB drive containing election results from ClearCast • Uploads the ClearCast election results from the newly detected USB drive to CountServer • Reports the status of the results as they are validated and merged on the CountServer
Election database	A centralized election database resides on the CountServer. An election database collects and collates the output of each Tabulator instance. The resulting data is accessible through election reports from a CountStation.
Election reports	The browser-based suite of reports provides election results and analysis and allows election officials to review individual card images. A web server on the CountServer computer provides the reports, which are viewable from a CountStation.
Card Resolutions tool	This tool allows election officials to review and appropriately resolve unreadable cards from a CountStation. Election officials can review the unreadable cards that the ClearCount system digitally outstacks, determine whether the cards are votable, and process the cards accordingly.
User and election management	From the User Administration pages, the administrator can add, rename, or delete users; assign access levels; and change user passwords. From the Election Administration pages, the administrator can create or delete an election, set an election as active, change the election phase, and back up or restore an election. These features are accessible from a CountStation.

All files that make up the ClearCount software reside on a single CountServer that is shared by all connected ScanStation computers. The Tabulator application on each ScanStation computer and the ResultsUploader on each CountStation are read at run-time from files that reside on the CountServer.

The only software programs that need to be installed on the ScanStation computers, besides the Microsoft Windows operating system and drivers, are the scanner software and drivers required by the scanner hardware.

The only software program that needs to be installed on the CountStations, besides the Microsoft Windows operating system and drivers, is Google Chrome.

Chapter 2. RAID configurations

CountServer computers with RAID (Redundant Array of Independent Disks) can be configured to create large reliable data stores from multiple computer hard-disk drives (HDDs or SSDs). RAID configurations can help provide protection against hardware defects, errors, and failures.

- If your CountServer computer has a hardware RAID controller, you likely already have RAID 1 or RAID 5 configured on your server. To verify if your server already has RAID, contact a Clear Ballot employee with your Dell Express Service Code.
- If your CountServer computer has a hardware RAID controller, you can create a RAID 1 or RAID 5 configuration *before* installing the ClearCount software. The configuration depends on the number of hard disks in the computer
  - "Configuring the RAID controller as RAID 1" below—2 Storage Drives
  - "Configuring the CountServer RAID controller for RAID 5" on page 18—3 to 4 Storage Drives
- If your CountServer computer does *not* have a hardware RAID controller, you can create a virtual RAID volume during the installation process for the ClearCount software. See the following sections:
  - "Creating a RAID 1 virtual volume" on page 35
  - "Creating a RAID 5 virtual volume" on page 38

2.1 Configuring the RAID controller as RAID 1

For a RAID 1 configuration, a computer must have at least two hard disks.

The following steps describe how to configure a Dell PowerEdge T440. Consult the computer manufacturer's documentation when configuring other servers.

To configure as RAID 1:

1. Power on the computer and while it is starting up, press the F2 key to enter the System Setup screen.
2. Use the arrow keys to navigate to and select the **Device Settings** option and press **Enter**.
3. From the Device Settings menu, select the **RAID Controller** option that is listed and press **Enter** to view the Main Menu screen.
4. From the Main Menu options, select **Configuration Management** and press **Enter**.
5. From the Configuration Management menu, select the **Convert to RAID Capable** option and press **Enter**.

   If you do not see the Convert to RAID Capable option, the computer's RAID controller has already been configured for RAID.

6. On the following screen, in the Physical Disk to Convert to RAID Capable section, select the checkbox for each disk you want to use for the RAID 1 configuration. You must select at least two.

7. Select **OK** and press **Enter**.

8. On the following screen, select the **Confirm** checkbox, select **Yes** and press **Enter**.

9. A screen indicates that the operation was successful. Select **OK** and press **Enter**.

10. The Configuration Management screen reappears. Tab to the **Back** button and press **Enter** to return to the Main Menu screen.

11. Select the **Configuration Management** option and press **Enter**.

12. Select the **Create Virtual Disk** option and press **Enter**.

13. On the following screen, in the Choose Unconfigured Physical Disks section, select the checkbox for each disk you want to use for the RAID 1 configuration.

14. Select **Apply Changes** and press Enter.

15. On the following screen, select the **Select RAID Level** drop-down list, use the arrow keys to select **RAID 1**, and press Enter.

16. Select the **Select Physical Disks** option and press Enter.

17. A screen indicates that the operation was successful. Select **OK** and press Enter.

18. On the Create Virtual Disk screen, scroll to the bottom of the page, select **Create Virtual Disk** and press Enter.

19. On the following screen, select the **Confirm** checkbox, select **Yes** and press Enter.

20. A screen indicates that the operation was successful. Select **OK** and press Enter.

    To verify that the RAID controller was configured successfully, navigate back to the Main Menu screen and select the **Virtual Disk Management** option. If the process was successful, a single configuration appears with a status of *Ready*.

21. Tab to the **Exit** option at the top right and exit out of the system setup.

22. Restart the computer and proceed with the ClearCount installation process described in "Installing the CountServer" on page 20.

2.2 Configuring the CountServer RAID controller for RAID 5

For a RAID 5 configuration, a computer must have a minimum of three hard disks.

The following steps describe how to configure a Dell PowerEdge T440. Consult the computer manufacturer's documentation when configuring other servers.

To configure for RAID 5:

1. Power on the computer and while it is starting up, press the F2 key to enter the System Setup screen.
2. Use the arrow keys to navigate to and select the **Device Settings** option and press the Enter key.
3. From the Device Settings menu, select the **RAID Controller** option that is listed and press Enter to enter the Main Menu screen.
4. From the Main Menu options, select **Configuration Management** and press Enter.
5. From the Configuration Management menu, select the **Convert to RAID Capable** option and press Enter.

   If you do not see the Convert to RAID Capable option, the computer's RAID controller has already been configured for RAID.
6. On the following screen, in the Physical Disk to Convert to RAID Capable section, select the checkbox for each disk you want to use for the RAID 5 configuration. You must select at least three.
7. Select **OK** and press Enter.
8. On the following screen, select the **Confirm** checkbox, select **Yes** and press Enter.
9. A screen indicates that the operation was successful. Select **OK** and press Enter.
10. The Configuration Management screen reappears. Tab to the **Back** button and press Enter to return to the Main Menu screen.
11. Select the **Configuration Management** option and press Enter.
12. Select the **Create Virtual Disk** option and press Enter.
13. On the following screen, select the **Select RAID Level** drop-down list, use the arrow keys to select **RAID 5**, and press Enter.
14. Select the **Select Physical Disks** option and press Enter.
15. On the following screen, in the Choose Unconfigured Physical Disks section, select the checkbox for each disk you want to use for the RAID 5 configuration.

16. Select **Apply Changes** and press Enter.

17. A screen indicates that the operation was successful. Select **OK** and press Enter.

18. On the Create Virtual Disk screen, scroll to the bottom of the page, select **Create Virtual Disk** and press Enter.

19. On the following screen, select the **Confirm** checkbox, select **Yes** and press Enter.

20. A screen indicates that the operation was successful. Select **OK** and press Enter.

    To verify that the RAID controller was configured successfully, navigate back to the Main Menu screen and select the **Virtual Disk Management** option. If the process was successful, a single configuration appears with a status of *Ready*.

21. Tab to the **Exit** option at the top right and exit out of the system setup.

22. Restart the computer and proceed with the ClearCount installation process as described in "Installing the CountServer" on page 20.

Chapter 3. Installing the CountServer

The ClearCount software is installed only on the CountServer, not on the ScanStations or CountStations. The CountServer installation generally takes 45 to 60 minutes, but may take longer depending on the hardware configuration.

During installation, the ClearCount software overwrites the existing operating system on the CountServer computer with its own Ubuntu Linux operating system. If you are performing an upgrade, back up data that resides on the computer before beginning the CountServer installation process. See "Updating the ClearCount software" on page 44.

The ClearCount CountServer installation process involves the following tasks:

1. See "Changing the BIOS boot setting" below.
2. See "Installing ClearCount software" on the next page.
   - (Optional) See "Creating a RAID 1 virtual volume" on page 35.
   - (Optional) See "Creating a RAID 5 virtual volume" on page 38.
3. See "Restricting access to the BIOS on the CountServer" on page 42.

If you make a mistake at any point during the installation, the best practice is to quit the installation and restart from the beginning. There is no need to uninstall. The Go Back options in the installation program sometimes lead to a summary of the preceding steps rather than to the previous screen.

Note: You will create several user names, passwords, and IP addresses during the installation. Print the Installation checklist (page 124) to track these items. Linux is case-specific so be sure to record each item accurately. Maintain this information in a safe and secure location.

3.1 Changing the BIOS boot setting

Before installing the ClearCount software, make sure that the BIOS boot setting of the CountServer is UEFI.

The following steps below are an example and may differ by computer manufacturer and computer model. Consult the computer manufacturer's documentation for more information.

To change the BIOS boot setting:

1. Ensure that no external drives are mounted.
2. Power on the CountServer computer and *immediately* press the key that accesses the system setup menu.

   For example, if using a Dell computer, press **F2** key to access the system setup menu.

The key used depends upon computer make and model. Consult your computer's documentation for details. To access the startup menu, you must press the key very quickly. If Windows begins to launch, it is too late. Restart the computer and try again.

3. From the System Setup Main Menu, select **System BIOS** and press the **Enter** key.
4. From the System BIOS Settings, select **Boot Settings** and press **Enter**.
5. Select the **UEFI** option, press the Tab key to select the **Back** button, and then press **Enter**.
6. From the System BIOS Settings, press the Tab key to select **Finish** and then press **Enter**.
7. When a warning dialog appears, select **Yes** and press **Enter**.
8. When a message indicating success appears, press **Enter**.
9. From the System Setup main menu, press the **Tab** key to select the **Finish** button and press **Enter**.
10. When a dialog appears to confirm exiting, select **Yes** and then press **Enter**.

    The computer restarts.

3.2 Installing ClearCount software

Installing the ClearCount software erases any election databases currently residing on the CountServer computer.

Before installing an upgrade, do the following:

- Back up all elections.
- Export the following:
  - The web activity log
  - The Windows log files
  - User accounts

See "Backing up an election", "Web activity log", "Exporting Windows logs", and "Exporting user accounts" in the *ClearCount Election Administration Guide*.

To install ClearCount software:

1. Make sure that the Ethernet cable is connected from the CountServer to the network switch and that the network switch is powered on.
2. Make sure you have performed the steps in "Changing the BIOS boot setting" on the previous page.
3. Ensure the CountServer computer is powered off and insert the ClearCount CountServer DVD into the disc drive.

4. Power on the CountServer.

   As the computer starts up, *immediately* press the key that accesses the startup menu. (For example, if using a Dell computer, press **F11** or **F12**.)

   The key used depends upon computer make and model. Consult your computer's documentation for details. To access the startup menu, press the key very quickly. If Windows begins to launch, it is too late. Restart the computer and try again.

5. When the Boot screen appears, press **Enter**.

   For some computers, you see a Boot menu screen. On these computers, do the following:

   a. Select the One-Shot BIOS boot menu.

   b. Select the appropriate drive.

      Example: Optical drive connected to USB1: DVDRAM GPGO NBSO

   c. Select the drive with the CountServer DVD.

   At this point, the installation program launches.

   As the installation program advances from screen to screen, delays can occur as the software loads.

6. On the Language screen, accept the default, **English**, by pressing **Enter**.

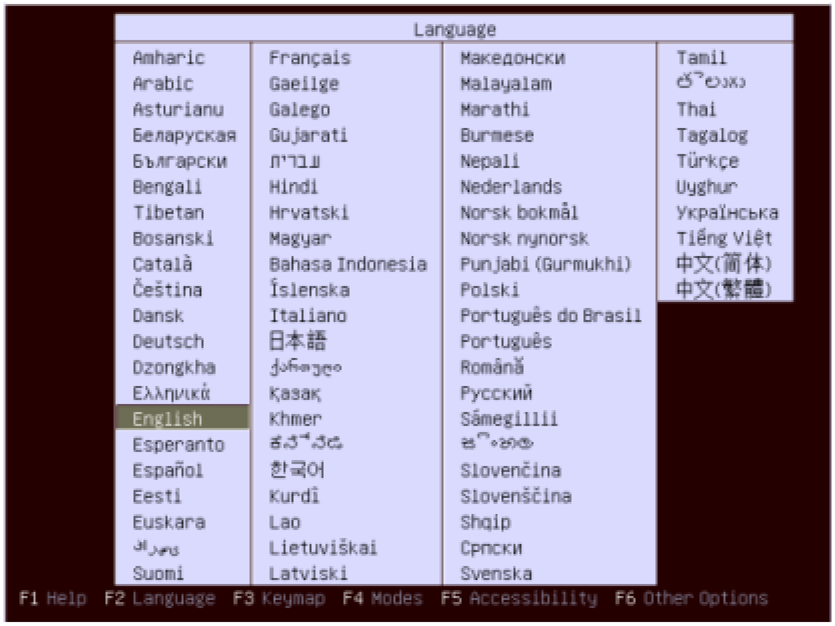
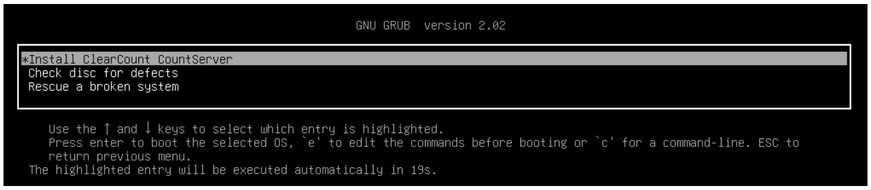


Figure 3-1. Language screen

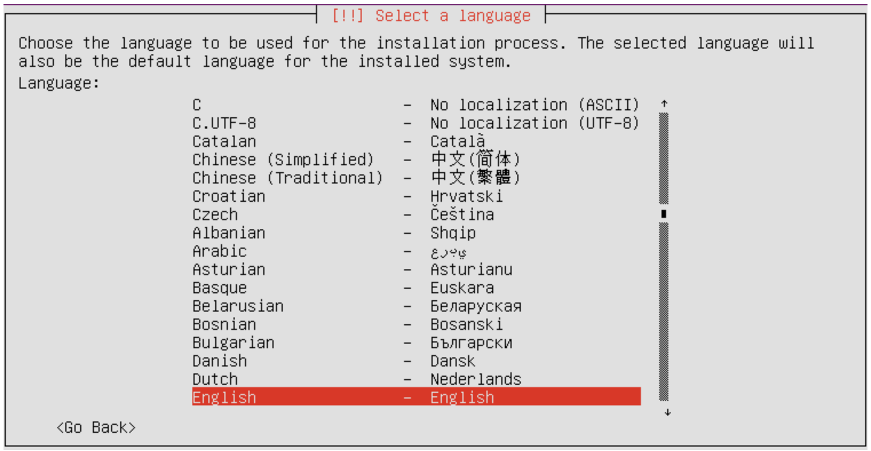
7. On the Ubuntu splash screen, select **Install ClearCount CountServer** and press **Enter**.



```
                         GNU GRUB  version 2.02

*Install ClearCount CountServer
 Check disc for defects
 Rescue a broken system

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line. ESC to
    return previous menu.
 The highlighted entry will be executed automatically in 19s.
```

Figure 3-2. Ubuntu splash screen

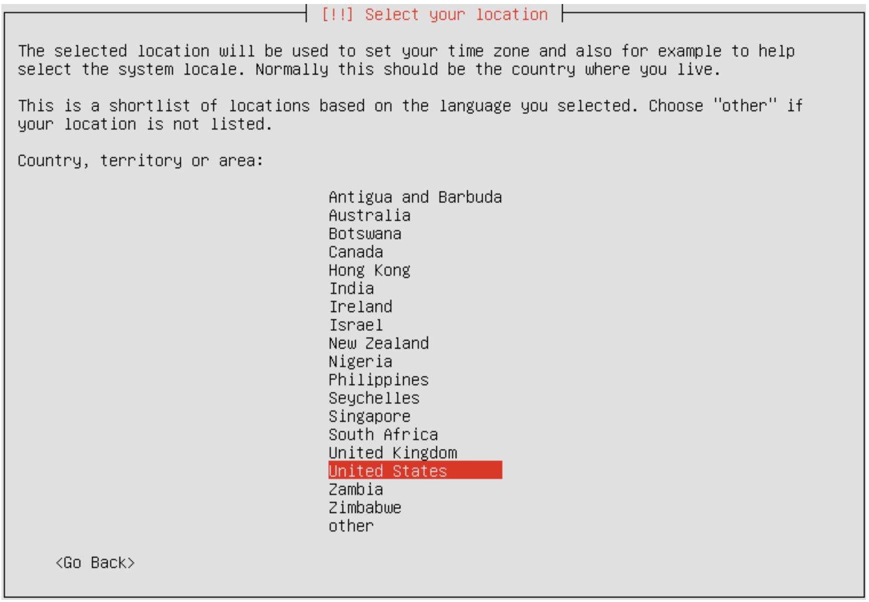
8. On the Select a language screen, accept the default, **English**, by pressing **Enter**.



```
                          [!!] Select a language

Choose the language to be used for the installation process. The selected language will
also be the default language for the installed system.
Language:
                   C                       -  No localization (ASCII)
                   C.UTF-8                 -  No localization (UTF-8)
                   Catalan                 -  Català
                   Chinese (Simplified)    -  中文(简体)
                   Chinese (Traditional)   -  中文(繁體)
                   Croatian                -  Hrvatski
                   Czech                   -  Čeština
                   Albanian                -  Shqip
                   Arabic                  -  عربي
                   Asturian                -  Asturianu
                   Basque                  -  Euskara
                   Belarusian              -  Беларуская
                   Bosnian                 -  Bosanski
                   Bulgarian               -  Български
                   Danish                  -  Dansk
                   Dutch                   -  Nederlands
                   English                 -  English

    <Go Back>
```

Figure 3-3. Select a language screen

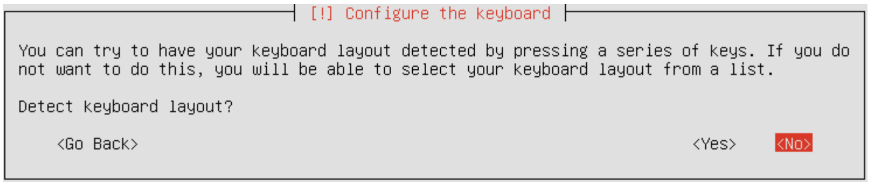
9. On the Select your location screen, accept the default, **United States**, by pressing **Enter**.



```
                          [!!] Select your location

The selected location will be used to set your time zone and also for example to help
select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if
your location is not listed.

Country, territory or area:

                                  Antigua and Barbuda
                                  Australia
                                  Botswana
                                  Canada
                                  Hong Kong
                                  India
                                  Ireland
                                  Israel
                                  New Zealand
                                  Nigeria
                                  Philippines
                                  Seychelles
                                  Singapore
                                  South Africa
                                  United Kingdom
                                  United States
                                  Zambia
                                  Zimbabwe
                                  other

    <Go Back>
```

Figure 3-4. Select your location screen

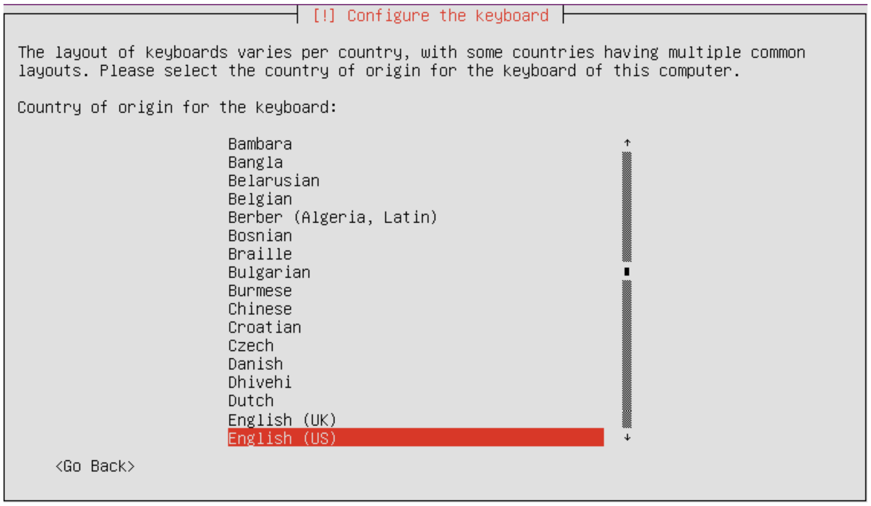
10. On the first Configure the keyboard screen, accept the default, **No**, by pressing **Enter**.



```
[!] Configure the keyboard

You can try to have your keyboard layout detected by pressing a series of keys. If you do
not want to do this, you will be able to select your keyboard layout from a list.

Detect keyboard layout?

    <Go Back>                                                             <Yes>    <No>
```

Figure 3-5. First Configure the keyboard screen

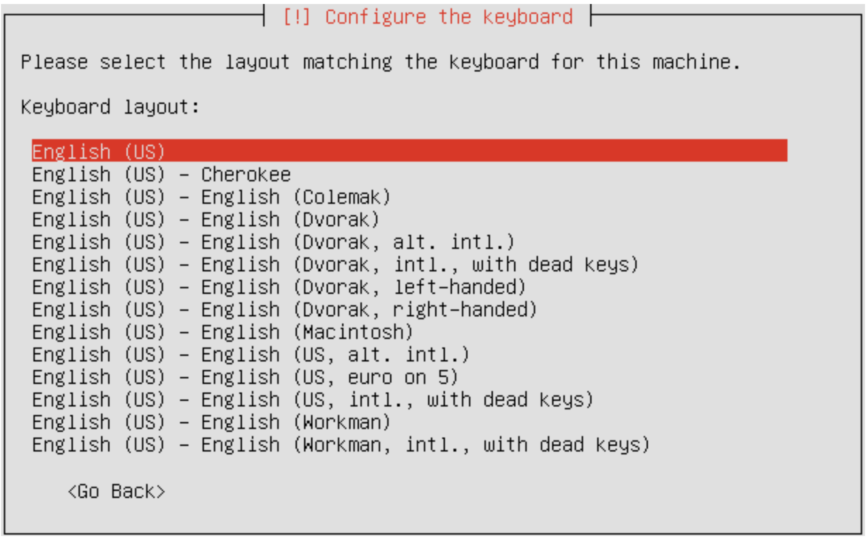
11. On the second Configure the keyboard screen, press **Enter** to accept the default of **English (US)**.



```
[!] Configure the keyboard

The layout of keyboards varies per country, with some countries having multiple common
layouts. Please select the country of origin for the keyboard of this computer.

Country of origin for the keyboard:

                      Bambara
                      Bangla
                      Belarusian
                      Belgian
                      Berber (Algeria, Latin)
                      Bosnian
                      Braille
                      Bulgarian
                      Burmese
                      Chinese
                      Croatian
                      Czech
                      Danish
                      Dhivehi
                      Dutch
                      English (UK)
                      English (US)

    <Go Back>
```

Figure 3-6. Second Configure the keyboard screen

12. On the third Configure the keyboard screen, accept the default, **English (US)**, by pressing **Enter**.

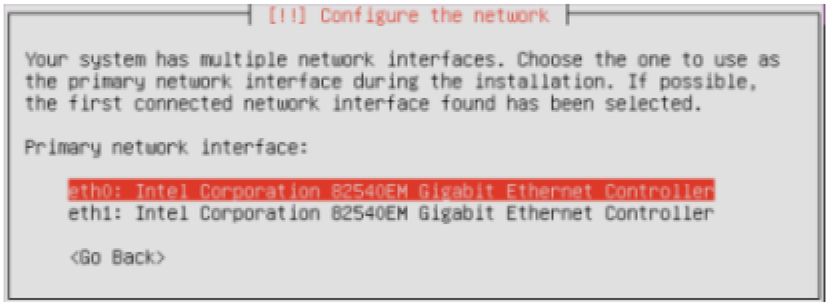


```
[!] Configure the keyboard

Please select the layout matching the keyboard for this machine.

Keyboard layout:

 English (US)
 English (US) - Cherokee
 English (US) - English (Colemak)
 English (US) - English (Dvorak)
 English (US) - English (Dvorak, alt. intl.)
 English (US) - English (Dvorak, intl., with dead keys)
 English (US) - English (Dvorak, left-handed)
 English (US) - English (Dvorak, right-handed)
 English (US) - English (Macintosh)
 English (US) - English (US, alt. intl.)
 English (US) - English (US, euro on 5)
 English (US) - English (US, intl., with dead keys)
 English (US) - English (Workman)
 English (US) - English (Workman, intl., with dead keys)

    <Go Back>
```

Figure 3-7. Third Configure the keyboard screen

13. (If applicable) On the Configure the Network screen, select the network port you want to use and press **Enter**. Generally, you want to select the first option (eth0).

    The installation program skips this screen if the computer has only one network port.

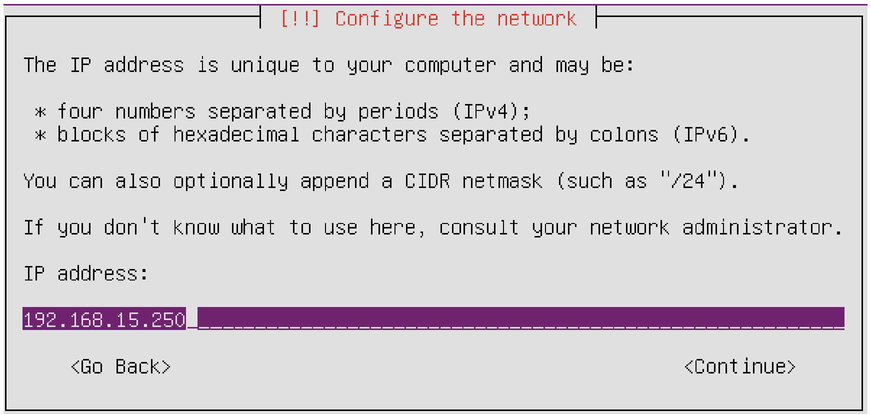
    

    ```
    [!!] Configure the network

    Your system has multiple network interfaces. Choose the one to use as
    the primary network interface during the installation. If possible,
    the first connected network interface found has been selected.

    Primary network interface:

        eth0: Intel Corporation 82540EM Gigabit Ethernet Controller
        eth1: Intel Corporation 82540EM Gigabit Ethernet Controller

        <Go Back>
    ```

    Figure 3-8. First Configure the Network screen

14. On the next (or first) Configure the Network screen, enter the server IP address and press **Enter**.

    The first three sections of the server’s IP address, separated by periods, must match those used by your network switch. "Installing the network switch" on page 55. The fourth section can be any unused number. Clear Ballot recommends 250. For example, if the network switch IP address is 192.168.15.1, use 192.168.15.250 for the server IP address. If you are installing on a backup server, ensure its IP address is not the same as the IP address of the primary server.

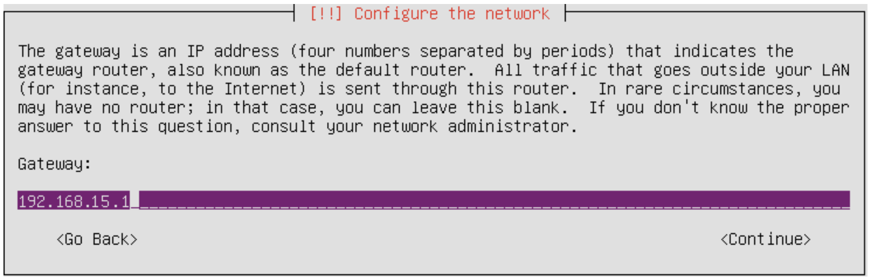
    

    ```
    [!!] Configure the network

    The IP address is unique to your computer and may be:

     * four numbers separated by periods (IPv4);
     * blocks of hexadecimal characters separated by colons (IPv6).

    You can also optionally append a CIDR netmask (such as "/24").

    If you don't know what to use here, consult your network administrator.

    IP address:

    192.168.15.250_

        <Go Back>                                              <Continue>
    ```

    Figure 3-9. Second Configure the Network screen

15. (Recommended) Record the server's IP address on the Installation checklist (page 124).

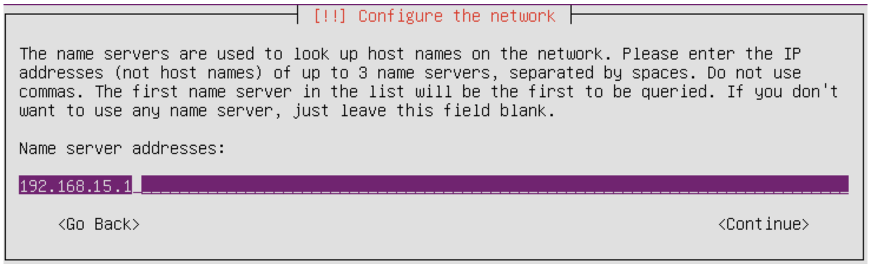
16. On the next Configure the Network screen, enter the network switch IP address that you set previously (such as 192.168.15.1) in the Gateway field and press **Enter**.



```
[!!] Configure the network

The gateway is an IP address (four numbers separated by periods) that indicates the
gateway router, also known as the default router.  All traffic that goes outside your LAN
(for instance, to the Internet) is sent through this router.  In rare circumstances, you
may have no router; in that case, you can leave this blank.  If you don't know the proper
answer to this question, consult your network administrator.

Gateway:

192.168.15.1

<Go Back>                                                                  <Continue>
```

Figure 3-10. Third Configure the Network screen

17. On the next Configure the Network screen, re-enter the network switch IP address in the Name server addresses field and press **Enter**.



```
[!!] Configure the network

The name servers are used to look up host names on the network. Please enter the IP
addresses (not host names) of up to 3 name servers, separated by spaces. Do not use
commas. The first name server in the list will be the first to be queried. If you don't
want to use any name server, just leave this field blank.

Name server addresses:

192.168.15.1

<Go Back>                                                                  <Continue>
```

Figure 3-11. Fourth Configure the Network screen

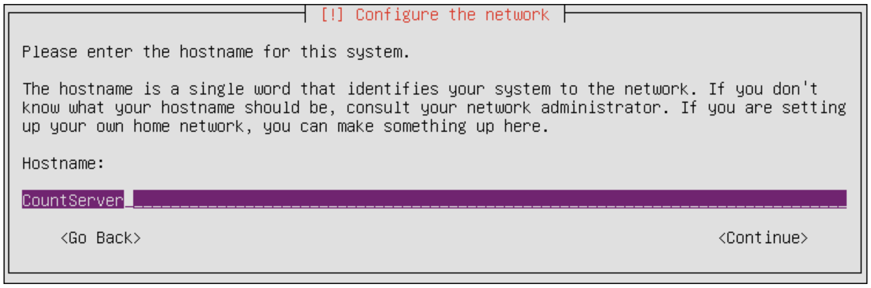
18. On the final Configure the Network screen shown in Figure 3-12 on page 27, enter the hostname and press **Enter**.

    The hostname identifies the CountServer computer and is used in browsers to navigate to the CountServer computer. Clear Ballot *strongly* recommends accepting the default hostname, *CountServer*.

    If you are installing on a backup server within the same network, ensure its hostname is not the same as the hostname of the primary server.

    Example: Use *CountServer1* and *CountServer2*.

    Note: If a jurisdiction has multiple CountServers, each one must have a distinct hostname.



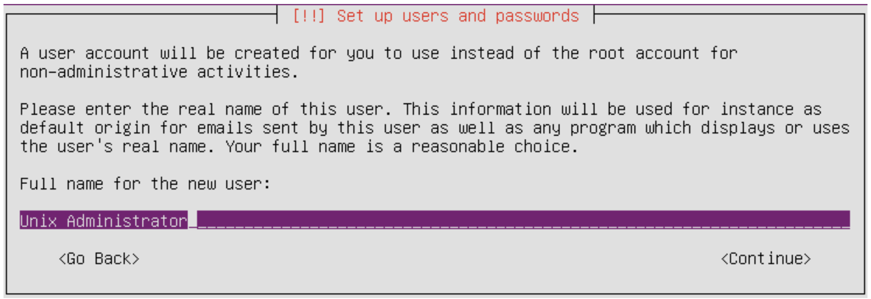
```
[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't
know what your hostname should be, consult your network administrator. If you are setting
up your own home network, you can make something up here.

Hostname:

CountServer

    <Go Back>                                                          <Continue>
```

Figure 3-12. Fifth Configure the Network screen

19. (Recommended) Record the hostname on the Installation checklist (page 124).

20. On the first Set Up Users and Passwords screen, accept **Unix administrator**, the default full user name for the administrator of the local Linux account, by pressing **Enter**.

    The ClearCount system records all logins for this account. Log in and use this account only if instructed to do so by Clear Ballot Technical Support. It is *not* for normal electoral duties.

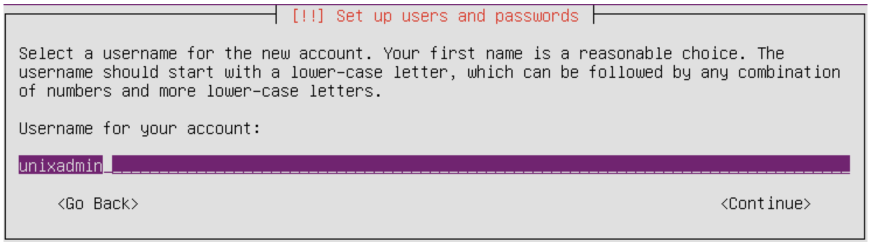


```
[!!] Set up users and passwords

A user account will be created for you to use instead of the root account for
non-administrative activities.

Please enter the real name of this user. This information will be used for instance as
default origin for emails sent by this user as well as any program which displays or uses
the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Unix Administrator

    <Go Back>                                                          <Continue>
```

Figure 3-13. First Set Up Users and Passwords screen

21. On the second Set up Users and Passwords screen, enter the user name for logging in to the CountServer administrator account and press **Enter**.

    Spaces are not allowed in the user name.



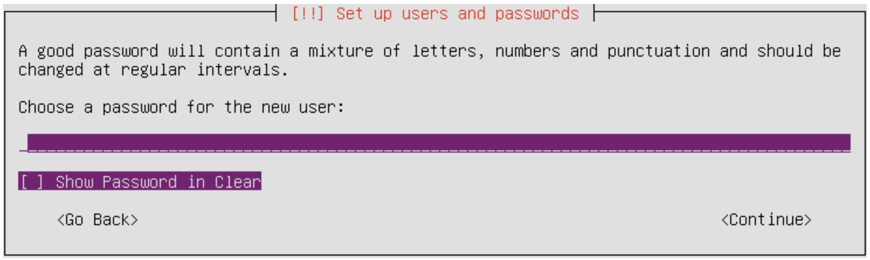
```
[!!] Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The
username should start with a lower-case letter, which can be followed by any combination
of numbers and more lower-case letters.

Username for your account:

unixadmin_______________________________________________________________________________

    <Go Back>                                                               <Continue>
```

Figure 3-14. Second Set Up Users and Passwords screen

22. (Recommended) Record the user name of the CountServer administrator on the Installation checklist (page 124).

23. On the third Set Up Users and Passwords screen, enter the password for the CountServer administrator account and press **Enter**.

    All passwords should meet the guidelines provided in "Login credential rules and guidelines" on page 121. Passwords are *case-sensitive*.

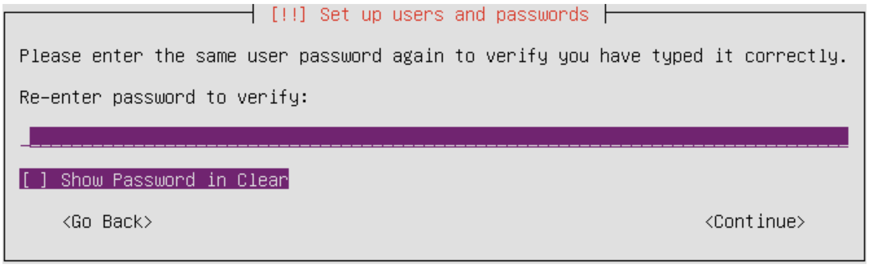


```
[!!] Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be
changed at regular intervals.

Choose a password for the new user:

________________________________________________________________________________________

[ ] Show Password in Clear

    <Go Back>                                                               <Continue>
```

Figure 3-15. Third Set Up Users and Passwords screen

    Before using the Show Password in Clear option, be aware of your surroundings and ensure that no one will see the password as you type.

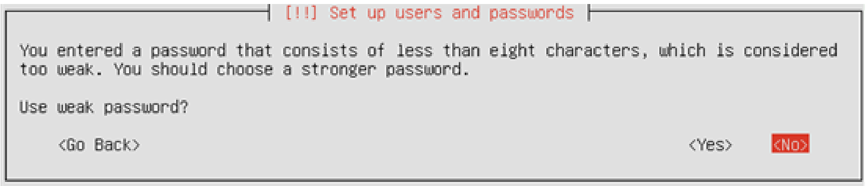
24. On the fourth Set Up Users and Passwords screen, reenter the password for the CountServer administrator account and press **Enter**.



```
[!!] Set up users and passwords

Please enter the same user password again to verify you have typed it correctly.

Re-enter password to verify:

_______________________________________________________________________________

[ ] Show Password in Clear

    <Go Back>                                                          <Continue>
```

Figure 3-16. Fourth Set Up Users and Passwords screen

25. (If applicable) If the following screen appears, press Tab to advance to **<No>**, press **Enter**, select **Set up users and passwords** from the menu of installation steps, and reenter all account settings for the Linux administrator.



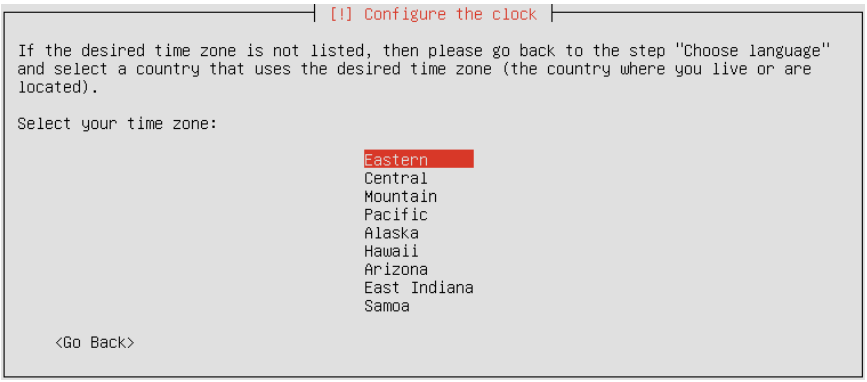
```
[!!] Set up users and passwords

You entered a password that consists of less than eight characters, which is considered
too weak. You should choose a stronger password.

Use weak password?
```

Figure 3-17. Fifth Set up Users and Passwords screen

The installation program skips this screen if password length is at least eight characters.

26. (Recommended) Record the password of the CountServer administrator on the Installation checklist (page 124).

27. On the Configure the Clock screen as shown in Figure 3-18 on page 29, select your time zone and then press **Enter**.



```
[!] Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language"
and select a country that uses the desired time zone (the country where you live or are
located).

Select your time zone:
```

Figure 3-18. Configure the Clock screen

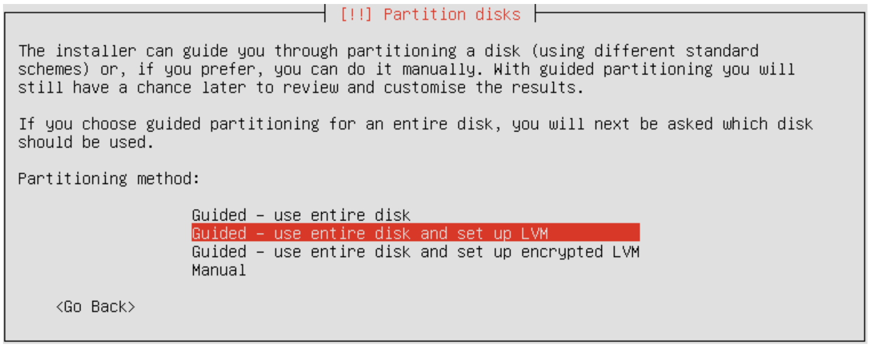
Optional RAID configuration

You can create a RAID 1 or a RAID 5 virtual volume.

- If you have a minimum of two hard disks, you can configure the CountServer computer as a RAID 1 virtual volume. Skip steps 28 through 32 and follow the procedure described in "Creating a RAID 1 virtual volume" on page 35. You will return to step 33.
- If you have three or four hard disks, you can configure the CountServer computer as a RAID 5 volume. Skip steps 28 through 32 and follow the procedure described in "Creating a RAID 5 virtual volume" on page 38. You will return to step 33.
- Do not create a RAID virtual volume if you have already configured a hardware RAID controller as described in "RAID configurations" on page 16. Continue with step 28.

28. On the first Partition Disks screen as shown in Figure 3-19 on page 30, accept the default, **Guided – use entire disk and set up LVM**, and press **Enter**. (*LVM* is *logical volume manager*, a flexible method of disk space allocation.)

The installation procedure overwrites the CountServer computer's existing operating system with the Ubuntu Linux operating system. All data on the computer becomes irretrievable at this point, even if you return to prior steps (using the Go Back option). You must ensure that any election data you want to retain is backed up. See "Backing up an election" in the ClearCount *Election Administration Guide*. If you have any doubts about continuing, exit the installation program.

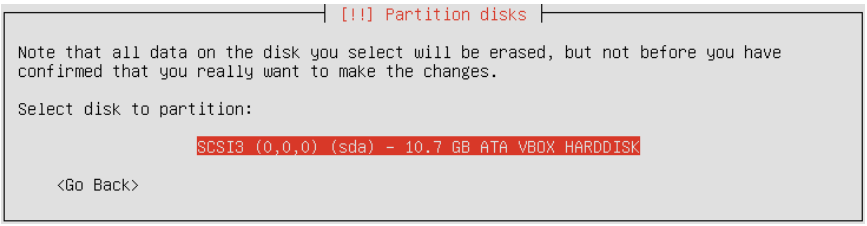


```
[!!] Partition disks

The installer can guide you through partitioning a disk (using different standard
schemes) or, if you prefer, you can do it manually. With guided partitioning you will
still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk
should be used.

Partitioning method:

                    Guided - use entire disk
                    Guided - use entire disk and set up LVM
                    Guided - use entire disk and set up encrypted LVM
                    Manual

    <Go Back>
```

Figure 3-19. First Partition Disks screen

29. On the second Partition Disks screen, select the disk to partition and press **Enter**.

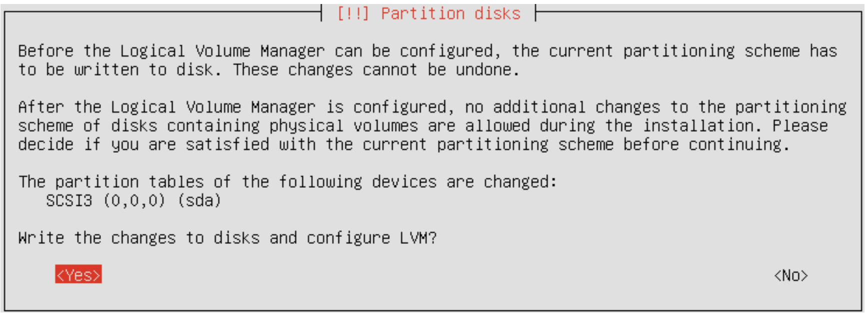
    The primary internal hard drive is selected by default. If the hardware configuration includes more than one drive, do *not* select an external drive.



```
[!!] Partition disks

Note that all data on the disk you select will be erased, but not before you have
confirmed that you really want to make the changes.

Select disk to partition:

                    SCSI3 (0,0,0) (sda) - 10.7 GB ATA VBOX HARDDISK

    <Go Back>
```

Figure 3-20. Second Partition Disks screen

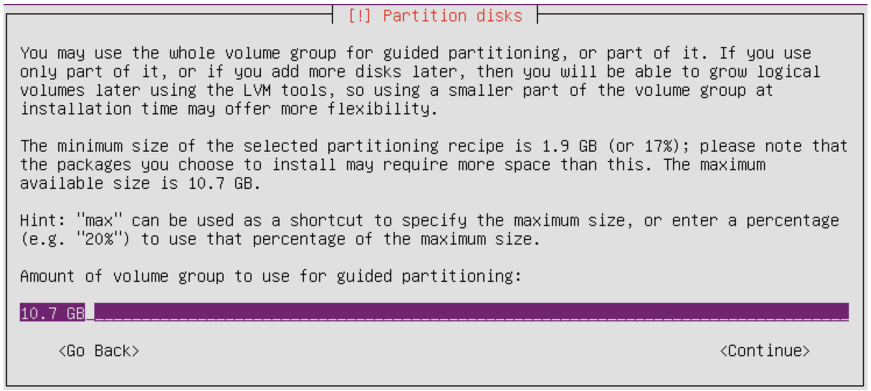
30. On the third Partition Disks screen, press Tab to select **Yes** and then press **Enter**.



```
[!!] Partition disks

Before the Logical Volume Manager can be configured, the current partitioning scheme has
to be written to disk. These changes cannot be undone.

After the Logical Volume Manager is configured, no additional changes to the partitioning
scheme of disks containing physical volumes are allowed during the installation. Please
decide if you are satisfied with the current partitioning scheme before continuing.

The partition tables of the following devices are changed:
   SCSI3 (0,0,0) (sda)

Write the changes to disks and configure LVM?

    <Yes>                                                                   <No>
```

Figure 3-21. Third Partition Disks screen

31. On the fourth Partition Disks screen as shown in Figure 3-22 on page 31, accept the default amount of the volume group for the primary partition by pressing **Enter**.

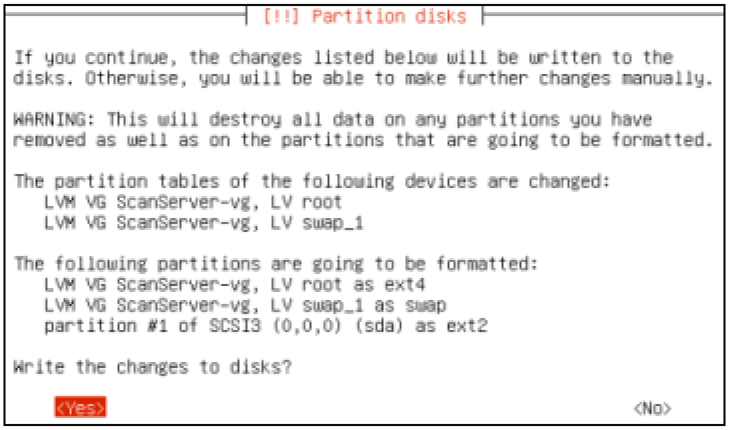


```
[!] Partition disks

You may use the whole volume group for guided partitioning, or part of it. If you use
only part of it, or if you add more disks later, then you will be able to grow logical
volumes later using the LVM tools, so using a smaller part of the volume group at
installation time may offer more flexibility.

The minimum size of the selected partitioning recipe is 1.9 GB (or 17%); please note that
the packages you choose to install may require more space than this. The maximum
available size is 10.7 GB.

Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage
(e.g. "20%") to use that percentage of the maximum size.

Amount of volume group to use for guided partitioning:

10.7 GB

    <Go Back>                                                              <Continue>
```

Figure 3-22. Fourth Partition Disks screen

32. (If applicable) During an upgrade, the following screen appears. Use the Tab key to select **Yes** to confirm the disk changes, and then press **Enter**.

    This overwrites any existing data.



```
[!!] Partition disks

If you continue, the changes listed below will be written to the
disks. Otherwise, you will be able to make further changes manually.

WARNING: This will destroy all data on any partitions you have
removed as well as on the partitions that are going to be formatted.

The partition tables of the following devices are changed:
   LVM VG ScanServer-vg, LV root
   LVM VG ScanServer-vg, LV swap_1

The following partitions are going to be formatted:
   LVM VG ScanServer-vg, LV root as ext4
   LVM VG ScanServer-vg, LV swap_1 as swap
   partition #1 of SCSI3 (0,0,0) (sda) as ext2

Write the changes to disks?

     <Yes>                                                    <No>
```

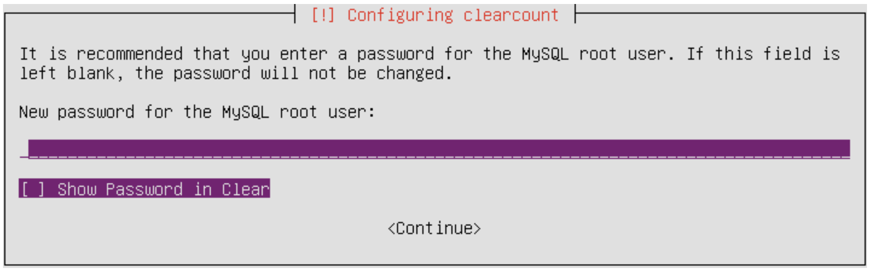
Figure 3-23. Fifth Partition Disks screen

The system installs files, which may take several minutes.

33. On the first Configuring ClearCount screen, enter a password for the MySQL database root user and press Enter.

    Ensure the password is accurate as you are not asked to confirm it. All passwords must satisfy the rules, and should meet the guidelines, provided in "Login credential rules and guidelines" on page 121.

    ClearCount records all logins for this account. Log in and use this account only if instructed to do so by Clear Ballot Technical Support. It is *not* for normal electoral duties.



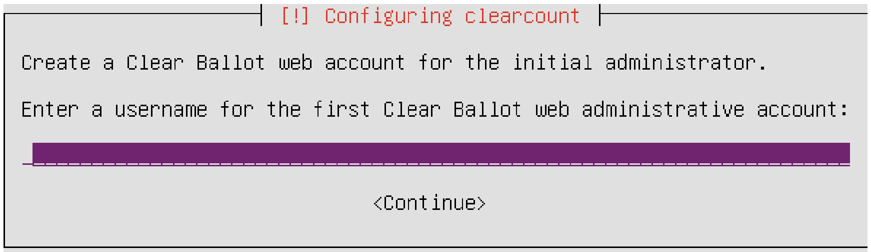
```
[!] Configuring clearcount

It is recommended that you enter a password for the MySQL root user. If this field is
left blank, the password will not be changed.

New password for the MySQL root user:

_______________________________________________________________________________________

[ ] Show Password in Clear

                                   <Continue>
```

Figure 3-24. First Configuring ClearCount screen

34. (Recommended) Record the database root user password on the Installation checklist (page 124).

35. On the second Configuring ClearCount screen, enter the user name for the ClearCount primary administrator account and press Enter.

    This is the account that manages users and elections via a CountStation computer. The ClearCount system records all logins for this account. Clear Ballot recommends using an easily distinguishable name, such as the actual name of the user, to facilitate tracking the user.



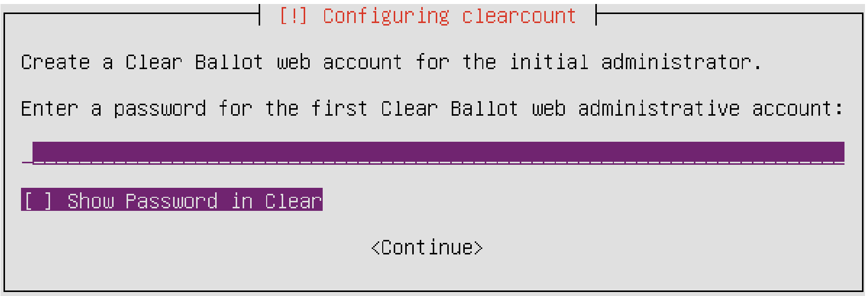
```
[!] Configuring clearcount

Create a Clear Ballot web account for the initial administrator.

Enter a username for the first Clear Ballot web administrative account:

_____________________________________________________________________

                              <Continue>
```

Figure 3-25. Second Configuring ClearCount screen

36. (Recommended) Record the user name for the ClearCount primary administrator account on the Installation checklist (page 124).

37. On the third Configuring ClearCount screen, enter the password for the ClearCount primary administrator account and press Enter.

    Ensure the password is accurate as you are not asked to confirm it. All passwords must satisfy the rules, and should meet the guidelines, provided in "Login credential rules and guidelines" on page 121.



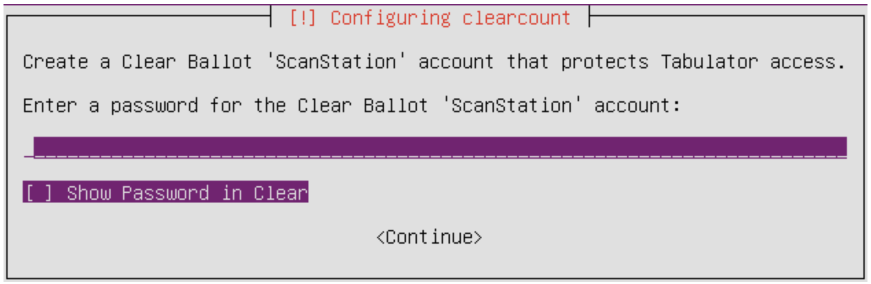
```
[!] Configuring clearcount

Create a Clear Ballot web account for the initial administrator.

Enter a password for the first Clear Ballot web administrative account:

_____________________________________________________________________

[ ] Show Password in Clear

                              <Continue>
```

Figure 3-26. Third Configuring ClearCount screen

38. (Recommended) Record the password for the ClearCount primary administrator account on the Installation checklist (page 124).

39. On the fourth Configuring ClearCount screen, enter the password for the ScanStation account. This account protects access to the Tabulator application. The scanning supervisor enters this password to start the Tabulator application on each ScanStation computer. All ScanStation computers use the same password. Press Enter.

    Ensure the password is accurate as you are not asked to confirm it. All passwords must satisfy the rules, and should meet the guidelines, provided in "Login credential rules and guidelines" on page 121.

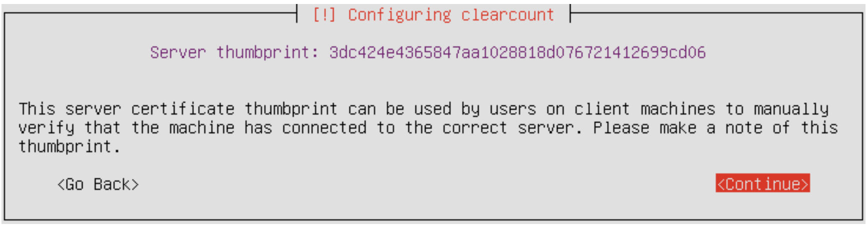


```
[!] Configuring clearcount

Create a Clear Ballot 'ScanStation' account that protects Tabulator access.

Enter a password for the Clear Ballot 'ScanStation' account:
```

Figure 3-27. Fourth Configuring ClearCount screen

40. (Recommended) Record the password for the ScanStation account on the Installation checklist (page 124).

    The system spends several minutes installing software and then presents a screen with the server thumbprint, which is a long string of characters used to verify server traffic.



```
[!] Configuring clearcount

Server thumbprint: 3dc424e4365847aa1028818d076721412699cd06

This server certificate thumbprint can be used by users on client machines to manually
verify that the machine has connected to the correct server. Please make a note of this
thumbprint.
```

Figure 3-28. Server Thumbprint screen

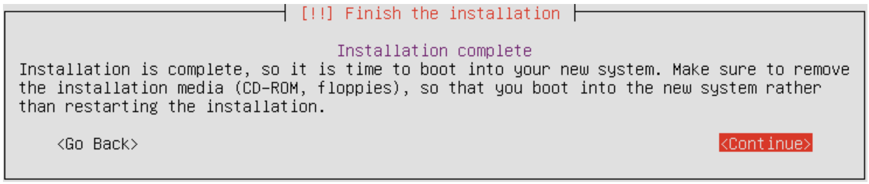
41. (Recommended) Record the server thumbprint on the Installation checklist (page 124).

42. Note the server thumbprint or take a picture of it, and then click **Continue**.

43. Wait for up to 30 minutes as software is installed.

    Do *not* unplug, close, or shut down the computer while you are waiting. Also do *not* remove the ClearCount CountServer DVD.

    Upon completion, the screen shown in Figure 3-29 on page 34 appears:

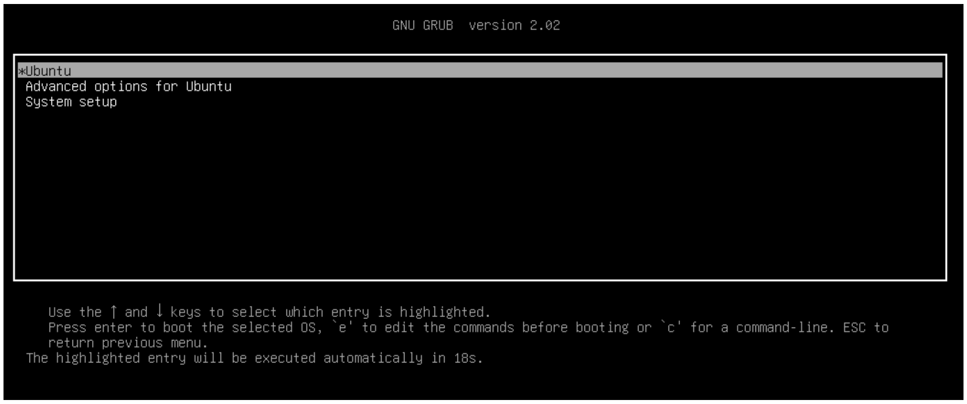


```
                     ┤ [!!] Finish the installation ├

                         Installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove
the installation media (CD-ROM, floppies), so that you boot into the new system rather
than restarting the installation.

    <Go Back>                                                        <Continue>
```

Figure 3-29. Finish the Installation screen

44. Click **Continue**.

45. When the screen shown in Figure 3-30 appears, remove and secure the ClearCount CountServer DVD.



```
                                 GNU GRUB  version 2.02

*Ubuntu
 Advanced options for Ubuntu
 System setup





    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line. ESC to
    return previous menu.
 The highlighted entry will be executed automatically in 18s.
```

Figure 3-30. Screen that appears when ready to remove the DVD

46. Select **Ubuntu** to proceed with the restart.

    The Ubuntu Login screen appears on restart, indicating that the CountServer computer is running and available. Do *not* log in.

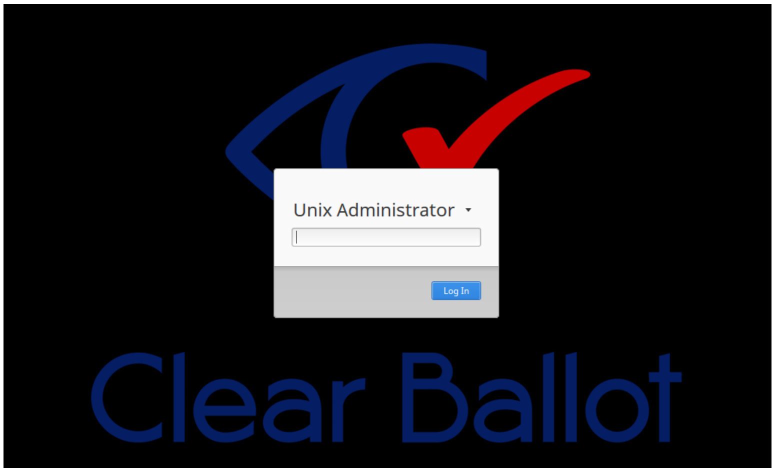


Figure 3-31. Ubuntu Login screen

> **Important**: Do *not* log in as the administrator at this time. If an issue occurs log in as the administrator, only under the direction of Clear Ballot Technical Support.

3.2.1 Creating a RAID 1 virtual volume

Combining the physical disk drives into a single logical hard disk improves performance and allows for data redundancy.

Both hard disks must be the same size to be configured as a RAID volume.

The following steps provide an example of how to configure two hard drives as a RAID 1 virtual volume when installing the ClearCount software. Consult the computer manufacturer's documentation for more information.

Begin "Installing ClearCount software" on page 21 . Then use the steps below instead of steps 28 through 32. You will return to step 33.

A. Ignore the existing RAID configuration

If the existing hard disks already have RAID configured (perhaps by the manufacturer), you may see the following prompt: "One or more drives containing RAID configurations have been found. Do you wish to activate these RAID devices?"

Answer **No**. You want to remove the existing RAID configuration, not activate it.

B. Select manual mode for partitioning disks

When the Partition Disks screen appears, select **Manual**.

C. Check for existing LVM partitions and delete them

If you see LVM next to the partitions of your hard drives, delete the existing LVM setups as follows:

1. Select **Configure the Logical Volume Manager**.
2. If prompted, allow the system to write any changes to disk.
3. Select **Delete logical volume** for any existing volumes.
4. Select **Delete volume group** for any existing volume groups.
5. Select any LVM partitions that are shown and select **Delete the Partition**.
6. Click **Finish**.

D. Create partition tables

If you see hard disks without a partition indented beneath them, create a partition table for each hard disk as follows:

1. Select the hard disk and press the Enter key to create the partition table.
2. At the Create new empty partition table on this device? prompt, select **Yes**. After the system creates the partition table, you see a partition table labeled FREE SPACE below the name of the hard disk.

When you are done, there are two hard disks listed (sda, sdb) with the label FREE SPACE beneath each.

E. Create partitions from all free space

Follow these steps for *each* hard disk:

1. Select each FREE SPACE below the hard disk and press Enter.
2. Select **Automatically partition the free space**.

When done, there are five partitions listed below each hard disk similar to the following.

The size allocated depends upon your particular hard drive.

Table 3-1. Partitions

Partition No.	Label	Size	Description
1	No label	1 MB	Required by the system. Do not touch this partition.
2	#1	1 MB	The boot partition.
3	#2	6 TB	The primary data and OS partition.
4	#3	17.1 GB	The swap area.
5	No label	597.5 K	Unused free space. Do not touch this partition.

F. Set up all partitions for use in RAID arrays

For *each* partition, perform the following:

1. For *each* drive (sda and sdb):
    a. Select the partition labeled *#1 partition* and press Enter.
    b. Select **Use as** and press Enter.
    c. Select **Reserved BIOS Boot Area** and press Enter.
    d. Select **Done setting up the partition** and press Enter.

2. For *each* drive (sda and sdb):
    a. Select the partition labeled *#2* and press Enter.
    b. Select **Use as** and press Enter.
    c. Select **Physical volume for RAID** and press Enter.
    d. Select **Done setting up the partition** and press Enter.
3. For *each* drive (sda and sdb):
    a. Select the partition labeled *#3* and press Enter.
    b. Select **Use as** and press Enter.
    c. Select **Physical volume for RAID** and press Enter.
    d. Select **Done setting up the partition** and press Enter.

G. Create the RAID array for the main partition

You create RAID arrays for the main data and swap partitions, but not the biosgrub partition.

1. Select **Configure software RAID** and click **Yes** to allow the software to write all changes to disk, if requested.
2. Select **Create MD device**. (*MD device* is a synonym for *RAID array*.)
3. Select the type of RAID array as **RAID1**. The system prompts for the number of active hard drives vs. spare hard drives.
4. Unless otherwise instructed, select **Active** for all hard drives. Make all hard drives active by accepting the default number of active devices and then select **Continue**.
5. Select **0** as the number of spare devices and select **Continue**.
6. Select the two largest devices and press Enter. You return to the Create MD Device screen.
7. To create the RAID array for the swap devices:
    a. Repeat steps 2 through 4.
    b. Select the two largest devices and press Enter. You return to the Create MD Device screen.
    c. Select **Finish** and press Enter. You return to the Partition Disks screen.

H. Designate the RAID array for the main partition

Follow these steps:

1. Under the 6 TB RAID device, select the first indented line and press Enter.
2. Select the **Use as** menu item.

3. Select **Ext4**.
4. Select **Mount point**.
5. Select **/ - the root file system** and press Enter.
6. Select **Done setting up the partition** and press Enter.

I. Designate the RAID array for the swap area

Follow these steps:

1. Select the first indented line under RAID device #1 and press Enter.
2. Select the **Use as** menu item and press Enter.
3. Select **Swap area** and press Enter.
4. Select **Done setting up the partition** and press Enter.

J. Complete the RAID configuration

Follow these steps:

1. Scroll down and select **Finish partitioning and write changes to disk.** You may see a warning about how the system behaves when the RAID array suffers a failure.
2. At the Do you want to boot your system if your RAID becomes degraded? prompt, select **Yes**.
3. At the Write changes to disk? prompt, select **Yes**.

The ClearCount installation process resumes at step 33. Follow the remaining steps.

3.2.2 Creating a RAID 5 virtual volume

Combining the physical disk drives into a single logical hard disk improves performance and allows for data redundancy.

All three hard disks must be the same size to be configured as a RAID volume.

The following steps describe how to configure a Dell PowerEdge T440 with three 6 TB hard drives as a RAID 5 virtual volume when installing the ClearCount software. Consult the computer's manufacturer's documentation when configuring other servers.

Begin the standard installation process beginning on page 21 and then use the steps below instead of steps 28 through 32. You will return to step 33.

A. Ignore the existing RAID configuration

If the existing hard disks already have RAID configured (perhaps by the manufacturer), you may see the following prompt: "One or more drives containing RAID configurations have been found. Do you wish to activate these RAID devices?"

Answer **No**. You want to remove the existing RAID configuration, not activate it.

B. Select manual mode for partitioning disks

When the Partition Disks screen appears, select **Manual**.

C. Check for existing LVM partitions and delete them

If you see LVM next to the partitions of your hard drives, delete the existing LVM setups as follows:

1. Select **Configure the Logical Volume Manager**.
2. If prompted, allow the system to write any changes to disk.
3. Select **Delete logical volume** for any existing volumes.
4. Select **Delete volume group** for any existing volume groups.
5. Select any LVM partitions that are shown and select **Delete the Partition**.
6. Click **Finish**.

D. Create partition tables

If you see hard disks without a partition indented beneath them, create a partition table for each hard disk as follows:

1. Select the hard disk and press the Enter key to create the partition table.
2. At the Create new empty partition table on this device? prompt, select **Yes**. After the system creates the partition table, you see a partition table labeled FREE SPACE below the name of the hard disk.

When you are done, there are three hard disks listed (sda, sdb, sdc) with the label FREE SPACE beneath each.

E. Create partitions from all free space

Follow these steps for *each* hard disk:

1. Select each FREE SPACE below the hard disk and press Enter.
2. Select **Automatically partition the free space**.

When done, there are five partitions listed below each hard disk similar to the following.

The size allocated depends upon your particular hard drive.

Table 3-2. Partitions

Partition No.	Label	Size	Description
1	No label	1 MB	Required by the system. Do not touch this partition.

Table 3-2. Partitions (continued)

Partition No.	Label	Size	Description
2	#1	1 MB	The boot partition.
3	#2	6 TB	The primary data and OS partition.
4	#3	17.1 GB	The swap area.
5	No label	597.5 K	Unused free space. Do not touch this partition.

F. Set up all partitions for use in RAID arrays

For *each* partition do the following:

1. For *each* drive (sda, sdb and sdc):
   a. Select the partition labeled *#1 partition* and press Enter.
   b. Select **Use as** and press Enter.
   c. Select **Reserved BIOS Boot Area** and press Enter.
   d. Select **Done setting up the partition** and press Enter.
2. For *each* drive (sda, sdb and sdc):
   a. Select the partition labeled *#2* and press Enter.
   b. Select **Physical volume for RAID** and press Enter.
   c. Select **Done setting up the partition** and press Enter.
3. For *each* drive (sda, sdb and sdc):
   a. Select the partition labeled *#3* and press Enter.
   b. Select **Physical volume for RAID** and press Enter.
   c. Select **Done setting up the partition** and press Enter.

G. Create the RAID array for the main partition

You create RAID arrays for the 6 TB main data and 17.1 GB swap partitions, but not the biosgrub partition.

1. Select **Configure software RAID** and allow the software to write all changes to disk, if requested.
2. Select **Create MD device**. (*MD device* is a synonym for *RAID array*.)
3. Select the type of RAID array as **RAID5**. The system prompts for the number of active hard drives vs. spare hard drives.

4. Unless otherwise instructed, select **Active** for all hard drives. Make all hard drives active by accepting the default number of active devices (3) and then select **Continue**.
5. Select **0** as the number of spare devices and select **Continue**.
6. Select the three 6 TB devices and press Enter. You return to the Create MD Device screen.
7. To create the RAID array for the 17.1 GB devices:
    a. Repeat steps 2 through 4.
    b. Select the three 17.1 GB devices and press Enter. You return to the Create MD Device screen.
    c. Select **Finish** and press Enter. You return to the Partition Disks screen.

H. Designate the RAID array for the main partition

Follow these steps:

1. Under the 6 TB RAID device, select the first indented line and press ENTER.
2. Select the **Use as** menu item.
3. Select **Ext4**.
4. Select **Mount point**.
5. Select **/ - the root file system** and press Enter.
6. Select **Done setting up the partition** and press Enter.

I. Designate the RAID array for the swap area

Follow these steps:

1. Select the first indented line under RAID device #1 and press Enter.
2. Select the **Use as** menu item and press Enter.
3. Select **Swap area** and press Enter.
4. Select **Done setting up the partition** and press Enter.

J. Complete the RAID configuration

Follow these steps:

1. Scroll down and select **Finish partitioning and write changes to disk.** You may see a warning about how the system behaves when the RAID array suffers a failure.
2. At the Do you want to boot your system if your RAID becomes degraded? prompt, select **Yes**.
3. At the Write changes to disk? prompt, select **Yes**.

The ClearCount installation process resumes at step 33. Follow the remaining steps.

3.3 Restricting access to the BIOS on the CountServer

Access to the BIOS is restricted by implementing a supervisor password. The behavior of the BIOS depends upon the computer make and model. Consult your computer’s documentation or contact Clear Ballot Technical Support for details.

The following procedure for a Dell PowerEdge T140 computer is an example. Consult the computer's manufacturer's documentation when configuring other servers.

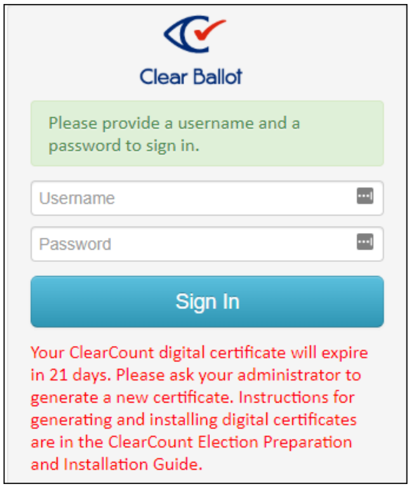
To restrict access to BIOS:

1. Press the Shift key while shutting down the computer. The CountServer computer shuts down.
2. Press the F1 key while starting up the computer. The BIOS manager appears.
3. Set the BIOS password:
   All user names and passwords must satisfy the rules and guidelines provided in "Login credential rules and guidelines" on page 121.
   a. Using the arrow keys, navigate to the Security screen and select **Administrator Password**.
   b. Enter and confirm the password.
   c. Record the BIOS password on the Installation checklist (page 124).
4. To save your changes, click **Apply** and then click **Exit**.
5. Turn the computer off and back on.
6. Verify the changes.

3.4 Regenerating a digital certificate

ClearCount uses digital certificates to encrypt and protect your data. The digital certificate can be valid for at most 825 days. When installing the CountServer, a default value of 365 days is used.

When the certificate is within 60 days of expiration, ClearCount begins displaying a message on the sign in screen that prompts you to ask the administrator to generate a new certificate (Figure 3-32).



Please provide a username and a password to sign in.

Your ClearCount digital certificate will expire in 21 days. Please ask your administrator to generate a new certificate. Instructions for generating and installing digital certificates are in the ClearCount Election Preparation and Installation Guide.

Figure 3-32. Message indicating the expiration of the digital certificate

To regenerate a certificate:

1. Log in to the CountServer with the administrator user name and password.
2. Enter:

   ```
   sudo bash /usr/share/cbg/web/scripts/generate_certificate.sh
   ```

   The CountServer displays the following message:

   ```
   Enter days until expiration, max 825. (365):
   ```

3. Do one of the following at the message "Enter days until expiration, max 825. (365):":
   a. Enter a new value at the end of the message.

      or

   b. Press **Enter** to accept the default value.

3.5 Hardening the CountServer computer

The CountServer 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 CountServer computer (other than during a support call with Clear Ballot or for the purpose of recreating the digital certificate). All normal pre-election, election, and postelection access to the CountServer computer is by remote connection from the ScanStation computers or CountStation 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, reinstall the software, or recreate the digital certificate. (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.

Note: Clear Ballot recommends that you record all logins to the CountServer computer by using the Access Log for the CountServer located in the *ClearCount Election Administration Guide*. If any unexpected logins to the CountServer 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 CountServer computer, see "Restricting access to the BIOS on the CountServer" on page 42.

3.6 Updating the ClearCount software

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 or certified by the state election governance office of the jurisdiction.

Note: Installing the ClearCount software erases any election databases currently residing on the CountServer computer. 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 network switch's IP address.
- Print the "Installation checklist" on page 124.
- Install the updated software following the process described in "Installing the CountServer" on page 20.

Chapter 4. Configuring ScanStations

After installing the ClearCount software on the CountServer, install software on all ScanStations and configure them. Follow the sections of this chapter in order on each ScanStation.

Note: To maintain ScanStation security, only election officials with the appropriate access level should know the passwords for the Microsoft Windows computers and the ScanStation account. Do not give the passwords to the scanner operators.

Likewise, do not give scanner operators access to the DeleteBox utility. If scanner operators must restart a process or correct an error, they must consult with the scanning supervisor, who enters the passwords.

After following the sections of this chapter, implement the hardening steps for all ScanStations before using them. See "Hardening the ScanStation computers" on page 78.

4.1   Updating the BIOS version on the Dell 5521

Before you install Windows on a Dell 5521 computer, follow this procedure to ensure the BIOS version is version 1.5.3 or greater:

1. If you are installing from the DVD drive, skip step 1 and continue with step 2.

   If you are using a USB drive, copy the downloaded BIOS file to a USB drive.

   The USB drive does not need to be a bootable device.

2. Insert the USB or DVD drive containing the installation files into any USB port on the Dell 5521 computer.

3. Turn on the computer.

4. At the Dell logo screen, press **F12** to access the one-time boot menu.

5. In the Other Options section, select **BIOS Flash Update**.

6. Browse to the location of the BIOS file. select it, and click **OK**.

7. Verify the existing system BIOS information and the BIOS update information.

8. If the BIOS version is less than version 1.5.3, click **Begin Flash Update**.

9. Review the Warning message and click **Yes** to proceed with the update.

   The computer restarts and displays a progress bar at the Dell logo screen. The computer restarts again when the update is complete.

10. Go back to the BIOS Boot Menu and check that the BIOS version is correct in the top right hand corner.

4.2 Installing the Windows 10 Pro operating system

To install Windows 10 Pro:

1. Turn off the computer and insert the Microsoft Windows 10 Pro DVD into the drive.
2. If you are using a Dell Latitude 5500 or 5511 model, turn on the computer and repeatedly press **F12** until the message "Preparing one-time boot menu" appears at the top right on the screen.

   The One-Time Boot menu appears.
3. If you are using a Dell Latitude 5500 or 5511 model, ensure that SATA Operation is set to **AHCI:**
   a. Under **Other Options**, select **BIOS Setup**.
   b. Expand **System Configuration** and select **SATA Operation**.
   c. If AHCI is not selected, select it and click **Yes** in the confirmation dialog.
   d. Click **Apply** and **OK** in the Apply Settings Confirmation dialog.
   e. Click **Exit**.
4. If you are usig a Dell Latitude 5521 model, do the following:
   a. Press **F2** at boot to enter the BIOS setup menu.
   b. In the left pane, select **Storage**.
   c. In the right pane at the top, **AHCI/NVMe**.
   d. In the left pane, select **Security**.
   e. Scroll all the way to the bottom of the right pane to the last section entitled "UEFI Boot Security" and select **Always**.
   f. Click **Apply Changes**.
5. When the computer restarts, repeatedly press **F12** until the message "Preparing one-time boot menu" appears at the top right of the screen.

   The One-Time Boot menu appears.
6. For the Latitude 5500 and 5511, access the One-Time Boot menu and do the following:
   a. Confirm that the Boot menu is set to **UEFI: Secure Boot: ON**.
   b. Select the disk/DVD mode option from the UEFI BOOT section.

      To find the disk, locate the line item that contains the characters "DVD."

7. For the Latitude 5521, press **F2** at boot to enter the BIOS setup menu and then do the following:

   a. In the left pane, select **Security**.

   b. Scroll all the way to the bottom of the right pane to the last section entitled "UEFI Boot Security and select **Always**.

8. To check the Secure Boot setting:

   a. Click the Start button on the Windows taskbar and search for and select **Powershell**.

   b. At the prompt in the Windows Powershell, enter:

      ```
      Confirm-SecureBootUEFI
      ```

      The PowerShell returns the value `True` if SecureBoot is correctly configured.

9. Reboot the computer.

10. When the computer restarts, repeatedly press **F12** until the message "Preparing one-time boot menu" appears at the top right of the screen.

    When the One-Time Boot menu appears, do the following:

    a. Select the disk/DVD mode option from the UEFI Boot section.

    b. To find the disk, locate the line item that contains the characters "DVD."

11. Select the disk/DVD mode option from the UEFI Boot section.

12. To find the disk, locate the line item that contains the characters "DVD."

13. Press **Enter** on the DVD line item.

    The installation begins.

14. If message "Press any key to boot from CD or DVD ..." appears, press any key on your keyboard.

15. When the Windows Setup dialog appears, select the desired language and click **Next**.

16. In the next dialog, click **Install Now**.

17. When the license terms appear, select the checkbox and click **Next**.

18. In the next dialog, select the **Custom: Install Windows only (advanced)** option.

19. When asked where you want to install Windows, do the following:

    a. Remove any existing partitions. Select the first partition and click the **Delete** icon. A message appears. Click **OK**.

   b. Remove each partition until a single drive named *Drive 0 Unallocated Space* remains.

   c. Click **Next**.

   The installation beings and takes about 10 minutes. Then the computer restarts.

20. At the Get going fast dialog, click **Customize**.

    The Customize settings dialog appears.

21. In the Personalization settings, click each option to turn it off and click **Next**.

22. In the Location settings, turn it off and click **Next**.

23. In the Connectivity and error reporting settings, click each option to turn it off and click **Next**.

24. In the Browsers, protection, and update settings, click each option to turn it off and click **Next**.

25. When the Create an account for this PC dialog appears, enter the user name and password for the Windows administrator and click **Next**.

26. (Recommended) Record the Windows administrator user name and password on the Installation Checklist.

27. In the Meet Cortana dialog, click **Not now** and then click **Next**.

    Windows finishes its setup.

28. Remove the Microsoft Windows 10 Pro DVD and insert the Windows Updates DVD.

29. Navigate to the Windows Tools folder, open the Windows Activation Key.txt file, and copy the text.

30. On the Windows taskbar, in the Ask me anything field, type *Settings*, and press Enter.

31. At the bottom of the Windows Settings window, click the **Activate Windows now** option and then click **Change product key**.

32. When asked if you want the app to make changes, click **Yes**.

33. Paste the activation key text string in the **Product Key** field.

34. On the resulting Activation dialog, click **Next**.

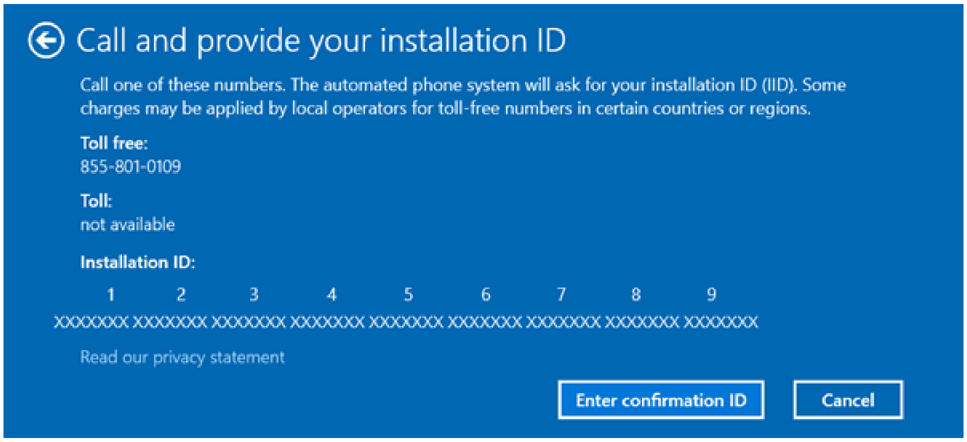
35. When the following dialog displays the message "We couldn't activate Windows," click **Close**.

36. Click the **Start** button on the Windows taskbar and search for and select **Run**.

37. In the Run dialog, type **slui.exe 4** in the **Open** field and click **OK**.

38. On the Select your country or region dialog, select a country from the drop-down list and click **Next**.

    A dialog appears that provides a toll-free telephone number to call for activation (Figure 4-1).



Call and provide your installation ID

Call one of these numbers. The automated phone system will ask for your installation ID (IID). Some charges may be applied by local operators for toll-free numbers in certain countries or regions.

Toll free:
855-801-0109

Toll:
not available

Installation ID:

1	2	3	4	5	6	7	8	9
XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX	XXXXXXX

Read our privacy statement

Figure 4-1. Call and provide your installation ID

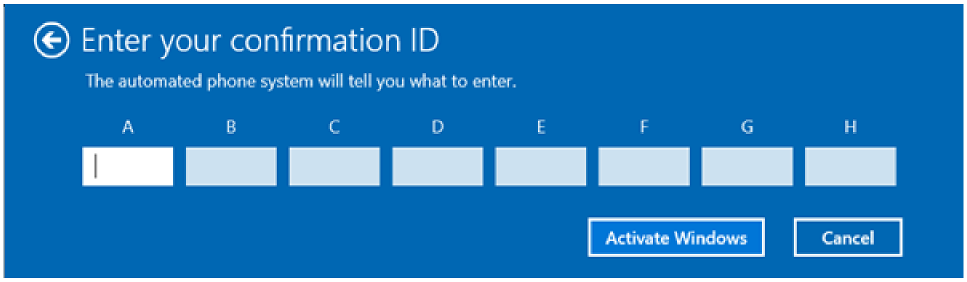
39. Call the activation service and follow the automated prompts.

    Make sure to state that this is not a new installation. Answering in this way sends you to the automated version of the service instead of sending you to a customer-service person.

    When prompted, provide the nine-part installation ID that appears on the dialog to get the Confirmation ID.

    If for any reason you cannot complete the activation using this fully automated service, call the number again and state that this is a new installation. A customer-service person will then help you activate the installation.

40. Click the **Enter confirmation ID** button on the dialog, enter the eight-part confirmation number that the automated activation service provides, and click **Activate Windows** (Figure 4-2).



Enter your confirmation ID

The automated phone system will tell you what to enter.

Figure 4-2. Enter your confirmation ID

41. When a confirmation message indicates that Windows has been activated, click **Close**.

42. To check that the BIOS settings are correct after the installation of Windows is complete, do the following:
    a. Open the Device Manager and select **IDE-ATA/ATAPI controllers**.
    b. Check that the device description contains "AHCI."

       Example: Standard SATA AHCI Controller

4.3 Installing the Windows patch

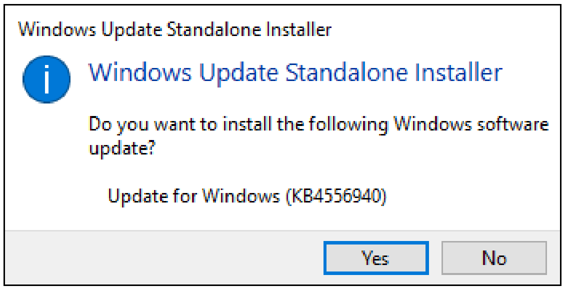
This topic describes how to patch Windows for some security updates. The patch process requires you to install two files: a service stack update and a Windows update.

Installing the service stack update

To install the service stack update:

1. Insert the Windows Updates disk and navigate to the Windows Patch directory in File Explorer.
2. Install the Service Stack Update, KB4556940, by double-clicking **Windows10.0-KB4556940-x64.msu**.

   The installation program displays the Windows Update Standalone Installer dialog (Figure 4-3).



Windows Update Standalone Installer

Windows Update Standalone Installer

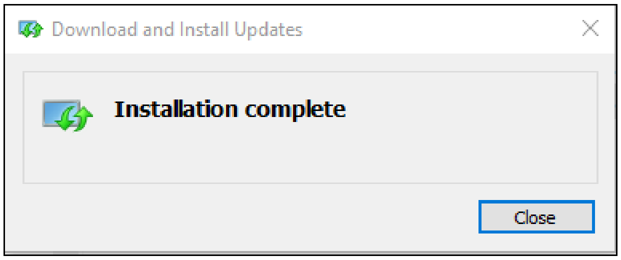
Do you want to install the following Windows software update?

Update for Windows (KB4556940)

Figure 4-3. Windows Update Standalone Installer dialog—Service stack update

3. Click **Yes** in the Windows Update Standalone Installer dialog (Figure 4-3).

   The update takes approximately a minute. When the service stack update is complete, the installation program displays the message shown in Figure 4-4.



Download and Install Updates

Installation complete

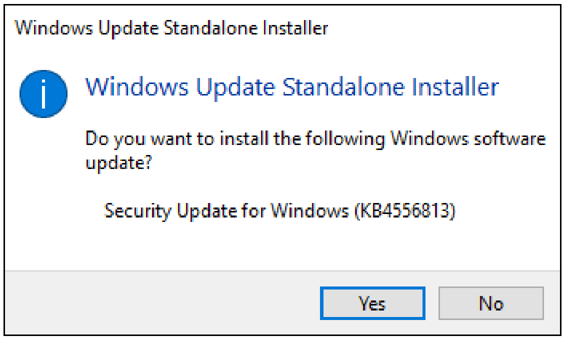
Figure 4-4. Installation Complete message—Service Stack Update

Installing the Windows updates

To install the Windows 10 KB4556813 update:

1. In the Windows Patch directory of the Windows update DVD, double-click the file named **windows10.0-kb4556813-x64_074956aa9f895643ea0768d516375d4a1cd732a2.msu**.

   The installation programs displays the Windows Update Standalone Installer dialog (Figure 4-5).

   Windows Update Standalone Installer

   Windows Update Standalone Installer

   Do you want to install the following Windows software update?

   Security Update for Windows (KB4556813)

   Figure 4-5. Windows Update Standalone Installer dialog—Windows security update

2. Click **Yes** to start the installation.

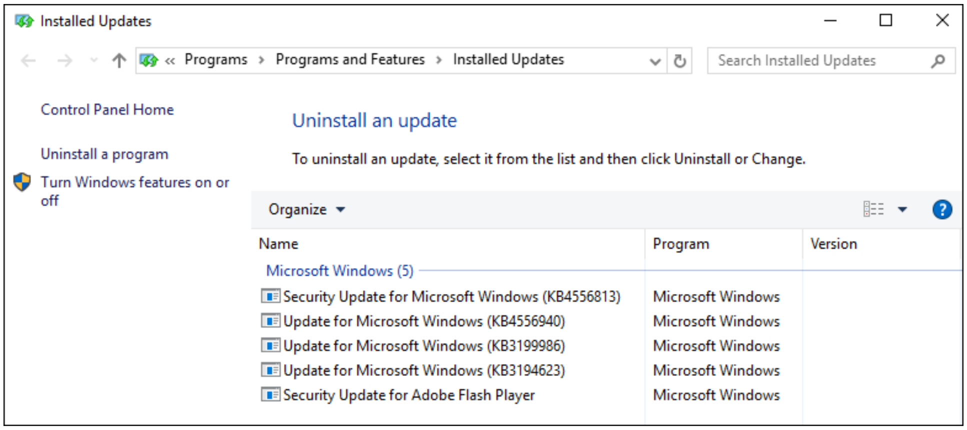
   After you click **Yes** to start the installation, Windows takes approximately 30 minutes to install the software. When prompted to do so, restart your computer.

   After you restart the computer, Windows takes approximately 30 minutes to process the updates.

3. Confirm that you have installed the updates:

   a. Click the **Start** button on the Windows taskbar and search for and select **View installed updates**.

   b. Confirm that KB4556940 and KB4556813 appear in the Installed Updates dialog (Figure 4-6).

   Installed Updates

   « Programs › Programs and Features › Installed Updates
   Search Installed Updates
   Control Panel Home
   Uninstall a program
   Turn Windows features on or off
   Organize ▾

   Uninstall an update

   To uninstall an update, select it from the list and then click Uninstall or Change.

Name	Program	Version
Microsoft Windows (5)		
Security Update for Microsoft Windows (KB4556813)	Microsoft Windows	
Update for Microsoft Windows (KB4556940)	Microsoft Windows	
Update for Microsoft Windows (KB3199986)	Microsoft Windows	
Update for Microsoft Windows (KB3194623)	Microsoft Windows	
Security Update for Adobe Flash Player	Microsoft Windows	

   Figure 4-6. Installed Updates dialog

4.4 Installing Windows drivers

Install the following Windows drivers:

- BIOS drivers
- Chipset drivers
- Graphics drivers
- Network drivers

Note: After you install all drivers, restart the computer.

To install the drivers:

1. Log in to the computer as the Windows administrator.
2. Insert the Windows Drivers DVD into the disc drive and navigate to the folder applicable to your computer model.
3. If there is a BIOS drivers folder for your computer, open it, double-click each application file, and follow the on-screen prompts to install each driver in the folder.

   After installing the BIOS drivers, restart the computer.
4. If there is a Chipset drivers folder for your computer, open it, double-click each application file, and follow the on-screen prompts to install each driver in the folder.

   If the Intel Rapid Storage Technology driver is being installed, click to accept the license agreement and click **Next**.

   IMPORTANT: On the following screen, select the option **Stay in AHCI mode** and click **Next**

   Click **Next** on Important Note.

   On the Include Intel Optane Memory and Storage Management screen, make sure to clear the checkbox **Include Intel Optane Memory and Storage Management** and click **Next**.
5. If there is a Graphics folder on your computer, double-click each application file and follow the on-screen prompts to install each driver in the folder.

   Depending on the model of your computer, you may not be able to install the AMD Graphics driver. In this situation, continue by installing the remaining drivers.

   Do not restart the computer after installing the graphics drivers.

6. If there is a Network drivers folder for your computer, open, double-click each application file, and follow the on-screen prompts to install each driver in the folder.

7. After you have installed all the drivers, restart the computer.

4.5 Displaying file extensions

After you restart the ScanStation computer, follow these steps to display file extensions:

1. Log in to Windows as an administrator.

2. Click the Start button on the Windows taskbar and search for and select **Show File Extensions**.

3. When Windows displays the File Options dialog, deselect the **Hide extension for known file types** checkbox.

4. Click **Apply** and then **OK**.

At this point, File Explorer displays the file extensions referenced in the remainder of this document.

4.6 Disabling BitLocker

When Windows is installed, BitLocker encrypts the drive. Because the mode of encryption does not meet Clear Ballot standards, you must decrypt the drive. After hardening the computer, which sets the encryption mode to FIPS 140-2, you may choose to re-enable BitLocker and encrypt the drive.

To disable BitLocker:

1. Click the Start button on the Windows taskbar, search for and select **Manage BitLocker**.

2. When Windows displays the BitLocker Drive Encryption window, click the option to **Turn on BitLocker** and accept any confirmation dialogs that appear.

3. When Windows displays the recovery key dialog, insert a USB drive into the computer and click **Save to a File**. Navigate to the desired location on the USB drive and click **Save**.

4. Follow the instructions to Activate BitLocker.

5. When BitLocker is activated, in the BitLocker Drive Encryption dialog, click **Turn off BitLocker**. Accept any confirmation dialogs that appear.

   The decryption process takes several minutes. When finished, the status **BitLocker Off** appears in the Bitlocker Drive Encryption dialog.

6. Navigate to the location on the USB drive where you saved the recovery key and delete it.

4.7 Installing the network switch

This topic describes how to set up the network switch.

4.7.1 Wired connections for ClearCount

All data communications in all ClearCount configurations take place over closed, wired Ethernet connections. ClearCount *never* connects to any of the following:

- Wi-Fi
- The Internet
- Any external networks

4.7.2 Overview: setting up the network switch

The topics that follow describe the recommended procedures for setting up the Cisco SG250 switch for ClearCount.

If your site uses a network switch other than the Cisco SG250, use the steps in this section as a guideline. The steps for setting up network switches other than the Cisco SG250 are similar with a few minor differences. If you have questions, contact Clear Ballot Technical Support.

Note: When setting up the network switch, use a Microsoft Windows 10 Pro computer that is not connected to the Internet.

You can use a ScanStation to set up the network switch.

This section describes two procedures required to set up the network switch:

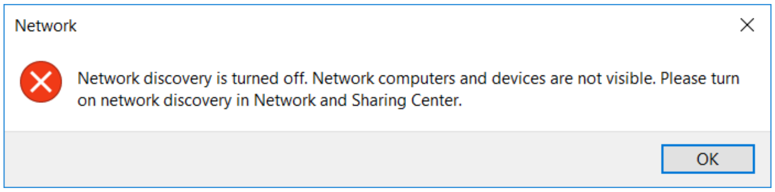
- Configuring the computer used to set up the network switch
- Configuring the network switch

4.7.3 Configuring the computer used to set up the network switch

To configure the computer used to set up the network switch:

1. Click the Start button on the Windows taskbar and search for and select **File Explorer**.
2. Select the **Network** option in the left navigation pane.
3. When a message appears, click **OK**.

4. When the message in Figure 4-7 appears, click **OK**.



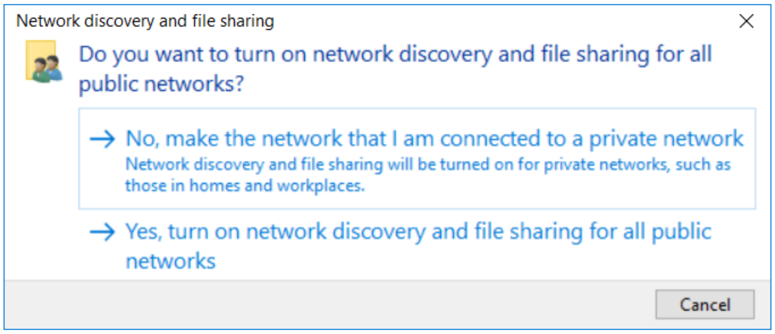
Network

Network discovery is turned off. Network computers and devices are not visible. Please turn on network discovery in Network and Sharing Center.

Figure 4-7. Message indicating that network discovery is turned off

5. When a yellow banner appears at the top of the Network window, click the banner and select **Turn on network discovery and file sharing** from the pop-up menu that appears.

6. When a message asks if you want to turn on network discovery and file sharing for all public networks (Figure 4-8), select **No, make the network that I am connected to a private network**.



Network discovery and file sharing

Do you want to turn on network discovery and file sharing for all public networks?

→ No, make the network that I am connected to a private network

Network discovery and file sharing will be turned on for private networks, such as those in homes and workplaces.

→ Yes, turn on network discovery and file sharing for all public networks

Figure 4-8. Network discovery and file sharing dialog

7. Click the **Network and Sharing Center** icon in the Network window.

8. Select **Change adapter settings** to open the Network Connections window.

9. Right-click the available Ethernet adapter and select the **Properties** option to open the Ethernet Properties dialog.

10. Double-click the **Internet Protocol Version 4 (TCP/IPv4)** option.

> **Note**: Note your current settings so that you can change them back after configuring the switch.

11. Select the **Use the following IP address** option and enter *10.0.0.254* in the IP address field.

12. Enter *255.255.255.0* in the Subnet mask field and click **OK**.

13. Click **OK** to close the Ethernet Properties dialog.

4.7.4 Configuring the network switch

To configure the network switch:

1. Plug one end of the AC power cord into the switch's AC power connector and plug the other end into an AC power outlet.

   During the initial setup process, the System LED indicator blinks green. After the network switch setup is complete, the System LED turns solid green. An amber LED indicates a problem with the switch.

2. Connect an Ethernet CAT cable to the Ethernet port on the computer and the other end to one of the numbered Ethernet ports on the front of the switch.

   > **Note**: Avoid plugging the Ethernet CAT cable into an unnumbered port as such ports are used as a terminal emulator.

3. Open a browser on the computer and navigate to 10.0.0.3 in the address field.

4. To log in, enter **cisco** for the user name and **cisco** for the password, and click **Log In**.

   > **Note**: The username, password and the IP address used to connect to the network switch can vary based on the model of network switch you are installing. Please refer to the manual of the network switch if you are encountering errors connecting.

5. On the Basic Configuration page, enter the physical location of the switch (such as, Clear County election central) in the **Host Name** field.

6. *On the Basic Configuration page enter a new username and new password.

7. On the Time Settings make sure it is set to the proper time zone for your area, click **Next**.

8. Enter **192.168.15.20** as the IP address under “Default gateway”, click **Next**.

9. On the Summary page, click **Apply** to save the configuration.

10. When a message asks if you want to proceed, click **OK**.

11. Close the browser window.

4.8 Assigning static IP addresses

Follow these steps to assign static IP addresses to the ScanStations:

1. Log in to the computer as a Windows administrator.

2. From the Windows taskbar, type **control** in the **Search** field, and select **Control Panel** from the search results.

3. Click **Network and Internet**, then click **Network and Sharing Center** and then click **Change Adapter Settings** on the left.
4. Right-click the available **Ethernet** adapter and select the **Properties** option to open the Ethernet Properties dialog.
5. Deselect the **Internet Protocol Version 6 (TCP/IPv6)** item.
6. Double-click the **Internet Protocol Version 4 (TCP/IPv4)** item.
7. Select the **Use the following IP address** option and enter an IP address in the **IP address** field that conforms to your IP schema (such as within the range of 192.168.15.2 to 192.168.15.249).
8. Click the **Subnet mask** field to populate it automatically.
9. In the **Default Gateway** field, enter the IP address of the gateway (such as 192.168.15.1) and then enter that same address in the **Preferred DNS server** field.
10. Click **OK**, close all open dialogs, and restart the computer for the changes to take effect.
11. Click the Start button on the Windows taskbar, search for and select **Command Prompt**.
12. To verify that the IP addresses are correct, type **ipconfig** in the Command Prompt windows and press **Enter**:
    - If the IP addresses are correct, close the Command Prompt window.
    - If you just changed any IP addresses and they appear to be incorrect, there may be some latency. In this situation, restart the computer, open a Command Prompt window, and enter the ipconfig command to verify that the changes have taken effect.

Repeat these steps for each ScanStation.

4.9 Mapping the ScanStation computer to the CountServer computer

All of the ClearCount software resides on the CountServer computer. Each ScanStation computer must connect to the CountServer computer through the network switch so the necessary files can be shared.

To map the ScanStation computer:

1. Log in to the ScanStation computer as the Windows administrator.
2. From the task bar, right-click the **Start** icon and select the **File Explorer** option.
3. Click the **This PC** option on the left.

4. On the Computer tab, click the **Map network drive** icon (Figure 4-9).

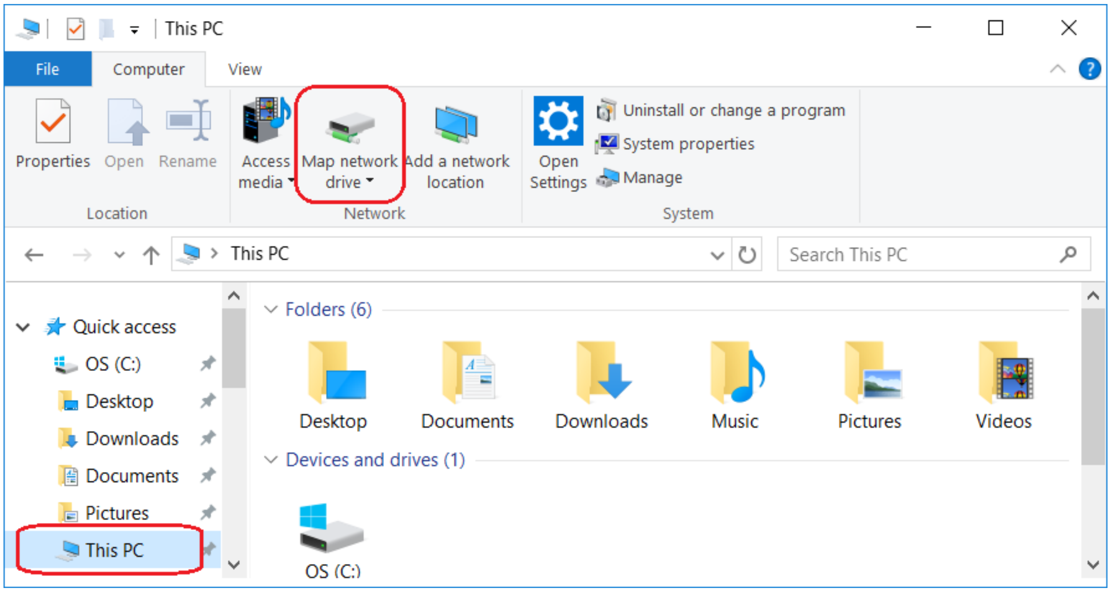
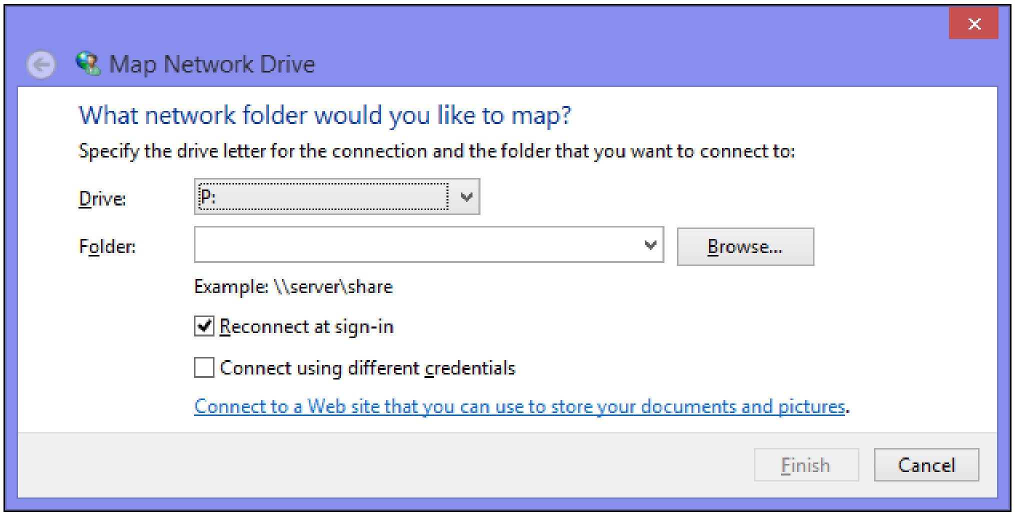


Figure 4-9. Selecting the Computer tab and Map Network Drive icon

5. In the Map Network Drive dialog (Figure 4-10), select the **P:** drive from the Drive drop-down list.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: P:

Folder:

Example: \\server\share

☑ Reconnect at sign-in

☐ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

Figure 4-10. Map Network Drive dialog

6. Enter the CountServer path using the CountServer computer's IP address (\\CountServerIPAddress\client) in the Folder field. For example, \\192.168.15.250\client\.

7. Ensure the **Reconnect at sign-in** option is selected.

8. Click **Finish**.

4.10 Creating a desktop shortcut to the P: drive

For convenience, you can create a desktop shortcut to the P: drive, which contains these commonly used ClearCount files:

- StartTabulator.cmd
- DeleteBox.bat
- UpdateScanner.bat

This drive also contains some system files that must *not* be opened except under the direction of Clear Ballot Technical Support.

To create a shortcut to the P: drive:

1. Log in to the ScanStation computer as the Windows administrator.
2. Click the Start button on the Windows task bar and search for and select **File Explorer**.
3. Locate the **P: drive** and drag it to your Desktop.

If you wish to do so, you can also create shortcuts directly to StartTabulator, DeleteBox, and Update Scanner by right-clicking each filename and selecting **Create Shortcut**.

4.11 Creating a restore point

Creating a restore point before making configuration changes to any ScanStation enables rolling back to the state that existed before the changes were made.

You can also create intermediate restore points at any time in the process.

To create a restore point:

1. Log in to the ScanStation computer as a Windows administrator.
2. From the task bar, type *restore* in the Search field and select **Create a restore point** from the search results.

   The System Properties dialog appears.
3. (If necessary) Click the **System Protection** tab.
4. Select the **OS (C:) (System)** available drive option and click **Configure**.

   The System Protection for OS (C:) appears.
5. Select the **Turn on system protection** option, click **Apply** and then click **OK**.
6. On the System Protection tab, click **Create**. The System Protection dialog appears.
7. Enter a descriptive name for the restore point using the following format:

   *yyyy-mm-dd-hh-mm*_Before_Clear_Ballot_configuration

8. Click **Create**.

   The restore point is created in a minute or two and the System Protection message box displays the message: *The restore point was created successfully*.

9. Click **Close** to dismiss the message.

10. Click **OK** to close the System Properties dialog.

4.12 Setting up the Fujitsu scanners

This section describes how to set up the Fujitsu scanners.

4.12.1 Installing the TWAIN driver

A TWAIN driver is required for communication between the ScanStation computer and the scanner. Use the same PSIPTWAIN driver for all scanner models.

To install the TWAIN driver:

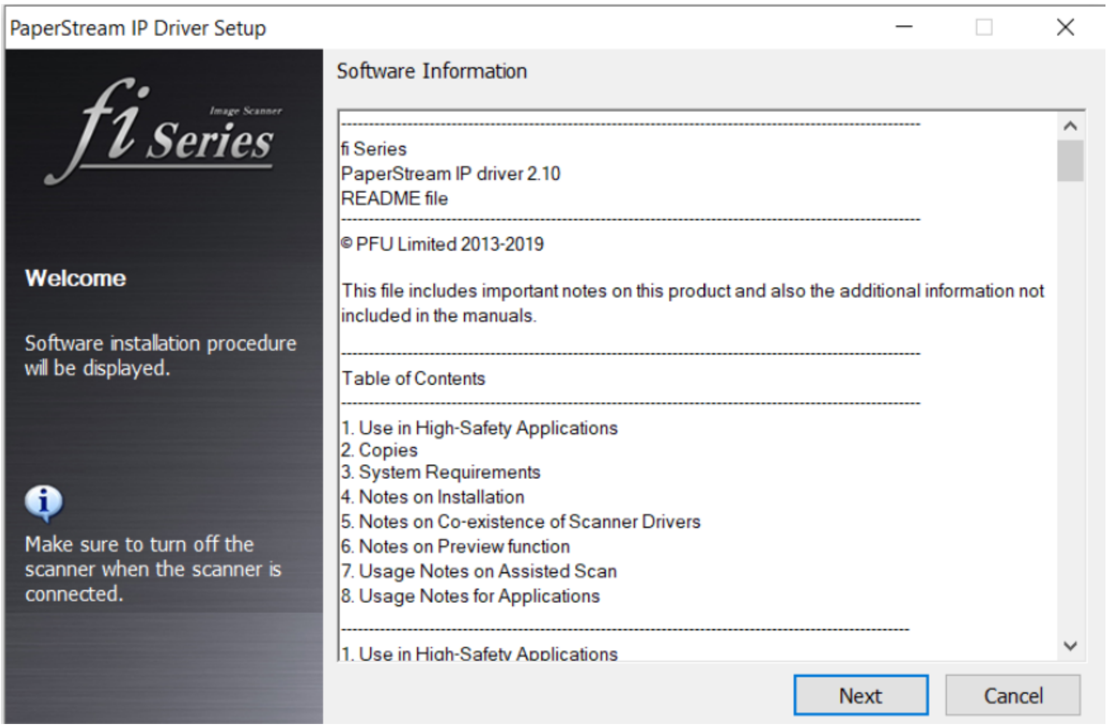
1. Ensure that the scanner is powered off.

   Note: If you are not performing a new installation or you used a previous model of Fujitsu scanner, uninstall the older TWAIN driver by typing *programs* in the **Search** field on the task bar and selecting **Add or remove programs** from the search results. Also, uninstall ScandAll Pro if it was previously installed for an older version of ClearCount.

2. On the Tools DVD, locate the file PSIPTWAIN-2_10_3.exe and double-click on it.

3. Select **Yes** to apply the changes to your system.

   The Welcome screen for the IP Driver Setup application appears (Figure 4-11).



PaperStream IP Driver Setup

Welcome

Software installation procedure will be displayed.

Make sure to turn off the scanner when the scanner is connected.

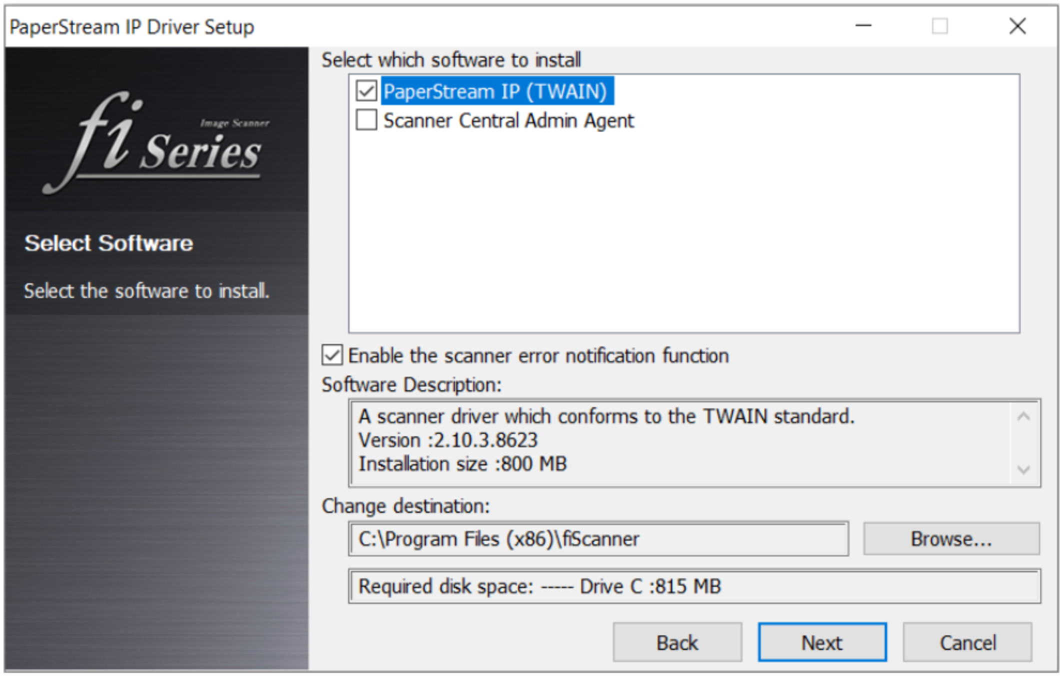
Software Information

```
--------------------------------------------------------------------------------
fi Series
PaperStream IP driver 2.10
README file
--------------------------------------------------------------------------------
© PFU Limited 2013-2019

This file includes important notes on this product and also the additional information not
included in the manuals.

--------------------------------------------------------------------------------
Table of Contents
--------------------------------------------------------------------------------
1. Use in High-Safety Applications
2. Copies
3. System Requirements
4. Notes on Installation
5. Notes on Co-existence of Scanner Drivers
6. Notes on Preview function
7. Usage Notes on Assisted Scan
8. Usage Notes for Applications

--------------------------------------------------------------------------------
1. Use in High-Safety Applications
```

Figure 4-11. Welcome screen for the PaperStream IP Driver Setup application

4. Click **Next**.

   The Select Software screen appears (Figure 4-12).



PaperStream IP Driver Setup

Select Software

Select the software to install.

Select which software to install

☑ PaperStream IP (TWAIN)
□ Scanner Central Admin Agent

☑ Enable the scanner error notification function

Software Description:

A scanner driver which conforms to the TWAIN standard.
Version :2.10.3.8623
Installation size :800 MB

Change destination:

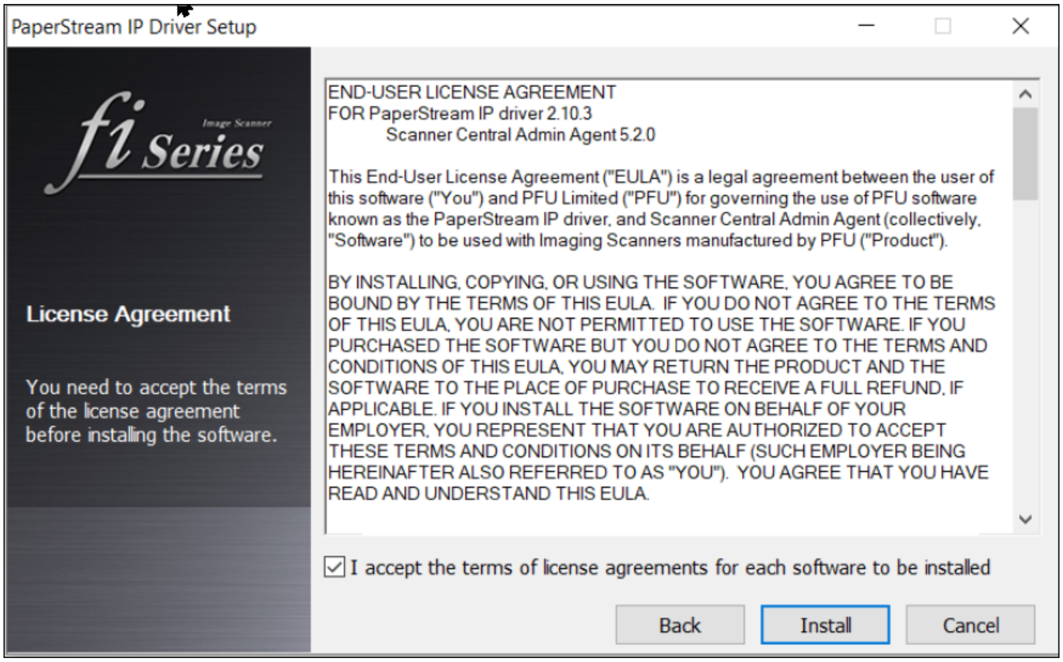
C:\Program Files (x86)\fiScanner

Required disk space: ----- Drive C :815 MB

Figure 4-12. Select Software screen

5. Clear the checkbox **Scanner Central Admin Agent** and click **Next**.

The License Agreement screen appears (Figure 4-13).


PaperStream IP Driver Setup
fi Series
Image Scanner
License Agreement
You need to accept the terms of the license agreement before installing the software.
Back
Install
Cancel

END-USER LICENSE AGREEMENT
FOR PaperStream IP driver 2.10.3
Scanner Central Admin Agent 5.2.0

This End-User License Agreement ("EULA") is a legal agreement between the user of this software ("You") and PFU Limited ("PFU") for governing the use of PFU software known as the PaperStream IP driver, and Scanner Central Admin Agent (collectively, "Software") to be used with Imaging Scanners manufactured by PFU ("Product").

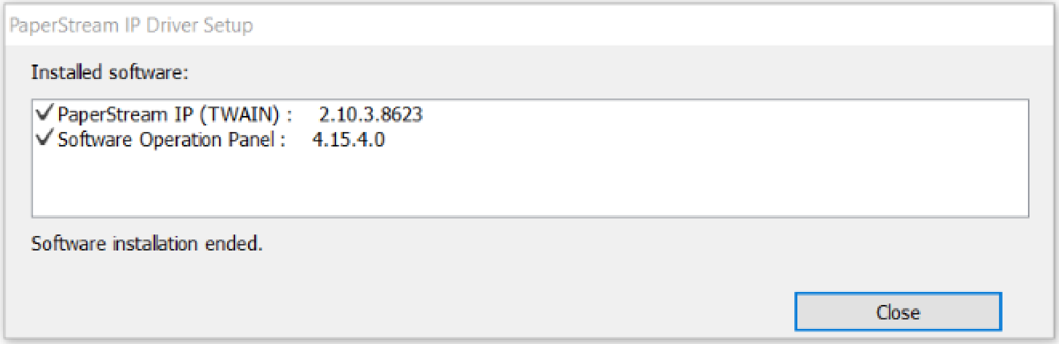
BY INSTALLING, COPYING, OR USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU ARE NOT PERMITTED TO USE THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE BUT YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS EULA, YOU MAY RETURN THE PRODUCT AND THE SOFTWARE TO THE PLACE OF PURCHASE TO RECEIVE A FULL REFUND, IF APPLICABLE. IF YOU INSTALL THE SOFTWARE ON BEHALF OF YOUR EMPLOYER, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS AND CONDITIONS ON ITS BEHALF (SUCH EMPLOYER BEING HEREINAFTER ALSO REFERRED TO AS "YOU"). YOU AGREE THAT YOU HAVE READ AND UNDERSTAND THIS EULA.

☑ I accept the terms of license agreements for each software to be installed

Figure 4-13. License agreement

6. Select the checkbox to accept the license terms, then click **Install**.

   When the installation is complete, the message shows that the software was installed (Figure 4-14).



Installed software:

✓ PaperStream IP (TWAIN) : 2.10.3.8623
✓ Software Operation Panel : 4.15.4.0

Software installation ended.

Figure 4-14. Message indicating that the software was installed successfully

7. Click **Close**.

4.12.2 Installing the Fujitsu Emulator software for previously-emulated scanners

Note: This section only applies to previously-emulated Fujitsu fi-7800 and fi-7900 scanners.

To install the Fujitsu Emulator software:

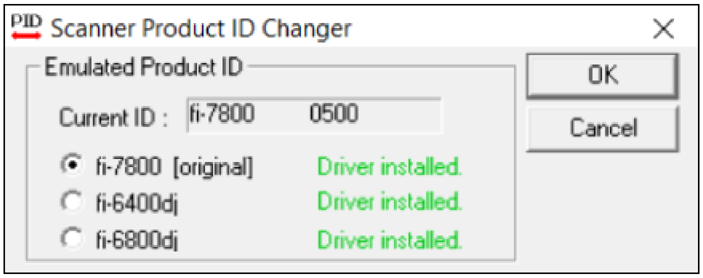
1. Connect the scanner to your computer and turn on the scanner.
2. On the ClearVote Tools DVD, navigate to the Fujitsu > Fujitsu Emulator folder.
3. Copy the folder from the DVD to the ScanStation computer's desktop.
4. Open the folder and double-click the FTLyEmu application file.

   The User Access Control dialog appears:

   (*Do you want to allow the following program to make changes to this computer?*).

5. Click **Yes**.

   The Scanner Product ID Changer dialog appears (Figure 4-15).



Scanner Product ID Changer

Emulated Product ID

Current ID : fi-7800 0500

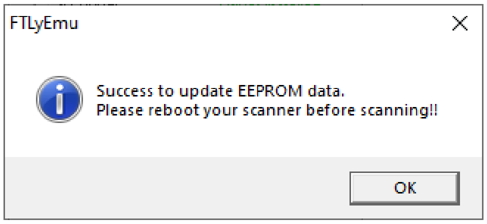
● fi-7800 [original] Driver installed.
○ fi-6400dj Driver installed.
○ fi-6800dj Driver installed.

Figure 4-15. Scanner Product ID Changer dialog

6. Select your model (fi-7800 or fi-7900) and click OK.

   Note: Do not interrupt the installation process.

7. When a confirmation message appears, click **OK** (Figure 4-16).



FTLyEmu

Success to update EEPROM data.
Please reboot your scanner before scanning!!

Figure 4-16. Confirmation message for a successful update

8. Delete the Fujitsu Emulator folder from the desktop and empty the recycle bin.
9. Turn the scanner off.

4.12.3 Installing the PaperStream Capture software

To install the PaperStream Capture software:

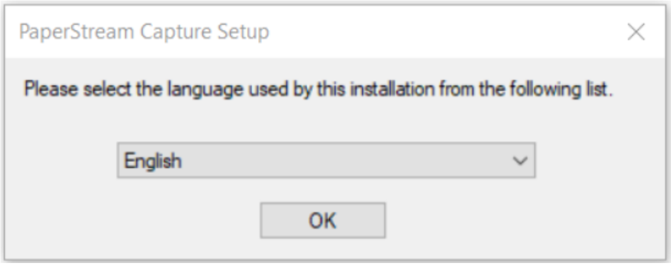
1. On the Tools DVD, locate the file PSC21000.exe and double-click it.

   The User Access Control dialog appears:

   (*Do you want to allow the following program to make changes to this computer?*).

2. Click **Yes**.

   The installer displays the Please select the language dialog (Figure 4-17).



PaperStream Capture Setup

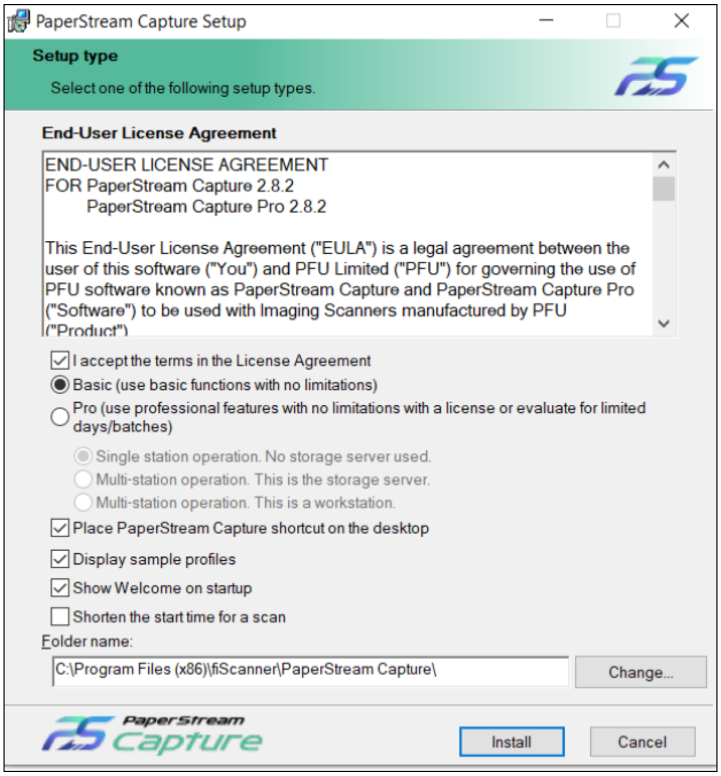
Please select the language used by this installation from the following list.

English

Figure 4-17. Please select the language dialog

3. Select **English** from the drop-down list and click **OK**.

   The Setup type dialog appears (Figure 4-18).



PaperStream Capture Setup

Setup type

Select one of the following setup types.

End-User License Agreement

END-USER LICENSE AGREEMENT
FOR PaperStream Capture 2.8.2
PaperStream Capture Pro 2.8.2

This End-User License Agreement ("EULA") is a legal agreement between the user of this software ("You") and PFU Limited ("PFU") for governing the use of PFU software known as PaperStream Capture and PaperStream Capture Pro ("Software") to be used with Imaging Scanners manufactured by PFU ("Product")

☑ I accept the terms in the License Agreement

● Basic (use basic functions with no limitations)

○ Pro (use professional features with no limitations with a license or evaluate for limited days/batches)

● Single station operation. No storage server used.

○ Multi-station operation. This is the storage server.

○ Multi-station operation. This is a workstation.

☑ Place PaperStream Capture shortcut on the desktop

☑ Display sample profiles

☑ Show Welcome on startup

□ Shorten the start time for a scan

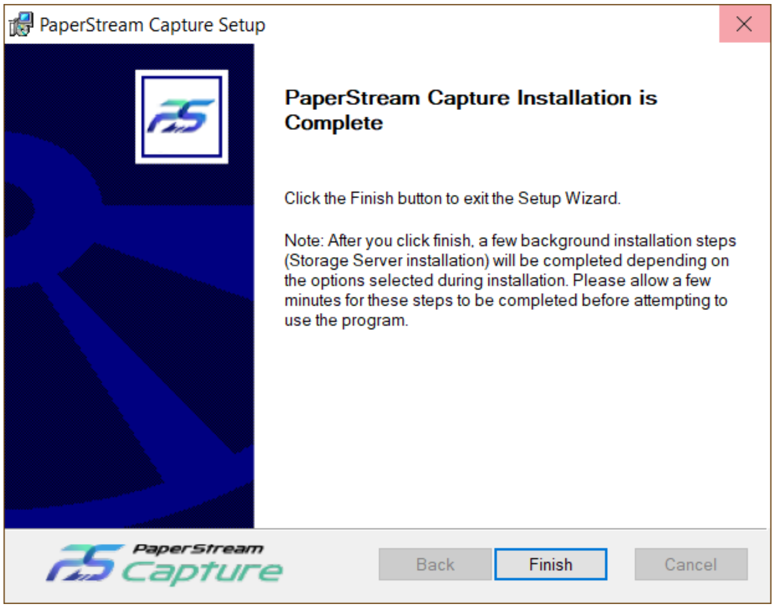
Folder name:

C:\Program Files (x86)\fiScanner\PaperStream Capture\

Figure 4-18. Setup Type dialog

4. On the Setup type dialog, do the following:
    a. Select the check box **I accept this license agreement**.
    b. Select the **Basic** option.
    c. Leave the other options in their default state.
    d. Click **Install**.

    A progress bar indicates the status of the installation and a dialog appears when it is complete (Figure 4-19).



PaperStream Capture Installation is Complete

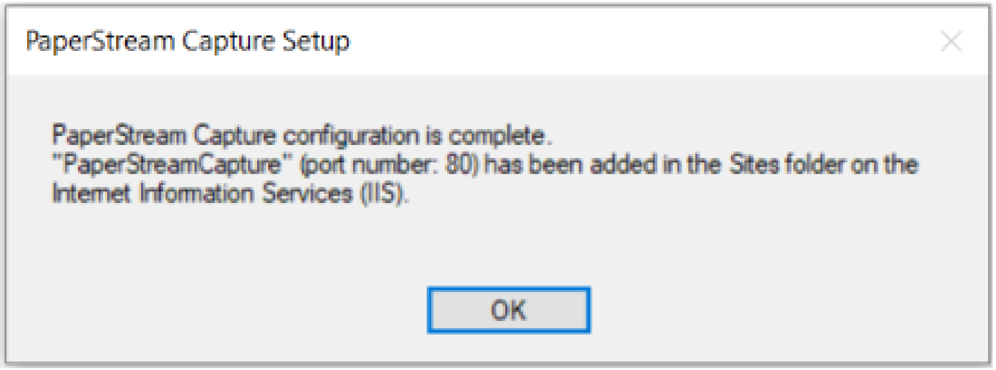
Click the Finish button to exit the Setup Wizard.

Note: After you click finish, a few background installation steps (Storage Server installation) will be completed depending on the options selected during installation. Please allow a few minutes for these steps to be completed before attempting to use the program.

Figure 4-19. Installation complete

5. Click **Finish**.

    The configuration process begins. When it is complete, a confirmation dialog appears (Figure 4-20).



PaperStream Capture configuration is complete.
"PaperStreamCapture" (port number: 80) has been added in the Sites folder on the Internet Information Services (IIS).

Figure 4-20. PaperStrean Capture—Configuration Complete

6. Click **OK**.

4.13 Installing the Fujitsu Scanner Error Recovery Guide

Fujitsu distributes an online Error Recovery Guide for each of its scanner models. A pop-up link to the guide appears whenever a scanner error occurs. There must be a local copy on each of the ScanStation computers.

To install the Error Recovery Guide:

1. Insert the ClearVote Tools DVD into the disc drive of the ScanStation computer and navigate to the Fujitsu > Scanner Error Recovery Guide folder.
2. Copy the executable (*.exe) for your scanner model number from the DVD to the ScanStation Desktop.
3. Double-click the executable file for your scanner.
4. Follow the on-screen prompts to complete the installation.

4.14 Configuring the scanner as a device

To ensure the ScanStation computer recognizes the scanner, the scanner must be configured as a device.

To configure the scanner as a device:

1. Use a USB cable to connect the scanner to a USB port on the ScanStation.
2. Power on the scanner.
3. Log in to the ScanStation computer as the Windows administrator.
4. From the task bar, type **scanner** in the **Search** field and select **Printers and scanners** from the search results.
5. In the Printers and scanners window, look for the scanner. If it appears in the list of devices by name or model, you can close the window.

If the scanner is not listed by name or model (if it appears as an unidentified device), this may mean that the scanner software needs to be reassociated with it. Repeat the steps in "Installing the TWAIN driver" on page 61 then repeat the steps in this section.

4.15 Running the scanner update script

A scanner update script imports the serial number of the scanner so that the ScanStation computer/scanner combination can be identified later if issues arise.

The scanner operator must ask an administrator who knows the administrative password for the ScanStation computer to run the update script. The scanner operator *cannot* know the password.

Note: Ensure that the scanner is connected to your ScanStation computer before running the update script.

To run the scanner update script:

1. Turn on the scanner.

2. Log in to the ScanStation computer.

3. Double-click the desktop shortcut to the P: drive.

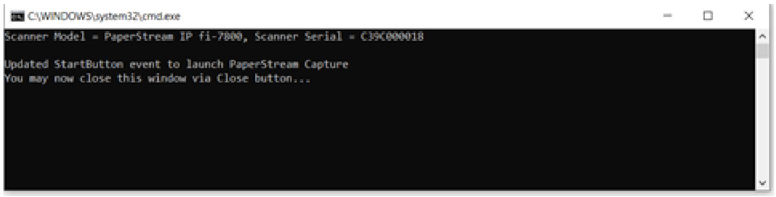
   See "Mapping the ScanStation computer to the CountServer computer" on page 58 for more information.

4. Double-click the update script **UpdateScanner.bat** and click **Run**.

5. When the User Account Control dialog appears, enter the administrator password (if run from a non-administrator account) and select **Yes**.

   The update script stores the scanner's model and serial numbers in the Windows Registry for use by the BallotSweeper and sets the Scan button event for the scanner to launch PaperStream Capture.

6. When the script is finished, checking the information in the Command Prompt window to ensure the system recognizes the scanner model and serial number (Figure 4-21).

   ```
   Scanner Model = PaperStream IP fi-7800, Scanner Serial = C39C000018

   Updated StartButton event to launch PaperStream Capture
   You may now close this window via Close button...
   ```

   Figure 4-21. Checking that the system recognizes the scanner model and serial number

7. If the information is correct, close the window.

   If the information is incorrect, try each of the following steps in order:

   a. Turn off and restart the scanner and then rerun the script.

   b. If (a) does not work, restart the computer and rerun the script.

   c. If (b) does not work, uninstall and reinstall the scanner TWAIN driver.

   d. If none of these troubleshooting steps work, contact Clear Ballot Technical Support.

4.16 Importing the Clear Ballot Profile

Use the PaperStream Capture Import tool to import ClearBallotProfile.CAB to the ScanStation.

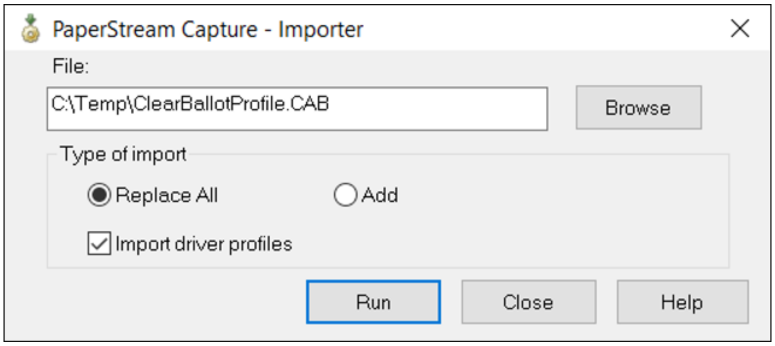
To import the profile:

1. Copy ClearBallotProfile.CAB from the P: drive to a local drive on the ScanStation.

2. From the Windows Start menu, navigate to the PaperStream Capture folder.

3. Expand the section and select **Importer**.

   The PaperStream Capture - Importer dialog appears (Figure 4-22).



File: C:\Temp\ClearBallotProfile.CAB

Type of import

● Replace All ○ Add

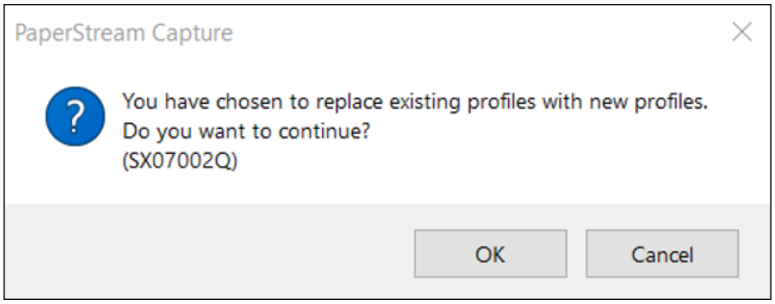
☑ Import driver profiles

Figure 4-22. PaperStream Capture - Importer dialog

4. Click **Browse** to navigate to the Clear Ballot profile on your local drive.

5. Keep the **Type of import** as **Replace All**, select **Import driver profiles**, and click **Run**.

   If you have previously imported PaperStream Capture profiles, a message appears asking if you want to replace existing profiles (Figure 4-23).



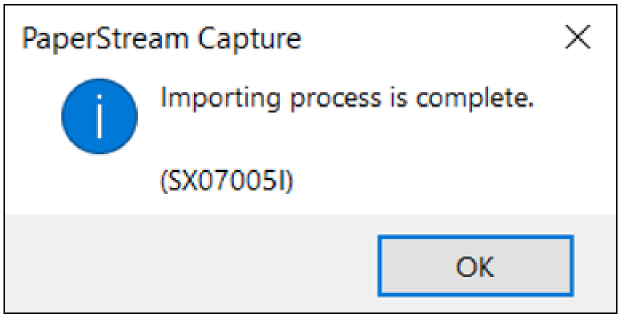
You have chosen to replace existing profiles with new profiles.
Do you want to continue?
(SX07002Q)

Figure 4-23. Message to replace existing profiles

6. Click **OK**.

7. When the Account Control dialog appears, click **Yes**.

   When the import process is complete, a confirmation message appears (Figure 4-24).



PaperStream Capture

Importing process is complete.

(SX07005I)

Figure 4-24. Confirmation message—import proces complete

8. Click **OK**.

4.17 Configuring PaperStream Capture

Use the Administrator and the Configure Profiles options to configure the PaperStream Capture tool.

To configure PaperStream Capture:

1. Open PaperStream Capture and close the Welcome dialog.

2. From the drop-down menu, select **Administrator Tool** (Figure 4-25).

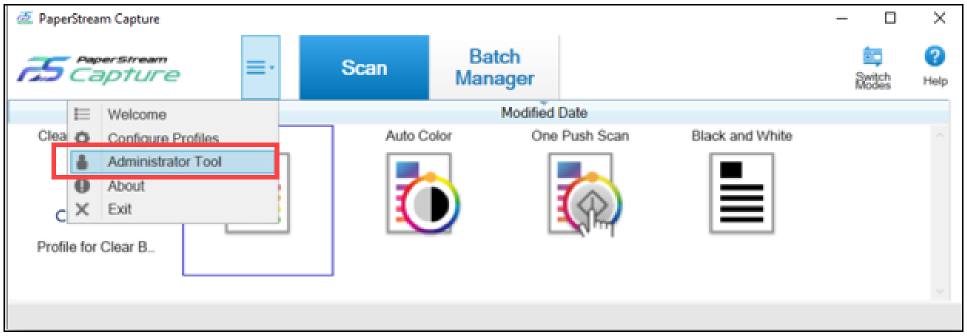
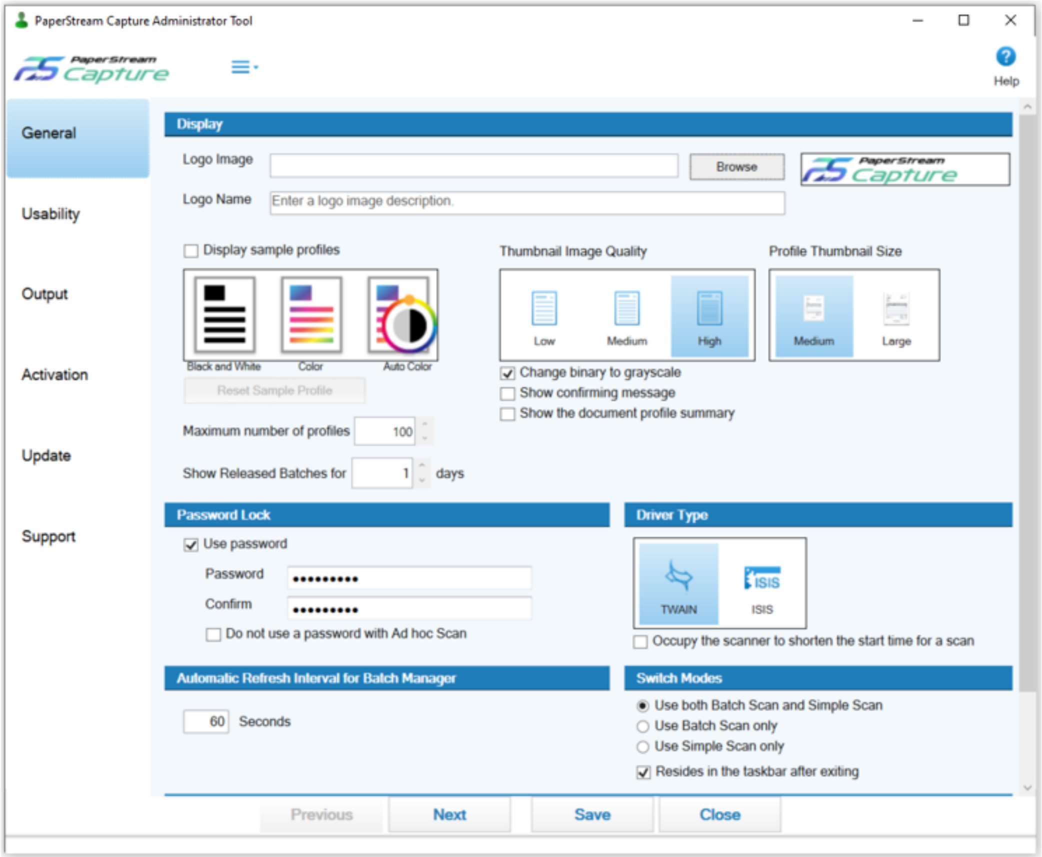


Figure 4-25. Selecting the Administrator tool

PaperStream Capture displays the Administrator Tool (Figure 4-26).



PaperStream Capture Administrator Tool

General | Usability | Output | Activation | Update | Support

Display

Logo Image [ ] Browse

Logo Name: Enter a logo image description.

□ Display sample profiles

Maximum number of profiles: 100

Show Released Batches for: 1 days

Thumbnail Image Quality: Low / Medium / [✓ High]

Profile Thumbnail Size: [✓ Medium] / Large

☑ Change binary to grayscale
□ Show confirming message
□ Show the document profile summary

Password Lock

☑ Use password

Password: •••••••••

Confirm: •••••••••

□ Do not use a password with Ad hoc Scan

Driver Type

[✓ TWAIN] / ISIS

□ Occupy the scanner to shorten the start time for a scan

Automatic Refresh Interval for Batch Manager

60 Seconds

Switch Modes

● Use both Batch Scan and Simple Scan
○ Use Batch Scan only
○ Use Simple Scan only
☑ Resides in the taskbar after exiting

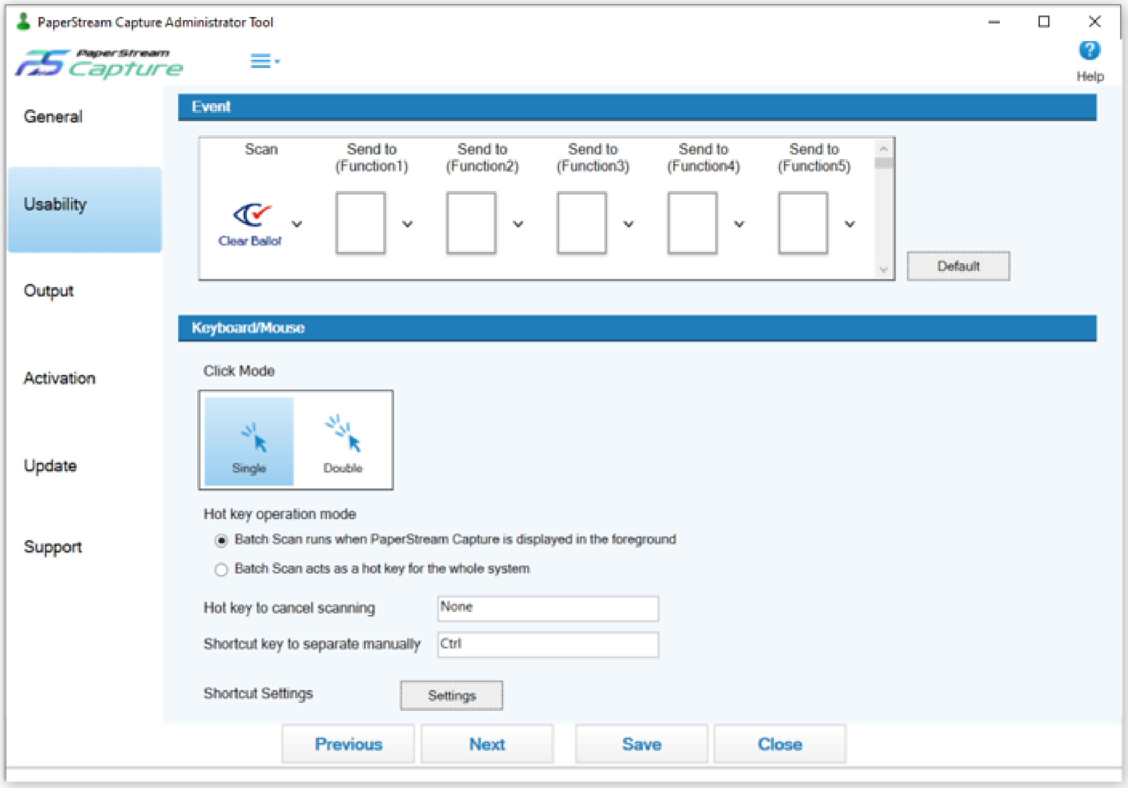
Figure 4-26. Administrator Tool

3. On the **General** tab, clear the checkbox to **Display sample profiles**.

4. (Optional) To require passwords for profiles and PaperStream Capture settings, select the **Use password** checkbox in the Password Lock section and enter a password.

5. Record the password in the Installation checklist.

6. Select the **Usability** tab and locate the **Scan** drop-down list in the Event section (Figure 4-27).



Scan: Clear Ballot

Click Mode: Single

Hot key operation mode

● Batch Scan runs when PaperStream Capture is displayed in the foreground

○ Batch Scan acts as a hot key for the whole system

Hot key to cancel scanning: None

Shortcut key to separate manually: Ctrl

Shortcut Settings

Figure 4-27. Scan selection on the Usability tab of the PaperStream Capture Administrator tool

7. Ensure that the Clear Ballot Profile is selected.

8. Select **Save** and **Close**.

4.18 Configuring PaperStream Capture Profiles

To configure PaperStream Capture profiles:

1. Open PaperStream Capture.

2. Select **Configure Profiles** from the drop-down list (Figure 4-28).

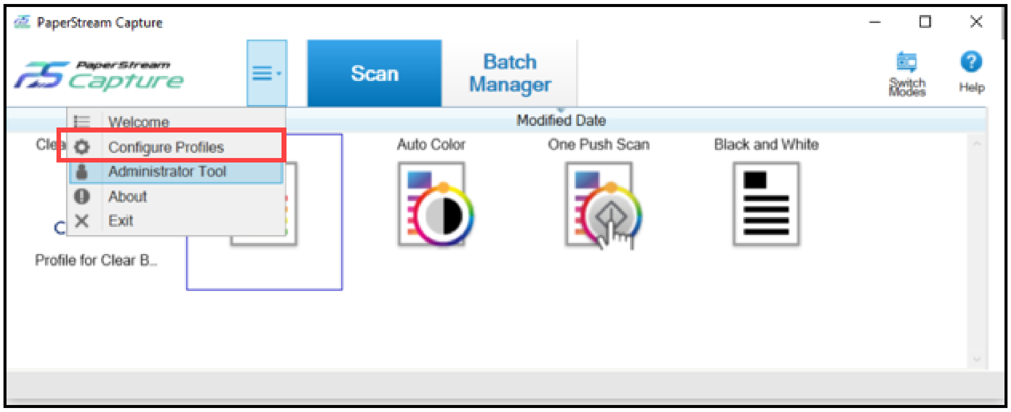


Figure 4-28. Selecting Configure Profiles

PaperStream Capture displays the Configure Profiles screen (Figure 4-29).

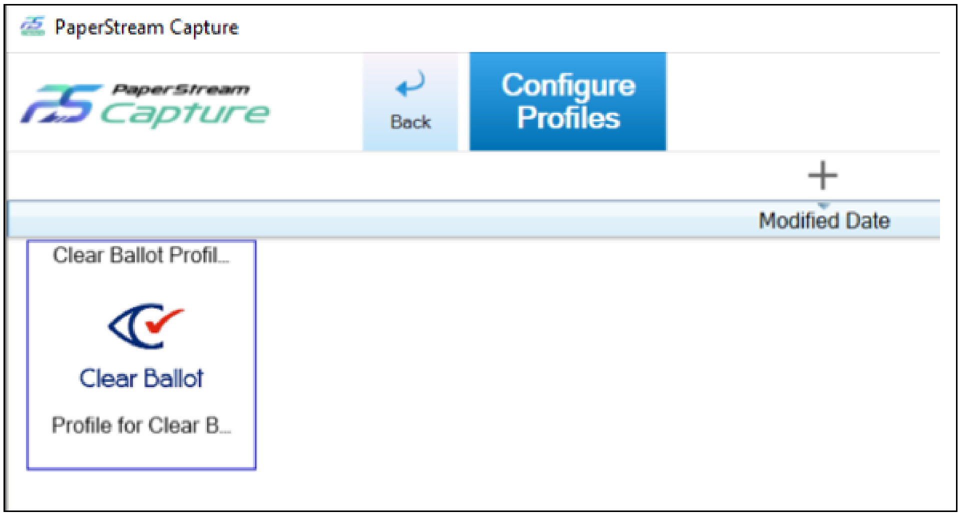
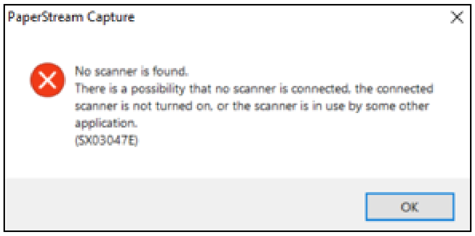


Figure 4-29. Configure Profiles screen

3. Hover your mouse over the Clear Ballot Profile and select the pencil icon to edit.

4. From the menu on the left, click **Source**.

   If you do not have a fi-7800 scanner connected to the ScanStation, the error message in Figure 4-30 appears:



PaperStream Capture

No scanner is found.
There is a possibility that no scanner is connected, the connected scanner is not turned on, or the scanner is in use by some other application.
(SX03047E)

OK

Figure 4-30. Error message—fi-7800 is not connected

5. Click **OK**.

6. Click the drop-down in the Source section and select the scanner model that is plugged into your ScanStation (Figure 4-31).

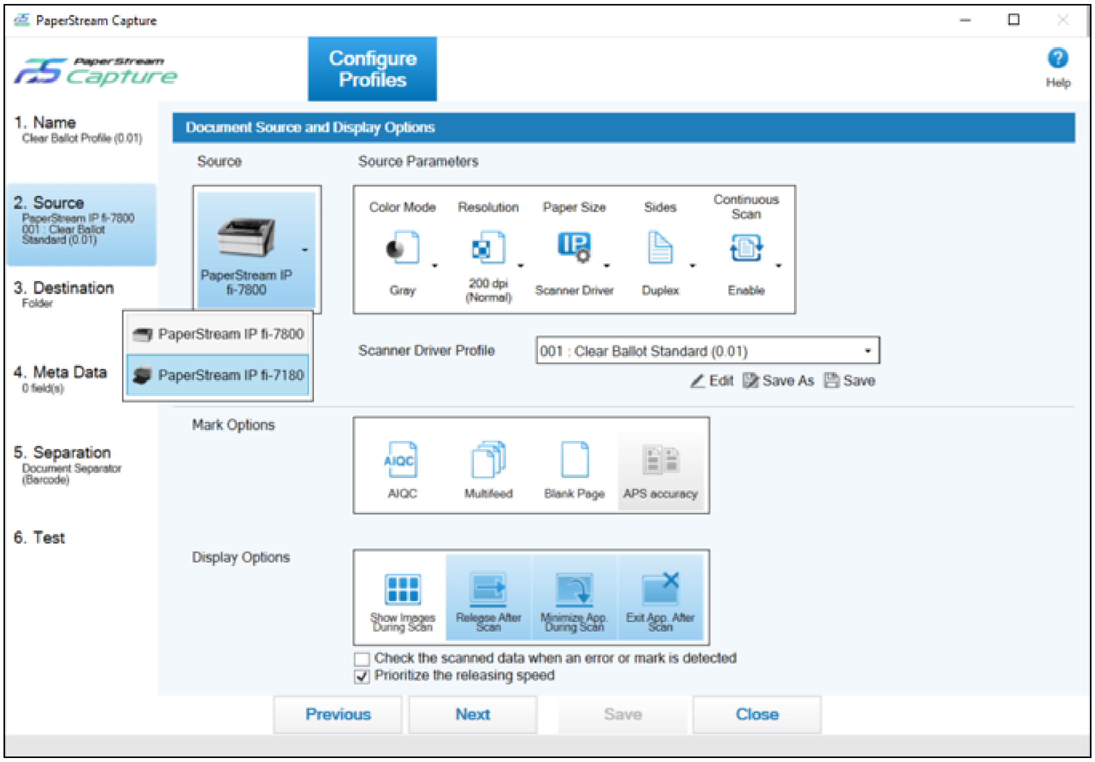


Figure 4-31. Selecting the scanner model

7. If a customer has a scanner with an imprinter installed and wants to enable imprinting and endorsing, select the option **Clear Ballot Imprinter** in the Scanner Driver Profile drop-down list.

8. Select **Save** and **Close**.

9. Click the **Back** button to the left of the Configure Profiles tab.

10. Exit PaperStream Capture.

4.19 Setting Windows passwords

Administrative users must have a nondefault password. Scanner operators are required to have a password that is not the Windows default. All passwords are subject to Windows complexity requirements.

Before assigning passwords to individuals, give consideration to who has the administrator password and which people have a scanner operator password.

4.19.1 Configuring the Windows password policy

To configure the password policy on Windows computers:

1. Log in to the computer as the Windows administrator.
2. Click the Start button on the Windows taskbar and search for and select **Edit group policy**.

   Windows display the Group Policy editor
3. In the navigation pane, select **Computer Configuration> Windows Settings> Security Settings> Account Policies**.
4. Double-click the **Password Policy** option on the right.
5. In the Password Policies options, double-click **Minimum Password Length**.
6. Set the length to 8 characters and click **OK**.
7. In the Policy options, double-click **Password must meet complexity requirements**.
8. Set to **Enabled** and click **OK**.
9. Close the Group Policy Editor.

Complexity requirements are enforced when passwords are changed or created. If the **Password must meet complexity requirements** option is checked, passwords must meet the following minimum requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Be at least six characters in length.
- Contain characters from three of the following four categories:
  - Latin uppercase characters (A through Z)
  - Latin lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Nonalphanumeric characters (for example, !, $, #, %)

4.19.2 Changing the Windows administrator password

Note: *Never* allow anyone who is not an administrator to learn the Windows administrator password.

To change the administrator password:

1. Log in to the computer as the default Windows administrator.
2. Click the Start button on the Windows taskbar and search for and select **Settings**.

3. Select **Accounts**.

   Windows displays the Your info page.

4. Select **Sign-in Options**.

   Windows displays the Sign-in Options page.

5. Under **Password**, click **Change**.

6. On the next page, enter the current (default) password and click **Next**.

7. On the next page, enter and reenter the new password, enter the password hint and click **Next**.

   The new password must meet the complexity requirements that you established in the previous section "Configuring the Windows password policy."

8. On the next page, click **Finish**.

9. Log out of Windows and log back in with the new password.

Record the Windows administrator password on the Installation checklist (page 124).

4.20 Creating the Windows non-administrative user

The non-administrative user account is for scanner operators. It is a standard Windows account with the addition of a password. This user:

- Can run the Tabulator application.
- Can run the scanner software.
- Requires the presence of the Windows administrator to run the scanner update script and start the DeleteBox application (by entering the ScanStation account password).

To create the non-administrative user account:

1. Log in to the ScanStation computer as the Windows administrator.

2. From the task bar, right-click the Microsoft Windows **Start** icon and select **Settings**.

3. Select **Accounts** and then select **Family and Other People**.

4. Select **Add Someone Else to this PC**. Because the computer is not connected to the Internet, you are automatically directed to create a local account.

5. Enter the user name (for example, *ScannerOperator1*.)

6. Enter and reenter the password.

7. Enter a password hint, click **Next** and click **Finish**.

8. To verify creation of the standard user:
   a. From the Accounts page, select the new user.
   b. Click **Change account type**.
   c. Verify the Account Type is set to **Standard User** and click **OK**.

Record the non-administrative user name and password on the Installation checklist (page 124).

4.21 Configuring the non-administrative user

To set up access to applications for the non-administrative user:

1. Log out as the administrator and log back in as the non-administrative user.
2. Map the ScanStation computer to the CountServer computer.

   See "Mapping the ScanStation computer to the CountServer computer" on page 58.
3. Create a desktop shortcut to the P: drive.

   See "Creating a desktop shortcut to the P: drive" on page 60.
4. Configure the scanner as a device.

   See "Configuring the scanner as a device" on page 67.
5. Run the scanner update script.

   See "Running the scanner update script" on page 67

   When you run the scanner update script from a non-administrative account, a supervisor must be present to provide the supervisor password.
6. Configure the scanner profile and event.

   See "Configuring PaperStream Capture" on page 70.

4.22 Creating a restore point

Creating a restore point before making configuration changes to any ScanStation computer enables rolling back to the state that existed before the changes were made.

You can also create intermediate restore points at any time in the process.

To create a restore point:

1. Log in to the ScanStation computer as a Windows administrator.
2. From the task bar, type *restore* in the Search field and select **Create a restore point** from the search results. The System Properties dialog appears.
3. (If necessary) Click the **System Protection** tab.

4. Click **Create**. The System Protection dialog appears.

5. Enter a descriptive name for the restore point using the following format:

   *yyyy-mm-dd--hh-mm*_Before_Clear_Ballot_configuration

6. Click **Create**. The restore point is created in a minute or two and the System Protection message box displays the message: *The restore point was created successfully*.

7. Click **Close** to dismiss the message.

8. Click **OK** to close the System Properties dialog.

4.23 Hardening the ScanStation computers

Hardening the ScanStation computers in the ClearCount system consists of minimizing routes of access to them and implementing malware protections.

Note: Hardening includes procedural and environmental elements that may be governed by jurisdictional statute. Follow all steps to harden your system. No steps are recommended or optional. Be sure to consult jurisdictional regulations as part of the hardening process. Jurisdictional voting system security regulations may dictate that you do more than described in this section.

4.23.1 Updating Microsoft Defender Antivirus

Microsoft provides the Microsoft Defender Antivirus program (also called Windows Defender) with its Windows operating system. To keep the virus definitions up to date, you must update the program. Clear Ballot recommends that the Microsoft Defender Antivirus program be updated on every ScanStation computer and CountStation computer when the following events occur:

- When the system is first installed and configured
- Before each election

Because computers used in elections must *never* be connected to the Internet, the virus definition update must be performed offline using removable media.

To download antivirus definitions:

1. On a computer outside the closed ClearCount network that has a USB port and Internet connection, navigate to https://www.microsoft.com/security/portal/definitions/adl.aspx.

2. Insert a USB drive in the USB port and download the antivirus definitions to the USB drive according to the instructions on that site for your operating system and bit version.

   The software is delivered as a single file named *mpam-fe.exe* or something similar.

3. Eject the USB drive and then remove it from the computer where you downloaded the antivirus definitions.

If Windows software restriction policies are in effect on the computer being updated, disable the restrictions or add a temporary path rule to allow the update to run.

To update Microsoft antivirus software offline:

1. Log in to the computer as the Windows administrator.
2. Insert the USB drive into a USB port on the computer and browse to the file.
3. Right-click the file and select the **Run as Administrator** option from the pop-up menu.
4. When the User Account Control dialog appears, click **Yes** to run the update. You may see the mouse pointer spinning as the update progresses. If not, wait 30 seconds.
5. From the task bar, type *settings* in the Search field and then select **Settings** from the search results.

   The Windows Settings page appears.
6. Click **Update & security**.
7. Select **Windows Defender** on the left and then click **Open Windows Defender**.

   The Windows Defender dialog opens.
8. Click the **Update** tab and check the date and time that the definitions were created. The date should be the date you downloaded the file.
9. Close the Windows Defender dialog.

Maintain the history and archive copies of each update.

4.23.2 ScanStation hardening script

Hardening the ClearCount system makes it more secure from threats. The ScanStation hardening script performs several critical procedures on the ScanStation computer, including the following:

- Enables FIPS 140-2 security mode
- Disables the wireless and Bluetooth Internet services
- Disables the autoplay feature
- Disables Cortana
- Disables Microsoft consumer experiences
- Enables the software execution control for non-administrator accounts and allows only the programs in the Windows system32 directory to run
- Disables browser updates

To run the ScanStation hardening script:

1. Log in to the ScanStation computer as an administrator
2. Insert the ClearVote Tools DVD into the disc drive and navigate to the Hardening Scripts folder.
3. Copy the ScanStation Harden folder to the ScanStation desktop.
4. Open the ScanStation Harden folder, right-click the file **harden.bat** and select **Run as administrator** from the pop-up menu.
5. When the script finishes, restart the computer.

   You must restart the computer for the changes to take effect.
6. Delete the ScanStation Harden folder from the desktop and empty the recycle bin.

4.23.3 Restricting access to the BIOS

Access to the BIOS is restricted by implementing an administrator password. The behavior of the BIOS depends upon the computer make and model. Consult your computer’s documentation or contact Clear Ballot Technical Support for details.

The following procedure for a Dell Latitude 5590 computer is an example.

To restrict access to the BIOS:

1. Press the Shift key while shutting down the computer. The computer shuts down.
2. Press the F2 key while starting up the computer. The BIOS manager appears.
3. Set the BIOS password:

   All user names and passwords must satisfy the rules and guidelines provided in "Login credential rules and guidelines" on page 121.

   a. Using the arrow keys, navigate to the Security screen and select **Admin Password**.

   b. Enter and confirm the password.

   c. Record the BIOS password on the Installation checklist (page 124).
4. To save your changes, click **Apply** and then click **Exit**.
5. Restart the computer and verify that the changes have been implemented.

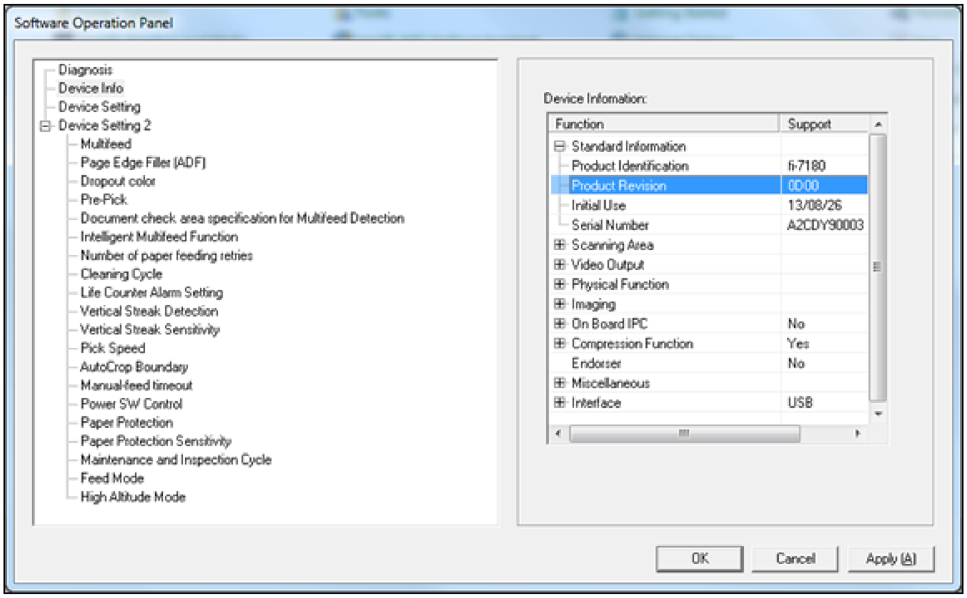
4.24 Hardening scanners

To harden each scanner so that its firmware is protected, perform these steps:

1. Log in to the ScanStation computer as an administrator.

2. Click the Start button on the Windows taskbar and search for and select **Software Operation panel**.

   Windows displays the Software Operation Panel dialog (Figure 4-32).



Device Information:

Function	Support
⊟ Standard Information	
Product Identification	fi-7180
Product Revision	0D00
Initial Use	13/08/26
Serial Number	A2CDY90003
⊞ Scanning Area	
⊞ Video Output	
⊞ Physical Function	
⊞ Imaging	
⊞ On Board IPC	No
⊞ Compression Function	Yes
Endorser	No
⊞ Miscellaneous	
⊞ Interface	USB

Figure 4-32. Software Operation Panel

3. In the left pane, select **Device Info**.

4. In the right pane, expand **Standard** information.

5. Record the values for Product Identification (scanner model), Serial Number, and Product Revision (firmware version) on the "Installation checklist" on page 124.

6. Apply tamper-evident tape on the screws along the bottom exterior of the scanner and press the tape down around the outside of each screw.

   The secured tape is a seal that deters tampering and provides evidence of any manipulation of the scanner firmware.

7. Monitor the scanner for evidence of tampering.

   If unauthorized access to scanner firmware occurs, the jurisdiction must contact Clear Ballot and Fujitsu. *Only* a licensed Fujitsu support technician can reinstall the proprietary scanner firmware.

4.25 Enabling BitLocker (optional)

When Windows is installed, BitLocker encrypts the drive. Because the mode of encryption does not meet Clear Ballot standards, you must decrypt the drive. After hardening the computer, which sets the encryption mode to FIPS 140-2, you may choose to re-enable BitLocker and encrypt the drive.

To enable BitLocker:

1. Click the Start button on the Windows taskbar, search for and select **Manage BitLocker**.
2. When Windows displays the BitLocker Drive Encryption window, click the option to **Turn on BitLocker** and accept any confirmation dialogs that appear.
3. When Windows displays the recovery key dialog, insert a USB drive into the computer and click **Save to a File**. Navigate to the desired location on the USB drive and click **Save**.

   Note: Store this file in a secure location so that it is available for future use.

4. On the How do you want to back up your recovery key dialog, click **Next**.
5. When Windows displays the Choose how much of your drive to encrypt dialog, select **Encrypt used disk space only (faster and best for new PCs and drives)** and click **Next**.
6. When Windows displays the Choose which encryption mode to use dialog, select **New encryption mode (best for fixed drives on this device)** and click **Next**.
7. When Windows displays the Are you ready to encrypt this drive dialog, check the **Run BitLocker system check** box and click **Continue**.
8. In the dialog that appears, click **Restart Now**.

   Windows restarts.

4.26 Powering down and restarting the ScanStation computer

Before validating the software setup, you *must* complete the hardening process by powering down and restarting the ScanStation computer.

4.27 Testing the ScanStation configuration

See the following topics in the *ClearCount Election Administration Guide*:

- "Readiness testing"
- "Logic and accuracy testing"

4.28 Preparing for daily scanning

Before the start of scanning each day, or if you change the physical configuration, follow the scanning procedures described in the *ClearCount Election Administration Guide*.

Chapter 5. Configuring CountStations

CountStation computers connect to the CountServer computer by using a browser on a closed, wired Ethernet network. Follow each section of this chapter in order to configure each CountStation computer.

5.1 Updating the BIOS version on the Dell 5521

Before you install Windows on a Dell 5521 computer, follow this procedure to ensure the BIOS version is version 1.5.3 or greater:

1. If you are installing from the DVD drive, skip step 1 and continue with step 2.

   If you are using a USB drive, copy the downloaded BIOS file to a USB drive.

   The USB drive does not need to be a bootable device.

2. Insert the USB or DVD drive containing the installation files into any USB port on the Dell 5521 computer.

3. Turn on the computer.

4. At the Dell logo screen, press **F12** to access the one-time boot menu.

5. In the Other Options section, select **BIOS Flash Update**.

6. Browse to the location of the BIOS file. select it, and click **OK**.

7. Verify the existing system BIOS information and the BIOS update information.

8. If the BIOS version is less than version 1.5.3, click **Begin Flash Update**.

9. Review the Warning message and click **Yes** to proceed with the update.

   The computer restarts and displays a progress bar at the Dell logo screen. The computer restarts again when the update is complete.

10. Go back to the BIOS Boot Menu and check that the BIOS version is correct in the top right hand corner.

5.2 Installing the Windows 10 Pro operating system

To install Windows 10 Pro:

1. Turn off the computer and insert the Microsoft Windows 10 Pro DVD into the drive.

2. If you are using a Dell Latitude 5500 or 5511 model, turn on the computer and repeatedly press **F12** until the message "Preparing one-time boot menu" appears at the top right on the screen.

   The One-Time Boot menu appears.

3. If you are using a Dell Latitude 5500 or 5511 model, ensure that SATA Operation is set to **AHCI:**
   a. Under **Other Options**, select **BIOS Setup**.
   b. Expand **System Configuration** and select **SATA Operation**.
   c. If AHCI is not selected, select it and click **Yes** in the confirmation dialog.
   d. Click **Apply** and **OK** in the Apply Settings Confirmation dialog.
   e. Click **Exit**.
4. If you are usig a Dell Latitude 5521 model, do the following:
   a. Press **F2** at boot to enter the BIOS setup menu.
   b. In the left pane, select **Storage**.
   c. In the right pane at the top, **AHCI/NVMe**.
   d. In the left pane, select **Security**.
   e. Scroll all the way to the bottom of the right pane to the last section entitled "UEFI Boot Security" and select **Always**.
   f. Click **Apply Changes**.
5. When the computer restarts, repeatedly press **F12** until the message "Preparing one-time boot menu" appears at the top right of the screen.

   The One-Time Boot menu appears.
6. For the Latitude 5500 and 5511, access the One-Time Boot menu and do the following:
   a. Confirm that the Boot menu is set to **UEFI: Secure Boot: ON**.
   b. Select the disk/DVD mode option from the UEFI BOOT section.

      To find the disk, locate the line item that contains the characters "DVD."
7. For the Latitude 5521, press **F2** at boot to enter the BIOS setup menu and then do the following:
   a. In the left pane, select **Security**.
   b. Scroll all the way to the bottom of the right pane to the last section entitled "UEFI Boot Security and select **Always**.

8. To check the Secure Boot setting:

   a. Click the Start button on the Windows taskbar and search for and select **Powershell**.

   b. At the prompt in the Windows Powershell, enter:

      ```
      Confirm-SecureBootUEFI
      ```

      The PowerShell returns the value `True` if SecureBoot is correctly configured.

9. Reboot the computer.

10. When the computer restarts, repeatedly press **F12** until the message "Preparing one-time boot menu" appears at the top right of the screen.

    When the One-Time Boot menu appears, do the following:

    a. Select the disk/DVD mode option from the UEFI Boot section.

    b. To find the disk, locate the line item that contains the characters "DVD."

11. Select the disk/DVD mode option from the UEFI Boot section.

12. To find the disk, locate the line item that contains the characters "DVD."

13. Press **Enter** on the DVD line item.

    The installation begins.

14. If message "Press any key to boot from CD or DVD ..." appears, press any key on your keyboard.

15. When the Windows Setup dialog appears, select the desired language and click **Next**.

16. In the next dialog, click **Install Now**.

17. When the license terms appear, select the checkbox and click **Next**.

18. In the next dialog, select the **Custom: Install Windows only (advanced)** option.

19. When asked where you want to install Windows, do the following:

    a. Remove any existing partitions. Select the first partition and click the **Delete** icon. A message appears. Click **OK**.

    b. Remove each partition until a single drive named *Drive 0 Unallocated Space* remains.

    c. Click **Next**.

    The installation beings and takes about 10 minutes. Then the computer restarts.

20. At the Get going fast dialog, click **Customize**.

    The Customize settings dialog appears.

21. In the Personalization settings, click each option to turn it off and click **Next**.

22. In the Location settings, turn it off and click **Next**.

23. In the Connectivity and error reporting settings, click each option to turn it off and click **Next**.

24. In the Browsers, protection, and update settings, click each option to turn it off and click **Next**.

25. When the Create an account for this PC dialog appears, enter the user name and password for the Windows administrator and click **Next**.

26. (Recommended) Record the Windows administrator user name and password on the Installation Checklist.

27. In the Meet Cortana dialog, click **Not now** and then click **Next**.

    Windows finishes its setup.

28. Remove the Microsoft Windows 10 Pro DVD and insert the Windows Updates DVD.

29. Navigate to the Windows Tools folder, open the Windows Activation Key.txt file, and copy the text.

30. On the Windows taskbar, in the Ask me anything field, type *Settings*, and press Enter.

31. At the bottom of the Windows Settings window, click the **Activate Windows now** option and then click **Change product key**.

32. When asked if you want the app to make changes, click **Yes**.

33. Paste the activation key text string in the **Product Key** field.

34. On the resulting Activation dialog, click **Next**.

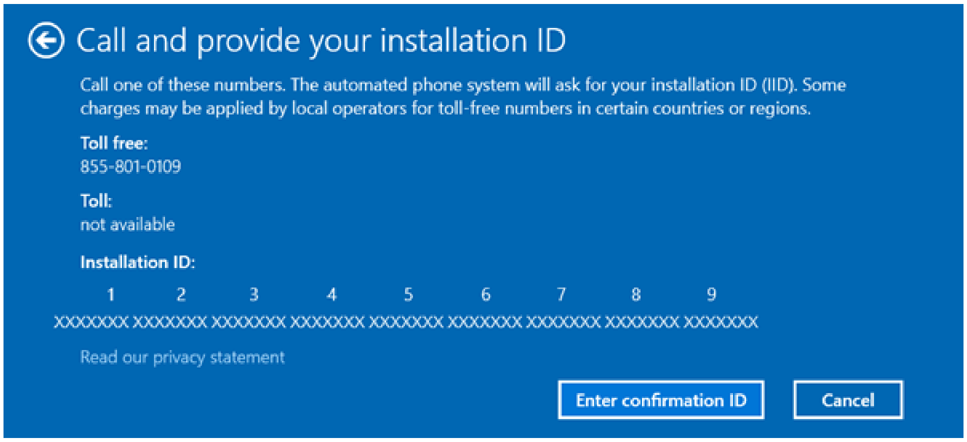
35. When the following dialog displays the message "We couldn't activate Windows," click **Close**.

36. Click the **Start** button on the Windows taskbar and search for and select **Run**.

37. In the Run dialog, type **slui.exe 4** in the **Open** field and click **OK**.

38. On the Select your country or region dialog, select a country from the drop-down list and click **Next**.

    A dialog appears that provides a toll-free telephone number to call for activation (Figure 5-1).



Call and provide your installation ID

Call one of these numbers. The automated phone system will ask for your installation ID (IID). Some charges may be applied by local operators for toll-free numbers in certain countries or regions.

Toll free:
855-801-0109

Toll:
not available

Installation ID:

```
   1       2       3       4       5       6       7       8       9
XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX XXXXXXX
```

Read our privacy statement

Figure 5-1. Call and provide your installation ID

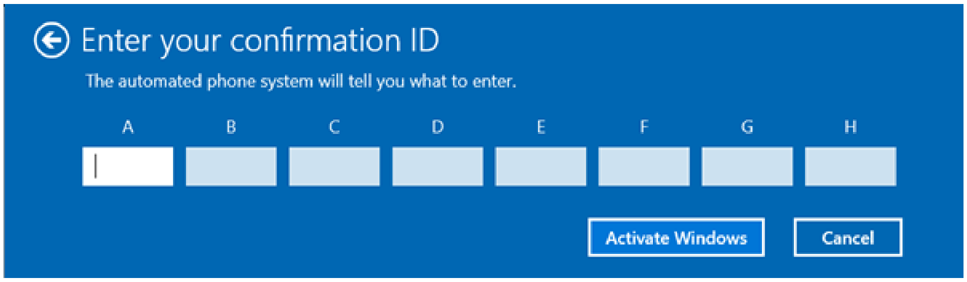
39. Call the activation service and follow the automated prompts.

    Make sure to state that this is not a new installation. Answering in this way sends you to the automated version of the service instead of sending you to a customer-service person.

    When prompted, provide the nine-part installation ID that appears on the dialog to get the Confirmation ID.

    If for any reason you cannot complete the activation using this fully automated service, call the number again and state that this is a new installation. A customer-service person will then help you activate the installation.

40. Click the **Enter confirmation ID** button on the dialog, enter the eight-part confirmation number that the automated activation service provides, and click **Activate Windows** (Figure 5-2).



Enter your confirmation ID

The automated phone system will tell you what to enter.

Figure 5-2. Enter your confirmation ID

41. When a confirmation message indicates that Windows has been activated, click **Close**.

42. To check that the BIOS settings are correct after the installation of Windows is complete, do the following:

    a. Open the Device Manager and select **IDE-ATA/ATAPI controllers**.

    b. Check that the device description contains "AHCI."

    Example: Standard SATA AHCI Controller

5.3 Installing the Windows patch

This topic describes how to patch Windows for some security updates. The patch process requires you to install two files: a service stack update and a Windows update.

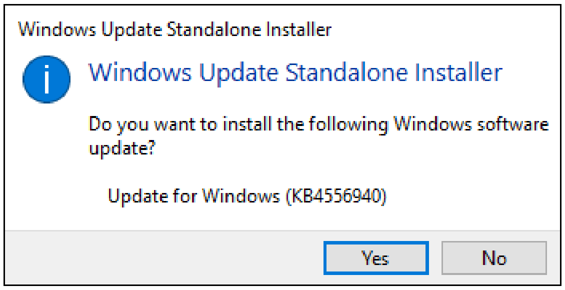
Installing the service stack update

To install the service stack update:

1. Insert the Windows Updates disk and navigate to the Windows Patch directory in File Explorer.

2. Install the Service Stack Update, KB4556940, by double-clicking **Windows10.0-KB4556940-x64.msu**.

   The installation program displays the Windows Update Standalone Installer dialog (Figure 5-3).



Windows Update Standalone Installer

Windows Update Standalone Installer

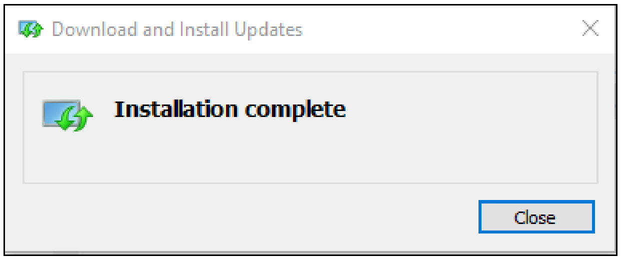
Do you want to install the following Windows software update?

Update for Windows (KB4556940)

Figure 5-3. Windows Update Standalone Installer dialog—Service stack update

3. Click **Yes** in the Windows Update Standalone Installer dialog (Figure 5-3).

   The update takes approximately a minute. When the service stack update is complete, the installation program displays the message shown in Figure 5-4.



Download and Install Updates

Installation complete

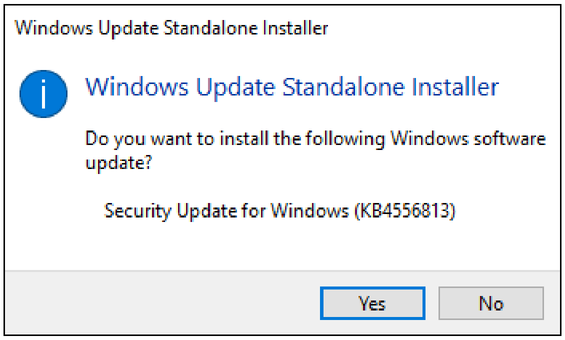
Figure 5-4. Installation Complete message—Service Stack Update

Installing the Windows updates

To install the Windows 10 KB4556813 update:

1. In the Windows Patch directory of the Windows update DVD, double-click the file named **windows10.0-kb4556813-x64_074956aa9f895643ea0768d516375d4a1cd732a2.msu**.

   The installation programs displays the Windows Update Standalone Installer dialog (Figure 5-5).

   Windows Update Standalone Installer

   Windows Update Standalone Installer

   Do you want to install the following Windows software update?

   Security Update for Windows (KB4556813)

   Figure 5-5. Windows Update Standalone Installer dialog—Windows security update

2. Click **Yes** to start the installation.

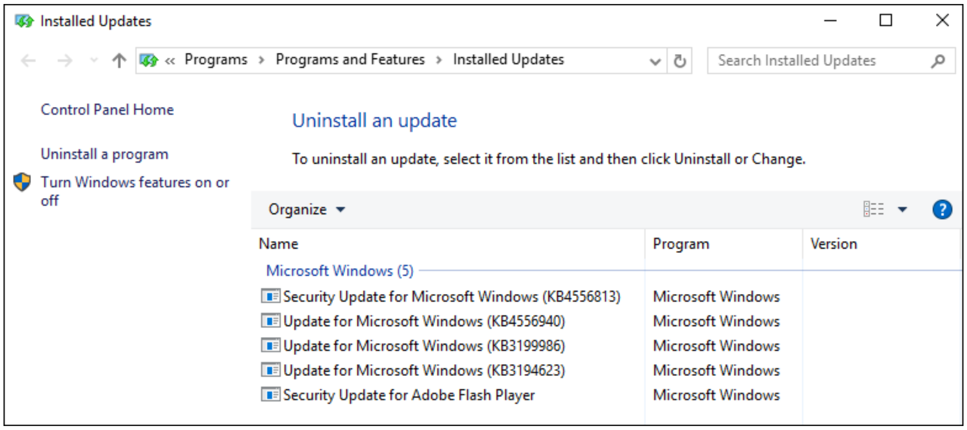
   After you click **Yes** to start the installation, Windows takes approximately 30 minutes to install the software. When prompted to do so, restart your computer.

   After you restart the computer, Windows takes approximately 30 minutes to process the updates.

3. Confirm that you have installed the updates:

   a. Click the **Start** button on the Windows taskbar and search for and select **View installed updates**.

   b. Confirm that KB4556940 and KB4556813 appear in the Installed Updates dialog (Figure 5-6).

   Uninstall an update

   To uninstall an update, select it from the list and then click Uninstall or Change.

Name	Program	Version
Microsoft Windows (5)		
Security Update for Microsoft Windows (KB4556813)	Microsoft Windows	
Update for Microsoft Windows (KB4556940)	Microsoft Windows	
Update for Microsoft Windows (KB3199986)	Microsoft Windows	
Update for Microsoft Windows (KB3194623)	Microsoft Windows	
Security Update for Adobe Flash Player	Microsoft Windows	

   Figure 5-6. Installed Updates dialog

5.4 Installing Windows drivers

Install the following Windows drivers:

- Chipset drivers
- Graphics drivers
- Network drivers

Note: After you install all drivers, restart the computer.

To install the drivers:

1. Log in to the computer as the Windows administrator.
2. Insert the Windows Updates DVD into the disc drive and navigate to the folder applicable to your computer model.
3. Open the Chipset folder, double-click each application file and follow the on-screen prompts to install each driver in the folder.

   After you have installed all the Chipset drivers, select **Restart Later**.

   Do not restart the computer after installing the chipset drivers.
4. Open the Graphics folder for your computer.

   Double-click each application file and follow the on-screen prompts to install each driver in the folder.

   Depending on the model of your computer, you may not be able to install the AMD Graphics driver. In this situation, continue by installing the remaining drivers.

   Do not restart the computer after installing the graphics drivers.
5. If there is a Network drivers folder for your computer, open, double-click each application file, and follow the on-screen prompts to install each of the drivers in the folder.
6. After you have installed all the drivers, restart the computer.

5.5 Turning off BitLocker

When Windows is installed, BitLocker encrypts the drive. Because the mode of encryption does not meet Clear Ballot standards, you must decrypt the drive. After hardening the computer, which sets the encryption mode to FIPS 140-2, you may choose to re-enable BitLocker and encrypt the drive.

To disable BitLocker:

1. Click the Start button on the Windows taskbar, search for and select **Manage BitLocker**.
2. When Windows displays the BitLocker Drive Encryption window, click the option to **Turn on BitLocker** and accept any confirmation dialogs that appear.
3. When Windows displays the recovery key dialog, insert a USB drive into the computer and click **Save to a File**. Navigate to the desired location on the USB drive and click **Save**.
4. Follow the instructions to Activate BitLocker.
5. When BitLocker is activated, in the BitLocker Drive Encryption dialog, click **Turn off BitLocker**. Accept any confirmation dialogs that appear.

   The decryption process takes several minutes. When finished, the status **BitLocker Off** appears in the Bitlocker Drive Encryption dialog.
6. Navigate to the location on the USB drive where you saved the recovery key and delete it.

5.6 Creating a restore point

Creating a restore point before making configuration changes to any CountStation computer enables rolling back to the state that existed before the changes were made.

You can also create intermediate restore points at any time in the process.

To create a restore point:

1. Log in to the CountStation computer as a Windows administrator.
2. From the task bar, type *restore* in the Search field and select **Create a restore point** from the search results. The System Properties dialog appears.
3. (If necessary) Click the **System Protection** tab.
4. Select the **OS (C:) (System)** available drive option and click **Configure**. The System Protection for OS (C:) appears.
5. Select the **Turn on system protection** option, click **Apply** and then click **OK**.
6. On the System Protection tab, click **Create**. The System Protection dialog appears.
7. Enter a descriptive name for the restore point using the following format:

   *yyyy-mm-dd-hh-mm*_Before_Clear_Ballot_configuration
8. Click **Create**. The restore point is created in a minute or two and the System Protection message box displays the message: *The restore point was created successfully*.

9. Click **Close** to dismiss the message.
10. Click **OK** to close the System Properties dialog.

5.7 Setting Windows passwords

Administrative users must have a nondefault password. Scanner operators are required to have a password that is not the Windows default. All passwords are subject to Windows complexity requirements.

Before assigning passwords to individuals, give consideration to who has the administrator password and which people have a scanner operator password.

5.7.1 Configuring the Windows password policy

To configure the password policy on Windows computers:

1. Log in to the computer as the Windows administrator.
2. Click the Start button on the Windows taskbar and search for and select **Edit group policy**.

   Windows display the Group Policy editor
3. In the navigation pane, select **Computer Configuration> Windows Settings> Security Settings> Account Policies**.
4. Double-click the **Password Policy** option on the right.
5. In the Password Policies options, double-click **Minimum Password Length**.
6. Set the length to 8 characters and click **OK**.
7. In the Policy options, double-click **Password must meet complexity requirements**.
8. Set to **Enabled** and click **OK**.
9. Close the Group Policy Editor.

Complexity requirements are enforced when passwords are changed or created. If the **Password must meet complexity requirements** option is checked, passwords must meet the following minimum requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Be at least six characters in length.
- Contain characters from three of the following four categories:
  - Latin uppercase characters (A through Z)
  - Latin lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Nonalphanumeric characters (for example, !, $, #, %)

5.7.2 Changing the Windows administrator password

Note: *Never* allow anyone who is not an administrator to learn the Windows administrator password.

To change the administrator password:

1. Log in to the computer as the default Windows administrator.
2. Click the Start button on the Windows taskbar and search for and select **Settings**.
3. Select **Accounts**.

   Windows displays the Your info page.
4. Select **Sign-in Options**.

   Windows displays the Sign-in Options page.
5. Under **Password**, click **Change**.
6. On the next page, enter the current (default) password and click **Next**.
7. On the next page, enter and reenter the new password, enter the password hint and click **Next**.

   The new password must meet the complexity requirements that you established in the previous section "Configuring the Windows password policy."
8. On the next page, click **Finish**.
9. Log out of Windows and log back in with the new password.

Record the Windows administrator password on the Installation checklist (page 124).

5.8 Assigning static IP addresses

Follow the steps below to assign static IP addresses to the CountStation computers. To ensure accuracy, check with your IT administrator before changing any settings.

To assign a static IP address:

1. Log in to the CountStation as a Windows administrator.
2. From the task bar, type *control* in the Search field and then select **Control Panel** from the search results.
3. Click **Network and Internet**, then click **Network and Sharing Center**, and then click **Change adapter settings** on the left.
4. Right-click the available **Ethernet** adapter and select the **Properties** option to open the Ethernet Properties dialog.
5. Deselect the **Internet Protocol Version 6 (TCP/IPv6)** item.
6. Double-click the **Internet Protocol Version 4 (TCP/IPv4)** option.

7. Select the **Use the following IP address** option and enter an IP address in the IP address field that conforms to your IP schema (such as, within the range of 192.168.15.2 to 192.168.15.249).

8. Click the **Subnet mask** field to automatically populate it.

9. In the Default Gateway field, enter the gateway's IP address (such as, 192.168.15.1) and then enter that same address in the Preferred DNS server field.

10. Click **OK** and close all open dialogs.

11. From the task bar, enter *command* in the Search field and then select **Command Prompt** from the search results.

12. Verify the IP addresses by typing *ipconfig* in the Command Prompt window and pressing the Enter key. Close the Command Prompt window.

13. Repeat this process for each CountStation.

5.9 Mapping the CountStation computer to the CountServer computer

All of the ClearCount software resides on the CountServer computer. Each CountStation computer must connect to the CountServer computer through the network switch to manage elections, manage users, and view election reports.

To map a CountStation:

1. Log in to the computer as the Windows administrator.

2. Click the Start button on the Windows taskbar and search for and select **File Explorer**.

3. When Windows displays the search results, click **File Explorer**.

   Windows displays File Explorer with the Computer tab selected.

4. In File Explorer, do the following (Figure 5-7):

   a. Click the **This PC** option on the left.

   b. Click the Map Network Drive icon in the toolbar at the top of the screen.

      If the toolbar with the Map Network Drive option is not visible, drop it down by using the small down arrow on the right side at the top of the File Explorer dialog.

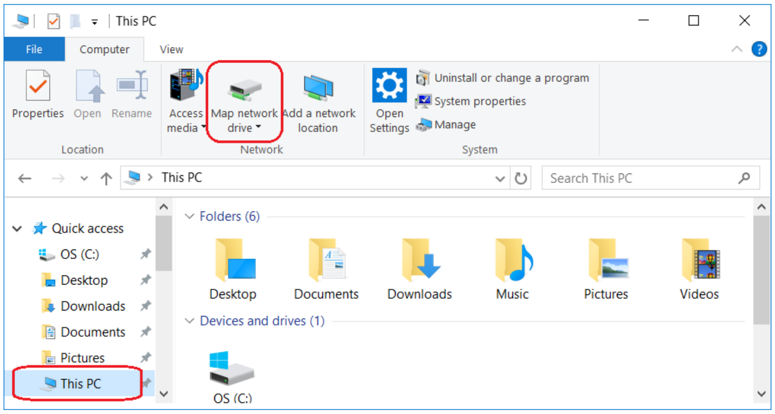


Figure 5-7. File Explorer: This PC and Map Network Drive enclosed in red

5. In the Map Network Drive dialog, do the following (5.9):

   a. Select the P: drive from the Drive drop-down list.

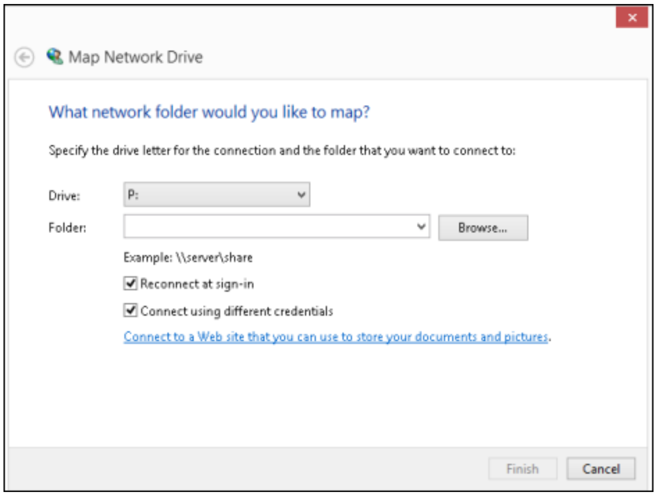
   b. In the Folder field, enter the IP address of the CountServer in the following format:

      \\CountServerIPAddress\client

      Example: \192.168.15.250\client

   c. Select (check) **Reconnect at sign-in** and **Connect using different credentials** if they are not already selected.

   d. Click **Finish**.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: P:

Folder:

Browse...

Example: \\server\share

☑ Reconnect at sign-in

☑ Connect using different credentials

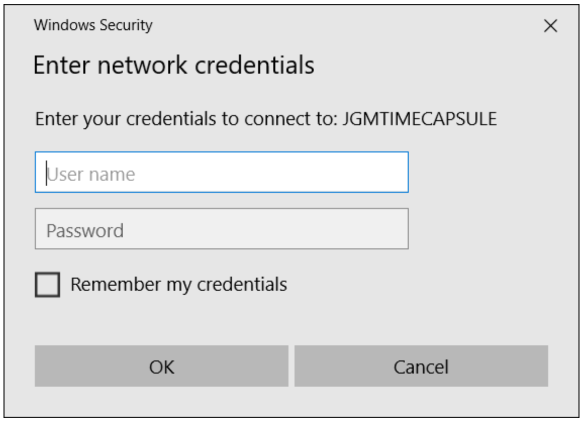
Connect to a Web site that you can use to store your documents and pictures.

Finish Cancel

Figure 5-8. Map network drive dialog

6. When the Enter network credentials dialog appears, enter the user name and password for the ClearCount primary administrator account that you created during installation and click **OK** (Figure 5-9).

   Do not select the **Remember my credentials option**.



Windows Security

Enter network credentials

Enter your credentials to connect to: JGMTIMECAPSULE

Figure 5-9. Enter Network Drive

5.10 Creating a desktop shortcut to the P: drive

For convenience, you can create a desktop shortcut to the P: drive, which contains the DeleteBox utility and StartUploader.

This drive also contains some system files that must *not* be opened except under the direction of Clear Ballot Technical Support.

To create a shortcut to the P: drive:

1. Log in to the CountStation computer as the Windows administrator.
2. Click the Start button on the Windows taskbar and search for and select **File Explorer**.
3. Locate the P: drive and drag it to your desktop.

5.11 Installing a browser

To access ClearCount election reports and administrative pages, you must install Google Chrome on the CountStations.

Because the computers used in an election must *never* be connected to the Internet, you must install the offline browser versions supplied by Clear Ballot.

To install a browser on a CountStation:

1. Insert the ClearVote Tools DVD into the disc drive of the CountStation.
2. Navigate to **Browsers > Offline Chrome Installer** and double-click the application file.
3. If you have more than one CountStation, repeat the installation process on each computer.

5.11.1 Installing browser certificates

When using the HTTPS protocol to access the CountServer computer, you receive a digital certificate warning about an untrusted site. This is because ClearVote products use self-signed certificates. This is perfectly safe in the kind of closed network environment that the ClearCount system uses, but a warning message appears when accessing the CountServer computer until you install the certificate on the CountStation computer.

5.11.2 Installing the browser certificate for Google Chrome

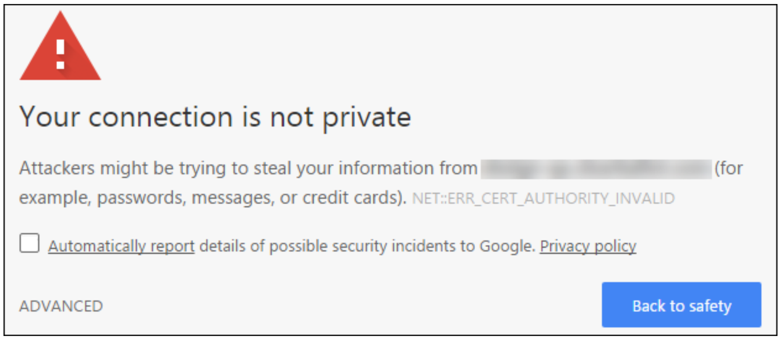
The Google Chrome certificate installation process consists of exporting and importing.

Exporting

To export the browser certificate for Google Chrome:

1. Log in to a CountStation computer, open Google Chrome, and navigate to https://<*servername*>.

   The installation program displays the screen shown in Figure 5-10.



Your connection is not private

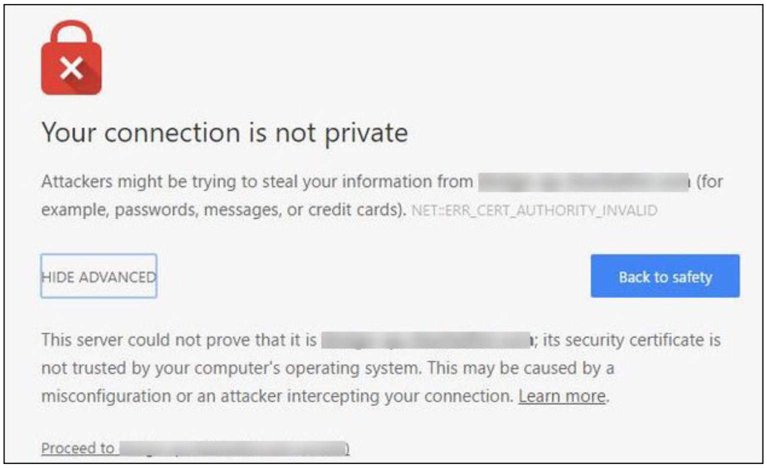
Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

Figure 5-10. Connection not private—Screen 1

2. Click the **Advanced** link that appears on the alert.

   The installation program displays the screen shown in Figure 5-11.



Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is [redacted]; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

Proceed to [redacted]

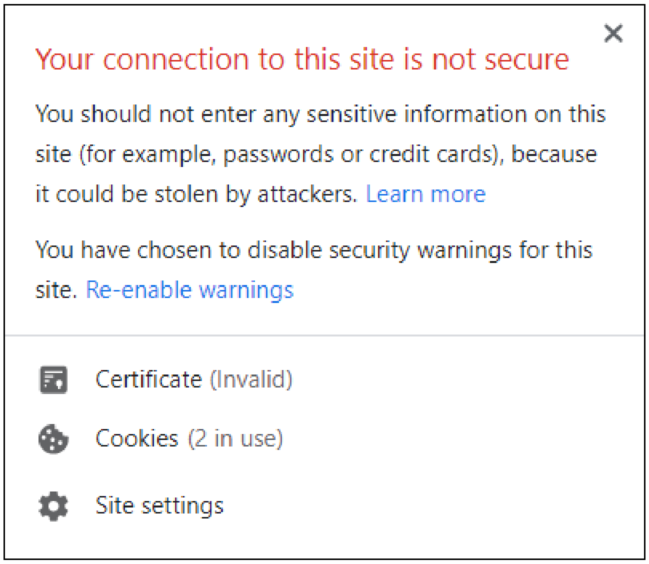
Figure 5-11. Connection not private—Screen 2

3. Click **Proceed to *<servername>* (unsafe)**.

   Google Chrome allows you to access the site, but the address bar shows a red line through the HTTPS because the site is not yet validated.

4. In the browser's address bar, click the red triangle containing the exclamation point.

   Google Chrome displays the window shown in Figure 5-12.



Your connection to this site is not secure

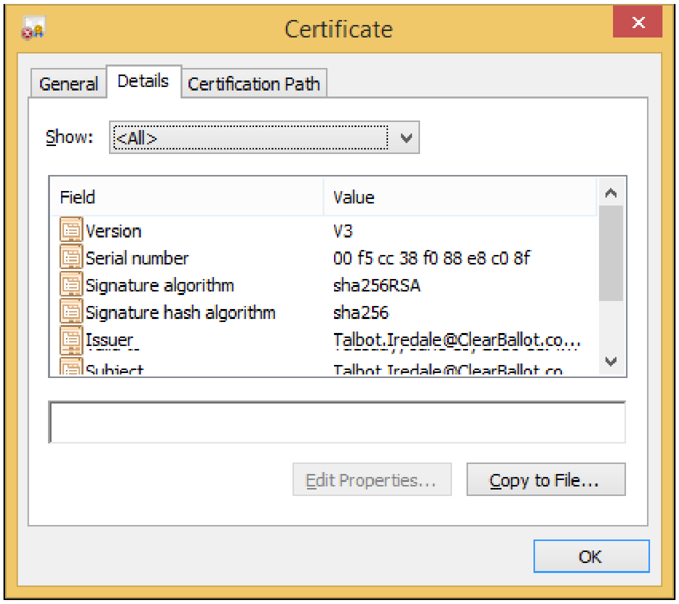
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

Figure 5-12. Your connection to this site is not secure

5. Click the **Certificate (Invalid)** link.

6. When the Certificate window appears, click the **Details** tab and then click the **Copy to File** button (Figure 5-13).

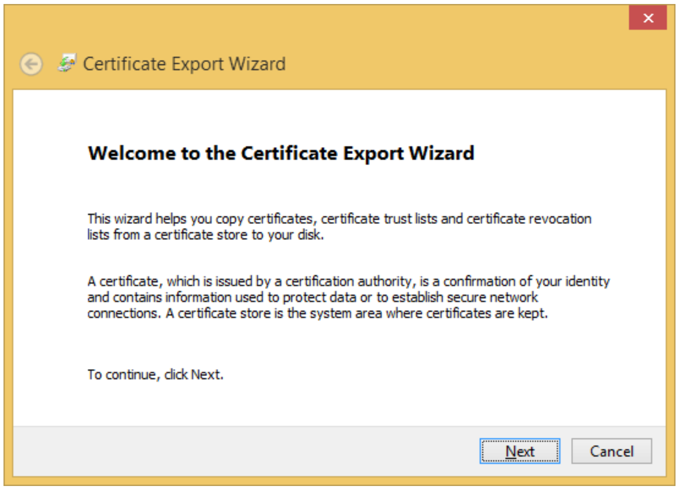


Show: <All>

Field	Value
Version	V3
Serial number	00 f5 cc 38 f0 88 e8 c0 8f
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Talbot.Iredale@ClearBallot.co...
Subject	Talbot.Iredale@ClearBallot.co

Figure 5-13. Certificate window

7. When the Welcome to the Certificate Export Wizard appears, click the **Next** button (Figure 5-14).



Welcome to the Certificate Export Wizard

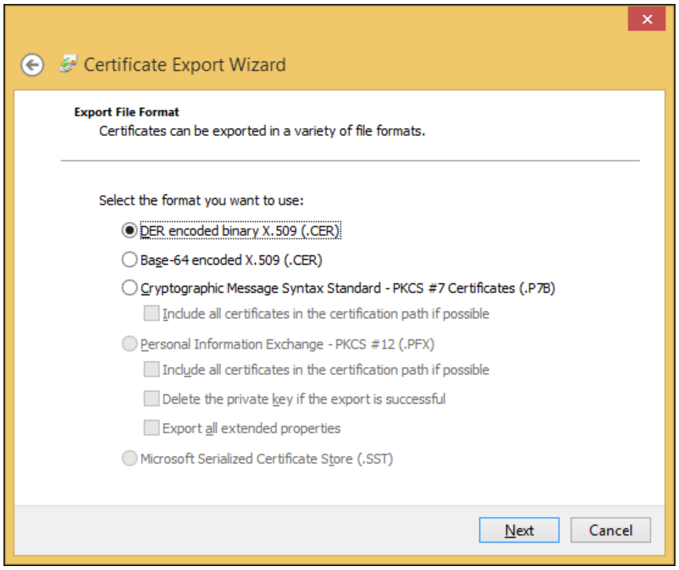
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 5-14. Welcome to the Certificate Export Wizard

8. On the Export File Format screen, select the **DER encoded binary X.509 (.CER)** option and click the **Next** button (Figure 5-15).



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

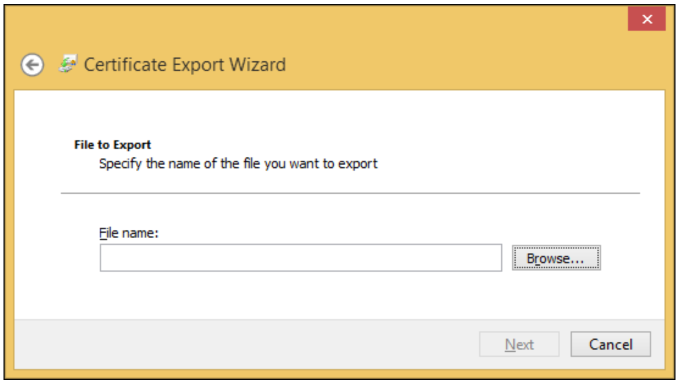
- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
- ○ Microsoft Serialized Certificate Store (.SST)

Figure 5-15. Export File Format screen

9. On the File to Export screen, click the **Browse** button to choose where to save the certificate and enter the name of the file (Figure 5-16).

   Example: chrome-cert.cer

   Clear Ballot recommends storing the certificate in your Documents folder, but you can store it any location. Record where you save the certificate on the Installation checklist (page 124).

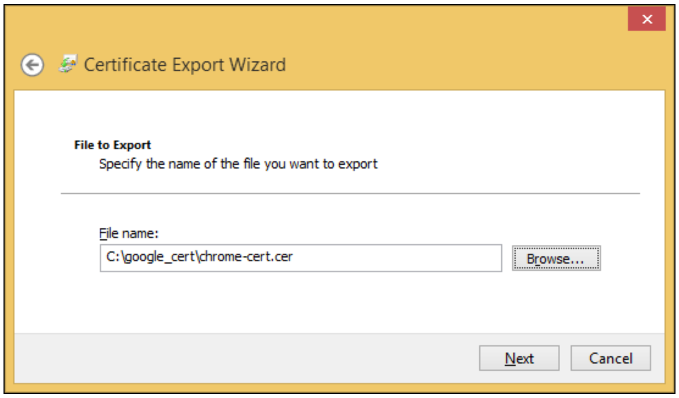


File to Export
Specify the name of the file you want to export

File name:

Figure 5-16. File to Export screen before filling in the File name field

10. After browsing to the location for saving the certificate, click the Next button (Figure 5-17).

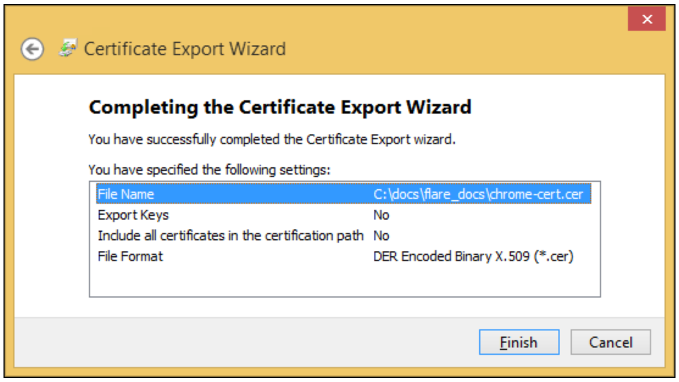


File to Export
Specify the name of the file you want to export

File name: C:\google_cert\chrome-cert.cer

Figure 5-17. File to export screen after selecting where to save the certificate

11. When the Completing the Export window appears, click the **Finish** button.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\docs\flare_docs\chrome-cert.cer
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

Figure 5-18. Completing the Export Wizard

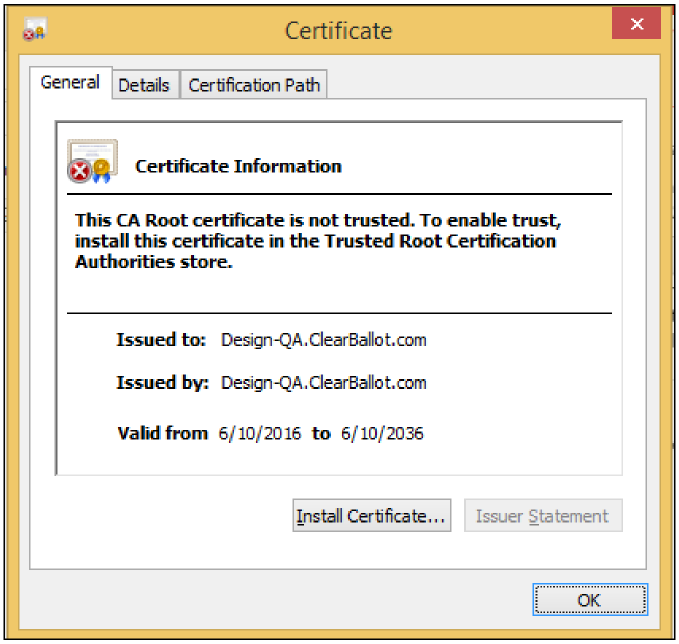
Google Chrome displays a confirmation message to indicate that installation of the certificate was successful. Click **OK** to close the message and click **OK** to close the certificate window.

Importing the certificate

Follow these steps to import the certificate:

1. Navigate to the location where you saved the certificate and double-click its filename.

   The Certificate window appears (Figure 5-19).



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Design-QA.ClearBallot.com

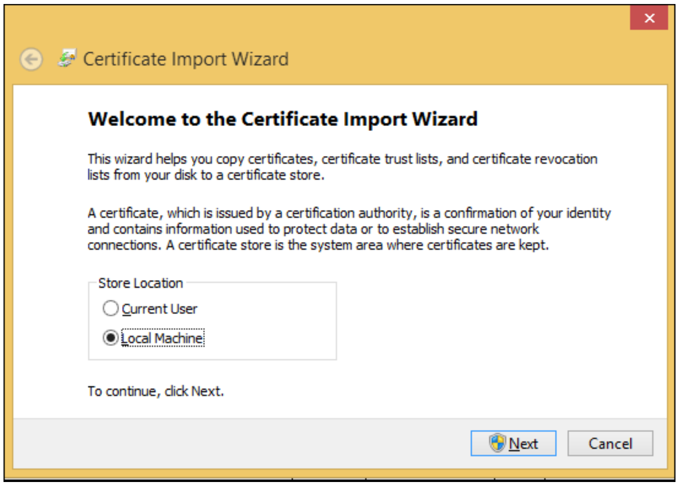
Issued by: Design-QA.ClearBallot.com

Valid from 6/10/2016 to 6/10/2036

Figure 5-19. Certificate window

2. In the Certificate window, click the **Install Certificate** button (Figure 5-19).

3. When the Welcome to the Certificate Import Wizard window appears, select **Local Machine** and click the **Next** button (Figure 5-20).



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

○ Current User

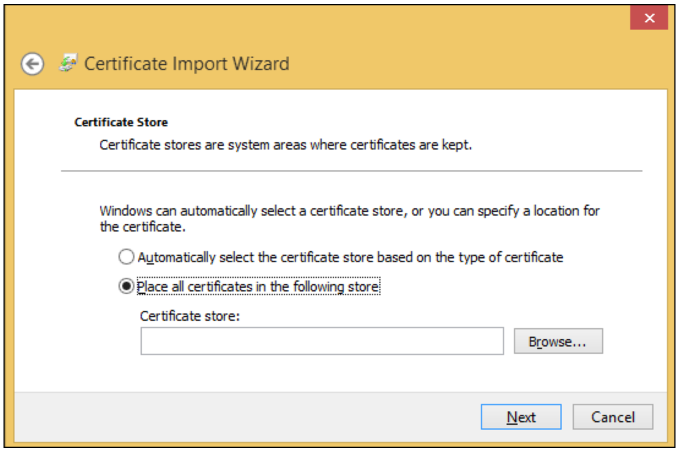
● Local Machine

To continue, click Next.

Figure 5-20. Welcome to the Certificate Import Wizard window

4. When a message asks if you want to allow the program to make changes to the computer, click **Yes**.

5. When the Certificate Store window appears, select **Place all certificates in the following store** and then click the **Browse** button (Figure 5-21).



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

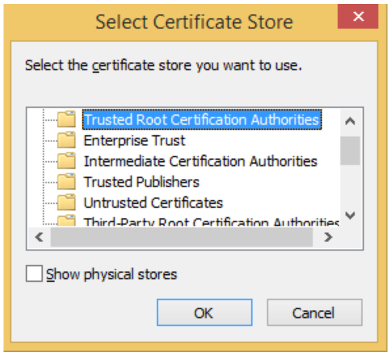
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Figure 5-21. Certificate Store window

6. When the Select Certificate Store window appears, select **Trusted Root Certificate Authorities** and click **OK** (Figure 5-22).



Select Certificate Store

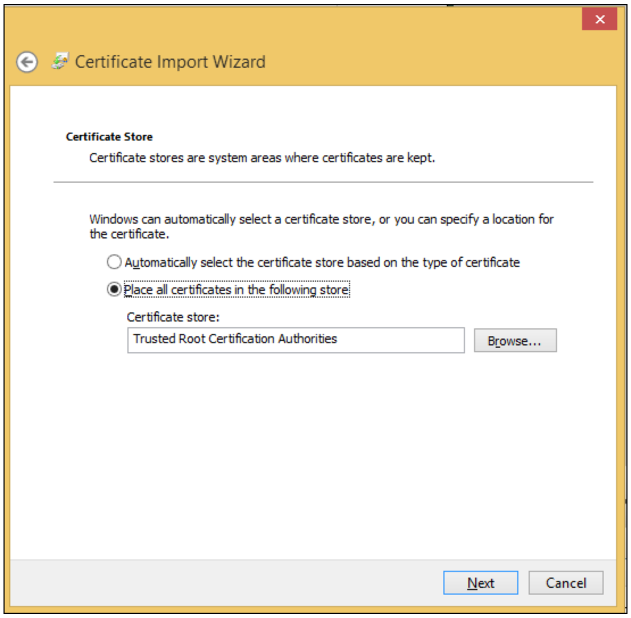
Select the certificate store you want to use.

- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities

□ Show physical stores

Figure 5-22. Select Certificate Store window

7. When the Certification Store window appears, click the **Next** button (Figure 5-23).



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

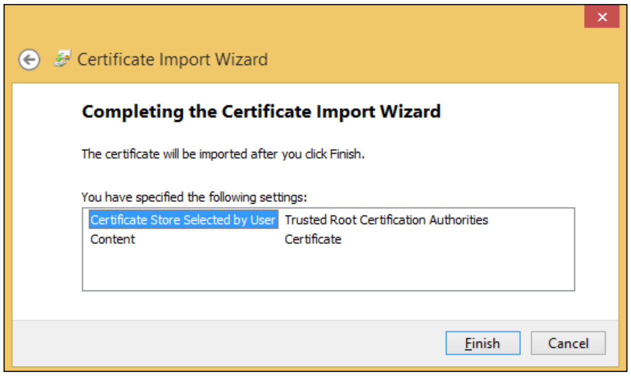
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

Figure 5-23. Certificate Store window

8. When the Completing the Certificate Import Wizard window appears, click the **Finish** button.



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Figure 5-24. Completing the Certificate Import Wizard

A confirmation message appears.

9. Restart Google Chrome and navigate back to https://<*servername*>.

You no longer receive the warning, and HTTPS no longer has a red line through it.

5.11.3 Removing a previous version of a browser certificate in Google Chrome

When the CountServer browser certificate is within 60 days of expiration, a message appears on the login screen. See "Regenerating a digital certificate" on page 42.

After the administrator has generated a new certificate, follow these directions to remove the previous version of a browser certificate in Google Chrome.

1. Start the certificate manager.
   a. Hold the Windows key and press R.
   b. Type **certmgr.msc** and press **Enter**.
2. When the Cert manager opens, expand **Trusted Root Certification Authorities**.
3. Select **Certificates**.
4. Find the desired certificate, which is named after the CountServer host name.
5. Right-click the certificate and select **Delete**.
6. Confirm the deletion.

After removing the old browser certificate, follow the instructions in "Installing browser certificates" on page 99.

5.12 Creating a restore point

Creating a restore point before making configuration changes to any CountStation computer enables rolling back to the state that existed before the changes were made.

You can also create intermediate restore points at any time in the process.

To create a restore point:

1. Log in to the CountStation as a Windows administrator.
2. From the task bar, type *restore* in the Search field and select **Create a restore point** from the search results.

   Windows displays the System Properties dialog.
3. (If necessary) Click the **System Protection** tab.
4. Click **Create**. The System Protection dialog appears.
5. Enter a descriptive name for the restore point using the following format:

   *yyyy-mm-dd-hh-mm*_Before_Clear_Ballot_configuration
6. Click **Create**.

   Windows creates the restore point in a minute or two, and the System Protection message box displays the message:

   The restore point was created successfully.

7. Click **Close** to dismiss the message.

8. Click **OK** to close the System Properties dialog.

5.13 Hardening the CountStation computers

Hardening the CountStations in the ClearCount system consists of minimizing routes of access to them and implementing malware protections.

Hardening includes procedural and environmental elements that may be governed by jurisdictional statute. Follow all steps to harden your system. No steps are recommended or optional. Be sure to consult jurisdictional regulations as part of the hardening process. Jurisdictional voting system security regulations may dictate that you do more than described in this section.

5.13.1 Updating Microsoft Defender Antivirus

Microsoft provides the Microsoft Defender Antivirus program (also called Windows Defender) with its Windows operating system. To keep the virus definitions up to date, you must update the program. Clear Ballot recommends that the Microsoft Defender Antivirus program be updated on every ScanStation computer and CountStation computer when the following events occur:

- When the system is first installed and configured
- Before each election

Because computers used in elections must *never* be connected to the Internet, the virus definition update must be performed offline using removable media.

To download antivirus definitions:

1. On a computer outside the closed ClearCount network that has a USB port and Internet connection, navigate to https://www.microsoft.com/security/portal/definitions/adl.aspx.

2. Insert a USB drive in the USB port and download the antivirus definitions to the USB drive according to the instructions on that site for your operating system and bit version.

   The software is delivered as a single file named *mpam-fe.exe* or something similar.

3. Eject the USB drive and then remove it from the computer where you downloaded the antivirus definitions.

If Windows software restriction policies are in effect on the computer being updated, disable the restrictions or add a temporary path rule to allow the update to run.

To update Microsoft antivirus software offline:

1. Log in to the computer as the Windows administrator.

2. Insert the USB drive into a USB port on the computer and browse to the file.

3. Right-click the file and select the **Run as Administrator** option from the pop-up menu.

4. When the User Account Control dialog appears, click **Yes** to run the update. You may see the mouse pointer spinning as the update progresses. If not, wait 30 seconds.

5. From the task bar, type *settings* in the Search field and then select **Settings** from the search results.

   The Windows Settings page appears.

6. Click **Update & security**.

7. Select **Windows Defender** on the left and then click **Open Windows Defender**.

   The Windows Defender dialog opens.

8. Click the **Update** tab and check the date and time that the definitions were created. The date should be the date you downloaded the file.

9. Close the Windows Defender dialog.

Maintain the history and archive copies of each update.

5.13.2 Hardening the CountStation computer

Hardening the ClearCount system makes it more secure from threats. The CountStations hardening script performs several critical procedures on the computer, including the following:

- Enables FIPS 140-2 security mode
- Disables the wireless and Bluetooth Internet services
- Disables the autoplay feature
- Disables Cortana
- Disables Microsoft consumer experiences
- Enables the software execution control for non-administrator accounts and only allows the programs that are in the Windows system32 directory to run, along with Google Chrome
- Disables Google Chrome updates

To run the hardening script:

1. Log in to the computer as an administrator.

2. Insert the ClearVote Tools DVD into the disc drive and navigate to the Hardening Scripts folder.

3. Copy the AdminStation Harden folder to the CountStation computer's desktop.

4. Open the AdminStation Harden folder, right-click the harden.bat file and select **Run as administrator** from the pop-up menu.

5. When the script finishes, restart the computer.

   You must restart the computer for the changes to take effect.

6. Delete the AdminStation Harden folder from the desktop and empty the recycle bin.

5.13.3 Restricting access to the BIOS

Access to the BIOS is restricted by implementing an administrator password. The behavior of the BIOS depends upon the computer make and model. Consult your computer's documentation or contact Clear Ballot Technical Support for details.

The following procedure for a Dell Latitude 5590 computer is an example.

To restrict access to the BIOS:

1. Press the Shift key while shutting down the computer. The computer shuts down.

2. Press the F2 key while starting up the computer. The BIOS manager appears.

3. Set the BIOS password:

   All user names and passwords must satisfy the rules and guidelines provided in "Login credential rules and guidelines" on page 121.

   a. Using the arrow keys, navigate to the Security screen and select **Admin Password**.

   b. Enter and confirm the password.

   c. Record the BIOS password on the Installation checklist (page 124).

4. To save your changes, click **Apply** and then click **Exit**.

5. Restart the computer and verify that the changes have been implemented.

5.14 Enabling BitLocker (optional)

When Windows is installed, BitLocker encrypts the drive. Because the mode of encryption does not meet Clear Ballot standards, you must decrypt the drive. After hardening the computer, which sets the encryption mode to FIPS 140-2, you may choose to re-enable BitLocker and encrypt the drive.

To enable BitLocker:

1. Click the Start button on the Windows taskbar, search for and select **Manage BitLocker**.

2. When Windows displays the BitLocker Drive Encryption window, click the option to **Turn on BitLocker** and accept any confirmation dialogs that appear.

3. When Windows displays the recovery key dialog, insert a USB drive into the computer and click **Save to a File**. Navigate to the desired location on the USB drive and click **Save**.

   > **Note**: Store this file in a secure location so that it is available for future use.

4. On the How do you want to back up your recovery key dialog, click **Next**.
5. When Windows displays the Choose how much of your drive to encrypt dialog, select **Encrypt used disk space only (faster and best for new PCs and drives)** and click **Next**.
6. When Windows displays the Choose which encryption mode to use dialog, select **New encryption mode (best for fixed drives on this device)** and click **Next**.
7. When Windows displays the Are you ready to encrypt this drive dialog, check the **Run BitLocker system check** box and click **Continue**.
8. In the dialog that appears, click **Restart Now**.

   Windows restarts.

Chapter 6. Validating and securing the system

After the computers used in the ClearCount system are installed, configured, and hardened, you need to take the following steps to validate and secure the system.

6.1 Validating software setup

The jurisdiction must validate that the system setup occurred properly, that no files were corrupted, and that no unapproved files are present on the system following an installation. If any issue is identified during the software setup validation process, the entire system must be reinstalled to ensure the jurisdiction is working with a certified system.

6.1.1 Obtaining the list of all software files present on the system

Clear Ballot provides a list of all approved files present on a CountServer in the documentation provided to the election authority for your jurisdiction. This list includes SHA-256 file digests for each file on the system.

To access the list of all files on the system:

1. At a CountStation, log in as an administrator.
2. From the Election Index page, click the login drop-down menu next to your user name and select **About this software**.

   The system displays the About this software page.

   The About this software page contains three tabs:

   - The Server Information tab provides information about the CountServer computer and the ClearCount software.
   - The Clear Ballot Product Files tab lists the files in the ClearCount software.
   - The Installed System Packages tab lists the third-party packages included with the ClearCount software.
3. Click the **Copy** button to copy the contents of the Clear Ballot Product Files tab, paste it into a text editor, such as Notepad, and save it to a USB drive.
4. Repeat the process to obtain the contents of the Installed System Packages tab.
5. Use a third-party tool to compare the official printed version of the *ClearCount System Identification Guide* to the copied contents of the installed version of the ClearCount software. If the two lists do not match, the system must be reinstalled. Also, if any of the file digests do not match, the system must be reinstalled.
   If mismatches persist between the list from your state and the software list, notify your state election authority and Clear Ballot before continuing to use the system.

6.1.2 Initial register and variable validation

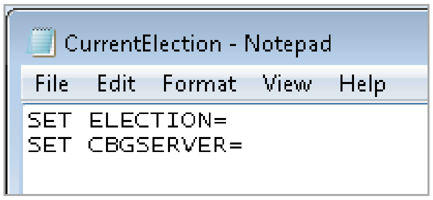
The CurrentElection.bat file contains the initial register and variable values for the ClearCount system. This file is located on the P: drive, which you mapped to the ScanStation computers and CountStation computers as part of the initial setup.

This file contains the values that are used to set the ELECTION and CBGSERVER values in the system. Initially, both of these values should be empty.

After the first election has been created on a system (or after an election has been set to Active following a restore), the ELECTION variable assumes the name of the active election, and the CBGSERVER variable assumes the name of the CountServer computer.

To verify that the values in CurrentElection.bat are empty:

1. Navigate to the P: drive.
2. Right-click the CurrentElection.bat file and select **Edit**.
3. Verify that the values in the file are empty, and then close the file.



```
SET ELECTION=
SET CBGSERVER=
```

Figure 6-1. CurrentElection.bat

6.2 Hardening the network switch

For enhanced security, the network switch can be configured to limit access to only the specific ClearCount system components by using their machine access code (MAC) addresses. This method authorizes a specific device to use a specific port on the network switch. When the ports are locked in this manner, other devices are not allowed access.

Clear Ballot recommends the following procedure to harden the Cisco SG250 switch for the ClearCount system. Consult the manufacturer's documentation when hardening other switches.

To harden the network switch:

1. Ensure that your ClearCount system components are set up, powered on, and connected to the network switch as desired.
2. Label each port on the network switch with its applicable connected device (such as, CountServer, ScanStation1, ScanStation2, CountStation).
3. Log in to a CountStation, open a browser and navigate to 192.168.15.1 in the URL address field.

4. Enter the user name and password that you created when you set up the switch. (See "Installing the network switch" on page 55.)

5. Select **Security> Port Security**. A list of the ports on the network switch appears.

6. Select the first interface and click the **Edit** button. The Edit Port Security Interface Setting dialog opens.

7. Select the **Interface Status Lock** option, and then click **Apply** and **Close** to apply the lock setting and close the dialog.

8. Select the first interface again and click the **Copy Settings** button. The Copy Settings dialog opens.

9. Type *2–n*, where *n* is the number of ports on the network switch (such as, 8), and then click **Apply** and **Close** to apply the lock to all of the other ports and close the dialog.

10. Click the **Save** button at the top of the page.

Access for each port is limited to the specific device connected to that port. If you need to change a device, you must unlock its designated port, connect the new device, and lock the port.

To change or add a device:

1. Log in to a CountStation, open a browser and navigate to 192.168.15.1 in the URL address field.

2. Enter the user name and password that you created when you set up the switch. (See "Installing the network switch" on page 55.)

3. Select **Security > Port Security**. A list of the ports on the network switch appears.

4. Select the desired port and click the **Edit** button. The Edit Port Security Interface Setting dialog opens.

5. Deselect the **Interface Status Lock** option, and then click **Apply** to unlock the port.

6. Connect the new device to the unlocked port, power it on, and wait for it to connect to the network.

7. Select the **Interface Status Lock** option, and then click **Apply** and **Close** to apply the lock setting and close the dialog.

8. Click the **Save** button at the top of the page.

To view the device MAC addresses and their respective ports:

1. Select **MAC Address Table> Static Addresses** to display the list.
2. If an unauthorized device appears in the list, select its checkbox and click the **Delete** button.

> **Note**: Never delete all devices as this requires the network switch to be reset and completely reconfigured.

6.3 Monitoring the Windows Event Log

The Windows operating system tracks application, hardware, security, system, and other events in the Windows Event Log. Attempts to access restricted or unapproved processes on the ScanStation computers or the CountStation computers are logged in the Windows Event Log.

You can use the Windows Event Viewer to monitor the logging of all activities taking place on the Windows computers used in the ClearCount system.

To access the Event Viewer, type *event* in the Search field on the task bar and select **Event Viewer** from the search results.

The Windows Event Log must *not* be disabled. The ClearCount system performs a check to ensure the Windows Event Log has not been disabled every time the Tabulator application runs. If the Windows Event Log is not enabled, a fatal error message is issued at the Tabulator application's startup.

For details about using the Windows Event Viewer, consult the Event Viewer help system, or access online information from Microsoft at https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/event-error-codes?view=o365-worldwide.

6.4 Viewing network connection and disconnection events

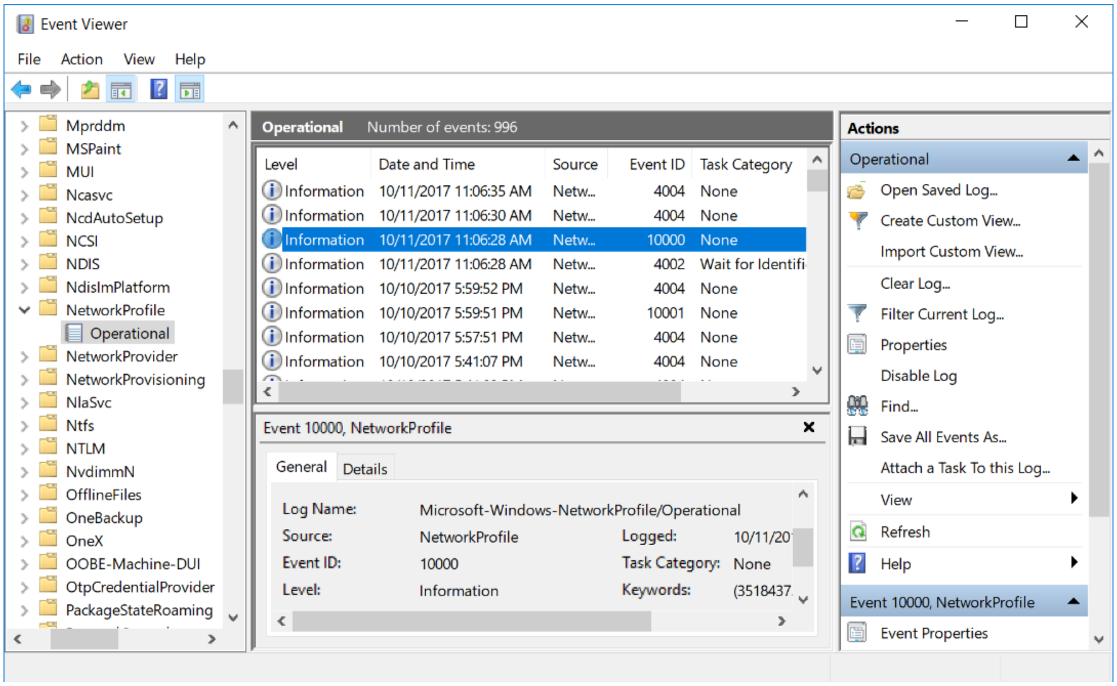
Microsoft Windows logs all network connections and disconnections so you can audit network activity.

To audit network events:

1. Log in to the ScanStation computer or the CountStation computer as a Windows administrator.

2. Click the Start button on the Windows taskbar and search for and select **Event Viewer**.

   Window displays the Event Viewer



Level	Date and Time	Source	Event ID	Task Category
Information	10/11/2017 11:06:35 AM	Netw...	4004	None
Information	10/11/2017 11:06:30 AM	Netw...	4004	None
Information	10/11/2017 11:06:28 AM	Netw...	10000	None
Information	10/11/2017 11:06:28 AM	Netw...	4002	Wait for Identifi
Information	10/10/2017 5:59:52 PM	Netw...	4004	None
Information	10/10/2017 5:59:51 PM	Netw...	10001	None
Information	10/10/2017 5:57:51 PM	Netw...	4004	None
Information	10/10/2017 5:41:07 PM	Netw...	4004	None

Log Name: Microsoft-Windows-NetworkProfile/Operational
Source: NetworkProfile Logged: 10/11/20
Event ID: 10000 Task Category: None
Level: Information Keywords: (3518437

Figure 6-2. Event Viewer

3. In the left pane, select **Applications and Services Logs** > **Microsoft> Windows > Network Profile > Operational**. All network connections and disconnections are displayed. (Double-click any event to view its details.) The display order is: Level, Date and Time, Source, Event ID, and Task Category. The important items are Date and Time, and Event ID. Relevant values for Event ID include:

   - 10000—Indicates a connection to the network.
   - 10001—Indicates a disconnection from the network.

6.5 Location security

Maintaining physical security of the ClearCount system is an important part of its operation and maintenance. When the components of the ClearCount system are not in use, they must be stored in a locked area under the custody and control of the jurisdiction. Access to this area must be controlled by the jurisdiction so the system cannot be accessed by unauthorized individuals, and so that any breaches in security can be recognized through the auditing functions of the system.

When in storage or in use, the ClearCount system must be kept within a controlled area where only individuals authorized by the jurisdiction to handle and process ballots, or to maintain the voting system, can come into direct contact with the ballots or components of the system.

Each jurisdiction must also follow all jurisdictional and state rules for the handling and processing of ballots in addition to this Clear Ballot procedure. This means that at least one security method is employed to provide deterrence and physical security:

- Receptionists or guards with a gate or other barrier to the scanning area
- Electronic door-locking mechanisms such as ID cards or key fobs that record the identity of the device used to unlock the door
- Security cameras
- A locking computer rack or other cabinet to contain components of the ClearCount system

The CountServer computer, attached network switch, and all data cable connections in the ClearCount system are especially security-sensitive. When in use, segregate and enforce enhanced security over the CountServer computer, the ClearCount network switch, and the Ethernet cable connections to the ScanStation computers and the CountStation computers on that closed network. Place the CountServer computer and network switch in a locked computer rack or an adjacent secure area away from the scanning operators to maintain a proper system security posture for the ClearCount system. Use cable locks or tamper-evident seals to provide an enhanced level of security for the cable connections within the system.

The following is a simplified view of the application of a tamper-evident seal to cable connections. Use tamper-evident tape to implement a seal that deters tampering and provides evidence of any manipulation of Ethernet connections. Apply the tape as shown, taking care to bridge the computer body and the Ethernet cable. (The tape can also be applied to the underside of the computer.) Ensure every portion of the length of the seal is pressed against the computer body, cable connector, or the cable itself for best tamper evidence.

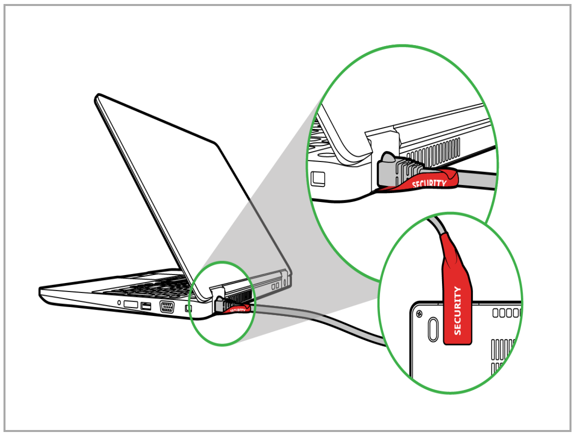


Figure 6-3. Tamper-evident seal applied to Ethernet cable connection

At no point can any unauthorized hardware be connected to the system. Tamper-evident seals or port locks/blockers can be applied to the USB and Ethernet ports on the CountServer, the ScanStation and the CountStation computers to deter unauthorized connections and access. Also apply tamper-evident tape to all Ethernet connections and seal all unused ports on the network switch.

If an unauthorized connection does occur, system integrity must be reverified.

The jurisdiction must record whenever the ClearCount system is brought out of storage. After setting up the system, examine the following logs to determine if any unauthorized access occurred while the system was not officially in use:

- The web activity log, which tracks access to the CountServer computer
- The Windows Event Logs on each ScanStation computer and CountStation computer (See "Monitoring the Windows Event Log" on page 114.)

If there is a break in the custody and control of the jurisdiction, the jurisdiction must reverify the integrity of the system and, if necessary, reinstall it.

6.5.1 Physical setup

Clear Ballot setup instructions include the configuration of tables and the placement of essential equipment in a dedicated scanning area. The equipment layout is a logical flow that follows the order of the steps for scanning.

Clear Ballot recommends that the scanning location be adjacent to the ballot boxes or have the capacity to store and manage all of the ballots to be scanned. This minimizes potentially destabilizing ballot transit time and enables all election operations staff to view the entire operation. Mistakes in ballot handling, recording, or scanning can be caught and corrected by other members of the election staff if a single worker or team is engaged in questionable behavior.

If sufficient space to manage and scan all of the ballots is not available in a single section of the scanning location, the jurisdiction must increase the number of staff dedicated to ballot preparation and recordkeeping to ensure proper ballot control and accounting.

See the *ClearCount Election Administration Guide* for detailed instructions about setting up the work area where the scanning process takes place. This setup facilitates the scanning process while also protecting the integrity of the ballots.

6.5.2 Staffing

The scanning location itself must be secured. Unauthorized individuals must not be allowed into the facility. Individuals who are not part of the jurisdiction’s permanent staff must sign in and sign out at the entrance. The log of this activity must be maintained.

The Clear Ballot model calls for supervisors and recordkeepers to support and monitor the work of ballot preparation staff and scanner operators. The supervisors and recordkeepers ensure the smooth flow of ballot processing while monitoring the overall process transparency.

Clear Ballot's recommended process accounts for human factors that could potentially destabilize the ballot-scanning process. If a scanner operator becomes confused about the appropriate response to a given situation, he or she should stop scanning cards immediately and alert the scanning supervisor. The scanning supervisor, who has administrator-level access to the system, can log in using a special secured password, resolve any issues, and then return control to the scanner operator.

6.5.3 Scanning operation workflow

The scanning process begins in the ballot preparation area. Ballots are delivered in boxes to the ballot preparation area in accordance with the procedures of the jurisdiction for the secure transfer of ballots. The ballot preparation area consists of a surface only. The purpose of this area is simply to unseal ballot boxes (if required), stage ballots for the jogging station, and reseal ballot boxes. It does not matter how many ballots are in each box or the order in which they arrive from the election committee.

Before ballots are brought to the scanning area, complete the following steps:

1. Set up a ballot preparation table next to the scanning area.
2. Designate a second area for scanning.
3. Print target cards and box labels by counter group (such as AB, EV, ED, or OT).
4. Place target cards and labels under the ballot preparation table.

The ballot preparation team assigns target cards and the corresponding labels to the ballot boxes. The correspondence of these two items, and proper ballot-handling procedures when moving cards from the scanner outstack to the ballot box, facilitate Clear Ballot's Image-to-Ballot Traceability feature. The target card informs the scanner that a new box is being scanned and assigns the value of the barcode as the Box ID prefix for all subsequent ballots.

A target card is similar to a header card used by other voting systems.

The box label helps locate the box that contains a ballot card when needed for physical inspection. Ballots are stored in sequential order, starting with the target card at the bottom of the box.

Additionally, any required ballot box recordkeeping occurs in the ballot preparation area. Typically, the recordkeeper records all activity regarding opening, recording, and resealing sealed ballot boxes.

6.5.4 Handling of ballot boxes

The ClearCount workflow begins when the boxes of ballots to be counted are delivered to the scanning location. Ballots must be transmitted securely, in keeping with the jurisdiction's policies. For example, it is common for law enforcement officials to oversee the secure transport of ballot boxes from precincts to the scanning location.

After ballots enter the scanning location, the ClearCount system relies on a combination of staffing and site organization to marshal them securely through the workflow.

In the ClearCount setup, all work areas are laid out to minimize the possibility of ballot disorder or misplacement. Work areas contain only the necessary elements. There should be no extraneous items (such as extra computer equipment or books) on any of the work surfaces.

The scanning operation is designed with an implicit workflow in mind. In a scanning area, a ballot can be in one of three statuses: unscanned, scanning, and scanned. There is a designated location for each of these statuses. Ballots are removed from a box and placed in the unscanned pile to the left of the scanner. They are sent through the scanner and then moved into the box to the right of the scanner after being scanned.

The scanning supervisor is responsible for monitoring all operations and ensuring any interruptions in the process flow are handled properly and swiftly. The scanning supervisor is also responsible for ensuring that proper procedures are followed to protect the ballot chain of custody and the tabulation process.

The recordkeeper tracks all activity regarding the opening and resealing of sealed ballot boxes.

The ballot preparation staff prepares the ballots for scanning and moves them through the workflow so the scanner operators can focus on their task without interruption. This improves efficiency and minimizes the potential for confusion and errors.

Scanner operators work on batches of ballots at a time. Their work areas are laid out to minimize the possibility of confusion or misplacement. In their training, scanner operators are taught to alert the scanning supervisor at the first sign of scanner problems or operator confusion. The scanning supervisor is trained to delete boxes from the system so the scanner operators can rescan boxes that caused problems.

When scanning is complete, all ballots are returned to boxes (which now contain target cards and box labels to facilitate ballot retrieval if needed at a later date). The boxes are taken from the scanning area to a secure storage location. They remain protected, to ensure Clear Ballot's Image-to-Ballot Traceability and system integrity before a future audit or recount, until their allowable date of destruction.

Chapter 7. Removing software

7.1   Removing the ClearCount software from the CountServer computer

You do not have to uninstall a previous version of the ClearCount software before installing a new version.

If you need to remove the ClearCount software, wipe the hard disk on the CountServer computer.

7.2   Removing scanning software from ScanStations

To uninstall supporting software from ScanStation computers, type **programs** in the **Search** field on the Windows taskbar and select **Add or remove programs** from the search results.

Appendix A. Login credential rules and guidelines

Clear Ballot provides the following rules and guidelines for creating and maintaining login credentials for ClearCount user accounts.

Login credential rules

User names can consist of up to 16 alphanumeric characters. Valid characters are limited to A–Z, a–z, 0–9, spaces, underscores, and dollar signs. Special characters (such as, apostrophes, quotation marks, single quote marks, hyphens, periods, question marks, ampersands, letters with diacritical marks, and others) are not allowed.

User name guidelines

User names appear extensively in the ClearCount reports and logs. Clear Ballot recommends using:

- All lowercase characters
- Employee names or derivatives, rather than roles

Requirements for passwords

The following requirements apply to passwords:

- A password must be at least 14 characters long.
- When you change a password, you cannot reuse any of the five previous passwords.
- If you enter a password incorrectly five times in a row, your account will be locked for five minutes.
- When logged in at the console, you will be automatically logged out after 15 minutes of inactivity.

Password-management guidelines

Clear Ballot also strongly recommends the following password-management guidelines:

Maintain privacy.

Passwords should be known by as few people as possible. A good practice is that each password should be known to only one person. Each person needing access to the system should be provided with a separate account.

Keep the password secret.

The password should not appear in clear text in any physical or digital media that is not stored securely (that is, it should not be taped to the monitor).

Longer passwords are more secure.

The general rule is that longer passwords are more secure than shorter passwords. Common practice is for a password to be at least eight characters long, but Clear Ballot recommends a password that is at least 14 characters.

Create a password that is easy to remember.

There is often a tradeoff between security and convenience. Short passwords are easy to remember but are insecure. Long passwords offer greater security but can be difficult to remember. One way to choose a password that is long enough to be secure, and yet still easily remembered, is to choose a phrase and to then use the first few letters of each word in that phrase.

Mix at least three of: uppercase letters, lowercase letters, digits, and nonalphanumeric characters.

Using a variety of characters in a password offers greater security because it makes it more complex and, therefore, more difficult to guess.

Do not use a word listed in a dictionary of any language.

Many password-guessing programs start with a dictionary of known words. This is another reason why deriving a password from a phrase makes password guessing more difficult.

Change passwords frequently.

Even a strong password can be discovered. For example, a password that is mistakenly entered in the user name field can be logged. An individual, possibly one not authorized to use the system, may discover someone's password.

Keep the system current.

An account on the system should have its access level changed to *none* when the owner of that account is no longer an active or permitted user of the system.

Create a unique password.

Do not use the same passwords for multiple applications or systems. If a reused password is discovered, the security of the other applications or systems is compromised.

The ClearCount system allows an administrator to reset a user’s password if it is lost or compromised. Forgotten passwords *cannot* be recovered.

Appendix B. Installation checklist

Individuals who install ClearCount software can use this form to record the various user names and passwords they create during the installation, as well as other vital system information.

The election administrator or other responsible election official *must* store this confidential information in a safe and secure location.

Table B-1. Network switch information

Network switch
IP address of the network switch:
IP address of the network switch:
Password for the network switch:

Table B-2. CountServer information

CountServer computer
IP address of the server:
Hostname of the server (default is CountServer):
Account name for CountServer administrator (default is Unix Administrator):
User name for CountServer administrator account:
Password for CountServer administrator account:
Password for MySQL database root user:
ClearCount primary administrator name:
ClearCount primary administrator password:
Password for ScanStation account:
Server thumbprint:
CountServer computer BIOS password:

Table B-3. ScanStation computer information

ScanStation computers
Windows administrator user name:

Table B-3. ScanStation computer information (continued)

ScanStation computers
Windows administrator password:
Windows non-administrative user name:
Windows non-administrative user password:
ScanStation computer BIOS password:

Table B-4. CountStation computer information

CountStation computers
Windows administrator user name:
Windows administrator password:
Google Chrome certificate name and location:
CountStation computer BIOS password:

Table B-5. Scanner information

Scanners
Model, serial number and firmware version:
Model, serial number and firmware version:
Model, serial number and firmware version:
Model, serial number and firmware version:
Model, serial number and firmware version:
Model, serial number and firmware version: