DOMINION VOTING

Our customers come first.

Democracy Suite® ImageCast® Central Installation and Configuration Procedure

Version: 5.2-CO::84

February 16, 2017

NOTICE OF CONFIDENTIALITY AND NONDISCLOSURE

PROPRIETARY NOTICE

RELEVANT DISCLAIMERS

The final list of items to be disclaimed in this release is to be confirmed.
Please be advised that this document may make reference to the following Democracy Suite® functionalities:

- AIMS Data Translator
- Avalue tablets
- EMS Enterprise configuration
- Election Data Exchange Station (EDES)
- ImageCast® Evolution
- ImageCast® Evolution Dual Monitor functionality
- ImageCast® Listener
- ImageCast® Precinct
- ImageCast® Precinct Audio
- ImageCast® Precinct Ballot Marking Device (BMD)
- ImageCast® Precinct BMD Audio
- Rank Choice Voting (RCV)
- Recall Issues
- Mode 2 asymmetric cryptography
- Mode 3 asymmetric cryptography
- NYS General and Primary Ballot Template
- Modem and transmission functionality
- WinEDS Importer

These functionalities are not components of the current Democracy Suite® 5.2-CO certification campaign, and should be disregarded throughout the document.

Revision History

Revision	Date	Author	Summary
84	2017-02-16	brian.fitzsimmons	Set majorrevision to 5.2-CO, set disclaimer to 5.2CO
83	2017-02-15	brian.fitzsimmons	Created 5.2CO branch from 5.2 branch
82	2017-02-09	brian.fitzsimmons	Propset on all .tex files
81	2017-02-08	brian.fitzsimmons	Propset on all .tex files
80	2017-02-07	brian.fitzsimmons	Created 5.2 branch from trunk
79	2017-02-07	brian.fitzsimmons	Revised Adjusting Power Options section
78	2017-02-02	brian.fitzsimmons	Added content for DR-X10C
77	2017-01-27	brian.fitzsimmons	Revised content for M160II and G1130 drivers
76	2016-12-22	brian.fitzsimmons	Revised content
75	2016-12-22	brian.fitzsimmons	Revised content, revised images
74	2016-12-20	brian.fitzsimmons	Adjusted image sizes
73	2016-12-20	brian.fitzsimmons	Revised content for 5.2, updated images
72	2016-12-15	brian.fitzsimmons	Set disclaimer to 5.2
71	2016-12-14	brian.fitzsimmons	Set majorrevision to 5.2
69	2016-11-28	matt.gawlik	Updating scanner settings
68	2016-11-22	brian.fitzsimmons	Merged 5.1 branch changes into trunk
53	2016-09-16	brian.fitzsimmons	Corrected issue with image file names, added new images
50	2016-09-16	brian.fitzsimmons	Edited content, added images
49	2016-09-15	brian.fitzsimmons	Edited content, added images, set disclaimer to 5.1
47	2016-09-08	matt.gawlik	Initial updates for TWAIN and project switching
46	2016-08-17	brian.fitzsimmons	Structural and grammar edits
44	2016-07-15	brian.fitzsimmons	Removed Installing MS Visual C ++ 2013 section. Grammar edits
43	2016-07-14	brian.fitzsimmons	Added content to 2.5.4 and 2.5.5
42	2016-07-11	brian.fitzsimmons	Updated trunk with content from 5.0 branch. Added new images
36	2016-06-07	brian.fitzsimmons	Updated trunk with changes from 5.0 branch
32	2016-05-17	brian.fitzsimmons	Upated trunk with changes from 5.0 branch
22	2016-04-24	brian.fitzsimmons	Edited content after feedback from QA
21	2016-04-22	matt.gawlik	Updated user information and added scan from user information
20	2016-04-20	brian.fitzsimmons	Edited content after feedback from QA
19	2016-04-19	brian.fitzsimmons	Added images, edited content for 5.0 cert
18	2016-04-14	brian.fitzsimmons	Revised cross referenced document names
17	2016-04-14	brian.fitzsimmons	Set disclaimer to 5.0. Minor edits from latest 4.21CO M160II install d ...
16	2016-03-24	xenofon.marangos	Various edits, added diagram
15	2016-03-24	xenofon.marangos	Update master.tex
14	2016-03-24	xenofon.marangos	Added chapter for offline updates
13	2016-03-23	xenofon.marangos	Intro and prep content, various edits, added images
12	2016-03-22	xenofon.marangos	Updated images
11	2016-03-22	xenofon.marangos	Added appendices, propset
10	2016-03-19	xenofon.marangos	Fix rev history
9	2016-03-19	xenofon.marangos	Updated Introduction
8	2016-03-19	xenofon.marangos	Propset
7	2016-03-19	xenofon.marangos	Merge X10C content
6	2016-03-19	xenofon.marangos	Merge M160II content
5	2016-03-19	xenofon.marangos	Merge G1130 content, propset
4	2016-03-19	xenofon.marangos	Propset
3	2016-03-19	xenofon.marangos	Merge ICC app install content
2	2016-03-18	peter	Propset svn:keywords Date, Author, Id, Rev on .tex files.
1	2016-03-18	root	Initial Import

Allowed Authors

subversionID	Firstname Lastname	TitlePosition
brian.fitzsimmons	Brian Fitzsimmons	Documentation Manager
matt.gawlik	Matt Gawlik	Product Manager
peter	Peter Androutsos	Director, PLM
root	root	system
xenofon.marangos	Xenofon Marangos	Senior Systems Manager

Contents

List of Figures

Chapter 1

Introduction

This document describes how to set up the ImageCast® Central hardware, install the ImageCast® Central application software, and all third-party prerequisites.

1.1 Related Documents

The following documents contain information on the operation and maintenance of the ImageCast® Central system:

- *2.02 - Democracy Suite® System Overview*
- *2.08 - Democracy Suite® ImageCast® Central System Operation Procedures*
- *Canon DR-G1130 User Manual*
- *Canon DR-M160II User Manual*
- *Canon DR-X10C User Manual*
- *Democracy Suite® EMS System Installation and Configuration Procedure*
- *Democracy Suite® ImageCast® Central User Guide*

1.2 System Overview

The ImageCast® Central (ICC) is an election ballot tabulator that consists of the following:

- Generic PC: Runs the ICC application software
- High-speed scanner: Converts paper ballots into electronic images
- ICC application software: Controls the scanner and processes the images
- Election Data Files: Informs the application on how to process the images
- iButton security key: Contains cryptographic values in order to decode election files in a secure and controlled manner
- 1-Wire interface device: Allows the application to read the values stored on the iButton
- Network connection: Transmits the results from the application

1.2.1 Hardware Platform

The ImageCast® Central application runs on the following minimum system requirements:

- Intel Core i3-series processor
- Windows 10 Professional 64-bit
- 4 GB of RAM
- 250 GB hard disk
- DVD-ROM drive
- 1 Gbps network adapter (if connected to the EMS network)
- Minimum of 5 USB ports to support the following USB devices:
  - Wired keyboard
  - Wired mouse
  - 1-Wire iButton reader/writer
  - Compact Flash reader or USB removable drive
  - Scanner

The recommended system requirements are:

- Intel Core i5-series processor
- Windows 10 Professional 64-bit
- 8 GB of RAM
- 500 GB or greater hard disk
- DVD-ROM drive
- 1 Gbps network adapter (if connected to the EMS network)
- 2 USB 3.0 ports (for CF reader and scanner)
- 3 or more USB 2.0 ports

The standard ImageCast® Central configuration uses an all-in-one touchscreen PC that meets or exceeds the recommended system requirements. The PC is coupled with a Canon high-speed scanner.

Figure 1.1: ImageCast® Central with Canon DR-X10C

Refer to *2.02 Democracy Suite® System Overview* for more information about the hardware platform.

1.2.2 Software Environment

The ImageCast® Central application runs on the Windows 10 Professional platform. Third-party device drivers and certain Windows Features are also installed.

1.2.3 Network Environment

The ImageCast® Central can be run as a stand-alone unit or as part of the Democracy Suite® EMS network. When connected to the EMS network, the ImageCast® Central saves scanned ballots directly to the EMS Server for tally or adjudication.

The EMS network is comprised of a central server and one or more connected client PCs, ImageCast® Central workstations and a report printer, connected by a passive or managed switch. ImageCast® Central workstations and other client machines are served IP addresses by a DHCP server.

The EMS network can be installed in a **Standard** or **Express** configuration.

The EMS Standard configuration uses server-grade hardware and is connected to an unmanaged network switch. The EMS Standard Server runs Microsoft Windows Server 2012 R2 Standard. At least one EMS client workstation is needed to use the EMS applications.

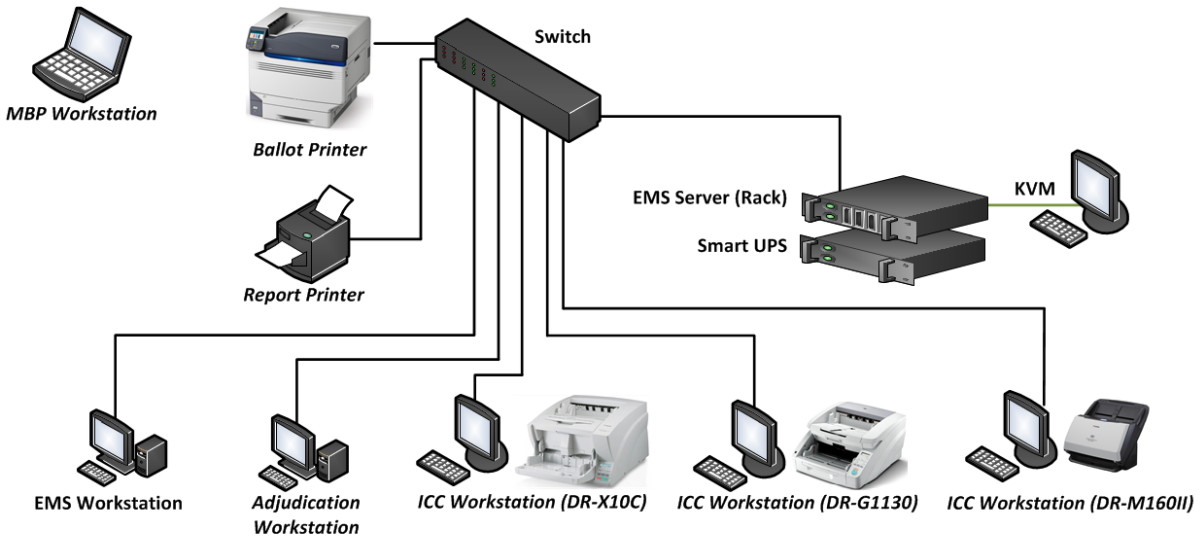


Figure 1.2: Democracy Suite® EMS Standard Configuration

The EMS Express configuration uses a desktop PC running Microsoft Windows 10 Professional. The computer is connected to a managed network switch which provides DHCP and DNS services. All EMS server and client applications are installed on the same machine. Additional client workstations are optional.

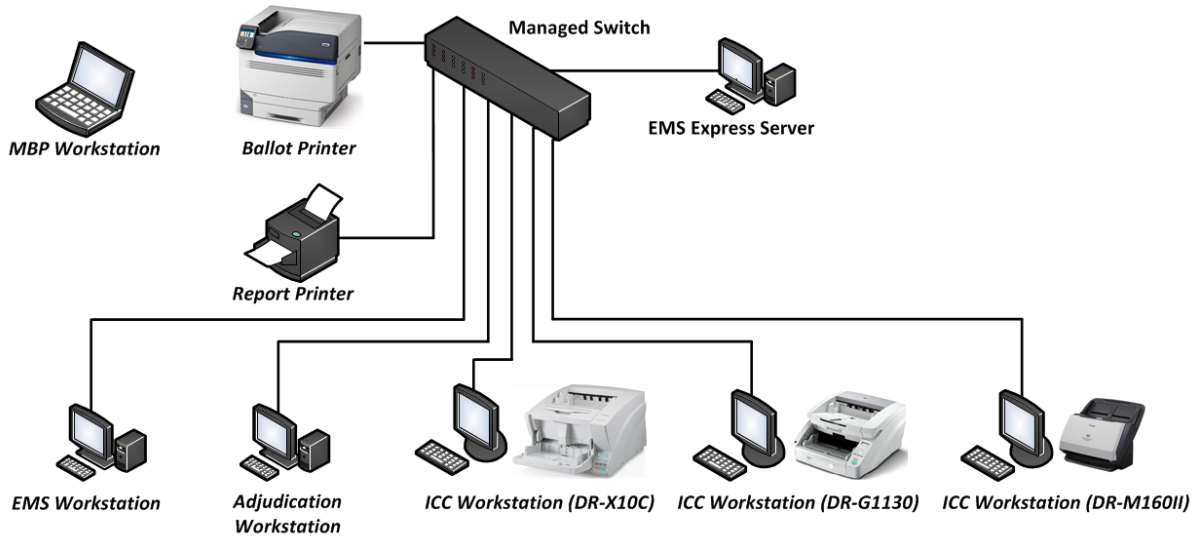


Figure 1.3: Democracy Suite® EMS Express Configuration

1.3 Additional Notes

1.3.1 Choice of Web Browser

The ICC application does not require the use of a web browser, but in order to download the scanner driver software, a web browser is necessary. This document describes the install process when using the Windows Edge browser built into Windows 10 Professional. You may choose to use a different browser, but it will be easier to follow along with the screen shots provided if Windows Edge is used.

1.3.2 User Access Control Prompts

Depending upon the security features installed on Windows, warning dialog prompts may be displayed at various points throughout the installation process. Those prompts may ask for an administrative password, or they may simply ask for confirmation. If presented with a dialog prompt, perform the action that will allow you to proceed, and continue with the installation process.

Chapter 2

Preparing for Installation and Configuration

This chapter describes the equipment and materials needed for the installation procedure and how to prepare them.

2.1 Prerequisites

Gather all of the hardware, software, tools and documentation that is needed for the installation.

Section 2.2 explains how to obtain the required software and documentation.

- Required hardware components:
  - ImageCast® Central computer
  - Canon scanner:
    - DR-G1130
    - DR-M160II
    - DR-X10C
  - Wired keyboard
  - Wired mouse
  - 2 power cables
  - USB-A to USB-B cable
  - Compact Flash card reader
  - 1-Wire iButton reader
- Required software components:
  - Windows 10 Professional 64-bit installation disc
  - Computer manufacturer's device drivers
  - Report printer drivers (Optional)

  - WSUS offline updates
  - Democracy Suite® installation disc
  - TWAIN scanner driver

- Tools and documentation:
  - Canon scanner user manual
  - Removable medium to transfer downloaded files
  - Spreadsheet or other document to record the machine names, IP addresses, user names, passwords and other important system information that will be entered throughout the course of the installation procedure.
  - Test election files and programmed iButton security key
  - Test ballots

2.2 Obtaining Software and Documentation

NOTE: Each jurisdiction has specific procedures for obtaining certified software and documentation packages. Consult your jurisdiction's voting systems certification authority for more information.

- Democracy Suite® installation disc:
  - ImageCast® Central software
  - Third-party prerequisites (Microsoft Visual C++ Redistributable 2013 (x86), Maxim 1-Wire iButton driver)
  - Windows hardening templates

  The following are provided by Dominion Voting, VSTL or certification authority:

- Windows 10 Professional 64-bit installation disc: License and installation media included with the computer
- Computer manufacturer's device drivers: Downloaded from the manufacturer's website or provided by Dominion Voting
- Report printer drivers (optional): Downloaded from the manufacturer's website, or installed from the included disc
- WSUS offline updates: In Section 5.2.1, WSUS offline updates must be installed. The update utility is downloaded from `http://download.wsusoffline.net/`
- Scanner driver: Can be installed from the driver disc included with the scanner, or downloaded from the manufacturer's website.

2.3 Network Planning

NOTE: This section applies to networked configurations only.

Before installing the ImageCast® Central system, the EMS Administrator should have a clear understanding of the network topology and have a plan for what machine names and user accounts will be on each system.

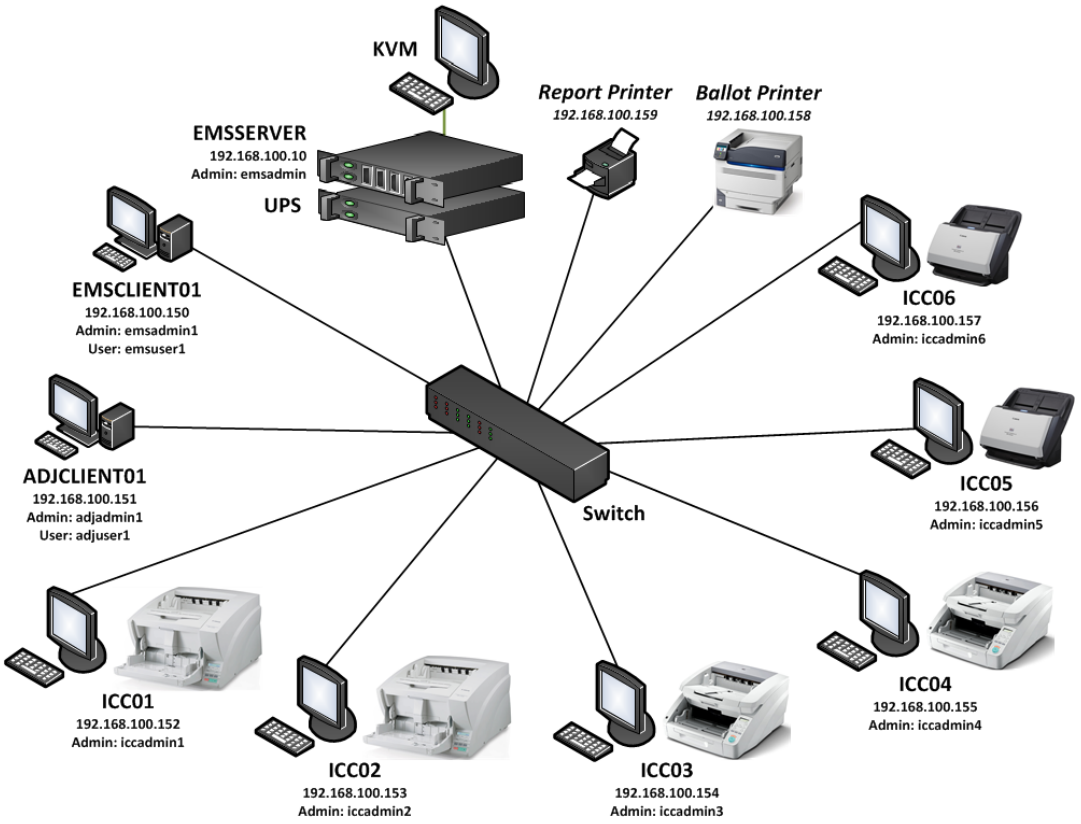


Figure 2.1: Democracy Suite® EMS Network Example

Refer to *2.02 Democracy Suite® System Overview* and *Democracy Suite® EMS Installation and Configuration Procedure* for more information about the EMS network.

2.4 User Accounts

Each ImageCast® Central machine must have at least one Windows administrator, who is the primary administrator of the system. In most cases this is the same person who performs the EMS Administrator role. Refer to *Democracy Suite® EMS Installation and Configuration Procedure* for more information on user accounts.

Additional users accounts can be created for other users of the system on each machine. Only those who should have the ability to configure and modify ICC and its files should be members of the Administrators group. Other users should be members of the Users group.

2.4.1 Accessing the EMS Server

To allow the ImageCast® Central application to connect to the EMS Server, the same user names and passwords used on the ICC should exist on the EMS Server as well. The user names and passwords must match on EMS Server and the ICC machines. User names are case sensitive.

Refer to *Democracy Suite® EMS Installation and Configuration Procedure* for more information on enabling sharing with the ImageCast® Central Workstation.

2.5 Passwords

2.5.1 Strong Passwords

Strong password definition featuring at least 14 characters. For example, **Password123abc!**.

2.5.2 Password Policy

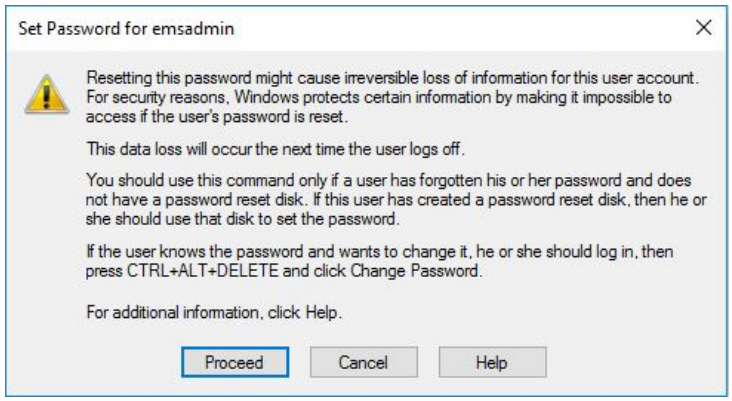
The following is the recommended password policy. The password must:

- Contain at least 14 characters
- Contain characters from at least three of the following categories:
  - Uppercase letters (A, B, C, etc.)
  - Lowercase letters (a, b, c, etc.)
  - Numbers (0, 1, 2, etc.)
  - Non-alphanumeric characters such as: `. _ ! $ & *`
- Not contain the words “Administrator” or “Admin” related to usernames or account/role names

NOTE: The policy is enforced when the hardening template is applied.

2.5.3 User Password Reset

If you have forgotten a user’s password or need to force a reset, reset the password:



1. To reset the password, right-click the created user, and click **Set Password**.
2. The *Set Password for test* screen appears.
3. Read the instructions, and click **Proceed**.

Figure 2.2: Set Password for emsadmin Screen

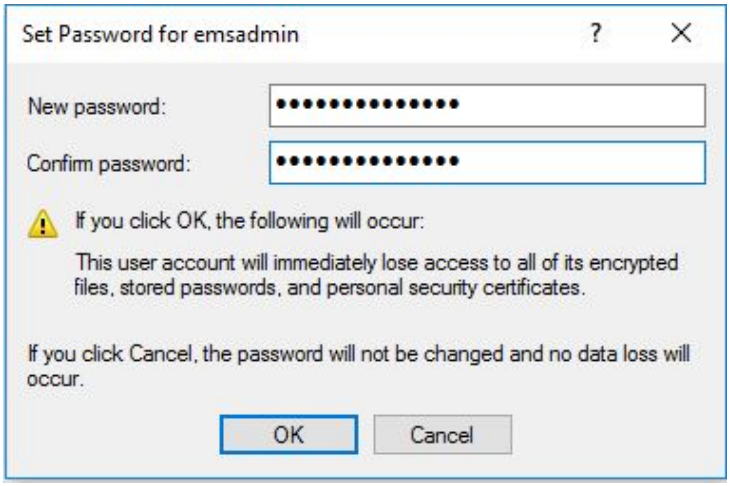


Figure 2.3: Set Password for emsadmin Screen

4. Add a new password and confirm it.
5. Click **OK**.

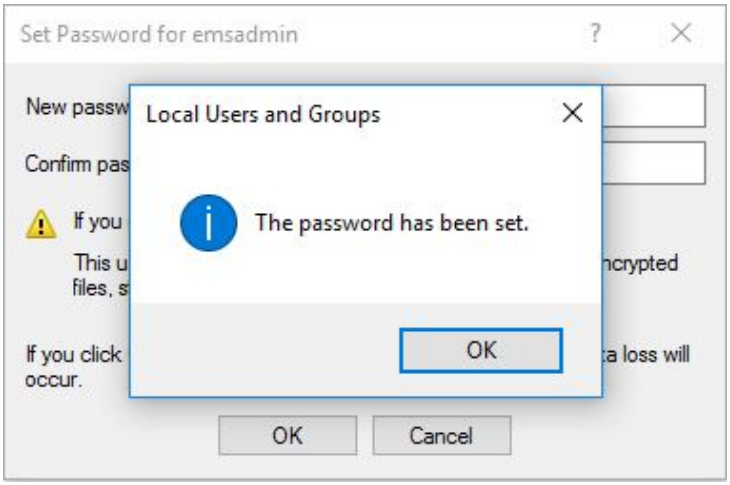


Figure 2.4: Local Users and Groups Screen

6. The **Local Users and Groups** window appears.
7. Click **OK**.
8. The new password is set.

2.5.4 Setting Password Reset at Next Login

1. Right-click the **Windows** button and then click **Computer Management**.
2. The **Computer Management** window appears.
3. Expand **System Tools** and then expand **Local Users and Groups**.
4. Click **Users**.
5. From the right-hand pane, right-click the user name that requires the password reset and click **Properties**.
6. The **Properties** window appears.
7. From the **General** tab, confirm the **User cannot change password** and **Password never expires** check boxes are cleared.
8. Select the **User must change password at next logon** check box.
9. Click **Apply** then click **OK**.
10. Close the **Computer Management** window.

2.5.5 BIOS Password

If the BIOS of the computer can be accessed, the "first boot device" setting can be changed. A password of at least 8 characters should be implemented to prevent this. Dominion Voting Systems recommends that the password contain a combination uppercase and lowercase letters. Adding special characters increases the password's resistance to brute force.

Chapter 3

Hardware Setup

This chapter covers the hardware setup for the ImageCast® Central system.

3.1 Prerequisites

To begin setting up an ImageCast® Central workstation, gather the following hardware equipment in the installation location:

- ImageCast® Central computer
- Canon scanner:
  - DR-G1130
  - DR-M160II
  - DR-X10C
- Wired keyboard
- Wired mouse
- 2 power cables
- Power strip or UPS
- USB-A to USB-B cable
- Compact Flash card reader
- 1-Wire iButton reader

Place the ImageCast® Central computer in an area where there is enough space for the scanner and stacks of ballots to be processed through the scanner. Place the scanner next to the computer.

3.2 Connecting the Devices

1. Connect the power cables provided to the UPS device or to a power strip (if you do not have a UPS device).
2. Connect the keyboard and mouse to the USB 2.0 ports on the computer.
3. Connect the Compact Flash card reader to the USB 3.0 ports on the computer, if available.
4. Connect the network interface on the computer to the switch using the CAT5e or CAT6 cables provided.

   NOTE: If the ImageCast® Central workstation is being deployed as a stand-alone unit, do not connect the network interface to the switch.
5. **DO NOT** connect the scanner to the computer at this time.
6. **DO NOT** connect the 1-Wire iButton reader to the computer at this time.

3.3 Initial BIOS Configuration

Before the operating system installation can begin, some initial configuration steps must be performed on the computer's BIOS.

- All installations should begin with a correct and known BIOS configuration. To ensure that the BIOS configuration is correct, perform a factory reset on the BIOS settings, restart the computer and then apply the appropriate settings.
- Before the operating system installation starts, the computer's boot mode should be set to **UEFI mode**. It is also recommended that the **Secure Boot** feature be enabled, if available.
- Wireless peripherals and network interfaces are not used with the Democracy Suite® system. On-board wireless adapters can be disabled from the BIOS menu.

Instructions for performing these initial configuration steps for **Dell** computers can be found in Appendix A, Section A.1.

Chapter 4

Operating System Installation

This chapter covers the installation of the Windows 10 Professional operating system for the ImageCast® Central Workstation.

4.1 Installing Windows 10 Professional

Use the following procedures to install and configure Windows 10 Professional.

1. Insert the Windows 10 Professional installation disc into the DVD-ROM drive.
2. Restart the system.
3. While booting, press the **Boot Options** key (**F12**) to enter the boot menu.
4. Select the option to boot from the DVD-ROM drive.

5. When prompted, press any key to boot from the disc.

Figure 4.1: Windows 10 Installation Boot From Disc

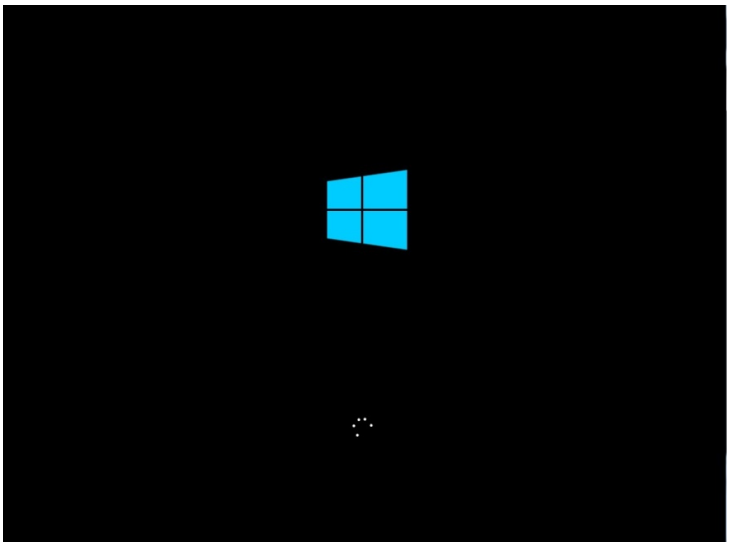


Figure 4.2: Windows 10 Installation Loading Files

6. The system begins loading the files.

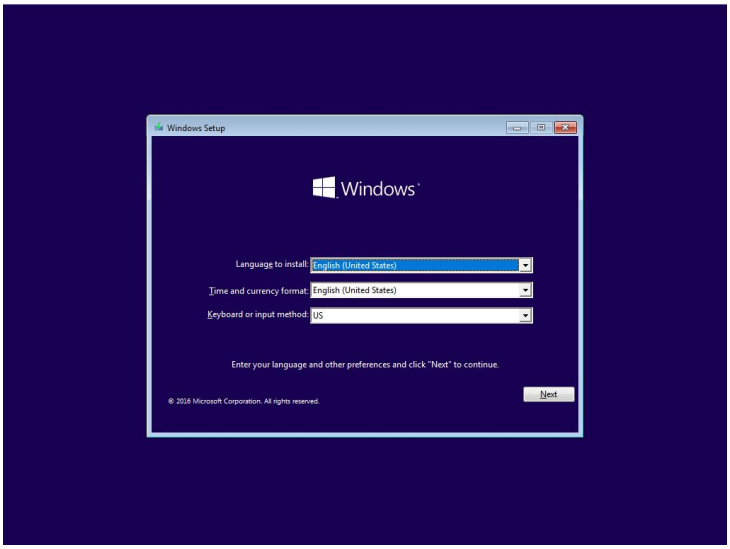


Figure 4.3: Windows 10 Installation Adjust Local Settings

7. After the workstation boots up, the **Windows Setup** screen appears.
8. Review the Windows 10 installation settings:
    - Set **Language to install** to **English (United States)**
    - Set **Time and Currency Format** to **English (United States)**
    - Set **Keyboard or input method** to **US**
9. Click **Next**.

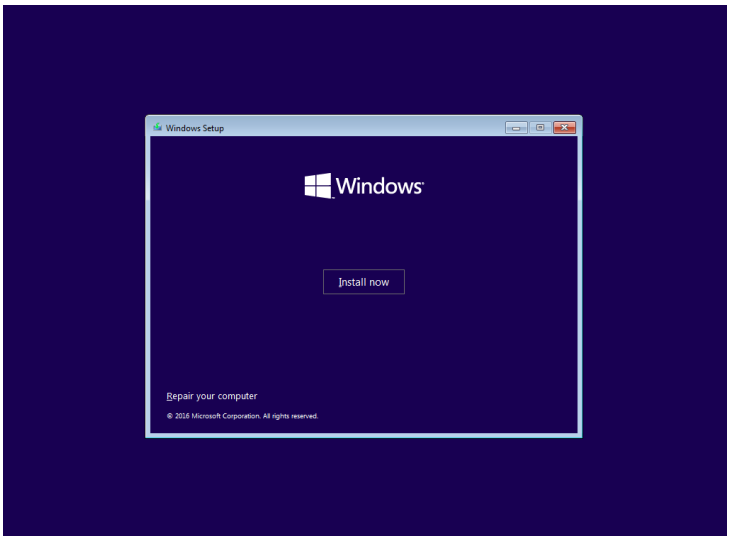
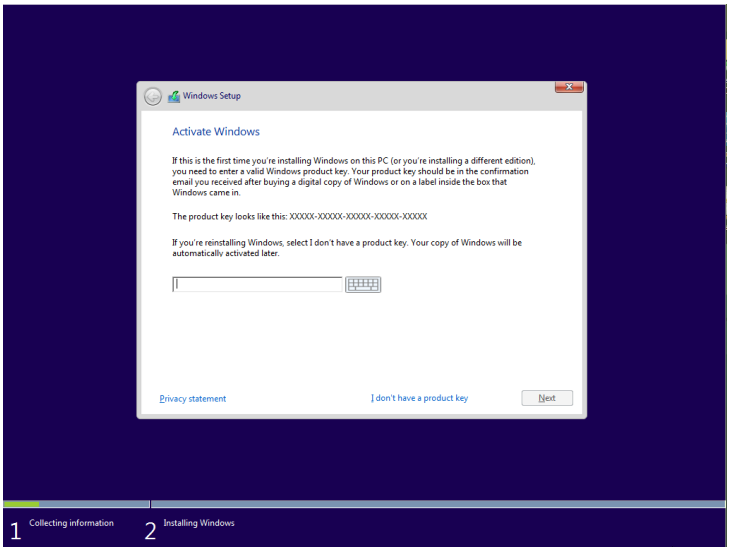


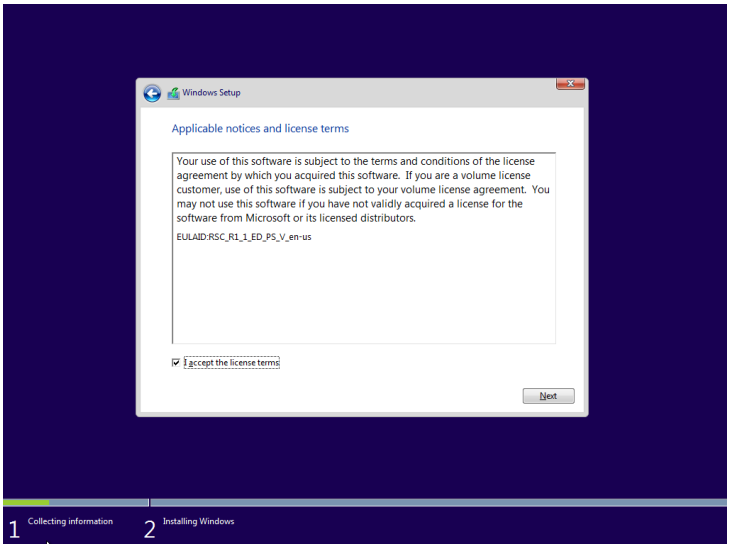
Figure 4.4: Windows 10 Installation Install Now

10. Click **Install Now**.



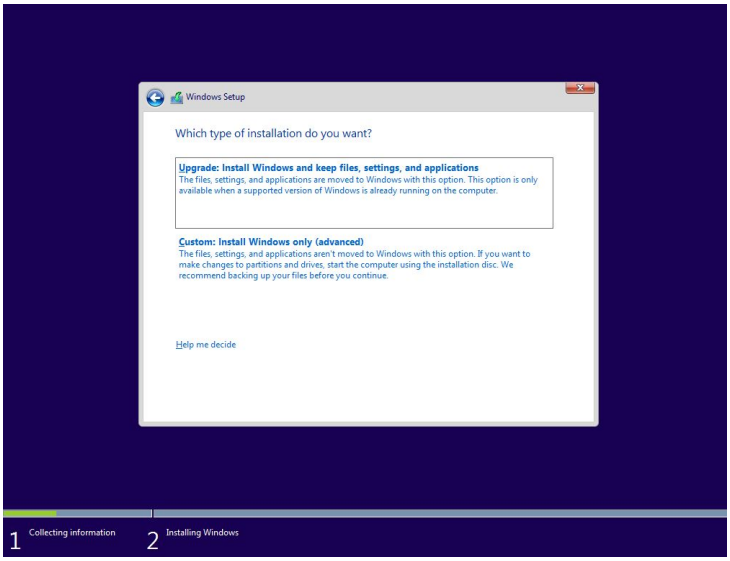
11. Depending on your version, the **License key** screen may appear. Type the product key, and click **Next**.

Figure 4.5: Activate Windows



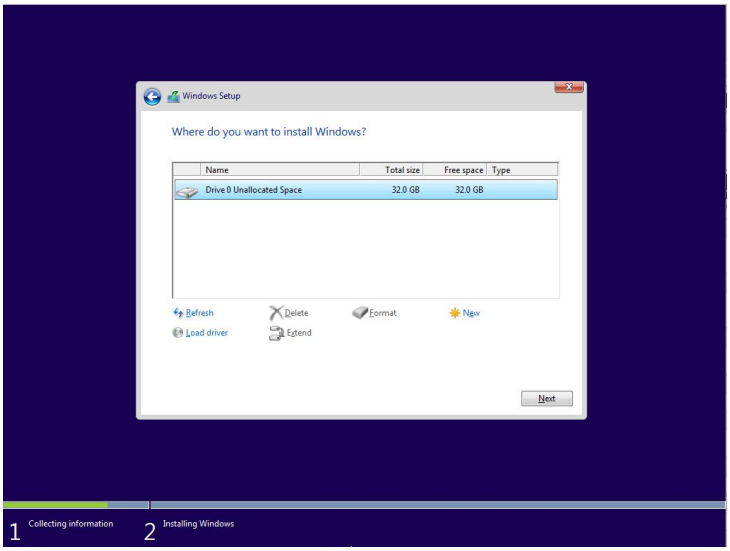
12. The **License Terms** screen appears.
13. Accept the terms of the End-User License Agreement, and click **Next**.

Figure 4.6: Windows 10 Installation License Terms



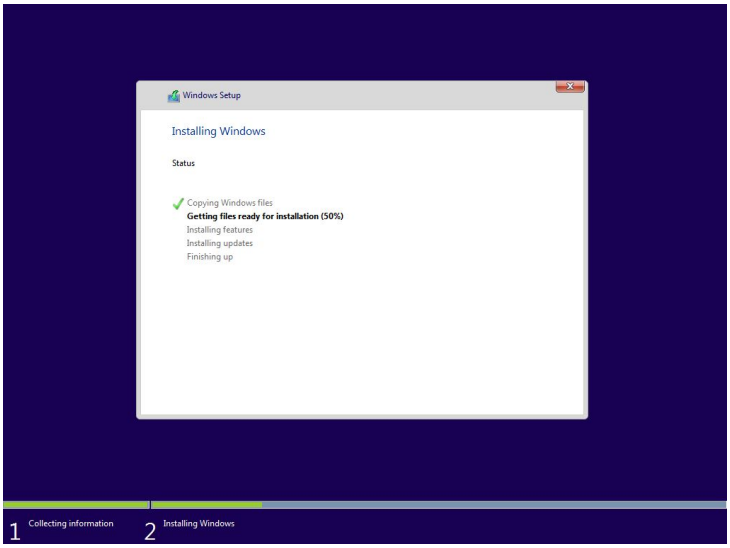
14. The **Installation Type** screen appears.
15. Click **Custom Installation option**.

Figure 4.7: Windows 10 Installation Type



16. In the **Windows Setup** screen, select one drive and click **Delete**. Repeat this step until there are no more drives to delete and **Drive 0 Unallocated Space** is the only option that appears.
17. Click **Next**.

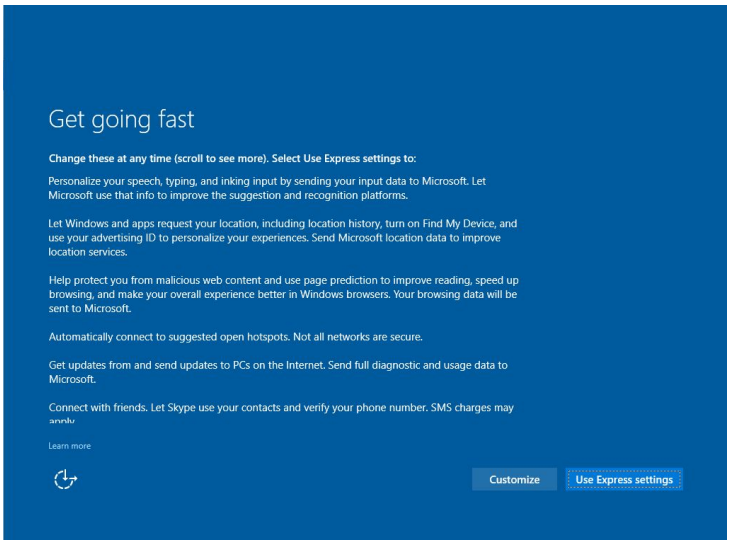
Figure 4.8: Windows 10 Installation Storage Management



18. The Windows 10 installation begins, and the following screen shows the progress of the installation.

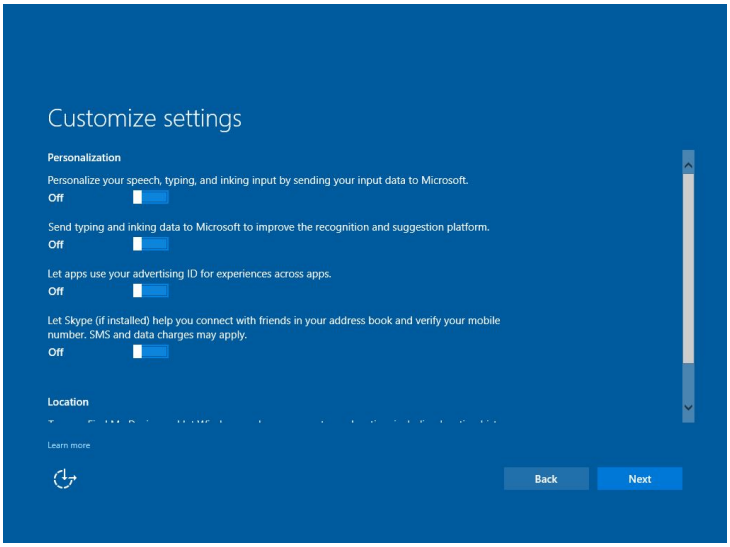
    NOTE: The system may reboot several times.

Figure 4.9: Windows 10 Installation Progress Screen



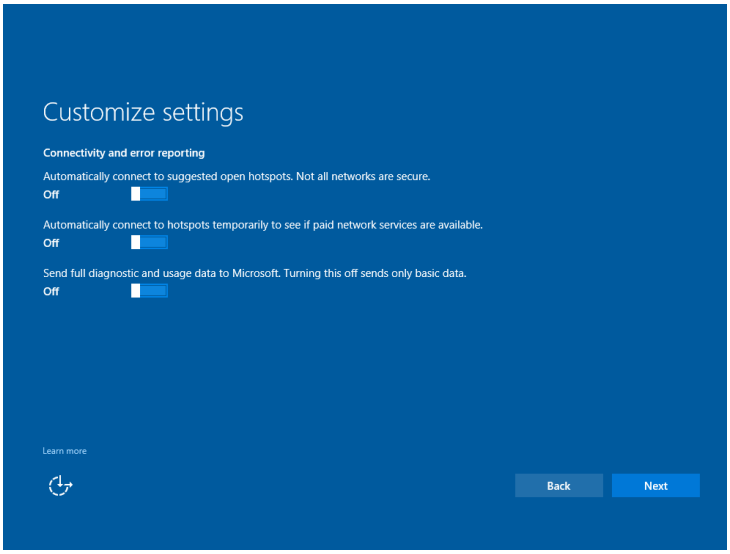
19. If the **Lets get connected** screen appears, click **Skip this Step**.
20. Click **Customize**.

Figure 4.10: Windows 10 Installation Get going fast Screen



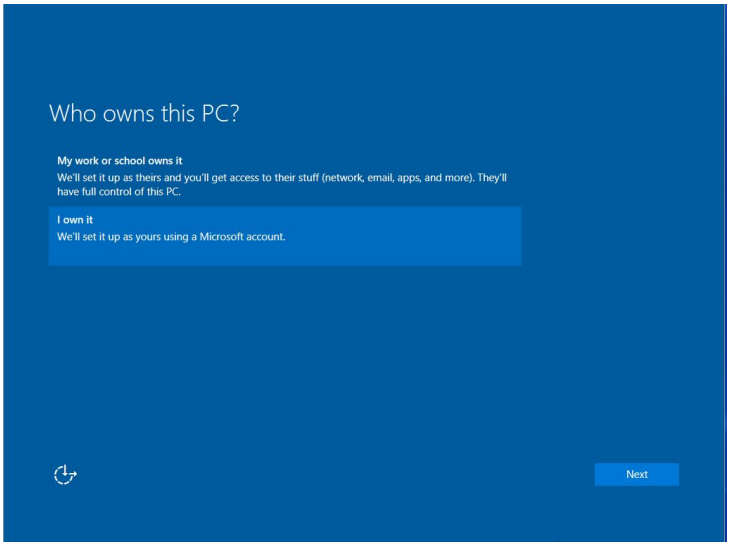
21. In the **Customize Settings** window, set all options to **Off** and then click **Next**.

Figure 4.11: Customize settings window



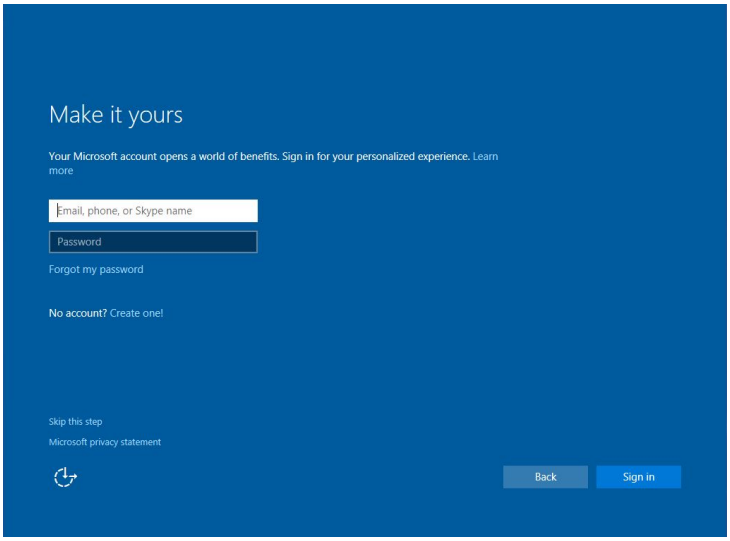
22. In the **Customize Settings** window, set all options to **Off** then click **Next**. Repeat the process if additional settings appear.

Figure 4.12: Continued customize setting window



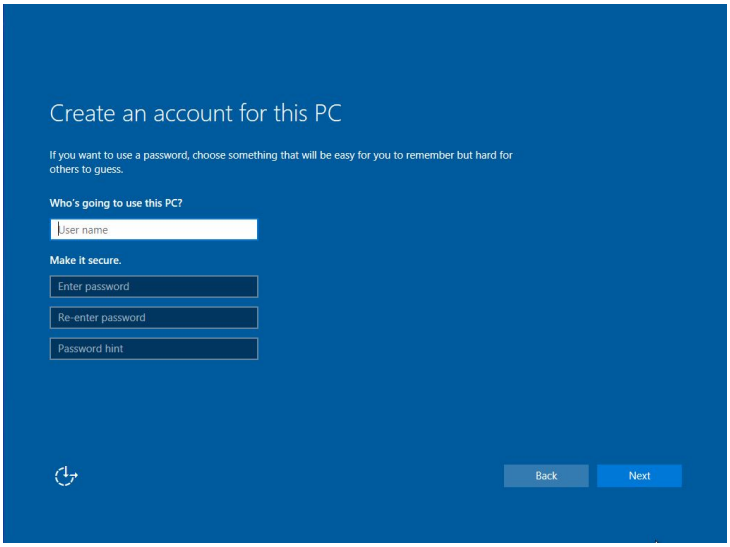
23. If the **Who owns this PC** window appears, select **I own it** and click **Next**.

Figure 4.13: Who owns this PC screen



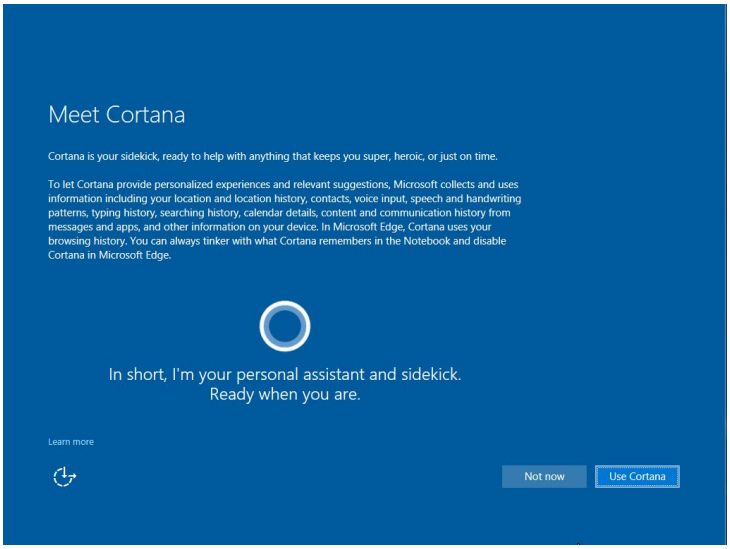
24. If the **Make it yours** screen appears, click **Skip this step**.

Figure 4.14: Make it yours screen



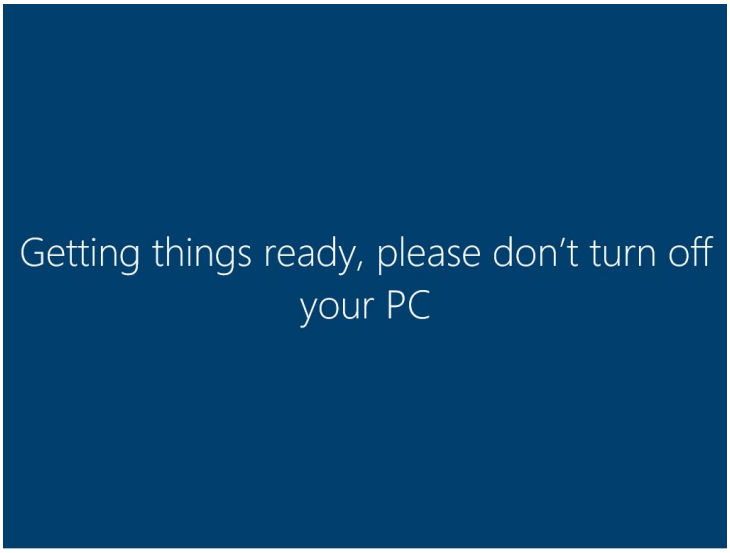
25. In the **Create an Account for this PC** window, type a user name (for example, iccadmin1), a strong password of at least 14 characters, set a password hint,
26. Click **Next**

Figure 4.15: Create an Account for this PC screen



27. In the **Meet Cortana** screen, click **Not now**.

Figure 4.16: Meet Cortana screen



28. It may take a few moments for Windows to start.

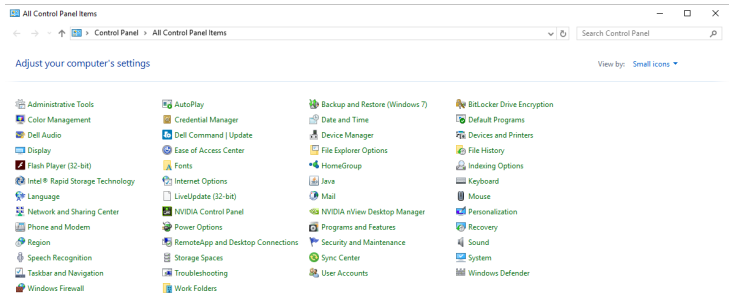
Figure 4.17: Windows Setting up for the first time

Chapter 5

Operating System Updates

This chapter covers the configuration and installation of operating system updates for Windows 10 Professional after it has been installed.

5.1 Disabling Automatic Updates



1. From the Windows desktop, right-click the **Start** menu and click **Control Panel**.
2. In the **View by** field, select either **Large icons** or **Small icons** if the screen has not already been set.
3. Click **Administrative Tools**

Figure 5.1: Configuring Windows Updates - Control Panel Screen

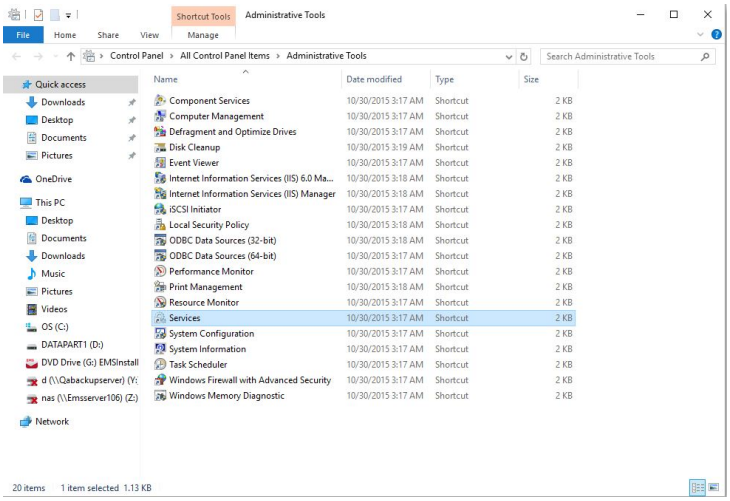


Figure 5.2: Administrative Tools screen

4. Click **Services**.

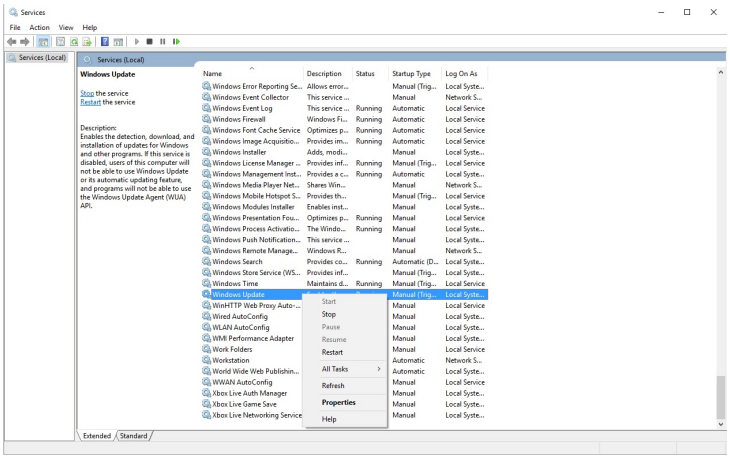


Figure 5.3: Services window

5. Locate and right-click **Windows Update** then click **Properties**.

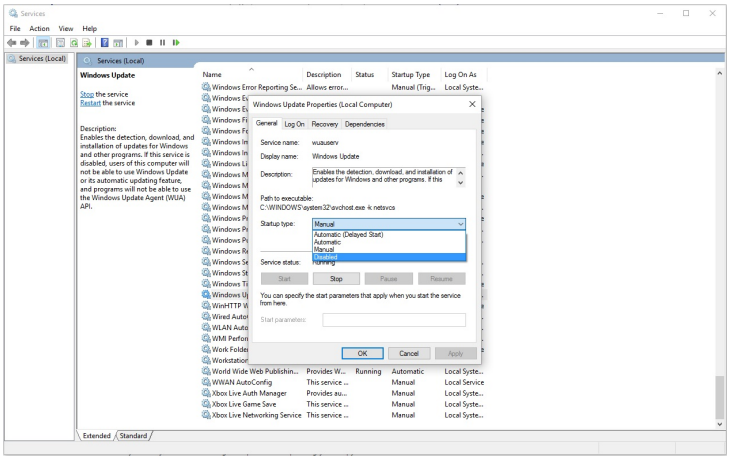


Figure 5.4: Windows update properties window

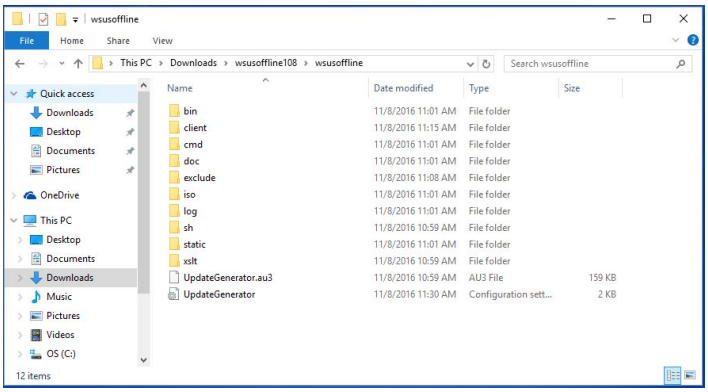
6. Click **Disabled** from **Startup type** dropdown menu and click **Ok**.
7. Close all windows.

5.2 WSUS Offline Updates

This section outlines the procedures for obtaining the security updates and patches for Windows 10 Professional. Microsoft publishes these updates through its online service called Windows Update. However, since the system works in a closed environment without internet access, an alternate tool called WSUS Offline Update must be used. This procedure requires a separate, internet-connected computer which is used to stage the security updates and patches and then transfer them to the offline machines.

5.2.1 Downloading WSUS Offline Updates

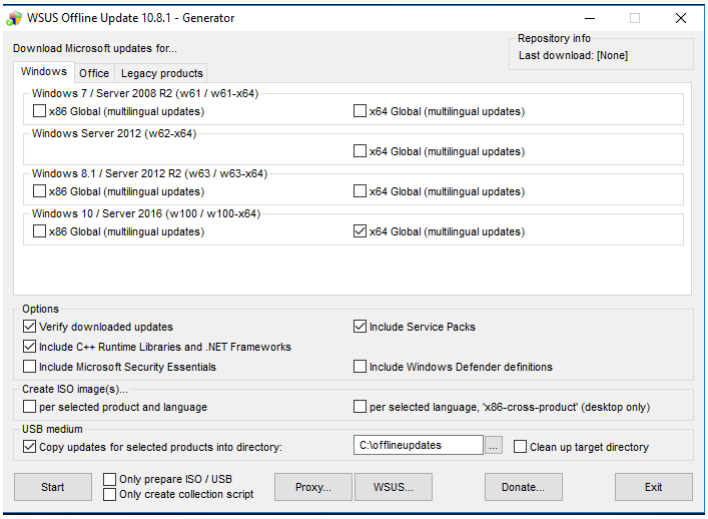
1. On a separate, internet-connected computer, download version 10.8.1 of WSUS Offline update from `http://download.wsusoffline.net/`.



2. Unpack the zip archive to a folder of your choice, and run **UpdateGenerator.exe**.

   NOTE: If you receive a Windows UAC prompt, accept it to access the WSUS Offline.

Figure 5.5: WSUS Offline - Unpacked folder Screen



3. The **WSUS Offline Update** window appears. Under **Windows 10 / Server 2016 (w100 / w100-x64)**, select the **x64 Global (multi-lingual up- dates** check box.
4. Under **Options**, select the **Verify downloaded updates**, **Include Service Packs**, and **Include C++ Runtime Libraries and .NET Frameworks** check boxes.
5. Select **Copy updates for selected products into directory** and select a folder you want to download the updates to.
6. Verify all options match those selected in Figure 5.6, and click **Start**.

Figure 5.6: WSUS Offline - Main window settings Screen

7. When asked to update WSUS Offline Update click **No**.
8. If the program prompts you to update to latest Trusted Root Certificates, click **Yes**.

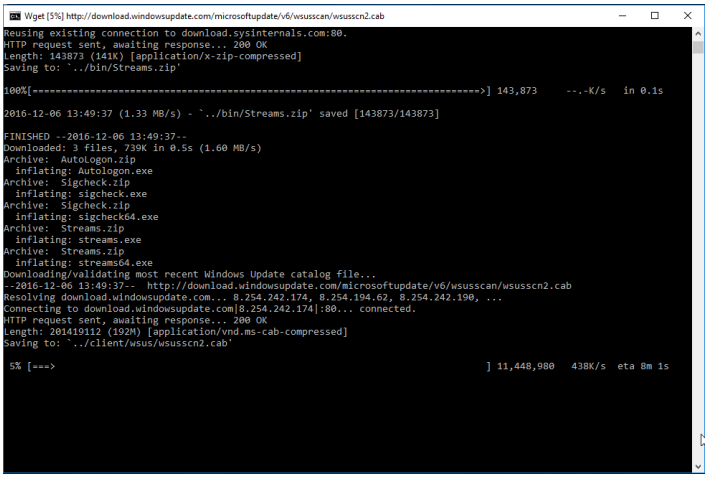


Figure 5.7: WSUS Offline - Update Download of security updates and patches Screen

9. WSUS Offline opens a **Command Line** window to download required updates. Please be patient and wait for all updates to be downloaded.

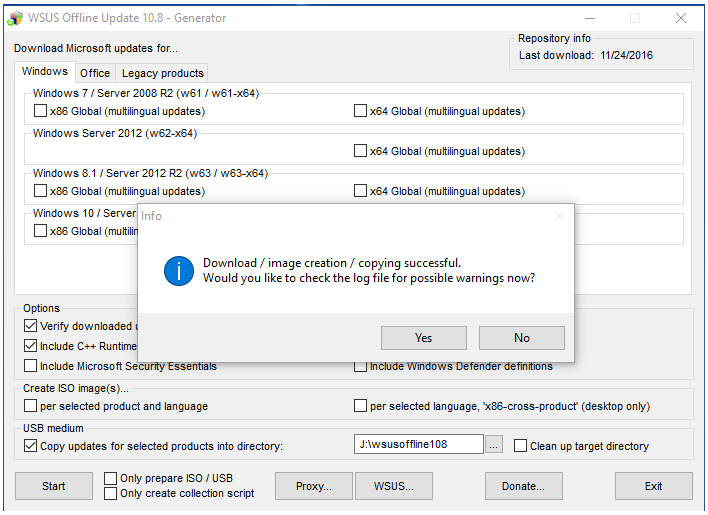


Figure 5.8: WSUS Offline - Download completed Screen

10. Once WSUS Offline completes the download, the command line window automatically closes, and you are prompted to review the log file. Click **Yes** to view the log, or click **No** to proceed without viewing the log, and close the program.
11. Obtain a USB Flash drive of at least 4 GB free space, and copy the entire folder containing the downloaded upgrades that you specified previously in the Main window settings.
12. Once the copy operation is completed, remove the USB Flash drive and connect it to the ICC workstation you want to patch.

5.2.2 Installing WSUS Offline Updates

The following steps are performed on the ImageCast® Central machine.

1. On the ImageCast® Central machine, double-click the folder you copied and run **UpdateInstaller.exe**
2. The **User Account Control** window appears. Click **Yes**

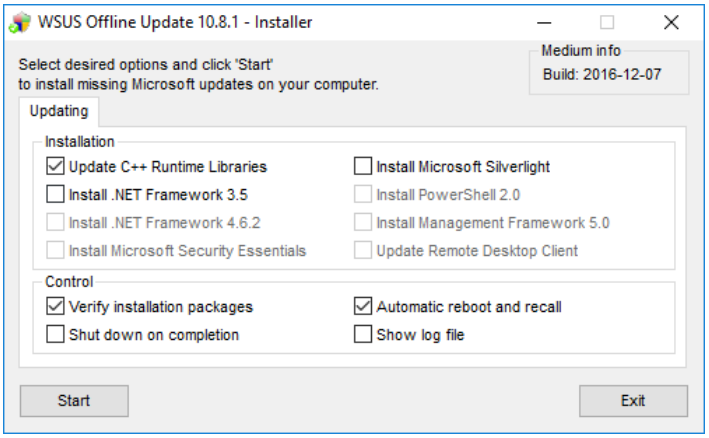


Figure 5.9: WSUS Offline Update Installer

3. The following items must be selected.

   NOTE: Some of these items may already be selected by default.

   - **Update C++ Runtime libraries**
   - **Verify installation packages**
   - **Automatic reboot and recall**

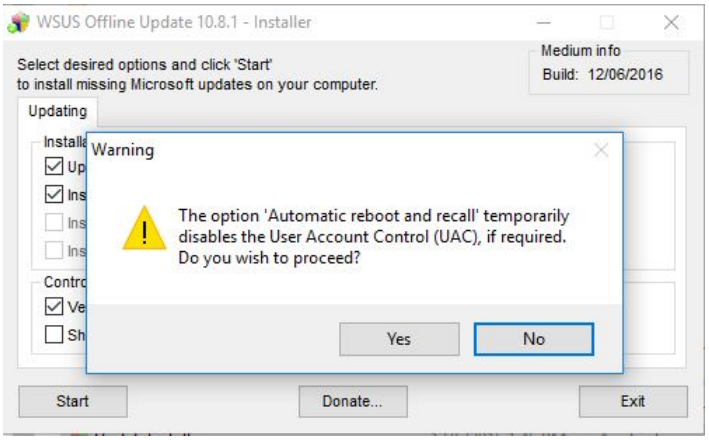


Figure 5.10: WSUS Offline - Warning disable UAC Screen

4. After selecting the **Automatic reboot and recall** check box, a warning for disabling UAC appears. Click **Yes**.

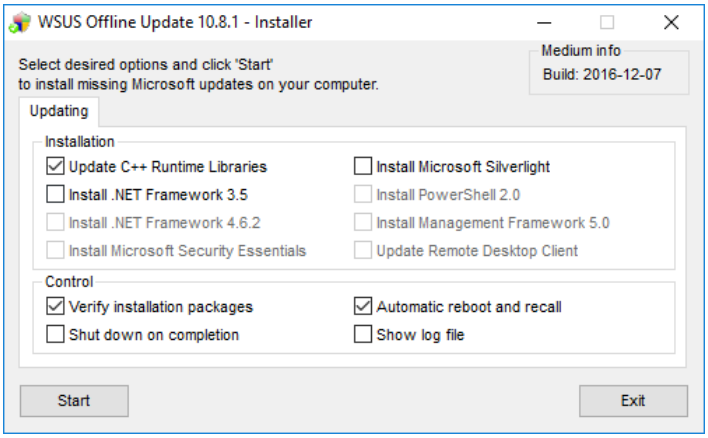


Figure 5.11: WSUS Offline - Main window with all options selected Screen

5. Ensure that the options you have selected match the following:
   - Update C++ Runtime libraries
   - Verify installation packages
   - Automatic reboot and recall
6. Click **Start** to commence the patching process.

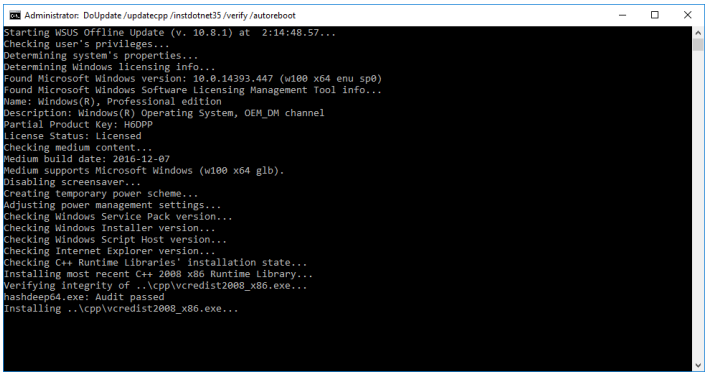


Figure 5.12: Command Prompt screen

7. UpdateInstaller begins patching the system in several stages. In the first stage, UpdateInstaller.exe updates C++ Runtime Libraries and .NET Framework to the latest version.

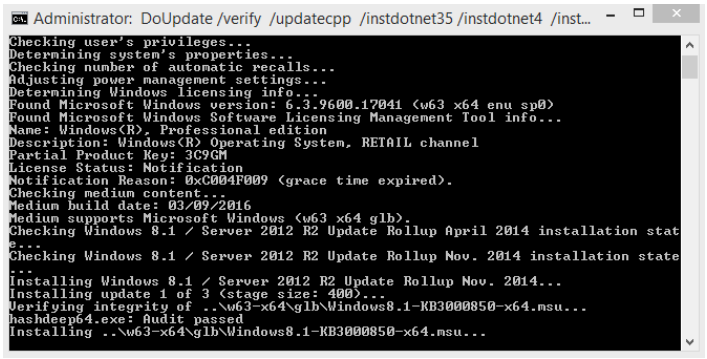


Figure 5.13: Command Prompt screen

8. After it finishes, in the second stage the computer reboots. Log back in as temporary administrator user ("WOUTempAdmin"), continuing the update process.

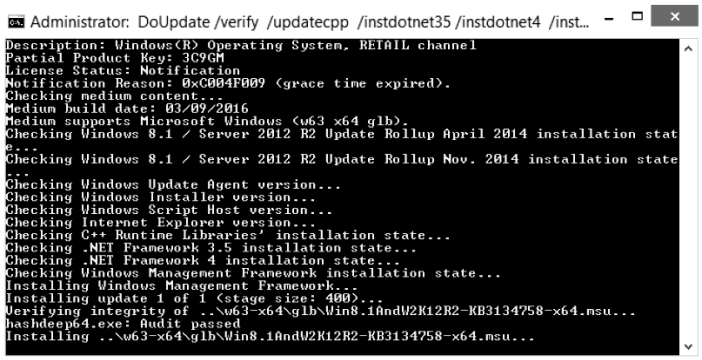


Figure 5.14: WSUS Offline - Installation of security patches Screen

9. In the fourth stage, UpdateInstaller.exe installs Windows security updates. This stage is the most time consuming, since it involves processing a large number of security patches. The number varies depending on which updates had previously been installed, the system's resources or the date on which you perform the patching process.

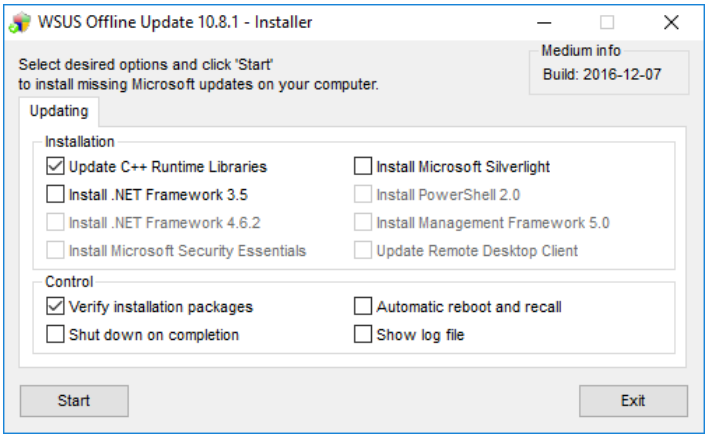


Figure 5.15: WSUS Offline - Patching completed Screen

10. When the UpdateInstaller does not automatically log you back into the OS, the update is complete. To verify that everything is installed correctly, run UpdateInstaller.exe one more time and ensure that all the following installation options (selected earlier) are now unavailable and cannot be selected:

    - Install .NET Framework 4.6.2
    - Install Management Framework 5.0

Chapter 6

Operating System Configuration

This chapter covers the configuration of the Windows 10 Professional operating system after it has been installed.

6.1 Installing Drivers and Tools

Device drivers must be installed on the system for the following the onboard devices:

- Chipset
- Video
- Audio
- USB 3.0
- Network drivers

Update the system BIOS to the latest release.

NOTE: Navigate to device manager and verify that there are no unknown devices. If there are any unknown devices please install those drivers before proceeding.

6.2 Setting Screen Resolution

1. Right-click on the desktop and click **Display Settings**.
2. From the **Screen Resolution** window, scroll down and click **Advanced Display Settings**.
3. From the **Resolution** dropdown menu, click **1920 x 1080 (Recommended)**.
4. Click **Apply**.
5. The screen resolution adjusts. If the resolution was applied successfully, click **Keep Changes**.
6. Close the **Screen Resolution** window.

6.3 Setting Computer Name and Workgroup

As described in section 1.2.3, the ImageCast® Central can be run as a stand-alone unit or as part of the Democracy Suite® EMS network. When connected to the EMS network, the ImageCast® Central saves scanned ballots directly to the EMS Server for tally or adjudication.

The EMS network is comprised of a central server and one or more connected client PCs, ImageCast® Central workstations and a report printer, connected by a passive or managed switch. ImageCast® Central workstations and other client machines are served IP addresses by a DHCP server.
In this configuration, it is recommended that the work group be defined and each computer be named appropriately. For example, if more than one ICC workstations are present in the configuration, then they should be named in a fashion that allows them to be distinguished between each other (for example ICC01, ICC02, ICC03 etc.).

To set the computer name and workgroup values:

1. Open the Windows Explorer window, right click on “This PC” and select “Properties”.
2. Select “Change Settings” from the right hand side.
3. In the “System Properties” dialogue, “Computer Name” tab, click on the **Change** button.
4. In the “Computer Name/Domain Changes” dialog window, type in the name of the workstation in the “Computer name:”
5. Select the “Workgroup” in the “Member of:” area and type in the “EMS.NET” name in the “Workgroup” field.

6.4 Setting Date, Time and Time Zone

Verify that the computer's date, time and time zone are set correctly. If not, set the correct date, time and time zone.

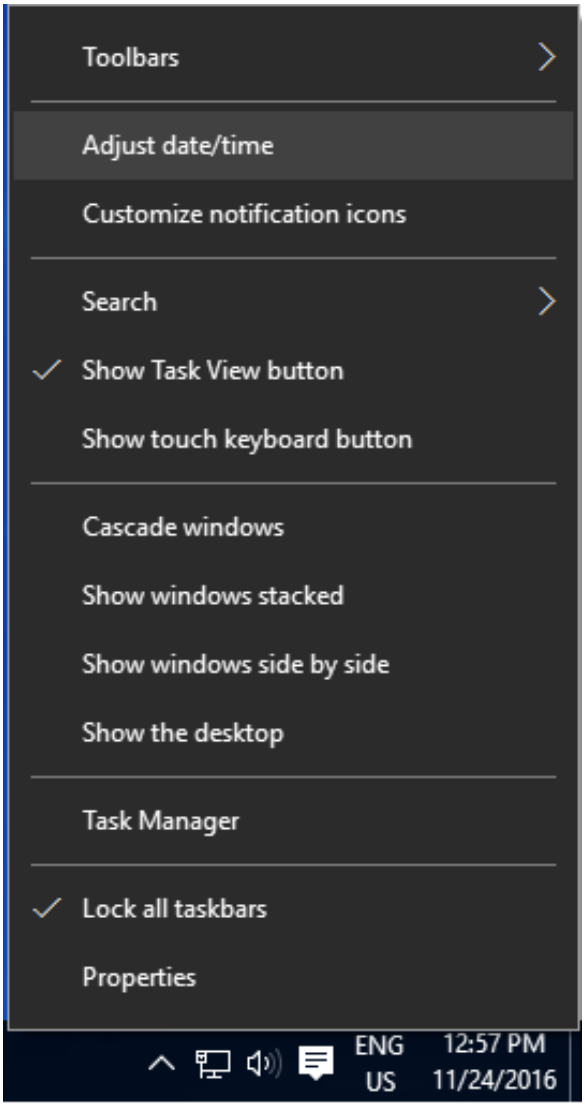


Figure 6.1: Adjust date/time

1. Right-click on the clock in the lower-right corner of the Taskbar.
2. Select **Adjust date/time** from the context menu.

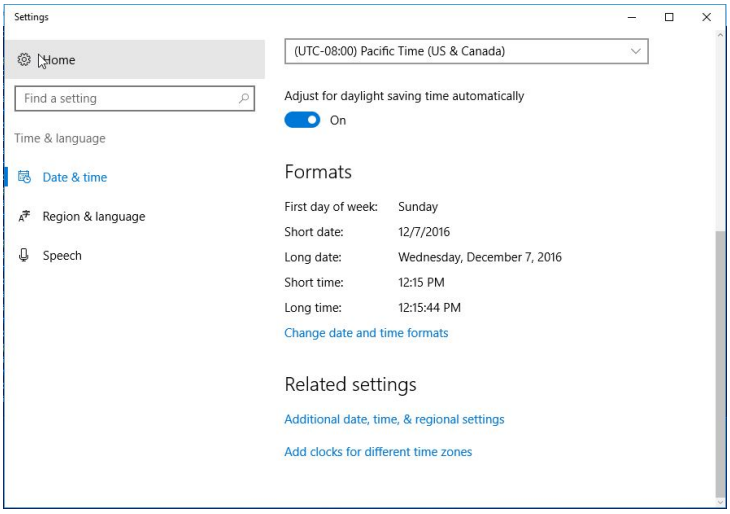


Figure 6.2: Date and Time window

3. Verify that the computer's date, time and time zone are set correctly. If so, continue to the next section.

4. Scroll Down and click **Additional date, time & Regional settings**.

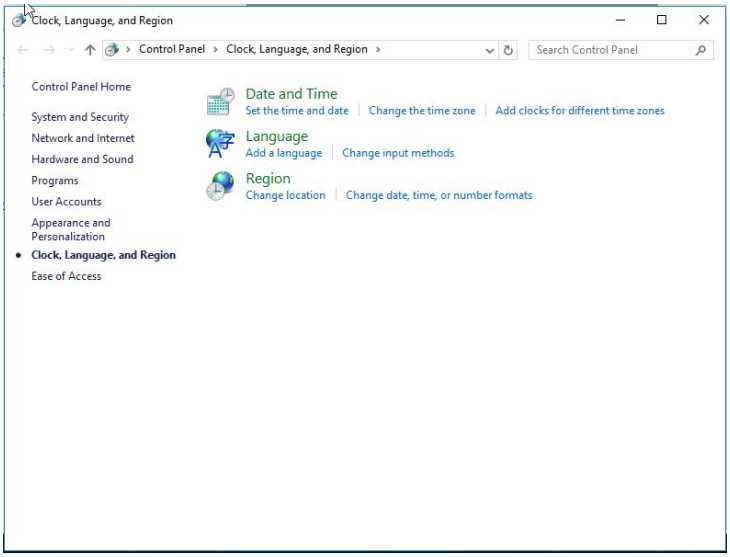


Figure 6.3: Clock, Language and Region window

5. Click **Set the time and date**.

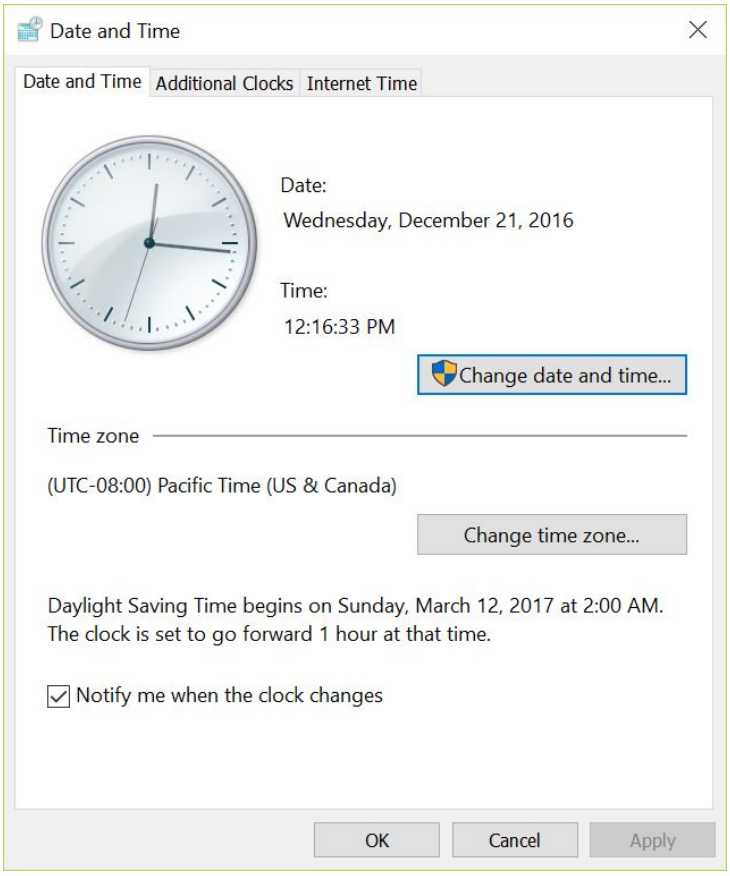


Figure 6.4: Setting window

6. In the **Date and Time** window, click **Change time zone**.

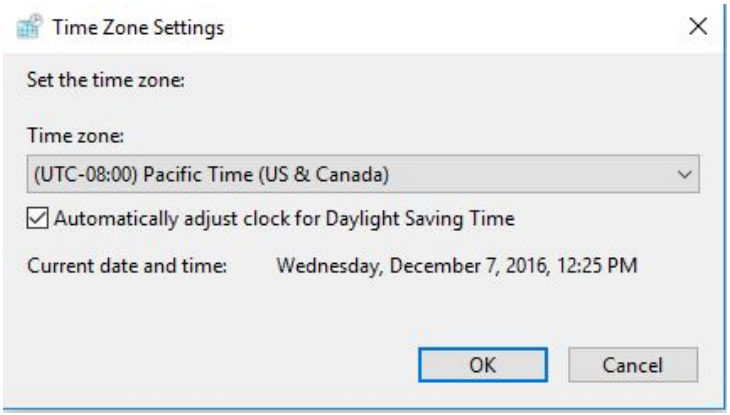


Figure 6.5: Set Time Zone

7. Set the correct time zone for your location.
8. If your jurisdiction adjusts its clocks during **Daylight Saving Time**, ensure that this check box is selected.
9. Click **OK** to close the **Time Zone Settings** dialog.

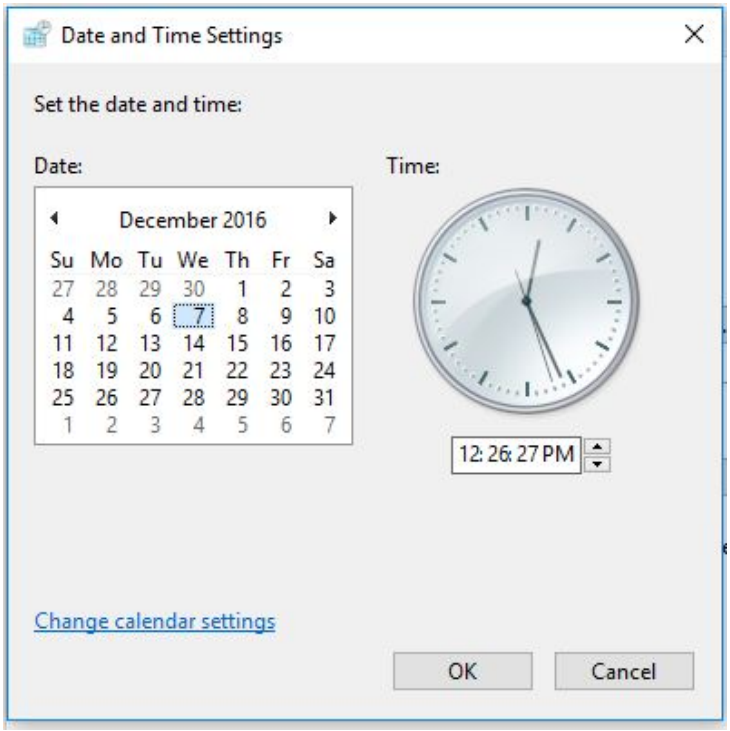


Figure 6.6: Set Date and Time

10. Click **Change date and time** to adjust the date and time.
11. Set the current date and time.
    NOTE: Use a trusted time source (for example, a mobile phone receiving time from the cellular network), to ensure that the time is synchronized exactly.
12. Click **OK** to close the **Date and Time Settings** dialog.
13. In the **Date and Time** dialog, click **OK** to close the dialog.

6.5 Activating Windows 10

Since the ICC computer cannot be connected to the internet, the Windows 10 installation must be activated by phone.

1. Click the **Windows** button, and in the **Search** field, type **slui.exe 4**
2. Select **slui.exe 4** application in the left pane.
3. Press **Enter**.
4. Select your **Country** from the list.
5. Select the **Phone Activation** option.
6. Stay on the phone and follow the instructions to perform the activation.

6.6 Adjusting Power Options

1. Right-click the **Windows** button and click **Control Panel**.
2. Click **View by** and change to Large or Small icons if your Control Panel is in Categories view.

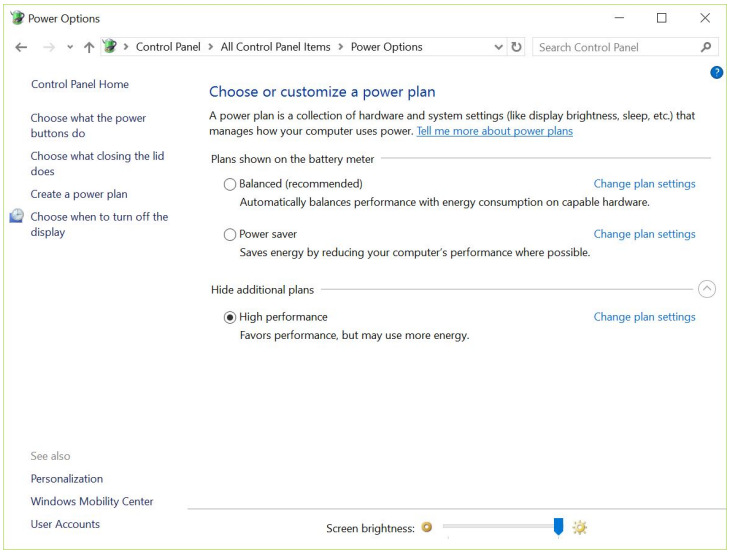
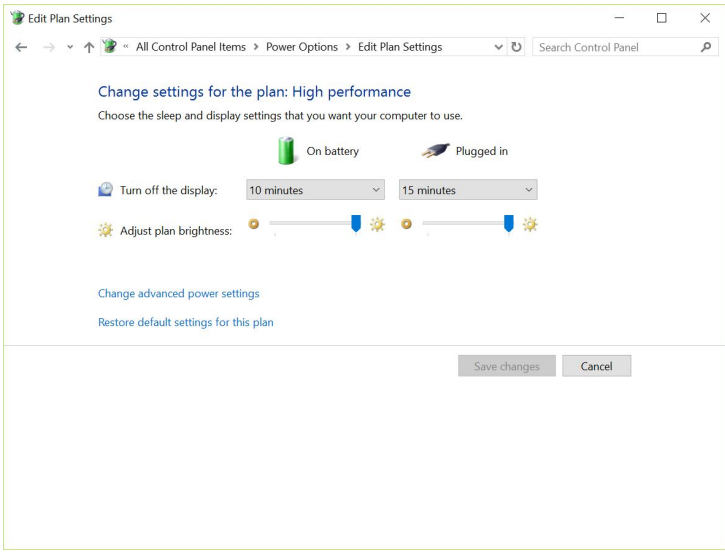


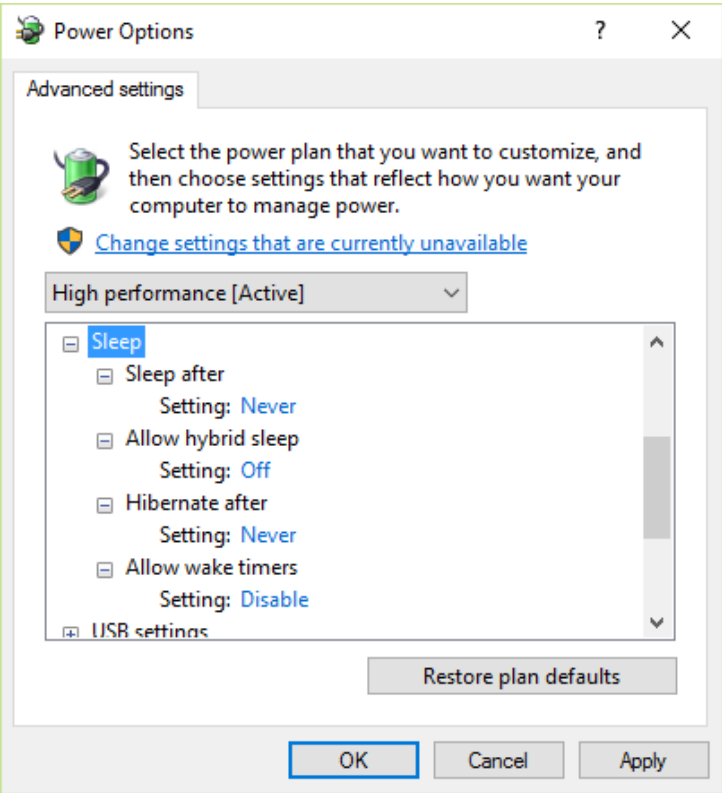
Figure 6.7: Changing Plan Settings - Power Options Screen

3. Click **Power Options**. In the newly opened window, expand the **Show additional plans** drop-down.
4. Click **High Performance plan** if it is not already selected, and then click **Change plan settings** next to it.



5. Click **Change advanced power settings**.

Figure 6.8: Changing Plan Settings - Edit Plan Settings Screen



6. The Power Options screen appears.
7. In the new window expand **Sleep** node and turn off all available features. This can be achieved by setting a drop-down value to **Never**, **Disable** or **Off**, or by entering **0** in a numeric field.

Figure 6.9: Power Options Screen

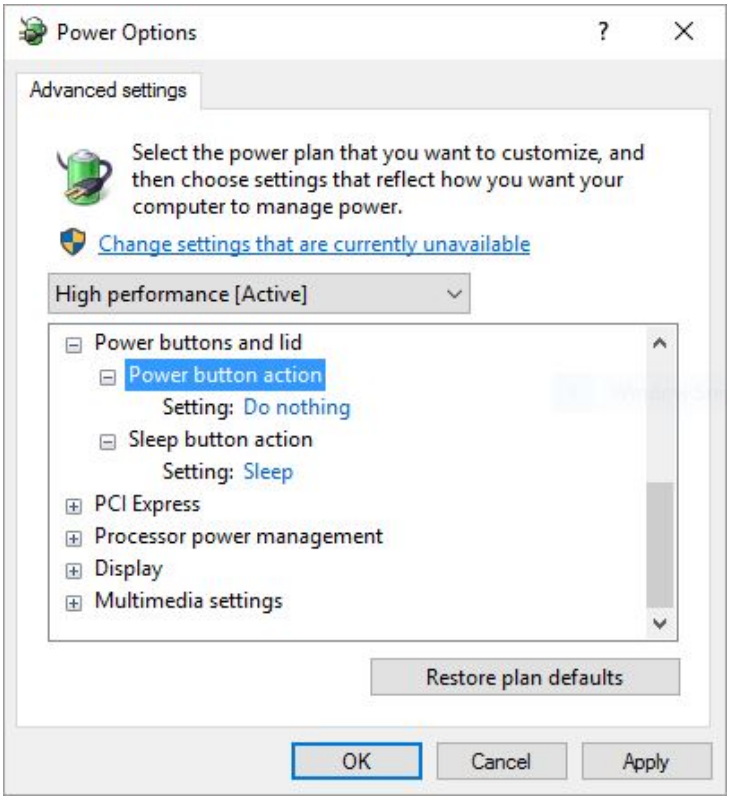


Figure 6.10: Power buttons and lid

8. If available, expand the **Power buttons and lid** node.
9. Set **Power Button Action** to **Do Nothing** and **Sleep Button Action** to **Sleep**.
10. Click **Apply** then **OK**.
11. Set the **Turn off the display** field to **Never**, then close the window.

6.7 Network Discovery and File Sharing

It is necessary to **Turn on network discovery** in order to map the secondary path to the EMS Server.

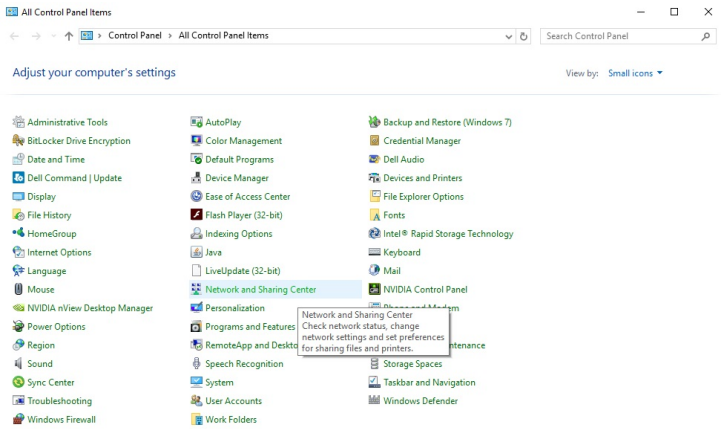


Figure 6.11: Turn on Network Discovery - All Control Panel Items Screen

1. Click the **Windows** button and click **Control Panel**.
2. Make sure **View by** is set to Large icons or Small icons.

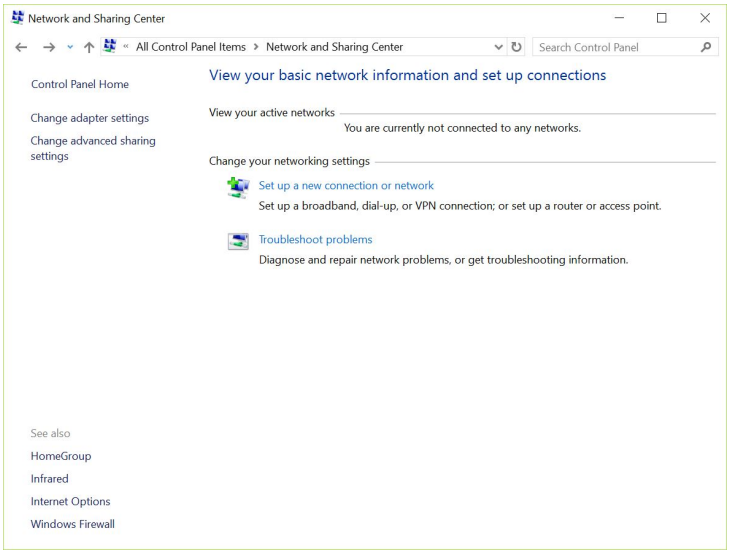


Figure 6.12: Turn on Network Discovery - Network and Sharing Center Screen

3. Click **Network and Sharing Center**.
4. In the left-hand pane of **Network and Sharing Center**, click **Change advanced sharing settings**.

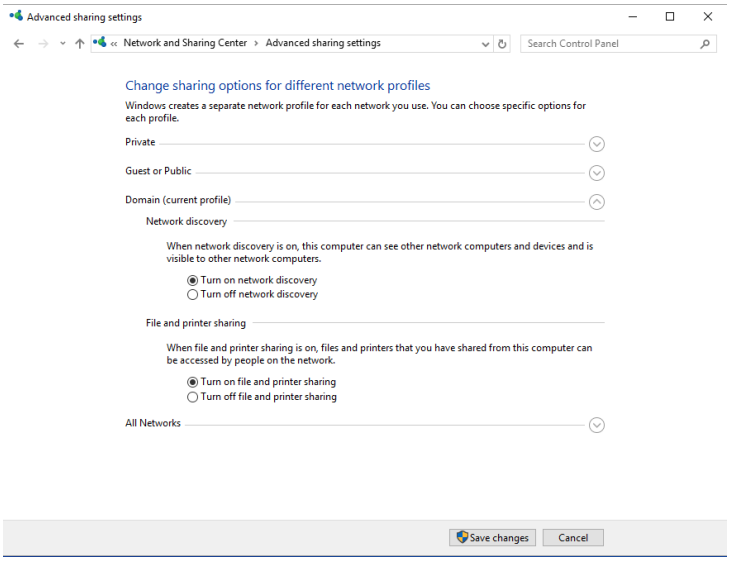


Figure 6.13: Turn on Network Discovery - Advanced sharing settings Screen

5. Expand the current profile section and select the following:
   - **Turn on network discovery**
   - **Turn on file and printer sharing**

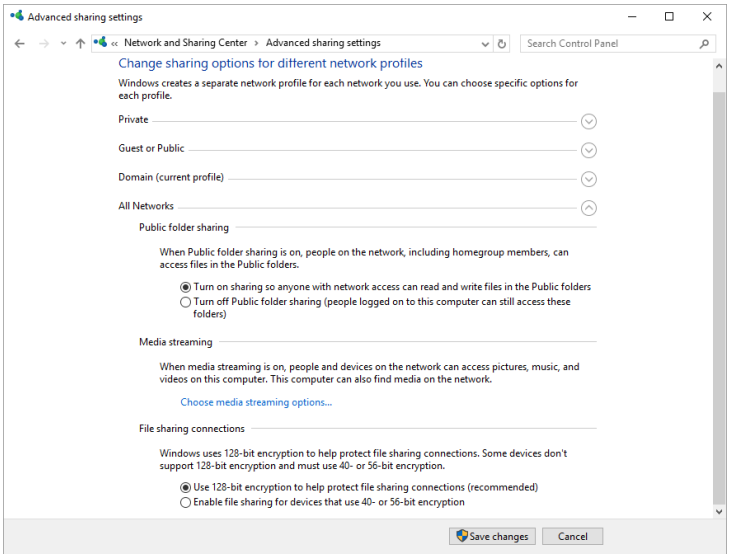


Figure 6.14: Turn on Network Discovery - Advanced sharing settings Screen

6. Expand All Networks and select the following:
   - **Turn on sharing so anyone with network access can read and write files in the Public folders**
   - **Turn on password protected sharing**
7. Click **Save changes** and close any opened windows.
8. Click **Change advanced sharing settings** and confirm that the changes were saved.
   NOTE: It will take some time for the DNS server to propagate the change. If the changes do not appear to be saved even after a while, please see the note below for the resolution.

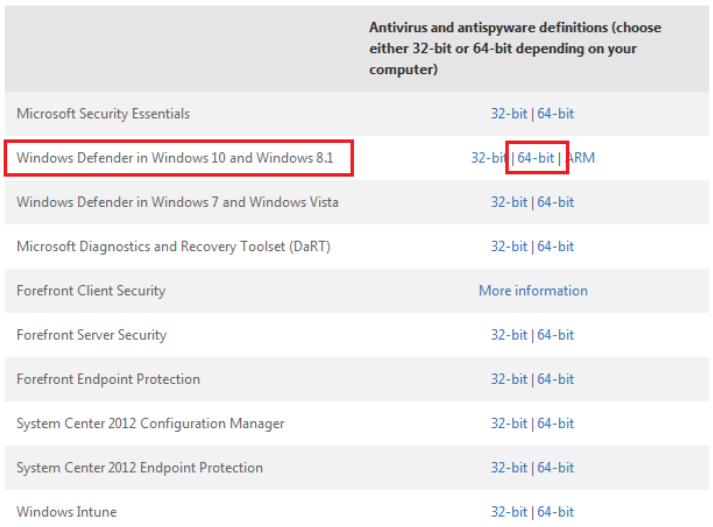
NOTE: If the changes do not appear to be saved even after a few minutes, then the following reasons might be the cause:

- The dependency services for Network Discovery are not running.
  - DNS Client
  - Function Discovery Resource Publication
  - SSDP Discovery
  - UPnP Device Host
- The Windows firewall or other firewalls do not allow Network Discovery. In this case, configure the Windows firewall to allow Network Discovery:
  - Right-click the **Widows** icon and select **Control Panel**. Click **System and Security**, and then click **Windows Firewall**.
  - In the left-hand pane, click **Allow a program or feature through Windows Firewall**.
  - Click **Change settings**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation. Select Network discovery, and then click **OK**.
- Configure other firewalls in the network to allow Network Discovery.
- Turn on Network Discovery in Network and Sharing Center.

For more information on this issue, please visit the Microsoft Support Center.

6.8 Downloading and Installing Offline Updates for Windows Defender

1. On a computer which is connected to the internet, open the internet browser and navigate to the following location:
   `https://www.microsoft.com/security/portal/definitions/adl.aspx`.



	Antivirus and antispyware definitions (choose either 32-bit or 64-bit depending on your computer)
Microsoft Security Essentials	32-bit | 64-bit
Windows Defender in Windows 10 and Windows 8.1	32-bit | 64-bit | ARM
Windows Defender in Windows 7 and Windows Vista	32-bit | 64-bit
Microsoft Diagnostics and Recovery Toolset (DaRT)	32-bit | 64-bit
Forefront Client Security	More information
Forefront Server Security	32-bit | 64-bit
Forefront Endpoint Protection	32-bit | 64-bit
System Center 2012 Configuration Manager	32-bit | 64-bit
System Center 2012 Endpoint Protection	32-bit | 64-bit
Windows Intune	32-bit | 64-bit

2. Scroll down and click the link for **Windows Defender in Windows 10 and Windows 8.1 (64-bit)**.
3. A dialog opens automatically, prompting to download the virus definition file (mpam-fe.exe). Click **Save** to download the file, if prompted.

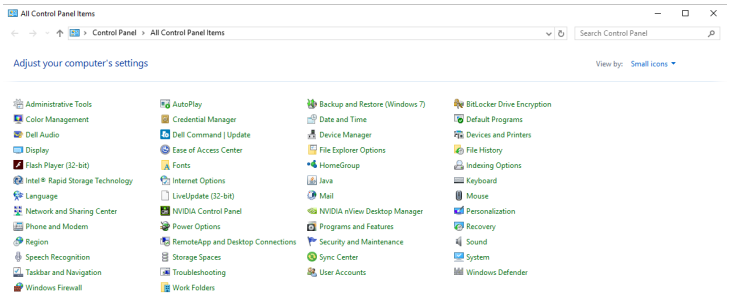
Figure 6.15: Updating Windows Defender - Download Virus Definitions

4. Use a removable drive to copy the update file to the workstation being updated.
5. Double-click the downloaded file to update the virus definitions.

   NOTE: There will be no window or message indicating that the installation was successful.

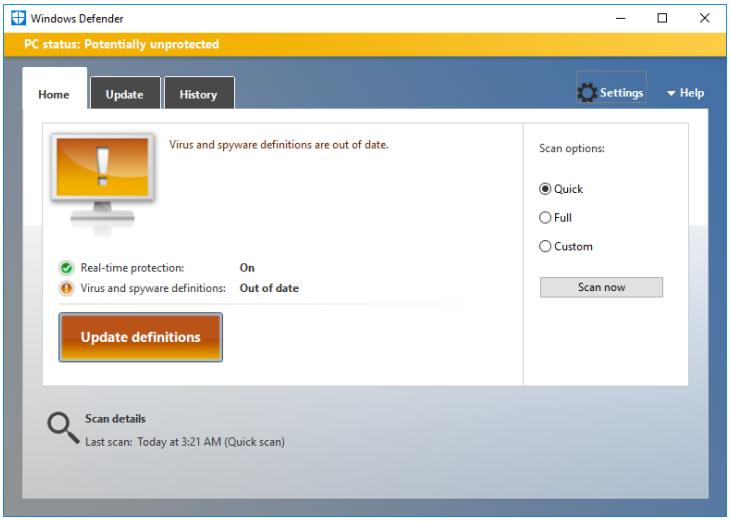
6.8.1 Windows Defender Installation

This section explains how to enable **Windows Defender** on machines running **Windows 10 Professional**.



1. Right-click the **Windows** button and select **Control Panel** from the context menu.
2. In Control Panel, click **Windows Defender**.

Figure 6.16: Enabling Windows Defender - Control Panel



3. The **Windows Defender** window opens.

   Windows Defender should be enabled by default. When enabled, "Real-time protection" is set to "On" and displays a green checkmark.

   If Windows Defender is already enabled, close the window and proceed to Section 6.8 to download and install offline updates. If Windows Defender is not enabled, continue to the next step.

Figure 6.17: Enabling Windows Defender - Windows Defender Window

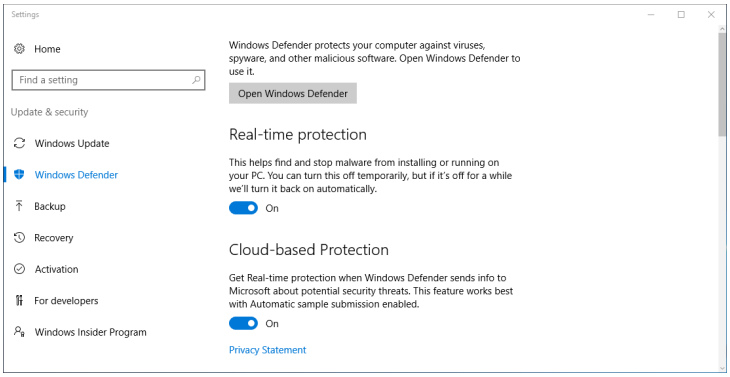


Figure 6.18: Enabling Windows Defender - Enabling Real-time Protection

4. Click the **Settings** icon.
5. Under **Real-time protection,** turn on real-time protection (recommended)

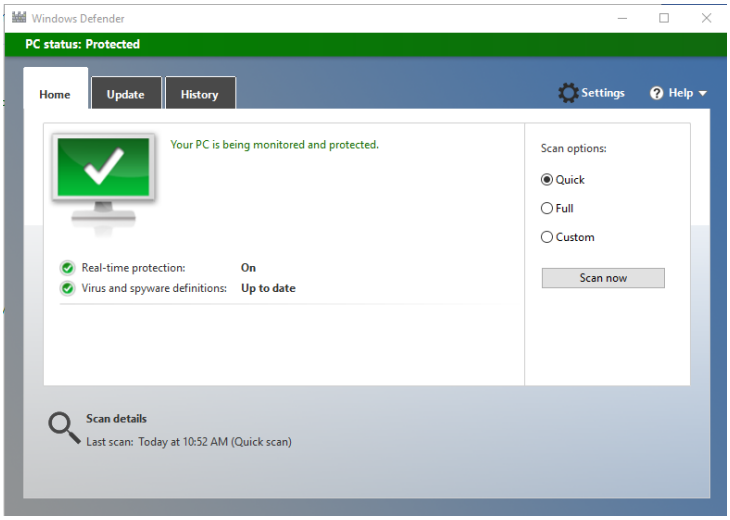


Figure 6.19: Updating Windows Defender - Windows Defender Up To Date

6. When virus and spyware definitions are up to date, the "Virus and spyware definitions" shows "Up to date" and displays a green checkmark, as shown in Figure 6.19.
7. Close the **Windows Defender** window.

6.9 Creating Additional User Accounts

Additional user accounts can be created for other users of the system.

The user names should exist on the EMS Server, are case sensitive and must share the same password as the account on the server.

See Section 2.4 for more information about user accounts.

1. Right-click the **Windows** button and click **Computer Management**.
2. The *Computer Management* screen appears.
3. Expand the *System Tools* and *Local Users and Groups* nodes and select the **Users** node.
4. Right-click the empty space in the middle panel, and select the **New User** option from the combo box.
5. In the *New User* screen enter the user name for the account (*iccuser*, for example).
6. Enter in a password using a combination of upper and lower case letters as well as numbers.
7. Clear the **User must change password at next logon** check box, and select the **Password never expires** check box.

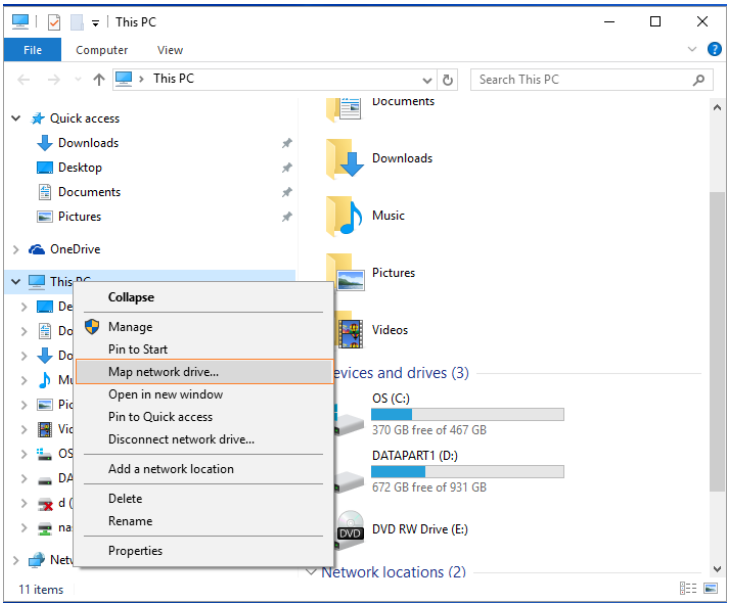
   NOTE: Please ensure that the administrators password has been set.
8. Click **Create**, and click **Close**.
9. The newly created user account appears in the list on the *Computer Management* screen.
10. If the user has rights to modify or configure election files, add the user to the Administrators group.
11. Close the *Computer Management* window.

6.10 Mapping the EMS NAS Folder

Create a mapped network drive so that the Results Tally & Reporting application can load ICC results files from the shared NAS folder on the EMS Server.

Refer to Section 2.4 of this document and *Democracy Suite® EMS Installation and Configuration Procedure* for more information on enabling sharing with the ImageCast® Central Workstation.

NOTE: These steps must be performed for each user on the ICC Workstation.



1. Open **File Explorer**.
2. Right-click on the **Computer** icon in the left panel of the window that appears, and select **Map network drive...**.

Figure 6.20: Mapping Shared EMS NAS Folder

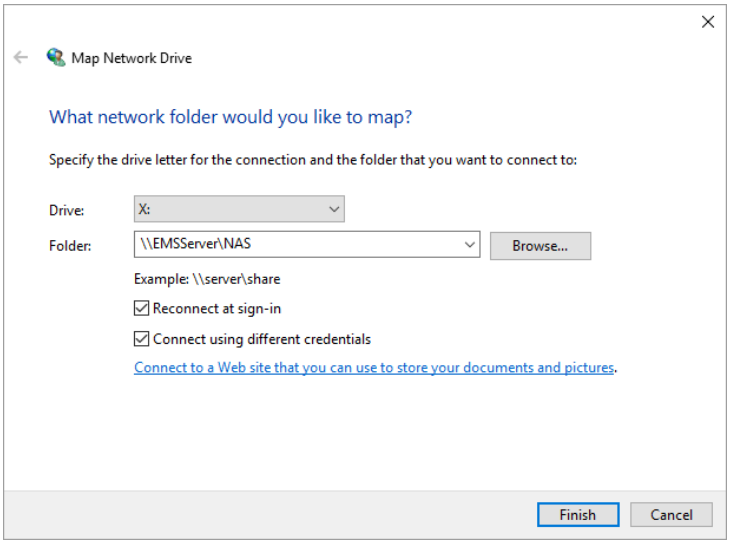


Figure 6.21: Mapping Shared EMS NAS Folder - Map Network Drive

3. The 'Map Network Drive' dialog appears. Enter the EMS NAS share path in the Folder field. The share path will be in the following format (replace **EMSServer** with the computer name or IP address of the server):
   \\EMSServer\NAS
4. Select the **Reconnect at logon** and **Connect using different credentials** check boxes.
5. Click **Finish**.

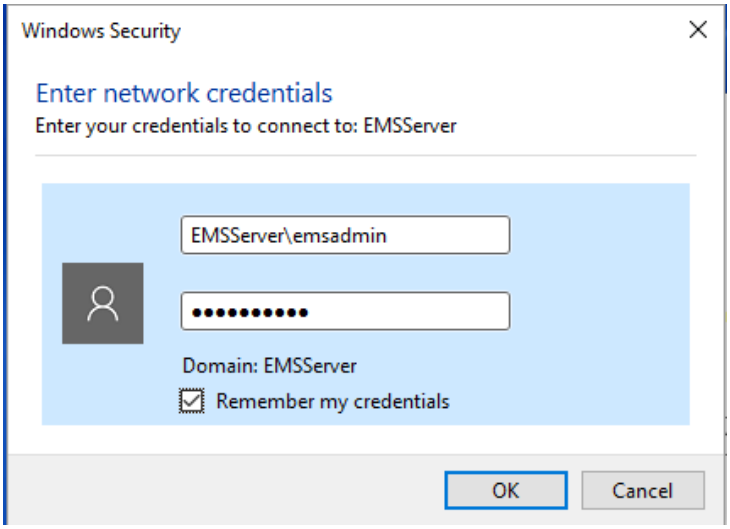
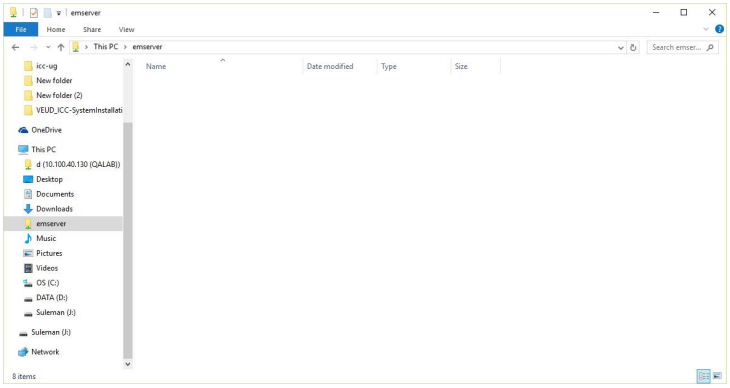


Figure 6.22: Mapping Shared EMS NAS Folder - Enter Credentials

6. The Windows Security prompt opens. Select **Use another account**
7. Select the **Remember my credentials** check box.
8. Enter the User Name and Password of the EMS Administrator user created during the EMS Server installation. You must include the server name in the User Name. For example:
   EMSServer\emsadmin
9. Click **OK**.



10. The mapped folder opens in a new window. Close this window.

Figure 6.23: Mapping Shared EMS NAS Folder - Finished

Chapter 7

Prerequisite Third-party Components

This Chapter covers the installation procedures for third-party prerequisites required by the ImageCast® Central . For a complete list of required software components, refer to Section 2.1.

7.1 Installing Report Printer Drivers

If a report printer is available on your network or connected directly to the computer, install the device drivers and configure the device. Refer to the manufacturer's documentation for instructions.

7.2 Canon DR-G1130 Installation

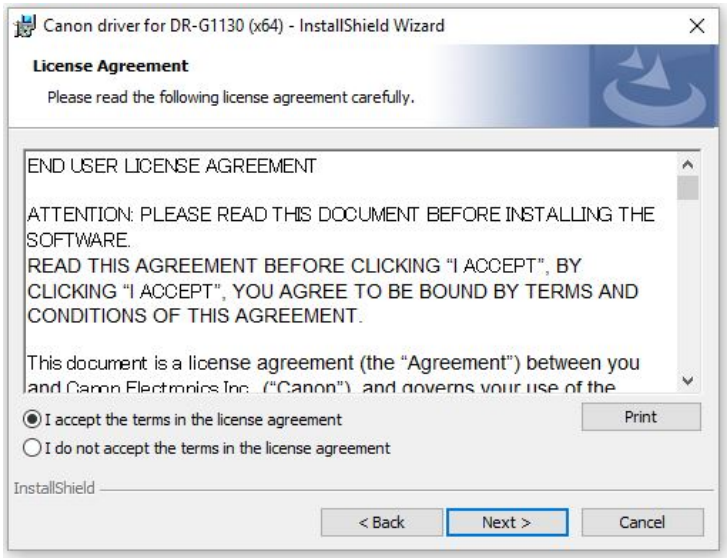
7.2.1 Installing the Canon DR-G1130 Driver

1. On a system which is connected to the internet, browse to `https://www.usa.canon.com/internet/portal/us/home/support/details/scanners/document-scanner/imageformula-dr-g1130`.
2. Click **Drivers & Downloads**, and then click **DR-G1130 ISIS/TWAIN Driver Version 1.2 SP6**.
3. Select the check box to agree to the terms of the disclaimer, and click **Download**.
4. A self-extracting zip file will download. Locate the file and open it.
5. Click **Unzip** in the window that appears to unpack the driver installer. A notification will appear saying the operation was successful; click **OK** and then **Close**.

6. From the **File Explorer** window, browse to **C:\DRG1130\ISIS-TWAIN\Version 1.2 SP6** and click **setup.exe**.

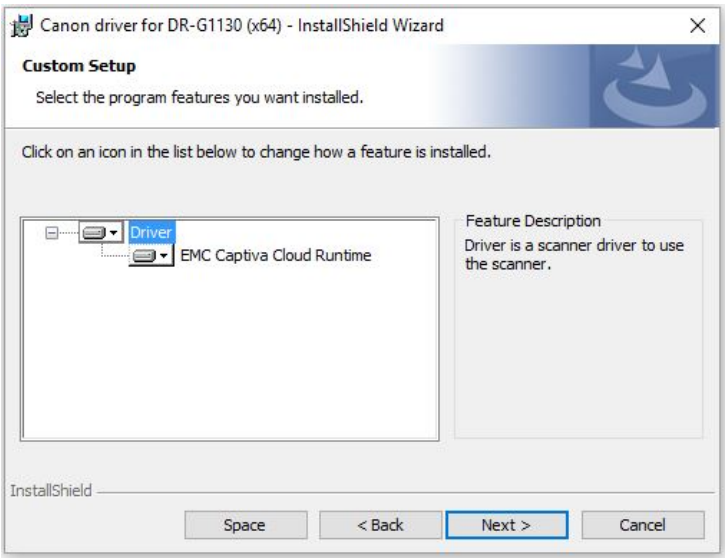
7. In the **DR-G1130 Setup** screen, click **Next**.

Figure 7.1: DR-G1130 Setup Welcome Screen.



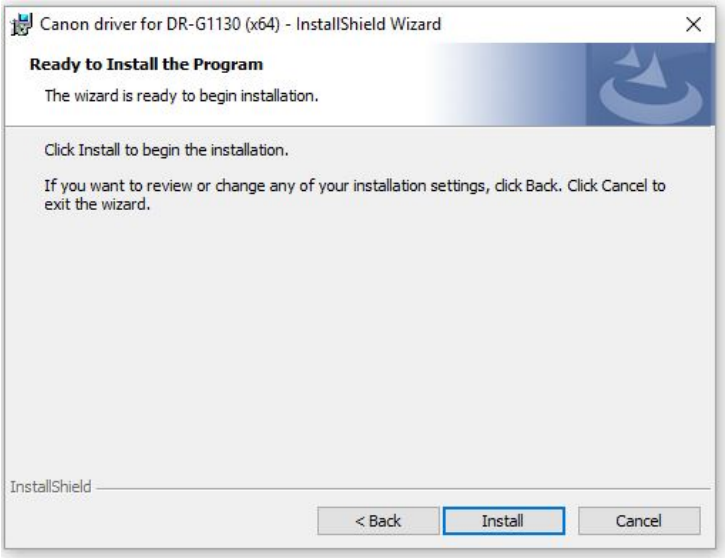
8. In the **License Agreement** screen, select the **I accept the terms** radio button, and then click **Next**.

Figure 7.2: DR-G1130 Setup License Agreement.



9. In the **Custom Setup** screen, click **Next**.

Figure 7.3: DR-G1130 Setup Custom Setup Screen.



10. In the **Ready to Install** screen, click **Install**.

Figure 7.4: Ready to Install Screen.

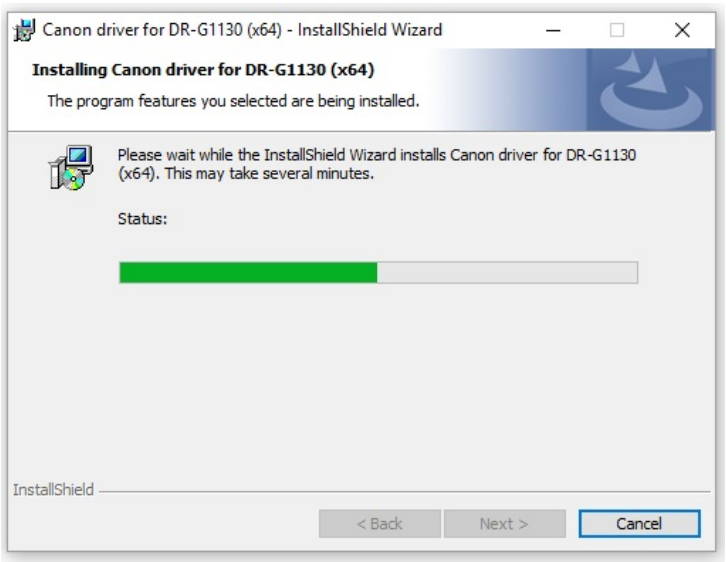


Figure 7.5: Installation Status Display.

11. During the installation, a progress bar is displayed.

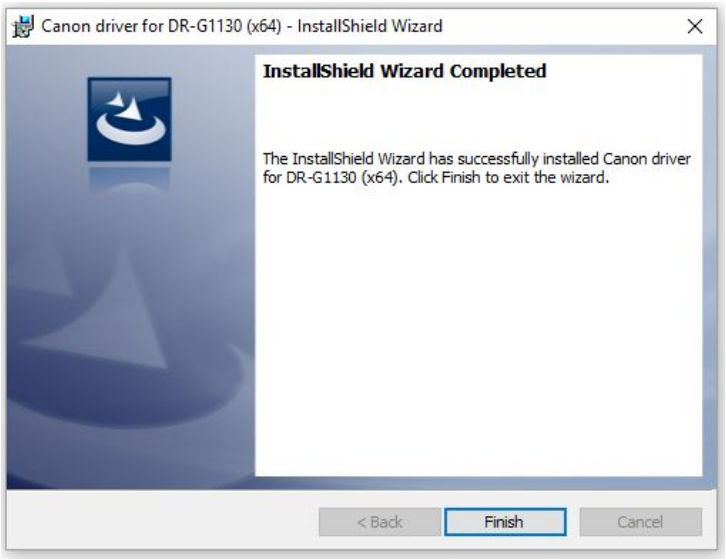


Figure 7.6: InstallShield Wizard After Installation.

12. When the installation completes, the **InstallShield Wizard Completed** window appears. Click **Finish**.
13. Close any **File Explorer** windows that are still open.

7.2.2 Connecting the Scanner

Now that the scanner driver has been installed, follow the steps below to connect the scanner to the system, and verify that the driver installation was successful.

Figure 7.7: USB Port on the Back of the Canon DR-G1130 Scanner.

1. Plug in and power on the scanner by locating the USB port on the back and near the top of the Canon DR-G1130 Scanner, connecting the port to a free USB port of the target PC, and pressing the power button on the scanner.

7.2.3 Verifying the Installation in Device Manager

The steps below are meant to verify that the newly-installed driver appears in the Device Manager. Ensure the scanner is attached to the PC via a USB port and that it is powered on before following the steps below.

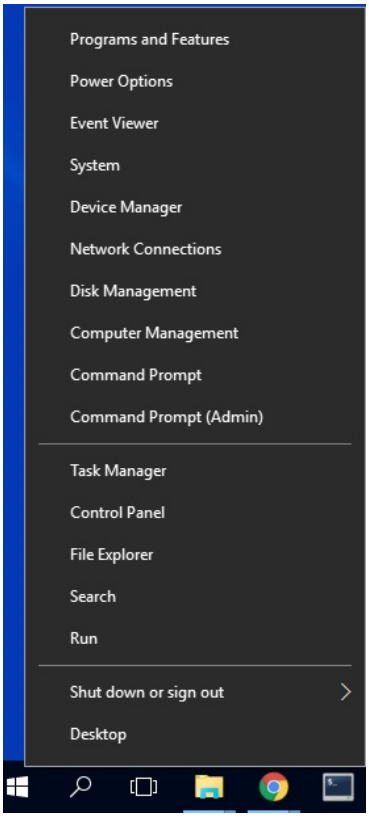


Figure 7.8: Right-click on Start menu

1. Right-click the **Windows** icon and click **Device Manager**.

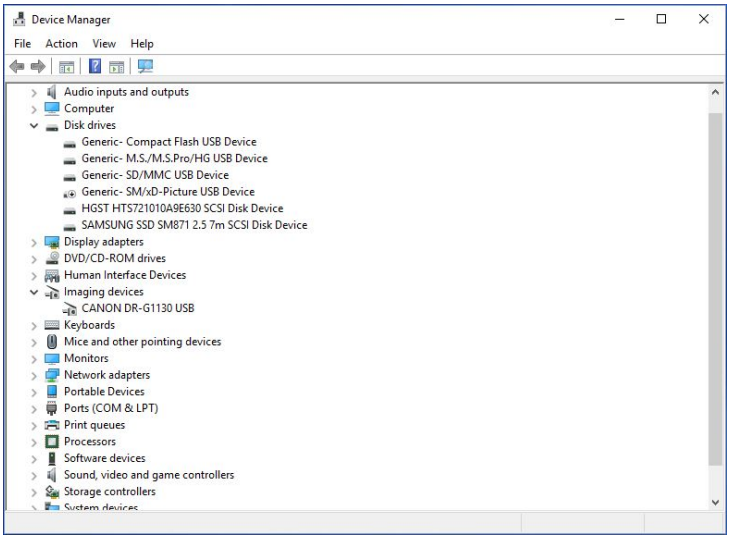


Figure 7.9: Device Manager.

2. In the Device Manager, look for the **'CANON-DR-G1130 USB'** device under the category **'Imaging devices'**.

   NOTE: If this does not appear, verify the steps in section 7.2.1 were properly executed.

3. Exit the Device Manager and then exit the Control Panel.

7.2.4 Upgrading the Scanner Firmware

For optimal performance with the TWAIN driver, an update to the scanner firmware may be necessary.

1. On a system which is connected to the internet, browse to `www.usa.canon.com/internet/portal/us/home/support/details/scanners/document-scanner/imageformula-dr-g1130`.
2. Click **Drivers & Downloads**.
3. From the **Drivers & Downloads** section, click **Firmware**.
4. Click **Select** for DR-G1130/G1100 Firmware Version 1.33.
5. Select the agree to the terms of the disclaimer check box, and click **Download**.
6. A self-extracting zip file downloads. Locate the file and open it.
7. Click **Unzip** in the window that appears to unpack the driver installer. A notification appears stating the operation was successful; click **OK** and then click **Close**.
8. From a **Windows Explorer** window, browse to `C:\DRG1100_G1130\Firmware\Version 1.33` and doubleclick READMEFIRST.pdf.
9. Follow the manufacturer's instructions in the PDF document to perform the firmware upgrade.

7.3 Canon DR-M160II Installation

7.3.1 Installing the Canon DR-M160II Driver

1. On a system which is connected to the internet, browse to `https://www.usa.canon.com/internet/portal/us/home/support/details/scanners/document-scanner/imageformula-dr-m160ii`.
2. Click **Drivers & Downloads**, and then click **DR-M160/M160II ISIS/TWAIN Driver Version 1.2 SP6**.
3. Select the check box to agree to the terms of the disclaimer, and click **Download**.
4. A self-extracting zip file will download. Locate the file and open it.
5. Click **Unzip** in the window that appears to unpack the driver installer. A notification will appear saying the operation was successful; click **OK** and then **Close**.
6. From the **File Explorer** window, browse to **C:\DRM160II\ISIS-TWAIN\Version 1.2 SP6**, and click **setup.exe**.

Figure 7.10: Custom Installation screen

7. After some time, the **Installshield Wizard** window appears.
8. Click **Next**.

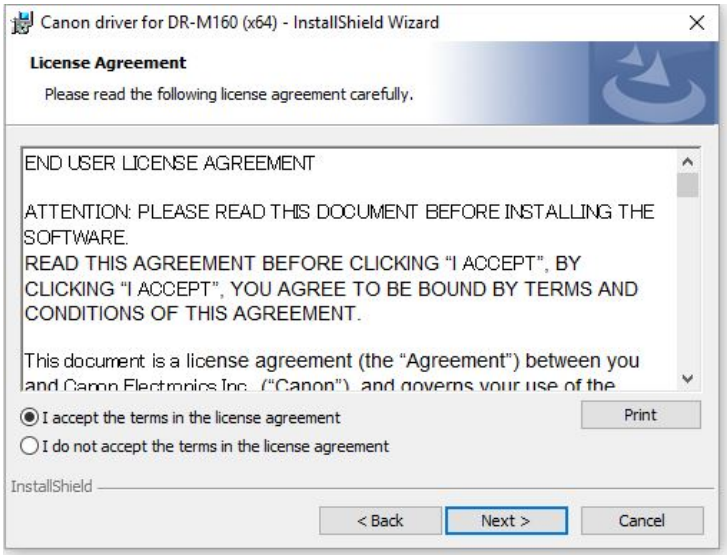


Figure 7.11: Custom Installation screen

9. The **License Agreement** appears. Read the terms and conditions in the **License Agreement**.
10. Select the **I accept the terms in the license agreement** check box.
11. Click **Next**.

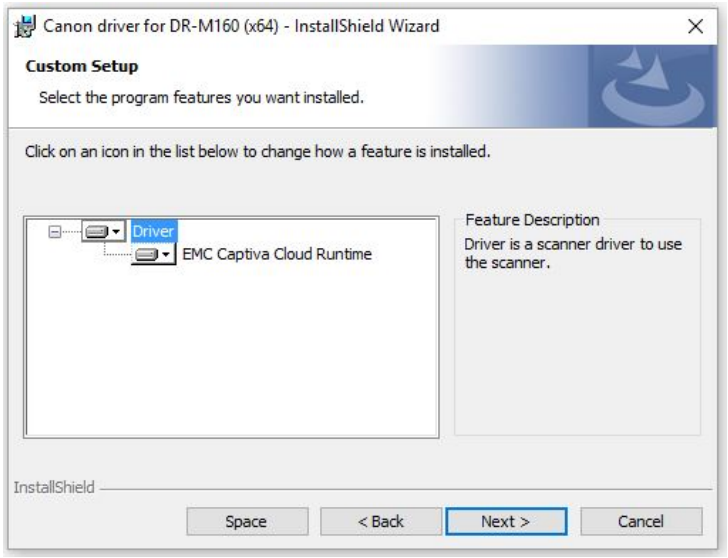
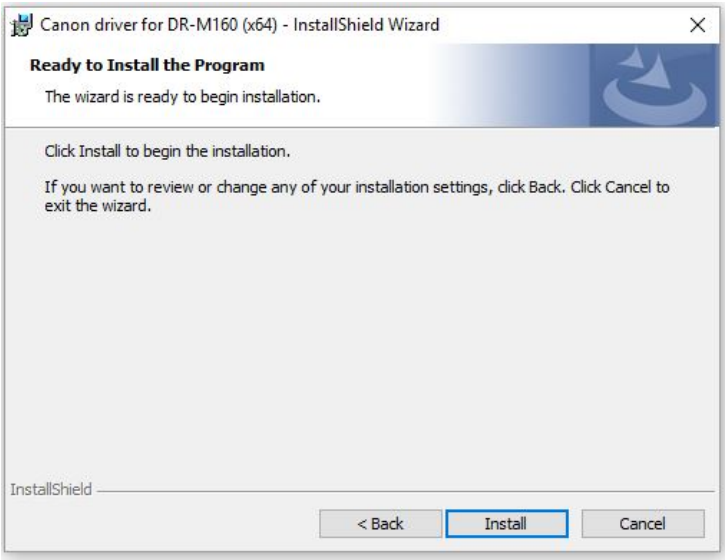


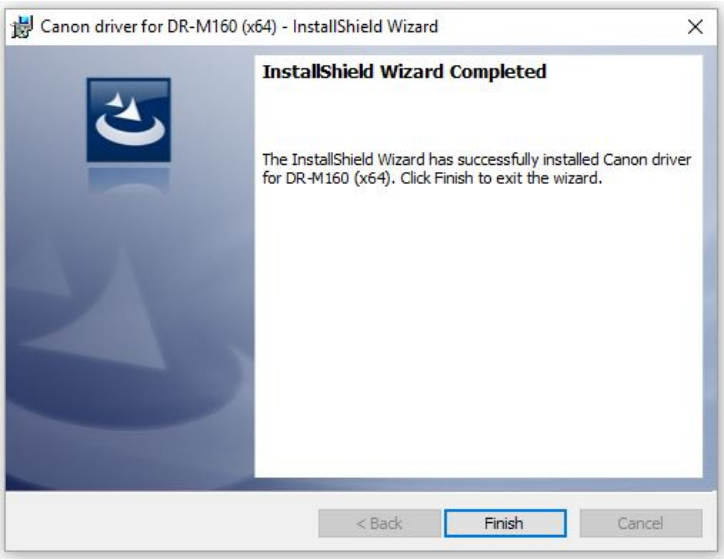
Figure 7.12: Custom Installation screen

12. Click **Next** to finish the installation setup.



13. Click **Install** to begin the installation.

Figure 7.13: Custom Installation screen



14. A progress bar displays to indicate the status of the installation. Click **Finish** once the installation is complete.

Figure 7.14: Custom Installation screen

7.3.2 Connecting the Scanner

Now that the scanner driver has been installed, follow the steps below to connect the scanner to the system, and verify that the driver installation was successful.

1. Connect the USB cable to the back of the scanner and to a free USB port on the workstation.
2. Plug the scanner into a wall outlet and power it on.
3. A notification appears indicating the DR-M160II driver installed successfully.

7.3.3 Verifying the Installation in Device Manager

The steps below are meant to verify that the newly-installed driver appears in the Device Manager. Ensure the scanner is attached to the PC via a USB port and that it is powered on before following the steps below.

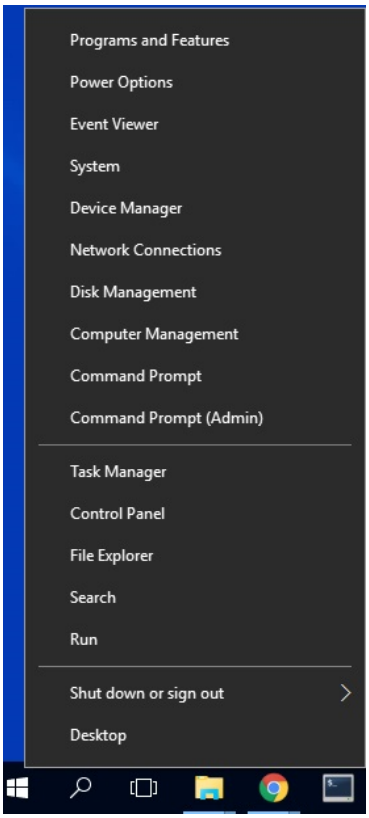


Figure 7.15: Right-click on Start menu

1. Go to the Control Panel and then click on ‘System’. This takes you to the screen shown in Figure 7.15. Click on ‘Device Manager’ in the left-side navigation panel.

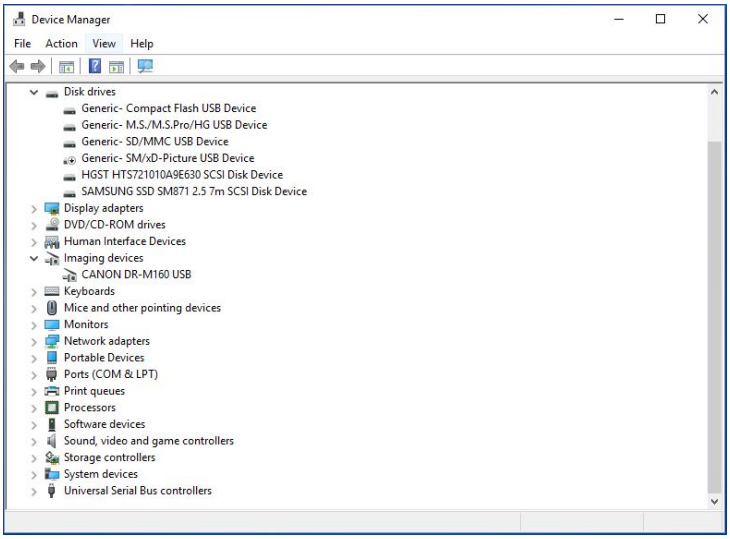


Figure 7.16: Device Manager

2. In the Device Manager, look for the **CANON DR-M160 USB** device under the category **Imaging devices**.
   NOTE: If this does not appear, verify the steps in Section and 7.2.1 were properly executed.
3. Exit the Device Manager and then exit the Control Panel.

7.4 Canon DR-X10C Installation

7.4.1 Installing the Canon DR-X10C Driver

1. On a system which is connected to the internet, browse to `https://www.usa.canon.com/internet/portal/us/home/support/details/scanners/document-scanner/imageformula-dr-x10c`
2. Click **Drivers & Downloads**, and then click **DR-X10C ISIS/TWAIN Driver Version 1.15 SP1**.
3. Select the check box to agree to the terms of the disclaimer, and click **Download**.
4. A self-extracting zip file is downloaded. Locate the file and open it.
5. Click **Unzip** in the window that appears to unpack the driver installer. A notification window appears stating the operation was successful; click **OK** and then **Close**.
6. From the **File Explorer** window, browse to `C:\DRX10C\ISIS-TWAIN\Version 1.15 SP1` and click **setup.exe**.
7. The **DR-X10C Setup** window appears.

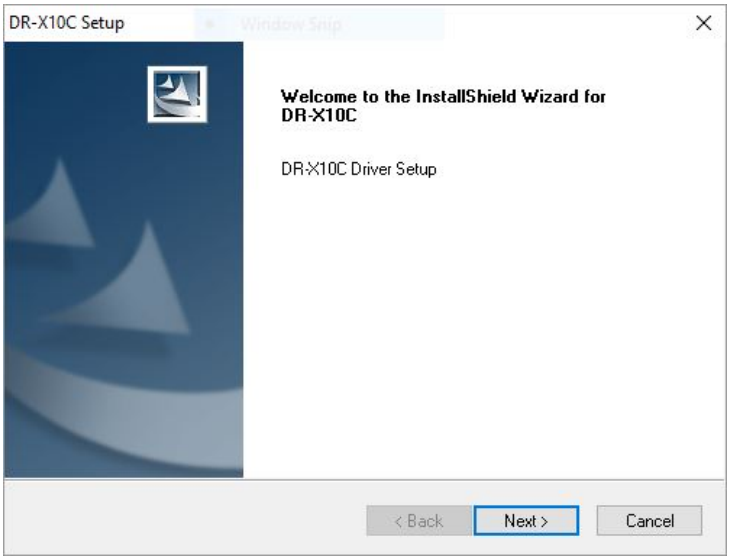


Figure 7.17: DR-X10C Setup window

8. From the **DR-X10C Setup** window, click **Next**.
9. The **License Agreement** window appears

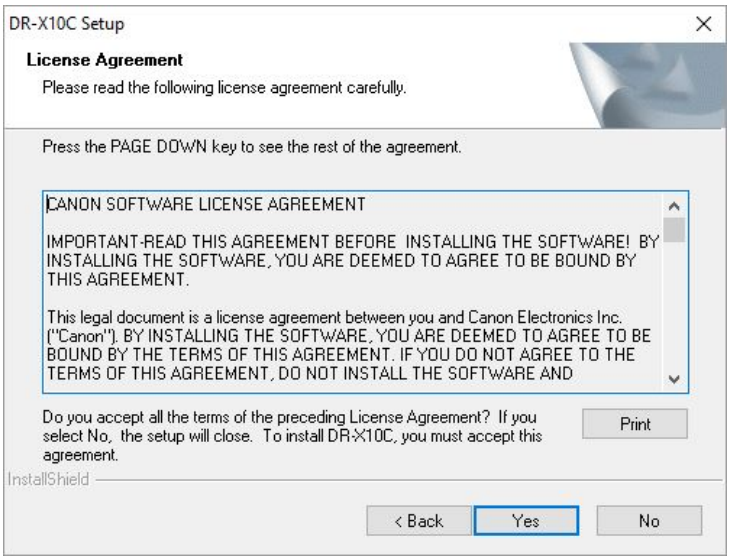


Figure 7.18: License Agreement window

10. From the **License Agreement** window, click **Yes**.
11. The installation begins.

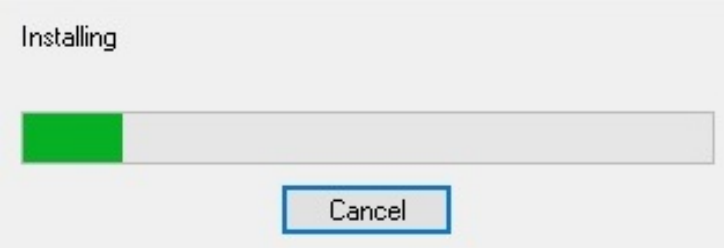


Figure 7.19: Installation progress bar

12. A progress bar appears.

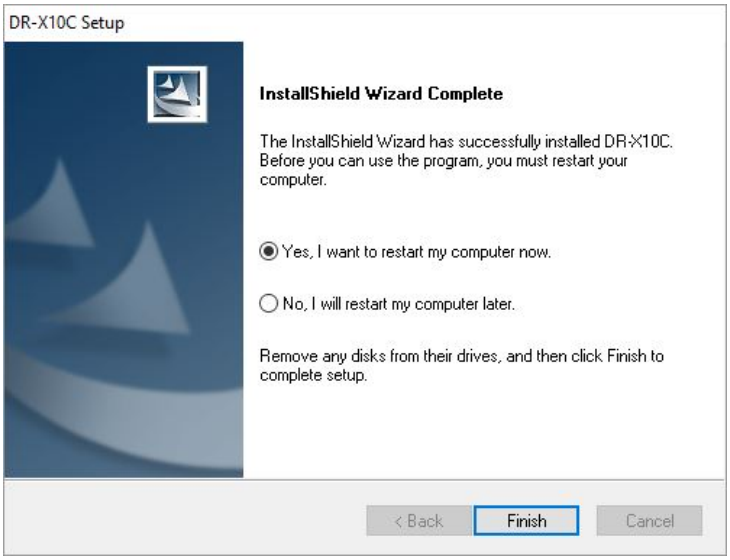


Figure 7.20: Install Shield Wizard Completed window

13. When the installation completes, the **Install Shield Wizard Completed** window appears. Select **Yes, I want to restart my computer now**, then Click **Finish**.

    NOTE: Before restarting the system ensure that all the files are saved.

7.4.2 Connecting the Scanner

Figure 7.21: USB Port on the Back of the Canon DR-X10C Scanner.

1. Locate the USB port on the back and near the bottom of the Canon DR-X10C scanner.
2. Connect the port to a free USB port of the target PC.

   NOTE: Ensure that the cable is not connected to the VRS USB port.
3. Press the power button on the scanner.

7.4.3 Verifying the Installation in Device Manager

NOTE: Ensure the scanner is attached to the PC via a USB port and that it is powered on before verifying that the newly-installed driver appears in Device Manager.

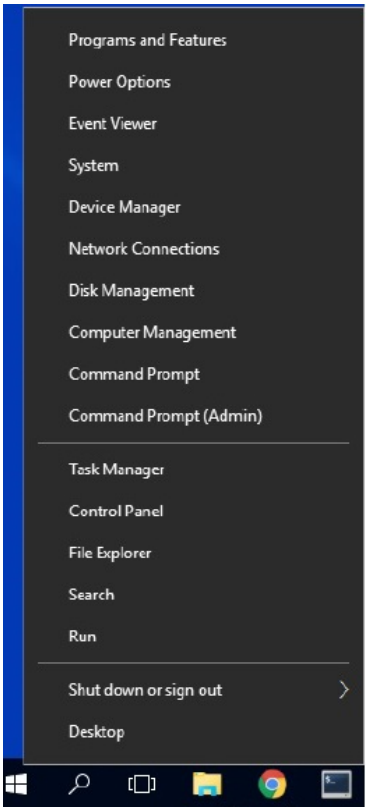


Figure 7.22: Start menu

1. Right-click the **Windows** icon and click **Device Manager**.
2. The **Device Manager** window appears.

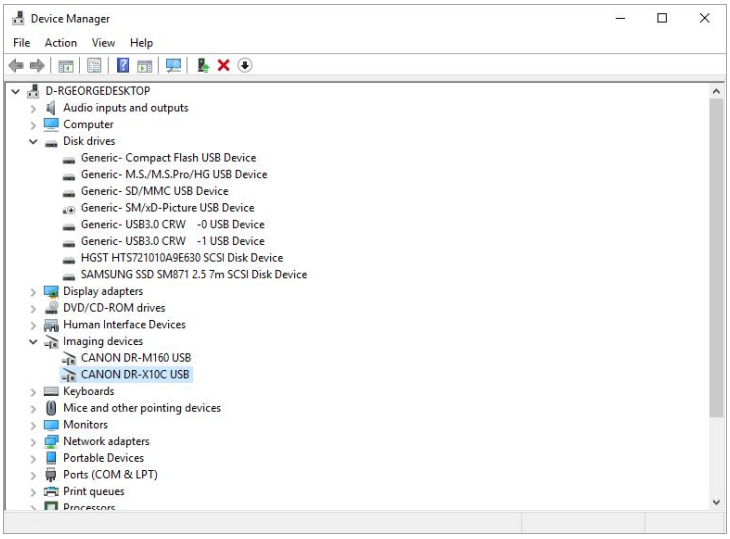


Figure 7.23:

3. From The **Device Manager** window, confirm **CANON-DR-X10C USB** is listed under **Imaging devices**.

   NOTE: If the device does not appear, verify the steps in Section 7.4.1 Installing the Canon DR-X10C Drive were properly executed.

4. Exit the **Device Manager** window and then exit the **Control Panel** window.

7.4.4 Upgrading the Scanner Firmware

For optimal performance with the TWAIN driver, an update to the scanner firmware may be necessary.

1. On a system which is connected to the internet, browse to `https://www.usa.canon.com/internet/portal/us/home/support/details/scanners/document-scanner/imageformula-dr-x10c`
2. Click **Drivers & Downloads**.
3. From the **Drivers & Downloads** section, click **Firmware**.
4. Click **Select** for DR-X10C Firmware Version 2.80
5. Select the agree to the terms of the disclaimer check box, and click **Download**.
6. A self-extracting zip file downloads. Locate the file and open it.
7. Click **Unzip** in the window that appears to unpack the driver installer. A notification appears stating the operation was successful; click **OK** and then click **Close**.
8. From a **Windows Explorer** window, browse to `C:\DRX10C\Firmware\Version 2.80` and double-click **READMEFIRST.pdf**.
9. Follow the manufacturer's instructions in the PDF document to perform the firmware upgrade.

Chapter 8

Canon Scanner Configuration

This chapter covers configuration procedures for Canon scanners.

8.1 Configuring the Canon DR-G1130 and DR-X10C LCD Menu Settings

1. On the scanner, press **Menu**.
2. Scroll using the arrow button until **Long Document** is displayed.
3. Press **Enter**.
4. Using the arrow buttons, select **ON1** and then press the **Enter** button.
5. Scroll using the arrow buttons until **Stand-By Mode** is displayed.
6. Press **Enter**.
7. Using the arrow buttons, select **240** and then press **Enter**.
8. Scroll using the arrow buttons until **Auto PWR Off** is displayed.
9. Press **Enter**.
10. Using the arrow buttons, select **Off** and press **Enter**.
11. To exit the menu and return to the counter screen click the red **Stop Key** on the control panel.

8.2 Canon DR-M160II Long Document Mode

8.2.1 Enabling Long Document Mode

1. From the Desktop, click the **Windows** button. In the **Search** field, type **Canon ImageFORMULA Utility** and press **Enter**. The **Canon ImageFORMULA Utility** window appears.

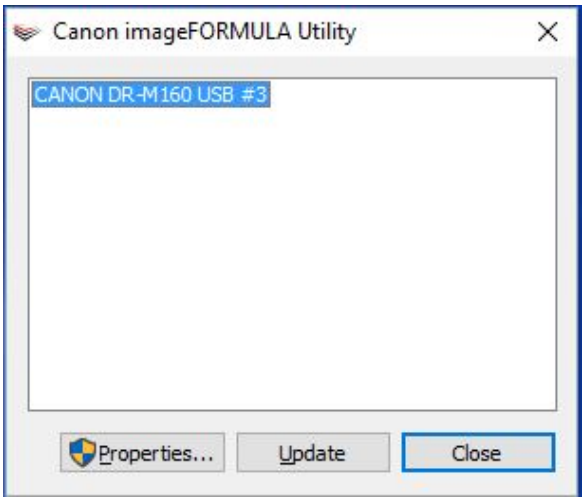


Figure 8.1: Canon ImageFORMULA window

2. From the **Canon ImageFORMULA** window, click **Canon DR-M160 USB** and click **Properties**.

   NOTE: If the Canon DR-M160 USB option does not appear, complete the process in Section 8.2.2 Restoring the STI/WIA Scanner Registry and return step 1 of this section..

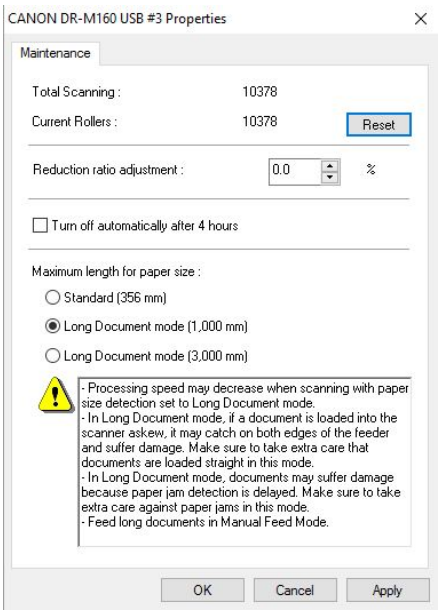


Figure 8.2: Canon DR-M160 USB Properties window

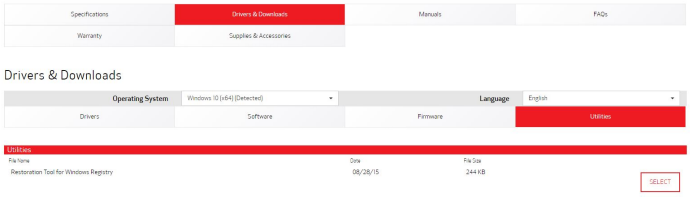
3. From the **Canon DR-M160 USB Properties** window, confirm the **Turn Off automatically after 4 hours** check box is not selected and the **Long Document mode (1,000 mm)** is selected and click **Apply**.

4. Click **OK** and close the **Canon imageFORMULA Utility** window.

8.2.2 Restoring the STI/WIA Scanner Registry

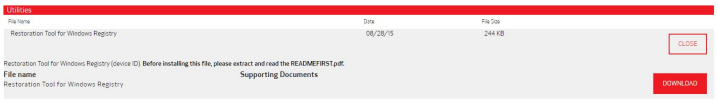
NOTE: Perform the following process only if the Canon DR-M160 USB option did not appear in step 2 of Section 8.2.1 Enabling Long Document Mode.

1. From a workstation connected to the internet, go to `https://www.usa.canon.com/internet/portal/us/home/support/details/scanners/document-scanner/imageformula-dr-m160ii`



2. From the **Drivers & Downloads** section of the webpage, click **Utilities**, and then click **Select** for **Restoration Tool for Windows Registry**.

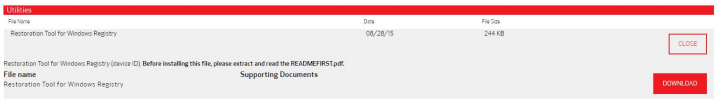
Figure 8.3: Select Restoration Tool for Windows Registry



3. Click **Download** to download the self-extracting executable file.

Figure 8.4: Download the Restoration Tool

4. Navigate to the location of the downloaded executable file. Double-click the file and click **RUN** **OK** if a security warning appears.
5. Select a location to extract to, and unzip or extract the file.
6. Copy the extracted folder/files to the ICC workstation and double-click **RepairReg.exe**.



7. From the **Restoring tool for scanner registry** window, click **Start**.

Figure 8.5: Restoring tool for scanner registry window

8. One of the following messages appears when the issues are found and repaired:

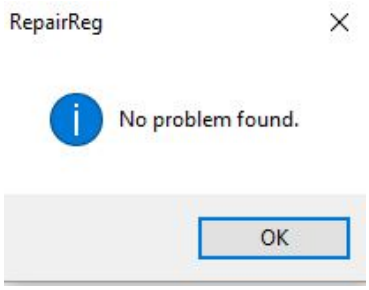


Figure 8.6: No Problem Found message

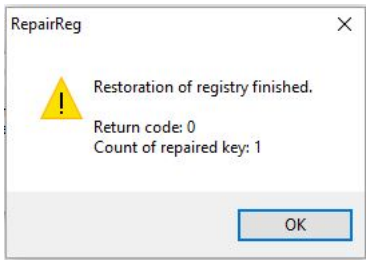


Figure 8.7: Restoration of Registry Finished message

9. Click **OK** and go back to Section 8.2.1 Enabling Long Document Mode.

Chapter 9

ImageCast® Central Application Installation

This chapter covers the installation of the ImageCast® Central application.

9.1 Installing the ImageCast® Central Application

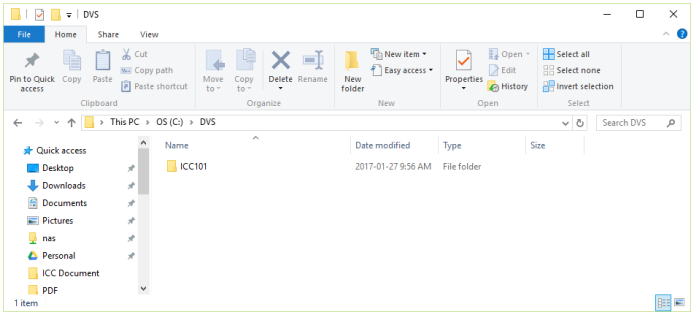


Figure 9.1: DVS Folder

1. Create a folder labeled **C:\DVS**.
2. Within the **C:\DVS** folder create a folder that will store the configuration and results for a single tabulator. Give this folder a name that easily allows for its contents to be identified, eg. **ICC101**.

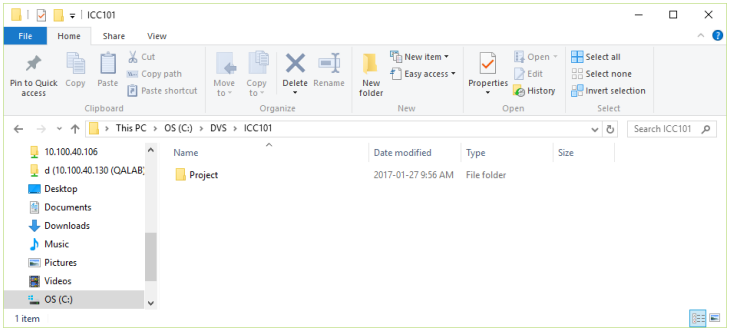


Figure 9.2: ICC101 folder

3. In the new folder created in Step 2, i.e. **C:\DVS\ICC101**, create a subfolder named “project”. Within the Project folder, create a subfolder named “config”. This is where the election files for that tabulator will go.
4. Repeat the previous 2 steps for each additional required tabulator, ensuring that each has its own directory.

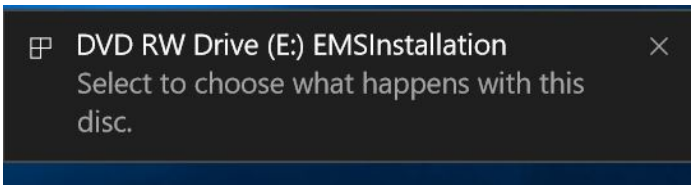


Figure 9.3: Notification (Windows 10)

5. Insert the ICC Installation CD into the CD/DVD drive on your computer.
6. Ignore the notification that appears.

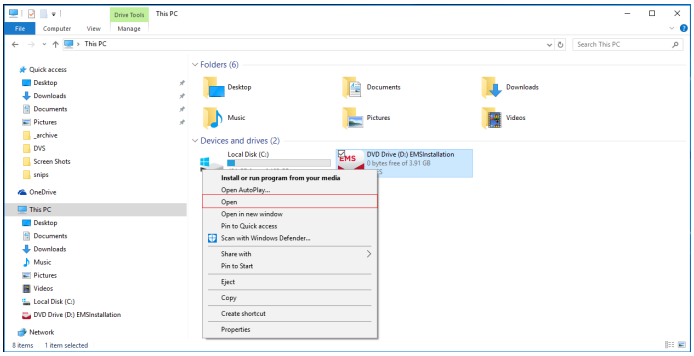


Figure 9.4: Explorer window Windows 10

7. If the installation window does not automatically appear, open **File Explorer**, go to "This PC," then right-click **DVD Driver (D) EMS Installation**. Click **Install or run**.
8. In the installation window, expand **Client Applications** and then **ImageCast Central Client**. Double-click **32 bit version** to open the installation program.

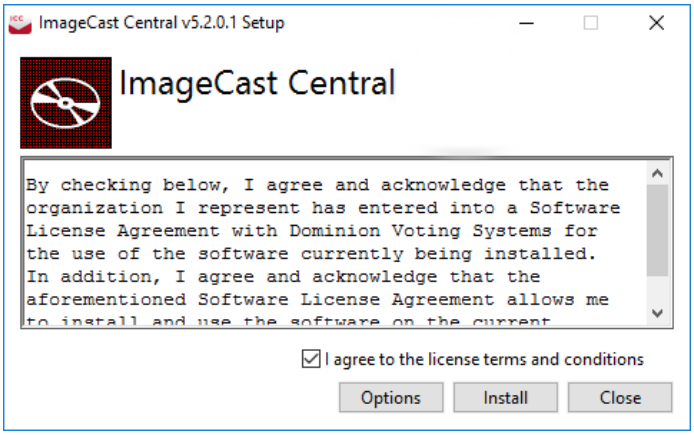


Figure 9.5: Accept license terms

9. The ImageCast Central installer window will open.
10. Select the **I agree to the license terms and conditions** check box then click **Install**.

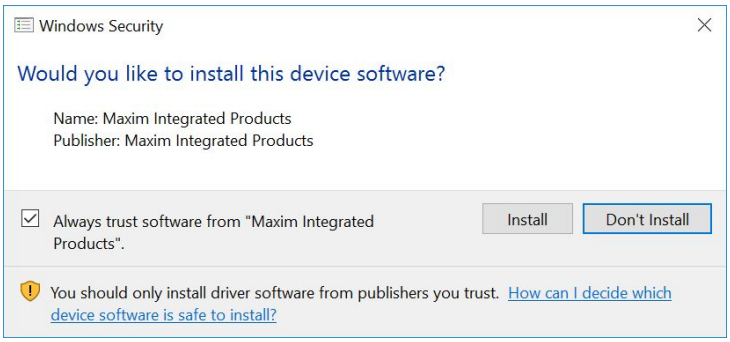


Figure 9.6: Always trust software

11. The first item to be installed will be the third-party software required to use iButton security key.
12. If a windows security screen appears with permission to install Maxim Integrated Products, select the **Always trust software from Maxim Integrated Products** check box and click **Install**.
13. Once the ICC Client application installation is done click the "Next" to proceed.

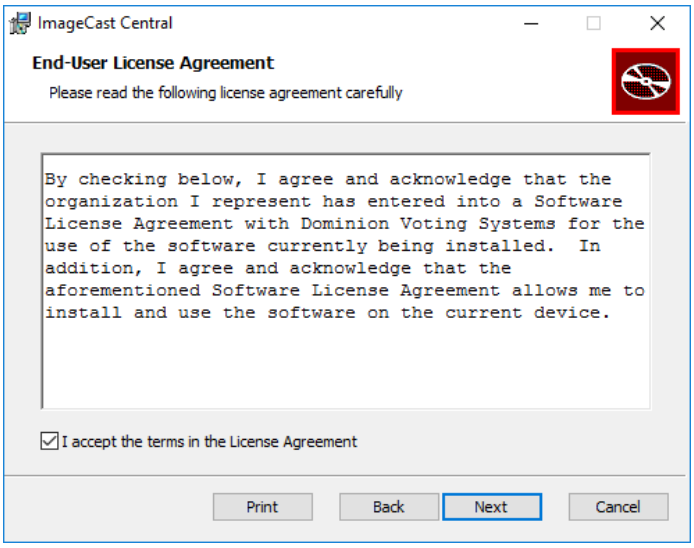


Figure 9.7: End user agreement

14. Select the **I accept the terms in the License Agreement** check box then click **Next** to proceed.
15. On the **Destination Folder** screen click **NEXT**.
16. Click **Install**.

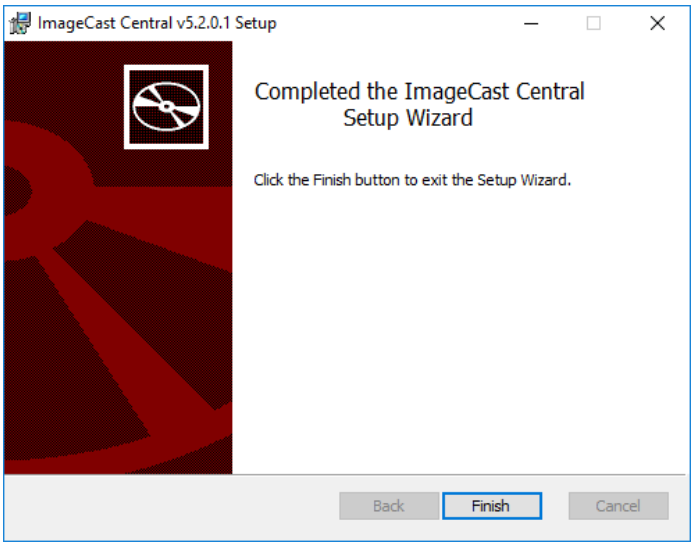


Figure 9.8: ImageCast Central setup complete

17. Click “Finish” to complete the installation process.
18. Click “Close” on the Installation Successfully Completed window.

Chapter 10

ImageCast® Central Acceptance Test Procedures

This chapter covers procedures for testing the ImageCast® Central system after installation and verifying the correct functioning of the system and all of its components.

10.1 Verifying Hardware Connections

Ensure that the 1-Wire reader is connected to the same USB port used in the above 1-Wire installation steps. Attach the scanner to the same USB port used when the scanner driver was installed. If results files are to be uploaded, ensure that the PC is connected to a network.

10.2 Installing Election Definition Files

All application programs need data, and the ICC application receives its data from Dominion Voting Systems' Election Management System (EMS).

The EMS files are specific to each election and to each tabulator. They must be installed prior to using ICC. Perform the following steps to do so:

1. Create directories for each tabulator that will be used in the election - see Section 9.1.
2. Copy, and unzip (if necessary) the election configuration files received from EMS. Two directories from EMS, "dcf" and "election", should be copied into the "\Project\config" folder corresponding to the appropriate tabulator.
3. The **Election** directory contains Voting Information Files (VIF) which describe the Election, Ballots, Contests, and Candidates of the particular election.
4. The **DCF** directory contains Device Configuration Files (DCFs) which define nuances in the way the particular ICC tabulator processes and reports the ballots scanned. The two subdirectories should contain the files seen in Figures 10.1 and 10.2, respectively.

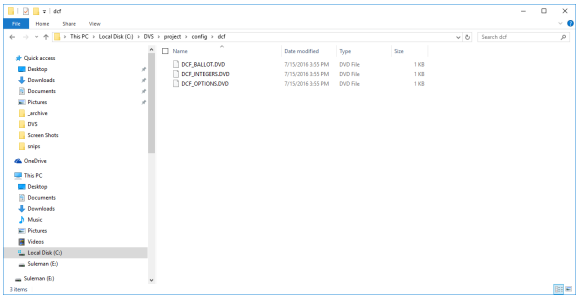


Figure 10.1: Contents of 'dcf' folder

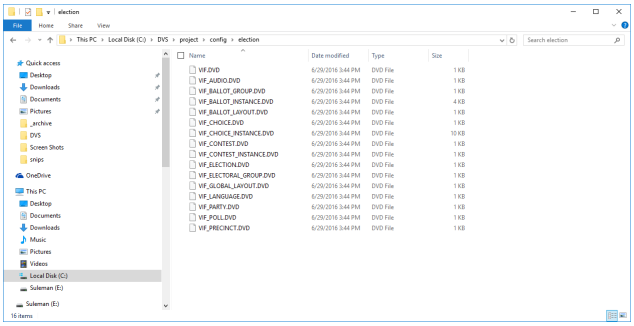


Figure 10.2: Contents of 'election' folder

10.3 Running the ImageCast® Central Application

You should also have the "Administrator Security Key" (iButton) programmed by EMS to match the installed election files. An accompanying passcode is required in order to use the iButton and unlock the election files at ICC startup.

1. On the Window's Taskbar, click the pinned ICC application icon.
2. Accept the UAC confirmation dialog by clicking **Yes**. Preliminary initialization will occur.

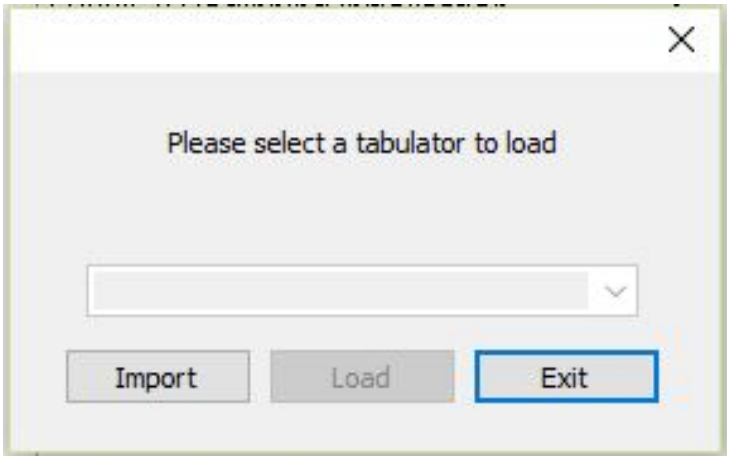


Figure 10.3: Select a tabulator to load

3. Once complete, you will be asked to select a tabulator to load. Click **Import**.

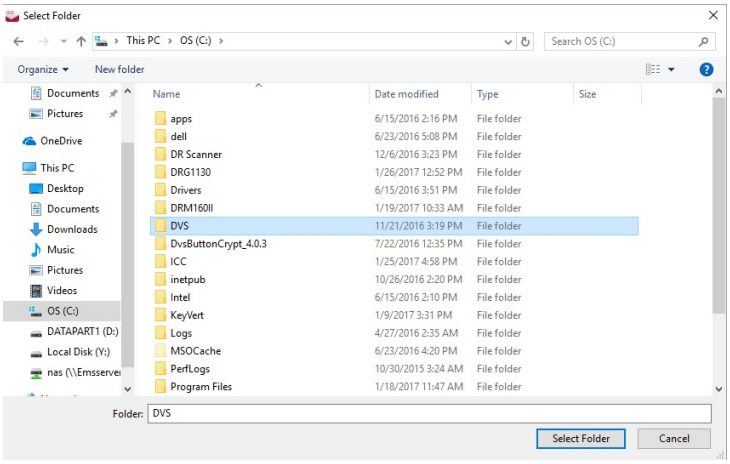


Figure 10.4: DVS filder

4. The **Select Folder** window appears. Browse to the folder created in Step 1 of Section 9.1 that contains the tabulator project subfolder, e.g. **C:\DVS**.

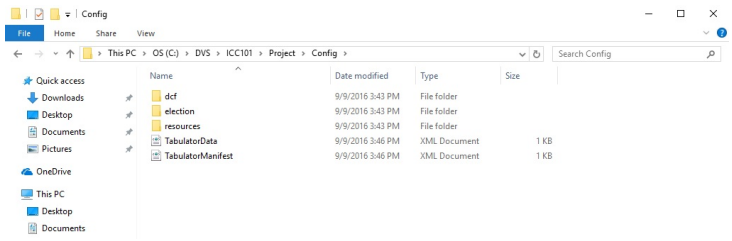


Figure 10.5: Contents of tabulator project subfolder

5. From within this folder, select the tabulator project subfolder created in Step 2 of Section 9.1 e.g. **C:\DVS\ICC101**, and click **Select Folder**.

   NOTE: Within the tabulator project subfolder is a folder named **Project** within which there is a folder named **Config** which contains the election files, e.g. **C:\DVS\ICC101\Project\Config** as seen in Figure 10.5

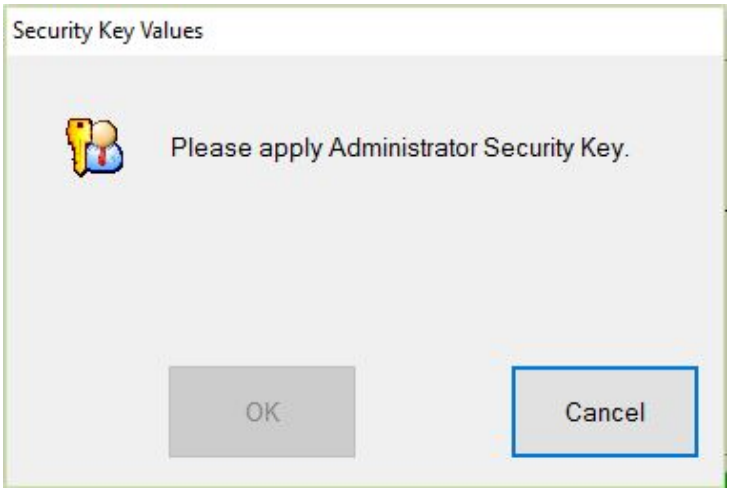


Figure 10.6: Apply the Administrator Security key

6. A prompt appears to apply the Administrator Security key to the 1-Wire Reader. When prompted, enter the passcode it was delivered with.

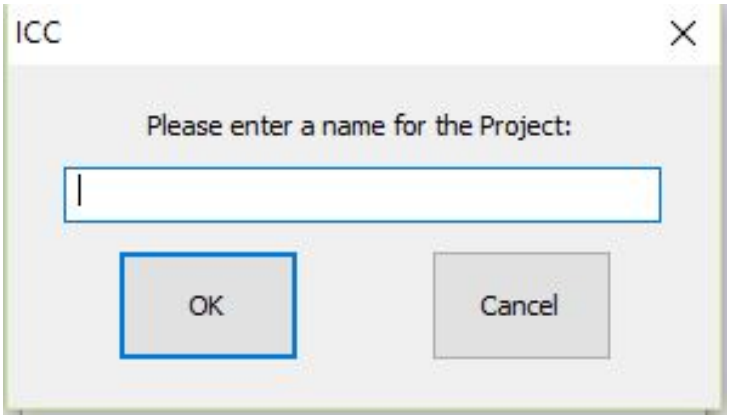


Figure 10.7: Enter a name for the project

7. Finally, enter a name that will help easily identify that specific tabulator in the list.

8. Repeat the last 4 steps until all necessary tabulators have been imported.
9. To begin, select a tabulator from the newly populated list, and click **Load**.
10. A prompt appears again to apply the Administrator Security key to the 1-Wire Reader. When prompted, enter the passcode it was delivered with.

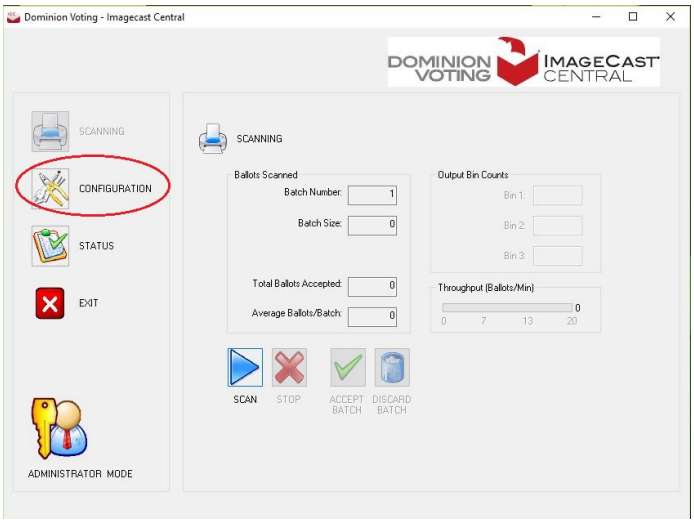


Figure 10.8: Scanning screen

11. The main ICC screen then loads.
12. On the left-hand side of the screen, click the **Configuration** icon.

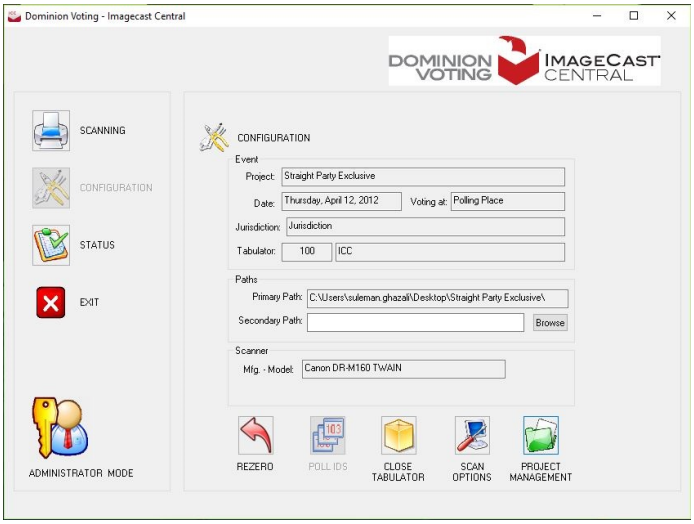


Figure 10.9: Configuration screen

13. Set the **Secondary Path** field to the appropriate location: to either a Mapped network drive or an IP address and folder name.

    NOTE: Ensure the Network Discovery has been enabled. See Section 6.7.

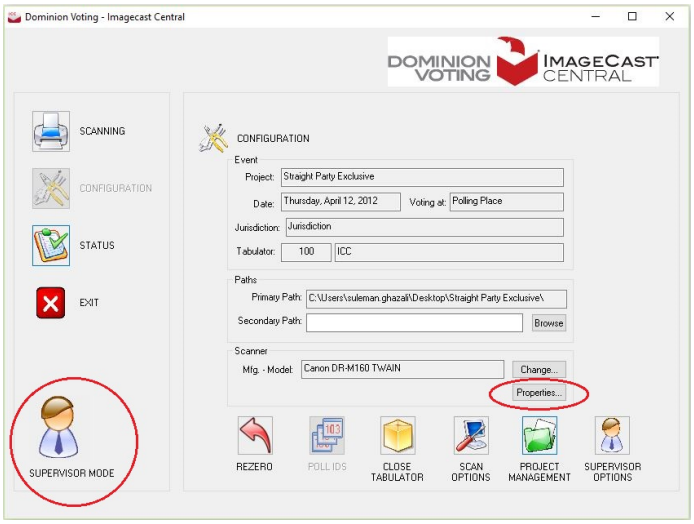


Figure 10.10: Scanner properties

14. Click the **Administrator Mode** icon to enter Supervisor Mode and enter the Supervisor passcode.
15. Click **Properties**.

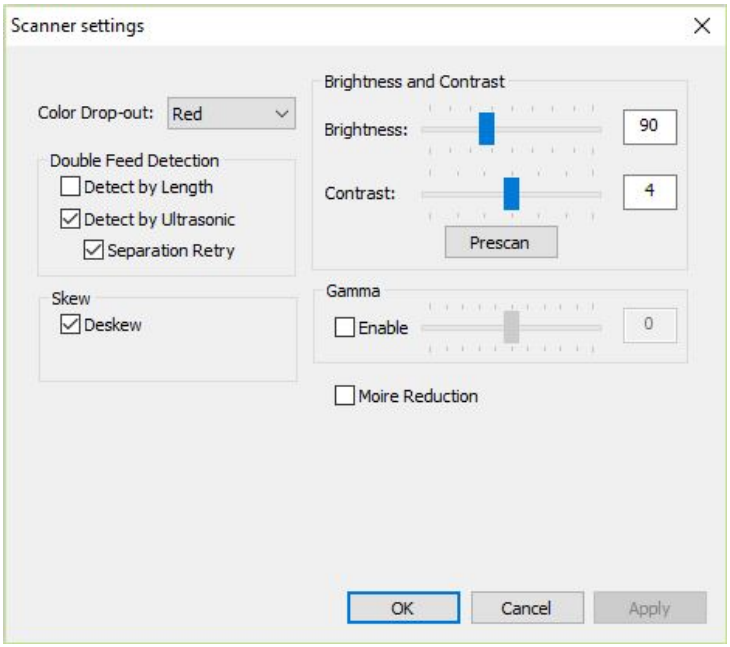
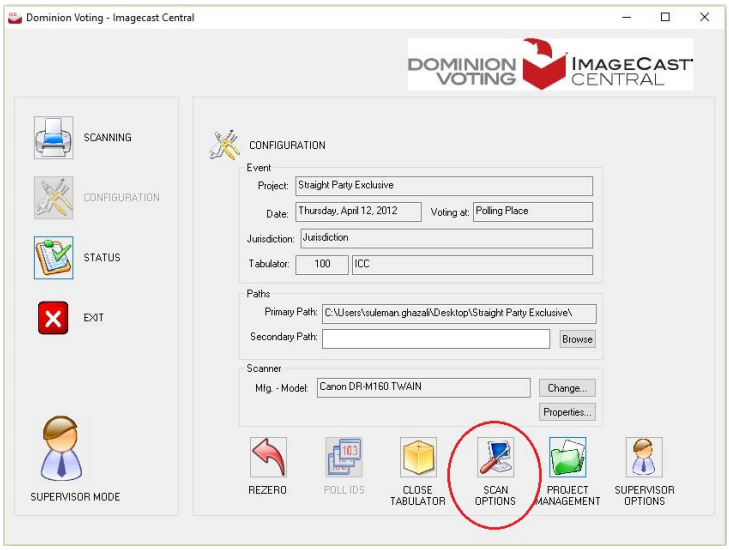


Figure 10.11: Scanner setting window

16. The **Scanner Settings** window appears. The settings presented here may need to change depending on a number of conditions, such as ballot print quality. However, the following settings are recommended: **NOTE:** The scanner setting options will vary depending on the scanner model.

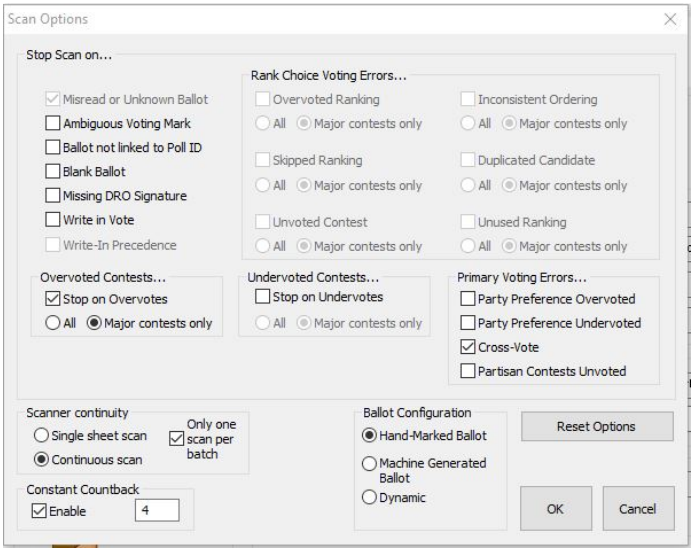
    - **Color Drop-out**: Red
    - **Detect by Ultrasonic**: Selected
    - **Separation Retry**: Selected (not available on all scanners)
    - **Deskew**: Selected
    - **Edge Cleanup**: Selected (not available on all scanners)
    - **Doc Orientation**: Portrait
    - **Brightness**:
        - Set to 90 for DR-G1130
        - Set to 110 for DR-M160II and DR-X10C
    - **Contrast**: 4
    - **Gamma**: Not selected
    - **Moire Reduction**: Not selected

17. The Prescan button can be used to test settings, by allowing for a ballot to be scanned so its image can be visually inspected but without the ballot actually being counted.
18. Click **OK**.



19. Click **Scan Options** to display the **Scan Options** window.

Figure 10.12: Scan Options window



20. From this window, the settings for when to stop ballots can be configured, as well as continuity and endorser settings.
21. Click **OK** to exit.
22. Return to Administrator Mode by clicking the **Supervisor Mode** icon. No passcode is required.

Figure 10.13: Scanner properties

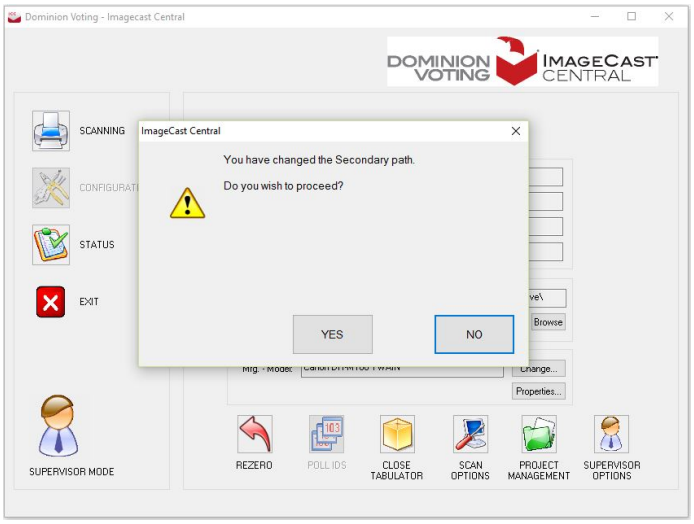


Figure 10.14: Server path confirmation

23. Click the **Scanning** icon in the left-hand panel to return to the Scanning page. The application will ask you to confirm the Server Path name change. Click **Yes**.

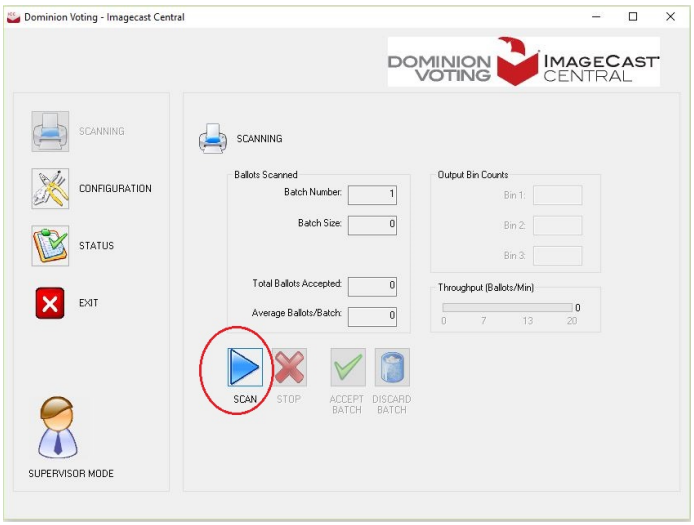


Figure 10.15: Scanning page

24. Place a batch of ballots onto the scanner input tray and press the **Scan** icon.

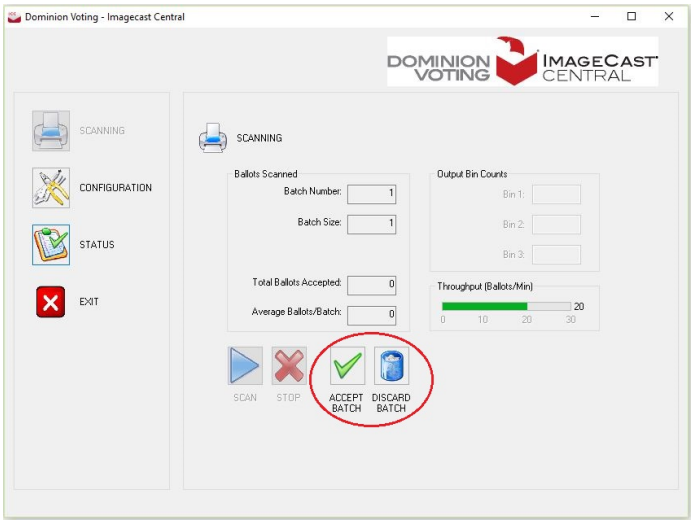


Figure 10.16: Accept/Discard Batch

25. The ballots are fed through the scanner and processed by the ICC application. You will notice the "Batch Size" increase appropriately. When all ballots have been scanned, you will be given the option to either "Accept" or "Discard" the batch.

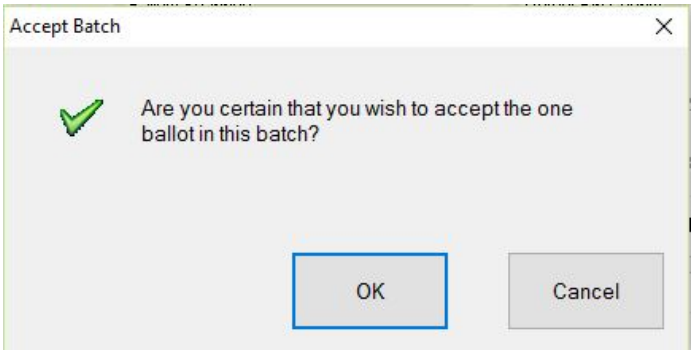


Figure 10.17: Accept Batch Confirmation

26. Click **Accept Batch** to accept this batch of ballots. You are prompted to confirm the choice. Click **OK**.

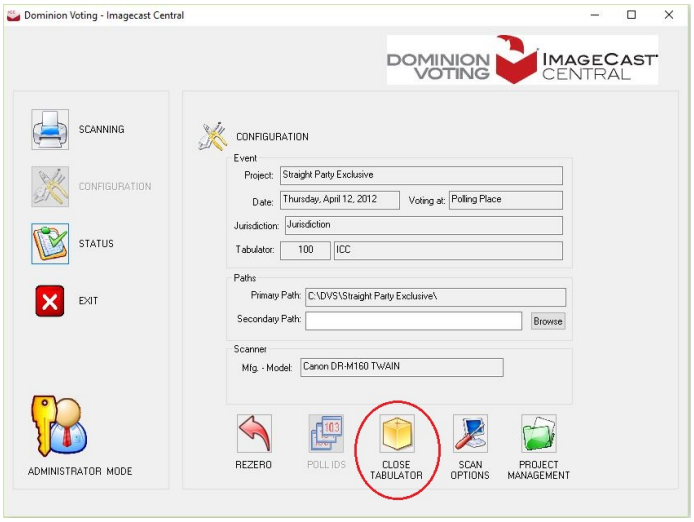


Figure 10.18: Close Tabulator button

27. Return to the **Configuration** screen and click the **Close Tabulator** icon at the bottom.

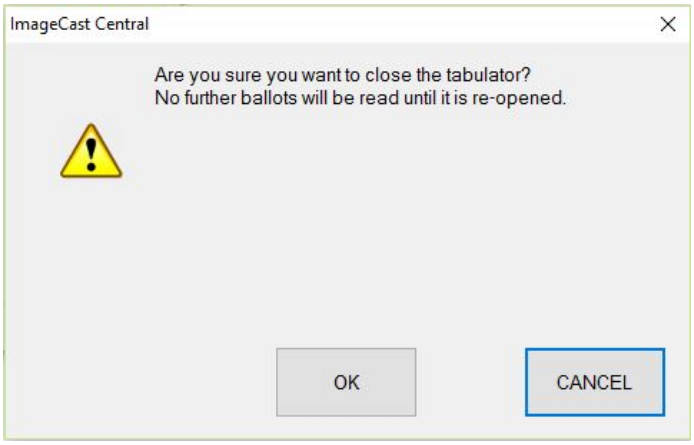


Figure 10.19: Close Tabulator Confirmation

28. You are again prompted to confirm your selection. Click **OK**.

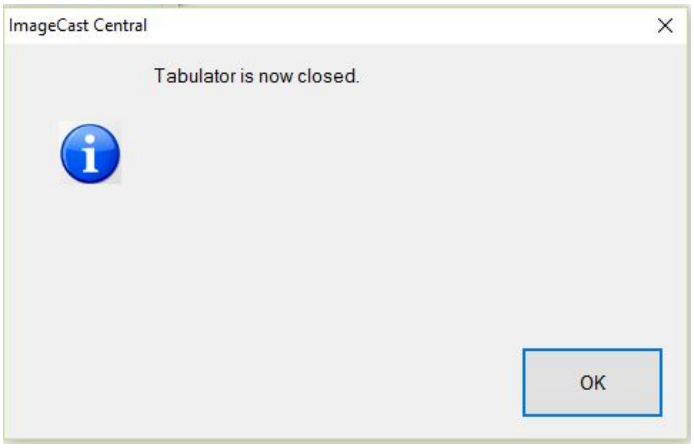


Figure 10.20: Close Tabulator Confirmation

29. A confirmation message that the tabulator has closed is displayed. Click **OK**.

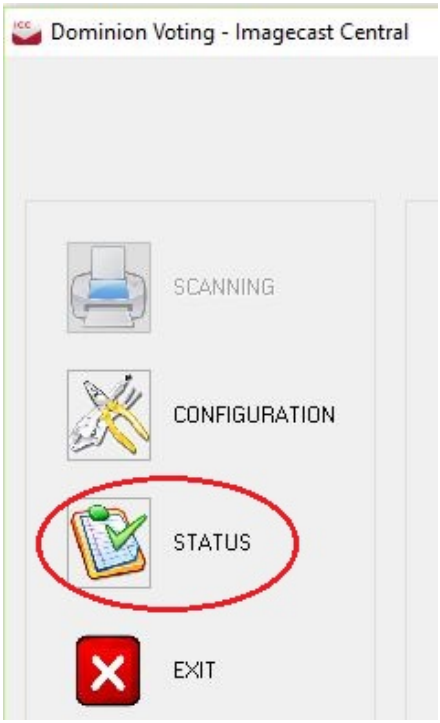


Figure 10.21: Status button

30. Go to the **Status** screen.

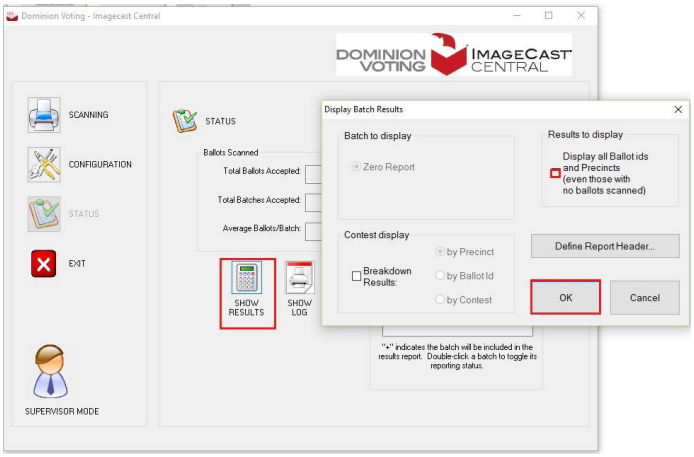


Figure 10.22: Show Results icon and dialog

31. From the **Status** screen, click the **Show Results** icon. This will bring up a dialog box.
32. Clear the **Display all Ballot ids and Precincts (even those with no ballots scanned)** check box. This removes ballots' IDs that have yet to be scanned from your results reports.
33. Click **OK**.

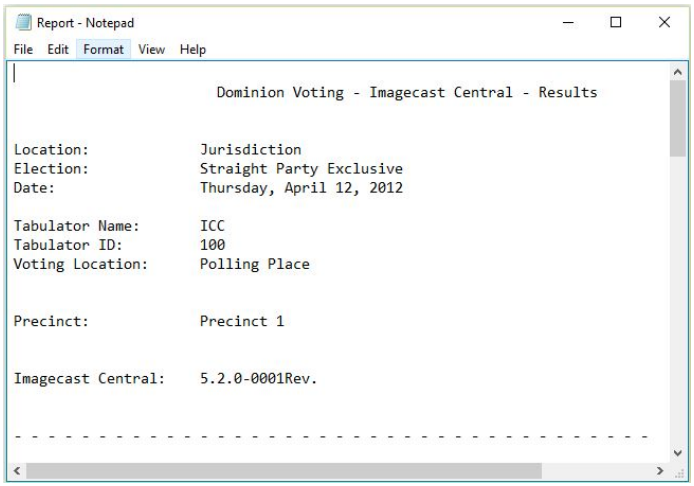


Figure 10.23: Results Report in Notepad

34. Notepad launches, and contains the election results for the batch of ballots just scanned. Verify the contents, and then close Notepad.

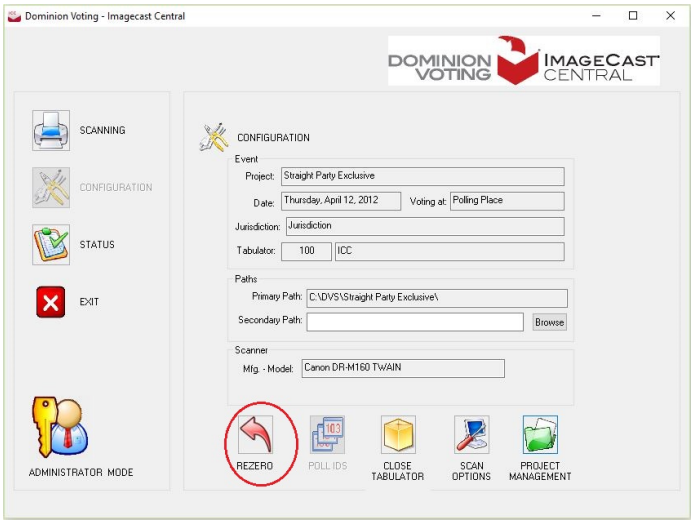


Figure 10.24: Re-zero button

35. Return to the **Configuration** screen.
36. Click **Rezero** at the bottom of the screen. This clears the system of the test batch scanned earlier.

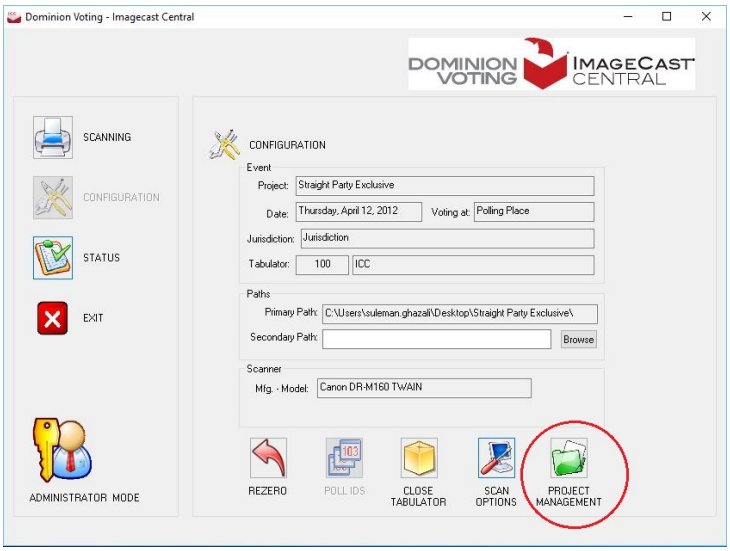
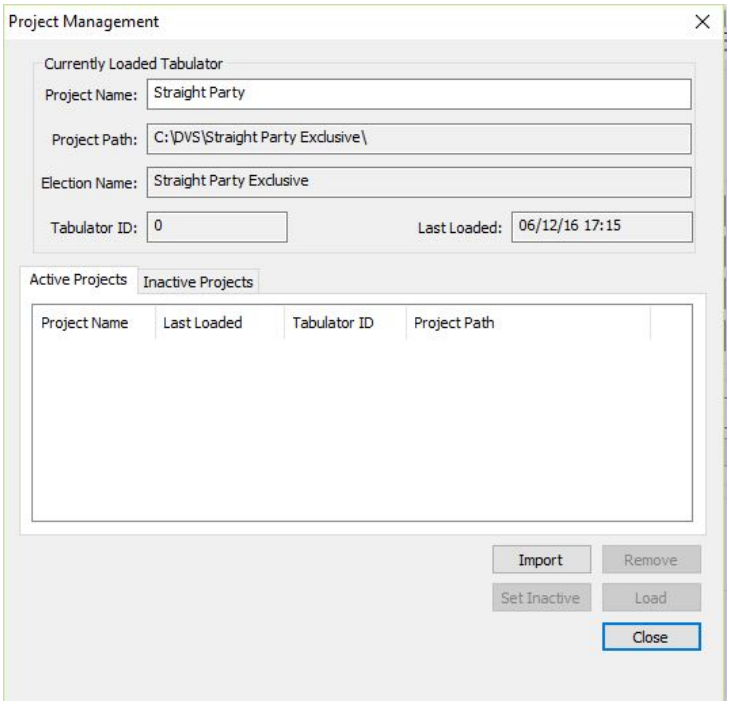


Figure 10.25: Project management window

37. Click **Project Management** to open the **Project Management** window.



38. From this window, new tabulators can be imported, and the active tabulator can be switched. Click **Close** to exit.

Figure 10.26: Project Manangement window

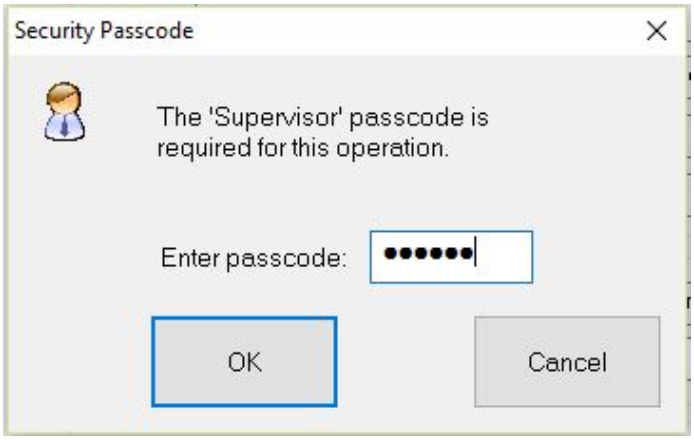


Figure 10.27: Security Password Prompt

39. Enter the Supervisor password and click **OK**.

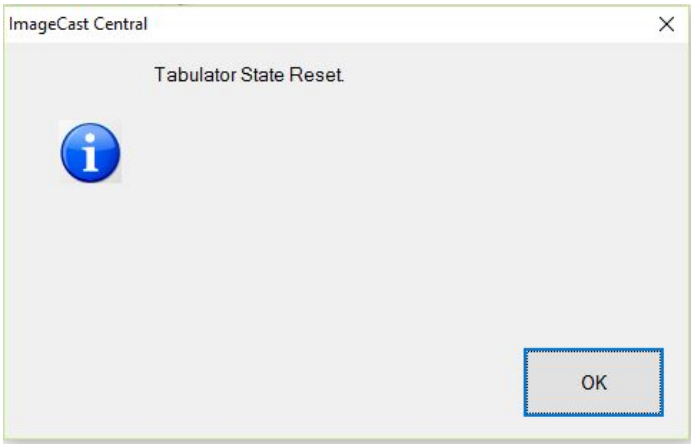


Figure 10.28: Security Password Prompt

40. A confirmation message that the tabulator is reset is displayed. Click **OK**.

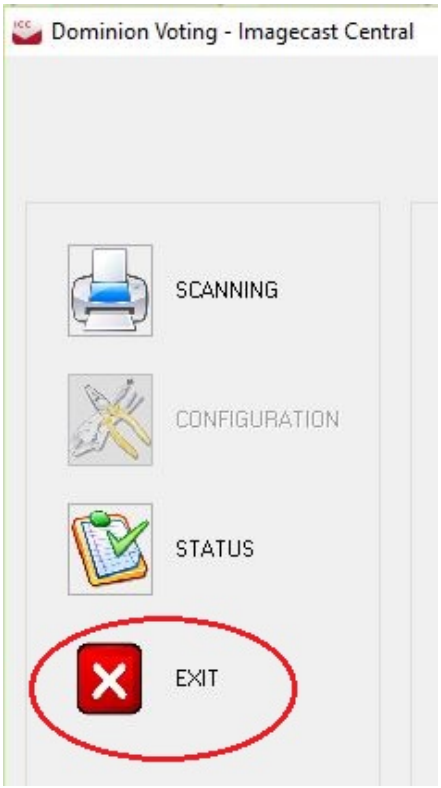


Figure 10.29: Exit button

41. Exit the ICC application by clicking the **Exit** icon located on the bottom of the left-hand panel.

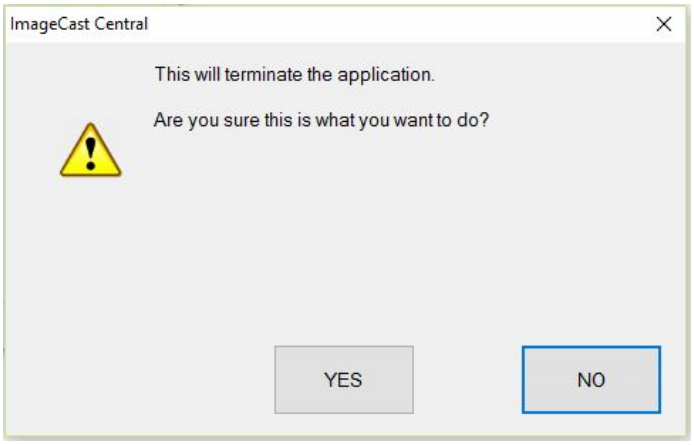


Figure 10.30: Exit button

42. A prompt appears asking to confirm the choice to exit. Click **Yes**.

Chapter 11

Hardening Procedures

This chapter covers hardening procedures for the ImageCast® Central Workstation.

11.1 Securing Tabulator Folders

Once ICC configuration is complete, the security permissions on the tabulator folders can be altered to ensure that only Administrators can modify the files within.

1. While logged in as an Administrator, open a File Explorer window to the C drive
2. Right-click on a tabulator folder (which contains the Project subfolder and election files for one tabulator) and select Properties
3. Select the Security tab, and select Advanced
4. At the top of the window, where it specifies the Owner, click Change
5. Hit the Cancel button on the user selection window to return back to the advanced settings window
6. To enable inheritances, click **Disable Inheritance**.
7. A pop-up appears asking how to handle the previously inherited permissions select the "explicit" option
8. From the list of user groups, select Users and click **Edit**.
9. Ensure that only **Read and Execute**, **List Folder contents**, and **Read** are the only permissions selected. Click **OK**.
10. Repeat steps 9 and 10 for the Authenticated Users group
11. Select the **Replace all child object permission** check box.
12. Click **OK**, and then **Yes** to confirm
13. Repeat these steps for each tabulator folder

Once these settings are in place, User-level accounts require the confirmation of an Administrator password to modify the contents of a tabulator folder in any way.

11.2 Final BIOS Configuration

After the system installation is complete, external boot devices must be disabled in the BIOS. An Admin password for the BIOS must also be set.

For final BIOS configuration steps specific to Dell computers, refer to Section A.2.

11.3 Applying Windows Hardening Templates

Advanced hardening procedures are available to place increased security measures on the ImageCast® Central workstation.

Please refer to *Democracy Suite EMS System Installation and Configuration Procedure*, section Operating System Hardening Procedures and follow the instructions, using the Windows 10 option where applicable.

Appendices

Appendix A

BIOS Configuration for Dell Computers

This appendix contains BIOS configuration steps for **Dell** servers and computers.

A.1 Pre-Installation BIOS Configuration

The following BIOS configuration steps are performed on a new system, before the the ImageCast® Central installation procedure, beginning with Chapter 4.

These steps are common to most non-server Dell computers, including:

- Dell Latitude 7440
- Dell Latitude 7450
- Dell OptiPlex 9020 All-In-One
- Dell OptiPlex 9030 All-In-One
- Dell OptiPlex 7440 All-In-One
- Dell Precision T1700
- Dell Precision T3420

The steps in each section are performed in the system's BIOS menu. To enter the BIOS menu:

1. Start the computer. If the computer is already running, restart the computer.
2. When the Dell logo appears, press **F2** to enter the BIOS menu.
3. If you have already enabled the Admin password, the BIOS settings menu will be locked and must be unlocked before making changes. Enter the Administrative password and click **OK**.

   NOTE: In some cases it may be required to click **Unlock** on the BIOS setup screen, to input the password.

A.1.1 Restoring Factory Settings

1. In the BIOS menu, click **Restore Settings**.
2. Select **Factory Settings**.
3. Click **OK**.
4. A warning message appears. Click **OK** to continue.
5. A notification appears. Click **OK** to restart the system.

NOTE: BIOS passwords are not affected by the Factory Settings restore. If the Admin Password has been set, it remains unchanged.

A.1.2 Enabling UEFI Boot Mode

1. In the BIOS menu, expand the **General** node and select **Boot Sequence**.
2. Under **Boot List Option**, select **UEFI**.
3. Click **Apply**.
4. A confirmation message appears. Click **OK** to continue.

A.1.3 Disabling Legacy Option ROMs

Before enabling Secure Boot, **Legacy Option ROMs** must be disabled.

1. In the BIOS menu, expand the **General** node and select **Advanced Boot Options**.
2. Clear the **Enable Legacy Option ROMSs** check box.
3. Click **Apply**.
4. A confirmation message appears. Click **OK** to continue.

A.1.4 Enabling Secure Boot

1. In the BIOS menu, expand the **Secure Boot** node and select **Secure Boot Enable**.
2. Under **Secure Boot Enable**, select **Enabled**.
3. Click **Apply**.
4. A confirmation message appears. Click **OK** to continue.

A.1.5 Disabling Wireless Devices

NOTE: This section applies only to computers with wireless network adapters. It does not apply to Dell Precision computers.

1. In the BIOS menu, expand the **Wireless** node and select **Wireless Device Enable**.
2. Under **Wireless Device Enable**, clear all check boxes for wireless devices (**WLAN/WiGig** and **Bluetooth**).
3. Click **Apply**.
4. A confirmation message appears. Click **OK** to continue.

A.1.6 Enabling SMART Reporting

1. In the BIOS menu, expand the **System Configuration** node and select **SMART Reporting**.
2. Under **SMART Reporting**, select **Enable SMART Reporting**.
3. Click **Apply**.
4. A confirmation message appears. Click **OK** to continue.

A.1.7 Restarting the Computer

Once the BIOS configuration is complete, click **Exit** to restart the computer.

A.2 Post-Installation BIOS Configuration

After the system installation is complete, external boot devices must be disabled in the BIOS. An Admin password for the BIOS must also be set.

A.2.1 Disabling External Boot Devices

1. With the system powered on, insert a disc into the DVD-ROM drive.
2. Restart the system.
3. When the Dell logo appears, press **F2** to enter the BIOS menu.
4. In the BIOS menu, expand the **General** node and select **Boot Sequence**.
5. Under **Boot Sequence**, clear the DVD-ROM drive check box. Ensure the **Windows Boot Manager** check box remains selected.
6. Click **Apply**.
7. A confirmation message appears. Click **OK** to continue.

A.2.2 Disabling Boot From USB

1. In the BIOS menu, expand the **System Configuration** node and select **USB Configuration**.
2. Under **USB Configuration**, clear the **Enable Boot Support** checkbox.
3. Click **Apply**.
4. A confirmation message appears. Click **OK** to continue.

A.2.3 Enabling Strong Password Requirement

To enable the requirement for strong BIOS passwords:

1. In the BIOS menu, expand the **Security** node and select **Strong Password**.
2. Under **Strong Password**, check **Enable Strong Password**.
3. Click **Apply**.
4. A confirmation message appears. Click **OK** to continue.

A.2.4 Enabling Admin Lockout

When Admin Lockout is enabled, the BIOS menu can not be viewed without entering the Admin password.

1. In the BIOS menu, expand the **Security** node and select **Admin Setup Lockout**.
2. Under **Admin Setup Lockout**, check **Enable Admin Setup Lockout**.
3. Click **Apply**.
4. A confirmation message appears. Click **OK** to continue.

A.2.5 Enabling Admin Password

The Admin password protects the computer by restricting access to the BIOS, where settings can be viewed and modified. A strong password is required.

1. In the BIOS menu, expand the **Security** node and select **Admin Password**.
2. Under **Admin Password**, enter the new password and confirm the new password. If a password has already been set, enter the old password as well.
3. Click **OK**.

NOTE: To remove an existing password, enter the old password, leave the new password fields blank and click **OK**.

A.2.6 Restarting the Computer

Once BIOS configuration is complete, click **Exit** to restart the computer.