# System Hardening Procedures

***URCVT v. 1.2.0 16-NY System Hardening Procedures v. 1.0.0*** document is solely for use in the State of New York. This document can be expanded or updated as is necessary or required. Any recommendations listed in this document should not supersede user jurisdiction procedures or other controlling governance entities.

***URCVT v. 1.2.0 16-NY System Hardening Procedures v. 1.0.0***

The hardware used to house the Universal Ranked Choice Voting Tabulator, URCVT, software should, at minimum, follow the steps below to ensure the hardware is adequately protected against unauthorized access, theft of data, and/or malicious attacks.

Hardening of the operating system (Windows 10) is a way to make the computer and data more secure. It may include removing unused applications and files, establishing password login protection on Windows 10, disabling automatic windows login, keeping the system updated appropriately, proper configuration of the system, applying patches, and security updates, among other things. No unauthorized software should be installed on the computer unless authorized by the NYSBOE or the vendor as per New York State Security Procedures. All URCVT systems must include only the following software:

- Windows 10 Pro with the latest service pack installed
- URCVT v. 1.2.0
- Microsoft Excel
- Notepad
- Microsoft .NET Framework 3.8
- Microsoft .NET Framework 4.5
- Users must also retain access to:
    - Command Prompt
    - Digital Signature tools
    - Decryption tools
- Optional anti-virus software
- Optional UPS and printer drivers

In addition to the system hardening protocols, it is recommended that only authorized users (no less than two bipartisan employees) should have physical access to the standalone computer. The computer should be in a secure location.

## Windows Update Procedures

### Preparing Offline Updates

URCVT should run on a workstation that is in a closed environment (not on a network) without access to the internet. Hardware drivers, updates, and virus protection should be downloaded on another computer and transferred to the workstation by a removable device such as a USB

flash drive. Prepare for offline updates by downloading the following to the USB drive designated for use for this purpose: Hardware Drivers, Windows Updates, Windows Defender Offline Updates.

**Hardware Drivers**

- Locate the computer identification information provided by the manufacturer.
- On a second internet connected computer, locate the appropriate hardware drivers necessary to complete computer setup.
- Download the .cab driver package and extract it.
- Copy the extracted files to a USB drive. Keep the USB drive for the next procedure.

**Windows Updates**

- On a second machine connected to the Internet, go to http://download.wsusoffline.net/ and download the latest WSUS Offline Update version.
- Extract the downloaded archive.
- Navigate to the extracted archive and double-click on UpdateGenerator.exe.
- Verify the following settings are checked:
    - Under Windows 10x64 versions, select:
        - Your current version of Windows 10
    - Under Options, select:
        - Verify downloaded updates
        - Use 'security only updates' instead of 'quality rollups.'
            - Include C++ Runtime LIbraries and .NET Frameworks
        - Under USB medium, select:
            - Copy **updates for selected products into the directory** and next to it set the directory where the program will download the updates.

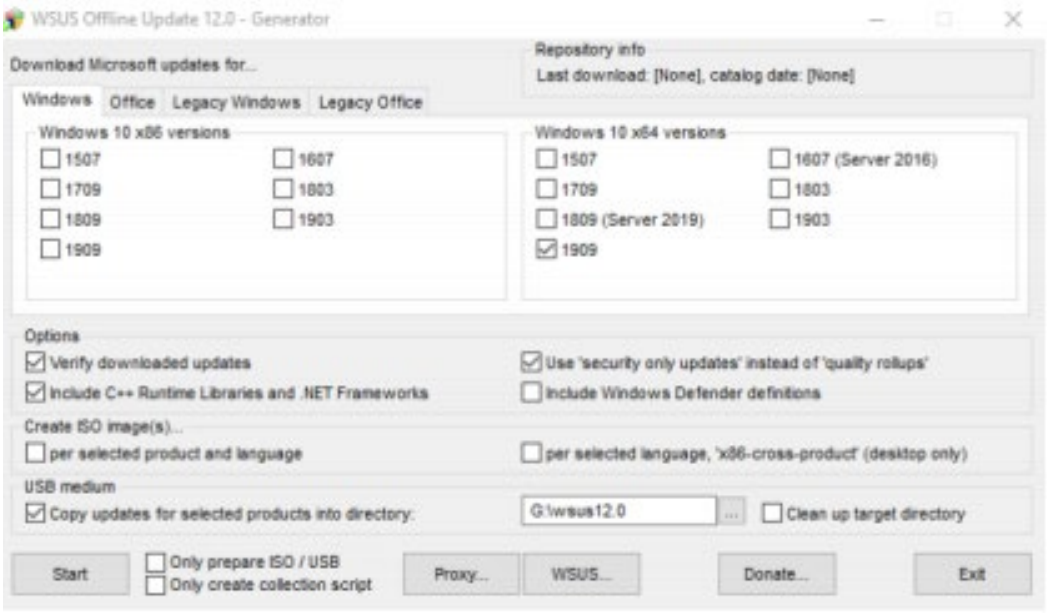

Figure 2-1: WSUS Offline Updater Settings

- Click **Start**.
- If the version check window appears asking to update WSUS click NO. WSUS opens several command line windows to perform operations.
- When the complete dialog window appears asking if you would like to review the log file, click **NO**.
- Copy extracted files to a USB drive. Keep the USB drive for the next procedure.

**Windows Defender Offline Updates**

- On a second computer connected to the Internet, go to the following website: https//www.microsoft.com/en-us/wdsi/definitions
- Find the link for Windows Defender in Windows 10 (64 bit). Click the link to download the update.
- Transfer the downloaded file to a USB drive and keep for later installation. As a note, all USB drives used for these purposes should be kept in a safe place in manufacturer recommended conditions.

## Configuration of Windows Updates

This section covers the configuration of the operating system and hardware drivers. Since the workstation is not connected to the internet, updates and security patches must be installed manually.

Note: Depending on the build of your Windows 10, the UI might be slightly different than described in the section below. This document follows Windows Pro 10, build 1909. You should use your current version of Windows 10.

Drivers and Tools

Proper drivers may be required for each device needing to be installed. This depends on the hardware that you are using.

- At the non-internet connected workstation, connect the USB drive prepared in section above, titled *Preparing for Updates*.
- Click **Start**, search **Device Manager** and open it.
- In **Device Manager**, expand the **Other Devices** section.
- Right-click the first driver with a yellow icon and select **Update Driver Software**.

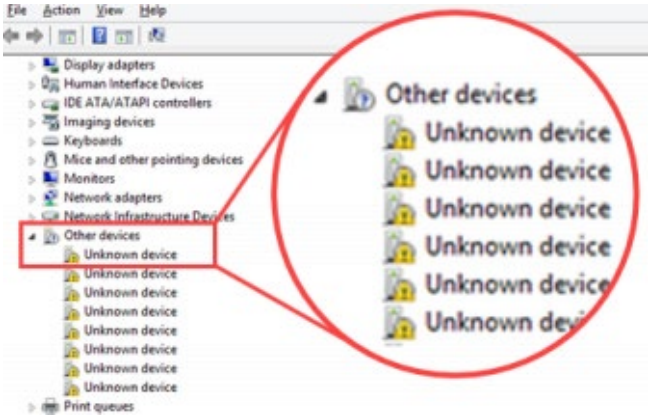


Figure above: Unknown devices in Device Manager

- Follow the prompts.
- When asked, "*How do you want to search for driver software,"* select **Browse my computer for driver software.**
- Click **Browse**.
- On the Browse for Folder dialog, navigate to the extracted driver files on the USB drive.
- Select the folder containing the drivers and click **OK**.
- On Update Drivers dialog, click Next to run the update.
- When you see a confirmation message, click Close and repeat the steps for every driver with a yellow icon. Not necessary for USB Device.

## Updating Windows

Updates to Windows 10 are vital to maintaining a system that is secure and optimized. These updates include security patches and updates. Since the URCVT workstation operates in a closed environment that is not connected to the internet, WSUS Offline Update is an alternate tool that must be used to install the updates on the standalone workstation. The tool was prepared in the section above, *Preparing Offline Updates.*

- At the URCVT workstation, connect the USB drive prepared in the above section.
- Navigate to the USB drive and run **UpdateInstaller.exe.**
- Verify the following boxes are selected:
  - Update C++ Runtime Libraries
  - Install .NET Framework 3.5
  - Install .NET Framework 4.8
  - Update Root Certificates
  - Verify installation packages

- Show log file

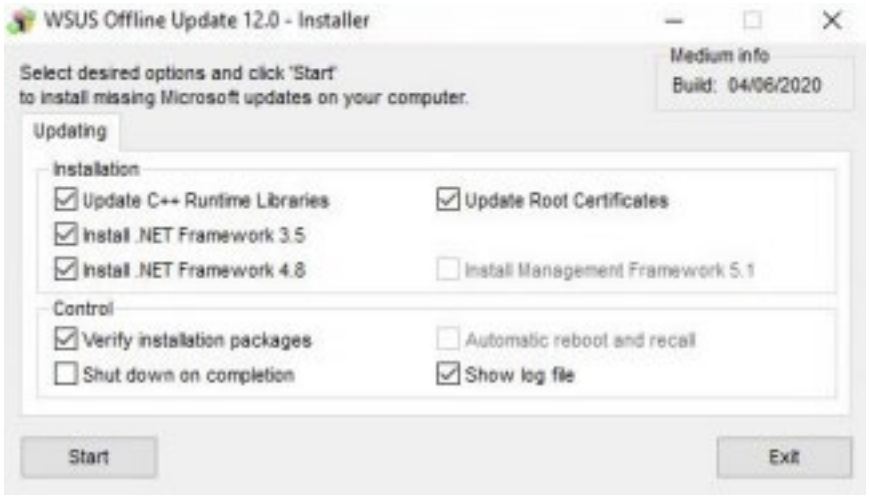


Figure above: WSUS Offline Update Installer Settings

**NOTE:** A warning window appears when Automatic reboot and recall is checked. Click **Yes** to disable User Account Control (UAC) temporarily. WSUS cannot operate unless UAC is disabled.

- Click **Start** to begin installing updates.
- When cmd window prompts you to reboot & recall the system, restart the machine and log back in.
- Navigate to the WSUS installer folder and run: **UpdateInstaller.exe.**
- Click **Start** on the installer to continue offline updates installation.
- Repeat reboot and recall until the cmd window prompts you to only **Reboot the machine.**

Additionally, the following items should be downloaded manually from the second internet connected computer. Download to the USB drive and install on URCVT computer that is operating in a closed environment and that is not connected to the internet.

**Please note that the following Windows Security Updates are meant to be examples ONLY. Jurisdictions should always check for the most up-to-date Windows 10 updates available from Microsoft.**

2020-03 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB4554364):

- Copy and paste the following web link to your browser: https://www.catalog.update.microsoft.com/Search.aspx?q=KB4554364
- Next to: *2020-03 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB4554364),* press **Download**. A *Download* window displays.
- Click on the *.msu* link. The file starts to download.

2020-01 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows Server, version 1909 for x64 (*KB4537572*):

- Copy and paste the following web link to your browser: https://www.catalog.update.microsoft.com/Search.aspx?q=KB4537572
- Next to: *2020-02 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1909 for x64 (KB4537572),* press **Download**. A *Download* window displays.
- Click on the *.msu* link. The file starts to download.

2020-01 Servicing Stack Update for Windows 10 Version 1909 for x64-based Systems (KB4541338):

- Copy and paste the following web link to your browser: https://www.catalog.update.microsoft.com/Search.aspx?q=KB4541338
- Next to: *2020-03 Servicing Stack Update for Windows 10 Version 1909 for x64-based Systems (KB4541338),* press **Download**. A *Download* window displays.
- Click on the *.msu* link. The file starts to download.

Updates for .Net Framework:

- Copy and paste the following web links to your browser, one at a time, and follow the instructions bellow for each link:
  - CVE-2020-0605: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2020-0605
  - CVE-2020-0606: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2020-0606
  - CVE-2020-0646: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/

    CVE-2020-0646
- Next to *.NET Framework 3.5 and 4.8* for *Windows 10 Version 1909 for x64,* press **Security Update**. The *Microsoft Update Catalog* page displays.
- Next to the: *2020-01 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1909 for x64 (KB4532938)* option, press **Download**. A *Download* window displays.
- Click on the *.msu* link. The file starts to download.
- Once all the files have been downloaded, double-click on each of them to run their installation.

**Installing Offline Updates for Windows Defender**

To update Windows Defender:

- Close the Windows Defender.
- Connect the USB drive prepared in the section above.
- On a non-internet connected workstation, double click the *mpam* file to install it. There will be no prompts or installation process.
- To verify the update was applied, open Windows Defender, locate *Virus and Spyware Definitions*. It will say *Up to date* if installation was successful.

**Disabling Automatic Updates**

Windows will use resources attempting to update Windows 10. Windows Update

must be disabled to prevent the system from using those resources.

To disable automatic updates:

- From the Start Menu , enter gpedit.msc. gpedit.msc appears in the search results.
- Launch **gpedit.msc**.
- From the Local Group Policy Editor expand the following nodes: **Computer Configuration** > **Administrative Templates** > **Windows Components**.
- Select **Windows Update**.
- From the Details Pane, double-click **Configure Automatic Updates**. 6. Select **Disabled**, then click **OK**.
- Close the Local Group Policy Editor.
- From the Start Menu , enter CMD. Command Prompt appears in the search results.
- Right-Click **Command Prompt** and then select **Run as Administrator**. If UAC dialog appears, click **Yes**.
- In the Administrator Command Prompt window enter the following two commands each followed by enter.
    - sc config wuauserv start=disabled
    - NET STOP wuauserv /y
- Close Command Prompt.

**Windows Security Procedures**

With the non internet connected computer now fully installed, security measures should be applied. Measures such as device encryption and hardening of the Operating System will help keep the integrity of the system and any data that is processed on the workstation. Step by step instructions for hardening the system are provided below.

***NOTE:*** *Before applying security settings, make sure all system and third-party components are installed and configured. After security settings are applied, some earlier steps may be impossible to perform due to the hardened state of the Operating System. Once applied, security settings cannot be undone.*

**Device Encryption**

Device encryption protects your data on your device. With device encryption, only authorized people can access the device. Device encryption is available on most devices. If not, standard BitLocker encryption may be allowable instead. For information about device encryption on Windows 10 and step by step processes for:

1. Determining if you can use the device encryption or should use BitLocker standard encryption.
2. How to turn on device encryption or BitLocker standard encryption.
3. How to obtain a recovery key.

Go to the Microsoft Windows 10 Device Encryption page at: https://support.microsoft.com/en-us/windows/device-encryption-in-windows-10-ad5dcf4b-dbe0-2331-228f-7925c2a3012d

**Physical Security and Hardening**

Users must physically seal all external ports on hardware URCVT is installed on, except ports used for power supply, necessary external displays, and one (1) USB port. The user jurisdiction should employ a policy where the use of tamper evident and tamper resistant seals are used to identify ports that should never be accessed, unlikely to be accessed, and can be accessed if

necessary.

**Operating System Hardening**
Operating system hardening can reduce the risk of a security breach by removing or disabling many non-essential software and hardware components that could act as a back door for attackers. Vendor highly recommends the following hardening procedures to protect your standalone computer.

**Disable Network Connection From Network Connection Settings:**
1) Press Win+R and enter *ncpa.cpl* to open the Network Connection window.
2) For each network connection right click on it:
4) Select disable.

**Set ScreenSaver Password:**
1) Open the Control Panel.
2) Click Appearance and Personalization.
3) Click Change screen saver.
4) In the Screen Saver Settings check the box *On resume, display logon screen*.

**Disable Automatic Login:**
1) Press Win+R, enter *netplwiz* to open the *User Accounts* window.
2) Check the option for *Users must enter a username and password to use this computer* and click Apply.

**Disable Remote Access:**
1) Type *remote settings* into the search box.
2) Select *Allow remote access to your computer* to open the Control Panel for Remote System Properties.
3) Check *Don't Allow Remote Connections* to this Computer.

**Enable Firewall:**
1) Open the Control Panel in Windows.
2) Click on System and Security.
3) Click on Windows Firewall.
4) In the left navigation pane click *Turn Windows Firewall On*.

**Disable all network interfaces:**
1) Enter cmd in the windows search bar.
2) *Command Prompt* application shows up in search results.
3) Right-click on the *Command Prompt*.
4) Select *Run as administrator*.
5) Type "netsh interface show interface" and press Enter.
6) For each network device listed enter the following command, replacing "Interface Name" with each of the names returned from step 5 (include the double-quotes):
*netsh interface set interface "Interface Name" disable*

## Document Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 04/25/2021 | 1.0.0 | System Hardening Procedures | Rosemary F. Blizzard |