Building a CrowdStrike Recovery ISO (Manual)

Published Date: Jul 22, 2024

Objective

- This guide shows you how to build your own bootable image files to automate the recovery of Windows hosts affected by the recent Falcon Content Update.

Procedure

There are two bootable image types available. Use the ISO image that best suits your needs.

1. **CSPERecovery** - This image uses Windows PE to remove the impacted Channel File 291 with minimal user interaction.
    a. If the volume has BitLocker Encryption, the bootable image will prompt for the BitLocker Recovery Key before performing the automated remediation.
2. **CSSafeBoot** - This image uses Windows PE to reboot the host into *Safe Mode with Networking* to allow manual removal of Channel File 291 using Windows Explorer or Command Prompt
    a. If the volume has BitLocker Encryption, **the Recovery Key is not required**
    b. Useful for systems having difficulty entering Safe Mode

Creating Bootable Image

Requirements

- A Windows 10 (or higher) 64-bit client with at least 8GB of free space, and administrative privileges .
- OPTIONAL: FAT32 formatted USB drive (1GB).

Procedure

IMPORTANT:

- Use all of the steps below to create bootable images for both CSPERecovery and CSSafeBoot
- You must accept all UAC prompts throughout these steps.

Step 1: Download and Install the Windows ADK

1. **Download Windows ADK:**
    - Visit the Microsoft ADK download page.

- Download the Windows Assessment and Deployment Kit (ADK) for Windows 10 or Windows 11, depending on your requirements.

2. **Install Windows ADK:**
   - Run the ADK installer adksetup.exe.
   - On the “Select the features you want to install” screen: only “Deployment Tools” should be selected.
     i. Drastically reduces the ADK download size

Step 2: Install Windows PE Add-ons

1. **Download Windows PE Add-on:**
   - On the same Microsoft ADK download page, download the Windows PE add-on for Windows ADK.
2. **Install Windows PE Add-ons:**
   - Run the installer for the Windows PE add-ons adkwinpesetup.exe.
   - Use all default settings and Install Windows PE environment.

Step 3: Create a Windows PE Working Directory

1. **Create the Working Directory:**
   a. On Windows 11, from the Start Menu, select “All Apps”, scroll down to Windows Kits, right-click on Deployment and Imaging Tools Environment, Run as an Administrator.
   b. On Windows 10, from the Start Menu, scroll down to Windows Kits, right-click on Deployment and Imaging Tools Environment, Run as an Administrator.
   c. In command prompt, copy and paste the following command to create a directory for the Windows PE image:
      i. `copype.cmd amd64 C:\CS_ISO`
   d. Copy and paste the following command to create a directory for Drivers:
      i. `mkdir C:\CS_ISO\drivers`
   e. Copy and paste the following command to create a directory for remediation scripts:
      i. `mkdir C:\CS_ISO\scripts`

Step 4: Add Drivers and CrowdStrike scripts to the Windows PE image

1. **Download drivers to support wide-device compatibility:**
   The Windows PE image contains a default set of device drivers, however, you may need additional drivers for your own environment. The following are examples of commonly used drivers to support chipset and storage device compatibility for common physical and virtual hardware platforms.
   - **OPTIONAL: Dell Windows PE Driver Packs (includes Intel, ILS, Acquanta, and Realtek drivers) (includes**
     a. Download the WinPE 10 driver pack | Dell US
     b. Download the WinPE 11 driver pack | Dell US

c. Use the `expand` utility to unpack each driver pack
    i. `expand "C:\Users\<your_user>\Downloads\WinPE10.0-Drivers-A33-CCKD7.cab" -F:"*" "C:\CS_ISO\drivers"`
    ii. `expand "C:\Users\<your_user>\Downloads\WinPE11.0-Drivers-A03-V81GV.cab" -F:"*" "C:\CS_ISO\drivers"`
d. Use the `xcopy` utility to stage the drivers for use with ADK
    i. `xcopy /s /e /h /y "C:\CS_ISO\drivers\winpe\x64" "C:\CS_ISO\drivers"`
e. Use rd utility to remove the temporary Dell driver pack directory
    i. `rd /s /q "C:\CS_ISO\drivers\winpe"`

- **OPTIONAL: HP Windows PE Driver Pack (includes**
    a. Download the SoftPaq Exe for "WinPE 10/11" driver pack HP Client Windows PE Driver Packs | HP Client Management Solutions
    b. Launch the driver pack
        i. On Location to Save Files screen, *set the Save files in folder to* "`C:\CS_ISO\drivers`" without quotes.
    c. Use the `xcopy` utility to stage the drivers for use with ADK
        i. `xcopy /s /e /h /y "C:\CS_ISO\drivers\WinPE10_2.70\x64_winpe10" "C:\CS_ISO\drivers"`
    d. Use rd utility to remove the HP driver pack directory
        i. `rd /s /q "C:\CS_ISO\drivers\WinPE10_2.70"`
- **OPTIONAL: KVM / VirtIO Drivers**
    a. Download the latest VirtIO drivers ISO https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/latest-virtio/virtio-win.iso
    b. From Edge browser, expand Downloads icon and click Open file link to open the ISO
        i. Or, from Windows Explorer, locate your Downloads folder and double-click to Open the virtio-win.iso file
    c. IMPORTANT: Note drive mount location of iso after opening
    d. Use `mkdir` to create a directory to store the VirtIO drivers and copy them: `mkdir C:\CS_ISO\drivers\virtio`
    e. Use xcopy to stage the VirtIO drivers
    IMPORTANT: Replace "E" drive letter in this command with your iso drive letter)
        i. `xcopy /s /e /h /y "E:\viostor\w11\amd64" "C:\CS_ISO\drivers\virtio"`
        ii. `xcopy /s /e /h /y "E:\vioscsi\w11\amd64" "C:\CS_ISO\drivers\virtio"`
        iii. `xcopy /s /e /h /y "E:\vioinput\w11\amd64"`

```
"C:\CS_ISO\drivers\virtio"
```

f. In Windows Explore, right-click on the mounted iso drive and select Eject

2. **Download and stage the CrowdStrike recovery scripts:**
   IMPORTANT: these scripts can be used to create BOTH bootable image types.
   - Download CrowdStrike recovery scripts from https://github.com/CrowdStrike/falcon-windows-host-recovery/tree/main/Scripts
     a. Click on each file to view
     b. Click the "Raw" download button and save each file to `C:\CS_ISO\scripts`
   - Verify `C:\CS_ISO\scripts`, contains
     a. `CSPERecovery.ps1`
     b. `CSPERecovery_startnet.cmd`
     c. `SafeBoot_startnet.cmd`
3. **Mount the Windows PE Image:**
   - Use `dism.exe` to mount the WinPE boot image:
   - `dism.exe /Mount-Image /ImageFile:C:\CS_ISO\media\sources\boot.wim /index:1 /MountDir:C:\CS_ISO\mount`
4. **Add Drivers to the Windows PE image:**
   - Use `dism.exe` to add drivers to the mounted WinPE boot image
     `dism.exe /Image:C:\CS_ISO\mount /Add-Driver /Driver:C:\CS_ISO\drivers\ /Recurse`
5. **Add the CSPERecovery scripts to the Windows PE image:**
   - Use `copy` to copy the script files to the mounted WinPE image:
   - IMPORTANT: this command will overwrite the existing startnet.cmd file
     a. `copy /Y "C:\CS_ISO\scripts\CSPERecovery.ps1" "C:\CS_ISO\mount\Windows\System32\CSPERecovery.ps1"`
     b. `copy /Y "C:\CS_ISO\scripts\CSPERecovery_startnet.cmd" "C:\CS_ISO\mount\Windows\System32\startnet.cmd"`
6. **Add the required WinPE component packages to the Windows PE image**
   - Use `dism.exe` to add the following WinPE component packages to the mounted WinPE boot image
     a. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-WMI.cab"`
     b. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\en-us\WinPE-WMI_en-us.cab"`

c. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-StorageWMI.cab"`
d. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\en-us\WinPE-StorageWMI_en-us.cab"`
e. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-Scripting.cab"`
f. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\en-us\WinPE-Scripting_en-us.cab"`
g. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-NetFx.cab"`
h. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\en-us\WinPE-NetFx_en-us.cab"`
i. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-PowerShell.cab"`
j. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\en-us\WinPE-PowerShell_en-us.cab"`

k. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-DismCmdlets.cab"`
l. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\en-us\WinPE-DismCmdlets_en-us.cab"`
m. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-FMAPI.cab"`
n. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-SecureBootCmdlets.cab"`
o. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-EnhancedStorage.cab"`
p. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\en-us\WinPE-EnhancedStorage_en-us.cab"`
q. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\WinPE-SecureStartup.cab"`
r. `dism.exe /Image:C:\CS_ISO\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation`

```
Environment\amd64\WinPE_OCs\en-us\WinPE-SecureStartup
_en-us.cab"
```

7. **Unmount and Commit Changes to the Windows PE image:**
    - Use `dism.exe` to unmount the image and commit changes
      `dism.exe /Unmount-Image /MountDir:C:\CS_ISO\mount /Commit`

Step 5: Create the CSPERecovery Bootable ISO Image File

1. **Create the ISO file using MakeWinPEMedia.cmd:**
    - Use `MakeWinPEMedia.cmd` to create the ISO file:
      `MakeWinPEMedia.cmd /ISO C:\CS_ISO C:\CS_ISO\CSPERecovery.iso`

Step 6: OPTIONAL - Create a CSPERecovery Bootable USB Drive (Optional)

WARNING: All existing data on your USB drive will be wiped upon creation of a bootable USB drive. Be sure to use a unique USB drive for each bootable image you create.

1. **Prepare a USB Drive:**
    - Insert a USB drive and note its drive letter (e.g., E:).
2. **Create the Bootable USB Drive:**
    - Run the following command and adjust the drive letter accordingly:
      `MakeWinPEMedia.cmd /UFD C:\CS_ISO E:`

Step 7: Create the CSSafeBoot Bootable ISO image

1. **Mount the Windows PE Image:**
    - Use `dism.exe` to mount the WinPE boot image:
      `dism.exe /Mount-Image /ImageFile:C:\CS_ISO\media\sources\boot.wim /index:1 /MountDir:C:\CS_ISO\mount`
2. **Remove the CSPERecovery script from the Windows PE image:**
    - Use del to delete the script file from the mounted WinPE image:
      `del /F /Q "C:\CS_ISO\mount\Windows\System32\CSPERecovery.ps1"`
3. **Add the CSSafeBoot script to the Windows PE image:**
    - Use `copy` to copy the script file to the mounted WinPE image:
    - IMPORTANT: this command will overwrite the existing startnet.cmd file
      `copy /Y "C:\CS_ISO\scripts\SafeBoot_startnet.cmd" "C:\CS_ISO\mount\Windows\System32\startnet.cmd"`
4. **Unmount and Commit Changes to the Windows PE image:**
    - Use `dism.exe` to unmount the image and commit changes
    - `dism.exe /Unmount-Image /MountDir:C:\CS_ISO\mount /Commit`
5. **Create the ISO file using MakeWinPEMedia.cmd:**
    - Use `MakeWinPEMedia.cmd` to create the ISO file:
      `MakeWinPEMedia.cmd /ISO C:\CS_ISO C:\CS_ISO\CSSafeBoot.iso`

Step 8: OPTIONAL - Create a the secondary Bootable USB Drive (Optional)
IMPORTANT: requires completion of Step 7 for success
WARNING: All existing data on your USB drive will be wiped upon creation of a bootable USB drive. Be sure to use a unique USB drive for each bootable image you create.

1. **Prepare a USB Drive:**
    - Insert a USB drive and note its drive letter (e.g., E:).
2. **Create the Bootable USB Drive:**
    - Run the following command and adjust the drive letter accordingly:
      `MakeWinPEMedia.cmd /UFD C:\CS_ISO E:`