ClearVote 2.3

ClearDesign Installation Guide

ClearDesign Installation Guide

Clear Ballot Part Number: 100063-10020

Document Type: Customer

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	Update 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

Date	Description	Version	Author
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
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

Date	Description	Version	Author
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
10/16/2020	Updated preface. Reorganized chapters and sections to place the sections about the network switch in the appropriate order. Indicated that a network switch is optional. Added "Installing the Window patch." Added "Disabling BitLocker and "Enabling BitLocker." Added "Changing the BIOS boot setting."	2.0	Joe Srednicki
12/16/2020	Minor edits	2.0.1	George Petta
01/25/2021	Updated the password requirements in the table "Installation parameters for Ubuntu."	2.0.2	Joe Srednicki
09/15/2021	Updated "Disabling BitLocker" and "Enabling BitLocker (optional)." Minor edits.	2.0.3	Eric Burz
02/03/2021	Updated cover page.	2.0.4	Joe Srednicki
03/18/2022	Updated "Installing the Windows operating system."	2.0.5	Joe Srednicki
03/23/2022	Added "Updating the BIOS version on the Dell 5521." Corrected the 03/18/2022 row in this table.	2.0.6	Joe Srednicki
03/21/2023	Minor edits	2.0.7	Douglas McCulloch
04/06/2023	Minor edits	2.0.8	Douglas McCulloch

Table of contents

Preface

This section defines the purpose of this document.

About this document

This document describes how to install ClearDesign.

Scope of this document

This document contains the following chapters:

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

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.

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 ClearDesign system consists of one DesignServer and one or more DesignStations connected on a closed network by an Ethernet CAT cable and an optional network switch. A ClearDesign 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
- (Optional) One network switch and power supply

  The network switch is required only in configurations where multiple DesignStations communicate with a DesignServer.
- One of more Ethernet CAT cables

  In configurations containing a DesignServer and one DesignStation, one Ethernet CAT cable is required to connect the two computers to one another.

  In configurations containing a DesignServer and multiple DesignStations, each computer requires an Ethernet CAT cable. In this configuration, the Ethernet CAT cables connect each computer to the network switch.
- 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.

Note: Do not turn on any hardware component.

After you unpack the hardware, connect the Ethernet cable from the DesignServer to the computer that will be used as a DesignStation or to the network switch if you are using one.

Chapter 2. Setting up the DesignServer

This chapter describes how to set up the DesignServer.

2.1 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.

2.1.1 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 50).
3. As you go through the installation process, record the parameters on the installation checklist.

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

2.1.2 Changing the BIOS boot setting

Before installing the ClearCount software, ensure that the BIOS boot setting of the DesignServer computer is set to UEFI.

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

To change the BIOS boot setting:

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

   For example, if you are 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, 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 **Enter**.
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 appears indicating success, press the **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.

2.1.3 Installation procedure

1. Insert the ClearDesign Ubuntu Server DVD.
2. Power on the DesignServer.
3. As the DesignServer starts up, *immediately* press the key that accesses the startup menu.

   For example, if you are using a Dell computer, press **F11** or **F12** key.

   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.
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 UEFI Boot Menu**.

   b. Select the appropriate drive.

      Example: Optical drive connected to USB1: DVDRAM GPGO NBSO
5. Select the drive with the ClearDesign Ubuntu Server DVD.

   The installation program launches.
6. Install Ubuntu on the computer by following the prompts on the screen and supplying the information in Table 2-1. 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 50.)

> **Note**: 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 2-1. Installation parameters for Ubuntu

Installation parameter	Selection or action
* Record this parameter on the Installation Checklist (See Appendix A, "ClearDesign installation checklist" on page 50.)	
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)

Table 2-1. Installation parameters for Ubuntu (continued)

Installation parameter	Selection or action
*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. **Note**: If a jurisdiction has multiple DesignServers, each one must have a distinct hostname.
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. 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 the console, you will be automatically logged after 15 minutes of inactivity.
*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**.

Table 2-1. Installation parameters for Ubuntu (continued)

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

2.1.4 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.

2.2 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 DesignServer with your user name and password.
2. Insert the ClearDesign DesignServer Application DVD into the disc drive on the computer.

   If you are using a 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 a 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
      ```

      Note: If the install command fails, make sure that the DesignServer is connected with an Ethernet cable to the computer that will be used as a DesignStation or to the network switch if one is used. The DesignStation computer or network switch must be powered on.

   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
      ```

2.3 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 a USB drive, insert it into a port on the computer.
3. Switch to the root:
   ```
   sudo su
   ```

4. Enter your password.
5. To copy the source code, do one of the following. In the following steps, the placeholder *x.x.x* indicates the version.
   a. If you are using a USB drive, enter:
      ```
      mount /dev/sdb1 /media/usb
      cp -r /media/usb/clearDesign-x.x.x.zip .
      ```
   b. If you are using a DVD, enter:
      ```
      mount /dev/cdrom /media/cdrom
      cp -r /media/cdrom/clearDesign-x.x.x.zip .
      ```
6. Enter:
   ```
   unzip clearDesign-x.x.x.zip install
   chmod +x install
   ./install clearDesign-x.x.x.zip
   ```
7. When prompted, enter the URL for the DesignServer (server domain name).
   Enter the value that you specified for the parameter **Configure the network: Hostname**. Alternatively, you can specify a different server domain name if you wish.
8. When prompted, enter the MySQL root user password.
   If you enter the password incorrectly, the installation script exits after third failed attempt.
9. If you are installing ClearDesign for the first time, the system generates a digital certificate for ClearDesign to use. (See "Regenerating a digital certificate" below.) Specify the days until expiration or press **Enter** to accept the default of 365 days.
10. Verify that the installation was successful by noting that the last line of the installation script reads "`SUCCESS" ClearDesign was successfully installed`."
11. Reboot the computer by entering the command:
    ```
    reboot
    ```

2.4 Regenerating a digital certificate

ClearDesign uses digital certificates to encrypt and protect your data. The digital certificate can be valid for 825 days. ClearDesign uses 365 days as a default value.

When the certificate is within 60 days of expiration, the system begins displaying a message on the user's sign in screen that prompts the user to ask their administrator to generate a new certificate.

To regenerate a certificate:

1. Log in to the computer with your user name and password.
2. Enter:

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

3. When prompted, enter the URL for the DesignServer. Enter the value that you specified for the parameter **Configure the network: hostname**.
4. 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 value and generate the certificate.

Chapter 3. Setting up DesignStations

This chapter describes how to set up DesignStations.

3.1 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.

3.2 Installing the Windows 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 3-1).

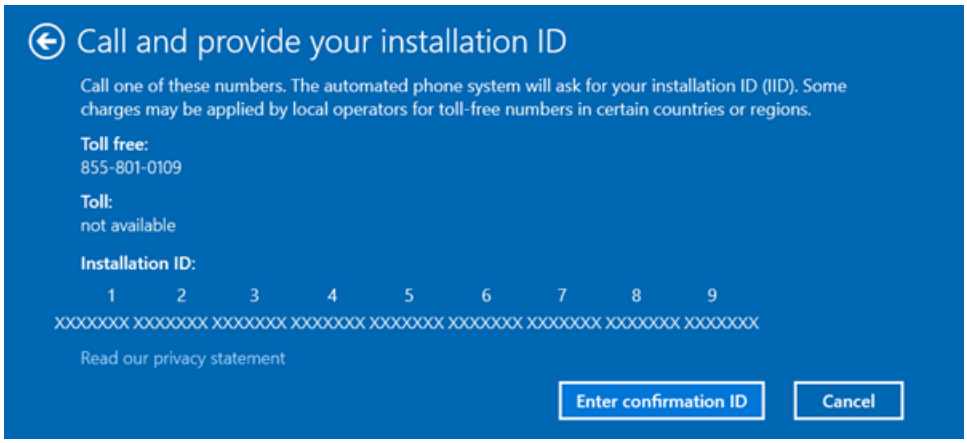


Figure 3-1. Call and provide your installation ID

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 3-2).

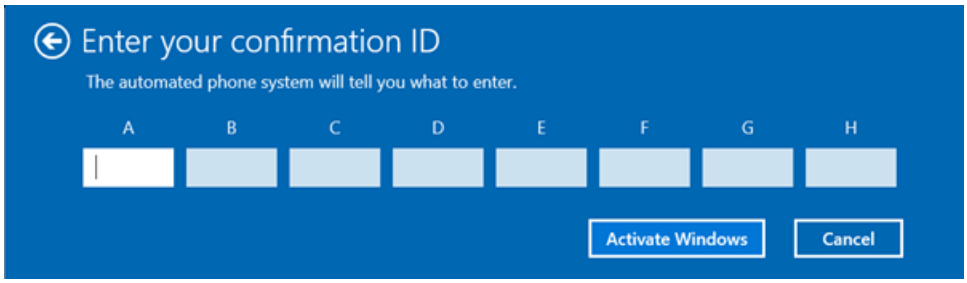


Figure 3-2. Enter your confirmation ID

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

3.3 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 KB4556940:

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

2. Double-click **Windows10.0-KB4556940-x64.msu**.

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

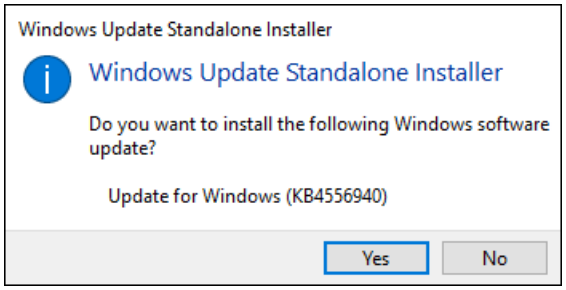


Figure 3-3. Windows Update Standalone Installer dialog—Service stack update

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

   The update takes approximately a minute. When the service stack update is complete, the installation program displays the message shown in Figure 3-4.

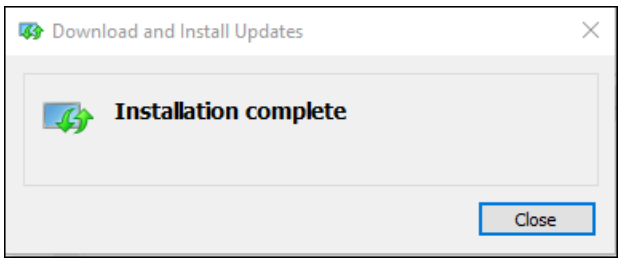


Figure 3-4. Installation Complete message—Service Stack Update

Installing the Windows Updates

To install the Windows updates KB4556813:

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 3-5).

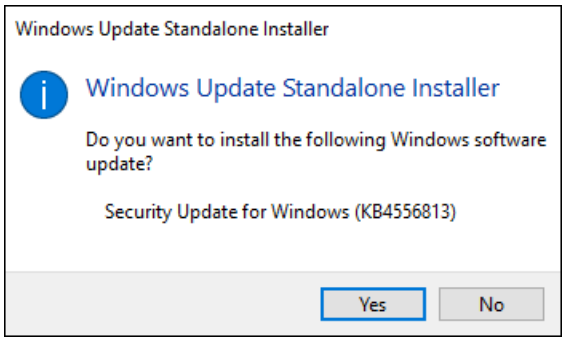


Figure 3-5. Windows Update Standalone Installer dialog—Windows security update

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. lick 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 3-6).

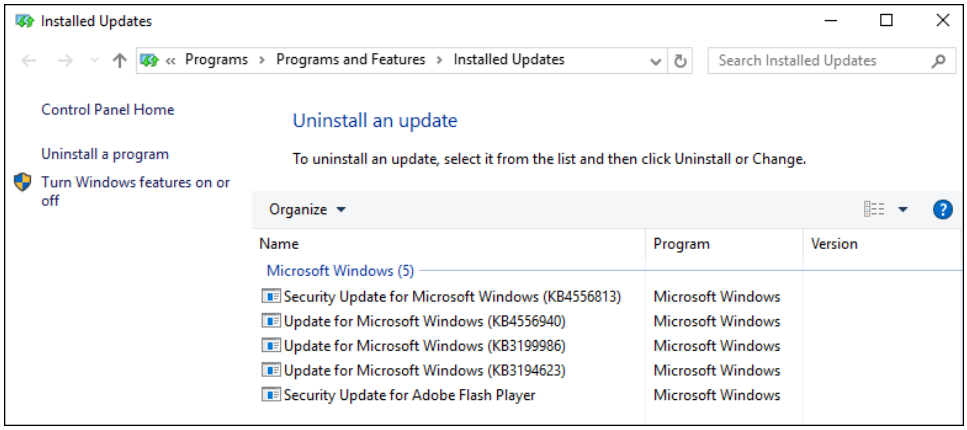


Figure 3-6. Installed Updates dialog

3.4 Installing Windows drivers

Install the following Windows drivers:

- Chipset drivers
- Graphics drivers
- Network drivers

Note: Installing Windows drivers requires restarting the system. Do not restart the computer until you have installed all drivers.

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 on-screen prompts to install each of the drivers in the folder.

   Do not restart the computer after installing the chipset drivers.
4. Open the Graphics folder, double-click each application file and follow the on-screen prompts to install each of the drivers 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 the Windows Updates DVD contains a Network drivers folder for your computer model, double-click each application file and follow the on-screen prompts to install each driver in the folder
6. After installing all drivers, restart the computer.

3.5 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** > **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.

3.6 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.

3.7 Setting up the network switch (optional)

This topic describes how to set up the network switch.

A network switch is required only when a configuration contains multiple DesignStations. If a configuration contains one Design Station and a Design Server, a network switch is unnecessary. In this configuration, an Ethernet CAT cable directly connects the DesignStation to the DesignServer.

3.7.1 Wired connections for ClearDesign

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

- Wi-Fi
- The Internet
- Any external networks

3.7.2 Overview: setting up the network switch

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

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 DesignStation 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

3.7.3 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 3-7 appears, click **OK**.

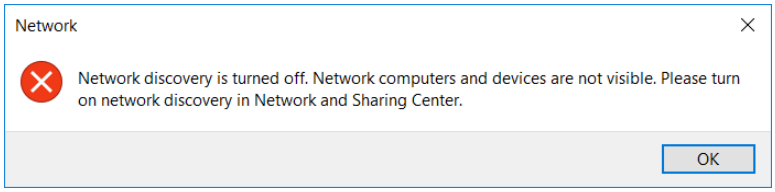


Figure 3-7. Message indicating that network discovery is turned off

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 3-8), select **No, make the network that I am connected to a private network**.

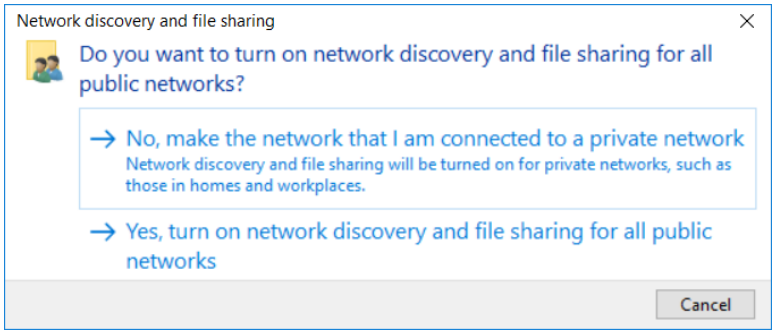


Figure 3-8. Network discovery and file sharing dialog

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.

3.7.4 Configuring the network switch

When you configure the network switch, record the items marked with a red asterisk (*) on the installation checklist in the appendix to this guide.

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.

3.8 Connecting DesignStations to the DesignServer

The method of connecting DesignStations to the DesignServer depends on your configuration:

- If a configuration has a DesignServer and one DesignStation, connect the two computers directly to one another with an Ethernet CAT cable.
- If a configuration has multiple DesignStations that communicate with a DesignServer, connect each computer to the network switch with Ethernet CAT cables.

To enable DesignStations to access the URL for the DesignServer, you must also configure the Ethernet adapter settings.

3.9 Assigning static IP addresses

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

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 assign a static IP address within the range of 192.168.15.2 to 192.168.15.249 to the DesignStation.
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 DesignStation.

3.10 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.

3.10.1 Beginning the installation of the browser certificate

To begin installing the browser certificate for Google Chrome:

1. Navigate to http://<servername> or https://<servername>.

   Google Chrome displays an alert.

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

   The following window appears:

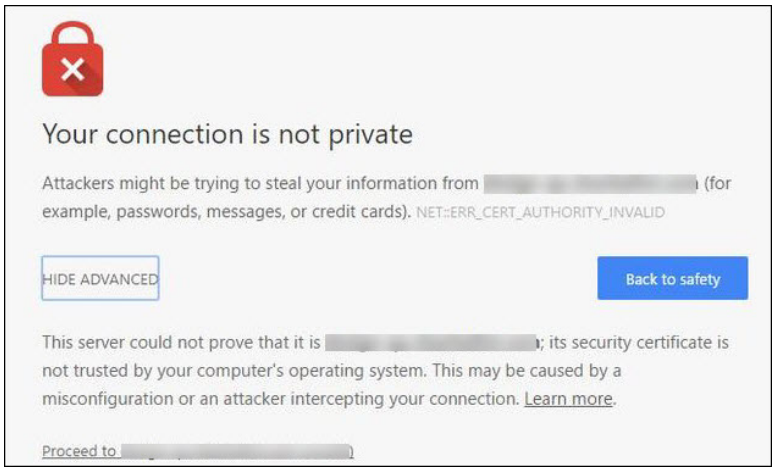


Figure 3-9. The Chrome browser security certificate trust warning.

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

   Google Chrome allows you to access the site, but the address bar shows an exclamation point in a red triangle and a red line through the HTTPS to indicate that the site is not yet validated (Figure 3-10 on page 32).

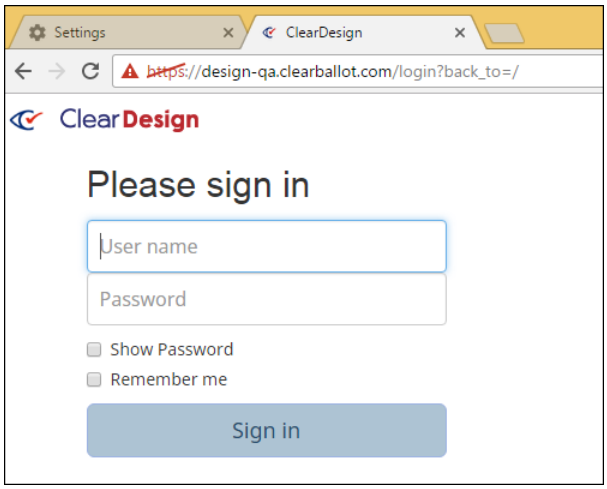


Figure 3-10. The ClearDesign login page.

3.10.2 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 window indicating that your connection is not secure.

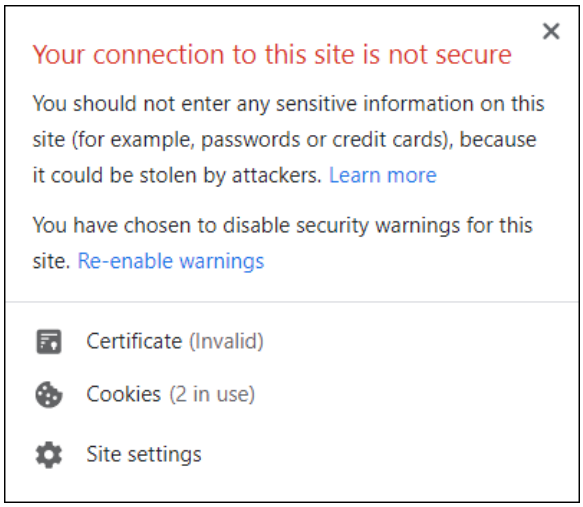


Figure 3-11. The Chrome secure browsing alert dialog

2. Click the **Certificate (Invalid)** link.
3. When the Certificate window appears, click the **Details** tab (Figure 3-12 on page 33).

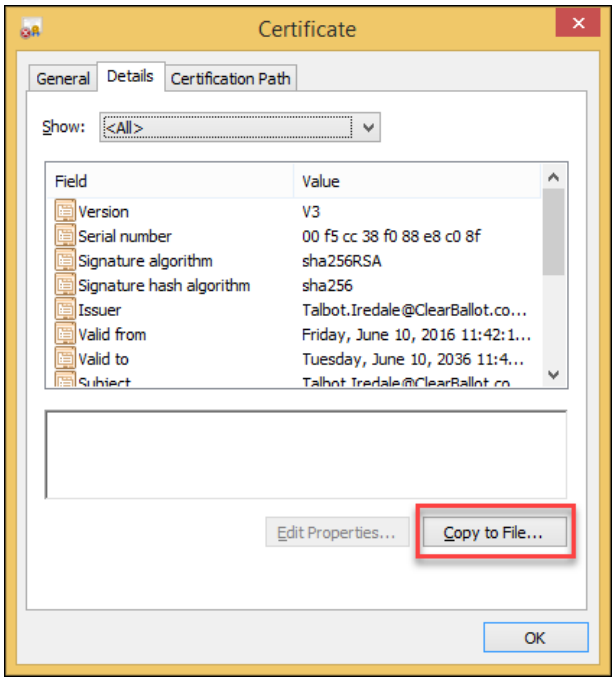


Figure 3-12. The Chrome Certificate window

4. On **Details** tab of the Certificate window, click the **Copy to File** button at the bottom right.
5. When the Certificate Export Wizard appears, click **Next**.

Figure 3-13. The Certificate Import Wizard

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

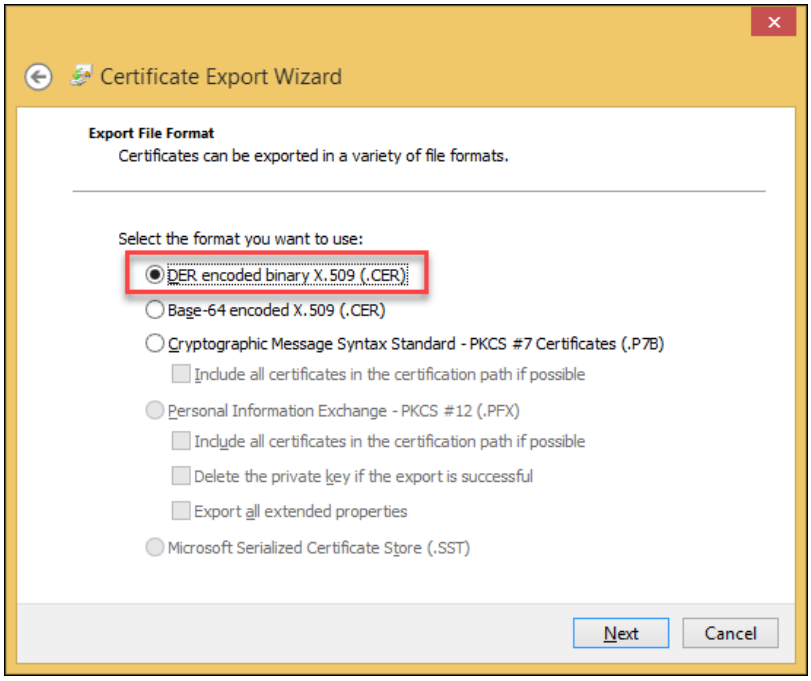
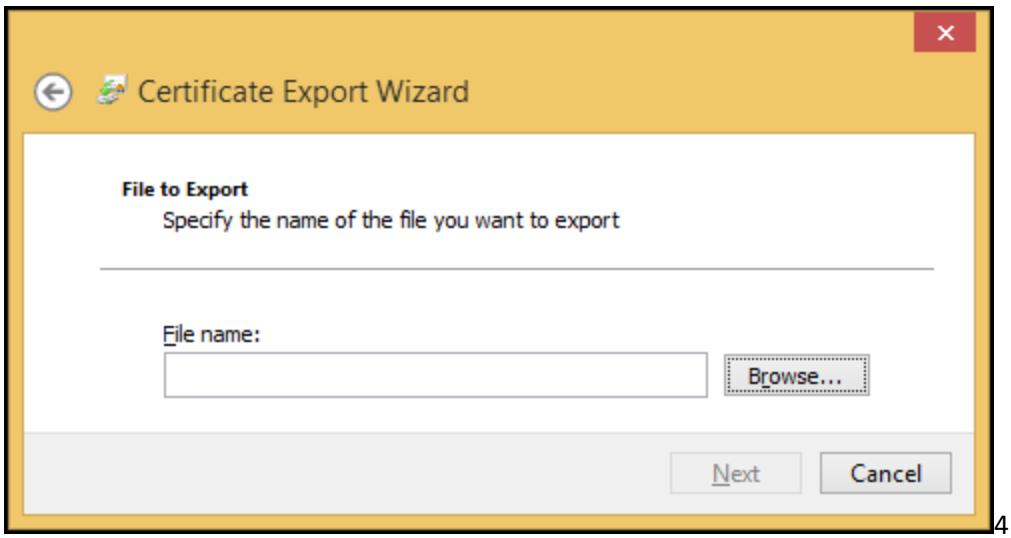


Figure 3-14. The Certificate Import Wizard File Format window

7. 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.



4

Figure 3-15. The Certificate Import Wizard File to Export window

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

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

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

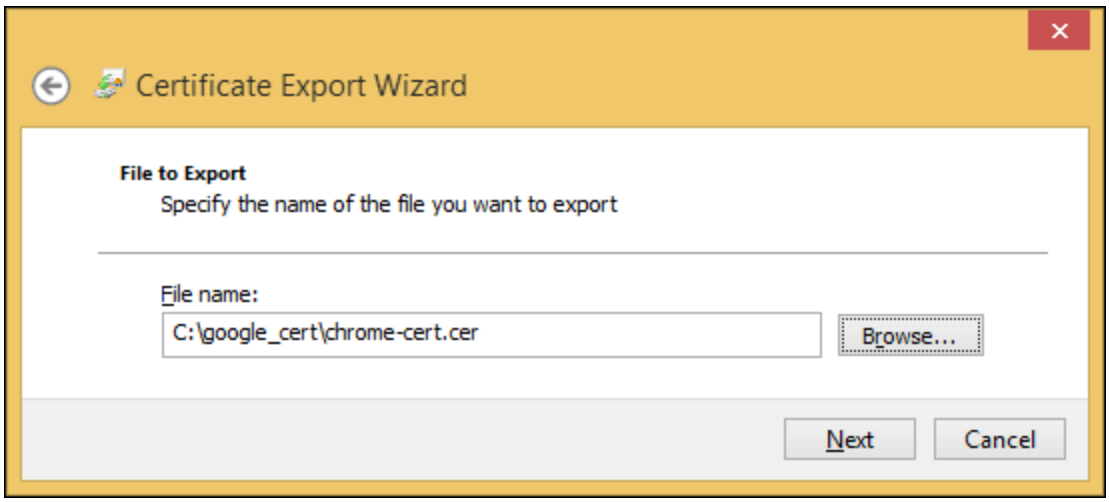


Figure 3-16. The Certificate Export Wizard File to Export window with a file name entered

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

Figure 3-17. The Certificate Export Wizard finish window with summary of settings

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

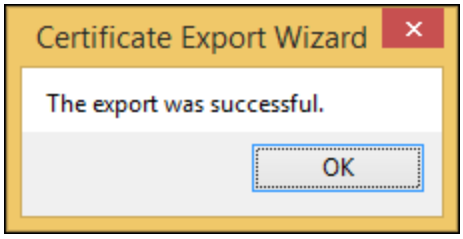


Figure 3-18. The Certificate Export Wizard success dialog

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

3.10.3 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.

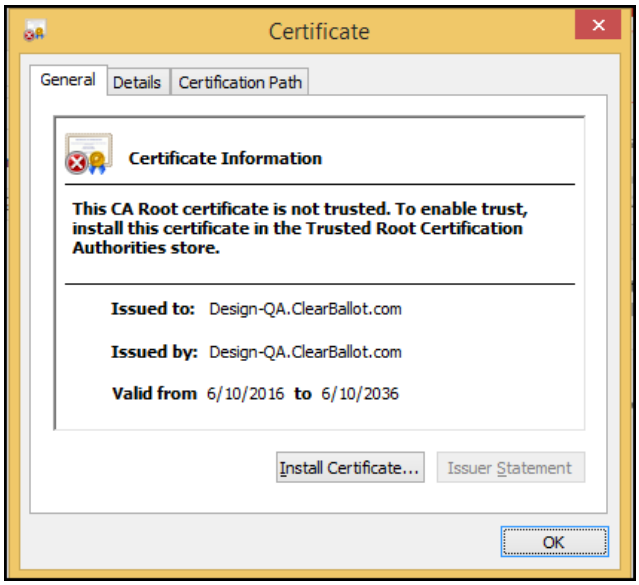


Figure 3-19. The Certificate window

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

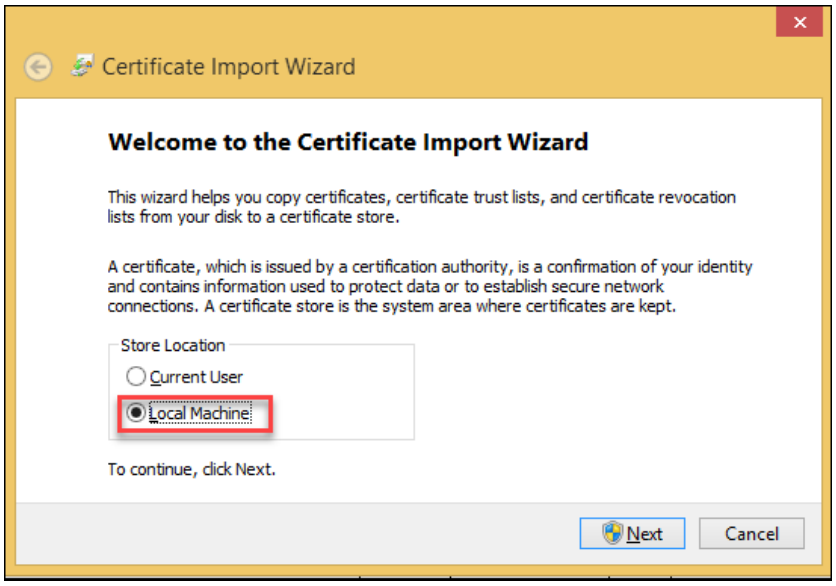


Figure 3-20. The Certificate Import Wizard Store Location window

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.

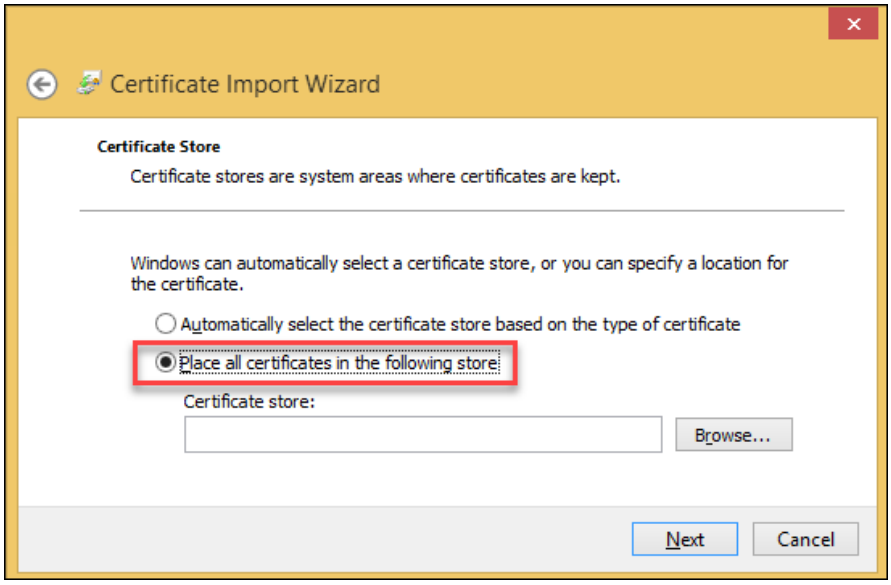


Figure 3-21. The Certificate Import Wizard Certificate Store window

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

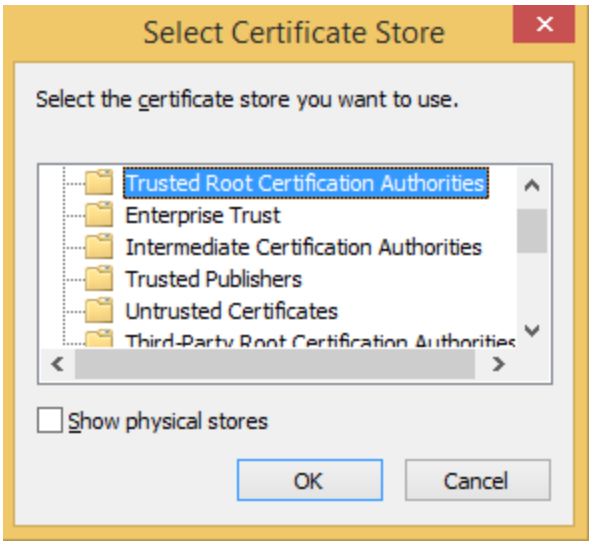


Figure 3-22. The Certificate Import Wizard Select Certificate Store window

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

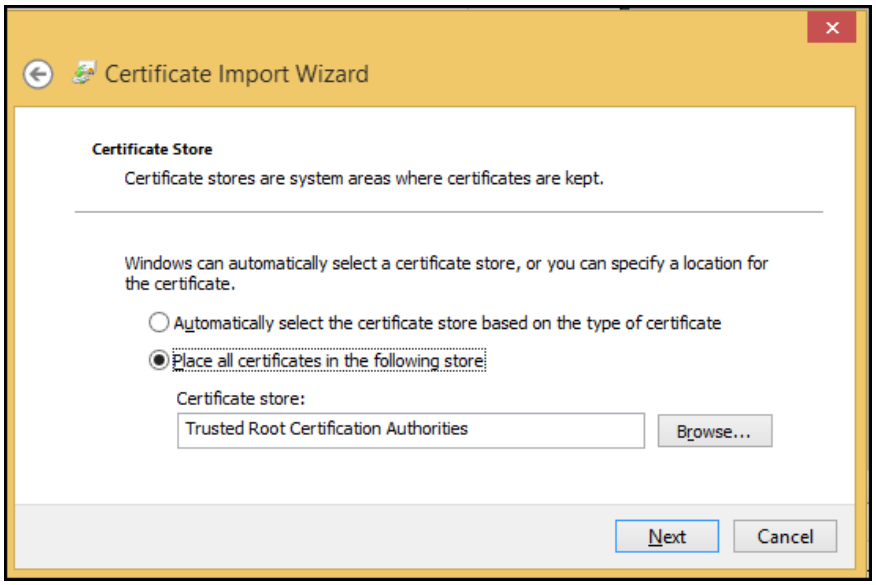


Figure 3-23. The Certificate Import Wizard Certificate Store window

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

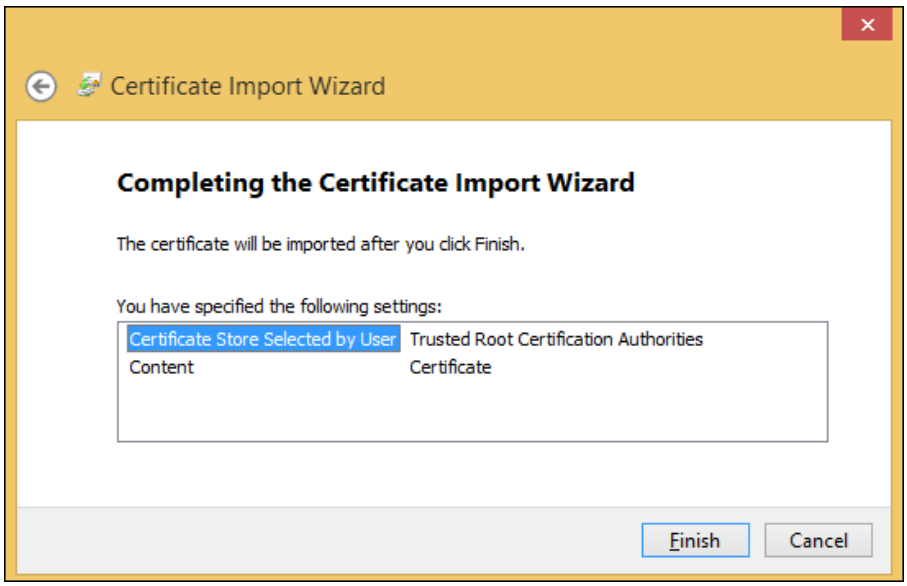


Figure 3-24. The Certificate Import Wizard completed window

Google Chrome displays the following confirmation message.

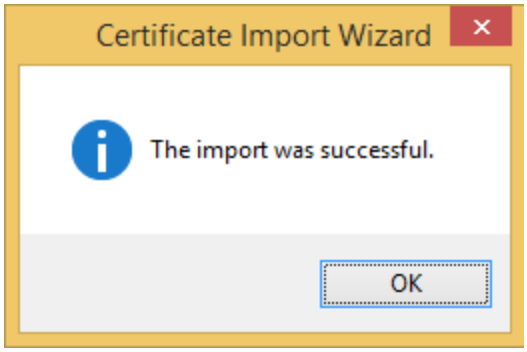


Figure 3-25. The Certificate Import Wizard success window

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 4. Security

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

4.1 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 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

Note: The DesignServer, the network switch, and all data cable connections in the ClearDesign system are security sensitive. Segregate and enforce enhanced security over the DesignServer, the network switch, and the Ethernet cable connections on the closed network.

Place the DesignServer and network switch in a locked computer rack or in a secure area to maintain a proper system security. A jurisdiction must also use cable locks or tamper-evident seals to provide enhanced security for the cable connections.

Figure 4-1 on page 42 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.

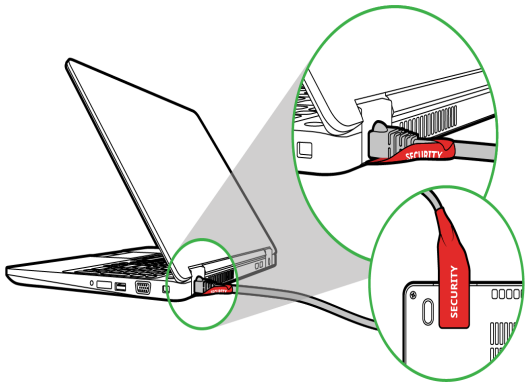


Figure 4-1. A tamper-evident seal attached to an Ethernet cable connection

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 you are using a network switch, 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.

4.2 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 DesignStation 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 ClearDesign 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.

4.3 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 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

4.3.1 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 ClearDesign Harden folder to the DesignStation desktop.
4. Open the ClearDesign 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.

   Note: You must restart the computer for the changes to take effect.

6. Delete the ClearDesign Harden folder from the desktop and empty the recycle bin.

4.3.2 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 50.)

4. To save your changes, click **OK** and then click **Exit**.

5. Restart the computer and verify that the changes have been implemented.

4.4 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.

4.5 Hardening the network switch (optional)

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 (optional)" on page 27.
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.

Note: 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 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 (optional)" on page 27.
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.

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 50.)

5.2 Updating the DesignServer

If you update the DesignServer, you are not required to reinstall Ubuntu.

When updating the DesignServer, use the installation media from the new release.

To install the update:

1. Install the third-party software for the new release on the DesignServer.

   See "Installing third-party software on the DesignServer" on page 14.

2. Install the DesignServer software for the new release.

   See "Installing the DesignServer software" on page 15. When following the steps in this section for an update, you can change the name of the name of the URL (server domain name), if desired.

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 **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 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

See the following topics:

- "Installing Google Chrome" on page 25
- "Installing the browser certificate for Google Chrome" on page 31

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 50.)

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.

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

Table A-1. ClearDesign installation checklist

Network switch (optional): IP address
Network switch (optional): User name
Network switch (optional): 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: