ESET Internet Security

افتح دليل المستخدم

أنقر هنا لعرض نسخة ألتعليمات على ألإنترنت من هذا ألمستند

Digital Security
Progress. Protected.

حقوق الطبع والنشر ©2024 محفوظة لـ ESET, spol. s r.o.

ESET Internet Security تم تطويره بواسطة ESET, spol. s r.o.

لمزيد من المعلومات قم بزيارة https://www.eset.com.

جميع الحقوق محفوظة. لا يجوز إعادة إنتاج أي جزء من هذه الوثائق أو تخزينه في نظام استرجاع أو نقله بأي شكل أو بأي وسيلة، إلكترونياً أو ميكانيكياً أو بالنسخ الضوئي أو التسجيل أو المسح الضوئي أو بأي طريقة أخرى دون إذن كتابي من المؤلف.

تحتفظ ESET, spol. s r.o. بالحق في تغيير أي من برامج التطبيق التي تم وصفها دون إشعار مسبق.

الدعم الفني: https://support.eset.com

REV. 12/04/2024

1 ESET Internet Security 1
1.1 ما الجديد 2
1.2 ما المنتج الذي أقتنيه؟ 2
1.3 متطلبات النظام 3
1.3 إصدار قديم من Microsoft Windows 4
1.4 الوقاية 5
1.5 صفحات التعليمات 6
2 التثبيت 7
2.1 برنامج التثبيت المباشر 8
2.2 تثبيت دون اتصال 9
2.2 ترقية الاشتراك 11
2.2 ترقية المنتج 12
2.2 الرجوع إلى إصدار أقدم من الاشتراك 12
2.2 الرجوع إلى إصدار سابق للمنتج 13
2.3 مستكشف أخطاء التثبيت ومصلحها 14
2.4 الفحص الأول بعد التثبيت 14
2.5 الترقية إلى إصدار أحدث 15
2.5 ترقية تلقائية للمنتج القديم 16
2.5 سيتم تثبيت ESET Internet Security 16
2.5 التغيير إلى خط منتج مختلف 16
2.5 التسجيل 17
2.5 تقدم التنشيط 17
2.5 نجح التنشيط 17
3 بدء الاستخدام 17
3.1 أيقونة علبة النظام 17
3.2 اختصارات لوحة المفاتيح 18
3.3 ملفات التعريف 19
3.4 تحديثات 20
3.5 تكوين حماية الشبكة 22
3.6 تمكين مكافحة السرقة 23
3.7 المراقبة الأبوية 24
4 تنشيط المنتج 24
4.1 إدخال مفتاح التنشيط أثناء التنشيط 25
4.2 استخدام حساب ESET HOME 25
4.3 تنشيط الإصدار التجريبي المجاني 26
4.4 مفتاح تنشيط ESET المجاني 27
4.5 فشل التنشيط – السيناريوهات الشائعة 27
4.6 حالة الاشتراك 28
4.6 فشل التنشيط نظراً لتجاوز حد استخدام الاشتراك 29
5 التعامل مع ESET Internet Security 30
5.1 نظرة عامة 31
5.2 فحص الكمبيوتر 34
5.2 مشغل الفحص المخصص 37
5.2 تقدم الفحص 38
5.2 سجل فحص جهاز الكمبيوتر 41
5.3 تحديث 42
5.3 نافذة الحوار – تلزم إعادة التشغيل 45
5.3 كيفية إنشاء مهام تحديث 45

5.4 الأدوات 46
5.4 ملفات السجل 47
5.4 تصفية السجل 50
5.4 العمليات الجارية 51
5.4 تقرير الأمان 52
5.4 اتصالات الشبكة 54
5.4 نشاط الشبكة 56
5.4 ESET SysInspector 57
5.4 المجدول 58
5.4 خيارات الفحص المجدول 60
5.4 نظرة عامة على المهمة المجدولة 61
5.4 تفاصيل المهمة 61
5.4 وقت المهمة 61
5.4 وقت المهمة – مرة واحدة 62
5.4 وقت المهمة – يومياً 62
5.4 وقت المهمة – أسبوعياً 62
5.4 وقت المهمة – منشئ الأحداث 62
5.4 المهمة المُتجاوزة 62
5.4 تفاصيل المهمة – تحديث 63
5.4 تفاصيل المهمة – تشغيل التطبيق 63
5.4 System cleaner 63
5.4 مراقب الشبكة 64
5.4 جهاز الشبكة في مراقب الشبكة 67
5.4 الإعلامات | مراقب الشبكة 67
5.4 العزل 68
5.4 إرسال عينة للتحليل 71
5.4 إرسال عينة للتحليل – ملف مريب 72
5.4 إرسال عينة للتحليل – موقع مريب 72
5.4 إرسال عينة للتحليل – ملف نتيجة إيجابية خاطئة 72
5.4 إرسال عينة للتحليل – موقع نتيجة إيجابية خاطئة 73
5.4 إرسال عينة للتحليل – أخرى 73
5.5 إعداد 73
5.5 حماية الكمبيوتر 74
5.5 تم اكتشاف حالة تسلل 75
5.5 حماية الإنترنت 78
5.5 حماية مضادة للتصيد الاحتيالي 80
5.5 المراقبة الأبوية 82
5.5 استثناءات موقع الويب 84
5.5 نسخ الاستثناء من المستخدم 86
5.5 نسخ الفئات من الحساب 86
5.5 حماية الشبكة 86
5.5 اتصالات الشبكة 87
5.5 تفاصيل اتصال الشبكة 88
5.5 استكشاف أخطاء الوصول إلى الشبكة وإصلاحها 88
5.5 قائمة حظر عناوين IP المؤقتة 89
5.5 سجلات حماية الشبكة 90
5.5 حل مشكلات في جدار الحماية من 91
5.5 التسجيل وإنشاء قواعد أو استثناءات من السجل 91
5.5 إنشاء قاعدة من السجل 91
5.5 إنشاء استثناءات من إعلامات جدار الحماية الشخصي 92

5.5 حماية الشبكة التسجيل المتقدم 92
5.5 حل المشكلات باستخدام أداة فحص حركة مرور الشبكة 92
5.5 تم حظر تهديد الشبكة 93
5.5 تم اكتشاف شبكة جديدة 94
5.5 إنشاء اتصال ـ اكتشاف 95
5.5 تغيير التطبيق 97
5.5 الاتصال الوارد الموثوق به 97
5.5 الاتصال الصادر الموثوق به 98
5.5 الاتصال الوارد 100
5.5 الاتصال الصادر 101
5.5 إعداد عرض الاتصال 102
5.5 أدوات الأمان 103
5.5 التصفح المصرفي الآمن 103
5.5 إعلام في المتصفح 104
5.5 خصوصية وأمان المتصفح 104
5.5 مكافحة السرقة 106
5.5 سجّل الدخول إلى حساب ESET HOME. 108
5.5 تعيين اسم جهاز 110
5.5 تم تمكين/تعطيل مكافحة السرقة 110
5.5 فشلت إضافة جهاز جديد 110
5.5 استيراد الإعدادات وتصديرها 110
5.6 المساعدة و الدعم 111
5.6 حول ESET Internet Security 112
5.6 أخبار ESET 112
5.6 إرسال بيانات تكوين النظام 113
5.6 الدعم الفني 114
5.7 حساب ESET HOME 114
5.7 الاتصال بـ ESET HOME 116
5.7 تسجيل الدخول إلى ESET HOME 117
5.7 فشل تسجيل الدخول – الأخطاء الشائعة 118
5.7 إضافة جهاز إلى ESET HOME 119
6 الإعداد المتقدم 119
6.1 محرك الكشف 120
6.1 الاستبعادات 120
6.1 استبعادات الأداء 121
6.1 إضافة استثناء أداء أو تحريره 122
6.1 تنسيق استبعاد المسار 123
6.1 استبعادات الاكتشاف 124
6.1 إضافة استثناء اكتشاف أو تحريره 126
6.1 إنشاء معالج استبعاد الاكتشاف 127
6.1 كشف محرك الخيارات المتقدمة 127
6.1 أداة فحص حركة نقل البيانات عبر الشبكة 128
6.1 الحماية المستندة إلى السحابة 128
6.1 عامل تصفية الاستبعاد للحماية المستندة إلى السحابة 131
6.1 عمليات فحص البرامج الضارة 131
6.1 ملفات تعريف الفحص 132
6.1 أهداف الفحص 132
6.1 فحص حالة الخمول 133
6.1 اكتشاف حالة الخمول 133
6.1 الفحص عند بدء التشغيل 134

6.1 فحص ملفات بدء التشغيل التلقائي 134
6.1 الوسائط القابلة للإزالة 135
6.1 حماية المستندات 136
6.1 HIPS - نظام منع اختراق المضيف 136
6.1 استبعادات HIPS 138
6.1 الإعداد المتقدم لـ HIPS 139
6.1 السماح بتحميل برامج التشغيل دائماً 139
6.1 نافذة HIPS التفاعلية 139
6.1 تم إنهاء وضع التعلم 141
6.1 تم اكتشاف سلوك محتمل لبرنامج رانسوم (الفدية) 141
6.1 إدارة قواعد HIPS 142
6.1 إعدادات قواعد HIPS 143
6.1 إضافة مسار التسجيل/التطبيق لـ HIPS 146
6.2 تحديث 146
6.2 التراجع عن التحديث 148
6.2 الفاصل الزمني للتراجع 150
6.2 تحديثات المنتج 150
6.2 خيارات الاتصال 150
6.3 وسائل الحماية 151
6.3 الحماية في الوقت الفعلي لنظام الملفات 154
6.3 استثناءات العمليات 156
6.3 إضافة استثناءات العمليات او تحريرها 157
6.3 متى تقوم بتعديل تكوين الحماية في الوقت الفعلي 157
6.3 التحقق من الحماية في الوقت الفعلي 158
6.3 ماذا تفعل إذا لم تعمل الحماية في الوقت الفعلي 158
6.3 حماية الوصول إلى الشبكة 158
6.3 ملفات تعريف اتصال شبكة 159
6.3 إضافة ملفات تعريف اتصال الشبكة أو تحريرها 160
6.3 المنشِطات 162
6.3 مجموعات IP 163
6.3 تحرير مجموعات IP 163
6.3 مراقب الشبكة 164
6.3 جدار حماية 165
6.3 إعدادات وضع التعرف 166
6.3 قواعد جدار الحماية 167
6.3 إضافة قواعد جدار الحماية أو تحريرها 169
6.3 اكتشاف تعديل التطبيقات 172
6.3 قائمة التطبيقات المستثناة من الاكتشاف 172
6.3 الحماية ضد هجمات الشبكة (IDS) 173
6.3 قواعد IDS 173
6.3 الحماية ضد هجمات القوة الغاشمة 176
6.3 القواعد 176
6.3 خيارات متقدمة 178
6.3 SSL/TLS 180
6.3 قواعد فحص التطبيق 182
6.3 قواعد الشهادة 182
6.3 حركة مرور شبكة مشفرة 183
6.3 حماية عميل البريد الإلكتروني 184
6.3 حماية نقل البريد 184
6.3 التطبيقات المستبعدة 185

6.3 عناوين IP المستبعدة 186
6.3 حماية صندوق البريد 187
6.3 عمليات التكامل 189
6.3 شريط أدوات Microsoft Outlook 189
6.3 مربع حوار التأكيد 190
6.3 إعادة فحص الرسائل 190
6.3 الاستجابة 190
6.3 إدارة قوائم العناوين 192
6.3 قوائم العناوين 192
6.3 إضافة/تحرير عنوان 194
6.3 نتيجة معالجة العنوان 194
6.3 ThreatSense 194
6.3 حماية الوصول إلى الويب 198
6.3 التطبيقات المستبعدة 199
6.3 عناوين IP المستبعدة 200
6.3 إدارة قائمة URL 201
6.3 قائمة العناوين 203
6.3 إنشاء قائمة جديدة لعناوين 204
6.3 كيفية إضافة قناع URL 204
6.3 فحص حركة نقل البيانات عبر HTTP(S) 205
6.3 ThreatSense 205
6.3 المراقبة الأبوية 209
6.3 حسابات المستخدمين 209
6.3 إعدادات حساب المستخدم 209
6.3 الفئات 212
6.3 حماية المتصفح 213
6.3 التصفح المصرفي الآمن 213
6.3 التحكم في الجهاز 214
6.3 محرر قواعد التحكم في الجهاز 215
6.3 الأجهزة التي تم اكتشافها 216
6.3 إضافة قواعد التحكم في الجهاز 216
6.3 مجموعات الأجهزة 219
6.3 حماية كاميرا الويب 220
6.3 محرر قواعد حماية كاميرا الويب 221
6.3 ThreatSense 221
6.3 مستويات التنظيف 224
6.3 قائمة العناوين المستبعدة من الفحص 225
6.3 معلمات ThreatSense الإضافية 225
6.4 الأدوات 226
6.4 تحديث Microsoft Windows® 226
6.4 نافذة الحوار ـ تحديثات النظام 226
6.4 معلومات التحديث 227
6.4 ESET CMD 227
6.4 ملفات السجل 228
6.4 وضع الألعاب 229
6.4 التشخيصات 230
6.4 الدعم الفني 232
6.5 إمكانية الاتصال 232
6.6 واجهة المستخدم 233
6.6 عناصر واجهة المستخدم 233

6.6 إعداد الوصول 234
6.6 كلمة المرور للإعداد المتقدم 235
6.6 دعم قارئ الشاشة 236
6.7 الإعلامات 236
6.7 نافذة الحوار ـ حالات التطبيق 237
6.7 إعلامات سطح المكتب 237
6.7 قائمة إعلامات سطح المكتب 239
6.7 التنبيهات التفاعلية 240
6.7 رسائل التأكيد 242
6.7 جارٍ إعادة التوجيه 243
6.8 إعدادات الخصوصية 245
6.8 إرجاع للإعدادات الافتراضية 246
6.8 إرجاع كل الإعدادات في القسم الحالي 246
6.8 حدث خطأ أثناء حفظ التكوين 246
6.9 فاحص سطر الأوامر 247
7 الأسئلة الشائعة 248
7.1 كيفية تحديث ESET Internet Security 249
7.2 كيفية إزالة فيروس من الكمبيوتر 249
7.3 كيفية السماح بالاتصال لتطبيق معين 250
7.4 كيفية تمكين المراقبة الأبوية لحساب 251
7.5 كيفية إنشاء مهمة جديدة في المجدول 252
7.6 كيفية جدولة فحص أسبوعي للكمبيوتر 252
7.7 كيفية إلغاء تأمين الإعداد المتقدم 253
7.8 كيفية حل إلغاء تنشيط المنتج من ESET HOME 253
7.8 تم إلغاء تنشيط المنتج، تم قطع اتصال الجهاز 254
7.8 لم يتم تنشيط المنتج 254
8.1 برنامج تحسين تجربة العميل 254
8.2 اتفاقية ترخيص المستخدم النهائي 255
8.3 سياسة الخصوصية 267

ESET Internet Security

يمثل ESET Internet Security أسلوباً جديداً لأمان كمبيوتر متكامل على نحو حقيقي. يستخدم أحدث إصدار من محرك فحص ESET LiveGrid® بالاشتراك مع جدار الحماية الخاص بنا ووحدات الحماية من برامج التجسس، السرعة والدقة للحفاظ على الكمبيوتر الخاص بك آمناً. والنتيجة هي نظام ذكي على حذر دائم من الهجمات والبرامج الضارة التي تهدد الكمبيوتر الخاص بك.

يعد ESET Internet Security حل أمان كاملاً لدمج الحماية القصوى والحد الأدنى من بصمة النظام. تستخدم التقنيات المتقدمة الذكاء الاصطناعي لمنع حالات التسلل من خلال الفيروسات وبرامج التجسس وأحصنة طروادة والفيروسات المتنقلة وبرامج الإعلانات وملفات روت كيت وغيرها من الهجمات دون إعاقة أداء النظام أو تعطيل الكمبيوتر.

الميزات والفوائد

واجهة المستخدم المعاد تصميمها	تمت إعادة تصميم واجهة المستخدم في هذا الإصدار بشكل ملحوظ وتبسيطها على أساس نتائج اختبار إمكانية الاستخدام. تمت مراجعة الإعلامات وكلامات واجهة المستخدم الرسومية بعناية وتوفر هذه الوجهة الآن دعماً للغات المكتوبة من اليمين لليسار مثل العبرية والعربية. تم دمجالتعليمات عبر الإنترنت الآن فيESET Internet Security وتوفر محتوى الدعم المحدث ديناميكياً.
الوضع الداكن	عبارة عن ملحق يساعدك في تبديل الشاشة بسرعة إلى مظهر داكن. يمكنك اختيار نظام الألوان المفضل لديك في عناصر واجهة المستخدم.
مكافحة الفيروسات وبرامج التجسس	الاكتشاف الاستباقي وتنظيف الفيروسات المعروفة وغير المعروفة والفيروسات المتنقلة ووأحصنة طروادة ووالروت كيت. تعمل الأساليب البحثية المتقدمة حمايتك من التهديدات غير المعروفة وإبطال مفعولها قبل حدوث أي ضرر وذلك حتى قبل التعرض لأية برامج ضارة. تعمل حماية استخدام الإنترنت والحماية ضد التصيد الاحتيالي من خلال مراقبة الاتصال بين متصفحات الويب والخوادم البعيدة (بما في ذلك SSL). توفر حماية عميل البريد الإلكتروني التحكم في اتصالات البريد الإلكتروني المستلَمة من خلال بروتوكولي POP3(S) وIMAP(S).
تحديثات منتظمة	التحديث المنتظم لمحرك الكشف (المعروف سابقاً باسم "قاعدة بيانات.توقيعات الفيروسات") ووحدات البرنامج أفضل طريقة للحصول على أقصى مستوى من الأمان على الكمبيوتر.
ESET LiveGrid® (السمعة المستندة إلى السحابة)	يمكنك فحص سمعة الملفات والعمليات الجارية مباشرةً منESET Internet Security.
التحكم في الجهاز	يعمل على فحص جميع محركات فلاش USB وبطاقات الذاكرة والأقراص المضغوطة وأقراص DVD. حظر الوسائط القابلة للإزالة على أساس نوع الوسائط والشركة المصنِّعة والحجم والسمات الأخرى.
وظيفة نظام منع اختراق المضيف	يمكنك تخصيص أداء النظام بالتفصيل وتحديد قواعد سجل النظام والعمليات النشطة والبرامج وضبط وضع الأمان لديك.
وضع الألعاب	يتم تأجيل كل النوافذ المنبثقة أو التحديثات أو الأنشطة المتعلقة بالنظام للحفاظ على موارد النظام للألعاب وأنشطة ملء الشاشة الأخرى.

الميزات في ESET Internet Security

التصفح المصرفي الآمن	يتيح التصفح المصرفي الآمن مستعرضاً آمناً للاستخدام عند الوصول إلى بوابة الصرافة أو الدفع عبر الإنترنت لضمان وقوع كل الحركات عبر الإنترنت في بيئة آمنة وموثوق فيها.

دعم توقيعات الشبكة	تتيح توقيعات الشبكة التحديد السريع وحظر حركات المرور الضارة الصادرة من أجهزة المستخدمين وإليها مثل البوتات وحزم الثغرات. يمكن اعتبار الميزة تحسين حماية البوت نت.
جدار الحماية الذكي	يمنع المستخدمين غير الموثوق فيهم من الوصول إلى الكمبيوتر الخاص بك والاستفادة من بياناتك الشخصية.
برنامج مكافحة البريد العشوائي لعميل البريد الإلكتروني	يمثل البريد العشوائي ما يصل إلى 50 بالمئة من جميع اتصالات البريد الإلكتروني. يحمي برنامج مكافحة البريد العشوائي لعميل البريد الإلكتروني من هذه المشكلة.
مكافحة السرقة	مكافحة السرقة تعمل على زيادة الأمان على مستوى المستخدم في حالة فقد الجهاز أو سرقته. عند تثبيت ESET Internet Security و مكافحة السرقة، سيتم إدراج جهازك في واجهة الويب. تتيح لك واجهة الويب إدارة تكوين مكافحة السرقة وإدارة ميزات مكافحة السرقة على جهازك.
المراقبة الأبوية	يمكنك حماية عائلتك من محتوى الويب المسيئة عن طريق حظر فئات مواقع الويب المتنوعة.

يجب أن يكون الاشتراك نشطاً حتى يتم تشغيل ميزات ESET Internet Security. نوصي بتجديد اشتراكك قبل عدة أسابيع من انتهاء صلاحية اشتراك ESET Internet Security.

ما الجديد

ما الجديد في ESET Internet Security 17.1

- تحسينات صغيرة على مراقب الشبكة
- تحسينات صغيرة على التصفح المصرفي الآمن
- إصلاحات الأخطاء الطفيفة الأخرى والتحسينات

لتعطيل **إعلامات "ما الجديد"**:
1. افتح الإعداد المتقدم > **الإعلامات** > **إعلامات سطح المكتب**.
2. انقر فوق **تحرير** بجوار **إعلامات سطح المكتب**.
3. انقر فوق تحرير بجوار إعلامات سطح المكتب وقم بإلغاء تحديد مربع الاختيار **عرض إعلامات "ما الجديد"** وانقر فوق **موافق**.

لمزيد من المعلومات حول الإعلامات، راجع قسم الإعلامات.

للحصول على قائمة مفصلة بالتغييرات في ESET Internet Security راجع سجلات التغيير ESET Internet Security سجلات التغيير.

ما المنتج الذي أقتنيه؟

تقدم ESET طبقات متعددة من الأمن مع منتجات جديدة بداية من حل مكافحة الفيروسات القوي والسريع حتى حل الأمان الكل في واحد مع أدنى حد من بصمة النظام:

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

لتحديد المنتج الذي قمت بتثبيته، افتح نافذة البرنامج الرئيسية و سترى اسم المنتج موجوداً أعلى النافذة (راجع مقالة قاعدة المعارف).

يفصّل الجدول الوارد أدناه الميزات المتوفرة في كل منتج محدد.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
محرك الكشف	✔	✔	✔	✔
التعلم الآلي المتقدم	✔	✔	✔	✔
استغلال مانع	✔	✔	✔	✔
الحماية ضد الهجمات المستندة إلى البرنامج النصي	✔	✔	✔	✔
حماية مضادة للتصيد الاحتيالي	✔	✔	✔	✔
حماية الوصول إلى الويب	✔	✔	✔	✔
HIPS (بما في ذلك الحماية من برامج الفدية)	✔	✔	✔	✔
الحماية ضد البريد العشوائي		✔	✔	✔
جدار حماية		✔	✔	✔
مراقب الشبكة		✔	✔	✔
حماية كاميرا الويب		✔	✔	✔
الحماية ضد هجمات الشبكة		✔	✔	✔
الحماية ضد البوت نت		✔	✔	✔
التصفح المصرفي الآمن		✔	✔	✔
خصوصية وأمان المتصفح		✔	✔	✔
المراقبة الأبوية		✔	✔	✔
مكافحة السرقة		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

قد لا تتوفر بعض المنتجات الموجودة أعلاه بلغتك / منطقتك.

متطلبات النظام

يجب أن يلبي نظامك متطلبات الجهاز والمتطلبات البرمجية التالية لبرنامج ESET Internet Security لتقديم أداء مثالي:

المعالجات المدعومة

معالج Intel أو AMD 32 بت (x86) مع مجموعة تعليمات SSE2 أو 64 بت (x64) 1 جيجاهرتز أو أعلى
معالج قائم على ARM64 1 جيجاهرتز أو أعلى

أنظمة التشغيل المدعومة

Microsoft® Windows® 11

Microsoft® Windows® 10

يجب تثبيت دعم توقيع كود Azure على جميع أنظمة تشغيل Windows لتثبيت أو ترقية منتجات ESET التي تم إصدارها بعد يوليو 2023. مزيد من المعلومات.

حاول دائماً تحديث نظام التشغيل لديك.

متطلبات ميزات ESET Internet Security

راجع متطلبات النظام لمعرفة ميزات ESET Internet Security المحددة في الجدول أدناه:

المتطلبات	ميزة
راجع المعالجات المدعومة.	Intel® Threat Detection Technology
راجع متصفحات الويب المدعومة.	التصفح المصرفي الآمن
إصدار Windows 10 RS4 والإصدارات الأحدث.	خلفية شفافة
معالج لا يستند إلى ARM64.	أداة المسح المخصصة
معالج لا يستند إلى ARM64.	System cleaner
معالج لا يستند إلى ARM64.	استغلال مانع
معالج لا يستند إلى ARM64.	فحص السلوك الشامل

أخرى

مطلوب اتصال بالإنترنت للتنشيط وتحديثات ESET Internet Security لتعمل بشكل صحيح.

يؤدي برنامجان لمكافحة الفيروسات يعملان في وقت واحد على جهاز واحد إلى تعارضات حتمية في موارد النظام، مثل إبطاء النظام لجعله غير قابل للتشغيل

إصدار قديم من Microsoft Windows

المشكلة

- تريد تثبيت أحدث إصدار من ESET Internet Security على جهاز كمبيوتر يعمل بنظام التشغيل Windows 7 أو

Windows 8 (8.1) أو Windows Home Server 2011

- ESET Internet Security يعرض خطأ **نظام تشغيل قديم** أثناء التثبيت

تفاصيل

يتطلب أحدث إصدار من ESET Internet Security نظام تشغيل Windows 10 أو Windows 11.

الحل

تتوفر الحلول التالية:

الترقية إلى نظام التشغيل Windows 10 أو Windows 11

عملية الترقية سهلة نسبياً ، وفي كثير من الحالات ، يمكنك القيام بذلك دون فقدان ملفاتك. قبل الترقية إلى Windows 10:

1. النسخ الاحتياطي للبيانات المهمة.
2. اقرأ الأسئلة الشائعة الخاصة بالترقية إلى Windows 10 أو الأسئلة الشائعة الخاصة بالترقية إلى Windows 11 من Microsoft وقم بتحديث نظام تشغيل Windows الخاص بك.

تثبيت ESET Internet Security الإصدار 16.0

إذا لم تتمكن من ترقية Windows فقم بتثبيت ESET Internet Security الإصدار 16.0. لمزيد من المعلومات، راجع ESET Internet Security الإصدار 16.0 التعليمات عبر الإنترنت.

الوقاية

عند العمل مع الكمبيوتر، وبخاصة عند استعراض الإنترنت، الرجاء تذكر أنه لا يوجد أي برنامج حماية ضد الفيروسات في العالم يمكنه الإزالة التامة خطر الاكتشافات والهجمات عن بعد. ولتوفير أقصى حماية وطمأنينة، من الضروري استخدام حل الحماية ضد الفيروسات بشكل صحيح والالتزام بقواعد مفيدة متعددة:

التحديث المنتظم

وفقاً لإحصاءات من ESET LiveGrid® يتم إنشاء آلاف حالات التسلل الجديدة والفريدة يومياً لتخطي مقاييس الأمان الحالية، وتحقيق أرباح لمؤلفيها، وذلك كله على نفقة مستخدمين آخرين. يحلل المتخصصون في مختبر البحث التابع لشركة ESET تلك التهديدات، ويُعدون تحديثات ويصدرونها لتحسين مستوى الحماية لمستخدمينا باستمرار. لضمان أقصى كفاءة لتلك التحديثات، من الضروري تكوين التحديثات بشكل صحيح على نظامك. لمزيد من المعلومات حول كيفية تكوين تحديثات، راجع الفصل إعداد التحديث.

تنزيل تصحيحات الأمان

يخترق مؤلفو البرامج الضارة عادةً مختلف ثغرات النظام لزيادة فاعلية نشر التعليمات البرمجية الضارة. مع أخذ ذلك في الاعتبار، تراقب شركات البرامج عن كثب لاكتشاف أي ثغرات تظهر في تطبيقاتها وتُصدر تحديثات أمان للتخلص من التهديدات المحتملة دورياً. من المهم تنزيل تحديثات الأمان تلك بمجرد إصدارها. ويعد نظام التشغيل Microsoft Windows ومستعرضات الويب مثل Internet Explorer مثالين على البرامج التي تصدُر لها تحديثات أمان دورياً.

النسخ الاحتياطي للبيانات المهمة

لا يراعي منشئو البرامج الضارة عادة احتياجات المستخدمين، وغالباً ما يؤدي نشاط البرامج الضارة إلى خلل وظيفي إجمالي لنظام التشغيل وفقد البيانات المهمة. من المهم إجراء نسخ احتياطي دوري لبياناتك المهمة والحساسة على مصدر خارجي كقرص DVD أو محرك أقراص ثابت خارجي. وسيسهِّل ذلك استرداد بياناتك في حالة تعطل النظام ويسرِّعه إلى حد كبير.

الفحص الدوري للكمبيوتر بحثاً عن فيروسات

يتم التعامل مع اكتشاف المزيد من الفيروسات والفيروسات المتنقلة وأحصنة طروادة وبرامج الروت كيت المعروفة وغير المعروفة بواسطة وحدة حماية نظام الملفات في الوقت الفعلي. وهذا يعني أنه كلما استخدمت ملفاً أو فتحته، يتم فحصه بحثاً عن نشاط برامج ضارة به. نوصى بإجراء فحص كمبيوتر كامل مرة على الأقل شهرياً، لأن توقيعات البرامج الضارة قد تختلف، وتحدِّث محرك الكشف نفسه مرة يومياً.

اتباع قواعد الأمان الأساسية

تعد هذه القاعدة أكثر القواعد إفادة وكفاءة ـ فاحرص عليها. يتطلب اليوم الكثير من حالات التسلل تدخل المستخدم ليتم تنفيذها وتوزيعها. لذا، إذا تحليت بالحذر المطلوب عند فتح ملفات جديدة، فستوفر وقتاً وجهداً كبيرين، كان من الممكن إهدارهما في تنظيف حالات التسلل. فيما يلي بعض الإرشادات المفيدة:

- لا تقم بزيارة مواقع ويب مريبة تحتوي على العديد من النوافذ المنبثقة والإعلامات الوامضة.
- توخَّ الحذر عند تثبيت برامج مجانية وحزم فك ترميز وغيرها. فلا تستخدم إلا البرامج الآمنة، ولا تزُر إلا مواقع الويب الآمنة.
- توخَّ الحذر عند فتح مرفقات بريد إلكتروني، وبخاصة الرسائل المرسلة بشكل جماعي والصادرة عن مرسلين غير معروفين.
- لا تستخدم حساب المسؤول لعملك اليومي على الكمبيوتر.

صفحات التعليمات

مرحباً بك في دليل مستخدم ESET Internet Security. ستصل بك المعلومات الموفرة هنا إلى مستوى إتقان التعامل مع منتجك، كما تساعدك على توفير أمان أكثر لجهاز الكمبيوتر.

بدء الاستخدام

قبل استخدام ESET Internet Security يمكنك أن تقرأ عن أنواع مختلفة من الاكتشافات والهجمات عن بُعد التي قد تواجهها عند استخدام جهاز الكمبيوتر الخاص بك. لقد قمنا أيضاً بتجميع قائمة بالميزات الجديدة المقدمة في ESET Internet Security.

ابدأ بتثبيت ESET Internet Security. إذا كنت قد قمت بتثبيت ESET Internet Security بالفعل، راجع العمل باستخدام ESET Internet Security.

كيفية استخدام صفحة تعليمات ESET Internet Security

التعليمات عبر الإنترنت مقسمة إلى عدة فصول وفصول فرعية. اضغط على **F1** في ESET Internet Security لعرض معلومات حول النافذة المفتوحة حالياً.

يتيح لك البرنامج إمكانية البحث عن موضوع خاص بالتعليمات حسب الكلمة (بالكلمات) الأساسية، أو البحث عن محتوى من خلال كتابة كلمات أو عبارات. يعد الفارق بين هاتين الطريقتين هو أن الكلمة الأساسية يمكن أن ترتبط منطقياً بصفحات تعليمات لا تحتوي على تلك الكلمة الأساسية تحديداً في النص. سيؤدي البحث بالكلمات والعبارات إلى البحث في محتوى جميع الصفحات وعرض تلك التي تحتوي على كلمة أو عبارة البحث فقط في النص الفعلي.

للتناسق ومنع حدوث التباس، فإن المصطلحات المستخدمة في هذا الدليل تستند إلى واجهة المستخدم في ESET Internet Security. كما أننا نستخدم مجموعة موحدة من الرموز لتسليط الضوء على الموضوعات ذات الاهتمام أو الأهمية الخاصة.

مجرد ملاحظة قصيرة. رُغم أنه يمكن حذفها، إلا أن الملاحظات بإمكانها توفير معلومات ذات قيمة مثل ميزات محددة أو رابط ذو صلة لبعض الموضوعات المرتبطة.

وهذا يتطلب الانتباه إلى أننا نشجعك على عدم التخطي. عادةً ما توفر معلومات غير حرجة ولكنها مهمة.

هذه معلومات تتطلب المزيد من الحيطة والحذر. وعادة ما توضع التحذيرات لمنع المستخدم من الوقوع في الأخطاء الضارة المحتملة. اقرأ النص وافهمه، لأنه يشير إلى إعدادات النظام شديدة الحساسية أو إلى شيء محظور.

هذا عبارة عن حالة استخدام أو مثال عملي يهدف إلى مساعدتك في فهم كيف يمكن استخدام وظيفة أو ميزة معينة.

الدلالة	التحويل
أسماء عناصر واجهة مثل المربعات وأزرار الخيارات.	**بخط عريض**
عناصر نائبة للمعلومات التي تقدمها. على سبيل المثال، اسم الملف أو المسار يعني أنك تكتب المسار أو الاسم الفعلي للملف.	بخط مائل
نماذج التعليمات البرمجية أو الأوامر.	Courier New
يوفر الوصول السريع والسهل إلى الموضوعات المُشار إليها أو إلى موقع ويب خارجي. الارتباطات التشعبية مميزة باللون الأزرق وربما بها شرطة سفلية.	الارتباط التشعبي
دليل نظام Windows الذي يتم فيه تخزين البرامج المثبتة على Windows.	*%ProgramFiles%*

التعليمات عبر الإنترنت هي المصدر الرئيسي لمحتوى التعليمات. سيتم عرض أحدث إصدار من التعليمات عبر الإنترنت تلقائياً عندما تكون متصلاً بالإنترنت.

التثبيت

توجد طرق متعددة لتثبيت ESET Internet Security على الكمبيوتر الخاص بك. قد تتنوع طرق التثبيت وفقاً للبلد ووسائل التوزيع:

- Live installer – تم تنزيله من موقع ويب ESET أو أقراص CD/DVD. حزمة التثبيت عالمية لكل اللغات (اختر اللغة

المناسبة). Live installer عبارة عن ملف صغير; يتم تنزيل الملفات الإضافية المطلوبة لتثبيت ESET Internet Security تلقائياً.

- تثبيت دون اتصال – يستخدم ملف .exe أكبر من ملف Live installer ولا يتطلب اتصال بالإنترنت أو ملفات إضافية لإتمام التثبيت.

> تأكد من عدم تثبيت برامج حماية ضد الفيروسات أخرى على الكمبيوتر قبل تثبيت ESET Internet Security. حيث قد يؤدي تثبيت حلين حماية ضد الفيروسات أو أكثر على كمبيوتر واحد، فقد يتعارضان مع بعضهما. يوصى بإزالة تثبيت أي برامج حماية ضد الفيروسات أخرى على نظامك. راجع مقالة قاعدة المعارف الخاصة بنا للاطلاع على قائمة بأدوات إزالة التثبيت لبرامج الحماية ضد الفيروسات الشائعة (متوفرة باللغة الإنجليزية وعدة لغات أخرى).

برنامج التثبيت المباشر

عند تنزيل حزمة تثبيت برنامج التثبيت المباشر، انقر نقراً مزدوجاً فوق ملف التثبيت واتبع التعليمات خطوة بخطوة في معالج برنامج التثبيت.

> لهذا النوع من التثبيت، يجب الاتصال بالإنترنت.

1. حدد اللغة المناسبة من القائمة المنسدلة وانقر فوق **متابعة**.

> إذا كنت تقوم بتثبيت إصدار أحدث فوق الإصدار السابق بإعدادات محمية بكلمة مرور، فاكتب كلمة المرور الخاصة بك. يمكنك تكوين كلمة مرور الإعدادات في إعداد الوصول.

2. حدد تفضيلاتك للميزات التالية واقرأ اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية وانقر فوق **متابعة**، أو انقر فوق **السماح للجميع والمتابعة** لتمكين جميع الميزات:

- نظام ملاحظات ESET LiveGrid®
- التطبيقات المحتملة أن تكون غير مرغوب فيها

- برنامج تحسين تجربة العميل

بالنقر فوق **متابعة** أو **السماح للجميع والمتابعة**، أنت بذلك توافق على اتفاقية ترخيص المستخدم النهائي وتقرّ بسياسة الخصوصية.

3. لتنشيط أمان الجهاز وإدارته وعرضه باستخدام ESET HOME قم بتوصيل جهازك بحساب ESET HOME. انقر فوق **تخطي تسجيل الدخول** للمتابعة بدون اتصال بـESET HOME. يمكنك توصيل جهازك بحساب ESET HOME لاحقاً.
4. إذا تابعت بدون اتصال بـESET HOME فاختر خيار تنشيط. إذا كنت تقوم بتثبيت إصدار أحدث فوق الإصدار السابق، فسيتم إدخال **مفتاح التنشيط** تلقائياً.
5. يحدد معالج التثبيت منتج ESET المثبت استناداً إلى الاشتراك. يتم دائماً تحديد الإصدار الذي يحتوي على معظم ميزات الأمان مسبقاً. انقر فوق **تغيير المنتج** إذا كنت تر غب في تثبيت إصدار مختلف من منتج ESET. انقر فوق **متابعة** لبدء عملية التثبيت. قد يستغرق ذلك بضع دقائق.

إذا كان هناك أي بقايا (ملفات أو مجلدات) من منتجات ESET تم إلغاء تثبيتها في الماضي، فستتم مطالبتك للسماح بإزالتها. انقر فوق **تثبيت** للمتابعة.

6. انقر فوق **تم** للخروج من معالج التثبيت.

مستكشف أخطاء التثبيت ومصلحها.

بعد تثبيت المنتج وتنشيطه، تبدأ الوحدة النمطية في التنزيل. تتم تهيئة الحماية وقد لا تعمل بعض الميزات بشكل كامل ما لم يكتمل التنزيل.

تثبيت دون اتصال

قم بتنزيل منتج ESET Windows المنزلي وتثبيته باستخدام برنامج التثبيت في وضع عدم الاتصال (.exe) أدناه. اختر أي إصدار من منتج ESET HOME لتنزيله (32 بت أو 64 بت أو ARM).

ESET Security Ultimate	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
تنزيل 64 بت تنزيل 32 بت تنزيل ARM	تنزيل 64 بت تنزيل 32 بت تنزيل ARM	تنزيل 64 بت تنزيل 32 بت تنزيل ARM	تنزيل 64 بت تنزيل 32 بت تنزيل ARM

إذا كان لديك اتصال إنترنت نشط، فقم بتثبيت منتج ESET باستخدام Live installer.

عند تشغيل برنامج التثبيت في وضع عدم الاتصال (.exe) سيرشدك معالج التثبيت خلال عملية الإعداد.

1. حدد اللغة المناسبة من القائمة المنسدلة وانقر فوق **متابعة**.

> إذا كنت تقوم بتثبيت إصدار أحدث فوق الإصدار السابق بإعدادات محمية بكلمة مرور، فاكتب كلمة المرور الخاصة بك. يمكنك تكوين كلمة مرور الإعدادات في إعداد الوصول.

2. حدد تفضيلاتك للميزات التالية واقرأ اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية وانقر فوق **متابعة**، أو انقر فوق **السماح للجميع والمتابعة** لتمكين جميع الميزات:

- نظام ملاحظات ESET LiveGrid®
- التطبيقات المحتملة أن تكون غير مرغوب فيها
- برنامج تحسين تجربة العميل

> بالنقر فوق **متابعة** أو **السماح للجميع والمتابعة**، أنت بذلك توافق على اتفاقية ترخيص المستخدم النهائي وتقرّ بسياسة الخصوصية.

3. انقر فوق **تخطي تسجيل الدخول**. عندما يكون لديك اتصال بالإنترنت، يمكنك توصيل جهازك بحساب ESET HOME.
4. انقر فوق **تخطي التنشيط**. يجب تفعيل ESET Internet Security بعد التثبيت ليعمل بشكل كامل. يتطلب تنشيط المنتج اتصالاً نشطاً بالإنترنت.
5. يوضح معالج التثبيت منتج ESET الذي سيتم تثبيته بناءً على برنامج التثبيت في وضع عدم الاتصال الذي تم تنزيله. انقر فوق **متابعة** لبدء عملية التثبيت. قد يستغرق ذلك بضع دقائق.

> إذا كان هناك أي بقايا (ملفات أو مجلدات) من منتجات ESET تم إلغاء تثبيتها في الماضي، فستتم مطالبتك للسماح بإزالتها. انقر فوق **تثبيت** للمتابعة.

6. انقر فوق **تم** للخروج من معالج التثبيت.

مستكشف أخطاء التثبيت ومصلحها.

ترقية الاشتراك

تظهر نافذة الإعلام هذه عند تغيير الاشتراك المستخدم لتنشيط منتج ESET لديك. يسمح لك الاشتراك الذي تم تغييره بتنشيط منتج بمزيد من ميزات الأمان. إذا لم يتم إجراء أي تغيير، فسيعرض ESET Internet Security نافذة تنبيه مرة واحدة تسمى **التغيير الي منتج بمزيد من الميزات**.

نعم (مُوصى به) – سيقوم تلقائياً بتثبيت المنتج بمزيد من ميزات الأمان.

لا، شكراً – لن يتم إجراء أي تغييرات، وسيختفي الإشعار نهائياً.

لتغيير المنتج لاحقاً، راجع مقالة قاعدة معارف ESET. لمزيد من المعلومات حول اشتراك ESET راجع الأسئلة الشائعة حول الاشتراك.

يفصّل الجدول الوارد أدناه الميزات المتوفرة في كل منتج محدد.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
محرك الكشف	✔	✔	✔	✔
التعلم الآلي المتقدم	✔	✔	✔	✔
استغلال مانع	✔	✔	✔	✔
الحماية ضد الهجمات المستندة إلى البرنامج النصي	✔	✔	✔	✔
حماية مضادة للتصيد الاحتيالي	✔	✔	✔	✔
حماية الوصول إلى الويب	✔	✔	✔	✔
HIPS (بما في ذلك الحماية من برامج الفدية)	✔	✔	✔	✔
الحماية ضد البريد العشوائي		✔	✔	✔
جدار حماية		✔	✔	✔
مراقب الشبكة		✔	✔	✔
حماية كاميرا الويب		✔	✔	✔
الحماية ضد هجمات الشبكة		✔	✔	✔
الحماية ضد البوت نت		✔	✔	✔
التصفح المصرفي الآمن		✔	✔	✔
خصوصية وأمان المتصفح		✔	✔	✔
المراقبة الأبوية		✔	✔	✔
مكافحة السرقة		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

ترقية المنتج

لقد قمت بتنزيل مثبت افتراضي وقررت تغيير المنتج المراد تنشيطه، أو تريد تغيير المنتج المثبت إلى منتج يحتوي على المزيد من ميزات الأمان.

تغيير المنتج أثناء التثبيت.

يفصّل الجدول الوارد أدناه الميزات المتوفرة في كل منتج محدد.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
محرك الكشف	✔	✔	✔	✔
التعلم الآلي المتقدم	✔	✔	✔	✔
استغلال مانع	✔	✔	✔	✔
الحماية ضد الهجمات المستندة إلى البرنامج النصي	✔	✔	✔	✔
حماية مضادة للتصيد الاحتيالي	✔	✔	✔	✔
حماية الوصول إلى الويب	✔	✔	✔	✔
HIPS (بما في ذلك الحماية من برامج الفدية)	✔	✔	✔	✔
الحماية ضد البريد العشوائي		✔	✔	✔
جدار حماية		✔	✔	✔
مراقب الشبكة		✔	✔	✔
حماية كاميرا الويب		✔	✔	✔
الحماية ضد هجمات الشبكة		✔	✔	✔
الحماية ضد البوت نت		✔	✔	✔
التصفح المصرفي الآمن		✔	✔	✔
خصوصية وأمان المتصفح		✔	✔	✔
المراقبة الأبوية		✔	✔	✔
مكافحة السرقة		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

الرجوع إلى إصدار أقدم من الاشتراك

تظهر نافذة الحوار هذه عند تغيير الاشتراك المستخدم لتنشيط منتج ESET لديك. يمكن استخدام الاشتراك الذي تم تغييره فقط مع منتج ESET مختلف بميزات أمان أقل. تم تغيير المنتج تلقائياً لمنع فقدان الحماية.

لمزيد من المعلومات حول اشتراك ESET راجع الأسئلة الشائعة حول الاشتراك.

يفصّل الجدول الوارد أدناه الميزات المتوفرة في كل منتج محدد.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
محرك الكشف	✔	✔	✔	✔
التعلم الآلي المتقدم	✔	✔	✔	✔
استغلال مانع	✔	✔	✔	✔
الحماية ضد الهجمات المستندة إلى البرنامج النصي	✔	✔	✔	✔
حماية مضادة للتصيد الاحتيالي	✔	✔	✔	✔
حماية الوصول إلى الويب	✔	✔	✔	✔
HIPS (بما في ذلك الحماية من برامج الفدية)	✔	✔	✔	✔
الحماية ضد البريد العشوائي		✔	✔	✔
جدار حماية		✔	✔	✔
مراقب الشبكة		✔	✔	✔
حماية كاميرا الويب		✔	✔	✔
الحماية ضد هجمات الشبكة		✔	✔	✔
الحماية ضد البوت نت		✔	✔	✔
التصفح المصرفي الآمن		✔	✔	✔
خصوصية وأمان المتصفح		✔	✔	✔
المراقبة الأبوية		✔	✔	✔
مكافحة السرقة		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

الرجوع إلى إصدار سابق للمنتج

يحتوي المنتج الذي قمت بتثبيته حالياً على ميزات أمان أكثر من الذي ستقوم بتنشيطه. ستفقد الحماية من السرقة والوصول إلى البيانات ذات الصلة المخزّنة في ESET HOME.

يفصّل الجدول الوارد أدناه الميزات المتوفرة في كل منتج محدد.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
محرك الكشف	✔	✔	✔	✔
التعلم الآلي المتقدم	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
استغلال مانع	✔	✔	✔	✔
الحماية ضد الهجمات المستندة إلى البرنامج النصي	✔	✔	✔	✔
حماية مضادة للتصيد الاحتيالي	✔	✔	✔	✔
حماية الوصول إلى الويب	✔	✔	✔	✔
HIPS (بما في ذلك الحماية من برامج الفدية)	✔	✔	✔	✔
الحماية ضد البريد العشوائي		✔	✔	✔
جدار حماية		✔	✔	✔
مراقب الشبكة		✔	✔	✔
حماية كاميرا الويب		✔	✔	✔
الحماية ضد هجمات الشبكة		✔	✔	✔
الحماية ضد البوت نت		✔	✔	✔
التصفح المصرفي الآمن		✔	✔	✔
خصوصية وأمان المتصفح		✔	✔	✔
المراقبة الأبوية		✔	✔	✔
مكافحة السرقة		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

مستكشف أخطاء التثبيت ومصلحها

في حالة حدوث مشكلات أثناء التثبيت، يوفر معالج التثبيت مستكشف الأخطاء ومصلحها لحل المشكلة، إن أمكن.

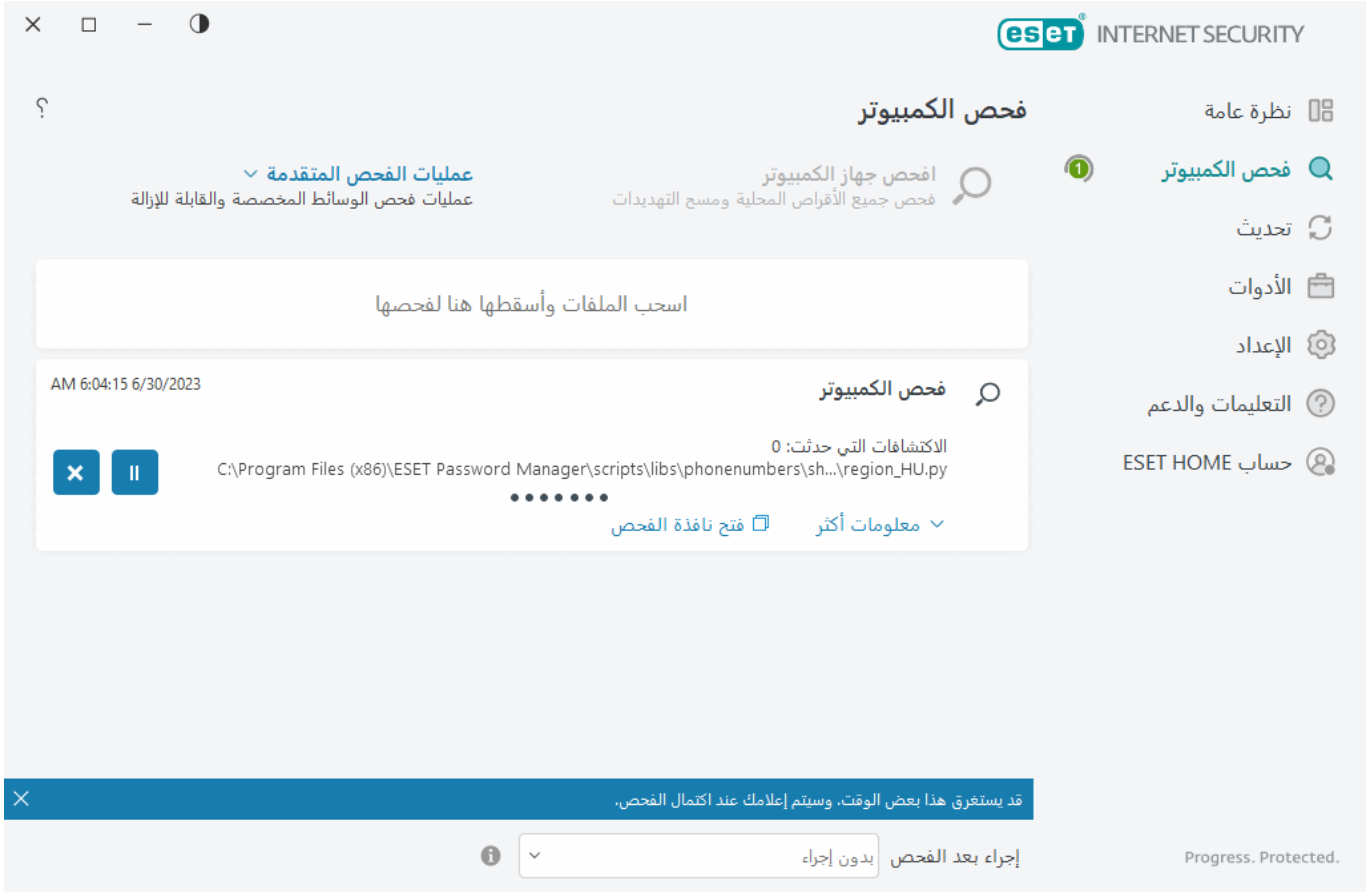
انقر فوق **تشغيل مستكشف الأخطاء ومصلحها** لبدء تشغيل مستكشف الأخطاء ومصلحها. عند انتهاء مستكشف الأخطاء ومصلحها، اتبع الحل الموصى به.

إذا استمرت المشكلة، فراجع قائمة أخطاء التثبيت الشائعة والحلول.

الفحص الأول بعد التثبيت

بعد تثبيت ESET Internet Security سيبدأ فحص الكمبيوتر تلقائياً بعد التحديث الناجح الأول لفحص التعليمات البرمجية الضارة.

يمكن بدء فحص الكمبيوتر يدوياً من نافذة البرنامج الرئيسية بالنقر فوق **فحص الكمبيوتر** > **فحص الكمبيوتر الخاص بك**. لمزيد من المعلومات حول أنواع فحص الكمبيوتر، راجع فحص الكمبيوتر.



الترقية إلى إصدار أحدث

تصدُر إصدارات أحدث من ESET Internet Security لتنفيذ تحسينات أو حل مشكلات لا يمكن حلها بواسطة التحديثات التلقائية لوحدات البرنامج. يمكن إجراء الترقية إلى إصدار أحدث بعدة طرق:

1. تلقائياً، بواسطة تحديث برنامج.
ونظراً لأن ترقية البرنامج يتم توزيعها إلى جميع المستخدمين، وقد تؤثر على تكوينات معينة للنظام، يتم إصدارها بعد فترة اختبار طويلة لتعمل مع جميع تكوينات النظام المحتملة. في حالة الحاجة إلى الترقية إلى إصدار أحدث فور إصداره، استخدم إحدى الطريقتين التاليتين.
تأكد من قيامك بتمكين **تحديثات ميزة التطبيق** في الإعداد المتقدم > **التحديث** > **ملفات التعريف** > **التحديثات**.
2. يدوياً، في نافذة البرنامج الرئيسية من خلال النقر فوق **فحص التحديثات** في القسم **التحديث**.
3. يدوياً، من خلال تنزيل إصدار أحدث من السابق وتثبيته.

لمزيد من المعلومات والإرشادات الموضحة، راجع:

- تحديث منتجات ESET - التحقق من وحدات المنتج الأخيرة
- ما الأنواع المختلفة لتحديث منتج ESET والإصدار؟

الترقية التلقائية للمنتج القديم

لم يعد إصدار منتج ESET الخاص بك مدعوماً، وتمت ترقية منتجك إلى أحدث إصدار.

مشكلات التثبيت الشائعة

يتميز كل إصدار جديد من منتجات ESET بالعديد من إصلاحات الأخطاء والتحسينات. يمكن للعملاء الحاليين الذين لديهم اشتراك صالح لمنتج ESET الترقية إلى أحدث إصدار من نفس المنتج مجاناً.

لإنهاء التثبيت:

1. انقر فوق **قبول ومتابعة** للموافقة على اتفاقية ترخيص المستخدم النهائي والأقرار بـ سياسة الخصوصية. إذا كنت لا توافق على اتفاقية ترخيص المستخدم النهائي، فانقر فوق **إزالة التثبيت**. لا يمكنك العودة إلى الإصدار السابق.
2. انقر فوق **السماح والمتابعة** للسماح بكل من نظام ملاحظات ESET LiveGrid® وبرنامج تحسين تجربة العميل أو انقر فوق **متابعة** إذا كنت لا تريد المشاركة.
3. بعد تنشيط منتج ESET الجديد باستخدام مفتاح التنشيط، سيتم عرض صفحة نظرة عامة. إذا لم يتم العثور على معلومات اشتراكك، فتابع باستخدام الاشتراك التجريبي المجاني. إذا كان اشتراكك المستخدم في المنتج السابق غير صالح، فقم بتنشيط منتج ESET لديك.
4. تلزم إعادة تشغيل الجهاز لإكمال التثبيت.

سيتم تثبيت ESET Internet Security

يمكن عرض نافذة الحوار هذه:

- أثناء عملية التثبيت ـ انقر فوق **متابعة** لتثبيت ESET Internet Security.
- عند تغيير الاشتراك في ESET Internet Security—انقر فوق **تنشيط** لتغيير الاشتراك وتنشيط ESET Internet Security.

وفقاً لاشتراك ESET يتيح لك خيار **تغيير المنتج** التبديل بين منتجات ESET Windows المنزلية. راجع ما المنتج الذي أقتنيه؟ لمزيد من المعلومات.

التغيير إلى خط منتج مختلف

وفقاً لاشتراك ESET يمكنك التبديل بين منتجات ESET Windows المنزلية المتنوعة. راجع ما المنتج الذي أقتنيه؟ لمزيد من المعلومات.

التسجيل

يرجى تسجيل اشتراكك باستكمال الحقول التي يتضمنها نموذج التسجيل والنقر فوق **تنشيط**. الحقول المميزة بعلامة مطلوب في الأقواس تعد إلزامية. لن يتم استخدام هذه المعلومات إلا فيما يخص اشتراك ESET الخاص بك.

تقدم التنشيط

انتظر بضع ثوانٍ لإتمام عملية التنشيط (قد يختلف الوقت المطلوب وفقاً لسرعة اتصالك بالإنترنت أو جهاز الكمبيوتر الخاص بك).

نجح التنشيط

اكتملت عملية التنشيط. اتبع معالج ما بعد التثبيت لإنهاء تثبيت ESET Internet Security.

سيبدأ تحديث الوحدة خلال بضع ثوانٍ. ستبدأ التحديثات المنتظمة لـESET Internet Security على الفور.

سيبدأ الفحص الأولي تلقائياً في خلال 20 دقيقة بعد تحديث الوحدة.

> i يمكن مقاطعة عملية التنشيط إذا لم يكن العرض مرتبطاً بـESET HOME. قم بتسجيل الدخول إلى حساب ESET HOME أو إنشاء حساب.

دليل المبتدئ

يوفر هذا الفصل نظرة عامة مبدئية عن ESET Internet Security وإعداداته الأساسية.

أيقونة علبة النظام

تتوفر بعض أهم خيارات وميزات الإعداد بالنقر بزر الماوس الأيمن فوق أيقونة علبة النظام.

إيقاف الحماية مؤقتاً – لعرض مربع حوار التأكيد الذي يعطِّل محرك الكشف، الذي يحمي من هجمات النظام الضارة بالتحكم في اتصال الملف والويب والبريد الإلكتروني. تتيح لك القائمة المنسدلة **الفاصل الزمني** تحديد المدة التي سيتم تعطيل الحماية خلالها.

إإيقاف جدار الحماية مؤقتاً (السماح بجميع حركات المرور) – لتبديل جدار الحماية إلى حالة غير نشطة. راجع الشبكة لمزيد من المعلومات.

حظر جميع حركات مرور الشبكة – حظر جميع حركات مرور الشبكة. يمكنك إعادة تمكينه بالنقر فوق **إيقاف حظر جميع حركات مرور الشبكة**.

الإعداد المتقدم – يتم فتح الإعداد المتقدم في ESET Internet Security. لفتح الإعداد المتقدم من نافذة المنتج الرئيسية، اضغط على F5 على لوحة المفاتيح أو انقر فوق **الإعداد** > **الإعداد المتقدم**.

ملفات السجل – ملفات السجل تحتوي على معلومات بشأن أحداث البرنامج المهمة التي وقعت، وتقديم نظرة عامة حول الاكتشافات.

فتح ESET Internet Security – يتم فتح نافذة البرنامج الرئيسية لـESET Internet Security.

إعادة تعيين تخطيط النافذة – لإعادة تعيين نافذة ESET Internet Security إلى حجمها وموضعها الافتراضيين على الشاشة.

وضع اللون—يتم فتح إعدادات واجهة المستخدم حيث يمكنك تغيير لون واجهة المستخدم الرسومية.

التحقق من وجود تحديثات – يبدأ تحديث الوحدة أو المنتج لضمان حمايتك. يتحقق ESET Internet Security من التحديثات تلقائياً عدة مرات في اليوم.

عن التطبيق – يوفر معلومات النظام وتفاصيل عن الإصدار المثبت من ESET Internet Security ووحدات البرنامج المثبت ومعلومات عن نظام التشغيل وموارد النظام.

اختصارات لوحة المفاتيح

للتنقل الأفضل في ESET Internet Security يمكنك استخدام اختصارات لوحة المفاتيح التالية:

الإجراء	اختصارات لوحة المفاتيح
فتح صفحات التعليمات	F1
لفتح "إعداد متقدم"	F5
التنقل في عناصر القائمة المنسدلة	سهم لأعلى / سهم لأسفل
الانتقال إلى عنصر واجهة المستخدم الرسومية التالي في نافذة	TAB
الانتقال إلى عنصر واجهة المستخدم الرسومية السابق في نافذة	Shift+TAB

الإجراء	اختصارات لوحة المفاتيح
لإغلاق نافذة الحوار النشطة	ESC
يُظهر معلومات حول اشتراك ESET والكمبيوتر الخاص بك (التفاصيل المخصصة للدعم الفني)	Ctrl+U
لإعادة تعيين نافذة المنتج إلى حجمها الافتراضي ووضعها على الشاشة	Ctrl+R
الانتقال إلى الخلف	ALT + سهم إلى اليسار
الانتقال إلى الأمام	ALT + سهم إلى اليمين
الانتقال إلى الصفحة الرئيسية	ALT+Home

يمكنك أيضاً استخدام أزرار الماوس إلى الخلف أو إلى الأمام للانتقال.

ملفات التعريف

تُستخدم إدارة ملفات التعريف في مكانين داخل ESET Internet Security هما: في قسم **الفحص عند الطلب** وفي قسم **التحديث**.

فحص الكمبيوتر

هناك 4 من ملفات تعريف الفحص المحددة مسبقاً في ESET Internet Security:

- **الفحص الذكي** – هذا هو ملف تعريف الفحص المتقدم الافتراضي. يستخدم ملف تعريف الفحص الذكي تقنية التحسين الذكي، والتي تستبعد الملفات التي عُثر عليها نظيفة في فحص سابق ولم يتم تعديلها منذ ذلك الفحص. وهذا يقلل من وقت الفحص وتأثير أقل على أمان النظام.
- **فحص القائمة السياقية** – يمكنك بدء فحص عند الطلب لأي ملف من القائمة السياقية. يسمح لك ملف تعريف فحص القائمة السياقية بتحديد تكوين الفحص الذي سيُستخدم عند تشغيل الفحص بهذه الطريقة.
- **الفحص المفصل** – لا يستخدم ملف تعريف الفحص المفصل التحسين الذكي بشكل افتراضي، لذلك لا يتم استبعاد أي ملفات من الفحص باستخدام ملف التعريف هذا.
- **فحص جهاز الكمبيوتر** – هذا هو ملف التعريف الافتراضي المستخدم في فحص جهاز الكمبيوتر القياسي.

يمكن حفظ معلمات الفحص المفضلة للفحص في المستقبل. يوصى بإنشاء ملف تعريف مختلف (بأهداف فحص وأساليب فحص متنوعة وغيرها من المعلمات) لكل فحص يُستخدم بشكل منتظم.

لإنشاء ملف تعريف جديد، قم بفتح الإعداد المتقدم > **محرك الكشف** > **عمليات فحص البرامج الضارة** > **الفحص عند الطلب** > **قائمة ملفات التعريف** > **تحرير**. تتضمن نافذة **إدارة ملفات التعريف** القائمة المنسدلة **ملف التعريف المحدد** الذي يضم ملفات تعريف الفحص الموجودة وخيار إنشاء ملف تعريف جديد. لمساعدتك في إنشاء ملف تعريف فحص بما يلائم احتياجاتك، راجع ThreatSense للاطلاع على وصف لكل معلمة إعداد فحص.

لنفترض أنك تريد إنشاء ملف تعريف فحص، ويعد تكوين **فحص الكمبيوتر** مناسباً بشكل جزئي، لكنك لا تريد فحص حزم وقت التشغيل أو التطبيقات المحتمل كونها غير آمنة ، كما تريد أيضاً تطبيق **اكتشاف العلاج دائماً**. أدخل اسم ملف التعريف الجديد في نافذة **إدارة ملفات التعريف** وانقر فوق **إضافة**. حدد ملف التعريف الجديد من القائمة المنسدلة **ملف التعريف المحدد** واضبط المعلمات المتبقية بما يلائم متطلباتك، وانقر فوق **موافق** لحفظ ملف التعريف الجديد.

تحديث

يسمح محرر ملفات التعريف في إعداد التحديث لك بإنشاء ملفات تعريف تحديث جديدة. أنشئ ملفات التعريف المخصصة (بخلاف **ملف التعريف الخاص بي**) الخاصة بك واستخدمها فقط إذا كان الكمبيوتر الخاص بك يستخدم عدة طرق للاتصال بخوادم التحديث.

على سبيل المثال، قد يستخدم الكمبيوتر المحمول الذي يتصل عادة بخادم محلي (نسخة مطابقة) في الشبكة المحلية، لكنه يقوم بتنزيل تحديثات مباشرة من خوادم تحديث ESET عند فصله من الشبكة المحلية (في رحلة عمل) ملفي تعريف كالتالي: الأول للاتصال بالخادم المحلي، والآخر للاتصال بخوادم ESET. بمجرد تكوين ملفي التعريف هذين، انتقل إلى **الأدوات** > **المجدول** وحرر معلمات مهمة التحديث. قم بتعيين ملف تعريف كرئيسي والآخر كثانوي.

تحديث ملف التعريف – ملف تعريف التحديث المستخدم حالياً. لتغييره، اختر ملف تعريف من القائمة المنسدلة.

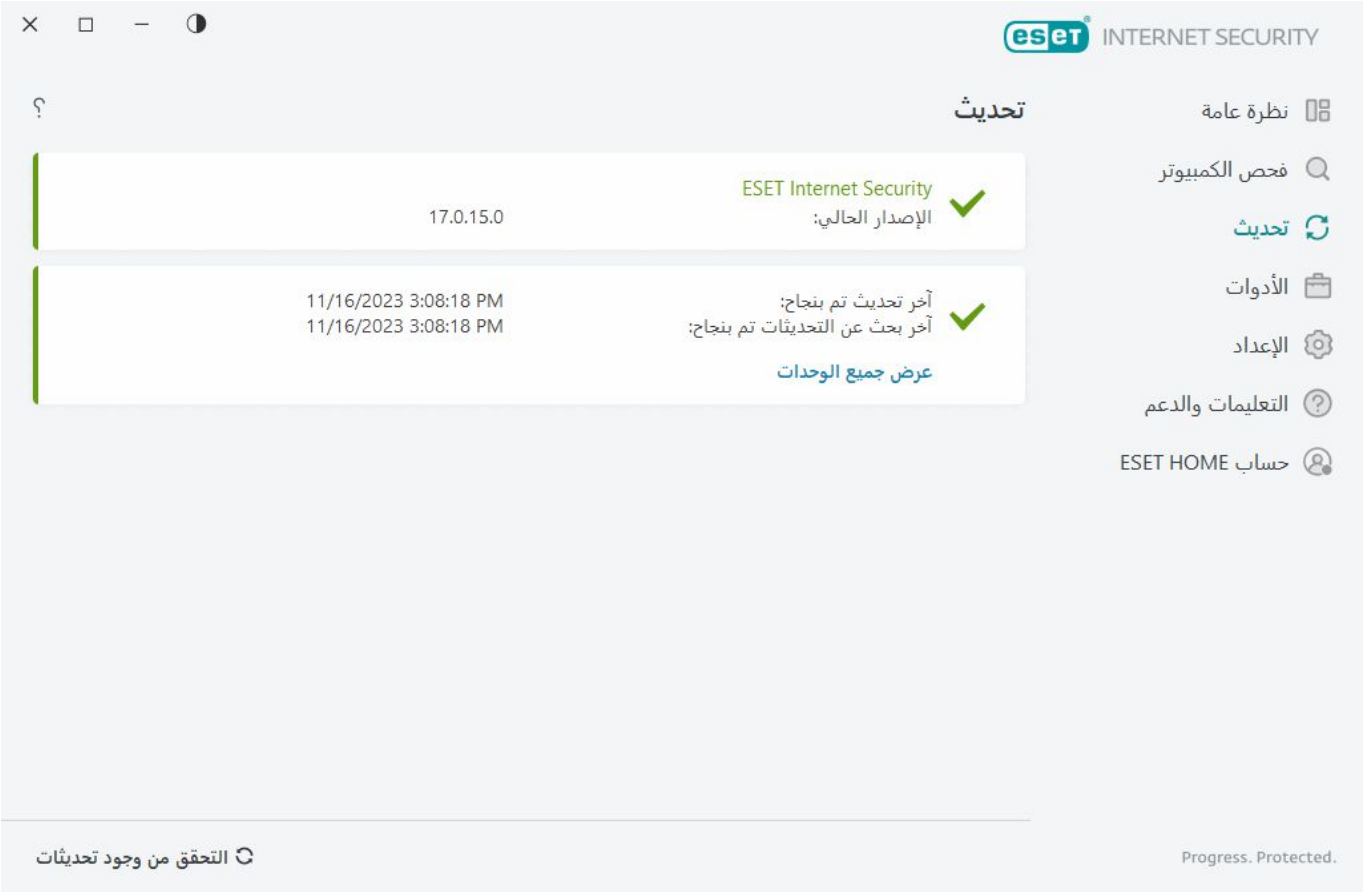
قائمة ملفات التعريف – أنشئ ملفات تعريف تحديث جديدة أو قم بإزالة أخرى موجودة.

تحديثات

يعد تحديث ESET Internet Security دورياً أفضل طريقة لضمان أقصى مستوى من الأمان على الكمبيوتر. تضمن وحدة التحديث أن كل من وحدات البرنامج ومكونات النظام دائماً محدثة.

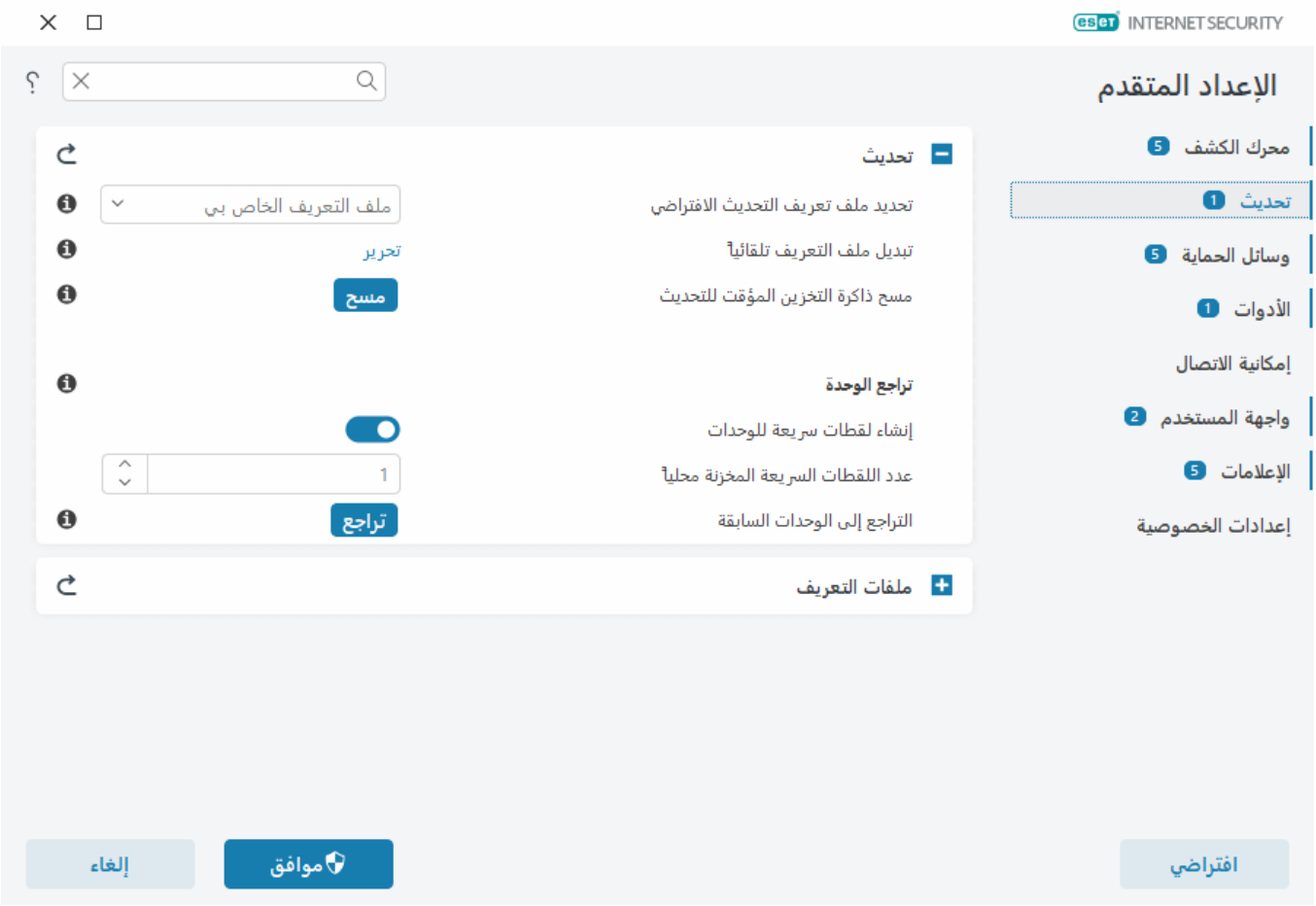
بالنقر فوق **تحديث** في نافذة البرنامج الرئيسية، يمكنك عرض حالة التحديث الحالية، بما فيها تاريخ ووقت آخر تحديث ناجح وما إذا كان التحديث مطلوباً.

بالإضافة إلى التحديثات التلقائية، يمكنك النقر فوق **التحقق من وجود تحديثات** لتشغيل تحديث يدوي.



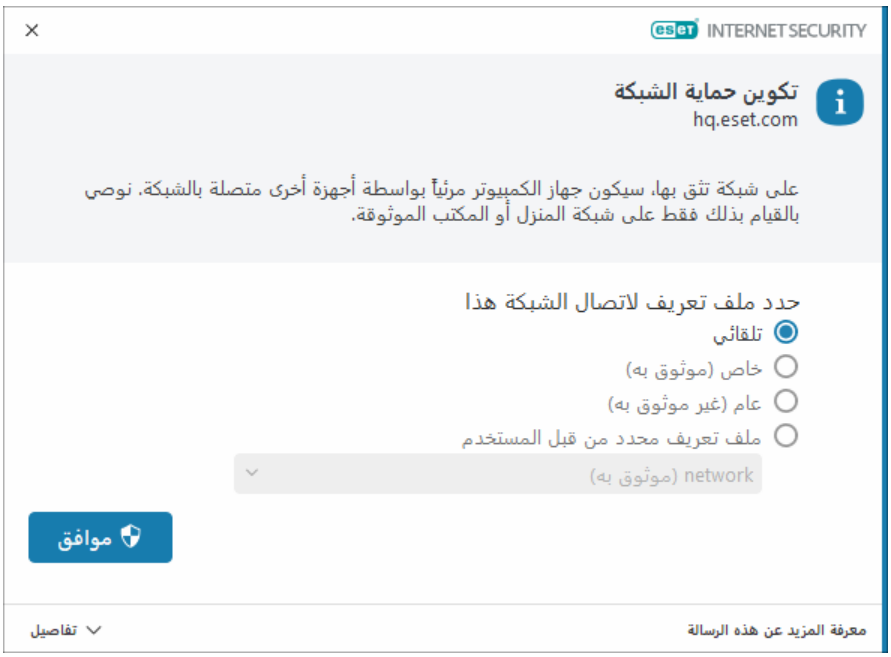
يحتوي **تحديث**الإعداد المتقدم على خيارات تحديث إضافية مثل وضع التحديث والوصول إلى خادم الوكيل واتصالات LAN.

إذا واجهت مشكلات مع أحد التحديثات، فانقر فوق **مسح** لمسح ذاكرة التخزين المؤقت للتحديث. إذا كان لا يزال يتعذّر عليك تحديث وحدات البرامج، فراجع قسم استكشاف الأخطاء وإصلاحها لرسالة "فشل تحديث الوحدات".



تكوين حماية الشبكة

بشكل افتراضي، يستخدم ESET Internet Security إعدادات Windows عند اكتشاف اتصال بالشبكة جديد. لعرض نافذة حوار عند اكتشاف شبكة جديدة، قم بتغيير تعيين ملف تعريف حماية الشبكة إلى **Ask**. يحدث تكوين حماية الشبكة كلما يتصل جهاز الكمبيوتر بشبكة جديدة.



يمكنك الاختيار من بين ملفات تعريف اتصال الشبكةالتالية:

تلقائياً— سيحددESET Internet Security ملف التعريف تلقائياً، استناداً إلى المنشطات التي تم تكوينها لكل ملف تعريف.

خاص—للشبكات الموثوق بها (شبكة منزلية أو شبكة مكتب). يُعد جهاز الكمبيوتر والملفات المشتركة المخزنة عليه مرئياً لمستخدمي الشبكة الآخرين، ويمكن الوصول إلى موارد النظام للمستخدمين الآخرين على الشبكة (تم تمكين الوصول إلى الملفات والطابعات المشتركة وتم تمكين الاتصال الوارد RPCوتُعد مشاركة سطح المكتب البعيد متاحة). نوصي باستخدام هذا الإعداد عند الوصول إلى شبكة محلية آمنة. يتم تعيين ملف التعريف هذا تلقائياً لاتصال الشبكة إذا تم تهيئته كمجال أو شبكة خاصة في Windows.

عام—للشبكات غير الموثوق بها (الشبكة العامة). لا تتم مشاركة الملفات والمجلدات الموجودة على نظامك مع مستخدمين آخرين على الشبكة ولا تكون مرئية لهم ويتم إلغاء تنشيط مشاركة موارد النظام. نوصي باستخدام هذا الإعداد عند الوصول إلى الشبكات اللاسلكية. يتم تعيين ملف التعريف هذا تلقائياً لأي اتصال شبكة لم يتم تهيئته كمجال أو شبكة خاصة في Windows.

ملف تعريف محدد من قبل المستخدم—يمكنك تحديد ملف تعريف قمت بإنشائه من القائمة المنسدلة. لا يُعد هذا الخيار متاحاً إلا إذا قمت بإنشاء ملف تعريف مخصص واحد على الأقل.

قد يُعرّض تكوين الشبكة غير الصحيح جهاز الكمبيوتر الخاص بك لخطر أمني.

تمكين مكافحة السرقة

تكون الأجهزة الشخصية دائماً معرضة لخطر السرقة أو الفقدان أثناء التنقل اليومي من المنزل إلى العمل وإلى الأماكن العامة الأخرى. مكافحة السرقة عبارة عن ميزة تعمل على زيادة الأمان على مستوى المستخدم في حالة فقدان الجهاز أو سرقته. تتيح لك مكافحة السرقة مراقبة استخدام الجهاز وتتبع جهازك المفقود باستخدام نظام التحديد من خلال عنوان IP في ESET HOME، مما يساعدك في استعادة جهازك وحماية بياناتك الشخصية.

من خلال استخدام التقنيات الحديثة مثل البحث الجغرافي بواسطة عنوان IP والتقاط الصور باستخدام كاميرا الويب، وحماية حساب المستخدم، ومراقبة الجهاز، يمكن لميزة مكافحة السرقة مساعدتك ثم تحدد جهة إنفاذ القانون موقع الكمبيوتر أو الجهاز في حالة فقدانه أو سرقته. في ESET HOME، يمكنك معرفة النشاط الذي يتم على جهاز الكمبيوتر أو الجهاز الخاص بك.

لمعرفة المزيد حول مكافحة السرقة في ESET HOME راجع تعليمات ESET HOME عبر الإنترنت.

قد لا يعمل مكافحة السرقة بشكل صحيح على أجهزة الكمبيوتر في المجالات بسبب القيود في إدارة حسابات المستخدمين.

لتمكين مكافحة السرقة جهازك وحماية جهازك في حالة فقدانه أو سرقته، اختر أحد الخيارات التالية:

- في نافذة البرنامج الرئيسية > **نظرة عامة**، انقر فوق **الإعداد** بجوار **مكافحة السرقة**.
- إذا رأيت رسالة "ميزة Anti-Theft متوفرة" في شاشة نافذة البرنامج الرئيسية > **نظرة عامة**، فانقر فوق **تمكين مكافحة السرقة**.
- من نافذة البرنامج الرئيسية، انقر فوق **الإعداد** > **أدوات الأمان**. قم بتمكين التبديل **مكافحة السرقة** واتبع التعليمات التي تظهر على الشاشة.

إذا لم يكن جهازك متصلاً بـ ESET HOME، فيجب عليك:
1. سجّل الدخول إلى حساب ESET HOME عند تمكين مكافحة السرقة.
2. تعيين اسم جهاز.

لا يدعم مكافحة السرقة Microsoft Windows Home Server.

بعد تمكين مكافحة السرقة، يمكنكتحسين أمان جهازك في نافذة البرنامج الرئيسية > **الإعداد** > **أدوات الأمان** > **مكافحة السرقة**.

المراقبة الأبوية

إذا كنت بالفعل قد قمت بتمكين ميزة Parental control في ESET Internet Security يجب أيضاً تكوين Parental control لجميع حسابات المستخدمين ذات الصلة.

عندما تكون الرقابة الأبوية نشطة ولا يتم تهيئة حسابات المستخدمين، يعرض ESET Internet Security إعلام "لم يتم إعداد الرقابة الأبوية" على شاشة **نظرة عامة**. انقر فوق **إعداد القواعد** وراجع قسم Parental control لمزيد من المعلومات.

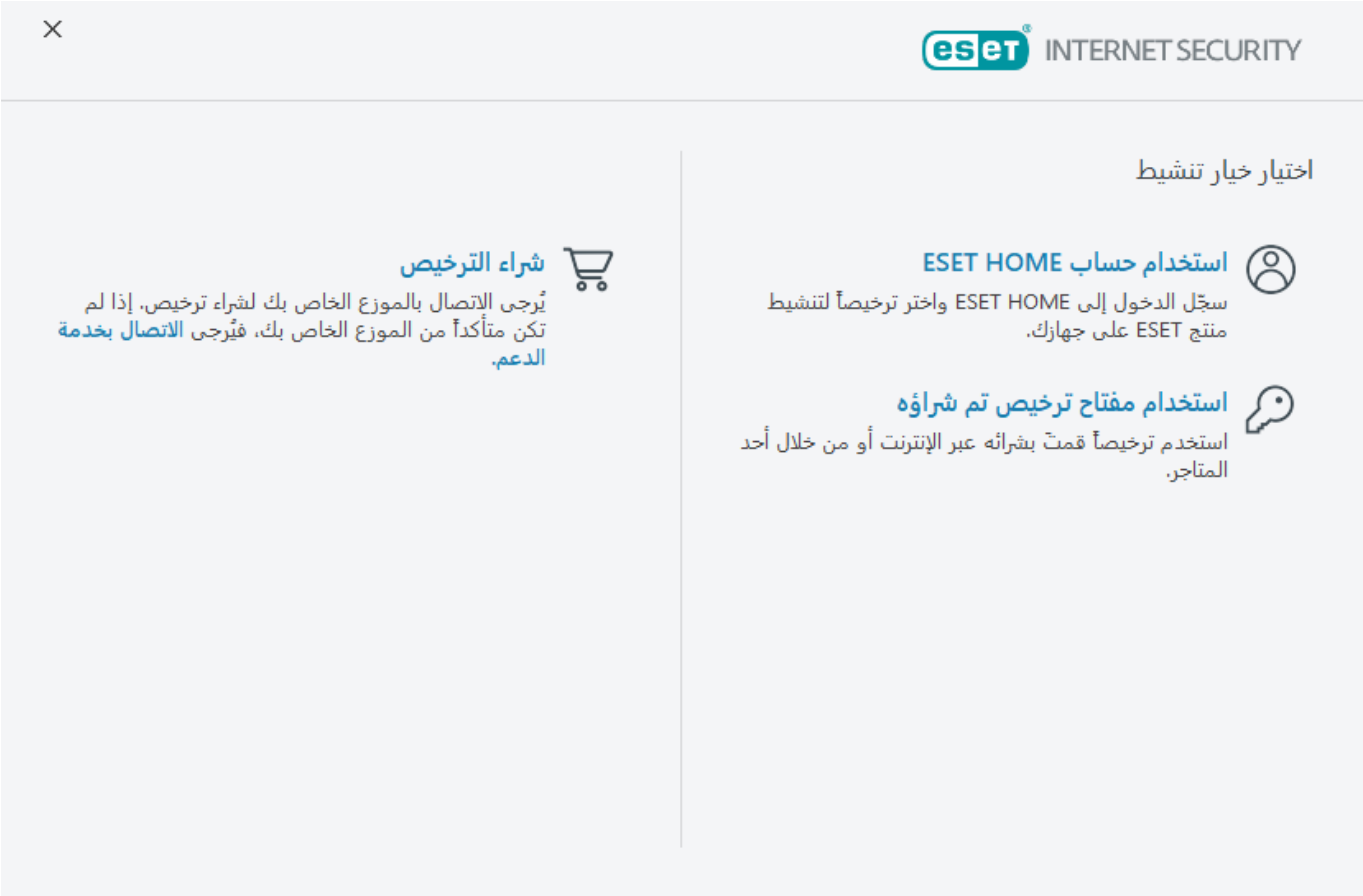
تنشيط المنتج

توجد عدة طرق لتنشيط منتجك. وقد يختلف توفر سيناريو تنشيط معين في نافذة التنشيط حسب البلد، ووسيلة التوزيع (قرص مضغوط/قرص DVD أو صفحة ويب وغير ذلك).

- إذا قمت بشراء إصدار صندوق البيع بالتجزئة للمنتج، أو تلقيت رسالة بريد إلكتروني بتفاصيل الاشتراك فقم بتنشيط منتجك بالنقر فوق **استخدام مفتاح التنشيط الذي تم شراؤه**. يجب إدخال مفتاح التنشيط كما تم توفيره لنجاح التنشيط. مفتاح التنشيط هو سلسلة فريدة بتنسيق XXXX-XXXX-XXXX-XXXX-XXXX أو XXXX-XXXXXXXX يستخدم لتعريف مالك الاشتراك وللتنشيط. يتم تحديد موقع مفتاح التنشيط داخل أو في الجانب الخلفي لحزمة المنتج.
- بعد تحديد استخدام حساب ESET HOME، سيُطلب منك تسجيل الدخول إلى حساب ESET HOME.
- إذا كنت تريد تقييم ESET Internet Security قبل إجراء عملية الشراء، فقم بتحديد النسخة التجريبية المجانية. قم بإدخال عنوان البريد الإلكتروني الخاص بك والبلد لتنشيط ESET Internet Security لمدة محددة. سيتم إرسال الاشتراك التجريبي المجاني إليك عبر البريد الإلكتروني. يمكن تنشيط الاشتراكات التجريبية فقط مرة واحدة لكل عميل.
- إذا لم يكن لديك اشتراك وتريد شراء اشتراك، فانقر فوق **شراء اشتراك**. ستتم إعادة توجيهك إلى موقع ويب موزع ESET المحلي الخاص بك. اشتراكات منتجات ESET Windows المنزلية ليست مجانية.

يُمكنك تغيير اشتراك المنتج في أي وقت. للقيام بذلك، انقر فوق **التعليمات والدعم** > **تغيير الاشتراك** في النافذة الرئيسية للبرنامج. سيظهر لك مُعرّف الاشتراك العام المستخدم لتحديد اشتراكك لدعم ESET.

فشل تنشيط المنتج؟



إدخال مفتاح التنشيط أثناء التنشيط

التحديث التلقائي من الأمور المهمة لأمانك. لن يتلقى ESET Internet Security التحديثات إلا بمجرد تنشيطه.

عند إدخال **مفتاح التنشيط** الخاص بك، من المهم إدخاله بدقة كما هو مكتوب: مفتاح التنشيط هو سلسلة فريدة بالتنسيق XXXX-XXXX-XXXX-XXXX يستخدم لتعريف مالك الاشتراك ولتنشيط الاشتراك.

نوصيك بنسخ مفتاح التنشيط ولصقه من البريد الإلكتروني للتسجيل لضمان الدقة.

وإذا لم يتم إدخال مفتاح التنشيط بعد التثبيت، فلت يتم تنشيط المنتج. يمكنك تنشيط ESET Internet Security في نافذة البرنامج الرئيسية > **المساعدة والدعم** > **تفعيل الاشتراك**.

اشتراكات منتجات ESET Windows المنزلية ليست مجانية.

استخدام حساب ESET HOME

قم بتوصيل جهازك بـ ESET HOME لعرض وإدارة جميع اشتراكات وأجهزة ESET التي تم تنشيطها. يمكنك تجديد الاشتراك أو ترقيته أو تمديده وعرض تفاصيل الاشتراك المهمة. في بوابة إدارة ESET HOME أو تطبيق الهاتف المحمول، يمكنك إضافة الاشتراكات المختلفة وتنزيل المنتجات على أجهزتك والتحقق من حالة أمان المنتج أو مشاركة الاشتراكات عبر البريد الإلكتروني. لمزيد من المعلومات، تفضل بزيارة التعليمات عبر الإنترنت في ESET HOME.

بعد تحديد **استخدام حساب ESET HOME** كطريقة تنشيط أو عند الاتصال بحساب ESET HOME أثناء التثبيت:

1. سجّل الدخول إلى حساب ESET HOME.

> إذا لم يكن لديك حساب ESET HOME فانقر فوق **إنشاء حساب** للتسجيل أو اطلع على الإرشادات في تعليمات ESET HOME عبر الإنترنت.
> إذا نسيت كلمة المرور، فانقر فوق **نسيت كلمة المرور** واتبع الخطوات التي تظهر على الشاشة أو راجع الإرشادات في تعليمات ESET HOME عبر الإنترنت.

2. قم بتعيين **اسم جهاز** لجهازك الذي سيتم استخدامه في جميع خدمات ESET HOME وانقر فوق **متابعة**.
3. اختر اشتراكاً لتنشيطه أو أضف اشتراكاً جديداً. انقر فوق **متابعة** لتنشيط ESET Internet Security.

تنشيط الإصدار التجريبي المجاني

لتنشيط النسخة التجريبية من ESET Internet Security أدخل عنوان بريد إلكتروني صالحاً في حقول **عنوان البريد الإلكتروني** و**تأكيد عنوان البريد الإلكتروني**. بعد التنشيط، سيتم إنشاء اشتراك ESET المطلوب لتحديث وإرساله إلى البريد الإلكتروني الخاص بك. سيتم استخدام البريد الإلكتروني هذا لإعلامات انتهاء صلاحية المنتج والاتصالات الأخرى بشركة ESET. يمكن تنشيط الاشتراك التجريبي المجاني مرة واحدة فقط.

حدد البلد من القائمة المنسدلة **البلد** لتسجيل ESET Internet Security بالموزع المحلي الذي يوفر الدعم الفني.

مفتاح تنشيط ESET المجاني

اشتراك ESET Internet Security ليس مجانياً.

مفتاح تنشيط ESET عبارة عن تسلسل فريد للأحرف والأرقام المفصولة بشرطة، توفره ESET للسماح بالاستخدام القانوني لـESET Internet Security بما يتوافق مع اتفاقية ترخيص المستخدم النهائي. يحق لكل مستخدم نهائي استخدام مفتاح التنشيط فقط إلى الحد الذي يكون له الحق في استخدام ESET Internet Security استناداً إلى عدد التراخيص الممنوحة من قِبل ESET. يعتبر مفتاح التنشيط سرياً ولا يمكن مشاركته؛ ومع ذلك، يمكنك مشاركة الاشتراك باستخدام ESET HOME.

هناك مصادر على الإنترنت قد تقدم لك مفاتيح تنشيط ESET "مجانية"، لكن تذكر ما يلي:

- قد يؤدي النقر فوق إعلان "اشتراك ESET مجاني" إلى تعريض جهاز الكمبيوتر أو الجهاز للخطر وقد يؤدي إلى الإصابة بالبرمجيات الخبيثة. يمكن إخفاء البرمجيات الخبيثة في محتوى الويب غير الرسمي (مثل مقاطع الفيديو) ومواقع ويب تعرض إعلانات لكسب المال بناءً على زياراتك وما إلى ذلك. عادة ما يكون هذا فخاً.
- يمكن لـESET تعطيل الاشتراكات المقرصنة ويقوم بذلك بالفعل.
- إن وجود مفتاح تنشيط مقرصن لا يتماشى مع اتفاقية ترخيص المستخدم النهائي التي يجب عليك قبولها لتثبيت ESET Internet Security.
- لا تشتري اشتراك ESET إلا من خلال القنوات الرسمية مثل www.eset.com، وموزعي ESET أو بائعي التجزئة (ولا تشتري اشتراكاً من مواقع الويب الخارجية غير الرسمية مثل eBay أو اشتراكاً مشتركاً من جهة خارجية).
- يُعد تنزيل منتج صفحة رئيسية ESET Internet Security مجانياً، لكن التنشيط أثناء التثبيت يتطلب مفتاح تنشيط ESET صالحاً (يمكنك تنزيله وتثبيته، لكن بدون التنشيط، لن يعمل).
- لا تقم بمشاركة اشتراكك على الإنترنت أو شبكة التواصل الاجتماعي (فقد يصبح منتشراً).

لتحديد اشتراك ESET مقرصن والإبلاغ عنه، قم بزيارة مقالة قاعدة المعرفة لدينا لمزيد من الإرشادات.

إذا كنت غير متأكد من شراء منتج أمان ESETشؤون فيمكنك استخدام إصدار تجريبي بينما تقرر:

1. قم بتنشيط ESET Internet Security باستخدام اشتراك تجريبي مجاني
2. المشاركة في برنامج ESET Beta
3. تثبيت ESET Mobile Security إذا كنت تستخدم جهاز محمول يعمل بنظام Android فهو freemium.

للحصول على خصم / تمديد للترخيص، تجديد ESET.

فشل التنشيط ـ السيناريوهات الشائعة

إذا لم يكن تنشيط ESET Internet Security ناجحاً، فإن السيناريوهات الأكثر شيوعاً هي:

- مفتاح التنشيط مستخدم بالفعل.
- لقد أدخلت مفتاح تنشيط غير صالح.

- المعلومات في نموذج التنشيط مفقودة أو غير صالحة.
- فشل الاتصال بخادم التنشيط.
- لا يوجد اتصال أو الاتصال معطل بخوادم تنشيط ESET.

تحقق من إدخال مفتاح التنشيط الصحيح وأن اتصال الإنترنت الخاص بك نشط. حاول تنشيط ESET Internet Security مرة أخرى. إذا كنت تستخدم حساب ESET HOME للتنشيط، فراجع اشتراك ESET HOME وإدارة الاشتراك ـ المساعدة عبر الإنترنت.

إذا تلقيت خطأ محدداً (على سبيل المثال، اشتراك معلق أو اشتراك مفرط الاستخدام)، فاتبع الإرشادات في حالة الاشتراك.

إذا كنت لا تزال غير قادر على تنشيط ESET Internet Security فستقوم أداة استكشاف أخطاء تنشيط ESET وإصلاحها بتوجيهك إلى الأسئلة والأخطاء والمشكلات الشائعة المتعلقة بالتنشيط والترخيص (متوفرة باللغة الإنجليزية وعدة لغات أخرى).

حالة الاشتراك

يمكن أن يكون لاشتراكك حالات مختلفة. يمكنك العثور على حالة اشتراكك في ESET HOME. لإضافة الاشتراك الخاص بك إلى حساب ESET HOME راجع إضافة اشتراك.

إذا لم يكن لديك حساب ESET HOME يمكنك إنشاء حساب ESET HOME جديد.

إذا كانت حالة الاشتراك غير **نشط**، فستتلقى خطأ أثناء التنشيط أو إعلاماً في نافذة البرنامج الرئيسية.

لتعطيل إعلامات حالة الاشتراك افتح الإعداد المتقدم > **الإعلامات** > **حالات التطبيق**. انقر فوق **تحرير** بجوار **حالات التطبيق**، وقم بتوسيع **الترخيص** وإلغاء تحديد مربع الاختيار بجوار الإعلام الذي تريد تعطيله. لا يؤدي تعطيل الإعلام إلى حل المشكلة.

راجع الأوصاف والحلول الموصى بها لحالات الاشتراك المختلفة في الجدول أدناه:

حالة الاشتراك	الوصف	الحل
نشط	الاشتراك صالح، وليس هناك حاجة لتفاعلك. يمكن تنشيط ESET Internet Security ويمكنك العثور على تفاصيل الاشتراك في نافذة البرنامج الرئيسية > **التعليمات والدعم**.	
تم تجاوز حد الاستخدام	الأجهزة التي تستخدم هذا الاشتراك أكثر مما هو مسموح به. سوف تتلقى خطأ في التنشيط.	راجع فشل التنشيط بسبب تجاوز حد استخدام الاشتراك لمزيد من المعلومات.
معلّق	تم تعليق الاشتراك الخاص بك بسبب مشكلات في الدفع. لاستخدام الاشتراك، تأكد من تحديث تفاصيل الدفع الخاصة بك في ESET HOME أو اتصل بموزع الاشتراك. يمكنك تلقي هذا الخطأ أثناء التنشيط أو في نافذة البرنامج الرئيسية.	المنتج المثبت ـ إذا كان لديك حساب ESET HOME في الإعلام المعروض في نافذة البرنامج الرئيسية، انقر فوق **إدارة اشتراكك في ESET HOME** و راجع تفاصيل الدفع الخاصة بك. بخلاف ذلك، اتصل بموزع الاشتراك الخاص بك. خطأ في التنشيط ـ إذا كان لديك حساب ESET HOME في نافذة خطأ في التنشيط، انقر فوق **فتح ESET HOME** وراجع تفاصيل الدفع الخاصة بك. بخلاف ذلك، اتصل بموزع الاشتراك الخاص بك.

الحل	الوصف	حالة الاشتراك
المنتج المثبت – في الإعلام المعروض في نافذة البرنامج الرئيسية، انقر فوق **تجديد الاشتراك** واتبع التعليمات الموجودة في كيف أجدد اشتراكي؟، أو انقر فوق **تنشيط المنتج** واختر طريقة التنشيطالخاصة بك. خطأ في التنشيط – في نافذة خطأ في التنشيط، انقر فوق **تجديد الاشتراك** واتبع التعليمات الموجودة في كيف أجدد اشتراكي؟، أو أدخل مفتاح تنشيط جديد أو مجدد وانقر فوق **تجديد الاشتراك**.	لقد انتهت صلاحية اشتراكك، ولا يمكنك استخدام هذا الاشتراك لتنشيط ESET Internet Security. يمكنك تلقي هذا الخطأ أثناء التنشيط أو في نافذة البرنامج الرئيسية. إذا كنت قد قمت بالفعل بتثبيت ESET Internet Security فإن جهاز الكمبيوتر الخاص بك غير محمي ولا يتم تحديثه.	انتهت الصلاحية
إذا تلقيت خطأ: تم إلغاء الاشتراك في نافذة البرنامج الرئيسية أو أثناء التنشيط ويجب أن يعمل اشتراكك بشكل صحيح، اتصل بموزّع الاشتراك الخاص بك.	تم إلغاء اشتراكك من قبل ESET أو من قبل موزّع الاشتراك الخاص بك.	تم الإلغاء

فشل التنشيط نظراً لتجاوز حد استخدام الاشتراك

المشكلة

- قد يكون تم تجاوز حد استخدام اشتراكك أو إساءة استخدامه
- فشل التنشيط نظراً لتجاوز حد استخدام الاشتراك

الحل

هناك أجهزة تستخدم هذا الاشتراك أكثر مما يسمح به. قد تكون ضحية قرصنة البرامج أو تزييفها. لا يمكن استخدام الاشتراك لتنشيط أي منتج ESET آخر. يمكنك حل هذه المشكلة مباشرة إذا تم السماح لك بإدارة الاشتراك في حساب ESET HOME أو اشتريت الاشتراك من مصدر قانوني. إذا لم يكن لديك حساب بعد، فقم بإنشاء حساب.

إذا كنت مالك اشتراك ولم تتم مطالبتك بإدخال عنوان بريدك الإلكتروني:

1. لإدارة اشتراك ESET افتح متصفح ويب وانتقل إلى https://home.eset.com. قم بالوصول إلى ESET License Manager وإزالة نقاط الترخيص أو إلغاء تنشيطها. لمزيد من المعلومات، راجع ما يجب القيام به في حالة تجاوز حد استخدام الاشتراك.
2. لتحديد والإبلاغ عن اشتراك ESET مقرصن، تفضل بزيارة مقالة تحديد اشتراك ESET مقرصن والإبلاغ عنه للتعليمات.
3. إذا كنت غير متأكد، فانقر فوق **"السابق"** وراسل الدعم الفني لـESET عبر البريد الإلكتروني.

إذا لم تكن مالك الاشتراك، فيرجى الاتصال بمالك هذا الاشتراك وإبلاغه بمعلومات حول عدم تمكنك من تنشيط منتج ESET بسبب تجاوز حد استخدام الاشتراك. يمكن للمالك حل المشكلة من خلال بوابة ESET HOME.

إذا طُلب منك تأكيد عنوان بريدك الإلكتروني (عدة حالات فقط)، فأدخل عنوان البريد الإلكتروني المستخدَم في الأصل لشراء حساب ESET Internet Security الخاص بك أو تنشيطه.

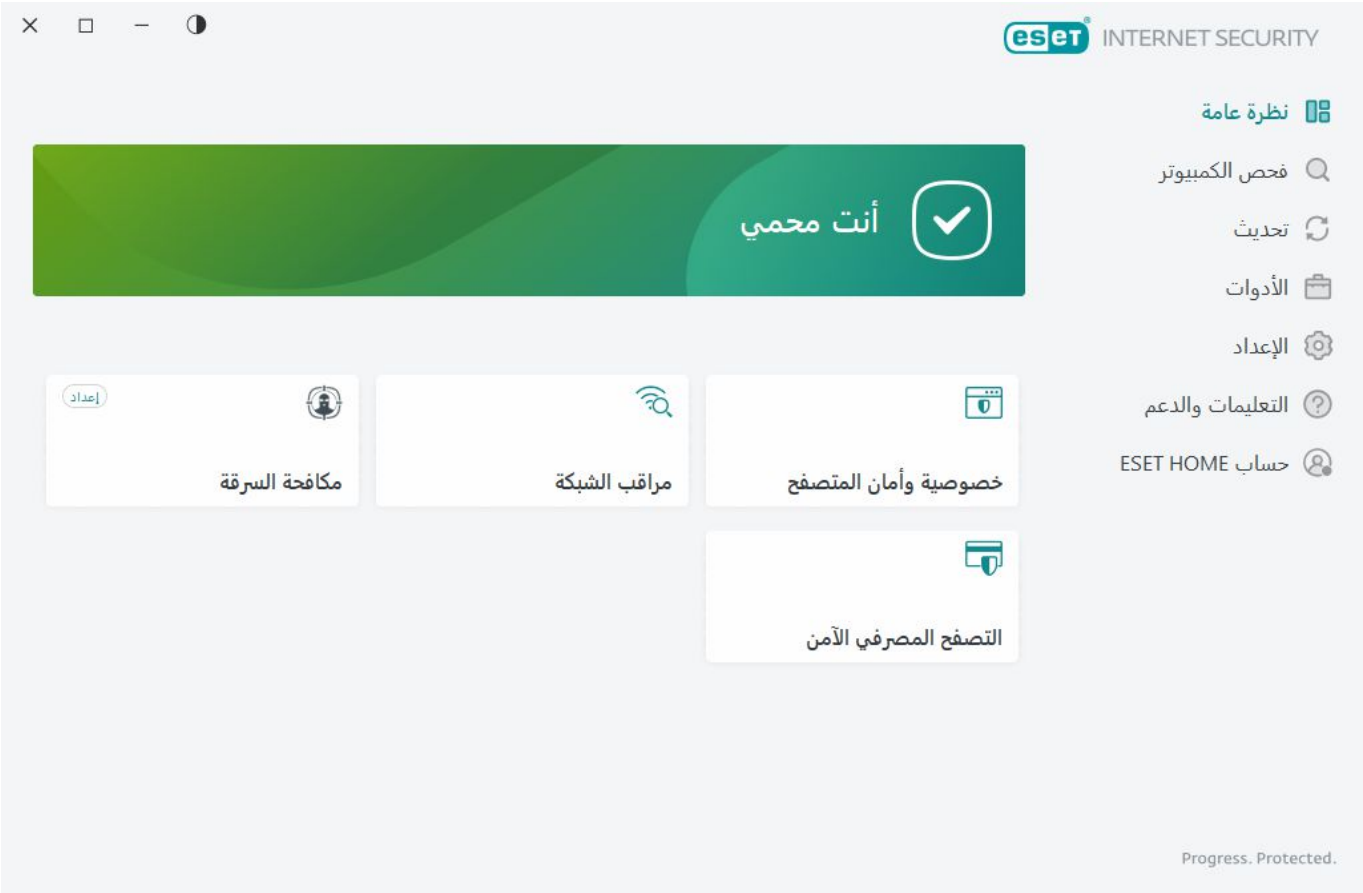
التعامل مع ESET Internet Security

تنقسم نافذة البرنامج الرئيسية ESET Internet Security إلى قسمين. تعرض النافذة الرئيسية على اليمين معلومات تناظر الخيار المحدد من القائمة الرئيسية على اليسار.

> **إرشادات موضحة**
> راجع فتح نافذة البرنامج الرئيسية لمنتجات ESET Windows للحصول على الإرشادات المشروحة باللغة الإنجليزية وغيرها من العديد من اللغات.

يمكنك تحديد نظام ألوان واجهة المستخدم الرسومية ESET Internet Security في الزاوية اليمنى العليا من نافذة البرنامج الرئيسية. انقر فوق أيقونة **نظام الألوان** (يتغير الرمز بناءً على نظام الألوان المحدد حالياً) بجوار أيقونة **تصغير** وحدد نظام الألوان من القائمة المنسدلة:

- **نفس الشيء مثل لون النظام**—يضبط نظام الألوان ESET Internet Security بناءً على إعدادات نظام التشغيل.
- **داكن**—ESET Internet Security سيكون له نظام ألوان داكن (الوضع الداكن).
- **فاتح**—ESET Internet Security سيكون له نظام ألوان فاتح قياسي.



خيارات القائمة الرئيسية:

نظرة عامة – توفر معلومات عن حالة حماية ESET Internet Security.

فحص الكمبيوتر – لتكوين فحص الكمبيوتر أو إنشاء فحص مخصص.

تحديث ـ يعرض معلومات حول الوحدة وتحديثات محرك الكشف.

توفر الأدوات—الوصول إلى مراقب الشبكة وميزات أخرى تساعد في تبسيط إدارة البرنامج وتقديم خيارات إضافية للمستخدمين المتقدمين.

يوفر الإعداد—خيارات التكوين لميزات الحماية ESET Internet Security (حمايةوحماية الكمبيوتر وحماية الإنترنت وحماية الشبكة وأدوات الأمان) والوصول إلى الإعداد المتقدم.

التعليمات والدعم ـ تعرض معلومات حول الاشتراك الخاص بك، ومنتج ESET المثبّت، وروابط إلى التعليمات عبر الإنترنت وقاعدة معرفة ESET والدعم الفني.

حساب ESET HOME - توصيل جهازك بـ ESET HOME أو مراجعة حالة اتصال حساب ESET HOME. استخدم ESET HOME لعرض وإدارة الإعدادات مكافحة السرقة لديك واشتراكات وأجهزة ESET المفعلة.

نظرة عامة

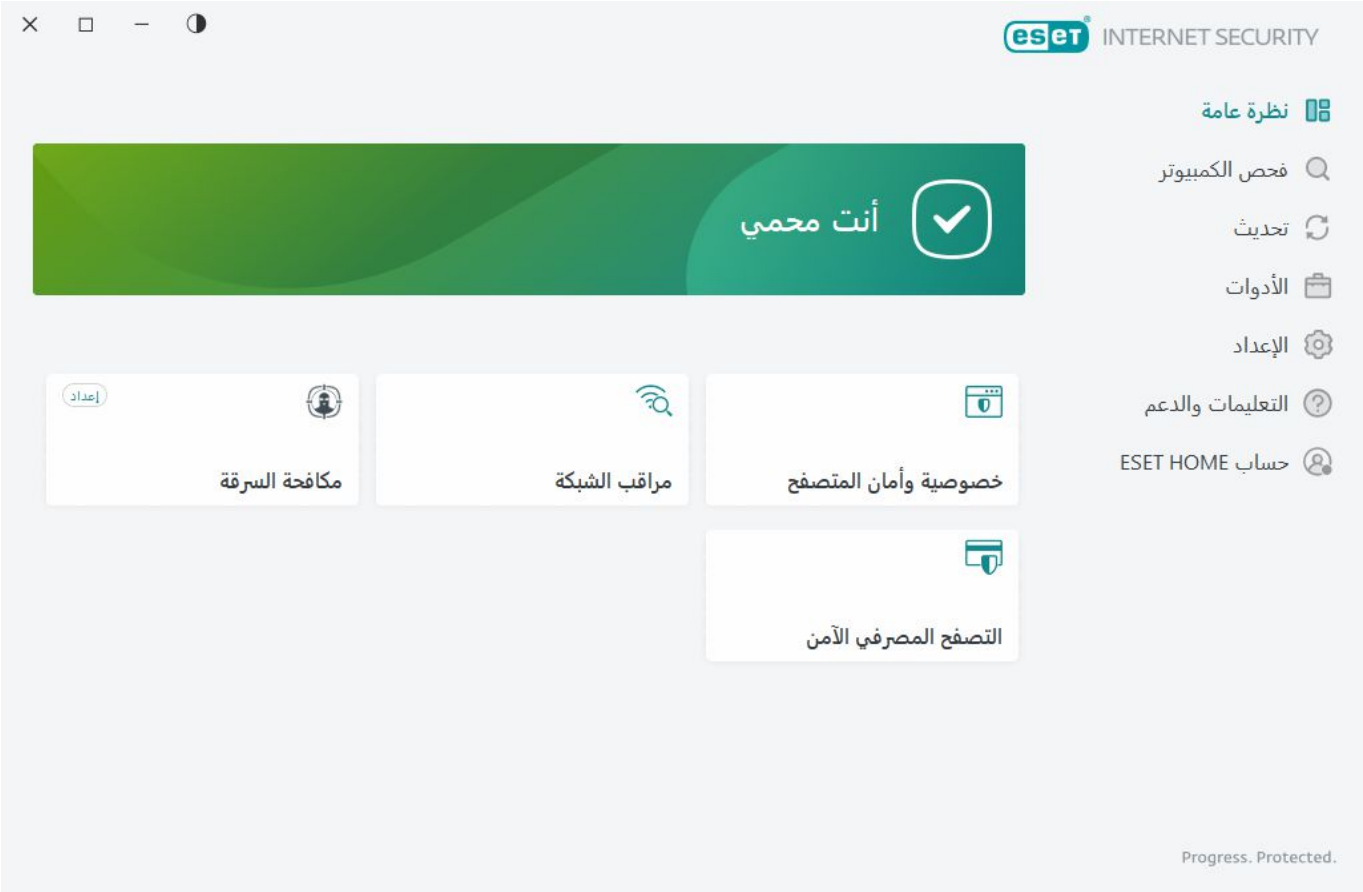
تعرض نافذة **نظرة عامة** معلومات حول الحماية الحالية لجهاز الكمبيوتر الخاص بك مع روابط سريعة لميزات الأمان الموجودة في ESET Internet Security.

تعرض نافذة **نظرة عامة** إعلامات تحتوي على معلومات تفصيلية وحلول موصى بها لتحسين الأمان في ESET Internet Security أو تشغيل الميزات الإضافية أو ضمان أقصى قدر من الحماية. إذا كان هناك المزيد من الإعلامات، فانقر فوق **X المزيد من الإعلامات** لتوسيع الكل.

مراقب الشبكة ـ التحقق من أمان الشبكة

التصفح المصرفي الآمنـيقوم بتشغيل المتصفح، الذي تم تعيينه كإعداد افتراضي في Windows في وضع آمن.

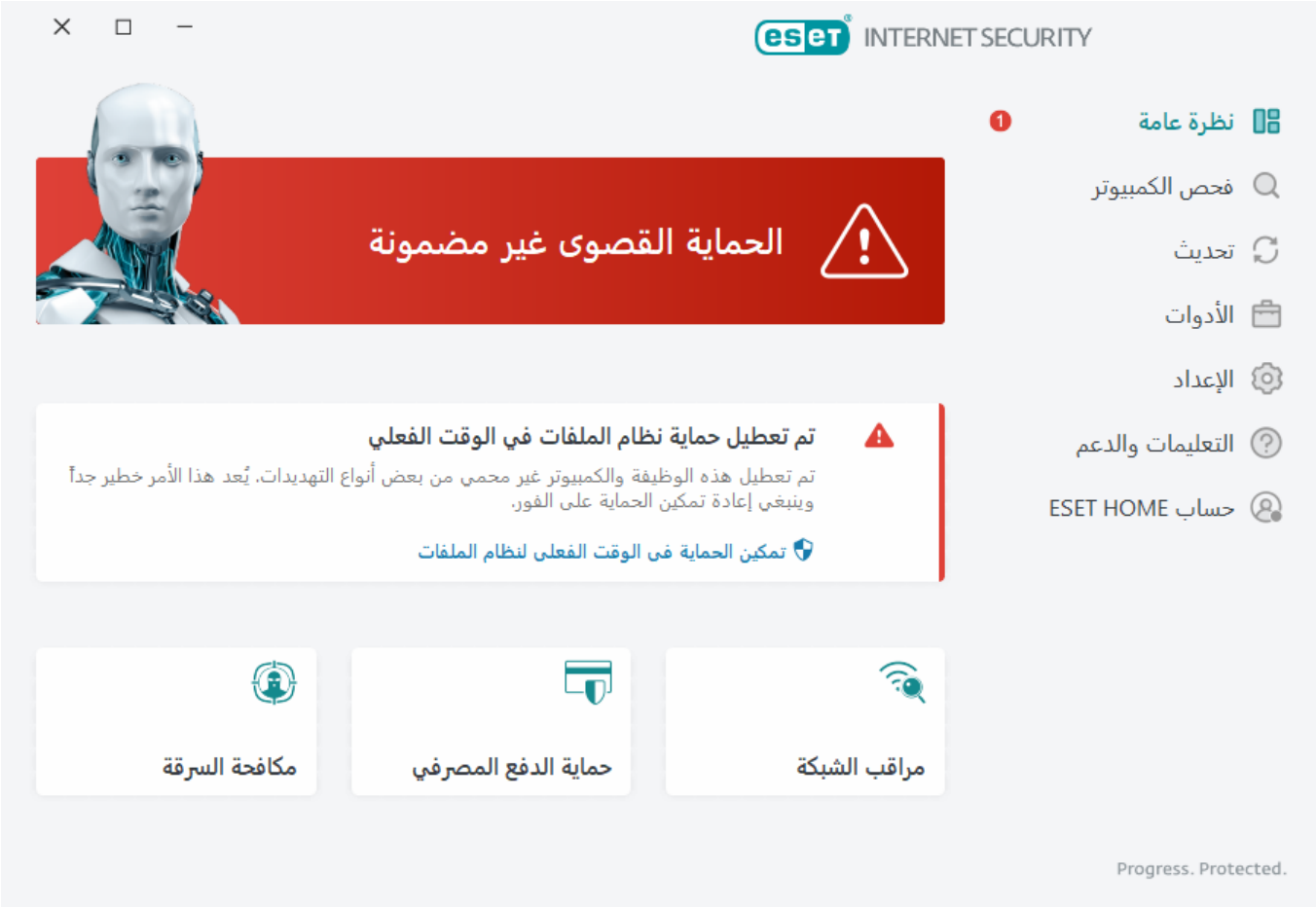
مكافحة السرقة—يبدأ إعداد مكافحة السرقة. إذا كنت قد قمت بإعداد مكافحة السرقة بالفعل، فسيفتح الرابط السريع صفحة مكافحة السرقة.



تشير حالة الأيقونة الخضراء وحالة **أنت محمي** الخضراء إلى ضمان أقصى حماية.

ما ينبغي فعله إذا لم يعمل البرنامج بشكل سليم

إذا كانت وحدة الحماية تعمل بشكلٍ سليم، فستضيء أيقونة حالة الحماية باللون الأخضر. بينما تشير علامة التعجب الحمراء أو أيقونة الإعلام البرتقالية إلى عدم تمتّعك بأقصى درجة من الحماية. سيتم عرض معلومات إضافية حول حالة الحماية الخاصة بكل وحدة، بالإضافة إلى الحلول المقترحة لاستعادة الحماية التامة على أنها إعلام في نافذة **نظرة عامة**. لتغيير حالة الوحدات الفردية، انقر فوق **إعداد** وحدد الوحدة المطلوبة.



تشير الأيقونة الحمراء وحالة **التنبيه الأمني** الحمراء إلى وجود مشكلات حرجة.
توجد أسباب عدة لظهور هذه الحالة، على سبيل المثال:

- **لم يتم تنشيط المنتج** أو **انتهت صلاحية الاشتراك**– يُشار إلى ذلك بتحول أيقونة حالة الحماية إلى اللون الأحمر. لا يستطيع البرنامج التحديث بعد انتهاء صلاحية الاشتراك. يوصى باتباع الإرشادات الواردة في نافذة التنبيه لتجديد اشتراكك.
- **محرك الكشف غير محدث** ـ سيظهر هذا الخطأ بعد عدة محاولات غير ناجحة لتحديث محرك الكشف. يوصى بالتحقق من إعدادات التحديث. وأكثر الأسباب شيوعاً لهذا الخطأ هو إدخال بيانات المصادقة بشكل غير صحيح، أو تكوين إعدادات الاتصال بشكل غير صحيح.
- **تم تعطيل حماية نظام الملفات الحالي** ـ قام المستخدم بتعطيل الحماية الحالية. جهاز الكمبيوتر غير محمي ضد التهديدات. انقر فوق **حماية نظام الملفات في الوقت الفعلي** لإعادة تمكين هذه الوظيفة.
- **الحماية ضد الفيروسات ومكافحة برامج التجسس معطلة** – يمكنك إعادة تمكين الحماية ضد الفيروسات وبرامج التجسس بالنقر فوق **تمكين الحماية ضد الفيروسات وبرامج التجسس**.
- **جدار الحماية من ESET معطل** – يُشار إلى هذه المشكلة بإعلام أمان بجوار العنصر **الشبكة** على سطح المكتب لديك. يمكنك إعادة تمكين حماية الشبكة بالنقر فوق **تمكين جدار الحماية**.

تشير الأيقونة البرتقالية إلى تمتّعك بمستوى محدود من الحماية. على سبيل المثال، قد يكون هناك مشكلة في تحديث البرنامج أو قد يكون اشتراكك موشكاً على الانتهاء.
توجد أسباب عدة لظهور هذه الحالة، على سبيل المثال:

- **تحذير تحسين مكافحة السرقة** – لم يتم تحسين هذا الجهاز لـ مكافحة السرقة. على سبيل المثال، قد لا يتم إنشاء حساب

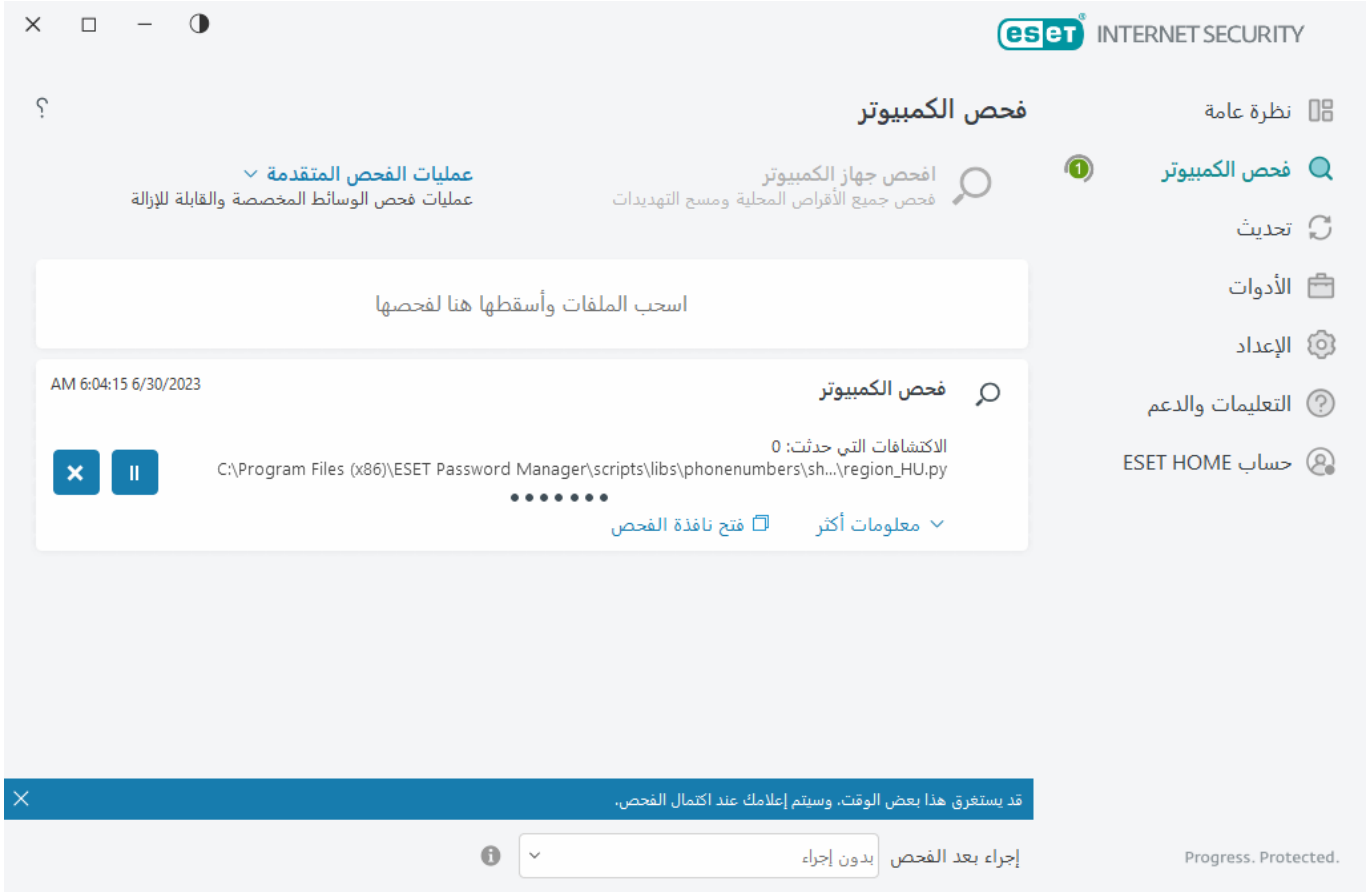
وهمي (ميزة أمان يتم تشغيلها تلقائياً عند تعليم الجهاز بعلامة مفقو.) على الكمبيوتر لديك. يمكنك إنشاء الحساب الوهمي باستخدام ميزة التحسين في واجهة ويب . يمكنك إنشاء الحساب الوهمي باستخدام ميزة التحسين في واجهة ويب مكافحة السرقة.

- **وضع الألعاب نشط** – يؤدي تمكين وضع الألعاب إلى تعريض جهازك لخطر أمان محتمل. إن تفعيل هذه الميزة يعمل على تعطيل جميع نوافذ إعلام/تنبيه وإيقاف أي مهام مجدولة.
- **ستنتهي صلاحية اشتراكك قريباً/ستنتهي صلاحية اشتراكك اليوم** — يُشار إلى ذلك بعرض أيقونة حالة الحماية لعلامة تعجب بجوار ساعة النظام. بعد انتهاء صلاحية اشتراكك، لن يتمكن البرنامج من التحديث وستتحول أيقونة حالة الحماية إلى اللون الأحمر.

إذا لم تستطع حل مشكلة باستخدام الحلول المقترحة، فانقر فوق **التعليمات والدعم** للوصول إلى ملفات التعليمات أو ابحث في ESET Knowledgebase. إذا كنت ما زلت محتاجاً إلى المساعدة، فيمكنك إرسال طلب دعم. سترد خدمة عملاء ESET بسرعة على أسئلتك وتساعدك في العثور على حل.

فحص الكمبيوتر

يعد برنامج الفحص عند الطلب جزءاً مهماً من حل الحماية ضد الفيروسات. وهو يُستخدم لتنفيذ عمليات فحص للملفات والمجلدات الموجودة على الكمبيوتر. من وجهة النظر المتعلقة بالأمان، من الضروري إجراء عمليات فحص الكمبيوتر بانتظام كجزء من مقاييس الأمان الروتينية وعدم الاكتفاء بإجراء فحص للكمبيوتر عند الاشتباه بوجود إصابة. يوصى بإجراء عمليات فحص شاملة بانتظام لنظامك لاكتشاف الفيروسات التي لا تكتشفها حماية نظام الملفات في الوقت الفعلي عند الكتابة إلى القرص. يمكن أن يحدث ذلك في حالة تعطيل حماية نظام الملفات في الوقت الفعلي في ذلك الوقت، أو إذا كان محرك الكشف قديماً، أو إذا لم يُكتشف الملف كفيروس عند حفظه على القرص.



يتوفر نوعان من **فحص جهاز الكمبيوتر**. **فحص جهاز الكمبيوتر** لفحص النظام بسرعة دون تحديد معلمات الفحص. **الفحص المخصص** (ضمن عمليات الفحص المتقدمة) يتيح لك تحديد ملفات تعريف الفحص المحددة مسبقاً المصممة إلى مواقع معينة مستهدفة، واختيار أهداف الفحص المحددة.

راجع تقدم الفحص لمزيد من المعلومات حول عملية الفحص.

> بشكل افتراضي، يحاول ESET Internet Security تنظيف أو حذف الاكتشافات التي تم العثور عليها أثناء فحص جهاز الكمبيوتر تلقائياً. في بعض الحالات، إذا لم يتم تنفيذ أي إجراء، فستتلقى تنبيهاً تفاعلياً ويجب تحديد إجراء تنظيف (على سبيل المثال، حذف أو تجاهل). لتغيير مستوى التنظيف ولمزيد من المعلومات التفصيلية، راجع التنظيف. لمراجعة عمليات المسح السابقة، راجع ملفات السجل.

افحص جهاز الكمبيوتر

يتيح لك **فحص جهاز الكمبيوتر** تشغيل فحص الكمبيوتر وتنظيف الملفات المصابة بسرعة دون الحاجة إلى تدخل من المستخدم. ويتميز **فحص جهاز الكمبيوتر** بسهولة تشغيله وعدم الحاجة إلى تكوين تفصيلي للفحص. يتحقق هذا الفحص من جميع الملفات الموجودة على محركات الأقراص المحلية وينظف حالات التسلل المكتشفة أو يزيلها تلقائياً. يتم تعيين مستوى المسح تلقائياً إلى القيمة الافتراضية. لمزيد من المعلومات التفصيلية حول أنواع المسح، راجع التنظيف.

يُمكنك أيضاً استخدام ميزة الفحص **بالسحب والإفلات** لفحص ملف أو مجلد يدوياً عن طريق النقر فوق الملف أو المجلد، ونقل مؤشر الماوس إلى المنطقة المميزة مع الاستمرار في الضغط على زر الماوس، ثم تحريره. بعد ذلك، يتم نقل التطبيق إلى المقدمة.

تتوفر خيارات الفحص التالية ضمن **عمليات الفحص المتقدمة**:

فحص مخصص

فحص مخصص يتيح لك تحديد معلمات الفحص مثل أهداف الفحص وأساليب الفحص. ميزة **الفحص المخصص** بحيث يمكنك تكوين المعلمات بالتفصيل. يمكن حفظ التكوينات إلى ملفات تعريف محددة بواسطة المستخدم، وهو ما يمكن أن يفيد في حالة إجراء الفحص بشكل متكرر باستخدام المعلمات نفسها.

فحص وسائط التخزين

يشبه فحص الكمبيوتر – يمكنك بسرعة تشغيل فحص لوسائط قابلة للإزالة (مثل CD/DVD/USB) متصل بالكمبيوتر حالياً. ويمكن أن يفيد ذلك عند توصيل محرك فلاش USB بجهاز كمبيوتر وتريد فحص محتوياته للتأكد من خلوها من البرامج الضارة وغيرها من التهديدات المحتملة.

يمكن بدء هذا النوع من الفحص أيضاً بالنقر فوق **الفحص المخصص**، وتحديد **الوسائط القابلة للإزالة** من القائمة المسندلة **أهداف الفحص**، ثم النقر فوق **فحص**.

تكرار الفحص الأخير

تتيح لك بدء تشغيل الفحص المُنفذ مسبقاً بسرعة باستخدام الإعدادات ذاتها كما كانت من قبل.

تتيح لك القائمة المنسدلة **الإجراء بعد الفحص** تعيين إجراء ليتم تنفيذه تلقائياً بعد انتهاء الفحص:

- **بدون إجراء** – بعد انتهاء الفحص، لا يتم اتخاذ أي إجراء.
- **إيقاف تشغيل** – يتم إيقاف تشغيل الكمبيوتر بعد انتهاء الفحص.
- **إعادة التشغيل إذا لزم الأمر**–يقوم جهاز الكمبيوتر بإعادة التشغيل إذا لزم الأمر فقط لإكمال تنظيف التهديدات المكتشفة.
- **أعد تشغيل** – إغلاق كل التطبيقات المفتوحة وإعادة تشغيل الكمبيوتر بعد انتهاء الفحص.
- **فرض إعادة التشغيل إذا لزم الأمر**–يقوم جهاز الكمبيوتر بفرض إعادة التشغيل إذا لزم الأمر فقط لإكمال تنظيف التهديدات المكتشفة.
- **فرض إعادة التشغيل** – فرض إغلاق جميع البرامج المفتوحة دون انتظار تفاعل المستخدم وإعادة تشغيل جهاز الكمبيوتر بعد انتهاء الفحص.
- **سكون** – حفظ جلسة العمل ووضع الكمبيوتر في حالة توفير الطاقة بحيث يمكنك استئناف العمل بسرعة.
- **إسبات** – أخذ كل ما هو قيد التشغيل في ذاكرة RAM ونقله إلى ملف خاص على القرص الثابت. يتم إيقاف تشغيل الكمبيوتر ولكنه سيستأنف العمل عند تشغيله في المرة القادمة من الحالة السابقة التي تم حفظها.

> i
> تتوفر إجراءات **السكون** أو **الإسبات** استناداً إلى إعدادات نظام تشغيل الطاقة والسكون في جهاز الكمبيوتر أو إمكانيات جهاز الكمبيوتر/الكمبيوتر المحمول تذكّر أن جهاز الكمبيوتر الذي بحالة السكون لا يزال قيد التشغيل. يُرجى العلم بأن الكمبيوتر الذي بحالة السكون لا يزال قيد التشغيل. فهو لا يزال يقوم بتشغيل الوظائف الأساسية ويستهلك الطاقة عندما يكون جهاز الكمبيوتر قيد التشغيل بطاقة البطارية. للحفاظ على عمر البطارية، على سبيل المثال عند مغادرة المكتب، يوصى باستخدام خيار "الإسبات".

سيبدأ الإجراء المحدد بعد انتهاء جميع عليات الفحص الجارية. عند تحديد **إيقاف التشغيل** أو **إعادة التشغيل**، ستظهر نافذة شاشة تأكيد البرنامج بعد عد تنازلي لمدة 30 ثانية (انقر فوق **إلغاء** لإلغاء تنشيط الإجراء المطلوب).

يوصى بتشغيل فحص كمبيوتر مرة شهرياً على الأقل. يمكن تكوين الفحص بإعداد مهمة مجدولة من **الأدوات** > **المجدول**.
كيف يمكنني جدولة فحص أسبوعي للكمبيوتر؟

مشغل الفحص المخصص

يُمكنك استخدام "فحص مخصص" لفحص ذاكرة التشغيل والشبكة وأجزاء معينة من قرص بدلاً من القرص بالكامل. للقيام بذلك، انقر فوق **عمليات الفحص المتقدمة** > **الفحص المخصص** وحدد أهدافاً معينة من بنية (شجرة) المجلد.

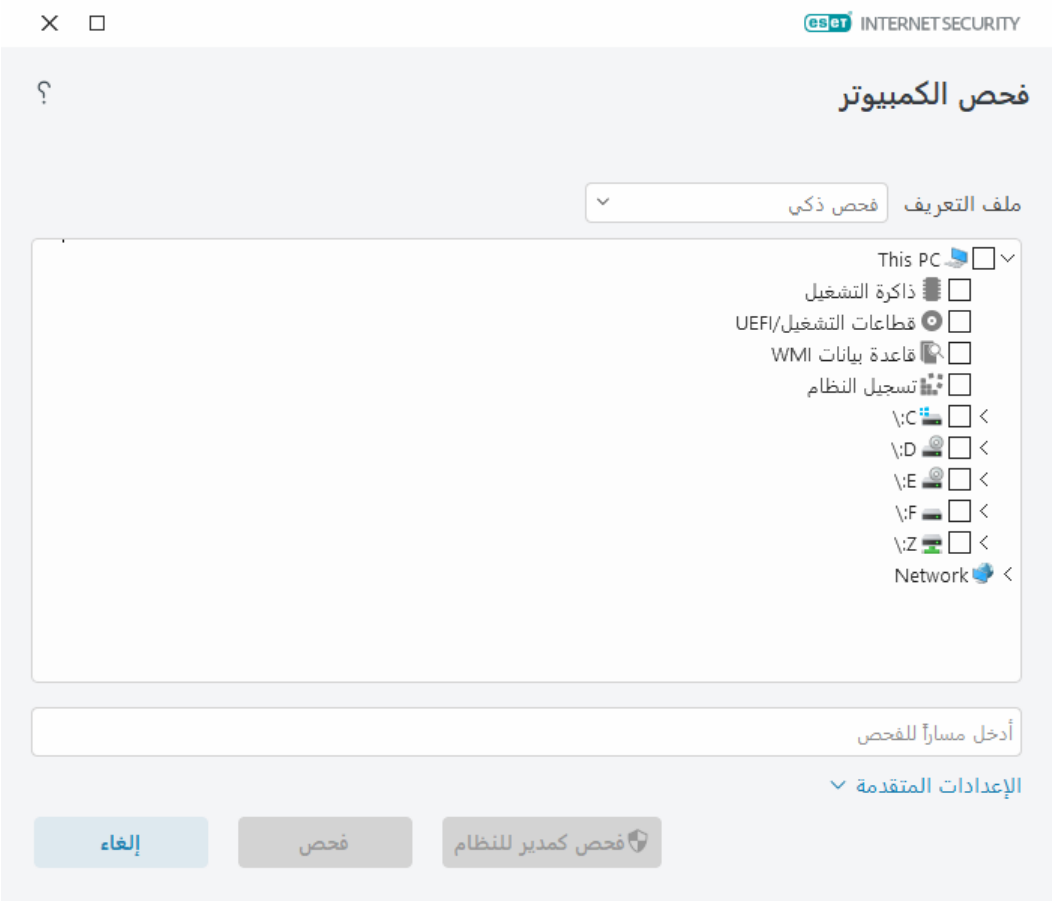
يمكنك اختيار ملف تعريف من القائمة المنسدلة **الملف الشخصي** ليتم استخدامه لفحص أهداف محددة. ملف التعريف الافتراضي هو **الفحص الذكي**. يوجد ثلاثة أوضاع فحص أخرى محددة مسبقاً تسمى: **الفحص المفصل** و**فحص القائمة السياقية** و**فحص جهاز الكمبيوتر**. وتستخدم ملفات تعريف الفحص هذه معلمات ThreatSense مختلفة. يتم ذكر الخيارات المتوفرة في الإعداد المتقدم > **محرك الكشف** > **عمليات فحص البرامج الضارة** > **فحص عند الطلب** > ThreatSense.

تحتوي بنية المجلد (الشجرة) أيضاً على أهداف فحص محددة.

- **ذاكرة التشغيل** – تقوم بفحص جميع العمليات والبيانات المستخدمة حالياً بواسطة ذاكرة التشغيل.
- **قطاعات التشغيل/UEFI** – تفحص قطاعات التشغيل وUEFI بحثاً عن وجود البرامج الضارة. اقرأ المزيد عن فاحص UEFI في المسرد.
- **قاعدة بيانات WMI** – تفحص قاعدة بيانات أدوات إدارة Windows (WMI) بالكامل وجميع مساحات الأسماء وجميع مثيلات الفئة وجميع الخصائص. يبحث عن المراجع إلى الملفات المصابة أو البرمجيات الخبيثة كبيانات.
- **سجل النظام** – يقوم بمسح سجل النظام بأكمله، وجميع المفاتيح، والمفاتيح الفرعية. يبحث عن المراجع إلى الملفات المصابة أو البرمجيات الخبيثة كبيانات. عند تنظيف الاكتشافات، يبقى المرجع في السجل للتأكد من عدم فقدان أي بيانات مهمة.

للانتقال بسرعة إلى هدف فحص (ملف أو مجلد)، اكتب مساره في حقل النص أسفل بنية الشجرة. المسار حساس لحالة الأحرف. لتضمين الهدف في الفحص، حدد خانة الاختيار الخاصة به في بنية الشجرة.

كيفية جدولة فحص أسبوعي للكمبيوتر
لجدولة مهمة منتظمة، راجع كيفية جدولة فحص أسبوعي لجهاز الكمبيوتر.



يمكنك تكوين تنظيف المعلمات للفحص في الإعداد المتقدم > **محرك الكشف** > **عمليات فحص البرامج الضارة** > **الفحص عند الطلب** > **ThreatSense** > **التنظيف**. لتشغيل فحص بدون إجراء التنظيف، انقر فوق **الإعدادات المتقدمة** وحدد **الفحص بدون التنظيف**. يتم حفظ سجل الفحص في سجل الفحص.

عند تحديد **تجاهل الاستبعادات**، سيتم فحص الملفات ذات امتدادات تم استبعادها مسبقاً بدون أي استثناء.

انقر فوق **فحص** لتنفيذ الفحص باستخدام المعلمات المخصصة التي قمت بتعيينها.

فحص كمسؤول يسمح لك بتنفيذ الفحص تحت حساب المسؤول. استخدم هذا إذا لم يكن لدى المستخدم الحالي امتيازات للوصول إلى الملفات التي تريد فحصها. هذا الزر لا يتوفر إذا لم يكن بإمكان المستخدم الحالي استدعاء عمليات UAC كمسؤول.

يُمكنك عرض سجل فحص الكمبيوتر عند اكتمال الفحص عن طريق النقر فوق إظهار السجل.

تقدم الفحص

تعرض نافذة تقدم الفحص الحالة الحالية للفحص ومعلومات حول عدد الملفات التي وُجد أنها تحتوي على تعليمة برمجية ضارة.

من المعتاد ألا يمكن فحص بعض الملفات، كالملفات المحمية بكلمة مرور أو التي يتم استخدامها بواسطة النظام فقط (وهي عادةً ملفات *pagefile.sys* وبعض ملفات السجل). يمكنك العثور على مزيد من التفاصيل في مقالة قاعدة المعرفةلدينا.

كيفية جدولة فحص أسبوعي للكمبيوتر
لجدولة مهمة منتظمة، راجعكيفية جدولة فحص أسبوعي لجهاز الكمبيوتر.

تقدم الفحص—يعرض شريط التقدم حالة الفحص الجاري.

الهدف ـ اسم الكائن الجاري فحصه حالياً وموقعه.

الاكتشافات التي حدثت – لعرض إجمالي عدد الملفات التي تم فحصها والتهديدات المكتشفة والتهديدات التي تم تنظيفها أثناء عملية الفحص.

انقر فوق المزيد من المعلومات لإظهار المعلومات التالية:

- **المستخدم**—اسم حساب المستخدم الذي بدأ الفحص.
- **الكائنات التي تم فحصها**—عدد الكائنات التي تم فحصها بالفعل.
- **المدة**—الوقت المنقضي.

أيقونة الإيقاف المؤقت—توقف الفحص مؤقتاً.

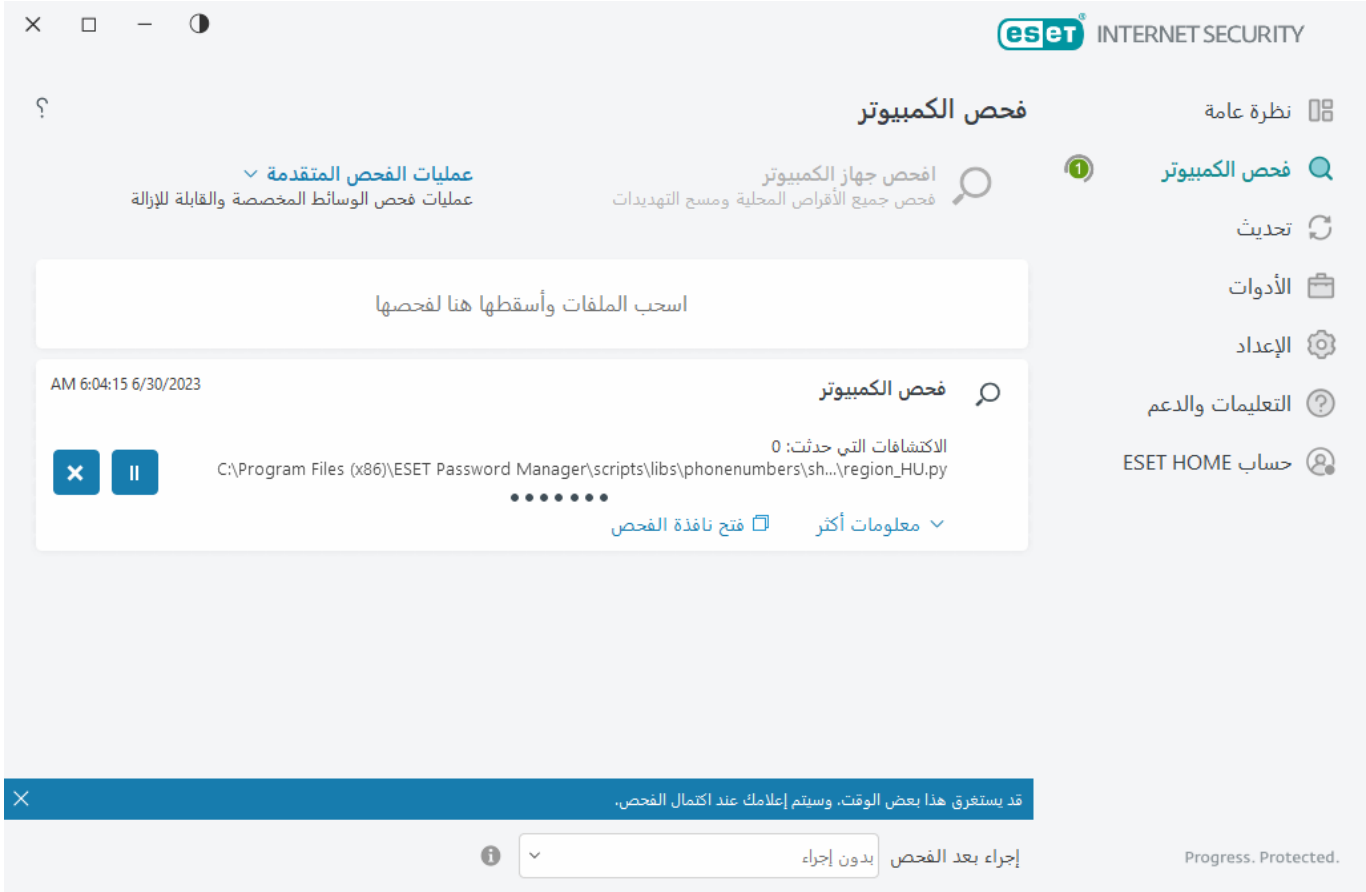
أيقونة الاستئناف — يكون هذا الخيار مرئياً عند إيقاف تشغيل تقدم الفحص مؤقتاً. انقر فوق الأيقونة لمتابعة الفحص.

أيقونة الإيقاف — تنهي الفحص.

انقر فوق **فتح نافذة الفحص** لفتح سجل فحص الكمبيوتر بمزيد من التفاصيل حول الفحص.

تمرير سجل الفحص ـ في حالة تمكينه، سيتم تمرير سجل الفحص لأسفل تلقائياً، كلما تمت إضافة إدخالات جديدة؛ حتى تصبح الإدخالات الأحدث مرئية.

> انقر فوق المكبر أو السهم لعرض تفاصيل الفحص الجاري تشغيله حالياً. يمكنك تشغيل فحص متوازي آخر من خلال النقر فوق **فحص جهاز الكمبيوتر** أو **عمليات الفحص المتقدمة** > **الفحص المخصص**.



تتيح لك القائمة المنسدلة **الإجراء بعد الفحص** تعيين إجراء ليتم تنفيذه تلقائياً بعد انتهاء الفحص:

- **بدون إجراء** – بعد انتهاء الفحص، لا يتم اتخاذ أي إجراء.
- **إيقاف تشغيل** – يتم إيقاف تشغيل الكمبيوتر بعد انتهاء الفحص.
- **إعادة التشغيل إذا لزم الأمر**–يقوم جهاز الكمبيوتر بإعادة التشغيل إذا لزم الأمر فقط لإكمال تنظيف التهديدات المكتشفة.
- **أعد تشغيل** – إغلاق كل التطبيقات المفتوحة وإعادة تشغيل الكمبيوتر بعد انتهاء الفحص.
- **فرض إعادة التشغيل إذا لزم الأمر**–يقوم جهاز الكمبيوتر بفرض إعادة التشغيل إذا لزم الأمر فقط لإكمال تنظيف التهديدات المكتشفة.
- **فرض إعادة التشغيل** – فرض إغلاق جميع البرامج المفتوحة دون انتظار تفاعل المستخدم وإعادة تشغيل جهاز الكمبيوتر بعد انتهاء الفحص.
- **سكون** – حفظ جلسة العمل ووضع الكمبيوتر في حالة توفير الطاقة بحيث يمكنك استئناف العمل بسرعة.
- **إسبات** – أخذ كل ما هو قيد التشغيل في ذاكرة RAM ونقله إلى ملف خاص على القرص الثابت. يتم إيقاف تشغيل الكمبيوتر ولكنه سيستأنف العمل عند تشغيله في المرة القادمة من الحالة السابقة التي تم حفظها.

> تتوفر إجراءات **السكون** أو **الإسبات** استناداً إلى إعدادات نظام تشغيل الطاقة والسكون في جهاز الكمبيوتر أو إمكانيات جهاز الكمبيوتر/الكمبيوتر المحمول تذكّر أن جهاز الكمبيوتر الذي بحالة السكون لا يزال قيد التشغيل. يُرجى العلم بأن الكمبيوتر الذي بحالة السكون لا يزال قيد التشغيل. فهو لا يزال يقوم بتشغيل الوظائف الأساسية ويستهلك الطاقة عندما يكون جهاز الكمبيوتر قيد التشغيل بطاقة البطارية. للحفاظ على عمر البطارية، على سبيل المثال عند مغادرة المكتب، يوصى باستخدام خيار "الإسبات".

سيبدأ الإجراء المحدد بعد انتهاء جميع عليات الفحص الجارية. عند تحديد **إيقاف التشغيل** أو **إعادة التشغيل**، ستظهر نافذة شاشة تأكيد البرنامج بعد عد تنازلي لمدة 30 ثانية (انقر فوق **إلغاء** لإلغاء تنشيط الإجراء المطلوب).

سجل فحص جهاز الكمبيوتر

يمكنك عرض المعلومات التفصيلية المتعلقة بفحص معين في ملفات السجل. يحتوي سجل الفحص على المعلومات التالية:

- إصدار محرك الكشف
- تاريخ البدء والوقت
- قائمة بالأقراص والمجلدات والملفات الممسوحة ضوئياً
- اسم الفحص المجدول (الفحص المجدول فقط)
- المستخدم الذي بدأ الفحص.
- حالة الفحص
- عدد الكائنات التي تم فحصها
- عدد الاكتشافات التي تم العثور عليها
- وقت الإكمال
- إجمالي وقت الفحص

i يتم تخطي بداية جديدة لمهمة فحص جهاز كمبيوتر مجدولة إذا كانت نفس المهمة المجدولة التي تم تنفيذها مسبقاً لا تزال قيد التشغيل. ستعمل مهمة الفحص المجدولة التي تم تخطيها على إنشاء سجل فحص لجهاز الكمبيوتر يحتوي على 0 من الكائنات التي تم فحصها وحالة **لم يبدأ الفحص لأن الفحص السابق كان لا يزال قيد التشغيل**..

للعثور على سجلات الفحص السابقة، في نافذة البرنامج الرئيسية، حدد **الأدوات** > **ملفات السجل**. في القائمة المنسدلة، حدد **فحص جهاز الكمبيوتر** وانقر نقراً مزدوجاً فوق السجل المطلوب.

لمعرفة المزيد حول سجلات "يتعذر الفتح" و/أو "حدث خطأ أثناء الفتح" و/أو "الأرشيف تالف"، راجع مقالة قاعدة معارف ESET.

انقر فوق أيقونة شريط التمرير **التصفية** لفتح نافذة تصفية السجل حيث يمكنك تحديد تضييق نطاق البحث حسب المعايير المخصصة. لعرض قائمة السياق، انقر بزر الماوس الأيمن فوق إدخال سجل محدد:

الاستخدام	الإجراء
يقوم بتنشيط تصفية السجل. سيعرض السجل فقط السجلات من نفس النوع مثل السجل المحدد.	تصفية السجلات نفسها
يفتح هذا الخيار نافذة تصفية السجل ويسمح لك بتحديد معايير لإدخالات السجل المحددة. الاختصار: Ctrl+Shift+F	تصفية
ينشّط إعدادات التصفية. إذا قمت بتنشيط عامل التصفية لأول مرة، يجب عليك تحديد الإعدادات، وفتح نافذة تصفية السجل.	تمكين عامل التصفية
لإيقاف تشغيل عامل التصفية (مثل النقر فوق المفتاح الموجود في الأسفل).	&تعطيل عامل التصفية
نسخ أبرز السجل (السجلات) في الحافظة. الاختصار: Ctrl+C	نسخ
نسخ جميع السجلات في النافذة.	نسخ الكل
تصدير السجل (السجلات) المميزة في الحافظة إلى ملف XML.	تصدير
يقوم هذا الخيار بتصدير جميع السجلات في النافذة إلى ملف XML.	تصدير الكل
لفتح موسوعة تهديدات ESET والتي تحتوي على معلومات تفصيلية عن مخاطر وأعراض التسلل المميز.	وصف الكشف

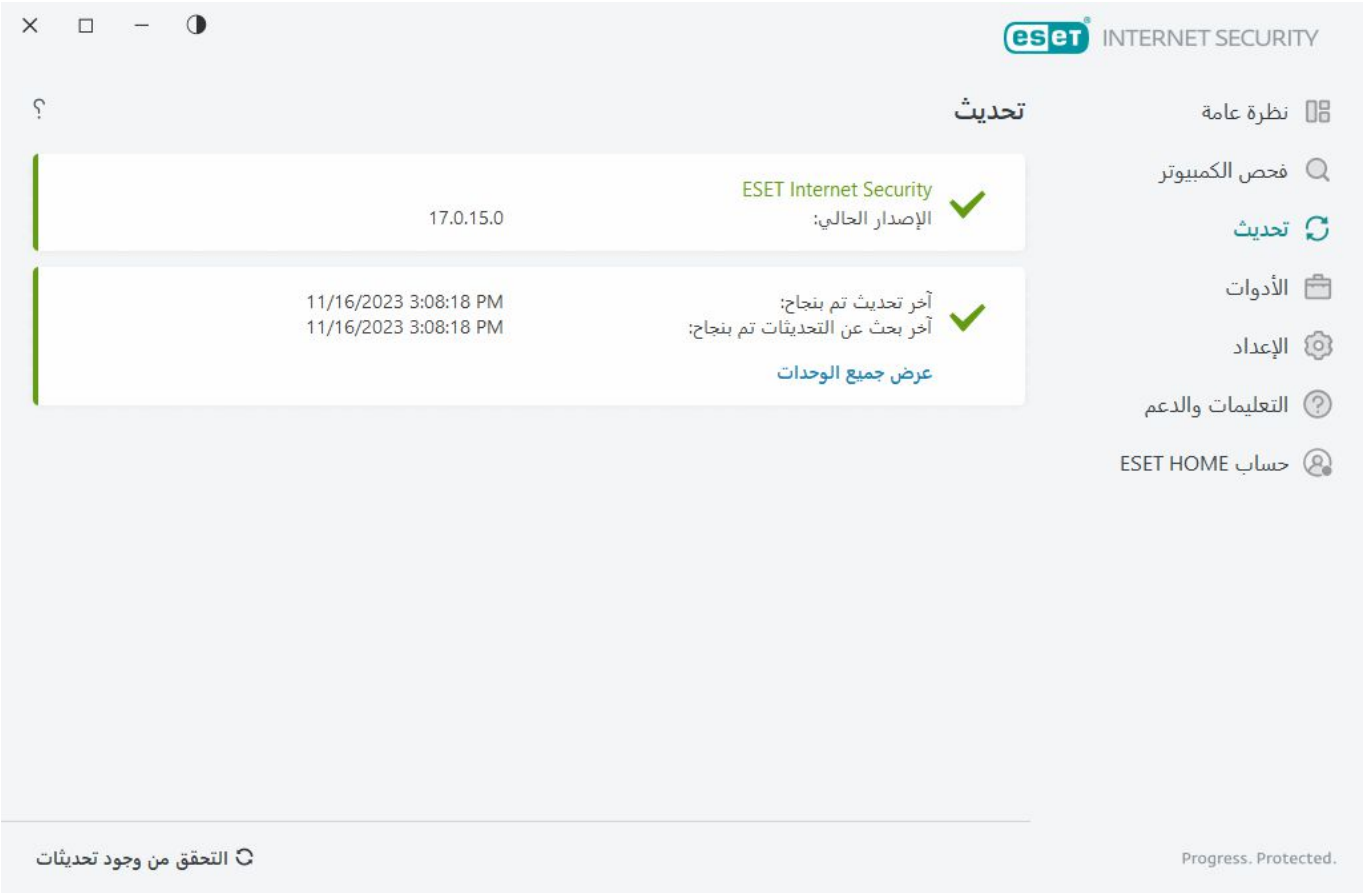
تحديث

يعد تحديث ESET Internet Security دورياً أفضل طريقة لضمان أقصى مستوى من الأمان على الكمبيوتر. تضمن وحدة التحديث أن كل من وحدات البرنامج ومكونات النظام دائماً محدثة.

بالنقر فوق **تحديث** في نافذة البرنامج الرئيسية، يمكنك عرض حالة التحديث الحالية، بما فيها تاريخ ووقت آخر تحديث ناجح وما إذا كان التحديث مطلوباً.

بالإضافة إلى التحديثات التلقائية، يمكنك النقر فوق **التحقق من وجود تحديثات** لتشغيل تحديث يدوي. تحديث وحدات البرنامج

والمكونات بانتظام من أهم الجوانب المتعلقة بالحفاظ على الحماية الكاملة ضد التعليمات البرمجية الضارة. الرجاء توخي الحذر لتكوين الوحدات النمطية للمنتج وتشغيلها. يجب تنشيط المنتج باستخدام مفتاح التنشيط حتى يتسنى لك تلقي التحديثات. وإذا لم تفعل ذلك خلال فترة التثبيت، فأنت بحاجة إلى تنشيط ESET Internet Security للوصول إلى خوادم تحديث ESET. تم إرسال مفتاح التنشيط إليك في رسالة بريد إلكتروني من ESET بعد شراء ESET Internet Security.



الإصدار الحالي – يعرض رقم إصدار المنتج الحالي الذي قمت بتثبيته.

آخر تحديث ناجح ـ يُظهر تاريخ آخر تحديث ناجح أجريته. إذا لم تكن ترى تاريخاً حديثاً، فلن تكون وحدات المنتج محدّثة.

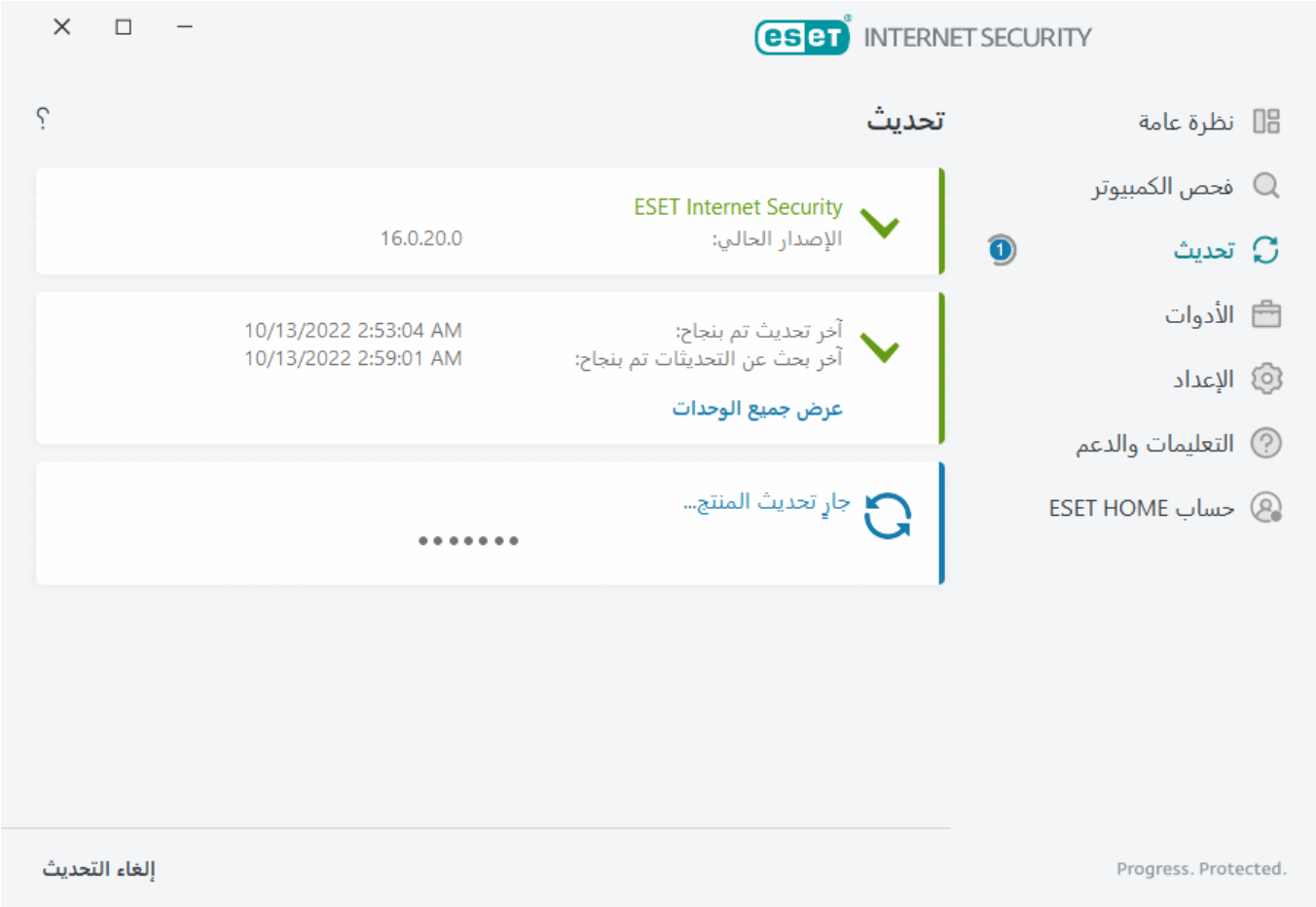
آخر بحث ناجح عن التحديثات ـ يعرض تاريخ آخر بحث ناجح عن التحديثات.

عرض جميع الوحدات – يظهر قائمة وحدات البرنامج المُثبَّت.

انقر فوق **التحقق من وجود تحديثات** للتحقق من أحدث إصدار متوفر من ESET Internet Security.

عملية التحديث

بعد النقر فوق **بحث عن التحديثات**، سيبدأ التنزيل. سيتم عرض شريط تقدم التنزيل والوقت المتبقي على التنزيل. لمقاطعة التحديث، انقر فوق **إلغاء التحديث**.



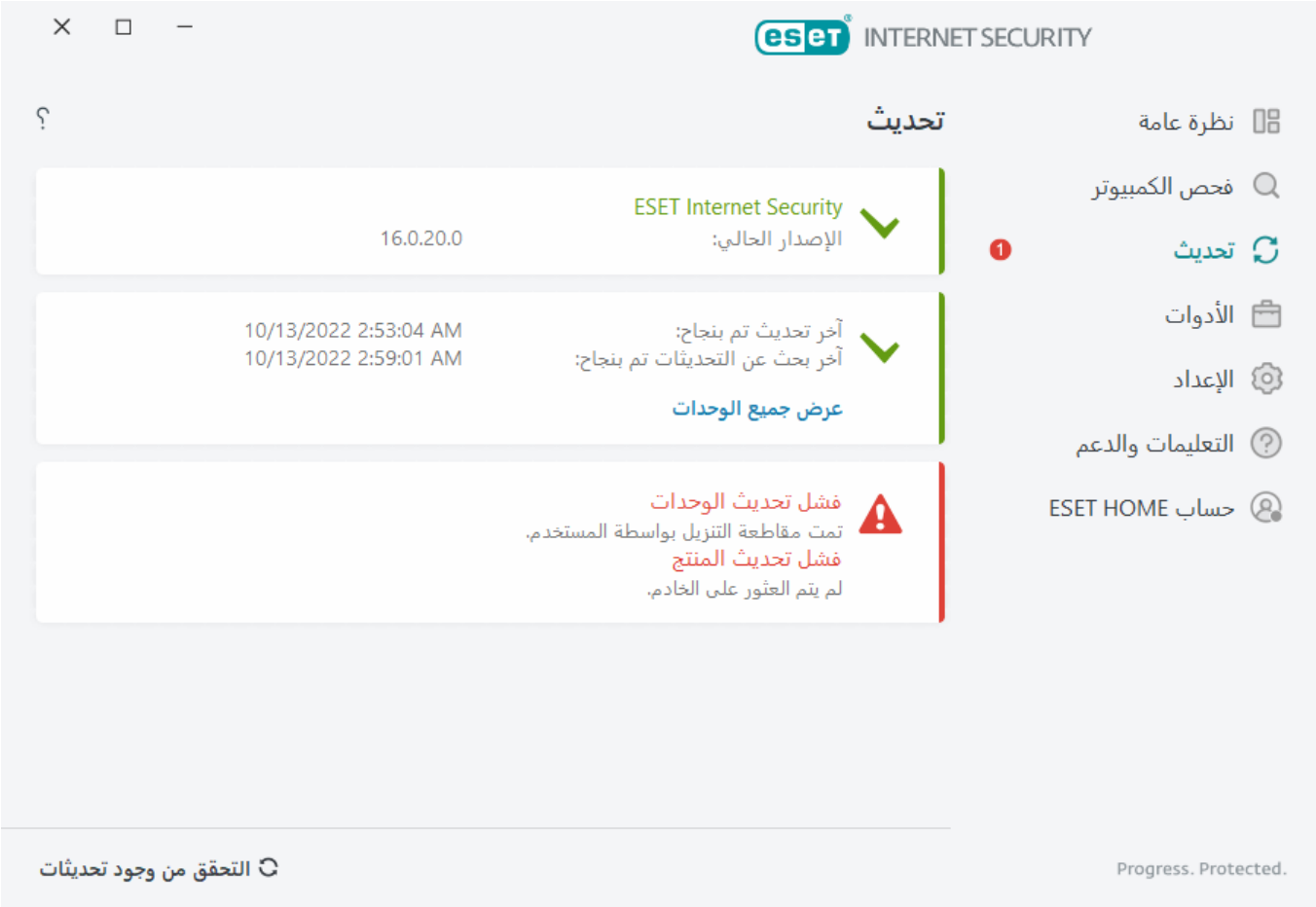
في ظل الظروف العادية، ستشاهد علامة الاختيار الخضراء في نافذة **تحديث** مما يشير إلى أن هذا البرنامج مُحدّث. إذا لم تشاهد علامة الاختيار الخضراء، سيكون البرنامج غير محدث وأكثر عرضة للإصابة. يُرجى تحديث الوحدات في أسرع وقت ممكن.

تحديث غير ناجح

إذا تلقيت رسالة تحديث وحدة نمطية، فربما يكون السبب في الأخطاء التالية:

1. **اشتراك غير صالح** ـ الاشتراك المستخدم للتفعيل غير صالح أو انتهت صلاحيته. في نافذة البرنامج الرئيسية، انقر فوق **المساعدة والدعم** > **تغيير الاشتراك** وقم بتنشيط منتجك.

2. **حدث خطأ أثناء تنزيل ملفات التحديث** – ربما يكون ذلك بسبب إعدادات الاتصال بالإنترنت غير صحيحة. يوصى بفحص اتصالك بالإنترنت (بفتح أي موقع ويب في مستعرض ويب). وإذا لم يفتح موقع ويب، فمن المرجح أنه لم يتم إنشاء الاتصال بالإنترنت أو وجود مشكلات في الاتصال بالكمبيوتر الخاص بك. الرجاء مراجعة موفر خدمة الإنترنت (ISP) إذا لم يكن الاتصال بالإنترنت نشطاً لديك.



يجب إعادة تشغيل جهاز الكمبيوتر بعد تحديث ESET Internet Security بنجاح إلى إصدار أحدث من المنتج لضمان أنه تم تحديث جميع الوحدات للبرنامج بشكل صحيح. ليس من الضروري إعادة تشغيل الكمبيوتر الخاص بك بعد تحديثات الوحدات النمطية الاعتيادية.

لمزيد من المعلومات، الرجاء زيارة استكشاف المشكلات وإصلاحها لرسالة "فشل تحديث الوحدات النمطية".

نافذة الحوار – تلزم إعادة التشغيل

تلزم إعادة تشغيل جهاز الكمبيوتر بعد تحديث ESET Internet Security إلى إصدار جديد. تصدُر إصدارات أحدث من ESET Internet Security لتنفيذ تحسينات أو حل مشكلات لا يمكن حلها بواسطة التحديثات التلقائية لوحدات البرنامج.

يمكن تثبيت الإصدار الجديد من ESET Internet Security تلقائياً، بناءً على إعدادات تحديث البرنامج، أو يدوياً من خلال تنزيل إصدار أحدث من السابق وتثبيته.

انقر فوق **إعادة التشغيل الآن** لإعادة تشغيل جهاز الكمبيوتر. إذا كنت تخطط لإعادة تشغيل جهاز الكمبيوتر لاحقاً، فانقر فوق **ذكّرني لاحقاً**. لاحقاً، يمكنك إعادة تشغيل جهاز الكمبيوتر يدوياً من خلال قسم **نظرة عامة** في نافذة البرنامج الرئيسية.

كيفية إنشاء مهام تحديث

يمكن تشغيل التحديثات يدوياً بالنقر فوق **بحث عن تحديثات** في النافذة الرئيسية التي تُعرض بعد النقر فوق **التحديث** من القائمة الرئيسية.

كما يمكن أيضاً تشغيل التحديثات كمهام مجدولة. لتكوين مهمة مجدولة، انقر فوق **الأدوات** > **المجدول**. افتراضياً، يتم تنشيط مهام التحديث التالية في ESET Internet Security:

- **التحديث التلقائي المنتظم**
- **التحديث التلقائي بعد تسجيل دخول المستخدم**

يمكن تعديل كل مهمة تحديث بما يلبي احتياجاتك. بالإضافة إلى مهام التحديث الافتراضية، يمكنك إنشاء مهام تحديث جديدة بتكوين يحدده المستخدم. لمزيد من التفاصيل حول إنشاء مهام تحديث وتكوينها، راجع قسم المجدول.

الأدوات

تتضمن قائمة **الأدوات** ميزات توفر أماناً إضافياً وتساعد في تبسيط إدارة ESET Internet Security. الأدوات التالية متوفرة:

ملفات السجل

العمليات الجارية (في حالة تمكين ESET LiveGrid® في ESET Internet Security)

تقرير الأمان

اتصالات الشبكة (إذا كان جدار الحماية ممكناً في ESET Internet Security)

ESET SysInspector

المجدول

System cleaner

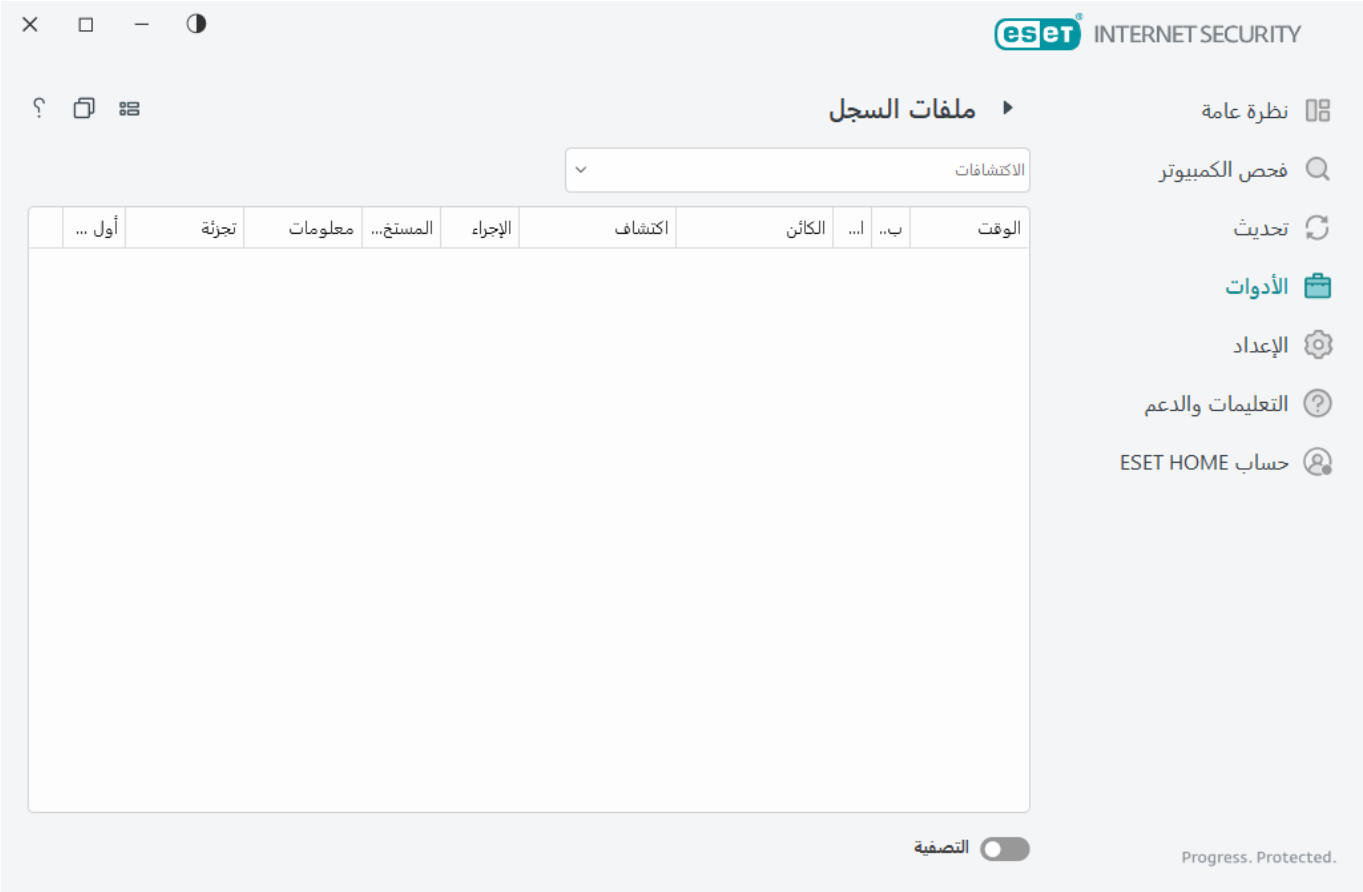
مراقب الشبكة

إرسال العينة للتحليل (ربما لا تكون متوفرة بناء على تكوين ESET LiveGrid®).

العزل

ملفات السجل

تحتوي ملفات السجل على معلومات بشأن أحداث البرنامج المهمة وتقدم نظرة عامة للتهديدات المكتشفة. يعد التسجيل جزءاً ضرورياً في تحليل النظام واكتشاف التهديدات واستكشاف الأخطاء وإصلاحها. ويجري التسجيل بنشاط في الخلفية دون تدخل المستخدم. حيث تُسجَّل المعلومات وفقاً لإعدادات الشرح التفصيلي للسجل الحالي. يمكن عرض الرسائل النصية والسجلات مباشرةً من بيئة ESET Internet Security بالإضافة إلى سجلات الأرشيف.



يمكن الوصول إلى ملفات السجل من نافذة البرنامج الرئيسية بالنقر فوق **الأدوات** > **ملفات السجل**. وحدد نوع السجل المطلوب من القائمة المنسدلة سجل.

- **الاكتشافات** – يقدم هذا السجل معلومات تفصيلية عن الاكتشافات وحالات التسلل التي تم اكتشافها بواسطة ESET Internet Security. وتتضمن معلومات السجل وقت الاكتشاف ونوع أداة الفحص ونوع الكائن وموقع الكائن واسم الاكتشاف والإجراء المتخذ واسم المستخدم الذي كان قيد تسجيل الدخول عند اكتشاف التسلل والمزيج ووقت أول حدوث. عادةً ما يتم تمييز عمليات التسلل التي لم يتم وضع علامة عليها بنص أحمر على خلفية حمراء فاتحة. يتم تمييز عمليات التسلل النظيفة بنص أصفر على خلفية بيضاء. لا يتم تنظيف التطبيقات المحتملة أن تكون غير آمنة أو غير مرغوب فيها بنص أصفر على خلفية بيضاء.
- **الأحداث** ـ يتم تسجيل جميع الإجراءات المهمة التي ينفذها ESET Internet Security في سجل الأحداث. ويحتوي سجل الأحداث على معلومات بشأن الأحداث والأخطاء في البرنامج. وقد تم تصميمه ليساعد مسؤولي ومستخدمي النظام في حل المشكلات. فعادةً ما تساعد المعلومات الموجودة هنا في الوصول إلى حل لمشكلة تحدث في البرنامج.
- **فحص جهاز الكمبيوتر** – يتم عرض جميع نتائج عمليات الفحص السابقة في هذه النافذة. وكل سطر يقابل عنصر تحكم فردي في الكمبيوتر. انقر نقراً مزدوجاً فوق أي إدخال لعرض تفاصيل الفحص ذي الصلة.
- **HIPS** – يحتوي على سجلات القواعد الخاصة HIPS الموضوع عليها علامة للتسجيل. ويعرض البروتوكول التطبيق الذي قام بتشغيل العملية والنتيجة (سواء كانت القاعدة مسموحاً بها أم ممنوعة) واسم القاعدة.
- **حماية المتصفح**—تحتوي على سجلات الملفات التي لم يتم التحقق منها/غير الموثوق بها والتي تم تحميلها في المتصفح.
- **حماية الشبكة** – يعرض سجل حماية الشبكة جميع الهجمات عن بُعد المكتشفة من خلال جدار الحماية والحماية ضد هجمات الشبكة (IDS) والحماية ضد البوت نت. ستجد هنا معلومات عن أي هجوم على جهاز الكمبيوتر لديك. ويعرض عمود الحدث الهجمات المكتشفة. كما يخبرك عمود المصدر بمزيد من المعلومات عن المهاجم. أما عمود البروتوكول فيعرض بروتوكول الاتصال المستخدم في الهجوم. جدير بالذكر أن تحليل سجل حماية الشبكة يساعد في اكتشاف

محاولات التسلل إلى النظام في الوقت المناسب لمنع الوصول غير المسموح به إلى النظام. لمزيد من التفاصيل عن هجمات الشبكة، راجع خيارات نظام كشف التسلل والخيارات المتقدمة.

- **مواقع الويب التي تمت تصفيتها**—هذه القائمة مفيدة إذا كنت تريد عرض قائمة بمواقع الويب التي تم حظرها بواسطة حماية الوصول إلى الويب أو الرقابة الأبوية. كل سجل يتضمن الوقت وعنوان URL والمستخدم والتطبيق الذي أنشأ اتصالاً بموقع ويب معين.
- **مكافحة البريد العشوائي لعميل البريد الإلكتروني**يحتوي على سجلات ذات صلة برسائل البريد الإلكتروني الموضوع عليها علامة بريد عشوائي.
- **المراقبة الأبوية** – تعرض صفحات الويب المحظورة أو المسموح بها بواسطة مراقبة أبوية. ويخبرك عمود نوع المطابقة وقيم المطابقة بطريقة تطبيق قواعد التصفية.
- **التحكم فالاجهزة المتصلة** ـ يحتوي على سجلات للوسائط القابلة للإزالة أو الأجهزة التي كانت متصلة بالكمبيوتر. ولن يتم تسجيل سوى الأجهزة ذات قواعد تحكم في الجهاز في ملف السجل. فإذا لم تطابق القاعدة جهازاً متصلاً، فسيتم إنشاء إدخال سجل للجهاز المتصل. ويمكنك هنا عرض تفاصيل مثل نوع الجهاز والرقم التسلسلي واسم المورِّد وحجم الوسائط (في حال التوفر).
- **حماية كاميرا الويب** – يحتوي على سجلات عن التطبيقات المحظورة من قبل حماية كاميرا الويب.

حدد محتويات أي سجل واضغط على **CTRL + C** لنسخها إلى الحافظة . اضغط مع الاستمرار على مفتاحي **CTRL** أو **SHIFT** لتحديد العديد من الإدخالات.

انقر فوق **تصفية** لفتح نافذة تصفية السجل حيث يمكنك تعريف معايير التصفية.

انقر برز الماوس الأيمن فوق سجل معين لفتح القائمة السياقية. تتوفر الخيارات التالية في القائمة السياقية:

- **إظهار** ـ إظهار المزيد من المعلومات التفصيلية عن السجل المحدد في نافذة جديدة.
- **تصفية السجلات المتماثلة** ـ بعد تنشيط عامل التصفية هذا، فلن ترى إلا السجلات ذات نفس النوع (التشخيصات، التحذيرات،).
- **تصفية** ـ بعد النقر فوق هذا الخيار، ستسمح لك نافذة تصفية السجل بتعريف معايير التصفية لإدخالات سجل معينة.
- **تمكين عامل التصفية** ـ لتنشيط إعدادات عامل التصفية.
- **تعطيل عامل التصفية** ـ لمسح كل إعدادات عامل التصفية (كما هو موضح بالأعلى).
- **نسخ/نسخ الكل** ـ لنسخ المعلومات عن السجلات المحددة في النافذة.
- **نسخ الخلية**—ينسخ محتوى الخلية التي تم النقر عليها بزر الماوس الأيمن.
- **حذف/حذف الكل** ـ لحذف السجلات المحددة أو كل السجلات المعروضة. يتطلب هذا الإجراء امتيازات المسؤول.
- **تصدير/تصدير الكل** ـ لتصدير معلومات عن السجلات المحددة أو جميع السجلات بتنسيق XML.
- **بحث/بحث عن التالي/بحث عن السابق** ـ بعد النقر فوق هذا الخيار، ستسمح لك نافذة تصفية السجل بتعريف معايير التصفية لتمييز الإدخال المحدد.
- **وصف الاكتشاف** — لفتح موسوعة تهديدات ESET والتي تحتوي على معلومات تفصيلية عن مخاطر وأعراض التسلل المسجل.
- **إنشاء استبعاد** – إنشاء جديد استبعاد الاكتشاف باستخدام معالج (غير متاح لاكتشافات البرامج الضارة).
- **إضافة إلى قائمة السماح بحماية المتصفح**—فتح نافذة قائمة السماح بحماية المتصفح وإضافة العنصر إلى القائمة.

تصفية السجل

انقر فوق **التصفية** في **الأدوات** > **ملفات ملفات السجل** لتحديد معايير التصفية.

ستساعدك ميزة تصفية السجل في العثور على المعلومات التي تبحث عنها، خاصة عندما تكون هناك العديد من السجلات. فهي تتيح لك تضييق نطاق السجلات، على سبيل المثال، إذا كنت تبحث عن نوع معين من حدث أو حالة فترة زمنية. يمكنك تصفية السجلات من خلال تحديد خيارات بحث معينة، ولن تظهر سوى السجلات ذات الصلة فقط (طبقاً لخيارات البحث هذه) في نافذة ملفات السجل.

اكتب الكلمة الأساسية التي تبحث عنها في حقل **بحث عن نص**. استخدم القائمة المنسدلة **بحث في الأعمدة** لصقل نتائج البحث. اختر سجلا أو أكثر من القائمة المنسدلة **أنواع السجل**. حدد **الفترة الزمنية** التي تود ظهور النتائج خلالها. يمكنك أيضاً استخدام المزيد من خيارات البحث، مثل **مطابقة الكلمات كلها فقط** او **تحسس حالة الأحرف**.

بحث عن نص

اكتب سلسلة (كلمة أو جزء من كلمة). لن يظهر سوى السجلات التي تحتوي على هذه السلسلة. وسيتم حذف السجلات الأخرى.

بحث في الأعمدة

حدد الأعمدة التي سيتم أخذها في الاعتبار عند البحث. يمكنك تحديد عمود أو أكثر لاستخدامها في البحث.

أنواع السجلات

اختر نوع سجل أو أكثر من القائمة المنسدلة:

- **التشخيص** – لتسجيل معلومات مطلوبة لضبط البرنامج وجميع السجلات الواردة أعلاه.
- **إخباري** – لتسجيل رسائل معلوماتية، تشمل رسائل التحديث الناجح، إضافة إلى جميع السجلات الواردة أعلاه.
- **التحذيرات** – لتسجيل رسائل الخطأ والتحذير الحرجة.
- **أخطاء** – سيتم تسجيل الأخطاء مثل "خطأ أثناء تنزيل الملف" والأخطاء الحرجة.
- **حرج** – لتسجيل الأخطاء الحرجة فقط (مثل: خطأ أثناء بدء الحماية ضد الفيروسات

الفترة الزمنية

حدد فترة زمنية تريد عرض النتائج منها.

- **غير محدد** (افتراضي) – لا يبحث ضمن الفترة الزمنية، بل يبحث في السجل بالكامل.
- **آخر يوم**
- **الأسبوع الماضي**
- **الشهر الماضي**
- **الفترة الزمنية** – يمكنك تحديد الفترة الزمنية بالضبط (من: وإلى:) لتصفية فقط السجلات الخاصة بالفترة الزمنية.

مطابقة الكلمات كلها فقط

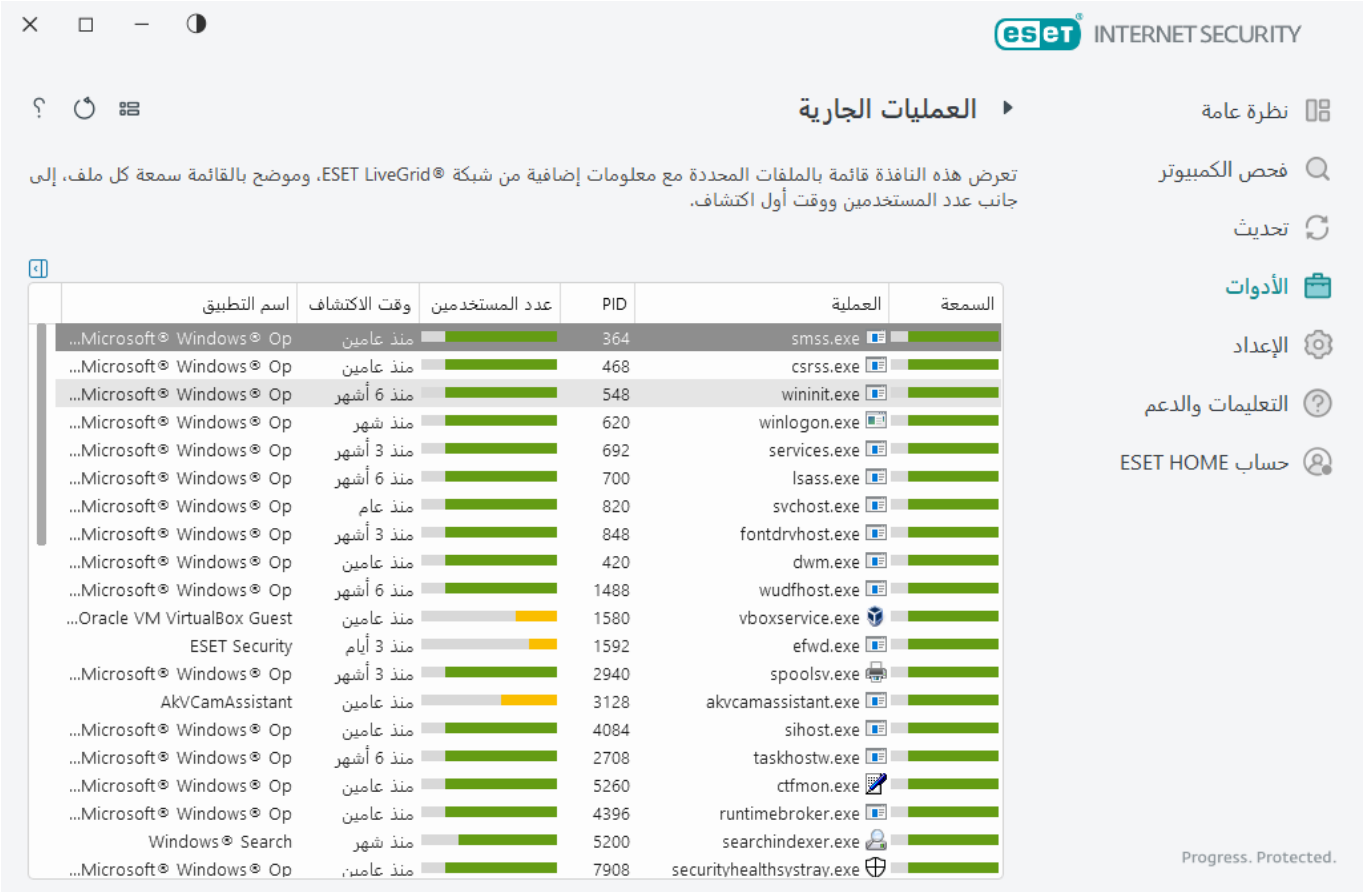
استخدم خانة الاختيار هذه إذا كنت تريد البحث عن كلمات كاملة للحصول على نتائج أكثر دقة.

تحسس حالة الأحرف

قم بتمكين هذا الخيار إذا كان من المهم بالنسبة لك استخدام أحرف صغيرة أو أحرف كبيرة أثناء التصفية. وبمجرد قيامك بتكوين خيارات التصفية / البحث، انقر فوق **موافق** لإظهار السجلات التي تمت تصفيتها أو **"بحث"** لبدء البحث. يتم البحث عن ملفات السجل من الأعلى إلى الأسفل، بدءاً من موضعك الحالي (السجل المميز). ويتوقف البحث عند العثور على أول سجل مطابق. اضغط على **F3** للبحث عن السجل التالي أو انقر بزر الماوس الأيمن وحدد **بحث** لصقل خيارات البحث.

العمليات الجارية

تعرض العمليات الجاريةالبرامج أو العمليات الجارية على الكمبيوتر وتبلغ ESET على الفور وبشكل مستمر بحالات التسلل الجديدة. ESET Internet Security ويوفر معلومات تفصيلية عن العمليات الجارية لحماية المستخدمين باستخدام®ESET LiveGrid التقنية.



السمعة – في أغلب الحالات، يقوم كل من ESET Internet Security وESET LiveGrid® بتعيين مستويات خطورة للكائنات (الملفات، العمليات، مفاتيح السجل، إلخ) باستخدام سلسلة من قواعد الأساليب البحثية التي تفحص سمات كل كائن ثم تقدر احتمالية أن يقوم بتنفيذ نشاط ضار. ووفقاً لهذه الأساليب البحثية، يتم تعيين مستوى خطورة للكائنات من المستوى 1 – جيد (أخضر) إلى المستوى 9 – محظور (أحمر).

العملية ـ اسم صورة البرنامج أو العملية التي تعمل حالياً على جهاز الكمبيوتر. يمكنك أيضاً استخدام مدير المهام في Windows لمشاهدة كل العمليات الجارية على الكمبيوتر. لفتح "مدير المهام"، انقر بزر الماوس الأيمن فوق أي منطقة فارغة في شريط المهام ثم انقر فوق **مدير المهام**, أو اضغط على **Ctrl+Shift+Esc** في لوحة المفاتيح.

> تعد التطبيقات المعروفة المعلّمة بعلامة جيد (أخضر) نظيفة بالتأكيد (مضافة في القائمة البيضاء) وسيتم استبعادها من الفحص لتحسين الأداء.

PID – يُمكن استخدام رقم معرّف العملية كمعلمة في استدعاءات وظائف متنوعة مثل ضبط أولوية العملية.

عدد المستخدمين ـ عدد المستخدمين الذين يستخدمون تطبيقاً معيناً. ويتم تجميع هذه المعلومات بواسطة تقنية ESET LiveGrid®.

وقت الاكتشاف ـ الفترة الزمنية منذ اكتشاف التطبيق بواسطة تقنية ESET LiveGrid®.

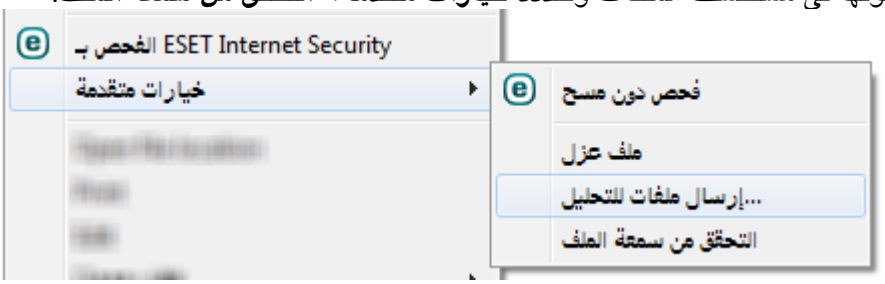
> التطبيق المعلّم بعلامة غير معروف (برتقالي) ليس بالضرورة برنامجاً ضاراً. وعادةً ما يكون مجرد تطبيق جديد. وإذا كنت غير متأكد من الملف، يمكنك إرسال الملف للتحليل إلى مختبر الأبحاث التابع لشركة ESET. وإذا تبين أن الملف تطبيق ضار، فستتم إضافة اكتشافه إلى تحديث تالٍ.

اسم التطبيق ـ الاسم المحدد لبرنامج أو عملية.

انقر فوق أي تطبيق لعرض التفاصيل التالية لهذا التطبيق:

- **المسار** ـ موقع تطبيق على الكمبيوتر.
- **الحجم** ـ حجم الملف إما بالكيلو بايت أو الميجا بايت.
- **الوصف** ـ خصائص الملف وفقاً للوصف الذي يوفره نظام التشغيل.
- **الشركة** ـ اسم عملية التطبيق أو المورِّد.
- **الإصدار** ـ معلومات من ناشر التطبيق.
- **المنتج** ـ اسم التطبيق و/أو اسم الشركة.
- **تاريخ الإنشاء / التعديل** – تاريخ ووقت الإنشاء (التعديل).

> يُمكنك أيضاً التحقق من سمعة الملفات التي لا تعمل كبرامج/عمليات قيد التشغيل. للقيام بذلك، انقر بزر الماوس الأيمن فوقها في مستكشف الملفات وحدد **خيارات متقدمة** > **التحقق من سمعة الملف**.



تقرير الأمان

هذه الميزة تعطي نظرة عامة حول الإحصائيات الخاصة بالفئات التالية:

- **تم حظر صفحات الويب**ـ عرض عدد صفحات الويب المحظورة (عناوين URL التي تم وضعها في القائمة السوداء

للتطبيقات التي يحتمل كونها غير مرغوب فيها أو التصيد الاحتيالي أو الموجه المخترق أو عنوان IP أو الشهادة).

- **تم اكتشاف كائنات بريد إلكتروني مصابة** – عرض عدد كائنات البريد الإلكتروني المصابة التي تم اكتشافها.
- **تم حظر صفحات ويب في المراقبة الأبوية** – عرض عدد صفحات الويب المحظورة في الرقابة الأبوية.
- **تم اكتشاف تطبيق يحتمل أن يكون غير مرغوب فيه** – عرض عدد التطبيقات المحتملة أن تكون غير مرغوب فيها(PUA).
- **تم اكتشاف رسائل بريد إلكتروني عشوائية** – عرض عدد رسائل البريد الإلكتروني العشوائية التي تم اكتشافها.
- **حظر الوصول إلى كاميرا الويب** – عرض عدد عمليات الوصول المحظورة إلى كاميرا الويب.
- **المستندات التي تم فحصها** – عرض عدد كائنات المستندات التي تم فحصها.
- **التطبيقات التي تم فحصها** – عرض عدد كائنات التطبيقات القابلة للتنفيذ التي تم فحصها.
- **الكائنات الأخرى التي تم فحصها** – عرض عدد كائنات التطبيقات الأخرى التي تم فحصها.
- **كائنات صفحات الويب التي تم فحصها** – عرض عدد كائنات صفحات الويب التي تم فحصها.
- **كائنات البريد الإلكتروني التي تم فحصها** – عرض عدد البريد الإلكتروني التي تم فحصها.

يعتمد ترتيب هذه الفئات على القيمة الرقمية من الأعلى إلى الأدنى. لا يتم عرض الفئات التي بها قيم صفر. انقر فوق **إظهار المزيد** لتوسيع الفئات المخفية وعرضها.

يعرض عليك الجزء الأخير من تقرير الأمان إمكانية تنشيط الميزات التالية:

- المراقبة الأبوية
- مكافحة السرقة

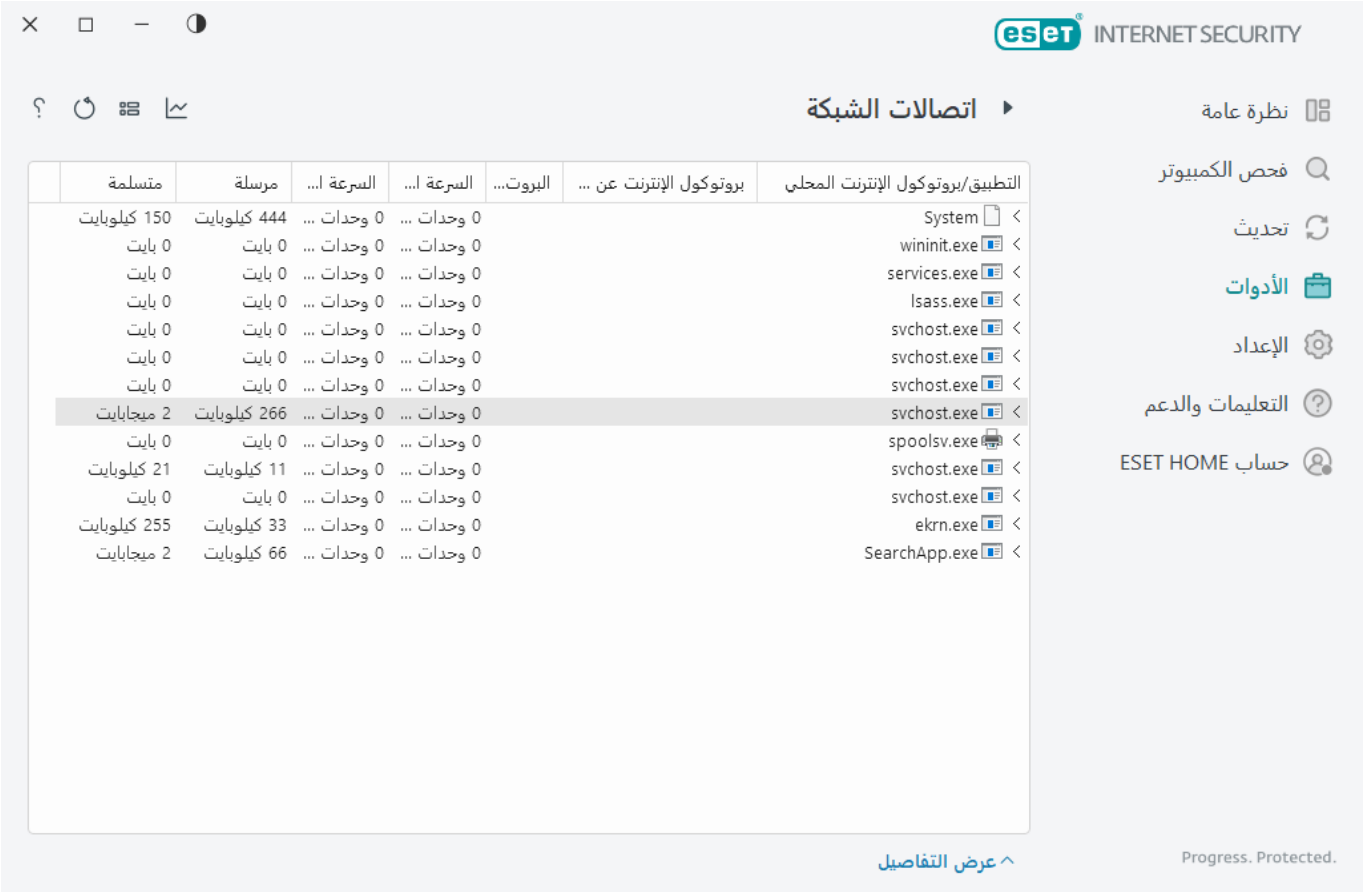
بمجرد تمكين الميزة، لا يتم عرضها بعد الآن على أنها لا تعمل في تقرير الأمان.

انقر فوق عجلة الترس⚙ في أعلى الجانب الأيسر حيث يمكنك **تمكين/تعطيل إعلامات تقرير الأمان** أو تحديد ما إذا كان سيتم عرض البيانات لآخر 30 يوماً أو منذ أن تم تنشيط المنتج. إذا تم تثبيت ESET Internet Security منذ أقل من 30 يوماً، فلا يمكن تحديد سوى عدد الأيام منذ التثبيت. يتم تعيين مدة الـ 30 يوماً افتراضياً.

إعادة تعيين البيانات ستؤدي إلى مسح جميع الإحصائيات وإزالة البيانات الموجودة لتقرير الأمان. نبغي تأكيد هذا الإجراء ما لم تقم بإلغاء تحديد خيار **السؤال قبل إعادة تعيين الإحصائيات** في الإعداد المتقدم > **الإشعارات** > **التنبيهات التفاعلية** > **رسائل التأكيد** > **تحرير**.

اتصالات الشبكة

في قسم "اتصالات الشبكة"، يمكنك رؤية قائمة بالاتصالات النشطة وقيد الانتظار. ويساعدك ذلك على التحكم في جميع التطبيقات التي تنشئ اتصالات صادرة.



انقر فوق رمز الرسم البياني لفتح نشاط الشبكة.

يعرض السطر الأول اسم التطبيق وسرعة نقل البيانات له. لعرض قائمة الاتصالات التي يجريها التطبيق (ومزيداً من المعلومات التفصيلية)، انقر فوق >.

الأعمدة

التطبيق/بروتوكول الإنترنت المحلي – اسم التطبيق وعناوين IP المحلية ومنافذ الاتصال.

IP بعيد – عنوان IP ورقم المنفذ الخاص بكمبيوتر بعيد معين.

البروتوكول – بروتوكول النقل المستخدَم.

سرعة الصادر/سرعة الوارد – السرعة الحالية للبيانات الصادرة والواردة.

المرسَل/المستلَم – مقدار البيانات التي يتم تبادلها داخل الاتصال.

إظهار التفاصيل – اختر هذا الخيار لعرض معلومات تفصيلية حول الاتصال المحدد.

انقر بزر الماوس الأيمن فوق اتصال لعرض خيارات إضافية تشمل:

حل أسماء الأجهزة المضيفة – إن أمكن، يتم عرض جميع عناوين الشبكة بتنسيق DNS وليس بتنسيق عنوان IP الرقمي.

عرض اتصالات TCP فقط – تعرض القائمة اتصالات تنتمي إلى مجموعة بروتوكولات TCP فقط.

إظهار اتصالات الاستماع – حدد هذا الخيار فقط لعرض اتصالات، عندما لا يوجد اتصال تم إنشاؤه حالياً، ولكن النظام قد فتح منفذاً وبانتظار اتصال.

إظهار الاتصالات داخل الكمبيوتر – حدد هذا الخيار لإظهار اتصالات فقط، بينما الجانب البعيد يكون نظاماً محلياً، وهو ما يسمى اتصالات localhost.

سرعة التحديث – اختر تكرار تحديث الاتصالات النشطة.

تحديث الآن – لإعادة تحميل نافذة **اتصالات الشبكة**.

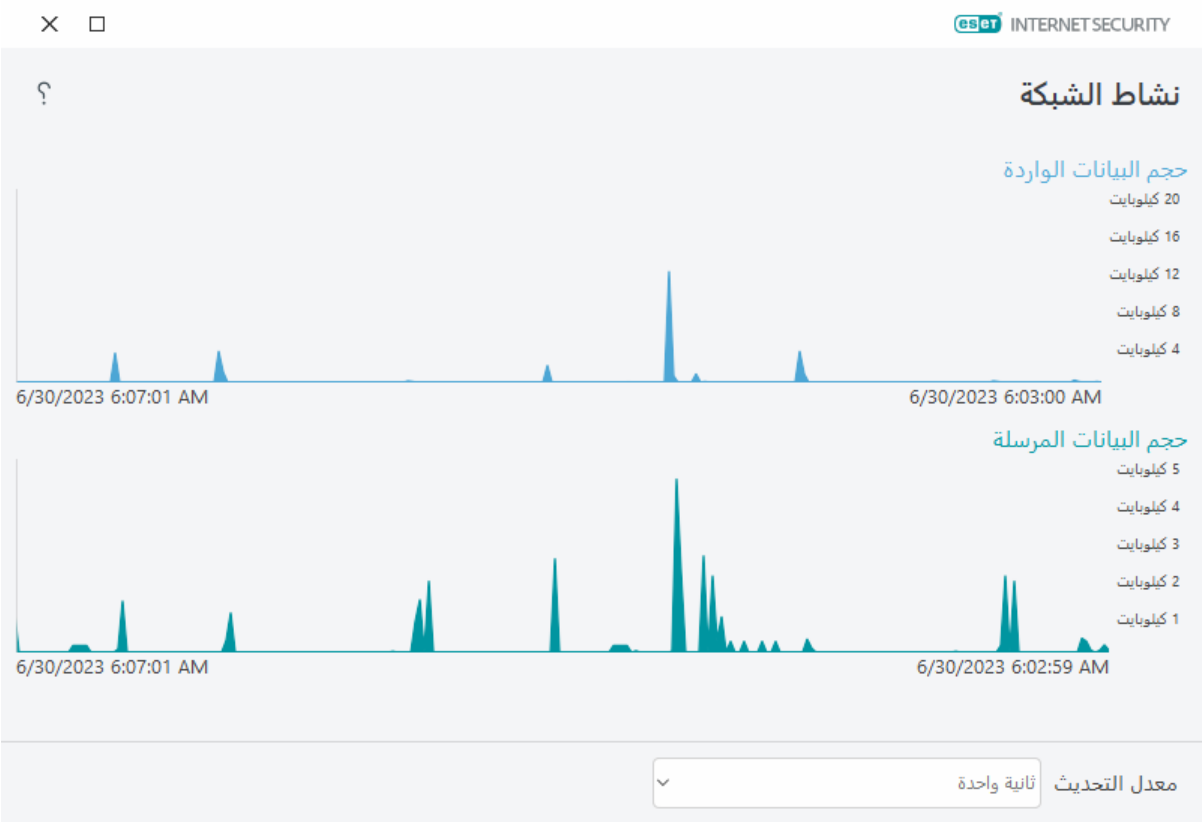
لا تتوفر الخيارات التالية إلا بعد النقر فوق تطبيق أو عملية، وليس فوق اتصال نشط:

رفض التواصل الخاص بالعملية مؤقتاً – لرفض الاتصالات الحالية للتطبيق المعين. في حالة إنشاء اتصال جديد، يستخدم جدار لحماية قاعدة محددة مسبقاً. يمكن العثور على وصف للإعدادات في قسم قواعد جدار الحماية.

السماح مؤقتاً بالتواصل الخاص بالعملية – للسماح بالاتصالات الحالية للتطبيق المعين. في حالة إنشاء اتصال جديد، يستخدم جدار لحماية قاعدة محددة مسبقاً. يمكن العثور على وصف للإعدادات في قسم قواعد جدار الحماية.

نشاط الشبكة

لعرض **نشاط الشبكة** الحالي بصيغة رسم بياني، انقر فوق **الأدوات** > **اتصالات الشبكة** وانقر فوق أيقونة الرسم البياني. . بأسفل الرسم البياني، يوجد مخطط زمني يسجل نشاط الشبكة في الوقت الفعلي بناءً على النطاق الزمني المحدد. لتغيير النطاق الزمني، حدد خياراً من القائمة المنسدلة **معدل التحديث**.



تتوفر الخيارات التالية:

- **1 ثانية** – يتم تحديث الرسم البياني كل ثانية، ويغطي المخطط الزمني آخر 4 دقائق.
- **1 دقيقة (آخر 24 ساعة)** – يتم تحديث الرسم البياني كل دقيقة، ويغطي المخطط الزمني 24 دقيقة الماضية.
- **1 ساعة (الشهر الماضي)** – يتم تحديث الرسم البياني كل ساعة، ويغطي المخطط الزمني الشهر الماضي.

يمثل المحور الرأسي للرسم البياني مقدار البيانات المستلمة أو المرسلة. مرر مؤشر الماوس فوق الرسم البياني لمعرفة المقدار الدقيق للبيانات المستلمة/المرسلة في وقت محدد.

ESET SysInspector

ESET SysInspector هو تطبيق يفحص جهاز الكمبيوتر الخاص بك بالكامل ويجمع معلومات تفصيلية حول مكونات النظام كبرامج التشغيل والتطبيقات أو اتصالات الشبكة أو إدخالات السجل المهمة، ويقوم بتقييم مستوى الخطورة لكل مكون. ويمكن أن تساعد هذه المعلومات على تحديد سبب سلوك النظام المريب الذي قد يرجع إلى عدم توافق البرامج أو الأجهزة، أو الإصابة ببرامج ضارة. لمعرفة كيفية استخدام ESET SysInspector راجع تعليمات ESET SysInspector عبر الإنترنت.

تعرض نافذة ESET SysInspector المعلومات التالية حول السجلات:

- **الوقت** – وقت إنشاء السجل.
- **تعليق** – تعليق مختصر.
- **المستخدم** – اسم المستخدم الذي أنشأ السجل.
- **الحالة** – حالة إنشاء السجل.

تتوفر الإجراءات التالية:

- **إظهار** – لفتح تسجيل الدخول المحدد في ESET SysInspector. يمكنك أيضاً النقر بزر الماوس الأيمن فوق ملف سجل محدد واختيار **إظهار** من القائمة السياقية.
- **إنشاء** – لإنشاء سجل جديد. انتظر حتى يتم إنشاء ESET SysInspector (حالة**تم الإنشاء**) قبل محاولة الوصول إلى السجل. تم حفظ السجل في C:\ProgramData\ESET\ESET Security\SysInspector.
- **حذف** – لإزالة السجل (السجلات) المحدد من القائمة.

تتوفر العناصر التالية في القائمة السياقية عند تحديد ملف سجل واحد أو أكثر:

- **إظهار** – لفتح السجل المحدد في ESET SysInspector (وظيفة النقر المزدوج فوق سجل نفسها).
- **إنشاء** – لإنشاء سجل جديد. انتظر حتى يتم إنشاء ESET SysInspector (حالة**تم الإنشاء**) قبل محاولة الوصول إلى السجل.
- **حذف** – لإزالة السجل (السجلات) المحدد من القائمة.
- **حذف الكل** – لحذف كل السجلات.
- **تصدير** – لتصدير السجل إلى ملف .xml أو ملف .xml مضغوط.

المجدول

يدير المجدول المهام المجدولة ذات التكوين والخصائص المحددة مسبقاً ويشغلها.

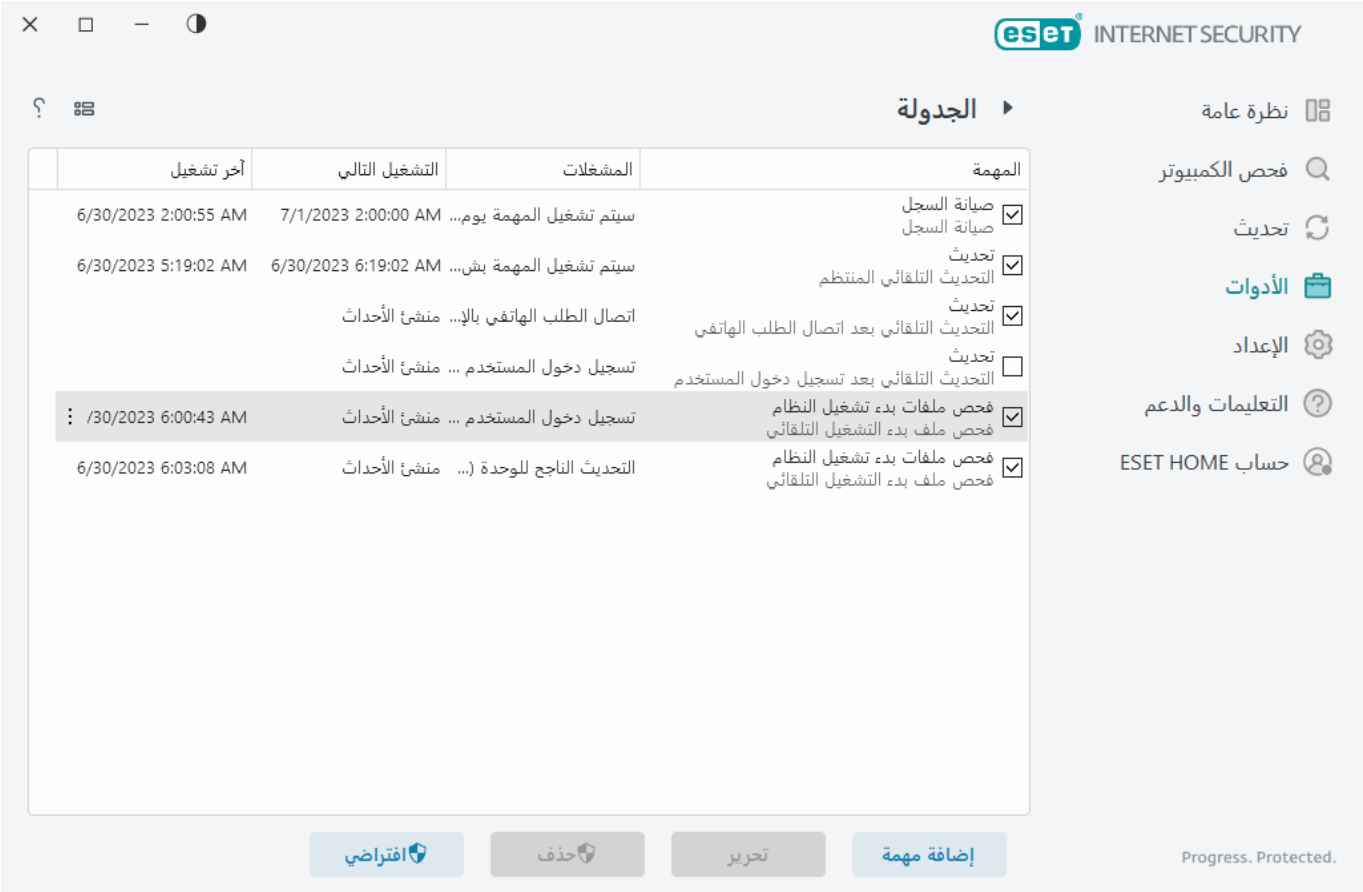
يمكن الوصول إلى المجدول من نافذة البرنامج الرئيسية الخاصة بـ ESET Internet Security من خلال النقر فوق **الأدوات** > **المجدول**. يحتوي **المجدول** على قائمة بكل المهام المجدولة وخصائص التكوين مثل التاريخ والوقت وملف تعريف الفحص المستخدم، المحددة مسبقاً.

يعمل المجدول على جدولة المهام التالية: تحديث الوحدات، ومهمة الفحص، وفحص ملف بدء تشغيل النظام، وصيانة السجل. ويمكنك إضافة مهام أو حذفها مباشرةً من نافذة المجدول الرئيسية (انقر فوق **إضافة مهمة** أو **حذف** في الأسفل). يمكنك إرجاع قائمة المهام المجدولة إلى الحالة الافتراضية وحذف جميع التغييرات بالنقر فوق **افتراضي**. انقر في أي مكان في نافذة المجدول لتنفيذ الإجراءات التالية: عرض معلومات تفصيلية، وتنفيذ المهمة على الفور، وإضافة مهمة جديدة، وحذف مهمة موجودة. استخدم خانات الاختيار في بداية كل إدخال لتنشيط/إلغاء تنشيط المهام.

بشكل افتراضي، يتم عرض المهام المجدولة التالية في **المجدول**:

- **صيانة السجل**
- **التحديث التلقائي المنتظم**
- **التحديث التلقائي بعد تسجيل دخول المستخدم**
- **فحص ملف بدء التشغيل التلقائي** (بعد تسجيل دخول المستخدم)
- **فحص ملف بدء التشغيل التلقائي** (بعد التحديث الناجح لمحرك الكشف)

لتحرير تكوين مهمة مجدولة موجودة (سواء افتراضية أم محددة بواسطة المستخدم)، انقر بزر الماوس الأيمن فوق المهمة وانقر فوق **تحرير** أو حدد المهمة التي تريد تعديلها وانقر فوق **تحرير**.



إضافة مهمة جديدة

1. انقر فوق **إضافة مهمة** بأسفل النافذة.
2. أدخل اسم المهمة.
3. حدد المهمة المطلوبة من القائمة المنسدلة:

- **تشغيل التطبيق الخارجي** – لجدولة تنفيذ تطبيق خارجي.
- **صيانة السجل** – تحتوي ملفات السجل كذلك على بقايا من السجلات المحذوفة. وهذه المهمة تعمل على تحسين السجلات في ملفات السجل بشكل دوري حتى تعمل بشكل فعال.
- **فحص ملفات بدء تشغيل النظام** – لفحص الملفات المسموح بتشغيلها عند بدء تشغيل النظام أو تسجيل الدخول.
- **إنشاء فحص كمبيوتر** – إنشاء لقطة سريعة لبرنامج ESET SysInspector على الكمبيوتر، جمع معلومات تفصيلية عن مكونات النظام (مثل برامج التشغيل، التطبيقات) وتقييم مستوى خطورة كل مكون.
- **فحص الكمبيوتر عند الطلب** – إجراء فحص ملفات ومجلدات على الكمبيوتر.
- **تحديث** – لجدولة مهمة تحديث عن طريق تحديث الوحدات.

4. انقر فوق شريط التمرير بجوار **ممكَّن** لتنشيط المهمة (يمكنك فعل ذلك لاحقاً بتحديد/إلغاء تحديد خانة الاختيار في قائمة المهام المجدولة)، فانقر فوق **التالي** وحدد أحد خيارات الوقت:

- **مرة واحدة** – سيتم تنفيذ المهمة في التاريخ والوقت المحددين.
- **بشكل متكرر** – سيتم تنفيذ المهمة خلال الفاصل الزمني المحدد.
- **يومياً** – سيتم تكرار تشغيل المهمة يومياً في الوقت المحدد.
- **أسبوعياً** – سيتم تنفيذ المهمة في اليوم والوقت المحددين.

- **تشغيل حدث** ـ سيتم تنفيذ المهمة عند وقوع حدث معين.

5. حدد **تجاوز المهمة عند العمل على طاقة البطارية** لتقليل استهلاك موارد النظام عندما يعمل الكمبيوتر المحمول بطاقة البطارية. سيتم تشغيل المهمة في التاريخ والوقت المحددين في حقول **تنفيذ المهام**. وإذا لم تعمل المهمة في الوقت المحدد مسبقاً، فيمكنك تحديد وقت تنفيذها مرة أخرى:

- **في الوقت المجدول التالي**
- **بأقرب ما يمكن**
- **على الفور، إذا تجاوز الوقت منذ آخر تشغيل (بالساعات)** ـ فسيمثل الوقت المنقضي منذ أول تشغيل تم تخطيه للمهمة. إذا تم تجاوز هذا الوقت، فسيتم تشغيل المهمة على الفور. اضبط الوقت باستخدام مؤشر التقدم الدائري أدناه.

لمراجعة المهمة المجدولة، انقر بزر الماوس الأيمن فوق المهمة وانقر فوق **إظهار تفاصيل المهمة**.

خيارات الفحص المجدول

في هذه النافذة، يمكنك تحديد خيارات متقدمة لمهمة فحص مجدولة لجهاز الكمبيوتر.

لتشغيل فحص بدون إجراء التنظيف، انقر فوق **الإعدادات المتقدمة** وحدد **الفحص بدون التنظيف**. يتم حفظ سجل الفحص في سجل الفحص.

عند تحديد **تجاهل الاستبعادات**، سيتم فحص الملفات ذات امتدادات التي تم استبعادها مسبقاً من الفحص بدون أي استبعاد.

تتيح لك القائمة المنسدلة **الإجراء بعد الفحص** تعيين إجراء ليتم تنفيذه تلقائياً بعد انتهاء الفحص:

- **بدون إجراء** ـ بعد انتهاء الفحص، لا يتم اتخاذ أي إجراء.
- **إيقاف تشغيل** ـ يتم إيقاف تشغيل الكمبيوتر بعد انتهاء الفحص.
- **إعادة التشغيل إذا لزم الأمر**–يقوم جهاز الكمبيوتر بإعادة التشغيل إذا لزم الأمر فقط لإكمال تنظيف التهديدات المكتشفة.
- **أعد تشغيل** ـ إغلاق كل التطبيقات المفتوحة وإعادة تشغيل الكمبيوتر بعد انتهاء الفحص.
- **فرض إعادة التشغيل إذا لزم الأمر**–يقوم جهاز الكمبيوتر بفرض إعادة التشغيل إذا لزم الأمر فقط لإكمال تنظيف التهديدات المكتشفة.
- **فرض إعادة التشغيل** ـ فرض إغلاق جميع البرامج المفتوحة دون انتظار تفاعل المستخدم وإعادة تشغيل جهاز الكمبيوتر بعد انتهاء الفحص.
- **سكون** ـ حفظ جلسة العمل ووضع الكمبيوتر في حالة توفير الطاقة بحيث يمكنك استئناف العمل بسرعة.
- **إسبات** ـ أخذ كل ما هو قيد التشغيل في ذاكرة RAM ونقله إلى ملف خاص على القرص الثابت. يتم إيقاف تشغيل الكمبيوتر ولكنه سيستأنف العمل عند تشغيله في المرة القادمة من الحالة السابقة التي تم حفظها.

> i
> تتوفر إجراءات **السكون** أو **الإسبات** استناداً إلى إعدادات نظام تشغيل الطاقة والسكون في جهاز الكمبيوتر أو إمكانيات جهاز الكمبيوتر/الكمبيوتر المحمول تذكّر أن جهاز الكمبيوتر الذي بحالة السكون لا يزال قيد التشغيل. يُرجى العلم بأن الكمبيوتر الذي بحالة السكون لا يزال قيد التشغيل. فهو لا يزال يقوم بتشغيل الوظائف الأساسية ويستهلك الطاقة عندما يكون جهاز الكمبيوتر قيد التشغيل بطاقة البطارية. للحفاظ على عمر البطارية، على سبيل المثال عند مغادرة المكتب، يوصى باستخدام خيار "الإسبات".

سيبدأ الإجراء المحدد بعد انتهاء جميع عليات الفحص الجارية. عند تحديد **إيقاف التشغيل** أو **إعادة التشغيل**، ستظهر نافذة شاشة

تأكيد البرنامج بعد عد تنازلي لمدة 30 ثانية (انقر فوق **إلغاء** لإلغاء تنشيط الإجراء المطلوب).

حدد **يتعذر إلغاء الفحص** لحرمان المستخدمين غير المعتمدين من القدرة على إيقاف الإجراءات التي يتم اتخاذها بعد الفحص.

حدد خيار **يمكن إيقاف الفحص من المستخدم خلال (دقائق)** إذا أردت السماح للمستخدم المحدود الامتيازات بإيقاف فحص الكمبيوتر مؤقتاً لفترة زمنية محددة.

راجع أيضاً تقدم الفحص.

نظرة عامة على المهمة المجدولة

تعرض نافذة الحوار هذه معلومات تفصيلية حول المهمة المجدولة المحددة عند النقر المزدوج فوق مهمة مخصصة أو النقر بزر الماوس الأيمن فوق مهمة مجدول مخصصة ثم فوق **عرض تفاصيل المهمة**.

تفاصيل المهمة

اكتب **اسم المهمة**، وحدد أحد خيارات **نوع المهمة**، ثم انقر فوق **التالي**:

- **تشغيل التطبيق الخارجي** – لجدولة تنفيذ تطبيق خارجي.
- **صيانة السجل** – تحتوي ملفات السجل كذلك على بقايا من السجلات المحذوفة. وهذه المهمة تعمل على تحسين السجلات في ملفات السجل بشكل دوري حتى تعمل بشكل فعال.
- **فحص ملفات بدء تشغيل النظام** – لفحص الملفات المسموح بتشغيلها عند بدء تشغيل النظام أو تسجيل الدخول.
- **إنشاء فحص كمبيوتر** – إنشاء لقطة سريعة لبرنامج ESET SysInspector على الكمبيوتر، جمع معلومات تفصيلية عن مكونات النظام (مثل برامج التشغيل، التطبيقات) وتقييم مستوى خطورة كل مكون.
- **فحص الكمبيوتر عند الطلب** – إجراء فحص ملفات ومجلدات على الكمبيوتر.
- **تحديث** – لجدولة مهمة تحديث عن طريق تحديث الوحدات.

وقت المهمة

سيتم تكرار تنفيذ المهمة خلال الفاصل الزمني المحدد. حدد أحد خيارات الوقت التالية:

- **مرة واحدة** – سيتم تنفيذ المهمة مرة واحدة فقط في التاريخ والوقت المحددين مسبقاً.
- **بشكل متكرر** – سيتم تنفيذ المهمة خلال الفاصل الزمني المحدد (بالساعات).
- **يومياً** – سيتم تشغيل المهمة يومياً في الوقت المحدد.
- **أسبوعياً** – سيتم تشغيل المهمة مرة أو أكثر في الأسبوع، في الأيام والأوقات المحددة.
- **تشغيل حدث** – سيتم تنفيذ المهمة بعد وقوع حدث معين.

تجاوز المهمة عند العمل على طاقة البطارية – لن تبدأ المهمة إذا كان الكمبيوتر يعمل على طاقة البطارية في الوقت المقرر لتشغيلها. كما ينطبق ذلك أيضاً على أجهزة الكمبيوتر التي تعمل على وحدات UPS.

وقت المهمة ـ مرة واحدة

تنفيذ المهام ـ سيتم تشغيل المهمة المحددة مرة واحدة فقط في التاريخ والوقت المحددين.

وقت المهمة ـ يومياً

سيتم تشغيل المهمة يومياً في الوقت المحدد.

وقت المهمة ـ أسبوعياً

سيتم تشغيل المهمة بشكل متكرر كل أسبوع في اليوم (الأيام) والوقت المحددين.

وقت المهمة ـ منشئ الأحداث

يمكن أن يشغِّل المهمة أيٌّ من الأحداث التالية:

- **كل مرة يبدأ فيها تشغيل الكمبيوتر**
- **أول مرة يبدأ فيها تشغيل الكمبيوتر كل يوم**
- **اتصال الطلب الهاتفي بالإنترنت/VPN**
- **التحديث الناجح للوحدة**
- **التحديث الناجح للمنتج**
- **تسجيل دخول المستخدم**
- **اكتشاف التهديد**

عند جدولة مهمة للتشغيل بواسطة حدث، يمكنك تحديد أدنى فاصل بين مرتي إكمال للمهمة. على سبيل المثال، في حالة تسجيل دخولك إلى الكمبيوتر عدة مرات يومياً، اختر 24 ساعة لتنفيذ المهمة عند أول تسجيل دخول في اليوم، ثم في اليوم التالي وهكذا.

المهمة المُتجاوزة

يمكن تجاوز المهمة عند تشغيل جهاز الكمبيوتر بطاقة بطارية أو إيقاف تشغيله. حدد الوقت الذي ينبغي تشغيل المهمة فيه من أحد هذه الخيارات وانقر فوق **التالي**:

- **في الوقت المجدول التالي** ـ سيتم تشغيل المهمة إذا كان جهاز الكمبيوتر قيد التشغيل في الوقت المجدول التالي.
- **في أقرب وقت ممكن** ـ سيتم تشغيل المهمة إذا كان جهاز الكمبيوتر قيد التشغيل.
- **على الفور، إذا تجاوز الوقت منذ آخر تشغيل مجدول (ساعات)** – فسيمثل الوقت المنقضي منذ أول تشغيل تم تخطيه للمهمة. إذا تم تجاوز هذا الوقت، فسيتم تشغيل المهمة على الفور.

على الفور، إذا تجاوز الوقت منذ آخر تشغيل مجدول (ساعات) – أمثلة

يتم تعيين مهمة كمثال للتشغيل بشكل متكرر كل ساعة. تم تحديد الخيار **على الفور، إذا تجاوز الوقت منذ آخر تشغيل مجدول (ساعات)** وتم تعيين الوقت الذي تم تجاوزه إلى ساعتين. يتم تشغيل المهمة في الساعة 13:00، وعند الانتهاء، يدخل جهاز الكمبيوتر في حالة السكون:

- يستيقظ جهاز الكمبيوتر في الساعة 15:30. كان أول تشغيل تم تخطيه للمهمة في الساعة 14:00. لم يمر سوى 1.5 ساعة منذ الساعة 14:00، لذلك سيتم تشغيل المهمة في الساعة 16:00.
- يستيقظ جهاز الكمبيوتر في الساعة 16:30. كان أول تشغيل تم تخطيه للمهمة في الساعة 14:00. لقد مرت ساعتان ونصف منذ الساعة 14:00، لذلك سيتم تشغيل المهمة على الفور.

تفاصيل المهمة ـ تحديث

إذا كنت تريد تحديث البرنامج من خادمي تحديث، فيلزم إنشاء ملفي تعريف تحديث مختلفين. بحيث إذا فشل الأول في تنزيل ملفات تحديث، يقوم البرنامج بالتبديل تلقائياً إلى ملف التعريف البديل. ويناسب ذلك أجهزة الكمبيوتر المحمول التي تقوم بالتحديث عادة من خادم تحديث LAN محلي، ولكن يتصل مالكوها عادة بالإنترنت باستخدام شبكات أخرى. لذلك، في حالة فشل ملف التعريف الأول، سيقوم الثاني تلقائياً بتنزيل ملفات تحديث تنزيل من خوادم تحديث ESET.

تفاصيل المهمة ـ تشغيل التطبيق

تُجدول هذه المهمة تنفيذ تطبيق خارجي.

الملف القابل للتنفيذ ـ اختر ملفاً قابلاً للتنفيذ من شجرة الدليل، وانقر فوق خيار **...** أو أدخل المسار يدوياً.

مجلد العمل ـ حدد دليل عمل التطبيق الخارجي. سيتم إنشاء جميع الملفات المؤقتة في **الملف القابل للتنفيذ** المحدد ضمن هذا الدليل.

المعلمات ـ معلمات سطر أوامر للتطبيق (اختيارية).

انقر فوق **إنهاء** لتطبيق المهمة.

System cleaner

System cleaner عبارة عن أداة تساعدك في إرجاع جهاز الكمبيوتر إلى حالة قابلة للاستخدام بعد تنظيفه من التهديدات. تستطيع البرامج الضارة تعطيل أدوات النظام مثل Registry Editor أو Task manager أو Windows Updates. تقوم أداة System cleaner باستعادة القيم الافتراضية والإعدادات للنظام المعني بنقرة واحدة.

تقوم أداة System cleaner بالإبلاغ عن أخطاء من خمس فئات للإعدادات وهي:

- **إعدادات الأمان**: التغييرات الموجودة في الإعدادات والتي قد تتسبب في زيادة الثغرات للكمبيوتر، مثل Windows Update
- **إعدادات النظام**: التغييرات الموجودة في إعدادات النظام، والتي يمكنها تغيير سلوك جهاز الكمبيوتر، مثل اقترانات الملفات.
- **شكل النظام**: الإعدادات التي تؤثر في شكل النظام، مثل خلفية شاشة سطح المكتب

- **الميزات المعطلة**: التطبيقات والميزات المهمة التي قد تكون معطلة
- **Windows System Restore**: إعدادات ميزة Windows System Restore التي تتيح لك إعادة النظام إلى حالة سابقة

ويُمكن طلب تنظيف النظام في الحالات التالية:

- عند وجود تهديد
- عندما ينقر المستخدم فوق **إعادة تعيين**

يُمكنك الاطلاع على التغييرات وإعادة تعيين الإعدادات إذا كان ذلك مناسباً.

مسموح فقط للمستخدم الذي يحمل حقوق المسؤول تنفيذ الإجراءات في System cleaner.

مراقب الشبكة

مراقب الشبكة يمكن أن يساعد في تحديد الثغرات في شبكتك (المنزلية أو المكتب) الموثوقة (على سبيل المثال، المنافذ المفتوحة أو كلمة مرور جهاز التوجيه الضعيفة). يوفر أيضاً قائمة بالأجهزة المتصلة، مصنفة حسب نوع الجهاز (على سبيل المثال، الطابعة، جهاز التوجيه، الجهاز المحمول، إلخ) لتظهر لك ما هو متصل بشبكتك (على سبيل المثال، وحدة التحكم في الألعاب أو إنترنت الأشياء أو غيرها من الأجهزة المنزلية الذكية).

يساعدك مراقب الشبكة في تحديد ثغرات جهاز التوجيه وزيادة مستوى الحماية عند الاتصال بشبكة خارجية.

لا يقوم مراقب الشبكة بإعادة تكوين جهاز التوجيه لديك. ستقوم بإجراء التغييرات بنفسك باستخدام الواجهة المخصصة لجهاز

التوجيه لديك. يمكن أن تكون الموجهات المنزلية أكثر عرضة للبرمجيات الخبيثة المستخدمة لتشغيل هجمات رفض الخدمة الموزعة (DDoS). إذ كانت كلمة مرور جهاز التوجيه لم يتم تغييرها من الحالة الافتراضية من قبل المستخدم، فبإمكان أي شخص متطفل تخمينها ومن ثم يقوم بالتسجيل في جهاز التوجيه وإعادة تكوينه أو إلحاق الضرر بشبكتك.

نوصي بضرورة وضع كلمة مرور قوية بحيث تكون طويلة بما يكفي وتحتوي على أرقام وأحرف كبيرة. لإنشاء كلمة مرور صعب توقعها، استخدم مجموعة متنوعة من الأحرف المختلفة.

إذا كانت الشبكة التي تتصل بها تم تكوينها على أنها موثوقة فيمكنك وضع علامة على الشبكة على أنها "شبكتي". انقر فوق **وضع علامة "شبكتي"** لإضافة علامة "شبكتي" إلى الشبكة. سيتم عرض هذه العلامة بجوار الشبكة عبر ESET Internet Security للحصول على نظرة عامة على التعريف والأمان بشكل أفضل. انقر فوق **إلغاء وضع علامة "شبكتي"** لإزالة العلامة.

يظهر كل جهاز متصل بشبكتك بالمعلومات الأساسية من خلال طريقة عرض قائمة. انقر فوق الجهاز المحدد لتحرير الجهاز أو لعرض معلومات مفصّلة عن الجهاز.

في عرض القائمة، تتيح لك القائمة المنسدلة **الشبكات** تصفية الأجهزة على أساس المعايير التالية:

- الأجهزة المتصلة بشبكة معينة
- الأجهزة المتصلة **بجميع الشبكات**
- أجهزة غير مصنفة

انقر فوق رمز الجهاز لتحرير الجهاز أو لعرض معلومات مفصّلة عنه. يتم عرض الأجهزة المتصلة مؤخراً بالقرب من جهاز التوجيه بحيث يمكنك اكتشافها بسهولة.

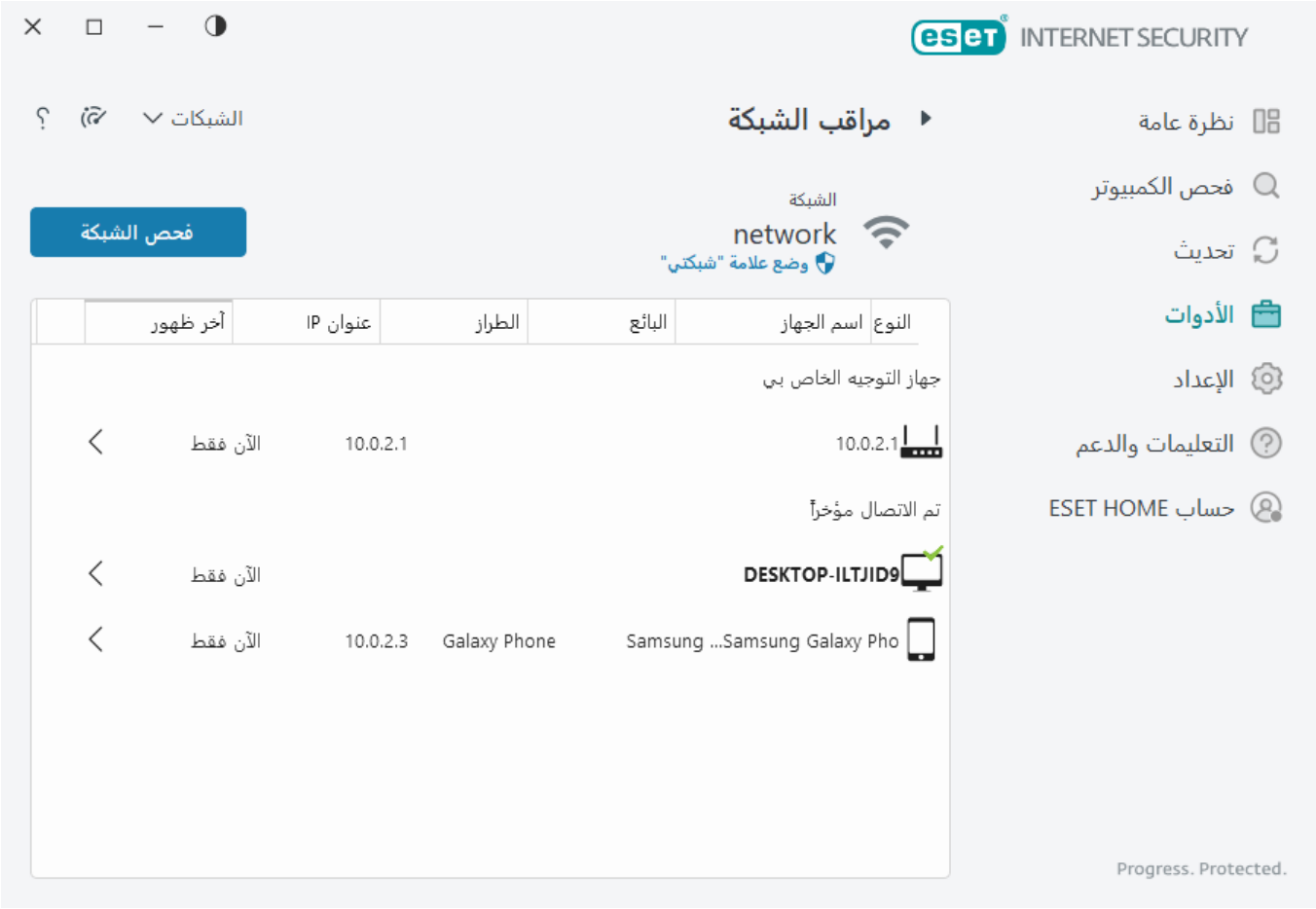
انقر فوق عجلة التروس ⚙ في الزاوية اليمنى العليا لتحديد ما إذا كنت تريد الإبلاغ عند اكتشاف جهاز جديد في الشبكة.

انقر فوق **فحص الشبكة** لفحص الشبكة، المتصل بها حالياً، يدوياً. لا يتوفّر **فحص الشبكة** إلا لشبكة موثوق بها. راجع ملفات تعريف اتصال الشبكة لمراجعة إعدادات الشبكة أو تحريرها.

ويمكنك الاختيار من الخيارات التالية:

- فحص الكل
- فحص جهاز التوجيه فقط
- فحص الأجهزة فقط

قم بإجراء عمليات فحص الشبكة على شبكتك الموثوق بها فقط! إذا قمت بذلك على شبكات غير موثوق بها، فانتبه للمخاطر المحتملة.



عند اكتمال الفحص، سيظهر إعلام به رابط يؤدي إلى المعلومات الأساسية عن الجهاز أو يُمكنك النقر المزدوج فوق الجهاز المشتبه به في طريقة عرض القائمة أو السونار. انقر فوق **استكشاف الأخطاء وإصلاحها** لرؤية الاتصالات المحظورة مؤخراً. المزيد من المعلومات حول استكشاف أخطاء جدار الحماية وإصلاحها.

هناك نوعان من الإعلامات التي يتم عرضها من خلال وحدة "مراقب الشبكة":

- **اتصال جهاز جديد بالشبكة** – يتم عرضه إذا كان هناك جهاز غير مرئي قبل ذلك يتصل بالشبكة بينما المستخدم متصل.
- **تم العثور على جهاز شبكة جديد**– يتم عرضه إذا قمت بإعادة الاتصال بالشبكة الموثوق بها وكان هناك جهاز غير مرئي قبل ذلك موجود الآن.

يقوم كلا الإشعارين بإعلامك ما إذا كان هناك جهاز غير موثوق يحاول الاتصال بشبكتك. انقر فوق **عرض الجهاز** / عرض الأجهزة لإظهار تفاصيل الجهاز.

ماذا تعني الرموز الموجودة على الأجهزة الموجودة في مراقب الشبكة؟

يشير رمز النجمة الصفراء إلى الأجهزة الجديدة على الشبكة أو التي تم اكتشافها بواسطة ESET للمرة الأولى.	
يشير رمز التحذير الأصفر إلى أن جهاز التوجيه الخاص بك قد يحتوي على نقاط ضعف. انقر فوق الرمز في منتجك للحصول على معلومات أكثر تفصيلاً حول المشكلة.	
يشير رمز التحذير الأحمر إلى الأجهزة التي تحتوي على جهاز التوجيه الخاص بك والذي يحتوي على نقاط ضعف وقد تكون مصابة. انقر فوق الرمز في منتجك للحصول على معلومات أكثر تفصيلاً حول المشكلة.	
قد يظهر الرمز الأزرق عندما يحتوي منتج ESET على معلومات إضافية لجهاز التوجيه الخاص بك ولكنه لا يتطلب اهتماماً فورياً لعدم وجود مخاطر أمنية. انقر فوق الرمز الموجود في منتجك للحصول على معلومات أكثر تفصيلاً.	

جهاز الشبكة في مراقب الشبكة

يُمكن العثور على معلومات مفصلّة عن الجهاز هنا، بما ذلك ما يلي:

- اسم الجهاز
- نوع الجهاز
- آخر ظهور
- اسم الشبكة
- عنوان بروتوكول الإنترنت (IP)
- عنوان MAC
- نظام التشغيل

تشير أيقونة القلم الرصاص التي يُمكن من خلالها تعديل اسم الجهاز أو نوعه.

إزالة من السجل ـ احذف الجهاز من قائمة الأجهزة. لا يتوفر هذا الخيار إلا للأجهزة غير المتصلة بشبكتك الآن.

لكل نوع من أنواع الأجهزة، تتوفر الإجراءات التالية:

جهاز التوجيه

إعدادات جهاز التوجيه – يمكن الوصول إلى إعدادات جهاز التوجيه من واجهة الويب أو تطبيق الهاتف المحمول أو النقر فوق **فتح واجهة جهاز التوجيه**. إذا كان لديك جهاز توجيه مقدم من مزود خدمة الإنترنت لديك، فقد يكون من الضروري الاتصال بمصادر دعم مزود خدمة الإنترنت أو الشركة المصنعة لجهاز التوجيه لحل مشكلات الأمان التي تم اكتشافها. اتبع دائماً احتياطات السلامة المناسبة كما هو موضح في دليل مستخدم جهاز التوجيه.
الحماية ـ لحماية جهاز التوجيه والشبكة من هجمات الأمن السيبراني، اتبع هذه التوصيات الأساسية.

جهاز الشبكة

تعريف الجهاز – إذا لم تكن متأكداً من الجهاز المتصل بشبكتك، فتحقق من اسم البائع أو الشركة المصنعة أسفل اسم الجهاز. يمكن أن يساعدك ذلك في تحديد نوع الجهاز. يمكنك تغيير اسم الجهاز للرجوع إليه في المستقبل.
فصل الجهاز – إذا لم تكن متأكداً من أن الجهاز المتصل آمن بشبكتك أو أجهزتك، فقم بإدارة الوصول إلى الشبكة لهذا الجهاز في إعدادات جهاز التوجيه الخاص بك أو قم بتغيير كلمة مرور الشبكة.
الحماية – لحماية جهازك من الهجمات والبرامج الضارة، قم بتثبيت حماية الأمن أثناء استخدام الإنترنت على جهازك واحرص دائماً على تحديث نظام التشغيل والبرامج المثبتة. للحفاظ على الحماية، لا تتصل بشبكات Wi-Fi غير آمنة.

هذا الجهاز

يمثل هذا الجهاز جهاز الكمبيوتر الخاص بك على الشبكة.
محولات الشبكة – تعرض معلومات محولات الشبكة.

الإعلامات | مراقب الشبكة

فيما يلي عدة إعلامات يُمكن عرضها عندما يكتشف ESET Internet Security بعض مشكلات الثغرات في جهاز التوجيه. يحتوي كل إعلام على وصف بسيط ويوفر بعض الحلول أو الخطوات الواجب اتباعها من أجل تقليل خطورة الثغرات على جهاز التوجيه

لديك. إذا لم تكن معتاداً على تغييرات جهاز التوجيه، نوصي بالاتصال بالشركة المصنّعة له أو موفّر خدمة الإنترنت.

تم العثور على ثغرة محتملة
قد يحتوي جهاز التوجيه على ثغرات معروفة التي تجعل من السهل الهجوم على جهازك واستغلاله. تحديث البرنامج الثابت لجهاز التوجيه.

تم العثور على ثغرة
يحتوي جهاز التوجيه على ثغرات معروفة تجعل من السهل الهجوم على جهازك واستغلاله. تحديث البرنامج الثابت لجهاز التوجيه.

تم العثور على تهديد
جهاز التوجيه مصاب ببرامج ضارة. إعادة تشغيل جهاز التوجيه وتكرار الفحص.

كلمة مرور جهاز التوجيه ضعيفة
كلمة مرور جهاز التجيه ضعيفة ويمكن تخمينها بسهولة عن طريق أي شخص آخر. تغيير كلمة المرور في جهاز التوجيه.

إعادة توجيه الشبكة ضار
تظهر حركة الإنترنت لإعادة توجيهها إلى مواقع ويب زائفة وضارة. وهذا يعني أن جهاز التوجيه معرض للخطر. تغيير إعداد خادم DNS في جهاز التوجيه.

خدمات الشبكة مفتوحة
يقوم جهاز التوجيه بتشغيل خدمات الشبكة التي يُمكن للآخرين اختراقها. وقد يكون هذا سبب لضعف التكوين أو تعرض جهاز التوجيه للخطر. تحقق من تكوين جهاز التوجيه.

خدمات الشبكة مفتوحة بدقة
يقوم جهاز التوجيه بتشغيل خدمات الشبكة الحساسة التي يُمكن للآخرين اختراقها. وقد يكون هذا سبب لضعف التكوين أو تعرض جهاز التوجيه للخطر. تحقق من تكوين جهاز التوجيه.

البرنامج الثابت قديم
البرنامج الثابت الموجود في جهاز التوجيه قديم وقد يحتوي على ثغرات. تحديث البرنامج الثابت في جهاز التوجيه.

إعداد جهاز التوجيه ضار
خادم DNS الذي تستخدمه ضار وقد يرسلك إلى مواقع خطرة. وهذا يعني أن جهاز التوجيه معرض للخطر. تغيير إعداد خادم DNS في جهاز التوجيه.

خدمات الشبكة
يقوم جهاز التوجيه بتشغيل خدمات الشبكة العامة. هذه الخدمات مطلوبة للشبكة وربما تكون آمنة. تحقق من تكوين جهاز التوجيه.

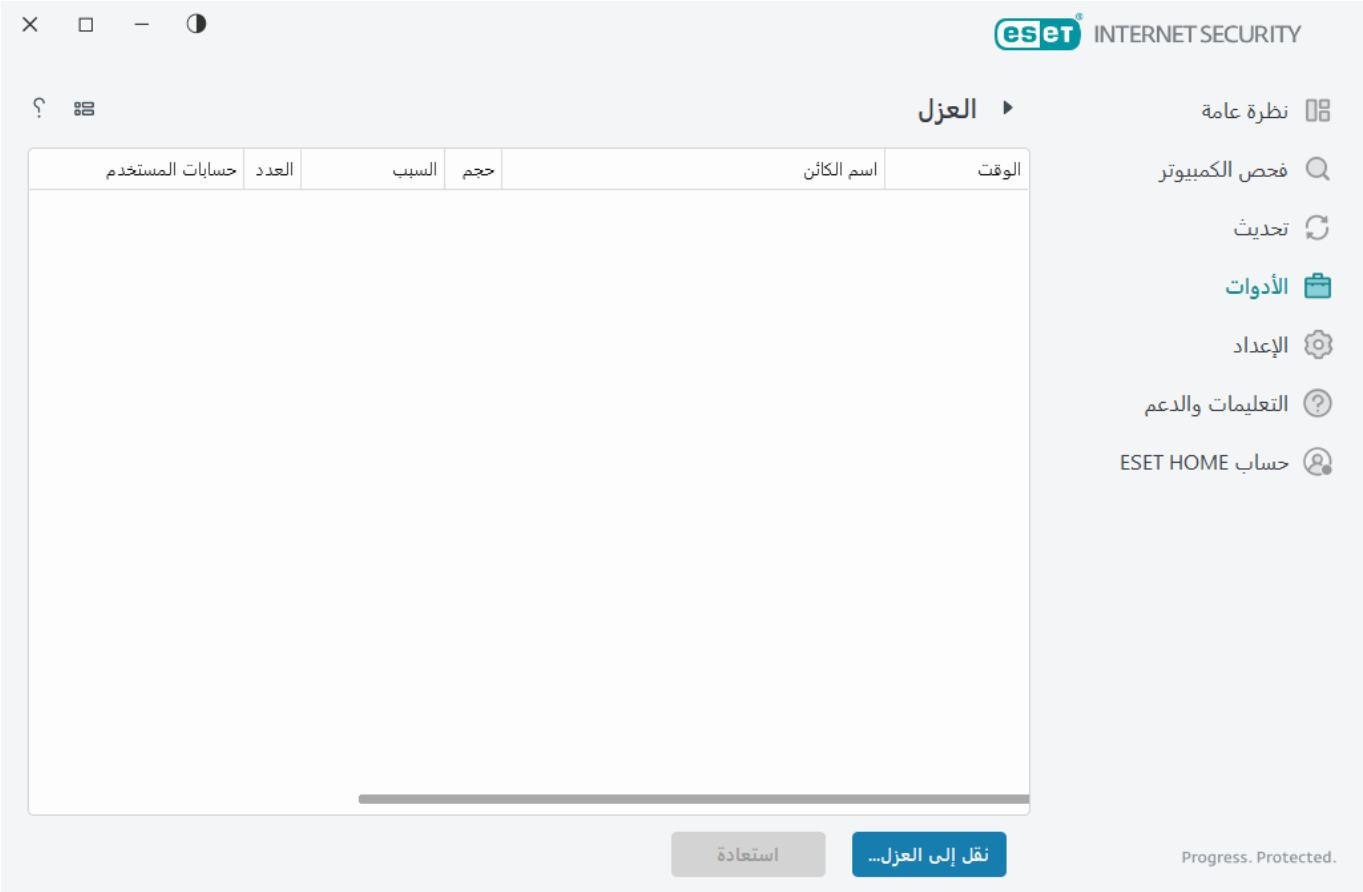
العزل

تتمثل الوظيفة الرئيسية للعزل في تخزين الأشياء المبلغ عنها بأمان (مثل البرمجيات الخبيثة أو الملفات المصابة أو التطبيقات المحتملة أن تكون غير مرغوب فيها).

يمكن الوصول إلى العزل من نافذة البرنامج الرئيسية الخاصة بـ ESET Internet Security من خلال النقر فوق **الأدوات** > **العزل**.

يمكن عرض الملفات المخزنة في مجلد العزل في جدول يعرض:

- تاريخ ووقت العزل،
- المسار إلى الموقع الأصلي للملف،
- حجمها بالبايت،
- السبب (على سبيل المثال، الكائن المضاف من قبل المستخدم)،
- وعدد عمليات الاكتشاف (على سبيل المثال، عمليات الاكتشاف المكررة للملف ذاته أو إذا كان أرشيفاً يحتوي على عمليات تسلل متعددة).



عزل ملفات

يعمل ESET Internet Security على عزل الملفات المحذوفة (في حال لم تقم بإلغاء هذا الخيار في نافذة التنبيه).

يُفترض أن يتم عزل ملفات أخرى في الحالات التالية:

a. لا يمكن تنظيفها،
b. إذا لم يكن من الآمن أو لم يكن من المستحسن حذفها،
c. إذا كان يتم اكتشافها بشكل زائف من قبل ESET Internet Security،
d. أو إذا كان سلوك الملف مريباً ولكن لم يتم اكتشافه بواسطة وسائل الحماية.

لعزل ملف، لديك العديد من الخيارات:

a. استخدام ميزة السحب والإفلات في عزل الملف يدوياً بالنقر فوق الملف، وتحريك مؤشر الماوس إلى المنطقة المحددة مع الاستمرار في الضغط على زر الماوس ثم تحريره. بعد ذلك، يتم نقل التطبيق إلى المقدمة.
b. انقر بزر الماوس الأيمن فوق الملف > انقر فوق **خيارات متقدمة** > **عزل الملف**.
c. انقر فوق **نقل إلى العزل** من نافذة **العزل**.
d. يمكن استخدام القائمة السياقية أيضاً لهذا الغرض؛ انقر بزر الماوس الأيمن في نافذة **العزل** وحدد **العزل**.

الاستعادة من العزل

يمكن أيضاً استعادة الملفات المعزولة إلى موقعها الأصلي:

- استخدم ميزة **الاستعادة** لهذا الغرض، والتي تتوفر من القائمة السياقية من خلال الضغط بزر الماوس الأيمن فوق ملف محدد في العزل.
- إذا تم وضع علامة على ملف كـ تطبيق يحتمل كونه غير مرغوب، يتم تمكين خيار **استعادة واستثناء من الفحص**. راجع أيضاً الاستثناءات.
- تعرض القائمة السياقية أيضاً خيار **استعادة إلى**، مما يسمح لك باستعادة ملف إلى موقع آخر غير الذي تم حذفه منه.
- لا تتوفر وظيفة الاستعادة في بعض الحالات، على سبيل المثال، للملفات الموجودة على مشاركة شبكة للقراءة فقط.

الحذف من العزل

انقر بزر الماوس الأيمن فوق عنصر محدد واختر **حذف من العزل**، أو حدد العنصر الذي تريد حذفه واضغط على مفتاح **Delete** في لوحة المفاتيح. إذا كنت ترغب في تحديد جميع العناصر وحذفها في العزل، يمكنك الضغط **Ctrl + A** ثم **Delete** على لوحة المفاتيح. ستتم إزالة العناصر المحذوفة من العزل والجهاز نهائياً.

إرسال ملف من العزل

إذا كنت قد عزلت ملفاً مريباً لم يكتشفه البرنامج، أو إذا تم تحديد أن هناك ملفاً مصاباً بشكل غير صحيح (على سبيل المثال، عن طريق التحليل الإرشادي للرمز) ثم تم عزله بعد ذلك، يرجى إرسال العينة للتحليل في معمل أبحاث ESET. لإرسال ملف، انقر بزر الماوس الأيمن فوق الملف وحدد **إرسال للتحليل** من القائمة السياقية.

وصف الكشف

انقر بزر الماوس الأيمن فوق عنصر وانقر فوق **وصف الاكتشاف** لفتح موسوعة تهديدات ESET والتي تحتوي على معلومات مفصلة حول مخاطر وأعراض التسلل المسجل.

إرشادات موضحة

قد لا تتوفر مقالات قاعدة معارف ESET التالية إلا باللغة الإنجليزية:

- استعادة ملف معزول في ESET Internet Security
- حذف ملف معزول في ESET Internet Security
- منتج ESET الخاص بي أبلغني باكتشاف – ما الذي ينبغي عليّ فعله؟

فشل العزل

فيما يلي أسباب تعذّر نقل ملفات معينة إلى العزل:

- **ليس لديك أذونات القراءة** – مما يعني أنه لا يمكنك عرض محتوى ملف.
- **ليس لديك أذونات الكتابة** – مما يعني أنه لا يمكنك تعديل محتويات الملف، كإضافة محتوى جديد أو حذف المحتوى الموجود.
- **الملف، الذي تحاول عزله، كبير للغاية** – يتعين عليك تقليل حجم الملف.

عندما تتلقى رسالة خطأ "فشل العزل"، انقر فوق **مزيد من المعلومات**. تظهر نافذة قائمة أخطاء العزل وسترى اسم الملف والسبب، لماذا لا يمكن عزل الملف.

إرسال عينة للتحليل

إذا وجدت ملفاً مريباً على جهاز الكمبيوتر لديك أو موقع مريب على الإنترنت، فيمكنك إرساله إلى معمل أبحاث ESET للتحليل (قد لا يكون متوفراً على حسب تكوين ESET LiveGrid® لديك).

قبل إرسال النماذج إلى ESET

لا تقم بإرسال أي نموذج ما لم يستوفي واحداً على الأقل من المعايير التالية:

- لا يتم اكتشاف النموذج من خلال منتج ESET الخاص بك على الإطلاق
- تم اكتشاف النموذج بشكل خاطئ كتهديد
- لا نقبل ملفاتك الشخصية (التي لا تريد فحصها بحثاً عن البرامج الضارة بواسطةESET) كنماذج (لا يقوم مختبر الأبحاث التابع لشركة ESET بإجراء عمليات الفحص بالطلب للمستخدمين)
- استخدم موضوعاً وصفياً، وقم بتضمين أكبر قدر ممكن من المعلومات حول الملف (لقطة شاشة أو موقع الويب الذي قمت بتنزيل هذا الملف منه مثلاً)

يمكنك إرسال نموذج ما (ملف ما أو موقع ويب) إلى ESET لتحليله باستخدام أحد الأساليب التالية:

1. استخدم إرسال استمارة نموذج في منتجك. توجد في **الأدوات** > **إرسال عينة للتحليل**. الحد الأقصى لحجم العينة المرسلة هو 256 ميجابايت.
2. وبدلاً من ذلك، يمكنك إرسال الملف بالبريد الإلكتروني. إذا كنت تفضل هذا الخيار، فقم بضغط الملف/الملفات باستخدام WinRAR/WinZIP واحمِ الأرشيف بكلمة المرور "infected" وأرسله إلى samples@eset.com.
3. للإبلاغ عن وجود بريد عشوائي أو نتائج إيجابية خاطئة للبريد العشوائي أو مواقع ويب مصنفة بطريقة خاطئة من خلال وحدة المراقبة الأبوية، يُرجى الرجوع إلى مقالة قاعدة معارف ESET لدينا.

في الاستمارة **تحديد عينة للتحليل** وحدد الوصف من القائمة المنسدلة **سبب إرسال العينة** التي تتلاءم بأفضل شكل مع الغرض من رسالتك:

- ملف مريب
- موقع مريب (موقع ويب مصاب بأي برامج ضارة)
- موقع نتيجة إيجابية خاطئة
- ملف نتيجة إيجابية خاطئة (ملف مكتشف كإصابة، لكنه ليس مصاباً)،
- غير ذلك

الملف/الموقع – المسار إلى الملف أو موقع ويب الذي تعتزم إرساله.

البريد الإلكتروني لجهة الاتصال – يتم إرسال البريد الإلكتروني لجهة الاتصال هذا مع الملفات المريبة إلى ESET ويجوز استخدامه للاتصال بك في حالة وجود معلومات أخرى مطلوبة للتحليل. يعد إدخال بريد إلكتروني لجهة الاتصال اختيارياً. حدد **الإرسال بصفة مجهولة** لتركها فارغة.

قد لا تحصل على سبب من ESET

لن تتلقى رداً من ESET ما لم توجد معلومات أخرى مطلوبة. تتلقى كل يوم عشرات الآلاف من الملفات، ما يجعل من غير الممكن الرد على جميع المواد المرسلة.

إذا تبين أن العينة هي تطبيق أو موقع ويب ضار، فستتم إضافة اكتشافه إلى تحديث ESET تالٍ.

إرسال عينة للتحليل ـ ملف مريب

العلامات والأعراض الملحوظة من الإصابة بالبرامج الضارة ـ أدخل وصفاً لسلوك الملف المريب الملحوظ على الكمبيوتر الخاص بك.

أصل الملف (عنوان URL أو المورِّد) – الرجاء إدخال أصل الملف (مصدره) وكيفية مصادفتك لهذا الملف.

ملاحظات ومعلومات إضافية ـ يمكنك هنا إضافة معلومات إضافية أو أوصاف ستساعد أثناء معالجة الملف المريب.

> المعلمة الأولى – **العلامات والأعراض الملحوظة من الإصابة بالبرامج الضارة** – مطلوبة، لكن سيساعد توفير معلومات إضافية مختبراتنا في عملية تحديد العينات بشكل كبير ومعالجتها.

إرسال عينة للتحليل ـ موقع مريب

الرجاء تحديد أحد ما يلي من القائمة المنسدلة **ما الخطأ في الموقع**:

- **مصاب** ـ موقع ويب يحتوي على فيروسات أو برامج ضارة أخرى يتم توزيعها بطرق مختلفة.
- **تصيد احتيالي** ـ يتم عادة إدراجها للحصول على وصول إلى بيانات حساسة كأرقام حسابات مصرفية وأرقام PIN وغيرها. اقرأ المزيد حول هذا النوع من الهجمات في المسرد.
- **مخادع** ـ موقع ويب مخادع أو احتيالي، وبخاصة لتحقيق ربح سريع.
- حدد **غير ذلك** إذا كانت الخيارات أعلاه لا تشير إلى الموقع الذي سترسله.

ملاحظات ومعلومات إضافية ـ يمكنك كتابة معلومات إضافية أو وصف يساعد في تحليل موقع الويب المشبوه.

إرسال عينة للتحليل ـ ملف نتيجة إيجابية خاطئة

نطلب منك إرسال الملفات المكتشفة كملفات مصابة، لكنها ليست مصابة لتحسين محرك الحماية ضد الفيروسات وبرامج التجسس، ومساعدة الآخرين في التمتع بالحماية. قد تحدث النتائج الإيجابية الخاطئة (FP) عندما يطابق نمط ملف النمط نفسه الموجود في محرك الكشف.

اسم التطبيق وإصداره ـ عنوان البرنامج وإصداره (رقمه أو اسمه المستعار أو اسم تعليمته البرمجية مثلاً).

أصل الملف (عنوان URL أو المورِّد) ـ الرجاء إدخال أصل ملف (مصدره) وكيفية مصادفتك لهذا الملف.

هدف التطبيق ـ الوصف العام للتطبيق، ونوع تطبيق (مستعرض أم مشغل وسائط مثلاً) ووظيفته.

ملاحظات ومعلومات إضافية ـ يمكنك هنا إضافة معلومات إضافية أو أوصاف ستساعد أثناء معالجة الملف المريب.

> المعلمات الثلاثة الأولى مطلوبة لتحديد التطبيقات القانونية، وتمييزها عن التعليمة البرمجية الضارة. عبر تقديم معلومات إضافية، ستساعد مختبراتنا بدرجة ملحوظة في التعرف على العينات ومعالجتها.

إرسال عينة للتحليل ـ موقع نتيجة إيجابية خاطئة

نطلب منك إرسال مواقع مكتشفة كمصابة أو مخادعة أو تنطوي على تصيد احتيالي، ولكنها ليست كذلك. قد تحدث النتائج الإيجابية الخاطئة (FP) عندما يطابق نمط ملف النمط نفسه الموجود في محرك الكشف. الرجاء توفير موقع ويب هذا لتحسين محرك الحماية ضد الفيروسات والحماية ضد التصيد الاحتيالي، ومساعدة الآخرين على التمتع بالحماية.

ملاحظات ومعلومات إضافية ـ يمكنك هنا إضافة معلومات إضافية أو أوصاف ستساعد أثناء معالجة الملف المريب.

إرسال عينة للتحليل ـ أخرى

استخدم هذا النموذج، إذا لم يمكن تصنيف الملف على أنه **ملف مريب** أو **نتيجة إيجابية خاطئة**.

سبب إرسال الملف ـ الرجاء إدخال وصف تفصيلي يتضمن سبب إرسال الملف.

إعداد

يمكنك العثور على مجموعات من ميزات الحماية المتاحة في نافذة البرنامج الرئيسية > **الإعداد**.

تنقسم قائمة **الإعداد** إلى المجموعات التالية:

حماية جهاز الكمبيوتر

حماية الإنترنت

حماية الشبكة

أدوات الأمان

توجد خيارات إضافية أسفل نافذة الإعداد. استخدم رابط الإعداد المتقدم لتكوين مزيد من المعلمات التفصيلية لكل وحدة. استخدم استيراد/تصدير الإعدادات لتحميل معاملات الإعداد باستخدام ملف التكوين.xml أو احفظ معاملات الإعداد الحالية الخاصة بك إلى ملف تكوين.

حماية الكمبيوتر

انقر فوق **حماية جهاز الكمبيوتر** في نافذة البرنامج الرئيسية > **الإعداد** لمراجعة نظرة عامة حول جميع وحدات الحماية:

- حماية نظام الملفات الحالي – يتم فحص جميع الملفات بحثاً عن تعليمات برمجية ضارة أثناء فتحها أو إنشائها أو تشغيلها على الكمبيوتر.
- التحكم في الجهاز – تسمح لك هذه الوحدة بفحص عولمل تصفية/أذونات ممتدة أو حظرها أو ضبطها وتحديد طريقة وصول المستخدم لجهاز معين واستخدامه (قرص مضغوط/قرص DVD/جهاز USB).
- نظام منع اختراق المضيف (HIPS) – يراقب نظام نظام منع اختراق المضيف الأحداث التي تجري في نظام التشغيل ويتفاعل معها وفقاً لمجموعة قواعد مخصصة.
- وضع الألعاب – تمكين أو تعطيل وضع الألعاب. ستحصل على رسالة تحذير (خطر أمني محتمل) وستتحول نافذة البرنامج الرئيسية إلىاللون البرتقالي بعد تمكين وضع الألعاب.
- حماية كاميرا الويب—تتحكم في العمليات والتطبيقات التي يمكنها الوصول إلى كاميرا الويب لديك على.

لإيقاف وحدات الحماية الفردية بشكل مؤقت أو تعطيلها، انقر فوق أيقونة التبديل .

قد يؤدي إيقاف تشغيل وحدات الحماية إلى تقليل مستوى الحماية لجهاز الكمبيوتر الخاص بك.

انقر فوق أيقونة الترس المجاورة لوحدة حماية للوصول إلى الإعدادات المتقدمة لهذه الوحدة.

للحصول على **حماية نظام الملفات الحالي**، انقر فوق رمز الترس واختر من الخيارات التالية:

- **تهيئة** – لفتح الإعداد المتقدم لـ "حماية نظام الملفات الحالي".
- **تحرير الاستثناءات** – لفتح نافذة إعداد الاستثناء بحيث يمكنك استثناء ملفات ومجلدات من الفحص.

للحصول على **حماية الكاميرا**، انقر فوق رمز الترس واختر من الخيارات التالية:

- **تهيئة** – لفتح الإعداد المتقدم لـ "حماية الكاميرا".
- **حظر جميع محاولات الدخول لحين إعادة التشغيل** – لحظر كل محاولات الدخول لكاميرا الويب لحين إعادة تشغيل

جهاز الكمبيوتر.

- **حظر جميع محاولات الوصول بشكل دائم** ـ لحظر جميع محاولات الوصول إلى كاميرا ويب لحين تعطيل هذا الإعداد.
- **إيقاف حظر جميع محاولات الوصول** ـ لتعطيل القدرة على حظر الوصول إلى كاميرا الويب. لا يتوفر هذا الخيار إلا في حالة حظر الوصول إلى كاميرا الويب.

إيقاف الحماية من الفيروسات ومكافحة التجسس مؤقتاً – لتعطيل كل وحدات الحماية ضد الفيروسات وبرامج التجسس. عند تعطيل الحماية، ستفتح نافذة لتحديد مدة تعطيل الحماية باستخدام القائمة المنسدلة **الفاصل الزمني**. لا تستخدمه إلا إذا كنت مستخدماً ذي خبرة أو تم إرشادك بواسطة الدعم الفني من ESET.

تم اكتشاف حالة تسلل

يمكن أن تصل حالات التسلل إلى النظام من مختلف نقاط الدخول كـ صفحات ويب، أو مجلدات المشاركة، أو عبر البريد الإلكتروني، أو من الأجهزة القابلة للإزالة (USB والأقراص الخارجية والأقراص المضغوطة وأقراص DVD وغيرها).

السلوك المعتاد

كمثال عام على كيفية تعامل ESET Internet Security مع حالات التسلل، يمكن اكتشاف حالات التسلل باستخدام:

- الحماية في الوقت الفعلي لنظام الملفات
- حماية الوصول إلى الويب
- حماية عميل البريد الإلكتروني

- فحص الكمبيوتر عند الطلب

وتستخدم كل منها مستوى التنظيف العادي وستحاول تنظيف الملف ونقله إلى العزل أو إنهاء الاتصال. يتم عرض نافذة إعلام في منطقة الإعلامات بالركن السفلي الأيمن من الشاشة. للحصول على معلومات تفصيلية حول الكائنات التي تم اكتشافها/تنظيفها، راجع ملفات السجل. لمزيد من المعلومات حول مستويات وسلوك التنظيف، راجع مستوى التنظيف.

فحص جهاز الكمبيوتر بحثاً عن ملفات مصابة

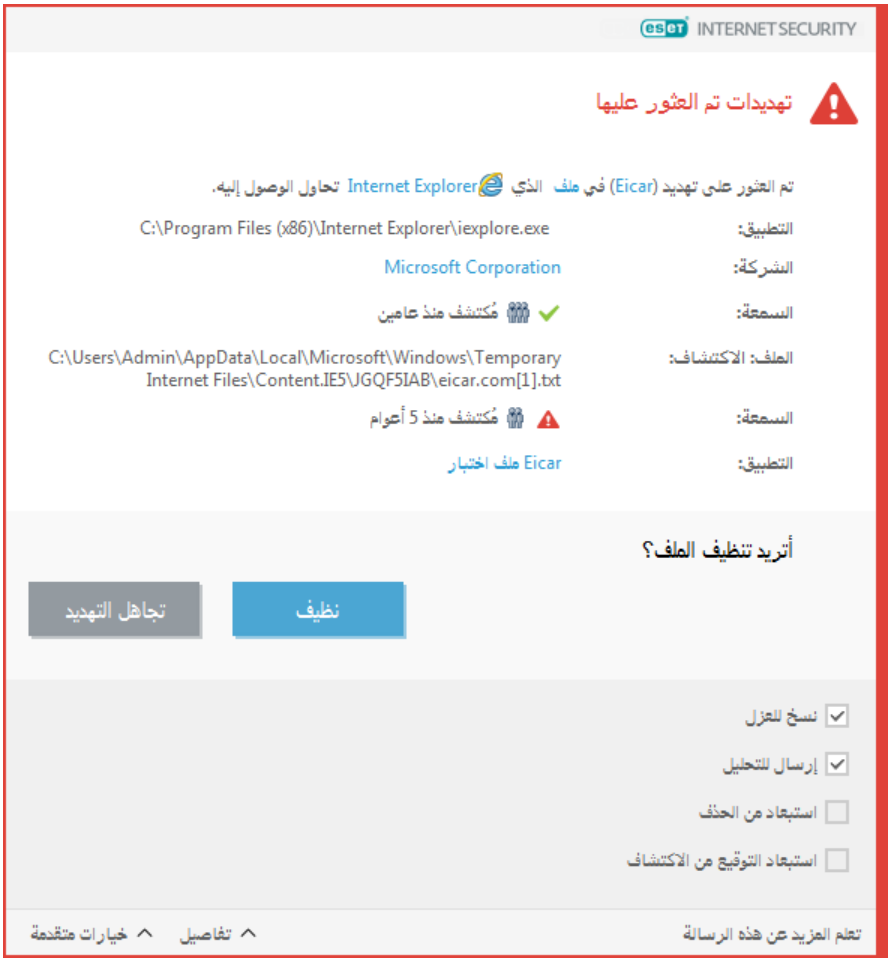
إذا كانت تظهر على الكمبيوتر علامات إصابة ببرامج ضارة، كبطء أدائه أو عدم استجابته باستمرار، فيوصى بالقيام بما يلي:

1. افتح ESET Internet Security وانقر فوق **فحص جهاز الكمبيوتر**.
2. انقر فوق **فحص الكمبيوتر** (لمزيد من المعلومات، راجع فحص الكمبيوتر)
3. بعد انتهاء الفحص، راجع السجل لمعرفة عدد الملفات التي شملها الفحص والمصابة والتي تم تنظيفها.

إذا كنت تريد فحص جزء معين من القرص فقط، فانقر فوق **فحص مخصص** وحدد أهدافاً يتم فحصها بحثاً عن فيروسات.

التنظيف والحذف

إذا لم يوجد إجراء محدد مسبقاً يُتخذ لحماية نظام الملفات في الوقت الفعلي، فستتم مطالبتك بتحديد خيار في نافذة التنبيه. تتوفر عادة الإجراءات: **تنظيف** و**وحذف** و**بدون إجراء**. يوصى بعد تحديد **بدون إجراء**، لأنه سيترك الملفات المصابة دون تنظيف. ويُستثنى من ذلك عندما تكون متأكداً من أن الملف ليس به ضرر وتم اكتشافه بطريق الخطأ.



قم بتطبيق التنظيف في حالة مهاجمة ملف بواسطة فيروس أرفق تعليمة برمجية ضارة بالملف. إذا كان الأمر كذلك، فحاول أولاً تنظيف الملف المصاب لاستعادته إلى حالته الأصلية. إذا كان الملف يحتوي على تعليمة برمجية ضارة فقط، فسيتم حذفه.

إذا كان ملف مصاب "مؤمناً" أو مستخدماً بواسطة عملية نظام، فلن يتم حذفه عادة إلا بعد تحريره (بعد إعادة تشغيل النظام عادة).

الاستعادة من العزل

يمكن الوصول إلى العزل من نافذة البرنامج الرئيسية الخاصة بـ ESET Internet Security من خلال النقر فوق **الأدوات** > **العزل**.

يمكن أيضاً استعادة الملفات المعزولة إلى موقعها الأصلي:

- استخدم ميزة **الاستعادة** لهذا الغرض، والتي تتوفر من القائمة السياقية من خلال الضغط بزر الماوس الأيمن فوق ملف محدد في العزل.
- إذا تم وضع علامة على ملف كـ تطبيق يحتمل كونه غير مرغوب، يتم تمكين خيار **استعادة واستثناء من الفحص**. راجع أيضاً الاستثناءات.
- تعرض القائمة السياقية أيضاً خيار **استعادة إلى**، مما يسمح لك باستعادة ملف إلى موقع آخر غير الذي تم حذفه منه.
- لا تتوفر وظيفة الاستعادة في بعض الحالات، على سبيل المثال، للملفات الموجودة على مشاركة شبكة للقراءة فقط.

تهديدات متعددة

إذا لم يتم تنظيف أي ملفات مصابة أثناء فحص الكمبيوتر (أو تم تعيين مستوى التنظيف إلى **دون تنظيف**)، يتم عرض نافذة تنبيه تطالبك بتحديد إجراءات لتلك الملفات. حدد إجراءات للملفات (يتم تعيين الإجراءات كل على حدة لكل ملف بالقائمة) ثم انقر فوق **إنهاء**.

حذف ملفات في الأرشيفات

في وضع التنظيف الافتراضي، سيتم حذف الأرشيف بالكامل فقط إذا كان يحتوي على ملفات مصابة ولا يحتوي على ملفات نظيفة. وبمعنى آخر، لا يتم حذف الأرشيفات إذا كانت تحتوي أيضاً على أي ملفات نظيفة وغير ضارة. توخَّ الحذر عند إجراء فحص تنظيف صارم، فمع تمكين تنظيف صارم، سيتم حذف الأرشيف إذا كان يحتوي على ملف واحد مصاب على الأقل، بصرف النظر عن حالة الملفات الأخرى التي يشملها الأرشيف.

حماية الإنترنت

الاتصال بالإنترنت هو ميزة عادية بالكمبيوتر الشخصي. ولكنه أصبح ـ للأسف ـ الوسيلة الرئيسية لنقل التعليمات البرمجية الضارة. افتح نافذة البرنامج الرئيسية > **الإعداد** > **حماية الإنترنت** لتكوين الميزات في ESET Internet Security التي تزيد من حماية الإنترنت لديك.

لإيقاف وحدات الحماية الفردية بشكل مؤقت أو تعطيلها، انقر فوق أيقونة التبديل .

قد يؤدي إيقاف تشغيل وحدات الحماية إلى تقليل مستوى الحماية لجهاز الكمبيوتر الخاص بك.

انقر فوق أيقونة الترس ⚙ المجاورة لوحدة حماية للوصول إلى الإعدادات المتقدمة لهذه الوحدة.

تحمي وحدة الرقابة الأبوية أطفالك عن طريق حظر المحتوى غير الملائم أو الضار على الإنترنت.

تقومحماية الوصول إلى الويب بفحص اتصال HTTP/HTTPS بحثاً عن البرامج الضارة وبرامج التصيد الاحتيالي. يجب إيقاف تشغيل حماية الوصول إلى الويب فقط لاستكشاف الأخطاء وإصلاحها.

الحماية ضد التصيد الاحتيالي يتيح لك حظر صفحات الويب المعروف عنها نشر المحتوى الضار. يوصى بشدة ترك حماية مضادة للتصيد الاحتيالي ممكّنة.

الإبلاغ عن موقع تصيد– أبلغ ESET عن موقع ويب للتصيد الاحتيالي أو موقع ويب ضار للتحليل.

> قبل إرسال موقع ويب إلى ESET تأكد من وفائه بمعيار أو أكثر مما يلي:
> • لم يسبق اكتشاف موقع ويب إطلاقاً،
> • تم اكتشاف موقع الويب بشكل خاطئ كتهديد. في هذه الحالة، يمكنك الإبلاغ عن صفحة محظورة بشكلٍ غير صحيح عبر الرابط التالي: Report an incorrectly blocked page.

توفر حماية برامج البريد الإلكتروني التحكم في اتصالات البريد الإلكتروني المستلَمة من خلال بروتوكولي POP3(S) وIMAP(S).
باستخدام برنامج المكون الإضافي لعميل البريد الإلكتروني، يوفر ESET Internet Security تحكماً في جميع الاتصالات الواردة من / إلى عميل البريد الإلكتروني.

يقوم برنامجمكافحة البريد العشوائي لعميل البريد الإلكتروني بتصفية رسائل البريد الإلكتروني غير المرغوب فيها.

للحصول على **مكافحة البريد العشوائي لعميل البريد الإلكتروني**، انقر فوق أيقونة الترس ⚙ واختر من الخيارات التالية:

- يفتح**التكوين**—الإعدادات المتقدمة لمكافحة البريد العشوائي لعميل البريد الإلكتروني.
- **قائمة عناوين المستخدم** (إذا تم تمكينه) — فسيفتح نافذة حوار حيث يمكنك إضافة العناوين أو تحريرها أو حذفها لتحديد قواعد مكافحة البريد العشوائي. سيتم تطبيق القواعد في هذه القائمة على المستخدم الحالي.
- **قائمة العناوين العامة** (إذا تم تمكينه) — فسيفتح نافذة حوار حيث يمكنك إضافة العناوين أو تحريرها أو حذفها لتحديد قواعد مكافحة البريد العشوائي. سيتم تطبيق القواعد في هذه القائمة على جميع المستخدمين.

حماية مضادة للتصيد الاحتيالي

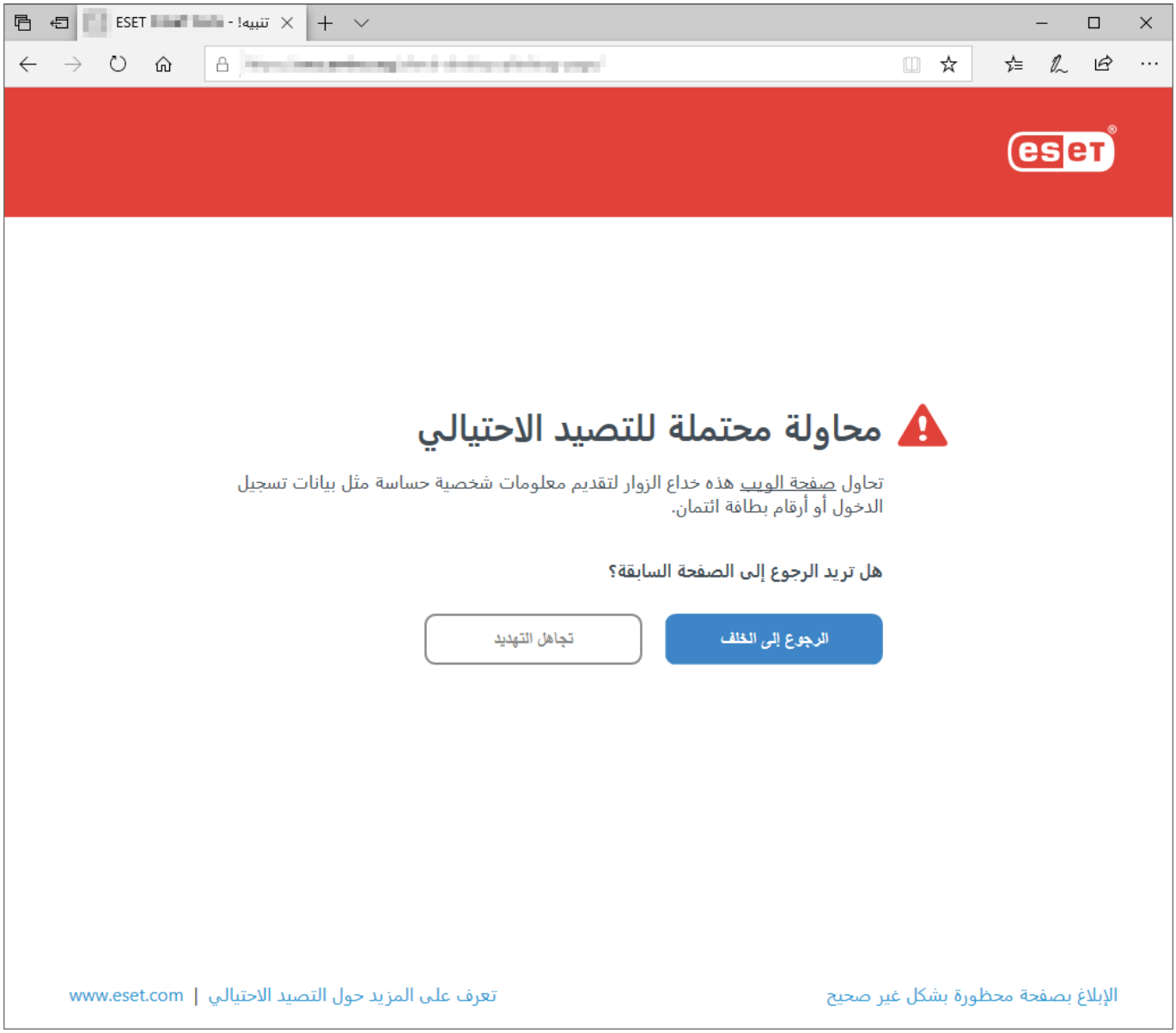
التصيد الاحتيالي هو نشاط إجرامي يستخدم الهندسة الاجتماعية (التلاعب بالمستخدمين للحصول على معلومات سرية منهم). يُستخدم التصيد الاحتيالي للوصول إلى بيانات حساسة كأرقام حسابات مصرفية وأرقام PIN وغيرها. لمزيد من المعلومات، راجع، المسرد. يشتمل ESET Internet Security على حماية مضاد التصيد، وهي تحظر صفحات الويب المعروفة بتوزيع هذا النوع من المحتوى.

يتم تمكين حماية مضاد التصيد افتراضياً. يمكن تكوين هذا الإعداد في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الويب**.

تفضل بزيارة مقالة قاعدة المعارف للاطلاع على المزيد من المعلومات عن الحماية ضد التصيد الاحتيالي في ESET Internet Security.

الوصول إلى موقع ويب تصيد احتيالي

عند الوصول إلى موقع ويب معروف بالتصيد الاحتيالي، سيعرض مستعرض الويب لديك مربع الحوار التالي. إذا كنت ما زلت ترغب في الوصول إلى موقع الويب، فانقر فوق **تجاهل التهديد** (غير مستحسن).



ستنتهي صلاحية مواقع ويب التي تتضمن تصيداً احتيالياً محتملاً المضمنة بقوائم سماح بعد عدة ساعات افتراضياً. وللسماح لموقع ويب بشكل دائم، استخدم أداة إدارة عناوين URL. من إعداد متقدم > **وسائل الحماية** > **حماية الوصول إلى الويب** > **إدارة عنوان URL** > **قائمة العناوين** > **تحرير**إضافة موقع الويب الذي تريد تحريره إلى القائمة.

الإبلاغ بموقع يقوم بالتصيد الاحتيالي

يتيح لك رابط **الإبلاغ عن صفحة محظورة بشكل غير صحيح** الإبلاغ عن موقع ويب تم اكتشافه بشكل غير صحيح كتهديد.

وبدلاً من ذلك، يمكنك إرسال موقع ويب بالبريد الإلكتروني. أرسل رسالة البريد الإلكتروني الخاصة بك إلى samples@eset.com. تذكر استخدام موضوع وصفي، وتضمين أكثر قدر ممكن من المعلومات حول موقع ويب (على سبيل المثال، موقع الويب الذي أحالك إليه وكيف سمعت عنه، إلخ).

المراقبة الأبوية

تتيح لك الوحدة النمطية للمراقبة الأبوية تكوين إعدادات المراقبة الأبوية التي توفر للأبوين أداة تلقائية تساعد في حماية الأبناء وتعيين قيود على الأجهزة والخدمات. وهي تهدف إلى منع الأطفال والمراهقين من الوصول إلى الصفحات ذات المحتوى الضار أو غير المناسب.

تتيح لك الرقابة الأبوية حظر صفحات ويب يمكن أن تحتوي على مواد قد تكون مسيئة. بالإضافة إلى ذلك، يمكن لأولياء الأمور منع الوصول إلى أكثر من 40 فئة موقع محددة مسبقاً وأكثر من 140 فئة فرعية.

لتنشيط المراقبة الأبوية لحساب مستخدم محدد، اتبع الخطوات أدناه:

1. بشكلٍ افتراضي، يتم تعطيل ميزة المراقبة الأبوية في ESET Internet Security. توجد طريقتان لتنشيط ميزة المراقبة الأبوية:

- انقر فوق أيقونة التبديل في القسم **إعداد** > **حماية الإنترنت** > **الرقابة الأبوية** من نافذة البرنامج الرئيسية وقم بتغيير حالة الرقابة الأبوية إلى ممكَّنة.
- افتح الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الويب** > **الرقابة الأبوية** ثم قم بتمكين التبديل بجوار **تمكين الرقابة الأبوية**.

2. انقر فوق **إعداد** > **حماية الإنترنت** > **المراقبة الأبوية** من نافذة البرنامج الرئيسية. على الرغم من ظهور الحالة **ممكَّنة** بجوار **المراقبة الأبوية**، يجب تكوين ميزة المراقبة الأبوية للحساب المطلوب من خلال النقر فوق رمز أحد الصفوف ثم في النافذة التالية حدد**حماية حساب الأطفال** أو **حساب ولي الأمر**. في النافذة التالية حدد تاريخ الميلاد لتحديد مستوى الوصول وصفحات الويب المناسبة لذلك العمر والموصى بها. سيتم الآن تمكين المراقبة الأبوية لحساب المستخدم المحدد. انقر فوق **المحتوى الممنوع والإعدادات** الموجود ضمن اسم حساب لتخصيص الفئات التي تريد السماح بها أو حظرها في علامة التبويب الفئات. للسماح بصفحات ويب مخصصة أو حظرها، مع مراعاة ألا تكون هذه الصفحات مطابقة لأي فئة، انقر فوق علامة التبويب الاستثناءات.

إذا نقرت فوق **إعداد** > **حماية الإنترنت** > **المراقبة الأبوية** من نافذة منتج ESET Internet Security الأساسية، فستشاهد أن النافذة الرئيسية تحتوي على:

حسابات مستخدمي Windows

إذا أنشأت دور لحساب موجود، فسيظهر هنا. انقر فوق مربع التمرير بحيث تظهر علامة الاختيار الخضراء المجاورة للمراقبة الأبوية للحساب. تحت تنشيط الحساب، انقر فوق المحتوى المحظور والإعدادات... للاطلاع على قائمة فئات صفحات الويب المسموح بها لهذا الحساب وصفحات الويب المحظورة والمسموح بها.

يحتوي الجزء السفلي من نافذة على

إضافة استثناء لموقع ويب – يمكن السماح بمواقع ويب معينة أو حظرها وفقاً لتفضيلات كل حساب أبوي على حدة.

عرض السجلات – يوضح سجلاً مفصلاً لنشاط المراقبة الأبوية (الصفحات المحظورة والحساب والصفحة المحظورة والفئة وما إلى ذلك). يمكنك تصفية هذا السجل وفقاً لمعايير من اختيارك بالنقر فوق **تصفية**.

المراقبة الأبوية

بعد تعطيل المراقبة الأبوية، ستظهر النافذة **تعطيل المراقبة الأبوية**. يمكنك من هنا ضبط الفاصل الزمني الذي يتم تعطيل الحماية له. يتغير الخيار بعد ذلك إلى **متوقف مؤقتاً** أو **معطل دائماً**.

ينبغي حماية الإعدادات في ESET Internet Security بكلمة مرور. يمكن تعيين كلمة المرور في القسم إعداد الوصول. في حالة

عدم تعيين كلمة مرور، سيظهر التحذير التالي – **حماية جميع الإعدادات بكلمة مرور** لمنع التغييرات غير المصرح بها. تؤثر القيود التي تم تعيينها في المراقبة الأبوية فقط على حسابات المستخدمين القياسية. ونظراً لأن المسؤول بإمكانه تجاوز أي قيود، فلن يكون لها أي تأثير.

> تتطلب الرقابة الأبوية تمكين أداة فحص حركة مرور الشبكة وفحص حركة مرور HTTP(S) وجدار الحماية للعمل بشكل صحيح. يتم تمكين هذه الوظائف افتراضياً.

استثناءات موقع الويب

لإضافة استثناء لموقع ويب، انقر فوق **إعداد** > **حماية الإنترنت** > **Parental control** ثم انقر فوق **إضافة استثناء لموقع ويب**.

أدخل عنوان URL في حقل **عنوان URL لموقع الويب**، وحدد ✔ (مسموح) أو ⊘ (محظور) لكل حساب مستخدم معين ثم انقر فوق **موافق** لإضافته إلى القائمة.

لحذف عنوان URL من القائمة، انقر فوق **إعداد** > **حماية الإنترنت** > **Parental control** > وانقر فوق **المحتوى المحظور والإعدادات** ضمن حساب المستخدم المرغوب، انقر فوق علامة التبويب **الاستثناء** وحدد الاستثناء وانقر فوق **إزالة**.

ولا يمكن ـ في قائمة عناوين URL - استخدام الرموز الخاصة مثل * (النجمة) و ? (علامة الاستفهام). على سبيل المثال، يجب إدخال عناوين صفحات ويب مع مجالات مستوى أعلى (TLD) متعددة يدوياً (*examplepage.com* و*examplepage.sk* وغيرهما.). عند إضافة مجال إلى القائمة، سيتم حظر جميع المحتويات الموجودة على هذا المجال وجميع المجالات الفرعية (مثل *sub.examplepage.com*) أو السماح بها حسب اختيارك للإجراء على أساس عنوان URL.

يمكن أن يكون حظر صفحة ويب معينة أو السماح بها أكثر دقة من حظر فئة مواقع ويب أو السماح بها. توخَّ الحذر عند تغيير هذه الإعدادات وإضافة فئة/صفحة ويب إلى القائمة.

نسخ الاستثناء من المستخدم

حدد مستخدماً من القائمة المنسدلة التي تريد نسخ الاستثناء الذي تم إنشاؤه منها.

نسخ الفئات من الحساب

يتيح لك هذا الإعداد إمكانية نسخ قائمة بالفئات المسموح بها أو المحظورة من حساب معدّل موجود.

حماية الشبكة

افتح نافذة البرنامج الرئيسية > **الإعداد** > **حماية الشبكة** لتكوين إعدادات حماية الشبكة الأساسية أو استكشاف أخطاء اتصال الشبكة وإصلاحها.

لإيقاف وحدات الحماية الفردية بشكل مؤقت أو تعطيلها، انقر فوق أيقونة التبديل .

قد يؤدي إيقاف تشغيل وحدات الحماية إلى تقليل مستوى الحماية لجهاز الكمبيوتر الخاص بك.

انقر فوق أيقونة الترس ⚙ المجاورة لوحدة حماية للوصول إلى الإعدادات المتقدمة لهذه الوحدة.

يقوم **جدار الحماية**—بتصفية جميع اتصالات الشبكة بناءً على التكوين ESET Internet Security.

يفتح **تكوين**—الإعداد المتقدم لجدار الحماية حيث يمكنك تحديد كيفية تعامل جدار الحماية مع اتصال الشبكة.

إيقاف جدار الحماية مؤقتاً (السماح لجميع حركات المرور)—يتم إيقاف تشغيل جميع خيارات تصفية جدار الحماية ويتم السماح بالاتصالات الواردة والصادرة. انقر فوق **تمكين جدار الحماية**من أجل إعادة تمكين جدار الحماية عندما تكون تصفية حركة مرور الشبكة في هذا الوضع.

حظر جميع عمليات نقل البيانات ـ سيتم حظر جميع الاتصالات الواردة والصادرة بواسطة جدار الحماية. لا تستخدم هذا الخيار إذا كنت تشتبه في وجود خطر أمان حرج يتطلب فصل النظام من الشبكة. عندما تكون تصفية حركة مرور الشبكة في وضع **حظر جميع حركات المرور**، انقر فوق **إيقاف حظر جميع حركات المرور** لاستعادة التشغيل الطبيعي لجدار الحماية.

الوضع التلقائي ـ (عند تمكين وضع تصفية آخر) ـ انقر لتغيير وضع التصفية إلى وضع التصفية التلقائي (بقواعد محددة بواسطة المستخدم).

الوضع التفاعلي ـ (عند تمكين وضع تصفية آخر) ـ انقر لتغيير وضع التصفية إلى وضع التصفية التفاعلي.

الحماية ضد هجمات الشبكة (IDS) ـ تحليل محتوى حركة مرور الشبكة والحماية من هجمات الشبكة. سيتم حظر أي حركة مرور تعتبر ضارة. سيبلغك ESET Internet Security عند الاتصال بشبكة لاسلكية غير محمية أو بشبكة ذات حماية ضعيفة.

الحماية ضد البوت نت – اكتشاف البرامج الضارة في النظام بسرعة ودقة.

تعرض اتصالات الشبكة—الشبكات التي تتصل بها محولات الشبكة بمعلومات مفصلة.

يساعدك **حل الاتصالات المحظورة**—في حل مشكلات التوصيل التي يسببها جدار الحماية من ESET. لمزيد من المعلومات التفصيلية، راجع معالج استكشاف الأخطاء وإصلاحها.

حل عناوين IP المحظورة مؤقتاً – عرض قائمة بعناوين IP التي تم اكتشافها كمصدر للهجمات، وتمت إضافتها إلى قائمة الحظر لحظر الاتصال لفترة زمنية معينة

يفتح **عرض السجلات**—حماية الشبكة ملف السجل.

اتصالات الشبكة

تعرض الشبكات المتصلة بها محولات شبكة. لمشاهدة اتصالات الشبكة، افتح نافذة البرنامج الرئيسية > **الإعداد** > **حماية الشبكة** > **اتصالات الشبكة**.

انقر نقراً مزدوجاً فوق اتصال في القائمة لعرض تفاصيله وتفاصيل محول الشبكة.

مرر مؤشر الماوس فوق اتصال شبكة معين وانقر فوق أيقونة القائمة ⋮ في عمود **موثوق به** لاختيار أحد الخيارات التالية:

- يفتح **تحرير**—نافذة تكوين حماية الشبكة حيث يمكنك تعيين ملف تعريف حماية الشبكة لشبكة معينة
- يُعيد **النسيان**—تعيين تكوين اتصال الشبكة إلى الوضع الافتراضي

- **فحص الشبكة باستخدام مراقب الشبكة** – يفتح مراقب الشبكة لتشغيل فحص الشبكة.
- **وضع علامة على أنها "شبكتي"** يضيف علامة "شبكتي" إلى الشبكة؛ سيتم عرض هذه العلامة بجوار الشبكة عبر ESET Internet Security للحصول على نظرة عامة على التعريف والأمان بشكل أفضل
- **إلغاء وضع علامة على أنها "شبكتي"**—يزيل علامة "شبكتي"؛ متاح فقط إذا تم وضع علامة على الشبكة بالفعل

تفاصيل اتصال الشبكة

انقر نقراً مزدوجاً فوق اتصال في قائمة اتصالات الشبكة لعرض تفاصيلها مع تفاصيل محول الشبكة. يمكن أن تساعدك تفاصيل اتصال الشبكة والمحول في تحديد الشبكة التي تحاول تكوينها في حماية الوصول إلى الشبكة.

تفاصيل اتصال الشبكة:

- حالة اتصال الشبكة
- تاريخ ووقت اكتشاف الشبكة الأول
- آخر مرة كانت فيها الشبكة نشطة
- إجمالي الوقت المستغرق في الاتصال بهذه الشبكة
- ملف تعريف اتصال شبكة
- ملف تعريف اتصال الشبكة المحدد في Windows
- تكوين حماية الشبكة (ما إذا كانت الشبكة موثوقة)

تفاصيل محول الشبكة:

- نوع الاتصال (سلكي، ظاهري، إلخ)
- اسم محول الشبكة
- وصف المحول
- عنوان IP مع عنوان MAC
- عنوان IPv4 و IPv6 للشبكة ذات الشبكة الفرعية
- لاحقة DNS
- عنوان IP لخادم DNS
- عنوان IP لخادم DHCP
- عنوان IP وMAC للبوابة الافتراضية
- عنوان MAC الخاص بالمحول

استكشاف أخطاء الوصول إلى الشبكة وإصلاحها

يساعدك معالج استكشاف الأخطاء وإصلاحها على حل مشكلات التوصيل التي يسببها جدار الحماية من. يمكن العثور على**استكشاف أخطاء الوصول إلى الشبكة وإصلاحها** في نافذة البرنامج الرئيسية > **الإعداد** > **حماية الشبكة** > **حل الاتصالات المحظورة**.

حدد ما إذا كنت تريد إظهار الاتصال المحظور **للتطبيقات المحلية** أو الاتصال المحظور من **الأجهزة البعيدة**.

من القائمة المنسدلة، حدد فترة أثناء حظر الاتصال. يوفر قائمة الاتصالات المحظورة نظرة عامة على نوع التطبيق أو الجهاز والسمعة وإجمالي عدد التطبيقات والأجهزة المحظورة أثناء الفترة الزمنية هذه. لمزيد من التفاصيل حول الاتصال المحظور، انقر فوق **التفاصيل**. تتمثل الخطوة التالية في إلغاء حظر التطبيق أو الجهاز الذي تواجه فيه مشكلات في التوصيل.

عند النقر فوق **إلغاء حظر**، سيتم السماح بالاتصال المحظور مسبقاً. إذا استمررت في مواجهة مشكلات مع أحد التطبيقات، أو أن الجهاز لديك لا يعمل كما هو متوقع، انقر فوق **إنشاء قاعدة أخرى** وسيتم السماح بكل الاتصالات المحظورة مسبقاً لهذا الجهاز. إذا استمرت المشكلة، قم بإعادة تشغيل الكمبيوتر.

انقر فوق **فتح قواعد جدار الحماية** لمشاهدة القواعد التي أنشأها المعالج. بالإضافة إلى ذلك، يمكنك الاطلاع على القواعد المنشأة بواسطة المعالج في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **جدار الحماية** > **القواعد** > **تحرير**.

إذا تعذر إنشاء القاعدة، فستتلقى رسالة خطأ. انقر فوق **المحاولة مرة أخرى** وكرر العملية لإلغاء حظر الاتصال، أو إنشاء قاعدة أخرى من قائمة الاتصالات المحظورة.

قائمة حظر عناوين IP المؤقتة

لعرض عناوين IP التي تم اكتشافها كمصادر للهجمات مضافة إلى القائمة السوداء لحظر الاتصال لفترة زمنية معينة، افتح نافذة البرنامج الرئيسية > **الإعداد** > **حماية الشبكة**> **حل عناوين IP المحظورة مؤقتاً**. يتم حظر قائمة حظر عناوين IP المؤقتة لمدة ساعة واحدة.

الأعمدة

عنوان IP – يعرض عنوان IP التي تم حظره.

سبب الحظر – يعرض نوع الهجمات التي تم منعها من العنوان (مثل هجمة ضد فحص منفذ TCP).

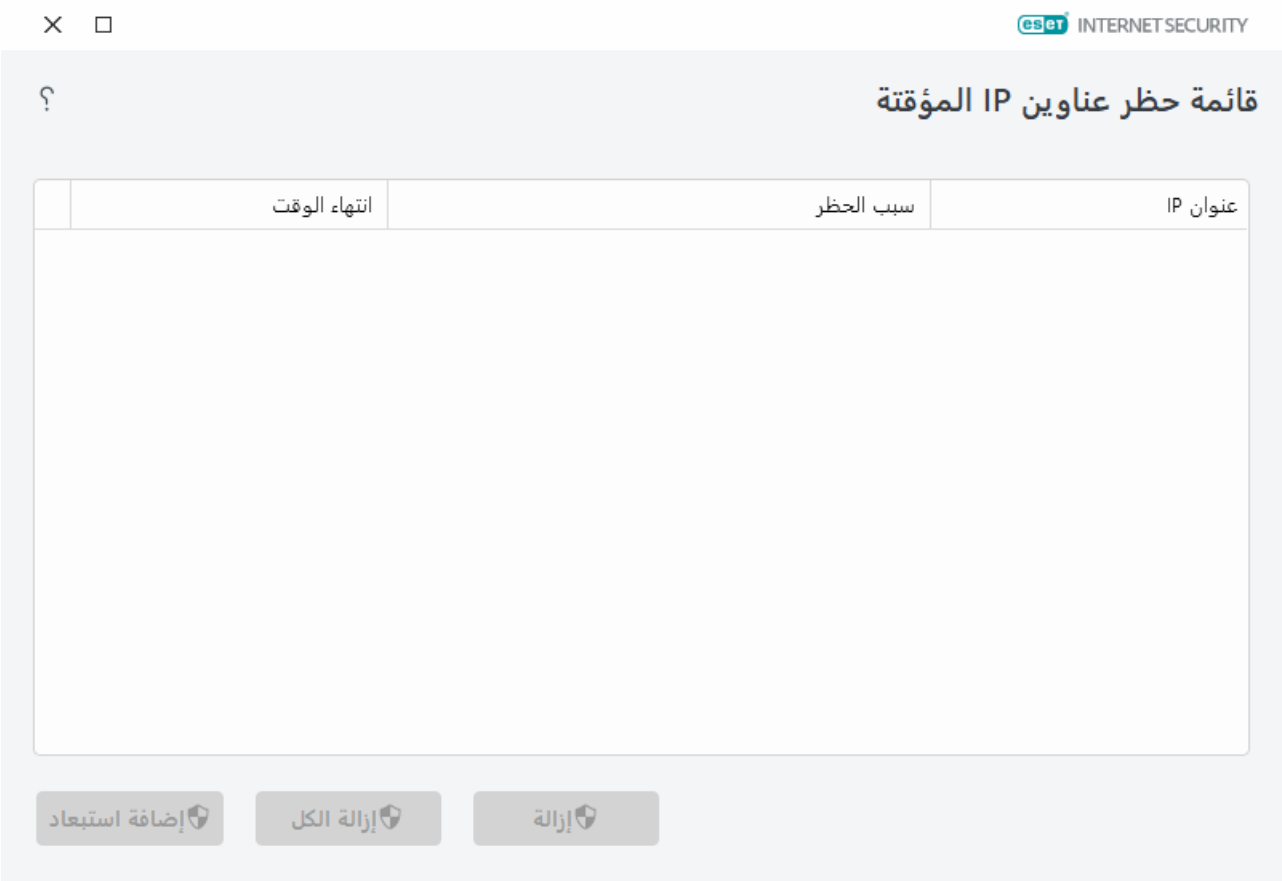
المهلة – تعرض الوقت وتاريخ انتهاء صلاحية العنوان من قائمة الحظر.

عناصر التحكم

إزالة – انقر فوقه لإزالة عنوان من قائمة الحظر قبل انتهاء صلاحيته.

إزالة الكل – انقر فوقه لإزالة جميع العناوين من قائمة الحظر على الفور.

إضافة استبعاد – انقر لإضافة استثناء جدار حماية إلى تصفية نظام كشف التسلل.



سجلات حماية الشبكة

تقوم ESET Internet Security حماية الشبكة بحفظ جميع الأحداث المهمة في ملف السجل. لعرض ملف السجل، افتح نافذة البرنامج الرئيسية > **الإعداد** > **حماية الشبكة** > **إظهار السجلات**.

يمكن استخدام ملفات السجل لاكتشاف أخطاء وكشف حالات اختراق في نظامك. تحتوي سجلات حماية الشبكة من على البيانات التالية:

- تاريخ الحدث ووقته
- اسم الحدث
- المصدر
- عنوان الشبكة الهدف
- بروتوكول الاتصال بالشبكة
- القاعدة المطبقة، أو اسم الفيروس المتنقل، إذا كان معروفاً.
- مسار التطبيق والاسم
- التجزئة
- المستخدم
- الموّقع على التطبيق (الناشر)
- اسم الحزمة
- اسم الخدمة

يمكن أن يساعد التحليل الكامل لهذه البيانات في اكتشاف محاولات اختراق أمان النظام. يشير العديد من العوامل الأخرى إلى مخاطر أمان محتملة، كما يسمح لك بالحد من آثارها: الاتصالات المتكررة من أماكن غير معروفة، أو المحاولات المتعددة لإنشاء اتصالات والتطبيقات غير المعروفة التي تتصل، أو أرقام المنافذ غير المعتادة التي تُستخدم.

> **استغلال الثغرة الأمنية**
> يتم تسجيل رسالة استغلال الثغرة الأمنية حتى إذا تم تصحيحها بالفعل منذ الكشف عن محاولة الاستغلال وحظرها على مستوى الشبكة قبل أن يحدث الاستغلال بالفعل.

حل مشكلات في جدار الحماية من

إذا واجهتك مشكلات متعلقة بالتوصيل في ESET Internet Security مثبت لديك، فلديك عدة طرق لمعرفة ما إذا كان جدار الحماية من هو سبب المشكلة. علاوة على ذلك، يمكن أن يساعدك جدار حماية في إنشاء قواعد أو استثناءات جديدة لحل مشكلات التوصيل.

راجع الموضوعات التالية لمساعدتك على حل المشكلات المتعلقة بجدار الحماية من:

- استكشاف أخطاء الوصول إلى الشبكة وإصلاحها
- التسجيل وإنشاء قواعد أو استثناءات من السجل
- إنشاء استثناءات من إعلامات جدار الحماية
- حماية الشبكة التسجيل المتقدم
- حل المشكلات باستخدام أداة فحص حركة مرور الشبكة

التسجيل وإنشاء قواعد أو استثناءات من السجل

افتراضياً، لا يسجِّل جدار الحماية من ESET جميع الاتصالات المحظورة. إذا كنت تريد الاطلاع على ما كان محظوراً بواسطة حماية الشبكة، فقم بفتح الإعداد المتقدم > **الأدوات** > **تشخيصات** > **التسجيل المتقدم** وتمكين **تمكين التسجيل المتقدم لحماية الشبكة**. وإذا رأيت شيئاً في السجل لم تكن تريد أن يحظره جدار الحماية، فيمكنك إنشاء قاعدة أو قاعدة IDS له بالنقر بزر الماوس الأيمن فوق ذلك العنصر وتحديد **عدم منع الأحداث المشابهة في المستقبل**. الرجاء ملاحظة أن سجل جميع الاتصالات المحظورة يمكن أن يحتوي على آلاف العناصر، وقد يكون من الصعب العثور على اتصال معين في ذلك السجل. يمكنك إيقاف تشغيل التسجيل بعد حل مشكلتك.

لمزيد من المعلومات حول السجل، راجع ملفات السجل.

> استخدم التسجيل لمعرفة ترتيب حظر حماية الشبكة لاتصالات معينة. علاوة على ذلك، يسمح لك إنشاء قواعد من السجل بإنشاء قواعد تعبر عما تريده بالضبط.

إنشاء قاعدة من السجل

يسمح لك الإصدار الجديد من ESET Internet Security بإنشاء قاعدة من السجل. من القائمة الرئيسية، انقر فوق **الأدوات** > **ملفات السجل**. اختر **حماية الشبكة** من القائمة المنسدلة، وانقر بزر الماوس الأيمن فوق إدخال السجل المطلوب وحدد **عدم منع**

الأحداث المشابهة في المستقبل من القائمة السياقية. ستعرض نافذة إعلام قاعدتك الجديدة.

للسماح بإنشاء قواعد جديدة من السجل، يجب تكوين ESET Internet Security بالإعدادات التالية:

1. تعيين أدنى شرح تفصيلي للتسجيل إلى **التشخيص** في إعداد متقدم > **الأدوات** > **ملفات السجل**.
2. قم بتمكين **الإخطار بالهجمات الواردة ضد الثغرات الأمنية** في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **الحماية ضد هجمات الشبكة** > **الخيارات المتقدمة** > **اكتشاف الاختراق**.

إنشاء استثناءات من إعلامات جدار الحماية

عند اكتشاف جدار الحماية من ESET لنشاط ضار على الشبكة، سيتم عرض نافذة إعلام تصف الحدث. ويحتوي هذا الإعلام على ارتباط سيسمح لك بمعرفة المزيد حول الحدث وإعداد قاعدة لهذا الحدث، إذا أردت ذلك.

> إذا لم يقم تطبيق أو جهاز شبكة بتنفيذ معايير الشبكة بشكل صحيح، فيمكنه تشغيل إعلامات نظام كشف التسلل متكررة لجدار الحماية. يمكنك إنشاء استثناء مباشرة من الإعلام لمنع اكتشاف جدار الحماية من ESET لهذا التطبيق أو الجهاز.

حماية الشبكة التسجيل المتقدم

هذه الميزة مصممة لتوفير ملفات سجل أكثر تعقيداً للدعم الفني لESET. لا تستخدم هذه الميزة إلا عند طلب الدعم الفني لESET ذلك منك؛ لأنها قد تنشئ ملف سجل ضخماً ما يبطئ أداء الكمبيوتر.

1. افتح الإعداد المتقدم > **الأدوات** > **التشخيصات** > **التسجيل المتقدم** وقم بتمكين **تمكين التسجيل المتقدم لحماية الشبكة**.
2. حاول إعادة إنشاء المشكلة التي واجهتها.
3. تعطيل التسجيل المتقدم لحماية الشبكة.
4. يمكن العثور على ملف سجل PCAP الذى تم إنشاؤه بواسطة التسجيل المتقدم لحماية الشبكة في الدليل ذاته الذي تم إنشاء تفريغات ذاكرة التشخيصات به: *C:\ProgramData\ESET\ESET Security\Diagnostics*

حل المشكلات باستخدام أداة فحص حركة مرور الشبكة

في حالة مواجهة مشكلات في المستعرض أو البرنامج العميل للبريد الإلكتروني، تعد الخطوة الأولى تحديد ما إذا كانت أداة فحص حركة مرور الشبكة هي السبب. للقيام بذلك، حاول تعطيل أداة فحص حركة مرور الشبكة مؤقتاً في الإعداد المتقدم > **محرك الكشف** > **أداة فحص حركة مرور الشبكة**(تذكر إعادة تشغيلها بعد الانتهاء، وإلا فسيظل المتصفح وعميل البريد الإلكتروني غير محميين). وفي حالة ظهور المشكلة بعد إيقاف تشغيلها، ففيما يلي قائمة بالمشكلات الشائعة وطريقة حلها:

مشكلات التحديث أو الاتصالات الآمنة

في حالة إبلاغ التطبيق بشأن عدم القدرة على التحديث أو من أن قناة الاتصال غير آمنة:

- إذا قمت بتمكين SSL/TLS ، فحاول إيقاف تشغيله مؤقتاً. إذا أفلح ذلك، فيمكنك استمرار استخدام SSL/TLS وجعل التحديث يعمل باستبعاد الاتصالات التي بها مشكلات:

تعطيل SSL/TLS أعد تشغيل التحديث. يجب ظهور مربع حوار يُخبرك بحركة مرور الشبكة المشفرة. تأكد من مطابقة التطبيق للذي تقوم باستكشاف أخطائه وإصلاحها، ومن صدور الشهادة عن الخادم الذي يقوم بالتحديث منه. ثم اختر تذكر الإجراء لهذه الشهادة وانقر فوق "تجاهل". وإذا لم تعد تظهر مربعات حوار أخرى ذات صلة، فيمكنك إعادة تبديل وضع التصفية إلى الوضع التلقائي ويجب أن تُحل المشكلة.

- إذا لم يكن التطبيق المعني مستعرضاً أو عميل بريد إلكتروني، فيمكنك استبعاده تماماً من حماية الوصول إلى الويب (بينما سيجعلك القيام بذلك بالنسبة للمستعرض أو عميل البريد الإلكتروني عُرضة للتهديدات). يجب أن يكون أي تطبيق تمت تصفية اتصاله في الماضي في القائمة الموفرة لك عند إضافة استثناء بالفعل؛ لذا لا يلزم إضافة تطبيق يدوياً.

مشكلة في الوصول إلى جهاز على الشبكة

إذا لم تتمكن من استخدام وظائف أي جهاز على شبكتك (قد يعني ذلك فتح صفحة ويب لكاميرا ويب أو تشغيل الفيديو على مشغل وسائط منزلي)، فحاول إضافة عناوين IPv4 و IPv6 إلى قائمة العناوين المستبعدة.

مشكلات في موقع ويب معين

يمكنك استبعاد مواقع ويب معينة من حماية الوصول إلى الويب باستخدام إدارة عناوين URL. على سبيل المثال، إذا لم تستطع الوصول إلى https://www.gmail.com/intl/en/mail/help/about.html، فجرِّب إضافة *gmail.com* إلى قائمة العناوين المستبعدة.

الخطأ "لا تزال بعض التطبيقات القادرة على استيراد شهادة الجذر قيد التشغيل"

عند تمكين SSL/TLS يتأكد ESET Internet Security أن التطبيقات المثبتة تثق في طريقة تصفية بروتوكول SSL باستيراد شهادة إلى مخزن الشهادات الخاص بها. قد تتطلب بعض التطبيقات إعادة التشغيل لاستيراد شهادة. يشمل ذلك Firefox وOpera. تأكد أن أياً منها ليس قيد التشغيل (أفضل طريقة لذلك من خلال فتح "مدير المهام" والتأكد من عدم وجود firefox.exe أو opera.exe تحت علامة تبويب "العمليات")، ثم أعد المحاولة.

خطأ حول مُصدِر غير موثوق به أو توقيع غير صالح

من المرجح أن يعني ذلك فشل الاستيراد المذكور أعلاه. تأكد أولاً من عدم تشغيل أي من التطبيقات المذكورة. ثم قم بتعطيل SSL/TLS وتمكينه مرة أخرى. حينئذٍ تتم إعادة تشغيل الاستيراد.

راجع مقالة قاعدة المعرفة للتعرف على كيفية إدارة أداة فحص حركة مرور الشبكة في المنتج المنزلي لـESET Windows.

تم حظر تهديد الشبكة

يمكن أن يحدث هذا الموقف عندما يحاول تطبيق جهاز الذي تستخدمه إرسال بيانات ضارة إلى جهاز آخر على الشبكة، باستغلال فجوة أمنية أو حتى اكتشاف محاولة مسح منفذ على جهازك.

يمكنك العثور على نوع التهديد وعنوان IP الخاص بالجهاز ذي الصلة في الإعلام. انقر فوق **تغيير معالجة هذا التهديد** لإظهار

الخيارات التالية:

استمرار الحظر – حظر التهديد المكتشف. إذا كنت ترغب في إيقاف تلقي إشعارات حول هذا النوع من التهديدات من العنوان البعيد المحدد، فحدد زر الخيار بجوار **عدم الإعلام** قبل النقر فوق **متابعة الحظر**. سيؤدي ذلك إلى إنشاء قاعدة خدمة اكتشاف الاختراق (IDS) بالتكوين التالي: **حظر** – الافتراضي، **إعلام** – لا، **سجل** – لا.

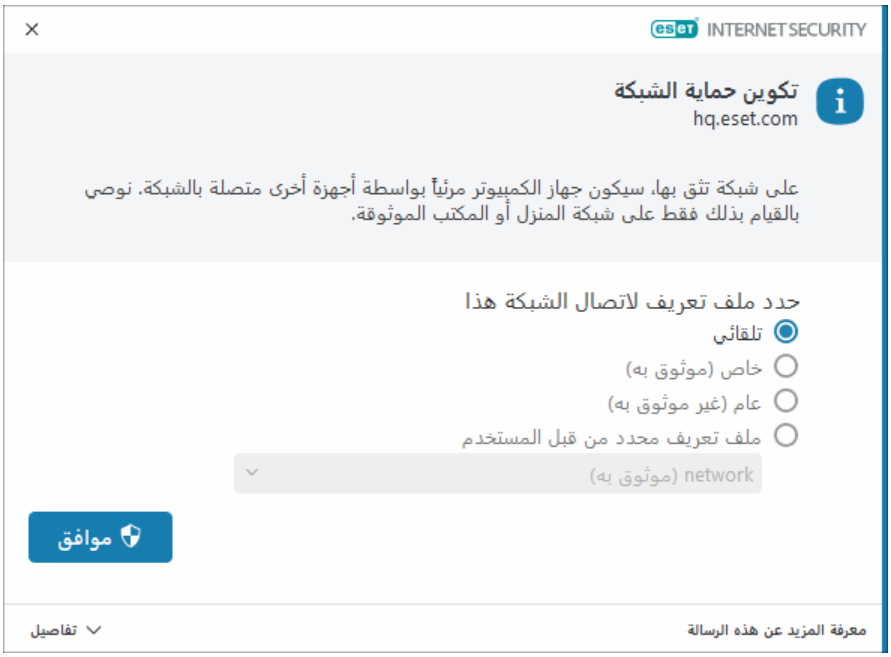
سماح—يقوم بإنشاء قاعدة خدمة اكتشاف الاختراق (IDS) للسماح بالتهديد المكتشف. حدد أحد الخيارات التالية قبل النقر فوق **سماح** لتحديد إعدادات القاعدة:

- **الإعلام فقط عند حظر هذا التهديد**—تكوين القاعدة: **حظر** – لا، **إعلام** – لا، **سجل** – لا.
- **الإعلام عند حدوث هذا التهديد**—تكوين القاعدة: **حظر** – لا، **إعلام** – الافتراضي، **سجل** – الافتراضي.
- **عدم الإعلام**—تكوين القاعدة: **حظر** – لا، **إعلام** – لا، **سجل** – لا.

> قد تختلف المعلومات التي تظهر في نافذة الإعلام هذه تبعاً لنوع التهديد المكتشف.
> لمزيد من المعلومات عن التهديدات وغيرها من المصطلحات ذات الصلة، راجع أنواع الهجمات البعيدة أو أنواع الاكتشافات.
> لحل حدث **عناوين IP المتكررة في الشبكة**، راجع مقالة قاعدة معارف ESET.

تم اكتشاف شبكة جديدة

بشكل افتراضي، يستخدم ESET Internet Security إعدادات Windows عند اكتشاف اتصال بالشبكة جديد. لعرض نافذة حوار عند اكتشاف شبكة جديدة، قم بتغيير تعيين ملف تعريف حماية الشبكة إلى **Ask**. يحدث تكوين حماية الشبكة كلما يتصل جهاز الكمبيوتر بشبكة جديدة.



يمكنك الاختيار من ملفات تعريف اتصال الشبكةالتالية:

تلقائياً— سيحددESET Internet Security ملف التعريف تلقائياً، استناداً إلى المنشطات التي تم تكوينها لكل ملف تعريف.

خاص—للشبكات الموثوق بها (شبكة منزلية أو شبكة مكتب). يُعد جهاز الكمبيوتر والملفات المشتركة المخزنة عليه مرئياً

لمستخدمي الشبكة الآخرين، ويمكن الوصول إلى موارد النظام للمستخدمين الآخرين على الشبكة (تم تمكين الوصول إلى الملفات والطابعات المشتركة وتم تمكين الاتصال الوارد RPCوتُعد مشاركة سطح المكتب البعيد متاحة). نوصي باستخدام هذا الإعداد عند الوصول إلى شبكة محلية آمنة. يتم تعيين ملف التعريف هذا تلقائياً لاتصال الشبكة إذا تم تهيئته كمجال أو شبكة خاصة في Windows.

عام—للشبكات غير الموثوق بها (الشبكة العامة). لا تتم مشاركة الملفات والمجلدات الموجودة على نظامك مع مستخدمين آخرين على الشبكة ولا تكون مرئية لهم ويتم إلغاء تنشيط مشاركة موارد النظام. نوصي باستخدام هذا الإعداد عند الوصول إلى الشبكات اللاسلكية. يتم تعيين ملف التعريف هذا تلقائياً لأي اتصال شبكة لم يتم تهيئته كمجال أو شبكة خاصة في Windows.

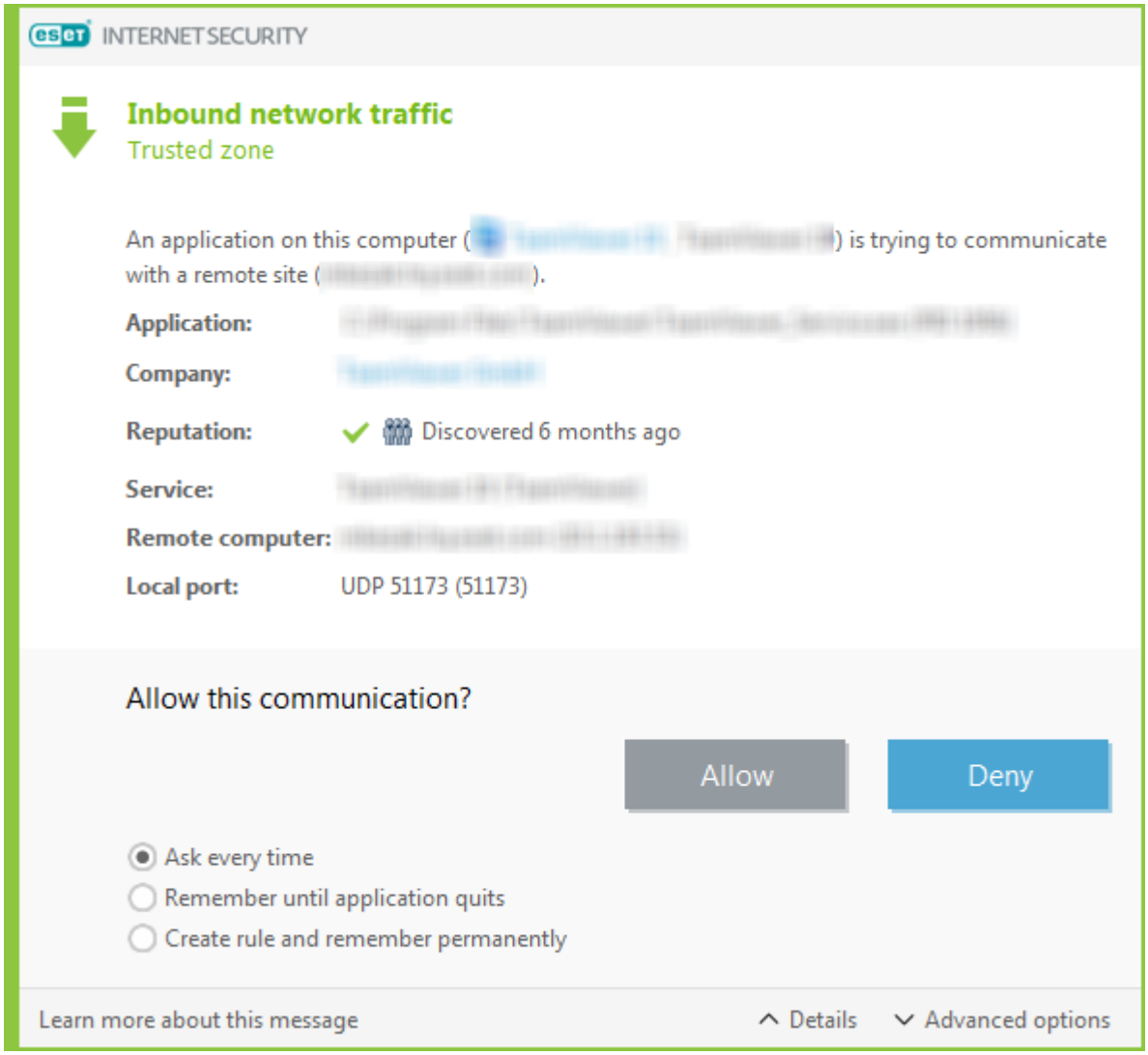
ملف تعريف محدد من قبل المستخدم—يمكنك تحديد أحد ملفات التعريف التي قمت بإنشائها من القائمة المنسدلة. يتوفر هذا الخيار فقط إذا قمت بإنشاء ملف تعريف مخصص واحد على الأقل.

قد يُعرّض تكوين الشبكة غير الصحيح جهاز الكمبيوتر الخاص بك لخطر أمني. ⚠

إنشاء اتصال ـ اكتشاف

يكتشف جدار الحماية كل اتصال بالشبكة تم إنشاؤه حديثاً. يحدد وضع جدار الحماية النشط الإجراءات التي يتم تنفيذها للقاعدة الجديدة. في حالة تنشيط **الوضع التلقائي** أو **وضع البوليصة المحدد**، سينفذ جدار الحماية إجراءات محددة مسبقاً دون تدخل المستخدم.

يعرض **الوضع التفاعلي** نافذة معلوماتية تُبلغ عن اكتشاف اتصال جديد بالشبكة، مع معلومات تفصيلية حول الاتصال. يمكنك اختيار **سماح** أو **رفض** (حظر) الاتصال. وفي حالة السماح باستمرار للاتصال نفسه في نافذة الحوار، يوصى بإنشاء قاعدة جديدة للاتصال. للقيام بذلك، حدد **إنشاء قاعدة وتذكرها دائماً** واحفظ الإجراء كقاعدة جديدة لجدار الحماية. إذا تعرف جدار الحماية على الاتصال نفسه في المستقبل، فسيطبق القاعدة الموجودة دون الحاجة إلى تفاعل من جانب المستخدم.



عند إنشاء قواعد جديدة، لا تسمح سوى بالاتصالات التي تعرف أنها آمنة. في حالة السماح بجميع الاتصالات، لن يستطيع جدار الحماية تحقيق الغرض. فيما يلي المعلمات المهمة للاتصالات:

التطبيق ـ موقع الملف القابل للتنفيذ ومعرّف العملية. لا تسمح بالاتصالات لتطبيقات وعمليات غير معروفة.

الموقّع—اسم ناشر التطبيق. انقر فوق النص لإظهار شهادة أمان للشركة.

السُّمعة ـ مستوى خطورة الاتصال. يتم تعيين الاتصالات على مستوى الخطورة: جيد (أخضر) أو غير معروف (برتقالي) أو محفوف بالمخاطر (أحمر)، باستخدام سلسلة من قواعد الأساليب البحثية التي تفحص سمات كل اتصال وعدد المستخدمين ووقت الاكتشاف. ويتم تجميع هذه المعلومات بواسطة تقنية ESET LiveGrid®.

الخدمة ـ اسم الخدمة، إذا كان التطبيق عبارة عن خدمة windows.

جهاز الكمبيوتر عن بُعد ـ عنوان الجهاز عن بُعد. السماح بالاتصالات إلى العناوين الموثوقة والمعروفة فقط.

المنفذ عن بُعد ـ منفذ الاتصال. يمكن السماح بالاتصال على المنافذ الشائعة (كحركة مرور ويب – رقم المنفذ 80.443) في ظل ظروف معينة.

غالباً ما تقوم حالات التسلل على جهاز الكمبيوتر باستخدام الإنترنت والاتصالات المخفية لتساعدها على إصابة أنظمة بعيدة. في حالة تكوين قواعد بشكل صحيح، يصبح جدار الحماية أداة مفيدة للحماية من مختلف هجمات التعليمات البرمجية الضارة.

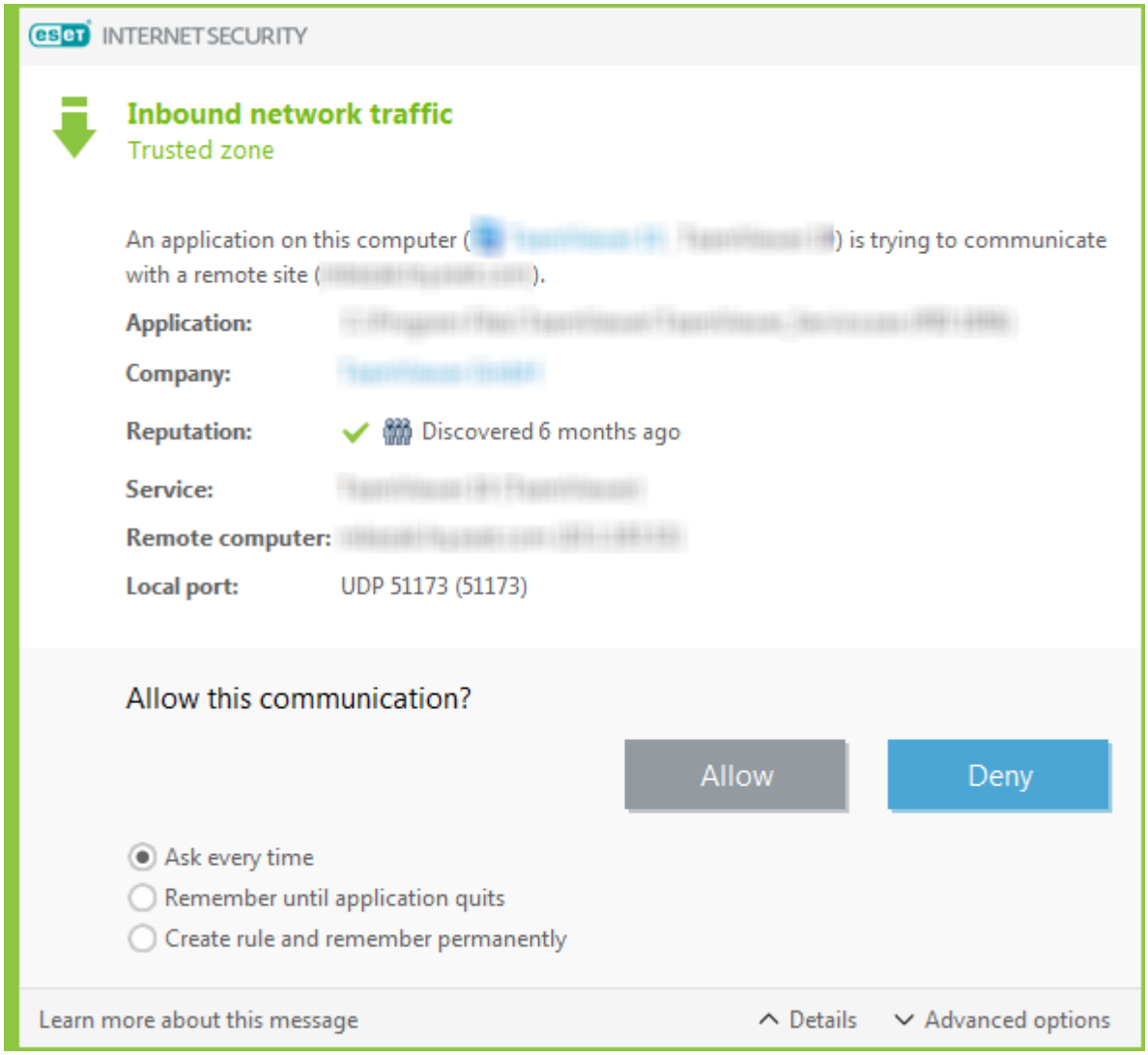
تغيير التطبيق

اكتشف جدار الحماية تعديلاً في تطبيق يُستخدم لإنشاء اتصالات صادرة من الكمبيوتر. ربما فقط تم تحديث هذا التطبيق إلى إصدار جديد. وربما في المقابل، يكون التعديل نتيجة تطبيق ضار. إذا لم يكن لديك علم بحدوث تعديل قانوني، فيوصى برفض الاتصال وفحص الكمبيوتر باستخدام أحدث قاعدة بيانات توقيعات فيروسات.

الاتصال الوارد الموثوق به

مثال على اتصال وارد ضمن المنطقة الموثوق بها:

كمبيوتر بعيد ضمن المنطقة الموثوق بها يحاول إنشاء اتصال مع تطبيق محلي مثبت على الكمبيوتر.



التطبيق—التطبيق الذي يتصل به جهاز بعيد.

مسار التطبيق—موقع التطبيق.

تطبيق متجر Microsoft—اسم التطبيق في متجر Microsoft.

الموقّع—اسم ناشر التطبيق. انقر فوق النص لإظهار شهادة أمان للشركة.

السمعة ـ سمعة التطبيق المستنتَجة بواسطة تقنية ESET LiveGrid®.

الخدمة – اسم الخدمة الجارية حالياً على جهاز الكمبيوتر.

الكمبيوتر عن بعد ـ كمبيوتر بعيد يحاول إنشاء اتصال بالتطبيق الموجود على الكمبيوتر.

المنفذ عن بعد ـ المنفذ المستخدم للاتصال.

السؤال كل مرة – إذا كان الإجراء الافتراضي لإحدى القواعد معيَّناً إلى **سؤال**، فسيتم عرض نافذة حوار كلما تم تشغيل القاعدة.

تذكر حتى إنهاء التطبيق – سيقوم ESET Internet Security بتذكر الإجراء المتخذ حتى إعادة التشغيل التالية.

إنشاء قاعدة وتذكرها دائماً – في حالة تحديد هذا الخيار قبل السماح باتصال أو رفضه، سيتذكر ESET Internet Security الإجراء ويستخدمه في حالة اتصال الكمبيوتر البعيد بالتطبيق مرة أخرى.

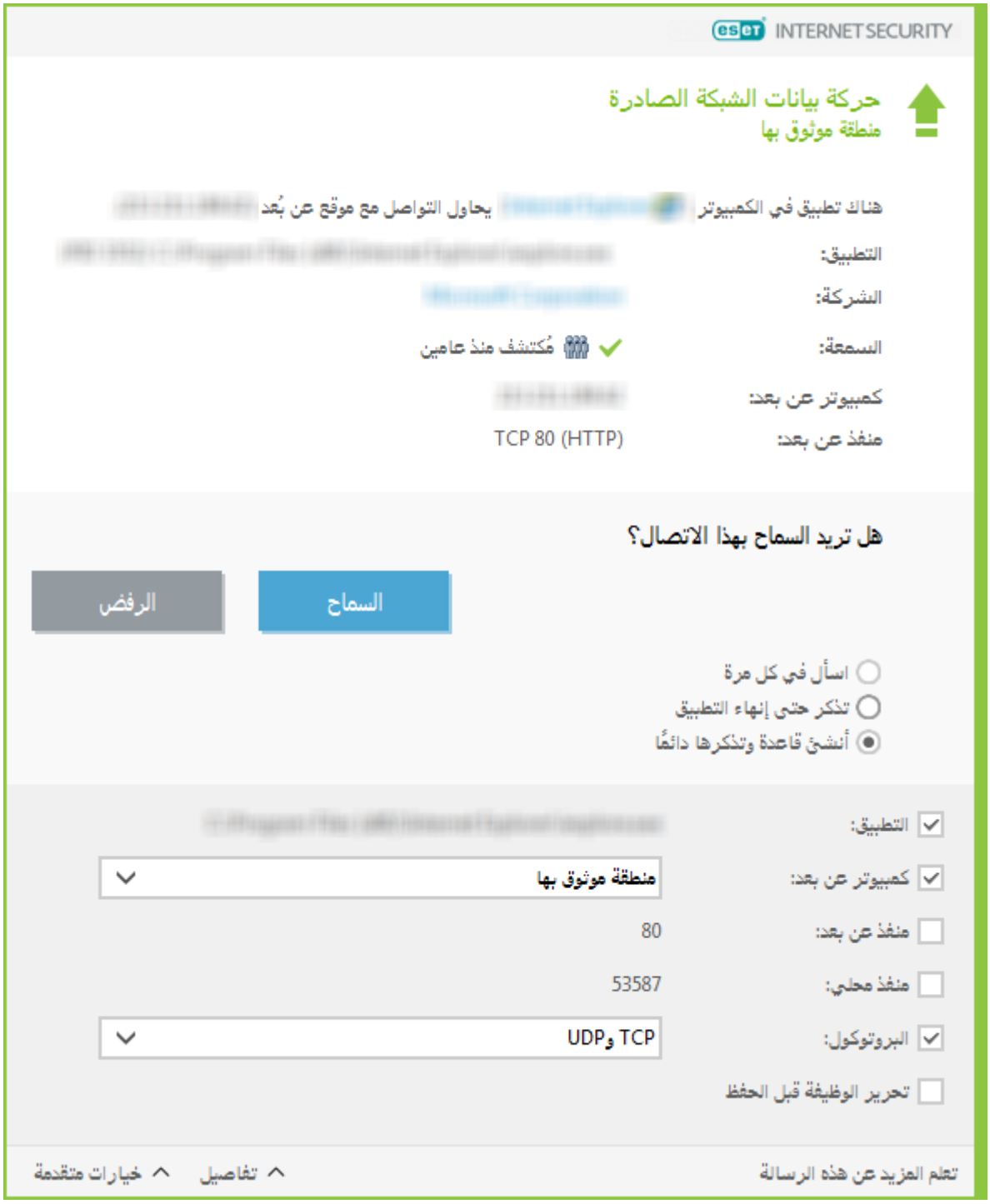
سماح ـ للسماح بالاتصال الوارد.

رفض ـ لرفض الاتصال الوارد.

تحرير القاعدة—يتيح لك تخصيص خصائص القاعدة باستخدام محرر قاعدة جدار الحماية.

الاتصال الصادر الموثوق به

مثال على اتصال صادر ضمن المنطقة الموثوق بها:
تطبيق محلي يحاول إنشاء اتصال بكمبيوتر آخر داخل الشبكة المحلية، أو داخل شبكة في المنطقة الموثوق بها.



التطبيق—التطبيق الذي يتصل به جهاز بعيد.

مسار التطبيق—موقع التطبيق.

تطبيق متجر Microsoft—اسم التطبيق في متجر Microsoft.

الموقّع—اسم ناشر التطبيق. انقر فوق النص لإظهار شهادة أمان للشركة.

السمعة ـ سمعة التطبيق المستنتَجة بواسطة تقنية ESET LiveGrid®.

الخدمة – اسم الخدمة الجارية حالياً على جهاز الكمبيوتر.

الكمبيوتر عن بعد ـ كمبيوتر بعيد يحاول إنشاء اتصال بالتطبيق الموجود على الكمبيوتر.

المنفذ عن بعد ـ المنفذ المستخدم للاتصال.

السؤال كل مرة – إذا كان الإجراء الافتراضي لإحدى القواعد معيَّناً إلى **سؤال**، فسيتم عرض نافذة حوار كلما تم تشغيل القاعدة.

تذكر حتى إنهاء التطبيق – سيقوم ESET Internet Security بتذكر الإجراء المتخذ حتى إعادة التشغيل التالية.

إنشاء قاعدة وتذكرها دائماً – في حالة تحديد هذا الخيار قبل السماح باتصال أو رفضه، سيتذكر ESET Internet Security الإجراء ويستخدمه في حالة اتصال الكمبيوتر البعيد بالتطبيق مرة أخرى.

سماح ـ للسماح بالاتصال الوارد.

رفض ـ لرفض الاتصال الوارد.

تحرير القاعدة—يتيح لك تخصيص خصائص القاعدة باستخدام محرر قاعدة جدار الحماية.

الاتصال الوارد

مثال على الاتصال بالإنترنت الوارد:
كمبيوتر بعيد يحاول الاتصال بتطبيق مثبت على الكمبيوتر.

التطبيق—التطبيق الذي يتصل به جهاز بعيد.

مسار التطبيق—موقع التطبيق.

تطبيق متجر Microsoft—اسم التطبيق في متجر Microsoft.

الموقّع—اسم ناشر التطبيق. انقر فوق النص لإظهار شهادة أمان للشركة.

السمعة ـ سمعة التطبيق المستنتَجة بواسطة تقنية ESET LiveGrid®.

الخدمة – اسم الخدمة الجارية حالياً على جهاز الكمبيوتر.

الكمبيوتر عن بعد ـ كمبيوتر بعيد يحاول إنشاء اتصال بالتطبيق الموجود على الكمبيوتر.

المنفذ عن بعد ـ المنفذ المستخدم للاتصال.

السؤال كل مرة – إذا كان الإجراء الافتراضي لإحدى القواعد معيَّناً إلى **سؤال**، فسيتم عرض نافذة حوار كلما تم تشغيل القاعدة.

تذكر حتى إنهاء التطبيق – سيقوم ESET Internet Security بتذكر الإجراء المتخذ حتى إعادة التشغيل التالية.

إنشاء قاعدة وتذكرها دائماً – في حالة تحديد هذا الخيار قبل السماح باتصال أو رفضه، سيتذكر ESET Internet Security الإجراء ويستخدمه في حالة اتصال الكمبيوتر البعيد بالتطبيق مرة أخرى.

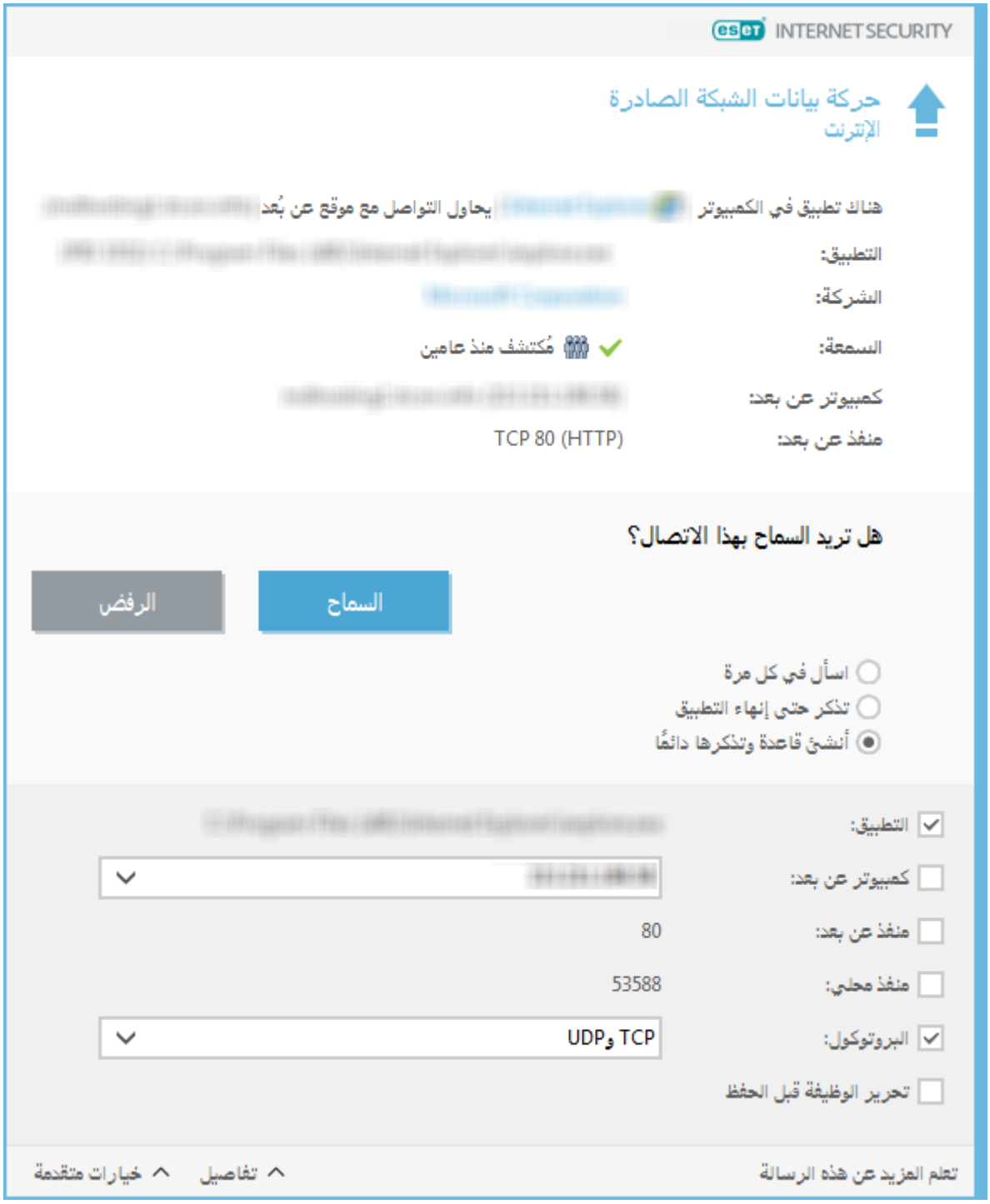
سماح – للسماح بالاتصال الوارد.

رفض – لرفض الاتصال الوارد.

تحرير القاعدة—يتيح لك تخصيص خصائص القاعدة باستخدام محرر قاعدة جدار الحماية.

الاتصال الصادر

مثال على الاتصال بالإنترنت الصادر:
تطبيق محلي يحاول إنشاء اتصال بالإنترنت.



التطبيق—التطبيق الذي يتصل به جهاز بعيد.

مسار التطبيق—موقع التطبيق.

تطبيق متجر Microsoft—اسم التطبيق في متجر Microsoft.

الموقّع—اسم ناشر التطبيق. انقر فوق النص لإظهار شهادة أمان للشركة.

السمعة ـ سمعة التطبيق المستنتَجة بواسطة تقنية ESET LiveGrid®.

الخدمة – اسم الخدمة الجارية حالياً على جهاز الكمبيوتر.

الكمبيوتر عن بعد ـ كمبيوتر بعيد يحاول إنشاء اتصال بالتطبيق الموجود على الكمبيوتر.

المنفذ عن بعد ـ المنفذ المستخدم للاتصال.

السؤال كل مرة – إذا كان الإجراء الافتراضي لإحدى القواعد معيَّناً إلى **سؤال**، فسيتم عرض نافذة حوار كلما تم تشغيل القاعدة.

تذكر حتى إنهاء التطبيق – سيقوم ESET Internet Security بتذكر الإجراء المتخذ حتى إعادة التشغيل التالية.

إنشاء قاعدة وتذكرها دائماً – في حالة تحديد هذا الخيار قبل السماح باتصال أو رفضه، سيتذكر ESET Internet Security الإجراء ويستخدمه في حالة اتصال الكمبيوتر البعيد بالتطبيق مرة أخرى.

سماح ـ للسماح بالاتصال الوارد.

رفض ـ لرفض الاتصال الوارد.

تحرير القاعدة—يتيح لك تخصيص خصائص القاعدة باستخدام محرر قاعدة جدار الحماية.

إعداد عرض الاتصال

انقر بزر الماوس الأيمن فوق اتصال لعرض خيارات إضافية تشمل:

حل أسماء الأجهزة المضيفة ـ إن أمكن، يتم عرض جميع عناوين الشبكة بتنسيق DNS وليس بتنسيق عنوان IP الرقمي.

عرض اتصالات TCP فقط ـ تعرض القائمة اتصالات تنتمي إلى مجموعة بروتوكولات TCP فقط.

إظهار اتصالات الاستماع ـ حدد هذا الخيار فقط لعرض اتصالات، عندما لا يوجد اتصال تم إنشاؤه حالياً، ولكن النظام قد فتح منفذاً وبانتظار اتصال.

إظهار الاتصالات داخل الكمبيوتر ـ حدد هذا الخيار لإظهار اتصالات فقط، بينما الجانب البعيد يكون نظاماً محلياً، وهو ما يسمى اتصالات localhost.

سرعة التحديث ـ اختر تكرار تحديث الاتصالات النشطة.

تحديث الآن – لإعادة تحميل نافذة **اتصالات الشبكة**.

أدوات الأمان

افتح نافذة البرنامج الرئيسية > **الإعداد** > **أدوات الأمان** لضبط الوحدات التالية:

التصفح المصرفي الآمن — يضيف طبقة حماية إضافية للمتصفح تم تصميمها لحماية البيانات المالية أثناء إجراء المعاملات عبر الإنترنت. تمكين **تأمين جميع المتصفحات** في الإعداد المتقدم للتصفح المصرفي الآمن لبدء كل متصفحات الويب المدعومة في وضع آمن.

خصوصية وأمان المتصفح—تبقي نشاطك عبر الإنترنت خاصاً وآمناً دون ترك بصمة رقمية.

Anti-Theft — قم بتمكين مكافحة السرقة لحماية جهاز الكمبيوتر في حالة فقدانه أو سرقته.

التصفح المصرفي الآمن

التصفح المصرفي الآمن عبارة عن طبقة حماية إضافية تم تصميمها لحماية البيانات المالية في أثنا إجراء المعاملات عبر الإنترنت.

افتراضياً، يبدأ تشغيل جميع متصفحات الويب المدعومة في وضع آمن. يتيح لك هذا تصفح الإنترنت والوصول إلى الخدمات المصرفية عبر الإنترنت وإجراء عمليات الشراء والمعاملات عبر الإنترنت في متصفح مؤمّن واحد تلقائياً.

يجب تمكين نظام السمعة في ESET LiveGrid® (يتم تمكينه افتراضياً) لضمان عمل التصفح المصرفي الآمن بشكل صحيح.

لتكوين سلوك المتصفح المؤمَّن، راجع الإعداد المتقدم للتصفح المصرفي الآمن. إذا قمت بتعطيل **تأمين جميع المتصفحات**، يمكنك الوصول إلى المتصفح المؤمَّن في نافذة البرنامج الرئيسية > **نظرة عامة** > **التصفح المصرفي الآمن** أو من خلال النقر على أيقونة **التصفح المصرفي الآمن** على سطح المكتب. يتم تشغيل المتصفح الذي تم تعيينه افتراضياً في Windows في وضع آمن.

ومن هنا يعد استخدام HTTPS المشفّر ضرورياً لحماية الاستعراض عبر المستعرض. المتصفحات التالية تدعم التصفح المصرفي الآمن:

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

فقط Microsoft Edge, Firefox ويتم دعمها على الأجهزة المزودة بمعالجات ARM.

لمزيد من التفاصيل حول ميزة التصفح المصرفي الآمن، اقرأ مقالة قاعدة معرفة ESET التالية المتوفرة باللغة العربية وغيرها من العديد من اللغات:

- كيف يمكنني استخدام التصفح المصرفي الآمن من ESET؟
- إيقاف التصفح المصرفي الآمن مؤقتاً أو تعطيله في منتجات ESET Windows المنزلية
- التصفح المصرفي الآمن لـESET؟—الأخطاء الشائعة
- مسرد ESET | التصفح المصرفي الآمن

إعلام في المتصفح

يعلمك المتصفح المؤمَّن بحالته الحالية من خلال الإعلامات في المتصفح ولون إطار المتصفح.

تظهر الإعلامات في المتصفح في علامة التبويب على الجانب الأيسر.

لتوسيع الإعلام في المتصفح، انقر فوق رمز ESET. لتصغير الإعلام، انقر فوق نص الإعلام. لرفض الإعلام وإطار المتصفح الأخضر، انقر فوق رمز الإغلاق.

يمكن رفض الإعلام الإخباري وإطار المتصفح الأخضر فقط.

الإعلامات في المتصفح

الحالة	نوع الإعلام
يتم ضمان الحماية القصوى ويتم تصغير الإعلامات في المتصفح افتراضياً. قم بتوسيع إعلام المتصفح وانقر فوق **الإعدادات** لفتح إعداد أدوات الأمان.	إعلام معلوماتي وإطار متصفح أخضر
يتطلب المتصفح المؤمّن انتباهك لمشكلة غير حرجة. لمزيد من المعلومات حول المشكلة أو الحل، اتبع التعليمات الواردة في الإعلام في المتصفح.	تحذير وإطار متصفح برتقالي
المتصفح غير محمي بواسطة التصفح المصرفي الآمن من ESET. أعد تشغيل المتصفح للتأكد من أن الحماية نشطة. لحل التعارض مع الملفات التي تم تحميلها في المتصفح، افتح ملفات السجل > **التصفح المصرفي الآمن** وتأكد من عدم تحميل الملفات المسجلة في المرة التالية التي تقوم فيها بتشغيل المتصفح. إذا استمرت المشكلة، فاتصل بالدعم الفني لـESET باتباع الإرشادات الموجودة في مقالة قاعدة المعرفة الخاصة بنا.	تنبيه الأمان وإطار المتصفح الأحمر

خصوصية وأمان المتصفح

يمكنك تمكين ميزة خصوصية وأمان المتصفح من خلال ملحق مخصص متاح على المتصفحات المدعومة (Google Chrome، و Mozilla Firefox و Microsoft Edge فقط).

لتثبيت الملحق وتمكينه:

1. تأكد من استخدام أحدث إصدار من ESET Internet Security وإعادة تشغيل الكمبيوتر بنجاح بعد التحديث.
2. افتح المتصفح لديك.
3. تم تثبيت الامتداد في ملحقك.
4. عليك تمكين الملحق وسيتم عرض صفحة تفاصيل المتصفح الذي به امتداد.

تنقسم القائمة الرئيسية لملحق خصوصية وأمان المتصفح إلى الأقسام التالية:

نظرة عامة

البحث الآمن

انقر فوق أيقونة التبديل بجوار **فحص نتائج البحث** لتمكين الميزة ومعرفة النتائج الآمنة للنقر عليها. يعمل البحث الآمن على تقييم عناوين الروابط المدرجة ولا يعني بالضرورة أن موقع الويب لا يحتوي على برمجيات خبيثة. يعمل محرك الكشف الخاص بنا بعد ذلك على اكتشاف أي برمجيات خبيثة على موقع الويب.

تنظيف المتصفح

احذف بيانات التصفح الخاصة بك أو قم بإعداد عمليات تنظيف منتظمة. يمكنك إضافة مواقع الويب التي تريد قبول ملفات تعريف الارتباط فيها واستمر في تسجيل الدخول حتى بعد إجراء تنظيف المتصفح من خلال **إضافتها إلى قائمة**.

- **التنظيف لمرة واحدة** ـ حدد النطاق الزمني من القائمة المنسدلة ونوع البيانات التي تريد حذفها. يمكنك الاختيار من بين الخيارات جميع البيانات والاختيارات الخاصة والمخصصة.
- **التنظيف العادي**ـ انقر فوق أيقونة التبديل بجوار **التنظيف العادي** لتمكين الميزة. حدد النطاق الزمني من القائمة المنسدلة ونوع البيانات الذي تريد حذفه بانتظام. يمكنك الاختيار من بين الخيارات جميع البيانات والاختيارات الخاصة والمخصصة.

يحتوي خيار **البيانات المخصصة** على الفئات التالية:

- سجل التصفح
- سجل التنزيل
- ملفات تعريف الارتباط وبيانات موقع الويب
- الصور والملفات المخزنة مؤقتاً
- كلمات المرور وبيانات تسجيل الدخول
- بيانات الملء التلقائي للنموذج

مراجعة إعدادات موقع الويب

يمكنك الوصول بسهولة إلى أذونات موقع الويب وإدارتها للتحكم في المعلومات التي يمكن لمواقع الويب استخدامها.

- **الإعلامات**—راجع مواقع الويب التي تريد **السماح/حظر** الإشعارات فيها أو إذا كنت تريد أن **يسألك ملحق المتصفح في كل مرة**.

الإعداد المتقدم

تنظيف المتصفح

إعدادات ملفات تعريف الارتباط المتقدمة

أضف مواقع الويب التي تريد قبول ملفات تعريف الارتباط فيها واستمر في تسجيل الدخول حتى بعد إجراء تنظيف المتصفح. أدخل عنوان URL في حقل النص، وانقر فوق **إضافة**. يمكنك إزالته في أي وقت من القائمة بالنقر فوق أيقونة ناقص بجوار

موقع الويب المحدد.

في الجزء السفلي من الصفحة توجد قائمة بالنطاقات المقترحة المفتوحة حالياً في المتصفح. إذا لم تتمكن من رؤية موقع الويب المحدد، فانقر فوق **تحديث القائمة**، وأضفه إلى قائمة ملفات تعريف الارتباط المقبولة بالنقر فوق أيقونة علامة زائد ⊕.

مراجعة إعدادات موقع الويب

يمكنك الوصول بسهولة إلى أذونات موقع الويب وإدارتها للتحكم في المعلومات التي يمكن لمواقع الويب استخدامها.

- **الإعلامات**—راجع مواقع الويب التي تريد **السماح/حظر** الإشعارات فيها أو إذا كنت تريد أن **يسألك ملحق المتصفح في كل مرة**.

المظهر

يمكنك تخصيص نظام ألوان الواجهة ليناسب تفضيلاتك. يمكنك اختيار نظام الألوان المفضل لديك عن طريق تحديد خانة الاختيار**فاتح** أو **داكن**.

مكافحة السرقة

تكون الأجهزة الشخصية دائماً معرضة لخطر السرقة أو الفقدان أثناء التنقل اليومي من المنزل إلى العمل وإلى الأماكن العامة الأخرى. مكافحة السرقة عبارة عن ميزة تعمل على زيادة الأمان على مستوى المستخدم في حالة فقدان الجهاز أو سرقته. تتيح لك مكافحة السرقة مراقبة استخدام الجهاز وتتبع جهازك المفقود باستخدام نظام التحديد من خلال عنوان IP في ESET HOME، مما يساعدك في استعادة جهازك وحماية بياناتك الشخصية.

من خلال استخدام التقنيات الحديثة مثل البحث الجغرافي بواسطة عنوان IP والتقاط الصور باستخدام كاميرا الويب، وحماية حساب المستخدم، ومراقبة الجهاز، يمكن لميزة مكافحة السرقة مساعدتك ثم تحدد جهة إنفاذ القانون موقع الكمبيوتر أو الجهاز في حالة فقدانه أو سرقته. في ESET HOME، يمكنك معرفة النشاط الذي يتم على جهاز الكمبيوتر أو الجهاز الخاص بك.

لمعرفة المزيد حول مكافحة السرقة في ESET HOME راجع تعليمات ESET HOME عبر الإنترنت.

قد لا يعمل مكافحة السرقة بشكل صحيح على أجهزة الكمبيوتر في المجالات بسبب القيود في إدارة حسابات المستخدمين.

بعد تمكين مكافحة السرقة، يمكنك تحسين أمان جهازك في نافذة البرنامج الرئيسية > **الإعداد** > **أدوات الأمان** > **مكافحة السرقة**.

خيارات التحسين

لم يتم إنشاء حساب وهمي

يزيد إنشاء حساب وهمي من فرصتك في تحديد موقع جهاز مفقود أو مسروق. إذا وضعت علامة على جهازك كمفقود، فستقوم ميزة مكافحة السرقة بحظر الوصول إلى حسابات المستخدم النشطة لحماية بياناتك الحساسة. لن يُسمح لأي شخص يحاول استخدام الجهاز إلا باستخدام الحساب الوهمي. الحساب الوهمي عبارة عن شكل من أشكال حساب الضيف بأذونات محدودة. سيُستخدم كحساب افتراضي للنظام حتى يتم وضع علامة على جهازك على أنه تم استرداده ـ مما يمنع أي شخص من تسجيل الدخول إلى حسابات المستخدم الأخرى أو الوصول إلى بيانات المستخدم.

> في أي وقت يقوم شخص ما بتسجيل الدخول إلى الحساب الوهمي عندما يكون جهاز الكمبيوتر في حالة طبيعية، سيتم إرسال إشعار بالبريد الإلكتروني يتضمن معلومات بشأن نشاط مشبوه على جهاز الكمبيوتر الخاص بك. بعد استلام إشعار عبر البريد الإلكتروني، يمكنك تحديد ما إذا كنت تريد وضع علامة على جهاز الكمبيوتر كمفقود.

لإنشاء حساب وهمي، انقر فوق **إنشاء حساب وهمي**، واكتب **اسم الحساب الوهمي** في حقل النص وانقر فوق **إنشاء**.

عند حصولك على حساب وهمي، انقر فوق **إعدادات الحساب الوهمي** لإعادة تسمية الحساب أو حذفه.

حماية كلمة المرور لحسابات Windows

حساب المستخدم الخاص بك ليس محمياً بكلمة مرور. ستتلقى تحذير التحسين هذا إذا لم يكن هناك حساب مستخدم واحد على الأقل محمياً بكلمة مرور. سيؤدي إنشاء كلمة مرور لجميع المستخدمين (باستثناء **الحساب الوهمي**) على جهاز الكمبيوتر إلى حل

هذه المشكلة.

لإنشاء كلمة مرور لحساب المستخدم، انقر فوق **إدارة حسابات Windows** وقم بتغيير كلمة المرور أو اتبع الإرشادات الواردة أدناه:

1. اضغط على CTRL+Alt+Delete في لوحة المفاتيح.
2. انقر فوق **تغيير كلمة مرور**.
3. اترك حقل **كلمة المرور القديمة** فارغاً.
4. أدخل كلمة المرور في الحقلين **كلمة المرور الجديدة** و**تأكيد كلمة المرور** واضغط على **Enter**.

تسجيل الدخول التلقائي لحسابات Windows

تم تمكين تسجيل الدخول التلقائي لحساب المستخدم الخاص بك؛ لذلك، حسابك ليس محمياً ضد الوصول غير المصرّح به. ستتلقى تحذير التحسين هذا إذا تم تمكين تسجيل الدخول التلقائي لحساب مستخدم واحد على الأقل. انقر فوق **تعطيل تسجيل الدخول التلقائي** لحل مشكلة التحسين هذه.

تسجيل الدخول التلقائي للحساب الوهمي

تم تمكين تسجيل الدخول التلقائي **للحساب الوهمي** على جهازك. عندما يكون الجهاز في حالة طبيعية، لا نوصي باستخدام تسجيل الدخول التلقائي لأنه قد يتسبب في حدوث مشكلات في الوصول إلى حساب المستخدم الحقيقي أو إرسال إنذارات كاذبة بشأن الحالة المفقودة لجهاز الكمبيوتر. انقر فوق **تعطيل تسجيل الدخول التلقائي** لحل مشكلة التحسين هذه.

سجّل الدخول إلى حساب ESET HOME.

لتمكين/تعطيل مكافحة السرقة وللوصول إلى موقع الجهاز والمعلومات في ESET HOME، قم بتسجيل الدخول إلى حساب ESET HOME.

ثمة عدة طرق متوفرة لتسجيل الدخول إلى حساب ESET HOME:

- **استخدم عنوان البريد الإلكتروني وكلمة المرور لـESET HOME** – اكتب **عنوان البريد الإلكتروني** و**كلمة المرور** الذين استخدمتهما لإنشاء حساب ESET HOME وانقر فوق **تسجيل الدخول**.
- **استخدم حساب Google/AppleID** – انقر فوق **المتابعة باستخدام Google** أو **المتابعة باستخدام Apple** وقم بتسجيل الدخول إلى الحساب المناسب. بعد نجاح تسجيل الدخول، ستتم إعادة توجيهك إلى صفحة الويب لتأكيد ESET HOME. للمتابعة، قم بالتبديل مرة أخرى إلى نافذة منتج ESET. لمزيد من المعلومات حول حساب Google/تسجيل الدخول إلىAppleID، راجع التعليمات في التعليمات عبر الإنترنت ESET HOME.
- **مسح رمز QR ضوئياً** – انقر فوق **مسح رمز QR ضوئياً** لعرض رمز QR. افتح تطبيق ESET HOME للهاتف المحمول وامسح رمز QR أو وجّه كاميرا جهازك إلى رمز QR. لمزيد من المعلومات، راجع التعليمات في التعليمات عبر ESET HOME الإنترنت.

فشل تسجيل الدخول ـ الأخطاء الشائعة.

إذا لم يكن لديك حساب ESET HOME فانقر فوق **إنشاء حساب** للتسجيل أو اطلع على الإرشادات في تعليمات ESET HOME عبر الإنترنت.
إذا نسيت كلمة المرور، فانقر فوق **نسيت كلمة المرور** واتبع الخطوات التي تظهر على الشاشة أو راجع الإرشادات في تعليمات ESET HOME عبر الإنترنت.

لا يدعم مكافحة السرقة Microsoft Windows Home Server.

تعيين اسم جهاز

يمثل حقل **اسم الجهاز** اسم جهاز الكمبيوتر الخاص بك (الجهاز) الذي سيتم عرضه كمعرف في جميع خدمات ESET HOME. يتم استخدام اسم جهاز الكمبيوتر لجهاز الكمبيوتر بشكل افتراضي. اكتب اسم الجهاز أو استخدم الاسم الافتراضي وانقر فوق **متابعة**.

تم تمكين/تعطيل مكافحة السرقة

تحتوي هذه النافذة على رسالة تأكيد عند تمكين/تعطيل مكافحة السرقة:

- تم التمكين – جهازك محمي الآن من خلال مكافحة السرقة، ويمكنك إدارة أمانه عن بُعد على بوابة ESET HOME باستخدام حسابك.
- تم التعطيل – تم تعطيل مكافحة السرقة على هذا الجهاز، وتمت إزالة جميع البيانات المتعلقة بـ <%ESET_ANTTHEFT%> لهذا الجهاز من بوابة ESET HOME.

فشلت إضافة جهاز جديد

لقد تلقيت خطأ أثناء تنشيط مكافحة السرقة.

السيناريوهات الأكثر شيوعاً هي:

- خطأ في تسجيل الدخول إلى ESET HOME
- لا يوجد اتصال بالإنترنت (أو أن الإنترنت لا يعمل حالياً).

إذا تعذّر عليك حل المشكلة، فاتصل بالدعم الفني لـ ESET.

استيراد الإعدادات وتصديرها

يمكنك استيراد ملف تكوين .xml المخصص لبرنامج ESET Internet Security أو تصديره من قائمة **إعداد**.

> **إرشادات موضحة**
> راجع استيراد أو تصدير إعدادات تكوين ESET باستخدام ملف.xml للحصول على إرشادات مشروحة باللغة الإنجليزية وغيرها من العديد من اللغات.

يفيد استيراد ملفات التكوين وتصديرها إذا كنت بحاجة إلى نسخ تكوين ESET Internet Security الحالي احتياطياً لاستخدامه في وقت لاحق. كما يلائم خيار تصدير الإعداد عندما تريد استخدام التكوين المفضل على عدة أنظمة. فيمكنك استيراد ملف .xml لنقل هذه الإعدادات.

لاستيراد تكوين، في نافذة البرنامج الرئيسية، انقر فوق **الإعداد** > **استيراد/تصدير الإعدادات** وحدد **استيراد الإعدادات**. أدخل اسم ملف التكوين أو انقر فوق زر **...** للاستعراض إلى ملف التكوين الذي تريد استيراده.

لتصدير تكوين، في نافذة البرنامج الرئيسية، انقر فوق **الإعداد** > **استيراد/تصدير الإعدادات**. حدد **تصدير الإعدادات** واكتب مسار الملف الكامل مع الاسم. انقر فوق **...** للانتقال إلى موقع على جهاز الكمبيوتر لحفظ ملف التكوين إليه.

قد تواجه خطأ أثناء تصدير الإعدادات إذا لم تكن لديك حقوق كافية لكتابة الملف المصدَّر إلى الدليل المحدد.

المساعدة و الدعم

انقر فوق **المساعدة والدعم** في نافذة البرنامج الرئيسية لعرض معلومات الدعم وأدوات استكشاف الأخطاء وإصلاحها التي تساعدك في حل المشكلات التي قد تواجهها.

الاشتراك

- استكشاف أخطاء الاشتراك وإصلاحها — انقر فوق هذا الرابط للعثور على حلول لمشكلات التنشيط أو تغيير الاشتراك.
- تغيير الاشتراك – انقر لتشغيل نافذة التنشيط وتنشيط المنتج. إذا كان جهازك متصلاً بـ ESET HOME، فاختر اشتراكاً من حساب ESET HOME أو أضف اشتراكاً جديداً.

المنتج المثبت

- ما الجديد – انقر فوق هذا لفتح نافذة المعلومات حول الميزات الجديدة والمحسّنة.
- حول ESET Internet Security – لعرض معلومات عن نسخة ESET Internet Security.
- استكشاف أخطاء المنتج وإصلاحها – انقر فوق هذا الرابط للعثور على حلول للمشكلات الأكثر شيوعاً.
- **تغيير المنتج** – انقر لترى ما إذا كان يمكن تغيير ESET Internet Security إلى خط منتج مختلف باستخدام اشتراك الحالي.

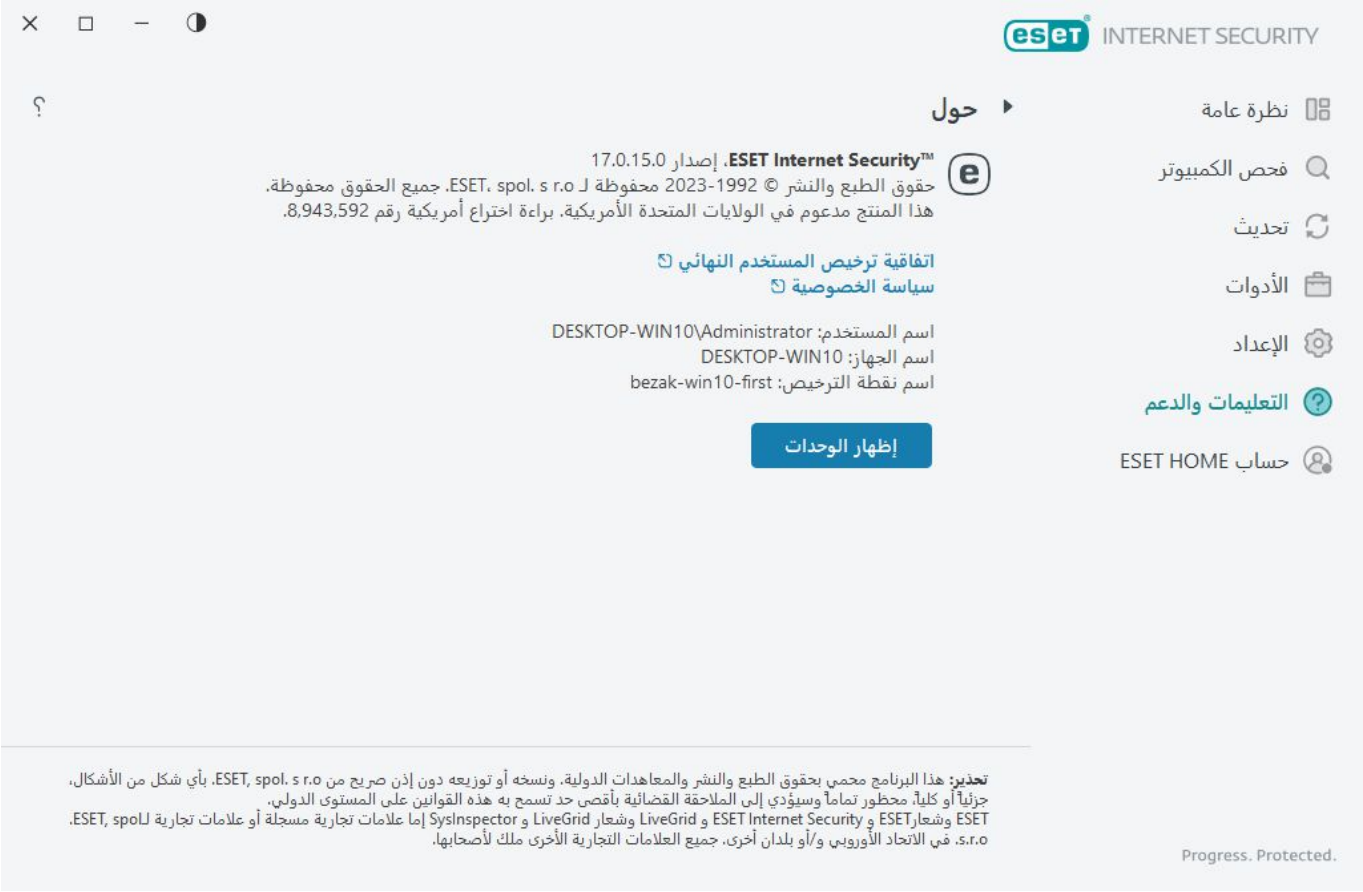
صفحة المساعدة – انقر فوق هذا الارتباط لتشغيل صفحات تعليمات ESET Internet Security.

الدعم الفني

قاعدة المعرفة – تحتوي قاعدة معارف ESET على إجابات للأسئلة المتداولة إضافة إلى حلول موصى بها لمشكلات متنوعة. تعد قاعدة المعارف، التي يتم تحديثها بانتظام بواسطة متخصصي ESET التقنيين، أكثر أدوات حل مختلف المشكلات كفاءة.

حول ESET Internet Security

توفر هذه النافذة التفاصيل المتعلقة بالإصدار المثبت من ESET Internet Security وجهاز الكمبيوتر لديك.



انقر فوق **إظهار الوحدات** للاطلاع على المعلومات المتعلقة بقائمة الوحدات للبرامج المحملة.

- يمكنك نسخ معلومات عن الوحدات إلى الحافظة بالنقر فوق **نسخ**. وقد يكون هذا مفيداً أثناء استكشاف الأخطاء وإصلاحها أو عند الاتصال بالدعم التقني.
- انقر فوق **محرك الكشف** في نافذة الوحدات لفتح رادار الفيروسات من ESET والذي يحتوي على معلومات عن كل إصدار من إصدارات محرك الكشف من ESET.

أخبار ESET

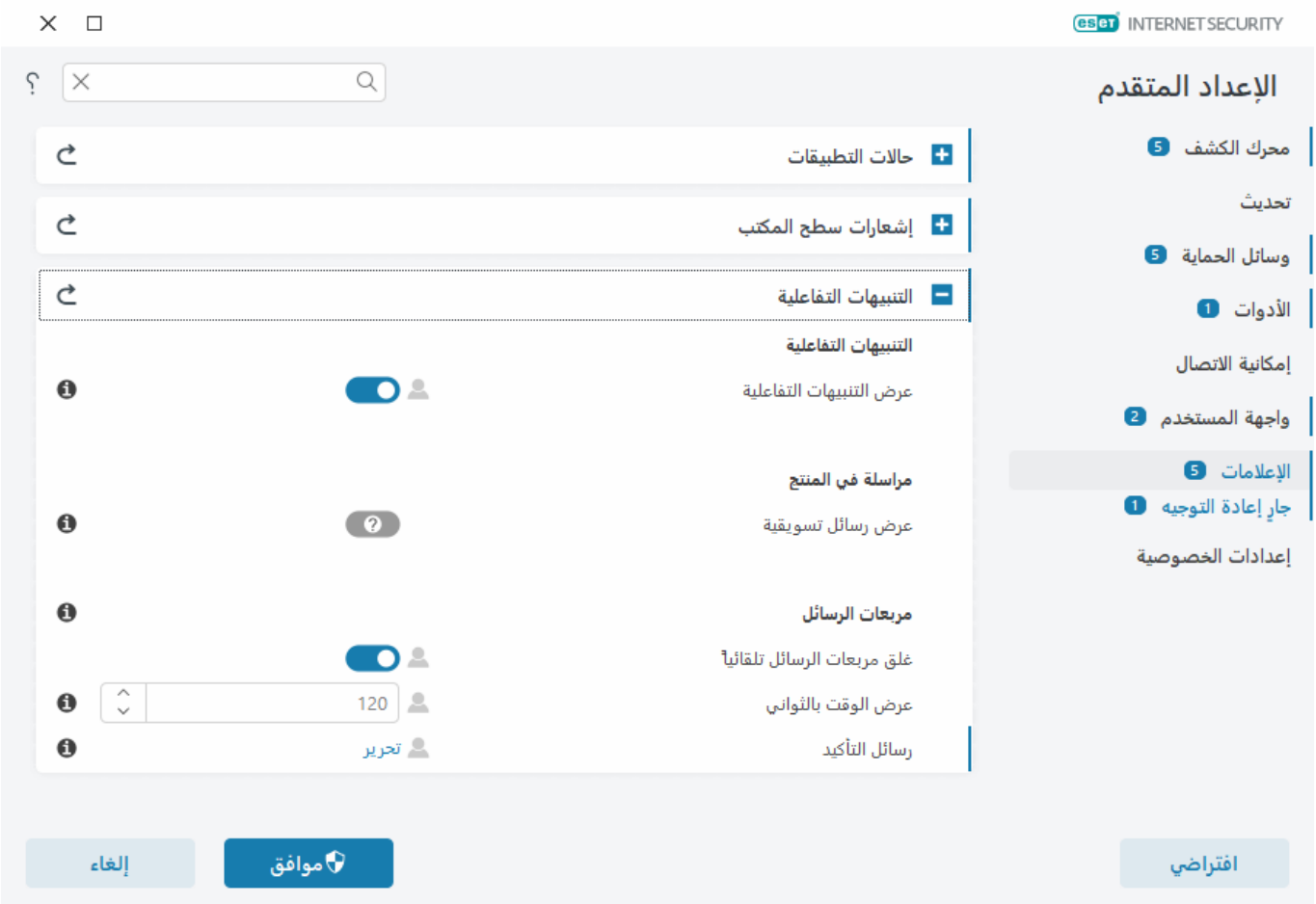
في هذه النافذة، يعلمك ESET Internet Security بأخبار ESET بصورة منتظمة.

تم تصميم المراسلة في المنتج لإعلام المستخدمين بأخبار ESET وغيرها من الاتصالات. يتطلب إرسال رسائل تسويقية موافقة

المستخدم. ومن ثمّ، لا يتم إرسال الرسائل التسويقية إلى أي مستخدم بشكل افتراضي (تظهر كعلامة تعجب). من خلال تمكين هذا الخيار، أنت بذلك توافق على تلقي رسائل ESET التسويقية. وإذا لم تكن ترغب في تلقي مواد ESET التسويقية، فقم بتعطيل خيار **عرض رسائل تسويقية**.

لتمكين تلقي الرسائل التسويقية أو تعطيلها عبر نافذة إعلام، اتبع الإرشادات أدناه.

1. لفتح "إعداد متقدم".
2. انقر فوق **الإعلامات** > **التنبيهات التفاعلية**.
3. قم بتعديل خيار **عرض رسائل تسويقية**.



إرسال بيانات تكوين النظام

لتتمكن شركة ESET من تقديم المساعدة بأقصى سرعة ودقة ممكنتين، فإنها تطلب الحصول على معلومات عن تكوين ESET Internet Security ومعلومات النظام التفصيلية والعمليات التي قيد التشغيل (ملف سجل ESET SysInspector) وبيانات السجل. لن تستخدم شركة ESET هذه البيانات إلا لتقديم المساعدة التقنية للعميل.

بعد إرسال نموذج الويب ***، سيتم إرسال بيانات تكوين النظام إلى ESET. حدد **إرسال هذه المعلومات دائماً** إذا كنت ترغب في تذكر هذا الإجراء لهذه العملية. عند تقديم نموذج الويب بدون إرسال أي بيانات، انقر فوق **عدم إرسال البيانات** والمتابعة.

يمكنك تكوين تقديم بيانات تكوين النظام في الإعداد المتقدم > **الأدوات** > **التشخيصات** > الدعم الفني.

إذا قررت إرسال بيانات تكوين النظام، فمن الضروري ملء نموذج الويب وإرساله. بخلاف ذلك، لن يتم إنشاء بطاقة الدعم لديك وستُفقد بيانات تكوين النظام. إذا تعذر إرسال بيانات تكوين النظام، فاملأ نموذج الويب وانتظر التعليمات من الدعم الفني.

الدعم الفني

في نافذة البرنامج الرئيسية، انقر فوق **المساعدة والدعم** > **الدعم الفني**.

الاتصال بالدعم الفني

طلب الدعم – إذا تعذر عليك العثور على إجابة لمشكلتك، فيمكنك استخدام هذا النموذج الموجود على موقع ويب ESET للاتصال بسرعة بقسم الدعم الفني من ESET. استناداً إلى إعداداتك، يتم عرض نافذة إرسال بيانات تكوين النظام قبل ملء نموذج الويب.

الحصول على معلومات للدعم الفني

تفاصيل الدعم الفني – عند مطالبتك، يمكنك نسخ المعلومات وإرسالها إلى الدعم الفني من ESET (مثل تفاصيل الاشتراك واسم المنتج وإصدار المنتج ونظام التشغيل ومعلومات جهاز الكمبيوتر).

ESET Log Collector – ارتباطات إلى مقالة قاعدة معارف ESET، يمكنك منها تنزيل أداة ESET Log Collector وهي تطبيق يجمع معلومات وسجلات من كمبيوتر تلقائياً للمساعدة في حل المشكلات بسرعة أكبر. لمزيد من المعلومات، راجع دليل مستخدم ESET Log Collector عبر الإنترنت.

قم بتمكين التسجيل المتقدم لإنشاء سجلات متقدمة لجميع الميزات المتوفرة لمساعدة المطورين في تشخيص المشكلات وحلها. يتم تعيين أدنى شرح تفصيلي على مستوى **التشخيص**. سيتم تعطيل التسجيل المتقدم تلقائياً بعد ساعتين، ما لم توقفه قبل ذلك بالنقر فوق **إيقاف التسجيل المتقدم**. عند إنشاء السجلات، يتم عرض نافذة الإشعار التي توفر الوصول المباشر إلى مجلد "التشخيص" الموجود به السجلات التي تم إنشاؤها.

حساب ESET HOME

يمكنك مراجعة ESET HOME حالة اتصال الحساب في نافذة البرنامج الرئيسية > **حساب ESET HOME**.

هذا الجهاز غير متصل بحساب ESET HOME

انقر فوق الاتصال بـ ESET HOME لتوصيل جهازك بـ ESET HOME وإدارة اشتراكاتك والأجهزة المحمية. يمكنك تجديد الاشتراك أو ترقيته أو تمديده وعرض التفاصيل المهمة. في بوابة إدارة ESET HOME أو تطبيق الهاتف المحمول، يمكنك إضافة اشتراكات المختلفة وتنزيل المنتجات على أجهزتك والتحقق من حالة أمان المنتج أو مشاركة اشتراك عبر البريد الإلكتروني. لمزيد من المعلومات، تفضل بزيارة التعليمات عبر الإنترنت في ESET HOME.

هذا الجهاز متصل بحساب ESET HOME

يمكنك إدارة أمان جهازك عن بُعد باستخدام بوابة ESET HOME أو تطبيق الهاتف المحمول. انقر فوق **App Store** أو **Google Play** لعرض رمز QR الذي يمكنك مسحه ضوئياً باستخدام هاتفك المحمول لتنزيل تطبيق الهاتف المحمول لـ ESET HOME من App Store أو Google Play.

حساب ESET HOME—اسم حساب ESET HOME الخاص بك.

اسم الجهاز—اسم هذا الجهاز المعروض في حساب ESET HOME.

فتح ESET HOME—يفتح بوابة إدارة ESET HOME.

لقطع اتصال جهازك من حساب ESET HOME الخاص بك، انقر فوق **قطع الاتصال من ESET HOME** > **قطع الاتصال**. سيظل الاشتراك المستخدم للتنشيط نشطاً، وستتم حماية جهازك.

الاتصال بـ ESET HOME

قم بتوصيل جهازك بـ ESET HOME لعرض وإدارة جميع اشتراكات وأجهزة ESET التي تم تنشيطها. يمكنك تجديد الاشتراك أو ترقيته أو تمديده وعرض تفاصيل الاشتراك المهمة. في بوابة إدارة ESET HOME أو تطبيق الهاتف المحمول، يمكنك إضافة الاشتراكات المختلفة وتنزيل المنتجات على أجهزتك والتحقق من حالة أمان المنتج أو مشاركة الاشتراكات عبر البريد الإلكتروني. لمزيد من المعلومات، تفضل بزيارة التعليمات عبر الإنترنت في ESET HOME.

توصيل جهازك بـ ESET HOME:

> إذا كنت متصل بـ ESET HOME أثناء التثبيت أو عند تحديد **استخدام حساب ESET HOME** كطريقة تنشيط، فاتبع التعليمات الواردة في موضوع استخدام حساب ESET HOME.
> إذا قمت بالفعل بتثبيت وتنشيط ESET Internet Security باستخدام اشتراك مضاف في حساب ESET HOME لديك، فيمكنك توصيل جهازك بـ ESET HOME باستخدام بوابة ESET HOME. اتبع التعليمات الواردة في دليل ESET HOME المساعدة عبر الإنترنت واسمح بالاتصال في ESET Internet Security.

1. في نافذة البرنامج الرئيسية، انقر فوق **حساب ESET HOME** > **توصيل بـ ESET HOME** أو انقر فوق **توصيل بـ ESET HOME** في **توصيل هذا الجهاز بإعلام حساب** ESET HOME.
2. سجّل الدخول إلى حساب ESET HOME.

> إذا لم يكن لديك حساب ESET HOME فانقر فوق **إنشاء حساب** للتسجيل أو اطلع على الإرشادات في تعليمات ESET HOME عبر الإنترنت.
> إذا نسيت كلمة المرور، فانقر فوق **نسيت كلمة المرور** واتبع الخطوات التي تظهر على الشاشة أو راجع الإرشادات في تعليمات ESET HOME عبر الإنترنت.

3. قم بتعيين **اسم جهاز** وانقر فوق **متابعة**.
4. بعد اتصال ناجح، يتم عرض نافذة تفاصيل. انقر فوق **تم**.

تسجيل الدخول إلى ESET HOME

ثمة عدة طرق متوفرة لتسجيل الدخول إلى حساب ESET HOME:

- **استخدم عنوان البريد الإلكتروني وكلمة المرور لـESET HOME** – اكتب **عنوان البريد الإلكتروني** و**كلمة المرور** الذين استخدمتهما لإنشاء حساب ESET HOME وانقر فوق **تسجيل الدخول**.
- **استخدم حساب Google/AppleID** – انقر فوق **المتابعة باستخدام Google** أو **المتابعة باستخدام Apple** وقم بتسجيل الدخول إلى الحساب المناسب. بعد نجاح تسجيل الدخول، ستتم إعادة توجيهك إلى صفحة الويب لتأكيد ESET HOME. للمتابعة، قم بالتبديل مرة أخرى إلى نافذة منتج ESET. لمزيد من المعلومات حول حساب Google/تسجيل الدخول إلىAppleID، راجع التعليمات في التعليمات عبر الإنترنت ESET HOME.
- **مسح رمز QR ضوئياً** – انقر فوق **مسح رمز QR ضوئياً** لعرض رمز QR. افتح تطبيق ESET HOME للهاتف المحمول وامسح رمز QR أو وجّه كاميرا جهازك إلى رمز QR. لمزيد من المعلومات، راجع التعليمات في التعليمات عبر الإنترنت ESET HOME.

> إذا لم يكن لديك حساب ESET HOME فانقر فوق **إنشاء حساب** للتسجيل أو اطلع على الإرشادات في تعليمات ESET HOME عبر الإنترنت.
> إذا نسيت كلمة المرور، فانقر فوق **نسيت كلمة المرور** واتبع الخطوات التي تظهر على الشاشة أو راجع الإرشادات في تعليمات ESET HOME عبر الإنترنت.

فشل تسجيل الدخول – الأخطاء الشائعة.

فشل تسجيل الدخول – الأخطاء الشائعة

تعذّر علينا العثور على حساب يطابق عنوان البريد الإلكتروني الذي تم إدخاله

لا يتطابق عنوان البريد الإلكتروني الذين أدخلته مع أي حساب ESET HOME. انقر فوق **رجوع** واكتب عنوان البريد الإلكتروني وكلمة المرور الصحيحين.

لتسجيل الدخول، يجب عليك إنشاء حساب ESET HOME. إذا لم يكن لديك حساب ESET HOME فانقر فوق **رجوع** > **إنشاء حساب** أو راجع إنشاء حساب ESET HOME جديد.

لا يتطابق اسم المستخدم وكلمة المرور

لا تتطابق كلمة المرور التي تمت كتابتها مع عنوان البريد الإلكتروني الذي تم إدخاله. انقر فوق **السابق**، واكتب كلمة المرور الصحيحة وتحقق من صحة عنوان البريد الإلكتروني المكتوب. إذا كان لا يزال يتعذّر عليك تسجيل الدخول, فانقر فوق **رجوع** > **نسيت كلمة المرور** لإعادة تعيين كلمة المرور واتبع الخطوات التي تظهر على الشاشة أو راجع نسيت كلمة مرور ESET HOME.

لا يتطابق خيار تسجيل الدخول المحدد مع حسابك

حسابك مرتبط بحساب الوسائط الاجتماعية لديك. لتسجيل الدخول إلى ESET HOME انقر فوق **المتابعة باستخدام Google** أو **المتابعة باستخدام Apple** وقم بتسجيل الدخول إلى الحساب المناسب. بعد نجاح تسجيل الدخول، ستتم إعادة توجيهك إلى صفحة الويب لتأكيد ESET HOME. يمكنك فصل حساب الوسائط الاجتماعية لديك عن حساب ESET HOME على بوابة ESET HOME.

كلمة المرور خاطئة

يمكن أن يحدث هذا الخطأ إذا كان ESET Internet Security متصلاً بالفعل بـ ESET HOME وكنت تجري تغييرات تتطلب منك تسجيل الدخول (على سبيل المثال، تعطيل Anti-Theft) وكلمة المرور التي أدخلتها لا تتطابق مع حسابك. انقر فوق **رجوع** واكتب كلمة المرور الصحيحة. إذا كان لا يزال يتعذّر عليك تسجيل الدخول, فانقر فوق **رجوع** > **نسيت كلمة المرور** لإعادة تعيين كلمة المرور واتبع الخطوات التي تظهر على الشاشة أو راجع نسيت كلمة مرور ESET HOME.

إضافة جهاز إلى ESET HOME

إذا قمت بالفعل بتثبيت وتنشيط ESET Internet Security باستخدام اشتراك مضاف في حساب ESET HOME لديك، فيمكنك توصيل جهازك بـ ESET HOME باستخدام بوابة ESET HOME:

1. أرسل طلب اتصال إلى جهازك.
2. يعرض ESET Internet Security **توصيل هذا الجهاز بنافذة مربع حوار حساب ESET HOME** باستخدام اسم حساب ESET HOME. انقر فوق **السماح** لتوصيل الجهاز بحساب ESET HOME المشار إليه.

إذا لم يحدث تفاعل، فسيتم إلغاء طلب الاتصال تلقائياً بعد حوالي 30 دقيقة.

الإعداد المتقدم

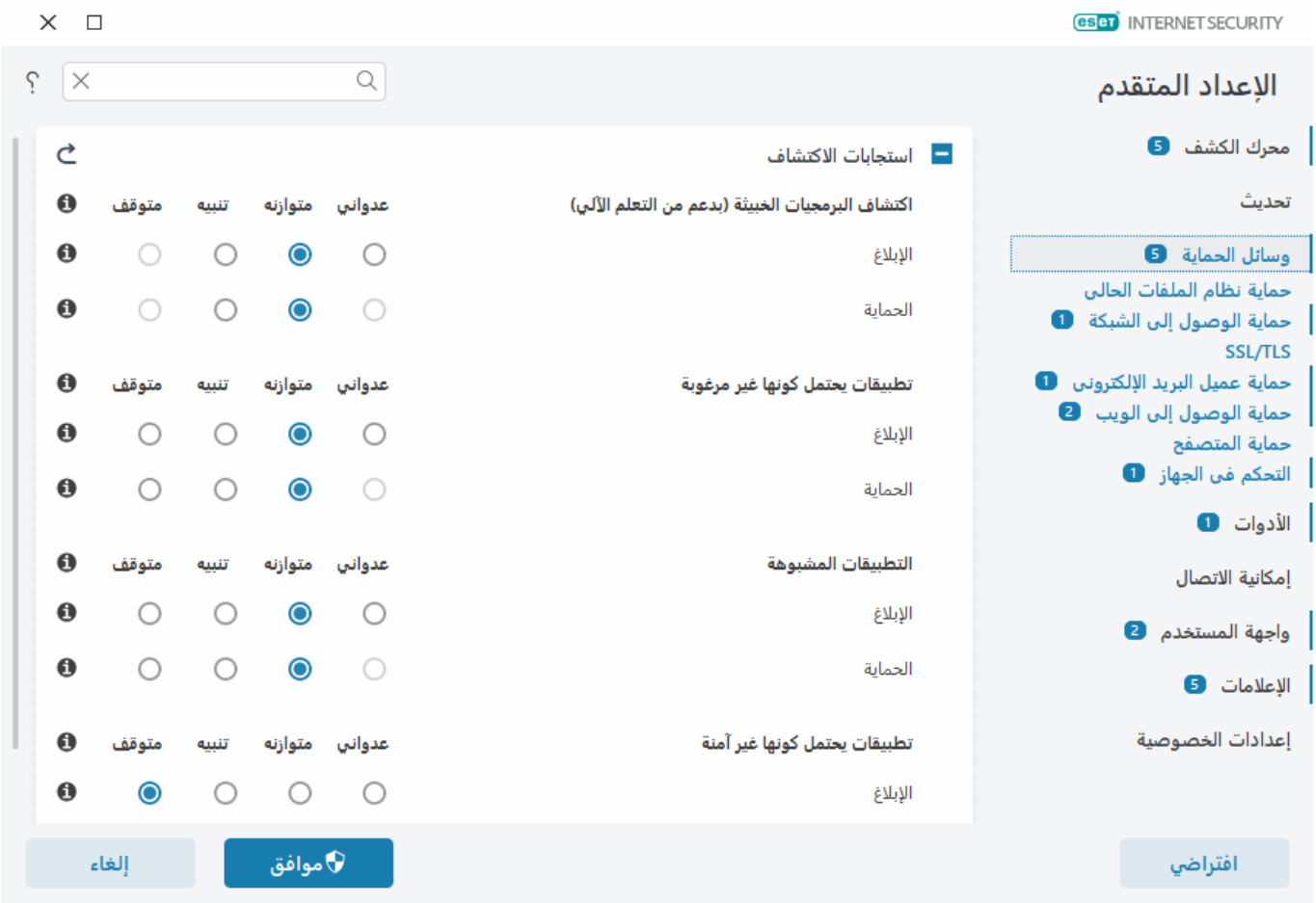
يتيح لك الإعداد المتقدم تهيئة الإعدادات التفصيلية ESET Internet Security لتناسب احتياجاتك.

لفتح الإعداد المتقدم، افتح نافذة البرنامج الرئيسية واضغط المفتاح **F5** على لوحة المفاتيح أو انقر فوق **إعداد** > **الإعداد المتقدم**.

استناداً إلى إعداد Access، قد تتم مطالبتك بكتابة كلمة مرور لفتح الإعداد المتقدم.

في الإعداد المتقدم، يمكنك تكوين الإعدادات التالية:

- محرك الكشف
- تحديث
- وسائل الحماية
- الأدوات
- إمكانية الاتصال
- واجهة المستخدم
- الإعلامات
- إعدادات الخصوصية



محرك الكشف

يتيح لكالإعداد المتقدم > **محرك الكشف** تكوين الخيارات التالية:

- الاستبعادات
- خيارات متقدمة
- أداة فحص حركة نقل البيانات عبر الشبكة

الاستبعادات

تتيح لك **الاستبعادات** استبعاد الكائنات من محرك الكشف. لضمان فحص جميع الكائنات، يوصى بعدم إنشاء استبعادات إلا عندما تكون ضرورية مطلقاً. ومن المواقف التي يمكنك فيها استبعاد كائن من الفحص، على سبيل المثال فحص إدخالات قاعدة بيانات كبيرة قد يؤدي إلى إبطاء جهاز الكمبيوتر خلال الفحص، أو برنامج يتعارض مع الفحص.

استبعادات الأداء ـ استبعاد الملفات والمجلدات من الفحص. تعد استثناءات الأداء مفيدة لاستبعاد الفحص على مستوى الملفات لتطبيقات الألعاب أو عند التسبب في سلوك غير طبيعي للنظام أو زيادة في الأداء.

تسمح لك استبعادات الاكتشاف باستبعاد الكائنات من الاكتشاف باستخدام اسم الكشف أو المسار أو التجزئة الخاصة به. لا تستبعد استبعادات الاكتشاف الملفات والمجلدات من الفحص كما تفعل استبعادات الأداء. تستبعد استبعادات الاكتشاف الكائنات

فقط عندما يتم الكشف عنها بواسطة محرك الاكتشاف وتكون القاعدة المناسبة موجودة في قائمة الاستبعاد.

يجب عدم الخلط بينه وبين أنواع الاستبعادات الأخرى:

- استبعادات الاكتشاف – يتم استبعاد جميع عمليات الملفات المنسوبة إلى عمليات التطبيق المستبعدة من الفحص (قد تكون هناك حاجة لتحسين سرعة النسخ الاحتياطي وتوافر الخدمة).
- ملحقات الملفات المستبعدة
- استبعادات HIPS
- عامل تصفية الاستبعاد للحماية المستندة إلى السحابة.

استبعادات الأداء

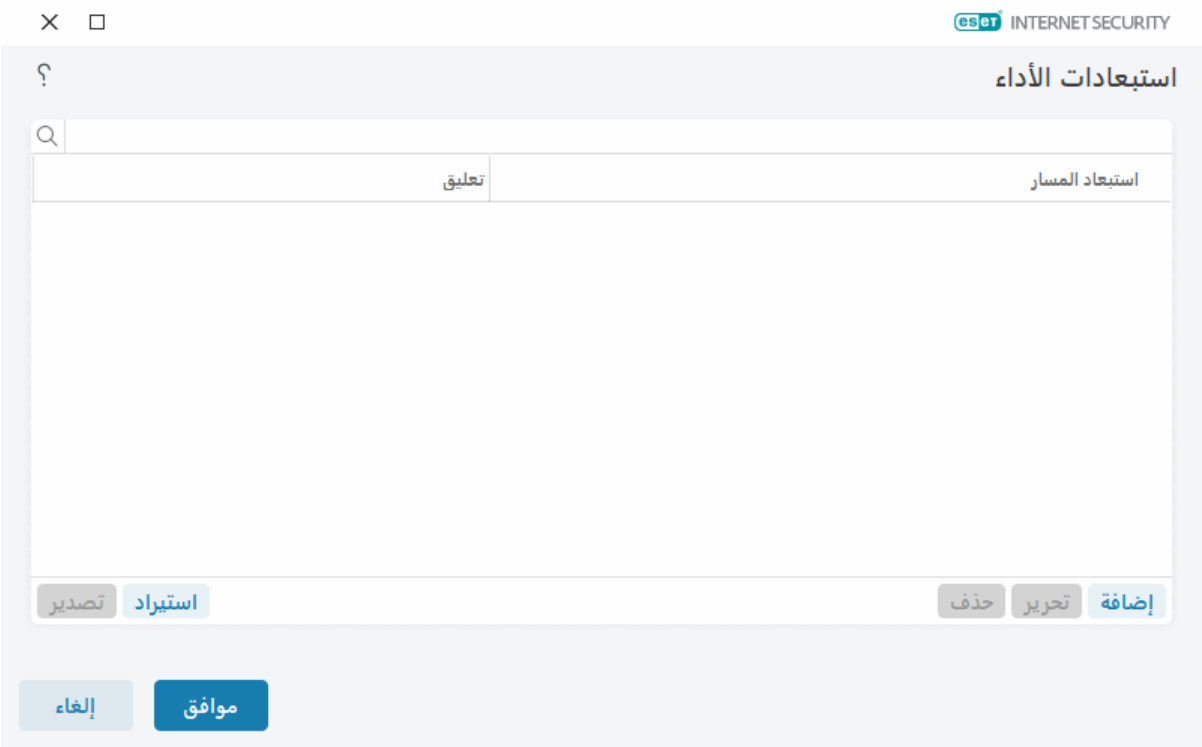
تسمح لك استبعادات الأداء باستبعاد الملفات والمجلدات من الفحص.

لضمان فحص جميع الكائنات بحثاً عن تهديدات، نوصي بإنشاء استبعادات الأداء فقط عندما يكون ذلك ضرورياً للغاية. ومع ذلك، هناك حالات قد تحتاج فيها إلى استثناء كائن، على سبيل المثال، إدخالات قاعدة البيانات الكبيرة التي من شأنها أن تبطئ جهاز الكمبيوتر الخاص بك أثناء الفحص أو البرنامج الذي يتعارض مع الفحص.

يمكنك إضافة الملفات والمجلدات التي سيتم استثنائها من الفحص إلى قائمة الاستثناءات عبر الإعداد المتقدم > **محرك الكشف** > **الاستثناءات** > **استثناءات الأداء** > **تحرير**.

> لا تخلط بين استثناءات الاكتشاف، أو امتدادات الملف المستثنى، أو استثناءات نظام منع اختراق المضيف (HIPS) أو استثناءات العمليات.

لاستثناء كائن (المسار: ملف أو مجلد) من الفحص، انقر فوق **إضافة** وأدخل المسار المناسب أو حدده في بنية الشجرة.



لن يتم اكتشاف أي تهديد داخل ملف بواسطة وحدة **حماية نظام الملفات في الوقت الفعلي** أو وحدة **فحص الكمبيوتر** إذا استوفى ذلك الملف معايير الاستبعاد من الفحص.

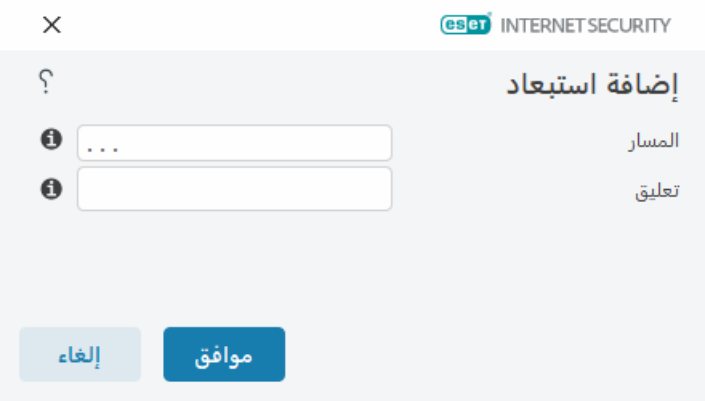
عناصر التحكم

- **إضافة** – استبعاد الكائنات من الاكتشاف.
- **تحرير** – يتيح لك تحرير إدخالات محددة.
- **حذف** – إزالة إدخالات محددة (CTRL + انقر لتحديد العديد من الإدخالات).

إضافة استثناء أداء أو تحريره

تستثني نافذة مربع الحوار هذا مساراً محدداً (ملف أو دليل) لجهاز الكمبيوتر هذا.

اختر المسار أو أدخله يدوياً
لاختيار مسار مناسب، انقر فوق **...** في حقل **المسار**.
عند الكتابة يدوياً، اطلع على مزيد من أمثلة تنسيق الاستثناءات أدناه.



يمكنك استخدام أحرف البدل لاستبعاد مجموعة من الملفات. تمثل علامة الاستفهام (?) حرفاً واحداً، بينما تمثل العلامة النجمية (*) سلسلة لا تحتوي على أحرف أو تحتوي على حرف أو أكثر.

تنسيق الاستبعادات

• إذا كنت تريد استبعاد جميع الملفات والمجلدات الفرعية الموجودة بمجلد، فاكتب المسار إلى المجلد واستخدم القناع *
• إذا كنت تريد استبعاد ملفات doc فقط، فاستخدم القناع *.doc
• إذا كان اسم ملف تنفيذي يحتوي على عدد أحرف معين (بأحرف مختلفة)، وليست لديك معرفة مؤكدة سوى بالحرف الأول (على سبيل المثال "D"⍰) فاستخدم التنسيق التالي:
D????.exe (تحل علامات الاستفهام محل الأحرف غير الموجودة/غير المعروفة)
أمثلة:
• C:\Tools* – يجب أن ينتهي المسار بخط مائل عكسي (\) وعلامة نجمة (*) للإشارة إلى أنه مجلد وسيتم استبعاد جميع محتوى المجلد (الملفات والمجلدات الفرعية).
• C:\Tools*.* – نفس سلوك C:\Tools*
• C:\Tools – لن يتم استبعاد المجلد Tools. من منظور الفاحص، يمكن أن يكون Tools أيضاً اسم ملف.
• C:\Tools*.dat – سيؤدي هذا إلى استبعاد ملفات .dat في المجلد Tools.
• C:\Tools\sg.dat – سيقوم باستبعاد هذا الملف المعين الذي يوجد في المسار الدقيق.

متغيرات النظام في الاستبعادات

يمكنك استخدام متغيرات النظام مثل %PROGRAMFILES% لتحديد استبعادات الفحص.
• لاستبعاد مجلد ملفات البرنامج باستخدام متغير النظام، استخدم المسار %PROGRAMFILES%* (تذكر إضافة شرطة مائلة وعلامة نجمة في نهاية المسار) عند الإضافة إلى الاستبعادات.
• لاستبعاد جميع الملفات والمجلدات الموجودة في الدليل الفرعي %PROGRAMFILES%، استخدم المسار %PROGRAMFILES%\Excluded_Directory*

توسيع قائمة متغيرات النظام المدعومة

يمكن استخدام المتغيرات التالية بتنسيق استبعاد المسار:
• %ALLUSERSPROFILE%
• %COMMONPROGRAMFILES%
• %COMMONPROGRAMFILES(X86)%
• %COMSPEC%
• %PROGRAMFILES%
• %PROGRAMFILES(X86)%
• %SystemDrive%
• %SystemRoot%
• %WINDIR%
• %PUBLIC%
تُعد متغيرات النظام الخاصة بالمستخدم (مثل %TEMP% أو %USERPROFILE%) أو متغيرات البيئة (مثل %PATH%) غير مدعومة.

أحرف البدل في منتصف المسار ليست مدعومة

قد يعمل استخدام أحرف البدل في منتصف المسار (على سبيل المثال C:\Tools*\Data\file.dat) ولكنه غير مدعوم رسمياً لاستثناءات الأداء.
ليس هناك قيود لاستخدام بطاقات البدل في وسط المسار عند استخدام استبعادات الاكتشاف.

ترتيب الاستبعادات

• لا توجد خيارات لضبط مستوى أولوية الاستبعادات باستخدام الأزرار العلوية / السفلية (كما في قواعد جدار الحماية حيث يتم تنفيذ القواعد من أعلى إلى أسفل).
• عندما تتطابق القاعدة الأولى القابلة للتطبيق من خلال الفحص، فلن يتم تقييم القاعدة الثانية القابلة للتطبيق.
• كلما قل عدد القواعد، كان أداء الفحص أفضل.
• تجنب إنشاء قواعد متزامنة.

تنسيق استبعاد المسار

يمكنك استخدام أحرف البدل لاستبعاد مجموعة من الملفات. تمثل علامة الاستفهام (?) حرفاً واحداً، بينما تمثل العلامة النجمية (*) سلسلة لا تحتوي على أحرف أو تحتوي على حرف أو أكثر.

تنسيق الاستبعادات

• إذا كنت تريد استبعاد جميع الملفات والمجلدات الفرعية الموجودة بمجلد، فاكتب المسار إلى المجلد واستخدم القناع *
• إذا كنت تريد استبعاد ملفات doc فقط، فاستخدم القناع *.doc
• إذا كان اسم ملف تنفيذي يحتوي على عدد أحرف معين (بأحرف مختلفة)، وليست لديك معرفة مؤكدة سوى بالحرف الأول (على سبيل المثال "D")، فاستخدم التنسيق التالي:
D????.exe (تحل علامات الاستفهام محل الأحرف غير الموجودة/غير المعروفة)
أمثلة:
• C:\Tools* – يجب أن ينتهي المسار بخط مائل عكسي (\) وعلامة نجمة (*) للإشارة إلى أنه مجلد وسيتم استبعاد جميع محتوى المجلد (الملفات والمجلدات الفرعية).
• C:\Tools*.* – نفس سلوك C:\Tools*
• C:\Tools – لن يتم استبعاد المجلد Tools. من منظور الفاحص، يمكن أن يكون Tools أيضاً اسم ملف.
• C:\Tools*.dat – سيؤدي هذا إلى استبعاد ملفات .dat في المجلد Tools.
• C:\Tools\sg.dat – سيقوم باستبعاد هذا الملف المعين الذي يوجد في المسار الدقيق.

متغيرات النظام في الاستبعادات

يمكنك استخدام متغيرات النظام مثل %PROGRAMFILES% لتحديد استبعادات الفحص.
• لاستبعاد مجلد ملفات البرنامج باستخدام متغير النظام، استخدم المسار %PROGRAMFILES%* (تذكر إضافة شرطة مائلة وعلامة نجمة في نهاية المسار) عند الإضافة إلى الاستبعادات.
• لاستبعاد جميع الملفات والمجلدات الموجودة في الدليل الفرعي %PROGRAMFILES%، استخدم المسار %PROGRAMFILES%\Excluded_Directory*

توسيع قائمة متغيرات النظام المدعومة

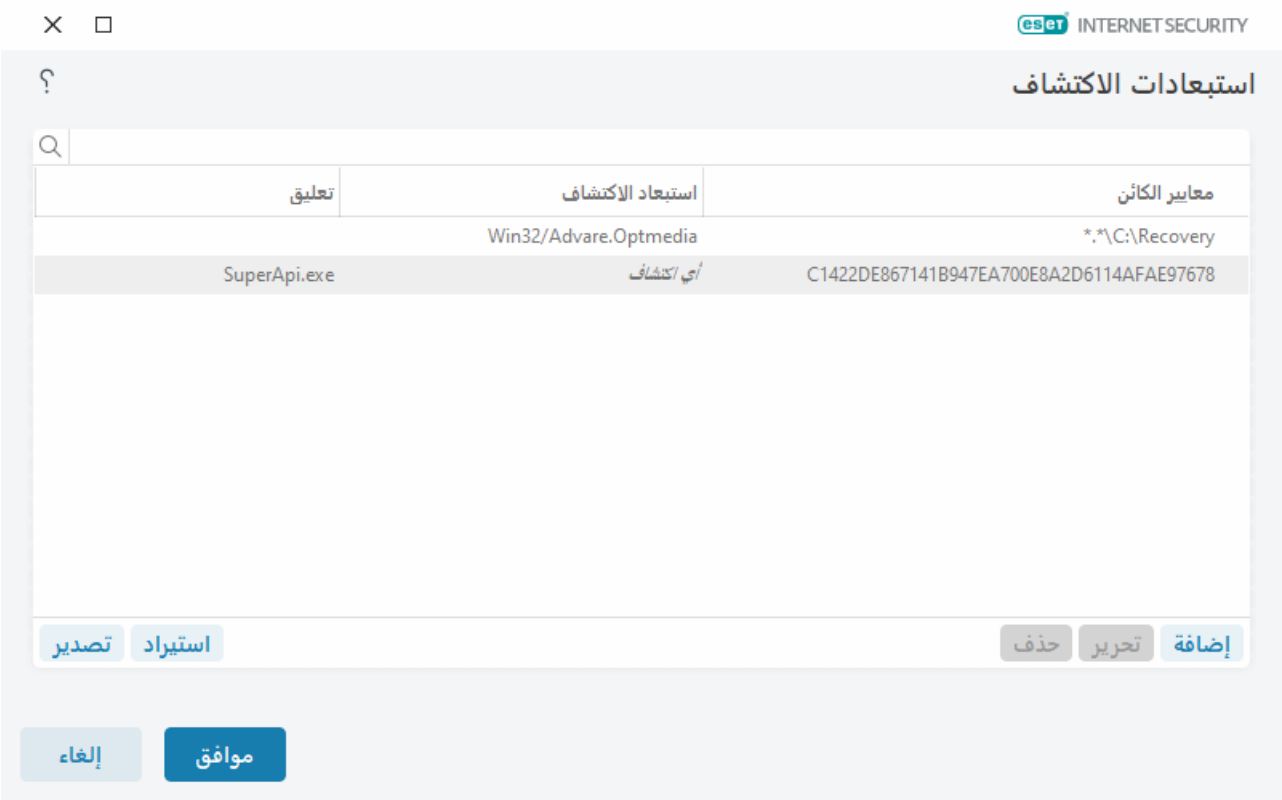
يمكن استخدام المتغيرات التالية بتنسيق استبعاد المسار:
• %ALLUSERSPROFILE%
• %COMMONPROGRAMFILES%
• %COMMONPROGRAMFILES(X86)%
• %COMSPEC%
• %PROGRAMFILES%
• %PROGRAMFILES(X86)%
• %SystemDrive%
• %SystemRoot%
• %WINDIR%
• %PUBLIC%
تُعد متغيرات النظام الخاصة بالمستخدم (مثل %TEMP% أو %USERPROFILE%) أو متغيرات البيئة (مثل %PATH%) غير مدعومة.

استبعادات الاكتشاف

تسمح لك استبعادات الاكتشاف باستبعاد الكائنات من الاكتشاف عن طريق تصفية اسم الكشف أو مسار الكائن أو التجزئة الخاصة به.

كيف تعمل استبعادات الاكتشاف

لا تستبعد استبعادات الاكتشاف الكشف الملفات والمجلدات من الفحص كما تفعل استبعادات الأداء. تستبعد استبعادات الاكتشاف الكائنات فقط عندما يتم الكشف عنها بواسطة محرك الاكتشاف وتكون القاعدة المناسبة موجودة في قائمة الاستبعاد.
على سبيل المثال (انظر الصف الأول في الصورة أدناه)، عندما يتم اكتشاف كائن باسم Win32/Adware.Optmedia ويكون الملف المكتشف هو C:\Recovery\file.exe. في الصف الثاني، سيتم دائماً استبعاد كل ملف يحتوي على علامة التجزئة SHA-1 المناسبة، على الرغم من اسم الكشف.



لضمان اكتشاف جميع التهديدات، نوصي بإنشاء استبعادات الاكتشاف فقط عند الضرورة القصوى.

لإضافة ملفات ومجلدات إلى قائمة الاستثناءات، انتقل إلى الإعداد المتقدم > **محرك الكشف** > **الاستثناءات** > **استثناءات الاكتشاف** > **تحرير**.

> لا تخلط بين استثناءات الأداء، أو امتدادات الملف المستثنى، أو استثناءات نظام منع اختراق المضيف (HIPS) أو استثناءات العمليات.

لاستبعاد كائن (بحسب اسم الكشف أو التجزئة) من محرك الكشف، انقر فوق **إضافة**.

بخصوص التطبيقات المحتمل كونها غير مرغوب فيها والتطبيقات المحتمل كونها غير آمنة، يمكن أيضاً إنشاء الاستبعاد باسم الكشف الخاص به:

- في نافذة التنبيه الإبلاغ عن الكشف (انقر فوق **عرض الخيارات المتقدمة** ثم حدد **استبعاد من الكشف**).
- من القائمة السياقية لملفات السجل باستخدام إنشاء معالج استبعاد الاكتشاف.
- بالنقر فوق **الأدوات** > **العزل** ثم النقر بزر الماوس الأيمن فوق الملف المعزول وتحديد **استعادة واستبعاد من الفحص** من القائمة السياقية.

اكتشاف معايير كائنات الاستبعادات

- **المسار** – الحد من استبعاد الكشف لمسار محدد (أو أي مسار).
- **اسم الكشف** – إذا كان هناك اسم للكشف بجوار ملف مستبعد، فهذا يعني أن الملف مستبعد فقط للاكتشاف المحدد، وليس بالكامل. إذا أصبح هذا الملف مصاباً فيما بعد ببرمجيات خبيثة أخرى، فسيتم اكتشافه.
- **تجزئة** – استثناء ملف استناداً إلى التجزئة المحددة (SHA-1), بغض النظر عن نوع الملف أو الموقع أو الاسم أو الامتداد.

إضافة استثناء اكتشاف أو تحريره

استبعاد الاكتشاف

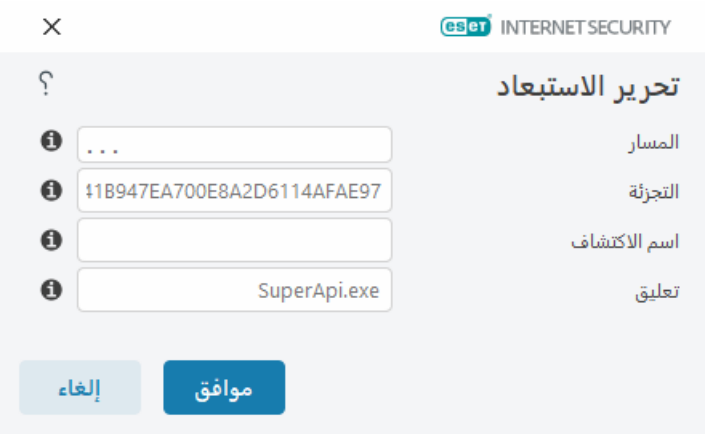
ينبغي تقديم اسم اكتشاف صالحاً لـ ESET. بالنسبة لاسم اكتشاف صالح، اطلع على ملفات السجل ثم حدد **الاكتشافات** من القائمة المنسدلة لملفات السجل. يُعد هذا مفيداً عند اكتشاف عينة موجبة في ESET Internet Security. تُعد استثناءات عمليات التسلل الحقيقية خطيرة جداً، فكر في استثناء الملفات / الدلائل المصابة فقط بالنقر فوق **...** في حقل **قناع المسار** و/أو فقط لفترة زمنية مؤقتة. تنطبق الاستثناءات أيضاً على التطبيقات المحتملة أن تكون غير مرغوب فيها، والتطبيقات المحتملة كونها غير آمنة والتطبيقات المريبة.

راجع أيضاً تنسيق مسار الاستبعاد.

راجع مثال على استبعادات الاكتشاف أدناه.

استبعاد التجزئة

استثناء ملف استناداً إلى التجزئة المحددة (SHA-1), بغض النظر عن نوع الملف أو الموقع أو الاسم أو الامتداد.



الاستثناءات حسب اسم الاكتشاف
لاستثناء اكتشاف محدد حسب الاسم، أدخل اسم اكتشاف صالحاً:
Win32/Adware.Optmedia
يمكنك أيضاً استخدام التنسيق التالي عندما تقوم باستبعاد اكتشاف من نافذة تنبيه ESET Internet Security:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

عناصر التحكم

- **إضافة** – استبعاد الكائنات من الاكتشاف.
- **تحرير** – يتيح لك تحرير إدخالات محددة.
- **حذف** – إزالة إدخالات محددة (CTRL + انقر لتحديد العديد من الإدخالات).

إنشاء معالج استبعاد الاكتشاف

يمكن أيضاً إنشاء استبعاد الاكتشاف من قائمة سياق ملفات السجل (غير متوفر لاكتشافات البرامج الضارة):

1. في نافذة البرنامج الرئيسي، انقر فوق **أدوات** > **ملفات السجل**.
2. انقر بزر الماوس الأيمن فوق الكشف في **سجل الاكتشافات**.
3. انقر فوق **إنشاء استبعاد**.

لاستبعاد اكتشاف واحد أو أكثر بناءً على **معايير الاستبعاد**، انقر فوق **معايير التغيير**:

- **الملفات المحددة** – استثناء كل ملف بحسب علامة التجزئة SHA-1.
- **الاكتشاف**استثناء كل ملف بحسب اسم الاكتشاف الخاص به.
- **المسار + الاكتشاف**استثناء كل ملف بحسب اسم الاكتشاف والمسار، بما في ذلك اسم الملف (على سبيل المثال *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

يتم تحديد الخيار الموصى به مسبقاً استناداً إلى نوع الاكتشاف.

اختيارياً، يمكنك إضافة **تعليق** قبل النقر فوق **إنشاء استبعاد**.

كشف محرك الخيارات المتقدمة

تمكين المسح المتقدم عبر AMSI – هو أداة واجهة Microsoft Antimalware Scan التي تسمح بمسح البرامج النصية لبرنامج PowerShell والبرامج النصية التي ينفذها Windows Script Host والبيانات الممسوحة ضوئياً باستخدام AMSI SDK.

أداة فحص حركة نقل البيانات عبر الشبكة

توفر أداة فحص حركة مرور الشبكة الحماية من البرامج الضارة لبروتوكولات التطبيقات، والتي تدمج العديد من تقنيات فحص البرامج الضارة المتقدمة. تقوم أداة فحص حركة مرور الشبكة بفحص بروتوكولات HTTP (S) وPOP3 (S) وIMAP (S) تلقائياً، بغض النظر عن متصفح الإنترنت أو عميل البريد الإلكتروني. يمكنك تمكين أو تعطيل أداة فحص حركة مرور الشبكة في الإعداد المتقدم > **محرك الكشف** > **أداة فحص حركة مرور الشبكة**.

تمكين أداة فحص حركة مرور الشبكة—إذا قمت بتعطيل هذا الخيار، فلن يتم فحص بروتوكولات HTTP (S) وPOP3 (S) وIMAP (S)). لاحظ أن ESET Internet Security الميزات التالية تتطلب تمكين أداة فحص حركة مرور الشبكة:

- حماية استخدام الإنترنت
- المراقبة الأبوية
- خصوصية وأمان المتصفح
- التصفح المصرفي الآمن
- SSL/TLS
- حماية مضادة للتصيد الاحتيالي
- حماية عميل البريد الإلكتروني

الحماية المستندة إلى السحابة

بفضل اعتماده على نظام التحذير المبكر المتقدم ThreatSense.Net يستخدم ESET LiveGrid® البيانات التي أرسلها مستخدمو ESET في جميع أنحاء العالم ويُرسلها إلى مختبر الأبحاث التابع لشركة ESET. عبر تقديم عينات مريبة وبيانات تعريف من كل مكان، يتيح ESET LiveGrid® لنا الاستجابة الفورية لاحتياجات عملائنا والإبقاء على سرعة استجابة ESET لأحدث التهديدات.

تتوفر الخيارات التالية:

تمكين نظام السمعة من ESET LiveGrid®

يوفر نظام سمعة ESET LiveGrid® القوائم البيضاء والقوائم السوداء المستندة إلى السحابة.

يمكن أن يفحص المستخدمون سمعة العمليات الجارية والملفات مباشرة من واجهة البرنامج أو من القائمة السياقية مع معلومات إضافية متوفرة من ESET LiveGrid®.

تمكين نظام الملاحظات من ESET LiveGrid®

بالإضافة إلى نظام سمعة ESET LiveGrid® سيقوم نظام ملاحظات ESET LiveGrid® بجمع معلومات حول جهاز الكمبيوتر متعلقة بالتهديدات المكتشفة حديثاً. قد تشمل هذه المعلومات ما يلي:

- عينة أو نسخة من الملف الذي ظهر فيه التهديد
- المسار إلى الملف

- اسم الملف
- التاريخ والوقت
- العملية التي أدت إلى ظهور التهديد على جهاز الكمبيوتر
- معلومات حول نظام تشغيل جهاز الكمبيوتر

افتراضياً، يكون ESET Internet Security مكوناً لإرسال الملفات المريبة لتحليلها بشكل تفصيلي إلى مختبر مكافحة الفيروسات التابع لشركة ESET. يتم دائماً استبعاد الملفات ذات امتدادات معينة مثل *doc.* أو *xls.*. يمكنك أيضاً إضافة امتدادات أخرى في حالة وجود ملفات أخرى معينة، تريد أو تريد مؤسستك عدم إرسالها.

اقرأ المزيد حول إرسال البيانات ذات الصلة في سياسة الخصوصية.

يمكنك اختيار عدم تمكين ESET LiveGrid®

لن تفقد أي وظيفة في البرنامج، ولكن في بعض الحالات، قد يستجيب ESET Internet Security لتهديدات جديدة بشكل أسرع عند تمكين ESET LiveGrid®. إذا استخدمت ESET LiveGrid® من قبل وقمت بتعطيله، فقد تكون هناك حزم بيانات ما زالت موجودة لإرسالها. وحتى بعد إلغاء التنشيط، سيتم إرسال هذه الحزم إلى ESET. بمجرد إرسال جميع المعلومات الحالية، لن يتم إنشاء أي حزم أخرى.

اقرأ المزيد عن ESET LiveGrid® في المسرد.
اطلع على الإرشادات المشروحة باللغة الإنجليزية وغيرها من العديد من اللغات حول تمكين ESET LiveGrid® أو تعطيله في ESET Internet Security.

تكوين الحماية المستندة إلى السحابة في الإعداد المتقدم

للوصول إلى الإعدادات لـ ESET LiveGuard افتح الإعداد المتقدم > **محرك الكشف** > **الحماية المستندة إلى السحابة**.

- **تمكين نظام سمعة ESET LiveGrid® (مستحسن)** – يحسّن نظام سمعة ESET LiveGrid® فعالية حلول الحماية ضد البرامج الضارة من ESET بمقارنة الملفات التي تم فحصها بقاعدة بيانات تضم عناصر بقوائم بيضاء وسوداء في السحابة.
- **تمكين ESET LiveGrid® نظام الملاحظات** – يرسل بيانات التقديم ذات الصلة (الموضحة في **قسم تقديم العينات** أدناه) إلى جانب تقارير وإحصائيات الأعطال إلى مختبر ESET Research لمزيد من التحليل.
- **تقديم تقارير الأعطال وبيانات التشخيص** – إرسال بيانات تشخيص ذات الصلة ESET LiveGrid® مثل تقارير الأعطال ومكبات الذاكرة الخاصة بالوحدات النمطية. نوصي بإتاحة تمكينه لمساعدة ESET في تشخيص المشكلات وتحسين المنتجات وضمان حماية أفضل للمستخدم النهائي.
- **إرسال إحصائيات مجهَّلة** – السماح لـ ESET بجمع معلومات حول التهديدات المكتشفة حديثاً، مثل اسم التهديد وتاريخ ووقت اكتشافه، وطريقة الاكتشاف وبيانات التعريف المقترنة وإصدار المنتج وتكوينه، بما في ذلك معلومات حول نظامك.
- **البريد الإلكتروني لجهة الاتصال (اختياري)** – يمكن إرسال البريد الإلكتروني لجهة الاتصال مع أي ملفات مريبة، كما يمكن استخدامه للاتصال بك في حالة وجود معلومات أخرى مطلوبة للتحليل. الرجاء ملاحظة أنك لن تتلقى رداً من ESET ما لم توجد معلومات أخرى مطلوبة.

إرسال عينات

الإرسال اليدوي للعينات – يتم تمكين خيار إرسال العينات يدوياً إلى ESET من القائمة السياقية أو وحدة العزل أو الأدوات.

الإرسال التلقائي للعينات المكتشفة

حدد نوع العيّنات التي سيتم تقديمها إلى ESET لتحليلها وتحسين الكشف في المستقبل(الحد الأقصى الافتراضي لحجم العينة هو 64 ميجابايت). تتوفر الخيارات التالية:

- **جميع العيّنات المكتشفة** ـ جميع الأهداف المكتشفة بواسطة محرك الكشف (بما في ذلك التطبيقات التي يحتمل أن تكون غير مرغوب فيها عند تمكينها في إعدادات الماسح الضوئي).
- **جميع العيّنات باستثناء الوثائق** – جميع الكائنات المكتشفة باستثناء **المستندات** (انظر أدناه).
- **لا تقم بالإرسال** – لن يتم إرسال الكائنات المكتشفة إلى ESET.

الإرسال التلقائي للعينات المشتبه بها

سيتم إرسال هذه العينات أيضاً إلى ESET في حالة عدم اكتشاف محرك الكشف عنها. على سبيل المثال، العينات التي فاتها الاكتشاف تقريباً، أو واحدة من ESET Internet Security الوحدات النمطية للحماية تعتبر هذه العينات مشبوهة أو لديها سلوك غير واضح.(الحد الأقصى الافتراضي لحجم العينة هو 64 ميجابايت).

- **القابلة للتنفيذ** – يتضمن الملفات القابلة للتنفيذ مثل .exe, .dll, .sys.
- **الأرشيفات** – يتضمن أنواع ملفات الأرشيف مثل .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **البرامج النصية** – يتضمن أنواع الملفات النصية مثل.bat, .cmd, .hta, .js, .vbs, .ps1.
- **أخرى** – تشمل أنواع ملفات مثل .jar, .reg, .msi, .sfw, .lnk.
- **رسائل البريد العشوائي المحتملة** ـ سيسمح هذا بإرسال الأجزاء العشوائية المحتملة أو رسائل البريد العشوائي المحتملة كاملة إلى ESET لتحليلها أكثر. يعمل تمكين هذا الخيار على تحسين الاكتشاف العالمي لرسائل البريد العشوائي بما في ذلك تحسينات في اكتشاف البريد العشوائي مستقبلاً.
- **المستندات** – تشمل Microsoft Office أو مستندات PDF مع المحتوى النشط أو بدونه.

قم بالتوسيع للحصول على قائمة بجميع أنواع ملفات المستندات المضمّنة

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

الاستبعادات

يسمح لك عامل تصفية "استبعاد" باستبعاد ملفات/مجلدات معينة من الإرسال (على سبيل المثال، يمكن أن يكون مفيداً في استبعاد ملفات يمكن أن تحمل معلومات سرية كالوثائق أو جداول البيانات). لن يتم إرسال الملفات المُدرجة إلى مختبرات ESET للتحليل، حتى وإن كانت تحتوي على تعليمة برمجية مريبة. يتم استبعاد أكثر أنواع الملفات شيوعاً (مثل .doc وغيرها) افتراضياً. ويمكنك الإضافة إلى قائمة الملفات المستبعدة حسب رغبتك.

لاستثناء الملفات التي تم تنزيلها من download.domain.com، انتقل إلى الإعداد المتقدم > **محرك الكشف** > **الحماية المستندة إلى السحابة** > **إرسال العينات**وانقر فوق **تحرير** بجوار **الاستثناءات**. أضِف الاستثناء download.domain.com.

يحدد **الحد الأقصى لحجم العينات (ميجابايت)**—الحد الأقصى لحجم العينات المرسلة تلقائياً (64-1 ميجابايت).

عامل تصفية الاستبعاد للحماية المستندة إلى السحابة

يتيح لك عامل تصفية الاستبعاد إمكانية استبعاد ملفات/مجلدات محددة من عملية الإرسال. لن يتم إرسال الملفات المُدرجة إلى مختبرات ESET للتحليل، حتى وإن كانت تحتوي على تعليمة برمجية مريبة. يتم استبعاد أنواع الملفات الشائعة (مثل doc. وغيرها) افتراضياً.

هذه الخاصية مفيدة لاستبعاد ملفات قد تضم معلومات سرية، مثل المستندات أو جداول البيانات.

لاستبعاد الملفات التي تم تنزيلها من download.domain.com، انقر فوق الإعداد المتقدم > **محرك الكشف** > **الحماية المستندة إلى السحابة** > **إرسال العينات** > **الاستثناءات** وأضِف الاستبعاد *download.domain.com.

عمليات فحص البرامج الضارة

يمكن الوصول إلى قسم **عمليات فحص البرامج الضارة** من الإعداد المتقدم > **محرك الكشف** > **عمليات فحص البرامج الضارة** ويسمح لك بتكوين معلمات الفحص لملفات تعريف الفحص.

فحص عند الطلب

ملف التعريف المحدد – مجموعة محددة من المعلمات المستخدمة من قبل الفاحص عند الطلب. لإنشاء ملف تعريف جديد، انقر فوق **تحرير** بجوار **قائمة ملفات التعريف**. اطلع على ملفات تعريف الفحص لمزيد من التفاصيل.

بعد تحديد ملف تعريف الفحص، يمكنك تكوين الخيارات التالية:

فحص الأهداففي حالة الرغبة في فحص هدف معين أو مجموعة من الأهداف، انقر فوق **تحرير** بجوار **فحص الأهداف** وتحديد خيار من بنية المجلدات (الشجرة). اطلع على فحص الأهداف لمزيد من التفاصيل.

حماية التعلم حسب الطلب والتعلم الآلي—يمكنك تكوين مستويات التقارير والحماية لكل ملف تعريف فحص. افتراضياً، تستخدم ملفات تعريف الفحص نفس الإعداد المحدد في حماية نظام الملفات في الوقت الفعلي. قم بتعطيل مفتاح التبديل بجوار **استخدام إعدادات الحماية في الوقت الفعلي** لتكوين التقارير المخصصة ومستويات الحماية. راجع وسائل الحماية للحصول على شرح مفصل لمستويات التقارير والحماية.

ThreatSense—خيارات الإعداد المتقدمة، مثل ملحقات الملفات التي تريد التحكم بها وطرق الكشف المستخدمة. راجع ThreatSense للحصول على مزيد من المعلومات.

ملفات تعريف الفحص

هناك 4 من ملفات تعريف الفحص المحددة مسبقاً في ESET Internet Security:

- **الفحص الذكي** – هذا هو ملف تعريف الفحص المتقدم الافتراضي. يستخدم ملف تعريف الفحص الذكي تقنية التحسين الذكي، والتي تستبعد الملفات التي عُثر عليها نظيفة في فحص سابق ولم يتم تعديلها منذ ذلك الفحص. وهذا يقلل من وقت الفحص وتأثير أقل على أمان النظام.
- **فحص القائمة السياقية** – يمكنك بدء فحص عند الطلب لأي ملف من القائمة السياقية. يسمح لك ملف تعريف فحص القائمة السياقية بتحديد تكوين الفحص الذي سيُستخدم عند تشغيل الفحص بهذه الطريقة.
- **الفحص المفصل** – لا يستخدم ملف تعريف الفحص المفصل التحسين الذكي بشكل افتراضي، لذلك لا يتم استبعاد أي ملفات من الفحص باستخدام ملف التعريف هذا.
- **فحص جهاز الكمبيوتر** – هذا هو ملف التعريف الافتراضي المستخدم في فحص جهاز الكمبيوتر القياسي.

يمكن حفظ معلمات الفحص المفضلة للفحص في المستقبل. يوصى بإنشاء ملف تعريف مختلف (بأهداف فحص وأساليب فحص متنوعة وغيرها من المعلمات) لكل فحص يُستخدم بشكل منتظم.

لإنشاء ملف تعريف جديد، قم بفتح الإعداد المتقدم > **محرك الكشف** > **عمليات فحص البرامج الضارة** > **الفحص عند الطلب** > **قائمة ملفات التعريف** > **تحرير**. تتضمن نافذة **إدارة ملفات التعريف** القائمة المنسدلة **ملف التعريف المحدد** الذي يضم ملفات تعريف الفحص الموجودة وخيار إنشاء ملف تعريف جديد. لمساعدتك في إنشاء ملف تعريف فحص بما يلائم احتياجاتك، راجع ThreatSense للاطلاع على وصف لكل معلمة إعداد فحص.

> لنفترض أنك تريد إنشاء ملف تعريف فحص، ويعد تكوين **فحص الكمبيوتر** مناسباً بشكل جزئي، لكنك لا تريد فحص حزم وقت التشغيل أو التطبيقات المحتمل كونها غير آمنة ، كما تريد أيضاً تطبيق **اكتشاف العلاج دائماً**. أدخل اسم ملف التعريف الجديد في نافذة **إدارة ملفات التعريف** وانقر فوق **إضافة**. حدد ملف التعريف الجديد من القائمة المنسدلة **ملف التعريف المحدد** واضبط المعلمات المتبقية بما يلائم متطلباتك، وانقر فوق **موافق** لحفظ ملف التعريف الجديد.

أهداف الفحص

تسمح لك القائمة المنسدلة **أهداف الفحص** بتحديد أهداف فحص محددة مسبقاً.

- **حسب إعدادات ملف التعريف** – لتحديد أهداف محددة في ملف تعريف الفحص المحدد.
- **الوسائط القابلة للإزالة** – لتحديد أقراص مرنة وأجهزة تخزين USB وأقراص مضغوطة/أقراص DVD.
- **محركات الأقراص المحلية** – لتحديد جميع محركات الأقراص الثابتة للنظام.
- **محركات أقراص الشبكة** – لفحص جميع محركات الشبكة المعينة.
- **التحديد المخصص** – يلغي جميع التحديدات السابقة.

تحتوي بنية المجلد (الشجرة) أيضاً على أهداف فحص محددة.

- **ذاكرة التشغيل** – تقوم بفحص جميع العمليات والبيانات المستخدمة حالياً بواسطة ذاكرة التشغيل.
- **قطاعات التشغيل/UEFI** – تفحص قطاعات التشغيل وUEFI بحثاً عن وجود البرامج الضارة. اقرأ المزيد عن فاحص UEFI في المسرد.

- **قاعدة بيانات WMI** – تفحص قاعدة بيانات أدوات إدارة Windows (WMI) بالكامل وجميع مساحات الأسماء وجميع مثيلات الفئة وجميع الخصائص. يبحث عن المراجع إلى الملفات المصابة أو البرمجيات الخبيثة كبيانات.
- **سجل النظام** – يقوم بمسح سجل النظام بأكمله، وجميع المفاتيح، والمفاتيح الفرعية. يبحث عن المراجع إلى الملفات المصابة أو البرمجيات الخبيثة كبيانات. عند تنظيف الاكتشافات، يبقى المرجع في السجل للتأكد من عدم فقدان أي بيانات مهمة.

للانتقال بسرعة إلى هدف فحص (ملف أو مجلد)، اكتب مساره في حقل النص أسفل بنية الشجرة. المسار حساس لحالة الأحرف. لتضمين الهدف في الفحص، حدد خانة الاختيار الخاصة به في بنية الشجرة.

فحص حالة الخمول

يمكنك تمكين برنامج فحص حالة الخمول في الإعداد المتقدم > **محرك الكشف** > **عمليات فحص البرامج الضارة** > **فحص حال**.

فحص حالة الخمول

قم بتمكين شريط التمرير الموجود بجوار **تمكين فحص حالة الخمول** لتمكين هذه الميزة. وعندما يكون جهاز الكمبيوتر في حالة خمول، يتم إجراء فحص صامت لجهاز الكمبيوتر في كل محركات الأقراص المحلية.

بشكل افتراضي، لن يعمل برنامج الفحص في حالة الخمول عند تشغيل الكمبيوتر (الكمبيوتر المحمول) باستخدام طاقة البطارية. ويمكنك تجاوز هذا الإعداد بتمكين شريط التمرير الموجود بجوار **تشغيل حتى وإن كان جهاز الكمبيوتر يعمل بطاقة مستمدة من بطارية** في الإعداد المتقدم.

قم بتمكين شريط التمرير بجوار **تمكين التسجيل** في الإعداد المتقدم لتسجيل مخرجات فحص جهاز الكمبيوتر في قسم ملفات السجل (من نافذة البرنامج الرئيسية انقر فوق **الأدوات** > **ملفات السجل** وحدد **فحص الكمبيوتر** من القائمة المنسدلة **السجل**).

اكتشاف حالة الخمول

راجع مشغلات اكتشاف حالة الخمول للحصول على قائمة كاملة بالشروط التي يجب استيفاؤها لتشغيل برنامج الفحص في حالة الخمول.

ThreatSense—خيارات الإعداد المتقدمة، مثل ملحقات الملفات التي تريد التحكم بها وطرق الكشف المستخدمة. راجع ThreatSense للحصول على مزيد من المعلومات.

اكتشاف حالة الخمول

يمكنك تكوين إعدادات الاكتشاف في حالة الخمول في إعداد متقدم > **محرك الكشف** > **عمليات فحص البرامج الضارة** > **فحص حالة الخمول** > **اكتشاف حالة الخمول**. تحدد هذه الإعدادات مشغلاً لـ فحص حالة الخمول:

- **إطفاء الشاشة أو شاشة التوقف**
- **قفل الكمبيوتر**

- **تسجيل خروج المستخدم**

استخدم مفاتيح التبديل لكل حالة معنية لتمكين مختلف مشغلات حالة الخمول أو تعطيلها.

الفحص عند بدء التشغيل

سيتم افتراضياً إجراء فحص تلقائي لملف بدء التشغيل عند بدء تشغيل النظام وأثناء تحديثات محرك الكشف. ويعتمد هذا الفحص على تكوين الجدولة والمهام.

تعد خيارات الفحص عند بدء التشغيل جزءاً من مهمة المجدول **فحص ملفات بدء تشغيل النظام**. لتعديل إعداداته، انتقل إلى **الأدوات > المجدول**، انقر فوق **فحص ملف بدء التشغيل التلقائي**، ثم انقر فوق **تحرير**. في الخطوة الأخيرة، ستظهر نافذة فحص ملف بدء التشغيل التلقائي. للحصول على إرشادات تفصيلية حول إنشاء مهمة مجدول وإدارتها، راجع إنشاء مهام جديدة.

ThreatSense—خيارات الإعداد المتقدمة، مثل ملحقات الملفات التي تريد التحكم بها وطرق الكشف المستخدمة. راجع ThreatSense للحصول على مزيد من المعلومات.

فحص ملفات بدء التشغيل التلقائي

عند إنشاء مهمة مجدولة "فحص ملفات بدء تشغيل النظام"، تتوفر لديك عدة خيارات لضبط المعلمات التالية:

تحدد القائمة المنسدلة **هدف فحص** مستوى الفحص للملفات التي تعمل عند بدء تشغيل النظام استناداً إلى خوارزمية معقدة سرية. يتم ترتيب الملفات تنازلياً حسب المعايير التالية:

- **كل الملفات المسجلة** (أكثر الملفات فحصاً)
- **الملفات المستخدمة نادراً**
- **الملفات المستخدمة بكثرة**
- **الملفات المستخدمة كثيراً**
- **الملفات المستخدمة كثيراً فقط** (أقل الملفات فحصاً)

كما توجد مجموعتان معينتان هما:

- **ملفات تعمل قبل تسجيل دخول المستخدم** ـ تحتوي على ملفات من أماكن يمكن الوصول إليها دون تسجيل دخول المستخدِم (وذلك يشمل معظم أماكن بدء التشغيل كالخدمات وكائنات مساعد المستعرض وإخطار winlogon وإدخالات مجدول Windows وملفات dll المعروفة وغيرها).
- **ملفات تعمل بعد تسجيل دخول المستخدم** ـ تحتوي على ملفات من أماكن لا يمكن الوصول إليها إلا بعدما يسجل المستخدم دخوله (تشمل الملفات التي لا تعمل إلا بواسطة مستخدم معين، الملفات الموجودة عادة في المسار *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

يتم إصلاح قوائم الملفات المراد فحصها لكل مجموعة أعلاه. إذا اخترت مستوى فحص أقل للملفات التي يتم تشغيلها عند بدء تشغيل النظام، فسيتم فحص الملفات التي لم يتم فحصها عند الفتح أو التنفيذ.

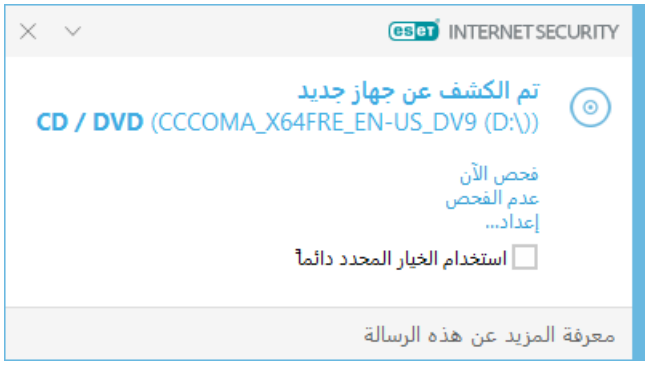
أولوية الفحص – مستوى الأولوية المستخدم لتحديد الوقت الذي يجب أن يبدأ فيه الفحص:

- **عند الخمول** – لن يتم تنفيذ المهمة إلا عند خمول النظام،
- **الأقل** – عندما يكون حمل النظام عند أدنى مستوى ممكن،
- **أقل** – عند حمل النظام المنخفض،
- **عادي** – عند حمل النظام المتوسط.

الوسائط القابلة للإزالة

ESET Internet Security يوفر فحصاً تلقائياً للوسائط القابلة للإزالة (الأقراص المضغوطة/أقراص DVD/أجهزة USB...) عند إدخاله إلى جهاز كمبيوتر. قد يكون ذلك مفيداً إذا كان مسؤول الكمبيوتر يريد منع المستخدمين من استخدام وسائط قابلة للإزالة بمحتوى غير مرغوب فيه.

عندما يتم إدراج الوسائط القابلة للإزالة، وتعيين **إظهار خيارات الفحص** في الإعداد المتقدم > **محرك الكشف** > **عمليات فحص البرامج الضارة** > **الوسائط القابلة للإزالة** سيتم عرض مربع الحوار التالي:



خيارات مربع الحوار هذا:

- **فحص الآن** – سيؤدي هذا إلى تشغيل فحص الوسائط القابلة للإزالة.
- **عدم الفحص** — لن يتم فحص الوسائط القابلة للإزالة.
- **إعداد** – يتم فتح الإعداد المتقدم.
- **استخدام الخيار المحدد دائماً** – عند تحديد هذا الخيار، سيتم تنفيذ نفس الإجراء عند إدخال الوسائط القابلة للإزالة في وقت آخر.

بالإضافة إلى ذلك، يتضمن ESET Internet Security ميزة تحكم في الجهاز، تسمح لك بتحديد قواعد لاستخدام أجهزة خارجية على كمبيوتر معين. يمكن العثور على مزيد من التفاصيل حول التحكم في الجهاز في قسم التحكم فالاجهزة المتصلة.

للوصول إلى إعدادات فحص الوسائط القابلة للإزالة، افتح الإعداد المتقدم > **محرك الاكتشاف** > **عمليات فحص البرامج الضارة** > **الوسائط القابلة للإزالة**.

الإجراء المطلوب اتخاذه بعد إدخال الوسائط القابلة للإزالة – حدد الإجراء الافتراضي الذي سيُتخذ عند إدخال وسيطة قابلة للإزالة في الكمبيوتر (قرص مضغوط/قرص DVD/جهاز USB). اختر الإجراء المطلوب عند إدخال وسائط قابلة للنقل على جهاز

كمبيوتر:

- **عدم الفحص** ـ لن يتم تنفيذ أي إجراء ولن يتم فتح نافذة **تم الكشف عن جهاز جديد**.
- **فحص الجهاز تلقائياً** ـ سيتم فحص جهاز الكمبيوتر لجهاز الوسائط القابلة للإزالة الذي يتم إدخاله.
- **عرض خيارات الفحص** – لفتح قسم **إعداد الوسائط القابلة للإزالة**.

حماية المستندات

تفحص ميزة حماية المستندات مستندات Microsoft Office قبل فتحها، إضافة إلى الملفات التي يتم تنزيلها تلقائياً بواسطة Internet Explorer مثل عناصر Microsoft ActiveX. توفر ميزة حماية المستندات طبقة حماية بالإضافة إلى حماية نظام الملفات في الوقت الفعلي، ويمكن تعطيلها لتحسين الأداء على الأنظمة التي لا تعالج حجماً كبيراً من مستندات Microsoft Office.

لتنشيط حماية المستندات، افتح الإعداد المتقدم > **محرك الكشف** > **عمليات فحص البرامج الضارة** > **حماية المستندات** وانقر فوق مفتاح التبديل بجوار **تمكين حماية المستندات**.

ThreatSense—خيارات الإعداد المتقدمة، مثل ملحقات الملفات التي تريد التحكم بها وطرق الكشف المستخدمة. راجع ThreatSense للحصول على مزيد من المعلومات.

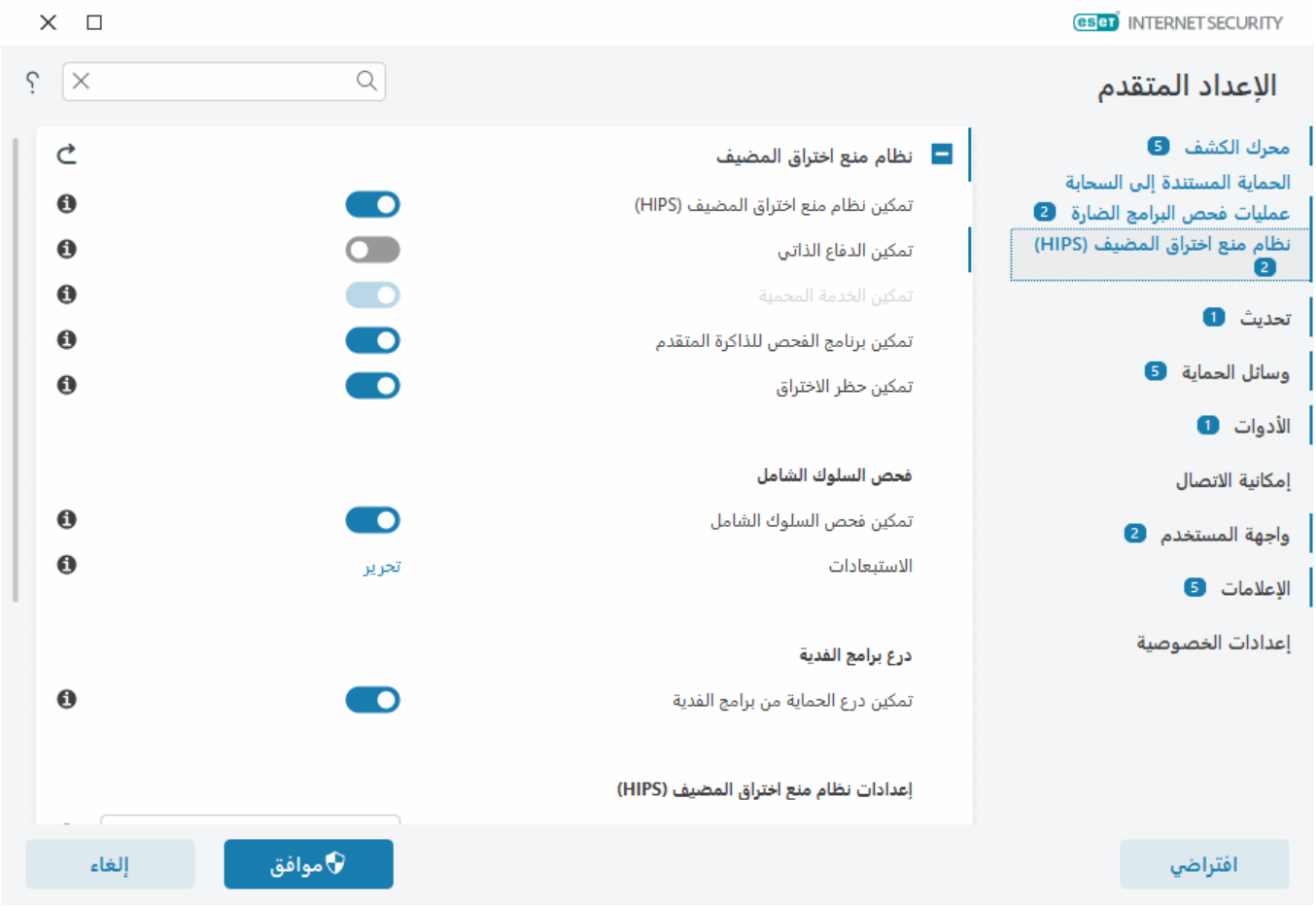
> يتم تنشيط هذه الميزة بواسطة التطبيقات التي تستخدم Microsoft Antivirus API (على سبيل المثال Microsoft Office 2000 والأحدث، أو Microsoft Internet Explorer 5.0 أحدث).

HIPS – نظام منع اختراق المضيف

> يجب عدم إجراء تغييرات على إعدادات نظام منع اختراق الجهاز إلا بواسطة مستخدم ذي خبرة. فقد يؤدي تكوين إعدادات نظام HIPS بشكل غير صحيح إلى عدم استقرار النظام.

يحمي **نظام منع اختراق المضيف (HIPS)** نظامك من البرامج الضارة والأنشطة غير المرغوب فيها التي تحاول التأثير سلباً على جهاز الكمبيوتر. يستخدم نظام منع اختراق الجهاز تحليل سلوك متقدماً مرفقاً بإمكانات اكتشاف لتصفية الشبكة لمراقبة العمليات الفعالة والملفات ومفاتيح السجلات. يعد نظام منع اختراق الجهاز منفصلاً عن حماية نظام الملفات في الوقت الفعلي وهو ليس جدار حماية، وإنما هو فقط يراقب العمليات الجارية في نظام التشغيل.

يمكنك تكوين إعدادات HIPS في الإعداد المتقدم > **محرك الكشف** > **HIPS** > **نظام منع اختراق المضيف**. تظهر حالة نظام HIPS (ممكّن/معطل) في نافذة برنامج ESET Internet Security الرئيسية، في > **إعداد** > **حماية الكمبيوتر**.



نظام منع اختراق المضيف

تمكين HIPS – يتم تمكين HIPS افتراضياً في ESET Internet Security. سيؤدي إيقاف تشغيل HIPS إلى تعطيل باقي ميزات HIPS مثل "حظر الاختراق".

تمكين الدفاع الذاتي – يستخدم ESET Internet Security تكنولوجيا **الدفاع الذاتي** المدمجة كجزء من HIPS لمنع البرامج الضارة من إتلاف حماية مكافحة البرامج الضارة وبرامج التجسس أو تعطيلها. تعمل ميزة الدفاع الذاتي على حماية النظام الهام وعمليات ESET ومفاتيح التسجيل والملفات من أن يتم العبث بها.

تمكين الخدمة المحمية – تمكّن الحماية من خدمة ekrn.exe) ESET). عند تمكين الخدمة، فإنها تبدأ كعملية Windows محمية للحماية من هجمات البرمجيات الخبيثة.

تمكين برنامج فحص الذاكرة المتقدم – يعمل بالاشتراك مع حظر الاختراق لتعزيز الحماية ضد البرامج الضارة المصممة لاختراق الاكتشاف بواسطة منتجات مكافحة برامج ضارة عبر استخدام الإخفاء أو التشفير. برنامج فحص الذاكرة المتقدم ممكّن افتراضياً. اقرأ المزيد حول هذا النوع من الحماية في المسرد.

تمكين حظر الاختراق – صُمم للحماية ضد أنواع التطبيقات الشائع اختراقها كمستعرضات ويب، أو قارئات ملفات PDF أو البرامج العميلة للبريد الإلكتروني، أو مكونات MS Office. حظر الاختراق ممكّن افتراضياً. اقرأ المزيد حول هذا النوع من الحماية في المسرد.

فحص السلوك الشامل

تمكين فحص السلوك الشامل ـ هي طبقة أخرى من الحماية تعمل كجزء من ميزة HIPS. يقوم هذا الامتداد لـ HIPS بتحليل سلوك جميع البرامج قيد التشغيل على الكمبيوتر ويحذرك إذا كان سلوك العملية ضاراً.

استبعادات HIPS من فحص السلوك الشامل تتيح لك الاستبعادات استبعاد العمليات من التحليل. لضمان فحص جميع العمليات بحثاً عن التهديدات المحتملة، نوصي بعدم إنشاء استبعادات إلا في حالة الضرورة القصوى.

درع برامج الفدية

تمكين درع برامج الفدية ـ طبقة أخرى من الحماية تعمل كجزء من ميزة HIPS. يجب أن يكون لديك نظام شمعة ESET LiveGrid® ممكّناً لدرع برامج الفدية للعمل. اقرأ المزيد حول هذا النوع من الحماية في هنا

التمكين Intel® Threat Detection Technology ـ يساعد على اكتشاف هجمات برامج الفدية من خلال استخدام القياس الفريد لوحدة المعالجة المركزية Intel لزيادة فعالية الكشف وتقليل التنبيهات الإيجابية الكاذبة وتوسيع الرؤية للقبض تقنيات التهرب المتقدمة. راجع المعالجات المدعومة.

إعدادات HIPS

يمكن إجراء **وضع التصفية** في وضع من الأوضاع التالية:

الوصف	وضع التصفية
يتم تمكين العمليات باستثناء العمليات المحظورة بواسطة قواعد معرفة مسبقاً تحمي النظام.	**الوضع التلقائي**
لن يتم إعلام المستخدم إلا بالأحداث المشكوك فيها بدرجة كبيرة.	**الوضع الذكي**
ستتم مطالبة المستخدم بتأكيد العمليات.	**الوضع التفاعلي**
يمنع جميع العمليات التي لم يتم تحديدها بواسطة قاعدة محددة تسمح بها.	**وضع مستند الى سياسه**
يتم تمكين العمليات ويتم إنشاء قاعدة بعد كل عملية. يمكن عرض القواعد التي يتم إنشاؤها في هذا الوضع في محرر **قواعد نظام منع اختراق المضيف (HIPS)**، ولكن أولويتها أقل من أولوية القواعد التي يتم إنشاؤها يدوياً أو القواعد التي يتم إنشاؤها في الوضع التلقائي. عند تحديد **وضع التعرف** من القائمة المنسدلة **وضع التصفية**، سيتوفر الإعداد **سينتهي وضع التعرف في**. حدد المدة التي تريدها لتشغيل وضع التعرف، ويُرجى العلم بأن الحد الأقصى للمدة هو 14 يوماً. عند انتهاء المدة المحددة، ستتم مطالبتك بتحرير القواعد التي تم إنشاؤها بواسطة HIPS أثناء تشغيله في وضع التعرف. يمكنك أيضاً اختيار وضع تصفية مختلف أو تأجيل القرار ومتابعة استخدام وضع التعرف.	**وضع التعرف**

وضع مجموعة بعد انتهاء وضع التعلم – حدد وضع التصفية الذي سيتم استخدامه بعد انتهاء صلاحية وضع التعلم. بعد انتهاء الصلاحية، يتطلب الخيار **اسأل المُستخدم** امتيازات إدارية لإجراء تغيير على وضع تصفية نظام منع اختراق المضيف (HIPS).

يراقب نظام منع اختراق المضيف أحداثاً داخل نظام التشغيل، ويستجيب وفقاً لذلك حسب قواعد مشابهة لتلك المستخدمة بواسطة جدار الحماية. انقر فوق **تحرير** بجانب **القواعد** لفتح المحرر **قوانين نظام منع اختراق المضيف (HIPS)**. في نافذة قواعد نظام منع اختراق المضيف (HIPS) يمكنك تحديد القواعد أو إضافتها أو تحريرها أو إزالتها. يمكن العثور على مزيد من التفاصيل حول إنشاء القواعد وعمليات نظام منع اختراق المضيف في تحرير قاعدة نظام منع اختراق المضيف (HIPS).

استبعادات HIPS

تمكّنك الاستبعادات من استبعاد العمليات من فحص السلوك الشامل لـ HIPS.

لتحرير استبعادات HIPS افتح الإعداد المتقدم > **محرك الكشف** > **HIPS** > **نظام منع اختراق المضيف** > **استبعادات** > **تحرير**.

لا تخلط بين استبعادات الملف المستبعد أو استبعادات الاكتشاف أو استبعادات الأداء أو استبعادات العمليات.

لاستثناء كائن، انقر فوق **إضافة** وأدخل مسار كائن أو حدده في بنية الشجرة. يمكنك أيضاً تحرير أو حذف الإدخالات المحددة.

الإعداد المتقدم لـ HIPS

تفيد الإعدادات التالية في تصحيح الأخطاء وتحليل سلوك تطبيق ما:

السماح بتحميل برامج التشغيل دائماً – يتم السماح بتحميل برامج التشغيل المحددة دائماً بصرف النظر عن وضع التصفية المكوَّن، ما لم يتم حظرها صراحة بواسطة قاعدة يعرّفها المستخدم.

تسجيل جميع العمليات المحظورة – ستتم كتابة جميع العمليات المحظورة إلى سجل نظام منع اختراق الجهاز. لا تستخدم هذه الميزة إلا عند استكشاف الأخطاء وإصلاحها أو طلب الدعم الفني لـ ESET ذلك منك؛ لأنها قد تنشئ ملف سجل ضخماً ما يبطئ أداء جهاز الكمبيوتر.

إعلام عند حدوث تغييرات في تطبيقات بدء التشغيل – لعرض إعلام سطح مكتب كلما تمت إضافة تطبيق إلى بدء تشغيل النظام أو إزالته منه.

السماح بتحميل برامج التشغيل دائماً

يتم السماح بتحميل برامج التشغيل الموجودة في هذه القائمة دائماً بصرف النظر عن وضع تصفية HIPS ما لم يتم حظرها صراحة بواسطة قاعدة يعرّفها المستخدم.

إضافة – إضافة برنامج تشغيل جديد.

تحرير – تحرير برنامج تشغيل محدد.

إزالة – إزالة برنامج تشغيل من القائمة.

إعادة تعيين – إعادة تحميل مجموعة من برامج تشغيل النظام.

انقر فوق **إعادة تعيين** إذا كنت لا ترغب في تضمين برامج التشغيل التي أضفتها يدوياً. يمكن أن يكون هذا مفيداً إذا كنت قد أضفت عدة برامج تشغيل ولا يمكنك حذفها من القائمة يدوياً.

بعد التثبيت، تكون قائمة برامج التشغيل فارغة. يملأ ESET Internet Security القائمة تلقائياً بمرور الوقت.

نافذة HIPS التفاعلية

تسمح لك نافذة إعلام HIPS بإنشاء قاعدة بناءً على إجراءات جديدة يكتشفها نظام منع اختراق المضيف (HIPS) ثم تحديد الشروط التي سيتم بموجبها السماح بذلك الإجراء أو رفضه.

تعد القواعد المنشأة من نافذة الإعلام مساوية للقواعد المنشأة يدوياً. لذلك يمكن أن تكون القاعدة المنشأة من نافذة إعلام أقل تحديداً من القاعدة التي تشغل نافذة الحوار هذه. يعني ذلك أنه بعد إنشاء هذه القاعدة، يمكن أن تشغل العملية نفسها النافذة نفسها. لمزيد من المعلومات، اطلع على الأولوية لقواعد HIPS.

إذا كان الإجراء الافتراضي لإحدى القواعد معيَّناً إلى **السؤال في كل مرة**، فسيتم عرض نافذة حوار كلما تم تشغيل القاعدة. يمكنك اختيار **رفض** أو **سماح** للعملية. وإذا لم تختر إجراءً في الوقت المحدد، فسيتم تحديد إجراء جديد بناءً على القواعد.

التذكر حتى إنهاء التطبيق يسبب استخدام الإجراء (**سماح/رفض**) حتى إجراء تغيير للقواعد أو وضع التصفية، أو تحديث وحدة نظام HIPS أو إعادة تشغيل النظام. بعد تنفيذ أي من هذه الإجراءات الثلاثة، سيتم حذف القواعد المؤقتة.

سيقوم خيار **إنشاء قاعدة وتذكرها دائماً** بإنشاء قاعدة HIPS جديدة والتي يمكن تغييرها لاحقاً في قسم إدارة قواعد HIPS (يتطلب امتيازات مسؤول).

انقر فوق **التفاصيل** في الأسفل للاطلاع على التطبيق الذي يقوم بتشغيل العملية، أو ما سمعة الملف أو ما نوع العملية التي تطلب السماح بها أو رفضها.

يمكن الوصول إلى الإعدادات الخاصة بمعلمات القاعدة الأكثر تفصيلاً من خلال النقر فوق **خيارات متقدمة**. تتوفر الخيارات أدناه في حال قمت باختيار **إنشاء قاعدة وتذكرها دائماً**:

- **إنشاء قاعدة صالحة فقط لهذا التطبيق** ـ إذا قمت بإلغاء تحديد خانة الاختيار هذه، فسيتم إنشاء القاعدة لجميع التطبيقات المصدر.
- **فقط بالنسبة للعملية** ـ اختر عملية (عمليات) لملف/تطبيق/سجل قاعدة. اطلع على أوصاف جميع عمليات HIPS.
- **فقط بالنسبة للهدف** ـ اختر هدف (أهداف) ملف/تطبيق/سجل قاعدة.

هل هناك إعلامات HIPS لا نهاية لها؟

لوقف ظهور الإعلامات، قم بتغيير وضع التصفية إلى **الوضع التلقائي** في الإعداد المتقدم > **محرك الكشف** > **HIPS** > **نظام منع اختراق المضيف**.

تم إنهاء وضع التعلم

يقوم وضع التعلم بإنشاء القواعد وحفظها تلقائياً. يمكنك التحقق من جميع القواعد التي تم إنشاؤها في إعدادات قواعد HIPS. يُفضل استخدام هذا الوضع للتكوين الأولي لـ HIPS ولكن يجب الاحتفاظ به لفترة قصيرة فقط. لا يوجد تدخل مطلوب من المستخدم لأن ESET Internet Security يحفظ القواعد وفقاً لمعلمات محددة مسبقاً. قم بالتبديل إلى الوضع **التفاعلي** أو **القائم على السياسة** بعد إنشاء جميع القواعد للعمليات المطلوبة التي تعمل داخل نظام التشغيل لتجنب مخاطر الأمان.

يمكنك تأجيل هذا القرار إذا كنت لا تريد تغيير الإعدادات.

تم اكتشاف سلوك محتمل لبرنامج رانسوم (الفدية)

ستظهر نافذة التفاعل عند اكتشاف سلوك محتمل لبرنامج رانسوم (الفدية). يمكنك اختيار **رفض** أو **سماح** للعملية.

انقر فوق **التفاصيل** لعرض معلمات اكتشاف معينة. تتيح للم نافذة الحوار **الإرسال للتحليل** أو **الاستبعاد من الاكتشاف**.

يجب تمكين ESET LiveGrid® لـ الحماية من رانسوم حتى يعمل جيداً.

إدارة قواعد HIPS

قائمة القواعد المعرفة بواسطة المستخدم والمضافة تلقائياً من نظام HIPS. يمكن العثور على مزيد من التفاصيل حول إنشاء القاعدة وعمليات نظام منع اختراق المضيف في إعدادات قواعد HIPS. اطلع أيضاً على المبدأ العام لـ HIPS.

الأعمدة

القاعدة – اسم القاعدة المعرف بواسطة المستخدم أو المختار تلقائياً.

ممكَّن—قم بتعطيل مفتاح التبديل إذا أردت الاحتفاظ بالقاعدة في القائمة ولكن لا ترغب في استخدامها.

الإجراء – تحدد القاعدة الإجراء – **سماح** أو **حظر** أو **سؤال** – الذي يجب تنفيذه إذا كانت الشروط صحيحة.

المصادر – لن يتم استخدام القاعدة إلا في حالة تشغيل الحدث بواسطة تطبيق (تطبيقات).

الأهداف– لن يتم استخدام القاعدة إلا إذا كانت العملية ذات صلة بملف أو تطبيق أو إدخال سجل معين.

تسجيل الخطورة: – في حالة تنشيط هذا الخيار، ستتم كتابة معلومات عن هذه القاعدة في سجل HIPS.

إعلام – نافذة إعلام صغيرة تظهر في الزاوية السفلية اليسرى في حالة تشغيل حدث.

عناصر التحكم

إضافة – لإنشاء قاعدة جديدة.

تحرير – يتيح لك تحرير إدخالات محددة.

حذف – إزالة إدخالات محددة.

الأولوية لقواعد HIPS

لا توجد خيارات لضبط مستوى أولوية قواعد HIPS باستخدام أزرار لأعلى/لأسفل (مثل، قواعد جدار الحماية حيث يتم تنفيذ القواعد من أعلى إلى أسفل).

- جميع القواعد التي تقوم بإنشائها لها الأولوية ذاتها
- كلما كانت القاعدة أكثر تحديداً، كانت الأولوية أعلى (على سبيل المثال، القاعدة لتطبيق معين لها أولوية أعلى من القاعدة لجميع التطبيقات)
- داخلياً، يتضمن HIPS قواعد ذات أولوية أعلى لا يمكن الوصول إليها من قبلك (على سبيل المثال، لا يمكنك تجاوز القواعد المحددة كدفاع ذاتي)
- لن يتم تطبيق قاعدة تقوم بإنشائها والتي قد تقوم بتجميد نظام التشغيل لديك (سيكون لها الأولوية الأقل)

تحرير قاعدة HIPS

راجع إدارة قاعدة نظام منع اختراق المضيف (HIPS) أولاً.

اسم القاعدة – اسم القاعدة المعرف بواسطة المستخدم أو المختار تلقائياً.

الإجراء – لتحديد الإجراء – **سماح** أو **حظر** أو **سؤال** – الذي يجب تنفيذه في حالة استيفاء الشروط.

العمليات المتضررة – يجب تحديد نوع العملية التي سيتم تطبيق القاعدة عليها. لن يتم استخدام القاعدة إلا مع نوع العملية هذا ومع الهدف المحدد فقط.

ممكَّن – قم بتعطيل شريط التمرير إذا أردت الاحتفاظ بالقاعدة في القائمة مع عدم تطبيقها.

تسجيل الخطورة: – في حالة تنشيط هذا الخيار، ستتم كتابة معلومات عن هذه القاعدة في سجل HIPS.

إعلام المستخدم – نافذة إعلام صغيرة تظهر في الزاوية السفلية اليسرى في حالة تشغيل حدث.

تتكون القاعدة من أجزاء تصف شروط تشغيل هذه القاعدة:

التطبيقات المصدر – لن يتم استخدام القاعدة إلا في حالة تشغيل الحدث بواسطة هذا التطبيق (التطبيقات). حدد **تطبيقات معينة** من القائمة المنسدلة وانقر فوق **إضافة** لإضافة ملفات جديدة أو حدد **كل التطبيقات** من القائمة المنسدلة لإضافة كل التطبيقات.

الملفات الهدف – سيتم استخدام القاعدة فقط إذا كانت العملية مرتبطة بهذا الهدف. حدد **ملفات معينة** من القائمة المنسدلة وانقر

فوق **إضافة** لإضافة ملفات أو مجلدات جديدة أو يمكنك تحديد **جميع الملفات** من القائمة المنسدلة لإضافة جميع الملفات.

التطبيقات – لن يتم استخدام القاعدة إلا إذا كانت العملية ذات صلة بهذا الهدف. حدد **تطبيقات معينة** من القائمة المنسدلة وانقر فوق **إضافة** لإضافة ملفات أو مجلدات جديدة أو حدد **كل التطبيقات** من القائمة المنسدلة لإضافة كل التطبيقات.

إدخالات السجل – لن يتم استخدام القاعدة إلا إذا كانت العملية ذات صلة بهذا الهدف. حدد **إدخالات معينة** من القائمة المنسدلة وانقر فوق**إضافة** لكتابته يدوياً أو يمكنك النقر فوق **فتح محرر التسجيل** لتحديد مفتاح من السجل. ويمكنك تحديد **كل الإدخالات**من القائمة المنسلة لإضافة جميع التطبيقات.

> لا يمكن حظر بعض العمليات الخاصة بالقواعد المعرفة مسبقاً بواسطة نظام HIPS ويتم السماح بها حسب الإعداد الافتراضي. إضافة إلى ذلك، لا تتم مراقبة كل عمليات النظام بواسطة HIPS. فنظام HIPS يراقب العمليات التي من المحتمل أن تكون غير آمنة.

أوصاف العمليات المهمة:

عمليات الملفات

- **حذف ملف** – يطلب التطبيق الحصول على إذن لحذف الملف الهدف.
- **كتابة إلى الملف** – يطلب التطبيق الحصول على إذن للكتابة في الملف الهدف.
- **وصول مباشر إلى القرص** – يحاول التطبيق القراءة من القرص أو الكتابة عليه بطريقة غير قياسية ستخدع إجراءات Windows المعتادة. قد يؤدي هذا إلى تعديل الملفات بدون تطبيق القواعد المقابلة. قد تحدث هذه العملية بسبب أن أحد البرامج الضارة يحاول تجنب الحذف، أو أن برنامج النسخ الاحتياطي يحاول إجراء نسخة طبق الأصل من القرص، أو أن إدارة الأقسام تحاول إعادة تنظيم وحدات التخزين على القرص.
- **تثبيت موضع الإضافة في الروتين العمومي** – تشير إلى استدعاء وظيفة SetWindowsHookEx من مكتبة MSDN.
- **تحميل برنامج التشغيل** – تثبيت برامج التشغيل وتحميلها على النظام.

عمليات التطبيقات

- **تصحيح أخطاء تطبيق آخر** – إرفاق مصحح أخطاء بالعملية. أثناء تصحيح أخطاء التطبيق، يمكن عرض العديد من تفاصيل السلوك الخاص به وتعديلها، كما يمكن الوصول إلى بياناته.
- **اعتراض أحداث من تطبيق آخر** – يحاول التطبيق المصدر التقاط الأحداث المستهدفة في تطبيق معين (على سبيل المثال، يحاول برنامج تسجيل ضغطات المفاتيح التقاط أحداث المستعرض).
- **إنهاء/تعليق تطبيق آخر** – تعليق عملية أو استئنافها أو إنهاؤها (يمكن الوصول إلى ذلك مباشرةً من مستكشف العمليات أو جزء العمليات).
- **بدء تطبيق جديد** – بدء تطبيقات أو عمليات جديدة.
- **تعديل حالة تطبيق آخر** – يحاول التطبيق المصدر الكتابة في ذاكرة التطبيقات الهدف أو تشغيل التعليمات البرمجية من أجلها. قد تكون هذه الوظيفة مفيدة لحماية تطبيق أساسي بتكوينه كتطبيق هدف في قاعدة تحظر استخدام هذه العملية.

عمليات التسجيل

- **تعديل إعدادات بدء التشغيل** – أي تغييرات في الإعدادات التي تعرّف التطبيقات التي يتم تشغيلها عند بدء تشغيل Windows. ويمكن العثور عليها، على سبيل المثال، عبر البحث عن مفتاح Run في تسجيل Windows.

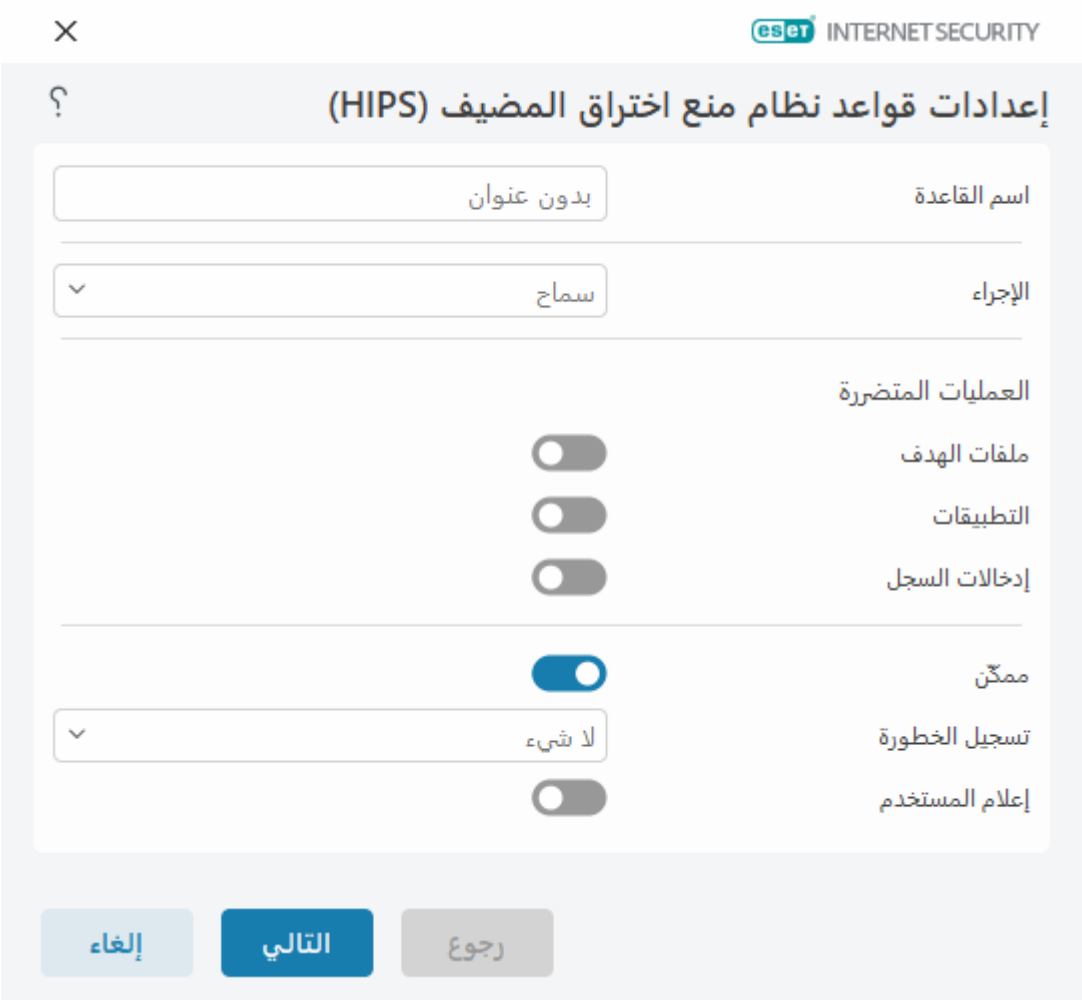
- **حذف من التسجيل** – حذف مفتاح تسجيل أو قيمته.
- **إعادة تسمية مفتاح التسجيل** – إعادة تسمية مفاتيح التسجيل.
- **تعديل التسجيل** – إنشاء قيم جديدة لمفاتيح التسجيل، أو تغيير القيم الموجودة، أو نقل البيانات في شجرة قاعدة البيانات، أو إعداد حقوق المستخدم أو المجموعة لمفاتيح التسجيل.

يمكنك استخدام أحرف البدل مع بعض التقييدات عند إدخال هدف. فبدلاً من مفتاح معين، يمكن استخدام الرمز * (النجمة) في مسارات السجل. على سبيل المثال، *HKEY_USERS*\software* يمكن أن يعني *HKEY_USER\.default\software* ولكن لا يمكن أن يعني *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. المسار *HKEY_LOCAL_MACHINE\system\ControlSet** ليس مسار مفتاح تسجيل صالحاً. يعرّف مسار مفتاح التسجيل الذي يحتوي على * "هذا المسار أو أي مسار في أي مستوى بعد هذا الرمز". هذه هي الطريقة الوحيدة لاستخدام أحرف البدل لأهداف الملفات. أولاً، سيتم تقييم الجزء المحدد من المسار، ثم المسار الذي يلي رمز حرف البدل (*).

في حالة إنشاء قاعدة عامة إلى حد بعيد، سيتم عرض تحذير عن هذا النوع من القواعد.

في المثال التالي، سنعرض كيفية تقييد السلوكيات غير المرغوب فيها لتطبيق معين:

1. أطلق اسماً للقاعدة وحدد **حظر** (أو **سؤال** إذا كنت تفضل الاختيار لاحقاً) من القائمة المنسدلة **إجراء**.
2. قم بتمكين شريط التمرير بجوار **إعلام المستخدم** لعرض إعلام في أي مرة يتم فيها تطبيق قاعدة.
3. حدد عملية واحدة على الأقل في قسم **العمليات المتضررة** للقاعدة التي سيتم تطبيقها.
4. انقر فوق **التالي**.
5. من نافذة **التطبيقات المصدر**، حدد **كل التطبيقات** من القائمة المنسدلة لتطبيق القاعدة الجديدة على تطبيقات معينة التي تحاول تنفيذ أي من عمليات التطبيقات المحددة في التطبيقات التي حددتها.
6. انقر فوق إضافة ثم **...** لاختيار مسار لتطبيق معين ثم اضغط على موافق. أضف المزيد من التطبيقات إذا كنت تريد ذلك. على سبيل المثال: *C:\Program Files (x86)\Untrusted application\application.exe*
7. حدد عملية **الكتابة في ملف**.
8. حدد **جميع الملفات** من القائمة المنسدلة . سيؤدي هذا إلى حظر أي محاولات للكتابة في أي ملفات من قبل التطبيق (التطبيقات) المحددة من الخطوة السابقة.
9. انقر فوق **إنهاء** لحفظ القاعدة الجديدة.



إضافة مسار التسجيل/التطبيق لـ HIPS

حدد مسار تطبيق ملف من خلال النقر فوق خيار .... عند تحديد مجلد، سيتم تضمين جميع التطبيقات الموجودة في هذا الموقع.

سيبدأ خيار **فتح محرر التسجيل** في تشغيل محرر تسجيل Windows. عند إضافة مسار تسجيل، قم بإدخال الموقع الصحيح إلى حقل**القيمة**.

من أمثلة مسار الملف أو التسجيل.

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

تحديث

تتوفر خيارات إعداد التحديث في الإعداد المتقدم > **تحديث**. يحدد هذا القسم معلومات مصدر التحديث كخوادم التحديث المستخدمة وبيانات المصادقة لهذه الخوادم.

يظهر ملف تعريف التحديث قيد الاستخدام حالياً في القائمة المنسدلة **تحديد ملف تعريف التحديث الافتراضي**.

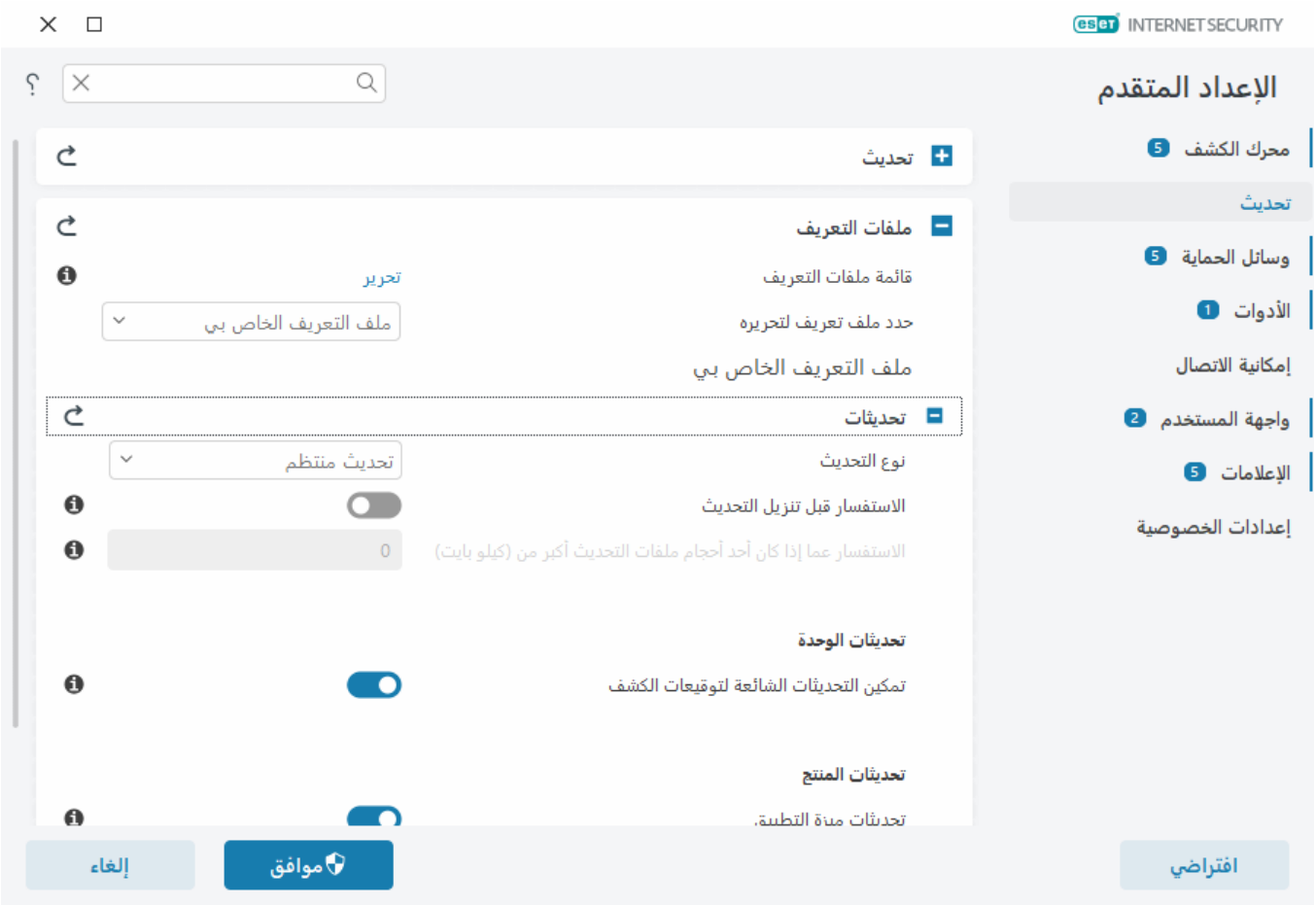
لإنشاء ملف تعريف جديد، اطلع على قسم تحديث ملفات تعريف التحديث.

يتيح لك **التبديل التلقائي لملف التعريف**—تعيين ملف تعريف تحديث لملف تعريف اتصال شبكةمعين.

إذا كنت تواجه صعوبة عند محاولة تنزيل محرك الكشف أو تحديثات الوحدات، فانقر فوق **مسح**بجانب **مسح ذاكرة التخزين المؤقت للتحديث** لمسح ملفات التحديث المؤقتة/ذاكرة التخزين المؤقت.

تراجع الوحدة النمطية

في حالة الاشتباه في أن تحديثاً جديداً لمحرك الكشف و/أو وحدات البرنامج قد يكون غير مستقر أو تالفاً، يمكنك التراجع إلى الإصدار السابق وتعطيل التحديثات لفترة زمنية تحددها.



ليتم تنزيل التحديثات بشكل سليم، من الضروري ملء جميع معلمات التحديث بشكل صحيح. في حالة استخدام جدار حماية، الرجاء التأكد من السماح باتصال برنامج ESET بالإنترنت (على سبيل المثال اتصال HTTP).

ملفات التعريف

يمكن إنشاء ملفات تعريف التحديث لمختلف تكوينات ومهام التحديث. يعد إنشاء ملفات تعريف تحديث مفيداً بشكل أساسي لمستخدمي الأجهزة المحمولة الذين يحتاجون إلى ملف تعريف بديل لخصائص الاتصال بالإنترنت التي تتغير باستمرار.

تعرض القائمة المنسدلة **تحديد ملف التعريف المراد تحريره** ملف التعريف المحدد حالياً والمعيَّن إلى **ملف التعريف الخاص بي** افتراضياً. لإنشاء ملف تعريف جديد، انقر فوق **تحرير** بجوار **قائمة ملفات التعريف**، ثم أدخل **اسم ملف التعريف** وانقر فوق **إضافة**.

التحديث

طبقاً للإعداد الافتراضي، يتم تعيين **نوع التحديث** على **تحديث منتظم** لضمان تنزيل ملفات التحديث تلقائياً من خادم ESET بأقل حركة مرور على الشبكة. تحديثات الإصدار التجريبي (خيار**تحديث الإصدار التجريبي**) هي تحديثات خضعت لاختبارات داخلية شاملة، وستتوفر قريباً للجمهور العام. يمكنك الاستفادة من تمكين تحديثات الإصدار التجريبي بإتاحة الوصول إلى أحدث طرق الاكتشاف والإصلاحات. ولكن، قد لا تكون تحديثات الإصدار التجريبي مستقرة بشكل كافٍ دائماً، كما يجب ألا تُستخدم على خوادم ومحطات عمل الإنتاج التي تتطلب الحد الأقصى من التوفر والثبات.

الاستفسار قبل تنزيل التحديث – سيعرض البرنامج إشعاراً يمكنك اختياره لتأكيد تنزيلات ملف التحديث أو رفضها.

معرفة ما إذا كان حجم ملف تحديث أكبر من (كيلوبايت) ـ سيعرض البرنامج مربع حوار تأكيد إذا كان حجم ملف التحديث أكبر من القيمة المحددة. إذا تم تعيين حجم ملف التحديث على 0 كيلو بايت، فسيعرض البرنامج دائماً مربع حوار تأكيد.

تحديثات الوحدة النمطية

تمكين التحديثات الأكثر تكراراً لتوقيعات الكشف – سيتم تحديث توقيعات الكشف خلال فاصل زمني قصير. قد يؤثر تعطيل هذا الإعداد بالسلب على معدل الكشف.

تحديثات المنتج

تحديثات ميزة التطبيق ـ يتم تثبيت إصدارات جديدة من ESET Internet Security تلقائياً.

خيارات الاتصال

لاستخدام خادم وكيل لتنزيل التحديثات، راجع قسم خيارات الاتصال.

التراجع عن التحديث

في حالة الاشتباه في أن تحديثاً جديداً لمحرك الكشف أو وحدات البرنامج قد يكون غير مستقر أو تالفاً، يمكنك التراجع إلى الإصدار السابق وتعطيل التحديثات مؤقتاً. وفي المقابل، يمكنك تمكين تحديثات سبق تعطيلها إذا كنت قد أرجأتها لأجل غير مسمى.

يسجل ESET Internet Security لقطات من محرك الكشف ووحدات البرنامج للاستخدام مع ميزة التراجع. لإنشاء لقطات لقاعدة بيانات الفيروسات، استمر في تمكين **إنشاء لقطات من الوحدات النمطية**. عند تمكين **إنشاء لقطات من الوحدات النمطية** ، يتم إنشاء اللقطة الأولى أثناء التحديث الأول. يتم إنشاء اللقطة التالية بعد 48 ساعة. يحدد حقل **عدد اللقطات المخزنة محلياً** عدد اللقطات لمحرك الكشف المخزنة.

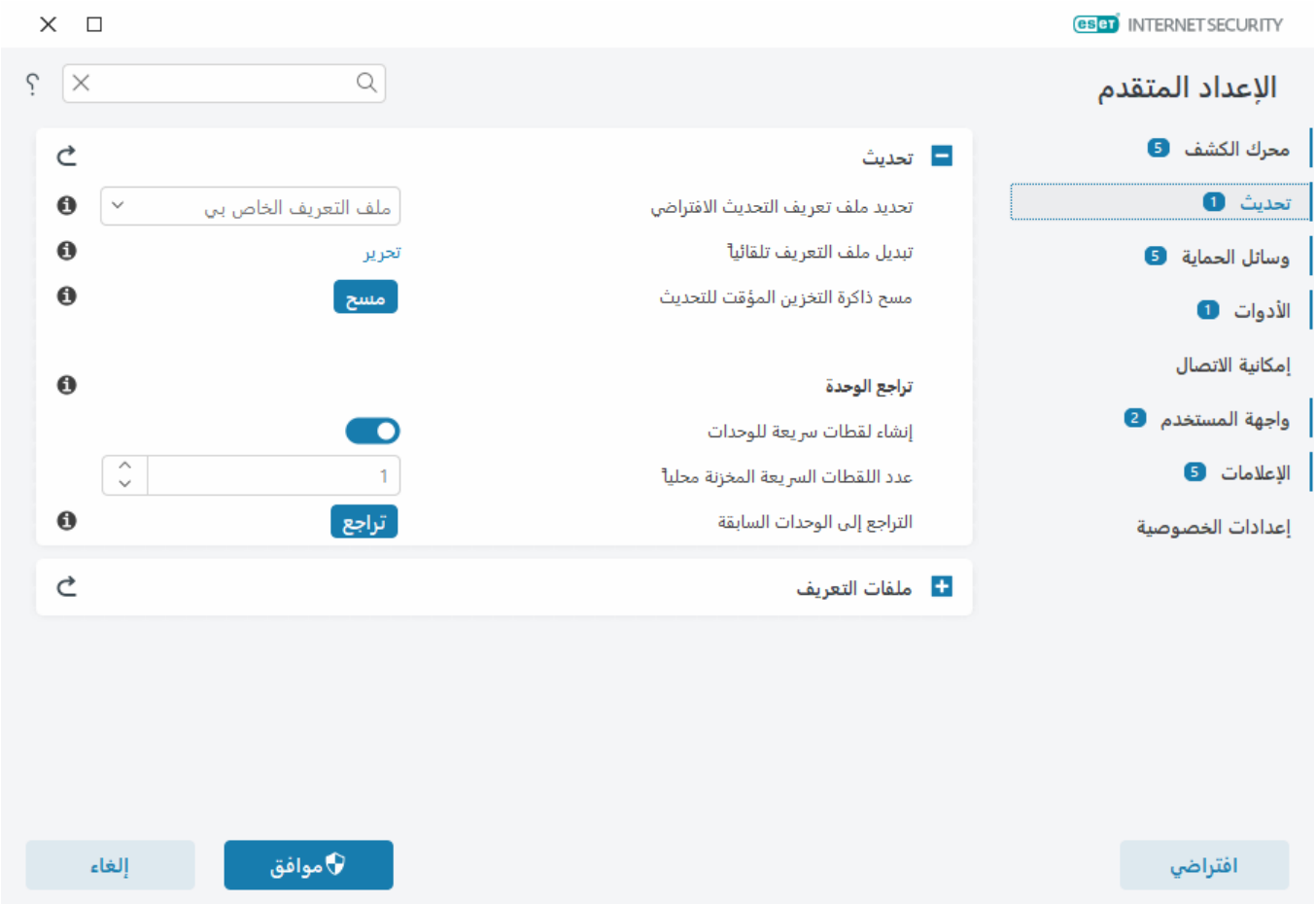
> عند الوصول إلى الحد الأقصى من اللقطات (على سبيل المثال، ثلاثة)، يتم استبدال أقدم لقطة بلقطة جديدة كل 48 ساعة. يُرجع ESET Internet Security إصدارات تحديث محرك الكشف ووحدة البرنامج إلى أقدم لقطة.

إذا نقرت فوق **تراجع** في الإعداد المتقدم > **تحديث** > **تحديث**)، فسيتعين عليك تحديد فاصل زمني من القائمة المنسدلة **المدة** التي

تمثل الفترة الزمنية التي سيتم فيها إيقاف تحديثات محرك الكشف ووحدة البرنامج مؤقتاً.

حدد **حتى الإبطال** لتأجيل تحديثات منتظمة لأجل غير مسمى حتى تسترد وظيفة التحديث يدوياً. لا توصي ESET بتحديد هذا الخيار نظراً لأنه يحتوي على خطر أمني محتمل.

في حالة تنفيذ تراجع، يتغير الزر **تراجع** إلى **السماح بالتحديثات**. لا يُسمح بالتحديثات في الفاصل الزمني المحدد من القائمة المسندلة **تعليق التحديثات**. يتم إرجاع إصدار محرك الكشف إلى أقدم إصدار متوفر، ويتم تخزينها كلقطة سريعة في نظام ملفات الكمبيوتر المحلي.



افترض أن 22700 يمثل أحدث إصدار لمحرك الكشف، ويتم تخزين 22698 و22696 كلقطتين لمحرك الكشف. لاحظ أن الرقم 22697 غير متوفر. في هذا المثال، تم إيقاف تشغيل جهاز الكمبيوتر أثناء التحديث 22697، وتم توفير تحديث أحدث قبل تنزيل الإصدار 22697. إذا كان حقل **عدد اللقطات المخزنة محلياً** هو اثنين ونقرت فوق **تراجع** ، فستتم استعادة محرك الكشف (بما في ذلك وحدات البرنامج) إلى الإصدار رقم 22696. قد تستغرق هذه العملية بعض الوقت. تحقق مما إذا كان قد تم إرجاع إصدار محرك الكشف إلى إصدار أقدم على شاشة التحديث.

الفاصل الزمني للتراجع

إذا نقرت فوق **تراجع** في الإعداد المتقدم > **تحديث** > **تحديث**)، فسيتعين عليك تحديد فاصل زمني من القائمة المنسدلة **المدة** التي تمثل الفترة الزمنية التي سيتم فيها إيقاف تحديثات محرك الكشف ووحدة البرنامج مؤقتاً.

حدد **حتى الإبطال** لتأجيل تحديثات منتظمة لأجل غير مسمى حتى تسترد وظيفة التحديث يدوياً. لا توصي ESET بتحديد هذا الخيار نظراً لأنه يحتوي على خطر أمني محتمل.

تحديثات المنتج

يتيح لك قسم **تحديثات المنتج** تثبيت تحديثات الميزات الجديدة تلقائياً عند توفرها.

تُحضر تحديثات ميزة التطبيق ميزات جديدة، أو تُجري تغييرات على الميزات الموجودة بالفعل من إصدارات سابقة. ويمكن إجراؤها تلقائياً دون تدخل المستخدم، أو يمكنك اختيار إعلامك بها. بعد تثبيت تحديث ميزة تطبيق، قد يلزم إعادة تشغيل جهاز الكمبيوتر.

تحديثات ميزة التطبيق – عند تمكين هذا الخيار، سيتم إجراء تحديثات ميزة التطبيق تلقائياً.

خيارات الاتصال

للوصول إلى خيارات إعداد خادم الوكيل لملف تعريف تحديث محدد، افتح الإعداد المتقدم > **تحديثات** > **ملفات التعريف** > **تحديثات** > **خيارات الاتصال**. انقر فوق القائمة المنسدلة **وضع الوكيل** وحدد أحد الخيارات الثلاث التالية:

- عدم استخدام خادم وكيل
- الاتصال عبر خادم وكيل
- استخدام الإعدادات العامة للخادم الوكيل

حدد **استخدام الإعدادات العامة للخادم الوكيل** لاستخدام تكوين الخادم الوكيل المحدد بالفعل في الإعداد المتقدم > **إمكانية الاتصال** > **الخادم الوكيل**.

حدد **عدم استخدام خادم وكيل** لتحديد عدم استخدام خادم وكيل لتحديث ESET Internet Security.

يجب تحديد خيار **الاتصال عبر خادم وكيل** في الحالات التالية:

- يتم استخدام خادم وكيل مختلف عن الخادم المحدد في الإعداد المتقدم > **إمكانية الاتصال** لتحديث ESET Internet Security. في هذا التكوين، يجب تحديد المعلومات للوكيل الجديد تحت عنوان **خادم الوكيل**، **منفذ** الاتصال (3128 افتراضياً)، و**اسم المستخدم** و **كلمة المرور** لخادم الوكيل إذا كان المطلوب.
- لم يتم تعيين إعدادات الخادم الوكيل بشكل عمومي، لكن ESET Internet Security سيتصل بخادم وكيل للتحديثات.
- يتصل الكمبيوتر بالإنترنت عبر خادم وكيل. يتم اكتساب الإعدادات من Internet Explorer أثناء تثبيت البرنامج، لكن إذا تم تغييرها لاحقاً (مثلاً إذا قمت بتغيير ISP) فالرجاء التحقق من صحة إعدادات وكيل الواردة بهذه النافذة. وإلا فلن يتمكن البرنامج من الاتصال بخوادم التحديث.

الإعداد الافتراضي للخادم الوكيل هو **استخدام الإعدادات العامة للخادم الوكيل**.

استخدام الاتصال المباشر إذا كان الوكيل غير متاح – سيتم تخطي الوكيل في أثناء التحديث إذا كان لا يمكن الوصول إليه.

> تُعد حقول **اسم المستخدم** و**كلمة المرور** في هذا القسم محددة للخادم الوكيل. لا تملأ هذين الحقلين إلا إذا كان اسم المستخدم وكلمة المرور مطلوبين للوصول إلى الخادم الوكيل. يجب عدم إكمال هذين الحقلين إلا إذا كنت تعرف أنك ستحتاج إلى كلمة مرور للوصول إلى الإنترنت عبر خادم وكيل.

وسائل الحماية

تحمي وسائل الحماية من هجمات النظام الضارة من خلال التحكم في اتصالات الملفات والبريد الإلكتروني والإنترنت. على سبيل المثال، إذا تم اكتشاف كائن مصنف على أنه برنامج ضار، فسيبدأ العلاج. يمكن لوسائل الحماية التخلص منه عن طريق حظره أولاً ثم تنظيفه أو حذفه أو نقله إلى الحجر الصحي.

لتكوين وسائل الحماية بالتفصيل، افتح الإعداد المتقدم > **وسائل الحماية**.

> لا يجب إجراء تغييرات على وسائل الحماية سوى بواسطة مستخدم متمرس. قد يؤدي التكوين غير الصحيح للإعدادات إلى انخفاض مستوى الحماية.

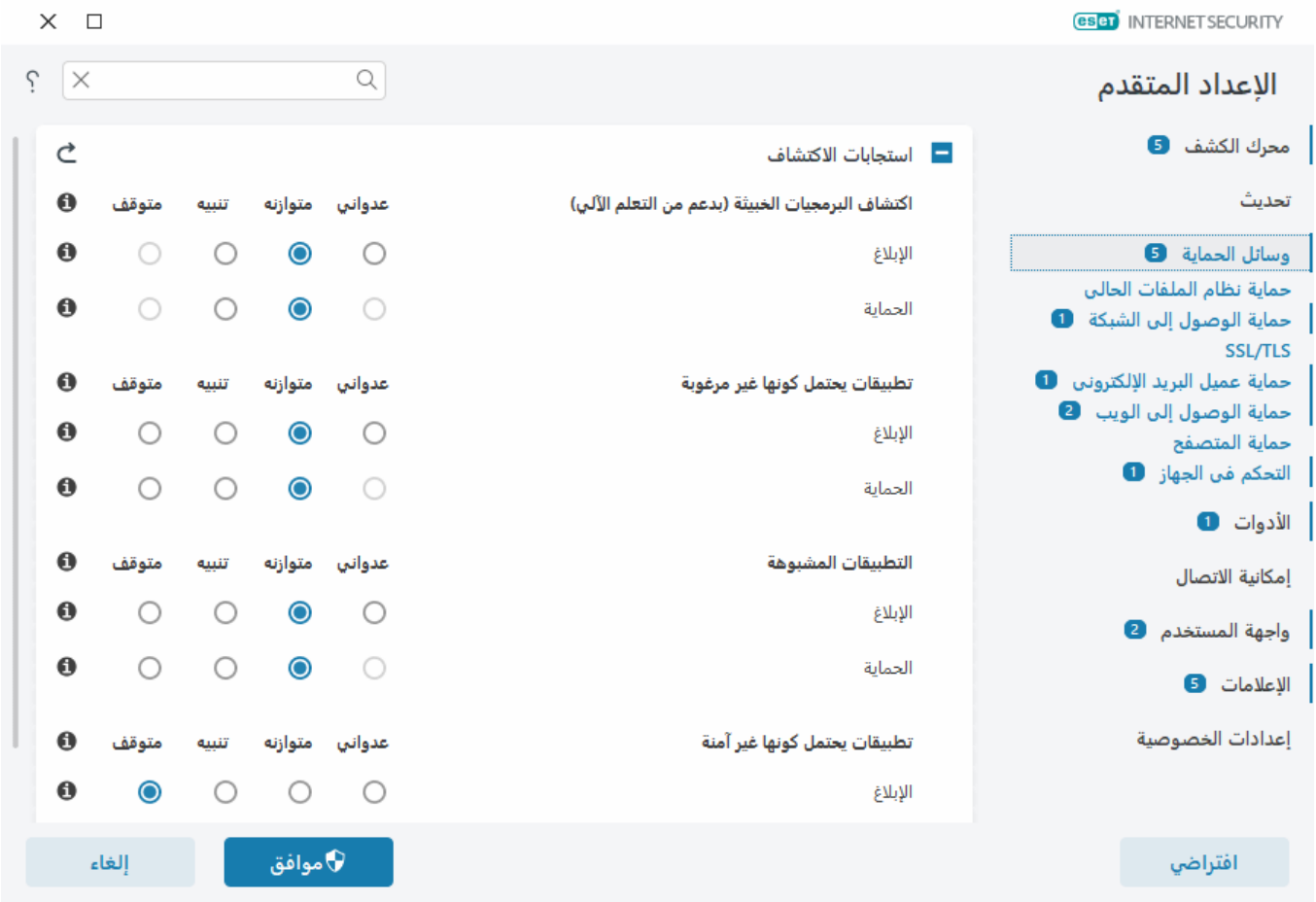
في هذا القسم:

- استجابات الاكتشاف
- إعداد الإبلاغ
- إعداد الحماية

استجابات الاكتشاف

تمكّنك استجابات الاكتشاف من تكوين مستويات التقارير والحماية للفئات التالية:

- **اكتشاف البرمجيات الخبيثة (بدعم من التعلم الآلي)** – فيروس الكمبيوتر هو تعليمة برمجية ضارة مرفق مسبقاً أو يتم إلحاقه بملفات موجودة على الكمبيوتر. ومع ذلك، فكثيراً ما يساء استخدام مصطلح "فيروس". لكن مصطلح "البرامج الضارة" أكثر دقة. يتم إجراء الكشف عن البرامج الضارة بواسطة وحدة محرك الكشف جنباً إلى جنب مع مكون التعلم الآلي. اقرأ المزيد حول هذه الأنواع من التطبيقات في المسرد.
- **التطبيقات المحتملة أن تكون غير مرغوب فيها** – التطبيقات الرمادية أو التطبيقات غير المرغوب فيها (PUAs) هي فئة واسعة من البرامج التي لا تهدف إلى إلحاق الضرر كما هو الحال مع الأنواع الأخرى من البرمجيات الخبيثة، مثل برامج مكافحة الفيروسات أو أحصنة طروادة. ومع ذلك، قد يثبت برامج إضافية غير مرغوب فيها أو يغير سلوك الجهاز الرقمي أو ينفذ أنشطة لا يوافق عليها المستخدم أو يتوقعها.. اقرأ المزيد حول هذه الأنواع من التطبيقات في المسرد.
- **التطبيقات المريبة** – تتضمن البرامج المضغوطة باستخدام أدوات ضاغط الفيروسات أو أدوات الحماية غالباً ما يقوم مؤلفو البرمجيات الخبيثة باستغلال أدوات الحماية هذه للتهرب من الكشف.
- **تطبيقات يحتمل كونها غير آمنة** – تشير إلى برامج تجارية قانونية يمكن إساءة استخدامها لأغراض ضارة. تشمل أمثلة التطبيقات التي يُحتمل كونها غير آمنة (PUAs) أدوات الوصول عن بُعد، وتطبيقات كسر كلمات المرور وبرامج تسجيل ضغطات المفاتيح (وهي برامج تسجل كل ضغطة مفتاح يقوم بها مستخدم). اقرأ المزيد حول هذه الأنواع من التطبيقات في المسرد.



الحماية المحسّنة
يُعد التعلم الآلي المتقدم الآن جزءً من وسائل الحماية كطبقة متقدمة من الحماية والتي تعمل على تحسين الاكتشاف بناءً على التعلم الآلي. اقرأ المزيد ن هذا النوع من الحماية في المسرد.

إعداد الإبلاغ

عند حدوث الكشف (على سبيل المثال، يتم العثور على تهديد وتصنيفه على أنه برنامج ضار)، يتم تسجيل المعلومات في سجل الاكتشافات، وإعلامات سطح المكتب تحدث إذا تم تكوينها في ESET Internet Security.

تم تكوين حد التقارير لكل فئة (يشار إليها باسم "CATEGORY"):

1. اكتشافات البرامج الضارة
2. التطبيقات المحتملة أن تكون غير مرغوب فيها
3. غير آمنة بشكل محتمل
4. التطبيقات المشبوهة

إعداد التقارير باستخدام محرك الكشف، بما في ذلك مكون التعلم الآلي. يمكنك تعيين حد أعلى للإبلاغ من حدالحماية الحالية. لا تؤثر إعدادات التقارير هذه على الحظر أو التنظيف أو حذف الكائنات.

اقرأ ما يلي قبل تعديل عتبة (أو مستوى) لإعداد تقارير "الفئة":

التوضيح	الحد
تم تكوين إبلاغ الفئة إلى أقصى درجة من الحساسية. يتم الإبلاغ عن المزيد من الاكتشافات. يمكن أن يحدد الإعداد **عدواني** بشكل خاطئ الكائنات على أنها الفئة.	**عدواني**
تم تكوين تقارير الفئة على أنها متوازنة. تم تحسين هذا الإعداد لموازنة أداء ودقة معدلات الكشف وعدد الكائنات المقلدة.	**متوازنة**
تم تكوين تقارير الفئة لتقليل الكائنات التي تم تحديدها بشكل خاطئ مع الحفاظ على مستوى كافٍ من الحماية. يتم الإبلاغ عن الكائنات فقط عندما يكون الاحتمال واضحاً ويطابق سلوك الفئة.	**تنبيه**
الإبلاغ عن الفئة غير نشط، ولم يتم العثور على الكشف من هذا النوع أو الإبلاغ عنه أو تنظيفه. ونتيجة لذلك، يعطل هذا الإعداد الحماية من نوع الكشف هذا. "إيقاف التشغيل" غير متاح للإبلاغ عن البرامج الضارة وهو القيمة الافتراضية للتطبيقات التي قد تكون غير آمنة.	**متوقف**

توافر وحدات التحكم في حماية ESET Internet Security

يكون توافر وحدة الحماية (ممكّن أو معطَل) لعتبة الفئة المحددة هي كما يلي:

إيقاف*	تنبيه	متوازنة	عدواني	
س	س	✓ (الوضع المحافظ)	✓ (الوضع العدواني)	وحدة التعلم الآلي المتقدمة
س	✓	✓	✓	وحدة محرك الاكتشاف
س	✓	✓	✓	وحدات الحماية الأخرى

*غير موصى به.

تحديد إصدار المنتج، وإصدارات وحدة البرنامج وتواريخ الإصدار

1. انقر فوق **التعليمات والدعم** > **حول** .**ESET Internet Security**
2. في الشاشة **حول**، يعرض السطر الأول من النص رقم إصدار منتج ESET.
3. انقر فوق **المكوّنات المثبتة** للوصول إلى معلومات حول وحدات محددة.

الملاحظات الأساسية

عدة عناصر أساسية عند إعداد عتبة مناسبة لبيئتك:

- يوصى باستخدام العتبة **متوازنه** لمعظم عمليات الإعداد.
- عتبة الإبلاغ الأعلى، معدل اكتشاف أعلى ولكن فرصة أكبر للأشياء المحددة بشكل خاطئ.
- من وجهة نظر العالم الواقعي، لا يوجد ضمان بنسبة 100٪ للكشف وكذلك فرصة بنسبة 0٪ لتجنب التصنيف غير الصحيح للأشياء النظيفة على أنها برامج ضارة.
- احتفظ بـ ESET Internet Security ووحداتها محدّثة لتضخيم التوازن بين الأداء ودقة معدلات الكشف وعدد الكائنات المبلغ عنها بشكل كاذب.

إعداد الحماية

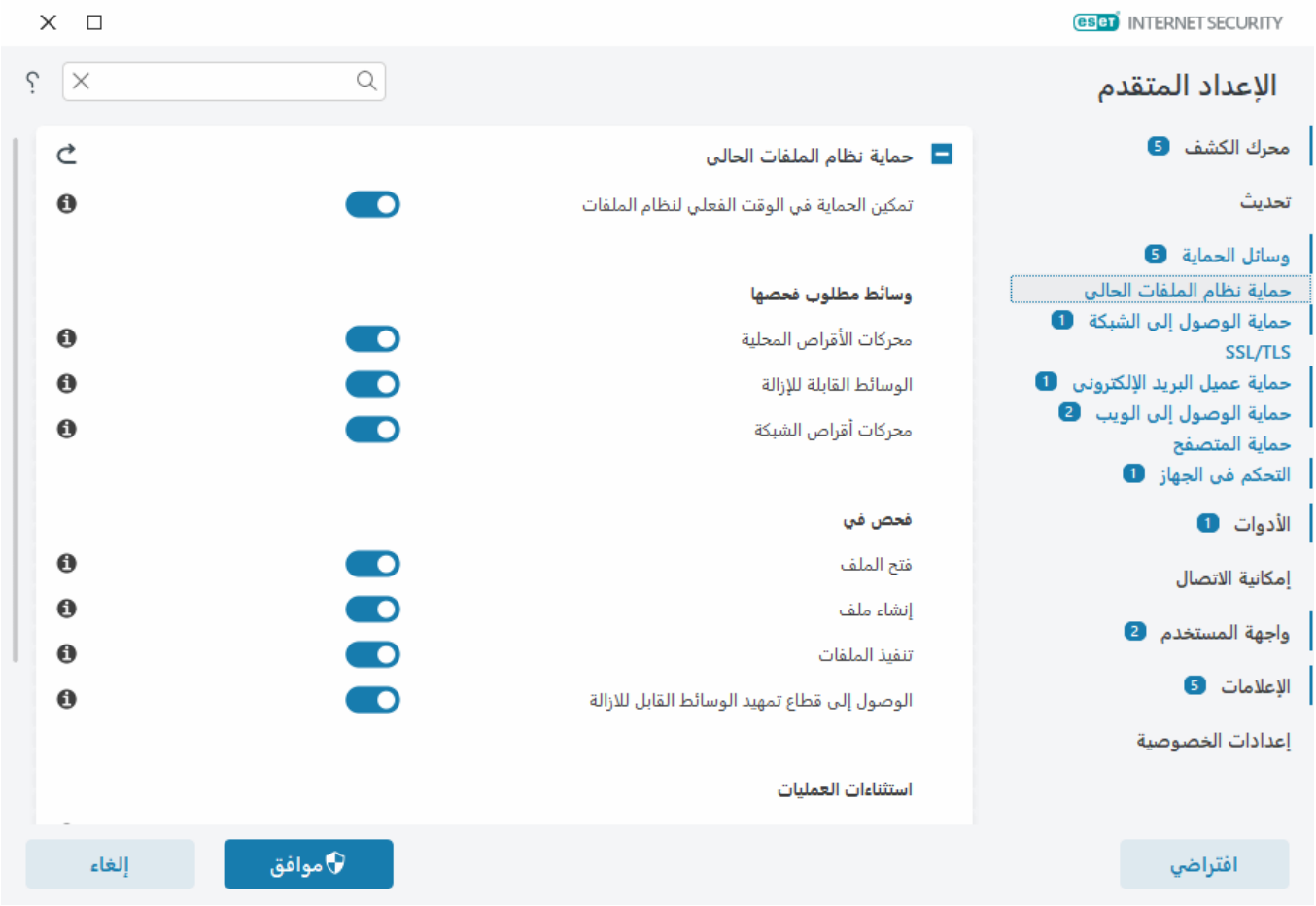
إذا تم الإبلاغ عن كائن مصنف على أنه "فئة"، يقوم البرنامج بحظر الكائن ثم تنظيفه أو حذفه أو نقله إلى عزل.

اقرأ ما يلي قبل تعديل عتبة (أو مستوى) لإعداد تقارير "الفئة":

الحد	التوضيح
عدواني	يتم حظر عمليات الكشف العدوانية (أو الأقل) المبلَغ عنها عن المستوى، حيث يتم بدء الإصلاح التلقائي (أي التنظيف). يوصى بهذا الإعداد عندما يتم فحص جميع نقاط النهاية بإعدادات عدوانية وإضافة كائنات مذكورة كاذبة للكشف عن الاستثناءات.
متوازنة	يتم حظر عمليات الكشف العدوانية (أو الأقل) المبلَغ عنها عن المستوى، حيث يتم بدء الإصلاح التلقائي (أي التنظيف).
تنبيه	تم حظر عمليات الكشف الحذرة المبلغ عنها عن المستويات، وبدء تشغيل الإصلاح التلقائي (أي التنظيف).
متوقف	مفيدة لتحديد الكائنات المبلَغ عنها بشكل كاذب واستبعادها. "إيقاف التشغيل" غير متاح للحماية من البرامج الضارة وهو القيمة الافتراضية للتطبيقات التي قد تكون غير آمنة.

الحماية في الوقت الفعلي لنظام الملفات

تتحكم حماية نظام الملفات في الوقت الفعلي في جميع الملفات الموجودة في النظام للحصول على تعليمات برمجية ضارة عند فتحها أو إنشائها أو تشغيلها.



افتراضياً، يتم تشغيل حماية نظام الملفات الحالي عند بدء تشغيل النظام وتوفر فحصاً دون انقطاع. لا نوصي بتعطيل **تمكين الحماية في الوقت الفعلي لنظام الملفات** في الإعداد المتقدم > **وسائل الحماية** > **حماية نظام الملفات في الوقت الفعلي** > **حماية نظام الملفات في الوقت الفعلي**.

الوسائط المطلوب فحصها

افتراضياً، يتم فحص جميع أنواع الوسائط بحثاً عن تهديدات محتملة:

- **برامج التشغيل المحلية** ـ لفحص جميع محركات الأقراص الثابتة والنظام (مثال: *C:*، *D:*).
- **الوسائط القابلة للإزالة** – لفحص CD/DVDs وتخزين USB وبطاقات الذاكرة وغيرها.
- **برامج تشغيل الشبكة** – لفحص جميع محركات أقراص الشبكة المعينة (مثال: *H:* مثل *\\store04*) أو محركات أقراص شبكة الوصول المباشر (مثال: *\\store08*).

يوصى باستخدام الإعدادات الافتراضية وعدم تعديلها إلا في حالات معينة، مثلاً عند فحص وسائط معينة تبطئ نقل البيانات بشكل واضح.

فحص في

يشكل افتراضي، يتم فحص جميع الملفات عند فتحها أو إنشائها أو تنفيذها. يوصى بالاحتفاظ بهذه الإعدادات الافتراضية، لأنها توفر أقصى مستوى من الحماية في الوقت الفعلي للكمبيوتر الخاص بك:

- **فتح ملف** – للفحص عند فتح ملف.
- **إنشاء ملف** – لفحص ملف تم إنشاؤه أو تعديله.
- **تنفيذ الملفات** – للفحص عند تنفيذ ملف أو تشغيله.
- **الوصول إلى قطاع تمهيد الوسائط القابل للازالة** – عند إدخال الوسائط القابلة للإزالة التي تحتوي على قطاع تمهيد في الجهاز، يتم فحص قطاع التمهيد على الفور. لا يمكّن هذا الخيار مسح ملف الوسائط القابل للإزالة. يقع مسح ملف الوسائط القابل للإزالة على **الوسائط التي سيتم فحصها** > **الوسائط القابلة للإزالة**. لكي يعمل **الوصول إلى قطاع تمهيد الوسائط القابلة للإزالة** بشكل صحيح، حافظ على تمكين **قطاعات التمهيد/UEFI** في ThreatSense.

استثناءات العمليات

اطلع على استثناءات العمليات.

ThreatSense

تفحص حماية نظام الملفات في الوقت الفعلي جميع أنواع الوسائط ويتم تشغيلها بواسطة أحداث النظام المتنوعة كالوصول إلى ملف. باستخدام أساليب اكتشاف تقنية **ThreatSense** (الموضحة في ThreatSense)، يمكن تكوين حماية نظام الملفات في الوقت الفعلي للتعامل مع الملفات المُنشأة حديثاً بشكل مختلف عن تعاملها مع الملفات الموجودة. على سبيل المثال، يمكنك تكوين حماية نظام الملفات في الوقت الفعلي لمراقبة الملفات المُنشأة حديثاً عن قرب أكثر.

لضمان الحد الأدنى من بصمة النظام عند استخدام الحماية في الوقت الفعلي، لا يتم تكرار فحص الملفات التي تم فحصها بالفعل (ما لم يكن قد تم تعديلها). يتم فحص الملفات على الفور مرة أخرى بعد كل عملية تحديث لمحرك الكشف. يتم التحكم في هذا السلوك بواسطة **التحسين الذكي**. في حالة تعطيل **التحسين الذكي** هذا، يتم فحص جميع الملفات كلما تم الوصول إليها. لتعديل هذا الإعداد، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية نظام الملفات في الوقت الفعلي**. انقر فوق **ThreatSense** > **غير ذلك** وحدد الخيار **تمكين التحسين الذكي** أو قم بإلغاء تحديده.

تتيح لك حماية نظام الملفات في الوقت الفعلي أيضاً تكوين المعلمات الإضافية ThreatSense.

استثناءات العمليات

تتيح لك ميزة استثناءات العمليات استثناء عمليات التطبيق من حماية نظام الملفات في الوقت الفعلي. لتحسين سرعة النسخ الاحتياطي، ونزاهة العملية وتوافر الخدمة، يتم استخدام بعض التقنيات المعروف عنها أنها تتعارض مع الحماية من البرامج الضارة على مستوى الملف أثناء النسخ الاحتياطي. الطريقة الوحيدة الفعالة لتجنب كلتا الحالتين عي إلغاء تنشيط برامج مكافحة البرمجيات الخبيثة. من خلال استثناء عملية معينة (على سبيل المثال التي لها حل نسخ احتياطي)، يتم تجاهل جميع عمليات الملفات المنسوبة إلى عملية الاستثناء هذه ويتم اعتبارها آمنة، ومن ثم الحد من التداخل مع عملية النسخ الاحتياطي. نوصيك بتوخي الحذر عند إنشاء استثناءات ـ يمكن لأداة النسخ الاحتياطي التي تم استثنائها الوصول إلى ملفات مصابة بدون إحداث تنبيه وهو سبب السماح للأذونات المستثناة فقط في وحدة تحكم الحماية في الوقت الفعلي.

لا تخلط بين امتدادات الملف المستبعد أو استبعادات HIPS أو استبعادات الاكتشاف أو استبعادات الأداء.

تساعد استثناءات العمليات في الحد من مخاطر التعارضات المحتملة وتحسين أداء التطبيقات المستبعدة، التي بدورها لها تأثير

إيجابي على الأداء الإجمالي واستقرار نظام التشغيل. استثناء عملية / تطبيق هو استثناء لملفه القابل للتنفيذ (*.exe*).

يمكنك إضافة ملفات قابلة للتنفيذ إلى قائمة العمليات المستبعدة في الإعداد المتقدم > **وسائل الحماية** > **حماية نظام الملفات في الوقت الفعلي** > **حماية نظام الملفات في الوقت الفعلي** > **استثناءات العمليات**.

تم تصميم هذه الميزة لاستثناء أدوات النسخ الاحتياطي. إن استثناء عملية أدوات النسخ الاحتياطي من الفح لا تضمن فقط استقرار النظام، لكنها أيضاً لا تؤثر في أداء النسخ الاحتياطي حيث لا يتم إبطاء النسخ الاحتياطي أثناء تشغيله.

انقر فوق **تحرير** لفتح نافذة الإدارة **استثناءات العمليات**، حيث يمكنك إضافة استثناءات واستعراض ملف قابل للتنفيذ (على سبيل المثال *Backup-tool.exe*)، والذي سيتم استبعاده من الفحص.
بمجرد أن تتم إضافة ملف *exe.* إلى الاستبعادات، لا تتم مراقبة نشاط هذه العملية من قبل ESET Internet Security ولا يتم تشغيل أي فحص على أي من عمليات الملفات التي تتم من خلال هذه العملية.

إذا لم تستخدم وظيفة الاستعراض عند تحديد الملف القابل للتنفيذ الخاص بالعملية، فستحتاج إلى إدخال مسار كامل يدوياً إلى الملف القابل للتنفيذ. وإلا، لن يعمل الملف القابل للتنفيذ بشكل صحيح وقد يقوم HIPS بالإبلاغ عن وجود أخطاء.

ويمكنك أيضاً **تحرير** العمليات الحالية أو القيام بعملية **حذف** لها من الاستبعادات.

لا تأخذ حماية الوصول إلى الويب هذا الاستثناء في الاعتبار، لذا إذا قمت باستثناء الملف القابل للتنفيذ لمستعرض الويب لديك، فلا يزال يتم فحص الملفات التي تم تنزيلها. وبهذه الطريقة، لا يزال يتم اكتشاف تسلسل. هذا السيناريو هو عبارة عن مثال فقط، ولا نوصيك بإنشاء استبعادات من مستعرضات الويب.

إضافة استثناءات العمليات او تحريرها

تعمل نافذة مربع الحوار هذه على تمكين **إضافة** العمليات المستثناة من محرك الاكتشاف. تساعد استثناءات العمليات في الحد من مخاطر التعارضات المحتملة وتحسين أداء التطبيقات المستبعدة، التي بدورها لها تأثير إيجابي على الأداء الإجمالي واستقرار نظام التشغيل. استثناء عملية / تطبيق هو استثناء لملفه القابل للتنفيذ (*.exe*).

حدد مسار الملف لتطبيق متوقع بالنقر فوق ... (على سبيل المثال *C:\Program Files\Firefox\Firefox.exe*). لا تقم بكتابة اسم التطبيق.
بمجرد أن تتم إضافة ملف *exe.* إلى الاستبعادات، لا تتم مراقبة نشاط هذه العملية من قبل ESET Internet Security ولا يتم تشغيل أي فحص على أي من عمليات الملفات التي تتم من خلال هذه العملية.

إذا لم تستخدم وظيفة الاستعراض عند تحديد الملف القابل للتنفيذ الخاص بالعملية، فستحتاج إلى إدخال مسار كامل يدوياً إلى الملف القابل للتنفيذ. وإلا، لن يعمل الملف القابل للتنفيذ بشكل صحيح وقد يقوم HIPS بالإبلاغ عن وجود أخطاء.

ويمكنك أيضاً **تحرير** العمليات الحالية أو القيام بعملية **حذف** لها من الاستبعادات.

متى تقوم بتعديل تكوين الحماية في الوقت الفعلي

تعد الحماية في الوقت الفعلي أهم مكون للحفاظ على أمان النظام. لذا توخَّ الحذر عند تعديل معلماته. يوصى بعدم تعديل معلماته إلا في حالات معينة.

بعد تثبيت ESET Internet Security يتم تحسين جميع الإعدادات لتوفير أقصى مستوى من أمان النظام للمستخدمين. لاستعادة الإعدادات الافتراضية، انقر فوق بجوار الإعداد المتقدم > **وسائل الحماية** > **استجابات الكشف**.

التحقق من الحماية في الوقت الفعلي

للتحقق من عمل الحماية في الوقت الفعلي واكتشافها للفيروسات، استخدم اختباراً من *www.eicar.com*. ملف الاختبار هذا ليس ضاراً ويمكن اكتشافه بواسطة جميع برامج مكافحة الفيروسات. وقد أنشأت الملف شركة EICAR (European Institute for Computer Antivirus Research) لاختبار عمل برامج مكافحة الفيروسات.

يتوفر الملف للتنزيل على الموقع http://www.eicar.org/download/eicar.com
بعد إدخال عنوان URL هذا في مستعرضك، سترى رسالة تفيد بأنه تمت إزالة التهديد.

ماذا تفعل إذا لم تعمل الحماية في الوقت الفعلي

في هذا الفصل، نتناول المشكلات التي قد تنشأ عند استخدام الحماية في الوقت الفعلي وكيفية استكشافها وإصلاحها.

الحماية في الوقت الفعلي معطلة

إذا قام مستخدم بتعطيل الحماية الحالية دون قصد، فيجب إعادة تنشيط الميزة. لإعادة تنشيط الحماية الحالية، انتقل إلى **الإعداد** في نافذة البرنامج الرئيسية وانقر فوق **حماية جهاز الكمبيوتر** > **حماية نظام الملفات الحالي**.

إذا لم تبدأ الحماية في الوقت الفعلي عند بدء تشغيل النظام، فيكون ذلك عادةً بسبب تعطيل **تمكين الحماية في الوقت الفعلي لنظام الملفات**. لضمان تمكين هذا الخيار، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية نظام الملفات في الوقت الفعلي**.

إذا لم تكتشف الحماية في الوقت الفعلي حالات التسلل وتنظفها

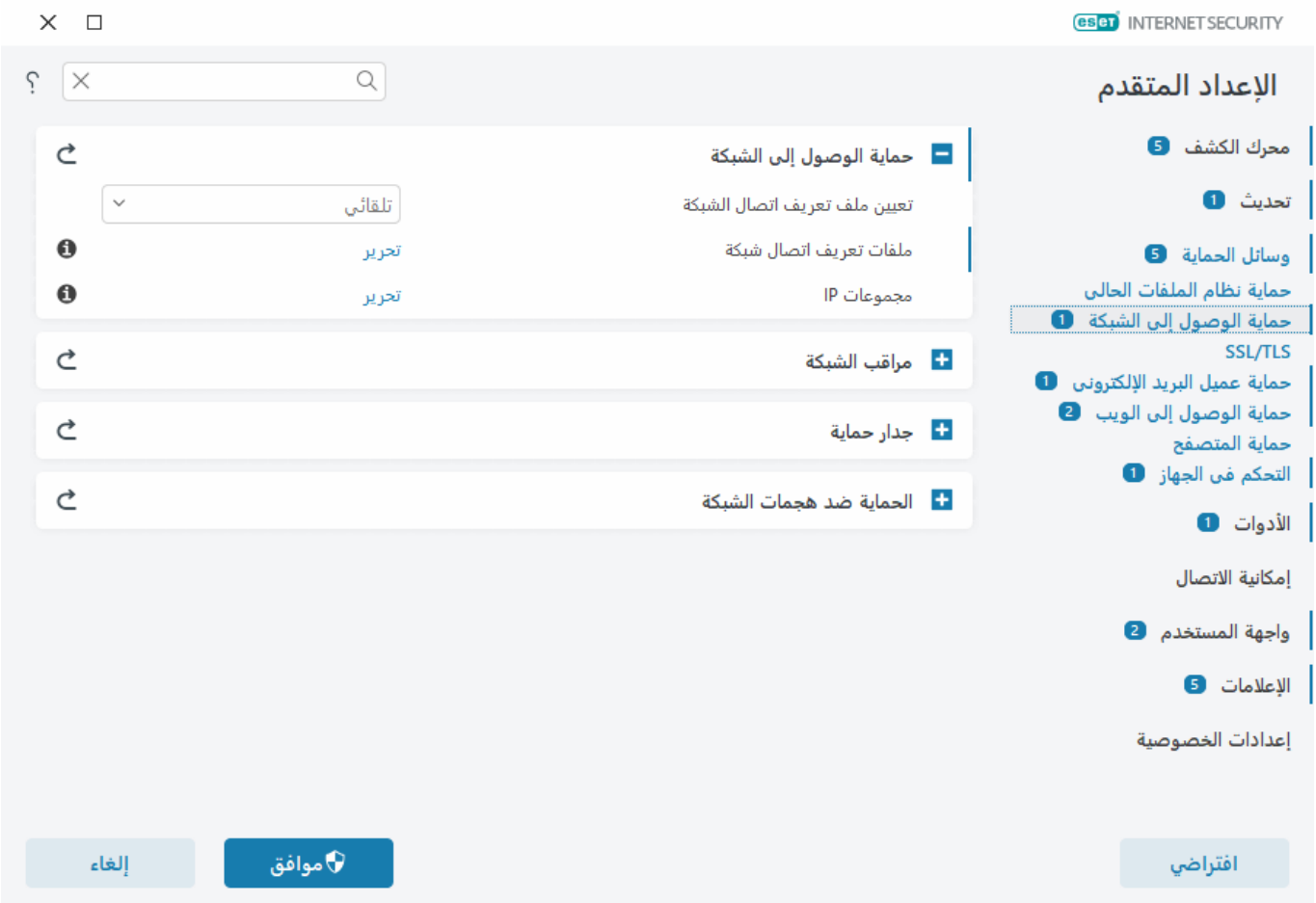
تأكد من عدم تثبيت برامج حماية ضد الفيروسات أخرى على الكمبيوتر. في حالة تثبيت برنامجي من برامج الحماية ضد الفيروسات، فقد يتعارضان مع بعضهما. يوصى بإزالة تثبيت أي برامج حماية ضد الفيروسات أخرى على نظامك قبل تثبيت ESET.

الحماية في الوقت الفعلي لا تبدأ

إذا لم تبدأ الحماية الحالية عند بدء تشغيل النظام (و**حماية نظام الملفات الحالي** ممكَّن)، فقد يكون بسبب تعارضات مع برامج أخرى. لحل المشكلة، يرجى إنشاء سجل ESET SysInspector وإرساله إلى الدعم الفني من ESET لتحليله.

حماية الوصول إلى الشبكة

تمكّنك حماية الوصول إلى الشبكة من تكوين جميع اتصالات الشبكة لديك بالتفصيل. يمكنك السماح أو رفض الوصول إلى جهاز الكمبيوتر لديك على شبكات محددة، والسماح أو رفض الوصول إلى أجهزة الشبكة من جهاز الكمبيوتر لديك والمزيد بناءً على التكوين. افتراضياً، يحتوي ESET Internet Security على قواعد جدار الحماية التي تم تكوينها مسبقاً وحماية الوصول إلى الشبكة للحصول على أقصى قدر من الأمان. ومع ذلك، قد تحتاج بيئات معينة إلى تكوين مخصص. ينبغي أن يتم تغيير الإعدادات الإفتراضية فقط من قبل مستخدم متمرس.



يمكنك تكوين الإعدادات التالية في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** (انقر فوق الروابط أدناه للحصول على وصف تفصيلي لكل خيار من خيارات حماية الوصول إلى الشبكة):

حماية الوصول إلى الشبكة

ملفات تعريف اتصال الشبكة—يمكنك استخدام ملفات التعريف للتحكم في سلوك جدار الحماية لاتصالات شبكة محددة.

مجموعات IP—يمكنك تحديد مجموعات عناوين IP التي تنشئ مجموعة منطقية واحدة من عناوين IP والتي يمكنك استخدامها لقواعد جدار الحماية.

مراقب الشبكة

جدار الحماية

الحماية ضد هجمات الشبكة

ملفات تعريف اتصال شبكة

يمكن استخدام ملفات التعريف للتحكم في سلوك ESET Internet Security حماية الشبكة لاتصالات شبكة محددة. عند إنشاء أو تحرير قاعدة جدار الحماية أو قاعدة IDS أو قاعدة الحماية من الهجوم القسري، يمكنك تعيينها لملف تعريف محدد أو تطبيقها على جميع ملفات التعريف. وعندما يكون ملف التعريف نشطاً في اتصالات شبكة، لا يتم تطبيق سوى القواعد العامة (القواعد التي لم

يتم تحديد ملف تعريف لها) والقواعد التي تم تعيينها إلى ملف التعريف هذا، عليه. يمكنك إنشاء ملفات تعريف متعددة بقواعد مختلفة مخصصة لاتصالات الشبكة لتغيير سلوك جدار الحماية بسهولة.

يمكنك تكوين ملفات تعريف اتصال الشبكة والواجبات في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **حماية الوصول إلى الشبكة**.

تعيين ملف تعريف اتصال الشبكة—يتيح لك اختيار ما إذا كان سيتم تلقائياً تعيين ملف تعريف محدد مسبقاً أو مخصص لاتصالات الشبكة المكتشفة حديثاً (حدد **تلقائي** من القائمة المنسدلة) استناداً إلى المنشطات التي تم تكوينها في ملفات تعريف اتصال الشبكة أو إذا كنت تريد أن يُطلب منك (حدد **السؤال** من القائمة المنسدلة) لتكوين حماية الشبكة وتعيين ملف تعريف يدوياً في كل مرة يتم فيها اكتشاف اتصال شبكة جديد.

يمكنك أيضاً تعيين ملف تعريف اتصال شبكة معين يدوياً في نافذة البرنامج الرئيسية > **الإعداد** > **حماية الشبكة** > **اتصالات الشبكة**. مرر مؤشر الماوس فوق اتصال شبكة معين وانقر فوق أيقونة القائمة ⋮ > **تحرير** لفتح نافذة تكوين حماية الشبكة وتحديد ملف تعريف.

ملفات تعريف اتصال الشبكة—انقر فوق **تحرير** لإضافة ملفات تعريف اتصال الشبكة أو تحريرها.

ملفات التعريف التالية محددة مسبقاً ولا يمكن تحريرها أو حذفها:

خاص—للشبكات الموثوق بها (شبكة منزلية أو شبكة مكتب). يُعد جهاز الكمبيوتر والملفات المشتركة المخزنة عليه مرئياً لمستخدمي الشبكة الآخرين، ويمكن الوصول إلى موارد النظام للمستخدمين الآخرين على الشبكة (تم تمكين الوصول إلى الملفات والطابعات المشتركة وتم تمكين الاتصال الوارد RPC وتُعد مشاركة سطح المكتب البعيد متاحة). نوصي باستخدام هذا الإعداد عند الوصول إلى شبكة محلية آمنة. يتم تعيين ملف التعريف هذا تلقائياً لاتصال الشبكة إذا تم تهيئته كمجال أو شبكة خاصة في Windows.

عام—للشبكات غير الموثوق بها (الشبكة العامة). لا تتم مشاركة الملفات والمجلدات الموجودة على نظامك مع مستخدمين آخرين على الشبكة ولا تكون مرئية لهم ويتم إلغاء تنشيط مشاركة موارد النظام. نوصي باستخدام هذا الإعداد عند الوصول إلى الشبكات اللاسلكية. يتم تعيين ملف التعريف هذا تلقائياً لأي اتصال شبكة لم يتم تهيئته كمجال أو شبكة خاصة في Windows.

عندما يتحول اتصال الشبكة إلى ملف تعريف آخر، يظهر إعلام في الزاوية اليمنى السفلية من شاشتك.

إضافة ملفات تعريف اتصال الشبكة أو تحريرها

يمكنك إضافة ملفات تعريف اتصال الشبكة أو تحريرها في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **حماية الوصول إلى الشبكة** > **ملفات تعريف اتصال الشبكة** > **تحرير**. لتحرير ملف تعريف، يجب تحديده من قائمة نافذة **ملفات تعريف اتصال الشبكة**.

ملفات التعريف التالية محددة مسبقاً ولا يمكن تحريرها أو حذفها:

خاص—للشبكات الموثوق بها (شبكة منزلية أو شبكة مكتب). يُعد جهاز الكمبيوتر والملفات المشتركة المخزنة عليه مرئياً لمستخدمي الشبكة الآخرين، ويمكن الوصول إلى موارد النظام للمستخدمين الآخرين على الشبكة (تم تمكين الوصول إلى الملفات والطابعات المشتركة وتم تمكين الاتصال الوارد RPC وتُعد مشاركة سطح المكتب البعيد متاحة). نوصي باستخدام هذا

الإعداد عند الوصول إلى شبكة محلية آمنة. يتم تعيين ملف التعريف هذا تلقائياً لاتصال الشبكة إذا تم تهيئته كمجال أو شبكة خاصة في Windows.

عام—للشبكات غير الموثوق بها (الشبكة العامة). لا تتم مشاركة الملفات والمجلدات الموجودة على نظامك مع مستخدمين آخرين على الشبكة ولا تكون مرئية لهم ويتم إلغاء تنشيط مشاركة موارد النظام. نوصي باستخدام هذا الإعداد عند الوصول إلى الشبكات اللاسلكية. يتم تعيين ملف التعريف هذا تلقائياً لأي اتصال شبكة لم يتم تهيئته كمجال أو شبكة خاصة في Windows.

أعلى/أعلى/أسفل/أسفل —يتيح لك ضبط مستوى الأولوية لملفات تعريف اتصال الشبكة (يتم تقييم ملفات تعريف اتصال الشبكة وتطبيقها حسب أولويتها. يتم تطبيق ملف التعريف المطابق الأول دائماً).

إضافة ملف تعريف أو تحريره

يتيح لك ملف تعريف اتصال الشبكة المخصص تطبيق قواعد جدار الحماية وتحديد إعدادات إضافية لاتصالات شبكة محددة. ستحدد اتصالات الشبكة التي سيتم تعيين ملف التعريف المخصص لها في قسم المنشطات.

لفتح محرر ملف التعريف، في نافذة **ملفات تعريف اتصال الشبكة**:

- انقر فوق **إضافة**
- حدد أحد ملفات التعريف الموجودة وانقر فوق **تحرير**.
- حدد أحد ملفات التعريف الموجودة وانقر فوق **نسخ**.

الاسم—اسم مخصص لملف التعريف لديك.

الوصف—وصف ملف التعريف للمساعدة في تحديد ملف التعريف.

عناوين موثوقة إضافية—تتم إضافة العناوين المحددة هنا إلى المنطقة الموثوق بها من اتصال الشبكة الذي يتم تطبيق ملف التعريف هذا عليه (بغض النظر عن نوع حماية الشبكة).

اتصال موثوق به—يُعد جهاز الكمبيوتر والملفات المشتركة المخزنة عليه مرئياً لمستخدمي الشبكة الآخرين، ويمكن الوصول إلى موارد النظام للمستخدمين الآخرين على الشبكة (تم تمكين الوصول إلى الملفات والطابعات المشتركة وتم تمكين الاتصال الوارد RPCوتُعد مشاركة سطح المكتب البعيد متاحة). نوصي باستخدام هذا الإعداد عند إنشاء ملف تعريف لاتصال شبكة محلية آمن. تُعد جميع الشبكات الفرعية للشبكة المتصلة بشكل مباشر موثوقة أيضاً. على سبيل المثال، إذا كان محول شبكة ما متصلاً بهذه الشبكة باستخدام عنوان IP رقم 192.168.1.5 وقناع الشبكة الفرعية هو 255.255.255.0، تتم إضافة الشبكة الفرعية 192.168.1.0/24 إلى المنطقة الموثوق بها لاتصال الشبكة هذا. إذا كان المحول يحتوي على المزيد من العناوين أو الشبكات الفرعية، فسيتم الوثوق بها جميعاً.

الإبلاغ عن ضعف تشفير شبكة WiFi—يقومESET Internet Security بعرض إعلام سطح المكتب عند الاتصال بشبكة لاسلكية غير محمية أو بشبكة ذات حماية ضعيفة.

المنشطات—الشروط المخصصة التي يجب الوفاء بها لتعيين ملف تعريف اتصال الشبكة هذا لاتصال الشبكة. راجع المنشطات للحصول على شرح مفصل.

المنشِطات

تُعد المنشطات شروطاً مخصصة يجب الوفاء بها لتعيين ملف تعريف اتصال الشبكة لاتصال الشبكة. إذا كانت الشبكة المتصلة لها نفس السمات المحددة في المنشطات لملف تعريف الشبكة المتصلة، فسيتم تطبيق ملف التعريف على الشبكة. يمكن أن يحتوي ملف تعريف اتصال الشبكة على منشط واحد أو أكثر. في حالة وجود العديد من المنشطات، يتم تطبيق منطق OR (يجب استيفاء شرط واحد على الأقل). يمكنك تعريف المنشطات في محرر ملف تعريف اتصال الشبكة. ينبغي أن يتم إنشاء ملفات تعريف اتصال شبكة مخصصة بواسطة مستخدم متمرس.

تتوفر المنشِطات التالية (إذا كنت تريد معرفة تفاصيل شبكتك الحالية، راجع اتصالات الشبكة):

المحوِّل

نوع المحول—قم بتطبيق ملف التعريف إذا تم تأسيس اتصال الشبكة على نوع المحول المحدد.
اسم المحول—قم بتطبيق ملف التعريف إذا كان اسم محول الشبكة لديك متطابقاً.
محول IP—قم بتطبيق ملف التعريف إذا كان عنوان IP لمحول الشبكة لديك متطابقاً.

DNS

لاحقة DNS—قم بتطبيق ملف التعريف إذا كان اسم النطاق مطابقاً.
DNS IP—قم بتطبيق ملف التعريف إذا كان عنوان IP لخادم DNS مطابقاً.

WINS

قم بتطبيق ملف التعريف إذا تطابق عنوان WINS (IP Windows Internet Name Service) المعين.

DHCP

يطابق **DHCP IP**— عنوان IP الخاص بخادم DHCP.

البوابة الافتراضية

IP—قم بتطبيق ملف التعريف إذا كان عنوان IP الخاص بالبوابة الافتراضية متطابقاً.
عنوان MAC—قم بتطبيق ملف التعريف إذا كان عنوان MAC الخاص بالبوابة الافتراضية متطابقاً.

Wi-Fi

SSID—قم بتطبيق ملف التعريف إذا كان SSID (اسم Wi-Fi) مطابقاً.
اسم ملف التعريف—قم بتطبيق ملف التعريف إذا كان اسم ملف تعريف Wi-Fi مطابقاً.
نوع الأمان—قم بتطبيق ملف التعريف إذا كان نوع الأمان يطابق النوع المحدد من القائمة المنسدلة. (إذا كنت تريد مطابقة أكثر من واحد، قم بإنشاء منشط آخر).
نوع التشفير—قم بتطبيق ملف التعريف إذا كان نوع التشفير يطابق النوع المحدد من القائمة المنسدلة. (إذا كنت تريد مطابقة أكثر من واحد، قم بإنشاء منشط آخر).
أمان الشبكة—قم بتطبيق ملف التعريف إذا كانت الشبكة **مفتوحة/مؤمنة**.

ملف تعريف Windows

قم بتطبيق ملف التعريف إذا تم تكوين الشبكة في Windows **كنطاق/خاص/عام**.

المصادقة

تبحث مصادقة الشبكة عن خادم معين في الشبكة وتستخدم التشفير غير المتماثل (RSA) لمصادقة ذلك الخادم. ينبغي أن يتطابق اسم الشبكة الذي تتم مصادقته مع الاسم المحدد في إعدادات خادم المصادقة. الاسم حساس لحالة الأحرف. يمكن كتابة اسم الخادم كعنوان IP أو DNS أو اسم NetBios.
تنزيل ESET Authentication Server.
يمكن استيراد المفتاح العام باستخدام أي من أنواع الملفات التالية:
• مفتاح PEM العام المشفر (.pem) يمكنك إنشاء هذا المفتاح باستخدام خادم مصادقة ESET
• مفتاح الشهادة المشفر
• شهادة المفتاح العام (.crt)
انقر فوق **اختبار** لاختبار إعداداتك. في حالة نجاح المصادقة، يتم عرض مصادقة الخادم تمت بنجاح. وإذا لم يتم تكوين المصادقة بشكل سليم، فستظهر إحدى رسائل الخطأ التالية:
مصادقة الخادم فشلت. توقيع غير صالح أو غير مطابق.
توقيع الخادم لا يطابق المفتاح العام الذي تم إدخاله.
مصادقة الخادم فشلت. اسم الشبكة غير متطابق.
اسم الشبكة المكوَّن لا يتطابق مع اسم شبكة خادم المصادقة. راجع الاسمين وتأكد من تطابقهما.
مصادقة الخادم فشلت. استجابة غير صالحة من الخادم أو لا توجد استجابة منه.
لم يتم تلقي استجابة إذا لم يكن الخادم يعمل أو لا يمكن الوصول إليه. ربما تم تلقي استجابة غير صالحة في حالة تشغيل خادم HTTP آخر على العنوان المحدد.
تم إدخال مفتاح عام غير صالح.
تحقق أن ملف المفتاح العام الذي قمت بتمكينه غير تالف.

مجموعات IP

تُعد مجموعة IP مجموعة من عناوين IP التي تنشئ مجموعة منطقية واحدة من عناوين IP وهي مفيدة عند إعادة استخدام نفس مجموعة العناوين في قواعد جدار الحماية المتعددة أو قواعد الحماية ضد الهجوم القسري. يحتوي ESET Internet Security أيضاً على مجموعات IP محددة مسبقاً والتي يتم تطبيق القواعد الداخلية عليها. وخير مثال على مثل تلك المجموعة هو **المنطقة الموثوق بها**. تمثل المنطقة الموثوقة مجموعة من عناوين الشبكة حيث يكون جهاز الكمبيوتر والملفات المشتركة المخزنة على جهاز الكمبيوتر لديك مرئية لمستخدمي الشبكة الآخرين، ويمكن الوصول إلى موارد النظام للمستخدمين الآخرين على الشبكة.

لإضافة مجموعة IP:

1. افتح الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **مجموعات IP** > **تحرير**.
2. انقر فوق **إضافة** واكتب **اسم** و**وصف** للمنطقة واكتب عنوان IP بعيد في **عنوان جهاز الكمبيوتر البعيد (IPv4/IPv6 نطاق، قناع)**.
3. انقر فوق **موافق**.

لمزيد من المعلومات، راجع تحرير مجموعات IP.

تحرير مجموعات IP

لمزيد من المعلومات حول مجموعات IP راجع مجموعات IP.

الأعمدة

الاسم – اسم مجموعة أجهزة كمبيوتر بعيدة.

الوصف – وصف عام للمجموعة.

عناوين IP—عناوين IP البعيدة التي تنتمي إلى مجموعة IP.

عناصر التحكم

عند **إضافة** أو **تحرير** منطقة، تكون الحقول التالية متوفرة:

الاسم ـ اسم مجموعة أجهزة كمبيوتر بعيدة.

الوصف – وصف عام للمجموعة.

عنوان الكمبيوتر البعيد (IPv6 IPv4 النطاق، القناع) ـ يتيح لك إضافة عنوان بعيد أو نطاق عناوين أو شبكة فرعية.

حذف – إزالة منطقة من القائمة.

لا يمكن إزالة مجموعات IP المحددة مسبقاً.

أمثلة لعناوين IP

إضافة عنوان IPv4:

العنوان الفردي— يضيف عنوان IP لجهاز كمبيوتر فردي (على سبيل المثال، *192.168.0.10*).

نطاق العناوين — أدخل عنوان البدء وعنوان الانتهاء لعنوان IP لتحديد نطاق IP لأجهزة كمبيوتر عديدة (على سبيل المثال 192.168.0.1 إلى 192.168.0.99).

الشبكة الفرعية – يتم تحديد الشبكة الفرعية (مجموعة من أجهزة الكمبيوتر) عن طريق قناع وعنوان IP. على سبيل المثال، 255.255.255.0 هو قناع الشبكة للشبكة الفرعية 192.168.1.0 . لاستبعاد نوع الشبكة الفرعية بالكامل في *192.168.1.0/24*.

إضافة عناوين IPv6:

العنوان الفردي— يضيف عنوان IP الخاص بكمبيوتر فردي (على سبيل المثال، *2001:718:1c01:16:214:22ff:fec9:ca5*).

الشبكة الفرعية – يتم تحديد الشبكة الفرعية (مجموعة من أجهزة الكمبيوتر) عن طريق قناع وعنوان IP (على سبيل المثال: *c0a8:6301:1::1/64:2002*).

مراقب الشبكة

مراقب الشبكة يمكن أن يساعد في تحديد الثغرات في شبكتك (المنزلية أو المكتب) الموثوقة (على سبيل المثال، المنافذ المفتوحة أو كلمة مرور جهاز التوجيه الضعيفة). يوفر أيضاً قائمة بالأجهزة المتصلة، مصنفة حسب نوع الجهاز (على سبيل المثال، الطابعة، جهاز التوجيه، الجهاز المحمول، إلخ) لتظهر لك ما هو متصل بشبكتك (على سبيل المثال، وحدة التحكم في الألعاب أو إنترنت الأشياء أو غيرها من الأجهزة المنزلية الذكية). يمكنك تهيئة مراقب الشبكة في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **مراقب الشبكة**.

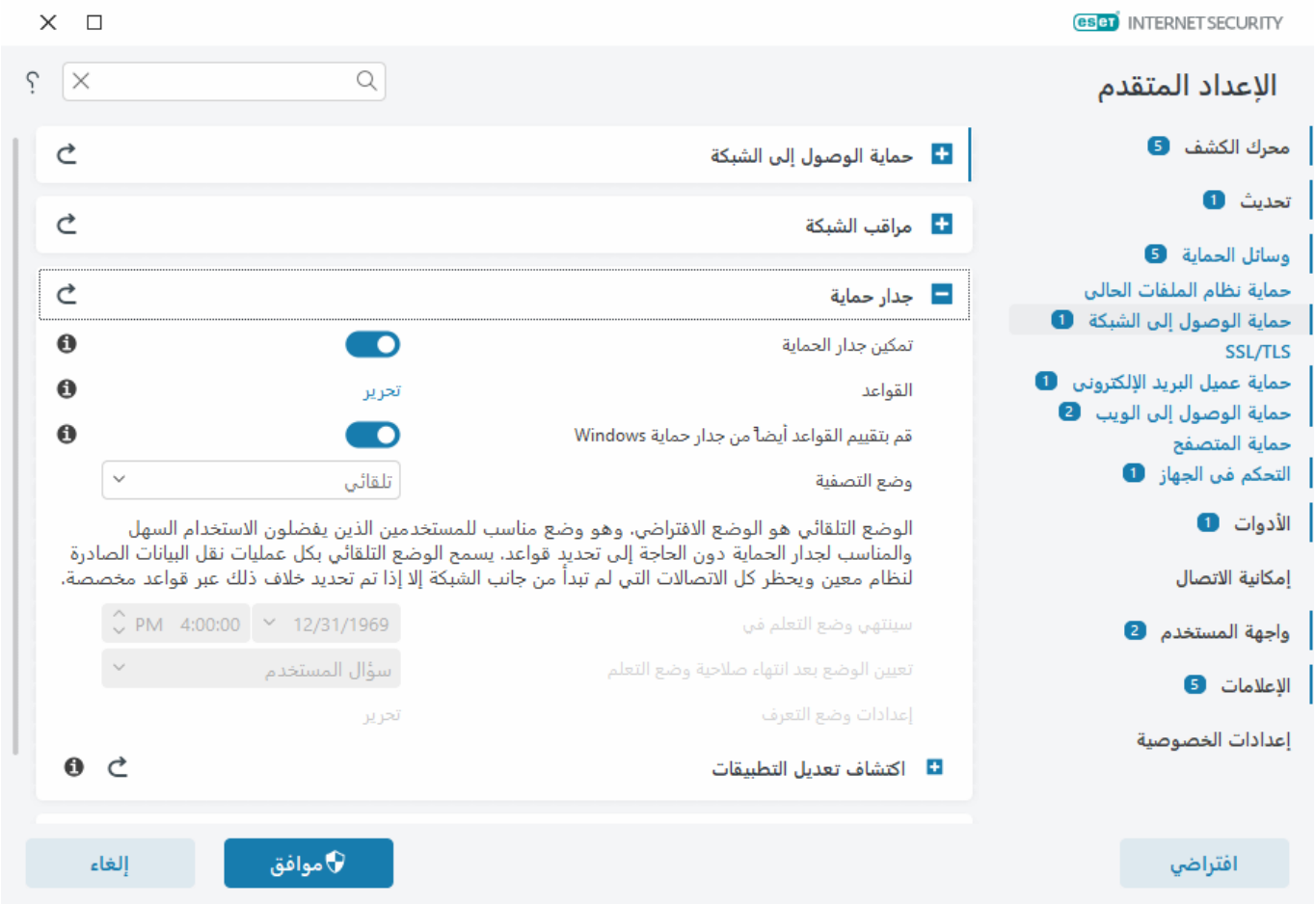
تمكين مراقب الشبكة – يساعد **مراقب الشبكة** في تحديد نقاط الضعف في الشبكة المنزلية مثل المنافذ المفتوحة أو كلمة مرور جهاز التوجيه الضعيفة. توفر أيضاً قائمة بالأجهزة المتصلة، مصنفة حسب نوع الجهاز.

إشعار بأجهزة الشبكات المكتشفة حديثاً – تعمل هذه الخاصية على إشعارك عندك اكتشاف أي جهاز جديد في الشبكة.

جدار حماية

يتحكم جدار الحماية في كل حركة مرور الشبكة الواردة والصادرة على جهاز الكمبيوتر لديك استناداً إلى القواعد الداخلية والقواعد التي تحددها أنت. ويتم ذلك من خلال السماح باتصالات الشبكة الفردية أو رفضها. يوفر جدار الحماية حماية من الهجمات الصادرة من أجهزة بعيدة، كما يمكنه حظر بعض الخدمات التي تحمل تهديدات محتملة.

لتهيئة جدار الحماية، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **جدار الحماية**.



جدار حماية

تمكين جدار الحماية

ننصحك بالإبقاء على تمكين هذه الميزة لضمان حماية نظامك. مع تمكين جدار الحماية، يتم فحص حركة مرور الشبكة في كلا الاتجاهين.

القواعد

يتيح لك إعداد القواعد عرض جميع قواعد جدار الحماية وتحريرها المطبقة على حركة المرور التي تم إنشاؤها بواسطة التطبيقات الفردية ضمن الاتصالات الموثوقة والإنترنت.

يمكنك إنشاء قاعدة IDS في نظام كشف التسلل عندما يهاجم أحد برامج البوت نت جهازك. يمكن تعديل القاعدة في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **الحماية ضد هجمات الشبكة** > **قواعد IDS** بالنقر فوق **تحرير** .

قم بتقييم القواعد أيضاً من جدار حماية Windows

في وضع التصفية التلقائي، اسمح أيضاً بنقل البيانات القادمة المسوح بها من قبل القواعد من جدار حماية Windows ما لم يتم حظرها صراحة من قبل قواعد ESET.

وضع التصفية

يتغير سلوك جدار الحماية حسب وضع التصفية. تؤثر أوضاع التصفية أيضاً على مستوى تدخل المستخدم المطلوب.

تتوفر أوضاع التصفية التالية لجدار الحماية في ESET Internet Security:

وضع التصفية	الوصف
الوضع التلقائي	الوضع الافتراضي. هذا الوضع مناسب للمستخدمين الذي يفضلون الاستخدام السهل والمريح لجدار الحماية دون الحاجة إلى تحديد قواعد. يمكن إنشاء قواعد مخصصة معرفة بواسطة المستخدم، لكنها ليست مطلوبة في **الوضع التلقائي**. يسمح الوضع التلقائي لجميع حركات المرور الصادرة للنظام المعين، ويحظر معظم حركة المرور الواردة عدا بعض حركات المرور من المنطقة الموثوق بها (كما هو محدد في IDS والخيارات المتقدمة / الخدمات المسموح بها) والاستجابات للاتصالات الصادرة الحالية.
الوضع التفاعلي	يسمح لك بإنشاء تكوين مخصص لجدار الحماية. في حالة اكتشاف اتصال مع عدم وجود قواعد تنطبق على هذا الاتصال، يتم عرض نافذة حوار للإبلاغ عن اتصال غير معروف. توفر نافذة الحوار خيار السماح بالاتصال أو رفضه، ويمكن حفظ قرار السماح أو الرفض كقاعدة جديدة لجدار الحماية. إذا اخترت إنشاء قاعدة جديدة، فسيتم السماح بجميع الاتصالات المستقبلية من هذا النوع أو حظرها وفقاً لهذه القاعدة.
وضع مستند الى سياسه	لحظر جميع الاتصالات غير المحددة بواسطة قاعدة معينة تسمح لها. يسمح هذا الوضع للمستخدمين المتقدمين بتحديد قواعد تسمح بالاتصالات المطلوبة والآمنة فقط. سيتم حظر جميع الاتصالات الأخرى غير المحددة بواسطة جدار الحماية.
وضع التعرف	يقوم بإنشاء قواعد وحفظها تلقائياً، هذا الوضع مناسب للتكوين الأولي لجدار الحماية، ولكن ينبغي عدم تركه يعمل لفترة طويلة من الوقت. لا يوجد تدخل مطلوب من المستخدم لأن ESET Internet Security يحفظ القواعد وفقاً لمعلمات محددة مسبقاً. يجب استخدام وضع التعرف فقط حتى يتم إنشاء جميع القواعد للاتصالات المطلوبة من أجل تجنب مخاطر الأمان.

سينتهي وضع التعلم عند—قم بتعيين التاريخ والوقت عندما ينتهي وضع التعلم تلقائياً. يمكنك أيضاً إيقاف تشغيل وضع التعلم يدوياً وقتما تشاء.

تعيين الوضع بعد انتهاء صلاحية وضع التعلم – حدد أي وضع تصفية سيقوم جدار الحماية لـ بالإرجاع إليه بعد انتهاء فترة وضع التعرّف. اقرأ المزيد حول أوضاع التصفية في الجدول أعلاه. عند الانتهاء، يتطلب خيار **اسأل المستخدم** امتيازات إدارية لإجراء تغيير على وضع تصفية جدار الحماية.

إعدادات وضع التعلم—انقر فوق **تحرير** لتكوين المعلمات لحفظ القواعد التي تم إنشاؤها في وضع التعلم.

اكتشاف تعديل التطبيقات

تعرض ميزة الكشف عن تعديل التطبيق الإشعارات إذا حاولت التطبيقات المعدلة، التي توجد لها قاعدة جدار حماية، إنشاء اتصالات.

إعدادات وضع التعرف

ينشئ وضع التعرف قاعدة ويحفظها تلقائياً لكل اتصال يتم إنشاؤه في النظام. لا يوجد تدخل مطلوب من المستخدم لأن ESET Internet Security يحفظ القواعد وفقاً للمعلمات المحددة مسبقاً.

يمكن أن يعرض هذا الوضع نظامك لخطر، ولا يوصى به إلا للتكوين الأولي لجدار الحماية.

حدد **التعلم** من القائمة المنسدلة في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **جدار الحماية جدار الحماية** > **وضع التصفية** لتنشيط خيارات وضع التعلم. انقر فوق **تحرير** بجوار **إعدادات وضع التعلم** لتكوين الخيارات التالية:

عندما تكون في وضع التعرف، لا يقوم جدار الحماية بتصفية الاتصال. يُسمح بجميع الاتصالات الصادرة والواردة. في هذا الوضع، لا يكون جهاز الكمبيوتر محمياً تماماً بواسطة جدار الحماية.

- **نقل البيانات الواردة من المنطقة الموثوق بها** – أحد أمثلة الاتصال الوارد داخل المنطقة الموثوق بها يمكن أن يكون جهاز بعيد من داخل المنطقة الموثوق بها يحاول إنشاء اتصال مع تطبيق محلي مثبت على جهاز الكمبيوتر.
- **نقل البيانات الصادرة إلى المنطقة الموثوق بها** – تطبيق محلي يحاول إنشاء اتصال بجهاز آخر داخل الشبكة المحلية، أو داخل شبكة في المنطقة الموثوق بها.
- **نقل بيانات الإنترنت الواردة** – محاولة جهاز بعيد الاتصال بتطبيق مثبت على جهاز الكمبيوتر.
- **نقل بيانات الإنترنت الصادرة** – محاولة تطبيق محلي إنشاء اتصال بجهاز آخر.

يسمح لك كل قسم بتحديد معلمات لتتم إضافتها إلى قواعد منشأة حديثاً:

إضافة منفذ محلي – يشمل رقم المنفذ المحلي لاتصال الشبكة. للاتصالات الصادرة، يتم عادة إنشاء أرقام عشوائية. لهذا السبب، يوصى بتمكين هذا الخيار للاتصالات الواردة فقط.

إضافة تطبيق – يشمل اسم التطبيق المحلي. هذا الخيار مناسب للقواعد من مستوى التطبيق المستقبلية (القواعد التي تحدد الاتصال لتطبيق بالكامل). على سبيل المثال، يمكنك تمكين الاتصال فقط لمستعرض ويب أو عميل بريد إلكتروني.

إضافة منفذ بعيد – يشمل رقم المنفذ البعيد لاتصال الشبكة. على سبيل المثال، يمكنك السماح بخدمة معينة مرتبطة برقم منفذ قياسي (80 - HTTP و110 - POP3 وغير ذلك) أو رفضها.

إضافة عنوان IP/منطقة موثوق بها عن بُعد – يمكن استخدام عنوان IP بعيد أو منطقة بعيدة كمعلمة للقواعد الجديدة التي تحدد جميع اتصالات الشبكة بين النظام المحلي وذلك العنوان البعيد / تلك المنطقة البعيدة. هذا الخيار مناسب إذا كنت تريد تحديد إجراءات لجهاز معين أو مجموعة أجهزة معينة مرتبطة بشبكة.

أقصى عدد من القواعد المختلفة لتطبيق – في حالة اتصال تطبيق عبر منافذ مختلفة بعناوين IP متنوعة وغيرها، ينشئ جدار الحماية في وضع التعرف عدداً ملائماً من القواعد لهذا التطبيق. يسمح لك هذا الخيار بتقييد عدد القواعد التي يمكن إنشاؤها لتطبيق واحد.

قواعد جدار الحماية

تمثل قواعد جدار الحماية مجموعة من الشروط المستخدمة لاختبار جميع اتصالات الشبكة وجميع الإجراءات المعينة إلى هذه الشروط. باستخدام قواعد جدار الحماية، يمكنك تعريف الإجراء الذي يتم اتخاذه عند إنشاء أنواع مختلفة من اتصالات الشبكة.

يتم تقييم القواعد من أعلى إلى أسفل ويمكنك رؤية أولويتها في العمود الأول. ويُستخدم إجراء أول قاعدة مطابقة لكل اتصال شبكة

يتم تقييمه.

يمكن تقسيم الاتصالات إلى اتصالات واردة واتصالات صادرة. أما الاتصالات الواردة فيتم بدؤها بواسطة جهاز بعيد يحاول إنشاء اتصال مع النظام المحلي. والاتصالات الصادرة تعمل على العكس من ذلك – النظام المحلي هو الذي يتصل بجهاز بعيد.

في حالة اكتشاف اتصال جديد غير معروف، عليك التفكير جيداً في السماح به أو رفضه. جدير بالذكر أن الاتصالات غير المرغوب فيها أو غير الآمنة أو غير المعروفة تشكل خطراً أمنياً على النظام. وفي حالة إنشاء اتصالات كهذه، يوصى بتوخي الحذر بالجهاز البعيد والتطبيق الذي يحاول الاتصال بجهاز الكمبيوتر لديك. فالعديد من حالات التسلل تحاول الحصول على بيانات خاصة وإرسالها، أو تنزيل تطبيقات ضارة أخرى لاستضافة محطات عمل. يتيح لك جدار الحماية اكتشاف هذه الاتصالات وإنهاءها.

يمكنك عرض قواعد جدار الحماية وتحريرها في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **جدار الحماية** > **القواعد** > **تحرير**.

إذا كان لديك العديد من قواعد جدار الحماية، يمكنك استخدام عامل تصفية لعرض قواعد محددة فقط. لتصفية قواعد جدار الحماية، انقر فوق **المزيد من عوامل التصفية** أعلى قائمة قواعد جدار الحماية. يمكنك تصفية القواعد بناءً على المعايير التالية:

- الأصل
- الاتجاه
- الإجراء
- التوافر

افتراضياً، يتم إخفاء قواعد جدار الحماية المحددة مسبقاً. لعرض جميع القواعد المحددة مسبقاً، قم بتعطيل مفتاح التبديل بجوار **إخفاء القواعد المدمجة (المحددة مسبقاً)**. يمكنك تعطيل هذه القواعد، لكن لا يمكنك حذف قاعدة محددة مسبقاً.

انقر فوق أيقونة البحث أعلى اليمين للبحث عن قاعدة (قواعد).

الأعمدة

الأولوية—يتم تقييم القواعد من أعلى إلى أسفل ويمكنك رؤية أولويتها في العمود الأول.

ممكّن ـ يظهر في حالة تمكين قاعدة أو تعطيلها، يجب تحديد خانة الاختيار المناظرة لتنشيط قاعدة.

التطبيق ـ التطبيق الذي تنطبق عليه القاعدة.

الاتجاه ـ اتجاه الاتصال (وارد/صادر/كلاهما).

الإجراء ـ لعرض حالة الاتصال (حظر/سماح/سؤال).

الاسم – اسم القاعدة. تمثل أيقونة ESET قاعدة محددة مسبقاً.

الأوقات المطبقة—إجمالي عدد المرات التي تم فيها تطبيق القاعدة.

انقر فوق أيقونة التوسيع لعرض تفاصيل القاعدة.

عناصر التحكم

إضافة - لإنشاء قاعدة جديدة.

تحرير – تحرير قاعدة موجودة.

حذف ـ إزالة قاعدة موجودة.

نسخ ـ إنشاء نسخة من قاعدة محددة.

للأعلى/لأعلى/لأسفل/للأسفل ـ تتيح لك ضبط مستوى الأولوية للقواعد (يتم تنفيذ القواعد من الأعلى للأسفل).

إضافة قواعد جدار الحماية أو تحريرها

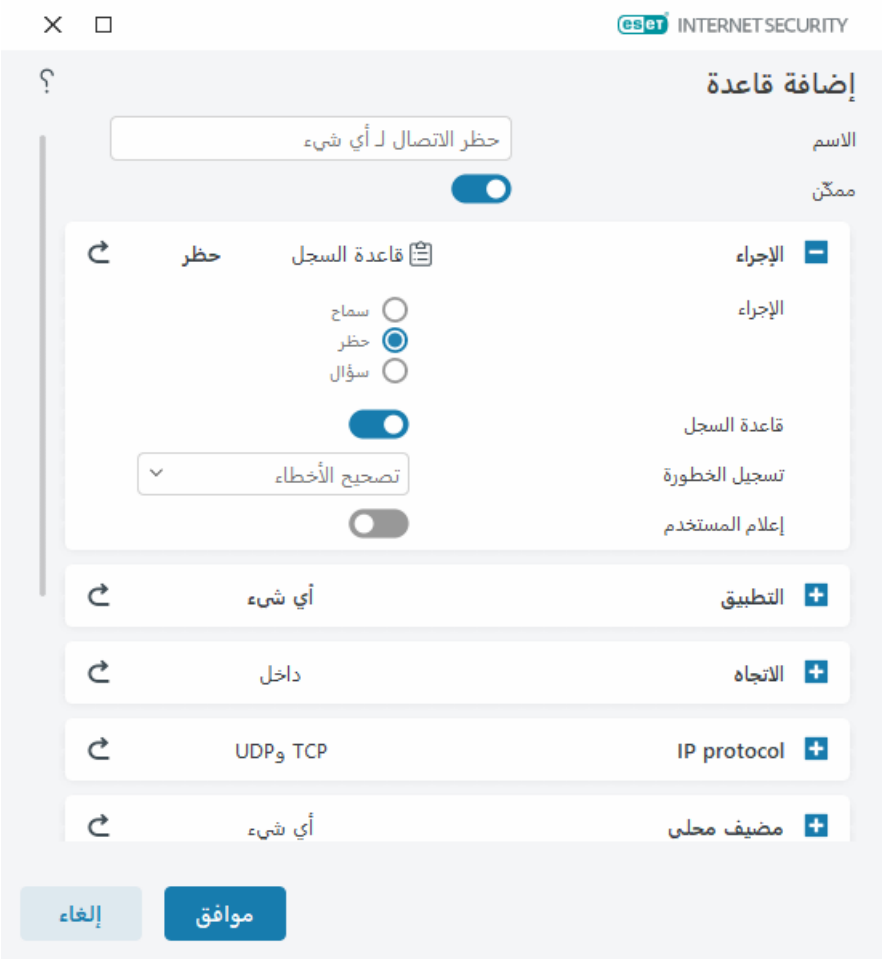
تمثل قواعد جدار الحماية الشروط المستخدمة لاختبار كل اتصالات الشبكة وكل الإجراءات المعينة إلى هذه الشروط. قد يلزم تحرير قواعد جدار الحماية أو إضافتها عند تغيير إعدادات الشبكة (على سبيل المثال، تغيير عنوان الشبكة أو رقم المنفذ للجانب البعيد.) لضمان التشغيل الصحيح لأحد التطبيقات المتأثر بالقاعدة. يجب على المستخدم المتمرس إنشاء قواعد جدار حماية مخصصة.

إرشادات موضحة

قد لا تتوفر مقالات قاعدة معارف ESET التالية إلا باللغة الإنجليزية:

- فتح أو إغلاق (سماح أو رفض) منفذ معين باستخدام جدار حماية
- إنشاء قاعدة جدار حماية من ملفات السجل في ESET Internet Security

لإضافة قاعدة جدار حماية أو تحريرها، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **جدار الحماية** > **القواعد** > **تحرير**. في نافذة قواعد جدار الحماية، انقر فوق **إضافة** أو **تحرير**.



الاسم—اكتب اسماً للقاعدة.

ممكّن—انقر فوق مفتاح التبديل لتنشيط القاعدة.

إضافة إجراءات وشروط لقاعدة جدار الحماية:

الإجراء

الإجراء—حدد ما إذا كنت تريد **السماح/حظر** الاتصال الذي يطابق الشروط المحددة في هذه القاعدة أو إذا كنت تريد ESET Internet Security **السؤال** في كل مرة يتم فيها إنشاء الاتصال.
قاعدة السجل—إذا تم تطبيق القاعدة، فسيتم تسجيلها في ملفات السجل.
خطورة التسجيل—حدد خطورة تسجيل السجل لهذه القاعدة.
إعلام المستخدم – لعرض إعلام عند تطبيق القاعدة.

التطبيق

حدد تطبيقاً حيث سيتم تطبيق هذه القاعدة.
مسار التطبيق—انقر فوق**...** وانتقل إلى تطبيق أو اكتب المسار الكامل للتطبيق (على سبيل المثال C:\Program Files\Firefox\Firefox.exe). لا تقم بكتابة اسم التطبيق وحده.
توقيع التطبيق—يمكنك تطبيق القاعدة على التطبيقات بناءً على توقيعاتها (اسم الناشر). حدد من القائمة المنسدلة إذا كنت تريد تطبيق القاعدة على تطبيقات ذات **أي توقيع صالح** أو على التطبيقات **الموقعة من قبل موقّع معين**. إذا قمت بتحديد التطبيقات **الموقعة من قبل موقّع معين**، يجب تحديد الموقّع في حقل **اسم الموقّع**.
تطبيق Microsoft Store—حدد تطبيقاً مثبتاً من متجر Microsoft Store في القائمة المنسدلة.
الخدمة—يمكنك تحديد خدمة النظام بدلاً من التطبيق. افتح القائمة المنسدلة لتحديد الخدمة.
التطبيق على العمليات الفرعية—قد تقوم بعض التطبيقات بتشغيل المزيد من العمليات بينما ترى نافذة تطبيق واحدة فقط. انقر فوق مفتاح التبديل لتمكين القاعدة لكل عملية في التطبيق المحدد.

الاتجاه

حدد **اتجاه** الاتصال لهذه القاعدة:
- **على حد سواء**—الاتصالات الواردة والصادرة
- **الوارد**—الاتصالات الواردة فقط
- **الصادر**—الاتصالات الصادرة فقط

بروتوكول عنوان IP

حدد **بروتوكولاً** من القائمة المنسدلة إذا كنت تريد فقط تطبيق هذه القاعدة على بروتوكول معين.

مضيف محلي

العناوين المحلية أو نطاق العناوين أو الشبكة الفرعية حيث يتم تطبيق هذه القاعدة. في حالة عدم تحديد عنوان، سيتم تطبيق القاعدة على جميع الاتصالات مع المضيفين المحليين. يمكنك إضافة عناوين IP أو نطاقات العناوين أو الشبكات الفرعية مباشرةً إلى حقل نص **IP** أو الاختيار من مجموعات IP الموجودة بالنقر فوق **تحرير** بجوار **مجموعات IP**.

المنفذ المحلي

رقم/أرقام **المنفذ** المحلي. في حالة عدم توفير أرقام، سيتم تطبيق القاعدة على أي منفذ. أضف منفذ اتصال واحداً أو مجموعة منافذ اتصال.

المضيف البعيد

العنوان البعيد أو نطاق العناوين أو الشبكة الفرعية حيث يتم تطبيق هذه القاعدة. في حالة عدم تحديد عنوان، سيتم تطبيق القاعدة على جميع الاتصالات مع المضيفين البعيدين. يمكنك إضافة عناوين IP أو نطاقات العناوين أو الشبكات الفرعية مباشرةً إلى حقل نص **IP** أو الاختيار من مجموعات IP الموجودة بالنقر فوق **تحرير** بجوار **مجموعات IP**.

المنفذ البعدي

رقم (أرقام) **المنفذ** البعيد. في حالة عدم توفير أرقام، سيتم تطبيق القاعدة على أي منفذ. أضف منفذ اتصال واحداً أو مجموعة منافذ اتصال.

ملف التعريف

يمكن تطبيق قاعدة جدار الحماية على ملفات تعريف اتصال شبكةمحددة.
أي—سيتم تطبيق القاعدة على أي اتصال بالشبكة رغم ملف التعريف المستخدم.
محدد—سيتم تطبيق القاعدة على اتصال شبكة معين بناءً على ملف التعريف المحدد. حدد خانة الاختيار الموجودة بجوار ملفات التعريف التي تريد تحديدها.

في هذا المثال، ننشئ فيه قاعدة جديدة للسماح بوصول تطبيق مستعرض الويب Firefox إلى مواقع ويب الشبكة المحلية / الإنترنت:
1. في قسم **الإجراء**، حدد **الإجراء** > **السماح**.
2. في قسم **التطبيق**، حدد **مسار التطبيق** لمتصفح الويب (على سبيل المثال C:\Program Files\Firefox\Firefox.exe). لا تقم بكتابة اسم التطبيق وحده.
3. في قسم **الاتجاه**، حدد **اتجاه** > **خروج**.
4. في قسم **بروتوكول IP**، حدد **TCP & UDP** من القائمة المنسدلة **للبروتوكول**.
5. في قسم **المنفذ البعيد**، أضف أرقام **المنفذ**: *80,443* للسماح بالتصفح القياسي.

اكتشاف تعديل التطبيقات

تعرض ميزة الكشف عن تعديل التطبيق الإشعارات إذا حاولت التطبيقات المعدلة، التي توجد لها قاعدة جدار حماية، إنشاء اتصالات. تعديل التطبيق هو آلية لاستبدال تطبيق أصلي مؤقتاً أو دائماً بتطبيق آخر بواسطة ملف آخر قابل للتنفيذ (يحمي من إساءة استخدام قواعد جدار الحماية).

الرجاء العلم بأن هذه الميزة ليست معدة لاكتشاف تعديلات على أي تطبيق بشكل عام. وإنما الهدف هو تجنب إساءة استخدام قواعد جدار الحماية الموجودة، ومراقبة التطبيقات التي توجد قواعد جدار حماية معينة لها فقط.

لتحرير **اكتشاف تعديل التطبيقات**، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **جدار الحماية** > **اكتشاف تعديل التطبيقات**.

تمكين اكتشاف تعديلات التطبيقات – في حالة تحديدها، سيراقب البرنامج التطبيقات بحثاً عن تغييرات (تحديثات أو إصابات أو تعديلات أخرى). عندما يحاول تطبيق تم تعديله إنشاء اتصال، سيتم إخطارك بواسطة جدار الحماية.

السماح بتعديل التطبيقات المسجلة (الموثوق بها) – لا يتم الإخطار إذا كان التطبيق يحتوي على التوقيع الرقمي الصالح نفسه قبل التعديل وبعده.

قائمة التطبيقات المستثناة من الفحص – تتيح لك هذه النافذة إضافة أو إزالة تطبيقات فردية مسموح بالتعديلات لها دون إعلام.

قائمة التطبيقات المستثناة من الاكتشاف

يكتشف جدار الحماية في ESET Internet Security تغييرات التطبيقات التي توجد لها قواعد (راجع اكتشاف تعديل التطبيقات).

في بعض الحالات، قد لا تريد استخدام هذه الوظيفة مع بعض التطبيقات إذا كنت تريد استبعادها من الفحص بواسطة جدار الحماية.

إضافة – لفتح نافذة يمكنك منها تحديد تطبيق لإضافته إلى قائمة التطبيقات المستبعدة من اكتشاف التعديل. يمكنك الاختيار من قائمة تطبيقات قيد التشغيل باستخدام اتصال شبكة مفتوح، والتي توجد لها قاعدة جدار حماية أو إضافة تطبيق معين.

تحرير – لفتح نافذة يمكنك منها تغيير موقع التطبيق الموجود في قائمة التطبيقات المستبعدة من اكتشاف التعديل. يمكنك الاختيار من قائمة تطبيقات قيد التشغيل باستخدام اتصال شبكة مفتوح، والتي توجد لها قاعدة جدار حماية أو تغيير الموقع يدوياً.

إزالة – لإزالة إدخالات من قائمة التطبيقات المستبعدة من اكتشاف التعديل.

الحماية ضد هجمات الشبكة (IDS)

تعمل الحماية ضد هجمات الشبكة (IDS) على تحسين الكشف عن عمليات استغلال للثغرات الأمنية المعروفة. اقرأ المزيد حول الحماية ضد هجمات الشبكة في المسرد. لتكوين الحماية ضد هجمات الشبكة، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **الحماية ضد هجمات الشبكة**.

تمكين الحماية ضد هجمات الشبكة (IDS) ـ تحليل محتوى حركة مرور الشبكة والحماية من هجمات الشبكة. وسيتم حظر أي حركة مرور تعد ضارة.

تمكين الحماية ضد البوت نت ـ اكتشاف الاتصال مع خوادم الأوامر والتحكم الضارة وحظر ذلك الاتصال، بناءً على أنماط معتادة عند إصابة الكمبيوتر ومحاولة برنامج بوت (bot) إجراء اتصال. اقرأ المزيد حول الحماية ضد البوت نت في المسرد.

قواعد IDS – يسمح لك هذا الخيار تكوين خيارات التصفية المتقدمة لاكتشاف الأنواع المتعددة من الهجمات وعمليات الاستغلال التي قد يتم استخدامها للإضرار بجهاز الكمبيوتر لديك.

> **إرشادات موضحة**
> قد لا تتوفر مقالات قاعدة معارف ESET التالية إلا باللغة الإنجليزية:
> • استبعاد عنوان IP من IDS في ESET Internet Security

يتم حفظ كافة الأحداث الهامة التي تم الكشف عنها بواسطة حماية الشبكة في ملف سجل. راجع سجل حماية الشبكة لمزيد من المعلومات.

القواعد IDS

في بعض الحالات، قد تكتشف خدمة اكتشاف الاختراق (IDS) التواصل بين أجهزة التوجيه أو غيرها من أجهزة الشبكات الداخلية بمثابة هجوم محتمل. على سبيل المثال، يمكنك إضافة العنوان الآمن المعروف إلى العناوين المستثناة من منطقة IDS لتجاوز IDS.

> **إرشادات موضحة**
> قد لا تتوفر مقالات قاعدة معارف ESET التالية إلا باللغة الإنجليزية:
> • استبعاد عنوان IP من IDS في ESET Internet Security

إدارة قواعد IDS

- **إضافة** – انقر لإنشاء قاعدة IDS جديدة.
- **تحرير** ـ انقر لتحرير قاعدة IDS موجودة.
- **إزالة** – حدده وانقر فوقها إذا كنت تريد إزالة قاعدة موجودة من قائمة قواعد IDS.
- **للأعلى/لأعلى/لأسفل/للأسفل** ـ تتيح لك ضبط مستوى الأولوية للقواعد (يتم تقييم الاستثناءات من الأعلى للأسفل).

محرر القواعد

الكشف – نوع الكشف.

اسم التهديد—يمكنك تحديد اسم تهديد لبعض الاكتشافات المتاحة.

التطبيق – حدد مسار الملف لتطبيق متوقع بالنقر فوق ... (على سبيل المثال *C:\Program Files\Firefox\Firefox.exe*). لا تقم بكتابة اسم التطبيق.

عنوان IP البعيد ـ قائمة بعنوان IPv4 أو IPv6 البعيد / النطاقات / الشبكات الفرعية. يجب الفصل بين العناوين المتعددة بفاصلة.

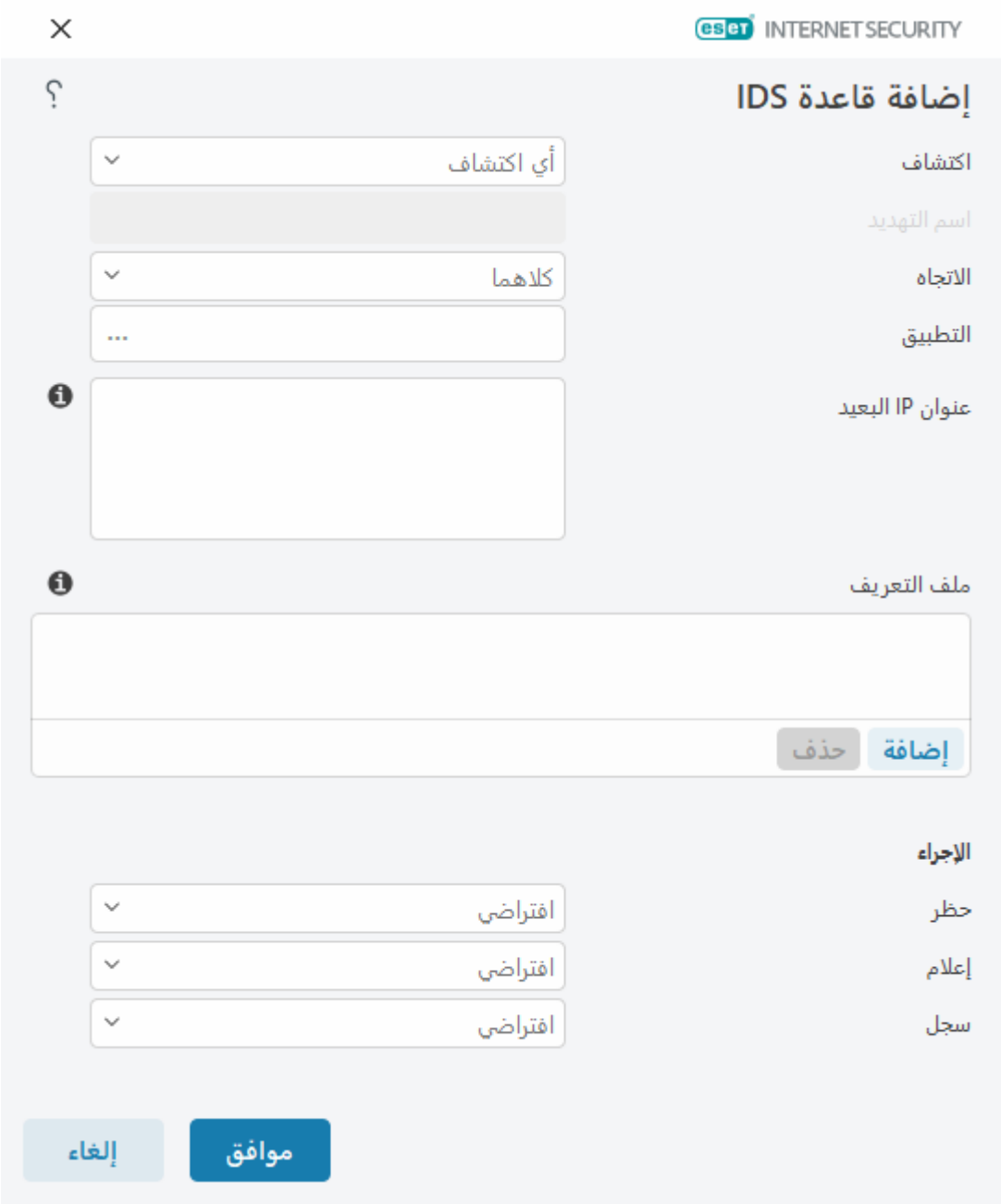
ملف التعريف—يمكنك اختيار ملف تعريف اتصال الشبكة الذي سيتم تطبيق هذه القاعدة عليه.

الإجراء

حظر ـ ـ لكل عملية نظام سلوك افتراضي خاص بها وإجراء معين لها (حظر أو سماح). لتجاوز سلوك افتراضي لـ ESET Internet Security يمكنك اختيار إما حظره أو السماح له باستخدام القائمة المنسدلة.

إعلام – حدد "نعم" لعرض إعلامات سطح المكتب على جهاز الكمبيوتر لديك. حدد "لا" إذا كنت لا تريد إعلامات سطح المكتب. القيم المتاحة هي "افتراضي/نعم/لا".

إعلام – حدد **نعم** لعرض إعلامات سطح المكتب على جهاز الكمبيوتر لديك. حدد **لا** إذا لم تكن تريد إعلامات سطح المكتب. القيم المتاحة هي **افتراضي/نعم/لا**.



أنت تريد عرض إعلام وجمع سجل في كل مرة يتم فيها الحدث:

1. انقر فوق **إضافة** لإضافة قاعدة IDS جديدة.
2. حدّد اكتشافاً معيناً من القائمة المنسدلة **الاكتشاف**.
3. اختر مسار تطبيق بالنقر فوق **...** الذي تريد تطبيق هذا الإعلام عليه.
4. اترك **افتراضي** في القائمة المنسدلة **حظر**. سيرث هذا الإجراء الافتراض المطبق من قبل ESET Internet Security.
5. قم بتعيين كل من القائمتين المنسدلتين **إعلام** و**سجل** على **نعم**.
6. انقر فوق **موافق** لحفظ هذا الإعلام.

إذا لم تكن ترغب في عرض إعلام تناوبي لم تعتبره كتهديد لنوع معين من **الكشف**:

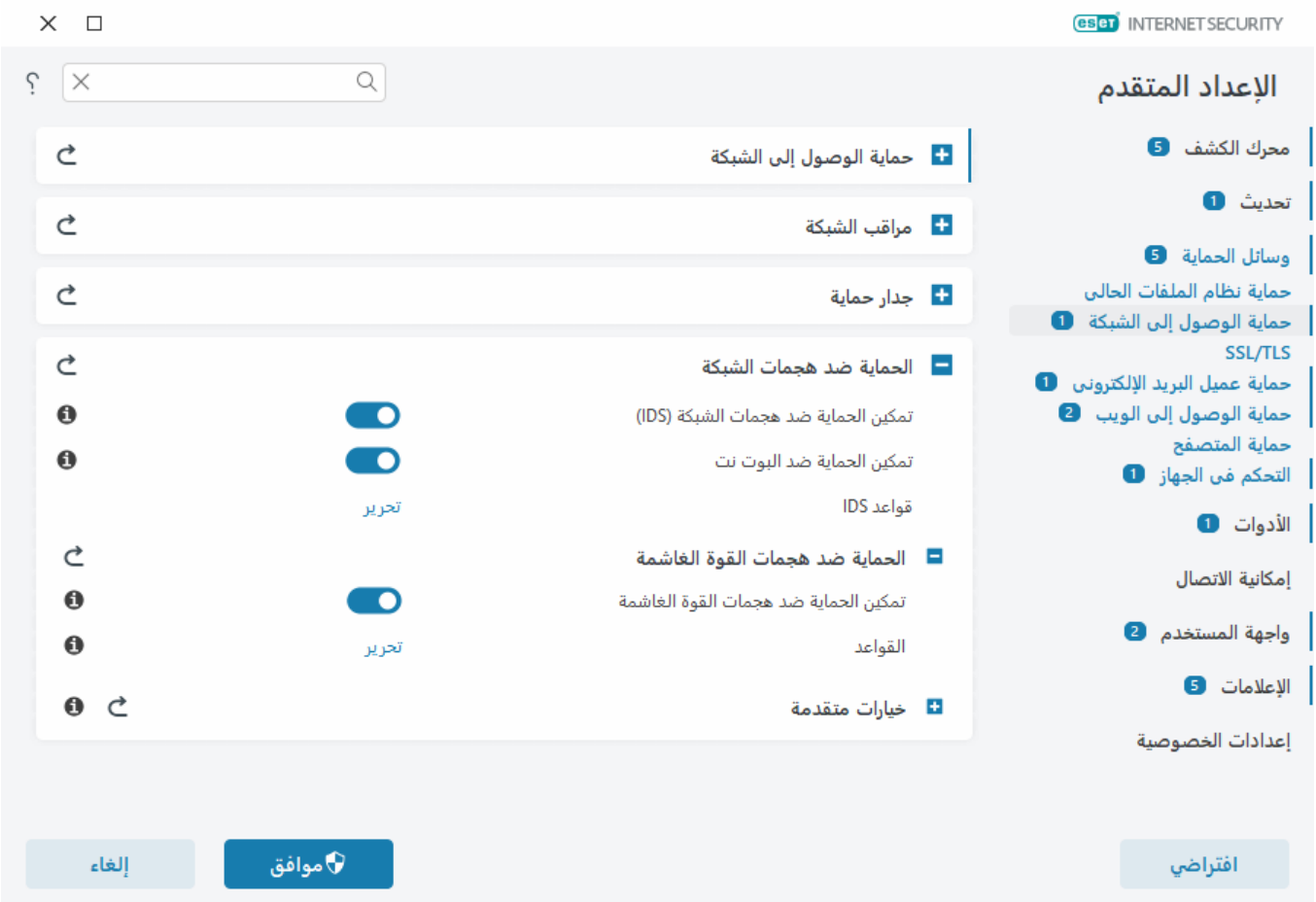
1. انقر فوق **إضافة** لإضافة قاعدة IDS جديدة.
2. حدّد تنبيهاً معيناً من القائمة المنسدلة **الكشف**، على سبيل المثال **جلسة SMB بدون ملحقات الأمان** أو **تهديد فحص البورتات (المداخل) لبروتوكول تحكم الإرسال**.
3. حدد **في** من القائمة المنسدلة الاتجاه في حال كونه من اتصال داخلي.
4. قم بتعيين القائمة المنسدلة **إعلام** على **لا**.
5. قم بتعيين القائمة المنسدلة **سجل** على **نعم**.
6. اترك **التطبيق** فارغاً.
7. إذا لم يكن الاتصال يأتي من عنوان IP معين، فاترك **عنوان IP بعيد** فارغاً.
8. انقر فوق **موافق** لحفظ هذا الإعلام.

الحماية ضد هجمات القوة الغاشمة

تمنع الحماية ضد هجمات القوة الغاشمة هجمات تخمين كلمة المرور لخدمات RDP وSMB. يعد هجوم القوة الغاشمة طريقة لاكتشاف كلمة مرور مستهدفة من خلال تجربة منهجية لجميع المجموعات من الأحرف والأرقام والرموز. لتكوين الحماية ضد الهجوم القسري، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **الحماية ضد هجمات الشبكة** > **الحماية ضد الهجوم القسري**.

تمكين الحماية ضد هجمات القوة الغاشمة – يفحص ESET Internet Security محتوى الضغط على الشبكة ويمنع محاولات هجمات تخمين كلمة المرور.

القواعد – تسمح لك بإنشاء قواعد اتصالات الشبكة الواردة والصادرة وتحريرها وعرضها. لمزيد من المعلومات، راجع فصل القواعد.



القواعد

تسمح لك قواعد الحماية ضد هجمات القوة الغاشمة بإنشاء قواعد اتصالات الشبكة الواردة والصادرة وتحريرها وعرضها. لا يمكن تحرير القواعد المعرّفة مسبقاً أو حذفها.

إدارة قواعد الحماية ضد هجمات القوة الغاشمة

إضافة ـ لإنشاء قاعدة جديدة.

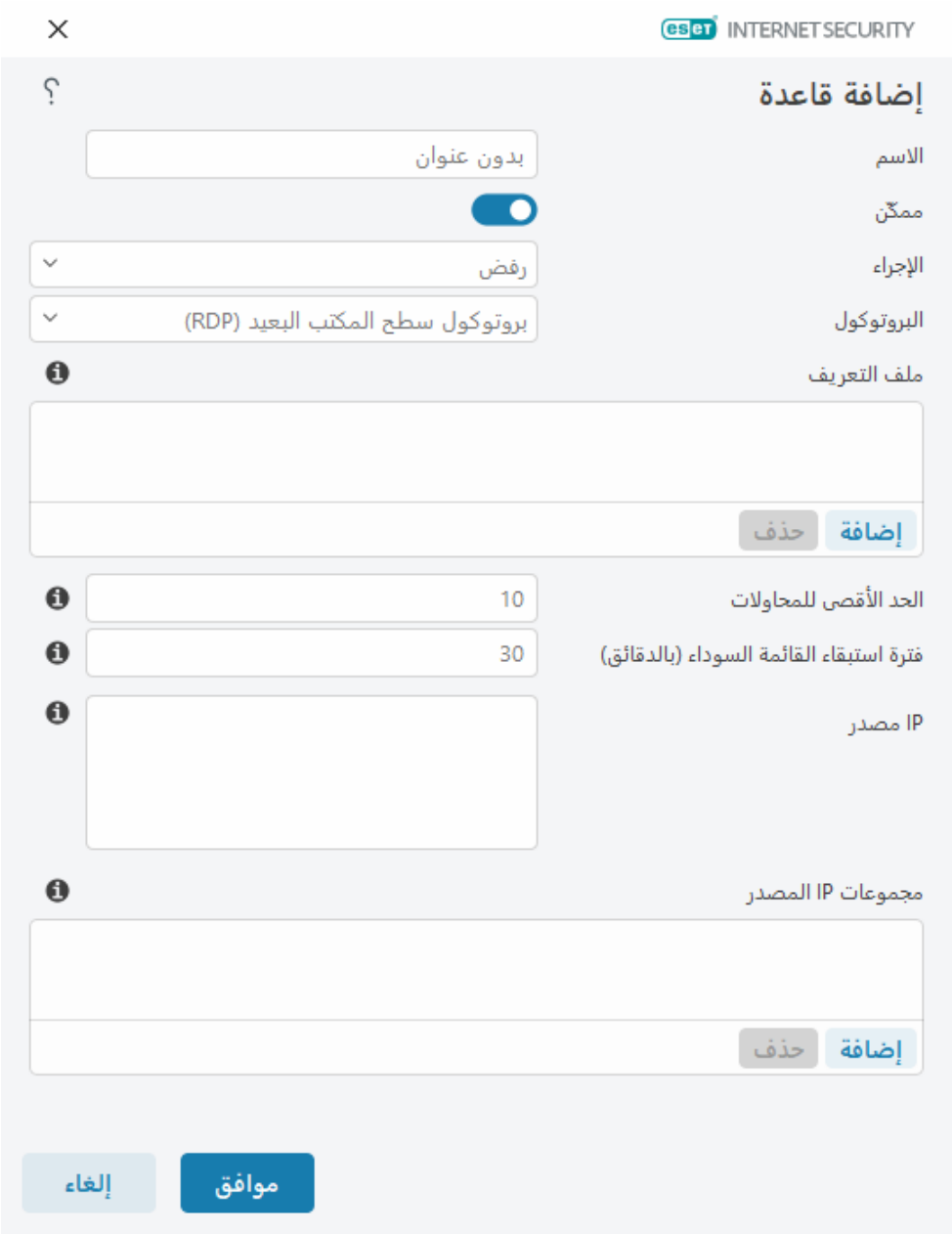
تحرير – تحرير قاعدة موجودة.

حذف ـ قم بإزالة قاعدة موجودة من قائمة القواعد.

للأعلى/لأعلى/لأسفل/للأسفل – اضبط مستوى الأولوية للقواعد.

لضمان أعلى درجة من الحماية الممكنة، يتم تطبيق قاعدة الحظر بأقل قيمة **الحد الأقصى للمحاولات** حتى إذا تم وضع القاعدة في أسفل قائمة القواعد عندما تتطابق قواعد الإغلاق المتعددة مع شروط الاكتشاف.

محرر القواعد



الاسم – اسم القاعدة.

ممكَّن ـ قم بتعطيل شريط التمرير إذا أردت الاحتفاظ بالقاعدة في القائمة مع عدم تطبيقها.

الإجراء ـ اختر ما إذا كنت تريد **رفض** أو **السماح** بالاتصال إذا تم استيفاء إعدادات القاعدة.

البروتوكول – بروتوكول الاتصال الذي ستفحصه هذه القاعدة.

الملف الشخصي ـ يمكن تعيين القواعد القابلة للتعديل وتطبيقها على ملفات تعريف معينة.

الحد الأقصى للمحاولات ـ الحد الأقصى لعدد محاولات تكرار الهجوم المسموح بها حتى يتم حظر عنوان IP وإضافته إلى القائمة السوداء.

فترة استبقاء بالقائمة السوداء (بالدقائق) ـ يحدد وقت انتهاء صلاحية العنوان من القائمة السوداء.

IP المصدر – قائمة بعناوين IP / النطاقات / الشبكات الفرعية. يجب الفصل بين العناوين المتعددة بفاصلة.

مجموعات IP المصدر—مجموعة عناوين IP التي قمت بتعريفها بالفعل في مجموعات IP.

خيارات متقدمة

في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الشبكة** > **الحماية ضد هجمات الشبكة** > **الخيارات المتقدمة**، يمكنك تمكين أو تعطيل اكتشاف العديد من أنواع الهجمات وعمليات الاختراق التي قد تضر بجهاز الكمبيوتر لديك.

في بعض الحالات، لن تتلقى إعلاماً بتهديد حول الاتصالات التي تم حظرها. الرجاء مراجعة قسم التسجيل وإنشاء قواعد أو استثناءات من السجل للاطلاع على إرشادات لعرض جميع الاتصالات التي تم حظرها في سجل جدار الحماية.

قد يختلف توفر خيارات معينة في هذه النافذة حسب نوع منتج ESET ووحدة جدار الحماية أو إصدارهما، وكذلك إصدار نظام التشغيل المثبت لديك.

اكتشاف الاختراق

يراقب الكشف عن التطفل اتصال شبكة الجهاز بحثاً عن أنشطة ضارة.

- **البروتوكولSMB** ـ يكتشف مختلف مشكلات الأمان في بروتوكول SMB ويحظرها.
- **البروتوكول RPC** ـ لاكتشاف مختلف الثغرات وعمليات التعرض الشائعة وحظرها في نظام استدعاء الإجراءات عن بُعد المطور لأجل بيئة الحوسبة الموزعة (DCE).
- **البروتوكول RDP** ـ لاكتشاف CVEs المختلفة وحظرها في بروتوكول RDP (انظر أعلاه).
- **ARP اكتشاف هجمة تسمم بروتوكول** ـ اكتشاف هجمات تسمم ARP التي يتم تشغيلها بواسطة شخص في الهجمات الوسيطة أو اكتشاف عمليات التعرف في محول الشبكة. يُستخدم ARP (بروتوكول تحليل العنوان) بواسطة تطبيق أو جهاز الشبكة لتحديد عنوان Ethernet.
- **اكتشاف هجمة فحص منفذ TCP/UDP** ـ لاكتشاف هجمات برنامج فحص المنفذ ـ تطبيق مصمم لاكتشاف مضيف للمنافذ المفتوحة بإرسال طلبات عملاء إلى مجموعة من عناوين المنافذ بهدف العثور على منافذ نشطة، واختراق ثغرات

الخدمة. اقرأ المزيد حول هذا النوع من الهجمات في المسرد.

- **حظر عنوان غير آمن بعد اكتشاف هجمة** ـ تتم إضافة عناوين IP المكتشفة كمصادر هجمات إلى قائمة الحظر لمنع الاتصال خلال مدة زمنية معينة. يمكنك تحديد **فترة استبقاء القائمة السوداء**، والتي تحدد الوقت الذي سيتم فيه حظر العنوان بعد اكتشاف الهجوم.
- **إعلام بشأن اكتشاف الهجمة** – لتشغيل إعلام منطقة Windows بفي الزاوية اليمنى السفلية من الشاشة.
- **عرض الإعلامات أيضاً لهجمات واردة ضد فجوات الأمان** ـ لتنبيهك في حالة اكتشاف هجمات ضد فجوات الأمان أو في حالة إجراء محاولة عبر تهديد يهدف إلى دخول النظام بهذه الطريقة.

فحص الحزمة

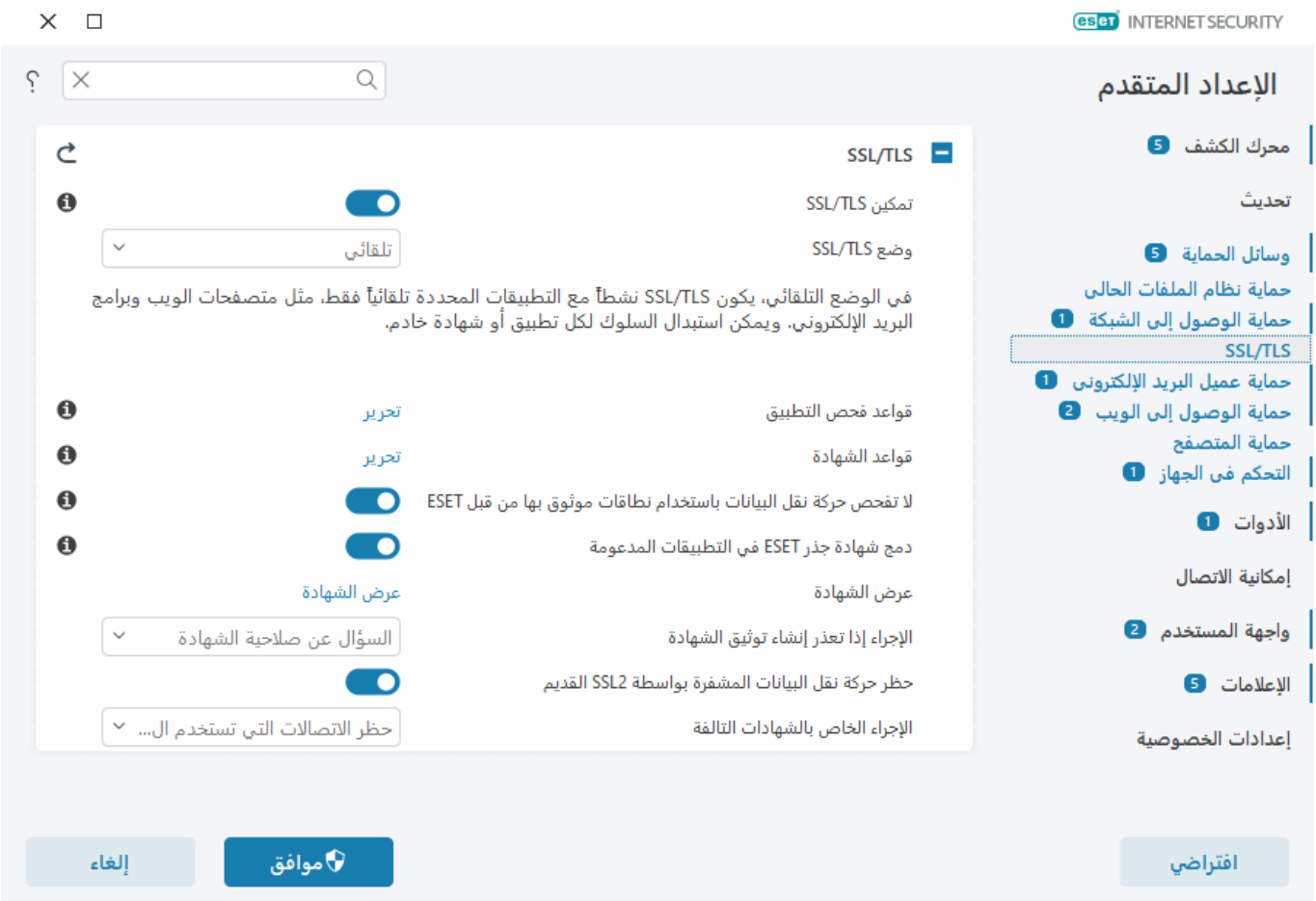
نوع من تحليل الحزمة يقوم بتصفية البيانات التي يتم نقلها عبر الشبكة.

- **السماح بالاتصال الوارد بمشاركات المسؤول في بروتوكول SMB** ـ تعد المشاركات الإدارية (مشاركات المسؤولين) مشاركات الشبكة الافتراضية التي تتشارك أقسام محرك الأقراص الثابت (*$C* و*$D*...) في النظام مع مجلد النظام (*$ADMIN*). يجب أن يقلل تعطيل الاتصال بمشاركات المسؤولين الكثير من مخاطر الأمان. على سبيل المثال، ينفذ الفيروس المتنقل Conficker هجمات قواميس للاتصال بمشاركات المسؤولين.
- **رفض لهجات SMB القديمة (غير المدعومة)** ـ رفض جلسات SMB التي تستخدم لهجة SMB قديمة غير مدعومة بواسطة IDS. تدعم أنظمة تشغيل Windows الحديثة لهجات SMB القديمة نظراً للتوافق مع إصدارات أقدم من أنظمة التشغيل مثل Windows 95. ويمكن للمهاجم استخدام لهجة قديمة في جلسة SMB للتهرب من فحص المرور. ارفض أي لهجات SMB قديمة إذا لم يكن الكمبيوتر الخاص بك بحاجة إلى مشاركة ملفات (أو استخدام اتصال SMB بشكل عام) مع كمبيوتر به إصدار أقدم من Windows.
- **رفض جلسات SMB بدون أمان موسع** ـ يمكن استخدام الأمان الموسع أثناء تفاوض جلسة SMB لتوفير آلية مصادقة أكثر أماناً من مصادقة LM (LAN Manager Challenge/Response). يعد مخطط LM ضعيفاً، ولا يوصى باستخدامه.
- **رفض فتح الملفات القابلة للتنفيذ على أحد الخوادم الموجودة خارج المنطقة الموثوق بها في بروتوكول SMB** ـ لإبعاد الاتصال عندما تحاول فتح ملف تنفيذي (.dll, .exe, ...) من مجلد مشترك على الخادم لا ينتمي إلى المنطقة الموثوقة في جدار الحماية. لاحظ أن نسخ الملفات القابلة للتنفيذ من مصادر موثوقة يمكن أن يكون قانونياً. لاحظ أن نسخ الملفات التنفيذية من مصادر موثوقة يمكن أن يكون قانونياً، ولكن هذا الاكتشاف يجب أن يحد من مخاطر الفتح غير المرغوب فيه لملف على خادم ضار (كملف يُفتح بالنقر فوق ارتباط تشعبي إلى ملف تنفيذي ضار مشترك مثلاً).
- **رفض مصادقة NTLM في بروتوكول SMB لتوصيل أحد الخوادم خارج المنطقة الموثوق بها** ـ تخضع البروتوكولات التي تستخدم مخططات مصادقة NTLMNTLM (الإصدارين كليهما) لهجمة إعادة توجيه بيانات اعتماد (تُعرف بهجمة ترحيل SMB في حالة بروتوكول SMB). يجب أن يحد رفض مصادقة NTLM بخادم خارج المنطقة الموثوق بها من المخاطر الناتجة عن إعادة توجيه بيانات الاعتماد بواسطة خادم ضار خارج المنطقة الموثوق بها. وبالمثل، يمكنك رفض مصادقة NTLM مع الخوادم في المنطقة الموثوق بها.
- **السماح بالاتصال بخدمة مدير حساب الأمان** – لمزيد من المعلومات حول هذه الخدمة، راجع [MS-SAMR].
- **السماح بالاتصال بخدمة جهة الأمان المحلية** ـ لمزيد من المعلومات حول هذه الخدمة، راجع [MS-LSAD] و[MS-LSAT].
- **السماح بالاتصال بخدمة السجل البعيد** ـ لمزيد من المعلومات حول هذه الخدمة، راجع [MS-RRP].
- **السماح بالاتصال بخدمة مدير التحكم بالخدمة** ـ لمزيد من المعلومات حول هذه الخدمة، راجع [MS-SCMR].

- **السماح بالاتصال بخدمة الخادم** – لمزيد من المعلومات حول هذه الخدمة، راجع [MS-SRVS].
- **السماح بالاتصال بالخدمات الأخرى** – خدمات MSRPC الأخرى. MSRPC هو تنفيذ Microsoft لآلية DCE RPC. علاوة على ذلك، يمكن أن يستخدم MSRPC ممرات بيانات مسماة محمولة في بروتوكول SMB (مشاركة ملفات الشبكة) للنقل (نقل ncacn_np). توفر خدمات MSRPC واجهات للوصول إلى أنظمة Windows وإدارتها عن بُعد. تم اكتشاف العديد من ثغرات الأمان واختراقها في الفضاء ضمن نظام Windows MSRPC (على سبيل المثال، الفيروس المتنقل Conficker والفيروس المتنقل Sasser وغيرها). قم بتعطيل الاتصال بخدمات MSRPC التي لا تحتاج إلى تقديمها للحد من مخاطر الأمان (مثل تنفيذ التعليمة البرمجية البعيدة أو هجمات فشل الخدمة).

SSL/TLS

يمكن لـ ESET Internet Security التحقق من تهديدات الاتصال التي تستخدم البروتوكول SSL. ويمكنك استخدام العديد من أوضاع التصفية لفحص الاتصالات المحمية ببروتوكول SSL ذات الشهادات الموثوق بها أو الشهادات غير المعروفة أو الشهادات المستبعدة من فحص الاتصالات المحمية ببروتوكول SSL. لتحرير إعدادات SSL/TLS افتح الإعداد المتقدم > **وسائل الحماية** > **SSL/TLS**.



التمكين SSL/TLS—في حالة التعطيل، لن يقوم ESET Internet Security بفحص الاتصال عبر SSL/TLS.

وضع SSL/TLS توفر بالخيارات التالية:

الوصف	وضع التصفية
سيقوم الوضع الافتراضي فقط بفحص التطبيقات المناسبة مثل مستعرضات الويب وعملاء البريد الإلكتروني. يمكنك تجاوزه عن طريق تحديد التطبيقات التي يتم فيها فحص الاتصال.	**تلقائي**

الوصف	وضع التصفية
إذا دخلت موقعاً جديداً محمياً ببروتوكول SSL (باستخدام شهادة غير معروفة)، يتم عرض مربع حوار لتحديد الإجراء. ويتيح لك هذا الوضع إنشاء قائمة بشهادات /تطبيقات SSL التي سيتم استبعادها من الفحص.	**تفاعلي**
حدد هذا الخيار لفحص كل الاتصالات المحمية ببروتوكول SSL عدا الاتصالات المحمية بالشهادات المستبعدة من الفحص. وفي حالة إنشاء اتصال جديد يستخدم شهادة موقعة غير معروفة، لن يتم إخطارك وستتم تصفية الاتصال تلقائياً. وعندما تتصل بخادم محمي بشهادة غير موثوق بها ومميزة كموثوق بها (أي أنها في قائمة الشهادات الموثوق بها)، يتم السماح بالاتصال بالخادم وتتم تصفية محتوى قناة الاتصال.	**مستند إلى السياسة**

قواعد فحص التطبيقات—تسمح لك بتخصيص ESET Internet Security السلوك لتطبيقات محددة.

قواعد الشهادة—تتيح لك دائماً تخصيص ESET Internet Securityسلوك لشهاداتSSL معينة.

لا تفحص حركة المرور بالمجالات الموثوقة من قبل ESET—عند التمكين، سيتم استبعاد الاتصال بالمجالات الموثوقة من الفحص. تحدد القائمة البيضاء المدمجة المُدارة من ESET موثوقية المجال.

دمج شهادة جذر ESET في التطبيقات المدعومة – لكي يعمل الاتصال المحمي ببروتوكول SSL بشكل سليم في المستعرضات/البرامج العميلة للبريد الإلكتروني لديك، يجب إضافة الشهادة الجذر لبرنامج ESET إلى قائمة الشهادات (الناشرين) الجذر المعروفة. عند تمكين ESET Internet Security سيقوم تلقائياً بإضافة شهادة ESET SSL Filter CA إلى مستعرضات معروفة (على سبيل المثال Opera). بالنسبة للمستعرضات التي تستخدم متجر شهادات النظام، تتم إضافة الشهادة تلقائياً. على سبيل المثال، يتم تكوين Firefox تلقائياً لاعتماد جهات الجذر الموثوقة في متجر شهادات النظام.

لتطبيق الشهادة على مستعرضات غير مدعومة، انقر فوق **عرض الشهادة** > **التفاصيل** > **نسخ إلى ملف...**، ثم قم باستيرادها يدوياً إلى المستعرض.

الإجراء إذا تعذر إنشاء الثقة بالشهادة—في بعض الحالات، لا يمكن التحقق من شهادة موقع الويب باستخدام مخزن Trusted Root Certification Authorities (TRCA) (على سبيل المثال، الشهادة منتهية الصلاحية أو الشهادة غير الموثوق بها أو الشهادة غير الصالحة للمجال المحدد أو التوقيع الذي يمكن تحليله ولكن لا يوقع الشهادة بشكل صحيح). ستستخدم مواقع الويب الشرعية دائماً الشهادات الموثوقة. في حالة عدم توفير واحد، فقد يعني ذلك أن المهاجم يقوم بفك تشفير اتصالاتك أو أن موقع الويب يواجه صعوبات تقنية.

وفي حالة تحديد الخيار **السؤال عن صلاحية الشهادة** (محدد افتراضياً)، ستتم مطالبتك باختيار إجراء عند إنشاء اتصال مشفر. سيظهر مربع تحديد إجراءات حيث يمكنك اتخاذ قرار بشأن تمييز الشهادة كموثوقة أو مستبعدة. وإذا لم تكن الشهادة موجودة في قائمة TRCA فستكون القائمة حمراء. أما إذا كانت الشهادة موجودة في قائمة TRCA فستكون القائمة خضراء.

يمكنك تحديد الخيار **حظر الاتصالات التي تستخدم الشهادة** لإنهاء الاتصالات المشفرة بالموقع الذي يستخدم الشهادة غير المصدقة دائماً.

حظر حركة المرور المشفرة بواسطة SSL2 القديم—سيتم حظر الاتصال باستخدام الإصدار السابق من SSL البروتوكول تلقائياً.

الإجراء الخاص بالشهادات التالفة—تعني الشهادة التالفة أن الشهادة تستخدم تنسيقاً لم يتم التعرف عليه من قبل ESET Internet Security أو تم استلامه تالفاً (على سبيل المثال، تمت الكتابة فوقه بواسطة بيانات عشوائية). في هذه الحالة، نوصي بترك **حظر الاتصالات التي تستخدم الشهادة** محدداً. إذا تم تحديد **السؤال عن صلاحية الشهادة** ، تتم مطالبة المستخدم بتحديد إجراء يجب اتخاذه عند إنشاء الاتصال المُشفر.

أمثلة مصورة

قد لا تتوفر مقالات قاعدة معارف ESET التالية إلا باللغة الإنجليزية:

- إعلامات الشهادة في منتجات الصفحة الرئيسية ESET Windows
- يتم عرض "حركة مرور الشبكة المشفرة: يتم عرض شهادة غير موثوق بها" عند زيارة صفحات الويب

قواعد فحص التطبيق

يمكن استخدام **قواعد فحص التطبيق** في تخصيص سلوك ESET Internet Security تجاه تطبيقات معينة وتذكر الإجراءات المتخذة عندما يكون **وضع SSL/TLS** في **الوضع التفاعلي**. يمكن عرض القائمة وتحريرها في الإعداد المتقدم > **وسائل الحماية** > **SSL/TLS** > **قواعد فحص التطبيق** > **تحرير**.

تتكون نافذة **قواعد فحص التطبيق** من:

الأعمدة

التطبيق – اختر ملفاً قابلاً للتنفيذ من شجرة الدليل، وانقر فوق خيار **...** أو أدخل المسار يدوياً.

إجراء الفحص – حدد **فحص** أو **تجاهل** لفحص الاتصال أو تجاهله. حدد **تلقائي** للفحص في الوضع التلقائي أو السؤال في الوضع التفاعلي. وحدد **سؤال** لسؤال المستخدم دائماً عما يجب فعله.

عناصر التحكم

إضافة – لإضافة تطبيق تمت تصفيته.

تحرير – حدد التطبيق الذي تريد تكوينه وانقر فوق **تحرير**.

حذف – حدد التطبيق الذي تريد حذفه وانقر فوق **حذف**.

استيراد/تصدير – استيراد التطبيقات من ملف أو حفظ قائمة التطبيقات الحالية إلى ملف.

موافق/إلغاء – انقر فوق **موافق** إذا كنت ترغب في حفظ التغييرات، أو انقر فوق **إلغاء** إذا كنت ترغب في الخروج دون حفظ.

قواعد الشهادة

يمكن استخدام**قواعد الشهادة** لتخصيص ESET Internet Security السلوك لشهادات SSL محددة ولتذكر الإجراءات المختارة عندما يكون **وضع SSL/TLS** في **الوضع التفاعلي**. يمكن عرض القائمة وتحريرها في الإعداد المتقدم > **وسائل الحماية** > **SSL/TLS** > **قواعد الشهادة** > **تحرير**.

تتكون نافذة **قواعد الشهادة** من:

الأعمدة

الاسم ـ اسم الشهادة.

مُصدر الشهادة ـ اسم مُنشئ الشهادة.

موضوع الشهادة ـ يحدد حقل الموضوع الهوية المقترنة بالمفتاح العام المخزن في حقل المفتاح العام للموضوع.

الوصولـ حدد **سماح** أو **حظر** في **إجراء الوصول** للسماح/حظر الاتصالات المؤمنة بواسطة هذه الشهادة بصرف النظر عن موثوقيتها. وحدد **تلقائي** للسماح بالشهادات الموثوق بها والسؤال للشهادات غير الموثوق بها. وحدد **سؤال** لسؤال المستخدم دائماً عما يجب فعله.

الفحص ـ حدد **فحص** أو **تجاهل** في **إجراء الفحص** لفحص أو تجاهل الاتصالات المؤمنة بواسطة هذه الشهادة. حدد **تلقائي** للفحص في الوضع التلقائي أو السؤال في الوضع التفاعلي. وحدد **سؤال** لسؤال المستخدم دائماً عما يجب فعله.

عناصر التحكم

إضافة – أضف شهادة جديدة واضبط الإعدادات الخاصة بها حسب خيارات الوصول والمسح.

تحرير ـ حدد الشهادة التي تريد تكوينها وانقر فوق**تحرير**.

حذف – حدد الشهادة التي تريد حذفها وانقر فوق **إزالة**.

موافق/إلغاء ـ انقر فوق **موافق** إذا كنت ترغب في حفظ التغييرات، أو انقر فوق **إلغاء** إذا كنت ترغب في الخروج دون حفظ.

حركة مرور شبكة مشفرة

في حالة تمكين نظامك لاستخدام فحص SSL/TLS سيتم عرض نافذة حوار تطالبك باختيار الإجراء في الحالتين التاليتين:

الأولى، في حالة استخدام موقع ويب لشهادة غير صالحة أو لا يمكن التحقق منها، وتكوين ESET Internet Security لمطالبة المستخدم في هذه الحالات (افتراضياً نعم للشهادات التي لا يمكن التحقق منها، ولا للشهادات غير الصالحة)، سيسألك مربع حوار ما إذا كنت تريد تحديد الخيار **سماح** أو **حظر** للاتصال. إذا كانت الشهادة غير موجودة في Trusted Root Certification Authorities store (TRCA) فسيتم اعتبارها غير موثوقة.

الثانية، في حالة تعيين **SSL/TLS**وضع على **الوضع التفاعلي**، سيتم سؤالك في مربع حوار لكل موقع ويب عما إذا كنت تريد تحديد الخيار **فحص** أم **تجاهل** لحركة نقل البيانات. تتحقق بعض التطبيقات من عدم تعديل حركة نقل البيانات عبر SSL لها وعدم مراقبتها بواسطة أي شخص، وفي هذه الحالات، يجب أن يتم **تجاهل** حركة نقل البيانات تلك بواسطة ESET Internet Security لاستمرار عمل التطبيق.

أمثلة مصورة

قد لا تتوفر مقالات قاعدة معارف ESET التالية إلا باللغة الإنجليزية:

- إعلامات الشهادة في منتجات الصفحة الرئيسية ESET Windows
- يتم عرض "حركة مرور الشبكة المشفرة: يتم عرض شهادة غير موثوق بها" عند زيارة صفحات الويب

وفي الحالتين كلتيهما، يمكن للمستخدم اختيار تذكر الإجراء المحدد. يتم تخزين الإجراءات المحفوظة في قواعد الشهادة.

حماية عميل البريد الإلكتروني

لتكوين حماية عميل البريد الإلكتروني، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية عميل البريد الإلكتروني** واختر من خيارات التكوين التالية:

- حماية نقل البريد
- حماية صندوق البريد
- إدارة قوائم العناوين
- ThreatSense

حماية نقل البريد

بروتوكولا IMAP(S) وPOP3(S) هما أكثر بروتوكولين انتشاراً من البروتوكولات المستخدمة لتلقي اتصالات البريد الإلكتروني في تطبيق عميل بريد إلكتروني. يعتبر بروتوكول الوصول إلى الرسائل عبر الإنترنت (IMAP) بروتوكول آخر لاسترداد البريد الإلكتروني عبر الإنترنت. يتمتع بروتوكول IMAP بميزات تميزه على بروتوكول POP3 فعلى سبيل المثال، يمكن لعدة تطبيقات عميلة الاتصال بنفس علبة البريد وتحديث معلومات حالة رسالةٍ ما، مثل ما إذا كان قد تمت قراءة هذه الرسالة أم لا، أو ما إذا كان قد تم الرد عليها أو حذفها. يتم بدء تشغيل وحدة الحماية التي توفر عنصر التحكم هذا تلقائياً عند بدء تشغيل النظام ثم تنشط في الذاكرة.

ESET Internet Security يوفر الحماية لهذه البروتوكولات بغض النظر عن عميل البريد الإلكتروني المستخدَم، ودون الحاجة إلى إعادة تكوين عميل البريد الإلكتروني. افتراضياً، يتم فحص جميع الاتصالات عبر بروتوكولي POP3 وIMAP بغض النظر عن أرقام منفذ IMAP / POP3 الافتراضية.

لم يتم فحص بروتوكول MAPI. لكن يمكن فحص التواصل مع خادم Microsoft Exchange من خلال الوحدة النمطية للتكامل في عملاء البريد الإلكتروني مثل Microsoft Outlook.

> يدعم ESET Internet Security أيضاً البحث عن بروتوكولات IMAPS (585, 993 و995) POP3S) التي تستخدم قناة مشفرة لنقل معلومات بين الخادم والعميل. يفحص ESET Internet Security الاتصال باستخدام بروتوكولي طبقة مأخذ التوصيل الآمنة (SSL) وأمان طبقة النقل (TLS).
> سيتم فحص الاتصال المشفر افتراضياً. لعرض إعداد أداة الفحص، افتح الإعداد المتقدم > **وسائل الحماية** > SSL/TLS.

لتكوين حماية نقل البريد، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية عميل البريد الإلكتروني** > **حماية نقل البريد**.

تمكين حماية نقل البريد—عند التمكين، سيتم فحص اتصالات نقل البريد بواسطة ESET Internet Security.

يمكنك اختيار بروتوكولات نقل البريد التي سيتم فحصها بالنقر فوق مفتاح التبديل بجوار الخيارات التالية (افتراضياً، يتم تمكين فحص جميع البروتوكولات):

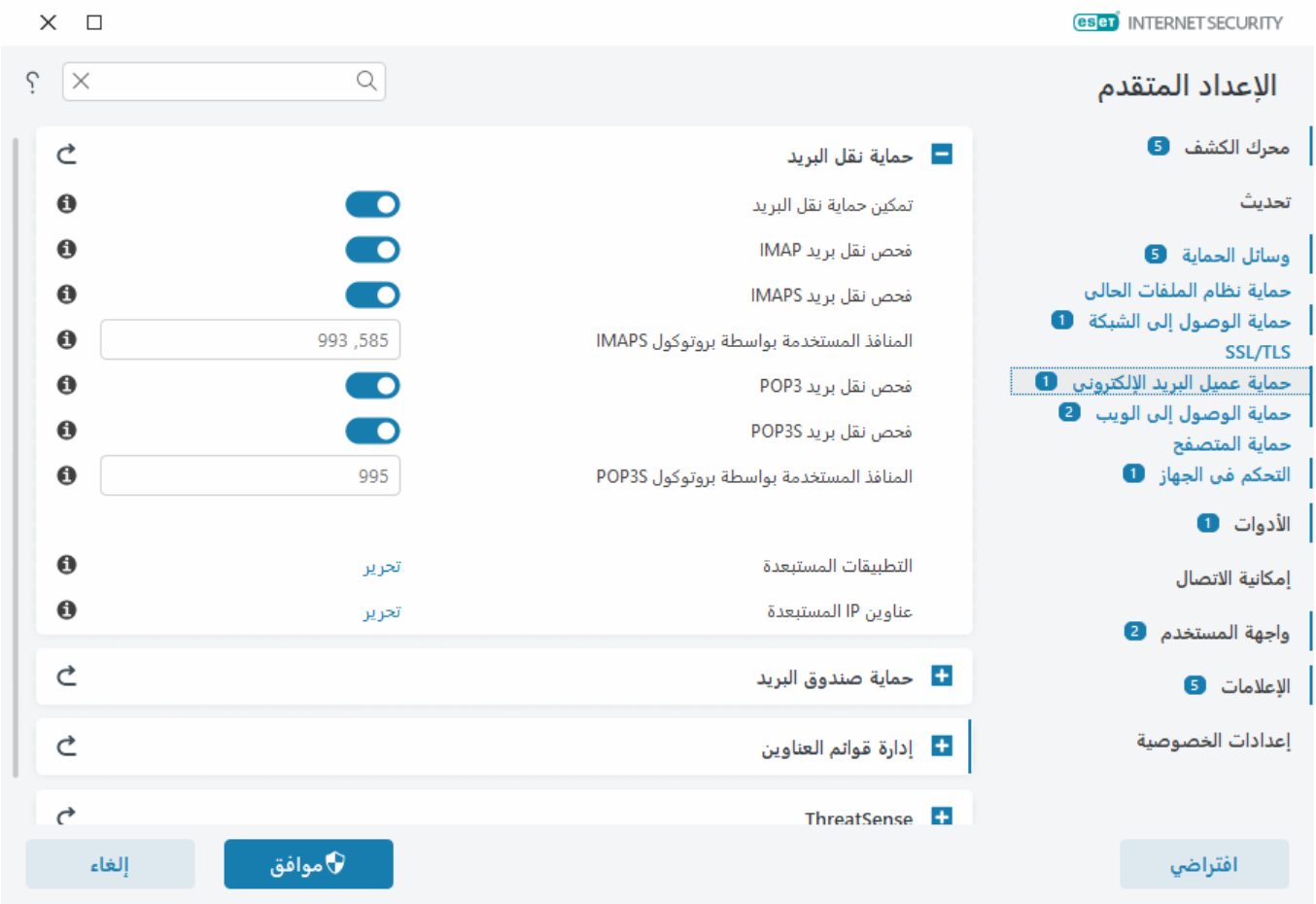
- **فحص نقل بريد IMAP**
- **فحص نقل بريد IMAPS**
- **فحص نقل بريد POP3**

- **فحص نقل بريد POP3S**

افتراضياً، سيقوم ESET Internet Security بفحص اتصال IMAPS وPOP3S على المنافذ القياسية. لإضافة منافذ مخصصة لبروتوكولات IMAPS وPOP3S قم بإضافتها إلى حقل النص بجوار **المنافذ المستخدمة بواسطة بروتوكول IMAPS** أو **المنافذ المستخدمة بواسطة بروتوكول POP3S**. يجب الفصل بين أرقام المنافذ المتعددة بفاصلة.

تمكنك التطبيقات المستبعدة—من استبعاد تطبيقات معينة من الفحص بواسطة حماية نقل البريد. يكون مفيداً عندما تتسبب حماية الوصول إلى الويب في حدوث مشكلات في التوافق.

تمكنك عناوين IP المستبعدة—من استبعاد عناوين بعيدة محددة من الفحص بواسطة حماية نقل البريد. يكون مفيداً عندما تتسبب حماية الوصول إلى الويب في حدوث مشكلات في التوافق.



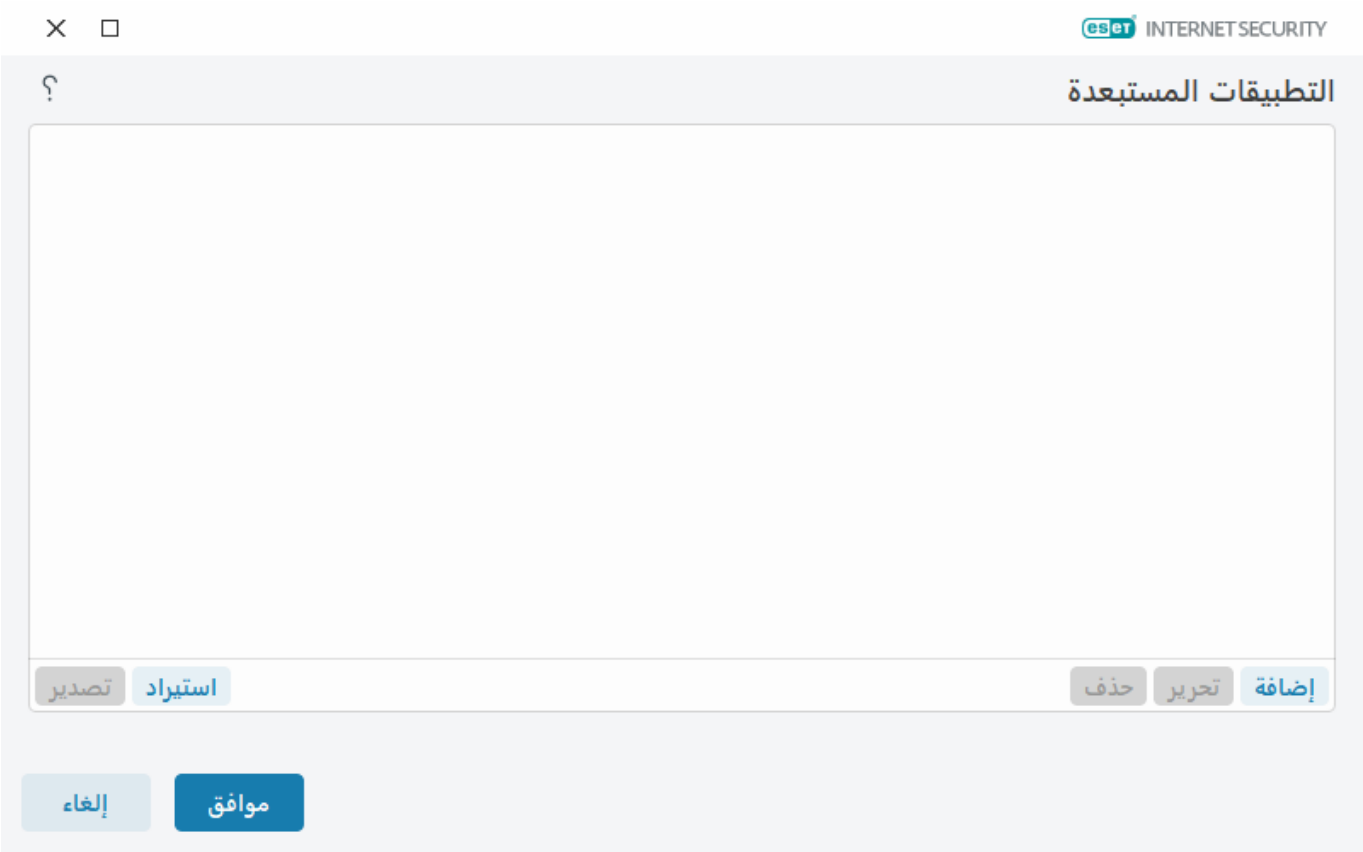
التطبيقات المستبعدة

لاستبعاد فحص الاتصالات لتطبيقات محددة، قم بإضافتها إلى القائمة. لن يتم فحص اتصال (HTTP(S)/POP3(S)/IMAP(S للتطبيقات المحددة بحثاً عن تهديدات. نوصي فقط باستخدام هذا للتطبيقات التي لا تعمل بشكل صحيح مع اتصالاتها الخاضعة للفحص.

ستكون التطبيقات والخدمات الجارية متوفرة هنا تلقائياً عند النقر فوق **إضافة**. انقر فوق **...** وانتقل إلى تطبيق لإضافة الاستبعاد يدوياً.

تحرير – تحرير الإدخالات المحددة من القائمة.

إزالة – إزالة الإدخالات المحددة من القائمة.



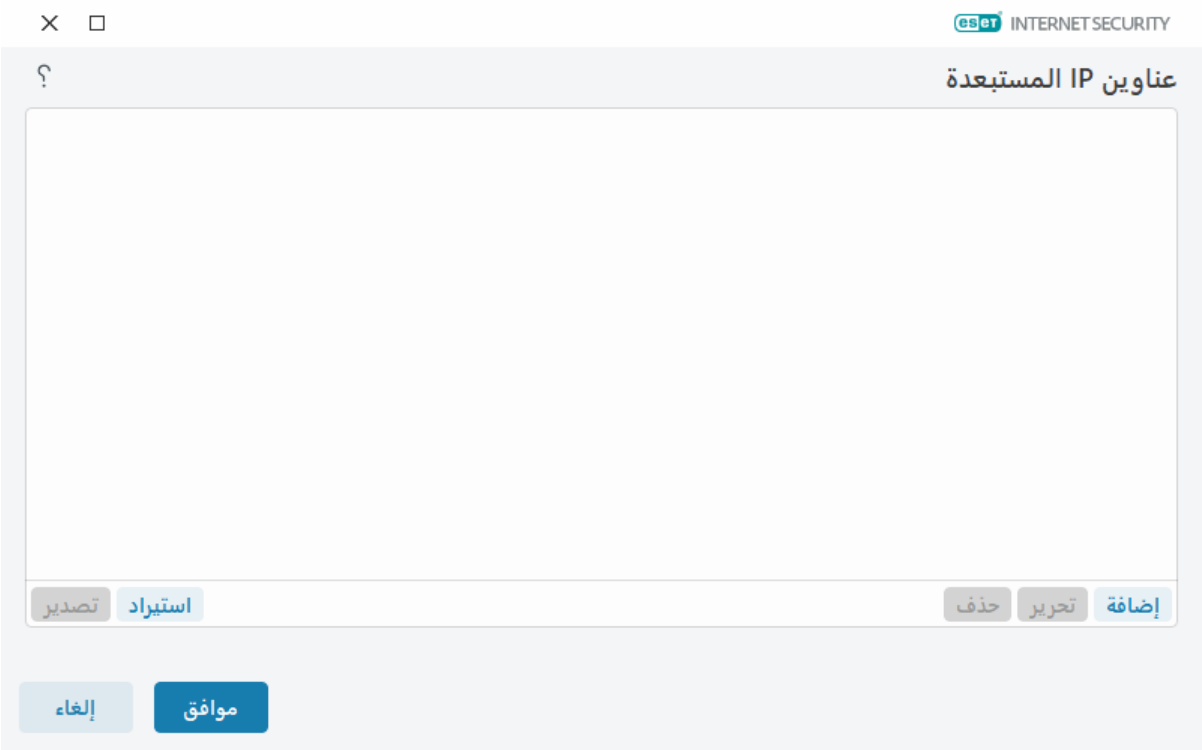
عناوين IP المستبعدة

سيتم استبعاد الإدخالات الموجودة في القائمة من الفحص. لن يتم فحص اتصال (HTTP(S)/POP3(S)/IMAP(S من/إلى العناوين المحددة بحثاً عن تهديدات. يوصى بعدم استخدام هذا الخيار مع العناوين المعروفة بكونها موثوقة.

انقر فوق **إضافة** لاستبعاد عنوان IP/نطاق العنوان/شبكة فرعية لنقطة بعيدة.

انقر فوق **تحرير** لتغيير عنوان IP المحدد.

انقر فوق **حذف** لإزالة الإدخالات المحددة من القائمة.



أمثلة لعناوين IP

إضافة عنوان IPv4:

العنوان الفردي— يضيف عنوان IP لجهاز كمبيوتر فردي (على سبيل المثال، *192.168.0.10*).

نطاق العناوين — أدخل عنوان البدء وعنوان الانتهاء لعنوان IP لتحديد نطاق IP لأجهزة كمبيوتر عديدة (على سبيل المثال 192.168.0.1 إلى 192.168.0.99).

الشبكة الفرعية – يتم تحديد الشبكة الفرعية (مجموعة من أجهزة الكمبيوتر) عن طريق قناع وعنوان IP. على سبيل المثال، 255.255.255.0 هو قناع الشبكة للشبكة الفرعية 192.168.1.0. لاستبعاد نوع الشبكة الفرعية بالكامل في *192.168.1.0/24*.

إضافة عناوين IPv6:

العنوان الفردي— يضيف عنوان IP الخاص بكمبيوتر فردي (على سبيل المثال، *2001:718:1c01:16:214:22ff:fec9:ca5*).

الشبكة الفرعية – يتم تحديد الشبكة الفرعية (مجموعة من أجهزة الكمبيوتر) عن طريق قناع وعنوان IP (على سبيل المثال: *c0a8:6301:1::1/64:2002*).

حماية صندوق البريد

يؤدي تكامل ESET Internet Security مع صندوق البريد لديك إلى زيادة مستوى الحماية النشطة ضد التعليمات البرمجية الضارة في رسائل البريد الإلكتروني.

لتكوين حماية صندوق البريد، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية عميل البريد الإلكتروني** > **حماية صندوق البريد**.

تمكين حماية البريد الإلكتروني بواسطة المكونات الإضافية للعميل – عند تعطيله، يتم إيقاف تشغيل الحماية بواسطة المكونات الإضافية لعميل البريد الإلكتروني.

حدد رسائل البريد الإلكتروني للفحص:

- **البريد الإلكتروني المستلم**
- **البريد الإلكتروني المرسل**

- **البريد الإلكتروني المقروء**
- **البريد الإلكتروني المعدّل**

> نوصي بالاحتفاظ بـ **تمكين البريد الإلكتروني للحماية من خلال المكونات الإضافية للعميل** ممكّناً. حتى إذا لم يتم تمكين التكامل أو تشغيله، فلا يزال الاتصال عبر البريد الإلكتروني محمياً بواسطة حماية نقل البريد (IMAP/IMAPS و POP3/POP3S).

الفحص بحثاً عن البريد العشوائي

يُصنف البريد الإلكتروني غير المرغوب فيه، والمسمى بالبريد العشوائي، ضمن أكبر المشكلات التي تهدد الاتصال الإلكتروني. يمثل البريد العشوائي ما يصل إلى 30 بالمئة من جميع اتصالات البريد الإلكتروني. يعمل برنامج مكافحة البريد العشوائي لعميل البريد الإلكتروني على الحماية من هذه المشكلة. من خلال الجمع بين العديد من مبادئ أمان البريد الإلكتروني، يوفر برنامج مكافحة البريد العشوائي لعميل البريد الإلكتروني تصفية فائقة للحفاظ على نظافة صندوق الوارد لديك. بالنسبة لاكتشاف البريد العشوائي، يتمثل أحد أهم المبادئ في التعرف على رسائل البريد الإلكتروني غير المرغوب فيها استناداً إلى عناوين موثوقة محددة مسبقاً (المسموح بها) وعناوين البريد العشوائي (المحظورة).

تتمثل الطريقة الرئيسية المستخدمة لاكتشاف البريد العشوائي في فحص خصائص رسالة البريد الإلكتروني. يتم فحص الرسائل المستلمة للتحقق من معايير أساسية للحماية من البريد العشوائي (تعريفات رسائل، وأساليب بحثية إحصائية، وخوارزميات للتعرف وغيرها من الأساليب الفريدة)، وتحدد قيمة الفهرسة الناتجة مدى كون الرسالة بريداً عشوائياً من عدمه.

تمكين برنامج مكافحة البريد العشوائي لعميل البريد الإلكتروني—عند التمكين، سيتم فحص الرسائل المستلمة بحثاً عن البريد العشوائي.

استخدام أداة فحص البريد العشوائي المتقدمة—سيتم تنزيل بيانات إضافية لمكافحة البريد العشوائي بشكل دوري، مما يزيد من قدرات مكافحة البريد العشوائي مما يؤدي إلى نتائج أفضل.

تسجيل درجات البريد العشوائي ـ يعين محرك الحماية ضد البريد العشوائي في ESET Internet Security درجات تصنيف حسب البريد العشوائي لكل رسالة تم فحصها. سيتم تسجيل الرسالة في سجل الحماية ضد البريد المزعج (نافذة البرنامج الرئيسية > **الأدوات** > **ملفات السجل** > **برنامج مكافحة البريد العشوائي لعميل البريد الإلكتروني**).

- **لا شيء** ـ لن يتم تسجيل الدرجة المسجلة من فحص الحماية ضد البريد العشوائي.
- **أُعيد التصنيف ووُضعت علامة بريد عشوائي عليه** ـ حدد هذا الخيار إذا كنت تريد تسجيل درجة بريد عشوائي للرسائل الموضوع عليها علامة بأنها SPAM.
- **الكل** ـ سيتم تسجيل جميع الرسائل في السجل بدرجة بريد عشوائي.

> عند النقر فوق رسالة موجودة بمجلد البريد الإلكتروني غير الهام، يمكنك اختيار **إعادة تصنيف رسائل محددة باعتبارها ليست بريداً عشوائياً** وسيتم نقل الرسالة إلى صندوق الوارد. عند النقر فوق رسالة تظن أنها بريداً عشوائياً في صندوق الوارد، حدد **إعادة تصنيف الرسائل باعتبارها بريداً عشوائياً** وسيتم نقل الرسالة إلى مجلد البريد الإلكتروني غير الهام. يمكنك تحديد عدة رسائل وتنفيذ الإجراء عليها جميعاً في وقت واحد.

تحسين التعامل مع المرفقـ إذا تم تعطيل التحسين، فسيتم فحص جميع المرفقات على الفور. قد تواجه بطء في أداء عميل البريد

الإلكتروني.

تمكنك **عمليات التكامل**—من دمج حماية صندوق البريد في عميل البريد الإلكتروني. راجع عمليات التكامل للحصول على مزيد من المعلومات.

تمكنك**الاستجابة**—من تخصيص معالجة رسائل البريد العشوائي. راجع الاستجابة للحصول على مزيد من المعلومات.

عمليات التكامل

يزيد تكامل ESET Internet Security مع التطبيقات العميلة للبريد الإلكتروني من مستوى الحماية النشطة للتعليمات البرمجية الضارة في رسائل البريد الإلكتروني. إذا كان عميل البريد الإلكتروني الخاص بك مدعوماً، فيمكنك تمكين التكامل فيه ESET Internet Security. عندما التكامل في عميل البريد الإلكتروني، يتم إدخال شريط أدوات ESET Internet Security مباشرة في عميل البريد الإلكتروني، مما يسمح بحماية أكثر كفاءة للبريد الإلكتروني. لتحرير إعدادات التكامل، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية عميل البريد الإلكتروني** > **صندوق البريد** > **التكامل**.

تكامل مع Microsoft Outlook – **Microsoft Outlook** هو عميل البريد الإلكتروني الوحيد المدعوم حالياً. تعمل حماية البريد الإلكتروني كمكون إضافي. وتعد الميزة الرئيسية للمكون الإضافي استقلالها عن البروتوكول المستخدم. عندما يتلقى عميل البريد الإلكتروني رسالة مشفرة، يتم فك تشفيرها وإرسالها إلى برنامج فحص الفيروسات. راجع مقالة قاعدة معارف ESET هذه للحصول على قائمة كاملة بإصدارات Microsoft Outlook المدعومة.

معالجة عميل البريد الإلكتروني المتقدمة—تعالج Outlook Messaging API (MAPI)الأحداثالإضافية: تم تعديل الكائن (`fnevObjectModified`) وإنشاء الكائن (`fnevObjectCreated`). إذا كنت تواجه بطأً بالنظام عند العمل على عميل البريد الإلكتروني لديك، فقم بتعطيل هذا الخيار.

شريط أدوات Microsoft Outlook

تعمل حماية Microsoft Outlook كوحدة مكون إضافي. بعد تثبيت ESET Internet Security تتم إضافة شريط الأدوات هذا الذي يحتوي على الحماية ضد الفيروسات وخيارات مكافحة البريد العشوائي لعميل البريد الإلكتروني إلى Microsoft Outlook:

بريد عشوائي – لوضع علامة على رسائل مختارة كبريد عشوائي. وبعد وضع تلك العلامة، يتم إرسال "بصمة" الرسالة إلى خادم مركزي يخزِّن توقيعات البريد العشوائي. في حالة تلقي الخادم لمزيد من "البصمات" المتشابهة من عدة مستخدمين، سيتم تصنيف الرسالة كبريد عشوائي في المستقبل.

ليست بريداً عشوائياً – لوضع علامة على رسائل مختارة باعتبارها ليست بريداً عشوائياً.

عنوان البريد العشوائي (محظور، قائمة بعناوين البريد العشوائي) – يضيف عنوان مرسل جديد إلى قائمة العناوين على أنه محظور. سيتم تصنيف جميع الرسائل المستلَمة من القائمة كبريد عشوائي تلقائياً.

احذر الانتحال – وهو تزوير عنوان مرسل على رسائل بريد إلكتروني لتضليل مستلمي البريد الإلكتروني بقراءتها والرد عليها.

عنوان موثوق به (مسموح به، قائمة بالعناوين الموثوق بها) ـ يضيف عنوان مرسل جديد إلى قائمة العناوين على أنه مسموح به. لن يتم تصنيف جميع الرسائل المستلمة من العناوين المسموح بها تلقائياً كرسائل لبريد عشوائي.

ESET Internet Security – انقر نقراً مزدوجاً فوق الأيقونة لفتح النافذة الرئيسية لـESET Internet Security.

إعادة فحص الرسائل ـ يتيح لك تشغيل فحص بريد إلكتروني يدوياً. يمكنك تحديد الرسائل التي سيتم فحصها، كما يمكنك تنشيط إعادة فحص البريد الإلكتروني المستلَم. لمزيد من المعلومات، راجع حماية صندوق البريد.

إعداد أداة الفحص—يعرض خيارات إعداد حماية صندوق البريد.

إعداد مكافحة البريد العشوائي— يعرض خيارات إعداد حماية صندوق البريد.

تفتح **دفاتر العناوين**—نافذة إدارة قوائم العناوين، التي يمكنك من خلالها الوصول إلى قوائم العناوين المستبعدة والموثوق بها وعناوين البريد العشوائي.

مربع حوار التأكيد

يخدم هذا الإعلام التحقق من أن المستخدم يريد فعلاً تنفيذ الإجراء المحدد، وذلك بهدف تجنب الأخطاء المحتملة.

كما يعرض مربع الحوار من ناحية أخرى خيار تعطيل تأكيدات.

إعادة فحص الرسائل

يتيح شريط أدوات ESET Internet Security المدمج في البرامج العميلة للبريد الإلكتروني للمستخدمين تحديد عدة خيارات للتحقق من البريد الإلكتروني. يوفر الخيار **إعادة فحص الرسائل** وضعي فحص هما:

جميع الرسائل في المجلد الحالي ـ لفحص الرسائل الموجودة في المجلد المعروض حالياً.

الرسائل المحددة فقط ـ لفحص الرسائل المميزة بواسطة المستخدم فقط.

توفر خانة اختيار **إعادة فحص رسائل تم فحصها بالفعل** للمستخدم خيار تشغيل عملية فحص أخرى على الرسائل التي سبق أن تم فحصها.

الاستجابة

استناداً إلى نتائج فحص الرسائل، يمكن لـESET Internet Security نقل الرسائل التي تم فحصها أو إضافة نص مخصص للموضوع. يمكنك تكوين هذه الإعدادات في الإعداد المتقدم: > **وسائل الحماية** > **حماية عميل البريد الإلكتروني** > **حماية صندوق البريد** > **الاستجابة**.

يتيح لك برنامج مكافحة البريد العشوائي لعميل البريد الإلكتروني في ESET Internet Security تكوين المعلمات التالية للرسائل:

إضافة نص إلى عنوان البريد الإلكتروني ـ يتيح لك إضافة سلسلة بادئة مخصصة إلى سطر الموضوع بالرسائل المصنفة كبريد عشوائي. **النص** الافتراضي هو "[SPAM]".

الانتقال إلى مجلد البريد العشوائي— عند التمكين، سيتم نقل رسائل البريد العشوائي إلى المجلد الافتراضي للبريد الإلكتروني غير الهام، كما أن الرسائل التي تمت إعادة تصنيفها على أنها ليست بريداً عشوائياً سيتم نقلها إلى صندوق الوارد. عند النقر بزر الماوس الأيمن فوق رسالة بريد إلكتروني وتحديد ESET Internet Security من القائمة السياقية، يمكنك الاختيار من بين الخيارات الملائمة.

الانتقال إلى مجلد مخصص— عند التمكين، سيتم نقل رسائل البريد العشوائي إلى مجلد محدد أدناه.

المجلد ـ حدد المجلد المخصص الذي ترغب في نقل رسائل البريد الإلكتروني المصابة إليه عند اكتشافها.

في حالة وجود رسالة تحتوي على الاكتشاف، افتراضياً، يقوم ESET Internet Security بمحاولة تنظيف الرسالة. إذا تعذر تنظيف الرسالة، يمكنك اختيار **إجراء لاتخاذه إذا لم يكن التنظيف ممكناً**:

- **بدون إجراء** ـ في حالة تمكينه، سيحدد البرنامج المرفقات المصابة، لكنه سيترك رسائل البريد الإلكتروني دون اتخاذ أي إجراء.
- **حذف البريد الإلكتروني** ـ سيُعلم البرنامج المستخدم حول حالات التسلل ويحذف الرسالة.
- **نقل البريد الإلكتروني إلى مجلد العناصر المحذوفة** ـ سيتم نقل رسائل البريد الإلكتروني المصابة تلقائياً إلى مجلد "العناصر المحذوفة".
- **نقل البريد الإلكتروني إلى مجلد** (إجراء افتراضي) – سيتم نقل رسائل البريد الإلكتروني المصابة تلقائياً إلى المجلد المحدد.

المجلد ـ حدد المجلد المخصص الذي ترغب في نقل رسائل البريد الإلكتروني المصابة إليه عند اكتشافها.

وضع علامة مقروء على الرسائل العشوائية ـ قم بتمكين هذا الخيار لوضع علامة مقروء على البريد العشوائي تلقائياً. وهو سيساعدك على تركيز اهتمامك على الرسائل "النظيفة" فقط.

وضع علامة غير مقروء على الرسائل المعاد تصنيفها ـ يتم تصنيف الرسائل في بادئ الأمر كبريد عشوائي، ولكن بعد تعليمها على أنها "نظيفة" ستظهر كغير مقروءة.

بعد فحص أي رسالة بريد إلكتروني، يمكن إلحاق إعلام بنتيجة الفحص بالرسالة. ويمكنك اختيار إما **إلحاق رسائل العلامة إلى تلقي البريد الإلكتروني وقراءته** أو **إلحاق رسائل العلامة إلى البريد الإلكتروني المرسل**. ويرجى العلم بأن رسائل تأكيد الفحص قد تُحذف في بعض الحالات النادرة في رسائل HTML التي بها مشكلات أو إذا تم تزوير الرسائل بواسطة برامج ضارة. ويمكن إضافة رسائل تأكيد الفحص إلى البريد الإلكتروني المستلم والمقروء أو البريد الإلكتروني المرسل أو كليهما. تتوفر الخيارات التالية:

- **أبداً** – لن تتم إضافة رسائل تأكيد الفحص.
- **عند حدوث اكتشاف** – لن يتم وضع علامة تم الفحص إلا على الرسائل التي تحتوي على برامج ضارة (الإعداد الافتراضي).
- **لكل رسائل البريد الإلكتروني عند فحصها** ـ سيقوم البرنامج بإلحاق رسائل إلى كل رسائل البريد الإلكتروني التي يتم فحصها.

تحديث موضوع البريد الإلكتروني المستلم والمقروء / تحديث موضوع البريد الإلكتروني المرسل— قم بتمكين هذا الخيار لإضافة نص مخصص محدد أدناه إلى الرسالة.

رسالة نصية لتتم إضافتها إلى موضوع البريد الإلكتروني الذي تم اكتشافه – قم بتحرير هذا القالب إذا كنت ترغب في تعديل تنسيق بادئة الموضوع في رسالة بريد إلكتروني مصابة. ستحل هذه الوظيفة محل موضوع الرسالة "Hello" بالتنسيق التالي: "Hello] %DETECTIONNAME% detection". يمثل المتغير %DETECTIONNAME% الاكتشاف.

إدارة قوائم العناوين

تسمح لك ميزة مكافحة البريد العشوائي لعميل البريد الإلكتروني في ESET Internet Security بتكوين معلمات مختلفة لقوائم العناوين. لتكوين قوائم العناوين، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية عميل البريد الإلكتروني** > **إدارة قوائم العناوين**.

تمكين قائمة عناوين المستخدم – قم بتمكين هذا الخيار لتنشيط قائمة عناوين المستخدم.

قائمة عناوين المستخدم - قائمة بعناوين البريد الإلكتروني حيث يمكنك إضافة العناوين أو تحريرها أو حذفها لتحديد قواعد مكافحة البريد العشوائي. سيتم تطبيق القواعد في هذه القائمة على المستخدم الحالي.

تمكين قائمة العناوين العامة – قم بتمكين هذا الخيار لتنشيط قائمة العناوين العامة التي تمت مشاركتها بواسطة جميع المستخدمين على هذا الجهاز.

قائمة العناوين العامة - قائمة بعناوين البريد الإلكتروني حيث يمكنك إضافة العناوين أو تحريرها أو حذفها لتحديد قواعد مكافحة البريد العشوائي. سيتم تطبيق القواعد في هذه القائمة على جميع المستخدمين.

السماح تلقائياً والإضافة إلى قائمة عناوين المستخدم

التعامل مع العناوين من دفتر العناوين كموثوقة – سيتم التعامل مع العناوين الموجودة في قائمة جهات الاتصال لديك كموثوقة بدون إضافتها إلى قائمة عناوين المستخدم.

إضافة عناوين المستلمين من الرسائل الصادرة – قم بإضافة عناوين مستلمين من الرسائل المرسلة إلى قائمة عناوين المستخدم كـ مسموح به.

إضافة العناوين من الرسائل المعاد تصنيفها كرسائل لا تنتمي إلى الرسائل العشوائية – إضافة عناوين مرسلين من الرسائل المعاد تصنيفها كرسائل لا تنتمي إلى رسائل عشوائية كـ مسموح به.

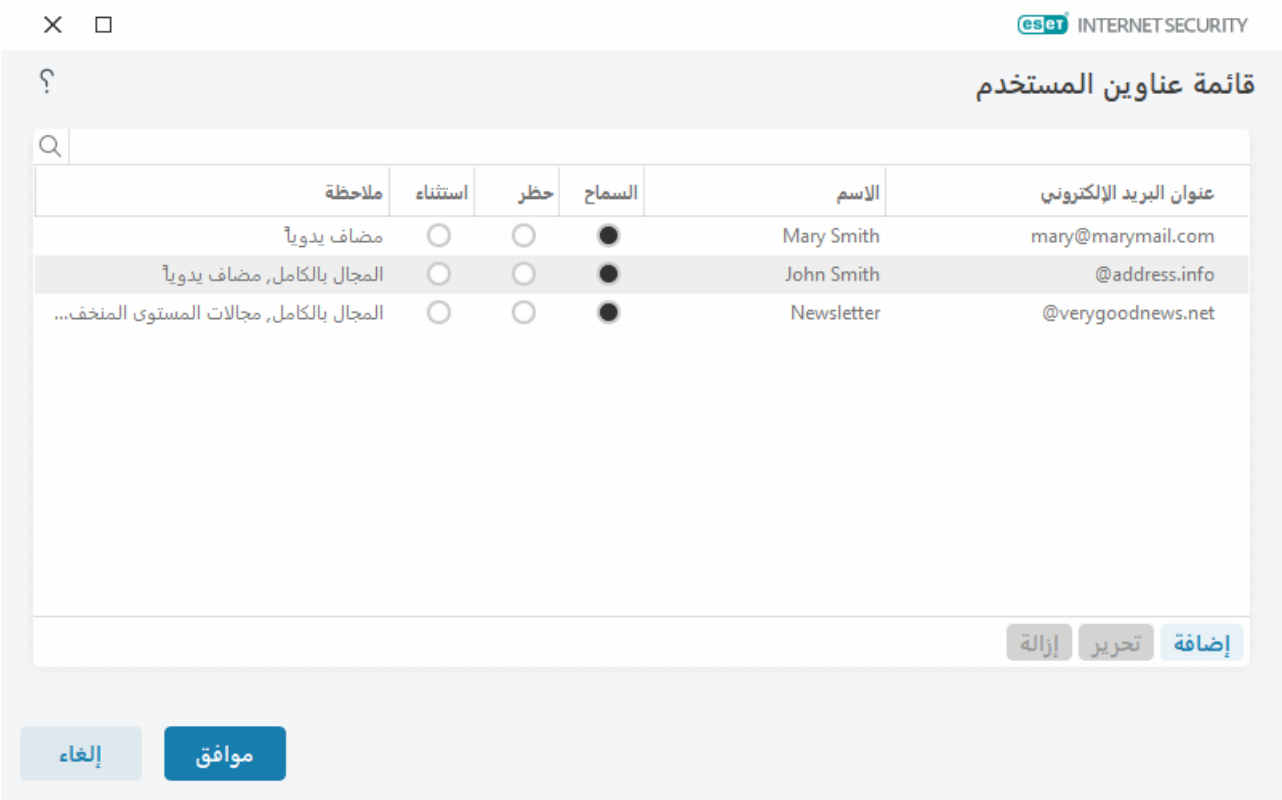
إضافة كاستثناء تلقائياً إلى قائمة عناوين المستخدم

إضافة العناوين من الحسابات الخاصة – قم بإضافة عناوين خاصة بك من حسابات موجودة ببرامج عميلة للبريد الإلكتروني إلى قائمة عناوين المستخدم كـاستثناء.

قوائم العناوين

للحماية من رسائل البريد الإلكتروني غير المرغوب فيها، يتيح لك ESET Internet Security تصنيف عناوين البريد الإلكتروني في قوائم العناوين.

لتحرير قوائم العناوين، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية عميل البريد الإلكتروني** > **إدارة قوائم العناوين**، وانقر فوق **تحرير** بجوار **قائمة عناوين المستخدم** أو **قائمة العناوين العامة**.



الأعمدة

عنوان البريد الإلكتروني – العنوان الذي ستنطبق عليه القاعدة. لا يتم دعم أحرف البدل.

الاسم – اسم القاعدة المخصص.

السماح/الحظر/الاستثناء – أزرار الخيارات المستخدمة لتحديد الإجراء الذي يجب اتخاذه لعنوان البريد الإلكتروني (انقر فوق زر الخيار في العمود المفضل لتغيير الإجراء بسرعة):

- **السماح** – العناوين التي تعد آمنة والتي تريد استلام الرسائل منها.
- **الحظر** – العناوين التي تعد غير آمنة / عشوائية والتي لا تريد استلام الرسائل منها.
- **الاستثناء** – العناوين التي يتم فحصها دائماً بحثاً عن بريد عشوائي والتي قد تكون منتحلة وتُستخدم لإرسال بريد عشوائي.

ملاحظة – معلومات حول كيفية إنشاء القاعدة وما إذا كانت تنطبق على المجال بالكامل / نطاقات المستوى الأدنى.

إدارة العناوين

- **إضافة** – انقر لإضافة قاعدة لعنوان جديد.
- **تحرير** – حدد وانقر لتحرير قاعدة موجودة.
- **إزالة** – حدد وانقر إذا كنت تريد حذف قاعدة من قائمة العناوين.

إضافة/تحرير عنوان

تتيح لك هذه النافذة إضافة عنوان أو تحريره في إدارة قوائم العناوين وتكوين الإجراء المتخذ:

عنوان البريد الإلكتروني – العنوان الذي ستنطبق عليه القاعدة.

الاسم – اسم القاعدة المخصص.

الإجراء – الإجراء المطلوب اتخاذه إذا كان عنوان البريد الإلكتروني لجهة الاتصال يطابق العنوان المحدد في حقل **عنوان البريد الإلكتروني**:

- **السماح** – العناوين التي تعد آمنة والتي تريد استلام الرسائل منها.
- **الحظر** – العناوين التي تعد غير آمنة / عشوائية والتي لا تريد استلام الرسائل منها.
- **الاستثناء** – العناوين التي يتم فحصها دائماً بحثاً عن بريد عشوائي والتي قد تكون منتحلة وتُستخدم لإرسال بريد عشوائي.

المجال بالكامل – حدد هذا الخيار للإدخال المطلوب تطبيقه على المجال بأكمله لجهة الاتصال (ليس فقط على العنوان المحدد في حقل **عنوان البريد الإلكتروني**، وإنما جميع عناوين البريد الإلكتروني الموجودة بالمجال *address.info*).

مجالات المستوى المنخفض – حدد هذا القسم للإدخال المطلوب تطبيقه على مجالات المستوى الأدنى لجهة الاتصال (يمثل *address.info* المجال، بينما يمثل *my.address.info* مجالاً فرعياً).

نتيجة معالجة العنوان

عند إضافة عناوين جديدة أو تغيير الإجراء المتخذ لعنوان البريد الإلكتروني، فإن ESET Internet Security يعرض رسائل التنبيهات. يختلف محتوى رسائل الإعلامات حسب الإجراء الذي تحاول اتخاذه.

حدد مربع الاختيار **عدم السؤال مرة أخرى** لتنفيذ الإجراء تلقائياً دون عرض الرسالة في المرة التالية.

ThreatSense

ThreatSense عبارة عن العديد من أساليب اكتشاف التهديدات المعقدة. وتتميز هذه التقنية بأنها استباقية، ما يعني أنها توفر الحماية أيضاً خلال الانتشار المبكر لتهديد جديد. كما تستخدم توليفة مكونة من تحليل التعليمات البرمجية ومحاكاة التعليمات البرمجية والتوقيعات العامة وتوقيعات الفيروسات، وتعمل هذه التوليفة في تناغم لتعزيز حماية النظام بدرجة كبيرة. ويستطيع محرك الفحص التحكم في العديد من تدفقات البيانات بالتزامن، مما يرفع من الكفاءة ومعدل الاكتشاف. كما أن تقنية ThreatSense تستطيع التخلص من برامج الاحتيال نهائياً.

تتيح لك خيارات إعداد محرك ThreatSense تحديد العديد من معلمات الفحص كما يلي:

- أنواع وامتدادات الملفات المطلوب فحصها
- توليفة أساليب الاكتشاف المتنوعة
- مستويات المسح، إلخ.

للدخول في نافذة الإعداد، انقر فوق**ThreatSense** في الإعداد المتقدم لأي وحدة نمطية تستخدم تقنية ThreatSense (انظر أدناه). جدير بالذكر أن خيارات الأمان المختلفة تتطلب تكوينات مختلفة. فمع وضع ذلك في الاعتبار، فإن ThreatSense قابل للتكوين لكل وحدة حماية مما يلي على حدة:

- الحماية في الوقت الفعلي لنظام الملفات
- فحص حالة الخمول
- الفحص عند بدء التشغيل
- حماية المستندات
- حماية عميل البريد الإلكتروني
- حماية الوصول إلى الويب
- فحص الكمبيوتر

معلمات ThreatSense محسنة إلى حد كبير لكل وحدة، وقد يتسبب تعديلها في التأثير على تشغيل النظام بدرجة كبيرة. على سبيل المثال، فإن تغيير المعلمات لفحص أدوات حزم وقت التشغيل، أو تمكين الأساليب البحثية المتقدمة في وحدة حماية نظام الملفات في الوقت الفعلي، قد يتسبب في إبطاء النظام (عادةً ما يتم فحص الملفات المنشأة حديثاً باستخدام هذه الأساليب). لذا يوصى بترك معلمات ThreatSense الافتراضية دون تغيير لكل الوحدات عدا فحص الكمبيوتر.

الكائنات المطلوب فحصها

يتيح هذا القسم تعريف مكونات وملفات الكمبيوتر التي سيتم فحصها بحثاً عن حالات تسلل.

ذاكرة التشغيل – للفحص بحثاً عن التهديدات التي تهاجم ذاكرة التشغيل في النظام.

تشغيل القطاعات/UEFI – يفحص قطاعات التشغيل بحثاً عن وجود برامج ضارة في سجل التشغيل الرئيسي. اقرأ المزيد عن UEFI في المسرد.

ملفات البريد الإلكتروني – يدعم البرنامج الامتدادات التالية: DBX (Outlook Express) وEML.

ملفات البريد الإلكتروني – يدعم البرنامج الامتدادات التالية: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE والعديد من البرامج الأخرى.

الأرشيفات ذاتية الاستخراج – الأرشيفات ذاتية الاستخراج (SFX) عبارة عن أرشيفات يمكنها الاستخراج ذاتياً.

أدوات حزم وقت التشغيل – بعد التنفيذ، يتم فك ضغط أدوات حزم وقت التشغيل (بخلاف أنواع الأرشيفات القياسية) في الذاكرة. إضافة إلى أدوات الحزم الثابتة القياسية (UPX, yoda, ASPack, FSG إلخ)، يستطيع برنامج الفحص التعرف على العديد من الأنواع الإضافية لأدوات الحزم من خلال استخدام محاكاة التعليمات البرمجية.

خيارات الفحص

حدد الأساليب التي يتم استخدامها عند فحص النظام للبحث عن حالات تسلل. تتوفر الخيارات التالية:

الأساليب البحثية – الأسلوب البحثي هو خوارزمية تقوم بتحليل نشاط البرامج (الضار). والميزة الأساسية لهذه التقنية هي القدرة على تحديد البرامج الضارة التي لم تكن موجودة أو لم تكن مغطاة بواسطة الإصدارات السابقة للوحدة النمطية لمحرك الكشف.

بينما العيب يتمثل في احتمالية (صغيرة جداً) صدور تنبيهات غير حقيقية.

الأساليب البحثية المتقدمة/التوقيعات DNA – تتكون الأساليب البحثية المتقدمة من خوارزمية بحث فريدة قامت شركة ESET بتطويرها وتحسينها لاكتشاف فيروسات الكمبيوتر المتنقلة وأحصنة طروادة والتعليمات البرمجية الضارة المكتوبة بلغات برمجة عالية المستوى. ويساعد استخدام الأساليب البحثية المتقدمة في زيادة إمكانات منتجات ESET لاكتشاف التهديدات بدرجة عالية. كما أن التوقيعات قادرة على اكتشاف الفيروسات والتعرف عليها بشكل يعتمد عليه. جدير بالذكر أنه باستخدام نظام التحديث التلقائي تكون التوقيعات الجديدة متوفرة بعد ساعات قليلة من اكتشاف أي تهديد. غير أن عيب التوقيعات يتمثل في أنها لا تكتشف سوى الفيروسات التي تعرفها (أو الإصدارات المعدلة بشكل بسيط من هذه الفيروسات).

التنظيف

تحدد إعدادات التنظيف سلوك ESET Internet Security أثناء تنظيف الكائنات. هناك 4 مستويات من التنظيف:

يحتوي ThreatSense على مستويات الإصلاح (أي التنظيف) التالية.

الإصلاح في ESET Internet Security

الوصف	مستوى التنظيف
حاول تصحيح الاكتشاف أثناء تنظيف الأشياء دون أي تدخل من المستخدم النهائي. في بعض الحالات النادرة (على سبيل المثال، ملفات النظام)، إذا كان لا يمكن معالجة الاكتشاف، يتم ترك الكائن المبلغ عنه في موقعه الأصلي.	**اكتشاف العلاج دائماً**
حاول إصلاح الاكتشاف أثناء تنظيف الكائنات دون أي تدخل من المستخدم النهائي. في بعض الحالات (على سبيل المثال، ملفات النظام أو الأرشيفات مع كلٍّ من الملفات النظيفة والمصابة بالعدوى)، إذا تعذر إصلاح هذا الاكتشاف، فسيتم ترك الكائن المبلغ عنه في موقعه الأصلي.	**اكتشاف العلاج إذا كان آمناً، والحفاظ عليه بخلاف ذلك**
حاول إصلاح الاكتشاف أثناء تنظيف الكائنات. في بعض الحالات، إذا تعذر تنفيذ أي إجراء، يتلقى المستخدم النهائي تنبيهاً تفاعلياً ويجب عليه تحديد إجراء إصلاح (على سبيل المثال، الحذف أو التجاهل). يوصى بهذا الإعداد في معظم الحالات.	**اكتشاف العلاج إذا كان آمناً، اسأل بخلاف ذلك**
يتلقى المستخدم النهائي نافذة تفاعلية أثناء تنظيف الكائنات ويجب عليه تحديد إجراء إصلاح (على سبيل المثال، حذف أو تجاهل). تم تصميم هذا المستوى للمستخدمين الأكثر تقدماً الذين يعرفون الخطوات التي يجب اتخاذها في حالة الاكتشاف.	**اسأل دائماً المستخدم النهائي**

الاستبعادات

الملحق هو جزء اسم الملف المحدد بنقطة. يحدد الامتداد نوع ملف ومحتواه. يتيح لك هذا القسم من إعداد ThreatSense تحديد أنواع الملفات المراد فحصها.

أخرى

عند تكوين معلمات محرك ThreatSense لعملية فحص جهاز كمبيوتر عند الطلب، تتوفر أيضاً الخيارات التالية في قسم **غير ذلك**:

فحص دفق البيانات البديل (ADS) ـ عمليات دفق البيانات البديلة التي يستخدمها نظام ملفات NTFS عبارة عن ملفات ومجلدات مقترنة لا تكتشفها تقنيات الفحص العادية. ويحاول العديد من حالات التسلل تجنب الاكتشاف بواسطة إخفاء أنفسها كعمليات دفق بيانات بديلة.

تشغيل عمليات الفحص في الخلفية بأولية منخفضة ـ يستهلك كل تسلسل فحص كمية معينة من موارد النظام. فإذا كنت تعمل باستخدام برامج تضع حملاً مرتفعً على موارد النظام، فيمكنك تنشيط الفحص في الخلفية المنخفض الأولوية وتوفير الموارد للتطبيقات التي تستخدمها.

تسجيل جميع الكائنات ـ يعرض سجل الفحص جميع الملفات التي تم فحصها في أرشيفات الاستخراج الذاتي، حتى تلك غير

المصابة (قد يقوم بإنشاء الكثير من بيانات سجل الفحص ويزيد من حجم ملف سجل الفحص).

تمكين التحسين الذكي – مع تمكين التحسين الذكي، يتم استخدام أفضل الإعدادات لضمان أكثر مستويات الفحص كفاءة، مع الاحتفاظ بأعلى سرعات فحص في الوقت نفسه. تُجري وحدات الحماية المختلفة الفحص بذكاء، مستخدمة مختلف طرق الفحص وتقوم بتطبيقها على أنواع ملفات معينة. في حالة تعطيل التحسين الذكي، يتم تطبيق الإعدادات المحددة بواسطة المستخدم في إعدادات ThreatSense الأساسية للوحدات المعينة عند إجراء فحص.

المحافظة على الطابع الزمني للوصول الأخير – حدد هذا الخيار للحفاظ على وقت الوصول الأصلي للملفات التي تم فحصها بدلاً من تحديثها (على سبيل المثال، للاستخدام مع أنظمة النسخ الاحتياطي للبيانات).

الحدود

يتيح قسم "الحدود" تحديد الحد الأقصى لحجم الكائنات ومستويات الأرشيفات المتشابكة المطلوب فحصها:

إعدادات الكائنات

أقصى حجم للكائن – تحديد أقصى حجم للكائنات المطلوب فحصها. وبالتالي ستقوم وحدة الحماية ضد الفيروسات المحددة بفحص الكائنات الصغرى عن الحجم المحدد فقط. ويجب عدم تغيير هذا الخيار إلا بواسطة المستخدمين المتقدمين الذين لديهم أسباب محددة لاستبعاد الكائنات الكبرى من الفحص. القيمة الافتراضية: غير محدودة.

أقصى وقت فحص للكائن (بالثانية) – لتحديد الحد الأقصى لقيمة الوقت لفحص الملفات في كائن حاوية (مثل أرشيف RAR/ZIP أو رسالة بريد إلكتروني تحتوي على مرفقات متعددة). لا ينطبق هذا الإعداد على الملفات المستقلة. إذا تم إدخال قيمة معرفة من قبل المستخدم وانقضى ذلك الوقت، فسيتوقف الفحص في أقرب وقت ممكن، بغض النظر عما إذا كان الفحص لكل ملف في كائن حاوية قد انتهى.
في حالة وجود أرشيف يحتوي على ملفات كبيرة، لن يتوقف الفحص قبل استخراج ملف من الأرشيف (على سبيل المثال، عندما يكون المتغير المحدد من قبل المستخدم هو 3 ثوانٍ، ولكن استخراج الملف يستغرق 5 ثوانٍ). لن يتم فحص بقية الملفات الموجودة في الأرشيف عند انقضاء ذلك الوقت.
للحد من وقت الفحص، بما في ذلك الأرشيفات الأكبر حجماً، استخدم **الحد الأقصى لحجم الكائن** و**الحجم الأقصى للملف في الأرشيف** (غير مستحسن بسبب المخاطر الأمنية المحتملة).
القيمة الافتراضية: غير محدودة.

إعداد فحص الأرشيفات

مستوى تداخل الأرشيف – تحديد أقصى عمق لفحص الأرشيف. القيمة الافتراضية: 10.

أقصى حجم للملف في الأرشيف – يسمح لك هذا الخيار بتحديد أقصى حجم ملف للملفات الموجودة في الأرشيفات (عند استخراجها) المطلوب فحصها. الحد الأقصى للقيمة **3 جيجابايت**.

> i يوصى بعدم تغيير القيم الافتراضية؛ ففي ظل الظروف العادية يفترض عدم وجود أي سبب لتعديلها.

حماية الوصول إلى الويب

تتيح لك حماية الوصول إلى الويب تكوين إعدادات وحدة حماية الإنترنت المتقدمة. تتوفر الخيارات التالية في الإعداد المتقدم > **وسائل الحماية > حماية الوصول إلى الويب > حماية الوصول إلى الويب**:

تمكين حماية الوصول إلى الويب – في حالة التعطيل، لن يتم تشغيل حماية الوصول إلى الويب والحماية ضد التصيد الاحتيالي.

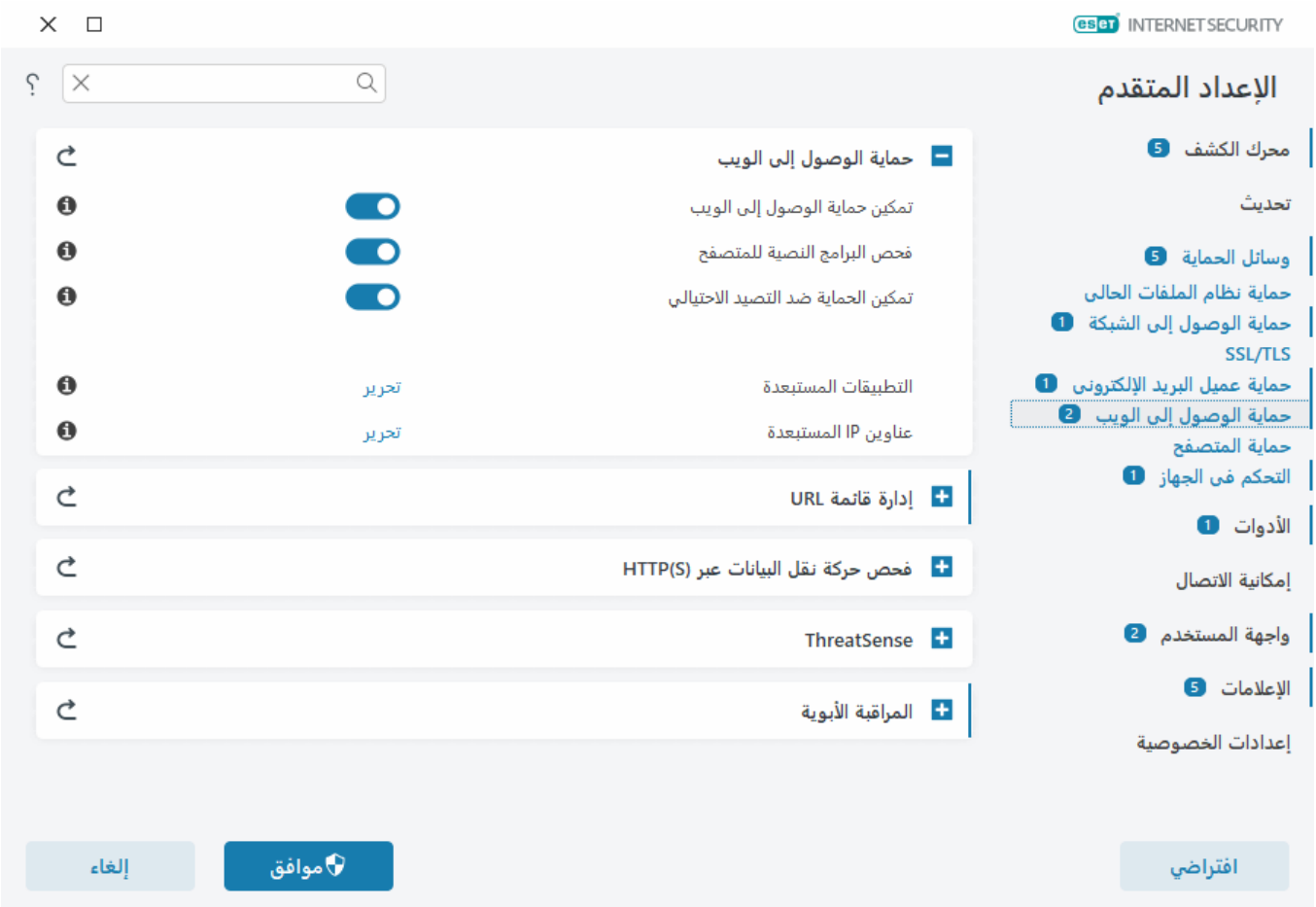
> نوصي بشدة بترك حماية الوصول إلى الويب ممكّنة وعدم استبعاد أي تطبيقات أو عناوين IP افتراضياً.

فحص البرامج النصية للمتصفح—عند التمكين، يقوم محرك الكشف بفحص جميع JavaScript البرامج التي تنفذها متصفحات الويب.

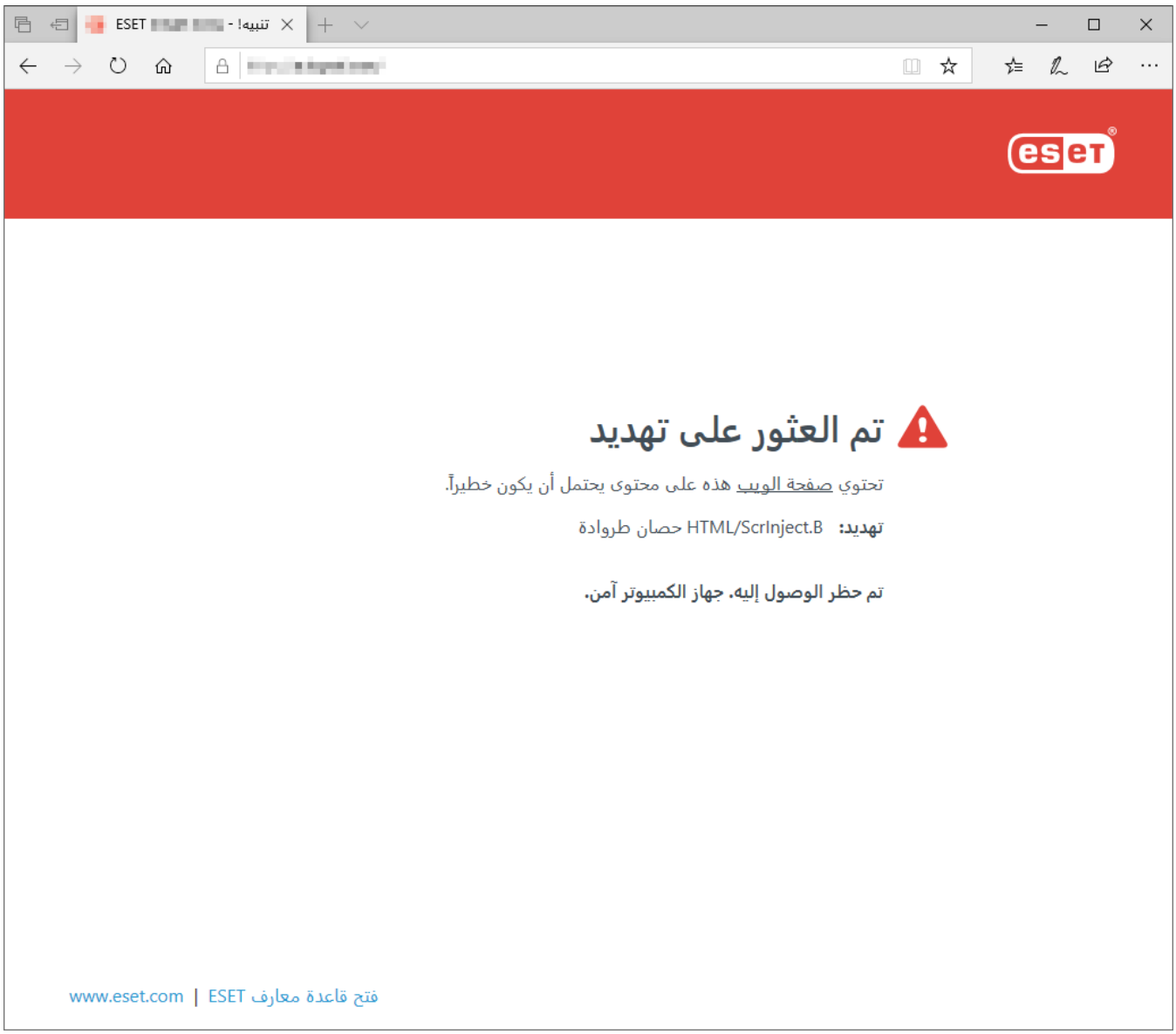
تمكين حماية مضاد التصيد—عند التمكين، يتم حظر صفحات الويب المخادعة. راجع حماية مضادة للتصيد الاحتيالي لمزيد من المعلومات.

تمكّنك التطبيقات المستبعدة— من استبعاد تطبيقات معينة من الفحص بواسطة حماية الوصول إلى الويب. يكون مفيداً عندما تتسبب حماية الوصول إلى الويب في حدوث مشكلات في التوافق.

تمكّنكعناوين IP المستبعدة—من استبعاد عناوين بعيدة محددة من الفحص بواسطة حماية الوصول إلى الويب. يكون مفيداً عندما تتسبب حماية الوصول إلى الويب في حدوث مشكلات في التوافق.



ستقوم حماية الوصول إلى الويب بعرض الرسالة التالية في مستعرضك عند حظر موقع الويب:



إرشادات موضحة

قد لا تتوفر مقالات قاعدة معارف ESET التالية إلا باللغة الإنجليزية:

- استبعاد موقع ويب آمن من الحظر من خلال حماية استخدام الإنترنت
- حظر موقع ويب باستخدام ESET Internet Security

التطبيقات المستبعدة

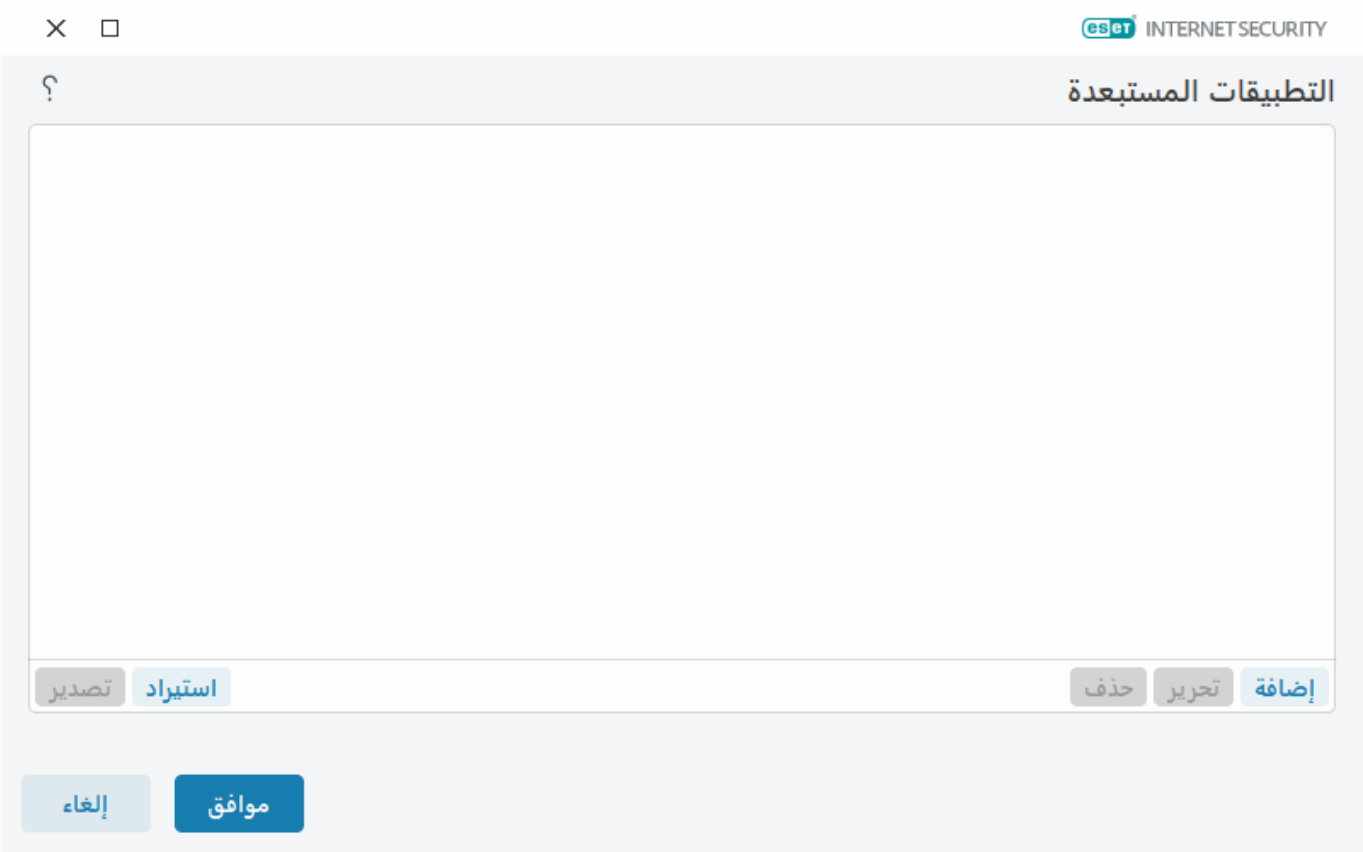
لاستبعاد فحص الاتصالات لتطبيقات محددة، قم بإضافتها إلى القائمة. لن يتم فحص اتصال (HTTP(S)/POP3(S)/IMAP(S للتطبيقات المحددة بحثاً عن تهديدات. نوصي فقط باستخدام هذا للتطبيقات التي لا تعمل بشكل صحيح مع اتصالاتها الخاضعة للفحص.

ستكون التطبيقات والخدمات الجارية متوفرة هنا تلقائياً عند النقر فوق **إضافة**. انقر فوق **...** وانتقل إلى تطبيق لإضافة الاستبعاد

يدوياً.

تحرير – تحرير الإدخالات المحددة من القائمة.

إزالة – إزالة الإدخالات المحددة من القائمة.



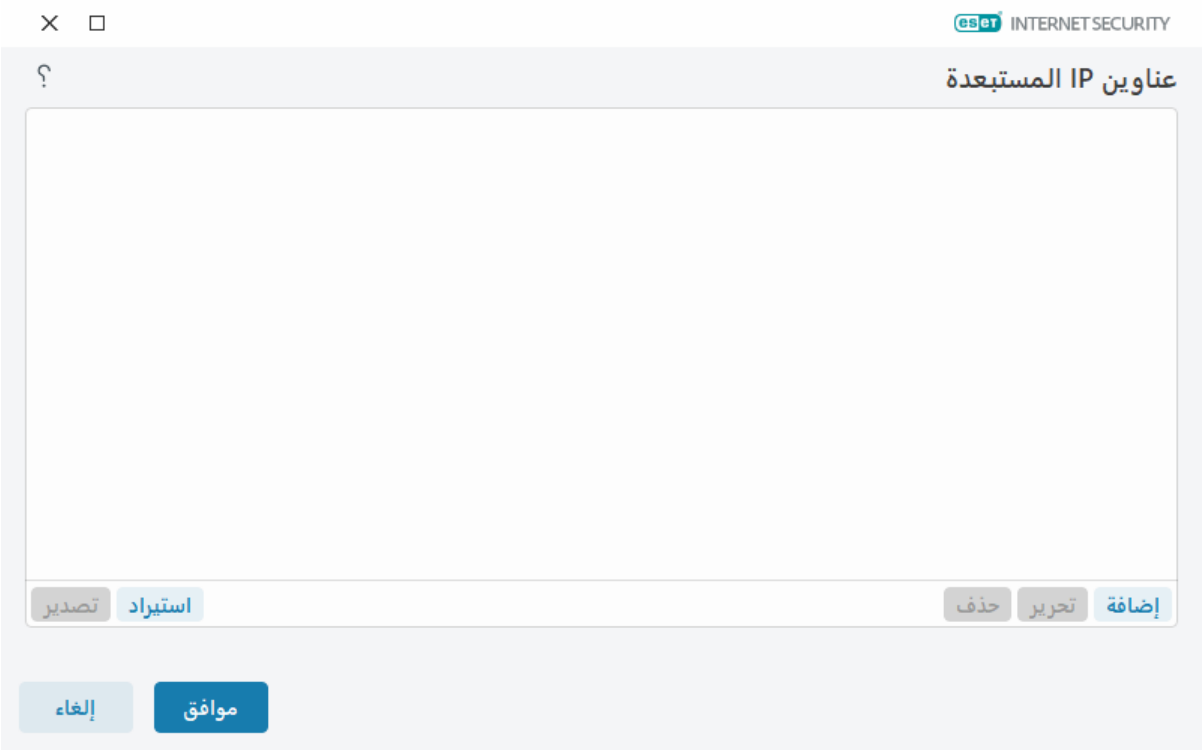
عناوين IP المستبعدة

سيتم استبعاد الإدخالات الموجودة في القائمة من الفحص. لن يتم فحص اتصال (HTTP(S)/POP3(S)/IMAP(S من/إلى العناوين المحددة بحثاً عن تهديدات. يوصى بعدم استخدام هذا الخيار مع العناوين المعروفة بكونها موثوقة.

انقر فوق **إضافة** لاستبعاد عنوان IP/نطاق العنوان/شبكة فرعية لنقطة بعيدة.

انقر فوق **تحرير** لتغيير عنوان IP المحدد.

انقر فوق **حذف** لإزالة الإدخالات المحددة من القائمة.



أمثلة لعناوين IP

إضافة عنوان IPv4:

العنوان الفردي— يضيف عنوان IP لجهاز كمبيوتر فردي (على سبيل المثال، *192.168.0.10*).

نطاق العناوين — أدخل عنوان البدء وعنوان الانتهاء لعنوان IP لتحديد نطاق IP لأجهزة كمبيوتر عديدة (على سبيل المثال 192.168.0.1 إلى 192.168.0.99).

الشبكة الفرعية – يتم تحديد الشبكة الفرعية (مجموعة من أجهزة الكمبيوتر) عن طريق قناع وعنوان IP. على سبيل المثال، 255.255.255.0 هو قناع الشبكة للشبكة الفرعية 192.168.1.0 . لاستبعاد نوع الشبكة الفرعية بالكامل في *192.168.1.0/24*.

إضافة عناوين IPv6:

العنوان الفردي— يضيف عنوان IP الخاص بكمبيوتر فردي (على سبيل المثال، *2001:718:1c01:16:214:22ff:fec9:ca5*).

الشبكة الفرعية – يتم تحديد الشبكة الفرعية (مجموعة من أجهزة الكمبيوتر) عن طريق قناع وعنوان IP (على سبيل المثال: *c0a8:6301:1::1/64:2002*).

إدارة قائمة URL

تتيح لك **إدارة قائمة عناوين URL** في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الويب** تحديد عناوين HTTP لحظرها أو السماح بها أو استبعادها من فحص المحتوى.

يجب تمكينSSL/TLS إذا كنت تريد تصفية HTTPS العناوين بالإضافة إلى HTTP. بخلاف ذلك، فلن تتم إضافة سوى نطاقات مواقع HTTPS التي تزورها، بينما لن تتم إضافة عنوان URL الكامل.

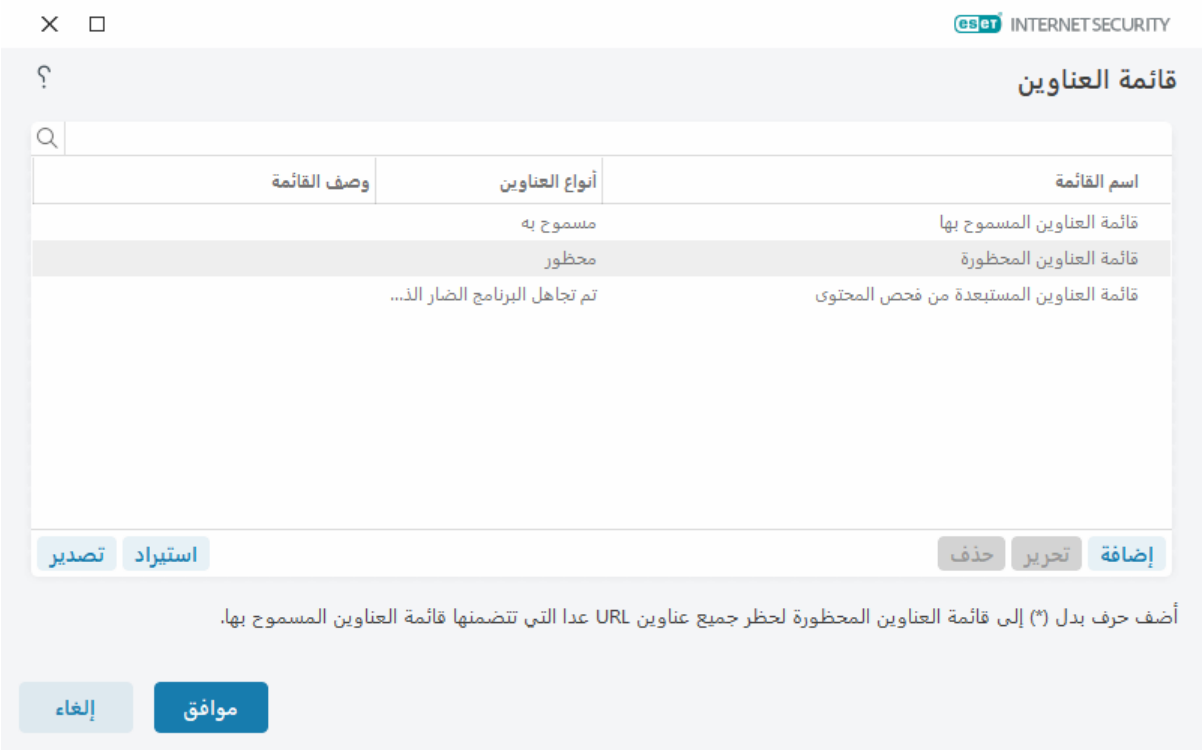
لا يمكن الوصول إلى مواقع الويب الموجودة في **قائمة العناوين المحظورة** ما لم تكن مضمنة كذلك في **قائمة العناوين المسموح بها**. وعند الوصول إلى مواقع الويب الموجودة في **قائمة العناوين المستبعدة من فحص المحتوى**، لن يتم فحصها للبحث عن التعليمات البرمجية الضارة.

إذا كنت ترغب في حظر كل عناوين HTTP باستثناء العناوين الموجودة في **قائمة العناوين المسموح بها** النشطة، فأضف * إلى

قائمة العناوين المحظورة النشطة.

ويمكن استخدام رموز خاصة مثل * (النجمة) و ? (علامة الاستفهام) في القوائم. تحل العلامة النجمية محل أية سلسلة أحرف، بينما تحل علامة الاستفهام محل أي رمز. يجب توخي الحذر عند تحديد عناوين مستبعدة، لأن القائمة يجب أن تحتوي فقط على العناوين الموثوقة والآمنة. وبالمثل، من الضروري ضمان استخدام الرمزين * و ? بشكل صحيح في هذه القائمة. راجع إضافة عنوان HTTP / قناع مجال لمعرفة كيف يمكن مطابقة مجال كامل بما في ذلك جميع المجالات الفرعية بأمان. لتنشيط قائمة، حدد **قائمة نشطة**. إذا كنت تريد أن يتم إعلامك عند إدخال عنوان من القائمة الحالية، فحدد **إعلام عند التطبيق**.

> **العناوين الموثوق بها من قبل ESET**
> في حالة تمكين **عدم فحص حركة المرور باستخدام مجالات موثوق بها من قبل ESET** في SSL/TLS، فلن تتأثر المجالات الموجودة في القائمة البيضاء التي تديرها ESET بتكوين إدارة قائمة عناوين URL.



عناصر التحكم

إضافة – إنشاء قائمة جديدة إلى جانب القوائم المحددة مسبقاً. ويمكن أن يكون هذا مفيداً إذا كنت تريد أن تقسم مجموعات مختلفة من العناوين تقسيماً منطقياً. على سبيل المثال، يمكن أن تحتوي قائمة بالعناوين المحظورة على عناوين من قائمة حظر عامة خارجية، بينما تحتوي قائمة أخرى على قائمة الحظر الخاصة بك، ما يسهل عملية تحديث القائمة الخارجية أثناء الاحتفاظ بقائمتك الخاصة دون تغيير.

تحرير – لتعديل القوائم الموجودة. يستخدم لإضافة العناوين أو إزالتها.

حذف – لحذف القوائم الموجودة. وهذا الخيار متاح فقط للقوائم التي تم إنشاؤها باستخدام **إضافة**، وليس للقوائم الافتراضية.

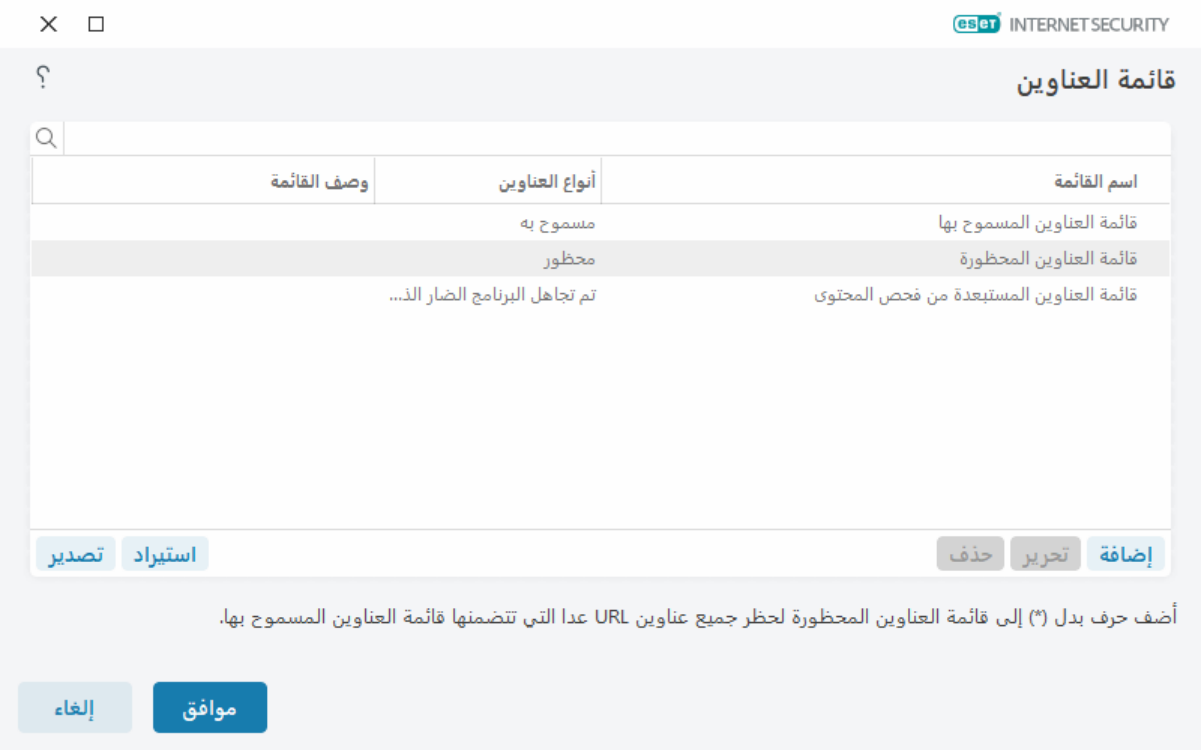
قائمة العناوين

في هذا القسم، يمكنك تحديد قوائم عناوين HTTP(S) التي سيتم حظرها أو السماح بها أو استبعادها من الفحص.

وتتوفر القوائم الثلاثة التالية بشكل افتراضي:

- **قائمة العناوين المستبعدة من فحص المحتوى** – لا يتم إجراء البحث عن التعليمات البرمجية الضارة لأي عنوان تتم إضافته إلى هذه القائمة.
- **قائمة العناوين المسموح بها** – إذا تم تمكين خيار "عدم السماح بالوصول إلا إلى عناوين HTTP المدرجة في قائمة العناوين المسموح بها"، وكانت قائمة العناوين المحظورة تشتمل على رمز * (مطابقة كل شيء)، فسيُسمح للمستخدم بالوصول إلى العناوين المحددة في هذه القائمة فقط. يُسمح بالعناوين الموجودة في هذه القائمة حتى إذا كانت مدرجة في قائمة العناوين المحظورة.
- **قائمة العناوين المحظورة** – لن يُسمح للمستخدم بالوصول إلى العناوين المحددة في هذه القائمة ما لم تكن موجودة في قائمة العناوين المسموح بها.

انقر فوق **إضافة** لإنشاء قائمة جديدة. ولحذف القوائم المحددة، انقر فوق **حذف**.



إرشادات موضحة

قد لا تتوفر مقالات قاعدة معارف ESET التالية إلا باللغة الإنجليزية:

- استبعاد موقع ويب آمن من الحظر من خلال حماية استخدام الإنترنت
- حظر موقع ويب باستخدام منتجات الصفحة الرئيسية لـ ESET Windows

لمزيد من المعلومات، راجع إدارة قائمة عناوين URL.

إنشاء قائمة جديدة لعناوين

تتيح لك نافذة الحوار هذه تكوين قائمة عناوين/أقنعة URL جديدة التي سيتم حظرها أو السماح بها أو استبعادها من الفحص.

يمكنك تكوين الخيارات التالية:

نوع قائمة العناوين – تتوفر أنواع القوائم الثلاث التالية:

- **تم تجاهل البرنامج الضار الذي تم العثور عليه** ـ لا يتم إجراء البحث عن التعليمات البرمجية الضارة لأي عنوان تتم إضافته إلى هذه القائمة.
- **محظور** ـ سيتم حظر الوصول إلى العناوين المحددة في هذه القائمة.
- **مسموح** ـ سيتم السماح بالوصول إلى العناوين المحددة في هذه القائمة. يُسمح بعناوين الموجودة في هذه القائمة حتى إذا كانت متطابقة مع قائمة العناوين المحظورة.

اسم القائمة ـ حدد اسم القائمة. سيكون هذا الحقل غير متوفر عند تحرير إحدى القوائم المحددة مسبقاً.

وصف القائمة – اكتب وصفاً مختصراً للقائمة (اختياري). غير متوفر عند تحرير إحدى القوائم المحددة مسبقاً.

لتنشيط قائمة، حدد **قائمة نشطة** بجوار تلك القائمة. إذا كنت تريد أن يتم إعلامك عند استخدام قائمة معينة عند الوصول إلى مواقع الويب، فحدد **إعلام عند التطبيق**. فمثلاً، ستتلقى إعلاماً عندما يتم حظر موقع ويب أو السماح به بسبب تضمينه في قائمة العناوين المحظورة أو المسموح بها. وسيحتوي الإعلام على اسم القائمة.

تسجيل الخطورة ـ يمكن كتابة معلومات حول القائمة المحددة المستخدمة عند الوصول إلى مواقع الويب إلى ملفات السجل.

عناصر التحكم

إضافة ـ أضف عنوان URL جديداً إلى القائمة (أدخل قيماً متعددة بفاصل بينها).

تحرير ـ لتعديل عنوان موجود في القائمة. متوفر للعناوين المنشأة باستخدام الخيار **إضافة** فقط.

إزالة ـ لحذف عناوين موجودة في القائمة. متوفر للعناوين المنشأة باستخدام الخيار **إضافة** فقط.

استيراد ـ استيراد ملف يشتمل على عناوين URL (افصل بين القيم بفاصل أسطر، مثلاً *.txt يستخدم الترميز UTF-8).

كيفية إضافة قناع URL

الرجاء الرجوع إلى الإرشادات الواردة بمربع الحوار هذا قبل إدخال العنوان/قناع المجال المطلوب.

يتيح ESET Internet Security للمستخدم حظر الوصول إلى مواقع ويب محددة، ومنع مستعرض الإنترنت من عرض محتواه. كما يسمح ـ علاوة على ذلك ـ للمستخدم بتحديد عناوين، يجب استثناؤها من الفحص. إذا كان الاسم الكامل للخادم البعيد غير معروف، أو رغب المستخدم في تحديد مجموعة كاملة من الخوادم البعيدة، فيمكن استخدام الأقنعة المذكورة لتحديد تلك المجموعة. يشمل القناع الرمزين "?" و"*":

- استخدم علامة ? لتحل محل رمز
- استخدم علامة * لتحل محل سلسلة نصية.

على سبيل المثال، ينطبق القناع *.c?m على جميع العناوين، التي يبدأ الجزء الأخير منها بالحرف c وينتهي بالحرف m ويحتوي على رمز غير معروف بينهما (مثل .com و.cam وغيرهما)

يتم التعامل مع تسلسل '*.' البادئ بشكل خاص في حالة استخدامه في بداية اسم المجال. أولاً، لا يطابق حرف البدل * حرف الشرطة المائلة للأمام ('/') في هذه الحالة. وذلك لتجنب خداع القناع، فمثلاً القناع *domain.com. لن يطابق *http://anydomain.com/anypath#.domain.com* (يمكن إلحاق هذه اللاحقة بأي عنوان URL دون التأثير على التنزيل). وثانياً، يطابق التسلسل "*." أيضاً سلسلة فارغة في هذه الحالة الخاصة. وذلك للسماح بمطابقة المجال بالكامل، بما فيه أي مجالات فرعية باستخدام قناع واحد. مثلاً القناع *domain.com. يطابق أيضاً *http://domain.com*. سيكون استخدام *domain.com غير صحيح، لأن ذلك يجب أن يطابق أيضاً *http://anotherdomain.com*.

فحص حركة نقل البيانات عبر HTTP(S)

افتراضياً، يتم تكوين ESET Internet Security لفحص حركة مرور HTTP و HTTPS التي تستخدمها متصفحات الإنترنت والتطبيقات الأخرى. يجب عليك تعطيل فحص حركة المرور فقط إذا كنت تواجه مشكلات مع برنامج تابع لجهة خارجية وتريد معرفة ما إذا كانت المشكلة ناتجة عن ذلك ESET Internet Security.

تمكين فحص حركة نقل البيانات عبر HTTP – تتم مراقبة حركة انتقال HTTP دائماً على جميع المنافذ لجميع التطبيقات.

تمكين فحص حركة مرور HTTPS—يتستخدم حركة مرور HTTPS قناة مشفرة لنقل المعلومات بين الخادم والعميل. ويقوم ESET Internet Securityبفحص الاتصالات التي تستخدمSSL بروتوكول (طبقة مأخذ التوصيل الآمنة) TLSوبروتوكول (أمان طبقة النقل). سيقوم البرنامج فقط بفحص حركة المرور على المنافذ المحددة في **المنافذ المستخدمة بواسطة بروتوكول HTTPS**، بغض النظر عن إصدار نظام التشغيل (يمكنك إضافة منافذ إلى 443 المعرفة مسبقاً و 0–65535).

ThreatSense

ThreatSense عبارة عن العديد من أساليب اكتشاف التهديدات المعقدة. وتتميز هذه التقنية بأنها استباقية، ما يعني أنها توفر الحماية أيضاً خلال الانتشار المبكر لتهديد جديد. كما تستخدم توليفة مكونة من تحليل التعليمات البرمجية ومحاكاة التعليمات البرمجية والتوقيعات العامة وتوقيعات الفيروسات، وتعمل هذه التوليفة في تناغم لتعزيز حماية النظام بدرجة كبيرة. ويستطيع محرك الفحص التحكم في العديد من تدفقات البيانات بالتزامن، مما يرفع من الكفاءة ومعدل الاكتشاف. كما أن تقنية ThreatSense تستطيع التخلص من برامج الاحتيال نهائياً.

تتيح لك خيارات إعداد محرك ThreatSense تحديد العديد من معلمات الفحص كما يلي:

- أنواع وامتدادات الملفات المطلوب فحصها
- توليفة أساليب الاكتشاف المتنوعة
- مستويات المسح، إلخ.

للدخول في نافذة الإعداد، انقر فوق**ThreatSense** في الإعداد المتقدم لأي وحدة نمطية تستخدم تقنية ThreatSense (انظر أدناه).

جدير بالذكر أن خيارات الأمان المختلفة تتطلب تكوينات مختلفة. فمع وضع ذلك في الاعتبار، فإن ThreatSense قابل للتكوين لكل وحدة حماية مما يلي على حدة:

- الحماية في الوقت الفعلي لنظام الملفات
- فحص حالة الخمول
- الفحص عند بدء التشغيل
- حماية المستندات
- حماية عميل البريد الإلكتروني
- حماية الوصول إلى الويب
- فحص الكمبيوتر

معلمات ThreatSense محسنة إلى حد كبير لكل وحدة، وقد يتسبب تعديلها في التأثير على تشغيل النظام بدرجة كبيرة. على سبيل المثال، فإن تغيير المعلمات لفحص أدوات حزم وقت التشغيل، أو تمكين الأساليب البحثية المتقدمة في وحدة حماية نظام الملفات في الوقت الفعلي، قد يتسبب في إبطاء النظام (عادةً ما يتم فحص الملفات المنشأة حديثاً باستخدام هذه الأساليب). لذا يوصى بترك معلمات ThreatSense الافتراضية دون تغيير لكل الوحدات عدا فحص الكمبيوتر.

الكائنات المطلوب فحصها

يتيح هذا القسم تعريف مكونات وملفات الكمبيوتر التي سيتم فحصها بحثاً عن حالات تسلل.

ذاكرة التشغيل – للفحص بحثاً عن التهديدات التي تهاجم ذاكرة التشغيل في النظام.

تشغيل القطاعات/UEFI – يفحص قطاعات التشغيل بحثاً عن وجود برامج ضارة في سجل التشغيل الرئيسي. اقرأ المزيد عن UEFI في المسرد.

ملفات البريد الإلكتروني – يدعم البرنامج الامتدادات التالية: DBX (Outlook Express) وEML.

ملفات البريد الإلكتروني – يدعم البرنامج الامتدادات التالية: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE والعديد من البرامج الأخرى.

الأرشيفات ذاتية الاستخراج – الأرشيفات ذاتية الاستخراج (SFX) عبارة عن أرشيفات يمكنها الاستخراج ذاتياً.

أدوات حزم وقت التشغيل – بعد التنفيذ، يتم فك ضغط أدوات حزم وقت التشغيل (بخلاف أنواع الأرشيفات القياسية) في الذاكرة. إضافة إلى أدوات الحزم الثابتة القياسية (UPX, yoda, ASPack, FSG إلخ)، يستطيع برنامج الفحص التعرف على العديد من الأنواع الإضافية لأدوات الحزم من خلال استخدام محاكاة التعليمات البرمجية.

خيارات الفحص

حدد الأساليب التي يتم استخدامها عند فحص النظام للبحث عن حالات تسلل. تتوفر الخيارات التالية:

الأساليب البحثية – الأسلوب البحثي هو خوارزمية تقوم بتحليل نشاط البرامج (الضار). والميزة الأساسية لهذه التقنية هي القدرة على تحديد البرامج الضارة التي لم تكن موجودة أو لم تكن مغطاة بواسطة الإصدارات السابقة للوحدة النمطية لمحرك الكشف. بينما العيب يتمثل في احتمالية (صغيرة جداً) صدور تنبيهات غير حقيقية.

الأساليب البحثية المتقدمة/التوقيعات DNA – تتكون الأساليب البحثية المتقدمة من خوارزمية بحث فريدة قامت شركة ESET بتطويرها وتحسينها لاكتشاف فيروسات الكمبيوتر المتنقلة وأحصنة طروادة والتعليمات البرمجية الضارة المكتوبة بلغات برمجة عالية المستوى. ويساعد استخدام الأساليب البحثية المتقدمة في زيادة إمكانات منتجات ESET لاكتشاف التهديدات بدرجة عالية. كما أن التوقيعات قادرة على اكتشاف الفيروسات والتعرف عليها بشكل يعتمد عليه. جدير بالذكر أنه باستخدام نظام التحديث التلقائي تكون التوقيعات الجديدة متوفرة بعد ساعات قليلة من اكتشاف أي تهديد. غير أن عيب التوقيعات يتمثل في أنها لا تكتشف سوى الفيروسات التي تعرفها (أو الإصدارات المعدلة بشكل بسيط من هذه الفيروسات).

التنظيف

تحدد إعدادات التنظيف سلوك ESET Internet Security أثناء تنظيف الكائنات. هناك 4 مستويات من التنظيف:

يحتوي ThreatSense على مستويات الإصلاح (أي التنظيف) التالية.

الإصلاح في ESET Internet Security

الوصف	مستوى التنظيف
حاول تصحيح الاكتشاف أثناء تنظيف الأشياء دون أي تدخل من المستخدم النهائي. في بعض الحالات النادرة (على سبيل المثال، ملفات النظام)، إذا كان لا يمكن معالجة الاكتشاف، يتم ترك الكائن المبلغ عنه في موقعه الأصلي.	**اكتشاف العلاج دائماً**
حاول إصلاح الاكتشاف أثناء تنظيف الكائنات دون أي تدخل من المستخدم النهائي. في بعض الحالات (على سبيل المثال، ملفات النظام أو الأرشيفات مع كلٍّ من الملفات النظيفة والمصابة بالعدوى)، إذا تعذر إصلاح هذا الاكتشاف، فسيتم ترك الكائن المبلغ عنه في موقعه الأصلي.	**اكتشاف العلاج إذا كان آمناً، والحفاظ عليه بخلاف ذلك**
حاول إصلاح الاكتشاف أثناء تنظيف الكائنات. في بعض الحالات، إذا تعذر تنفيذ أي إجراء، يتلقى المستخدم النهائي تنبيهاً تفاعلياً ويجب عليه تحديد إجراء إصلاح (على سبيل المثال، الحذف أو التجاهل). يوصى بهذا الإعداد في معظم الحالات.	**اكتشاف العلاج إذا كان آمناً، اسأل بخلاف ذلك**
يتلقى المستخدم النهائي نافذة تفاعلية أثناء تنظيف الكائنات ويجب عليه تحديد إجراء إصلاح (على سبيل المثال، حذف أو تجاهل). تم تصميم هذا المستوى للمستخدمين الأكثر تقدماً الذين يعرفون الخطوات التي يجب اتخاذها في حالة الاكتشاف.	**اسأل دائماً المستخدم النهائي**

الاستبعادات

الملحق هو جزء اسم الملف المحدد بنقطة. يحدد الامتداد نوع ملف ومحتواه. يتيح لك هذا القسم من إعداد ThreatSense تحديد أنواع الملفات المراد فحصها.

أخرى

عند تكوين معلمات محرك ThreatSense لعملية فحص جهاز كمبيوتر عند الطلب، تتوفر أيضاً الخيارات التالية في قسم **غير ذلك**:

فحص دفق البيانات البديل (ADS) – عمليات دفق البيانات البديلة التي يستخدمها نظام ملفات NTFS عبارة عن ملفات ومجلدات مقترنة لا تكتشفها تقنيات الفحص العادية. ويحاول العديد من حالات التسلل تجنب الاكتشاف بواسطة إخفاء أنفسها كعمليات دفق بيانات بديلة.

تشغيل عمليات الفحص في الخلفية بأولية منخفضة – يستهلك كل تسلسل فحص كمية معينة من موارد النظام. فإذا كنت تعمل باستخدام برامج تضع حملاً مرتفعً على موارد النظام، فيمكنك تنشيط الفحص في الخلفية المنخفض الأولوية وتوفير الموارد للتطبيقات التي تستخدمها.

تسجيل جميع الكائنات – يعرض سجل الفحص جميع الملفات التي تم فحصها في أرشيفات الاستخراج الذاتي، حتى تلك غير المصابة (قد يقوم بإنشاء الكثير من بيانات سجل الفحص ويزيد من حجم ملف سجل الفحص).

تمكين التحسين الذكي – مع تمكين التحسين الذكي، يتم استخدام أفضل الإعدادات لضمان أكثر مستويات الفحص كفاءة، مع الاحتفاظ بأعلى سرعات فحص في الوقت نفسه. تُجري وحدات الحماية المختلفة الفحص بذكاء، مستخدمة مختلف طرق الفحص وتقوم بتطبيقها على أنواع ملفات معينة. في حالة تعطيل التحسين الذكي، يتم تطبيق الإعدادات المحددة بواسطة المستخدم في إعدادات ThreatSense الأساسية للوحدات المعينة عند إجراء فحص.

المحافظة على الطابع الزمني للوصول الأخير – حدد هذا الخيار للحفاظ على وقت الوصول الأصلي للملفات التي تم فحصها بدلاً من تحديثها (على سبيل المثال، للاستخدام مع أنظمة النسخ الاحتياطي للبيانات).

الحدود

يتيح قسم "الحدود" تحديد الحد الأقصى لحجم الكائنات ومستويات الأرشيفات المتشابكة المطلوب فحصها:

إعدادات الكائنات

أقصى حجم للكائن – تحديد أقصى حجم للكائنات المطلوب فحصها. وبالتالي ستقوم وحدة الحماية ضد الفيروسات المحددة بفحص الكائنات الصغرى عن الحجم المحدد فقط. ويجب عدم تغيير هذا الخيار إلا بواسطة المستخدمين المتقدمين الذين لديهم أسباب محددة لاستبعاد الكائنات الكبرى من الفحص. القيمة الافتراضية: غير محدودة.

أقصى وقت فحص للكائن (بالثانية) – لتحديد الحد الأقصى لقيمة الوقت لفحص الملفات في كائن حاوية (مثل أرشيف RAR/ZIP أو رسالة بريد إلكتروني تحتوي على مرفقات متعددة). لا ينطبق هذا الإعداد على الملفات المستقلة. إذا تم إدخال قيمة معرفة من قبل المستخدم وانقضى ذلك الوقت، فسيتوقف الفحص في أقرب وقت ممكن، بغض النظر عما إذا كان الفحص لكل ملف في كائن حاوية قد انتهى.
في حالة وجود أرشيف يحتوي على ملفات كبيرة، لن يتوقف الفحص قبل استخراج ملف من الأرشيف (على سبيل المثال، عندما يكون المتغير المحدد من قبل المستخدم هو 3 ثوانٍ، ولكن استخراج الملف يستغرق 5 ثوانٍ). لن يتم فحص بقية الملفات الموجودة في الأرشيف عند انقضاء ذلك الوقت.
للحد من وقت الفحص، بما في ذلك الأرشيفات الأكبر حجماً، استخدم **الحد الأقصى لحجم الكائن** و**الحجم الأقصى للملف في الأرشيف** (غير مستحسن بسبب المخاطر الأمنية المحتملة).
القيمة الافتراضية: غير محدودة.

إعداد فحص الأرشيفات

مستوى تداخل الأرشيف – تحديد أقصى عمق لفحص الأرشيف. القيمة الافتراضية: 10.

أقصى حجم للملف في الأرشيف – يسمح لك هذا الخيار بتحديد أقصى حجم ملف للملفات الموجودة في الأرشيفات (عند استخراجها) المطلوب فحصها. الحد الأقصى للقيمة **3 جيجابايت**.

> i يوصى بعدم تغيير القيم الافتراضية؛ ففي ظل الظروف العادية يفترض عدم وجود أي سبب لتعديلها.

المراقبة الأبوية

يعمل خيار **تمكين الرقابة الأبوية** على دمج الرقابة الأبوية في ESET Internet Security. انقر فوق **تحرير** بجوار حسابات المستخدم لربط حسابات مستخدمي Windows المُستخدمة بواسطة ميزة المراقبة الأبوية مع مستخدمين محددين لتقييد وصولهم إلى محتوى ضار أو غير مناسب عبر الإنترنت.

حسابات المستخدمين

في الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الويب** > **المراقبة الأبوية** > **حسابات المستخدم** > **تحرير** يمكنك ربط حسابات مستخدمي Windows المُستخدمة بواسطة المراقبة الأبوية مع مستخدمين محددين لتقييد وصولهم إلى محتوى ضار أو غير مناسب عبر الإنترنت.

الأعمدة

حساب Windows – اسم المستخدم.

ممكَّن – عند تمكين هذه الميزة، فإن عناصر المراقبة الأبوية لحساب مستخدم محدد تكون نشطة.

المجال – اسم المجال الذي ينتمي إليه المستخدم.

تاريخ الميلاد – عمر المستخدم الذي ينتمي إليه هذا الحساب.

عناصر التحكم

إضافة – سيظهر مربع الحوار التعامل مع حسابات المستخدمين.

تحرير—يتيح لك هذا الخيار إمكانية تحرير الحسابات المحددة.

حذف – حذف الحساب المحدد.

تحديث – إذا قمت بإضافة حساب مستخدم، يمكن من خلال ESET Internet Security تحديث قائمة حسابات المستخدمين دون الحاجة إلى إعادة فتح هذه النافذة.

إعدادات حساب المستخدم

تحتوي النافذة على ثلاث علامات تبويب:

عام

قم بتمكين مفتاح التبديل بجوار **ممكّن** لتشغيل المراقبة الأبوية لحساب Windows المحدد أدناه.

حدد حساب Windows من الكمبيوتر لديك. لا تؤثر القيود المعيّنة في ميزة المراقبة الأبوية إلا على حسابات Windows القياسية.

ويمكن للحسابات الإدارية تجاوز هذه القيود.

إذا كان الحساب يُستخدم بواسطة أحد الوالدين، فحدد **حساب ولي الأمر**.

قم بتعيين **تاريخ ميلاد الطفل** للحساب لتحديد مستوى الوصول وتعيين قواعد الوصول لصفحات الويب الملائمة لعمره.

تسجيل الخطورة

يحفظ ESET Internet Security جميع الأحداث المهمة في ملف سجل يمكن عرضه مباشرة من القائمة الرئيسية.الأدوات انقر فوق **الأدوات** > **ملفات السجل** ثم حدد **الرقابة الأبوية** من القائمة المنسدلة **السجل**.

- **التشخيص** ـ لتسجيل معلومات مطلوبة لضبط البرنامج.
- **المعلومات** ـ تسجل الرسائل الإخبارية، بما في ذلك الاستثناءات المسموح بها والمحظورة، إلى جانب جميع السجلات أعلاه.
- **التحذيرات** ـ لتسجيل رسائل الخطأ والتحذير الحرجة.
- **لا شيء** ـ لن يتم تسجيل أي سجلات.

الاستثناءات

يمكن أن يؤدي إنشاء أي استثناء إلى السماح بوصول مستخدم إلى مواقع ويب غير مُدرجة بقائمة الاستثناءات أو رفض هذا الوصول. وهذا الإجراء مفيد إذا أردت التحكم في الوصول إلى مواقع محددة بدلاً من استخدام الفئات. يمكن نسخ الاستثناءات المُنشأة لأحد الحسابات واستخدامها لحساب آخر. يمكنك أن تستفيد من هذه الميزة إذا أردت إنشاء قواعد متطابقة للأطفال الذين ينتمون لفئة عمرية واحدة.

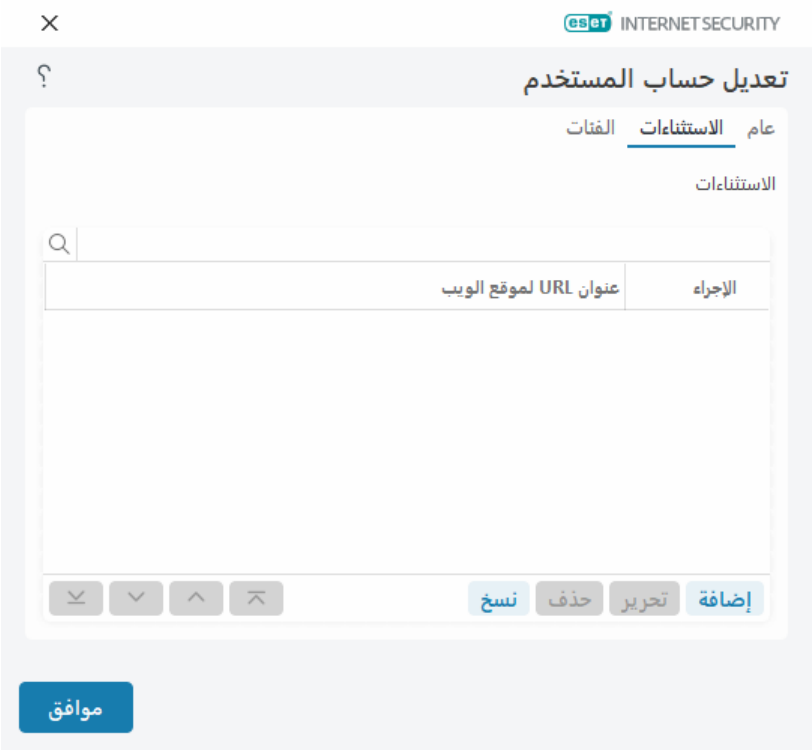
انقر فوق **إضافة** لإنشاء استثناء جديد. حدد **الإجراء** (على سبيل المثال، **حظر**) وباستخدام القائمة المنسدلة، اكتب **عنوان URL لموقع الويب** الذي ينطبق هذا الاستثناء عليه، ثم انقر فوق **موافق**. ستتم إضافة الاستثناء إلى قائمة الاستثناءات الموجودة مع عرض حالته.

إضافة – لإنشاء استنثناء جديد.

تحرير – يمكنك تحرير **عنوان URL لموقع الويب** أو **الإجراء** الخاص بالاستثناء المحدد.

حذف – إزالة الاستثناء المحدد.

نسخ – حدد مستخدماً من القائمة المنسدلة التي تريد نسخ الاستثناء الذي تم إنشاؤه منها.

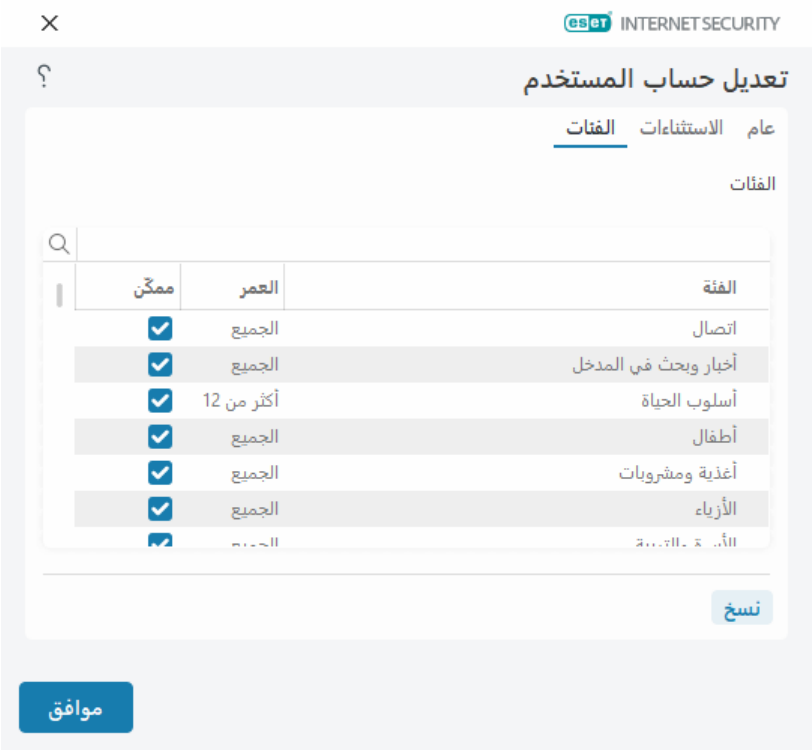


تتجاوز الاستثناءات المحددة الفئات المعينة للحساب (الحسابات) المحدد. على سبيل المثال، إذا كانت فئة الحساب **أخبار** محظورة لكنك حددت صفحة ويب أخبار كاستثناء مسموح به، يمكن حينئذ للحساب الوصول إلى صفحة الويب المسموح بها. ويمكنك عرض أية تغييرات تمت هنا في القسم استثناءات.

الفئات

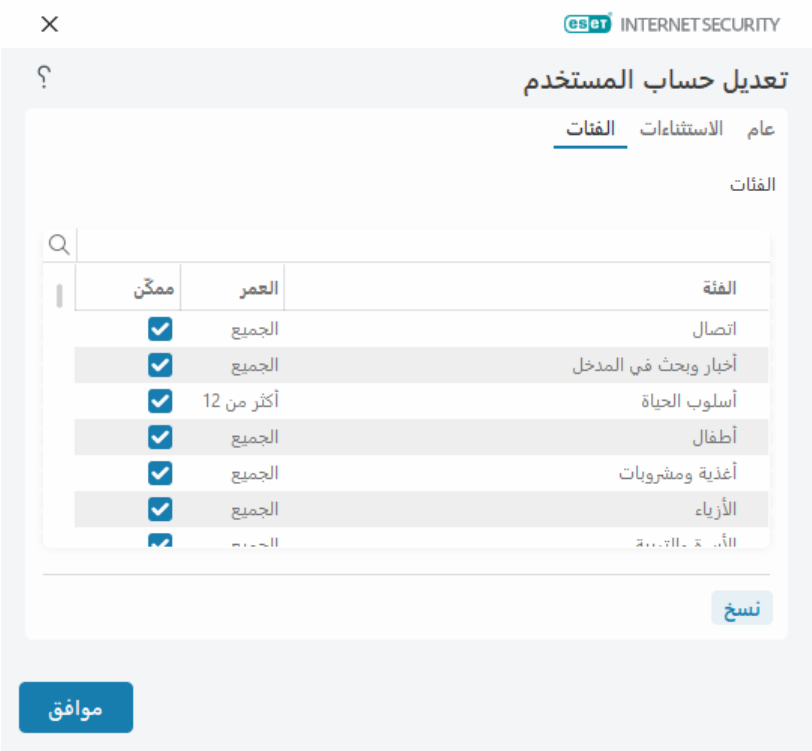
في علامة التبويب **الفئات**، يمكنك تحديد الفئات العامة لمواقع الويب التي تريد حظرها أو السماح بها لكل حساب. قم بإشراك المفتاح الموجود بجوار أي فئة للسماح بها. إذا تركت المفتاح في وضع إيقاف التشغيل، فلن يُسمح بالفئة لهذا الحساب.

نسخ – يتيح لك هذا الإعداد إمكانية نسخ قائمة بالفئات المسموح بها أو المحظورة من حساب معدّل موجود.



الفئات

حدد من خانة الاختيار في العمود **ممكّن** بجوار أي فئة للسماح بها. إذا تركت مربع الاختيار فارغاً، فلن يتم السماح بالفئة لهذا الحساب.



فيما يلي بعض أمثلة الفئات (المجموعات) التي قد لا يكون المستخدمون على علم بها:

- **متنوع** – عناوين IP خاصة (محلية) عادة كشبكة إنترانت، 127.0.0.0/8 و192.168.0.0/16 وغيرهما، وعندما يظهر لديك

الخطأ رقم 403 أو 404، فسيكون موقع ويب ملائماً لهذه الفئة أيضاً. وعندما يظهر لديك الخطأ رقم 403 أو 404، فسيكون موقع ويب ملائماً لهذه الفئة أيضاً.

- **غير محلول** – تتضمن هذه الفئة صفحات ويب التي لم يتم تحليلها لحدوث خطأ عند الاتصال بمحرك قاعدة بيانات المراقبة الأبوية.
- **غير مصنف** – صفحات ويب غير معروفة لم تُضف بعد إلى قاعدة بيانات المراقبة الأبوية.
- **ديناميكي** – صفحات الويب التي تقوم بإعادة التوجيه إلى صفحات أخرى على مواقع الويب.

حماية المتصفح

حماية المتصفح هي طبقة أخرى من الحماية لأمنك وخصوصيتك تحمي ذاكرة المتصفح من الفحص من خلال العمليات الأخرى، وتزيد من الحماية ضد برامج تسجيل ضغطات المفاتيح وتمنع لصق أي بيانات متعلقة بالدفع عبر الإنترنت تم تعديلها بواسطة البرمجيات الخبيثة من الحافظة إلى المتصفح المؤمَّن. لتكوين حماية المتصفح، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية المتصفح** واختر من خيارات التكوين التالية:

- التصفح المصرفي الآمن
- قائمة السماح بحماية المتصفح
- إطار المتصفح

التصفح المصرفي الآمن

يمكنك تكوين التصفح المصرفي الآمن في الإعداد المتقدم > **وسائل الحماية** > **حماية المتصفح** > **التصفح المصرفي الآمنالإعداد المتقدم**.

التصفح المصرفي الآمن

تمكين التصفح المصرفي الآمنـ عند تمكين التصفح المصرفي الآمن، ستبدأ جميع متصفحات الويب المدعومة في الوضع الآمن افتراضياً.

حماية المتصفح

تمكين **تأمين جميع المتصفحات** لبدء كافة متصفحات الويب المدعومة في وضع آمن.

وضع تثبيت الملحق – يمكنك تحديد الملحقات التي سيُسمح بتثبيتها على متصفح مؤمّن من القائمة المنسدلة بواسطة ESET:

- **الملحقات الأساسية** – فقط الملحقات الأكثر أهمية التي طوّرتها شركة مصنعة لمتصفح معين.
- **جميع الملحقات** ـ جميع الملحقات التي يدعمها متصفح معين.

> لا يؤثر تغيير وضع تثبيت الإضافة على ملحقات المتصفح المثبّتة مسبقاً:

المتصفح المؤمَّن

حماية الذاكرة المحسّنة ـ في حال تمكينها، ستتم حماية ذاكرة المتصفح المؤمَّن من الفحص من قبل العمليات الأخرى.

حماية لوحة المفاتيح ـ إذا تم تمكينه، سيتم إخفاء المعلومات التي تدخلها عبر لوحة المفاتيح إلى المتصفح المؤمَّن من التطبيقات الأخرى. يعمل هذا على زيادة الحماية من برامج تسجيل ضغطات المفاتيح.

حماية الحافظةـ في حالة التمكين، سيقوم ESET Internet Security بمنع لصق أي بيانات متعلقة بالدفع عبر الإنترنت تم تعديلها بواسطة البرمجيات الخبيثة من الحافظة إلى المتصفح الآمن. هذا يضمن الحماية من التغييرات المحتملة التي تجريها البرمجيات الضارة.

إطار المتصفح— عليك تخصيص إعدادات العرض لإطار المتصفح في المتصفحات المحمية.

قائمة السماح بحماية المتصفح ـ **إدارة الملفات المضافة إلى قائمة السماح لحماية المتصفح.**

خصوصية وأمان المتصفح

تمكين خصوصية وأمان المتصفحـ في حالة التعطيل، ستتم إزالة تثبيت ملحق خصوصية وأمان المتصفح من جميع المتصفحات المدعومة عبر جميع حسابات Windows.

عرض إعلامات خصوصية وأمان المتصفحـ في حالة التمكين، سيقوم ESET Internet Security بعرض إعلامات خصوصية وأمان المتصفح.

أداة فحص البرنامج النصي للمتصفح

تمكين الفحص المتقدم للبرامج النصية للمتصفحـ في حالة التمكين، ستتحقق أداة فحص الحماية ضد الفيروسات من جميع برامج JavaScript التي تنفذها متصفحات الإنترنت.

00

التحكم في الجهاز

يوفر ESET Internet Security التحكم التلقائي في الأجهزة (CD/DVD/USB/إلخ). تتيح لك هذه الوحدة حظر عوامل التصفية/الأذونات الممتدة أو ضبطها، وتحديد قدرة المستخدمين على الوصول إلى جهاز معين واستخدامه. قد يكون ذلك مفيداً إذا كان مسؤول جهاز الكمبيوتر يريد منع استخدام أجهزة تحتوي على محتوى غير مرغوب فيه.

الأجهزة الخارجية المدعومة:

- جهاز تخزين على القرص (محرك الأقراص الثابت USB والقرص القابل للإزالة)
- القرص المضغوط/قرص DVD
- الطابعة USB
- التخزين FireWire

- الجهاز Bluetooth
- قارئ البطاقة الذكية
- جهاز التصوير
- المودم
- المنفذ LPT/COM
- الجهاز المحمول (الأجهزة التي تعمل بالبطارية مثل مشغلات الوسائط والهواتف الذكية وأجهزة التوصيل والتشغيل وغيرها)
- كل أنواع الأجهزة

يمكن تعديل خيارات إعداد التحكم في الجهاز من إعداد متقدم > **وسائل الحماية** > **التحكم فالاجهزة المتصلة**.

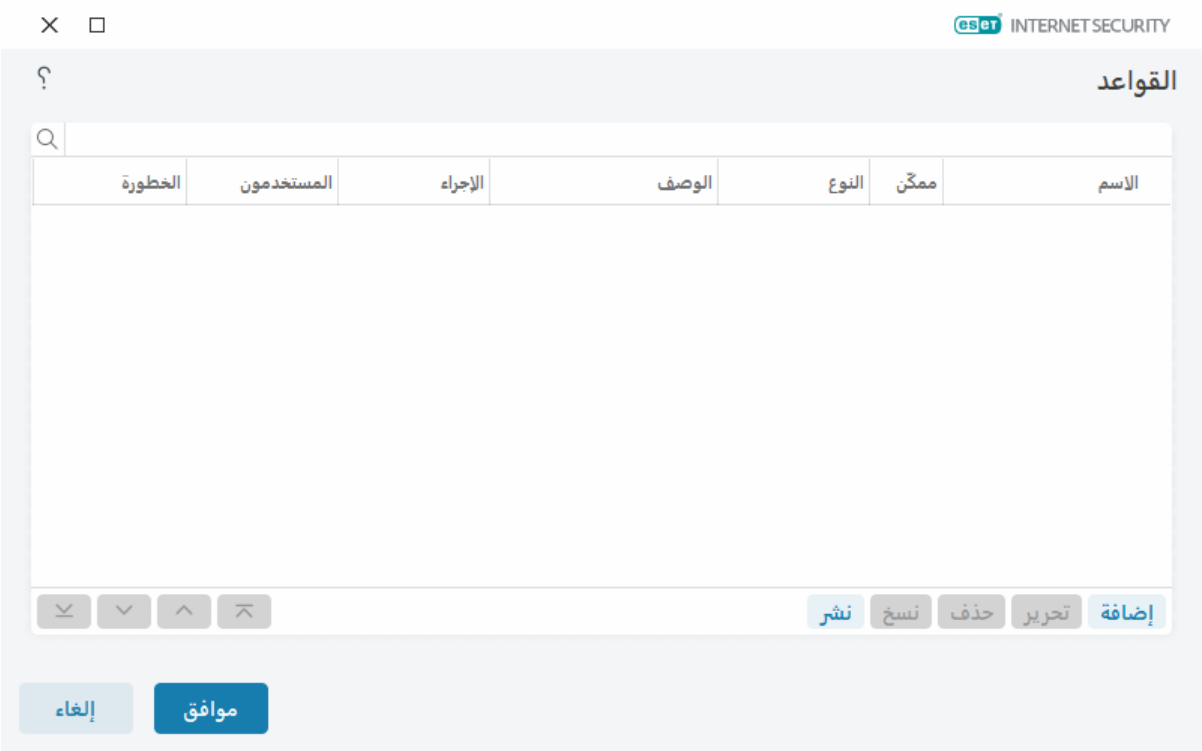
انقر فوق تبديل **تمكين التحكم في الأجهزة** لتمكين ميزة التحكم في الأجهزة في ESET Internet Security يجب إعادة تشغيل الكمبيوتر حتى يصبح هذا التغيير ساري المفعول. بمجرد تمكين التحكم في الأجهزة، يمكنك تحديد **القواعد** في نافذة محرر القواعد.

> يمكنك إنشاء مجموعات مختلفة من الأجهزة يتم تطبيق القواعد المختلفة عليها. كما يمكنك إنشاء مجموعة واحدة الأجهزة التي سيتم فيها تطبيق القاعدة بالإجراء **السماح** أو **منع الكتابة**. من شأن هذا أن يضمن حظر الأجهزة غير المتعرف عليها بواسطة قواعد التحكم في الجهاز عند اتصالها بالكمبيوتر الذي تستخدمه.

في حالة إدخال جهاز محظور بقاعدة موجودة، سيتم عرض نافذة إعلام ولن يتم منح وصول إلى الجهاز.

محرر قواعد التحكم في الجهاز

تعرض نافذة **محرر قواعد التحكم في الجهاز** القواعد الحالية، كما تسمح بالتحكم الدقيق في الأجهزة الخارجية التي يقوم المستخدمون بتوصيلها بالكمبيوتر.



يمكن السماح بأجهزة معينة أو حظرها بواسطة المستخدم أو مجموعة المستخدمين واستناداً إلى أي معلمات إضافية للجهاز يمكن تحديدها في تكوين القاعدة. تحتوي قائمة القواعد على عدة أوصاف للقواعد كالاسم ونوع الجهاز الخارجي والإجراء المطلوب اتخاذه بعد توصيل جهاز خارجي بجهاز الكمبيوتر وخطورة السجل. راجع أيضاً إضافة قواعد الأجهزة الملحقة.

انقر فوق **إضافة** أو **تحرير** لإدارة قاعدة. يتم عرض سلاسل XML عند النقر فوق قاعدة يمكن **نسخها** إلى الحافظة لمساعدة مسؤولي النظام على تصدير/استيراد هذه البيانات واستخدامها، على سبيل المثال في .

بالضغط على **Ctrl** والنقر، يمكنك تحديد قواعد متعددة وتطبيق الإجراءات، مثل حذفها أو تحريكها للأعلى أو للأسفل في القائمة، على جميع القواعد المحددة. يعمل مربع الاختيار **ممكّن** على تعطيل قاعدة معينة أو تمكينها؛ وقد يكون ذلك مفيداً إذا كنت تريد الاحتفاظ بالقاعدة.

انقر فوق **نشر** لنشر معلمات جهاز الوسائل القابلة للإزالة للأجهزة المتصلة بالكمبيوتر تلقائياً.

يتم إدراج القواعد بترتيب الأولوية، وتكون القواعد ذات الأولوية العليا بالقرب من الأعلى. يمكن نقل القواعد بالنقر فوق **للأعلى/لأعلى/لأسفل/للأسفل** ويمكن نقلها فرادى أو في مجموعات.

يمكن عرض إدخالات السجل في نافذة البرنامج الرئيسية > **الأدوات** > ملفات السجل.

يقومسجل التحكم بملحقات الأجهزة بتسجيل كل حالات تشغيل مكون التحكم بملحقات الأجهزة.

الأجهزة التي تم اكتشافها

يوفر زر **نشر** نظرة عامة على جميع الأجهزة المتصلة حالياً مع معلومات حول: نوع الجهاز، حول مورد الجهاز، والطراز والرقم التسلسلي (إن وُجد). إذا كنت تريد رؤية جميع الأجهزة المخفية، فحدد **إظهار الأجهزة المخفية**.

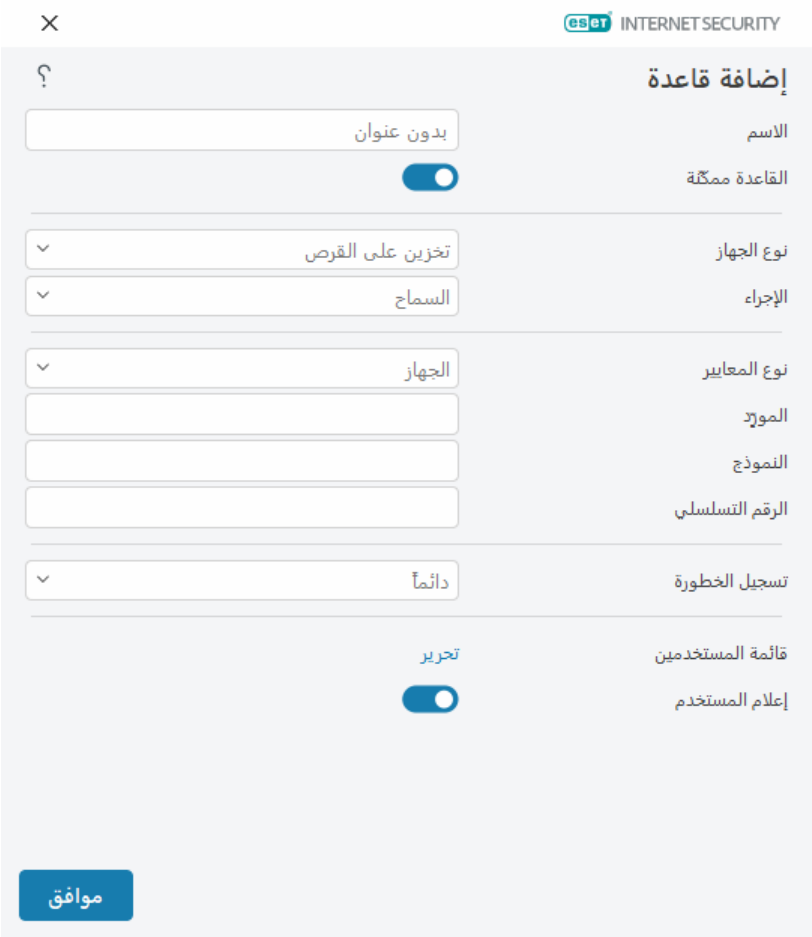
حدد جهازاً من قائمة الأجهزة التي تم اكتشافها وانقر فوق **موافق** لإضافة قاعدة تحكم في الجهاز بمعلومات محددة مسبقاً (يمكن ضبط جميع الإعدادات).

يتم تمييز الأجهزة في وضع الطاقة المنخفضة (السكون) برمز تحذير . لتمكين زر **موافق** وإضافة قاعدة لهذا الجهاز:

- أعِد توصيل الجهاز
- استخدم الجهاز (على سبيل المثال، ابدأ تشغيل تطبيق الكاميرا في Windows لإيقاظ كاميرا الويب)

إضافة قواعد التحكم في الجهاز

تحدد قاعدة التحكم بملحقات الأجهزة الإجراء الذي سيُتخذ عند توصيل جهاز يفي بمعيار جهاز الكمبيوتر.



أدخل وصفاً للقاعدة في حقل **الاسم** لتعريفه بشكل أفضل. انقر فوق شريط التمرير بجوار **القاعدة ممكّنة** لتعطيل هذه القاعدة أو تمكينها، ويمكن أن يكون ذلك مفيداً إذا كنت لا تريد حذف القاعدة بشكل دائم.

نوع الجهاز

اختر نوع الجهاز الخارجي من القائمة المنسدلة (تخزين على القرص/جهاز محمول/Bluetooth/FireWire/...). يتم تجميع معلومات نوع الجهاز من نظام التشغيل ويمكن رؤيتها في إدارة الأجهزة بالنظام إذا كان الجهاز متصلاً بالكمبيوتر. تشمل أجهزة التخزين مخاطر خارجية أو أجهزة قراءة بطاقات الذاكرة المألوفة التي يتم توصيلها عبر USB أو FireWire. تشمل أجهزة قراءة البطاقات الذكية جميع أجهزة قراءة البطاقات الذكية المزودة بدائرة متكاملة مدمجة، كبطاقات SIM أو بطاقات المصادقة. من أمثلة أجهزة التصوير الماسحات الضوئية أو الكاميرات. ولأن هذه الأجهزة توفر معلومات عن الإجراءات الخاصة بها فقط ولا توفر أي معلومات عن المستخدمين، فلا يمكن حظرها إلا بشكل عمومي.

الإجراء

يمكن السماح بالوصول إلى الأجهزة غير الخاصة بالتخزين أو حظرها فقط. وفي المقابل، تسمح لك قواعد أجهزة التخزين بتحديد أحد إعدادات الحقوق التالية:

- **يسمح** – سيتم السماح بوصول كامل إلى الجهاز.
- **حظر** – سيتم حظر الوصول إلى الجهاز.
- **منع الكتابة** – سيتم السماح بوصول قراءة فقط إلى الجهاز.
- **تحذير** – في كل مرة يتم فيها توصيل جهاز، يتم إعلام المستخدم بما إذا كان الجهاز مسموحاً/محظوراً، ويتم إنشاء إدخال

بالسجل. جدير بالذكر أن الأجهزة لا يتم تذكرها، وسيتم عرض الإعلام باستمرار عند توصيل نفس الجهاز عدة مرات متتابعة.

الرجاء ملاحظة أنه ليست جميع الإجراءات (الأذونات) متوفرة لجميع أنواع الأجهزة. فإذا كان أحد أجهزة التخزين، فستتوفر الإجراءات الأربعة جميعاً. بالنسبة للأجهزة غير الخاصة بالتخزين، تتوفر ثلاثة إجراءات فقط (مثلا، لا يتوفر **منع الكتابة** مع Bluetooth لذلك يمكن السماح بأجهزة Bluetooth أو حظرها أو التحذير بها فقط).

نوع المعايير

ـ حدد **مجموعات الأجهزة** أو **الجهاز**.

يمكن استخدام المعلمات الإضافية الموضحة أدناه لضبط القواعد للأجهزة المختلفة. جميع المعلمات حساسة لحالة الأحرف وتدعم أحرف البدل (*،؟):

- **المورِّد** ـ التصفية حسب اسم أو معرف المورِّد.
- **النموذج** ـ الاسم المحدد للجهاز.
- **الرقم التسلسلي** ـ الأجهزة الخارجية لها عادةً أرقام تسلسلية خاصة بها. في حالة كون تلك الأجهزة CD/DVD يكون هذا الرقم التسلسلي للوسائط المحددة، وليس لمحرك الأقراص CD.

في حالة عدم تعريف هذه المعلمات، ستتجاهل القاعدة هذه الحقول أثناء المطابقة. معلمات التصفية في جميع الحقول النصية حساسة لحالة الأحرف وتدعم أحرف البدل (تمثل علامة الاستفهام (؟) حرفاً واحداً، بينما تمثل العلامة النجمية (*) سلسلة من صفر أو حرف أو أكثر).

لعرض معلومات عن الجهاز، قم بتكوين قاعدة لنوع الجهاز هذا، ووصّل الجهاز بالكمبيوتر، بعد ذلك اطلع على تفاصيل الجهاز في سجل التحكم في الجهاز.

تسجيل الخطورة

يحفظ ESET Internet Security جميع الأحداث المهمة في ملف سجل يمكن عرضه مباشرة من القائمة الرئيسية.الأدوات انقر فوق **الأدوات** > **ملفات السجل** ثم حدد **التحكم في الجهاز** من القائمة المنسدلة **سجل**.

- **دائماً** ـ لتسجيل جميع الأحداث.
- **التشخيص** ـ لتسجيل معلومات مطلوبة لضبط البرنامج.
- **إخباري** ـ لتسجيل رسائل معلوماتية، تشمل رسائل التحديث الناجح، إضافة إلى جميع السجلات الواردة أعلاه.
- **التحذيرات** ـ لتسجيل رسائل الخطأ والتحذير الحرجة.
- **لا شيء** ـ لن يتم تسجيل أي سجلات.

قائمة المستخدمين

يمكن تقييد القواعد على مستخدمين معينين أو مجموعات مستخدمين معينة بإضافتهم إلى قائمة المستخدمين بالنقر فوق **تحرير** بجوار **قائمة المستخدمين**.

- **إضافة** ـ فتح نافذة حوار **أنواع الكائنات: مستخدمون أو مجموعات** التي تتيح لك تحديد المستخدمين المطلوبين.

- **إزالة** ـ لإزالة المستخدم المحدد من عامل التصفية.

> **قيود قائمة المستخدمين**
> لا يمكن تعريف قائمة المستخدمين للقواعد ذات أنواع الأجهزةالمحددة:
> - طابعة USB
> - جهاز Bluetooth
> - قارئ البطاقة الذكية
> - جهاز التصوير
> - المودم
> - منفذ COM/LPT

إعلام المستخدم – في حالة إدخال جهاز محظور بقاعدة موجودة، فسيتم عرض نافذة إعلام.

مجموعات الأجهزة

> قد يشكل الجهاز المتصل بالكمبيوتر الذي تستخدمه خطراً على أمان النظام.

تنقسم نافذة "مجموعات الأجهزة" إلى جزأين. يحتوي الجزء الأيسر من النافذة على قائمة بالأجهزة التي تنتمي إلى المجموعة ذات الصلة، بينما يحتوي الجانب الأيمن من النافذة على المجموعات التي تم إنشاؤها. حدد مجموعة لعرض الأجهزة في الجزء الأيسر.

عند فتح نافذة مجموعات الأجهزة وتحديد مجموعة، يمكنك إضافة الأجهزة إلى القائمة أو إزالتها منها. توجد طريقة أخرى لإضافة الأجهزة إلى المجموعة وذلك عبر استيرادها من ملف. أو بدلاً من ذلك، يمكنك النقر فوق زر **نشر** وسيتم عرض كل الأجهزة المتصلة بالكمبيوتر في نافذة **الأجهزة التي تم اكتشافها**. حدد الأجهزة من القائمة التي تم نشرها لإضافتها إلى المجموعة بالنقر فوق **موافق**.

عناصر التحكم

إضافة — يمكنك إضافة مجموعة بكتابة اسمها أو جهاز إلى مجموعة موجودة، استناداً إلى أي جزء من النافذة قمت بالنقر فوق الزر.

تحرير ـ يتيح لك تعديل اسم المجموعة المحددة أو معلمات الجهاز (المورّد، الطراز، الرقم التسلسلي).

حذف ـ حذف المجموعة المحددة أو الجهاز المحدد تبعاً لجزء النافذة الذي نقرت فيه فوق الزر.

استيراد ـ استيراد قائمة بالأجهزة من ملف نصي. يتطلب استيراد الأجهزة من ملف نصي تنسيقاً صحيحاً:

- تشغيل كل جهاز في سطر جديد.
- يجب أن يكون**المورِّد** و**الطراز** و**الرقم التسلسلي** موجودة لكل جهاز ويفصل بينها بفاصلة.

> نقدم لك هنا مثالاً على محتوى الملف النصي:
> ```
> Kingston,DT 101 G2,001CCE0DGRFC0371
> 04081-0009432,USB2.0 HD WebCam,20090101
> ```

تصدير ـ تصدير قائمة بالأجهزة إلى ملف.

يوفر زر **نشر** نظرة عامة على جميع الأجهزة المتصلة حالياً مع معلومات حول: نوع الجهاز، حول مورد الجهاز، والطراز والرقم التسلسلي (إن وُجد).

إضافة جهاز

انقر فوق **إضافة** في النافذة اليمنى لإضافة جهاز إلى مجموعة موجودة. يمكن استخدام المعلمات الإضافية الموضحة أدناه لضبط القواعد للأجهزة المختلفة. جميع المعلمات حساسة لحالة الأحرف وتدعم أحرف البدل (*،؟):

- **المورِّد** – التصفية بحسب الاسم أو ID.
- **النموذج** – الاسم المحدد للجهاز.
- **الرقم التسلسلي** – الأجهزة الخارجية لها عادةً أرقام تسلسلية خاصة بها. في حالة كون تلك الأجهزة CD/DVD يكون هذا الرقم التسلسلي للوسائط المحددة، وليس لمحرك الأقراص CD.
- **الوصف**—وصفك للجهاز من أجل تنظيم أفضل.

> في حالة عدم تعريف هذه المعلمات، ستتجاهل القاعدة هذه الحقول أثناء المطابقة. تعد معلمات التصفية في جميع حقول النص حساسة لحالة الأحرف وتدعم أحرف البدل (علامة الاستفهام [؟] تمثل حرفاً واحداً، بينما تمثل العلامة النجمية [*] سلسلة من الأصفار أو حرف أو أكثر).

انقر فوق **موافق** لحفظ التغييرات. انقر فوق **إلغاء** لمغادرة نافذة **مجموعات الأجهزة** دون حفظ التغييرات.

> بعد إنشاء مجموعة أجهزة، يجب إضافة قاعدة التحكم بملحقات الأجهزة لمجموعة الأجهزة التي تم إنشاؤها واختيار الإجراء الذي تريد اتخاذه.

الرجاء ملاحظة أنه ليست جميع الإجراءات (الأذونات) متوفرة لجميع أنواع الأجهزة. إذا كان جهاز من نوع التخزين، فستتوفر الإجراءات الأربعة جميعاً. بالنسبة للأجهزة غير الخاصة بالتخزين، تتوفر ثلاثة إجراءات فقط (مثلا، لا يتوفر **منع الكتابة** لـ Bluetooth لذلك يمكن السماح بأجهزة Bluetooth أو حظرها أو التحذير بها فقط).

حماية الكاميرا

تعلمك **حماية الكاميرا** بالعمليات والتطبيقات التي تقوم بالوصول إلى كاميرا الويب بجهاز الكمبيوتر. عندما يحاول أحد التطبيقات الوصول إلى الكاميرا، تحصل على إعلام حيث يمكنك **السماح** أو **حظر** الوصول. يعتمد لون نافذة التنبيه على سمعة التطبيق.

يمكن تعديل خيارات إعداد حماية كاميرا الويب في الإعداد المتقدم > **وسائل الحماية** > **التحكم في الجهاز** > **حماية كاميرا الويب**.

لتنشيط ميزة حماية كاميرا الويب في ESET Internet Security قم بتمكين مفتاح التبديل بجوار **تمكين حماية كاميرا الويب**.

عند تمكين حماية الكاميرا، تصبح **القواعد** نشطة، مما يسمح لك بفتح نافذة محرر القواعد.

لإيقاف تشغيل التنبيهات للتطبيقات ذات قاعدة حالية تم تعديلها ولكن لا يزال لها توقيع رقمي صالح (على سبيل المثال، تحديث تطبيق)، قم بتمكين شريط التمرير بجوار **تعطيل تنبيهات الوصول إلى الكاميرا للتطبيقات المعدلة**.

محرر قواعد حماية كاميرا الويب

تعرض هذه النافذة القواعد الموجودة كما تسمح بالتحكم في التطبيقات والعمليات التي لها تصل إلى كاميرا ويب جهاز الكمبيوتر بناءً على الإجراء الذي اتخذته.

تتوفر الإجراءات التالية:

- **السماح بالوصول**
- **حظر الوصول**
- **السؤال** (يسأل المستخدم في كل مرة يحاول فيها أحد التطبيقات الوصول إلى كاميرا الويب)

قم بإلغاء تحديد خانة الاختيار في عمود "**إعلام**" لإيقاف تلقي الإعلامات عند وصول أحد التطبيقات إلى كاميرا الويب.

إرشادات موضحة
كيفية إنشاء قواعد كاميرا الويب وتحريرها في ESET Internet Security.

ThreatSense

ThreatSense عبارة عن العديد من أساليب اكتشاف التهديدات المعقدة. وتتميز هذه التقنية بأنها استباقية، ما يعني أنها توفر الحماية أيضاً خلال الانتشار المبكر لتهديد جديد. كما تستخدم توليفة مكونة من تحليل التعليمات البرمجية ومحاكاة التعليمات البرمجية والتوقيعات العامة وتوقيعات الفيروسات، وتعمل هذه التوليفة في تناغم لتعزيز حماية النظام بدرجة كبيرة. ويستطيع محرك الفحص التحكم في العديد من تدفقات البيانات بالتزامن، مما يرفع من الكفاءة ومعدل الاكتشاف. كما أن تقنية ThreatSense تستطيع التخلص من برامج الاحتيال نهائياً.

تتيح لك خيارات إعداد محرك ThreatSense تحديد العديد من معلمات الفحص كما يلي:

- أنواع وامتدادات الملفات المطلوب فحصها
- توليفة أساليب الاكتشاف المتنوعة
- مستويات المسح، إلخ.

للدخول في نافذة الإعداد، انقر فوق**ThreatSense** في الإعداد المتقدم لأي وحدة نمطية تستخدم تقنية ThreatSense (انظر أدناه). جدير بالذكر أن خيارات الأمان المختلفة تتطلب تكوينات مختلفة. فمع وضع ذلك في الاعتبار، فإن ThreatSense قابل للتكوين لكل وحدة حماية مما يلي على حدة:

- الحماية في الوقت الفعلي لنظام الملفات
- فحص حالة الخمول
- الفحص عند بدء التشغيل
- حماية المستندات
- حماية عميل البريد الإلكتروني
- حماية الوصول إلى الويب
- فحص الكمبيوتر

معلمات ThreatSense محسنة إلى حد كبير لكل وحدة، وقد يتسبب تعديلها في التأثير على تشغيل النظام بدرجة كبيرة. على سبيل المثال، فإن تغيير المعلمات لفحص أدوات حزم وقت التشغيل، أو تمكين الأساليب البحثية المتقدمة في وحدة حماية نظام الملفات في الوقت الفعلي، قد يتسبب في إبطاء النظام (عادةً ما يتم فحص الملفات المنشأة حديثاً باستخدام هذه الأساليب). لذا يوصى بترك معلمات ThreatSense الافتراضية دون تغيير لكل الوحدات عدا فحص الكمبيوتر.

الكائنات المطلوب فحصها

يتيح هذا القسم تعريف مكونات وملفات الكمبيوتر التي سيتم فحصها بحثاً عن حالات تسلل.

ذاكرة التشغيل – للفحص بحثاً عن التهديدات التي تهاجم ذاكرة التشغيل في النظام.

تشغيل القطاعات/UEFI – يفحص قطاعات التشغيل بحثاً عن وجود برامج ضارة في سجل التشغيل الرئيسي. اقرأ المزيد عن UEFI في المسرد.

ملفات البريد الإلكتروني – يدعم البرنامج الامتدادات التالية: DBX (Outlook Express) وEML.

ملفات البريد الإلكتروني – يدعم البرنامج الامتدادات التالية: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE والعديد من البرامج الأخرى.

الأرشيفات ذاتية الاستخراج – الأرشيفات ذاتية الاستخراج (SFX) عبارة عن أرشيفات يمكنها الاستخراج ذاتياً.

أدوات حزم وقت التشغيل – بعد التنفيذ، يتم فك ضغط أدوات حزم وقت التشغيل (بخلاف أنواع الأرشيفات القياسية) في الذاكرة. إضافة إلى أدوات الحزم الثابتة القياسية (UPX, yoda, ASPack, FSG إلخ)، يستطيع برنامج الفحص التعرف على العديد من الأنواع الإضافية لأدوات الحزم من خلال استخدام محاكاة التعليمات البرمجية.

خيارات الفحص

حدد الأساليب التي يتم استخدامها عند فحص النظام للبحث عن حالات تسلل. تتوفر الخيارات التالية:

الأساليب البحثية – الأسلوب البحثي هو خوارزمية تقوم بتحليل نشاط البرامج (الضار). والميزة الأساسية لهذه التقنية هي القدرة على تحديد البرامج الضارة التي لم تكن موجودة أو لم تكن مغطاة بواسطة الإصدارات السابقة للوحدة النمطية لمحرك الكشف. بينما العيب يتمثل في احتمالية (صغيرة جداً) صدور تنبيهات غير حقيقية.

الأساليب البحثية المتقدمة/التوقيعات DNA – تتكون الأساليب البحثية المتقدمة من خوارزمية بحث فريدة قامت شركة ESET بتطويرها وتحسينها لاكتشاف فيروسات الكمبيوتر المتنقلة وأحصنة طروادة والتعليمات البرمجية الضارة المكتوبة بلغات برمجة عالية المستوى. ويساعد استخدام الأساليب البحثية المتقدمة في زيادة إمكانات منتجات ESET لاكتشاف التهديدات بدرجة عالية. كما أن التوقيعات قادرة على اكتشاف الفيروسات والتعرف عليها بشكل يعتمد عليه. جدير بالذكر أنه باستخدام نظام التحديث التلقائي تكون التوقيعات الجديدة متوفرة بعد ساعات قليلة من اكتشاف أي تهديد. غير أن عيب التوقيعات يتمثل في أنها لا تكتشف سوى الفيروسات التي تعرفها (أو الإصدارات المعدلة بشكل بسيط من هذه الفيروسات).

التنظيف

تحدد إعدادات التنظيف سلوك ESET Internet Security أثناء تنظيف الكائنات. هناك 4 مستويات من التنظيف:

يحتوي ThreatSense على مستويات الإصلاح (أي التنظيف) التالية.

الإصلاح في ESET Internet Security

الوصف	مستوى التنظيف
حاول تصحيح الاكتشاف أثناء تنظيف الأشياء دون أي تدخل من المستخدم النهائي. في بعض الحالات النادرة (على سبيل المثال، ملفات النظام)، إذا كان لا يمكن معالجة الاكتشاف، يتم ترك الكائن المبلغ عنه في موقعه الأصلي.	**اكتشاف العلاج دائماً**
حاول إصلاح الاكتشاف أثناء تنظيف الكائنات دون أي تدخل من المستخدم النهائي. في بعض الحالات (على سبيل المثال، ملفات النظام أو الأرشيفات مع كلٍّ من الملفات النظيفة والمصابة بالعدوى)، إذا تعذر إصلاح هذا الاكتشاف، فسيتم ترك الكائن المبلغ عنه في موقعه الأصلي.	**اكتشاف العلاج إذا كان آمناً، والحفاظ عليه بخلاف ذلك**
حاول إصلاح الاكتشاف أثناء تنظيف الكائنات. في بعض الحالات، إذا تعذر تنفيذ أي إجراء، يتلقى المستخدم النهائي تنبيهاً تفاعلياً ويجب عليه تحديد إجراء إصلاح (على سبيل المثال، الحذف أو التجاهل). يوصى بهذا الإعداد في معظم الحالات.	**اكتشاف العلاج إذا كان آمناً، اسأل بخلاف ذلك**
يتلقى المستخدم النهائي نافذة تفاعلية أثناء تنظيف الكائنات ويجب عليه تحديد إجراء إصلاح (على سبيل المثال، حذف أو تجاهل). تم تصميم هذا المستوى للمستخدمين الأكثر تقدماً الذين يعرفون الخطوات التي يجب اتخاذها في حالة الاكتشاف.	**اسأل دائماً المستخدم النهائي**

الاستبعادات

الملحق هو جزء اسم الملف المحدد بنقطة. يحدد الامتداد نوع ملف ومحتواه. يتيح لك هذا القسم من إعداد ThreatSense تحديد أنواع الملفات المراد فحصها.

أخرى

عند تكوين معلمات محرك ThreatSense لعملية فحص جهاز كمبيوتر عند الطلب، تتوفر أيضاً الخيارات التالية في قسم **غير ذلك**:

فحص دفق البيانات البديل (ADS) ـ عمليات دفق البيانات البديلة التي يستخدمها نظام ملفات NTFS عبارة عن ملفات ومجلدات مقترنة لا تكتشفها تقنيات الفحص العادية. ويحاول العديد من حالات التسلل تجنب الاكتشاف بواسطة إخفاء أنفسها كعمليات دفق بيانات بديلة.

تشغيل عمليات الفحص في الخلفية بأولية منخفضة ـ يستهلك كل تسلسل فحص كمية معينة من موارد النظام. فإذا كنت تعمل باستخدام برامج تضع حملاً مرتفعً على موارد النظام، فيمكنك تنشيط الفحص في الخلفية المنخفض الأولوية وتوفير الموارد للتطبيقات التي تستخدمها.

تسجيل جميع الكائنات ـ يعرض سجل الفحص جميع الملفات التي تم فحصها في أرشيفات الاستخراج الذاتي، حتى تلك غير المصابة (قد يقوم بإنشاء الكثير من بيانات سجل الفحص ويزيد من حجم ملف سجل الفحص).

تمكين التحسين الذكي ـ مع تمكين التحسين الذكي، يتم استخدام أفضل الإعدادات لضمان أكثر مستويات الفحص كفاءة، مع الاحتفاظ بأعلى سرعات فحص في الوقت نفسه. تُجري وحدات الحماية المختلفة الفحص بذكاء، مستخدمة مختلف طرق الفحص وتقوم بتطبيقها على أنواع ملفات معينة. في حالة تعطيل التحسين الذكي، يتم تطبيق الإعدادات المحددة بواسطة المستخدم في إعدادات ThreatSense الأساسية للوحدات المعينة عند إجراء فحص.

المحافظة على الطابع الزمني للوصول الأخير ـ حدد هذا الخيار للحفاظ على وقت الوصول الأصلي للملفات التي تم فحصها بدلاً من تحديثها (على سبيل المثال، للاستخدام مع أنظمة النسخ الاحتياطي للبيانات).

الحدود

يتيح قسم "الحدود" تحديد الحد الأقصى لحجم الكائنات ومستويات الأرشيفات المتشابكة المطلوب فحصها:

إعدادات الكائنات

أقصى حجم للكائن – تحديد أقصى حجم للكائنات المطلوب فحصها. وبالتالي ستقوم وحدة الحماية ضد الفيروسات المحددة بفحص الكائنات الصغرى عن الحجم المحدد فقط. ويجب عدم تغيير هذا الخيار إلا بواسطة المستخدمين المتقدمين الذين لديهم أسباب محددة لاستبعاد الكائنات الكبرى من الفحص. القيمة الافتراضية: غير محدودة.

أقصى وقت فحص للكائن (بالثانية) – لتحديد الحد الأقصى لقيمة الوقت لفحص الملفات في كائن حاوية (مثل أرشيف RAR/ZIP أو رسالة بريد إلكتروني تحتوي على مرفقات متعددة). لا ينطبق هذا الإعداد على الملفات المستقلة. إذا تم إدخال قيمة معرفة من قبل المستخدم وانقضى ذلك الوقت، فسيتوقف الفحص في أقرب وقت ممكن، بغض النظر عما إذا كان الفحص لكل ملف في كائن حاوية قد انتهى.
في حالة وجود أرشيف يحتوي على ملفات كبيرة، لن يتوقف الفحص قبل استخراج ملف من الأرشيف (على سبيل المثال، عندما يكون المتغير المحدد من قبل المستخدم هو 3 ثوانٍ، ولكن استخراج الملف يستغرق 5 ثوانٍ). لن يتم فحص بقية الملفات الموجودة في الأرشيف عند انقضاء ذلك الوقت.
للحد من وقت الفحص، بما في ذلك الأرشيفات الأكبر حجماً، استخدم **الحد الأقصى لحجم الكائن** و**الحجم الأقصى للملف في الأرشيف** (غير مستحسن بسبب المخاطر الأمنية المحتملة).
القيمة الافتراضية: غير محدودة.

إعداد فحص الأرشيفات

مستوى تداخل الأرشيف – تحديد أقصى عمق لفحص الأرشيف. القيمة الافتراضية: 10.

أقصى حجم للملف في الأرشيف – يسمح لك هذا الخيار بتحديد أقصى حجم ملف للملفات الموجودة في الأرشيفات (عند استخراجها) المطلوب فحصها. الحد الأقصى للقيمة **3 جيجابايت**.

> i يوصى بعدم تغيير القيم الافتراضية؛ ففي ظل الظروف العادية يفترض عدم وجود أي سبب لتعديلها.

مستويات التنظيف

لتغيير إعدادات مستوى التنظيف لوحدة الحماية المطلوبة، قم بتوسيع **ThreatSense**(على سبيل المثال، **حماية نظام الملفات في الوقت الفعلي**) ثم اختر **مستوى التنظيف** من القائمة المنسدلة.

يحتوي ThreatSense على مستويات الإصلاح (أي التنظيف) التالية.

الإصلاح في ESET Internet Security

الوصف	مستوى التنظيف
حاول تصحيح الاكتشاف أثناء تنظيف الأشياء دون أي تدخل من المستخدم النهائي. في بعض الحالات النادرة (على سبيل المثال، ملفات النظام)، إذا كان لا يمكن معالجة الاكتشاف، يتم ترك الكائن المبلغ عنه في موقعه الأصلي.	**اكتشاف العلاج دائماً**
حاول إصلاح الاكتشاف أثناء تنظيف الكائنات دون أي تدخل من المستخدم النهائي. في بعض الحالات (على سبيل المثال، ملفات النظام أو الأرشيفات مع كلٍّ من الملفات النظيفة والمصابة بالعدوى)، إذا تعذر إصلاح هذا الاكتشاف، فسيتم ترك الكائن المبلغ عنه في موقعه الأصلي.	**اكتشاف العلاج إذا كان آمناً، والحفاظ عليه بخلاف ذلك**
حاول إصلاح الاكتشاف أثناء تنظيف الكائنات. في بعض الحالات، إذا تعذر تنفيذ أي إجراء، يتلقى المستخدم النهائي تنبيهاً تفاعلياً ويجب عليه تحديد إجراء إصلاح (على سبيل المثال، الحذف أو التجاهل). يوصى بهذا الإعداد في معظم الحالات.	**اكتشاف العلاج إذا كان آمناً، اسأل بخلاف ذلك**
يتلقى المستخدم النهائي نافذة تفاعلية أثناء تنظيف الكائنات ويجب عليه تحديد إجراء إصلاح (على سبيل المثال، حذف أو تجاهل). تم تصميم هذا المستوى للمستخدمين الأكثر تقدماً الذين يعرفون الخطوات التي يجب اتخاذها في حالة الاكتشاف.	**اسأل دائماً المستخدم النهائي**

قائمة العناوين المستبعدة من الفحص

تعد ملحقات الملفات المستبعدة جزءاً من ThreatSense. لتهيئة ملحقات الملفات المستبعدة، انقر فوق **ThreatSense** في الإعداد المتقدم لأي وحدة نمطية تستخدم تقنية ThreatSense.

الامتداد هو جزء اسم الملف المحدد بنقطة. يحدد الامتداد نوع ملف ومحتواه. يتيح لك هذا القسم من إعداد ThreatSense تحديد أنواع الملفات المراد فحصها.

لا تخلط بين استثناءات العمليات, أو استثناءات HIPS أو استثناءات الملف/المجلد.

يتم افتراضياً فحص جميع الملفات. ويمكن إضافة امتداد إلى قائمة الملفات المستبعدة من الفحص.

يكون استبعاد ملف ضرورياً أحياناً إذا كان استبعاد أنواع ملفات معينة يمنع البرنامج الذي يستخدم امتدادات معينة من العمل بشكل سليم. على سبيل المثال، يمكن أن يوصى باستبعاد امتدادات `edb.` و`eml.` و`tmp.` عند استخدام خوادم Microsoft Exchange.

لإضافة استثناء جديد إلى القائمة، انقر فوق **إضافة**. اكتب الاستثناء في الحقل الفارغ على سبيل المثال (tmp) وانقر فوق **موافق**. عند تحديد **إدخال قيم متعددة**، يمكنك إضافة عدة امتدادات ملفات محددة بأسطر أو فاصلات أو فاصلات منقوطة (على سبيل المثال، اختر **فاصلة منقوطة** من القائمة المنسدلة كفاصل واكتب `edb;eml;tmp`).
يمكنك استخدام رمز خاص ؟ (علامة استفهام). تمثل علامة الاستفهام أي رمز (على سبيل المثال `db?`).

لمشاهدة الامتداد الدقيق (إن وجد) للملف في نظام تشغيل Windows يجب عليك تحديد خانة اختيار **امتدادات أسماء الملفات** في **View** > **Windows Explorer** (علامة تبويب).

معلمات ThreatSense الإضافية

لتحرير هذه الإعدادات، افتح الإعداد المتقدم > **وسائل الحماية** > **حماية نظام الملفات في الوقت الفعلي** > **المعلمات الإضافية ThreatSense**.

معلمات ThreatSense الإضافية للملفات المنشأة والمعدلة حديثاً

تعد احتمالية الإصابة في الملفات المنشأة حديثاً أو المعدَّلة أكبر نسبياً منها في الملفات الموجودة. لهذا السبب، يفحص البرنامج هذه الملفات بمعلمات فحص إضافية. يستخدم ESET Internet Security الاستدلال المتقدم، القادر على كشف التهديدات الجديدة قبل إصدار تحديث محرك الكشف بالاشتراك مع أساليب الفحص القائمة على التوقيعات.

بالإضافة إلى الملفات المنشأة حديثاً، يتم إجراء الفحص على **الأرشيفات ذاتية الاستخراج** (.sfx) و**أدوات حزم وقت التشغيل**

(الملفات التنفيذية المضغوطة داخلياً). افتراضياً، يتم فحص الأرشيفات حتى مستوى التداخل العاشر ويتم فحصها بصرف النظر عن حجمها الفعلي. لتعديل إعدادات فحص الأرشيف، قم بإلغاء تحديد **إعدادات فحص الأرشيفات الافتراضية**.

معلمات ThreatSense الإضافية للملفات المُنفذة

الاستدلال المتقدم في تنفيذ الملف – بشكل افتراضي، يُستخدم الاستدلال المتقدم عند تنفيذ الملفات. عند تمكين هذا الإعداد، نوصى بشدة بالإبقاء على تمكين التحسين الذكي وESET LiveGrid® لتخفيف التأثير على أداء النظام.

الأساليب البحثية المتقدمة عند تنفيذ الملفات من الوسائط القابلة للإزالة – تعمل الأساليب البحثية المتقدمة على تقليد الرمز في بيئة افتراضية وتقييم سلوكه قبل السماح له بالعمل من وسائط قابلة للإزالة.

الأدوات

يمكنك تكوين الإعدادات المتقدمة للميزات التي توفر أماناً إضافياً وتساعد في تبسيط ESET Internet Security الإدارة في الإعداد المتقدم > **الأدوات**.

- تحديث Microsoft Windows®
- ESET CMD
- ملفات السجل
- وضع الألعاب
- التشخيصات

تحديث Microsoft Windows®

تعد ميزة Windows Update مكوناً مهماً لحماية المستخدمين من البرامج الضارة. لهذا السبب، من الضروري للغاية تثبيت تحديثات Microsoft Windows بمجرد توفرها. يُعلمك ESET Internet Security حول التحديثات غير الموجودة حسب المستوى الذي تحدده في الإعداد المتقدم > **الأدوات**. يتتوفر المستويات التالية:

- **بدون تحديثات** – لن يتم عرض تنزيل أي تحديثات للنظام.
- **تحديثات اختيارية** – سيتم عرض تنزيل التحديثات المميزة بعلامة أولوية منخفضة والأولويات الأعلى.
- **تحديثات مستحسنة** – سيتم عرض تنزيل التحديثات المميزة بعلامة شائعة والمستويات الأعلى.
- **تحديثات مهمة** – سيتم عرض تنزيل التحديثات المميزة بعلامة مهمة والمستويات الأعلى.
- **تحديثات حرجة** – سيتم عرض تنزيل التحديثات الحرجة فقط.

نافذة الحوار – تحديثات النظام

في حالة وجود تحديثات لنظام التشغيل الخاص بك، يعرض ESET Internet Security إعلاماً في نافذة البرنامج الرئيسية > **نظرة عامة**. انقر فوق **المزيد من المعلومات** لفتح نافذة تحديثات النظام.

تعرض نافذة "تحديثات النظام" قائمة بالتحديثات المتوفرة، والجاهزة للتنزيل والتثبيت. كما يُعرض نوع التحديث بجوار اسم التحديث.

انقر نقراً مزدوجاً فوق أي صف تحديث لعرض نافذة معلومات التحديث مع المعلومات الإضافية.

انقر فوق **تشغيل تحديث النظام** لتنزيل كافة تحديثات نظام التشغيل المدرجة وتثبيتها.

معلومات التحديث

تعرض نافذة "تحديثات النظام" قائمة بالتحديثات المتوفرة، والجاهزة للتنزيل والتثبيت. كما يُعرض مستوى أولوية التحديث بجوار اسم التحديث.

انقر فوق **تشغيل تحديث النظام** لبدء تنزيل تحديثات نظام التشغيل وتثبيتها.

انقر بزر الماوس الأيمن فوق أي صف تحديث وفوق **إظهار المعلومات** لعرض نافذة جديدة بمعلومات إضافية.

ESET CMD

هذه ميزة تعمل على تمكين أوامر ecmd المتقدمة. حيث يسمح لك بتصدير أو استيراد الإعدادات باستخدام سطر الأوامر (ecmd.exe). حتى الآن، من الممكن تصدير الإعدادات واستيرادها باستخدام GUI فقط. ESET Internet Security يُمكن تصدير التكوين إلى ملف *.xml*.

عندما تقوم بتمكين ESET CMD فهناك طريقتان متوفرتان مسموح بهما:

- **لا يوجد** – لا يوجد تصريح. لا نوصي باتباع هذه الطريقة لأنها تسمح باستيراد أي تكوين غير موقّع وهذا يمثل خطراً محتملاً.
- **كلمة مرور الإعداد المتقدم** – كلمة مرور مطلوبة لاستيراد تكوين من ملف .xml يجب توقيع هذا الملف (راجع توقيع ملف تكوين .xml بالأسفل). يجب توفير كلمة المرور المحددة في إعداد الوصول قبل أن يتم استيراد تكوين جديد. إذا لم يكن لديك إمكانية الوصول إلى الإعداد أو أن كلمة المرور غير مطابقة أو أن ملف التكوين .xml غير موقّع، فإن التكوين لن يتم استيراده.

بمجرد تمكين ESET CMD يُمكنك استخدام سطر الأوامر لاستيراد تكوينات ESET Internet Security أو تصديرها. يُمكنك فعل ذلك يدوياً أو إنشاء برنامج نصي بغرض الأتمتة.

لاستخدام أوامر ecmd المتقدمة، أنت بحاجة إلى تشغيلها مع امتيازات المسؤول أو افتح موجّه أوامر (Windows cmd) باستخدام **تشغيل كمسؤول**. وإلا، ستصلك رسالة **Error executing command**. كما ينبغي وجود المجلد الوجهة عند تصدير التكوين. لا يزال أمر التصدير يعمل عند إيقاف إعداد ESET CMD.

تصدير أمر الإعدادات:

```
ecmd /getcfg c:\config\settings.xml
```

استيراد أمر الإعدادات:

```
ecmd /setcfg c:\config\settings.xml
```

يُمكن تشغيل أوامر ecmd المتقدمة محلياً فقط.

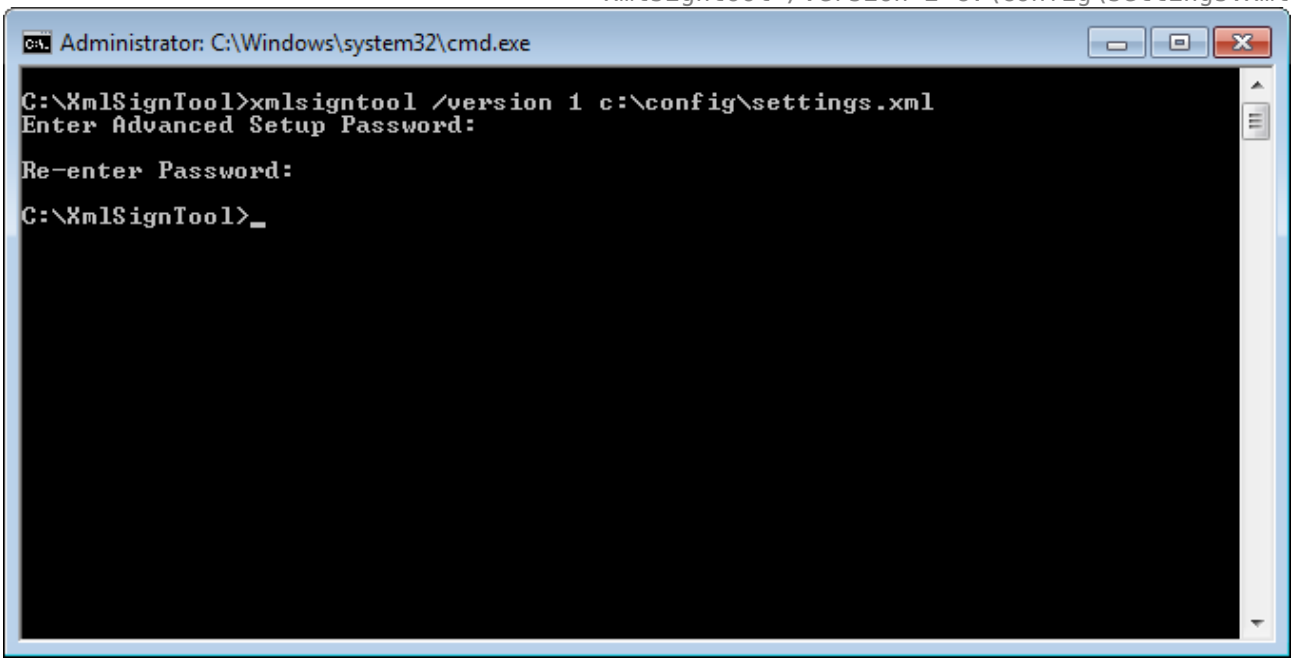
توقيع ملف تكوين *.xml*:

1. قم بتنزيل الملف القابل للتنزيل XmlSignTool.
2. افتح موجّه أمر (cmd Windows) باستخدام **تشغيل كمسؤول**.
3. انتقل إلى موقع حفظ `xmlsigntool.exe`
4. تنفيذ أمر لتوقيع ملف تكوين *.xml*، استخدام: `<xmlsigntool /version 1|2 <xml_file_path`

تعتمد قيمة معلمة `/version` على إصدار ESET Internet Security لديك. استخدم `/version 1` لإصدارات ESET Internet Security الأقدم من 11.1. استخدم `/version 2` لإصدار ESET Internet Security الحالي.

5. اكتب وأعد كتابة كلمة مرور الإعداد المتقدم عند مطالبتك من قبل XmlSignTool. ملف التكوين *.xml* موقّع الآن ويمكن استخدامه للاستيراد في مثيل آخر لـ ESET Internet Security مع ESET CMD باستخدام طريقة مصادقة كلمة المرور.

أمر توقيع ملف التكوين الذي تم تصديره:
`xmlsigntool /version 2 c:\config\settings.xml`



إذا تغيرت كلمة مرور إعداد الوصول وتريد استيراد تكوين تم توقيعه باستخدام كلمة مرور قديمة، فيتعين عليك توقيع ملف تكوين *.xml* مرةأخرى باستخدام كلمة المرور الحالية. يتيح لك هذا استخدام ملف تكوين قديم بدون تصديره إلى جهاز آخر يعمل بنظام ESET Internet Security قبل الاستيراد.

يوصى بعدم تمكين ESET CMD دون تخويل؛ لأن ذلك سيتيح استيراد أي تكوين غير موقَّع. ضع كلمة المرور في الإعداد المتقدم > **واجهة المستخدم** > **إعداد الوصول** لمنع التعديل بواسطة المستخدمين دون تصريح.

ملفات السجل

يمكنك العثور على تكوين التسجيل لـ ESET Internet Security في الإعداد المتقدم > **الأدوات** > **ملفات السجل**. يُستخدم قسم السجلات لتعريف طريقة إدارة السجلات. يكتشف البرنامج تلقائياً السجلات القديمة لتوفير مساحة القرص الثابت. جدير بالذكر

أنه يمكنك تحديد الخيارات التالية لملفات السجل:

أدنى شرح تفصيلي للتسجيل ـ تحديد أدنى مستوى للشرح التفصيلي للحدث المطلوب تسجيله:

- **التشخيص** ـ لتسجيل معلومات مطلوبة لضبط البرنامج وجميع السجلات الواردة أعلاه.
- **إخباري** ـ لتسجيل رسائل معلوماتية، تشمل رسائل التحديث الناجح، إضافة إلى جميع السجلات الواردة أعلاه.
- **التحذيرات** ـ لتسجيل رسائل الخطأ والتحذير الحرجة.
- **أخطاء** ـ سيتم تسجيل الأخطاء مثل "خطأ أثناء تنزيل الملف" والأخطاء الحرجة.
- **حرج** – لتسجيل الأخطاء الحرجة فقط (مثل: خطأ أثناء بدء الحماية ضد الفيروسات، جدار الحماية، وغيرها).

سيتم تسجيل جميع الاتصالات المحظورة عند تحديد مستوى الشرح التفصيلي التشخيصي.

سيتم تلقائياً حذف إدخالات السجلات الأقدم من عدد الأيام المحدد في حقل **حذف السجلات الأقدم من (يوماً/أيام) تلقائياً**.

تحسين ملفات السجلات تلقائياً – عند تحديد هذا الخيار، سيتم إلغاء تجزئة ملفات السجل تلقائياً إذا كانت النسبة أعلى من القيمة المحددة في الحقل **إذا تجاوز عدد السجلات غير المستخدمة (%)**.

انقر فوق **تحسين** لبدء إلغاء تجزئة ملفات السجل. تتم إزالة كل إدخالات السجل الفارغة لتحسين الأداء وزيادة سرعة معالجة السجلات. يمكن ملاحظة هذا التحسين خاصة إذا كانت السجلات تحتوي على عدد كبير من الإدخالات.

يتيح لك خيار **تمكين بروتوكول النص** تمكين تخزين السجلات بتنسيق ملفات آخر من ملفات السجل:

- **الدليل الهدف** – الدليل الذي سيتم فيه تخزين ملفات السجلات (ينطبق فقط على النصوص/ملفات CSV). يكون لكل قسم سجل ملفه الخاص به ويحمل اسماً محدداً مسبقاً (على سبيل المثال virlog.txt لقسم **التي تم اكتشافها** في ملفات السجل، إذا استخدمت تنسيق ملف النص العادي لتخزين السجلات).
- **النوع** ـ إذا حددت تنسيق الملف **نص**، فسيتم تخزين السجلات في ملف نصي، وسيتم فصل البيانات بعلامات جدولة. وينطبق الأمر نفسه على تنسيق الملفات **CSV** المفصولة بفاصلات. إذا اخترت **حدث**، فسيتم تخزين السجلات في سجل أحداث Windows (يمكن عرضه باستخدام "عارض الأحداث" في "لوحة التحكم") مقارنة بالملف.
- **حذف السجلات** ـ حذف كل السجلات المخزنة والمحددة حالياً في القائمة المنسدلة **النوع**. سيظهر إعلام ليخبرك بنجاح عملية حذف السجلات.

للمساعدة في سرعة حل المشكلات، قد تطلب شركة ESET منك توفير سجلات من جهاز الكمبيوتر لديك. تسهل أداة ESET Log Collector عليك تجميع المعلومات المطلوبة. لمزيد من المعلومات عن ESET Log Collector الرجاء الاطلاع على مقالة قاعدة معارف ESET.

وضع الألعاب

وضع الألعاب عبارة عن ميزة للمستخدمين الذين يحتاجون استخداماً غير متقطع لبرامجهم، ولا يريدون إزعاجهم بنوافذ إعلام/تنبيه، ويرغبون في تقليل استخدام وحدة المعالجة المركزية (CPU). ويمكن كذلك استخدام وضع الألعاب خلال العروض التقديمية التي لا يمكن مقاطعتها بنشاط برنامج الحماية من الفيروسات. من خلال تمكين هذه الميزة، يتم تعطيل جميع النوافذ المنبثقة ويتم إيقاف نشاط البرنامج المجدول تماماً. وتظل حماية النظام تعمل في الخلفية، ولكن لا تتطلب أي تدخل من المستخدم.

يمكنك تمكين "وضع الألعاب" أو تعطيله في نافذة البرنامج الرئيسية ضمن **الإعداد** > **حماية الكمبيوتر** بالنقر فوق أو بجوار **وضع الألعاب**. من الجدير بالذكر أن تمكين وضع الألعاب يشكل خطراً أمنياً محتملاً، لذلك ستتحول أيقونة حالة الحماية في شريط المهام إلى اللون البرتقالي وستعرض تحذيراً. كما ستشاهد هذا التحذير في نافذة البرنامج الرئيسية حيث سترى عبارة **وضع الألعاب نشط** باللون البرتقالي.

تنشيط الخيار **تمكين وضع الألعاب عند تشغيل تطبيقات في وضع ملء الشاشة تلقائياً** الموجود ضمن القسم إعداد متقدم () **الأدوات** > **وضع الألعاب** لبدء وضع الألعاب كلما قمت بتشغيل تطبيق في وضع ملء الشاشة وإيقافه بعد الخروج من التطبيق.

تنشيط **تعطيل وضع الألعاب تلقائياً بعد** لتحديد مقدار الوقت الذي سيتم بعده تعطيل وضع الألعاب تلقائياً.

> إذا كان جدار الحماية في الوضع التفاعلي وكان وضع الألعاب ممكّناً، فقد تواجه مشكلة في الاتصال بالإنترنت. ويمثل هذا مشكلة في حالة تشغيل لعبة تتصل بالإنترنت. عادة، يُطلب منك تأكيد مثل هذا الإجراء (إذا لم يتم تحديد أي قواعد اتصال أو استثناءات)، ولكن يكون تفاعل المستخدم معطلاً في وضع الألعاب. للسماح بالاتصال، حدد قاعدة اتصال لأي تطبيق قد يتعرض لهذه المشكلة، أو استخدم وضع تصفية مختلفاً في جدار الحماية. وضع في اعتبارك أنه إذا كان وضع الألعاب ممكّناً وانتقلت إلى صفحة ويب أو تطبيق قد يشكل خطراً أمنياً، فقد يتم حظره، ولكن لن ترى أي تفسير أو تحذير لأن تفاعل المستخدم معطل.

التشخيصات

توفر التشخيصات تفريغات أعطال التطبيق الخاصة بعمليات ESET (على سبيل المثال، ekrn). عند تعطل تطبيق ما، سيتم إنشاء تفريغ. ويمكن أن يساعد هذا المطورين على تصحيح العديد من مشكلات ESET Internet Security وحلها.

انقر فوق القائمة المنسدلة الموجودة بجوار **نوع التفريغ** وحدد أحد الخيارات الثلاثة المتوفرة التالية:

- حدد **تعطيل** لتعطيل هذه الميزة.
- **أقل** (افتراضي) ـ لتسجيل أصغر مجموعة معلومات مفيدة يمكن أن تساعد في تحديد سبب تعطل التطبيق على نحو غير متوقع. يمكن أن يكون هذا النوع من ملفات التفريغ مفيداً عندما تكون المساحة محدودة. ولكن، نظراً لمحدودية المعلومات التي يشملها، قد لا يتم اكتشاف الأخطاء التي لم تنشأ مباشرة عن العملية الجزئية التي كانت تعمل في وقت حدوث المشكلة بواسطة تحليل هذا الملف.
- **كامل** – لتسجيل جميع محتويات ذاكرة النظام عند توقف التطبيق بشكل غير متوقع. قد يحتوي التفريغ الكامل للذاكرة على بيانات من عمليات كانت تعمل أثناء جمع تفريغ الذاكرة.

المجلد المستهدف ـ الدليل الذي سيتم فيه إنشاء التفريغ أثناء العطل.

فتح مجلد التشخيصات ـ انقر فوق **فتح** لفتح هذا الدليل في نافذة مستكشف *Windows* جديدة.

إنشاء تفريغ تشخيصي – انقر فوق **إنشاء** لإنشاء ملفات تفريغ تشخيصي في **المجلد المستهدف**.

التسجيل المتقدم

تمكين التسجيل المتقدم في رسائل التسويق ـ سجّل جميع الأحداث المتعلقة برسائل التسويق داخل المنتج.

تمكين التسجيل المتقدم لمحرك مكافحة البريد العشوائي – سجِّل جميع الأحداث التي تحدث أثناء فحص مكافحة البريد العشوائي. وهذا من شأنه مساعدة المطورين في تشخيص المشكلات المتعلقة بمحرك مكافحة البريد العشوائي لـ ESET وإصلاحها.

تمكين التسجيل المتقدم لمحرك مكافحة السرقة – سجّل جميع الأحداث التي تحدث في مكافحة السرقة للسماح بتشخيص المشكلات وحلها.

تمكين التسجيل المتقدم لحماية المتصفح–تسجيل جميع الأحداث التي تحدث في التصفح المصرفي الآمن.

تمكين التسجيل المتقدم لأداة فحص جهاز الكمبيوتر – سجّل جميع الأحداث التي تحدث أثناء فحص الملفات والمجلدات عن طريق فحص جهاز كمبيوتر.

تمكين التسجيل المتقدم للتحكم في الأجهزة – سجِّل جميع الأحداث التي تحدث في التحكم في الأجهزة. وهذا من شأنه مساعدة المطورين في تشخيص المشكلات المتعلقة بالتحكم في الأجهزة وإصلاحها.

تمكين التسجيل المتقدم لـ Direct Cloud – سجِّل جميع الأحداث التي تحدث في ESET LiveGrid®. وهذا من شأنه مساعدة المطورين في تشخيص المشكلات المتعلقة بـ ESET LiveGrid® وإصلاحها.

تمكين السجل المتقدم لحماية الوثائق – تسجيل جميع الأحداث التي تتم في حماية الوثائق للسماح بتشخيص المشكلات وحلها.

تمكين التسجيل المتقدم لحماية برامج البريد الإلكتروني – سجّل جميع الأحداث التي تحدث في حماية برامج البريد الإلكتروني والمكون الإضافي لبرامج البريد الإلكتروني للسماح بتشخيص المشكلات وحلها.

تمكين تسجيل Kernel المتقدم – سجّل جميع الأحداث التي تحدث في ESET kernel (ekrn).

تمكين التسجيل المتقدم للترخيص – قم بتسجيل جميع اتصالات المنتج باستخدام تنشيط ESET أو خوادم ESET License Manager.

تمكين تتبع الذاكرة – سجّل جميع الأحداث التي تساعد المطورين في تشخيص تسريب الذاكرة.

تمكين تسجيل دخول متقدم لحماية الشبكة – قم بتسجيل جميع بيانات الشبكة التي تمر عبر جدار حماية بتنسيق PCAP لمساعدة المطورين في تشخيص المشكلات المتعلقة بجدار الحماية وإصلاحها.

تمكين التسجيل المتقدم لماسح حركة مرور الشبكة—سجل جميع البيانات التي تمر عبر ماسح حركة مرور الشبكة PCAP بالتنسيق لمساعدة المطوّرين في تشخيص المشكلات المتعلقة بماسح حركة مرور الشبكة وإصلاحها.

تمكين التسجيل المتقدم لنظام التشغيل – سجّل المزيد من المعلومات حول نظام التشغيل مثل العمليات الفعالة ونشاط لوحة المعالجة المركزية وعمليات القرص. يمكن أن يساعد هذا المطورين في تشخيص وإصلاح المشكلات المرتبطة بمنتج ESET الذي يعمل على نظام التشغيل.

تمكين التسجيل المتقدم للمراقبة الأبوية – سجِّل جميع الأحداث التي تحدث في المراقبة الأبوية. وهذا من شأنه مساعدة المطورين في تشخيص المشكلات المتعلقة بالمراقبة الأبوية وإصلاحها.

تمكين التسجيل المتقدم للمراسلة الفورية – سجّل جميع الأحداث التي تحدث أثناء المراسلة الفورية.

تمكين التسجيل المتقدم لحماية نظام الملفات الحالي – سجّل جميع الأحداث التي تحدث أثناء فحص الملفات والمجلدات عن طريق حماية نظام الملفات الحالي.

تمكين التسجيل المتقدم لمحرك لتحديث – قم بتسجيل جميع الأحداث التي تحدث أثناء التحديث. وهذا قد يساعد المطورين في تشخيص المشكلات المتعلقة بمحرك التحديث وإصلاحها.

توجد ملفات السجل في *C:\ProgramData\ESET\ESET Security\Diagnostics*.

الدعم الفني

عند الاتصال بالدعم الفني لـESET من خلال ESET Internet Security يمكنك إرسال بيانات تكوين النظام. حدد **الإرسال دائماً** من القائمة المنسدلة **إرسال بيانات تكوين النظام** لإرسال البيانات تلقائياً، أو حدد **السؤال قبل الإرسال** ليتم سؤالك قبل إرسال البيانات.

إمكانية الاتصال

في شبكات محددة، يمكن للخادم الوكيل التوسط في الاتصال بين الكمبيوتر والإنترنت. إذا كنت تستخدم خادم وكيل، فأنت بحاجة إلى تحديد الإعدادات التالية. خلاف ذلك، لا يمكن تحديث ESET Internet Security والوحدات الخاصة به تلقائياً. في ESET Internet Security يتوفر إعداد خادم الوكيل في قسمين مختلفين من الإعداد المتقدم.

يمكن تكوين إعدادات الخادم الوكيل العامة في الإعداد المتقدم > **الاتصال** > **الخادم الوكيل**. يحدد تعيين خادم الوكيل في هذا المستوى إعدادات خادم الوكيل العمومية لجميع ESET Internet Security. سيتم استخدام المعلمات الواردة هنا بواسطة جميع الوحدات التي تتطلب اتصالاً بالإنترنت.

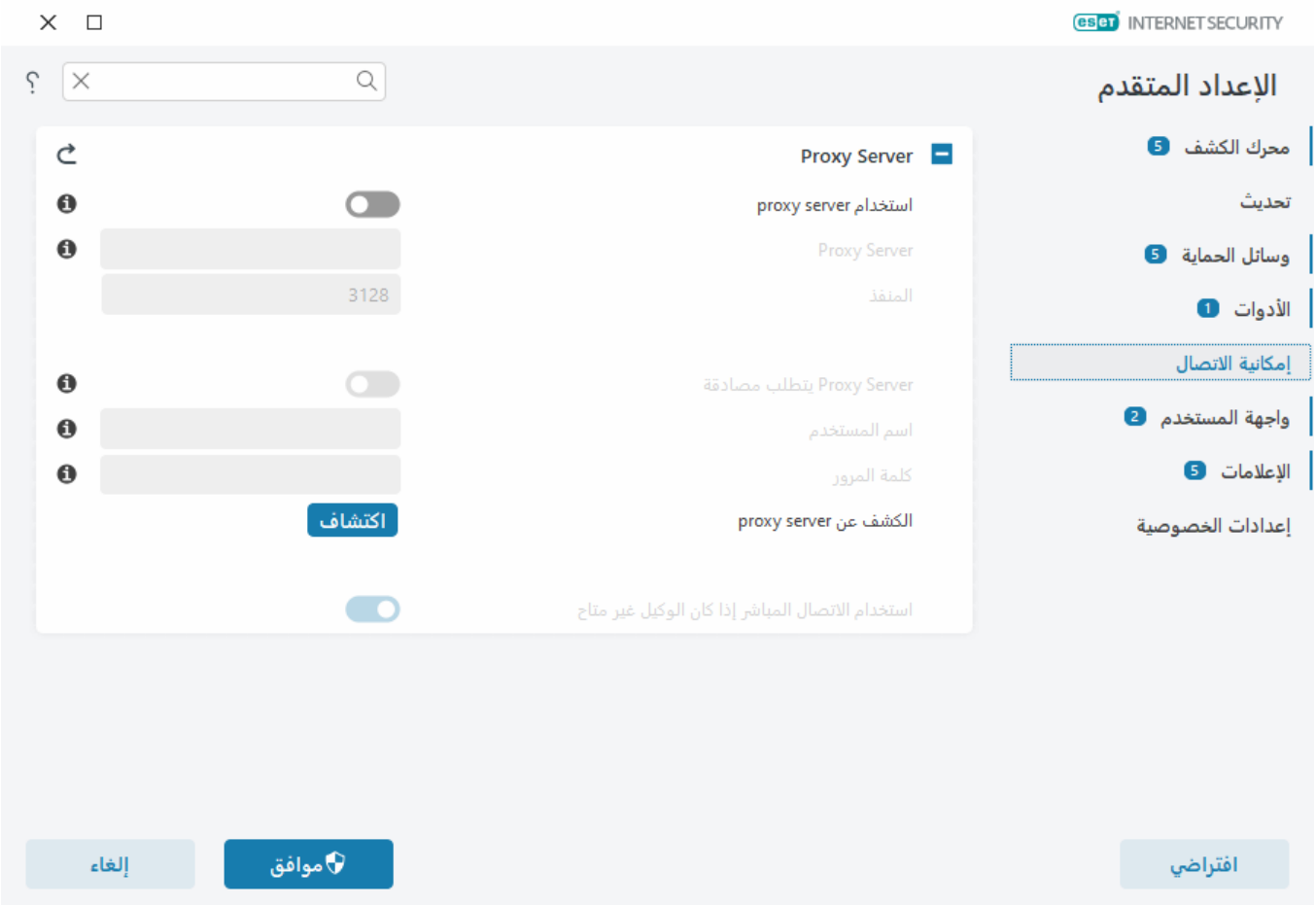
لتحديد إعدادات خادم الوكيل العامة، قم بتمكين **استخدام خادم الوكيل** واكتب عنوان **خادم الوكيل** مع رقم **منفذ** الخادم الوكيل.

إذا كان الاتصال بالخادم الوكيل يتطلب مصادقة، فحدد **الخادم الوكيل يتطلب مصادقة** وأدخل **اسم المستخدم** و**كلمة المرور** الصحيحين في الحقلين المناسبين لهما. انقر فوق **اكتشاف خادم الوكيل** لاكتشاف إعدادات خادم الوكيل وتعبئتها تلقائياً. سيقوم ESET Internet Security بنسخ المعلمات المحددة في خيارات الإنترنت لـInternet Explorer أو Google Chrome.

> يجب إدخال كلمة المرور واسم المستخدم يدوياً في إعدادات **خادم ESET للادارة عن بعد**.

استخدام الاتصال المباشر إذا كان الوكيل غير متاح – إذا تم تكوين ESET Internet Security للاتصال عبر الوكيل وكان الوكيل لا يمكن الوصول إليه، فسيتخطى ESET Internet Security الوكيل ويتصل مباشرة مع خوادم ESET.

يمكن أيضاً تهيئة إعدادات الخادم الوكيل في إعداد متقدم>**تحديث** > **ملفات التعريف** > **التحديثات** > **خيارات الاتصال** من خلال تحديد **الاتصال عبر خادم وكيل** من القائمة المنسدلة **لوضع الوكيل**. ينطبق هذا التكوين على التحديثات فقط ويوصى به لأجهزة الكمبيوتر المحمولة التي تتلقى تحديثات الوحدة من مواقع بعيدة. لمزيد من المعلومات، راجع إعداد التحديث المتقدم.



واجهة المستخدم

لتكوين سلوك واجهة المستخدم الرسومية (GUI) للبرنامج، افتح الإعداد المتقدم > **واجهة المستخدم**.

يمكنك تعديل المظهر والمؤثرات البصرية للبرنامج في شاشة الإعداد المتقدم عناصر واجهة المستخدم.

لتوفير أقصى درجات الأمان لبرنامج الأمان، يمكنك منع إزالة التثبيت أو أي تغييرات غير مسموح بها من خلال حماية الإعدادات بكلمة مرور باستخدام أداة إعداد الوصول.

لتهيئة سلوك إعلامات النظام وتنبيهات الكشف وحالات التطبيق، راجع قسم الإعلامات.

عناصر واجهة المستخدم

يمكنك ضبط ESET Internet Securityبيئة العمل (واجهة المستخدم الرسومية) لتلائم احتياجاتك في الإعداد المتقدم >**واجهة المستخدم** > **عناصر واجهة المستخدم**.

وضع اللون—حدد نظام ألوان ESET Internet Security واجهة المستخدم الرسومية من القائمة المنسدلة:

- **نفس الشيء مثل لون النظام**—يضبط نظام الألوان ESET Internet Security بناءً على إعدادات نظام التشغيل.
- **داكن**—ESET Internet Security سيكون له نظام ألوان داكن (الوضع الداكن).

- **فاتح**—ESET Internet Security سيكون له نظام ألوان فاتح قياسي.

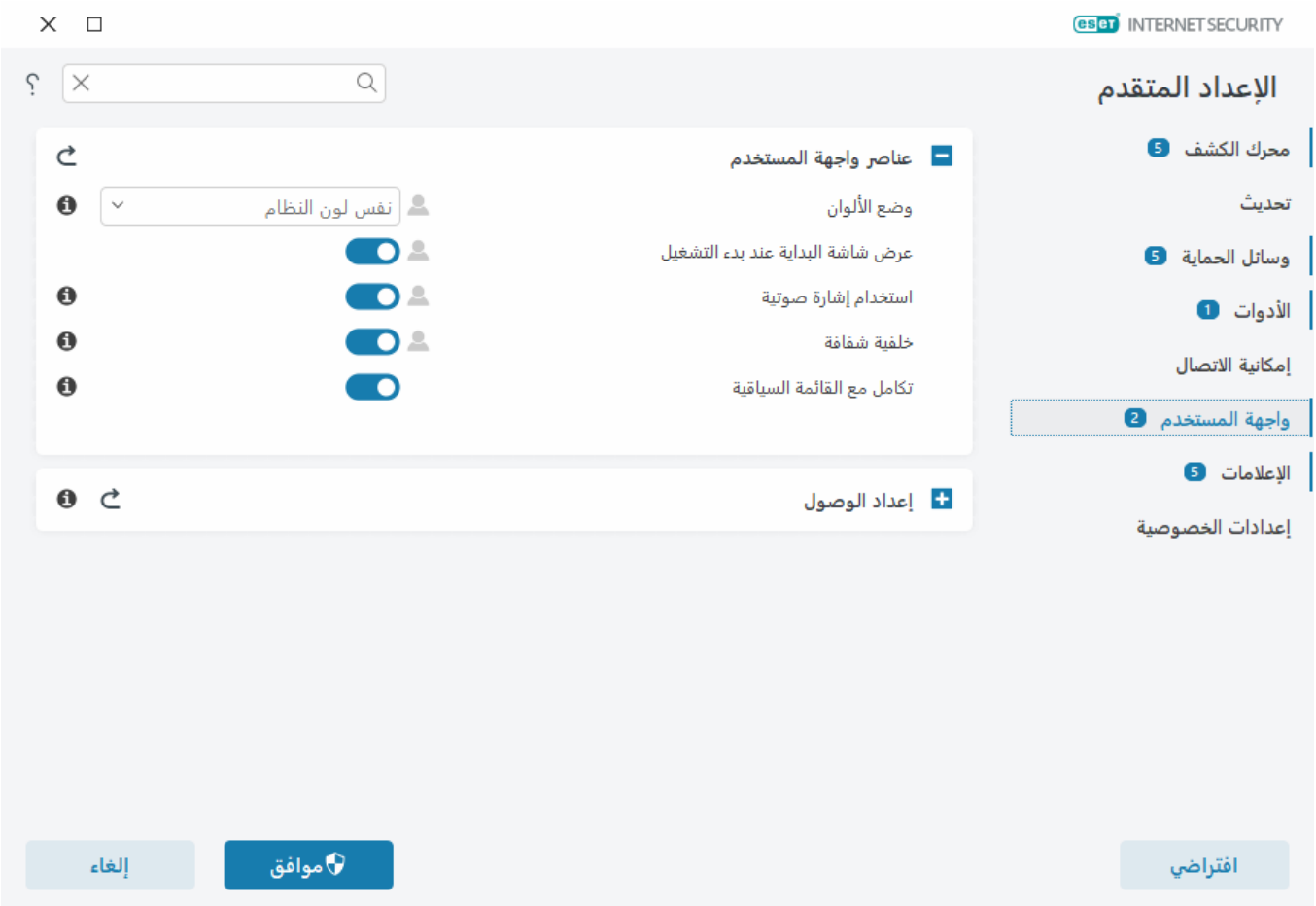
> يمكنك أيضاً تحديد نظام ألوان واجهة المستخدم الرسومية لـESET Internet Security في أعلى الجانب الأيمن من نافذة البرنامج الرئيسية لـ ***.

عرض شاشة البداية عند بدء التشغيل – تعرض ESET Internet Security شاشة البداية أثناء بدء التشغيل.

استخدام إشارة صوتية – يُصدر صوتاً عند وقوع أحداث مهمة أثناء عملية فحص، على سبيل المثال عند اكتشاف تهديد أو انتهاء الفحص، حدد استخدام إشارة صوتية.

خلفية شفافة — تتيح تأثير الخلفية الشفافة لنافذة البرنامج الرئيسية. تتوفر الخلفية الشفافة فقط لأحدث إصدارات Windows (RS4 والإصدارات الأحدث).

تكامل مع القائمة السياقية – لتكامل عناصر تحكم ESET Internet Security في القائمة السياقية.



إعداد الوصول

تلعب إعدادات ESET Internet Security دوراً مهماً في سياسة الأمان لديك. فالتعديلات غير المصرّح بها يمكنها أن تُعرّض ثبات نظامك وحمايته للخطر. لتجنب التعديلات غير المصرَّح بها، يمكن حماية معلمات إعداد ESET Internet Security وإزالة تثبيته بكلمة مرور. يمكن تكوين إعداد الوصول في الإعداد المتقدم > **واجهة المستخدم** > **إعداد الوصول**.

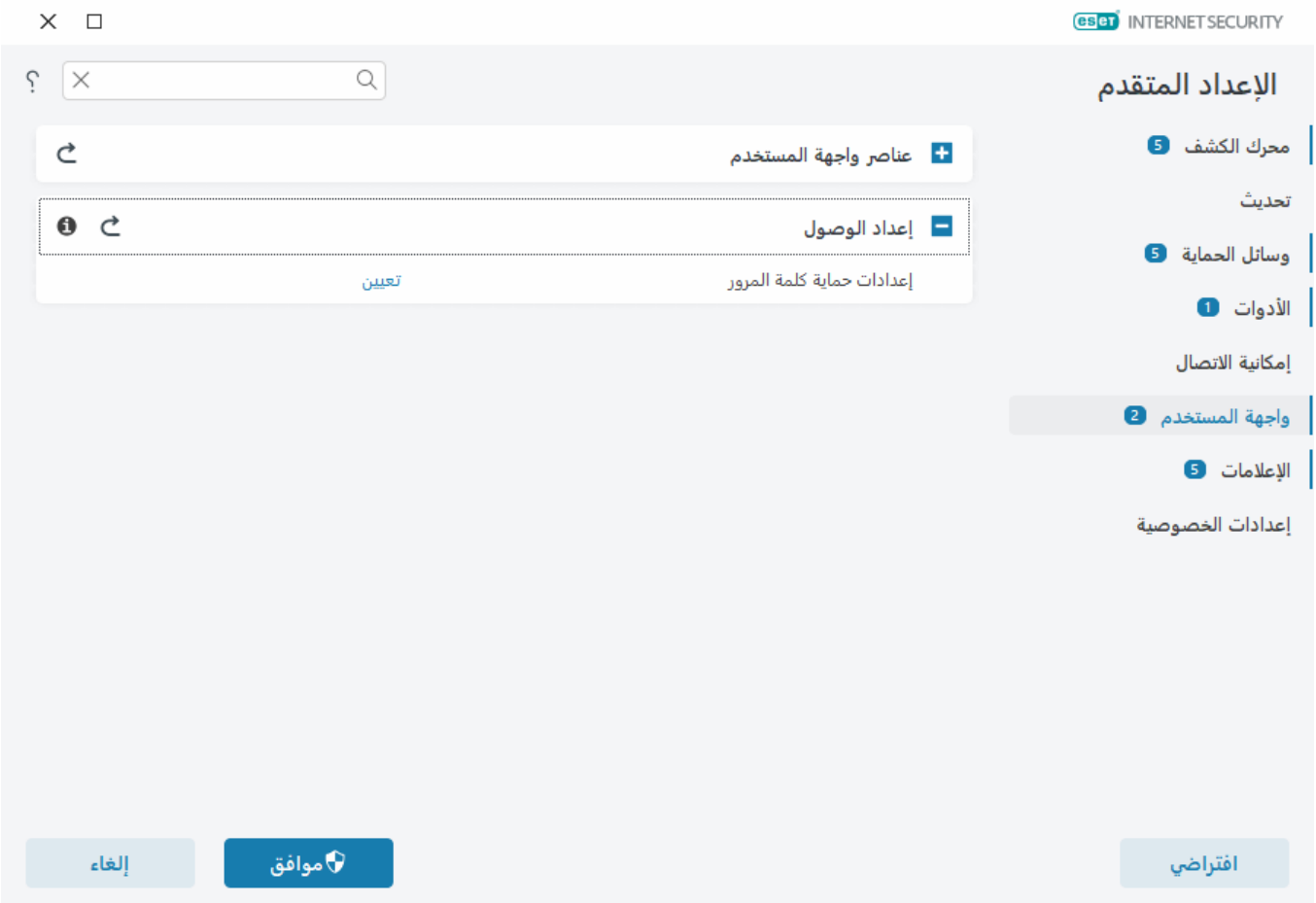
لتعيين كلمة مرور لحماية معلمات الإعداد وإزالة تثبيت ESET Internet Security انقر فوق **تعيين** بجوار **إعدادات حماية كلمة**

المرور.

> عندما تريد الوصول إلى الإعداد المتقدم المحمي، يتم عرض نافذة لإدخال كلمة المرور. وإذا نسيت كلمة المرور أو فقدتها، فانقر فوق خيار **استعادة كلمة المرور** أدناه وأدخل عنوان البريد الإلكتروني الذي استخدمته لتسجيل الاشتراك. سيرسل لك ESET رسالة بريد إلكتروني بها رمز التحقق وتعليمات حول كيفية كلمة المرور.
> • كيفية إلغاء تأمين الإعداد المتقدم

لتغيير كلمة المرور، انقر فوق **تغيير كلمة المرور** بجوار **إعدادات حماية كلمة المرور**.

لإزالة كلمة المرور، انقر فوق **إزالة** بجوار **إعدادات حماية كلمة المرور**.



كلمة المرور للإعداد المتقدم

لحماية ESET Internet Security الإعداد المتقدم وتجنب التعديل غير المصرح به، اكتب كلمة المرور الجديدة في حقلي **كلمة المرور الجديدة وتأكيد كلمة المرور**. انقر فوق **موافق**.

عندما تريد تغيير كلمة المرور الحالية:

1. اكتب كلمة المرور القديمة في الحقل **كلمة المرور القديمة**.
2. أدخل كلمة المرور الجديدة في الحقلين **كلمة المرور الجديدة** و**تأكيد كلمة المرور**.
3. انقر فوق **موافق**.

ستكون كلمة المرور هذه مطلوبة للوصول إلى الإعداد المتقدم.

إذا نسيت كلمة المرور الخاصة بك، راجع فتح كلمة مرور الإعدادات في منتجات ESET home.

لاستعادة مفتاح تنشيط ESET المفقود، أو تاريخ انتهاء صلاحية اشتراكك، أو معلومات اشتراك أخرى لـESET Internet Security راجع فقدت مفتاح التنشيط الخاص بي.

دعم قارئ الشاشة

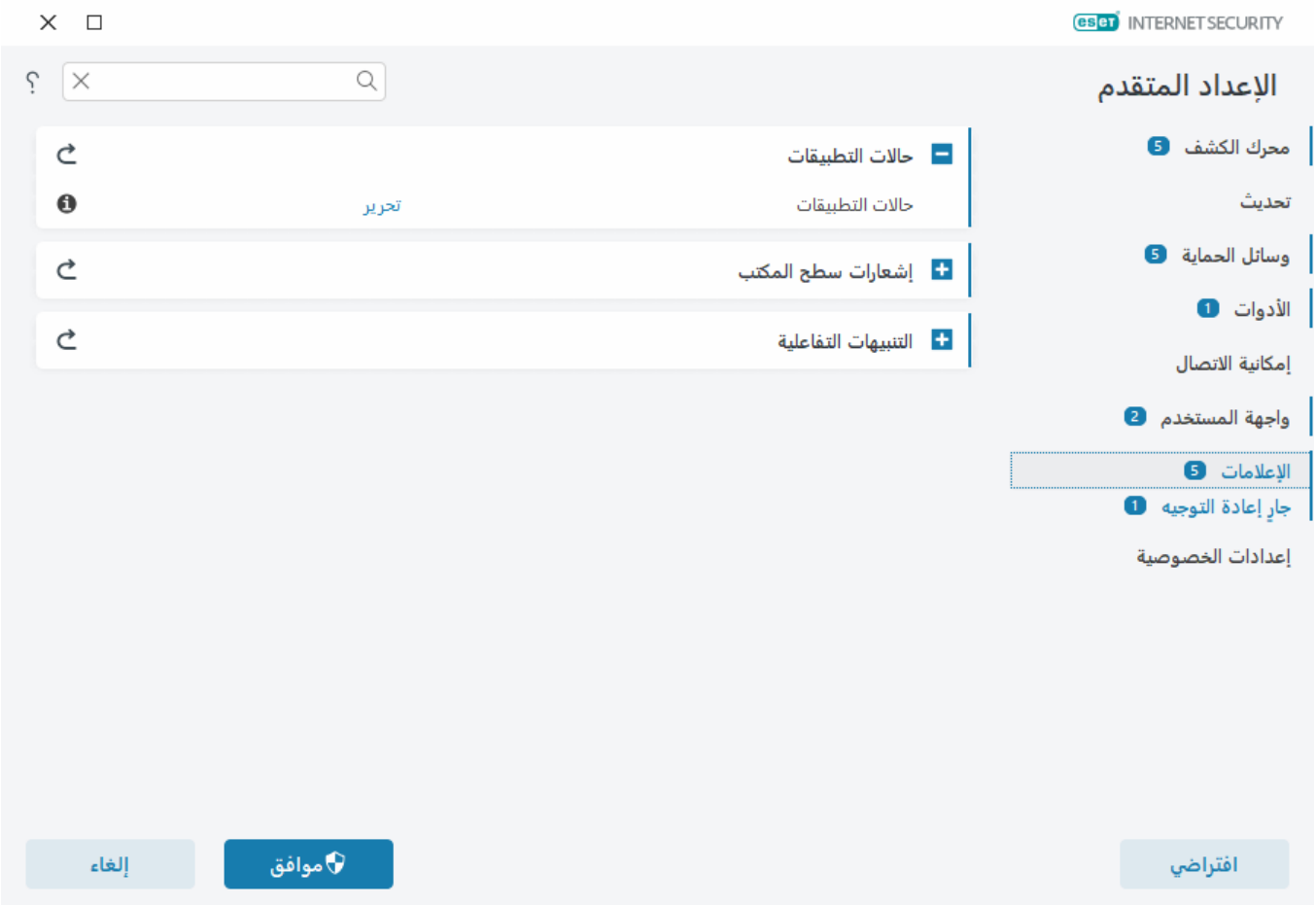
يمكن استخدام ESET Internet Security مع قارئات الشاشة للسّماح لمستخدمي ESET الذين يعانون من ضعف في الرؤية بالتنقل في المنتج أو لتكوين الإعدادات. يتم دعم قارئات الشاشة التالية (JAWS, NVDA, Narrator).

للتأكد من أن برنامج قارئ الشاشة يمكنه الوصول إلى واجهة المستخدم الرسومية لـESET Internet Security بشكل صحيح، اتبع الإرشادات الواردة في مقالة قاعدة المعرفة لدينا.

الإعلامات

لإدارة الإعلامات ESET Internet Security افتح الإعداد المتقدم > **الإعلامات**. يمكنك تهيئة الأنواع التالية من الإعلامات:

- حالات التطبيق ـ الإعلامات المعروضة في نافذة البرنامج الرئيسية > **نظرة عامة**.
- إعلامات سطح المكتب – نوافذ إعلام صغيرة بجانب شريط مهام النظام.
- التنبيهات التفاعلية ـ نوافذ التنبيه ومربعات الرسائل التي تتطلب تفاعل المستخدم.
- جارٍ إعادة التوجيه – يتم إرسال إعلامات البريد الإلكتروني إلى عنوان البريد الإلكتروني المحدد.



حالات التطبيقات

حالات التطبيق – انقر فوق **تحرير** لتحديد حالات التطبيق التي سيتم عرضها في القسم الرئيسي من نافذة البرنامج الرئيسية > **نظرة عامة**.

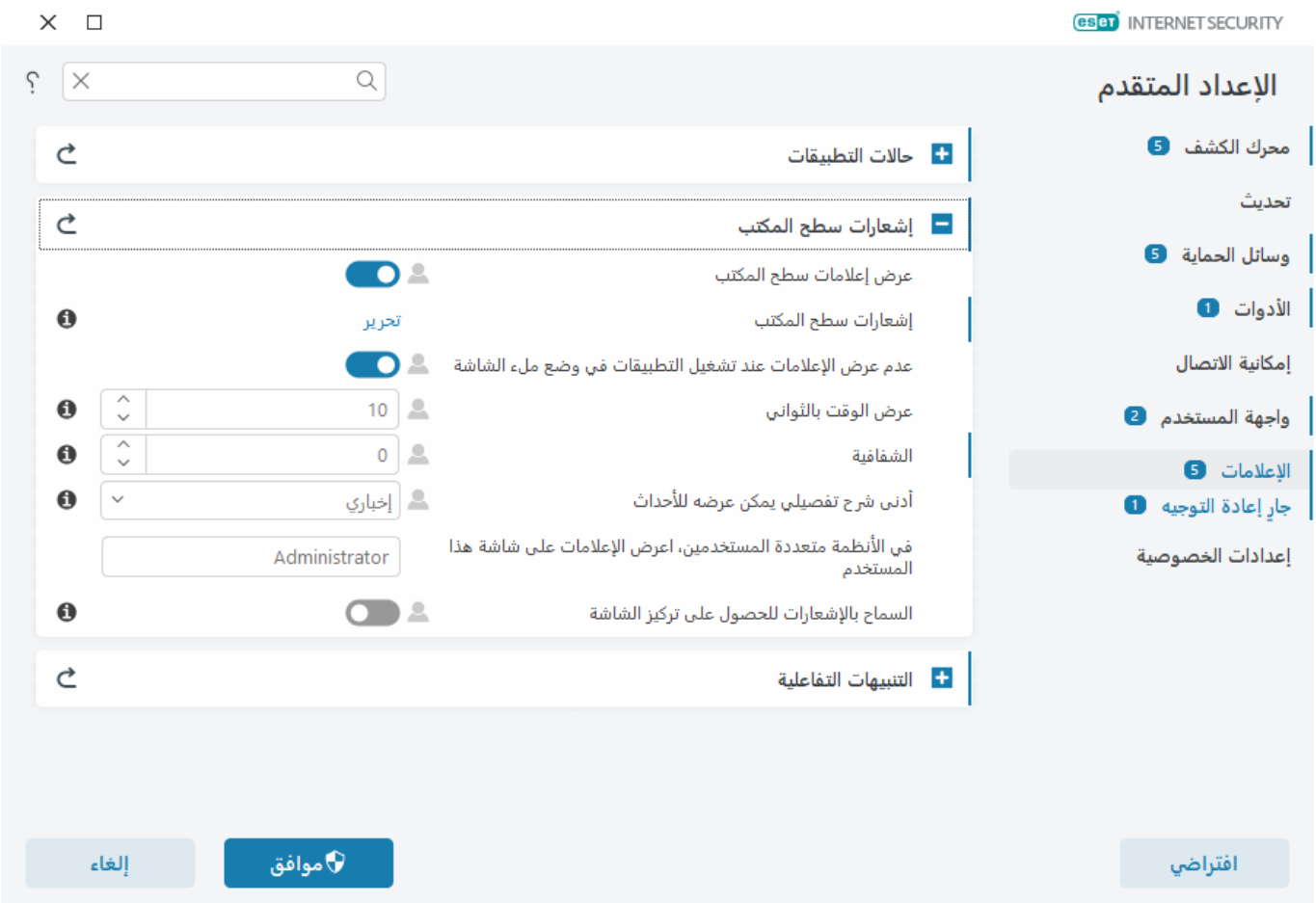
نافذة الحوار – حالات التطبيق

في نافذة الحوار هذه، يمكنك تحديد حالات التطبيق التي سيتم عرضها. على سبيل المثال، عند إيقاف الحماية من الفيروسات ومكافحة التجسس أو عند تمكين وضع "الألعاب".

سيتم أيضاً عرض حالة التطبيق إذا لم يتم تنشيط منتجك أو انتهت صلاحية اشتراكك.

إعلامات سطح المكتب

يتم تمثيل إعلامات سطح المكتب من خلال نافذة إعلام صغيرة بجانب شريط مهام النظام. وبشكل افتراضي، يظهر لمدة 10 ثوانٍ، ثم يختفي ببطء. تشمل الإعلامات تحديثات المنتج الناجحة، أو الأجهزة الجديدة المتصلة، أو إتمام مهام مسح الفيروسات، أو العثور على تهديدات جديدة.



عرض الإعلامات على سطح المكتب – نوصي بإبقاء هذا الخيار ممكناً حتى يتمكن المنتج من إعلامك عند حدوث حدث جديد.

إعلامات سطح المكتب – انقر فوق **تحرير** لتمكين أو تعطيل إعلامات سطح المكتب المحددة.

عدم عرض الإعلامات عند تشغيل التطبيقات في وضع ملء الشاشة – قمع جميع الإعلامات غير التفاعلية عند تشغيل التطبيقات في وضع ملء الشاشة.

عرض الوقت بالثواني– قم بتعيين مدة رؤية الإعلام. يجب أن تكون القيمة بين 3–30 ثانية.

الشفافية – قم بتعيين نسبة شفافية الإعلام. النطاق المدعوم هو 0 (بدون شفافية) إلى 80 (شفافية عالية جداً).

الحد الأدنى لألفاظ الأحداث التي سيتم عرضها – قم بتعيين مستوى الخطورة البادئ للإعلامات المطلوب عرضها. من القائمة المنسدلة، حدد أحد الخيارات التالية:

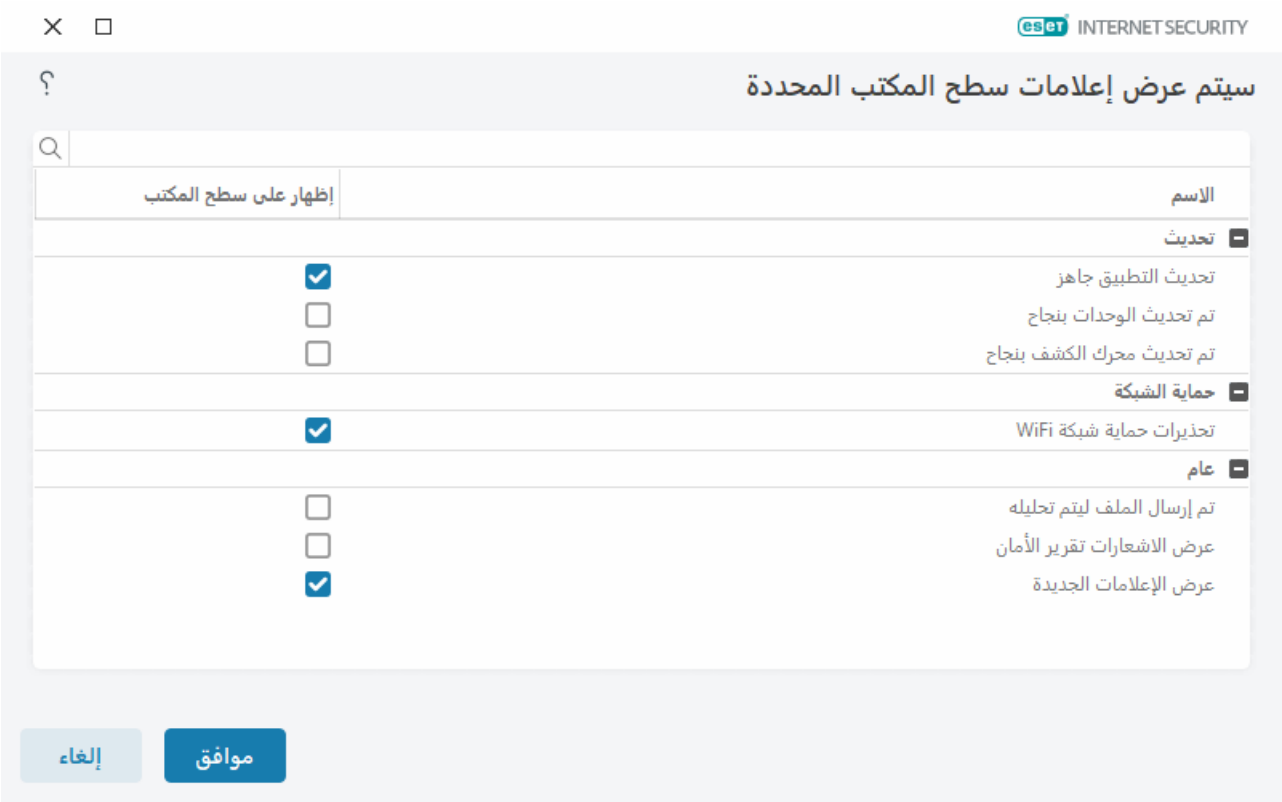
- **التشخيص** – لتسجيل معلومات مطلوبة لضبط البرنامج وجميع السجلات الواردة أعلاه.
- **إخباري** – لتسجيل رسائل معلوماتية، مثل أحداث الشبكة غير القياسية، بما في ذلك رسائل التحديث الناجح، إضافة إلى جميع السجلات الواردة أعلاه.
- **تحذيرات** – يعرض رسائل التحذير والأخطاء الحرجة (على سبيل المثال، أداة مكافحة التسلل لا تعمل بشكل جيد أو فشل التحديث).
- **الأخطاء** – يعرض الأخطاء (على سبيل المثال، لم يتم بدء تشغيل حماية الوثائق) والأخطاء الحرجة.
- **حرج** – لعرض الأخطاء الحرجة فقط (خطأ أثناء بدء الحماية ضد الفيروسات أو إصابة النظام، إلخ.).

على أنظمة متعددة المستخدمين، اعرض الإعلامات على شاشة هذا المستخدم ـ يسمح للحسابات المحددة باستلام إعلامات سطح المكتب. على سبيل المثال، إذا كنت لا تستخدم حساب المسؤول، فاكتب اسم الحساب الكامل وسيتم عرض إعلامات سطح المكتب للحساب المحدد. يمكن لحساب مستخدم واحد فقط استلام إعلامات سطح المكتب.

السماح للإعلامات بالتركيز على الشاشة ـ يسمح للإعلامات بالتركيز على الشاشة ويمكن الوصول إليها في قائمة **ALT + Tab**.

قائمة إعلامات سطح المكتب

لضبط رؤية إعلامات سطح المكتب (المعروضة في أسفل يسار الشاشة)، قم بفتح الإعداد المتقدم > **الإعلامات** > **إعلامات سطح المكتب**. انقر فوق **تحرير** بجوار **إعلامات سطح المكتب** وحدد خانة الاختيار المناسبة **إظهار**.



عام

عرض إعلامات تقرير الأمان – تلقي إعلاماً عندما يتم إنشاء تقرير أمان جديد.

عرض الإعلامات الجديدة – إعلامات حول جميع الميزات الجديدة والمحسّنة لأحدث إصدار للمنتج.

تم إرسال الملف للتحليل — تلقي إعلام في كل مرة يرسل فيها ESET Internet Security ملفاً للتحليل.

مراقب الشبكة

إعلام بأجهزة الشبكة المكتشفة حديثاً—تلقي إعلام عند توصيل جهاز جديد بالشبكة.

حماية الشبكة

تم تغيير ملف تعريف الشبكة—تلقي إعلام عند تغيير ملف تعريف الشبكة.

تحذيرات حماية Wifi—قم بتلقي إعلام عند محاولتك الاتصال بشبكة Wi-Fi بكلمة مرور ضعيفة أو بدون كلمة مرور.

تحديث

يتم إعداد تحديث التطبيق ـ تلقي إعلام عندما يكون هناك تحديث لإصدار جديد من ESET Internet Security يتم إعداده.

تم تحديث محرك الكشف بنجاح ـ تلقي إعلام عندما يقوم المنتج بتحديث وحدات محرك الكشف.

تم تحديث الوحدات بنجاح ـ تلقي إعلام عندما يقوم المنتج بتحديث مكونات البرنامج.

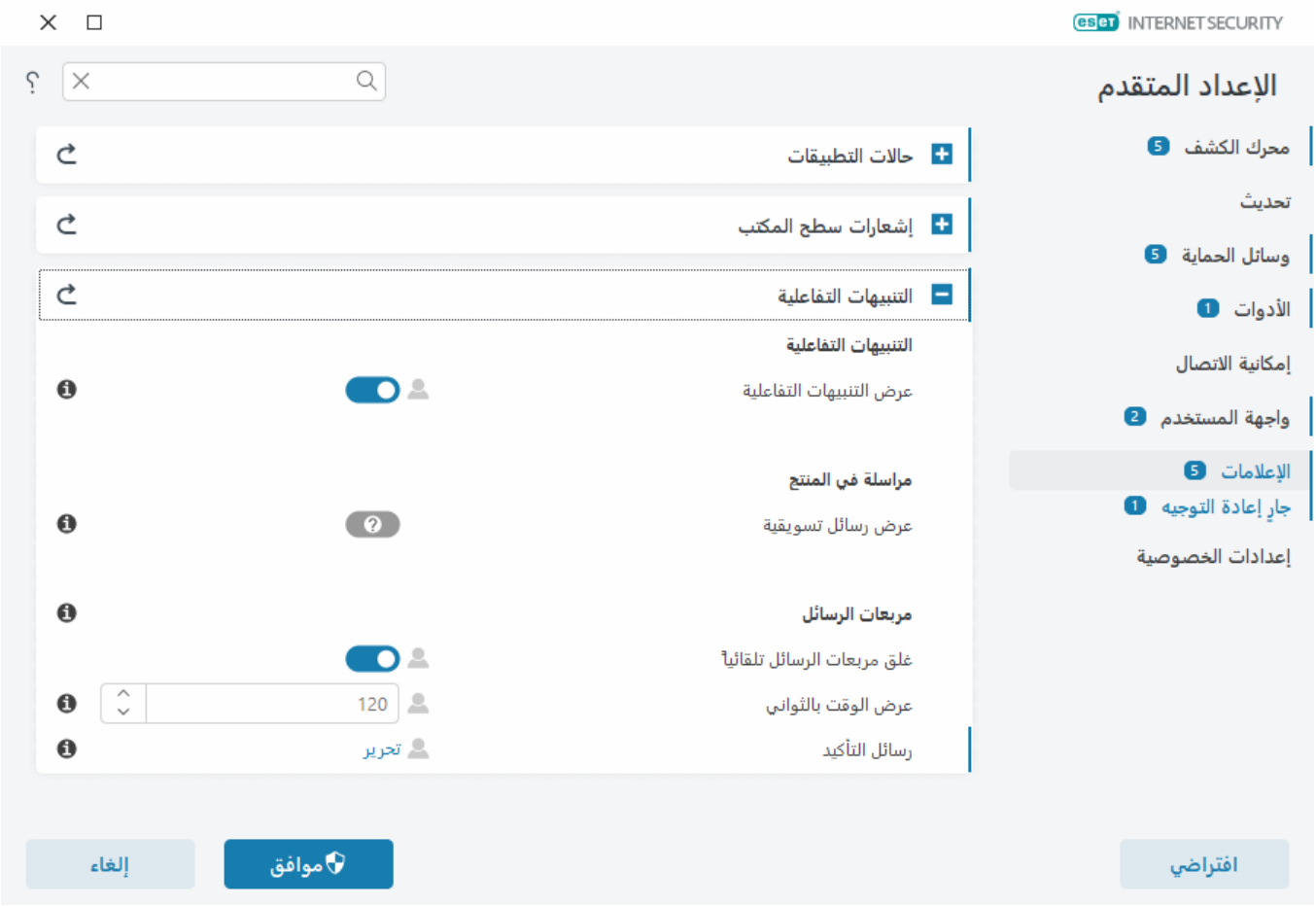
لتعيين الإعدادات العامة لإعلامات سطح المكتب، على سبيل المثال، الوقت المنقضي في عرض الرسالة أو الحد الأدنى لألفاظ الأحداث التي سيتم عرضها، راجع إعلامات سطح المكتب في الإعداد المتقدم > **الإعلامات**.

التنبيهات التفاعلية

هل تبحث عن معلومات عن التنبيهات والإعلامات الشائعة؟

- تم العثور على تهديد
- تم حظر العنوان
- لم يتم تنشيط المنتج
- التغيير الي المنتج الأدنى
- التغيير إلى منتج ذي ميزات أقل
- يتوفر التحديث
- معلومات التحديث غير متسقة
- استكشاف المشكلات وإصلاحها لرسالة "فشل تحديث الوحدات النمطية"
- حل أخطاء تحديث الوحدات
- تم حظر تهديد الشبكة
- تم إبطال شهادة موقع الويب

يتيح لك قسم **التنبيهات التفاعلية** في الإعداد المتقدم > **الإعلامات** إمكانية تكوين كيفية تكوين مربعات الرسائل والتنبيهات التفاعلية للاكتشافات، حيث يلزم اتخاذ قرار من قِبل مستخدم (على سبيل المثال، مواقع التصيّد المحتملة) يتم التعامل معها بواسطة ESET Internet Security.



التنبيهات التفاعلية

سيؤدي تعطيل **عرض التنبيهات التفاعلية** إلى إخفاء جميع نوافذ التنبيه ومربعات حوار الاستعراض، ولا يكون مناسباً إلا لمواقف معينة محدودة. نوصي بإبقاء هذا الخيار ممكّناً.

مراسلة في المنتج

تم تصميم المراسلة في المنتج لإعلام المستخدمين بأخبار ESET وغيرها من الاتصالات. يتطلب إرسال رسائل تسويقية موافقة المستخدم. ومن ثمّ، لا يتم إرسال الرسائل التسويقية إلى أي مستخدم بشكل افتراضي (تظهر كعلامة تعجب). من خلال تمكين هذا الخيار، أنت بذلك توافق على تلقي رسائل ESET التسويقية. وإذا لم تكن ترغب في تلقي مواد ESET التسويقية، فقم بتعطيل خيار **عرض رسائل تسويقية**.

مربعات الرسائل

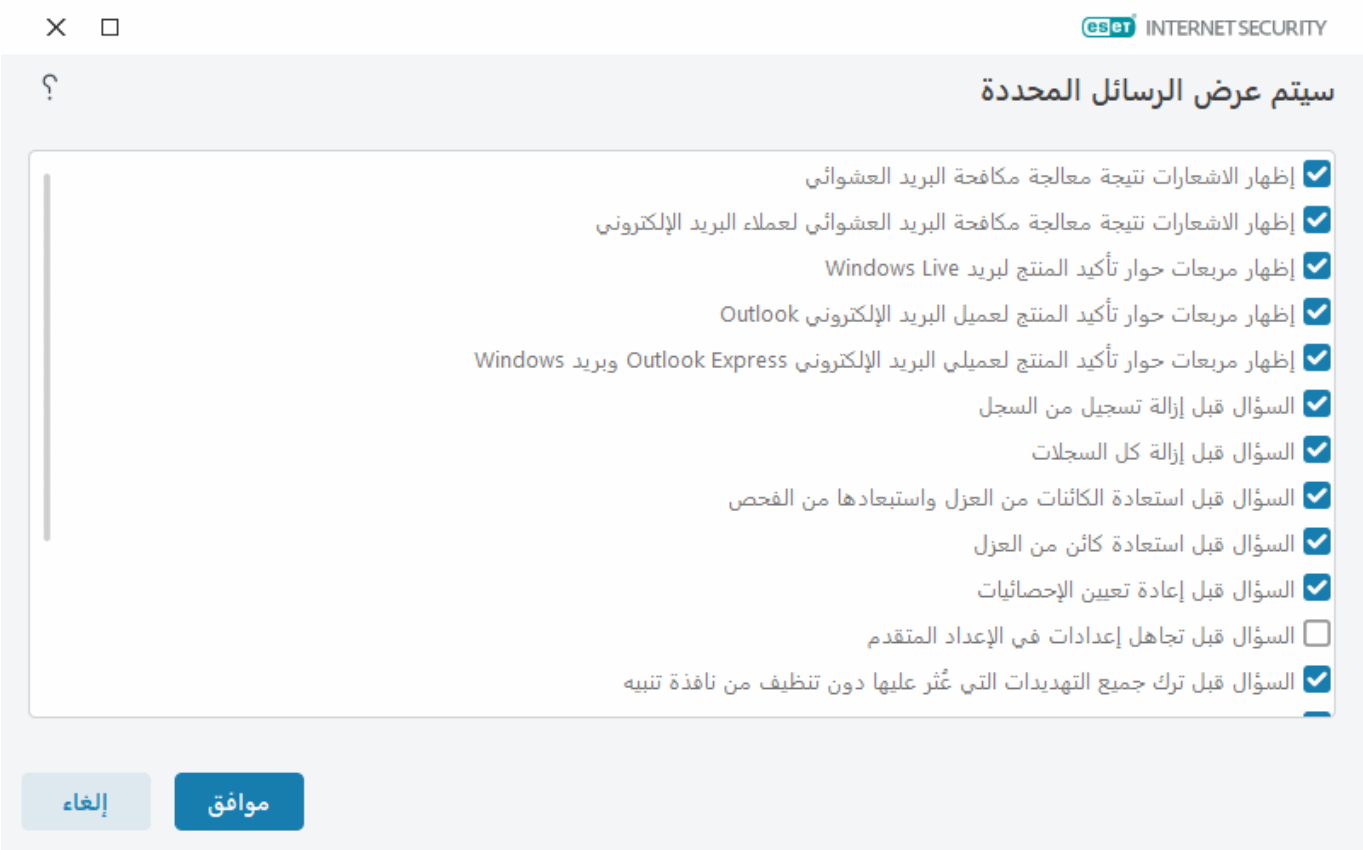
لإغلاق مربعات الرسائل تلقائياً بعد وقت معين، حدد **غلق مربعات الرسائل تلقائياً**. إذا لم يتم إغلاق نوافذ التنبيهات يدوياً، فيتم إغلاقها تلقائياً بعد انقضاء الوقت المحدد.

عرض الوقت بالثواني – قم بتعيين مدة رؤية التنبيه. يجب أن تكون القيمة بين 10–999 ثانية.

رسائل التأكيد – انقر فوق **تحرير** لعرض قائمة برسائل التأكيد التي يمكنك تحديد عرضها أو عدم عرضها.

رسائل التأكيد

لضبط رسائل التأكيد، انتقل إلى الإعداد المتقدم > **الإعلامات** > **التنبيهات التفاعلية** وانقر فوق **تحرير** بجوار **رسائل التأكيد**.



تعرض نافذة الحوار هذه رسائل تأكيد تفيد بأن ESET Internet Security سيتم عرضه قبل اتخاذ أي إجراء. قم بتحديد خانة الاختيار الموجودة بجوار كل رسالة تأكيد أو إلغاء تحديدها للسماح به أو تعطيله.

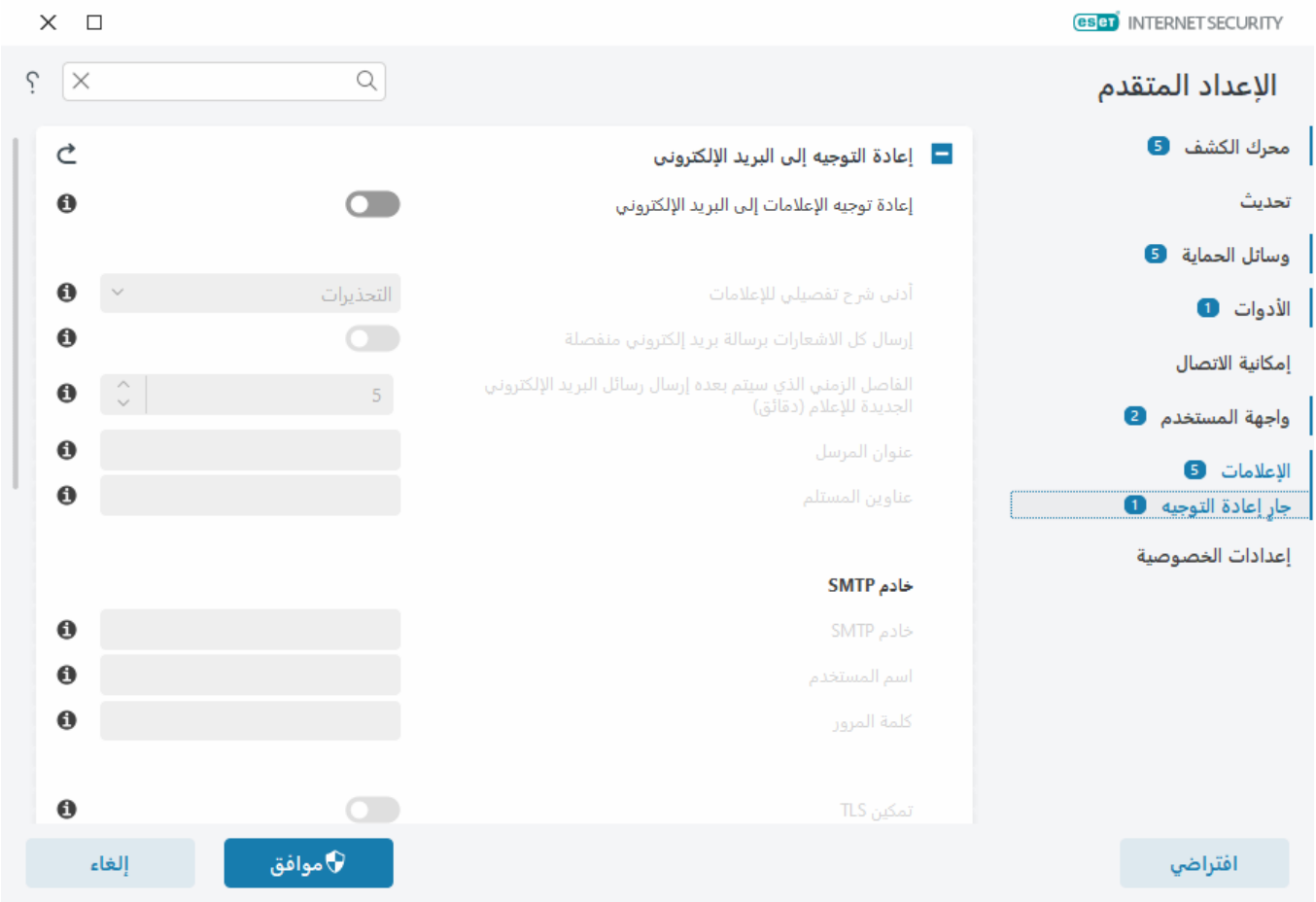
معرفة المزيد حول ميزة محددة متعلقة برسائل التأكيد:

- السؤال قبل حذف سجلات ESET SysInspector
- السؤال قبل حذف كل سجلات ESET SysInspector
- السؤال قبل حذف كائن من العزل
- السؤال قبل تجاهل إعدادات في الإعداد المتقدم
- السؤال قبل ترك جميع التهديدات التي عُثر عليها دون تنظيف من نافذة تنبيه
- السؤال قبل إزالة تسجيل من السجل
- سؤال قبل إزالة مهمة مجدولة في المجدول
- السؤال قبل إزالة كل السجلات
- السؤال قبل إعادة تعيين الإحصائيات
- السؤال قبل استعادة كائن من العزل
- السؤال قبل استعادة الكائنات من العزل واستبعادها من الفحص
- السؤال قبل تشغيل مهمة مجدولة في المجدول
- إظهار الاشعارات نتيجة معالجة مكافحة البريد العشوائي

- إظهار الاشعارات نتيجة معالجة مكافحة البريد العشوائي لعملاء البريد الإلكتروني
- إظهار مربعات حوار تأكيد المنتج لعميلي البريد الإلكتروني Outlook Express و بريد Windows
- إظهار مربعات حوار تأكيد المنتج لبريد Windows Live
- إظهار مربعات حوار تأكيد المنتج لعميل البريد الإلكتروني Outlook

جارٍ إعادة التوجيه

يمكن أن يقوم ESET Internet Security بإرسال رسائل بريد إلكتروني للإعلام تلقائياً في حالة وقوع حدث بمستوى الشرح التفصيلي المحدد. قم بفتح الإعداد المتقدم > **الإعلامات** > **إعادة التوجيه** وتمكين **إعادة توجيه الإعلامات إلى البريد الإلكتروني** لتنشيط رسائل البريد الإلكتروني للإعلام.



من القائمة المنسدلة **أدنى شرح تفصيلي للإعلامات**، يمكنك تحديد مستوى الخطورة الأولي للإعلامات المطلوب إرسالها.

- **التشخيص** ـ لتسجيل معلومات مطلوبة لضبط البرنامج وجميع السجلات الواردة أعلاه.
- **إخباري** ـ لتسجيل رسائل معلوماتية، مثل أحداث الشبكة غير القياسية، بما في ذلك رسائل التحديث الناجح، إضافة إلى جميع السجلات الواردة أعلاه.
- **التحذيرات**—لتسجيل رسائل الخطأ والتحذير الحرجة (على سبيل المثال: فشل التحديث).
- **أخطاء** ـ سيتم تسجيل الأخطاء (لم يتم بدء حماية المستندات) والأخطاء الحرجة.
- **حرج** ـ لتسجيل الأخطاء الحرجة فقط (على سبيل المثال، خطأ أثناء بدء الحماية ضد الفيروسات، أو التهديد الذي عُثر عليه).

إرسال كل إعلام برسالة بريد إلكتروني منفصلة ـ عند تمكين هذا الخيار، يتلقى المستلم رسالة بريد إلكتروني جديدة لكل إعلام. قد يؤدي هذا إلى استلام العديد من رسائل البريد الإلكتروني خلال فترة قصيرة.

الفاصل الزمني الذي سيتم بعده إرسال رسائل البريد الإلكتروني الجديدة للإعلام (دقائق) ـ الفاصل الزمني بالدقائق الذي سيتم بعده إرسال إعلامات جديدة إلى البريد الإلكتروني. إذا قمت بتعيين هذه القيمة على 0، فسيتم إرسال الإعلامات على الفور.

عنوان المرسل ـ يحدد عنوان المرسل الذي سيُعرض في رأس رسائل البريد الإلكتروني الخاصة بالإعلام.

عناوين المستلم ـ يحدد عناوين المستلم المعروضة في رأس رسائل البريد الإلكتروني الخاصة بالإعلام. يتم دعم العديد من القيم. الرجاء استخدام الفاصلة المنقوطة كفاصل.

خادم SMTP

خادم SMTP – خادم SMTP المستخدم لإرسال الإشعارات (على سبيل المثال، منفذ smtp.provider.com:587, المحدد مسبقاً هو 25).

يتم دعم خوادم SMTP المزودة بتشفير TLS بواسطة ESET Internet Security.

اسم المستخدم و**كلمة المرور** ـ إذا تطلب خادم SMTP مصادقة، فيجب ملء هذين الحقلين باسم مستخدم وكلمة مرور صحيحين للوصول إلى خادم SMTP.

تمكين TLS – تنبيه آمن وإشعارات استخدام تشفير TLS.

اختبار اتصال SMTP – سيتم إرسال بريد إلكتروني تجريبي إلى عنوان البريد الإلكتروني للمستلم. يجب ملء خادم SMTP واسم المستخدم وكلمة المرور وعنوان المرسل وعناوين المستلم.

تنسيق الرسالة

يتم إجراء الاتصالات بين البرنامج ومستخدم بعيد أو مسؤول نظام عبر رسائل البريد الإلكتروني أو رسائل شبكة LAN (باستخدام خدمة المراسلة في Windows). سيكون **استخدام تنسيق الرسالة الافتراضية** لرسائل التنبيهات والإعلامات هو الأمثل لمعظم المواقف. وفي بعض الأحوال، قد تحتاج إلى تغيير تنسيق الرسالة لرسائل الأحداث.

تنسيق رسائل الحدث ـ تنسيق رسائل الحدث التي تُعرض على أجهزة كمبيوتر بعيدة.

تنسيق رسائل التحذير من التهديدات– لرسائل التنبيهات والإعلامات بالتهديدات تنسيق افتراضي محدد مسبقاً. نوصي بإبقاء التنسيق المحدد مسبقاً. ولكن، في بعض الأحيان (إذا كان لديك نظام معالجة بريد إلكتروني تلقائي مثلاً)، قد تحتاج إلى تغيير تنسيق الرسائل.

مجموعة الأحرف – لتحويل رسالة بريد إلكتروني إلى ترميز أحرف ANSI بناءً على الإعدادات الإقليمية لنظام Windows (على سبيل المثال windows-1250 أو Unicode (UTF-8) أو ACSII 7-bit أو اليابانية (ISO-2022-JP)). ونتيجة لذلك، سيتم تغيير "á" إلى "a" ورمز غير معروف إلى "?".

استخدام الترميز المقتبس القابل للطباعة ـ سيتم ترميز مصدر رسالة البريد الإلكتروني إلى تنسيق QP (Quoted-printable)

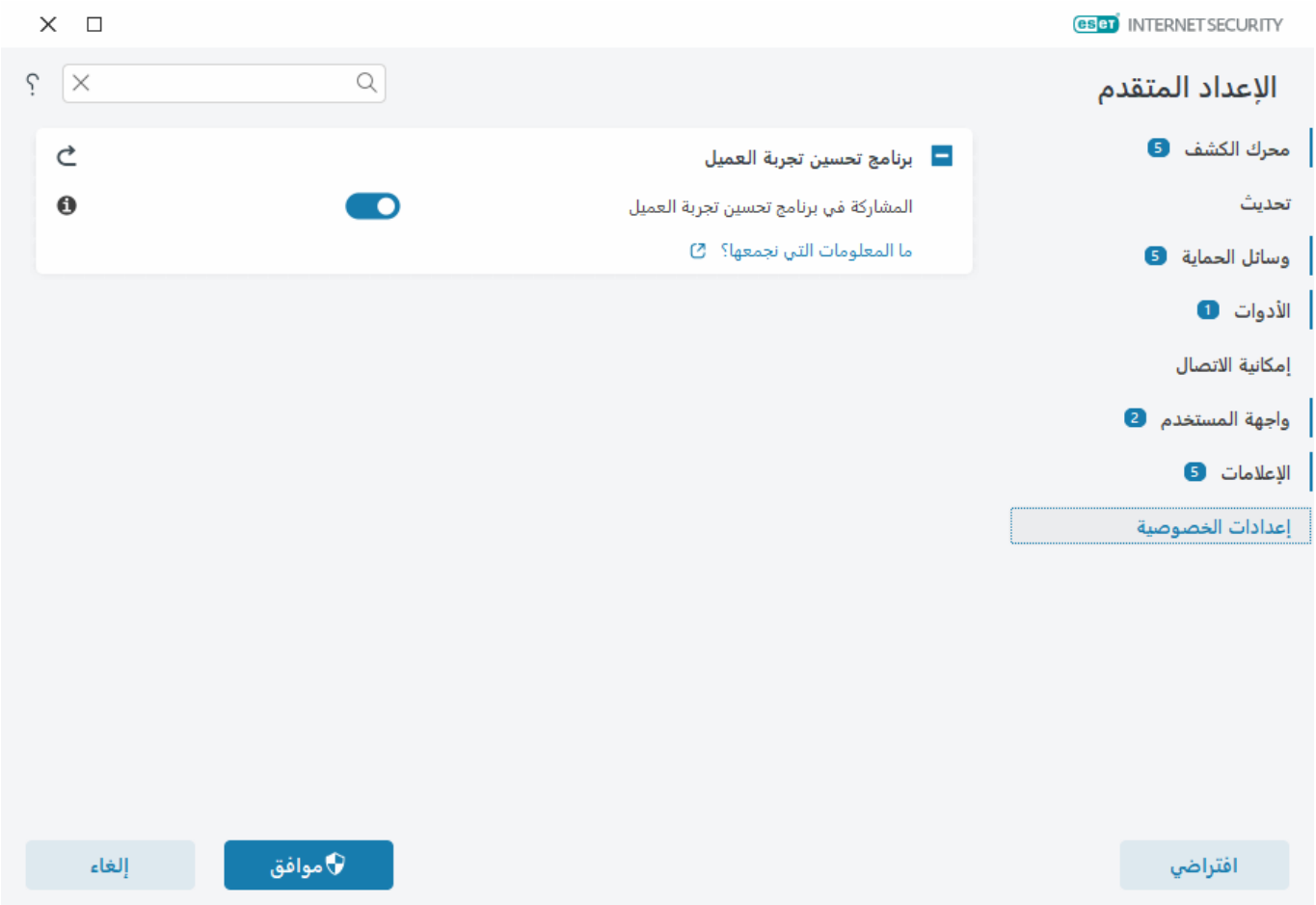
الذي يستخدم أحرف ASCII ويمكنه نقل أحرف وطنية خاصة بالبريد الإلكتروني بتنسيق 8-بت (áéíóú).

- **%TimeStamp%** – تاريخ الحدث ووقته
- **%Scanner%** – الوحدة المعنية
- **%ComputerName%** – اسم الكمبيوتر الذي حدث عليه التنبيه
- **%ProgramName%** – البرنامج الذي أصدر التنبيه
- **%InfectedObject%** – اسم الملف أو الرسالة المصابة أو ما إلى ذلك.
- **%VirusName%** – تحديد الإصابة
- **%Action%** – الإجراء المتخذ في حالة التسلل
- **%ErrorDescription%** – وصف لحدث ليس فيروساً

لا تُستخدم الكلمتان الأساسيتان **%InfectedObject%** و**%VirusName%** إلا في رسائل التحذير من التهديدات، كما لا تُستخدم **%ErrorDescription%** إلا في رسائل الأحداث.

إعدادات الخصوصية

افتح الإعداد المتقدم > **إعدادات الخصوصية**.



برنامج تحسين تجربة العميل

قم بتمكين مفتاح التبديل بجوار **المشاركة في برنامج تحسين تجربة العميل** للانضمام إلى برنامج تحسين تجربة العميل. من خلال الانضمام إلى "برنامج تحسين تجربة العميل"، أنت بذلك تزود ESET بمعلومات مجهولة تتعلق باستخدام منتجات ESET. ستساعدنا البيانات التي يتم جمعها في تحسين تجربتك ولن تتم مشاركتها أبداً مع جهات خارجية. ما المعلومات التي نجمعها؟

إرجاع للإعدادات الافتراضية

انقر فوق **افتراضي** في الإعداد المتقدم لإعادة تعيين جميع إعدادات البرنامج، لكل الوحدات. إلى الحالة التي كانت عليها بعد إجراء تثبيت جديد.

راجع أيضاً استيراد الإعدادات وتصديرها.

إرجاع كل الإعدادات في القسم الحالي

انقر فوق سهم التقويس للعودة بكل الإعدادات في القسم الحالي إلى الإعدادات الافتراضية المحددة بواسطة ESET.

الرجاء ملاحظة أن أي تغييرات أُجريت ستُفقد بعد النقر فوق **إرجاع للافتراضي**.

إرجاع محتويات الجداول – عند تمكين هذا الخيار، ستُفقد المهام أو ملفات التعريف التي تمت إضافتها يدوياً أو تلقائياً.

راجع أيضاً استيراد الإعدادات وتصديرها.

حدث خطأ أثناء حفظ التكوين

تشير رسالة الخطأ هذه إلى أن الإعدادات لم تُحفظ بشكل صحيح بسبب حدوث خطأ.

هذا يعني عادة أن المستخدم الذي حاول تعديل معلمات البرنامج:

- يمتلك حقوق وصول غير كافية أو ليس لديه امتيازات نظام التشغيل اللازمة المطلوبة لتعديل ملفات التكوين وسجل النظام.
  > لإجراء التعديلات المطلوبة، يجب على مسؤول النظام تسجيل الدخول.
- قام مؤخراً بتمكين وضع التعلم في HIPS أو جدار الحماية ومحاولة إجراء تغييرات على الإعداد المتقدم.
  > لحفظ التكوين وتجنب تعارض التكوين، أغلق الإعداد المتقدم دون حفظ ومحاولة إجراء التغييرات المطلوبة مرة أخرى.

وربما تكون الحالة الثانية الأكثر شيوعاً أن البرنامج لم يعد يعمل بشكل سليم، أو تلف ويحتاج إلى إعادة تثبيت نتيجة لذلك.

فاحص سطر الأوامر

يمكن تشغيل وحدة الحماية ضد الفيروسات في ESET Internet Security عبر سطر الأوامر – يدوياً (باستخدام الأمر "ecls") أو باستخدام ملف دفعي ("bat").

استخدام الماسح الضوئي لسطر أوامر ESET:

```
..ecls [OPTIONS..] FILES
```

يمكن استخدام المعلمات ومفاتيح التبديل التالية أثناء تشغيل برنامج الفحص عند الطلب من سطر الأوامر:

الخيارات

تحميل وحدات نمطية من FOLDER	base-dir=FOLDER/
عزل FOLDER	quar-dir=FOLDER/
استبعاد الملفات المطابقة لقناع MASK من الفحص	exclude=MASK/
فحص المجلدات الفرعية (افتراضي)	subdir/
عدم فحص المجلدات الفرعية	no-subdir/
الحد الأقصى للمستوى الفرعي للمجلدات داخل المجلدات المطلوب فحصها	max-subdir-level=LEVEL/
اتباع الارتباطات الرمزية (افتراضي)	symlink/
تخطي الارتباطات الرمزية	no-symlink/
فحص الإعلانات (افتراضي)	ads/
عدم فحص الإعلانات	no-ads/
تسجيل المخرجات في FILE	log-file=FILE/
الكتابة فوق ملف الإخراج (افتراضي – إلحاق)	log-rewrite/
تسجيل المخرجات في وحدة التحكم (افتراضي)	log-console/
عدم تسجيل المخرجات في وحدة التحكم	no-log-console/
تسجيل الملفات النظيفة أيضاً	log-all/
عدم تسجيل الملفات النظيفة (افتراضي)	no-log-all/
إظهار مؤشر النشاط	aind/
الفحص والمسح التلقائي لجميع الأقراص المحلية	auto/

خيارات برنامج الفحص

فحص الملفات (افتراضي)	files/
عدم فحص الملفات	no-files/
فحص الذاكرة	memory/
فحص قطاعات التشغيل	boots/
عدم فحص قطاعات التشغيل (افتراضي)	no-boots/
فحص الأرشيفات (افتراضي)	arch/
عدم فحص الأرشيفات	no-arch/
فحص الملفات الأصغر من SIZE ميجابايت فقط (الافتراضي 0 = غير محدود)	max-obj-size=SIZE/
الحد الأقصى للمستوى الفرعي للأرشيفات داخل الأرشيفات (الأرشيفات المتداخلة) المطلوب فحصها	max-arch-level=LEVEL/
فحص الأرشيفات لمدة LIMIT ثوانٍ كحد أقصى	scan-timeout=LIMIT/
عدم فحص إلا الملفات داخل أرشيف إذا كانت الملفات أصغر من SIZE (افتراضي 0 = غير محدود)	max-arch-size=SIZE/
فحص الملفات الموجودة في أرشيف ذاتي الاستخراج إذا كانت أصغر من SIZE ميجابايت (الافتراضي 0 = غير محدود)	max-sfx-size=SIZE/
فحص ملفات البريد الإلكتروني (افتراضي)	mail/
عدم فحص ملفات البريد الإلكتروني	no-mail/
فحص علب البريد (افتراضي)	mailbox/
عدم فحص علب البريد	no-mailbox/
فحص الأرشيفات ذاتية الاستخراج (افتراضي)	sfx/
عدم فحص الأرشيفات ذاتية الاستخراج	no-sfx/

فحص حزم وقت التشغيل (افتراضي)	rtp/
عدم فحص حزم وقت التشغيل	no-rtp/
فحص التطبيقات المحتمل أن تكون غير آمنة	unsafe/
عدم فحص التطبيقات المحتمل أن تكون غير آمنة (افتراضي)	no-unsafe/
فحص التطبيقات المحتمل أن تكون غير مرغوب فيها	unwanted/
عدم فحص التطبيقات المحتمل أن تكون غير مرغوب فيها (افتراضي)	no-unwanted/
فحص التطبيقات المريبة (افتراضي)	suspicious/
عدم فحص التطبيقات المريبة	no-suspicious/
استخدام التوقيعات (افتراضي)	pattern/
عدم استخدام التوقيعات	no-pattern/
تمكين الأساليب البحثية (افتراضي)	heur/
تعطيل الأساليب البحثية	no-heur/
تمكين الأساليب البحثية المتقدمة (افتراضي)	adv-heur/
تعطيل الأساليب البحثية المتقدمة	no-adv-heur/
استبعاد الامتدادات المحددة بعلامة النقطتين من الفحص	ext-exclude=EXTENSIONS/
استخدام وضع التنظيف MODE للكائنات المصابة تتوفر الخيارات التالية: • لا شيء (افتراضي) – لن يحدث تنظيف تلقائي. • standard – سيحاول ecls.exe تنظيف الملفات المصابة أو حذفها تلقائياً. • strict – سيحاول ecls.exe تنظيف الملفات المصابة أو حذفها تلقائياً دون تدخل المستخدم (لن تتم مطالبتك قبل حذف الملفات). • rigorous – سيحذف ecls.exe ملفات دون محاولة تنظيفها، بصرف النظر عن نوع الملف. • delete – سيحذف ecls.exe الملفات دون محاولة تنظيفها، لكنه لن يحذف الملفات الحساسة كملفات نظام Windows.	clean-mode=MODE/
نسخ الملفات المصابة (في حالة تنظيفها) إلى منطقة العزل (مكمِّل للإجراء المنفذ أثناء التنظيف)	quarantine/
عدم نسخ الملفات المصابة في منطقة العزل	no-quarantine/

خيارات عامة

إظهار التعليمات والخروج	help/
إظهار معلومات الإصدار والخروج	version/
المحافظة على الطابع الزمني للوصول الأخير	preserve-time/

رموز الإنهاء

لم يتم العثور على أي تهديد	0
تم اكتشاف تهديد وتنظيفه	1
يتعذر فحص بعض الملفات (ربما تكون تهديدات)	10
تم العثور على تهديد	50
خطأ	100

تعني رموز الإنهاء الأكبر من 100 أن الملف لم يتم فحصه، ولذلك يمكن أن يكون مصاباً.

الأسئلة الشائعة

يمكنك العثور على بعض الأسئلة المتداولة والمشكلات التي تتم مواجهتها أدناه. انقر فوق عنوان الموضوع لتتعرف على كيفية حل مشكلتك:

- كيفية تحديث ESET Internet Security
- اكتشف ESET Internet Security تهديداً
- كيفية إزالة فيروس من الكمبيوتر
- كيفية السماح بالاتصال لتطبيق معين
- كيفية تمكين المراقبة الأبوية لحساب

- كيفية إنشاء مهمة جديدة في المجدول
- كيفية جدولة مهمة الفحص (أسبوعياً)
- كيفية إلغاء تأمين الإعداد المتقدم
- كيفية حل إلغاء تنشيط المنتج من ESET HOME

إذا لم تكن مشكلتك موجودة في القائمة أعلاه، فحاول البحث في تعليمات ESET Internet Security عبر الإنترنت.

إذا لم تتمكن من العثور على حل لمشكلتك/سؤالك في تعليمات ESET Internet Security عبر الإنترنت، فيمكنك زيارة قاعدة معارف ESET على الإنترنت التي يتم تحديثها بانتظام. ارتباطات أكثر مقالات قواعد المعرفة الخاصة بنا انتشاراً مدرجة بالأسفل:

- كيف أجدد اشتراكي؟
- ظهر لي خطأ في التنشيط أثناء تثبيت منتج ESET الخاص بي. ماذا يعني هذا؟
- تنشيط منتج ESET Windows المنزلي الخاص بي باستخدام مفتاح التنشيط
- إلغاء تثبيت أو إعادة تثبيت لمنتج ESET المنزلي
- تظهر لي رسالة تفيد بإنهاء تثبيت ESET الخاص بي قبل الأوان
- ما الذي على فعله بعد تجديد اشتراكي؟ (مستخدمو الشبكات المنزلية)
- ماذا لو غيرتُ عنوان بريدي الإلكتروني؟
- نقل منتج ESET إلى جهاز كمبيوتر أو جهاز جديد
- كيفية بدء تشغيل Windows في الوضع الآمن أو الوضع الآمن مع تصفح الشبكة
- استبعاد موقع ويب آمن من الحظر
- السماح بالوصول لبرنامج برامج قراءة الشاشة إلى ESET GUI

متى لزم الأمر، يمكنك الاتصال بالدعم التقني لطرح أسئلتك أو مناقشة مشكلاتك.

كيفية تحديث ESET Internet Security

يمكن إجراء تحديث ESET Internet Security إما يدوياً أو تلقائياً. لتشغيل التحديث، انقر فوق **تحديث** في النافذة الرئيسية للبرنامج ثم انقر فوق **التحقق من وجود تحديثات**.

تنشئ إعدادات التثبيت الافتراضية مهمة تحديث تلقائية يتم تنفيذها كل ساعة. إذا كنت تريد تغيير الفاصل الزمني، فالرجاء الانتقال إلى **الأدوات** > المجدول.

كيفية إزالة فيروس من الكمبيوتر

إذا كانت تظهر على الكمبيوتر أعراض إصابة ببرامج ضارة، مثل بطء أدائه أو عدم استجابته باستمرار، فيوصى بالقيام بما يلي:

1. في نافذة البرنامج الرئيسية، انقر فوق **فحص جهاز الكمبيوتر**.
2. انقر فوق **فحص الكمبيوتر** لبدء فحص نظامك.
3. بعد انتهاء الفحص، راجع السجل الذي يضم عدد الملفات التي شملها الفحص والمصابة والتي تم تنظيفها.
4. إذا كنت تريد فحص جزء محدد فقط من القرص، انقر فوق **الفحص المخصص** وحدد أهدافاً يتم فحصها بحثاً عن

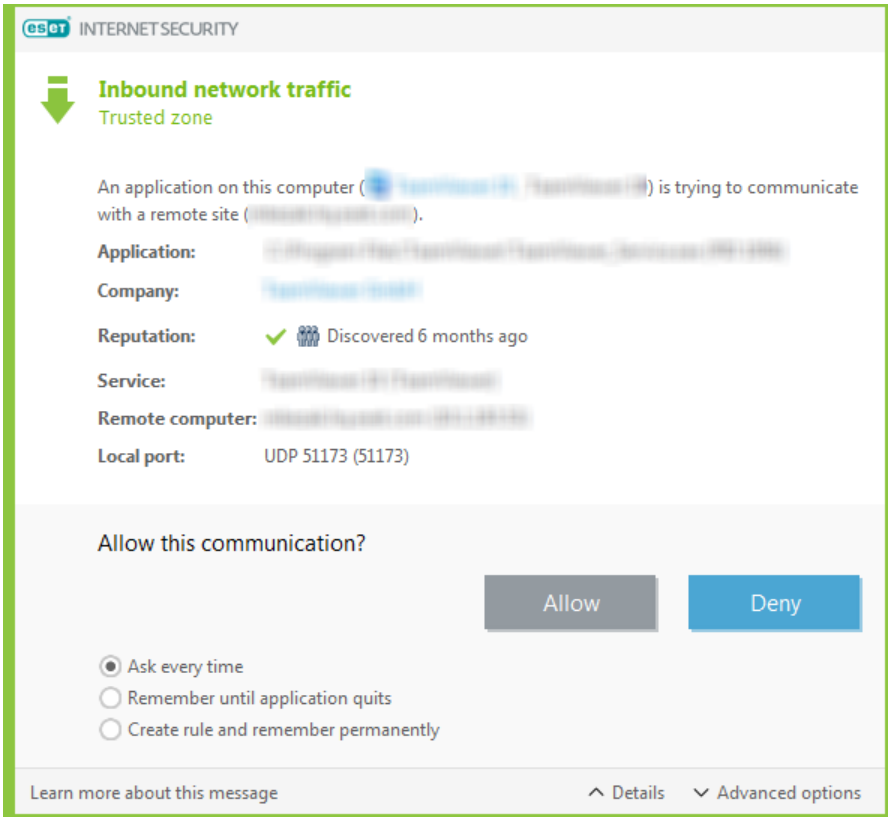
فيروسات.

للحصول على معلومات إضافية، راجع:

- مقالة قاعدة المعرفة ESET
- العزل

كيفية السماح بالاتصال لتطبيق معين

في حالة اكتشاف اتصال جديد في الوضع التفاعلي وعدم وجود قاعدة مطابقة، ستتم مطالبتك **بالسماح** بالاتصال أو **رفضه**. إذا كنت تريد أن يتخذ ESET Internet Security الإجراء نفسه كلما حاول التطبيق إنشاء اتصال، فحدد خانة الاختيار **قم بإنشاء قاعدة وتذكرها دائماً**.



في إعداد جدار الحماية، يمكنك إنشاء قواعد جدار حماية جديدة للتطبيقات قبل اكتشافها بواسطة ESET Internet Security.
افتح نافذة البرنامج الرئيسية > **الإعداد** > **حماية الشبكة** > انقر فوق ⚙ التالي **جدار الحماية** > **التهيئة** > **الإعدادات المتقدمة** > **القواعد** > **تحرير**.

انقر فوق زر **إضافة** وفي علامة التبويب **عام**، أدخل الاسم والاتجاه وبروتوكول الاتصال للقاعدة. تسمح لك هذه النافذة بتحديد الإجراء المطلوب اتخاذه عند تطبيق القاعدة.

أدخل المسار إلى الملف التنفيذي للتطبيق، ومنفذ الاتصال المحلي في علامة التبويب **محلي**. انقر فوق علامة التبويب **بعيد** لإدخال العنوان والمنفذ البعيدين (إن أمكن). سيتم تطبيق القاعدة المنشأة حديثاً بمجرد محاولة التطبيق إعادة الاتصال.

كيفية تمكين المراقبة الأبوية لحساب

لتنشيط المراقبة الأبوية لحساب مستخدم محدد، اتبع الخطوات أدناه:

1. بشكلٍ افتراضي، يتم تعطيل ميزة المراقبة الأبوية في ESET Internet Security. توجد طريقتان لتنشيط ميزة المراقبة الأبوية:

- انقر فوق أيقونة التبديل في القسم **إعداد** > **حماية الإنترنت** > **الرقابة الأبوية** من نافذة البرنامج الرئيسية وقم بتغيير حالة الرقابة الأبوية إلى ممكَّنة.
- افتح الإعداد المتقدم > **وسائل الحماية** > **حماية الوصول إلى الويب** > **الرقابة الأبوية** ثم قم بتمكين التبديل بجوار **تمكين الرقابة الأبوية**.

2. انقر فوق **إعداد** > **حماية الإنترنت** > **المراقبة الأبوية** من نافذة البرنامج الرئيسية. على الرغم من ظهور الحالة **ممكَّنة** بجوار **المراقبة الأبوية**، يجب تكوين ميزة المراقبة الأبوية للحساب المطلوب من خلال النقر فوق رمز أحد الصفوف ثم في النافذة التالية حددحماية **حساب الأطفال** أو **حساب ولي الأمر**. في النافذة التالية حدد تاريخ الميلاد لتحديد مستوى الوصول وصفحات الويب المناسبة لذلك العمر والموصى بها. سيتم الآن تمكين المراقبة الأبوية لحساب المستخدم المحدد. انقر فوق **المحتوى الممنوع والإعدادات** الموجود ضمن اسم حساب لتخصيص الفئات التي تريد السماح بها أو حظرها في علامة التبويب الفئات. للسماح بصفحات ويب مخصصة أو حظرها، مع مراعاة ألا تكون هذه الصفحات مطابقة لأي فئة، انقر فوق علامة التبويب الاستثناءات.

كيفية إنشاء مهمة جديدة في المجدول

لإنشاء مهمة جديدة في **الأدوات > المجدول**، انقر فوق **إضافة مهمة** أو انقر بزر الماوس الأيمن وحدد **إضافة** من القائمة السياقية. تتوفر خمسة أنواع من المهام المجدولة:

- **تشغيل التطبيق الخارجي** – لجدولة تنفيذ تطبيق خارجي.
- **صيانة السجل** – تحتوي ملفات السجل كذلك على بقايا من السجلات المحذوفة. وهذه المهمة تعمل على تحسين السجلات في ملفات السجل بشكل دوري حتى تعمل بشكل فعال.
- **فحص ملفات بدء تشغيل النظام** – لفحص الملفات المسموح بتشغيلها عند بدء تشغيل النظام أو تسجيل الدخول.
- **إنشاء فحص كمبيوتر** – إنشاء لقطة سريعة لبرنامج ESET SysInspector على الكمبيوتر، جمع معلومات تفصيلية عن مكونات النظام (مثل برامج التشغيل، التطبيقات) وتقييم مستوى خطورة كل مكون.
- **فحص الكمبيوتر عند الطلب** – إجراء فحص ملفات ومجلدات على الكمبيوتر.
- **تحديث** – لجدولة مهمة تحديث عن طريق تحديث الوحدات.

نظراً لأن **التحديث** هو أحد المهام المجدولة الأكثر استخداماً، فسنوضح كيفية إضافة مهمة تحديث جديدة أدناه:

من القائمة المنسدلة **مهمة مجدولة**، حدد **التحديث**. أدخل اسماً للمهمة في الحقل **اسم المهمة** وانقر فوق **التالي**. حدد تكرار المهمة. تتوفر الخيارات التالية: **مرة واحدة** و**بشكلٍ متكرر** و**يومياً** و**أسبوعياً** و**منشئ الأحداث**. حدد **تجاوز المهمة عند العمل على طاقة البطارية** لتقليل استهلاك موارد النظام عندما يعمل الكمبيوتر المحمول بطاقة البطارية. سيتم تشغيل المهمة في التاريخ والوقت المحددين في حقول **تنفيذ المهام**. بعد ذلك، حدد الإجراء المطلوب اتخاذه إذا تعذر إجراء المهمة أو إكمالها في الوقت المجدول لها. تتوفر الخيارات التالية:

- **في الوقت المجدول التالي**
- **بأقرب ما يمكن**
- **فوراً، إذا تجاوز الوقت منذ آخر تشغيل قيمة معينة** (يمكن تحديد الفاصل باستخدام مربع التمرير **الوقت منذ آخر تشغيل**)

وفي الخطوة التالية، يتم عرض نافذة ملخص تشمل معلومات حول المهمة المجدولة الحالية. انقر فوق **إنهاء** عند الانتهاء من إجراء التغييرات.

ستظهر نافذة حوار، تتيح لك تحديد ملفات التعريف الواجب استخدامها للمهمة المجدولة. ومنها يمكنك تعيين ملف التعريف الرئيسي والبديل. يُستخدم ملف التعريف الرئيسي إذا تعذر إكمال المهمة باستخدام ملف التعريف الرئيسي. قم بتأكيد ذلك بالنقر فوق **إنهاء** وستتم إضافة المهمة المجدولة الجديدة إلى قائمة المهام المجدولة حالياً.

كيفية جدولة فحص أسبوعي للكمبيوتر

لجدولة مهمة منتظمة، افتح نافذة البرنامج الرئيسية وانقر فوق **الأدوات > الجدولة**. يمكنك فيما يلي العثور على دليل مختصر لكيفية جدولة مهمة ستقوم بفحص محركات الأقراص المحلية لديك كل أسبوع. لمزيد من التعليمات التفصيلية، راجع قاعدة المعارف لدينا على الرابط التالي: Knowledgebase article.

لجدولة مهمة فحص:

1. انقر فوق **إضافة** في شاشة المجدول الرئيسية.
2. أدخل اسماً للمهمة وحدد **فحص جهاز الكمبيوتر عند الطلب** من القائمة المنسدلة **نوع المهمة**.
3. حدد **أسبوعياً** لتكرار المهمة.
4. حدد الوقت واليوم الذي تريد فيه تنفيذ المهمة.
5. حدد **تشغيل المهمة في أقرب وقت ممكن** لأداء المهمة في وقتٍ لاحق إذا لم يتم تشغيل المهمة لأي سبب (على سبيل المثال، في حالة إيقاف تشغيل الكمبيوتر).
6. راجع ملخص المهمة المجدولة وانقر فوق **إنهاء**.
7. من القائمة المنسدلة **الأهداف**، حدد **محركات الأقراص المحلية**.
8. انقر فوق **إنهاء** لتطبيق المهمة.

كيفية إلغاء تأمين الإعداد المتقدم المحمي بكلمة مرور

عندما تريد الوصول إلى الإعداد المتقدم المحمي، يتم عرض نافذة لإدخال كلمة المرور. وإذا نسيت كلمة المرور أو فقدتها، فانقر فوق **استعادة كلمة المرور** واكتب عنوان البريد الإلكتروني الذي استخدمته لتسجيل الاشتراك. يرسل ESET رسالة بريد إلكتروني بها رمز التحقق. اكتب رمز التحقق ثم اكتب كلمة المرور الجديدة وقم بتأكيدها. رمز التحقق صالح لمدة سبعة أيام.

استعادة كلمة المرور عبر حساب ESET HOME – استخدم هذا الخيار إذا كان اشتراك المستخدم للتنشيط مرتبطاً بحساب ESET HOME. اكتب عنوان البريد الإلكتروني الذي تستخدمه لتسجيل الدخول إلى حساب ESET HOME.

إذا كان يتعذر عليك تذكر عنوان البريد الإلكتروني أو تواجه صعوبات في استعادة كلمة المرور، فانقر فوق **الاتصال بالدعم الفني**. وسيتم إعادة توجيهك إلى موقع ESET على الويب للاتصال بقسم الدعم الفني.

إنشاء رمز للدعم الفني – ينشئ هذا الخيار رمزاً للدعم الفني. انسخ الرمز المتوفر من "الدعم الفني" وانقر فوق **لديّ رمز تحقق**. اكتب رمز التحقق ثم اكتب كلمة المرور الجديدة وقم بتأكيدها. رمز التحقق صالح لمدة سبعة أيام.

لمزيد من المعلومات، راجع إلغاء تأمين كلمة مرور الإعدادات في منتجات الصفحة الرئيسية من ESET Windows.

كيفية حل إلغاء تنشيط المنتج من ESET HOME

لم يتم تنشيط المنتج

تظهر رسالة الخطأ هذه عند إلغاء تنشيط مالك الاشتراك ESET Internet Security من بوابة ESET HOME أو أن الاشتراك الذي تمت مشاركته مع حساب ESET HOME لم يعد مشتركاً. لحل هذه المشكلة:

- انقر فوق **تنشيط** واستخدم إحدى طرق التنشيط لتنشيط ESET Internet Security.
- اتصل بمالك الاشتراك وأبلغه بمعلومات حول أنه تم إلغاء تنشيط ESET Internet Security من قبل مالك الاشتراك أو أن الاشتراك لم يعد مشتركاً معك. يمكن للمالك حل المشكلة في ESET HOME.

تم إلغاء تنشيط المنتج، تم قطع اتصال الجهاز

تظهر رسالة الخطأ هذه بعد إزالة جهاز من حساب ESET HOME. لحل هذه المشكلة:

- انقر فوق **تنشيط** واستخدم إحدى طرق التنشيط لتنشيط ESET Internet Security.
- اتصل بمالك الاشتراك وأبلغه بمعلومات حول أنه تم إلغاء تنشيط ESET Internet Security وتم قطع اتصال الجهاز من ESET HOME.
- إذا كنت مالك اشتراك وغير مدرك لهذه التغييرات، فراجع موجز نشاط ESET HOME. إذا وجدت أي نشاط مريب، فقم بتغيير كلمة مرور حساب ESET HOME وواتصل بالدعم الفني لـESET.

تم إلغاء تنشيط المنتج، تم قطع اتصال الجهاز

تظهر رسالة الخطأ هذه بعد إزالة جهاز من حساب ESET HOME. لحل هذه المشكلة:

- انقر فوق **تنشيط** واستخدم إحدى طرق التنشيط لتنشيط ESET Internet Security.
- اتصل بمالك الاشتراك وأبلغه بمعلومات حول أنه تم إلغاء تنشيط ESET Internet Security وتم قطع اتصال الجهاز من ESET HOME.
- إذا كنت مالك اشتراك وغير مدرك لهذه التغييرات، فراجع موجز نشاط ESET HOME. إذا وجدت أي نشاط مريب، فقم بتغيير كلمة مرور حساب ESET HOME وواتصل بالدعم الفني لـESET.

لم يتم تنشيط المنتج

تظهر رسالة الخطأ هذه عند إلغاء تنشيط مالك الاشتراك ESET Internet Security من بوابة ESET HOME أو أن الاشتراك الذي تمت مشاركته مع حساب ESET HOME لم يعد مشتركاً. لحل هذه المشكلة:

- انقر فوق **تنشيط** واستخدم إحدى طرق التنشيط لتنشيط ESET Internet Security.
- اتصل بمالك الاشتراك وأبلغه بمعلومات حول أنه تم إلغاء تنشيط ESET Internet Security من قبل مالك الاشتراك أو أن الاشتراك لم يعد مشتركاً معك. يمكن للمالك حل المشكلة في ESET HOME.

0

برنامج تحسين تجربة العميل

من خلال الانضمام إلى "برنامج تحسين تجربة العميل"، أنت بذلك تزود ESET بمعلومات مجهولة تتعلق باستخدام منتجاتنا. تتوفر المزيد من المعلومات حول معالجة البيانات في سياسة الخصوصية لدينا.

موافقتك

المشاركة في البرنامج تطوعية وتعتمد على موافقتك. بعد الانضمام، تكون المشاركة مجهولة، مما يعني أنك لست بحاجة إلى اتخاذ أي إجراء آخر. يمكنك إلغاء موافقتك عن طريق تغيير إعدادات المنتج في أي وقت. سيؤدي ذلك إلى منعنا من إجراء مزيد من

المعالجة لبياناتك المجهولة.

يمكنك إلغاء موافقتك عن طريق تغيير إعدادات المنتج في أي وقت:

- تغيير إعدادات برنامج تحسين تجربة العميل في منتجات الصفحة الرئيسية ESET Windows

ما أنواع المعلومات التي نقوم بجمعها؟

بيانات حول التفاعل مع المنتج

تخبرنا هذه المعلومات أكثر عن كيفية استخدام منتجاتنا. وبفضل هذا نعرف، على سبيل المثال، الوظائف التي يتم استخدامها في كثير من الأحيان، والإعدادات التي يقوم المستخدمون بتعديلها أو مقدار الوقت الذي يقضونه في استخدام المنتج.

بيانات حول الأجهزة

نقوم بجمع هذه المعلومات لفهم مكان ونوع الأجهزة التي تُستخدم عليها منتجاتنا. تتضمن الأمثلة النموذجية طراز الجهاز والبلد والإصدار واسم نظام التشغيل.

بيانات تشخيص الأخطاء

يتم أيضاً جمع معلومات حول حالات الأخطاء والأعطال. على سبيل المثال، ما الخطأ الذي حدث والإجراءات التي أدت إلى حدوثه.

لماذا نجمع هذه المعلومات؟

تتيح لنا هذه المعلومات المجهولة تحسين منتجاتنا لك ولمستخدمينا. فهي تساعدنا في جعلها أكثر ملاءمة وسهلة الاستخدام وبدون أخطاء قدر الإمكان.

من يتحكم في هذه المعلومات؟

ESET, spol. s r.o. هي المتحكم الوحيد في البيانات التي يتم جمعها في البرنامج. لا تتم مشاركة هذه المعلومات مع أطراف خارجية.

اتفاقية ترخيص المستخدم النهائي

اعتباراً من 19 أكتوبر 2021.

هام: الرجاء قراءة شروط وأحكام تطبيق المنتج المحددة أدناه بعناية قبل تنزيله أو تثبيته أو نسخه أو استخدامه. **يُعدّ تنزيل البرنامج أو تثبيته أو نسخه أو استخدامه، بمثابة إقرار صريح منك بموافقتك على هذه الشروط والأحكام كما تقر بـ سياسة الخصوصية.**

اتفاقية ترخيص المستخدم النهائي

بموجب شروط اتفاقية ترخيص المستخدم النهائي ("الاتفاقية") المبرمة بين شركة ESET, spol. s r. o.. الكائن مكتبها المسجَّل بالعنوان Einsteinova 24, 85101 Bratislava, Slovak Republic والمسجَّلة في السجل التجاري للمحكمة الجزئية لمدينة براتيسلافا، قسم Sro برقم القيد B/3586 ورقم تعريف الشركة: 31333532 ("ESET" أو "المزود") وبينك أو أي شخص حقيقي أو كيان قانوني ("أنت" أو "المستخدم النهائي")، يحق لك استخدام البرنامج الوارد تعريفه في المادة 1 من هذه الاتفاقية. يمكن تخزين البرنامج المحدد في المادة 1 من هذه الاتفاقية على وسيطة تخزين بيانات، أو إرساله عبر البريد الإلكتروني، أو تنزيله من الإنترنت، أو تنزيله من خوادم الموفر، أو الحصول عليه من مصادر أخرى، وفقاً للشروط والأحكام المحددة أدناه.

هذه اتفاقية حول حقوق المستخدم النهائي، وليست متعلقة بالبيع. يستمر الموفر في امتلاك نسخة البرنامج والوسائط المادية التي تحتوي عليها عبوة البيع وأي نسخ أخرى للمستخدم النهائي حق إنشائها بموجب هذه الاتفاقية.

بالنقر فوق خيار "أوافق" أو "أنا أوافق..." أثناء تنزيل البرنامج أو تثبيته أو نسخه أو استخدامه، توافق على شروط وأحكام هذه الاتفاقية وتقر بسياسة الخصوصية. في حالة عدم موافقتك على جميع شروط وأحكام هذه الاتفاقية و/أو سياسة الخصوصية، انقر فوراً فوق خيار الإلغاء أو ألغِ التثبيت أو التنزيل، أو أتلِف البرنامج ووسائط التثبيت والوثائق المرفقة وإيصال الشراء أو أعدها جميعاً إلى المزود أو إلى منفذ البيع الذي حصلت منه على البرنامج.

أنت توافق على أن استخدامك للبرنامج يشير إلى أنك قد قرأت هذه الاتفاقية وتفهمها وتوافق على الالتزام بشروطها وأحكامها.

1. **البرنامج**. كما هو مستخدم في هذه الاتفاقية، مصطلح "البرنامج" يعني: (i) برنامج الكمبيوتر المصاحب لهذه الاتفاقية وجميع مكوناتها (ii) كل محتويات الأقراص أو الأقراص المضغوطة أو أقراص DVD أو رسائل البريد الإلكتروني وأي مرفقات، أو وسائط أخرى تم إرفاق هذه الاتفاقية بها، بما في ذلك نموذج التعليمات البرمجية للبرنامج المتوفر في ناقل بيانات أو المرسَل عبر بريد إلكتروني أو المنزَل عبر الإنترنت، و(iii) أي مواد خطية إيضاحية ذات صلة وأي مستندات ممكنة أخرى متعلقة بالبرنامج، وفوق ذلك كله أي وصف للبرنامج، ومواصفاته وأي وصف لخصائص البرنامج أو تشغيله، وأي وصف لبيئة التشغيل التي يُستخدم فيها البرنامج، وتعليمات استخدام البرنامج أو تثبيته أو أي وصف لكيفية استخدام البرنامج (ي"المستندات")، و(iv) نُسخ البرنامج وتصحيحات الأخطاء المحتملة في البرنامج وإضافات البرنامج وملحقات البرنامج والإصدارات المعدَّلة للبرنامج وتحديثات مكونات البرنامج، إن وُجدت، المرخَّصة لك من قِبل الموفر بموجب المادة 3 من هذه الاتفاقية. يجب توفير البرنامج حصرياً بصيغة رمز كائن قابل للتنفيذ.

2. **التثبيت والكمبيوتر ومفتاح الترخيص**. يتطلب البرنامج المتوفر على وسيطة تخزين بيانات ـ أو الذي تم إرساله عبر البريد الإلكتروني أو تنزيله من الإنترنت أو تنزيله من خوادم الموفر أو الحصول عليه من مصادر أخرى ـ التثبيت. عليك تثبيت البرنامج على كمبيوتر مكون تكويناً صحيحاً ويتوافق مع المتطلبات الموضحة في الوثائق على الأقل. ويتم توضيح طريقة التثبيت في الوثائق. لا يجوز تثبيت برامج أو مكونات كمبيوتر ـ قد تؤثر سلباً على البرنامج ـ على الكمبيوتر الذي تثبت عليه البرنامج. الكمبيوتر يعني الأجهزة، ويشمل على سبيل المثال لا الحصر أجهزة الكمبيوتر الشخصية أو أجهزة الكمبيوتر المحمول أو محطات العمل أو أجهزة الكمبيوتر الكفي أو الهواتف الذكية أو الأجهزة الإلكترونية المحمولة باليد أو غيرها من الأجهزة الإلكترونية المصمم لها البرنامج، والذي سيثبت و/أو يستخدم عليها. مفتاح الترخيص يعني التسلسل الفريد للرموز أو الأحرف أو الأرقام أو العلامات الخاصة المتوفرة للمستخدم النهائي للسماح بالاستخدام القانوني للبرامج أو إصدارها الخاص أو تمديد مدة الترخيص بما يتوافق مع الاتفاقية.

3. **الترخيص**. وفقاً للشرط الذي وافقت بموجبه على بنود هذه الاتفاقية والالتزام بكل الشروط والأحكام المنصوص عليها في هذا المستند، يمنحك الموفر الحقوق التالية ("الترخيص"):

أ) **التثبيت والاستخدام**. يجب أن يكون لديك حق غير حصري وغير قابل للتنازل عنه لتثبيت البرنامج على القرص الثابت للكمبيوتر أو على وسيطة أخرى للتخزين الدائم للبيانات، وتثبيت البرنامج وتخزينه على ذاكرة نظام كمبيوتر، ولتنفيذ البرنامج

وتخزينه وعرضه.

ب) **اشتراط عدد التراخيص**. يجب أن يتقيد الحق في استخدام البرنامج بعدد المستخدمين النهائيين. (1) تثبيت البرنامج في نظام كمبيوتر واحد. أو (2) إذا كان مدى الترخيص مرتبط بعدد علب البريد، إذن يُقصد بالمستخدم الواحد مستخدم الكمبيوتر الذي يوافق على البريد الإلكتروني عبر عميل مستخدم البريد ("عميل مستخدم البريد"). إذا وافق عميل مستخدم البريد على البريد الإلكتروني وتولى لاحقاً توزيعه تلقائياً على العديد من المستخدمين، يتم تحديد عدد المستخدمين وفقاً للعدد الفعلي للمستخدمين الذين يُوزع عليهم البريد الإلكتروني. إذا أدى خادم بريد وظيفة بوابة بريد، يتساوى عدد المستخدمين النهائيين مع عدد مستخدمي خوادم البريد الذين تقدم لهم هذه البوابة خدمات. في حالة توجيه عدد غير محدد من عناوين البريد الإلكتروني عبر مستخدم واحد (على سبيل المثال، من خلال الاسم المستعار) وقبول ذلك المستخدم لتلك العناوين، ولا يتم توزيع الرسائل تلقائياً من جانب العميل إلى عدد أكبر من المستخدمين، فيلزم توفر ترخيص لكمبيوتر واحد فقط. يجب ألا تستخدم ترخيصاً واحداً في وقت واحد على أكثر من جهاز كمبيوتر واحد. يحق للمستخدم إدخال مفتاح الترخيص إلى البرنامج فقط إلى الحد الذي يسمح له باستخدام البرنامج وفقاً للقيود الناشئة عن عدد التراخيص الممنوحة من قبل الموفر. ويعد مفتاح الترخيص سرياً، ويجب عدم مشاركة الترخيص مع أطراف أخرى أو السماح لأطراف أخرى باستخدام مفتاح الترخيص ما لم تسمح به هذه الاتفاقية أو الموفر. وفي حال تم اختراق مفتاح الترخيص، فأبلغ الموفر على الفور.

ج) **الإصدار المنزلي/إصدار الأعمال**. ينبغي استخدام الإصدار المنزلي من البرنامج حصرياً في بيئات خاصة و/أو غير تجارية للاستخدام المنزلي والعائلي فقط. يجب الحصول على نسخة من إصدار الأعمال من البرنامج لاستخدامه في بيئة تجارية وكذلك على خوادم البريد أو ناقلات البريد أو بوابات البريد أو بوابات الإنترنت.

د) **مدة الترخيص**. يجب أن يكون حقك في استخدام البرنامج لمدة محددة.

هـ) **برامج OEM**. يقتصر البرنامج المصنّف على الأجهزة الأصلية "OEM" على جهاز الكمبيوتر الذي حصلت عليه معه. ولا يمكن نقلها إلى كمبيوتر مختلف.

و) **البرامج غير المخصصة للبيع أو الإصدارات التجريبية**. لا يمكن تخصيص البرامج المصنفة باعتبارها "غير مخصصة للبيع" أو "إصدارات تجريبية" كبرامج مدفوعة، ويجب عدم استخدامها إلا لتقديم عرض توضيحي لميزات البرنامج أو لاختبارها.

ز) **إنهاء الترخيص**. يجب أن ينتهي الترخيص تلقائياً في نهاية الفترة الممنوحة له. وفي حالة العجز عن الالتزام بأي من أحكام هذه الاتفاقية، يحق للموفر الانسحاب من الاتفاقية، دون الإخلال بأي حق أو تعويض قانوني مفتوح إلى الموفر في مثل هذه الاحتمالات. وفي حالة إلغاء الترخيص، يجب عليك حذف البرنامج وكل النسخ الاحتياطية أو تدميرها أو إعادتها فوراً على نفقتك الخاصة إلى ESET أو إلى منفذ البيع الذي اشتريت منه البرنامج. عند انتهاء الترخيص، يحق للموفر أيضاً إلغاء حق المستخدم النهائي في استخدام وظائف البرنامج التي تتطلب الاتصال بخوادم الموفر أو خوادم أطراف ثالثة.

4. **وظائف جمع البيانات ومتطلبات الاتصال بالإنترنت**. لتشغيل البرنامج بشكل صحيح، يجب الاتصال بالإنترنت والاتصال على فترات زمنية منتظمة بخوادم الموفر أو خوادم أطراف أخرى وجمع البيانات المعمول بها بما يتوافق مع سياسة الخصوصية. يتعين الاتصال بالإنترنت وجمع البيانات المعمول بها لاستخدام وظائف البرنامج التالية:

أ) **التحديثات على البرنامج**. يحق للمزود إصدار تحديثات أو ترقيات للبرنامج من وقت لآخر ("التحديثات")، ولكن لا يلتزم بتوفير التحديثات. ويتم تمكين هذه الوظيفة ضمن إعدادات البرنامج القياسية، ولذلك يتم تثبيت التحديثات تلقائياً، ما لم يكن المستخدم النهائي قد قام بتعطيل التثبيت التلقائي للتحديثات. لتوفير التحديثات، يلزم التحقق من صحة الترخيص بما في ذلك معلومات حول جهاز الكمبيوتر و/أو النظام الأساسي التي تم تثبيت البرنامج عليه وفقاً لسياسة الخصوصية.

قد يخضع تقديم أي تحديثات لسياسة انتهاء الصلاحية ("سياسة EOL") والتي تتوفر على https://go.eset.com/eol_home. لن يتم إرسال أي تحديثات بعد وصول البرنامج أو أي من ميزاته إلى تاريخ انتهاء الصلاحية الافتراضي كما هو محدد في سياسة انتهاء الصلاحية (EOL).

ب) **إعادة توجيه حالات التسلل والمعلومات إلى الموفر.** يحتوي البرنامج على وظائف تعمل على جمع عينات فيروسات جهاز الكمبيوتر وغيرها من برامج الكمبيوتر الضارة المشابهة والكائنات غير الآمنة والمريبة وغير المرغوبة والمسببة للمشكلات مثل الملفات وعناوين URL وحزم IP وإطارات ethernet (المشار إليها فيما بعد في هذه الاتفاقية باسم الموجودة في الشبكة المحلية مثل نوع الجهاز والمورّد والطراز و/أو المنصة التي تم تثبيت البرنامج عليها والمعلومات حول عمليات التشغيل والوظائف للبرنامج ("المعلومات"). قد تحتوي المعلومات وحالات التسلل على بيانات)بما في ذلك البيانات الشخصية التي تم الحصول عليها عشوائياً او بدون قصد (عن المستخدم النهائي أو المستخدمين الآخرين للكمبيوتر المثبت عليه البرنامج والملفات المتضررة بسبب حالات التسلل مع بينات التعريف المرتبطة.

يُمكن جمع المعلومات وحالات التسلل عن طريق وظائف البرنامج التالية:

i. تتضمن وظيفة نظام سمعة LiveGrid جمع وإرسال تجزئات أحادية الاتجاه مرتبطة بحالات التسلل للموفر. هذه الوظيفة ممكَّنة ضمن الإعدادات القياسية للبرنامج.

ii. تتضمن وظيفة نظام ملاحظات LiveGrid جمع وإرسال عمليات التسلل مع بيانات التعريف ذات الصلة بالموفر. يتم تنشيط هذه الوظيفة من قبل المستخدم أثناء عملية تثبيت 2. يتم تنشيط هذه الوظيفة من قبل المستخدم أثناء عملية تثبيت البرنامج.

لا يستخدم الموفر المعلومات والتسللات المستلمة إلا بغرض التحليل والبحث في التسللات وكذلك تحسين التحقق من صحة موثوقية البرنامج والترخيص، ويتخذ الإجراءات المناسبة لضمان الحفاظ على سرية التسللات والمعلومات المستلمة. بتنشيط وظيفة البرنامج هذه، يمكن جمع التسللات والمعلومات ومعالجتها من قبل الموفر على النحو المحدد في "سياسة الخصوصية" وبما يتوافق مع اللوائح القانونية ذات الصلة. ويمكنك إلغاء تنشيط هذه الوظائف في أي وقت.

لأغراض هذه الاتفاقية، من الضروري جمع البيانات التي تمكن موفر الخدمة من تحديد هويتك ومعالجتها وتخزينها بما يتوافق مع "سياسة الخصوصية". تقر أنت بموجب هذه الاتفاقية بأن مقدم الخدمة يقوم بالتحقق باستخدام وسائله ما إذا كنت تستخدم البرنامج وفقاً لأحكام هذه الاتفاقية. وتقر بموجب هذه الاتفاقية انه بغرض هذه الاتفاقية، من الضروري نقل بياناتك أثناء الاتصال بين البرنامج وانظمة كمبيوتر مقدم الخدمة أو شركاء الأعمال لديه كجزء من توزيع مقدم الخدمة وشبكة الدعم لضمان تشغيل وظائف البرنامج والمصادقة لاستخدام البرنامج ولحماية حقوق مقدم الخدمة.

بعد إبرام هذه الاتفاقية، يحق للموفر أو أي من شركائه في العمل، كجزء من توزيع مقدم الخدمة وشبكة الدعم، نقل البيانات الأساسية التي تحدد هويتك ومعالجتها وتخزينها، لأغراض الفوترة وأداء هذه الاتفاقية، ونقل الإشعارات على الكمبيوتر الخاص بك.

يمكن العثور على تفاصيل حول الخصوصية وحماية البيانات الشخصية وحقوقك كموضوع البيانات في "سياسة الخصوصية" التي تتوفر على موقع مقدم الخدمة ويمكن الوصول إليها مباشرة من عملية التثبيت. يمكنك أيضا زيارته من قسم تعليمات البرنامج.

5. **ممارسة حقوق المستخدم النهائي.** يجب ممارسة حقوق المستخدم النهائي شخصياً أو عبر موظفيك. يحق لك استخدام البرنامج لحماية عملياتك وحماية أجهزة الكمبيوتر أو أنظمة الكمبيوتر التي حصلت على ترخيص لها فقط.

6. **القيود المفروضة على الحقوق.** لا يجوز لك نسخ البرنامج أو توزيعه أو استخراج مكونات منه أو إنشاء أعمال مشتقة منه. عند استخدام البرنامج، يُطلب منك الالتزام بالقيود التالية:

أ) يجوز لك إنشاء نسخة واحدة من البرنامج على وسيطة تخزين دائمة كنسخة احتياطية أرشيفية، شريطة ألا يتم تثبيت النسخة الاحتياطية الأرشيفية أو استخدامها على أي كمبيوتر. وتشكِّل أي نسخ أخرى تقوم بإنشائها من البرنامج خرقا لهذه الاتفاقية.

ب) لا يجوز لك استخدام البرنامج أو تعديله أو ترجمته أو إعادة إنشائه أو نقل حقوق استخدام البرنامج أو نُسخ منه بأية طريقة خلافاً للواردة في هذه الاتفاقية.

ج) لا يحق لك بيع البرنامج أو ترخيصه من الباطن أو تأجيره أو استئجاره أو إعارته، أو استخدامه لتقديم لخدمات تجارية.

د) لا يجوز لك إجراء هندسة عكسية للبرنامج، أو عكس تجميعه أو تفكيكه، أو محاولة اكتشاف التعليمة البرمجية المصدر للبرنامج بأية وسيلة، إلا في حالة حظر القانون لهذا التقييد صراحة.

هـ) توافق على عدم استخدام البرنامج إلا بالطريقة التي تتوافق مع جميع القوانين المعمول بها في الولاية القضائية التي تستخدم البرنامج فيها، بما في ذلك ـ على سبيل المثال، لا الحصر ـ القيود المعمول بها فيما يتعلق بحقوق الطبع والنشر وغيرها من حقوق الملكية الفكرية.

و) توافق على عدم استخدام البرنامج ووظائفه إلا بطريقة لا تحد من إمكانية المستخدمين النهائيين في الوصول إلى هذه الخدمات. يحتفظ الموفر بحق تقييد نطاق الخدمات الموفرة لمستخدمين نهائيين بعينهم، لتمكين استخدام الخدمات بواسطة أكبر عدد ممكن من المستخدمين النهائيين. كما يجب أن يعني تقييد نطاق الخدمات أيضاً الإنهاء التام لإمكانية استخدام أي من وظائف البرنامج وحذف البيانات والمعلومات الموجودة على خوادم الموفر أو الخوادم التابعة لطرف ثالث فيما يتعلق بوظيفة معينة من وظائف البرنامج.

ز) أنت توافق على عدم ممارسة أي أنشطة تنطوي على استخدام مفتاح الترخيص، خلافاً لشروط هذه الاتفاقية أو توفير مفتاح الترخيص لأي شخص لا يحق له استخدام البرنامج، مثل نقل مفتاح الترخيص المستخدم أو غير المستخدم بأي شكل من الأشكال، وكذلك الاستنساخ غير المصرح به، أو توزيع مفاتيح الترخيص المكررة أو التي تم إنشاؤها أو استخدام البرنامج نتيجة لاستخدام مفتاح الترخيص الذي تم الحصول عليه من المصدر بخلاف مقدم الخدمة.

7. **حقوق الطبع والنشر**. يخضع البرنامج وجميع الحقوق ـ بما في ذلك على سبيل المثال، لا الحصر ـ حقوق الملكية والملكية الفكرية المملوكة لشركة ESET و/أو حاملي تراخيصها. وتحظى هذه الحقوق بالحماية بموجب أحكام المعاهدات الدولية وجميع القوانين الأخرى المعمول بها في البلد الذي يُستخدَم فيه البرنامج. يُعد هيكل البرنامج وتنظيمه وتعليمته البرمجية أسراراً تجارية ومعلومات سرية خاصة بشركة ESET و/أو حاملي تراخيصها. لا يجوز لك نسخ البرنامج، إلا وفقاً للمنصوص عليه في المادة 6(أ). لا بد أن تحتوي أي نُسخ مسموح لك بإنشائها بموجب هذه الاتفاقية على إشعارات حقوق الطبع والنشر وإشعارات الملكية الأخرى نفسها التي تظهر في البرنامج. في حالة عكس هندسة تعليمة برمجية مصدر أو عكس تجميعها أو تفكيكها أو محاولة اكتشافها بأية طريقة أخرى، بما يمثل خرقاً لأحكام هذه الاتفاقية، توافق بموجب ذلك على أن أي معلومات يتم الحصول عليها نتيجة لذلك يتم نقل ملكيتها إلى الموفر وتعد مملوكة له بالكامل تلقائياً وبشكلٍ دائم منذ لحظة إنشائها، دون الإخلال بحقوق الموفر المترتبة على خرق هذه الاتفاقية.

8. **الاحتفاظ بالحقوق**. يحتفظ الموفر بموجب ذلك بجميع الحقوق في البرنامج، باستثناء الحقوق الممنوحة لك صراحةً بموجب شروط هذه الاتفاقية باعتبارك المستخدم النهائي للبرنامج.

9. **الإصدارات متعددة اللغات، وبرامج الوسائط المزدوجة، والنُسخ المتعددة**. في حالة دعم البرنامج لعدة أنظمة أساسية أو لغات، أو في حالة استلام عدة نسخ من البرنامج، يمكنك فقط استخدام البرنامج لعدد أنظمة الكمبيوتر والإصدارات التي حصلت على ترخيص لها. ولا يجوز لك بيع إصدارات أو نُسخ البرنامج التي لا تستخدمها، ولا تأجيرها أو استئجارها أو ترخيصها من

الباطن أو إعارتها أو نقل ملكيتها.

10. **سريان الاتفاقية وفسخها.** تعد هذه الاتفاقية نافذة المفعول اعتباراً من تاريخ موافقتك على شروط هذه الاتفاقية. ويجوز لك فسخها في أي وقت بإزالة تثبيت البرنامج، وجميع النسخ الاحتياطية وجميع المواد ذات الصلة ـ الموفرة بواسطة الموفر أو شركاء العمل التابعين له ـ وإتلافها وإرجاعها على نفقتك. قد يخضع حقك في استخدام البرنامج وأي من ميزاته لسياسة انتهاء الصلاحية (EOL). بعد وصول البرنامج أو أي من ميزاته إلى تاريخ انتهاء الصلاحية المحدد في سياسة انتهاء الصلاحية (EOL) سينتهي حقك في استخدام البرنامج. وبصرف النظر عن طريقة فسخ هذه الاتفاقية، تظل أحكام المواد 7 و8 و11 و13 و20 و22 سارية لمدة غير محددة.

11. **إقرارات المستخدم النهائي.** بوصفك المستخدم النهائي، تقر بموجب هذا المستند بأن البرنامج يتم توفيره "كما هو" دون ضمان من أي نوع، سواء كان صريحاً أو ضمنياً، وإلى الحد الأقصى الذي يسمح به القانون المعمول به. ولا يقدِّم الموفر ولا حاملو التراخيص التابعون له ولا شركاته التابعة ولا أصحاب حقوق الطبع والنشر أي تعهدات أو ضمانات سواء صريحة أو ضمنية، بما في ذلك ـ على سبيل المثال لا الحصر ـ ضمانات الرواج التجاري أو الملاءمة لغرض محدد أو أن البرنامج لا ينتهك أي براءات اختراع أو حقوق طبع ونشر أو علامات تجارية أو أي حقوق أخرى لطرف ثالث. ولا يقدِّم الموفر أو أي طرف آخر أي ضمان بأن الوظائف المضمنة في البرنامج ستلبي متطلباتك أو أن تشغيل البرنامج لا تتم مقاطعته أو أنه خالٍ من الأخطاء. وتتحمل وحدك كل المسؤوليات والمخاطر المتعلقة باختيار البرنامج واستخدامه في تحقيق نتائجك المرجوة والنتائج التي يتم الحصول عليها منه.

12. **لا توجد التزامات أخرى.** لا تفرض هذه الاتفاقية أي التزامات على جانب الموفر وحاملي تراخيصه بخلاف المنصوص عليها تحديداً بهذه الاتفاقية.

13. **تحديد المسؤولية.** إلى الحد الأقصى الذي يسمح به القانون المعمول به، لا يتحمل المزود أو موظفوه أو حاملو تراخيصه بأي شكل من الأشكال أي مسؤولية عن أي خسارة في أرباح أو عائدات أو مبيعات أو بيانات، أو تكاليف شراء سلع أو خدمات بديلة، أو خسارة في ممتلكات، أو إصابة بدنية، أو توقف نشاط تجاري، أو فقدان معلومات متعلقة بنشاط تجاري، أو أي أضرار خاصة أو مباشرة أو غير مباشرة أو عرضية أو اقتصادية أو تأمينية أو تأديبية أو تبعية، مهما كان سببها وسواء كانت ناشئة من عقد أو ضرر أو إهمال أو أي نظرية أخرى تتعلق بالمسؤولية الناشئة عن التثبيت، سواء كانت ناتجة من استخدام البرنامج أو عدم القدرة على استخدامه، حتى لو تم إبلاغ الموفر أو حاملي تراخيصه أو شركاته التابعة باحتمال حدوث مثل هذه الأضرار. ونظراً لأن بعض البلدان أو الاختصاصات القضائية لا تسمح باستثناء المسؤولية، ولكن يجوز أن تسمح بالمسؤولية المحدودة؛ ففي مثل هذه الحالات، تصبح مسؤولية الموفر أو موظفيه أو حاملي تراخيصه أو شركاته التابعة مقتصرة على إجمالي المدفوع مقابل ذلك الترخيص.

14. لا يمس أي شيء وارد بهذه الاتفاقية الحقوق القانونية لأي طرف يتعامل كمستهلك إذا كان يتناقض مع ما هو وارد بهذه الاتفاقية.

15. **الدعم الفني.** يجب على ESET أو الأطراف الأخرى المكلفة من ESET تقديم الدعم الفني، بمحض تقديرها، دون أي ضمانات أو إعلانات. لن يتم إرسال أي دعم فني بعد وصول البرنامج أو أي من ميزاته إلى تاريخ انتهاء الصلاحية الافتراضي في سياسة انتهاء الصلاحية (EOL). كما يجب مطالبة المستخدم النهائي بإجراء نسخ احتياطي لجميع البيانات والبرامج ومرافق البرامج قبل توفير الدعم الفني. لا يمكن أن تتحمل ESET أو الأطراف الأخرى المكلفة من ESET مسؤولية عن أي تلف أو فقد لبيانات أو ممتلكات أو برامج أو أجهزة، أو خسارة ربح بسبب توفير الدعم الفني. تحتفظ ESET و/أو الأطراف الأخرى المكلفة من ESET بالحق في تحديد أن حل المشكلة خارج نطاق الدعم الفني. كما تحتفظ ESET بالحق في رفض تقديم الدعم الفني أو تعليقه أو إنهائه، بمحض تقديرها. قد تطلب معلومات الترخيص والمعلومات وغيرها من البيانات بما يتوافق مع "سياسة الخصوصية" لغرض توفير الدعم الفني.

16. **نقل الترخيص.** يمكن نقل البرنامج من نظام كمبيوتر إلى آخر، ما لم يتعارض مع أحكام هذه الاتفاقية. وإذا لم يتعارض مع أحكام الاتفاقية، فلا يجوز للمستخدم النهائي نقل الترخيص وجميع الحقوق المترتبة على هذه الاتفاقية بشكل دائم لمستخدم نهائي آخر إلا بموافقة من الموفر، وبموجب الشروط التالية: (1) عدم احتفاظ المستخدم النهائي الأصلي بأي نسخ من البرنامج، (2) يجب أن يكون نقل ملكية الحقوق مباشراً، أي من المستخدم النهائي الأصلي لمستخدم نهائي جديد، (3) يجب أن يتحمل المستخدم النهائي الجديد جميع الحقوق والالتزامات المفروضة على المستخدم النهائي الأصلي وفقا لأحكام هذه الاتفاقية، و(4) على المستخدم النهائي الأصلي أن يقدم للمستخدم النهائي الجديد الوثائق التي تتيح له التحقق من أن البرنامج أصلي، كما هو محدد بموجب المادة 17.

17. **التحقق من أصالة البرنامج.** يجوز للمستخدم النهائي إثبات حقه في استخدام البرنامج بإحدى الطرق التالية (1) :من خلال شهادة ترخيص صادرة من الموفر أو طرف ثالث معيَّن من قِبل الموفر، و (2)من خلال اتفاقية ترخيص خطية، إذا كانت مثل هذه الاتفاقية مبرمة، و (3)من خلال تقديم رسالة بريد إلكتروني مرسلة من قِبل الموفر وتحتوي على تفاصيل الترخيص)اسم المستخدم وكلمة المرور). قد تكون هناك حاجة لمعلومات الترخيص وبيانات تعريف المستخدم النهائي بما يتوافق مع "سياسة الخصوصية" لغرض التحقق من صحة البرنامج.

18. **الترخيص للهيئات العامة والحكومة الأمريكية.** يجب توفير البرنامج للهيئات العامة ـ بما في ذلك الحكومة الأمريكية ـ مع حقوق الترخيص والقيود الموضحة في هذه الاتفاقية.

19. **امتثال الرقابة التجارية.**

أ) يحظر تصدير البرنامج أو إعادة تصديره أو نقله إو إرساله أو استخدامه بأي شكل من الأشكال، سواء بشكل مباشر أو غير مباشر، أو مشاركته في أي عمل من شأنه أن يُعرض شركة ESET أو الشركات القابضة وشركاتها التابعة والشركات التابعة لأي من شركاتها القابضة وكذلك الكيانات التي تديرها شركاتها القابضة (الشركات التابعة) إلى مخالفة القوانين أو العواقب السلبية المفروضة بموجب قوانين الرقابة التجارية، والتي تتضمن ما يلي:

i. جميع القوانين التي تحكم أو تقيد أو تفرض شروط التراخيص على تصدير أو إعادة تصدير أو نقل البضائع أو البرامج أو التكنولوجيا أو الخدمات، سواء الصادرة أو المعتمدة من قبل أي حكومة أو ولاية أو سلطة تنظيمية للولايات المتحدة الأمريكية أو سنغافورة أو المملكة المتحدة أو الاتحاد الأوروبي أو أي من الدول الأعضاء، أو أي دولة يجب فيها تنفيذ الالتزامات بموجب أحكام وشروط الاتفاقية أو التي يجري فيها دمج أو تشغيل شركة ESET أو أي من الشركات التابعة لها

ii. جميع العقوبات الاقتصادية أو المالية أو التجارية أو غيرها، بالإضافة إلى العقوبات المفروضة أو تقييدات أو حظر أو منع استيراد أو تصدير أو حظر تحويل الأموال أو الأصول أو تقديم الخدمات أو التدابير المفروضة من قبل أي حكومة أو ولاية أو سلطة تنظيمية للولايات المتحدة الأمريكية أو سنغافورة أو المملكة المتحدة أو الاتحاد الأوروبي أو أي من الدول الأعضاء، أو أي دولة يجب فيها تنفيذ الالتزامات بموجب أحكام وشروط الاتفاقية أو التي يجري فيها دمج أو تشغيل شركة ESET أو أي من الشركات التابعة لها ("قوانين العقوبات").

(الأفعال القانونية المشار إليها في النقطتين 1 و 2 أعلاه معاً باسم "قوانين الرقابة التجارية").

ب) يحق لشركة ESET تعليق التزاماتها بموجب هذه الشروط أو إنهاؤها فوراً في الحالة التالية:

i. إذا قررت شركة ESET بناءً على تقديرها المعقول، مخالفة المستخدم أو احتمالية مخالفته لأحكام المادة 19-أ من الاتفاقية؛

ii. يخضع المستخدم النهائي و/ أو البرنامج إلى قوانين الرقابة التجارية، وبناءً على ذلك قررت شركة ESET بناءً على تقديرها المعقول، أن استمرار تنفيذ التزاماتها المفروضة بموجب الاتفاقية يمكن أن يؤدي إلى انتهاك سياسات شركة ESET أو الشركات

التابعة لها أو التعرض للعواقب السلبية بموجب قوانين الرقابة التجارية.

ج) لا تتضمن الاتفاقية ولا يُفسر أو يؤول أي بند من بنودها على حث أو مطالبة أي من الطرفين بالعمل أو الامتناع عن العمل (أو الموافقة على العمل أو الامتناع عن العمل) بما يتعارض أو يخالف قوانين المراقبة التجارية السارية.

20. **الإخطارات**. يجب إرسال جميع الإخطارات والبرامج والوثائق المرتجعة إلى العنوان التالي: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic دون الإخلال بحق ESET في إبلاغك بأي تغييرات تطرأ على هذه الاتفاقية وسياسات الخصوصية وسياسة انتهاء الصلاحية (EOL) والوثائق وفقاً للمادة 22 من الاتفاقية. يجوز لـESET إرسال رسائل بريد إلكتروني إليك أو إخطارات داخل التطبيق عبر البرنامج أو نشر الاتصال على موقع الويب. أنت توافق على تلقي اتصالات قانونية من ESET بشكل إلكتروني، بما في ذلك أي اتصالات بشأن التغيير في الشروط أو الشروط الخاصة أو سياسات الخصوصية، أو أي اقتراح/قبول عقد أو دعوات للمعالجة، أو أي إشعارات أو اتصالات قانونية أخرى. يجب اعتبار هذا الاتصال الإلكتروني على أنه تم استلامه كتابياً، ما لم تتطلب القوانين المعمول بها على وجه التحديد شكلاً مختلفاً من أشكال الاتصال.

21. **القانون المعمول به**. تخضع هذه الاتفاقية وتفسَّر وفقا لقوانين جمهورية سلوفاكيا. يوافق المستخدم النهائي والموفر بموجب ذلك على عدم سريان مبادئ تنازع القوانين واتفاقية الأمم المتحدة بشأن عقود البيع الدولي للبضائع. كما توافق صراحة على أنه يجب تسوية أي نزاع أو دعاوى ناجمة عن هذه الاتفاقية تتعلق بالموفر أو أي نزاعات أو دعاوى تتعلق باستخدام البرنامج أمام محكمة الدرجة الأولى في براتيسلافا، وتوافق صراحة على ممارسة المحكمة المذكورة للاختصاص القضائي.

22. **الأحكام العامة**. في حالة عدم صلاحية أي حكم من أحكام هذه الاتفاقية أو عدم قابليته للتنفيذ، لا يؤثر ذلك على بقية أحكام الاتفاقية، التي تظل سارية وقابلة للتنفيذ بموجب الشروط المنصوص عليها في هذه الاتفاقية. تم تنفيذ هذه الاتفاقية باللغة الإنجليزية. في حالة إعداد أي ترجمة للاتفاقية للتسهيل أو لأي غرض آخر أو في أي حالة وجود تعارض بين النسخ اللغوية المختلفة الصادرة من هذه الاتفاقية، تسود النسخة الإنجليزية لهذه الاتفاقية.

تحتفظ ESET بالحق في إجراء تغييرات على البرنامج وكذلك مراجعة شروط هذه الاتفاقية وملحقاتها وإضافاتها وسياسة الخصوصية وسياسة انتهاء الصلاحية والوثائق أو أي جزء منها في أي وقت عن طريق تحديث المستند ذات الصلة (1) لتعكس التغييرات على البرنامج أو في كيفية قيام ESET بالأعمال، (2) لأسباب قانونية أو تنظيمية أو أمنية، أو (3) لمنع إساءة الاستخدام أو الضرر. سيتم إخطارك بأي مراجعة للاتفاقية عن طريق البريد الإلكتروني أو الإعلام داخل التطبيق أو بأي وسيلة إلكترونية أخرى. إذا كنت لا توافق على التغييرات المقترحة على الاتفاقية، فيجوز لك فسخها وفقاً للمادة. 10 في غضون 30 يوماً بعد تلقي إشعار بالتغيير. ما لم تقم بفسخ الاتفاقية خلال هذه الفترة الزمنية، سيتم اعتبار التغييرات المقترحة مقبولة وتصبح سارية تجاهك اعتباراً من التاريخ الذي تلقيت فيه إشعاراً بالتغيير.

هذا هو مجمل الاتفاق بين الموفر وبينك، فيما يتعلق بالبرنامج، وهو يُبطل أي إقرارات أو مناقشات أو تعهدات أو مراسلات أو إعلانات تتعلق بالبرنامج.

تضاف إلى الاتفاقية

د) **تقييم الأمان للأجهزة المتصلة بالشبكة**. تنطبق أحكام إضافية على تقييم الأمان للأجهزة المتصلة بالشبكة على النحو التالي:

يحتوي البرنامج على وظيفة للتحقق من أمان الشبكة المحلية للمستخدم النهائي وأمن الأجهزة في الشبكة المحلية والتي تتطلب اسم الشبكة المحلية ومعلومات حول الأجهزة في الشبكة المحلية مثل التواجد والنوع والاسم وعنوان IP وعنوان MAC للجهاز في الشبكة المحلية فيما يتعلق بمعلومات الترخيص. تتضمن المعلومات أيضاً نوع الأمان اللاسلكي ونوع التشفير اللاسلكي لأجهزة التوجيه. قد توفر هذه الوظيفة أيضاً معلومات تتعلق بتوفر حل برامج الأمان لتأمين الأجهزة في الشبكة المحلية.

الحماية من إساءة استخدام البيانات تنطبق أحكام إضافية على الحماية من إساءة استخدام البيانات على النحو التالي:

يشتمل البرنامج على وظيفة تحول دون فقد البيانات الهامة أو إساءة استخدامها عند تعرض الكمبيوتر للسرقة بطريقة مباشرة. يتم إيقاف تشغيل هذه الوظيفة وفقًا للإعدادات الافتراضية الخاصة بالبرنامج. يجب إنشاء حساب ESET HOME لكي يتم تنشيطها، والتي تقوم من خلالها الوظيفة بتنشيط جمع البيانات في حالة تعرض الكمبيوتر للسرقة. وفي حالة تنشيط وظيفة البرنامج هذه، يتم إرسال البيانات الخاصة بالكمبيوتر المسروق إلى موفر الخدمة، والذي يجوز له بدوره تضمين البيانات الخاصة بموقع شبكة الكمبيوتر والبيانات الخاصة بتكوين الكمبيوتر والبيانات المسجلة باستخدام الكاميرا المتصلة بالكمبيوتر أو المحاولات الفاشلة لإلغاء قفل الكمبيوتر (والمشار إليها في هذه الوثيقة باسم "البيانات"). يحق للمستخدم النهائي استخدام البيانات التي يتم الحصول عليها بهذه الطريقة والمتوفرة عبر حساب ESET HOME فقط لغرض التحقق من موقف عكسي كنتيجة لسرقة الكمبيوتر. لغرض هذه الوظيفة فقط، يقوم موفر الخدمة بمعالجة البيانات على النحو المحدد في "سياسة الخصوصية" وبما يتوافق مع اللوائح القانونية ذات الصلة. يسمح موفر الخدمة للمستخدم النهائي بالوصول إلى البيانات على الأجهزة الفنية التابعة له للفترة المطلوب تحقيق هذا الهدف خلالها للحصول على البيانات والتي ينبغي ألا تتجاوز فترة الاحتفاظ المحددة في "سياسة الخصوصية". يمكن استخدام ميزة الحماية من إساءة استخدام البيانات بشكل حصري على أجهزة الكمبيوتر والحسابات التي يستطيع المستخدم النهائي الوصول إليها بشكل قانوني. وسيتم إبلاغ الجهات المعنية بأي استخدام غير قانوني لاتخاذ ما يلزم من إجراءات. يمتثل الموفر للقوانين ذات الصلة ويساعد سلطات إنفاذ القانون في حالة إساءة استخدام البيانات. تقر وتعترف بأنك تتحمل المسؤولية عن حماية كلمة المرور للوصول إلى حساب ESET HOME وتتعهد بعدم الكشف عن كلمة المرور الخاصة بك لأي طرف آخر. يتحمل المستخدم النهائي المسؤولية عن أي نشاط باستخدام وظيفة الحماية من إساءة استخدام البيانات وحساب ESET HOME المخول أو غير المخول. أبلغ موفر الخدمة على الفور في حالة تعرض حساب ESET HOME للخطر. تنطبق أحكام إضافية للحماية من إساءة استخدام البيانات حصرياً على ESET Internet Security والمستخدمين النهائيين لـ ESET Smart Security Premium.

ESET Secure Data. تنطبق أحكام إضافية على ESET Secure Data على النحو التالي:

1. التعاريف. في هذه الأحكام الإضافية إلى ESET Secure Data الكلمات التالية لها المعاني المقابلة:

أ) "المعلومات "أي معلومات أو بيانات مشفرة أو تم فك تشفيرها باستخدام البرنامج؛

ب) "المنتجات"برنامج ESET Secure Data والتوثيق؛

ج) "ESET Secure Data" البرنامج (البرامج) المستخدمة لتشفير البيانات الإلكترونية وفك تشفيرها؛

يجب أن يتضمن جميع ما يُشار به إلى الجمع على المفرد ويجب أن يتضمن جميع ما يُشار به إلى المذكر على المؤنث والعكس صحيح. وينبغي استخدام الكلمات التي ليست لها تعاريف محددة وفقاً للتعاريف المنصوص عليها في الاتفاقية.

2. تصريح مستخدم إضافي. أنت تقر وتوافق على ما يلي

أ) تتحمل مسؤولية حماية المعلومات والاحتفاظ بها ونسخها احتياطياً؛

ب) يجب عليك نسخ جميع المعلومات والبيانات بشكل كامل (بما في ذلك على سبيل المثال لا الحصر أي معلومات وبيانات هامة) على جهاز الكمبيوتر لديك قبل تثبيت ESET Secure Data

ج) يجب عليك الاحتفاظ بسجل آمن لأي من كلمات المرور وغيرها من المعلومات المستخدمة لإعداد ESET Secure Data واستخدامه، ويجب عليك أيضاً عمل نُسخ احتياطية لجميع مفاتيح التشفير ورموز الترخيص والملفات الرئيسية وغيرها من البيانات التي يتم إنشاؤها لفصل وسائط التخزين؛

د) أنت المسؤول عن استخدام المنتجات. ولا يتحمل الموفر أي مسؤولية عن أي فقدان أو ادعاء أو تلف ناتج عن أي تشفير أو فك تشفير غير مصرح به أو خاطئ للمعلومات أو البيانات أينما وكيفما كانت المعلومات أو البيانات مخزّنة؛

هـ) في حين اتخذ الموفر كافة الخطوات المعقولة اللازمة لضمان سلامة وأمن ESET Secure Data يجب عدم استخدام المنتجات (أو أي جزء منها) في أي منطقة تستند إلى مستوى أمان احتياط الأمان عند التعطل أو ينطوي على مخاطر محتملة بما في ذلك على سبيل المثال لا الحصر المنشآت النووية، أو الملاحة الجوية، أو أنظمة التحكم أو الاتصال، أو أنظمة الأسلحة والدفاع ودعم الحياة أو أنظمة مراقبة الحياة؛

و) كما تقع على المستخدم النهائي مسؤولية ضمان أن مستوى الأمان والتشفير المقدم للمنتجات يلبي متطلباتك؛

ز) أنت المسؤول عن استخدامك للمنتجات أو أي منها بما في ذلك على سبيل المثال لا الحصر ضمان أن هذا الاستخدام يتوافق مع جميع القوانين والأنظمة المعمول بها في الجمهورية السلوفاكية أو أي بلد آخر، أو منطقة أو دولة يُستخدم فيها المنتج. ويجب عليك قبل أي استخدام للمنتجات ضمان انها لا تخالف أي حظر حكومي (في الجمهورية السلوفاكية أو غيرها)؛

ح) قد يتصل ESET Secure Data بخوادم الموفر من وقت لآخر للتحقق من معلومات الترخيص، والتصحيحات المتوفرة، وتصحيحات الخدمة وغيرها من التحديثات التي قد تعمل على تحسين تشغيل ESET Secure Data أو الاحتفاظ به أو تعديله أو تعزيزه. قد يقوم البرنامج بإرسال معلومات عامة حول النظام مرتبطة بعمله بما يتوافق مع "سياسة الخصوصية".

ط) لا يتحمل الموفر مسؤولية أي فقدان أو تلف أو نفقات أو ادعاء ناتج عن فقدان كلمات المرور أو سرقتها أو إساءة استخدامها أو تلفها او تدميرها، أو إعداد المعلومات، أو مفاتيح التشفير، أو رموز تفعيل الترخيص وغيرها من البيانات التي تم إنشاؤها أو تخزينها في أثناء استخدام البرنامج.

تنطبق أحكام إضافية لـESET Secure Data حصرياً على المستخدمين النهائيين لـESET Smart Security Premium.

برنامج Password Manager. تنطبق أحكام إضافية على برنامج Password Manager على النحو التالي:

1. تصريح مستخدم إضافي. أنت تقر وتوافق بأنه لا يجوز لك:

أ (استخدام برنامج مدير كلمة المرور لتشغيل أي من التطبيقات ذات المهام الحرجة التي تنطوي على مخاطر على الحياة البشرية أو الممتلكات. أنت تتفهم أن برنامج مدير كلمة المرور غير مصمم لهذه الأغراض وأن استخدامه بشكل خاطئ في مثل هذه الحالات قد يؤدي إلى الوفاة او الإصابة الشخصية أو تلف كبير في الممتلكات أو البيئة والتي لا يتحمل الموفر أي مسؤولية عنها.

لم يتم تصميم برنامج مدير كلمة المرور أو ترخيصه أو بغرض الاستخدام في البيئات الخطرة التي تتطلب ضوابط احتياط الأمان عند التعطل بما في ذلك، على سبيل المثال لا الحصر، تصميم أو إنشاء أو صيانة المنشآت النووية أو الملاحة الجوية أو أنظمة الاتصال أو المراقبة الجوية ودعم الحياة أو أنظمة الأسلحة. لا يعترف الموفر على وجه التحديد بأي ضمان صريح أو ضمني للمطابقة لمثل هذه الأغراض.

ب) استخدام برنامج مدير كلمة المرور بطريقة تنتهك هذه الاتفاقية أو تنهتك قوانين الجمهورية السلوفاكية أو السلطة القانونية لديك. لا يجوز لك على وجه التحديد استخدام برنامج مدير كلمة المرور للقيام بأي أنشطة غير مشروعة أو الترويج لها بما في ذلك تحميل بيانات تحتوي على محتوى ضار أو محتوى يُمكن استخدامه في أي أنشطة غير قانونية أو بأي شكل من الأشكال تنتهك القانون أو حقوق الجهة الخارجية (بما في ذلك حقوق الملكية الفكرية)، بما في ذلك على سبيل المثال لا الحصر أية محاولات للوصول إلى الحسابات الموجودة في مساحة التخزين (لأغراض هذه الشروط الإضافية لبرنامج Password Manager تشير كلمة "مساحة التخزين" إلى مساحة تخزين البيانات التي تتم إدارتها من قبل الموفر أو جهة خارجية غير المزود والمستخدم لغرض

تمكين المزامنة ونسخ بيانات المستخدم احتياطياً) أو أية حسابات وبيانات لبرنامج مدير كلمة المرور أو مستخدمي مساحة التخزين. إذا انتهكت أي من هذه الاحكام، يحق للموفر إنهاء هذه الاتفاقية على الفور وفرض أي تكلفة إصلاح عليك، وكذلك اتخاذ أي خطوات ضرورية لمنعك من استخدام برنامج مدير كلمة المرور بعد الآن دون إمكانية الاسترداد.

2. تحديد المسؤولية. يتم توفير برنامج مدير كلمة المرور "كما هو". دون ضمان من أي نوع، سواء كان صريحاً أو ضمنياً. كما أنك تستخدم البرناج على مسؤوليتك الخاصة. والمنتج غير مسؤول عن أي فقدان في البيناات أو تلف أو تقييد توافر البيانات بما في ذلك أي بيانات ترل بواسطة برنامج مدير كلمة المرور إلى وحدة تخزين خارجية بغرض مزامنة البيناات والنسخ الاحتياطي. وتشفير البيانات باستخدام برنامج مدير كلمة المرور لا يفرض أي مسؤولية على الموفر فيما يخص أمان البيانات. أنت توافق صراحةً على أن البيانات التي يتم الحصول عليها أو استخدامها أو تشفيرها أو تخزينها أو مزامنتها او إرسالها باستخدام برنامج مدير كلمة المرور يُمكن أيضاً تخزينها على خدمات تابعة لجهة خارجية)ينطبق فقط على استخدام برنامج مدير كلمة المرور حيث تكون خدمات المزامنة والنسخ الاحتياطي ممكّنة). إذا كان الموفر، وفقاً لتقديره الخاص، يختار استخدام مثل مساحة التخزين هذه الخاصة بجهة خارجية أو موقع ويب أو بوابة ويب أو خادم أو خدمة، فلا يكون الموفر مسؤولاً عن الجودة أو الأمان أو توافر مثل هذه الخدمة التابعة لجهة خارجية ولا يكون المستخدم مسؤولاً بأي حال عن أي انتهاك للالتزامات التعاقدية أو القانونية من قبل الجهة الخارجية او عن التلف أو خسارة الأرباح أو الأضرار المالية أو غير المالية او أي نوع آخر من الفقدان في أثناء استخدام هذا البرنامج. لا يتحمل الموفر مسؤولية أي محتوى يتم الحصول عليه أو استخدامه أو تشفيره أو تخزينه أو مزامنته أو إرساله باستخدام برنامج مدير كلمة المرور أو موجود في مساحة التخزين. أنت تقر بأن الموفر لا يُمكنه الوصول إلى المحتوى الخاص بالبيانات المخزّنة ولا يُمكنه مراقبتها أو إزالة المحتوى الضار قانوناً.

الموفر لديه جميع حقوق القيام بالتحسينات وعمليات الترقية والإصلاحات المرتبطة ببرنامج مدير كلمة المرور "(التحسينات(" حتى في حال القيام بمثل هذه التحسينات على أساس التعليقات أو الأفكار أو الاقتراحات الواردة من جانبك بأي شكل. ولن يكون لك الحق في الحصول على أي تعويض، بما في ذلك أية عوائد مرتبطة بهذه التحسينات.

لا تتحمل كيانات الموفر أو المرخصين مسؤولية المطالبات والالتزامات الصادرة منك عن أي نوع ينشأ أو مرتبط بأي حال باستخدام برنامج مدير كلمة المرور من خلالك أو من خلال جهات خارجية، لاستخدام أو عدم استخدام أي شركة سمسرة أو تاجر، أو بيع أو شراء أي أوراق مالية، سواء كانت هذه الادعاءات تستند إلى أي نظرية قانونية أو عادلة.

لا تتحمل كيانات الموفر والمرخصين المسؤولية تجاهك عن أي أضرار مباشرة أو عرضية أو خاصة أو غير مباشرة أو لاحقة أو ناتجة عن أو مرتبطة بأي برامج تابعة لجهات خارجية أو أي بيانات يتم الوصول إليها من خلال برامج إدارة كلمات المرور، أو استخدامك لبرامج إدارة كلمات المرور أو عدم قدرتك على استخدامها أو الوصول إليها، أو أي بيانات متوفرة من خلال برامج إدارة كلمات المرور، سواء كانت ادعاءات هذا الضرر صادرة عن أي نظرية قانون أو مبدئ، دون تقييد، أو خسارة أرباح الأعمال أو إصابات الأشخاص أو أضرار الممتلكات أو توقف العمل أو فقدان العمل أو المعلومات الشخصية. لا تسمح بعض السلطات القضائية بتقييد الأضرار التبعية أو العرضية ولذا قد لا ينطبق عليك هذا القيد. في هذه الحالة ستكون مسؤولية الموفر هي الحد الأدنى المسموح بموجب القانون المعمول به.

المعلومات المتوفرة من خلال برنامج مدير كلمة المرور، بما في ذلك أسعار الأسهم والتحليل ومعلومات السوق والأخبار والبيانات المالية قد تتأخر أو قد تكون غير دقيقة أو تتضمن أخطاء أو نسيان، ولن تتحمل كيانات الموفر والمرخصين أية مسؤولية فيما يتعلق بذلك. ويجوز للموفر تغيير أي جانب أو ميزة لبرنامج مدير كلمة المرور أو استخدام أي من الميزات أو التقنيات الموجودة في برنامج مدير كلمة المرور في أي وقت دون إشعار مسبق.

إذا كانت الأحكام الواردة في هذه المادة باطلة لأي سبب أو كان الموفر مسؤولاً عن أي خسائر، أو تلفيات أو غيرها وفقاً للقوانين المعمول بها. يوافق طرفا العقد على أن مسؤولية الموفر تجاهك ستقتصر على المبلغ الإجمالي لتكاليف الترخيص المدفوعة من

قبلك.

أنت توافق على تعويض الموفر والدفاع عنه وتحمل خسائره والموظفين التابعين له، والشركات الفرعية والشركات التابعة وإعادة تسمية العلامة التجارية وغيرها من الشركاء ضد أي ادعاءات أو مساءلات أو أضرار أو فقدان أو تكاليف أو نفقات أو أتعاب أي من الجهات الخارجية)بما في ذلك مالكي الجهاز أو الذين تأثرت حقوقهم من خلال البيانات المستخدمة في برنامج كلمة المرور أو مساحة التخزين(، والتي قد تتكبدها هذه الجهات نتيجة استخدامك لبرنامج مدير كلمة المرور.

3. البيانات الموجودة في برنامج مدير كلمة المرور ما لم يرد خلاف ذلك، وبشكل واضح، محدد من قبلك، يتم تخزين جميع البيانات التي قمت بإدخالها والتي تم حفظها في قاعدة بيانات برنامج مدير كلمة المرور في تنسيق مشفر على الكمبيوتر لديك أو غيره من أجهزة التخزين كم هو محدد من قبلك. أنت تتفهم أنه في حالة حذف أي محتوى ضمن قاعدة بيانات برنامج مدير كلمة المرور أو غيره من الملفات أو تلفه، فسيتم فقدان كافة البيانات الواردة فيه بشكل لا رجعة فيه كما تفهم وتقر بخطورة هذه الخسارة. حقيقة أنه يتم تخزين بياناتك الشخصية في تنسيق مشفر على الكمبيوتر لا تعني أن المعلومات لا يُمكن سرقتها أو إساءة استخدامها من قبل شخص ما يكتشف "كلمة المرور الرئيسية "أو يحصل على جهاز التفعيل المحدد بالمستهلك لفتح قاعدة البيانات. أنت المسؤول عن الحفاظ على أمان جميع طرق الوصول.

4. نقل البيانات الشخصية إلى موفر أو جهاز تخزين إذا حددت ذلك وفقط لغرض ضمان المزامنة والنسخ الاحتياطي في الوقت المحدد، يقوم برنامج مدير كلمة المرور بنقل البيانات الشخصية أو إرسالها من خلال قاعدة بيانات برنامج مدير كلمة المرور ـ أي كلمات المرور، ومعلومات تسجيل الدخولن والحسابات والكيانات ـ عبر الإنترنت إلى مساحة التخزين. يتم نقل البيانات حصرياً بتنسيق مشفر. وقد يتطلب استخدام برنامج مدير كلمة المرور لملء حقول عبر الإنترنت تحتوي على كلمات مرور، أو عمليات تسجيل الدخول أو غيرها من البيانات إرسال المعلومات عبر الإنترنت إلى موقع الويب المحدد من قبلك. لا يبدأ نقل البيانات هذا عن طريق برنامج مدير كلمة المرور ومن ثم لا يتحمل الموفر مسؤولية أمان مثل هذه العمليات مع أي موقع ويب مدعوم من قبل العديد من الموفرين. وتتم أي معاملات عبر الإنترنت سواء كانت مرتبطة ببرنامج مدير كلمة المرور أم لا على مسؤوليتك الخاصة، وستكون وحدك المسؤول عن أي تلف يحدث لنظام الكمبيوتر أو فقدان البيانات نتيجة تنزيل و/أو استخدام أي من هذه المواد أو الخدمات. وللحد من خطورة فقدان البيانات القيّمة، يوصي الموفر بإجراء نسخ احتياطي دوري لقاعدة البيانات وغيرها من الملفات الحساسة إلى محركات أقراص خارجية. لا يُمكن للمستخدم تقديم أي مساعدة بشأن استرداد البيانات المفقودة أو التالفة. وإذا كان الموفر يقدم خدمات نسخ احتياطي لملفات قاعدة بيانات المستخدم في حالة تلف أو حذف ملفات موجودة على أجهزة الكمبيوتر الشخصي للمستخدمين، فتكون خدمة النسخ الاحتياطي هذه بدون أي ضمان ولا تعني تحمل الموفر لأية مسؤولية تجاهك على الإطلاق.

باستخدام برنامج مدير كلمة المرور، أنت توافق على أن البرنامج قد يتصل بخوادم الموفر من وقت لآخر للتحقق من معلومات الترخيص، والتصحيحات المتوفرة، وتصحيحات الخدمة وغيرها من التحديثات التي قد تعمل على تحسين تشغيل برنامج مدير كلمة المرور أو الاحتفاظ به أو تعديله أو تعزيزه. قد يقوم البرنامج بإرسال معلومات عامة حول النظام مرتبطة بعمل برنامج مدير كلمة المرور بما يتوافق مع "سياسة الخصوصية".

5. معلومات وإرشادات إزالة التثبيت قبل إزالة تثبيت برنامج مدير كلمة المرور، يجب تصدير أي معلومات في قاعدة البيانات ترغب في الاحتفاظ بها.

تنطبق أحكام إضافية لبرنامج Password Manager حصرياً على المستخدمين النهائيين لـ ESET Smart Security Premium.

ESET LiveGuard. تنطبق أحكام إضافية على ESET LiveGuard على النحو التالي:

يحتوي البرنامج على وظيفة التحليل الإضافي للملفات المرسلة من قبل المستخدم النهائي. لا يجب على المزود استخدام الملفات

المرسلة إلا من قبل المستخدم النهائي ونتائج التحليل وفقاً لسياسة الخصوصية واللوائح القانونية ذات الصلة.

تنطبق أحكام إضافية لـ ESET LiveGuard حصرياً على المستخدمين النهائيين لـ ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

سياسة الخصوصية

تعد حماية البيانات الشخصية ذات أهمية خاصة لشركة ESET, spol. s r. o. بمكتبها المسجل في Einsteinova 24, 851 01 Bratislava, Slovak Republic المسجلة في السجل التجاري الذي تديره محكمة مقاطعة براتيسلافا الأولى، القسم Sro رقم الإدخال B/3586 رقم تسجيل الأعمال التجارية: 31333532 باعتبارها الجهة المتحكمة في البيانات ("ESET" أو "نحن"). نريد الامتثال لمتطلبات الشفافية كما هو موحد قانونياً بموجب النظام الأوروبي العام لحماية البيانات ("GDPR"). لتحقيق هذا الهدف، ننشر سياسة الخصوصية هذه لغرض إعلام عملائنا ("المستخدم النهائي" أو "أنت") بصفتك صاحب بيانات حول مواضيع حماية البيانات الشخصية التالية:

- القاعدة القانونية لمعالجة البيانات الشخصية،
- مشاركة البيانات والسرية،
- أمان البيانات،
- حقوقك بصفتك صاحب بيانات،
- معالجة بياناتك الشخصية
- معلومات الاتصال.

القاعدة القانونية لمعالجة البيانات الشخصية

لا يوجد سوى عدد قليل من القواعد القانونية لمعالجة البيانات التي نستخدمها وفقاً للإطار التشريعي المعمول به المتعلق بحماية البيانات الشخصية. تعد معالجة البيانات الشخصية في ESET ضرورية بشكل أساسي لأداء اتفاقية ترخيص المستخدم النهائي ("اتفاقية ترخيص المستخدم النهائي") مع المستخدم النهائي (المادة 6 (1) (ب) من اللائحة العامة لحماية البيانات)، والتي تكون قابلة للتطبيق على توفير منتجات أو خدمات ESET ما لم يُنص صراحة على خلاف ذلك، على سبيل المثال:

- القاعدة القانونية للمصلحة المشروعة (المادة 6 (1) (و) من اللائحة العامة لحماية البيانات) والتي تمكننا من معالجة البيانات حول كيفية استخدام عملائنا للخدمات ورضاهم لتزويد المستخدمين بأفضل حماية ودعم وخبرة يمكن تقديمها. حتى التسويق معترف به في التشريعات المعمول بها كمصلحة مشروعة، لذلك نعتمد عليه عادةً في التواصل التسويقي مع عملائنا.

- الموافقة (المادة 6 (1) (أ) من اللائحة العامة لحماية البيانات)، والتي قد نطلبها منك في مواقف معينة عندما نرى أن هذا الأساس القانوني هو الأنسب أو إذا كان مطلوباً بموجب القانون.

- الامتثال لالتزامات قانونية (المادة 6 (1) (ج) من اللائحة العامة لحماية البيانات) مثل، متطلبات اشتراط للاتصالات الإلكترونية للاحتفاظ بالفواتير الفواتير أو مستندات الفوترة.

مشاركة البيانات والسرية

لا نشارك بياناتك مع جهات خارجية. ومع ذلك، فإن ESET عبارة عن شركة تعمل على مستوى العالم عن طريق الكيانات التابعة أو الشركاء كجزء من شبكة المبيعات والخدمات والدعم لدينا. قد يتم نقل معلومات الترخيص والفوترة والدعم الفني التي تتم معالجتها بواسطة ESET من الكيانات التابعة أو الشركاء وإليها بغرض الوفاء باتفاقية ترخيص المستخدم النهائي (EULA) مثل تقديم الخدمات أو الدعم.

تفضل ESET معالجة بياناتها في الاتحاد الأوروبي (EU). ومع ذلك، بناءً على موقعك (استخدام منتجاتنا و / أو خدماتنا خارج الاتحاد الأوروبي) و / أو الخدمة التي تختارها، فقد يكون من الضروري نقل بياناتك إلى بلد خارج الاتحاد الأوروبي. على سبيل المثال، نستخدم خدمات الأطراف الخارجية فيما يتعلق بالحوسبة السحابية. في هذه الحالات، نختار بعناية مزودي الخدمات لدينا ونضمن مستوى مناسباً من حماية البيانات عبر التدابير التعاقدية والفنية والتنظيمية. كقاعدة عامة، نتفق على البنود التعاقدية القياسية للاتحاد الأوروبي، وإذا لزم الأمر، مع اللوائح التعاقدية التكميلية.

بالنسبة لبعض البلدان خارج الاتحاد الأوروبي، مثل المملكة المتحدة وسويسرا، فقد حدد الاتحاد الأوروبي بالفعل مستوى مماثلاً لحماية البيانات. ونظراً للمستوى المماثل لحماية البيانات، لا يتطلب نقل البيانات إلى هذه البلدان أي ترخيص أو تخويل خاص.

أمان البيانات

تنفذ ESET التدابير الفنية والتنظيمية المناسبة لضمان مستوى أمان يتناسب مع المخاطر المحتملة. نبذل قصارى جهدنا لضمان السرية المستمرة والنزاهة وإتاحة ومرونة أنظمة المعالجة والخدمات. ومع ذلك، في حال اختراق البيانات الذي يؤدي إلى وجود مخاطر على الحقوق والحريات لديك، نحن على استعداد لإخطار السلطة الإشرافية ذات الصلة وكذلك المستخدمين النهائيين المتأثرين كأصحاب بيانات.

حقوق صاحب البيانات.

تعد حقوق كل مستخدم نهائي أمراً مهماً ونود أن نعلمك أن جميع المستخدمين النهائيين (من أي دولة داخل أو خارج الاتحاد الأوروبي) لديهم الحقوق التالية المضمونة في ESET. لممارسة حقوقك كصاحب بيانات، يمكنك الاتصال بنا عبر نموذج الدعم أو من خلال البريد الإلكتروني على dpo@eset.sk. لأغراض تحديد الهوية، نطلب منك المعلومات التالية: الاسم وعنوان البريد الإلكتروني – إذا كان متوفراً – ومفتاح الترخيص أو رقم العميل وانتساب الشركة. يرجى الامتناع عن إرسال أية بيانات شخصية أخرى إلينا، مثل تاريخ الميلاد. نود أن نشير إلى أنه لنتمكن من معالجة طلبك، وكذلك لأغراض تحديد الهوية، سنعالج بياناتك الشخصية.

الحق في سحب الموافقة. يكون الحق في سحب الموافقة قابل للتطبيق إذا كانت المعالجة بناءً على الموافقة فقط. إذا عالجنا بياناتك الشخصية بناءً على موافقتك، فيحق لك سحب الموافقة في أي وقت دون إبداء أسباب. لا يسري سحب الموافقة إلا في المستقبل، ولا يؤثر على قانونية البيانات التي تمت معالجتها قبل السحب.

الحق في الاعتراض. يكون الحق في الاعتراض على المعالجة قابل للتطبيق إذا كانت المعالجة بناءً على المصلحة المشروعة لـ ESET أو الأطراف الخارجية. إذا عالجنا بياناتك الشخصية لحماية أحد المصالح المشروعة، فلديك الحق بصفتك صاحب البيانات في الاعتراض على المصلحة المشروعة التي حددناها ومعالجة بياناتك الشخصية في أي وقت. لا يسري الحق في الاعتراض إلا في المستقبل، ولا يؤثر على قانونية البيانات التي تمت معالجتها قبل الاعتراض. إذا عالجنا بياناتك الشخصية لأغراض التسويق المباشر، فليس من الضروري إبداء أسباب الاعتراض. ينطبق هذا أيضاً على جمع المعلومات، بقدر ما يرتبط بمثل هذا التسويق

المباشر. في جميع الحالات الأخرى، نطلب منك إعلامنا بإيجاز بشكواك ضد المصلحة المشروعة لـ ESET لمعالجة بياناتك الشخصية.

يرجى ملاحظة أنه في بعض الحالات وعلى الرغم من سحب موافقتك، يحق لنا إجراء مزيد من المعالجة لبياناتك الشخصية بناءً على قاعدة قانونية أخرى، على سبيل المثال، لتنفيذ عقد.

الحق في الوصول. بصفتك صاحب بيانات، لديك الحق في الحصول على معلومات حول بياناتك المخزنة بواسطة ESET مجاناً في أي وقت.

الحق في التصحيح. إذا عالجنا عن غير قصد بيانات شخصية غير صحيحة عنك، فيحق لك تصحيح ذلك.

الحق في المحو والحق في تقييد المعالجة. بصفتك صاحب بيانات، لديك الحق في طلب حذف معالجة بياناتك الشخصية أو تقييدها. إذا عالجنا بياناتك الشخصية، على سبيل المثال، بموافقتك، يحق لك سحبها وليس هناك أي قاعدة قانونية أخرى، على سبيل المثال، أحد العقود، سنحذف بياناتك الشخصية على الفور. سيتم أيضاً حذف بياناتك الشخصية بمجرد أن تصبح غير مطلوبة للأغراض المذكورة لها في نهاية فترة الاحتفاظ لدينا.

إذا استخدمنا بياناتك الشخصية لغرض وحيد وهو التسويق المباشر وألغيت موافقتك أو اعترضت على المصلحة المشروعة الأساسية لـ ESET فسنقوم بتقييد معالجة بياناتك الشخصية للحد الذي نقوم فيه بتضمين بيانات اتصالك في القائمة السوداء الداخلية لدينا لتجنب الاتصال غير المرغوب فيه. خلاف ذلك، سيتم حذف بياناتك الشخصية.

يرجى ملاحظة أنه قد يُطلب منا تخزين بياناتك حتى انتهاء الالتزامات وفترات الاحتفاظ الصادرة عن المُشرّع أو الهيئات المشرفة. قد تنشأ التزامات وفترات احتفاظ أيضاً من التشريع السلوفاكي. بعد ذلك، سيتم حذف البيانات المقابلة بشكل روتيني.

الحق في إمكانية نقل البيانات. بصفتك صاحب بيانات، يسعدنا أن نقدم لك البيانات الشخصية التي تتم معالجتها بواسطة ESET بتنسيق xls.

الحق في تقديم شكوى. بصفتك صاحب بيانات، يحق لك تقديم شكوى إلى هيئة مشرفة في أي وقت. تخضع ESET للائحة قوانين دولة سلوفاكيا ونحن ملزمون بقانون حماية البيانات لأننا جزء من الاتحاد الأوروبي. الهيئة المشرفة على البيانات ذات الصلة هي مكتب حماية البيانات الشخصية للجمهورية السلوفاكية، يقع في Hraničná 12, 82007 Bratislava 27, Slovak Republic.

معالجة بياناتك الشخصية

يتم توفير الخدمات التي تقدمها ESET المطبقة في منتجاتنا بموجب شروط إتفاقية ترخيص المستخدم، ولكن بعضها قد يتطلب اهتماماً خاصاً. نود أن نزودك بمزيد من التفاصيل حول جمع البيانات المرتبطة بتقديم خدماتنا. نقدم خدمات متنوعة موصوفة في إتفاقية ترخيص المستخدم والمنتج مستند. ولكي نجعل كل شيء يعمل، نحتاج إلى جمع المعلومات التالية:

بيانات الترخيص والفوترة. يتم جمع الاسم وعنوان البريد الإلكتروني ومفتاح الترخيص وعنوانه (إن وُجد) وانتساب الشركة وبيانات الدفع ومعالجتها بواسطة ESET من أجل تسهيل تنشيط الترخيص وتسليم مفتاح الترخيص والتذكير بانتهاء الصلاحية وطلبات الدعم والتحقق من أصالة الترخيص وتقديم الخدمات والإشعارات الأخرى التي تتضمن الرسائل التسويقية بما يتماشى مع التشريعات المعمول بها أو موافقتك. تلتزم ESET قانوناً بالاحتفاظ بمعلومات الفوترة لمدة 10 سنوات، ومع ذلك، ستكون معلومات الترخيص مجهولة المصدر في موعد لا يتجاوز 12 شهراً بعد انتهاء صلاحية الترخيص.

التحديث والإحصائيات الأخرى. تتضمن المعلومات التي تمت معالجتها المعلومات المتعلقة بعملية التثبيت وجهاز الكمبيوتر

الخاص بك بما في ذلك النظام الأساسي الذي تم تثبيت منتجنا عليه ومعلومات حول عمليات ووظائف منتجاتنا مثل نظام التشغيل ومعلومات الأجهزة ومعرفات التثبيت ومعرفات الترخيص وعنوان IP وعنوان MAC وإعدادات التكوين الخاصة بالمنتج التي تمت معالجتها بغرض توفير خدمات التحديث والترقية ولغرض الصيانة والأمان وتحسين البنية التحتية للواجهة الخلفية لدينا.

يتم الاحتفاظ بهذه المعلومات بصرف النظر عن معلومات التعريف المطلوبة لأغراض الترخيص والفوترة لأنها لا تتطلب تحديد هوية المستخدم النهائي. تصل فترة الاحتفاظ إلى 4 سنوات.

نظام سمعة ESET LiveGrid®. تتم معالجة عمليات التجزئة أحادية الاتجاه بالتسلل لغرض نظام سمعة ESET LiveGrid® الذي يعمل على تحسين كفاءة حلول مكافحة البرمجيات الخبيثة لدينا من خلال مقارنة الملفات المفحوصة مع قاعدة بيانات تحتوي على عناصر مدرجة في القائمة البيضاء وقائمة سوداء في السحابة. لم يتم التعرف على المستخدم النهائي خلال هذه العملية.

نظام ملاحظات ESET LiveGrid®. عينات وبيانات تعريف مريبة من كل مكان كجزء من نظام ملاحظات ESET LiveGrid® الذي يعمل على تمكين ESET من التفاعل على الفور مع احتياجات مستخدمينا النهائيين وإبقائنا مستجيبين لأحدث التهديدات المقدمة. نحن نعتمد على إرسالك لنا

- عمليات التسلل مثل العينات المحتملة من الفيروسات والبرمجيات الخبيثة الأخرى والكائنات المريبة أو المزعجة أو غير مرغوب فيها أو غير الآمنة مثل الملفات القابلة للتنفيذ أو رسائل البريد الإلكتروني التي أبلغت عنها كرسائل غير مرغوب فيها أو تم الإبلاغ عنها بواسطة منتجنا؛
- معلومات تتعلق باستخدام الإنترنت مثل عنوان بروتوكول الإنترنت IP وحزم IP وعناوين URL وإطارات الإيثرنت؛
- ملفات تفريغات الأعطال والمعلومات الواردة.

لا نرغب في جمع بيانات خارج هذا النطاق ولكن في بعض الأحيان يستحيل تجنب ذلك. قد تُضمن البيانات المجمعة دون قصد في المحتوى الضار ولا ننوي أن تكون جزءاً من أنظمتنا أو معالجتها للغرض المصرح به في سياسة الخصوصية هذه.

من المفترض أن تُستخدم جميع المعلومات التي تم الحصول عليها ومعالجتها من خلال نظام ملاحظات ESET LiveGrid® دون تحديد هوية المستخدم النهائي.

د) **تقييم الأمان للأجهزة المتصلة بالشبكة.** لتوفير وظيفة تقييم الأمان، نقوم بمعالجة اسم الشبكة المحلية ومعلومات حول الأجهزة في الشبكة المحلية لديك مثل التواجد والنوع والاسم وعنوان IP وعنوان MAC للجهاز في الشبكة المحلية لديك فيما يتعلق بمعلومات الترخيص. تتضمن المعلومات أيضاً نوع الأمان اللاسلكي ونوع التشفير اللاسلكي لأجهزة التوجيه. ستكون معلومات الترخيص التي تحدد المستخدم النهائي مجهولة المصدر في موعد لا يتجاوز 12 شهراً بعد انتهاء صلاحية الترخيص.

الدعم الفني. قد تكون معلومات الاتصال والترخيص والبيانات الواردة في طلبات الدعم لديك مطلوبة لخدمة الدعم. بناءً على القناة التي تختارها للتواصل معنا، قد نجمع عنوان بريدك الإلكتروني ورقم هاتفك ومعلومات الترخيص وتفاصيل المنتج ووصف حالة الدعم الخاصة بك. قد يُطلب منك تزويدنا بمعلومات أخرى لتسهيل خدمة الدعم. يتم تخزين البيانات التي تتم معالجتها للحصول على الدعم الفني لمدة 4 سنوات.

الحماية من إساءة استخدام البيانات إذا تم إنشاء حساب ESET HOME على https://home.eset.com وتم تنشيط الوظيفة بواسطة المستخدم النهائي فيما يتعلق بسرقة جهاز الكمبيوتر، فسيتم جمع المعلومات التالية ومعالجتها: بيانات الموقع ولقطات الشاشة وبيانات تكوين جهاز الكمبيوتر والبيانات المسجلة بواسطة كاميرا جهاز الكمبيوتر. يتم تخزين البيانات التي تم جمعها على خوادمنا أو على خوادم مزودي خدماتنا بفترة احتفاظ مدتها 3 أشهر.

Password Manager. إذا اخترت تنشيط وظيفة Password Manager فسيتم تخزين البيانات المتعلقة بتفاصيل تسجيل الدخول لديك في نموذج مشفر فقط على جهاز الكمبيوتر الخاص بك أو جهاز آخر معين. إذا قمت بتفعيل خدمة المزامنةشؤون فسيتم تخزين البيانات المشفرة على خوادمنا أو على خوادم مزودي الخدمة لدينا لضمان هذه الخدمة. لا يوجد لدي ESET أو مزود الخدمة حق الوصول إلى البيانات المشفرة. فقط لديك مفتاح فك تشفير البيانات. ستتم إزالة البيانات عند إلغاء تنشيط الوظيفة.

ESET LiveGuard. إذا اخترت تنشيط وظيفة ESET LiveGuard فستتطلب تقديم عينات مثل الملفات المحددة مسبقاً والمحددة بواسطة المستخدم النهائي. سيتم تحميل العينات التي تختارها للتحليل عن بُعد إلى خدمة ESET وسيتم إرسال نتيجة التحليل مرة أخرى إلى جهاز الكمبيوتر الخاص بك. تتم معالجة أي عينات مريبة بطريقة المعلومات التي يتم جمعها بواسطة نظام ملاحظات ESET LiveGrid®.

برنامج تحسين تجربة العميل. إذا اخترت التنشيط برنامج تحسين تجربة العميل ، فسيتم جمع معلومات القياس عن بُعد المجهولة المتعلقة باستخدام منتجاتنا واستخدامها بناءً على موافقتك.

يرجى ملاحظة أنه إذا لم يكن الشخص الذي يستخدم منتجاتنا وخدماتنا هو المستخدم النهائي الذي اشترى المنتج أو الخدمة وأبرم اتفاقية ترخيص المستخدم النهائي (EULA) معنا، (على سبيل المثال، موظف لدى المستخدم النهائي أو أحد أفراد العائلة أو شخص مخول لاستخدام منتج أو خدمة بخلاف ذلك من قِبل المستخدم النهائي بما يتوافق مع اتفاقية ترخيص المستخدم النهائي، فستتم معالجة البيانات في المصلحة المشروعة لـ ESET بالمعنى المقصود في المادة 6 (1) و) من القانون العام لحماية البيانات (GDPR) لتمكين المستخدم المصرّح له من قبل المستخدم النهائي من استخدام المنتجات والخدمات التي نقدمها وفقاً لاتفاقية ترخيص المستخدم النهائي.

معلومات الاتصال

إذا كنت ترغب في ممارسة حقك كصاحب بيانات أو لديك سؤال أو مشكلة، فأرسل لنا رسالة على العنوان التالي:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk