ClearVote 2.1

ClearDesign Installation Guide

ClearDesign Installation Guide

Clear Ballot Part Number: 100063-10017

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

Document history

Date	Description	Version	Author
01/10/2017	Initial submission to EAC	1.0	Joe Srednicki
02/03/2017	Minor typographical and reference-related edits	1.0.1	Joe Srednicki
05/09/2017	Minor update based on feedback from the state of Colorado and Clear Ballot Quality Assurance	1.0.2	Joe Srednicki
06/01/2017	Updated the sections "ClearDesign parts checklist" and "Installation Procedure" (for Installing the DesignServer software). Changed the title of Chapter 2 to "Installing third-party software on the DesignServer."	1.0.3	Joe Srednicki
06/16/2017	Update for vote-by-mail campaign	1.0.4	Joe Srednicki
06/22/2017	Updated the section "Installation procedure" in Chapter 3.	1.0.5	Joe Srednicki
06/23/2017	Removed Linksys EA2700 N600 Dual-Band Wi-Fi Wireless Router from the section "ClearDesign Parts List."	1.0.6	Joe Srednicki
06/28/2017	Added section "Assigning static IP addresses"	1.0.7	Joe Srednicki
07/20/2017	Add Chapter 7, Updating ClearDesign	1.0.8	Joe Srednicki
07/21/2017	Udpate the version number for Colorado	1.0.9	Joe Srednicki
08/03/2017	In the chapter "Installing the Design Server," we corrected the cp command in step 4c of the section "Installation procedure."	1.0.10	Joe Srednicki
09/18/2017	In Chapter 3, "Installing the Design Server," in the section "Installation procedure," we clarified the step on entering the URL for the DesignServer.	1.0.11	Joe Srednicki
09/27/2017	Revise the following sections: "Steps for installing Google Chrome", "Installing Adobe Flash Player", "Installing the browser certificate for Google Chrome," "Hardening Windows DesignStations". Removed the sections: "Disabling wireless and Bluetooth Internet access", "Restricting program access and adding application whitelists", "Implementing a software restriction policy (SRP)"	1.0.12	Joe Srednicki

Date	Description	Version	Author
10/05/2017	Reordered the chapters and reorganized the content at the request of Clear Ballot Development to ensure the appropriate order for installation.	1.0.13	Joe Srednicki
10/06/2017	Added "Verifying the operating system" and "Updating the Windows 10 Pro operating system to version 1607"	1.0.14	Joe Srednicki
10/11/2017	Updated "ClearDesign parts checklist." Removed "Disabling autoplay."	1.0.15	Joe Srednicki
10/25/2017	Updated "Running the hardening script"	1.0.16	Joe Srednicki
11/29/2017	Updated "What the hardening script accomplishes" to indicate that the script denies the execution of unauthorized programs.	1.0.17	Joe Srednicki
01/19/2018	Vote-by-Mail campaign 2, added Installing Windows Drivers section, updated Windows installation procedure, minor edits	1.0.18	Joni G. McNutt
06/15/2018	Updates and rearrangement of topics for version 1.4.5.	1.0.19	Joe Srednicki
08/07/2018	Added information that USB drives are encrypted. Minor corrections.	1.0.20	Joe Srednicki
11/28/2018	Corrected a command in "Installing third-party software on the DesignServer."	1.0.21	Joe Srednicki
04/12/2019	Proofreading updates. Updated "Setting up the network switch." Added "Hardening the network switch." Other minor edits.	1.0.22	Joe Srednicki
06/21/2019	Minor edits. Removed information about updating BIOS.	1.0.23	Joe Srednicki
11/04/2019	Updated the cover page.	1.0.24	Joe Srednicki
02/12/2020	Minor edits	1.0.25	Joe Srednicki

Table of contents

Preface

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

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

About this document

This document describes how to install ClearDesign.

A ClearVote® system can comprise the ClearAccess®, ClearAudit®, 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.

Scope of this document

This document contains the following chapters:

- Chapter 1. Checking and unpacking the hardware
- Chapter 2. Setting up the network switch
- Chapter 3. Setting up the DesignServer
- Chapter 4. Setting up DesignStations
- Chapter 5. Updating ClearDesign
- Chapter 6. Security

Intended audience

This document is intended for election officials and election staff who are responsible for operations and maintenance before, during, and after an election. This document is also used by Clear Ballot personnel who support election officials and election staff.

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. Checking and unpacking the hardware

A complete ClearDesign system consists of one DesignServer and one or more DesignStations joined together in a closed Ethernet by a router. Your system may also include an external drive and a UPS.

1.1 Components checklist

Before you begin the installation, make sure that you have the necessary components:

- One DesignServer computer and power supply
- One or more DesignStation computers and power supplies
- One network router and power supply
- An Ethernet cable for each computer
- ClearDesign Ubuntu Server DVD
- ClearDesign DesignServer Application and ClearDesign Tools DVD
- Microsoft Windows 10 Pro DVD
- Windows Updates DVD

If a computer does not have a DVD drive, attach an external DVD drive.

For a list of approved hardware models, see the *ClearDesign Approved Parts List*.

1.2 Unpacking

Unpack the hardware for your ClearDesign system and follow the manufacturer's recommendations to set it up.

Do not turn on any hardware component.

Chapter 2. Setting up the network switch

This chapter describes how to set up the network switch.

ClearDesign operates on a closed, wired Ethernet. All ClearDesign computers are connected through a network switch. ClearDesign does not use Wi-Fi and does not connect to the Internet.

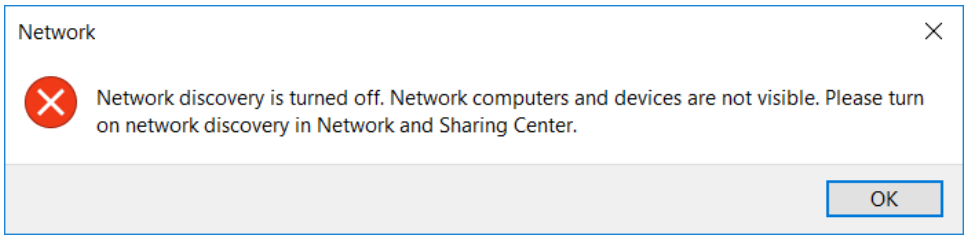
Clear Ballot recommends the following procedure to set up the Cisco SG250 switch for ClearDesign. Consult the manufacturer's documentation when configuring other switches.

Hardware used in elections must *never* be connected to the Internet. When setting up the network switch, you must use a Microsoft Windows 10 Pro computer that is not connected to the Internet.

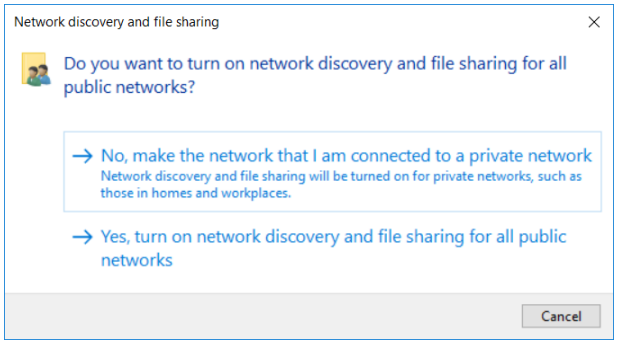
In the following procedure, a red asterisk (*) means that you should record this information on the "ClearDesign installation checklist" on page 41

To set up the network switch:

1. Configure the computer as follows:
    a. On the computer, right-click the **Windows Start** icon and select **File Explorer** from the pop-up menu.
    b. Select the **Network** option in the left navigation pane. A message appears. Click **OK**.



    c. 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.
    d. A message asks if you want to turn on network discovery and file sharing for all public networks. Select **No, make the network that I am connected to a private network**.



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

f. Select **Change adapter options** to open the Network Connections window.

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

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

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

i. Select the **Use the following IP address** option and enter *192.168.1.2* into the IP address field.

j. Enter *255.255.255.0* into the Subnet mask field and click **OK**.

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

2. Configure the switch as follows:

a. 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.

b. Connect an Ethernet 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.

c. Open a browser on the computer and navigate to 192.168.1.254 in the address field.

d. To log in, enter *cisco* for the user name and *cisco* for the password.

e. On the Change Password page, enter a new password.

f. *Record the password on the "ClearDesign installation checklist" on page 41.

g. On the Cisco configuration page, select **Configuration Wizards> Getting Started Wizard**.

h. Select **Launch Wizard** and then click **Next**.

i. On the General Information page, enter the physical location of the switch (such as, Clear County election central) in the System Location field.

j. In the System Contact field, enter the name of a contact person (such as, the election administrator) and click **Next**.

k. On the IP Settings page, select **VLAN** as the Interface and select **Static** as the IP Interface Source.

l. Enter *192.168.15.1* as the IP address, enter *255.255.255.0* as the Network Mask and click **Next**.

m. On the User Account page, enter a new user name (between 0 and 20 characters) and password, and click **Next**.

n. *Record the user name and password on the "ClearDesign installation checklist" on page 41.

o. On the Time Settings page, click **Next**.

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

The computer may appear to hang while the changes are applying. However, the computer actually gets disconnected because you have changed the IP address of the network switch to 192.168.15.1. However, the address of your computer is 192.168.1.2. Later, when you assign static IP addresses as part of securing the DesignStations, you will be able to reconnect. See "Assigning static IP addresses" on page 36.

q. Close the browser window.

3. Disconnect the computer from the switch and restore the computer's previous IPv4 settings.

4. Apply tamper-evident tape to all Ethernet connections and seal all unused ports on the network switch.

Jurisdictions must ensure the following:

- Limit physical access to the switch and its connections.
- Never connect a device to the switch that is not a component of the ClearDesign system.
- Never connect the switch to an outside network.

Chapter 3. Setting up the DesignServer

This chapter describes how to set up the DesignServer.

3.1 Installing the operating system on the DesignServer

The DesignServer uses the Ubuntu Linux Server operating system. This section describes how to install the operating system.

3.1.1 Before beginning

1. Ensure that the computer is not connected to any network.
2. Print a new blank Installation Checklist (See Appendix A, "ClearDesign installation checklist" on page 41).
3. As you go through the installation process, record the parameters on the installation checklist.

As you read through this document, a red asterisk (*) indicates a parameter that you should record on the installation checklist.

3.1.2 Installation procedure

1. Insert the ClearDesign Ubuntu Server DVD.
2. Power on the DesignServer.
3. Depending upon the computer model of the DesignServer, press **F11** or **F12** to display the Boot screen.
4. When the Boot screen appears, press **Enter**.

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

   a. Select the One-Shot BIO 160;Boot Menu.

   b. Select the appropriate drive.

      Example: Optical drive connected to USB1: DVDRAM GPGO NBSO
5. Install Ubuntu on the computer by following the prompts on the screen and supplying the information in Table 3-1. In this table and throughout the remainder of this a document, a red asterisk (*) indicates a parameter to record on the installation checklist. (See Appendix A, "ClearDesign installation checklist" on page 41.)

   After you enter some parameters, the installation process can take a few minutes to update the computer. The installation process displays various progress messages while the updates occur.

Table 3-1. Installation parameters for Ubuntu

Installation parameter	Selection or action
* Record this parameter on the Installation Checklist (See Appendix A, "ClearDesign installation checklist" on page 41.)	
Language	English
Install	Ubuntu Server
Select a Language	English
Select your location	United States
Detect Keyboard	No
Configure Keyboard	Country of Origin: English (US)
Configure Keyboard	Keyboard layout English (US)
Configure the network: Primary network interface (This prompt appears only when there are multiple network interfaces.)	Press **Enter**.
Configure the network: Network autoconfiguration failed	Continue
Configure the network: Network configuration method	Configure network manually
*Configure the network: IP address	192.168.15.249
*Configure the network: Netmask	Use default (255.255.255.0)
*Configure the network: Gateway	Use default (192.168.15.1)
*Configure the network: Name server address	Use default (192.168.15.1)
*Configure the network: Hostname	Use DesignServer1 for first DesignServer, DesignServer2 for second DesignServer, and so on unless your jurisdiction has established a different naming scheme.

Table 3-1. Installation parameters for Ubuntu (continued)

Installation parameter	Selection or action
Configure the network: Domain name	Use default (blank field)
*Set up users and passwords - Full name for the new user	Enter the first and last name of the ClearDesign administrator. (The ClearDesign administrator does not require a password.)
*Set up users and passwords - Username for your account	Press **Enter** to accept the default username for the Linux administrator—which is the first name from the previous row of this table—or enter a different username and press **Enter**.
*Set up users and passwords - Choose a password for the new user	Enter the Linux administrator password.
*Set up users and passwords - Re-enter password to verify	Confirm the Linux administrator password.
Configure Clock	Select time zone
Partition disks - Partitioning method	Guided – use entire disk and set up LVM
Partition disks – Select disk to partition	Press **Enter**.
Partition disks – Write the changes to disks and configure LVM	Yes
Partition disks – Amount of volume to group to use for guided partitioning	Press **Enter**.
Partition disks – Write changes to disk	Yes
Configure the package manager - HTTP proxy information	Press **Enter**.
Configuring tasksel – How do you want to manage upgrades to this system	No automatic updates
Software Selection – Choose software to install	Press **Enter**. (Install no additional software.)

Table 3-1. Installation parameters for Ubuntu (continued)

Installation parameter	Selection or action
Install the GRUB boot loader	Yes
Finish the installation	Press **Enter**.

3.1.3 Completing the installation of the operating system

After you enter all the installation parameters, the installation process takes approximately 20 minutes to update the DesignServer. After the updating is complete, the DesignServer automatically restarts.

3.2 Installing third-party software on the DesignServer

The ClearDesign DesignServer requires the installation of several third-party software tools. Clear Ballot provides a setup script for the installation.

To install the third-party software tools:

1. Log in to the computer with your user name and password.
2. Insert the ClearDesign DesignServer Application DVD into the disc drive on the computer.

   If you are using an encrypted USB drive, insert it into a port on the computer.
3. Copy the install-setup directory from the DVD to the server:
   a. Switch to the root:

      ```
      sudo su
      ```

   b. Enter your password.
   c. If you are using an encrypted USB drive, enter:

      ```
      mkdir /media/usb
      mount /dev/sdb1 media/usb
      cp -r /media/usb/install-setup .
      ```

   d. If you are using a DVD, enter:

      ```
      mount /dev/cdrom /media/cdrom
      cp -r /media/cdrom/install-setup .
      ```

e. Enter:

```
cd install-setup
chmod +x install*
./install
```

f. Enter a password for the MySQL root user. Re-enter the password for the MySQL root user. Make sure to record this password for later use.

g. Restart the computer by entering the following command:

```
reboot
```

3.3 Installing the DesignServer software

To install the DesignServer software:

1. Log in to the computer with your user name and password.
2. Insert the ClearDesign Server Application DVD into the disc drive of the computer.

   If you are using an encrypted USB drive, insert it into a port on the computer.
3. Copy the source code:

   a. Enter:

   ```
   sudo su
   ```

   b. Enter your password.

   c. If you are using an encrypted USB drive, enter:

   ```
   mkdir /media/usb
   mount /dev/sdb1 /media/usb
   cp -r /media/usb/clearDesign-x.x.x.zip .
   ```

   The placeholder *x.x.x* specifies the version.

   d. If you are using a DVD, enter:

   ```
   mount /dev/cdrom /media/cdrom
   cp -r /media/cdrom/clearDesign-x.x.x.zip .
   ```

   The placeholder *x.x.x* specifies the version.

e. Enter:

```
unzip clearDesign-x.x.x.zip install
chmod +x install
./install clearDesign-x.x.x.zip
```

To regenerate the digital certificate mentioned in step 3 g, enter the following instead:

```
./install –f clearDesign-x.x.x.zip
```

f. When prompted, enter the MySQL root user password. If you enter the password incorrectly, the installation script exits after third failed attempt.

g. If you are installing ClearDesign for the first time or are using the -f option as shown in step 3e, the system generates a digital certificate for ClearDesign to use.

h. When prompted, enter the URL for the DesignServer. Enter the value that you specified for the parameter **Configure the network: hostname**.

4. Verify that the installation was successful by noting that the last line of the installation script reads " installed."

5. Reboot the computer by entering the command:

```
reboot
```

Chapter 4. Setting up DesignStations

This chapter describes how to install Microsoft Windows 10 Pro, the Windows drivers, Google Chrome, and browser certificates on DesignStations.

4.1 Installing the Windows operating system

To install Windows:

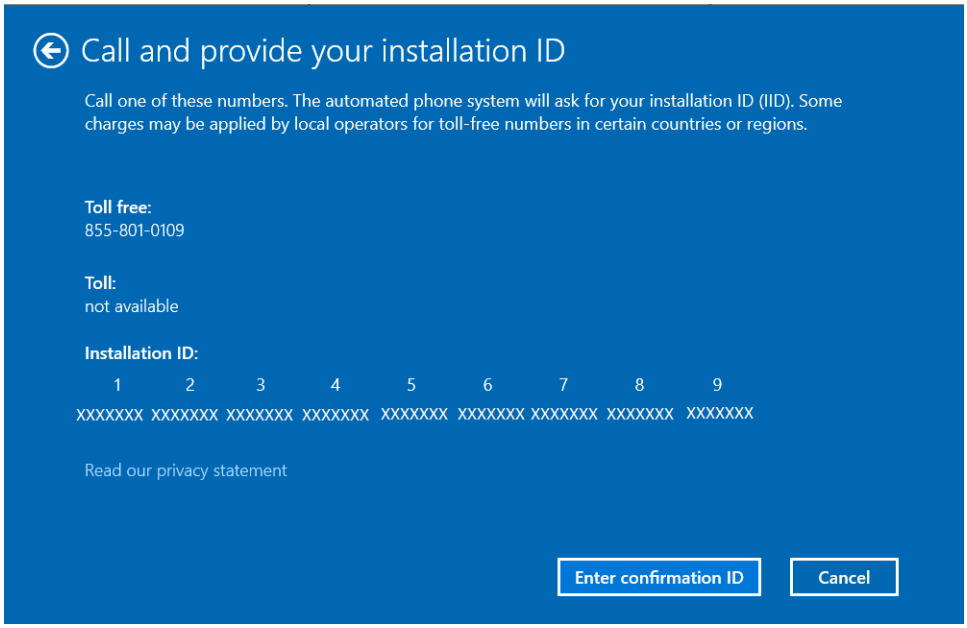
1. Turn off the computer and insert the Microsoft Windows 10 Pro DVD into the drive.
2. Turn on the computer and immediately press **F12** when the Dell logo appears.
3. Select **Change Boot Mode settings** and press **Enter**.

   If the BIOS has been restricted previously, you are prompted for the administrator password. Enter the password and press **Enter**. This password is recorded on the ClearDesign Installation Checklist from the previous installation.
4. From the **Change Boot Mode to** options, select **Legacy Boot Mode, Secure Boot Off** and press **Enter**.
5. When a warning appears asking if you want to proceed, select **Yes** and press **Enter**.
6. When another warning appears asking for your final confirmation, select **Apply the Charges** and press **Enter**. The computer restarts.
7. When the Dell logo appears, immediately press **F12**.
8. From the **Legacy Boot** options, select the **Boot Device for CD/DVD** option.
9. When the Windows Setup dialog appears, select the desired language and click **Next**.
10. In the next dialog, click **Install Now**.
11. When the license terms appear, select the checkbox and click **Next**.
12. In the next dialog, select the **Custom: Install Windows only (advanced)** option.
13. When asked where you want to install Windows, select the first partition and click the **Delete** icon. A message appears. Click **OK**. A single drive named *Drive 0 Unallocated Space* remains. Click **Next**.
14. The installation begins and takes about 10 minutes. Then the computer restarts.
15. When the Let's get connected dialog appears, click **Skip this step**.
16. When the Get going fast dialog appears, click **Customize settings**.
17. In the Personalization settings, click each option to turn it off and click **Next**.

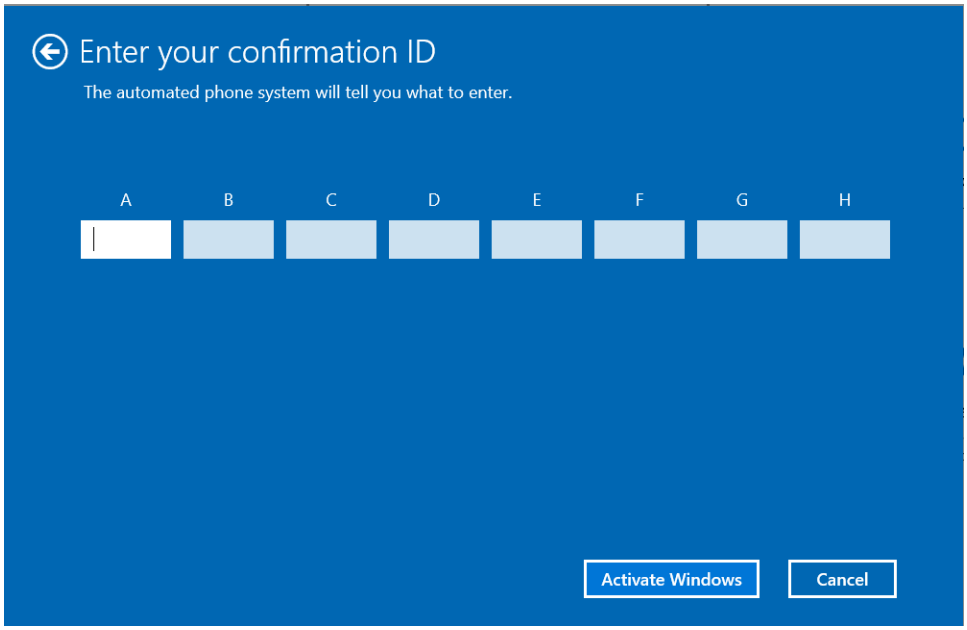
18. In the Connectivity and error reporting settings, click each option to turn it off and click **Next**.
19. In the Browsers, protection and update settings, click each option to turn it off and click **Next**.
20. When the Create an account for this PC dialog appears, enter the user name and password for the Windows administrator and click **Next**.
21. (Recommended) Record the Windows administrator user name and password on the Installation checklist. (See Appendix A, "ClearDesign installation checklist" on page 41.)
22. In the Meet Cortana dialog, click **Not now** and then click **Next**. Windows finishes its setup.
23. Remove the Microsoft Windows 10 Pro DVD and insert the Windows Updates DVD.
24. Navigate to the Windows Tools folder, open the Windows Activation Key.txt file, and copy the text.
25. From the task bar, type *settings* into the Search field and select **Settings** from the search results.
26. Click the **Activate Windows now** option at the bottom of the Windows settings window, and then click **Change product key**. Click **Yes** when asked if you want the app to make changes.
27. Paste the activation key text string into the Product Key field and click **Next**.
28. A dialog indicates that the device will need to connect to the activation service. Click **Close**.
29. Right-click the Windows icon on the task bar and select **Run** from the pop-up menu.
30. In the Run dialog, type *slui.exe 4* into the Open text field and click **OK**.
31. On the screen that appears, select your country from the drop-down list and click **Next**.

32. A screen appears that provides a toll-free telephone number to call for activation.



33. Call the activation service, follow the automated prompts, and provide the nine-part installation ID that appears on the screen.

34. Click the **Enter confirmation ID** button on the screen, enter the eight-part confirmation number that the automated activation service provides, and click **Activate Windows**.



35. A confirmation message indicates that Windows has been activated. Click **Close**.

4.2 Installing Windows drivers

Install the following Windows drivers:

- Chipset drivers
- Graphics drivers

Installing Windows drivers requires restarting the system.

To install the drivers:

1. Log in to the computer as the Windows administrator.
2. Insert the Windows Updates DVD into the DVD drive and navigate to the folder applicable to your computer model.
3. Open the Chipset folder, double-click each application file and follow the onscreen prompts to install each of the drivers in the folder. Do not restart the computer after installation.
4. Open the Graphics folder, double-click each application file and follow the onscreen prompts to install each of the drivers in the folder. Do not restart the computer after installation.
5. When you have installed all of the drivers, restart the computer.

4.3 Installing Google Chrome

The specific steps for installing Google Chrome may change from time to time.

To install Google Chrome:

1. Insert the ClearVote Tools DVD into the DesignStation computer.
2. Navigate to Browsers and Flash> Offline Chrome Installer and double-click the application file.
3. When the User Account Control dialog appears, click **Yes** and then follow the instructions to complete the installation.

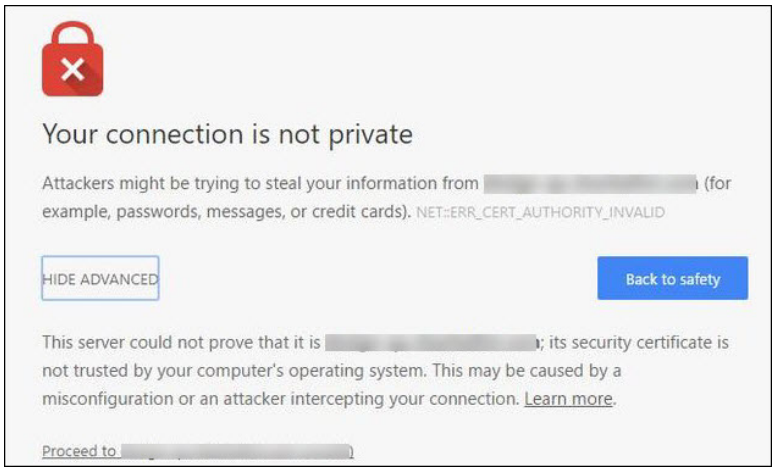
4.4 Installing the browser certificate for Google Chrome

When using the HTTPS protocol to access a ClearDesign server, you receive a digital certificate warning about an untrusted site. This is because Clear Ballot products use self-signed certificates. This is perfectly safe in the kind of closed network environment that Clear Ballot products are used in, but a warning message will appear when accessing the site until you install the certificate on the local computer.

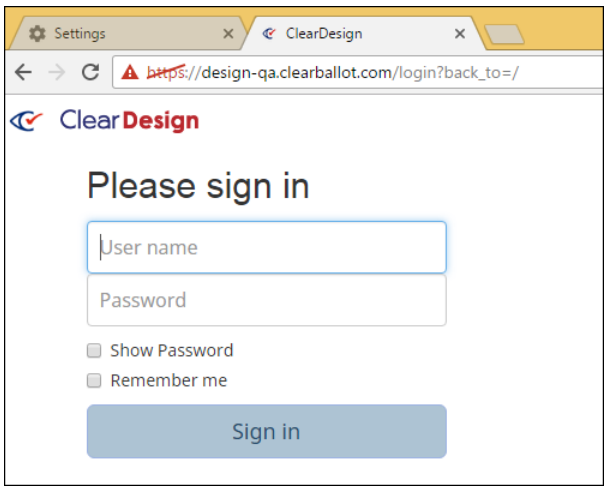
4.4.1 Beginning the installation of the browser certificate

To begin installing the browser certificate for Google Chrome:

1. Navigate to http://<servername> or https://<servername>. An alert appears.
2. Click the **Advanced** link that appears on the alert. The following window appears:



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.

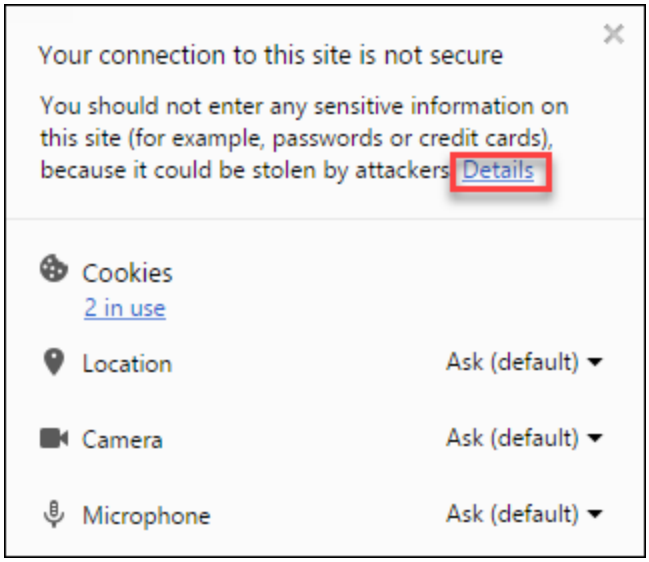


4.4.2 Adding the certificate

To add the certificate, do the following:

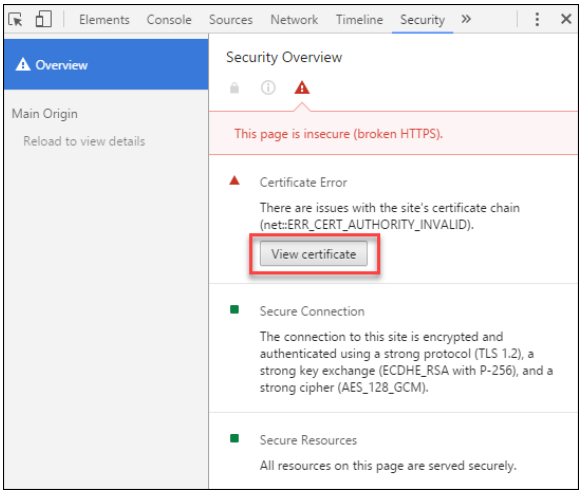
1. In the browser's address bar, click the red triangle containing the exclamation point.

   Google Chrome displays a settings window. The following image shows the top portion of this window:



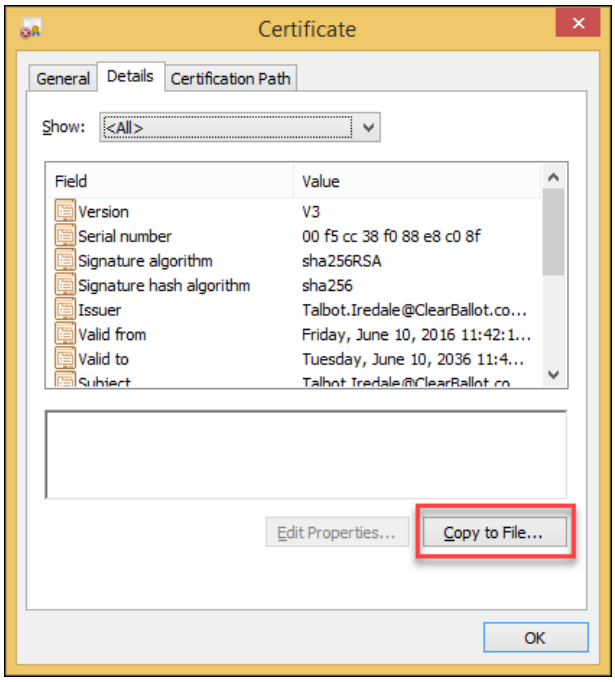
2. Click the **Details** link next to the text that says, “You should not enter any sensitive information on this site ... "

   The Security Overview window appears.



3. On the Security Overview window, click the **View Certificate** button.

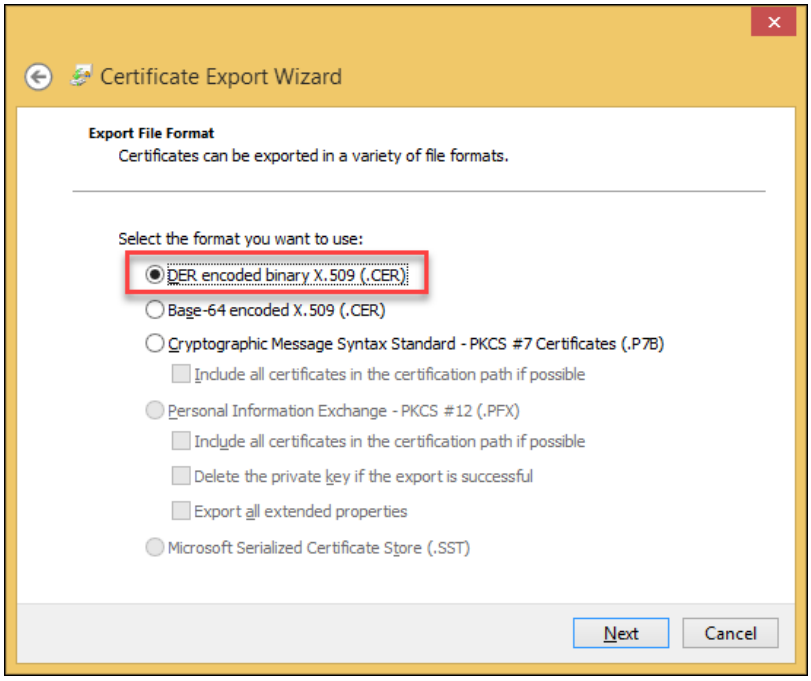
4. When the Certificate window appears, click the **Details** tab.



5. On **Details** tab of the Certificate window, click the **Copy to File** button at the bottom right.

6. When the Certificate Export Wizard appears, click **Next**.

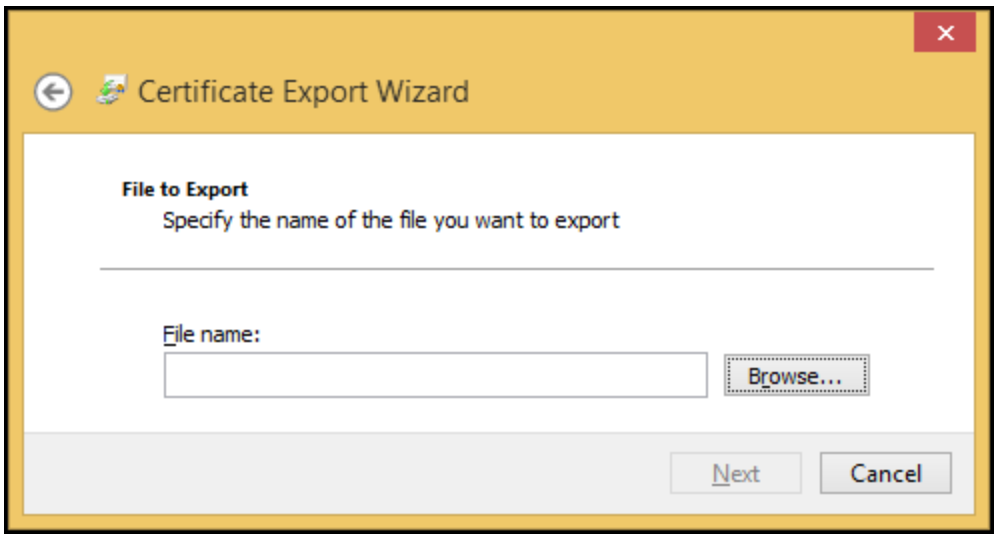
7. When the Certificate Export Wizard-Export File Format window appears, select the**DER encoded binary X.509 (.CER)** option, and click the **Next** button.



8. When the Certificate Export Wizard-File to Export window appears, click the **Browse** button to choose where to save the certificate and enter the name of the file.

   Example: chrome-cert.cer

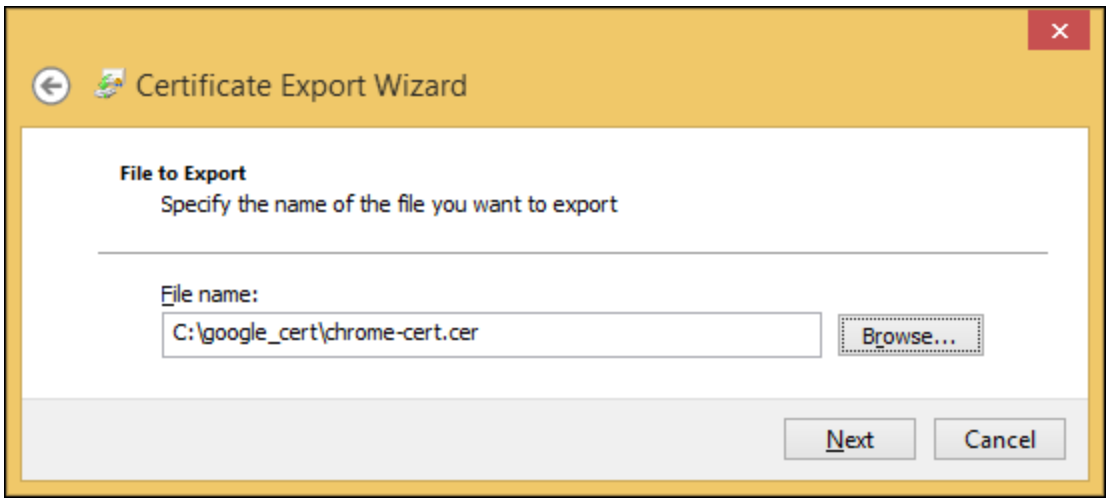
   Clear Ballot recommends storing the certificate in your Documents folder. However, you can store it any location as long as you record where you save it.



9. After you navigate to the appropriate location and enter the filename, click **Save**.

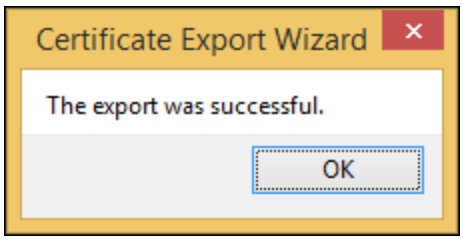
   Be sure to note the name and location of the file.

10. When the following window appears, click the **Next** button.



11. When the following window appears, click the **Finish** button.

Google Chrome displays the following confirmation message to indicate that installation of the certificate was successful.



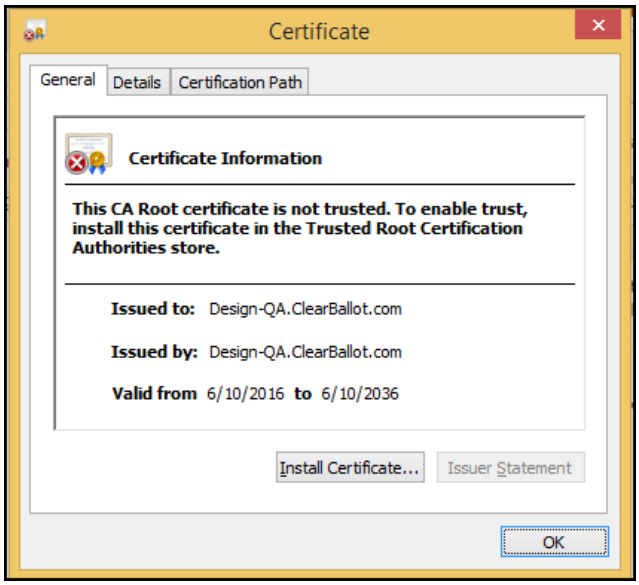
12. Click **OK** to close the confirmation message and click **OK** to close the Certificate window.

4.4.3 Installing the certificate

Follow these steps to install the certificate:

1. Use Windows Explorer to navigate to the location where you saved the certificate.
2. Double-click the filename for the certification.

   The Certificate window appears.

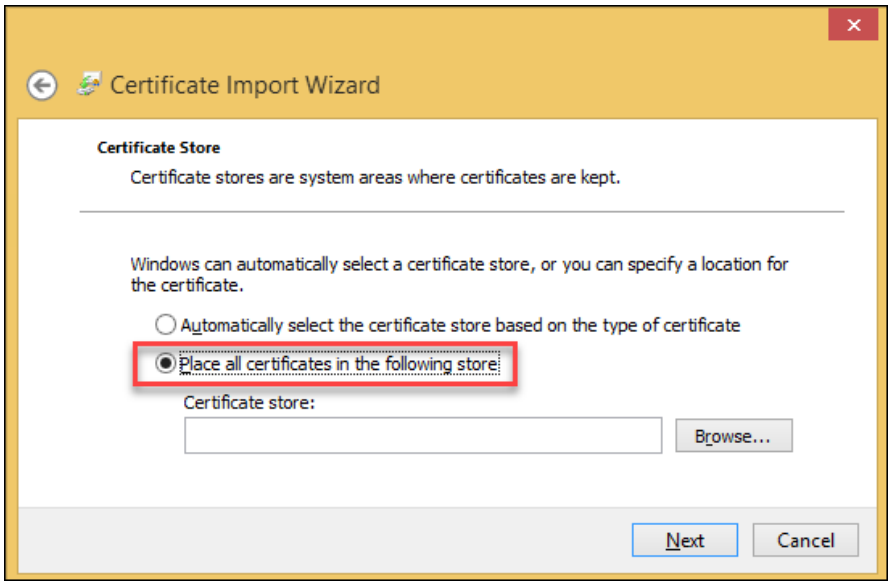


3. Click the **Install Certificate...** button.
4. When the following window appears, select **Local Machine** as the Store Location and click the **Next** button.

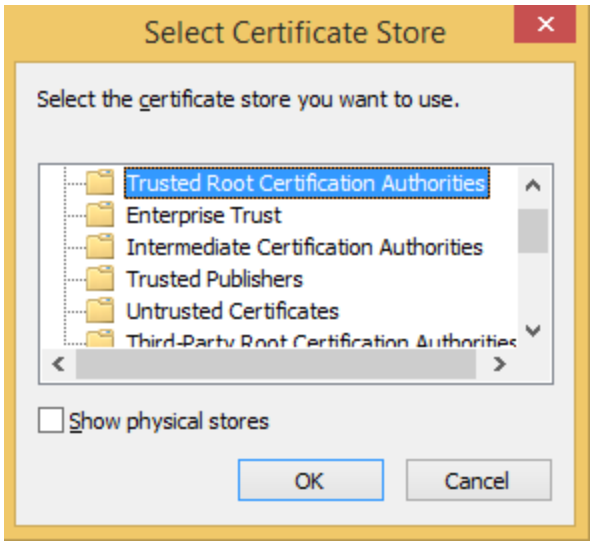
5. A message asks if you want to allow the program to make changes to the computer.

   Click **Yes**.

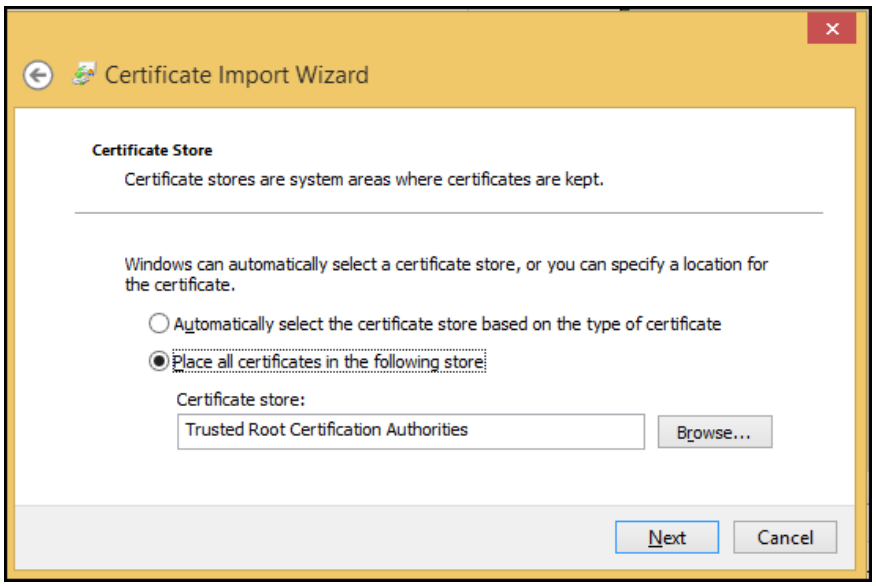
6. When the following window appears, select **Place all certificates in the following store** and then click the **Browse** button.



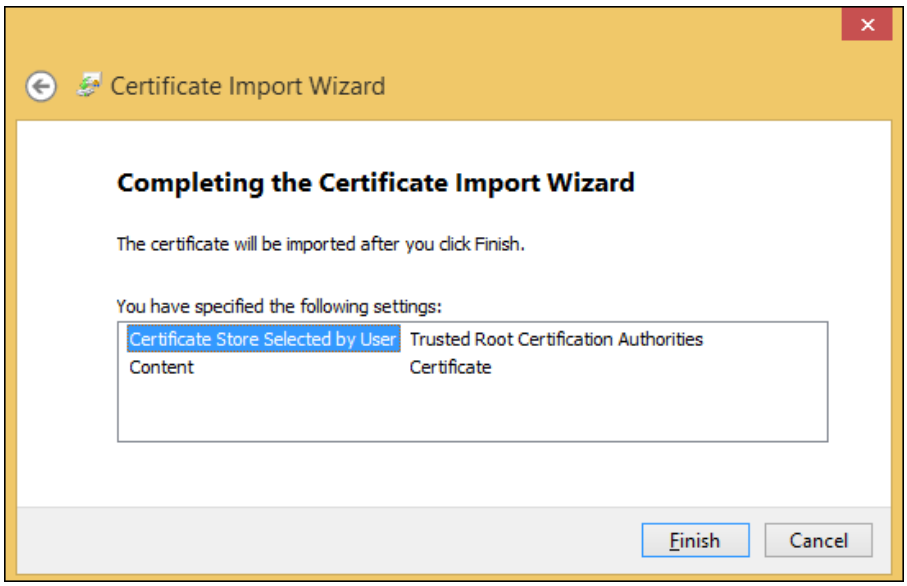
7. When the following window appears, select **Trusted Root Certification Authorities** and then click the **OK** button.



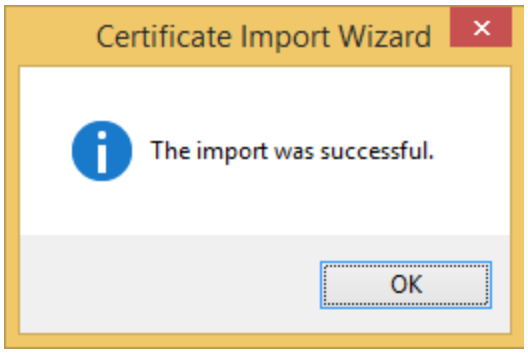
8. When the following window appears, click the **Next** button.



9. When the following window appears, click the **Finish** button.



Google Chrome displays the following confirmation message.



10. Click **OK** to dismiss the confirmation message
11. Click **OK** to dismiss the Certificate window.
12. Restart Chrome and navigate back to http://<servername> or https://<servername>.

    You no longer receive the warning, and HTTPS no longer has a red line through it.

Chapter 5. Updating ClearDesign

This chapter describes how to update ClearDesign.

To update the DesignServer, you install the updated software over the previous version. You do not need to uninstall the previous version.

Security updates should be made to ClearDesign periodically, but must be in the form of new software versions issued by Clear Ballot and approved by the jurisdiction's state election governance office.

5.1 Before beginning an update

- Ensure that all elections are backed up.
- Ensure that all user accounts are exported.
- Locate and print the installation checklist that you used for the previous installation.
- Print a new blank installation checklist found at the end of this manual. As you go through the upgrade process, record the items on this checklist. (See Appendix A, "ClearDesign installation checklist" on page 41.)

5.2 Updating the DesignServer

To update the DesignServer:

1. Install the third-party software on the DesignServer as described in Chapter 3.
2. Install the DesignServer software as described in Chapter 3.

5.2.1 Changing the Common Name of the server (optional)

If you want to change the Common Name of the server, do the following:

1. Enter:

   ```
   sudo su
   ```

2. When prompted, enter the password.
3. Enter the following:
   a. If you are using an encrypted USB drive, enter:

      ```
      mkdir /media/usb
      mount /dev/sdb /media/usb
      cp -r /media/usb/clearDesign-x.x.x.zip .
      ```

      The placeholder *x.x.x* specifies the version.

b. When using a DVD, enter:

```
mount /dev/cdrom /media/cdrom
cp -r /media/cdrom/clearDesign-x.x.x.zip .
```

The placeholder *x.x.x* specifies the version.

c. Enter:

```
unzip clearDesign-x.x.x.zip install
chmod +x install
./install clearDesign-x.x.x.zip
```

To regenerate the digital certificate mentioned in step 4 g, enter the following instead:

```
./install –f clearDesign-x.x.x.zip
```

d. When prompted, enter the MySQL root user password. If you enter the password incorrectly, the installation script exits after third failed attempt.

e. If you are installing for the first time or you use the –f option as shown in step 3e, the system generates a digital certificate for to use.

f. When prompted, enter the URL for the DesignServer. Enter the value that you specified for the parameter **Configure the network: Hostname**. See Table 3-1 on page 13.

4. Enter the following:

```
chmod+x install
./install -f clearDesign-x.x.x.zip
```

The placeholder *x.x.x* is the current version that you are upgrading.

The installation script then prompts for the MySQL root password as described in Chapter 3.

5. Follow the remainder of the steps in Chapter 3.

5.3 Updating DesignStations

To update DesignStations, uninstall previous versions of Google Chrome and browser certificates and install the new versions.

5.3.1 Removing a previous version of Google Chrome

Use the Add/Remove Programs functionality of the Control Panel in Windows to uninstall previous versions of Google Chrome.

5.3.2 Removing a previous version of a browser certificate in Google Chrome

To remove a previous version of a browser certificate in Google Chrome:

1. Start the certificate manager:
   a. Hold the Windows key and press R.
   b. Type **certmagr.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 DesignServer.

   Example: design-qa.clearballot.com
5. Right-click the certificate and select **Delete**.
6. Confirm the deletion.

5.3.3 Reinstalling Google Chrome and browser certificates

Install Google Chrome and the browser certificates as described in Chapter 4.

5.4 After upgrading

Verify that ClearDesign is working properly.

Request the jurisdiction to perform the following tasks:

- Restore the backed up election
- Add user accounts
- Store the installation checklist that you filled out during the upgrade in a secure location. (See Appendix A, "ClearDesign installation checklist" on page 41.)

Chapter 6. Security

After installing and configuring the computers used for ClearDesign, follow the directions in this chapter to secure the system.

6.1 Use of encrypted USB drives

Clear Ballot recommends the use of encrypted USB drives. See the *ClearVote Approved Parts List* for information about approved devices.

6.2 Location security

Maintaining physical security of the ClearDesign system is an important part of its operation and maintenance. When the components of the ClearDesign system are not in use, store them in a locked area under the custody and control of the jurisdiction. The jurisdiction must control access to this area for the following reasons:

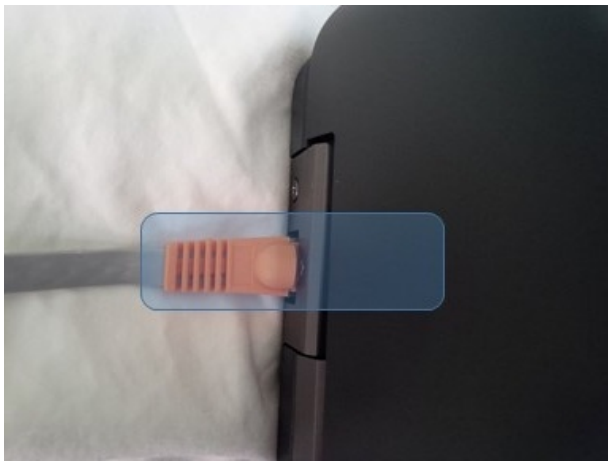
- To prevent access by unauthorized individuals
- To enable system audit functions to identify any security breaches

When in storage or in use, keep the ClearDesign system must be kept within a controlled area where only individuals authorized by the jurisdiction can come into direct contact with the components of the system. Each jurisdiction must also follow all jurisdictional and state rules. This means using at least one of the following security methods to provide deterrence and physical security:

- Receptionists or guards with a gate or other barrier to the area
- Security cameras
- Electronic door-locking mechanisms such as ID cards or key fobs that record the identity of the device used to unlock the door
- A locking computer rack or other cabinet to contain components of the ClearDesign system

The DesignSever, attached network switch router, and all data cable connections in the ClearDesign system are especially security-sensitive. When in use, segregate and enforce enhanced security over the DesignServer, the ClearDesign closed network switch router, and the Ethernet cable connections to the DesignStations on that closed network. Placing the DesignServer and network switch router in a locked computer rack or in a secure area is necessary to maintain a proper system security posture for ClearDesign. Likewise, the jurisdiction must use cable locks or tamper-evident seals to provide an enhanced level of security over 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 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.



The jurisdiction must record whenever the ClearDesign 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 DesignStation access
- The Windows Event Logs on each DesignStation computer

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.

At no point can any unauthorized hardware be connected to the system. The tamper-evident seals shown above can be applied to cover the Ethernet ports on DesignServer and DesignStation computers to deter unauthorized connections. If an unauthorized connection does occur, system integrity must be reverified.

6.3 Securing DesignStations

This section describes procedures for securing DesignStations. Complete the procedures in this section before you run the hardening script as described on page 38.

6.3.1 Assigning static IP addresses

Follow the steps below to assign static IP addresses to the DesignStations.

1. Log in to the computer as a Windows administrator.
2. From the task bar, right-click the Microsoft Windows **Start** icon and select the **Control Panel** option.
3. Click **Network and Internet** and then click **Network and Sharing Center**.
4. Click **Ethernet** to open the Ethernet Status dialog.
5. Click the **Properties** button and then double-click the **Internet Protocol Version 4 (TCP/IPv4)** option.
6. Select the **Use the following IP address** option and assign a static IP address (from within the range of 192.168.15.2 to 192.168.15.249) to the DesignStation.
7. Click **OK** and close all open dialogs.
8. From the task bar, right-click the Microsoft Windows **Start** icon and select the **Command Prompt** option.
9. Verify the IP address by typing *ipconfig* in the Command Prompt window and pressing the Enter key. Close the Command Prompt window.
10. Repeat this process for each DesignStation.

6.3.2 Updating Windows Defender Antivirus

Microsoft provides the Windows Defender Antivirus program with its Windows operating system. To keep the virus definitions up-to-date, you must update the program. Microsoft recommends that Windows Defender Antivirus be updated at least once a week. Clear Ballot recommends that the Windows Defender Antivirus program be updated on every ScanStation and election administration station prior to each election.

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

To download antivirus definitions:

1. On a computer outside the closed ClearCount network, and that has a USB port and Internet connection, navigate to https://www.microsoft.com/security/portal/definitions/adl.aspx.
2. Download the antivirus definitions 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. Insert an encrypted USB drive into a USB port on the computer you downloaded the software to, copy the file to the encrypted USB drive and then eject the encrypted USB drive.

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. From the task bar, type defender into the Search field and then select Windows Defender Security Center from the search results.
3. Click Virus & threat protection.
4. Click Protection Updates and note the date and time that the definitions were created. Do not close the Protection Updates window.
5. Insert the encrypted USB drive into a USB port on the computer and browse to the file.
6. Right-click the file and select the Run as Administrator option from the pop-up menu.
7. 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.
8. Return to the Protection Updates window and check the date and time that the definitions were created. The date should be the date you downloaded the file. Close the Protection Updates window.

Repeat the update process on each election administration station and ScanStation computer.

Maintain the history and archive copies of each update.

6.4 Hardening the DesignStations

Hardening the DesignStations in a ClearDesign system consists of running a script. This script accomplishes the following:

- Enables FIPS 140-2 security mode
- Disables the wireless and Bluetooth Internet services
- Denies the execution of unauthorized programs
- Disables the autoplay feature
- Disables the Edge browser
- 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 and Mozilla Firefox
- Disables Google Chrome updates

6.4.1 Running the hardening script

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 DesignStation Harden folder to the DesignStation desktop.
4. Open the DesignStation 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 DesignStation Harden folder from the desktop, and empty the recycle bin.

6.4.2 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:
   a. Using the arrow keys, navigate to the Security screen and select Admin Password.
   b. Enter and confirm the admin password.
   c. Record the password on the ClearDesign Installation Checklist. (See "ClearDesign installation checklist" on page 41.)

4. To save your changes, click **OK** and then click **Exit**.
5. Restart the computer and verify that the changes have been implemented.

6.5 Hardening the network switch

For enhanced security, the network switch can be configured to limit access to only the specific ClearDesign 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 ClearDesign system. Consult the manufacturer's documentation when configuring other switches.

To harden the network switch:

1. Ensure that your ClearDesign 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 DesignServer, DesignStation1, DesignServer2, and so on).
3. Log in to an election administration station, open a browser and navigate to 192.168.15.1 in the address field.
4. Enter the user name and password that you created when you set up the switch. (See"Setting up the network switch" on page 9.)
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 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 an DesignStation, open a browser and navigate to 192.168.15.1 in the address field.
2. Enter the user name and password that you created when you set up the switch. (See "Setting up the network switch" on page 9.)
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.

Never delete all devices as this requires the network switch to be reset and completely reconfigured.

Appendix A. ClearDesign installation checklist

Before you install ClearDesign, print a new blank version of this checklist to record the various parameters as you perform the installation process. As you go through this manual, a red asterisk (x) indicates a parameter to record on this checklist.

After you complete the installation process, store this confidential information in a safe and secure location.

Network switch: IP address
Network switch: User name
Network switch: Password
Configure the network: IP address:
Configure the network: Netmask (default):
Configure the network: Gateway (default):
Configure the network: Name server address (default):
Configure the network: Hostname (default): (Clear Ballot suggests using DesignServer when there is a single server. If there are multiple servers, you can use the scheme DesignServer1, DesignServer2, and so on. Alternatively, follow any naming convention that your jurisdiction has established.)
Configure the network: Domain Name (default, blank):
Set up users and passwords - Full name for the new user: (Enter the first and last name of the ClearDesign administrator. The ClearDesign administrator does not require a password.)
Set up users and passwords - User name for your account: (Press Enter to accept the default username for the Linux administrator—which is first name from the previous row—or enter a different user name.)
Set up users and passwords - Choose a password for the new user: (Enter the Linux administrator password.)
Set up users and passwords - Re-enter password to verify: (Confirm the Linux administrator password.)
BIOS password:
MySQL Root User Password:

Clear Ballot recommends using **cbg** for this password unless your jurisdiction requires using another password.
Organization Name:
Organizational Unit Name:
Email address (primary contact person):
Google Chrome certificate name and location: