ESET Internet Security

User guide

Click here to display the Online help version of this document

ESET Internet Security was developed by ESET, spol. s r. o.

For more information visit www.eset.com.

Worldwide Customer Support: support.eset.com

REV. 22/10/2019

ESET Internet Security

ESET Internet Security מציג גישה חדשה לאבטחת מחשב באמת משולבת. הגרסה העדכנית ביותר של מנגנון הסריקה של ESET LiveGrid®, יחד עם מודולי חומת האש ומסנן דואר הזבל שלנו, שניתנים להתאמה אישית, פועלת במהירות ובדיוק רב כדי לשמור על בטיחות המחשב שלך. התוצאה היא מערכת חכמה שמוכנה תמיד להתריע על התקפות וקודים זדוניים שעשויים לסכן את המחשב.

ESET Internet Security הוא פתרון אבטחה שלם המשלב מקסימום הגנה עם מינימום צריכה של משאבי מערכת. הטכנולוגיות המתקדמות שלנו משתמשות בבינה מלאכותית כדי למנוע חדירות של וירוסים, תוכנות ריגול, סוסים טרויאניים, תולעים, תוכנות פרסום, תוכניות rootkit ואיומים אחרים, וכל זאת מבלי להאט את ביצועי המערכת או לפגוע במחשב.

תכונות ויתרונות

ממשק משתמש שעוצב מחדש	ממשק המשתמש בגרסה זו זכה בעיצוב מחודש ופשוט יותר משמעותית, המבוסס על תוצאות שהתקבלו בבדיקת שימושיות. כל הביטויים וההודעות בממשק המשתמש הגרפי נבדקו היטב, וכעת הממשק מעניק תמיכה בשפות הנכתבות מימין לשמאל, כגון עברית וערבית. עזרה מקוונת משולבת כעת ב-ESET Internet Security ומציעה תוכן תמיכה המתעדכן באופן דינמי.
אנטי-וירוס והגנה מפני תוכנות ריגול	זיהוי וניקוי יזומים של יותר וירוסים, תולעים, סוסים טרויאניים ותוכניות rootkits - מוכרים ולא מוכרים. היריסטיקה מתקדמת מסמנת אפילו תוכנות זדוניות שמעולם לא נראו, ובכך מגנה עליך מפני איומים לא מוכרים ומנטרלת אותם לפני שהם יכולים לגרום נזק. הגנה על גישה לאינטרנט והגנה מפני פישינג פועלות על-ידי ניטור התקשורת בין דפדפני אינטרנט ושרתים מרוחקים (לרבות SSL). הגנת לקוח דואר אלקטרוני מספקת בקרה על תקשורת דואר אלקטרוני המתקבלת באמצעות הפרוטוקולים POP3(S) ו-IMAP(S).
עדכונים סדירים	עדכון סדיר של מנגנון האיתור (לשעבר 'מסד הנתונים של חתימות הווירוסים') ושל מודולי התוכנית הוא הדרך הטובה ביותר להבטיח את רמת האבטחה המרבית למחשב שלך.
ESET LiveGrid® (מוניטין בכוח הענן)	באפשרותך לבדוק את המוניטין של תהליכים וקבצים פעילים ישירות מתוך ESET Internet Security.
בקרת התקנים	סריקה אוטומטית של כל כונני הבזק ה-USB, כרטיסי הזיכרון והתקליטורים/DVD. חסימה של מדיה נשלפת על-פי סוג המדיה, היצרן, הגודל ותכונות אחרות.
פונקציונליות HIPS	באפשרותך להתאים אישית את אופן הפעולה של המערכת בפירוט רב יותר; לציין כללים לרישום המערכת, לתהליכים ולתוכניות הפעילים, ולהתאים במדויק את מצב האבטחה.
מצב משחק	השהיית כל החלונות הקופצים, העדכונים או פעילויות אחרות שמעמיסות על המערכת כדי לשמר את משאבי המערכת למשחק ולפעילויות אחרות המתבצעות במסך מלא.

התכונות הכלולות ב- ESET Internet Security

הגנה על שירותים בנקאיים ותשלומים מקוונים	הגנה על שירותים בנקאיים ותשלומים מקוונים מספקת דפדפן מאובטח לשימוש בעת הגישה לשערי בנקאות או תשלום מקוונים, כדי להבטיח שכל העסקאות המקוונות יתבצעו בסביבה מהימנה ובטוחה.
תמיכה בחתימות רשת	חתימות רשת מאפשרות זיהוי מהיר וחסימה של תעבורה זדונית המגיעה מתוך ואל מכשירים של משתמשים, כגון מחשבי בוט וחבילות ניצול. ניתן להתייחס לתכונה כשיפור של ההגנה מפני רשת 'זומבי' (Botnet).
חומת אש חכמה	מניעת גישה של משתמשים בלתי מורשים למחשב שלך וניצול משאביך האישיים.
מסנן דואר זבל של ESET	דואר זבל מייצג עד 80 אחוזים מכלל התקשורת בדואר אלקטרוני. הגנת מסנן דואר זבל מגנה מפני בעיה זו.
'המערכת נגד גניבה' של ESET	'המערכת נגד גניבה' של ESET מרחיב את האבטחה ברמת המשתמש במקרה של מחשב שאבד או נגנב. אחרי שהמשתמשים יתקינו את ESET Internet Security ואת 'המערכת נגד גניבה' של ESET, המכשיר שלהם יירשם בממשק האינטרנט. ממשק האינטרנט מאפשר למשתמשים לנהל את התצורה של 'המערכת נגד גניבה' של ESET ולפקח כל תכונות המערכת נגד גניבה במכשיר שלהם.
בקרת הורים	הגנה על משפחתך מפני תוכן אינטרנטי שעלול להיות פוגעני על-ידי חסימת קטגוריות שונות של אתרי אינטרנט.

הפעלת כל התכונות של ESET Internet Security מצריכה רישיון פעיל. מומלץ לחדש את הרישיון מספר שבועות לפני מועד תפוגת

הרישיון של ESET Internet Security.

מה חדש בגרסה זו?

הגרסה החדשה של ESET Internet Security כוללת את השיפורים הבאים:

- **רישום ביומן בלחיצה אחת** – באפשרותך ליצור רשומות יומן מתקדמות בלחיצה אחת בלבד.
- **סורק ממשק קושחה מורחב מאוחד (UEFI)** – מוסיף רמות מוגברות של הגנה מפני תוכנות זדוניות על-ידי איתור והסרה של איומים שעלולים להיות מופעלים לפני אתחול מערכות ההפעלה. קרא עוד על סוג זה של טכנולוגיה במילון.
- **ביצועים גבוהים והשפעה נמוכה על המערכת** – גרסה זו תוכננה לשימוש יעיל במשאבי המערכת, ובכך היא מאפשרת לך ליהנות מביצועי המחשב ובמקביל להגן מפני סוגים חדשים של איומים.
- **ארגון מחדש של ההגדרות המתקדמות** – ההגדרות של ESET LiveGrid® עברו למקטע 'מנגנון איתור', הרישום המתקדם ביומן של מערכת האנטי-ספאם עברה למקטע 'אבחון' וכו'.
- **תמיכה משופרת בקורא מסך** – ESET Internet Security תומך בקוראי המסך הפופולריים ביותר (JAWS, NVDA ו-Narrator).
- **סריקת קבצים על-ידי גרירה ושחרור** – באפשרותך לסרוק קובץ או תיקיה פשוט על-ידי גרירתם לאזור המסומן.
- **הפניית מוצר של ESET לחבר**- ESET Internet Security מציע כעת בונוסים על הפניות, כך שבאפשרותך לשתף את חוויית השימוש שלך במוצר של ESET עם בני משפחה או חברים.
- ESET Internet Security מותקן כעת בפורמט קומפקטי כדי להפוך את ההתקנה למהירה יותר. לאחר ההתקנה וההפעלה של המוצר, הורדת המודולים תתחיל.
- ESET Internet Security מיידע אותך כאשר אתה מתחבר לרשת אלחוטית לא מאובטחת או לרשת עם הגנה חלשה.

לקבלת פרטים נוספים על התכונות החדשות של ESET Internet Security, קרא את המאמר הבא במאגר הידע של ESET:
מה חדש בגרסה זו של המוצרים הביתיים של ESET

איזה מוצר יש לי?

ESET מציעה מספר שכבות אבטחה עם מוצרים חדשים, החל מפתרון אנטי-וירוס מהיר ורב-עוצמה ועד לפתרון אבטחה מקיף עם טביעת רגל מזערית של המערכת:

- ESET NOD32 Antivirus
- ESET Internet Security
- ESET Smart Security Premium

כדי לקבוע איזה מוצר התקנת, פתח את חלון התוכנית הראשי (ראה מאמר במאגר הידע) ותראה את שם המוצר בחלקו העליון של החלון (בכותרת).

בטבלה שלהלן מפורטות התכונות הזמינות בכל מוצר ספציפי.

ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus	
✔	✔	✔	אנטי-וירוס
✔	✔	✔	הגנה מפני תוכנות ריגול
✔	✔	✔	חוסם קוד ניצול לרעה
✔	✔	✔	הגנה מבוססת-Script מפני מתקפות
✔	✔	✔	מערכת אנטי פישינג
✔	✔	✔	הגנת גישה לאינטרנט
✔	✔	✔	HIPS (כולל הגנה מפני נוזקות כופר)

✔	✔		אנטי-ספאם
✔	✔		חומת אש
✔	✔		בקרת רשת ביתית
✔	✔		הגנת מצלמת אינטרנט
✔	✔		הגנה מפני מתקפות רשת
✔	✔		הגנה מפני 'מחשב זומבי' (Botnet)
✔	✔		הגנה על שירותים בנקאיים ותשלומים מקוונים
✔	✔		בקרת הורים
✔	✔		מערכת נגד גניבה
✔			ESET Password Manager
✔			ESET Secure Data

הערה
ייתכן שחלק מהמוצרים לעיל לא יהיו זמינים בשפה / באזור שלך.

דרישות מערכת

על המערכת לעמוד בדרישות החומרה והתוכנה הבאות כדי ש- ESET Internet Security יפעל בצורה מיטבית:

המעבדים הנתמכים
Intel® או AMD x86-x64

מערכות ההפעלה הנתמכות
Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 SP1
Microsoft® Windows® Vista SP2
Microsoft® Windows® Home Server 2011 64-bit

הערה
'המערכת נגד גניבה' של ESET אינו תומך ב-Microsoft Windows Home Server.

מניעה

כשאתה עובד עם המחשב, ובעיקר כשאתה גולש באינטרנט, אנא זכור שאף מערכת אנטי-וירוס בעולם אינה מסוגלת למנוע באופן מלא את הסיכון לחדירות והתקפות מרוחקות. כדי לספק את מרב ההגנה והנוחות, חיוני שתשתמש בפתרון האנטי-וירוס שלך כהלכה ותקפיד על מספר כללים שימושיים:

עדכן באופן קבוע

על-פי הסטטיסטיקה של ESET LiveGrid®, מדי יום נוצרות אלפי חדירות ייחודיות חדשות כדי לעקוף את אמצעי האבטחה הקיימים ולהפיק רווחים למחבריהן והכול על חשבונם של משתמשים אחרים. המומחים במעבדת המחקר של ESET מנתחים איומים אלה על-בסיס יומיומי, ומכינים ומפיצים עדכונים כדי לשפר בהתמדה את רמת ההגנה של משתמשינו. כדי להבטיח את מרב היעילות של העדכונים הללו, חשוב שהעדכונים יוגדרו כהלכה במערכת שלך. לקבלת מידע נוסף על אופן ההגדרה של עדכונים עיין בסעיף הגדרות העדכון.

הורד תיקוני אבטחה

לעתים קרובות, המחברים של תוכנות זדוניות מנצלים פגיעויות מערכת שונות כדי להגביר את יעילות ההתפשטות של קוד זדוני. לאור זאת, חברות תוכנה בוחנות מקרוב את כל הפגיעויות ביישומים שלהן כדי לזהותן ולהפיץ עדכוני אבטחה שימזערו את האיומים הפוטנציאליים באופן קבוע. חשוב להוריד את עדכוני האבטחה הללו מיד עם הפצתם. Microsoft Windows ודפדפני אינטרנט כגון Internet Explorer הם שתי דוגמאות לתוכנית שעבורן מופצים עדכוני אבטחה באופן קבוע.

גבה נתונים חשובים

בדרך-כלל, מחברי תוכנות זדוניות אינם מגלים אכפתיות לצרכים של המשתמשים ופעילות התוכניות הזדוניות לרוב מובילה להיעדר תפקוד כולל של מערכת ההפעלה ולאובדן נתונים חשובים. חשוב לגבות באופן קבוע את הנתונים החשובים והרגישים במקור חיצוני, כגון DVD או כונן קשיח חיצוני. במקרה של כשל במערכת, פעולה זו תאפשר לשחזר את נתוניך ביתר קלות ומהירות.

סרוק את המחשב באופן קבוע לאיתור וירוסים

זיהוי וירוסים, תולעים, סוסים טרויאניים ותוכניות rootkit, מוכרים יותר או פחות, מתבצע באמצעות מודול ההגנה על מערכת קבצים בזמן אמת. המשמעות היא שבכל פעם שאתה ניגש לקובץ מסוים או פותח אותו, הקובץ נסרק לאיתור פעילות זדונית. מומלץ שתפעיל סריקת מחשב מלאה לפחות אחת לחודש, מפני שחתימות של תוכנות זדוניות עשויות להשתנות ומנגנון האיתור מעדכן את עצמו מדי יום.

פעל על-פי כללי האבטחה הבסיסיים

זהו הכלל השימושי והיעיל ביותר מכולם: היזהר תמיד. כיום, חדירות רבות מצריכות התערבות של המשתמש כדי לפעול ולהפיץ עצמן. אם תהיה זהיר בעת פתיחת קבצים חדשים, תחסוך לעצמך זמן ומאמצים ניכרים שאחרת היו מתבזבזים על ניקוי חדירות. להלן מספר הנחיות שימושיות:

- אל תבקר באתרי אינטרנט חשודים שבהם מספר חלונות קופצים ופרסומות מהבהבות.
- היזהר בעת התקנת תוכניות חופשיות, חבילות codec, וכו'. השתמש רק בתוכניות בטוחות ובקר רק באתרי אינטרנט בטוחים.
- שמור על ערנות בעת פתיחת קבצים המצורפים לדואר אלקטרוני, במיוחד כאלה המגיעים בהודעות שנשלחות לנמענים רבים והודעות משולחים לא מוכרים.
- אל תשתמש בחשבון מנהל מערכת בעבודה היומיומית עם המחשב.

דפי עזרה

ברוך הבא למדריך למשתמש של ESET Internet Security. המידע המופיע כאן יסייע לך להכיר את המוצר ולהפוך את המחשב שלך לבטוח יותר.

תחילת העבודה

לפני שתשתמש ב-ESET Internet Security, מומלץ שתכיר את סוגי החדירות וההתקפות המרוחקות שבהם אתה עשוי להיתקל בעת השימוש במחשב.

הכנו גם רשימה של תכונות חדשות שנוספו ל- ESET Internet Security, ומדריך שיסייע לך לקבוע את תצורת ההגדרות הבסיסיות.

כיצד להשתמש בדפי העזרה של ESET Internet Security

נושאי העזרה מחולקים למספר פרקים ותתי-פרקים. הקש **F1** כדי להציג מידע על החלון שבו אתה נמצא כעת.

התוכנית מאפשרת לך לחפש נושא עזרה לפי מילות מפתח, או לחפש תוכן על-ידי הקלדת מילים או ביטויים. ההבדל בין שתי השיטות הללו הוא שלמילת מפתח עשוי להיות קשר לוגי לדפי עזרה שהטקסט שלהם אינו כולל את אותה מילת מפתח. חיפוש לפי מילים וביטויים יחפש בתוכן של כל הדפים ויציג רק את אלה שהטקסט שלהם כולל את המילה או הביטוי שחיפשת.

כדי לשמור על עקביות ולעזור למנוע בלבול, המינוח שבו משתמש מדריך זה מבוסס על שמות הפרמטרים של ESET Internet Security. אנו משתמשים גם במערכת סמלים אחידה כדי להדגיש נושאים בעלי עניין או משמעות מיוחדים.

הערה

הערה היא נקודה קצרה להסבת תשומת לב. אמנם באפשרותך להסירן, אך ההערות יכולות לספק מידע בעל ערך, כגון תכונות מיוחדות או קישור לנושא קשור כלשהו.

חשוב

נושא זה דורש את תשומת לבך ומומלץ לא לדלג עליו. בדרך-כלל הוא נותן מידע לא קריטי אך משמעותי.

אזהרה

זהו מידע שמצריך יתר תשומת לב וזהירות. אזהרות ממוקמות ספציפית כדי למנוע ממך לבצע טעויות שעלולות לגרום נזק. אנא קרא והבן את הטקסטים לאזהרה שבסוגריים המרובעים, מאחר שהם מתייחסים להגדרות מערכת רגישות ביותר או לנושא מסוכן.

דוגמה

זהו מקרה שימוש או דוגמה שימושית שמטרתם לסייע לך להבין כיצד ניתן להשתמש בפונקציה או בתכונה מסוימות.

משמעות	מוסכמה
שמות של פריטי ממשק, כגון תיבות ולחצני אפשרויות.	**הקלדה מודגשת**
סמלים כלליים למידע שאתה מספק. לדוגמה, שם קובץ או נתיב פירושו שאתה מקליד את הנתיב או את שם הקובץ בפועל.	*הקלדה נטויה*
דוגמאות קוד או פקודות.	Courier New
נותן גישה קלה ומהירה לנושאים שהנושא מתייחס אליהם או למיקום חיצוני באינטרנט. היפר-קישורים מודגשים בכחול ועשויים להיות מסומנים גם בקו תחתון.	היפר-קישור
ספריית המערכת של Windows, בה מאוחסנות התוכניות המותקנות ב- Windows.	*%ProgramFiles%*

עזרה מקוונת היא המקור העיקרי לתוכן עזרה. הגירסה העדכנית ביותר של העזרה המקוונת תוצג אוטומטית כשאתה מחובר לאינטרנט.

התקנה

יש מספר שיטות להתקין את ESET Internet Security במחשב. שיטות ההתקנה עשויות להשתנות בהתאם למדינה ולאמצעי ההפצה:

- את Live installer ניתן להוריד מאתר האינטרנט של ESET. חבילת ההתקנה היא אוניברסלית לכל השפות (בחר שפה מבוקשת). Live installer עצמו הוא קובץ קטן; ההורדה של קבצים נוספים שנדרשים להתקנת ESET Internet Security תתבצע אוטומטית.

- התקנה לא מקוונת – סוג ההתקנה הזה נמצא בשימוש כאשר מתקינים באמצעות תקליטור/DVD של המוצר. הוא משתמש בקובץ *.exe*, אשר גדול יותר מקובץ ה-Live installer ואינו מצריך חיבור לאינטרנט או קבצים נוספים כדי שההתקנה תושלם.

חשוב

לפני שתתקין את ESET Internet Security ודא שלא מותקנות במחשב שלך תוכניות אנטי-וירוס אחרות. שני פתרונות אנטי-וירוס או יותר המותקנים באותו מחשב עלולים להתנגש זה עם זה. מומלץ להסיר את ההתקנה של כל תוכנית האנטי-וירוס האחרות במערכת. עיין במאמר במאגר הידע של ESET לקבלת רשימה של כלי הסרת ההתקנה של תוכנות אנטי-וירוס נפוצות (זמינה באנגלית ובמספר שפות נוספות).

Live installer

אחרי שהורדת את חבילת ההתקנה של Live installer, לחץ לחיצה כפולה על קובץ ההתקנה ופעל על-פי ההוראות המפורטות שב-Installer Wizard.

חשוב

בסוג ההתקנה הזה עליך להיות מחובר לאינטרנט.

1. בחר את השפה הרצויה בתפריט הנפתח ולחץ על **המשך**. המתן מספר דקות להורדת קובצי ההתקנה.

2. קרא וקבל את **הסכם הרישיון למשתמש קצה**.

3. השלב הבא הוא לבחור אפשרות הפעלה. אם אתה מתקין גרסה חדשה יותר במקום הגרסה הקודמת, מפתח הרישיון שלך יוזן אוטומטית.

4. בחר את ההעדפה שלך למערכת המשוב של ESET LiveGrid® ולזיהוי אפליקציות העלולות להיות לא רצויות. תוכנות אפורות או אפליקציות העלולות להיות לא רצויות (PUA) היא קטגוריה רחבה של תוכנות, שכוונתן אינה בהכרח זדונית כמו עם סוגים אחרים של תוכנות זדוניות, כגון וירוסים וסוסים טרויאניים. עיין בפרק אפליקציות העלולות להיות לא רצויות לפרטים נוספים.

5. בחר את ההעדפה שלך להשתתפות בתכנית לשיפור חוויית הלקוח. בעצם ההצטרפות אל התכנית לשיפור חוויית הלקוח אתה מספק ל-ESET מידע אנונימי בנוגע לשימוש במוצרים שלנו. הנתונים שייאספו יסייעו לנו בשיפור החוויה שאנו מספקים לך ולעולם לא נשתף אותם עם גורמי צד שלישי. איזה מידע אנו אוספים?

6. לחץ על **התקן** כדי להתחיל בתהליך ההתקנה. פעולה זו עשויה להימשך מספר רגעים.

7. לחץ על **סיום** כדי לצאת מאשף ההתקנה.

הערה

לאחר ההתקנה וההפעלה של המוצר, הורדת המודולים תתחיל. ההגנה תאותחל וייתכן שחלק מהתכונות לא יתפקדו במלואן לפני השלמת ההורדה.

הערה

אם יש ברשותך רישיון שמאפשר לך להתקין גרסאות אחרות של המוצר, תוכל לבחור מוצר בהתאם להעדפותיך. לקבלת מידע נוסף על התכונות בכל מוצר ספציפי, לחץ כאן.

התקנה לא מקוונת

אחרי שתפעיל את ההתקנה הלא מקוונת (.exe), אשף ההתקנה ינחה אותך לאורך התהליך.

1. בחר את השפה הרצויה בתפריט הנפתח ולחץ על **המשך**. המתן מספר דקות להורדת קובצי ההתקנה.

2. קרא וקבל את **הסכם הרישיון למשתמש קצה**.

3. השלב הבא הוא לבחור אפשרות הפעלה. אם אתה מתקין גרסה חדשה יותר במקום הגרסה הקודמת, מפתח הרישיון שלך יוזן אוטומטית.

4. בחר את ההעדפה שלך למערכת המשוב של ESET LiveGrid® ולזיהוי אפליקציות העלולות להיות לא רצויות. תוכנות אפורות או אפליקציות העלולות להיות לא רצויות (PUA) היא קטגוריה רחבה של תוכנות, שכוונתן אינה בהכרח זדונית כמו עם סוגים אחרים של תוכנות זדוניות, כגון וירוסים וסוסים טרויאניים. עיין בפרק אפליקציות העלולות להיות לא רצויות לפרטים נוספים.

5. בחר את ההעדפה שלך להשתתפות בתכנית לשיפור חוויית הלקוח. בעצם ההצטרפות אל התכנית לשיפור חוויית הלקוח אתה מספק ל-ESET מידע אנונימי בנוגע לשימוש במוצרים שלנו. הנתונים שייאספו יסייעו לנו בשיפור החוויה שאנו מספקים לך ולעולם לא נשתף אותם עם גורמי צד שלישי. איזה מידע אנו אוספים?

6. לחץ על **התקן** כדי להתחיל בתהליך ההתקנה. פעולה זו עשויה להימשך מספר רגעים.

7. לחץ על **סיום** כדי לצאת מאשף ההתקנה.

> **הערה**
> לאחר ההתקנה וההפעלה של המוצר, הורדת המודולים תתחיל. ההגנה תאותחל וייתכן שחלק מהתכונות לא יתפקדו במלואן לפני השלמת ההורדה.

> **הערה**
> אם יש ברשותך רישיון שמאפשר לך להתקין גרסאות אחרות של המוצר, תוכל לבחור מוצר בהתאם להעדפותיך. לקבלת מידע נוסף על התכונות בכל מוצר ספציפי, לחץ כאן.

הפעלת מוצר

ישנן מספר שיטות להפעלת המוצר. הזמינות של תרחיש הפעלה מסוים בחלון ההפעלה עשויה להשתנות בתלות במדינה ובאמצעי ההפצה (תקליטור/DVD, דף אינטרנט של ESET, וכו'):

- אם רכשת גרסה ארוזה של המוצר מקמעונאי, הפעל את המוצר על-ידי לחיצה על **הזן מפתח רישיון**. מפתח הרישיון לרוב ממוקם בתוך אריזת המוצר או בחלקה האחורי. את מפתח הרישיון יש להזין בדיוק כפי שסופק כדי שההפעלה תצליח. מפתח

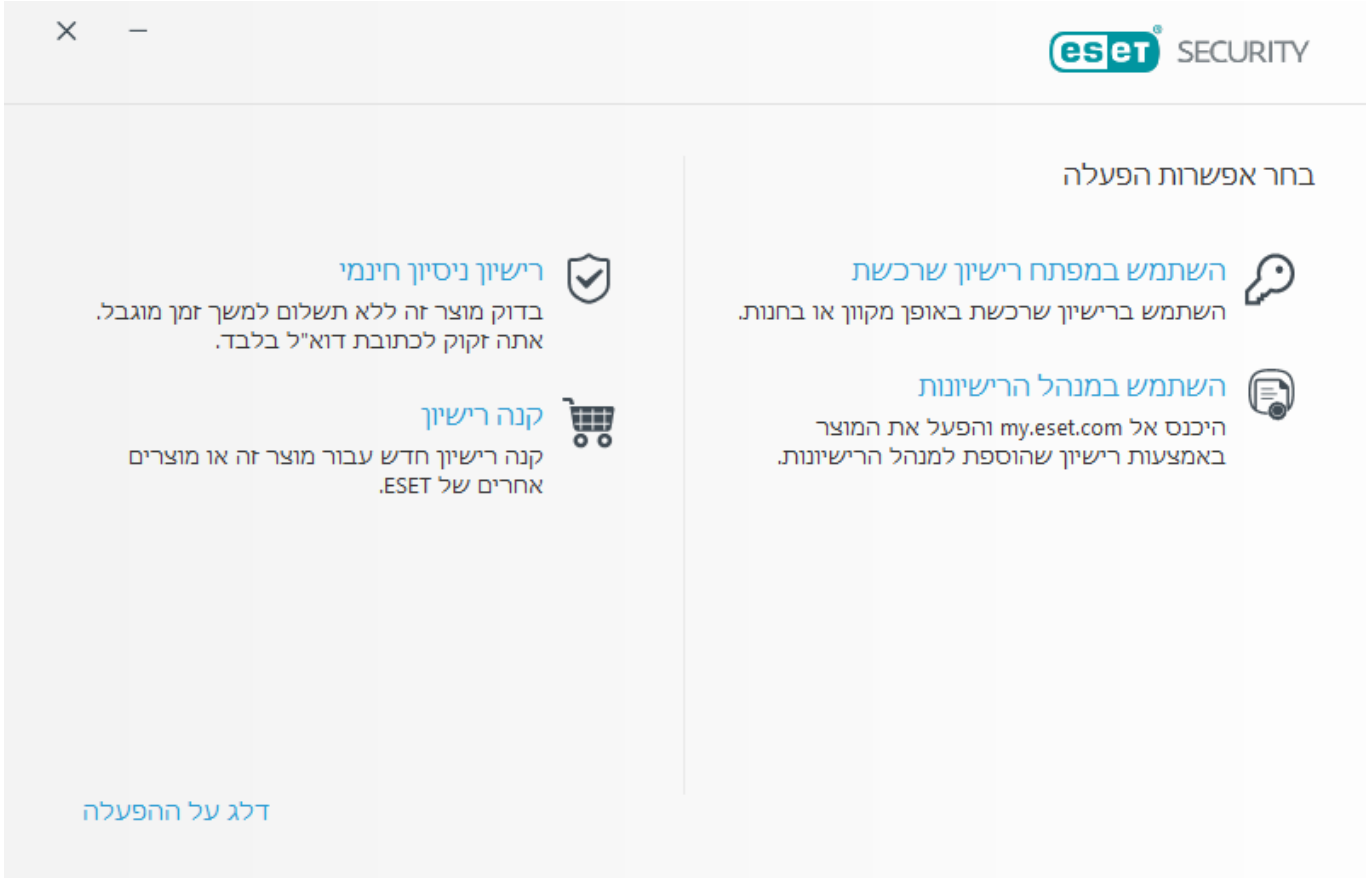
רישיון – מחרוזת ייחודית בתבנית של XXXX-XXXX-XXXX-XXXX-XXXX או XXXX-XXXXXXXX, אשר משמשת לזיהוי בעלי הרישיון ולהפעלת הרישיון.

- לאחר בחירה באפשרות **השתמש במנהל הרישיונות** תתבקש לספק את אישורי my.eset.com בחלון חדש.
- אם ברצונך לנסות את ESET Internet Security לפני רכישה, בחר **גרסת ניסיון חינם**. הזן את כתובת הדואר האלקטרוני שלך ואת ארצך כדי להפעיל את ESET Internet Security לפרק זמן מוגבל. רישיון הניסיון יישלח אליך בדואר אלקטרוני. כל לקוח יכול להפעיל את רישיון גרסת הרישיון פעם אחת בלבד.

- אם אין לך רישיון וברצונך לרכוש אחד, לחץ על 'קנה רישיון'. פעולה זו תעביר אותך לאתר האינטרנט של מפיץ ESET באזורך. הרישיונות המלאים של המוצרים הביתיים של ESET עבור Windows אינם ניתנים ללא תשלום.

ניתן לשנות את רישיון המוצר בכל עת. לשם כך, לחץ על **עזרה ותמיכה** > **שנה רישיון** בחלון התוכנית הראשי. תראה את מזהה הרישיון הציבורי המשמש לזהות את הרישיון שלך מול התמיכה של ESET.

אם יש לך שם משתמש וסיסמה ששימשו להפעלת מוצרי ESET ישנים יותר ואינך יודע כיצד להפעיל את ESET Internet Security, המר את האישורים מדור קודם למפתח רישיון.



הזנת מפתח הרישיון שלך במהלך ההפעלה

עדכונים אוטומטיים חשובים לבטיחותך. ESET Internet Security יקבל עדכונים רק לאחר שיופעל באמצעות **מפתח הרישיון** שלך.

אם לא תזין את מפתח הרישיון שלך לאחר ההתקנה, המוצר לא יופעל. תוכל להחליף את הרישיון בחלון התוכנית הראשי. לשם כך, לחץ על **עזרה ותמיכה** > **הפעל רישיון** והזן את נתוני הרישיון שקיבלת עם מוצר האבטחה של ESET לחלון הפעלת המוצר.

הרישיונות המלאים של המוצרים הביתיים של ESET עבור Windows אינם ניתנים ללא תשלום.

בעת הזנת **מפתח הרישיון** שלך, חשוב להקלידו בדיוק כפי שנכתב:

- מפתח הרישיון שלך הוא מחרוזת ייחודית בתבנית של XXXX-XXXX-XXXX-XXXX-XXXX אשר משמשת לזיהוי בעלי הרישיון ולהפעלת הרישיון.

להבטחת הדיוק, מומלץ שתעתיק ותדביק את מפתח הרישיון שלך מהודעת הדואר האלקטרוני של ההרשמה.

שימוש במנהל הרישיונות

לאחר בחירה באפשרות **השתמש במנהל הרישיונות** תתבקש לספק את אישורי my.eset.com בחלון חדש. הזן את אישורי my.eset.com שלך ולחץ על **כניסה** כדי להשתמש ברישיון ב-ESET License Manager. בחר רישיון להפעלה, לחץ על **המשך** ו-ESET Internet Security יופעל.

הערה

אם אין לך עדיין חשבון my.eset.com, הירשם על-ידי לחיצה הלחצן **צור חשבון**.

הערה

אם שכחת את הסיסמה, לחץ על **שכחתי את הסיסמה** ופעל בהתאם להנחיות בדף האינטרנט שאליו תנותב.

ESET License Manager מסייע לך בניהול כל רישיונות ESET שברשותך. תוכל לחדש, לשדרג או להאריך בקלות את הרישיון שלך ולראות את פרטי הרישיון החשובים. תחילה, הזן את מפתח הרישיון שלך. לאחר מכן, תראה את המוצר, ההתקן המשויך, מספר העמדות הזמינות ותאריך התפוגה. באפשרותך לבטל את ההפעלה או לשנות את השם של התקנים ספציפיים. כאשר תלחץ על **חידוש**, תנותב לחנות המקוונת שבה תוכל לאשר את הרכישה ולקנות את החידוש.

אם ברצונך לשדרג את הרישיון (לדוגמה מ-ESET NOD32 Antivirus ל-ESET Smart Security Premium) או שברצונך להתקין מוצר אבטחה של ESET בהתקן אחר, תנותב לחנות המקוונת כדי להשלים את הרכישה.

ב-ESET License Manager תוכל גם להוסיף רישיונות שונים, להוריד מוצרים להתקנים שלך או לשתף רישיונות באמצעות דוא"ל

הפעלת רישיון של גרסת ניסיון

הזן את שמך ואת כתובת הדואר האלקטרוני שלך כדי להפעיל את גרסת הניסיון של ESET Internet Security. את גרסת הניסיון ניתן להפעיל פעם אחת בלבד.

בחר את ארצך בתפריט הנפתח **מדינה** כדי לרשום את ESET Internet Security אצל המפיץ המקומי, אשר יספק לך תמיכה טכנית.

הזן כתובת דואר אלקטרוני חוקית בשדה **כתובת דואר אלקטרוני**. לאחר ההפעלה ייווצרו שם המשתמש והסיסמה שלך, הנדרשים לעדכון של ESET Internet Security, ויישלחו אליך בדואר אלקטרוני. כתובת דואר אלקטרוני זו תשמש גם להעברת הודעות על תפוגת תוקף המוצר ומסרים אחרים מאת ESET.

מפתח רישיון של ESET ללא תשלום

הרישיונות המלאים של המוצרים הביתיים של ESET עבור Windows אינם ניתנים ללא תשלום.

מפתח רישיון של ESET הוא רצף ייחודי של סמלים, אותיות, מספרים או סימנים מיוחדים שסופק על-ידי ESET על מנת לאפשר שימוש חוקי ב-ESET Internet Security בהתאם ל[הסכם הרישיון למשתמש קצה]. כל משתמש קצה רשאי להשתמש במפתח הרישיון רק עד למידה שבה יש לו את הזכות להשתמש ב-ESET Internet Security בהתאם למספר הרישיונות שהוענקו על-ידי ESET. מפתח הרישיון נחשב לסודי והוא אינו ניתן לשיתוף.

ישנם מקורות באינטרנט שעשויים לספק לך מפתחות רישיון של ESET "ללא תשלום", אבל זכור:

- לחיצה על פרסומת של "רישיון של ESET ללא תשלום" עלולה לחשוף את המחשב או ההתקן שלך לסיכון ועלולה לגרום להדבקתם בתוכנה זדונית. תוכנה זדונית עלולה להיות מוסתרת בסרטונים לא רשמיים של YouTube, באתרי אינטרנט המציגים פרסומות כדי להרוויח כסף בהתבסס על הביקורים שלך וכו'. לרוב, מקורות אלה הם מלכודת.
- ESET יכולה להשבית רישיונות פיראטיים ואף עושה זאת.
- החזקת מפתח רישיון פיראטי אינה עומדת בתנאים של [הסכם הרישיון למשתמש קצה] שאותם עליך לקבל כדי להתקין את ESET Internet Security.
- קנה רישיונות של ESET רק באמצעות ערוצים רשמיים כדוגמת www.eset.com, מפיצים של ESET או משווקים (אל תקנה רישיונות מאתרים לא-רשמיים של גורמי צד שלישי כגון eBay או רישיונות משותפים מצד שלישי).

- הורדת מוצר ביתי של ESET עבור Windows אינה כרוכה בתשלום, אך ההפעלה במהלך ההתקנה דורשת מפתח רישיון חוקי של ESET (ניתן להוריד את המוצר ולהתקין אותו, אך הוא לא יפעל ללא הפעלה)
- אל תשתף את הרישיון שלך באינטרנט או במדיה החברתית (כדי למנוע את הפצתו).

כדי לזהות רישיון פיראטי של ESET ולדווח עליו, בקר במאמר מאגר הידע שלנו לקבלת הוראות.

אם אינך בטוח לגבי רכישת מוצר אבטחה של ESET, תוכל להשתמש בגרסת ניסיון שתאפשר לך בינתיים:

1. להפעיל את ESET Internet Security באמצעות רישיון ניסיון ללא תשלום

2. להשתתף בתוכנית הביתא של ESET

3. להתקין את ESET Mobile Security אם אתה משתמש בהתקן נייד מסוג Android. מוצר זה הוא מוצר מסוג Freemium.

כדי לקבל הנחה / להאריך את הרישיון שלך:

- הפנה את ESET Internet Security לחבר
- חדש את הרישיון של ESET (אם היה לך רישיון פעיל קודם לכן) או הפעל אותו למשך זמן ארוך יותר

בעיות התקנה נפוצות

אם מתרחשות בעיות במהלך ההתקנה, עיין ברשימת שגיאות ההתקנה הנפוצות והפתרונות כדי למצוא פתרון לבעיה.

ההפעלה נכשלה

במקרה שהפעלת ESET Internet Security לא הצליחה, התרחישים האפשריים הנפוצים ביותר הם:

- מפתח הרישיון כבר נמצא בשימוש
- מפתח רישיון לא חוקי. שגיאה בטופס הפעלת מוצר
- מידע נוסף שנדרש לצורך ההפעלה חסר או לא חוקי
- התקשורת עם מסד הנתונים של ההפעלה נכשלה. אנא נסה להפעיל שוב בעוד 15 דקות
- אין חיבור או שהחיבור בושבת לשרתי הפעלת ESET, למידע נוסף ראה יציאות וכתובות הנדרשות לשימוש במוצר ESET שלך עם חומת אש של צד שלישי

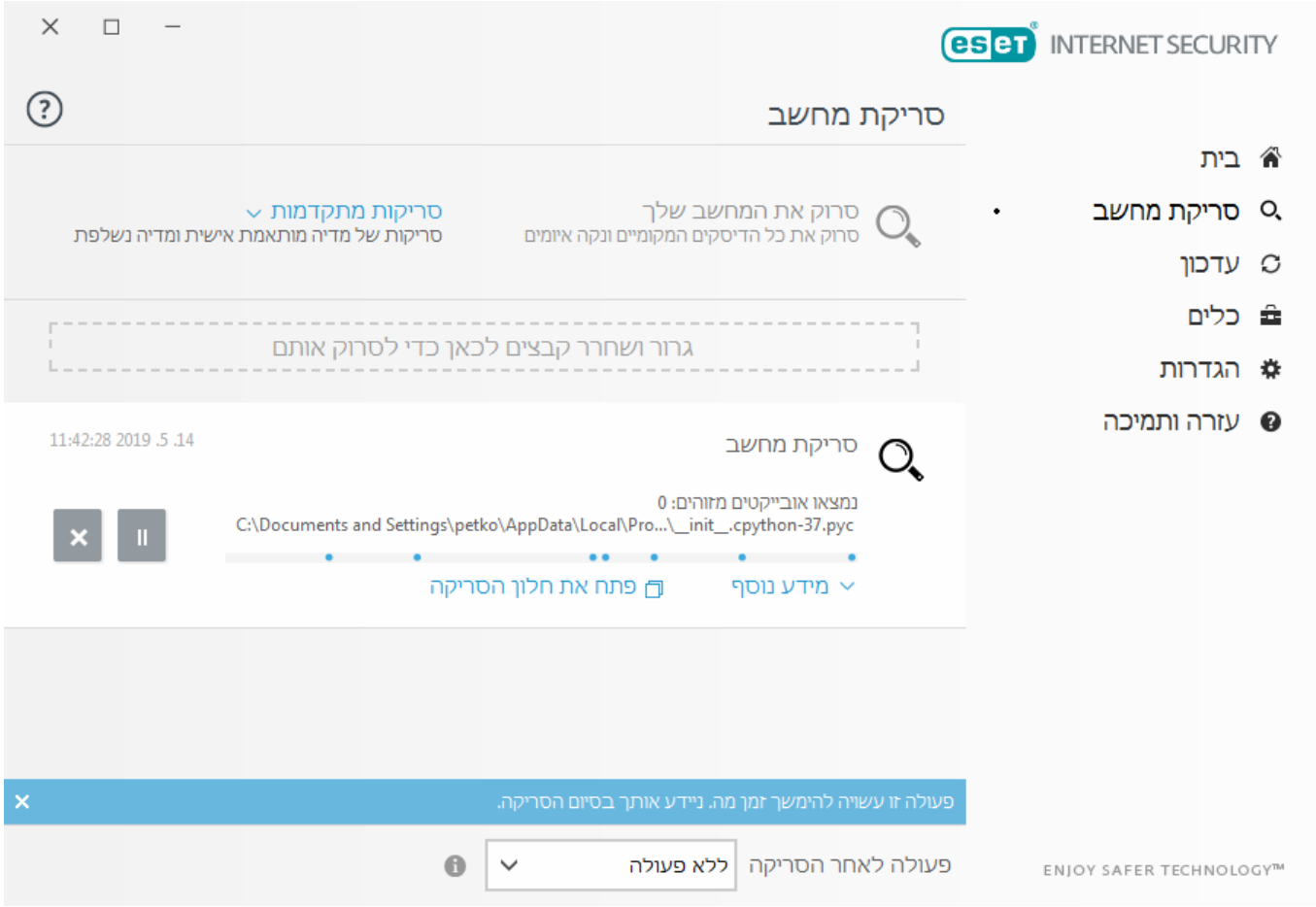
ודא שהזנת את מפתח הרישיון המתאים ונסה לבצע שוב את ההפעלה.

אם אין לך אפשרות לבצע הפעלה, קרא את פתרון שגיאות ACT או ECP במהלך ההפעלה.

סריקה ראשונה לאחר ההתקנה

לאחר התקנת ESET Internet Security, סריקה של המחשב תתחיל אוטומטית לאחר העדכון המוצלח הראשון כדי לחפש קודים זדוניים.

תוכל גם להפעיל סריקה של המחשב באופן ידני, דרך חלון התוכנית הראשי, על-ידי לחיצה על **סריקת מחשב** > **סרוק את המחשב שלך**. לקבלת מידע נוסף על סריקות מחשבים עיין בסעיף סריקת מחשב.



שדרוג לגרסה עדכנית יותר

גרסאות חדשות של ESET Internet Security יוצאות כדי לממש שיפורים או לתקן בעיות שלא ניתן לזהותן באמצעות עדכונים אוטומטיים של מודולי התוכנית. שדרוג לגרסה עדכנית יותר ניתן לבצע במספר דרכים:

1. אוטומטית, באמצעות עדכון תוכנית.
מאחר ששדרוג התוכנית מופץ לכל המשתמשים ועשוי להשפיע על תצורות מערכת מסוימות, הוא יוצא לאחר תקופת בדיקה ממושכת כדי להבטיח תפקוד עם כל תצורות המערכת האפשריות. אם עליך לשדרג לגרסה חדשה יותר מיד לאחר ההפצה, השתמש באחת מהשיטות הבאות.
ודא שאפשרת את **עדכון אפליקציות** ב**הגדרות מתקדמות** (F5) > **עדכון**.

2. ידנית, בחלון התוכנית הראשי, בלחיצה על **חפש עדכונים** במקטע **עדכון**.

3. ידנית, על-ידי הורדה ו[התקנה של גרסה חדשה יותר] שתחליף את הקודמת.

לקבלת מידע נוסף והנחיות מאוירות ראה:

- [עדכון מוצרי ESET – חיפוש מודולי המוצר העדכניים ביותר]
- [מהם סוגי העדכונים והמהדורות השונים של מוצרי ESET?]

הפניית מוצר של ESET לחבר

גרסה זו של ESET Internet Security מציעה כעת בונוסים על הפניות, כך שבאפשרותך לשתף את חוויית השימוש שלך במוצר של ESET עם בני משפחה או חברים. תוכל אפילו לשתף הפניות מתוך מוצר שהופעל באמצעות רישיון של גרסת ניסיון. כאשר אתה משתמש בגרסת ניסיון, עבור כל הפניה מוצלחת שתשלח שתתבטא בהפעלת מוצר, גם אתה וגם החבר תיהנו מהארכה של רישיון גרסת הניסיון.

תוכל לבצע הפניה באמצעות ESET Internet Security שהתקנת. המוצר שאותו באפשרותך להפנות תלוי במוצר שממנו אתה מבצע את ההפניה. עיין בטבלה להלן.

המוצר שאותו באפשרותך להפנות	המוצר המותקן
ESET Internet Security	ESET NOD32 Antivirus
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

הפניית מוצר

כדי לשלוח קישור הפניה, לחץ על **הפנה חבר** בתפריט הראשי של ESET Internet Security. לחץ על **שתף קישור הפניה**. המוצר ייצר קישור הפניה שיוצג בחלון חדש. העתק את הקישור ושלח אותו לחברים ולבני המשפחה שלך. תוכל לשתף את קישור ההפניה ישירות מתוך המוצר של ESET באמצעות האפשרויות **שתף ב-Facebook**, **הפנה את אנשי הקשר שלך ב-Gmail** ו**שתף ב-Twitter**.

כאשר החבר שלך ילחץ על קישור ההפניה ששלחת אליו, הוא ינותב לדף אינטרנט שבו הוא יוכל להוריד את המוצר ולהשתמש בו למשך חודש נוסף של הגנה ללא תשלום. כמשתמש בגרסת ניסיון, תקבל הודעה על כל קישור הפניה שהופעל בהצלחה והרישיון שלך יורחב באופן אוטומטי למשך חודש נוסף של הגנה ללא תשלום. כך תוכל להאריך את ההגנה שלך ללא תשלום בעד חמישה חודשים. באפשרותך לבדוק את מספר קישורי ההפניה שהופעלו בהצלחה בחלון **הפנה חבר** שבמוצר של ESET.

מדריך למשתמש המתחיל

פרק זה מעניק סקירה כללית על המוצר ESET Internet Security ועל הגדרותיו הבסיסיות.

חלון התוכנית הראשי

חלון התוכנית הראשי של ESET Internet Security מחולק לשני מקטעים עיקריים. החלון הראשי מימין מציג מידע התואם לאפשרות שנבחרה בתפריט הראשי שמשמאל.

להלן תיאור האפשרויות בתפריט הראשי:

דף הבית – מספק מידע על סטטוס ההגנה של ESET Internet Security.

סריקת מחשב – הגדרה והפעלה של סריקת המחשב או יצירת סריקה מותאמת אישית.

עדכון – הצגת מידע על עדכונים של מנגנון האיתור.

כלים – אספקת גישה לקובצי היומן, סטטיסטיקה ההגנה, צפייה בפעילות, תהליכים פועלים, חיבורי רשת, (בקרת רשת ביתית, הגנה על בנקאות ותשלומים, Anti-Theft ב'כלים נוספים'), מתזמן, ESET SysInspector ו-ESET SysRescue. לקבלת מידע נוסף על כלים, עיין בפרק כלים ב-ESET Internet Security.

הגדרות – בחר באפשרות זו כדי להתאים את רמת האבטחה של המחשב, האינטרנט, ההגנה על הרשת וכלי האבטחה..

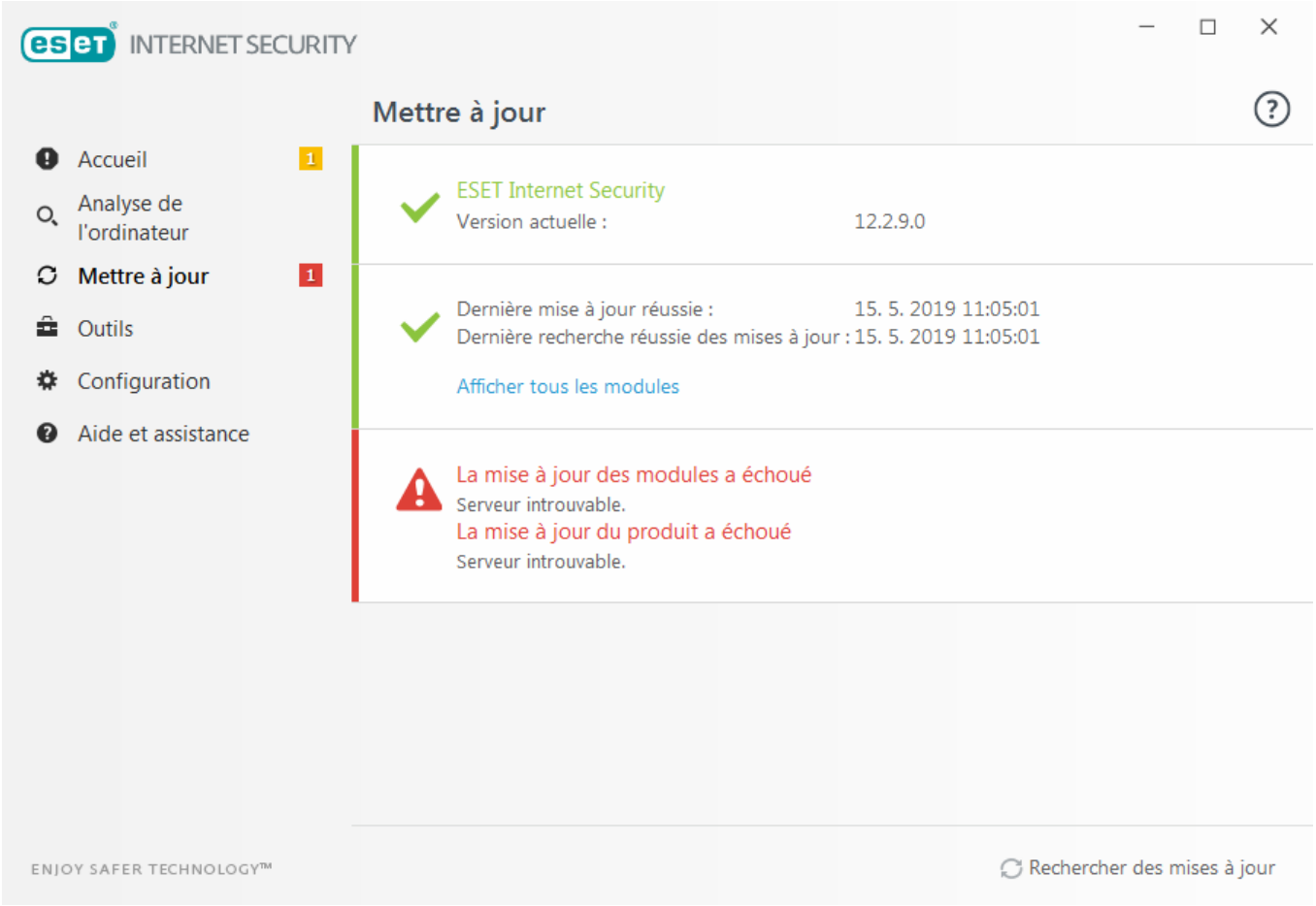
עזרה ותמיכה – גישה לקובצי עזרה, למאגר הידע של ESET, לאתר האינטרנט של ESET, וקישורים לשליחת בקשת תמיכה.

המסך **דף הבית** כולל מידע חשוב על רמת ההגנה הנוכחית של המחשב שלך. חלון הסטטוס מציג תכונות נפוצות בשימוש ב-ESET Internet Security. כאן תוכל למצוא גם מידע על העדכון החדש ביותר ותאריך התפוגה של התוכנית שלך.

הסמל הירוק והסטטוס **הגנה מרבית** הירוק מציין שמובטחת הגנה מרבית.

מה לעשות כשהתוכנית אינה פועלת כראוי?

כאשר מודול הגנה פעיל עובד כהלכה, סמל סטטוס ההגנה שלו ירוק. סימן קריאה אדום או סמל התראה כתום מציינים שלא ניתן להבטיח הגנה מרבית. מידע נוסף על סטטוס ההגנה של כל אחד מהמודולים, וכן הצעות לפתרונות לשחזור הגנה מלאה, יוצגו תחת **בית**. כדי לשנות את הסטטוס של מודולים בודדים, לחץ על **הגדרות** ובחר את המודול הרצוי.



הסמל האדום והסטטוס 'לא ניתן להבטיח הגנה מרבית' המוצג באדום מציינים בעיות קריטיות. סטטוס זה יכול להיות מוצג מסיבות שונות, למשל:

- **המוצר אינו מופעל** – באפשרותך להפעיל את ESET Internet Security דרך **בית** על-ידי לחיצה על **הפעל מוצר** או **קנה עכשיו** תחת 'סטטוס הגנה'.
- **מנגנון האיתור אינו עדכני** – שגיאה זו תופיע לאחר מספר ניסיונות לא מוצלחים לעדכן את מסד הנתונים של חתימות הווירוסים. מומלץ שתבדוק את הגדרות העדכון. הסיבה הנפוצה ביותר לשגיאה זו היא נתוני אימות שלא הוזנו כהלכה או הגדרות חיבור שגויות.
- **אנטי-וירוס והגנה מפני תוכנות ריגול מושבתים** – באפשרותך להפעיל מחדש את ההגנה מפני וירוסים ותוכנות ריגול על-ידי לחיצה על **הפעל הגנה מפני וירוסים ותוכנות ריגול**.
- **חומת אש של ESET מושבתת** – חיווי לבעיה זו מופיע גם כהתראת אבטחה ליד הסמל **רשת** בשולחן העבודה. באפשרותך להפעיל מחדש את ההגנה על הרשת על-ידי לחיצה על **הפעל חומת אש**.
- **תוקף הרישיון פג** – מצב זה מצוין באמצעות סמל סטטוס הגנה אדום. עדכון התוכנית אינו מתאפשר אחרי שתוקף הרישיון פג. פעל בהתאם להוראות שבחלון ההתראות כדי לחדש את הרישיון.

הסמל הכתום מציין הגנה מוגבלת. לדוגמה, ייתכן שיש בעיה בעדכון התוכנית או שתוקף הרישיון שלך עומד להסתיים. סטטוס זה יכול להיות מוצג מסיבות שונות, למשל:

- **מצב משחק מופעל** – הפעלת מצב משחק מהווה סיכון אבטחה פוטנציאלי. הפעלת תכונה זו משביתה את כל החלונות הקופצים ועוצרת את כל המשימות המתוזמנות.
- **תוקף הרישיון שלך יפוג בקרוב** – מצב זה מצוין באמצעות סמל סטטוס ההגנה המציג סימן קריאה לצד שעון המערכת. אחרי שתוקף רישיונך יפוג, התוכנית לא תוכל להתעדכן וסמל סטטוס ההגנה יהפוך לאדום.

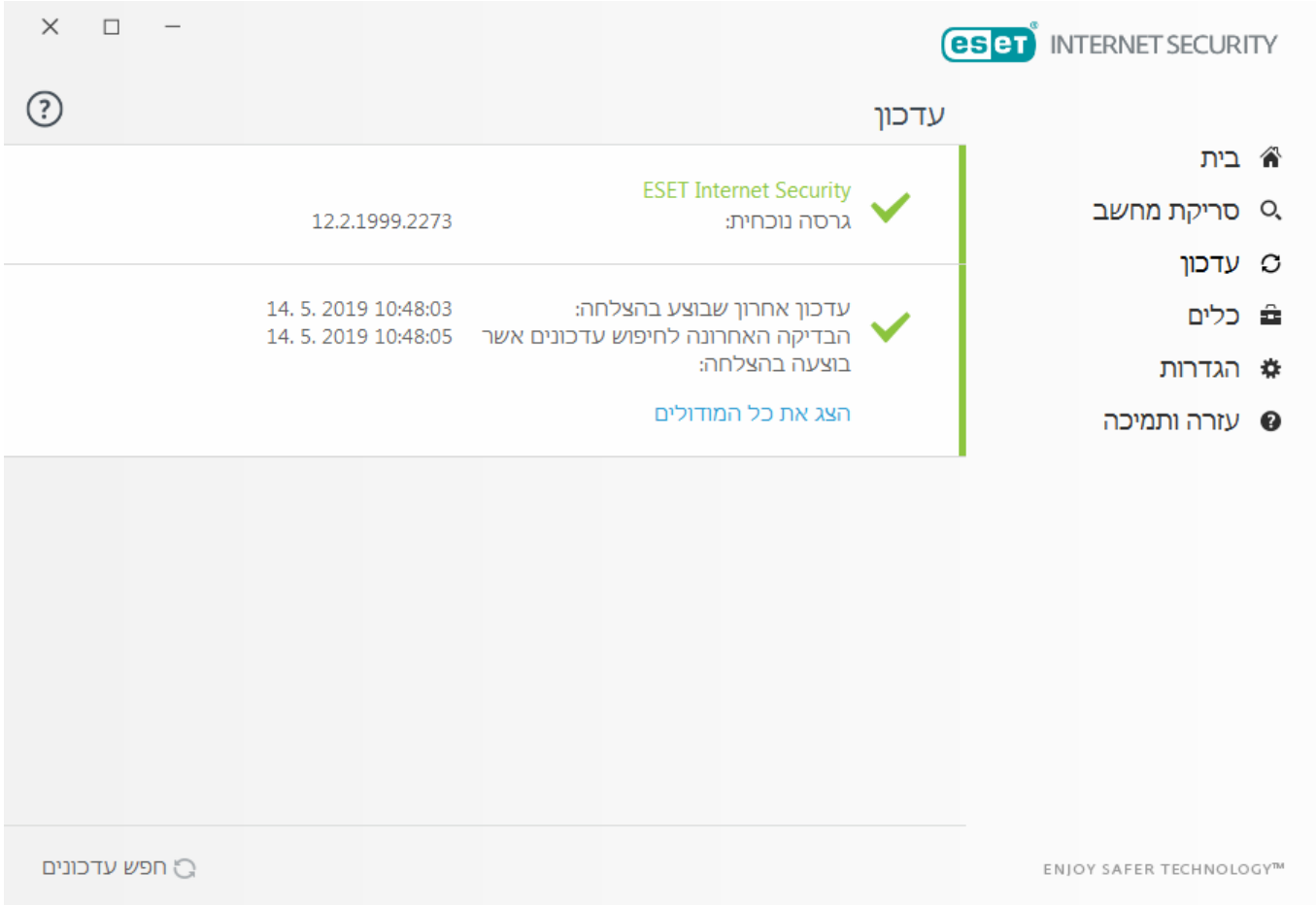
אם אינך מצליח לפתור בעיה בעזרת הפתרונות המוצעים, לחץ על **עזרה ותמיכה** כדי לגשת אל קובצי העזרה או חפש במאגר הידע של ESET. אם עדיין דרושה לך עזרה, באפשרותך לשלוח בקשת תמיכה. התמיכה הטכנית של ESET תשיב במהירות על שאלותיך ותסייע

במציאת פתרון.

עדכונים

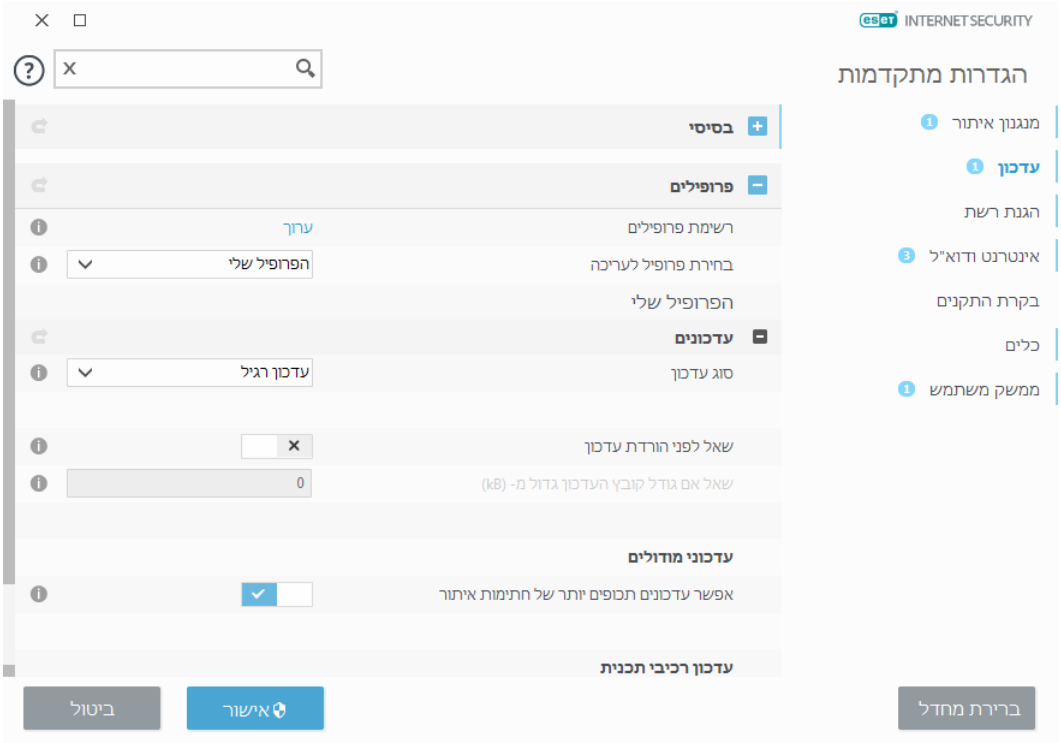
עדכון מנגנון האיתור ורכיבי התכנית הוא חלק חשוב בהגנה על המערכת מפני קוד זדוני. שים לב במיוחד לתצורה ולפעולה שלהם. בתפריט הראשי, לחץ על **עדכן** ולאחר מכן לחץ על **בדוק אם קיימים עדכונים** כדי לבדוק אם יש עדכון של מנגנון האיתור.

אם מפתח הרישיון לא הוזן במהלך ההפעלה של ESET Internet Security, תונחה לציין אותו בשלב זה.



חלון ההגדרות המתקדמות (לחץ על **הגדרות** בתפריט הראשי ולאחר מכן לחץ על **הגדרות מתקדמות**, או הקש **F5** במקלדת) מכיל אפשרויות עדכון נוספות. כדי לקבוע את התצורה של אפשרויות עדכון מתקדמות, כגון מצב עדכון, גישה לשרת proxy וחיבורי LAN, לחץ על **עדכון** בעץ ההגדרות המתקדמות.

- אם אתה נתקל בבעיות בעדכון, לחץ על **נקה** כדי לנקות את מטמון העדכון הזמני.



• אם אינך רוצה להציג את הודעת מגש המערכת בפינה השמאלית התחתונה של המסך, לחץ על **השבת הצגת התראה על עדכון שבוצע בהצלחה**.

הגדר כלי אבטחה נוספים של ESET

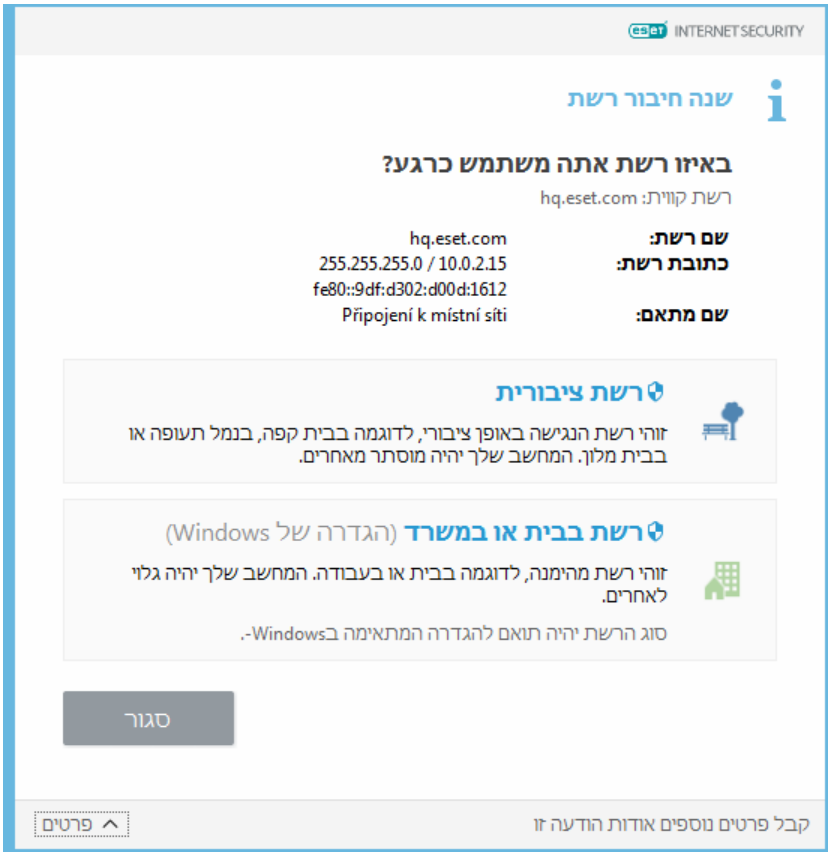
לפני התחלת השימוש ב-ESET Internet Security, מומלץ להגדיר את כלי האבטחה הנוספים כדי למקסם את ההגנה באינטרנט.

לקבלת מידע נוסף על אופן הגדרת כלי האבטחה ב-ESET Internet Security, קרא את המאמר הבא במאגר הידע של ESET.

הגדרת אזור מהימן

הגדרת אזור מהימן הכרחית כדי להגן על המחשב שלך בסביבת רשת. באפשרותך להגדיר אזורים מהימנים שיאפשרו שיתוף, ובכל לאפשר למשתמשים אחרים לגשת למחשב שלך. לחץ על **הגדרות** > **הגנה על הרשת** > **רשתות מחוברות** ואז לחץ על הקישור שמתחת לרשת המחוברת. יוצג חלון עם אפשרויות, בו תוכל לבחור את מצב ההגנה הרצוי לחשבונך ברשת.

זיהוי אזור מהימן מתבצע לאחר התקנה של ESET Internet Security ובכל פעם שמחשבך מתחבר לרשת חדשה. לפיכך, בדרך-כלל אין צורך להגדיר אזורים מהימנים. כברירת מחדל, כאשר מזוהה אזור חדש, חלון דו-שיח ינחה אותך להגדיר את רמת ההגנה לאזור זה.



אזהרה
תצורה שגויה של אזור מהימן עשויה לחשוף את המחשב שלך לסיכון אבטחה.

הערה
כברירת מחדל, תחנות עבודה מאזור מהימן מסוים מקבלות גישה לקבצים ומדפסות משותפים, תקשורת RPC נכנסת מופעלת בהן, ושיתוף שולחן עבודה מרוחק זמין בהן.

לקבלת פרטים נוספים על תכונה זו, קרא את המאמר הבא במאגר הידע של ESET:

- שנה את הגדרת חומת האש של חיבור הרשת במוצרים הביתיים של ESET עבור Windows

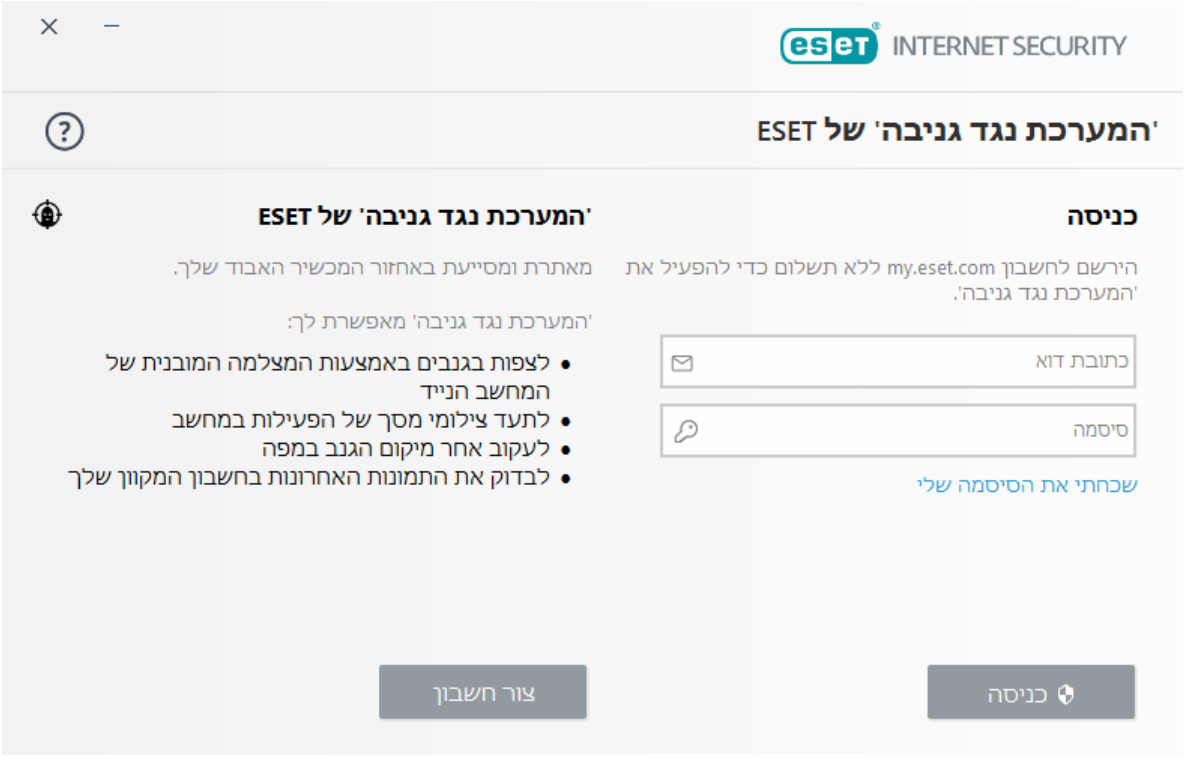
מערכת נגד גניבה

כדי להגן על המחשב במקרה של אובדן או גניבה, בחר אחת מהאפשרויות הבאות לרישום המחשב שלך ב-'המערכת נגד גניבה' של ESET.

1. לאחר הפעלה שבוצעה בהצלחה, לחץ על **הפעל מערכת נגד גניבה** כדי להפעיל את תכונות 'המערכת נגד גניבה' של ESET במחשב שזה עתה רשמת.

2. אם מופיעה ההודעה **'המערכת נגד גניבה' של ESET זמינה** בחלונית **בית** של ESET Internet Security, שקול הפעלה של תכונה זו במחשב שלך. לחץ על **הפעל 'המערכת נגד גניבה' של ESET** כדי לרשום את המחשב ב-'המערכת נגד גניבה' של ESET.

3. בחלון התוכנית הראשי, לחץ על **הגדרות** > **כלי אבטחה**. לחץ על  ליד **'המערכת נגד גניבה' של ESET** ופעל בהתאם להוראות בחלון הקופץ.



הערה
'המערכת נגד גניבה' של ESET אינו תומך ב-Microsoft Windows Home Server.

לקבלת הוראות נוספות על השיוך בין 'המערכת נגד גניבה' של ESET והמחשב, ראה כיצד להוסיף מכשיר חדש.

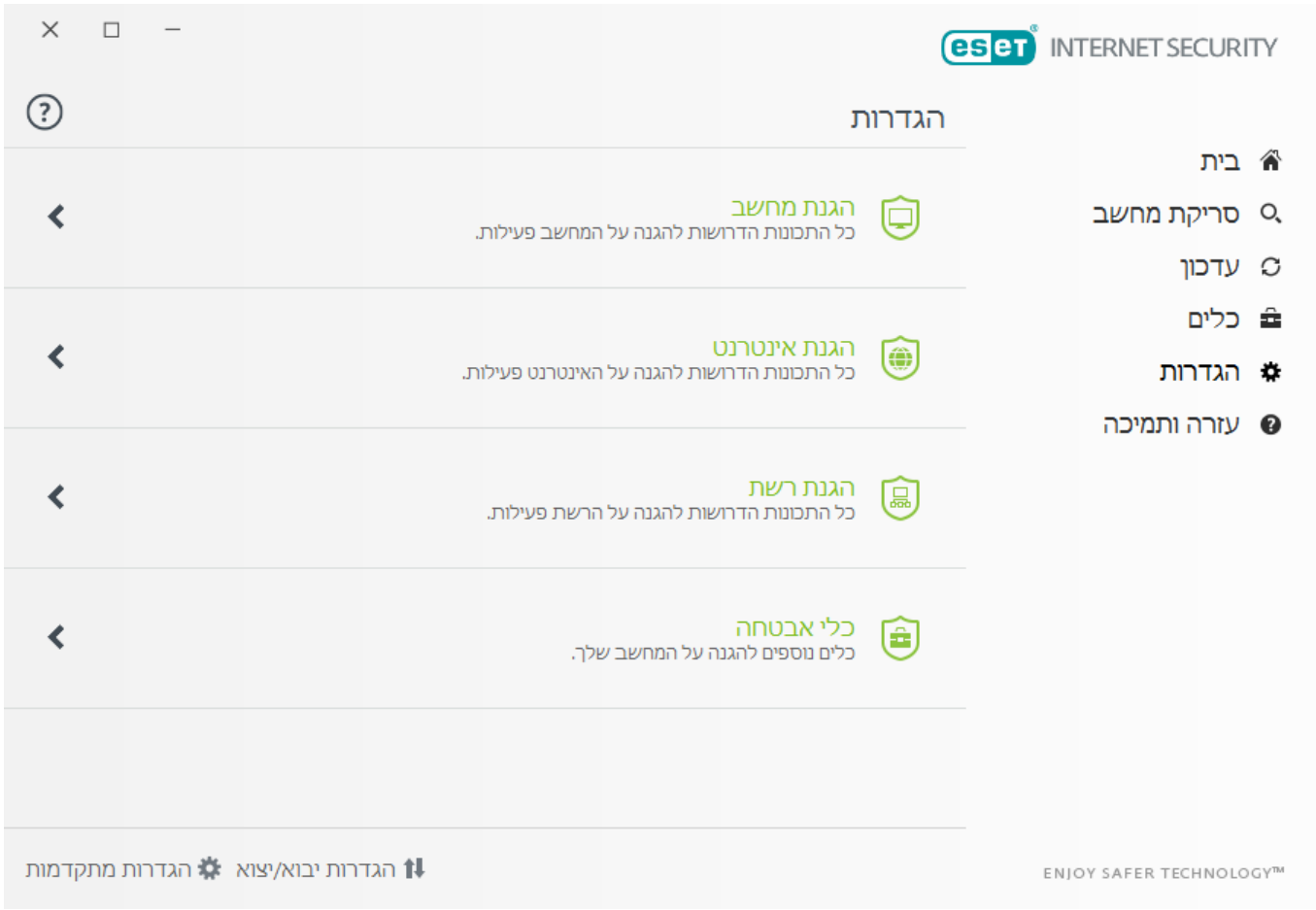
כלי בקרת הורים

אם כבר הפעלת את בקרת ההורים במוצר ESET Internet Security, עליך גם להגדיר את בקרת ההורים עבור חשבונות משתמש רצויים, כדי שבקרת ההורים תפעל כהלכה.

כאשר בקרות ההורים פעילות אך לא הוגדרו חשבונות משתמש, הכיתוב **בקרת הורים אינה מוגדרת** יוצג בחלונית **בית** של חלון התוכנית הראשי. לחץ על **הגדר כללים** ועיין בפרק בקרת הורים לקבלת הוראות כיצד ליצור הגבלות ספציפיות עבור ילדיך, כדי להגן עליהם מפני חומר שעשוי להיות פוגעני.

עבודה עם ESET Internet Security

אפשרויות ההגדרה של ESET Internet Security מאפשרות לך להתאים את רמות ההגנה של המחשב והרשת שלך.



התפריט **הגדרות** מחולק למקטעים הבאים:

הגנה על מחשב

הגנת אינטרנט

הגנת רשת

כלי אבטחה

לחץ על רכיב מסוים כדי לכוונן את ההגדרות המתקדמות של מודול ההגנה המתאים.

הגדרות **הגנה על מחשב** מאפשרות לך להפעיל את להשבית את הרכיבים הבאים:

- **הגנה על מערכת קבצים בזמן אמת** – כל הקבצים נסרקים לאיתור קודים זדוניים בעת פתיחתם, יצירתם או הפעלתם במחשב.
- **בקרת התקנים** – מודול זה מאפשר לך לסרוק, לחסום או להתאים הרשאות/מסננים מורחבים ולבחור כיצד המשתמש יוכל לגשת להתקן נתון (CD/DVD/USB...) ולהשתמש בו.
- **HIPS** – מערכת HIPS מנטרת את האירועים בתוך מערכת ההפעלה ומגיבה אליהם בהתאם למערכת כללים מותאמת אישית.
- **מצב משחק** – הפעלה או השבתה של מצב משחק. תקבל הודעת אזהרה (סיכון אבטחה אפשרי) והחלון הראשי יהפוך לכתום אחרי שתפעיל את מצב המשחק.
- **הגנת מצלמת אינטרנט** – שליטה בתהליכים וביישומים שניגשים למצלמה המחוברת למחשב. לקבלת מידע נוסף לחץ כאן.

הגדרות **הגנה על אינטרנט** מאפשרות לך להפעיל את להשבית את הרכיבים הבאים:

- **הגנת גישה לאינטרנט** – אם אפשרות זו מופעלת, כל התעבורה דרך HTTP או HTTPS תיסרק לאיתור תוכנות זדוניות.
- **הגנת לקוח דוא"ל** – ניטור התקשורת המתקבלת דרך הפרוטוקולים (POP3(S ו-IMAP(S).
- **הגנת מסנן דואר זבל** – סריקת דואר אלקטרוני שלא התבקש, כלומר דואר זבל או ספאם.
- **הגנה מפני פישינג** – סינון אתרי אינטרנט החשודים בהפצת תוכן שמיועד לגרום למשתמשים לשלוח מידע סודי.

המקטע **הגנת רשת** מאפשר לך להפעיל או להשבית את חומת האש, הגנה מפני מתקפות רשת (IDS) והגנה מפני רשת 'זומבי' (Botnet).

הגדרות **כלי אבטחה** מאפשרות לך להתאים את המודולים הבאים:

- הגנה על שירותים בנקאיים ותשלומים מקוונים
- בקרת הורים
- מערכת נגד גניבה

בקרת הורים מאפשרת לך לחסום דפי אינטרנט שייתכן שמכילים תוכן שעשוי להיות פוגעני. בנוסף, הורים יכולים לאסור גישה ליותר מ-40 קטגוריות אתרים ויותר מ-140 קטגוריות-משנה שהוגדרו מראש.

כדי להפעיל מחדש רכיב אבטחה שהושבת, לחץ על המחוון כך שיציג סימן ביקורת ירוק.

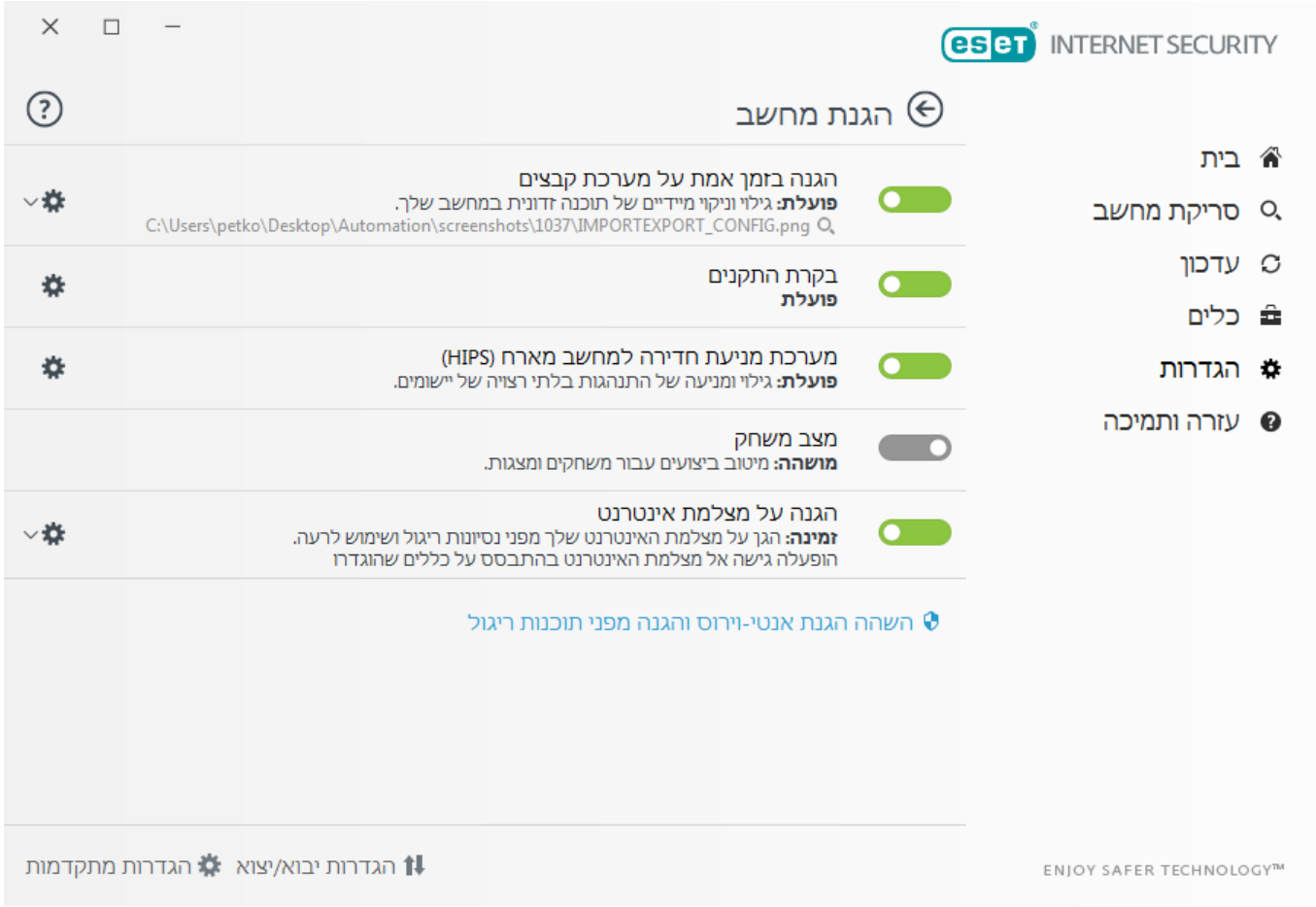
> **הערה**
> כאשר אתה משבית הגנה באמצעות שיטה זו, כל מודולי ההגנה שהושבתו יהפכו לזמינים לאחר הפעלה מחדש של המחשב.

אפשרויות נוספות זמינות בחלק התחתון של חלון ההגדרות. השתמש בקישור **הגדרות מתקדמות** כדי להגדיר פרמטרים מפורטים יותר לכל אחד מהמודולים. השתמש ב**הגדרות יבוא/יצוא** כדי לטעון פרמטרי הגדרות באמצעות קובץ תצורה מסוג *.xml* או כדי לשמור את פרמטרי ההגדרות הנוכחיים שלך בקובץ תצורה.

הגנה על מחשב

לחץ על 'הגנה על מחשב' בחלון ההגדרות כדי לראות סריקה כללית של כל מודולי ההגנה. כדי לכבות זמנית מודולים בודדים, לחץ על . שים לב שפעולה זו עשויה להוריד את רמת ההגנה של המחשב. לחץ על ליד מודול ההגנה כדי לגשת אל ההגדרות המתקדמות של מודול זה.

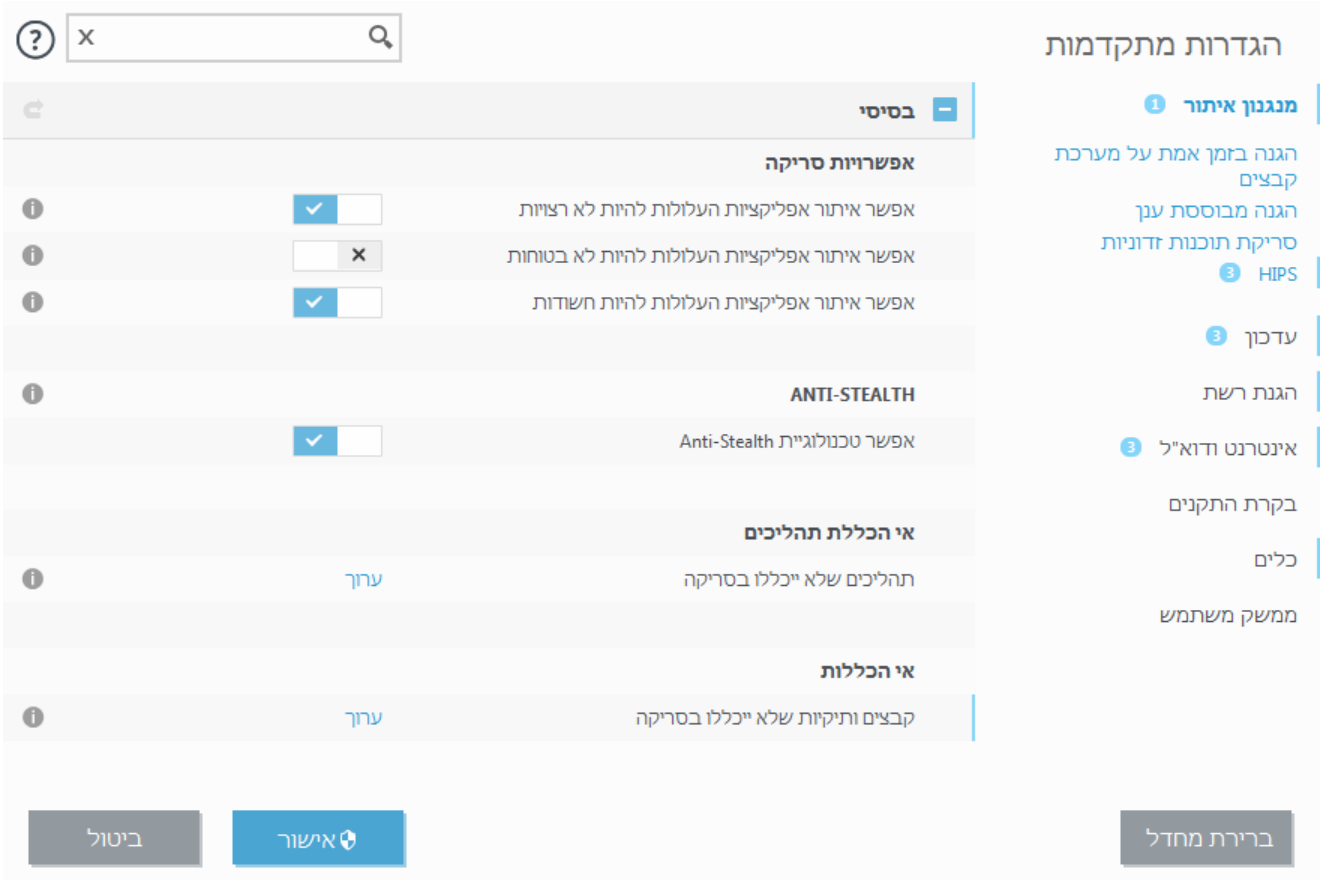
לחץ על > **עריכת אי-הכללות** לצד **הגנה על מערכת קבצים בזמן אמת** כדי לפתוח את חלון ההגדרות חריגות, המאפשר לך לא לכלול קבצים ותיקיות בסריקה.



השהה הגנה והגנה מפני תוכנות ריגול השבתת כל מודולי האנטי-וירוס וההגנה מפני תוכנות ריגול. כשאתה משבית הגנה, נפתח חלון שבו באפשרותך לקבוע למשך כמה זמן ההגנה תושבת, דרך החלון הנפתח **מרווח זמן**. לחץ על **החל** כדי לאשר.

מנגנון איתור

אנטי-וירוס מגן מפני התקפות זדוניות על המערכת על-ידי שליטה בקבצים, בדואר אלקטרוני ובתקשורת אינטרנט. בעת זיהוי איום עם קוד זדוני, מודול האנטי-וירוס יכול לסלקו, תחילה על-ידי חסימה שלו ואז על-ידי ניקויו, מחיקתו או העברתו להסגר.



אפשרויות סריקה עבור כל מודולי ההגנה (למשל הגנה על מערכת קבצים בזמן אמת, הגנה על גישה לאינטרנט, ...) מאפשרות לך להפעיל או להשבית זיהוי של:

- **אפליקציות העלולות להיות לא רצויות** – תוכנות אפורות או אפליקציות העלולות להיות לא רצויות (PUA) היא קטגוריה רחבה של תוכנות, שכוונתן אינה בהכרח זדונית כמו בסוגים אחרים של תוכנות זדוניות, כגון וירוסים וסוסים טרויאניים. עם זאת, הן עלולות להתקין תוכנות נוספות שאינן רצויות, לשנות את אופן הפעולה של המכשיר הדיגיטלי או לבצע פעילויות שלא אושרו או שאינן צפויות על ידי המשתמש.
קרא עוד על סוגי היישומים הללו במילון.

- **יישומים שעלולים להיות לא בטוחים** הם תוכנות מסחריות לגיטימיות שעלולות להיות מנוצלות למטרות זדוניות. דוגמאות ליישומים שעלולים להיות בלתי רצויים כוללות כלים לגישה מרחוק, יישומים לפיצוח סיסמאות ומעקב אחר הקשות במקלדת (תוכניות המתעדות כל הקשה של משתמש על המקלדת). אפשרות זו מושבתת כברירת מחדל.
קרא עוד על סוגי היישומים הללו במילון.

- **יישומים חשודים** כוללים תוכניות שנדחסו באמצעות אוריזם או מגנים. לעתים קרובות, סוגי המגנים הללו מנוצלים על-ידי מחברי תוכנות זדוניות כדי שלא יזוהו.

טכנולוגיית הגנה מפני התגנבות היא מערכת מתוחכמת המספקת זיהוי של תוכניות מסוכנות, כגון rootkit, אשר מסוגלות להסתתר ממערכת ההפעלה. המשמעות היא שלא ניתן לזהותן בשיטות הבדיקה הרגילות.

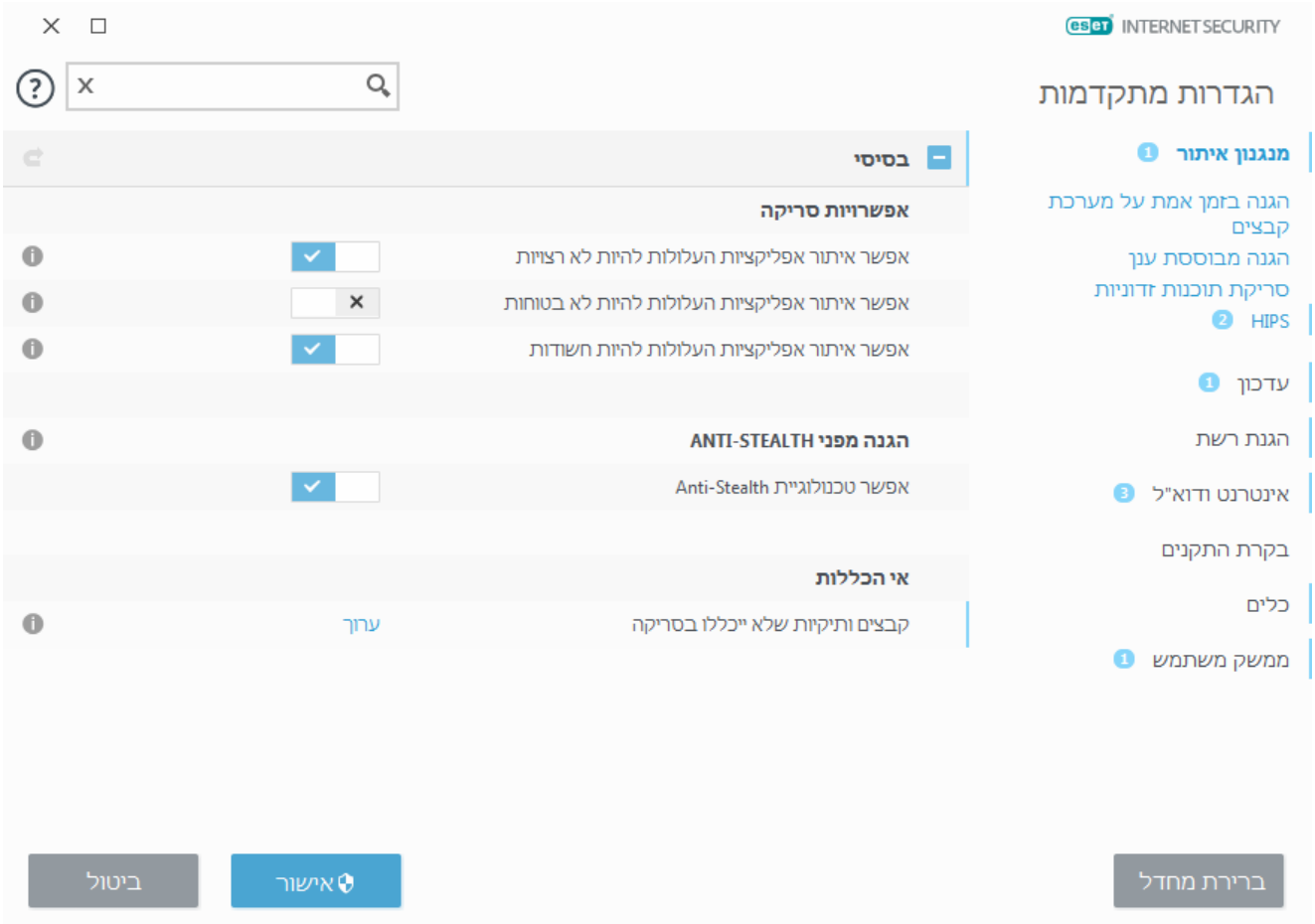
אי הכללות מאפשרות לך לא לכלול קבצים ותיקיות בסריקה. כדי לוודא שכל האובייקטים יישרקו לבדיקת איומים, מומלץ להגדיר אי הכללות רק כשהדבר הכרחי. מצבים לדוגמה שבהם תצטרך לא לכלול אובייקט כוללים סריקת ערכים במסד נתונים גדול, שבמהלכה פעילות המחשב מואטת, או תוכנה המתנגשת עם הסריקה. כדי לא לכלול אובייקט בסריקה, ראה אי הכללות.

הפעל סריקה מתקדמת באמצעות AMSI – כלי ממשק סריקה של Microsoft למניעת תוכנות זדוניות שמעניק למפתחי יישומים הגנות חדשות מפני תוכנות זדוניות (Windows 10 בלבד).

הגנה בזמן אמת על מערכת קבצים

הגנה בזמן אמת על מערכת קבצים שולטת בכל אירועי המערכת שקשורים לאנטי-וירוס. כל הקבצים נסרקים לאיתור קודים זדוניים

בעת פתיחתם, יצירתם או הפעלתם במחשב.



כברירת מחדל, הגנה בזמן אמת על מערכת קבצים מופעלת בעת אתחול המערכת ומספקת סריקה ללא הפרעות. מומלץ שלא להשבית את האפשרות **אפשר הגנה בזמן אמת על מערכת הקבצים** ב**הגדרות מתקדמות** תחת **מנגנון איתור** > **הגנה בזמן אמת על מערכת קבצים** > **בסיסי**.

מדיה לסריקה

כברירת מחדל, כל סוגי המדיה נסרקים לאיתור איומים פוטנציאליים:

- **כוננים מקומיים** – שליטה בכל הכוננים הקשיחים של המערכת.
- **מדיה נשלפת** – שליטה בתקליטורים/DVD, התקני אחסון בחיבור USB, התקני Bluetooth וכו'
- **כונני רשת** – סריקת כל הכוננים הממופים.

מומלץ להשתמש בהגדרות ברירת המחדל ולשנותם רק במצבים ספציפיים, למשל כאשר סריקת מדיה מסוימת מאטה משמעותית העברות נתונים.

מועד הסריקה

כברירת מחדל, כל הקבצים נסרקים בעת פתיחתם, יצירתם או פעולתם. מומלץ לשמור על הגדרות ברירת המחדל הללו, מאחר שהן מספקות את דרגת ההגנה המרבית בזמן אמת למחשב שלך:

- **פתיחת קובץ** – הפעלה או השבתה של הסריקה בעת פתיחת קבצים.
- **יצירת קובץ** – הפעלה או השבתה של הסריקה בעת יצירה או שינוי של קבצים.
- **הפעלת קובץ** – הפעלה או השבתה של הסריקה בעת הפעלת קבצים.
- **גישה למדיה נשלפת** – הפעלה או השבתה של סריקה המופעלת על-ידי גישה למדיה נשלפת מסוימת עם שטח אחסון.

הגנה בזמן אמת על מערכת קבצים בודקת את כל סוגי המדיה ומופעלת על-ידי אירועי מערכת שונים, כגון גישה לקובץ. באמצעות שיטות זיהוי של טכנולוגיית ThreatSense (כפי שמתוארות במקטע הגדרת פרמטר של מנוע ThreatSense), ניתן להגדיר את ההגנה

בזמן אמת על מערכת קבצים כך שתטפל אחרת בקבצים חדשים שנוצרו ובקבצים קיימים. לדוגמה, באפשרותך להגדיר את ההגנה בזמן אמת על מערכת קבצים כך שתפקח יותר מקרוב על קבצים חדשים שנוצרו.

כדי להבטיח צריכה מינימלית של משאבי המערכת בעת השימוש בהגנה בזמן אמת, קבצים שכבר נסרקו אינם נסרקים שוב ושוב (אלא אם שונו). קבצים נסרקים שוב מיד לאחר כל עדכון של מנגנון האיתור. פעילות זו נשלטת על-ידי **מיטוב חכם**. אם **מיטוב חכם** זה מושבת, כל הקבצים נסרקים בכל פעם שמתבצעת גישה אליהם. לשינוי הגדרה זו, הקש **F5** כדי לפתוח את **הגדרות מתקדמות** והרחב את **מנגנון איתור** > **הגנה בזמן אמת על מערכת קבצים**. לחץ על **פרמטר ThreatSense** > **אחר** ובחר או בטל את הבחירה באפשרות **אפשר מיטוב חכם**.

פרמטרים נוספים של ThreatSense

פרמטרים נוספים של ThreatSense עבור קבצים חדשים שנוצרו וקבצים ששונו

ההסתברות להדבקה בקבצים חדשים שנוצרו או בקבצים ששונו היא גבוהה יחסית, בהשוואה לקבצים קיימים. מסיבה זו התוכנית בודקת את הקבצים הללו באמצעות פרמטרי סריקה נוספים. ESET Internet Security משתמש בהיריסטיקה מתקדמת, המאפשרת לזהות איומים חדשים לפני הפצה של עדכון מנגנון האיתור בשילוב עם שיטות סריקה מבוססות-חתימה. בנוסף לקבצים חדשים שנוצרו, סריקה מבוצעת גם על **קובצי ארכיון בחילוץ עצמי** (sfx.) ו**אורזים של זמן ריצה** (קובצי הפעלה פנימיים דחוסים). כברירת מחדל, קובצי ארכיון נסרקים עד לרמת הקינון העשירית, ונבדקים ללא קשר לגודלם הממשי. כדי לשנות את הגדרות סריקת קובצי הארכיון, בטל את הבחירה באפשרות **הגדרות סריקת ארכיון שנקבעו כברירת מחדל**.

פרמטרים נוספים של ThreatSense עבור קובצי הפעלה

היריסטיקה מתקדמת בעת הפעלת קובץ – כברירת מחדל, האפשרות היריסטיקה מתקדמת משמשת בעת הפעלה של קבצים. כאשר היא מופעלת, מומלץ להשאיר את האפשרויות מיטוב חכם ו-ESET LiveGrid® פעילות כדי למזער את ההשפעה על ביצועי המערכת.

היריסטיקה מתקדמת בקובצי הפעלה שמקורם במדיה נשלפת – היריסטיקה מתקדמת מחקה את הקוד בסביבה וירטואלית ומעריכה את פעילותו לפני שמתאפשרת הפעלה של הקוד מהמדיה הנשלפת.

רמות ניקוי

להגנה בזמן אמת יש שלוש רמות ניקוי (כדי לגשת להגדרות רמת הניקוי לחץ על **הגדרות פרמטרי המנוע של ThreatSense** במקטע **הגנה על מערכת קבצים בזמן אמת** ואז לחץ על **ניקוי**).

ללא ניקוי – הקבצים הנגועים לא ינוקו אוטומטית. התוכנית תציג חלון אזהרה ותאפשר למשתמש לבחור פעולה. רמה זו תוכננה עבור משתמשים מתקדמים יותר, שיודעים אילו שלבים לנקוט במקרה של חדירה.

ניקוי רגיל – התוכנית תנסה לנקות או למחוק קובץ נגוע בצורה אוטומטית, על-פי פעולה שהוגדרה מראש (בתלות בסוג החדירה). הודעה על זיהוי ומחיקה של קובץ נגוע מופיעה בפינה הימנית התחתונה של המסך. אם לא ניתן לבחור את פעולת התיקון באופן אוטומטי, התוכנית מספקת פעולות אחרות למעקב. אותו הדבר קורה כאשר לא ניתן להשלים פעולה שהוגדרה מראש.

ניקוי מחמיר – התוכנית תנקה או תמחק את כל הקבצים הנגועים. החריגות היחידות הן קובצי המערכת. אם לא ניתן לנקותם, המשתמש יונחה לבחור פעולה בחלון אזהרה.

> **אזהרה**
> אם ארכיון מסוים מכיל קובץ או קבצים נגועים, ישנן שתי אפשרויות לטיפול בארכיון. במצב הסטנדרטי (ניקוי רגיל), אם כל הקבצים הכלולים בארכיון נגועים, הארכיון כולו יימחק. במצב **ניקוי מחמיר**, הארכיון יימחק אם הוא מכיל לפחות קובץ נגוע אחד, ללא תלות במצבם של הקבצים האחרים בארכיון.

מתי לשנות את תצורת ההגנה בזמן אמת

הגנה בזמן אמת היא המרכיב החיוני ביותר לשמירה על מערכת מאובטחת. היזהר תמיד כשאתה משנה את הפרמטרים שלה. מומלץ לשנות את הפרמטרים שלה רק במקרים ספציפיים.

לאחר התקנת ESET Internet Security, כל ההגדרות פועלות באופן המיטבי כדי לספק למשתמשים את רמת אבטחת המערכת המקסימלית. כדי לשחזר את הגדרות ברירת המחדל, לחץ על לצד כל אחת מהכרטיסיות בחלון (**הגדרות מתקדמות** > **מנגנון**

איתור > הגנה על מערכת קבצים בזמן אמת).

בדיקת הגנה בזמן אמת

כדי לוודא שהגנה בזמן אמת פועלת ומזהה וירוסים, השתמש בקובץ בדיקה של *www.eicar.com*. קובץ בדיקה זה הוא קובץ לא מזיק שמזוהה על-ידי כל תכניות האנטי וירוס. הקובץ נוצר על-ידי חברת EICAR (European Institute for Computer Antivirus Research) כדי לבדוק את התפקוד של תכניות אנטי וירוס.

הקובץ זמין להורדה בכתובת http://www.eicar.org/download/eicar.com

הערה
לפני ביצוע בדיקת הגנה בזמן אמת, יש להשבית את חומת האש. אם חומת האש פעילה, היא תזהה את הקובץ ותמנע הורדה של קובצי בדיקה. הקפד לאפשר שוב את חומת האש מיד לאחר בדיקת ההגנה בזמן אמת של מערכת הקבצים.

מה לעשות אם ההגנה בזמן אמת אינה פועלת

בפרק זה אנו מתארים בעיות שעשויות להתעורר כשמשתמשים בהגנה בזמן אמת וכיצד לפתור אותן.

הגנה בזמן אמת מושבתת

אם המשתמש השבית את ההגנה בזמן אמת בשוגג, יש להפעילה מחדש. כדי להפעיל מחדש את ההגנה בזמן אמת, נווט אל **הגדרות** בחלון התוכנית הראשי ולחץ על **הגנה על מחשב > הגנה על מערכת קבצים בזמן אמת**.

אם הגנה בזמן אמת אינה מופעלת בעת אתחול המערכת, לרוב הסיבה היא שהאפשרות **הפעל הגנה בזמן אמת על מערכת קבצים** מושבתת. כדי לוודא שאפשרות זו פעילה, נווט אל **הגדרות מתקדמות** (**F5**) ולחץ על **מנגנון איתור > הגנה בזמן אמת על מערכת קבצים**.

אם ההגנה בזמן אמת אינה מזהה ומנקה חדירות

ודא שלא מותקנות במחשב שלך תוכניות אנטי-וירוס אחרות. שתי תוכניות אנטי-וירוס המותקנות במחשב בו-זמנית עשויות להתנגש זו עם זו. לפני ההתקנה של ESET מומלץ להסיר את ההתקנה של כל תוכנית האנטי-וירוס האחרות במערכת.

הגנה בזמן אמת לא מופעלת

אם הגנה בזמן אמת לא מופעלת בעת אתחול המערכת (והאפשרות **הפעל הגנה בזמן אמת על מערכת קבצים** מופעלת), ייתכן שיש התנגשויות עם תכניות אחרות. לקבלת סיוע בפתרון הבעיה פנה לתמיכה הטכנית של ESET.

אי הכללת תהליכים

התכונה 'אי הכללת תהליכים' מאפשרת לך לא לכלול תהליכי אפליקציה בהגנה בזמן אמת על מערכת קבצים. כדי לשפר את מהירות הגיבוי, תקינות התהליכים וזמינות השירות, כמה טכניקות שידוע כי הן מתנגשות עם הגנה מפני תוכנה זדונית ברמת הקובץ נמצאות בשימוש במהלך הגיבוי. הדרך היעילה היחידה למנוע את שני המצבים היא להשבית את התוכנה הפועלת נגד תוכנה זדונית. על-ידי אי הכללה של תהליך ספציפי (לדוגמה התהליכים של פתרון הגיבוי) המערכת מתעלמת מכל פעולות הקבצים המיוחסות לתהליך שלא נכלל והן נחשבות לבטוחות, כך שההפרעה לתהליך הגיבוי מזערית. אנו ממליצים שתפעל בזהירות בעת יצירת אי הכללות – כלי גיבוי שלא נכלל יכול לגשת לקבצים נגועים בלי להפעיל התראה, ולכן הרשאות מורחבות מותרות רק במודול הגנה בזמן אמת.

הערה
אל תתבלבל עם סיומות קובץ שלא ייכללו, אי הכללות HIPS או אי הכללת קובץ/תיקייה.

אי הכללות של תהליכים עוזרות למזער את הסיכון של התנגשויות פוטנציאליות ולשפר את הביצועים של האפליקציות שלא נכללות, ויש לכך השפעה חיובית על היציבות והביצועים הכוללים של מערכת ההפעלה. אי ההכללה של תהליך / אפליקציה היא אי הכללה של

קובץ ההפעלה של התהליך או האפליקציה (*.exe*).

אתה יכול להוסיף קובצי הפעלה לרשימת התהליכים שלא נכללים דרך **הגדרות מתקדמות** (**F5**) > **מנגנון איתור** > **אי הכללת תהליכים**.

תכונה זו תוכננה כדי לא לכלול כלי גיבוי. אי הכללת התהליך של כלי הגיבוי בסריקה לא רק מבטיח את יציבות המערכת, אלא גם לא משפיע על ביצועי הגיבוי מאחר שהגיבוי לא מאט כאשר הוא פועל.

דוגמה

לחץ על **ערוך** כדי לפתוח את חלון הניהול של **אי הכללת תהליכים**, שבו ניתן **להוסיף** אי הכללות ולחפש את קובץ ההפעלה (לדוגמה *Backup-tool.exe*) שלא ייכלל בסריקה.
מיד כשקובץ ה-*exe.* מתווסף לאי ההכללות, הפעילות של תהליך זה אינה מנוטרת על-ידי ESET Internet Security ולא מופעלת סריקה בפעולות הקבצים שמבצע תהליך זה.

חשוב

אם אינך משתמש בפונקציית העיון בעת בחירת קובץ הפעלה של תהליך, עליך להזין ידנית נתיב מלא לקובץ ההפעלה. אחרת, אי ההכללה לא תפעל כראוי ו-HIPS עלול לדווח על שגיאות.

אתה יכול גם **לערוך** תהליכים קיימים או **להסיר** אותם מאי ההכללה.

הערה

הגנת גישה לאינטרנט לא לוקחת בחשבון את אי ההכללה הזו, ולכן אם לא תכלול את קובץ ההפעלה של דפדפן האינטרנט שלך, קבצים שיורדו עדיין יעברו סריקה. באופן זה, עדיין ניתן לזהות חדירה. תרחיש זה הוא דוגמה בלבד, ואיננו ממליצים לך ליצור אי הכללות לדפדפני אינטרנט.

הוספה או עריכה של אי-הכללות של תהליכים

תיבת דו-שיח זו מאפשרת לך **להוסיף** תהליכים שאינם נכללים בזיהוי איומים. אי הכללות של תהליכים עוזרות למזער את הסיכון של התנגשויות פוטנציאליות ולשפר את הביצועים של האפליקציות שלא נכללות, ויש לכך השפעה חיובית על היציבות והביצועים הכוללים של מערכת ההפעלה. אי ההכללה של תהליך / אפליקציה היא אי הכללה של קובץ ההפעלה של התהליך או האפליקציה (*.exe*).

דוגמה

בחר את נתיב הקובץ של אפליקציה שלא נכללה על ידי לחיצה על ... (לדוגמה *C:\Program Files\Firefox\Firefox.exe*). אל תזין את שם האפליקציה.
מיד כשקובץ ה-*exe.* מתווסף לאי ההכללות, הפעילות של תהליך זה אינה מנוטרת על-ידי ESET Internet Security ולא מופעלת סריקה בפעולות הקבצים שמבצע תהליך זה.

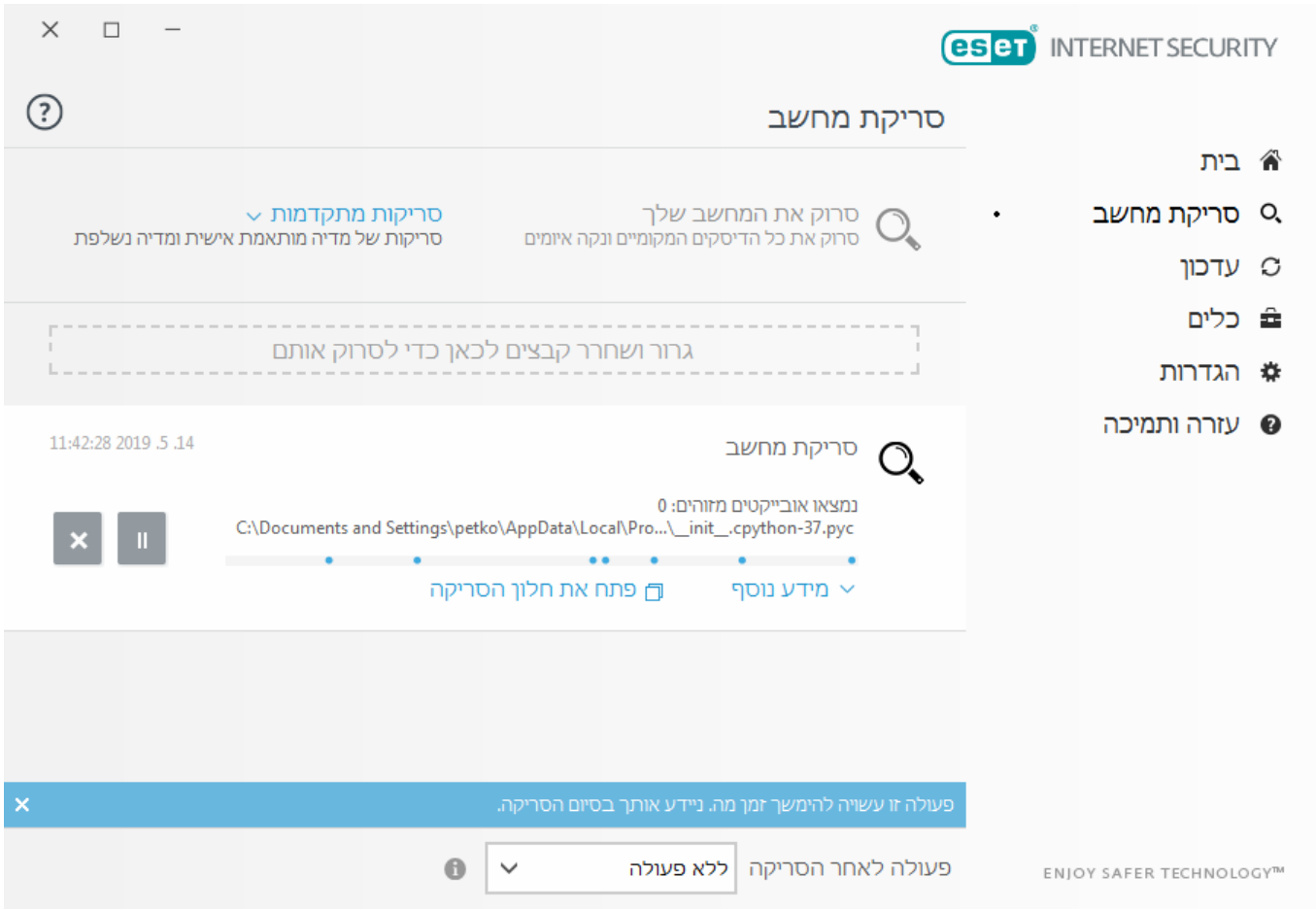
חשוב

אם אינך משתמש בפונקציית העיון בעת בחירת קובץ הפעלה של תהליך, עליך להזין ידנית נתיב מלא לקובץ ההפעלה. אחרת, אי ההכללה לא תפעל כראוי ו-HIPS עלול לדווח על שגיאות.

אתה יכול גם **לערוך** תהליכים קיימים או **להסיר** אותם מאי ההכללה.

סריקת מחשב

הסורק לפי דרישה הוא חלק חשוב מפתרון האנטי-וירוס שלך. הוא משמש לביצוע סריקות של קבצים ותיקיות במחשב. מבחינת האבטחה, הכרחי שסריקות המחשב יבוצעו באופן סדיר כחלק מאמצעי האבטחה השגרתיים ולא רק כשעולה חשד להדבקה. מומלץ שתבצע סריקות מערכת מעמיקות וקבועות כדי לזהות וירוסים שאינם נלכדים על-ידי הגנה על מערכת קבצים בזמן אמת כשהם נכתבים בדיסק. הדבר עשוי לקרות כאשר הגנה על מערכת קבצים בזמן אמת מושבתת באותו רגע, מנגנון האיתור אינו מעודכן או שהקובץ לא זוהה כווירוס כשנשמר בדיסק.



ישנם שני סוגי **סריקות מחשב** זמינים. האפשרות **סרוק את המחשב שלך** סורקת במהירות את המערכת ללא צורך בציון פרמטרי הסריקה. **סריקה מותאמת אישית** מאפשרת לך לבחור מתוך פרופילי סריקה שהוגדרו מראש, אשר תוכננו לטפל במיקומים מסוימים, כמו גם לבחור יעדי סריקה ספציפיים.

ראה התקדמות הסריקה לקבלת מידע נוסף על תהליך הסריקה.

סרוק את המחשב שלך

האפשרות 'סרוק את המחשב שלך' מאפשרת לך להפעיל סריקת מחשב במהירות ולנקות קבצים נגועים ללא צורך בהתערבות של המשתמש. היתרון של 'סרוק את המחשב שלך' הוא קלות ההפעלה והיעדר הצורך בהגדרות סריקה מפורטות. סריקה זו בודקת את כל הקבצים בכוננים המקומיים ומנקה או מוחקת את החדירות שזוהו באופן אוטומטי. רמת הניקוי מוגדרת אוטומטית כערך ברירת המחדל. לקבלת מידע מפורט יותר על סוגי הניקוי השונים, ראה ניקוי.

באפשרותך להשתמש גם בתכונה **סריקה בגרירה ושחרור** כדי לסרוק קובץ או תיקיה באופן ידני על-ידי לחיצה על הקובץ או התיקייה, העברת סמן העכבר לאזור המסומן תוך לחיצה על לחצן העכבר ולאחר מכן שחרור הלחיצה. לאחר מכן, האפליקציה תועבר לחזית.

אפשרויות הסריקה הבאות זמינות תחת **סריקות מתקדמות**:

סריקה מותאמת אישית

סריקה מותאמת אישית מאפשרת לך לציין פרמטרי סריקה, כגון יעדי הסריקה ושיטות הסריקה. היתרון של סריקה מותאמת אישית הוא היכולת להגדיר את הפרמטרים בפירוט. ניתן לשמור את התצורות בפרופילי סריקה המוגדרים על-ידי המשתמש, אשר עשויים להיות שימושיים כאשר הסריקה מתבצעת שוב ושוב עם אותם פרמטרים.

סורק מדיה נשלפת

בדומה לאפשרות 'סרוק את המחשב שלך' הפעלה מהירה של סריקת מדיה נשלפת (כגון CD/DVD/USB) שמחוברת כעת למחשב. אפשרות זו שימושית כשאתה מחבר כונן הבזק USB למחשב ומעוניין לסרוק את תכניו לאיתור תוכנות זדוניות ואיומים פוטנציאליים אחרים.

ניתן ליזום את סוג הסריקה הזה גם על-ידי לחיצה על **סריקה מותאמת אישית,** בחירה באפשרות **מדיה נשלפת** בתפריט הנפתח **יעדי סריקה** ולחיצה על **סריקה**.

חזרה על סריקה אחרונה

מאפשרת לך להפעיל במהירות את הסריקה הקודמת שבוצעה באמצעות אותן הגדרות שבהן היא הופעלה.

באפשרותך לבחור באפשרות **ללא פעולה**, **כיבוי** או **אתחול מחדש** בתפריט הנפתח **פעולה לאחר הסריקה**. הפעולות **שינה** או **מצב שינה** זמינות על בסיס הגדרות צריכת החשמל והשינה במערכת ההפעלה במחשב שלך או יכולות המחשב השולחני או הנייד שלך. הפעולה הנבחרת תתחיל לאחר סיום כל הסריקות. כאשר האפשרות **כיבוי** נבחרת, חלון דו-שיח לאישור הכיבוי יציג ספירה לאחור של 30 שניות (לחץ על **ביטול** כדי להשבית את הכיבוי המבוקש). ראה אפשרויות סריקה מתקדמות לפרטים נוספים.

> **הערה**
> מומלץ שתפעיל סריקת מחשב לפחות פעם בחודש. ניתן להגדיר את הסריקה כמשימה מתוזמנת תחת **כלים** > **כלים נוספים** > **מתזמן**. כיצד לתזמן סריקת מחשב שבועית?

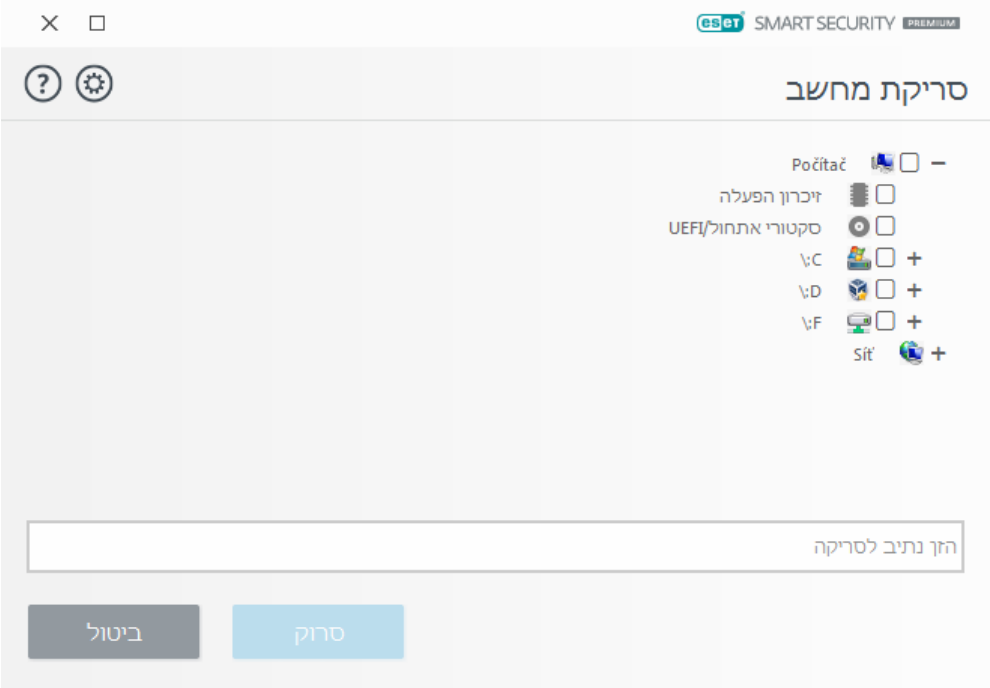
מפעיל סריקה מותאמת אישית

באפשרותך להשתמש בסריקת הלקוח כדי לסרוק חלקים מסוימים בדיסק במקום את הדיסק כולו. כדי לבצע פעולה זו, לחץ על **סריקות מתקדמות** > **סריקה מותאמת אישית** ובחר אפשרות בתפריט הנפתח **יעדי סריקה** או בחר יעדים ספציפיים מתוך מבנה התיקיות (העץ).

התפריט הנפתח **יעדי הסריקה** מאפשר לך לבחור יעדי סריקה שהוגדרו מראש.

- **הגדרות לפי פרופיל** בחירת יעדים שצוינו בפרופיל הסריקה שנבחר.
- **מדיה נשלפת** בחירת תקליטונים, כונני אחסון בחיבור USB, תקליטורים/DVD.
- **כוננים מקומיים** בחירת כל הכוננים הקשיחים של המערכת.
- **כונני רשת** בחירת כל הכוננים הממופים.
- **ללא בחירה** ביטול כל הבחירות.

כדי לנווט במהירות אל יעד סריקה או כדי להוסיף תיקיית או קבצי יעד, הזן את ספריית היעד בשדה הריק שמתחת לרשימת התיקיות. אפשרות זו זמינה רק בתנאי שלא נבחרו יעדים במבנה העץ ושבתפריט **יעדי סריקה** מוגדרת האפשרות **ללא בחירה**.



באפשרותך להגדיר את תצורת הפרמטרים של הניקוי לסריקה תחת **הגדרות מתקדמות** > **מנגנון איתור** > **סריקה לפי דרישה** > פרמטרים של **ThreatSense** > **ניקוי**. כדי להפעיל סריקה ללא פעולת ניקוי, בחר **סרוק ללא ניקוי**. היסטוריית הסריקות נשמרת ביומן הסריקות.

כאשר האפשרות **התעלם מחריגות** נבחרת, הקבצים עם הסיומות שהוחרגו בעבר מהסריקה ייסרקו ללא יוצא מן הכלל.

בתפריט הנפתח **פרופיל סריקה** תוכל לבחור פרופיל שישמש לסריקת יעדים ספציפיים. פרופיל ברירת המחדל הוא **סריקה חכמה**. ישנם עוד שני פרופילי סריקה מוגדרים מראש, המכונים **סריקה מעמיקה** ו**סריקת תפריט הקשר**. פרופילי הסריקה הללו משתמשים ב[פרמטרים שונים של ThreatSense]. האפשרויות הזמינות מתוארות ב**הגדרות מתקדמות** > **מנגנון איתור** > **סריקת תוכנות זדוניות** > **סריקה לפי דרישה** > [פרמטרים של ThreatSense].

לחץ על **סרוק** כדי לבצע את הסריקה באמצעות פרמטרים מותאמים אישית שהגדרת.

האפשרות **סרוק כמנהל מערכת** מאפשרת לך לבצע את הסריקה תחת חשבון מנהל המערכת. השתמש באפשרות זו אם למשתמש הנוכחי אין הרשאות לגשת לקבצים שברצונך לסרוק. לחצן זה אינו זמין כאשר למשתמש הנוכחי אין אפשרות להתקשר לתפעול UAC כמנהל מערכת.

> **הערה**
> בתום סריקה תוכל ללחוץ על **הצג יומן** כדי להציג את יומן סריקת המחשב.

התקדמות הסריקה

חלון התקדמות הסריקה מציג את המצב הנוכחי של הסריקה ומידע על מספר הקבצים שנמצאו שמכילים קוד זדוני.

> **הערה**
> אם אין אפשרות לסרוק קבצים מסוימים, למשל קבצים המוגנים באמצעות סיסמה או קבצים שנמצאים בשימוש בלעדי של המערכת (לרוב *pagefile.sys* וקובצי יומן מסוימים), זהו מצב נורמלי. ניתן למצוא פרטים נוספים ב[מאמר במאגר הידע] שלנו.

התקדמות הסריקה ▯ סרגל ההתקדמות מציג את הסטטוס של אובייקטים שכבר נסרקו בהשוואה לאובייקטים שעדיין ממתינים להיסרק. סטטוס התקדמות הסריקה נגזר מהמספר הכולל של אובייקטים הכלולים בסריקה.

יעד ▯ שם האובייקט הנסרק כעת ומיקומו.

איומים שנמצאו – הצגת מספר הקבצים שנסרקו, האיומים שנמצאו והאיומים שנוקו במהלך סריקה.

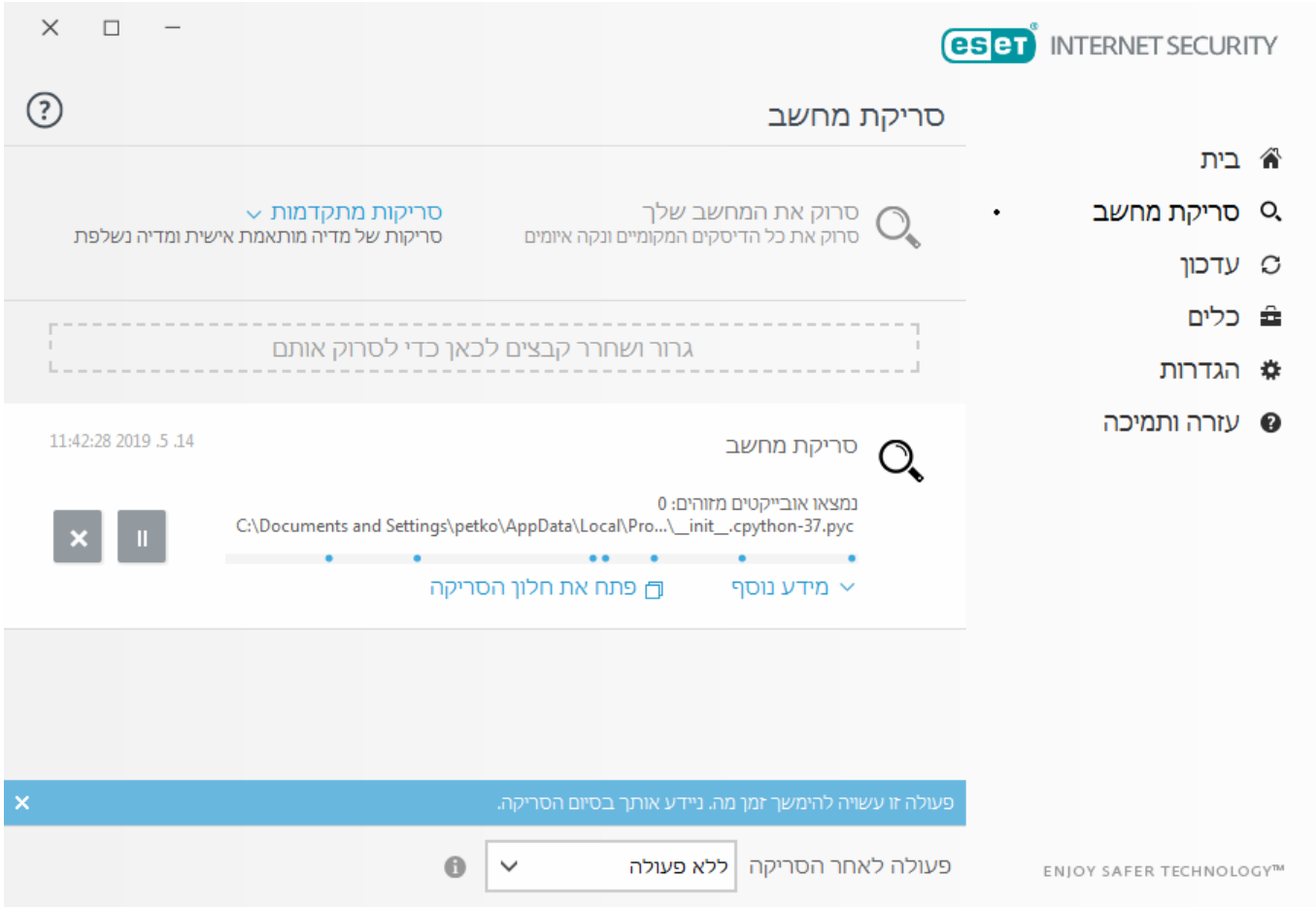
השהיה – השהיית סריקה.

המשך – אפשרות זו גלויה כאשר התקדמות הסריקה מושהית. לחץ על **המשך** כדי להמשיך בסריקה.

עצור – עצירת הסריקה.

גלול יומן סריקה – אם אפשרות זו מופעלת, יומן הסריקה יגלול מטה אוטומטית כאשר מתווספות הזנות חדשות, כך שייראו ההזנות החדשות ביותר.

> **הערה**
> לחץ על סמל הזכוכית המגדלת או החץ כדי להציג פרטים על הסריקה שמתבצעת כעת. באפשרותך להפעיל סריקה מקבילה אחרת על-ידי לחיצה על **סרוק את המחשב שלך** או **סריקה מותאמת אישית**.



פעולה לאחר הסריקה – הפעלת כיבוי , אתחול מחדש או שינה מתוזמנים כשסריקת המחשב מסתיימת. אחרי שהסריקה מסתיימת נפתח חלון דו-שיח לאישור הכיבוי, עם קוצב זמן של 30 שניות.

יומן רישום של המחשב

יומן סריקות מחשב נותן לך מידע כללי על סריקות, למשל:

- שעת השלמה
- זמן סריקה כולל
- מספר איומים שנמצאו
- מספר אובייקטים שנסרקו
- דיסקים, תיקיות וקבצים שנסרקו
- תאריך ושעת הסריקה

• גרסת מנגנון האיתור

סריקת תוכנות זדוניות

המקטע **סריקת תוכנות זדוניות** נגיש מ**הגדרות מתקדמות** (F5) > **מנגנון איתור** > **סריקת תוכנות זדוניות** ומספק אפשרויות לבחירת פרמטרים לסריקה. המקטע כולל את הפריטים הבאים:

הפרופיל שנבחר – סדרה ספציפית של פרמטרים שבהם משתמש הסורק לפי דרישה. כדי ליצור פרופיל חדש, לחץ על **ערוך** לצד **רשימת פרופילים**. ראה פרופילי סריקה לקבלת פרטים נוספים.

יעדי סריקה – אם ברצונך לסרוק יעד ספציפי בלבד, אתה יכול ללחוץ על **ערוך** לצד **יעדי סריקה** ולבחור אפשרות מהתפריט הנפתח או לבחור יעדים ספציפיים ממבנה (עץ) התיקיות. ראה יעדי סריקה לקבלת פרטים נוספים.

פרמטרים של ThreatSense – במקטע זה ניתן למצוא אפשרויות של הגדרות מתקדמות, כמו סיומות קבצים שברצונך לשלוט בהן, שיטות איתור שבשימוש וכן הלאה. לחץ כדי לפתוח לשונית עם אפשרויות סורק מתקדמות.

סרוק במצב לא פעיל

ניתן לאפשר סורק במצב לא פעיל ב**הגדרות מתקדמות** תחת **מנגנון איתור** > **סריקת תוכנות זדוניות** > **סריקה במצב לא פעיל.**

סרוק במצב לא פעיל

הגדר את המתג לצד אפשר סריקה במצב לא פעיל לפעיל כדי לאפשר תכונה זו. כאשר המחשב במצב לא פעיל, מתבצעת סריקת מחשב שקטה בכוננים המקומיים.

כברירת מחדל, הסורק במצב לא פעיל לא יופעל כאשר המחשב (הנייד) מופעל בכוח הסוללה. תוכל להחליף הגדרה זו על-ידי הפעלת המתג ליד **הפעל אפילו אם המחשב פועל באמצעות סוללה** בהגדרות המתקדמות.

הפעל את המתג **אפשר רישום ביומן** בהגדרות המתקדמות כדי לתעד פלט סריקת מחשב במקטע רשומות יומן (בחלון התוכנית הראשי לחץ על **כלים** > **כלים נוספים** > **רשומות יומן** ואז בחר באפשרות **סריקת מחשב** בתפריט הנפתח **יומן**).

איתור במצב לא פעיל

ראה גורמים מפעילים לאיתור במצב לא פעיל להצגת רשימה מלאה של תנאים שצריכים להתקיים כדי להפעיל את הסורק במצב לא פעיל.

לחץ על הגדרת פרמטרים של מנגנון ThreatSense כדי לשנות את פרמטרי הסריקה (לדוגמה שיטות זיהוי) של הסורק במצב לא פעיל.

פרופילי סריקה

תוכל לשמור את פרמטרי הסריקה המועדפים עליך לסריקה עתידית. מומלץ שתיצור פרופיל שונה (עם מגוון יעדי סריקה, שיטות סריקה ופרמטרים אחרים) עבור כל סריקה שנמצאת בשימוש קבוע.

כדי ליצור פרופיל חדש, פתח את חלון ההגדרות המתקדמות (F5) ולחץ על **מנגנון איתור** > **סריקות לאיתור נוזקות** > **סריקה לפי דרישה** > **רשימת פרופילים**. החלון **מנהל הפרופילים** כולל את התפריט **פרופיל נבחר**, בו מפורטים פרופילי הסריקה הקיימים והאפשרות ליצור פרופיל חדש. כדי לסייע לך ליצור פרופיל חדש שיענה על דרישותיך, עיין במקטע הגדרות פרמטרי המנוע של ThreatSense לקבלת תיאור של כל אחד מהפרמטרים של הגדרות הסריקה.

> **הערה**
> נניח שברצונך ליצור פרופיל סריקה משלך והתצורה **סרוק את המחשב שלך** מתאימה באופן חלקי, אך אינך מעוניין לסרוק אורזים של זמן ריצה או אפליקציות העלולות להיות לא בטוחות, ובנוסף ברצונך להחיל **ניקוי מחמיר**. הזן את שם הפרופיל החדש שלך בחלון **מנהל הפרופילים** ולחץ על **הוסף**. בחר את הפרופיל החדש בתפריט הנפתח **פרופיל נבחר** והתאם את הפרמטרים שנותרו כך שיענו על דרישותיך. לאחר מכן לחץ על **אישור** כדי לשמור את הפרופיל החדש.

יעדי סריקה

התפריט הנפתח **יעדי הסריקה** מאפשר לך לבחור יעדי סריקה שהוגדרו מראש.

- **הגדרות לפי פרופיל** ← בחירת יעדים שצוינו בפרופיל הסריקה שנבחר.
- **מדיה נשלפת** ← בחירת תקליטונים, כונני אחסון בחיבור USB, תקליטורים/DVD.
- **כוננים מקומיים** ← בחירת כל הכוננים הקשיחים של המערכת.
- **כונני רשת** ← בחירת כל הכוננים הממופים.
- **ללא בחירה** ← ביטול כל הבחירות.

אפשרויות סריקה מתקדמות

בחלון זה אתה יכול לציין אפשרויות מתקדמות למשימה של סריקת מחשב מתוזמנת. אתה יכול להגדיר פעולה שתבוצע אוטומטית לאחר סיום הסריקה בעזרת התפריט הנפתח:

- **כיבוי** ← המחשב יכבה לאחר סיום הסריקה.
- **אתחול מחדש** ← סגירת כל התוכניות הפתוחות והפעלה מחדש של המחשב לאחר סיום הסריקה.
- **שינה** ← שמירת ההפעלה והעברת המחשב למצב של צריכת חשמל נמוכה כדי שתוכל לחזור לעבוד במהירות.
- **מצב שינה** ← העברת כל מה שפועל ב-RAM לקובץ מיוחד בכונן הקשיח. המחשב יכבה, אך יחזור למצבו הקודם בפעם הבאה שתפעיל אותו.
- **ללא פעולה** ← לאחר סיום הסריקה לא תתבצע כל פעולה.

> הערה
> זכור שמחשב ישן הוא עדיין מחשב פועל. הוא עדיין מפעיל פונקציות בסיסיות ומשתמש בחשמל כשהמחשב פועל על סוללה. כדי לשמר את חיי הסוללה, למשל כשאתה מחוץ למשרד, אנו ממליצים להשתמש באפשרות 'מצב שינה'.

בחר **המשתמש לא יכול לבטל את הפעולה** כדי למנוע ממשתמשים ללא הרשאות את היכולת להפסיק את הפעולות המבוצעות לאחר הסריקה.

בחר **המשתמש יכול להשהות את הסריקה למשך (דקות)** אם ברצונך לאפשר למשתמש המוגבל להשהות את סריקת המחשב לפרק זמן שצוין.

עיין גם בפרק התקדמות הסריקה.

סריקה בעת אתחול המערכת

כברירת מחדל, בדיקת קובץ האתחול האוטומטית תבוצע בעת אתחול המערכת ובמהלך עדכוני מנגנון האיתור. סריקה זו תלויה בתצורת המתזמן ובמשימות.

אפשרויות הסריקה בעת אתחול המערכת הן חלק ממשימת מתזמן של **בדיקת קובץ אתחול מערכת**. כדי לשנות את ההגדרה שלו, נווט אל **כלים** > **מתזמן**, לחץ על **בדיקת קובץ אתחול אוטומטית** ולאחר מכן על **עריכה**. בשלב האחרון, החלון בדיקת קובץ אתחול אוטומטית יופיע (עיין בסעיף הבא לקבלת פרטים נוספים).

לקבלת הוראות מפורטות על יצירה וניהול של משימת מתזמן, ראה יצירת משימות חדשות.

בדיקת קובץ אתחול אוטומטית

בעת יצירת משימה מתוזמנת של בדיקת קובץ אתחול אוטומטית, יש לך מספר אפשרויות להתאמת הפרמטרים הבאים:

התפריט הנפתח **קבצים בשימוש שכיח** מציין את עומק הסריקה של קבצים הפועלים בעת אתחול המערכת, על-בסיס אלגוריתם מתוחכם וסודי. הקבצים מסודרים בסדר יורד, בהתאם לקריטריונים הבאים:

- **כל הקבצים הרשומים** (רוב הקבצים הנסרקים)

- **קבצים בשימוש לעתים נדירות**
- **קבצים בשימוש שכיח**
- **קבצים בשימוש לעתים קרובות**
- **רק הקבצים שבהם אתה משתמש הכי הרבה** (הכי פחות קבצים נסרקים)

נכללות גם שתי קבוצות ספציפיות:

- **קבצים הפועלים לפני כניסת המשתמש** – מכילה קבצים ממיקומים שניתן לגשת אליהם מבלי שהמשתמש מחובר (כוללת כמעט את כל מיקומי האתחול, כגון שירותים, אובייקטי עוזר דפדפן, יידוע של winlogon, הזנות מתזמן Windows, קובצי dll מוכרים, וכו').
- **קבצים הפועלים אחרי כניסת המשתמש** - מכילה קבצים ממיקומים שאליהם ניתן לגשת רק אחרי שמשתמש התחבר (לרבות קבצים שמופעלים רק על-ידי משתמש ספציפי, בדרך-כלל קבצים בנתיב *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

רשימות הקבצים לסריקה קבועות עבור כל אחת מהקבוצות שתוארו לעיל.

עדיפות סריקה – רמת העדיפות שבה תשתמש המערכת כדי לקבוע מתי תופעל סריקה:

- **במצב לא פעיל** – המשימה תבוצע רק כאשר המערכת לא פעילה,
- **הכי נמוך** – כאשר העומס על המערכת הוא הנמוך ביותר האפשרי,
- **נמוך** – עומס מערכת נמוך,
- **רגיל** – עומס מערכת ממוצע.

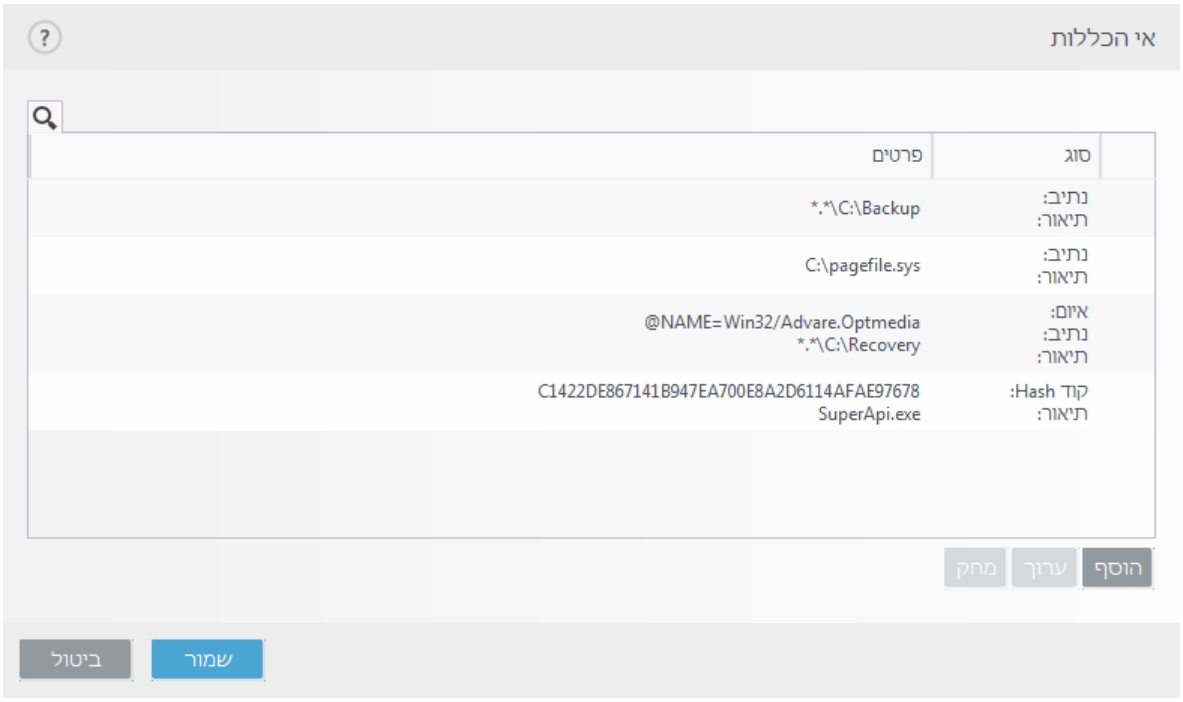
חריגות

חריגות מאפשרות לך לא לכלול קבצים ותיקיות בסריקה. כדי לוודא שכל האובייקטים ייסרקו לבדיקת איומים, מומלץ להגדיר חריגות רק כשהדבר הכרחי. עם זאת, ישנם מצבים שבהם תצטרך להחריג אובייקט, למשל סריקת ערכים במסד נתונים גדול, שבמהלכה פעילות המחשב מואטת, או תוכנה המתנגשת עם הסריקה.

אתה יכול להוסיף קבצים ותיקיות שלא ייכללו בסריקה לרשימת האי הכללות דרך **הגדרות מתקדמות** (**F5**) > **מנגנון איתור** > **אי הכללות** > **קבצים ותיקיות שלא ייכללו בסריקה** > **ערוך**.

> **הערה**
> אל תתבלבל עם סיומות קובץ שלא ייכללו, אי הכללות HIPS או אי הכללת תהליכים.

כדי לא לכלול אובייקט (נתיב, איום או קוד Hash) בסריקה, לחץ על **הוסף** והזן את הנתיב לאובייקט או בחר אותו במבנה העץ. באפשרותך גם **לערוך** או **למחוק** ערכים נבחרים.



סוגי אי הכללה

נתיב – הנתיב לקבצים ולתיקיות שיוחרגו.

איתור (או **איום**) – אם ישנו שם של איתור / איום ליד קובץ שלא נכלל, פירוש הדבר שהקובץ לא יכלל רק עבור האיום הנתון, ולא באופן מוחלט. אם קובץ זה יזוהם בתוכנה זדונית בשלב מאוחר יותר, מודול האנטי-וירוס יזהה אותו. סוג זה של אי הכללה יכול לשמש רק עבור סוגים מסוימים של חדירות, וניתן ליצור אותו בחלון ההתראה על איומים שמדווח על החדירה (לחץ על **הצג אפשרויות מתקדמות** ואז בחר באפשרות **אי-הכללת איתור**) או על-ידי לחיצה על **כלים** > **כלים נוספים** > **הסגר** ואז לחיצה בלחצן העכבר הימני על הקובץ שהועבר להסגר ובחירה באפשרות **שחזר ואל תכלול בסריקה** בתפריט ההקשר.

קוד Hash – לא כולל קובץ על בסיס קוד Hash שצוין (SHA1), ללא קשר לסוג הקובץ, המיקום, השם או הסיומת שלו.

> הערה
> כאשר קובץ מסוים עומד בקריטריונים להחרגה מהסריקה, מודול ה**הגנה בזמן אמת על מערכת קבצים** או מודול **סריקת המחשב** לא יזהו איום בקובץ.

רכיבי בקרה

הוסף – החרגת אובייקטים מהזיהוי.

ערוך – אפשרות לעריכת ערכים שנבחרו.

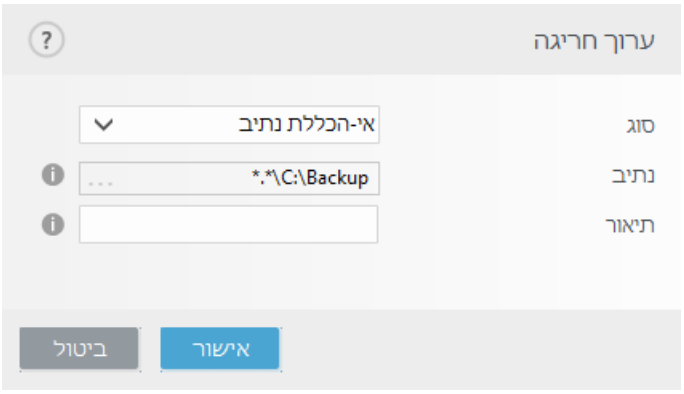
מחק – הסרת ערכים שנבחרו (CTRL + לחץ כדי לבחור ערכים מרובים).

הוספה או עריכה של אי-הכללות

חלון דו-שיח זה מאפשר לך להוסיף או לערוך פריטים שלא ייכללו. בחר את **סוג** אי ההכללה מהתפריט הנפתח:

אי-הכללת נתיב

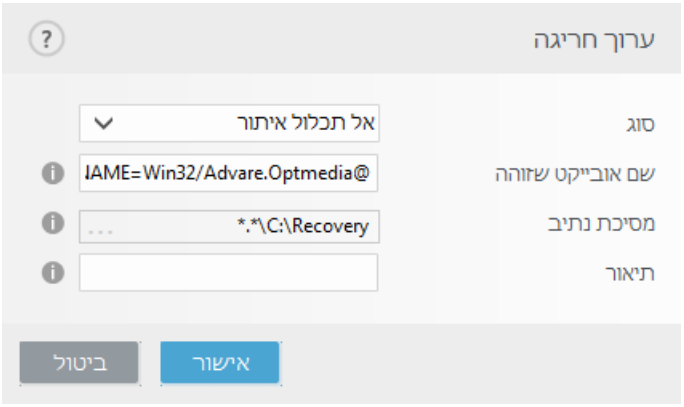
אי הכללה של נתיב ספציפי (קובץ או ספרייה) עבור מחשב זה. בחר נתיב מתאים על-ידי לחיצה על **...** בשדה **נתיב**.



ראה עוד דוגמאות לתבניות אי הכללה בהמשך.

'אי-הכללת איתור' או 'אי-הכללת איום'

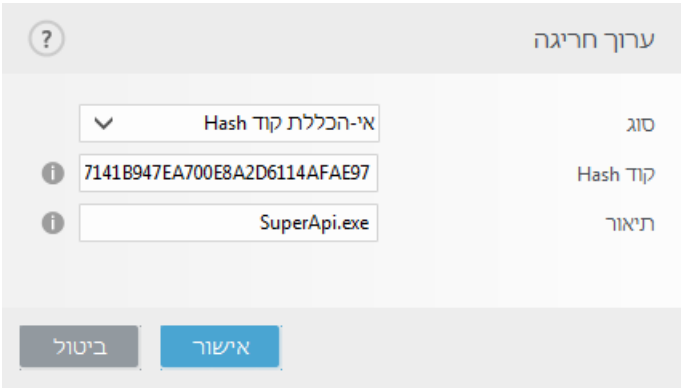
יש לספק שם זיהוי / איום חוקי של ESET. להצגת שם זיהוי חוקי, ראה רשומות יומן ולאחר מכן בחר **אובייקטים מזוהים** מהתפריט הנפתח של רשומות היומן. הדבר שימושי כאשר דגימה של זיהוי חיובי שגוי מזוהה ב-ESET Internet Security. אי הכללות עבור חדירות אמיתיות הן מסוכנות מאוד, שקול לא לכלול קבצים / ספריות מושפעים בלבד על-ידי לחיצה על **...** בשדה **מסיכת נתיב** ו/או רק לתקופה זמנית. אי הכללות חלות גם על אפליקציות העלולות להיות לא רצויות, אפליקציות העלולות להיות לא בטוחות ואפליקציות חשודות.



ראה גם דוגמה לאי הכללות של איומים בהמשך.

אי-הכללת קוד Hash

לא כולל קובץ על בסיס קוד Hash שצוין (SHA1), ללא קשר לסוג הקובץ, המיקום, השם או הסיומת שלו.



באפשרותך להשתמש בתווים כלליים כדי לא לכלול קבוצת קבצים. סימן שאלה (?) מייצג תו יחיד וכוכבית (*) מייצגת מחרוזת של אפס תווים או יותר.

תבנית אי-הכללה

- אם ברצונך לא לכלול את כל הקבצים בתיקייה, הקלד את הנתיב לתיקייה והשתמש במסיכה *.*.
- כדי לא לכלול כונן שלם, עם כל הקבצים ותיקיות המשנה, השתמש במסיכה "*D:*".
- אם ברצונך לא לכלול קובצי doc בלבד, השתמש במסיכה "*.doc".
- אם השם של קובץ הפעלה מסוים כולל מספר מסוים של תווים (עם תווים משתנים) ואתה יודע רק את הראשון (לדוגמה, "D"), השתמש בתבנית הבאה:
D????.exe (סימני השאלה מחליפים את התווים הלא ידועים/החסרים)

משתני מערכת באי הכללות

ניתן להשתמש במשתני מערכת כמו *%PROGRAMFILES%* כדי להגדיר אי הכללות בסריקה.

- כדי לא לכלול את התיקייה Program Files באמצעות משתנה מערכת זה, השתמש בנתיב *%PROGRAMFILES%* (זכור להוסיף קו נטוי הפוך בסוף הנתיב) בעת הוספה לאי ההכללות
- כדי לא לכלול את כל הקבצים בספריית המשנה %HOMEDRIVE%, השתמש בנתיב *%HOMEDRIVE%\Excluded_Directory*.*

הרחב את רשימת משתני המערכת הנתמכים

ניתן להשתמש במשתנים הבאים בתבנית אי ההכללה של הנתיב:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%HOMEDRIVE%*
- *%HOMEPATH%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

משתני מערכת ספציפיים למשתמש (כמו *%TEMP%* או *%USERPROFILE%*) או משתני סביבה (כמו *%PATH%*) אינם נתמכים.

אי הכללות באמצעות כוכבית

מספר דוגמאות נוספות לאי הכללה באמצעות כוכבית:

C:\Tools ← המרה אוטומטית ל-*C:\Tools*.*

C:\Tools.dat* ← אי הכללת קובצי *dat.* בתיקיה Tools

C:\Tools\sg.dat ← אי הכללת קובץ ספציפי זה הממוקם בנתיב המדויק

בעת בחירה ב**אי הכללת נתיב**, אנו ממליצים מאוד לא להשתמש בתווים כלליים באמצע נתיב (לדוגמה *C:\Tools*\Data\file.dat*) אלא אם תשתית המערכת דורשת זאת. עיין במאמר מאגר הידע הבא לקבלת מידע נוסף.

בעת בחירה באפשרות **אי-הכללת איתור** או **אי-הכללת איום**, אין הגבלות על שימוש בתווים כלליים באמצע נתיב.

סדר אי ההכללות

- אין אפשרויות להתאמת רמת העדיפות של אי הכללות באמצעות לחצני עליון/תחתון (בכל הנוגע לכללי חומת אש כאשר הפעלת הכללים מתבצעת מלמעלה למטה)
- כאשר הסורק מוצא התאמה לכלל הישים הראשון, הכלל הישים השני לא יוערך
- ככל שהכללים מועטים יותר, ביצועי הסריקה יהיו טובים יותר
- הימנע מיצירת כללים החלים בו זמנית

אי הכללות של איומים

אם ברצונך שלא לכלול איום, הזן שם חוקי של אובייקט שזוהה:

Win32/Adware.Optmedia

ניתן גם להשתמש בתבנית הבאה בעת אי הכללה של אובייקט שזוהה בחלון ההתראות של ESET Internet Security:

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

תבנית אי הכללה של נתיב

באפשרותך להשתמש בתווים כלליים כדי לא לכלול קבוצת קבצים. סימן שאלה (*?*) מייצג תו יחיד וכוכבית (*) מייצגת מחרוזת של אפס תווים או יותר.

תבנית אי-הכללה

- אם ברצונך לא לכלול את כל הקבצים בתיקייה, הקלד את הנתיב לתיקייה והשתמש במסיכה *.*.
- כדי לא לכלול כונן שלם, עם כל הקבצים ותיקיות המשנה, השתמש במסיכה "*D:*".
- אם ברצונך לא לכלול קובצי doc בלבד, השתמש במסיכה "*.doc*".
- אם השם של קובץ הפעלה מסוים כולל מספר מסוים של תווים (עם תווים משתנים) ואתה יודע רק את הראשון (לדוגמה, "D"), השתמש בתבנית הבאה:

D????.exe (סימני השאלה מחליפים את התווים הלא ידועים/החסרים)

משתני מערכת באי הכללות

ניתן להשתמש במשתני מערכת כמו *%PROGRAMFILES%* כדי להגדיר אי הכללות בסריקה.

- כדי לא לכלול את התיקייה Program Files באמצעות משתנה מערכת זה, השתמש בנתיב *%PROGRAMFILES%* (זכור להוסיף קו נטוי הפוך בסוף הנתיב) בעת הוספה לאי ההכללות
- כדי לא לכלול את כל הקבצים בספריית המשנה %HOMEDRIVE%, השתמש בנתיב *%HOMEDRIVE%\Excluded_Directory*.**

הרחב את רשימת משתני המערכת הנתמכים

ניתן להשתמש במשתנים הבאים בתבנית אי ההכללה של הנתיב:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%HOMEDRIVE%*
- *%HOMEPATH%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

משתני מערכת ספציפיים למשתמש (כמו *%TEMP%* או *%USERPROFILE%*) או משתני סביבה (כמו *%PATH%*) אינם נתמכים.

הפרמטרים של ThreatSense

ThreatSense מורכב ממספר שיטות לזיהוי איומים. טכנולוגיה זו פועלת באופן יזום, והמשמעות היא שהיא גם מספקת הגנה במהלך ההתפשטות המוקדמת של איום חדש. היא משתמשת בשילוב של ניתוח קוד, הדמיית קוד, חתימות גנריות וחתימות וידאו, אשר פועלים יחדיו כדי לשפר משמעותית את בטיחות המערכת. מנוע הסריקה מסוגל לשלוט במספר הזרמות נתונים בו-זמנית, ובכך מאפשר להשיג את היעילות וקצב הזיהוי המרביים. טכנולוגיית ThreatSense אף מסלקת תוכניות rootkit בהצלחה.

אפשרויות ההגדרה של מנוע ThreatSense מאפשרות לך לציין מספר פרמטרי סריקה:

- סוגי וסיומות קבצים שיש לסרוק
- שילוב שיטות הזיהוי השונות
- רמות הניקוי, וכו'.

כדי להיכנס לחלון ההגדרות, לחץ על **הפרמטרים של ThreatSense** בחלון ההגדרות המתקדמות עבור כל מודול שמשתמש בטכנולוגיית ThreatSense (ראה להלן). תרחישי אבטחה שונים עשויים להצריך הגדרות תצורה שונות. לאור זאת, את ThreatSense ניתן להגדיר בנפרד עבור כל אחד ממודולי ההגנה הבאים:

- הגנה בזמן אמת על מערכת קבצים
- סריקה במצב לא פעיל
- סריקה בעת האתחול
- הגנה על מסמכים
- הגנת לקוח דוא"ל
- הגנת גישה לאינטרנט
- סריקת מחשב

הפרמטרים של ThreatSense עברו אופטימיזציה עבור כל מודול ומודול, ושינוי שלהם עלול להשפיע משמעותית על פעולת המערכת. לדוגמה, שינוי הפרמטרים כך שיסרקו תמיד אורזים של זמן ריצה, או באופן שיאפשר היריסטיקה מתקדמת במודול ההגנה על מערכת קבצים בזמן אמת, עשויים להוביל להאטה בפעילות המערכת (בדרך-כלל רק קבצים חדשים שנוצרו נסרקים בשיטות אלו). מומלץ להשאיר את פרמטרי ברירת המחדל של ThreatSense ללא שינוי עבור כל המודולים, למעט סריקת מחשב.

אובייקטים לסריקה
מקטע זה מאפשר לך להגדיר אילו רכיבי מחשב וקבצים ייסרקו לאיתור חדירות.

זיכרון הפעלה – סריקה לאיתור איומים שתוקפים את זיכרון ההפעלה של המערכת.

סקטורי אתחול/UEFI – סריקת סקטורי האתחול לאיתור וירוסים ברשומת האתחול המרכזית. קרא עוד על UEFI במילון.

קובצי דוא"ל – התוכנית תומכת בסיומות הבאות: DBX (Outlook Express) ו-EML.

קובצי ארכיון – התוכנית תומכת בסיומות הבאות: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE ובסיומות רבות אחרות.

קובצי ארכיון בחילוץ עצמי – קובצי ארכיון בחילוץ עצמי (SFX) הם קובצי ארכיון שמסוגלים לחלץ את עצמם.

אורזים של זמן ריצה – לאחר הפעלתם, אורזים של זמן ריצה (בשונה מסוגי ארכיון רגילים) נחלצים בזיכרון. בנוסף לאורזים סטטיים רגילים (UPX, yoda, ASPack, FSG וכו'), הסורק מסוגל לזהות מספר סוגים נוספים של אורזים באמצעות הדמיית קוד.

אפשרויות סריקה
בחר באילו שיטות תתבצע סריקת המערכת לאיתור חדירות. האפשרויות הבאות זמינות:

היריסטיקה – היריסטיקה היא אלגוריתם המנתח את הפעילות (הזדונית) של תוכניות. היתרון העיקרי של טכנולוגיה זו הוא היכולת לזהות תוכנה זדונית שלא הייתה קיימת, או שלא כוסתה על-ידי מסד הנתונים הקודם של חתימות הווירוסים. החיסרון הוא הסתברות (נמוכה מאוד) של התראות שווא.

היריסטיקה מתקדמת/חתימות DNA – היריסטיקה מתקדמת היא אלגוריתם היריסטיקה ייחודי שפותח על-ידי ESET, שעבר אופטימיזציה לזיהוי תולעי מחשב וסוסים טרויאניים ונכתב בשפות תכנות ברמה גבוהה. השימוש בהיריסטיקה מתקדמת משפר במידה רבה את יכולות זיהוי האיומים של מוצרי ESET. החתימות מסוגלות לגלות ולזהות וירוסים בצורה מהימנה. באמצעות מערכת העדכון האוטומטית, חתימות חדשות זמינות בתוך שעות ספורות מרגע שהתגלה איום. חסרונן של החתימות הוא שהן מזהות רק וירוסים שהן מכירות (או גרסאות של הווירוסים הללו בשינוי קל).

ניקוי
הגדרות הניקוי קובעות את אופן פעולת הסורק בעת ניקוי קבצים נגועים. ישנן 3 רמות ניקוי:

ללא ניקוי – הקבצים הנגועים לא ינוקו אוטומטית. התוכנית תציג חלון אזהרה ותאפשר למשתמש לבחור פעולה. רמה זו תוכננה עבור

משתמשים מתקדמים יותר, שיודעים אילו שלבים לנקוט במקרה של חדירה.

ניקוי רגיל – התוכנית תנסה לנקות או למחוק קובץ נגוע בצורה אוטומטית, על-פי פעולה שהוגדרה מראש (בתלות בסוג החדירה). הודעה על זיהוי ומחיקה של קובץ נגוע מופיעה בפינה הימנית התחתונה של המסך. אם לא ניתן לבחור את פעולת התיקון באופן אוטומטי, התוכנית מספקת פעולות אחרות למעקב. אותו הדבר קורה כאשר לא ניתן להשלים פעולה שהוגדרה מראש.

ניקוי מחמיר – התוכנית תנקה או תמחק את כל הקבצים הנגועים. החריגות היחידות הן קובצי המערכת. אם לא ניתן לנקותם, המשתמש יונחה לבחור פעולה בחלון אזהרה.

אזהרה

אם ארכיון מסוים מכיל קובץ או קבצים נגועים, ישנן שתי אפשרויות לטיפול בארכיון. במצב הסטנדרטי (ניקוי רגיל), אם כל הקבצים הכלולים בארכיון נגועים, הארכיון כולו יימחק. במצב **ניקוי מחמיר**, הארכיון יימחק אם הוא מכיל לפחות קובץ נגוע אחד, ללא תלות במצבם של הקבצים האחרים בארכיון.

חריגות

סיומת היא החלק של שם הקובץ המופרד ממנו באמצעות נקודה. סיומת מגדירה את סוג הקובץ ותכולתו. מקטע זה של הגדרות פרמטר ThreatSense מאפשר לך להגדיר את סוגי הקבצים לסריקה.

אחר

בעת הגדרת התצורה של פרמטרי מנוע ThreatSense לסריקת מחשב לפי דרישה, האפשרויות הבאות במקטע **אחר** זמינות אף הן:

סריקת הזרמות נתונים חלופיות (ADS) – הנתונים החלופיות שבהן משתמשת מערכת הקבצים NTFS הן שיוכים של קובץ ותיקייה שאינם גלויים לשיטות סריקה רגילות. חדירות רבות מנסות להימנע מזיהוי על-ידי התחזות להזרמות נתונים חלופיות.

הפעלת סריקות ברקע עם עדיפות נמוכה – רצף סריקה צורך כמות מסוימת של משאבי מערכת. אם אתה עובד עם תוכניות שמטילות עומס גבוה על משאבי המערכת, באפשרותך להפעיל סריקה ברקע עם עדיפות נמוכה ולחסוך במשאבים עבור היישומים שלך.

רישום כל האובייקטים ביומן – אם אפשרות זו נבחרת, קובץ היומן יציג את כל הקבצים שנסרקו, גם אם אינם נגועים. לדוגמה, אם מתגלה חדירה בארכיון, יומן הרישום יכלול ברשימה גם את הקבצים הכלולים בארכיון.

אפשור מיטוב חכם – כאשר המיטוב החכם מופעל, המערכת משתמשת בהגדרות האופטימליות ביותר כדי להבטיח את רמת הסריקה היעילה ביותר יחד עם שמירה על מהירויות הסריקה הגבוהות ביותר. מודולי ההגנה השונים סורקים באופן חכם, תוך שימוש בשיטות סריקה שונות והחלתן על סוגי קבצים ספציפיים. אם המיטוב החכם מושבת, רק ההגדרות שקובע המשתמש בליבת ThreatSense של המודולים המסוימים מוחלות בעת ביצוע סריקה.

שמירת חותמת זמן של הגישה האחרונה – בחר באפשרות זו כדי לשמור על זמן הגישה המקורי של קבצים שנסרקו במקום לעדכן אותו (לדוגמה, לשימוש עם מערכות גיבוי נתונים).

הגבלות

מקטע ההגבלות מאפשר לך לציין את הגודל המרבי של אובייקטים ורמות הארכיונים המקוננים שיש לסרוק:

הגדרות אובייקטים

גודל אובייקט מרבי – הגדרת הגודל המרבי של אובייקטים שייסרקו. במצב זה, מודול האנטי-וירוס הנתון יסרוק רק אובייקטים שקטנים מהגודל שצוין. את האפשרות הזו אמורים לשנות רק משתמשים מתקדמים, שעשויות להיות להם סיבות ספציפיות לאי-הכללת קבצים גדולים בסריקה. ערך ברירת המחדל: ללא הגבלה.

זמן סריקה מרבי לאובייקט (שניות) – הגדרת ערך הזמן המרבי לסריקה של אובייקט. אם ערך המוגדר על-ידי משתמש הוזן כאן, מודול האנטי-וירוס יפסיק סריקה של אובייקט לאחר שזמן זה יחלוף, בין אם הסריקה הסתיימה ובין אם לא הסתיימה. ערך ברירת המחדל: ללא הגבלה.

הגדרות סריקת ארכיון

רמת קינון ארכיון – העומק המרבי של סריקת הארכיון. ערך ברירת המחדל: 10.

הגודל המרבי של קובץ בארכיון – עם אפשרות זו אתה יכול לציין את גודל הקובץ המרבי עבור קבצים הנכללים בארכיונים (בעת חילוצם) שאותם יש לסרוק. ערך ברירת המחדל: ללא הגבלה.

הערה
לא מומלץ לשנות את ערכי ברירת המחדל; בנסיבות רגילות לא צריכה להיות סיבה לשנותם.

סיומות קבצים שלא ייכללו בסריקה

סיומת היא החלק של שם הקובץ המופרד ממנו באמצעות נקודה. סיומת מגדירה את סוג הקובץ ותכולתו. מקטע זה של הגדרות פרמטר ThreatSense מאפשר לך להגדיר את סוגי הקבצים לסריקה.

הערה
אל תתבלבל עם אי הכללת תהליכים, אי הכללות HIPS או אי הכללות קובץ/תיקייה.

כברירת מחדל, כל הקבצים נסרקים. ניתן להוסיף כל סיומת לרשימת הקבצים שלא ייכללו בסריקה.

לעתים הכרחי לא לכלול קבצים, וזאת כאשר סריקת סוגי קבצים מסוימים מונעת מהתוכנית שמשתמשת באותן סיומות מלפעול כהלכה. לדוגמה, מומלץ שלא לכלול את הסיומות .edb, .eml ו-.tmp בעת שימוש בשרתי Microsoft Exchange.

דוגמה
כדי להוסיף סיומת חדשה לרשימה, לחץ על **הוסף**. הקלד את הסיומת בשדה הריק (לדוגמה tmp) ולחץ על **אישור**. כאשר אתה בוחר **הזן ערכים מרובים**, באפשרותך להוסיף מספר סיומות קבצים, שביניהן מפרידים קווים, פסיקים או סימני נקודה-פסיק (לדוגמה, בחר מהתפריט הנפתח **נקודה-פסיק** כמפריד והקלד tmp;eml;edb).
באפשרותך להשתמש בסימן מיוחד ? (סימן שאלה). סימן השאלה מייצג כל סמל שהוא (לדוגמה, db?).

הערה
כדי לראות את הסיומת המדויקת (אם ישנה) של קובץ במערכת ההפעלה Windows עליך לבטל את סימון האפשרות **הסתר סיומות של סוגי קבצים מוכרים** תחת **לוח הבקרה** > **אפשרויות תיקיה** > **תצוגה** (כרטיסיה) ולהחיל שינוי זה.

זוהתה חדירה

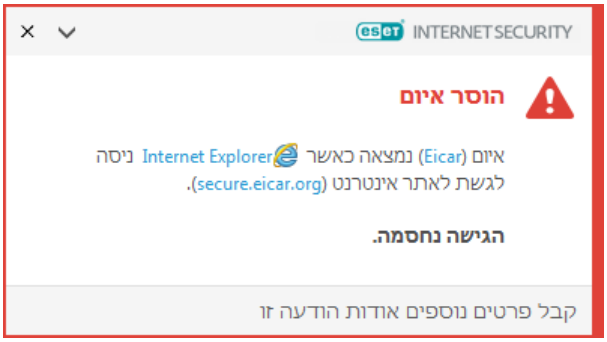
חדירות יכולות להגיע למערכת מנקודות כניסה שונות, כגון דפי אינטרנט, תיקיות משותפות, דרך הדואר האלקטרוני או ממכשירים נשלפים (USB, דיסקים חיצוניים, תקליטורים, DVD, דיסקטים וכו').

אופן הפעולה הרגיל

דוגמה כללית לאופן הטיפול של ESET Internet Security בחדירות היא שניתן לזהות את החדירות באמצעות:

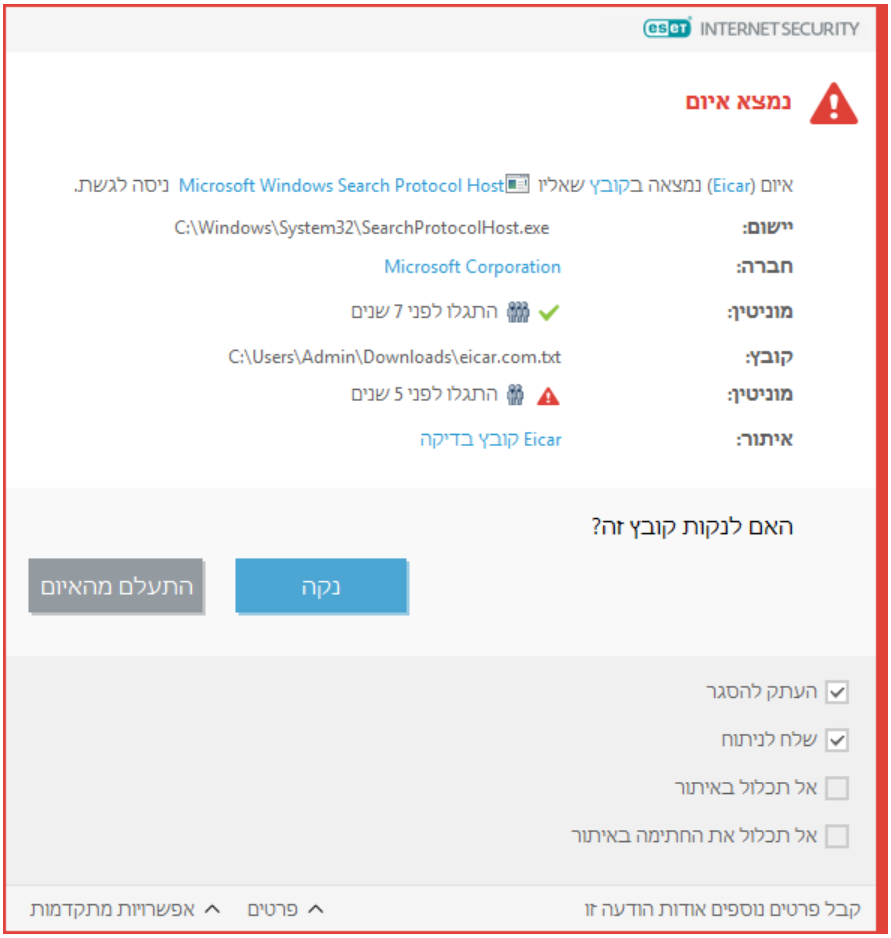
- הגנה בזמן אמת על מערכת קבצים
- הגנה על גישה לאינטרנט
- הגנת לקוח דוא"ל
- סריקת מחשב לפי דרישה

כל אחד מהכלים הללו משתמש ברמת ניקוי סטנדרטית, וינסה לנקות את הקובץ ולהעבירו להסגר או לסיים את החיבור. יוצג חלון הודעות באזור ההודעות שבפינה הימנית התחתונה של המסך. לקבלת מידע נוסף על רמות הניקוי ואופן הפעולה, ראה ניקוי.



ניקוי ומחיקה

אם אין פעולה מוגדרת מראש שאותה יש לנקוט להשגת הגנה על מערכת קבצים בזמן אמת, תונחה לבחור אפשרות בחלון ההתראה. בדרך-כלל זמינות האפשרויות האפשרויות **ניקוי**, **מחיקה** ו**ללא פעולה**. לא מומלץ לבחור באפשרות **ללא פעולה**, מפני שכך קבצים נגועים לא ינוקו. המצב החריג הוא כאשר אתה בטוח שקובץ מסוים אינו מזיק וזוהה בשוגג.



החל את הניקוי כאשר קובץ מסוים הותקף על-ידי וירוס, שהצמיד לקובץ קוד זדוני. אם זהו המקרה, תחילה נסה לנקות את הקובץ הנגוע כדי לשחזר את מצבו המקורי. אם הקובץ כולל קוד זדוני בלבד, הוא יימחק.

אם קובץ נגוע מסוים "נעול" או נמצא בשימושו של תהליך מערכת, הוא בדרך-כלל יימחק לאחר שישוחרר (בדרך-כלל בעקבות הפעלה מחדש של המערכת).

מספר איומים

אם קבצים נגועים מסוימים לא נוקו במהלך סריקת המחשב (או אם רמת הניקוי הוגדרה כ**ללא ניקוי**), יוצג חלון התראה המנחה אותך לבחור את הפעולות שיוחלו על קבצים אלה. בחר את הפעולות עבור הקבצים (הפעולות מוגדרות עבור כל אחד מהקבצים ברשימה בנפרד) ולאחר מכן לחץ על **סיום**.

מחיקת קבצים בארכיונים

במצב הניקוי שנקבע כברירת מחדל, הארכיון כולו יימחק רק אם הוא מכיל קבצים נגועים בלבד, ואין בו קבצים נקיים. במילים אחרות, ארכיונים אינם נמחקים אם הם מכילים גם קבצים נקיים שאינם מזיקים. היזהר כשאתה מבצע סריקה עם ניקוי מחמיר, מפני שכאשר ניקוי מחמיר מופעל - ארכיון יימחק אם הוא מכיל לפחות קובץ נגוע אחד, ללא תלות במצבם של הקבצים האחרים בארכיון.

אם במחשב שלך מופיעים סימנים של הדבקה בתוכנה זדונית, למשל האטה בפעילות, או חוסר תגובה לעתים קרובות, מומלץ לבצע את הפעולות הבאות:

1. פתח את ESET Internet Security **ולחץ על 'סריקת מחשב'**
2. לחץ על **סרוק את המחשב שלך** (לקבלת מידע נוסף ראה סריקת מחשב)
3. בסיום הסריקה, סקור את היומן הכולל את מספר הקבצים שנסרקו, שנפגעו ושנוקו.

אם ברצונך לסרוק רק חלק מסוים מהדיסק, לחץ על **סריקה מותאמת אישית** ובחר יעדים שייסרקו לאיתור וירוסים.

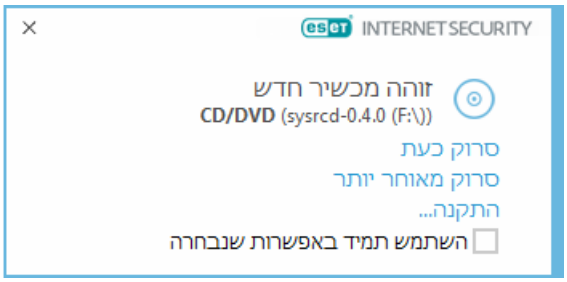
מדיה נשלפת

ESET Internet Security מספק סריקה אוטומטית של מדיה נשלפת (CD/DVD/USB/...). מודול זה מאפשר לך לסרוק מדיה שהוכנסה. אפשרות זו שימושית כאשר מנהל המערכת של המחשב מעוניין למנוע מהמשתמשים להשתמש במדיה נשלפת עם תוכן שלא התבקש.

הפעולה שיש לנקוט לאחר הכנסת מדיה נשלפת - בחר את פעולת ברירת המחדל שתבוצע בעת הכנסה של התקן מדיה נשלפת למחשב (CD/DVD/USB). אם האפשרות **הצג אפשרויות סריקה** נבחרת, תוצג הודעה המאפשרת לך לבחור פעולה מבוקשת:

- **אל תסרוק** – לא תבוצע אף פעולה והחלון **זוהה מכשיר חדש** ייסגר.
- **סריקת מכשיר אוטומטית** – תבוצע סריקת מחשב לפי דרישה של התקן המדיה הנשלפת שהוכנס.
- **הצג אפשרויות סריקה** – פתיחת מקטע הגדרות המדיה הנשלפת.

בעת הכנסה של מדיה נשלפת יוצג חלון הדו-שיח הבא:



סרוק עכשיו – פעולה זו תפעיל סריקה של המדיה הנשלפת.

סרוק מאוחר יותר – סריקת המדיה הנשלפת תושהה.

הגדרות – פתיחת ההגדרות המתקדמות.

השתמש תמיד באפשרות שנבחרה – כאשר אפשרות זו נבחרת, אותה פעולה תבוצע בפעם אחרת שבה תוכנס מדיה נשלפת.

בנוסף, ESET Internet Security כולל את פונקציונליות בקרת ההתקנים, אשר מאפשרת לך להגדיר כללים לשימוש בהתקנים חיצוניים במחשב נתון. פרטים נוספים על בקרת התקנים ניתן למצוא במקטע בקרת התקנים.

הגנה על מסמכים

תכונת ההגנה על מסמכים סורקת את מסמכי Microsoft Office לפני פתיחתם, וכן קבצים ש-Internet Explorer מוריד אוטומטית, כגון רכיבי Microsoft ActiveX. הגנה על מסמכים מספקת שכבת הגנה המתווספת להגנה בזמן אמת על מערכת קבצים, וניתן להשביתה כדי לשפר את הביצועים במערכות שאינן מטפלות במסמכי Microsoft Office רבים.

כדי להפעיל הגנה על מסמכים, פתח את החלון **הגדרות מתקדמות** (הקש F5) > **מנגנון איתור** > **סריקות לאיתור תוכנות זדוניות** >

הגנה על מסמכים ולחץ על המתג **שלב במערכת**.

הערה
תכונה זו מופעלת על-ידי יישומים המשתמשים ב-Antivirus API של Microsoft (לדוגמה Microsoft Office 2000 ואילך או Microsoft Internet Explorer 5.0 ואילך).

בקרת התקנים

בקרת התקנים

ESET Internet Security מספק בקרה אוטומטית של התקנים (.../CD/DVD/USB). מודול זה מאפשר לך לחסום או להתאים הרשאות/מסננים מורחבים ולהגדיר את יכולת המשתמשים לגשת להתקן נתון ולעבוד אתו. אפשרות זו שימושית כאשר מנהל המערכת של המחשב רוצה למנוע את השימוש בהתקנים המכילים תוכן שלא התבקש.

ההתקנים החיצוניים הנתמכים:

- אחסון בדיסק (HDD, דיסק נשלף בחיבור USB)
- תקליטור/dvd
- מדפסת USB
- אחסון בחיבור FireWire
- התקן Bluetooth
- קורא כרטיסים חכמים
- התקן הדמיה
- מודם
- יציאה LPT/COM
- התקן נייד
- כל סוגי ההתקנים

את אפשרויות ההגדרה של בקרת ההתקנים ניתן לשנות תחת **הגדרות מתקדמות** (F5) > **בקרת התקנים**.

העברת המתג שליד **שלב במערכת** למצב פעיל מפעילה את תכונת בקרת ההתקנים במוצר ESET Internet Security; כדי ששינוי זה ייכנס לתוקף עליך להפעיל מחדש את המחשב. לאחר שבקרת ההתקנים הופעלה, ה**כללים** יהפכו לפעילים ויאפשרו לך לפתוח את חלון עורך הכללים.

הערה
באפשרותך ליצור קבוצות התקנים שונות, שבהן יוחלו כללים שונים. באפשרותך גם ליצור רק קבוצת התקנים אחת שבה יוחל הכלל עם הפעולה **קריאה/כתיבה** או **קריאה בלבד**. כך תובטח חסימה של התקנים בלתי מזוהים על-ידי בקרת ההתקנים, בעת חיבורם למחשב.

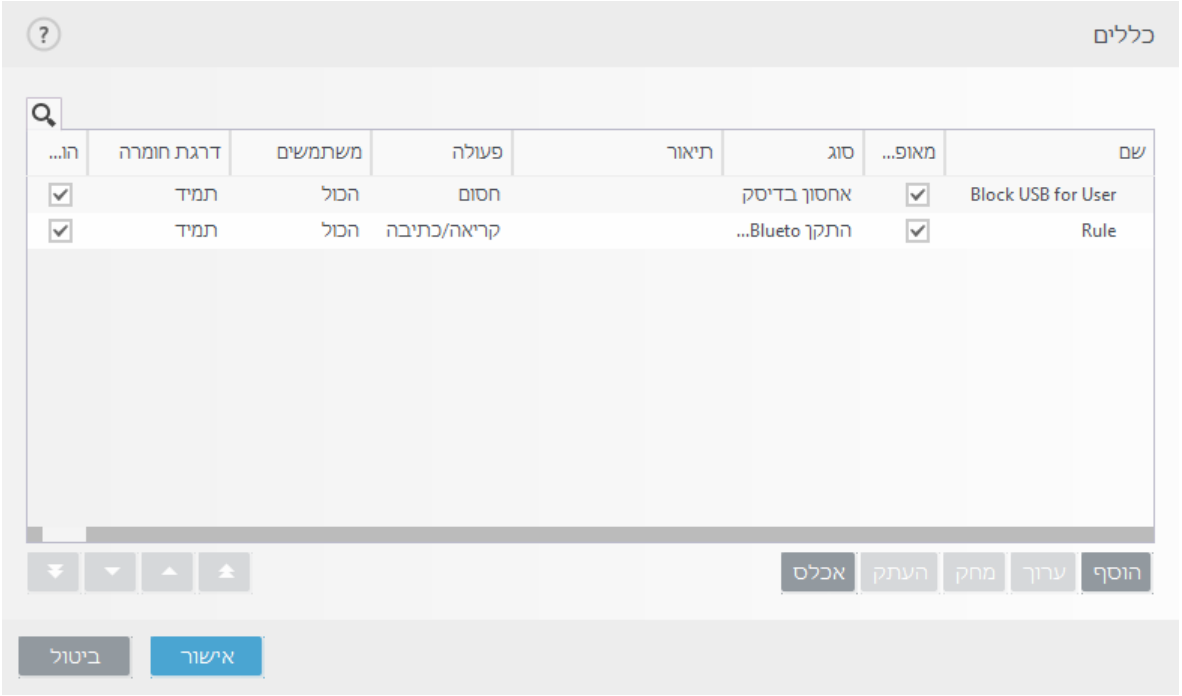
אם חובר התקן שנחסם על-ידי כלל קיים, יוצג חלון הודעה ולא תוענק גישה להתקן.

הגנת מצלמת אינטרנט

העברת המתג שליד **שלב במערכת** למצב פעיל מפעילה את תכונת ההגנה על מצלמת אינטרנט ב- ESET Internet Security. לאחר שההגנה על מצלמת האינטרנט הופעלה, ה**כללים** יהפכו לפעילים ויאפשרו לך לפתוח את חלון עורך הכללים.

עורך כללי בקרת התקנים

החלון **עורך כללי בקרת התקנים** מציג את הכללים הקיימים ומאפשר שליטה מדויקת בהתקנים חיצוניים שהמשתמשים מחברים למחשב.



ניתן להתיר או לחסום התקנים מסוימים לכל משתמש או קבוצת משתמשים ובהתאם לפרמטרים נוספים של ההתקן, אותם ניתן לפרט בתצורת הכלל. רשימת הכללים מכילה מספר תיאורים של כלל, כגון שם, סוג התקן חיצוני, פעולה לביצוע לאחר חיבור התקן חיצוני למחשב וחומרת היומן.

לחץ על **הוסף** או על **ערוך** כדי לנהל כלל. לחץ על **העתק** כדי ליצור כלל חדש עם אפשרויות מוגדרות מראש, שנמצאות בשימוש בכלל אחר שנבחר. את הגדרות ה-XML שמוצגות כאשר לוחצים על כלל מסוים ניתן להעתיק ללוח, כדי לסייע למנהלי המערכת לייצא/לייבא את הנתונים הללו ולהשתמש בהם, לדוגמה ב-.

באמצעות הקשה על **CTRL** ולחיצה, באפשרותך לבחור מספר כללים ולהחיל פעולות, למשל מחיקה או הזזה שלהן מעלה/מטה ברשימה, על כל הכללים שנבחרו. תיבת הסימון **מופעל** משביתה או מפעילה כלל; שימושית כשאינך מעוניין למחוק כלל לצמיתות, למקרה שתרצה להשתמש בו בעתיד.

הבקרה מושגת באמצעות כללים שממוינים בסדר הקובע את עדיפותם, כאשר הכללים בעלי העדיפות הגבוהה יותר נמצאים למעלה.

את הזנות יומן הרישום ניתן לראות מהחלון הראשי של ESET Internet Security, תחת **כלים** > **כלים נוספים** > רשומות יומן.

יומן בקרת ההתקנים מתעד את כל המופעים שבהם בקרת ההתקנים מופעלת.

התקנים שאותרו

הלחצן **אכלס** מספק סקירה כללית של כל המכשירים המחוברים כעת, בתוספת מידע על: סוג המכשיר, ספק המכשיר, הדגם והמספר הסידורי (אם זמינים).

אם נבחר התקן מסוים (מתוך רשימת התקנים שזוהו) ונלחצה האפשרות **אישור**, מופיע חלון עורך כללים עם מידע שהוגדר מראש (ניתן להתאים את כל ההגדרות).

קבוצות התקנים

אזהרה
התקן המחובר למחשב שלך עלול לחשוף אותו לסיכון אבטחה.

חלון קבוצות ההתקנים מחולק לשני חלקים. החלק הימני של החלון כולל רשימת התקנים המשתייכים לקבוצה תואמת, והחלק השמאלי של החלון כולל את הקבוצות שנוצרו. בחר את הקבוצה עם רשימת ההתקנים שברצונך להציג בחלונית הימנית.

כאשר אתה פותח את חלון קבוצות ההתקנים ובוחר קבוצה, באפשרותך להוסיף או להסיר התקנים מהרשימה. דרך אחרת להוסיף

התקנים לקבוצה היא לייבא אותם מתוך קובץ. לחלופין באפשרותך ללחוץ על הלחצן **אכלס**, וכל ההתקנים המחוברים למחשב שלך יפורטו בחלון **התקנים שזוהו**. בחר את ההתקנים מתוך הרשימה המאוכלסת כדי להוסיפה לקבוצה על-ידי לחיצה על **אישור**.

רכיבי בקרה

הוספה – באפשרותך להוסיף קבוצה על-ידי הזנת שמה, או התקן לקבוצה קיימת (קיימת אופציה לציין פרטים, כגון שם ספק, דגם ומספר סידורי), בתלות בחלק של החלון שבו לחצת על הלחצן.

עריכה – מאפשרת לך לשנות את של קבוצה שנבחרה או של פרמטרים של התקן (ספק, דגם, מספר סידורי).

הסר – מוחקת את הקבוצה או ההתקן שנבחרו, בתלות בחלק של החלון שבו לחצת על הלחצן.

ייבוא – מייבא רשימת התקנים מקובץ.

הלחצן **אכלס** מספק סקירה כללית של כל המכשירים המחוברים כעת, בתוספת מידע על: סוג המכשיר, ספק המכשיר, הדגם והמספר הסידורי (אם זמינים).

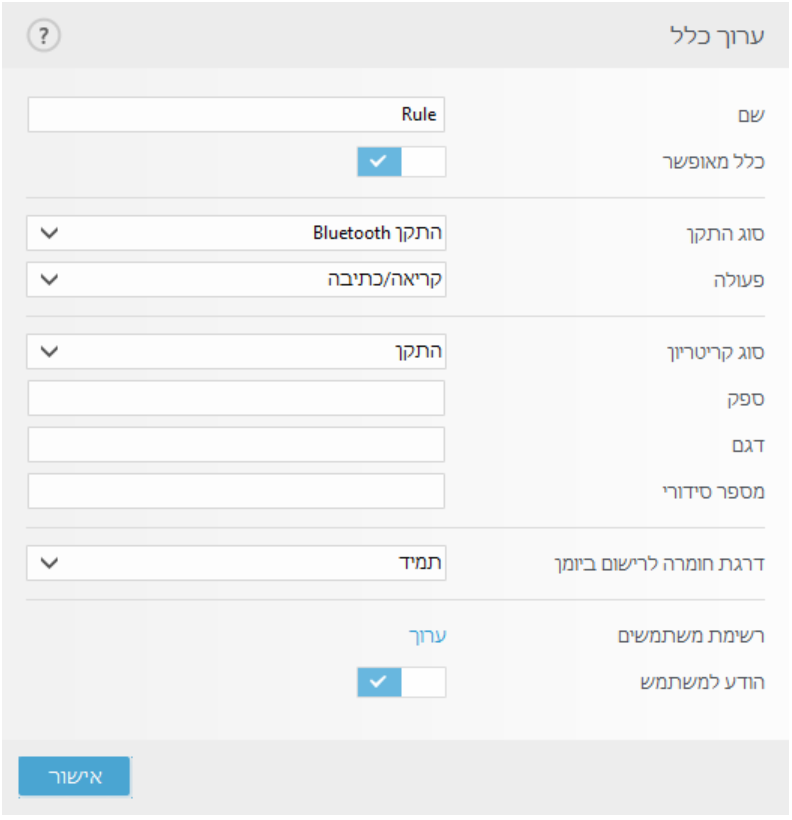
לאחר שתסיים את ההתאמה האישית לחץ על **אישור**. לחץ על **ביטול** אם ברצונך לצאת מהחלון **קבוצות התקנים** מבלי לשמור את השינויים.

> **הערה**
> באפשרותך ליצור קבוצות התקנים שונות, שבהן יוחלו כללים שונים. באפשרותך גם ליצור רק קבוצת התקנים אחת שבה יוחל הכלל עם הפעולה **קריאה/כתיבה** או **קריאה בלבד**. כך תובטח חסימה של התקנים בלתי מזוהים על-ידי בקרת ההתקנים, בעת חיבורם למחשב.

שים לב שכל הפעולות (ההרשאות) זמינות עבור כל סוגי המכשירים. אם זהו מכשיר מסוג אחסון, כל ארבע הפעולות זמינות. עבור מכשירים שאינם מסוג אחסון, זמינות רק שלוש אפשרויות (לדוגמה האפשרות **קריאה בלבד** אינה זמינה עבור Bluetooth, ולכן מכשירי Bluetooth ניתן רק להתיר, לחסום או להזהיר).

הוספת כללי בקרת התקנים

כלל בקרת התקנים מגדיר את הפעולה שתינקט כאשר התקן מסוים שעומד בקריטריונים של הכלל מחובר למחשב.



לזיהוי טוב יותר, הזן תיאור של הכלל בשדה **שם**. לחץ על המתג שליד **כלל מופעל** כדי להפעיל או להשבית כלל זה; מצב זה שימושי

כשאינך רוצה למחוק את הכלל לצמיתות.

סוג התקן

בחר את סוג ההתקן החיצוני בתפריט הנפתח (אחסון בדיסק/התקן נייד/FireWire/Bluetooth/...). מידע על סוג ההתקן נאסף ממערכת ההפעלה וניתן לראותו במנהל ההתקנים של המערכת, כאשר התקן מחובר למחשב. התקני אחסון כוללים דיסקים חיצוניים או קוראי כרטיסי זיכרון רגילים המחוברים באמצעות USB או FireWire. קוראי כרטיסים חכמים כוללים את כל קוראי הכרטיסים החכמים שמוטבע בהם מעגל משולב, כגון כרטיסי SIM או כרטיסי אימות. דוגמאות להתקני הדמיה כוללות סורקים או מצלמות. מאחר שהתקנים אלה מספקים מידע רק על הפעולות שלהם ולא על המשתמשים, ניתן לחסום אותם רק באופן גלובלי.

פעולה

את הגישה להתקן שאינו התקן אחסון ניתן להתיר או לחסום. לעומת זאת, כללים להתקני אחסון מאפשרים לך לבחור את או יותר מההגדרות הבאות המתייחסות לזכויות:

- **קריאה/כתיבה** - תותר גישה מלאה להתקן.
- **חסימה** - הגישה להתקן תיחסם.
- **קריאה בלבד** - תותר גישת קריאה להתקן.
- **אזהרה** - בכל פעם שמחובר התקן כלשהו, המשתמש יקבל הודעה אם הוא מותר/חסום, וכן יתבצע רישום ביומן. המערכת אינה זוכרת את ההתקנים, והודעה תמשיך להופיע בחיבורים עתידיים של אותו התקן.

שים לב שכל הפעולות (ההרשאות) זמינות עבור כל סוגי המכשירים. אם זהו מכשיר מסוג אחסון, כל ארבע הפעולות זמינות. עבור מכשירים שאינם מסוג אחסון, זמינות רק שלוש אפשרויות (לדוגמה האפשרות **קריאה בלבד** אינה זמינה עבור Bluetooth, ולכן מכשירי Bluetooth ניתן רק להתיר, לחסום או להזהיר).

סוג קריטריונים - בחר קבוצת התקנים או התקן.

ניתן להשתמש בפרמטרים הבאים, המוצגים להלן, לצורך התאמה מפורטת של כללים להתקנים. כל הפרמטרים תלויי-רישיות:

- **ספק** – סינון לפי שם הספק או ה-ID שלו.
- **דגם** - השם הנתון של ההתקן.
- **מספר סידורי** – להתקנים חיצוניים יש בדרך-כלל מספרים סידוריים משלהם. במקרה של תקליטורCD/DVD, זהו המספר הסידורי של המדיה הנתונה, ולא של כונן ה-CD.

> **הערה**
> אם הפרמטרים הללו אינם מוגדרים, הכלל יתעלם משדות אלו בעת ביצוע ההתאמה. פרמטרי הסינון בכל שדות הטקסט הם תלויי-רישיות ואין תמיכה בתווים כלליים (*, ?).

> **הערה**
> להצגת מידע על התקן כלשהו, צור כלל עבור סוג התקן זה, חבר את ההתקן למחשב ואז בדוק את פרטי ההתקן ביומן בקרת ההתקנים.

רישום החומרה ביומן

ESET Internet Security שומר את כל האירועים החשובים בקובץ יומן, אותו ניתן להציג ישירות מהתפריט הראשי. לחץ על **כלים** > **כלים נוספים** **רשומות יומן** ואז בחר באפשרות **בקרת התקנים** בתפריט הנפתח **יומן**.

- **תמיד** - רישום כל האירועים.
- **אבחוני** - רישום מידע שנדרש להתאמה מפורטת של התוכנית.
- **מידע** - תיעוד הודעות מסירת מידע, לרבות הודעות על עדכון מוצלח, בנוסף לכל הרשומות שלעיל.
- **אזהרה** - תיעוד שגיאות קריטיות והודעות אזהרה.
- **ללא** - לא יתועדו יומנים.

את הכללים ניתן להגביל למשתמשים מסוימים או לקבוצות משתמשים מסוימות, על-ידי הוספתם ל**רשימת המשתמשים**:

- **הוספה** - פתיחת חלון הדו-שיח **סוגי אובייקטים: משתמשים או קבוצות** המאפשר לך לבחור את המשתמשים הרצויים.
- **הסר** - הסרת המשתמש שנבחר מהמסנן.

> **הערה**
> את כל ההתקנים ניתן לסנן לפי כללי משתמש (לדוגמה התקני הדמיה אינם מספקים מידע על משתמשים אלא רק על פעולות).

עורך כללי הגנת מצלמת אינטרנט

חלון זה מציג את הכללים הקיימים ומאפשר לשלוט ביישומים ובתהליכים שניגשים למצלמת האינטרנט של המחשב שלך בהתאם לפעולה שאתה מבצע.

הפעולות הבאות זמינות:

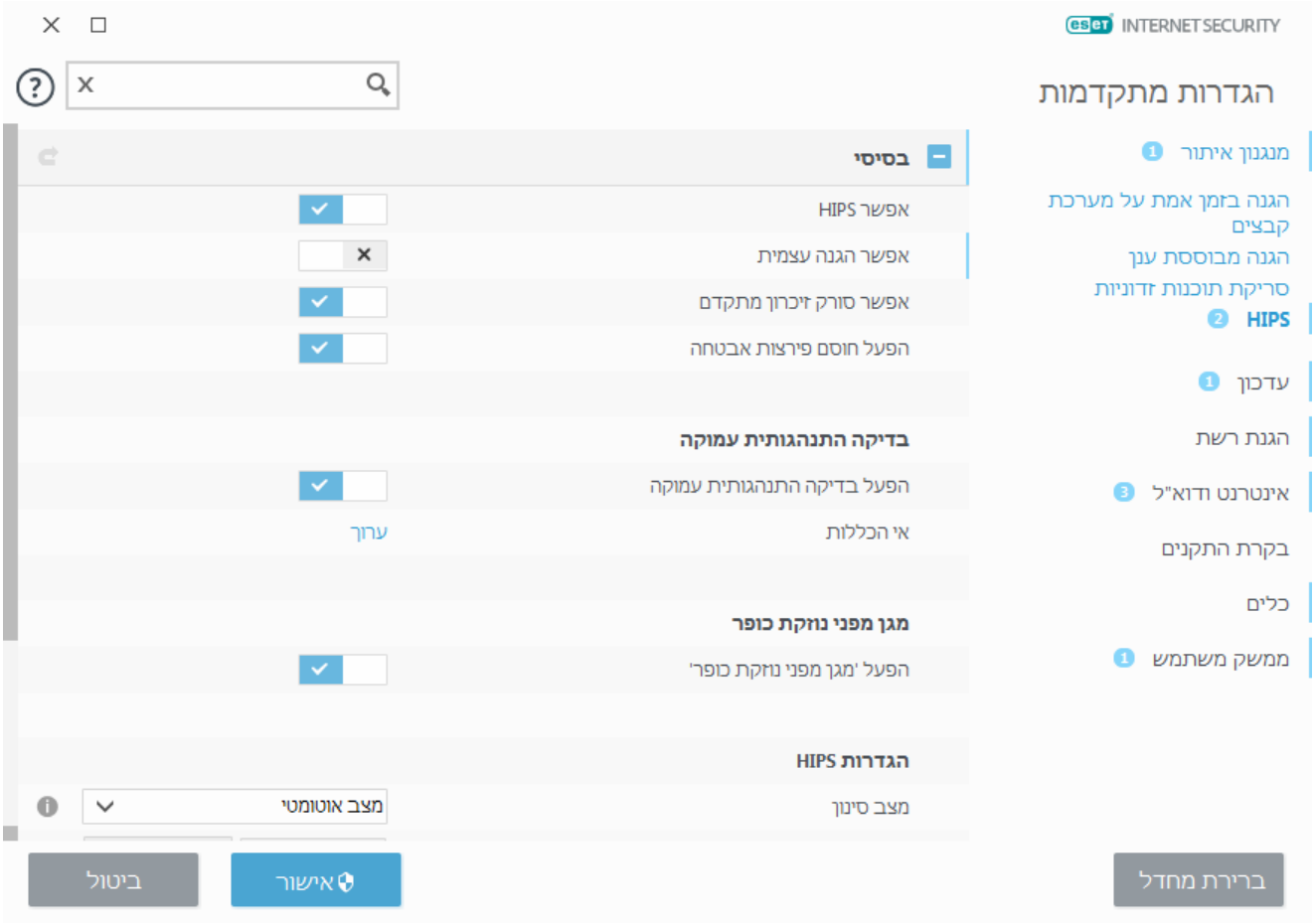
- **חסום גישה**
- **שאל בכל פעם**
- **אפשר גישה**

מערכת להגנה מפני חדירה למחשב מארח (HIPS)

> **אזהרה**
> שינויים בהגדרות של HIPS יבוצעו רק על-ידי משתמש מנוסה. קביעה שגויה של הגדרות HIPS עלולה להוביל לאי-יציבות של המערכת.

המערכת להגנה מפני חדירה למחשב מארח (HIPS) מגנה על המערכת שלך מפני תוכנות זדוניות ופעילויות בלתי רצויות המנסות להשפיע על המחשב שלך באופן שלילי. HIPS משתמש בניתוח פעילות מתקדם, המשולב ביכולות הזיהוי של סינון רשת, כדי לפקח על תהליכים פועלים, קבצים ומפתחות רישום. HIPS היא מערכת נפרדת מההגנה על מערכת קבצים בזמן אמת, ואינה חומת אש; היא אך ורק מנטרת את התהליכים הפועלים בתוך מערכת ההפעלה.

ההגדרות של HIPS נמצאות תחת **הגדרות מתקדמות**(F5) > **מנגנון איתור** > **HIPS** > **בסיסי**. המצב של HIPS (מופעלת/מושבתת) מוצג בחלון התוכנית הראשי של ESET Internet Security, תחת **הגדרות** > **הגנה על המחשב**.



בסיסי

אפשר HIPS – HIPS מאופשר כברירת מחדל ב-ESET Internet Security. השבתת HIPS תשבית את שאר התכונות של HIPS כמו 'חוסם פירצות אבטחה'.

אפשר הגנה עצמית – ESET Internet Security משתמש בטכנולוגיית **הגנה עצמית** המוכללת כחלק מ-HIPS כדי למנוע מתוכנות זדוניות מלהשחית או להשבית את הגנת האנטי וירוס וההגנה מפני תוכנות ריגול. ההגנה העצמית מגינה על תהליכים חיוניים של המערכת ושל ESET, מפתחות הרישום וקבצים מפני טיפול שלא כדין.

אפשר שירות מוגן – מאפשר הגנת ליבה (אפשרות זו זמינה ב-Windows 8.1 וב-Windows 10).

אפשר סורק זיכרון מתקדם פועל בשילוב עם 'חוסם פירצות אבטחה' כדי לחזק את ההגנה מפני תוכנות זדוניות שתוכננו להתחמק מהמוצרים למניעת תוכנות זדוניות באמצעות הסתרה או הצפנה. סורק זיכרון מתקדם זמין כברירת מחדל. קרא עוד על סוג ההגנה הזה במילון.

אפשר חוסם פירצות אבטחה - תוכנן לחזק סוגי אפליקציות שמרבים לנצלן, כגון דפדפני אינטרנט, קוראי PDF, לקוחות דוא"ל ורכיבים של MS Office. חוסם פירצות אבטחה מופעל כברירת מחדל. קרא עוד על סוג ההגנה הזה במילון.

בדיקה התנהגותית עמוקה

אפשר בדיקה התנהגותית עמוקה - שכבה נוספת של הגנה שפועלת כחלק מהתכונה HIPS. הרחבה זו של HIPS מנתחת את אופן הפעולה של כל התכניות הפועלות במחשב ומזהירה אותך אם אופן הפעולה של התהליך זדוני.

אי הכללות HIPS מבדיקה התנהגותית עמוקה מאפשרות לך לא לכלול תהליכים בניתוח. כדי לוודא שכל התהליכים ייסרקו לבדיקת איומים אפשריים, מומלץ ליצור אי הכללות רק כשהדבר הכרחי.

הגנה מפני נוזקות כופר

אפשר הגנה מפני נוזקות כופר - שכבת הגנה נוספת הפועלת כחלק מתכונת HIPS. כדי שההגנה מפני נוזקות כופר תופעל, על מערכת

המוניטין ESET LiveGrid® להיות זמינה. קרא עוד על סוג ההגנה הזה.

הגדרות HIPS

מצב סינון ניתן לביצוע באחד מתוך ארבעה מצבים:

- **מצב אוטומטי** – פעולות מתאפשרות, להוציא אלו שנחסמו באמצעות כללים מוגדרים מראש שמגנים על המערכת שלך.
- **מצב חכם** – המשתמש יקבל הודעה רק על אירועים חשודים מאוד.
- **מצב אינטראקטיבי** – המשתמש יונחה לאשר את הפעולות.
- **מצב מבוסס-מדיניות** – הפעולות נחסמות.
- **מצב למידה** – הפעולות מתאפשרות ולאחר כל פעולה נוצר כלל. את הכללים הנוצרים במצב זה ניתן להציג בעורך הכללים, אולם העדיפות שלהם נמוכה מזו של כללים שנוצרו ידנית או כללים שנוצרו במצב אוטומטי. כשאתה בוחר מצב למידה בתפריט הנפתח של מצב סינון HIPS, ההגדרה **מצב הלמידה יסתיים ב** הופכת לזמינה. בחר את טווח הזמן שבו תרצה שמצב הלמידה יופעל, לכל היותר 14 ימים. אחרי שמשך הזמן שצוין יחלוף, תונחה לערוך את הכללים שנוצרו על-ידי HIPS כשהיה במצב למידה. באפשרותך גם לבחור מצב סינון אחר, או להשהות את ההחלטה ולהמשיך להשתמש במצב למידה.

המצב נקבע לאחר סיום מצב למידה – בחר את מצב הסינון שבו ייעשה שימוש לאחר שתוקף מצב הלמידה יפוג.

מערכת HIPS מנטרת אירועים בתוך מערכת ההפעלה ומגיבה בהתאם, על-בסיס כללים הדומים לאלה שבהם משתמשת חומת האש. לחץ על **עריכה** שליד **כללים** כדי לפתוח את חלון ניהול הכללים של HIPS. בחלון הכללים של HIPS תוכל לבחור, להוסיף, לערוך או להסיר כללים. פרטים נוספים על יצירת כללים ופעולות HIPS ניתן למצוא בעריכת כלל HIPS.

חלון אינטראקטיבי של HIPS

חלון ההתראה של HIPS מאפשר לך ליצור כלל המבוסס על פעולות חדשות ש-HIPS מזהה, ולאחר מכן להגדיר את התנאים שבהם יש לאשר או למנוע פעולה זו.

כללים הנוצרים מחלון ההתראות נחשבים כשווי-ערך לכללים שנוצרו ידנית. כלל שנוצר מחלון התראות יכול להיות פחות ספציפי מהכלל שהפעיל את אותו חלון דו-שיח. פירוש הדבר שאחרי יצירה של כלל בתיבת הדו-שיח, אותה פעולה יכולה להפעיל את אותו חלון. לקבלת מידע נוסף, ראה עדיפות עבור כללי HIPS.

אם הפעולה שהוגדרה כברירת מחדל עבור כלל היא **שאל בכל פעם**, חלון דו-שיח יוצג בכל פעם שכלל זה מופעל. תוכל לבחור **למנוע** או **לאפשר** את הפעולה. אם לא תבחר פעולה כלשהי בזמן הנתון, הפעולה החדשה תיבחר בהתאם לכללים.

האפשרות **זכור עד ליציאה מהיישום** גורמת לשימוש בפעולה (**אישור/מניעה**) עד שיבוצעו שינוי של הכללים או מצב הסינון, עדכון של מודול HIPS או הפעלה מחדש של המערכת. אחרי כל אחת משלוש הפעולות הללו, הכללים הזמניים יימחקו.

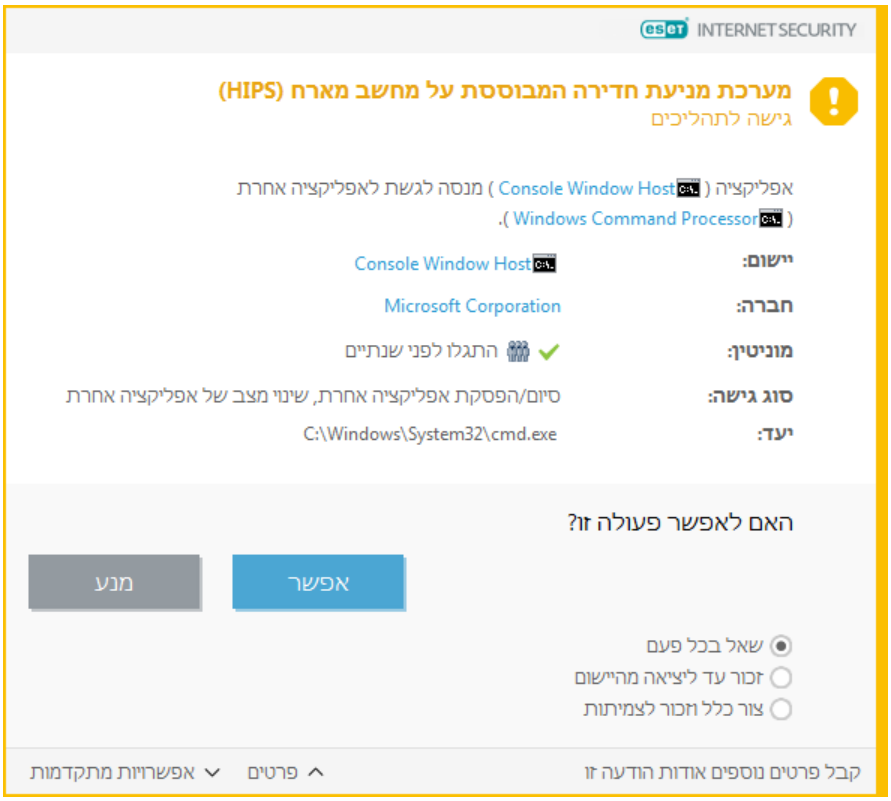
האפשרות **צור כלל וזכור לצמיתות** תיצור כלל HIPS חדש שניתן לשנותו לאחר מכן במקטע ניהול הכללים של HIPS (נדרשות הרשאות ניהול).

לחץ על **פרטים** בחלק התחתון כדי לראות איזו אפליקציה מפעילה את הפעולה, מה המוניטין של הקובץ או איזה סוג פעולה אתה מתבקש לאפשר או לדחות.

ניתן לגשת להגדרות עבור פרמטרי הכללים המפורטים יותר על-ידי לחיצה על **אפשרויות מתקדמות**. האפשרויות הבאות זמינות אם תבחר **צור כלל וזכור לצמיתות**:

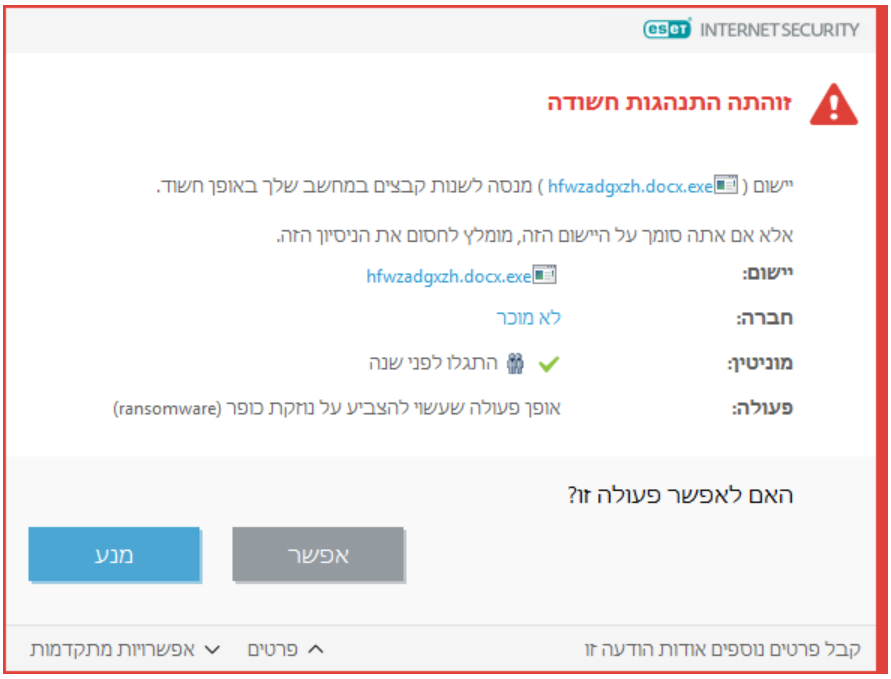
- **צור כלל התקף עבור אפליקציה זו בלבד** – אם תבטל את הבחירה בתיבת סימון זו, הכלל ייווצר עבור כל אפליקציות המקור.
- **עבור פעולה בלבד** – בחר את פעולות הקובץ/האפליקציה/הרישום של הכלל. ראה תיאורים עבור כל פעולות HIPS.
- **עבור יעד בלבד** – בחר את יעדי הקובץ/האפליקציה/הרישום של הכלל.

התראות HIPS אינסופיות?
כדי להפסיק את הופעת ההתראות, שנה את מצב הסינון ל**מצב אוטומטי** ב**הגדרות מתקדמות** (F5) > **מנגנון איתור** > **HIPS** > **בסיסי**.



זוהה אופן פעולה שעשוי להצביע על נוזקת כופר (ransomware)

חלון אינטראקטיבי זה יופיע בעת זיהוי אופן פעולה אפשרי של נוזקת כופר. תוכל לבחור **למנוע** או **לאשר** את הפעולה.



לחץ על **פרטים כדי להציג פרמטרים של זיהוי ספציפי**. חלון הדו-שיח מאפשר לך **לשלוח לניתוח** או **לא לכלול בזיהוי**.

חשוב

ESET LiveGrid® חייב לפעול כדי שהגנה מפני נוזקות כופר תפעל כהלכה.

ניהול הכללים של HIPS

רשימת כללים המוגדרים על-ידי המשתמשים והמתווספים אוטומטית ממערכת HIPS. פרטים נוספים על יצירת כללים ופעולות HIPS ניתן למצוא בפרק הגדרות כללי HIPS. ראה גם העיקרון הכללי של HIPS.

עמודות

כלל – שם כלל שמוגדר על-ידי המשתמש או נבחר אוטומטית.

מופעל – בטל פעולת מתג זה אם ברצונך להשאיר את הכלל ברשימה אך לא להשתמש בו.

פעולה – הכלל מציין פעולה – **התרה**, **חסימה** או **הצגת שאלה** – שיש לבצע אם התנאים מתקיימים.

מקורות – הכלל יהיה בשימוש רק אם האירוע יופעל על-ידי יישומים אלה.

יעדים – הכלל יהיה בשימוש רק אם הפעולה קשורה לקובץ, יישום או ערך רישום ספציפיים.

יומן רישום – אם תפעיל אפשרות זו, מידע על כלל זה ייכתב ביומן ה-HIPS.

הודעה – אם מופעל אירוע, חלון קופץ קטן מופיע בפינה הימנית התחתונה.

רכיבי בקרה

הוסף – יצירת כלל חדש.

ערוך – אפשרות לעריכת ערכים שנבחרו.

מחק – הסרת ערכים שנבחרו.

העדיפות של כללי HIPS

אין אפשרויות להתאמת רמת העדיפות של כללי HIPS באמצעות לחצני עליון/תחתון (בכל הנוגע לכללי חומת אש כאשר הפעלת הכללים מתבצעת מלמעלה למטה).

- לכל הכללים שתיצור יש אותה עדיפות
- ככל שהכלל ספציפי יותר, העדיפות גבוהה יותר (לדוגמה, הכלל לאפליקציה ספציפית הוא בעל עדיפות גבוהה יותר מהכלל לכל האפליקציות)
- באופן פנימי, HIPS מכיל כללים בעלי עדיפות גבוהה יותר שאינם נגישים לך (לדוגמה, אינך יכול לעקוף כללים מוגדרים להגנה עצמית)
- כלל שתיצור שעלול להקפיא את מערכת ההפעלה שלך לא יוחל (תהיה לו העדיפות הנמוכה ביותר)

ערוך כלל HIPS

ראה את ניהול הכללים של HIPS כראשון.

שם כלל – שם כלל שמוגדר על-ידי המשתמש או נבחר אוטומטית.

פעולה – מציינת פעולה – **התרה**, **חסימה** או **הצגת שאלה** – שיש לבצע כשתנאים מסוימים מתקיימים.

פעולות מושפעות – הנך נדרש לבחור את סוג הפעולה שעליה הכלל יוחל. כלל זה יימצא בשימוש רק עבור סוג הפעולה הזה ועבור היעד הנבחר.

מופעל – השבת מתג זה אם ברצונך להשאיר את הכלל ברשימה מבלי להחילו.

דרגת חומרה לרישום ביומן – אם תפעיל אפשרות זו, מידע על כלל זה ייכתב ביומן HIPS.

הודע למשתמש – אם מופעל אירוע, חלון קופץ קטן מופיע בפינה הימנית התחתונה.

הכלל מורכב מחלקים שמתארים את התנאים המפעילים אותו:

יישומי מקור – הכלל יהיה בשימוש רק אם האירוע יופעל על-ידי יישומים אלה. בחר **יישומים ספציפיים** בתפריט הנפתח ולחץ על **הוספה** כדי להוסיף קבצים חדשים; לחלופין תוכל לבחור באפשרות **כל היישומים** בתפריט הנפתח ולהוסיף את כל היישומים.

קבצים – הכלל יהיה בשימוש רק אם הפעולה מקושרת ליעד זה. בחר **קבצים ספציפיים** בתפריט הנפתח ולחץ על **הוספה** כדי להוסיף קבצים או תיקיות חדשים; לחלופין תוכל לבחור באפשרות **כל היישומים** בתפריט הנפתח ולהוסיף את כל היישומים.

יישומים – הכלל יהיה בשימוש רק אם הפעולה מקושרת ליעד זה. בחר **יישומים ספציפיים** בתפריט הנפתח ולחץ על **הוספה** כדי להוסיף קבצים ותיקיות חדשים; לחלופין תוכל לבחור באפשרות **כל היישומים** בתפריט הנפתח ולהוסיף את כל היישומים.

ערכי רישום – הכלל יהיה בשימוש רק אם הפעולה מקושרת ליעד זה. בחר **ערכים ספציפיים** בתפריט הנפתח ולחץ על **הוספה** כדי להקלידו ידנית; לחלופין תוכל ללחוץ על **פתח עורך רישום** כדי לבחור מפתח מסוים מהרישום. בנוסף, תוכל לבחור באפשרות **על הערכים** בתפריט הנפתח כדי להוסיף את כל היישומים.

הערה

פעולות מסוימות של כללים ספציפיים שהוגדרו מראש על-ידי HIPS אינן יכולות להיחסם וזמינות כברירת מחדל. בנוסף, HIPS לא מפקחת על כל פעולות המערכת. HIPS מנטרת פעולות שעלולות להיחשב כלא בטוחות.

תיאורים של פעולות חשובות:

פעולות עם קבצים

- **מחיקת קובץ** – היישום מבקש הרשאה למחיקת קובץ היעד.
- **כתיבה בקובץ** – היישום מבקש הרשאה לכתיבה בקובץ היעד.
- **גישה ישירה לדיסק** – היישום מנסה לקרוא מתוך הדיסק או לכתוב בו בצורה יוצאת דופן, שתעקוף פרוצדורות שכיחות של Windows. כתוצאה מכך, קבצים עשויים להשתנות מבלי שהוחלו הכללים המתאימים. פעולה זו עשויה להיגרם על-ידי תוכנה זדונית המנסה לחמוק מזיהוי, תוכנת גיבוי המנסה ליצור עותק מדויק של דיסק או מנהל מחיצות המנסה לארגן מחדש את אמצעי האחסון.
- **התקנת קרס כללי** – מתייחסת לקריאה לפונקציה SetWindowsHookEx מתוך הספרייה של MSDN.
- **טעינת מנהל התקן** – התקנה וטעינה של מנהלי התקנים במערכת.

פעולות עם יישומים

- **איתור באגים ביישום אחר** – חיבור מאתר באגים לתהליך. בעת איתור באגים ביישום, אפשר להציג ולשנות רבים מפרטי אופן הפעולה ולגשת אל הנתונים שלו.
- **יירוט אירועים מיישום אחר** – יישום המקור מנסה לתפוס אירועים המופנים ליישום ספציפי (לדוגמה לרישום הקשות המנסה ללכוד אירועי דפדפן).
- **עצירת/השהיית יישום אחר** – השהיה, חידוש או עצירה של תהליך (ניתן לגשת ישירות מ-Process Explorer או מחלונית התהליכים).
- **הפעלת יישום חדש** – הפעלת יישומים או תהליכים חדשים.
- **שינוי מצב של יישום אחר** – יישום המקור מנסה לכתוב בזיכרון של יישומי היעד או להריץ קוד בשמו. פונקציונליות זו עשויה להיות שימושית להגנה על יישום חיוני על-ידי הגדרתו כיישום יעד בכלל החוסם את השימוש ביישום זה.

הערה

לא ניתן ליירט פעולות עיבוד בגרסת ה-64 סיביות של Windows XP.

פעולות רישום

- **שינוי הגדרות אתחול** – כל השינויים בהגדרות שקובעות אילו יישומים יופעלו בעת האתחול של Windows. ניתן לאתרן,

לדוגמה, על-ידי חיפוש המפתח Run ברישום של Windows.

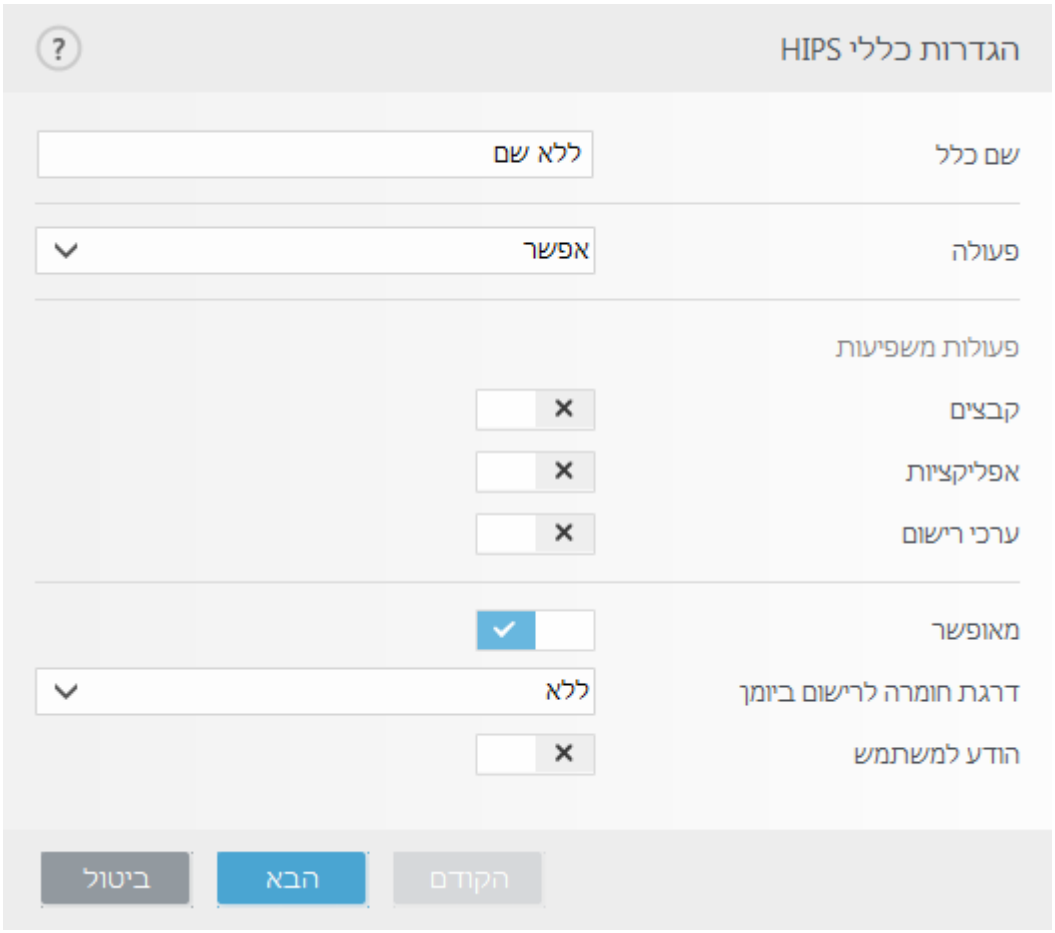
- **מחיקה מהרישום** ← מחיקת מפתח רישום או הערך שלו.
- **שינוי שם מפתח רישום** ← שינוי שם של מפתחות רישום.
- **שינוי רישום** ← יצירת ערכים חדשים של מפתחות רישום, החלפת ערכים קיימים, הזזת נתונים בעץ מסד הנתונים או הגדרת הזכויות של משתמש או קבוצה במפתחות רישום.

> **הערה**
> בעת הזנת יעד, באפשרותך להשתמש בתווים כלליים עם הגבלות מסוימות. במקום מפתח מסוים, ניתן להשתמש בסמל * (כוכבית) בנתיבי יישומים. לדוגמה, המשמעות של *HKEY_USERS*\software* יכולה להיות *HKEY_USER\.default\software* אך לא *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*.
> *HKEY_LOCAL_MACHINE\system\ControlSet** אינו נתיב חוקי של מפתח רישום. נתיב של מפתח רישום הכולל *\ מגדיר את "הנתיב הזה, או כל נתיב אחר, בכל רמה שהיא אחרי סמל זה". זוהי הדרך היחידה להשתמש בתווים כלליים עבור יעדים של קבצים. תחילה תתבצע הערכה של החלק הספציפי של נתיב, ולאחר מכן יימצא הנתיב לאחר סמל התו הכללי (*).

> **אזהרה**
> אם הכלל שאתה יוצר כללי מאוד, תופיע האזהרה על סוג כלל זה.

בדוגמה הבאה נראה כיצד להגביל פעילות לא רצויה של אפליקציה ספציפית:

1. תן לכלל שם ובחר באפשרות **חסום** (או **שאל** אם אתה מעדיף לבחור מאוחר יותר) מהתפריט הנפתח **פעולה**.
2. העבר את המתג **הודע למשתמש** למצב פעיל כדי להציג הודעה בכל פעם שכלל מסוים מוחל.
3. בחר פעולה אחת לפחות במקטע **פעולות משפיעות** שעבורה יוחל הכלל.
4. לחץ על **הבא**.
5. בחלון **אפליקציות מקור**, בחר באפשרות **אפליקציות מסוימות** בתפריט הנפתח כדי להחיל את הכלל החדש שלך על כל האפליקציות שמנסות לבצע אחת מפעולות האפליקציה שנבחרו באפליקציות שציינת.
6. לחץ על **הוסף** ולאחר מכן על **...** כדי לבחור נתיב לאפליקציה ספציפית ולאחר מכן לחץ על **אישור**. הוסף עוד אפליקציות כרצונך.
לדוגמה: *C:\Program Files (x86)\Untrusted application\application.exe*
7. בחר את הפעולה **כתיבה לקובץ**.
8. בחר **כל הקבצים** מהתפריט הנפתח. פעולה זו תחסום כל ניסיונות לכתוב לקבצים על-ידי האפליקציות הנבחרות מהשלב הקודם.
9. לחץ על **סיום** כדי לשמור את הכלל החדש.



הוספת נתיב רישום/אפליקציה עבור HIPS

בחר נתיב של קובץ יישום על-ידי לחיצה על **בחירת קובץ...** בעת בחירת תיקייה, כל היישומים שנמצאים במיקום זה נכללים.

האפשרות **הפעלת RegEdit...** תפעיל את עורך הרישום של Windows (regedit). בעת הוספת נתיב רישום, הזן את המיקום הנכון בשדה **ערך**.

דוגמאות לנתיב הרישום או הקובץ:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

אי הכללות HIPS

אי הכללות מאפשרות לך לא לכלול תהליכים בבדיקה התנהגותית עמוקה של HIPS.

> **הערה**
> אל תתבלבל עם סיומות קובץ שלא ייכללו, אי הכללות קובץ/תיקייה או אי הכללת תהליכים.

כדי לא לכלול אובייקט, לחץ על הוסף והזן את הנתיב לאובייקט או בחר אותו במבנה העץ. באפשרותך גם לערוך או להסיר ערכים נבחרים.

הגדרות מתקדמות של HIPS

האפשרויות הבאות שימושיות לאיתור באגים ולניתוח אופן פעולה של יישום:

טעינת מנהלי התקן מתאפשרת תמיד – טעינתם של מנהלי ההתקן הנבחרים תתאפשר תמיד, ללא קשר למצב הסינון שהוגדר, אלא אם נחסמו מפורשות באמצעות כלל של המשתמש.

רשום את כל הפעולות החסומות ⮜ כל הפעולות החסומות יירשמו ביומן ה-HIPS.

הודע כשחלים שינויים ביישומי אתחול ⮜ הצגת הודעה בשולחן העבודה בכל פעם שיישום מתווסף לאתחול המערכת או מוסר ממנו.

טעינת מנהלי התקן מתאפשרת תמיד

טעינתם של מנהלי ההתקן המוצגים ברשימה זו תתאפשר תמיד, ללא תלות במצב סינון ה-HIPS, אלא אם נחסמו מפורשות באמצעות כלל של המשתמש.

הוסף ⮜ הוספת מנהל התקן חדש.

ערוך ⮜ עריכת מנהל התקן שנבחר.

הסר ⮜ הסרת מנהל התקן מהרשימה.

אפס ⮜ טעינה מחדש של קבוצת מנהלי התקן של מערכת.

> **הערה**
> לחץ על **אפס** אם אינך מעוניין לכלול את מנהלי ההתקן שהוספת באופן ידני. מצב זה עשוי להיות שימושי אם הוספת מספר מנהלי התקן ואין באפשרותך למחוק אותם מהרשימה באופן ידני.

מצב משחק

מצב משחק הוא תכונה המיועדת למשתמשים שצריכים שימוש רציף בתוכנה, שאינם רוצים הפרעות של חלונות קופצים ושמעוניינים למזער את השימוש ב-CPU. ניתן להשתמש במצב משחק גם בעת העברת מצגות שלא ניתן להפסיקן בשל פעילות האנטי-וירוס. הפעלת תכונה זו תגרום להשבתה של כל החלונות הקופצים ולעצירה מוחלטת של פעילות המתזמן. ההגנה על המערכת תמשיך לפעול ברקע, אולם לא תצריך אינטראקציה כלשהי עם המשתמש.

באפשרותך להפעיל או להשבית מצב משחק בחלון התוכנית הראשי תחת **הגדרות** > **הגנה על המחשב**, על-ידי לחיצה על  או על  לצד **מצב משחק**. הפעלת מצב משחק מציבה סיכון אבטחה אפשרי, ולכן סמל סטטוס ההגנה בשורת המשימות יהפוך לכתום ויציג אזהרה. תוכל לראות אזהרה זו גם בחלון התוכנית הראשי, בו יופיע הכיתוב **מצב משחק מופעל** בכתום.

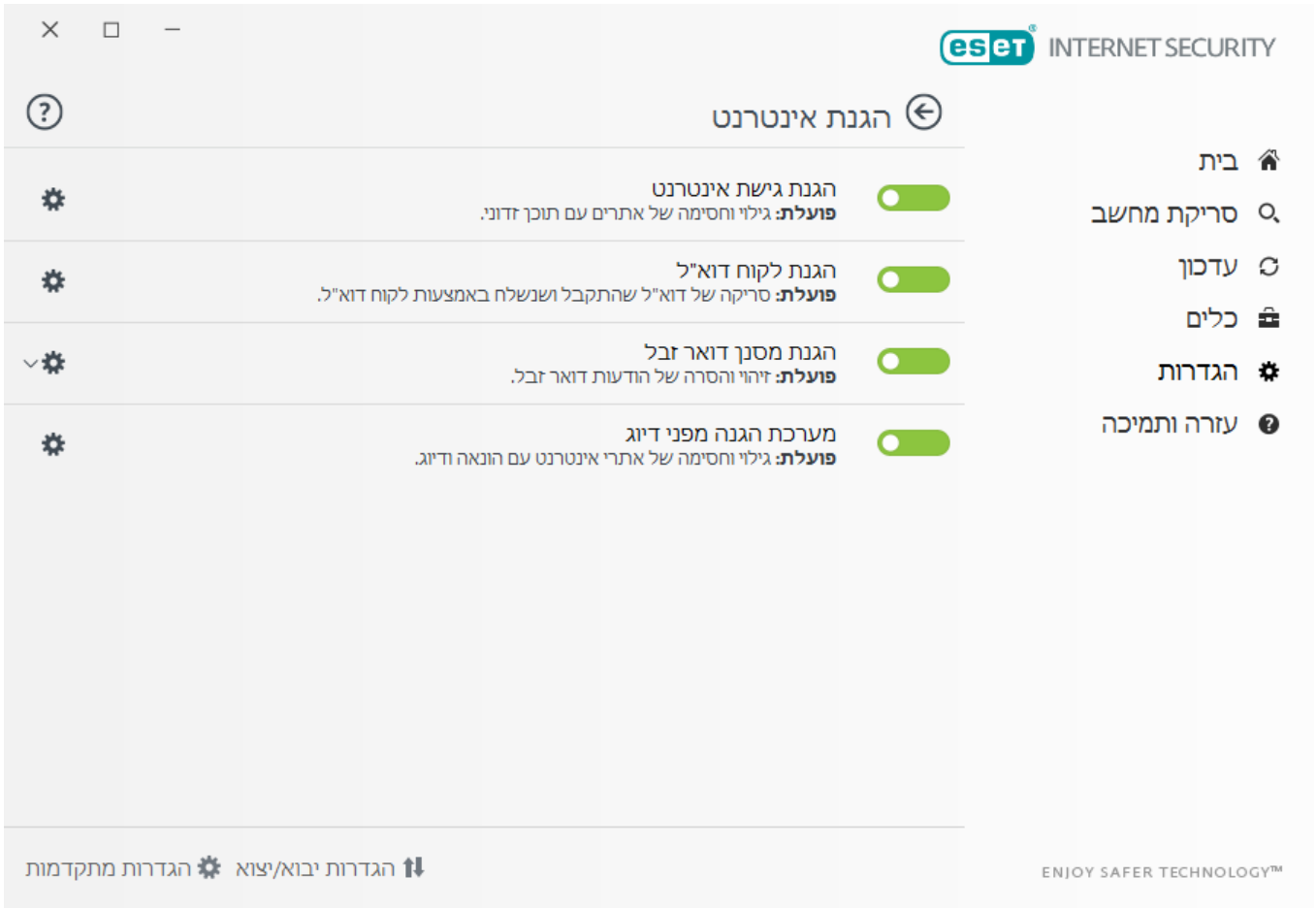
הפעל את האפשרות **הפעל מצב משחק אוטומטית בעת הפעלת יישומים במצב מסך מלא** תחת **הגדרות מתקדמות** (F5) > **כלים** > **מצב משחק** כדי שמצב משחק יופעל בכל פעם שתפעיל יישום המוצג במסך מלא ויעצור כשתצא מהיישום.

הפעל את האפשרות **השבת מצב משחק אוטומטית לאחר** כדי להגדיר כמה זמן צריך לחלוף עד שמצב משחק יושבת באופן אוטומטי.

> **הערה**
> אם חומת האש נתונה במצב אינטראקטיבי ומצב משחק פעיל, ייתכן שקיימת בעיה בחיבור לאינטרנט. מצב זה עשוי להוות בעיה אם תפעיל משחק שמתחבר לאינטרנט. במצב הרגיל תתבקש לאשר פעולה כזו (אם לא הוגדרו כללי תקשורת או חריגות), אולם ממשק המשתמש מושבת במצב משחק. כדי להתיר את התקשורת, הגדר כלל תקשורת עבור כל יישום שעשוי להיתקל בבעיה זו או השתמש במצב סינון אחר בחומת האש. זכור שכאשר מצב משחק מופעל ואתה עובר לדף אינטרנט או ליישום שעשויים להוות סיכון אבטחה, אלה עשויים להיחסם ללא כל הסבר או אזהרה מפני שהאינטראקציה עם המשתמש מושבתת.

הגנת אינטרנט

את הגדרות התצורה של האינטרנט והדואר האלקטרוני ניתן להגיע דרך החלונית **הגדרות**, בלחיצה על **הגנת אינטרנט**. מכאן תוכל לגשת להגדרות מפורטות יותר של התוכנית.



קישוריות אינטרנט היא תכונה סטנדרטית במחשבים אישיים. למרבה הצער האינטרנט הפך לאמצעי הראשי להפצת קודים זדוניים. מסיבה זו חיוני שתשקול היטב את הגדרות **ההגנה על הגישה לאינטרנט** שלך.

לחץ על ⚙ כדי לפתוח את ההגדרות של הגנת אינטרנט/דואר אלקטרוני/אנטי-פישינג/מסנן דואר זבל תחת ההגדרות המתקדמות.

הגנת לקוח דואר אלקטרוני מספקת בקרה על תקשורת דואר אלקטרוני המתקבלות באמצעות הפרוטוקולים POP3 ו-IMAP. באמצעות תוכנית ה-plug-in ללקוח הדואר האלקטרוני שלך, ESET Internet Security מספק בקרה על כל התקשורת אל לקוח הדואר האלקטרוני שלך וממנו (HTTP ,IMAP ,MAPI ,POP3).

הגנת מסנן דואר זבל מסננת הודעות דואר אלקטרוני שלא התבקשו.

כשאתה לוחץ על גלגל השיניים ⚙ לצד**הגנת מסנן דואר זבל,** האפשרויות הבאות זמינות:

קבע תצורה... ⍰ פתיחת ההגדרות המתקדמות עבור הגנת מסנן דואר זבל של לקוח דואר אלקטרוני.

רשימה לבנה/רשימה שחורה/רשימת חריגים של משתמש ⍰ פתיחת חלון דו-שיח שבו באפשרותך להוסיף, לערוך או למחוק כתובות דואר אלקטרוני שנחשבות כבטוחות או כלא בטוחות. על-פי הכללים המוגדרים כאן, דואר אלקטרוני מהכתובות הללו לא ייסרק או ייחשב כדואר זבל. לחץ על **רשימת חריגים של המשתמש** כדי להוסיף, לערוך או למחוק כתובות דואר אלקטרוני שעשויות להיות מזויפות ושמשמשות לשליחת דואר זבל. הודעות דואר אלקטרוני שמתקבלות מהכתובות המפורטות ברשימת החריגים תמיד ייסרקו לאיתור דואר זבל.

הגנה מפני פישינג מאפשרת לך לחסום דפי אינטרנט שידוע שמפיצים תוכן פישינג. מומלץ מאוד להשאיר את מערכת ההגנה מפני פישינג במצב פעיל.

באפשרותך להשבית את מודול הגנת האינטרנט/דואר אלקטרוני/אנטי-פישינג/מסנן דואר זבל באופן זמני על-ידי לחיצה על .

סינון פרוטוקולים

הגנת אנטי-וירוס לפרוטוקולי יישומים מסופקת על-ידי מנוע הסריקה של ThreatSense, אשר משתלב בצורה חלקה בכל השיטות המתקדמות לסריקה של תוכנות זדוניות. סינון פרוטוקולים פועל אוטומטית, ללא תלות בדפדפן האינטרנט או בלקוח הדואר האלקטרוני שבו נעשה שימוש. כדי לערוך הגדרות מוצפנות (SSL/TLS), עבור אל **אינטרנט ודואר אלקטרוני** > **SSL/TLS**.

אפשר סינון תוכן בפרוטוקול יישומים ניתן להשתמש באפשרות זו להשבתת סינון פרוטוקולים. שים לב שרבים מרכיבי ESET Internet Security (הגנה על גישה לאינטרנט, הגנה על פרוטוקולי דואר אלקטרוני, הגנה מפני פישינג, בקרת אינטרנט) תלויים באפשרות זו ולא יפעלו בלעדיה.

יישומים לא כלולים מאפשרת לך לא לכלול יישומים מסוימים בסינון הפרוטוקולים. שימושית כאשר סינון הפרוטוקולים גורם בעיות תאימות.

כתובות IP לא כלולות מאפשרת לך לא לכלול כתובות מרוחקות מסוימות בסינון הפרוטוקולים. שימושית כאשר סינון הפרוטוקולים גורם בעיות תאימות.

לקוחות אינטרנט ודוא"ל

שילוב של ESET Internet Security בלקוח הדואר אלקטרוני שלך מגביר את רמת ההגנה הפעילה מפני קוד זדוני בהודעות דואר אלקטרוני. אם לקוח הדואר האלקטרוני שלך נתמך, ניתן להפעיל את השילוב ב-ESET Internet Security. כאשר הוא משולב בלקוח הדואר האלקטרוני שלך, סרגל הכלים של ESET Internet Security מתווסף ישירות ללקוח הדואר האלקטרוני (סרגל הכלים לגירסאות חדשות יותר של Windows Live Mail לא מתווסף), להגנה יעילה יותר על דואר אלקטרוני. הגדרות שילוב ממוקמות תחת **הגדרות מתקדמות** (F5) > **אינטרנט ודואר אלקטרוני** > **הגנה על לקוח דוא"ל** > **לקוחות דואר אלקטרוני**.

שילוב עם לקוח דוא"ל
לקוחות הדואר האלקטרוני הנתמכים כעת כוללים את Microsoft Outlook, Outlook Express, Windows Mail ו-Windows Live Mail. הגנת דואר אלקטרוני פועלת כיישום plug-in עבור תוכניות אלו. היתרון העיקרי של יישום ה-plug-in הוא היעדר תלות בפרוטוקול שבו נעשה שימוש. כאשר לקוח הדואר האלקטרוני מקבל הודעה מוצפנת, ההודעה מפוענחת ונשלחת אל סורק הווירוסים. לקבלת רשימה מלאה של לקוחות הדואר האלקטרוני הנתמכים והגרסאות שלהם, עיין במאמר הבא במאגר הידע של ESET.

גם אם השילוב אינו מופעל, תקשורת דואר אלקטרוני עדיין מוגנת על-ידי מודול הגנת לקוח דואר אלקטרוני (IMAP ,POP3).

הפעל את האפשרות **השבת בדיקה בעת שינוי תוכן בתיבת דואר נכנס** אם אתה מבחין בהאטה של המערכת בעת עבודה עם Microsoft Outlook. מצב זה עשוי להתרחש בעת אחזור דוא"ל מהמאגר של Kerio Outlook Connector.

דואר אלקטרוני לסריקה

אפשר הגנת דוא"ל באמצעות יישומי plug-in של לקוח כאשר הגנת לקוח דואר אלקטרוני באמצעות לקוח דואר אלקטרוני מושבתת, הגנת לקוח דואר אלקטרוני באמצעות סינון פרוטוקולים עדיין תפעל.

דואר אלקטרוני שהתקבל משנה את מצב הבדיקה של הודעות שהתקבלו.

דואר אלקטרוני שנשלח משנה את מצב הבדיקה של הודעות שנשלחו.

דואר אלקטרוני שנקרא משנה את מצב הבדיקה של הודעות שנקראו.

הפעולה שיש לבצע בדואר אלקטרוני נגוע

ללא פעולה אם אפשרות זו מופעלת, התוכנית תזהה קבצים מצורפים נגועים אך תשאיר את הודעות הדואר האלקטרוני מבלי לנקוט פעולה כלשהי.

מחק דואר אלקטרוני התוכנית תיידע את המשתמש על החדירות ותמחק את ההודעה.

העבר דואר אלקטרוני לתיקיית הפריטים שנמחקו הודעות הדואר האלקטרוני הנגועות יועברו אוטומטית לתיקיית הפריטים שנמחקו.

העבר דוא"ל לתיקייה (פעולת ברירת מחדל) הודעות הדוא"ל הנגועות יועברו אוטומטית לתיקייה שצוינה.

תיקייה ▯ ציין את התיקייה המותאמת אישית שאליה ברצונך להעביר את הודעות הדואר האלקטרוני לאחר זיהוין.

חזור על הסריקה לאחר העדכון ▯ משנה את מצב הסריקה מחדש לאחר עדכון מנגנון האיתור.

אשר תוצאות סריקה ממודולים אחרים ▯ אם אפשרות זו נבחרת, מודול הגנת הדואר האלקטרוני מאשר תוצאות סריקה של מודולי הגנה אחרים (סריקת פרוטוקולי POP3, IMAP).

הערה

מומלץ להפעיל את האפשרויות **אפשר הגנת דוא"ל באמצעות יישומי plug-in** של לקוח ו- **אפשר הגנת דוא"ל על-ידי סינון פרוטוקולים. הגדרות אלו נמצאות תחת הגדרות מתקדמות** (F5) > **אינטרנט ודוא"ל** > **הגנת לקוח דוא"ל** > **פרוטוקולי דוא"ל**).

פרוטוקולי דואר אלקטרוני

הפרוטוקולים IMAP ו-POP3 הם הפרוטוקולים הנפוצים ביותר המשמשים לקבלת תקשורת דואר אלקטרוני ביישום לקוח דוא"ל. Internet Message Access Protocol (IMAP) הוא פרוטוקול אינטרנט אחר לאחזור דואר אלקטרוני. ל-IMAP מספר יתרונות לעומת POP3, לדוגמה, מספר לקוחות יכולים להתחבר בו-זמנית לאותה תיבת דואר ולשמור על פרטי מצב ההודעה, למשל אם ההודעה נקראה, נמחקה או קיבלה מענה. ESET Internet Security מספק הגנה לפרוטוקולים אלה, ללא קשר ללקוח הדואר האלקטרוני שבו נעשה שימוש, ומבלי לחייב הגדרה חוזרת של לקוח הדואר האלקטרוני.

מודול ההגנה המספק בקרה זו מופעל אוטומטית בעת אתחול המערכת, ולאחר מכן הוא מופעל בזיכרון. בקרת פרוטוקול IMAP מבוצעת אוטומטית, ללא צורך בזיהוי לקוח הדואר האלקטרוני. כברירת מחדל, כל התקשורת ביציאה 143 נסרקת, אולם ניתן להוסיף יציאות תקשורת אחרות במידת הצורך. בין מספרי יציאות שונים יש להפריד באמצעות פסיקים.

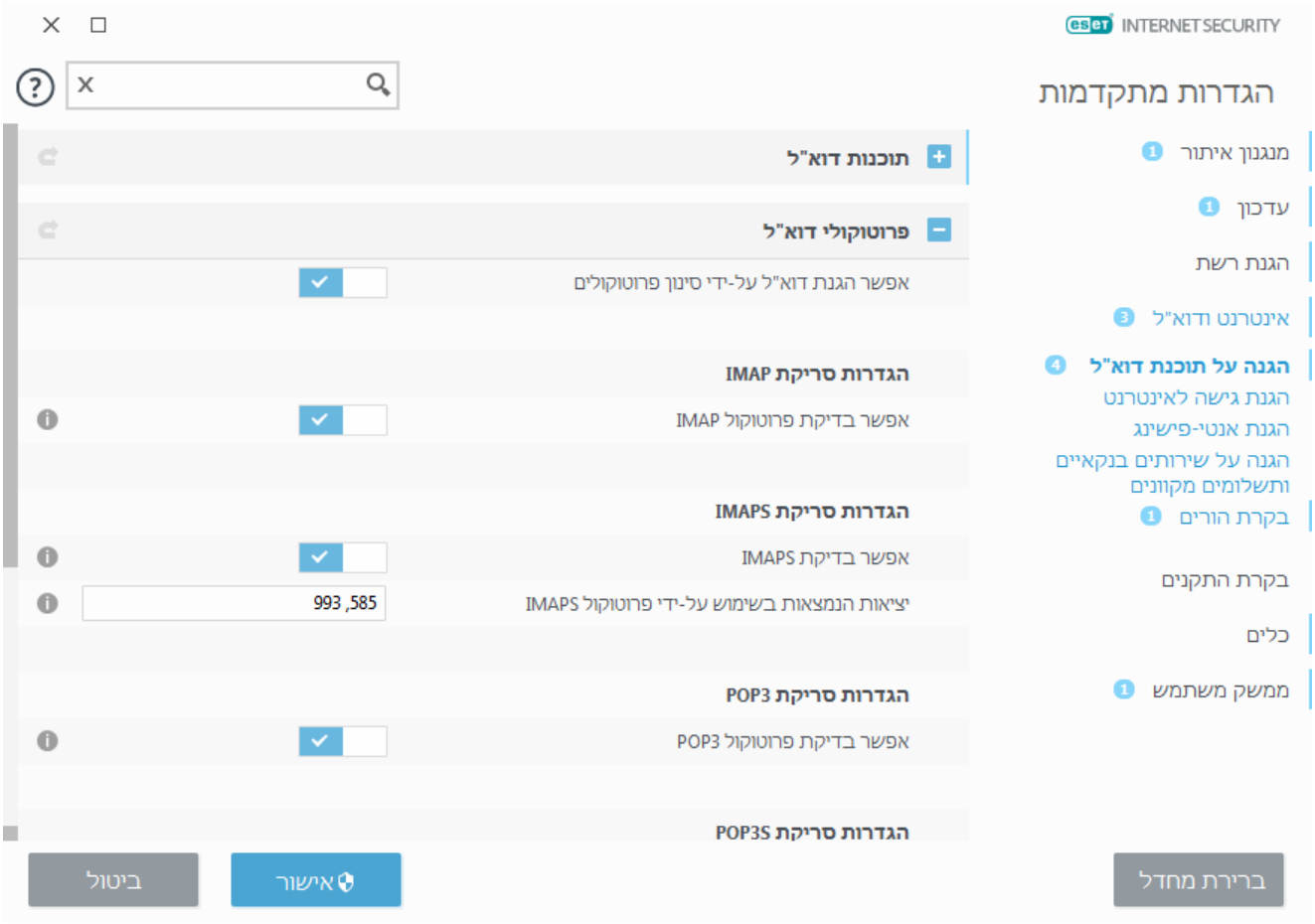
באפשרותך להגדיר בדיקה של פרוטוקול IMAP/IMAPS ו-POP3/POP3S בהגדרות המתקדמות. כדי לגשת להגדרה זו, הרחב את **אינטרנט ודואר אלקטרוני** > **הגנה על לקוח דוא"ל** > **פרוטוקולי דואר אלקטרוני**.

אפשר הגנת דוא"ל על-ידי סינון פרוטוקולים ▯ מאפשר בדיקה של פרוטוקולי דוא"ל.

במערכת Windows Vista ובמערכות חדשות יותר, הפרוטוקולים IMAP ו-POP3 מזוהים ונסרקים אוטומטית בכל היציאות. במערכת Windows XP, רק **היציאות שנמצאות בשימוש הפרוטוקול IMAP/POP3** ושהוגדרו נסרקות לבדיקת כל היישומים, וכל היציאות נסרקות לאיתור יישומים המסומנים כלקוחות אינטרנט ודואר אלקטרוני.

ESET Internet Security גם תומך בסריקה של פרוטוקולי IMAPS ו-POP3S, אשר משתמשת בערוץ מוצפן להעברת מידע בין השרת והלקוח. ESET Internet Security בודק את התקשורת באמצעות פרוטוקולי SSL (Secure Socket Layer) ו-TLS (Transport Layer Security). התוכנית תסרוק את התעבורה רק ביציאות המוגדרות ב**יציאות שמשמשות את פרוטוקול IMAPS/POP3S**, ללא קשר לגרסת מערכת ההפעלה.

תקשורת מוצפנת תיסרק כברירת מחדל. כדי להציג את הגדרות הסורק, נווט אל SSL / TLS במקטע 'הגדרות מתקדמות', לחץ על **אינטרנט ודוא"ל** > **SSL/TLS** ואפשר את האפשרות **אפשר סינון פרוטוקולים של SSL/TLS**.



התראות והודעות בדוא"ל

סינון יומן

לחץ על **סינון** ב- **כלים** > **כלים נוספים** > **רשומות יומן** כדי להגדיר קריטריוני סינון.

התכונה סינון יומן תעזור לך למצוא את המידע שאתה מחפש, בעיקר כשיש רשומות רבות. היא מאפשרת לך לצמצם את רשומות היומן, לדוגמה, אם אתה מחפש סוג מסוים של אירוע, סטטוס או פרק זמן. ניתן לסנן את רשומות היומן על-ידי ציון אפשרויות חיפוש מסוימות, ורק רשומות רלוונטיות (לפי אפשרויות חיפוש אלה) יוצגו בחלון רשומות היומן.

הקלד את מילת המפתח שאתה מחפש בשדה **חפש טקסט**. השתמש בתפריט הנפתח **חפש בעמודות** כדי למקד את החיפוש. בחר רשומה אחת או יותר מהתפריט הנפתח **סוגי רשומות יומן**. הגדר את **תקופת הזמן** שממנה ברצונך להציג רשומות. אפשר גם להשתמש באפשרויות חיפוש נוספות, כמו **התאם מילים מלאות בלבד** או **תלוי-רישיות**.

חפש טקסט

הקלד מחרוזת (מילה או חלק ממילה). רק רשומות המכילות את המחרוזת יוצגו. רשומות אחרות יושמטו.

חפש בעמודות

בחר אילו עמודות יילקחו בחשבון בעת החיפוש. ניתן לסמן עמודה אחת או יותר שישמשו לחיפוש.

סוגם רשומות

בחר סוג רשומות יומן אחד או יותר מהתפריט הנפתח:

- **אבחוני** – רישום מידע שנדרש להתאמה מפורטת של התוכנית ושל כל הרשומות שלעיל.
- **אינפורמטיבי** – תיעוד הודעות מסירת מידע, לרבות הודעות על עדכון מוצלח, בנוסף לכל הרשומות שלעיל.
- **אזהרות** – תיעוד שגיאות קריטיות והודעות אזהרה.
- **שגיאות** – שגיאות כגון "שגיאה בהורדת קובץ" ושגיאות קריטיות יתועדו.

- **קריטי** – רישום שגיאות קריטיות בלבד (שגיאה בהפעלה של הגנת אנטי-וירוס

תקופת זמן

הגדר את תקופת הזמן שממנה ברצונך להציג תוצאות:

- **לא צוין** (ברירת מחדל) - לא מתבצע חיפוש בתקופת זמן אלא ביומן כולו.
- **יום אחרון**
- **בשבוע שעבר**
- **בחודש שעבר**
- **תקופת זמן** - ניתן לציין את תקופת הזמן המדויקת (’מ:’ ו’עד:’) כדי לסנן רק את הרשומות מתקופת הזמן שצוינה.

התאם מילים מלאות בלבד

השתמש בתיבת החיפוש אם ברצונך לחפש מילים מלאות לתוצאות מדויקות יותר.

תלוי-רישיות

הפעל אפשרות זו אם חשוב לך להשתמש באותיות רישיות או קטנות בעת הסינון. לאחר שתקבע את התצורה של אפשרויות הסינון/חיפוש, לחץ על **אישור** כדי להציג רשומות יומן מסוננות או על **חפש** כדי להתחיל לחפש. החיפוש ברשומות היומן מתבצע מלמעלה למטה, החל במיקום הנוכחי שלך (הרשומה המסומנת). החיפוש ייפסק כשימצא את הרשומה המתאימה הראשונה. הקש על **F3** כדי לחפש את הרשומה הבאה או לחץ על לחצן העכבר הימני ובחר **חפש** כדי למקד את אפשרויות החיפוש.

תצורת רישום ביומן

ניתן לגשת אל תצורת הרישום ביומן של ESET Internet Security מחלון התוכנית הראשי. לחץ על **הגדרות** > **הגדרות מתקדמות** > **כלים** > **רשומות יומן**. מקטע קובצי היומן משמש כדי להגדיר את אופן הניהול של קובצי היומן. התוכנית מוחקת אוטומטית את יומני הרישום הישנים יותר כדי לחסוך מקום בכונן הקשיח. באפשרותך לציין את אפשרויות קובצי היומן הבאות:

פירוט מינימלי של רישום ביומן – מציין את רמת הפירוט המינימלית שתירשם.

- **אבחוני** – רישום מידע שנדרש להתאמה מפורטת של התוכנית ושל כל הרשומות שלעיל.
- **אינפורמטיבי** – תיעוד הודעות מסירת מידע, לרבות הודעות על עדכון מוצלח, בנוסף לכל הרשומות שלעיל.
- **אזהרות** – תיעוד שגיאות קריטיות והודעות אזהרה.
- **שגיאות** – שגיאות כגון ”שגיאה בהורדת קובץ” ושגיאות קריטיות יתועדו.
- **קריטי** – רישום שגיאות קריטיות בלבד (שגיאה בהפעלה של הגנת אנטי-וירוס, חומת אש, וכו’...).

> **הערה**
> בעת בחירה ברמת הפירוט ’אבחון’, כל החיבורים החסומים נרשמים.

הזנות יומן רישום שישנות ממספר הימים שצוין בשדה **מחק אוטומטית רשומות בנות מעל (ימים)** יימחקו אוטומטית.

מטב קובצי יומן אוטומטית – אם אפשרות זו מסומנת, קובצי יומן יאוחו אוטומטית אם האחוז גבוה מהערך המפורט בשדה **אם מספר הרשומות שאינן בשימוש עולה על (%)**.

לחץ על **מטב** כדי להתחיל באיחוי קובצי היומן. כל הזנות היומן הריקות יוסרו בתהליך זה, אשר משפר את הביצועים ואת מהירות עיבוד היומן. שיפור זה ניכר במיוחד כאשר קובצי היומן כוללים מספר רב של הזנות.

אפשר פרוטוקול טקסט מאפשר אחסון של קובצי יומן בתבנית קובץ אחרת, בנפרד מ[רשומות יומן]:

- **ספריית יעד** – הספרייה שבה קובצי היומן יאוחסנו (חל רק על טקסט/CSV). לכל מקטע יומן יש קובץ משלו עם שם קובץ שהוגדר מראש (לדוגמה, *virlog.txt* עבור המקטע **אובייקטים מזוהים** בקובצי היומן, אם אתה משתמש בתבנית קובץ טקסט פשוט לאחסון קובצי יומני הרישום).

- **סוג** – אם תבחר בתבנית קובץ **טקסט**, יומני הרישום יאוחסנו בקובץ טקסט והנתונים יופרדו בטאבים. אותו כלל חל על תבנית

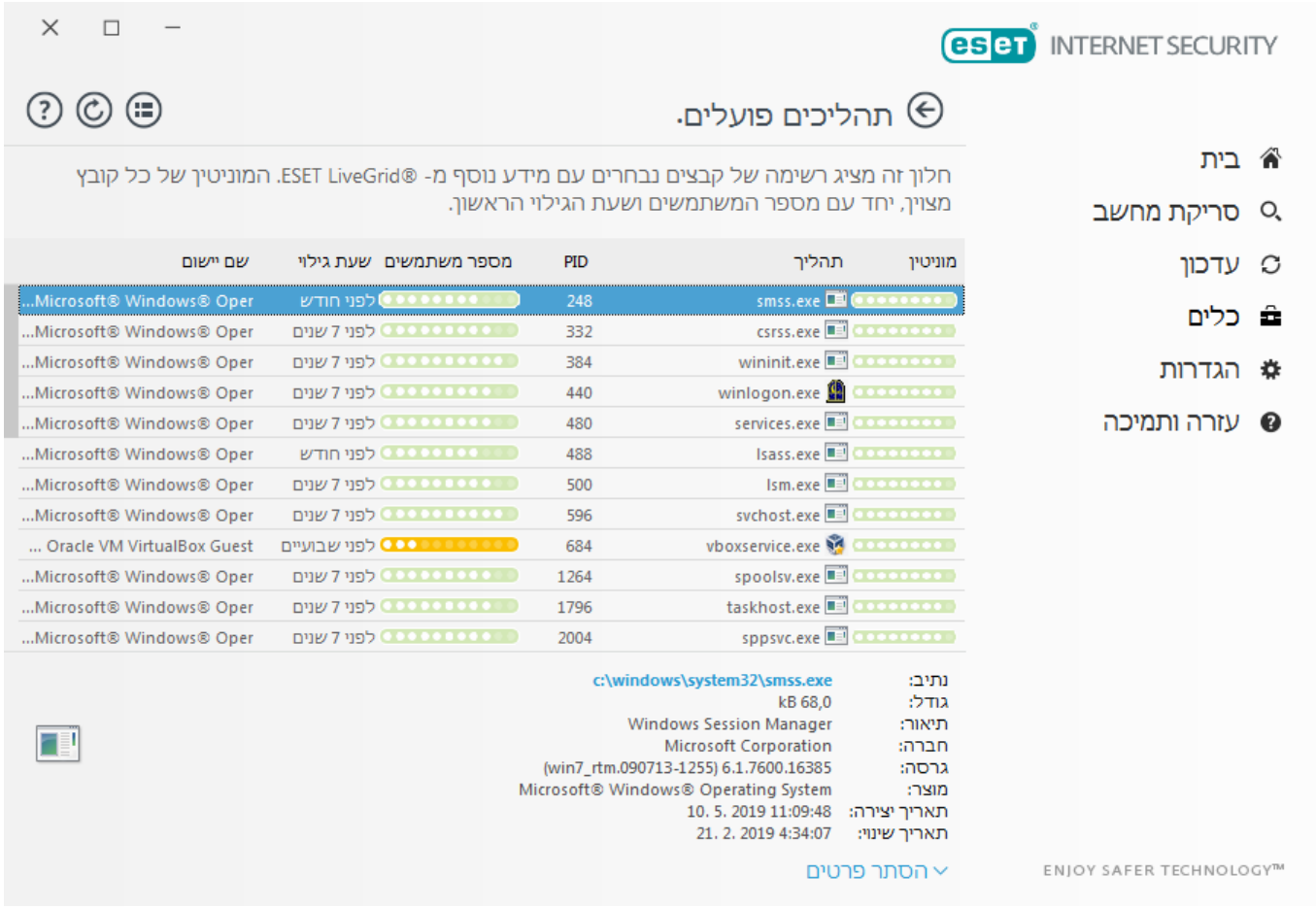
הקובץ **CSV** עם הפרדה באמצעות פסיקים. אם תבחר**אירוע**, יומני הרישום יאוחסנו ביומן האירועים של Windows (שניתן להציגו דרך מציג האירועים בלוח הבקרה) במקום בקובץ.

- **מחק את כל קובצי היומן** – מוחק את כל יומני הרישום המאוחסנים שנבחרו כעת בתפריט הנפתח **סוג**. תוצג הודעה שכל יומני הרישום נמחקו בהצלחה.

> **הערה**
> כדי לסייע בפתרון מהיר יותר של בעיות, ESET עשויה לבקש ממך לספק יומני רישום מהמחשב שלך. ESET Log Collector מאפשר לך לאסוף את המידע הדרוש בקלות. לקבלת מידע נוסף על ESET Log Collector בקר ב[מאמר במאגר הידע של ESET].

תהליכים פועלים

המקטע 'תהליכים פועלים' מציג את התוכניות או התהליכים שפעילים במחשב שלך ומיידע את ESET על חדירות חדשות באופן מיידי ורציף. ESET Internet Security מספק מידע מפורט על תהליכים פועלים כדי להגן על משתמשים עם טכנולוגיית [ESET LiveGrid®].



מוניטין – ברוב המקרים, ESET Internet Security וטכנולוגיית ESET LiveGrid® מקצים רמות סיכון לאובייקטים (קבצים, תהליכים, מפתחות רישום וכו') באמצעות סדרת כללי היריסטיקה שבוחנים את המאפיינים של כל אובייקט ואובייקט ולאחר מכן משקללים את פוטנציאל הפעילות הזדונית שלהם. על-סמך היריסטיקות אלו, לאובייקטים מוקצית רמת סיכון החל מ-1 – תקין (ירוק) ועד 9 – מסוכן (אדום).

תהליך – שם התמונה של התוכנית או התהליך שפועלים כעת במחשב שלך. באפשרותך גם להשתמש במנהל המשימות של Windows כדי לראות את כל התהליכים הפעילים במחשב שלך. כדי לפתוח את מנהל המשימות, לחץ באמצעות לחצן העכבר הימני באזור ריק כלשהו בשורת המשימות ואז לחץ על **מנהל המשימות**, או הקש **Ctrl+Shift+Esc** במקלדת.

הערה
יישומים מוכרים הנושאים את הסימון תקין (ירוק) הם בבירור נקיים (נמצאים ברשימה הלבנה) ולא ייכללו בסריקה כדי לשפר את הביצועים.

PID – המספר המזהה של התהליך יכול לשמש כפרמטר במספר קריאות לפונקציות, כגון התאמת העדיפות של התהליך.

מספר משתמשים – מספר המשתמשים שמשתמשים ביישום נתון. מידע זה נאסף באמצעות טכנולוגיית ESET LiveGrid®.

זמן הגילוי – פרק הזמן שחלף מאז שהיישום התגלה על-ידי טכנולוגיית ESET LiveGrid®.

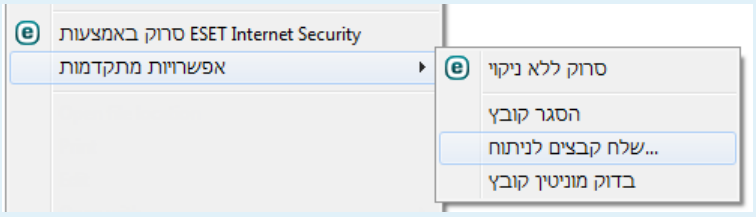
הערה
יישום הנושא את הסימון לא ידוע (כתום) אינו בהכרח תוכנה זדונית. בדרך-כלל זהו יישום חדש יחסית. אם אינך בטוח לגבי הקובץ, באפשרותך לשלוח את הקובץ לניתוח במעבדת המחקר של ESET. אם יסתבר שהקובץ הוא יישום זדוני, זיהויו יתווסף לעדכון הבא.

שם היישום – השם הנתון של תוכנית או תהליך.

לחץ על יישום כלשהו כדי להציג את הפרטים הבאים לגביו:

- **נתיב** – מיקום של יישום במחשב שלך.
- **גודל** – גודל הקובץ ביחידות B (בתים).
- **תיאור** – מאפייני הקובץ בהתבסס על תיאור ממערכת ההפעלה.
- **חברה** – שם הספק או תהליך היישום.
- **גרסה** – מידע מהמפרסם של היישום.
- **מוצר** – שם היישום ו/או שם העסק.
- **תאריך יצירה/תאריך שינוי** – תאריך ושעת היצירה (שינוי).

הערה
תוכל גם לבדוק את המוניטין של הקבצים שאינם פועלים כתכניות/תהליכים פעילים. כדי לבצע זאת לחץ עליהם באמצעות לחצן העכבר הימני בסייר קבצים ובחר **אפשרויות מתקדמות** > **בדוק מוניטין קובץ**.



דוח אבטחה

תכונה זה מספקת מבט כולל של הנתונים הסטטיסטיים עבור הקטגוריות להלן:

דפי אינטרנט נחסמו – הצגת המספר של דפי אינטרנט שנחסמו (כתובת URL הרשומה ברשימה שחורה עבור אפליקציות העלולות להיות לא רצויות, פישינג, נתב שנפרץ, כתובת IP או אישור).

אובייקטים פגועים של דוא"ל אותרו – הצגת המספר של האובייקטים הפגועים של דוא"ל שאותרו.

דפי אינטרנט ב'בקרת הורים' נחסמו – הצגת המספר של הדפי האינטרנט ב'בקרת הורים' שנחסמו.

אפליקציות העלולות להיות לא רצויות אותרו – הצגת המספר של אפליקציות העלולות להיות לא רצויות (PUA).

הודעות דואר זבל אותרו – הצגת המספר של הודעות דואר הזבל שאותרו.

גישה חסומה למצלמת אינטרנט – הצגת המספר של ניסיונות הגישה למצלמת האינטרנט שנחסמו.

חיבורים מוגנים לבנקאות באינטרנט – הצגת מספר ניסיונות הגישה המוגנים לאתרים דרך התכונה הגנה על בנקאות ותשלומים.

מסמכים נבדקו – הצגת המספר של אובייקטים של מסמכים שנסרקו.

אפליקציות נבדקו – הצגת המספר של אובייקטים של קובצי הפעלה שנסרקו.

אובייקטים אחרים נבדקו – הצגת המספר של אובייקטים אחרים שנסרקו.

אובייקטים בדף אינטרנט נסרקו – הצגת מספר האובייקטים בדפי אינטרנט שנסרקו.

אובייקטים של דוא"ל נסרקו – הצגת המספר של אובייקטים של דוא"ל שנסרקו.

הסדר של קטגוריות אלה מבוסס על הערך המספרי מהגבוה ביותר לנמוך ביותר. הקטגוריות עם ערך אפס אינן מוצגות. לחץ על **הצג עוד** כדי להרחיב ולהציג קטגוריות מוסתרות.

מתחת לקטגוריות, תוכל לראות את מצב הווירוסים בפועל על גבי מפת העולם. הנוכחות של וירוס בכל מדינה מצוין באמצעות צבע (ככל שהצבע כהה יותר, המספר גבוה יותר). מדינות ללא נתונים מסומנות באפור. ריחוף עם סמן העכבר מעל המדינה יציג נתונים עבור המדינה שנבחרה. באפשרותך לבחור את היבשת הספציפית והיא תוצג בתצוגה מוגדלת באופן אוטומטי.

החלק האחרון בדוח האבטחה מאפשר לך להפעיל את התכונות להלן:

- בקרת הורים
- מערכת נגד גניבה

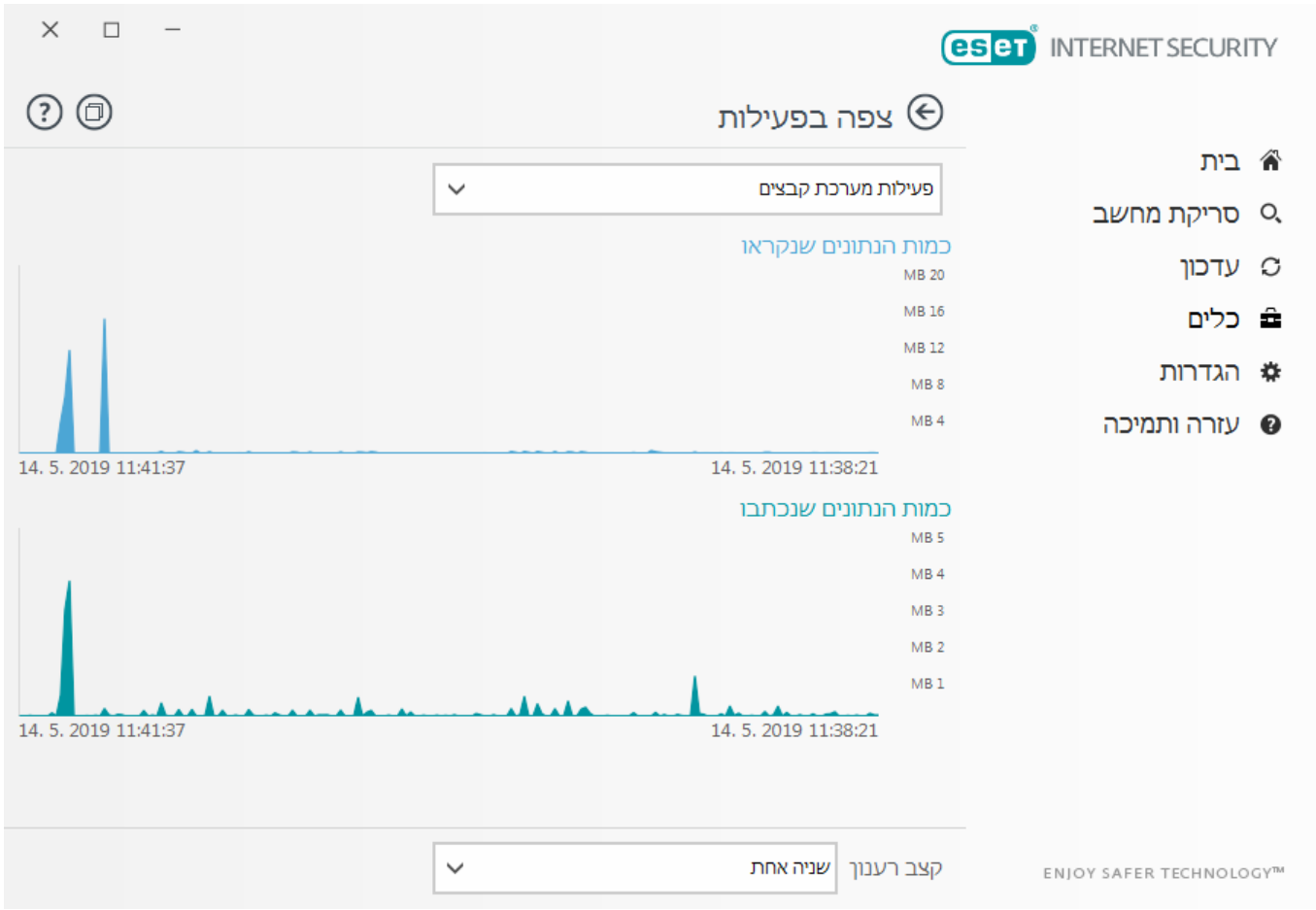
לאחר ההפעלה של תכונה, היא לא תוצג עוד כמושבתת בדוח האבטחה.

לחיצה על גלגל השיניים ⚙ בפינה השמאלית העליונה מאפשרת לך **להפעיל/להשבית הודעות של דוח אבטחה** או לבחור האם הנתונים יוצגו עבור 30 הימים האחרונים או מאז שהמוצר הופעל. אם התקנת את ESET Internet Security לפי פחות מ-30 ימים, אזי תוכל לבחור רק את מספר הימים שחלפו מתאריך ההתקנה. התקופה של 30 ימים מוגדרת כברירת מחדל.

איפוס נתונים ינקה את כל הנתונים הסטטיסטיים ויסיר את הנתונים הקיימים עבור דוח אבטחה. יש לאשר פעולה זו מלבד במקרה של ביטול הבחירה של האפשרות **שאל לפני איפוס נתונים סטטיסטיים** במסך **הגדרות מתקדמות** > **ממשק משתמש** > **התראות והודעות** > **הודעות אישור**.

צפייה בפעילות

כדי לראות את **פעילות מערכת הקבצים** בגרף, לחץ על **כלים** > **כלים נוספים** > **צפה בפעילות**. בחלק התחתון של הגרף נמצא ציר זמן המתעד את פעילות מערכת הקבצים בזמן אמת, בהתאם לטווח הזמן שנבחר. כדי לשנות את טווח הזמן, בחר אפשרות מתוך התפריט הנפתח **קצב רענון**.



האפשרויות הבאות זמינות:

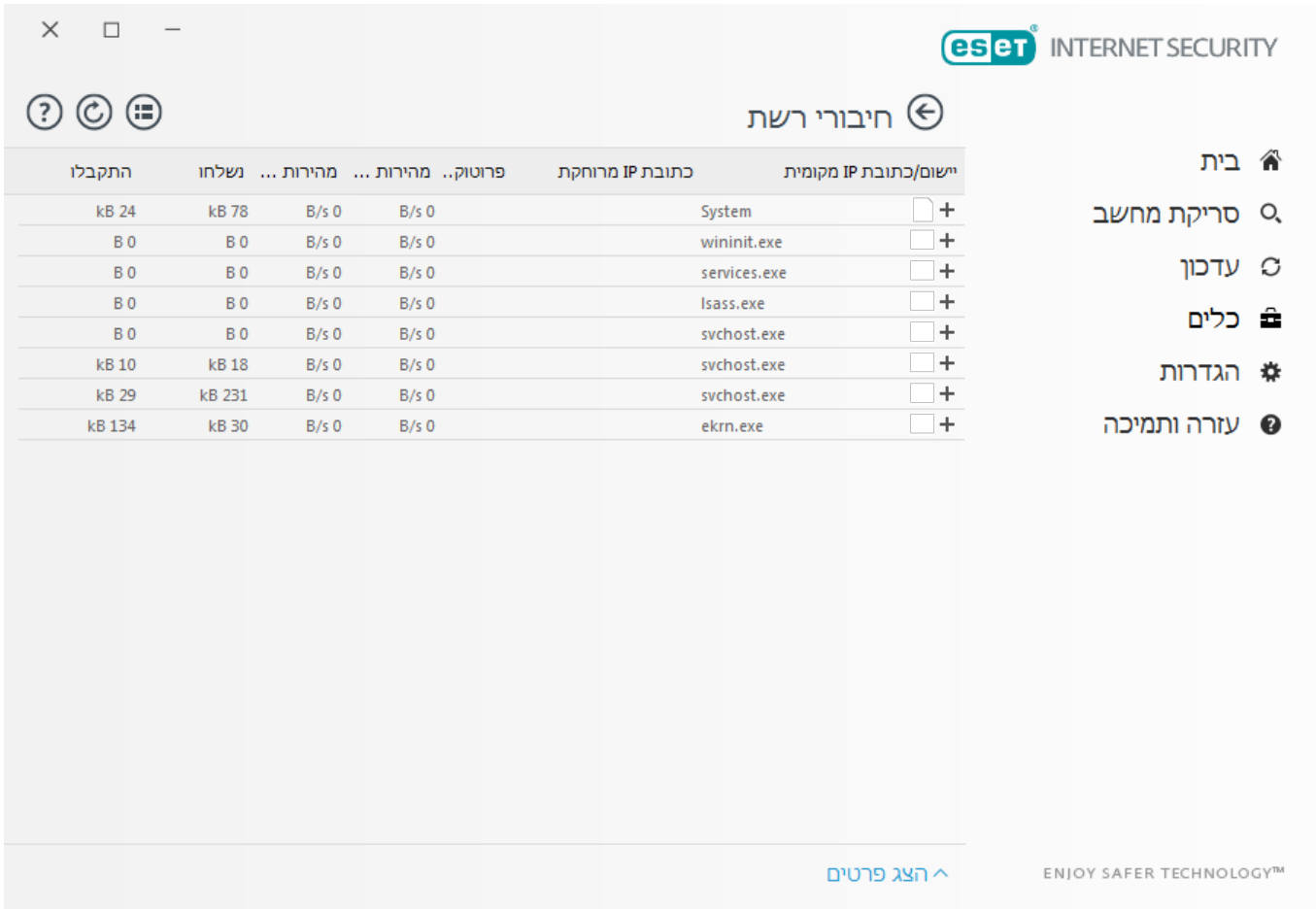
- **שלב: שנייה 1** – הגרף עובר רענון מדי שנייה וציר הזמן מכסה את 10 השניות האחרונות.
- **שלב: דקה 1 (24 השעות האחרונות)** – הגרף עובר רענון מדי דקה וציר הזמן מכסה את 24 השעות האחרונות.
- **שלב: שעה 1 (החודש האחרון)** – הגרף עובר רענון מדי שעה וציר הזמן מכסה את החודש האחרון.
- **שלב: שעה 1 (החודש שנבחר)** – הגרף עובר רענון מדי שעה וציר הזמן מכסה את X החודשים שנבחרו.

הציר האנכי של **גרף פעילות מערכת הקבצים** מייצג נתונים שנקראו (צבע כחול) ונתונים שנכתבו (צבע טורקיז). שני הערכים נתונים ב-KB (קילו-בתים) או ב-GB/MB. אם תעביר את העכבר מעל הנתונים שנקראו או הנתונים שנכתבו במקרא שמתחת לגרף, הגרף יציג רק נתונים עבור סוג פעילות זה.

באפשרותך גם לבחור **פעילות רשת** בתפריט הנפתח. תצוגת הגרף והאפשרויות עבור **פעילות מערכת קבצים** ו**פעילות רשת** הן זהות, למעט העובדה שהשנייה מביניהן מציגה את הנתונים שהתקבלו (צבע כחול) ואת הנתונים שנשלחו (צבע טורקיז).

חיבורי רשת

במקטע חיבורי הרשת תוכל לראות רשימת חיבורים פעילים וממתינים. הדבר יוכל לסייע לך לפקח על כל היישומים היוצרים חיבורים יוצאים.



בשורה הראשונה מוצגים שם היישום ומהירות העברת הנתונים שלו. להצגת רשימת החיבורים שביצע היישום (ומידע מפורט יותר) לחץ על +.

עמודות

יישום/כתובת IP מקומית – שם של יישום, כתובות IP מקומיות ויציאות תקשורת.

כתובת IP מרוחקת – IP ומספר יציאה של המחשב המרוחק המסוים.

פרוטוקול – פרוטוקול ההעברה שבו נעשה שימוש.

מהירות העלאה/מהירות הורדה – המהירות הנוכחית של הנתונים היוצאים והנכנסים.

נשלח/התקבל – כמות הנתונים שהועברו בחיבור.

הצג פרטים – בחר אפשרות זו כדי להציג מידע מפורט על החיבור שנבחר.

לחץ באמצעות לחצן העכבר הימני על חיבור מסוים כדי לראות אפשרויות נוספות, הכוללות:

פענח שמות מארחים – אם ניתן, כל כתובות הרשת מוצגות בתבנית DNS, ולא בתבנית כתובת ה-IP המספרית.

הצב חיבורי TCP בלבד – הרשימה מציגה רק חיבורים המשתייכים לחבילה של פרוטוקול TCP.

הצג חיבורים מאזינים – בחר באפשרות זו כדי להציג רק חיבורים, כאשר אין תקשורת כרגע, אולם המערכת פתחה יציאה וממתינה לחיבור.

הצג חיבורים בתוך המחשב – בחר באפשרות זו כדי להציג רק חיבורים, כאשר הצד המרוחק הוא מערכת מקומית – המכונים חיבורי localhost.

מהירות רענון – בחר את תדירות הרענון של החיבורים הפעילים.

רענן כעת – טעינה מחדש של החלון **חיבור רשת**.

האפשרויות הבאות זמינות רק לאחר לחיצה על יישום או תהליך מסוימים, ולא על חיבור פעיל:

מנע זמנית תקשורת עבור התהליך – דחיית החיבורים הנוכחיים עבור היישום הנתון. אם נוצר חיבור חדש, חומת האש משתמשת בכלל שהוגדר מראש. תיאור של ההגדרות ניתן למצוא בסעיף הגדרת כללים ושימוש בהם.

אפשר זמנית תקשורת עבור התהליך – התרת החיבורים הנוכחיים עבור היישום הנתון. אם נוצר חיבור חדש, חומת האש משתמשת בכלל שהוגדר מראש. תיאור של ההגדרות ניתן למצוא בסעיף הגדרת כללים ושימוש בהם.

ESET SysInspector

ESET SysInspector היא אפליקציה שבודקת את המחשב שלך באופן יסודי ואוספת מידע מפורט על רכיבי מערכת, כגון מנהלי התקנים ואפליקציות, חיבורי רשת או הזנות רישום חשובות, ומעריכה את רמת הסיכון של כל אחד מהרכיבים. מידע זה מסוגל לסייע בזיהוי הסיבה לפעילות חשודה של המערכת, שעשויה להיגרם כתוצאה מאי-תאימות של תוכנה או חומרה או מהידבקות בתוכנה זדונית. ראה גם מדריך משתמש מקוון ל-ESET SysInspector.

החלון SysInspector מציג את המידע הבא את היומנים שנוצרו:

- **שעה** – שעת יצירת היומן.
- **הערה** – הערה קצרה.
- **משתמש** – שם המשתמש שיצר את היומן.
- **סטטוס** – סטטוס יצירת היומן.

הפעולות הבאות זמינות:

- **הצג** – פתיחת היומן שנוצר. באפשרותך גם ללחוץ באמצעות לחצן העכבר הימני על קובץ יומן נתון ולבחור באפשרות **הצג** בתפריט ההקשר.
- **השוואה** – השוואה בין שני יומנים קיימים.
- **צור...** – יצירת יומן חדש. אנא המתן עד ש-ESET SysInspector יסיים את פעולתו (סטטוס היומן יוצג כיומן שנוצר) לפני שתנסה לגשת ליומן.
- **הסר** – הסרת היומנים שנבחרו מהרשימה.

הפריטים הבאים זמינים בתפריט ההקשר בעקבות בחירה של קובץ יומן אחד או יותר:

- **הצג** – פתיחת היומן שנבחר ב-ESET SysInspector (פונקציה הזהה ללחיצה כפולה על יומן).
- **השוואה** – השוואה בין שני יומנים קיימים.
- **צור...** – יצירת יומן חדש. אנא המתן עד ש-ESET SysInspector יסיים את פעולתו (סטטוס היומן יוצג כיומן שנוצר) לפני שתנסה לגשת ליומן.
- **הסר** – הסרת היומנים שנבחרו מהרשימה.
- **מחק הכול** – מחיקת כל היומנים.
- **יצא...** – ייצוא היומן לקובץ xml. או לקובץ xml. מכווץ.

מתזמן

המתזמן מנהל ומפעיל משימות מתוזמנות עם תצורה ומאפיינים שהוגדרו מראש.

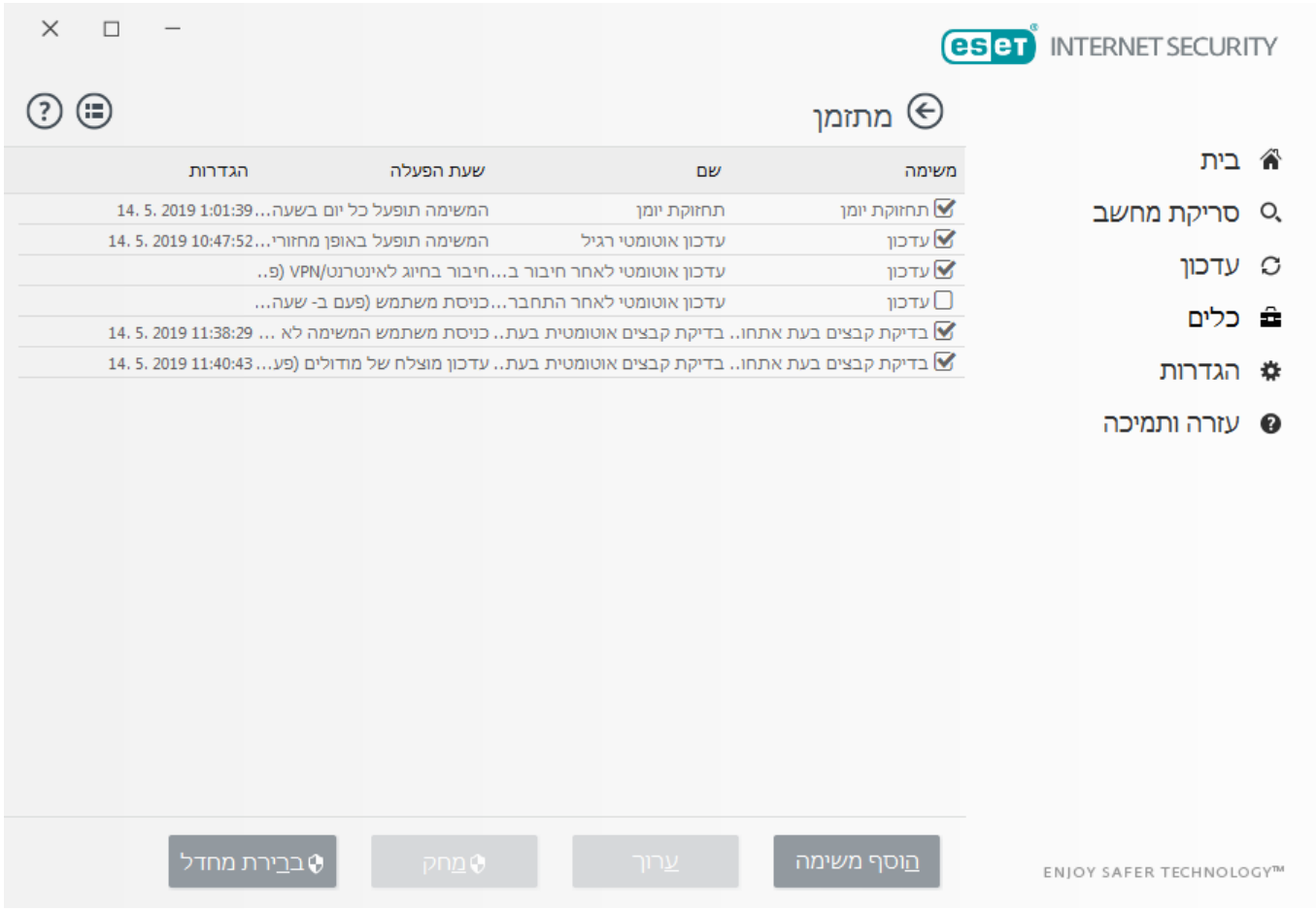
ניתן לגשת אל המתזמן מחלון התוכנית הראשי של ESET Internet Security על-ידי לחיצה על **כלים** > **כלים נוספים** > **מתזמן**. ה**מתזמן** מכיל רשימה של כל המשימות המתוזמנות ומאפייני תצורה, כגון התאריך והשעה שנקבעו ופרופיל הסריקה שבו נעשה שימוש.

המתזמן משמש לתזמון המשימות הבאות: עדכון מודולים, משימת סריקה, בדיקת קובץ אתחול מערכת ותחזוקת יומן. באפשרותך להוסיף או למחוק משימות ישירות מחלון המתזמן הראשי (לחץ על **הוסף משימה** או **מחק** בחלק התחתון). באפשרותך להחזיר את רשימת המשימות המתוזמנות לברירת מחדל ולמחוק את כל השינויים על-ידי לחיצה על **ברירת מחדל**. לחץ באמצעות לחצן העכבר הימני במקום כלשהו בחלון המתזמן כדי לבצע את הפעולות הבאות: הצגת מידע מפורט, ביצוע המשימה באופן מיידי, הוספת משימה חדשה ומחיקת משימה קיימת. השתמש בתיבות הסימון שבתחילת כל הזנה כדי להפעיל/לבטל הפעלה של המשימות.

כברירת מחדל, המשימות המתוזמנות הבאות מוצגות ב**מתזמן**:

- **תחזוקת יומן**
- **עדכון אוטומטי רגיל**
- **עדכון אוטומטי לאחר חיבור בחיוג**
- **עדכון אוטומטי לאחר התחברות של המשתמש**
- **בדיקת קובץ אתחול אוטומטית** (לאחר התחברות של המשתמש)
- **בדיקת קובץ אתחול אוטומטית** (לאחר עדכון מוצלח של מנגנון האיתור)

כדי לערוך את ההגדרות של משימה מתוזמנת קיימת (הן ברירת המחדל והן המוגדרת על-ידי המשתמש), לחץ באמצעות לחצן העכבר הימני ואז לחץ על **ערוך...** או בחר את המשימה שברצונך לשנות ולחץ על **ערוך**.



הוספת משימה חדשה

1. לחץ על **הוסף משימה** בחלק התחתון של החלון.

2. הזן שם למשימה.

3. בחר את המשימה הרצויה מהתפריט הנפתח:

- **הפעלת יישום חיצוני** – תזמון ההפעלה של יישום חיצוני.
- **תחזוקת יומן** – קובצי היומן מכילים גם שאריות מרשומות שנמחקו. משימה זו ממטבת את הרשומות בקובצי היומן על בסיס קבוע כדי שיופעלו ביעילות.
- **בדיקת קובץ אתחול מערכת** – הקבצים המורשים לפעול בעת אתחול המערכת או התחברות אליה.
- **צור תמונת מצב של המחשב** – יצירת תמונת מחשב של ESET SysInspector - איסוף מידע מפורט על חיבורי המערכת (לדוגמה מנהלי התקן, יישומים) והערכת רמת הסיכון של כל אחד מהרכיבים.
- **סריקת מחשב לפי דרישה** – ביצוע סריקה של הקבצים והתיקיות במחשב שלך.
- **עדכון** – תזמון משימת עדכון על-ידי עדכון המודולים.

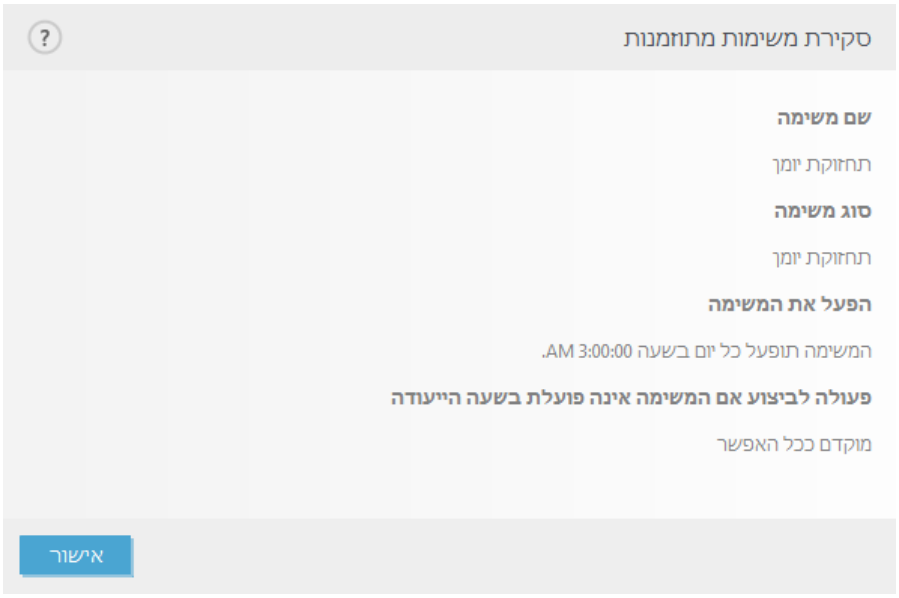
4. העבר את המתג **מאופשר** למצב פעיל אם ברצונך להפעיל את המשימה (באפשרותך לעשות זאת מאוחר יותר על-ידי סימון/ביטול הסימון בתיבה שברשימת המשימות המתוזמנות), לחץ על **הבא** ובחר אחת מאפשרויות התזמון הבאות:

- **פעם אחת** – המשימה תבוצע בתאריך ובשעה שהוגדרו מראש.
- **שוב ושוב** – המשימה תבוצע במרווח הזמנים שצוין.
- **יומית** – המשימה תופעל שוב ושוב מדי יום בשעה המפורטת.
- **שבועית** – המשימה תופעל ביום ובשעה הנבחרים.
- **מופעלת על-ידי אירוע** – המשימה תבוצע באירוע שצוין.

5. **בחר דלג על המשימה בעת פעולה בכוח הסוללה** כדי למזער את משאבי המערכת כאשר מחשב נייד מופעל בכוח סוללה. משימה זו תופעל בתאריך ובשעה שצוינו בשדות **ביצוע המשימה**. אם המשימה לא הופעלה בשעה שהוגדרה, באפשרותך לציין מתי היא תבוצע שוב:

- **במועד המתוזמן הבא**
- **בהקדם האפשרי**
- **מיידית, אם הזמן שחלף מאז ההפעלה האחרונה חורג מערך שצוין** (את פרק הזמן ניתן להגדיר באמצעות תיבת הגלילה **זמן מההפעלה האחרונה**)

באפשרותך לסקור את המשימה המתוזמנת על-ידי לחיצה ימנית ואז לחיצה על **הצג פרטי משימה**.



כלי ניקוי המערכת

כלי ניקוי המערכת הוא כלי שמסייע בשחזור המחשב למצב שמיש לאחר ניקוי האיום. תוכנות זדוניות יכולות להשבית את כלי השירות של המערכת כגון עורך הרישום, מנהל המשימות או עדכוני Windows. כלי ניקוי המערכת משחזר את ערכי והגדרות ברירת המחדל של מערכת נתונה בלחיצה בודדת.

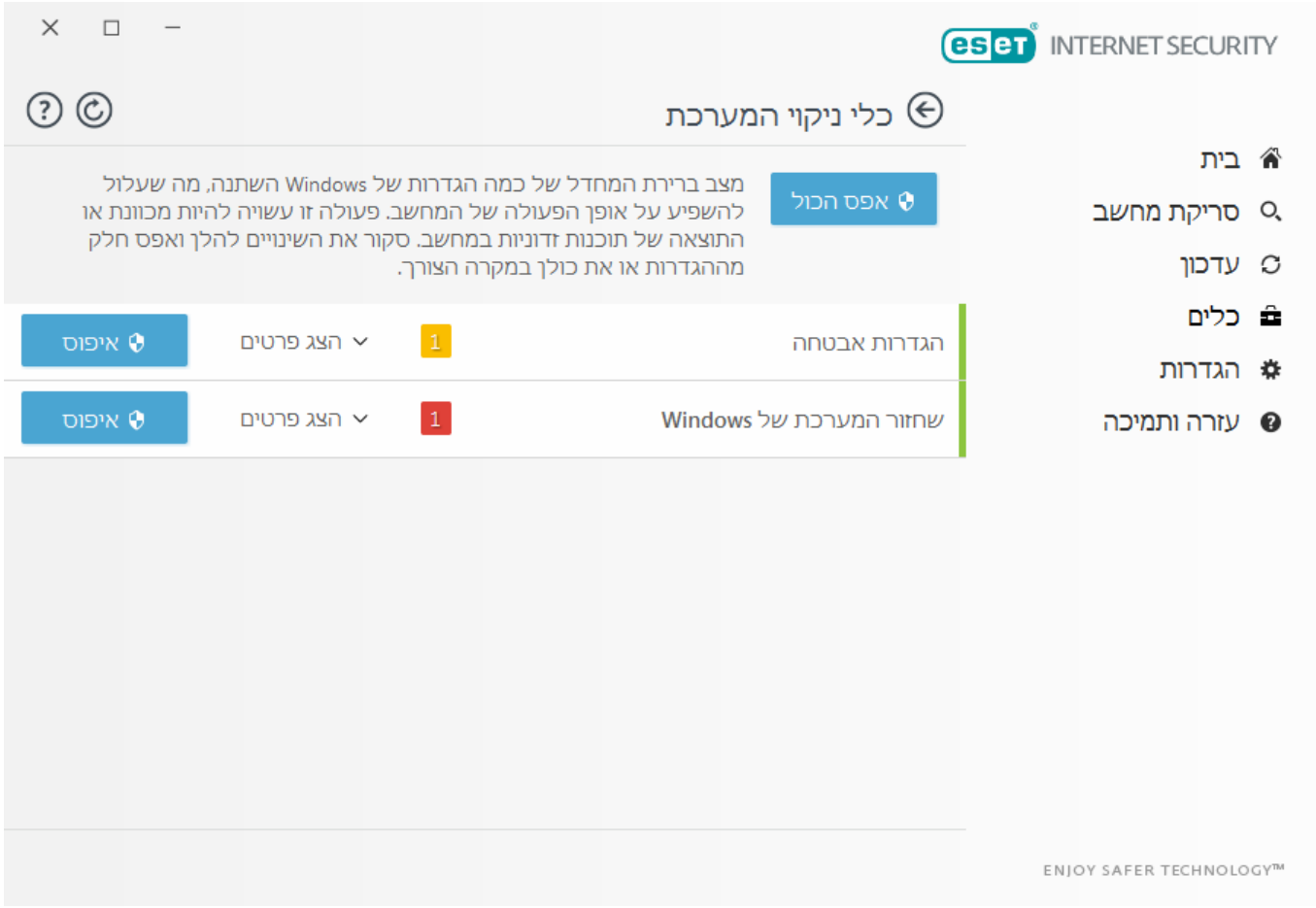
כלי ניקוי המערכת מדווח על בעיות מחמש קטגוריות של הגדרות:

- **הגדרות אבטחה**: שינויים בהגדרות שעשויים לגרום לפגיעות מוגברת של המחשב, כגון Windows Update
- **הגדרות מערכת**: שינויים בהגדרות המערכת, שיכולים לשנות אופן הפעולה של המחשב, כגון שיוכי קבצים
- **מראה המערכת**: הגדרות שמשפיעות על מראה המערכת, כגון הרקע של שולחן העבודה (טפט)
- **תכונות מושבתות**: תכונות ויישומים חשובים מסוימים הניתנים להשבתה
- **שחזור המערכת של Windows**: הגדרות של התכונה 'שחזור המערכת של Windows', המאפשרות לך להחזיר את המערכת

ניתן לבקש את ניקוי המערכת:

- כאשר נמצא איום
- כאשר המשתמש לוחץ על **איפוס**

באפשרותך לסקור את השינויים ולאפס את ההגדרות במידת הצורך.



הערה
רק משתמש עם הרשאות מנהל מערכת יכול לבצע פעולה בכלי ניקוי המערכת.

ESET SysRescue Live

ESET SysRescue Live הוא כלי שירות ללא תשלום המאפשר לך ליצור תקליטור CD/DVD או כונן USB הניתנים לאתחול לצורך שחזור. באפשרותך לאתחל מחשב נגוע מתוך מדיית השחזור וכך לבצע סריקה לאיתור תוכנות זדוניות ולנקות קבצים נגועים.

היתרון העיקרי של ESET SysRescue Live הוא העובדה שהוא פועל ללא תלות במערכת ההפעלה המארחת, אך יש לו גישה ישירה לדיסק ולמערכת הקבצים. מצב זה מאפשר להסיר איומים שמחיקתם עלולה להיות בלתי אפשרית בתנאי הפעלה רגילים (למשל כאשר מערכת ההפעלה פועלת וכו').

- עזרה מקוונת עבור ESET SysRescue Live

הגנה מבוססת ענן

ESET LiveGrid® (אשר בנוי על מערכת האזהרה המוקדמת המתקדמת ESET ThreatSense.Net) משתמש בנתונים שהגישו משתמשי ESET מכל רחבי העולם ושולח אותם אל מעבדת המחקר של ESET. על-ידי אספקת דוגמאות חשודות ומטה-נתונים מהשטח, ESET LiveGrid® מאפשר לנו להגיב מיידית לצורכי הלקוחות שלנו ולהמשיך לשמור על כושר התגובה של ESET לאיומים

החדשים ביותר.

משתמש יכול לבדוק את המוניטין של תהליכים פועלים וקבצים ישירות מהממשק או מהתפריט ההקשרי של התוכנית, עם מידע נוסף הזמין מ-ESET LiveGrid®. ישנן שתי אפשרויות:

1. תוכל לבחור לא להפעיל את ESET LiveGrid®. לא תאבד שום פונקציונליות של התוכנה, אולם במקרים מסוימים ESET Internet Security עשוי להגיב לאיומים חדשים מהר יותר מעדכון מנגנון האיתור כאשר ESET LiveGrid® מופעל.
2. תוכל לקבוע את תצורת ESET LiveGrid® לשליחת מידע אנונימי על איומים חדשים ועל המקום שבו נכלל הקוד המאיים החדש. ניתן לשלוח קובץ זה אל ESET לצורך ניתוח מפורט. חקירת איומים אלה תסייע ל-ESET לעדכן את יכולות הזיהוי שלה.

ESET LiveGrid® יאסוף מידע על האיומים החדשים שזוהו אשר קשורים למחשב שלך. מידע זה עשוי לכלול דגימה או עותק של קובץ שבו האיום הופיע, את הנתיב לקובץ, שם הקובץ, התאריך והשעה, התהליך שבו האיום הופיע במחשב שלך והמידע על מערכת ההפעלה של המחשב שלך.

כברירת מחדל, ESET Internet Security מוגדר לשלוח קבצים חשודים לצורך ניתוח מפורט למעבדת הווירוסים של ESET. קבצים עם סיומות מסוימות, כגון *.doc* או *.xls*, כמעט תמיד אינם נכללים. באפשרותך גם להוסיף סיומות אחרות, אם ישנם קבצים מסוימים שאתה או הארגון שלך רוצים להימנע משליחתם.

מידע קשור
קרא עוד על ESET LiveGrid® במילון.
ראה את ההנחיות המאוירות שלנו הזמינות באנגלית ובמספר שפות אחרות לגבי אופן ההפעלה או ההשבתה של ESET LiveGrid® ב-ESET Internet Security.

מערכת המוניטין של ESET LiveGrid® מספקת רישום בענן ברשימות לבנות וברשימות שחורות. כדי לגשת להגדרות של ESET LiveGrid®, לחץ על **F5** כדי לעבור להגדרות המתקדמות והרחב את **מנגנון איתור** > הגנה מבוססת ענן.

הגנה מבוססת ענן בהגדרות מתקדמות

הפעל את מערכת המוניטין של ESET LiveGrid® (מומלץ) – מערכת המוניטין של ESET LiveGrid® משפרת את יעילות הפתרונות של ESET נגד תוכנות זדוניות על-ידי השוואת קבצים שנסרקו למסד נתונים של פריטים ברשימה לבנה וברשימה שחורה, אשר ממוקם בענן.

אפשר את מערכת המשוב של ESET LiveGrid® – נתונים יישלחו למעבדת המחקר של ESET להמשך ניתוח.

שלח דוחות קריסה ונתוני אבחון – שלח נתונים כגון דוחות קריסה, ומצבורי זיכרון של מודולים.

שלח נתונים סטטיסטיים אנונימיים – אפשר ל-ESET לאסוף מידע אודות איומים שזוהו לאחרונה כגון שם האיום, תאריך ושעת האיתור, שיטת האיתור ומטה-נתונים קשורים, גרסת המוצר ותצורתו, כולל מידע אודות המערכת שלך.

דואר אלקטרוני ליצירת קשר (אופציונלי) – באפשרותך להוסיף לכל הקבצים החשודים את כתובת הדואר בה ניתן ליצור עמך קשר, וייתכן שנשתמש בה אם יידרש מידע נוסף לצורך הניתוח. שים לב: לא תקבל תשובה מ-ESET אם לא יהיה צורך במידע נוסף.

שליחת דוגמאות

שליחה אוטומטית של דוגמאות של פריטים נגועים

אפשרות זו תשלח את כל הדוגמאות של פריטים נגועים ל-ESET למטרות ניתוח ושיפור ביצועי איתור עתידיים. האפשרויות הבאות זמינות:

- כל הדוגמאות של פריטים נגועים
- כל הדוגמאות למעט מסמכים

• אל תשלח

שליחה אוטומטית של דוגמאות של פריטים חשודים

• **קובצי הפעלה** – כולל קבצים כגון: .exe, .dll, .sys
• **קובצי ארכיון** – כולל סוגי קבצים כגון: .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
• **קובצי Script** – כולל סוגי קבצים כגון: .bat, .cmd, .hta, .js, .vbs, .ps1.
• **אחר** – כולל סוגי קבצים כגון: .jar, .reg, .msi, .sfw, .lnk.
• **דוא"ל החשוד כדואר זבל** – אפשרות זו תאפשר שליחה של חלקים מהודעות דוא"ל שעשויות להיות דואר זבל או את ההודעות המלאות עם קבצים מצורפים אל ESET להמשך ניתוח. הפעלת אפשרות זו תשפר את היכולת הכללית לאיתור דואר זבל, כולל שיפורים באיתור של דואר זבל עבורך בעתיד.
• **מסמכים** – כולל מסמכים של Microsoft Office או קובצי PDF עם תוכן פעיל.

אי הכללה

מסנן החריגות מאפשר לך לא לכלול קבצים/תיקיות מסוימים בחומר המוגש (למשל, כדאי שלא להכליל קבצים שעשויים לכלול מידע סודי, כגון מסמכים או גיליונות אלקטרוניים). הקבצים המפורטים בו לעולם לא יישלחו לניתוח במעבדת ESET, גם אם הם מכילים קוד חשוד. סוגי הקבצים הנפוצים ביותר (למשל doc.) אינם נכללים כברירת מחדל. אם תרצה תוכל להוסיף אותם לרשימת הקבצים שאינם נכללים.

אם השתמשת ב-ESET LiveGrid® בעבר והשבתת אותו, ייתכן שעדיין ישנן חבילות נתונים לשליחה. גם לאחר ביטול ההפעלה חבילות אלו יישלחו אל ESET. אחרי שכל המידע הנוכחי יישלח, לא ייווצרו חבילות נוספות.

קבצים חשודים

אם אתה מאתר קובץ חשוד, באפשרותך לשלוח אותו לניתוח במעבדת המחקר של ESET. אם זהו יישום זדוני, זיהויו יתווסף לעדכון חתימות הווירוסים הבא.

מסנן חריגות – החריגות מאפשר לך לא לכלול קבצים/תיקיות מסוימים בהגשה. הקבצים המפורטים בו לעולם לא יישלחו לניתוח במעבדת המחקר של ESET, גם אם הם מכילים קוד חשוד. לדוגמה, כדאי להחריג קבצים שעשויים לכלול מידע סודי, כגון מסמכים או גיליונות אלקטרוניים. סוגי הקבצים הנפוצים ביותר (למשל doc.) מוחרגים כברירת מחדל. אם תרצה תוכל להוסיף אותם לרשימת הקבצים המוחרגים.

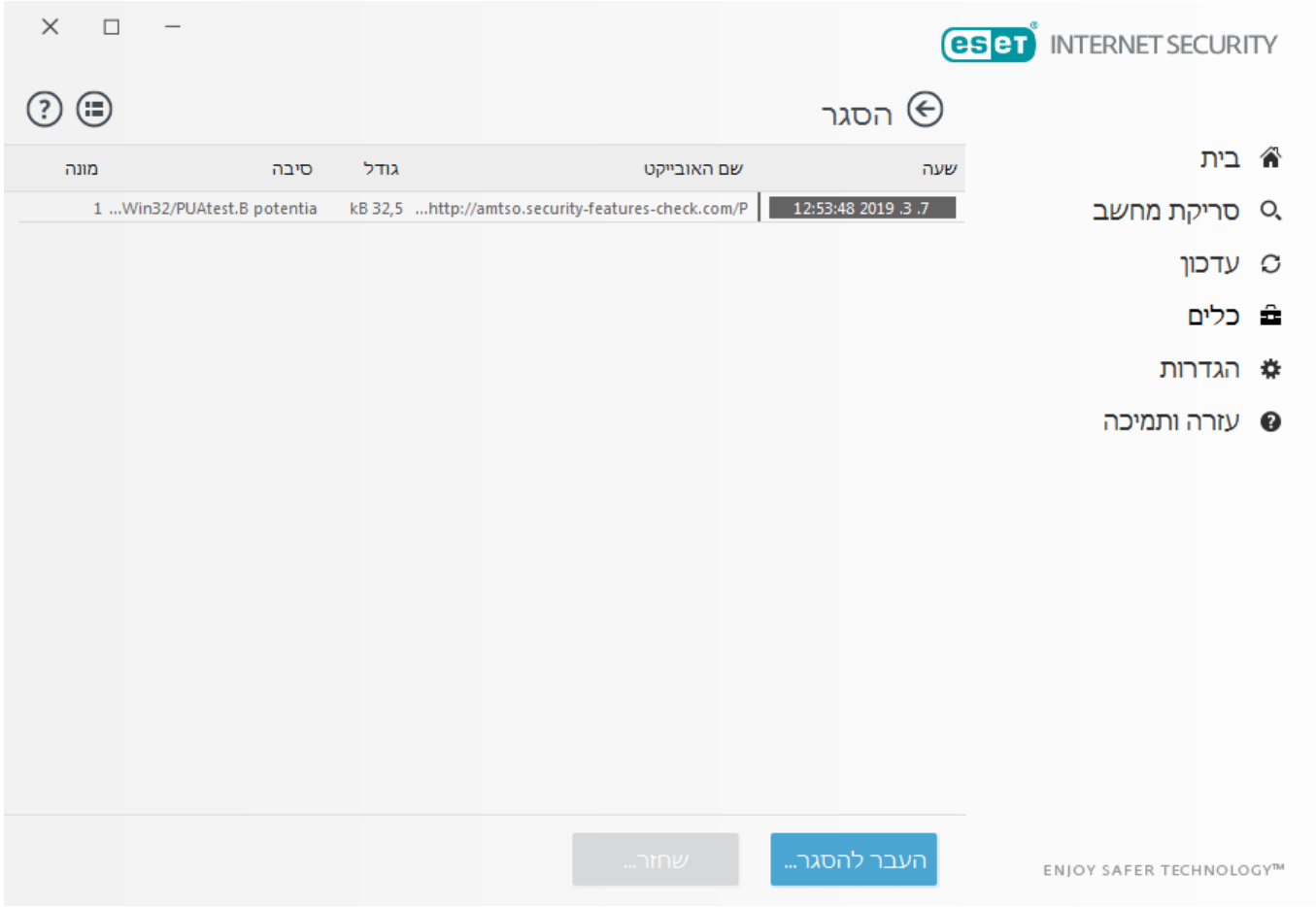
דואר אלקטרוני ליצירת קשר (אופציונלי) – באפשרותך להוסיף לכל הקבצים החשודים את כתובת הדואר בה ניתן ליצור עמך קשר, וייתכן שנשתמש בה אם יידרש מידע נוסף לצורך הניתוח. שים לב: לא תקבל תשובה מ-ESET אם לא יהיה צורך במידע נוסף.

בחר **אפשר רישום ביומן** כדי ליצור יומן אירועים לתיעוד הגשות של קבצים ומידע סטטיסטי. פעולה זו תאפשר רישום ביומן האירועים כאשר נשלחים קבצים או נתונים סטטיסטיים.

הסגר

התפקיד העיקרי של ההסגר הוא לאחסן בבטחה את הקבצים הנגועים. יש להעביר קבצים להסגר אם לא ניתן לנקותם, אם מחיקתם אינה בטיחותית או מומלצת או אם הם זוהו בשוגג על-ידי ESET Internet Security.

תוכל לבחור להעביר להסגר כל קובץ שתרצה. לחלופין, באפשרותך גם להשתמש בתכונה של גרירה ושחרור כדי להעביר קובץ להסגר באופן ידני על-ידי לחיצה על הקובץ, העברת סמן העכבר לאזור המסומן תוך לחיצה על לחצן העכבר ולאחר מכן שחרור הלחיצה. לאחר מכן, האפליקציה תועבר לחזית. אפשרות זו מומלצת כאשר קובץ מסוים פועל בצורה חשודה אך אינו מזוהה על-ידי סורק האנטי-וירוס. את הקבצים שהועברו להסגר ניתן לשלוח לניתוח במעבדת המחקר של ESET.



את הקבצים המאוחסנים בתיקיית ההסגר ניתן לראות בטבלה המציגה את תאריך ושעת ההסגר, הנתיב למיקום המקורי של הקובץ הנגוע, גודלו בבתים, הסיבה (לדוגמה, האובייקט נוסף על-ידי המשתמש), ומספר האיומים (לדוגמה, אם מדובר בארכיון המכיל מספר חדירות).

העברת קבצים להסגר

ESET Internet Security מעביר להסגר באופן אוטומטי את הקבצים שהוסרו (אם לא ביטלת אפשרות זו בחלון ההתראה). אם תרצה, תוכל להעביר להסגר באופן ידני כל קובץ חשוד על-ידי לחיצה על **הסגר...** או על-ידי לחיצה על הקובץ, העברת סמן העכבר לאזור המסומן תוך לחיצה על לחצן העכבר ולאחר מכן שחרור הלחיצה. לאחר מכן, הקובץ יועבר להסגר. במקרה זה, הקובץ המקורי לא יוסר ממיקומו המקורי. ניתן להשתמש בתפריט ההקשר גם למטרה זו; לחץ באמצעות לחצן העכבר הימני בחלון **הסגר** ולחץ על **הסגר...**.

שחזור מההסגר

את הקבצים שהועברו להסגר ניתן גם לשחזר במיקומם המקורי. לשם כך השתמש בתכונה **שחזור**, אשר זמינה דרך תפריט ההקשר, בלחיצה ימנית על קובץ נתון בחלון ההסגר. אם קובץ מסוים סומן כיישום שעשוי להיות בלתי רצוי, האפשרות **שחזר ואל תכלול בסריקה** מופעלת. קרא עוד על סוג היישום הזה במילון. תפריט ההקשר גם מציע אפשרות **שחזור אל...** שמאפשרת לך לשחזור קובץ במיקום שונה מזה שממנו נמחק.

מחק מהסגר לחץ לחיצה ימנית על פריט נתון ובחר באפשרות **מחק מהסגר**, או בחר בפריט שאותו ברצונך למחוק והקש על מקש **Delete** במקלדת. באפשרותך לבחור גם מספר פריטים ולמחוק אותם בו-זמנית.

> **הערה**
> אם התוכנית העבירה להסגר בשוגג קובץ שאינו מזיק, אנא אל תכלול את הקובץ בסריקה לאחר השחזור ושלח אותו לתמיכה הטכנית של ESET.

שליחת קובץ מההסגר.

אם העברת להסגר קובץ חשוד שהתוכנית לא זיהתה, או אם קובץ מסוים נקבע בשוגג כנגוע (לדוגמה על-ידי ניתוח היריסטיקה של

הקוד) וכתוצאה מכך הועבר להסגר, אנא שלח את הקובץ למעבדת הווירוסים של ESET. כדי לשלוח קובץ מתוך ההסגר, לחץ על הקובץ באמצעות לחצן העכבר הימני ובחר באפשרות **שלח לניתוח** מתוך תפריט ההקשר.

שרת Proxy

ברשתות LAN גדולות, ניתן לתווך את התקשורת בין המחשב והאינטרנט באמצעות שרת proxy. עם תצורה זו יש להגדיר את ההגדרות הבאות. אחרת התוכנית לא תוכל להתעדכן אוטומטית. במוצר ESET Internet Security, הגדרה של שרת proxy זמינה דרך שני מקטעים של עץ ההגדרות המתקדמות.

תחילה ניתן לקבוע את ההגדרות של שרת proxy ב**הגדרות מתקדמות**, תחת **כלים** > **שרת Proxy**. ציון שרת ה-proxy ברמה זו קובע את ההגדרות הכלליות של שרתי proxy ב-ESET Internet Security כולו. הפרמטרים כאן ישמשו את כל המודולים שצריכים חיבור לאינטרנט.

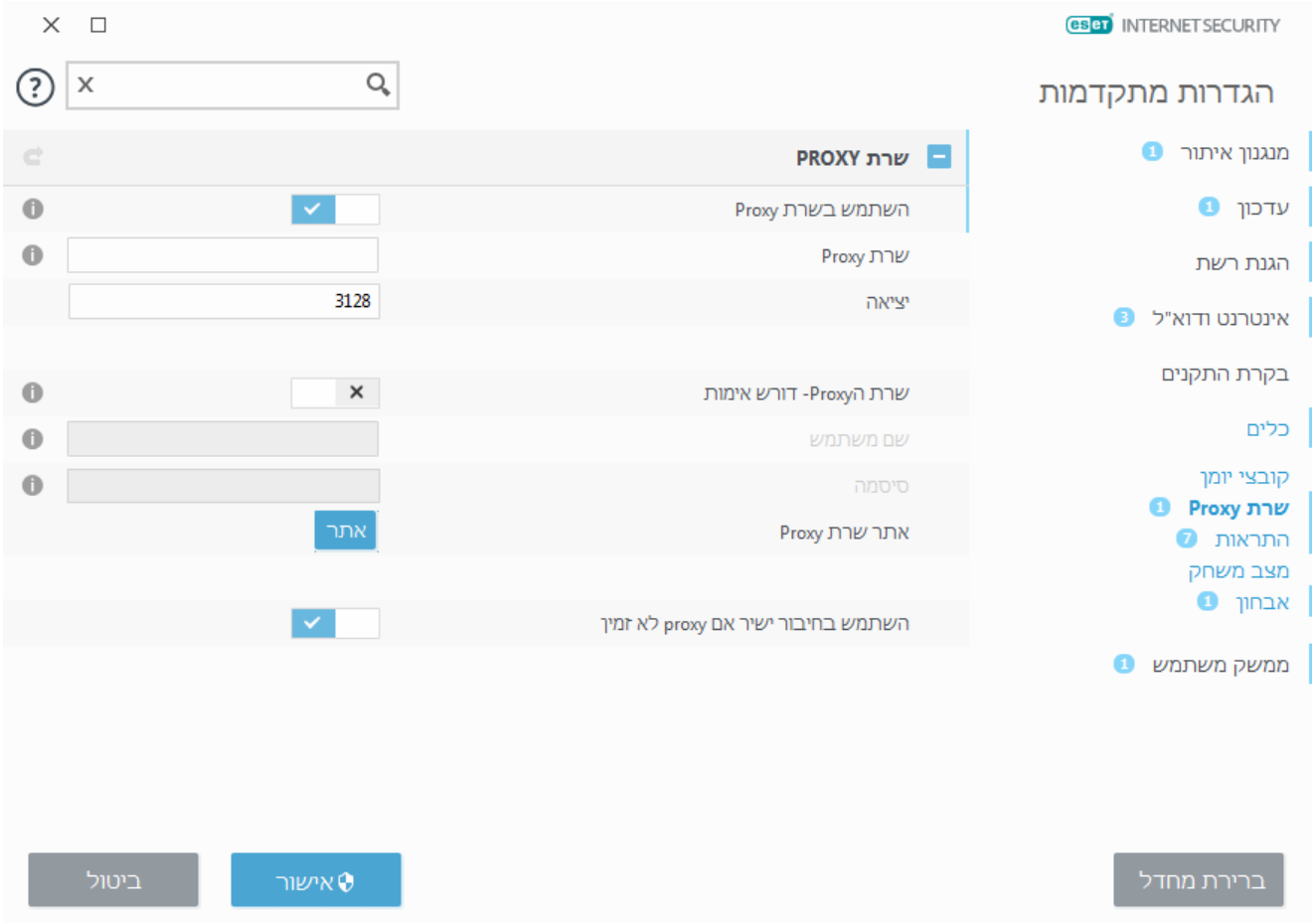
כדי לציין את ההגדרות של שרת proxy עבור רמה זו, בחר **השתמש בשרת proxy** והזן את כתובת שרת ה-proxy בשדה **שרת Proxy**, יחד עם מספר ה**יציאה** של שרת ה-proxy.

אם התקשורת עם שרת ה-proxy מחייבת אימות, בחר **שרת Proxy מחייב אימות** והזן **שם משתמש** חוקי ו**סיסמה** בשדות המתאימים. לחץ על **אתר שרת Proxy** כדי לאתר הגדרות של שרת proxy ולאכלס אותן אוטומטית. הפרמטרים המפורטים באפשרויות אינטרנט עבור Internet Explorer או Google Chrome יועתקו.

> **הערה**
> עליך להזין ידנית את שם המשתמש והסיסמה שלך בהגדרות **שרת Proxy**.

השתמש בחיבור ישיר אם proxy לא זמין - אם התצורה של ESET Internet Security הוגדרה להתחברות דרך proxy ואין אפשרות להגיע ל-proxy, ESET Internet Security יעקוף את ה-proxy וינהל תקשורת ישירה עם שרתי ESET.

את הגדרות שרת ה-Proxy ניתן לבסס גם דרך הגדרות עדכון מתקדמות (**הגדרות מתקדמות עדכון** > **פרופילים** > **עדכונים** > **אפשרויות חיבור** על-ידי בחירת **התחברות דרך שרת proxy** בתפריט הנפתח **מצב Proxy**). הגדרה זו חלה על פרופיל העדכון הנתון; היא מומלצת עבור מחשבים ניידים, שלעתים קרובות מקבלים עדכוני חתימות וירוסים ממיקומים מרוחקים. לקבלת מידע נוסף על הגדרה זו ראה הגדרות עדכון מתקדמות.



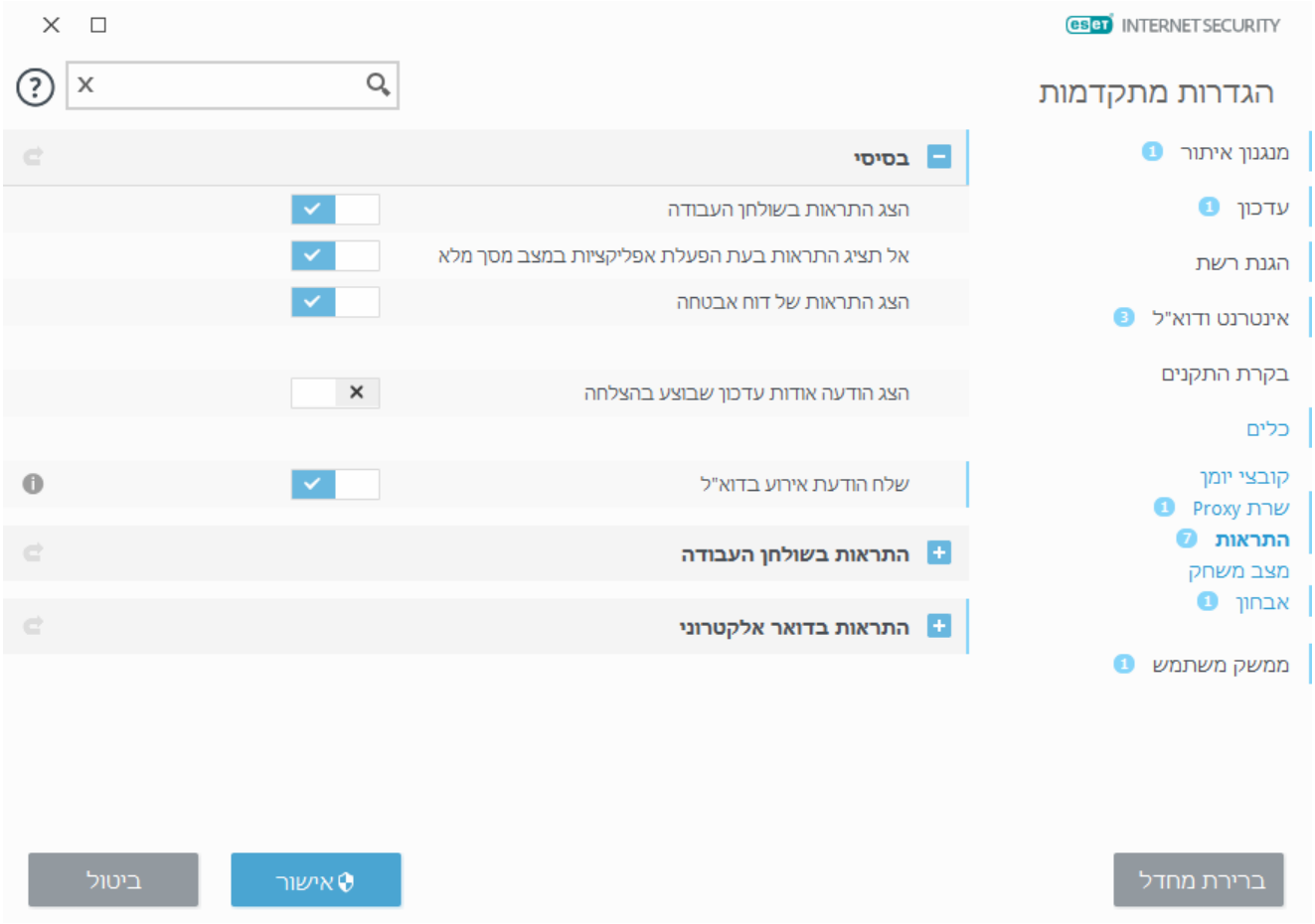
התראות

כדי לנהל את האופן שבו ESET Internet Security מודיע למשתמש על אירועים, נווט אל **הגדרות מתקדמות (F5)** > **כלים** > **התראות**. חלון הגדרת תצורה זה מאפשר לך להגדיר את סוגי ההתראות הבאים:

- התראות בשולחן העבודה – התראה בשולחן העבודה המוצגת כחלון מוקפץ קטן לצד שורת המשימות של המערכת.
- התראות בדוא"ל – התראות בדוא"ל נשלחות לכתובת הדוא"ל שצוינה.

במקטע **בסיסי**, השתמש במתגים המתאימים כדי להתאים את האפשרויות הבאות:

תיאור	ברירת מחדל	מתג
השבת כדי להסתיר התראות מוקפצות לצד שורת המשימות של המערכת. מומלץ להשאיר אפשרות זו מאופשרת כדי שהמוצר יוכל להודיע לך על אירוע חדש.	✓	**הצג התראות בשולחן העבודה**
השאר את האפשרות **אל תציג התראות בעת הפעלת אפליקציות במצב מסך מלא** מאופשרת כדי להעלים את כל ההתראות שאינן אינטראקטיביות.	✓	**אל תציג התראות בעת...**
אפשר לקבל התראה כאשר נוצרת גרסה חדשה של דוח אבטחה.	×	**הצג התראות של דוח אבטחה**
אפשר לקבל התראה כאשר המוצר מעדכן את הרכיבים שלו ואת המודולים של מנגנון האיתור.	×	**הצג הודעה אודות עדכון שבוצע בהצלחה**
אפשר כדי להפעיל התראות בדוא"ל.	×	**שלח התראה בדוא"ל**



הודעות שולחן עבודה

התראה בשולחן העבודה מיוצגת באמצעות חלון מוקפץ קטן לצד שורת המשימות של המערכת. כברירת מחדל, היא מוצגת במשך 10 שניות ונעלמת באיטיות. זוהי הדרך העיקרית שבה ESET Internet Security מתקשר עם המשתמש, מודיע על עדכוני מוצר שבוצעו בהצלחה, התקנים חדשים שחוברו, השלמה של משימות סריקת וירוסים או איומים חדשים שנמצאו.

המקטע **התראות בשולחן העבודה** מאפשר להתאים אישית את אופן הפעולה של התראות מוקפצות. ניתן להגדיר את המאפיינים הבאים:

משך זמן - קביעת משך הזמן שבו הודעת ההתראה תהיה גלויה. על הערך להיות בטווח של 3 עד 30 שניות.

שקיפות - קביעת השקיפות באחוזים של הודעת התראה. הטווח הנתמך הוא 0 (ללא שקיפות) עד 80 (שקיפות גבוהה מאוד).

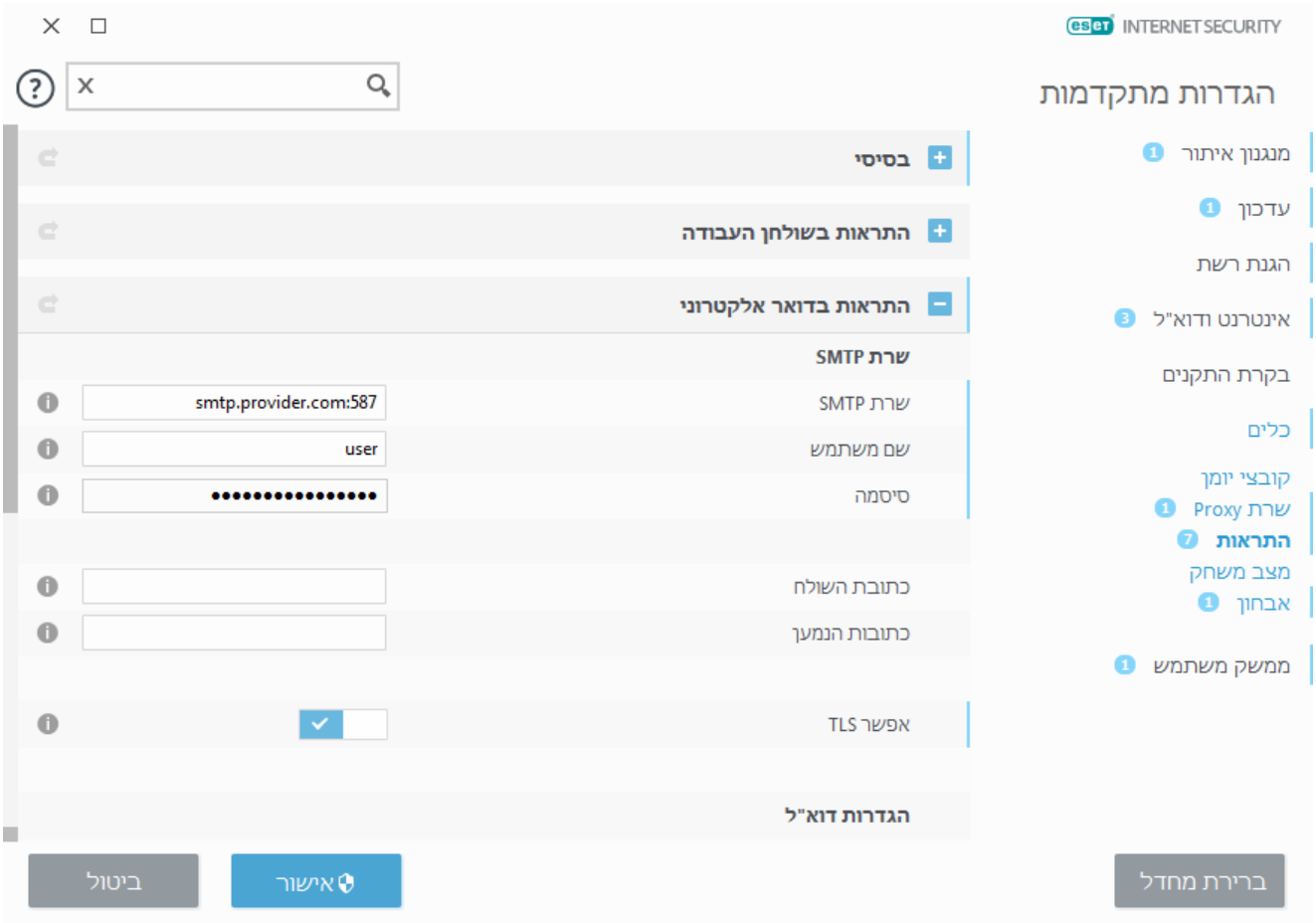
פירוט מינימלי של אירועים להצגה - בתפריט הנפתח באפשרותך לבחור את רמת החומרה ההתחלתית להצגת התראות:

- **אבחוני** – רישום מידע שנדרש להתאמה מפורטת של התוכנית ושל כל הרשומות שלעיל.
- **למסירת מידע** – תיעוד הודעות מסירת מידע, כגון אירועים יוצאי דופן ברשת, לרבות הודעות על עדכון מוצלח, בנוסף לכל הרשומות שלעיל.
- **אזהרות** – תיעוד שגיאות קריטיות והודעות אזהרה (הגנה מפני התגנבות אינה פועלת כהלכה או שהעדכון נכשל).
- **שגיאות** – שגיאות (לא הופעלה הגנה על מסמכים) ושגיאות קריטיות יתועדו.
- **קריטי** – רישום שגיאות קריטיות בלבד, כגון שגיאה בהפעלה של הגנת אנטי-וירוס או מערכת נגועה.

במערכות עם מספר משתמשים, הצגת התראות על המסך של משתמש זה – הקלד את שמות החשבון המלאים של משתמשים שיש לאפשר להם לקבל התראות בשולחן עבודה. לדוגמה, אם אתה משתמש במחשב שלך באמצעות חשבון אחר ולאחר מכן ברצונך להמשיך לקבל מידע על אירועים חדשים במוצר.

התראות בדואר אלקטרוני

ESET Internet Security יכול לשלוח אוטומטית התראות בדוא"ל כשמתרחש אירוע ברמת הפירוט שנבחרה. הפעל את האפשרות **שלח התראות בדוא"ל** כדי להפעיל התראות בדוא"ל.



SMTP server

שרת SMTP – שרת ה-SMTP שמשמש לשליחת התראות (למשל *smtp.provider.com:587*, היציאה המוגדרת מראש היא 25).

> **הערה**
> ESET Internet Security תומך בשרתי SMTP עם הצפנת TLS.

שם משתמש וסיסמה – אם שרת ה-SMTP מחייב אימות, יש לפרט בשדות אלו שם משתמש וסיסמה חוקיים כדי לגשת לשרת ה-SMTP.

כתובת השולח – קבע את כתובת השולח שתוצג בכותרת של הודעות ההתראה.

כתובות הנמענים – קבע את את כתובות הנמענים שיוצגו בכותרת של הודעות ההתראה. יש תמיכה בערכים מרובים. השתמש בנקודה-פסיק בתור מפריד.

הגדרות דוא"ל
בתפריט הנפתח **רמת פירוט מינימלית להתראות** באפשרותך לבחור את רמת החומרה ההתחלתית שממנה יישלחו התראות.

- **אבחוני** – רישום מידע שנדרש להתאמה מפורטת של התוכנית ושל כל הרשומות שלעיל.
- **למסירת מידע** – תיעוד הודעות מסירת מידע, כגון אירועים יוצאי דופן ברשת, לרבות הודעות על עדכון מוצלח, בנוסף לכל הרשומות שלעיל.
- **אזהרות** – תיעוד שגיאות קריטיות והודעות אזהרה (הגנה מפני התגנבות אינה פועלת כהלכה או שהעדכון נכשל).
- **שגיאות** – שגיאות (לא הופעלה הגנה על מסמכים) ושגיאות קריטיות יתועדו.

• **קריטי** – רישום שגיאות קריטיות בלבד, כגון שגיאה בהפעלה של הגנת אנטי-וירוס או מערכת נגועה.

אפשרTLS – אפשר שליחת הודעות והתראות הנתמכות על-ידי הצפנת TLS.

מרווח זמן שאחריו יישלחו התראות חדשות בדואר אלקטרוני (דקות) – זמן, בדקות, שאחריו יישלחו התראות חדשות בדואר אלקטרוני. אם תגדיר ערך זה כ-"0", ההתראות יישלחו מיידית.

שלח כל התראה בדואר אלקטרוני נפרד – כאשר אפשרות זו מופעלת, הנמען יקבל הודעת דואר אלקטרוני חדשה עבור כל התראה בודדת. מצב זה עלול להוביל לקבלת הודעות דואר אלקטרוני רבות בפרק זמן קצר.

תבנית הודעה

התקשורת בין התוכנית לבין משתמש מרוחק או מנהל מערכת מתבצעת באמצעות הודעות דוא"ל או הודעות LAN (באמצעות שירות העברת ההודעות של Windows). תבנית ברירת המחדל של הודעות ההתראה וההודעות תתאים לרוב המצבים. במקרים מסוימים, ייתכן שיהיה עליך לשנות את תבנית ההודעה של הודעות אירוע.

תבנית הודעות על אירועים – ההודעות על אירועים שמוצגות במחשבים מרוחקים.

תבנית הודעות התראה על איומים – להודעות התראה על איומים תבנית ברירת מחדל מוגדרת מראש. מומלץ שלא לשנות תבנית זו. עם זאת, בנסיבות מסוימות (למשל אם יש לך מערכת עיבוד דואר אלקטרוני אוטומטית), ייתכן שתצטרך לשנות את תבנית ההודעה.

ערכת תווים – המרת הודעת הדואר האלקטרוני לקידוד התווים של ANSI בהתאם להגדרות האזור של Windows (לדוגמה, windows-1250), Unicode (UTF-8), ACSII 7-bit (לדוגמה, "á" יוחלף ב-"a" וסימן לא מוכר יוחלף ב-"?") או יפנית (ISO-2022-JP).

השתמש בקידוד Quoted-printable – מקור הודעת הדואר האלקטרוני יקודד לתבנית Quoted-printable (QP), אשר משתמשת בתווי ASCII ומסוגלת לשדר תווים מקומיים מיוחדים כראוי בדואר אלקטרוני, בתבנית 8 סיביות (áéíóú).

- **%TimeStamp%** – התאריך והשעה של האירוע
- **%Scanner%** – המודול שבו מדובר
- **%ComputerName%** – שם המחשב שבו ההודעה אירעה
- **%ProgramName%** – התוכנית שהפיקה את ההתראה
- **%InfectedObject%** – שם הקובץ, ההודעה, או פריט אחר כלשהו שנדבקו
- **%VirusName%** – זיהוי ההדבקה
- **%Action%** – פעולה שננקטת לאחר חדירה
- **%ErrorDescription%** – תיאור אירוע שאינו וירוס

מילות המפתח **%InfectedObject%** ו-**%VirusName%** נמצאות בשימוש רק בהודעות אזהרה מפני איומים, ו-**%ErrorDescription%** נמצאת בשימוש בהודעות על אירועים.

בחירת דוגמה לניתוח

אם אתה מאתר במחשב קובץ חשוד או אתר אינטרנט חשוד, באפשרותך לשלוח אותו לניתוח במעבדת המחקר של ESET.

לפני שליחת דגימות אל ESET

אל תשלח דגימה אלא אם היא עומדת לפחות באחד מהקריטריונים להלן:

- המוצר של ESET שברשותך לא איתר כלל את הדגימה
- הדגימה זוהתה כאיום באופן שגוי
- איננו מקבלים קבצים אישיים (שאותם ברצונך ש-ESET תסרוק לאיתור תוכנות זדוניות) כדגימות (מעבדת המחקר של ESET אינה מבצעת סריקות לפי דרישה עבור משתמשים)
- השתמש בשורת נושא תיאורית וצרף כמה שיותר מידע על הקובץ (לדוגמה צילום מסך או אתר האינטרנט שממנו הורדת אותו)

באפשרותך לשלוח ל-ESET דגימה (קובץ או אתר אינטרנט) לניתוח באמצעות אחת משיטות אלה:

1. השתמש בטופס שליחת הדגימה מתוך המוצר שברשותך. הוא ממוקם בתפריט **כלים** > **כלים נוספים** > **שלח דגימה לניתוח**.

2. לחלופין, תוכל לשלוח את הקובץ בדוא"ל. אם אתה מעדיף את האפשרות הזו, ארוז את הקובץ/הקבצים בחבילת WinRAR/WinZIP, הגן על הארכיון באמצעות הסיסמה "infected" ושלח אותו אל samples@eset.com.

3. כדי לדווח על דואר זבל, הודעות דוא"ל שזוהו כדואר זבל למרות שאינן כאלה או על אתרי אינטרנט שסווגו באופן שגוי באמצעות המודול של בקרת הורים, עיין במאמר במאגר הידע של ESET.

בטופס **בחר דגימה לשליחה ולניתוח**, בחר את התיאור המתאים ביותר למטרת הודעתך מתוך התפריט הנפתח **סיבה לשליחת הדגימה**:

- קובץ חשוד
- אתר חשוד (אתר אינטרנט שנגוע בתוכנה זדונית כלשהי),
- זיהוי חיובי שגוי של קובץ (קובץ שזוהה כנגוע למרות שאינו נגוע),
- אתר תוצאה חיובית מוטעית
- אחר

קובץ/אתר – הנתיב לקובץ או לאתר האינטרנט שבכוונתך להגיש.

דוא"ל ליצירת קשר – דוא"ל זה נשלח אל ESET עם הקבצים החשודים וייתכן שנשתמש בו כדי ליצור עמך קשר במקרה שיידרש מידע נוסף לצורך הניתוח. הזנת כתובת דוא"ל ליצירת קשר אינה הכרחית. סמן את תיבת הסימון **שלח באופן אנונימי** כדי להשאיר שדה זה ריק.

ייתכן שלא תקבל תשובה מ-ESET

לא תקבל תשובה מ-ESET אם לא יהיה צורך במידע נוסף. שרתינו מקבלים מדי יום עשרות אלפי קבצים ואין באפשרותנו להשיב על כל ההגשות.
אם יסתבר שהדגימה היא יישום או אתר אינטרנט זדוניים, זיהויים יתווסף לעדכון הבא של ESET.

בחר דגימה לשליחה ולניתוח - קובץ חשוד

סימנים ותסמינים של הדבקת תוכנה זדונית שנצפו – הזן תיאור של אופן פעולת הקובץ החשוד שנצפה במחשב שלך.

מקור הקובץ (כתובת URL או ספק) – אנא הזן את מקור הקובץ ופרט כיצד נתקלת בקובץ.

הערות ומידע נוסף – כאן תוכל להזין עוד פרטים או תיאורים שיסייעו בעיבוד זיהויו של הקובץ החשוד.

הערה

הפרמטר הראשון – **סימנים ותסמינים של הדבקת תוכנה זדונית שנצפו** – הוא פרמטר חובה, אולם מסירת מידע נוסף תסייע משמעותית למעבדות שלנו בתהליך הזיהוי ובעיבוד של דוגמאות.

בחר דגימה לשליחה ולניתוח - אתר חשוד

אנא בחר אחת מהאפשרויות הבאות מהתפריט הנפתח **מה לא תקין באתר**:

- **נגוע** – אתר אינטרנט המכיל וירוסים או תוכנות זדוניות אחרות אשר מופצים בשיטות שונות.
- **פישינג** – לעתים קרובות משמש לקבלת גישה לנתונים רגישים, כגון מספרים של חשבונות בנק, מספרי PIN, ועוד. קרא עוד על סוג המתקפה הזה במילון.
- **הונאה** – אתר אינטרנט לרמייה או להונאה, במיוחד להפקת רווח מהיר.
- בחר באפשרות **אחר** אם האפשרויות שצוינו לעיל אינן מתייחסות לאתר שאתה עומד לשלוח.

הערות ומידע נוסף – כאן תוכל להזין עוד פרטים או תיאורים שיסייעו בניתוח אתר האינטרנט החשוד.

בחר דגימה לשליחה ולניתוח – זיהוי חיובי שגוי של קובץ

אנו מבקשים שתשלח אלינו קבצים אשר מזוהים כנגועים למרות שאינם נגועים, כדי לשפר את מנגנון ההגנה שלנו מפני וירוסים ותוכנות ריגול ולסייע בהגנה על משתמשים אחרים. מצבי זיהוי חיובי שגוי (FP) עשויים להתרחש כאשר דפוס של קובץ מסוים תואם

לדפוס הכלול במנגנון איתור.

שם יישום וגרסה – שם התוכנית והגרסה שלה (לדוגמה מספר, כינוי או שם קוד).

מקור הקובץ (כתובת URL או ספק) – אנא הזן את מקור הקובץ וציין כיצד נתקלת בקובץ.

מטרת היישום – תיאור כללי של היישום, סוג היישום (למשל דפדפן, נגן מדיה...) והפונקציונליות שלו.

הערות ומידע נוסף – כאן תוכל להוסיף פרטים או תיאורים שיסייעו בעיבוד הקובץ החשוד.

> **הערה**
> הפרמטרים הראשונים נדרשים לזיהוי יישומים לגיטימיים ולהבחנה ביניהם לבין קודים זדוניים. כשאתה מספק מידע נוסף אתה מסייע משמעותית למעבדות שלנו בתהליך הזיהוי ובעיבוד של דוגמאות.

בחר דגימה לשליחה ולניתוח - זיהוי חיובי שגוי של אתר

אנו מבקשים שתשלח פרטי אתרים שזוהו כאתרים נגועים, כאתרי הונאות או כאתרי פישינג, למרות שאינם כאלה. מצבי זיהוי חיובי שגוי (FP) עשויים להתרחש כאשר דפוס של קובץ מסוים תואם לדפוס הכלול במנגנון איתור. אנא ציין את אתר האינטרנט הזה כדי לשפר את מנוע האנטי-וירוס וההגנה מפני אתרי פישינג שלנו ולסייע בהגנה על משתמשים אחרים.

הערות ומידע נוסף – כאן תוכל להוסיף פרטים או תיאורים שיסייעו בעיבוד הקובץ החשוד.

בחר דגימה לשליחה ולניתוח - אחר

השתמש בטופס זה אם לא ניתן לקטלג קובץ כ**קובץ חשוד** או כ**זיהוי חיובי שגוי**.

סיבה להגשת הקובץ – אנא הזן תיאור מפורט ואת הסיבה לשליחת הקובץ.

עדכון Microsoft Windows®

תכונת העדכון של Windows היא רכיב חשוב בהגנה על משתמשים מפני תוכנות זדוניות. מסיבה זו, חיוני להתקין את העדכונים של Microsoft Windows מיד כשהם זמינים. ESET Internet Security מודיע לך על עדכונים חסרים בהתאם לרמה שתציין. הרמות הבאות זמינות:

- **ללא עדכונים** – לא יוצע לך להוריד עדכוני מערכת.
- **עדכונים אופציונליים** – יוצע לך להוריד עדכונים המסומנים כבעלי עדיפות נמוכה ומעלה.
- **עדכונים מומלצים** – יוצע לך להוריד עדכונים המסומנים כנפוצים ומעלה.
- **עדכונים חשובים** – יוצע לך להוריד עדכונים המסומנים כחשובים ומעלה.
- **עדכונים קריטיים** – יוצע לך להוריד רק עדכונים קריטיים.

לחץ על **אישור** לשמירת השינויים. חלון עדכוני המערכת יוצג לאחר אימות הסטטוס מול שרת העדכון. בהתאם לכך, ייתכן שפרטי עדכון המערכת לא יהיו זמינים מיידית לאחר שמירת השינויים.

ממשק משתמש

המקטע **ממשק משתמש** מאפשר לך להגדיר את אופן פעולת ממשק המשתמש הגרפי (GUI) של התוכנית.

באמצעות הכלי גרפיקה באפשרותך לשנות את המראה של התוכנית ואת האפקטים שבהם היא משתמשת.

קביעת התצורה של התראות ותיבות הודעה והתראות מאפשרת לך לשנות את אופן פעולתן של התראות איתור והודעות מערכת. ניתן להתאימן אישית כדי שיענו על צרכיך.

כדי לספק אבטחה מרבית של תוכנת האבטחה שלך, באפשרותך להוסיף סיסמה להגנה על ההגדרות דרך הכלי הגדרות גישה.

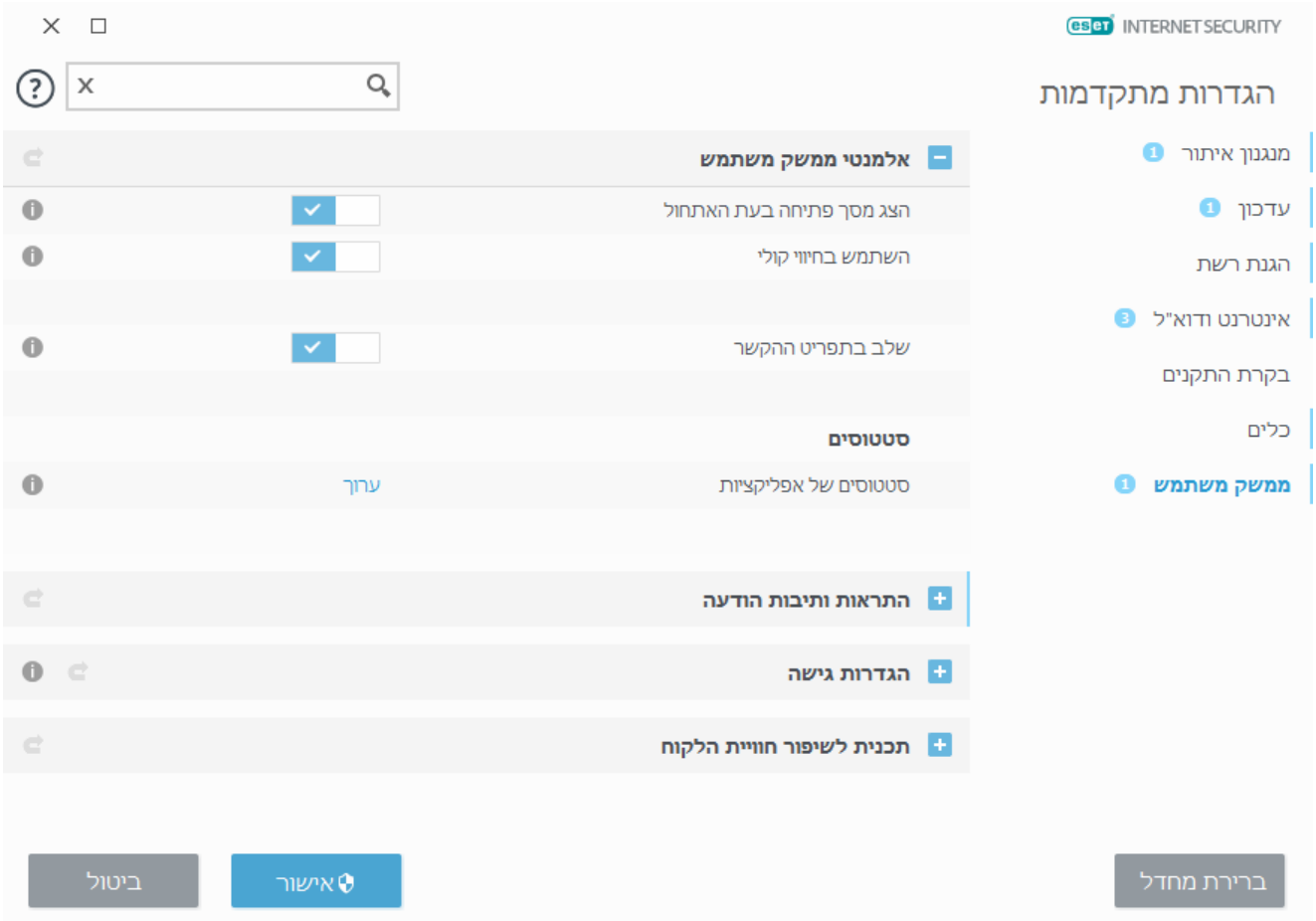
רכיבי ממשק משתמש

אפשרויות התצורה של ממשק המשתמש ב-ESET Internet Security מאפשרות לך להתאים את סביבת העבודה לצרכיך. אפשרויות תצורה אלה נגישות מהתפריט **הגדרות מתקדמות** > **ממשק משתמש** > **רכיבי ממשק משתמש**.

- אם ברצונך לבטל את פעילות מסך הפתיחה של ESET Internet Security, בטל את הבחירה באפשרות **הצג את מסך הפתיחה בעת האתחול**.
- כדי ש-ESET Internet Security ישמיע צליל כשמתרחשים אירועים חשובים במהלך סריקה, לדוגמה כאשר מתגלה איום או כאשר הסריקה מסתיימת, בחר **השתמש באות קול**.
- **שלב בתפריט ההקשר** שלב את רכיבי הבקרה של ESET Internet Security בתפריט ההקשר.
- **סטטוסים של יישומים** לחץ על הלחצן **ערוך** כדי לנהל (להשבית) סטטוסים שמוצגים בחלונית הראשונה בתפריט הראשי.

ראה גם:

- התראות והודעות
- הגדרות גישה
- תכנית לשיפור חוויית הלקוח

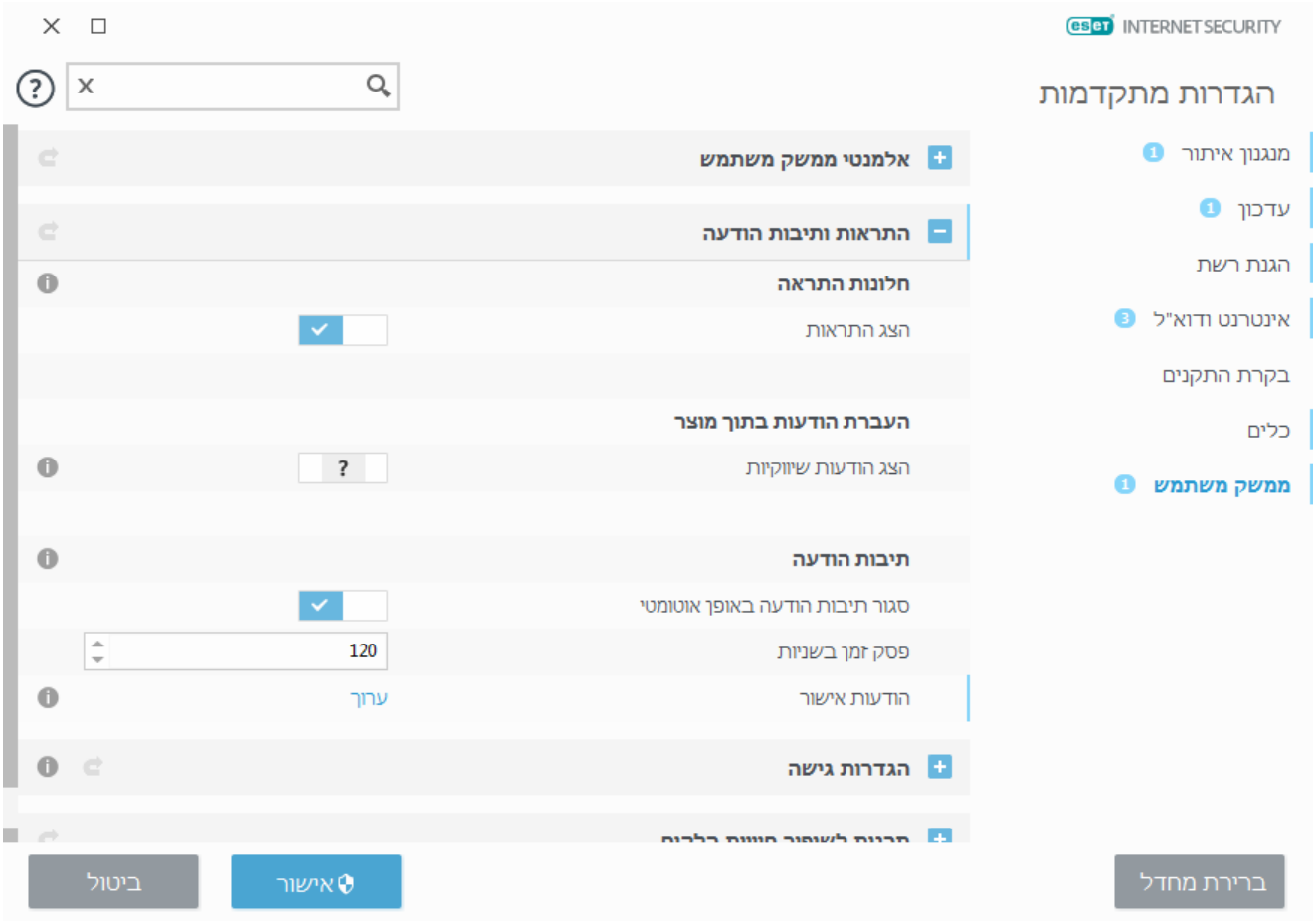


התראות ותיבות הודעה

מחפש מידע אודות התראות והודעות נפוצות?

- נמצא איום
- הכתובת נחסמה
- המוצר אינו מופעל
- קיים עדכון זמין
- פתרון בעיות עבור ההודעה "עדכון המודולים נכשל"
- 'קובץ פגום' או 'שינוי שם הקובץ נכשל'
- האישור של אתר האינטרנט בוטל
- איום רשת נחסם

המקטע **התראות ותיבות הודעה** (לשעבר **התראות והודעות**) תחת **ממשק משתמש** מאפשר לך לקבוע כיצד ESET Internet Security יטפל בהתראות על איומים ובהודעות מערכת (לדוגמה, הודעות על עדכון מוצלח). באפשרותך גם להגדיר את זמן התצוגה ואת השקיפות של הודעות מגש המערכת (חל רק על מערכות שתומכות בהודעות מגש מערכת).



חלונות התראה

השבתה של **התראות תצוגה** תגרום לביטול כל חלונות ההתראה, ומתאימה רק לכמות מוגבלת של מצבים ספציפיים. עבור מרבית המשתמשים מומלץ שאפשרות זו תישאר בהגדרת ברירת המחדל (מופעלת).

הודעות במוצר

הצגת הודעות שיווקיות – הודעות במוצר תוכננו ליידע את המשתמשים על החדשות של ESET ולמסור להם מידע נוסף. שליחת הודעות שיווקיות דורשת את הסכמת המשתמש. לכן, הודעות שיווקיות אינן נשלחות למשתמש כברירת מחדל (מוצגות כסימן שאלה). בעצם הפעלת אפשרות זו, אתה מסכים לקבל הודעות שיווקיות מ-ESET. אם אינך מעוניין בקבלת חומר שיווקי מ-ESET, השבת אפשרות זו.

הודעות שולחן עבודה

התראות בשולחן העבודה ועצות בבלון נפתח מיועדות למסירת מידע בלבד, הן אינן מחייבות אינטראקציה עם המשתמש והועברו תחת **כלים** > **התראות** בהגדרות המתקדמות.

תיבות הודעות
כדי לסגור חלונות קופצים אוטומטית לאחר פרק זמן מסוים, בחר **סגור תיבות הודעות אוטומטית**. אם הם אינם נסגרים ידנית, חלונות התראה נסגרים אוטומטית לאחר שחולף פרק הזמן שצוין.

הודעות אישור ▯ הצגת רשימה של הודעות אישור שבאפשרותך לבחור שיוצגו או שלא יוצגו.

הודעות אישור

חלון דו-שיח זה מציג הודעות מידע שאותן ESET Internet Security יציג לפני ביצוע פעולה מסוימת. סמן את תיבת הסימון שליד כל הודעת אישור, או הסר את הסימון בה, כדי לאפשר או להשבית אותה.

הגדרות גישה

ההגדרות של ESET Internet Security הן חלק מכריע של מדיניות האבטחה שלך. שינויים בלתי מורשים עלולים לסכן את יציבות המערכת שלך וההגנה עליה. כדי להימנע משינויים בלתי מורשים, ניתן להגן על פרמטרי ההגדרות של ESET Internet Security באמצעות סיסמה.

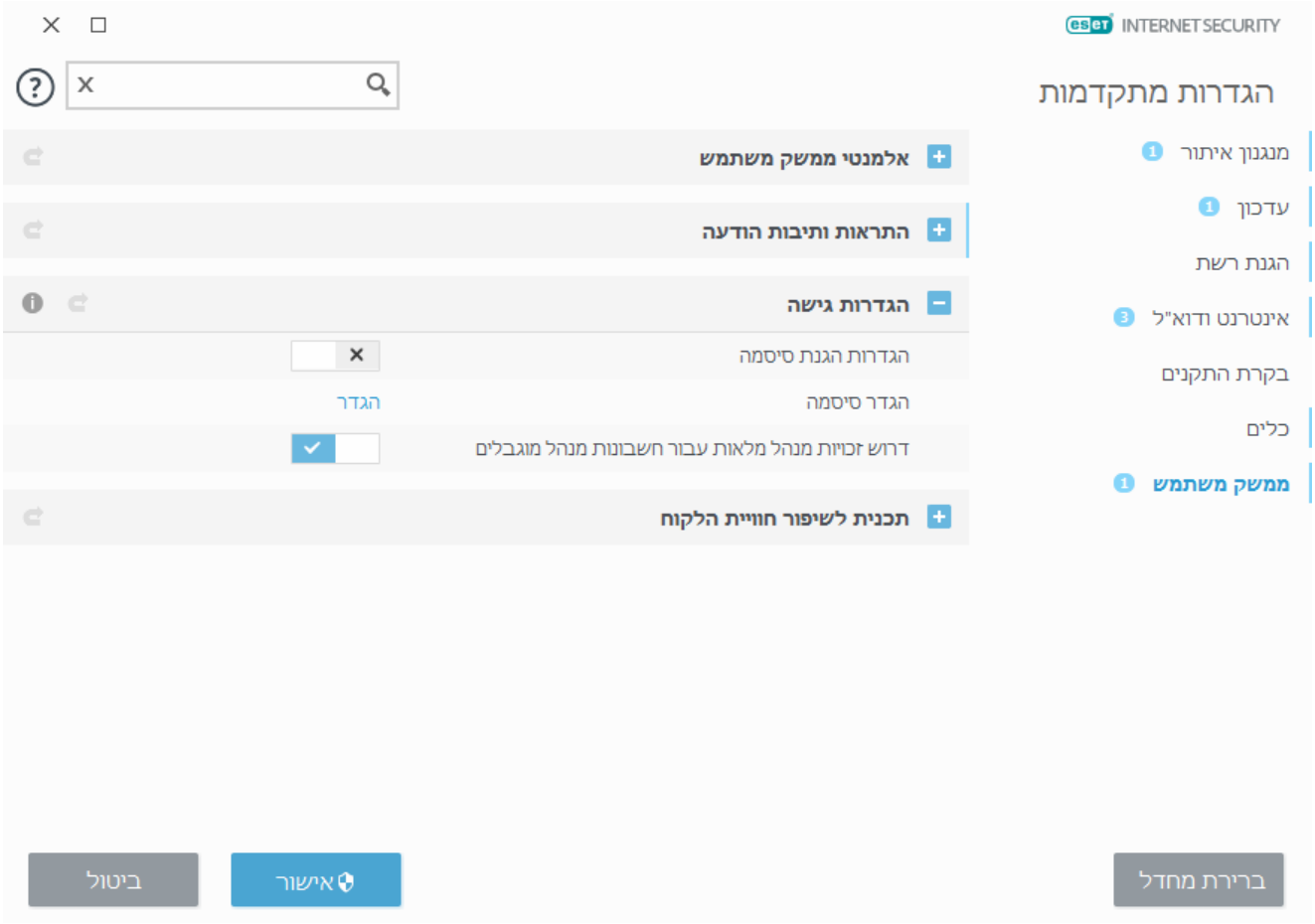
הגדרות הגנה באמצעות סיסמה ▯ מציינות הגדרות של הסיסמה. לחץ כדי לפתוח את חלון הגדרות הסיסמה.

כדי להגדיר או לשנות סיסמה להגנה על פרמטרים של תכנית ההתקנה, לחץ על **הגדר** לצד **הגדר סיסמה**.

> **הערה**
> כאשר תרצה לגשת להגדרות מתקדמות המוגנות באמצעות סיסמה, החלון להזנת הסיסמה יוצג. אם שכחת או איבדת את הסיסמה, לחץ על האפשרות **שחזר סיסמה** להלן והזן את כתובת הדוא"ל שבה השתמשת לרישום הרישיון. ESET תשלח לך דוא"ל עם קוד האימות והוראה לאיפוס הסיסמה.
> • כיצד לבטל את הנעילה של הגדרות מתקדמות

דרוש זכויות מנהל מלאות עבור חשבונות מנהל מוגבלים ▯ בחר באפשרות זו כדי להנחות את המשתמש הנוכחי (אם אין לו הרשאות מנהל מערכת) להזין שם משתמש וסיסמה של מנהל מערכת בעת שינוי פרמטרים מסוימים של המערכת (בדומה לבקרת חשבון משתמש (UAC) ב-WindowsVista וב-Windows 7). שינויים כאלה כוללים השבתה של מודולי הגנה או כיבוי חומת האש.

דרוש זכויות מנהל מערכת (מערכת ללא תמיכת UAC) ▯ במערכות Windows XP שבהן UAC אינה פעילה, האפשרות **דרוש זכויות מנהל מערכת (מערכת ללא תמיכת UAC)** זמינה למשתמשים.



סיסמה להגדרות מתקדמות

כדי להגן על פרמטרי ההגדרות של ESET Internet Security ולהימנע משינוי בלתי מורשה שלהן, יש להגדיר סיסמה חדשה.

כאשר ברצונך לשנות סיסמה קיימת:

1. הקלד את סיסמתך הישנה בשדה **סיסמה ישנה**.
2. הזן את סיסמתך החדשה בשדות **סיסמה חדשה** ו**אשר סיסמה**.
3. לחץ על **אישור**.

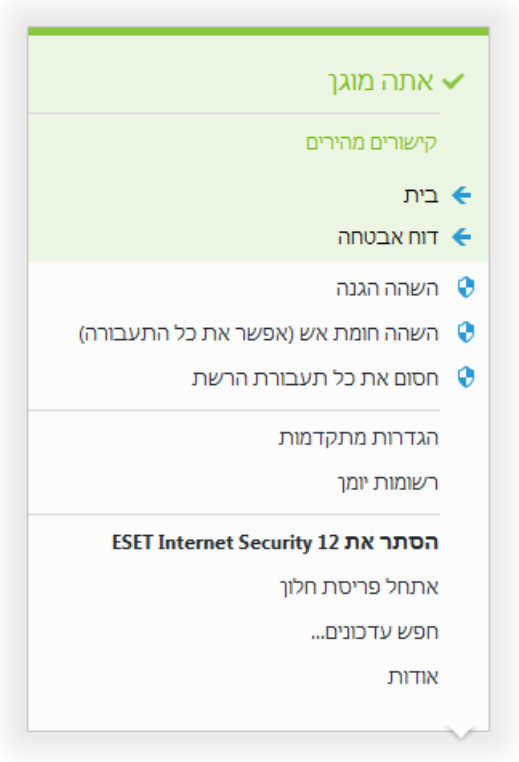
סיסמה זו תידרש לכל שינוי עתידי ב-ESET Internet Security.

אם שכחת את הסיסמה, ניתן לשחזר את הגישה להגדרות המתקדמות באמצעות הכלי של ESET לביטול נעילה.

לחץ כאן אם שכחת את מפתח הרישיון שנופק לך על-ידי ESET, תאריך תפוגה של הרישיון שלך או פרטי רישיון אחרים של ESET Internet Security.

סמל מגש מערכת

כמה מאפשרויות ההגדרה והתכונות החשובות ביותר זמינות בלחיצה ימנית על סמל מגש המערכת.



קישורים מהירים – הצגת החלקים השימושיים ביותר של ESET Internet Security. באפשרותך לגשת אליהם במהירות דרך תפריט התוכנית.

השהה הגנה – הצגת תיבת הדו-שיח של האישור המשביתה את מנגנון האיתור, אשר מגן על המערכת מפני תקיפות של תוכנות זדוניות על-ידי בקרה על הקבצים, האינטרנט ותקשורת הדוא"ל.

התפריט הנפתח **מרווח זמן** מייצג את פרק הזמן שבו ההגנה תושבת.

השהה חומת אש (אפשר את כל התעבורה) – העברת חומת האש למצב לא פעיל. לקבלת מידע נוסף ראה רשת.

חסום את כל תעבורת הרשת – חסימת כל תעבורת הרשת. באפשרותך להתירה מחדש על-ידי לחיצה על **הפסק לחסום את כל תעבורת הרשת**.

הגדרות מתקדמות – בחר באפשרות זו כדי להיכנס לעץ **הגדרות מתקדמות**. ישנן דרכים נוספות לפתיחת ההגדרות המתקדמות, כגון הקשה על המקש F5 או ניווט אל **הגדרות** > **הגדרות מתקדמות**.

רשומות יומן – רשומות יומן מכילות מידע על אירועי תוכנית חשובים שהתרחשו ומספקות סקירה כללית של אובייקטים מזוהים.

פתח את ESET Internet Security – פתיחת חלון התוכנית הראשי של ESET Internet Security מסמל המגש.

אתחל פריסת חלון – איפוס החלון של ESET Internet Security לגודל ולמיקום במסך שנקבעו כברירת מחדל.

בדוק אם קיימים עדכונים – הפעלת עדכון של מנגנון האיתור (לשעבר 'מסד נתונים של חתימות וירוסים') כדי להבטיח את רמת ההגנה שלך מפני קודים זדוניים.

אודות – מסירת מידע על המערכת, פרטים על גרסת ESET Internet Security המותקנת והמודולים המותקנים של התוכנית. כאן

תוכל למצוא גם את תאריך תפוגת הרישיון ומידע על מערכת ההפעלה ועל משאבי המערכת.

עזרה ותמיכה

ESET Internet Security מכיל כלי פתרון בעיות ומידע תומך שיעזרו לך לפתור בעיות שעשויות להופיע.

עזרה

חיפוש במאגר הידע של ESET – מאגר הידע של ESET מכיל תשובות לשאלות הנפוצות ביותר, וכן פתרונות מומלצים לבעיות שונות. מאגר הידע, אשר מעודכן אוטומטית על-ידי המומחים הטכניים של ESET, הוא הכלי החזק ביותר לפתרון בעיות שונות.

פתח עזרה – לחץ על קישור זה להפעלת דפי העזרה של ESET Internet Security.

חפש פתרון מהיר – לחץ על קישור זה כדי לאתר פתרונות לבעיות הנפוצות ביותר שמשתמשים נתקלים בהן. מומלץ שתקרא סעיף זה לפני שתפנה לתמיכה הטכנית.

תמיכה טכנית

שלח בקשת תמיכה – אם לא מצאת תשובה לבעייתך, באפשרותך להשתמש בטופס זה הנמצא באתר האינטרנט של ESET כדי לפנות במהירות אל מחלקת התמיכה הטכנית שלנו.

פרטים עבור תמיכה טכנית – כשתונחה לכך, תוכל להעתיק ולשלוח מידע לתמיכה הטכנית של ESET (למשל שם המוצר, גרסת המוצר, מערכת ההפעלה וסוג המעבד). אפשר **רישום מתקדם ביומן** כדי ליצור קובצי יומן מתקדמים עבור כל התכונות הזמינות על מנת לסייע למפתחים לאבחן ולפתור בעיות. המלל המינימלי לרישום ביומן מוגדר לרמת **אבחון**. הרישום המתקדם ביומן יושבת באופן אוטומטי לאחר שעתיים, אלא אם תעצור אותו מוקדם יותר על-ידי לחיצה על **עצור רישום מתקדם ביומן**. לאחר יצירת כל קובצי היומן, חלון ההתראות יוצג כדי לספק גישה ישירה לתיקייה Diagnostic עם קובצי היומן שנוצרו.

כלי תמיכה

אנציקלופדיית איומים – קישורים לאנציקלופדיית האיומים של ESET, אשר כוללת מידע על הסכנות והתסמינים של סוגי חדירות שונים.

היסטוריית מנגנון איתור – קישורים ל'רדאר הווירוסים של ESET', המכיל מידע על כל גרסה של מנגנון האיתור של ESET (לשעבר 'מסד הנתונים של חתימות הווירוסים').

ESET Log Collector – קישורים למאמר במאגר הידע של ESET, שבו תוכל להוריד את ESET Log Collector – יישום שאוסף אוטומטית מידע ויומנים ממחשב מסוים כדי לסייע לפתור בעיות ביתר מהירות. לקבלת מידע נוסף עיין במדריך המקוון של ESET למשתמש Log Collector.

כלי ניקוי ייעודי של ESET – כלים להסרת הדבקות בתוכנות זדוניות נפוצות. לקבלת מידע נוסף אנא עיין במאמר זה במאגר הידע של ESET.

פרטי מוצר ורישיון

אודות ESET Internet Security – הצגת מידע על העותק של ESET Internet Security שברשותך.

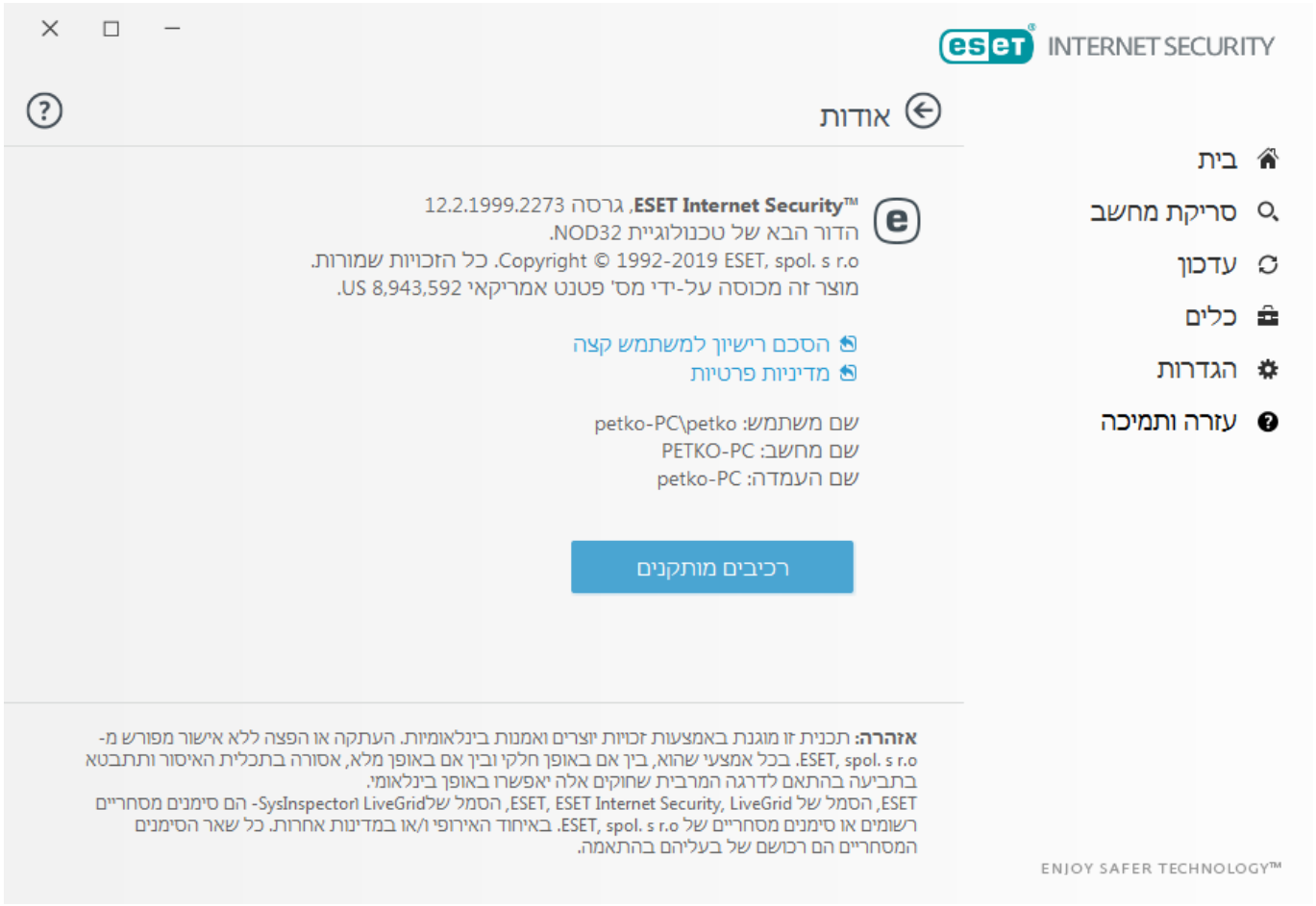
הפעל מוצר/החלף רישיון – לחץ כדי להפעיל את חלון ההפעלה ולהפעיל את המוצר שלך.

שנה מוצר – לחץ כדי לבדוק אם ניתן לשנות את ESET Internet Security לקו מוצרים שונה באמצעות הרישיון הנוכחי.

אודות ESET Internet Security

חלון זה מספק פרטים על גירסת ESET Internet Security שמותקנת, מערכת ההפעלה שלך ומשאבי המערכת.

לחץ על **רכיבים מותקנים** כדי לראות מידע על רשימת המודולים המותקנים של התוכנית. באפשרותך ללחוץ על **העתק** כדי להעתיק את המידע על המודולים ללוח. פעולה זו עשויה להועיל בעת פתרון בעיות או בעת יצירת קשר עם התמיכה הטכנית.



חדשות ESET

בחלון זה ESET Internet Security מיידע אותך על החדשות של ESET.

אם ברצונך לקבל הודעות שיווקיות בחלון קופץ, הפעל את האפשרות **הצגת הודעות שיווקיות** תחת הגדרות מתקדמות (**F5**) > **ממשק משתמש** > **התראות והודעות**.

שלח נתוני תצורת מערכת

כדי לספק את הסיוע המהיר והמדויק ביותר שניתן, ESET צריכה מידע על התצורה של ESET Internet Security, מידע מפורט על המערכת ועל התהליכים הפעילים (קובץ יומן של ESET SysInspector), ואת נתוני הרישום. ESET תשתמש בנתונים אלה אך ורק למטרת אספקת סיוע טכני ללקוח.

בעת שליחת הטופס המקוון, נתוני תצורת המערכת שלך יישלחו אל ESET. בחר באפשרות **שלח תמיד מידע זה** אם ברצונך לזכור את הפעולה עבור תהליך זה. כדי לשלוח את הטופס מבלי לשלוח נתונים כלשהם, לחץ על **אל תשלח מידע** ותוכל ליצור קשר עם התמיכה הטכנית של ESET באמצעות טופס התמיכה המקוון.

את ההגדרה הזו ניתן לקבוע גם תחת **הגדרות מתקדמות** > **כלים** > **אבחון** > **תמיכה טכנית**.

הערה
אם החלטת לשלוח את נתוני המערכת, יש למלא ולשלוח את הטופס המקוון, ולא קריאתך לא תיפתח ונתוני המערכת שלך יאבדו.

פרופילים

מנהל הפרופילים נמצא בשימוש בשני מקומות ב-ESET Internet Security – במקטע **סריקת מחשב לפי דרישה** ובמקטע **עדכון**.

סריקת מחשב

תוכל לשמור את פרמטרי הסריקה המועדפים עליך לסריקה עתידית. מומלץ שתיצור פרופיל שונה (עם מגוון יעדי סריקה, שיטות סריקה ופרמטרים אחרים) עבור כל סריקה שנמצאת בשימוש קבוע.

כדי ליצור פרופיל חדש, פתח את חלון ההגדרות המתקדמות (F5) ולחץ על **מנגנון איתור** > **סריקות לאיתור נוזקות** > **סריקה לפי דרישה** > **רשימת פרופילים**. החלון **מנהל הפרופילים** כולל את התפריט **פרופיל נבחר**, בו מפורטים פרופילי הסריקה הקיימים והאפשרות ליצור פרופיל חדש. כדי לסייע לך ליצור פרופיל חדש שיענה על דרישותיך, עיין במקטע הגדרות פרמטרי המנוע של ThreatSense לקבלת תיאור של כל אחד מהפרמטרים של הגדרות הסריקה.

הערה

נניח שברצונך ליצור פרופיל סריקה משלך והתצורה **סרוק את המחשב שלך** מתאימה באופן חלקי, אך אינך מעוניין לסרוק אורזים של זמן ריצה או אפליקציות העלולות להיות לא בטוחות, ובנוסף ברצונך להחיל **ניקוי מחמיר**. הזן את שם הפרופיל החדש שלך בחלון **מנהל הפרופילים** ולחץ על **הוסף**. בחר את הפרופיל החדש בתפריט הנפתח **פרופיל נבחר** והתאם את הפרמטרים שנותרו כך שיענו על דרישותיך. לאחר מכן לחץ על **אישור** כדי לשמור את הפרופיל החדש.

עדכון

עורך הפרופילים במקטע ההגדרות 'עדכון' מאפשר למשתמשים ליצור פרופילי עדכון חדשים. צור פרופילים מותאמים אישית משלך (שונים מ**הפרופיל שלי**, שנקבע כברירת מחדל) והשתמש בהם רק אם המחשב שלך משתמש במספר אמצעים להתחברות לשרתי העדכון.

לדוגמה, מחשב נייד שבדרך-כלל מתחבר לשרת מקומי (שיקוף) ברשת המקומית, אך מוריד עדכונים ישירות משירותי העדכון של ESET כשהוא מנותק מהרשת המקומית (נסיעה עסקית) עשוי להשתמש בשני פרופילים: הראשון להתחברות לשרת המקומי; השני להתחברות לשרתי ESET. אחרי שהפרופילים הללו הוגדרו, נווט אל **כלים** > **מתזמן** וערוך את הפרמטרים של משימת העדכון. יעד פרופיל אחד להיות הראשי ואת האחר להיות המשני.

פרופיל עדכון – פרופיל העדכון שנמצא בשימוש כעת. כדי להחליפו בחר פרופיל בתפריט הנפתח.

רשימת פרופילים – צור פרופילי עדכון חדשים או הסר פרופילי עדכון קיימים.

מקשי קיצור במקלדת

לניווט משופר ב-ESET Internet Security, ניתן להשתמש במקשי הקיצור הבאים במקלדת:

הפעולה בוצעה	מקשי קיצור במקלדת
פתיחת דפי העזרה	F1
פתיחת הגדרות מתקדמות	F5
ניווט בין פריטים במוצר	Up/Down
הזזת הסמן בחלון	TAB
סגירת חלון הדו-שיח הפעיל	Esc
הצגת פרטים על רישיון ESET ועל המחשב שלך (פרטים עבור תמיכה טכנית)	Ctrl+U
איפוס חלון המוצר לגודלו ולמיקומו במסך שנקבעו כברירת מחדל	Ctrl+R

אבחון

האבחון מספק קובצי Dump של קריסת אפליקציות של תהליכי ESET (לדוגמה, ekrn). אם אפליקציה קורסת, ייווצר קובץ Dump. דבר זה יכול לסייע למפתחים לאתר באגים ולתקן בעיות שונות ב-ESET Internet Security.

לחץ על התפריט הנפתח שליד **סוג מצבור** ובחר אחת משלוש האפשרויות הזמינות:

- בחר **השבת** כדי להשבית תכונה זו.
- **מיני** (ברירת מחדל) – רישום ערכת המידע השימושי הקטנה ביותר שמסוגלת לעזור בזיהוי הסיבה לקריסתה הבלתי צפויה

של האפליקציה. סוג זה של קובץ מצבור יכול להיות שימושי כאשר השטח מוגבל, אולם מאחר שהמידע המוגבל כלול, ייתכן ששגיאות שלא נגרמו ישירות על-ידי האיום שפעל כשקרתה הבעיה לא יזוהו בניתוח של קובץ זה.

- **מלא** – רישום כל תכני זיכרון המערכת מהרגע שבו היישום נעצר באופן בלתי צפוי. מצבור זיכרון שלם עשוי להכיל נתונים מתהליכים שפעלו כאשר מצבור הזיכרון נאסף.

ספריית יעד – הספרייה שבה ייווצר המצבור בעת הקריסה.

פתיחת תיקיית אבחון – לחץ על **פתח** כדי לפתוח ספרייה זו בחלון חדש של *סייר Windows*.

צור מצבור אבחוני – לחץ על **צור** כדי ליצור קבצי מצבור אבחוני ב**ספריית היעד**.

רישום מתקדם ביומן

אפשר רישום מתקדם של מנגנון אנטי-ספאם – תעד את כל האירועים שמתרחשים במהלך סריקת אנטי-ספאם. פעולה זו תוכל לסייע למפתחים לאבחן ולתקן בעיות הקשורות למנגנון האנטי-ספאם של ESET.

אפשר רישום מתקדם של מנגנון מערכת נגד גניבה – תעד את כל האירועים שמתרחשים במערכת נגד גניבה כדי לאפשר אבחון ופתרון בעיות.

אפשר רישום מתקדם של מערכת בקרת התקנים – תיעוד כל האירועים שמתרחשים במערכת בקרת ההתקנים. פעולה זו תוכל לסייע למפתחים לאבחן ולתקן בעיות הקשורות למערכת בקרת ההתקנים.

אפשר רישום מתקדם ביומן של רכיב ליבה – תעד את כל האירועים המתרחשים ברכיב ליבה של ESET (ekrn) (זמין בגרסה 12.2 ואילך).

אפשר רישום מתקדם של רישוי – תעד את התקשורת של המוצר עם שרתי ההפעלה או ESET License Manager של ESET.

אפשר רישום מתקדם של הגנת רשת – תעד את כל נתוני הרשת העוברים דרך חומת האש בתבנית PCAP כדי לסייע למפתחים לאבחן ולתקן בעיות הקשורות לחומת האש.

אפשר רישום מתקדם של מערכת ההפעלה – ייאסף מידע נוסף אודות מערכת ההפעלה, כגון תהליכים פעילים, פעילות ה-CPU ופעולות הדיסק. פעולה זו עשויה לסייע למפתחים לאבחן ולתקן בעיות הקשורות למוצר של ESET הפועל במערכת ההפעלה שלך (זמין עבור Windows 10).

אפשר רישום מתקדם של מערכת בקרת ההורים – תיעוד כל האירועים שמתרחשים במערכת בקרת ההורים. פעולה זו תוכל לסייע למפתחים לאבחן ולתקן בעיות הקשורות למערכת בקרת ההורים.

אפשר רישום מתקדם של סינון פרוטוקולים – תיעוד כל הנתונים העוברים דרך מנוע סינון פרוטוקולים בתבנית PCAP כדי לסייע למפתחים לאבחן ולתקן בעיות הקשורות לסינון הפרוטוקולים.

אפשר רישום מתקדם ביומן עבור הסורק – תעד בעיות המתרחשות בעת סריקת קבצים ותיקיות על-ידי סריקת מחשב או הגנה בזמן אמת על מערכת קבצים (זמין בגירסה 12.2 ואילך).

אפשר רישום מתקדם של מנגנון העדכון – תעד את כל האירועים שמתרחשים בתהליך העדכון. כך יוכלו המפתחים לאבחן ולתקן בעיות הקשורות למנגנון העדכון.

מיקום רשומות היומן

ספריית רשומות היומן	מערכת הפעלה
C:\ProgramData\ESET\ESET Security\Diagnostics\	Windows Vista ואילך
C:\Documents and Settings\All Users\...	גרסאות קודמות של Windows

ייבוא וייצוא הגדרות

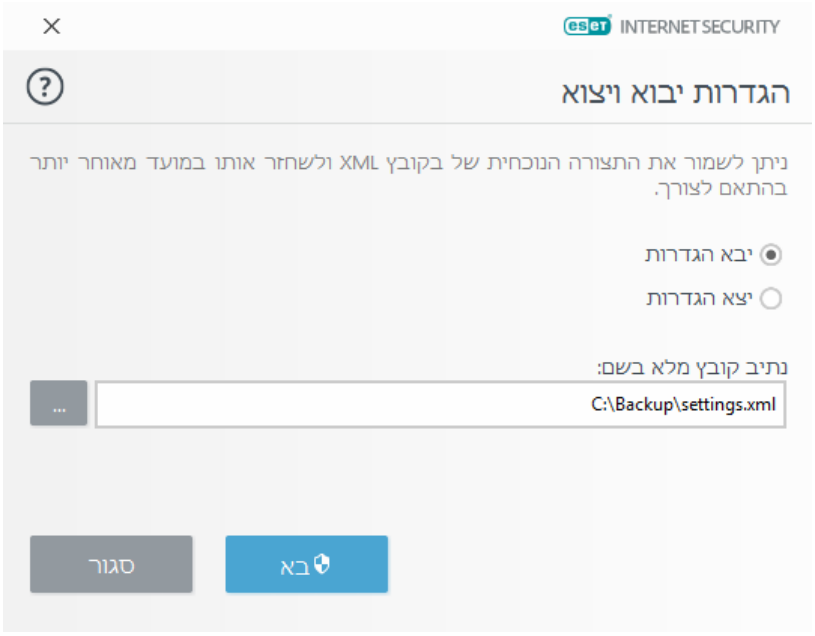
באפשרותך לייבא או לייצא את קובץ התצורה מסוג .xml של ESET Internet Security מתוך התפריט **הגדרות**.

ייבוא או ייצוא של קובצי תצורה שימושיים כשעליך לגבות את התצורה הנוכחית של ESET Internet Security לשימוש במועד מאוחר יותר. אפשרות הגדרות הייצוא נוחה גם למשתמשים המעוניים להשתמש בתצורה המועדפת עליהם במערכות שונות; באפשרותם לייבא

קובץ .xml בקלות כדי להעביר את ההגדרות הללו.

קל מאוד לייבא תצורה. בחלון התוכנית הראשי לחץ על **הגדרות** > **ייבוא וייצוא הגדרות**, ולאחר מכן בחר **יבא הגדרות**. הזן את שם קובץ התצורה או לחץ על הלחצן **...** כדי לעיין לאיתור קובץ התצורה שברצונך לייבא.

השלבים לייצוא תצורה דומים מאוד. בחלון התוכנית הראשי, לחץ על **הגדרות** > **ייבוא וייצוא הגדרות**. בחר **ייצוא הגדרות** והזן את שם קובץ התצורה (למשל *export.xml*). השתמש בדפדפן כדי לבחור מיקום במחשב לשמירת קובץ התצורה.



הערה
אם אין לך את ההרשאות מספיקות לכתיבה של הקובץ שיוצא בספרייה שצוינה, ייתכן שתיתקל בשגיאה בעת ייצוא ההגדרות.

סורק של שורת הפקודה

ESET Internet Security ניתן להפעיל את מודול האנטי-וירוס של המוצר דרך שורת הפקודה – ידנית (עם הפקודה ecls) או באמצעות קובץ אצווה (bat). שימוש בסורק שורת הפקודה של ESET:

```
..ecls [OPTIONS..] FILES
```

בפרמטרים ובמתגים הבאים ניתן להשתמש בעת הפעלת הסורק לפי דרישה דרך שורת הפקודה:

אפשרויות

טען מודולים מתיקיה	base-dir=FOLDER/
העבר תיקיה להסגר	quar-dir=FOLDER/
אל תכלול בסריקה קבצים התואמים למסיכה	exclude=MASK/
סרוק תיקיות משנה (ברירת מחדל)	subdir/
אל תסרוק תיקיות משנה	no-subdir/
מספר מקסימלי של רמות משנה של תיקיות בתיקיות לסריקה	max-subdir-level=LEVEL/
עקוב אחר קישורים סמליים (ברירת מחדל)	symlink/
דלג על קישורים סמליים	no-symlink/
סרוק זרמי נתונים חלופיים (ADS) (ברירת מחדל)	ads/
אל תסרוק זרמי נתונים חלופיים (ADS) (ברירת מחדל)	no-ads/
תעד פלט בקובץ	log-file=FILE/
החלף קובץ פלט (ברירת מחדל – הוסף)	log-rewrite/
תעד פלט במסוף (ברירת מחדל)	log-console/
אל תתעד פלט במסוף	no-log-console/
תעד גם קבצים נקיים	log-all/
אל תתעד קבצים נקיים (ברירת מחדל)	no-log-all/
הצג מחוון פעילות	aind/
סרוק ונקה באופן אוטומטי את כל הדיסקים המקומיים	auto/

אפשרויות סריקה

סרוק קבצים (ברירת מחדל)	/files
אל תסרוק קבצים	/no-files
סרוק זיכרון	/memory
סרוק סקטורי אתחול	/boots
אל תסרוק סקטורי אתחול (ברירת מחדל)	/no-boots
סרוק קובצי ארכיון (ברירת מחדל)	/arch
אל תסרוק קובצי ארכיון	/no-arch
סרוק רק קבצים הקטנים מגודל במגה-בתים (ברירת מחדל 0 = בלתי מוגבל)	/max-obj-size=SIZE
מספר מקסימלי של רמות משנה של קובצי ארכיון בתוך קובצי ארכיון (קובצי ארכיון מקוננים) לסריקה	/max-arch-level=LEVEL
סרוק קובצי ארכיון במשך גבול שניות מקסימלי	/scan-timeout=LIMIT
סרוק קבצים בארכיון רק אם הם קטנים מגודל (ברירת מחדל 0 = בלתי מוגבל)	/max-arch-size=SIZE
סרוק את הקבצים בארכיון חילוץ עצמי רק אם הם קטנים מגודל במגה-בתים (ברירת מחדל 0 = בלתי מוגבל)	/max-sfx-size=SIZE
סרוק קובצי דואר אלקטרוני (ברירת מחדל)	/mail
אל תסרוק קובצי דואר אלקטרוני	/no-mail
סרוק תיבות דואר (ברירת מחדל)	/mailbox
אל תסרוק תיבות דואר	/no-mailbox
סרוק קובצי ארכיון בחילוץ עצמי (ברירת מחדל)	/sfx
אל תסרוק קובצי ארכיון בחילוץ עצמי	/no-sfx
סרוק אורזים של זמן ריצה (ברירת מחדל)	/rtp
אל תסרוק אורזים של זמן ריצה	/no-rtp
סרוק אחר יישומים לא בטוחים פוטנציאליים	/unsafe
אל תסרוק אחר יישומים לא בטוחים פוטנציאליים (ברירת מחדל)	/no-unsafe
סרוק אחר יישומים לא רצויים פוטנציאליים	/unwanted
אל תסרוק אחר יישומים לא רצויים פוטנציאליים (ברירת מחדל)	/no-unwanted
סרוק אחר יישומים חשודים (ברירת מחדל)	/suspicious
אל תסרוק אחר יישומים חשודים	/no-suspicious
השתמש בחתימות (ברירת מחדל)	/pattern
אל תשתמש בחתימות	/no-pattern
הפעל היוריסטיקה (ברירת מחדל)	/heur
השבת היוריסטיקה	/no-heur
הפעל היוריסטיקה מתקדמת (ברירת מחדל)	/adv-heur
השבת היוריסטיקה מתקדמת	/no-adv-heur
אל תכלול בסריקה סיומות קבצים המופרדות בנקודתיים	/ext-exclude=EXTENSIONS
השתמש במצב ניקוי עבור אובייקטים נגועים האפשרויות הבאות זמינות: • ללא – לא יתבצע ניקוי אוטומטי. • רגיל(ברירת מחדל) – ecls.exe ינסה לנקות או למחוק אוטומטית את הקבצים הנגועים. • מחמיר – ecls.exe ינסה לנקות או למחוק אוטומטית את הקבצים הנגועים, ללא התערבות של המשתמש (לא תונחה לבצע פעולה כלשהי לפני שהקבצים יימחקו). • קפדני – ecls.exe ימחק את הקבצים מבלי לנסות למחוק, ללא קשר לקובץ. • מחק – ecls.exe ימחק את הקבצים מבלי לנסות למחוק, אך יימנע ממחיקת קבצים רגישים, כגון קובצי מערכת של Windows.	/clean-mode=MODE
העתק קבצים נגועים (אם נוקו) להסגר (משלים את הפעולה שבוצעה במהלך הניקוי)	/quarantine
אל תעתיק קבצים נגועים להסגר	/no-quarantine

אפשרויות כלליות

הצג עזרה וצא	/help
הצג פרטי גרסה וצא	/version
שמור חותמת זמן של הגישה האחרונה	/preserve-time

קודי יציאה

לא נמצא איום	0
איום נמצא ונוקה	1
חלק מהקבצים לא נסרקו (ייתכנו איומים)	10
נמצא איום	50
שגיאה	100

הערה

קודי יציאה גדולים מ-100 פירושם שהקובץ לא נסרק ולכן עשוי להיות נגוע.

ESET CMD

זוהי תכונה שמאפשרת פקודות ecmd מתקדמות. היא מאפשרת לייצא ולייבא הגדרות באמצעות שורת הפקודה (ecmd.exe). עד עכשיו, היה ניתן רק לייצא הגדרות רק באמצעות ממשק המשתמש הגרפי (GUI). ESET Internet Security ניתן לייצא את התצורה לקובץ *xml*.xml..

לאחר שתאפשר את ESET CMD, שתי שיטות הרשאה יהיו זמינות:

- **ללא** – ללא הרשאה. לא מומלץ להשתמש בשיטה זו מאחר שהיא מאפשרת ייבוא של תצורות לא חתומות המהוות סיכון אפשרי.

• **סיסמה להגדרות מתקדמות** – נדרשת סיסמה לייבוא תצורה מקובץ *xml*.xml. על קובץ זה להיות חתום (ראה חתימה על קובץ תצורה *xml* בהמשך). חובה לספק את הסיסמה שצוינה בהגדרות גישה לפני שניתן לייבא תצורה חדשה. אם הגדרות הגישה אינן מאופשרות, הסיסמה אינה תואמת או שקובץ התצורה *xml* אינו חתום, התצורה לא תיובא.

לאחר ש-ESET CMD מאופשר, ניתן להשתמש בשורת הפקודה כדי לייבא או לייצא תצורות של ESET Internet Security. באפשרותך לבצע זאת באופן ידני או ליצור קובץ Script למטרות אוטומציה.

חשוב

כדי להשתמש בפקודות ecmd מתקדמות, עליך להפעיל אותן באמצעות הרשאות של מנהל מערכת, או לפתוח את שורת הפקודה של Windows (cmd) על-ידי בחירה באפשרות **הפעל כמנהל**. אחרת, ההודעה **Error executing command.** תוצג. כמו כן, בעת ייצוא תצורה, על תיקיית היעד להיות קיימת. פקודת הייצוא עדיין תפעל כאשר ההגדרה ESET CMD אינה פעילה.

דוגמה

פקודת ייצוא הגדרות:

```
ecmd /getcfg c:\config\settings.xml
```

פקודת ייבוא הגדרות:

```
ecmd /setcfg c:\config\settings.xml
```

הערה

ניתן להפעיל פקודות ecmd מתקדמות באופן מקומי בלבד.

חתימה על קובץ תצורה *xml*:

1. הורד את קובץ ההפעלה XmlSignTool.

2. פתח את שורת הפקודה של Windows (cmd) על-ידי בחירה באפשרות **הפעל כמנהל**.

3. נווט אל מיקום השמירה של `xmlsigntool.exe`

4. בצע פקודה לחתימה על קובץ תצורה *xml*, שימוש: `xmlsigntool /version 1|2 <xml_file_path>`

חשוב

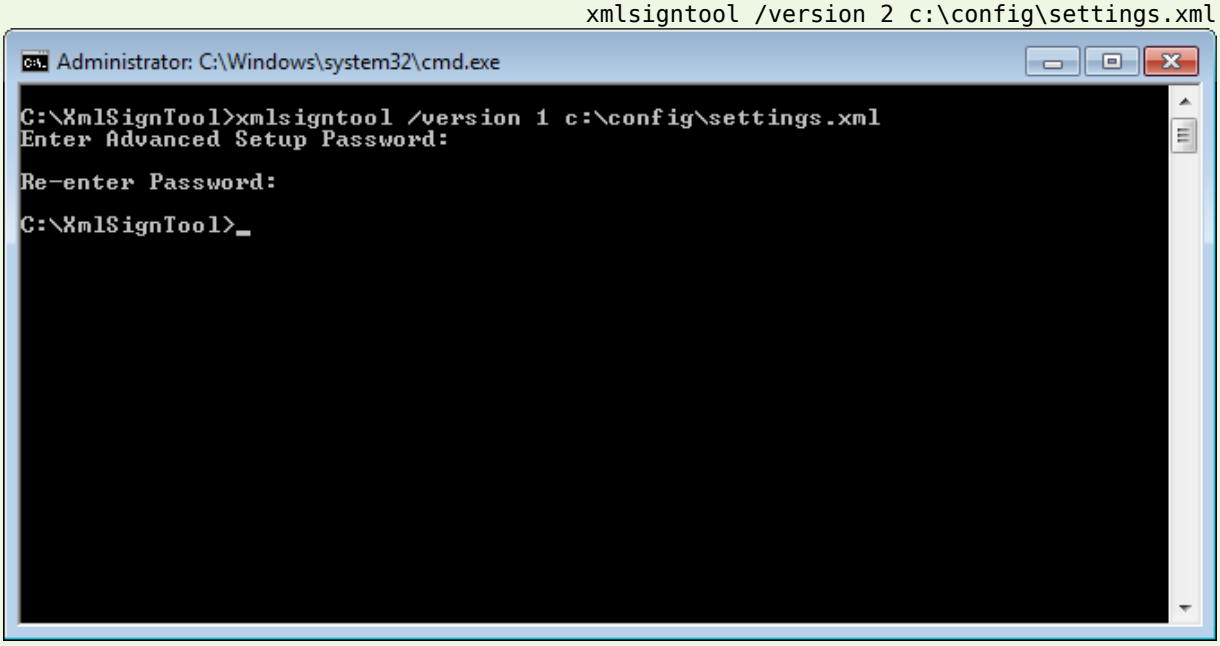
הערך של הפרמטר `/version` תלוי בגרסה של ESET Internet Security שברשותך. השתמש ב-`/version 1` עבור גרסאות של ESET Internet Security שקודמות לגרסה 11.1. השתמש ב-`/version 2` עבור הגרסה הנוכחית של ESET Internet Security.

5. הזן את הסיסמה להגדרות מתקדמות והזן אותה שנית לאישור כאשר תוצג לך הנחיה לכך בכלי XmlSignTool. קובץ התצורה *xml* יהיה חתום כעת וניתן יהיה להשתמש בו לביצוע ייבוא במופע אחר של ESET Internet Security באמצעות ESET CMD ושיטת ההרשאה באמצעות סיסמה.

דוגמה

פקודה לחתימה על קובץ תצורה מיוצא:

```
xmlsigntool /version 2 c:\config\settings.xml
```



הערה

אם הסיסמה להגדרות גישה השתנתה וברצונך לייבא תצורה שנחתמה קודם לכן באמצעות סיסמה ישנה, עליך לחתום שוב על קובץ התצורה *xml*. באמצעות הסיסמה הנוכחית. פעולה זו מאפשרת לך להשתמש בקובץ תצורה ישן יותר מבלי לייצא אותו למחשב אחר שבו פועל ESET Internet Security לפני ביצוע הייבוא.

אזהרה

לא מומלץ לאפשר ESET CMD ללא הרשאה מאחר שהדבר יאפשר ייבוא של תצורות שאינן חתומות. הגדר את הסיסמה ב**הגדרות מתקדמות** > **ממשק משתמש** > **הגדרות גישה** כדי למנוע מהמשתמשים מלבצע שינויים בלתי מורשים.

רשימת פקודות ECMD

סקור את רשימת הפקודות עבור כל תכונת אבטחה להלן:

פקודת 'הפוך לזמין'	פקודת 'השהה זמנית'	תכונת אבטחה
ecmd /setfeature onaccess enable	ecmd /setfeature onaccess pause	הגנה בזמן אמת על מערכת קבצים
ecmd /setfeature document enable	ecmd /setfeature document pause	הגנה על מסמכים
ecmd /setfeature devcontrol enable	ecmd /setfeature devcontrol pause	בקרת התקנים
ecmd /setfeature gamer enable	ecmd /setfeature gamer pause	מצב משחק
ecmd /setfeature antistealth enable	ecmd /setfeature antistealth pause	טכנולוגיה נגד התגנבות
ecmd /setfeature firewall enable	ecmd /setfeature firewall pause	חומת אש אישית
ecmd /setfeature ids enable	ecmd /setfeature ids pause	הגנה מפני מתקפות רשת (IDS)
ecmd /setfeature botnet enable	ecmd /setfeature botnet pause	הגנה מפני 'מחשב זומבי' (Botnet)
ecmd /setfeature webcontrol enable	ecmd /setfeature webcontrol pause	בקרת גישה לאינטרנט
ecmd /setfeature webaccess enable	ecmd /setfeature webaccess pause	הגנה על גישה לאינטרנט
ecmd /setfeature email enable	ecmd /setfeature email pause	הגנת לקוח דוא"ל
ecmd /setfeature antispam enable	ecmd /setfeature antispam pause	הגנת מסנן דואר זבל
ecmd /setfeature antiphishing enable	ecmd /setfeature antiphishing pause	הגנת אנטי-פישינג

איתור במצב לא פעיל

ניתן לקבוע את תצורת ההגדרות של איתור במצב לא פעיל ב**הגדרות מתקדמות** תחת **מנגנון איתור** > **סריקת תוכנות זדוניות** >

סריקה במצב לא פעיל > **איתור במצב לא פעיל**. הגדרות אלה מציינות גורם מפעיל עבור סריקה במצב לא פעיל, כאשר:

- שומר המסך פועל,
- המחשב נעול,
- משתמש מתנתק.

השתמש במתגים עבור כל מצב מתאים כדי להפעיל או להשבית את הגורמים המפעילים השונים לאיתור במצב לא פעיל.

שאלות נפוצות

פרק זה כולל כמה מהשאלות והבעיות הנפוצות שמופיעות. לחץ על כותרת הנושא כדי לגלות כיצד לפתור את הבעיה שלך:

- כיצד לעדכן את ESET Internet Security
- כיצד להסיר וירוס מהמחשב
- כיצד לאפשר תקשורת עבור יישום מסוים
- כיצד להפעיל בקרת הורים בחשבון
- כיצד ליצור משימה חדשה במתזמן
- כיצד לתזמן משימת סריקה (בכל 24 שעות)
- כיצד לפתור את השגיאה "לא הייתה אפשרות לנתב את ההגנה על שירותים בנקאיים ותשלומים מקוונים לדף האינטרנט המבוקש"
- כיצד לבטל את הנעילה של הגדרות מתקדמות

אם בעייתך אינה מופיעה ברשימת דפי העזרה שלעיל, נסה לחפש בדפי העזרה של ESET Internet Security.

אם אינך מוצר את הפתרון לבעיה/שאלה שלך בדפי העזרה, תוכל לבקר במאגר הידע של ESET, המתעדכן באופן קבוע. להלן קישורים למאמרי מאגר הידע הפופולריים ביותר שלנו, כדי לסייע לך לפתור בעיות נפוצות:

- קיבלתי שגיאת הפעלה בעת התקנת מוצר ESET שברשותי. מה פירוש הדבר?
- הפעלת המוצר הביתי של ESET שברשותי עבור Windows באמצעות שם המשתמש, הסיסמה או מפתח הרישיון שלי
- הסרת ההתקנה או התקנה מחדש של המוצר הביתי של ESET שברשותי
- קיבלתי הודעה שההתקנה של ESET הסתיימה מוקדם מדי
- מה עליי לעשות לאחר חידוש הרישיון שלי? (משתמשים ביתיים)
- מה יקרה אם אחליף את כתובת הדואר האלקטרוני שלי?
- כיצד להפעיל את Windows במצב בטוח או במצב בטוח עם עבודה ברשת

במידת הצורך תוכל להפנות את השאלות או הבעיות שלך לתמיכה הטכנית שלנו.

כיצד לעדכן את ESET Internet Security

עדכון ESET Internet Security יכול להתבצע בצורה ידנית או אוטומטית. כדי להפעיל את העדכון, לחץ על **עדכן** בחלון התוכנית הראשי ולאחר מכן לחץ על **חפש עדכונים**.

הגדרות ההתקנה שנקבעו כברירת מחדל יוצרות משימת עדכון אוטומטית, אשר מבוצעת על-בסיס שעתי. אם עליך לשנות את מרווח הזמן, נווט אל **כלים** > **מתזמן** (לקבלת מידע נוסף על המתזמן לחץ כאן).

כיצד להסיר וירוס מהמחשב

אם במחשב שלך מופיעים תסמינים של הדבקה בתוכנה זדונית, למשל האטה בפעילות, או חוסר תגובה לעתים קרובות, מומלץ לבצע את הפעולות הבאות:

1. בחלון התוכנית הראשי, לחץ על **סריקת מחשב**.
2. לחץ על **סרוק את המחשב שלך** כדי להתחיל בסריקת המערכת.

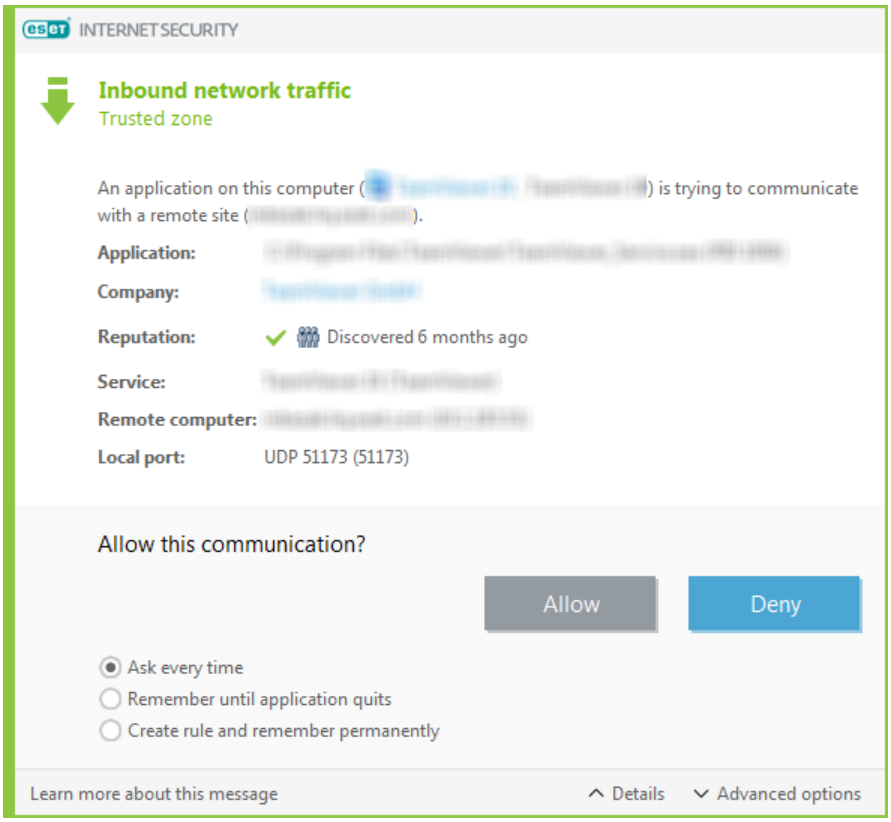
3. בסיום הסריקה, סקור את היומן הכולל את מספר הקבצים שנסרקו, שנפגעו ושנוקו.

4. אם ברצונך לסרוק רק חלק מסוים מהדיסק, לחץ על **סריקה מותאמת אישית** ובחר יעדים שייסרקו לאיתור וירוסים.

לקבלת מידע נוסף אנא עיין במאמר מאגר הידע של ESET, המתעדכן באופן קבוע.

כיצד לאפשר תקשורת עבור יישום מסוים

אם מזוהה חיבור חדש במצב אינטראקטיבי, ואם אין כלל תואם, תונחה לאשר או למנוע את החיבור. אם תרצה שהמוצר ESET Internet Security יבצע את אותה פעולה בכל פעם שהיישום מנסה ליצור חיבור, סמן את תיבת הסימון **זכור את הפעולה (יצירת כלל)**.



באפשרותך ליצור כללי חומת אש חדשים ליישומים, עוד לפני שיזוהו על-ידי ESET Internet Security, בחלון הגדרת חומת האש , הממוקם תחת **רשת** > **חומת אש** > **כללים ואזורים** > **הגדרות**. כדי שהכרטיסייה **כללים** תהיה זמינה תחת **הגדרות אזור וכלל**, מצב סינון חומת האש חייב להיות מוגדר כאינטראקטיבי.

בכרטיסייה **כללי** הזן את השם, הכיוון ופרוטוקול התקשורת של הכלל. חלון זה מאפשר לך להגדיר את הפעולה שתתבצע כאשר הכלל מוחל.

הזן את הנתיב אל קובץ ההפעלה של היישום ואת יציאת התקשורת המקומית בכרטיסייה **מקומי**. לחץ על הכרטיסייה **מרוחק** כדי להזין את הכתובת המרוחקת והיציאה (אם רלוונטי). הכלל החדש שנוצר יוחל כאשר היישום ינסה לנהל תקשורת פעם נוספת.

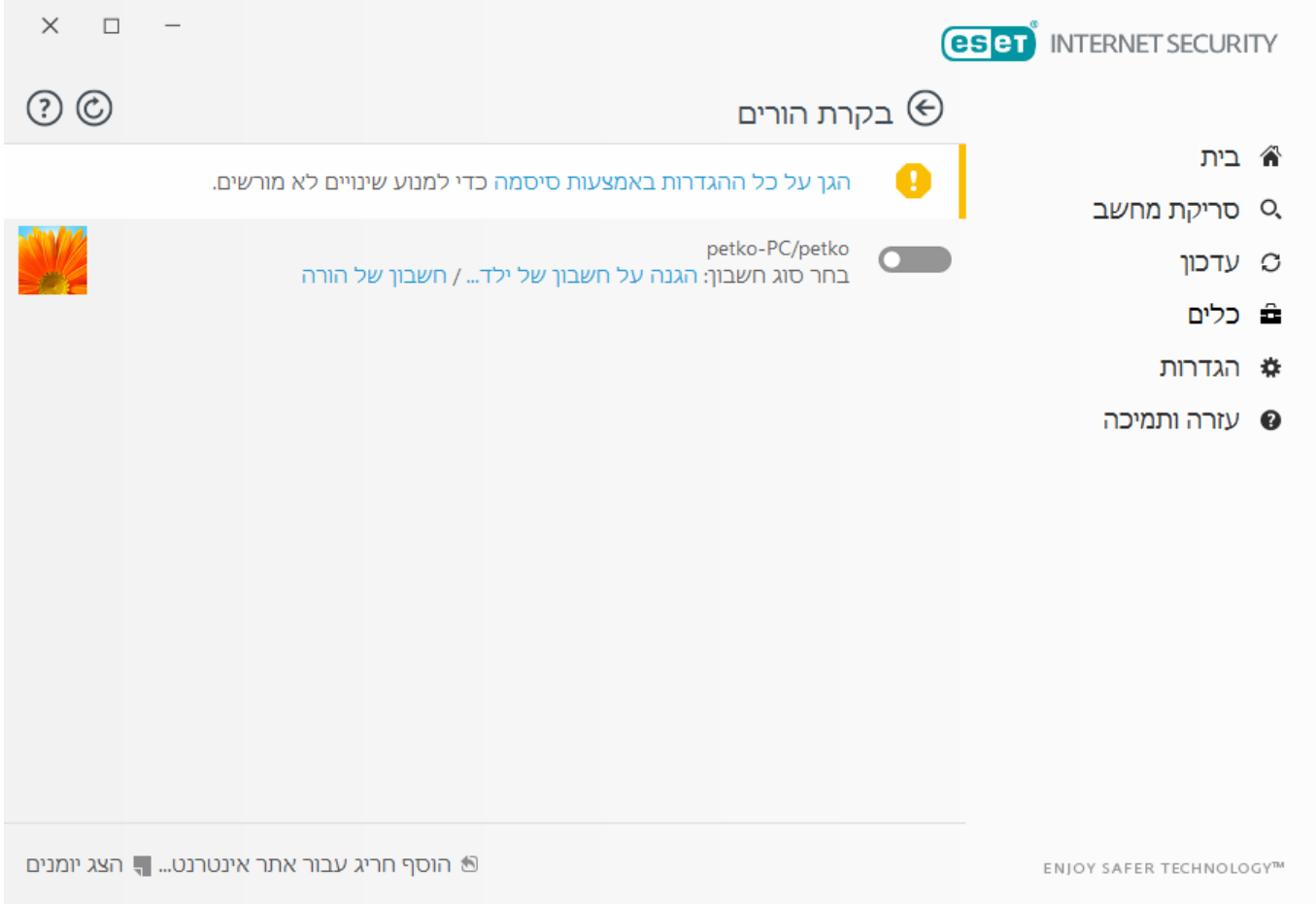
כיצד להפעיל בקרת הורים בחשבון

כדי להפעיל בקרת הורים של חשבון משתמש ספציפי, בצע את הפעולות הבאות:

1. כברירת מחדל, בקרת הורים מושבתת במוצר ESET Internet Security. ישנן שתי שיטות להפעלת בקרת הורים:

   - לחץ על תחת **הגדרות** > **כלי אבטחה** > **בקרת הורים** בחלון התוכנית הראשי והעבר את מצב בקרת ההורים למצב מופעל.
   - הקש F5 כדי לגשת לעץ **הגדרות מתקדמות**, נווט אל **אינטרנט ודוא"ל** > **בקרת הורים** ואז העבר את המתג שליד **שלב במערכת** למצב פעיל.

2. לחץ על **הגדרות** > **כלי אבטחה** > **בקרת הורים** בחלון התוכנית הראשי. למרות שהאפשרות **מופעל** מופיעה לצד **בקרת הורים**, עליך להגדיר את בקרת ההורים לחשבון הרצוי על-ידי לחיצה על **הגן על חשבון ילד** או על **חשבון הורים**. בחלון הבא בחר את תאריך הלידה כדי לקבוע את רמת הגישה ודפי האינטרנט המומלצים בהתאם לגיל. בקרת ההורים תופעל כעת עבור חשבון המשתמש שצוין. לחץ על **תוכן חסום והגדרות...** תחת שם החשבון כדי להתאים אישית את הקטגוריות שברצונך להתיר או לחסום בכרטיסייה קטגוריות. כדי להתאים אישית התרה או חסימה של דפי אינטרנט שאינם תואמים לקטגוריה זו, לחץ על הכרטיסייה חריגים.



כיצד ליצור משימה חדשה במתזמן

כדי ליצור משימה חדשה בתפריט **כלים** > **כלים נוספים** > **מתזמן**, לחץ על **הוסף** או לחץ על לחצן העכבר הימני ובחר **הוסף...** בתפריט ההקשר. חמישה סוגי משימות מתוזמנות זמינים:

- **הפעלת יישום חיצוני** – תזמון ההפעלה של יישום חיצוני.
- **תחזוקת יומן** – קובצי היומן מכילים גם שאריות מרשומות שנמחקו. משימה זו ממטבת את הרשומות בקובצי היומן על בסיס קבוע כדי שיופעלו ביעילות.
- **בדיקת קובץ אתחול מערכת** – הקבצים המורשים לפעול בעת אתחול המערכת או התחברות אליה.
- **צור תמונת מצב של המחשב** – יצירת תמונת מחשב של ESET SysInspector - איסוף מידע מפורט על חיבורי המערכת (לדוגמה מנהלי התקן, יישומים) והערכת רמת הסיכון של כל אחד מהרכיבים.
- **סריקת מחשב לפי דרישה** – ביצוע סריקה של הקבצים והתיקיות במחשב שלך.
- **עדכון** – תזמון משימת עדכון על-ידי עדכון המודולים.

מאחר ש**עדכון** היא אחת מהמשימות המתוזמנות הנפוצות ביותר בשימוש, להלן נסביר כיצד להוסיף משימת עדכון חדשה:

בתפריט הנפתח **משימה מתוזמנת**, בחר **עדכון**. הזן את שם המשימה בשדה **שם משימה** ולחץ על **הבא**. בחר את תדירות המשימה. האפשרויות הבאות זמינות: **פעם אחת**, **שוב ושוב**, **יומית**, **שבועית** ו**מופעלת על-ידי אירוע**. **בחר דלג על המשימה בעת פעולה בכוח הסוללה** כדי למזער את משאבי המערכת כאשר מחשב נייד מופעל בכוח סוללה. משימה זו תופעל בתאריך ובשעה שצוינו בשדות **ביצוע המשימה**. בשלב הבא הגדר את הפעולה שיש לנקוט כאשר לא ניתן לבצע או להשלים משימה במועד המתוזמן. האפשרויות הבאות זמינות:

- **במועד המתוזמן הבא**
- **בהקדם האפשרי**
- **מיידית, אם הזמן שחלף מאז ההפעלה האחרונה חורג מערך שצוין** (את פרק הזמן ניתן להגדיר באמצעות תיבת הגלילה **זמן מההפעלה האחרונה (שעות)**)

בשלב הבא יוצג חלון סיכום עם מידע על המשימה המתוזמנת הנוכחית. לחץ על **סיום** כשתסיים לבצע את השינויים.

יופיע חלון דו-שיח, בו תוכל לבחור את הפרופילים שבהם תשתמש המערכת במשימה המתוזמנת. כאן תוכל להגדיר את הפרופילים הראשי והחלופי. הפרופיל החלופי יהיה בשימוש כאשר לא יתאפשר להשלים את המשימה עם הפרופיל הראשי. אשר בלחיצה על **סיום** והמשימה המתוזמנת החדשה תתווסף לרשימת המשימות המתוזמנות כעת.

כיצד לתזמן סריקת מחשב שבועית

כדי לתזמן משימה קבועה, פתח את חלון התוכנית הראשי ולחץ על **כלים** > **כלים נוספים** > **מתזמן**. להלן מדריך קצר המתאר כיצד לתזמן משימה שתסרוק את הכוננים המקומיים שלך בכל שבוע. לקבלת הוראות מפורטות יותר עיין במאמר מאגר הידע שלנו.

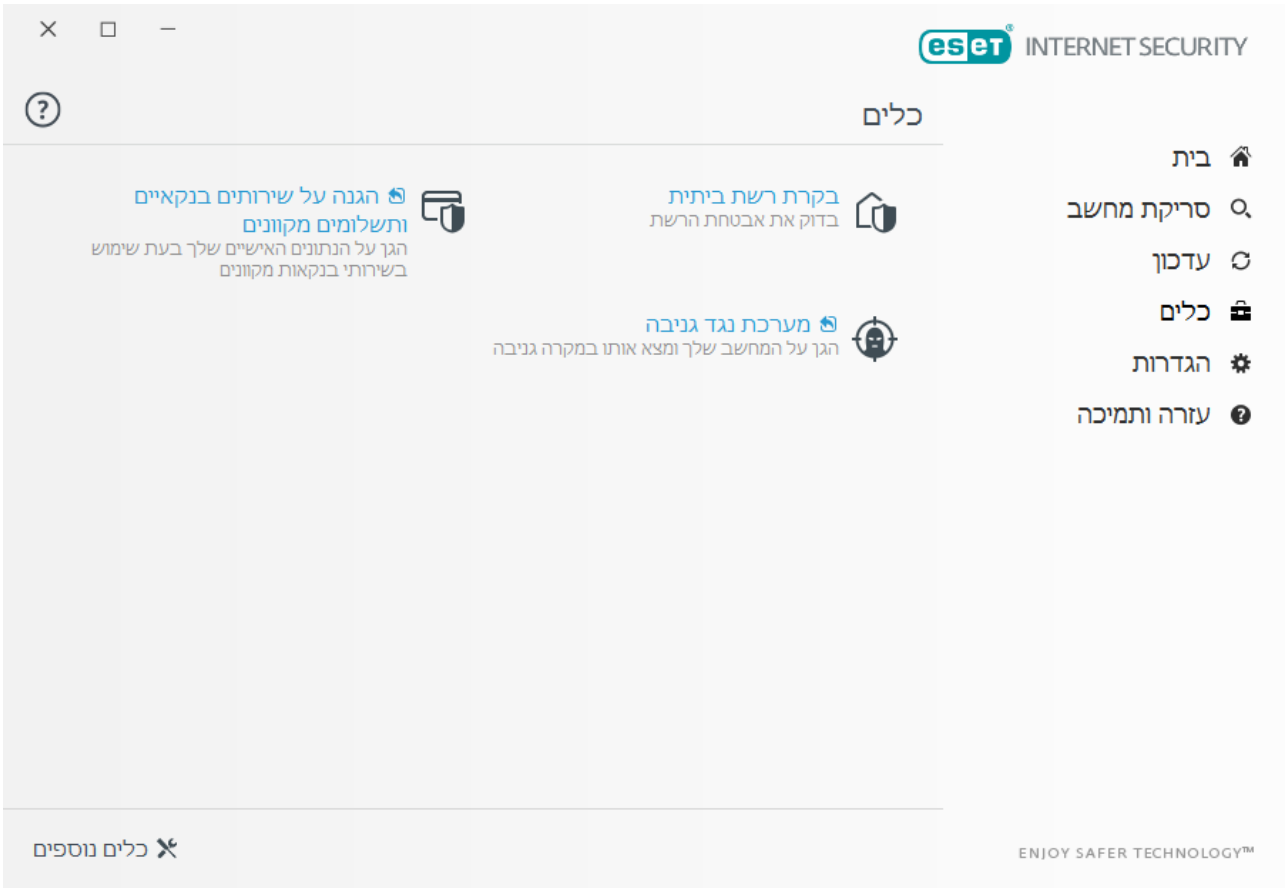
כדי לתזמן משימת סריקה:

1. לחץ על **הוספה** במסך המתזמן הראשי.
2. בחר **סריקת מחשב לפי דרישה** בתפריט הנפתח.
3. הזן שם למשימה ובחר באפשרות **שבועית כתדירות המשימה**.
4. הגדר את היום והשעה שבהם המשימה תבוצע.
5. בחר באפשרות **הפעל את המשימה בהקדם האפשרי** כדי לבצע את המשימה מאוחר יותר, במקרה שהמשימה המתוזמנת לא הופעלה מסיבה כלשהי (למשל אם המחשב היה כבוי).
6. סקור את סיכום המשימה המתוזמנת ולחץ על **סיום**.
7. בתפריט הנפתח **יעדים**, בחר **כוננים מקומיים**.
8. לחץ על **סיום** כדי להחיל את המשימה.

כיצד לפתור את השגיאה "לא הייתה אפשרות לנתב את ההגנה על שירותים בנקאיים ותשלומים מקוונים לדף האינטרנט המבוקש"

כדי לפתור שגיאה זו, פעל בהתאם להנחיות להלן:

1. פתח את חלון התוכנית הראשי במוצר של ESET שברשותך.
2. לחץ על **כלים** > **הגנה על שירותים בנקאיים ותשלומים מקוונים**. כאשר החלון של 'הגנה על שירותים בנקאיים ותשלומים מקוונים' פתוח, המשך לשלב הבא.



לאחר השלמת כל שלב, בדוק אם ההגנה על שירותים בנקאיים ותשלומים מקוונים פועלת
אם חלון הדפדפן עדיין אינו פועל, השלם את השלב הבא עד שחלון הדפדפן ישוב לפעול.

3. נקה את מטמון הדפדפן. כיצד לנקות את המטמון של Firefox או לנקות את המטמון של Google Chrome בדפדפן שלי?

4. הקפד להשתמש בגרסה העדכנית ביותר של מערכת ההפעלה Windows ושל המוצר הביתי של ESET עבור Windows: שדרג את המוצרים הביתיים של ESET עבור Windows לגרסה העדכנית ביותר.

5. השבת את ההגנה על שירותים בנקאיים ותשלומים מקוונים אפשר מחדש את ההגנה על שירותים בנקאיים ותשלומים מקוונים ונסה להפעיל חלון דפדפן מוגן של 'הגנה על שירותים בנקאיים ותשלומים מקוונים'.

6. ודא שדפדפן ברירת המחדל שלך נכלל ב-**הגדרות מתקדמות > אינטרנט ודוא"ל > סינון פרוטוקולים > אפליקציות שאינן נכללות**. גש לתפריט 'הגדרות מתקדמות'.

7. ייתכן שתבחין בהתנגשות עם תוכנת אבטחה או חומת אש של צד שלישי שברשותך. שקול סקירה והסרה של תוכנת צד שלישי זו בחלון 'הוספה/הסרה של תכניות'.

8. אם לא שדרגת את המוצר של ESET שברשותך בשלבים הקודמים, הסר את התקנת המוצר של ESET והתקן אותו שוב. לאחר שהמחשב יופעל מחדש, השבת את ההגנה על שירותים בנקאיים ותשלומים מקוונים ולאחר מכן אפשר אותה מחדש.

הגנה על שירותים בנקאיים ותשלומים מקוונים היא שכבת הגנה נוספת שתוכננה להגן על נתוניך הכספיים במהלך ביצוע עסקאות מקוונות.

במרבית המקרים, 'ESET הגנה על שירותים בנקאיים ותשלומים מקוונים' תופעל בדפדפן ברירת המחדל לאחר ביקור באתר בנקאות מוכר. כדי לגשת לדפדפן המוגן ישירות, לחץ על **כלים** ב-ESET Internet Security ולאחר מכן לחץ על **ESET הגנה על שירותים בנקאיים ותשלומים מקוונים**.

לקבלת פרטים נוספים על התכונות של 'ESET הגנה על שירותים בנקאיים ותשלומים מקוונים', קרא את המאמרים הבאים במאגר הידע של ESET הזמינים באנגלית ובמספר שפות נוספות:

- כיצד אני משתמש בהגנה של ESET על בנקאות ותשלומים?
- אפשר או השבת את ההגנה של ESET על שירותים בנקאיים ותשלומים מקוונים באתר אינטרנט ספציפי
- האם להשהות או להשבית את ההגנה על שירותים בנקאיים ותשלומים מקוונים?
- הגנה של ESET על שירותים בנקאיים ותשלומים מקוונים: שגיאות נפוצות
- מילון של ESET | הגנה על שירותים בנקאיים ותשלומים מקוונים

אם הבעיה עדיין לא נפתרה, שלח דוא"ל אל התמיכה הטכנית של ESET.

כיצד לבטל את הנעילה של הגדרות מתקדמות המוגנות באמצעות סיסמה

כאשר תרצה לגשת להגדרות מתקדמות המוגנות באמצעות סיסמה, החלון להזנת הסיסמה יוצג. אם שכחת או איבדת את הסיסמה, לחץ על האפשרות **שחזר סיסמה** להלן והזן את כתובת הדוא"ל שבה השתמשת לרישום הרישיון. ESET תשלח לך דוא"ל עם קוד האימות. הזן את קוד האימות ולאחר מכן כתוב ואשר את הסיסמה החדשה. קוד האימות יהיה תקף למשך 7 ימים.

באפשרותך גם **לשחזר את הסיסמה באמצעות חשבון my.eset.com**. השתמש באפשרות זו אם הרישיון משויך למנהל הרישיונות של ESET.

אם אינך זוכר את כתובת הדוא"ל, לחץ על **אני לא יודע את כתובת הדוא"ל שלי** ותנותב לאתר האינטרנט של ESET, שם תוכל ליצור קשר במהירות עם מחלקת התמיכה הטכנית שלנו.

צור קוד עבור התמיכה הטכנית – אפשרות זו תיצור את הקוד שאותו יש לספק למחלקת התמיכה הטכנית. העתק את הקוד שסופק על-ידי התמיכה הטכנית ולחץ על **יש ברשותי קוד אימות**. הזן את קוד האימות ולאחר מכן כתוב ואשר את הסיסמה החדשה. קוד האימות יהיה תקף למשך 7 ימים.

לקבלת מידע נוסף קרא את המאמר במאגר הידע של ESET.

תכנית לשיפור חוויית הלקוח

בעצם ההצטרפות אל ה'תכנית לשיפור חוויית הלקוח' אתה מספק ל-ESET מידע אנונימי בנוגע לשימוש במוצרים שלנו. ניתן לקבל מידע נוסף על עיבוד נתונים במדיניות הפרטיות שלנו.

ההסכמה שלך

ההשתתפות בתכנית נעשית בהתנדבות ובהתאם להסכמתך. לאחר ההצטרפות ההשתתפות היא פאסיבית, כלומר, אתה לא צריך לבצע שום פעולה נוספת. באפשרותך לבטל את הסכמתך בכל עת על ידי שינוי הגדרות המוצר. פעולה זו תמנע מאיתנו להמשיך לעבד את הנתונים האנונימים שלך.

אילו סוגי מידע אנו אוספים?

מידע אודות האינטראקציה עם המוצר

אנו לומדים ממידע זה על האופן שבו משתמשים במוצרים שלנו. הודות לכך, אנחנו יודעים למשל באילו פונקציות נעשה שימוש לעתים קרובות, אילו הגדרות משנים המשתמשים או למשך כמה זמן הם משתמשים במוצר.

נתונים אודות מכשירים

אנו אוספים את המידע הזה כדי להבין איפה ובאמצעות אילו מכשירים נעשה שימוש במוצרים שלנו. דוגמאות טיפוסיות הן דגם המכשיר, ארץ, גרסה ושם מערכת ההפעלה.

נתוני אבחון שגיאות

נאסף גם מידע על שגיאות ומצבי קריסה. למשל, איזו שגיאה אירעה ואילו פעולות הובילו לכך.

מדוע אנו אוספים מידע זה?

מידע אנונימי זה מאפשר לנו לשפר את המוצרים שלנו עבורך, המשתמש. הוא עוזר לנו להפוך אותם לרלוונטים יותר, לקלים לשימוש ולנטולי שגיאות ככל האפשר.

מי שולט במידע זה?

ל- ESET, spol. s r.o יש שליטה בלעדית על כל המידע שנאסף במסגרת התכנית. מידע זה לא משותף עם גורמי צד שלישי.

הסכם רישיון תוכנה למשתמש קצה.

חשוב: קרא בקפידה את התנאים וההגבלות של אפליקציית המוצר המפורטים להלן לפני הורדה, התקנה, העתקה או שימוש. **על ידי הורדה, התקנה, העתקה או שימוש בתוכנה אתה מביע את הסכמתך לתנאים והגבלות אלה.**

הסכם רישיון תוכנה למשתמש קצה.

בכפוף לתנאים של הסכם רישיון תוכנה זה למשתמש קצה (להלן "ההסכם"), המבוצע על ידי ובין ESET, spol. s r. o., שמשרדה רשום בכתובת Einsteinova 24, 851 01 Bratislava, Slovak Republic, הרשומה ברשם המסחרי המנוהל על ידי בית המשפט המחוזי l של ברטיסלבה, אזור סרו, רשומה מס' 3586/B, מספר רישום עסק: 31 333 535 (להלן "ESET" או "הספק"), לבינך, אדם פיזי או ישות משפטית (להלן "אתה" או "משתמש הקצה"). אתה זכאי להשתמש בתוכנה המוגדרת בסעיף 1 של הסכם זה. התוכנה המוגדרת בסעיף 1 להסכם זה ניתנת לאחסון אצל ספק נתונים, למשלוח באמצעות דואר אלקטרוני, להורדה משרתי הספקית או להשגה ממקורות אחרים, בכפוף לתנאים המפורטים להלן.

זהו הסכם לגבי זכויות משתמש הקצה ולא הסכם למכירה. הספקית ממשיכה להיות הבעלים של עותק התוכנה והמדיה הפיזית הכלולה באריזת המכירה וכל עותק אחר שמשתמש הקצה רשאי ליצור בכפוף להסכם זה.

על ידי לחיצה על "אני מקבל" במהלך התקנה, הורדה, העתקה או שימוש בתוכנה, אתה מסכים לתנאים ולהגבלות של הסכם זה. אם אינך מסכים לכל התנאים וההגבלות של הסכם זה, לחץ מיד על האפשרות "אינני מקבל", בטל את ההתקנה או ההורדה, או השמד או החזר את התוכנה, מדיית ההתקנה, מסמכים נלווים וקבלת המכירה לספקית או לחנות שממנה השגת את התוכנה.

אתה מסכים שהשימוש שלך בתוכנה מהווה הכרה שקראת הסכם זה, הבנת אותו ואתה מסכים להיות מחויב לתנאים ולהגבלות שבו.

1. **תוכנה**. משמעות המונח "תוכנה", כפי שמשמש בהסכם זה: (1) תוכנית מחשב שהסכם זה נלווה לה, כולל כל הרכיבים שלה; (2) כל התוכן של הדיסקים, התקליטורים ודיסקי ה-DVD, הודעות הדואר האלקטרוני והקבצים המצורפים או מדיה אחרת שבמסגרתה ניתן הסכם זה, לרבות צורת קוד האובייקט של התוכנה, אותו יש לספק בנקודת מחסום נתונים, באמצעות דואר אלקטרוני או בהורדה מהאינטרנט; (3) כל חומר הסברה קשור בפורמט כתוב וכל תיעוד אפשרי אחר הקשור לתוכנה, ובמיוחד, כל תיאור של התוכנה, המפרטים שלה, כל תיאור של מאפייני התוכנה או הפעולה שלה, כל תיאור של סביבת ההפעלה שבה התוכנה נמצאת בשימוש, הוראות שימוש בתוכנה או התקנה שלה או כל תיאור של אופן השימוש בתוכנה (מכאן ואילך ייקרא "תיעוד"); (4) עותקים של התוכנה, תיקונים לשגיאות אפשריות בתוכנה, תוספות לתוכנה, הרחבות לתוכנה, גירסאות שונות של התוכנה ועדכונים לרכיבי התוכנה, אם בכלל, הניתנים לך ברישיון על-ידי הספק לפי סעיף 3 של הסכם זה. התוכנה תסופק באופן בלעדי בצורה של קוד אובייקט לביצוע.

2. **התקנה.** תוכנה שסופקה באמצעות ספקית תקשורת נתונים, נשלחה באמצעות דואר אלקטרוני, הורדה מהאינטרנט, הורדה משרתי הספקית או שהושגה ממקורות אחרים, מצריכה התקנה. עליך להתקין את התוכנה במחשב שתצורתו נקבעה כהלכה, בהתאם לדרישות הסף שצוינו בתיעוד. שיטת ההתקנה מתוארת בתיעוד. אין להתקין במחשב בו הנך מתקין את התוכנה אף תכנית מחשב או חומרה שעשויות להיות להן השפעה שלילית על התוכנה.

3. **רישיון.** בכפוף לתנאים שהסכמת להם, תנאי ההסכם ואתה עומדים בכל התנאים וההגבלות המתוארים בזאת, הספק יעניק לך את הזכויות הבאות ("הרישיון"):

א) **התקנה ושימוש.** תהיה לך זכות לא בלעדית, לא ניתנת להעברה להתקין את התוכנה בכונן הקשיח של מחשב או אמצעי קבוע אחר לאחסון נתונים, התקנה ואחסון של התוכנה בזיכרון של מערכת מחשב וליישם, לאחסן ולהציג את התוכנה.

ב) **התניית מספר הרישיונות.** הזכות להשתמש בתוכנה תהיה מוגבלת בהתאם למספר משתמשי הקצה. משתמש קצה אחד יתייחס לתנאים הבאים: (i) התקנת התוכנה במערכת מחשב אחת; או (ii) אם תחום הרישיון מוגבל למספר תיבות דואר, משתמש קצה אחד יתייחס למשתמש במחשב המקבל דואר אלקטרוני באמצעות סוכן משתמש דואר (להלן: "סוכן"). אם סוכן מקבל דואר אלקטרוני

ומפיץ אותו לאחר מכן באופן אוטומטי למספר משתמשים, אז מספר משתמשי הקצה ייקבע בהתאם למספר המשתמשים בפועל עבורם הדואר האלקטרוני מופץ. אם שרת דואר משמש כשער דואר, מספר משתמשי הקצה יהיה שווה למספר משתמשי שרת הדואר עבורו השער האמור מספקית שירותים. אם מספר בלתי מוגדר של כתובות דואר אלקטרוני מפנות ומתקבלות על-ידי משתמש אחד (למשל, באמצעות כינויים) וההודעות אינן מופצות באופן אוטומטי על-ידי הלקוח למספר גדול יותר של משתמשים, נדרש רישיון עבור מחשב אחד. אסור להשתמש באותו רישיון ביותר ממחשב אחד בו-זמנית.

ג) **גירסת Businnes Edition**. יש להשיג את גירסת Businnes Edition של התוכנה כדי להשתמש בתוכנה בשרתי דואר, בממסרי דואר, בשערי דואר או בשערי אינטרנט.

ד) **תקופת הרישיון.** הזכות שלך להשתמש בתוכנה תוגבל בזמן.

ד) תוכנת יצרן ציוד מקורי (OEM). תוכנת יצרן ציוד מקורי (OEM) תהיה מוגבלת למחשב שאיתו קיבלת אותה. לא ניתן להעביר אותה למחשב אחר.

ה) **תוכנת יצרן ציוד מקורי (OEM)**. תוכנת יצרן ציוד מקורי (OEM) תהיה מוגבלת למחשב שאיתו קיבלת אותה. לא ניתן להעביר אותה למחשב אחר.

ו) **NFR, גרסת ניסיון**. תוכנה המסווגת כתוכנה "שאינה למכירה חוזרת", כ-NFR או כגרסת ניסיון לא ניתן להקצות תמורת תשלום, ויש להשתמש בה אך ורק להדגמה או לבדיקה של תכונות התוכנה.

ו) **סיום הרישיון.** הרישיון יסתיים באופן אוטומטי בסוף התקופה שעבורה הוא הוענק. אם לא תמלא אחר כל אחד מתנאי הסכם זה, הספקית תהיה רשאית לסגת מההסכם, ללא פגיעה בזכויותיה לכל זכאות או פיצוי משפטי הפתוחים לספקית במקרים כאלה. במקרה של ביטול הרישיון, עליך למחוק, להשמיד או להחזיר מיד ועל חשבונך את התוכנה וכל עותקי הגיבוי אל ESET או לחנות שממנה רכשת את התוכנה. עם סיום הרישיון, הספקית תהיה זכאית גם לבטל את זכאות משתמש הקצה לשימוש בפונקציות התוכנה, הדורשות חיבור לשרתי הספקית או לשרתים של צד שלישי.

4. **חיבור לאינטרנט.** הפעלה נכונה של התוכנה דורשת חיבור לאינטרנט ויש להתחבר במרווחי זמן קבועים לשרתי הספקית או לשרתים של צד שלישי. חיבור לאינטרנט נחוץ לצורך הפונקציות הבאות של התוכנה:

א) **עדכונים לתוכנה.** הספקית תהיה זכאית מדי פעם להנפיק עדכונים לתוכנה ("עדכונים"), אך לא תהיה מחויבת לספק עדכונים. פונקציה זו מאופשרת בהגדרות הרגילות של התוכנה. לפיכך, עדכונים יותקנו באופן אוטומטי אלא אם כן משתמש הקצה השבית התקנה אוטומטית של עדכונים.

ד) **העברת הסתננויות ומידע לספקית.** התוכנה מכילה פונקציות אשר אוספות דוגמאות של וירוסי מחשב ותוכנות מחשב זדוניות אחרות ואובייקטים חשודים, בעייתיים, שעשויים להיות בלתי רצויים או שעשויים להיות בלתי בטוחים כגון קבצים, כתובות URL, מנות IP ומסגרות Ethernet (להלן: "הסתננויות") ושולחות אותן לאחר מכן לספקית, לרבות אך ללא הגבלה, מידע אודות תהליך ההתקנה, המחשב ו/או הפלטפורמה שבהם התוכנה מותקנת, מידע אודות הפעולות והתפקודיות של התוכנה ומידע אודות מכשירים ברשת מקומית כגון סוג, ספק, דגם ו/או שם של מכשיר (להלן: "מידע"). המידע וההסתננויות עשויים להכיל נתונים (לרבות נתונים אישיים שהושגו באקראי או בשוגג) אודות משתמש הקצה או משתמשים אחרים במחשב שבו התוכנה מותקנת, ואודות הקבצים המושפעים מההסתננויות עם המטה-נתונים הקשורים.

המידע וההסתננויות עשויים להיאסף באמצעות פונקציות התוכנה הבאות:

i. פונקציית LiveGrid Reputation System כוללת איסוף של קודי Hash חד-כיווניים הקשורים להסתננויות ושליחתם אל הספקית. פונקציה זו זמינה באמצעות הגדרות התוכנה הרגילות.

ii. פונקציית LiveGrid Feedback System כוללת איסוף של הסתננויות עם המטה-נתונים והמידע הקשורים ושליחתם אל הספקית. פונקציה זו מופעלת על-ידי משתמש הקצה במהלך תהליך התקנת התוכנה.

הספקית תשתמש במידע ובהסתננויות שהתקבלו למטרות ניתוח ומחקר של הסתננויות, שיפורי תוכנה ואימות מקוריות רישיון והיא תנקוט באמצעים מתאימים כדי להבטיח שההסתננויות והמידע שהתקבלו יישארו מאובטחים. באמצעות הפעלת פונקציה זו בתוכנה, אתה מביע את הסכמתך לשליחת ההסתננויות והמידע אל הספקית ואתה מעניק לה גם את האישור הנחוץ, כמוגדר בתקנות המשפטיות הרלוונטיות, לעיבוד ההסתננויות והמידע שהושגו. תוכל להשבית פונקציות אלו בכל עת.

ג) **הגנה מפני שימוש לרעה בנתונים.** התוכנה מכילה פונקציה המונעת אובדן או שימוש לרעה בנתונים חיוניים הקשורים ישירות לגניבת מחשב. פונקציה זו מושבתת בתוכנה כברירת מחדל ויש ליצור חשבון MEC במסגרת תנאי שימוש מיוחדים הזמינים בדף

https://my.eset.com, כדי להפעיל אותה ולאפשר איסוף נתונים במקרה של גניבת מחשב. אם תפעיל פונקציה זו בתוכנה, תביע את הסכמתך לשליחת נתונים אודות המחשב הגנוב אל הספק, העשויים להכיל נתונים אודות מיקום הרשת של המחשב, נתונים אודות התוכן המוצג במסך המחשב, נתונים אודות תצורת המחשב או נתונים המוקלטים באמצעות מצלמה המובנית במחשב (להלן: "נתונים"). משתמש הקצה יהיה זכאי להשתמש באופן בלעדי בנתונים שהושגו בדרך זו כדי לתקן מצב שלילי שנגרם על-ידי גניבת מחשב והוא גם מעניק לספקית את האישור הנחוץ, כמוגדר בתקנות המשפטיות הרלוונטיות, לעיבוד הנתונים. הספקית תאפשר למשתמש הקצה לאחסן את הנתונים בציוד הטכני שלה לפרק הזמן הנדרש להשגת המטרה עבורה הנתונים הושגו. תוכל להשבית פונקציה זו בכל עת. יש להשתמש באופן בלעדי בהגנה מפני שימוש לרעה בנתונים באמצעות מחשבים וחשבונות אליהם יש למשתמש הקצה גישה חוקית. כל שימוש בלתי חוקי ידווח לרשות המתאימה. הספקית תפעל בהתאם לחוקים הרלוונטיים ותסייע לרשויות אכיפת החוק במקרה של שימוש לרעה. אתה מביע את הסכמתך ואתה מודע לכך שאתה אחראי להגנה על הסיסמה המשמשת לגישה לחשבון MEC ואתה מביע את הסכמתך שלא תגלה אותה לצד שלישי כלשהו. משתמש הקצה אחראי לכל פעילות באמצעות שימוש בפונקציית 'הגנה מפני שימוש לרעה בנתונים' וחשבון MEC, בהרשאה או לא. הודע מיד לספקית במקרה של חשיפת חשבון MEC. ההגנה מפני שימוש לרעה בנתונים תחול בלעדית על משתמשי הקצה של ESET Smart Security ושל ESET Smart Security Premium.

ד) **סינון, קטגוריזציה ומיקום**. התוכנה מכילה פונקציות אשר מאפשרות למשתמש הקצה להגדיר את הגישה של משתמשים מנוהלים לקבוצה מסוימת של דפי אינטרנט ו/או אפליקציות של מכשירים ניידים, לניהול זמן ולאיתור מיקום. על מנת להפוך תכונות אלה לזמינות, היא שולחת מידע לספקית, לרבות אך ללא הגבלה, מידע אודות אתרי אינטרנט שנכנסו אליהם, מיקומים, אפליקציות של מכשירים ניידים, מידע אודות המחשב, לרבות מידע אודות הפעולות והתפקודיות של התוכנה (להלן: "נתונים"). הנתונים עשויים לכלול מידע (לרבות נתונים אישיים שהושגו באקראי או בשוגג) אודות משתמש הקצה או משתמשים מנוהלים אחרים, מידע אודות המחשב, מערכת ההפעלה והאפליקציות שהותקנו, וקבצים מהמחשב שבו מותקנת התוכנה. הספקית תנקוט את האמצעים הדרושים על מנת להבטיח שהנתונים שמתקבלים נותרים חסויים. הינך מסכים לכך שנתונים יישלחו לספקית וכן הינך מעניק לספקית את האישור הנדרש, כמפורט בתקנות החוקיות הרלוונטיות, לעיבוד הנתונים שהתקבלו. בתכונות אלה ייעשה שימוש בלעדי רק במכשירים של משתמשים מנוהלים אשר למשתמש הקצה יש גישה חוקית אליהם. כל שימוש לא חוקי ידווח לגורם המוסמך. הספקית תציית לחוקים הרלוונטיים ותסייע לרשויות לאכיפת החוק במקרה של שימוש לרעה. הינך מסכים ומאשר כי אתה אחראי על אבטחת סיסמת הגישה לחשבון MEC, והינך מסכים שלא לחשוף את הסיסמה בפני אף גורם שלישי. משתמש הקצה אחראי לכל פעילות העושה שימוש בתכונות של התוכנה ושל חשבון MEC, בין אם השימוש מורשה ובין אם לאו. במקרה של פגיעה כלשהי בבטיחות של חשבון MEC, עליך ליידע את הספקית באופן מיידי. הינך מסכים ומאשר כי הספקית רשאית לפנות אליך באמצעות הודעות בחשבון MEC ובתוכנה, לרבות אך ללא הגבלה, הודעות דואר אלקטרוני עם דוחות ו/או הודעה שבאפשרותך להתאים אישית. סינון, סיווג לקטגוריות ומיקום יחולו בלעדית על משתמשי הקצה של ESET Smart Security ושל ESET Smart Security Premium.

5. **שימוש בזכויות של משתמש הקצה.** עליך להשתמש בזכויות משתמש הקצה באופן אישי או דרך העובדים שלך. אתה רשאי להשתמש בתוכנה אך ורק כדי להגן על פעולותיך וכדי להגן על אותן מערכות מחשב שעבורן השגת רישיון.

6. **הגבלות לזכויות.** אינך רשאי להעתיק, להפיץ, לחלץ רכיבים או ליצור עבודות נגזרות של התוכנה. במהלך השימוש בתוכנה אתה נדרש לציית להגבלות הבאות:

(א) אתה רשאי ליצור עותק אחד של התוכנה על אמצעי אחסון קבוע כעותק גיבוי לארכיון, בתנאי שעותק הגיבוי לארכיון אינו מותקן או משמש בכל מחשב אחר. כל עותק אחר שתכין של התוכנה יהווה הפרה של הסכם זה.

(ב) אינך רשאי להשתמש, לשנות, לתרגם או לשכפל את התוכנה או להעביר זכויות לשימוש בתוכנה או עותקים של התוכנה בכל אופן שהוא פרט לזה המפורט בהסכם זה.

(ג) אינך רשאי למכור, להעביר ברישיון משנה, לחכור או להשכיר או ללוות את התוכנה או להשתמש בתוכנה לצורך מתן שירותים מסחריים.

(ד) אינך רשאי לבצע הנדסה לאחור, קומפילציה לאחור או לפרק את התוכנה או לנסות בכל דרך אחרת לגלות את קוד המקור של התוכנה, פרט למידה שהגבלה זו נאסרת במפורש על פי חוק.

(ה) אתה מסכים שתשתמש בתוכנה אך ורק באופן שמציית לכל החוקים החלים בסמכות השיפוט שבה אתה משתמש בתוכנה, לרבות אך ללא הגבלה, הגבלות ישימות הנוגעות לזכויות יוצרים וזכויות אחרות הקשורות לקניין רוחני.

(ו) אתה מסכים שתשתמש בתוכנה ובפונקציות שלה אך ורק באופן שאינו מגביל את האפשרויות של משתמשי קצה אחרים לגשת לשירותים אלה. הספקית שומרת לעצמה את הזכות להגביל את היקף השירותים המסופקים למשתמשי קצה נפרדים, לאפשר שימוש בשירותים על ידי המספר הגבוה ביותר האפשרי של משתמשי קצה. הגבלת היקף השירותים פירושה גם סיום מוחלט של האפשרות להשתמש בכל אחת מפונקציות התוכנה ומחיקת נתונים ומידע בשרתי הספקית או בשרתים של צד שלישי הקשורים לפונקציה

ספציפית של התוכנה.

7. **זכויות יוצרים.** התוכנה וכל הזכויות, כולל, אך לא רק, כולל זכויות קניין וזכויות קניין רוחני הנובעות מכך, הן בבעלות ESET ו/או מעניקי הרישיונות שלה. הן מוגנות באמצעות הוראות באמנות בינלאומיות ובאמצעות חוקים ארציים אחרים התקפים במדינה בה נעשה שימוש בתוכנה. המבנה, הארגון והקוד של התוכנה הם הסודות המסחריים והמידע החסוי יקרי הערך של ESET ו/או מעניקי הרישיונות שלה. אסור להעתיק את התוכנה, מלבד כפי שנקבע בסעיף 6(א). העותקים אותם אתה רשאי להעתיק בעקבות הסכם זה חייבים להכיל את אותן זכויות יוצרים והודעות קניין אחרות המוצגות בתוכנה. אם תבצע הנדסה או הידור לאחור ואם תנסה לפרק או לגלות בדרך אחרת את קוד המקור של התוכנה, תוך הפרה של התנאים בהסכם זה, תביע בכך את הסכמתך שכל המידע שהושג עד כה יועבר באופן אוטומטי ובאופן שלא ניתן לבטלו או לשנותו אל הספקית ויהיה בבעלותה המלאה, מרגע יצירתו, מבלי לפגוע בזכויות הספקית במקרה של הפרת הסכם זה.

8. **שימור זכויות.** הספקית שומרת בזאת לעצמה את כל הזכויות על התוכנה, פרט לזכויות שהוענקו במפורט בכפוף לתנאי הסכם זה לך כמשתמש הקצה בתוכנה.

9. **גרסאות בשפות מרובות, תוכנה במדיה כפולה, עותקים מרובים.** במקרה שהתוכנה תומכת בפלטפורמות מרובות או בשפות מרובות, או אם קיבלת עותקים מרובים של התוכנה, אתה רשאי להשתמש בתוכנה אך ורק עבור מספר מערכות המחשב ועבור הגרסאות שעבורן השגת רישיון. אינך רשאי למכור, להשכיר, להשכיר בשכירות משנה, להלוות או להעביר גרסאות או עותקים של התוכנה שבהם לא השתמשת.

10. **התחלה וסיום של ההסכם.** הסכם זה ייכנס לתוקף מהתאריך שבו תסכים לתנאי הסכם זה. אתה רשאי לסיים הסכם זה בכל עת על ידי הסרה לצמיתות, השמדה והחזרה, על חשבונך, של התוכנה, של כל עותקי הגיבוי וכל החומרים הקשורים שסופקו על ידי הספקית או שותפיה העסקיים. ללא קשר לאופן הסיום של הסכם זה, התנאים בסעיפים 7, 8, 11, 13, 20 ו-22 ימשיכו לחול למשך זמן בלתי מוגבל.

11. **הצהרות של משתמש הקצה.** כמשתמש קצה, אתה מכיר בזאת שהתוכנה מסופקת כפי שהיא ("AS IS"), ללא אחריות מכל סוג שהוא, מפורשת או משתמעת, ועד למידה המרבית המותרת על פי החוק הישים. הספקית, בעלי הרישיון או חברות המסונפות לה, וכן בעלי זכויות היוצרים לא מייצגים כל טענה או מביעים כל אחריות, במפורש או במשתמע, לרבות אך ללא הגבלה, אחריות של סחירות או התאמה למטרה מסוימת או שהתוכנה לא תפר פטנטים כלשהם, זכויות יוצרים, סימנים מסחריים או זכויות אחרות של צד שלישי. אין כל אחריות של הספק או של כל צד אחר שהפונקציות הכלולות בתוכנה ימלאו את הדרישות שלך או שהפעלת התוכנה תהיה ללא הפרעות או ללא שגיאות. אתה נוטל את כל האחריות והסיכון על בחירת התוכנה להשגת התוצאות המיועדות שלך ועל ההתקנה, השימוש והתוצאות שהושגו ממנו.

12. **אין כל מחויבות אחרת.** הסכם זה לא יוצר כל מחויבות מצד הספקית ובעלי הרישיון שלה פרט לאלה המפורטות באופן ספציפי בזאת.

13. **הגבלת חבות.** עד למידה המרבית המותרת על פי החוק הישים, בכל מקרה הספקית או עובדיה או בעלי הרישיון שלה לא יישאו בחבות על כל אובדן רווחים, הכנסה, מכירות, נתונים או עלויות של רכישת סחורות או שירותים תחליפיים, נזק לרכוש, פציעה אישית, הפרעה לעסקים, אובדן של מידע עסקי או כל נזק מיוחד, ישיר, עקיף, מקרי, כלכלי, כיסויי, עונשי, מיוחד או תוצאתי, בכל דרך שנגרם ואם נובע מחוזה, עוולה, רשלנות או תיאוריית חבות אחרת, הנובעת משימוש או חוסר יכולת להשתמש בתוכנה, גם אם הספקית או בעלי הרישיון שלה או החברות המסונפות לה ידעו על האפשרות של נזקים כאלה. מכיוון שארצות וסמכויות שיפוט מסוימות אינן מתירות אי הכללה של חבות, אך עשויות להתיר הגבלת חבות, החבות של הספקית, עובדיה, בעלי הרישיון שלה או החברות המסונפות לה תוגבל לסכום ששילמת עבור הרישיון.

14. דבר מהאמור בהסכם זה לא יפגע בזכויות המעוגנות בחוק של כל צד הנוהג כצרכן אם הוא נוהג בניגוד לכך.

15. **תמיכה טכנית.** ESET או גורמי צד שלישי שמונו על ידי ESET יספקו תמיכה טכנית לפי שיקול דעתם, ללא כל אחריות או הצהרות. משתמש הקצה יידרש לגבות את כל הנתונים, התוכנות והתוכניות הקיימות לפני שימוש בתמיכה הטכנית. ESET ו/או גורמי צד שלישי שמונו על ידי ESET לא יכולים לקבל חבות על נזקים או אבדן נתונים, רכוש, תוכנות או חומרה או אובדן רווחים עקב שימוש בתמיכה טכנית. ESET ו/או גורמי צד שלישי שמונו על ידי ESET שומרים לעצמם את הזכות להחליט שפתירת בעיה היא מעבר להיקף התמיכה הטכנית. ESET שומרת לעצמה את הזכות לסרב, להשהות או לסיים את אספקת התמיכה הטכנית לפי שיקול דעתה.

16. **העברת הרישיון.** ניתן להעביר את התוכנה ממערכת מחשב אחת לאחרת, אלא אם הדבר מנוגד לתנאי ההסכם. אם הדבר אינו מנוגד לתנאי ההסכם, משתמש הקצה יהיה רשאי להעביר לצמיתות את הרישיון ואת כל הזכויות הנובעות מהסכם זה למשתמש קצה אחר עם הסכמת הספקית, בכפוף לתנאי כי (i) משתמש הקצה המקורי אינו שומר כל עותק של התוכנה; (ii) העברת הזכויות חייבת להיות ישירה, כלומר ממשתמש הקצה המקורי למשתמש הקצה החדש; (iii) משתמש הקצה החדש חייב ליטול על עצמו את כל

הזכויות והמחויבויות שהוטלו על משתמש הקצה המקורי בכפוף לתנאי הסכם זה; (iv) משתמש הקצה המקורי חייב לספק למשתמש הקצה החדש את המסמכים המאפשרים אימות של מקוריות התוכנה כפי שצוין בסעיף 17.

17. **אימות המקוריות של התוכנה** משתמש הקצה יכול להוכיח את זכאותו לשימוש בתוכנה באחת מהדרכים הבאות: (i) באמצעות אישור רישיון המונפק על ידי הספקית או צד שלישי שמונה על ידי הספקית; (ii) באמצעות הסכם רישיון כתוב, אם נערך הסכם כזה; (iii) על ידי שליחת דואר אלקטרוני שנשלח על ידי הספקית, המכיל את פרטי הרישוי (שם משתמש וסיסמה).

18. **נתונים הנוגעים למשתמש הקצה ולהגנה על זכויות.** כמשתמש הקצה, אתה מאשר בזאת לספקית להעביר, לעבד ולאחסן נתונים המאפשרים לה לזהות אותך. אתה מסכים בזאת לשימוש של הספקית באמצעיה שלה כדי לבדוק אם אתה משתמש בתוכנה בהתאם לתנאי הסכם זה. אתה מביע בכך את הסכמתך להעברת הנתונים, במהלך התקשורת בין התוכנה למערכות המחשב של הספקית או של שותפיה העסקיים, למטרת הבטחת התפקודיות והאישור לשימוש בתוכנה ובהגנה על זכויות הספקית. המסקנה הבאה של הסכם זה, הספקית או כל אחד משותפיה העסקיים יהיו זכאים להעביר, לעבד ולאחסן נתונים חיוניים המזהים אותך למטרות חיוב, ביצוע הסכם זה והעברת התראות ו/או הודעות למחשב שלך. אתה מביע בזאת את הסכמתך לקבל התראות והודעות הנוגעות למוצר, כולל, אך לא רק, מידע שיווקי. תוכל להשבית את התכתובת בכל עת. תוכל למצוא פרטים אודות פרטיות והגנה על נתונים אישיים בדף: http://www.eset.com/privacy.

19. **רישוי לרשויות ציבוריות וממשל ארה"ב.** התוכנה תסופק לרשויות ציבוריות, לרבות הממשל של ארה"ב, עם זכויות הרישיון וההגבלות המתוארות בהסכם זה.

20. **יצוא ובקרת יצוא חוזר.** התוכנה, המסמכים או רכיבים שלה, כולל מידע על התוכנה ורכיבים שלה, יהיו כפופים לבקרת ייבוא וייצוא בכפוף לתקנות משפטיות שיונפקו על ידי ממשלות האחריות להנפקת תקנות כאלה בכפוף לחוק החל עליהן, כולל תקנות מנהל הייצוא של ארה"ב, והגבלות על משתמש קצה, משתמש קצה ויעדים שהונפקו על ידי ממשל ארהב וממשלות אחרות. אתה מסכים לציית בקפידה לכל התקנות החלות של ייבוא וייצוא ומסכים שתישא באחריות להשיג את כל הרישיונות הנדרשים כדי לייצא, לייצא מחדש, להעביר או לייבא את התוכנה.

21. **הודעות.** כל ההודעות והחזרות התוכנה והמסמכים יימסרו אל: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

22. **החוק הישים.** הסכם זה יהיה כפוף ובנוי בהתאם לחוקים של הרפובליקה הסלובקית. משתמש הקצה והספקית מסכימים בזאת שהעקרונות של התנגשות חוקים ואמנת האומות המאוחדות לגבי חוזים בינלאומיים ומכירה בינלאומית של סחורות לא יחולו. אתה מסכים במפורש שכל מחלוקת או תביעה הנובעות מהסכם זה ביחס לספקית או כל מחלוקת או תביעה לגבי השימוש בתוכנה ייפתרו על ידי בית המשפט המחוזי I של ברטיסלבה ואתה מסכים במפורש למימוש סמכות השיפוט של בית המשפט האמור.

23. **הוראות כלליות.** במקרה שכל אחד מהתנאים בהסכם זה לא יהיה תקף או לא ניתן לאכיפה, הדבר לא ישפיע על התקפות של תנאים אחרים בהסכם, שיישארו בתוקף וניתנים לאכיפה בהתאם לתנאים שנקבעו בזאת. הסכם זה ניתן לשינוי אך ורק בכתב, כשהוא נושא חתימה של נציג מוסמך של הספקית או אדם שהוסמך במפורש לפעול בתפקיד זה בכפוף לתנאים של כתב הרשאה. זהו ההסכם המלא בין הספקית ובינך בנוגע לתוכנה והוא מחליף כל ייצוג, דיון, התחייבות, תקשורת או פרסום בנוגע לתוכנה.

נספח מספר 1 להסכם רישיון למשתמש קצה בנושא נתונים מאובטחים של Eset

1. הגדרות

1.1 בהסכם זה, למילים הבאות יש את המשמעויות הללו בהתאמה:

"מידע" כל מידע או נתונים שהוצפנו או שפוענחו באמצעות התוכנה;

"מוצרים" התוכנה והתיעוד של ESET Secure Data;

"ESET Secure Data" התוכנה/התוכנות שנעשה בה/ן שימוש להצפנה ולפענוח של נתונים אלקטרוניים;

1.2 כל אזכור של לשון רבים יכלול את לשון יחיד וכל אזכור של לשון זכר יכלול את לשון נקבה ולשון סתמי, ולהיפך.

2. מענק רישיון והתחייבויות מצד הספקית

בהתחשב בהסכמתך וציותך לתנאי הסכם זה, ולאחר ששילמת עבור רישיון, הספקית מעניקה לך זכות לא-בלעדית ובלתי ניתנת להעברה להתקין ולהשתמש בתוכנה עבור מספר המשתמשים שעבורם רכשת רישיון. נדרש רישיון נפרד לכל משתמש.

3. הצהרת משתמש קצה נוספת

3.1 הינך מאשר ומסכים כי:

3.2.1 מתוקף אחריותך להגן, לתחזק ולגבות מידע;

3.2.2 עליך לגבות באופן מלא את כל המידע והנתונים (לרבות, אך ללא הגבלה, כל מידע ונתונים קריטיים) במחשב שלך לפני התקנת ESET Secure Data;

3.2.3 עליך לנהל רישום של כל הסיסמאות או מידע אחר המשמש להגדרת התוכנה ולשימוש בה, ולשמור אותו במקום בטוח. כמו כן, עליך ליצור עותקים לגיבוי של כל מפתחות ההצפנה, קודי הרישיון, קבצי המפתח ונתונים אחרים המופקים כדי להפריד מדיית אחסון;

3.2.4 הינך אחראי על השימוש במוצרים. אין הספקית נושאת באחריות בגין כל אובדן, טענה או נזק אשר נגרמו כתוצאה מהצפנה או פענוח לא מורשים או מוטעים של מידע או נתונים (לרבות אך ללא הגבלה, מידע) בכל מקום ובכל דרך שבהם מידע או נתונים אלה מאוחסנים;

3.2.5 על אף שהספקית נקטה בכל הצעדים המתקבלים על הדעת על מנת להבטיח את התקינות ואת האבטחה של ESET Secure Data, אין להשתמש במוצרים (או בכל אחד מהם) באזורים הנתמכים במערך אבטחה ברמת אל-כשל או באזורים העלולים להיות מסוכנים, לרבות אך ללא הגבלה, מתקנים גרעיניים, מערכות ניווט של כלי טיס, מערכות בקרה או תקשורת, מערכות נשק והגנה ומערכות תומכות חיים או מערכות ניטור רפואי;

3.2.6 הינך אחראי להבטיח שרמת האבטחה וההצפנה שמספקים המוצרים הולמת את דרישותיך;

3.2.7 הינך אחראי על השימוש שלך במוצרים (או בכל אחד מהם), לרבות אך ללא הגבלה, ההבטחה ששימוש זה מציית לכל התקנות והחוקים הרלוונטיים של הרפובליקה הסלובקית או של מדינה או אזור אחרים שבהם נעשה שימוש במוצר. עליך להבטיח כי לפני שנעשה שימוש כלשהו במוצרים, וידאת שהשימוש לא מפר אמברגו של ממשלה כלשהי (ברפובליקה הסלובקית או במקומות אחרים);

3.2.8 הינך אחראי לנהל רישום של כל המידע המשמש להגדרת התוכנה ולשימוש בה, ולשמור אותו במקום בטוח. עליך לנהל רישום של כל הסיסמאות או פרטי מידע אחרים המשמשים להגדרת התוכנה ולשימוש בה, ולשמור אותו במקום בטוח. כמו כן, עליך ליצור עותקים לגיבוי של כל מפתחות ההצפנה, קודי ההפעלה ונתונים אחרים המופקים כדי להפריד מדיית אחסון;

3.2.9 אין הספקית נושאת באחריות בגין כל אובדן, נזק, הוצאה או טענה אשר נובעים מאובדן, גניבה, שימוש לרעה, השחתה, נזק או הרס של סיסמאות, מידע התקנה, מפתחות הצפנה, קודי הפעלת רישיון ונתונים אחרים אשר מופקים או מאוחסנים במהלך השימוש בתוכנה.

נספח מס' 1 יחול בלעדית על משתמשי הקצה של ESET Smart Security Premium.

נספח מספר 2 להסכם רישיון למשתמש קצה בנושא Password Manager Software

1. אינך רשאי

א) להשתמש ב-Password Manager Software להפעלת אפליקציות בעלות חשיבות קריטית היכולות להעמיד בסכנה חיי אדם או רכוש. הינך מבין כי Password Manager Software אינה מיועדת למטרות אלה וכי כשלון פעולה שלה במקרים כגון אלה עלול להוביל למוות, לנזק גופני, לנזק חמור לרכוש או לנזק סביבתי חמור שהספקית אינה אחראית בגינו.

Password Manager Software אינה מותאמת, מיועדת או מורשית לשימוש בסביבות מסוכנות שבהן נדרשים פקדי אל-כשל, לרבות אך ללא הגבלה, העיצוב, הבנייה, התחזוקה או התפעול של מתקנים גרעיניים, מערכות ניווט של כלי טיס או מערכות תקשורת, מערכות לבקרת תנועה אווירית, מערכות תומכות חיים או מערכות נשק. הספקית מסירה את אחריותה באופן מובהק מכל אחריות התאמה מפורשת או מרומזת למטרות אלה.

ב) להשתמש ב-Password Manager Software באופן המהווה הפרה של הסכם זה או של החוקים של הרפובליקה הסלובקית או של תחום השיפוט שלך. במיוחד אינך רשאי להשתמש ב-Password Manager Software על מנת לבצע או לקדם פעילויות בלתי חוקיות כלשהן, לרבות העלאת נתונים בעלי תוכן מזיק או בעלי תוכן שעלול לשמש לביצוע פעילויות בלתי חוקיות או תוכן שמפר בדרך כלשהי את החוק או את הזכויות של צד שלישי כלשהו (לרבות זכויות קניין רוחני כלשהן), לרבות אך ללא הגבלה, ניסיונות כלשהם לגשת לחשבונות באחסון (למטרות הסכם זה, "אחסון" מתייחס לשטח אחסון הנתונים המנוהל על ידי הספקית או על ידי צד שלישי שאינו הספקית או המשתמש, ומיועד לאפשר סינכרון וגיבוי של נתוני המשתמש) או לכל חשבון או נתונים של משתמשים אחרים ב-Password Manager Software או באחסון. במקרה של הפרה של אחד מתנאים אלה, הספקית רשאית לסיים הסכם זה באופן

מיידי ולחייב אותך בעלויות של כל תיקון שנדרש. כמו כן, היא רשאית לנקוט בכל הצעדים הנדרשים על מנת למנוע ממך את המשך השימוש ב-Password Manager Software ללא אפשרות לקבלת החזר כספי.

2. Password Manager Software מסופקת "כפי שהיא", ללא כל אחריות מפורשת או מרומזת. השימוש בתוכנה הוא על אחריותך בלבד. אין היצרן אחראי בגין אובדן נתונים, נזיקין, מגבלות בזמינות השירות לרבות נתונים כלשהם הנשלחים על ידי Password Manager Software לאחסון חיצוני למטרת סינכרון נתונים וגיבוי. הצפנת הנתונים באמצעות Password Manager Software אינה מרמזת על אחריות כלשהי של הספקית באשר לאבטחת נתונים אלה. הינך מסכים במפורש כי הנתונים שנעשה בהם שימוש או הנתונים שהושגו, הוצפנו, אוחסנו, סונכרנו או נשלחו באמצעות Password Manager Software יכולים להיות מאוחסנים גם בשרתים של צד שלישי (חל רק על שימוש ב-Password Manager Software שבמסגרתו הופעלו שירותי סינכרון וגיבוי). אם הספקית בוחרת על פי שיקול דעתה הבלעדי להשתמש באחסון, באתר אינטרנט, בפורטל אינטרנט, בשרת או בשירות של צד שלישי מסוג זה, אין הספקית אחראית לאיכות, לאבטחה או לזמינות של שירות צד שלישי מסוג זה, ובשום אופן אין הספקית אחראית בגין הפרה כלשהי של מחויבויות חוזיות או משפטיות שבוצעה על ידי הצד השלישי ואף אין היא אחראית בגין נזיקין, אובדן רווחים, נזקים פיננסיים או לא פיננסיים, או בגין כל סוג אחר של אובדן שהתרחש במהלך השימוש בתוכנה זו. אין הספקית אחראית לתוכן של הנתונים שנעשה בהם שימוש או של הנתונים שהושגו, הוצפנו, אוחסנו, סונכרנו או נשלחו באמצעות Password Manager Software או של הנתונים שבאחסון. הינך מאשר כי לספקית אין גישה לתוכן של הנתונים שאוחסנו וכי אין באפשרותה לנטר אותם או להסיר תוכן הנחשב מזיק מבחינה משפטית.

כל הזכויות על השיפורים, השדרוגים והתיקונים הקשורים ל-Password Manager Software ("שיפורים") שמורות לספקית, גם במקרה ששיפורים מסוג זה נוצרו על סמך משוב, רעיונות או הצעות שהגשת בדרך כלשהי. לא תהיה זכאי לפיצוי כלשהו, לרבות תמלוגים כלשהם הקשורים לשיפורים אלה.

3. הגבלת אחריות נוספת.

ישויות ומעניקי רישיונות מטעם הספקית אינם אחראים בגין תביעות ומחויבויות מכל סוג אשר נובעות או קשורות בדרך כלשהי לשימוש ב-Password Manager Software על ידך או על ידי צדדים שלישיים, לשימוש או לחוסר השימוש בחברות תיווך או במשווקים כלשהם, או למכירה או רכישה של אבטחה כלשהי, גם אם תביעות ומחויבויות כגון אלו מבוססות על דינים משפטיים או על דיני יושר כלשהם.

הישויות ומעניקי הרישיונות מטעם הספקית אינם אחראים בגין נזיקין ישירים, מקריים, מיוחדים, עקיפים או נסיבתיים אשר נובעים או קשורים לתוכנה כלשהי של צד שלישי, לנתונים כלשהם שבוצעה אליהם גישה דרך Password Manager Software, לשימוש שלך ב-Password Manager Software או לחוסר היכולת שלך להשתמש בה או לגשת אליה, או לנתונים כלשהם שסופקו באמצעות Password Manager Software, גם אם טענות אלה בגין נזק נכללות בדינים משפטיים או בדיני יושר כלשהם. נזיקין שאינם נכללים בסעיף זה כוללים, ללא הגבלה, נזיקין בגין אובדן של רווחים עסקיים, נזק גופני או נזק לרכוש, הפרעה עסקית, אובדן עסקים או אובדן של מידע אישי. תחומי שיפוט מסוימים אינם מאפשרים הגבלה על נזיקין מקריים או נסיבתיים, לכן ייתכן שמגבלה זו לא תחול עליך. במקרה מסוג זה, אחריות הספקית תהיה ברמה המינימלית המותרת בחוק הרלוונטי.

מידע שסופק באמצעות Password Manager Software, לרבות מחירי מניות, אנליזת שוק, חדשות ונתונים פיננסיים, עשוי להתעכב, להיות לא מדויק, או להכיל שגיאות או השמטות, והישויות ומעניקי הרישיונות מטעם הספקית לא יהיו אחראים באשר לכך. הספקית רשאית לשנות או להפסיק כל היבט או תכונה של Password Manager Software או לשנות או להפסיק את השימוש בכל התכונות או בכל אחת מהתכונות או הטכנולוגיות ב-Password Manager Software בכל עת מבלי להודיע לך על כך מראש.

אם התנאים המופיעים בפרק זה יבוטלו מכל סיבה או אם הספקית תימצא אחראית בגין אובדנים, נזיקין וכדומה במסגרת החוקים הרלוונטיים, הצדדים מסכימים כי אחריות הספקית כלפיך תהיה מוגבלת לערך הכולל של דמי הרישיון ששילמת.

הינך מסכים לפצות, להגן ולשמור ללא כל נזק על הספקית ועובדיה, חברות הבת שלה, הסניפים שלה, המותגים שלה ושותפיה האחרים מכל וכנגד כל תביעה, אחריות, נזיקין, אובדן, עלות, הוצאה ועמלה של צד שלישי (לרבות הבעלים של המכשיר או גורמים שזכויותיהם הושפעו מהנתונים שנעשה בהם שימוש ב-Password Manager Software או באחסון) אשר גורמים כגון אלה עשויים להיות חשופים להם כתוצאה מהשימוש שלך ב-Password Manager Software.

4. נתונים ב-Password Manager Software.

אלא אם בחרת אחרת באופן מפורש, כל הנתונים שהזנת שנשמרים במסד הנתונים של Password Manager Software מאוחסנים בתבנית מוצפנת במחשב שלך, או בהתקן אחסון אחר שהגדרת. הינך מבין כי במקרה של מחיקה או של נזק למסד נתונים כלשהו של Password Manager Software או לקבצים אחרים, כל הנתונים הנמצאים בהם יאבדו באופן בלתי הפיך, והינך מבין ומקבל על עצמך את הסיכון הכרוך באובדן מסוג זה. העובדה שנתוניך האישיים מאוחסנים בתבנית מוצפנת במחשב אינה מבטיחה כי אדם

כלשהו שמגלה את הסיסמה הראשית או מקבל גישה להתקן ההפעלה שהוגדר על ידי הלקוח לפתיחת מסד הנתונים לא יוכל לגנוב את המידע או לעשות בו שימוש לרעה. הינך אחראי על תחזוקת האבטחה של כל אמצעי הגישה.

העברת נתונים אישיים לספקית או לאחסון

בהתאם לבחירתך ורק על מנת להבטיח סינכרון נתונים וגיבוי במועד, Password Manager Software מעבירה או שולחת נתונים אישיים ממסד הנתונים של Password Manager Software - כלומר סיסמאות, פרטי כניסה, חשבונות וזהויות - דרך האינטרנט לאחסון. הנתונים מועברים באופן מוצפן בלבד. ייתכן שלצורך השימוש ב-Password Manager Software למילוי טפסים מקוונים עם סיסמאות, פרטי כניסה או נתונים אחרים תידרש שליחה של נתונים דרך האינטרנט אל אתר אינטרנט שזוהה על ידך. העברת נתונים זו אינה מופעלת על ידי Password Manager Software, ולכן לא ניתן להטיל על הספקית את האחריות על אבטחת אינטראקציות כאלו עם אתר אינטרנט כלשהו הנתמך על ידי ספקים שונים. כל עסקה דרך האינטרנט, בין אם נעשה במסגרתה שימוש ב-Password Manager Software ובין אם לאו, נעשית על פי שיקול דעתך הבלעדי ועל אחריותך בלבד, ואתה תהיה האחראי הבלעדי לכל נזק למערכת המחשב או לכל אובדן נתונים הנובע מהורדה ו/או שימוש בחומר או שירות מסוג זה. כדי למזער את הסיכון לאבד נתונים בעלי ערך, הספקית ממליצה לבצע גיבוי תקופתי של מסד הנתונים ושל קבצים רגישים אחרים בכוננים חיצוניים. אין באפשרות הספקית לספק לך סיוע כלשהו בשחזור נתונים שאבדו או שניזוקו. אם הספקית מספקת שירותי גיבוי לקבצי מסד נתונים של המשתמש במקרה של נזק או מחיקה של הקבצים במחשבים של משתמשים, שירותי גיבוי מסוג זה מגיעים ללא כל אחריות ואינם מרמזים על התחייבות כלשהי של הספקית כלפיך.

Password Manager Software אינה מנטרת בשום אופן את היסטוריית הגלישה שלך באינטרנט. כמו כן, Password Manager Software אינה אוספת, וגם אינה שולחת, מידע אודות אתרים שביקרת בהם או מידע כלשהו אודות היסטוריית הגלישה שלך לגורם כלשהו. ייתכן שגרסאות מסוימות של Password Manager Software תומכות בזיהוי משתמש של אתרי אינטרנט ותכניות שאתה, המשתמש, יכול להביא לתשומת לבה של הספקית על ידי שליחה באמצעות הכלי הייעודי ב-GUI; מידע זה לא יישלח מבלי שתלחץ על אישור המביע את הסכמתך לשלוח את שם אתר האינטרנט או התכנית. בדרך כלל מידע מסוג זה שנשלח משמש לשיפור התפקודיות של Password Manager Software.

מתוקף השימוש שלך ב-Password Manager Software, הינך מסכים לכך שהתוכנה רשאית לפנות אל שרתי הספקית מעת לעת על מנת לבדוק אם קיימים פרטי רישיון, תיקונים זמינים, ערכות שירות ועדכונים אחרים העשויים לשפר, לתחזק או לחזק את התפעול של Password Manager Software. התוכנה עשויה לשלוח פרטי מערכת כלליים הקשורים לתפקוד של Password Manager Software.

5. מידע והוראות בנושא הסרת התקנה

לפני הסרת ההתקנה של Password Manager Software, יש לייצא את כל המידע שברצונך לשמור ממסד הנתונים.

נספח מס׳ 2 יחול בלעדית על משתמשי הקצה של ESET Smart Security Premium.

מדיניות פרטיות

ESET, spol. s r. o., שמשרדה הרשום ממוקם ב-Einsteinova 24, 851 01 Bratislava, Slovak Republic והרשומה במרשם המסחרי המנוהל על ידי בית המשפט המחוזי Bratislava I, Section Sro, מס׳ רשומה B/3586, מספר רישום עסקי: 31 333 535 (ה"ESET" או "אנחנו") מעוניינים לנהוג בשקיפות בכל הנוגע לעיבוד נתונים אישיים ולפרטיות של לקוחותינו. כדי להשיג מטרה זו, אנו מפרסמים מדיניות פרטיות זו מתוך מטרה יחידה ליידע את הלקוח שלנו ("משתמש קצה" או "אתה") אודות הנושאים הבאים:

- עיבוד של נתונים אישיים,
- סודיות נתונים,
- זכויות של נושא הנתונים.

עיבוד של נתונים אישיים

השירותים המסופקים על-ידי ESET והמיושמים במוצר שלנו מסופקים תחת תנאי הסכם הרישיון למשתמש קצה ("EULA") אך חלק מהם עשויים לדרוש תשומת לב ספציפית. ברצוננו לספק לך פרטים נוספים על איסוף נתונים ביחס לאספקת השירותים שלנו. אנו

מספקים נתונים שונים המתוארים בהסכם הרישיון למשתמש הקצה או בתיעוד המוצרים, כגון שירות עדכון/שדרוג, ®Livegrid, הגנה מפני ניצול לרעה של נתונים, תמיכה ועוד. כדי לאפשר שירותים אלה, עלינו לאסוף את המידע להלן:

• עדכון ונתונים סטטיסטיים אחרים המכסים מידע על תהליך ההתקנה והמחשב שלך כולל הפלטפורמה שעליה המוצר שלנו מותקן ומידע על הפעולות והפונקציונליות של המוצרים שלנו, כגון מערכת הפעלה, מידע על חומרה, מזהי התקנה, מזהי רישיון, כתובת IP, כתובת MAC והגדרות התצורה של המוצר.

• קודי Hash חד-כיווניים המשויכים לחדירות, כחלק ממערכת המוניטין של ®ESET LiveGrid, המשפרת את יעילות הפתרונות שלנו נגד תוכנות זדוניות על-ידי השוואת קבצים שנסרקו למסד נתונים בענן הכולל פריטים ברשימות לבנות ופריטים ברשימות שחורות.

• דגימות חשודות ומטה-נתונים חשודים מרחבי הרשת, כחלק ממערכת המשוב של ®ESET LiveGrid, המאפשרת ל-ESET להגיב באופן מיידי לצרכים של משתמשי הקצה שלה ולאפשר לה יכולת תגובה לאיומים האחרונים. לכן אנו תלויים בך שתשלח לנו

oמידע על חדירות כגון דגימות אפשריות של וירוסים ותוכנות זדוניות וחשודות אחרות; אובייקטים בעייתיים, אובייקטים העלולים להיות לא רצויים או אובייקטים העלולים להיות לא בטוחים, כגון קובצי הפעלה, הודעות דוא"ל שדווחו על-ידך כדואר זבל או שסומנו על-ידי המוצר שלנו;

oמידע על התקנים ברשת המקומית כגון סוג, ספק, דגם ו/או שם של התקן;

oמידע בנוגע לשימוש באינטרנט כגון כתובת IP ומידע גיאוגרפי, מנות IP, כתובות URL ומסגרות Ethernet;

oקובצי dump של קריסה והמידע הכלול בה.

איננו מעוניינים באיסוף הנתונים שלך מעבר להיקף זה, אך לפעמים בלתי אפשרי למנוע זאת. נתונים שנאספו באופן מקרי עשויים להיכלל בתוכנה זדונית עצמה (והם נאספו ללא ידיעתך או אישורך) או כחלק משמות קבצים או כתובות URL ואיננו מתכוונים להשתמש בהם כחלק מהמערכות שלנו או לעבד אותם למטרה המוצהרת במדיניות פרטיות זו.

• פרטי הרישוי, כגון מזהה הרישיון ונתונים אישיים כגון שם, שם משפחה, כתובת וכתובת דוא"ל נדרשים למטרות חיוב, אימות מקוריות הרישיון ואספקת השירותים שלנו.

• פרטי יצירת הקשר והנתונים הכלולים בבקשות התמיכה שלך עשויים להידרש לשירות התמיכה. בהתבסס על הערוץ שתבחר ליצירת קשר עמנו, אנו עשויים לאסוף את כתובת הדוא"ל ומספר הטלפון שלך, את פרטי הרישיון, פרטי המוצר והתיאור של מקרה התמיכה. ייתכן שתתבקש לספק לנו פרטים אחרים כדי לאפשר את שירות התמיכה.

• נתוני מיקום, צילומי מסך, נתונים על תצורת המחשב והנתונים שהוקלטו על-ידי המצלמה של המחשב שלך עשויים להיאסף לשם הגנה מפני ניצול לרעה של פונקציית הנתונים לתקופת שמירה של שלושה חודשים. יש ליצור חשבון ב-https://my.eset.com, שבאמצעותו הפונקציה מפעילה איסוף נתונים במקרה של גניבת המחשב. נתונים שנאספו מאוחסנים בשרתים שלנו או בשרתים של ספקי השירות שלנו.

• נתוני Password Manager, כגון סיסמאות וכתובות, מאוחסנים בצורה מוצפנת רק במחשב או בהתקן ייעודי אחר. אם תפעיל את שירות הסינכרון, הנתונים המוצפנים יאוחסנו בשרתים שלנו או בשרתים של ספקי השירות שלנו כדי להבטיח שירות כזה. ל-ESET או לספק השירות אין גישה לנתונים המוצפנים. רק לך יש את המפתח לפענוח הנתונים.

סודיות נתונים

ESET היא חברה שפועלת ברחבי העולם דרך ישויות מסונפות או שותפים כחלק מרשת ההפצה, השירות והתמיכה שלנו. המידע המעובד על-ידי ESET עשוי להיות מועבר אל ישויות מסונפות או שותפים או מהם, לצורך ביצוע הסכם הרישיון למשתמש קצה, כגון אספקת שירותים, תמיכה או חיוב. בהתבסס על המיקום שלך והשירות שבו תבחר להשתמש, ייתכן שנידרש להעביר את הנתונים שלך למדינה שאינה מיישמת את ההתאמה להגנה על נתונים בהתאם להחלטות האיחוד האירופי. אפילו במקרה זה, כל העברה של מידע כפופה לרגולציה מתוקף החקיקה בנושא הגנת נתונים והיא תתבצע רק אם יש צורך בכך. יש לבסס מנגנון Privacy Shield, סעיפים חוזיים רגילים, תקנות ארגוניות מחייבות או אמצעי הגנה מתאימים אחרים ללא יוצא מן הכלל.

אנו עושים כמיטב יכולתנו כדי למנוע אחסון של מידע לפרק זמן ארוך מהנדרש תוך אספקת שירותים במסגרת הסכם הרישיון למשתמש הקצה. תקופת השמירה שלנו עשויה להיות ארוכה מתוקף הרישיון שלך רק כדי לתת לך זמן לחידוש קל ונוח. נתונים סטטיסטיים ממוזערים ונתונים סטטיסטיים שאינם מאפשרים זיהוי אישי ונתונים אחרים מ-®ESET LiveGrid עשויים לעבור עיבוד נוסף למטרות סטטיסטיקה.

ESET נוקטת אמצעים טכניים וארגוניים מתאימים כדי להבטיח רמת אבטחה שמתאימה לסיכונים אפשריים. אנו עושים את המרב כדי להבטיח את הסודיות, השלמות, הזמינות והעמידות השוטפות של מערכות ושירותי העיבוד. עם זאת, במקרה של הפרת נתונים הגורמת לסיכון הזכויות והחירויות שלך, אנו מוכנים ליידע את הרשות המפקחת וכן את נושאי הנתונים. כנושא נתונים, עומדת לך הזכות להגיש תלונה לרשות מפקחת.

זכויות של נושא הנתונים

ESET כפופה לרגולציה של החוקים הסלובקיים ואנו מחויבים לחקיקה בנושא הגנת נתונים כחלק מהאיחוד האירופי. אתה זכאי לזכויות הבאות כנושא נתונים:

- זכות לבקש מ-ESET גישה לנתונים האישיים שלך,
- זכות לתיקון הנתונים האישיים שלך אם הם לא מדויקים (עומדת לך גם הזכות להשלמת נתונים אישיים חסרים),
- זכות לבקש מחיקה של הנתונים האישיים שלך,
- זכות לבקש הגבלה של עיבוד הנתונים האישיים שלך
- זכות להתנגד לעיבוד וכן
- זכות לניידות נתונים.

אם ברצונך ליישם את זכותך כנושא נתונים או שיש לך שאלה או חשש, שלח לנו הודעה לכתובת:

ESET, spol. s r.o
הממונה על הגנת נתונים
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk