ESET SYSRESCUE LIVE

מדריך מוצר

תוכן עינייינים

1. ESET SysRescue Live 3

2. יצירת דיסק/התקן USB עם ESET SysRescue Live 3

2.1 יצירת התקן USB של ESET SysRescue Live בעזרת CD/DVD 5

3. הפעלת ESET SysRescue Live 6

4. שימוש ב- ESET SysRescue Live 7

4.1 סריקה יזומה 8

4.1.1 הגדרות מנוע ThreatSense 9

4.2 עדכון מאגר חתימות הוירוסים 11

4.3 מהי תוכנה לא רצויה? 12

4.4 כלים 12

4.4.1 Log Files 12

4.4.2 סטטיסטיקות הגנה 12

4.4.3 הסגר 12

4.4.4 שליחת קובץ לאבחון 13

4.5 העדפות 13

4.6 תפריט התוכנה 13

5. יציאה מ- ESET SysRescue Live 14

6. מחיקת ESET SysRescue Live מהתקן ה- USB 15

7. Bomgar and TeamViewer 16

8. סביבת שולחן העבודה 16

8.1 חיבורי רשת 17

9. פתרון בעיות 19

1.ESET SysRescue Live

ESET SysRescue Live הוא כלי חינמי המאפשר למשתמש ליצור דיסק/התקן USB הצלה. ניתן להריצו על מנת לסרוק את המערכת לקבצים נגועים ולנקותם.

היתרון המשמעותי של ESET SysRescue Live הוא שמערכת ההפעלה עולה בצורה עצמאית מתוך הדיסק/התקן USB, אך עדיין ישנה גישה למערכת ההפעלה הקיימת במערכת. כך ניתן להסיר נוזקות מקבצים נגועים שבמצב הפעלה רגיל לא ניתן להסירן (לדוגמה, קבצי מערכת הפעלה וכו').

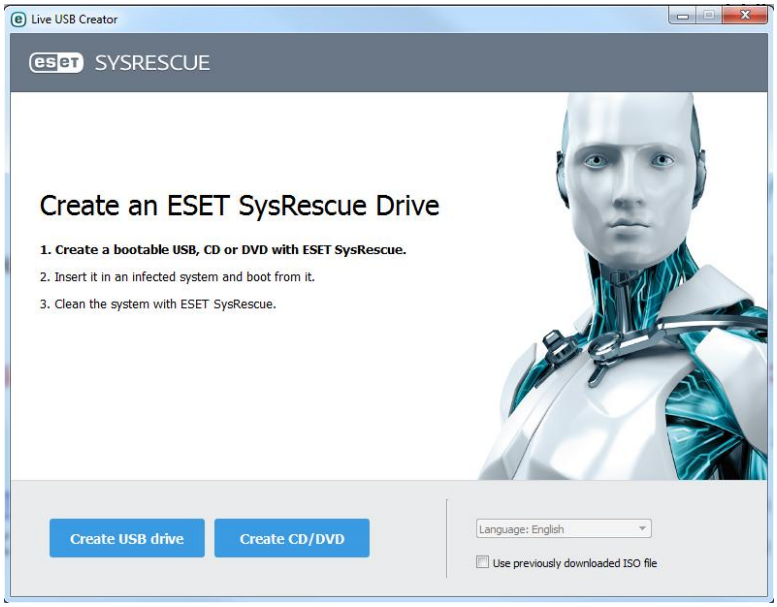
2. יצירת דיסק/התקן USB של ESET SysRescue Live

על מנת ליצור את דיסק/התקן USB הצלה של ESET SysRescue Live יש להשתמש במערכת הפעלה של windows.

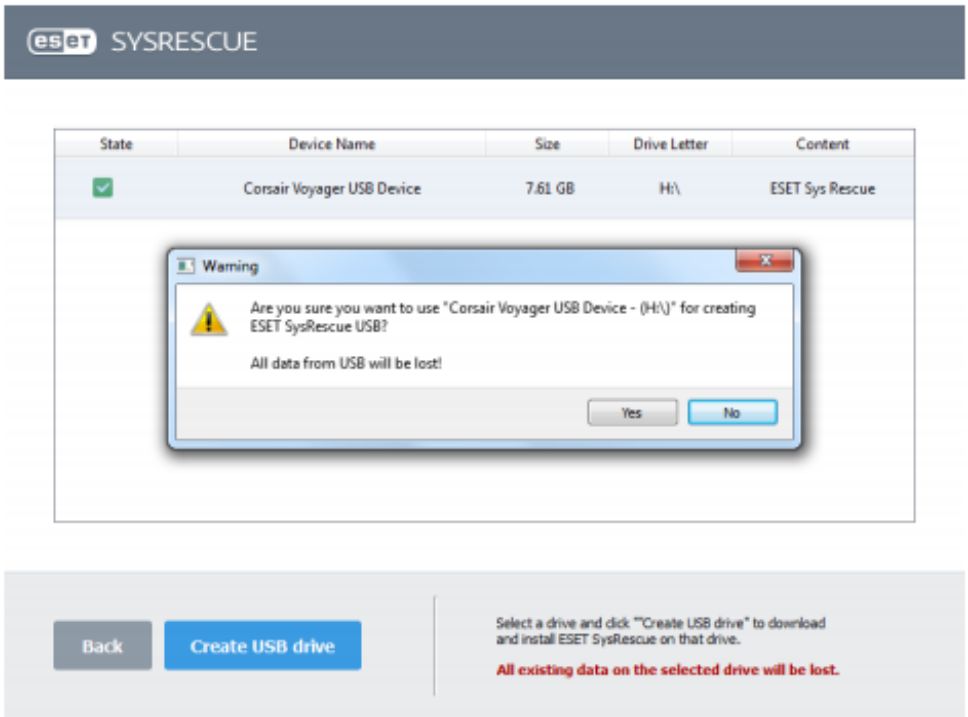
אזהרה: אם משתמשים בהתקן נייד ליצירת דיסק ההצלה, כל המידע בהתקן הנייד יימחק.

על מנת ליצור את דיסק ההצלה יש לפעול לפי השלבים הבאים:

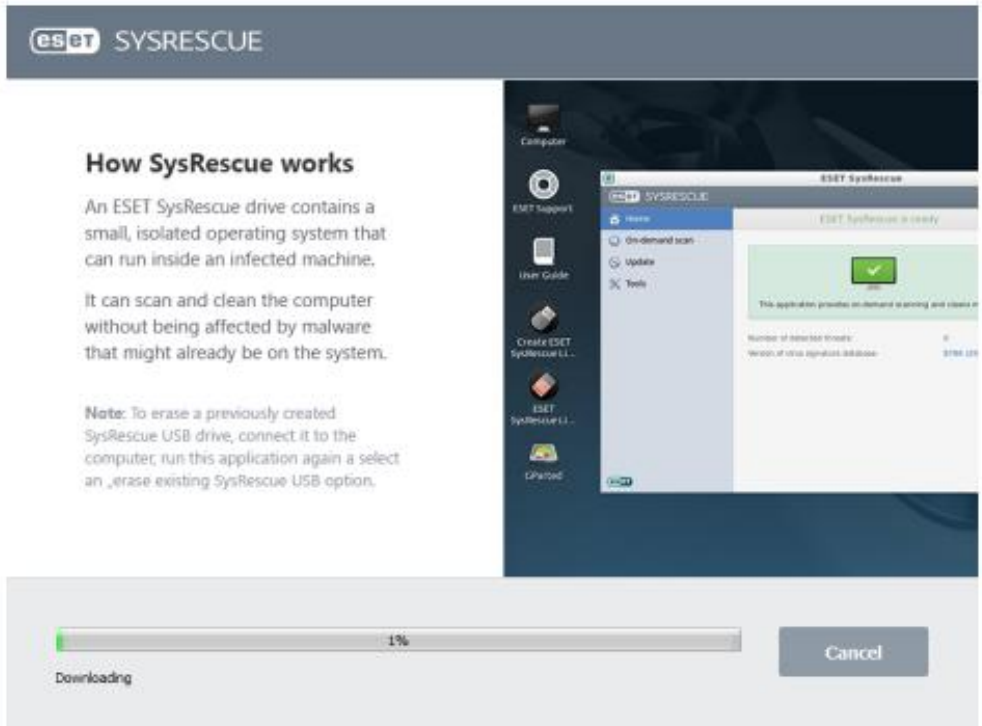
1. יש להוריד את ESET Live USB Creator מהקישור הבא: ESET SysRescue Live.
2. יש להריץ את הקובץ שירד ולבחור ב- **Create USB drive** או **Create CD/DVD.**



3. יש לבחור בסוג המדיה הרצויה וללחוץ אישור.

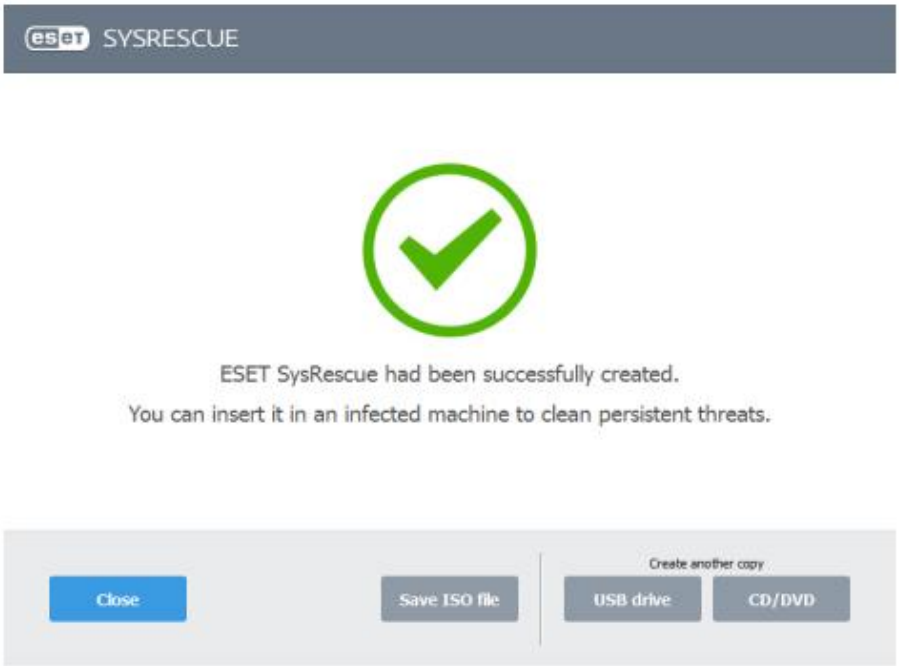


4. יש לחכות עד סיום יצירת דיסק ההצלה של ESET SysRescue Live.



5. ההודעה "**ESET SysRescue has been successfully created**" תופיע בסיום התהליך.

על מנת ליצור עותק נוסף בזמן מאוחר יותר, מומלץ לבחור ב-**Save ISO file**.
במהלך יצירת הדיסק בסעיף 2 יש לסמן את "**Use previously downloaded ISO image**" על מנת לבחור את הקובץ ששמרת קודם.



6. כאשר דיסק ההצלה מוכן, יש לשמור אותו במקום בטוח. כעת ניתן להשתמש בדיסק ההצלה על מחשב נגוע.

2.1 יצירת התקן USB של ESET SysRescue Live בעזרת CD/DVD

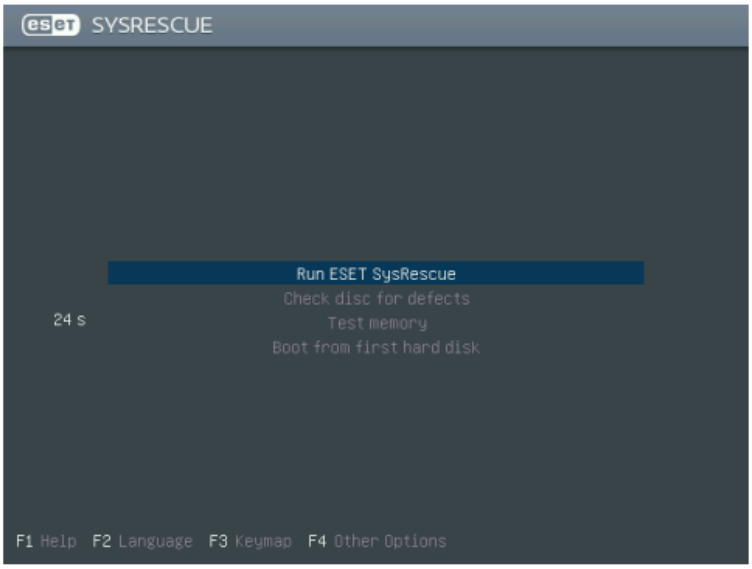
לחילופין, ניתן גם ליצור התקן USB עם ESET SysRescue Live ישירות מתוך דיסק ההצלה.

על מנת לעשות זאת יש להכניס התקן USB למחשב וללחוץ על הסמל Create ESET SysRescue Live USB בשולחן העבודה. בחר בהתקן ה-USB הרצוי מהרשימה ולחץ OK על מנת להתחיל את ההתקנה.

3. הפעלת ESET SysRescue Live

על מנת ש- ESET SysRescue Live יתפקד באופן תקין, יש לאפשר העלאת המערכת מהתקן חיצוני. ניתן לאפשר זאת ב- BIOS על ידי שינוי Boot Priority, בלחיצה על מקש F8 בדר"כ או מקש ESC תלוי בסוג ה-BIOS. הוראות לכניסה ל- BIOS מופיעות ברגע הפעלת המערכת.

בהעלאת המערכת דרך ESET SysRescue Live יופיע מסך אפשרויות לבחירה. במידה ולא תיבחר אפשרות, האפשרות המסומנת תיבחר לאחר 30 שניות.



האפשרויות הזמינות הן:

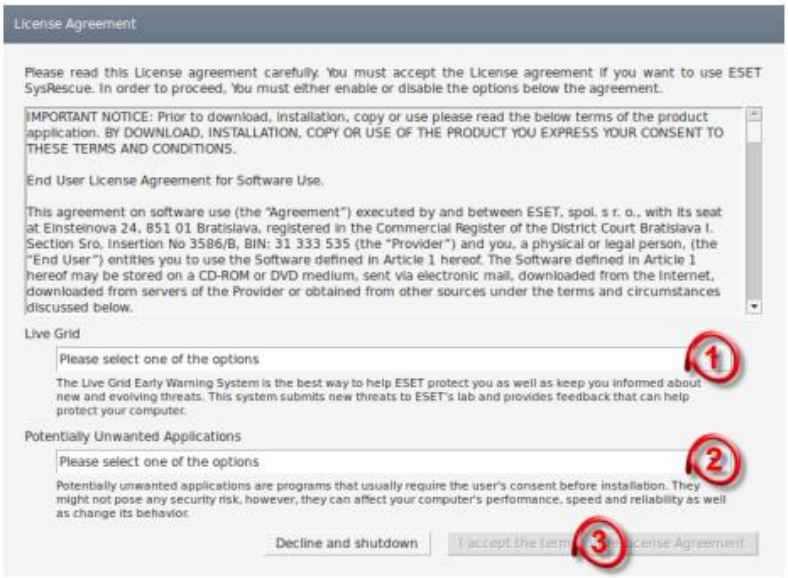
- **Run ESET SysRescue Live**- מריץ את ESET SysRescue Live עם השפה שנבחרה.
- **Check disc for defects**- בודק את תקינות דיסק/התקן USB. במידה ובדיקת הדיסק תסתיים עם שגיאות ייתכן והדיסק פגום. במקרה כזה יהיה צורך ליצור דיסק/התקן USB חדש בעזרת שלבי ההתקנה.
- **Test memory**- מריץ כלי ייעודי לבדיקת הזיכרון (Memtest+86) הבודק את הזיכרון הפיזי במערכת ומאתר שגיאות.
- **Boot from first hard disk**- יש לבחור באפשרות זו להעלאת המערכת באופן רגיל.

מקשי הפונקציות F1-F4 שימושיים להגדרות מיוחדות להעלאת המערכת.
האפשרויות הזמינות הן:

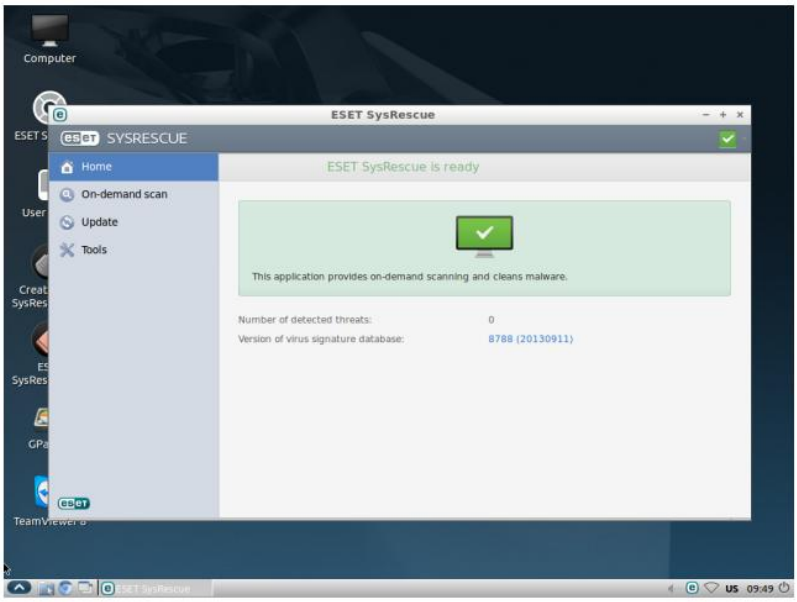
- **F1 Help**- מציג את תפריט העזרה של ESET SysRescue Live.
- **F2 Language**- מאפשר לבחור את השפה הממשק ל-ESET SysRescue Live .
- **F3 Keymap**- מאפשר לשנות את הגדרות המקלדת.
- **F4 Other Options**- מאפשר לשנות הגדרות kernel.
- **ESC**- סוגר כל חלון פתוח. מאפשר להחליף למצב טקסט (מומלץ למשתמשים מתקדמים בלבד).

4. שימוש ב- ESET SysRescue Live

לאחר הפעלת ESET SysRescue Live יש לקרוא ולקבל את הסכם הרישוי. יש לבחור האם להשתמש ב- Live Grid (1), הגדרה לגילוי תוכניות לא רצויות (2), לאחר מכן יש ללחוץ על **"I Accept the Terms in the license Agreement"** (3) על מנת לאשר את הסכם הרישוי.



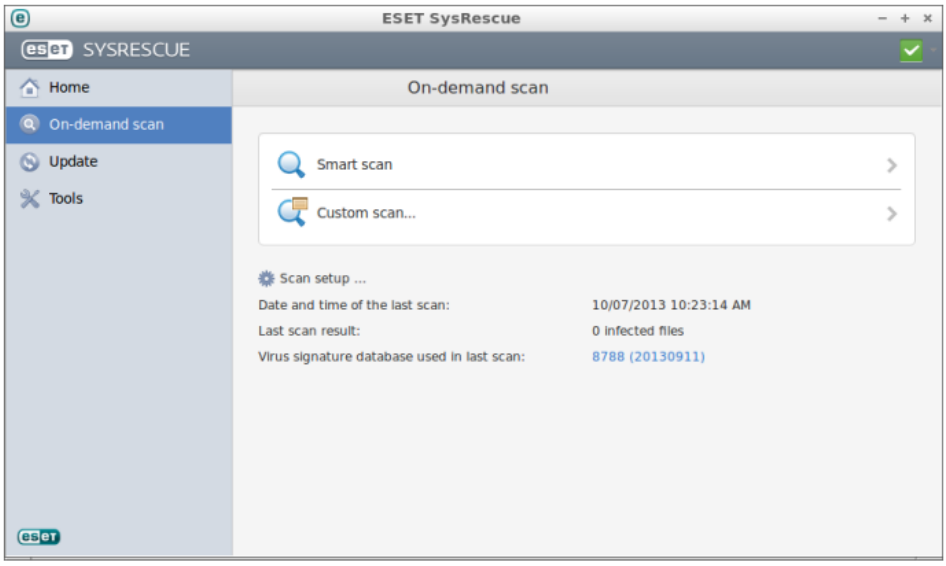
לאחר אישור הסכם הרישוי, החלון הראשי יופיע.



4.1 סריקה יזומה

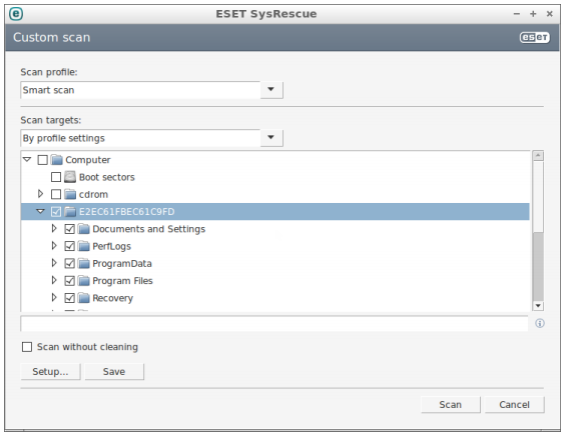
ESET SysRescue מסוגל לסרוק ולנקות מחיצות עם מערכות קבצים של Windows ו-Linux, כגון: ntfs, vfat (fat32), reiserfs, ext4, ext3. אפשרויות הסריקה הזמינות הן:

- **Smart scan**- אפשרות זאת מתחילה את סריקת המחשב וניקוי האיומים במהירות ללא הגדרה מראש. היתרון העיקרי בסוג סריקה זה הוא תפעול קל ללא הגדרת המשתמש.
- **Custom scan**- הפיתרון האופטימלי לקביעת הגדרות מראש לסריקה, כגון: כוננים לסריקה ושיטות לסריקה. היתרון העיקרי בסוג סריקה זה הוא שניתן לקבוע את האפשרויות הרצויות.



הערה: שתי אפשרויות הסריקה מוגדרות לסרוק את הכוננים ששויכו לאות (C:) תחת ספריית **/media**

במידה ומריצים **Custom scan**, ניתן לבחור באחת מאפשרויות ברירת המחדל, או ללחוץ על **setup**, על מנת להגדיר את אפשרויות הסריקה או לבחור את הכוננים שברצונך לסרוק. ניתן לבחור ב-**Scan without cleaning** על מנת שלא יתבצע ניקוי לאיומים המתגלים בסריקת המערכת.



4.1.1 הגדרות מנוע ThreatSense

הגדרות מנוע ה- **ThreatSense** מאפשרות לקבוע מספר אפשרויות סריקה:

- סוגי קבצים וסיומות שייסרקו.
- סוגי שיטות הגילוי.
- רמת הניקוי.

תחת **Objects**, ניתן להגדיר אילו קבצים ייסרקו לאיומים:

- **Files**- סריקת כל סוגי הקבצים הנפוצים (תוכנות, תמונות, קבצי שמע, קבצי וידאו, קבצי נתונים וכו')
- **Symbolic links**- (בסורק On-demand בלבד) סורק סוגי קבצים מיוחדים המכילים מלל המקשר לקובץ אחר או תיקייה.
- **Email files**- (לא זמין בסריקה בזמן אמת) סורק קבצים מיוחדים המכילים הודעות מייל.
- **Mailboxes**- (לא זמין בסריקה בזמן אמת) סורק תיבות דואר של משתמשים במערכת. שימוש לא נכון האפשרות זו יכול לגרום להתנגשות עם תיבת הדואר של המשתמש.
- **Archives**- (לא זמין בסריקה בזמן אמת) סורק קבצים המקובצים כארכיון (.rar,.zip,.arj,.tar. וכו').
- **Self-extracting archives**- (לא זמין בסריקה בזמן אמת) סורק קבצים המכילים קבצי ארכיון הנפתחים עצמאית.
- **Runtime packers**- בניגוד לקבצי ארכיון רגילים, קבצים אלה נפתחים בזיכרון בנוסף להפעלה סטטית רגילה.
- **Boot sectors**- סורק את סקטור האיתחול על מנת למצוא איומים ב-MBR.

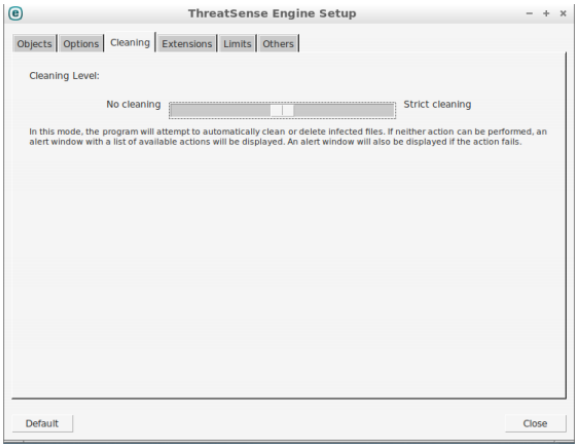
תחת **Options**, ניתן להגדיר את השיטות לסריקת המערכת לאיומים:

- **Heuristics**- שיטה המשתמשת באלגוריתם המנתח את הפעילות הזדונית של התוכנה. היתרון המשמעותי של שיטה זו הוא גילוי של נוזקות חדשות ולא מוכרות.
- **Advanced heuristics**- שיטה מתקדמת, שפותחה ע"י ESET לגילוי תולעים וטרויאנים הכתובים בשפות תכנות ברמה גבוהה. דבר המגביר את רמת הגילוי של הסריקה.
- **Potentially unwanted applications**- תוכנות אלה לא נועדו להזיק למערכת במכוון אך יכולות לפגוע בביצועי המערכת. תוכנות אלה בדר"כ מותקנות בהרשאת המשתמש. השינויים הנגרמים במערכת הם: חלונות/הודעות קופצות, תהליכים מוסתרים רצים, עלייה בשימוש במשאבי מערכת, שינויים בתוצאות חיפוש ותוכנות המתקשרות מול שרתים מרוחקים.
- **Potentially unsafe applications**- תוכנות מסחריות לגיטימיות היכולות להוות פירצת אבטחה לתוקפים. תוכנות אלה כוללות תוכנות לשליטה מרחוק ולכן האפשרות הזו אינה זמינה בברירת מחדל.

תחת **Cleaning**, ניתן להגדיר את האופן בו הסורק ינקה את הקבצים הנגועים. ישנן 3 אפשרויות:

- **No cleaning**- קבצים נגועים לא ינוקו אוטומטית. בסוף הסריקה יתקבל חלון אזהרה עם אפשרויות לבחירה.

- **Standard cleaning**- התוכנה תבצע ניקוי או מחיקה אוטומטית לקבצים נגועים. במידה ואין אפשרות לבצע זאת, התוכנה תציע אפשרויות לבחירה.
- **Strict cleaning**- התוכנה תנקה או תימחק אוטומטית את כל הקבצים הנגועים (כולל ארכיון). למעט קבצי מערכת הפעלה שבמידה ולא ניתן לנקותם התוכנה תציע אפשרויות לבחירה.



תחת **Extentions**, ניתן להגדיר את סיומות הקבצים שלא ייסרקו. סיומות אלה קובעות את סוגי ותוכן הקבצים. בברירת מחדל, כל הקבצים נסרקים ללא קשר לסיומת. ניתן להוסיף או להסיר סיומות קבצים מסריקה בעזרת מקשי **Add** או **Remove**. לעיתים הוצאת סיומות קבצים מסריקה היא הכרחית על מנת לאפשר פעולה נכונה של תוכנה המשתמשת בקבצים אלה.

תחת **Limits**, ניתן להגדיר את הגודל המקסימלי של האובייקטים ורמת הארכיונים הנסרקים.

- **Maximum Size**- מגדיר את הגודל המקסימלי של האובייקטים שייסרקו. האנטי וירוס יסרוק אך ורק אובייקטים שגודלם קטן מהמכסה שהוגדרה. לא מומלץ לשנות הגדרה זו מכיוון שברוב המוחלט של המקרים אין צורך.
- **Maximum Scan Time**- מגדיר את הזמן המקסימלי שניתן לסרוק כל אובייקט. האנטי וירוס יסרוק את האובייקט עד מכסת הזמן שהוגדרה ויעבור לאובייקט הבא אפילו שהסריקה לא הסתיימה.
- **Maximum Nesting Level**- מגדיר את העומק המקסימלי לסריקת קבצי ארכיון. לא מומלץ לשנות הגדרה זו.
- **Maximum File Size**- מגדיר את הגודל המקסימלי לסריקת קבצים הנמצאים בתוך ארכיון (לאחר חילוץ).

במידה ותרצה לבטל את סריקת תיקיות המערכת כגון: /proc, /sys , בחר ב- **Exclude system control folders from scanning** (אפשרות זו אינה זמינה עבור סריקה בהפעלה).

תחת **Others**, ניתן להגדיר אפשרויות נוספות למנוע **ThreatSense**.

- **Enable Smart optimization**- ההגדרות האופטימליות ביותר יהיו בשימוש ויבטיחו רמת סריקה יעילה ביותר, תוך כדי שמירה על מהירות סריקה גבוהה. מודולי ההגנה השונים סורקים בחוכמה, ומתאימים שיטות סריקה שונות לסוגי הקבצים השונים. צוות הפיתוח של ESET מיישם שינויים חדשים ברציפות, על מנת לשפר את הסריקות. במידה ו- **Smart optimization** לא זמין, רק ההגדרות שהמשתמש קבע במנוע ה- **ThreatSense** יקבעו את אופן הסריקה.
- **Scan alternative data streams**- מידע הנמצא בשימוש של מערכת ההפעלה הכולל קבצים ותיקיות המוסתרים משיטות סריקה רגילות. ישנם איומים רבים המנסים להתחזות למידע זה על מנת לחמוק מגילוי.
- **Preserve last access timestamp**- אפשרות זאת שומרת על הזמן המקורי של סריקת הקבצים ולא משנה אותו.

4.2 עדכון מאגר חתימות הוירוסים

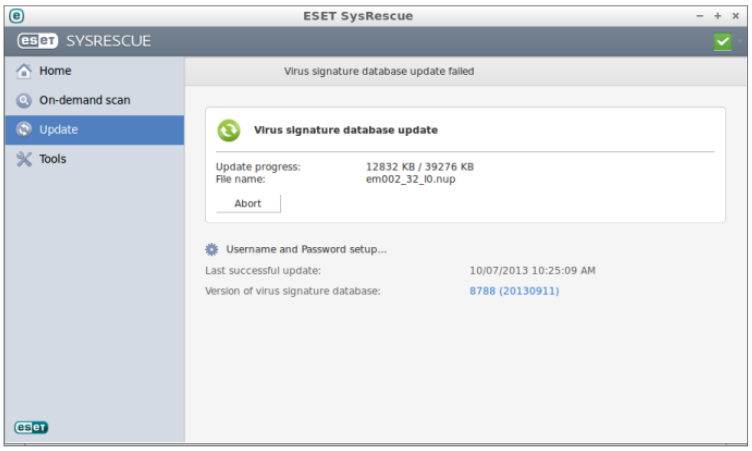
היכולת לעדכן את מאגר חתימות הוירוסים היא מרכיב הכרחי ב- **ESET SysRescue**. אנו ממליצים לעדכן את מאגר החתימות לפני ביצוע סריקה.

בתפריט הראשי יש ללחוץ **Update** על מנת לבדוק את חתימת הוירוסים האחרונה כולל תאריך ושעה, וכמו כן האם יש צורך בעדכון מאגר חתימות הוירוסים. על מנת להתחיל עדכון לחתימות הוירוסים באופן ידני יש ללחוץ על **Update virus signature database**.

במידה והעדכון נכשל, יש לבדוק תחילה את חיבור האינטרנט ב- **Network connection settings** הממוקם בתפריט **Preferences** בתחתית המסך מצד שמאל.

בנסיבות רגילות, כאשר העדכון יורד בהצלחה, ההודעה **"Virus signature database is up to date"** תופיע בחלון **Update**.

חלון ה-**Update** גם מכיל מידע לגבי גרסת מאגר חתימות הוירוסים. גרסה זו משמשת כקישור לאתר ESET העולמי, שם מתוארות כל החתימות שהוספו לעדכון זה.



הערה: מאחר ש- **ESET SysRescue** הוא חינמי, אין צורך בשם משתמש וסיסמה על מנת לבצע עדכון, אך ניתן לשנות את הגדרות שרת העדכון בהגדרות מתקדמות (**F5**) > **Updates** > **Edit**.

4.3 מהי תוכנה לא רצויה?

תוכנה לא רצויה (**PUA**) לא בהכרח נועדה להיות מזיקה, אך בכל זאת יכולה לגרום לפגיעה בביצועי המערכת. תוכנות אלו מותקנות בדר"כ עם הרשאות המשתמש. במקרה ותוכנות אלו מותקנות במערכת השינויים העיקריים הם:

- חלונות חדשים שלא ראית מעולם (חלונות קופצים, פרסומות וכו').
- הפעלה והרצה של תהליכים מוסתרים.
- עלייה בשימוש במשאבי מערכת.
- שינויים בחיפושים ותוצאות.
- תוכנות שמתקשרות עם שרתים מרוחקים.

4.4 כלים

4.4.1 Log Files

קבצי הרישום מכילים מידע לגבי כל ארועים החשובים שהתרחשו במערכת, ומספקים סקירה על איומים שנמצאו. רישום הוא כלי הכרחי לניתוח המערכת, גילוי איומים ופתרון בעיות. הרישום פעיל ברקע ללא התערבות משתמש.
ניתן לצפות בקבצי הרישום במסך ה-ESET SysRescue הראשי, לחיצה על **Tools** > **Log files**.
יש לבחור את סוג הרישום הרצוי בעזרת תפריט הגלילה **Log** בחלק העליון של החלון.
הרישומים הבאים זמינים:

- **Detected threats**- מציג את כל הארועים הקשורים לגילוי איומים.
- **Events**- אפשרות הנועדה למנהלי רשת ומשתמשים לפיתרון בעיות. כל הפעולות החשובות שבוצעו ע"י ESET SysRescue מתועדות ברישום זה.
- **On-demand scan**- מציג את תוצאות כל הסריקות שבוצעו במערכת. לחיצה כפולה על שורת הסריקה תציג את דו"ח הסריקה המפורט.

4.4.2 סטטיסטיקות הגנה

ניתן לצפות בגרף סטטיסטיקות ההגנה של ESET SysRescue ע"י לחיצה על **Tools** > **Protection statistics**. גרף ה-**Antivirus and Antispyware Protection Statistics** מציג את מספר האובייקטים הנגועים והאובייקטים שנוקו. מתחת לגרף הסטטיסטיקות, ניתן לראות את סך האובייקטים שנסרקו, האובייקטים האחרונים שנסרקו וזמן הסטטיסטיקה. יש ללחוץ **Reset** כדי לנקות את כל המידע.

4.4.3 הסגר

תפקיד ההסגר הוא לאחסן באופן בטוח קבצים נגועים. קבצים מועברים להסגר במידה ולא ניתן לנקותם, לא בטוח למחוק אותם או אם זוהו באופן שגוי ע"י ESET SysRescue.
ניתן להסגיר כל קובץ במידה והוא מתנהג באופן חשוד אך לא מזוהה ע"י סורק האנטי-וירוס.
ניתן לשלוח קבצים מוסגרים לאבחון במעבדות הפיתוח של ESET.

על מנת לשחזר קובץ למיקומו המקורי, יש לסמן אותו וללחוץ **Restore**. ניתן גם לבחור כל קובץ מהרשימה ללחוץ קליק ימני ו-**Restore** או **Restore to** על מנת לשחזר את הקובץ למיקום אחר מהמיקום המקורי.

4.4.4 שליחת קובץ לאבחון

חלון שליחת הקובץ לאבחון מאפשר לשלוח קבצים החשודים כמזיקים לצוות הפיתוח של ESET על מנת לאבחן אותם ולקבוע האם הם באמת מזיקים ולעדכן את גרסת מאגר חתימות הוירוסים בהתאם.

לחילופין, ניתן לשלוח קובץ גם בצורת דואר אלקטרוני. ראשית צריך לקבץ את הקובץ החשוד ב-**ZIP/RAR**, לקבוע סיסמה "**infected**" ולשלוח אותו לכתובת **Samples@eset.com**. יש לרשום מידע מקיף עד כמה שניתן לגבי הקובץ (כגון: מהיכן הורד הקובץ).

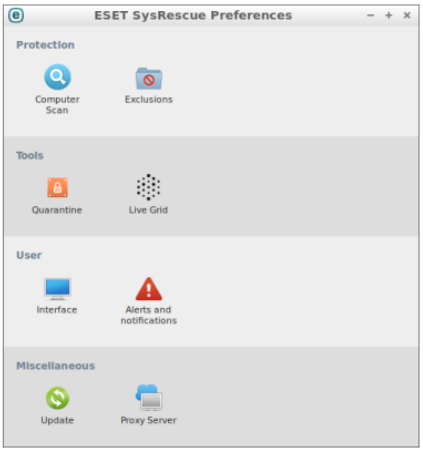
הערה: לפני שליחת קובץ לאבחון, יש לוודא מתקיים בו אחד או יותר מהקריטריונים הבאים:

- הקובץ אינו מתגלה בסריקה כלל.
- הקובץ מתגלה בטעות בסריקה.

לא תתקבל תשובה חזרה במידה והמידע לעיל לא יירשם בפנייה.

4.5 העדפות

על מנת להיכנס להעדפות ה-**ESET SysRescue**, יש ללחוץ על (**F5**) או ללחוץ על ה-**V** בפינה הימנית העליונה ו-**Preferences**.



האפשרויות הבאות זמינות:

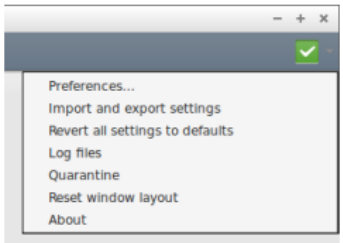
Computer scan- ניתן לבחור בפרמטרי הסריקה, פרופיל הסריקה ויצירת פרופיל סריקה חדש, שינוי הגדרות **ThreatSense engine** (כגון: סיומות קבצים לסריקה, שיטות זיהוי וכו').ניתן לבחור גם יעדי סריקה, תיקיות וקבצים לסריקה.
Exclusions- מאפשר להוציא קבצים ותיקיות מסריקה. על מנת לוודא שכל האובייקטים יסרקו לאיומים, מומלץ לא הוציא אובייקטים מסריקה אלא אם הדבר הכרחי, לדוגמה: כאשר ישנו קובץ בסיס נתונים גדול שיאט את הסריקה או תוכנה שתתנגש עם הסריקה.

Quarantine- אפשור/ביטול סריקת הקבצים בהסגר לאחר כל עדכון חתימות וירוסים.
Live Grid- אפשור/ביטול **ESET Live Grid**, שליחה של קבצים חשודים לאבחון ומידע סטטיסטי אנונימי.
Interface- שינוי ממשק המשתמש של **ESET SysRescue**. משתמשים יכולים לאפשר תפריט סטנדרטי, הסתר תיאורי כלים או הראה קבצים מוסתרים.
Alerts and notifications- ניתן לבחור אלו הודעות יופיעו ב-**Advanced Setup**, ביטול כל ההודעות, שינוי זמן הופעת ההודעות או שינוי הגדרות מצב מסך מלא.
Update- ניתן לבחור בשרת העדכון, לשנות שם משתמש וסיסמה, לבטל הודעות על עידכון או לנקות את ה- **Update cach**.
הערה: מכיוון ש- **ESET SysRescue** הוא כלי חינמי, לא נדרש שם משתמש וסיסמה לביצוע עדכון. במידה ויש צורך לשנות את שרת העדכון, ניתן לשנות ע"י לחיצה על **Edit**.
Proxy Server- במידה וישנו שרת פרוקסי ברשת המנהל את תעבורת הרשת יש להזין את פרטי השרת בחלק זה.

ניתן ללחוץ **Default** על מנת לאפס את ההגדרות.

4.6 תפריט התוכנה

כדי להיכנס לתפריט התוכנה, יש ללחוץ על ה-**V** הירוק בפינה הימנית העליונה של החלון הראשי של **ESET SysRescue**.



Preferences- יש לבחור באפשרות זו על מנת לשנות את אפשרויות **ESET SysRescue**.
Import and Export settings- שימוש באפשרות זו על מנת לייצא או לייבא קובץ הגדרות ל-**ESET SysRescue**.
Revert all settings to default- מאפס את כל השינויים שנעשו בהגדרות לברירת מחדל.
Log files- קבצי הרישום מכילים את כל המידע לגבי ארועי המערכת החשובים ומספקים סקירה על האיומים שנמצאו.
Quarantine- הוספה, שחזור ומחיקה של אובייקטים בהסגר.
Reset windows layout- מאפס את גודל ומיקום החלון לברירת מחדל.
About- מראה את גרסת המוצר של **ESET SysRescue**. יש ללחוץ על **More information** בחלון **About ESET SysRescue** להצגת מידע על מודולי התוכנה השונים.

5. יציאה מ-ESET SysRescue Live

על מנת לצאת מ-**ESET SysRescue Live** יש ללחוץ על > **Logout** ולאחר מכן לבחור **Reboot** או **Shutdown**.

אזהרה: מומלץ לא להכריח כיבוי או הפעלה מחדש (בעזרת כפתורי המחשב).

6. מחיקת ESET SysRescue Live מהתקן ה-USB

יש להשתמש בכלי זה על מנת לשחזר את התקן ה-USB למצב רגיל. יש לוודא שהתקן ה-USB מחובר למחשב. ישנן 2 דרכים לביצוע פעולה זאת:

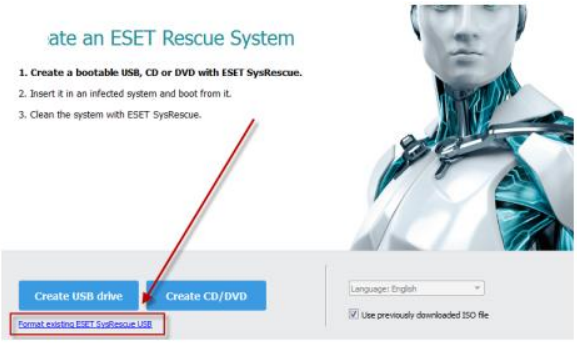
1. בעזרת ESET SysRescue Live

יש ללחוץ לחיצה כפולה על סמל **ESET SysRescue Live Live USB Cleaner** (נמצא על שולחן העבודה) ועקוב אחר ההוראות באשף.

הערה: אפשרות ניקוי זאת זמינה רק מתוך דיסק **ESET SysRescue Live**.

2. ניקוי **ESET SysRescue Live using ESET Live USB Creator**

- יש להוריד ולהריץ את **ESET Live USB Creator** על מערכת הפעלה של **Windows**.
- יש ללחוץ על **Format existing ESET SysRescue Live USB**.
- יש לבחור בהתקן **ESET SysRescue Live** ולאשר את פעולת **Erase USB drive**.



הערה: הניקוי יתאפשר אך ורק בהתקן עם **ESET SysRescue Live** על מנת למנוע מחיקה של התקני **USB** אחרים.

7. Bomgar and TeamViewer

במקרה של תקלה טכנית קשה לפיתרון (כגון: לא ניתן לסרוק את המערכת בגלל וירוס), ניתן להשתמש ב- **TeamViewer** או **Bogmar** כדי לאפשר חיבור מרחוק, שיתוף שולחן עבודה, והעברת קבצים למחלקת התמיכה הטכנית של **ESET**.

כדי לפתוח חיבור **Bogmar** יש לבצע את הפעולות הבאות:

1. מתוך שולחן העבודה של **ESET SysRescue Live** יש ללחוץ על > **Internet** < **Bogmar Support**.
2. יש ליצור קשר עם מחלקת התמיכה הטכנית של **Comsecure** בשעות הפעילות.
3. יש להזין את מפתח החיבור שמתקבל ממחלקת התמיכה.

כדי לפתוח חיבור **TeamViewer** יש לבצע את הפעולות הבאות:

1. מתוך שולחן העבודה של **ESET SysRescue Live** יש ללחוץ על > **Internet** < **TeamViewer**.

2. יש לוודא ש- *Ready to connect (secure connection)* מופיע.
3. יש ליצור קשר עם מחלקת התמיכה הטכנית של **Comsecure** בשעות הפעילות.
4. יש פרט את המזהה שלך (**Your ID**) ואת הסיסמה (**Password**) על מנת ליצור את החיבור מרחוק.

לאחר פתרון התקלה, נציג התמיכה הטכנית של **Comsecure** ינתק את החיבור מרחוק.

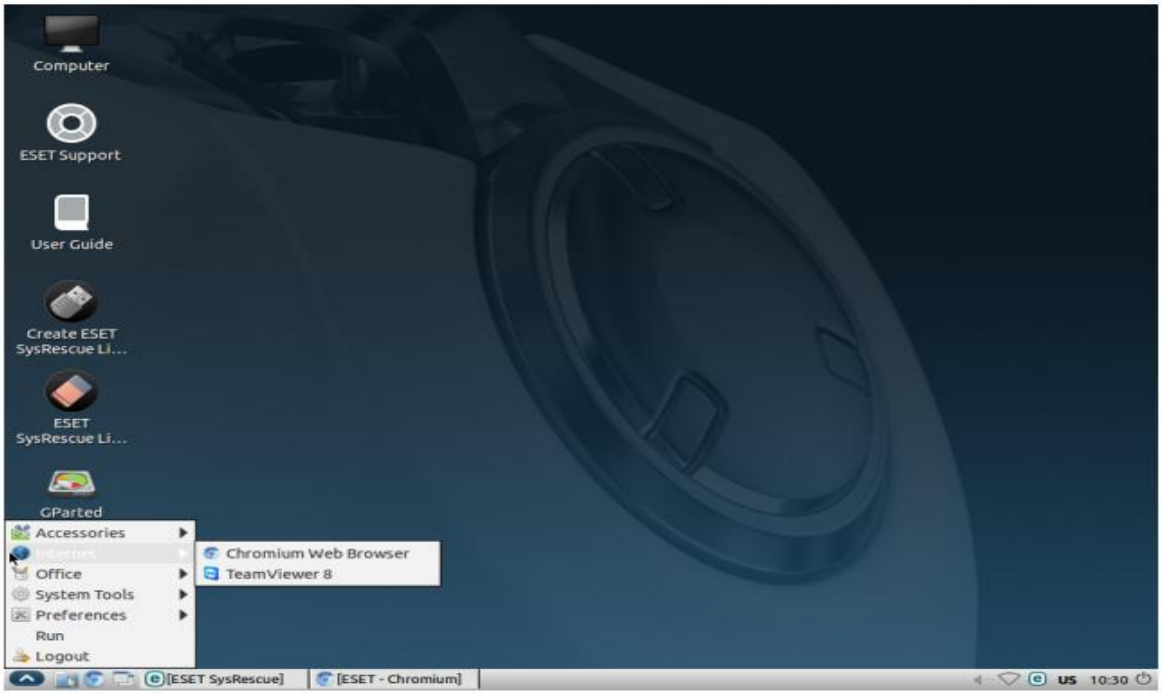
8. סביבת שולחן העבודה

ESET SysRescue Live רץ על מערכת הפעלה **GNU** של **Linux**. שולחן העבודה ע"ב **LDXE** קל משקל וגורם לביצועים מהירים.

מערכת ה-**APT** מאפשרת להתקין תוכנות או דרייברים שימושיים.

למנהלי רשתות מנוסים של **Linux** ניתן להשתמש ב- **LXTerminal** על מנת לבצע פעולות הכרחיות תחת הרשאות **root**, כמו **fsck** לבדיקת קבצי מערכת ההפעלה, **cfdisk** או **GParted**.

כדי להתחבר לאינטרנט, יש להשתמש ב-**Chromium web browser** ע"י לחיצה על > **Internet** < **Chromium web browser**.



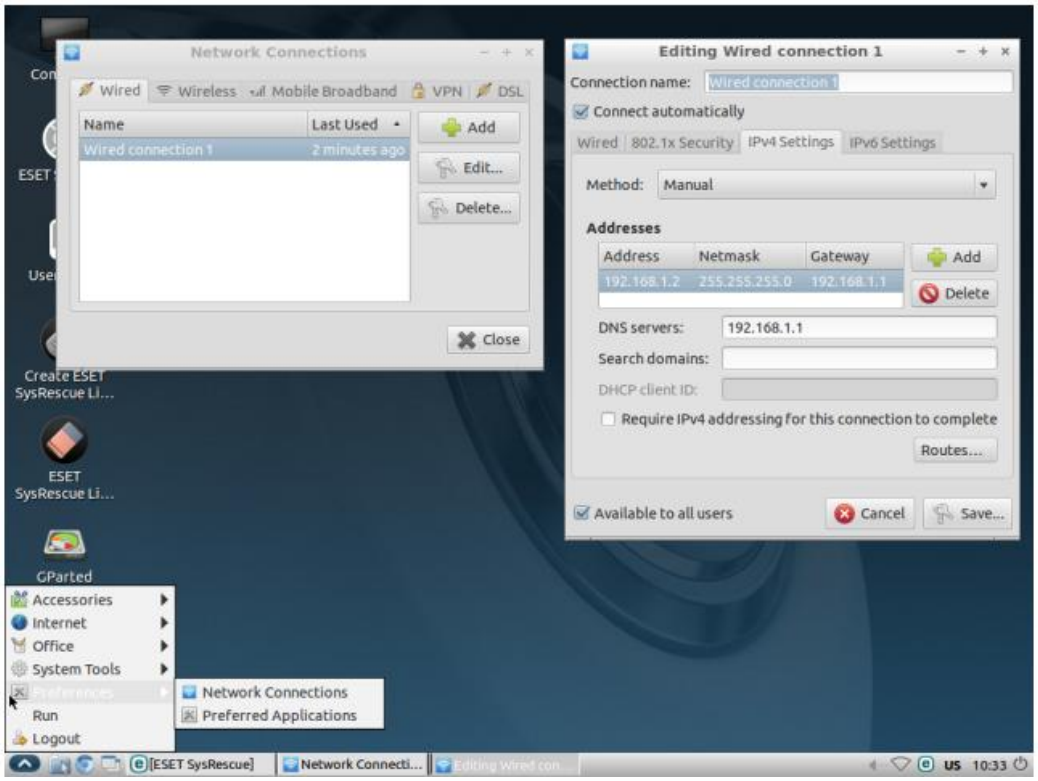
הערה: בסביבת **ESET SysRescue**, תוכנות מסויימות יפעלו באיטיות במיוחד אם מדובר ב-**CD/DVD**.

8.1 חיבורי רשת

שרת ה-DHCP אמור לחלק כתובת IP לחיבור לאינטרנט אוטומטית.

יש להשתמש בכלי Network Connections על מנת לשנות את הגדרות הרשת:

1. יש ללחוץ על סמל המערכת בפינה השמאלית התחתונה.
2. יש לבחור ב-Preferences ואז לבחור ב- Network Connections.
3. על מנת לשנות את הגדרות הרשת יש לבחור את חיבור הרשת וללחוץ Edit.
4. בחלון Editing Wired Connection יש לבחור בלשונית IPv4 Settings.
5. יש לשנות ב- Method ל-Manual ולהזין את המידע הרצוי בשדות Address, Netmask, Gateway ו- DNS servers.
6. יש ללחוץ Save ולהתחבר שוב לאינטרנט.



נדרש חיבור אינטרנט פעיל על מנת לעדכן את גרסת מאגר חתימות הוירוסים.

במידה ויש שימוש בשרת Proxy, יש צורך להזין את פרטי השרת. על מנת לבצע זאת יש ללחוץ **F5** להיכנס ל-**Preferences> Miscellaneous> Proxy server .**

9. פתרון בעיות

בעזרת ההוראות מטה ניתן לפתור בעיות נפוצות ב- ESET SysRescue Live.

לא ניתן להריץ את ESET SysRescue Live מהתקן ה-USB

על מנת ש- ESET SysRescue Live יתפקד באופן תקין, יש לאפשר העלאת המערכת מהתקן חיצוני. ניתן לאפשר זאת ב- BIOS על ידי שינוי Boot Priority, בלחיצה על מקש F8 בדר"כ או מקש ESC תלוי בסוג ה-BIOS. הוראות לכניסה ל- BIOS מופיעות ברגע הפעלת המערכת.

לא ניתן לבצע עידכון למאגר חתימות הוירוסים

במידה והעדכון נכשל, יש לבדוק תחילה את חיבור האינטרנט ב- **Network connection settings** הממוקם בתפריט **Preferences** בתחתית המסך מצד שמאל.

לא ידוע מה שם המשתמש והסיסמה

מכיוון ש- ESET SysRescue הוא כלי חינמי, לא נדרש שם משתמש וסיסמה לביצוע עדכון.

חלון ה- ESET SysRescue לא נפתח לאחר עליית המערכת

חלון ה- ESET SysRescue אמור להיפתח בצורה אוטומטית בנסיבות רגילות. במידה ולא, יש להפעילו ידנית בעזרת LXTerminal.

1. יש ללחוץ על סמל המערכת בפינה השמאלית התחתונה.
2. יש לבחור ב-Accessories ואז ב- LXTerminal.
3. יש להריץ את הפקודות הבאות:

```
Killall esets_gui
/opt/eset/esets/bin/esets_gui
```

לא ניתן לסרוק מחיצה בדיסק הקשיח

רשימה מלאה למערכות הקבצים הנתמכות ע"י ESET SysRescue Live נמצאת בתיקיית:
`/lib/modules/$(uname-r)/kernel/fs`