

## איתור תקלות בזמן האתחול וביצוע שחזור מערכת

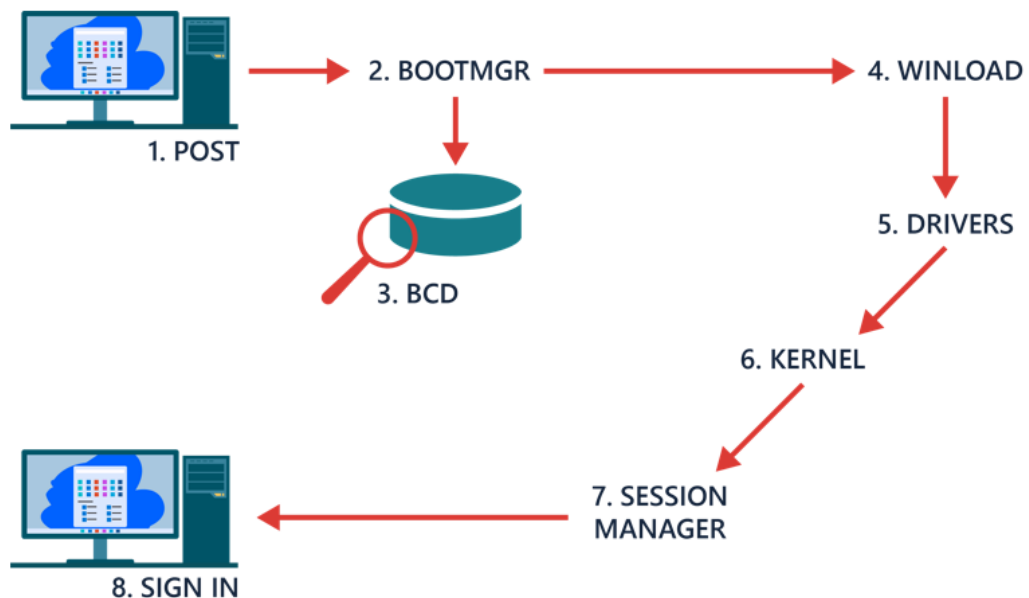
טיפול בתקלות הקורות בתהליך האתחול דורש ידע וכלים שונים מטיפול בתקלות רגילות של מע' ההפעלה וזו מהסיבה שבחלק גדול מהמקרים לא תהיה לנו גישה לממשק הגרפי של מע' ההפעלה.

פתרון בעיות בשלב עליית המע' מחייב ידע בשלבי התהליך והיכרות עם התקלות האופייניות לכל שלב ושלב.

פרק זה יתמקד ב:

- הבנה של תהליך האתחול עצמו ומה מתרחש בכל שלב
- ההגדרות השונות והדרך לשנות אותן
- איתור תקלות והטיפול בהן

### Windows 11 startup architecture



## שליבי האתחול מהדלקת המחשב ועד לרגע שמופיע שולחן העבודה :

1. הביוס מבצע בדיקה עצמית POST , וניגש לטעון את ה-MBR
2. MBR טוען את ה- (Bootmgr.exe) Windows Boot Manager , קובץ זה החליף את מרבית הפונקציות שבעבר ביצע NTLDR ששימש במע' ההפעלה XP , הקובץ הזה עומד בפני עצמו והוא מעביר את המעבד למצב מוגן ולעבודה ב-32 ביט או 64 ביט בהתאם למע' ההפעלה. הוא מציג לנו את התפריט שמאפשר לנו בחירה במידה ויש מס' מערכות הפעלה וכמו כן במידה ומותקנת מע' הפעלה XP במחשב הוא יעלה את NTLDR
3. Windows Boot Manager טוען את ה-BCD – ה-BCD מספק מנגנון שאינו תלוי בחומרה המאפשר העלאת מע' הפעלה מבוססות ווינדוס ויסטה ומעלה . הוא בעל יכולות להריץ אפליקציות בשלב ה-BOOT כמו דיאגנוסטיקה של הזיכרון ועוד. המבנה שלו דומה לריגסטרי אך את העריכה שלו נבצע באמצעות כלים יעודיים.
4. BCD טוען את Winload.exe - קובץ זה תפקידו לטעון את הליבה של מע' ההפעלה ואת הדרייברים של המערכת , הוא מכין את הזיכרון להפעלה ומעביר את השליטה לליבה של המערכת . אם היה ב-BCD רישום על כך שהמערכת הופעלה לאחר שהייתה במצב Hibernation - יופעל תהליך בשם Winresume.exe והמערכת תשתמש בקובץ ה-Hibernation ע"מ לשחזר את המערכת לנקודה בה היא הופסקה
5. Winload.exe מתחיל לטעון את הליבה Ntoskrnl.exe
6. דרייברים ושירותי מערכת מתקדמים נטענים - המסך עובר למצב גרפי ומע' המשנה של ווינדוס נטענת (smss.exe)
7. המשתמש יכול לבצע Log in ולהתחיל להשתמש במערכת

מידע נוסף תמצאו בקישור הבא : <https://docs.microsoft.com/en-us/windows/client-management/advanced-troubleshooting-boot-problems>

### Boot Configuration Data (BCD)

מערכת ההפעלה Windows 11 שונה בניהול תהליך האתחול שלה, בעבר היה נהוג לנהל את תהליך האתחול של המחיצות מתוך קובץ שנקרא Boot.ini, אך כיום תהליך הניהול השתנה לחלוטין.

בשביל לשנות את תהליך האתחול צריך להיות איש מקצוע בעל ידע ולא כל אחד יכול להוסיף איזה רשומה שהוא רוצה לתהליך האתחול, הדרך לנהל את תהליך האתחול ב-Windows 11 היא בעזרת פקודה שנקראת Bcdedit שרמת השליטה שלה על תהליך האתחול היא גבוהה מהקודמות לה ונותנת לנו שליטה מלאה על קביעת כל פרמטר קטן.

הקובץ שמנהל את האתחול הוא קובץ שמכיל בתוכו אינפורמציה על תהליך האתחול של המחשב.

- הקובץ שמנהל את האתחול ב-Windows 11 הוא Bootmgr

- הקובץ שמנהל את האתחול ב-Windows XP הוא ntldr

Bcdedit יכול לתמוך bootloaders אחרים מדי, לדוגמה Linux ו-Windows.

הקובץ שמוסיף Bcdedit ב-Windows 11 נקרא bcd והוא נמצא ב- boot\bcd , מערכת ההפעלה בהתקנה שמה את הקובץ במחיצה נסתרת מעין המשתמש כדי שאם יקרה משהו לכונן C שמכיל את ה-Windows לא יקרה כלום לקבצי האיתחול.

קובץ BCD זה מחליף את הקובץ boot.ini ששימש אותנו בגירסאות קודמות של מע' הפעלה XP וישנות יותר. הוא מאפשר למע' ההפעלה לאתר את מיקום קבצי ההפעלה ועלייה וזיהוי של מגוון מע' הפעלה . כמו גם תכונות חדשות (כמו סביבת התיקון לדוגמה) . ה-BCD מאוחסן בפורמט זהה לרגיסטרי והוא ממוקם בדיסק הקשיח בתיקיית הסיסטם . במע' עם EFI - [Extensible Firmware Interface](#) נמצא אותו ב- EFI\MICROSOFT\BOOT . במע' מבוססות BIOS רגיל נמצא אותו ב- BOOT\BCD .

הקובץ מכיל את האינפורמציה הבאה :

- רשומות המתארות את מנהל ה Bootmgr (Windows Boot Manager)
- רשומות המתארות את Winload.exe (Windows Boot Loader) – בלעדי קובץ זה לא תוכל להתבצע עלייה של מע' הפעלה
- רשומות האחראיות על חזרה ממצב קפיאה – (Windows\System32\WinResume.exe)
- רשומות המאפשרות בדיקה של הזיכרון (Boot\MemTest.exe)
- רשומות היודעות לטעון את NTLDR ע"מ להעלות מע' הפעלה ישנות יותר
- רשומות היודעות להעלות מע' הפעלה לא מבוססות NT

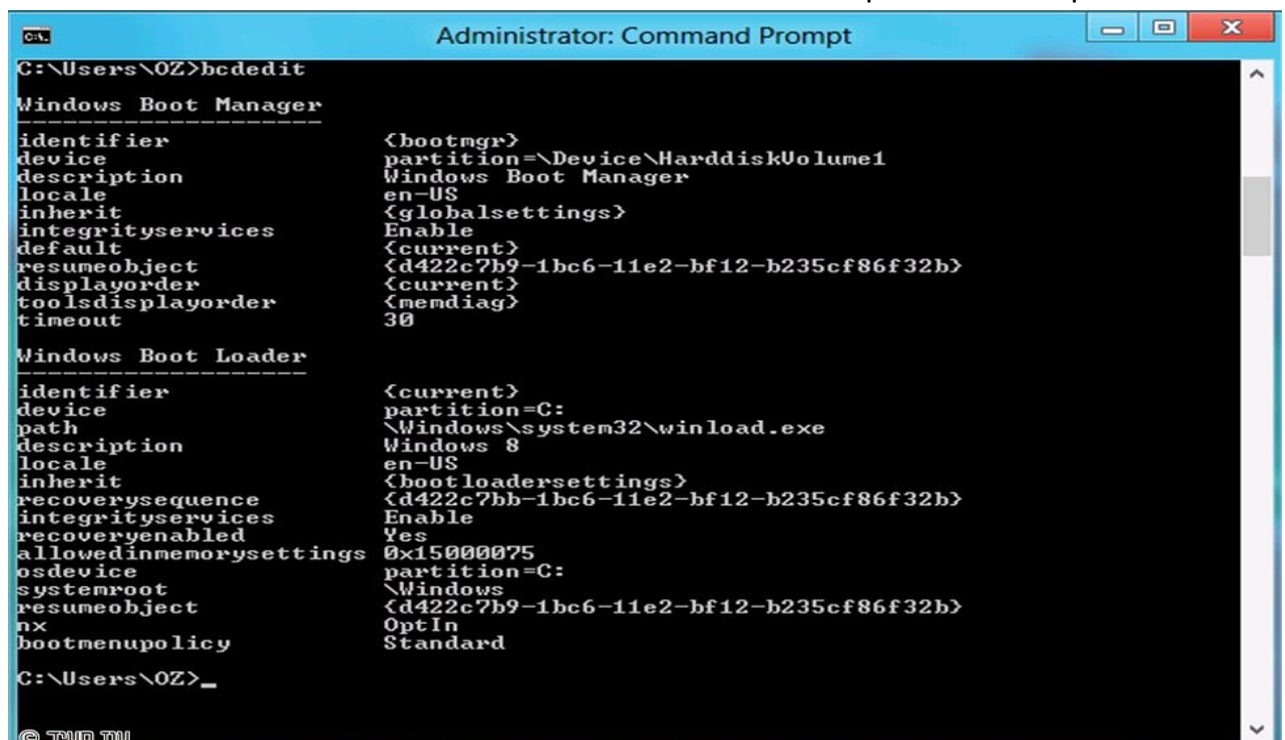
חובה לעבוד עם חשבון בעל הרשאות מנהל כדי לעבוד עם הפקודה Bcdedit.

## כלים לשינוי הגדרות אתחול :

שימוש בפקודת Bcdedit.exe

1. פתחו CMD .
2. והקישו bcdedit.

הערה: על ידי הקלדת bcdedit נקבל את הערכי האתחול



```
C:\Users\OZ>bcdedit

Windows Boot Manager
-----
identifier               <bootmgr>
device                   partition=\Device\HarddiskVolume1
description               Windows Boot Manager
locale                   en-US
inherit                   <globalsettings>
integrityservices        Enable
default                  <current>
resumeobject              <d422c7b9-1bc6-11e2-bf12-b235cf86f32b>
displayorder             <current>
toolsdisplayorder        <memdiag>
timeout                  30

Windows Boot Loader
-----
identifier               <current>
device                   partition=C:
path                     \Windows\system32\winload.exe
description               Windows 8
locale                   en-US
inherit                   <bootloadersettings>
recoverysequence         <d422c7bb-1bc6-11e2-bf12-b235cf86f32b>
integrityservices        Enable
recoveryenabled          Yes
allowedinmemorysettings  0x15000075
osdevice                 partition=C:
systemroot                \Windows
resumeobject              <d422c7b9-1bc6-11e2-bf12-b235cf86f32b>
nx                       OptIn
bootmenupolicy            Standard

C:\Users\OZ>_
```

## תהליך האתחול כולל 4 מרכיבים עיקריים:

1. **Identifier** - מזהה את השם שהמערכת נתנה לתהליך האתחול.
2. **Device** - המחיצה ממנה המערכת תחפש את קבצי האתחול
3. **Path** - הנתיב שבו נמצא מנהל האתחול.
4. **Description** - השם שאנחנו נותנים למערכת ההפעלה לשם זיהוי המערכת כאשר נגיע לתפריט שבו אנו קובעים מאיזה מערכת הפעלה יאתחל המחשב.

יש לבצע גיבוי של הקובץ BCD לפני שמבצעים שינויים כלשהם בקובץ. כדי לעשות זאת, הקלד:

```
bcdedit /export C:\savedbcd
```

פעולה זו תיצור קובץ תיכונת את קובץ הגיבוי:

```
_bcdedit /import c:\savedbcd
```

פעולה זו תייבא את הקובץ שגיבוינו

## דוגמאות כיצד לשלוט על יצירת תהליך האתחול

```
bcdedit /set {current} description "My edited Windows Boot Entry"
```

פעולה זו משנה את הכותרת של רשומת האתחול בתפריט "(השם הנוכחי)".

### הערה:

ניתן להשתמש Bcdedit לשנות כל פרמטר בתהליך האתחול, בשונה מ-bcdedit משמש ניתן לשנות ערכים מסוימים

### הערה:


ניתן להגדיר למחשב כמה זמן להמתין לפני שהוא נכנס למערכת ההפעלה שהוגדרה כראשונה בתהליך האתחול, נשתמש בפקודה:

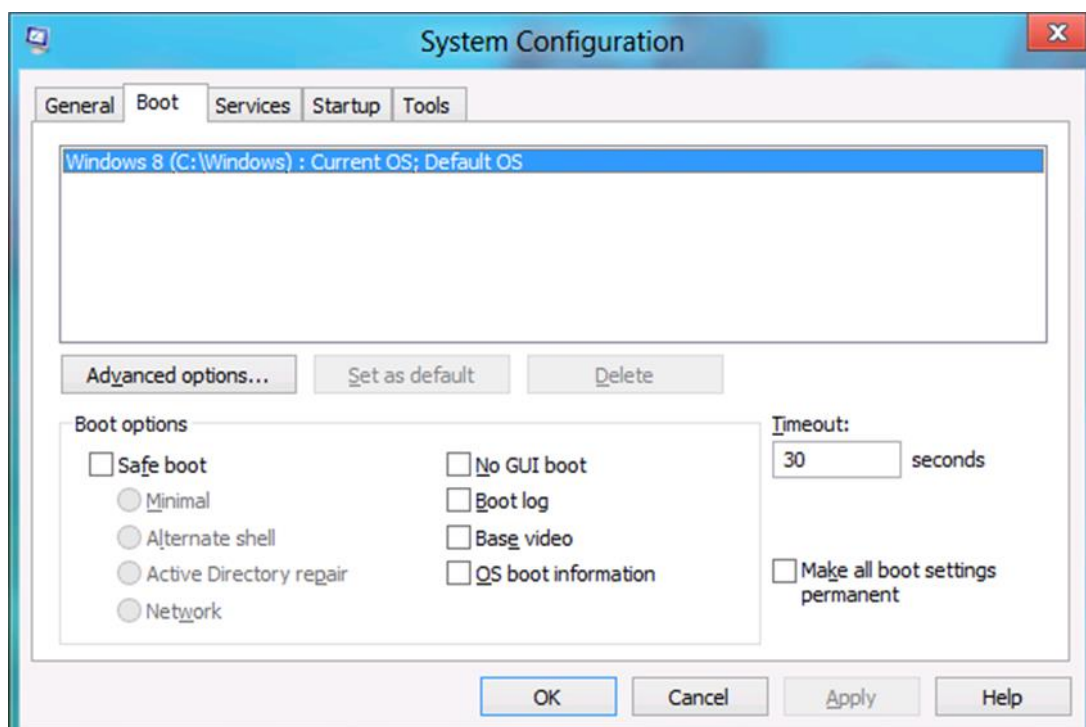
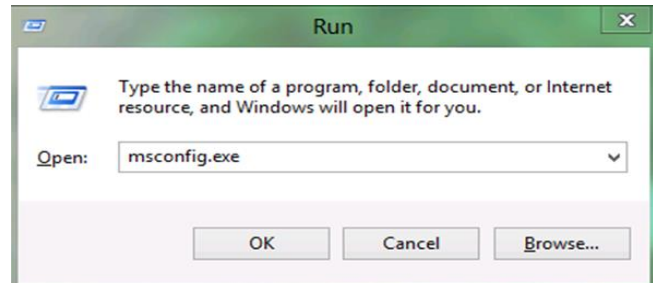
```
bcdedit /timeout 5
```

נוכל באמצעות BCDEDIT ליצור שתי רשומות אתחול אחת עם HYPERV פעיל והשניה ללא וכך למעשה להתקין גם את VMWARE וגם את HYPERV על אותה מע' ההפעלה.

## שינוי הגדרות דרך Msconfig.exe

MSCONFIG - הוא כלי שמאפשר לשלוט על מספר הגדרות של האתחול.

הפעלה ע"י  + R וכתובת msconfig.exe בתיבת ההפעלה

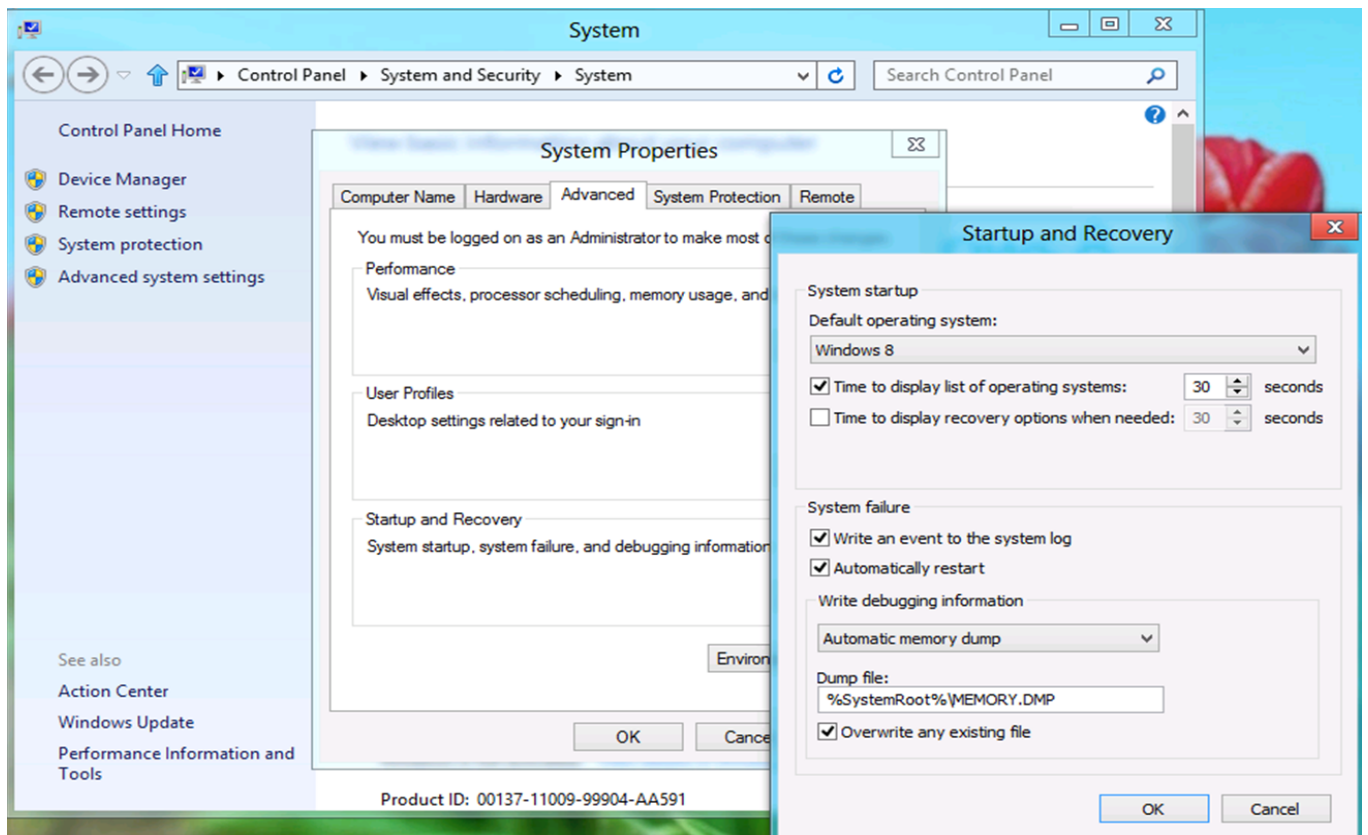


נבחר בלשונית BOOT , נוכל לשים לב למס' אפשרויות שמאפשרות לנו שליטה על הדרך בה תעלה מערכת ההפעלה וכמו כן אם היו מס' מע' הפעלה יכלנו לבחור איזו מערכת הפעלה תעלה כברירת מחדל.

ניתן לבחור במשך כמה זמן יוצג התפריט שמאפשר להעלות מס' מערכות הפעלה ואיזו מע' הפעלה תעלה כברירת מחדל.

ניתן לקבוע שמערכת ההפעלה תעלה במצב בטוח, ישנה אפשרות לבחור שהשינויים יקרו רק להפעלה הבאה או שיישארו קבועים

## דרך לחיצה ימנית על Computer כניסה למאפיינים (Properties) ובחירה ב-Advanced system settings

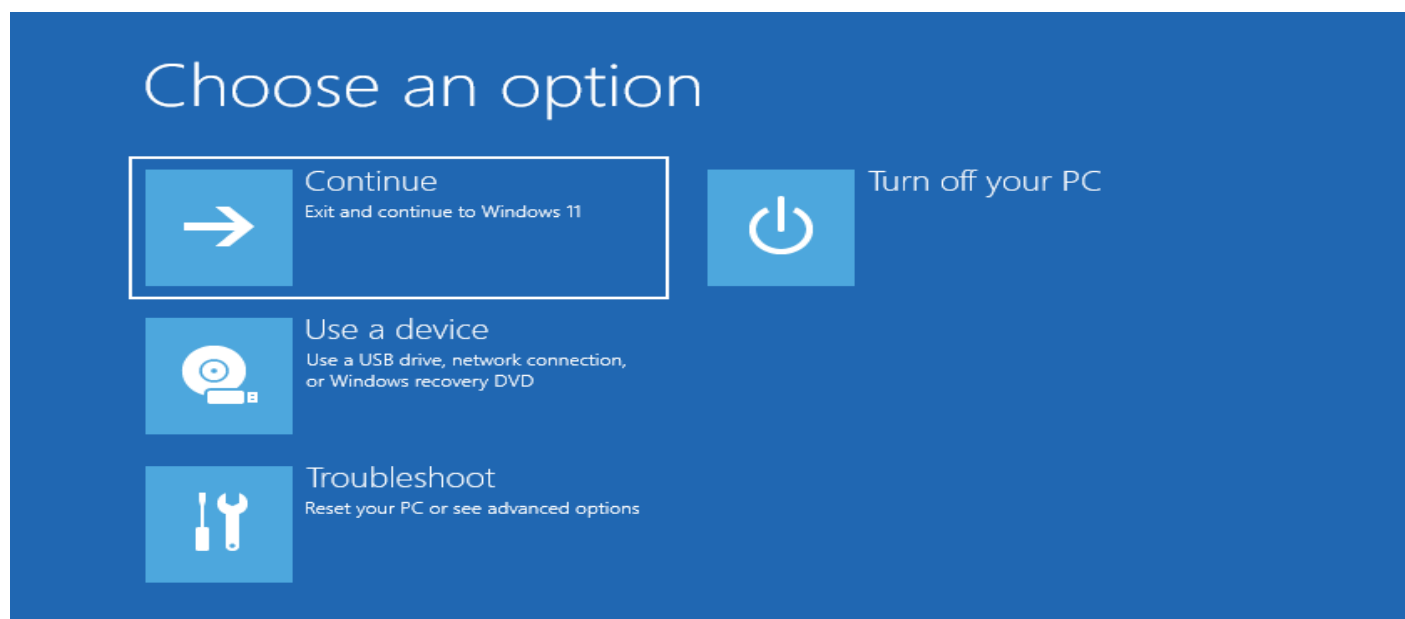


נבחר בלשונית Advanced ובאופציה Startup and Recovery ונוכל לשנות מס' הגדרות. ההגדרות החשובות לנו הן האפשרות לצור קבצי LOG (קבצים המבצעים רישום של הפעולות שקורות בזמן האתחול) וכך במקרה של תקלה נוכל לעבור על קבצים אילו ולקבל מידע שימושי שיוכל לעזור לנו לאבחן את הבעיה.

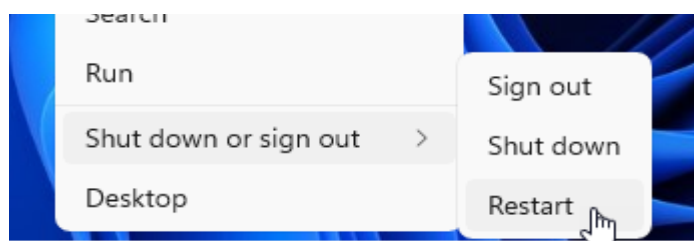
כמו כן יש לנו את האפשרות לשנות את המע' ההפעלה שתעלה כברירת מחדל ואת זמן הצגת התפריט.

## סביבת התיקון של ווינדוס:

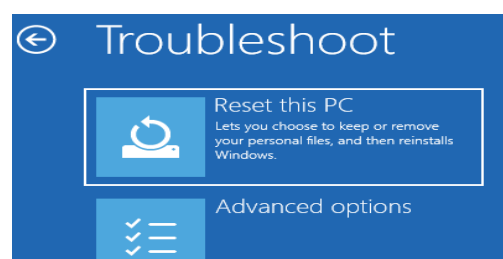
ווינדוס מכילה סביבת תיקון מתקדמת בעלת כלים רבים המאפשרים לבצע תיקון לבעיות בזמן האתחול. תקלות אילו יכולות להיגרם מכיבוי לא תקין של מע' ההפעלה עקב הפסקת חשמל או שהשתמש כיבה את המחשב מכפתור הכיבוי ולא המתין לכיבוי מסודר. תקלות אתחול יכולות להיגרם עקב עדכון מע' שכשל או התקנה של דרייבר חדש או התקנת חומרה חדשה. עדכון ביוס גם יכול לצור כשל בתהליך האתחול. את כל התקלות הללו ועוד נוכל לתקן דרך סביבת התיקון של ווינדוס



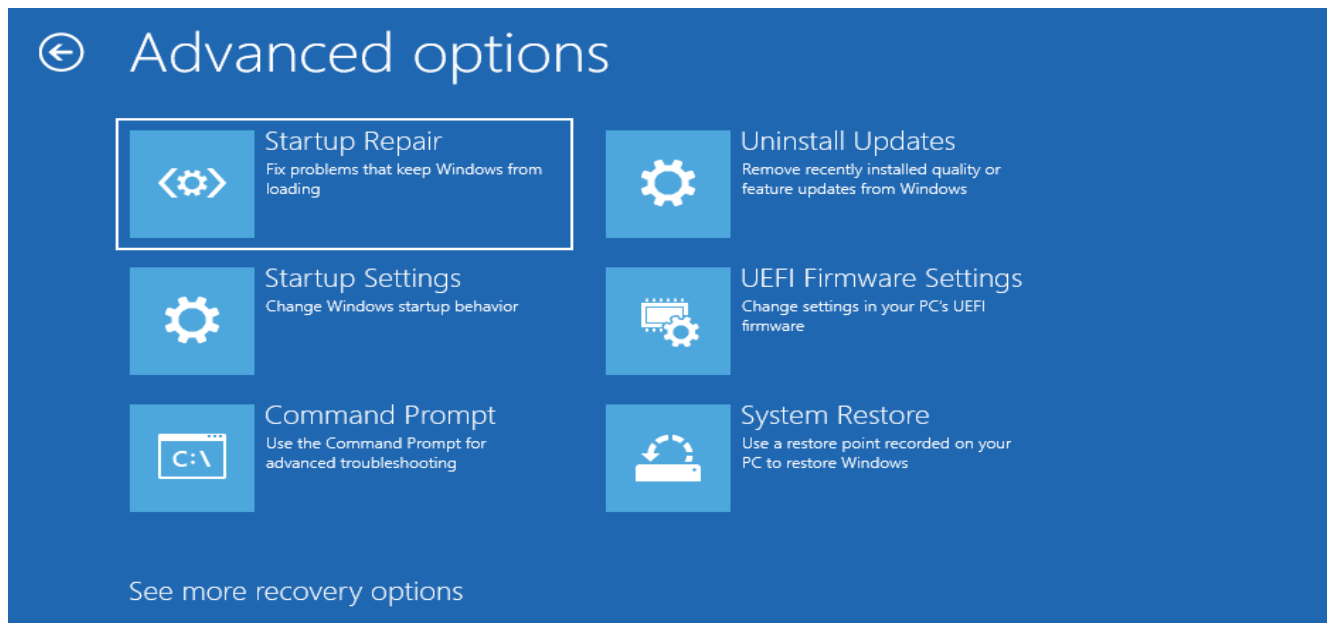
לאחר שלושה נסיונות לא מוצלחים לבצע אתחול המע' תיכנס אוט' לסביבת התיקון ניתן להיכנס לסביבה הזו באמצעות ההגדרות או בזמן ביצוע הפעלה מחדש להשאיר את מקש ה SHIFT לחוץ.



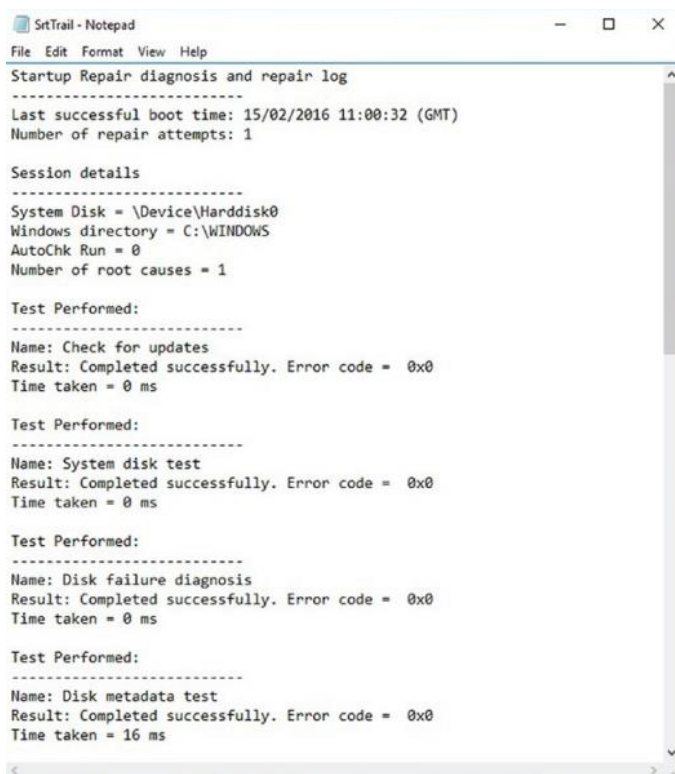
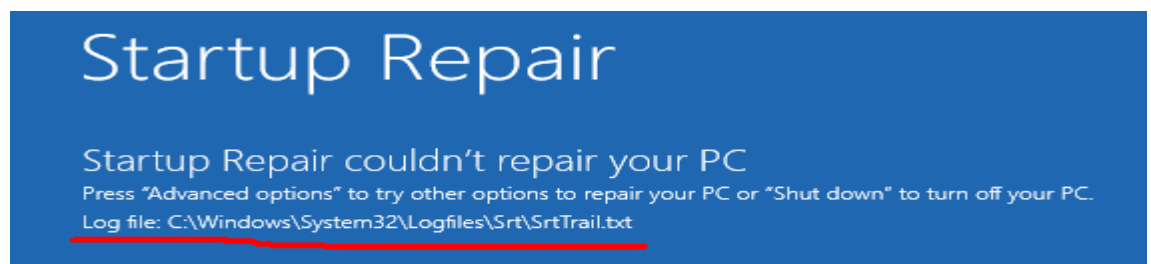
במצב זה נוכל להיכנס גם לאפשרות של איפוס המחשב Reset This PC – אפשרות זו נועדה לבצע מחיקה של המחשב וההגדרות על מנת למסור אותו הלאה או לבצע מחיקה של כל התוכנות אך לשמור את הקבצים שלנו על מנת להתחיל ממצב נקי.



בהגדרות המתקדמות נוכל לראות מגוון כלים לטיפול בבעיות אתחול :



Startup Repair - הכלי יריץ לנו סקריפטים מוכנים לטיפול בבעיות אתחול , נוכל לנסות להריץ אותו בצורה מיידית על מנת לטפל בבעיות



שימו לב שיש לנו קובץ LOG שמפרט לנו את הפעולות שנעשו לאיתור וטיפול בבעיה התמונה יש דגש על המיקום בו הוא נוצר, דוגמה לקובץ כזה :

**Uninstall Updates** – יאפשר לנו להסיר עדכונים שגורמים לבעיה באתחול המחשב

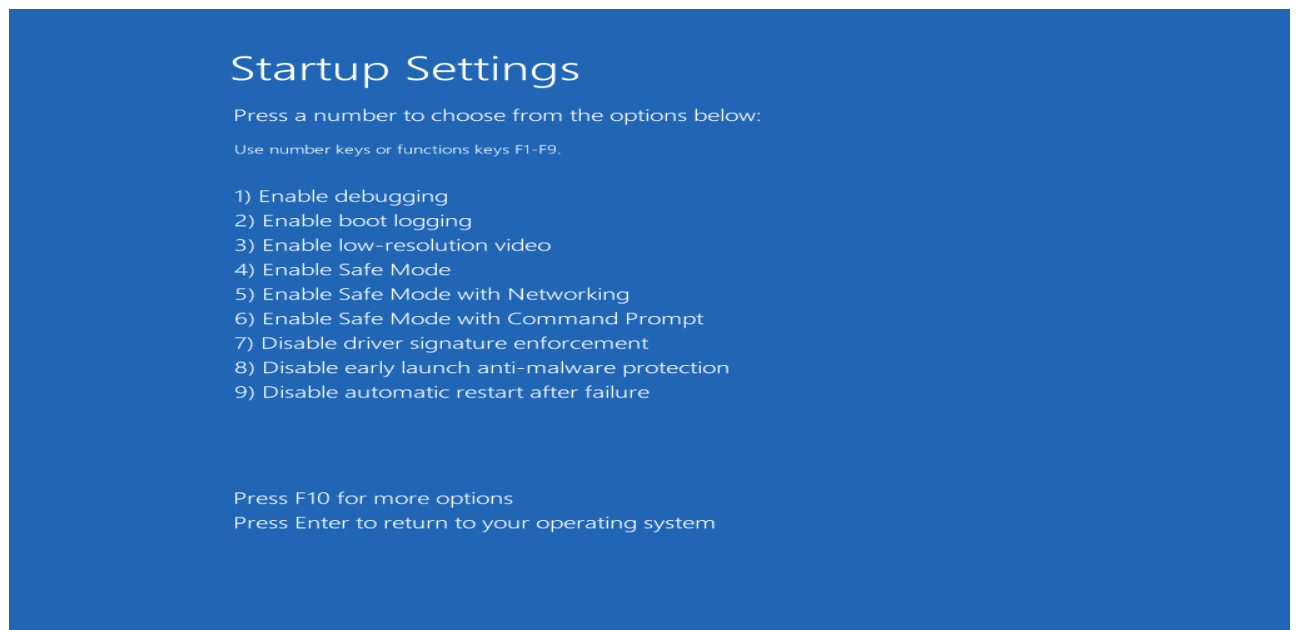
**System Restore** - יאפשר לנו לבצע שחזור מע' לנקודת זמן קודמת

**System Image Recovery** - יאפשר לנו לשחזר את המע' באמצעות קובץ גיבוי מלא שיצרנו מראש



**Startup Settings** - יפתח לנו את התפריט עם הגדרות האתחול המתקדמות (תפריט דומה לתפריט שהיה במע' הפעלה קודמות)

מנך Startup Settings



**Enable Debugging** - יריץ את המערכת במצב איתור תקלות מתקדם נועד לאתר תקלות בהתנהגות של דרייברים מול מע' ההפעלה

**Enable Boot logging** – ייצור קובץ בשם ntbtlog.txt קובץ זה יכיל רישום של כל הדרייברים שעלו בזמן ההתקנה

**Enable low-resolution video** – אפשרות זו תעלה את המערכת עם הגדרות גרפיקה הבסיסיות ביותר (מראה תמונה של 640x480x256), מצב זה נועד לטפל במקרים שכרטיס המסך לא תקין או לא הותקן כראוי.

**Safe Mode** - Windows עולה עם מינימום דרייברים ולא מפעיל תוכניות שעולות בזמן האתחול. זהו מצב שנועד לפתור תקלות במחשב, במיוחד כאשר חומרה כלשהי גרמה ל"תקיעת" המחשב.

**Safe Mode with Networking** - Windows עולה ב safe Mode, אך כל מה שקשור לרשת עובד. זוהי פונקציה שמאפשרת למנהל הרשת לבדוק מחשב מרחוק למרות שעלה ב safe Mode.

**Safe mode with command prompt** - כניסה לממשק הלא גרפי ואפשרות להריץ פקודות דוס בסיסיות לתיקון.

**Disable Driver Signature Enforcement** – מאפשר למע' ההפעלה להעלות גם דרייברים שאינם חתומים דיגיטלית ע"י מייקרוסופט

**Disable automatic restart on system failure** - אפשרות זו תמנע ממע' ההפעלה לבצע אתחול מחדש בכל פעם שיש תקלה

**Command Prompt** - מאפשר לנו גישה לממשק CMD, ולפקודות שימושיות כמו BCDEDIT, או פקודות CMD הידועות לנטרל דרייברים או שירותי מערכת שפוגעים בהעלאת הווירוס בצורה תקינה

#### פקודות שניתן להריץ מה **Command Prompt**:

**Bootrec /Fixmbr**: כאשר ישנה בעייה עם ה mbr פקודה זו מתקנת את המבר. פקודה זו אינה דורסת את טבלת המחיצות .

**Bootrec /Fixboot**: כאשר סקטור האתחול נפגם, או הותקנה מערכת הפעלה ישנה יותר. פקודה זו תתקן את סקטור האתחול.

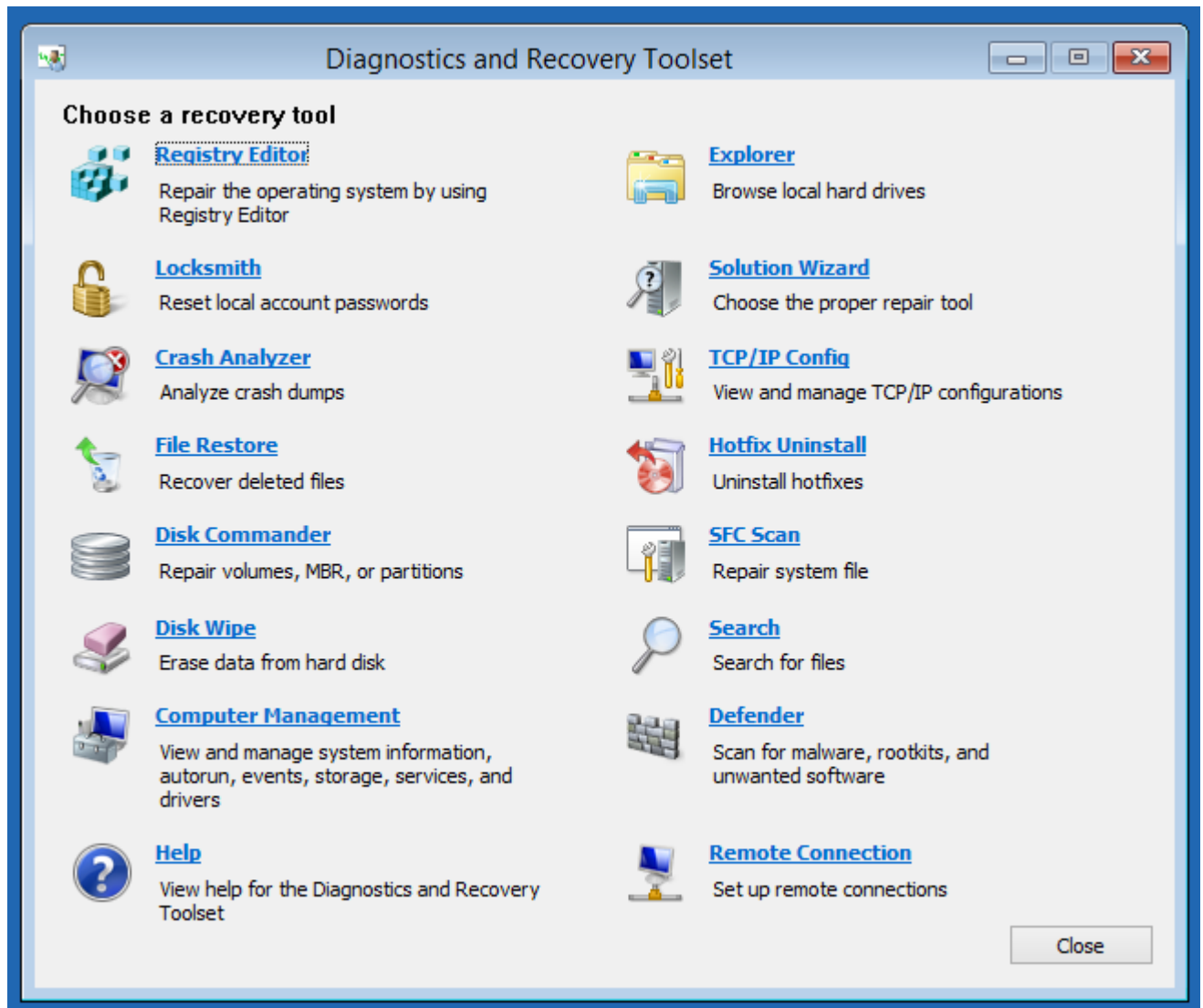
**Bootrec /Rebuildbcd**: סורק את המחשב להתקנות של windows ומוסיף אותם לטבלת הבcd (המכילה את הרשימה של כל מערכות ההפעלה על המחשב) .

**BcdBoot C:\Windows /s F: /f ALL** – הפקודה הזו נועדה במקרה שפקודת bootrec נכשלה, היא תעתיק את כל קבצי האתחול הדרושים מתיקיית ווינדוס אל המחיצה שנוצרה ב F כונן F וכמו כן היא יכולה לתמוך באתחול UEFI או MBR במקרה זה ציינו בשניהם.

## כלים נוספים לתיקון תקלות (DART)

מיקרוסופט מספקת לארגונים את היכולת להוריד כלי נוסף שעולה מדיסק און קי או CD ויכול לשמש לתיקון המע' לכלי הזה קוראים DART שהוא קיצור של Diagnostics and Recovery Toolset והוא מגיע כחלק מחבילה משלימה של כלים לתמיכה במע' הפעלה בארגון .

הכלי מספק מגוון רחב של אפשרויות תיקון מעבר לסביבת התיקון הרגילה , בתמונה תוכלו להתרשם ממגוון הכלים כולל כלי גיבוי ושחזור מידע שנמחק מהדיסק.



אחד הכלים היותר שימושיים הינו Locksmith שמאפשר איפוס סיסמה עבור משתמש מקומי שננעל , כמו כן יש אפשרות להשתלט מרחוק על המחשב , כלומר הטכנאי יכול להריץ את הכלי על המחשב התקול וטכנאי אחר יכול מהעמדה שלו להשתלט על המחשב ולראות את התפריט של DART אצלו בעמדה ולבצע את הפעולות כאילו הוא פיזית מול המחשב התקול.

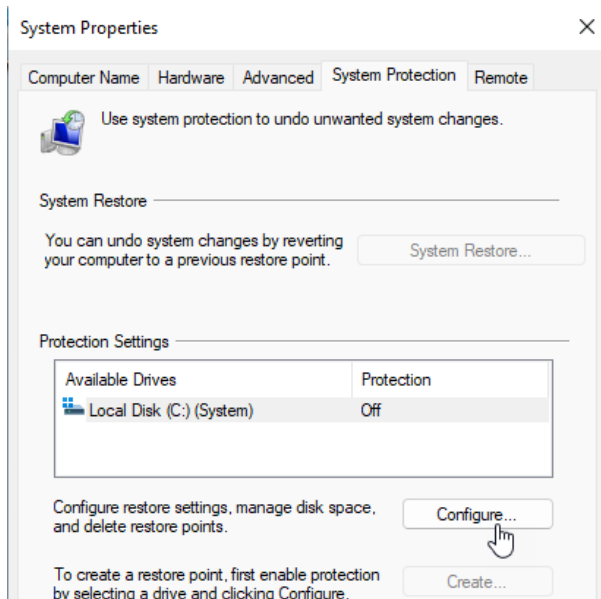
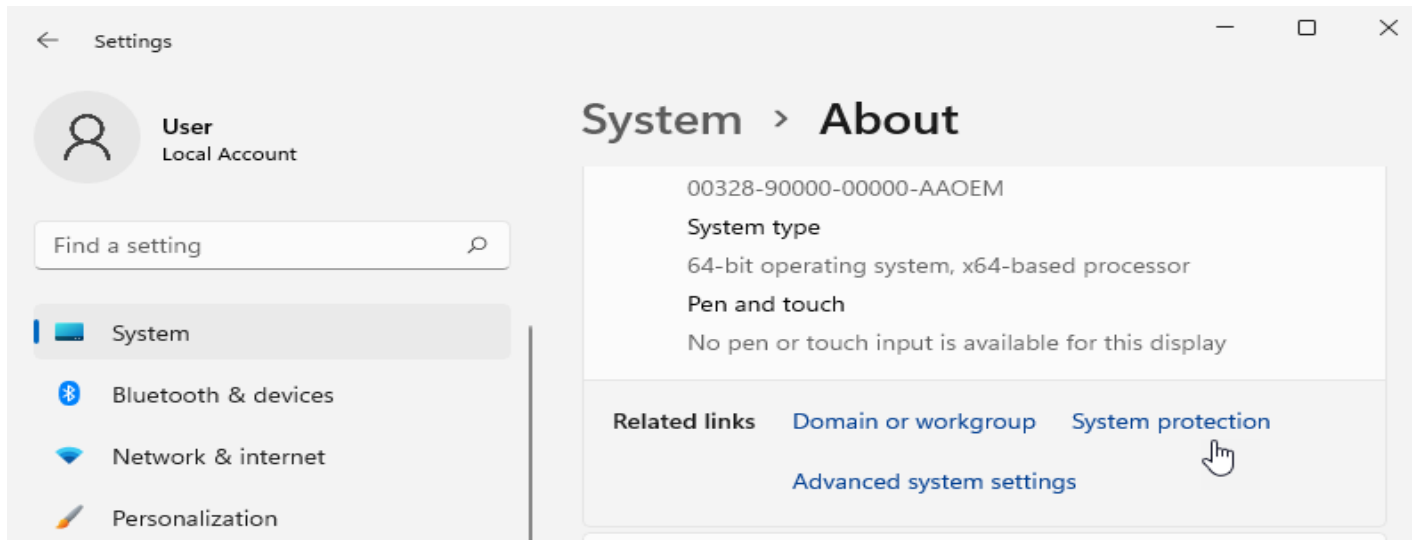
## ביצוע שחזור מערכת – System Restore

שחזור מע' יאפשר לנו לחזור להגד' וקבצים שהיו קיימים בנק' זמן שבה בוצעה יצירה של נק' שחזור.

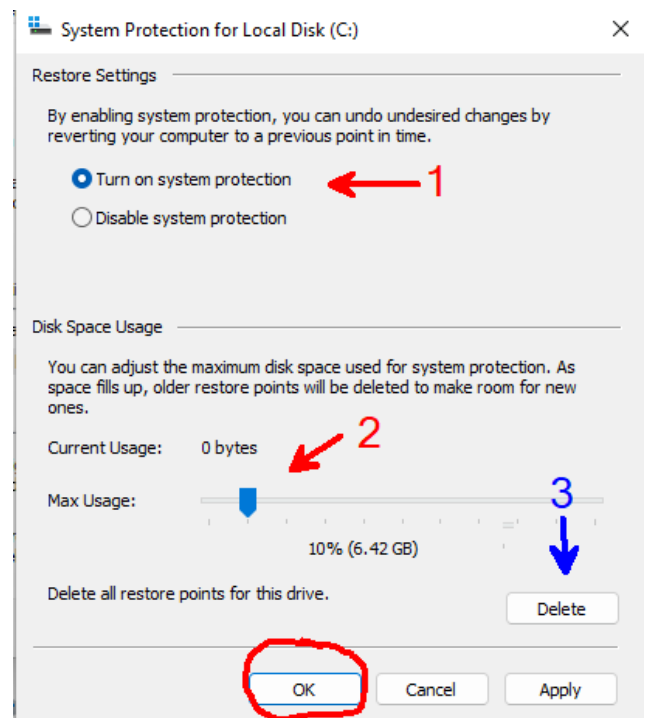
כאשר המנגנון מופעל (הוא כבוי בתור ברירת מחדל) נוצרות לנו נקודות שחזור, נקודות אילו יכולות להיווצר בצורה אוטו' – כאשר יש עדכון מע' או התקנה של תוכנה גדולה, עוד אפשרות היא יצירה מתוזמנת אחת לשבוע.

ובנוסף נוכל ליצור נקודת שחזור ידנית שנוצרה על ידנו בצורה יזומה.

הגישה דרך החיפוש או לוח הבקרה וכניסה להגדרות מתקדמות ומשם לבחור System Protection



ניכנס לתפריט ונראה שהאפשרות כבויה, נוכל לבחור להפעיל אותה



1. נפעיל את האפשרות

2. נבחר כמה מקום מהדיסק להקצות לשמירת קבצים והגדרות

3. נוכל לבחור למחוק את המידע ששמור בדיסק על מנת לפנות מקום למידע חדש. קחו בחשבון שבמצב זה לא יהיו לנו נקודות שחזור לחזור אליהן.

לאחר שביצענו הפעלה של האפשרות , נוכל לראות שיש לנו אפשרות לבצע נק' שחזור בצורה ידנית

