ESET Smart Security Premium

מדריך למשתמש

לחץ כאן כדי להציג את הגרסה המקוונת של מסמך זה

Digital Security
Progress. Protected.

זכויות יוצרים ©2024 מאת ESET, spol. s r.o.

ESET Smart Security Premium פותח על-ידי ESET, spol. s r.o.

בקר בכתובת https://www.eset.com לקבלת מידע נוסף.

כל הזכויות שמורות. אין לשכפל, לאחסן במערכת אחזור או לשדר מסמך זה בכל צורה או אמצעים כלשהם, אלקטרוניים, מכניים, העתקה, הקלטה, סריקה, או בכל דרך אחרת ללא אישור בכתב מהמחבר.

ESET, spol. s r.o. שומרת לעצמה את הזכות לשנות ללא כל הודעה מוקדמת את תוכנות האפליקציה המתוארות במסמך זה.

תמיכה טכנית: https://support.eset.com

REV. 12/04/2024

1 ESET Smart Security Premium 1
1.1 מה חדש 2
1.2 איזה מוצר יש לי? 3
1.3 דרישות מערכת 4
1.3 גרסה מיושנת של Microsoft Windows 5
1.4 מניעה 5
1.5 דפי עזרה 6
2 התקנה 7
2.1 Live installer 8
2.2 התקנה לא מקוונת 9
2.2 שדרוג מינוי 11
2.2 שדרוג המוצר 12
2.2 בוצע שדרוג לאחור של המינוי 12
2.2 שדרוג לאחור של מוצר 13
2.3 פותר בעיות התקנה 14
2.4 סריקה ראשונה לאחר ההתקנה 14
2.5 שדרוג לגרסה עדכנית יותר 15
2.5 עדכון אוטומטי של מוצר מדור קודם 15
2.5 ESET Smart Security Premium יותקן 16
2.5 עבור לקו מוצרים אחר 16
2.5 רישום 16
2.5 התקדמות ההפעלה 16
2.5 ההפעלה בוצעה בהצלחה 17
3 תחילת העבודה 17
3.1 סמל מגש מערכת 17
3.2 מקשי קיצור במקלדת 18
3.3 פרופילים 18
3.4 עדכונים 19
3.5 קבע את התצורה של הגנת הרשת 21
3.6 הפעל מערכת נגד גניבה 22
3.7 בקרת הורים 23
4 הפעלת מוצר 23
4.1 הזנת מפתח ההפעלה במהלך ההפעלה 24
4.2 השתמש ESET HOME בחשבון 24
4.3 הפעל גרסת ניסיון ללא תשלום 25
4.4 מפתח הפעלה ללא תשלום של ESET 26
4.5 ההפעלה נכשלה - תרחישים נפוצים 26
4.6 סטטוס המינוי 27
4.6 ההפעלה נכשלה עקב מינוי שנעשה בו שימוש יתר 28
5 עבודה עם ESET Smart Security Premium 29
5.1 מבט כולל 30
5.2 סריקת מחשב 33
5.2 מפעיל סריקה מותאמת אישית 35
5.2 התקדמות הסריקה 36
5.2 יומן רישום של המחשב 38
5.3 עדכון 39
5.3 חלון דו-שיח ? נדרשת הפעלה מחדש 42

5.3 כיצד ליצור משימות עדכון 42
5.4 כלים 43
5.4 רשומות יומן 44
5.4 סינון יומן 46
5.4 תהליכים פועלים 48
5.4 דוח אבטחה 49
5.4 חיבורי רשת 50
5.4 פעילות רשת 52
5.4 ESET SysInspector 53
5.4 מתזמן 53
5.4 אפשרויות סריקה מתוזמנת 55
5.4 סקירת משימות מתוזמנות 56
5.4 פרטי משימה 56
5.4 תזמון משימה 56
5.4 תזמון המשימה - פעם אחת 57
5.4 תזמון המשימה - יומי 57
5.4 תזמון המשימה - שבועי 57
5.4 תזמון המשימה - הפעלה באמצעות אירוע 57
5.4 דילוג על משימה 57
5.4 פרטי משימה - עדכון 58
5.4 פרטי משימה - הפעלת אפליקציה 58
5.4 כלי ניקוי המערכת 58
5.4 מפקח הרשת 59
5.4 התקן רשת במפקח הרשת 61
5.4 התראות | מפקח הרשת 62
5.4 הסגר 63
5.4 בחירת דוגמה לניתוח 66
5.4 בחר דגימה לשליחה ולניתוח - קובץ חשוד 67
5.4 בחר דגימה לשליחה ולניתוח - אתר חשוד 67
5.4 בחר דגימה לשליחה ולניתוח � זיהוי חיובי שגוי של קובץ 67
5.4 בחר דגימה לשליחה ולניתוח - זיהוי חיובי שגוי של אתר 67
5.4 בחר דגימה לשליחה ולניתוח - אחר 68
5.5 הגדרות 68
5.5 הגנת מחשב 69
5.5 זוהתה חדירה 70
5.5 הגנת אינטרנט 73
5.5 הגנת אנטי-פישינג 74
5.5 בקרת הורים 75
5.5 חריגות אתר אינטרנט 77
5.5 העתקת חריגה מהמשתמש 79
5.5 העתקת קטגוריות מהחשבון 79
5.5 הגנת רשת 79
5.5 חיבורי רשת 81
5.5 פרטי חיבור הרשת 81
5.5 פתרון בעיות בגישה לרשת 82
5.5 רשימה שחורה זמנית של כתובות IP 82
5.5 יומני הגנת רשת 83
5.5 פתרון בעיות עם חומת האש של 84
5.5 רישום ויצירת כללים או חריגות ביומן 84

5.5 יצירת כלל מיומן רישום 84
5.5 יצירת חריגות מהודעות חומת אש אישית 85
5.5 רישום מתקדם ביומן של הגנת רשת 85
5.5 פתרון בעיות עם סורק תעבורת הרשת 85
5.5 איום רשת נחסם 86
5.5 זוהתה רשת חדשה 87
5.5 יצירת חיבור - זיהוי 88
5.5 שינוי ביישום 89
5.5 תקשורת מהימנה נכנסת 89
5.5 תקשורת מהימנה יוצאת 91
5.5 תקשורת נכנסת 92
5.5 תקשורת יוצאת 93
5.5 הגדרות תצוגת חיבור 95
5.5 כלי אבטחה 95
5.5 גלישה ושירותים בנקאיים בטוחים 96
5.5 התראה בדפדפן 96
5.5 פרטיות ואבטחה בדפדפן 97
5.5 מערכת נגד גניבה 99
5.5 התחבר לחשבון ESET HOME שלך 100
5.5 הגדר שם מכשיר 101
5.5 מערכת נגד גניבה מופעל/מושבת 102
5.5 הוספת מכשיר חדש נכשלה 102
5.5 102 .... Secure Data
5.5 יצירת כונן וירטואלי מוצפן 103
5.5 הצפנת קבצים בכונן נשלף 104
5.5 104 .... Password Manager
5.5 הגדרות יבוא ויצוא 104

5.6 עזרה ותמיכה 105
5.6 אודות 106 .... ESET Smart Security Premium
5.6 חדשות 107 .... ESET
5.6 שלח נתוני תצורת מערכת 107
5.6 תמיכה טכנית 108

5.7 חשבון 108 .... ESET HOME
5.7 התחבר אל 110 .... ESET HOME
5.7 התחברות לחשבון 111 .... ESET HOME
5.7 ההתחברות נכשלה ? שגיאות נפוצות 112
5.7 הוספת מכשיר ב-112 .... ESET HOME

6 הגדרות מתקדמות 113

6.1 מנגנון איתור 114
6.1 החרגות 114
6.1 החרגות לביצועים 114
6.1 הוספה או עריכה של אי הכללה של ביצועים 115
6.1 תבנית אי הכללה של נתיב 117
6.1 החרגות לזיהויים 118
6.1 הוספה או עריכה של אי הכללה באיתור 119
6.1 אשף יצירת ההחרגות לאיתור 120
6.1 אפשרויות מתקדמות של מנגנון האיתור 121
6.1 סורק תעבורת רשת 121
6.1 הגנה מבוססת ענן 121

6.1 מסנן החרגה עבור הגנה מבוססת ענן 124
6.1 ESET LiveGuard 124
6.1 סריקת תוכנות זדוניות 126
6.1 פרופילי סריקה 126
6.1 יעדי סריקה 127
6.1 סרוק במצב לא פעיל 128
6.1 איתור במצב לא פעיל 128
6.1 סריקה בעת אתחול המערכת 128
6.1 בדיקת קובץ אתחול אוטומטית 129
6.1 מדיה נשלפת 129
6.1 הגנה על מסמכים 130
6.1 HIPS - מערכת למניעת חדירות למארח 131
6.1 אי הכללות HIPS 133
6.1 הגדרות מתקדמות של HIPS 133
6.1 טעינת מנהלי התקן מתאפשרת תמיד 133
6.1 חלון אינטראקטיבי של HIPS 134
6.1 מצב למידה הסתיים 135
6.1 זוהה אופן פעולה שעשוי להצביע על נוזקת כופר (ransomware) 135
6.1 ניהול הכללים של HIPS 136
6.1 הגדרות כללי HIPS 137
6.1 הוספת נתיב רישום/אפליקציה עבור HIPS 140
6.2 עדכון 140
6.2 חזרה למצב קודם לאחר עדכון 142
6.2 מרווח זמן לחזרה למצב קודם 143
6.2 עדכוני מוצר 144
6.2 אפשרויות חיבור 144
6.3 הגנות 145
6.3 הגנה בזמן אמת על מערכת קבצים 148
6.3 אי הכללת תהליכים 150
6.3 הוספה או עריכה של אי-הכללות של תהליכים 150
6.3 מתי לשנות את תצורת ההגנה בזמן אמת 151
6.3 בדיקת הגנה בזמן אמת 151
6.3 מה לעשות אם ההגנה בזמן אמת אינה פועלת 151
6.3 הגנת גישה לאינטרנט 152
6.3 פרופילים של חיבורי רשת 153
6.3 הוספה או עריכה של פרופילי חיבור רשת 153
6.3 מפעילים 155
6.3 קבוצות של כתובות IP 156
6.3 ערוך קבוצות של כתובות IP 156
6.3 מפקח הרשת 157
6.3 חומת אש 157
6.3 הגדרות מצב למידה 159
6.3 כללים של חומת אש 160
6.3 הוספה או עריכה של כללי חומת אש 162
6.3 איתור שינוי אפליקציות 165
6.3 רשימת אפליקציות שאינן כלולות באיתור 165
6.3 הגנה מפני מתקפות רשת (IDS) 166
6.3 כללי IDS 166
6.3 הגנה מפני מתקפות Brute Force 169

6.3 כללים ... 170
6.3 אפשרויות מתקדמות ... 172
6.3 SSL/TLS ... 173
6.3 כללי סריקת יישומים ... 175
6.3 כללי אישור ... 176
6.3 תעבורת רשת מוצפנת ... 177
6.3 ThreatSense ... 177
6.3 הגנת גישה לאינטרנט ... 180
6.3 אפליקציות שאינן נכללות ... 182
6.3 כתובות IP שלא נכללו ... 183
6.3 ניהול רשימה של כתובות URL ... 184
6.3 רשימת כתובות ... 185
6.3 יצירת רשימת כתובות חדשה ... 186
6.3 כיצד להוסיף מסיכת URL ... 187
6.3 סריקה של תעבורת HTTP (S) ... 188
6.3 ThreatSense ... 188
6.3 בקרת הורים ... 191
6.3 חשבונות משתמש ... 191
6.3 הגדרות של חשבון משתמש ... 192
6.3 קטגוריות ... 194
6.3 הגנת דפדפן ... 195
6.3 גלישה ושירותים בנקאיים בטוחים ... 195
6.3 בקרת התקנים ... 196
6.3 עורך כללי בקרת התקנים ... 197
6.3 התקנים שאותרו ... 198
6.3 הוספת כללי בקרת התקנים ... 198
6.3 קבוצות התקנים ... 201
6.3 הגנת מצלמת אינטרנט ... 202
6.3 עורך כללי הגנת מצלמת אינטרנט ... 202
6.3 ThreatSense ... 203
6.3 רמות ניקוי ... 206
6.3 סיומות קבצים שלא ייכללו בסריקה ... 206
6.3 פרמטרים נוספים של ThreatSense ... 207
6.4 כלים ... 207
6.4 Microsoft Windows® Update ... 208
6.4 חלון דו-שיח עדכוני מערכת ... 208
6.4 פרטי עדכון ... 208
6.4 ESET CMD ... 208
6.4 רשומות יומן ... 210
6.4 מצב משחק ... 211
6.4 אבחון ... 212
6.4 תמיכה טכנית ... 213
6.5 קישוריות ... 213
6.6 ממשק משתמש ... 214
6.6 אלמנטי ממשק משתמש ... 215
6.6 הגדרות גישה ... 216
6.6 סיסמה להגדרות מתקדמות ... 217
6.6 תמיכה בקוראי מסך ... 217
6.7 התראות ... 218

6.7 חלון דו-שיח - סטטוסים של אפליקציות 219
6.7 הודעות שולחן עבודה 219
6.7 רשימת התראות בשולחן העבודה 220
6.7 התראות אינטראקטיביות 221
6.7 הודעות אישור 223
6.7 העברה 224
6.8 הגדרות פרטיות 226
6.8 אפס להגדרות ברירת המחדל 226
6.8 החזרת כל ההגדרות במקטע הנוכחי למצב הקודם 227
6.8 שגיאה במהלך שמירת התצורה 227
6.9 סורק שורת פקודה 227
7 שאלות נפוצות 229
7.1 כיצד לעדכן את ESET Smart Security Premium 230
7.2 כיצד להסיר וירוס מהמחשב 230
7.3 כיצד לאפשר תקשורת עבור יישום מסוים 230
7.4 כיצד להפעיל בקרת הורים בחשבון 231
7.5 כיצד ליצור משימה חדשה במתזמן 232
7.6 כיצד לתזמן סריקת מחשב שבועית 233
7.7 כיצד לבטל את הנעילה של הגדרות מתקדמות 233
7.8 כיצד לפתור את ביטול ההפעלה של המוצר מתוך ESET HOME 234
7.8 הפעלת המוצר בוטלה, המכשיר נותק 234
7.8 המוצר אינו מופעל 234
8.1 תכנית לשיפור חוויית הלקוח 235
8.2 הסכם רישיון למשתמש קצה 236
8.3 מדיניות פרטיות 246

ESET Smart Security Premium

ESET Smart Security Premium 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 Smart Security Premium 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 Smart Security Premium ומציעה תוכן תמיכה המתעדכן באופן דינמי.
מצב כהה	הרחבה המסייעת לך להחליף במהירות את המסך לערכת נושא כהה. באפשרותך לבחור את ערכת הצבעים המועדפת עליך ברכיבי ממשק המשתמש.
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 Smart Security Premium.
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 Smart Security Premium

גלישה ושירותים בנקאיים בטוחים	גלישה ושירותים בנקאיים בטוחים מספקת דפדפן מאובטח לשימוש בעת הגישה לשערי בנקאות או תשלום מקוונים, כדי להבטיח שכל העסקאות המקוונות יתבצעו בסביבה מהימנה ומאובטחת.
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.
אנטי ספאם בלקוח דוא"ל	דואר זבל מייצג עד 50 אחוזים מכלל התקשורת בדואר אלקטרוני. אנטי ספאם בלקוח דוא"ל מגן מפני בעיה זו.
מערכת נגד גניבה	מערכת נגד גניבה מרחיב את האבטחה ברמת המשתמש במקרה של מחשב שאבד או נגנב. לאחר התקנת ESET Smart Security Premiumומערכת נגד גניבה, המכשיר שלך יירשם בממשק האינטרנט. ממשק האינטרנט מאפשר לך לנהל את התצורה של מערכת נגד גניבה ולפקח על כל תכונות מערכת נגד גניבה במכשיר שלך.
בקרת הורים	הגנה על משפחתך מפני תוכן אינטרנטי שעלול להיות פוגעני על-ידי חסימת קטגוריות שונות של אתרי אינטרנט.
Password Manager	הכלי Password Manager המגן על הסיסמאות ועל הנתונים האישיים שלך ומאחסן אותם.
Secure Data	התכונה Secure Data מאפשרת לך להצפין נתונים במחשב שלך וכוננים נשלפים כדי למנוע שימוש לרעה במידע פרטי וסודי.
ESET LiveGuard	מגלה ומפסיק איומים שטרם נראו בעבר ומעבד אותם לצורך איתור עתידי.

מינוי צריך להיות פעיל כדי שתכונות ESET Smart Security Premium יפעלו. אנו ממליצים לחדש את המינוי מספר שבועות לפני תום המינוי ל-ESET Smart Security Premium.

מה חדש

מה חדש ב-ESET Smart Security Premium 17.1

- שיפורים קטנים במפקח הרשת
- שיפורים קטנים בגלישה ושירותים בנקאיים בטוחים
- ESET LiveGuard – שליחת המסמכים מופעלת כעת כברירת מחדל
- תיקוני באגים ושיפורים קלים אחרים

כדי להשבית **התראות 'מה חדש'**:
1. פתח את הגדרות מתקדמות > **התראות** > **התראות בשולחן העבודה**.
2. לחץ על **ערוך** לצד **התראות שולחן העבודה**.
3. בטל את הבחירה בתיבת הסימון **הצג התראות 'מה חדש'** ולחץ על **אישור**.

למידע נוסף על התראות, עיין במקטע התראות.

לרשימה מפורטת של השינויים ב-ESET Smart Security Premium, ראה יומן רישום שינויים של ESET Smart Security Premium.

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**
- **ESET Security Ultimate**

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

בטבלה שלהלן מפורטות התכונות הזמינות בכל מוצר ספציפי.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
מנגנון איתור	✔	✔	✔	✔
למידת מכונה מתקדמת	✔	✔	✔	✔
חוסם פירצות אבטחה	✔	✔	✔	✔
הגנה מבוססת-Script מפני מתקפות	✔	✔	✔	✔
מערכת אנטי פישינג	✔	✔	✔	✔
הגנת גישה לאינטרנט	✔	✔	✔	✔
HIPS (כולל הגנה מפני נוזקות כופר)	✔	✔	✔	✔
אנטי-ספאם		✔	✔	✔
חומת אש		✔	✔	✔
מפקח הרשת		✔	✔	✔
הגנת מצלמת אינטרנט		✔	✔	✔
הגנה מפני מתקפות רשת		✔	✔	✔
הגנה מפני 'מחשב זומבי' (Botnet)		✔	✔	✔
גלישה ושירותים בנקאיים בטוחים		✔	✔	✔
פרטיות ואבטחה בדפדפן		✔	✔	✔
בקרת הורים		✔	✔	✔
מערכת נגד גניבה		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

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

דרישות מערכת

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

המעבדים הנתמכים

מעבד Intel או AMD, 32 סיביות (x86) עם מערכת הוראות SSE2 או מעבד 64 סיביות (x64), במהירות 1 GHz ומעלה
מעבד מבוסס ARM64, במהירות 1GHz ומעלה

מערכות הפעלה נתמכות

Microsoft® Windows® 11

Microsoft® Windows® 10

יש להתקין תמיכה בחתימת קוד ב-Azure בכל מערכות ההפעלה של Windows כדי להתקין או לשדרג את מוצרי ESET שיצאו לאחר יולי 2023. מידע נוסף.

נסה תמיד לשמור על מערכת הפעלה עדכנית.

דרישות עבור תכונות של ESET Smart Security Premium

עיין בדרישות המפורטות בטבלה שלהלן עבור תכונות ספציפיות של ESET Smart Security Premium:

דרישות	תכונה
עיין ברשימת המעבדים הנתמכים.	Intel® Threat Detection Technology
עיין ברשימת דפדפני האינטרנט הנתמכים.	גלישה ושירותים בנקאיים בטוחים
Windows 10 גרסה RS4 ואילך.	רקע שקוף
מעבד שאינו מבוסס ARM64.	מנקה מומחה
מעבד שאינו מבוסס ARM64.	כלי ניקוי המערכת
מעבד שאינו מבוסס ARM64.	חוסם פירצות אבטחה
מעבד שאינו מבוסס ARM64.	בדיקה התנהגותית עמוקה

אחר

נדרש חיבור לאינטרנט כדי שההפעלה והעדכונים של ESET Smart Security Premium יפעלו כהלכה.

שתי תכניות אנטי-וירוס הפועלות בו-זמנית יגרמו להתנגשויות בלתי נמנעות במערכת, כגון האטת מערכת שתפגע בפעולתה.

גרסה מיושנת של Microsoft Windows

בעיה

- אתה מעוניין להתקין את הגרסה האחרונה של ESET Smart Security Premium במחשב שבו פועל Windows 7, Windows 8 (8.1) או Windows Home Server 2011
- ESET Smart Security Premium מציג שגיאה **מערכת הפעלה מיושנת** במהלך ההתקנה

פרטים

הגרסה האחרונה של ESET Smart Security Premium דורשת את מערכות ההפעלה Windows 10 או Windows 11.

פתרון

הפתרונות הבאים זמינים:

שדרג ל-Windows 10 או ל-Windows 11

תהליך השדרוג קל יחסית, ובמקרים רבים ניתן לעשות זאת מבלי לאבד את הקבצים. לפני שדרוג ל-Windows 10:

1. גבה נתונים חשובים.
2. קרא את השאלות הנפוצות לגבי שדרוג ל-Windows 10 או את השאלות הנפוצות לגבי שדרוג ל-Windows 11 של Microsoft ועדכן את מערכת ההפעלה Windows.

התקן את ESET Smart Security Premium גרסה 16.0

אם אין באפשרותך לשדרג את Windows, התקן את ESET Smart Security Premium גרסה 16.0. עיין בעזרה מקוונת לגרסה 16.0 של ESET Smart Security Premium לקבלת מידע נוסף.

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 Smart Security Premium. המידע המופיע כאן יסייע לך להתוודע למוצר ולהפוך את המחשב שלך לבטוח יותר.

תחילת העבודה

לפני שתשתמש ב-ESET Smart Security Premium, אתה מוזמן לקרוא על סוגי האובייקטים המזוהים וההתקפות המרוחקות שבהם אתה עשוי להיתקל בעת השימוש במחשב. הכנו גם רשימה של תכונות חדשות שנוספו ל-ESET Smart Security Premium.

התחל בהתקנת ESET Smart Security Premium. אם כבר התקנת את ESET Smart Security Premium, עיין בעבודה עם ESET Smart Security Premium.

כיצד להשתמש בדפי העזרה של ESET Smart Security Premium

העזרה המקוונת מחולקת למספר פרקים ותתי-פרקים. הקש **F1** ב-ESET Smart Security Premium 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 ולמנוע בלבול, המינוח שבו משתמש מדריך זה מבוסס על ממשק המשתמש של ESET Smart Security Premium. אנו משתמשים גם במערכת סמלים אחידה כדי להדגיש נושאים בעלי עניין או משמעות מיוחדים.

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.

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

זהו מידע שמצריך יותר תשומת לב וזהירות. אזהרות ממוקמות ספציפית כדי למנוע ממך לבצע טעויות שעלולות לגרום נזק. קרא והבן את הטקסט, מאחר שהוא מתייחס להגדרות מערכת רגישות ביותר או לנושא מסוכן.

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

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

עזרה מקוונת היא המקור העיקרי לתוכן עזרה. הגרסה העדכנית ביותר של העזרה המקוונת תוצג באופן אוטומטי כשאתה מחובר לאינטרנט.

התקנה

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

- Live installer הורדתו מתבצעת מאתר האינטרנט של ESET או מתקליטור/DVD. חבילת ההתקנה היא אוניברסלית לכל השפות (בחר בשפה המתאימה). Live installer הוא קובץ קטן; ההורדה של קבצים נוספים שנדרשים להתקנת ESET Smart Security Premium מתבצעת אוטומטית.
- התקנה לא מקוונת משתמשת בקובץ exe. גדול יותר מקובץ ה-Live installer ואין צורך בחיבור לאינטרנט או בקבצים נוספים כדי להשלים את ההתקנה.

לפני שתתקין את ESET Smart Security Premium 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 ב-Installer Wizard.

בסוג ההתקנה הזה עליך להיות מחובר לאינטרנט.

1. בחר את השפה המתאימה בתפריט הנפתח ולחץ על **המשך**.

אם אתה מתקין גרסה חדשה יותר במקום הגרסה הקודמת תוך שימוש בהגדרות המוגנות באמצעות סיסמה, הקלד את הסיסמה שלך. באפשרותך לקבוע את התצורה של סיסמת ההגדרות בהגדרות גישה.

2. בחר את ההעדפה שלך עבור התכונות הבאות, קרא את הסכם הרישיון למשתמש קצה ואת מדיניות הפרטיות ולחץ על **המשך**, או לחץ על **אפשר הכל והמשך** כדי להפעיל את כל התכונות:

- מערכת המשוב של ESET LiveGrid®
- אפליקציה העלולה להיות לא רצויה
- תכנית לשיפור חוויית הלקוח

בהקשה על **המשך** או **אפשר הכל והמשך**, אתה מסכים להסכם הרישיון למשתמש קצה ומאשר את מדיניות הפרטיות.

3. כדי להפעיל, לנהל ולהציג את אבטחת המכשיר באמצעות ESET HOME, חבר את המכשיר לחשבון ESET HOME.
לחץ על **דלג על ההתחברות** כדי להמשיך מבלי להתחבר אל ESET HOME. תוכל לחבר את המכשיר שלך לחשבון

ESET HOME שלך במועד מאוחר יותר.

4. אם תמשיך בלי להתחבר אל ESET HOME, בחר אפשרות הפעלה. אם אתה מתקין גרסה חדשה יותר במקום הגרסה הקודמת, **מפתח ההפעלה** שלך מוזן אוטומטית.
5. אשף ההתקנה קובע איזה מוצר ESET מותקן לפי המינוי שלך. הגרסה עם תכונות האבטחה הרבות ביותר תמיד נבחרת מראש. לחץ על **שנה מוצר** אם ברצונך להתקין גרסה אחרת של מוצר ESET. לחץ על **המשך** כדי להתחיל את תהליך ההתקנה. הפעולה עשויה להימשך מספר רגעים.

> אם נותרו שאריות (קבצים או תיקיות) ממוצרי ESET שהוסרו בעבר, תתבקש לאפשר את הסרתם. לחץ על **התקן** כדי להמשיך.

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

פותר בעיות התקנה.

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

התקנה לא מקוונת

הורד והתקן את המוצר הביתי של ESET עבור Windows באמצעות המתקין הלא מקוון (.exe) להלן. בחר איזו גרסה של המוצר הביתי של ESET להוריד (32 סיביות, 64 סיביות או ARM).

ESET Security Ultimate	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
הורדה של 64 סיביות הורדה של 32 סיביות הורדת ARM	הורדה של 64 סיביות הורדה של 32 סיביות הורדת ARM	הורדה של 64 סיביות הורדה של 32 סיביות הורדת ARM	הורדה של 64 סיביות הורדה של 32 סיביות הורדת ARM

> אם יש לך חיבור אינטרנט פעיל, התקן את מוצר ESET שלך באמצעות Live installer.

כשתפעיל את המתקין הלא מקוון (.exe), אשף ההתקנה ינחה אותך לאורך התהליך.

1. בחר את השפה המתאימה בתפריט הנפתח ולחץ על **המשך**.

> אם אתה מתקין גרסה חדשה יותר במקום הגרסה הקודמת תוך שימוש בהגדרות המוגנות באמצעות סיסמה, הקלד את הסיסמה שלך. באפשרותך לקבוע את התצורה של סיסמת ההגדרות בהגדרות גישה.

2. בחר את ההעדפה שלך עבור התכונות הבאות, קרא את הסכם הרישיון למשתמש קצה ואת מדיניות הפרטיות ולחץ על **המשך**, או לחץ על **אפשר הכל והמשך** כדי להפעיל את כל התכונות:

- מערכת המשוב של ESET LiveGrid®
- אפליקציה העלולה להיות לא רצויה
- תכנית לשיפור חוויית הלקוח

> בהקשה על **המשך** או **אפשר הכל והמשך**, אתה מסכים להסכם הרישיון למשתמש קצה ומאשר את מדיניות הפרטיות.

3. לחץ על **דלג על ההתחברות**. כשיהיה לך חיבור לאינטרנט, תוכל לחבר את המכשיר שלך לחשבון ESET HOME שלך.
4. לחץ על **דלג על ההפעלה**. יש להפעיל את ESET Smart Security Premium לאחר ההתקנה כדי שתהיה לו פונקציונליות מלאה. הפעלת המוצר דורשת חיבור אינטרנט פעיל.
5. אשף ההתקנה מראה איזה מוצר של ESET יותקן לפי המתקין הלא מקוון שהורד. לחץ על **המשך** כדי להתחיל את תהליך ההתקנה. הפעולה עשויה להימשך מספר רגעים.

> אם נותרו שאריות (קבצים או תיקיות) ממוצרי ESET שהוסרו בעבר, תתבקש לאפשר את הסרתם. לחץ על **התקן** כדי להמשיך.

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

⚠ פותר בעיות התקנה.

שדרוג מינוי

חלון ההתראה הזה מופיע כאשר המינוי ששימש להפעלת מוצר ESET שלך השתנה. המינוי שהשתנה מאפשר לך להפעיל מוצר עם יותר תכונות אבטחה. אם לא בוצע שינוי, ESET Smart Security Premium יציג פעם אחת חלון התראה עם הכותרת **עבור למוצר עם יותר תכונות**.

כן (מומלץ) □ אפשרות זו תתקין אוטומטית את המוצר הכולל יותר תכונות אבטחה.

לא, תודה □ לא יתבצעו שינויים, וההתראה תיעלם לצמיתות.

כדי להחליף את המוצר מאוחר יותר, עיין במאמר מאגר הידע של ESET. למידע נוסף על מינוי ESET, ראה שאלות נפוצות בנושא מינוי.

בטבלה שלהלן מפורטות התכונות הזמינות בכל מוצר ספציפי.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
מנגנון איתור	✔	✔	✔	✔
למידת מכונה מתקדמת	✔	✔	✔	✔
חוסם פירצות אבטחה	✔	✔	✔	✔
הגנה מבוססת-Script מפני מתקפות	✔	✔	✔	✔
מערכת אנטי פישינג	✔	✔	✔	✔
הגנת גישה לאינטרנט	✔	✔	✔	✔
HIPS (כולל הגנה מפני נוזקות כופר)	✔	✔	✔	✔
אנטי-ספאם		✔	✔	✔
חומת אש		✔	✔	✔
מפקח הרשת		✔	✔	✔
הגנת מצלמת אינטרנט		✔	✔	✔
הגנה מפני מתקפות רשת		✔	✔	✔
הגנה מפני 'מחשב זומבי' (Botnet)		✔	✔	✔
גלישה ושירותים בנקאיים בטוחים		✔	✔	✔
פרטיות ואבטחה בדפדפן		✔	✔	✔
בקרת הורים		✔	✔	✔
מערכת נגד גניבה		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

שדרוג המוצר

הורדת מתקין ברירת מחדל והחלטת להחליף את המוצר שיופעל, או שברצונך להחליף את המוצר המותקן למוצר עם יותר תכונות אבטחה.

[החלף מוצר במהלך ההתקנה](#).

בטבלה שלהלן מפורטות התכונות הזמינות בכל מוצר ספציפי.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
מנגנון איתור	✔	✔	✔	✔
למידת מכונה מתקדמת	✔	✔	✔	✔
חוסם פירצות אבטחה	✔	✔	✔	✔
הגנה מבוססת-Script מפני מתקפות	✔	✔	✔	✔
מערכת אנטי פישינג	✔	✔	✔	✔
הגנת גישה לאינטרנט	✔	✔	✔	✔
HIPS (כולל הגנה מפני נוזקות כופר)	✔	✔	✔	✔
אנטי-ספאם		✔	✔	✔
חומת אש		✔	✔	✔
מפקח הרשת		✔	✔	✔
הגנת מצלמת אינטרנט		✔	✔	✔
הגנה מפני מתקפות רשת		✔	✔	✔
הגנה מפני 'מחשב זומבי' (Botnet)		✔	✔	✔
גלישה ושירותים בנקאיים בטוחים		✔	✔	✔
פרטיות ואבטחה בדפדפן		✔	✔	✔
בקרת הורים		✔	✔	✔
מערכת נגד גניבה		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

שדרוג לאחור של המינוי

חלון תיבת הדו-שיח מופיע כאשר המינוי ששימש להפעלת מוצר ESET שלך השתנה. המינוי שהשתנה יכול להיות בשימוש רק עם מוצר אחר של ESET הכולל פחות תכונות אבטחה. המוצר שונה אוטומטית כדי למנוע את אובדן ההגנה.

למידע נוסף על מינוי ESET, ראה [שאלות נפוצות בנושא מינוי](#).

בטבלה שלהלן מפורטות התכונות הזמינות בכל מוצר ספציפי.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
מנגנון איתור	✔	✔	✔	✔
למידת מכונה מתקדמת	✔	✔	✔	✔
חוסם פירצות אבטחה	✔	✔	✔	✔
הגנה מבוססת-Script מפני מתקפות	✔	✔	✔	✔
מערכת אנטי פישינג	✔	✔	✔	✔
הגנת גישה לאינטרנט	✔	✔	✔	✔
HIPS (כולל הגנה מפני נוזקות כופר)	✔	✔	✔	✔
אנטי-ספאם		✔	✔	✔
חומת אש		✔	✔	✔
מפקח הרשת		✔	✔	✔
הגנת מצלמת אינטרנט		✔	✔	✔
הגנה מפני מתקפות רשת		✔	✔	✔
הגנה מפני 'מחשב זומבי' (Botnet)		✔	✔	✔
גלישה ושירותים בנקאיים בטוחים		✔	✔	✔
פרטיות ואבטחה בדפדפן		✔	✔	✔
בקרת הורים		✔	✔	✔
מערכת נגד גניבה		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

שדרוג לאחור של מוצר

המוצר שמותקן אצלך עכשיו כולל יותר תכונות אבטחה מהמוצר שאתה עומד להפעיל. התכונות Secure Data ו-Password Manager אינן חלק ממוצר זה. לא תוכל ליצור קבצים מוצפנים.

בטבלה שלהלן מפורטות התכונות הזמינות בכל מוצר ספציפי.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
מנגנון איתור	✔	✔	✔	✔
למידת מכונה מתקדמת	✔	✔	✔	✔
חוסם פירצות אבטחה	✔	✔	✔	✔
הגנה מבוססת-Script מפני מתקפות	✔	✔	✔	✔
מערכת אנטי פישינג	✔	✔	✔	✔
הגנת גישה לאינטרנט	✔	✔	✔	✔
HIPS (כולל הגנה מפני נוזקות כופר)	✔	✔	✔	✔

	ESET Security Ultimate	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
אנטי-ספאם	✔	✔	✔	
חומת אש	✔	✔	✔	
מפקח הרשת	✔	✔	✔	
הגנת מצלמת אינטרנט	✔	✔	✔	
הגנה מפני מתקפות רשת	✔	✔	✔	
הגנה מפני 'מחשב זומבי' (Botnet)	✔	✔	✔	
גלישה ושירותים בנקאיים בטוחים	✔	✔	✔	
פרטיות ואבטחה בדפדפן	✔	✔	✔	
בקרת הורים	✔	✔	✔	
מערכת נגד גניבה	✔	✔	✔	
Password Manager	✔	✔		
ESET Secure Data	✔	✔		
ESET LiveGuard	✔	✔		
VPN	✔			
Identity Protection	✔			

פותר בעיות התקנה

אם מתרחשות בעיות במהלך ההתקנה, אשף ההתקנה מספק פותר בעיות שפותר את הבעיה, אם הדבר אפשרי.

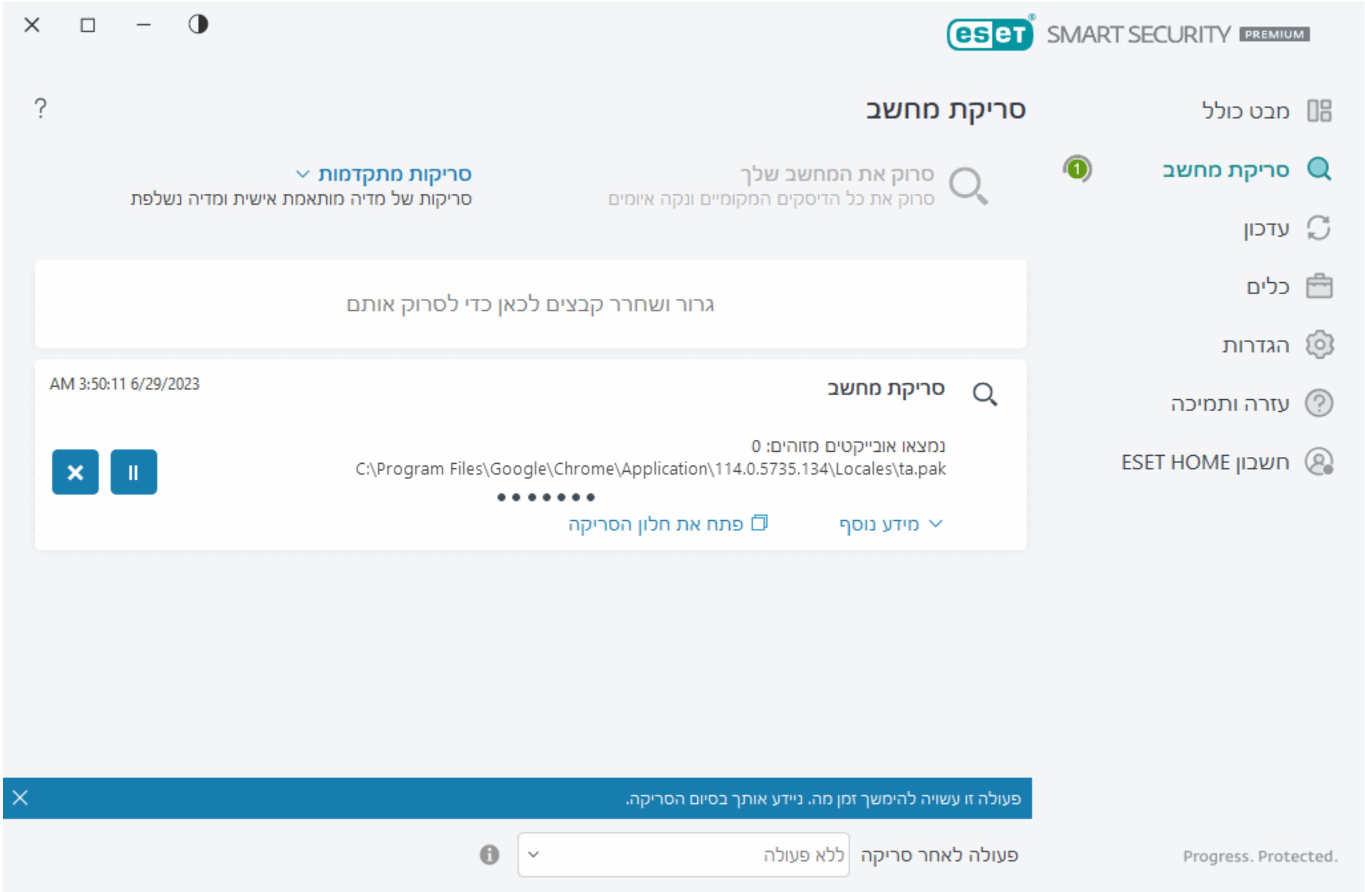
לחץ על **הפעל פותר בעיות** כדי להפעיל את פותר הבעיות. לאחר סיום פעולת פותר הבעיות, בצע את הפעולות המומלצות לפתרון הבעיה.

אם הבעיה נמשכת, עיין ברשימה של שגיאות התקנה נפוצות ופתרונות.

סריקה ראשונה לאחר ההתקנה

לאחר התקנת ESET Smart Security Premium, 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, ראה סריקת מחשב.



שדרוג לגרסה עדכנית יותר

גרסאות חדשות של ESET Smart Security Premium יוצאות כדי לממש שיפורים או לתקן בעיות שלא ניתן לזהותן באמצעות עדכונים אוטומטיים של מודולי התוכנית. ניתן לבצע את השדרוג לגרסה עדכנית יותר 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 **עדכוני תכונות אפליקציה** בהגדרות מתקדמות > **עדכון** > **פרופילים** > **עדכונים**.
2. ידנית, בחלון התוכנית הראשי, בלחיצה על **חפש עדכונים** במקטע **עדכון**.
3. ידנית, על-ידי הורדה והתקנה 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?

עדכון אוטומטי של מוצר מדור קודם

גרסת המוצר של ESET שברשותך אינה נתמכת עוד והמוצר שברשותך שודרג לגרסה העדכנית ביותר.

בעיות התקנה נפוצות

כל גרסה חדשה של המוצרים של ESET כוללת תיקוני באגים ושיפורים רבים. לקוחות קיימים שברשותם מינוי חוקי למוצר של ESET יכולים לשדרג ללא תשלום את המוצר לגרסה העדכנית ביותר של אותו מוצר.

כדי לסיים את ההתקנה:

1. לחץ על **קבל והמשך** כדי לקבל את הסכם הרישיון למשתמש קצה ולאשר את מדיניות הפרטיות. אם אינך מסכים להסכם הרישיון למשתמש קצה, לחץ על **הסר התקנה**. לא ניתן לחזור לגרסה הקודמת.
2. לחץ על **אפשר הכל והמשך** כדי לאפשר את מערכת המשוב של ESET LiveGrid® ואת התכנית לשיפור חוויית הלקוח או לחץ על **המשך** אם אינך מעוניין להשתתף.
3. לאחר הפעלת מוצר ESET החדש באמצעות מפתח הפעלה מופיע הדף 'סקירה כללית'. אם פרטי המינוי שלך לא נמצאו, המשך עם גרסת ניסיון ללא תשלום. אם המינוי שהיה בשימוש במוצר הקודם אינו בתוקף, הפעל את מוצר ESET שלך.
4. נדרשת הפעלה מחדש של ההתקן כדי להשלים את ההתקנה.

ESET Smart Security Premium יותקן

ניתן להציג חלון דו-שיח זה:

- במהלך תהליך ההתקנה לחץ על **המשך** כדי להתקין את ESET Smart Security Premium.
- בעת שינוי מינוי ב-ESET Smart Security Premium - לחץ על **הפעל** כדי לשנות את המינוי ל-ESET Smart Security Premium ולהפעיל אותו.

לפי המינוי שלך ל-ESET, עם האפשרות **שנה מוצר** תוכל לעבור בין המוצרים הביתיים של ESET ל-Windows. ראה איזה מוצר יש לי? לקבלת מידע נוסף.

עבור לקו מוצרים אחר

בהתאם למינוי ESET שלך, אתה יכול לעבור בין המוצרים הביתיים השונים של ESET ל-Windows. ראה איזה מוצר יש לי? לקבלת מידע נוסף.

רישום

רשום את המינוי על-ידי מילוי השדות הכלולים בטופס הרישום ולחיצה על **הפעל**. השדות המסומנים כנדרשים בסוגריים מרובעים הם שדות חובה. במידע זה ייעשה שימוש רק עבור נושאים הנוגעים למינוי ESET שלך.

התקדמות ההפעלה

המתן מספר שניות עד שתהליך ההפעלה יושלם (הזמן הדרוש עשוי להשתנות בהתאם למהירות החיבור לאינטרנט או בהתאם למחשב).

ההפעלה בוצעה בהצלחה

תהליך ההפעלה הושלם. פעל בהתאם להוראות אשף הפעולות לביצוע לאחר ההתקנה כדי לסיים את ההגדרה של ESET Smart Security Premium.

עדכון מודולים יתחיל לאחר מספר שניות. עדכונים סדירים של ESET Smart Security Premium יתחילו מיד.

סריקה התחלתית תתחיל אוטומטית תוך 20 דקות ממועד עדכון המודולים.

> אפשר להפסיק באמצע את תהליך ההפעלה אם ההצעה לא קשורה ל-ESET HOME. היכנס לחשבון ESET HOME שלך או צור חשבון.

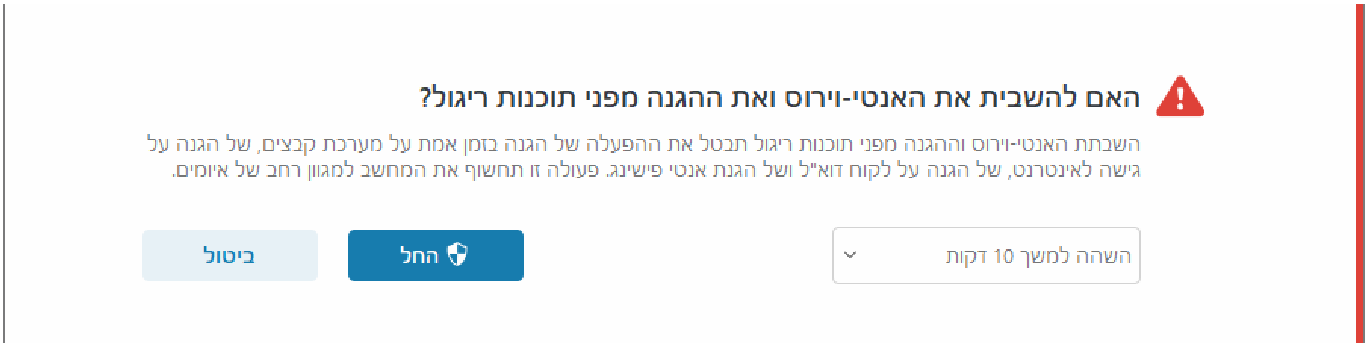
מדריך למשתמש המתחיל

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

סמל מגש מערכת

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

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** מאפשר לך לציין את משך הזמן להשבתת ההגנה.



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 פתיחת הגדרות מתקדמות של ESET Smart Security Premium. כדי לפתוח את ההגדרות המתקדמות מתוך חלון המוצר הראשי, הקש F5 במקלדת או לחץ על **הגדרות** > **הגדרות מתקדמות**.

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

פתח את ESET Smart Security Premium פתיחת חלון התוכנית הראשי של ESET Smart Security Premium.

אתחל פריסת חלון ⯑ איפוס החלון של ESET Smart Security Premium לגודל ולמיקום במסך שנקבעו כברירת מחדל.

מצב צבע ⯑ פתיחת הגדרות ממשק המשתמש שבאמצעותן ניתן לשנות את הצבע של ממשק המשתמש הגרפי.

בדוק אם קיימים עדכונים ⯑ הפעלת מודול או עדכון מוצר כדי לוודא שאתה מוגן. ESET Smart Security Premium בודק אם קיימים עדכונים, באופן אוטומטי ומספר פעמים ביום.

אודות ⯑ מסירת מידע על המערכת, פרטים על גרסת ESET Smart Security Premium המותקנת, המודולים המותקנים של התוכנית ומידע על מערכת ההפעלה ועל משאבי המערכת.

מקשי קיצור במקלדת

לניווט משופר ב-ESET Smart Security Premium, באפשרותך להשתמש במקשי הקיצור הבאים במקלדת:

פעולה	מקשי קיצור במקלדת
פתיחת דפי העזרה	F1
פתיחת הגדרות מתקדמות	F5
ניווט בין פריטי התפריט הנפתח	חץ למעלה/חץ למטה
מעבר אל רכיב ה-GUI הבא בחלון	TAB
מעבר אל רכיב ה-GUI הקודם בחלון	Shift+TAB
סגירת חלון הדו-שיח הפעיל	ESC
הצגת פרטים על מינוי ל-ESET ועל המחשב שלך (פרטים עבור תמיכה טכנית)	Ctrl+U
איפוס חלון המוצר לגודלו ולמיקומו במסך שנקבעו כברירת מחדל	Ctrl+R
ניווט אל הדף הקודם	חץ שמאלה + ALT
ניווט אל הדף הבא	חץ ימינה + ALT
ניווט אל דף הבית	ALT+Home

באפשרותך גם להשתמש בלחצני העכבר 'הקודם' או 'הבא' לצורך ניווט.

פרופילים

מנהל הפרופילים נמצא בשימוש בשני מקומות ב-ESET Smart Security Premium – במקטע **סריקה לפי דרישה** ובמקטע **עדכון**.

סריקת מחשב

ישנם 4 פרופילי סריקה מוגדרים מראש ב-ESET Smart Security Premium:

- **סריקה חכמה** - זהו פרופיל הסריקה המתקדם המוגדר כברירת מחדל. הפרופיל 'סריקה חכמה' משתמש בטכנולוגיה 'אופטימיזציה חכמה', שמחריגה קבצים שסריקה קודמת מצאה שהם נקיים ושלא השתנו מאז סריקה זו. הדבר מאפשר זמני סריקה קצרים יותר עם השפעה מינימלית על אבטחת המערכת.
- **סריקת תפריט הקשר** - אתה יכול להתחיל בסריקה לפי דרישה של כל קובץ מתפריט ההקשר. הפרופיל 'סריקת תפריט הקשר' מאפשר לך להגדיר תצורת סריקה שתהיה בשימוש כשתפעיל את הסריקה באופן זה.

- **סריקה מעמיקה** - הפרופיל 'סריקה מעמיקה' לא משתמש ב'אופטימיזציה חכמה' כברירת מחדל, ולכן אף קובץ לא מוחרג מהסריקה בעת שימוש בפרופיל זה.
- **סריקת מחשב** זהו פרופיל ברירת המחדל המשמש בסריקת מחשב רגילה.

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 הגדרות מתקדמות > **מנגנון איתור** > **סריקת תוכנות זדוניות** > **סריקה לפי דרישה** > **רשימת פרופילים** > **ערוך**. 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, ראה ThreatSense לקבלת תיאור של כל אחד מהפרמטרים של הגדרות הסריקה.

> 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 **תקן את האיתור תמיד**. 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 הגדרות עדכון מאפשר 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.

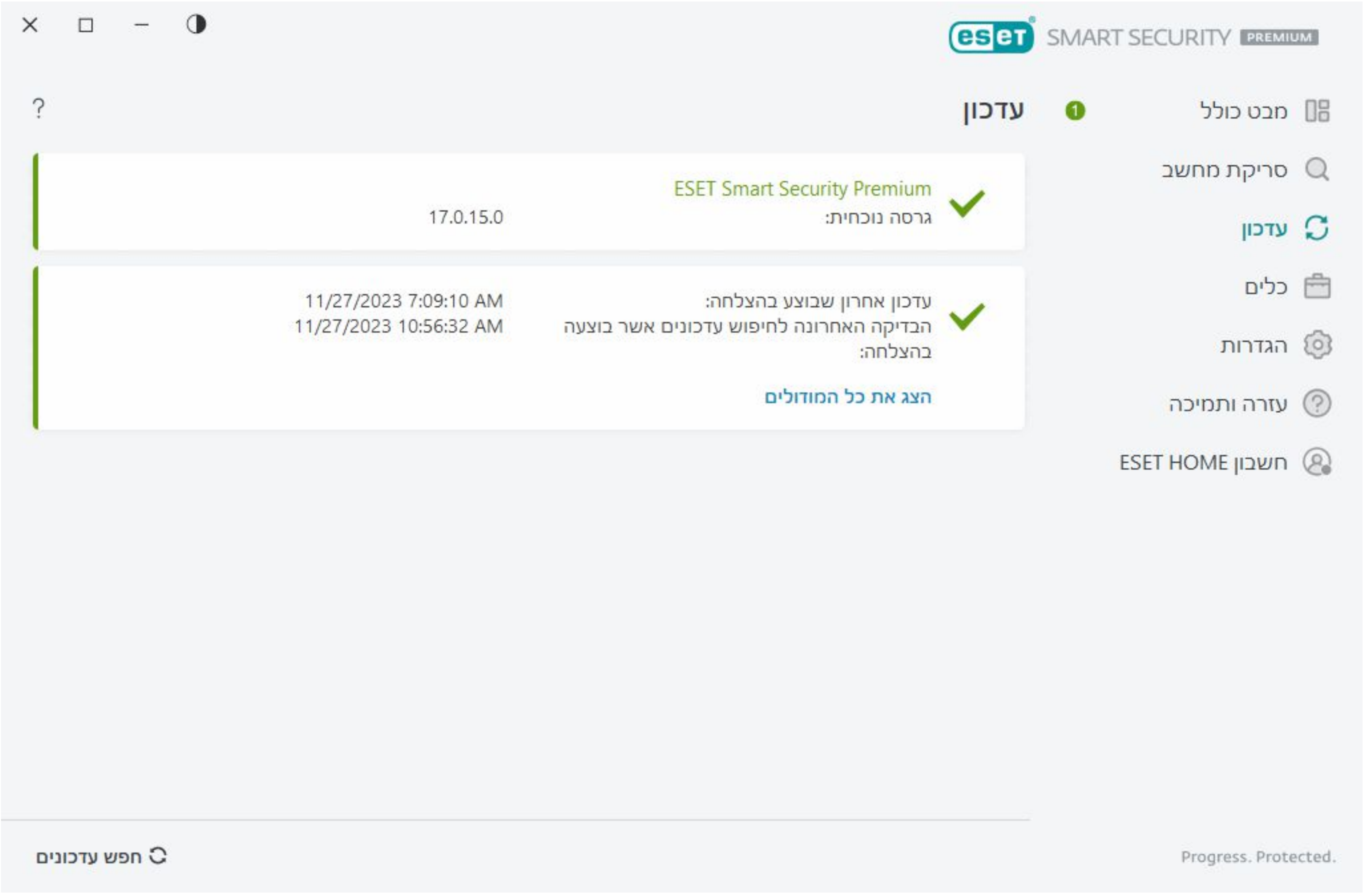
רשימת פרופילים צור פרופילי עדכון חדשים או הסר פרופילי עדכון קיימים.

עדכונים

עדכון סדיר של ESET Smart Security Premium הוא הדרך הטובה ביותר להבטיח את רמת האבטחה המרבית למחשב שלך. מודול העדכון מבטיח שמודולי התוכנית ושרכיבי התוכנית יהיו עדכניים תמיד.

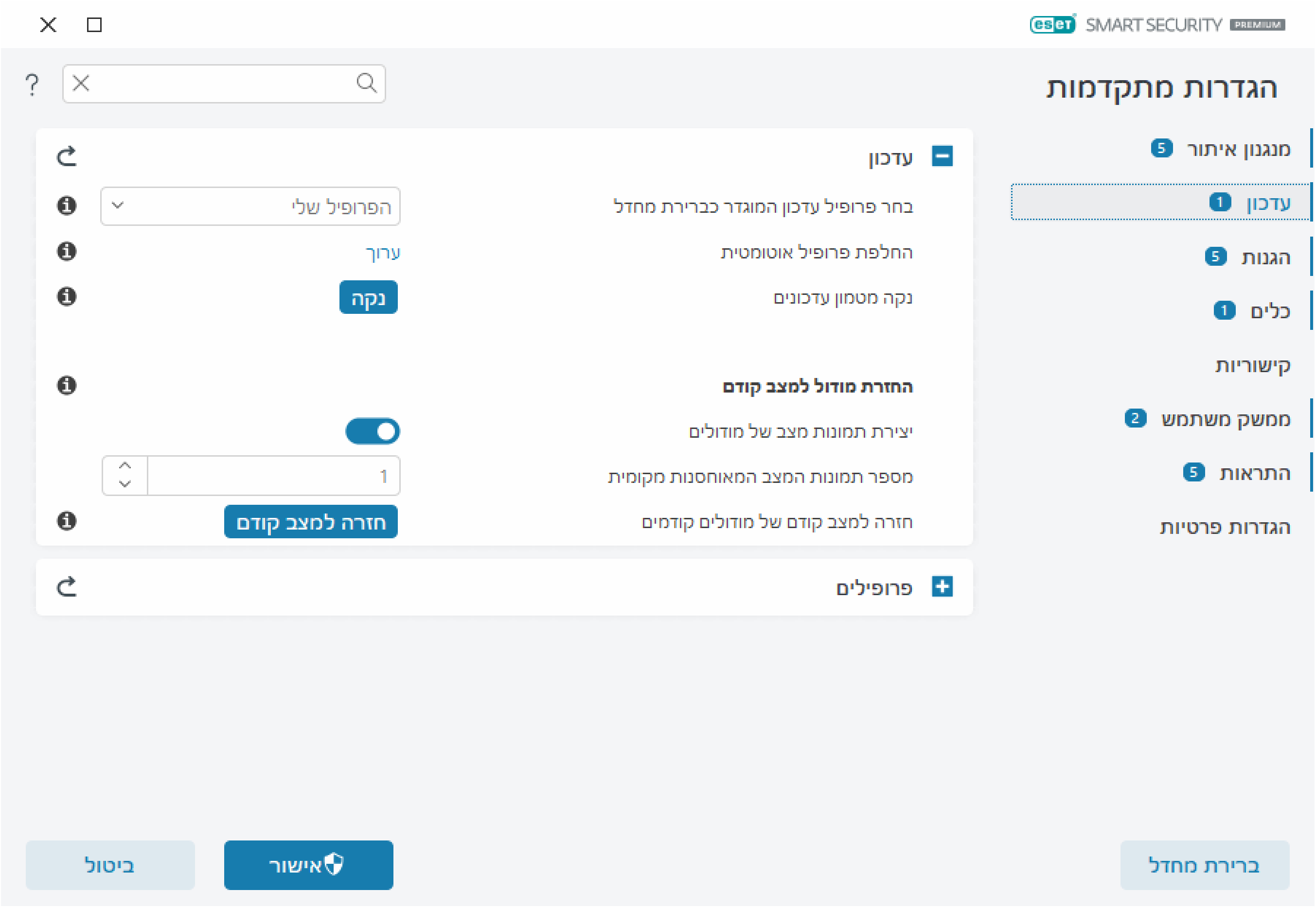
לחיצה על **עדכון** בחלון התוכנית הראשי מאפשרת לך להציג את סטטוס העדכון הנוכחי, לרבות התאריך והשעה של העדכון המוצלח האחרון ומידע אם יש צורך בעדכון.

בנוסף לעדכונים אוטומטיים, באפשרותך ללחוץ על **בדוק אם קיימים עדכונים** כדי להפעיל עדכון ידני.



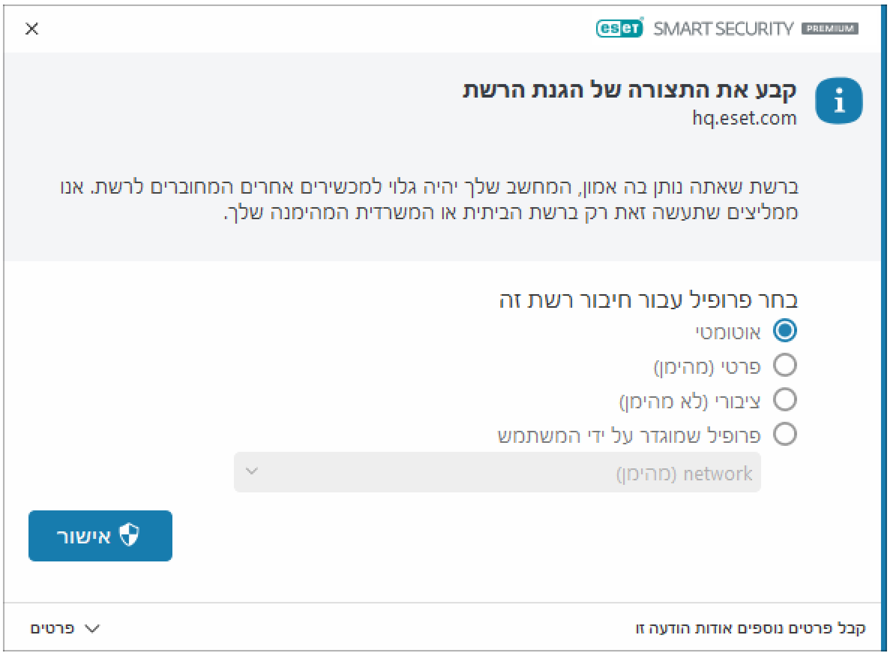
הגדרות מתקדמות > **עדכון** מכילות אפשרויות נוספות של עדכון, כמו מצב עדכון, גישה לשרת Proxy וחיבורי LAN.

אם אתה נתקל בבעיות בעדכון, לחץ על **נקה** כדי לנקות את מטמון העדכון. אם עדיין אינך מצליח לעדכן את המודולים של התכנית, עיין בסעיף פתרון בעיות עבור ההודעה "עדכון המודולים נכשל".



קבע את התצורה של הגנת הרשת

כברירת מחדל, ESET Smart Security Premium משתמש בהגדרות Windows כשמזוהה חיבור רשת חדש. כדי להציג חלון דו-שיח כאשר מזוהה רשת חדשה, שנה את [הקצאת פרופיל הגנת רשת] כך שיהיה **שאל**. הגדרת התצורה של הגנת הרשת תוצג בכל פעם שהמחשב מתחבר לרשת חדשה.



באפשרותך לבחור מבין [הפרופילים הבאים של חיבור רשת]:

אוטומטי - ESET Smart Security Premium יבחר את הפרופיל באופן אוטומטי, בהתבסס על מפעילים שהוגדרו עבור כל פרופיל.

פרטי ⍰ עבור רשת מהימנה (רשת ביתית או משרדית). המחשב שלך וקבצים משותפים המאוחסנים במחשב שלך גלויים למשתמשי רשת אחרים, ומשאבי מערכת נגישים למשתמשים אחרים ברשת (הגישה לקבצים משותפים ולמדפסות מופעלת, תקשורת נכנסת של RPC מופעלת ושיתוף שולחן עבודה מרוחק זמין). אנו ממליצים להשתמש בהגדרה זו בעת גישה לרשת מקומית מאובטחת. פרופיל זה מוקצה באופן אוטומטי לחיבור רשת אם הוא מוגדר כתחום או רשת פרטית ב-Windows.

ציבורי ⍰ עבור רשתות לא מהימנות (רשת ציבורית). קבצים ותיקיות במערכת שלך אינם משותפים עם משתמשים אחרים ואינם גלויים להם ברשת, ושיתוף משאבי מערכת מושבת. אנו ממליצים להשתמש בהגדרה זו בעת גישה לרשתות אלחוטיות. פרופיל זה מוקצה באופן אוטומטי לכל חיבור רשת שאינו מוגדר בתור תחום או רשת פרטית ב-Windows.

פרופיל מוגדר על ידי המשתמש - באפשרותך לבחור פרופיל שיצרת מהתפריט הנפתח. אפשרות זו זמינה רק אם יצרת פרופיל מותאם אישית אחד לפחות.

תצורת רשת שגויה עשויה לחשוף את המחשב שלך לסיכון אבטחה.

הפעל מערכת נגד גניבה

המכשירים האישיים שלנו נתונים בסיכון מתמיד לאובדן או גניבה בנסיעותינו היומיומיות מהבית לעבודה או במקומות ציבוריים אחרים. מערכת נגד גניבה היא תכונה שמרחיבה את האבטחה ברמת המשתמש במקרה של מכשיר שאבד או נגנב. מערכת נגד גניבה תאפשר לך לנטר את השימוש במכשיר החסר ולעקוב אחריו על-ידי איתור לפי כתובת IP ב-ESET HOME, ובכך תסייע לך להחזיר את המכשיר ולהגן על נתונים אישיים.

באמצעות טכנולוגיות מודרניות, כגון חיפוש גיאוגרפי של כתובת IP, צילום תמונות במצלמה אינטרנט, הגנה על חשבון משתמש וניטור מכשיר, מערכת נגד גניבה עשויה לעזור לך ולארגוני אכיפת החוק לאתר את המחשב או המכשיר שאבד או נגנב. תוכל לראות ב-ESET HOME איזו פעילות מתרחשת במחשב או במכשיר שלך.

למידע נוסף על מערכת נגד גניבה ב-ESET HOME, עיין בעזרה המקוונת של ESET HOME.

מערכת נגד גניבה יהיה עשוי שלא לפעול כראוי במחשבים המחוברים לתחומים עקב מגבלות בניהול חשבונות משתמשים.

כדי להפעיל מערכת נגד גניבה ולהגן על המכשיר שלך במקרה של אובדן או גניבה, בחר באחת מהאפשרויות הבאות:

- בחלון התוכנית הראשי > **מבט כולל**, לחץ על **הגדרה** ליד **מערכת נגד גניבה**.
- אם ההודעה "מערכת נגד גניבה זמינה" מופיעה בחלון התוכנית הראשי > מסך **מבט כולל**, לחץ על **הפעל את מערכת נגד גניבה**.
- בחלון התוכנית הראשי, לחץ על **הגדרות** > **כלי אבטחה**. הפעל את המתג **מערכת נגד גניבה** ופעל לפי ההוראות שבמסך.

אם המכשיר אינו מחובר ל-ESET HOME, עליך:
1. להתחבר לחשבון ESET HOME שלך בעת הפעלת מערכת נגד גניבה.
2. הגדר שם מכשיר.

מערכת נגד גניבה אינו תומך ב-Microsoft Windows Home Server.

לאחר הפעלת מערכת נגד גניבה, באפשרותך למטב את אבטחת המכשיר שלך בחלון התוכנית הראשי > **הגדרות** > **כלי אבטחה** > **מערכת נגד גניבה**.

בקרת הורים

אם כבר הפעלת את בקרת ההורים ב-ESET Smart Security Premium, עליך גם לקבוע את תצורת בקרת ההורים עבור כל חשבונות המשתמשים הקשורים.

כאשר בקרת ההורים פעילה וחשבונות המשתמשים לא הוגדרו, ההודעה "בקרת ההורים אינה מוגדרת" תוצג במסך **מבט כולל** של ESET Smart Security Premium. לחץ על **הגדר כללים** ועיין בסעיף בקרת הורים לקבלת מידע נוסף.

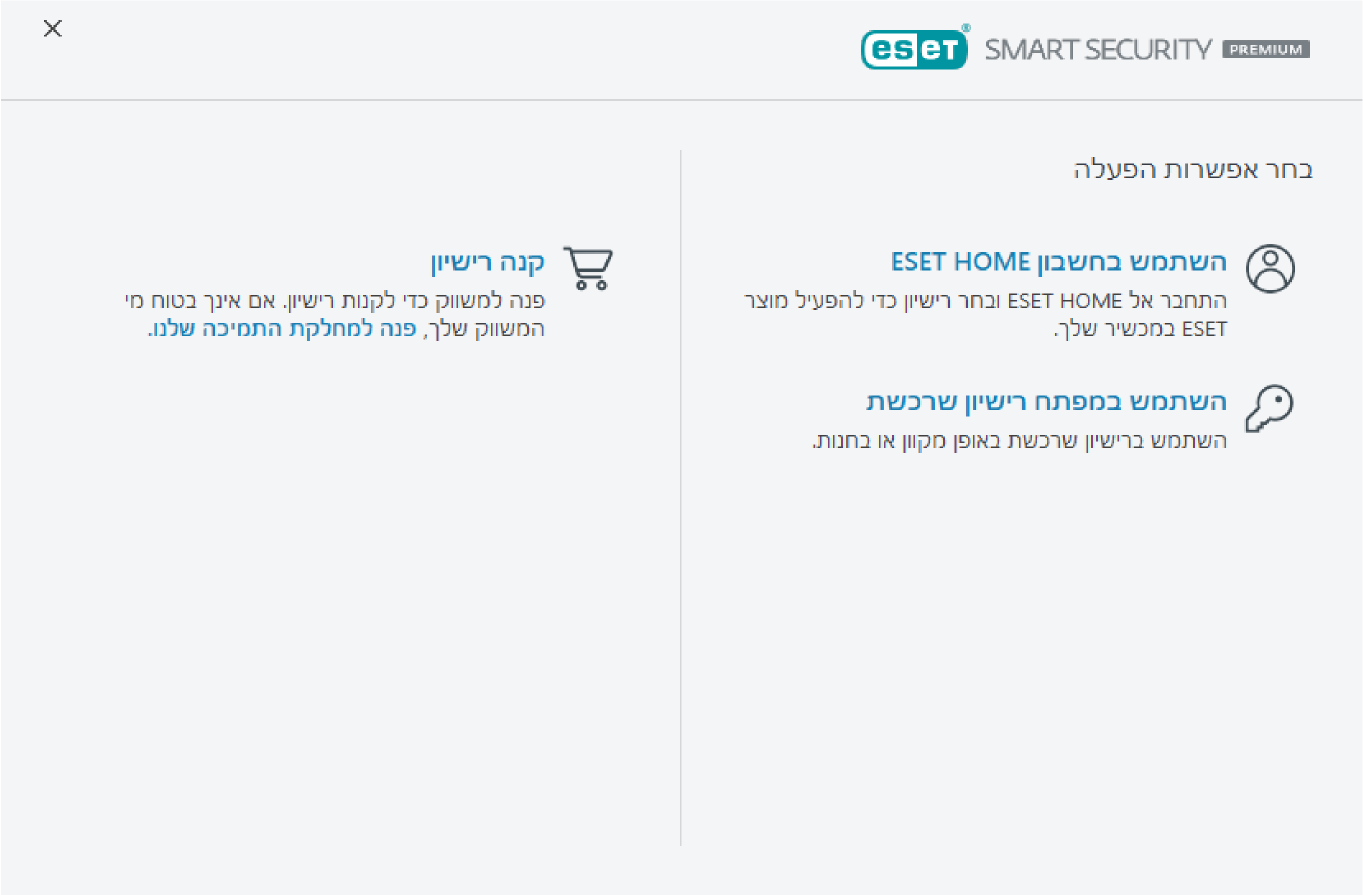
הפעלת מוצר

ישנן מספר שיטות זמינות 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 או שקיבלת הודעת דוא"ל עם פרטי המינוי, הפעל את המוצר על-ידי לחיצה על **השתמש במפתח ההפעלה שרכשת**. את מפתח הרישיון יש להזין בדיוק כפי שסופק כדי שההפעלה תצליח. מפתח ההפעלה הוא מחרוזת ייחודית בתבנית של XXXX-XXXX-XXXX-XXXX-XXXX או XXXX-XXXXXXXX, אשר משמשת לזיהוי בעלי המינוי ולהפעלת המינוי. מפתח המינוי נמצא בדרך כלל בתוך אריזת המוצר או בחלקה האחורי.
- לאחר בחירה באפשרות השתמש בחשבון ESET HOME, תתבקש להתחבר לחשבון ESET HOME שלך.
- אם ברצונך לנסות את ESET Smart Security Premium לפני רכישה, בחר גרסת ניסיון חינם. הזן את כתובת הדואר האלקטרוני שלך ואת ארצך כדי להפעיל את ESET Smart Security Premium לפרק זמן מוגבל. גרסת הניסיון ללא תשלום תישלח אליך בדוא"ל. כל לקוח יכול להפעיל את גרסת הניסיון ללא תשלום פעם אחת בלבד.
- אם אין לך מינוי וברצונך לרכוש מינוי, לחץ על **קנה מינוי**. פעולה זו תעביר אותך לאתר האינטרנט של מפיץ ESET באזורך. המינויים למוצר הביתי של ESET Windows אינם חינמיים.

ניתן לשנות את המינוי למוצר בכל עת. לשם כך, לחץ על **עזרה ותמיכה** > **שנה מינוי** בחלון התוכנית הראשי. תראה את המזהה הציבורי המשמש לזהות את המינוי שלך מול התמיכה של ESET.

הפעלת המוצר נכשלה?



הזנת מפתח ההפעלה שלך במהלך ההפעלה

עדכונים אוטומטיים חשובים לבטיחותך. ESET Smart Security Premium יקבל עדכונים רק לאחר הפעלתו.

בעת הזנת **מפתח הפעלה**, חשוב להקליד אותו בדיוק כפי שהוא נכתב. מפתח ההפעלה שלך הוא מחרוזת ייחודית בתבנית של XXXX-XXXX-XXXX-XXXX-XXXX שמשמשת לזיהוי בעלי המינוי ולהפעלת המינוי.

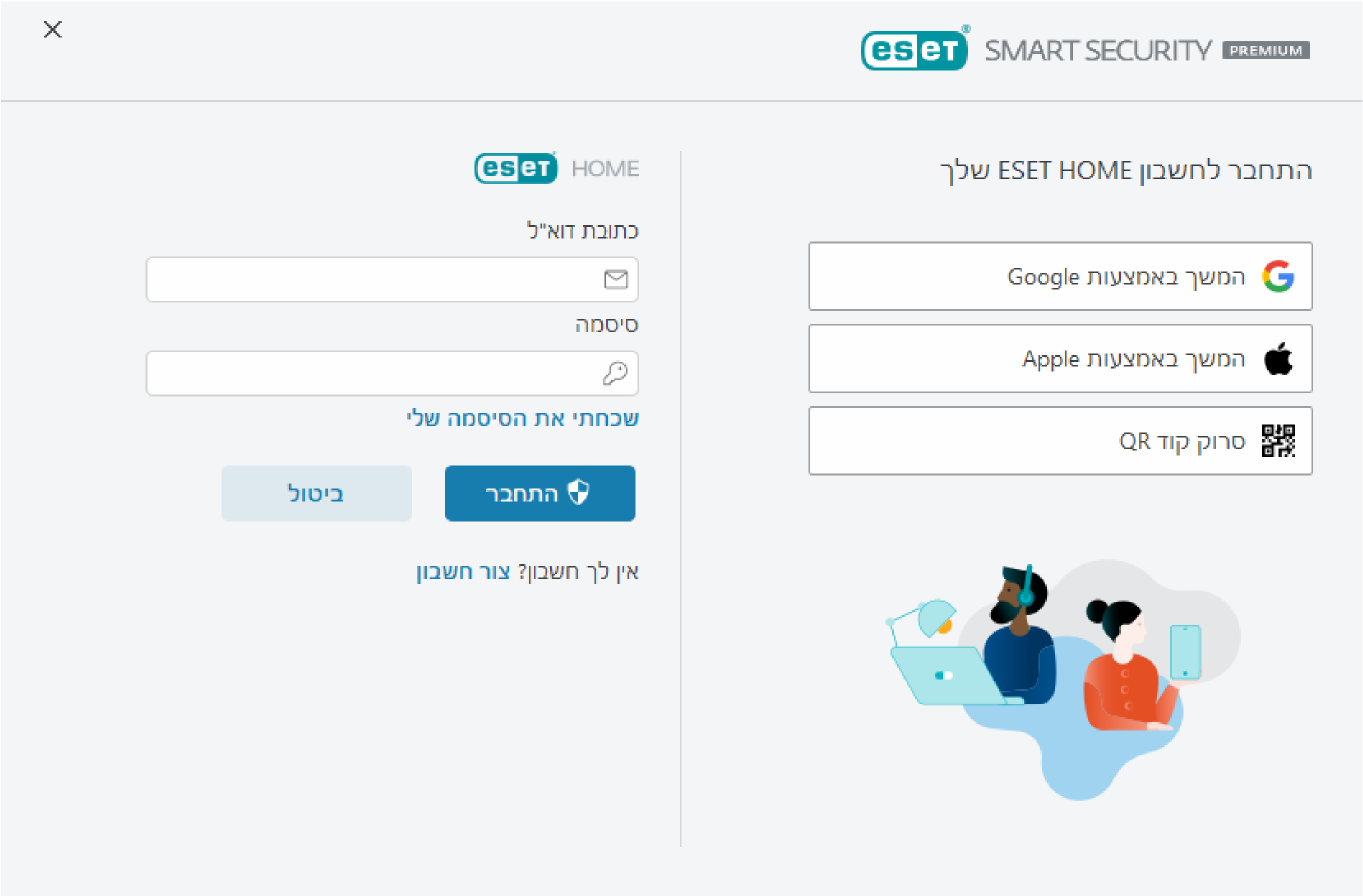
להבטחת הדיוק, מומלץ להעתיק ולהדביק את מפתח ההפעלה מהודעת הדואר האלקטרוני של ההרשמה.

אם לא תזין את מפתח ההפעלה לאחר ההתקנה, המוצר לא יופעל. באפשרותך להפעיל את ESET Smart Security Premium דרך חלון התוכנית הראשי < **עזרה ותמיכה** < **הפעל מינוי**.

המינויים למוצר הביתי של ESET Windows אינם חינמיים.

השתמש ESET HOME בחשבון

חבר את המכשיר שלך אל ESET HOME כדי להציג ולנהל את כל המינויים והמכשירים המופעלים של ESET שברשותך. באפשרותך לחדש, לשדרג ולהאריך את המינוי שלך ולהציג פרטים חשובים של המינוי. בפורטל הניהול או באפליקציה לנייד של ESET HOME, באפשרותך להוסיף מינויים שונים, להוריד מוצרים למכשירים שלך, לבדוק את סטטוס האבטחה של המוצר או לשתף מינוי בדוא"ל. למידע נוסף, בקר בעזרה המקוונת של ESET HOME.



לאחר בחירת האפשרות **השתמש בחשבון ESET HOME** כשיטת הפעלה או בעת התחברות לחשבון ESET HOME במהלך ההתקנה:

1. התחבר לחשבון ESET HOME שלך.

> אם אין לך חשבון ESET HOME, לחץ על **צור חשבון** כדי להירשם או עיין בהוראות בעזרה המקוונת של ESET HOME.
> אם שכחת את הסיסמה, לחץ על **שכחתי את הסיסמה שלי** ובצע את השלבים המוצגים במסך או עיין בהוראות בעזרה המקוונת ESET HOME.

2. הגדר **שם מכשיר** למכשיר שלך שיהיה בשימוש בכל שירותי ESET HOME ולחץ על **המשך**.
3. בחר מינוי להפעלה או הוסף מינוי חדש. לחץ על **המשך** כדי להפעיל את ESET Smart Security Premium.

הפעל גרסת ניסיון ללא תשלום

כדי להפעיל את גרסת הניסיון של ESET Smart Security Premium, הזן כתובת דוא"ל חוקית בשדות **כתובת דוא"ל** ו**אשר כתובת דוא"ל**. לאחר ההפעלה, מינוי ESET שלך ייווצר ויישלח לדוא"ל שלך. כתובת דוא"ל זו תשמש גם להתראות על תפוגת תוקף המוצר ולתקשורת אחרת עם ESET. ניתן להפעיל את גרסת הניסיון ללא תשלום פעם אחת בלבד.

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

מפתח הפעלה ללא תשלום של ESET

מנוי עבור ESET Smart Security Premium אינו בחינם.

מפתח הפעלה של ESET הוא רצף ייחודי של אותיות ומספרים המופרדים בקו מפריד שניתן על-ידי ESET על מנת לאפשר שימוש חוקי ב-ESET Smart Security Premium בהתאם להסכם הרישיון למשתמש קצה. כל משתמש קצה רשאי להשתמש במפתח הפעלה רק אם יש לו את הזכות להשתמש ב-ESET Smart Security Premium בהתאם למספר הרישיונות שהוענקו על-ידי ESET. מפתח ההפעלה הוא סודי, ואין לשתף אותו; עם זאת, אתה יכול לשתף מינוי באמצעות ESET HOME.

יש באינטרנט מקורות שעשויים לספק לך מפתחות הפעלה של ESET "ללא תשלום", אבל זכור:

- לחיצה על פרסומת של "מינוי ESET ללא תשלום" עלולה לחשוף את המחשב או המכשיר שלך לסיכון ועלולה לגרום להדבקתם בתוכנה זדונית. תוכנה זדונית עלולה להיות מוסתרת בתוכן לא רשמי באינטרנט (למשל סרטונים), באתרי אינטרנט המציגים פרסומות כדי להרוויח כסף בהתבסס על הביקורים שלך וכו'. לרוב, מקורות אלה הם מלכודת.
- ESET יכולה להשבית מינויים פיראטיים והיא אף עושה זאת.
- החזקת מפתח הפעלה פיראטי אינה בהתאם לתנאים של הסכם הרישיון למשתמש קצה שאותם עליך לקבל כדי להתקין את ESET Smart Security Premium.
- קנה מינוי של ESET רק דרך ערוצים רשמיים כמו www.eset.com, מפיצים של ESET או משווקים (אל תקנה מינוי מאתרים לא-רשמיים של גורמי צד שלישי כמו eBay או מינוי משותפים מצד שלישי).
- הורדת ESET Smart Security Premium אינה כרוכה בתשלום, אך ההפעלה במהלך ההתקנה דורשת מפתח הפעלה חוקי של ESET (ניתן להוריד את המוצר ולהתקין אותו, אך הוא לא יפעל ללא הפעלה)
- אל תשתף את המינוי שלך באינטרנט או במדיה החברתית (כדי למנוע את הפצתו).

כדי לזהות מינוי 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 Smart Security Premium באמצעות ניסיון ללא תשלום
2. להשתתף בתוכנית הביתא של ESET
3. להתקין את ESET Mobile Security אם אתה משתמש במכשירים ניידים מסוג Android. מוצר זה הוא מוצר מסוג Freemium.

כדי לקבל הנחה / להאריך את הרישיון שלך, חדש את מוצר ESET שברשותך.

ההפעלה נכשלה - תרחישים נפוצים

אם ההפעלה של ESET Smart Security Premium נכשלה, התרחישים הנפוצים ביותר הם:

- מפתח ההפעלה כבר נמצא בשימוש.
- הזנת מפתח הפעלה לא חוקי.
- מידע בטופס ההפעלה חסר או לא חוקי.

- התקשורת עם שרת ההפעלה נכשלה.
- אין חיבור או שהחיבור הושבת לשרתי ההפעלה של ESET.

ודא שהזנת את מפתח ההפעלה המתאים ושהחיבור לאינטרנט פעיל. נסה להפעיל שוב את ESET Smart Security Premium. אם אתה משתמש בחשבון ESET HOME להפעלת המוצר, עיין בניהול מינויים של ESET HOME - עזרה מקוונת.

> אם תקבל שגיאה ספציפית (לדוגמה, מינוי מושעה או מינוי שנעשה בו שימוש יתר), בצע את ההוראות במקטע סטטוס המינוי.

אם עדיין אין באפשרותך לבצע הפעלה ESET Smart Security Premium, פותר הבעיות בהפעלה של ESET יסייע לך בשאלות נפוצות, בשגיאות, בבעיות בהפעלה וברישוי (זמין באנגלית ובמספר שפות אחרות).

סטטוס המינוי

למינוי שלך יכולים להיות סטטוסים שונים. אפשר למצוא את סטטוס המינוי ב-ESET HOME. כדי להוסיף את המינוי לחשבון ESET HOME שלך, ראה הוספת מינוי.

> אם אין לך חשבון ESET HOME, באפשרותך ליצור חשבון ESET HOME חדש.

אם סטטוס המינוי אינו **פעיל**, תוצג שגיאה במהלך ההפעלה או תוצג התראה בחלון התוכנית הראשי.

כדי להשבית את ההתראות על סטטוס המינוי, פתח את הגדרות מתקדמות < **התראות** < **סטטוסים של אפליקציות**. לחץ על **ערוך** לצד **סטטוסים של אפליקציות**, הרחב את **רישוי** ובטל את הבחירה בתיבת הסימון לצד ההתראה שאותה ברצונך להשבית. השבתת ההתראה אינה פותרת את הבעיה.

ראה תיאורים ופתרונות מומלצים לסטטוסים שונים של מינוי בטבלה הבאה:

סטטוס המינוי	תיאור	פתרון
פעיל	המינוי תקף, ואין צורך בביצוע פעולות כלשהן. ניתן להפעיל את ESET Smart Security Premium ובאפשרותך לאתר את פרטי המינוי בחלון התוכנית הראשי < **עזרה ותמיכה**.	
נעשה שימוש יתר	מכשירים רבים יותר משתמשים במינוי זה מכפי שהוא מאפשר. תוצג שגיאת הפעלה.	ראה ההפעלה נכשלה עקב מינוי שנעשה בו שימוש יתר לקבלת מידע נוסף.
מושעה	המינוי שלך הושעה עקב בעיות תשלום. כדי להשתמש במינוי, ודא שפרטי התשלום ב-ESET HOME מעודכנים או פנה למשווק המינוי. שגיאה זו עשויה להיות מוצגת במהלך ההפעלה או בחלון התוכנית הראשי.	מוצר מותקן ▯ אם יש ברשותך חשבון ESET HOME, בהתראה המוצגת בחלון התוכנית הראשי, לחץ על **נהל את המינוי שלך ב-ESET HOME** ובדוק את פרטי התשלום. אחרת, פנה למשווק המינויים שלך. שגיאת הפעלה ▯ אם יש ברשותך חשבון ESET HOME, בחלון שגיאת ההפעלה, לחץ על **פתח את ESET HOME** וסקור את פרטי התשלום. אחרת, פנה למשווק המינויים שלך.

סטטוס המינוי	תיאור	פתרון
התוקף פג	תוקף המינוי שלך פג ואין באפשרותך להשתמש במינוי זה כדי להפעיל את ESET Smart Security Premium. שגיאה זו עשויה להיות מוצגת במהלך ההפעלה או בחלון התוכנית הראשי. אם התקנת כבר את ESET Smart Security Premium, המחשב שלך אינו מוגן ואינו מעודכן.	מוצר מותקן ⍰ בהתראה המוצגת בחלון התוכנית הראשי, לחץ על **חדש מינוי** ופעל בהתאם להנחיות במאמר כיצד לחדש את המינוי שלי?, או לחץ על **הפעל מוצר** ובחר את שיטת ההפעלה. שגיאת הפעלה ⍰ בחלון שגיאת ההפעלה, לחץ על **חדש את המינוי שלך** ופעל בהתאם להנחיות במאמר כיצד לחדש את המינוי שלי?, או הקלד מפתח הפעלה חדש או מחודש ולחץ על **חדש מינוי**.
מבוטל	המינוי שלך בוטל על ידי ESET או על ידי משווק המינוי שלך.	אם נתקלת בשגיאה: מינוי בוטל בחלון התוכנית הראשי או במהלך ההפעלה, והמינוי אמור לפעול כראוי, פנה למשווק המינויים שלך.

ההפעלה נכשלה עקב מינוי שנעשה בו שימוש יתר

בעיה

- ייתכן שנעשה שימוש יתר במינוי שלך או שהוא מנוצל לרעה
- ההפעלה נכשלה עקב מינוי שנעשה בו שימוש יתר

פתרון

מינוי זה משמש מכשירים רבים יותר מכפי שהוא מאפשר. ייתכן שנפלת קורבן לפיראטיות תוכנה או לזיוף. לא ניתן להשתמש במינוי כדי להפעיל מוצרי ESET נוספים. באפשרותך לפתור בעיה זו ישירות אם אתה רשאי לנהל את המינוי בחשבון ESET HOME שלך או אם רכשת את המינוי ממקור לגיטימי. אם עדיין אין לך חשבון, צור חשבון.

אם אתה בעל המינוי ולא התבקשת להזין את כתובת הדוא"ל שלך:

1. כדי לנהל את מינוי ESET שלך, פתח דפדפן אינטרנט ועבור אל https://home.eset.com. גש אל ESET License Manager והסר או השבת עמדות. למידע נוסף, ראה מה לעשות במקרה של מינוי שנעשה בו שימוש יתר.
2. כדי לזהות מינוי פיראטי של ESET ולדווח עליו, בקר במאמר 'זיהוי' של מינויים פיראטיים של ESET ודיווח עליהם' לקבלת הוראות.
3. אם אינך בטוח, לחץ על '**הקודם**' ושלח דוא"ל לתמיכה הטכנית של ESET.

אם אינך הבעלים של המינוי, פנה לבעלים של המינוי עם מידע על כך שאין לך אפשרות להפעיל את מוצר ESET מכיוון שנעשה שימוש יתר במינוי. הבעלים יכול לפתור את הבעיה בפורטל ESET HOME.

אם התבקשת לאשר את הדוא"ל שלך (מקרים מסוימים בלבד), הזן את כתובת הדוא"ל ששימשה במקור לרכישה או להפעלה של ESET Smart Security Premium.

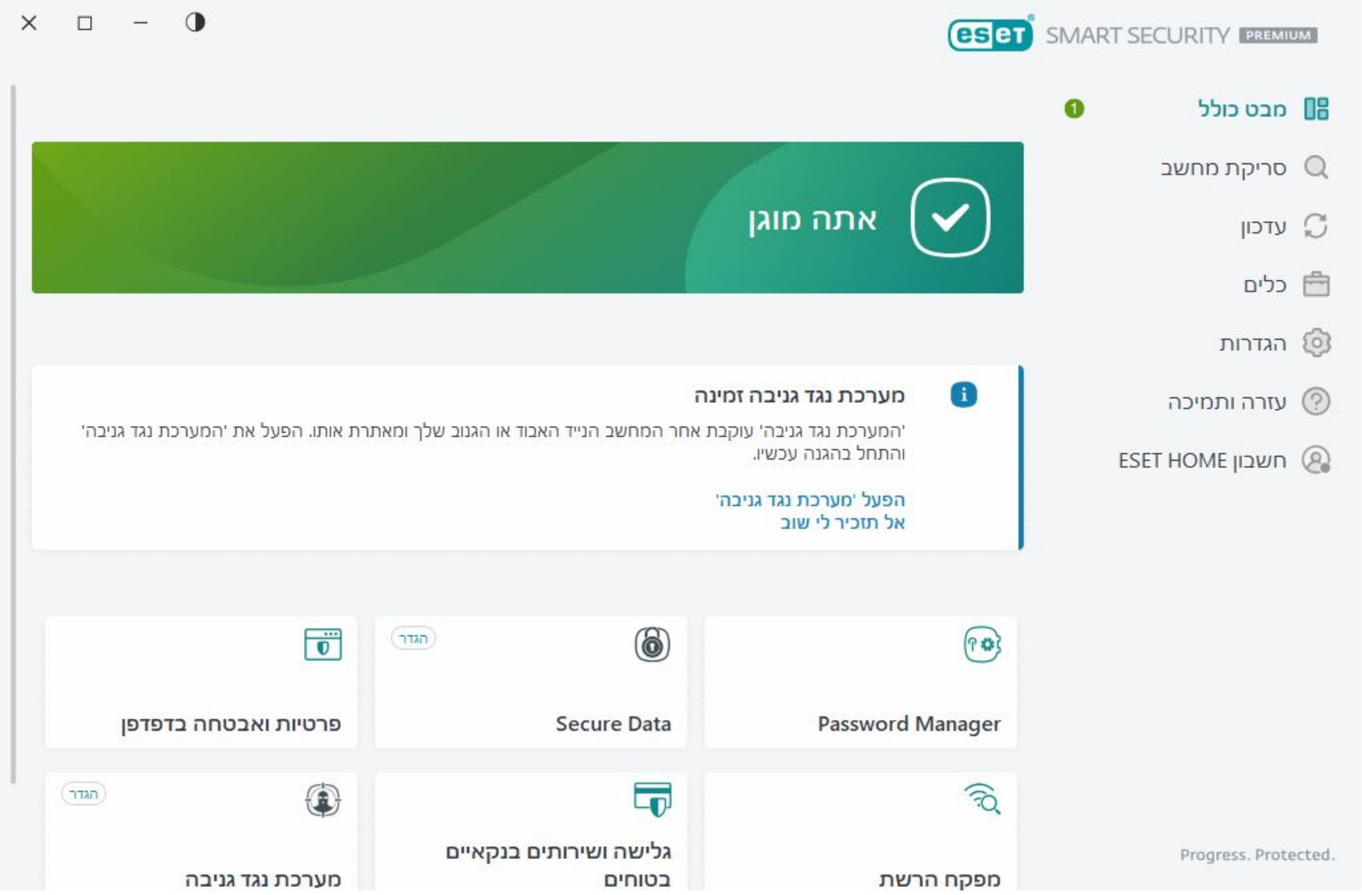
עבודה עם ESET Smart Security Premium

חלון התוכנית הראשי של ESET Smart Security Premium מפוצל לשני מקטעים עיקריים. החלון הראשי מימין מציג מידע התואם לאפשרות שנבחרה בתפריט הראשי שמשמאל.

> **הנחיות מאוירות**
>
> ראה [פתיחת חלון התוכנית הראשי של מוצרי ESET עבור Windows](#) לקבלת הנחיות מאוירות הזמינות באנגלית ובמספר שפות אחרות.

ניתן לבחור את ערכת הצבעים של הממשק של ESET Smart Security Premium GUI בפינה הימנית העליונה של חלון התוכנית הראשי. לחץ על סמל **ערכת הצבעים** (הסמל משתנה בהתאם לסכמת הצבעים שנבחרה כעת) לצד הסמל **מזער** ובחר את ערכת הצבעים מהתפריט הנפתח:

- **זהה לצבע המערכת** – בחר באפשרות זו כדי להגדיר את ערכת הצבעים של ESET Smart Security Premium בהתאם להגדרות מערכת ההפעלה.
- **כהה** – ערכת הצבעים של ESET Smart Security Premium תהיה כהה (מצב כהה).
- **בהיר** – ערכת הצבעים של ESET Smart Security Premium תהיה רגילה ובהירה.



אפשרויות בתפריט הראשי:

[מבט כולל](#) – מספק מידע על סטטוס ההגנה של ESET Smart Security Premium.

[סריקת מחשב](#) – הגדרה והפעלה של סריקת המחשב או יצירת סריקה מותאמת אישית.

[עדכון](#) – הצגת מידע על עדכונים של המודולים ומנגנון האיתור.

כלים - מספק גישה אל מפקח הרשת ותכונות נוספות שעוזרות לפשט את הניהול של תוכניות ומציעות אפשרויות נוספות למשתמשים מתקדמים.

הגדרה - מספק אפשרויות תצורה עבור תכונות ההגנה של ESET Smart Security Premium (הגנת מחשב, הגנת אינטרנט, הגנת רשת וכלי אבטחה) וגישה להגדרות המתקדמות.

עזרה ותמיכה הצגת מידע על המינוי שלך, מוצר ESET שמותקן וקישורים אל עזרה מקוונת, מאגר הידע של ESET ואל התמיכה הטכנית.

חשבון ESET HOME – חבר את המכשיר שלך אל ESET HOME או סקור את סטטוס החיבור של חשבון ESET HOME. השתמש ב-ESET HOME כדי להציג ולנהל את הגדרות מערכת נגד גניבה שלך ואת המינויים והמכשירים שלך שבהם מופעל ESET.

מבט כולל

החלון **מבט כולל** מציג מידע אודות ההגנה הנוכחית של המחשב שלך יחד עם קישורים מהירים לתכונות האבטחה ב-ESET Smart Security Premium.

החלון **מבט כולל** מציג התראות עם מידע מפורט ופתרונות מומלצים לשיפור האבטחה של ESET Smart Security Premium, להפעלת תכונות נוספות או להבטחת הגנה מרבית. אם קיימות התראות נוספות, לחץ על **X התראות נוספות** כדי להרחיב את כל ההתראות.

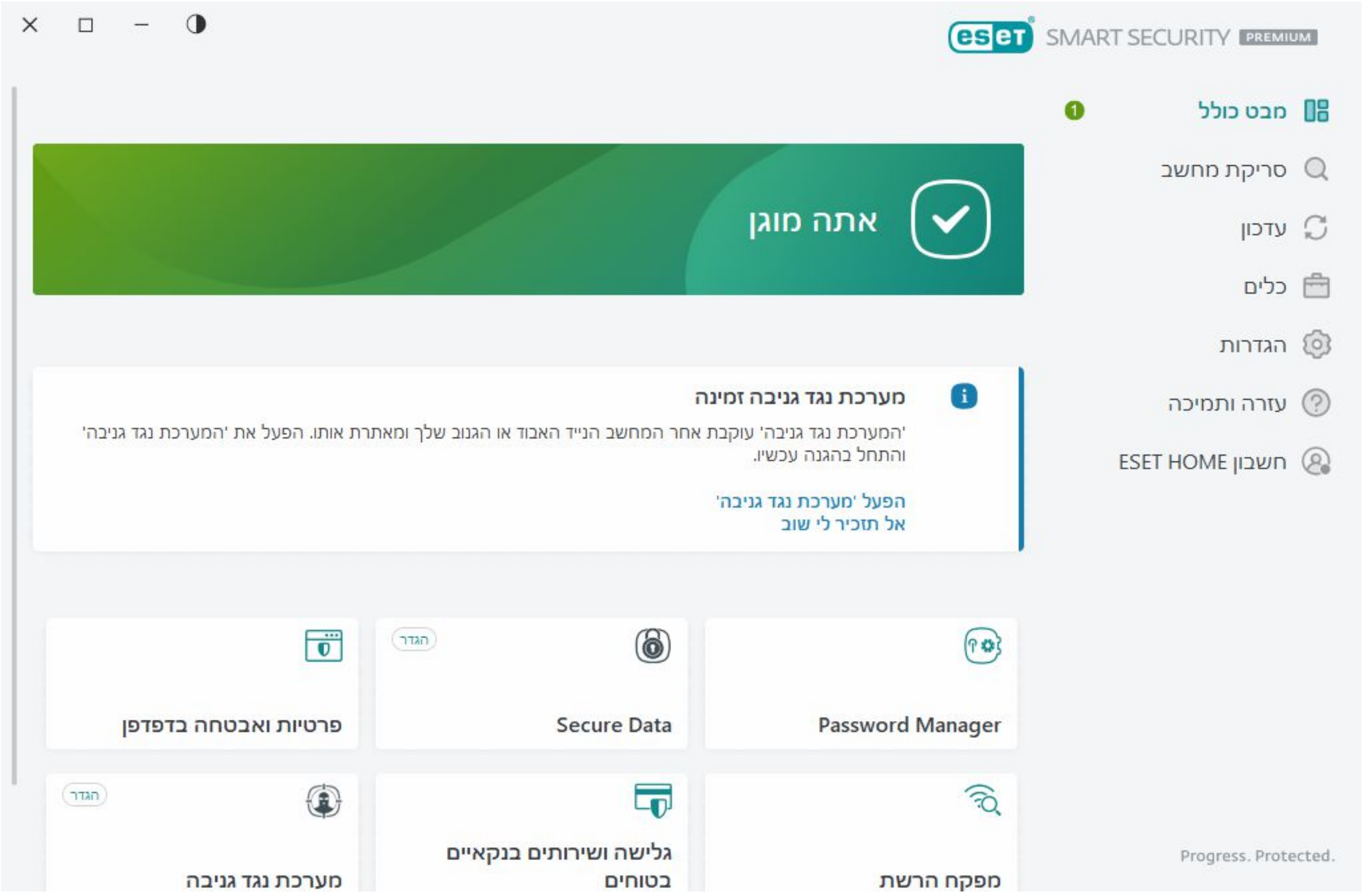
Password Manager - פותח הוראות כיצד להגדיר את Password Manager.

מפקח הרשת - בדוק את אבטחת הרשת

Secure Data - פותח את כלי אבטחה. לחץ על המתג שליד **Secure Data** כדי להפעיל אותו. אם כבר הפעלת את Secure Data, הקישור המהיר פותח את הדף Secure Data.

הגנה על שירותים בנקאיים ותשלומים מקוונים - מפעיל את הדפדפן, מוגדר כברירת מחדל ב-Windows, במצב מאובטח.

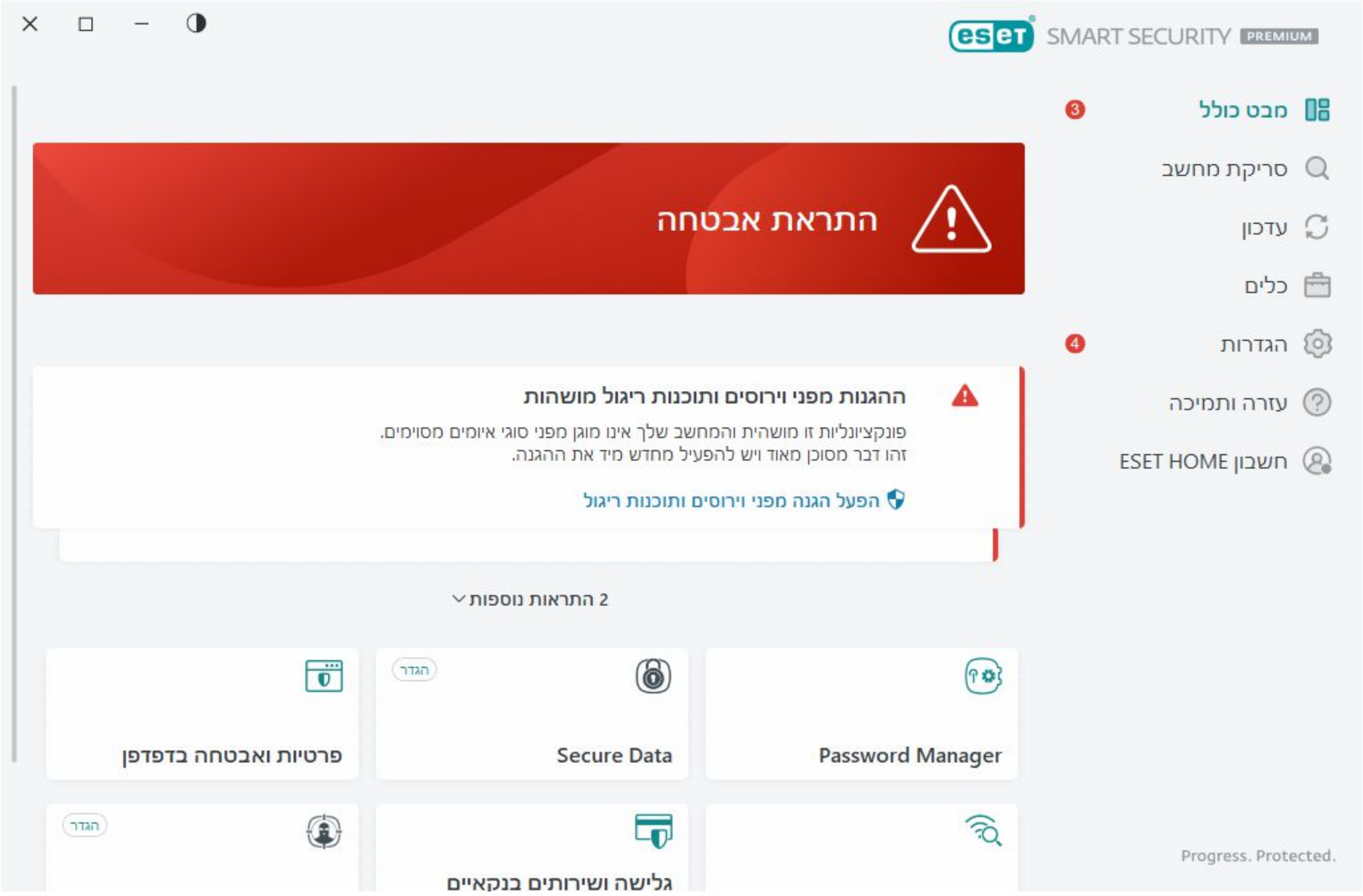
מערכת נגד גניבהמתחיל את מערכת נגד גניבה ההתקנה. אם כבר הגדרת את מערכת נגד גניבה, הקישור המהיר פותח את הדף מערכת נגד גניבה.



הסמל הירוק והסטטוס הירוק **אתה מוגן** 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 כהתראה בחלון **מבט כולל**. כדי לשנות את הסטטוס של מודולים בודדים, לחץ על **הגדרות** ובחר את המודול הרצוי.



הסמל האדום והסטטוס האדום **התראת אבטחה** מציינים בעיות קריטיות.
סטטוס זה יכול להיות מוצג מסיבות שונות, למשל:

- **המוצר לא הופעל** או **שתוקף המינוי פג** – מצב זה מיוצג על ידי סמל סטטוס הגנה אדום. עדכון התוכנית אינו מתאפשר אחרי שתוקף המינוי פג. פעל בהתאם להוראות שבחלון ההתראות כדי לחדש את המינוי.

- **מנגנון האיתור אינו עדכני** – שגיאה זו תופיע לאחר מספר ניסיונות לא מוצלחים לעדכן את מנגנון האיתור. מומלץ שתבדוק את הגדרות העדכון. הסיבה הנפוצה ביותר לשגיאה זו היא [נתוני אימות](#) שלא הוזנו כהלכה או [הגדרות חיבור](#) שגויות.

- **הגנה בזמן אמת על מערכת קבצים מושבתת** – הגנה בזמן אמת הושבתה על ידי המשתמש. המחשב שלך אינו מוגן מפני איומים. לחץ על **אפשר הגנה בזמן אמת על מערכת קבצים** כדי להפעיל מחדש פונקציונליות זו.
- **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**.

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

- **אזהרת מיטוב של מערכת נגד גניבה** – מכשיר זה אינו ממוטב עבור מערכת נגד גניבה. לדוגמה, ייתכן שלא ניתן יהיה ליצור במחשבך חשבון פנטום (תכונת אבטחה המופעלת אוטומטית כאשר אתה מסמן מכשיר כחסר). באפשרותך ליצור חשבון פנטום בעת השימוש בתכונת ה[מיטוב](#) בממשק האינטרנט של מערכת נגד גניבה.

- **מצב משחק מופעל** – הפעלת [מצב משחק](#) מהווה סיכון אבטחה פוטנציאלי. הפעלת תכונה זו משביתה את כל

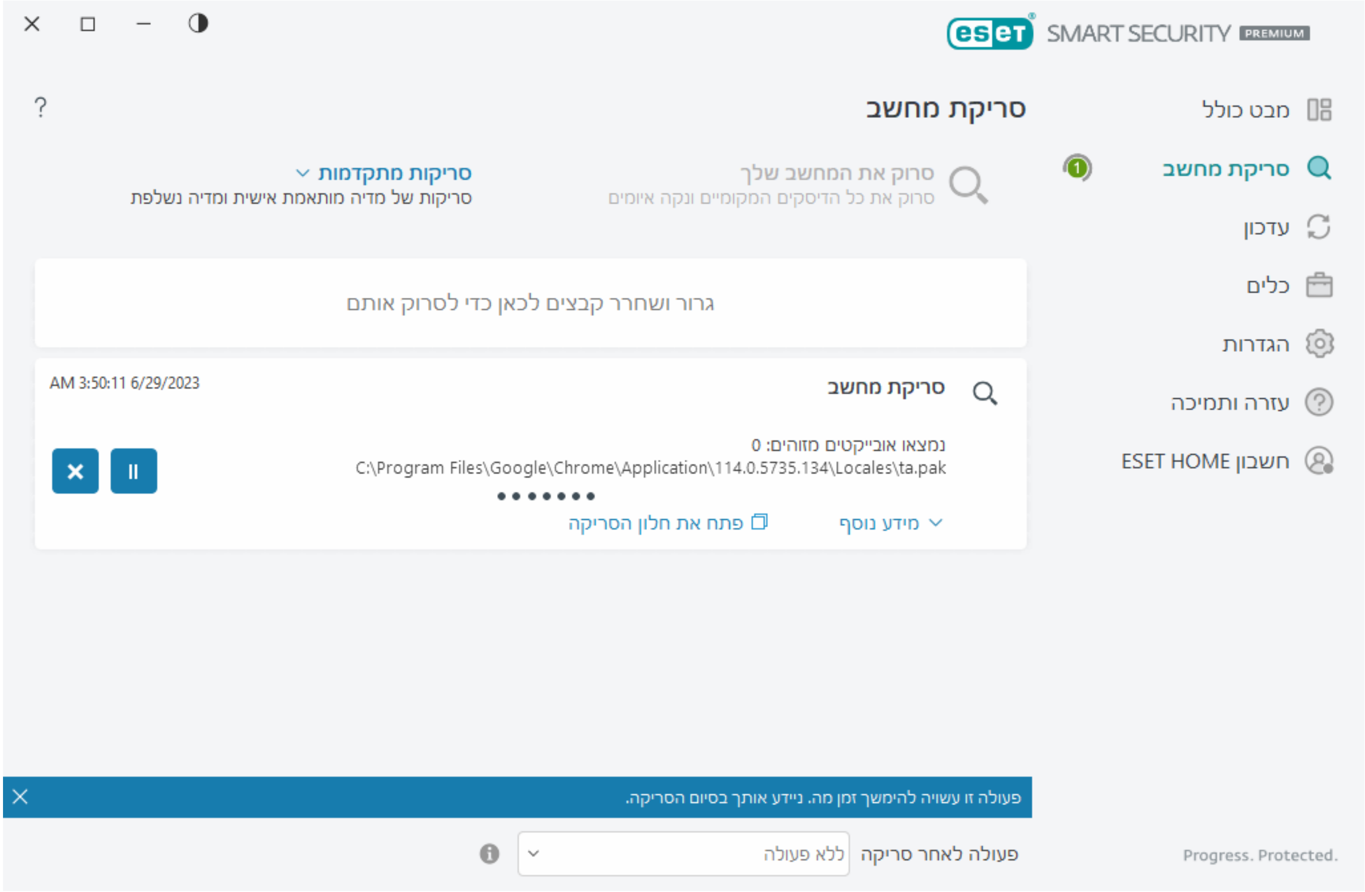
החלונות של התראות\הודעות ועוצרת את כל המשימות המתוזמנות.

- **תוקף המינוי שלך יפוג בקרוב/תוקף המינוי יפוג היום** מצב זה מיוצג על ידי סמל סטטוס ההגנה המציג סימן קריאה לצד שעון המערכת. אחרי שתוקף המינוי שלך 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.

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 סוגים זמינים של **סריקת מחשב**. האפשרות **סרוק את המחשב שלך** סורקת במהירות את המערכת ללא ציון פרמטרי הסריקה. **סריקה מותאמת אישית** (תחת 'סריקה מתקדמת') מאפשרת לך לבחור מתוך פרופילי סריקה שהוגדרו מראש, אשר תוכננו לטפל במיקומים מסוימים, ולבחור יעדי סריקה ספציפיים.

ראה התקדמות הסריקה לקבלת מידע נוסף על תהליך הסריקה.

כברירת מחדל, ESET Smart Security Premium מנסה לנקות או להסיר באופן אוטומטי אובייקטים מזוהים שנמצאו במהלך סריקת המחשב. במקרים מסוימים, אם לא ניתן לבצע פעולה, תקבל התראה אינטראקטיבית ועליך לבחור פעולת ניקוי (לדוגמה, הסרה או התעלמות). כדי לשנות את רמת הניקוי ולקבל מידע מפורט יותר, ראה ניקוי. לעיון בסריקות קודמות, ראה רשומות יומן.

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 מסירה 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 ושיטות הסריקה. היתרון של **סריקה מותאמת אישית** הוא שבאפשרותך 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 התוכן שלו 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.

התפריט הנפתח **פעולה לאחר הסריקה** מאפשר לך להגדיר פעולה שתבוצע באופן אוטומטי לאחר סיום הסריקה:

- **ללא פעולה** – לאחר סיום הסריקה לא תתבצע כל פעולה.
- **כיבוי** – המחשב יכבה לאחר סיום הסריקה.
- **הפעלה מחדש בעת הצורך** – המחשב מבצע הפעלה מחדש רק אם הדבר נדרש כדי להשלים ניקוי של איומים שאותרו.
- **אתחול מחדש** – סגירת כל התוכניות הפתוחות והפעלה מחדש של המחשב לאחר סיום הסריקה.
- **כפה הפעלה מחדש במידת הצורך** – המחשב מבצע הפעלה מחדש רק אם הדבר נדרש כדי להשלים ניקוי של איומים שאותרו.

- **כפה אתחול מחדש** – כופה סגירה של כל התוכניות הפתוחות מבלי להמתין לאינטראקציה עם המשתמש ומפעיל מחדש את 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.

> הפעולות **שינה** או **מצב שינה** זמינות בהתאם להגדרות צריכת החשמל והשינה במערכת ההפעלה במחשב שלך או יכולות המחשב השולחני או הנייד שלך. זכור שמחשב ישן הוא עדיין מחשב פועל. הוא עדיין מפעיל פונקציות בסיסיות וצורך חשמל כשהמחשב פועל על סוללה. כדי לשמר את חיי הסוללה, למשל כשאתה מחוץ למשרד, אנו ממליצים להשתמש באפשרות 'מצב שינה'.

הפעולה הנבחרת תתחיל לאחר סיום כל הסריקות הפועלות. כאשר תבחר באפשרות **כיבוי** או **אתחול מחדש**, חלון דו-שיח לאישור יציג ספירה לאחור של 30 שניות (לחץ על **ביטול** כדי לבטל את הפעולה המבוקשת).

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

מפעיל סריקה מותאמת אישית

באפשרותך להשתמש בסריקה מותאמת אישית כדי לסרוק את זיכרון ההפעלה, הרשת או חלקים מסוימים בדיסק במקום לסרוק את כל הדיסק. לשם כך, לחץ על **סריקות מתקדמות** > **סריקה מותאמת אישית** ובחר יעדים ספציפיים ממבנה התיקיות (העץ).

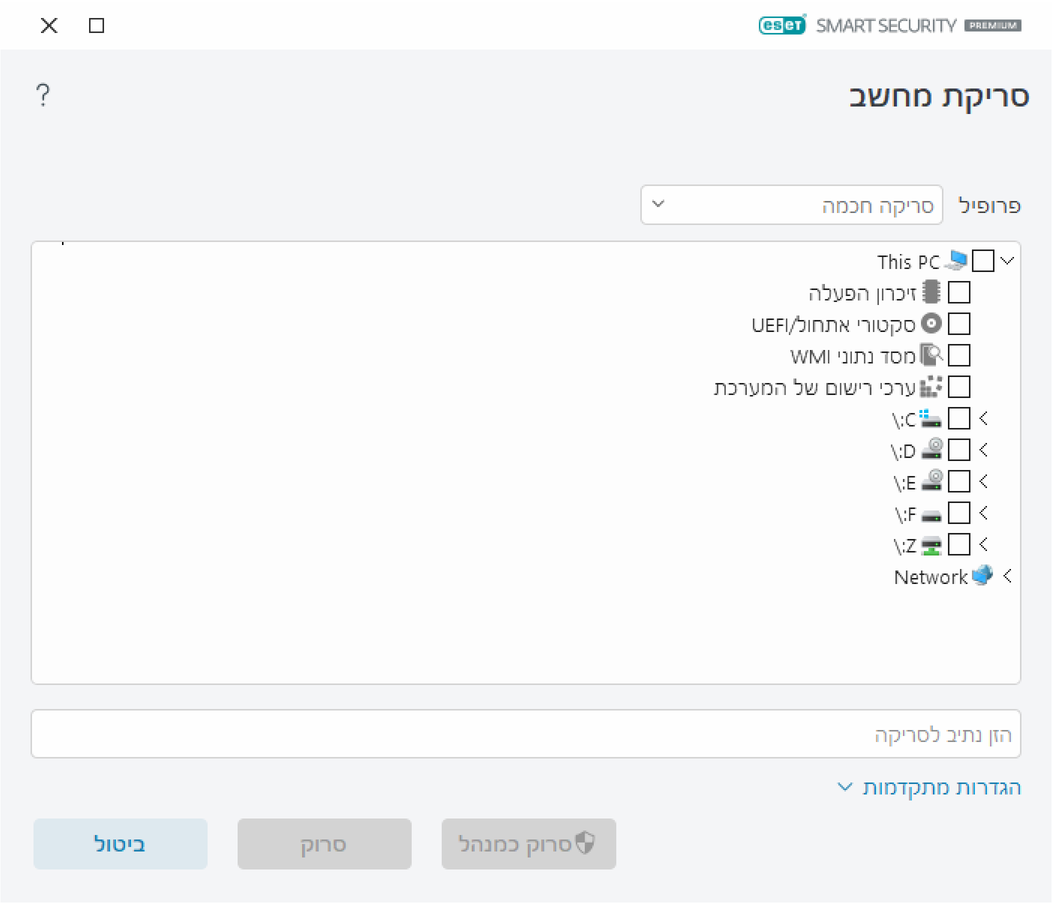
בתפריט הנפתח **פרופיל** תוכל לבחור פרופיל שישמש לסריקת יעדים ספציפיים. פרופיל ברירת המחדל הוא **סריקה חכמה**. ישנם עוד שלושה פרופילי סריקה מוגדרים מראש, המכונים **סריקה מעמיקה**, **סריקת תפריט הקשר** ו**סריקת מחשב**. פרופילי הסריקה הללו משתמשים בThreatSense. האפשרויות הזמינות מתוארות בהגדרות מתקדמות > **מנגנון איתור** > **סריקת תוכנות זדוניות** > **סריקה לפי דרישה** > ThreatSense.

מבנה (עץ) התיקיות מכיל גם יעדי סריקה ספציפיים.

- **זיכרון הפעלה** – סריקת כל התהליכים והנתונים הנמצאים כעת בשימוש של זיכרון ההפעלה.
- **סקטורי אתחול/UEFI** – סריקת סקטורי האתחול ו-UEFI לאיתור תוכנות זדוניות. קרא מידע נוסף על סורק UEFI במילון.
- **מסד נתוני WMI** – סריקה של כלל מסד נתוני Windows Media Instrumentation (WMI), של כל מרחבי השמות, של מופעי המחלקות ושל כל המאפיינים. בנוסף, מתבצע חיפוש של הפניות לקבצים נגועים או של תוכנות זדוניות המוטבעות כנתונים.
- **ערכי רישום של המערכת** – סריקה של כלל ערכי הרישום של המערכת, של כל המפתחות ושל כל מפתחות המשנה. בנוסף, מתבצע חיפוש של הפניות לקבצים נגועים או של תוכנות זדוניות המוטבעות כנתונים. בעת ניקוי האיתורים, ההפניות נשארות ברישום כדי לוודא שנתונים חשובים לא יאבדו.

כדי לנווט במהירות ליעד סריקה (קובץ או תיקייה), הקלד את הנתיב בשדה הטקסט שמתחת למבנה העץ. הנתיב הוא תלוי-רישיות. כדי לכלול את היעד בסריקה, בחר בתיבת הסימון שלו במבנה העץ.

> **כיצד לתזמן סריקת מחשב שבועית**
> כדי לתזמן סריקה קבועה, ראה כיצד לתזמן סריקת מחשב שבועית.



אפשר להגדיר את תצורת הפרמטרים של הניקוי לסריקה דרך הגדרות מתקדמות > **מנגנון איתור** > **סריקת תוכנות זדוניות** > **סריקה לפי דרישה** > **ThreatSense** > **ניקוי**. כדי להפעיל סריקה ללא פעולת ניקוי, לחץ על **הגדרות מתקדמות** ובחר **סרוק ללא ניקוי**. היסטוריית הסריקות נשמרת ביומן הסריקות.

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

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.

> 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.

> 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. פרטים נוספים ניתן למצוא במאמר על מאגר הידע שלנו.

> **כיצד לתזמן סריקת מחשב שבועית**
> כדי לתזמן סריקה קבועה, ראה כיצד לתזמן סריקת מחשב שבועית.

התקדמות סריקה - סרגל ההתקדמות מציג את מצב הסריקה שפועלת.

יעד – שם האובייקט הנסרק כעת ומיקומו.

נמצאו אובייקטים מזוהים – הצגת מספר הקבצים שנסרקו, האיומים שנמצאו והאיומים שנוקו במהלך סריקה.

לחץ על 'מידע נוסף' כדי להציג את המידע הבא:

- **משתמש** - שם חשבון המשתמש שהחל את הסריקה.
- **אובייקטים שנסרקו** - מספר האובייקטים שכבר נסרקו.
- **משך** - משך הזמן שחלף.

סמל השהיה - משהה את הסריקה.

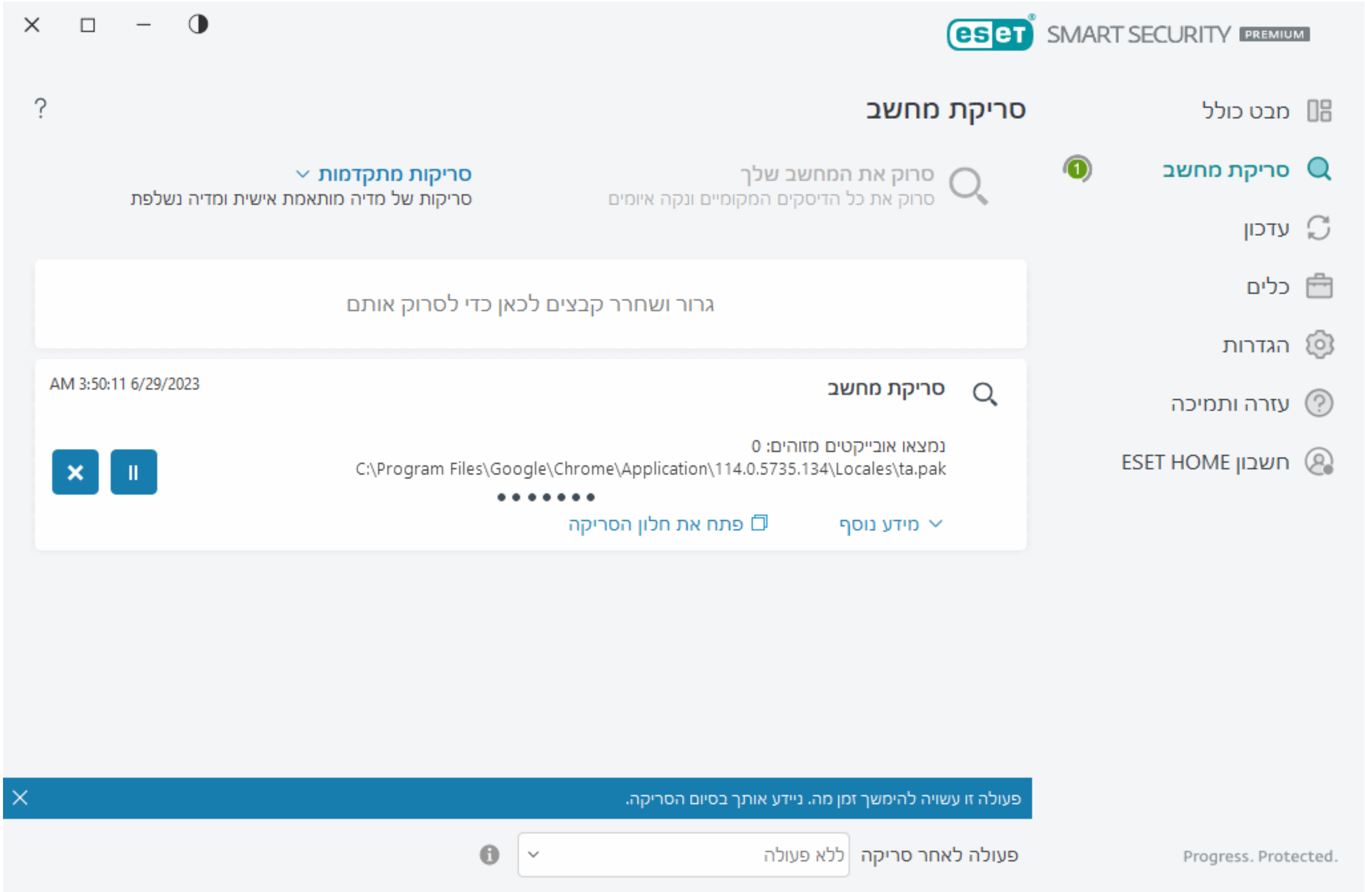
סמל המשך – אפשרות זו מופיעה כאשר התקדמות הסריקה מושהית. לחץ על הסמל כדי להמשיך בסריקה.

סמל עצור - מסיים את הסריקה.

לחץ על **פתח חלון סריקה** כדי לפתוח את יומן הסריקות של המחשב עם פרטים נוספים על הסריקה.

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

> 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 **סריקות מתקדמות** > **סריקה מותאמת אישית**.



התפריט הנפתח **פעולה לאחר הסריקה** מאפשר לך להגדיר פעולה שתבוצע באופן אוטומטי לאחר סיום הסריקה:

- **ללא פעולה** לאחר סיום הסריקה לא תתבצע כל פעולה.
- **כיבוי** המחשב יכבה לאחר סיום הסריקה.
- **הפעלה מחדש בעת הצורך** המחשב מבצע הפעלה מחדש רק אם הדבר נדרש כדי להשלים ניקוי של איומים שאותרו.
- **אתחול מחדש** סגירת כל התוכניות הפתוחות והפעלה מחדש של המחשב לאחר סיום הסריקה.
- **כפה הפעלה מחדש במידת הצורך** המחשב מבצע הפעלה מחדש רק אם הדבר נדרש כדי להשלים ניקוי של איומים שאותרו.
- **כפה אתחול מחדש** כופה סגירה של כל התוכניות הפתוחות מבלי להמתין לאינטראקציה עם המשתמש ומפעיל מחדש את 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.

> i הפעולות **שינה** או **מצב שינה** זמינות בהתאם להגדרות צריכת החשמל והשינה במערכת ההפעלה במחשב שלך או יכולות המחשב השולחני או הנייד שלך. זכור שמחשב ישן הוא עדיין מחשב פועל. הוא עדיין מפעיל פונקציות בסיסיות וצורך חשמל כשהמחשב פועל על סוללה. כדי לשמר את חיי הסוללה, למשל כשאתה מחוץ למשרד, אנו ממליצים להשתמש באפשרות 'מצב שינה'.

הפעולה הנבחרת תתחיל לאחר סיום כל הסריקות הפועלות. כאשר תבחר באפשרות **כיבוי** או **אתחול מחדש**, חלון דו-שיח לאישור יציג ספירה לאחור של 30 שניות (לחץ על **ביטול** כדי לבטל את הפעולה המבוקשת).

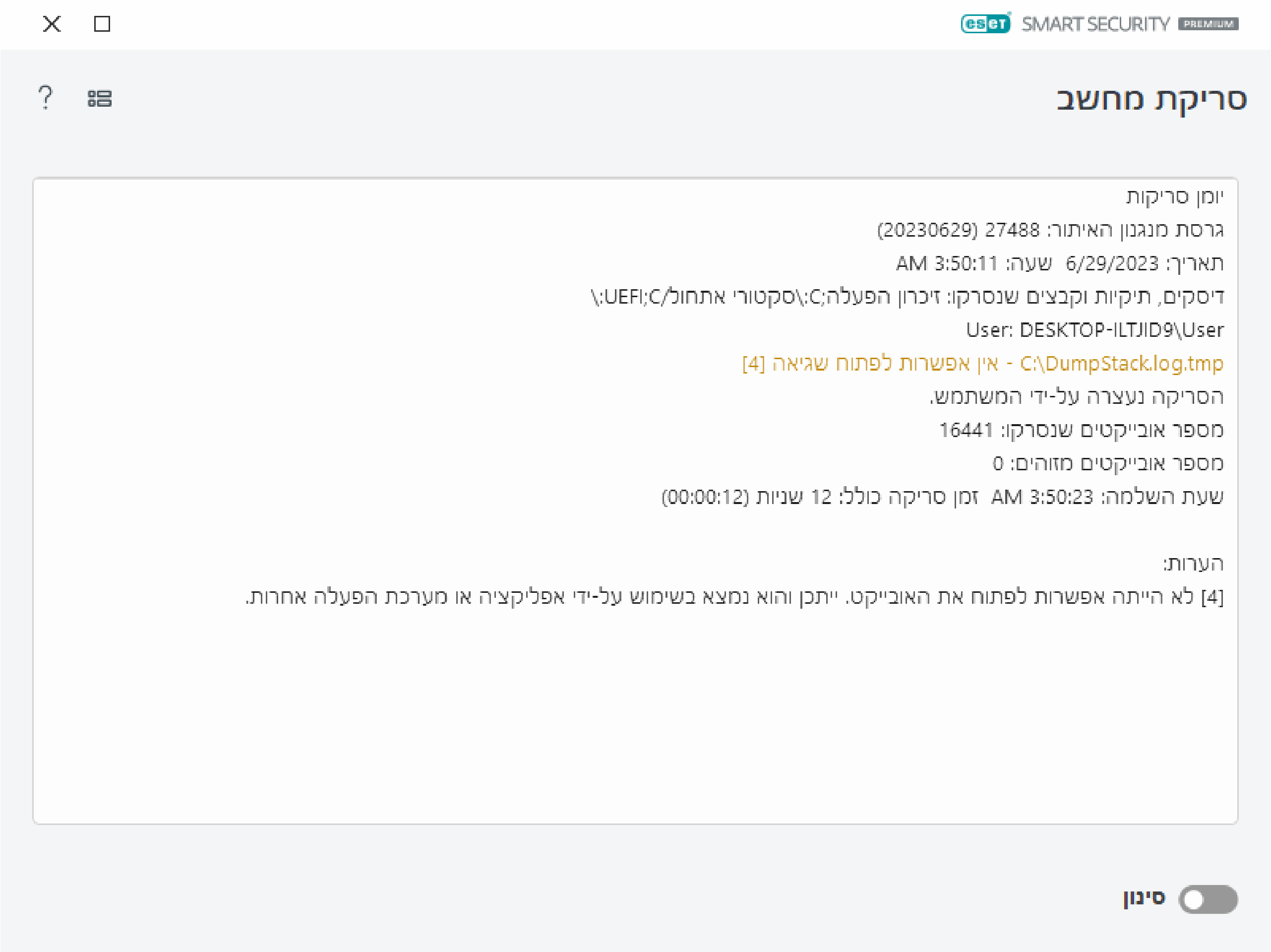
יומן רישום של המחשב

באפשרותך להציג מידע מפורט הקשור לסריקה ספציפית ברשומות יומן. יומן הסריקות מכיל את הפרטים הבאים:

- גרסת מנגנון האיתור
- התאריך והשעה של התחלת הסריקה
- רשימה של הדיסקים, התיקיות והקבצים שנסרקו
- שם סריקה מתוזמנת (סריקה מתוזמנת בלבד)
- המשתמש שהתחיל את הסריקה.
- מצב סריקה
- מספר אובייקטים שנסרקו
- מספר האובייקטים המזוהים שנמצאו
- שעת השלמה
- זמן סריקה כולל

> i המערכת תדלג על התחלה חדשה של משימה מתוזמנת של סריקת מחשב אם אותה משימה מתוזמנת שהופעלה קודם לכן עדיין פועלת. משימת הסריקה המתוזמנת שעליה המערכת דילגה תיצור יומן סריקות של המחשב עם 0 אובייקטים שנסרקו וסטטוס של **הסריקה לא התחילה מכיוון שהסריקה הקודמת עדיין פעלה**.

כדי לאתר יומני סריקות קודמים, בחר באפשרות **כלים** > **רשומות יומן** מתוך חלון התוכנית הראשי. בחר באפשרות **סריקת מחשב** מתוך התפריט הנפתח ולחץ פעמיים על הרשומה הרצויה.



לקבלת מידע נוסף על הרשומות "אין אפשרות לפתוח", "שגיאת פתיחה" ו/או "ארכיון פגום", עיין במאמר מאגר הידע של ESET.

לחץ על סמל המתג **סינון** כדי לפתוח את החלון סינון יומן, שבו תוכל לצמצם את החיפוש לפי קריטריונים מותאמים אישית. כדי להציג את התפריט תלוי ההקשר, לחץ באמצעות לחצן העכבר הימני על רשומת יומן ספציפית:

שימוש	פעולה
הפעלת סינון היומן. היומן יציג רשומות מאותו סוג בלבד של הרשומה שנבחרה.	סנן את אותן רשומות
אפשרות זו פותחת את החלון 'סינון יומן' ומאפשרת לך להגדיר קריטריונים עבור הזנות יומן ספציפיות. קיצור דרך: `Ctrl+Shift+F`	סינון
הפעלת הגדרות המסנן. אם אתה מפעיל את המסנן לראשונה, עליך להגדיר את ההגדרות והחלון 'סינון יומן' ייפתח.	השבת מסנן
כיבוי המסנן (פעולה השקולה ללחיצה על המתג בחלק התחתון של החלון).	השבת מסנן
העתקת הרשומות המודגשות ללוח. קיצור דרך: `Ctrl+C`	העתק
העתקת כל הרשומות שבחלון.	העתק הכול
העתקת הרשומות המודגשות ללוח לקובץ XML.	יצא
אפשרות זו מייצאת את כל הרשומות שבחלון לקובץ XML.	יצא הכול
פתיחת אנציקלופדיית האיומים של ESET, אשר כוללת מידע מפורט אודות הסכנות והתסמינים של החדירה שהודגשה.	תיאור האיתור

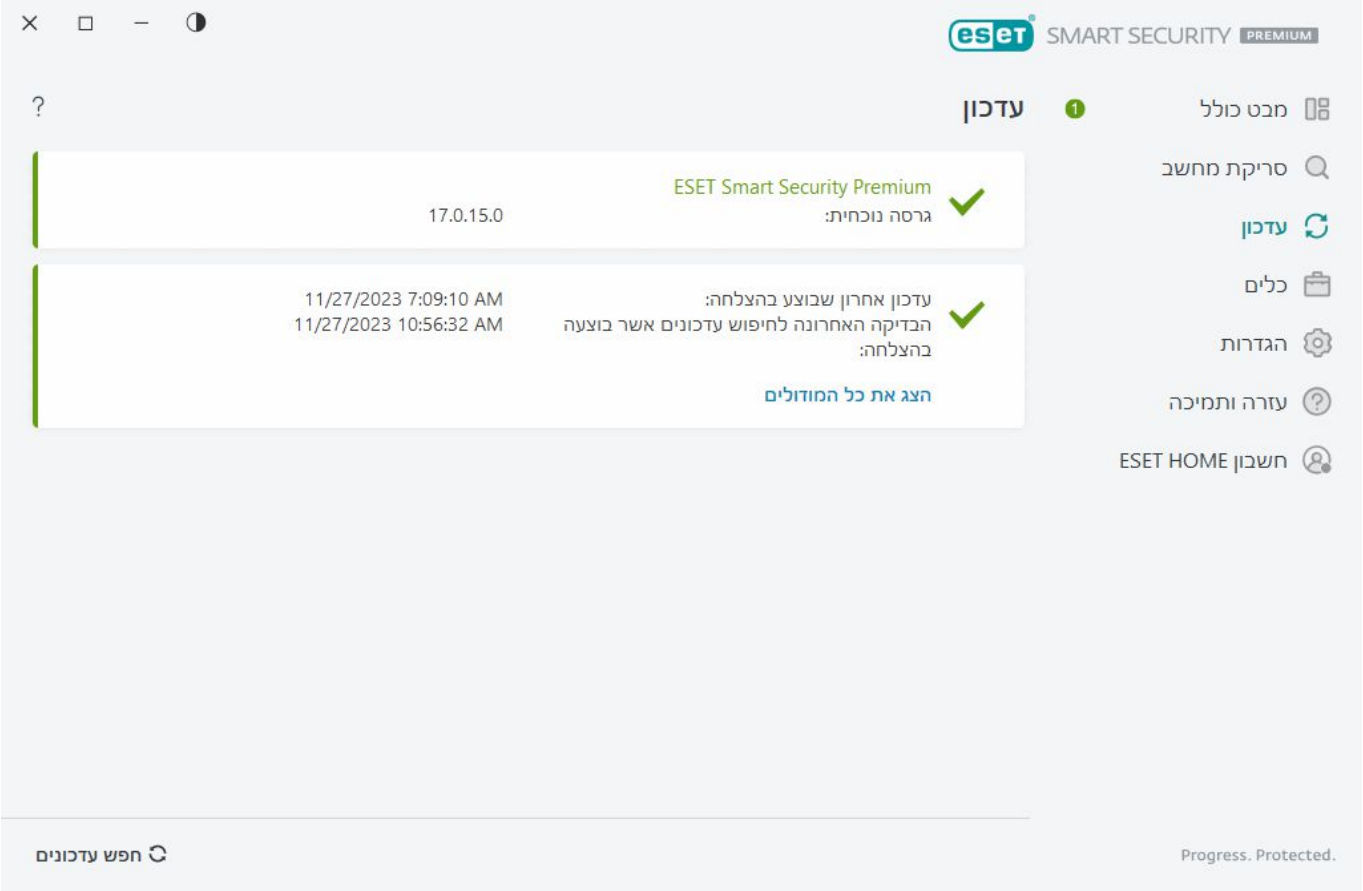
עדכון

עדכון סדיר של ESET Smart Security Premium הוא הדרך הטובה ביותר להבטיח את רמת האבטחה המרבית למחשב שלך. מודול העדכון מבטיח שמודולי התוכנית ורכיבי התוכנית יהיו עדכניים תמיד.

לחיצה על **עדכון** בחלון התוכנית הראשי מאפשרת לך להציג את סטטוס העדכון הנוכחי, לרבות התאריך והשעה של העדכון המוצלח האחרון ומידע אם יש צורך בעדכון.

בנוסף לעדכונים אוטומטיים, באפשרותך ללחוץ על **בדוק אם קיימים עדכונים** כדי להפעיל עדכון ידני. עדכון קבוע של המודולים והרכיבים של התוכנית הוא חלק חשוב בשמירה על הגנה מלאה מפני קודים זדוניים. שים לב היטב לתצורה

ולפעולה של מודולי המוצר. כדי לקבל עדכונים עליך להפעיל את המוצר באמצעות מפתח ההפעלה. אם לא עשית זאת במהלך ההתקנה, יהיה עליך [להפעיל את ESET Smart Security Premium](#) כדי לגשת אל שרתי העדכון של ESET. מפתח ההפעלה נשלח אליך בדוא"ל מ-ESET לאחר הרכישה של ESET Smart Security Premium.



גרסה נוכחית הצגת מספר הגרסה של גרסת המוצר הנוכחית שהותקנה.

עדכון מוצלח אחרון הצגת תאריך העדכון המוצלח האחרון. אם אינך רואה תאריך מהתקופה האחרונה, ייתכן שמודולי המוצר אינם מעודכנים.

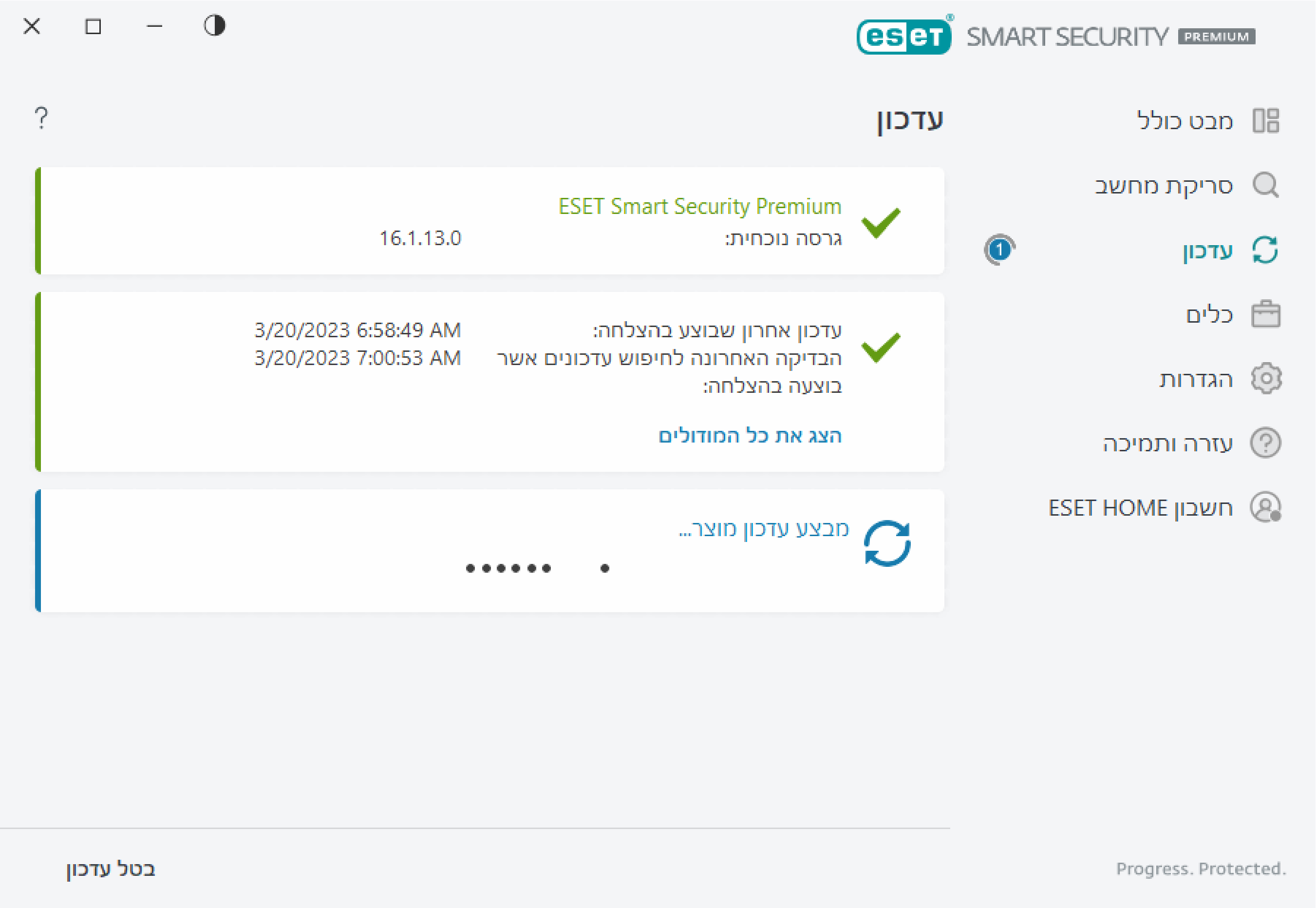
חיפוש מוצלח אחרון אחר עדכונים קיימים הצגת תאריך החיפוש המוצלח האחרון אחר עדכונים קיימים.

הצג את כל המודולים הצגת רשימת מודולי התוכנית המותקנים.

לחץ על **חפש עדכונים** כדי לבדוק מהי הגרסה העדכנית ביותר של ESET Smart Security Premium שזמינה.

תהליך העדכון

לאחר שתלחץ על **חפש עדכונים**, ההורדה תתחיל. יופיע סרגל התקדמות המציג את התקדמות ההורדה והזמן שנותר להורדה. כדי לעצור את העדכון לחץ על **בטל עדכון**.



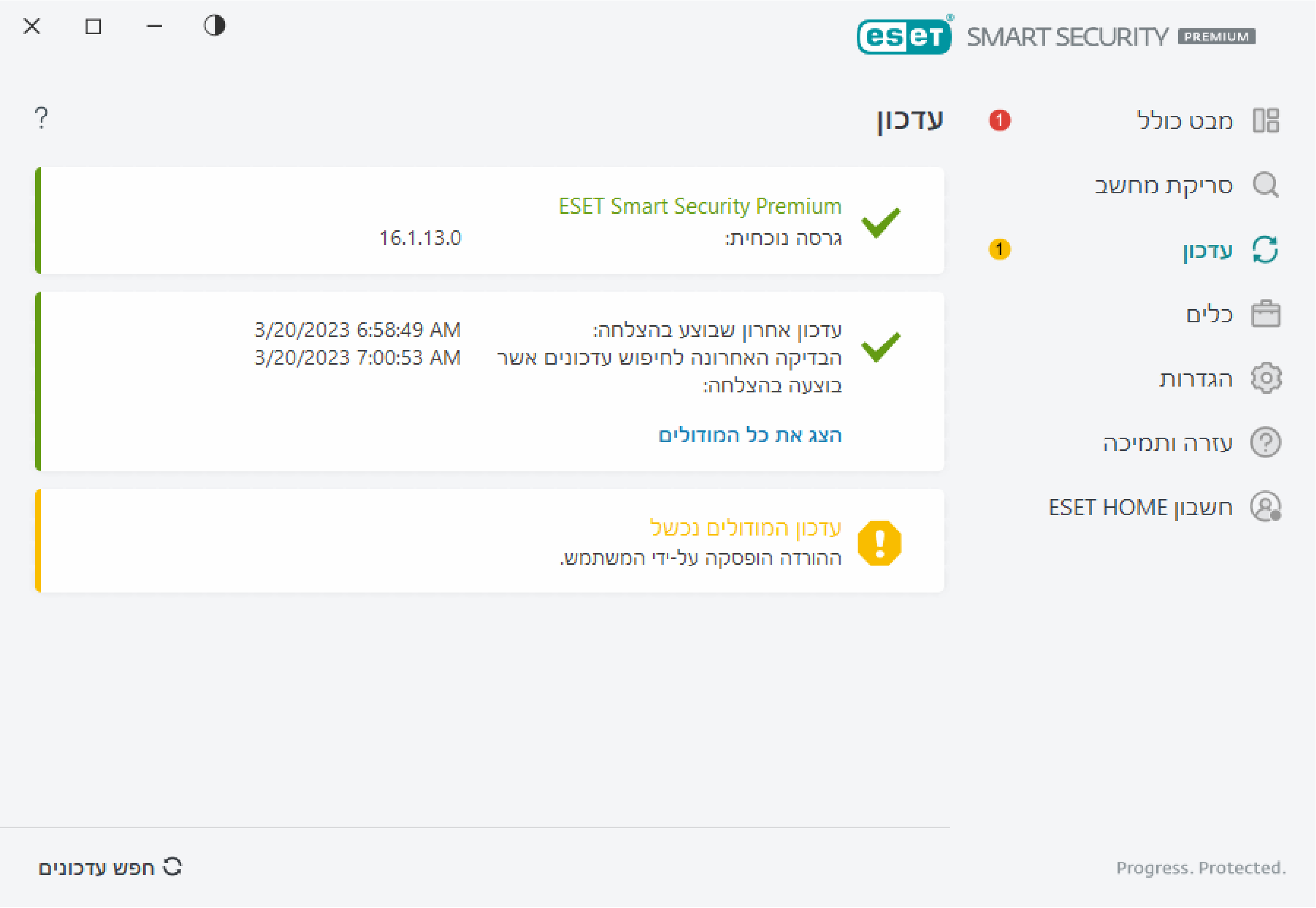
בתנאים רגילים, תראה סימן ביקורת ירוק בחלון **עדכון** שמציין שהתכנית עדכנית. אם אינך רואה סימן ביקורת ירוק, התוכנית אינה מעודכנת והיא פגיעה יותר להידבקות. עדכן את מודולי התכנית בהקדם האפשרי.

עדכון שלא הצליח

אם קיבלת הודעה על כישלון בעדכון המודולים, ייתכן שהוא נגרם עקב הבעיות להלן:

1. **מינוי לא חוקי** - המינוי ששימש להפעלה אינו חוקי או שפג תוקפו. בחלון התוכנית הראשי, לחץ על **עזרה ותמיכה** > **החלף מינוי** והפעל את המוצר.

2. **אירעה שגיאה בעת הורדת קובצי עדכון** הסיבה עשויה להיות שגיאה בהגדרות החיבור לאינטרנט. מומלץ שתבדוק את קישוריות האינטרנט שלך (על-ידי פתיחת אתר אינטרנט כלשהו בדפדפן). אם אתר האינטרנט אינו נפתח, סביר להניח שלא נוצר חיבור לאינטרנט או שישנן בעיות קישוריות במחשב. אנא ברר עם ספק שירותי האינטרנט (ISP) שלך אם אין לך חיבור פעיל לאינטרנט.



עליך להפעיל מחדש את המחשב לאחר עדכון מוצלח של ESET Smart Security Premium לגרסת מוצר חדשה יותר, כדי להבטיח שכל מודולי התכנית עודכנו כהלכה. אין צורך להפעיל מחדש את המחשב לאחר עדכון רגיל של מודולים.

לקבלת מידע נוסף בקר בפתרון בעיות עבור ההודעה "עדכון המודולים נכשל".

חלון דו-שיח – נדרשת הפעלה מחדש

נדרשת הפעלה מחדש של המחשב לאחר עדכון ESET Smart Security Premium לגרסה חדשה. גרסאות חדשות של ESET Smart Security Premium יוצאות כדי לממש שיפורים או לתקן בעיות שאותן עדכונים אוטומטיים של מודולי התוכנית אינם מסוגלים לזהות.

ניתן להתקין את הגרסה החדשה של ESET Smart Security Premium באופן אוטומטי, על סמך הגדרות עדכון התוכנית, או באופן ידני על ידי הורדה והתקנה של גרסה חדשה יותר שתחליף את הקודמת.

לחץ על **הפעל מחדש כעת** כדי להפעיל מחדש את המחשב. אם בכוונתך להפעיל מחדש את המחשב במועד מאוחר יותר, לחץ על **הזכר לי מאוחר יותר**. לאחר מכן, יהיה באפשרותך להפעיל מחדש את המחשב באופן ידני מתוך המקטע **מבט כולל** בחלון התוכנית הראשי.

כיצד ליצור משימות עדכון

ניתן להפעיל את העדכונים באופן ידני על-ידי לחיצה על **חפש אם קיימים עדכונים** בחלון הראשי המוצג לאחר לחיצה על **עדכון** בתפריט הראשי.

ניתן להפעיל את העדכונים גם כמשימות מתוזמנות. כדי להגדיר משימה מתוזמנת, לחץ על **כלים** > **מתזמן**. כברירת מחדל, משימות העדכון הבאות מופעלות ב-ESET Smart Security Premium:

- **עדכון אוטומטי רגיל**
- **עדכון אוטומטי לאחר התחברות של המשתמש**

כל אחת ממשימות העדכון ניתנת לשינוי בהתאם לצרכיך. בנוסף למשימות העדכון שנקבעו כברירת מחדל, באפשרותך ליצור משימות עדכון חדשות עם תצורת המוגדרת על-ידי המשתמש. לקבלת פרטים נוספים על יצירה והגדרה של משימות עדכון עיין בסעיף מתזמן.

כלים

התפריט **כלים** כולל תכונות המציעות אבטחה נוספת ומסייעות לפשט את הניהול של ESET Smart Security Premium. הכלים הבאים זמינים:

רשומות יומן

תהליכים פועלים (אם ESET LiveGrid® מופעל ב-ESET Smart Security Premium)

דוח אבטחה

חיבורי רשת (אם חומת האש מופעלת ב-ESET Smart Security Premium)

ESET SysInspector

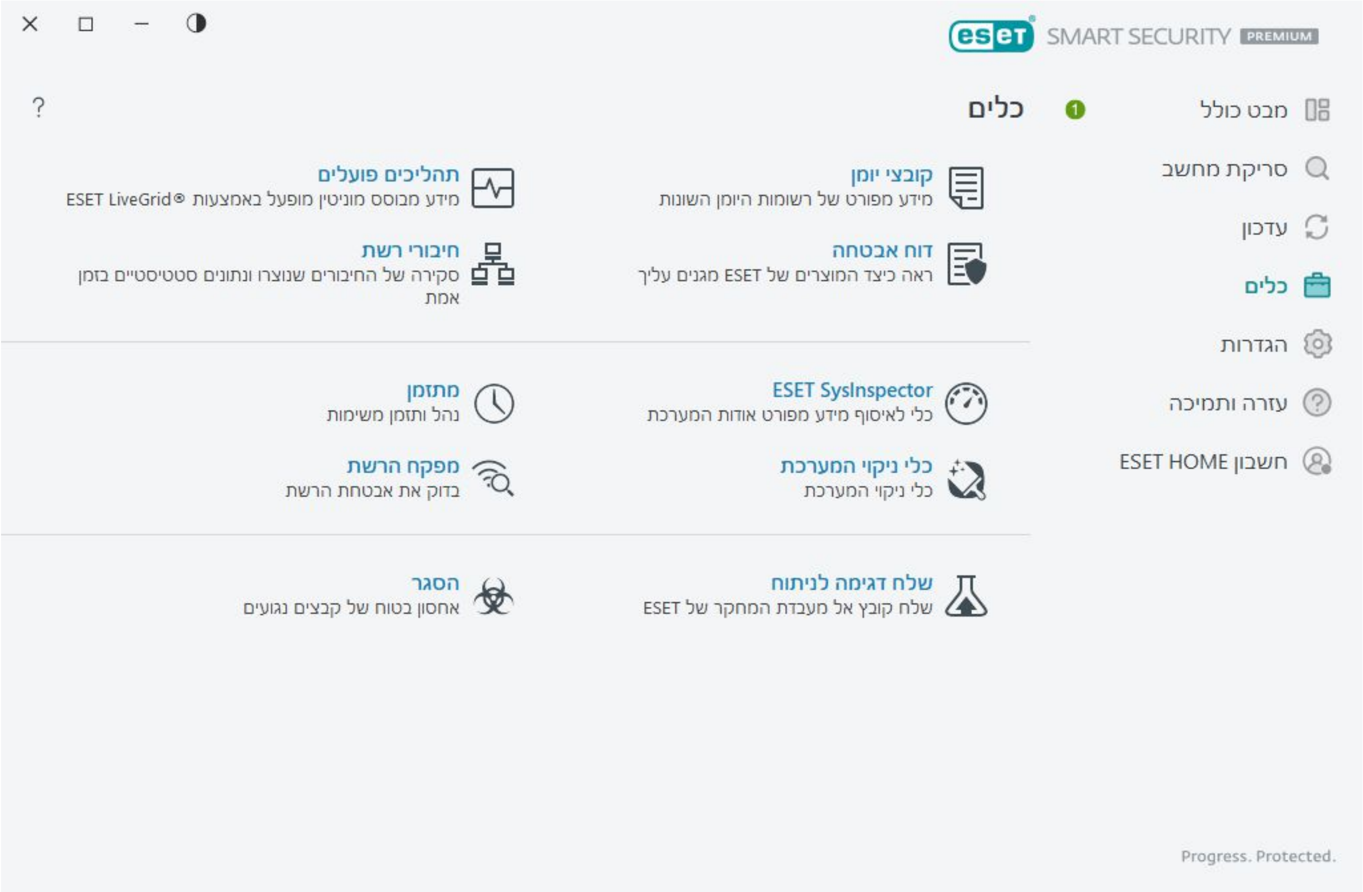
מתזמן

כלי ניקוי המערכת

מפקח הרשת

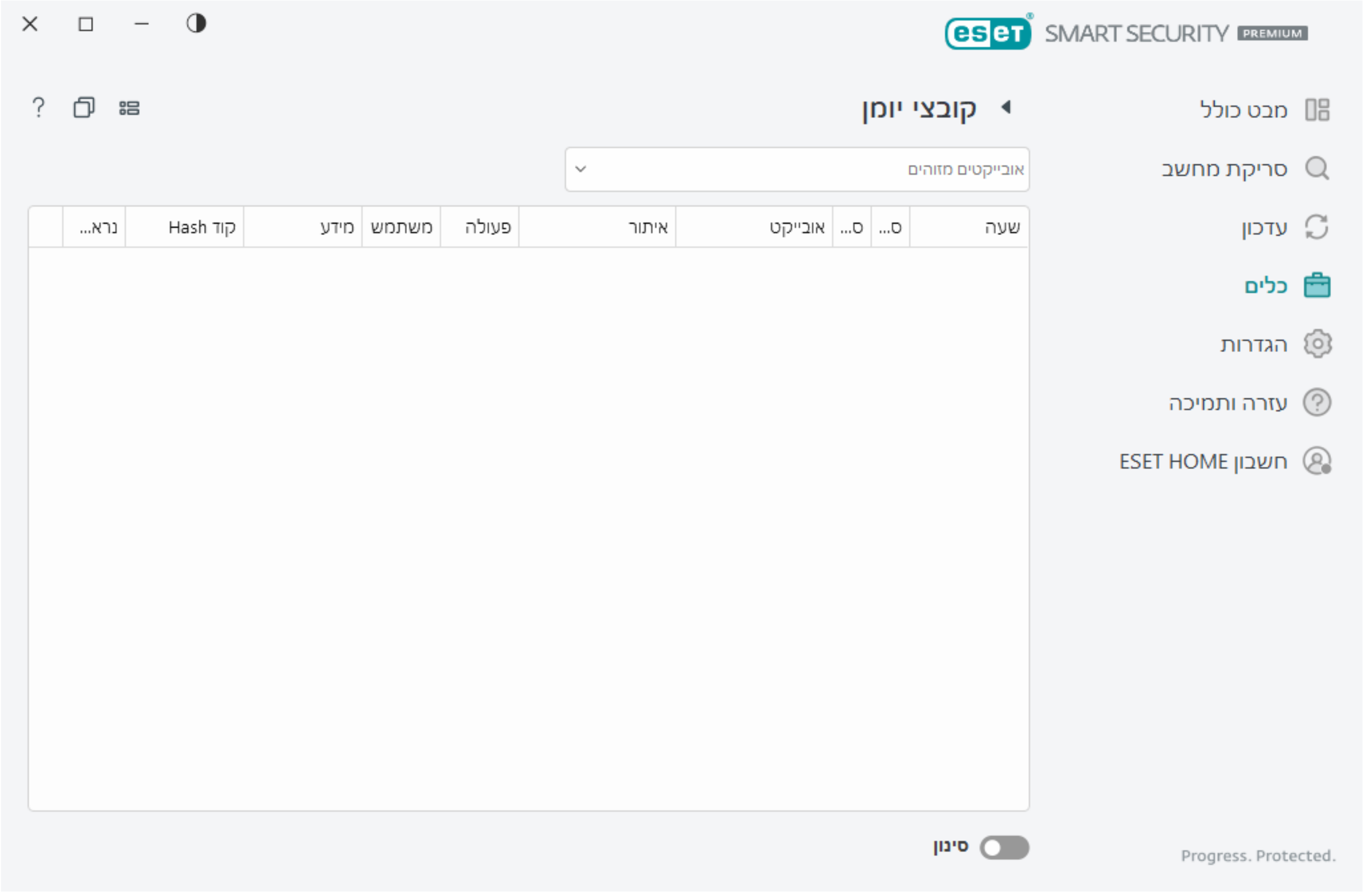
שלח מדגם לניתוח (ייתכן שלא יהיה זמין לפי תצורת ESET LiveGrid® שלך).

הסגר



רשומות יומן

קובצי יומן מכילים מידע על האירועים החשובים של התוכנית אשר התרחשו ומספקים סקירה כללית של איומים שזוהו. הרישום הוא חלק חיוני של ניתוח המערכת, זיהוי איומים ופתרון בעיות. הרישום מבוצע באופן פעיל ברקע, ללא אינטראקציה עם המשתמש. המידע מתועד בהתאם לרמות הפירוט שהוגדרו עבור היומן הנוכחי. ניתן להציג הודעות טקסט ויומנים ישירות מתוך הסביבה של ESET Smart Security Premium, וכן לאחסן יומנים בארכיון.



ניתן לגשת אל רשומות יומן מ[חלון התוכנית הראשי](#) בלחיצה על **כלים** > **רשומות יומן**. בחר את סוג היומן הרצוי מהתפריט הנפתח יומן.

- **אובייקטים מזוהים** – יומן זה מציע מידע מפורט על אובייקטים מזוהים וחדירות שזוהו על-ידי ESET Smart Security Premium. המידע ביומן כולל את מועד הזיהוי, סוג הסורק, סוג האובייקט, מיקום האובייקט, שם האובייקט המזוהה, הפעולה שננקטה, שם המשתמש שהיה מחובר כשהחדירה זוהתה, קוד ה-Hash והמופע הראשון. חדירות שלא נוקו מסומנות תמיד בטקסט אדום על רקע אדום בהיר, וחדירות שנוקו מסומנות בטקסט צהוב על רקע לבן. אפליקציות העלולות להיות לא בטוחות או לא רצויות שלא נוקו מוצגות בטקסט צהוב על רקע לבן. אפליקציות העלולות להיות לא בטוחות או לא רצויות שלא נוקו מוצגות בטקסט צהוב על רקע לבן.
- **אירועים** – כל הפעולות החשובות שמבוצעות על-ידי ESET Smart Security Premium מתועדות ביומן האירועים. יומן האירועים מכיל מידע על אירועים ושגיאות שאירעו בתוכנית הוא תוכנן עבור מנהלי מערכת ומשתמשים למטרת פתרון בעיות. לעתים קרובות, המידע שנמצא כאן יכול לסייע לך למצוא פתרון לבעיה שמתרחשת בתוכנית.
- **סריקת מחשב** – תוצאותיהן של כל הסריקות הקודמות מוצגות בחלון זה. כל שורה מתייחסת לבקרה של מחשב יחיד. לחץ לחיצה כפולה על ערך כלשהו כדי להציג את [פרטי הסריקה שנבחרה](#).
- **קבצים שנשלחו** – מכיל רשומות של הדגימות שנשלחו אל ESET LiveGuard.
- **HIPS** – מכילה רשומות של כללי [HIPS](#) ספציפיים המסומנים לתיעוד. הפרוטוקול מציג את היישום שהפעיל את הפעולה, את התוצאה (אם הכלל אושר או נאסר) ואת שם הכלל.
- **הגנת דפדפן** – מכילה רשומות של קבצים לא מאומתים/לא מהימנים שנטענו בדפדפן.
- **הגנת רשת** – [יומן הגנת הרשת](#) מציג את כל המתקפות המרוחקות שאותרו על ידי חומת האש, הגנה מפני מתקפות רשת (IDS) והגנה מפני 'מחשב זומבי' (Botnet). כאן תמצא מידע על כל המתקפות במחשב שלך. העמודה אירוע מפרטת את המתקפות שאותרו. העמודה מקור תספר לך יותר על התוקף. העמודה פרוטוקול חושפת את פרוטוקול התקשורת המשמש למתקפה. ניתוח יומן הגנת הרשת עשוי לעזור לך לאתר את ניסיונות החדירה למערכת בזמן כדי למנוע גישה בלתי מורשית למערכת. לקבלת פרטים נוספים על מתקפות רשת, ראה

IDS ואפשרויות מתקדמות.

- **אתרי אינטרנט מסוננים** - רשימה זו שימושית אם ברצונך להציג רשימה של אתרי אינטרנט שנחסמו על-ידי הגנת גישה לאינטרנט או בקרת הורים.כל יומן כולל את השעה, כתובת ה-URL, המשתמש והיישום ששימשו ליצירת חיבור לאתר אינטרנט מסוים.
- **אנטי ספאם בלקוח דוא"ל** כוללת רשומות הקשורות להודעות דואר אלקטרוני שסומנו כדואר זבל.
- **בקרת הורים** מציגה דפי אינטרנט שנחסמו או הותרו על-ידי בקרת ההורים. העמודות סוג התאמה וערכי התאמה מספרות לך כיצד כללי הסינון הוחלו.
- **בקרת התקנים** כוללת רשומות של מדיה נשלפת או התקנים שחוברו למחשב. רק התקנים עם כללי בקרת ההתקנים המתאימים יתועדו בקובץ היומן. אם הכלל אינו תואם להתקן מחובר, לא תיווצר הזנת יומן עבור התקן מחובר. תוכל לראות גם פרטים דוגמת סוג ההתקן, המספר הסידורי, שם הספק וגודל המדיה (אם זמינים).
- **הגנת מצלמת אינטרנט** כוללת רשומות על יישומים שנחסמו על-ידי הגנת מצלמת אינטרנט.

בחר את התוכן של כל יומן והקש **CTRL + C** כדי להעתיק אותו ללוח. החזק את **CTRL** או את **SHIFT** כדי לבחור מספר ערכים.

לחץ על **סינון** לפתיחת החלון סינון יומן, בו תוכל להגדיר את קריטריוני הסינון.

לחץ באמצעות לחצן העכבר הימני על רשומה ספציפית כדי לפתוח את תפריט ההקשר. האפשרויות הבאות זמינות בתפריט ההקשר:

- **הצג** הצגת מידע מפורט יותר על היומן שנבחר בחלון חדש.
- **סנן את אותן רשומות** לאחר הפעלת מסנן זה תראה רק רשומות מאותו סוג (אבחון, אזהרות, ...).
- **סינון** לאחר לחיצה על אפשרות זו, החלון סינון יומן יאפשר לך להגדיר קריטריוני סינון עבור הזנות יומן ספציפיות.
- **הפעל מסנן** הפעלת הגדרות המסנן.
- **השבת מסנן** ניקוי כל הגדרות הסינון (כמתואר לעיל).
- **העתק/העתק הכול** העתקת מידע אודות כל הרשומות שנבחרו בחלון.
- **העתק תא** העתקת תוכן התא שעליו לחצת באמצעות לחצן העכבר הימני.
- **מחק/מחק הכול** מחיקת הרשומות שנבחרו או כל הרשומות המוצגות. פעולה זו מחייבת הרשאות מנהל מערכת.
- **יצא/יצא הכול** ייצוא מידע אודות הרשומות שנבחרו בתבנית XML.
- **חפש/חפש את הבא/חפש את הקודם** לאחר לחיצה על אפשרות זו, תוכל להגדיר קריטריוני סינון להדגשת הזנת היומן הספציפית באמצעות החלון 'סינון יומן'.
- **תיאור האיתור** פתיחת אנציקלופדיית האיומים של ESET, אשר כוללת מידע מפורט אודות הסכנות והתסמינים של החדירה שתועדה.
- **צור החרגה** צור החרגה חדשה מאיתור באמצעות אשף (לא זמין עבור איתורי תוכנה זדונית).
- **הוסף לרשימת ההרשאות של הגנת דפדפן** פותח את החלון של רשימת ההרשאות של הגנת דפדפן ומוסיף את הפריט לרשימה.

סינון יומן

לחץ על **סינון** בכלים > **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.

סוגמ 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

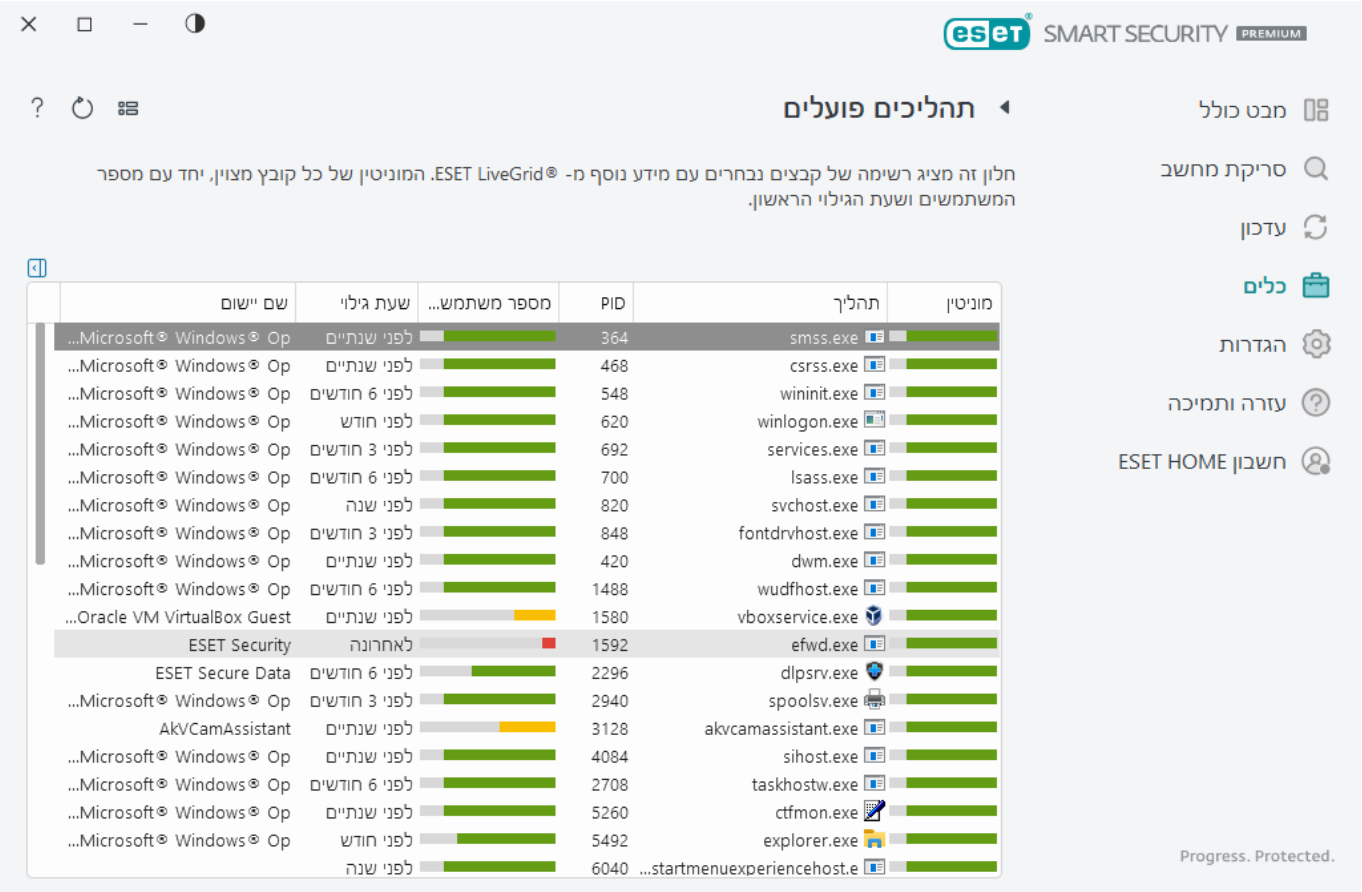
השתמש בתיבת החיפוש אם ברצונך לחפש מילים מלאות לתוצאות מדויקות יותר.

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.

תהליכים פועלים

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



מוניטין – ברוב המקרים, ESET Smart Security Premium 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.

> ⓘ 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®.

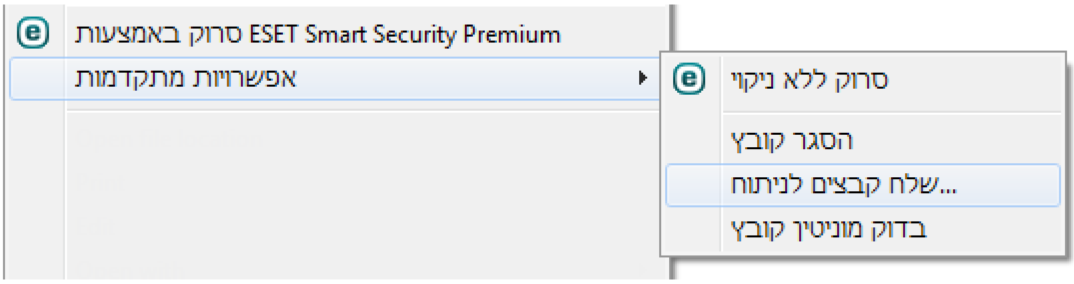
יישום הנושא את הסימון לא ידוע (כתום) אינו בהכרח תוכנה זדונית. בדרך-כלל זהו יישום חדש יחסית. אם אינך בטוח לגבי הקובץ, באפשרותך לשלוח את הקובץ לניתוח במעבדת המחקר של ESET. אם יסתבר שהקובץ הוא יישום זדוני, זיהויו יתווסף לעדכון הבא.

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 ב-kB (קילו-בתים) או ב-MB (מגה-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).

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 זו 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 נגועים של דוא"ל אותרו** – הצגת מספר האובייקטים הנגועים של דוא"ל שאותרו.
- **דפי אינטרנט ב'בקרת הורים' נחסמו** – הצגת המספר של הדפי האינטרנט ב'בקרת הורים' שנחסמו.
- **אפליקציה העלולה להיות לא רצויה אותרו** – הצגת המספר של אפליקציה העלולה להיות לא רצויה (PUA).
- **הודעות דואר זבל אותרו** – הצגת המספר של הודעות דואר הזבל שאותרו.
- **גישה חסומה למצלמת אינטרנט** – הצגת המספר של ניסיונות הגישה למצלמת האינטרנט שנחסמו.
- **מסמכים נסרקו** – מופיע מספר האובייקטים במסמכים שנסרקו.
- **אפליקציות שנסרקו** – הצגת מספר האובייקטים של קובצי הפעלה שנסרקו.
- **אובייקטים אחרים נסרקו** – מופיע מספר האובייקטים האחרים שנסרקו.
- **אובייקטים בדף אינטרנט נסרקו** – הצגת מספר האובייקטים בדפי אינטרנט שנסרקו.
- **אובייקטים של דוא"ל נסרקו** – הצגת המספר של אובייקטים של דוא"ל שנסרקו.
- **קבצים שנותחו באמצעות ESET LiveGuard** – הצגת מספר הדגימות שנותחו באמצעות ESET LiveGuard.

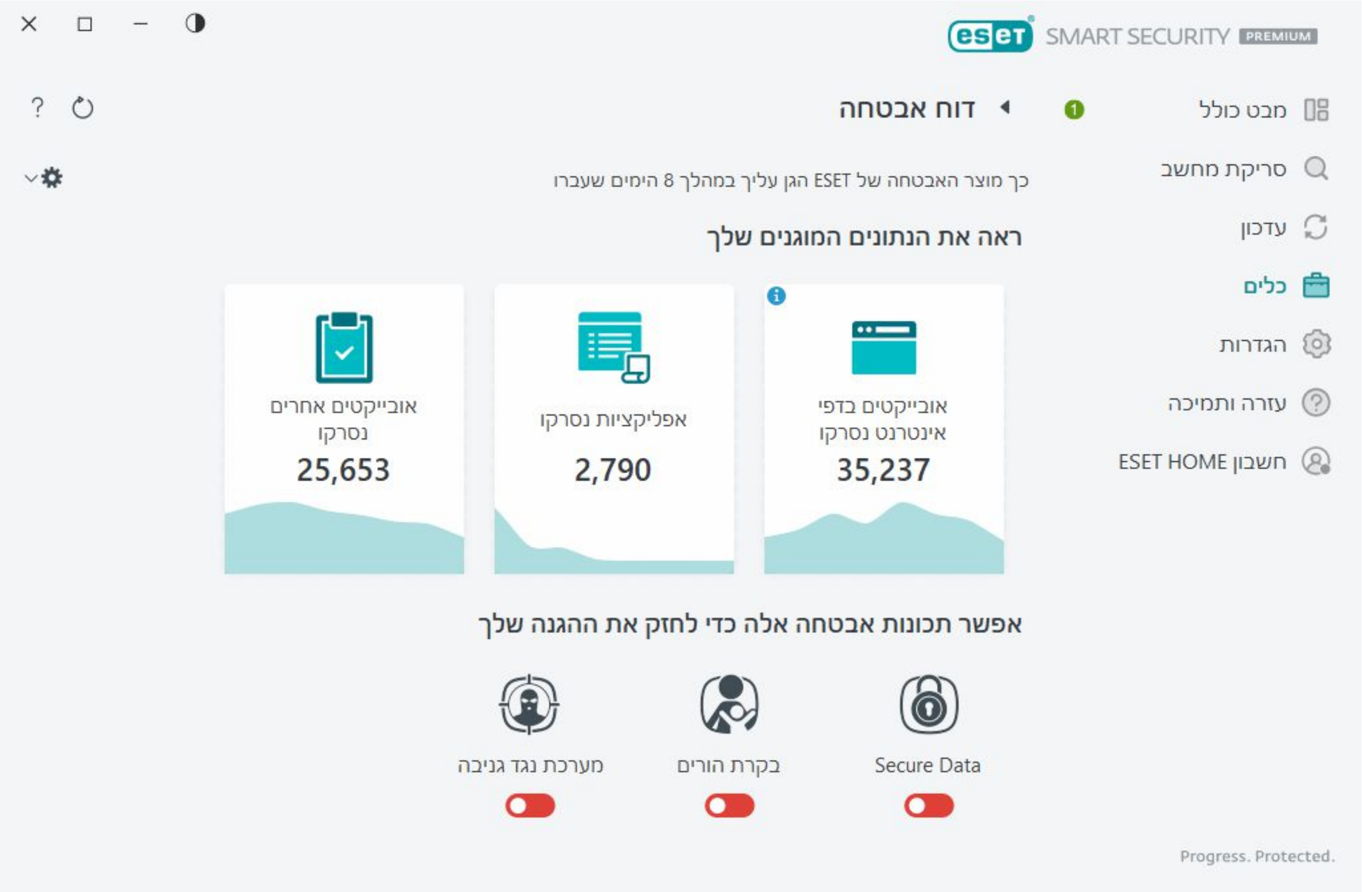
הסדר של קטגוריות אלה מבוסס על הערך המספרי מהגבוה ביותר לנמוך ביותר. הקטגוריות עם ערך אפס אינן מוצגות. לחץ על **הצג עוד** כדי להרחיב ולהציג קטגוריות מוסתרות.

החלק האחרון בדוח האבטחה מאפשר לך להפעיל את התכונות להלן:

- ESET LiveGuard
- Secure Data
- בקרת הורים
- מערכת נגד גניבה

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

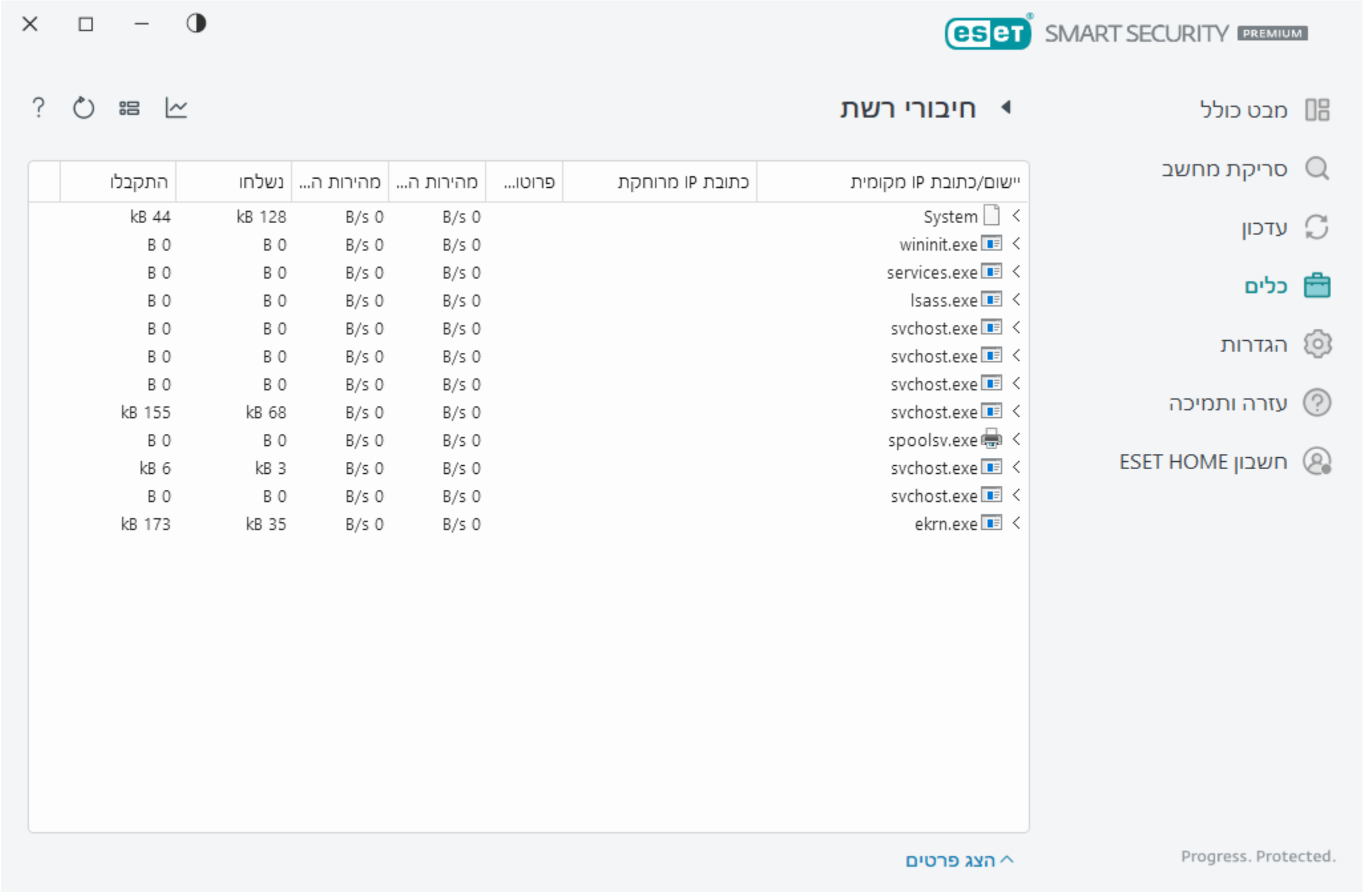
לחיצה על גלגל השיניים בפינה השמאלית העליונה מאפשרת לך **להפעיל/להשבית הודעות של דוח אבטחה** או לבחור האם הנתונים יוצגו עבור 30 הימים האחרונים או מאז שהמוצר הופעל. אם התקנת את ESET Smart Security Premium לפני פחות מ-30 ימים, אזי תוכל לבחור רק את מספר הימים שחלפו מתאריך ההתקנה. התקופה של 30 ימים מוגדרת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



איפוס נתונים ינקה את כל הנתונים הסטטיסטיים וימחק את הנתונים הקיימים עבור דוח אבטחה. יש לאשר פעולה זו מלבד במקרה של ביטול הבחירה באפשרות **שאל לפני איפוס נתונים סטטיסטיים** בחלון הגדרות מתקדמות > **התראות** > **התראות אינטראקטיביות** > **הודעות אישור** > **עריכה**.

חיבורי רשת

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



לחץ על סמל הגרף כדי לפתוח את [פעילות רשת](#).

בשורה הראשונה מוצגים שם האפליקציה ומהירות העברת הנתונים שלה. להצגת רשימת החיבורים שביצעה האפליקציה (ומידע מפורט יותר) לחץ על **<**.

עמודות

יישום/כתובת IP מקומית שם של יישום, כתובת 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.

נשלחו/התקבלו 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.

הצג 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**.

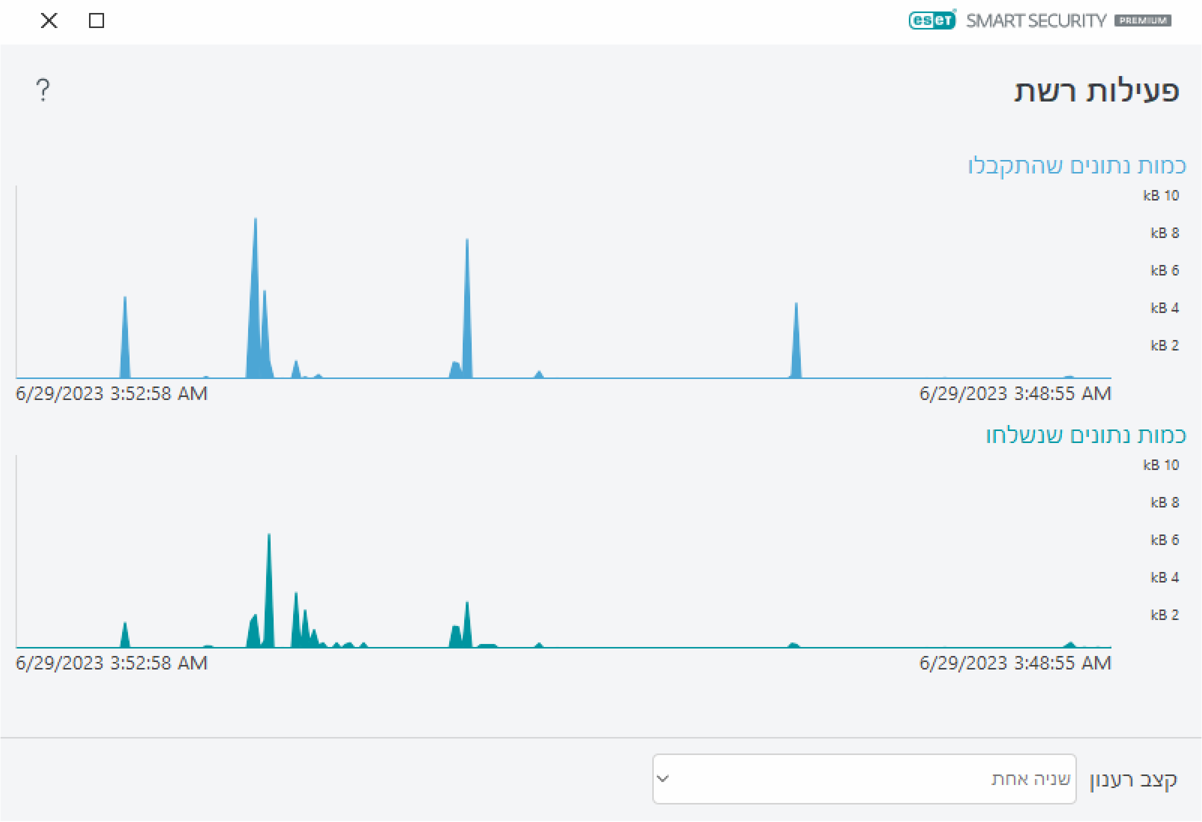
האפשרויות הבאות זמינות רק לאחר לחיצה על יישום או תהליך מסוימים, ולא על חיבור פעיל:

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 במקטע כללים של חומת אש.

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 במקטע כללים של חומת אש.

פעילות רשת

כדי לראות את **פעילות הרשת** הנוכחית בצורת גרף, לחץ על **כלים** > **חיבורי רשת** ולחץ על סמל הגרף . בחלק התחתון של הגרף נמצא ציר זמן המתעד את פעילות הרשת בזמן אמת, בהתאם לטווח הזמן שנבחר. כדי לשנות את טווח הזמן, בחר בערך הרלוונטי מתוך התפריט הנפתח **קצב רענון**.



האפשרויות הבאות זמינות:

- **שנייה 1** הגרף עובר רענון מדי שנייה וציר הזמן מכסה את 4 השניות האחרונות.
- **דקה 1 (24 השעות האחרונות)** הגרף עובר רענון מדי דקה וציר הזמן מכסה את 24 השעות האחרונות.
- **שעה 1 (החודש האחרון)** הגרף עובר רענון מדי שעה וציר הזמן מכסה את החודש האחרון.

הציר האנכי של הגרף מייצג את כמות הנתונים שהתקבלו או שנשלחו. העבר את העכבר מעל הגרף כדי לראות את הכמות המדויקת של נתונים שהתקבלו/נשלחו בזמן מסוים.

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. כדי ללמוד כיצד להשתמש ב-ESET SysInspector, עיין בעזרה המקוונת של ESET SysInspector.

החלון ESET SysInspector מציג את המידע הבא אודות יומנים:

- **זמן** שעת יצירת היומן.
- **תגובה** הערה קצרה.
- **משתמש** שם המשתמש שיצר את היומן.
- **סטטוס** סטטוס יצירת היומן.

הפעולות הבאות זמינות:

- **הצג** פתיחת היומן שנבחר ב-ESET SysInspector. באפשרותך גם ללחוץ באמצעות לחצן העכבר הימני על קובץ יומן נתון ולבחור באפשרות **הצג** בתפריט ההקשר.
- **צור** יצירת יומן חדש. המתן עד לסיום יצירת היומן של ESET SysInspector (סטטוס **נוצר**) לפני שתנסה לגשת אליו. היומן נשמר ב-C:\ProgramData\ESET\ESET Security\SysInspector.
- **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).
- **צור** יצירת יומן חדש. המתן עד לסיום יצירת היומן של ESET SysInspector (סטטוס **נוצר**) לפני שתנסה לגשת אליו.
- **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 Smart Security Premium על-ידי לחיצה על **כלים** > **מתזמן**. **המתזמן** מכיל רשימה של כל המשימות המתוזמנות ומאפייני תצורה, כגון התאריך והשעה שנקבעו ופרופיל הסריקה שבו נעשה שימוש.

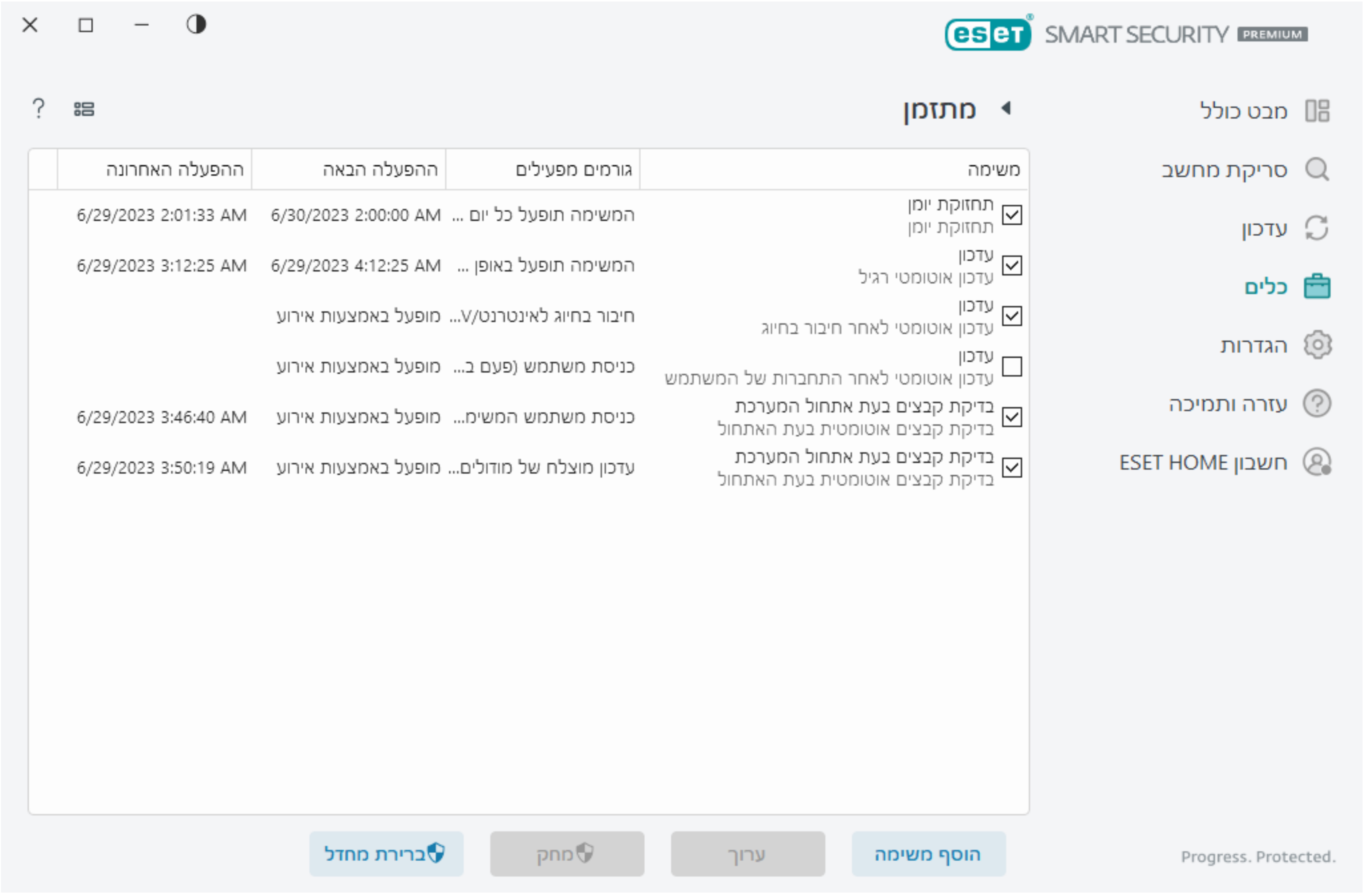
המתזמן משמש לתזמון המשימות הבאות: עדכון מודולים, משימת סריקה, בדיקת קובץ אתחול מערכת ותחזוקת יומן. באפשרותך להוסיף או למחוק משימות ישירות מחלון המתזמן הראשי (לחץ על **הוסף משימה** או **מחק** בחלק התחתון). באפשרותך להחזיר את רשימת המשימות המתוזמנות לברירת מחדל ולמחוק את כל השינויים על-ידי לחיצה על **ברירת**

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 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 פס המחוון שלצד **מאופשר** למצב פעיל כדי 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**
- **באופן מיידי, אם הזמן מאז ההפעלה האחרונה חורג מ- (שעות)** ⍰ אפשרות זו מייצגת את הזמן שחלף מאז ההפעלה הראשונה של המשימה שעליה המערכת דילגה. אם אירעה חריגה מזמן זה, המשימה תופעל באופן מיידי. הגדר את הזמן באמצעות פקד הטווח להלן.

כדי לסקור את המשימה המתוזמנת, לחץ באמצעות לחצן העכבר הימני על המשימה ולחץ על **הצג פרטי משימה**.

אפשרויות סריקה מתוזמנת

בחלון זה אתה יכול לציין אפשרויות מתקדמות למשימה של סריקת מחשב מתוזמנת.

כדי להפעיל סריקה ללא פעולת ניקוי, לחץ על **הגדרות מתקדמות** ובחר **סרוק ללא ניקוי**. היסטוריית הסריקה נשמרת ביומן הסריקות.

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

התפריט הנפתח **פעולה לאחר הסריקה** מאפשר לך להגדיר פעולה שתבוצע באופן אוטומטי לאחר סיום הסריקה:

- **ללא פעולה** ⍰ לאחר סיום הסריקה לא תתבצע כל פעולה.
- **כיבוי** ⍰ המחשב יכבה לאחר סיום הסריקה.
- **הפעלה מחדש בעת הצורך** ⍰ המחשב מבצע הפעלה מחדש רק אם הדבר נדרש כדי להשלים ניקוי של איומים שאותרו.
- **אתחול מחדש** ⍰ סגירת כל התוכניות הפתוחות והפעלה מחדש של המחשב לאחר סיום הסריקה.
- **כפה הפעלה מחדש במידת הצורך** ⍰ המחשב מבצע הפעלה מחדש רק אם הדבר נדרש כדי להשלים ניקוי של איומים שאותרו.
- **כפה אתחול מחדש** ⍰ כופה סגירה של כל התוכניות הפתוחות מבלי להמתין לאינטראקציה עם המשתמש ומפעיל מחדש את 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.

> הפעולות **שינה** או **מצב שינה** זמינות בהתאם להגדרות צריכת החשמל והשינה במערכת ההפעלה במחשב שלך או יכולות המחשב השולחני או הנייד שלך. זכור שמחשב ישן הוא עדיין מחשב פועל. הוא עדיין מפעיל פונקציות בסיסיות וצורך חשמל כשהמחשב פועל על סוללה. כדי לשמור את חיי הסוללה, למשל כשאתה מחוץ למשרד, אנו ממליצים להשתמש באפשרות 'מצב שינה'.

הפעולה הנבחרת תתחיל לאחר סיום כל הסריקות הפועלות. כאשר תבחר באפשרות **כיבוי** או **אתחול מחדש**, חלון דו-שיח לאישור יציג ספירה לאחור של 30 שניות (לחץ על **ביטול** כדי לבטל את הפעולה המבוקשת).

בחר **לא ניתן לבטל את הסריקה** 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.

ראה גם התקדמות הסריקה.

סקירת משימות מתוזמנות

חלון דו-שיח זה מציג מידע מפורט על המשימה המתוזמנת שנבחרה כאשר אתה לוחץ לחיצה כפולה על משימה מותאמת אישית, או כשאתה לוחץ באמצעות לחצן העכבר הימני על משימת מתזמן מותאמת אישית ואז לוחץ על **הצג פרטי משימה**.

פרטי משימה

הקלד את **שם המשימה**, בחר אחת מהאפשרויות של **סוג המשימה** ולאחר מכן לחץ על **הבא**:

- **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.

תזמון משימה

המשימה תחזור על עצמה במרווח הזמנים שצוין. בחר אחת מאפשרויות התזמון:

- **פעם אחת** – המשימה תבוצע פעם אחת בלבד, בתאריך ובשעה שהוגדרו מראש.
- **שוב ושוב** – המשימה תבוצע במרווח הזמנים שצוין (בשעות).
- **יומית** – המשימה תופעל מדי יום בשעה המפורטת.
- **שבועית** – המשימה תופעל פעם אחת או יותר בשבוע, בשעה מוגדרת ביום/ימים שנבחרו.

- **מופעלת על-ידי אירוע** – המשימה תבוצע לאחר אירוע שצוין.

דלג על המשימה בעת פעולה בכוח הסוללה – משימה מסוימת לא תופעל אם ברגע שבו היא אמורה להתבצע המחשב מופעל באמצעות סוללה. כלל זה חל גם על מחשבים הפועלים עם UPS.

תזמון המשימה - פעם אחת

ביצוע משימה – המשימה שצוינה תופעל רק פעם אחת, בתאריך ובשעה שיפורטו.

תזמון המשימה - יומי

המשימה תופעל מדי יום בשעה המפורטת.

תזמון המשימה - שבועי

המשימה תפעל באופן מחזורי מדי שבוע בימים ובשעות הנבחרים.

תזמון המשימה - הפעלה באמצעות אירוע

המשימה תופעל על-ידי אחד מהאירועים הבאים:

- **בכל פעם שהמחשב מופעל**
- **ההפעלה הראשונה של המחשב ביום**
- **חיבור בחיוג לאינטרנט/VPN**
- **עדכון מוצלח של מודולים**
- **עדכון מוצלח של המוצר**
- **התחברות של המשתמש**
- **זיהוי איום**

בעת תזמון משימה המופעלת על-ידי אירוע, באפשרותך לציין את מרווח הזמן המינימלי בין שתי השלמות של המשימה. לדוגמה, אם אתה מתחבר למחשב מספר פעמים ביום, בחר 24 שעות לביצוע המשימה רק בהתחברות הראשונה ביום, ואז ביום הבא.

דילוג על משימה

ניתן לדלג על משימה כאשר המחשב מופעל באמצעות סוללה או כבוי. בחר מתי יש להפעיל משימה שדילגת עליה מאחת מהאפשרויות הבאות ולחץ על **הבא**:

- **במועד המתוזמן הבא** – המשימה תופעל אם המחשב יופעל במועד המתוזמן הבא.
- **בהקדם האפשרי** – המשימה תופעל כאשר המחשב יופעל.
- **באופן מיידי, אם הזמן מאז ההפעלה המתוזמנת האחרונה חורג מ- (שעות)** – אפשרות זו מייצגת את הזמן שחלף מאז ההפעלה הראשונה של המשימה שעליה המערכת דילגה. אם אירעה חריגה מזמן זה, המשימה תופעל באופן מיידי.

באופן מיידי, אם הזמן מאז ההפעלה המתוזמנת האחרונה חורג מ- (שעות) - דוגמאות

לדוגמה, הוגדרה הפעלה מחזורית של משימה מדי שעה. האפשרות **באופן מיידי, אם הזמן מאז ההפעלה המתוזמנת האחרונה חורג מ- (שעות)** תיבחר והזמן לחריגה יוגדר לשעתיים. המשימה תפעל בשעה 13:00, וכאשר היא תסתיים, המחשב יעבור למצב שינה:

- המחשב יתעורר בשעה 15:30. המשימה הופעלה לראשונה בשעה 14:00. שעה וחצי בלבד חלפו מהשעה 14:00, ולכן המשימה תופעל בשעה 16:00.
- המחשב יתעורר בשעה 16:30. המשימה הופעלה לראשונה בשעה 14:00. חלפו שעתיים וחצי מהשעה 14:00, ולכן המשימה תופעל באופן מיידי.

פרטי משימה - עדכון

אם ברצונך לעדכן את התוכנית משני שרתי עדכון, הכרחי ליצור שני פרופילי עדכון שונים. אם הראשון לא מצליח להוריד את קובצי העדכון, התוכנית עוברת אוטומטית לפרופיל החלופי. מצב זה מתאים, לדוגמה, למחשבים ניידים, שבדרך-כלל מתעדכנים מרשת עדכון LAN מקומי, אולם בעליהם מרבים להתחבר לרשת דרך רשתות אחרות. לכן, אם הפרופיל הראשון נכשל, השני יוריד אוטומטית את קובצי העדכון משרתי העדכון של ESET.

פרטי משימה - הפעלת אפליקציה

משימה זו מתזמנת את ההפעלה של אפליקציה חיצונית.

קובץ הפעלה ▯ בחר קובץ הפעלה מעץ הספרייה, לחץ על האפשרות **...** או הזן את הנתיב ידנית.

תיקיית עבודה ▯ הגדר את ספריית העבודה של היישום החיצוני. כל הקבצים הזמניים של **קובץ ההפעלה** שנבחר ייווצרו בתוך ספרייה זו.

פרמטרים ▯ פרמטרים של שורת פקודה עבור היישום (אופציונלי).

לחץ על **סיום** כדי להחיל את המשימה.

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.

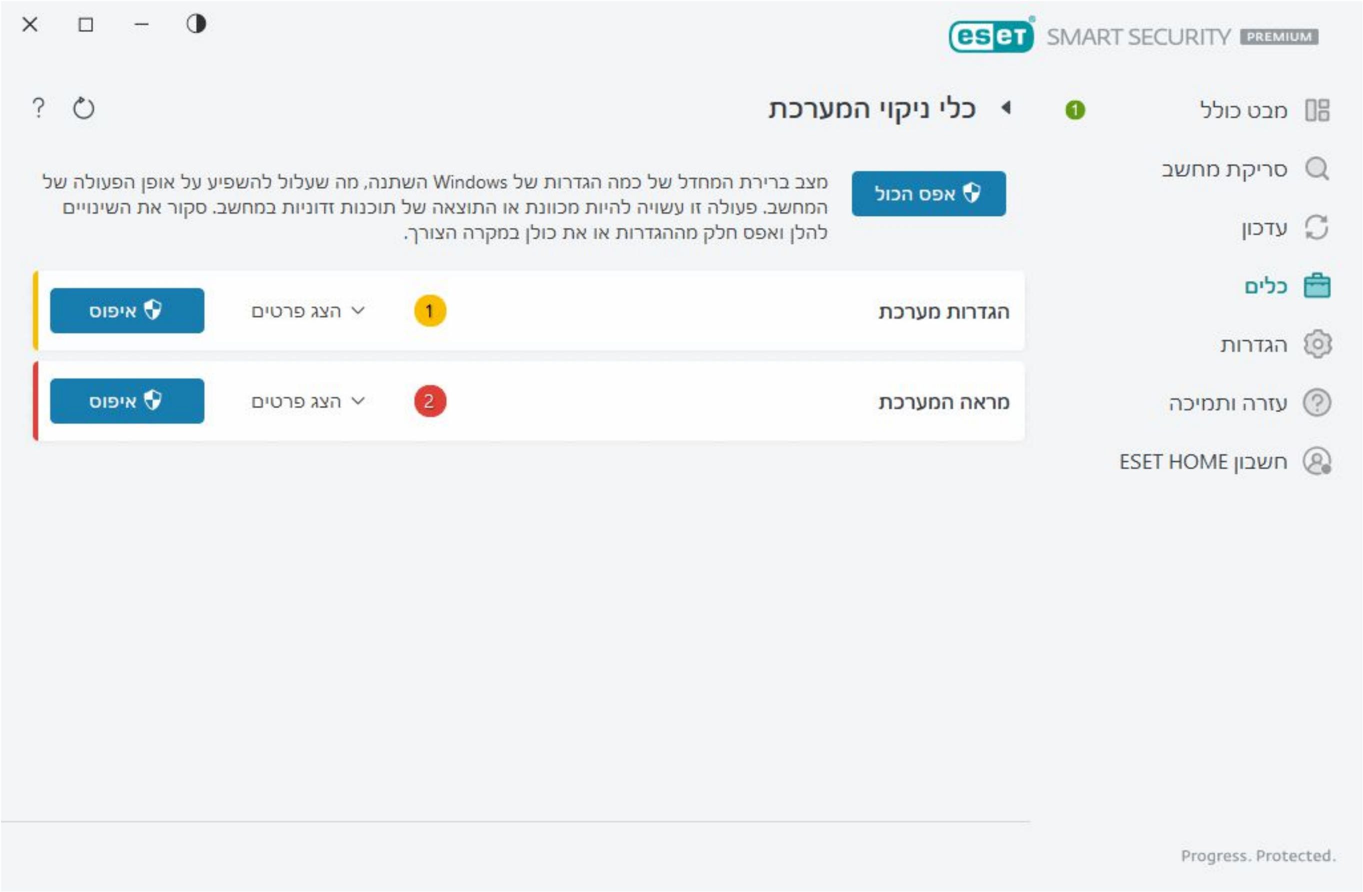
כלי ניקוי המערכת מדווח על בעיות מחמש קטגוריות של הגדרות:

- **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 למצב קודם

ניתן לבקש את ניקוי המערכת:

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

באפשרותך לסקור את השינויים ולאפס את ההגדרות במידת הצורך.



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

מפקח הרשת

התכונה 'מפקח הרשת' יכולה לעזור בזיהוי פגיעויות ברשת מהימנה (רשת ביתית או משרדית) (לדוגמה, יציאות פתוחות או סיסמה נתב חלשה). היא מספקת גם רשימה של ההתקנים המחוברים, עם חלוקה לקטגוריות לפי סוגי ההתקנים (לדוגמה, מדפסת, נתב, מכשיר נייד וכן הלאה), כדי להראות לך מה מחובר לרשת שלך (לדוגמה, קונסולת משחקים, IoT או התקנים אחרים של בית חכם).

מפקח הרשת מסייע לך לזהות את הפגיעויות בנתב ומעלה את רמת ההגנה כשאתה מחובר לרשת.

מפקח הרשת אינו מגדיר מחדש את תצורת הנתב במקומך. תבצע את השינויים בעצמך באמצעות הממשק הייעודי של הנתב. נתבים ביתיים יכולים להיות פגיעים במיוחד לתוכנות זדוניות המשמשות להפעלת מתקפות מבוזרות של מניעת שירות (DDoS). אם סיסמת הנתב המוגדרת כברירת מחדל לא השתנתה על-ידי המשתמש, קל להאקרים לנחש אותה ולאחר מכן להתחבר לנתב ולהגדיר מחדש את התצורה שלו או לחשוף את הרשת שלך לסכנה.

מומלץ בחום ליצור סיסמה חזקה וארוכה מספיק הכוללת מספרים, סימנים או אותיות רישיות. כדי להפוך את הסיסמה לקשה יותר לפיצוח, השתמש בשילוב של סוגי תווי שונים.

אם הרשת שאליה אתה מחובר מוגדרת כמהימנה, באפשרותך לסמן את הרשת בתור "הרשת שלי". לחץ על **סמן**

כ"הרשת שלי" כדי להוסיף תג של 'הרשת שלי' לרשת. תג זה יוצג לצד הרשת ב-ESET Smart Security Premium כדי לאפשר זיהוי טוב יותר ומבט כולל טוב יותר על האבטחה. לחץ על **בטל את הסימון כ"הרשת שלי"** כדי להסיר את התג.

כל התקן שמחובר לרשת שלך מוצג עם מידע בסיסי בתצוגת רשימה. לחץ על המכשיר הספציפי כדי לערוך את המכשיר או להציג מידע מפורט לגבי המכשיר.

התפריט הנפתח **רשתות** מאפשר לך לסנן התקנים בהתאם לקריטריונים הבאים:

- התקנים המחוברים לרשת ספציפית
- מכשירים המחוברים **לכל הרשתות**
- מכשירים ללא קטגוריה

לחץ על סמל המכשיר כדי לערוך את המכשיר או להציג מידע מפורט על המכשיר. מכשירים שחוברו לאחרונה מוצגים קרוב יותר לנתב כך שניתן לאתר אותם בקלות.

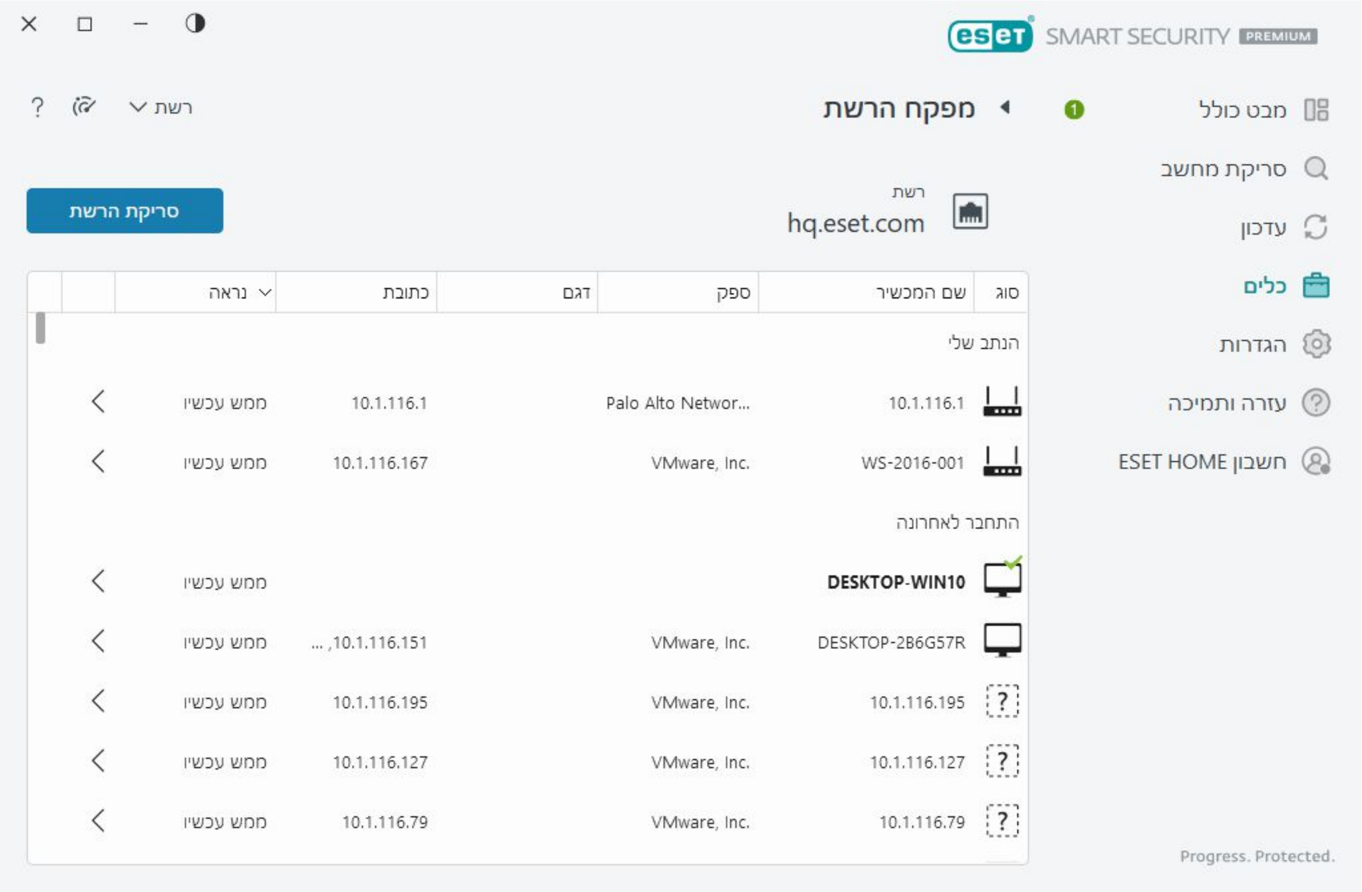
לחץ על גלגל השיניים בפינה השמאלית העליונה כדי לבחור אם להודיע כאשר מתגלה מכשיר חדש ברשת.

לחץ על **סרוק את הרשת שלך** כדי לבצע סריקה ידנית של הרשת שאליה אתה מחובר כעת. האפשרות **סרוק את הרשת שלך** זמינה רק לרשת מהימנה. ראה פרופילי חיבור רשת כדי לסקור או לערוך את הגדרות הרשת שלך.

באפשרותך לבחור מתוך אפשרויות הסריקה הבאות:

- סרוק הכל
- סרוק את הנתב בלבד
- סרוק מכשירים בלבד

בצע סריקות רשת רק ברשת מהימנה! אם תבצע את הפעולה ברשתות לא מהימנות, עליך להיות מודע לסכנה אפשרית.



בסיום הסריקה, תופיע התראה עם קישור למידע בסיסי על ההתקן או שבאפשרותך ללחוץ לחיצה כפולה על ההתקן החשוד בתצוגת רשימה או סונר. לחץ על **פתור בעיות** כדי לעיין בתקשורת שנחסמה לאחרונה. מידע נוסף על פתרון בעיות בחומת אש.

ישנם שני סוגים של התראות המוצגים באמצעות המודול 'מפקח הרשת':

- **התקן חדש מחובר לרשת** מוצגת אם התקן שלא נראה בעבר מתחבר לרשת כאשר המשתמש מחובר.
- **נמצאו התקני רשת חדשים** אפשרות זו תוצג אם תתחבר מחדש לרשת המהימנה שלך וימצא התקן שלא נראה בעבר.

שני סוגי ההתראות מיידעים אותך אם מכשיר בלתי מורשה מנסה להתחבר לרשת שלך. לחץ על **הצג את פרטי המכשיר** כדי להציג את הפרטים.

מה מציינים הסמלים המוצגים בהתקנים ב'מפקח הרשת'?

סמל הכוכב הצהוב מציין שההתקנים נוספו לאחרונה לרשת או שזהו האיתור הראשון שלהם על-ידי המוצר של ESET.	
סמל האזהרה הצהוב מציין שעשויות להיות חולשות בנתב. לחץ על הסמל במוצר כדי לקבל מידע מפורט יותר על הבעיה.	
סמל האזהרה האדום מציין שקיימות חולשות בנתב ושהוא עלול להיות נגוע. לחץ על הסמל במוצר כדי לקבל מידע מפורט יותר על הבעיה.	
הסמל הכחול עשוי להופיע כאשר יש למוצר של ESET מידע נוסף על הנתב אך מידע זה אינו מצריך פעולה מיידית מאחר שלא קיימים סיכוני אבטחה. לחץ על הסמל במוצר כדי לקבל מידע מפורט יותר.	

התקן רשת במפקח הרשת

באפשרותך למצוא כאן מידע מפורט על ההתקן, כולל הפרטים הבאים:

- שם המכשיר
- סוג התקן

- נראה לאחרונה
- שם רשת
- כתובת IP
- כתובת MAC
- מערכת הפעלה

סמל העיפרון מציין שבאפשרותך לשנות את שם המכשיר או את סוג המכשיר.

הסר מההיסטוריה מחק את המכשיר מרשימת המכשירים. אפשרות זו זמינה רק עבור מכשירים שאינם מחוברים לרשת שלך כרגע.

לכל סוג התקן, הפעולות הבאות זמינות:

נתב

הגדרות נתב - גש אל הגדרות הנתב מהממשק האינטרנטי, מהאפליקציה לנייד או לחץ על **פתח את ממשק הנתב**. אם יש לך נתב שסופק על-ידי ספק שירותי האינטרנט שלך, ייתכן שתצטרך לפנות אל משאבי התמיכה של ספק שירותי האינטרנט או אל יצרן הנתב כדי לפתור בעיות אבטחה שאותרו. הישמע תמיד להוראות הבטיחות הנאותות כפי שצוינו במדריך למשתמש של הנתב שלך.
הגנה כדי להגן על הנתב ועל הרשת שלך מפני התקפות של אבטחת סייבר, פעל בהתאם להמלצות בסיסיות אלה.

התקן רשת

זיהוי התקן - אם אינך בטוח לגבי ההתקן המחובר לרשת שלך, בדוק את שם הספק או היצרן מתחת לשם ההתקן. הדבר יכול לסייע לך לזהות באיזה סוג התקן מדובר. ניתן לשנות את שם ההתקן לשימוש בעתיד.
ניתוק ההתקן - אם אינך בטוח שהתקן מחובר בטוח לרשת או להתקנים שלך, נהל את הגישה לרשת עבור התקן זה בהגדרות הנתב שלך או שנה את סיסמת הרשת.
הגנה - כדי להגן על ההתקן שלך מפני מתקפות ותוכנה זדונית, התקן הגנה של אבטחת סייבר בהתקן שלך ושמור תמיד על עדכניות מערכת ההפעלה והתוכנה המותקנת. כדי להישאר מוגן, אל תתחבר לרשתות Wi-Fi לא מאובטחות.

התקן זה

התקן זה מייצג את המחשב שלך ברשת.
מתאמי רשת - מציג את פרטי מתאמי הרשת שלך.

התראות | מפקח הרשת

להלן מספר התראות שעשויות להיות מוצגות כאשר ESET Smart Security Premium מזהה בעיית פגיעות מסוימת בנתב שלך. כל התראה כוללת תיאור קצר ומספקת פתרונות מסוימים או פעולות מסוימות שיש לבצע כדי למזער את הסיכון לפגיעות בנתב שלך. אם אינך מכיר את השינויים בנתב, אנו ממליצים לפנות ליצרן הנתב או לספק האינטרנט.

נמצאה נקודת חולשה פוטנציאלית
ייתכן שבנתב שלך יש נקודות חולשה שעלולות להקל על התקפות עליו וניצולו. עדכן את קושחת הנתב שלך.

נמצאה נקודת חולשה
בנתב שלך יש נקודות חולשה ידועות שבגללן קל להתקיפו. עדכן את קושחת הנתב שלך.

נמצא איום
הנתב שלך נגוע בתוכנה זדונית. הפעל מחדש את הנתב וחזור על הסריקה.

סיסמת נתב חלשה
הסיסמה בנתב שלך חלשה ומישהו אחר יכול לנחש אותה בקלות. שנה את הסיסמה בנתב.

הפניה מחדש זדונית לרשת
נראה שהתנועה שלך באינטרנט מופנית לאתרים זדוניים. ייתכן שפירוש הדבר שהנתב שלך נחשף לסכנה. שנה את ההגדרה של שרת ה-DNS בנתב.

פתח שירותי רשת
הנתב שלך מפעיל שירותי רשת שמישהו אחר עלול לנצל לרעה. ייתכן שהדבר נובע מתצורה שגויה או מנתב שנחשף לסכנה. בדוק את תצורת הנתב.

שירותים רגישים של רשת פתוחה
לך מפעיל שירותי רשת רגישים שמישהו אחר עלול לנצל לרעה. ייתכן שהדבר נובע מתצורה שגויה או מנתב שנחשף לסכנה. בדוק את תצורת הנתב.

קושחה מיושנת
הקושחה בנתב שלך מיושנת ועלולה לכלול נקודות חולשה. עדכן את הקושחה בנתב.

הגדרה של נתב זדוני
שרת DNS זה שבו הנתב שלך משתמש הנו זדוני והוא עלול לשלוח אותך לאתרים זדוניים. ייתכן שפירוש הדבר שהנתב שלך נחשף לסכנה. שנה את ההגדרה של שרת ה-DNS בנתב.

שירותי רשת
הנתב שלך מפעיל שירותי רשת נפוצים. שירותים אלה נחוצים לפעולת הרשת וסביר להניח שהם בטוחים. בדוק את תצורת הנתב.

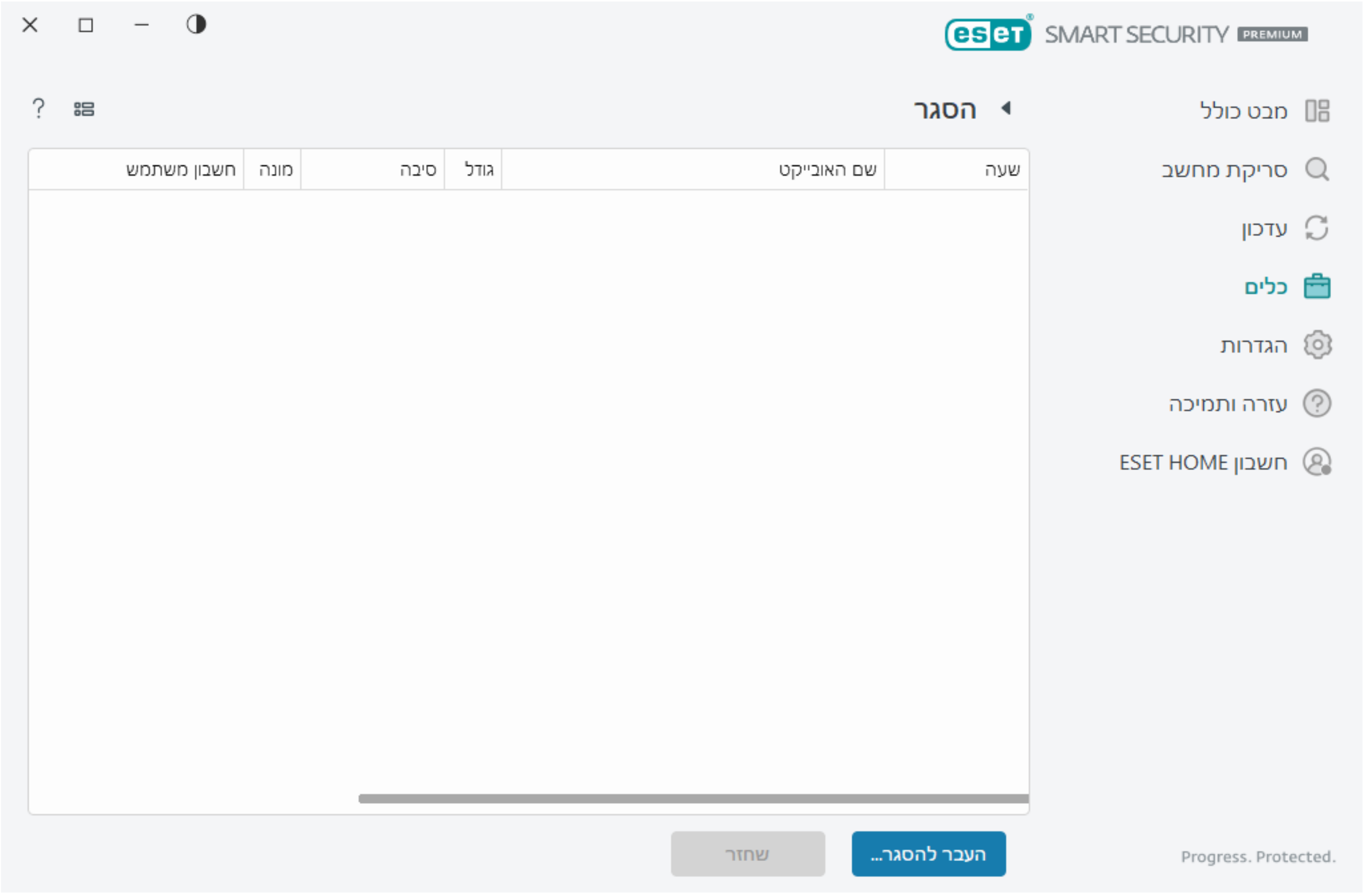
הסגר

התפקיד העיקרי של ההסגר הוא אחסון של קבצים מדווחים באופן בטוח (כגון תוכנות זדוניות, קבצים נגועים או אפליקציות העלולות להיות לא רצויות).

ניתן לגשת אל ההסגר מחלון התוכנית הראשי של ESET Smart Security Premium על-ידי לחיצה על **כלים** > **הסגר**.

ניתן להציג את הקבצים המאוחסנים בתיקיית ההסגר בטבלה שמציגה:

- את תאריך ושעת ההסגר,
- את הנתיב למיקום המקורי של הקובץ,
- את הגודל בבתים,
- סיבה (לדוגמה, האובייקט נוסף על-ידי המשתמש),
- ומספר של אובייקטים מזוהים (לדוגמה, אובייקטים מזוהים כפולים של אותו קובץ או אם הקובץ הוא ארכיון שמכיל מספר חדירות).



העברת קבצים להסגר

ESET Smart Security Premium מעביר באופן אוטומטי קבצים שנמחקו להסגר (אם לא ביטלת אפשרות זו בחלון ההתראות).

יש להעביר להסגר קבצים נוספים אם:

a. הם לא ניתנים לניקוי,
b. לא בטוח או לא מומלץ למחוק אותם,
c. הם מאותרים באופן שגוי על-ידי ESET Smart Security Premium,
d. קובץ פועל בצורה חשודה אך אינו מאותר על-ידי ההגנות.

כדי להוסיף קובץ להסגר, עומדות לרשותך מספר אפשרויות:

a. השתמש בתכונה של גרירה ושחרור כדי להעביר קובץ באופן ידני להסגר על-ידי לחיצה על הקובץ, העברת סמן העכבר לאזור המסומן תוך לחיצה על לחצן העכבר ולאחר מכן שחרור הלחיצה. לאחר מכן, האפליקציה תועבר לחזית.
b. לחץ באמצעות לחצן העכבר הימני על הקובץ > לחץ על **אפשרויות מתקדמות** > **הסגר קובץ**.
c. לחץ על **העבר להסגר** מחלון **הסגר**.
d. ניתן להשתמש בתפריט ההקשר גם למטרה זו; לחץ באמצעות לחצן העכבר הימני על החלון **הסגר** ואז בחר **הסגר**.

שחזור מההסגר

ניתן לשחזר קבצים שהועברו להסגר למיקומם המקורי:

- השתמש למטרה זו בתכונה **שחזור** הזמינה בתפריט ההקשר על-ידי לחיצה על קובץ נתון בהסגר באמצעות לחצן העכבר הימני.
- אם קובץ מסומן כאפליקציה העלולה להיות לא רצויה, האפשרות **שחזר ואל תכלול בסריקה** מאופשרת. ראה גם אי הכללות.
- תפריט ההקשר גם מציע אפשרות **שחזור אל** שמאפשרת לך לשחזר קובץ במיקום שונה מזה שממנו נמחק.
- פונקציית השחזור אינה זמינה במקרים מסוימים, לדוגמה עבור קבצים הממוקמים במיקום משותף לקריאה בלבד ברשת.

מחיקה מההסגר

לחץ באמצעות לחצן העכבר הימני על פריט נתון ובחר באפשרות **הסר מהסגר**, או בחר בפריט שאותו ברצונך להסיר והקש על מקש **Delete** במקלדת. אם ברצונך לבחור ולמחוק את כל הפריטים בהסגר, תוכל להקיש **Ctrl + A** ולאחר מכן **Delete** במקלדת. פריטים שנמחקו יוסרו לצמיתות מהמכשיר שלך ומההסגר.

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 הדגימה למעבדת המחקר של ESET. כדי לשלוח קובץ, לחץ על הקובץ באמצעות לחצן העכבר הימני ובחר באפשרות **שלח לניתוח** מתוך תפריט ההקשר.

תיאור האיתור

לחץ באמצעות לחצן העכבר הימני על פריט ולחץ על **תיאור האיתור** לפתיחת אנציקלופדיית האיומים של ESET, אשר כוללת מידע מפורט אודות הסכנות והתסמינים של החדירה שתועדה.

> **הנחיות מאוירות**
>
> מאמר מאגר הידע הבא של ESET עשוי להיות זמין באנגלית בלבד:
> - שחזור קובץ שהועבר להסגר ב-ESET Smart Security Premium
> - מחיקת קובץ שהועבר להסגר ב-ESET Smart Security Premium
> - קיבלתי הודעה על איתור מהמוצר של ESET – מה עליי לעשות?

ההסגר נכשל

סיבות לכך שלא ניתן להעביר קבצים מסוימים להסגר:

- **אין לך הרשאות קריאה** כך שאינך יכול להציג את תוכן הקובץ.
- **אין לך הרשאות כתיבה** כך שאינך יכול לשנות את תוכן הקובץ, כלומר להוסיף תוכן חדש או להסיר את התוכן הישן.
- **הקובץ שאתה מנסה להעביר להסגר גדול מדי** עליך להקטין את גודל הקובץ.

כשמופיעה הודעת השגיאה "ההסגר נכשל", לחץ על **מידע נוסף**. רשימת שגיאות הסגר מופיעה ותראה את שם הקובץ ואת הסיבה לכך שלא ניתן להעבירו להסגר.

בחירת דוגמה לניתוח

אם אתה מאתר במחשב קובץ חשוד או אתר אינטרנט חשוד, באפשרותך לשלוח אותו לניתוח במעבדת המחקר של ESET (ייתכן שאפשרות זו לא תהיה זמינה בהתאם לאופן שבו הגדרת את התצורה של ESET LiveGrid®).

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** > **שלח דגימה לניתוח**. הגודל המקסימלי של דגימה שנשלחת הוא 256MB.
2. לחלופין, תוכל לשלוח את הקובץ בדואר אלקטרוני. 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),
- אתר תוצאה חיובית מוטעית
- קובץ של תוצאה חיובית מוטעית (קובץ שזוהה כנגוע למרות שאינו נגוע),
- 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 להוסיף פרטים או תיאורים שיסייעו בעיבוד הקובץ החשוד.

> 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 נעשה שימוש בפישינג לשם קבלת גישה לנתונים רגישים, כגון מספרים של חשבונות בנק, מספרי PIN, ועוד. קרא עוד על סוג המתקפה הזה ב<u>מילון</u>.
- **הונאה** – אתר אינטרנט לרמייה או להונאה, במיוחד להפקת רווח מהיר.
- בחר באפשרות **אחר** אם האפשרויות לעיל אינן מתייחסות לאתר שאותו תשלח.

הערות ומידע נוסף – באפשרותך להקליד מידע נוסף או תיאור 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.

> 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 אתר האינטרנט החשוד.

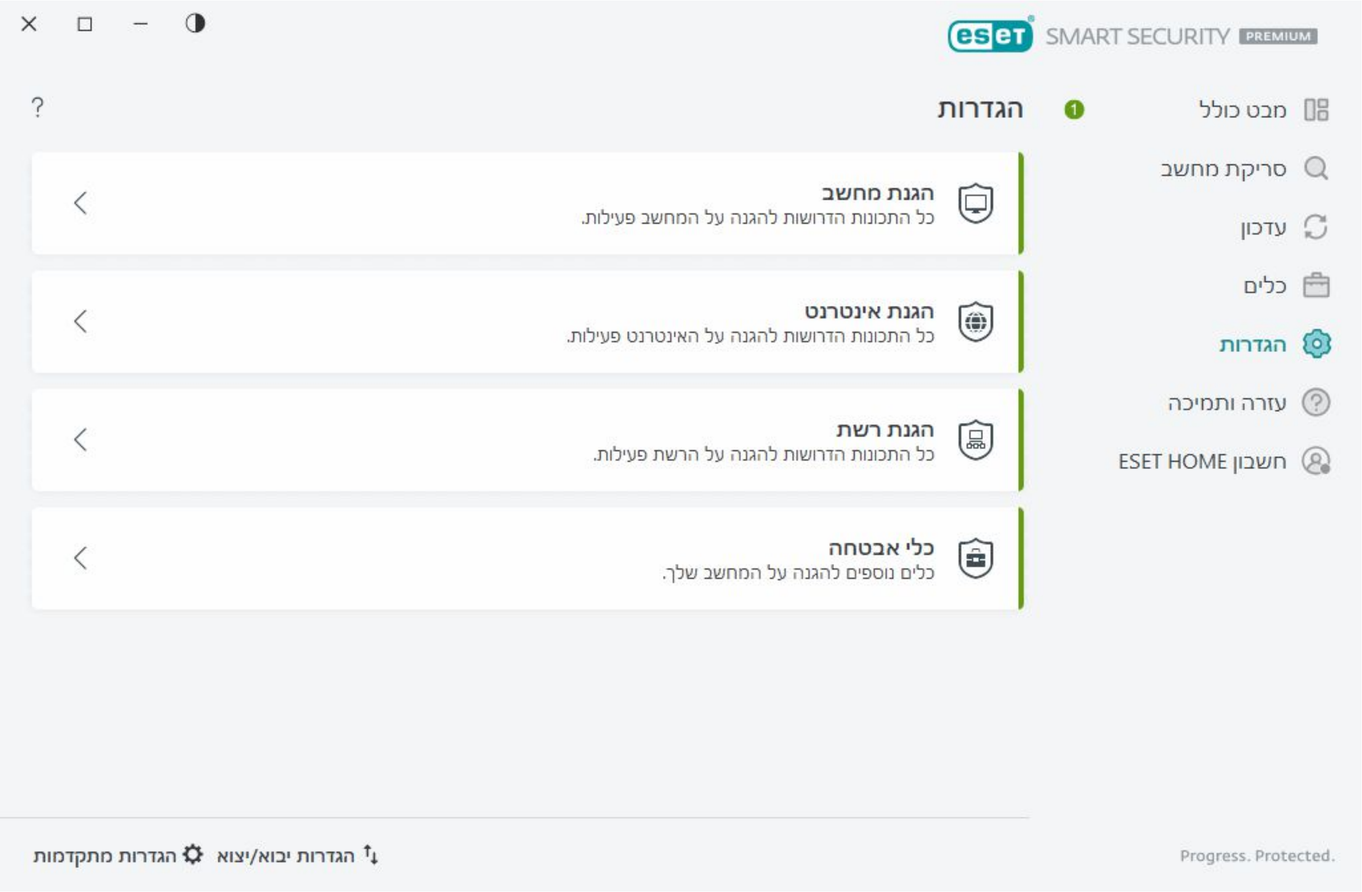
בחר דגימה לשליחה ולניתוח - אחר

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.

הגדרות

ניתן למצוא קבוצת של תכונות הגנה זמינות בחלון התוכנית הראשי > **הגדרות**.



התפריט **הגדרות** מחולק לקבוצות הבאות:

הגנת מחשב

הגנת אינטרנט

הגנת רשת

כלי אבטחה

אפשרויות נוספות זמינות בחלק התחתון של חלון ההגדרות. לחץ על הגדרות מתקדמות כדי להגדיר פרמטרים מפורטים יותר לכל מודול. השתמש בהגדרות יבוא/יצוא כדי לטעון פרמטרי הגדרות באמצעות קובץ תצורה מסוג .xml או כדי לשמור את פרמטרי ההגדרות הנוכחיים שלך בקובץ תצורה.

הגנת מחשב

לחץ על **הגנת מחשב** בחלון התוכנית הראשי > **הגדרה** כדי לראות סקירה כללית של כל מודולי ההגנה:

- הגנה בזמן אמת על מערכת קבצים כל הקבצים נסרקים לאיתור קוד זדוני בעת פתיחתם, יצירתם או הפעלתם.
- ESET LiveGuard מוסיף שכבה של הגנה מבוססת ענן שתוכננה במיוחד לצמצום איומים שטרם נראו בעבר.
- הגנה פרואקטיבית חסימת ההפעלה של קבצים חדשים עד לקבלת תוצאת הניתוח של ESET LiveGuard. אם ברצונך לבטל את החסימה של הקובץ המנותח, לחץ באמצעות לחצן העכבר הימני על הקובץ ולחץ על **בטל את חסימת הקובץ המנותח באמצעות ESET LiveGuard**.
- 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.

כדי להשהות או להשבית מודולי הגנה נפרדים, לחץ על הסמל של המתג .

השבתה של מודולי ההגנה עלולה להפחית את רמת ההגנה של המחשב.

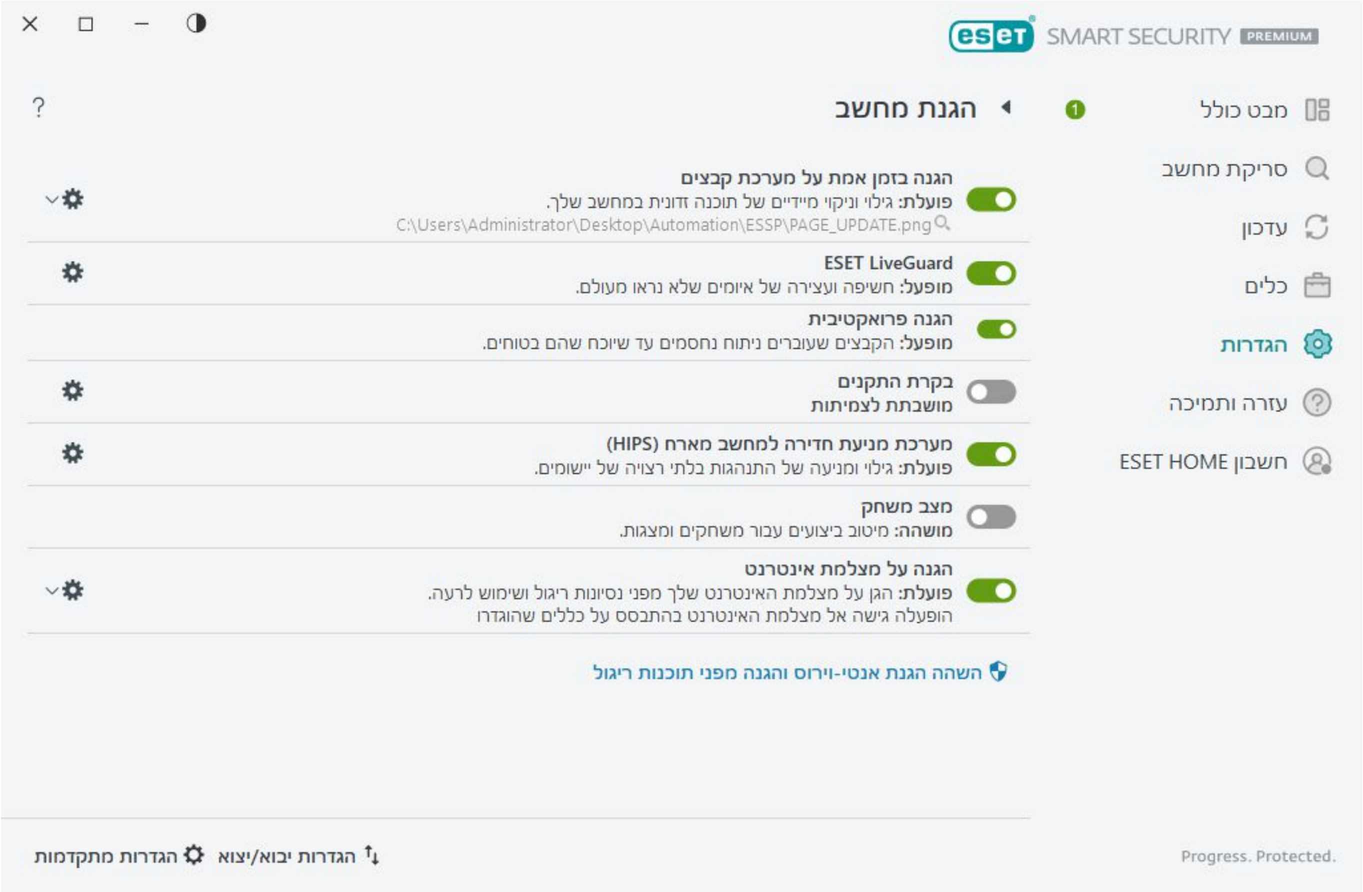
לחץ על סמל גלגל השיניים שלצד מודול ההגנה כדי לגשת אל ההגדרות המתקדמות של מודול זה.

עבור **הגנה בזמן אמת על מערכת קבצים**, לחץ על סמל גלגל השיניים ובחר מתוך האפשרויות הבאות:

- **קביעת תצורה** פתיחת ההגדרות המתקדמות של הגנה בזמן אמת על מערכת קבצים.
- **עריכת אי-הכללות** פתיחת חלון ההגדרות של החרגות על מנת לאפשר לך לא לכלול קבצים ותיקיות בסריקה.

עבור **הגנת מצלמת אינטרנט**, לחץ על סמל גלגל השיניים ובחר מתוך האפשרויות הבאות:

- **קביעת תצורה** פתיחת ההגדרות המתקדמות של הגנת מצלמת אינטרנט.
- **חסום כל גישה עד להפעלה מחדש** חסימת כל גישה למצלמת האינטרנט עד להפעלה מחדש של המחשב.
- **חסום כל גישה לצמיתות** חסימת כל גישה למצלמת האינטרנט עד להשבתה של הגדרה זו.
- **הפסק לחסום כל גישה** השבתת היכולת לחסימה של הגישה למצלמת האינטרנט. אפשרות זו זמינה רק אם הגישה למצלמת האינטרנט חסומה.



השהה אנטי-וירוס והגנה מפני תוכנות ריגול – השבתת כל המודולים של אנטי-וירוס והגנה מפני תוכנות ריגול. כשאתה משבית הגנה, ייפתח חלון שבו באפשרותך לקבוע למשך כמה זמן ההגנה תושבת, באמצעות התפריט הנפתח **מרווח זמן**. השתמש באפשרות זו רק אם אתה משתמש מנוסה או אם קיבלת הנחיה לכך מהתמיכה הטכנית של ESET.

זוהתה חדירה

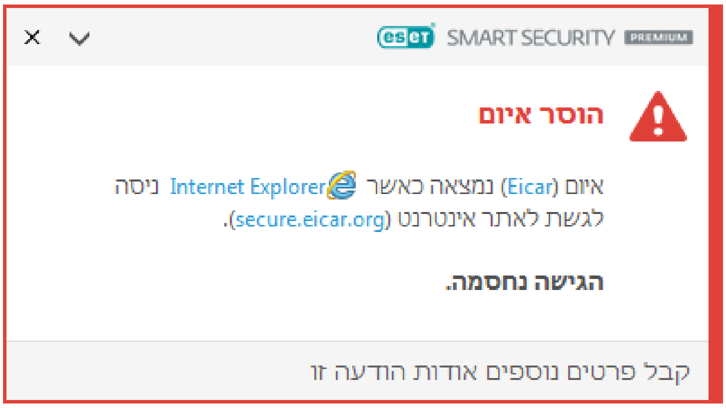
חדירות יכולות להגיע למערכת מנקודות כניסה שונות, כגון דפי אינטרנט, תיקיות משותפות, דרך הדוא"ל או מהתקנים נשלפים (USB, דיסקים חיצוניים, תקליטורים, DVD וכו').

אופן הפעולה הרגיל

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

- הגנה בזמן אמת על מערכת קבצים
- הגנת 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. למידע מפורט על האובייקטים שזוהו/נוקו, ראה רשומות יומן. לקבלת מידע נוסף על רמות הניקוי ואופן הפעולה, ראה רמות ניקוי.



סריקת המחשב לאיתור קבצים נגועים

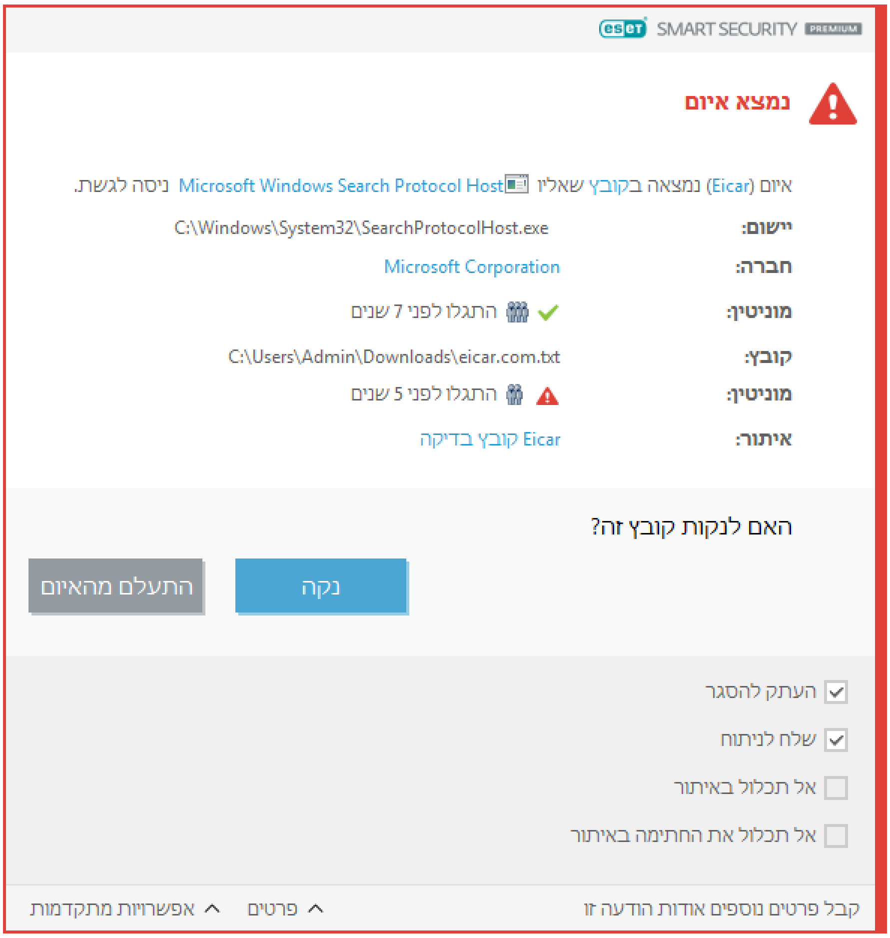
אם במחשב שלך מופיעים סימנים של הדבקה בתוכנה זדונית, למשל האטה בפעילות, או חוסר תגובה לעתים קרובות, מומלץ לבצע את הפעולות הבאות:

1. פתח את ESET Smart Security Premium 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.

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 **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).

שחזור מההסגר

ניתן לגשת אל ההסגר מחלון התוכנית הראשי של ESET Smart Security Premium על-ידי לחיצה על **כלים** > **הסגר**.

ניתן לשחזר קבצים שהועברו להסגר למיקומם המקורי:

- השתמש למטרה זו בתכונה **שחזור** הזמינה בתפריט ההקשר על-ידי לחיצה על קובץ נתון בהסגר באמצעות לחצן העכבר הימני.
- אם קובץ מסומן כאפליקציה העלולה להיות לא רצויה, האפשרות **שחזר ואל תכלול בסריקה** מאופשרת. ראה גם אי הכללות.
- תפריט ההקשר גם מציע אפשרות **שחזור אל** שמאפשרת לך לשחזר קובץ במיקום שונה מזה שממנו נמחק.
- פונקציית השחזור אינה זמינה במקרים מסוימים, לדוגמה עבור קבצים הממוקמים במיקום משותף לקריאה בלבד ברשת.

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

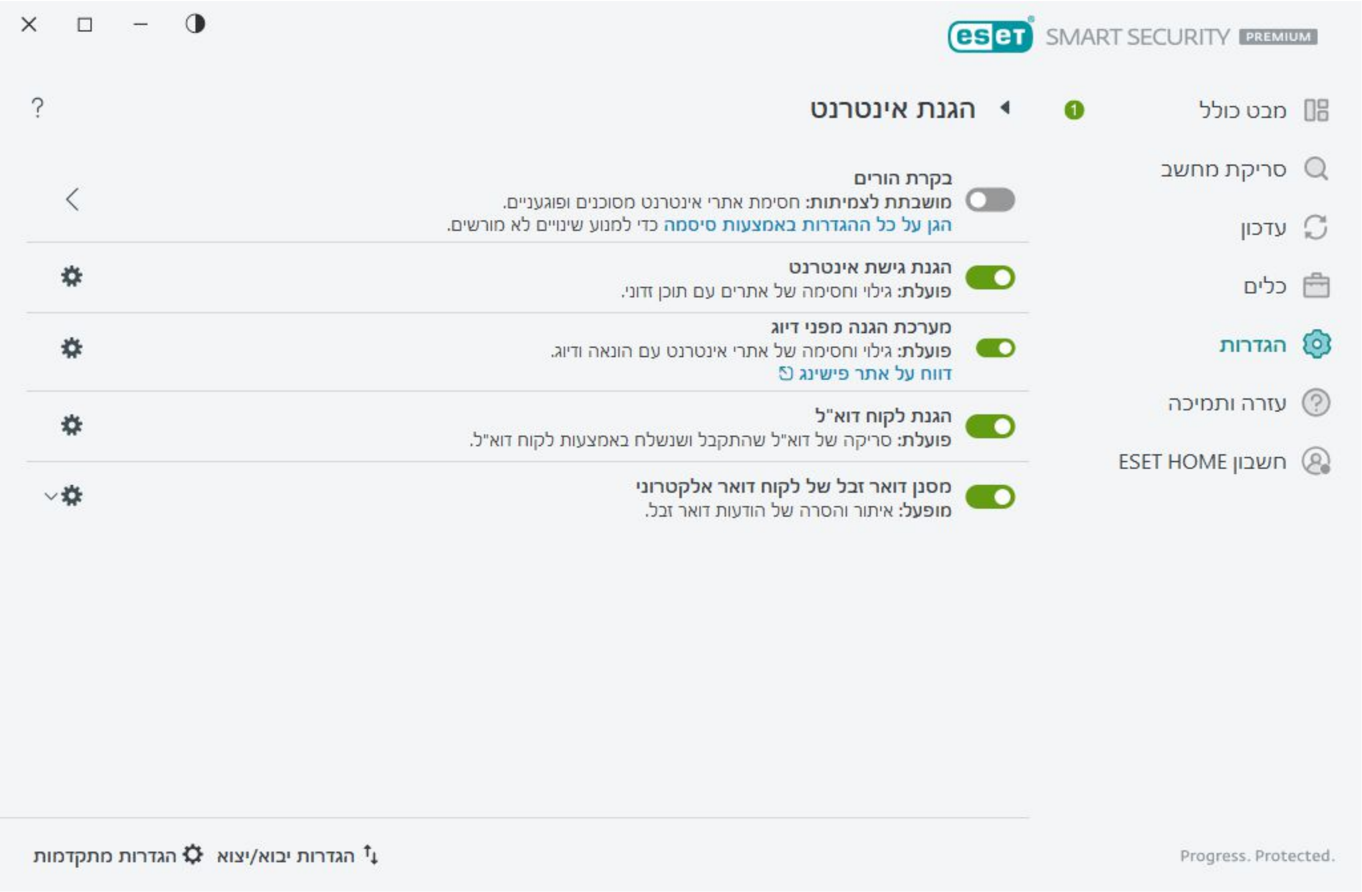
במצב הניקוי שנקבע כברירת מחדל, הארכיון כולו יימחק רק אם הוא מכיל קבצים נגועים בלבד, ואין בו קבצים נקיים. במילים אחרות, ארכיונים אינם נמחקים אם הם מכילים גם קבצים נקיים שאינם מזיקים. היזהר כשאתה מבצע סריקה עם ניקוי מחמיר, מפני שכאשר ניקוי מחמיר מופעל - ארכיון יימחק אם הוא מכיל לפחות קובץ נגוע אחד, ללא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

הגנת אינטרנט

קישוריות אינטרנט היא תכונה סטנדרטית במחשב אישי. למרבה הצער, היא גם הפכה לאמצעי הראשי להעברת קודים זדוניים. פתח את חלון התוכנית הראשי > **הגדרה** > **הגנת אינטרנט** כדי להגדיר תכונות ב-ESET Smart Security Premium שמשפרות את הגנת האינטרנט שלך.

כדי להשהות או להשבית מודולי הגנה נפרדים, לחץ על הסמל של המתג.

ההשבתה של מודולי ההגנה עלולה להפחית את רמת ההגנה של המחשב.



לחץ על סמל גלגל השיניים שלצד מודול ההגנה כדי לגשת אל ההגדרות המתקדמות של מודול זה.

המודול בקרת הורים מגן על ילדיך על ידי חסימת תוכן מזיק או בלתי הולם באינטרנט.

הגנת גישה לאינטרנט סורקת תקשורת HTTP/HTTPS לאיתור תוכנות זדוניות ודיוג. יש לכבות את ההגנה על גישה לאינטרנט רק לצורך פתרון בעיות.

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

דווח על אתר דיוג - דווח ל-ESET על אתר אינטרנט של פישינג/זדוני לצורך ניתוח.

> לפני שתשלח אתר אינטרנט אל ESET, ודא שהוא עומד באחד או יותר מהקריטריונים הבאים:
> • אתר האינטרנט לא זוהה כלל.
> • אתר האינטרנט זוהה כאיום באופן שגוי. אם זה המקרה, באפשרותך לדווח על דף שנחסם בשוגג.

הגנת לקוח דוא"ל מספקת בקרה על תקשורות דוא"ל המתקבלות באמצעות הפרוטוקולים (POP3(S ו-(IMAP(S.
באמצעות תוכנית התוסף ללקוח הדוא"ל שלך, ESET Smart Security Premium מספק בקרה על כל התקשורת אל לקוח הדוא"ל שלך וממנו.

אנטי ספאם בלקוח דוא"ל מסנן הודעות דואר אלקטרוני לא רצויות.

עבור **אנטי ספאם בלקוח דוא"ל**, לחץ על סמל גלגל השיניים ⚙ ובחר מבין האפשרויות הבאות:

- **קבע תצורה** פותח את ההגדרות המתקדמות עבור הגנת אנטי ספאם בלקוח דוא"ל.
- **רשימת כתובות של המשתמש** (אם מופעלת) פתיחת חלון דו-שיח שבו באפשרותך להוסיף, לערוך או להסיר כתובות לצורך הגדרה של כללי מסנן דואר זבל. הכללים ברשימה זו יוחלו על המשתמש הנוכחי.
- **רשימת כתובות כללית** (אם מופעלת) פתיחת חלון דו-שיח שבו באפשרותך להוסיף, לערוך או להסיר כתובות לצורך הגדרה של כללי מסנן דואר זבל. הכללים ברשימה זו יוחלו על כל המשתמשים.

הגנת אנטי-פישינג

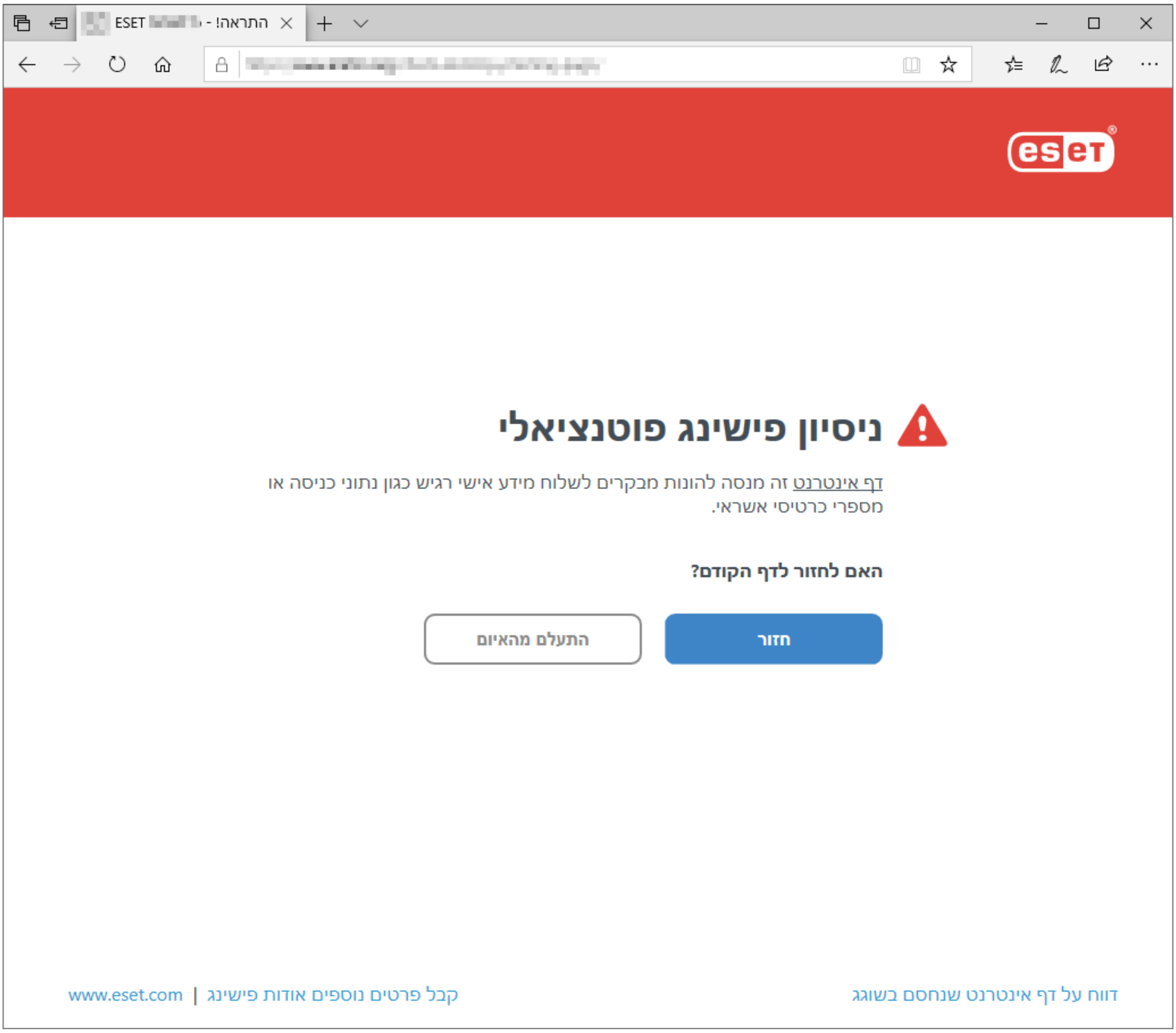
פישינג היא פעילות פלילית המשתמשת בהנדסה חברתית (מניפולציה של משתמשים כדי להשיג מידע סודי). לעתים קרובות נעשה שימוש בפישינג לשם גישה לנתונים רגישים, כגון מספרים של חשבונות בנק, מספרי PIN וכדומה. קרא עוד על פעילות זו במילון. ESET Smart Security Premium כולל הגנה מפני פישינג, אשר חוסמת דפי אינטרנט שידוע שמפיצים תוכן מסוג זה.

הגנת אנטי-פישינג מאופשרת כברירת מחדל. ניתן לקבוע את התצורה של הגדרה זו דרך הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט**.

בקר במאמר מאגר הידע שלנו לקבלת מידע נוסף על הגנה מפני פישינג במוצר ESET Smart Security Premium.

גישה לאתר אינטרנט המשמש לפישינג

כאשר אתה מבקר באתר אינטרנט המזוהה כאתר פישינג, הדפדפן יציג את תיבת הדו-שיח להלן. אם אתה עדיין רוצה לגשת לאתר האינטרנט, לחץ על **התעלם מהאיום** (לא מומלץ).



כברירת מחדל, תוקף ההימצאות של אתרי פישינג פוטנציאליים ברשימה הלבנה יפוג לאחר מספר שעות. כדי לאשר אתר אינטרנט מסוים לצמיתות, השתמש בכלי ניהול כתובות URL. תחת הגדרות מתקדמות > **הגנות** > **הגנה על גישה לאינטרנט** > **ניהול כתובות URL** > **רשימת כתובות** > **עריכה** ולאחר מכן הוסף לרשימה את אתר האינטרנט שברצונך לערוך.

דווח על אתר פישינג

הקישור **דווח על דף חסום באופן לא תקין** מאפשר לך לדווח על אתר אינטרנט שזוהה באופן שגוי כאיום.

לחלופין, תוכל לשלוח את פרטי אתר האינטרנט בדואר אלקטרוני. שלח את הודעת הדואר האלקטרוני לכתובת samples@eset.com. זכור להשתמש בנושא תיאורי וצרף כמה שיותר מידע על אתר האינטרנט (לדוגמה אתר האינטרנט שהפנה אותך לכאן, כיצד שמעת על אתר זה, וכו').

בקרת הורים

מודול בקרת ההורים מאפשר לך לקבוע את הגדרות בקרת ההורים, אשר מספקות להורים כלים אוטומטיים שמסייעים בהגנה על הילדים ומגבילים מכשירים ושירותים. המטרה היא למנוע מילדים ומצעירים לגשת לדפים

המכילים תוכן פוגעני או בלתי הולם.

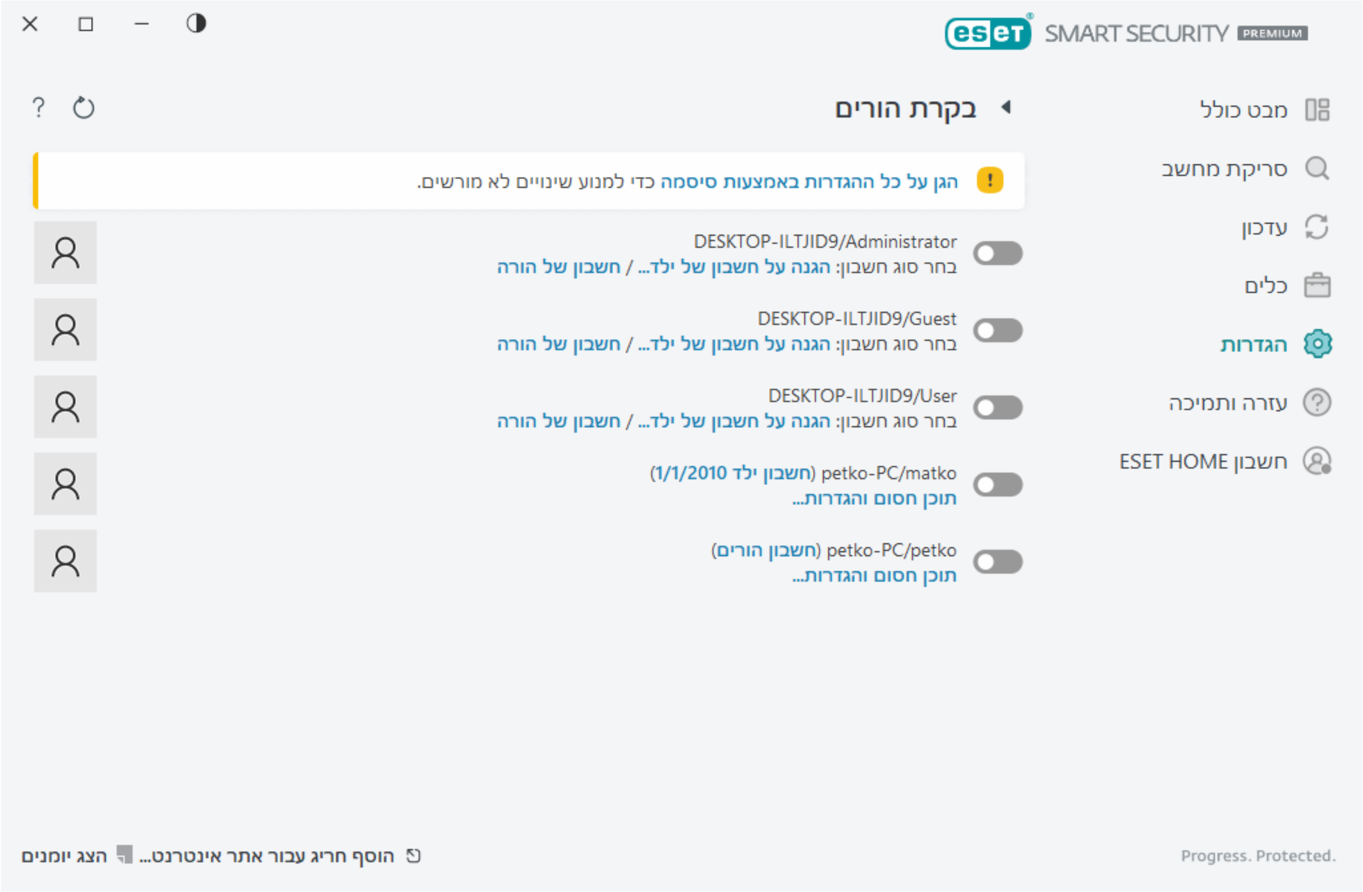
בקרת הורים מאפשרת לך לחסום דפי אינטרנט שייתכן שמכילים תוכן שעשוי להיות פוגעני. בנוסף, הורים יכולים לאסור גישה ליותר מ-40 קטגוריות אתרים ויותר מ-140 קטגוריות-משנה שהוגדרו מראש.

כדי להפעיל בקרת הורים של חשבון משתמש ספציפי, בצע את הפעולות הבאות:

1. כברירת מחדל, בקרת הורים מושבתת במוצר ESET Smart Security Premium. ישנן שתי שיטות להפעלת בקרת הורים:

- לחץ על הסמל במקטע **הגדרות** > **הגנת אינטרנט** > **בקרת הורים** בחלון התוכנית הראשי והעבר את מצב בקרת ההורים למצב מופעל.
- פתח את הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **בקרת הורים** ולאחר מכן הפעל את המתג שליד **הפעל בקרת הורים**.

2. לחץ על **הגדרות** > **הגנת אינטרנט** > **בקרת הורים** בחלון התוכנית הראשי. למרות שהאפשרות **מופעל** מופיעה לצד **בקרת הורים**, עליך להגדיר את בקרת ההורים לחשבון הרצוי על-ידי לחיצה על סמל החץ ולאחר מכן לחיצה על **הגן על חשבון ילד** או על **חשבון הורים** בחלון הבא. 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.



אם תלחץ על **הגדרות** > **הגנת אינטרנט** > **בקרת הורים** בחלון המוצר הראשי של ESET Smart Security Premium, תראה שהחלון הראשי מכיל:

חשבונות של משתמשי Windows

אם יצרת תפקיד לחשבון קיים, הוא יוצג כאן. לחץ על המתג כך שיציג סימן ביקורת ירוק לצד בקרת ההורים עבור החשבון. תחת החשבון הפעיל, לחץ על תוכן חסום והגדרות כדי להציג את רשימת קטגוריות דפי האינטרנט המותרות עבור חשבון זה ואת דפי האינטרנט החסומים והמותרים.

החלק התחתון של החלון כולל

הוסף חריג עבור אתר אינטרנט ניתן לחסום או להתיר את אתר האינטרנט הספציפי בהתאם להעדפותיך עבור כל אחד מחשבונות ההורה בנפרד.

הצג יומנים מציג רישום מפורט של פעילות בקרת ההורים (דפים שנחסמו, החשבון, הסיבה לחסימת הדף, קטגוריה, וכו'). באפשרותך גם לסנן יומן זה על-פי הקריטריונים שתבחר על-ידי לחיצה על **סינון**.

בקרת הורים

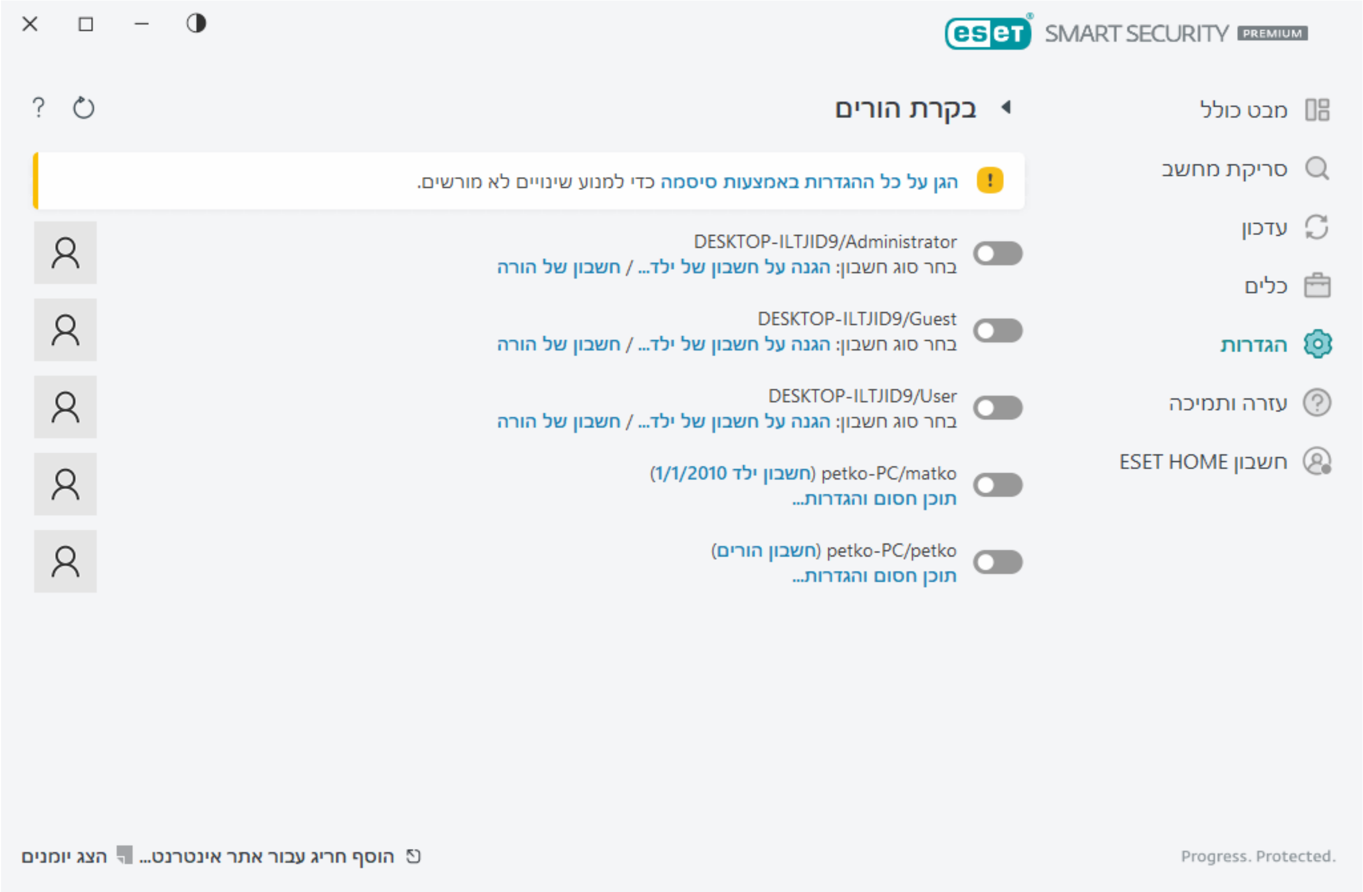
לאחר השבתת בקרת ההורים יופיע חלון **השבתת בקרת הורים**. כאן תוכל להגדיר את מרווח הזמן שבו ההגנה תושבת. האפשרות תשונה ל**מושהית** או **מושבתת לצמיתות**.

חשוב להגן את ההגדרות במוצר ESET Smart Security Premium באמצעות סיסמה. סיסמה זו ניתן להגדיר במקטע הגדרות גישה. אם לא הוגדרה סיסמה, תופיע אזהרה בנוסח הבא **הגן על בקרת כל ההגדרות באמצעות סיסמה** כדי למנוע שינויים בלתי מורשים. ההגבלות המוגדרות בבקרת ההורים משפיעות רק על חשבונות המשתמש הרגילים. מאחר שמנהל מערכת יכול להחליף כל הגבלה, לא תהיה להן כל השפעה.

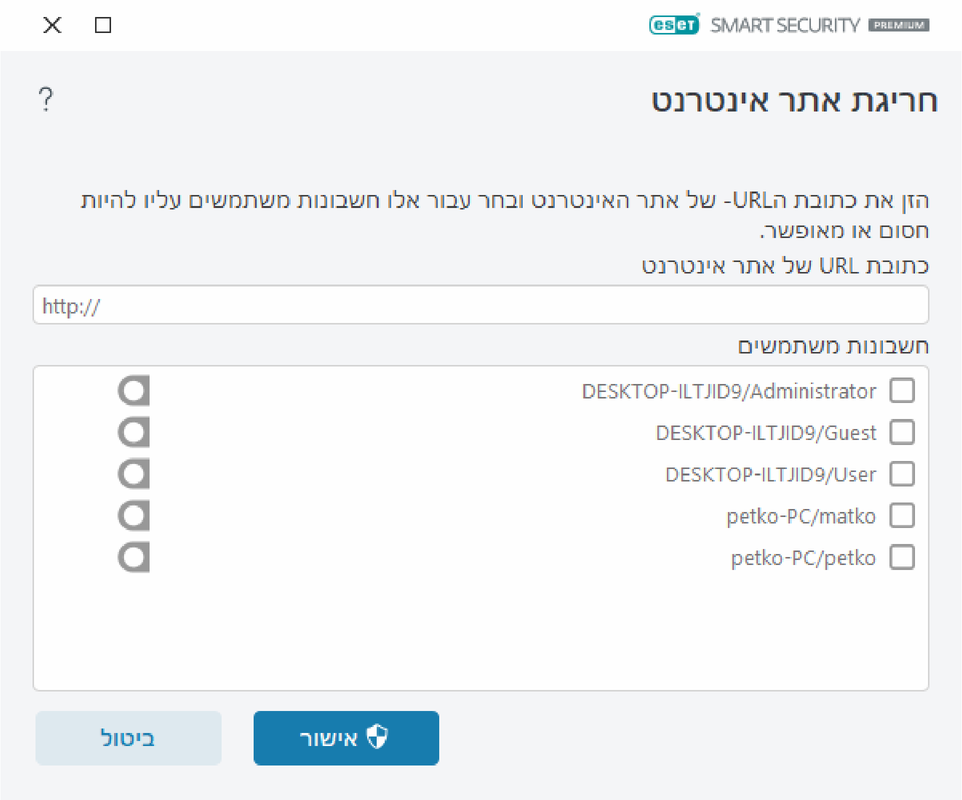
> בקרת הורים דורשת סורק תעבורת רשת, סריקת תעבורת (HTTP (S וחומת אש כדי לתפקד כראוי. כל הפונקציונליות הללו מופעלות כברירת מחדל.

חריגות אתר אינטרנט

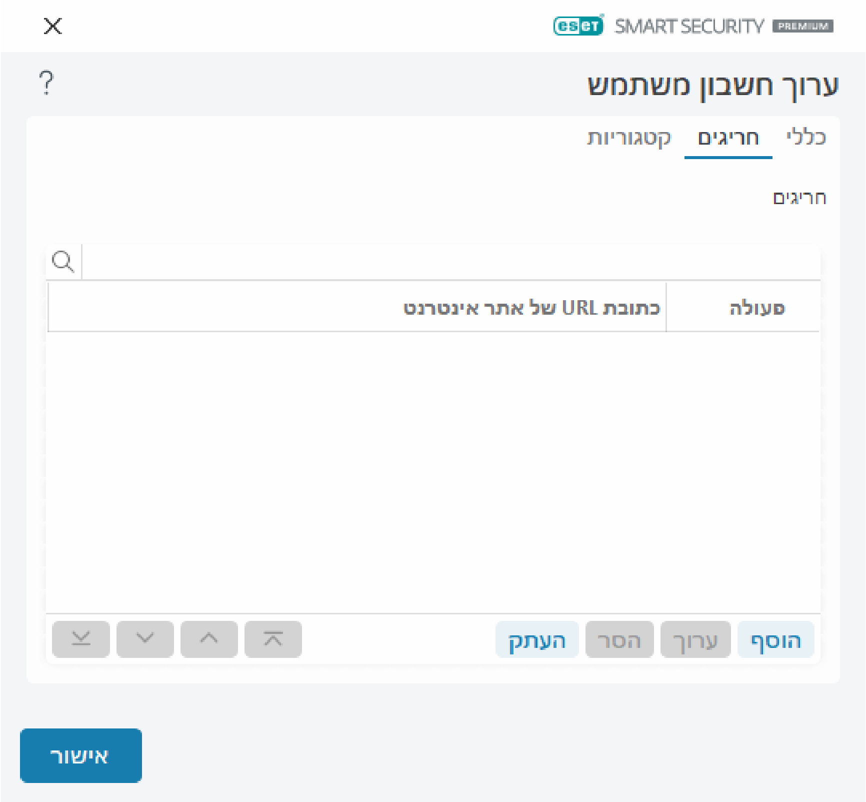
כדי להוסיף חריג לאתר אינטרנט, לחץ על **הגדרות** > **הגנת אינטרנט** > **בקרת הורים** ואז לחץ על **הוסף חריג עבור אתר אינטרנט**.



הזן כתובת URL בשדה **כתובת URL של אתר אינטרנט**, בחר (מותר) או (חסום) עבור כל חשבון משתמש ספציפי ואז לחץ על **אישור** כדי להוסיף אותו לרשימה.



כדי למחוק כתובת URL מהרשימה, לחץ על **הגדרות** > **הגנת אינטרנט** > **בקרת הורים**, לחץ על **תוכן חסום והגדרות** תחת חשבון המשתמש הרצוי, לחץ על הכרטיסייה **חריגה**, בחר את החריגה ואז לחץ על **הסר**.



ברשימת כתובות ה-URL, התווים המיוחדים * (כוכבית) ו-? (סימן שאלה) אינם ניתנים לשימוש. לדוגמה, יש להזין באופן ידני כתובות של דפי אינטרנט הכוללות מספר פריטי TLD (*examplepage.com, examplepage.sk* וכו'). כשאתה מוסיף תחום לרשימה, כל התוכן הממוקם בתחום זה וכל תחומי-המשנה (לדוגמה *sub.examplepage.com*) ייחסמו או יותרו, בהתאם לבחירתך את הפעולה מבוססת ה-URL.

חסימה או התרה של דף אינטרנט ספציפי יכולה להיות מדויקת יותר מחסימה או התרה של קטגוריית דפי אינטרנט. היזהר כשאתה משנה את ההגדרות הללו ומוסיף קטגוריה/דף אינטרנט מסוים לרשימה.

העתקת חריגה מהמשתמש

בחר בתפריט הנפתח משתמש שממנו ברצונך להעתיק את החריגה שנוצרה.

העתקת קטגוריות מהחשבון

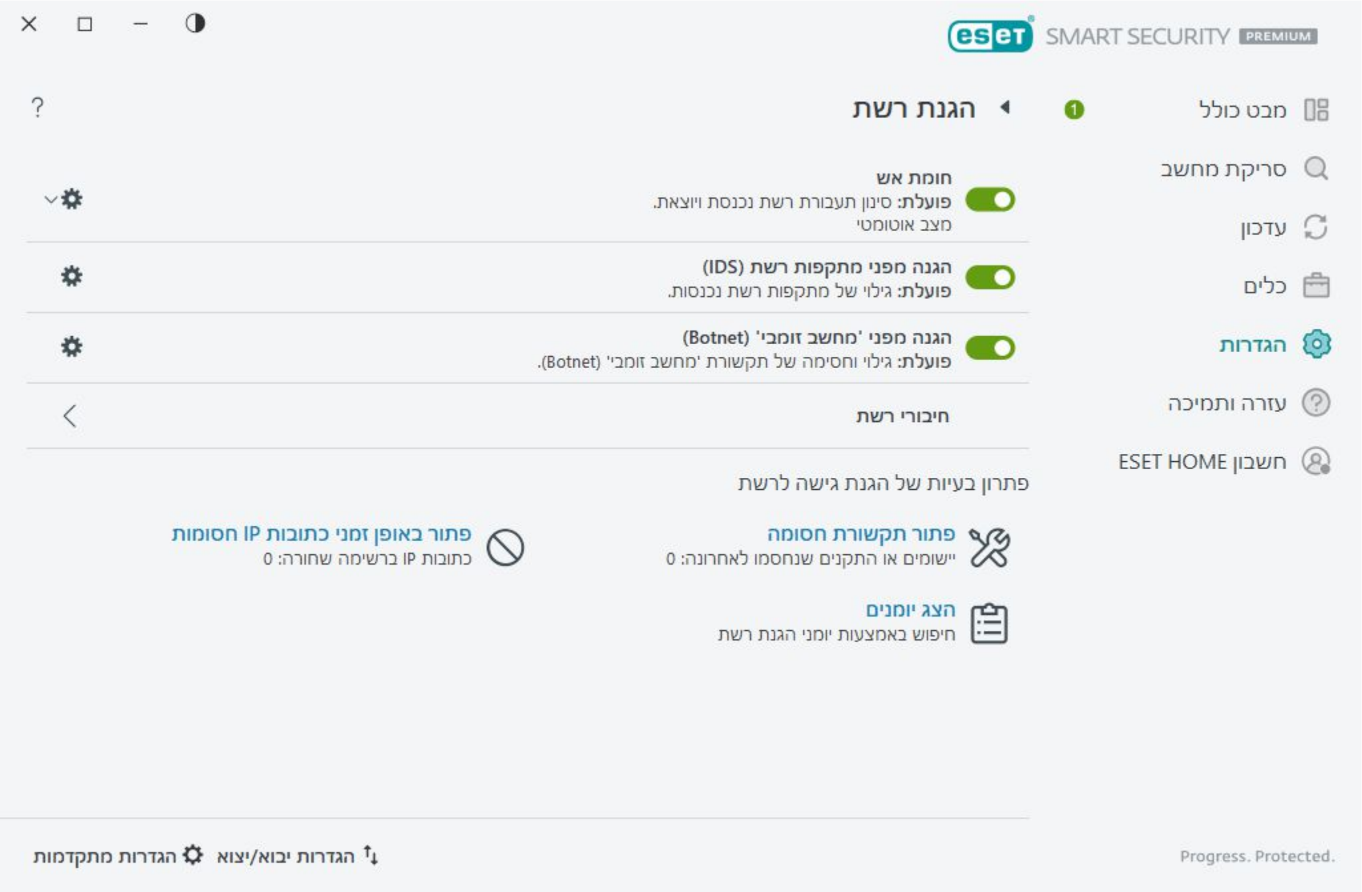
מאפשרת לך להעתיק רשימת קטגוריות חסומות או מותרות מחשבון קיים ששונה.

הגנת רשת

פתח את חלון התוכנית הראשי > **הגדרה** > **הגנת רשת** כדי לקבוע הגדרות בסיסיות של הגנת רשת או לפתור בעיות בתקשורת רשת.

כדי להשהות או להשבית מודולי הגנה נפרדים, לחץ על הסמל של המתג .

ההשבתה של מודולי ההגנה עלולה להפחית את רמת ההגנה של המחשב.



לחץ על סמל גלגל השיניים שלצד מודול ההגנה כדי לגשת אל ההגדרות המתקדמות של מודול זה.

חומת אש - מסנן את כל תקשורת הרשת בהתבסס על תצורת ESET Smart Security Premium.

קבע תצורה פותח את הגדרות מתקדמות של חומת אש, שם תוכל להגדיר כיצד חומת האש תטפל בתקשורת הרשת.

השהה חומת אש (אפשר את כל התעבורה) - אם אפשרות זו נבחרת, כל אפשרויות הסינון של חומת האש כבות וכל החיבורים הנכנסים והיוצאים מותרים. לחץ על **הפעל חומת אש** כדי להפעיל מחדש את חומת האש כאשר סינון תעבורת רשת נתון במצב זה.

חסום את כל התעבורה כל התקשורת הנכנסת והיוצאת תיחסם על-ידי חומת האש. השתמש באפשרות זו רק אם אתה חושד שסיכון אבטחה קריטי מחייב ניתוק של המערכת מהרשת. כאשר סינון תעבורת הרשת נתון במצב **חסום את כל התעבורה**, לחץ על **הפסק את חסימת כל התעבורה** כדי לשחזר את פעולת חומת האש הרגילה.

מצב אוטומטי (כאשר מצב סינון אחר פעיל) לחץ כדי לשנות את מצב הסינון למצב סינון אוטומטי (עם כללים המוגדרים על-ידי המשתמש).

מצב אינטראקטיבי (כאשר מצב סינון אחר פעיל) לחץ כדי לשנות את מצב הסינון למצב סינון אינטראקטיבי.

הגנה מפני מתקפות רשת (IDS) ניתוח התוכן של תעבורת רשת והגנה מפני מתקפות רשת. תעבורה שנחשבת למזיקה תיחסם. ESET Smart Security Premium יודיע לך אם תתחבר לרשת אלחוטית לא מוגנת או לרשת עם הגנה חלשה.

הגנה מפני רשת 'זומבי' (Botnet) זיהוי מהיר ומדויק של תוכנות זדוניות במערכת.

חיבורי רשת - מציג את הרשתות שאליהן מחוברים מתאמי הרשת.

פתור תקשורת חסומה מסייע לך לפתור בעיות קישוריות שנגרמות כתוצאה מחומת האש של ESET. לקבלת מידע

מפורט יותר, ראה אשף פתרון בעיות.

פתור באופן זמני כתובות IP חסומות - הצג רשימת כתובות IP שזוהתה כמקור למתקפות והתווספה לרשימה השחורה כדי לחסום את החיבור לפרק זמן מוגבל.

הצגת יומנים - פותח את קובץ יומן רישום של הגנת רשת.

חיבורי רשת

הצגת הרשתות שאליהן מחוברים מתאמי הרשת. כדי לראות חיבורי רשת, פתח את חלון התוכנית הראשי > **הגדרה** > **הגנת רשת** > **חיבורי רשת**.

לחץ פעמיים על חיבור ברשימה כדי להציג את פרטיו ואת פרטי מתאם הרשת שלו.

העבר את העכבר מעל חיבור רשת מסוים ולחץ על סמל התפריט ⋮ בעמודה **מהימן** כדי לבחור אחת מהאפשרויות הבאות:

- **ערוך** - פתח את החלון קביעת תצורה של הגנת רשת שבו באפשרותך להקצות פרופיל הגנת רשת לרשת מסוימת
- **שכח** - מאפס את תצורת חיבור הרשת לברירת המחדל
- **סרוק את הרשת באמצעות מפקח הרשת** פתיחת מפקח הרשת לצורך הפעלת סריקת רשת.
- **סמן בתוך "הרשת שלי"**מוסיף לרשת את התג "הרשת שלי". התג הזה יופיע לצד הרשת ב-ESET Smart Security Premium לצורך זיהוי טוב יותר ומבט כולל טוב יותר על האבטחה
- **בטל את הסימון "הרשת שלי"** מסיר את התג "הרשת שלי". זמין רק אם הרשת כבר מתויגת

פרטי חיבור הרשת

לחץ פעמיים על חיבור ברשימת חיבורי הרשת כדי להציג את הפרטים שלו יחד עם פרטי מתאם הרשת. הפרטים של חיבור רשת ומתאם יכולים לסייע לך בזיהוי הרשת שאתה מנסה להגדיר דרך הגנת גישה לאינטרנט.

פרטי חיבור הרשת:

- סטטוס החיבור לרשת
- תאריך ושעה של איתור הרשת הראשון
- הפעם האחרונה שהרשת הייתה פעילה
- משך הזמן הכולל של החיבור לרשת הזו
- פרופיל חיבור רשת
- פרופיל חיבור הרשת המוגדר ב-Windows
- תצורת הגנת רשת (אם הרשת מהימנה)

פרטי מתאם הרשת:

- סוג החיבור (קווי, וירטואלי וכו')
- שם מתאם רשת
- תיאור המתאם
- כתובת IP עם כתובת MAC

- כתובת IPv4 ו- IPv6 של הרשת עם רשת משנה
- סיומת DNS
- IP של שרת DNS
- IP של שרת DHCP
- כתובת IP וכתובת MAC של שער ברירת המחדל
- מתאם של כתובת MAC

פתרון בעיות בגישה לרשת

אשף פתרון הבעיות מסייע לך לפתור בעיות קישוריות שנגרמות כתוצאה מחומת האש של. **פתרון בעיות בגישה לרשת** ניתן למצוא בחלון התוכנית הראשי > **הגדרה** > **הגנת רשת** > **פתור תקשורת חסומה**.

בחר אם ברצונך להציג תקשורת חסומה עבור **אפליקציות מקומיות** או תקשורת חסומה מ**מכשירים מרוחקים**.

בתפריט הנפתח, בחר פרק זמן שבו התקשורת נחסמת. רשימת התקשורת שנחסמה לאחרונה מעניקה לך סקירה כללית על סוג היישום או המכשיר, המוניטין, והמספר הכולל של יישומים ומכשירים שנחסמו במהלך אותו פרק זמן. לקבלת פרטים נוספים על תקשורת שנחסמה לחץ על **פרטים**. השלב הבא הוא לבטל את החסימה של יישום או מכשיר שבו אתה נתקל בבעיות קישוריות.

כשאתה לוחץ על **בטל חסימה**, התקשורת הקודמת שנחסמה תותר. אם תמשיך להיתקל בבעיות עם אפליקציה מסוימת, או אם המכשיר שלך אינו פועל באופן הצפוי, לחץ על **יצירת כלל נוסף** וכל התקשורות שנחסמו קודם במכשיר זה יופעלו. אם הבעיה נמשכת, הפעל מחדש את המחשב.

לחץ על **פתח כללי חומת אש** כדי לראות כללים שנוצרו על-ידי האשף. בנוסף תוכל לראות כללים שנוצרו על-ידי האשף דרך הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **חומת אש** > **כללים** > **ערוך**.

אם לא ניתן ליצור את הכלל, תקבל הודעת שגיאה. לחץ על **נסה שוב** וחזור על התהליך כדי לבטל את חסימת התקשורת, או צור כלל אחר מרשימת התקשורת החסומה.

רשימה שחורה זמנית של כתובת IP

להצגת כתובות IP שאותרו כמקור למתקפות והתווספו לרשימה השחורה כדי לחסום את החיבור לפרק זמן מסוים, פתח את חלון התוכנית הראשי > **הגדרה** > **הגנת רשת** > **פתור באופן זמני כתובות IP חסומות**. כתובות IP שנחסמו באופן זמני חסומות למשך שעה אחת.

עמודות

כתובת IP □ הצגת כתובת IP שנחסמה.

סיבת החסימה □ הצגת סוג המתקפה שנמנעה מהכתובת (לדוגמה מתקפה של סריקת יציאת TCP).

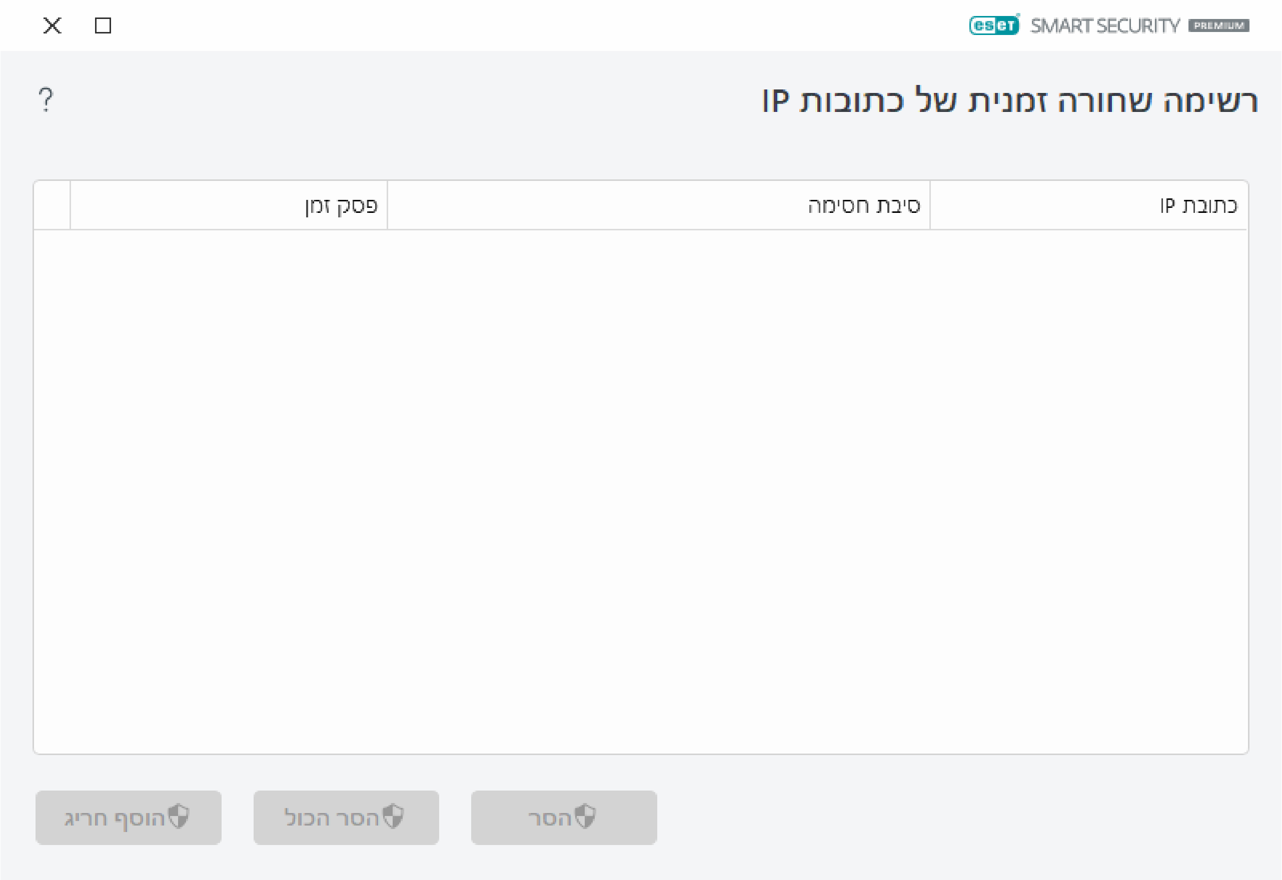
זמן קצוב □ הצגת השעה והתאריך שבהם תוקף הימצאותה של הכתובת ברשימה השחורה יפוג.

רכיבי בקרה

הסר לחץ להסרת כתובת מהרשימה השחורה לפני שתוקפה יפוג.

הסר הכול לחץ להסרת כל הכתובות מהרשימה השחורה באופן מיידי.

הוסף חריג לחץ להוספת חריג חומת אש לסינון ה-IDS.



יומני הגנת רשת

הגנת הרשת של ESET Smart Security Premium שומרת את כל האירועים החשובים בקובץ יומן רישום. כדי להציג את קובץ היומן, פתח את חלון התוכנית הראשי > **הגדרה** > **הגנת רשת** > **הצג יומנים**.

ניתן להשתמש ברשומות היומן כדי לאתר שגיאות ולחשוף חדירות למערכת. יומני הגנת הרשת של כוללים את הנתונים הבאים:

- התאריך והשעה של האירוע
- שם האירוע
- מקור
- כתובת רשת היעד
- פרוטוקול התקשורת של הרשת
- הכלל שהוחל, או שם התולעת, אם זוהו
- נתיב האפליקציה והשם
- קוד Hash

- משתמש
- חותם הבקשה (המפרסם)
- שם החבילה
- שם השירות

ניתוח מקיף של נתונים אלה עשוי לסייע בזיהוי ניסיונות לפגוע באבטחת המחשב. גורמים רבים אחרים מצביעים על סיכוני אבטחה פוטנציאליים ומאפשרים לך למזער את השפעתם: חיבורים תכופים ממיקומים לא מוכרים, ניסיונות רבים להתחבר, יישומים לא מוכרים המנהלים תקשורת, או שימוש במספרי יציאות יוצאי דופן.

ניצול לרעה של פגיעות אבטחה
ההודעה על ניצול לרעה של פגיעות אבטחה נרשמת גם אם הפגיעות הספציפית כבר תוקנה מאז איתור ניסיון הניצול ובוצעה חסימה ברמת הרשת לפני שהניצול לרעה היה יכול להתרחש.

פתרון בעיות עם חומת האש של

אם אתה נתקל בבעיות קישוריות כאשר ESET Smart Security Premium מותקן, ישנן מספר דרכים לדעת אם חומת האש של גורמת לבעיה. יתרה מכך, חומת האש של עשויה לסייע לך ליצור כללים או חריגות חדשים כדי לזהות בעיות בקישוריות.

עיין בנושאים הבאים לקבלת עזרה בפתרון בעיות עם חומת האש של:

- פתרון בעיות בגישה לרשת
- רישום ויצירת כללים או חריגות ביומן
- יצירת חריגות מהודעות חומת האש
- רישום מתקדם ביומן של הגנת רשת
- פתרון בעיות עם סורק תעבורת הרשת

רישום ויצירת כללים או חריגות ביומן

כברירת מחדל, חומת האש של ESET אינה רושמת ביומן את כל החיבורים החסומים. אם ברצונך לראות מה נחסם על ידי הגנת הרשת, פתח את הגדרות מתקדמות > **כללים** > **אבחון** > **רישום מתקדם ביומן** והפעל את **אפשר רישום מתקדם של הגנת רשת**. אם אתה רואה ביומן דבר מה שאינך רוצה שחומת האש תחסום, באפשרותך ליצור עבורו כלל או כלל IDS על ידי לחיצה ימנית על פריט זה ואז בחירה באפשרות **אל תחסום אירועים דומים בעתיד**. שים לב שהיומן של כל החיבורים החסומים עשוי להכיל אלפי פריטים, וייתכן שיהיה קשה למצוא חיבור ספציפי ביומן זה. באפשרותך להשבית את הרישום אחרי שתפתור את הבעיה.

לקבלת מידע נוסף על היומן, ראה רשומות יומן.

השתמש ברישום ביומן כדי לראות את הסדר שבו הגנת הרשת חסמה חיבורים מסוימים. בנוסף, יצירת כללים מהיומן מאפשרת לך ליצור כללים שמבצעים בדיוק את מה שאתה רוצה.

יצירת כלל מיומן רישום

הגרסה החדשה של ESET Smart Security Premium מאפשרת לך ליצור כלל מיומן הרישום. בחלון הראשי לחץ על **כלים** > **רשומות יומן**. בחר **הגנת רשת** בתפריט הנפתח, לחץ באמצעות לחצן העכבר הימני על הזנת היומן הרצויה, ואז בחר

אל תחסום אירועים דומים בעתיד בתפריט ההקשר. חלון הודעה יציג את הכלל החדש שלך.

כדי לאפשר יצירת כללים חדשים מהיומן, יש לקבוע ב-ESET Smart Security Premium את ההגדרות הבאות:

1. הגדר את הפירוט המינימלי של רישום ביומן כ**אבחוני** תחת הגדרות מתקדמות > **כלים** > **רשומות יומן**,
2. הפעל את האפשרות **הודע על התקפות נכנסות נגד פרצות אבטחה** במקטע הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **הגנה מפני מתקפות רשת** > **אפשרויות מתקדמות** > **איתור חדירות**.

יצירת חריגות מהודעות חומת האש

כאשר חומת האש של ESET מזהה פעילות רשת זדונית, מוצג חלון התראה המתאר את האירוע. התראה זו כוללת קישור שיאפשר לך לקבל מידע נוסף על האירוע, ואם תרצה ▯ גם להגדיר כלל לאירוע זה.

> אם יישום רשת או מכשיר מסוימים אינם מממשים את הסטנדרטים של הרשת כהלכה, תיתכן הפעלה חוזרת של הודעות IDS של חומת אש. תוכל ליצור חריגה ישירות מההודעה כדי למנוע מחומת האש של ESET לזהות את היישום או ההתקן הללו.

רישום מתקדם ביומן של הגנת רשת

תכונה זו מיועדת לספק רשומות יומן מורכבות יותר לתמיכה הטכנית של ESET. השתמש בתכונה זו רק כשצוות התמיכה הטכנית של ESET יבקש ממך לעשות זאת, מאחר שהיא עשויה ליצור רשומת יומן עצומה ולהאט את פעולת המחשב.

1. פתח את הגדרות מתקדמות > **כלים** > **אבחון** > **רישום מתקדם ביומן** והפעל את **אפשר רישום מתקדם ביומן של הגנת רשת**.
2. נסה לשחזר את הבעיה שבה נתקלת.
3. השבת רישום מתקדם ביומן של הגנת רשת.
4. קובץ יומן ה-PCAP שנוצר על ידי הרישום המתקדם ביומן של הגנת רשת נמצא באותה ספרייה שבה נוצרים מצבורי הזיכרון האבחוני:*C:\ProgramData\ESET\ESET Security\Diagnostics*

פתרון בעיות עם סורק תעבורת הרשת

אם אתה נתקל בבעיות עם הדפדפן או לקוח הדואר האלקטרוני שלך, השלב הראשון יהיה לקבוע אם 'סורק תעבורת רשת' אחראי לכך. כדי לעשות זאת, נסה להשבית זמנית את 'סורק תעבורת רשת' דרך הגדרות מתקדמות > **מנגנון איתור** > **סורק תעבורת רשת** (זכור להפעילו מחדש אחרי שתסיים, כך שהדפדפן ולקוח הדואר האלקטרוני שלך לא יישארו ללא הגנה). אם הבעיה תיעלם לאחר הכיבוי, להלן רשימת בעיות נפוצות ודרך לפתור אותן:

בעיות בעדכון או באבטחת תקשורת

אם היישום שלך מאותת על חוסר יכולת לעדכן או שערוץ תקשורת מסוים אינו מאובטח:

- אם SSL/TLS מופעל אצלך, נסה לכבות אותו זמנית. אם הפעולה עזרה, תוכל להמשיך להשתמש בסינון SSL/TLS ולגרום לעדכון לפעול על-ידי החרגת התקשורת הבעייתית:

  הפוך ללא זמין SSL/TLS הפעל את העדכון מחדש. אמור להופיע חלון דו-שיח שיידע אותך על תעבורת הרשת שהוצפנה. ודא שהיישום תואם לזה שבו אתה פותר בעיות ושהאישור נראה כאילו הגיע מהשרת שממנו בוצע

העדכון. לאחר מכן בחר לזכור את הפעולה עבור אישור זה ולחץ על 'התעלם'. אם לא מופיעים חלונות דו-שיח רלוונטיים נוספים, באפשרותך להחזיר את הסינון למצב האוטומטי, והבעיה אמורה להיפתר.

- אם האפליקציה הרלוונטית אינה דפדפן או לקוח דואר אלקטרוני, באפשרותך שלא לכלול אותה כלל בהגנת גישה לאינטרנט (ביצוע פעולה זו על דפדפן או לקוח דואר אלקטרוני ישאיר אותך חשוף). כל היישומים שהתקשורת שלהם סוננה בעבר אמורים כבר להופיע ברשימה שסופקה לך בעת הוספת חריגה, כך שאין צורך להוסיף באופן ידני.

בעיה בגישה למכשיר ברשת שלך

אם אינך מצליח להשתמש בפונקציונליות כלשהי של מכשיר ברשת שלך (המשמעות עשויה להיות פתיחת דף אינטרנט של מצלמת האינטרנט שלך או הפעלת סרטון בנגן מדיה ביתי), נסה להוסיף את כתובות ה-IPv4 וה-IPv6 שלו לרשימת הכתובות המוחרגות שלך.

בעיות עם אתר אינטרנט מסוים

באפשרותך להחריג אתרי אינטרנט ספציפיים מהגנת גישה לאינטרנט באמצעות ניהול כתובות URL. לדוגמה, אם אינך מצליח לגשת לכתובת https://www.gmail.com/intl/en/mail/help/about.html, נסה להוסיף *gmail.com* לרשימת הכתובות המוחרגות.

שגיאת "חלק מהיישומים המסוגלים לייבא את אישור הבסיס עדיין פועלים"

כשאתה מפעיל את ESET Smart Security Premium SSL/TLS, מוודא שהאפליקציות המותקנות סומכות על האופן שבו הוא מסנן את פרוטוקול SSL על-ידי ייבוא אישור למאגר האישורים שלהם. חלק מהאפליקציות עשויות להצריך הפעלה מחדש לצורך ייבוא אישור. עם אלה נמנים Firefox ו-Opera. ודא שאף אחד מהם אינו פועל (הדרך הטובה ביותר לעשות זאת היא לפתוח את מנהל המשימות ולוודא ש-firefox.exe או opera.exe אינם מופיעים תחת כרטיסיית התהליכים), ולאחר מכן לחץ על נסה שוב.

שגיאה הנוגעת למנפיק לא מהימן או לחתימה לא חוקית

המשמעות האפשרית ביותר לכך היא שהייבוא המתואר לעיל נכשל. תחילה ודא שאף אחד מהיישומים המוזכרים אינו פועל. לאחר מכן השבת את SSL/TLS והפעל אותו שוב. פעולה זו תפעיל את הייבוא מחדש.

> i ראה את המאמר במאגר הידע כדי ללמוד כיצד לנהל את 'סורק תעבורת רשת' במוצר ביתי של ESET עבור Windows.

איום רשת נחסם

מצב זה עשוי להתרחש כאשר אפליקציה מסוימת במחשב שלך מנסה לשדר תעבורה זדונית למחשב אחר ברשת, תוך ניצול פרצת אבטחה, או אפילו אם מזוהה ניסיון לסריקת יציאות במערכת שלך.

בהתראה תוכל למצוא את סוג האיום ואת כתובת ה- IP הקשורה למכשיר. לחץ על **שינוי הטיפול באיום זה** כדי להציג את האפשרויות הבאות:

המשך חסימה חסימת האיום שזוהה. אם ברצונך להפסיק לקבל התראות על איום מסוג זה מהכתובת המרוחקת הספציפית, בחר בלחצן הבחירה שליד **אל תודיע** לפני שתלחץ על **המשך חסימה**. פעולה זו תיצור כלל לשירות איתור

[חדירות (IDS)](#) עם התצורה הבאה: **חסום** - ברירת מחדל, **שלח הודעה** - לא, **יומן** - לא.

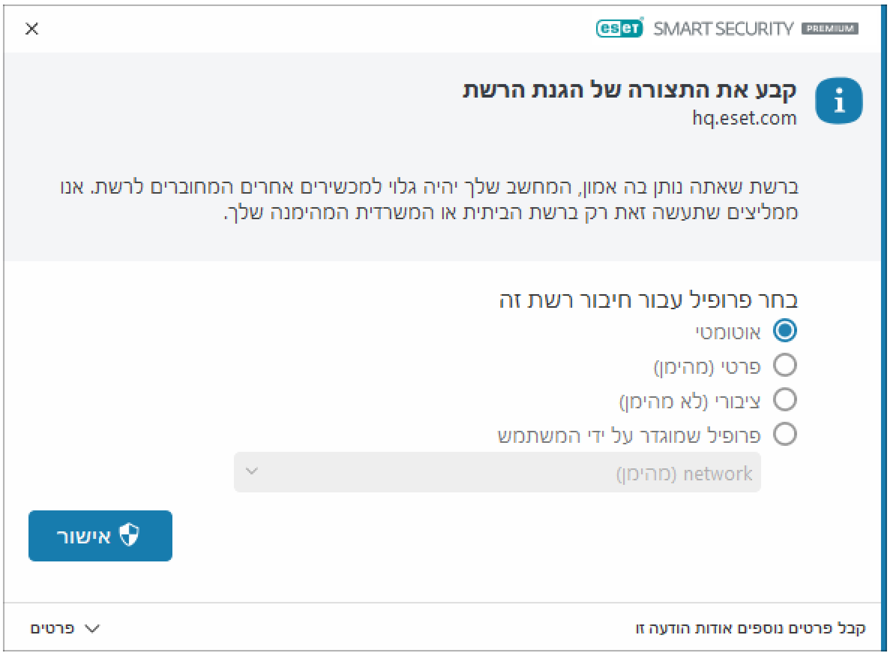
אפשר - יצירת [כלל לשירות איתור חדירות (IDS)](#) כדי לאפשר את האיום שזוהה. בחר אחת מהאפשרויות הבאות לפני שתלחץ על **אפשר** כדי לציין את הגדרות הכלל:

- **הודע לי כאשר איום זה נחסם** - הגדרת כלל: **חסום** - לא, **הודע** - לא, **יומן** - לא.
- **הודע לי כאשר איום זה מתרחש** - הגדרת כלל: **חסום** - לא, **הודע** - ברירת מחדל, **יומן** - ברירת מחדל.
- **אל תודיע**תצורת כלל: **חסום** - לא, **הודע** - לא, **יומן** - לא.

> המידע המוצג בחלון התראה זה עשוי להשתנות בהתאם לסוג האיום שזוהה.
> לקבלת מידע נוסף על איומים ומונחים קשורים אחרים, ראה [סוגי מתקפות מרוחקות](#) או [סוגי איתורים](#).
> כדי לפתור את האירוע **כתובות IP כפולות ברשת**, עיין ב[מאמר מאגר הידע של ESET](#).

זוהתה רשת חדשה

כברירת מחדל, ESET Smart Security Premium משתמש בהגדרות Windows כשמזוהה חיבור רשת חדש. כדי להציג חלון דו-שיח כאשר מזוהה רשת חדשה, שנה את [הקצאת פרופיל הגנת רשת](#) כך שיהיה **שאל**. הגדרת התצורה של הגנת הרשת תוצג בכל פעם שהמחשב מתחבר לרשת חדשה.



באפשרותך לבחור מבין [הפרופילים הבאים לחיבור רשת](#):

אוטומטי - ESET Smart Security Premium יבחר את הפרופיל באופן אוטומטי, בהתבסס על [מפעילים](#) שהוגדרו עבור כל פרופיל.

פרטי עבור רשת מהימנה (רשת ביתית או משרדית). המחשב שלך וקבצים משותפים המאוחסנים במחשב שלך גלויים למשתמשי רשת אחרים, ומשאבי מערכת נגישים למשתמשים אחרים ברשת (הגישה לקבצים משותפים ולמדפסות מופעלת, תקשורת נכנסת של RPC מופעלת ושיתוף שולחן עבודה מרוחק זמין). אנו ממליצים להשתמש בהגדרה זו בעת גישה לרשת מקומית מאובטחת. פרופיל זה מוקצה באופן אוטומטי לחיבור רשת אם הוא מוגדר כתחום או רשת פרטית ב-Windows.

ציבורי עבור רשתות לא מהימנות (רשת ציבורית). קבצים ותיקיות במערכת שלך אינם משותפים עם משתמשים

אחרים ואינם גלויים להם ברשת, ושיתוף משאבי מערכת מושבת. אנו ממליצים להשתמש בהגדרה זו בעת גישה לרשתות אלחוטיות. פרופיל זה מוקצה באופן אוטומטי לכל חיבור רשת שאינו מוגדר בתור תחום או רשת פרטית ב-Windows.

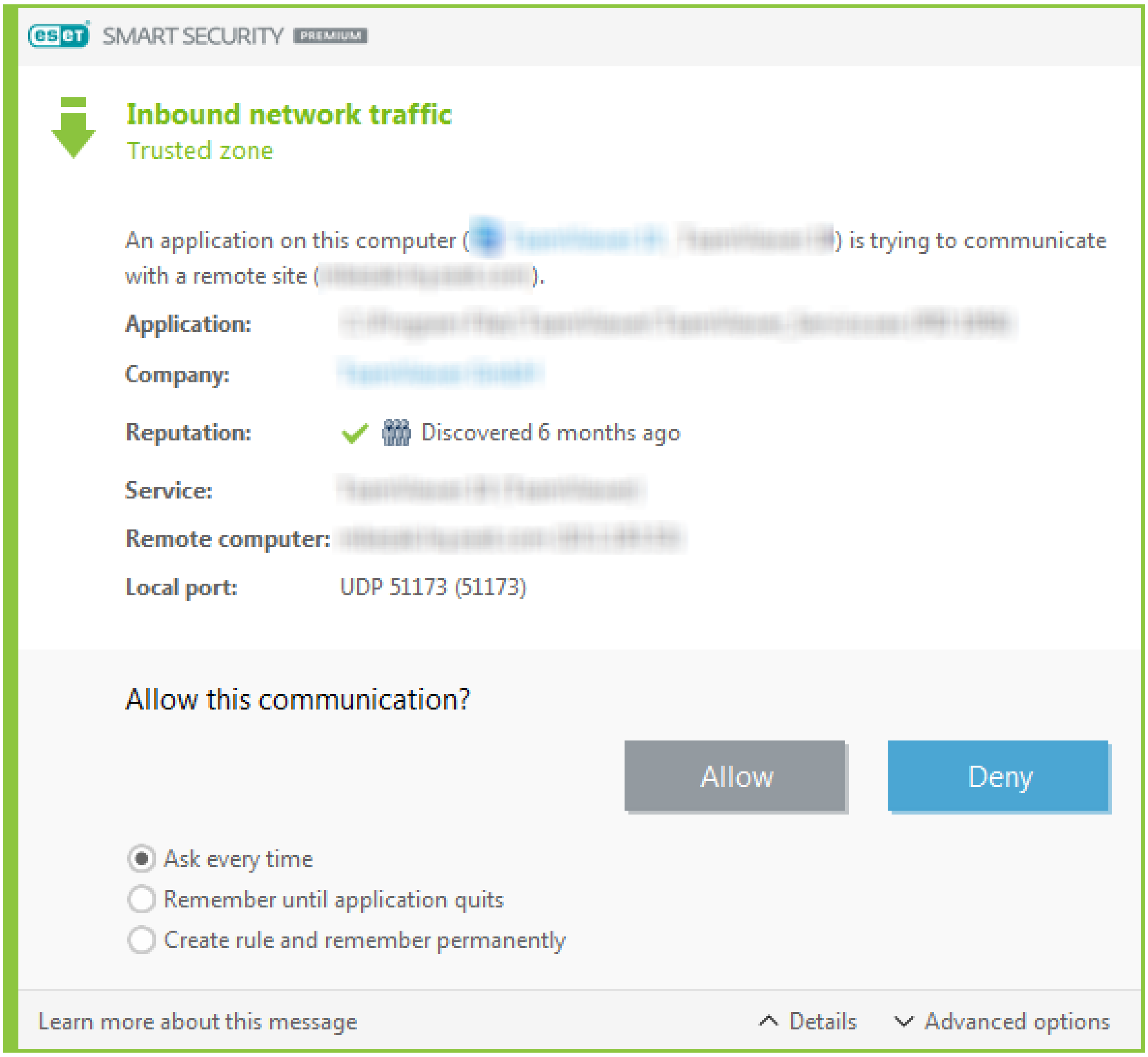
פרופיל מוגדר על ידי המשתמש - באפשרותך לבחור אחד מהפרופילים שיצרת מהתפריט הנפתח. אפשרות זו זמינה רק אם יצרת פרופיל מותאם אישית אחד לפחות.

תצורת רשת שגויה עשויה לחשוף את המחשב שלך לסיכון אבטחה.

יצירת חיבור – זיהוי

חומת האש מזהה כל חיבור רשת חדש שנוצר. מצב חומת האש הפעיל קובע אילו פעולות יבוצעו עבור הכלל החדש. אם **מצב אוטומטי** או **מצב מבוסס-מדיניות** מופעלים, חומת האש תבצע פעולות שהוגדרו מראש מבלי שתהיה אינטראקציה עם המשתמש.

האפשרות **מצב אינטראקטיבי** מציגה חלון מידע המדווח על זיהוי חיבור רשת חדש יחד עם מידע מפורט על החיבור. באפשרותך לבחור **לאפשר** או **למנוע** (לחסום) את החיבור. אם אתה מאשר את אותו חיבור בחלון הדו-שיח שוב ושוב, מומלץ שתיצור כלל חדש עבור החיבור. לשם כך, בחר **צור כלל וזכור לצמיתות** ואז שמור את הפעולה ככלל חדש עבור חומת האש. אם חומת האש תזהה את אותו חיבור בעתיד, היא תחיל את הכלל הקיים ללא צורך באינטראקציה עם המשתמש.



בעת יצירת כללים חדשים, אפשר רק חיבורים שאתה יודע שהם מאובטחים. אם כל החיבורים יאושרו, חומת האש לא תשיג את מטרתה. אלה הם הפרמטרים החשובים לחיבורים:

אפליקציה מיקום קובץ ההפעלה ומזהה תהליך. אל תאפשר חיבורים לאפליקציות לא מוכרות ולתהליכים לא מוכרים.

חותם - השם של מפרסם האפליקציה. לחץ על הטקסט כדי להציג אישור אבטחה של החברה.

מוניטין רמת הסיכון של החיבור. מוקצית רמת סיכון לחיבורים: תקין (ירוק), לא מוכר (כתום) או מסוכן (אדום), בעזרת סדרה של כללים היוריסטיים הבוחנים את המאפיינים של כל חיבור, את מספר המשתמשים ואת שעת הגילוי. מידע זה נאסף באמצעות טכנולוגיית ESET LiveGrid®.

שירות שם השירות, אם האפליקציה היא שירות של Windows.

מחשב מרוחק כתובת המכשיר המרוחק. אשר רק חיבורים לכתובות מהימנות ומוכרות.

יציאה מרוחקת יציאת תקשורת. ניתן לאשר את התקשורת ביציאות נפוצות (למשל תעבורת אינטרנט יציאות מספר 80, 443) בנסיבות רגילות.

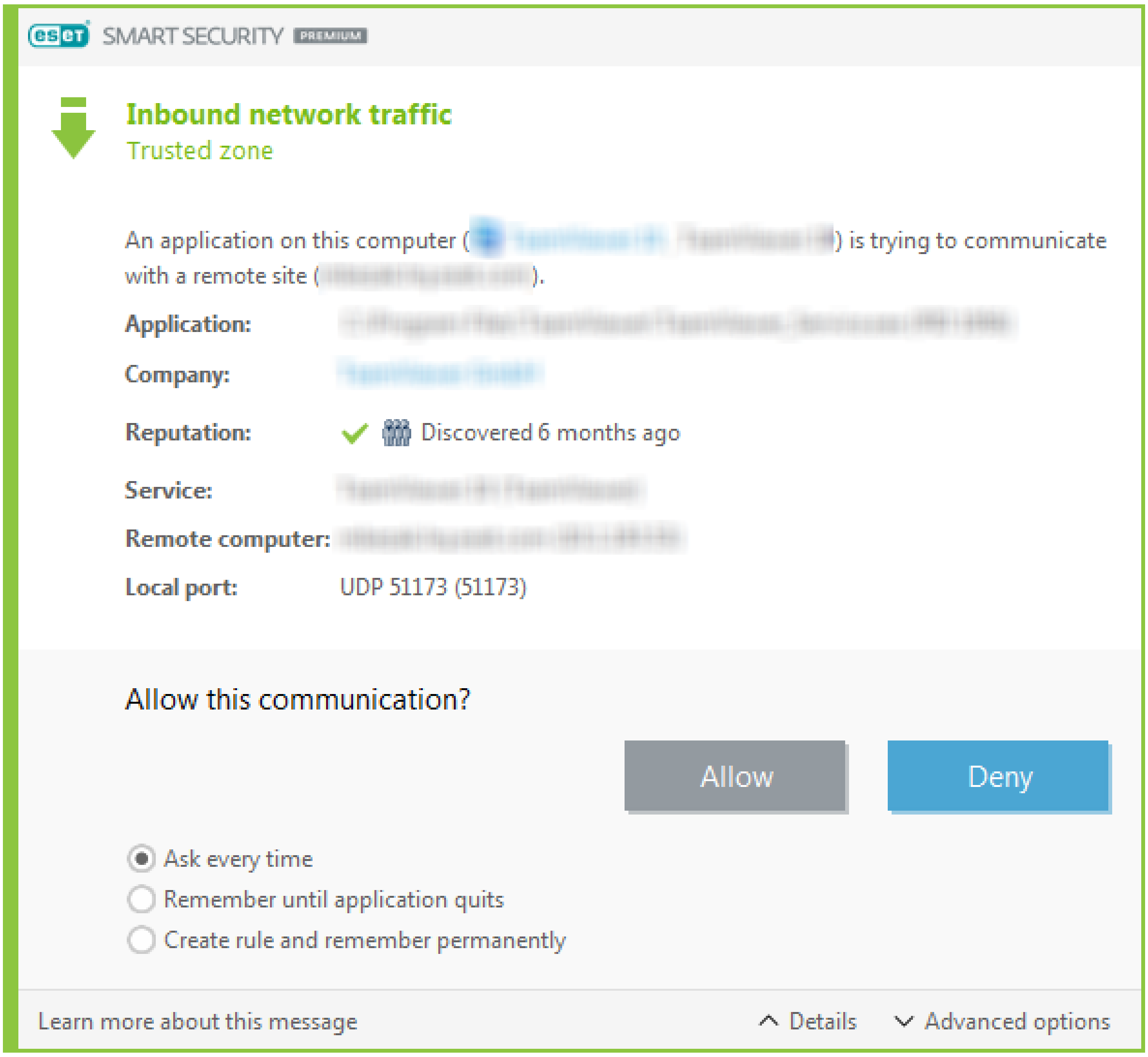
חדירות מחשב מרבות להשתמש באינטרנט ובחיבורים נסתרים, אשר מסייעים להן להדביק מערכות מרוחקות. אם הכללים מוגדרים כהלכה, חומת האש הופכת לכלי שימושי להגנה מפני מגוון מתקפות של קודים זדוניים.

שינוי ביישום

חומת האש זיהתה שינוי ביישום שמשמש ליצירת חיבורים יוצאים מהמחשב שלך. ייתכן שהיישום פשוט עודכן לגרסה חדשה. מאידך, שינוי עלול להיגרם גם כתוצאה מיישום זדוני. אם אינך מודע לקיומו של שינוי לגיטימי כלשהו, מומלץ למנוע את החיבור ולסרוק את המחשב באמצעות מסד נתוני חתימות הווירוסים העדכני ביותר.

תקשורת מהימנה נכנסת

דוגמה לחיבור נכנס באזור המהימן:
מחשב מרוחק מהאזור המהימן מנסה ליצור תקשורת עם יישום מקומי הפועל במחשב שלך.



אפליקציה – האפליקציה שאיתה מכשיר מרוחק יוצר קשר.

נתיב אפליקציה מיקום האפליקציה.

אפליקציה מ-Microsoft Store שם האפליקציה ב-Microsoft Store.

חותם - השם של מפרסם האפליקציה. לחץ על הטקסט כדי להציג אישור אבטחה של החברה.

מוניטין – מוניטין היישום, כפי שהושג על-ידי טכנולוגיית ®ESET LiveGrid.

שירות – שם השירות שפועל כעת במחשב שלך.

מחשב מרוחק – מחשב מרוחק המנסה ליצור תקשורת עם היישום במחשב שלך.

יציאה מרוחקת – היציאה המשמשת לצורך התקשורת.

שאל בכל פעם – אם הפעולה שהוגדרה כברירת מחדל עבור כלל היא **הצגת שאלה**, חלון דו-שיח יוצג בכל פעם שכלל זה מופעל.

זכור עד ליציאה מהיישום – ESET Smart Security Premium יזכור את הפעולה שנבחרה עד ההפעלה מחדש הבאה.

צור כלל וזכור לצמיתות – אם תבחר באפשרות זו לפני שתאפשר או תמנע תקשורת מסוימת, ESET Smart Security Premium יזכור את הפעולה וישתמש בה, במקרה שהמחשב המרוחק ייצור קשר עם היישום פעם נוספת.

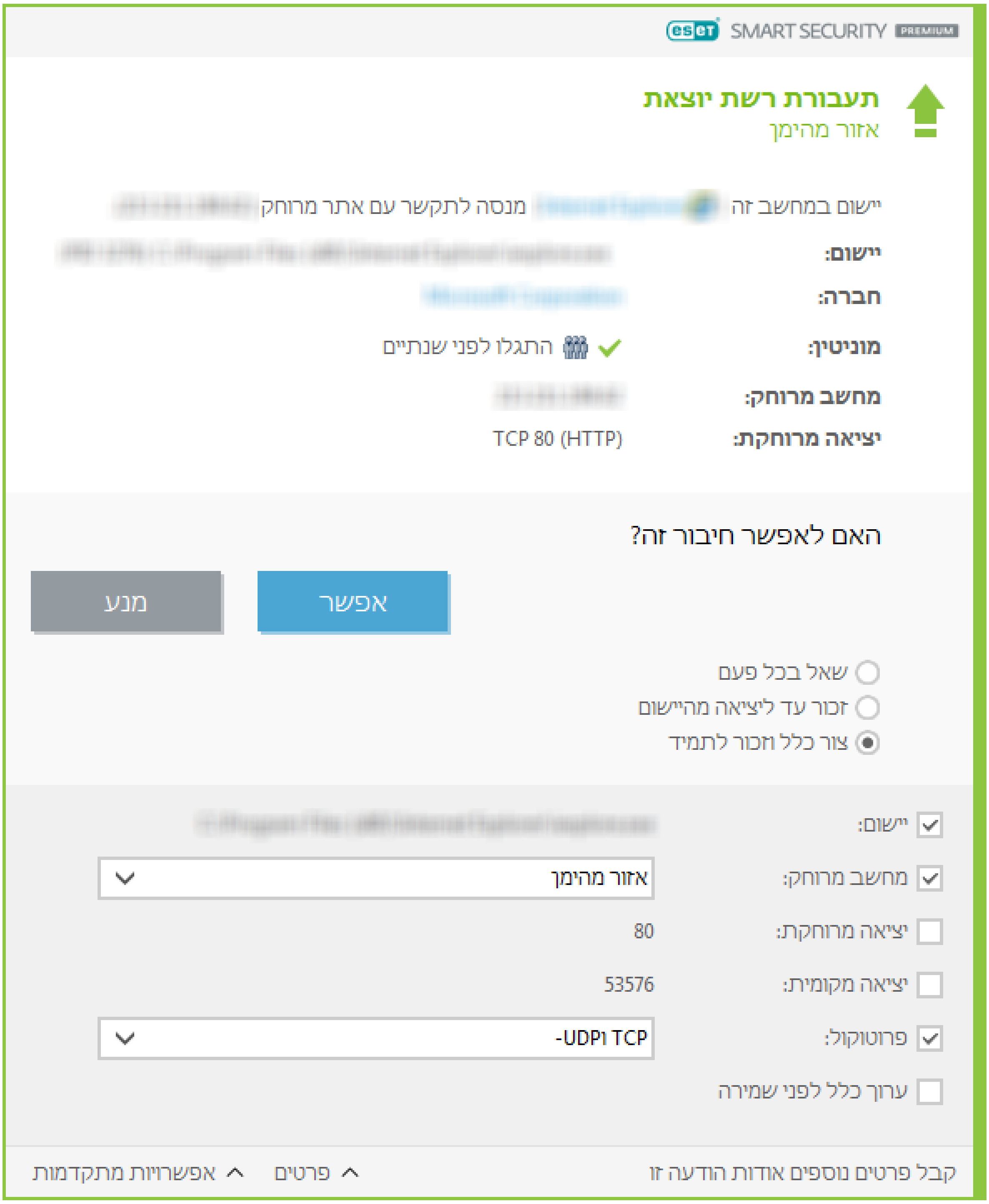
אישור – מאפשר את התקשורת הנכנסת.

מניעה – מונע את התקשורת הנכנסת.

עריכת כלל - מאפשר להתאים אישית את מאפייני הכללים באמצעות עורך כללי חומת האש.

תקשורת מהימנה יוצאת

דוגמה לחיבור יוצא באזור המהימן:
יישום מקומי המנסה ליצור חיבור למחשב אחר ברשת המקומית, או ברשת באזור המהימן.



אפליקציה – האפליקציה שאיתה מכשיר מרוחק יוצר קשר.

נתיב אפליקציה מיקום האפליקציה.

אפליקציה מ-Microsoft Store שם האפליקציה ב-Microsoft Store.

חותם - השם של מפרסם האפליקציה. לחץ על הטקסט כדי להציג אישור אבטחה של החברה.

מוניטין – מוניטין היישום, כפי שהושג על-ידי טכנולוגיית ESET LiveGrid®.

שירות – שם השירות שפועל כעת במחשב שלך.

מחשב מרוחק – מחשב מרוחק המנסה ליצור תקשורת עם היישום במחשב שלך.

יציאה מרוחקת – היציאה המשמשת לצורך התקשורת.

שאל בכל פעם – אם הפעולה שהוגדרה כברירת מחדל עבור כלל היא **הצגת שאלה**, חלון דו-שיח יוצג בכל פעם שכלל זה מופעל.

זכור עד ליציאה מהיישום – ESET Smart Security Premium יזכור את הפעולה שנבחרה עד ההפעלה מחדש הבאה.

צור כלל וזכור לצמיתות – אם תבחר באפשרות זו לפני שתאפשר או תמנע תקשורת מסוימת, ESET Smart Security Premium יזכור את הפעולה וישתמש בה, במקרה שהמחשב המרוחק ייצור קשר עם היישום פעם נוספת.

אישור – מאפשר את התקשורת הנכנסת.

מניעה – מונע את התקשורת הנכנסת.

עריכת כלל - מאפשר להתאים אישית את מאפייני הכללים באמצעות עורך כללי חומת האש.

תקשורת נכנסת

דוגמה לחיבור אינטרנט נכנס:
מחשב מרוחק המנסה להתקשר עם יישום הפועל במחשב.

אפליקציה – האפליקציה שאיתה מכשיר מרוחק יוצר קשר.

נתיב אפליקציה מיקום האפליקציה.

אפליקציה מ-Microsoft Store שם האפליקציה ב-Microsoft Store.

חותם - השם של מפרסם האפליקציה. לחץ על הטקסט כדי להציג אישור אבטחה של החברה.

מוניטין – מוניטין היישום, כפי שהושג על-ידי טכנולוגיית ESET LiveGrid®.

שירות – שם השירות שפועל כעת במחשב שלך.

מחשב מרוחק – מחשב מרוחק המנסה ליצור תקשורת עם היישום במחשב שלך.

יציאה מרוחקת – היציאה המשמשת לצורך התקשורת.

שאל בכל פעם – אם הפעולה שהוגדרה כברירת מחדל עבור כלל היא **הצגת שאלה**, חלון דו-שיח יוצג בכל פעם שכלל זה מופעל.

זכור עד ליציאה מהיישום – ESET Smart Security Premium יזכור את הפעולה שנבחרה עד ההפעלה מחדש הבאה.

צור כלל וזכור לצמיתות אם תבחר באפשרות זו לפני שתאפשר או תמנע תקשורת מסוימת, ESET Smart Security Premium יזכור את הפעולה וישתמש בה, במקרה שהמחשב המרוחק ייצור קשר עם היישום פעם נוספת.

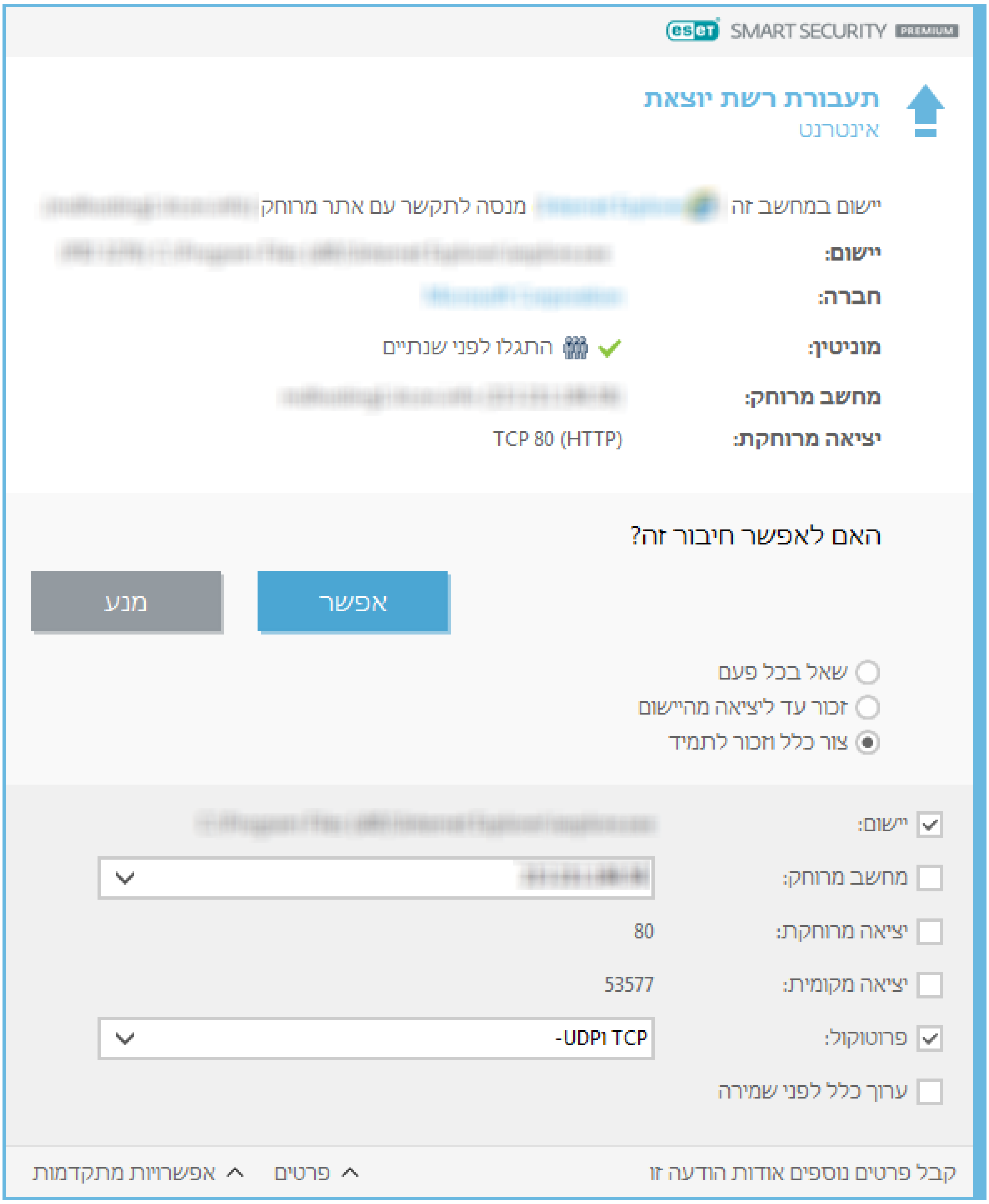
אישור מאפשר את התקשורת הנכנסת.

מניעה מונע את התקשורת הנכנסת.

עריכת כלל - מאפשר להתאים אישית את מאפייני הכללים באמצעות עורך כללי חומת האש.

תקשורת יוצאת

דוגמה לחיבור אינטרנט יוצא:
יישום מקומי מנסה ליצור חיבור לאינטרנט.



אפליקציה האפליקציה שאיתה מכשיר מרוחק יוצר קשר.

נתיב אפליקציה מיקום האפליקציה.

אפליקציה מ-Microsoft Store שם האפליקציה ב-Microsoft Store.

חותם - השם של מפרסם האפליקציה. לחץ על הטקסט כדי להציג אישור אבטחה של החברה.

מוניטין מוניטין היישום, כפי שהושג על-ידי טכנולוגיית ®ESET LiveGrid.

שירות שם השירות שפועל כעת במחשב שלך.

מחשב מרוחק מחשב מרוחק המנסה ליצור תקשורת עם היישום במחשב שלך.

יציאה מרוחקת היציאה המשמשת לצורך התקשורת.

שאל בכל פעם אם הפעולה שהוגדרה כברירת מחדל עבור כלל היא **הצגת שאלה**, חלון דו-שיח יוצג בכל פעם שכלל זה מופעל.

זכור עד ליציאה מהיישום – ESET Smart Security Premium יזכור את הפעולה שנבחרה עד ההפעלה מחדש הבאה.

צור כלל וזכור לצמיתות אם תבחר באפשרות זו לפני שתאפשר או תמנע תקשורת מסוימת, ESET Smart Security Premium יזכור את הפעולה וישתמש בה, במקרה שהמחשב המרוחק ייצור קשר עם היישום פעם נוספת.

אישור מאפשר את התקשורת הנכנסת.

מניעה מונע את התקשורת הנכנסת.

עריכת כלל - מאפשר להתאים אישית את מאפייני הכללים באמצעות עורך כללי חומת האש.

הגדרות תצוגת חיבור

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.

הצג 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**.

כלי אבטחה

פתח את חלון התוכנית הראשי > **הגדרות** > **כלי אבטחה** כדי להגן על המודולים הבאים:

גלישה ושירותים בנקאיים בטוחים הוספת שכבה נוספת של הגנת דפדפן שנועדה להגן על הנתונים הפיננסיים שלך במהלך עסקאות מקוונות. הפעל את האפשרות **אבטח את כל הדפדפנים** במקטע הגדרות מתקדמות של גלישה ושירותים בנקאיים בטוחים כדי להפעיל את כל דפדפני האינטרנט הנתמכים במצב מאובטח.

פרטיות ואבטחה בדפדפן -שומרת שהפעילות המקוונת שלך תהיה פרטית ובטוחה מבלי להשאיר טביעת רגל דיגיטלים.

מערכת נגד גניבה הפעל את מערכת נגד גניבה כדי להגן על המחשב שלך במקרה של אובדן או גניבה.

Secure Data כאשר התכונה Secure Data מופעלת, אתה יכול להצפין את הנתונים שלך כדי למנוע שימוש לרעה במידע פרטי וסודי.

Password Manager ⍰ הכלי Password Manager מגן על הסיסמאות ועל הנתונים האישיים שלך ומאחסן אותם.

גלישה ושירותים בנקאיים בטוחים

גלישה ושירותים בנקאיים בטוחים היא שכבת הגנה נוספת שתוכננה להגן על הנתונים הכספיים שלך במהלך ביצוע עסקאות מקוונות.

כברירת מחדל, כל דפדפני האינטרנט הנתמכים מופעלים במצב מאובטח. כך תוכל לגלוש באינטרנט, לגשת לאתרי בנקאות מקוונת ולבצע רכישות ועסקאות מקוונות בחלון אחד של דפדפן מאובטח ללא ניתוב מחדש.

> יש לאפשר את מערכת המוניטין של ®ESET LiveGrid (פועלת כברירת מחדל) כדי להבטיח את הפעולה התקינה של גלישה ושירותים בנקאיים בטוחים.

כדי להגדיר את ההתנהגות של דפדפן מאובטח, ראה הגדרות מתקדמות של גלישה ושירותים בנקאיים בטוחים. אם תשבית את **אבטח את כל הדפדפנים** תוכל לגשת לדפדפן המאובטח דרך חלון התוכנית הראשי > **סקירה כללית** > **גלישה ושירותים בנקאיים בטוחים** או על ידי לחיצה על סמל שולחן העבודה **גלישה ושירותים בנקאיים בטוחים**. הדפדפן, המוגדר כברירת מחדל ב-Windows, מופעל במצב מאובטח.

השימוש בתקשורת HTTPS מוצפנת הכרחי להשגת גלישה מאובטחת. הדפדפנים הבאים תומכים בגלישה ושירותים בנקאיים בטוחים:

- +Internet Explorer 8.0.0.0
- +Microsoft Edge 83.0.0.0
- +Google Chrome 64.0.0.0
- +Firefox 24.0.0.0

> המוצר תומך ב-Firefox וב-Microsoft Edge בלבד במכשירים עם מעבדי ARM.

לקבלת פרטים נוספים על התכונות של 'גלישה ושירותים בנקאיים בטוחים', קרא את המאמרים הבאים במאגר הידע של ESET הזמינים באנגלית ובמספר שפות נוספות:

- כיצד אוכל להשתמש בגלישה ושירותים בנקאיים בטוחים של ESET?
- השהה או השבת גלישה ושירותים בנקאיים בטוחים במוצרים הביתיים של ESET Windows
- גלישה ושירותים בנקאיים בטוחים של ESET
- מילון מונחים של ESET | גלישה ושירותים בנקאיים בטוחים

התראה בדפדפן

הדפדפן המאובטח מודיע לך על המצב הנוכחי שלו באמצעות התראות בדפדפן והצבע של מסגרת הדפדפן.

התראות בדפדפן מוצגות בכרטיסייה בצד.

כדי להרחיב את ההתראה בדפדפן, לחץ על סמל ESET. כדי למזער את ההתראה, לחץ על טקסט ההתראה. כדי

לבטל את ההודעה ואת מסגרת הדפדפן הירוקה, לחץ על סמל הסגירה .

ניתן לדחות רק את ההודעה האינפורמטיבית ואת מסגרת הדפדפן הירוקה.

התראות בדפדפן

סטטוס	סוג ההתראה
הגנה מרבית מובטחת וההתראה בדפדפן ממוזערת כברירת מחדל. הרחב את ההודעה בדפדפן ולחץ על **הגדרות** כדי לפתוח את הגדרת כלי האבטחה.	התראה אינפורמטיבית ומסגרת דפדפן ירוקה
הדפדפן המאובטח דורש את תשומת הלב שלך עבור בעיה לא קריטית. לקבלת מידע נוסף על הבעיה או פתרון, בצע את ההוראות שבהתראה בדפדפן.	אזהרה ומסגרת דפדפן כתומה
הדפדפן אינו מוגן על ידי התכונה 'גלישה ושירותים בנקאיים בטוחים של ESET'. הפעל מחדש את הדפדפן כדי להבטיח שההגנה פעילה. כדי לפתור התנגשות בקבצים שנטענו בדפדפן, פתח את רשומות יומן > '**גלישה ושירותים בנקאיים בטוחים**' וודא שהקבצים שנרשמו ביומן לא נטענו בהפעלה הבאה של הדפדפן. אם הבעיה נמשכת, פנה לתמיכה הטכנית של ESET על ידי ביצוע ההנחיות במאמר מאגר הידע שלנו.	התראת אבטחה ומסגרת דפדפן אדומה

פרטיות ואבטחה בדפדפן

באפשרותך להפעיל את התכונה 'פרטיות ואבטחה בדפדפן' באמצעות הרחבה מותאמת אישית שזמינה בדפדפנים נתמכים (Mozilla Firefox, Google Chrome ו-Microsoft Edge).

כדי להתקין ולהפעיל את התוסף:

1. ודא שאתה משתמש בגירסה העדכנית ביותר של ESET Smart Security Premium והפעל מחדש את המחשב לאחר העדכון.
2. פתח דפדפן.
3. התוסף מותקן בדפדפן שלך.
4. הפעל את התוסף ודפדפן כאשר דף הפרטים של התוסף מוצג.

התפריט הראשי של הרחבת הדפדפן 'פרטיות ואבטחה בדפדפן' מחולק לסעיפים הבאים:

מבט כולל

חיפוש בטוח

לחץ על סמל ההחלפה שליד **סרוק תוצאות חיפוש** כדי להפעיל את התכונה ולראות על אילו תוצאות אפשר ללחוץ. חיפוש בטוח מבצע הערכה של כתובות הקישורים המפורטות. זה לא בהכרח אומר שהאתר אינו מכיל תוכנות זדוניות. לאחר מכן, מנגנון האיתור שלנו מזהה כל תוכנה זדונית באתר.

ניקוי דפדפן

מחק את נתוני הגלישה שלך או הגדר ניקוי קבוע. אפשר להוסיף אתרים שבהם ברצונך לקבל קובצי Cookie ולהישאר מחובר גם לאחר ניקוי הדפדפן על ידי **הוספה שלהם לרשימה**.

- **ניקוי חד פעמי-** בחר את טווח הזמן מהתפריט הנפתח ואת סוג הנתונים שברצונך למחוק. אתה יכול לבחור בין כל הנתונים, פרטי או בהתאמה אישית.
- **ניקוי קבוע**לחץ על סמל ההחלפה שליד **ניקוי קבוע** כדי להפעיל את התכונה. בחר את טווח הזמן מהתפריט הנפתח ואת סוג הנתונים שברצונך למחוק באופן קבוע. אתה יכול לבחור בין כל הנתונים, פרטי או בהתאמה אישית.

האפשרות **נתונים מותאמים אישית** מכילה את הקטגוריות הבאות:

- היסטוריית גלישה
- היסטוריית הורדות
- קובצי Cookie ונתוני אתר
- תמונות וקבצים במטמון
- סיסמאות ונתוני כניסה
- נתוני מילוי אוטומטי של טפסים

ניקוי מטה-נתונים

התכונה 'ניקוי מטה-נתונים' שולטת בנתוני פרטיות שעלולים להיחשף באמצעות מטה-נתונים של EXIF ששותפו בקובצי מדיה, מסמכים ופורמטים אחרים של קבצים נתמכים. לחץ על סמל ההחלפה לצד **ניקוי מטה-נתונים בכל פעם שאתה מעלה תמונה** כדי לאפשר הסרת מטה-נתונים.

> עליך להפעיל מחדש את הדפדפן כדי לוודא ש**ניקוי מטה-נתונים** פועל כראוי.

לחץ על סמל ההחלפה שליד **קבל התראות בדפדפן** כדי לאפשר הצגת התראות לאחר ניקוי מטה-נתונים.

בדיקת הגדרות של אתר אינטרנט

גש ונהל הרשאות אתר בקלות כדי לקבוע באיזה מידע אתרי אינטרנט יכולים להשתמש.

- **התראות** - בדוק עבור אילו אתרים ברצונך **להתיר/לחסום** את ההתראות או אם ברצונך שהרחבת הדפדפן **תשאל אותך בכל פעם**.

הגדרות מתקדמות

ניקוי דפדפן

הגדרות מתקדמות של קובצי Cookie

רשימת אתרים שבהם ברצונך לקבל קובצי Cookie ולהישאר מחובר גם לאחר ניקוי הדפדפן. הזן את כתובת ה-URL בשדה הטקסט ולחץ על **הוסף**. אפשר להסיר אותה בכל עת מהרשימה על ידי לחיצה על סמל המינוס ליד האתר הספציפי.

בתחתית הדף מופיעה רשימת התחומים המוצעים שנפתחים עכשיו בדפדפן. אם אינך יכול לראות את האתר הספציפי, לחץ על **רענן את הרשימה** והוסף אותה לרשימת קובצי ה-Cookie שאושרו, על ידי לחיצה על סמל הפלוס .

בדיקת הגדרות של אתר אינטרנט

גש ונהל הרשאות אתר בקלות כדי לקבוע באיזה מידע אתרי אינטרנט יכולים להשתמש.

- **התראות** - בדוק עבור אילו אתרים ברצונך **להתיר/לחסום** את ההתראות או אם ברצונך שהרחבת הדפדפן **תשאל אותך בכל פעם**.

מראה

התאם אישית את ערכת הצבעים של הממשק כך שתתאים להעדפות שלך. באפשרותך לבחור את ערכת הצבעים המועדפת עליך על-ידי בחירה בתיבת הסימון **בהיר** או **כהה**.

מערכת נגד גניבה

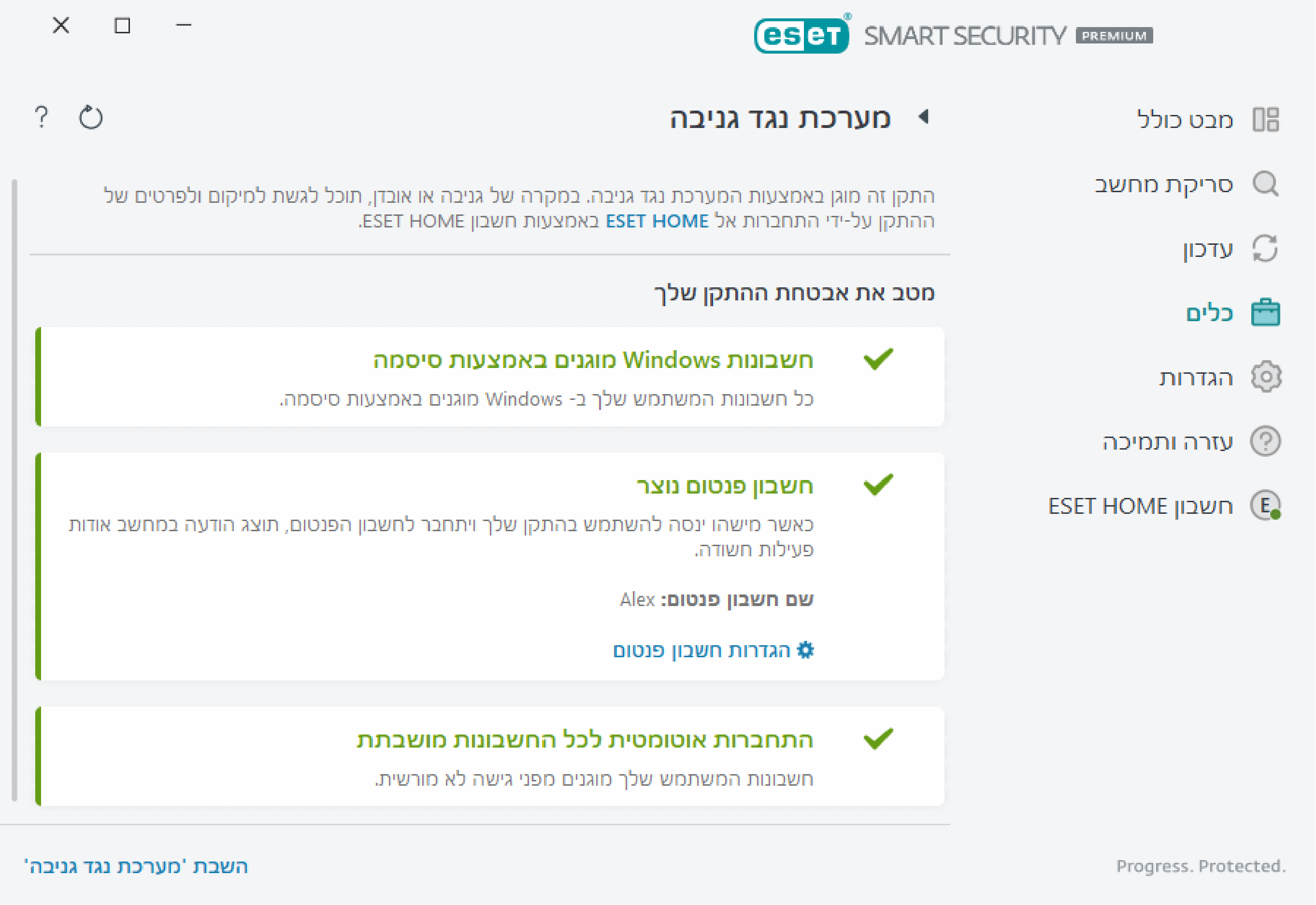
המכשירים האישיים שלנו נתונים בסיכון מתמיד לאובדן או גניבה בנסיעותינו היומיומיות מהבית לעבודה או במקומות ציבוריים אחרים. מערכת נגד גניבה היא תכונה שמרחיבה את האבטחה ברמת המשתמש במקרה של מכשיר שאבד או נגנב. מערכת נגד גניבה תאפשר לך לנטר את השימוש במכשיר החסר ולעקוב אחריו על-ידי איתור לפי כתובת IP ב-ESET HOME, ובכך תסייע לך להחזיר את המכשיר ולהגן על נתונים אישיים.

באמצעות טכנולוגיות מודרניות, כגון חיפוש גיאוגרפי של כתובת IP, צילום תמונות במצלמה אינטרנט, הגנה על חשבון משתמש וניטור מכשיר, מערכת נגד גניבה עשויה לעזור לך ולארגוני אכיפת החוק לאתר את המחשב או המכשיר שאבד או נגנב. תוכל לראות ב-ESET HOME איזו פעילות מתרחשת במחשב או במכשיר שלך.

למידע נוסף על מערכת נגד גניבה ב-ESET HOME, עיין בעזרה המקוונת של ESET HOME.

מערכת נגד גניבה יהיה עשוי שלא לפעול כראוי במחשבים המחוברים לתחומים עקב מגבלות בניהול חשבונות משתמשים.

לאחר הפעלת מערכת נגד גניבה, באפשרותך למטב את אבטחת המכשיר שלך בחלון התוכנית הראשי > **הגדרות** > **כלי אבטחה** > **מערכת נגד גניבה**.



אפשרויות מיטוב

לא נוצר חשבון פנטום

יצירת חשבון פנטום מגדילה את הסיכוי לאתר מכשיר שאבד או נגנב. אם תסמן את המכשיר כחסר, מערכת נגד גניבה יחסום את הגישה לחשבונות המשתמש הפעילים שלך כדי להגן על הנתונים הרגישים שלך. כל מי שינסה להשתמש במכשיר יורשה להשתמש בחשבון הפנטום בלבד. חשבון פנטום הוא סוג של חשבון אורח עם הרשאות מוגבלות. הוא ישמש כחשבון ברירת המחדל של המערכת עד שהמכשיר שלך יסומן כמכשיר שהוחזר תוך מניעת התחברות לחשבונות משתמש אחרים או גישה לנתונים של המשתמש.

> בכל פעם שמישהו יתחבר לחשבון הפנטום כאשר המחשב שלך במצב רגיל, תקבל הודעה בדוא"ל עם מידע לגבי פעילות חשודה במחשב שלך. לאחר קבלת ההודעה בדוא"ל, תוכל להחליט אם ברצונך לסמן את המחשב כחסר.

כדי ליצור חשבון פנטום, לחץ על **צור חשבון פנטום**, הקלד את **שם חשבון הפנטום** בשדה הטקסט ולחץ על **צור**.

לאחר שיצרת חשבון פנטום, לחץ על **הגדרות חשבון פנטום** כדי לשנות את שם החשבון או להסיר אותו.

הגנה באמצעות סיסמה על חשבונות Windows

חשבון המשתמש שלך אינו מוגן באמצעות סיסמה. אזהרת מיטוב זו תוצג אם חשבון משתמש אחד לפחות אינו מוגן באמצעות סיסמה. יצירת סיסמה עבור כל המשתמשים (למעט **חשבון פנטום**) במחשב תפתור בעיה זו.

כדי ליצור סיסמה עבור חשבון המשתמש, לחץ על **ניהול חשבונות Windows** ושנה את הסיסמה או בצע את ההוראות להלן:

1. הקש CTRL+Alt+Delete במקלדת.
2. לחץ על **שנה סיסמה**.
3. השאר את השדה **סיסמה ישנה** ריק.
4. הקלד את הסיסמה בשדות **סיסמה חדשה** ו**אשר סיסמה** והקש **Enter**.

התחברות אוטומטית לחשבונות Windows

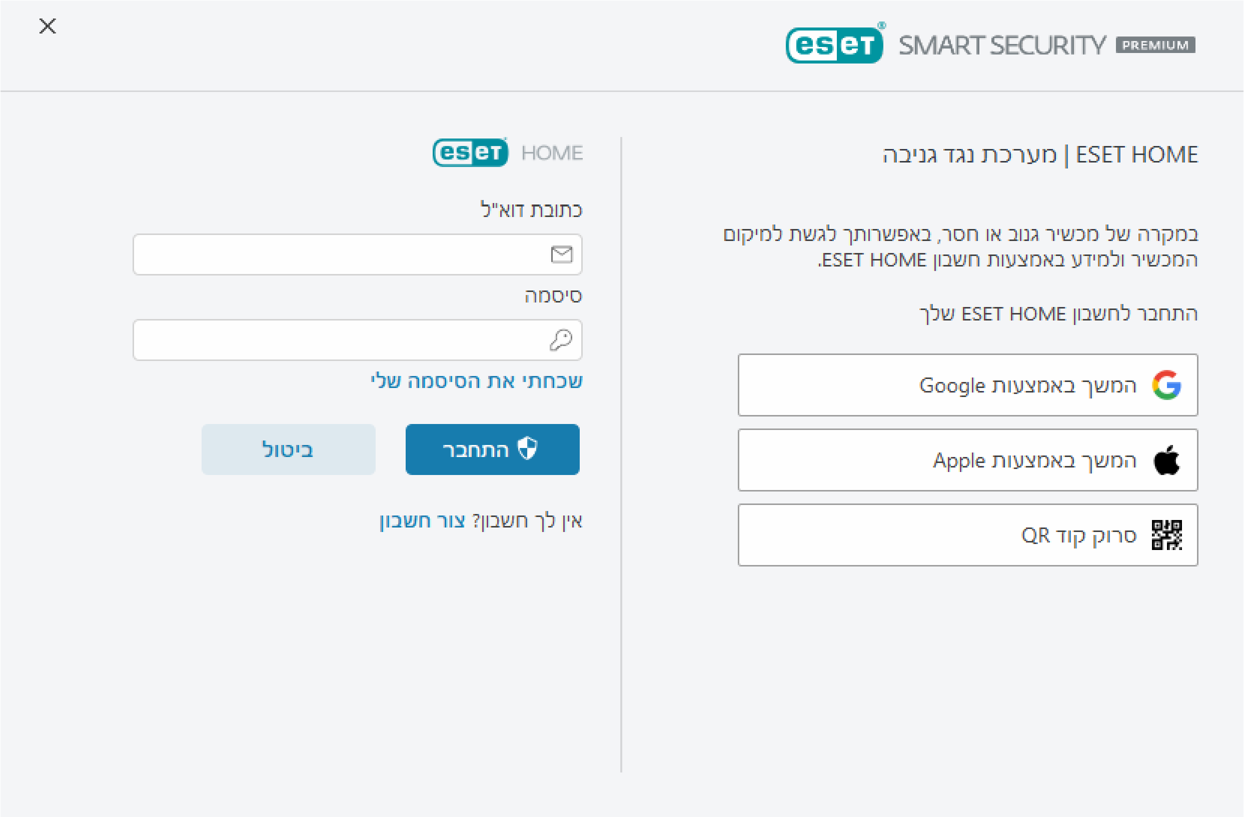
מופעלת התחברות אוטומטית לחשבון המשתמש שלך ולכן החשבון שלך אינו מוגן מפני גישה לא מורשית. אזהרת מיטוב זו תוצג אם מופעלת התחברות אוטומטית לחשבון משתמש אחד לפחות. לחץ על **השבת התחברות אוטומטית** כדי לפתור בעיית מיטוב זו.

התחברות אוטומטית לחשבון פנטום

מופעלת התחברות אוטומטית ל**חשבון פנטום** במכשיר שלך. כאשר המכשיר נמצא במצב רגיל, לא מומלץ להשתמש בהתחברות אוטומטית מכיוון שהיא עלולה לגרום לבעיות בגישה לחשבון המשתמש האמיתי שלך או לשלוח התראות שווא לגבי המצב החסר של המחשב. לחץ על **השבת התחברות אוטומטית** כדי לפתור בעיית מיטוב זו.

התחבר לחשבון ESET HOME שלך

כדי להפעיל/להשבית את מערכת נגד גניבה ולגשת למיקום המכשיר ולמידע ב-ESET HOME, התחבר לחשבון ESET HOME שלך.



קיימות מספר שיטות זמינות להתחברות לחשבון ESET HOME שלך:

- **השתמש בכתובת הדוא"ל והסיסמה של חשבון ESET HOME שלך** הזן את **כתובת הדוא"ל** ואת **הסיסמה** שבהן השתמשת כדי ליצור את חשבון ESET HOME שלך ולחץ על **התחברות**.
- **השתמש בחשבון Google/AppleID** לחץ על **המשך באמצעות Google** או על **המשך באמצעות Apple** והתחבר לחשבון המתאים. לאחר שתתחבר בהצלחה, תנותב אל דף האישור המקוון של ESET HOME. כדי להמשיך, חזור לחלון המוצר של ESET. לקבלת מידע נוסף על התחברות באמצעות חשבון Google/AppleID, עיין בהוראות ESET HOMEבעזרה המקוונת.
- **סרוק קוד QR** לחץ על **סרוק קוד QR** כדי להציג את קוד ה-QR. פתח את אפליקציית ESET HOME לנייד וסרוק את קוד ה-QR או כוון את מצלמת המכשיר לקוד ה-QR. לקבלת מידע נוסף, עיין בהוראות ESET HOMEבעזרה המקוונת.

ההתחברות נכשלה שגיאות נפוצות.

אם אין לך חשבון ESET HOME, לחץ על **צור חשבון** כדי להירשם או עיין בהוראות בעזרה המקוונת של ESET HOME.
אם שכחת את הסיסמה, לחץ על **שכחתי את הסיסמה שלי** ובצע את השלבים המוצגים במסך או עיין בהוראות בעזרה המקוונת ESET HOME.

מערכת נגד גניבה אינו תומך ב-Microsoft Windows Home Server.

הגדר שם מכשיר

השדה **שם המכשיר** מייצג את שם המחשב (המכשיר) שלך שיוצג כמזהה בכל שירותי ESET HOME. ייעשה שימוש כברירת מחדל בשם המחשב של המחשב שלך. הקלד את שם המכשיר או השתמש בשם ברירת המחדל ולחץ על **המשך**.

מערכת נגד גניבה מופעל/מושבת

חלון זה מכיל הודעת אישור בעת הפעלה/השבתה של מערכת נגד גניבה:

- מופעל המכשיר שלך מוגן כעת באמצעות מערכת נגד גניבה, ותוכל לנהל את האבטחה שלו מרחוק בפורטל ESET HOME באמצעות החשבון שלך.
- מושבת מערכת נגד גניבה מושבתת במכשיר זה, וכל הנתונים הקשורים של <%ESET_ANTTHEFT%> לגבי מכשיר זה יוסרו מפורטל ESET HOME.

הוספת מכשיר חדש נכשלה

קיבלת הודעת שגיאה בעת הפעלת מערכת נגד גניבה.

התרחישים הנפוצים ביותר הם:

- שגיאה בהתחברות אל ESET HOME
- אין קישוריות אינטרנט (או שהאינטרנט לא פעיל כרגע)

אם אינך מצליח לפתור את הבעיה, פנה אל התמיכה הטכנית של ESET.

Secure Data

Secure Data היא תכונה ב-ESET Smart Security Premium המאפשרת לך להצפין נתונים במחשב שלך ובכוננים נשלפים כדי להגן על המידע הפרטי שלך ולמנוע שימוש לרעה. עיין בשאלות הנפוצות על ESET Secure Data לקבלת מידע נוסף.

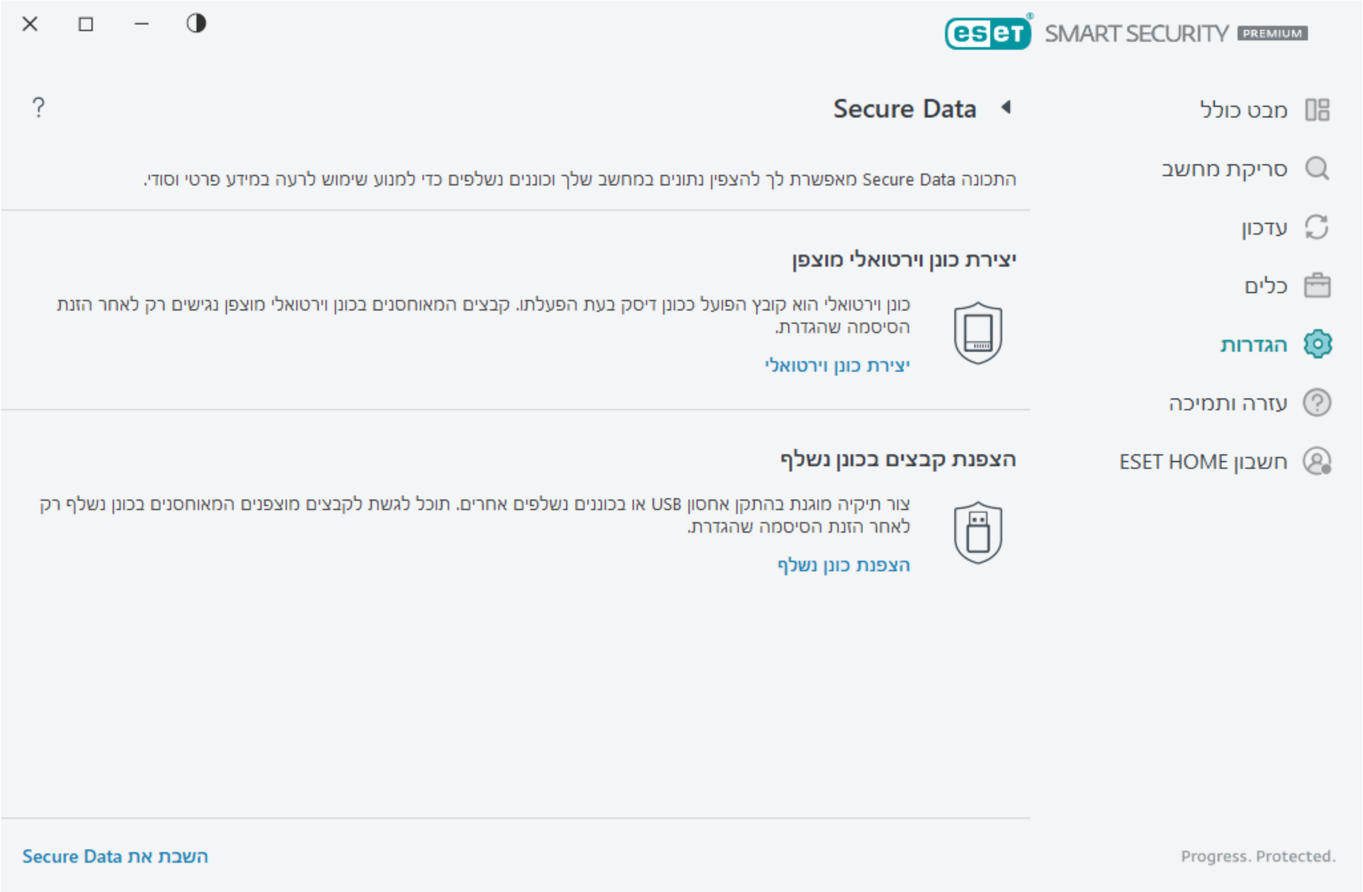
כדי לאפשר את Secure Data, בחר באחת מהאפשרויות להלן:

- בחלון התוכנית הראשי > **מבט כולל**, לחץ על **הגדרה** ליד **Secure Data**.
- בחלון התוכנית הראשי > **הגדרה** > **כלי אבטחה**, הפעל את המתג **Secure Data**.

> לא ניתן להתקין את ESET Endpoint Encryption באותו מחשב שבו כבר מותקן Secure Data.

כאשר התכונה Secure Data פעילה, בחלון התוכנית הראשי, לחץ על **הגדרה** > **כלי אבטחה** > **Secure Data** ובחר אחת מאפשרויות ההצפנה הבאות:

- יצירת כונן וירטואלי מוצפן
- הצפנת קבצים בכונן נשלף



יצירת כונן וירטואלי מוצפן

אתה יכול להשתמש ב- Secure Data ליצירת כוננים וירטואליים מוצפנים. אין מגבלה למספר הכוננים שאפשר ליצור, כל עוד יש להם שטח לשימוש בכונן הקשיח. בצע את השלבים הבאים כדי ליצור כונן וירטואלי מוצפן:

1. בחלון התוכנית הראשי, לחץ על **הגדרה** > **כלי אבטחה** > **Secure Data** > **יצירת כונן וירטואלי**.
2. לחץ על **עיון** כדי לבחור במיקום שבו ברצונך לשמור את הכונן הווירטואלי.
3. הזן שם עבור הכונן הווירטואלי ולחץ על **שמור**.
4. השתמש בתפריט הנפתח **קיבולת מקסימלית** כדי להגדיר את גודל הכונן הווירטואלי שלך ולחץ על **המשך**.
5. הגדר סיסמה עבור הכונן הווירטואלי שלך. אם אינך רוצה שהכונן הווירטואלי יפוענח אוטומטית כשאתה מתחבר לחשבון Windows שלך, בטל את הבחירה באפשרות **פענח אוטומטית בחשבון Windows זה**. לחץ על **המשך**.
6. לחץ על **סיום**. הכונן הווירטואלי המוצפן שלך נוצר ומוכן לשימוש. הוא יופיע כדיסק מקומי אם תפתח את **מחשב זה**.

כדי לגשת לכונן המוצפן לאחר הפעלה מחדש של המחשב, אתר את הקובץ של הכונן המוצפן (סוג קובץ .eed) שיצרת ולחץ עליו פעמיים. אם תתבקש לעשות זאת, הזן את הסיסמה שהוגדרה כשיצרת את הכונן המוצפן. הכונן ייטען ויופיע ככונן מקומי ב'מחשב זה'. כאשר הכונן המוצפן נטען כדיסק מקומי, הדיסק המקומי ותוכנו המוצפן יהיו זמינים למשתמשים אחרים במחשב שלך, אלא אם תתנתק או תפעיל מחדש את המחשב.

> **האם ניתן להסיר כונן וירטואלי?**
> כן. כדי להסיר כונן וירטואלי מוצפן, בצע את ההוראות בשאלות הנפוצות על ESET Secure Data.

הצפנת קבצים בכונן נשלף

Secure Data מאפשר לך ליצור תיקיה מוצפנת בכוננים נשלפים. בצע את השלבים הבאים כדי להצפין קבצים בכונן נשלף:

1. הכנס את הכונן הנשלף (כונן הבזק מסוג USB, דיסק קשיח מסוג USB) לתוך המחשב.
2. בחלון התוכנית הראשי, לחץ על **הגדרות** > **כלי אבטחה** > **Secure Data** > **הצפנת כונן נשלף**.
3. בחר בכונן הנשלף המחובר להצפנה ולחץ על **המשך**.
לחץ על **רענן** כדי לעדכן את רשימת הכוננים הניתנים להצפנה. כוננים מוצפנים או כוננים שאינם נתמכים אינם מוצגים ברשימה.
אם ברצונך לפענח את התיקיה המאובטחת בכונן הנשלף שנבחר במכשיר Windows ללא צורך להתקין את ESET Smart Security Premium, בחר **פענח את התיקיה במכשיר Windows**.
4. הגדר סיסמה עבור הספריה המוצפנת. אם אינך רוצה שהכונן הווירטואלי יפוענח אוטומטית כשאתה מתחבר לחשבון Windows שלך, בטל את הבחירה באפשרות **פענח אוטומטית בחשבון Windows זה**. לחץ על **המשך**.
5. הכונן הנשלף שלך מוגן והספריה המוצפנת בו מוכנה לשימוש.

מעתה והלאה, אם תחבר את הכונן הנשלף שלך למחשב שבו Secure Data אינו מותקן, התיקיה המוצפנת לא תוצג. אם הכונן הנשלף יחובר למחשב שבו מותקן Secure Data, תתבקש להזין את הסיסמה כדי לפענח את הכונן הנשלף. אם לא תקליד סיסמה, התיקיה המוצפנת תוצג, אך לא תהיה נגישה.

Password Manager

Password Manager הוא חלק מחבילת ESET Smart Security Premium.

זהו מנהל סיסמאות שמגן על הסיסמאות ועל הנתונים האישיים שלך ומאחסן אותם. הוא גם כולל תכונת מילוי טפסים, אשר חוסכת זמן הודות למילוי אוטומטי ומדויק של טופסי אינטרנט.

עיין בעזרה המקוונת של Password Manager לקבלת מידע נוסף:

- התקנת Password Manager
- התחל להשתמש ב-Password Manager.
- ניהול מאגרי סיסמאות של Password Manager ב-ESET HOME

הגדרות יבוא ויצוא

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

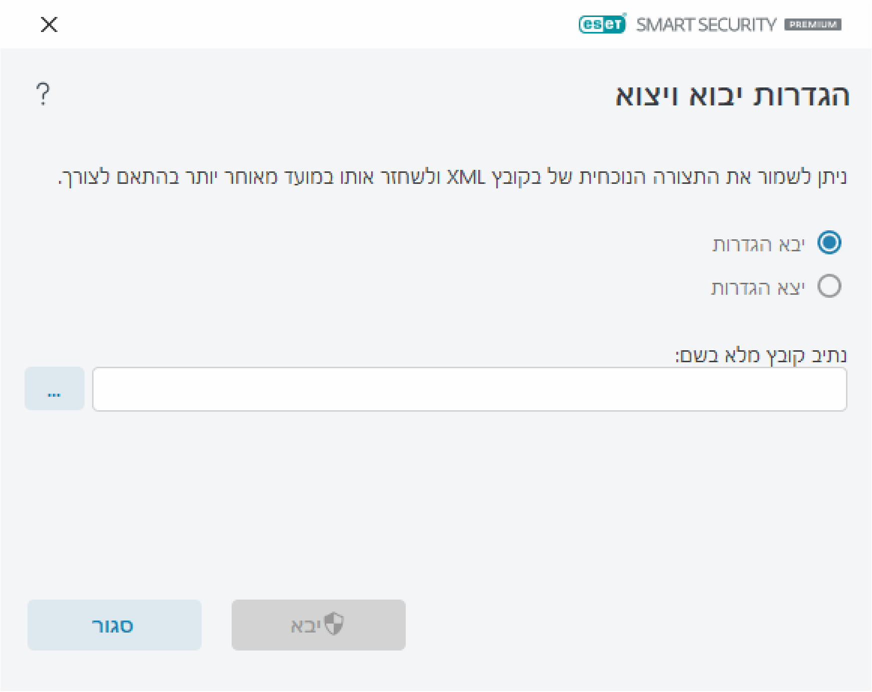
> **הנחיות מאוירות**
> ראה ייבוא או ייצוא של הגדרות תצורה של ESET באמצעות קובץ .xml לקבלת הנחיות מאוירות הזמינות באנגלית ובמספר שפות אחרות.

ייבוא או ייצוא של קובצי תצורה שימושיים כשעליך לגבות את התצורה הנוכחית של ESET Smart Security Premium לשימוש במועד מאוחר יותר. אפשרות הגדרות הייצוא נוחה גם כאשר אתה מעוניין להשתמש בתצורה המועדפת עליך במערכות שונות. באפשרותם לייבא קובץ .xml כדי להעביר את ההגדרות הללו.

כדי לייבא תצורה, ב[חלון התוכנית הראשי](#), לחץ על **הגדרות** < **ייבוא/ייצוא הגדרות** ובחר באפשרות **ייבא הגדרות**. הזן את שם קובץ התצורה או לחץ על הלחצן **...** כדי לאתר את קובץ התצורה שברצונך לייבא.

כדי לייצא תצורה, ס[חלון התוכנית הראשי](#), לחץ על **הגדרות** < **ייבוא/ייצוא הגדרות**. בחר באפשרות **ייצוא הגדרות** והזן את נתיב הקובץ המלא ביחד עם שם הקובץ. לחץ על **...** כדי לנווט אל מיקום שמירת קובץ התצורה במחשב.

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



עזרה ותמיכה

לחץ על **עזרה ותמיכה** [בחלון התוכנית הראשי](#) כדי להציג את פרטי התמיכה וכלים לפתרון בעיות שיסייעו לך לפתור בעיות שבהן אתה עלול להיתקל.

מנוי

- [פתרון בעיות במינוי](#) לחץ על קישור זה כדי למצוא פתרונות לבעיות בהפעלה או בשינוי של מינוי.
- [החלף מינוי](#) לחץ כדי להפעיל את חלון ההפעלה ולהפעיל את המוצר. אם המכשיר [מחובר אל ESET HOME](#), בחר מינוי מחשבון ESET HOME שלך או הוסף מינוי חדש.

מוצר מותקן

- [מה חדש](#) לחץ על אפשרות זו כדי לפתוח את חלון המידע על תכונות חדשות ומשופרות.
- [אודות ESET Smart Security Premium](#) הצגת מידע על העותק של ESET Smart Security Premium שברשותך.
- [פתרון בעיות במוצר](#)לחץ על הקישור הזה כדי למצוא פתרונות לבעיות הנפוצות ביותר.
- **שנה מוצר** לחץ כדי לבדוק אם ניתן לשנות את ESET Smart Security Premium [לקו מוצרים שונה](#) באמצעות המינוי הנוכחי.

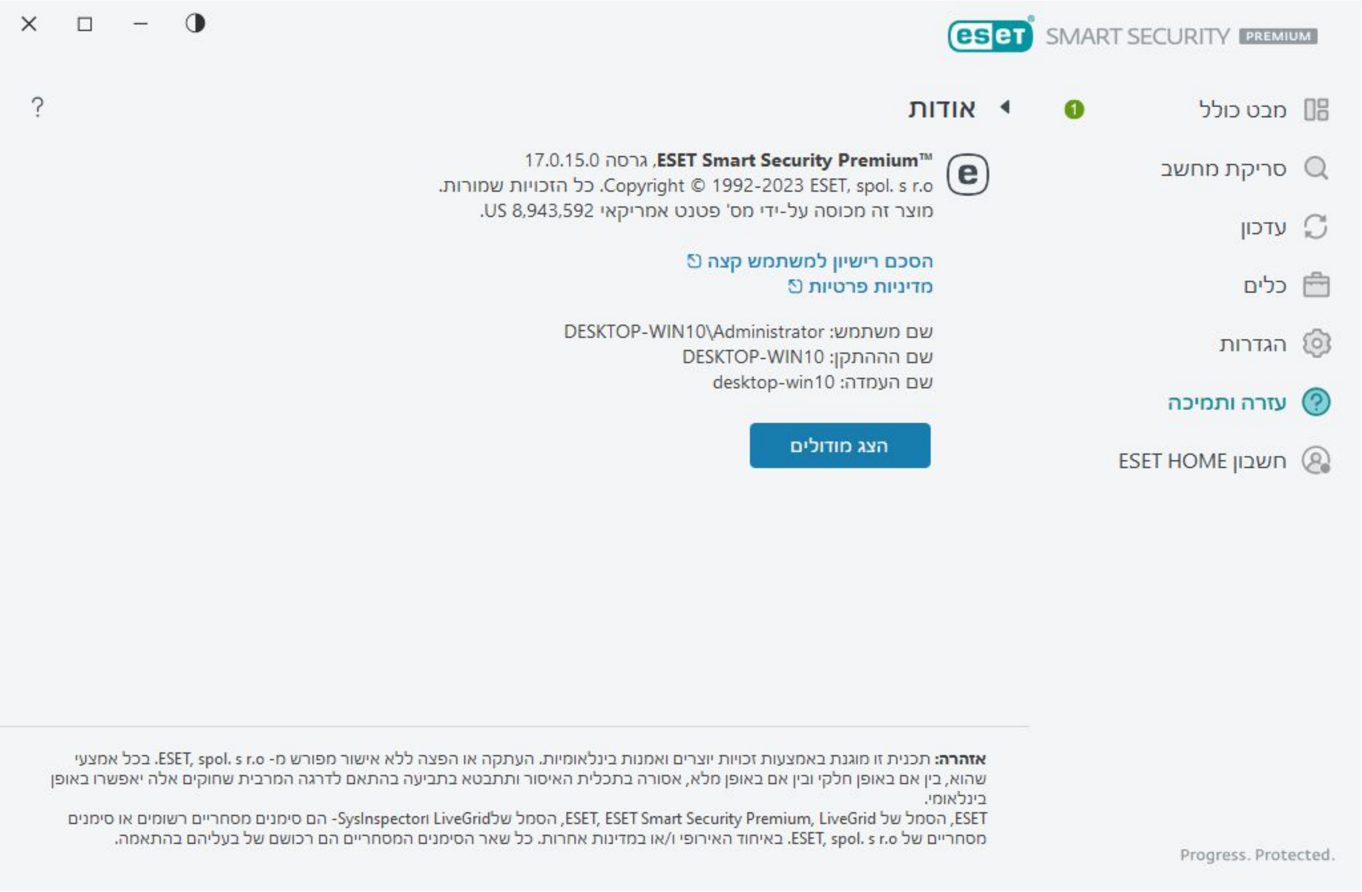
דף העזרה לחץ על קישור זה להפעלת דפי העזרה של ESET Smart Security Premium.

[תמיכה טכנית](#)

מאגר הידע של – [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.

אודות ESET Smart Security Premium

חלון זה מספק פרטים על הגירסה המותקנת של ESET Smart Security Premium והמחשב שלך.



לחץ על **הצג מודולים** כדי לראות מידע על רשימת מודולי התכנית שנטענו.

- 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.
- לחץ על **מנגנון איתור** בחלון 'מודולים' כדי לפתוח את רדאר הווירוסים של ESET, המכיל מידע על כל גרסה של מנגנון האיתור של ESET.

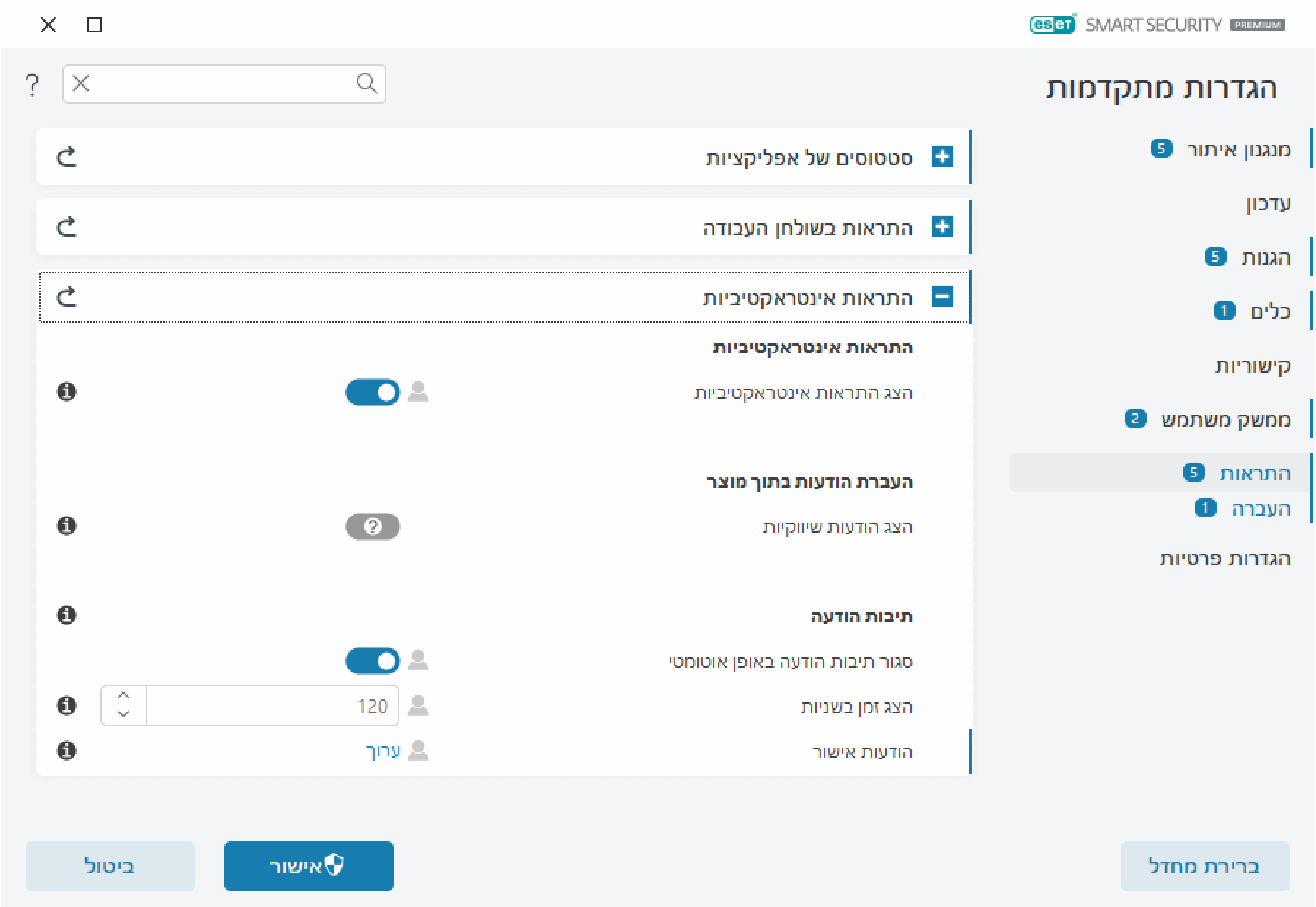
חדשות ESET

בחלון זה, ESET Smart Security Premium מיידע אותך על החדשות של ESET באופן קבוע.

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 את האפשרות **הצג הודעות שיווקיות**.

כדי להפעיל או להשבית קבלת הודעות שיווקיות דרך חלון ההתראות, פעל בהתאם להוראות הבאות.

1. פתיחת הגדרות מתקדמות.
2. לחץ על **התראות** > **התראות אינטראקטיביות**.
3. שנה את האפשרות **הצג הודעות שיווקיות**.



שלח נתוני תצורת מערכת

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

לאחר שליחת טופס האינטרנט, נתוני תצורת המערכת שלך יישלחו אל ESET. בחר באפשרות **שלח תמיד מידע זה** אם

ברצונך לזכור את הפעולה עבור תהליך זה. כדי לשלוח את טופס האינטרנט מבלי לשלוח נתונים כלשהם, לחץ על **אל תשלח נתונים** והמשך.

באפשרותך לקבוע את התצורה של שליחת נתוני תצורת המערכת דרך הגדרות מתקדמות > **כלים** > **אבחון** > תמיכה טכנית.

אם החלטת לשלוח נתוני תצורת מערכת, יש למלא ולשלוח את טופס האינטרנט. אחרת, הכרטיס שלך לא ייווצר ונתוני תצורת המערכת שלך יילכו לאיבוד. אם לא ניתן לשלוח את נתוני תצורת המערכת, מלא את טופס האינטרנט והמתן להוראות מהתמיכה הטכנית.

תמיכה טכנית

לחץ על **עזרה ותמיכה** > **תמיכה טכנית** בחלון התוכנית הראשי.

צור קשר עם התמיכה הטכנית

בקש תמיכה ⍰ אם לא מצאת תשובה לבעייתך, באפשרותך להשתמש בטופס זה הנמצא באתר האינטרנט של ESET כדי לפנות במהירות אל התמיכה הטכנית של ESET. החלון שליחת נתוני תצורת המערכת שלך יוצג לפני מילוי הטופס המקוון, בהתבסס על ההגדרות שלך.

קבל מידע עבור תמיכה טכנית

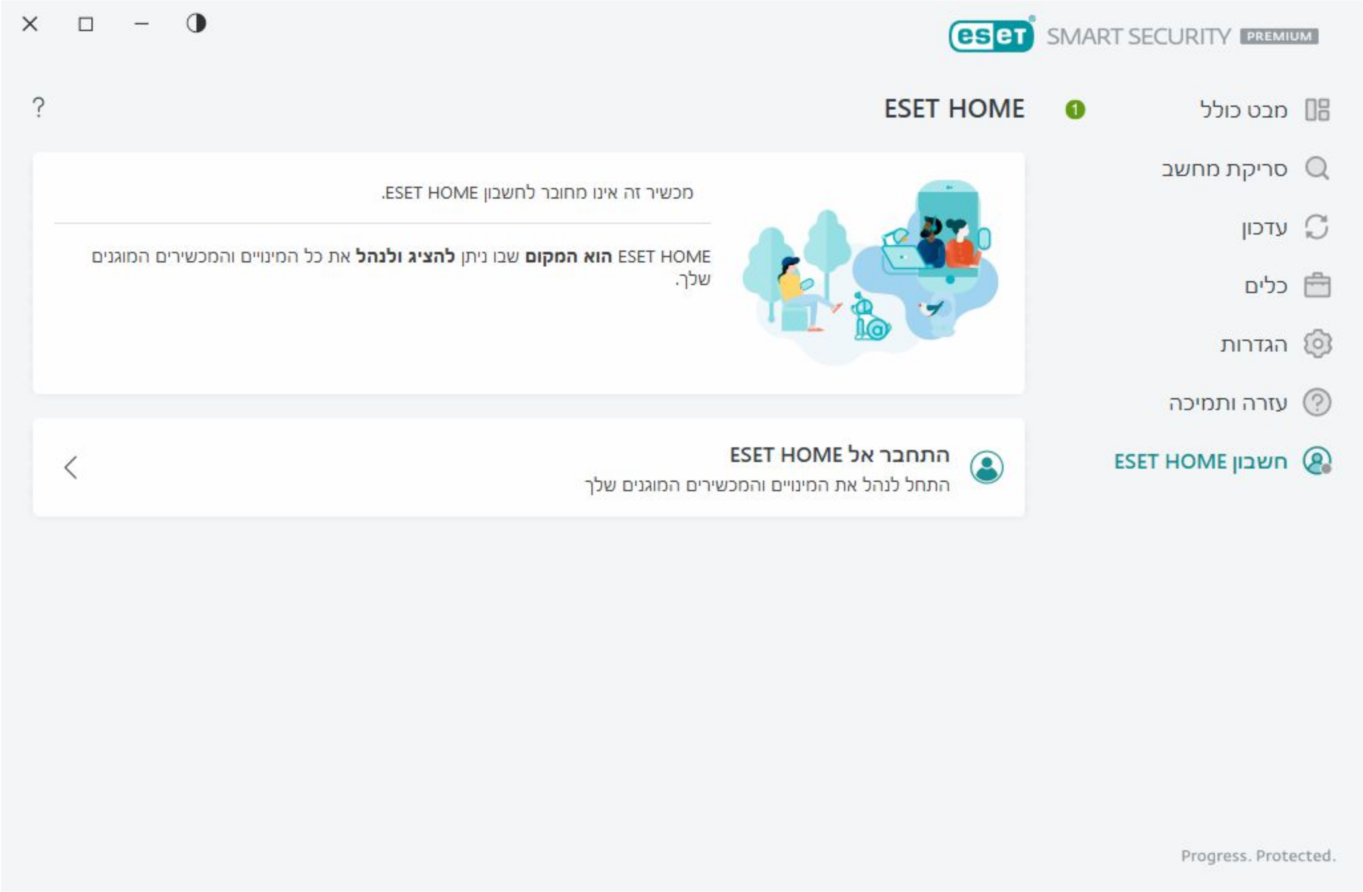
פרטים לתמיכה טכנית ⍰ כאשר תתבקש, תוכל להעתיק ולשלוח מידע לתמיכה הטכנית של ESET (כגון פרטי המינוי, שם המוצר, גרסת המוצר, מערכת ההפעלה ופרטי המחשב).

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 Log Collector למשתמש.

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.

חשבון ESET HOME

תוכל לסקור את סטטוס החיבור של חשבון ESET HOME בחלון התוכנית הראשי > **חשבון ESET HOME**.



מכשיר זה אינו מחובר לחשבון ESET HOME

לחץ על התחבר אל ESET HOME כדי לחבר את המכשיר שלך אל ESET HOME ולנהל את המינויים והמכשירים המוגנים שלך. באפשרותך לחדש, לשדרג ולהאריך את המינוי שלך ולהציג פרטים חשובים. בפורטל הניהול או באפליקציה לנייד של ESET HOME, באפשרותך להוסיף מינויים שונים, להוריד מוצרים למכשירים שלך, לבדוק את סטטוס האבטחה של המוצר או לשתף מינוי בדוא"ל. למידע נוסף, בקר בעזרה המקוונת של ESET HOME.

מכשיר זה מחובר לחשבון ESET HOME

באפשרותך לנהל מרחוק את אבטחת המכשיר שלך באמצעות פורטל ESET HOME או האפליקציה לנייד. לחץ על **App Store** או על **Google Play** כדי להציג קוד QR שניתן לסרוק באמצעות הטלפון הנייד כדי להוריד את אפליקציית ESET HOME לנייד מה-App Store או מ-Google Play.

חשבון ESET HOME שם חשבון ESET HOME שלך.

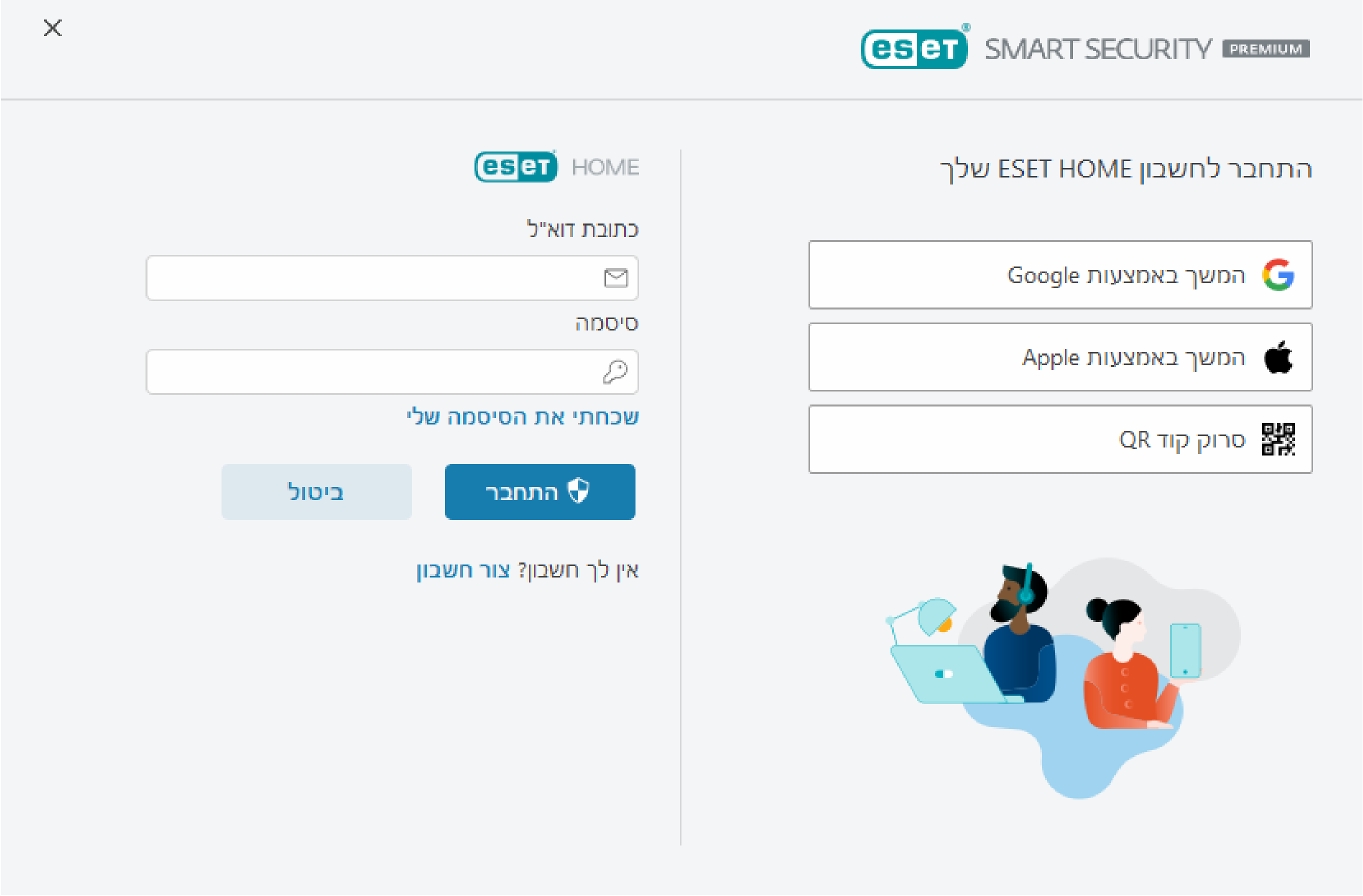
שם המכשיר השם של מכשיר זה המוצג בחשבון ESET HOME.

פתח את ESET HOME פתיחת פורטל הניהול של ESET HOME.

כדי לנתק את המכשיר מחשבון ESET HOME, לחץ על **נתק מ-ESET HOME** > **נתק**. המינוי המשמש להפעלה יישאר פעיל, והמכשיר שלך יהיה מוגן.

התחבר אל ESET HOME

חבר את המכשיר שלך אל ESET HOME כדי להציג ולנהל את כל המינויים והמכשירים המופעלים של ESET שברשותך. באפשרותך לחדש, לשדרג ולהאריך את המינוי שלך ולהציג פרטים חשובים של המינוי. בפורטל הניהול או באפליקציה לנייד של ESET HOME, באפשרותך להוסיף מינויים שונים, להוריד מוצרים למכשירים שלך, לבדוק את סטטוס האבטחה של המוצר או לשתף מינוי בדוא"ל. למידע נוסף, בקר בעזרה המקוונת של ESET HOME.



כדי לחבר את המכשיר שלך ל-ESET HOME:

> אם אתה מתחבר אל ESET HOME במהלך התקנה או בעת בחירה באפשרות **השתמש בחשבון ESET HOME** כשיטת הפעלה, בצע את ההוראות המפורטות בנושא שימוש בחשבון ESET HOME.
> אם כבר התקנת והפעלת את ESET Smart Security Premium באמצעות מינוי שהוספת לחשבון ESET HOME שלך, תוכל לחבר את המכשיר שלך ל-ESET HOME באמצעות פורטל ESET HOME. בצע את ההוראות בESET HOME מדריך העזרה המקוונת ואפשר את החיבור ב-ESET Smart Security Premium.

1. בחלון התוכנית הראשי, לחץ על **חשבון ESET HOME** < **התחבר אל ESET HOME** או לחץ על **התחבר אל ESET HOME** בהתראה **חבר מכשיר זה לחשבון ESET HOME**.
2. התחבר לחשבון ESET HOME שלך.

> אם אין לך חשבון ESET HOME, לחץ על **צור חשבון** כדי להירשם או עיין בהוראות בעזרה המקוונת של ESET HOME.
> אם שכחת את הסיסמה, לחץ על **שכחתי את הסיסמה שלי** ובצע את השלבים המוצגים במסך או עיין בהוראות בעזרה המקוונת ESET HOME.

3. הגדר **שם מכשיר** ולחץ על **המשך**.

4. לאחר שתצליח להתחבר יוצג חלון פרטים. לחץ על **סיום**.

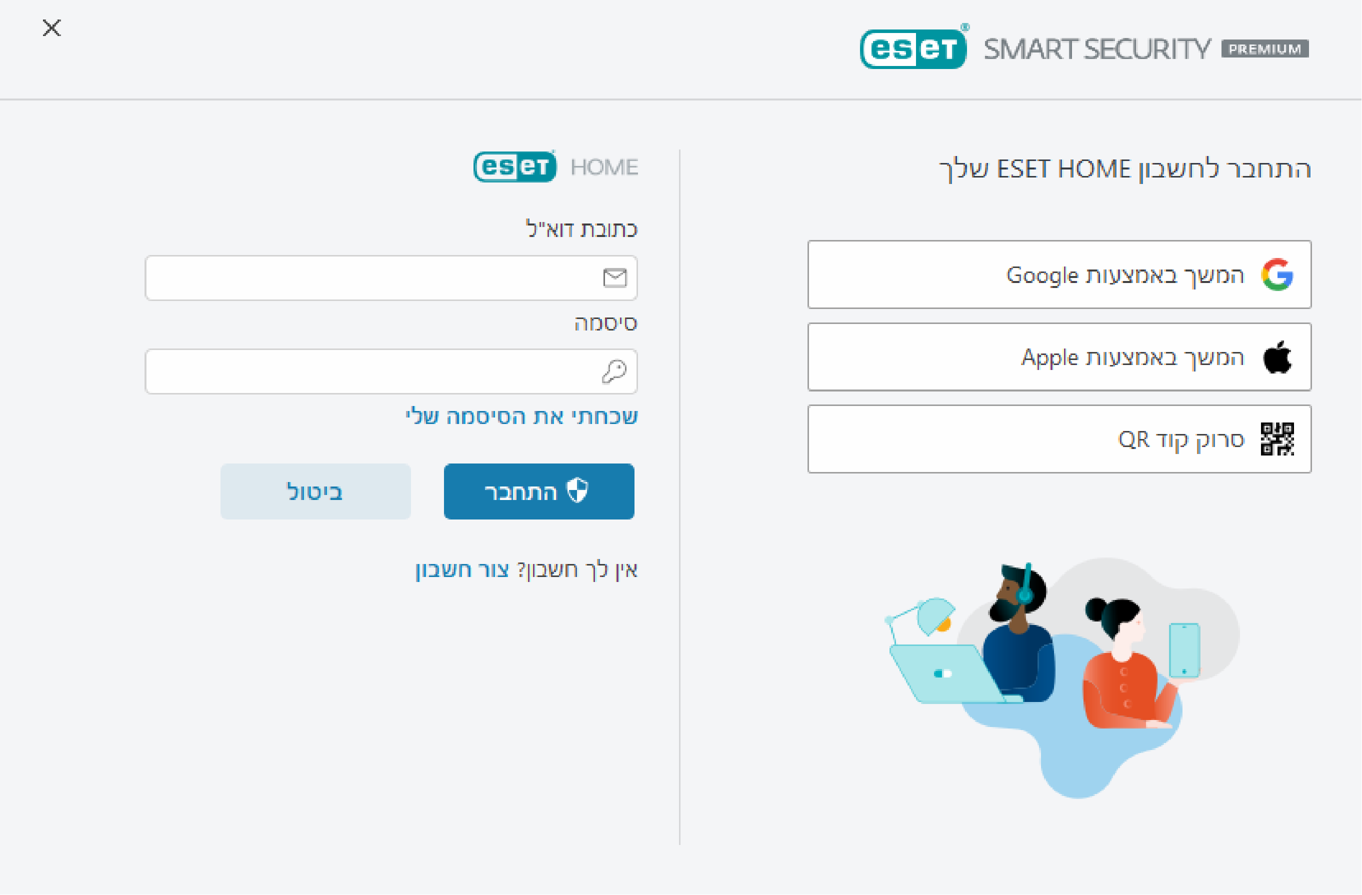
התחברות לחשבון ESET HOME

קיימות מספר שיטות זמינות להתחברות לחשבון ESET HOME שלך:

- **השתמש בכתובת הדוא"ל והסיסמה של חשבון ESET HOME שלך** הזן את **כתובת הדוא"ל** ואת **הסיסמה** שבהן השתמשת כדי ליצור את חשבון ESET HOME שלך ולחץ על **התחברות**.
- **השתמש בחשבון Google/AppleID** לחץ על **המשך באמצעות Google** או על **המשך באמצעות Apple** והתחבר לחשבון המתאים. לאחר שתתחבר בהצלחה, תנותב אל דף האישור המקוון של ESET HOME. כדי להמשיך, חזור לחלון המוצר של ESET. לקבלת מידע נוסף על התחברות באמצעות חשבון Google/AppleID, עיין בהוראות ESET HOMEבעזרה המקוונת.
- **סרוק קוד QR** לחץ על **סרוק קוד QR** כדי להציג את קוד ה-QR. פתח את אפליקציית ESET HOME לנייד וסרוק את קוד ה-QR או כוון את מצלמת המכשיר לקוד ה-QR. לקבלת מידע נוסף, עיין בהוראות ESET HOMEבעזרה המקוונת.

אם אין לך חשבון ESET HOME, לחץ על **צור חשבון** כדי להירשם או עיין בהוראות בעזרה המקוונת של ESET HOME.
אם שכחת את הסיסמה, לחץ על **שכחתי את הסיסמה שלי** ובצע את השלבים המוצגים במסך או עיין בהוראות בעזרה המקוונת ESET HOME.

ההתחברות נכשלה שגיאות נפוצות.



ההתחברות נכשלה שגיאות נפוצות

לא הצלחנו למצוא חשבון שתואם לכתובת הדוא"ל שהוזנה

כתובת הדוא"ל שהזנת אינה תואמת לאף חשבון ESET HOME. לחץ על **הקודם** והזן את כתובת הדוא"ל והסיסמה המתאימים.

עליך ליצור חשבון ESET HOME כדי להתחבר. אם אין לך חשבון ESET HOME, לחץ על **הקודם** > **צור חשבון** או עיין ביצירת חשבון ESET HOME חדש.

שם המשתמש והסיסמאות לא מתאימים

הסיסמה שהוזנה לא מתאימה לכתובת הדוא"ל שהוזנה. לחץ על **חזרה**, הקלד את הסיסמה הנכונה וודא שכתובת הדוא"ל שהוקלדה נכונה. אם עדיין אינך מצליח להתחבר, לחץ על **הקודם** > **שכחתי את הסיסמה שלי** כדי לאפס את הסיסמה שלך ובצע את השלבים המוצגים במסך או עיין בשכחתי את סיסמת ESET HOME שלי.

אפשרות ההתחברות שנבחרה לא תואמת את החשבון שלך

החשבון שלך מקושר לחשבון המדיה החברתית שלך. כדי להתחבר אל ESET HOME, לחץ על **המשך באמצעות Google** או על **המשך באמצעות Apple** והתחבר לחשבון המתאים. לאחר שתתחבר בהצלחה, תנותב אל דף האישור המקוון של ESET HOME. תוכל לנתק את חשבון המדיה החברתית שלך מחשבון ESET HOME בפורטל ESET HOME.

סיסמה שגויה

שגיאה זו עלולה להתרחש אם ESET Smart Security Premium כבר מחובר ל-ESET HOME ואתה מבצע שינויים המחייבים התחברות (לדוגמה, השבתת המערכת נגד גניבה) והסיסמה שהזנת אינה תואמת לחשבון שלך. לחץ על **הקודם** והקלד את הסיסמה המתאימה. אם עדיין אינך מצליח להתחבר, לחץ על **הקודם** > **שכחתי את הסיסמה שלי** כדי לאפס את הסיסמה שלך ובצע את השלבים המוצגים במסך או עיין בשכחתי את סיסמת ESET HOME שלי.

הוספת מכשיר ב-ESET HOME

אם כבר התקנת והפעלת את ESET Smart Security Premium באמצעות מינוי שהוספת לחשבון ESET HOME שלך, תוכל לחבר את המכשיר שלך ל-ESET HOME באמצעות פורטל ESET HOME:

1. שלח בקשת חיבור למכשיר שלך.
2. ESET Smart Security Premium יציג את חלון תיבת הדו-שיח **חיבור מכשיר זה לחשבון ESET HOME** בצירוף שם חשבון ESET HOME. לחץ על **אפשר** כדי לחבר את המכשיר לחשבון ESET HOME שהוזכר.

> אם לא תבצע פעולה כלשהי, בקשת החיבור תבוטל באופן אוטומטי לאחר כ-30 דקות.

הגדרות מתקדמות

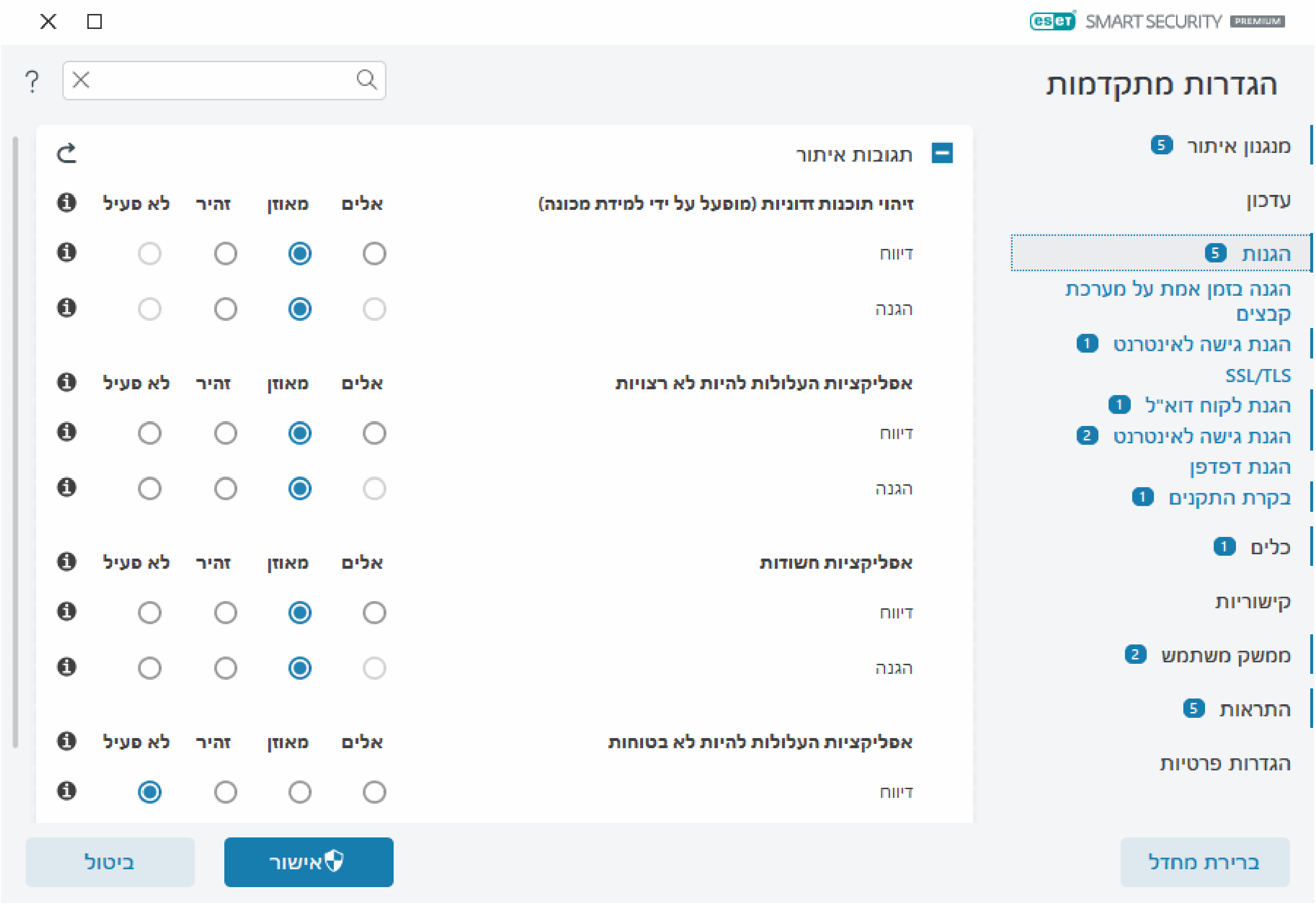
הגדרות מתקדמות מאפשרות לך להגדיר הגדרות מפורטות של ESET Smart Security Premium כך שיתאימו לצרכים שלך.

כדי לפתוח הגדרות מתקדמות, פתח את חלון התוכנית הראשי ולחץ על מקש **F5** במקלדת או לחץ על **הגדרה** > **הגדרות מתקדמות**.

בהתאם להגדרת הגישה שלך, ייתכן שתתבקש להקליד סיסמה כדי לפתוח את ההגדרות המתקדמות.

בהגדרות המתקדמות אפשר לקבוע את ההגדרות הבאות:

- מנגנון איתור
- עדכון
- הגנות
- כלים
- קישוריות
- ממשק משתמש
- התראות
- הגדרות פרטיות



מנגנון איתור

הגדרות מתקדמות > **מנגנון איתור** מאפשר לך להגדיר את האפשרויות הבאות:

- אי הכללה
- אפשרויות מתקדמות
- סורק תעבורת רשת

החרגות

החרגות מאפשרות לך להחריג אובייקטים ממנגנון האיתור. כדי לוודא שכל האובייקטים ייסרקו, מומלץ ליצור החרגות רק כשהדבר הכרחי. מצבים שבהם ייתכן שתצטרך להחריג אובייקט עשויים לכלול סריקת ערכים במסד נתונים גדול, שבמהלכה פעילות המחשב מואטת, או תוכנה המתנגשת עם הסריקה.

החרגות לביצועים ▯ בחר באפשרות זו כדי להחריג קבצים ותיקיות מסריקה. החרגות לביצועים מועילות להחרגת סריקה ברמת הקובץ של אפליקציות גיימינג, כאשר המערכת פועלת באופן חריג או לשיפור הביצועים.

החרגות לאיתור מאפשרות לך להחריג אובייקטים מתהליך האיתור באמצעות שם האיתור, הנתיב או קוד ה-Hash שלו. החרגות לאיתור אינן מחריגות קבצים ותיקיות מהסריקה כמו החרגות לביצועים. החרגות לאיתור מחריגות אובייקטים רק כשהם מאותרים על-ידי מנגנון האיתור וכלל מתאים קיים ברשימת ההחרגות.

אל תתבלבל עם סוגים אחרים של החרגות:

- החרגות לתהליכים ▯ כל פעולות הקבצים המיוחסות לתהליכי אפליקציות שהוחרגו אינן נכללות בסריקה (ייתכן שיהיה צורך לשפר את מהירות הגיבוי וזמינות השירות).
- החרגות לסיומות קבצים
- אי הכללות HIPS
- מסנן החרגה עבור הגנה מבוססת ענן

החרגות לביצועים

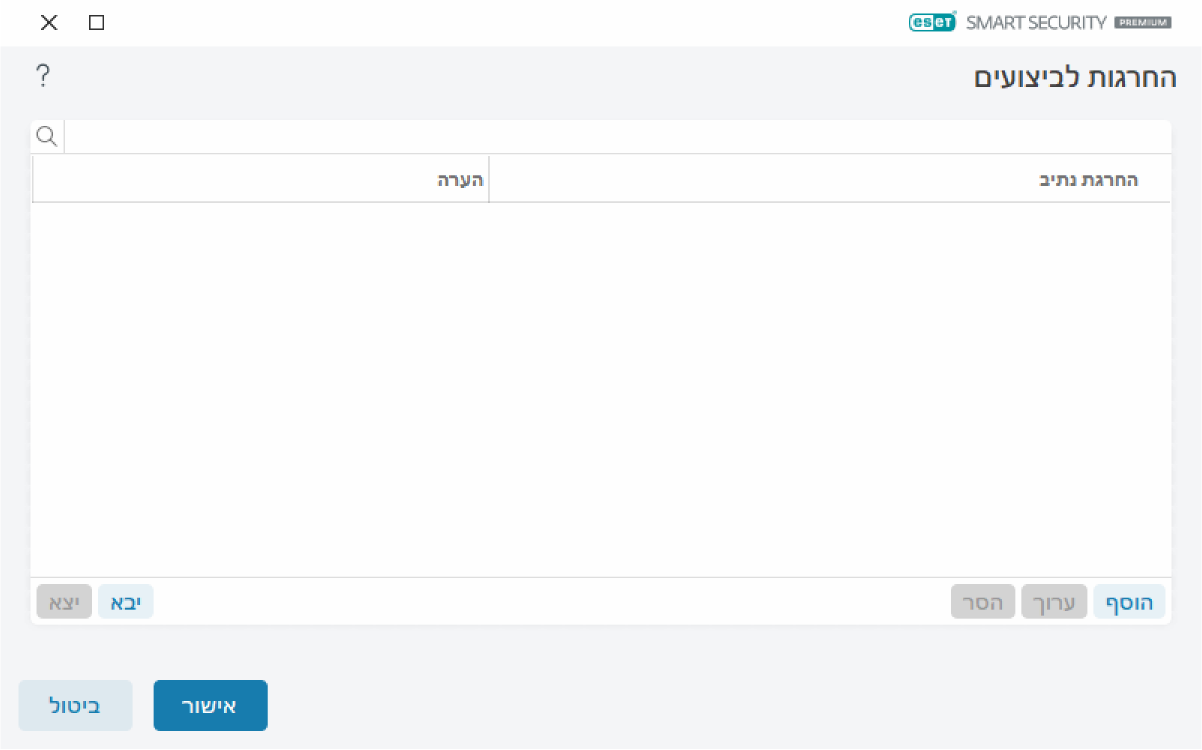
החרגות לביצועים מאפשרות לך להחריג קבצים ותיקיות מסריקה.

כדי לוודא שכל האובייקטים ייסרקו לבדיקת איומים, מומלץ להגדיר אי הכללות רק כשהדבר הכרחי. עם זאת, ישנם מצבים שבהם תצטרך לא לכלול 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 אי ההכללות דרך הגדרות מתקדמות > **מנגנון איתור** > **אי הכללות** > **אי הכללות לביצועים** > **ערוך**.

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

כדי לא לכלול אובייקט (נתיב: קובץ או תיקייה) בסריקה, לחץ על **הוסף** והזן את הנתיב הרלוונטי או בחר אותו במבנה העץ.



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

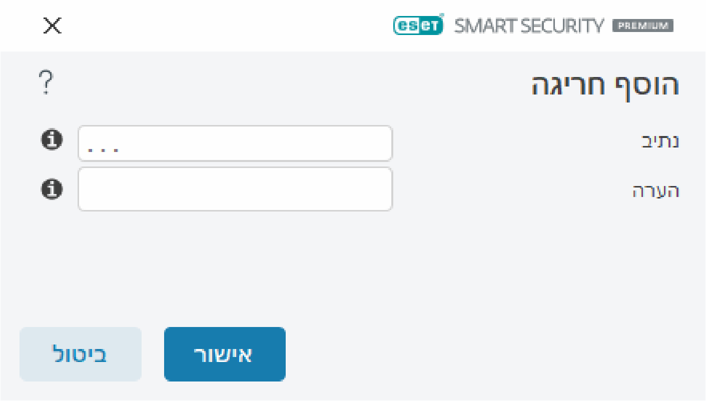
- **הוסף** – החרגת אובייקטים מהזיהוי.
- **ערוך** – אפשרות לעריכת ערכים שנבחרו.
- **מחק** – הסרת ערכים שנבחרו (CTRL + לחץ כדי לבחור ערכים מרובים).

הוספה או עריכה של אי הכללה של ביצועים

חלון תיבת דו-שיח זו לא כולל נתיב ספציפי (קובץ או ספרייה) עבור מחשב זה.

בחר נתיב או הזן ידנית

כדי לבחור נתיב מתאים, לחץ על **...** בשדה **נתיב**.
בעת הקלדה ידנית, ראה עוד דוגמאות לתבניות החרגה בהמשך.



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 ותיקיות המשנה בתיקייה, הקלד את הנתיב לתיקייה והשתמש במסיכה *
- 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 שאלה מחליפים את התווים החסרים/לא ידועים)
דוגמאות:

- *C:\Tools** - הנתיב חייב להסתיים בקו נטוי הפוך (\) ובכוכבית (*) כדי לציין שמדובר בתיקייה ושכל תוכן התיקייה (קבצים ותיקיות משנה) לא ייכלל.
- *C:\Tools*.** - אותה התנהגות כמו *C:\Tools**
- *C:\Tools* • התיקייה *Tools* לא תוחרג. מנקודת המבט של הסורק, *Tools* יכול להיות גם שם קובץ.
- *C:\Tools*.dat* אפשרות זו תחריג קובצי dat. בתיקיה *Tools.*
- *C:\Tools\sg.dat* • אי הכללת קובץ ספציפי זה הממוקם בנתיב המדויק

משתני מערכת באי הכללות

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

- כדי להחריג את התיקיה Program Files באמצעות משתנה מערכת זה, השתמש בנתיב *%PROGRAMFILES%** (זכור להוסיף קו נטוי הפוך וכוכבית בסוף הנתיב) בעת הוספה להחרגות.
- כדי להחריג את כל הקבצים והתיקיות בספריית המשנה *%PROGRAMFILES%*, השתמש בנתיב *%PROGRAMFILES%\Excluded_Directory%**

הרחב את רשימת משתני המערכת הנתמכים

ניתן להשתמש במשתנים הבאים בתבנית אי ההכללה של הנתיב:

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

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

תווים כלליים באמצע נתיב אינם נתמכים

שימוש בתווים כלליים באמצע נתיב (לדוגמה *C:\Tools*\Data\file.dat*) עשוי לפעול אך אינו נתמך באופן רשמי עבור החרגות לביצועים.

אין הגבלות על שימוש בתווים כלליים באמצע נתיב בעת שימוש בהחרגות לזיהויים.

סדר אי ההכללות

- אין אפשרויות להתאמת רמת העדיפות של אי הכללות באמצעות לחצני עליון/תחתון (לגבי כללים של חומת אש כאשר הכללים מופעלים 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.

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 ותיקיות המשנה בתיקייה, הקלד את הנתיב לתיקייה והשתמש במסיכה *
- 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 שאלה מחליפים את התווים החסרים/לא ידועים)

דוגמאות:

- *C:\Tools** - הנתיב חייב להסתיים בקו נטוי הפוך (\) ובכוכבית (*) כדי לציין שמדובר בתיקייה ושכל תוכן התיקייה (קבצים ותיקיות משנה) לא ייכלל.
- *C:\Tools*.** - אותה התנהגות כמו *C:\Tools**
- *C:\Tools* ⮕ התיקייה *Tools* לא תוחרג. מנקודת המבט של הסורק, *Tools* יכול להיות גם שם קובץ.
- *C:\Tools*.dat* ⮕ אפשרות זו תחריג קובצי dat. בתיקיה *Tools.*
- *C:\Tools\sg.dat* ⮕ אי הכללת קובץ ספציפי זה הממוקם בנתיב המדויק

משתני מערכת באי הכללות

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

- כדי להחריג את התיקיה Program Files באמצעות משתנה מערכת זה, השתמש בנתיב *%PROGRAMFILES%** (זכור להוסיף קו נטוי הפוך וכוכבית בסוף הנתיב בעת הוספה להחרגות.
- כדי להחריג את כל הקבצים והתיקיות בספריית המשנה *%PROGRAMFILES%*, השתמש בנתיב *%PROGRAMFILES%\Excluded_Directory**

הרחב את רשימת משתני המערכת הנתמכים

ניתן להשתמש במשתנים הבאים בתבנית אי ההכללה של הנתיב:

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

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

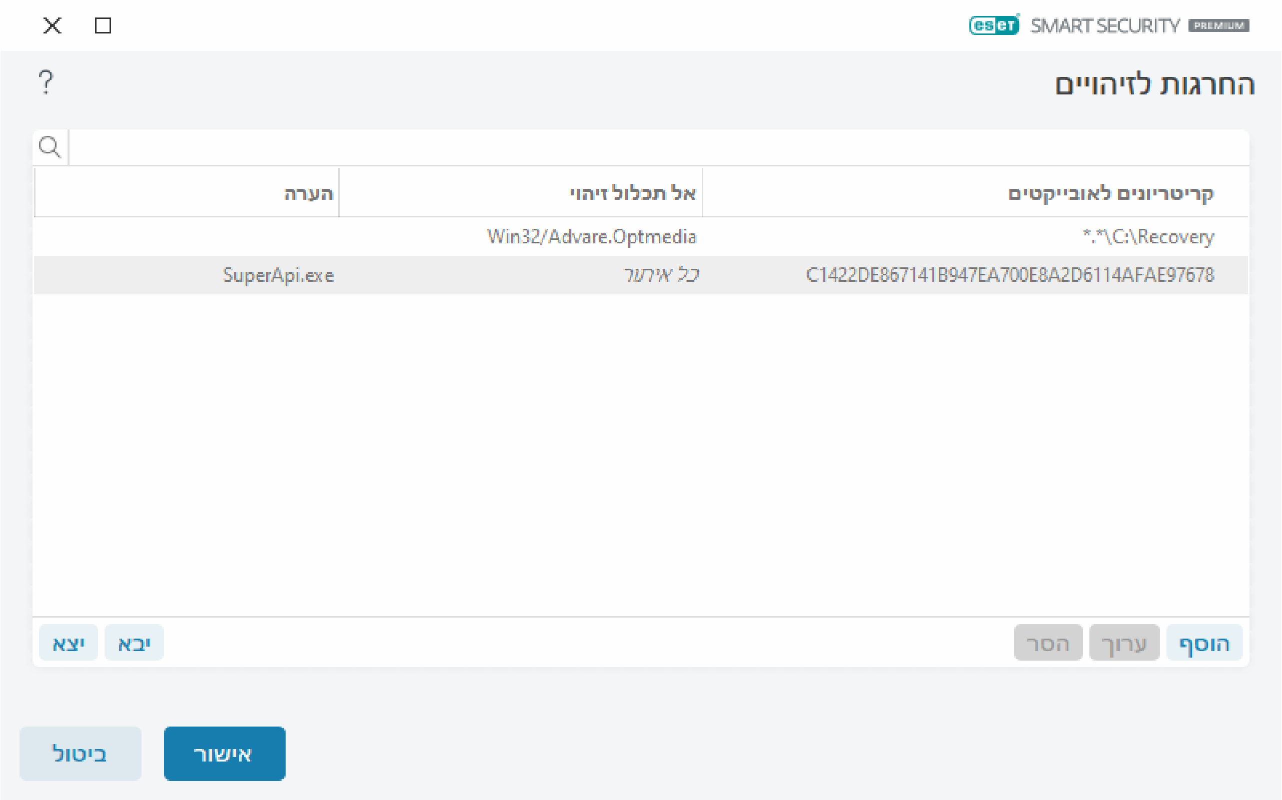
החרגות לזיהויים

החרגות לזיהויים מאפשרות לך להחריג אובייקטים מאיתור על-ידי סינון שם האיתור, הנתיב לאובייקט או קוד ה-Hash שלו.

אופן הפעולה של החרגות לזיהויים

החרגות לזיהויים אינן מחריגות קבצים ותיקיות מהסריקה כמו [החרגות לביצועים](). החרגות לאיתור מחריגות אובייקטים רק כשהם מאותרים על-ידי מנגנון האיתור וכלל מתאים קיים ברשימת ההחרגות.

לדוגמה (ראה את השורה הראשונה בתמונה בהמשך) כאשר אובייקט מזוהה כ-Win32/Adware.Optmedia והקובץ המזוהה הוא *C:\Recovery\file.exe*. בשורה השנייה, כל קובץ עם קוד ה-Hash המתאים SHA-1 תמיד יוחרג ללא קשר לשם האיתור.



כדי להבטיח שכל האיומים יזוהו, אנו ממליצים ליצור החרגות לזיהויים רק כאשר הדבר הכרחי לחלוטין.

כדי להוסיף קבצים ותיקיות לרשימת אי ההכללות, [הגדרות מתקדמות]() < **מנגנון איתור** < **אי הכללות** < **אי הכללות באיתור** < **ערוך**.

אל תתבלבל עם [אי הכללות של ביצועים](), [סיומות קובץ שלא ייכללו](), [אי הכללות HIPS]() או [אי הכללת תהליכים]().

כדי [להחריג אובייקט (לפי שם האיתור או קוד ה-Hash)]() ממנגנון האיתור, לחץ על **הוסף**.

עבור [אפליקציות העלולות להיות לא רצויות]() ו[אפליקציות העלולות להיות לא בטוחות](), אפשר גם ליצור החרגה לפי שם האיתור:

- בחלון ההתראה המדווח על האיתור (לחץ על **הצג אפשרויות מתקדמות** ולאחר מכן בחר באפשרות **אל תכלול באיתור**).
- מתפריט ההקשר של רשומות היומן, באמצעות [אשף יצירת ההחרגות לאיתור]().

- על ידי לחיצה על **כלים** < **הסגר** ואז לחיצה עם לחצן העכבר הימני על הקובץ שהועבר להסגר ובחירה באפשרות **שחזר ואל תכלול בסריקה** בתפריט ההקשר.

קריטריונים לאובייקטים של החרגות לזיהויים

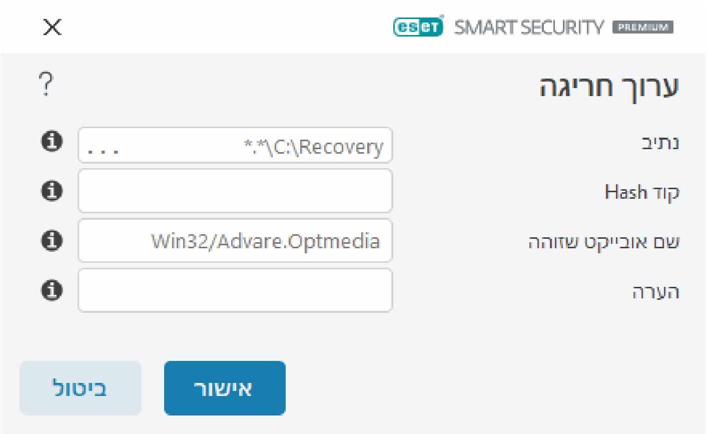
- **נתיב** הגבלת החרגה לזיהוי לנתיב ספציפי (או לנתיב כלשהו).
- **שם האיתור** - אם ישנו שם של איתור ליד קובץ שלא נכלל, פירוש הדבר שהקובץ לא ייכלל רק באיתור הנתון, ולא באופן מוחלט. אם קובץ זה יהיה נגוע בתוכנה זדונית אחרת בשלב מאוחר יותר, הוא יאותר.
- **קוד Hash** לא כולל קובץ על בסיס קוד Hash שצוין (SHA-1), ללא קשר לסוג הקובץ, המיקום, השם או הסיומת שלו.

הוספה או עריכה של אי הכללה באיתור

אל תכלול זיהוי

יש לספק שם איתור חוקי של ESET. להצגת שם איתור 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 Smart Security Premium. 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.

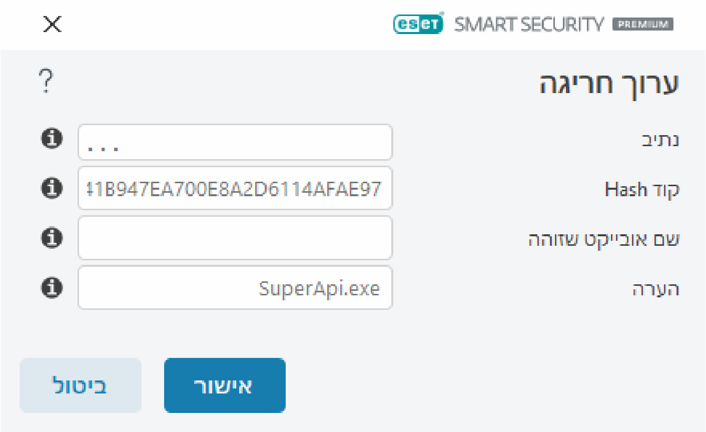
ראה גם תבנית אי הכללה של נתיב.



ראה דוגמה להחרגות לזיהויים בהמשך.

אי-הכללת קוד Hash

לא כולל קובץ על בסיס קוד Hash שצוין (SHA-1), ללא קשר לסוג הקובץ, המיקום, השם או הסיומת שלו.



אי הכללות לפי שם איתור

כדי לא לכלול איתור לפי שם, הזן את שם האיתור החוקי:

Win32/Adware.Optmedia

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

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt

@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan

@NAME=Win32/Bagle.D@TYPE=worm

רכיבי בקרה

- **הוסף** החרגת אובייקטים מהזיהוי.
- **ערוך** אפשרות לעריכת ערכים שנבחרו.
- **מחק** הסרת ערכים שנבחרו (CTRL + לחץ כדי לבחור ערכים מרובים).

אשף יצירת ההחרגות לאיתור

אפשר ליצור החרגה לאיתור גם מתפריט ההקשר של רשומות יומן (לא זמין עבור איתורי תוכנה זדונית):

1. בחלון התוכנית הראשי, לחץ על **כלים** > **רשומות יומן**.
2. לחץ באמצעות לחצן העכבר הימני על איתור ב**יומן האיתורים**.
3. לחץ על **צור החרגה**.

כדי להחריג איתור אחד או יותר על סמך **הקריטריונים להחרגה**, לחץ על **שנה קריטריונים**:

- **קבצים מדויקים** החרג כל קובץ לפי קוד Hash SHA-1 שלו.
- **איתור** החרג כל קובץ לפי שם האיתור שלו.
- **איתור + נתיב** החרג כל קובץ לפי שם האיתור והנתיב שלו, כולל שם הקובץ (לדוגמה, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

האפשרות המומלצת נבחרת מראש על סמך סוג האיתור.

באופן אופציונלי, אפשר להוסיף **הערה** לפני הלחיצה על **צור החרגה**.

אפשרויות מתקדמות של מנגנון האיתור

אפשר סריקה מתקדמת באמצעות AMSI ⍰ הכלי AMSI הוא ממשק הסריקה של Microsoft למניעת תוכנות זדוניות המאפשר לסרוק קובצי Script של PowerShell, קובצי Script המופעלים באמצעות Windows Script Host ונתונים הנסרקים באמצעות SDK של AMSI .

סורק תעבורת רשת

סורק תעבורת הרשת מספק הגנה מפני תוכנות זדוניות לפרוטוקולים של אפליקציות, שמשלבת מספר טכניקות סריקה מתקדמות של תוכנות זדוניות. סורק תעבורת הרשת סורק את הפרוטוקולים POP3 (S), (HTTP (S ו- (IMAP(S באופן אוטומטי, ללא קשר לדפדפן האינטרנט או ללקוח הדואר האלקטרוני. באפשרותך להפעיל/להשבית את סורק תעבורת הרשת דרך הגדרות מתקדמות > **מנגנון איתור** > **סורק תעבורת רשת**.

הפעל סורק תעבורת רשת - אם תשבית את האפשרות הזו, הפרוטוקולים POP3 (S), (HTTP (S ו- (IMAP(S לא ייסרקו. שים לב שהתכונות הבאות של ESET Smart Security Premium דורשות הפעלה של סורק תעבורת רשת:

- הגנת גישה לאינטרנט
- בקרת הורים
- פרטיות ואבטחה בדפדפן
- גלישה ושירותים בנקאיים בטוחים
- SSL/TLS
- הגנת אנטי-פישינג
- הגנת לקוח דוא"ל

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.

ESET LiveGuard היא תכונה המוסיפה שכבת הגנה שתוכננה במיוחד לצמצום איומים שטרם נראו בעבר. כאשר אפשרות זו מופעלת, דגימות חשודות שטרם אושרו כדגימות זדוניות והעלולות להכיל תוכנות זדוניות נשלחות באופן אוטומטי לענן של ESET.

האפשרויות הבאות זמינות:

אפשר את מערכת המוניטין של ESET LiveGrid®, מערכת המשוב של ESET LiveGrid® ו-ESET LiveGuard

מערכת המוניטין של ESET LiveGrid® מספקת רישום בענן ברשימות לבנות וברשימות שחורות. מערכת המשוב של ESET LiveGrid® תאסוף מידע על המחשב שלך הקשור לאיומים חדשים שאותרו. התכונה ESET LiveGuard מאתרת איומים חדשים שלא נראו מעולם על ידי ניתוח אופן הפעולה שלהם בארגז חול.

משתמש יכול לבדוק את המוניטין של [תהליכים פועלים] וקבצים ישירות מהממשק או מהתפריט ההקשרי של התוכנית, עם מידע נוסף הזמין מ-ESET LiveGrid®. ההגנה הפרואקטיבית של ESET LiveGuard מונעת את ההפעלה של קבצים חדשים עד לקבלת תוצאת הניתוח.

אפשר את מערכת המוניטין של ESET LiveGrid®

מערכת המוניטין של ESET LiveGrid® מספקת רישום בענן ברשימות לבנות וברשימות שחורות.

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

אפשר את מערכת המשוב של ESET LiveGrid®

בנוסף למערכת המוניטין של ESET LiveGrid®, מערכת המשוב של ESET LiveGrid® תאסוף מידע על האיומים החדשים שזוהו אשר קשורים למחשב שלך. מידע זה עשוי לכלול:

- דגימה או עותק של קובץ שבו האיום הופיע
- הנתיב לקובץ
- שם הקובץ
- תאריך ושעה
- התהליך שבו האיום הופיע במחשב שלך
- מידע על מערכת ההפעלה של המחשב שלך

כברירת מחדל, ESET Smart Security Premium 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.

> קרא עוד על שליחת נתונים רלוונטיים ב[מדיניות הפרטיות].

באפשרותך לבחור שלא לאפשר את ESET LiveGrid®

לא תאבד שום פונקציונליות של התוכנה, אולם במקרים מסוימים ESET Smart Security Premium עשוי להגיב לאיומים חדשים מהר יותר כאשר ESET LiveGrid® מופעל. אם השתמשת בעבר ב-ESET LiveGrid® והשבתת אותו, ייתכן שיהיו קיימות עדיין חבילות נתונים לשליחה. גם לאחר ביטול ההפעלה חבילות כאלה יישלחו אל ESET. לא ייווצרו חבילות נוספות לאחר שליחת כל המידע הנוכחי.

> קרא עוד על ESET LiveGrid® ב[מילון].
> ראה את [ההנחיות המאוירות] שלנו הזמינות באנגלית ובמספר שפות אחרות להפעלה או להשבתה של ESET LiveGrid® ב-ESET Smart Security Premium.

תצורה של הגנה מבוססת ענן ב'הגדרות מתקדמות'

כדי לגשת להגדרות של ESET LiveGrid® ושל ESET LiveGuard, פתח את [הגדרות מתקדמות] > **מנגנון איתור** > **הגנה מבוססת ענן**.

- **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.
- **הפעל את מערכת המשוב של ®ESET LiveGrid** – שליחת נתוני השליחה הרלוונטיים (המתוארים בסעיף **שליחת דוגמאות** להלן) יחד עם דיווחי קריסה וסטטיסטיקות למעבדת המחקר של ESET לצורך ניתוח נוסף.
- **הפעל את ESET LiveGuard** – התכונה ESET LiveGuard מזהה איומים חדשים שלא נראו מעולם על-ידי ניתוח אופן הפעולה שלהם בארגז חול. ניתן להפעיל את ESET LiveGuard רק אם ®ESET LiveGrid מופעל.
- **שלח דוחות קריסה ונתוני אבחון** – שלח נתוני אבחון הקשורים ל-®ESET LiveGrid, כגון דוחות קריסה ומצבורי זיכרון של מודולים. מומלץ להשאיר אפשרות זו מאופשרת כדי לעזור ל-ESET באבחון בעיות, בשיפור המוצרים ובהבטחת הגנה טובה יותר על משתמש הקצה.
- **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 ידנית של דגימות – הפעלת האפשרות לשלוח דגימות ל-ESET באופן ידני מתוך התפריט תלוי ההקשר, הסגר או כלים.

שליחה אוטומטית של הדגימות שאותרו

בחר איזה סוג של דגימות יוגש ל-ESET למטרות ניתוח ושיפור ביצועי האיתור העתידיים (גודל הדגימה המקסימלי המהווה ברירת מחדל הוא 64MB). האפשרויות הבאות זמינות:

- **כל הדגימות שאותרו** – כל האובייקטים שאותרו על-ידי מנגנון האיתור (לרבות אפליקציות העלולות להיות לא רצויות כאשר אפשרות זו מאופשרת בהגדרות הסורק).
- **כל הדוגמאות למעט מסמכים** – כל האובייקטים שאותרו למעט **מסמכים** (ראה להלן).
- **אל תשלח** – אובייקטים שאותרו לא יישלחו ל-ESET.

שליחה אוטומטית של דוגמאות של פריטים חשודים

דגימות אלה יישלחו ל-ESET גם אם מנגנון האיתור לא מאתר אותן. לדוגמה, דגימות שכמעט הוחמצו באיתור או שאחד ממודולי ההגנה של ESET Smart Security Premium מחשיב דגימות אלה כחשודות או כפועלות באופן לא ברור (גודל הדגימה המקסימלי המהווה ברירת מחדל הוא 64MB).

- **קובצי הפעלה** – כולל קובצי הפעלה כגון: .exe, .dll, .sys.
- **קובצי ארכיון** – כולל סוגי קובצי ארכיון כגון: .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **קובצי Script** – כולל סוגי קובצי Script 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.
- **מחק קובצי הפעלה, קובצי ארכיון, קובצי Script, דגימות אחרות ודוא"ל החשוד כדואר זבל מהשרתים של ESET**

אפשרות זו מגדירה מתי למחוק דגימות שנשלחו לניתוח באמצעות ESET LiveGuard.

- **מסמכים** כולל מסמכי Microsoft Office או PDF עם תוכן פעיל או ללא תוכן פעיל.
- **מחק מסמכים מהשרתים של ESET** אפשרות זו מגדירה מתי למחוק מסמכים שנשלחו לניתוח באמצעות ESET LiveGuard.

הרחב לקבלת רשימה של כל סוגי קובצי המסמכים הכלולים

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

החרגות

מסנן ההחרגות 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.

כדי לא לכלול קבצים שהורדו מ-`download.domain.com`, נווט אל הגדרות מתקדמות > **מנגנון איתור** > **הגנה מבוססת ענן** > **שליחת דגימות** ולחץ על **ערוך** לצד **החרגות**. הוסף את ההחרגה `.download.domain.com`.

גודל מקסימלי של דגימות (MB) מגדיר את הגודל המקסימלי של דגימות שנשלחו אוטומטית (1-64 MB).

ESET LiveGuard

מסנן החרגה עבור הגנה מבוססת ענן

מסנן ההחרגה מאפשר לך להחריג קבצים או תיקיות מסוימים בשליחת דגימות. הקבצים המפורטים בו לעולם לא יישלחו לניתוח במעבדת ESET, גם אם הם מכילים קוד חשוד. סוגי קבצים נפוצים (כמו .doc וכדומה) מוחרגים כברירת מחדל.

תכונה זו מועילה כדי להחריג קבצים שעשויים לכלול מידע חסוי, כגון מסמכים או גיליונות אלקטרוניים.

כדי לא לכלול קבצים שהורדו מ-download.domain.com, לחץ על הגדרות מתקדמות > **מנגנון איתור** > **הגנה מבוססת ענן** > **שליחת דגימות** > **החרגות**, והוסף את ההחרגה **download.domain.com.

ESET LiveGuard

ESET LiveGuard היא תכונה המוסיפה שכבה של הגנה מבוססת ענן שתוכננה במיוחד לצמצום איומים שטרם נראו בעבר.

כאשר אפשרות זו מופעלת, דגימות חשודות שטרם אושרו כדגימות זדוניות והעלולות להכיל תוכנות זדוניות נשלחות באופן אוטומטי לענן של ESET. הדגימות שנשלחו מופעלות בארגז חול והמנגנונים המתקדמים שלנו לזיהוי תוכנות זדוניות מבצעים הערכה שלהן. דגימות זדוניות או הודעות דואר זבל חשודות נשלחות אל ESET LiveGrid®. קבצים מצורפים לדוא"ל מטופלים בנפרד והם מחייבים שליחה אל ESET LiveGuard. באפשרותך להגדיר את היקף הקבצים שיישלחו ואת תקופת השמירה של הקבצים בענן של ESET. מסמכים וקובצי PDF עם תוכן פעיל (פקודות מאקרו,

JavaScript) אינם נשלחים כברירת מחדל.

ניתן להפעיל או להשבית את ESET LiveGuard ב:

- חלון התוכנית הראשי > **הגדרות** > **הגנה על מחשב**
- הגדרות מתקדמות > **מנגנון איתור** > **הגנה מבוססת ענן**

כדי לגשת להגדרות המתקדמות של ESET LiveGuard, פתח את הגדרות מתקדמות > **מנגנון איתור** > **הגנה מבוססת ענן** > **ESET LiveGuard**.

פעולה לאחר איתור הגדרת הפעולה שיש לנקוט אם הדגימה המנותחת מוערכת כאיום.

הגנה פרואקטיבית מאפשרת או חוסמת את הפעלת הקבצים המנותחים באמצעות ESET LiveGuard. אם קובץ הוא קובץ חשוד, ההגנה הפרואקטיבית תחסום את הפעלתו עד לסיום הניתוח. הגנה פרואקטיבית מזהה קבצים מהמקורות הבאים:

- קבצים שהורדו באמצעות דפדפן אינטרנט נתמך
- הורד מלקוח דואר
- קבצים שחולצו מארכיון לא מוצפן או מוצפן באמצעות אחד מכלי השירות הנתמכים של קובצי ארכיון
- קבצים הממוקמים בהתקן נשלף שהופעלו ונפתחו

עיין באפליקציות הנתמכות בטבלה שלהלן:

התקנים נשלפים	כלי שירות לקובצי ארכיון	לקוחות דואר	דפדפני אינטרנט
כונן הבזק מסוג USB	WinRAR	Microsoft Outlook	Internet Explorer
כונן קשיח מסוג USB	WinZIP	Mozilla Thunderbird	Microsoft Edge
תקליטור/dvd	מחלץ קובצי ארכיון מובנה של Microsoft Explorer	Microsoft Mail	Chrome
תקליטון	7zip		Firefox
קורא כרטיסים מובנה			Opera
			דפדפן Brave

> **הערה**
> קבצים שהועתקו באמצעות סייר Windows ממיקום שלא נכלל למיקום מוגן ייחסמו על-ידי ההגנה הפרואקטיבית מכיוון ש-ESET Smart Security Premium זיהה את `explorer.exe` ככלי שירות לקובצי ארכיון.

> אם ההגנה הפרואקטיבית מוגדרת לאפשרות **חסום את ההפעלה עד לקבלת תוצאת הניתוח** וברצונך לבטל את החסימה של הקובץ המנותח, לחץ באמצעות לחצן העכבר הימני על הקובץ ולחץ על **בטל את חסימת הקובץ המנותח באמצעות ESET LiveGuard**.

זמן המתנה מקסימלי לתוצאת הניתוח (בדקות) הגדרת פרק הזמן שלאחריו חסימת הקבצים המנותחים תבוטל גם אם ניתוחם טרם הסתיים.

ESET LiveGuard יידע אותך לגבי סטטוס הניתוח באמצעות התראות. להלן ההתראות הזמינות:

תיאור	כותרת ההתראה
ESET LiveGuard חסם את הקובץ. ESET LiveGuard מנתח את הקובץ כדי להבטיח שהוא בטוח לשימוש. באפשרותך להמתין או לבחור באחת מהאפשרויות להלן: • **בטל את חסימת הקובץ** ⍰ חסימת הקובץ מבוטלת, אך הניתוח נמשך. ויידע אותך לגבי התוצאה. פעולה זו אינה מומלצת אם אינך בטוח לגבי מהימנות הקובץ. • **שנה הגדרות** ⍰ פתיחת חלון ההגדרות של הגנה על מחשב, שבו באפשרותך להשבית את ESET LiveGuard וההגנה הפרואקטיבית שלו.	הקובץ נחסם בעקבות ניתוח
הקובץ אינו חסום עוד. הניתוח נמשך, ויידע אותך לגבי התוצאה. באפשרותך לפתוח את הקובץ.	חסימת הקובץ בוטלה
ESET LiveGuard זקוק לזמן נוסף כדי לסיים את הניתוח. באפשרותך לפתוח את הקובץ במידת הצורך.	הקובץ עדיין בניתוח
ESET LiveGuard סיים את הניתוח והקובץ הכיל איום. הקובץ נוקה.	הוסר איום
ESET LiveGuard סיים את הניתוח והקובץ בטוח לשימוש.	הקובץ בטוח לשימוש

אם ESET LiveGuard אינו פועל כראוי, תוצג התראה בחלון התוכנית הראשי > **מבט כולל**. בצע את ההוראות המפורטות בהתראה כדי לפתור את הבעיה. אם אינך מצליח לפתור את הבעיה, פנה לתמיכה הטכנית.

סריקת תוכנות זדוניות

המקטע **סריקת תוכנות זדוניות** נגיש דרך הגדרות מתקדמות > **מנגנון איתור** > **סריקת תוכנות זדוניות** ומאפשר להגדיר פרמטרים של פרופילי סריקה.

סריקה לפי דרישה

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

לאחר בחירת פרופיל הסריקה ניתן להגדיר את האפשרויות הבאות:

יעדי סריקה - אם ברצונך לסרוק יעד מסוים או קבוצת יעדים, לחץ על **ערוך** לצד **יעדי סריקה** ובחר אפשרות ממבנה התיקיות (עץ). ראה פרטים נוספים בנושא יעדי סריקה.

הגנה לפי דרישה והגנה של למידת מכונה - באפשרותך להגדיר רמות דיווח והגנה עבור כל פרופיל סריקה. כברירת מחדל, פרופילי סריקה משתמשים באותה הגדרה שנקבעה בהגנה בזמן אמת על מערכת קבצים. השבת את המתג שליד **השתמש בהגדרות הגנה בזמן אמת** כדי לקבוע תצורה של רמות דיווח והגנה מותאמות אישית. עיין בסעיף הגנות לקבלת הסבר מפורט על רמות הדיווח וההגנה.

ThreatSense - אפשרויות של הגדרות מתקדמות, כגון סיומות קבצים שברצונך לשלוט בהן ושיטות איתור שבהן נעשה שימוש. ראה פרטים נוספים בנושא ThreatSense.

פרופילי סריקה

ישנם 4 פרופילי סריקה מוגדרים מראש ב-ESET Smart Security Premium:

• **סריקה חכמה** - זהו פרופיל הסריקה המתקדם המוגדר כברירת מחדל. הפרופיל 'סריקה חכמה' משתמש

בטכנולוגיה 'אופטימיזציה חכמה', שמחריגה קבצים שסריקה קודמת מצאה שהם נקיים ושלא השתנו מאז סריקה זו. הדבר מאפשר זמני סריקה קצרים יותר עם השפעה מינימלית על אבטחת המערכת.

- **סריקת תפריט הקשר** - אתה יכול להתחיל בסריקה לפי דרישה של כל קובץ מתפריט ההקשר. הפרופיל 'סריקת תפריט הקשר' מאפשר לך להגדיר תצורת סריקה שתהיה בשימוש כשתפעיל את הסריקה באופן זה.
- **סריקה מעמיקה** - הפרופיל 'סריקה מעמיקה' לא משתמש ב'אופטימיזציה חכמה' כברירת מחדל, ולכן אף קובץ לא מוחרג מהסריקה בעת שימוש בפרופיל זה.
- **סריקת מחשב** זהו פרופיל ברירת המחדל המשמש בסריקת מחשב רגילה.

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 הגדרות מתקדמות > **מנגנון איתור** > **סריקת תוכנות זדוניות** > **סריקה לפי דרישה** > **רשימת פרופילים** > **ערוך**. 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, ראה ThreatSense לקבלת תיאור של כל אחד מהפרמטרים של הגדרות הסריקה.

> i 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 **תקן את האיתור תמיד**. 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.
- **בחירה מותאמת אישית** ביטול כל הבחירות הקודמות.

מבנה (עץ) התיקיות מכיל גם יעדי סריקה ספציפיים.

- **זיכרון הפעלה** סריקת כל התהליכים והנתונים הנמצאים כעת בשימוש של זיכרון ההפעלה.
- **סקטורי אתחול/UEFI** סריקת סקטורי האתחול ו-UEFI לאיתור תוכנות זדוניות. קרא מידע נוסף על סורק UEFI במילון.
- **מסד נתוני WMI** סריקה של כלל מסד נתוני Windows Media Instrumentation (WMI), של כל מרחבי השמות, של מופעי המחלקות ושל כל המאפיינים. בנוסף, מתבצע חיפוש של הפניות לקבצים נגועים או של תוכנות זדוניות המוטבעות כנתונים.
- **ערכי רישום של המערכת** סריקה של כלל ערכי הרישום של המערכת, של כל המפתחות ושל כל מפתחות המשנה. בנוסף, מתבצע חיפוש של הפניות לקבצים נגועים או של תוכנות זדוניות המוטבעות כנתונים. בעת ניקוי האיתורים, ההפניות נשארות ברישום כדי לוודא שנתונים חשובים לא יאבדו.

כדי לנווט במהירות ליעד סריקה (קובץ או תיקייה), הקלד את הנתיב בשדה הטקסט שמתחת למבנה העץ. הנתיב הוא תלוי-רישיות. כדי לכלול את היעד בסריקה, בחר בתיבת הסימון שלו במבנה העץ.

סרוק במצב לא פעיל

ניתן לאפשר סורק במצב לא פעיל דרך הגדרות מתקדמות < **מנגנון איתור** < **סריקת תוכנות זדוניות** < **סריקה במצב לא פעיל**.

סרוק במצב לא פעיל

העבר את המתג שלצד **אפשר סריקה במצב לא פעיל** למצב פעיל כדי לאפשר תכונה זו. כאשר המחשב במצב לא פעיל, מתבצעת סריקת מחשב שקטה בכל הכוננים המקומיים.

כברירת מחדל, הסורק במצב לא פעיל לא יופעל כאשר המחשב (הנייד) מופעל בכוח הסוללה. תוכל לעקוף הגדרה זו על-ידי העברת פס המחוון שלצד **הפעל אפילו אם המחשב פועל באמצעות סוללה** בהגדרות המתקדמות למצב פעיל.

העבר את פס המחוון שלצד **אפשר רישום ביומן** בהגדרות המתקדמות למצב פעיל כדי לתעד פלט סריקת מחשב במקטע רשומות יומן (מתוך חלון התוכנית הראשי לחץ על **כלים** < **רשומות יומן** ובחר **סריקת מחשב** מהתפריט 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.

ThreatSense - אפשרויות של הגדרות מתקדמות, כגון סיומות קבצים שברצונך לשלוט בהן ושיטות איתור שבהן נעשה שימוש. מידע נוסף ניתן למצוא ב-ThreatSense.

איתור במצב לא פעיל

ניתן לקבוע את תצורת ההגדרות של איתור במצב לא פעיל בהגדרות 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:

- **מסך או שומר מסך כבויים**
- **נעילת מחשב**
- **יציאת משתמש**

השתמש במתגים עבור כל מצב מתאים כדי להפעיל או להשבית את הגורמים המפעילים השונים לאיתור במצב לא פעיל.

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 **קובץ אתחול אוטומטי** ולאחר מכן על **ערוך**. בשלב האחרון, החלון

בדיקת קובץ אתחול אוטומטית יופיע. לקבלת הוראות מפורטות על יצירה וניהול של משימת מתזמן, ראה יצירת משימות חדשות.

ThreatSense - אפשרויות של הגדרות מתקדמות, כגון סיומות קבצים שברצונך לשלוט בהן ושיטות איתור שבהן נעשה שימוש. מידע נוסף ניתן למצוא ב-ThreatSense.

בדיקת קובץ אתחול אוטומטית

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

התפריט הנפתח **יעד סריקה** מציין את עומק הסריקה של קבצים הפועלים בעת אתחול המערכת, על-בסיס אלגוריתם מתוחכם. 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 קבוצה למעלה. אם תבחר בעומק סריקה נמוך יותר עבור קבצים הפועלים בעת הפעלת המערכת, הקבצים שאינם נסרקים ייסרקו בעת הפתיחה או ההפעלה שלהם.

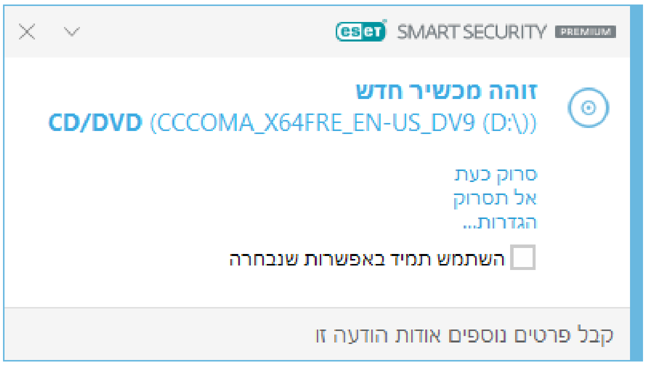
עדיפות סריקה רמת העדיפות שבה תשתמש המערכת כדי לקבוע מתי תופעל סריקה:

- **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.

מדיה נשלפת

ESET Smart Security Premium מספק סריקה אוטומטית של מדיה נשלפת (CD/DVD/USB/...) לאחר הכנסתה למחשב. אפשרות זו שימושית כאשר מנהל המערכת של המחשב מעוניין למנוע מהמשתמשים להשתמש במדיה נשלפת עם תוכן שלא התבקש.

בעת הכנסה של מדיה נשלפת והגדרה של האפשרות **הצג אפשרויות סריקה** דרך הגדרות מתקדמות > **מנגנון איתור** > **סריקת תוכנות זדוניות** > **מדיה נשלפת**, יופיע חלון הדו-שיח הבא:



אפשרויות עבור חלון הדו-שיח:

- **סרוק עכשיו** פעולה זו תפעיל סריקה של המדיה הנשלפת.
- **אל תסרוק** מדיה נשלפת לא תעבור סריקה.
- **הגדרות** פתיחת הגדרות מתקדמות.
- **השתמש תמיד באפשרות שנבחרה** כאשר אפשרות זו נבחרת, אותה פעולה תבוצע בפעם אחרת שבה תוכנס מדיה נשלפת.

בנוסף, ESET Smart Security Premium 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.

כדי לגשת להגדרות של סריקת מדיה נשלפת, פתח את הגדרות מתקדמות > **מנגנון איתור** > **סריקת תוכנות זדוניות** > **מדיה נשלפת**.

הפעולה שיש לנקוט לאחר הכנסת מדיה נשלפת בחר את פעולת ברירת המחדל שתבוצע בעת הכנסה של התקן מדיה נשלפת למחשב (CD/DVD/USB). בחר את הפעולה המבוקשת בעת הכנסת מדיה נשלפת למחשב:

- **אל תסרוק** לא תבוצע אף פעולה והחלון **אותר התקן חדש** לא ייפתח.
- **סריקת התקנים אוטומטית** תבוצע סריקת מחשב של התקן המדיה הנשלפת שהוכנס.
- **הצג אפשרויות סריקה** פתיחת מקטע ההגדרות **מדיה נשלפת**.

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 > **מנגנון איתור** > **סריקות לאיתור תוכנות זדוניות** > **הגנה על מסמכים** ולחץ על פס המחוון שלצד **הפעל הגנה על מסמכים**.

ThreatSense - אפשרויות של הגדרות מתקדמות, כגון סיומים קבצים שברצונך לשלוט בהן ושיטות איתור שבהן נעשה שימוש. מידע נוסף ניתן למצוא ב-ThreatSense.

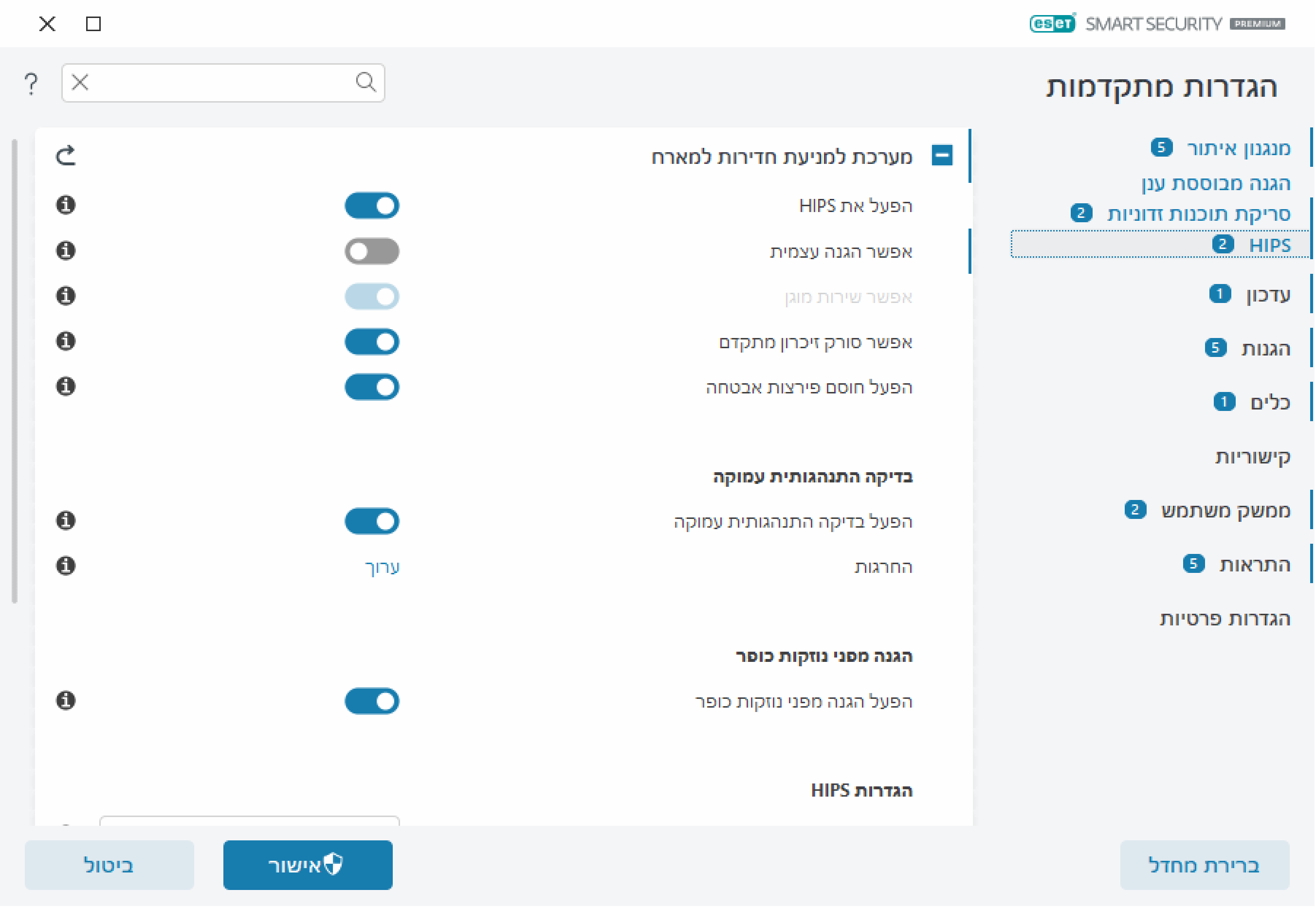
> **i** תכונה זו מופעלת על-ידי יישומים המשתמשים ב-Microsoft Antivirus API (לדוגמה, Microsoft Office 2000 ואילך או Microsoft Internet Explorer 5.0 ואילך).

HIPS - מערכת למניעת חדירות למארח

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.

באפשרותך לקבוע את התצורה של הגדרות HIPS דרך הגדרות מתקדמות > **מנגנון איתור** > **HIPS** > **מערכת למניעת חדירות למארח**. המצב של HIPS (מופעלת/מושבתת) מוצג בחלון התוכנית הראשי של ESET Smart Security Premium > **הגדרות** > **הגנת מחשב**.



מערכת למניעת חדירות למארח

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

אפשר הגנה עצמית – ESET Smart Security Premium 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 הגנה עבור שירות ESET (ekrn.exe). כאשר האפשרות מופעלת, השירות מופעל כתהליך מוגן של Windows להגנה מפני התקפות של תוכנה זדונית.

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 הגנה זה ב[מילון](#).

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 ב[מילון](#).

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 נוזקת כופר תופעל, על מערכת המוניטין ESET LiveGrid® להיות זמינה. [קרא עוד על סוג ההגנה הזה](#).

אפשר את Intel® Threat Detection Technology 󠀠 טכנולוגיה זו מסייעת באיתור התקפות של תוכנות כופר באמצעות מדידת שימוש ייחודית המשולבת במעבדי Intel וכך מגבירה את יעילות האיתור, מפחיתה את ההתראות לגבי תוצאות חיוביות מוטעות ומרחיבה את הנראות כדי לזהות טכניקות התחמקות מתקדמות. עיין ברשימת [המעבדים הנתמכים](#).

הגדרות HIPS

מצב סינון ניתן לביצוע באחד מהמצבים הבאים:

מצב סינון	תיאור
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	חוסם את כל הפעולות שאינן מוגדרות על ידי כלל ספציפי שמאפשר אותן.
מצב למידה	הפעולות מתאפשרות ולאחר כל פעולה נוצר כלל. את הכללים הנוצרים במצב זה ניתן להציג בעורך **כללי HIPS**, אך העדיפות שלהם נמוכה מזו של כללים שנוצרו ידנית או כללים שנוצרו במצב אוטומטי. כשאתה בוחר ב**מצב למידה** מהתפריט הנפתח **מצב סינון**, 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. לאחר סיום מצב הלמידה, האפשרות **שאל את המשתמש** תחייב הרשאות ניהול לצורך ביצוע שינוי במצב הסינון של HIPS.

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 עורך **הכללים של HIPS**. בחלון הכללים של HIPS תוכל לבחור, להוסיף, לערוך או להסיר כללים. פרטים נוספים על יצירת כללים ופעולות HIPS ניתן למצוא ב[עריכת כלל HIPS](#).

אי הכללות HIPS

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

כדי לערוך אי הכללות של HIPS, פתח את הגדרות מתקדמות > **מנגנון איתור** > **HIPS** > **מערכת למניעת חדירות למארח** > **החרגות** > **עריכה**.

אל תתבלבל עם סימות קובץ שלא ייכללו, החרגות לזיהויים, החרגות לביצועים או אי הכללת תהליכים.

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

תעד את כל הפעולות החסומות – כל הפעולות החסומות יירשמו ביומן HIPS. השתמש בתכונה זו רק במהלך פתרון בעיות או כשצוות התמיכה הטכנית של ESET יבקש ממך לעשות זאת, מפני שהיא עלולה ליצור קובץ יומן גדול מאוד ולהאט את פעולת המחשב.

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.

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.

לאחר ההתקנה, רשימת מנהלי ההתקנים ריקה. ESET Smart Security Premium ממלא את הרשימה באופן אוטומטי במשך הזמן.

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).

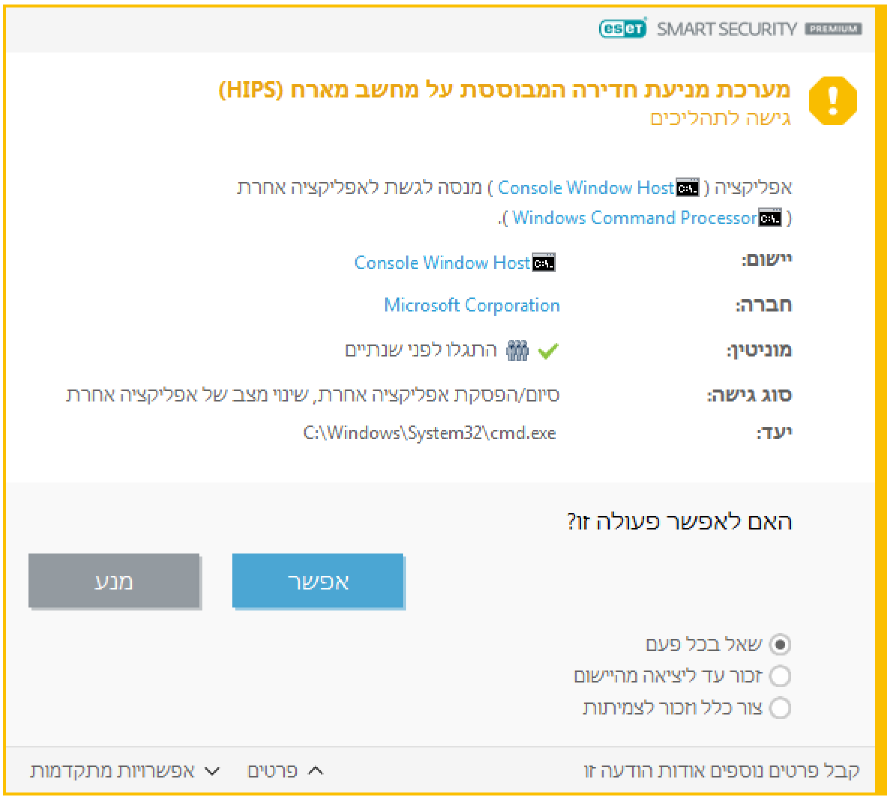
לחץ על **פרטים** בחלק התחתון כדי לראות איזו אפליקציה מפעילה את הפעולה, מה המוניטין של הקובץ או איזה סוג פעולה אתה מתבקש לאפשר או לדחות.

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 שיהיה **אוטומטי** בהגדרות מתקדמות > **מנגנון איתור** > **HIPS** > **מערכת למניעת חדירות למארח**.



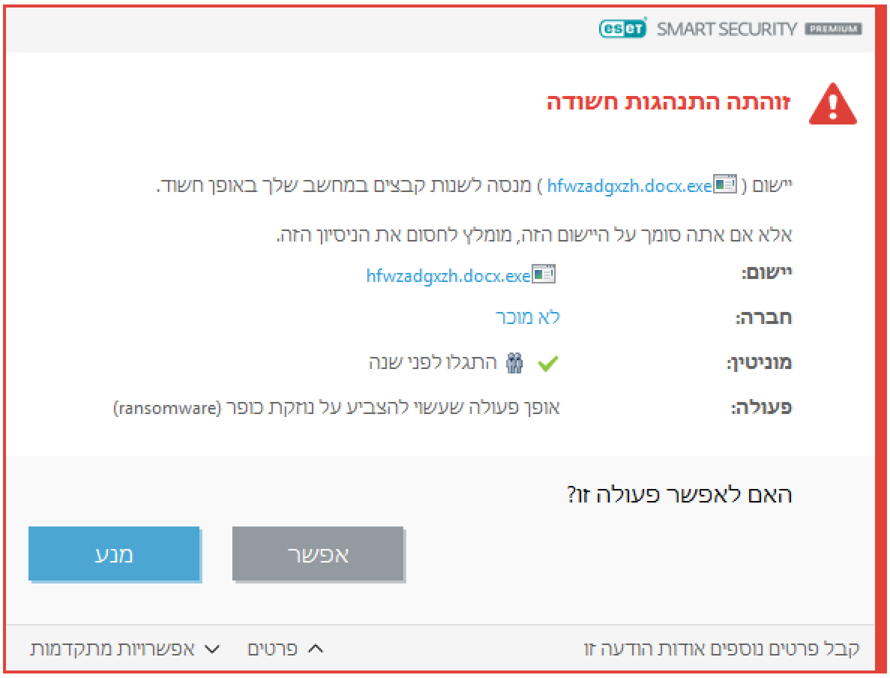
מצב למידה הסתיים

מצב למידה יוצר ושומר כללים באופן אוטומטי. באפשרותך לבדוק את כל הכללים שנוצרו בהגדרות כלל HIPS. הכי טוב להשתמש במצב זה לתצורה הראשונית של HIPS, אבל יש לשמור עליו רק לזמן קצר. אין צורך באינטראקציה עם המשתמש, מפני ש-ESET Smart Security Premium שומר את הכללים בהתאם לפרמטרים שהוגדרו מראש. עבור למצב **אינטראקטיבי** או **מצב מבוסס-מדיניות** לאחר שנוצרו כל הכללים לתהליכים הנדרשים הפועלים במערכת ההפעלה, כדי למנוע סיכוני אבטחה.

אפשר לדחות החלטה זו אם אינך רוצה לשנות את ההגדרות.

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 **לאפשר** את הפעולה.



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

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 – כבה את המתג 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.

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

הודעה – אם מופעל אירוע, חלון התראות 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 (לגבי כללים של חומת אש כאשר הכללים מופעלים 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)

עריכת כלל HIPS

ראה ניהול כלל HIPS תחילה.

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 כבה את המתג הזה אם ברצונך להשאיר את הכלל ברשימה מבלי להחילו.

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

הודעה למשתמש אם מופעל אירוע, חלון התראות 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.

קובצי יעד 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 הקבצים** בתפריט הנפתח ולהוסיף את כל הקבצים.

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.

> 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.

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.

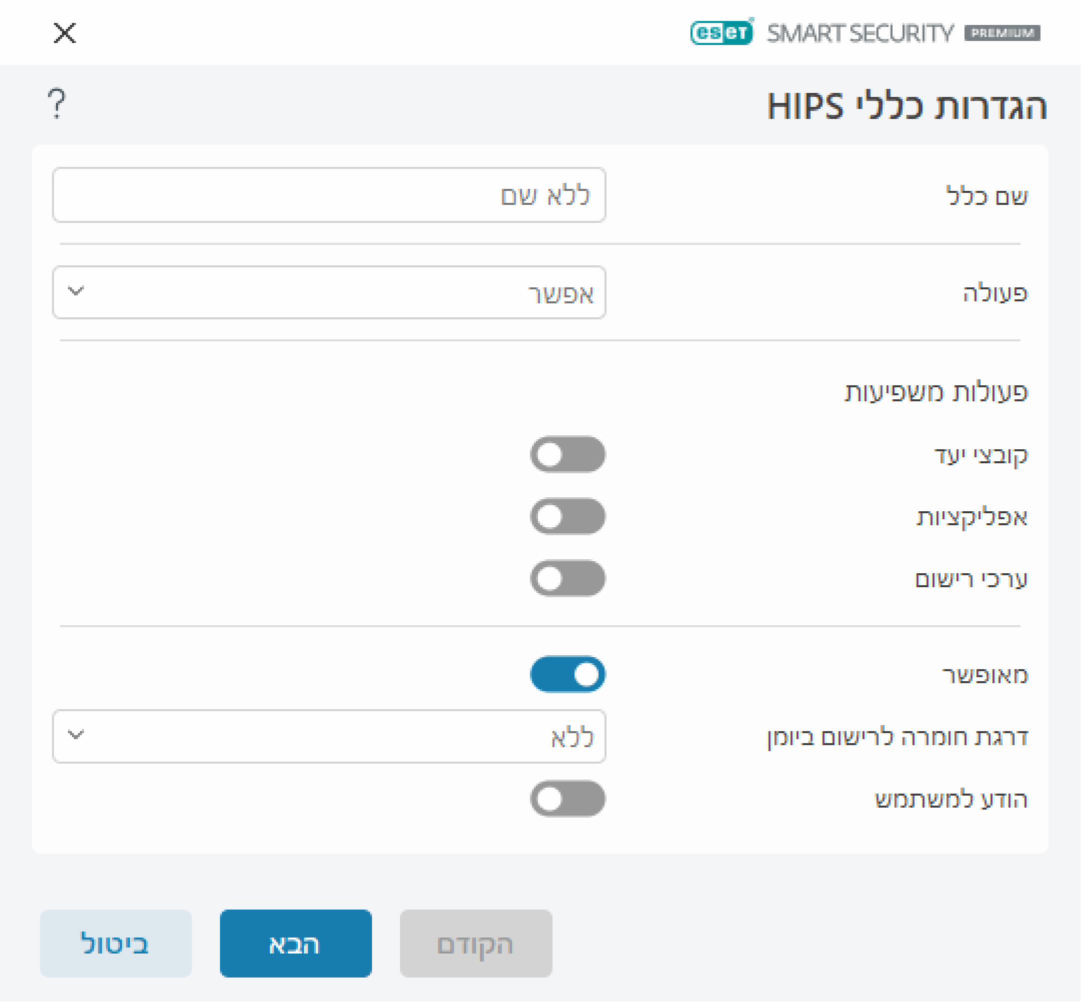
> בעת הזנת יעד, באפשרותך להשתמש בתווים כלליים עם הגבלות מסוימות. במקום מפתח מסוים, ניתן להשתמש בסמל * (כוכבית) בנתיבי יישומים. לדוגמה, המשמעות של *HKEY_USERS*\software* יכולה להיות *HKEY_USER\.default\software* אך לא
> *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software.*
> *HKEY_LOCAL_MACHINE\system\ControlSet** 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 (*).

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 שלצד **הודע למשתמש** למצב פעיל כדי להציג התראה 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 **...** בעת בחירת תיקייה, כל היישומים שנמצאים במיקום זה נכללים.

האפשרות **פתח את עורך הרישום** 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*

עדכון

אפשרויות הגדרת העדכון זמינות דרך הגדרות מתקדמות > **עדכון**. מקטע זה מציין פרטים על מקור העדכון, כגון שרתי העדכון שבהם נעשה שימוש ונתוני האימות של שרתים אלה.

עדכון

פרופיל העדכון שנמצא בשימוש מוצג בתפריט הנפתח **בחר פרופיל עדכון המוגדר כברירת מחדל**.

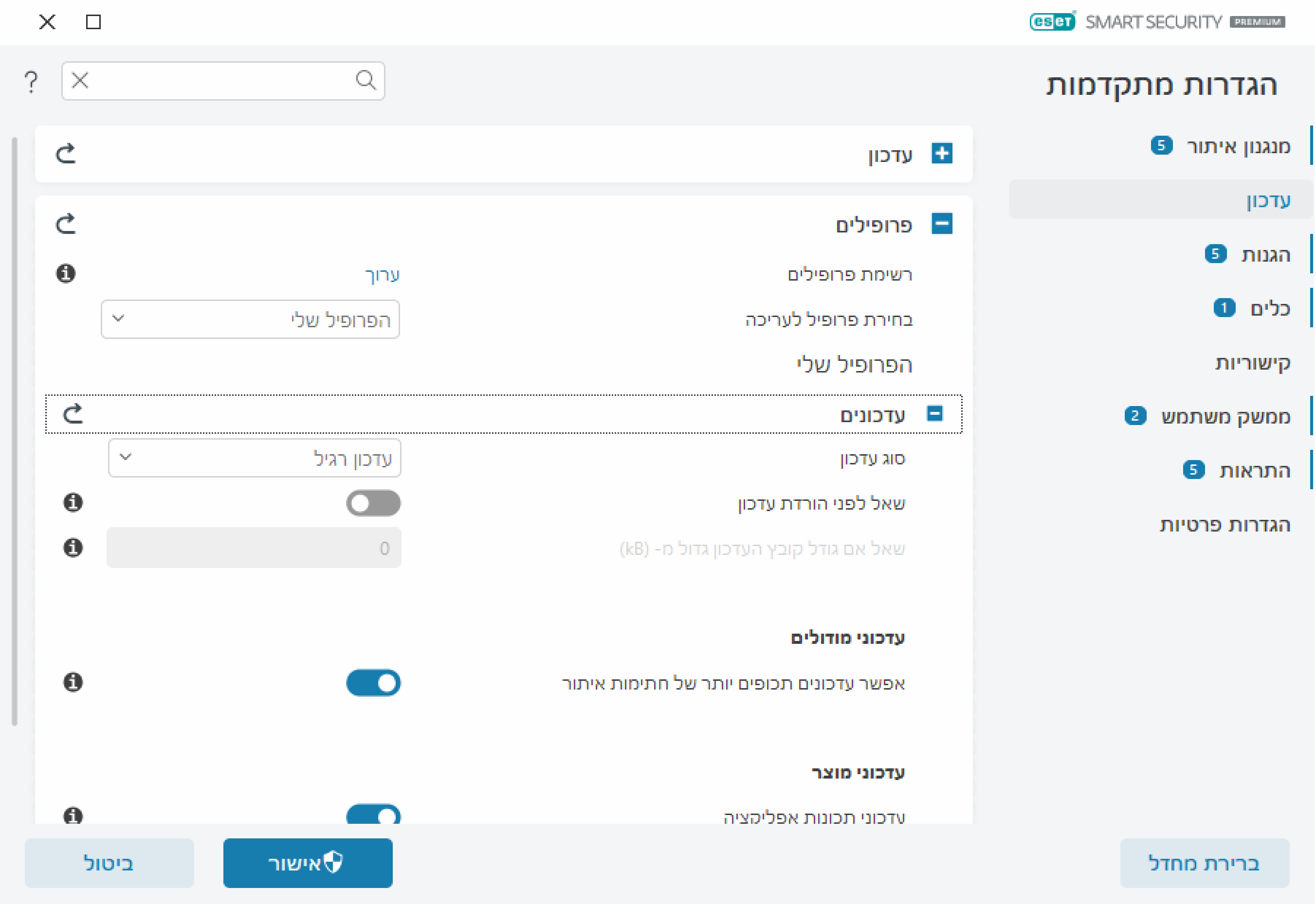
כדי ליצור פרופיל חדש, עיין בסעיף עדכון פרופילים.

מיתוג אוטומטי של פרופיל - מאפשר להקצות פרופיל עדכון לפרופיל מסוים של חיבור רשת.

אם אתה נתקל בקושי בעת ניסיון להוריד עדכונים של מנגנון האיתור או של מודולים, לחץ על **נקה** ליד **נקה מטמון עדכונים** כדי לנקות את קובצי העדכון הזמניים/המטמון.

החזרת מודול למצב קודם

אם אתה חושד שאחד מהעדכונים החדשים של מנגנון האיתור ו/או מודולי התכנית עשוי להיות לא יציב או פגום, באפשרותך לחזור לגרסה הקודמת ולהשבית את העדכונים לפרק זמן מוגדר.



כדי שהורדת העדכונים תתבצע כהלכה, הכרחי שתמלא את כל פרמטרי העדכון בצורה נכונה. אם אתה משתמש בחומת אש, אנא ודא שלתוכנית ESET שברשותך מותר לנהל תקשורת עם האינטרנט (לדוגמה תקשורת HTTP).

פרופילים

ניתן ליצור פרופילי עדכון עבור מגוון תצורות ומשימות עדכון. יצירת פרופילי עדכון שימושית במיוחד עבור משתמשי התקנים ניידים, שצריכים פרופיל חלופי עבור מאפייני חיבור לאינטרנט שמשתנים בקביעות.

התפריט הנפתח **בחר פרופיל לעריכה** מציג את הפרופיל שנבחר כעת, וכברירת מחדל מוגדר כ**הפרופיל שלי**. כדי ליצור פרופיל חדש, לחץ על **עריכה** לצד **רשימת פרופילים**, הזן **שם פרופיל** ואז לחץ על **הוסף**.

עדכונים

כברירת מחדל, **סוג העדכון** מוגדר כ**עדכון סדיר** כדי להבטיח הורדה אוטומטית של קובצי העדכון מהשרת של ESET תוך שימוש מינימלי בתעבורת רשת. עדכוני קדם-הפצה (האפשרות **עדכון קדם-הפצה**) הם עדכונים שעברו בדיקה פנימית מקיפה ויהיו זמינים בקרוב לציבור הרחב. הפעלת עדכוני קדם-הפצה יכולה להועיל לך בכך שתהיה לך גישה לשיטות הזיהוי ולתיקונים העדכניים ביותר. עם זאת, ייתכן שעדכוני קדם-הפצה לא יהיו יציבים מספיק כל הזמן, ואין להשתמש בהם בשרתים ותחנות עבודה המשמשים לייצור, כשנדרשות יציבות וזמינות מקסימליות.

שאל לפני הורדת עדכון התוכנית תציג התראה שבה תוכל לבחור אם לאשר או לדחות הורדות של קובצי עדכון.

שאל אם גודל קובץ העדכון גדול מ- (kB) התוכנית תציג תיבת דו-שיח לאישור אם גודל קובץ העדכון גדול מהערך שצוין. אם גודל קובץ העדכון מוגדר ל-0 kB, התוכנית תציג תיבת דו-שיח לאישור.

עדכוני מודולים

אפשר עדכונים תכופים יותר של חתימות האיתור חתימות האיתור יעודכנו במרווח זמן קצר יותר. ביטול הגדרה זו עלול להשפיע לרעה על שיעור האיתור.

עדכוני מוצר

עדכוני תכונות אפליקציה התקן באופן אוטומטי גרסאות חדשות של ESET Smart Security Premium.

אפשרויות חיבור

כדי להשתמש בשרת Proxy להורדת עדכונים, עיין במקטע אפשרויות חיבור.

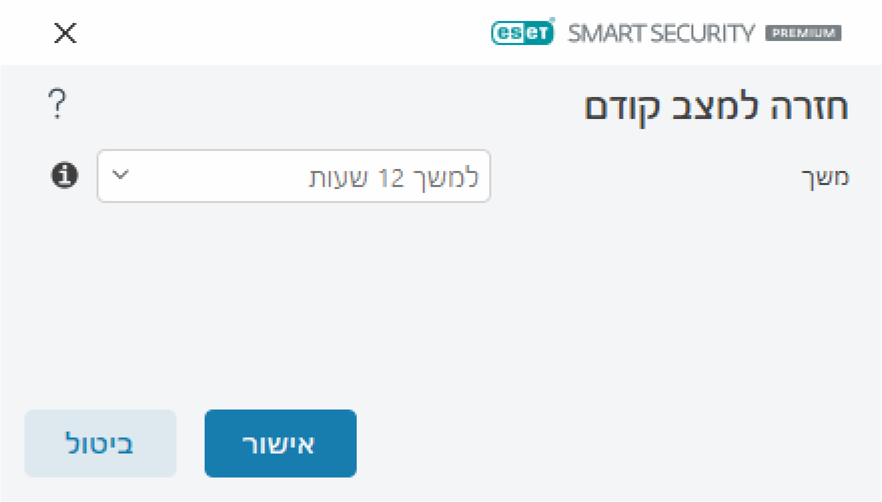
חזרה למצב קודם לאחר עדכון

אם אתה חושד שעדכון חדש של מנגנון האיתור או שמודולי תכניות חדשים עשויים להיות לא יציבים או פגומים, באפשרותך לחזור לגרסה הקודמת ולהשבית את העדכונים באופן זמני. לחלופין, באפשרותך להפעיל עדכונים שהושבתו בעבר, אם השהית אותם לפרק זמן בלתי מוגבל.

ESET Smart Security Premium מתעדת תמונות של מנגנון האיתור ושל מודולי התכניות לשימוש עם התכונה חזרה למצב קודם. כדי ליצור תמונות של מסד נתוני וירוסים, השאר את האפשרות **יצירת תמונות מצב של מודולים** מופעלת. כאשר האפשרות **יצירת תמונות מצב של מודולים** מופעלת, התמונה הראשונה נוצרת במהלך העדכון הראשון. התמונה הבאה נוצרת לאחר 48 שעות. השדה **מספר תמונות המצב המאוחסנות מקומית** מגדיר את מספר התמונות המאוחסנות של מנגנון האיתור.

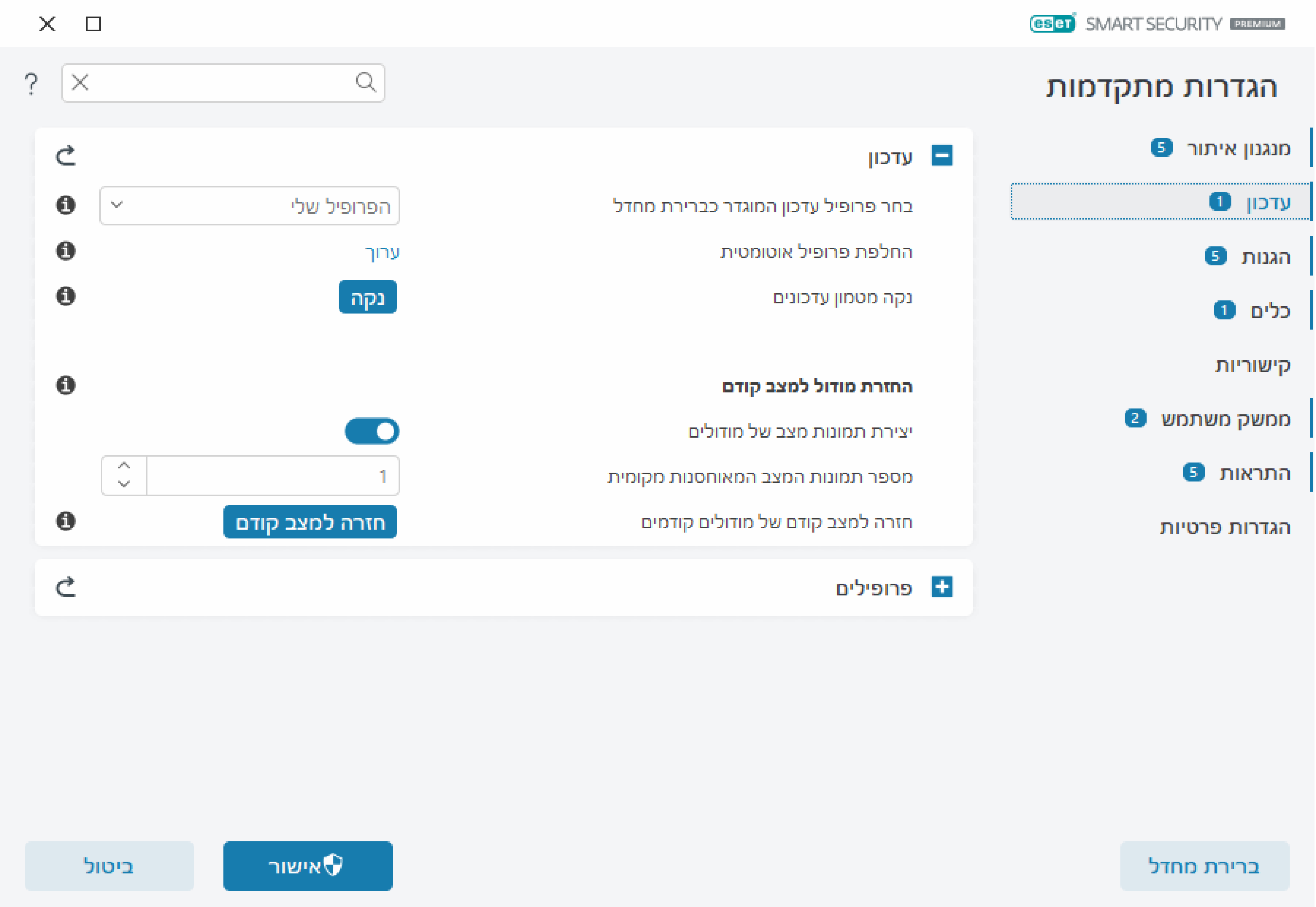
> כשתגיע למספר התמונות המרבי (לדוגמה, שלוש), התמונה הישנה ביותר תוחלף בתמונה חדשה מדי 48 שעות. ESET Smart Security Premium מחזיר את הגרסאות של מנגנון האיתור ושל עדכון מודולי התכניות לתמונה הישנה ביותר.

אם תלחץ על **חזרה למצב קודם** בהגדרות מתקדמות > **עדכון** > **עדכון**, יהיה עליך לבחור מהתפריט הנפתח **משך זמן** מרווח זמן שמייצג את פרק הזמן להשהיית עדכוני מנגנון האיתור ומודולי התוכנית.



בחר **עד לביטול** כדי להשהות את העדכונים השוטפים לפרק זמן בלתי מוגבל, עד שתשחזר את פונקציונליות העדכון באופן ידני. ESET לא ממליצה לבחור באפשרות זו מפני שהיא מהווה סיכון אבטחה אפשרי.

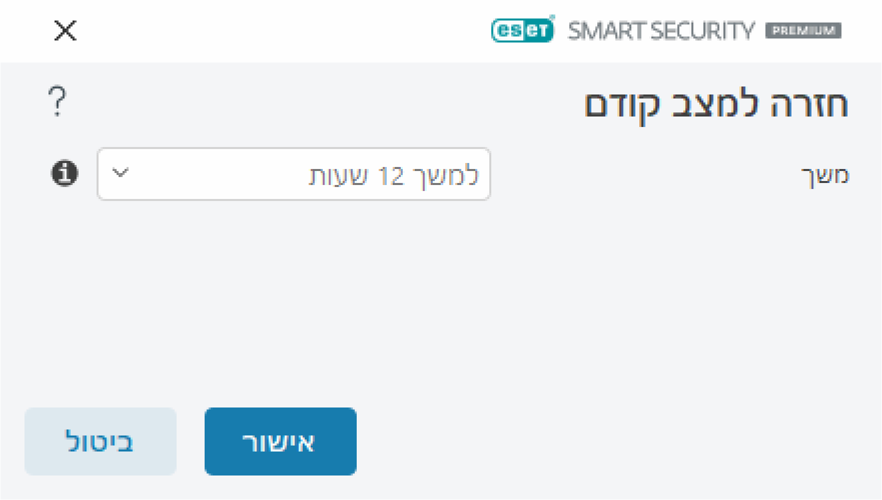
אם מבוצעת חזרה למצב קודם, הלחצן **חזרה למצב קודם** משתנה והופך ל**אפשר עדכונים**. לא יותרו עדכונים במרווח הזמן שנבחר בתפריט הנפתח **השהיית עדכונים**. גרסת מנגנון האיתור עוברת שדרוג לאחור לגרסה הישנה ביותר שזמינה ומאוחסנת כתמונה במערכת הקבצים המקומית של המחשב.



ניח שהמספר 22700 הוא מספר הגרסה העדכנית ביותר של מנגנון האיתור, ו-22698 ו-22696 מאוחסנות כתמונות של מנגנון האיתור. שים לב ש-22697 אינה זמינה. בדוגמה זו, המחשב כובה במהלך עדכון 22697, ועדכון חדש יותר הפך לזמין לפני ההורדה של 22697. אם השדה **מספר תמונות המצב המאוחסנות מקומית** מוגדר כ-2 ותלחץ על **חזרה למצב קודם**, מנגנון האיתור (כולל מודולי התכנית) ישוחזר לגרסה מספר 22696. תהליך זה עשוי להימשך זמן מה. בדוק אם גרסת מנגנון האיתור שודרגה לאחור במסך עדכון.

מרווח זמן לחזרה למצב קודם

אם תלחץ על **חזרה למצב קודם** בהגדרות מתקדמות < **עדכון** < **עדכון**, יהיה עליך לבחור מהתפריט הנפתח **משך זמן** מרווח זמן שמייצג את פרק הזמן להשהיית עדכוני מנגנון האיתור ומודולי התוכנית.



בחר **עד לביטולם** כדי להשהות את העדכונים השוטפים לפרק זמן בלתי מוגבל, עד שתשחזר את פונקציונליות העדכון באופן ידני. ESET לא ממליצה לבחור באפשרות זו מפני שהיא מהווה סיכון אבטחה אפשרי.

עדכוני מוצר

המקטע **עדכוני מוצר** מאפשר לך להתקין באופן אוטומטי עדכוני תכונות חדשות כאשר הם זמינים.

עדכוני תכונות האפליקציה מוסיפים תכונות חדשות או שהם משנים תכונות שכבר קיימות בגרסאות הקודמות. ניתן לבצע אותם באופן אוטומטי ללא התערבות המשתמש, או שבאפשרותך לבחור לקבל הודעה כאשר קיימים עדכונים חדשים זמינים. אחרי שעדכון תכונת אפליקציה כלשהו הותקן, ייתכן שיהיה צורך בהפעלה מחדש של המחשב.

עדכוני תכונות אפליקציה ⍰ כאשר אפשרות זו מופעלת, עדכוני תכונות האפליקציה יבוצעו באופן אוטומטי.

אפשרויות חיבור

כדי לגשת לאפשרויות ההתקנה של שרת ה-Proxy עבור פרופיל עדכון מסוים, פתח את הגדרות מתקדמות > **עדכון** > **פרופילים** > **עדכונים** > **אפשרויות חיבור**. לחץ על התפריט הנפתח **מצב Proxy** ובחר אחת משלוש האפשרויות הבאות:

- אל תשתמש בשרת proxy
- חיבור באמצעות שרת proxy
- שימוש בהגדרות שרת proxy גלובליות

בחר באפשרות **שימוש בהגדרות שרת Proxy גלובליות** כדי להשתמש בהגדרת התצורה של שרת ה-Proxy שכבר צוינה בהגדרות מתקדמות > **חיבוריות** > **שרת Proxy**.

בחר באפשרות **אל תשתמש בשרת proxy** כדי לציין שהמערכת לא תשתמש בשרת proxy לעדכון של ESET Smart Security Premium.

באפשרות **חיבור באמצעות שרת proxy** יש לבחור אם:

- שרת proxy שונה מזה שהוגדר תחת הגדרות מתקדמות > **קישוריות** משמש לצורך עדכון ESET Smart Security Premium. בתצורה זו, המידע בשרת ה- proxy החדש אמור להיות מצוין תחת כתובת של **שרת Proxy**, **יציאת** תקשורת (3128 כברירת מחדל), ונדרשים **שם משתמש** ו**סיסמה** לשרת ה- proxy.

- הגדרות שרת ה-proxy לא מוגדרות גלובלית, אולם ESET Smart Security Premium יתחבר לשרת proxy לצורך עדכונים.
- המחשב שלך מחובר לאינטרנט דרך שרת proxy. ההגדרות נלקחות מ-Internet Explorer במהלך התקנת התוכנית, אולם אם בסופו של דבר משנים אותן (למשל אם אתה מחליף את ה-ISP שלך), אנא ודא שהגדרות proxy המפורטות בחלון זה נכונות. אם תנאי זה לא יתקיים, התוכנית לא תוכל להתחבר לשרתי העדכון.

הגדרת ברירת המחדל של שרת ה-proxy היא **שימוש בהגדרות שרת proxy גלובליות**.

השתמש בחיבור ישיר אם proxy לא זמין – אם לא ניתן להגיע אליו, תהיה עקיפה של ה- Proxy במהלך העדכון.

> השדות **שם משתמש** ו**סיסמה** במקטע זה ספציפיים לשרת ה- proxy. מלא שדות אלה רק אם נדרשים שם משתמש וסיסמה כדי לגשת לשרת ה- proxy. עליך למלא שדות אלה רק אם אתה יודע שדרושה לך סיסמה כדי לגשת לאינטרנט דרך שרת proxy.

הגנות

אמצעי הגנה מפני התקפות זדוניות על המערכת על-ידי שליטה בקבצים, בדואר אלקטרוני ובתקשורת אינטרנט. לדוגמה, תחל פעולת תיקון בעת סיווג של אובייקט כתוכנה זדונית. ההגנות יכולות למנוע אותו על-ידי חסימה שלו ולאחר מכן ניקוי, מחיקה או העברה של האובייקט להסגר.

כדי להגדיר הגנות בצורה מפורטת, פתח את הגדרות מתקדמות > **הגנות**.

> שינויים בהגנות יבוצעו רק על-ידי משתמש מנוסה. קביעה שגויה של הגדרות מנגנון האיתור עלולה להוביל לפגיעה ברמת ההגנה.

במקטע זה:

- תגובות איתור
- הגדרת דיווח
- הגדרת הגנה

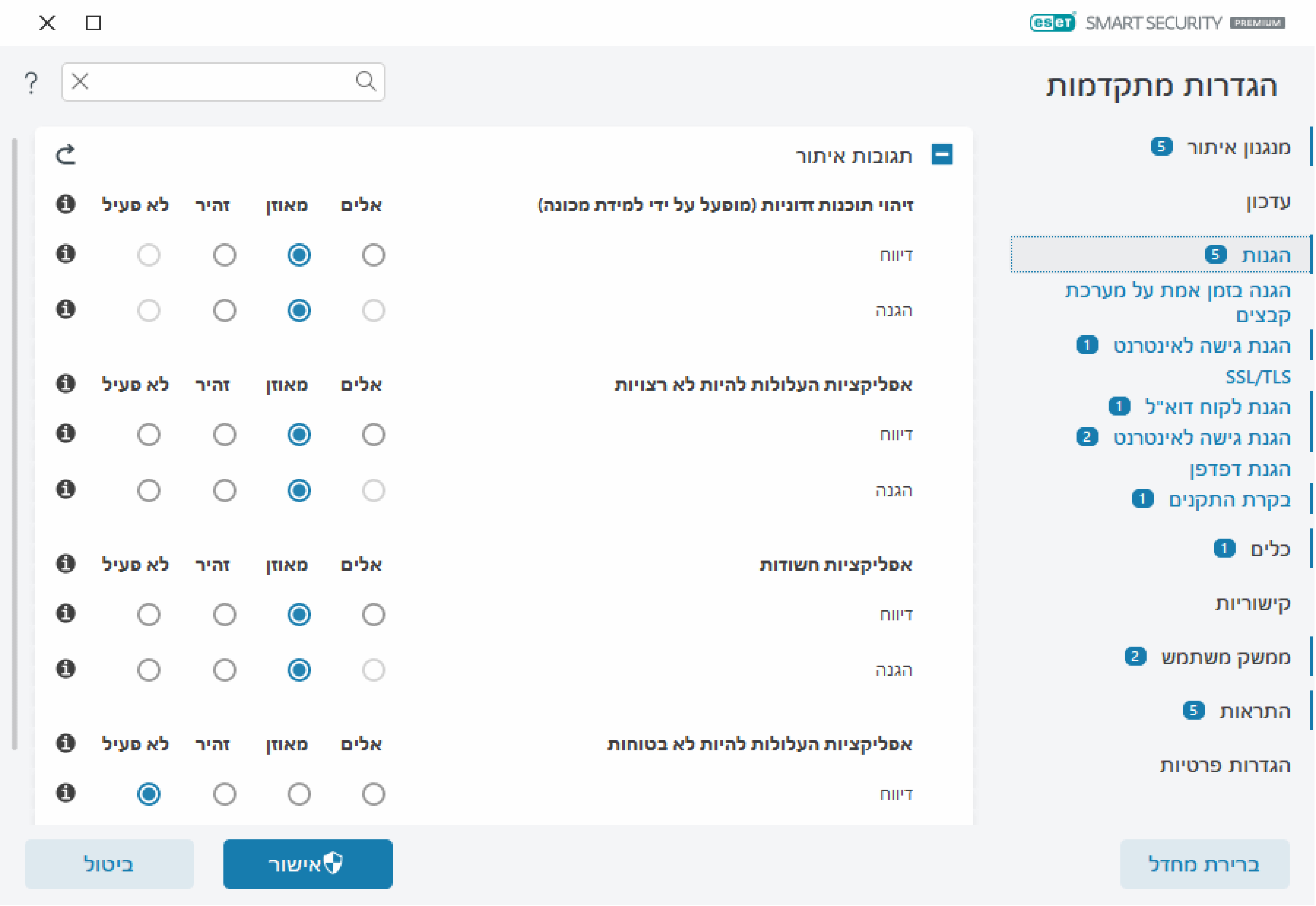
תגובות איתור

תגובות איתור מאפשרות לך לקבוע תצורה של רמות דיווח והגנה עבור הקטגוריות הבאות:

- **זיהוי תוכנות זדוניות (מופעל על ידי למידת מכונה)** – וירוס מחשב הוא פיסת קוד זדוני אשר מתווספת או מתחברת לקבצים קיימים במחשב. עם זאת, לעתים קרובות השימוש במונח "וירוס" הוא שגוי. המונח "תוכנה זדונית" (Malware) הוא מדויק יותר. איתור תוכנות זדוניות מבוצע על ידי מודול מנגנון האיתור בשילוב עם רכיב למידת המכונה. קרא עוד על סוגי האפליקציות הללו במילון.

- **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 האפליקציות הללו במילון.

- **אפליקציות חשודות** כוללות תכניות שנדחסו באמצעות אורזים או מגנים. המגנים הללו מנוצלים לעתים קרובות על-ידי מחברי תוכנות זדוניות כדי להתחמק מאיתור האפליקציות.
- **אפליקציות העלולות להיות לא בטוחות** – הן תוכנות מסחריות לגיטימיות שעלולות להיות מנוצלות למטרות זדוניות. דוגמאות לאפליקציות העלולות להיות לא בטוחות (PUA) כוללות כלים לגישה מרחוק, אפליקציות לפיצוח סיסמאות ורשמי הקשות (תוכניות המתעדות כל הקשה של משתמש על המקלדת). קרא עוד על סוגי האפליקציות הללו במילון.



> **הגנה משופרת**
> למידת מכונה מתקדמת היא כעת חלק ממנגנון האיתור, כשכבה מתקדמת של הגנה שמשפרת את האיתור ומבוססת על למידת מכונה. קרא עוד על סוג הגנה זה במילון.

הגדרות דיווח

כאשר מתרחש איתור (כלומר איום מאותר ומסווג כתוכנה זדונית), המידע נרשם ביומן האובייקטים שאותרו והתראות בשולחן העבודה מתרחשות אם הוגדרו ב-ESET Smart Security Premium.

סף דיווח מוגדר לכל קטגוריה (להלן "קטגוריה"):

1. איתור תוכנות זדוניות
2. אפליקציה העלולה להיות לא רצויה
3. עלולה להיות לא בטוחה
4. אפליקציות חשודות

הדיווח מבוצע בעזרת מנגנון האיתור, כולל רכיב למידת המכונה. באפשרותך להגדיר סף דיווח גבוה יותר מאשר סף ההגנה הנוכחי. הגדרות דיווח אלה אינן משפיעות על חסימה, ניקוי או מחיקה של אובייקטים.

קרא להלן לפני שינוי סף (או רמה) של דיווח על קטגוריה:

סף	הסבר
אגרסיבי	הדיווח על קטגוריה מוגדר לרגישות מקסימלית. אובייקטים מזוהים רבים יותר מדווחים. ההגדרה **אגרסיבי** יכולה לאתר אובייקטים כקטגוריה באופן שגוי.
מאוזן	הדיווח על קטגוריה מוגדר כמאוזן. הגדרה זו ממוטבת לאיזון הביצועים והדיוק של שיעורי האיתור ומספר האובייקטים המדווחים באופן כוזב.
זהיר	הדיווח על קטגוריה מוגדר למזעור האובייקטים המזוהים באופן שגוי תוך שמירה על רמת הגנה מספקת. אובייקטים מדווחים רק כאשר ההסתברות ניכרת ומתאימה לאופן הפעולה של קטגוריה.
לא פעיל	הדיווח על אפליקציות חשודות אינו פעיל, ואובייקטים מזוהים מסוג זה לא נמצאים, מדווחים או מנוקים. כתוצאה מכך, הגדרה זו משביתה את ההגנה מפני סוג זיהוי זה. האפשרות 'כבוי' לא זמינה עבור דיווח על תוכנות זדוניות והיא ערך ברירת המחדל עבור אפליקציות העלולות להיות לא בטוחות.

זמינות מודולי ההגנה של ESET Smart Security Premium

הזמינות (מאופשרת או מושבתת) של מודול הגנה עבור סף קטגוריה נבחר היא כדלהלן:

	אגרסיבי	מאוזן	זהיר	כבוי*
מודול למידת מכונה מתקדמת	✓ (מצב אגרסיבי)	✓ (מצב שמרני)	X	X
מודול מנגנון איתור	✔	✔	✔	X
מודולי הגנה אחרים	✔	✔	✔	X

* לא מומלץ

הצגת גרסת המוצר, גרסאות מודול התוכנית ותאריכי גרסאות Build

1. לחץ על **עזרה ותמיכה** > **אודות ESET Smart Security Premium.**
2. שורת הטקסט הראשונה במסך **אודות** מציגה את מספר הגרסה של מוצר ESET שברשותך.
3. לחץ על **רכיבים מותקנים** כדי לגשת למידע אודות מודולים ספציפיים.

הערות חשובות

כמה הערות חשובות לגבי הגדרת סף מתאים לסביבה שלך:

- הסף **מאוזן** מומלץ עבור מרבית ההגדרות.
- ככל שסף הדיווח גבוה יותר, שיעור האיתור גבוה יותר, אך כך גם עולה הסיכוי לזיהוי באופן שגוי של אובייקטים.
- מנקודת מבט מציאותית, אין ערובה לשיעור איתור של 100% וכן אין ערובה לסיכוי של 0% למניעת חלוקה שגויה לקטגוריות של אובייקטים נקיים כתוכנות זדוניות.
- שמור על עדכניות ESET Smart Security Premium והמודולים שלו כדי למקסם את האיזון בין הביצועים לדיוק של שיעורי האיתור ומספר האובייקטים המדווחים באופן שגוי.

הגדרות הגנה

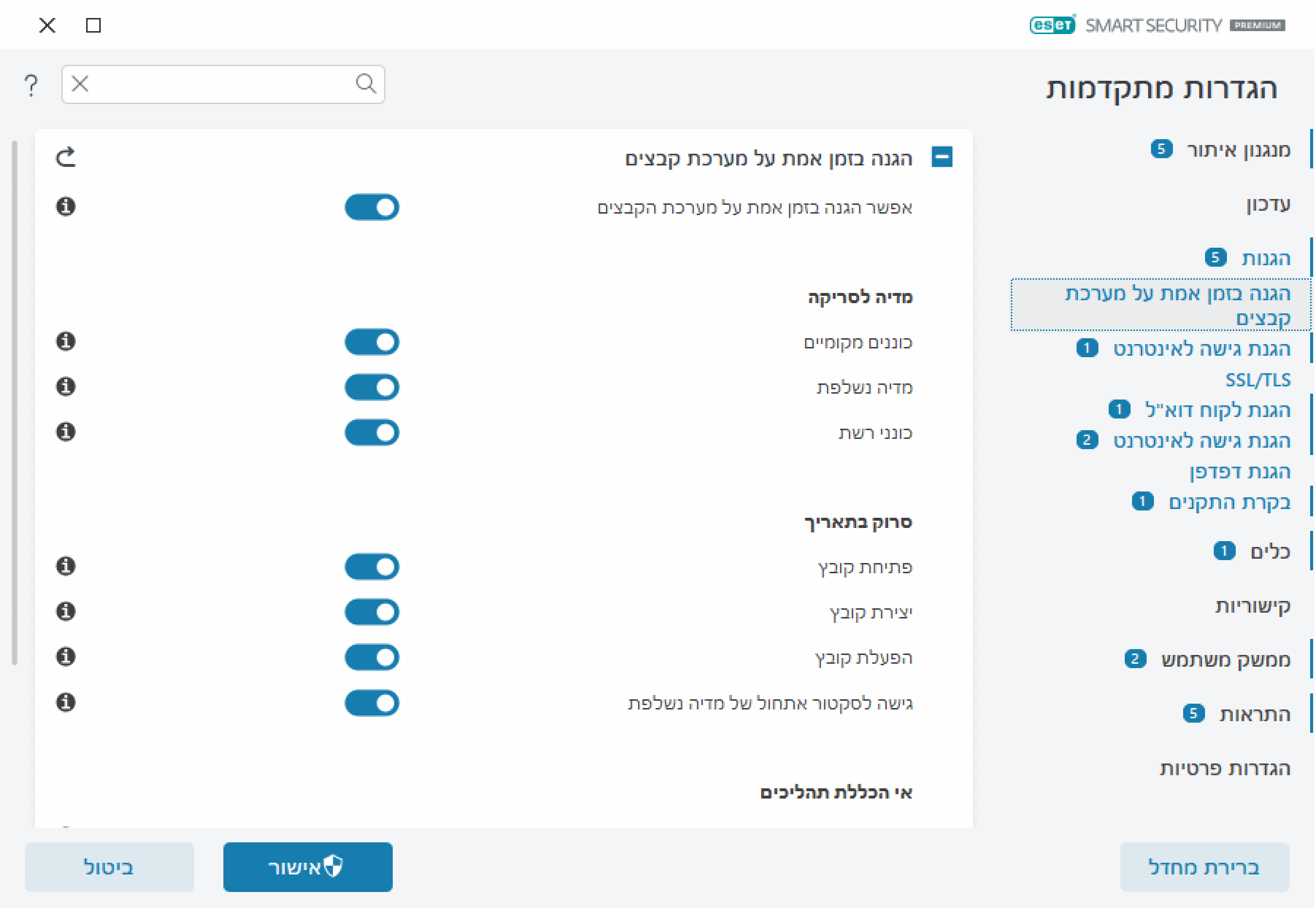
אם דווח אובייקט המסווג כקטגוריה, התוכנית חוסמת את האובייקט ולאחר מכן מנקה, מסירה או מעבירה אותו להסגר.

קרא להלן לפני שינוי סף (או רמה) של הגנה על קטגוריה:

סף	הסבר
אגרסיבי	אובייקטים מזוהים שדווחו ברמה 'אגרסיבית' (או ברמה נמוכה יותר) נחסמים, ותיקון אוטומטי (כלומר, ניקוי) מופעל. הגדרה זו מומלצת כאשר כל נקודות הקצה נסרקו עם הגדרות 'אגרסיביות' ואובייקטים שדווחו באופן שגוי נוספו לאי ההכללות באיתור.
מאוזן	אובייקטים מזוהים שדווחו ברמה 'מאוזן' (או ברמה נמוכה יותר) נחסמים, ותיקון אוטומטי (כלומר, ניקוי) מופעל.
זהיר	אובייקטים מזוהים שדווחו ברמה 'זהיר' נחסמים, ותיקון אוטומטי (כלומר, ניקוי) מופעל.
לא פעיל	שימושי לזיהוי ולאי-הכללה של אובייקטים שדווחו באופן שגוי. האפשרות 'כבוי' לא זמינה עבור הגנה על תוכנות זדוניות והיא ערך ברירת המחדל עבור אפליקציות העלולות להיות לא בטוחות.

הגנה בזמן אמת על מערכת קבצים

הגנה בזמן אמת על מערכת קבצים מפקחת על כל הקבצים במערכת לאיתור קוד זדוני בעת פתיחה, יצירה או הפעלה.



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** דרך הגדרות מתקדמות > **הגנות** > **הגנה**

בזמן אמת על מערכת קבצים < **הגנה בזמן אמת על מערכת קבצים**.

מדיה לסריקה

כברירת מחדל, כל סוגי המדיה נסרקים לאיתור איומים פוטנציאליים:

- **כוננים מקומיים** סריקת כל הכוננים הקשיחים הקבועים והכוננים הקשיחים של המערכת (לדוגמה: *C:*, *D:*).
- **מדיה נשלפת** סריקת CD/DVD, אחסון USB, כרטיסי זיכרון וכן הלאה
- **כונני רשת** סריקת כל כונני הרשת הממופים (לדוגמה: *H:* כ- *\\store04*) או כונני הרשת של גישה ישירה (לדוגמה: *\\store08*).

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 עם פתיחתם, יצירתם או הפעלתם. מומלץ לשמור על הגדרות ברירת המחדל הללו, מאחר שהן מספקות את דרגת ההגנה המרבית בזמן אמת למחשב שלך:

- **פתיחת קובץ** סריקה כאשר קובץ נפתח.
- **יצירת קובץ** סריקת קובץ שנוצר או השתנה.
- **הפעלת קובץ** סריקה כאשר קובץ מופעל.
- **גישה לסקטור אתחול של מדיה נשלפת** כאשר מדיה נשלפת המכילה סקטור אתחול מוכנסת למכשיר, סקטור האתחול נסרק מיד. אפשרות זו אינה מאפשרת סריקת קבצים במדיה נשלפת. סריקת קבצים במדיה נשלפת ממוקמת תחת **מדיה לסריקה** < **מדיה נשלפת**. כדי ש**גישה לסקטור אתחול במדיה נשלפת** תפעל כראוי, השאר את האפשרות **סקטורי אתחול/UEFI** מופעלת ב-ThreatSense.

אי הכללת תהליכים

ראה אי הכללת תהליכים.

ThreatSense

הגנה בזמת אמת על מערכת קבצים בודקת את כל סוגי המדיה ומופעלת על-ידי אירועי מערכת שונים, כגון גישה לקובץ. באמצעות שיטות איתור של טכנולוגיית **ThreatSense** (כפי שמתוארות במקטע ThreatSense), ניתן להגדיר 'הגנה בזמן אמת על מערכת קבצים' כך שתטפל בצורה 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. כדי לשנות הגדרה זו, פתח את הגדרות מתקדמות < **הגנות** < **הגנה בזמן אמת על מערכת קבצים**. לחץ על **ThreatSense** < **אחר** ובחר או בטל את הבחירה באפשרות **אפשר מיטוב חכם**.

הגנה בזמן אמת על מערכת קבצים מאפשרת לך גם להגדיר פרמטרים נוספים של ThreatSense.

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.

אל תתבלבל עם סימונים קובץ שלא ייכללו, אי הכללות HIPS, החרגות לזיהויים או החרגות לביצועים.

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*).

באפשרותך להוסיף קבצי הפעלה לרשימת התהליכים שלא נכללו דרך הגדרות מתקדמות > **הגנות** > **הגנה בזמן אמת על מערכת קבצים** > **הגנה בזמן אמת על מערכת קבצים** > **החרגות של 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.

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 Smart Security Premium ולא מופעלת סריקה בפעולות הקבצים שמבצע תהליך זה.

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.

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

חלון דו-שיח זה מאפשר לך **להוסיף** תהליכים שאינם נכללים במנגנון האיתור. 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*).

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

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.

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 Smart Security Premium, כל ההגדרות פועלות באופן המיטבי כדי לספק למשתמשים את רמת אבטחת המערכת המקסימלית. כדי לשחזר את הגדרות ברירת המחדל, לחץ על לצד הגדרות מתקדמות > **הגנות** > **תגובות איתור**.

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
לאחר הזנת כתובת URL זו בדפדפן, תראה הודעה על כך שהאיום הוסר.

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 בשוגג את ההגנה בזמן אמת, יש להפעיל מחדש את התכונה. כדי להפעיל מחדש את ההגנה בזמן אמת, עבור אל **הגדרות** בחלון התוכנית הראשי ולחץ על **הגנת מחשב** > **הגנה בזמן אמת על מערכת קבצים**.

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 מופעלת, פתח את הגדרות מתקדמות > **הגנות** > **הגנה בזמן אמת על מערכת קבצים**.

אם ההגנה בזמן אמת אינה מזהה ומנקה חדירות

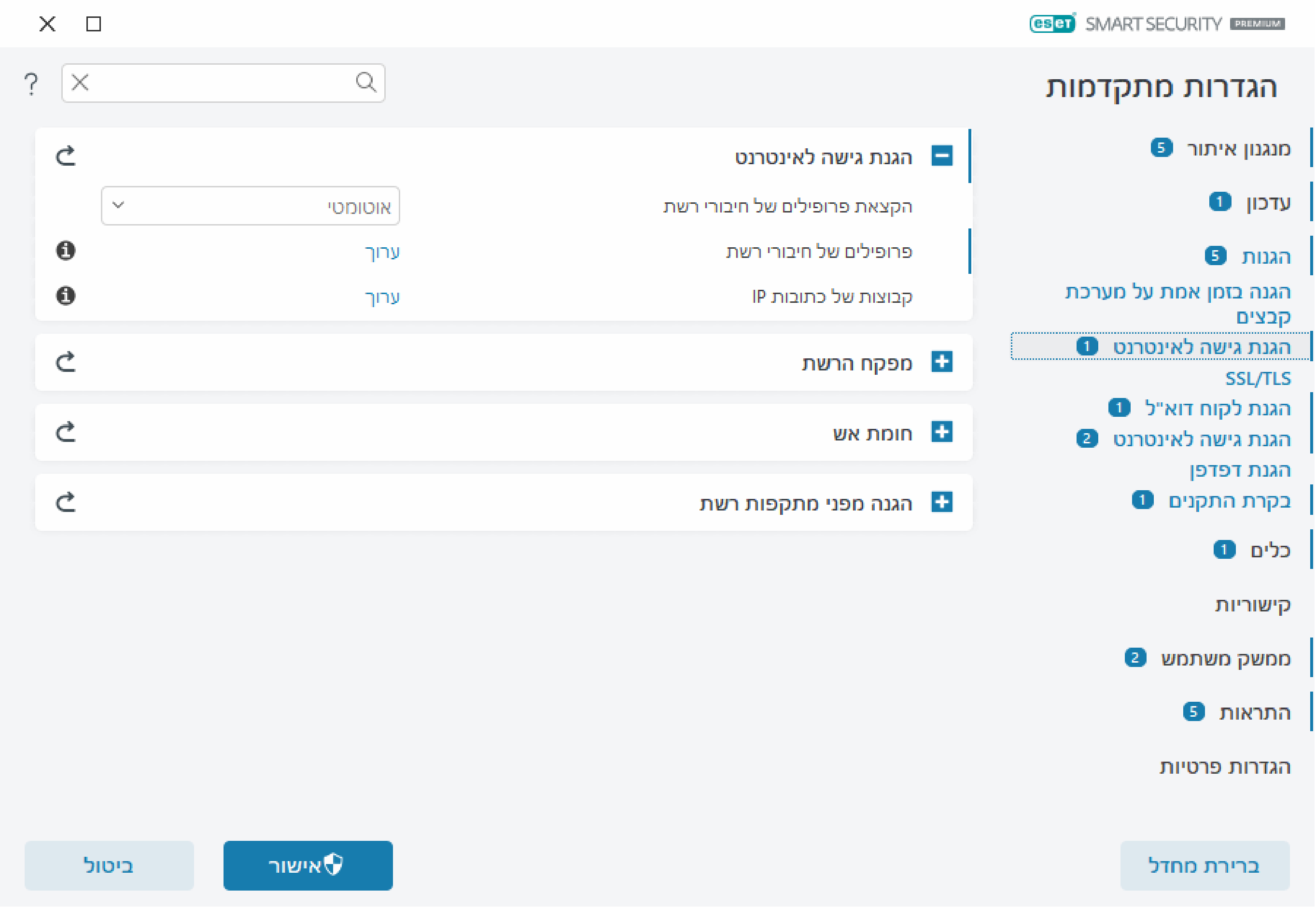
ודא שלא מותקנות במחשב שלך תוכניות אנטי-וירוס אחרות. שתי תוכניות אנטי-וירוס המותקנות במחשב בו-זמנית עשויות להתנגש זו עם זו. לפני ההתקנה של ESET מומלץ להסיר את ההתקנה של כל תוכנית האנטי-וירוס האחרות במערכת.

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. כדי לפתור את הבעיה, צור לוג של ESET SysInspector ושלח אותו לתמיכה הטכנית של ESET לצורך ניתוח.

הגנת גישה לאינטרנט

על ידי הגנת גישה לאינטרנט אפשר להגדיר את כל חיבורי הרשת שלך בצורה מפורטת. באפשרותך למנוע/לאפשר גישה למחשב שלך ברשתות מסוימות, לאפשר/למנוע גישה להתקני רשת מהמחשב שלך ועוד בהתאם לתצורה. כברירת מחדל, ל-ESET Smart Security Premium יש כללים מוגדרים מראש של חומת אש והגנה על גישה לרשת כדי להשיג את האבטחה המקסימלית. עם זאת, יש סביבות שעשויות להזדקק לתצורה מותאמת אישית. רק משתמש מנוסה אמור לשנות את הגדרות ברירת המחדל.



באפשרותך לקבוע את התצורה של ההגדרות הבאות דרך הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** (לחץ על הקישורים בהמשך לקבלת תיאור מפורט של כל אפשרות של הגנת גישה לאינטרנט):

הגנת גישה לאינטרנט

פרופילי חיבור רשת - אפשר להשתמש בפרופילים כדי לשלוט בהתנהגות של חומת האש עבור חיבורי רשת ספציפיים.

ערכות IP - אפשר להגדיר אוספים של כתובות IP שיוצרים קבוצה לוגית אחת של כתובות IP, שבה ניתן להשתמש עבור כללי חומת אש.

מפקח הרשת

חומת אש

הגנה מפני מתקפות רשת

פרופילים של חיבורי רשת

ניתן להשתמש בפרופילים כדי לשלוט באופן הפעולה של הגנת רשת של ESET Smart Security Premium עבור חיבורי רשת מסוימים. בעת יצירה או עריכה של כלל חומת אש, כלל IDS או כלל הגנה מפני מתקפות Brute Force, אפשר להקצות אותו לפרופיל מסוים או להחיל אותו על כל הפרופילים. כאשר פרופיל מסוים פעיל בחיבור רשת, רק הכללים הגלובליים (כללים שלא צוין בהם פרופיל) והכללים שהוקצו לפרופיל זה מוחלים עליו. באפשרותך ליצור מספר פרופילים עם כללים שונים, שמוקצים לחיבורי רשת, כדי לשנות בקלות את אופן הפעולה של חומת האש.

באפשרותך לקבוע את התצורה של פרופילי חיבור רשת והקצאות של חיבורי רשת דרך הגדרות מתקדמות < **הגנות** < **הגנת גישה לאינטרנט** < **הגנת גישה לאינטרנט**.

הקצאת פרופיל חיבור רשת - מאפשר לבחור אם לחיבורי רשת חדשים שהתגלו באופן אוטומטי (בחר **אוטומטי** מהתפריט הנפתח) מוקצה פרופיל מוגדר מראש או מותאם אישית המבוסס על מפעילים שמוגדרים בפרופילי חיבור רשת או אם ברצונך להישאל (בחר **שאל** מהתפריט הנפתח) כדי להגדיר הגנת רשת ולהקצות פרופיל באופן ידני בכל פעם שרשת חדשה מזוהה.

באפשרותך גם להקצות באופן ידני פרופיל חיבור רשת ספציפי בחלון התוכנית הראשי < **הגדרה** < **הגנת רשת** < **חיבורי רשת**. העבר את העכבר מעל חיבור רשת מסוים ולחץ על סמל התפריט ⋮ < **ערוך** כדי לפתוח את החלון הגדר הגנת רשת ובחר פרופיל.

פרופילי חיבור רשת - לחץ על **ערוך** כדי להוסיף או לערוך פרופילי חיבור רשת.

הפרופילים הבאים מוגדרים מראש ולא ניתן לערוך/למחוק אותם:

פרטי ⍰ עבור רשת מהימנה (רשת ביתית או משרדית). המחשב שלך וקבצים משותפים המאוחסנים במחשב שלך גלויים למשתמשי רשת אחרים, ומשאבי מערכת נגישים למשתמשים אחרים ברשת (הגישה לקבצים משותפים ולמדפסות מופעלת, תקשורת נכנסת של RPC מופעלת ושיתוף שולחן עבודה מרוחק זמין). אנו ממליצים להשתמש בהגדרה זו בעת גישה לרשת מקומית מאובטחת. פרופיל זה מוקצה באופן אוטומטי לחיבור רשת אם הוא מוגדר כתחום או רשת פרטית ב-Windows.

ציבורי ⍰ עבור רשתות לא מהימנות (רשת ציבורית). קבצים ותיקיות במערכת שלך אינם משותפים עם משתמשים אחרים ואינם גלויים להם ברשת, ושיתוף משאבי מערכת מושבת. אנו ממליצים להשתמש בהגדרה זו בעת גישה לרשתות אלחוטיות. פרופיל זה מוקצה באופן אוטומטי לכל חיבור רשת שאינו מוגדר בתור תחום או רשת פרטית ב-Windows.

כאשר חיבור חומת אש עובר לפרופיל אחר, תופיע התראה בפינה השמאלית התחתונה של המסך.

הוספה או עריכה של פרופילי חיבור רשת

אפשר להוסיף או לערוך פרופילי חיבור רשת דרך הגדרות מתקדמות < **הגנות** < **הגנת גישה לאינטרנט** < **הגנת גישה לאינטרנט** < **פרופילים של חיבורי רשת** < **ערוך**. כדי לערוך פרופיל, יש לבחור אותו מהרשימה בחלון **פרופילי חיבור**

לרשת.

הפרופילים הבאים מוגדרים מראש ולא ניתן לערוך/למחוק אותם:

פרטי □ עבור רשת מהימנה (רשת ביתית או משרדית). המחשב שלך וקבצים משותפים המאוחסנים במחשב שלך גלויים למשתמשי רשת אחרים, ומשאבי מערכת נגישים למשתמשים אחרים ברשת (הגישה לקבצים משותפים ולמדפסות מופעלת, תקשורת נכנסת של RPC מופעלת ושיתוף שולחן עבודה מרוחק זמין). אנו ממליצים להשתמש בהגדרה זו בעת גישה לרשת מקומית מאובטחת. פרופיל זה מוקצה באופן אוטומטי לחיבור רשת אם הוא מוגדר כתחום או רשת פרטית ב-Windows.

ציבורי □ עבור רשתות לא מהימנות (רשת ציבורית). קבצים ותיקיות במערכת שלך אינם משותפים עם משתמשים אחרים ואינם גלויים להם ברשת, ושיתוף משאבי מערכת מושבת. אנו ממליצים להשתמש בהגדרה זו בעת גישה לרשתות אלחוטיות. פרופיל זה מוקצה באופן אוטומטי לכל חיבור רשת שאינו מוגדר בתור תחום או רשת פרטית ב-Windows.

בחלק העליון/למעלה/למטה/בחלק התחתון - מאפשר להתאים את רמת העדיפות של פרופילי חיבור רשת (פרופילי חיבור רשת מוערכים ומוחלים לפי העדיפות שלהם. פרופיל ההתאמה הראשון מוחל תמיד).

הוספה או עריכה של פרופיל

פרופיל חיבור רשת מותאם אישית מאפשר להחיל כללי חומת אש ולהגדיר הגדרות נוספות עבור חיבורי רשת ספציפיים. תציין לאילו חיבורי רשת יוקצה הפרופיל המותאם אישית במקטע מפעילים.

כדי לפתוח את עורך הפרופילים, בחלון **פרופילי חיבור רשת**:

- לחץ על **הוספה**.
- בחר אחד מהפרופילים הקיימים ולחץ על **ערוך**.
- בחר אחד מהפרופילים הקיימים ולחץ על **העתק**.

שם - שם מותאם אישית לפרופיל שלך.

תיאור - תיאור הפרופיל כדי לסייע בזיהוי הפרופיל.

כתובות מהימנות נוספות - כתובות שמוגדרות כאן מתווספות לאזור המהימן של חיבור הרשת שעליו מוחל פרופיל זה (ללא תלות בסוג ההגנה של הרשת).

חיבור מהימן - המחשב שלך וקבצים משותפים שמאוחסנים במחשב שלך גלויים למשתמשי רשת אחרים, ומשאבי מערכת נגישים למשתמשים אחרים ברשת (הגישה לקבצים משותפים ולמדפסות מופעלת, תקשורת נכנסת של RPC מופעלת ושיתוף שולחן עבודה מרוחק זמין). מומלץ להשתמש בהגדרה זו בעת יצירת פרופיל עבור חיבור רשת מקומי מאובטח. כל רשתות המשנה המחוברות ישירות נחשבות מהימנות גם הן. לדוגמה, אם מתאם רשת מסוים מחובר לרשת זו עם כתובת ה-IP 192.168.1.5 ומסיכת רשת המשנה 255.255.255.0, רשת המשנה 192.168.1.0/24 מתווספת לאזור המהימן של חיבור הרשת הזה. אם למתאם יש יותר כתובות/רשתות משנה, כולן יהיו מהימנות.

דווח על הצפנת W-Fi חלשה – ESET Smart Security Premium יציג התראת שולחן עבודה כאשר תתחבר לרשת אלחוטית לא מאובטחת או לרשת עם הגנה חלשה.

מפעילים - תנאים מותאמים אישית שיש לעמוד בהם כדי להקצות פרופיל חיבור רשת זה לחיבור רשת. ראה מפעילים להסבר מפורט.

מפעילים

מפעילים הם תנאים מותאמים אישית שיש לעמוד בהם כדי להקצות [פרופיל חיבור רשת](#) ל[חיבור רשת](#). אם לרשת המחוברת יש את אותן תכונות כפי שהוגדרו במפעילים עבור פרופיל רשת מחובר, הפרופיל יחול על הרשת. פרופיל חיבור רשת יכול להכיל מפעיל אחד או כמה מפעילים. אם יש כמה מפעילים, הלוגיקה OR חלה (יש לעמוד בתנאי אחד לפחות). אפשר להגדיר מפעילים [בעורך פרופיל החיבור לרשת](#). יצירת פרופילי חיבור רשת מותאמים אישית צריכה להיעשות על ידי משתמש מנוסה.

המפעילים הבאים זמינים (אם ברצונך לדעת פרטים עבור הרשת הנוכחית שלך, ראה [חיבורי רשת](#)):

[מתאם](#)

סוג מתאם - החל פרופיל אם חיבור הרשת נוצר בסוג המתאם שנבחר.
שם המתאם - החל פרופיל אם שם מתאם הרשת תואם.
מתאם IP - החל פרופיל אם כתובת ה-IP של מתאם הרשת תואמת.

[DNS](#)

סיומת DNS - החל פרופיל אם שם התחום תואם.
DNS IP - החל את הפרופיל אם כתובת ה-IP של שרת DNS תואמת.

[WINS](#)

החל את הפרופיל אם כתובת ה-IP של WINS (Windows Internet Name Service) שמופתה תואמת.

[DHCP](#)

IP של DHCP - התאם את כתובת ה-IP של שרת DHCP.

[שער ברירת מחדל](#)

IP - החל פרופיל אם כתובת ה-IP של שער ברירת המחדל תואמת.
כתובת MAC - החל פרופיל אם כתובת ה-MAC של שער ברירת המחדל תואמת.

[Wi-Fi](#)

SSID - החל פרופיל אם ה-SSID (שם ה-Wi-Fi) תואם.
שם פרופיל - החל פרופיל אם שם פרופיל ה-Wi-Fi תואם.
סוג אבטחה - החל פרופיל אם סוג האבטחה תואם לזה שנבחר מהתפריט הנפתח. (אם אתה רוצה להתאים יותר מאחד, צור מפעיל אחר.)
סוג הצפנה - החל פרופיל אם סוג ההצפנה תואם לזה שנבחר מהתפריט הנפתח. (אם אתה רוצה להתאים יותר מאחד, צור מפעיל אחר.)
אבטחת רשת - החל פרופיל אם הרשת **פתוחה/מאובטחת**.

[פרופיל Windows](#)

החל פרופיל אם הרשת מוגדרת ב-Windows **כתחום/פרטי/ציבורי**.

[אימות](#)

אימות רשת מחפש שרת ספציפי ברשת ומשתמש בהצפנה אסימטרית (RSA) כדי לאמת שרת זה. שם הרשת המאומת חייב להתאים לשם שנקבע בהגדרות שרת האימות. השם הוא תלוי אותיות רישיות. ניתן להקליד את שם השרת ככתובת IP, DNS או שם NetBIOS.

הורד את ESET Authentication Server

ניתן לייבא את המפתח הציבורי באמצעות אחד מסוגי הקבצים הבאים:

- מפתח ציבורי מוצפן של PEM (.pem); באפשרותך ליצור מפתח זה באמצעות שרת האימות של ESET
- מפתח ציבורי מוצפן
- אישור מפתח ציבורי (.crt)

לחץ על **בדיקה** כדי לבדוק את ההגדרות שלך. אם האימות מוצלח, מופיעה הודעה אימות השרת בוצע בהצלחה.

אם האימות לא הוגדר כהלכה, תוצג אחת מהודעות השגיאה הבאות:

אימות השרת נכשל. חתימה לא חוקית או לא תואמת.

חתימת השרת אינה תואמת למפתח הציבורי שהוזן.

אימות השרת נכשל. שם הרשת אינו תואם.

שם הרשת שהוגדר לא תואם לשם הרשת של שרת האימות. בדוק את שני השמות וודא שהם זהים.

אימות השרת נכשל. לא חוקי או שאין תשובה מהשרת.

לא התקבלה תשובה אם השרת אינו פעיל או שלא ניתן לגשת אליו. תשובה בלתי חוקית עשויה להתקבל כאשר שרת HTTP אחר פועל בכתובת שצוינה.

הוזן מפתח ציבורי לא חוקי.

ודא שקובץ המפתח הציבורי שהזנת אינו פגום.

קבוצות של כתובות IP

ערכת IP היא אוסף של כתובות IP שיוצר קבוצה לוגית אחת של כתובות IP, מה שעוזר כשעושים שימוש חוזר באותה קבוצת כתובות בכמה כללי חומת אש או בכללי הגנה מפני מתקפת Brute Force. ESET Smart Security Premium מכיל גם ערכות IP שמוגדרות מראש, שעבורן יש כללים פנימיים. דוגמה אחת לקבוצה כזו היא **אזור מהימן**. אזור מהימן מייצג קבוצה של כתובות רשת שבהן המחשב וקבצים משותפים המאוחסנים במחשב גלויים למשתמשי רשת אחרים, ומשאבי מערכת נגישים למשתמשים אחרים ברשת.

כדי להוסיף ערכת IP:

1. פתח את הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **ערכות IP** > **ערוך**.
2. לחץ על **הוסף**, הקלד **שם** ו**תיאור** עבור האזור, והקלד כתובת IP מרוחקת ב**כתובת מחשב מרוחק (IPv4/IPv6, טווח, מסיכה)**.
3. לחץ על **אישור**.

למידע נוסף, ראה עריכת ערכת IP.

ערוך קבוצות של כתובות IP

למידע נוסף על קבוצות של כתובות IP, ראה קבוצות של כתובות IP.

עמודות

שם שם של קבוצת מחשבים מרוחקים.

תיאור תיאור כללי של הקבוצה.

כתובות IP כתובות IP מרוחקות ששייכות לקבוצה של כתובות IP.

רכיבי בקרה

כשאתה **מוסיף** או **עורך** קבוצה של כתובות IP, השדות הבאים זמינים:

שם שם של קבוצת מחשבים מרוחקים.

תיאור תיאור כללי של הקבוצה.

כתובת מחשב מרוחקת (IPv4, IPv6, טווח, מסיכה) מאפשרת לך להוסיף כתובת מרוחקת, טווח כתובות או רשת משנה.

מחק הסרת אזור מהרשימה.

לא ניתן להסיר קבוצות של כתובות IP שהוגדרו מראש.

דוגמאות לכתובות IP

הוספת כתובת IPv4:
כתובת יחידה - הוספת כתובת IP של מחשב אחד (לדוגמה, *192.168.0.10*).
טווח כתובות הזן את כתובת ה-IP הפותחת והסוגרת כדי לציין את טווח כתובות ה-IP של מספר מחשבים (לדוגמה 192.168.0.1 עד 192.168.0.99).
רשת משנה רשת משנה (קבוצת מחשבים) מוגדרת באמצעות כתובת IP ומסיכה. לדוגמה, 255.255.255.0 היא מסיכת הרשת עבור רשת המשנה 192.168.1.0. כדי לא לכלול את כל הסוג של רשת המשנה ב-*192.168.1.0/24*.
הוספת כתובת IPv6:
כתובת יחידה - הוספת כתובת IP של מחשב בודד (לדוגמה, *2001:718:1c01:16:214:22ff:fec9:ca5*).
רשת משנה רשת משנה (קבוצת מחשבים) מוגדרת באמצעות כתובת IP ומסיכה (לדוגמה: *2002:c0a8:6301:1::1/64*).

מפקח הרשת

התכונה 'מפקח הרשת' יכולה לעזור בזיהוי פגיעויות ברשת מהימנה (רשת ביתית או משרדית) (לדוגמה, יציאות פתוחות או סיסמת נתב חלשה). היא מספקת גם רשימה של ההתקנים המחוברים, עם חלוקה לקטגוריות לפי סוגי ההתקנים (לדוגמה, מדפסת, נתב, מכשיר נייד וכן הלאה), כדי להראות לך מה מחובר לרשת שלך (לדוגמה, קונסולת משחקים, IoT או התקנים אחרים של בית חכם). באפשרותך להגדיר את מפקח הרשת דרך הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **מפקח הרשת**.

הפעל את מפקח הרשת – **'מפקח הרשת'** מסייע בזיהוי פגיעויות ברשת הביתית כגון יציאות פתוחות או סיסמת נתב חלשה. בנוסף, הוא מספק רשימה של התקנים מחוברים, עם חלוקה לקטגוריות לפי סוג ההתקן.

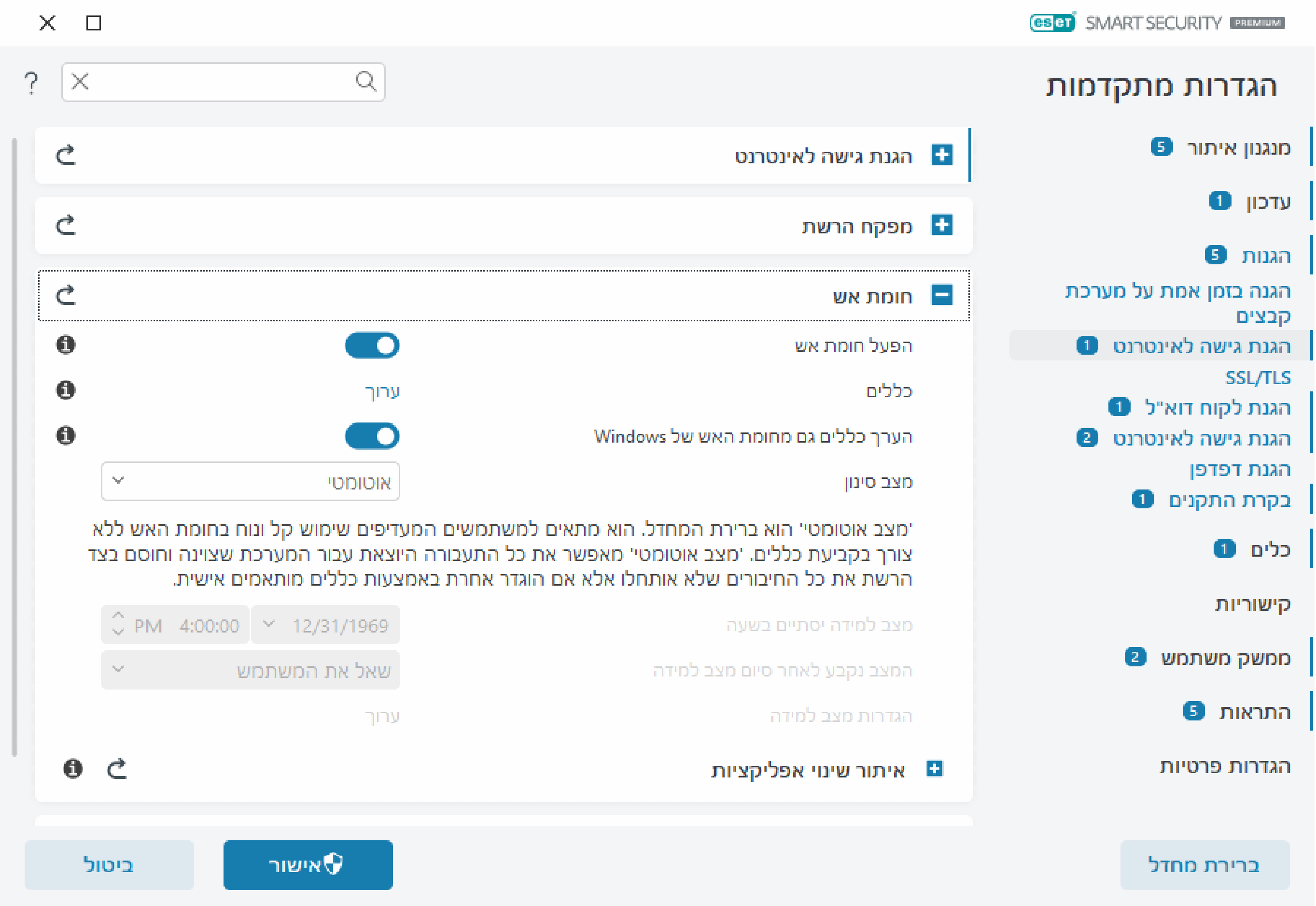
עדכן אודות מכשירי רשת חדשים שזוהו תקבל הודעה כאשר יזוהה מכשיר חדש ברשת שלך.

חומת אש

חומת האש שולטת בכל תעבורת הרשת הנכנסת והיוצאת במחשב שלך, לפי כללים וכללים פנימיים שהוגדרו על ידך. מצב זה מושג על-ידי הפעלה או מניעה של חיבורי רשת יחידים. הוא מספק הגנה מפני התקפות מהתקנים מרוחקים

ומאפשר לחסום שירותים מסוימים שעשויים לאיים.

כדי לקבוע את תצורת חומת האש, פתח את הגדרות מתקדמות < **הגנות** < **הגנת גישה לאינטרנט** < **חומת אש**.



חומת אש

הפעל חומת אש

מומלץ להשאיר תכונה זו במצב פעיל כדי להבטיח את בטיחות המערכת. כאשר חומת האש מופעלת, תעבורת הרשת נסרקת בשני הכיוונים.

כללים

הגדרת כללים מאפשרת לך להציג ולערוך את הכללים של חומת אש שמוחלים על תעבורה שנוצרה על-ידי אפליקציות יחידות באזורים מהימנים ובאינטרנט.

> באפשרותך ליצור כלל IDS כאשר 'מחשב זומבי' (Botnet) תוקף את המחשב שלך. ניתן לשנות כלל בתפריט הגדרות מתקדמות < **הגנות** < **הגנת רשת** < **הגנה מפני מתקפות רשת (IDS)** < **כללי IDS** על-ידי לחיצה על **ערוך**.

הערך כללים גם מחומת האש של Windows

במצב סינון אוטומטי, יש לאפשר גם תעבורה נכנסת המותרת על-ידי כללים מחומת האש של Windows, אלא אם היא נחסמת מפורשות על-ידי הכללים של ESET.

מצב סינון

אופן הפעולה של חומת האש משתנה בהתאם למצב הסינון. מצבי הסינון משפיעים גם על רמת האינטראקציה הנדרשת עם המשתמש.

מצבי הסינון הבאים זמינים בחומת האש של ESET Smart Security Premium:

מצב סינון	תיאור
מצב אוטומטי	מצב ברירת המחדל. מצב זה מתאים למשתמשים שמעדיפים שימוש קל ונוח בחומת האש, ללא הצורך להגדיר כללים. ניתן ליצור כללים מותאמים אישית, המוגדרים על-ידי המשתמש, אולם אלה אינם נדרשים ב**מצב האוטומטי**. המצב האוטומטי מתיר את כל התעבורה היוצאת של מערכת נתונה וחוסם את רוב התעבורה הנכנסת, פרט לחלק מהתעבורה מהאזור המהימן (כמפורט ב-IDS ואפשרויות מתקדמות/שירותים מותרים) ומגיב על תקשורת יוצאת שבוצעה לאחרונה.
מצב אינטראקטיבי	מאפשר לך לבנות תצורה מותאמת אישית עבור חומת האש שלך. כאשר המערכת מזהה תקשורת ולא חלים כללים קיימים על תקשורת זו, מוצג חלון דו-שיח המדווח על חיבור לא מוכר. חלון הדו-שיח מאפשר להתיר או למנוע את התקשורת, ואת ההחלטה אם להתיר או למנוע ניתן לשמור ככלל חדש עבור חומת האש. אם תבחר ליצור כלל חדש, כל החיבורים העתידיים מסוג זה יותרו או ייחסמו, בהתאם לכלל זה.
מצב מבוסס-מדיניות	חוסם את כל החיבורים שאינם מוגדרים על-ידי כלל ספציפי שמתיר אותם. מצב זה מאפשר למשתמשים מתקדמים להגדיר כללים שמתירים רק חיבורים רצויים ומאובטחים. חומת האש תחסום את כל שאר החיבורים שלא צוינו.
מצב למידה	יוצר ושומר כללים באופן אוטומטי; השימוש המיטבי במצב זה הוא הגדרה התחלתית של חומת האש, אולם אין להשאירו פעיל לפרקי זמן ממושכים. אין צורך באינטראקציה עם המשתמש, מפני ש-ESET Smart Security Premium שומר את הכללים בהתאם לפרמטרים שהוגדרו מראש. במצב למידה יש להשתמש רק עד שכל הכללים עבור התקשורת הנדרשת ייווצרו, כדי להימנע מסיכוני אבטחה.

מצב הלמידה יסתיים ב- - קבע תאריך ושעה כאשר מצב הלמידה יסתיים באופן אוטומטי. ניתן גם לכבות את מצב הלמידה באופן ידני מתי שתרצה.

המצב נקבע לאחר סיום מצב למידה הגדר את מצב הסינון שאליו חומת האש של תחזור בתום הזמן שהוקצב למצב הלמידה. מידע נוסף על מצבי סינון נמצא בטבלה שלמעלה. לאחר סיום מצב הלמידה, האפשרות **שאל את המשתמש** תחייב הרשאות ניהול לצורך ביצוע שינוי במצב הסינון של חומת האש.

הגדרות מצב למידה - לחץ על **ערוך** כדי להגדיר פרמטרים לשמירת כללים שנוצרו במצב למידה.

איתור שינוי אפליקציות

תכונת איתור שינוי אפליקציות מציגה התראות כאשר אפליקציות ששונו, אשר עבורן קיים כלל חומת אש, מנסות ליצור חיבורים.

הגדרות מצב למידה

מצב למידה יוצר ושומר כלל אוטומטית עבור כל תקשורת שנוצרה במערכת. אין צורך באינטראקציה עם המשתמש, מפני ש-ESET Smart Security Premium שומר את הכללים בהתאם לפרמטרים שהוגדרו מראש.

מצב זה עשוי לחשוף את המערכת שלך לסיכון, ומומלץ להשתמש בו רק לשם הגדרת התצורה ההתחלתית של חומת האש.

בחר **למידה** בתפריט הנפתח של הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **חומת אש** > **חומת אש** > **מצב סינון** כדי להפעיל את האפשרויות של מצב למידה. לחץ על **עריכה** לצד **הגדרות מצב למידה** כדי לקבוע את התצורה של האפשרויות הבאות:

> במצב למידה חומת האש אינה מסננת את התקשורת. כל התקשורת, הנכנסת והיוצאת, מותרת. במצב זה חומת האש אינה מגנה על המחשב שלך באופן מלא.

תעבורה נכנסת מהאזור המהימן דוגמה לחיבור נכנס באזור המהימן תהיה התקן מרוחק, מתוך האזור המהימן, שמנסה ליצור תקשורת עם אפליקציה מקומית הפועלת במחשב שלך.

- **תעבורה יוצאת מהאזור המהימן** אפליקציה מקומית המנסה ליצור חיבור להתקן אחר ברשת המקומית, או ברשת באזור המהימן.

- **תעבורת אינטרנט נכנסת** התקן מרוחק המנסה להתקשר עם אפליקציה הפועלת במחשב.

- **תעבורת אינטרנט יוצאת** אפליקציה מקומית המנסה ליצור חיבור למחשב אחר.

כל מקטע מאפשר לך להגדיר פרמטרים שיתווספו לכללים חדשים שנוצרו:

הוספת יציאה מקומית כולל את מספר היציאה המקומית של תקשורת הרשת. במקרה של תקשורת יוצאת, לרוב מופקים מספרים אקראיים. מסיבה זו מומלץ להפעיל אפשרות זו רק עבור תקשורת נכנסת.

הוספת יישום כולל את שם היישום המקומי. אפשרות זו מתאימה לכללים עתידיים ברמת היישום (כללים שמגדירים תקשורת עבור יישום שלם). לדוגמה, באפשרותך לאפשר תקשורת רק עבור דפדפן אינטרנט או לקוח דוא"ל.

הוספת יציאה מרוחקת כולל את מספר היציאה המרוחקת של תקשורת הרשת. לדוגמה, באפשרותך להתיר או למנוע שירות ספציפי המשויך למספר יציאה סטנדרטי (HTTP – 80, POP3 – 110, וכו').

הוספת כתובת IP/אזור מהימן מרוחקים כתובת IP או אזור מרוחקים יכולים לשמש כפרמטר לכללים חדשים המגדירים את כל חיבורי הרשת בין המערכת המקומית לבין אותם כתובת/אזור מרוחקים. אפשרות זו מתאימה כאשר ברצונך להגדיר פעולות עבור התקן מסוים או קבוצת התקנים המחוברים ברשת.

מספר מרבי של כללים שונים ליישום אם יישום מסוים מנהל תקשורת דרך יציאות שונות לכתובות IP שונות, וכו', חומת האש במצב למידה יוצרת ספירה מתאימה של כללים עבור יישום זה. עם אפשרות זו אתה יכול להגביל את מספר הכללים שניתן ליצור עבור יישום אחד.

כללים של חומת אש

כללים הם מערכת תנאים שבהם נעשה שימוש כדי לבדוק באופן משמעותי את כל חיבורי הרשת ואת כל הפעולות שהוקצו עבור תנאים אלה. באמצעות כללים של חומת אש באפשרותך להגדיר את הפעולה שתינקט כאשר נוצרים סוגים שונים של חיבורי רשת.

מבוצעת הערכה של הכללים מלמעלה למטה ואפשר לראות את העדיפות שלהם בעמודה הראשונה. הפעולה של כלל ההתאמה הראשון נמצאת בשימוש עבור כל חיבור רשת שמוערך.

את החיבורים ניתן לחלק לנכנסים ויוצאים. את החיבורים הנכנסים יוזם התקן מרוחק המנסה ליצור חיבור למערכת המקומית. החיבורים היוצאים פועלים בכיוון ההפוך המערכת המקומית יוצרת קשר עם התקן מרוחק.

אם מזוהה תקשורת חדשה ובלתי מוכרת, עליך לשקול היטב אם להתיר או למנוע אותה. חיבורים שלא התבקשו, שאינם בטוחים או שאינם מכירים מהווים סיכון אבטחה למערכת. אם נוצר חיבור כזה, מומלץ לשים לב להתקן המרוחק ולאפליקציה המנסה להתחבר למחשב שלך. חדירות רבות מנסות להשיג ולשלוח נתונים פרטיים, או להוריד יישומים זדוניים אחרים לתחנות עבודה מארחות. חומת האש מאפשרת לך לזהות ולעצור חיבורים כאלה.

אפשר להציג ולערוך כללי חומת אש דרך הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **חומת אש** > **כללים** > **ערוך**.

אם יש לך כללי חומת אש רבים, באפשרותך להשתמש במסנן כדי להציג רק כללים ספציפיים. כדי לסנן כללי חומת אש, לחץ על **מסננים נוספים** מעל לרשימה של כללי חומת אש. ניתן לסנן את הכללים לפי הקריטריונים הבאים:

- מקור
- כיוון
- פעולה
- זמינות

כברירת מחדל, כללי חומת האש שהוגדרו מראש מוסתרים. כדי להציג את כל הכללים שהוגדרו מראש, השבת את המתג שליד **הסתר כללים מובנים (מוגדרים מראש)**. באפשרותך להשבית כללים אלה, אולם לא תוכל למחוק כלל שהוגדר מראש.

> לחץ על סמל החיפוש בפינה השמאלית העליונה כדי לחפש את הכללים.

עמודות

עדיפות - ההערכה של הכללים מבוצעת מלמעלה למטה ואפשר לראות את העדיפות שלהם בעמודה הראשונה.

מופעל אפשרות זו מציגה אם הכללים מופעלים או מושבתים. כדי להפעיל כלל יש לסמן את תיבת הסימון המתאימה.

אפליקציה היישום שעליו יחול הכלל.

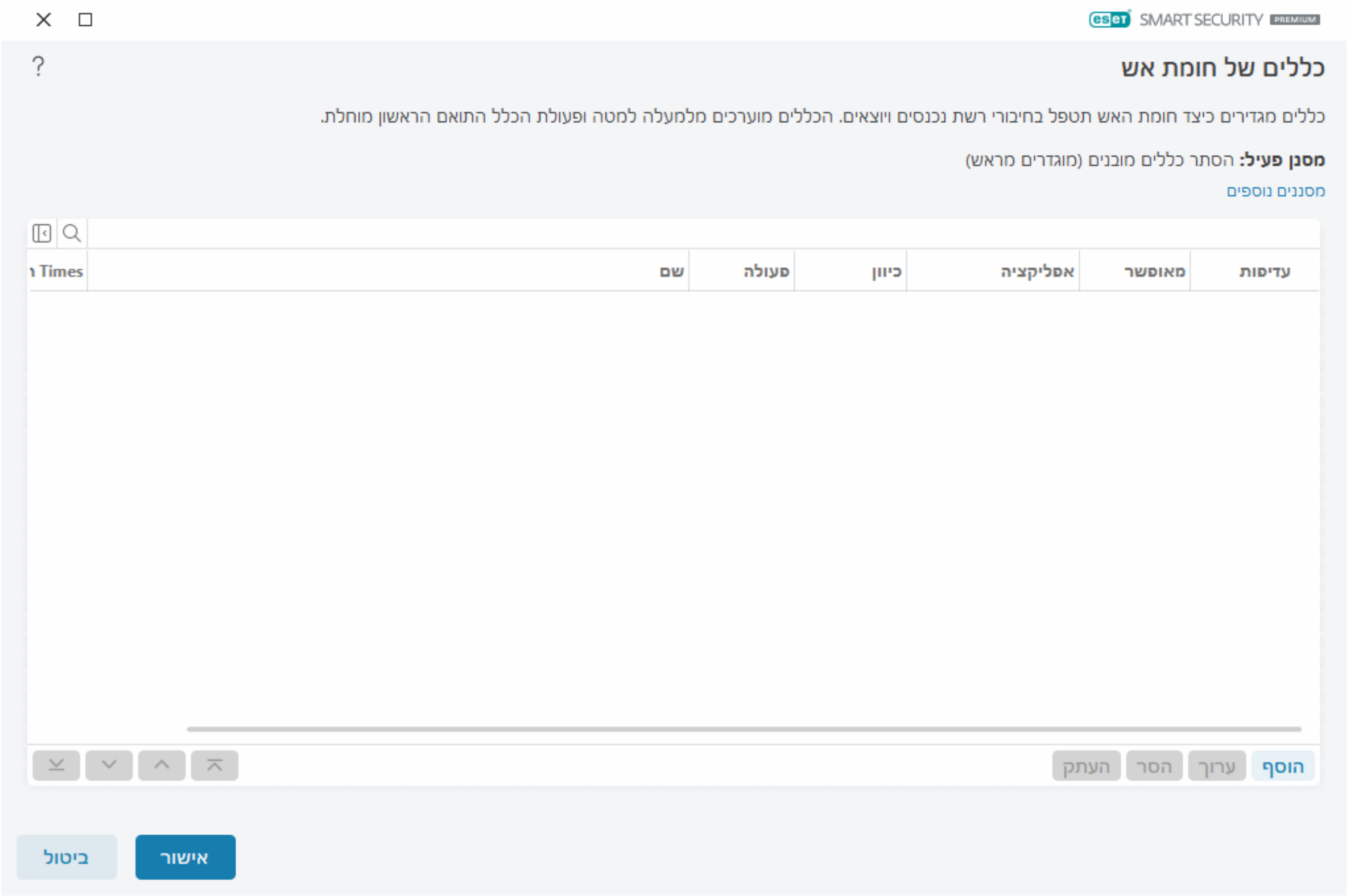
כיוון כיוון התקשורת (נכנסת/יוצאת/גם וגם).

פעולה הצגת סטטוס התקשורת (חסומה/מותרת/הצגת שאלה).

שם שם הכלל. סמל ESET מייצג כלל מוגדר מראש.

פעמים שהוחלו - מספר הפעמים הכולל שבהן הכלל הוחל.

לחץ על סמל ההרחבה כדי להציג את פרטי הכלל.



רכיבי בקרה

הוסף – יצירת כלל חדש.

ערוך – ערוך כלל קיים.

מחק הסר כלל קיים.

העתק צור עותק של כלל שנבחר.

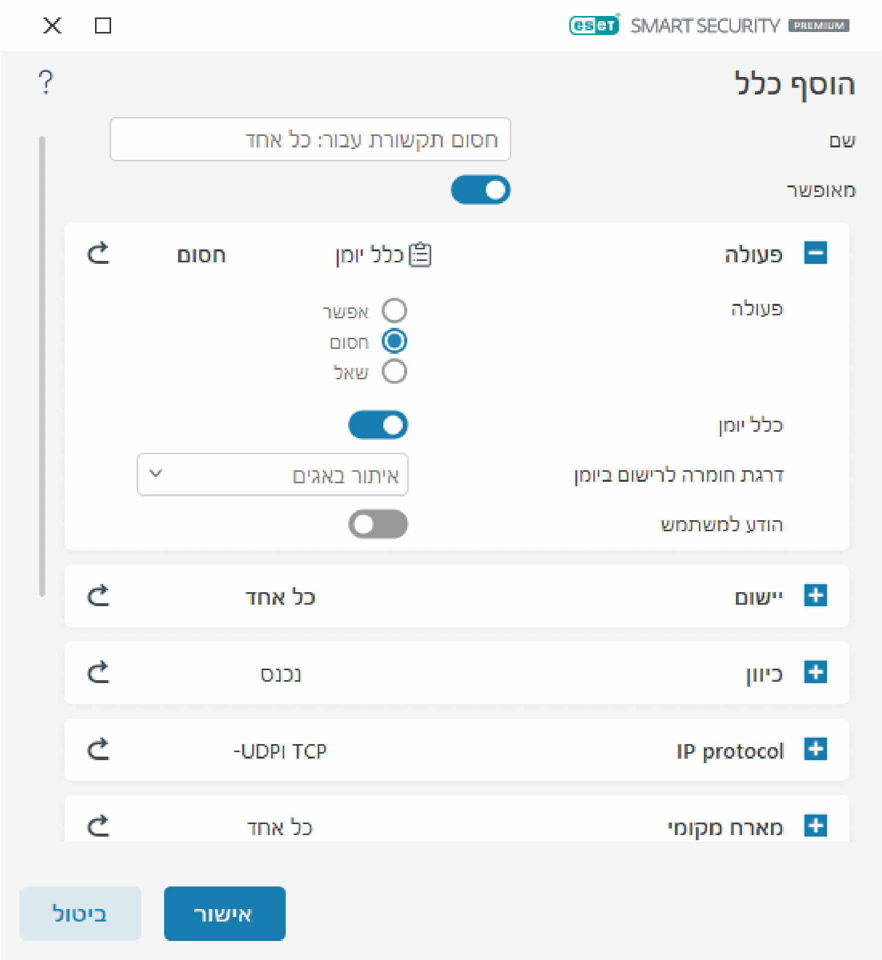
עליון/מעלה/מטה/תחתון מאפשר לך להתאים את רמת העדיפות של הכללים (הפעלת הכללים מתבצעת מלמעלה למטה).

הוספה או עריכה של כללי חומת אש

כללי חומת אש מייצגים תנאים שבהם נעשה שימוש כדי לבדוק באופן משמעותי את כל חיבורי הרשת והפעולות שהוקצו לתנאים אלה. עריכה או הוספה של כללי חומת אש עשויות להידרש במקרה של שינוי הגדרות הרשת (לדוגמה, כתובת הרשת או מספר היציאה של הצד המרוחק השתנו) כדי להבטיח את פעולתה התקינה של אפליקציה המושפעת מכלל. משתמש מנוסה צריך ליצור כללי חומת אש מותאמים אישית.

> **הנחיות מאוירות**
>
> מאמר מאגר הידע הבא של ESET עשוי להיות זמין באנגלית בלבד:
> - פתח או סגור (אפשר או דחה) יציאה ספציפית באמצעות חומת אש
> - צור כלל חומת אש מרשומות היומן ב-ESET Smart Security Premium

כדי להוסיף או לערוך כלל חומת אש, פתח את הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **חומת אש** > **כללים** > **ערוך**. בחלון כללי חומת אש, לחץ על **הוסף** או **ערוך**.



שם - הקלד שם עבור הכלל.

מופעל - לחץ על המתג כדי להפוך את הכלל לפעיל.

הוסף פעולות ותנאים עבור כלל חומת אש:

פעולה

פעולה - בחר אם ברצונך **להתיר/לחסום** את התקשורת התואמת לתנאים שהוגדרו בכלל זה או אם ברצונך ש-ESET Smart Security Premium **ישאל** בכל פעם שיש תקשורת.
כלל יומן רישום - אם הכלל מוחל, הוא יתועד בקובצי יומן רישום.
דרגת חומרה לרישום ביומן - בחר את דרגת החומרה לרישום ביומן עבור כלל זה.
האפשרות **הודע למשתמש** מציגה התראה כאשר הכלל מוחל.

יישום

ציין אפליקציה שבה יחול כלל זה.
נתיב אפליקציה - לחץ על **...** ועבור לאפליקציה או הקלד את הנתיב המלא של האפליקציה (לדוגמה C:\Program Files\Firefox\Firefox.exe). אל תקליד רק את שם האפליקציה.
חתימת אפליקציה - באפשרותך להחיל את הכלל על אפליקציות לפי החתימות שלהן (שם המפרסם). בחר מהתפריט הנפתח אם ברצונך להחיל את הכלל על אפליקציות עם **חתימה חוקית כלשהי** או על אפליקציות **שנחתמו על ידי חותם מסוים**. אם תבחר אפליקציות **שנחתמו על-ידי חותם מסוים**, עליך להגדיר את החותם בשדה **שם החותם**.
אפליקציה ב-Microsoft Store - בחר אפליקציה שמותקנת מתוך Microsoft Store בתפריט הנפתח.
שירות - באפשרותך לבחור שירות מערכת במקום אפליקציה. פתח את התפריט הנפתח כדי לבחור שירות.
החל על תהליכי צאצא - אפליקציות מסוימות עשויות להפעיל תהליכים נוספים למרות שאתה רואה רק חלון אפליקציה אחד. לחץ על המתג כדי לאפשר את הכלל עבור כל תהליך באפליקציה שצוינה.

כיוון

בחר את **כיוון** התקשורת עבור כלל זה:
- **שניהם** - תקשורת נכנסת ויוצאת
- **נכנסת** - תקשורת נכנסת בלבד
- **יוצאת** - תקשורת יוצאת בלבד

פרוטוקול IP

בחר **פרוטוקול** מהתפריט הנפתח אם ברצונך שכלל זה יחול רק על פרוטוקול מסוים.

מארח מקומי

כתובות מקומיות, טווח כתובות או רשת משנה שעליהן חל כלל זה. אם לא צוינה כתובת, הכלל יחול על כל התקשורת עם המארחים המקומיים. באפשרותך להוסיף כתובות IP, טווחי כתובות או רשתות משנה ישירות לשדה הטקסט של ה-**IP** או לבחור מתוך קבוצות של כתובות IP קיימות על ידי לחיצה על **ערוך** לצד **קבוצות של כתובות IP**.

יציאה מקומית

יציאה - מספרי היציאות המקומיות. אם לא צוינו מספרים, הכלל יחול על כל היציאות. הוסף יציאת תקשורת יחידה או טווח יציאות תקשורת.

מארח מרוחק

כתובת מרוחקת, טווח כתובות או רשת משנה שעליהן חל כלל זה. אם לא צוינה כתובת, הכלל יחול על כל התקשורת עם מארחים מרוחקים. באפשרותך להוסיף כתובות IP, טווחי כתובות או רשתות משנה ישירות לשדה הטקסט של ה-**IP** או לבחור מתוך קבוצות של כתובות IP קיימות על ידי לחיצה על **ערוך** לצד **קבוצות של כתובות IP**.

יציאה מרוחקת

יציאה ⍰ מספרי היציאות המרוחקות. אם לא צוינו מספרים, הכלל יחול על כל היציאות. הוסף יציאת תקשורת יחידה או טווח יציאות תקשורת.

פרופיל

ניתן להחיל כלל חומת אש על [פרופילים ספציפיים של חיבור רשת](#).
כל אחד - הכלל יחול על כל חיבור רשת, בלי קשר לפרופיל שבו נעשה שימוש.
נבחר - הכלל יחול על חיבור רשת מסוים, לפי הפרופיל שנבחר. בחר בתיבת הסימון לצד הפרופילים שברצונך לבחור.

אנו יוצרים כלל חדש כדי לאפשר לאפליקציית דפדפן האינטרנט Firefox לגשת ל / לאתרי אינטרנט ברשת המקומית.

1. במקטע **פעולה**, בחר **פעולה** > **אפשר**.
2. במקטע **אפליקציה**, ציין את **נתיב האפליקציה** של דפדפן האינטרנט (לדוגמה C:\Program Files\Firefox\Firefox.exe). אל תקליד רק את שם האפליקציה.
3. במקטע **כיוון**, בחר **כיוון** > **יציאה**.
4. במקטע **פרוטוקול IP**, בחר **TCP & UDP** מהתפריט הנפתח **פרוטוקול**.
5. במקטע **יציאה מרוחקת**, הוסף מספרי **יציאות**: *80,443* כדי לאפשר גלישה רגילה.

איתור שינוי אפליקציות

תכונת איתור השינויים באפליקציות מציגה התראות כאשר אפליקציות ששונו, אשר עבורן קיים כלל חומת אש, מנסות ליצור חיבורים. איתור השינויים באפליקציות הוא מנגנון להחלפה זמנית או קבועה של קובץ ההפעלה של האפליקציה המקורית בקובץ ההפעלה של אפליקציה אחרת (הוא מגן מפני שימוש לרעה בכללים של חומת האש).

קח בחשבון שתכונה זו אינה מיועדת לאיתור שינויים ביישום כלשהו באופן כללי. המטרה היא להימנע משימוש לרעה בכללי חומת אש קיימים, ורק יישומים שעבורם קיימים כללי חומת אש ספציפיים נמצאים בפיקוח.

כדי לערוך **איתור שינויים באפליקציות**, פתח את [הגדרות מתקדמות](#) > **הגנות** > **הגנת גישה לאינטרנט** > **חומת אש** > **איתור שינויים באפליקציות**.

הפעל זיהוי שינויים ביישומים אם אפשרות זו נבחרת, התוכנית מנטרת שינויים (עדכונים, הדבקות, שינויים אחרים ביישומים. כאשר יישום ששונה מנסה להתחבר, תקבל הודעה מחומת האש.

אפשר שינוי של יישומים חתומים (מהימנים) אל תודיע אם החתימה הדיגיטלית החוקית של היישום לפני ואחרי השינוי נותרה ללא שינוי.

רשימת אפליקציות שלא ייכללו באיתור חלון זה מאפשר לך להוסיף או להסיר אפליקציות בודדות שעבורן מותרים שינויים ללא התראה.

רשימת אפליקציות שאינן כלולות באיתור

חומת האש ב-ESET Smart Security Premium מאתרת שינויים באפליקציות שעבורן קיימים כללים (ראה [איתור שינוי אפליקציות](#)).

במקרים מסוימים ייתכן שלא תרצה להשתמש בפונקציונליות זו עבור חלק מהיישומים, ושתעדיף לא לכלול אותם בבדיקה שמבצעת חומת האש.

הוספה פתיחת חלון שבו באפשרותך לבחור אפליקציה להוספה לרשימת האפליקציות שלא ייכללו באיתור השינויים. ניתן לבחור מתוך רשימה של אפליקציות פועלות עם תקשורת רשת פתוחה שעבורן קיים כלל חומת אש, או להוסיף אפליקציה ספציפית.

עריכה פתיחת חלון שבו באפשרותך לשנות את המיקום של אפליקציה שנמצאת ברשימת האפליקציות שלא ייכללו

באיתור השינויים. ניתן לבחור מתוך רשימה של אפליקציות פועלות עם תקשורת רשת פתוחה שעבורן קיים כלל חומת אש, או לשנות את המיקום ידנית.

הסר הסרת ערכים מרשימת היישומים שלא ייכללו בזיהוי השינויים.

הגנה מפני מתקפות רשת (IDS)

'הגנה מפני מתקפות רשת (IDS)' משפרת את האיתור של מקרי ניצול לרעה עבור פגיעויות מוכרות. קרא עוד על הגנה מפני מתקפות רשת במילון. כדי להגדיר הגנה מפני מתקפות רשת (IDS), פתח את הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **הגנה מפני מתקפות רשת (IDS)**.

אפשר הגנה מפני מתקפות רשת (IDS) ניתוח התוכן של תעבורת רשת והגנה מפני מתקפות רשת. כל תעבורה שנחשבת מזיקה תיחסם.

הפעלת הגנה מפני מחשב 'זומבי' (Botnet) זיהוי וחסימת תקשורת עם שרתי פקודה ובקרה זדוניים על סמך דפוסים טיפוסיים כאשר המחשב נדבק ומחשב בוט מנסה לתקשר. קרא עוד על הגנה מפני מחשב 'זומבי' (Botnet) במילון.

כללי IDS - מאפשרים לקבוע את התצורה של אפשרויות סינון מתקדמות כדי לזהות סוגים מסוימים של מתקפות וניצול לרעה שעלולים לפגוע במחשב שלך.

> הנחיות מאוירות
> מאמר מאגר הידע הבא של ESET עשוי להיות זמין באנגלית בלבד:
> • אל תכלול כתובת IP מ-IDS ב-ESET Smart Security Premium

כל האירועים החשובים המאותרים על ידי הגנת רשת נשמרים בקובץ יומן. ראה יומן הגנת רשת למידע נוסף.

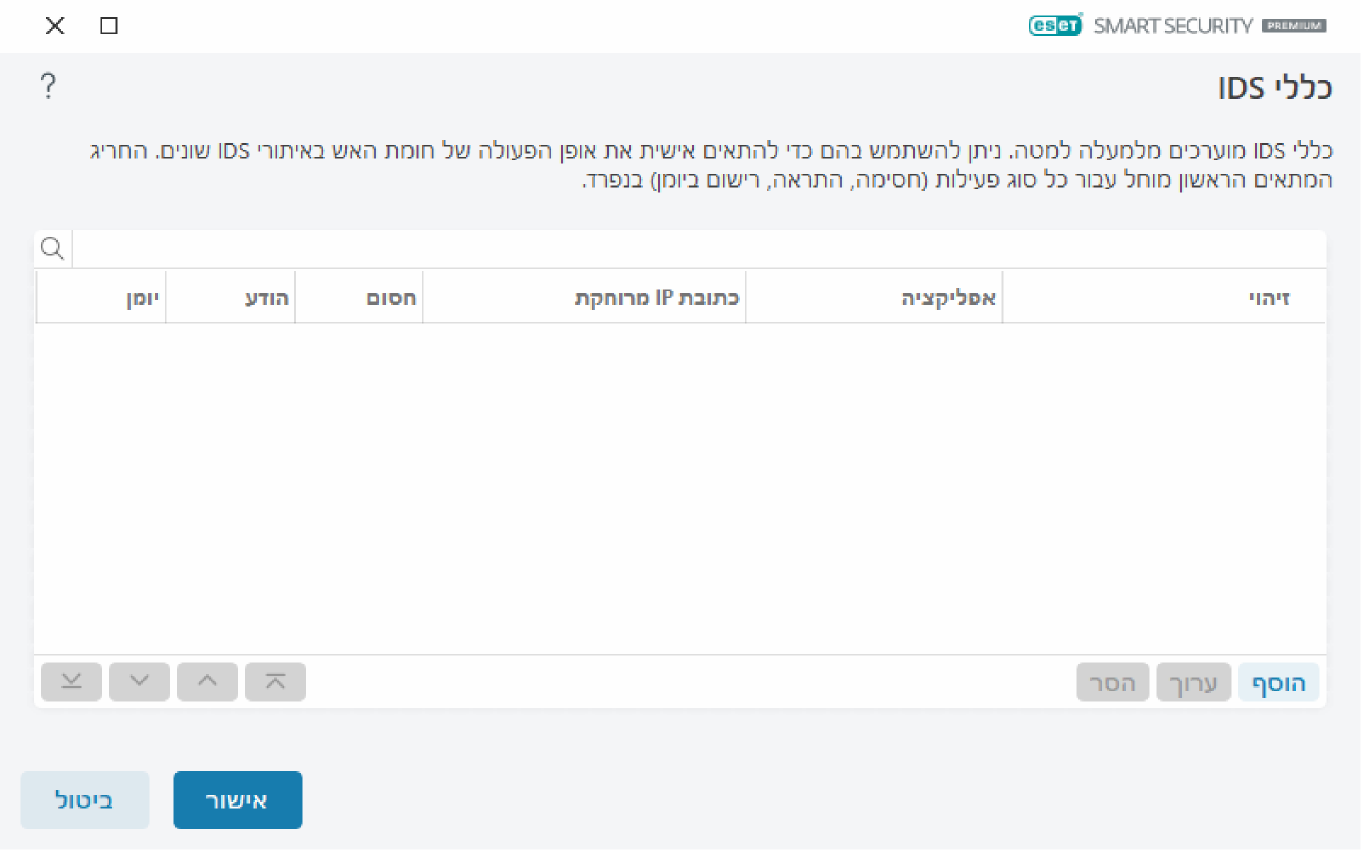
כללי IDS

במצבים מסוימים, שירות איתור חדירה (IDS) עשוי לאתר תקשורת בין נתבים או מכשירים אחרים של רשת פנימית כמתקפה פוטנציאלית. לדוגמה, ניתן להוסיף את הכתובת הבטוחה הידועה לכתובות שאינן נכללות באזור IDS כדי לעקוף את ה-IDS.

> הנחיות מאוירות
> מאמר מאגר הידע הבא של ESET עשוי להיות זמין באנגלית בלבד:
> • אל תכלול כתובת IP מ-IDS ב-ESET Smart Security Premium

ניהול כללי IDS

- **הוסף** לחץ כדי ליצור חריגות של IDS חדשת.
- **ערוך** לחץ כדי לערוך חריגות של IDS קיימת.
- **הסר** בחר ולחץ אם ברצונך להסיר כלל מהרשימה של חריגות של IDS.
- **בחלק העליון/למעלה/למטה/בחלק התחתון** - התאם את רמת העדיפות של הכללים (חריגים מוערכים מלמעלה למטה).



עורך כללים

איתור – סוג האיתור.

שם איום - אפשר לציין את שם האיום עבור חלק מהאיתורים הזמינים.

אפליקציה – בחר את נתיב הקובץ של אפליקציה שלא נכללה על ידי לחיצה על ... (לדוגמה *C:\Program Files\Firefox\Firefox.exe*). אל תקליד את שם האפליקציה.

כתובת IP מרוחקת – רשימת כתובות IPv4 או IPv6 מרוחקות/טווחים/רשתות משנה. יש להפריד כתובות מרובות באמצעות פסיק.

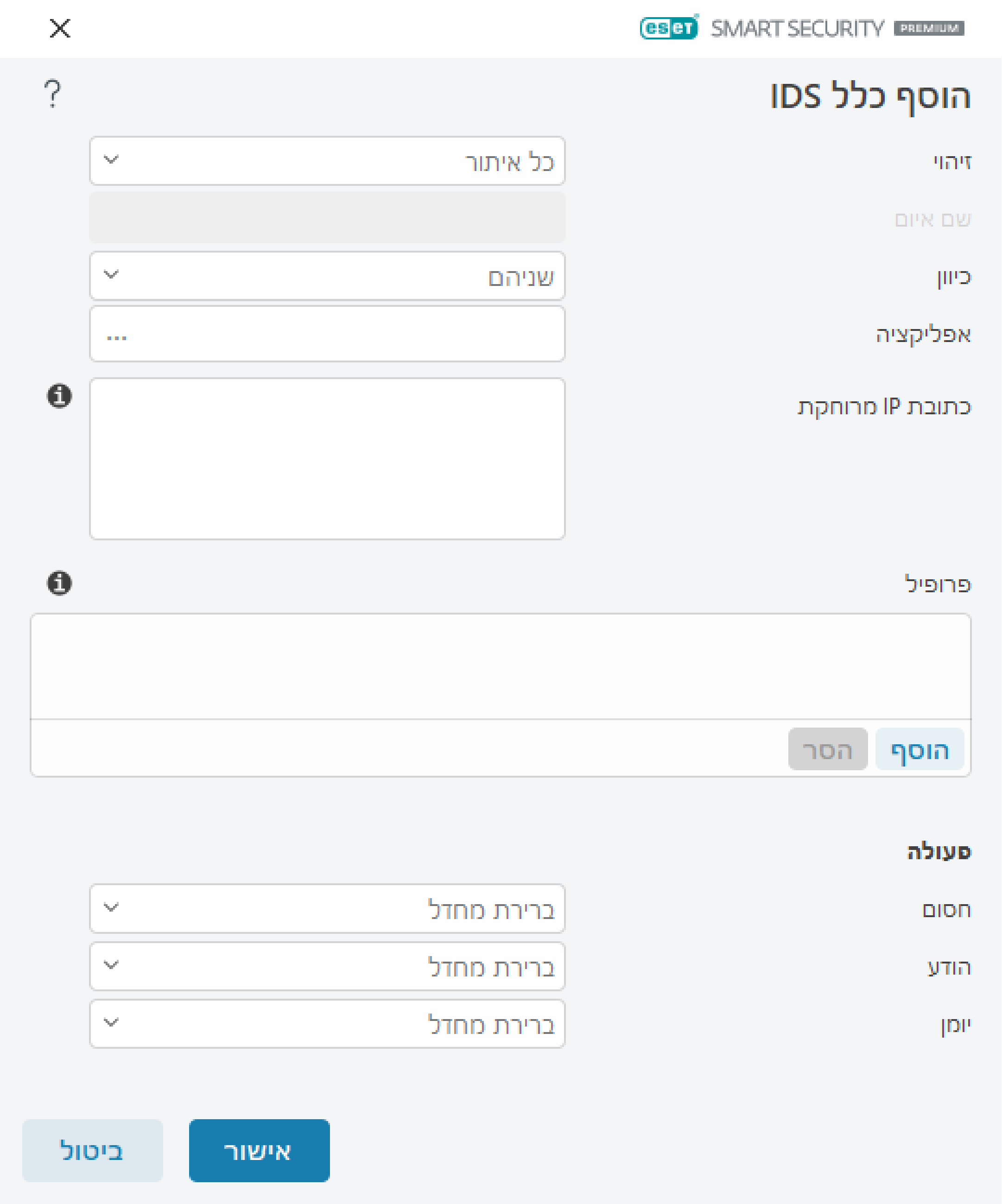
פרופיל - אפשר לבחור פרופיל חיבור רשת שעליו יחול כלל זה.

פעולה

חסימה – לכל תהליך במערכת יש אופן פעילות ופעולה מוקצית שהוגדרו כברירת מחדל עבורו (חסימה או התרה). כדי לשנות את אופן הפעולה שנקבע כברירת מחדל עבור ESET Smart Security Premium, ניתן לבחור באפשרויות החסימה או ההפעלה בתפריט הנפתח.

הודע - בחר 'כן' כדי להציג התראות בשולחן העבודה במחשב שלך. בחר 'לא' אם אינך מעוניין לקבל התראות בשולחן העבודה. הערכים הזמינים הם ברירת מחדל/כן/לא.

יומן רישום - בחר **כן** כדי לרשום אירועים ברשומות יומן. בחר **לא** אם אינך מעוניין לרשום אירועים. הערכים הזמינים הם **ברירת מחדל/כן/לא**.



אם ברצונך להציג התראה ולאסוף יומן בכל פעם שהאירוע מתרחש:

1. לחץ על **הוסף** כדי להוסיף כלל IDS חדש.
2. בחר איתור ספציפי מהתפריט הנפתח **איתור**.
3. בחר נתיב אפליקציה על-ידי לחיצה על **...** שעבורו ברצונך להחיל התראה זו.
4. השאר את האפשרות **ברירת מחדל** בתפריט הנפתח **חסימה**. הדבר יגרום לירושה של פעולת ברירת המחדל שמחיל ESET Smart Security Premium.
5. הגדר את שני התפריטים הנפתחים **הצגת התראה** ו**יומן** ל**כן**.
6. לחץ על **אישור** כדי לשמור התראה זו.

אם אינך רוצה להציג התראה חוזרת שאינך מחשיב כאיום עבור סוג מסוים של **איתור**:

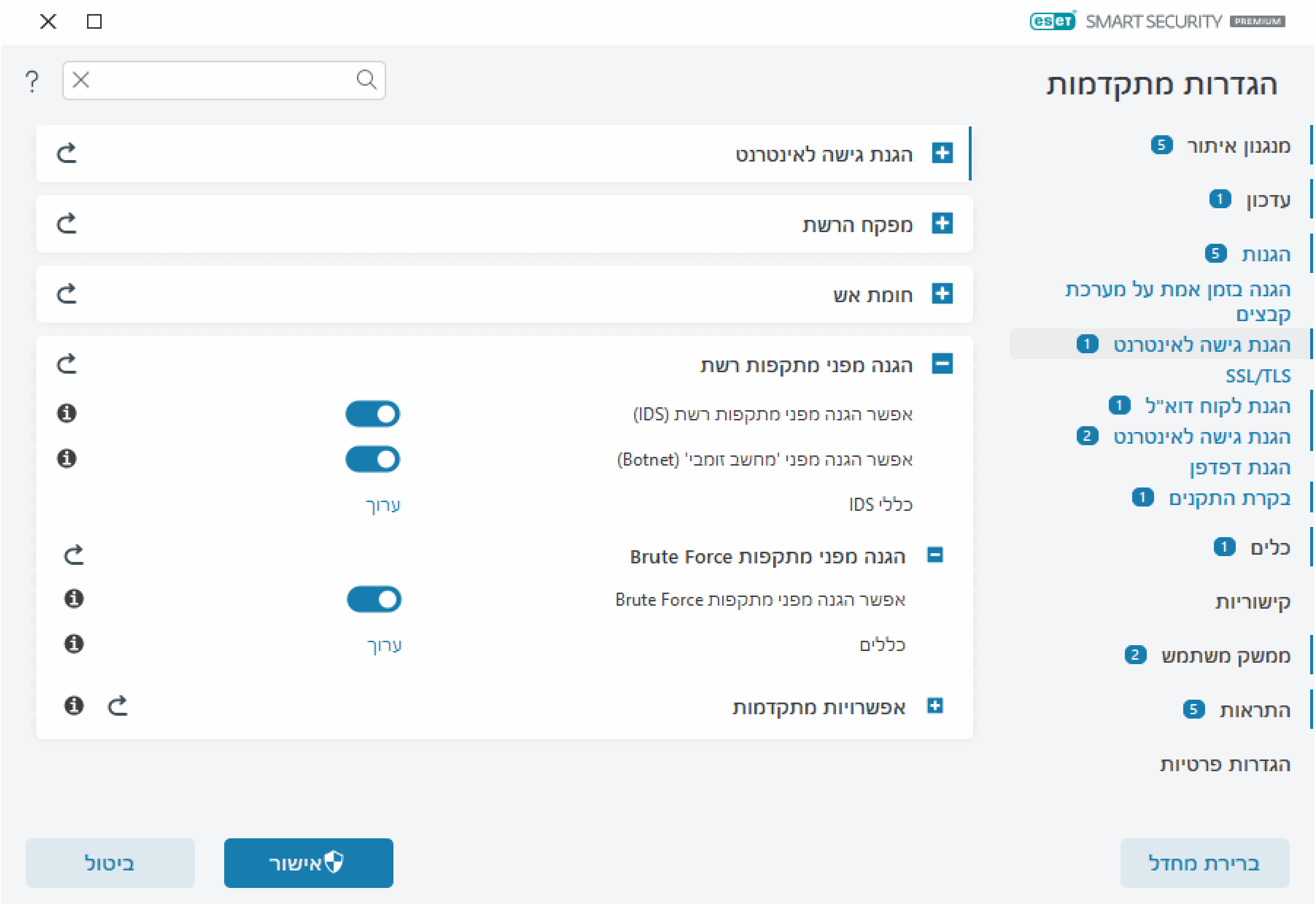
1. לחץ על **הוסף** כדי להוסיף כלל IDS חדש.
2. בחר איתור ספציפי מהתפריט הנפתח **איתור**, לדוגמה **הפעלת SMB ללא הרחבות אבטחה** או **מתקפה של סריקת יציאי TCP**.
3. בחר **פנימה** מהתפריט הנפתח של הכיוון במקרה שמדובר בתקשורת נכנסת.
4. הגדר את התפריט הנפתח **הצגת התראה** ללא.
5. הגדר את התפריט הנפתח **יומן** לכן.
6. השאר את **אפליקציה** ריק.
7. אם התקשורת לא מגיעה מכתובת IP מסוימת, השאר את **כתובות IP מרוחקות** ריק.
8. לחץ על **אישור** כדי לשמור התראה זו.

הגנה מפני מתקפות Brute Force

המערכת להגנה מפני מתקפות Brute Force חוסמת מתקפות של ניחוש סיסמה עבור שירותי RDP ו-SMB. מתקפת Brute Force היא שיטה לגילוי סיסמה ייעודית על ידי ניסוי שיטתי של כל שילובי האותיות, המספרים והסמלים. כדי להגדיר את ההגנה מפני מתקפת Brute Force, פתח את הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **הגנה מפני מתקפות רשת** > **הגנה מפני מתקפות Brute Force**.

אפשר הגנה מפני מתקפות ESET Smart Security Premium – **Brute Force** בודק את תעבורת הרשת וחוסם את הניסיונות של מתקפות ניחוש סיסמה.

כללים ⍰ מאפשרים לך ליצור, לערוך ולהציג כללים עבור חיבורי רשת נכנסים ויוצאים. למידע נוסף, עיין במקטע כללים.



כללים

הכללים של המערכת להגנה מפני מתקפות Brute Force מאפשרים לך ליצור, לערוך ולהציג כללים עבור חיבורי רשת נכנסים ויוצאים. לא ניתן לערוך או להסיר את הכללים המוגדרים מראש.

ניהול הכללים להגנה מפני מתקפות Brute Force

הוסף יצירת כלל חדש.

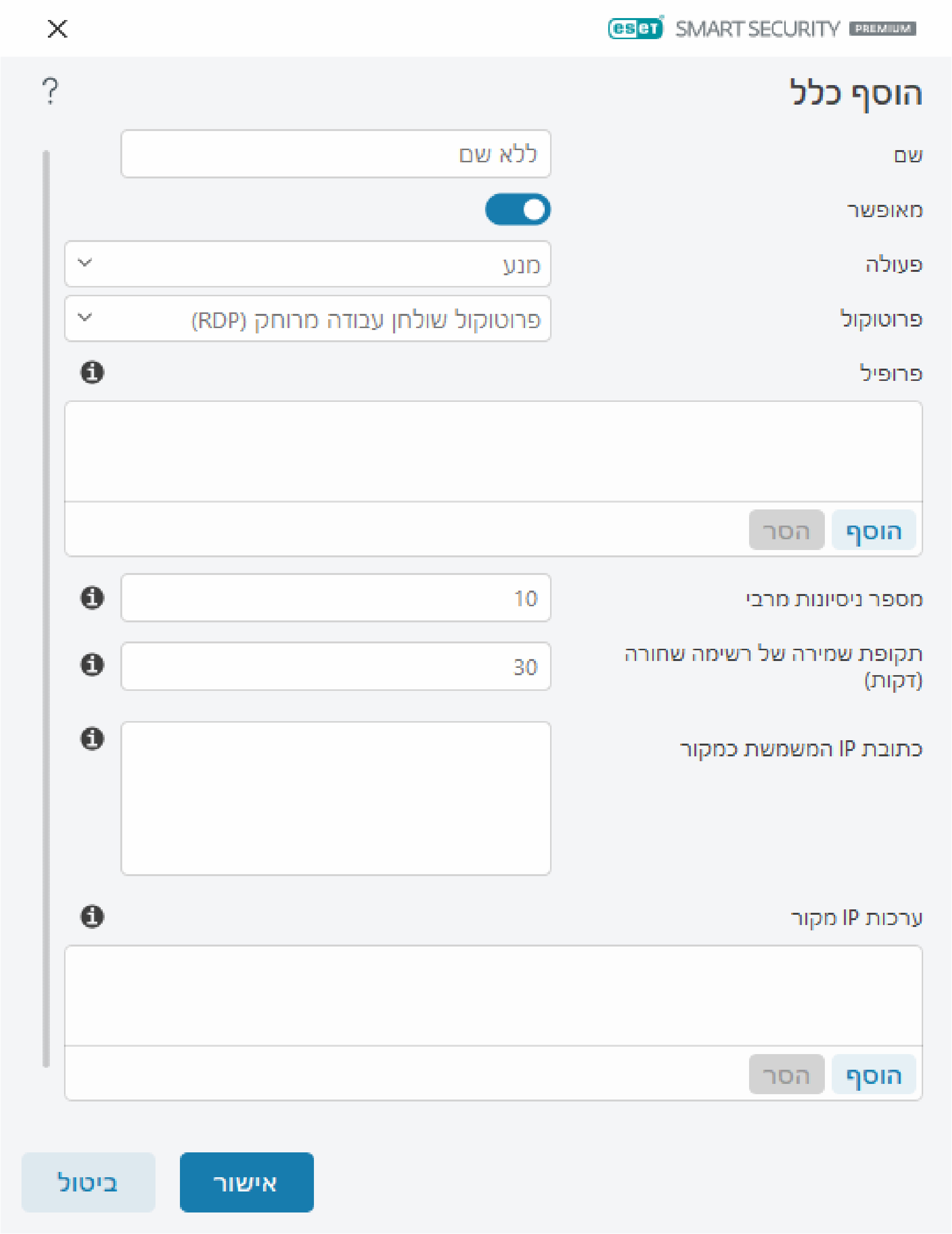
ערוך ערוך כלל קיים.

הסר הסר כלל קיים מרשימת הכללים.

עליון/מעלה/מטה/תחתון התאם את רמת העדיפות של הכללים.

> כדי להבטיח את רמת ההגנה הגבוהה ביותר, כלל החסימה עם ערך **מספר הניסיונות המרבי** הנמוך ביותר חל גם אם הכלל ממוקם נמוך יותר ברשימת הכללים כשכללי חסימה מרובים תואמים לתנאי האיתור.

עורך כללים



שם שם הכלל.

מופעל כבה את המתג אם ברצונך להשאיר את הכלל ברשימה מבלי להחילו.

פעולה בחר אם **למנוע** או **לאפשר** את החיבור אם הגדרות הכלל מתקיימות.

פרוטוקול פרוטוקול התקשורת שכלל זה יבדוק.

פרופיל ניתן להגדיר ולהחיל כללים מותאמים אישית על פרופילים ספציפיים.

מספר ניסיונות מרבי המספר המרבי של הניסיונות המותרים לחזרה על מתקפה עד לחסימה של כתובת ה-IP ולהוספתה לרשימה השחורה.

תקופת שמירה של רשימה שחורה (דקות) קובע את השעה לתפוגת התוקף של הכתובת ברשימה השחורה.

כתובת IP המשמשת כמקור רשימה של כתובות IP/טווחים/רשתות משנה. יש להפריד כתובות מרובות באמצעות פסיק.

קבוצות של כתובות IP של מקור - קבוצה של כתובות IP שכבר הגדרת דרך קבוצות של כתובות IP.

אפשרויות מתקדמות

דרך הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **הגנה מפני מתקפות רשת** > **אפשרויות מתקדמות**, אפשר להפעיל או לבטל איתור סוגים שונים של מתקפות וניצול לרעה שעלולים לפגוע במחשב שלך.

במקרים מסוימים לא תקבל הודעת איום על תקשורת חסומה. עיין במקטע רישום ויצירת כללים או חריגות ביומן לקבלת הוראות להצגת כל התקשורת החסומה ביומן חומת האש.

הזמינות של אפשרויות מסוימות בחלון זה עשויה להשתנות בתלות בסוג או בגרסה של מוצר ESET ומודול חומת האש שברשותך, וכן בגרסת מערכת ההפעלה שלך.

זיהוי פריצות

איתור חדירה מנטר את תקשורת ההתקנים ברשת לאיתור פעילות זדונית.

- **פרוטוקול SMB** – זיהוי וחסימה של בעיות אבטחה שונות בפרוטוקול SMB.
- **פרוטוקול RPC** – זיהוי וחסימה של פגיעויות CVE שונות במערכת הקריאה לפרוצדורה המרוחקת שפותחה עבור סביבת מחשוב מבוזרת (DCE).
- **פרוטוקול RDP** – זיהוי וחסימה של פגיעויות CVE שונות בפרוטוקול RDP (ראה לעיל).
- **זיהוי מתקפת הרעלת ARP** – זיהוי מתקפת הרעלת ARP המופעלות על-ידי אדם במתקפות התווך או זיהוי איומים במתג הרשת. ARP (פרוטוקול זיהוי כתובת) משמש את התקן או יישום הרשת לקביעת כתובת ה-Ethernet.
- **זיהוי התקפה של סריקת יציאת TCP/UDP**– זיהוי התקפות של תוכנת סריקת יציאות – יישום שתוכנן לחקור יציאות פתוחות במארח על-ידי שליחת בקשות לקוח לכתובות יציאות שונות במטרה לאתר יציאות פעילות ולנצל את פגיעויות השירות. קרא עוד על סוג המתקפה הזה במילון.
- **חסימת כתובת לא בטוחה לאחר זיהוי התקפה** – כתובות IP שזוהו כמקורות התקפה מתווספות לרשימה השחורה כדי למנוע חיבור לפרק זמן מסוים. באפשרותך להגדיר **תקופת שמירה של רשימה שחורה**, אשר קובעת למשך כמה זמן הכתובת תיחסם לאחר איתור מתקפה.
- **הצג התראות אודות איתור מתקפות** – בחר באפשרות זו כדי להפעיל הצגת התראות באזור ההודעות של Windows בפינה השמאלית התחתונה של המסך.
- **הצגת הודעות גם עבור התקפות נכנסות נגד פרצות אבטחה** – במקרה של זיהוי התקפות נגד פרצות אבטחה, או כשאיום מסוים מנסה להיכנס למערכת בדרך זו.

בדיקת מנות

זהו סוג של ניתוח מנות המסנן נתונים שעוברים ברשת.

- **אפשר חיבור נכנס לשיתופי מנהל מערכת בפרוטוקול SMB** - השיתופים האדמיניסטרטיביים (שיתופי מנהל מערכת) הם שירותי הרשת שנקבעו כברירת מחדל, אשר משתפים מחיצות כוננים קשיחים (*C$, D$*, ...) במערכת עם תיקיית המערכת (*ADMIN$*). השבתת החיבור לשיתופי מנהל המערכת אמורה למתן סיכוני אבטחה רבים. לדוגמה, התולעת Conficker מבצעת התקפות מילון כדי להתחבר לשיתופי מנהל מערכת.
- **מניעת ניבי SMB ישנים (בלתי נתמכים)** – מניעת הפעלות SMB שמשתמשות בניבי SMB ישנים שאינם נתמכים על-ידי IDS. מערכות ההפעלה המודרניות של Windows תומכות בניבי SMB ישנים עקב תאימות לאחור למערכות

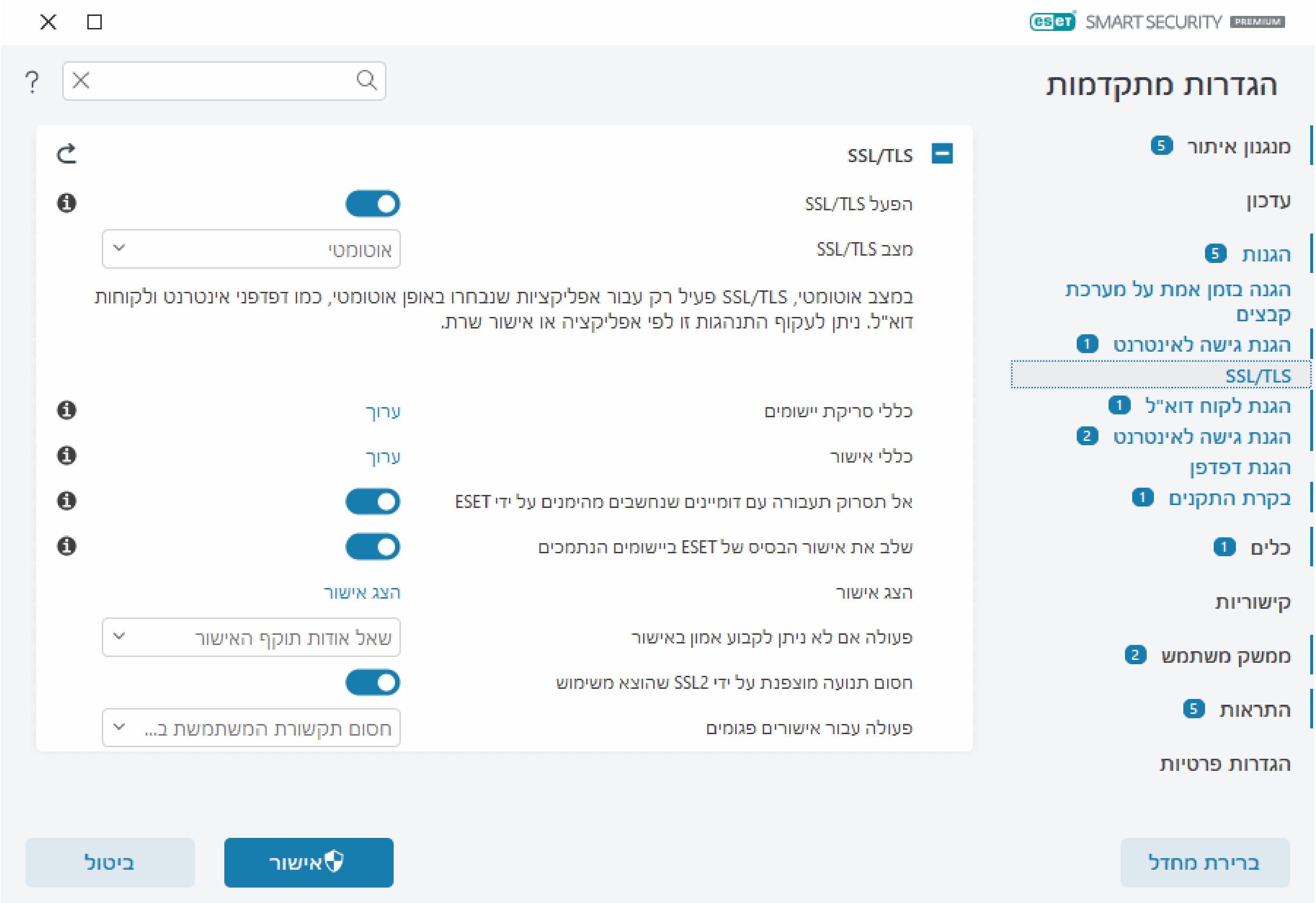
הפעלה ישנות, כגון Windows 95. התוקף יכול להשתמש בניב ישן בהפעלת SMB כדי להתחמק מבדיקת תעבורה. מנע ניבי SMB ישנים אם המחשב אינו צריך לשתף קבצים (או להשתמש בתקשורת SMB באופן כללי) עם מחשב הפועל בגרסה ישנה של Windows.

- **מניעת הפעלות SMB ללא אבטחה מורחבת** ‑ ניתן להשתמש באבטחה מורחבת במהלך המו"מ על הפעלת ה-SMB כדי לספק מנגנון אימות בטוח יותר מאימות LM (LAN Manager Challenge/Response). סכמת ה-LM נחשבת כחלשה ולא מומלץ להשתמש בה.
- **מניעת פתיחה של קובצי הפעלה בשרת מחוץ לאזור המהימן בפרוטוקול SMB** ‑ של החיבור כשאתה מנסה לפתוח קובץ הפעלה (.dll, .exe, ...) מתוך תיקייה משותפת בשרת שאינה שייכת לאזור המהימן בחומת האש. שים לב שהעתקת קובצי הפעלה ממקורות מהימנים עשויה להיות פעולה לגיטימית. מתוך תיקייה משותפת בשרת שאינה שייכת לאזור המהימן בחומת האש. שים לב שהעתקת קובצי הפעלה ממקורות מהימנים יכולה להיות לגיטימית, אולם זיהוי זה אמור למזער סיכונים כתוצאה מפתיחה בלתי רצויה של קובץ בשרת זדוני (לדוגמה, קובץ שנפתח על-ידי לחיצה על היפר-קישור לקובץ הפעלה זדוני משותף).
- **מניעת אימות NTLM בפרוטוקול SMB להתחברות לשרת בתוך או מחוץ לאזור המהימן** ‑ פרוטוקולים שמשתמשים בסכמות אימות NTLM (שתי הגרסאות) חשופים למתקפת העברת הרשאות (מכונה גם מתקפת מסירת SMB Relay] [SMB] במקרה של פרוטוקול SMB). מניעת אימות NTLM עם שרת מחוץ לאזור המהימן אמורה לצמצם את הסיכונים הנגרמים מהעברת הרשאות על-ידי שרת זדוני מחוץ לאזור המהימן. באותו אופן, באפשרותך למנוע אימות NTLM עם שרתים באזור המהימן.

- **אפשר תקשורת עם שירות מנהל חשבון אבטחה** ‑ לקבלת מידע נוסף על שירות זה ראה [MS-SAMR].
- **אפשר תקשורת עם שירות רשות האבטחה המקומית** ‑ לקבלת מידע נוסף על שירות זה ראה [MS-LSAD] ו-[MS-LSAT].
- **אפשר תקשורת עם שירות רישום מרחוק** ‑ לקבלת מידע נוסף על שירות זה ראה [MS-RRP].
- **אפשר תקשורת עם שירות מנהל בקרת שירותים** ‑ לקבלת מידע נוסף על שירות זה ראה [MS-SCMR].
- **אפשר תקשורת עם שירות השרת** ‑ לקבלת מידע נוסף על שירות זה ראה [MS-SRVS].
- **אפשר תקשורת עם שירותים אחרים** ‑ שירותי MSRPC אחרים. MSRPC הוא המימוש של Microsoft למנגנון DCE RPC. יתרה מכן, MSRPC יכול להשתמש ברכיבי named pipe המועברים לתוך פרוטוקול ה-SMB (שיתוף קובצי רשת) להעברה (ncacn_np transport). שירותי MSRPC מספקים ממשקים לגישה אל ולניהול של מערכות windows מרחוק. מספר פגיעויות אבטחה התגלו ונוצלו בשטח במערכת Windows MSRPC (תולעת Conficker, תולעת Sasser,...). השבת את התקשורת עם שירותי MSRPC שאינם דרושים לך כדי להפחית רבים מסיכוני האבטחה (למשל הפעלת קוד מרחוק או תקיפות כשל שירות).

SSL/TLS

ESET Smart Security Premium יכול לבדוק איומי תקשורת שמשתמשים בפרוטוקול SSL. באפשרותך להשתמש בשיטות סינון שונות כדי לבדוק תקשורות המוגנות ב-SSL עם אישורים מהימנים, אישורים לא מוכרים או אישורים שאינם כלולים בבדיקת תקשורת המוגנת באמצעות SSL. כדי לערוך הגדרות SSL/TLS, פתח את הגדרות מתקדמות > **הגנות** > **SSL/TLS**.



הפעל את SSL/TLS - אם הוא מושבת, ESET Smart Security Premium לא יסרוק תקשורת מעל SSL/TLS.

מצב SSL/TLS זמין באפשרויות הבאות:

מצב סינון	תיאור
אוטומטי	מצב ברירת המחדל יסרוק רק את היישומים המתאימים, כגון דפדפני אינטרנט ולקוחות דואר אלקטרוני. אפשר לעקוף אותו על-ידי בחירת האפליקציות שבהן התקשורת נסרקת.
אינטראקטיבי	אם תיכנס לאתר חדש המוגן ב-SSL (עם אישור לא מוכר), יוצג חלון דו-שיח לבחירת פעולה. מצב זה מאפשר לך ליצור רשימת אישורי SSL / אפליקציות שלא ייכללו בסריקה.
מבוסס-מדיניות	בחר באפשרות זו כדי לסרוק את כל התקשורות המוגנות באמצעות SSL, למעט תקשורות המוגנות על-ידי אישורים שלא נכללים בבדיקה. אם נוצרת תקשורת חדשה המשתמשת באישור חתום ובלתי ידוע, לא תקבל הודעה על כך והתקשורת תסונן באופן אוטומטי. כשאתה ניגש לשרת עם אישור לא מהימן שמסומן כמהימן (נמצא ברשימת האישורים המהימנים), התקשורת עם השרת מותרת והתוכן בערוץ התקשורת מסונן.

כללי סריקת אפליקציות - מאפשר להתאים אישית את ההתנהגות של ESET Smart Security Premium באפליקציות מסוימות.

כללי אישור - מאפשר להתאים אישית את ההתנהגות של ESET Smart Security Premium באישורי SSL מסוימים.

אל תסרוק תעבורה עם תחומים מהימנים על ידי ESET - כאשר אפשרות זו מופעלת, התקשורת עם תחומים מהימנים לא תיכלל בסריקה. רשימה לבנה מובנית המנוהלת על ידי ESET קובעת את מהימנות התחום.

שלב את אישור הבסיס של ESET ביישומים הנתמכים - כדי שתקשורת SSL תפעל כהלכה בדפדפנים/לקוחות הדואר האלקטרוני שלך, הכרחי להוסיף את אישור הבסיס של ESET לרשימת אישורי הבסיס (המפרסמים) המוכרים. כאשר אפשרות זו זמינה, ESET Smart Security Premium יוסיף באופן אוטומטי את אישור הבסיס של ESET SSL Filter CA לדפדפנים המוכרים (לדוגמה Opera). עבור דפדפנים המשתמשים המאגר האישורים של המערכת, האישור מתווסף באופן אוטומטי. לדוגמה, התצורה של Firefox מוגדרת באופן אוטומטי לתת אמון ברשויות הבסיס הכלולות במאגר

האישורים של המערכת.

כדי להחיל את האישור על דפדפנים שאינם נתמכים, לחץ על **הצג אישור** < **פרטים** < **העתקה לקובץ** וייבא אותו לתוך הדפדפן.

פעולה אם לא ניתן לקבוע אמון באישור - במקרים מסוימים, לא ניתן לאמת אישור אתר אינטרנט באמצעות המאגר של רשויות אישורי הבסיס המהימנים (TRCA) (לדוגמה, אישור שפג תוקפו, אישור לא מהימן, אישור שאינו תקף עבור התחום או החתימה הספציפיים שניתן לנתח אך אינם חותמים על האישור כראוי). אתרי אינטרנט לגיטימיים תמיד ישתמשו באישורים מהימנים. אם הם לא מספקים אישור כזה, יכול להיות שיש תוקף שמפענח את התקשורת שלך או שהאתר נתקל בקשיים טכניים.

אם נבחרה האפשרות **שאל אודות תוקף האישור** (אפשרות זו נבחרת כברירת מחדל), המשתמש יונחה לבחור את הפעולה שיש לבצע כשנוצרת תקשורת מוצפנת. יוצג חלון דו-שיח לבחירת פעולה, בו תוכל להחליט לסמן את האישור כמהימן או כלא כלול. אם האישור אינו מופיע ברשימת TRCA, החלון יהיה אדום. אם האישור מופיע ברשימת TRCA, החלון יהיה ירוק.

אפשר לבחור **חסום את התקשורת המשתמשת באישור** כדי לעצור תמיד חיבור מוצפן לאתר שמשתמש באישור בלתי מאומת.

חסום תנועה מוצפנת על ידי SSL2 שהוצא משימוש - תקשורת באמצעות הגרסה הקודמת של פרוטוקול SSL תיחסם באופן אוטומטי.

פעולה עבור אישורים פגומים - אישור פגום פירושו שהאישור משתמש בתבנית שאינה מזוהה על-ידי ESET Smart Security Premium או שהתבנית פגומה (לדוגמה, הוחלפה על-ידי נתונים אקראיים). במצב זה מומלץ לבחור באפשרות **חסום את התקשורת המשתמשת באישור**. אם האפשרות **שאל אודות תוקף האישור** נבחרת, המשתמש יונחה לבחור את הפעולה שיש לבצע כשנוצרת תקשורת מוצפנת.

> **דוגמאות מאוירות**
>
> מאמר מאגר הידע הבא של ESET עשוי להיות זמין באנגלית בלבד:
>
> - התראות על אישורים במוצרים הביתיים של ESET עבור Windows
> - "תעבורת רשת מוצפנת אישור לא מהימן" מוצג בעת ביקור בדפי אינטרנט

כללי סריקת יישומים

ניתן להשתמש ב**כללי סריקת יישומים** כדי להתאים את אופן הפעולה של ESET Smart Security Premium לאפליקציות ספציפיות ולזכור את הפעולות שנבחרו כאשר **מצב SSL/TLS** נמצא ב**מצב אינטראקטיבי**. אפשר להציג ולערוך את הרשימה דרך הגדרות מתקדמות < **הגנות** < **SSL/TLS** < **כללי סריקת יישומים** < **ערוך**.

החלון **כללי סריקת יישומים** כולל:

עמודות

אפליקציה ⍰ בחר קובץ הפעלה מעץ הספרייה, לחץ על האפשרות **...** או הזן את הנתיב ידנית.

פעולת סריקה ⍰ בחר **סרוק** או **התעלם** כדי לסרוק את התקשורת או להתעלם ממנה. בחר **אוטומטי** כדי לסרוק במצב אוטומטי ולשאול במצב אינטראקטיבי. בחר **שאל** כדי לשאול את המשתמש תמיד מה לעשות.

רכיבי בקרה

הוספה ⍰ הוסף יישום מסונן.

ערוך - בחר את האפליקציה שברצונך לקבוע את תצורתה ולחץ על **ערוך**.

הסר - בחר את האפליקציה שברצונך להסיר ולחץ על **הסר**.

ייבוא/ייצוא - ייבוא אפליקציות מקובץ או שמירת הרשימה הנוכחית של אפליקציות בקובץ.

אישור/ביטול ⍰ לחץ על **אישור** אם ברצונך לשמור את השינויים, או לחץ על **ביטול** אם ברצונך לצאת מבלי לשמור.

כללי אישור

ניתן להשתמש ב**כללי אישור** להתאמה אישית של אופן הפעולה של ESET Smart Security Premium עבור אישורי SSL ספציפיים וכדי לזכור פעולות שנבחרו כאשר **מצב SSL/TLS** נמצא ב**מצב אינטראקטיבי**. ניתן להציג ולערוך את הרשימה דרך הגדרות מתקדמות > **הגנות** > **SSL/TLS** > **כללי אישור** > **ערוך**.

החלון **כללי אישור** מורכב מ:

עמודות

שם ⍰ שם האישור.

מנפיק האישור ⍰ שם יוצר האישור.

נושא האישור ⍰ הנושא מזהה את הישות המשויכת למפתח הציבורי המאוחסן בשדה הנושא של המפתח הציבורי.

גישה ⍰ בחר **התרה** או **חסימה** כ**פעולת הגישה** כדי להתיר/לחסום תקשורת המאובטחת על-ידי אישור זה, ללא תלות במהימנותה. בחר **אוטומטי** כדי להתיר פעולת אישורים מהימנים ולשאול במקרה של הלא מהימנים. בחר **שאל** כדי לשאול את המשתמש תמיד מה לעשות.

סריקה ⍰ בחר **סרוק** או **התעלם** כ**פעולת הסריקה** כדי לסרוק או להתעלם מתקשורת המאובטחת על-ידי אישור זה. בחר **אוטומטי** כדי לסרוק במצב אוטומטי ולשאול במצב אינטראקטיבי. בחר **שאל** כדי לשאול את המשתמש תמיד מה לעשות.

רכיבי בקרה

הוספה - הוסף אישור חדש והתאם את ההגדרות שלו ביחס לאפשרויות גישה וסריקה.

עריכה ⍰ בחר את האישור שברצונך להגדיר ולחץ על **ערוך**.

הסר ⍰ בחר את האישור שברצונך למחוק ולחץ על **הסר**.

אישור/ביטול ⍰ לחץ על **אישור** אם ברצונך לשמור את השינויים, או לחץ על **ביטול** אם ברצונך לצאת מבלי לשמור.

תעבורת רשת מוצפנת

אם המערכת שלך מוגדרת להשתמש בסריקה של SSL/TLS, יופיע חלון תיבת דו-שיח שינחה אותך לבחור פעולה בשני מצבים:

ראשית, אם אתר אינטרנט משתמש באישור שאינו ניתן לאימות או באישור לא חוקי, ו-ESET Smart Security Premium מוגדר לשאול את המשתמש במקרים כאלה (כברירת מחדל, 'כן' עבור אישורים שאינם ניתנים לאימות, ו'לא' עבור אישורים לא חוקיים), תוצג תיבת דו-שיח שבה תישאל אם **לאפשר** או **לחסום** את החיבור. אם האישור אינו ממוקם ב-Trusted Root Certification Authorities store (TRCA), הוא נחשב כלא מהימן.

שנית, אם מצב **SSL/TLS** מוגדר **מצב אינטראקטיבי**, תופיע תיבת דו-שיח לכל אתר עם שאלה האם **לסרוק** את התעבורה או **להתעלם** ממנה. חלק מהאפליקציות מוודאות שאף גורם לא שינה או בדק את תעבורת ה-SSL שלהן. במקרים כאלה, על ESET Smart Security Premium **להתעלם** מתעבורה זו כדי לאפשר לאפליקציה להמשיך ולפעול כרגיל.

> **דוגמאות מאוירות**
>
> מאמר מאגר הידע הבא של ESET עשוי להיות זמין באנגלית בלבד:
>
> - התראות על אישורים במוצרים הביתיים של ESET עבור Windows
> - "תעבורת רשת מוצפנת אישור לא מהימן" מוצג בעת ביקור בדפי אינטרנט

בשני המקרים, המשתמש יכול לבחור לזכור את הפעולה שנבחרה. פעולות שמורות מאוחסנות בכללי האישור.

הגנה על לקוח דוא"ל

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 **ThreatSense** בהגדרות מתקדמות 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 אתחול המערכת
- הגנה על מסמכים
- הגנה על 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 תוכנות זדוניות 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 הגרסאות הקודמות של מודול מנגנון האיתור. 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 הפעולה של ESET Smart Security Premium בעת ניקוי אובייקטים. ישנן 4 רמות ניקוי:

ThreatSense כולל את רמות התיקון (כלומר, הניקוי) הבאות.

תיקון ב-ESET Smart Security Premium

תיאור	דרגת ניקוי
נסה לתקן את האיתור בעת ניקוי אובייקטים ללא התערבות של משתמש הקצה. במקרים נדירים (לדוגמה, קובצי מערכת), אם לא ניתן לתקן את האיתור, האובייקט המדווח נשאר במיקומו המקורי.	**תקן את האיתור תמיד**
נסה לתקן את האיתור בעת ניקוי אובייקטים ללא התערבות של משתמש הקצה. במקרים מסוימים (לדוגמה, קובצי מערכת או ארכיונים עם קבצים נקיים ונגועים), אם לא ניתן לתקן איתור, האובייקט המדווח נשאר במיקומו המקורי.	**תקן את האיתור אם בטוח, אחרת השאר**
נסה לתקן את האיתור בעת ניקוי אובייקטים. במקרים מסוימים, אם לא ניתן לבצע פעולה, משתמש הקצה מקבל התראה אינטראקטיבית ועליו לבחור בפעולת תיקון (לדוגמה, הסרה או התעלמות). הגדרה זו מומלצת במרבית המקרים.	**תקן את האיתור אם בטוח, אחרת שאל**
משתמש הקצה מקבל חלון אינטראקטיבי בעת ניקוי אובייקטים ועליו לבחור פעולת תיקון (לדוגמה, הסרה או התעלמות). רמה זו תוכנה עבור משתמשים מתקדמים, שיודעים באילו פעולות לנקוט במקרה של איתור.	**שאל תמיד את משתמש הקצה**

החרגות

סיומת היא החלק של שם הקובץ שמופרד ממנו באמצעות נקודה. סיומת מגדירה את סוג הקובץ ותכולתו. במקטע זה של הגדרות ThreatSense אפשר 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.

תעד את כל האובייקטים – יומן הסריקות יציג את כל הקבצים שנסרקו בארכיונים של חילוץ עצמי, גם את אלה שלא הושפעו (הדבר עלול ליצור נתונים רבים ביומן הסריקות ולהגדיל את קובץ יומן הסריקות).

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 קבצים באובייקט של גורם מכיל (כגון ארכיון RAR/ZIP או הודעת דוא"ל עם מספר קבצים מצורפים). הגדרה זו אינה חלה על קבצים נפרדים. אם ערך המוגדר על-ידי משתמש הוזן כאן וזמן זה חלף, הסריקה תסתיים בהקדם האפשרי, בין אם הסריקה של כל קובץ באובייקט של גורם מכיל ובין אם היא לא הסתיימה.
במקרה של ארכיון המכיל קבצים רבים, הסריקה לא תסתיים לפני חילוץ של קובץ מהארכיון (לדוגמה, כאשר ערך שהוגדר על-ידי המשתמש הוא 3 שניות, אך החילוץ של קובץ נמשך 5 שניות). שאר הקבצים בארכיון לא ייסרקו בחלוף זמן זה.
כדי להגביל את זמן הסריקה, כולל קובצי ארכיון גדולים יותר, השתמש באפשרויות **גודל אובייקט מקסימלי** ו**גודל מקסימלי של קובץ בארכיון** (לא מומלץ עקב סיכוני אבטחה אפשריים).
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. הערך המרבי הוא **3GB**.

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

הגנת גישה לאינטרנט

הגנת גישה לאינטרנט מאפשרת לך להגדיר הגדרות מתקדמות של מודול הגנת אינטרנט. האפשרויות הבאות זמינות דרך הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **הגנת גישה לאינטרנט**:

הפעל הגנת גישה לאינטרנט � כאשר אפשרות זו מושבתת, לא יופעלו הגנת גישה לאינטרנט והגנת אנטי-פישינג.

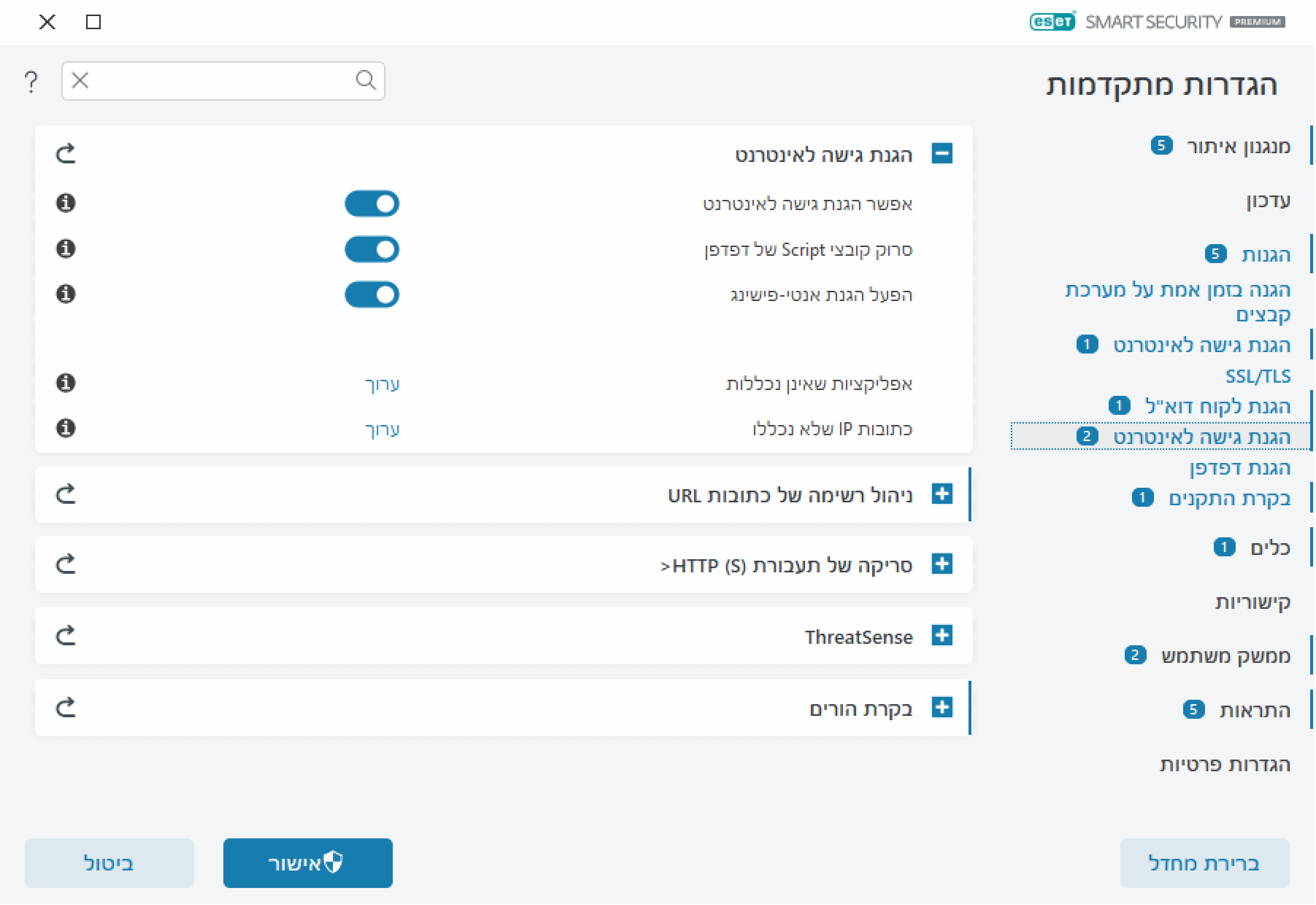
אנו ממליצים להשאיר את 'הגנת גישה לאינטרנט' מופעלת ולא לכלול אפליקציות או כתובות IP כברירת מחדל.

סרוק סקריפטים של דפדפן - כאשר האפשרות הזו מופעלת, מנגנון האיתור בודק את כל תוכניות JavaScript שמופעלות על ידי דפדפני אינטרנט.

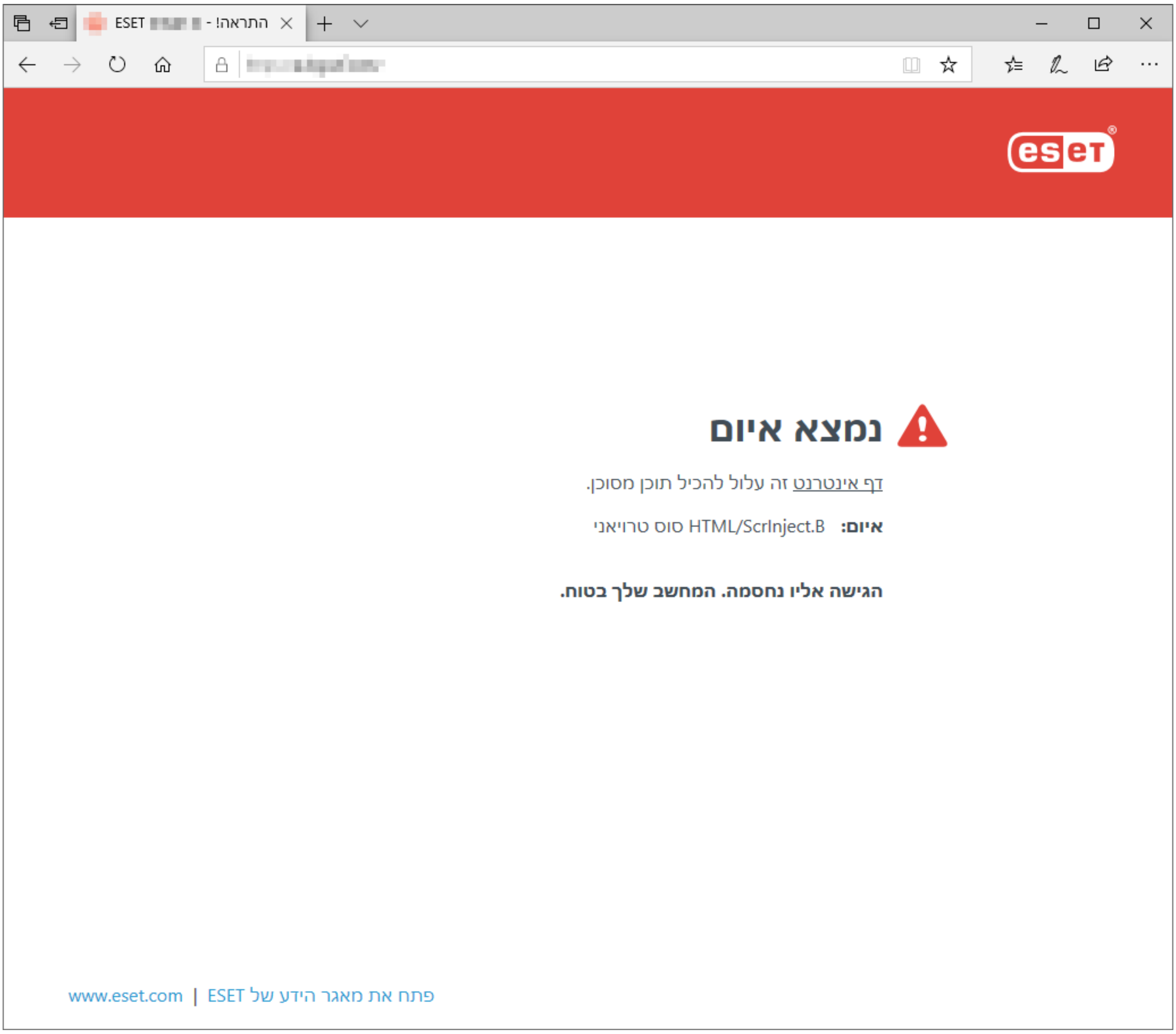
הפעל הגנת אנטי-פישינג - כאשר אפשרות זו מופעלת, דפי אינטרנט של פישינג חסומים. ראה פרטים נוספים בנושא הגנת אנטי-פישינג.

אפליקציות שאינן נכללות - מאפשר להחריג אפליקציות מסוימות בסריקה של 'הגנת גישה לאינטרנט'. האפשרות הזו שימושית כאשר הגנת גישה לאינטרנט גורמת לבעיות תאימות.

כתובות IP שלא נכללו - מאפשר להחריג כתובות מרוחקות ספציפיות בסריקה של 'הגנת גישה לאינטרנט'. האפשרות הזו שימושית כאשר הגנת גישה לאינטרנט גורמת לבעיות תאימות.



'הגנת גישה לאינטרנט' תציג את ההודעה הבאה בדפדפן שלך כאשר אתר האינטרנט נחסם:



הנחיות מאוירות

מאמר מאגר הידע הבא של ESET עשוי להיות זמין באנגלית בלבד:
- החרג אתר אינטרנט בטוח מחסימה על ידי 'הגנת גישה לאינטרנט'
- חסימת אתר אינטרנט באמצעות ESET Smart Security Premium

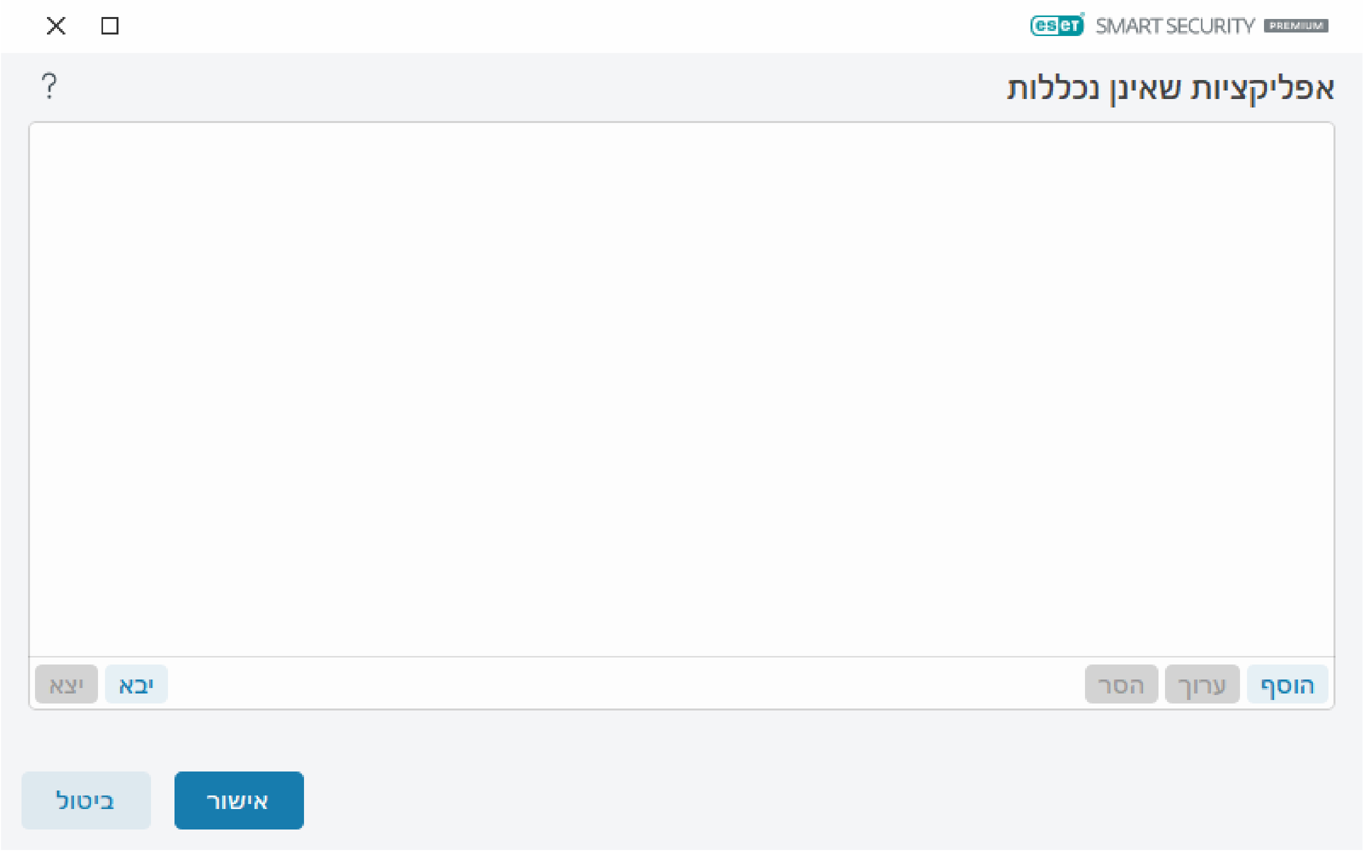
אפליקציות שאינן נכללות

כדי לא לכלול סריקה של תקשורת עבור אפליקציות מסוימות, הוסף אותן לרשימה. התקשורת (HTTP(S)/POP3(S)/IMAP(S של היישומים שנבחרו לא תיבדק לאיתור איומים. אנו ממליצים להשתמש במצב זה רק עבור יישומים שאינם פועלים כהלכה עם התקשורת הנבדקת.

האפליקציות והשירותים הפועלים יהיו זמינים כאן באופן אוטומטי לאחר לחיצה על **הוסף**. לחץ על **...** ונווט לאפליקציה כדי להוסיף החרגה באופן ידני.

ערוך - ערוך ערכים נבחרים מהרשימה.

מחק - הסר את הערכים הנבחרים מהרשימה.



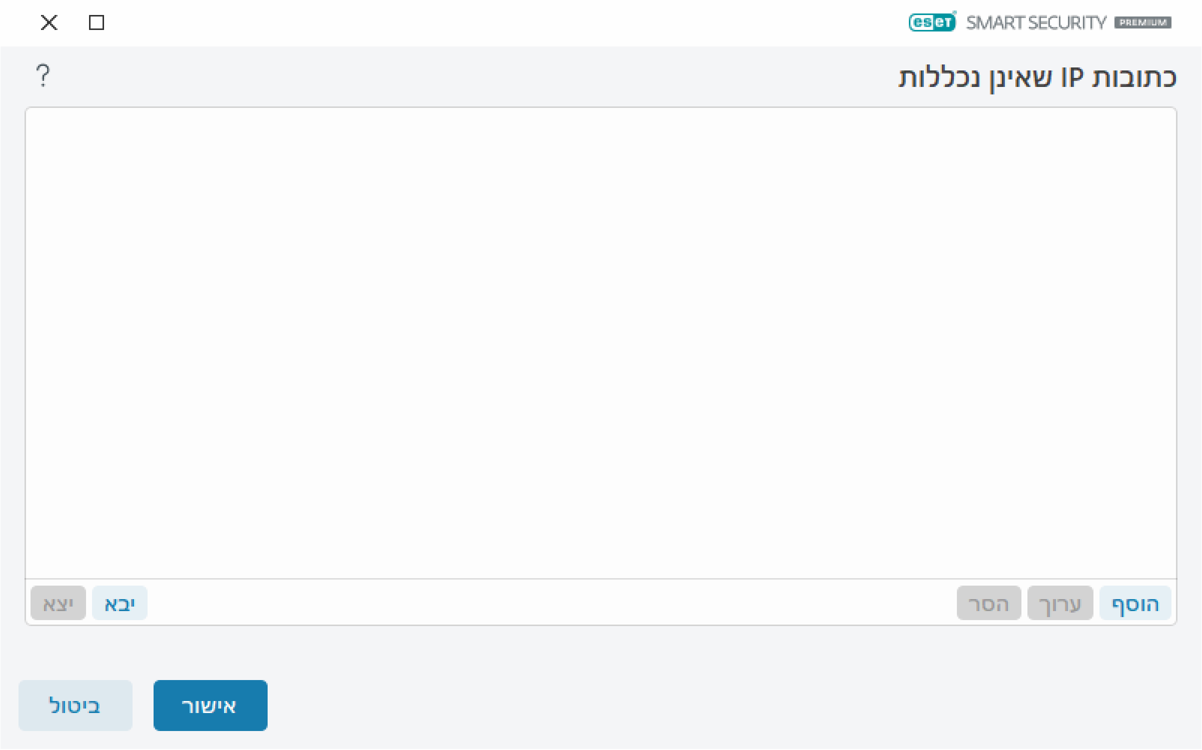
כתובות IP שלא נכללו

הערכים שברשימה לא ייכללו בסינון. תקשורת HTTP(S)/POP3(S)/IMAP(S) מהכתובות שנבחרו ואליהן לא תיבדק לאיתור איומים. מומלץ להשתמש באפשרות זו רק עבור כתובות שידועות כמהימנות.

לחץ על **הוספה** כדי לא לכלול כתובת IP/טווח כתובות/רשת משנה של נקודה מרוחקת.

לחץ על **ערוך** כדי לשנות את כתובת ה-IP שנבחרה.

לחץ על **מחק** כדי להסיר את הערכים הנבחרים מהרשימה.



דוגמאות לכתובות IP

הוספת כתובת IPv4:

כתובת יחידה - הוספת כתובת IP של מחשב אחד (לדוגמה, *192.168.0.10*).

טווח כתובות – הזן את כתובת ה-IP הפותחת והסוגרת כדי לציין את טווח כתובות ה-IP של מספר מחשבים (לדוגמה 192.168.0.1 עד 192.168.0.99).

רשת משנה – רשת משנה (קבוצת מחשבים) מוגדרת באמצעות כתובת IP ומסיכה. לדוגמה, 255.255.255.0 היא מסיכת הרשת עבור רשת המשנה 192.168.1.0. כדי לא לכלול את כל הסוג של רשת המשנה ב-*192.168.1.0/24*.

הוספת כתובת IPv6:

כתובת יחידה - הוספת כתובת IP של מחשב בודד (לדוגמה, *2001:718:1c01:16:214:22ff:fec9:ca5*).

רשת משנה – רשת משנה (קבוצת מחשבים) מוגדרת באמצעות כתובת IP ומסיכה (לדוגמה: *2002:c0a8:6301:1::1/64*).

ניהול רשימה של כתובות URL

ניהול רשימת כתובות URL דרך [הגדרות מתקדמות](#) > **הגנות** > **הגנת גישה לאינטרנט** > מאפשר לציין כתובות HTTP לצורך חסימה, הפעלה או אי הכללה מסריקת התוכן.

[SSL/TLS](#) צריך להיות מופעל אם ברצונך לסנן כתובות HTTPS בנוסף לכתובות HTTP. אם אפשרות זו לא תיבחר, ייתווספו רק התחומים של אתרי HTTPS שבהם ביקרת, אך לא כתובת ה-URL המלאה.

אתרי האינטרנט ש**ברשימת הכתובות החסומות** לא יהיו נגישים, אלא אם ייכללו אף הם ב**רשימת הכתובות המותרות**.
אתרי האינטרנט ב**רשימת כתובות שאינן נכללות בסריקת תוכן** לא ייסרקו לאיתור קוד זדוני בעת הגישה אליהם.

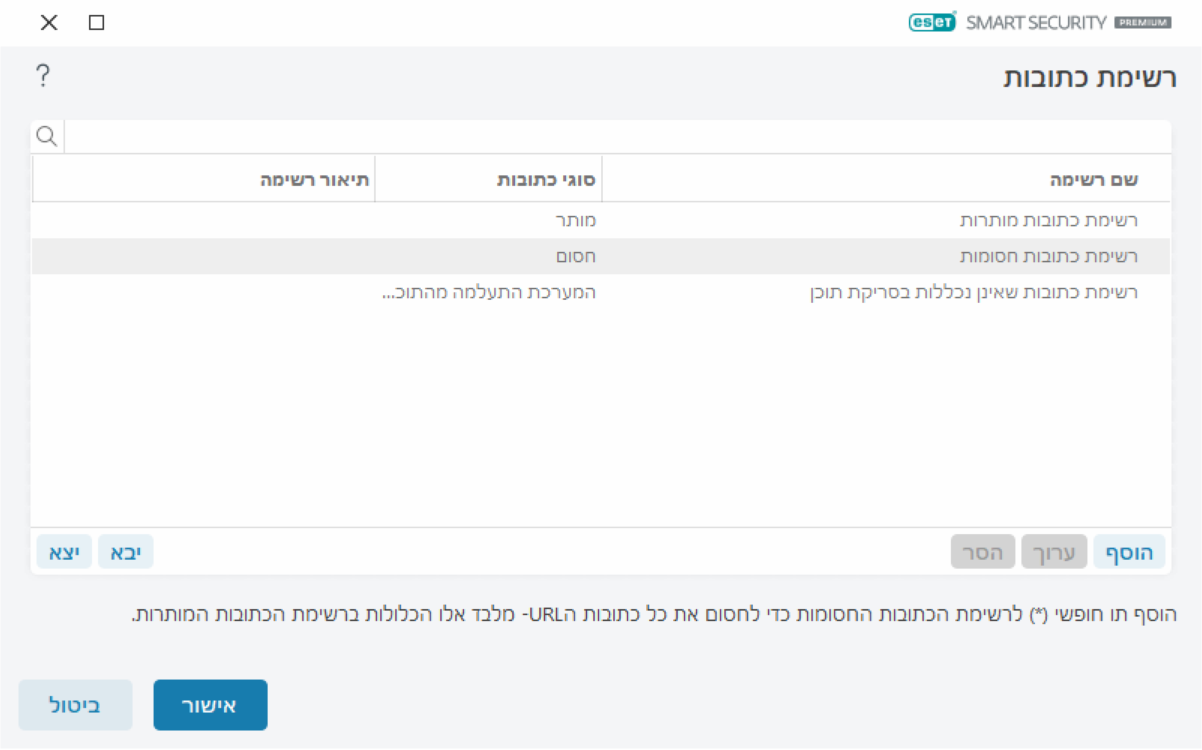
אם ברצונך לחסום את כל כתובות ה-HTTP, למעט הכתובות שנמצאות ב**רשימת הכתובות המותרות** הפעילה, הוסף * ל**רשימת הכתובות החסומות**.

הסמלים המיוחדים * (כוכבית) ו-? (סימן שאלה) ניתנים לשימוש ברשימות. הכוכבית מחליפה כל מחרוזת תווים שהיא, וסימן השאלה מחליף כל סמל שהוא. יש לשים לב כאשר מציינים כתובות שלא ייכללו, מפני שעל הרשימה להכיל רק

כתובות מהימנות ובטוחות. באותה מידה, הכרחי לוודא שהשימוש בסמלים * ו-? ברשימה זו נעשה באופן הראוי. ראה [הוספת מסיכת תחום / כתובת HTTP](#) לקבלת פרטים כיצד ניתן להתאים בבטחה תחום שלם הכולל את כל תחומי המשנה. כדי להפעיל רשימה בחר **רשום כפעילה**. אם ברצונך לקבל הודעה כשאתה נכנס לכתובת הנכללת ברשימה הנוכחית, בחר **הודע בעת החלה**.

כתובות מהימנות על ידי ESET

אם האפשרות **אל תסרוק תעבורה עם תחומים מהימנים על ידי ESET** שמופעלת היא [SSL/TLS](#), תחומים ברשימה הלבנה שמנוהלים על ידי ESET לא יושפעו מהגדרת הניהול של רשימת כתובות URL.



רכיבי בקרה

הוסף – יצירת רשימה חדשה, בנוסף לאלו שהוגדרו מראש. אפשרות זו עשויה להועיל כשברצונך לבצע חלוקה לוגית של קבוצות כתובות שונות. לדוגמה, רשימה אחת של כתובות חסומות עשויה להכיל כתובות מרשימה שחורה ציבורית חיצונית, ושנייה עשויה להכיל רשימה שחורה שלך; בצורה זו קל יותר לעדכן את הרשימה החיצונית מבלי לפגוע ברשימה שלך.

ערוך – שינוי רשימות קיימות. השתמש באפשרות זו כדי להוסיף או להסיר כתובות.

מחק – מחיקת רשימות קיימות. אפשרות זו זמינה רק עבור רשימות שנוצרו בעזרת האפשרות **הוסף**, ולא עבור רשימות ברירת המחדל.

רשימת כתובות

במקטע זה באפשרותך לציין רשימות של כתובות HTTP(S) שייחסמו, יותרו או יוחרגו מהבדיקה.

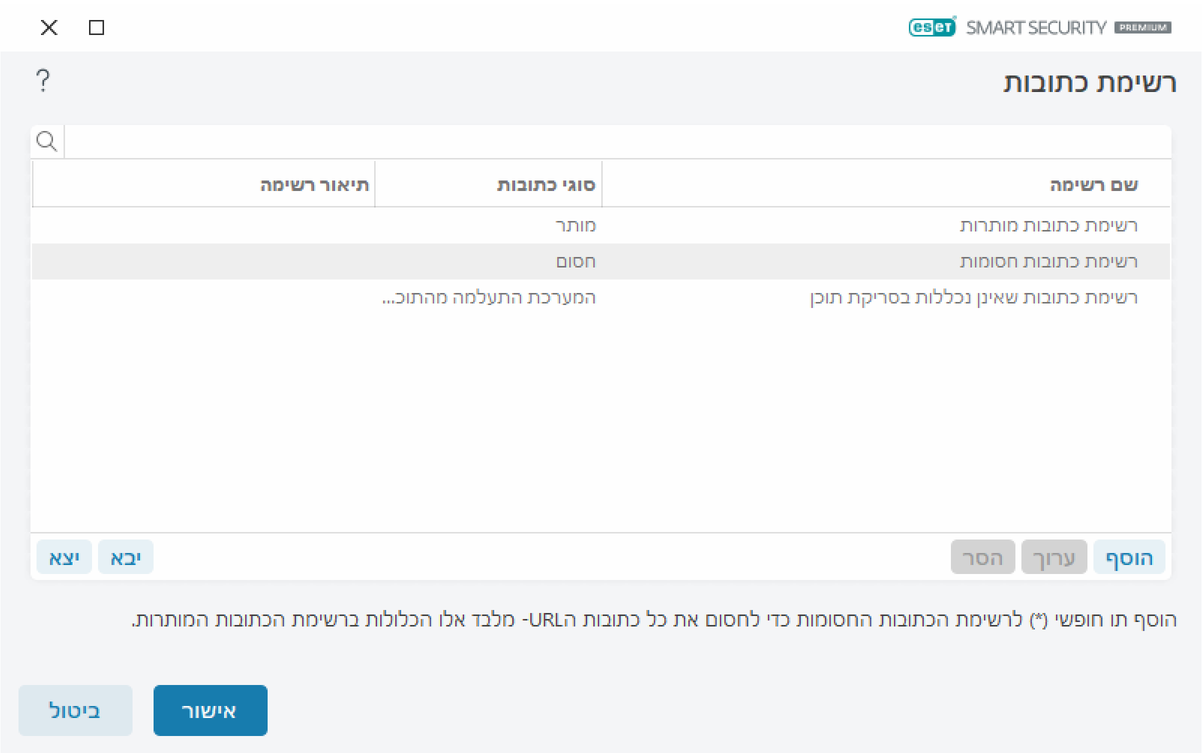
כברירת מחדל זמינות שלוש הרשימות הבאות:

- **רשימת כתובות שאינן נכללות בסריקת תוכן** – לא תבוצע בדיקת קוד זדוני לאף אחת מהכתובות שתתווסף

לרשימה זו.

- **רשימת כתובות מותרות** אם אם מתן אפשרות גישה רק לכתובות HTTP ברשימת הכתובות המותרות פעיל ורשימת הכתובות החסומות כוללת * (התאמה להכול), המשתמש יורשה לגשת לכתובות שצוינו ברשימה זו בלבד. הכתובות ברשימה זו יותרו גם אם ייכללו ברשימת הכתובות החסומות.
- **רשימת כתובות חסומות** - למשתמש לא יותר לגשת לכתובות שצוינו ברשימה זו, אלא אם הן יופיעו ברשימת הכתובות המותרות.

לחץ על **הוסף** כדי ליצור רשימה חדשה. כדי למחוק את הרשימות שנבחרו, לחץ על **מחק**.



הנחיות מאוירות

מאמר מאגר הידע הבא של ESET עשוי להיות זמין באנגלית בלבד:

- החרג אתר אינטרנט בטוח מחסימה על ידי 'הגנת גישה לאינטרנט'
- חסום אתר אינטרנט באמצעות המוצרים הביתיים של ESET ל-Windows

ראה פרטים נוספים בנושא ניהול רשימת כתובות URL.

יצירת רשימת כתובות חדשה

תיבת דו-שיח זו מאפשרת לך לציין רשימה חדשה של מסיכות/כתובות URL שייחסמו, יותרו או יוחרגו מהבדיקה.

באפשרותך לקבוע את התצורה של האפשרויות הבאות:

סוג רשימת כתובות זמינים שלושה סוגי רשימות:

- **המערכת התעלמה מהתוכנה הזדונית שנמצאה** לא תבוצע בדיקת קוד זדוני לאף אחת מהכתובות שתתווסף לרשימה זו.
- **חסומות** הגישה לכתובות שצוינו ברשימה זו תיחסם.
- **מותרות** הגישה לכתובות שצוינו ברשימה זו תותר. כתובות ברשימה זו יותרו גם אם תהיה התאמה בינן לבין

רשימת הכתובות החסומות.

שם רשימה ￼ ציין את שם הרשימה. שדה זה לא יהיה זמין בעת עריכת אחת מהרשימות שהוגדרו מראש.

תיאור רשימה ￼ הקלד תיאור קצר לרשימה (אופציונלי). לא זמין בעת עריכת אחת מהרשימות שהוגדרו מראש.

כדי להפעיל רשימה בחר **רשום כפעילה** לצד הרשימה. אם ברצונך לקבל הודעה כאשר נעשה שימוש ברשימה מסוימת בעת ביקור באתרי אינטרנט, בחר באפשרות **הודע בעת החלה**. לדוגמה, תוצג הודעה כאשר אתר אינטרנט מסוים נחסם או מותר עקב השתייכותו לרשימת כתובות חסומות או מותרות. ההודעה תכלול את שם הרשימה.

חומרת רישום ביומן ￼ ניתן לכתוב ב<u>רשומות היומן</u> מידע אודות הרשימה הספציפית שבה נעשה שימוש בעת גישה לאתרי אינטרנט.

רכיבי בקרה

הוסף ￼ הוספת כתובת URL חדשה לרשימה (הזן מספר ערכים מופרדים).

ערוך ￼ שינוי כתובת קיימת ברשימה. זמין רק עבור כתובות שנוצרו בעזרת **הוספה**.

הסר ￼ מחיקת כתובות שקיימות ברשימה. זמין רק עבור כתובות שנוצרו בעזרת **הוספה**.

ייבוא ￼ ייבוא קובץ עם כתובות URL (הפרד בין הערכים באמצעות מעבר שורה, לדוגמה ‎*.txt‎ המשתמש בקידוד UTF-8).

כיצד להוסיף מסיכת URL

אנא עיין בהוראות שבחלון דו-שיח זה לפני שתזין את הכתובת/מסיכת התחום המבוקשות.

ESET Smart Security Premium מאפשר למשתמש לחסום את הגישה לאתרי אינטרנט שצוינו ולמנוע מדפדפן האינטרנט להציג את תוכנם. יתרה מכך, הוא מאפשר למשתמש לציין כתובות שאין לכלול בבדיקה. אם השם המלא של השרת המרוחק אינו ידוע, או שהמשתמש מעוניין לציין קבוצה שלמה של שרתים מרוחקים, ניתן להשתמש באותן "מסיכות" כדי לזהות את הקבוצה. המסיכות כוללות את הסימנים "?" ו-"*":

- השתמש בסימן ? כתחליף לסמל
- השתמש בסימן * כתחליף למחרוזת טקסט.

לדוגמה ‎*.c?m‎ מתייחס לכל הכתובות שבהן החלק האחרון מתחיל באות c ומסתיים באות m, כשביניהן סמל לא ידוע (‎.com, .cam‎ וכו').

רצף "‎*.‎" לפני המחרוזת יקבל יחס מיוחד אם הוא מופיע בתחילת שם תחום. ראשית, התו הכללי * אינו תואם לתו הקו הנטוי ('/') במקרה זה. זאת כדי להימנע מעקיפת המסיכה, לדוגמה, המסיכה ‎*.domain.com‎ לא תתאים ל-*http://anydomain.com/anypath#.domain.com* (סיומת כזו ניתן לצרף לכל כתובת URL מבלי להשפיע על ההורדה). שנית, "‎*.‎" גם מתאימה למחרוזת ריקה במקרה מסוים זה. זאת כדי לאפשר התאמה לתחום שלם, לרבות כל תחומי המשנה המשתמשים במסיכה יחידה. לדוגמה, המסיכה ‎*.domain.com‎ מתאימה גם ל-*http://domain.com*. שימוש ב-*domain.com‎* יהיה שגוי, מאחר שעשוי להתאים גם ל-*http://anotherdomain.com*.

סריקה של תעבורת HTTP(S)

כברירת מחדל, ESET Smart Security Premium מוגדר לסרוק את תעבורת HTTP ו- HTTPS המשמשת דפדפני אינטרנט ואפליקציות אחרות. עליך להשבית את סריקת התנועה רק אם אתה נתקל בבעיות בתוכנת צד שלישי וברצונך לדעת אם הבעיה נגרמת על ידי ESET Smart Security Premium.

אפשר סריקה של תעבורת HTTP - תעבורת HTTP מנוטרת תמיד בכל היציאות עבור כל האפליקציות.

הפעל סריקה של תעבורת HTTPS - תעבורתHTTPS משתמשת בערוץ מוצפן להעברת מידע בין השרת ללקוח. ESET Smart Security Premium 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 HTTPS**, ללא קשר לגרסת מערכת ההפעלה (באפשרותך להוסיף יציאות 443 ו-65535-0 שהוגדרו מראש).

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 **ThreatSense** ב<u>הגדרות מתקדמות</u> 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 אתחול המערכת
- הגנה על מסמכים
- הגנה על 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 תוכנות זדוניות 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 הגרסאות הקודמות של מודול מנגנון האיתור. 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 הפעולה של ESET Smart Security Premium בעת ניקוי אובייקטים. ישנן 4 רמות ניקוי:

ThreatSense כולל את רמות התיקון (כלומר, הניקוי) הבאות.

תיקון ב-ESET Smart Security Premium

תיאור	דרגת ניקוי
נסה לתקן את האיתור בעת ניקוי אובייקטים ללא התערבות של משתמש הקצה. במקרים נדירים (לדוגמה, קובצי מערכת), אם לא ניתן לתקן את האיתור, האובייקט המדווח נשאר במיקומו המקורי.	**תקן את האיתור תמיד**
נסה לתקן את האיתור בעת ניקוי אובייקטים ללא התערבות של משתמש הקצה. במקרים מסוימים (לדוגמה, קובצי מערכת או ארכיונים עם קבצים נקיים ונגועים), אם לא ניתן לתקן איתור, האובייקט המדווח נשאר במיקומו המקורי.	**תקן את האיתור אם בטוח, אחרת השאר**
נסה לתקן את האיתור בעת ניקוי אובייקטים. במקרים מסוימים, אם לא ניתן לבצע פעולה, משתמש הקצה מקבל התראה אינטראקטיבית ועליו לבחור בפעולת תיקון (לדוגמה, הסרה או התעלמות). הגדרה זו מומלצת במרבית המקרים.	**תקן את האיתור אם בטוח, אחרת שאל**
משתמש הקצה מקבל חלון אינטראקטיבי בעת ניקוי אובייקטים ועליו לבחור פעולת תיקון (לדוגמה, הסרה או התעלמות). רמה זו תוכנה עבור משתמשים מתקדמים, שיודעים באילו פעולות לנקוט במקרה של איתור.	**שאל תמיד את משתמש הקצה**

החרגות

סיומת היא החלק של שם הקובץ שמופרד ממנו באמצעות נקודה. סיומת מגדירה את סוג הקובץ ותכולתו. במקטע זה של הגדרות ThreatSense אפשר 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.

תעד את כל האובייקטים – יומן הסריקות יציג את כל הקבצים שנסרקו בארכיונים של חילוץ עצמי, גם את אלה שלא הושפעו (הדבר עלול ליצור נתונים רבים ביומן הסריקות ולהגדיל את קובץ יומן הסריקות).

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 קבצים באובייקט של גורם מכיל (כגון ארכיון RAR/ZIP או הודעת דוא"ל עם מספר קבצים מצורפים). הגדרה זו אינה חלה על קבצים נפרדים. אם ערך המוגדר על-ידי משתמש הוזן כאן וזמן זה חלף, הסריקה תסתיים בהקדם האפשרי, בין אם הסריקה של כל קובץ באובייקט של גורם מכיל ובין אם היא לא הסתיימה.
במקרה של ארכיון המכיל קבצים רבים, הסריקה לא תסתיים לפני חילוץ של קובץ מהארכיון (לדוגמה, כאשר ערך שהוגדר על-ידי המשתמש הוא 3 שניות, אך החילוץ של קובץ נמשך 5 שניות). שאר הקבצים בארכיון לא ייסרקו בחלוף זמן זה.
כדי להגביל את זמן הסריקה, כולל קובצי ארכיון גדולים יותר, השתמש באפשרויות **גודל אובייקט מקסימלי** ו**גודל מקסימלי של קובץ בארכיון** (לא מומלץ עקב סיכוני אבטחה אפשריים).

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. הערך המרבי הוא **3GB**.

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

בקרת הורים

האפשרות **הפעל בקרת הורים** משלבת בקרת הורים בתוך ESET Smart Security Premium. לחץ על **ערוך** ליד חשבונות משתמשים כדי לשייך חשבונות של משתמשי Windows שבהם משתמשת בקרת ההורים למשתמשים ספציפיים, כדי להגביל את הגישה שלהם לתוכן בלתי הולם או מזיק באינטרנט.

חשבונות משתמש

דרך הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **בקרת הורים** > **חשבונות משתמשים** > **ערוך** באפשרותך לשייך חשבונות של משתמשי Windows שבהם משתמשת בקרת ההורים למשתמשים ספציפיים, כדי להגביל את הגישה שלהם לתוכן בלתי הולם או מזיק באינטרנט.

עמודות

חשבון Windows שם המשתמש.

מופעל המופעל, בקרות הורים מופעלות עבור חשבון משתמש ספציפי.

תחום שם התחום שאליו המשתמש שייך.

יום הולדת גיל המשתמש שלו חשבון זה שייך.

רכיבי בקרה

הוסף חלון הדו-שיח עבודה עם חשבונות משתמש יוצג.

ערוך עם אפשרות זו ניתן לערוך את החשבונות שנבחרו.

מחק מחק את החשבון שנבחר.

רענן אם הוספת חשבון משתמש, ESET Smart Security Premium יכול לרענן את רשימת חשבונות המשתמש ללא צורך לפתוח חלון זה מחדש.

הגדרות של חשבון משתמש

החלון כולל שלוש כרטיסיות:

כללי

הפעל את המתג לצד **מופעל** כדי להפעיל את בקרת ההורים עבור חשבון Windows שנבחר למטה.

תחילה, **בחר** חשבון Windows מהמחשב שלך. ההגבלות המוגדרות בבקרת ההורים משפיעות רק על חשבונות Windows רגילים. חשבונות מנהל מערכת מסוגלים להחליף את ההגבלות.

אם החשבון משמש הורה, בחר **חשבון הורה**.

הגדר את **תאריך הלידה של הילד** עבור החשבון כדי לקבוע את רמת הגישה שלו ולהגדיר כללי גישה לדפי אינטרנט המתאימים לגיל.

רישום החומרה ביומן

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

- **אבחוני** - רישום מידע שנדרש להתאמה מפורטת של התוכנית.
- **מידע** תיעוד הודעות מסירת מידע, לרבות הודעות על חריגים מותרים וחסומים, בנוסף לכל הרשומות שלעיל.
- **אזהרה** - תיעוד שגיאות קריטיות והודעות אזהרה.
- **ללא** - לא יתועדו יומנים.

חריגות

יצירת חריגה יכולה להתיר או למנוע גישה של משתמש לאתרי אינטרנט שאינם נמצאים ברשימת החריגות. מצב זה שימושי כאשר ברצונך לשלוט בגישה לאתרי אינטרנט ספציפיים במקום להשתמש בקטגוריות. את החריגות שנוצרו עבור חשבון אחד ניתן להעתיק לחשבון אחר ושם להשתמש בהן. הדבר שימושי כשברצונך ליצור כללים זהים עבור ילדים באותו גיל.

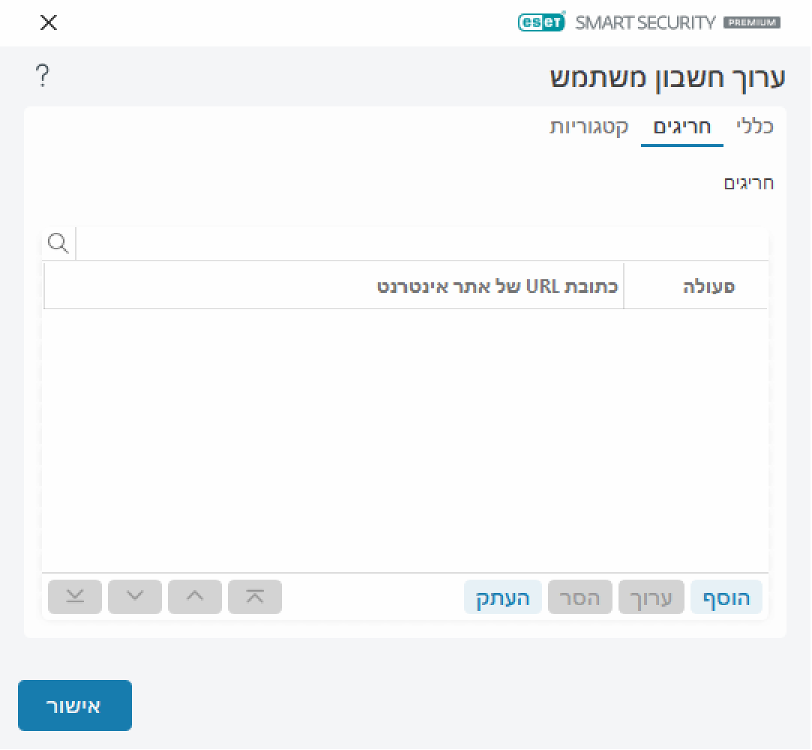
לחץ על **הוסף** כדי ליצור חריגה חדשה. ציין את ה**פעולה** (לדוגמה **חסימה**) באמצעות התפריט הנפתח, סוג **כתובת ה-URL של אתר אינטרנט** שאליו תוחל חריגה זו ולאחר מכן לחץ על **אישור**. החריגה תתווסף לרשימת החריגות הקיימות ומצבה יוצג.

הוסף יצירת חריגה חדשה.

ערוך באפשרותך לערוך את **כתובת ה-URL של אתר האינטרנט** או את ה**פעולה** של החריגה שנבחרה.

הסר הסרת החריגה שנבחרה.

העתק בחר בתפריט הנפתח משתמש שממנו ברצונך להעתיק את החריגה שנוצרה.

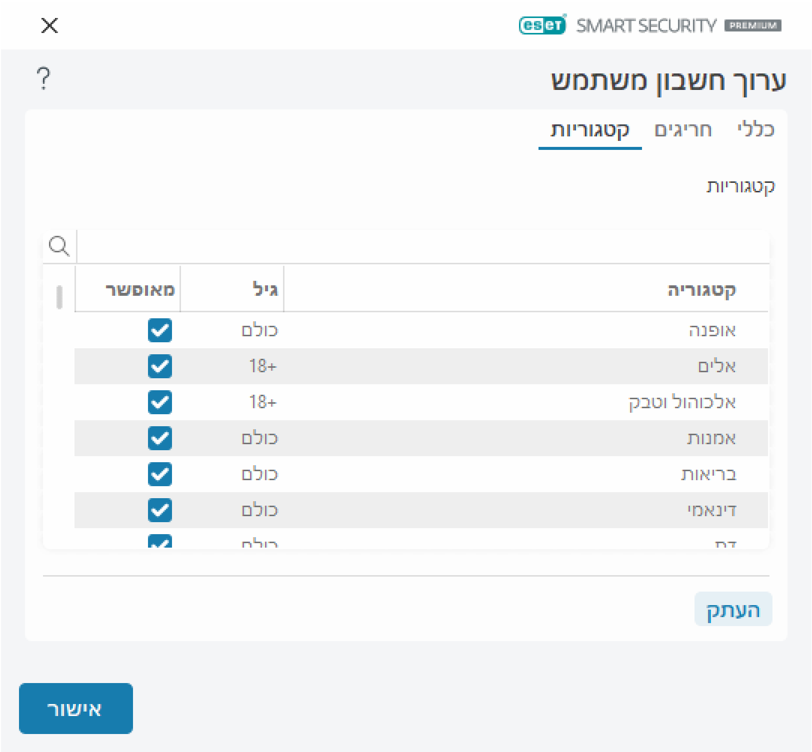


חריגות שהוגדרו מחליפות את הקטגוריות שהוגדרו עבור החשבונות שנבחרו. לדוגמה, אם הקטגוריה **חדשות** בחשבון נחסמה אך הגדרת דף אינטרנט של חדשות כחריגה מותרת, החשבון יוכל לגשת לדף האינטרנט המותר. תוכל להציג את כל השינויים שבוצעו כאן במקטע חריגות.

קטגוריות

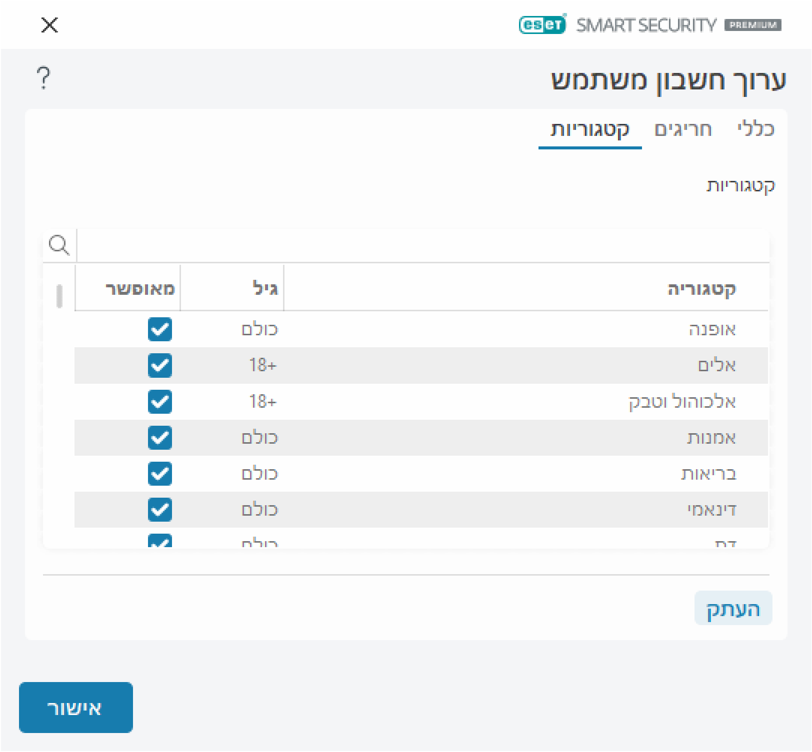
בכרטיסייה **קטגוריות**, באפשרותך להגדיר את הקטגוריות הכלליות של אתרי האינטרנט שברצונך לחסום או לאפשר עבור כל חשבון וחשבון. סמן את תיבת הסימון שלצד הקטגוריה כדי לאפשר אותה. אם תשאיר את תיבת הסימון ריקה, הקטגוריה לא תאופשר עבור חשבון זה.

העתק מאפשרת לך להעתיק רשימת קטגוריות חסומות או מותרות מחשבון קיים ששונה.



קטגוריות

סמן את תיבת הסימון בעמודה **מופעל** לצד הקטגוריה כדי להתיר אותה. אם תשאיר את תיבת הסימון ריקה, הקטגוריה לא תותר עבור חשבון זה.



להלן מספר דוגמאות לקטגוריות (קבוצות) שקיימת סבירות שמשתמשים אינם מודעים להן:

- **שונות** – בדרך-כלל כתובות IP פרטיות (מקומיות), כגון אינטרא-נט, 127.0.0.0/8, 192.168.0.0/16 וכו'. כשאתה מקבל קוד שגיאה 403 או 404, אתר האינטרנט גם תואם לקטגוריה זו.

- **לא מזוהה** – קטגוריה זו כוללת דפי אינטרנט שאינם מזוהים בשל שגיאה בחיבור למנגנון מסד הנתונים של בקרת ההורים.
- **לא מסווג** – דפי אינטרנט לא מוכרים שעדיין אינם קיימים במסד הנתונים של בקרת ההורים.
- **Dynamic** – דפי אינטרנט שמנתבים מחדש לדפים אחרים באתרי אינטרנט אחרים.

הגנת דפדפן

הגנת דפדפן היא שכבה נוספת של הגנה על האבטחה והפרטיות שלך, והיא מגנה על זיכרון הדפדפן מפני בדיקה על ידי תהליכים אחרים, מגבירה את ההגנה מפני כלים לרישום הקשות ומונעת הדבקת נתונים הקשורים לתשלום מקוון ששונו על ידי תוכנות זדוניות מהלוח לדפדפן המאובטח. כדי לקבוע את התצורה של הגנת הדפדפן, פתח את הגדרות מתקדמות < **הגנות** < **הגנת דפדפן** ובחר מבין אפשרויות התצורה הבאות:

- גלישה ושירותים בנקאיים בטוחים
- רשימת הרשאות להגנת הדפדפן
- מסגרת הדפדפן

גלישה ושירותים בנקאיים בטוחים

אפשר להגדיר את גלישה ושירותים בנקאיים בטוחים דרך הגדרות מתקדמות < **הגנות** < **הגנת דפדפן** < **גלישה ושירותים בנקאיים בטוחים**.

גלישה ושירותים בנקאיים בטוחים

הפעל גלישה ושירותים בנקאיים בטוחים – כאשר האפשרות מופעלת, כל דפדפני האינטרנט הנתמכים יתחילו לפעול במצב בטוח כברירת מחדל.

הגנת דפדפן

הפעל את האפשרות **אבטח את כל הדפדפנים** כדי להפעיל את כל דפדפני האינטרנט הנתמכים במצב מאובטח.

מצב התקנת הרחבות – מהתפריט הנפתח, אפשר לבחור אילו הרחבות מותר להתקין בדפדפן המאובטח על ידי ESET:

- **הרחבות חיוניות** – רק ההרחבות החיוניות ביותר שפותחו על ידי יצרן דפדפנים מסוים.
- **כל ההרחבות** – כל ההרחבות הנתמכות על ידי דפדפן מסוים.

> שינוי מצב ההתקנה של ההרחבות לא ישפיע על הרחבות דפדפן שהותקנו בעבר:

דפדפן מאובטח

הגנה מתקדמת על הזיכרון – אם אפשרות זו מאופשרת, המערכת תגן על זיכרון הדפדפן המאובטח מפני בחינה של תהליכים אחרים.

הגנה על המקלדת – אם אפשרות זו מאופשרת, המידע שתזין באמצעות מקלדת לדפדפן המאובטח יוסתר מאפליקציות אחרות. תכונה זו מגבירה את ההגנה מפני מעקבים אחרי הקשות מקלדת.

הגנת הלוח - אם האפשרות מופעלת, ESET Smart Security Premium ימנע הדבקה של נתונים שקשורים לתשלום מקוון ששונו על ידי תוכנות זדוניות מהלוח לדפדפן המאובטח. זה מבטיח הגנה מפני שינויים פוטנציאליים שנעשו על ידי תוכנות זדוניות.

מסגרת הדפדפן התאם אישית את הגדרות התצוגה עבור מסגרת הדפדפן בדפדפנים מוגנים.

רשימת ההרשאות להגנת דפדפן - נהל קבצים שנוספו לרשימת ההרשאות להגנת הדפדפן.

פרטיות ואבטחה בדפדפן

הפעלת פרטיות ואבטחה בדפדפן - על ידי השבתת תכונה זו, ההתקנה של ההרחבה 'פרטיות ואבטחה בדפדפן' תוסר מכל הדפדפנים הנתמכים בכל חשבונות Windows.

הצג התראות של פרטיות ואבטחה בדפדפן - אם האפשרות פועלת, ESET Smart Security Premium יציג את ההתראות של פרטיות ואבטחה בדפדפן.

סורק קובצי Script בדפדפן

הפעל סריקה מתקדמת של קובצי Script לדפדפן - אם האפשרות מופעלת, סורק האנטי-וירוס יבדוק את כל תוכניות ה-JavaScript שמופעלות על ידי דפדפני אינטרנט.

00

בקרת התקנים

ESET Smart Security Premium מספק בקרת מכשיר אוטומטית (CD/DVD/USB/וכדומה). 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:

- התקן אחסון (HDD, דיסק נשלף בחיבור USB)
- תקליטור/dvd
- מדפסת USB
- אחסון בחיבור FireWire
- התקן Bluetooth
- קורא כרטיסים חכמים
- התקן הדמיה
- מודם
- יציאה LPT/COM
- מכשיר נייד (מכשירים שמופעלים באמצעות סוללות כמו נגני מדיה, סמארטפונים, התקני USB וכדומה)
- כל סוגי ההתקנים

את אפשרויות ההגדרה של בקרת התקנים ניתן לשנות דרך הגדרות מתקדמות > **הגנות** > **בקרת התקנים**.

לחץ על המתג **הפעל בקרת התקנים** כדי להפעיל את תכונת בקרת ההתקנים ב-ESET Smart Security Premium; יש

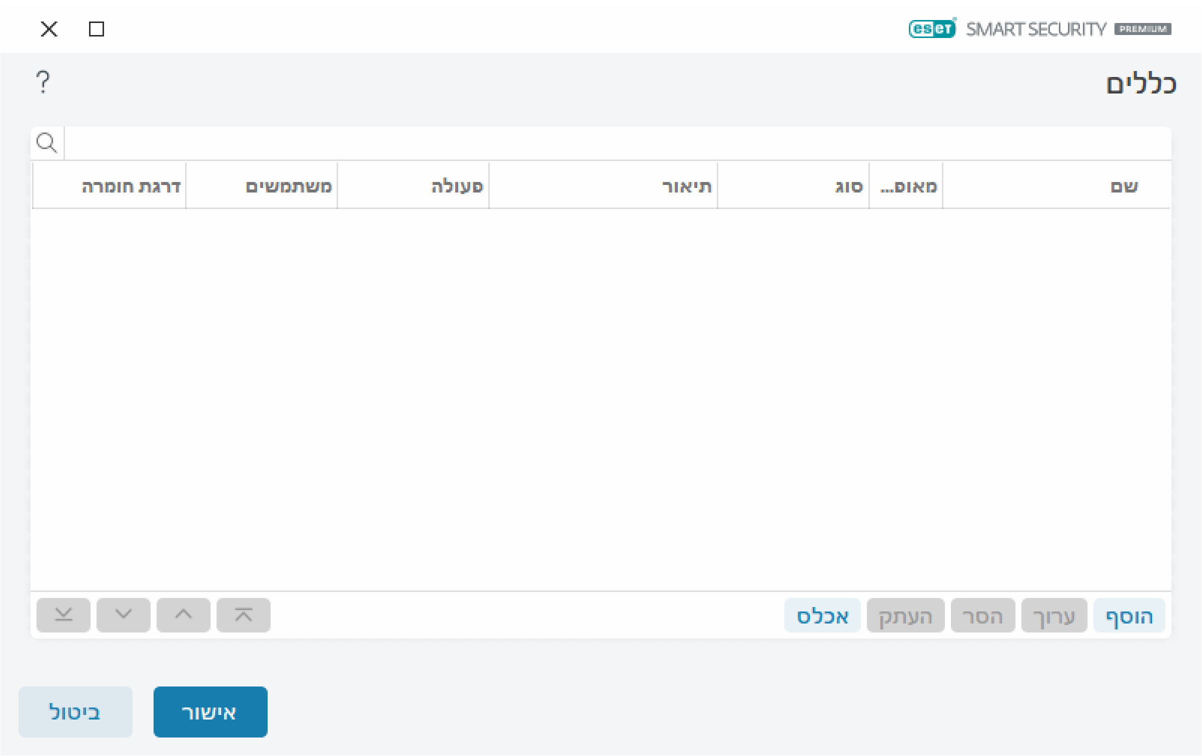
להפעיל מחדש את המחשב כדי ששינוי זה ייכנס לתוקף. לאחר ההפעלה של בקרת ההתקנים, יהיה באפשרותך להגדיר **כללים** בחלון עורך הכללים.

> באפשרותך ליצור קבוצות התקנים שונות, שבהן יוחלו כללים שונים. באפשרותך גם ליצור רק קבוצת התקנים אחת שבה יוחל הכלל עם הפעולה **אפשר** או **חסימת כתיבה**. 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.

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. ראה גם הוספת כללי בקרת התקנים.

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 **מאופשר** משביתה או מאפשרת כלל; שימושית כשברצונך להשאיר את הכלל.

לחץ על **אכלס** כדי לאכלס באופן אוטומטי פרמטרים של מדיה נשלפת עבור התקני מדיה שמחוברים למחשב שלך.

הכללים מפורטים לפי סדר עדיפות כאשר כללים בעדיפות גבוהה יותר מופיעים למעלה. ניתן להעביר כללים על ידי

לחיצה על **בראש הרשימה/למעלה/למטה/בתחתית הרשימה** וניתן להעביר אותם בנפרד או בקבוצות.

ניתן לצפות ברשומות יומן [בחלון התוכנית הראשי] > **כלים** > [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 ברצונך לראות את כל המכשירים המוסתרים, בחר **הצג מכשירים מוסתרים**.

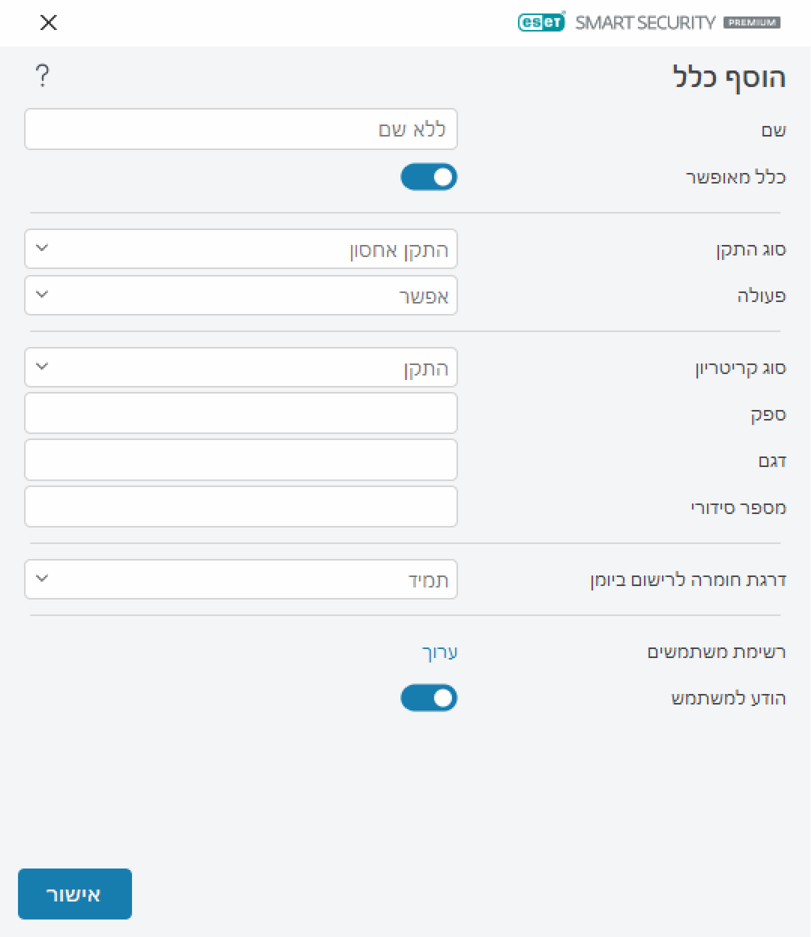
בחר התקן מרשימת ההתקנים שזוהו ולחץ על **אישור** כדי [להוסיף כלל בקרת התקנים] עם מידע שהוגדר מראש (ניתן להתאים את כל ההגדרות).

התקנים במצב צריכת חשמל נמוכה (שינה) מסומנים בסמל אזהרה . כדי לאפשר את הלחצן **אישור** ולהוסיף כלל עבור התקן זה:

- חבר מחדש את ההתקן
- השתמש בהתקן (לדוגמה, הפעל את האפליקציה 'מצלמה' ב-Windows כדי להעיר מצלמת אינטרנט)

הוספת כללי בקרת התקנים

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



לזיהוי טוב יותר, הזן תיאור של הכלל בשדה **שם**. לחץ על המתג שלצד **כלל מופעל** כדי להפעיל או להשבית את הכלל הזה; מצב זה שימושי כשאינך רוצה למחוק את הכלל לצמיתות.

סוג התקן

בחר את סוג ההתקן החיצוני בתפריט הנפתח (אחסון בדיסק/התקן נייד/Bluetooth/FireWire/...). 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 אחת או יותר מההגדרות הבאות המתייחסות לזכויות:

- **אפשר** - תותר גישה מלאה להתקן.
- **חסימה** - הגישה להתקן תיחסם.
- **חסימת כתיבה** - 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 במקרה של חיבורים 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 **חסימת כתיבה** 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 שונים. כל הפרמטרים תלויי-רישיות ותומכים בתווים כלליים (*, ?):

- **ספק** - סינון לפי שם הספק או המזהה 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.

> אם הפרמטרים הללו אינם מוגדרים, הכלל יתעלם משדות אלו בעת ביצוע ההתאמה. הפרמטרים של סינון בכל שדות הטקסט הם תלויי-רישיות ותומכים בתווים כלליים (סימן שאלה (?) מייצג תו יחיד וכוכבית (*) מייצגת מחרוזת של אפס תווים או יותר).

> 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 Smart Security Premium שומר את כל האירועים החשובים בקובץ יומן, אותו ניתן להציג ישירות מהתפריט הראשי. לחץ על **כלים** > **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.

רשימת משתמשים

אפשר להגביל את הכללים למשתמשים מסוימים או לקבוצות משתמשים מסוימות על ידי הוספתם לרשימת משתמשים בלחיצה על **ערוך** לצד **רשימת משתמשים**.

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

הגבלות לגבי רשימות משתמשים

לא ניתן להגדיר את רשימת המשתמשים עבור כללים עם סוגי מכשירים ספציפיים:

- מדפסת USB
- התקן Bluetooth
- קורא כרטיסים חכמים
- סורקים ומצלמות
- מודם
- יציאת LPT/COM

הודע למשתמש אם חובר התקן שנחסם על ידי כלל קיים, יוצג חלון התראה.

קבוצות התקנים

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 קבוצה כדי להציג התקנים בחלונית השמאלית.

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 התקנים מתוך הרשימה המאוכלסת כדי להוסיף אותם לקבוצה על-ידי לחיצה על **אישור**.

רכיבי בקרה

הוספה באפשרותך להוסיף קבוצה על-ידי הקלדת שמה, או התקן לקבוצה קיימת, 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 מכשירים מקובץ טקסט. ייבוא מכשירים מקובץ טקסט דורש עיצוב נכון:

- כל התקן יתחיל בשורה חדש.
- **ספק**, **דגם** ו**מספר סידורי** חייבים להיות נוכחים עבור כל מכשיר ולהיות מופרדים בפסיקים.

הנה דוגמה לתוכן קובץ הטקסט:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

ייצוא מייצא רשימת מכשירים לקובץ.

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

הוסף התקן

לחץ על **הוספה** בחלון השמאלי כדי להוסיף התקן לקבוצה קיימת. ניתן להשתמש בפרמטרים הבאים, המוצגים להלן, לצורך התאמה מפורטת של כללים להתקנים שונים. כל הפרמטרים תלויי-רישיות ותומכים בתווים כלליים (*, ?):

- **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.
- **תיאור** ⍰ תיאור משלך של ההתקן כדי להקל על ארגון רשימת ההתקנים.

> i אם הפרמטרים הללו אינם מוגדרים, הכלל יתעלם משדות אלו בעת ביצוע ההתאמה. הפרמטרים של סינון בכל שדות הטקסט הם תלויי-רישיות ותומכים בתווים כלליים (סימן שאלה [?] מייצג תו יחיד וכוכבית [*] מייצגת מחרוזת של אפס תווים או יותר).

לחץ על **אישור** לשמירת השינויים. לחץ על **ביטול** כדי לצאת מהחלון **קבוצות התקנים** מבלי לשמור את השינויים.

> i לאחר יצירת קבוצת התקנים, יש להוסיף כלל בקרת התקנים חדש עבור קבוצת ההתקנים שנוצרה ולבחור את הפעולה שתינקט.

שים לב שכל הפעולות (ההרשאות) זמינות עבור כל סוגי המכשירים. כל ארבע הפעולות זמינות אם זהו התקן מסוג אחסון. עבור התקנים שאינם מסוג אחסון, רק שלוש אפשרויות זמינות (לדוגמה, האפשרות **חסימת כתיבה** אינה זמינה עבור Bluetooth, ולכן ניתן רק להתיר, לחסום או להזהיר מפני התקני Bluetooth).

הגנת מצלמת אינטרנט

הגנת מצלמת אינטרנט מיידעת אותך על תהליכים ואפליקציות שניגשים למצלמת האינטרנט של המחשב שלך. כאשר אפליקציה מנסה לגשת למצלמה שלך, תקבל הודעה שבה תוכל **לאפשר** או **לחסום** את הגישה. צבע חלון ההתראה תלוי במוניטין של האפליקציה.

אפשר לשנות את אפשרויות ההגדרה של הגנת מצלמת אינטרנט תחת הגדרות מתקדמות > **הגנות** > **בקרת התקנים** > **הגנת מצלמת אינטרנט**.

כדי להפעיל את התכונה 'הגנת מצלמת אינטרנט' ב-ESET Smart Security Premium, הפעל את המתג שלצד **הפעל הגנת מצלמת אינטרנט**.

לאחר ההפעלה של הגנת מצלמת אינטרנט, ה**כללים** יהפכו לפעילים, ויאפשרו לך לפתוח את חלון עורך הכללים.

כדי לבטל התראות עבור אפליקציות עם כלל קיים ששונו אך שעדיין יש להן חתימה דיגיטלית חוקית (לדוגמה, עדכון אפליקציות), העבר את המתג שלצד **השבת התראות גישה למצלמת אינטרנט עבור אפליקציות שהשתנו** למצב פעיל.

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:

- **אפשר גישה**
- **חסום גישה**
- **שאל** (הצגת שאלה למשתמש בכל פעם שאפליקציה מנסה לגשת למצלמת אינטרנט)

בטל את בחירת תיבת הסימון בעמודה '**הודע**' כדי להפסיק לקבל התראות כשאפליקציות ניגשות אל מצלמת האינטרנט.

> **הנחיות מאוירות**
> כיצד ליצור ולערוך כללי מצלמת אינטרנט ב-ESET Smart Security Premium.

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 **ThreatSense** בהגדרות מתקדמות 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 אתחול המערכת
- הגנה על מסמכים
- הגנה על 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 תוכנות זדוניות 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 הגרסאות הקודמות של מודול מנגנון האיתור. 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 הפעולה של ESET Smart Security Premium בעת ניקוי אובייקטים. ישנן 4 רמות ניקוי:

ThreatSense כולל את רמות התיקון (כלומר, הניקוי) הבאות.

תיקון ב-ESET Smart Security Premium

תיאור	דרגת ניקוי
נסה לתקן את האיתור בעת ניקוי אובייקטים ללא התערבות של משתמש הקצה. במקרים נדירים (לדוגמה, קובצי מערכת), אם לא ניתן לתקן את האיתור, האובייקט המדווח נשאר במיקומו המקורי.	**תקן את האיתור תמיד**
נסה לתקן את האיתור בעת ניקוי אובייקטים ללא התערבות של משתמש הקצה. במקרים מסוימים (לדוגמה, קובצי מערכת או ארכיונים עם קבצים נקיים ונגועים), אם לא ניתן לתקן איתור, האובייקט המדווח נשאר במיקומו המקורי.	**תקן את האיתור אם בטוח, אחרת השאר**
נסה לתקן את האיתור בעת ניקוי אובייקטים. במקרים מסוימים, אם לא ניתן לבצע פעולה, משתמש הקצה מקבל התראה אינטראקטיבית ועליו לבחור בפעולת תיקון (לדוגמה, הסרה או התעלמות). הגדרה זו מומלצת במרבית המקרים.	**תקן את האיתור אם בטוח, אחרת שאל**
משתמש הקצה מקבל חלון אינטראקטיבי בעת ניקוי אובייקטים ועליו לבחור פעולת תיקון (לדוגמה, הסרה או התעלמות). רמה זו תוכנה עבור משתמשים מתקדמים, שיודעים באילו פעולות לנקוט במקרה של איתור.	**שאל תמיד את משתמש הקצה**

החרגות

סיומת היא החלק של שם הקובץ שמופרד ממנו באמצעות נקודה. סיומת מגדירה את סוג הקובץ ותכולתו. במקטע זה של הגדרות ThreatSense אפשר 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.

תעד את כל האובייקטים – יומן הסריקות יציג את כל הקבצים שנסרקו בארכיונים של חילוץ עצמי, גם את אלה שלא הושפעו (הדבר עלול ליצור נתונים רבים ביומן הסריקות ולהגדיל את קובץ יומן הסריקות).

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 קבצים באובייקט של גורם מכיל (כגון ארכיון RAR/ZIP או הודעת דוא"ל עם מספר קבצים מצורפים). הגדרה זו אינה חלה על קבצים נפרדים. אם ערך המוגדר על-ידי משתמש הוזן כאן וזמן זה חלף, הסריקה תסתיים בהקדם האפשרי, בין אם הסריקה של כל קובץ באובייקט של גורם מכיל ובין אם היא לא הסתיימה.
במקרה של ארכיון המכיל קבצים רבים, הסריקה לא תסתיים לפני חילוץ של קובץ מהארכיון (לדוגמה, כאשר ערך שהוגדר על-ידי המשתמש הוא 3 שניות, אך החילוץ של קובץ נמשך 5 שניות). שאר הקבצים בארכיון לא ייסרקו בחלוף זמן זה.
כדי להגביל את זמן הסריקה, כולל קובצי ארכיון גדולים יותר, השתמש באפשרויות **גודל אובייקט מקסימלי** ו**גודל מקסימלי של קובץ בארכיון** (לא מומלץ עקב סיכוני אבטחה אפשריים).

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. הערך המרבי הוא **3GB**.

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

רמות ניקוי

כדי לשנות את הגדרות רמת הניקוי עבור מודול ההגנה הרצוי, הרחב את **ThreatSense** (לדוגמה, **הגנה בזמן אמת על מערכת קבצים**) ולאחר מכן בחר **רמת ניקוי** מהתפריט הנפתח.

ThreatSense כולל את רמות התיקון (כלומר, הניקוי) הבאות.

תיקון ב-ESET Smart Security Premium

תיאור	דרגת ניקוי
נסה לתקן את האיתור בעת ניקוי אובייקטים ללא התערבות של משתמש הקצה. במקרים נדירים (לדוגמה, קובצי מערכת), אם לא ניתן לתקן את האיתור, האובייקט המדווח נשאר במיקומו המקורי.	**תקן את האיתור תמיד**
נסה לתקן את האיתור בעת ניקוי אובייקטים ללא התערבות של משתמש הקצה. במקרים מסוימים (לדוגמה, קובצי מערכת או ארכיונים עם קבצים נקיים ונגועים), אם לא ניתן לתקן איתור, האובייקט המדווח נשאר במיקומו המקורי.	**תקן את האיתור אם בטוח, אחרת השאר**
נסה לתקן את האיתור בעת ניקוי אובייקטים. במקרים מסוימים, אם לא ניתן לבצע פעולה, משתמש הקצה מקבל התראה אינטראקטיבית ועליו לבחור בפעולת תיקון (לדוגמה, הסרה או התעלמות). הגדרה זו מומלצת במרבית המקרים.	**תקן את האיתור אם בטוח, אחרת שאל**
משתמש הקצה מקבל חלון אינטראקטיבי בעת ניקוי אובייקטים ועליו לבחור פעולת תיקון (לדוגמה, הסרה או התעלמות). רמה זו תוכנה עבור משתמשים מתקדמים, שיודעים באילו פעולות לנקוט במקרה של איתור.	**שאל תמיד את משתמש הקצה**

סיומות קבצים שלא ייכללו בסריקה

סיומות קבצים שלא ייכללו הן חלק מה ThreatSense. כדי להגדיר סיומות קבצים שלא ייכללו, לחץ על **ThreatSense** בהגדרות מתקדמות לכל מודול שמשתמש בטכנולוגיה של ThreatSense.

סיומת היא החלק של שם הקובץ המופרד ממנו באמצעות נקודה. סיומת מגדירה את סוג הקובץ ותכולתו. במקטע זה של הגדרת ThreatSense אפשר להגדיר את סוגי הקבצים לסריקה.

> i 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 `.eml`, `.edb` ו-`.tmp` בעת שימוש בשרתי Microsoft Exchange.

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 edb;eml;tmp).
באפשרותך להשתמש בסימן מיוחד (סימן שאלה). סימן השאלה מייצג כל סמל שהוא (לדוגמה ?db).

כדי לראות את הסיומת המדויקת (אם קיימת) של קובץ במערכת הפעלה של Windows, עליך לבחור בתיבת הסימון **סיומות שמות קבצים** שנמצאת בסייר **Windows** > **תצוגה** (כרטיסייה).

פרמטרים נוספים של ThreatSense

כדי לערוך את ההגדרות האלה פתח את הגדרות מתקדמות > **הגנה בזמן אמת על מערכת קבצים** > **הגנה בזמן אמת על מערכת קבצים** > **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 Smart Security Premium משתמש בהיוריסטיקה 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) ועל **קובצי Packer 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 הארכיון, בטל את הבחירה באפשרות **הגדרות ברירת מחדל של סריקת קובצי ארכיון**.

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.

כלים

באפשרותך לקבוע תצורה של הגדרות מתקדמות עבור תכונות המציעות אבטחה נוספת ועוזרות לפשט את הניהול של ESET Smart Security Premium דרך הגדרות מתקדמות > **כלים**.

- Microsoft Windows® Update
- ESET CMD
- רשומות יומן
- מצב משחק
- אבחון

Microsoft Windows® Update

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 Smart Security Premium מודיע לך על עדכונים חסרים בהתאם לרמה שתציין בהגדרות מתקדמות > **כלים**. 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.

חלון דו-שיח עדכוני מערכת

אם קיימים עדכונים עבור מערכת ההפעלה שלך, ESET Smart Security Premium יציג התראה בחלון התוכנית הראשי > **מבט כולל**. לחץ על **מידע נוסף** כדי לפתוח את החלון 'עדכוני מערכת'.

חלון עדכוני המערכת מציג את רשימת העדכונים הזמינים המוכנים להורדה ולהתקנה. סוג העדכון מוצג לצד שם העדכון.

לחץ לחיצה כפולה על שורת עדכון כלשהי כדי להציג את החלון פרטי עדכון עם מידע נוסף.

לחץ על **הפעל עדכון מערכת** כדי להוריד ולהתקין את כל עדכוני מערכת ההפעלה הזמינים.

פרטי עדכון

חלון עדכוני המערכת מציג את רשימת העדכונים הזמינים המוכנים להורדה ולהתקנה. רמת העדיפות של העדכון מוצגת לצד שם העדכון.

לחץ על **הפעל עדכון מערכת** כדי להתחיל להוריד ולהתקין עדכונים של מערכת ההפעלה.

לחץ באמצעות לחצן העכבר הימני על שורת עדכון כלשהי ולחץ על **הצג מידע** כדי להציג חלון חדש עם מידע נוסף.

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 Smart Security Premium 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 Smart Security Premium. באפשרותך לבצע זאת באופן ידני או ליצור קובץ Script למטרות אוטומציה.

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.

פקודת ייצוא הגדרות:

```
ecmd /getcfg c:\config\settings.xml
```

פקודת ייבוא הגדרות:

```
ecmd /setcfg c:\config\settings.xml
```

ניתן להפעיל פקודות ecmd מתקדמות באופן מקומי בלבד.

חתימה על קובץ תצורה *.xml*:

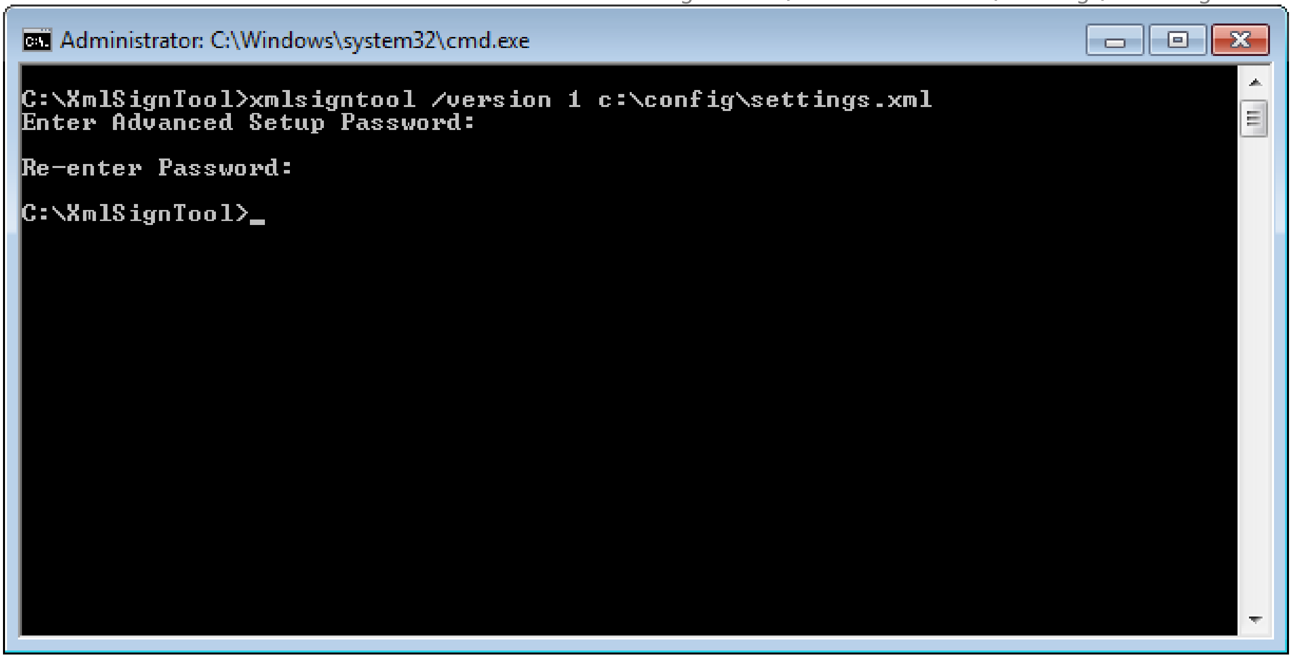
1. הורד את קובץ ההפעלה XmlSignTool.
2. פתח את שורת הפקודה של Windows (cmd) על-ידי בחירה באפשרות **הפעל כמנהל**.
3. נווט אל מיקום השמירה של `xmlsigntool.exe`
4. בצע פקודה לחתימה על קובץ תצורה *.xml*, שימוש: `<xmlsigntool /version 1|2 <xml_file_path`

הערך של הפרמטר `/version` תלוי בגרסה של ESET Smart Security Premium שברשותך. השתמש ב- `/version 1` עבור גרסאות של ESET Smart Security Premium שקודמות לגרסה 11.1. השתמש ב-`/version 2` עבור הגרסה הנוכחית של ESET Smart Security Premium.

5. הזן את הסיסמה להגדרות מתקדמות והזן אותה שנית לאישור כאשר תופיע הנחיה לכך בכלי XmlSignTool. קובץ התצורה *.xml* יהיה חתום כעת וניתן יהיה להשתמש בו לביצוע ייבוא במופע אחר של ESET Smart Security Premium באמצעות ESET CMD ושיטת ההרשאה באמצעות סיסמה.

פקודה לחתימה על קובץ תצורה מיוצא:

`xmlsigntool /version 2 c:\config\settings.xml`



אם הסיסמה ל[הגדרות 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 Smart Security Premium לפני ביצוע הייבוא.

לא מומלץ לאפשר ESET CMD ללא הרשאה מאחר שהדבר יאפשר ייבוא של תצורות שאינן חתומות. הגדר את הסיסמה ב[הגדרה מתקדמת](#) > **ממשק משתמש** > **הגדרות גישה** כדי למנוע מהמשתמשים מלבצע שינויים בלתי מורשים.

רשומות יומן

באפשרותך למצוא את תצורת הרישום של ESET Smart Security Premium דרך [הגדרה מתקדמת](#) > **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 וכדומה).

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.

> i 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].

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 להפסיק 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 ב[חלון התוכנית הראשי] תחת **הגדרות** > **הגנה על המחשב** על-ידי לחיצה על או על שלצד **מצב משחק**. הפעלת מצב משחק מציבה סיכון אבטחה אפשרי, ולכן סמל סטטוס ההגנה בשורת המשימות יהפוך לכתום ויציג אזהרה. תוכל לראות אזהרה זו גם ב[חלון התוכנית הראשי], שבו יופיע הכיתוב **מצב משחק מופעל** בכתום.

הפעל את האפשרות **הפעל מצב משחק אוטומטית בעת הפעלת יישומים במצב מסך מלא** תחת [הגדרות מתקדמות] > **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.

> i 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 ב[מצב 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.

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 Smart Security Premium.

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 ביומן בהודעות שיווקיות – תעד את כל האירועים הקשורים להודעות שיווקיות בתוך המוצר.

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 לצורך הגנת דפדפן - רשום את כל האירועים שמתרחשים ב'גלישה ושירותים בנקאיים בטוחים'.

אפשר רישום מתקדם ביומן עבור סריקת מחשב – תעד את כל האירועים המתרחשים בעת סריקת קבצים ותיקיות על-ידי סריקת מחשב.

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 של Direct Cloud – תעד את כל האירועים המתרחשים ב-ESET LiveGrid®. פעולה זו תוכל לסייע למפתחים לאבחן ולתקן בעיות הקשורות ל-ESET LiveGrid®.

הפעל רישום מתקדם ביומן של הגנה על מסמכים – תעד את כל האירועים המתרחשים בהגנה על מסמכים כדי לאפשר אבחון בעיות ופתרונן.

הפעל רישום מתקדם ביומן של הגנת לקוח דוא"ל – תעד את כל האירועים המתרחשים בהגנת לקוח דוא"ל ובתוסף של לקוח דוא"ל כדי לאפשר אבחון בעיות ופתרונן.

הפעל רישום מתקדם ביומן של ESET LiveGuard – תעד את כל האירועים המתרחשים ב-ESET LiveGuard כדי לאפשר

אבחון בעיות ופתרונן.

אפשר רישום מתקדם ביומן עבור רכיב ליבה תעד את כל האירועים המתרחשים ברכיב הליבה של ESET (ekrn).

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

אפשר מעקב זיכרון תעד את כל האירועים שיעזרו למפתחים לאבחן דליפות בזיכרון.

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 סורק תעבורת רשת - רשום את כל הנתונים העוברים דרך סורק תעבורת הרשת בפורמט PCAP כדי לעזור למפתחים לאבחן ולתקן בעיות שקשורות לסורק תעבורת הרשת.

אפשר רישום מתקדם ביומן עבור מערכת ההפעלה תעד 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.

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 ביומן עבור הודעות דחיפה תעד את כל האירועים המתרחשים במהלך העברת הודעות דחיפה.

אפשר רישום מתקדם ביומן עבור הגנה בזמן אמת על מערכת קבצים תעד את כל האירועים המתרחשים בעת סריקת קבצים ותיקיות על-ידי הגנה בזמן אמת על מערכת קבצים.

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

רשומות היומן נמצאות ב-*C:\ProgramData\ESET\ESET Security\Diagnostics*.

תמיכה טכנית

בעת יצירת קשר עם התמיכה הטכנית של ESET מתוך ESET Smart Security Premium, באפשרותך לשלוח את נתוני תצורת המערכת. לחץ על **שלח תמיד** בתפריט הנפתח של **שלח נתוני תצורת מערכת** כדי לשלוח את הנתונים באופן אוטומטי, או לחץ על **שאל לפני שליחה** כדי להציג בקשה לפני שליחת נתונים.

קישוריות

ברשתות ספציפיות, שרת Proxy יכול לתווך תקשורת בין המחשב שלך לאינטרנט. אם אתה משתמש בשרת Proxy, עליך להגדיר את ההגדרות הבאות. אחרת, ESET Smart Security Premium והמודולים שלו לא יכולים להתעדכן באופן אוטומטי. ב-ESET Smart Security Premium, הגדרת שרת Proxy זמינה בשני מקטעים שונים של הגדרות מתקדמות.

ניתן לקבוע את ההגדרות של שרת Proxy דרך הגדרות מתקדמות > **קישוריות** > **שרת Proxy**. ציון שרת ה-proxy ברמה זו קובע את ההגדרות הכלליות של שרתי proxy ב-ESET Smart Security Premium כולו. הפרמטרים כאן ישמשו את כל המודולים שצריכים חיבור לאינטרנט.

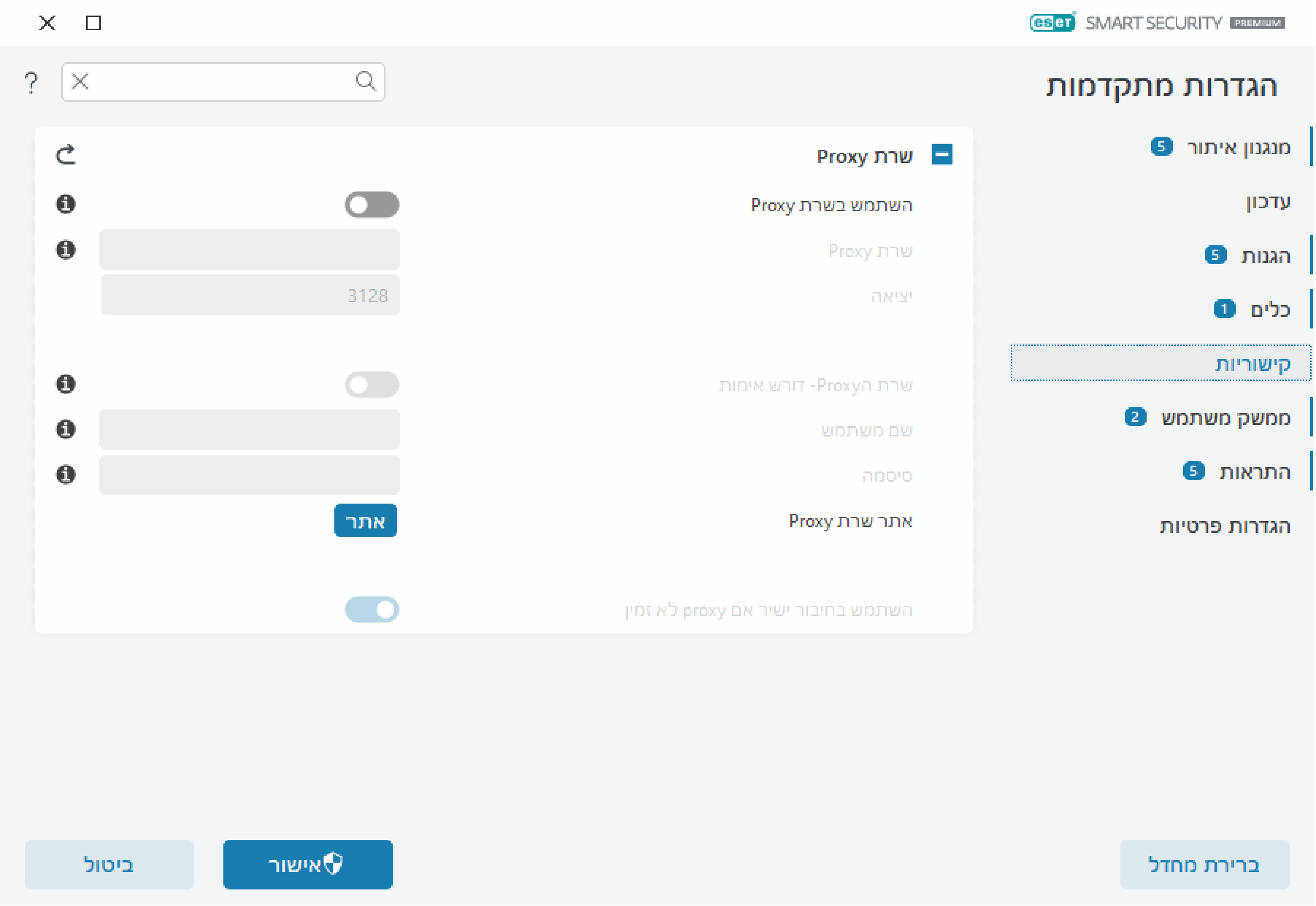
כדי לציין הגדרות שרת Proxy גלובליות, הפעל את **השתמש בשרת Proxy** והקלד את הכתובת של **שרת Proxy** יחד עם מספר **היציאה** של שרת ה-Proxy.

אם התקשורת עם שרת ה-proxy מחייבת אימות, בחר **שרת Proxy מחייב אימות** והזן **שם משתמש** חוקי ו**סיסמה** בשדות המתאימים. לחץ על **זיהוי שרת Proxy** כדי לזהות ולאכלס הגדרות שרת Proxy באופן אוטומטי. ESET Smart Security Premium יעתיק את הפרמטרים שצוינו באפשרויות אינטרנט עבור Internet Explorer או Google Chrome.

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

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

אפשר לקבוע את הגדרות שרת ה-Proxy גם דרך הגדרות מתקדמות > **עדכון** > **פרופילים** > **עדכונים** > **אפשרויות חיבור** על-ידי בחירה באפשרות **התחברות דרך שרת Proxy** בתפריט הנפתח **מצב Proxy**. תצורה זו חלה רק על עדכונים, והיא מומלצת למחשבים ניידים שמקבלים עדכוני מודולים ממיקומים מרוחקים. למידע נוסף, ראה הגדרות עדכון מתקדמות.



ממשק משתמש

כדי להגדיר את אופן הפעולה הגרפי של ממשק המשתמש (GUI) של התוכנית, פתח את הגדרות מתקדמות > **ממשק משתמש**.

ניתן להתאים את המראה החזותי ואת האפקטים של התוכנית במסך ההגדרות המתקדמות של רכיבי ממשק

המשתמש.

כדי לספק אבטחה מרבית של תוכנת האבטחה שלך, באפשרותך למנוע הסרת התקנה או שינויים לא מורשים על ידי הגנה על ההגדרות באמצעות סיסמה עם כלי הגדרות הגישה.

> i כדי להגדיר את אופן הפעולה של התראות מערכת, התראות על איתור וסטטוסים של אפליקציות, עיין במקטע התראות.

אלמנטי ממשק משתמש

באפשרותך להתאים את סביבת העבודה (ממשק המשתמש הגרפי) של ESET Smart Security Premium לצרכיך מהתפריט הגדרות מתקדמות > **ממשק משתמש** > **רכיבי ממשק משתמש**.

מצב צבע בחר את ערכת הצבעים של ממשק המשתמש הגרפי של ESET Smart Security Premium מהתפריט הנפתח:

- **זהה לצבע המערכת** בחר באפשרות זו כדי להגדיר את ערכת הצבעים של ESET Smart Security Premium בהתאם להגדרות מערכת ההפעלה.
- **כהה** ערכת הצבעים של ESET Smart Security Premium תהיה כהה (מצב כהה).
- **בהיר** ערכת הצבעים של ESET Smart Security Premium תהיה רגילה ובהירה.

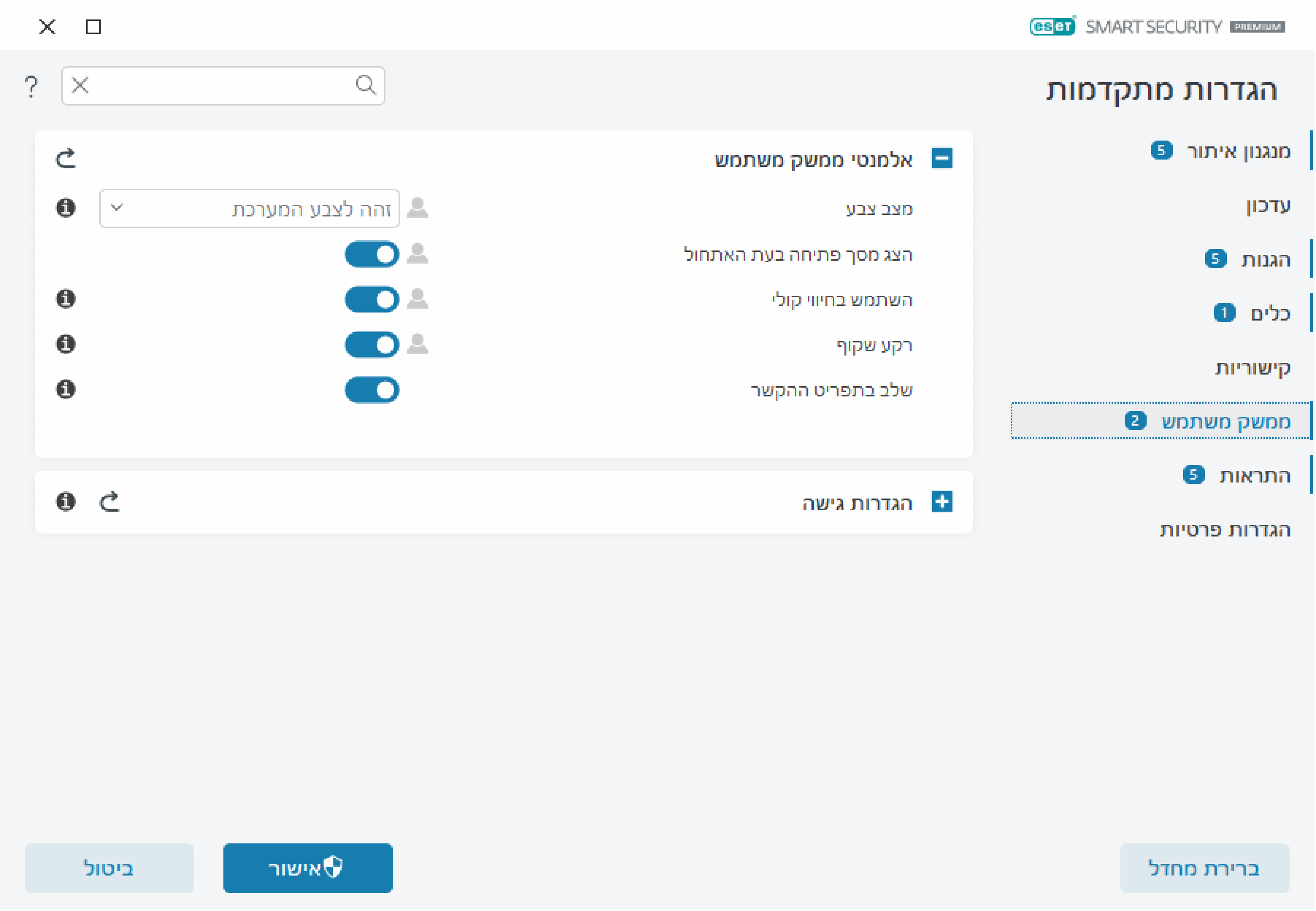
> i ניתן גם לבחור את ערכת הצבעים של ESET Smart Security Premium GUI בפינה הימנית העליונה של חלון התוכנית הראשי.

הצג מסך פתיחה בעת האתחול בחר באפשרות זו כדי להציג את מסך הפתיחה של ESET Smart Security Premium בעת האתחול.

השתמש בחיווי קולי משמיע צליל כשמתרחשים אירועים חשובים במהלך סריקה, לדוגמה כאשר מתגלה איום או כאשר הסריקה מסתיימת.

רקע שקוף בחר באפשרות זו כדי לאפשר אפקט של רקע שקוף בחלון התוכנית הראשי. רקע שקוף זמין רק עבור הגרסאות העדכניות ביותר של Windows (RS4 ואילך).

שלב בתפריט ההקשר שלב את רכיבי הבקרה של ESET Smart Security Premium בתפריט ההקשר.



הגדרות גישה

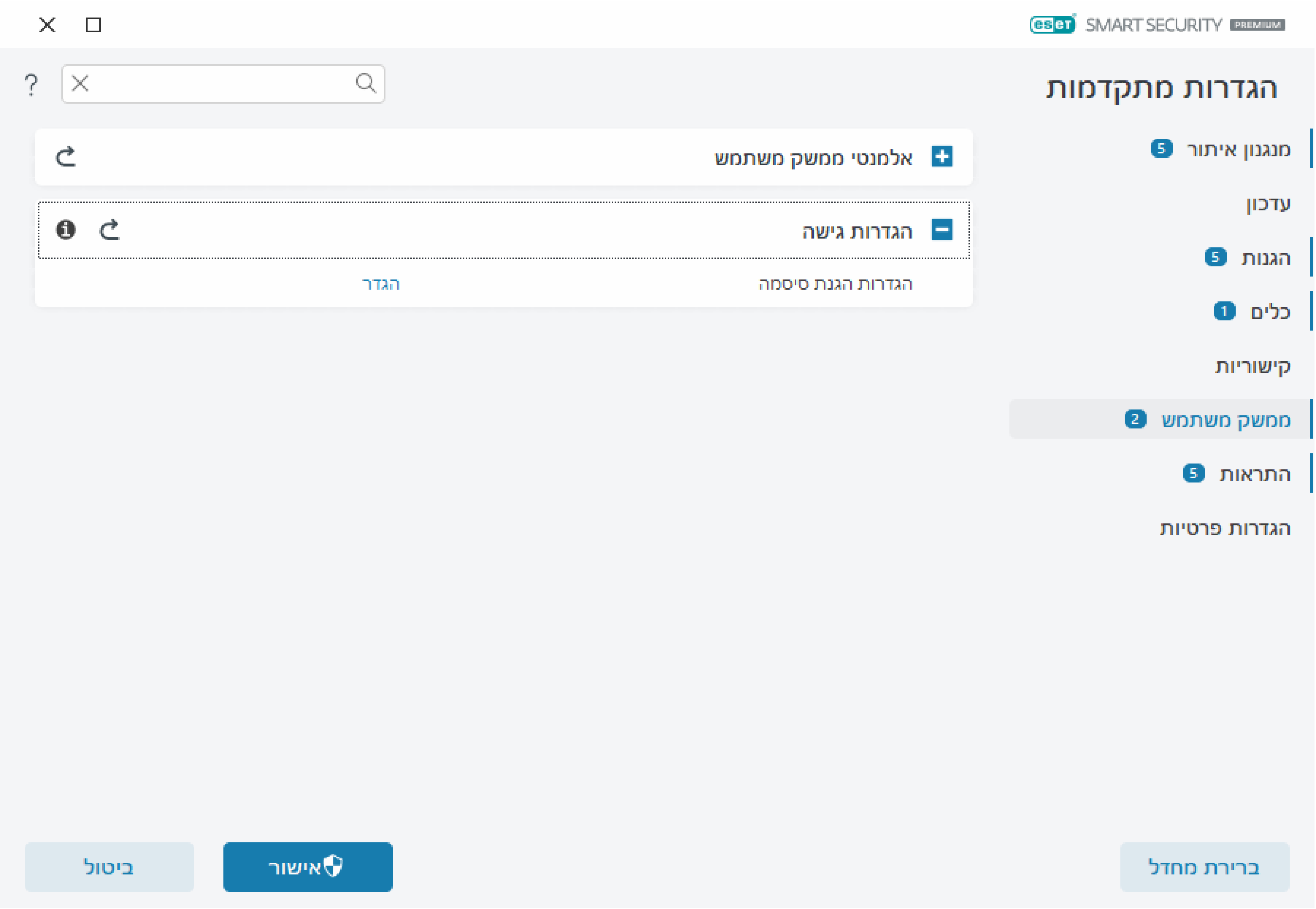
ההגדרות של ESET Smart Security Premium הן חלק מכריע של מדיניות האבטחה שלך. שינויים בלתי מורשים עלולים לסכן את יציבות המערכת שלך וההגנה עליה. כדי להימנע משינויים בלתי מורשים, ניתן להגן על הפרמטרים של תכנית ההתקנה ועל הסרת ההתקנה של ESET Smart Security Premium באמצעות סיסמה. ניתן לקבוע את התצורה של הגדרת הגישה דרך הגדרות מתקדמות < **ממשק משתמש** < **הגדרת גישה**.

כדי להגדיר סיסמה להגנה על פרמטרים של תכנית ההתקנה ועל הסרת ההתקנה של ESET Smart Security Premium, לחץ על **הגדר** לצד **הגדרות הגנה 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** והזן את כתובת הדוא"ל שבה השתמשת לרישום המינוי. ESET תשלח לך דוא"ל עם קוד האימות והוראה לאיפוס הסיסמה.
>
> • כיצד לבטל את הנעילה של הגדרה מתקדמת

כדי לשנות את הסיסמה שלך, לחץ על **שנה סיסמה** לצד **הגדרות הגנה באמצעות סיסמה**.

כדי להסיר את הסיסמה שלך, לחץ על **הסר** לצד **הגדרות הגנה באמצעות סיסמה**.



סיסמה להגדרות מתקדמות

כדי להגן על ההגדרות המתקדמות של ESET Smart Security Premium וכדי להימנע משינוי בלתי מורשה, הזן את סיסמתך החדשה בשדות **סיסמה חדשה** ו**אשר סיסמה**. לחץ על **אישור**.

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 לגישה להגדרות המתקדמות.

אם שכחת את הסיסמה, ראה ביטול נעילת סיסמת ההגדרות שלך במוצרים הביתיים של ESET עבור Windows.

כדי לשחזר מפתח הפעלה של ESET שאבד, תאריך התפוגה של המינוי שלך או פרטי מינוי אחרים עבור ESET Smart Security Premium, ראה איבדתי את מפתח ההפעלה שלי.

תמיכה בקוראי מסך

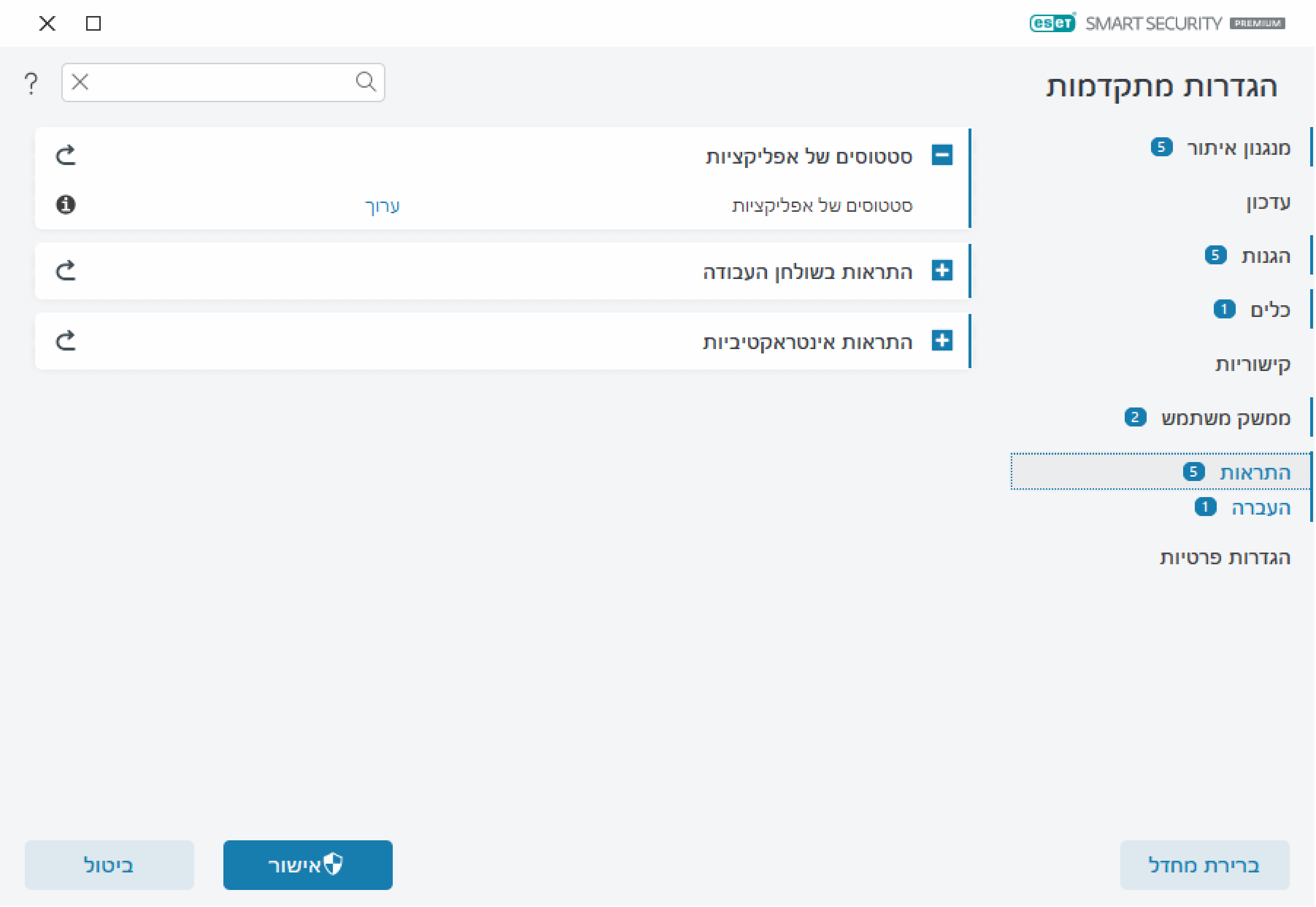
ניתן להשתמש ב-ESET Smart Security Premium יחד עם קוראי מסך כדי לאפשר למשתמשי ESET שראייתם לקויה לנווט במוצר או לקבוע את תצורת ההגדרות. קוראי המסך הבאים נתמכים (JAWS, NVDA, Narrator).

כדי לוודא שתוכנת קורא המסך יכולה לגשת ל-GUI של ESET Smart Security Premium כראוי, בצע את ההוראות במאמר מאגר הידע שלנו.

התראות

כדי לנהל התראות של ESET Smart Security Premium, פתח את הגדרות מתקדמות > **התראות**. תוכל לקבוע את התצורה של סוגי ההתראות הבאים:

- סטטוסים של אפליקציות – התראות שמוצגות בחלון התוכנית הראשי > **מבט כולל**.
- התראות בשולחן העבודה – חלונות התראה קטנים ליד שורת המשימות של המערכת.
- התראות אינטראקטיביות – חלונות התראה ותיבות הודעה הדורשים אינטראקציה עם המשתמש.
- העברה (התראות בדואר אלקטרוני) – התראות בדוא"ל נשלחות לכתובת הדוא"ל שצוינה.



סטטוסים של אפליקציות

סטטוסים של אפליקציות – לחץ על **ערוך** כדי לבחור אילו סטטוסים של אפליקציות יוצגו במקטע הבית של חלון התוכנית הראשי> **מבט כולל**.

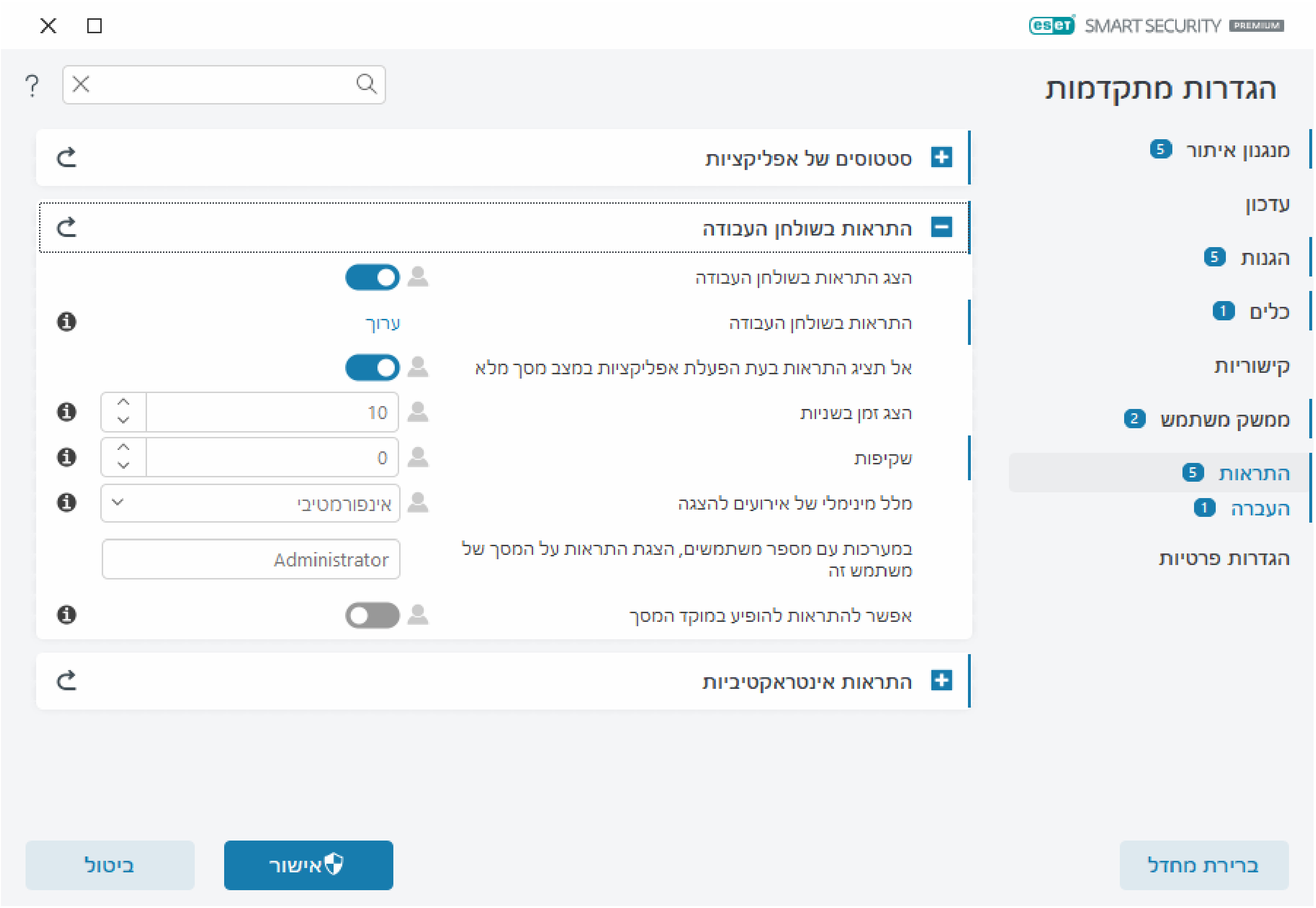
חלון דו-שיח - סטטוסים של אפליקציות

בחלון דו-שיח זה, באפשרותך לבחור אילו סטטוסים של אפליקציות יוצגו. לדוגמה, כשאתה משהה את האנטי-וירוס וההגנה מפני תוכנות ריגול או מפעיל מצב משחק.

הסטטוס של האפליקציה יוצג גם אם המוצר שלך לא מופעל או שתוקף המינוי שלך פג.

הודעות שולחן עבודה

התראות בשולחן העבודה מיוצגות באמצעות חלון התראות קטן לצד שורת המשימות של המערכת. כברירת מחדל, הן מוצגות במשך 10 שניות ונעלמות באיטיות. התראות מודיעות על עדכוני מוצר שבוצעו בהצלחה, התקנים חדשים שחוברו, השלמה של משימות סריקת וירוסים או איומים חדשים שנמצאו.



הצג התראות בשולחן העבודה מומלץ להשאיר אפשרות זו מופעלת כדי שהמוצר יוכל להודיע לך על אירוע חדש.

התראות בשולחן העבודה לחץ על **ערוך** כדי להפעיל או להשבית התראות מסוימות בשולחן העבודה.

אל תציג התראות בעת הפעלת אפליקציות במצב מסך מלא העלם את כל ההתראות שאינן אינטראקטיביות בעת הפעלת אפליקציות במצב מסך מלא.

הצג זמן בשניות קבע כמה זמן ההתראות יופיעו. על הערך להיות בין 3 ל-30 שניות.

שקיפות קבע את השקיפות באחוזים של התראות. הטווח הנתמך הוא 0 (ללא שקיפות) עד 80 (שקיפות גבוהה מאוד).

מלל מינימלי של אירועים להצגה – קבע את רמת החומרה ההתחלתית להצגת התראות. בחר אחת מהאפשרויות הבאות מהתפריט הנפתח:

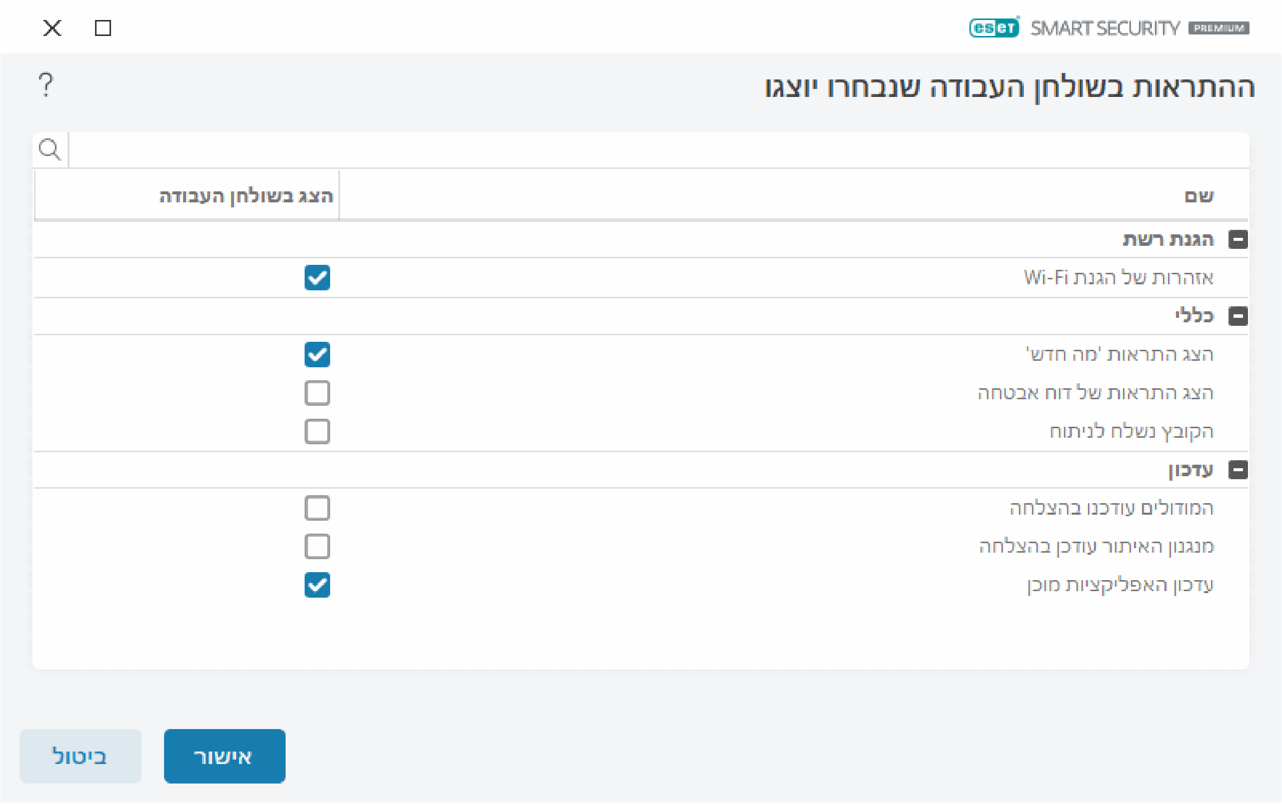
- **אבחוני** – הצגת מידע שנדרש להתאמה מפורטת של התוכנית ושל כל הרשומות שלעיל.
- **מסירת מידע** – הצגת הודעות מסירת מידע, כגון אירועים יוצאי דופן ברשת, לרבות הודעות על עדכון מוצלח, בנוסף לכל הרשומות שלעיל.
- **אזהרות** – הצגת הודעות אזהרה, שגיאות ושגיאות קריטיות (לדוגמה, העדכון נכשל).
- **שגיאות** – הצגת שגיאות (לדוגמה, לא הופעלה הגנה על מסמכים) ושגיאות קריטיות.
- **קריטי** – הצגת שגיאות קריטיות בלבד (כגון שגיאה בהפעלה של הגנת אנטי-וירוס או מערכת נגועה וכו').

במערכות עם מספר משתמשים, הצגת התראות על המסך של משתמש זה – מאפשר לחשבון נבחר לקבל התראות בשולחן העבודה. לדוגמה, אם אינך משתמש בחשבון מנהל המערכת, הקלד את שם החשבון המלא וההתראות בשולחן העבודה יוצגו עבור החשבון הספציפי. רק חשבון משתמש אחד יכול לקבל התראות בשולחן העבודה.

אפשר להתראות להופיע במוקד המסך – אפשרות זו מאפשרת להתראות להופיע במוקד המסך ולהיות נגישות בתפריט **ALT + Tab**.

רשימת התראות בשולחן העבודה

כדי להתאים את ההצגה של התראות שולחן העבודה (המוצגות בצד השמאלי התחתון של המסך), פתח את הגדרות מתקדמות > **התראות** > **התראות בשולחן העבודה**. לחץ על **ערוך** לצד **התראות בשולחן העבודה** ובחר בתיבת הסימון **הצג** המתאימה.



כללי

הצג התראות של דוח אבטחה – קבל התראה כאשר נוצרת גרסה חדשה של דוח אבטחה.

הצג התראות 'מה חדש' התראות על כל התכונות החדשות והמשופרות של גרסת המוצר האחרונה.

הקובץ נשלח לניתוח קבל התראה בכל פעם ש-ESET Smart Security Premium שולח קובץ לניתוח.

מפקח הרשת

שלח הודעה על התקני רשת שהתגלו לאחרונה קבל התראה כאשר מכשיר חדש מחובר לרשת.

הגנת רשת

פרופיל הרשת השתנה קבל הודעה כאשר פרופיל הרשת משתנה.

אזהרות הגנת WiFi - קבל הודעה בעת ניסיון להתחבר לרשת Wi-Fi עם סיסמה חלשה או ללא סיסמה.

עדכון

עדכון האפליקציות מוכן קבל התראה כאשר מוכן עדכון לגרסה חדשה של ESET Smart Security Premium.

מנגנון האיתור עודכן בהצלחה קבל התראה כאשר המוצר מעדכן מודולים של מנגנון האיתור.

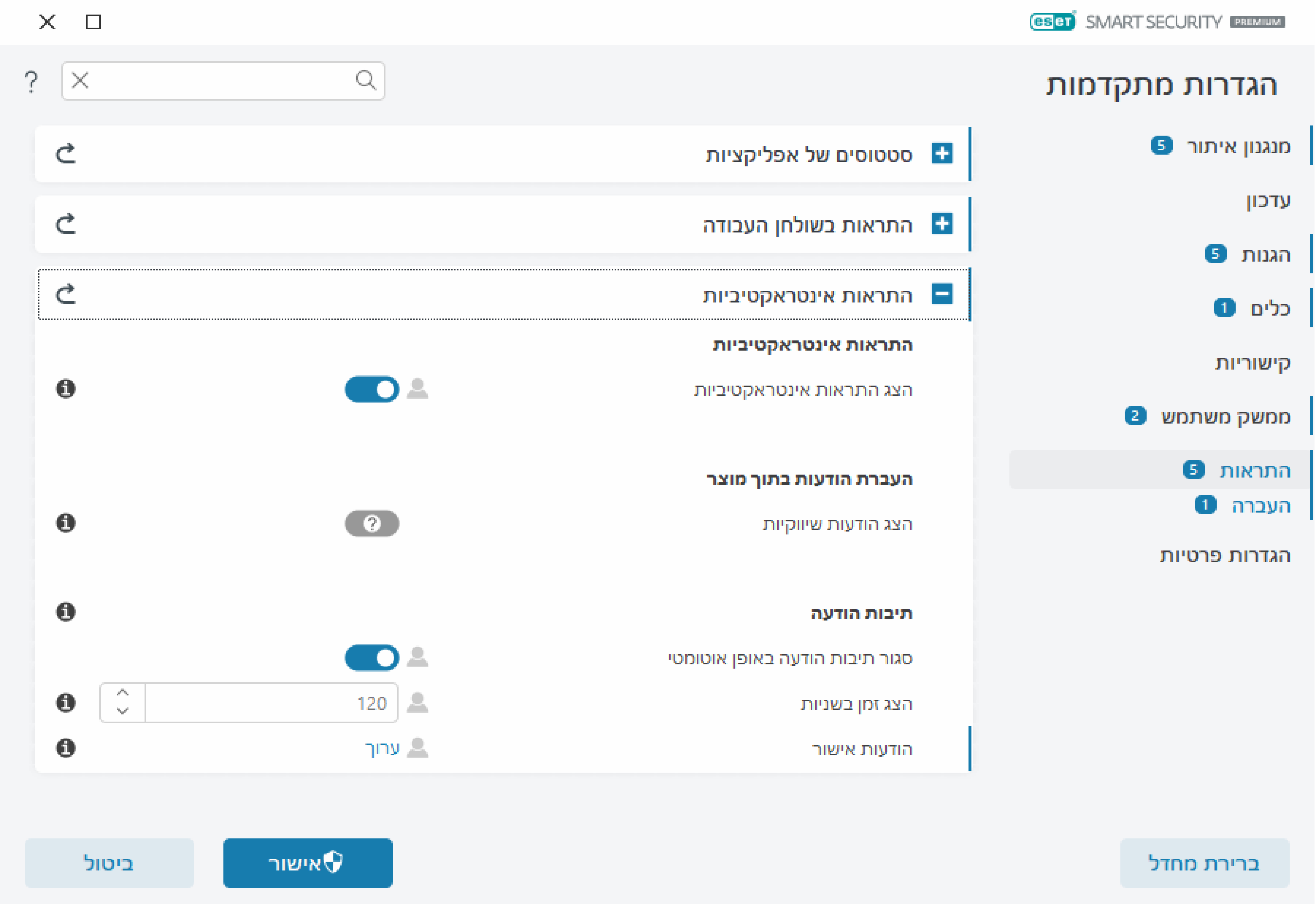
המודולים עודכנו בהצלחה קבל התראה כאשר המוצר מעדכן את רכיבי התוכנית.

כדי לקבוע הגדרות כלליות של התראות בשולחן העבודה (לדוגמה, כמה זמן מוצגת הודעה או המלל המינימלי של אירועים להצגה), ראה התראות בשולחן העבודה בהגדרות מתקדמות > **התראות**.

התראות אינטראקטיביות

מחפש מידע אודות התראות והודעות נפוצות?
- נמצא איום
- הכתובת נחסמה
- המוצר אינו מופעל
- עבור למוצר עם יותר תכונות
- עבור למוצר עם פחות תכונות
- קיים עדכון זמין
- מידע העדכון אינו עקבי
- פתרון בעיות עבור ההודעה "עדכון המודולים נכשל"
- פתרון שגיאות בעדכון מודולים
- איום רשת נחסם
- האישור של אתר האינטרנט בוטל

המקטע **התראות אינטראקטיביות** בתוך הגדרות מתקדמות > **התראות** מאפשר לך לקבוע כיצד ESET Smart Security Premium מטפל בתיבות הודעה ובהתראות אינטראקטיביות עבור איתורים, כאשר המשתמש צריך לקבל החלטה (לדוגמה, במקרה של אתר פישינג פוטנציאלי).



התראות אינטראקטיביות

השבתה של **הצג התראות אינטראקטיביות** תגרום להסתרת כל חלונות ההתראה ותיבות הדו-שיח של הדפדפן, ומתאימה רק לכמות מוגבלת של מצבים ספציפיים. אנו ממליצים להשאיר את האפשרות הזו מופעלת.

הודעות במוצר

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 את האפשרות **הצג הודעות שיווקיות**.

תיבות הודעות

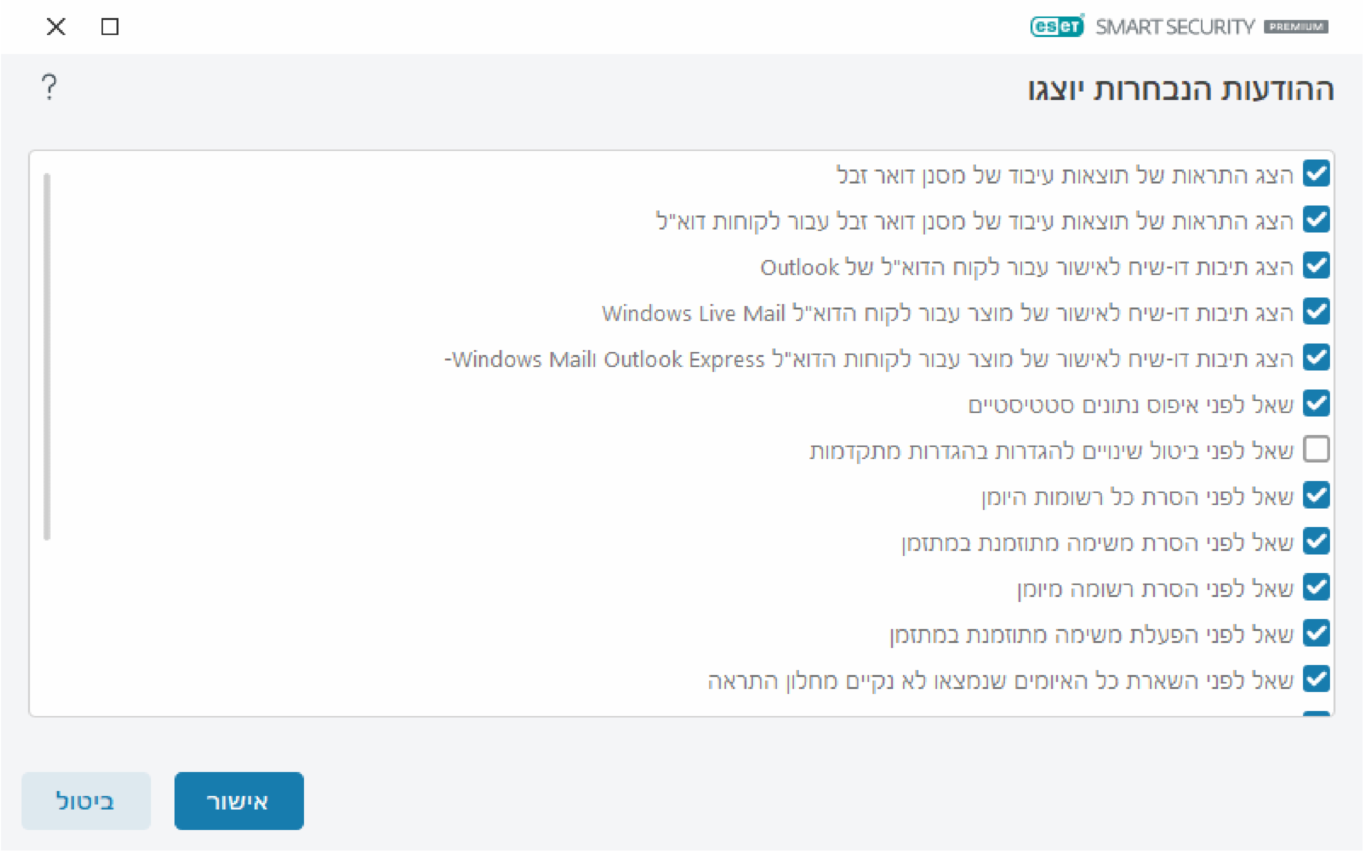
כדי לסגור את תיבות ההודעה אוטומטית לאחר זמן מסוים, בחר **סגור תיבות הודעה באופן אוטומטי**. אם חלונות ההתראה לא נסגרים ידנית, הם ייסגרו אוטומטית לאחר שיחלוף הזמן שצוין.

הצג זמן בשניות קובע את משך התצוגה של התראות. על הערך להיות בין 10 ל-999 שניות.

הודעות אישור לחץ על **ערוך** כדי להציג רשימה של הודעות אישור שבאפשרותך לבחור שיוצגו או שלא יוצגו.

הודעות אישור

כדי להתאים את הודעות האישור, פתח את הגדרות מתקדמות > **התראות** > **התראות אינטראקטיביות** ולחץ על **ערוך** לצד **הודעות אישור**.



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

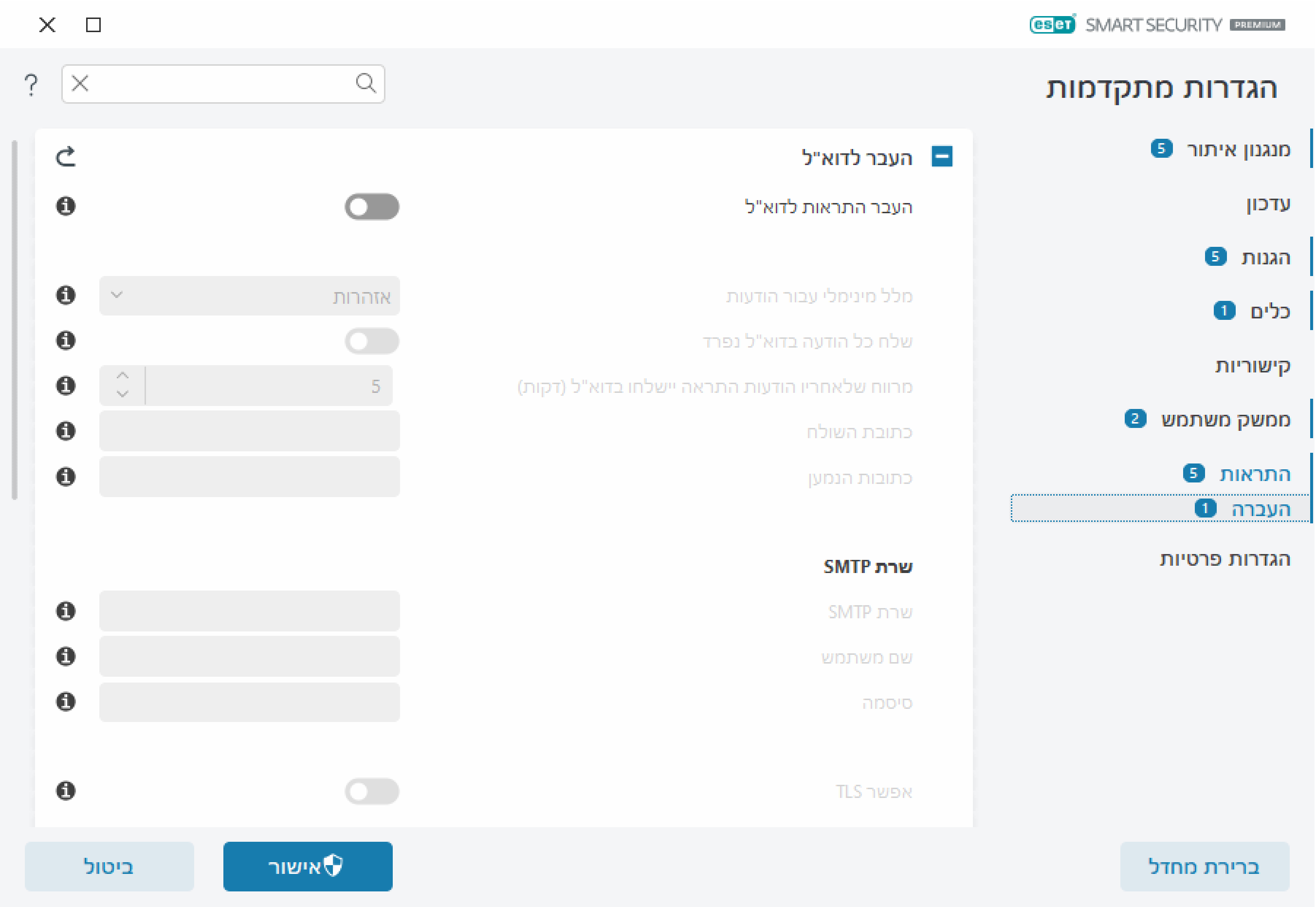
קבל מידע נוסף אודות תכונה ספציפית הקשורה להודעות אישור:

- שאל לפני מחיקת יומני ESET SysInspector
- שאל לפני מחיקת כל יומני ESET SysInspector
- שאל לפני מחיקת אובייקט מהסגר
- שאל לפני ביטול שינויים להגדרות בהגדרות מתקדמות
- שאל לפני השארת כל האיומים שנמצאו לא נקיים מחלון התראה
- שאל לפני הסרת רשומה מיומן
- שאל לפני הסרת משימה מתוזמנת במתזמן
- שאל לפני הסרת כל רשומות היומן
- שאל לפני איפוס נתונים סטטיסטיים
- שאל לפני שחזור אובייקט מהסגר
- שאל לפני שחזור אובייקטים מהסגר ואי הכללתם בסריקה
- שאל לפני הפעלת משימה מתוזמנת במתזמן
- הצג התראות של תוצאות עיבוד של מסנן דואר זבל
- הצג התראות של תוצאות עיבוד של מסנן דואר זבל עבור לקוחות דוא"ל

- [הצג תיבות דו-שיח לאישור של מוצר עבור לקוחות הדוא"ל Outlook Express ו-Windows Mail]
- [הצג תיבות דו-שיח לאישור של מוצר עבור לקוח הדוא"ל] Mail [Windows Live]
- [הצג תיבות דו-שיח לאישור של מוצר עבור לקוח הדוא"ל של Outlook]

העברה

ESET Smart Security Premium יכול לשלוח באופן אוטומטי התראות בדוא"ל כשמתרחש אירוע ברמת הפירוט שנבחרה. פתח את [הגדרות מתקדמות] < **התראות** < **העברה** והפעל את האפשרות **העבר התראות לדוא"ל** כדי להפעיל התראות בדוא"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 (למשל על עדכון שנכשל).
- **שגיאות** שגיאות (לא הופעלה הגנה על מסמכים) ושגיאות קריטיות יתועדו.
- **קריטי** רישום שגיאות קריטיות בלבד (לדוגמה, שגיאה בהפעלה של הגנת אנטי-וירוס או איום שנמצא).

שלח כל התראה בדוא"ל נפרד כאשר אפשרות זו מופעלת, הנמען יקבל הודעת דוא"ל חדשה עבור כל התראה. מצב זה עלול להוביל לקבלת הודעות דוא"ל רבות בפרק זמן קצר.

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.

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

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

שרת SMTP

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

ESET Smart Security Premium 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.

אפשר TLS – התראות והודעות מאובטחות המשתמשות בהצפנת TLS.

בדוק חיבור SMTP – הודעת בדיקה בדוא"ל תישלח לכתובת הדוא"ל של המשתמש. יש למלא את שרת ה-SMTP, שם המשתמש, הסיסמה, כתובת השולח וכתובות הנמענים.

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). האפשרות **השתמש בתבנית ההודעה המהווה ברירת מחדל** עבור הודעות ההתראה וההתראות 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 אזהרות איומים – להודעות התראה על איומים יש תבנית ברירת מחדל מוגדרת מראש. אנו ממליצים שלא לשנות את התבנית המוגדרת מראש. עם זאת, בנסיבות מסוימות (למשל אם יש לך מערכת עיבוד דוא"ל אוטומטית), ייתכן שתצטרך לשנות את תבנית ההודעה.

ערכת תווים – המרת הודעת דוא"ל לקידוד התווים של ANSI בהתאם להגדרות האזוריות של Windows (לדוגמה, windows-1250, Unicode (UTF-8), ACSII 7-bit או יפנית (ISO-2022-JP)). כתוצאה מכך, "á" ישתנה ל-"a" וסמל לא מוכר ישתנה ל-"?".

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

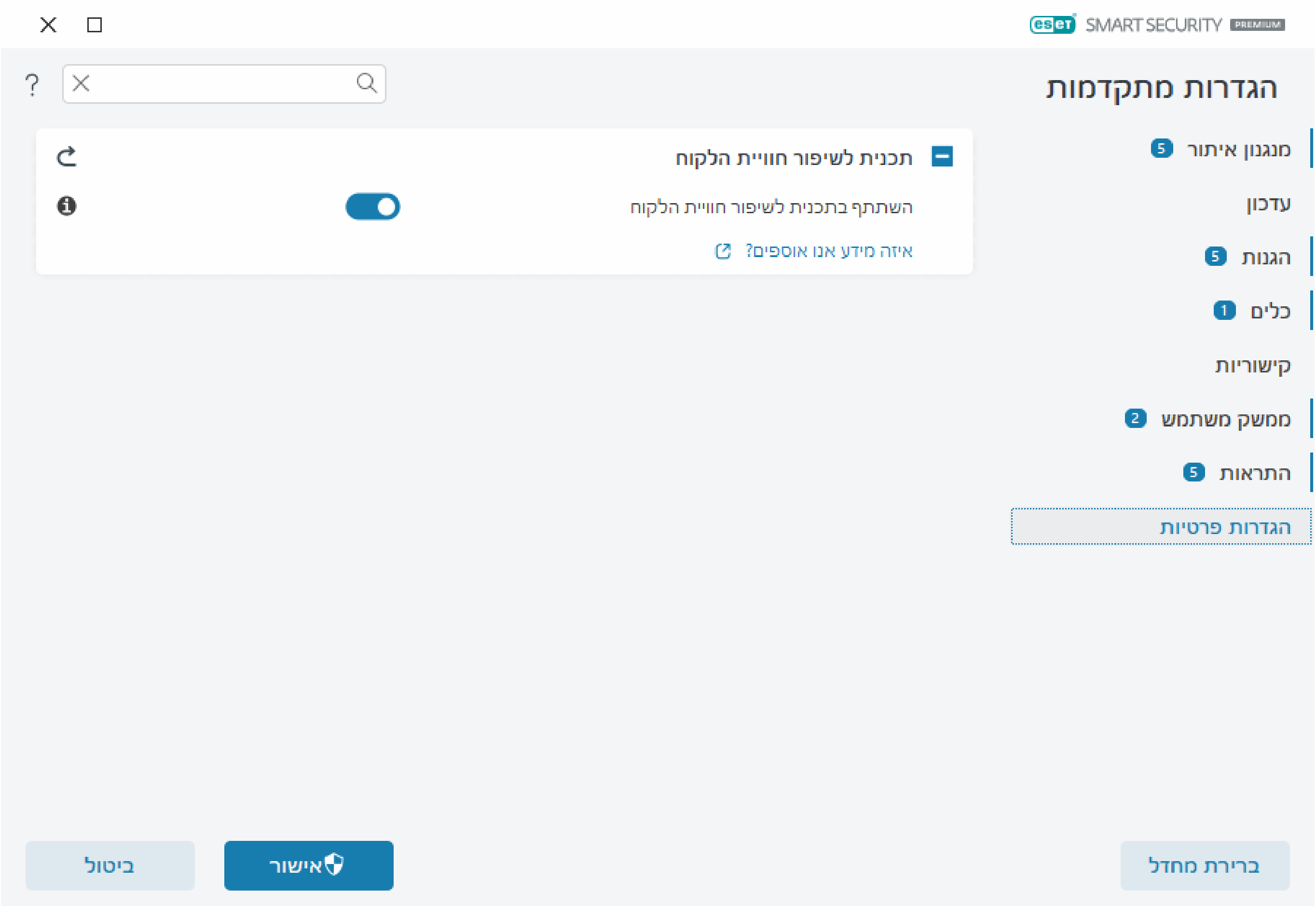
- **%TimeStamp%** – התאריך והשעה של האירוע
- **%Scanner%** – המודול שבו מדובר
- **%ComputerName%** – שם המחשב שבו ההודעה אירעה
- **%ProgramName%** – התוכנית שהפיקה את ההתראה
- **%InfectedObject%** – שם הקובץ הנגוע, ההודעה וכן הלאה.
- **%VirusName%** – זיהוי ההדבקה
- **%Action%** – פעולה שננקטה לאחר חדירה

- %ErrorDescription% – תיאור אירוע שאינו וירוס

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

הגדרות פרטיות

פתח את הגדרות מתקדמות > **הגדרות פרטיות**.



תכנית לשיפור חוויית הלקוח

הפעל את המתג לצד **השתתפות בתכנית לשיפור חוויית הלקוח** כדי להצטרף לתכנית לשיפור חוויית הלקוח. בעצם ההצטרפות, אתה מספק ל-ESET מידע אנונימי בנוגע לשימוש במוצרי ESET. הנתונים שייאספו יסייעו לנו בשיפור החוויה שאנו מספקים לך ולעולם לא נשתף אותם עם גורמי צד שלישי. איזה מידע אנו אוספים?

אפס להגדרות ברירת המחדל

לחץ על **ברירת מחדל** בהגדרות מתקדמות כדי להחזיר למצב קודם את כל הגדרות התכנית עבור כל המודולים. ההגדרות יאופסו לסטטוס שהיה מוגדר עבורן לאחר התקנה חדשה.

ראה גם ייבוא וייצוא הגדרות.

החזרת כל ההגדרות במקטע הנוכחי למצב הקודם

לחץ על החץ המעוגל כדי להחזיר את כל ההגדרות במקטע הנוכחי להגדרות ברירת המחדל שהוגדרו על ידי ESET.

שים לב, כל השינויים שביצעת יאבדו לאחר שתלחץ על **אפס לברירת המחדל**.

החזר תוכן טבלאות למצב קודם כשאפשרות זו מופעלת, המשימות או הפרופילים שנוספו ידנית או אוטומטית יאבדו.

ראה גם ייבוא וייצוא הגדרות.

שגיאה במהלך שמירת התצורה

הודעת שגיאה זו מציינת שההגדרות לא נשמרו כהלכה בשל שגיאה.

בדרך כלל משמעות הדבר היא שלמשתמש שניסה לשנות את פרמטרי התכנית:

- אין זכויות גישה מספיקות או שחסרות לו הרשאות מערכת ההפעלה הנדרשות כדי לשנות קובצי קביעת התצורה ואת רישום המערכת.
  > כדי לבצע את השינויים הרצויים, מנהל המערכת חייב להתחבר.
- הפעיל לאחרונה מצב למידה ב-HIPS או בחומת אש וניסה לבצע שינויים בהגדרות מתקדמות.
  > כדי לשמור את התצורה ולמנוע התנגשויות תצורה, סגור את ההגדרות המתקדמות מבלי לשמור ונסה שוב לבצע את השינויים הרצויים.

המקרה השני הנפוץ ביותר האפשרי הוא שהתוכנית אינה פועלת יותר כהלכה, או פגומה, ולכן יש להתקינה מחדש.

סורק שורת פקודה

ESET Smart Security Premium 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 (ברירת מחדל) □ לא יתבצע ניקוי אוטומטי. • רגיל – 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. • מחיקה – 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

קודי יציאה גדולים מ-100 פירושם שהקובץ לא נסרק ולכן עשוי להיות נגוע.

שאלות נפוצות

הרשימה להלן מפרטת חלק מהשאלות ומהבעיות הנפוצות ביותר. לחץ על כותרת הנושא כדי לגלות כיצד לפתור את הבעיה שלך:

- כיצד לעדכן את ESET Smart Security Premium
- ESET Smart Security Premium איתר איום
- כיצד להסיר וירוס מהמחשב
- כיצד לאפשר תקשורת עבור יישום מסוים
- כיצד להפעיל בקרת הורים בחשבון
- כיצד ליצור משימה חדשה במתזמן
- כיצד לתזמן משימת סריקה (שבועית)
- כיצד לבטל את הנעילה של הגדרות מתקדמות
- כיצד לפתור את ביטול ההפעלה של המוצר מתוך ESET HOME

אם בעייתך אינה מופיעה ברשימה שלעיל, נסה לחפש בעזרה המקוונת של ESET Smart Security Premium.

אם אינך מוצא פתרון לבעיה/שאלה שלך בעזרה המקוונת של ESET Smart Security Premium, תוכל לבקר במאגר הידע של ESET, המתעדכן באופן קבוע. להלן קישורים למאמרי מאגר הידע הפופולריים ביותר שלנו:

- איך אוכל לחדש את המינוי שלי?
- קיבלתי שגיאת הפעלה בעת התקנת מוצר ESET שברשותי. מה פירוש הדבר?
- הפעל את המוצר הביתי של ESET Windows באמצעות מפתח ההפעלה
- הסרת ההתקנה או התקנה מחדש של המוצר הביתי של ESET שברשותי
- קיבלתי הודעה שההתקנה של ESET הסתיימה מוקדם מדי
- מה עליי לעשות לאחר חידוש המינוי שלי? (משתמשים ביתיים)
- מה יקרה אם אחליף את כתובת הדואר האלקטרוני שלי?
- העברת מוצר ESET שלי למחשב או למכשיר חדש
- כיצד להפעיל את Windows במצב בטוח או במצב בטוח עם עבודה ברשת
- החרגת אתר אינטרנט בטוח מחסימה
- אפשר גישה לתוכנת קוראי מסך לממשק המשתמש הגרפי של ESET

במידת הצורך תוכל להפנות את השאלות או הבעיות שלך לתמיכה הטכנית שלנו.

כיצד לעדכן את ESET Smart Security Premium

עדכון ESET Smart Security Premium יכול להתבצע בצורה ידנית או אוטומטית. כדי להפעיל את העדכון, לחץ על **עדכון** 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.

כיצד להסיר וירוס מהמחשב

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

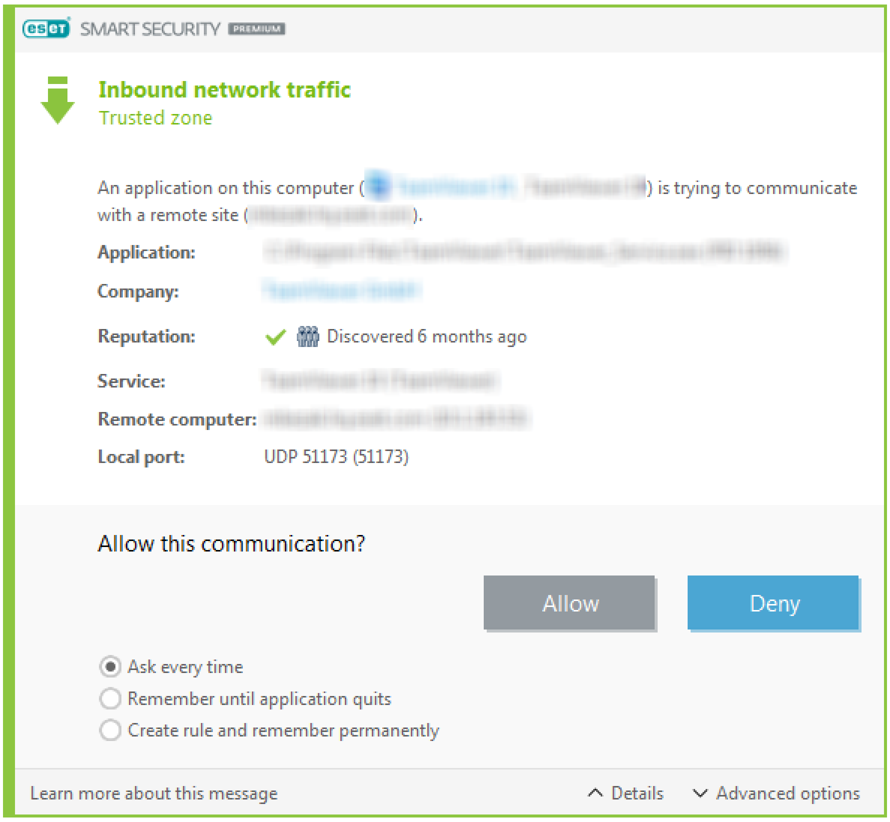
1. בחלון התוכנית הראשי, לחץ על **סריקת מחשב**.
2. לחץ על **סרוק את המחשב שלך** כדי להתחיל בסריקת המערכת.
3. בסיום הסריקה, סקור את היומן הכולל את מספר הקבצים שנסרקו, שנפגעו ושנוקו.
4. אם ברצונך לסרוק רק חלק נבחר מהדיסק, לחץ על **סריקה מותאמת אישית** ובחר יעדים שייסרקו לאיתור וירוסים.

למידע נוסף, ראה:

- מאמר מאגר הידע של ESET
- הסגר

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 Smart Security Premium יבצע את אותה פעולה בכל פעם שהיישום מנסה ליצור חיבור, סמן את תיבת הסימון **צור כלל וזכור לצמיתות**.



בהגדרות חומת האש, באפשרותך ליצור כללי חומת אש חדשים ליישומים, עוד לפני שיזוהו על-ידי ESET Smart Security Premium. פתח את חלון התוכנית הראשי > **הגדרות** > **הגנת רשת** > לחץ על ⚙ שלצד **חומת אש** > **קבע תצורה** > **מתקדם** > **כללים** > **ערוך**.

לחץ על הלחצן **הוסף** ובכרטיסייה **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

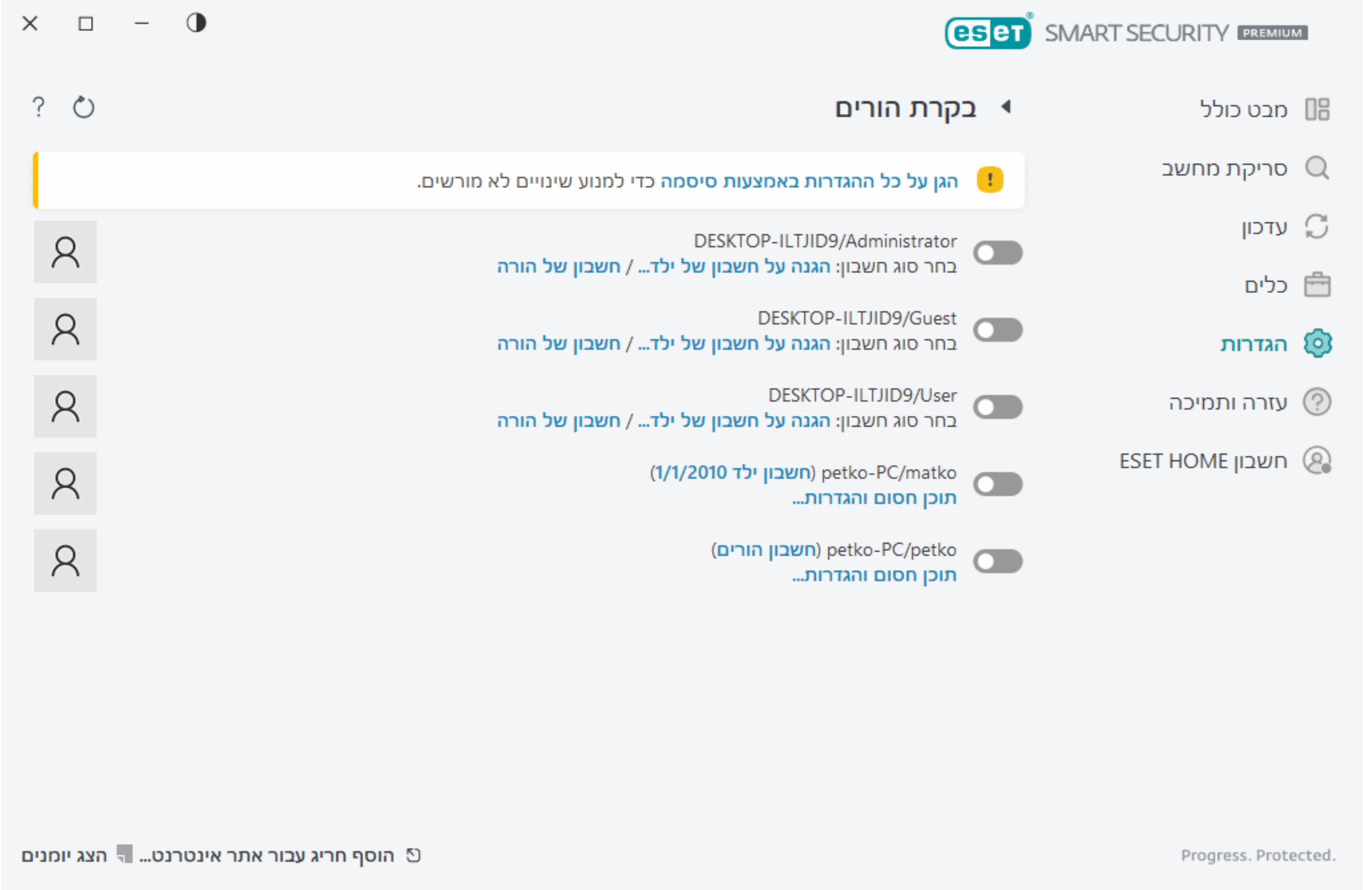
כדי להפעיל בקרת הורים של חשבון משתמש ספציפי, בצע את הפעולות הבאות:

1. כברירת מחדל, בקרת הורים מושבתת במוצר ESET Smart Security Premium. ישנן שתי שיטות להפעלת בקרת הורים:

• לחץ על הסמל במקטע **הגדרות** > **הגנת אינטרנט** > **בקרת הורים** בחלון התוכנית הראשי והעבר את מצב בקרת ההורים למצב מופעל.
• פתח את הגדרות מתקדמות > **הגנות** > **הגנת גישה לאינטרנט** > **בקרת הורים** ולאחר מכן הפעל את המתג שליד **הפעל בקרת הורים**.

2. לחץ על **הגדרות** > **הגנת אינטרנט** > **בקרת הורים** בחלון התוכנית הראשי. למרות שהאפשרות **מופעל** מופיעה לצד **בקרת הורים**, עליך להגדיר את בקרת ההורים לחשבון הרצוי על-ידי לחיצה על סמל החץ ולאחר מכן לחיצה על **הגן על חשבון ילד** או על **חשבון הורים** בחלון הבא. 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 ב**כלים** < **מתזמן**, לחץ על **הוסף משימה** 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** > **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. הזן שם עבור המשימה ובחר **סריקת מחשב לפי דרישה** מהתפריט הנפתח **סוג משימה**.
3. בחר 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 לבטל את הנעילה של הגדרות מתקדמות המוגנות באמצעות סיסמה

כאשר תרצה לגשת להגדרות המתקדמות המוגנות באמצעות סיסמה, החלון להזנת הסיסמה יוצג. אם שכחת או איבדת את הסיסמה, לחץ על **שחזר סיסמה** והזן את כתובת הדוא"ל שבה השתמשת לרישום המינוי. ESET תשלח לך דוא"ל עם קוד האימות. הזן את קוד האימות ולאחר מכן כתוב ואשר את הסיסמה החדשה. קוד האימות יהיה תקף למשך שבעה ימים.

שחזר סיסמה באמצעות חשבון ESET HOME שלך – השתמש באפשרות זו אם המינוי המשמש להפעלה משויך לחשבון ESET HOME שלך. הזן את כתובת הדוא"ל שבה אתה משתמש להתחברות לחשבון ESET HOME שלך.

אם אינך זוכר את כתובת הדוא"ל או שאתה נתקל בקשיים בשחזור הסיסמה, לחץ על **צור קשר עם התמיכה הטכנית** ותנותב לאתר האינטרנט של ESET. שם תוכל ליצור קשר עם מחלקת התמיכה הטכנית שלנו.

צור קוד עבור התמיכה הטכנית אפשרות זו תיצור קוד עבור מחלקת 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 שבעה ימים.

לקבלת מידע נוסף, ראה ביטול נעילת סיסמת ההגדרות שלך במוצרים הביתיים של ESET עבור Windows.

כיצד לפתור את ביטול ההפעלה של המוצר מתוך ESET HOME

המוצר אינו מופעל

הודעת שגיאה זו מופיעה כאשר בעל המינוי מבטל את ההפעלה של ESET Smart Security Premium מתוך פורטל ESET HOME או שהמינוי ששותף עם חשבון ESET HOME שלך אינו משותף עוד. כדי לפתור בעיה זו:

- לחץ על **הפעל** והשתמש באחת משיטות ההפעלה כדי להפעיל את ESET Smart Security Premium.
- צור קשר עם בעל המינוי וידע אותו שההפעלה של ESET Smart Security Premium בוטלה על-ידי בעל המינוי או שהמינוי אינו משותף איתך עוד. הבעלים יוכל לפתור את הבעיה ב-ESET HOME.

הפעלת המוצר בוטלה, המכשיר נותק

הודעת שגיאה זו מופיעה לאחר הסרת התקן מפורטל ESET HOME. כדי לפתור בעיה זו:

- לחץ על **הפעל** והשתמש באחת משיטות ההפעלה כדי להפעיל את ESET Smart Security Premium.
- צור קשר עם הבעלים של המינוי כדי שהוא ידע שההפעלה של ESET Smart Security Premium בוטלה ושהמכשיר נותק מ-ESET HOME.
- אם אתה הבעלים של המינוי ואינך מודע לשינויים אלה, עיין בפיד הפעילות של ESET HOME. אם גילית פעילות חשודה כלשהי, שנה את סיסמת חשבון ESET HOME וצור קשר עם התמיכה הטכנית של ESET.

הפעלת המוצר בוטלה, המכשיר נותק

הודעת שגיאה זו מופיעה לאחר הסרת התקן מפורטל ESET HOME. כדי לפתור בעיה זו:

- לחץ על **הפעל** והשתמש באחת משיטות ההפעלה כדי להפעיל את ESET Smart Security Premium.
- צור קשר עם הבעלים של המינוי כדי שהוא ידע שההפעלה של ESET Smart Security Premium בוטלה ושהמכשיר נותק מ-ESET HOME.
- אם אתה הבעלים של המינוי ואינך מודע לשינויים אלה, עיין בפיד הפעילות של ESET HOME. אם גילית פעילות חשודה כלשהי, שנה את סיסמת חשבון ESET HOME וצור קשר עם התמיכה הטכנית של ESET.

המוצר אינו מופעל

הודעת שגיאה זו מופיעה כאשר בעל המינוי מבטל את ההפעלה של ESET Smart Security Premium מתוך פורטל ESET HOME או שהמינוי ששותף עם חשבון ESET HOME שלך אינו משותף עוד. כדי לפתור בעיה זו:

- לחץ על **הפעל** והשתמש באחת משיטות ההפעלה כדי להפעיל את ESET Smart Security Premium.
- צור קשר עם בעל המינוי וידע אותו שההפעלה של ESET Smart Security Premium בוטלה על-ידי בעל המינוי או שהמינוי אינו משותף איתך עוד. הבעלים יוכל לפתור את הבעיה ב-ESET HOME.

0

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 מאתנו להמשיך לעבד את הנתונים האנונימיים שלך.

באפשרותך לבטל את הסכמתך בכל עת על ידי שינוי הגדרות המוצר.

- שנה את הגדרות התוכנית לשיפור חוויית הלקוח במוצרים הביתיים של ESET עבור Windows

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 לרלוונטיים יותר, לקלים לשימוש ולנטולי שגיאות ככל האפשר.

מי שולט במידע זה?

ESET, spol. s r.o-ל. יש שליטה בלעדית על כל המידע שנאסף במסגרת התכנית. מידע זה לא משותף עם גורמי צד שלישי.

הסכם רישיון למשתמש קצה

בתוקף החל מיום 19 באוקטובר 2021.

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 ולהגבלות אלה ומאשר את מדיניות הפרטיות.**

הסכם רישיון למשתמש קצה

בכפוף לתנאים של הסכם רישיון זה למשתמש קצה ("הסכם"), הנערך בין ESET, spol. s r. o., שמשרדה הרשום בכתובת Einsteinova 24, 85101 Bratislava, Slovak Republic, הרשומה במרשם המסחרי המנוהל על ידי בית המשפט המחוזי I של ברטיסלבה, אזור סרו, רשומה מס' B/3586, מספר רישום עסק: 31333532 ("ESET" או "הספקית") ובינך, אדם או ישות חוקית ("אתה" או "משתמש הקצה"), אתה זכאי להשתמש בתוכנה המוגדרת בסעיף 1 להסכם זה. אתה רשאי 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" או "אני מקבל..." במהלך התקנה, הורדה, העתקה או שימוש בתוכנה, אתה מסכים לתנאים ולהגבלות של הסכם זה ומאשר את מדיניות הפרטיות. אם אינך מסכים לכל התנאים וההגבלות של הסכם זה ו/או למדיניות הפרטיות, לחץ מיד על אפשרות הביטול, בטל את ההתקנה או ההורדה, או השמד או החזר את התוכנה, מדיית ההתקנה, מסמכים נלווים וקבלת המכירה לספקית או לחנות שממנה רכשת את התוכנה.

אתה מסכים שהשימוש שלך בתוכנה מהווה הכרה שקראת הסכם זה, הבנת אותו ואתה מסכים להיות מחויב לתנאים ולהגבלות שבו.

1. **תוכנה.** בהתאם להסכם זה, המונח "תוכנה" פירושו: (i) תוכנית המחשב המלווה בהסכם זה וכל מרכיביו; (ii) כל התוכן של הדיסקים, התקליטורים, דיסקי ה-DVD, הודעות הדואר האלקטרוני וקבצים מצורפים כלשהם, או מדיה אחרת שבאמצעותה הסכם זה מסופק, לרבות תבנית קוד האובייקט של התוכנה המסופקת בספק נתונים, באמצעות דואר אלקטרוני או בהורדה מהאינטרנט; (iii) חומרי הסבר בכתב קשורים כלשהם וכל תיעוד אפשרי אחר הקשור לתוכנה, מעל כל תיאור של התוכנה, של המפרטים שלה, כל תיאור של מאפייני התוכנה או של פעולתה, כל תיאור של סביבת הפעולה שבה התוכנה נמצאת בשימוש, הוראות לשימוש ולהתקנה של התוכנה או כל תיאור של אופן השימוש בתוכנה ("מסמכים"); (iv) עותקים של התוכנה, תיקונים לשגיאות אפשריות בתוכנה, תוספות לתוכנה, הרחבות לתוכנה, גירסאות ערוכות של התוכנה ועדכונים לרכיבי התוכנה, אם ישנם, שהוענקו לך ברישיון על ידי הספק בכפוף לסעיף 3 של הסכם זה. התוכנה תסופק באופן בלעדי בצורה של קוד אובייקט לביצוע.

2. **התקנה, מחשב ומפתח רישיון.** תוכנה המתקבלת מספק נתונים, נשלחת בדואר אלקטרוני, מורדת מהאינטרנט, מורדת משרתי הספקית או מושגת ממקורות אחרים מצריכה התקנה. עליך להתקין את התוכנה במחשב שהוגדר כראוי, וממלא לכל הפחות את הדרישות המתוארות בתיעוד. מתודולוגיית ההתקנה מתוארת בתיעוד. אין להתקין במחשב שבו אתה מתקין את התוכנה תוכניות מחשב או חומרה שעלולה להיות להן השפעה שלילית על התוכנה להתקנה. מחשב פירושו חומרה, לרבות אך ללא הגבלה, מחשבים אישיים, מחשבים ניידים, תחנות עבודה, מחשבי כף יד, טלפונים חכמים, מכשירים אלקטרוניים נישאים או מכשירים אלקטרוניים אחרים שעבורם התוכנה מתוכננת, שבהם היא תותקן ו/או ייעשה בה שימוש. מפתח רישיון פירושו הרצף הייחודי של סימנים, אותיות, מספרים או תווים מיוחדים שמסופק למשתמש הקצה כדי לאפשר את השימוש החוקי בתוכנה, הגרסה הספציפית שלה או הרחבת תקופת הרישיון בהתאם להסכם זה.

3. **רישיון.** בכפוף להסכמתך לתנאי הסכם זה ולכך שאתה עומד 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 ("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. משתמש הקצה רשאי להזין את מפתח הרישיון לתוכנה רק עד למידה שבה יש לו את הזכות להשתמש בתוכנה בהתאם למגבלה הנובעת ממספר הרישיונות שהוענקו על ידי הספקית. מפתח הרישיון נחשב לסודי. אסור לשתף את מפתח הרישיון עם גורמי צד שלישי או לאפשר לגורמי צד שלישי להשתמש במפתח הרישיון אלא אם הדבר הותר בהסכם זה או על ידי הספקית. במקרה של פגיעה כלשהי בבטיחות של מפתח הרישיון, עליך ליידע את הספקית באופן מיידי.

ג) **גירסת Home/Business Edition.** יש להשתמש בגירסת Home Edition של התוכנה אך ורק בסביבה פרטית ו/או לא מסחרית לשימוש ביתי ומשפחתי בלבד. יש להשיג את גירסת Business Edition של התוכנה לשימוש בסביבה מסחרית וכדי להשתמש בתוכנה בשרתי דואר, בממסרי דואר, בשערי דואר או בשערי אינטרנט.

ד) **תקופת הרישיון.** הזכות שלך להשתמש בתוכנה תוגבל בזמן.

ה) **תוכנת יצרן ציוד מקורי (OEM).** תוכנה המסווגת כתוכנת יצרן ציוד מקורי "OEM" תוגבל 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.

ז) **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. **פונקציות עם דרישות של איסוף נתונים וחיבור לאינטרנט.** הפעלה נכונה של התוכנה דורשת חיבור לאינטרנט ויש להתחבר במרווחי זמן קבועים לשרתי הספקית או לשרתים של צד שלישי ולצורך איסוף ישים של נתונים בהתאם למדיניות הפרטיות. חיבור לאינטרנט ואיסוף ישים של נתונים נחוצים לצורך הפונקציות הבאות של התוכנה:

א) **עדכונים לתוכנה.** הספקית תהיה זכאית להפיק עדכונים או שדרוגים לתוכנה ("עדכונים") מפעם לפעם, אך לא תהיה מחויבת לספק עדכונים. פונקציה זו מאופשרת בהגדרות הרגילות של התוכנה ולפיכך עדכונים יותקנו באופן אוטומטי, אלא אם משתמש הקצה השבית התקנה אוטומטית של עדכונים. למטרת אספקה של עדכונים, נדרש אימות של מקוריות הרישיון כולל מידע אודות המחשב ו/או הפלטפורמה שבה התוכנה מותקנת בהתאם למדיניות הפרטיות.

אספקת העדכונים עשויה להיות כפופה למדיניות סוף מחזור החיים ("מדיניות ה-EOL"), הזמינה בכתובת

https://go.eset.com/eol_home. לא יסופקו עדכונים לאחר שהתוכנה או כל אחת מהתכונות שלה יגיעו לתאריך סוף מחזור החיים המוגדר במדיניות ה-EOL.

ב) **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 ("הסתננויות") ושולחות אותן לאחר מכן לספקית, לרבות אך ללא הגבלה, מידע אודות תהליך ההתקנה, המחשב ו/או הפלטפורמה שבהם התוכנה מותקנת ומידע אודות הפעולות והתפקודיות של התוכנה ("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 מערכת המשוב של LiveGrid® כוללת איסוף של הסתננויות עם המטה-נתונים והמידע הקשורים ושליחתם אל הספקית. משתמש הקצה עשוי להפעיל פונקציה זו במהלך תהליך התקנת התוכנה.

הספקית תשתמש במידע ובחדירות שהתקבלו רק למטרת ניתוח ומחקר של חדירות, שיפור התוכנה ואימות מקוריות הרישיון והיא תנקוט באמצעים מתאימים כדי להבטיח שהחדירות והמידע שהתקבלו יישארו מאובטחים. מתוקף הפעלת פונקציה זו של התוכנה, הספקית עשויה לאסוף ולעבד את החדירות והמידע כפי שמפורט במדיניות הפרטיות ובהתאם לתקנות המשפטיות הרלוונטיות. באפשרותך לבטל את ההפעלה של פונקציות אלה בכל עת.

למטרות הסכם זה, נדרש לאסוף, לעבד ולאחסן נתונים שיאפשרו לספקית לזהות אותך בהתאם למדיניות הפרטיות. אתה מאשר בזאת שהספקית מבצעת בדיקות באמצעות אמצעים משלה כדי לוודא שאתה משתמש בתוכנה בהתאם לתנאים בהסכם זה. אתה מאשר בזאת שלמטרות הסכם זה, העברת הנתונים שלך נחוצה במהלך תקשורת בין התוכנה למערכות המחשב של הספקית או לאלה של שותפיה העסקיים כחלק מרשת ההפצה והתמיכה של הספקית כדי להבטיח את הפונקציונליות של התוכנה וההרשאה לשימוש בתוכנה וכן כדי להבטיח את זכויות הספקית.

בהתאם לסיום של הסכם זה, הספקית או כל מי משותפיה העסקיים כחלק מרשת ההפצה והתמיכה של הספקית יהיו רשאים להעביר, לעבד ולאחסן נתונים חיוניים המזהים אותך למטרות חיוב, ביצוע הסכם זה והעברת התראות במחשב שלך.

תוכל למצוא פרטים אודות פרטיות, הגנה על נתונים אישיים והזכויות שלך כנושא הנתונים במדיניות הפרטיות הזמינה באתר האינטרנט של הספקית והנגישה ישירות במהלך תהליך ההתקנה. תוכל לעיין בה גם מתוך מקטע העזרה של התוכנה.

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 אותם מחשבים או מערכות מחשב שעבורם השגת רישיון.

6. **הגבלות על הזכויות.** 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.

ז) אתה מסכים שלא לבצע פעילויות הכוללות שימוש במפתח הרישיון בניגוד לתנאי הסכם זה או המובילות לאספקת מפתח הרישיון לכל אדם אחר שאינו רשאי להשתמש בתוכנה, כגון העברה של מפתח רישיון שנעשה בו שימוש או שלא נעשה בו שימוש בכל צורה שהיא, כמו גם שכפול לא מורשה, או הפצה של מפתחות רישיון משוכפלים או מיוצרים או שימוש בתוכנה כתוצאה מהשימוש במפתח רישיון שהושג ממקור שאינו הספקית.

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 הזכויות.** הספקית שומרת בזאת לעצמה את כל הזכויות על התוכנה, פרט לזכויות שהוענקו במפורש 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, להחכיר, להעניק ברישיון משנה, להלוות או להעביר גרסאות או עותקים של התוכנה שאינך משתמש בהם.

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. הזכות שלך להשתמש בתוכנה ובכל התכונות שלה עשויה להיות כפופה למדיניות ה-EOL. לאחר שהתוכנה או כל אחת מהתכונות שלה יגיעו לתאריך סיום החיים המוגדר במדיניות ה-EOL, הזכות שלך להשתמש בתוכנה תסתיים. ללא קשר לאופן הסיום של הסכם זה, התנאים בסעיפים 7, 8, 11, 13, 19 ו-21 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 ממנה.

12. **אין כל מחויבות אחרת.** הסכם זה אינו יוצר כל מחויבות מצד הספקית ומצד מעניקי הרישיון שלה, פרט לאלה המפורטות בזאת באופן ספציפי.

13. **הגבלת חבות.** במלוא ההיקף המותר בדין תקף, בכל מקרה הספקית, עובדיה או בעלי הרישיון שלה לא יישאו בחבות בגין כל הפסד רווחים, הכנסה, מכירות, נתונים או עלויות של רכישת טובין או שירותים חליפיים, נזקי רכוש, נזקי גוף, 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, מנזיקין, מרשלנות או מתיאוריית חבות אחרת, הנובע מהתקנה, משימוש או מחוסר יכולת להשתמש בתוכנה, גם אם הספקית או בעלי הרישיון שלה או החברות המסונפות אליה ידעו על האפשרות של נזקים כאלה. מכיוון שארצות וסמכויות שיפוט מסוימות אינן מתירות אי הכללה של חבות, אך עשויות להתיר הגבלת חבות, במקרים כאלה החבות של הספקית, של עובדיה, של מעניקי הרישיון שלה או של החברות המסונפות אליה 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. לא תסופק תמיכה טכנית לאחר שהתוכנה או כל אחת מהתכונות שלה יגיעו לתאריך סוף מחזור החיים המוגדר במדיניות ה-EOL. 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. פרטי רישיון, מידע ונתונים אחרים בהתאם למדיניות הפרטיות עשויים להידרש למטרה של אספקת תמיכה טכנית.

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). פרטי רישיון ונתוני זיהוי של משתמש הקצה בהתאם למדיניות הפרטיות עשויים להידרש למטרה של אימות מקוריות התוכנה.

18. **רישוי לרשויות ציבוריות וממשל ארה"ב.** התוכנה תסופק לרשויות ציבוריות, לרבות הממשל של ארה"ב, עם זכויות הרישיון וההגבלות המתוארות בהסכם זה.

19. **תאימות לבקרת סחר.**

א) לא תייצא, תייצא מחדש, תעביר את התוכנה או תעמיד אותה לרשום אדם כלשהו בדרך כזו או אחרת, במישרין או

בעקיפין, ולא תשתמש בה בכל דרך שהיא, או תנצל אותה לביצוע מעשים שעלולים לגרום ל-ESET או לחברות האחזקות שלה, לחברות הבנות ולחברות הבנות של חברות האחזקות שלה, וכן לישויות בשליטת חברות האחזקות שלה ("חברות מסונפות") להפר את חוקי בקרת הסחר או להיחשף לסנקציות שלו, לרבות

i. כל החוקים אשר מבקרים, מגבילים או משיתים דרישות רישוי על ייצוא, ייצוא מחדש או העברה של טובין, תוכנה, טכנולוגיה או שירותים, אשר נחקקו או אומצו על-ידי ממשלות, מדינות או רשויות רגולטוריות בארצות הברית, בסינגפור, בבריטניה, באיחוד האירופי או בכל אחת מהמדינות החברות בו, או בכל מדינה המחויבת להסכם, או במדינות שבהן ESET או החברות המסונפות לה מאוגדות או פועלות ("חוקי בקרת יצוא") וכן

ii. כל סנקציה, הגבלה ואמברגו כלכליים, פיננסיים, מסחריים או אחרים, חרם על יבוא או יצוא, איסור על העברת כספים או נכסים או על ביצוע שירותים, או אמצעי שווה ערך אשר הושתו על-ידי ממשלות, מדינות או רשויות רגולטוריות בארצות הברית, בסינגפור, בבריטניה, באיחוד האירופי או בכל אחת מהמדינות החברות בו, או בכל מדינה המחויבת להסכם, או במדינות שבהן ESET או החברות המסונפות לה מאוגדות או פועלות ("חוקי סנקציה").

(הפעולות החוקיות הנזכרות בנקודות i, ו- ii לעיל יכונו יחד "חוקי בקרת סחר").

ב) ל-ESET תהיה הזכות להשעות את התחייבויותיה במסגרת תנאים אלה או לסיים אותן באופן מיידי במקרה שבו:

i. חברת ESET קובעת, בהתאם לשיקול דעתה הסביר, כי המשתמש הפר או עלול להפר את הוראות סעיף 19א' להסכם; או

ii. משתמש הקצה ו/או התוכנה כפופים לחוקי בקרת סחר וכתוצאה מכך, ESET קובעת, לשיקול דעתה הסביר, כי המשך ביצוע התחייבויותיה על פי ההסכם עלול לגרום ל-ESET או לחברות המסונפות לה להפר את חוקי בקרת הסחר או להיחשף לסנקציות שלו.

ג) אף פרט בהסכם אינו מיועד, ואין לפרש או להבהיר אותו, ככזה שמעודד את הצדדים להסכם או הדורש מהם לפעול או להימנע מפעולה (או להסכים לפעולה או להימנעות מפעולה) בכל דרך שהיא שאינה עולה בקנה אחד עם חוקי בקרת הסחר הרלוונטיים או החשופה לעונשים או האסורה במסגרת ההסכם.

20. **הודעות.** כל ההודעות והחזרות התוכנה והתיעוד יימסרו אל: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, מבלי לפגוע בזכותה של ESET לתקשר איתך לגבי שינויים בהסכם זה, במדיניות פרטיות, במדיניות ה-EOL ובתיעוד בהתאם לסעיף 22 להסכם. ESET עשויה לשלוח לך הודעות דוא"ל, התראות בתוך האפליקציה באמצעות התוכנה או לפרסם את התקשורת באתר שלנו. אתה מסכים לקבל תקשורת משפטית מאת ESET בצורה אלקטרונית, לרבות תקשורת כלשהי לגבי שינוי בתנאים, בתנאים מיוחדים או במדיניות פרטיות, כל הצעת חוזה/קבלתו או הזמנות לטיפול, הודעות או תקשורת משפטית אחרת. תקשורת אלקטרונית כזו תיחשב כאילו התקבלה בכתב, אלא אם דינים תקפים דורשים באופן ספציפי צורה שונה של תקשורת.

21. **החוק החל.** 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.

22. **תנאים כלליים.** 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 נערך באנגלית. במקרה שתרגום כלשהו של ההסכם מוכן לנוחות או לכל מטרה אחרת או בכל מקרה של אי התאמה בין גרסאות השפה של הסכם זה, הגרסה האנגלית תגבר.

ESET שומרת לעצמה את הזכות לערוך שינויים בתוכנה וכן לשנות תנאים בהסכם זה, בנספחיו, בצרופותיו, במדיניות

הפרטיות, במדיניות ה-EOL ובמסמכים או כל חלק מהם בכל עת באמצעות עדכון המסמך הרלוונטי (i) כך שישקף שינויים בתוכנה או בתהליכים העסקיים של ESET, (ii) מסיבות משפטיות, רגולטוריות או מסיבות אבטחה, או (iii) כדי למנוע שימוש לרעה או נזק. תקבל הודעה על כל שינוי בהסכם בדוא"ל, בהודעה בתוך האפליקציה או באמצעי אלקטרוני אחר. אם אינך מסכים לשינויים המוצעים בהסכם, אתה רשאי לבטל אותו בהתאם לסעיף 10 בתוך 30 יום מקבלת הודעה על השינוי. אלא אם תבטל את ההסכם בתוך מגבלת זמן זו, השינויים המוצעים ייחשבו מקובלים ויחולו עליך מהתאריך שבו קיבלת הודעה על השינוי.

זהו ההסכם המלא בין הספקית ובינך בנוגע לתוכנה והוא מחליף כל ייצוג, דיון, התחייבות, תקשורת או פרסום בנוגע לתוכנה.

נספח להסכם

הערכת האבטחה של מכשירים המחוברים לרשת. הוראות נוספות חלות על מכשירים המחוברים לרשת כדלקמן:

התוכנה כוללת פונקציה לבדיקת האבטחה של הרשת המקומית של משתמש הקצה ולבדיקת האבטחה של מכשירים ברשת מקומית, הדורשת את שם הרשת המקומית ומידע על מכשירים ברשת מקומית כגון הנוכחות, הסוג, השם, כתובת ה-IP וכתובת ה-MAC של המכשיר ברשת המקומית בקשר לפרטי הרישיון. המידע כולל גם את סוג האבטחה האלחוטית וסוג ההצפנה האלחוטית של נתבים. פונקציה זו עשויה לספק גם מידע על זמינות פתרון תוכנת האבטחה למכשירים מאובטחים ברשת המקומית.

הגנה מפני שימוש לרעה בנתונים. הוראות נוספות חלות על ההגנה מפני שימוש לרעה בנתונים כדלקמן:

התוכנה מכילה פונקציה שמונעת אובדן או שימוש לרעה בנתונים חיוניים הקשורים ישירות לגניבת מחשב. כברירת מחדל, פונקציה זו מושבתת בהגדרות התוכנה. יש ליצור עבורה חשבון ESET HOME כדי להפעיל אותה, שדרכו הפונקציה תפעיל איסוף נתונים במקרה של גניבת המחשב. אם תבחר להפעיל פונקציה זו של התוכנה, מידע אודות המחשב הגנוב ייאסף ויישלח לספקית. מידע זה עשוי להכיל נתונים אודות מיקום הרשת של המחשב, נתונים אודות התוכן המוצג במסך המחשב, נתונים אודות תצורת המחשב ו/או נתונים שהוקלטו באמצעות מצלמה המחוברת למחשב (להלן "נתונים"). משתמש הקצה יהיה רשאי להשתמש בנתונים שהושגו באמצעות פונקציה זו ושסופקו דרך חשבון ESET HOME אך ורק כדי לתקן מצב שלילי שנגרם בעקבות גניבת מחשב. למטרת פונקציה זו בלבד, הספקית מעבדת את הנתונים כפי שמפורט במדיניות הפרטיות ובהתאם לתקנות המשפטיות הרלוונטיות. הספקית תאפשר למשתמש הקצה לגשת אל הנתונים לתקופה הנדרשת להשגת המטרה שלשמה הנתונים הושגו. תקופה זו לא תעלה על תקופת השמירה שמפורטת במדיניות הפרטיות. ייעשה שימוש בהגנה על נתונים מפני שימוש לרעה אך ורק במחשבים ובחשבונות שאליהם יש למשתמש הקצה גישה חוקית. כל שימוש לא חוקי ידווח לגורם המוסמך. הספקית תציית לחוקים הרלוונטיים ותסייע לרשויות אכיפת החוק במקרה של שימוש לרעה. אתה מסכים ומאשר כי אתה אחראי על אבטחת סיסמת הגישה לחשבון ESET HOME, ואתה מסכים שלא לחשוף את הסיסמה בפני אף גורם שלישי. משתמש הקצה אחראי לכל פעילות העושה שימוש בפונקציית ההגנה על נתונים מפני שימוש לרעה ושל חשבון ESET HOME, בין אם השימוש מורשה ובין אם לאו. אם חשבון ESET HOME נפגע, הודע מיד לספקית. הוראות נוספות לגבי ההגנה מפני שימוש לרעה בנתונים יחולו רק על משתמשי קצה של ESET Internet Security ושל ESET Smart Security Premium.

ESET Secure Data. הוראות נוספות חלות על ESET Secure Data כדלקמן:

1. הגדרות. בהוראות נוספות אלה ל-ESET Secure Data המילים הבאות מקבלות את המשמעויות המתאימות:

א) "מידע"כל מידע או נתונים שהוצפנו או שפוענחו באמצעות התוכנה;

ב) "מוצרים" התוכנה והתיעוד של ESET Secure Data;

ג) "ESET Secure Data"התוכנה/התוכנות שנעשה בה/ן שימוש להצפנה ולפענוח של נתונים אלקטרוניים;

כל אזכור של לשון רבים יכלול את לשון יחיד וכל אזכור של לשון זכר יכלול את לשון נקבה ולשון סתמי, ולהיפך. יש להשתמש במילים ללא הגדרה ספציפית בהתאם להגדרות המתוארות בהסכם.

2. הצהרה נוספת של משתמש הקצה. אתה מאשר ומקבל את התנאים הבאים:

א) מתוקף אחריותך להגן, לתחזק ולגבות מידע;

ב) עליך לגבות באופן מלא את כל המידע והנתונים (לרבות, אך ללא הגבלה, כל מידע ונתונים קריטיים) במחשב שלך לפני התקנת ESET Secure Data;

ג) עליך לנהל רישום של כל הסיסמאות או מידע אחר המשמש להגדרת ESET Secure Data ולשימוש בתוכנה, ולשמור אותו במקום בטוח. כמו כן, עליך ליצור עותקים לגיבוי של כל מפתחות ההצפנה, קודי הרישיון, קבצי המפתח ונתונים אחרים המופקים במדיות אחסון נפרדות;

ד) אתה 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 אחרים בכל מקום ובכל דרך שבהם מידע או נתונים אלה מאוחסנים;

ה) 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;

ו) משתמש הקצה אחראי להבטיח שרמת האבטחה וההצפנה שמספקים המוצרים הולמת את דרישותיך;

ז) אתה 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);

ח) תוכנת ESET Secure Data 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 ESET Secure Data. התוכנה עשויה לשלוח פרטי מערכת כלליים הקשורים לתפקוד שלה בהתאם למדיניות הפרטיות.

ט) 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.

הוראות נוספות לגבי ESET Secure Data יחולו רק על משתמשי קצה של ESET Smart Security Premium.

Password Manager תוכנה. הוראות נוספות חלות על תוכנת Password Manager כדלקמן:

1. הצהרה נוספת של משתמש הקצה. אתה מאשר ומקבל שלא תבצע את הפעולות הבאות:

א) להשתמש ב-Password Manager Software להפעלת אפליקציות בעלות חשיבות קריטית היכולות להעמיד בסכנה חיי אדם או רכוש. הנך מבין כי Password Manager Software אינה מיועדת למטרות אלה וכי כישלון 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 בתוכנת Password Manager באופן המהווה הפרה של הסכם זה או של החוקים של הרפובליקה הסלובקית או של תחום השיפוט שלך. במיוחד, אינך רשאי להשתמש בתוכנת Password Manager 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 בין היתר, ניסיונות כלשהם לגשת לחשבונות באחסון (למטרות תנאים נוספים אלה לתוכנת Password Manager, "אחסון" מתייחס לשטח אחסון הנתונים המנוהל על ידי הספקית או על ידי צד שלישי שאינו הספקית או המשתמש, ומיועד לאפשר סנכרון וגיבוי של נתוני המשתמש) או לכל חשבון או נתונים של משתמשים אחרים בתוכנת Password Manager 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 בתוכנת Password Manager ללא אפשרות לקבלת החזר כספי.

2. הגבלת חבות. 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 סנכרון נתונים וגיבוי. הצפנת הנתונים באמצעות PASSWORD MANAGER SOFTWARE אינה מרמזת על אחריות כלשהי של הספקית באשר לאבטחת נתונים אלה. הנך 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 סנכרון 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. הנך 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.

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.

הנך 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.

3. 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. הנך 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, והנך 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. הנך אחראי על תחזוקת האבטחה של כל אמצעי הגישה.

4. 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 לקובצי 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.

מתוקף השימוש שלך בתוכנת Password Manager, אתה 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 תוכנת Password Manager. התוכנה עשויה לשלוח פרטי מערכת כלליים הקשורים לתפקוד של תוכנת Password Manager בהתאם למדיניות הפרטיות.

5. מידע והוראות בנושא הסרת התקנה. מידע והוראות בנושא הסרת התקנה. לפני הסרת ההתקנה של Password Manager Software, יש לייצא את כל המידע שברצונך לשמור ממסד הנתונים.

הוראות נוספות לגבי תוכנת Password Manager יחולו רק על משתמשי קצה של ESET Smart Security Premium.

ESET LiveGuard. הוראות נוספות חלות על ESET LiveGuard כדלקמן:

התוכנה מכילה פונקציה של ניתוח נוסף של קבצים שנשלחו על ידי משתמש קצה. הספקית תשתמש בקבצים שנשלחו על ידי משתמש קצה ובתוצאות הניתוח אך ורק בהתאם למדיניות הפרטיות ובהתאם לתקנות החוקיות הרלוונטיות.

הוראות נוספות לגבי ESET LiveGuard יחולו רק על משתמשי קצה של ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

מדיניות פרטיות

ההגנה על נתונים אישיים היא בעלת חשיבות מיוחדת עבור 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: 31333532 כבקרית נתונים ("ESET" או ״אנחנו״). ברצוננו לציית לדרישה לשקיפות כפי שנקבעה במסגרת התקנה הכללית של האיחוד האירופי להגנה על נתונים ("GDPR"). כדי להשיג מטרה זו, אנו מפרסמים מדיניות פרטיות זו מתוך מטרה יחידה ליידע את הלקוח שלנו (״משתמש קצה״ או ״אתה״) כנושא נתונים אודות הנושאים הבאים בדבר הגנה על נתונים אישיים:

- בסיס משפטי לעיבוד של נתונים אישיים,
- שיתוף וסודיות של נתונים,
- אבטחת נתונים,
- זכויותיך כנושא נתונים,
- עיבוד הנתונים האישיים שלך
- פרטי יצירת קשר.

בסיס משפטי לעיבוד של נתונים אישיים

קיימים רק בסיסים משפטיים מועטים לעיבוד נתונים בהם אנו משתמשים בהתאם למסגרת החקיקה הרלוונטית הקשורה להגנה על נתונים אישיים. העיבוד של נתונים אישיים ב-ESET נחוץ בעיקר למימוש של הסכם רישיון למשתמש קצה הסכם הרישיון למשתמש קצה ("EULA") מול משתמש קצה (סעיף 6 (1) (b) ב-GDPR), אשר חל על אספקת מוצרים או שירותים של ESET, אלא אם צוין במפורש אחרת, למשל:

- בסיס משפטי לאינטרס לגיטימי (סעיף 6 (1) (f) ב-GDPR), המאפשר לנו לעבד נתונים לגבי האופן שבו הלקוחות שלנו משתמשים בשירותים שלנו ולגבי שביעות רצונם כדי לספק למשתמשים שלנו את ההגנה, התמיכה והניסיון הטובים ביותר שאנו יכולים להציע. אפילו שיווק מוכר על ידי החקיקה החלה כאינטרס לגיטימי, ולכן אנחנו בדרך כלל מסתמכים על כך לשם תקשורת שיווקית עם הלקוחות שלנו.
- הסכמה (סעיף 6 (1) (a) ב-GDPR), שאותה אנו עשויים לבקש ממך במצבים ספציפיים כאשר אנו רואים בסיס משפטי זה כבסיס המתאים ביותר או אם נדרש על פי חוק.
- עמידה בהתחייבות משפטית (סעיף 6 (1) (c) ב-GDPR), למשל, קביעת דרישות לתקשורת אלקטרונית, שמירת מסמכי חשבוניות או חיוב כספי.

שיתוף וסודיות של נתונים

איננו משתפים את הנתונים שלך עם צדדים שלישיים. עם זאת, ESET היא חברה שפועלת ברחבי העולם דרך חברות

מסונפות או שותפים כחלק מרשת המכירות, השירות והתמיכה שלנו. פרטי הרישוי, החיוב הכספי והתמיכה הטכנית המעובדים על-ידי ESET עשויים להיות מועברים אל חברות מסונפות או שותפים או מהם, למטרת מימוש הסכם הרישיון למשתמש קצה, כגון אספקת שירותים או תמיכה.

ESET מעדיפה לעבד את הנתונים שלה באיחוד האירופי (EU). עם זאת, בהתאם למיקום שלך (שימוש במוצרים ו/או בשירותים שלנו מחוץ לאיחוד האירופי) ו/או לשירות שתבחר, ייתכן שיהיה צורך להעביר את הנתונים שלך למדינה מחוץ לאיחוד האירופי. לדוגמה, אנו משתמשים בשירותי צד שלישי בקשר למחשוב ענן. במקרים אלה, אנו בוחרים בקפידה את ספקיות השירות שלנו ומבטיחים רמה מתאימה של הגנה על נתונים באמצעות אמצעים חוזיים, טכניים וארגוניים. ככלל, אנו מסכימים לסעיפים החוזיים הסטנדרטיים של האיחוד האירופי, במידת הצורך, בתוספת תקנות חוזיות משלימות.

במדינות מסוימות מחוץ לאיחוד האירופי, כגון בריטניה ושווייץ, האיחוד האירופי כבר קבע רמה דומה של הגנה על נתונים. בשל הרמה הדומה של הגנה על נתונים, העברת נתונים למדינות אלה אינה מחייבת אישורים או הסכמים מיוחדים כלשהם.

אבטחת נתונים

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 המתאימה וכן את משתמשי הקצה המושפעים מכך כנושאי הנתונים.

זכויות של נושא הנתונים

הזכויות של כל משתמש קצה חשובות וברצוננו ליידע אותך ש-ESET מבטיחה את הזכויות הבאות של כל משתמשי הקצה (מכל מדינה החברה באיחוד האירופי או מכל מדינה אחרת). כדי לממש את זכויותיך כנושא נתונים, באפשרותך ליצור איתנו קשר באמצעות טופס התמיכה או באמצעות דוא"ל בכתובת dpo@eset.sk. נבקש ממך לספק את המידע הבא למטרות זיהוי: שם, כתובת דוא"ל, ואם רלוונטיים, מפתח רישיון או מספר לקוח והשתייכות לחברה. נא הימנע מלשלוח לנו נתונים אישיים אחרים, כגון תאריך הלידה. ברצוננו לציין כי על מנת שנוכל לעבד את בקשתך, וכן למטרות זיהוי, נעבד את הנתונים האישיים שלך.

הזכות לבטל את ההסכמה. הזכות לבטל את ההסכמה חלה רק במקרה של עיבוד נתונים על סמך הסכמה. אם אנו מעבדים את הנתונים האישיים שלך על סמך הסכמתך, עומדת לך הזכות לבטל בכל עת את ההסכמה מבלי לציין סיבות להחלטתך. ביטול הסכמתך יחול רק על עיבוד עתידי של נתונים ולא ישפיע על חוקיות הנתונים שעובדו לפני ביטול ההסכמה.

זכות להתנגד. הזכות להתנגד לעיבוד נתונים חלה במקרה של עיבוד נתונים על סמך האינטרס הלגיטימי של ESET או של צד שלישי. אם אנו מעבדים את הנתונים האישיים לצורך הגנה על אינטרס לגיטימי, עומדת לך הזכות כנושא הנתונים להתנגד בכל עת לאינטרס הלגיטימי שלנו ולעיבוד הנתונים האישיים שלך. התנגדותך תחול רק על עיבוד עתידי של נתונים ולא תשפיע על חוקיות הנתונים שעובדו לפני הבעת ההתנגדות. אם אנו מעבדים את הנתונים האישיים שלך למטרות שיווק ישיר, אינך נדרש לציין סיבות להתנגדותך. דבר זה חל גם על יצירת פרופיל, ככל שהדבר קשור לפעילויות שיווק ישיר כאלה. בכל שאר המקרים, נבקש ממך ליידע אותנו בקצרה לגבי התלונות שלך כנגד האינטרס הלגיטימי של ESET לעיבוד הנתונים האישיים שלך.

לתשומת ליבך: במקרים מסוימים, למרות ביטול הסכמתך, נהיה רשאים להמשיך לעבד את הנתונים האישיים שלך על סמך בסיס משפטי אחר, לדוגמה, לצורך מימוש חוזה.

זכות גישה. כנושא נתונים, עומדת לך הזכות לקבל מידע על הנתונים שלך המאוחסנים על-ידי ESET – בכל עת וללא

תשלום.

זכות לתיקון. אם עיבדנו בשוגג נתונים אישיים שגויים אודותיך, עומדת לך הזכות לתקן אותם.

זכות למחיקה וזכות להגבלת העיבוד. כנושא נתונים, עומדת לך הזכות לבקש את המחיקה או ההגבלה של עיבוד הנתונים האישיים שלך. אם אנו מעבדים את הנתונים האישיים שלך, לדוגמה, בהסכמתך, ותחליט לבטל אותה בהיעדר כל בסיס משפטי אחר, לדוגמה, חוזה, נסיר את הנתונים האישיים שלך באופן מיידי. בנוסף, הנתונים האישיים שלך יוסרו מיד כאשר הם לא יידרשו עוד למטרות שצוינו עבורם בסוף תקופת השמירה שלנו.

אם אנו משתמשים בנתונים האישיים שלך למטרה הבלעדית של שיווק ישיר ותבטל את הסכמתך או תתנגד לאינטרס הלגיטימי הבסיסי של ESET, נגביל את עיבוד הנתונים האישיים שלך עד למידה שבה נכלול את פרטי יצירת הקשר שלך ברשימה השחורה הפנימית שלנו כדי להימנע מקשר לא רצוי. אחרת, הנתונים האישיים שלך יוסרו.

לתשומת ליבך: ייתכן שנידרש לאחסן את הנתונים שלך עד לתפוגת ההתחייבויות והתקופות לשמירת נתונים, כפי שנקבעו על-ידי המחוקק או הרשויות המפקחות. ההתחייבויות והתקופות לשמירת נתונים עשויות להיקבע גם בחקיקה הסלובקית. לאחר מכן, הנתונים המתאימים יוסרו באופן שגרתי.

זכות לניידות נתונים. אנו שמחים לספק לך, כנושא נתונים, את הנתונים האישיים שעובדו על-ידי ESET – בתבנית XLS.

זכות להגשת תלונה. כנושא נתונים, עומדת לך הזכות להגיש בכל עת תלונה לרשות מפקחת. ESET כפופה לרגולציה של החוקים הסלובקיים ואנו מחויבים לחקיקה בנושא הגנת נתונים כחלק מהאיחוד האירופי. הרשות המתאימה לפיקוח על נתונים היא המשרד הסלובקי להגנה על נתונים אישיים, שכתובתו Hraničná 12, 82007 Bratislava 27, Slovak Republic.

עיבוד הנתונים האישיים שלך

השירותים המסופקים על-ידי ESET והמיושמים במוצר שלנו מסופקים תחת תנאי EULA, אך חלקם עשויים לדרוש תשומת לב ספציפית. ברצוננו לספק לך פרטים נוספים על איסוף נתונים ביחס לאספקת השירותים שלנו. אנו מספקים שירותים שונים המתוארים בהסכם הרישיון למשתמש קצה ובמוצר תיעוד של. כדי לאפשר שירותים אלה, עלינו לאסוף את המידע להלן:

נתוני רישוי וחיוב כספי. השם, כתובת הדוא"ל, מפתח הרישיון (ואם רלוונטיים) הכתובת, ההשתייכות לחברה ונתוני התשלום נאספים ומעובדים על-ידי ESET כדי לסייע בהפעלת הרישיון, מסירת מפתחות הרישיון, שליחת תזכורות לגבי תפוגה, בקשות תמיכה, אימות מקוריות הרישיון, אספקת השירותים שלנו והתראות אחרות לרבות הודעות שיווקיות בהתאם לחקיקה הרלוונטית או להסכמתך. ESET מחויבת לפי חוק לשמור את פרטי החיוב הכספי לתקופה של 10 שנים. עם זאת, פרטי הרישוי יהפכו לאנונימיים לא יאוחר מ-12 חודשים ממועד תפוגת הרישיון.

עדכון ונתונים סטטיסטיים אחרים. המידע המעובד כולל 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, מעובד למטרת אספקת שירותי עדכון ושדרוג ולמטרת תחזוקה, אבטחה ושיפור של התשתית העורפית שלנו.

מידע זה נשמר מלבד פרטי הזיהוי הנדרשים למטרות רישוי וחיוב כספי מאחר והוא אינו מחייב זיהוי של משתמש הקצה. תקופת השמירה היא עד 4 שנים.

מערכת המוניטין של ESET LiveGrid®. קודי Hash חד-כיווניים המשויכים לחדירה מעובדים לצורך פעולתה של מערכת המוניטין של ESET LiveGrid®, המשפרת את יעילות הפתרונות שלנו למניעת תוכנות זדוניות על-ידי השוואת קבצים שנסרקו למסד נתונים בענן הכולל פריטים ברשימות לבנות ופריטים ברשימות שחורות. משתמש הקצה אינו מזוהה במהלך תהליך זה.

מערכת המשוב של ®ESET LiveGrid. 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

- מידע 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;
- מידע בנוגע לשימוש באינטרנט כגון כתובת IP ומידע גיאוגרפי, מנות IP, כתובות URL ומסגרות Ethernet;
- קובצי 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.

כל המידע המתקבל והמעובד באמצעות מערכת המשוב של ®ESET LiveGrid נועד לשימוש ללא זיהוי של משתמש הקצה.

הערכת האבטחה של מכשירים המחוברים לרשת. על מנת לספק את הפונקציה לבדיקת האבטחה, אנו מעבדים את שם הרשת המקומית ומידע על התקנים ברשת המקומית שלך כגון הנוכחות, הסוג, השם, כתובת ה-IP וכתובת ה-MAC של ההתקן ברשת המקומית שלך בקשר לפרטי הרישיון. המידע כולל גם את סוג האבטחה האלחוטית וסוג ההצפנה האלחוטית של נתבים. פרטי הרישוי המזהים את משתמש הקצה יהפכו לאנונימיים לא יאוחר מ-12 חודשים ממועד תפוגת הרישיון.

תמיכה טכנית. פרטי יצירת הקשר והרישוי 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. הנתונים המעובדים לצורך תמיכה טכנית מאוחסנים במשך 4 שנים.

הגנה מפני שימוש לרעה בנתונים. המידע הבא ייאסף ויעובד אם משתמש הקצה יצר חשבון ESET HOME בכתובת https://home.eset.com והפעיל את הפונקציה במקרה של גניבת מחשב: נתוני המיקום, צילומי המסך, נתונים לגבי תצורת המחשב ונתונים שתועדו באמצעות המצלמה של המחשב. הנתונים שנאספו יאוחסנו בשרתים שלנו או בשרתים של ספקיות השירות שלנו עם תקופת שמירה של 3 חודשים.

Password Manager. אם תבחר להפעיל את הפונקציה של Password Manager, הנתונים הקשורים לפרטי ההתחברות שלך יאוחסנו בצורה מוצפנת רק במחשב שלך 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. הנתונים יוסרו עם ביטול ההפעלה של הפונקציה.

ESET LiveGuard. אם תבחר להפעיל את פונקציית ESET LiveGuard המחייבת משלוח של דגימות, כגון קבצים שהוגדרו מראש וקבצים שבחר משתמש הקצה. הדגימות שתבחר לשלוח לניתוח המרוחק יועלו לשירות ESET, ותוצאת הניתוח תישלח בחזרה למחשב שלך. הדגימות החשודות מעובדות בצורה של איסוף מידע באמצעות מערכת המשוב של ESET ®LiveGrid.

תכנית לשיפור חוויית הלקוח. אם בחרת להפעיל תכנית לשיפור חוויית הלקוח , פרטי מדידת השימוש האנונימיים הנוגעים לשימוש במוצרים שלנו ייאספו וייעשה בהם שימוש בכפוף להסכמתך.

לתשומת ליבך: אם האדם שמשתמש במוצרים ובשירותים שלנו אינו משתמש הקצה שרכש את המוצר או השירות והוא סיים את הסכם הרישיון למשתמש קצה איתנו, (למשל, עובד של משתמש הקצה, בן משפחה או אדם המורשה

להשתמש במוצר או בשירות מטעם משתמש הקצה בהתאם להסכם הרישיון למשתמש קצה, עיבוד הנתונים יתבצע על סמך האינטרס הלגיטימי של ESET כמשמעותו בסעיף 6 (1) (f) ב-GDPR כדי לאפשר למשתמש המורשה מטעם משתמש הקצה להשתמש במוצרים ובשירותים המסופקים על-ידינו בהתאם להסכם הרישיון למשתמש קצה.

פרטי יצירת קשר

אם ברצונך ליישם את זכותך כנושא נתונים או שיש לך שאלה או חשש, שלח לנו הודעה לכתובת:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk