ESET Internet Security

Οδηγος χρηστη

Κάντε κλικ εδώ για να εμφανίσετε την ηλεκτρονική έκδοση αυτού του εγγράφου

Digital Security
Progress. Protected.

Το ESET Internet Security αναπτύχθηκε από την ESET, spol. s r.o.

Για περισσότερες πληροφορίες επισκεφθείτε τη διεύθυνση https://www.eset.com.

Τεχνική Υποστήριξη: https://support.eset.com

REV. 12/4/2024

ESET Internet Security

Το ESET Internet Security αντιπροσωπεύει μια νέα προσέγγιση για πραγματικά ολοκληρωμένη ασφάλεια του υπολογιστή. Η πιο πρόσφατη έκδοση του μηχανισμού σάρωσης ESET LiveGrid®, σε συνδυασμό με τις προσαρμοσμένες μονάδες Firewall και Antispam, αξιοποιεί την ταχύτητα και την ακρίβεια για να διατηρεί ασφαλή τον υπολογιστή σας. Το αποτέλεσμα είναι ένα έξυπνο σύστημα που βρίσκεται συνεχώς σε εγρήγορση για επιθέσεις και κακόβουλο λογισμικό που μπορεί να θέσει τον υπολογιστή σας σε κίνδυνο.

Το ESET Internet Security είναι μια πλήρης λύση ασφάλειας που συνδυάζει μέγιστη προστασία και ελάχιστο αποτύπωμα στο σύστημα. Οι προηγμένες τεχνολογίες μας χρησιμοποιούν τεχνητή νοημοσύνη για να αποτρέψουν τη διείσδυση από ιούς, spyware, trojan horses, worm, adware, rootkit και άλλες απειλές, χωρίς να παρακωλύουν την απόδοση του συστήματος ή να διαταράσσουν τον υπολογιστή σας.

Δυνατότητες και οφέλη

Εκ νέου σχεδιασμένο περιβάλλον χρήστη	Το περιβάλλον χρήστη σε αυτή την έκδοση έχει επανασχεδιαστεί και απλοποιηθεί σημαντικά βάσει των αποτελεσμάτων των δοκιμών χρηστικότητας. Όλα τα περιεχόμενα και οι ειδοποιήσεις του γραφικού περιβάλλοντος έχουν μελετηθεί προσεκτικά και το περιβάλλον χρήστη παρέχει πλέον υποστήριξη για γλώσσες που γράφονται από δεξιά προς τα αριστερά, όπως εβραϊκά και αραβικά. Η Ηλεκτρονική βοήθεια είναι πλέον ενοποιημένη με το ESET Internet Security και παρέχει περιεχόμενο υποστήριξης το οποίο ενημερώνεται δυναμικά.
Antivirus και Antispyware	Προληπτική ανίχνευση και καθαρισμός των περισσότερων γνωστών και άγνωστων ιών, worm, trojan και rootkit. Ο Προηγμένος ευριστικός έλεγχος επισημαίνει ακόμη και κακόβουλο λογισμικό που δεν έχει παρουσιαστεί ξανά, προστατεύοντάς σας από άγνωστες απειλές και εξουδετερώνοντάς τις προτού κάνουν κακό. Η Προστασία πρόσβασης στο διαδίκτυο και η προστασία Anti-Phishing λειτουργούν με παρακολούθηση της επικοινωνίας μεταξύ των προγραμμάτων περιήγησης στον ιστό και των απομακρυσμένων διακομιστών (συμπεριλαμβανομένου του SSL). Η Ενεργοποίηση προστασίας ηλεκτρονικής αλληλογραφίας παρέχει έλεγχο της επικοινωνίας email που λαμβάνεται μέσω των πρωτοκόλλων POP3(S) και IMAP(S).
Τακτικές ενημερώσεις	Η τακτική ενημέρωση του μηχανισμού ανίχνευσης (ο οποίος ονομαζόταν παλαιότερα «βάση αναγνώρισης ιών») και των μονάδων του προγράμματος είναι ο καλύτερος τρόπος για να διασφαλίσετε το μέγιστο επίπεδο ασφάλειας στον υπολογιστή σας.
ESET LiveGrid® (Φήμη που βασίζεται σε Cloud)	Μπορείτε να ελέγξετε τη φήμη των διεργασιών που εκτελούνται και των αρχείων απευθείας από το ESET Internet Security.
Έλεγχος συνδεδεμένων συσκευών	Σαρώνει αυτόματα όλες τις μονάδες δίσκου USB flash, τις κάρτες μνήμης και τα CD/DVD. Αποκλείει τα αφαιρούμενα μέσα με βάση τους τύπους του μέσου, τον κατασκευαστή, το μέγεθος και άλλα χαρακτηριστικά.
Λειτουργικότητα HIPS	Μπορείτε να προσαρμόσετε τη συμπεριφορά του συστήματος με μεγάλη λεπτομέρεια, να καθορίσετε κανόνες για το μητρώο του συστήματος, τις ενεργές διεργασίες και τα προγράμματα και να ρυθμίσετε τη στάση ασφάλειας που κρατάτε.

Λειτουργία Gamer	Αναβάλλει την εμφάνιση αναδυόμενων παραθύρων, ενημερώσεων και άλλων δραστηριοτήτων που εντείνουν τη λειτουργία του συστήματος για να διατηρούνται οι πόροι του συστήματος για παιχνίδια και άλλες δραστηριότητες πλήρους οθόνης.

Δυνατότητες του ESET Internet Security

Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών	Η Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών παρέχει ένα ασφαλές πρόγραμμα περιήγησης που μπορείτε να χρησιμοποιείτε σε πύλες ηλεκτρονικών τραπεζικών συναλλαγών ή ηλεκτρονικών πληρωμών, για να διασφαλίζεται ότι όλες οι ηλεκτρονικές συναλλαγές πραγματοποιούνται σε αξιόπιστο και ασφαλές περιβάλλον.
Υποστήριξη για υπογραφές δικτύου	Οι υπογραφές δικτύου επιτρέπουν γρήγορη εξακρίβωση στοιχείων και αποκλείουν την κακόβουλη κυκλοφορία προς και από συσκευές που σχετίζονται με bot και προγράμματα που εκμεταλλεύονται κενά ασφαλείας. Αυτή η δυνατότητα μπορεί να θεωρηθεί ως βελτίωση της Προστασίας botnet.
Έξυπνο Firewall	Αποτρέπει την πρόσβαση στον υπολογιστή σας από μη εξουσιοδοτημένους χρήστες και την εκμετάλλευση των προσωπικών σας δεδομένων.
ESET Antispam	Τα μηνύματα spam αντιπροσωπεύουν 50 τοις εκατό του συνόλου της επικοινωνίας με ηλεκτρονική αλληλογραφία. Η προστασία Antispam προστατεύει από αυτό το πρόβλημα.
Anti-Theft	Το Anti-Theft επεκτείνει την ασφάλεια σε επίπεδο χρήστη σε περίπτωση απώλειας ή κλοπής του υπολογιστή. Όταν οι χρήστες εγκαταστήσουν το ESET Internet Security και το Anti-Theft, η συσκευή τους θα αναγράφεται στη διασύνδεση ιστού. Η διασύνδεση ιστού επιτρέπει στους χρήστες να διαχειρίζονται τη διαμόρφωση ρυθμίσεων του Anti-Theft και να παρέχουν δυνατότητες anti-theft στη συσκευή τους.
Γονικός έλεγχος	Προστατεύει την οικογένειά σας από δυνητικά προσβλητικό περιεχόμενο ιστού αποκλείοντας διάφορες κατηγορίες ιστότοπων.

Για να λειτουργούν οι δυνατότητες του ESET Internet Security πρέπει να είναι ενεργή η άδεια χρήσης. Συνιστάται να ανανεώνετε την άδεια χρήσης σας αρκετές εβδομάδες πριν από τη λήξη της άδειας χρήσης για το ESET Internet Security.

Τι νέο υπάρχει

Τι νέο υπάρχει στο ESET Internet Security 15

Βελτιωμένος Ελεγκτής δικτύου (πρώην Συνδέσεις οικιακού δικτύου)

Βοηθά στην προστασία του δικτύου σας και των συσκευών IoT, και εμφανίζει συσκευές που είναι συνδεδεμένες με τον δρομολογητή. Μάθετε πώς μπορείτε να ελέγξετε τα δίκτυα που χρησιμοποιείτε και ποιες συσκευές είναι συνδεδεμένες.

ESET HOME (πρώην myESET)

Παρέχει αυξημένη ορατότητα και έλεγχο της ασφάλειάς σας. Εγκαταστήστε προστασία για νέες συσκευές, προσθέστε και κάντε κοινή χρήση αδειών χρήσης, και λάβετε σημαντικές ειδοποιήσεις μέσω της εφαρμογής για κινητές συσκευές και της διαδικτυακής πύλης. Για περισσότερες

πληροφορίες, επισκεφτείτε το θέμα Οδηγός Ηλεκτρονικής βοήθειας του ESET HOME.

Βελτιωμένο Σύστημα αποτροπής εισβολών από κεντρικό υπολογιστή (HIPS)

Σαρώνει τμήματα μνήμης που μπορούν να τροποποιηθούν με προηγμένες τεχνικές εισαγωγής κακόβουλου λογισμικού. Οι βελτιώσεις επεκτείνουν την τεχνολογική δυνατότητα ανίχνευσης για τις πιο προηγμένες εισβολές κακόβουλου λογισμικού.

Για εικόνες και πρόσθετες πληροφορίες σχετικά με τις νέες δυνατότητες στο ESET Internet Security, ανατρέξτε στο θέμα Τι νέο υπάρχει στην πιο πρόσφατη έκδοση των οικιακών προϊόντων της ESET.

> **i** Για να απενεργοποιήσετε τις **Ειδοποιήσεις της εφαρμογής What's new**, κάντε κλικ στα στοιχεία **Ρυθμίσεις για προχωρημένους** > **Ειδοποιήσεις** > **Ειδοποιήσεις επιφάνειας εργασίας**. Κάντε κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Ειδοποιήσεις επιφάνειας εργασίας** και καταργήστε την επιλογή του πλαισίου ελέγχου **Εμφάνιση ειδοποιήσεων της εφαρμογής What's new**. Για περισσότερες πληροφορίες σχετικά με τις ειδοποιήσεις, ανατρέξτε στην ενότητα Ειδοποιήσεις.

Ποιο προϊόν έχω;

Η ESET προσφέρει πολλά επίπεδα ασφάλειας με νέα προϊόντα από μια ισχυρή και γρήγορη λύση antivirus μέχρι μια λύση ασφάλειας "όλα σε ένα" με ελάχιστες επιπτώσεις στο σύστημα:

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

Για να προσδιορίσετε το προϊόν που έχετε εγκαταστήσει, ανοίξτε το κύριο παράθυρο του προγράμματος και θα δείτε το όνομα του προϊόντος στο επάνω μέρος του παραθύρου (ανατρέξτε στο άρθρο της Γνωσιακής βάσης).

Στον παρακάτω πίνακα περιγράφονται λεπτομερώς οι δυνατότητες που είναι διαθέσιμες σε κάθε συγκεκριμένο προϊόν.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Μηχανισμός ανίχνευσης:	✔	✔	✔
Προηγμένη εκμάθηση υπολογιστή	✔	✔	✔
Λειτουργία αποτροπής κενών ασφαλείας	✔	✔	✔
Προστασία από επιθέσεις βασισμένες σε δέσμες ενεργειών	✔	✔	✔
Anti-Phishing	✔	✔	✔
Προστασία πρόσβασης στο διαδίκτυο	✔	✔	✔
HIPS (συμπεριλαμβάνει Προστασία Ransomware)	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Antispam		✔	✔
Τείχος προστασίας		✔	✔
Ελεγκτής δικτύου		✔	✔
Προστασία κάμερας		✔	✔
Προστασία από επιθέσεις δικτύου		✔	✔
Προστασία botnet		✔	✔
Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών		✔	✔
Γονικός έλεγχος		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Ορισμένα από τα παραπάνω προϊόντα ενδέχεται να μην είναι διαθέσιμα στη γλώσσα/περιοχή σας.

Απαιτήσεις συστήματος

Το σύστημά σας θα πρέπει να πληροί τις ακόλουθες απαιτήσεις υλικού και λογισμικού προκειμένου να λειτουργεί το ESET Internet Security με βέλτιστο τρόπο:

Επεξεργαστές που υποστηρίζονται

Επεξεργαστής Intel ή επεξεργαστής AMD 32 bit (x86) με σύνολο οδηγιών SSE2 ή 64 bit (x64), 1 GHz ή νεότερη έκδοση
Επεξεργαστής με βάση το ARM64, 1GHz ή ταχύτερος

Υποστηριζόμενα λειτουργικά συστήματα*

Microsoft® Windows® 11
Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 SP1 με τις πιο πρόσφατες ενημερώσεις των Windows
Microsoft® Windows® Home Server 2011 64-bit

Προσπαθείτε πάντα να διατηρείτε το λειτουργικό σύστημα ενημερωμένο.

Το Anti-Theft δεν υποστηρίζει το Microsoft Windows Home Server.

Άλλα

Απαιτείται σύνδεση στο Internet για την ενεργοποίηση και για να λειτουργούν σωστά οι ενημερώσεις του ESET Internet Security.

Δύο προγράμματα Antivirus που εκτελούνται ταυτόχρονα σε μία συσκευή προκαλούν αναπόφευκτες διενέξεις πόρων συστήματος, όπως επιβράδυνση του συστήματος που το καθιστά μη λειτουργικό.

* Η ESET δεν θα μπορεί να παρέχει προστασία για μη υποστηριζόμενα λειτουργικά συστήματα μετά τον Φεβρουάριο του 2021.

Η έκδοση των Windows 7 δεν έχει ενημερωθεί

Ζήτημα

Εκτελείτε μια μη ενημερωμένη έκδοση του λειτουργικού συστήματος. Για να παραμένετε προστατευμένοι, προσπαθείτε πάντα να διατηρείτε το λειτουργικό σύστημα ενημερωμένο.

Λύση

Έχετε εγκαταστήσει το ESET Internet Security που εκτελείται σε {GET_OSNAME} {GET_BITNESS}.

Επαληθεύστε ότι έχετε εγκαταστήσει το Windows 7 Service Pack 1 (SP1) με τις πιο πρόσφατες ενημερώσεις των Windows (τουλάχιστον τα KB4474419 και KB4490628).

Εάν τα Windows 7 δεν έχουν διαμορφωθεί ώστε να ενημερώνονται αυτόματα, κάντε κλικ στα στοιχεία **Μενού Έναρξης** > **Πίνακας ελέγχου** > **Σύστημα και ασφάλεια** > **Windows Update** > **Έλεγχος για ενημερώσεις** και στη συνέχεια κάντε κλικ στο στοιχείο **Εγκατάσταση ενημερώσεων**.

Δείτε επίσης το θέμα Τα Windows 7 δεν υποστηρίζονται πλέον από τη Microsoft.

Τα Windows 7 δεν υποστηρίζονται πλέον από τη Microsoft

Ζήτημα

Η υποστήριξη της Microsoft για τα Windows 7 έληξε στις 14 Ιανουαρίου 2020. Τι σημαίνει αυτό;

Αν συνεχίσετε να χρησιμοποιείτε τα Windows 7 μετά τη λήξη της υποστήριξης, ο υπολογιστής σας θα εξακολουθεί να λειτουργεί, αλλά μπορεί να γίνει πιο ευάλωτος σε κινδύνους ασφαλείας και ιούς. Ο υπολογιστής σας δεν θα λαμβάνει πλέον ενημερώσεις των Windows (συμπεριλαμβανομένων των ενημερώσεων ασφαλείας).

Λύση

Θα πραγματοποιήσετε αναβάθμιση από τα Windows 7 στα Windows 10; Ενημερώστε το προϊόν ESET

Η διαδικασία αναβάθμισης είναι σχετικά εύκολη και σε πολλές περιπτώσεις μπορείτε να το κάνετε χωρίς να χάσετε τα αρχεία σας. Πριν από την αναβάθμιση σε Windows 10:

1. Έλεγχος/ενημέρωση του προϊόντος ESET
2. Δημιουργία αντιγράφων ασφαλείας για σημαντικά δεδομένα
3. Διαβάστε τις Συχνές ερωτήσεις για την αναβάθμιση σε Windows 10 της Microsoft και ενημερώστε το λειτουργικό σύστημα των Windows

Απόκτηση νέου υπολογιστή ή συσκευής; Μεταφέρετε το προϊόν ESET

Εάν πρόκειται να αγοράσετε ή έχετε αγοράσει νέο υπολογιστή ή συσκευή - μάθετε πώς να μεταφέρετε το υπάρχον προϊόν ESET σε μια νέα συσκευή.

Δείτε επίσης Η υποστήριξη για Windows 7 τελείωσε.

Τα Windows Vista δεν υποστηρίζονται πλέον

Ζήτημα

Λόγω τεχνικών περιορισμών στα Windows Vista, το ESET Internet Security δεν μπορεί να παρέχει προστασία μετά το **Φεβρουάριο 2021**. Το προϊόν ESET θα είναι πλέον **μη λειτουργικό**. Αυτό μπορεί να έχει ως αποτέλεσμα το σύστημά σας να είναι ευάλωτο σε εισβολές.

Η υποστήριξη της Microsoft για τα Windows Vista έληξε στις 11 Απριλίου 2017. Τι σημαίνει αυτό;

Αν συνεχίσετε να χρησιμοποιείτε τα Windows Vista μετά τη λήξη της υποστήριξης, ο υπολογιστής σας θα εξακολουθεί να λειτουργεί, αλλά μπορεί να γίνει πιο ευάλωτος σε κινδύνους ασφαλείας και ιούς. Ο υπολογιστής σας δεν θα λαμβάνει πλέον ενημερώσεις των Windows (συμπεριλαμβανομένων των ενημερώσεων ασφαλείας).

Λύση

Αναβάθμιση από Windows Vista σε Windows 10; Αποκτήστε νέο υπολογιστή ή συσκευή και μεταφέρετε το προϊόν ESET

Πριν από την αναβάθμιση σε Windows 10:

1. Δημιουργία αντιγράφων ασφαλείας για σημαντικά δεδομένα
2. Διαβάστε τις Συχνές ερωτήσεις για την αναβάθμιση σε Windows 10 της Microsoft και ενημερώστε το λειτουργικό σύστημα των Windows
3. Εγκαταστήστε ή μεταφέρετε το υπάρχον προϊόν ESET σε μια νέα συσκευή.

Δείτε επίσης Η υποστήριξη για Windows Vista τελείωσε.

Πρόληψη

Όταν εργάζεστε με τον υπολογιστή σας και ιδιαίτερα όταν περιηγείστε στο Internet, έχετε υπόψη σας ότι κανένα σύστημα Antivirus στον κόσμο δεν εξαφανίζει εντελώς τον κίνδυνο ανιχνεύσεων και απομακρυσμένων επιθέσεων. Για τη μέγιστη δυνατή προστασία και άνεσή σας, είναι σημαντικό να χρησιμοποιείτε τη λύση Antivirus σωστά και να τηρείτε κάποιους χρήσιμους κανόνες:

Τακτική ενημέρωση

Σύμφωνα με στατιστικά στοιχεία από το ESET LiveGrid®, χιλιάδες νέες, μοναδικές εισβολές δημιουργούνται καθημερινά με σκοπό να παρακάμψουν υφιστάμενα μέτρα ασφαλείας και να φέρουν κέρδη στους δημιουργούς τους – σε βάρος άλλων χρηστών. Οι ειδικοί τεχνικοί του Εργαστηρίου ερευνών της ESET αναλύουν αυτές τις απειλές σε καθημερινή βάση, προετοιμάζουν και δημοσιεύουν ενημερώσεις, με σκοπό να βελτιώνουν συνεχώς το επίπεδο προστασίας των πελατών μας. Για τη διασφάλιση της μέγιστης αποτελεσματικότητας αυτών των ενημερώσεων, είναι σημαντικό οι ενημερώσεις να είναι σωστά διαμορφωμένες στο σύστημά σας. Για περισσότερες πληροφορίες σχετικά με τον τρόπο διαμόρφωσης των ενημερώσεων, ανατρέξτε στο κεφάλαιο Ρυθμίσεις ενημέρωσης.

Λήψη ενημερώσεων κώδικα ασφαλείας

Οι δημιουργοί κακόβουλου κώδικα εκμεταλλεύονται συχνά διάφορα κενά ασφαλείας των συστημάτων, προκειμένου να αυξήσουν την αποτελεσματικότητα της διασποράς κακόβουλου κώδικα. Έχοντας υπόψη τους αυτό, οι εταιρείες λογισμικού παρακολουθούν στενά τις εφαρμογές τους για τυχόν ζητήματα ευπάθειας και δημοσιεύουν τακτικά ενημερώσεις ασφαλείας με σκοπό να εξαφανίσουν δυνητικές απειλές. Τα Microsoft Windows και προγράμματα περιήγησης όπως ο Internet Explorer είναι δύο παραδείγματα προγραμμάτων για τα οποία διατίθενται τακτικά ενημερώσεις ασφαλείας.

Δημιουργία αντιγράφων ασφαλείας για σημαντικά δεδομένα

Οι δημιουργοί κακόβουλου λογισμικού δεν ενδιαφέρονται για τις ανάγκες των χρηστών και η δραστηριότητα των κακόβουλων προγραμμάτων συχνά οδηγεί σε πλήρη δυσλειτουργία ενός λειτουργικού συστήματος και σε απώλεια σημαντικών δεδομένων. Είναι σημαντικό να δημιουργείτε κατά περιόδους αντίγραφα ασφαλείας για τα σημαντικά και ευαίσθητα δεδομένα σας σε ένα εξωτερικό μέσο αποθήκευσης, όπως DVD ή εξωτερικό σκληρό δίσκο. Με αυτόν τον τρόπο θα μπορείτε πιο εύκολα και πιο γρήγορα να ανακτήσετε τα δεδομένα σας σε περίπτωση βλάβης του συστήματος.

Τακτική σάρωση του υπολογιστή για ιούς

Η ανίχνευση γνωστών και άγνωστων ιών, worm, trojan και rootkit πραγματοποιείται από τη μονάδα προστασίας συστήματος αρχείων σε πραγματικό χρόνο. Αυτό σημαίνει ότι κάθε φορά που αποκτάτε πρόσβαση ή ανοίγετε ένα αρχείο, γίνεται σάρωση του αρχείου για κακόβουλη δραστηριότητα. Συνιστάται να εκτελείτε πλήρη σάρωση του υπολογιστή τουλάχιστον μία φορά το μήνα, επειδή οι υπογραφές κακόβουλου λογισμικού ενδέχεται να ποικίλλουν και επειδή ο μηχανισμός ανίχνευσης ενημερώνεται καθημερινά.

Τήρηση βασικών κανόνων ασφαλείας

Αυτός είναι ο πιο χρήσιμος και αποτελεσματικός κανόνας από όλους – να είστε πάντοτε προσεκτικοί. Σήμερα, πολλές εισβολές απαιτούν συμμετοχή του χρήστη για την εκτέλεση και την εξάπλωσή τους. Εάν είστε προσεκτικοί κατά το άνοιγμα νέων αρχείων, θα εξοικονομήσετε αρκετό χρόνο και κόπο, τον οποίο διαφορετικά θα σπαταλούσατε στον καθαρισμό εισβολών. Ακολουθούν μερικές χρήσιμες οδηγίες:

• Μην επισκέπτεστε ύποπτους ιστότοπους με πολλά αναδυόμενα παράθυρα και διαφημίσεις που αναβοσβήνουν.

• Να χρησιμοποιείτε μόνο ασφαλή προγράμματα και να επισκέπτεστε μόνο ασφαλείς ιστότοπους στο Internet. Να χρησιμοποιείτε μόνο ασφαλή προγράμματα και να επισκέπτεστε μόνο ασφαλείς ιστότοπους στο Internet.

• Να είστε προσεκτικοί κατά το άνοιγμα συνημμένων αρχείων σε email, ιδιαίτερα εκείνων που προέρχονται από μηνύματα μαζικής αλληλογραφίας και μηνύματα από άγνωστους αποστολείς.

• Μην χρησιμοποιείτε λογαριασμό διαχειριστή για την καθημερινή σας εργασία στον υπολογιστή σας.

Σελίδες βοήθειας

Καλώς ορίσατε στον οδηγό χρήσης του ESET Internet Security. Οι πληροφορίες που παρέχονται εδώ θα σας εξοικειώσουν με το προϊόν και θα σας βοηθήσουν να κάνετε τον υπολογιστή σας πιο ασφαλή.

Ξεκινώντας

Προτού χρησιμοποιήσετε το ESET Internet Security, συνιστάται να εξοικειωθείτε με τους διάφορους τύπους ανιχνεύσεων και τις απομακρυσμένες επιθέσεις που μπορεί να αντιμετωπίσετε όταν χρησιμοποιείτε τον υπολογιστή σας.

Επίσης, έχουμε συντάξει μια λίστα με τις νέες δυνατότητες που διαθέτει το ESET Internet Security, καθώς και έναν οδηγό που σας βοηθά να διαμορφώσετε τις βασικές ρυθμίσεις.

Πώς να χρησιμοποιήσετε τις σελίδες βοήθειας του ESET Internet Security

Τα θέματα βοήθειας χωρίζονται σε διάφορα κεφάλαια και υποκεφάλαια. Πατήστε **F1** για να δείτε πληροφορίες σχετικά με το παράθυρο στο οποίο βρίσκεστε αυτή τη στιγμή.

Το πρόγραμμα σάς επιτρέπει να κάνετε αναζήτηση για ένα θέμα βοήθειας με λέξη ή λέξεις κλειδιά ή αναζήτηση περιεχομένου πληκτρολογώντας λέξεις ή φράσεις. Η διαφορά μεταξύ αυτών των δύο μεθόδων είναι ότι η λέξη κλειδί μπορεί να σχετίζεται λογικά με σελίδες βοήθειας που δεν περιέχουν τη συγκεκριμένη λέξη κλειδί στο κείμενο. Η αναζήτηση με λέξεις και φράσεις θα αναζητήσει το περιεχόμενο σε όλες τις σελίδες και θα εμφανίσει μόνο εκείνες που περιέχουν τη λέξη ή τη φράση αναζήτησης σε πραγματικό κείμενο.

Για λόγους συνέπειας και για την αποφυγή σύγχυσης, η ορολογία που χρησιμοποιείται σε αυτό τον

οδηγό βασίζεται στα ονόματα παραμέτρων του ESET Internet Security. Επίσης, χρησιμοποιούμε ένα ομοιόμορφο σύνολο συμβόλων για την επισήμανση θεμάτων ιδιαίτερου ενδιαφέροντος ή σημασίας.

Η σημείωση είναι μια σύντομη παρατήρηση. Παρόλο που μπορείτε να τις παραβλέψετε, οι σημειώσεις μπορεί να προσφέρουν πολύτιμες πληροφορίες, όπως συγκεκριμένες δυνατότητες ή έναν σύνδεσμο για κάποιο σχετικό θέμα.

Αυτό απαιτεί την προσοχή σας και συνιστάται να μην το παρακάμψετε. Συνήθως παρέχει σημαντικές, αν και όχι κρίσιμες, πληροφορίες.

Αυτές οι πληροφορίες απαιτούν επιπλέον προσοχή. Οι προειδοποιήσεις εμφανίζονται κυρίως για να σας αποτρέψουν από λάθη που μπορεί να έχουν σοβαρές συνέπειες. Διαβάστε και κατανοήστε το κείμενο στις παρενθέσεις των προειδοποιήσεων, καθώς αναφέρει ιδιαίτερα κρίσιμες ρυθμίσεις συστήματος ή κάποιον ενδεχόμενο κίνδυνο.

Αυτή είναι μια περίπτωση χρήσης ή ένα πρακτικό παράδειγμα που έχει σκοπό να σας βοηθήσει να κατανοήσετε πώς μπορεί να χρησιμοποιηθεί μια συγκεκριμένη λειτουργία ή δυνατότητα.

Σύμβαση	Σημασία
Έντονη γραφή	Ονόματα στοιχείων διασύνδεσης, όπως πλαίσια και κουμπιά επιλογής.
Πλάγια γραφή	Σύμβολα κράτησης θέσης για πληροφορίες που παρέχετε. Για παράδειγμα, όνομα αρχείου ή διαδρομή σημαίνει ότι πληκτρολογείτε τη διαδρομή ή το όνομα ενός αρχείου.
`Courier New`	Δείγματα κώδικα ή εντολές.
Υπερσύνδεσμος	Παρέχει γρήγορη και εύκολη πρόσβαση σε άλλα θέματα ή σε εξωτερικές τοποθεσίες στο διαδίκτυο. Οι υπερσύνδεσμοι επισημαίνονται με μπλε χρώμα και μπορεί να έχουν υπογράμμιση.
%ProgramFiles%	Ο κατάλογος συστήματος των Windows στον οποίο αποθηκεύονται τα προγράμματα που έχουν εγκατασταθεί στα Windows.

Η **ηλεκτρονική βοήθεια** είναι η κύρια προέλευση περιεχομένου βοήθειας. Η πιο πρόσφατη έκδοση της ηλεκτρονικής βοήθειας εμφανίζεται αυτόματα όταν έχετε ενεργή σύνδεση στο Internet.

Εγκατάσταση

Υπάρχουν διάφορες μέθοδοι για την εγκατάσταση του ESET Internet Security στον υπολογιστή σας. Οι μέθοδοι εγκατάστασης διαφέρουν ανάλογα με τη χώρα και τα μέσα διανομής:

- Πρόγραμμα ζωντανής εγκατάστασης – Λαμβάνεται από ιστότοπο της ESET ή από CD/DVD. Το πακέτο εγκατάστασης είναι το ίδιο για όλες τις γλώσσες (επιλέξτε τη κατάλληλη γλώσσα). Το Πρόγραμμα ζωντανής εγκατάστασης είναι ένα μικρό αρχείο. Η λήψη των πρόσθετων αρχείων που απαιτούνται για την εγκατάσταση του ESET Internet Security θα πραγματοποιηθεί αυτόματα.

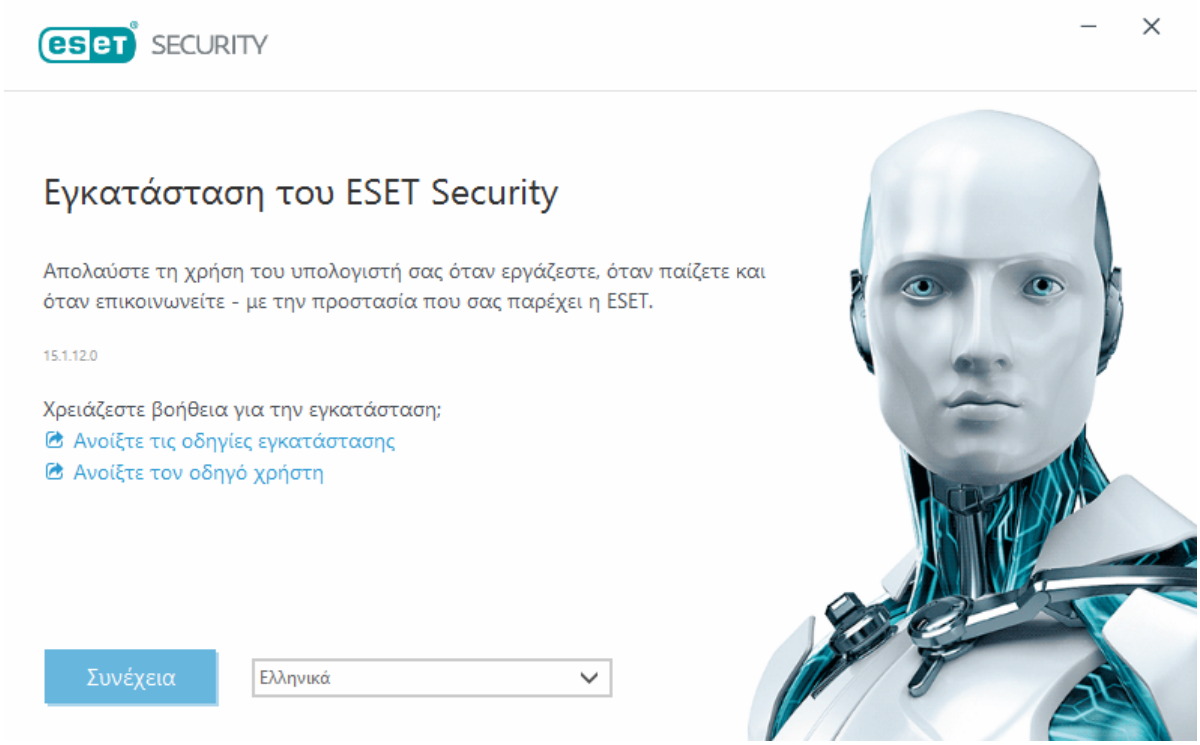
- Εγκατάσταση εκτός σύνδεσης – Χρησιμοποιεί ένα αρχείο .exe το οποίο είναι μεγαλύτερο από το Πρόγραμμα ζωντανής εγκατάστασης και δεν απαιτεί σύνδεση στο Internet ή πρόσθετα αρχεία για την ολοκλήρωση της εγκατάστασης.

Βεβαιωθείτε ότι δεν είναι εγκατεστημένα άλλα προγράμματα antivirus στον υπολογιστή σας, προτού εγκαταστήσετε το ESET Internet Security. Εάν υπάρχουν δύο ή περισσότερες λύσεις antivirus εγκατεστημένες σε έναν υπολογιστή, ενδέχεται να έρχονται σε διένεξη η μία με την άλλη. Συνιστούμε να καταργήσετε την εγκατάσταση κάθε άλλου προγράμματος antivirus από τον υπολογιστή σας. Ανατρέξτε στο άρθρο της Γνωσιακής βάσης της ESET για μια λίστα με εργαλεία κατάργησης απεγκατάστασης γνωστών προγραμμάτων antivirus (διαθέσιμη στα αγγλικά και σε διάφορες άλλες γλώσσες).

Πρόγραμμα ζωντανής εγκατάστασης

Μόλις ολοκληρώσετε τη λήψη για το Πακέτο εγκατάστασης προγράμματος ζωντανής εγκατάστασης, κάντε διπλό κλικ στο αρχείο εγκατάστασης και ακολουθήστε τις αναλυτικές οδηγίες στον Οδηγό του προγράμματος εγκατάστασης.

Για αυτόν τον τύπο εγκατάστασης, πρέπει να είστε συνδεδεμένοι στο Internet.



1. Επιλέξτε την κατάλληλη γλώσσα από το αναπτυσσόμενο μενού και κάντε κλικ στο στοιχείο **Συνέχεια**.

Εάν εγκαθιστάτε μια πιο πρόσφατη έκδοση επάνω από την προηγούμενη έκδοση με ρυθμίσεις που προστατεύονται με κωδικό πρόσβασης, πληκτρολογήστε τον κωδικό πρόσβασης. Μπορείτε να ρυθμίσετε τις παραμέτρους του κωδικού ρυθμίσεων στις Ρυθμίσεις πρόσβασης.

2. Επιλέξτε την προτίμησή σας για τις ακόλουθες δυνατότητες, διαβάστε τη Συμφωνία άδειας χρήσης τελικού χρήστη και την Πολιτική απορρήτου και κάντε κλικ στο στοιχείο **Συνέχεια** ή στο στοιχείο **Να επιτρέπονται όλες και συνέχεια** για να ενεργοποιήσετε όλες τις δυνατότητες:

- Σύστημα σχολίων ESET LiveGrid®
- Ενδεχομένως ανεπιθύμητες εφαρμογές

- Πρόγραμμα βελτίωσης εμπειρίας του πελάτη

Εάν κάνετε κλικ στο στοιχείο **Συνέχεια** ή **Να επιτρέπονται όλες και συνέχεια**, αποδέχεστε τη Συμφωνία άδειας χρήσης τελικού χρήστη και την Πολιτική απορρήτου.

3. Για να ενεργοποιήσετε, να διαχειριστείτε και να προβάλετε την ασφάλεια της συσκευής χρησιμοποιώντας την ESET HOME, συνδέστε τη συσκευή σας με το λογαριασμό ESET HOME. Κάντε κλικ στο στοιχείο **Παράλειψη σύνδεσης** για να συνεχίσετε χωρίς να συνδεθείτε στο ESET HOME. Μπορείτε να συνδέσετε τη συσκευή σας στον λογαριασμό σας στο ESET HOME αργότερα.

4. Εάν συνεχίσετε χωρίς να συνδεθείτε στο ESET HOME, ορίστε μια επιλογή ενεργοποίησης. Εάν εγκαθιστάτε μια πιο πρόσφατη έκδοση σε μια παλαιότερη, το κλειδί άδειας χρήσης σας θα εισαχθεί αυτόματα.

5. Ο Οδηγός εγκατάστασης καθορίζει ποιο προϊόν ESET έχει εγκατασταθεί με βάση την άδεια χρήσης σας. Η προεπιλεγμένη είναι πάντα η έκδοση με τις περισσότερες δυνατότητες ασφαλείας. Κάντε κλικ στο στοιχείο **Αλλαγή προϊόντος,** εάν θέλετε να εγκαταστήσετε μια διαφορετική έκδοση του προϊόντος ESET. Κάντε κλικ στο στοιχείο **Συνέχεια** για να ξεκινήσετε τη διεργασία εγκατάστασης. Αυτό μπορεί να διαρκέσει μερικά λεπτά.

Εάν υπάρχουν υπολείμματα (αρχεία ή φάκελοι) από προϊόντα ESET η εγκατάσταση των οποίων καταργήθηκε στο παρελθόν, θα σας ζητηθεί να επιτρέψετε την κατάργησή τους. Κάντε κλικ στο στοιχείο **Εγκατάσταση** για να συνεχίσετε.

6. Κάντε κλικ στο στοιχείο **Τέλος** για έξοδο από τον Οδηγό εγκατάστασης.

Πρόγραμμα αντιμετώπισης προβλημάτων εγκατάστασης.

Μετά την εγκατάσταση και ενεργοποίηση του προϊόντος, αρχίζει η λήψη των μονάδων. Η προστασία προετοιμάζεται και ορισμένες δυνατότητες μπορεί να μην είναι πλήρως λειτουργικές εάν δεν ολοκληρωθεί η λήψη.

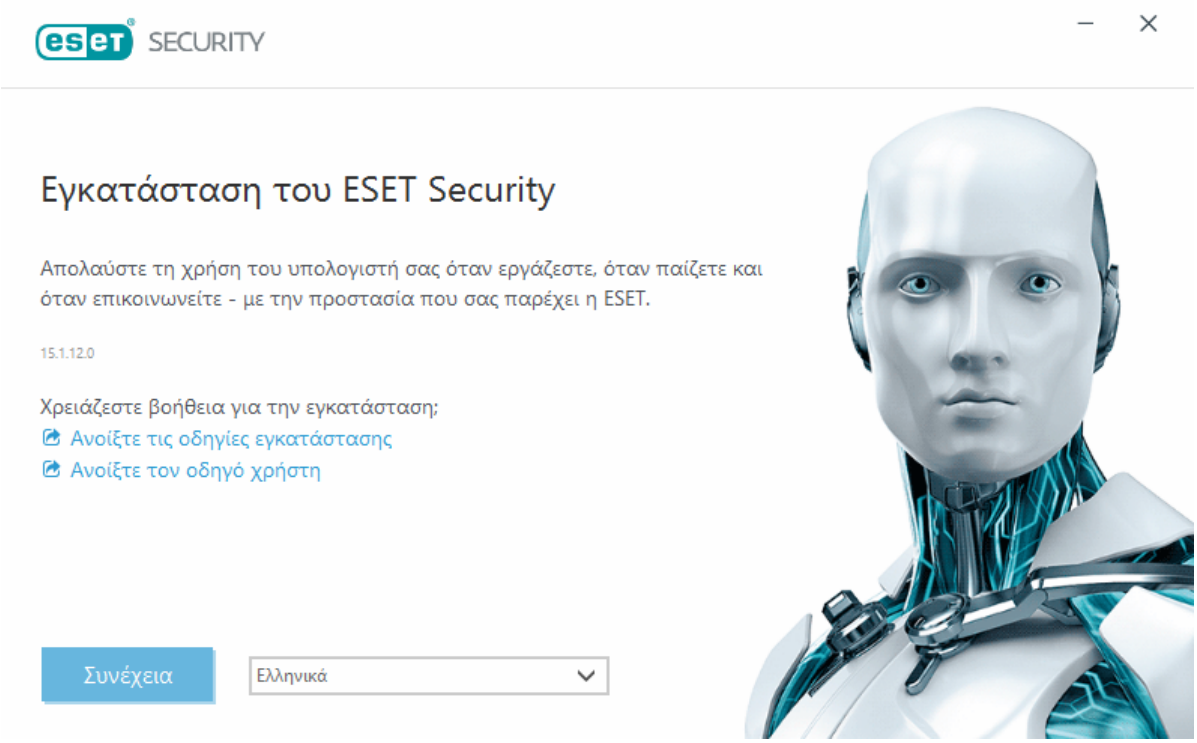
Εγκατάσταση εκτός σύνδεσης

Πραγματοποιήστε λήψη και εγκατάσταση του οικιακού προϊόντος ESET για Windows χρησιμοποιώντας το παρακάτω πρόγραμμα εγκατάστασης εκτός σύνδεσης (.exe). Επιλέξτε την έκδοση του οικιακού προϊόντος ESET που θα λάβετε (32 bit, 64 bit ή ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Λήψη 64 bit Λήψη 32 bit Λήψη ARM	Λήψη 64 bit Λήψη 32 bit Λήψη ARM	Λήψη 64 bit Λήψη 32 bit Λήψη ARM

Εάν έχετε ενεργή σύνδεση στο Internet, εγκαταστήστε το προϊόν ESET χρησιμοποιώντας ένα Πρόγραμμα ζωντανής εγκατάστασης.

Μόλις εκκινήσετε το πρόγραμμα εγκατάστασης εκτός σύνδεσης (.exe), ο Οδηγός εγκατάστασης θα σας καθοδηγήσει στη διεργασία ρύθμισης.



1. Επιλέξτε την κατάλληλη γλώσσα από το αναπτυσσόμενο μενού και κάντε κλικ στο στοιχείο **Συνέχεια**.

Εάν εγκαθιστάτε μια πιο πρόσφατη έκδοση επάνω από την προηγούμενη έκδοση με ρυθμίσεις που προστατεύονται με κωδικό πρόσβασης, πληκτρολογήστε τον κωδικό πρόσβασης. Μπορείτε να ρυθμίσετε τις παραμέτρους του κωδικού ρυθμίσεων στις Ρυθμίσεις πρόσβασης.

2. Επιλέξτε την προτίμησή σας για τις ακόλουθες δυνατότητες, διαβάστε τη Συμφωνία άδειας χρήσης τελικού χρήστη και την Πολιτική απορρήτου και κάντε κλικ στο στοιχείο **Συνέχεια** ή στο στοιχείο **Να επιτρέπονται όλες και συνέχεια** για να ενεργοποιήσετε όλες τις δυνατότητες:

- Σύστημα σχολίων ESET LiveGrid®
- Ενδεχομένως ανεπιθύμητες εφαρμογές
- Πρόγραμμα βελτίωσης εμπειρίας του πελάτη

Εάν κάνετε κλικ στο στοιχείο **Συνέχεια** ή **Να επιτρέπονται όλες και συνέχεια**, αποδέχεστε τη Συμφωνία άδειας χρήσης τελικού χρήστη και την Πολιτική απορρήτου.

3. Κάντε κλικ στο στοιχείο **Παράλειψη σύνδεσης**. Όταν συνδεθείτε στο Internet, μπορείτε να συνδέσετε τη συσκευή σας με το λογαριασμό στο ESET HOME.

4. Κάντε κλικ στο στοιχείο **Παράλειψη ενεργοποίησης**. Το ESET Internet Security πρέπει να ενεργοποιηθεί μετά την εγκατάσταση για να είναι πλήρως λειτουργικό. Η ενεργοποίηση προϊόντος απαιτεί ενεργή σύνδεση στο Internet.

5. Ο Οδηγός εγκατάστασης εμφανίζει το προϊόν ESET που θα εγκατασταθεί με βάση το πρόγραμμα εγκατάστασης χωρίς σύνδεση που έχετε λάβει. Κάντε κλικ στο στοιχείο **Συνέχεια** για να ξεκινήσετε τη διεργασία εγκατάστασης. Αυτό μπορεί να διαρκέσει μερικά λεπτά.

Εάν υπάρχουν υπολείμματα (αρχεία ή φάκελοι) από προϊόντα ESET η εγκατάσταση των οποίων καταργήθηκε στο παρελθόν, θα σας ζητηθεί να επιτρέψετε την κατάργησή τους. Κάντε κλικ στο στοιχείο **Εγκατάσταση** για να συνεχίσετε.

6. Κάντε κλικ στο στοιχείο **Τέλος** για έξοδο από τον Οδηγό εγκατάστασης.

Πρόγραμμα αντιμετώπισης προβλημάτων εγκατάστασης.

Ενεργοποίηση προϊόντος

Υπάρχουν διάφορες διαθέσιμες μέθοδοι για να ενεργοποιήσετε το προϊόν σας. Η διαθεσιμότητα ενός συγκεκριμένου σεναρίου ενεργοποίησης στο παράθυρο ενεργοποίησης ενδέχεται να ποικίλλει ανάλογα με τη χώρα και με τα μέσα διανομής (CD/DVD, ιστότοπος της ESET κ.λπ.):

• Εάν αγοράσατε το προϊόν σε συσκευασία πώλησης ή λάβατε ένα email με στοιχεία άδειας χρήσης, ενεργοποιήστε το προϊόν σας κάνοντας κλικ στο στοιχείο **Χρησιμοποιήστε ένα Κλειδί άδειας χρήσης που έχετε αγοράσει**. Το Κλειδί άδειας χρήσης βρίσκεται συνήθως μέσα ή στο πίσω μέρος της συσκευασίας του προϊόντος. Για να είναι επιτυχής η ενεργοποίηση, πρέπει να εισαγάγετε το Κλειδί άδειας χρήσης όπως σας παραδίδεται. Κλειδί άδειας χρήσης – Μια μοναδική συμβολοσειρά της μορφής XXXX-XXXX-XXXX-XXXX-XXXX ή XXXX-XXXXXXXX, η οποία χρησιμοποιείται για την ταυτοποίηση του κατόχου της άδειας χρήσης και για την ενεργοποίηση της άδειας χρήσης.

• Αφού επιλέξετε Χρήση του λογαριασμού ESET HOME, θα σας ζητηθεί να συνδεθείτε στον λογαριασμό σας στο ESET HOME.

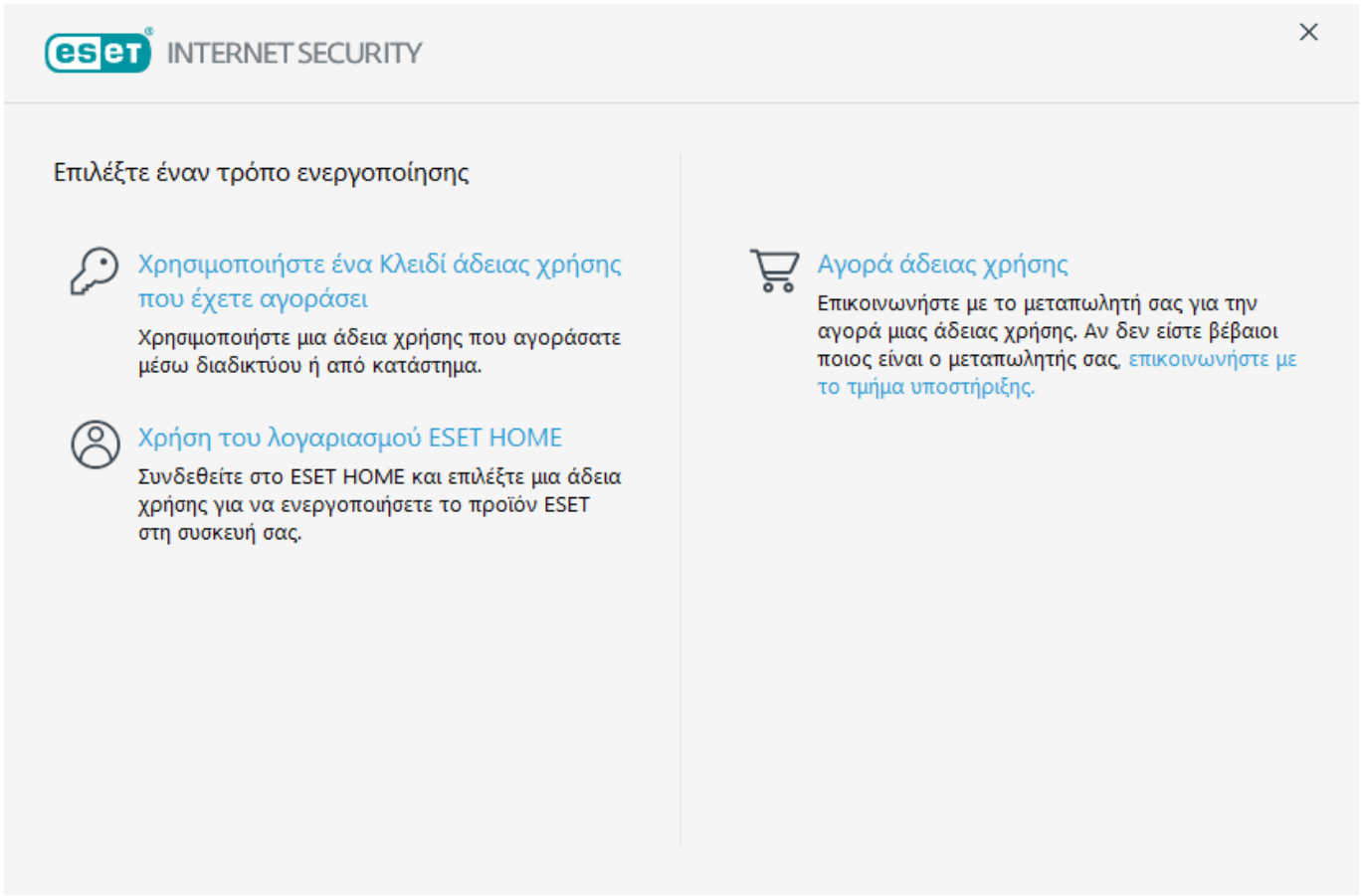
• Εάν θέλετε να αξιολογήσετε το ESET Internet Security προτού το αγοράσετε, επιλέξτε Δωρεάν δοκιμαστική έκδοση. Συμπληρώστε τη διεύθυνση email και τη χώρα σας για να ενεργοποιήσετε το ESET Internet Security για περιορισμένο χρόνο. Η δοκιμαστική άδεια χρήσης θα σας αποσταλεί μέσω email. Οι δοκιμαστικές άδειες χρήσης μπορούν να ενεργοποιηθούν μόνο μία φορά για κάθε πελάτη.

• Εάν δεν έχετε άδεια χρήσης και θέλετε να αγοράσετε μία, κάντε κλικ στην επιλογή "**Αγορά άδειας χρήσης**". Θα ανακατευθυνθείτε στον ιστότοπο του τοπικού διανομέα της ESET. Οι πλήρεις άδειες χρήσης των οικιακών προϊόντων της ESET για Windows δεν είναι δωρεάν.

Μπορείτε να αλλάξετε την άδεια χρήσης του προϊόντος οποιαδήποτε στιγμή. Για να το κάνετε αυτό, κάντε κλικ στα στοιχεία **Βοήθεια και υποστήριξη** > **Αλλαγή άδειας χρήσης** στο κύριο παράθυρο του προγράμματος. Θα δείτε ένα δημόσιο αναγνωριστικό άδειας χρήσης που χρησιμοποιείται για την ταυτοποίηση της άδειας χρήσης σας στην Υποστήριξη της ESET.

Εάν έχετε ένα όνομα χρήστη και κωδικό πρόσβασης για την ενεργοποίηση παλιότερων προϊόντων της ESET και δεν γνωρίζετε πώς να ενεργοποιήσετε το ESET Internet Security, μπορείτε να μετατρέψετε τα παλιά διαπιστευτήριά σας σε Κλειδί άδειας χρήσης.

Απέτυχε η ενεργοποίηση προϊόντος;



Εισαγωγή του κλειδιού άδειας χρήσης κατά την ενεργοποίηση

Οι αυτόματες ενημερώσεις είναι σημαντικές για την ασφάλειά σας. Το ESET Internet Security θα λαμβάνει ενημερώσεις μόνο αφού ενεργοποιηθεί.

Όταν εισάγετε το **Κλειδί άδειας χρήσης**, είναι σημαντικό να το πληκτολογείτε ακριβώς όπως είναι:

- Το κλειδί άδειας χρήσης σας είναι μια μοναδική συμβολοσειρά της μορφής XXXX-XXXX-XXXX-XXXX-XXXX, η οποία χρησιμοποιείται για την ταυτοποίηση του κατόχου της άδειας χρήσης και την ενεργοποίηση της άδειας χρήσης.

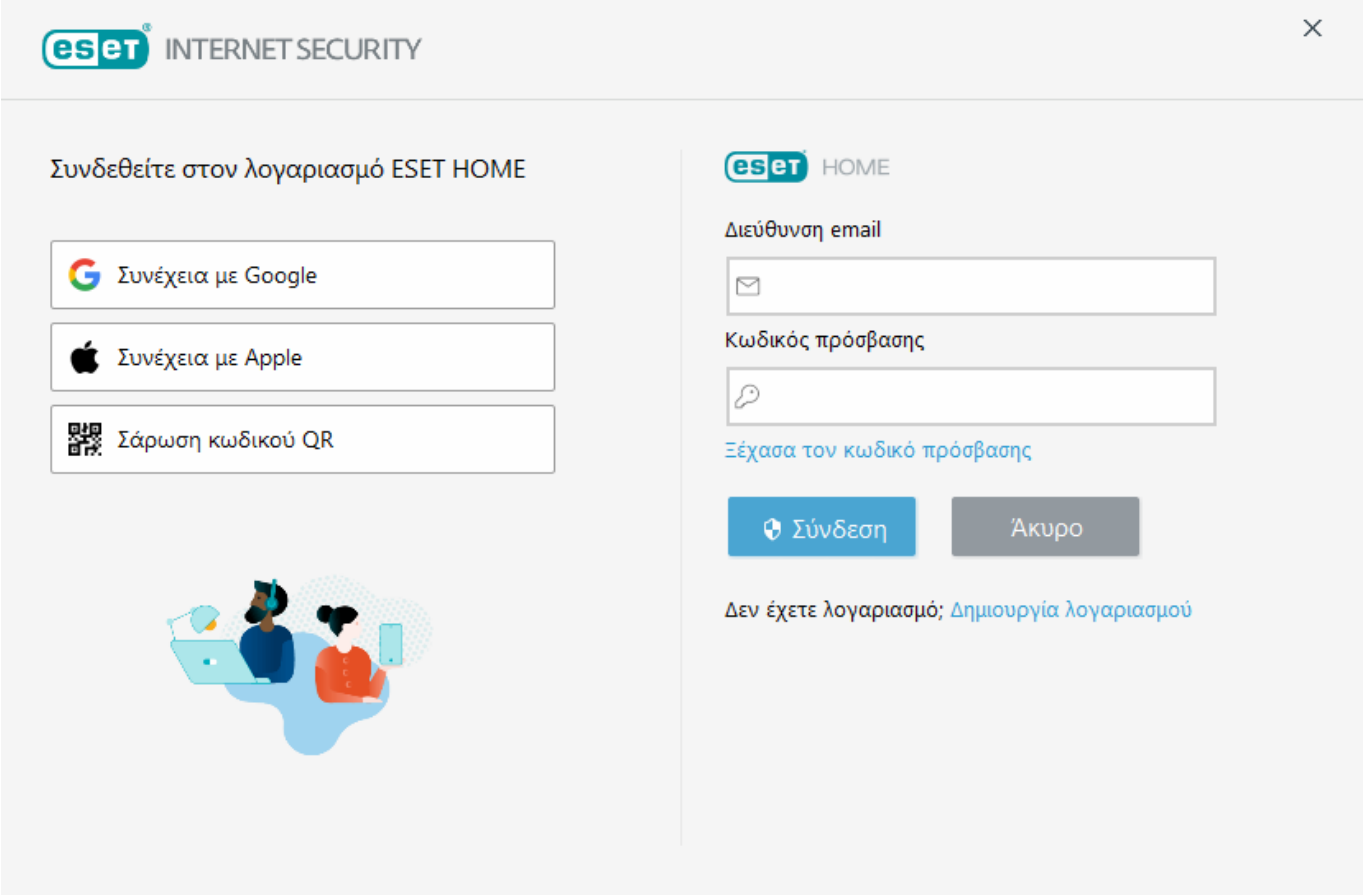
Για να διασφαλίσετε την ακρίβεια, συνιστούμε να αντιγράψετε και να επικολλήσετε το κλειδί άδειας χρήσης από το μήνυμα εγγραφής σας.

Εάν δεν καταχωρίσατε το κλειδί άδειας χρήσης μετά την εγκατάσταση, το προϊόν δεν θα ενεργοποιηθεί. Μπορείτε να ενεργοποιήσετε το ESET Internet Security στο κύριο παράθυρο του προγράμματος > **Βοήθεια και υποστήριξη** > **Ενεργοποίηση άδειας χρήσης**.

Οι πλήρεις άδειες χρήσης των οικιακών προϊόντων της ESET για Windows δεν είναι δωρεάν.

Χρήση του λογαριασμού ESET HOME

Συνδέστε τη συσκευή σας με την ESET HOME για να προβάλλετε και να διαχειρίζεστε όλες τις ενεργοποιημένες άδειες χρήσης της ESET και τις συσκευές σας. Μπορείτε να ανανεώσετε, να αναβαθμίσετε ή να επεκτείνετε την άδεια χρήσης σας και να δείτε σημαντικές λεπτομέρειες της άδειας χρήσης. Στην πύλη διαχείρισης ESET HOME ή στην εφαρμογή για κινητές συσκευές, μπορείτε να επεξεργαστείτε τις ρυθμίσεις του Anti-Theft, προσθέσετε διάφορες άδειες χρήσης, να πραγματοποιήσετε λήψη προϊόντων στις συσκευές σας, να ελέγξετε την κατάσταση ασφάλειας του προϊόντος ή να κάνετε κοινή χρήση αδειών χρήσης μέσω email. Για περισσότερες πληροφορίες, επισκεφθείτε τις σελίδες ηλεκτρονικής βοήθειας του ESET HOME.



Αφού επιλέξετε **Χρήση λογαριασμού ESET HOME** ως μεθόδου ενεργοποίησης ή κατά τη σύνδεση με το λογαριασμό ESET HOME κατά την εγκατάσταση:

1. Σύνδεση στον λογαριασμό σας στο ESET HOME.

> Εάν δεν έχετε λογαριασμό στο ESET HOME, κάντε κλικ στο στοιχείο **Δημιουργία λογαριασμού** για να εγγραφείτε ή δείτε τις οδηγίες στην Ηλεκτρονική βοήθεια του ESET HOME.
> Εάν ξεχάσατε τον κωδικό πρόσβασής σας, κάντε κλικ στο στοιχείο **Ξέχασα τον κωδικό πρόσβασης** και ακολουθήστε τα βήματα στην οθόνη ή δείτε τις οδηγίες στην Ηλεκτρονική βοήθεια του ESET HOME.

2. Ρυθμίστε ένα **Όνομα συσκευής** για τη συσκευή σας, το οποίο θα χρησιμοποιείται σε όλες τις υπηρεσίες ESET HOME και κάντε κλικ στο στοιχείο **Συνέχεια**.

3. Επιλέξτε μια άδεια χρήσης για ενεργοποίηση ή προσθέστε μια νέα άδεια χρήσης. Κάντε κλικ στο στοιχείο **Συνέχεια** για να ενεργοποιήσετε το ESET Internet Security.

Ενεργοποίηση δοκιμαστικής άδειας χρήσης

Για να ενεργοποιήσετε τη δοκιμαστική έκδοση του ESET Internet Security, εισαγάγετε μια έγκυρη διεύθυνση email στα πεδία **Διεύθυνση email** και **Επιβεβαίωση διεύθυνσης email**. Μετά την ενεργοποίηση, θα δημιουργηθεί και θα σταλεί στο email σας η άδεια χρήσης ESET. Αυτή η διεύθυνση email θα χρησιμοποιείται επίσης για τις ειδοποιήσεις λήξης του προϊόντος και τις άλλες επικοινωνίες σας με την ESET. Η δοκιμαστική έκδοση μπορεί να ενεργοποιηθεί μόνο μία φορά.

Επιλέξτε τη χώρα σας από το αναπτυσσόμενο μενού **Χώρα** για να δηλώσετε το ESET Internet Security στον τοπικό σας διανομέα, ο οποίος θα σας παρέχει τεχνική υποστήριξη.

Δωρεάν κλειδί άδειας χρήσης της ESET

Η πλήρης άδεια χρήσης του ESET Internet Security δεν είναι δωρεάν.

Το Κλειδί άδειας χρήσης της ESET είναι μια μοναδική ακολουθία γραμμάτων και αριθμών που διαχωρίζονται με μια παύλα, το οποίο παρέχεται από την ESET για να επιτρέπεται η νόμιμη χρήση του ESET Internet Security σε συμμόρφωση με τη Συμφωνία Άδειας Χρήσης Τελικού Χρήστη. Κάθε τελικός χρήστης δικαιούται να χρησιμοποιεί το κλειδί άδειας χρήσης μόνο στο βαθμό που έχει το δικαίωμα να χρησιμοποιεί το ESET Internet Security με βάση τον αριθμό αδειών χρήσης που έχουν εκχωρηθεί από την ESET. Το Κλειδί άδειας χρήσης θεωρείται εμπιστευτικό και δεν πρέπει να κοινοποιείται. Ωστόσο, ο χρήστης μπορεί να κάνει κοινή χρήση των θέσεων της άδειας χρήσης μέσω της ESET HOME.

Υπάρχουν πηγές στο Internet οι οποίες ενδέχεται να σας παράσχουν «δωρεάν» κλειδιά άδειας χρήσης της ESET, αλλά να θυμάστε:

• Εάν κάνετε κλικ σε μια διαφήμιση «Δωρεάν άδεια χρήσης της ESET», ενδέχεται να τεθεί σε κίνδυνο ο υπολογιστής ή η συσκευή σας και αυτό μπορεί να οδηγήσει σε μόλυνση από κακόβουλο λογισμικό. Το κακόβουλο λογισμικό μπορεί να κρύβεται σε ανεπίσημο περιεχόμενο του διαδικτύου (π.χ. βίντεο), σε ιστότοπους που εμφανίζουν διαφημίσεις για να κερδίσουν χρήματα με βάση τις επισκέψεις σας κ.λπ. Συνήθως, πρόκειται για παγίδα.

• Η ESET μπορεί και απενεργοποιεί τις πειρατικές άδειες χρήσης.

• Η κατοχή ενός κλειδιού πειρατικής άδειας χρήσης δεν ευθυγραμμίζεται με τη Συμφωνία Άδειας Χρήσης Τελικού Χρήστη την οποία πρέπει να αποδεχτείτε για να εγκαταστήσετε το ESET Internet Security.

• Αγοράζετε τις άδειες χρήσης της ESET μόνο μέσω επίσημων καναλιών, όπως το www.eset.com, τους διανομείς ή μεταπωλητές της ESET (μην αγοράζετε άδειες χρήσης από ανεπίσημους ιστότοπους τρίτων όπως το eBay ή κοινόχρηστες άδειες χρήσης από τρίτους).

• Η λήψη ενός οικιακού ESET Internet Security είναι δωρεάν, αλλά η ενεργοποίηση κατά την εγκατάσταση απαιτεί ένα έγκυρο κλειδί άδειας χρήσης της ESET (μπορείτε να το λάβετε και να το εγκαταστήσετε, αλλά χωρίς ενεργοποίηση δεν θα λειτουργεί)

• Μη κοινοποιείτε την άδεια χρήσης σας στο Internet ή στα μέσα κοινωνικής δικτύωσης (ενδέχεται να διαδοθεί ευρέως).

Για να ταυτοποιήσετε και να αναφέρετε μια πειρατική άδεια χρήσης της ESET, επισκεφτείτε το άρθρο

της Γνωσιακής βάσης για οδηγίες.

Εάν δεν είστε βέβαιοι ότι θέλετε να αγοράσετε ένα προϊόν ασφάλειας ESET, μπορείτε να χρησιμοποιήσετε μια δοκιμαστική έκδοση μέχρι να αποφασίσετε:

1. Ενεργοποίηση του ESET Internet Security χρησιμοποιώντας μια δωρεάν δοκιμαστική άδεια χρήσης
2. Συμμετοχή στο Πρόγραμμα Beta της ESET
3. Εγκαταστήστε το ESET Mobile Security εάν χρησιμοποιείτε κινητή συσκευή Android, είναι freemium (δωρεάν με την αγορά προϊόντος).

Για να εξασφαλίσετε έκπτωση / παρατείνετε την άδεια χρήσης σας:

- Παραπέμψτε το ESET Internet Security σε έναν φίλο ή μια φίλη σας
- Ανανεώστε το ESET (εάν είχατε ενεργή άδεια χρήσης προηγουμένως) ή ενεργοποιήστε το για μεγαλύτερο χρονικό διάστημα

Η ενεργοποίηση απέτυχε - συνήθη σενάρια

Εάν η ενεργοποίηση του ESET Internet Security δεν είναι επιτυχής, τα πιο συνηθισμένα σενάρια είναι:

- Το κλειδί άδειας χρήσης χρησιμοποιείται ήδη
- Μη έγκυρο κλειδί άδειας χρήσης. Σφάλμα φόρμας ενεργοποίησης προϊόντος
- Πρόσθετες πληροφορίες απαραίτητες για την ενεργοποίηση λείπουν ή δεν είναι έγκυρες.
- Η επικοινωνία με τη βάση δεδομένων ενεργοποίησης απέτυχε. Δοκιμάστε να επαναλάβετε την ενεργοποίηση σε 15 λεπτά.
- Καμία σύνδεση ή απενεργοποιημένη σύνδεση με τους διακομιστές ενεργοποίησης της ESET

Βεβαιωθείτε ότι πληκτρολογήσατε το σωστό κλειδί άδειας χρήσης και προσπαθήστε να το ενεργοποιήσετε ξανά. Εάν χρησιμοποιείτε λογαριασμό ESET HOME για την ενεργοποίηση, ανατρέξτε στο θέμα Διαχείριση αδειών χρήσης ESET HOME - Ηλεκτρονική Βοήθεια.

Εάν η ενεργοποίηση εξακολουθεί να μην είναι δυνατή, το Πρόγραμμα αντιμετώπισης προβλημάτων ενεργοποίησης της ESET σάς καθοδηγεί σε συνήθεις ερωτήσεις, σφάλματα και προβλήματα σχετικά με την ενεργοποίηση και την αδειοδότηση (διαθέσιμο στα Αγγλικά και σε πολλές άλλες γλώσσες).

Η ενεργοποίηση απέτυχε λόγω υπέρβασης ορίου της άδειας χρήσης

Ζήτημα

- Μπορεί να έχει γίνει υπέρβαση ορίου ή κατάχρηση της άδειας χρήσης σας
- Η ενεργοποίηση απέτυχε λόγω υπέρβασης ορίου της άδειας χρήσης

Λύση

Υπάρχουν περισσότερες συσκευές που χρησιμοποιούν αυτή την άδεια χρήσης από αυτές που επιτρέπει η άδεια. Μπορεί να έχετε πέσει θύμα πειρατείας λογισμικού ή πλαστού λογισμικού. Η άδεια δεν μπορεί να χρησιμοποιηθεί για να ενεργοποιήσετε οποιοδήποτε άλλο προϊόν ESET. Μπορείτε να λύσετε αυτό το πρόβλημα άμεσα εάν επιτρέπεται να διαχειριστείτε την άδεια χρήσης στο λογαριασμό ESET HOME ή να αγοράσετε την άδεια χρήσης από μια νόμιμη πηγή. Αν δεν έχετε ακόμα λογαριασμό, δημιουργήστε έναν.

Εάν είστε κάτοχος άδειας χρήσης και δεν σας έχει ζητηθεί να εισαγάγετε τη διεύθυνση email σας:

1. Για να διαχειριστείτε την άδεια χρήσης ESET, ανοίξτε ένα πρόγραμμα περιήγησης και πλοηγηθείτε στη διεύθυνση https://home.eset.com. Αποκτήστε πρόσβαση στο ESET License Manager και καταργήστε ή απενεργοποιήστε θέσεις. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Τι να κάνετε σε περίπτωση υπέρβασης ορίου της άδειας χρήσης.

2. Για να ταυτοποιήσετε και να αναφέρετε μια πειρατική άδεια χρήσης της ESET, επισκεφτείτε το άρθρο «Ταυτοποίηση και αναφορά πειρατικών αδειών χρήσης ESET» για οδηγίες.

3. Εάν δεν είστε βέβαιοι, κάντε κλικ στο κουμπί «**Πίσω**» και στείλτε email στην Τεχνική υποστήριξη της ESET.

Εάν δεν είστε ο κάτοχος της άδειας χρήσης, επικοινωνήστε με τον κάτοχο αυτής της άδειας χρήσης για να τον ενημερώσετε ότι δεν μπορείτε να ενεργοποιήσετε το προϊόν ESET λόγω υπέρβασης ορίου της άδειας χρήσης. Ο κάτοχος μπορεί να λύσει το πρόβλημα στην πύλη ESET HOME.

Εάν σας ζητηθεί να επιβεβαιώσετε τη διεύθυνση email σας (μόνο σε ορισμένες περιπτώσεις), εισαγάγετε τη διεύθυνση email που χρησιμοποιήσατε αρχικά για να αγοράσετε ή να ενεργοποιήσετε το ESET Internet Security.

Αναβάθμιση άδειας χρήσης

Αυτό το παράθυρο ειδοποίησης εμφανίζεται εάν έχει αλλάξει η άδεια χρήσης που χρησιμοποιήθηκε για την ενεργοποίηση του προϊόντος ESET. Η τροποποιημένη άδεια χρήσης σάς επιτρέπει να ενεργοποιήσετε ένα προϊόν με περισσότερες δυνατότητες ασφάλειας. Εάν δεν έχει πραγματοποιηθεί καμία αλλαγή, το ESET Internet Security θα εμφανίσει ένα παράθυρο συναγερμού μία φορά, με τίτλο **Αλλαγή σε προϊόν με περισσότερες δυνατότητες**.

Ναι (συνιστάται) – θα εγκατασταθεί αυτόματα το προϊόν με περισσότερες δυνατότητες ασφαλείας.

Όχι, ευχαριστώ - δεν θα πραγματοποιηθούν αλλαγές και η ειδοποίηση θα εξαφανιστεί οριστικά.

Για να αλλάξετε το προϊόν αργότερα, ανατρέξτε στο άρθρο της Γνωσιακής βάσης της ESET. Για περισσότερες πληροφορίες σχετικά με τις άδειες χρήσης ESET, ανατρέξτε στο θέμα Συχνές ερωτήσεις για τις άδειες χρήσης.

Στον παρακάτω πίνακα περιγράφονται λεπτομερώς οι δυνατότητες που είναι διαθέσιμες σε κάθε συγκεκριμένο προϊόν.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Μηχανισμός ανίχνευσης:	✔	✔	✔
Προηγμένη εκμάθηση υπολογιστή	✔	✔	✔
Λειτουργία αποτροπής κενών ασφαλείας	✔	✔	✔
Προστασία από επιθέσεις βασισμένες σε δέσμες ενεργειών	✔	✔	✔
Anti-Phishing	✔	✔	✔
Προστασία πρόσβασης στο διαδίκτυο	✔	✔	✔
HIPS (συμπεριλαμβάνει Προστασία Ransomware)	✔	✔	✔
Antispam		✔	✔
Τείχος προστασίας		✔	✔
Ελεγκτής δικτύου		✔	✔
Προστασία κάμερας		✔	✔
Προστασία από επιθέσεις δικτύου		✔	✔
Προστασία botnet		✔	✔
Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών		✔	✔
Γονικός έλεγχος		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Αναβάθμιση προϊόντος

Έχετε πραγματοποιήσει λήψη ενός προεπιλεγμένου προγράμματος εγκατάστασης και αποφασίσατε να αλλάξετε το προϊόν που θα ενεργοποιηθεί ή θέλετε να αλλάξετε το εγκατεστημένο προϊόν σας σε ένα με περισσότερες δυνατότητες ασφαλείας.

Αλλαγή προϊόντος κατά την εγκατάσταση.

Στον παρακάτω πίνακα περιγράφονται λεπτομερώς οι δυνατότητες που είναι διαθέσιμες σε κάθε συγκεκριμένο προϊόν.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Μηχανισμός ανίχνευσης:	✔	✔	✔
Προηγμένη εκμάθηση υπολογιστή	✔	✔	✔
Λειτουργία αποτροπής κενών ασφαλείας	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Προστασία από επιθέσεις βασισμένες σε δέσμες ενεργειών	✔	✔	✔
Anti-Phishing	✔	✔	✔
Προστασία πρόσβασης στο διαδίκτυο	✔	✔	✔
HIPS (συμπεριλαμβάνει Προστασία Ransomware)	✔	✔	✔
Antispam		✔	✔
Τείχος προστασίας		✔	✔
Ελεγκτής δικτύου		✔	✔
Προστασία κάμερας		✔	✔
Προστασία από επιθέσεις δικτύου		✔	✔
Προστασία botnet		✔	✔
Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών		✔	✔
Γονικός έλεγχος		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Υποβάθμιση άδειας χρήσης

Αυτό το παράθυρο διαλόγου εμφανίζεται εάν έχει αλλάξει η άδεια χρήσης που χρησιμοποιήθηκε για την ενεργοποίηση του προϊόντος ESET. Η τροποποιημένη άδεια χρήσης μπορεί να χρησιμοποιηθεί μόνο με διαφορετικό προϊόν ESET με λιγότερες δυνατότητες ασφάλειας. Το προϊόν αλλάζει αυτόματα για να αποφευχθεί η απώλεια προστασίας.

Για περισσότερες πληροφορίες σχετικά με τις άδειες χρήσης ESET, ανατρέξτε στο θέμα Συχνές ερωτήσεις για τις άδειες χρήσης.

Στον παρακάτω πίνακα περιγράφονται λεπτομερώς οι δυνατότητες που είναι διαθέσιμες σε κάθε συγκεκριμένο προϊόν.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Μηχανισμός ανίχνευσης:	✔	✔	✔
Προηγμένη εκμάθηση υπολογιστή	✔	✔	✔
Λειτουργία αποτροπής κενών ασφαλείας	✔	✔	✔
Προστασία από επιθέσεις βασισμένες σε δέσμες ενεργειών	✔	✔	✔
Anti-Phishing	✔	✔	✔
Προστασία πρόσβασης στο διαδίκτυο	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
HIPS (συμπεριλαμβάνει Προστασία Ransomware)	✔	✔	✔
Antispam		✔	✔
Τείχος προστασίας		✔	✔
Ελεγκτής δικτύου		✔	✔
Προστασία κάμερας		✔	✔
Προστασία από επιθέσεις δικτύου		✔	✔
Προστασία botnet		✔	✔
Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών		✔	✔
Γονικός έλεγχος		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Υποβάθμιση προϊόντος

Το προϊόν που είναι εγκατεστημένο αυτή τη στιγμή έχει περισσότερες δυνατότητες ασφαλείας από αυτό που πρόκειται να ενεργοποιήσετε. Θα χάσετε την αντικλεπτική προστασία και την πρόσβαση σε σχετικά δεδομένα που είναι αποθηκευμένα στο ESET HOME.

Στον παρακάτω πίνακα περιγράφονται λεπτομερώς οι δυνατότητες που είναι διαθέσιμες σε κάθε συγκεκριμένο προϊόν.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Μηχανισμός ανίχνευσης:	✔	✔	✔
Προηγμένη εκμάθηση υπολογιστή	✔	✔	✔
Λειτουργία αποτροπής κενών ασφαλείας	✔	✔	✔
Προστασία από επιθέσεις βασισμένες σε δέσμες ενεργειών	✔	✔	✔
Anti-Phishing	✔	✔	✔
Προστασία πρόσβασης στο διαδίκτυο	✔	✔	✔
HIPS (συμπεριλαμβάνει Προστασία Ransomware)	✔	✔	✔
Antispam		✔	✔
Τείχος προστασίας		✔	✔
Ελεγκτής δικτύου		✔	✔
Προστασία κάμερας		✔	✔
Προστασία από επιθέσεις δικτύου		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Προστασία botnet		✔	✔
Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών		✔	✔
Γονικός έλεγχος		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Πρόγραμμα αντιμετώπισης προβλημάτων εγκατάστασης

Εάν προκύψουν προβλήματα κατά την εγκατάσταση, ο Οδηγός εγκατάστασης παρέχει ένα πρόγραμμα αντιμετώπισης προβλημάτων που επιλύει το ζήτημα, εάν είναι εφικτό.

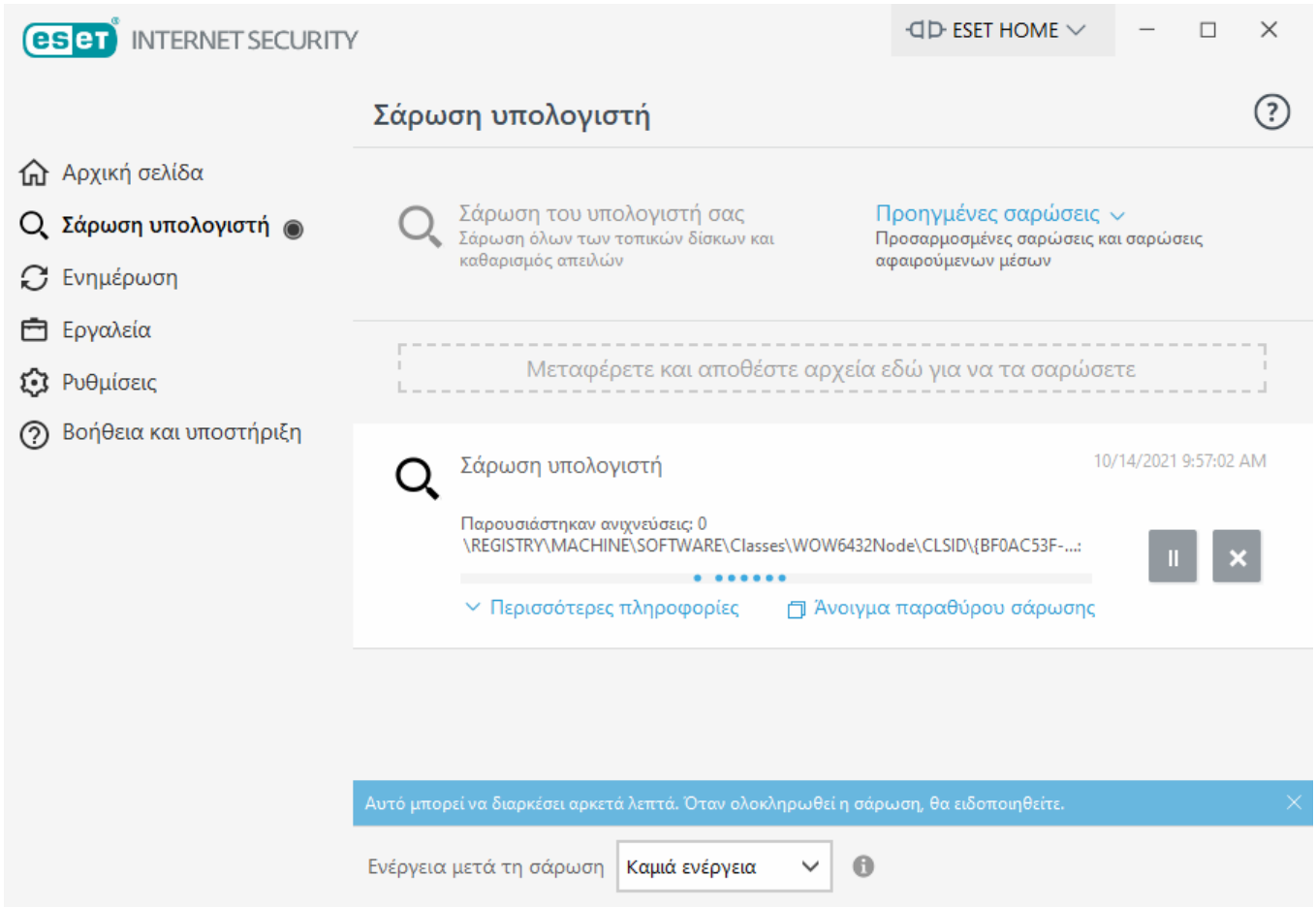
Κάντε κλικ στο στοιχείο **Εκτέλεση προγράμματος αντιμετώπισης προβλημάτων** για να εκκινήσει το πρόγραμμα αντιμετώπισης προβλημάτων. Όταν ολοκληρωθεί το πρόγραμμα αντιμετώπισης προβλημάτων, ακολουθήστε τη συνιστώμενη λύση.

Εάν το πρόβλημα παραμένει, ανατρέξτε στην λίστα που περιέχει συνηθισμένα σφάλματα εγκατάστασης και λύσεις.

Πρώτη σάρωση μετά την εγκατάσταση

Μετά την εγκατάσταση του ESET Internet Security, θα ξεκινήσει αυτόματη σάρωση του υπολογιστή μετά την πρώτη επιτυχή ενημέρωση του υπολογιστή, προκειμένου να γίνει έλεγχος για κακόβουλο κώδικα.

Μπορείτε επίσης να ξεκινήσετε σάρωση του υπολογιστή μη αυτόματα από το κύριο παράθυρο του προγράμματος, επιλέγοντας **Σάρωση υπολογιστή** > **Σάρωση του υπολογιστή σας**. Για περισσότερες λεπτομέρειες σχετικά με τη σάρωση υπολογιστή, ανατρέξτε στην ενότητα Σάρωση υπολογιστή.



Αναβάθμιση σε πιο πρόσφατη έκδοση

Εκδίδονται νέες εκδόσεις του ESET Internet Security για την υλοποίηση βελτιώσεων ή τη διόρθωση ζητημάτων τα οποία δεν μπορούν να επιλυθούν από αυτόματες ενημερώσεις των μονάδων προγράμματος. Η αναβάθμιση σε πιο πρόσφατη έκδοση μπορεί να επιτευχθεί με πολλούς τρόπους:

1. Αυτόματα, μέσω ενημέρωσης του προγράμματος.
Επειδή οι αναβαθμίσεις προγράμματος διανέμονται σε όλους τους χρήστες και είναι δυνατό να επηρεάζουν συγκεκριμένες διαμορφώσεις συστήματος, εκδίδονται ύστερα από μακρά περίοδο δοκιμών για τη διασφάλιση της λειτουργικότητας με όλες τις δυνατές διαμορφώσεις συστήματος. Εάν θέλετε να κάνετε αναβάθμιση σε νεότερη έκδοση αμέσως μετά την κυκλοφορία της, χρησιμοποιήστε μία από τις παρακάτω μεθόδους.
Βεβαιωθείτε ότι έχετε ενεργοποιήσει το στοιχείο **Ενημερώσεις δυνατοτήτων εφαρμογής** στην ενότητα **Ρυθμίσεις για προχωρημένους** (F5) > **Ενημέρωση** > **Προφίλ** > **Ενημερώσεις**.

2. Μη αυτόματα, από το κύριο παράθυρο του προγράμματος, κάνοντας κλικ στην επιλογή **Έλεγχος για ενημερώσεις** στην ενότητα **Ενημέρωση**.

3. Μη αυτόματα, πραγματοποιώντας λήψη και εγκατάσταση μιας πιο πρόσφατης έκδοσης επάνω από την προηγούμενη.

Για πρόσθετες πληροφορίες και εικονογραφημένες οδηγίες ανατρέξτε στην ενότητα:

- Ενημέρωση προϊόντων ESET—έλεγχος για τις πιο πρόσφατες λειτουργικές μονάδες προϊόντων

- Ποιοι είναι οι διάφοροι τύποι ενημερώσεων και εκδόσεων των προϊόντων ESET;

Αυτόματη αναβάθμιση προϊόντος παλαιού τύπου

Η έκδοση του προϊόντος ESET που διαθέτετε δεν υποστηρίζεται πλέον και το προϊόν σας έχει αναβαθμιστεί στην πιο πρόσφατη έκδοση.

⚠ Συνηθισμένα προβλήματα εγκατάστασης

ℹ Κάθε νέα έκδοση των προϊόντων ESET διαθέτει πολλές διορθώσεις σφαλμάτων και βελτιώσεις. Οι υπάρχοντες πελάτες με έγκυρη άδεια χρήσης για ένα προϊόν ESET μπορούν να αναβαθμίσουν δωρεάν στην πιο πρόσφατη έκδοση του ίδιου προϊόντος.

Για να ολοκληρώσετε την εγκατάσταση:

1. Κάντε κλικ στο στοιχείο **Αποδοχή και συνέχεια** για να αποδεχτείτε τη Συμφωνία άδειας χρήσης τελικού χρήστη και την Πολιτική Απορρήτου. Εάν δεν συμφωνείτε με τη Συμφωνία άδειας χρήσης τελικού χρήστη, κάντε κλικ στο στοιχείο **Κατάργηση εγκατάστασης**. Δεν είναι δυνατή η επιστροφή στην προηγούμενη έκδοση.

2. Κάντε κλικ στην επιλογή **Να επιτρέπονται όλα και συνέχεια** για να επιτρέπετε τόσο το Σύστημα ανατροφοδότησης ESET LiveGrid® όσο και το Πρόγραμμα βελτίωσης εμπειρίας του πελάτη ή κάντε κλικ στο κουμπί **Συνέχεια** εάν δεν θέλετε να συμμετάσχετε.

3. Αφού ενεργοποιήσετε το νέο προϊόν ESET με το κλειδί άδειας χρήσης, θα εμφανιστεί η αρχική σελίδα. Εάν δεν βρεθούν οι πληροφορίες άδειας χρήσης, συνεχίστε με μια νέα δοκιμαστική άδεια χρήσης. Εάν η άδεια χρήσης που χρησιμοποιήθηκε στο προηγούμενο προϊόν δεν είναι έγκυρη, ενεργοποιήστε το προϊόν ESET.

4. Απαιτείται επανεκκίνηση της συσκευής για την ολοκλήρωση της εγκατάστασης.

Παραπομπή ενός προϊόντος ESET σε έναν φίλο

Αυτή η έκδοση του ESET Internet Security προσφέρει πλέον μπόνους παραπομπής, ώστε να μπορείτε να μοιραστείτε την εμπειρία σας με το προϊόν ESET με την οικογένεια ή τους φίλους σας. Μπορείτε ακόμα να μοιραστείτε παραπομπές από ένα προϊόν που έχει ενεργοποιηθεί με δοκιμαστική άδεια χρήσης. Εάν είστε χρήστης δοκιμαστικής έκδοσης, για κάθε επιτυχή παραπομπή που στέλνετε και έχει σαν αποτέλεσμα ενεργοποίηση προϊόντος, τόσο εσείς όσο και ο φίλος σας θα λαμβάνετε επιπλέον χρόνο στην δοκιμαστική άδεια χρήσης.

Μπορείτε να κάνετε παραπομπή χρησιμοποιώντας το εγκατεστημένο ESET Internet Security. Το προϊόν που μπορείτε να παραπέμψετε εξαρτάται από το προϊόν από το οποίο κάνετε την παραπομπή. Δείτε τον παρακάτω πίνακα.

Το εγκατεστημένο προϊόν σας	Προϊόν που μπορείτε να παραπέμψετε
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security

Το εγκατεστημένο προϊόν σας	Προϊόν που μπορείτε να παραπέμψετε
ESET Smart Security Premium	ESET Smart Security Premium

Παραπομπή ενός προϊόντος

Για να στείλετε έναν παραπεμπτικό σύνδεσμο, κάντε κλικ στο στοιχείο **Παραπομπή σε έναν φίλο/η** στο κύριο μενού του ESET Internet Security. Κάντε κλικ στο στοιχείο **Κοινοποίηση παραπεμπτικού συνδέσμου**. Το προϊόν σας θα δημιουργήσει έναν παραπεμπτικό σύνδεσμο που θα εμφανιστεί σε ένα νέο παράθυρο. Αντιγράψτε το σύνδεσμο και στείλτε τον στην οικογένεια και τους φίλους σας. Μπορείτε να μοιραστείτε τον παραπεμπτικό σύνδεσμο απευθείας από το προϊόν ESET χρησιμοποιώντας τις επιλογές **Κοινοποίηση στο Facebook**, **Παραπομπή των επαφών σας στο Gmail** και **Κοινοποίηση στο Twitter**.

Όταν ο φίλος σας κάνει κλικ στον παραπεμπτικό σύνδεσμο που θα του στείλετε, θα ανακατευθυνθεί σε μια ιστοσελίδα, όπου μπορεί να λάβει το προϊόν και να το χρησιμοποιήσει για έναν επιπλέον μήνα ΔΩΡΕΑΝ προστασίας. Ως χρήστης δοκιμαστικής έκδοσης, θα λάβετε μια ειδοποίηση για κάθε παραπεμπτικό σύνδεσμο που έχει ενεργοποιηθεί επιτυχώς και η άδεια χρήσης σας θα παραταθεί αυτόματα για έναν επιπλέον μήνα ΔΩΡΕΑΝ προστασίας. Με αυτό τον τρόπο μπορείτε να επεκτείνετε τη ΔΩΡΕΑΝ προστασία σας μέχρι και 5 μήνες. Μπορείτε να ελέγξετε τον αριθμό παραπεμπτικών συνδέσμων που ενεργοποιήθηκαν επιτυχώς στο παράθυρο **Παραπομπή σε έναν φίλο/η** στο προϊόν ESET που διαθέτετε.

ℹ Η δυνατότητα παραπομπής ενδέχεται να μην είναι διαθέσιμη για τη γλώσσα/την περιοχή σας.

Το προϊόν ESET Internet Security θα εγκατασταθεί

Μπορείτε να εμφανίσετε αυτό το παράθυρο διαλόγου:

- Κατά τη διεργασία εγκατάστασης – Κάντε κλικ στο στοιχείο **Συνέχεια** για να εγκαταστήσετε το ESET Internet Security.

- Εάν αλλάξετε μια άδεια χρήσης στο ESET Internet Security – Κάντε κλικ στο στοιχείο **Ενεργοποίηση** για να αλλάξετε την άδεια χρήσης και να ενεργοποιήσετε το ESET Internet Security.

Η επιλογή **Αλλαγή προϊόντος** σάς επιτρέπει να κάνετε εναλλαγή μεταξύ των οικιακών προϊόντων ESET για Windows ανάλογα με την άδεια χρήσης ESET που διαθέτετε. Για περισσότερες πληροφορίες, δείτε την ενότητα Ποιο προϊόν έχω;.

Αλλαγή σε διαφορετική γραμμή προϊόντων

Ανάλογα με την άδεια χρήσης ESET που διαθέτετε, μπορείτε να κάνετε εναλλαγή μεταξύ διαφόρων οικιακών προϊόντων ESET για Windows. Για περισσότερες πληροφορίες, δείτε την ενότητα Ποιο προϊόν έχω;.

Εγγραφή

Δηλώστε την άδεια χρήσης σας συμπληρώνοντας τα πεδία που περιέχονται στη φόρμα εγγραφής και κάντε κλικ στο κουμπί Ενεργοποίηση. Πρέπει οπωσδήποτε να συμπληρώσετε τα πεδία που επισημαίνονται ως υποχρεωτικά. Αυτές οι πληροφορίες θα χρησιμοποιηθούν μόνο για θέματα που αφορούν την άδεια χρήσης του προϊόντος ESET που χρησιμοποιείτε.

Εξέλιξη ενεργοποίησης

Αφήστε να περάσουν μερικά δευτερόλεπτα μέχρι να ολοκληρωθεί η διαδικασία ενεργοποίησης (ο απαιτούμενος χρόνος ενδέχεται να ποικίλλει ανάλογα με την ταχύτητα της σύνδεσής σας στο Internet ή του υπολογιστή σας).

Η ενεργοποίηση ήταν επιτυχής

Η διαδικασία ενεργοποίησης έχει ολοκληρωθεί. Ακολουθήστε τον οδηγό μετά την εγκατάσταση για να ολοκληρώσετε τη ρύθμιση του ESET Internet Security.

Σε λίγα δευτερόλεπτα θα ξεκινήσει η ενημέρωση μονάδων. Οι τακτικές ενημερώσεις του ESET Internet Security θα ξεκινήσουν αμέσως.

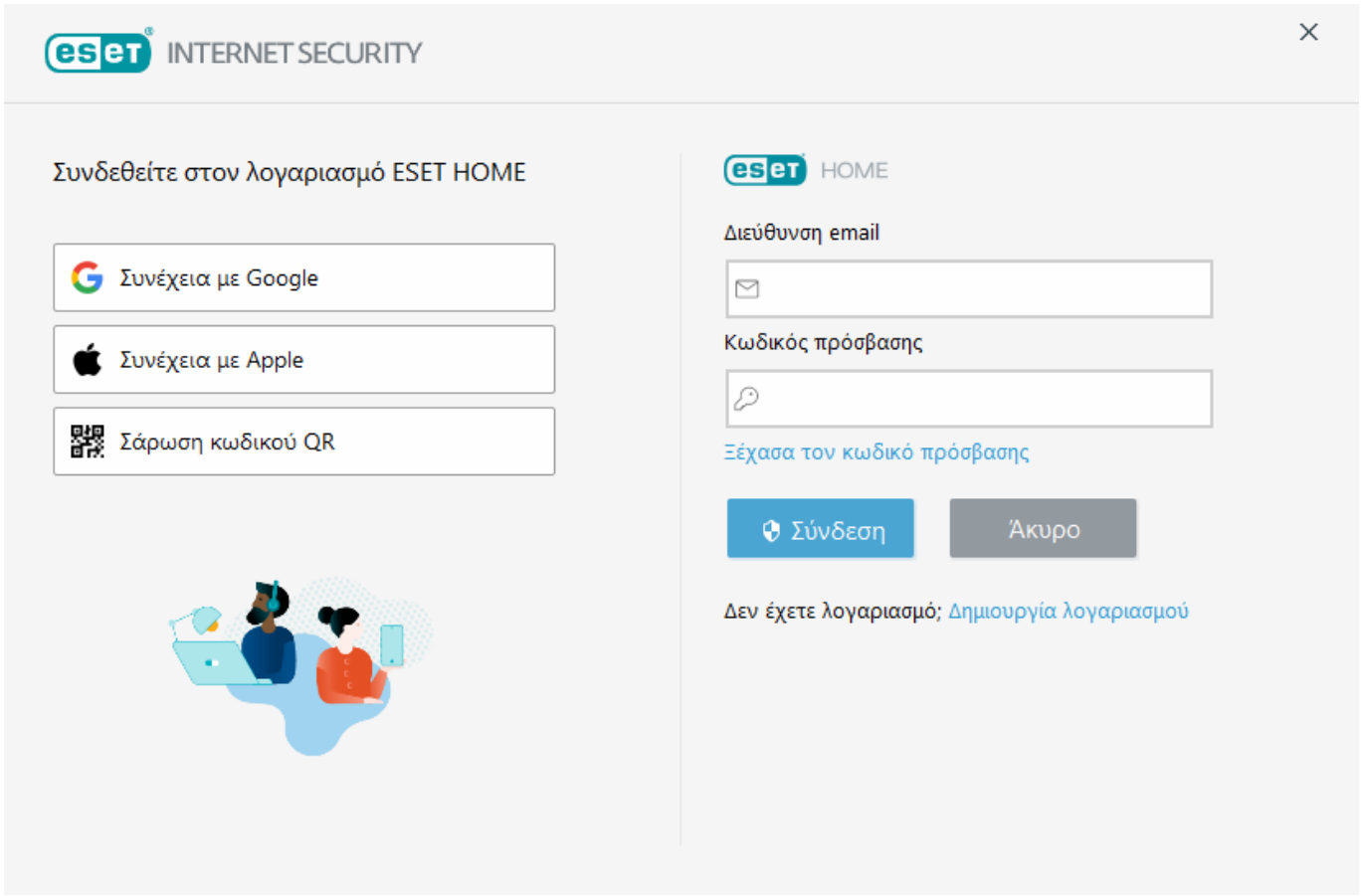
Μια αρχική σάρωση θα ξεκινήσει αυτόματα μέσα σε 20 λεπτά μετά την ενημέρωση μονάδων.

Εγχειρίδιο για αρχάριους

Το κεφάλαιο αυτό παρέχει μια αρχική επισκόπηση του ESET Internet Security και των βασικών του ρυθμίσεων.

Συνδεθείτε στο ESET HOME

Συνδέστε τη συσκευή σας με την ESET HOME για να προβάλλετε και να διαχειρίζεστε όλες τις ενεργοποιημένες άδειες χρήσης της ESET και τις συσκευές σας. Μπορείτε να ανανεώσετε, να αναβαθμίσετε ή να επεκτείνετε την άδεια χρήσης σας και να δείτε σημαντικές λεπτομέρειες της άδειας χρήσης. Στην πύλη διαχείρισης ESET HOME ή στην εφαρμογή για κινητές συσκευές, μπορείτε να επεξεργαστείτε τις ρυθμίσεις του Anti-Theft, προσθέσετε διάφορες άδειες χρήσης, να πραγματοποιήσετε λήψη προϊόντων στις συσκευές σας, να ελέγξετε την κατάσταση ασφάλειας του προϊόντος ή να κάνετε κοινή χρήση αδειών χρήσης μέσω email. Για περισσότερες πληροφορίες, επισκεφθείτε τις σελίδες ηλεκτρονικής βοήθειας του ESET HOME.



Συνδέστε τη συσκευή σας με το ESET HOME:

Εάν συνδεθείτε στο ESET HOME κατά την εγκατάσταση ή εάν επιλέξετε το στοιχείο **Χρήση λογαριασμού ESET HOME** ως μέθοδο ενεργοποίησης, ακολουθήστε τις οδηγίες στο θέμα Χρήση του λογαριασμού ESET HOME.
Εάν έχετε εγκαταστήσει ήδη το ESET Internet Security και το έχετε ενεργοποιήσει με μια άδεια χρήσης που έχει προστεθεί στον λογαριασμό σας στο ESET HOME, μπορείτε να συνδέσετε τη συσκευή σας στο ESET HOME χρησιμοποιώντας την πύλη ESET HOME. Ακολουθήστε τις οδηγίες στον Οδηγό ηλεκτρονικής βοήθειας του ESET HOME και επιτρέψτε τη σύνδεση στο ESET Internet Security.

1. Στο κύριο παράθυρο του προγράμματος, κάντε κλικ στα στοιχεία **ESET HOME** > **Σύνδεση στο ESET HOME** ή κάντε κλικ στο στοιχείο **Σύνδεση στο ESET HOME** στην ειδοποίηση **Σύνδεση αυτής της συσκευής με έναν λογαριασμό ESET HOME**.

2. Σύνδεση στον λογαριασμό σας στο ESET HOME.

Εάν δεν έχετε λογαριασμό στο ESET HOME, κάντε κλικ στο στοιχείο **Δημιουργία λογαριασμού** για να εγγραφείτε ή δείτε τις οδηγίες στην Ηλεκτρονική βοήθεια του ESET HOME.
Εάν ξεχάσατε τον κωδικό πρόσβασής σας, κάντε κλικ στο στοιχείο **Ξέχασα τον κωδικό πρόσβασης** και ακολουθήστε τα βήματα στην οθόνη ή δείτε τις οδηγίες στην Ηλεκτρονική βοήθεια του ESET HOME.

3. Ρυθμίστε ένα **Όνομα συσκευής** και κάντε κλικ στο στοιχείο **Συνέχεια**.

4. Αφού συνδεθείτε επιτυχώς, θα εμφανιστεί ένα παράθυρο λεπτομερειών. Κάντε κλικ στο στοιχείο **Τέλος**.

Σύνδεση στο ESET HOME

Υπάρχουν πολλές διαθέσιμες μέθοδοι σύνδεσης στον λογαριασμό σας στο ESET HOME:

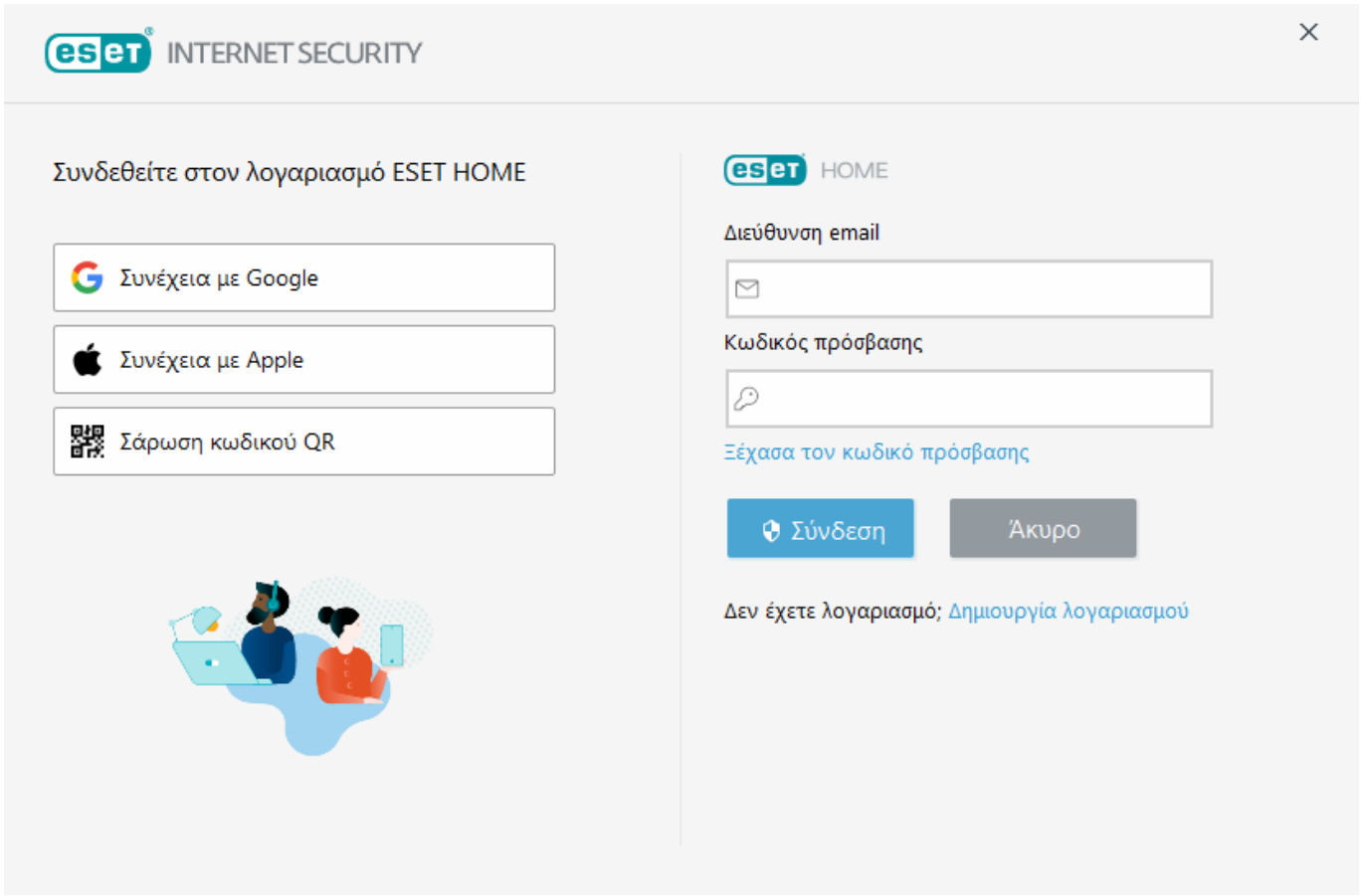
• **Χρήση της διεύθυνσης email και του κωδικού πρόσβασης στο ESET HOME** - Πληκτρολογήστε τη **Διεύθυνση email** και τον **Κωδικό πρόσβασης** που χρησιμοποιήσατε για να δημιουργήσετε τον λογαριασμό σας στο ESET HOME και κάντε κλικ στο στοιχείο **Σύνδεση**.

• **Χρήση του λογαριασμού σας στο Google/AppleID** – Κάντε κλικ στο στοιχείο **Συνέχεια με Google** ή **Συνέχεια με Apple** και συνδεθείτε στον κατάλληλο λογαριασμό. Μετά από επιτυχημένη σύνδεση, θα μεταφερθείτε στην ιστοσελίδα επιβεβαίωσης του ESET HOME. Για να συνεχίσετε, επιστρέψτε στο παράθυρο του προϊόντος ESET. Για περισσότερες πληροφορίες σχετικά με τη σύνδεση μέσω λογαριασμού Google/AppleID, ανατρέξτε στις οδηγίες στο θέμα Ηλεκτρονική βοήθεια του ESET HOME.

• **Σάρωση κωδικού QR** – Κάντε κλικ στην επιλογή **Σάρωση κωδικού QR** για να εμφανίσετε τον κωδικό QR. Ανοίξτε την εφαρμογή για κινητά ESET HOME και σαρώστε τον κωδικό QR ή στρέψτε την κάμερα της συσκευής σας στον κωδικό QR. Για περισσότερες πληροφορίες, ανατρέξτε στις οδηγίες της Ηλεκτρονικής βοήθειας του ESET HOME.

Εάν δεν έχετε λογαριασμό στο ESET HOME, κάντε κλικ στο στοιχείο **Δημιουργία λογαριασμού** για να εγγραφείτε ή δείτε τις οδηγίες στην Ηλεκτρονική βοήθεια του ESET HOME.
Εάν ξεχάσατε τον κωδικό πρόσβασής σας, κάντε κλικ στο στοιχείο **Ξέχασα τον κωδικό πρόσβασης** και ακολουθήστε τα βήματα στην οθόνη ή δείτε τις οδηγίες στην Ηλεκτρονική βοήθεια του ESET HOME.

Η σύνδεση απέτυχε - συνήθη σφάλματα.



Η σύνδεση απέτυχε - συνήθη σφάλματα

Δεν ήταν δυνατή η εύρεση λογαριασμού που να ταιριάζει με τη διεύθυνση email που εισαγάγατε

Η διεύθυνση email που πληκτρολογήσατε δεν αντιστοιχεί σε κανέναν λογαριασμό του ESET HOME. Κάντε κλικ στο στοιχείο **Πίσω** και πληκτρολογήστε σωστά τη διεύθυνση email και τον κωδικό πρόσβασης.

Για να συνδεθείτε, πρέπει να δημιουργήσετε έναν λογαριασμό στο ESET HOME. Εάν δεν έχετε λογαριασμό στο ESET HOME, κάντε κλικ στο στοιχείο **Πίσω** > **Δημιουργία λογαριασμού** ή ανατρέξτε στο θέμα Δημιουργία νέου λογαριασμού στο ESET HOME.

Το όνομα χρήστη και ο κωδικός πρόσβασης δεν ταιριάζουν

Ο κωδικός πρόσβασης που έχετε εισαγάγει δεν συμφωνεί με την διεύθυνση email που καταχωρίσατε. Κάντε κλικ στο στοιχείο **Πίσω**, πληκτρολογήστε σωστά τον κωδικό πρόσβασης και βεβαιωθείτε ότι η διεύθυνση email που έχετε εισαγάγει είναι σωστή. Εάν εξακολουθείτε να μην μπορείτε να συνδεθείτε, κάντε κλικ στο στοιχείο **Πίσω** > **Ξέχασα τον κωδικό πρόσβασης** για να επαναφέρετε τον κωδικό πρόσβασής σας και ακολουθήστε τα βήματα στην οθόνη ή ανατρέξτε στο θέμα Ξέχασα τον κωδικό πρόσβασής μου στο ESET HOME.

Η καθορισμένη επιλογή σύνδεσης δεν αντιστοιχεί στον λογαριασμό σας

Ο λογαριασμός σας είναι συνδεδεμένος με τον λογαριασμό σας στα μέσα κοινωνικής δικτύωσης. Για να συνδεθείτε στο ESET HOME κάντε κλικ στο στοιχείο **Συνέχεια με Google** ή **Συνέχεια με Apple** και συνδεθείτε στον κατάλληλο λογαριασμό. Μετά από επιτυχημένη σύνδεση, θα μεταφερθείτε στην ιστοσελίδα επιβεβαίωσης του ESET HOME. Μπορείτε να αποσυνδέσετε τον λογαριασμό σας στα μέσα κοινωνικής δικτύωσης από τον λογαριασμό σας στο ESET HOME στην πύλη ESET HOME.

Εσφαλμένος κωδικός πρόσβασης

Αυτό το σφάλμα μπορεί να προκύψει εάν το ESET Internet Security είναι ήδη συνδεδεμένο στο ESET HOME και κάνετε αλλαγές που απαιτούν να συνδεθείτε (π.χ. απενεργοποίηση του Anti-Theft) και ο κωδικός πρόσβασης που πληκτρολογήσατε δεν αντιστοιχεί στον λογαριασμό σας. Κάντε κλικ στο στοιχείο **Πίσω** και πληκτρολογήστε σωστά τον κωδικό πρόσβασης. Εάν εξακολουθείτε να μην μπορείτε να συνδεθείτε, κάντε κλικ στο στοιχείο **Πίσω** > **Ξέχασα τον κωδικό πρόσβασης** για να επαναφέρετε τον κωδικό πρόσβασής σας και ακολουθήστε τα βήματα στην οθόνη ή ανατρέξτε στο θέμα Ξέχασα τον κωδικό πρόσβασής μου στο ESET HOME.

Προσθήκη συσκευής στο ESET HOME

Εάν έχετε εγκαταστήσει ήδη το ESET Internet Security και το έχετε ενεργοποιήσει με μια άδεια χρήσης που έχει προστεθεί στον λογαριασμό σας στο ESET HOME, μπορείτε να συνδέσετε τη συσκευή σας στο ESET HOME χρησιμοποιώντας την πύλη ESET HOME:

1. Αποστολή αιτήματος σύνδεσης στη συσκευή σας.

2. Το ESET Internet Security εμφανίζει το παράθυρο διαλόγου **Σύνδεση αυτής της συσκευής με έναν λογαριασμό ESET HOME** με ένα όνομα του λογαριασμού στο ESET HOME. Κάντε κλικ στο στοιχείο **Να επιτρέπεται** για να συνδέσετε τη συσκευή με τον προαναφερθέντα λογαριασμό στο ESET HOME.

> Εάν δεν υπάρχει αλληλεπίδραση, το αίτημα σύνδεσης θα ακυρωθεί αυτόματα μετά από 30 λεπτά περίπου.

Το κύριο παράθυρο του προγράμματος

Το κύριο παράθυρο προγράμματος του ESET Internet Security χωρίζεται σε δύο κύριες ενότητες. Το κύριο παράθυρο στα δεξιά εμφανίζει πληροφορίες που αντιστοιχούν στην επιλογή που έχει γίνει από το κύριο μενού στα αριστερά.

> Εικονογραφημένες οδηγίες
> Ανατρέξτε στο θέμα Άνοιγμα του κύριου παραθύρου του προγράμματος των προϊόντων ESET για Windows για εικονογραφημένες οδηγίες που είναι διαθέσιμες στα Αγγλικά και σε αρκετές άλλες γλώσσες.

ESET HOME– Συνδέστε τη συσκευή σας με το ESET HOME. Χρησιμοποιήστε το ESET HOME για να δείτε και να διαχειριστείτε τις ρυθμίσεις Anti-Theft και τις ενεργοποιημένες άδειες χρήσης ESET και τις

συσκευές.

Ακολουθεί μια περιγραφή των επιλογών στο κύριο μενού:

Αρχική σελίδα – Παρέχει πληροφορίες σχετικά με την κατάσταση προστασίας του ESET Internet Security.

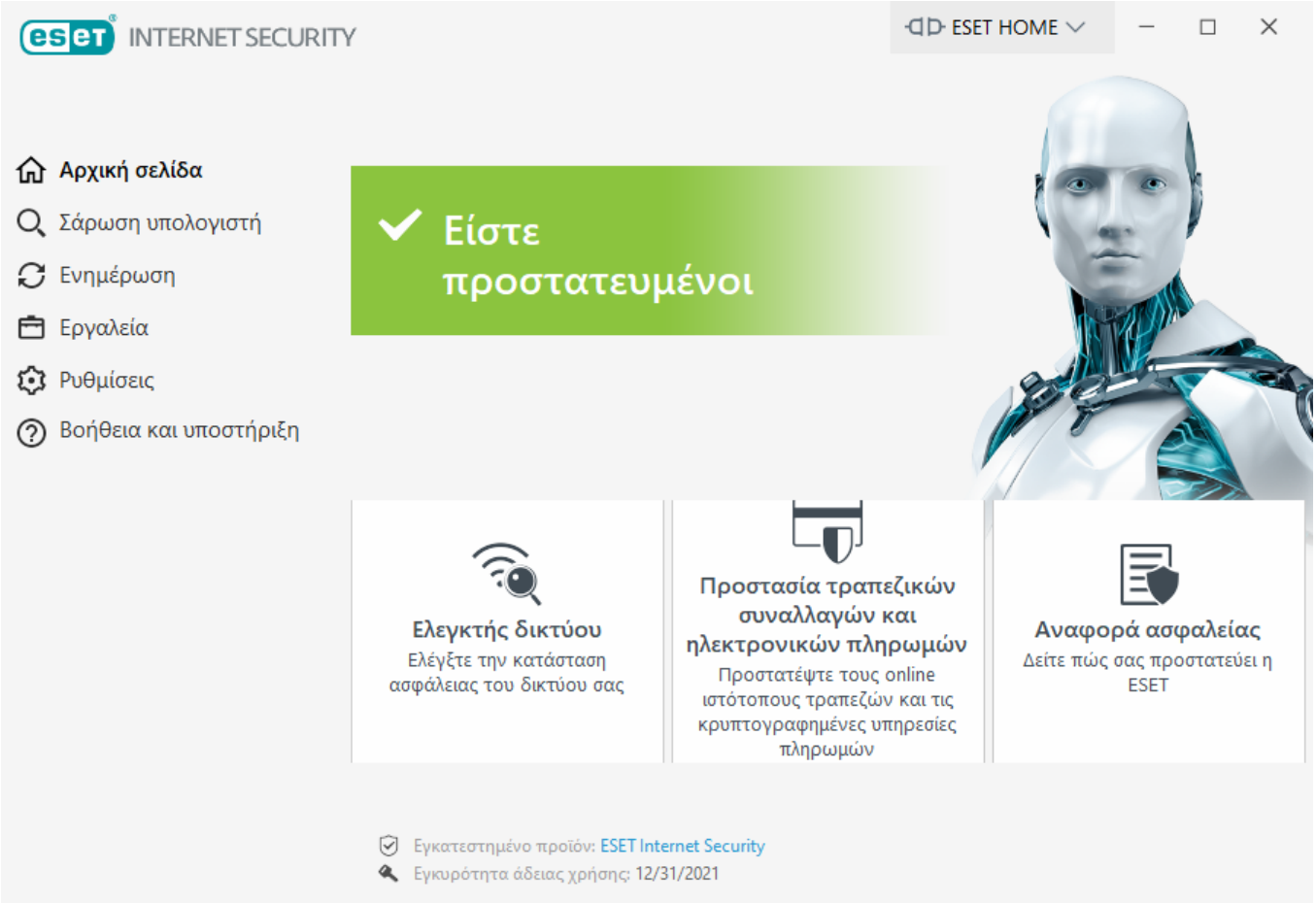
Σάρωση υπολογιστή – Διαμορφώστε και ξεκινήστε σάρωση του υπολογιστή σας ή δημιουργήστε μια προσαρμοσμένη σάρωση.

Ενημέρωση – Εμφανίζει πληροφορίες σχετικά με τις ενημερώσεις του μηχανισμού ανίχνευσης.

Εργαλεία – Παρέχει πρόσβαση στο Ελεγκτής δικτύου, στην Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών, στο Anti-Theft και σε άλλες λειτουργικές μονάδες που βοηθούν να απλοποιηθεί η διαχείριση του προγράμματος και προσφέρουν πρόσθετες επιλογές για προχωρημένους χρήστες. Για περισσότερες πληροφορίες, ανατρέξτε στα Εργαλεία στο ESET Internet Security.

Ρυθμίσεις – Επιλέξτε για να ρυθμίσετε το επίπεδο ασφαλείας για τον Υπολογιστή, το Internet, την Προστασία δικτύου και τα Εργαλεία ασφαλείας.

Βοήθεια και υποστήριξη – Παρέχει πρόσβαση σε αρχεία βοήθειας, στη Γνωσιακή βάση της ESET, στον ιστότοπο της ESET και συνδέσμους για την υποβολή αιτήματος υποστήριξης.



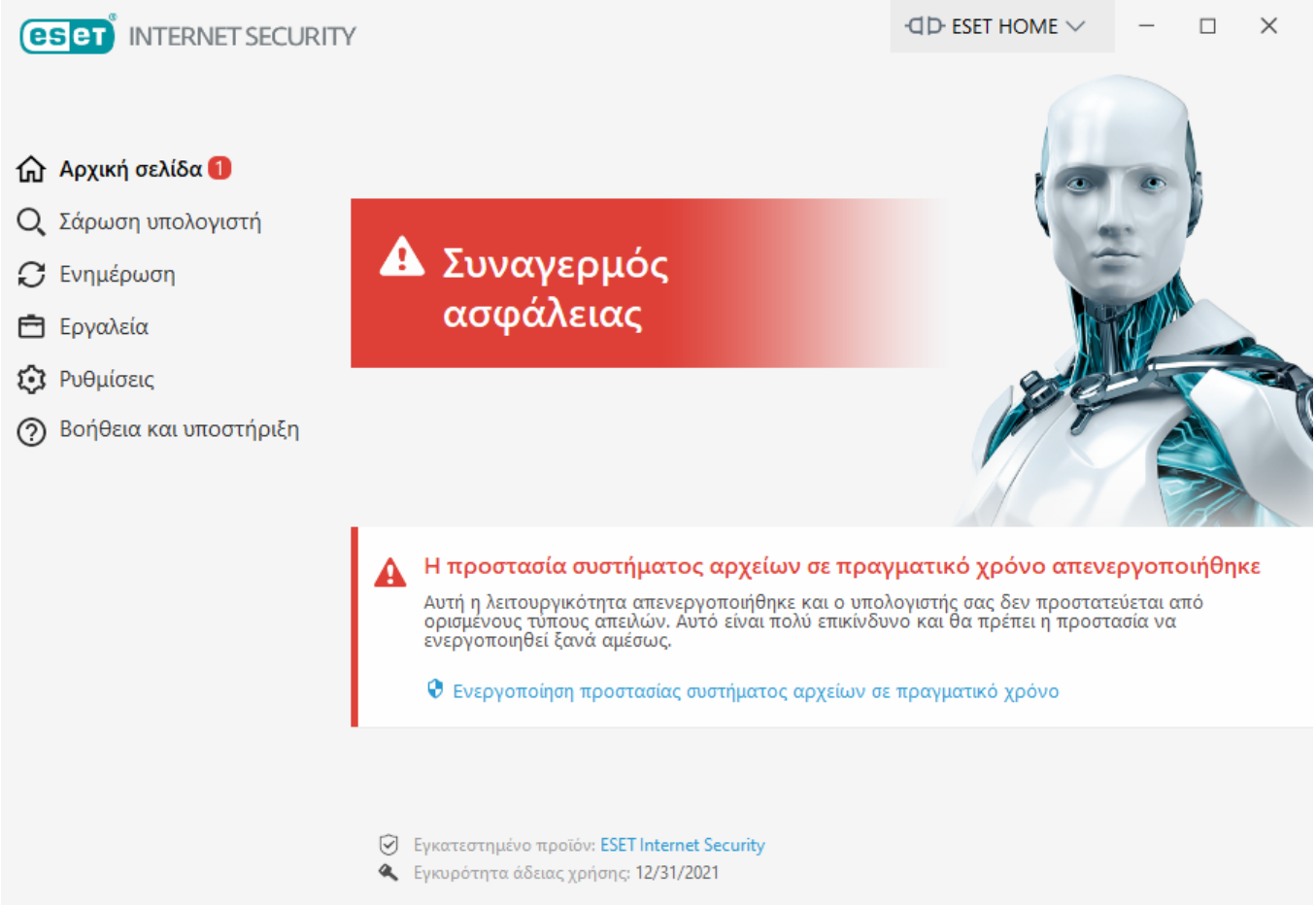
Η **Αρχική οθόνη** περιέχει σημαντικές πληροφορίες για το τρέχον επίπεδο προστασίας του υπολογιστή σας. Το παράθυρο κατάστασης εμφανίζει δυνατότητες που χρησιμοποιούνται συχνά στο ESET Internet Security. Εδώ μπορείτε επίσης να βρείτε πληροφορίες για το εγκατεστημένο προϊόν και

την ημερομηνία λήξης της άδειας χρήσης. Κάντε κλικ στο στοιχείο **ESET Internet Security** εάν θέλετε να εγκαταστήσετε μια άλλη έκδοση του προϊόντος ESET. Περισσότερες πληροφορίες σχετικά με τις δυνατότητες κάθε συγκεκριμένου προϊόντος.

Το πράσινο εικονίδιο και η πράσινη ένδειξη κατάστασης **Είστε ασφαλείς** υποδεικνύουν ότι διασφαλίζεται μέγιστη προστασία.

Τι να κάνετε αν δεν λειτουργεί σωστά το πρόγραμμα;

Όταν μια ενεργή μονάδα προστασίας λειτουργεί σωστά, το αντίστοιχο εικονίδιο κατάστασης προστασίας θα είναι πράσινο. Το κόκκινο θαυμαστικό ή η πορτοκαλί εικονίδιο προειδοποίησης υποδηλώνουν ότι δεν διασφαλίζεται μέγιστη προστασία. Πρόσθετες πληροφορίες σχετικά με την κατάσταση προστασίας κάθε μονάδας, καθώς και προτεινόμενες λύσεις για την επαναφορά πλήρους προστασίας θα εμφανίζονται στην ενότητα **Αρχική σελίδα**. Για να αλλάξετε την κατάσταση μεμονωμένων μονάδων, κάντε κλικ στο στοιχείο **Ρυθμίσεις** και επιλέξτε τη μονάδα που θέλετε.



Το κόκκινο εικονίδιο και η κόκκινη ένδειξη κατάστασης **Συναγερμός ασφάλειας** υποδεικνύουν κρίσιμα προβλήματα.
Υπάρχουν πολλοί λόγοι για τους οποίους μπορεί να εμφανίζεται αυτή η κατάσταση, όπως για παράδειγμα:

- **Το προϊόν δεν ενεργοποιήθηκε** ή **Η άδεια χρήσης έληξε** – Αυτό υποδηλώνεται με ένα κόκκινο εικονίδιο κατάστασης προστασίας. Το πρόγραμμα δεν μπορεί να κάνει ενημέρωση μετά τη λήξη της άδειας χρήσης. Ακολουθήστε τις οδηγίες στο παράθυρο ειδοποίησης για να ανανεώσετε την άδεια χρήσης σας.

- **Ο μηχανισμός ανίχνευσης δεν είναι ενημερωμένος** – Αυτό το σφάλμα εμφανίζεται ύστερα από αρκετές ανεπιτυχείς προσπάθειες ενημέρωσης του μηχανισμού ανίχνευσης. Συνιστούμε να ελέγξετε τις ρυθμίσεις ενημέρωσης. Η συνηθέστερη αιτία αυτού του σφάλματος είναι η εισαγωγή εσφαλμένων δεδομένων ελέγχου ταυτότητας ή η εσφαλμένη διαμόρφωση των ρυθμίσεων σύνδεσης.

- **Η Προστασία συστήματος αρχείων σε πραγματικό χρόνο απενεργοποιήθηκε** – Η προστασία πραγματικού χρόνου απενεργοποιήθηκε από το χρήστη. Ο υπολογιστής σας δεν προστατεύεται από απειλές. Κάντε κλικ στο στοιχείο **Ενεργοποίηση προστασίας συστήματος αρχείων σε πραγματικό χρόνο** για να ενεργοποιήσετε ξανά αυτήν τη λειτουργικότητα.

- **Η προστασία Antivirus και Antispyware έχει απενεργοποιηθεί** – Μπορείτε να ενεργοποιήσετε ξανά την προστασία antivirus και antispyware κάνοντας κλικ στην επιλογή **Ενεργοποίηση της προστασίας antivirus και antispyware**.

- **Το Firewall της ESET απενεργοποιήθηκε** – Αυτό το πρόβλημα σηματοδοτείται επίσης από μια ειδοποίηση ασφαλείας δίπλα στο στοιχείο **Δίκτυο** στην επιφάνεια εργασίας. Μπορείτε να ενεργοποιήσετε ξανά την προστασία δικτύου κάνοντας κλικ στο στοιχείο **Ενεργοποίηση τείχους προστασίας**.

Το πορτοκαλί εικονίδιο δηλώνει περιορισμένη προστασία. Για παράδειγμα, ίσως υπάρχει πρόβλημα με την ενημέρωση του προγράμματος ή μπορεί να πλησιάζει η ημερομηνία λήξης της άδειας χρήσης.
Υπάρχουν πολλοί λόγοι για τους οποίους μπορεί να εμφανίζεται αυτή η κατάσταση, όπως για παράδειγμα:

- **Προειδοποίηση βελτιστοποίησης αντικλεπτικής μονάδας** – Αυτή η συσκευή δεν είναι βελτιστοποιημένη για Anti-Theft. Για παράδειγμα, ίσως να μην έχει δημιουργηθεί λογαριασμός Phantom (μια δυνατότητα ασφαλείας που ενεργοποιείται αυτόματα όταν επισημαίνετε μια συσκευή ως χαμένη). Μπορείτε να δημιουργήσετε έναν λογαριασμό Phantom χρησιμοποιώντας τη δυνατότητα Βελτιστοποίηση στη διασύνδεση ιστού του Anti-Theft.

- **Η λειτουργία Gamer ενεργοποιήθηκε** – Η ενεργοποίηση της λειτουργίας Gamer είναι δυνητικός κίνδυνος ασφαλείας. Εάν ενεργοποιήσετε αυτήν τη δυνατότητα, απενεργοποιούνται όλα τα αναδυόμενα παράθυρα και διακόπτονται όλες οι προγραμματισμένες εργασίες.

- **Η άδειά σας θα λήξει σύντομα** – Αυτό υποδεικνύεται από το εικονίδιο της κατάστασης προστασίας που εμφανίζει ένα θαυμαστικό δίπλα στο ρολόι του συστήματος. Μετά από τη λήξη της άδειας χρήσης σας, το πρόγραμμα δεν θα μπορεί να ενημερώνεται και το εικονίδιο της Κατάστασης προστασίας θα γίνει κόκκινο.

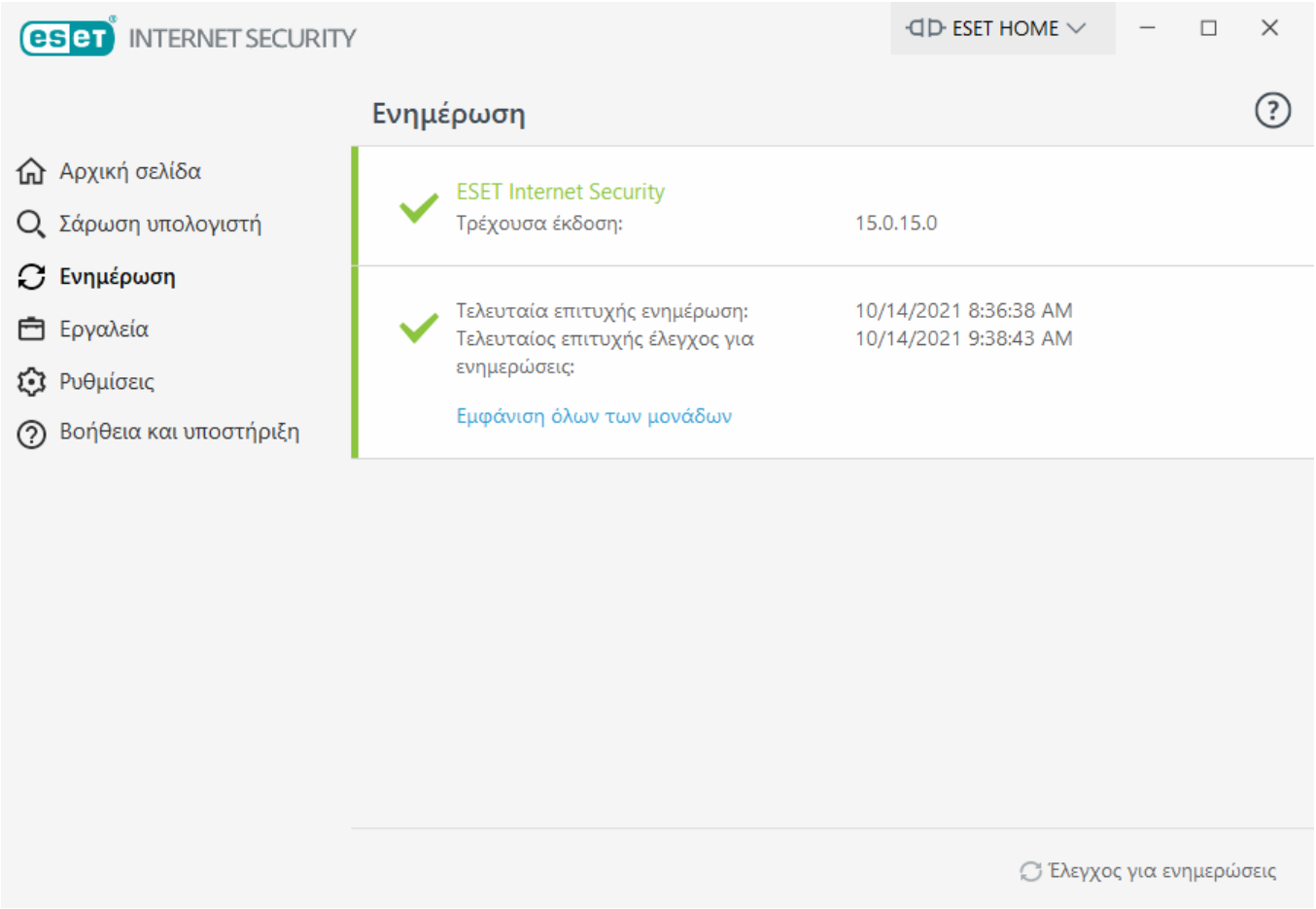
Εάν δεν μπορείτε να λύσετε ένα πρόβλημα χρησιμοποιώντας τις προτεινόμενες λύσεις, κάντε κλικ στο στοιχείο **Βοήθεια και υποστήριξη** για να αποκτήσετε πρόσβαση σε αρχεία βοήθειας ή για να κάνετε αναζήτηση στη Γνωσιακή βάση της ESET. Αν χρειάζεστε και πάλι βοήθεια, μπορείτε να υποβάλετε ένα αίτημα υποστήριξης. Η Τεχνική υποστήριξη της ESET θα απαντήσει γρήγορα στις ερωτήσεις σας και θα σας βοηθήσει να βρείτε μια λύση.

Ενημερώσεις

Η τακτική ενημέρωση του ESET Internet Security είναι η καλύτερη μέθοδος για να διασφαλίσετε μέγιστο επίπεδο ασφάλειας στον υπολογιστή σας. Η μονάδα Ενημέρωσης διασφαλίζει ότι είναι πάντα ενημερωμένες οι μονάδες προγράμματος και τα στοιχεία συστήματος.

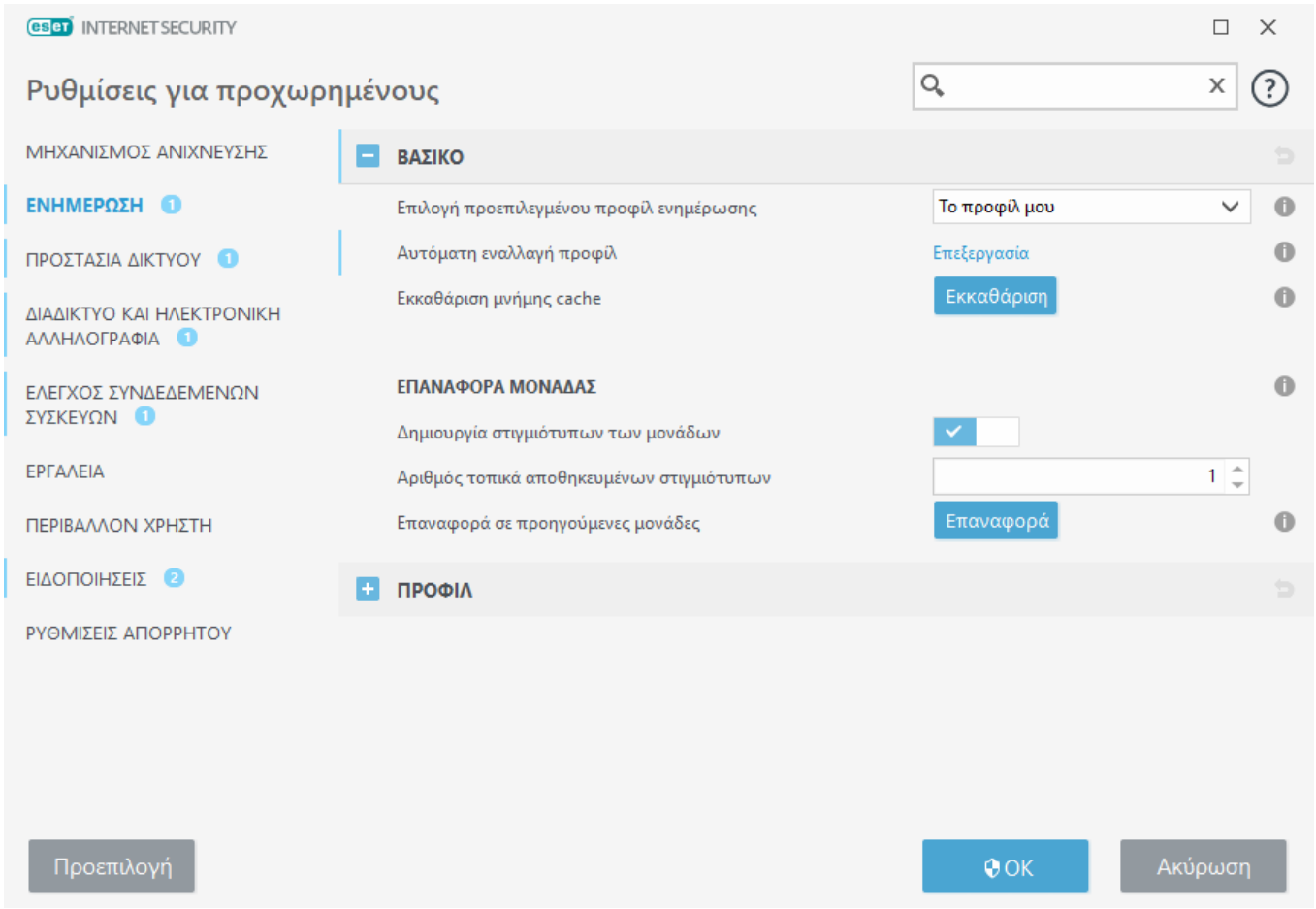
Εάν κάνετε κλικ στο στοιχείο **Ενημέρωση** στο κύριο παράθυρο του προγράμματος, μπορείτε να δείτε την τρέχουσα κατάσταση ενημέρωσης που συμπεριλαμβάνει την ημερομηνία και την ώρα της τελευταίας επιτυχημένης ενημέρωσης, καθώς και αν χρειάζεται ενημέρωση.

Εκτός από τις αυτόματες ενημερώσεις, μπορείτε να κάνετε κλικ στο στοιχείο **Έλεγχος για ενημερώσεις** για να ενεργοποιήσετε μια μη αυτόματη ενημέρωση.



Το παράθυρο «Εγκατάσταση για προχωρημένους» (κάντε κλικ στις **Ρυθμίσεις** στο κύριο μενού και κατόπιν κάντε κλικ στο στοιχείο **Ρυθμίσεις για προχωρημένους** ή πατήστε το πλήκτρο **F5** στο πληκτρολόγιό σας) περιέχει πρόσθετες επιλογές ενημέρωσης. Για να ρυθμίσετε τις παραμέτρους για επιλογές ενημέρωσης για προχωρημένους, όπως η λειτουργία ενημέρωσης, η πρόσβαση του διακομιστή μεσολάβησης και οι συνδέσεις LAN, κάντε κλικ στην επιλογή **Ενημέρωση** στο δέντρο του στοιχείου «Εγκατάσταση για προχωρημένους».

Εάν αντιμετωπίζετε δυσκολίες με μια ενημέρωση, κάντε κλικ στο στοιχείο **Καθαρισμός** για να εκκαθαρίσετε τη μνήμη της ενημέρωσης. Εάν εξακολουθείτε να μην μπορείτε να ενημερώσετε τις μονάδες προγράμματος, ανατρέξτε στην ενότητα Αντιμετώπιση προβλημάτων με το μήνυμα «Αποτυχία ενημέρωσης των μονάδων».



Ρύθμιση πρόσθετων εργαλείων ασφάλειας της ESET

Προτού αρχίσετε να χρησιμοποιείτε το ESET Internet Security, μπορείτε να ρυθμίσετε πρόσθετα εργαλεία ασφαλείας για να μεγιστοποιήσετε την προστασία σας:

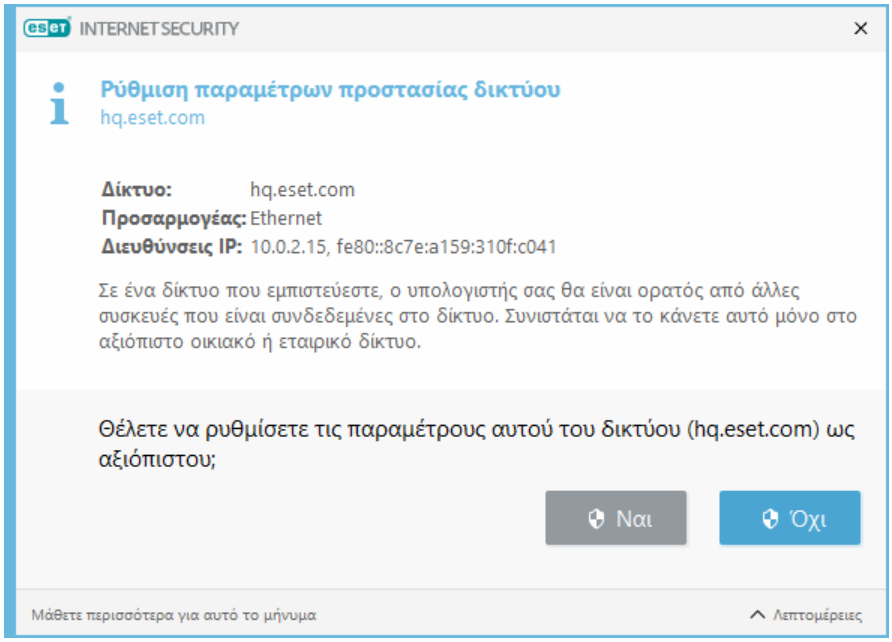
- Γονικός έλεγχος
- Anti-Theft

Για περισσότερες πληροφορίες σχετικά με τη ρύθμιση εργαλείων ασφαλείας στο ESET Internet Security διαβάστε το ακόλουθο άρθρο της Γνωσιακής βάσης της ESET.

Ρύθμιση παραμέτρων προστασίας δικτύου

Είναι απαραίτητο να ρυθμίσετε τις παραμέτρους των συνδεδεμένων δικτύων για να προστατέψετε τον υπολογιστή σας σε ένα περιβάλλον δικτύου. Μπορείτε να επιτρέπετε σε άλλους χρήστες να αποκτούν πρόσβαση στον υπολογιστή σας με τη ρύθμιση παραμέτρων της προστασίας δικτύου, ώστε να επιτρέπεται η κοινή χρήση. Κάντε κλικ στα στοιχεία **Ρυθμίσεις** > **Προστασία δικτύου** > **Συνδεδεμένα δίκτυα** και μετά στο σύνδεσμο κάτω από το συνδεδεμένο δίκτυο. Σε ένα αναδυόμενο παράθυρο θα εμφανιστούν οι επιλογές για τη ρύθμιση παραμέτρων του επιλεγμένου δικτύου ως αξιόπιστου.

Από προεπιλογή, το ESET Internet Security χρησιμοποιεί τις ρυθμίσεις των Windows όταν ανιχνεύεται ένα νέο δίκτυο. Για να εμφανιστεί ένα παράθυρο διαλόγου όταν ανιχνεύεται ένα νέο δίκτυο, αλλάξτε τον τύπο προστασίας των νέων δικτύων στα Γνωστά δίκτυα για να ερωτάται ο χρήστης. Η ρύθμιση παραμέτρων της προστασίας δικτύου προκύπτει κάθε φορά που ο υπολογιστής σας συνδέεται σε ένα νέο δίκτυο. Κατά συνέπεια, δεν απαιτείται συνήθως ο ορισμός Ζωνών αξιοπιστίας.



Υπάρχουν δύο λειτουργίες προστασίας δικτύου που μπορείτε να επιλέξετε στο παράθυρο ρύθμισης παραμέτρων προστασίας δικτύου:

• **Ναι** – Για αξιόπιστο δίκτυο (οικιακό ή εταιρικό δίκτυο). Ο υπολογιστής σας και τα κοινόχρηστα αρχεία που είναι αποθηκευμένα στον υπολογιστή σας είναι ορατά σε άλλους χρήστες του δικτύου και άλλοι χρήστες έχουν πρόσβαση στους πόρους συστήματος. Συνιστάται η χρήση αυτής της ρύθμισης όταν αποκτάτε πρόσβαση σε ένα ασφαλές τοπικό δίκτυο.

• **Όχι** – Για μη αξιόπιστο δίκτυο (δημόσιο δίκτυο). Τα αρχεία και οι φάκελοι στο σύστημά σας δεν είναι κοινόχρηστα ή ορατά σε άλλους χρήστες στο δίκτυο και η κοινή χρήση των πόρων του συστήματος έχει απενεργοποιηθεί. Συνιστάται να χρησιμοποιείτε αυτή τη ρύθμιση όταν αποκτάτε πρόσβαση σε ασύρματα δίκτυα.

Μια λανθασμένη ρύθμιση παραμέτρων ίσως αποτελεί κίνδυνο ασφάλειας για τον υπολογιστή σας.

Από προεπιλογή, στους σταθμούς εργασίας από ένα αξιόπιστο δίκτυο παρέχεται πρόσβαση σε κοινόχρηστα αρχεία και εκτυπωτές, ενεργοποιείται η εισερχόμενη επικοινωνία RPC και είναι διαθέσιμη η κοινή χρήση απομακρυσμένης επιφάνειας εργασίας.

Για περισσότερες λεπτομέρειες σχετικά με αυτήν τη δυνατότητα, ανατρέξτε στο άρθρο της Γνωσιακής βάσης της ESET:

• Αλλαγή της ρύθμισης τείχους προστασίας της σύνδεσης δικτύου στα οικιακά προϊόντα της ESET για Windows

Ενεργοποίηση Anti-Theft

Οι προσωπικές συσκευές κινδυνεύουν διαρκώς με απώλεια ή κλοπή κατά τις καθημερινές μας μετακινήσεις από το σπίτι στο γραφείο και σε άλλους δημόσιους χώρους. Το Anti-Theft είναι μια δυνατότητα που επεκτείνει την ασφάλεια σε επίπεδο χρήστη σε περίπτωση που μια συσκευή χαθεί ή κλαπεί. Το Anti-Theft σάς επιτρέπει να παρακολουθείτε τη χρήση της συσκευής και να εντοπίζετε τη χαμένη συσκευή χρησιμοποιώντας τον εντοπισμό μέσω της διεύθυνσης IP στο ESET HOME, βοηθώντας σας έτσι να ανακτήσετε τη συσκευή σας και να προστατέψετε τα δεδομένα προσωπικού χαρακτήρα.

Με τη χρήση σύγχρονων τεχνολογιών, όπως αναζήτηση γεωγραφικών διευθύνσεων, καταγραφή εικόνων με την ενσωματωμένη κάμερα, προστασία λογαριασμών χρήστη και παρακολούθηση συσκευών, η μονάδα Anti-Theft μπορεί να βοηθήσει εσάς και τις αρχές να εντοπίσουν τον υπολογιστή ή τη συσκευή σας εάν έχει χαθεί ή κλαπεί. Στο ESET HOME, μπορείτε να δείτε τις δραστηριότητες που πραγματοποιούνται στον υπολογιστή ή στη συσκευή σας.

Για να μάθετε περισσότερα σχετικά με το Anti-Theft στο ESET HOME, ανατρέξτε στην Ηλεκτρονική βοήθεια του ESET HOME.

Για να ενεργοποιήσετε το Anti-Theft και να προστατεύσετε τη συσκευή σας σε περίπτωση απώλειας ή κλοπής, επιλέξτε μία από τις ακόλουθες επιλογές:

- Μετά την εγκατάσταση του προϊόντος, κάντε κλικ στο στοιχείο **Ενεργοποίηση του Anti-Theft** για να ενεργοποιήσετε το Anti-Theft.
- Εάν εμφανιστεί το μήνυμα «Το Anti-Theft είναι διαθέσιμο» στο κύριο παράθυρο του προγράμματος > **Αρχική** οθόνη, κάντε κλικ στο στοιχείο **Ενεργοποίηση του Anti-Theft**.
- Από το κύριο παράθυρο του προγράμματος, κάντε κλικ στα στοιχεία **Εργαλεία** > **Anti-Theft**.
- Από το κύριο παράθυρο του προγράμματος, κάντε κλικ στα στοιχεία **Ρυθμίσεις** > **Εργαλεία ασφαλείας**. Κάντε κλικ στο εικονίδιο αλλαγής **Anti-Theft** και ακολουθήστε τις οδηγίες στην οθόνη.

Εάν η συσκευή σας δεν είναι συνδεδεμένη στο ESET HOME, θα πρέπει να κάνετε τα εξής:
1. Συνδεθείτε στον λογαριασμό σας στο ESET HOME όταν ενεργοποιήσετε το Anti-Theft.
2. Ορισμός ονόματος συσκευής.

Το Anti-Theft δεν υποστηρίζει το Microsoft Windows Home Server.

Αφού ενεργοποιήσετε το Anti-Theft, μπορείτε να βελτιστοποιήσετε την ασφάλεια της συσκευής σας από το κύριο παράθυρο του προγράμματος > **Εργαλεία** > **Anti-Theft**.

Εργαλεία Γονικού ελέγχου

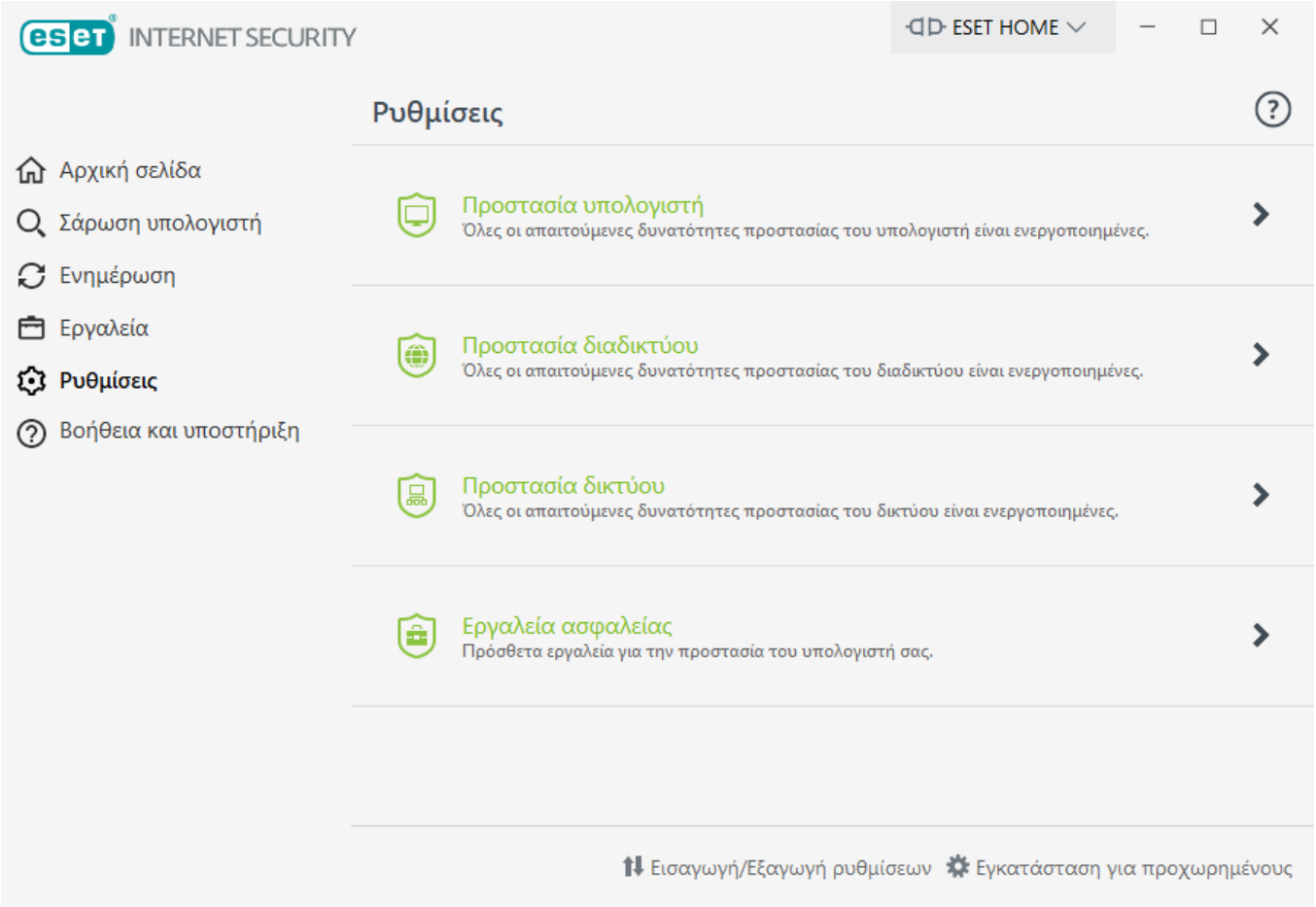
Εάν έχετε ήδη ενεργοποιήσει τον Γονικό έλεγχο στο ESET Internet Security, πρέπει να ρυθμίσετε τις παραμέτρους του Γονικού ελέγχου και για όλους τους σχετικούς λογαριασμούς χρήστη.

Εάν είναι ενεργός ο Γονικός έλεγχος και δεν έχει γίνει ρύθμιση παραμέτρων για τους λογαριασμούς χρηστών, θα εμφανιστεί η ένδειξη «Ο Γονικός έλεγχος δεν ρυθμίστηκε» στην **Αρχική οθόνη**. Κάντε

κλικ στο στοιχείο **Ρύθμιση των κανόνων** και ανατρέξτε στην ενότητα Γονικός έλεγχος για περισσότερες πληροφορίες.

Εργασία με το ESET Internet Security

Οι επιλογές ρυθμίσεων του ESET Internet Security σάς επιτρέπουν να προσαρμόσετε τα επίπεδα προστασίας του υπολογιστή και του δικτύου σας.



Το μενού **Ρυθμίσεις** περιλαμβάνει τις εξής ενότητες:

Προστασία υπολογιστή

Προστασία διαδικτύου

Προστασία δικτύου

Εργαλεία ασφαλείας

Κάντε κλικ σε ένα στοιχείο για να προσαρμόσετε προηγμένες ρυθμίσεις για την αντίστοιχη μονάδα προστασίας.

Οι ρυθμίσεις προστασίας του υπολογιστή στο στοιχείο **Υπολογιστής** σάς επιτρέπουν να ενεργοποιήσετε ή να απενεργοποιήσετε τα παρακάτω στοιχεία:

• **Προστασία συστήματος αρχείων σε πραγματικό χρόνο** – Σαρώνονται όλα τα αρχεία για κακόβουλο κώδικα όταν ανοίγουν, δημιουργούνται ή εκτελούνται.

• **Έλεγχος συνδεδεμένων συσκευών** – Η μονάδα αυτή σάς επιτρέπει να κάνετε σάρωση, αποκλεισμό ή ρύθμιση εκτεταμένων φίλτρων/δικαιωμάτων και να επιλέξετε τον τρόπο με τον οποίο ο χρήστης μπορεί να αποκτήσει πρόσβαση και να χρησιμοποιήσει μια συγκεκριμένη συσκευή (CD/DVD/USB...).

• **HIPS** – Το σύστημα HIPS παρακολουθεί τα συμβάντα μέσα στο λειτουργικό σύστημα και αντιδρά σε αυτά σύμφωνα με ένα προσαρμοσμένο σύνολο κανόνων.

• **Λειτουργία Gamer** – Ενεργοποιεί ή απενεργοποιεί τη Λειτουργία Gamer. Θα λάβετε ένα μήνυμα προειδοποίησης (για πιθανό κίνδυνο ασφαλείας) και, μετά την ενεργοποίηση της λειτουργίας Gamer, το χρώμα του κύριου παραθύρου θα μετατραπεί σε πορτοκαλί.

• **Προστασία κάμερας** – Ελέγχει τις διεργασίες και τις εφαρμογές που αποκτούν πρόσβαση στην κάμερα που είναι συνδεδεμένη με τον υπολογιστή.

Οι ρυθμίσεις στο στοιχείο **Προστασία διαδικτύου** σάς επιτρέπουν να ενεργοποιήσετε ή να απενεργοποιήσετε τα παρακάτω στοιχεία:

• **Προστασία πρόσβασης στο διαδίκτυο** – Εάν ενεργοποιηθεί, όλη η κυκλοφορία μέσω HTTP ή HTTPS σαρώνεται για κακόβουλο λογισμικό.

• **Προστασία προγράμματος-πελάτη email** – Παρακολουθεί την επικοινωνία που λαμβάνεται μέσω πρωτοκόλλου POP3(S) και IMAP(S).

• **Προστασία Antispam** – Σαρώνει ανεπιθύμητη ηλεκτρονική αλληλογραφία.

• **Προστασία Anti-Phishing** – Φιλτράρει ιστότοπους που είναι ύποπτοι για διανομή περιεχομένου που προορίζεται για να παραπλανήσει χρήστες, ώστε να υποβάλλουν εμπιστευτικές πληροφορίες.

Η ενότητα **Προστασία δικτύου** σάς επιτρέπει να ενεργοποιείτε ή να απενεργοποιείτε το Προσωπικό Firewall, την Προστασία επιθέσεων δικτύου (IDS) και την Προστασία botnet.

Η ρύθμιση **Εργαλεία ασφαλείας** σάς επιτρέπει να προσαρμόσετε τις ακόλουθες λειτουργικές μονάδες:

• **Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών** – Προσθέτει ένα επιπλέον επίπεδο προστασίας στο πρόγραμμα περιήγησης που έχει σχεδιαστεί για να προστατεύει τα οικονομικά δεδομένα σας κατά τη διάρκεια ηλεκτρονικών συναλλαγών. Ενεργοποιήστε το στοιχείο **Προστασία όλων των προγραμμάτων περιήγησης** ώστε όλα τα υποστηριζόμενα προγράμματα περιήγησης να εκκινούν σε ασφαλή λειτουργία. Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών.

• **Γονικός έλεγχος** – Η λειτουργική μονάδα Γονικός έλεγχος προστατεύει τα παιδιά σας αποτρέποντας ακατάλληλο ή επιβλαβές περιεχόμενο στο Internet.

• **Anti-Theft** – Ενεργοποιήστε το Anti-Theft για να προστατέψετε τον υπολογιστή σας σε περίπτωση απώλειας ή κλοπής.

Ο Γονικός έλεγχος σάς επιτρέπει να αποκλείετε ιστοσελίδες που ενδέχεται να περιέχουν ενδεχομένως προσβλητικό περιεχόμενο. Επιπλέον, οι γονείς μπορούν να εμποδίζουν την πρόσβαση σε περισσότερες από 40 προκαθορισμένες κατηγορίες ιστότοπων και περισσότερες από 140 υποκατηγορίες.

Για να ενεργοποιήσετε ξανά ένα απενεργοποιημένο στοιχείο ασφαλείας, κάντε κλικ στο ρυθμιστικό  ώστε να εμφανίζει ένα πράσινο σημάδι ελέγχου  .

> Όταν απενεργοποιείτε την προστασία με αυτή τη μέθοδο, όλες οι απενεργοποιημένες μονάδες προστασίας θα ενεργοποιηθούν μετά την επανεκκίνηση του υπολογιστή.

Διατίθενται πρόσθετες επιλογές στο κάτω μέρος του παραθύρου ρυθμίσεων. Χρησιμοποιήστε τον σύνδεσμο **Ρυθμίσεις για προχωρημένους** για να ρυθμίσετε πιο λεπτομερείς παραμέτρους για κάθε μονάδα. Χρησιμοποιήστε τις **Ρυθμίσεις εισαγωγής/εξαγωγής** για να φορτώσετε παραμέτρους ρυθμίσεων χρησιμοποιώντας ένα αρχείο διαμόρφωσης .xml ή για να αποθηκεύσετε τις τρέχουσες παραμέτρους ρυθμίσεων σε ένα αρχείο διαμόρφωσης.

Προστασία υπολογιστή

Κάντε κλικ στο στοιχείο **Προστασία υπολογιστή** από το παράθυρο **Ρυθμίσεις** για να δείτε μια επισκόπηση όλων των λειτουργικών μονάδων προστασίας.

- Προστασία συστήματος αρχείων σε πραγματικό χρόνο
- Έλεγχος συνδεδεμένων συσκευών
- Σύστημα αποτροπής απειλών με βάση (HIPS)
- Λειτουργία Gamer
- Προστασία web κάμερας

Για να διακόψετε προσωρινά ή να απενεργοποιήσετε μεμονωμένες λειτουργικές μονάδες προστασίας, κάντε κλικ στο εικονίδιο ρυθμιστικού  .

> Η απενεργοποίηση των λειτουργικών μονάδων προστασίας ενδέχεται να μειώσει το επίπεδο προστασίας του υπολογιστή σας.

Κάντε κλικ στο εικονίδιο γραναζιού ⚙ που βρίσκεται δίπλα σε μια λειτουργική μονάδα προστασίας, για να αποκτήσετε πρόσβαση στις ρυθμίσεις για προχωρημένους της συγκεκριμένης λειτουργικής μονάδας.

Για το στοιχείο **Προστασία συστήματος αρχείων σε πραγματικό χρόνο**, κάντε κλικ στο εικονίδιο γραναζιού ⚙ και επιλέξτε από τις ακόλουθες επιλογές:

- **Ρύθμιση παραμέτρων** – Ανοίγει την «Εγκατάσταση για προχωρημένους» του στοιχείου «Προστασία συστήματος αρχείων σε πραγματικό χρόνο».
- **Επεξεργασία εξαιρέσεων** – Ανοίγει το παράθυρο ρυθμίσεων «Εξαιρέσεις», ώστε να μπορείτε να εξαιρέσετε αρχεία και φακέλους από τη σάρωση.

Για το στοιχείο **Προστασία web κάμερας**, κάντε κλικ στο εικονίδιο γραναζιού ⚙ και επιλέξτε από

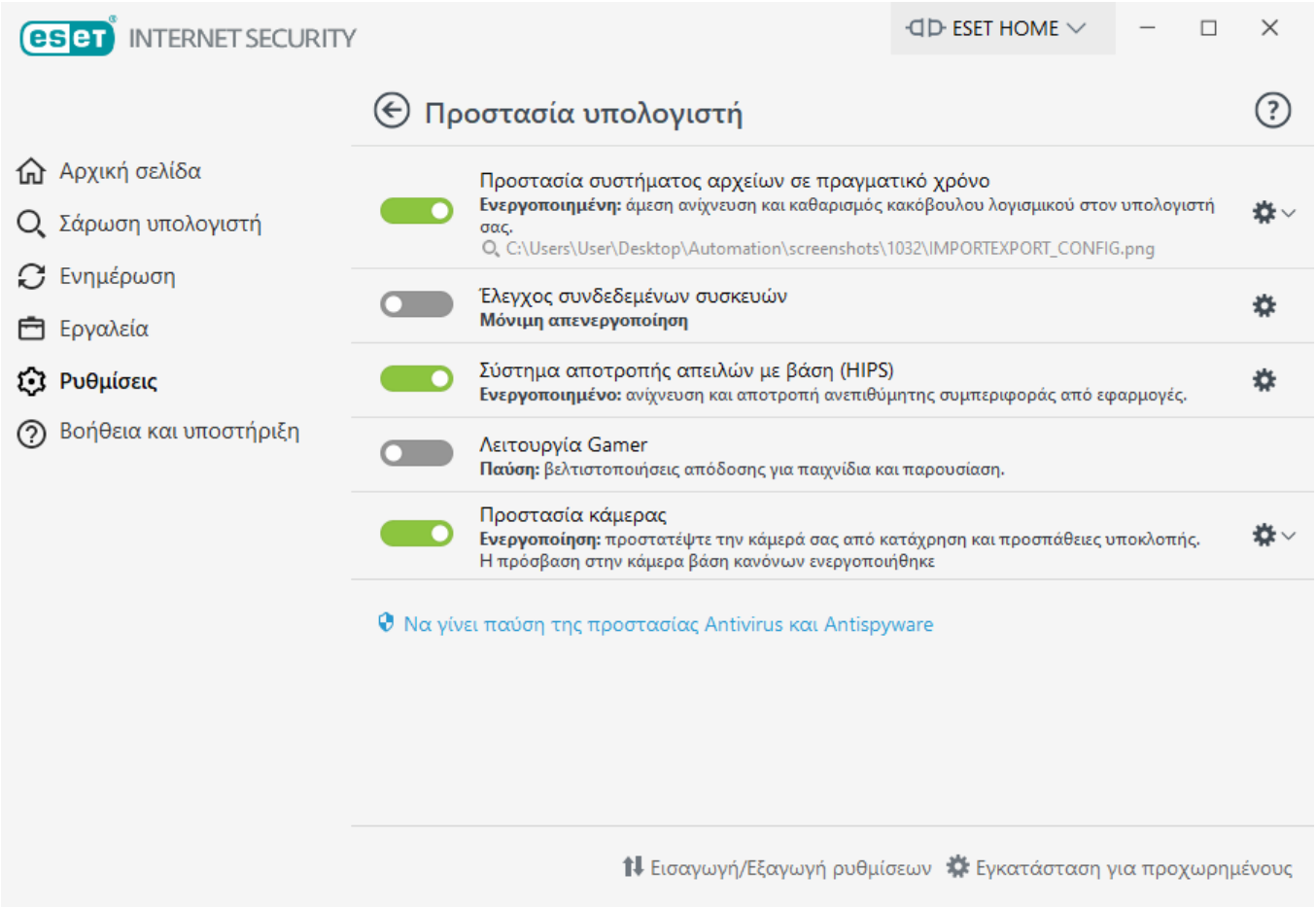
τις ακόλουθες επιλογές:

• **Ρύθμιση παραμέτρων** – Ανοίγει την «Εγκατάσταση για προχωρημένους» του στοιχείου «Προστασία web κάμερας».

• **Αποκλεισμός κάθε πρόσβασης μέχρι την επανεκκίνηση** – Αποκλείει κάθε πρόσβαση στην web κάμερα μέχρι την επανεκκίνηση του υπολογιστή.

• **Μόνιμος αποκλεισμός κάθε πρόσβασης** – Αποκλείει κάθε πρόσβαση στην web κάμερα μέχρι να απενεργοποιηθεί αυτή η ρύθμιση.

• **Διακοπή αποκλεισμού κάθε πρόσβασης** – Απενεργοποιεί τη δυνατότητα αποκλεισμού της πρόσβασης στην web κάμερα. Αυτή η επιλογή είναι διαθέσιμη μόνο εάν έχει αποκλειστεί η πρόσβαση στην web κάμερα.



Παύση προστασίας Antivirus και antispyware – Απενεργοποιεί όλες τις λειτουργικές μονάδες προστασίας antivirus και antispyware. Εάν απενεργοποιήσετε την προστασία, θα ανοίξει ένα παράθυρο στο οποίο θα μπορείτε να προσδιορίσετε το διάστημα απενεργοποίησης χρησιμοποιώντας το αναπτυσσόμενο μενού **Χρονικό διάστημα**. Αυτό θα πρέπει να χρησιμοποιείται μόνο από έμπειρους χρήστες ή με οδηγίες από την Τεχνική υποστήριξη της ESET.

Μηχανισμός ανίχνευσης:

Ο μηχανισμός ανίχνευσης προστατεύει από επιθέσεις κακόβουλου λογισμικού στο σύστημα ελέγχοντας την επικοινωνία των αρχείων, των email και του διαδικτύου. Για παράδειγμα, εάν ανιχνευτεί ένα αντικείμενο που ταξινομείται ως κακόβουλο λογισμικό, θα ξεκινήσει η αποκατάσταση.

Ο μηχανισμός ανίχνευσης μπορεί να το εξαλείψει πρώτα αποκλείοντάς το και μετά καθαρίζοντας, καταργώντας ή μετακινώντας το στην καραντίνα.

Για να ρυθμίσετε τις παραμέτρους του μηχανισμού ανίχνευσης λεπτομερώς, κάντε κλικ στο στοιχείο **Εγκατάσταση για προχωρημένους** ή πιέστε το πλήκτρο **F5**.

> ⚠ Οι αλλαγές στις ρυθμίσεις του μηχανισμού ανίχνευσης πρέπει να γίνονται μόνο από έμπειρο χρήστη. Η εσφαλμένη ρύθμιση παραμέτρων των ρυθμίσεων μπορεί να οδηγήσει σε μειωμένο επίπεδο προστασίας.

Σε αυτή την ενότητα:

Κατηγορίες Προστασίας πραγματικού χρόνου και εκμάθησης υπολογιστή

Η **Προστασία πραγματικού χρόνου και εκμάθησης υπολογιστή** για όλες τις λειτουργικές μονάδες (για παράδειγμα, Προστασία συστήματος αρχείων σε πραγματικό χρόνο, Προστασία πρόσβασης στο διαδίκτυο...) σάς επιτρέπει να ρυθμίσετε τις παραμέτρους των επιπέδων αναφοράς και προστασίας των ακόλουθων κατηγοριών:

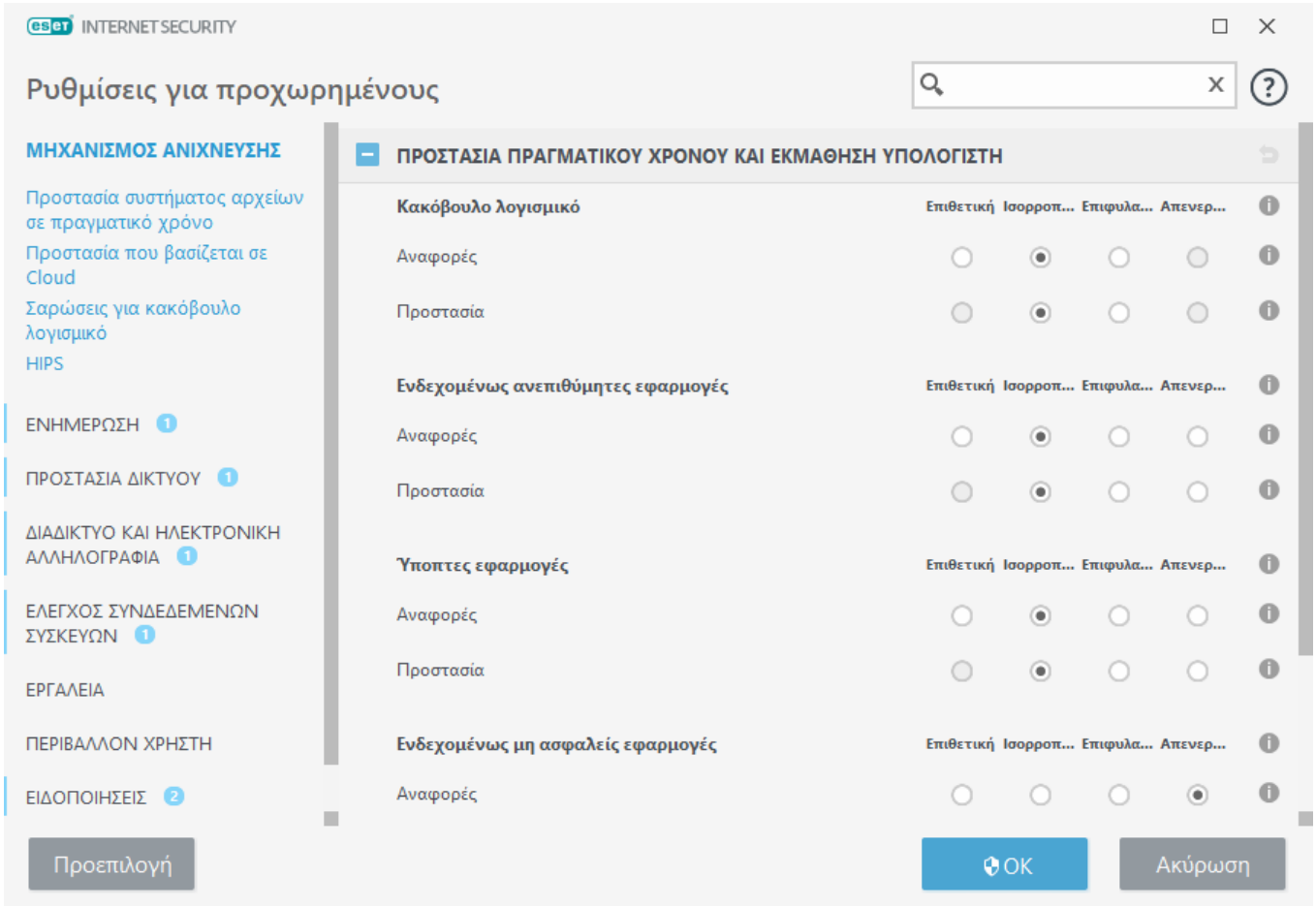
- **Κακόβουλο λογισμικό** – Ένας ιός υπολογιστή είναι ένα κομμάτι κακόβουλου κώδικα που προσυνάπτεται ή επισυνάπτεται σε υπάρχοντα αρχεία στον υπολογιστή σας. Ωστόσο, ο όρος «ιός» χρησιμοποιείται συχνά καταχρηστικά. Ο όρος «κακόβουλο λογισμικό» είναι πιο ακριβής. Ο εντοπισμός κακόβουλου λογισμικού εκτελείται από τη λειτουργική μονάδα μηχανισμού ανίχνευσης σε συνδυασμό με το στοιχείο εκμάθησης υπολογιστή. Διαβάστε περισσότερα για αυτούς τους τύπους εφαρμογών στο Γλωσσάρι.

- **Ενδεχομένως ανεπιθύμητες εφαρμογές** – Το Grayware ή ενδεχομένως ανεπιθύμητες εφαρμογές (PUA) είναι μια μεγάλη κατηγορία λογισμικού, ο σκοπός του οποίου δεν είναι αναμφίβολα κακόβουλος, όπως συμβαίνει με άλλους τύπους κακόβουλου λογισμικού, όπως οι ιοί και τα trojan horse. Ωστόσο, μπορεί να εγκαταστήσει πρόσθετο ανεπιθύμητο λογισμικό, να αλλάξει τη συμπεριφορά ή τις ρυθμίσεις της ψηφιακής συσκευής ή να εκτελέσει δραστηριότητες που δεν εγκρίνονται ή δεν αναμένονται από το χρήστη. Διαβάστε περισσότερα για αυτούς τους τύπους εφαρμογών στο Γλωσσάρι.

- Οι **ύποπτες εφαρμογές** περιλαμβάνουν προγράμματα που έχουν συμπιεστεί με προγράμματα συσκευασίας ή προστασίας. Αυτά τα προγράμματα προστασίας γίνονται συχνά αντικείμενο εκμετάλλευσης από δημιουργούς κακόβουλου λογισμικού για να αποφεύγουν την ανίχνευση.

- **Ενδεχομένως μη ασφαλείς εφαρμογές** – Αναφέρονται σε νόμιμο λογισμικό που διατίθεται στο εμπόριο το οποίο υπάρχει πιθανότητα να χρησιμοποιηθεί εσφαλμένα για κακόβουλους σκοπούς.

Παραδείγματα ενδεχομένως μη ασφαλών εφαρμογών (PUA) περιλαμβάνουν εργαλεία απομακρυσμένης πρόσβασης, εφαρμογές διάρρηξης κωδικών πρόσβασης και εφαρμογές καταγραφής πλήκτρων (προγράμματα που καταγράφουν κάθε πλήκτρο που πατάει ο χρήστης). Διαβάστε περισσότερα για αυτούς τους τύπους εφαρμογών στο Γλωσσάρι.



Βελτιωμένη προστασία

Η Προηγμένη εκμάθηση υπολογιστή είναι πλέον μέρος του μηχανισμού ανίχνευσης ως προηγμένο επίπεδο προστασίας που βελτιώνει την ανίχνευση με βάση την εκμάθηση υπολογιστή. Διαβάστε περισσότερα σχετικά με αυτό τον τύπο προστασίας στο Γλωσσάρι.

Σαρώσεις για κακόβουλο λογισμικό

Η ρύθμιση παραμέτρων των Ρυθμίσεων σάρωσης μπορεί να γίνει ξεχωριστά για τη σάρωση πραγματικού χρόνου και τη σάρωση κατ' απαίτηση. Από προεπιλογή, το στοιχείο **Χρήση ρυθμίσεων προστασίας πραγματικού χρόνου** είναι ενεργοποιημένη. Όταν είναι ενεργοποιημένη η ρύθμιση, οι σχετικές ρυθμίσεις σάρωσης κατ' απαίτηση μεταφέρονται από την ενότητα **Προστασία πραγματικού χρόνου και εκμάθησης υπολογιστή**. Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα σαρώσεις για κακόβουλο λογισμικό.

Ρύθμιση αναφορών

Όταν προκύψει μια ανίχνευση (π.χ. εάν εντοπιστεί μια απειλή και ταξινομηθεί ως κακόβουλο λογισμικό), οι πληροφορίες εγγράφονται στο Αρχείο καταγραφής ανιχνεύσεων και οι Ειδοποιήσεις επιφάνειας εργασίας εμφανίζονται εάν ρυθμιστούν οι παράμετροι στο ESET Internet Security.

Οι ρυθμίσεις παραμέτρων για το Κατώφλι αναφορών διαμορφώνονται για κάθε κατηγορία (αναφέρεται ως «ΚΑΤΗΓΟΡΙΑ»):

1. Κακόβουλο λογισμικό
2. Ενδεχομένως ανεπιθύμητες εφαρμογές
3. Ενδεχομένως μη ασφαλείς
4. Ύποπτες εφαρμογές

Οι αναφορές εκτελούνται με το μηχανισμό ανίχνευσης, συμπεριλαμβανομένου του στοιχείου εκμάθησης υπολογιστή. Είναι δυνατόν να ρυθμιστεί ένα υψηλότερο κατώφλι αναφοράς από το τρέχον κατώφλι προστασίας. Αυτές οι ρυθμίσεις αναφοράς δεν επηρεάζουν τον αποκλεισμό, τον καθαρισμό ή την κατάργηση αντικειμένων.

Διαβάστε τα ακόλουθα προτού τροποποιήσετε ένα κατώφλι (ή επίπεδο) για τις αναφορές «ΚΑΤΗΓΟΡΙΑ»:

Κατώφλι	Επεξήγηση
Επιθετική	Η ρύθμιση παραμέτρων των αναφορών για το στοιχείο ΚΑΤΗΓΟΡΙΑ έχει διαμορφωθεί στη μέγιστη ευαισθησία. Αναφέρονται περισσότερες ανιχνεύσεις. Η ρύθμιση **Επιθετική** μπορεί να αναγνωρίσει ψευδώς αντικείμενα ως ΚΑΤΗΓΟΡΙΑ.
Ισορροπημένη	Η ρύθμιση παραμέτρων των αναφορών για το στοιχείο ΚΑΤΗΓΟΡΙΑ έχει διαμορφωθεί ως ισορροπημένη. Αυτή η ρύθμιση έχει βελτιστοποιηθεί για να εξισορροπεί τις επιδόσεις και την ακρίβεια των ποσοστών ανίχνευσης και του αριθμού των ψευδώς αναφερόμενων αντικειμένων.
Επιφυλακτική	Η ρύθμιση παραμέτρων των αναφορών για το στοιχείο ΚΑΤΗΓΟΡΙΑ έχει διαμορφωθεί για ελαχιστοποίηση των ψευδώς ταυτοποιημένων αντικειμένων, διατηρώντας παράλληλα επαρκές επίπεδο προστασίας. Τα αντικείμενα αναφέρονται μόνο όταν η πιθανότητα είναι εμφανής και αντιστοιχεί στη συμπεριφορά ΚΑΤΗΓΟΡΙΑ.
Ανενεργή	Οι αναφορές για το στοιχείο ΚΑΤΗΓΟΡΙΑ δεν είναι ενεργές και οι ανιχνεύσεις αυτού του τύπου δεν εντοπίζονται, δεν αναφέρονται ή δεν καθαρίζονται. Ως αποτέλεσμα, αυτή η ρύθμιση απενεργοποιεί την προστασία από αυτό τον τύπο ανίχνευσης. Η απενεργοποίηση δεν είναι διαθέσιμη για την αναφορά κακόβουλου λογισμικού και είναι η προεπιλεγμένη τιμή για ενδεχομένως μη ασφαλείς εφαρμογές.

Διαθεσιμότητα των λειτουργικών μονάδων προστασίας του ESET Internet Security

Η διαθεσιμότητα (ενεργή ή ανενεργή) μιας λειτουργικής μονάδας προστασίας για ένα επιλεγμένο κατώφλι του στοιχείου ΚΑΤΗΓΟΡΙΑ είναι η εξής:

	Επιθετική	Ισορροπημένη	Επιφυλακτική	Ανενεργή**
Λειτουργική μονάδα προηγμένης εκμάθησης υπολογιστή*	✔ (επιθετική λειτουργία)	✔ (συντηρητική λειτουργία)	X	X
Λειτουργική μονάδα μηχανισμού ανίχνευσης	✔	✔	✔	X
Άλλες λειτουργικές μονάδες προστασίας	✔	✔	✔	X

* Διαθέσιμες στο ESET Internet Security έκδοση 13.1 και νεότερες εκδόσεις.
** Δεν συνιστάται

Προσδιορισμός της έκδοσης του προϊόντος, των εκδόσεων της λειτουργικής μονάδας προγράμματος και των ημερομηνιών δόμησης

1. Κάντε κλικ στο στοιχείο **Βοήθεια και υποστήριξη** > **Σχετικά με το ESET Internet Security**.

2. Στην οθόνη **Σχετικά**, η πρώτη γραμμή κειμένου εμφανίζει τον αριθμό έκδοσης του προϊόντος ESET.

3. Κάντε κλικ στο στοιχείο **Εγκατεστημένα στοιχεία** για να αποκτήσετε πρόσβαση στις πληροφορίες σχετικά με τις συγκεκριμένες λειτουργικές μονάδες.

Σημαντικά σημεία

Κάποια σημαντικά σημεία κατά τη ρύθμιση ενός κατάλληλου κατωφλίου για το περιβάλλον σας:

• Το κατώφλι **Ισορροπημένη** συνιστάται για τις περισσότερες ρυθμίσεις.

• Το κατώφλι **Επιφυλακτική** αντιπροσωπεύει ένα αντίστοιχο επίπεδο προστασίας με τις προηγούμενες εκδόσεις του ESET Internet Security (13.0 και παλαιότερες εκδόσεις). Αυτό συνιστάται για περιβάλλοντα όπου η προτεραιότητα εστιάζει στην ελαχιστοποίηση των ψευδώς ταυτοποιημένων αντικειμένων από το λογισμικό ασφαλείας.

• Όσο υψηλότερο είναι το κατώφλι αναφορών, τόσο υψηλότερο είναι το ποσοστό ανίχνευσης, αλλά και τόσο μεγαλύτερη είναι η πιθανότητα ψευδώς ταυτοποιημένων αντικειμένων.

• Από την άποψη του πραγματικού κόσμου, δεν υπάρχει εγγύηση ποσοστού ανίχνευσης 100% ούτε 0% πιθανότητα να αποφευχθεί η εσφαλμένη κατηγοριοποίηση των καθαρών αντικειμένων ως κακόβουλο λογισμικό.

• Διατηρείτε το ESET Internet Security και τις λειτουργικές μονάδες του ενημερωμένα για να μεγιστοποιήσετε την ισορροπία μεταξύ των επιδόσεων και της ακρίβειας των ποσοστών ανίχνευσης και του αριθμού ψευδώς ταυτοποιημένων αντικειμένων.

Ρύθμιση προστασίας

Εάν αναφερθεί ένα αντικείμενο που έχει ταξινομηθεί ως ΚΑΤΗΓΟΡΙΑ, το πρόγραμμα αποκλείει το αντικείμενο και, στη συνέχεια, το καθαρίζει, το καταργεί ή το μετακινεί στην Καραντίνα.

Διαβάστε τα ακόλουθα προτού τροποποιήσετε ένα κατώφλι (ή επίπεδο) για την προστασία «ΚΑΤΗΓΟΡΙΑ»:

Κατώφλι	Επεξήγηση
Επιθετική	Οι αναφερθείσες ανιχνεύσεις επιθετικού (ή χαμηλότερου) επιπέδου αποκλείονται και εκκινεί αυτόματη αποκατάσταση (δηλ. καθαρισμός). Αυτή η ρύθμιση συνιστάται όταν όλα τα τερματικά έχουν σαρωθεί με επιθετικές ρυθμίσεις και έχουν προστεθεί αντικείμενα με ψευδή αναφορά στις εξαιρέσεις ανίχνευσης.
Ισορροπημένη	Οι αναφερθείσες ανιχνεύσεις ισορροπημένου (ή χαμηλότερου) επιπέδου αποκλείονται και εκκινεί αυτόματη αποκατάσταση (δηλ. καθαρισμός).
Επιφυλακτική	Οι αναφερθείσες ανιχνεύσεις επιφυλακτικού επιπέδου αποκλείονται και εκκινεί αυτόματη αποκατάσταση (δηλ. καθαρισμός).
Ανενεργή	Αυτό είναι χρήσιμο για τον εντοπισμό και την εξαίρεση ψευδώς αναφερόμενων αντικειμένων. Η απενεργοποίηση δεν είναι διαθέσιμη για την προστασία από κακόβουλο λογισμικό και είναι η προεπιλεγμένη τιμή για ενδεχομένως μη ασφαλείς εφαρμογές.

Πίνακας μετατροπής για το ESET Internet Security 13.0 και παλαιότερες εκδόσεις

Κατά την αναβάθμιση από την έκδοση 13.0 και παλαιότερες εκδόσεις έως την έκδοση 13.1 και νεότερες εκδόσεις, η νέα κατάσταση κατωφλίου θα είναι η εξής:

Διακόπτης κατηγορίας πριν την αναβάθμιση		
Νέο κατώφλι για «ΚΑΤΗΓΟΡΙΑ» μετά την αναβάθμιση	Ισορροπημένη	Ανενεργή

Επιλογές για προχωρημένους του μηχανισμού ανίχνευσης

Η **τεχνολογία Anti-Stealth** είναι ένα πρωτοποριακό σύστημα που παρέχει ανίχνευση επικίνδυνων προγραμμάτων όπως rootkit, τα οποία είναι σε θέση να κρύβονται από το λειτουργικό σύστημα. Αυτό σημαίνει ότι δεν είναι δυνατή η ανίχνευσή τους χρησιμοποιώντας συνηθισμένες τεχνικές εξέτασης.

Ενεργοποίηση προηγμένης σάρωσης μέσω AMSI – Εργαλείο διασύνδεσης σάρωσης κακόβουλου λογισμικού της Microsoft που επιτρέπει στους προγραμματιστές της εφαρμογής να χρησιμοποιήσουν νέες άμυνες κατά του κακόβουλου λογισμικού (μόνο για Windows 10).

Ανιχνεύτηκε μια εισβολή

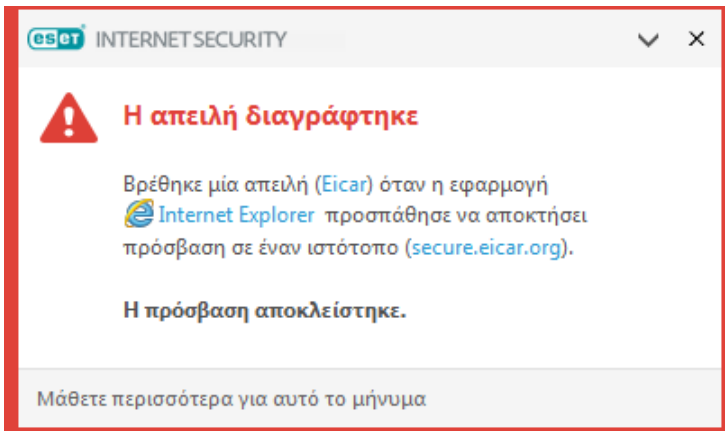
Οι εισβολές μπορούν να φτάσουν στο σύστημα από διάφορα σημεία εισόδου, όπως ιστοσελίδες, φακέλους κοινής χρήσης, μέσω ηλεκτρονικής αλληλογραφίας ή από αφαιρούμενες συσκευές (USB, εξωτερικοί δίσκοι, CD, DVD, κ.λπ.).

Τυπική συμπεριφορά

Ως γενικό παράδειγμα του χειρισμού των εισβολών από το ESET Internet Security, οι εισβολές μπορεί να ανιχνευτούν χρησιμοποιώντας τα παρακάτω:

- Προστασία συστήματος αρχείων σε πραγματικό χρόνο
- Προστασία πρόσβασης στο διαδίκτυο
- Προστασία ηλεκτρονικής αλληλογραφίας
- Σάρωση υπολογιστή κατ' απαίτηση

Κάθε τρόπος χρησιμοποιεί το τυπικό επίπεδο καθαρισμού και θα επιχειρήσει να καθαρίσει το αρχείο και να το μετακινήσει στην Καραντίνα ή να τερματίσει τη σύνδεση. Εμφανίζεται ένα παράθυρο ειδοποίησης στην περιοχή ειδοποιήσεων στην κάτω δεξιά γωνία της οθόνης. Για λεπτομερείς πληροφορίες σχετικά με τα ανιχνευμένα/καθαρισμένα αντικείμενα, ανατρέξτε στο θέμα Αρχεία καταγραφής. Για περισσότερες πληροφορίες σχετικά με τα επίπεδα καθαρισμού και τη συμπεριφορά, δείτε την ενότητα Επίπεδο καθαρισμού.



Σάρωση υπολογιστή για μολυσμένα αρχεία

Αν ο υπολογιστής σας παρουσιάζει ενδείξεις μόλυνσης από κακόβουλο λογισμικό, π.χ. είναι πιο αργός, συχνά «παγώνει», κ.λπ., συνιστάται να κάνετε τα ακόλουθα:

1.Ανοίξτε το ESET Internet Security και κάντε κλικ στη **Σάρωση υπολογιστή**.

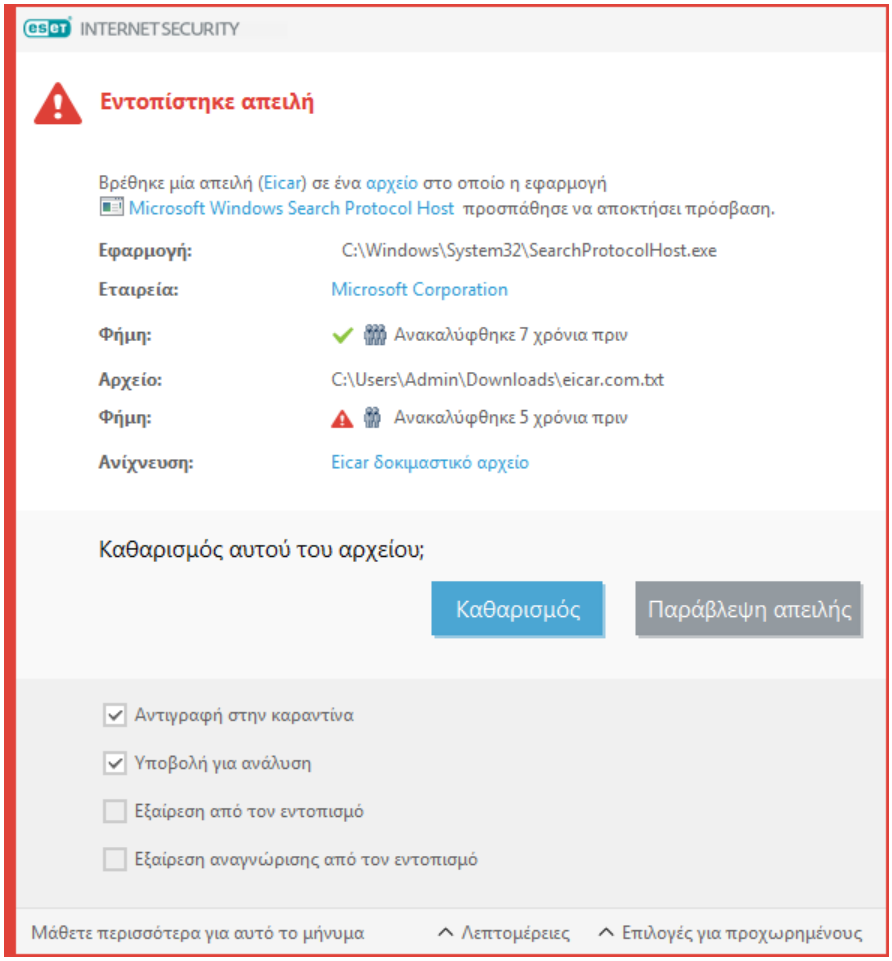
2.Κάντε κλικ στο στοιχείο **Σάρωση του υπολογιστή σας** (για περισσότερες πληροφορίες, δείτε την ενότητα Σάρωση υπολογιστή)

3.Όταν ολοκληρωθεί η σάρωση, κάντε μια ανασκόπηση στο αρχείο καταγραφής με τον αριθμό των σαρωμένων, μολυσμένων και καθαρισμένων αρχείων.

Αν επιθυμείτε να σαρώσετε μόνο ένα συγκεκριμένο μέρος του δίσκου σας, κάντε κλικ στην επιλογή **Προσαρμοσμένη σάρωση** και επιλέξτε τους προορισμούς που θέλετε να σαρωθούν για ιούς.

Καθαρισμός και διαγραφή

Αν δεν υπάρχει προκαθορισμένη ενέργεια που θα εκτελεστεί για την προστασία συστήματος αρχείων σε πραγματικό χρόνο, θα σας ζητηθεί να κάνετε μια επιλογή στο παράθυρο συναγερμού. Συνήθως είναι διαθέσιμες οι επιλογές **Καθαρισμός**, **Διαγραφή** και **Καμία ενέργεια**. Δεν συνιστάται να επιλέξετε **Καμία ενέργεια**, επειδή αυτό θα αφήσει τα μολυσμένα αρχεία χωρίς καθαρισμό. Η εξαίρεση σε αυτή τη σύσταση είναι όταν είστε βέβαιοι ότι ένα αρχείο είναι αβλαβές και ανιχνεύτηκε κατά λάθος.



Εφαρμόστε τον καθαρισμό αν ένα αρχείο έχει υποστεί επίθεση από έναν ιό και έχει επισυνάψει κακόβουλο κώδικα στο αρχείο. Αν συμβαίνει αυτό, προσπαθήστε πρώτα να καθαρίσετε το μολυσμένο αρχείο για να το επαναφέρετε στην αρχική του κατάσταση. Αν το αρχείο αποτελείται αποκλειστικά από κακόβουλο κώδικα, θα διαγραφεί.

Εάν ένα μολυσμένο αρχείο είναι «κλειδωμένο» ή χρησιμοποιείται από μια διεργασία του συστήματος, θα διαγράφεται συνήθως μόνο αφού αποδεσμευτεί (κανονικά μετά από επανεκκίνηση του συστήματος).

Επαναφορά από την καραντίνα

Η πρόσβαση στην καραντίνα είναι δυνατή από το κύριο παράθυρο του ESET Internet Security κάνοντας κλικ στα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Καραντίνα**.

Επίσης, μπορεί να γίνει επαναφορά των αρχείων που βρίσκονται στην καραντίνα στην αρχική τους θέση:

• Για αυτό το σκοπό, χρησιμοποιήστε τη δυνατότητα **Επαναφορά**, η οποία είναι διαθέσιμη από το μενού περιβάλλοντος, κάνοντας δεξί κλικ σε ένα συγκεκριμένο αρχείο που βρίσκεται στην Καραντίνα.

• Εάν ένα αρχείο έχει επισημανθεί ως ενδεχομένως ανεπιθύμητη εφαρμογή, ενεργοποιείται η επιλογή **Επαναφορά και εξαίρεση από τη σάρωση**. Ανατρέξτε επίσης στην ενότητα Εξαιρέσεις.

• Το μενού περιβάλλοντος προσφέρει επίσης την επιλογή **Επαναφορά σε**, η οποία σάς επιτρέπει να επαναφέρετε ένα αρχείο σε μια τοποθεσία διαφορετική από εκείνη από την οποία καταργήθηκε.

• Η λειτουργία επαναφοράς δεν είναι διαθέσιμη σε ορισμένες περιπτώσεις, για παράδειγμα, για αρχεία που βρίσκονται σε κοινόχρηστο δίκτυο με δικαίωμα μόνο για ανάγνωση.

Πολλαπλά νήματα

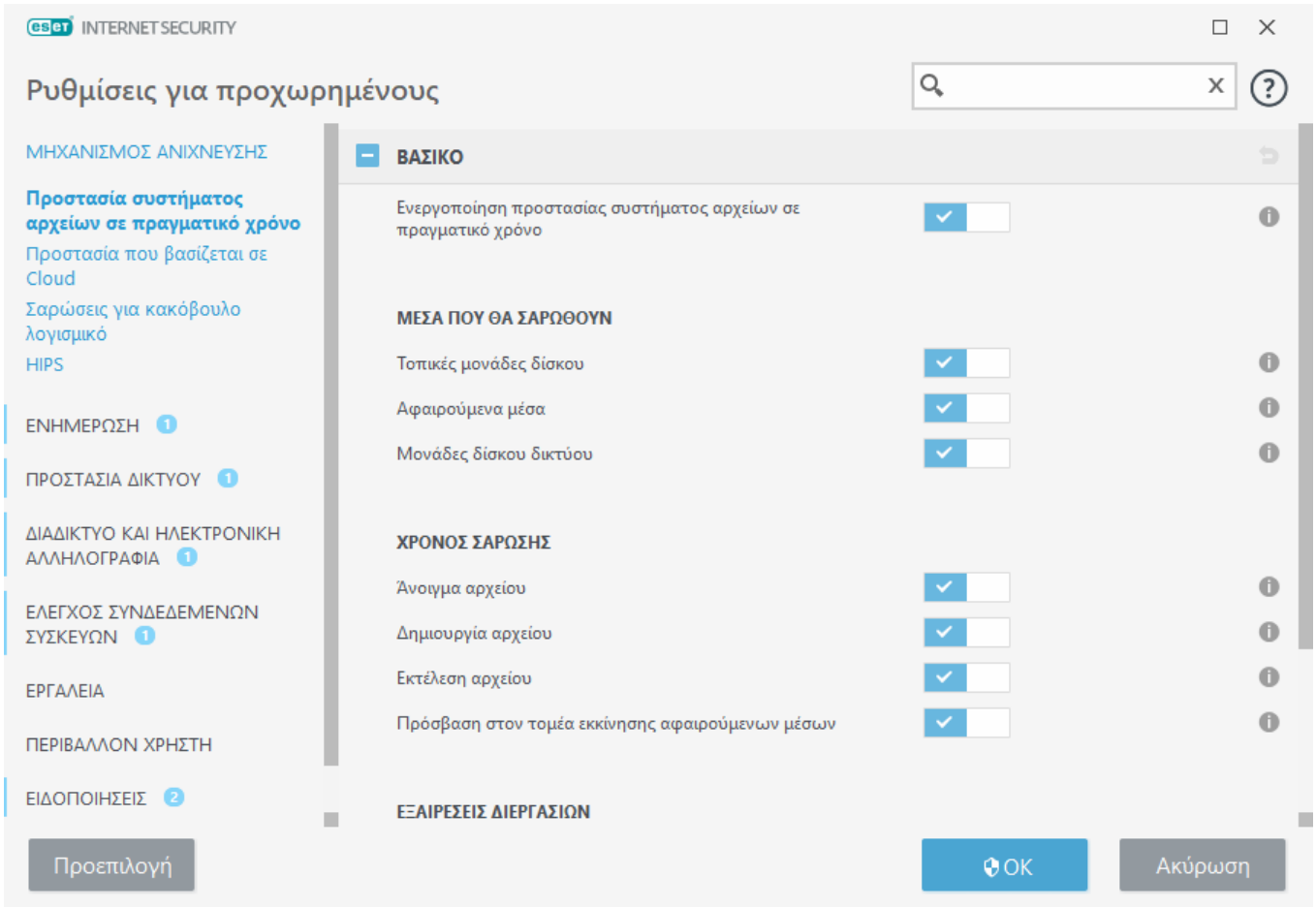
Αν κάποια μολυσμένα αρχεία δεν καθαρίστηκαν κατά τη Σάρωση υπολογιστή (ή το στοιχείο Επίπεδο καθαρισμού είχε οριστεί σε **Κανένας καθαρισμός**), θα εμφανιστεί ένα παράθυρο συναγερμού που σας ζητά να επιλέξετε ενέργειες για αυτά τα αρχεία. Επιλέξτε ενέργειες για τα αρχεία (οι ενέργειες ορίζονται ξεχωριστά για κάθε αρχείο στη λίστα) και στη συνέχεια κάντε κλικ στο **Τέλος**.

Διαγραφή αρχείων σε αρχειοθήκες

Στη λειτουργία Καθαρισμού προεπιλογής, θα διαγραφεί ολόκληρη η αρχειοθήκη μόνο αν περιέχει μολυσμένα αρχεία και κανένα καθαρό αρχείο. Με άλλα λόγια, οι αρχειοθήκες δεν διαγράφονται αν περιέχουν και αβλαβή καθαρά αρχεία. Απαιτείται προσοχή όταν εκτελείτε σάρωση Αυστηρού καθαρισμού. Όταν είναι ενεργοποιημένος ο Αυστηρός καθαρισμός, θα διαγραφεί μια αρχειοθήκη αν περιέχει τουλάχιστον ένα μολυσμένο αρχείο, ανεξάρτητα από την κατάσταση των άλλων αρχείων στην αρχειοθήκη.

Προστασία συστήματος αρχείων σε πραγματικό χρόνο

Η Προστασία συστήματος αρχείων σε πραγματικό χρόνο ελέγχει όλα τα αρχεία στο σύστημα για κακόβουλο κώδικα κατά το άνοιγμα, τη δημιουργία ή την εκτέλεση.



Από προεπιλογή, η προστασία συστήματος αρχείων σε πραγματικό χρόνο ξεκινά κατά την εκκίνηση του συστήματος και παρέχει αδιάλειπτη σάρωση. Δεν συνιστάται η απενεργοποίηση των στοιχείων **Ενεργοποίηση προστασίας συστήματος αρχείων σε πραγματικό χρόνο** στο στοιχείο **Εγκατάσταση για προχωρημένους**, στην διαδρομή **Μηχανισμός ανίχνευσης** > **Προστασία συστήματος αρχείων σε πραγματικό χρόνο** > **Βασικό**.

Μέσα που θα σαρωθούν

Από προεπιλογή, σαρώνονται όλοι οι τύποι μέσων για πιθανές απειλές:

- **Τοπικές μονάδες δίσκου** – Σαρώνει όλες τις μονάδες δίσκου του συστήματος και τις σταθερές μονάδες σκληρού δίσκου (παράδειγμα: *C:*\, *D:*\).
- **Αφαιρούμενα μέσα** – Σαρώνει CD/DVD, το χώρο αποθήκευσης USB, κάρτες μνήμης, κ.λπ.
- **Μονάδες δίσκου δικτύου** – Σαρώνει όλες τις χαρτογραφημένες μονάδες δίσκου δικτύου (παράδειγμα: *H:*\ ως *store04*) ή μονάδες δίσκου δικτύου απευθείας πρόσβασης (παράδειγμα: *store08*).

Συνιστάται να χρησιμοποιείτε τις προεπιλεγμένες ρυθμίσεις και να τις τροποποιείτε μόνο σε συγκεκριμένες περιπτώσεις, όπως όταν η σάρωση ορισμένων μέσων επιβραδύνει σημαντικά τις μεταφορές δεδομένων.

Χρόνος σάρωσης

Από προεπιλογή, όλα τα αρχεία σαρώνονται κατά το άνοιγμα, τη δημιουργία ή την εκτέλεση.

Συνιστάται να διατηρείτε αυτές τις προεπιλεγμένες ρυθμίσεις, επειδή παρέχουν το μέγιστο επίπεδο προστασίας σε πραγματικό χρόνο για τον υπολογιστή σας:

- **Άνοιγμα αρχείου** – Σαρώνει κατά το άνοιγμα ενός αρχείου.
- **Δημιουργία αρχείου** – Σαρώνει ένα αρχείο που δημιουργήθηκε ή τροποποιήθηκε.
- **Εκτέλεση αρχείου** – Σαρώνει κατά την εκτέλεση ή λειτουργία ενός αρχείου.
- **Πρόσβαση τομέα εκκίνησης αφαιρούμενου μέσου** – Εάν ένα αφαιρούμενο μέσο που περιέχει έναν τομέα εκκίνησης εισαχθεί στη συσκευή, ο τομέας εκκίνησης σαρώνεται αμέσως. Αυτή η επιλογή δεν επιτρέπει τη σάρωση αρχείων του αφαιρούμενου μέσου. Η σάρωση αρχείων του αφαιρούμενου μέσου βρίσκεται στη διαδρομή **Μέσα που θα σαρωθούν** > **Αφαιρούμενα μέσα**. Για να λειτουργήσει σωστά το στοιχείο **Πρόσβαση τομέα εκκίνησης αφαιρούμενου μέσου**, διατηρήστε ενεργό το στοιχείο **Τομείς εκκίνησης/UEFI** στις παραμέτρους ThreatSense.

Η προστασία συστήματος αρχείων σε πραγματικό χρόνο ελέγχει όλους τους τύπους μέσων και ενεργοποιείται από διάφορα συμβάντα συστήματος όπως η πρόσβαση σε ένα αρχείο. Με τη χρήση μεθόδων ανίχνευσης της τεχνολογίας ThreatSense (όπως περιγράφεται στην ενότητα Ρύθμιση παραμέτρων μηχανισμού ThreatSense), η προστασία συστήματος αρχείων σε πραγματικό χρόνο μπορεί να διαμορφωθεί ώστε να αντιμετωπίζει να αρχεία που έχουν δημιουργηθεί πρόσφατα διαφορετικά από ότι τα υπάρχοντα αρχεία. Για παράδειγμα, μπορείτε να διαμορφώσετε την προστασία συστήματος αρχείων σε πραγματικό χρόνο για να παρακολουθεί πιο στενά αρχεία που έχουν δημιουργηθεί πρόσφατα.

Για να διασφαλίζεται ελάχιστη κατανάλωση μνήμης συστήματος, τα αρχεία που έχουν ήδη σαρωθεί δεν σαρώνονται επανειλημμένως (παρά μόνο αν έχουν τροποποιηθεί). Τα αρχεία σαρώνονται πάλι αμέσως μετά από κάθε ενημέρωση του μηχανισμού ανίχνευσης. Για τον έλεγχο αυτής της συμπεριφοράς χρησιμοποιείται η λειτουργία **Έξυπνη βελτιστοποίηση**. Εάν απενεργοποιηθεί η **Έξυπνη βελτιστοποίηση**, σαρώνονται όλα τα αρχεία κάθε φορά που γίνεται πρόσβαση σε αυτά. Για να τροποποιήσετε αυτήν τη ρύθμιση, πιέστε **F5** για να ανοίξετε τις **Ρυθμίσεις για προχωρημένους** και αναπτύξτε το στοιχείο **Μηχανισμός ανίχνευσης** > **Προστασία συστήματος αρχείων σε πραγματικό χρόνο**. Κάντε κλικ στην επιλογή **Ρύθμιση παραμέτρων ThreatSense** > **Άλλα** και επιλέξτε ή καταργήστε την επιλογή **Ενεργοποίηση έξυπνης βελτιστοποίησης**.

Επίπεδα καθαρισμού

Για να αποκτήσετε πρόσβαση στις ρυθμίσεις επιπέδου καθαρισμού για τη λειτουργική μονάδα προστασίας που θέλετε, αναπτύξτε το στοιχείο **Παράμετροι ThreatSense** (για παράδειγμα, **Προστασία συστήματος αρχείων σε πραγματικό χρόνο**) και, στη συνέχεια, εντοπίστε τα στοιχεία **Καθαρισμός > Επίπεδο καθαρισμού**.

Οι παράμετροι ThreatSense έχουν τα ακόλουθα επίπεδα αποκατάστασης (π.χ. καθαρισμός).

Αποκατάσταση στο ESET Internet Security

Επίπεδο καθαρισμού	Περιγραφή
Πάντα αποκατάσταση ανίχνευσης	Προσπάθεια αποκατάστασης της ανίχνευσης κατά τον καθαρισμό αντικειμένων χωρίς παρέμβαση του τελικού χρήστη. Σε ορισμένες σπάνιες περιπτώσεις (για παράδειγμα, αρχεία συστήματος), εάν δεν είναι δυνατή η αποκατάσταση της ανίχνευσης, το αναφερόμενο αντικείμενο μένει στην αρχική του θέση.
Αποκατάσταση ανίχνευσης εάν είναι ασφαλές, διαφορετικά διατήρηση	Προσπάθεια αποκατάστασης της ανίχνευσης κατά τον καθαρισμό αντικειμένων χωρίς παρέμβαση του τελικού χρήστη. Σε ορισμένες περιπτώσεις (για παράδειγμα, αρχεία συστήματος ή αρχειοθήκες με καθαρά και μολυσμένα αρχεία), εάν δεν είναι δυνατή η αποκατάσταση μιας ανίχνευσης, το αναφερόμενο αντικείμενο μένει στην αρχική του θέση.
Αποκατάσταση ανίχνευσης εάν είναι ασφαλές, διαφορετικά ερώτηση	Προσπάθεια αποκατάστασης της ανίχνευσης κατά τον καθαρισμό αντικειμένων. Σε ορισμένες περιπτώσεις, εάν δεν είναι δυνατή η εκτέλεση οποιασδήποτε ενέργειας, ο τελικός χρήστης λαμβάνει έναν αλληλεπιδραστικό συναγερμό και πρέπει να επιλέξει μια ενέργεια αποκατάστασης (για παράδειγμα, κατάργηση ή παράλειψη). Αυτή η ρύθμιση συνιστάται στις περισσότερες περιπτώσεις.
Να ερωτάται πάντα ο τελικός χρήστης	Ο τελικός χρήστης λαμβάνει ένα αλληλεπιδραστικό παράθυρο κατά τον καθαρισμό αντικειμένων και πρέπει να επιλέξει μια ενέργεια αποκατάστασης (για παράδειγμα, κατάργηση ή παράβλεψη). Αυτό το επίπεδο έχει σχεδιαστεί για πιο προχωρημένους χρήστες που γνωρίζουν τα βήματα που πρέπει να ακολουθήσουν σε περίπτωση ανίχνευσης.

Πότε να τροποποιείτε τη διαμόρφωση ρυθμίσεων προστασίας συστήματος σε πραγματικό χρόνο

Η προστασία πραγματικού χρόνου είναι το πιο σημαντικό στοιχείο για τη διατήρηση ενός ασφαλούς συστήματος. Να είστε πάντοτε προσεκτικοί όταν τροποποιείτε τις παραμέτρους της. Συνιστούμε να τροποποιείτε τις παραμέτρους της μόνο σε ειδικές περιπτώσεις.

Μετά την εγκατάσταση του ESET Internet Security, όλες οι ρυθμίσεις βελτιστοποιούνται για να παρέχουν το μέγιστο επίπεδο ασφάλειας συστήματος για τους χρήστες. Για να επαναφέρετε τις προεπιλεγμένες ρυθμίσεις, κάντε κλικ στο εικονίδιο δίπλα σε κάθε καρτέλα στο παράθυρο (**Ρυθμίσεις για προχωρημένους** > **Μηχανισμός ανίχνευσης** > **Προστασία συστήματος αρχείων σε πραγματικό χρόνο**).

Έλεγχος προστασίας συστήματος σε πραγματικό χρόνο

Για να επαληθεύσετε ότι η προστασία σε πραγματικό χρόνο λειτουργεί και ανιχνεύει ιούς, χρησιμοποιήστε ένα δοκιμαστικό αρχείο από την *www.eicar.com*. Αυτό το δοκιμαστικό αρχείο είναι ένα αβλαβές αρχείο που μπορεί να ανιχνευτεί από όλα τα προγράμματα antivirus. Το αρχείο έχει δημιουργηθεί από την εταιρεία EICAR (European Institute for Computer Antivirus Research) για τον έλεγχο της λειτουργικότητας προγραμμάτων antivirus.

Το αρχείο είναι διαθέσιμο για λήψη στη διεύθυνση http://www.eicar.org/download/eicar.com
Αφού εισαγάγετε αυτή τη διεύθυνση URL στο πρόγραμμα περιήγησης, θα πρέπει να δείτε ένα μήνυμα ότι η απειλή καταργήθηκε.

Τι να κάνετε αν δεν λειτουργεί η προστασία συστήματος σε πραγματικό χρόνο

Σε αυτό το κεφάλαιο περιγράφουμε προβλήματα που ενδέχεται να προκύψουν όταν χρησιμοποιείτε προστασία πραγματικού χρόνου, καθώς και τον τρόπο με τον οποίο μπορείτε να τα αντιμετωπίσετε.

Η προστασία σε πραγματικό χρόνο είναι απενεργοποιημένη

Εάν ένας χρήστης απενεργοποιήσει κατά λάθος την προστασία πραγματικού χρόνου, θα πρέπει να ενεργοποιήσετε ξανά τη δυνατότητα. Για να ενεργοποιήσετε ξανά την προστασία πραγματικού χρόνου, μεταβείτε στο στοιχείο **Ρυθμίσεις** στο κύριο παράθυρο του προγράμματος και κάντε κλικ στα στοιχεία **Προστασία υπολογιστή** > **Προστασία συστήματος αρχείων σε πραγματικό χρόνο**.

Εάν η προστασία σε πραγματικό χρόνο δεν ενεργοποιείται κατά την εκκίνηση του συστήματος, αυτό συνήθως συμβαίνει επειδή το στοιχείο **Ενεργοποίηση προστασίας συστήματος αρχείων σε πραγματικό χρόνο** είναι απενεργοποιημένο. Για να διασφαλίσετε ότι αυτή η επιλογή είναι ενεργοποιημένη, μεταβείτε στις **Ρυθμίσεις για προχωρημένους** (**F5**) και κάντε κλικ στα στοιχεία **Μηχανισμός ανίχνευσης** > **Προστασία συστήματος αρχείων σε πραγματικό χρόνο**.

Εάν η προστασία σε πραγματικό χρόνο δεν πραγματοποιεί ανίχνευση και καθαρισμό εισβολών

Βεβαιωθείτε ότι δεν υπάρχουν εγκατεστημένα άλλα προγράμματα antivirus στον υπολογιστή σας. Εάν δυο προγράμματα antivirus είναι εγκατεστημένα ταυτόχρονα, ενδέχεται να έρθουν σε διένεξη μεταξύ τους. Συνιστούμε να καταργήσετε την εγκατάσταση κάθε άλλου προγράμματος antivirus από τον υπολογιστή σας προτού εγκαταστήσετε το προϊόν της ESET.

Η προστασία σε πραγματικό χρόνο δεν ξεκινά

Εάν η προστασία πραγματικού χρόνου δεν ενεργοποιείται κατά την εκκίνηση συστήματος (και η επιλογή **Ενεργοποίηση προστασίας συστήματος αρχείων σε πραγματικό χρόνο** είναι ενεργοποιημένη), αυτό ενδέχεται να οφείλεται σε διενέξεις με άλλα προγράμματα. Για να επιλύσετε το ζήτημα, δημιουργήστε ένα αρχείο καταγραφής SysInspector και υποβάλετέ το στην Τεχνική υποστήριξη της ESET για ανάλυση.

Εξαιρέσεις διεργασιών

Η δυνατότητα εξαιρέσεων διεργασιών σάς επιτρέπει να εξαιρείτε διεργασίες εφαρμογών από την προστασία συστήματος αρχείων σε πραγματικό χρόνο. Για τη βελτίωση της ταχύτητας στη δημιουργία αντιγράφων ασφαλείας, στην ακεραιότητα διεργασιών και στη διαθεσιμότητα υπηρεσίας, χρησιμοποιούνται κατά τη δημιουργία αντιγράφων ασφαλείας ορισμένες τεχνικές που είναι γνωστό ότι συγκρούονται με την προστασία κακόβουλου λογισμικού σε επίπεδο αρχείων. Ο μόνος

αποτελεσματικός τρόπος για να αποφευχθούν και οι δύο καταστάσεις είναι η απενεργοποίηση του λογισμικού κατά του κακόβουλου λογισμικού. Με την εξαίρεση μιας συγκεκριμένης διεργασίας (για παράδειγμα η διεργασία της λύσης δημιουργίας αντιγράφων ασφαλείας), όλες οι λειτουργίες αρχείου που αποδίδονται στη συγκεκριμένη εξαιρεθείσα διεργασία αγνοούνται και θεωρούνται ασφαλείς, ελαχιστοποιώντας έτσι την παρεμβολή με τη διεργασία δημιουργίας αντιγράφων ασφαλείας. Συνιστάται προσοχή κατά τη δημιουργία εξαιρέσεων – ένα εργαλείο δημιουργίας αντιγράφων ασφαλείας που έχει εξαιρεθεί μπορεί να αποκτήσει πρόσβαση σε μολυσμένα αρχεία χωρίς να ενεργοποιηθεί συναγερμός και για αυτό το λόγο τα εκτεταμένα δικαιώματα επιτρέπονται μόνο στη μονάδα προστασίας σε πραγματικό χρόνο.

Μη συγχέετε τα στοιχεία Εξαιρούμενες επεκτάσεις αρχείων, Εξαιρέσεις HIPS, Εξαιρέσεις ανιχνεύσεων ή Εξαιρέσεις επιδόσεων.

Οι εξαιρέσεις διεργασιών βοηθούν ώστε να ελαχιστοποιείται ο κίνδυνος δυνητικών συγκρούσεων και βελτιώνουν τις επιδόσεις των εφαρμογών που έχουν εξαιρεθεί. Αυτό με τη σειρά του έχει θετική επίδραση στις γενικές επιδόσεις και στη σταθερότητα του λειτουργικού συστήματος. Η εξαίρεση μιας διεργασίας / εφαρμογής είναι μια εξαίρεση του εκτελέσιμου αρχείου της (*.exe*).

Μπορείτε να προσθέσετε εκτελέσιμα αρχεία στη λίστα διεργασιών που εξαιρούνται μέσω της διαδρομής **Εγκατάσταση για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **Προστασία συστήματος αρχείων σε πραγματικό χρόνο** > **Εξαιρέσεις διεργασιών**.

Αυτή η λειτουργία σχεδιάστηκε για να εξαιρούνται τα εργαλεία δημιουργίας αντιγράφων ασφαλείας. Η εξαίρεση της διεργασίας δημιουργίας αντιγράφων ασφαλείας από τη σάρωση δεν διασφαλίζει μόνο τη σταθερότητα του συστήματος, αλλά επιπλέον δεν επηρεάζει τις επιδόσεις της δημιουργίας αντιγράφων ασφαλείας, επειδή η δημιουργία αντιγράφων ασφαλείας δεν επιβραδύνεται κατά την εκτέλεσή της.

Κάντε κλικ στο στοιχείο **Επεξεργασία** για να ανοίξετε το παράθυρο διαχείρισης **Εξαιρέσεις διεργασιών**, όπου μπορείτε να προσθέσετε εξαιρέσεις και να αναζητήσετε το εκτελέσιμο αρχείο (για παράδειγμα *Backup-tool.exe*), το οποίο θα εξαιρεθεί από τη σάρωση.
Μόλις προστεθεί το αρχείο *.exe* στις εξαιρέσεις, η δραστηριότητα αυτής της διεργασίας δεν θα παρακολουθείται από το ESET Internet Security και δεν θα εκτελείται σάρωση σε οποιεσδήποτε λειτουργίες αρχείων οι οποίες εκτελούνται από αυτή τη διεργασία.

Εάν δεν χρησιμοποιήσετε τη λειτουργία αναζήτησης κατά την επιλογή του εκτελέσιμου αρχείου της διεργασίας, θα πρέπει να εισαγάγετε μη αυτόματα μια πλήρη διαδρομή προς το εκτελέσιμο αρχείο. Διαφορετικά, η εξαίρεση δεν θα λειτουργήσει σωστά και το HIPS μπορεί να αναφέρει σφάλματα.

Επίσης, μπορείτε να **Επεξεργαστείτε** υπάρχουσες διεργασίες ή να τις **Καταργήσετε** από τις εξαιρέσεις.

Η προστασία πρόσβασης στο διαδίκτυο δεν λαμβάνει υπόψη αυτή την εξαίρεση, συνεπώς εάν εξαιρέσετε το εκτελέσιμο αρχείο του προγράμματος περιήγησης, τα ληφθέντα αρχεία θα εξακολουθούν να σαρώνονται. Με αυτό τον τρόπο μπορεί να ανιχνευτεί μια εισβολή. Αυτό το σενάριο αποτελεί μόνο ένα παράδειγμα και δεν συνιστάται να δημιουργήσετε εξαιρέσεις για τα προγράμματα περιήγησης.

Προσθήκη ή επεξεργασία εξαιρέσεων διεργασιών

Αυτό το παράθυρο διαλόγου σάς επιτρέπει να κάνετε **προσθήκη** διεργασιών που εξαιρούνται από το μηχανισμό ανίχνευσης. Οι εξαιρέσεις διεργασιών βοηθούν ώστε να ελαχιστοποιείται ο κίνδυνος δυνητικών συγκρούσεων και βελτιώνουν τις επιδόσεις των εφαρμογών που έχουν εξαιρεθεί. Αυτό με τη σειρά του έχει θετική επίδραση στις γενικές επιδόσεις και στη σταθερότητα του λειτουργικού συστήματος. Η εξαίρεση μιας διεργασίας / εφαρμογής είναι μια εξαίρεση του εκτελέσιμου αρχείου της (*.exe*).

Επιλέξτε τη διαδρομή αρχείου μιας εξαιρούμενης εφαρμογής κάνοντας κλικ στο ... (για παράδειγμα *C:\Program Files\Firefox\Firefox.exe*). ΜΗΝ εισαγάγετε το όνομα της εφαρμογής. Μόλις προστεθεί το αρχείο *.exe* στις εξαιρέσεις, η δραστηριότητα αυτής της διεργασίας δεν θα παρακολουθείται από το ESET Internet Security και δεν θα εκτελείται σάρωση σε οποιεσδήποτε λειτουργίες αρχείων οι οποίες εκτελούνται από αυτή τη διεργασία.

Εάν δεν χρησιμοποιήσετε τη λειτουργία αναζήτησης κατά την επιλογή του εκτελέσιμου αρχείου της διεργασίας, θα πρέπει να εισαγάγετε μη αυτόματα μια πλήρη διαδρομή προς το εκτελέσιμο αρχείο. Διαφορετικά, η εξαίρεση δεν θα λειτουργήσει σωστά και το HIPS μπορεί να αναφέρει σφάλματα.

Επίσης, μπορείτε να **Επεξεργαστείτε** υπάρχουσες διεργασίες ή να τις **Καταργήσετε** από τις εξαιρέσεις.

Προστασία βασισμένη σε cloud

Το ESET LiveGrid® (βασισμένο στο προηγμένο σύστημα έγκαιρης προειδοποίησης ESET ThreatSense.Net) αξιοποιεί δεδομένα που υποβάλλουν οι χρήστες της ESET σε όλο τον κόσμο και τα αποστέλλει στο Εργαστήριο ερευνών της ESET. Παρέχοντας ύποπτα δείγματα και μεταδεδομένα από το Διαδίκτυο, το ESET LiveGrid® μάς επιτρέπει να ανταποκρινόμαστε αμέσως στις ανάγκες των πελατών μας και ενημερώνει την ESET για τις πιο πρόσφατες απειλές.

Οι διαθέσιμες επιλογές είναι οι παρακάτω:

Ενεργοποιήστε το σύστημα φήμης ESET LiveGrid®

Το σύστημα φήμης ESET LiveGrid® παρέχει λίστα μη αποκλεισμένων διευθύνσεων και λίστα αποκλεισμένων διευθύνσεων που βασίζονται στο cloud.

Ελέγξτε τη φήμη των Εκτελούμενων διεργασιών και των αρχείων απευθείας από τη διασύνδεση του προγράμματος ή από το μενού περιβάλλοντος με πρόσθετες πληροφορίες που διατίθεται από το ESET LiveGrid®.

Ενεργοποιήστε το σύστημα σχολίων ESET LiveGrid®

Εκτός από το σύστημα φήμης ESET LiveGrid®, το σύστημα σχολίων ESET LiveGrid® θα συλλέγει πληροφορίες για τον υπολογιστή σας, οι οποίες σχετίζονται με απειλές που εντοπίστηκαν πρόσφατα. Οι πληροφορίες αυτές μπορεί να περιλαμβάνουν:

- Δείγμα ή αντίγραφο του αρχείου στο οποίο εμφανίστηκε η απειλή
- Τη διαδρομή προς το αρχείο
- Όνομα αρχείου
- Ημερομηνία και ώρα
- Τη διεργασία με την οποία εμφανίστηκε η απειλή στον υπολογιστή σας
- Πληροφορίες σχετικά με το λειτουργικό σύστημα του υπολογιστή σας

Από προεπιλογή, το ESET Internet Security είναι διαμορφωμένο ώστε να υποβάλλει ύποπτα αρχεία στο Εργαστήριο ιών της ESET για λεπτομερή ανάλυση. Αρχεία με ορισμένες επεκτάσεις όπως *.doc* ή *.xls* εξαιρούνται πάντα. Μπορείτε επίσης να προσθέσετε άλλες επεκτάσεις αν υπάρχουν συγκεκριμένα αρχεία των οποίων την αποστολή θέλετε, εσείς ή ο οργανισμός σας, να αποφύγετε.

Διαβάστε περισσότερα σχετικά με την αποστολή των σχετικών δεδομένων στην Πολιτική απορρήτου.

Μπορείτε να επιλέξτε να μην ενεργοποιήσετε το ESET LiveGrid®

Δεν θα χάσετε καμία λειτουργικότητα στο λογισμικό, αλλά σε ορισμένες περιπτώσεις, το ESET Internet Security ενδέχεται να αποκρίνεται πιο γρήγορα σε νέες απειλές εάν ενεργοποιηθεί το ESET LiveGrid®. Εάν έχετε χρησιμοποιήσει το ESET LiveGrid® προηγουμένως και το έχετε απενεργοποιήσει, ενδεχομένως να υπάρχουν ακόμα πακέτα δεδομένων για αποστολή. Ακόμη και μετά την απενεργοποίηση, αυτά τα πακέτα θα αποσταλούν στην ESET. Μόλις αποσταλούν όλες οι τρέχουσες πληροφορίες, δεν θα δημιουργηθούν άλλα πακέτα.

Διαβάστε περισσότερα για το ESET LiveGrid® στο γλωσσάρι.
Δείτε τις εικονογραφημένες οδηγίες που είναι διαθέσιμες στα Αγγλικά και αρκετές άλλες γλώσσες, για την ενεργοποίηση και απενεργοποίηση του ESET LiveGrid® στο ESET Internet Security.

Ρύθμιση παραμέτρων για την προστασία βασισμένη σε cloud στην Εγκατάσταση για προχωρημένους

Για να αποκτήσετε πρόσβαση στις ρυθμίσεις για το ESET LiveGrid®, ανοίξτε το στοιχείο **Εγκατάσταση για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **Προστασία που βασίζεται σε Cloud**.

- **Ενεργοποίηση του συστήματος φήμης ESET LiveGrid® (συνιστάται)** – Το σύστημα φήμης ESET LiveGrid® βελτιώνει την αποτελεσματικότητα των λύσεων της ESET για την προστασία από κακόβουλο λογισμικό, συγκρίνοντας σαρωμένα αρχεία σε μια βάση δεδομένων με λίστες αποκλεισμένων και λίστες μη αποκλεισμένων στοιχείων στο cloud.

- **Ενεργοποίηση του συστήματος σχολίων ESET LiveGrid®** – Αποστέλλει τα σχετικά δεδομένα υποβολής (περιγράφονται στην παρακάτω ενότητα **Υποβολής δειγμάτων**), μαζί με αναφορές τερματισμού λειτουργίας και στατιστικά στοιχεία, στο εργαστήριο της ESET για περαιτέρω ανάλυση.

• **Υποβολή αναφορών διακοπής λειτουργίας και διαγνωστικών δεδομένων** – Υποβολή δεδομένων διαγνωστικών ελέγχων που σχετίζονται με το ESET LiveGrid®, όπως αναφορές διακοπής λειτουργίας και αρχεία ένδειξης σφαλμάτων μνήμης των λειτουργικών μονάδων. Συνιστάται να παραμένει ενεργό για να βοηθά την ESET στη διάγνωση προβλημάτων, στη βελτίωση των προϊόντων και στη διασφάλιση της προστασίας του τελικού χρήστη.

• **Υποβολή ανώνυμων στατιστικών** – Επιτρέψτε στην ESET να συλλέγει πληροφορίες σχετικά με νέες ανιχνευμένες απειλές, όπως το όνομα της απειλής, την ημερομηνία και ώρα του εντοπισμού, τη μέθοδο ανίχνευσης και τα σχετικά μεταδεδομένα, την έκδοση και τη διαμόρφωση του προϊόντος, συμπεριλαμβανομένων πληροφοριών για το σύστημά σας.

• **Email επικοινωνίας (προαιρετικά)** – Το email επικοινωνίας σας μπορεί να συμπεριληφθεί μαζί με ύποπτα αρχεία και να χρησιμοποιηθεί για επικοινωνία μαζί σας, αν απαιτούνται περισσότερες πληροφορίες για την ανάλυση. Σημειώνεται ότι δεν θα λάβετε απάντηση από την ESET παρά μόνο αν απαιτούνται περισσότερες πληροφορίες.

Υποβολή δειγμάτων

Μη αυτόματη υποβολή δειγμάτων – Επιτρέπει την επιλογή μη αυτόματης υποβολής δειγμάτων στην ESET από το μενού περιβάλλοντος, Καραντίνα ή Εργαλεία.

Αυτόματη υποβολή ανιχνευμένων δειγμάτων

Επιλέξτε το είδος δειγμάτων που θα υποβληθούν στην ESET για ανάλυση και για βελτίωση της μελλοντικής ανίχνευσης (το προεπιλεγμένο μέγιστο μέγεθος δείγματος είναι 64MB). Οι διαθέσιμες επιλογές είναι οι παρακάτω:

• **Όλα τα ανιχνευμένα δείγματα** – Όλα τα αντικείμενα που ανιχνεύονται από τον Μηχανισμό ανίχνευσης (συμπεριλαμβανομένων ενδεχομένως ανεπιθύμητων εφαρμογών όταν έχουν ενεργοποιηθεί στις ρυθμίσεις σάρωσης).

• **Όλα τα δείγματα εκτός από έγγραφα** – Όλα τα ανιχνευμένα αντικείμενα εκτός από **Έγγραφα** (δείτε παρακάτω).

• **Να μην υποβάλλονται** – Τα ανιχνευμένα αντικείμενα δεν θα αποστέλλονται στην ESET.

Αυτόματη υποβολή ύποπτων δειγμάτων

Αυτά τα δείγματα θα αποστέλλονται επίσης στην ESET εάν δεν τα ανιχνεύσει ο μηχανισμός ανίχνευσης. Για παράδειγμα, τα δείγματα τα οποία παραλίγο να διαφύγουν την ανίχνευση ή τα οποία θεωρούνται από μία από τις λειτουργικές μονάδες προστασίας του ESET Internet Security ως ύποπτα ή έχουν ασαφή συμπεριφορά (το προεπιλεγμένο μέγιστο μέγεθος δείγματος είναι 64MB).

• **Εκτελέσιμα αρχεία** – Περιλαμβάνονται εκτελέσιμα αρχεία όπως .exe, .dll, .sys.

• **Αρχειοθήκες** – Περιλαμβάνονται τύποι αρχείων αρχειοθήκης όπως .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Δέσμες ενεργειών** – Περιλαμβάνονται τύποι αρχείων δέσμης ενεργειών όπως .bat, .cmd, .hta, .js, .vbs, .ps1.

• **Άλλα** – Περιλαμβάνονται τύποι αρχείων όπως .jar, .reg, .msi, .sfw, .lnk.

• **Πιθανώς ανεπιθύμητη αλληλογραφία** – Αυτή η ενέργεια θα επιτρέπει την αποστολή πιθανώς ανεπιθύμητων τμημάτων ή ολόκληρων πιθανώς ανεπιθύμητων μηνυμάτων ηλεκτρονικής αλληλογραφίας με επισύναψη στην ESET για περαιτέρω ανάλυση. Εάν ενεργοποιήσετε αυτή την επιλογή, θα βελτιωθεί ο γενικός εντοπισμός της ανεπιθύμητης αλληλογραφίας, συμπεριλαμβανομένων βελτιώσεων για μελλοντικό εντοπισμό της δικής σας ανεπιθύμητης αλληλογραφίας.

• **Έγγραφα** – Περιλαμβάνονται έγγραφα του Microsoft Office ή PDF με ή χωρίς ενεργό περιεχόμενο.

Ανάπτυξη για μια λίστα με όλους τους τύπους αρχείων εγγράφων που συμπεριλαμβάνονται

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

Εξαιρέσεις

Το φίλτρο «Εξαίρεση» σάς επιτρέπει να εξαιρείτε συγκεκριμένα αρχεία ή φακέλους από την υποβολή (για παράδειγμα, μπορεί να είναι χρήσιμο να εξαιρείτε αρχεία που περιέχουν εμπιστευτικές πληροφορίες, όπως έγγραφα ή υπολογιστικά φύλλα). Τα αρχεία που θα περιλαμβάνονται στην εξαίρεση δεν θα αποστέλλονται ποτέ στα εργαστήρια της ESET για ανάλυση, ακόμη κι αν περιέχουν ύποπτο κώδικα. Οι πιο συνηθισμένοι τύποι αρχείων εξαιρούνται από προεπιλογή (.doc κ.λπ.). Αν θέλετε, μπορείτε να προσθέστε στοιχεία στη λίστα εξαιρούμενων αρχείων.

Για να εξαιρέσετε αρχεία που έχουν ληφθεί από τη διεύθυνση `download.domain.com`, μεταβείτε στα στοιχεία **Εγκατάσταση για προχωρημένους** > **Μηχανισμός ανίχνευσης** > **Προστασία που βασίζεται σε cloud** > **Υποβολή δειγμάτων** και κάντε κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Εξαιρέσεις**. Προσθέστε την εξαίρεση `.download.domain.com`.

Μέγιστο μέγεθος δειγμάτων (MB) – Καθορίζει το μέγιστο μέγεθος των δειγμάτων (1-64 MB).

Φίλτρο εξαίρεσης για προστασία που βασίζεται σε cloud

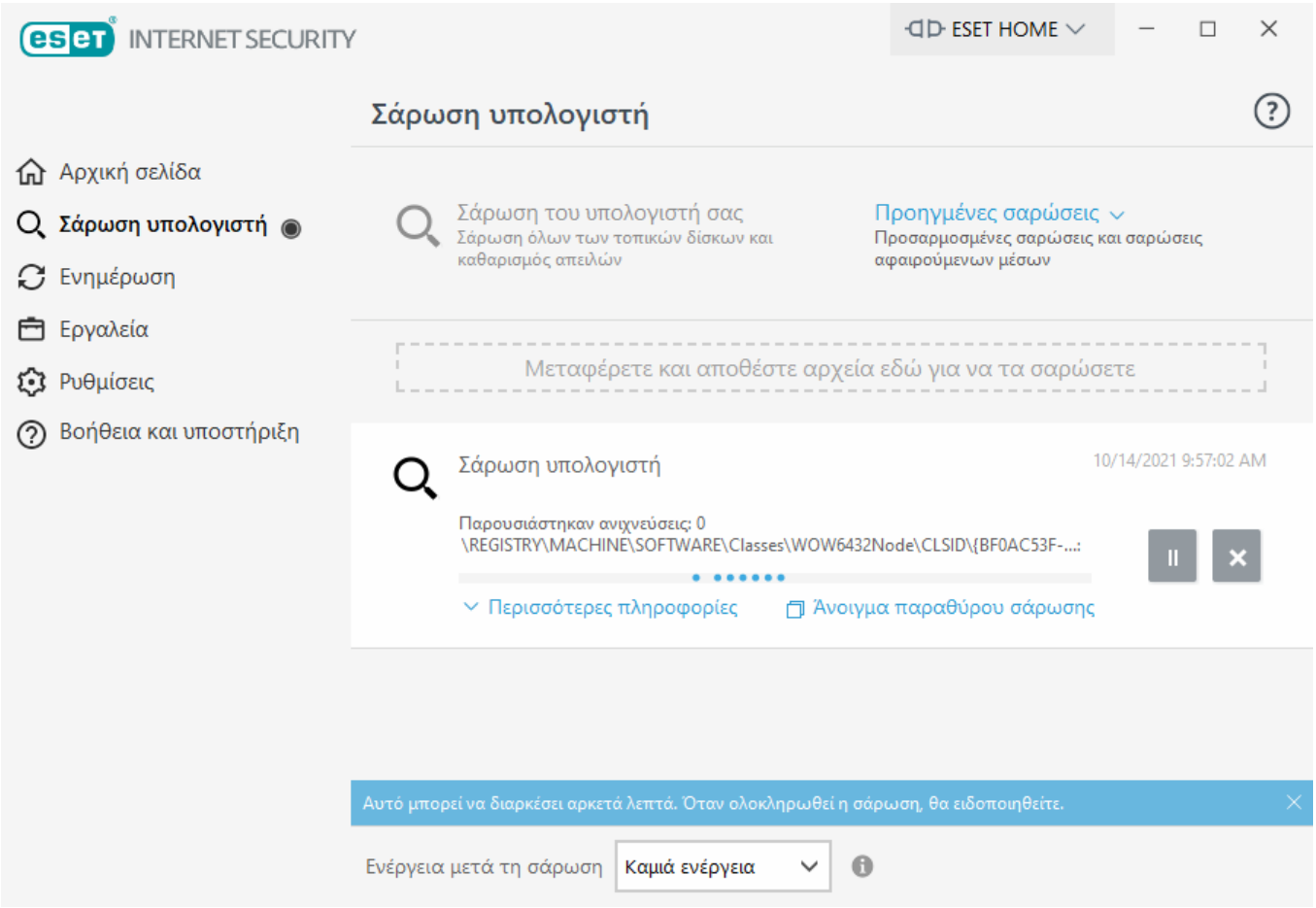
Το Φίλτρο εξαίρεσης σάς επιτρέπει να εξαιρείτε ορισμένα αρχεία ή φακέλους από την υποβολή δειγμάτων. Τα αρχεία που θα αναγράφονται δεν θα αποστέλλονται ποτέ στα εργαστήρια της ESET για ανάλυση, ακόμη κι αν περιέχουν ύποπτο κώδικα. Οι συνηθισμένοι τύποι αρχείων (όπως .doc κ.λπ.) εξαιρούνται από προεπιλογή.

Αυτή η δυνατότητα είναι χρήσιμη για να εξαιρείτε αρχεία που μπορεί να περιέχουν εμπιστευτικές πληροφορίες, όπως έγγραφα ή υπολογιστικά φύλλα.

Για να εξαιρέσετε αρχεία που έχουν ληφθεί από τη διεύθυνση download.domain.com, κάντε κλικ στο στοιχείο **Εγκατάσταση για προχωρημένους** > **Μηχανισμός ανίχνευσης** > **Προστασία που βασίζεται σε cloud** > **Υποβολή δειγμάτων** > **Εξαιρέσεις** και προσθέστε την εξαίρεση *download.domain.com*.

Σάρωση υπολογιστή

Η σάρωση κατ' απαίτηση είναι ένα σημαντικό μέρος της λύσης antivirus που διαθέτετε. Χρησιμοποιείται για την εκτέλεση σαρώσεων σε αρχεία και φακέλους στον υπολογιστή σας. Από άποψη ασφάλειας, είναι απαραίτητο οι σαρώσεις υπολογιστή να εκτελούνται τακτικά και να αποτελούν μέρος των συνηθισμένων μέτρων ασφαλείας, και να μην εκτελούνται μόνο όταν υπάρχει υποψία μόλυνσης. Συνιστάται να εκτελείτε τακτικά σαρώσεις σε βάθος του συστήματός σας για να ανιχνεύονται ιοί που δεν συλλαμβάνονται από την Προστασία συστήματος αρχείων σε πραγματικό χρόνο όταν εγγράφονται στο δίσκο. Αυτό μπορεί να συμβεί εάν η Προστασία συστήματος αρχείων σε πραγματικό χρόνο είναι απενεργοποιημένη εκείνη τη στιγμή, εάν ο μηχανισμός ανίχνευσης είναι παλιός ή εάν το αρχείο δεν ανιχνεύεται ως ιός κατά την αποθήκευσή του στο δίσκο.



Η **Σάρωση υπολογιστή** διατίθεται σε δύο τύπους. Το στοιχείο **Σάρωση του υπολογιστή σας** σαρώνει γρήγορα το σύστημα χωρίς τον καθορισμό παραμέτρων σάρωσης. Το στοιχείο **Προσαρμοσμένη σάρωση** (στην ενότητα «Προηγμένη σάρωση») σάς επιτρέπει να επιλέξετε από προκαθορισμένα προφίλ σάρωσης, που είναι σχεδιασμένα να στοχεύουν συγκεκριμένες τοποθεσίες, και να επιλέγετε συγκεκριμένους προορισμούς σάρωσης.

Δείτε την ενότητα Εξέλιξη σάρωσης για περισσότερες πληροφορίες σχετικά με τη διεργασία σάρωσης.

Από προεπιλογή, το ESET Internet Security επιχειρεί να καθαρίσει ή να καταργήσει αυτόματα τις ανιχνεύσεις που εντοπίστηκαν κατά τη σάρωση υπολογιστή. Σε ορισμένες περιπτώσεις, εάν δεν είναι δυνατή η εκτέλεση καμίας ενέργειας, θα λάβετε έναν αλληλεπιδραστικό συναγερμό και θα πρέπει να επιλέξετε μια ενέργεια καθαρισμού (για παράδειγμα, κατάργηση ή παράβλεψη). Για να αλλάξετε το επίπεδο καθαρισμού και για πιο λεπτομερείς πληροφορίες, ανατρέξτε στο θέμα Καθαρισμός. Για να ελέγξετε προηγούμενες σαρώσεις, ανατρέξτε στο θέμα Αρχεία καταγραφής.

Σάρωση του υπολογιστή σας

Η «**Σάρωση του υπολογιστή σας**» σάς επιτρέπει να ξεκινήσετε γρήγορα μια σάρωση υπολογιστή και να καθαρίσετε μολυσμένα αρχεία χωρίς να χρειάζεται παρέμβαση του χρήστη. Το πλεονέκτημα της επιλογής «**Σάρωση του υπολογιστή σας**» είναι ότι είναι εύκολη στη λειτουργία και δεν απαιτεί λεπτομερή διαμόρφωση σάρωσης. Αυτή η σάρωση ελέγχει όλα τα αρχεία στις τοπικές μονάδες δίσκου και καθαρίζει ή διαγράφει αυτόματα τις μολυσμένες εισβολές. Το επίπεδο καθαρισμού ρυθμίζεται αυτόματα στην προεπιλεγμένη τιμή. Για πιο λεπτομερείς πληροφορίες για τους τύπους καθαρισμού, δείτε την ενότητα Καθαρισμός.

Επίσης, μπορείτε να χρησιμοποιήσετε τη δυνατότητα **Μεταφορά και απόθεση** για να σαρώσετε ένα αρχείο ή φάκελο μη αυτόματα, κάνοντας κλικ στο αρχείο ή στο φάκελο, μετακινώντας το δείκτη του ποντικιού στην επισημασμένη περιοχή, ενώ κρατάτε πατημένο το κουμπί του ποντικιού και ελευθερώνοντάς το στη συνέχεια. Μετά από αυτό, η εφαρμογή μετακινείται στο προσκήνιο.

Οι ακόλουθες επιλογές σάρωσης είναι διαθέσιμες στην ενότητα **Προηγμένες σαρώσεις**:

Προσαρμοσμένη σάρωση

Το στοιχείο **Προσαρμοσμένη σάρωση** σάς επιτρέπει να καθορίσετε τις παραμέτρους σάρωσης, όπως προορισμούς και μεθόδους σάρωσης. Το πλεονέκτημα του στοιχείου **Προσαρμοσμένη σάρωση** είναι ότι μπορείτε να ρυθμίσετε τις παραμέτρους λεπτομερώς. Οι ρυθμίσεις παραμέτρων μπορούν να αποθηκευτούν σε προφίλ σάρωσης που καθορίζονται από το χρήστη, κάτι που μπορεί να είναι χρήσιμο αν η σάρωση εκτελείται επανειλημμένα με τις ίδιες παραμέτρους.

Σάρωση αφαιρούμενων μέσων

Παρόμοια με τη «**Σάρωση του υπολογιστή σας**» – ξεκινά γρήγορα μια σάρωση στα αφαιρούμενα μέσα (όπως CD/DVD/USB) που είναι συνδεδεμένα εκείνη τη στιγμή στον υπολογιστή. Αυτό μπορεί να είναι χρήσιμο όταν συνδέετε μια μονάδα USB flash σε έναν υπολογιστή και θέλετε να κάνετε σάρωση στο περιεχόμενό της για κακόβουλο λογισμικό και άλλες πιθανές απειλές.

Μπορείτε να ξεκινήσετε αυτόν τον τύπο σάρωσης επίσης κάνοντας κλικ στο στοιχείο **Προσαρμοσμένη σάρωση**, επιλέγοντας **Αφαιρούμενα μέσα** από το αναπτυσσόμενο μενού **Προορισμοί σάρωσης** και κάνοντας κλικ στο στοιχείο **Σάρωση**.

Επανάληψη τελευταίαας σάρωσης

Σάς επιτρέπει να ξεκινήσετε γρήγορα τη σάρωση που πραγματοποιήσατε προηγουμένως, χρησιμοποιώντας τις ίδιες ρυθμίσεις.

Το αναπτυσσόμενο μενού **Ενέργεια μετά τη σάρωση** σάς επιτρέπει να ρυθμίσετε μια ενέργεια που

θα εκτελείται αυτόματα μετά την ολοκλήρωση μιας σάρωσης:

• **Καμιά ενέργεια** – Μετά την ολοκλήρωση της σάρωσης δεν θα πραγματοποιηθεί καμιά ενέργεια.

• **Τερματισμός λειτουργίας** – Η λειτουργία του υπολογιστή τερματίζεται όταν ολοκληρωθεί η σάρωση.

• **Επανεκκίνηση** – Κλείνει όλα τα ανοιχτά προγράμματα και επανεκκινεί τον υπολογιστή όταν ολοκληρωθεί η σάρωση.

• **Επανεκκίνηση εάν απαιτείται** - Ο υπολογιστής πραγματοποιεί επανεκκίνηση μόνο εάν απαιτείται για να ολοκληρωθεί ο καθαρισμός των ανιχνευμένων απειλών.

• **Επιβολή επανεκκίνησης** - Επιβάλει το κλείσιμο όλων των ανοιχτών προγραμμάτων χωρίς να περιμένει την αλληλεπίδραση του χρήστη και επανεκκινεί τον υπολογιστή μετά την ολοκλήρωση μιας σάρωσης.

• **Επιβολή επανεκκίνησης, εάν χρειάζεται** - Ο υπολογιστής πραγματοποιεί επανεκκίνηση μόνο εάν απαιτείται για να ολοκληρωθεί ο καθαρισμός των ανιχνευμένων απειλών.

• **Αναστολή λειτουργίας** – Αποθηκεύει την περίοδο λειτουργίας σας και θέτει τον υπολογιστή σε κατάσταση χαμηλής κατανάλωσης, έτσι ώστε να μπορείτε γρήγορα να συνεχίσετε την εργασία σας.

• **Αδρανοποίηση** – Αποτυπώνει οτιδήποτε εκτελείται στη μνήμη RAM και το μετακινεί σε ένα ειδικό αρχείο στον σκληρό δίσκο. Η λειτουργία του υπολογιστή τερματίζεται, αλλά θα συνεχίσει από την προηγούμενη κατάσταση την επόμενη φορά που θα τον ξεκινήσετε.

Οι ενέργειες **Αναστολή λειτουργίας** ή **Αδρανοποίηση** είναι διαθέσιμες ανάλογα με τις ρυθμίσεις του λειτουργικού συστήματος «Ενέργεια και αναστολή λειτουργίας» ή τις δυνατότητες του υπολογιστή/φορητού υπολογιστή σας. Έχετε υπόψη ότι, ακόμη και σε κατάσταση αναστολής λειτουργίας, ο υπολογιστής εξακολουθεί να λειτουργεί. Συνεχίζει να εκτελεί βασικές λειτουργίες και να καταναλώνει ρεύμα όταν τροφοδοτείται με μπαταρία. Για να εξοικονομήσετε τη διάρκεια ζωής της μπαταρίας, για παράδειγμα όταν ταξιδεύετε μακριά από το γραφείο, συνιστάται να χρησιμοποιείτε την επιλογή «Αδρανοποίηση».

Η επιλεγμένη ενέργεια θα ξεκινήσει αφού ολοκληρωθούν όλες οι σαρώσεις που εκτελούνται. Εάν επιλέξετε **Τερματισμός λειτουργίας** ή **Επανεκκίνηση**, θα εμφανιστεί αντίστροφη μέτρηση 30 δευτερολέπτων σε ένα παράθυρο επιβεβαίωσης (κάντε κλικ στο στοιχείο **Ακύρωση** για να απενεργοποιήσετε την ενέργεια που ζητήθηκε).

Συνιστάται να εκτελείτε μια σάρωση υπολογιστή τουλάχιστον μία φορά το μήνα. Η σάρωση μπορεί να διαμορφωθεί ως προγραμματισμένη εργασία από τη διαδρομή **Εργαλεία** > **Περισσότερα εργαλεία** > **Προγραμματισμός εργασιών**. Πώς μπορώ να προγραμματίσω μια εβδομαδιαία εργασία σάρωσης;

Πρόγραμμα εκκίνησης προσαρμοσμένης

σάρωσης

Μπορείτε να χρησιμοποιήσετε την Προσαρμοσμένη σάρωση για να σαρώσετε τη λειτουργική μνήμη, το δίκτυο ή συγκεκριμένα μέρη ενός δίσκου, αντί για ολόκληρο το δίσκο. Για να το κάνετε αυτό, επιλέξτε **Προηγμένες σαρώσεις** > **Προσαρμοσμένη σάρωση** επιλέξτε συγκεκριμένους προορισμούς από τη δομή φακέλων (δέντρο).

Μπορείτε να επιλέξετε ένα προφίλ από το αναπτυσσόμενο μενού **Προφίλ** που θα χρησιμοποιείται κατά τη σάρωση συγκεκριμένων προορισμών. Το προεπιλεγμένο προφίλ είναι η **Έξυπνη σάρωση**. Υπάρχουν τρία ακόμα προκαθορισμένα προφίλ σάρωσης που ονομάζονται **Σάρωση σε βάθος Σάρωση μενού περιβάλλοντος** και **Σάρωση υπολογιστή**. Αυτά τα προφίλ σάρωσης χρησιμοποιούν διαφορετικές παραμέτρους ThreatSense. Οι διαθέσιμες επιλογές περιγράφονται στη διαδρομή **Εγκατάσταση για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **Σαρώσεις για κακόβουλο λογισμικό** > **Σάρωση κατ' απαίτηση** > Παράμετροι ThreatSense.

Η δομή φακέλων (δέντρου) περιέχει επίσης συγκεκριμένους προορισμούς σάρωσης.

- **Λειτουργική μνήμη** – Σαρώνει όλες τις διεργασίες και τα δεδομένα που χρησιμοποιούνται αυτή τη στιγμή από τη λειτουργική μνήμη.

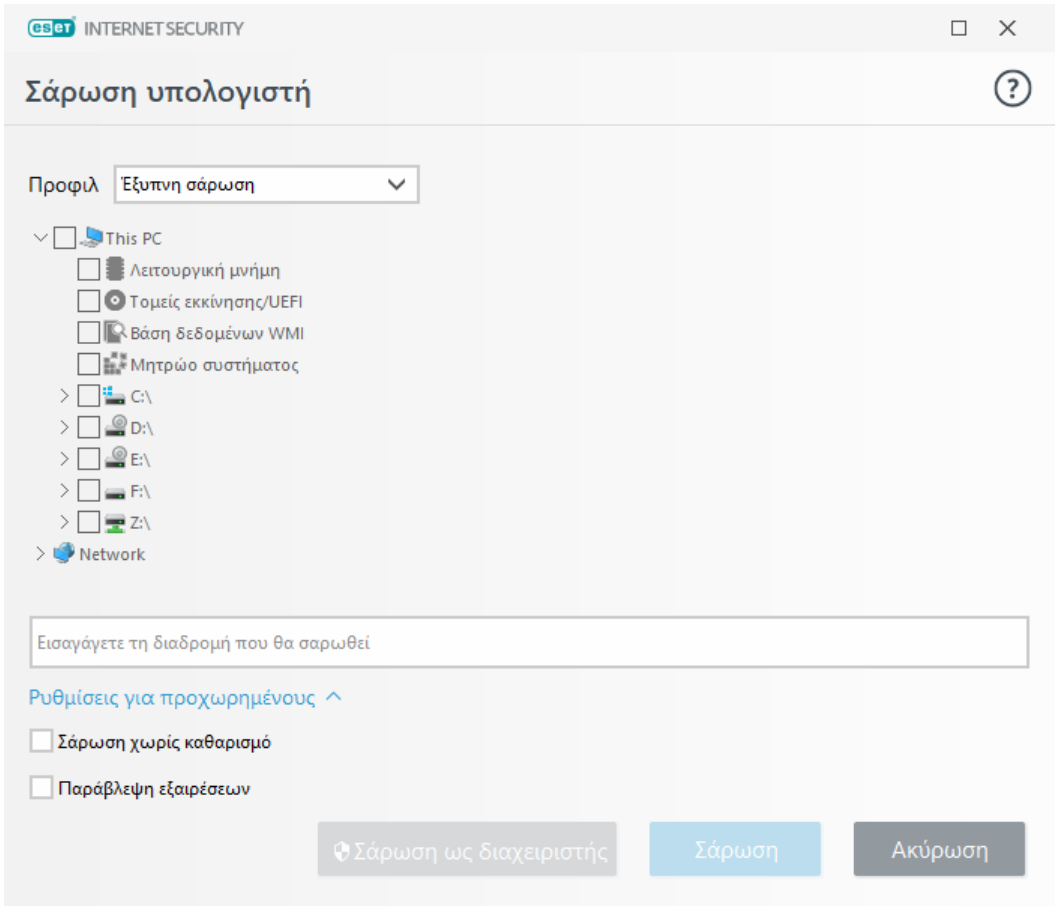
- **Τομείς εκκίνησης/UEFI** – Σαρώνει τους τομείς εκκίνησης και UEFI για την παρουσία κακόβουλου λογισμικού. Διαβάστε περισσότερα σχετικά με το Εργαλείο σάρωσης UEFI στο γλωσσάρι.

- **Βάση δεδομένων WMI** – Σαρώνει ολόκληρη τη βάση δεδομένων Windows Management Instrumentation WMI, όλους τους χώρους ονομάτων, όλες τις παρουσίες κλάσεων και όλες τις ιδιότητες. Αναζητά αναφορές σε μολυσμένα αρχεία ή κακόβουλο λογισμικό που είναι ενσωματωμένα ως δεδομένα.

- **Μητρώο συστήματος** – Σαρώνει ολόκληρο το μητρώο συστήματος, όλα τα κλειδιά και τα δευτερεύοντα κλειδιά. Αναζητά αναφορές σε μολυσμένα αρχεία ή κακόβουλο λογισμικό που είναι ενσωματωμένα ως δεδομένα. Κατά τον καθαρισμό των ανιχνεύσεων, η αναφορά παραμένει στο μητρώο για να διασφαλίζεται ότι δεν θα χαθούν σημαντικά δεδομένα.

Για να μεταβείτε γρήγορα σε έναν προορισμό σάρωσης (αρχείο ή φάκελο), πληκτρολογήστε τη διαδρομή του στο πεδίο κειμένου κάτω από τη δομή δέντρου. Στη διαδρομή γίνεται διάκριση πεζών-κεφαλαίων. Για να συμπεριλάβετε τον προορισμό στη σάρωση, επιλέξτε το πλαίσιο ελέγχου του στη δομή δέντρου.

> **Πώς να προγραμματίσετε μια εβδομαδιαία εργασία σάρωσης**
> Για να προγραμματίσετε μια τακτική εργασία, διαβάστε το κεφάλαιο Πώς να προγραμματίσετε μια εβδομαδιαία εργασία σάρωσης υπολογιστή.



Μπορείτε να ρυθμίσετε τις παραμέτρους καθαρισμού για τη σάρωση στην ενότητα **Ρυθμίσεις για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **Σάρωση κατ' απαίτηση** > **Παράμετροι του ThreatSense** > **Καθαρισμός**. Για να εκτελέσετε μια σάρωση χωρίς καμία ενέργεια καθαρισμού, κάντε κλικ στο στοιχείο **Ρυθμίσεις για προχωρημένους** και επιλέξτε **Σάρωση χωρίς καθαρισμό**. Το ιστορικό σάρωσης αποθηκεύεται στο αρχείο καταγραφής σάρωσης.

Όταν είναι επιλεγμένο το στοιχείο **Παράβλεψη εξαιρέσεων**, τα αρχεία με επεκτάσεις που εξαιρούνταν προηγουμένως θα σαρώνονται χωρίς εξαίρεση.

Κάντε κλικ στη **Σάρωση** για να εκτελέσετε τη σάρωση χρησιμοποιώντας τις προσαρμοσμένες παραμέτρους που έχετε ορίσει.

Η **Σάρωση ως διαχειριστής** σάς επιτρέπει να εκτελέσετε τη σάρωση από τον λογαριασμό του Διαχειριστή. Χρησιμοποιήστε αυτή την επιλογή, αν ο τρέχων χρήστης δεν έχει δικαιώματα πρόσβασης στα αρχεία που θέλετε να σαρωθούν. Αυτό το κουμπί δεν είναι διαθέσιμο αν ο τρέχων χρήστης δεν μπορεί να δώσει εντολή για λειτουργίες UAC ως Διαχειριστής.

Μπορείτε να δείτε το αρχείο καταγραφής σάρωσης υπολογιστή μετά την ολοκλήρωση μιας σάρωσης κάνοντας κλικ στο Εμφάνιση αρχείου καταγραφής.

Εξέλιξη σάρωσης

Το παράθυρο εξέλιξης σάρωσης εμφανίζει την τρέχουσα κατάσταση της σάρωσης και πληροφορίες για τον αριθμό αρχείων που βρέθηκε ότι περιέχουν κακόβουλο κώδικα.

Είναι φυσιολογικό να μην μπορούν να σαρωθούν ορισμένα αρχεία, όπως αρχεία που προστατεύονται με κωδικό πρόσβασης ή αρχεία που χρησιμοποιούνται αποκλειστικά από το σύστημα (συνήθως αρχεία *pagefile.sys* και ορισμένα αρχεία καταγραφής). Για περισσότερες λεπτομέρειες, ανατρέξτε σε αυτό το άρθρο της Γνωσιακής βάσης.

Πώς να προγραμματίσετε μια εβδομαδιαία εργασία σάρωσης

Για να προγραμματίσετε μια τακτική εργασία, διαβάστε το κεφάλαιο Πώς να προγραμματίσετε μια εβδομαδιαία εργασία σάρωσης υπολογιστή.

Γραμμή προόδου – Η γραμμή προόδου εμφανίζει την κατάσταση των αντικειμένων που έχουν ήδη σαρωθεί σε σύγκριση με αντικείμενα που αναμένουν ακόμα σάρωση. Η κατάσταση προόδου σάρωσης προκύπτει από τον συνολικό αριθμό αντικειμένων που περιλαμβάνονται σε μια σάρωση.

Προορισμός – Το όνομα του αντικειμένου που σαρώνεται αυτήν τη στιγμή και η τοποθεσία του.

Βρέθηκαν απειλές – Εμφανίζει τον συνολικό αριθμό σαρωμένων αρχείων, τις απειλές που βρέθηκαν και τις απειλές που καθαρίστηκαν κατά τη διάρκεια μιας σάρωσης.

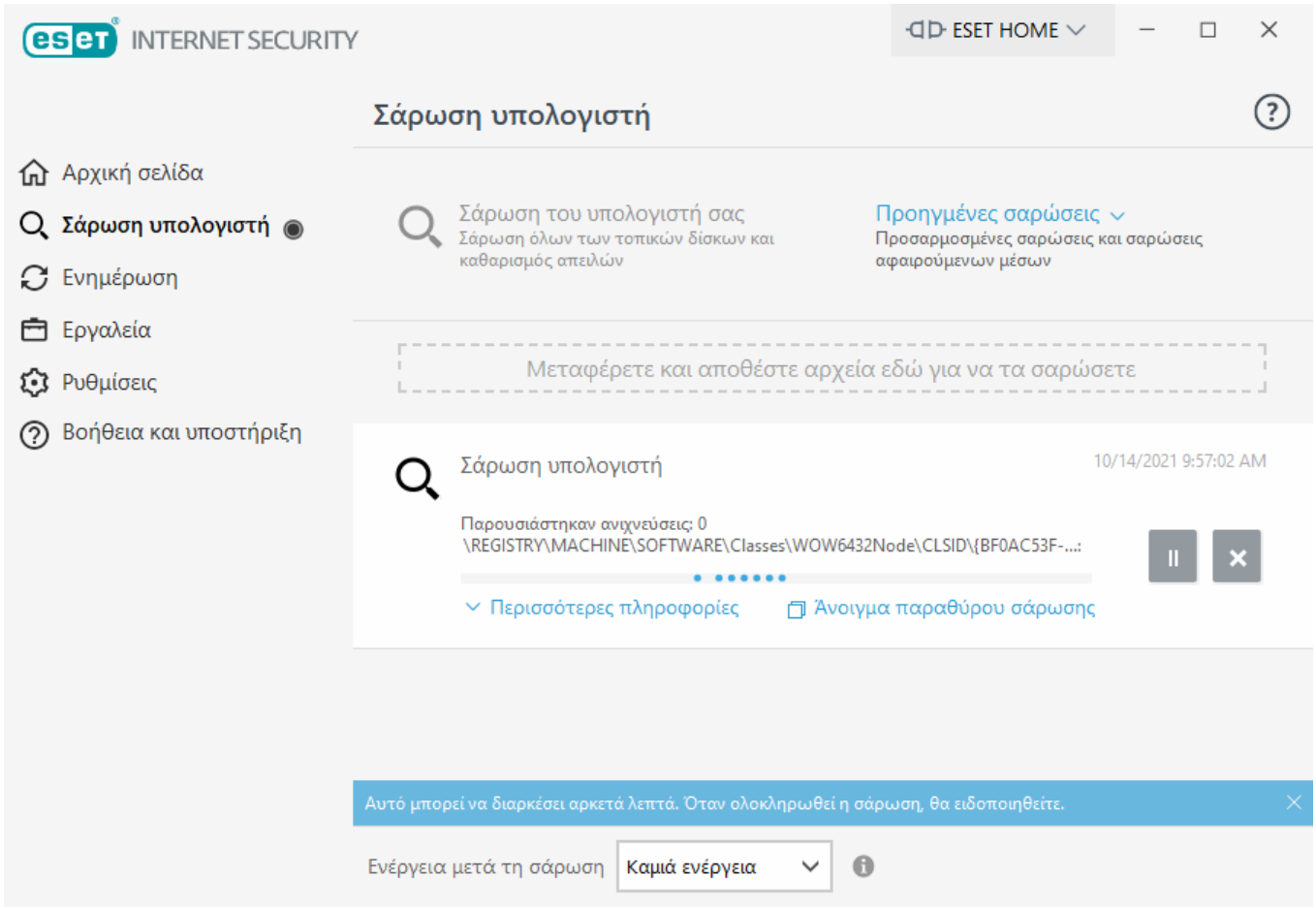
Παύση – Διακόπτει προσωρινά μια σάρωση.

Συνέχιση – Αυτή η επιλογή είναι ορατή όταν έχει γίνει παύση της σάρωσης. Κάντε κλικ στο κουμπί **Συνέχιση** για να συνεχίσετε τη σάρωση.

Διακοπή – Τερματίζει τη σάρωση.

Κύλιση αρχείου καταγραφής σάρωσης – Εάν ενεργοποιήσετε αυτή την επιλογή, το αρχείο καταγραφής σάρωσης θα πραγματοποιεί αυτόματη κύλιση καθώς προστίθενται νέες καταχωρίσεις, έτσι ώστε να εμφανίζονται οι πιο πρόσφατες καταχωρίσεις.

Κάντε κλικ στον μεγεθυντικό φακό ή στο βέλος για να εμφανιστούν λεπτομέρειες για τη σάρωση που εκτελείται αυτή τη στιγμή. Μπορείτε να εκτελέσετε και άλλη παράλληλη σάρωση κάνοντας κλικ στο στοιχείο **Σάρωση του υπολογιστή σας** ή **Προηγμένες σαρώσεις** > **Προσαρμοσμένη σάρωση**.



Το αναπτυσσόμενο μενού **Ενέργεια μετά τη σάρωση** σάς επιτρέπει να ρυθμίσετε μια ενέργεια που θα εκτελείται αυτόματα μετά την ολοκλήρωση μιας σάρωσης:

• **Καμιά ενέργεια** – Μετά την ολοκλήρωση της σάρωσης δεν θα πραγματοποιηθεί καμιά ενέργεια.

• **Τερματισμός λειτουργίας** – Η λειτουργία του υπολογιστή τερματίζεται όταν ολοκληρωθεί η σάρωση.

• **Επανεκκίνηση** – Κλείνει όλα τα ανοιχτά προγράμματα και επανεκκινεί τον υπολογιστή όταν ολοκληρωθεί η σάρωση.

• **Επανεκκίνηση εάν απαιτείται** - Ο υπολογιστής πραγματοποιεί επανεκκίνηση μόνο εάν απαιτείται για να ολοκληρωθεί ο καθαρισμός των ανιχνευμένων απειλών.

• **Επιβολή επανεκκίνησης** - Επιβάλει το κλείσιμο όλων των ανοιχτών προγραμμάτων χωρίς να περιμένει την αλληλεπίδραση του χρήστη και επανεκκινεί τον υπολογιστή μετά την ολοκλήρωση μιας σάρωσης.

• **Επιβολή επανεκκίνησης, εάν χρειάζεται** - Ο υπολογιστής πραγματοποιεί επανεκκίνηση μόνο εάν απαιτείται για να ολοκληρωθεί ο καθαρισμός των ανιχνευμένων απειλών.

• **Αναστολή λειτουργίας** – Αποθηκεύει την περίοδο λειτουργίας σας και θέτει τον υπολογιστή σε κατάσταση χαμηλής κατανάλωσης, έτσι ώστε να μπορείτε γρήγορα να συνεχίσετε την εργασία σας.

• **Αδρανοποίηση** – Αποτυπώνει οτιδήποτε εκτελείται στη μνήμη RAM και το μετακινεί σε ένα

ειδικό αρχείο στον σκληρό δίσκο. Η λειτουργία του υπολογιστή τερματίζεται, αλλά θα συνεχίσει από την προηγούμενη κατάσταση την επόμενη φορά που θα τον ξεκινήσετε.

Οι ενέργειες **Αναστολή λειτουργίας** ή **Αδρανοποίηση** είναι διαθέσιμες ανάλογα με τις ρυθμίσεις του λειτουργικού συστήματος «Ενέργεια και αναστολή λειτουργίας» ή τις δυνατότητες του υπολογιστή/φορητού υπολογιστή σας. Έχετε υπόψη ότι, ακόμη και σε κατάσταση αναστολής λειτουργίας, ο υπολογιστής εξακολουθεί να λειτουργεί. Συνεχίζει να εκτελεί βασικές λειτουργίες και να καταναλώνει ρεύμα όταν τροφοδοτείται με μπαταρία. Για να εξοικονομήσετε τη διάρκεια ζωής της μπαταρίας, για παράδειγμα όταν ταξιδεύετε μακριά από το γραφείο, συνιστάται να χρησιμοποιείτε την επιλογή «Αδρανοποίηση».

Η επιλεγμένη ενέργεια θα ξεκινήσει αφού ολοκληρωθούν όλες οι σαρώσεις που εκτελούνται. Εάν επιλέξετε **Τερματισμός λειτουργίας** ή **Επανεκκίνηση**, θα εμφανιστεί αντίστροφη μέτρηση 30 δευτερολέπτων σε ένα παράθυρο επιβεβαίωσης (κάντε κλικ στο στοιχείο **Ακύρωση** για να απενεργοποιήσετε την ενέργεια που ζητήθηκε).

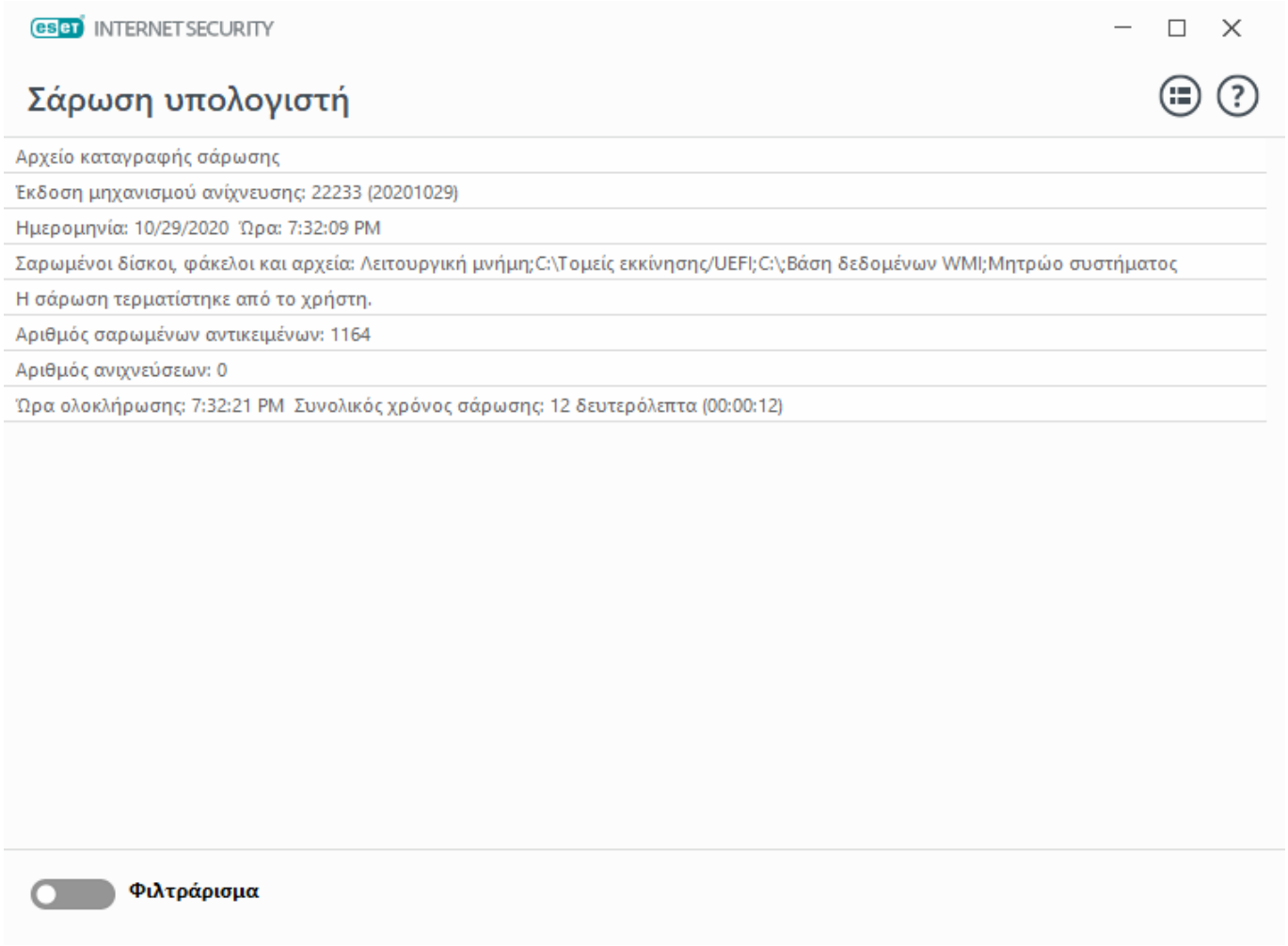
Αρχείο καταγραφής σάρωσης υπολογιστή

Όταν ολοκληρωθεί η σάρωση, ανοίγει το Αρχείο καταγραφής σάρωσης υπολογιστή με όλες τις σχετικές πληροφορίες που αφορούν τη συγκεκριμένη σάρωση. Το αρχείο καταγραφής σάρωσης παρέχει πληροφορίες όπως:

- Έκδοση μηχανισμού ανίχνευσης
- Ημερομηνία και ώρα έναρξης
- Λίστα σαρωμένων δίσκων, φακέλων και αρχείων
- Όνομα προγραμματισμένης σάρωσης (μόνο για προγραμματισμένη σάρωση)
- Κατάσταση σάρωσης
- Αριθμός σαρωμένων αντικειμένων
- Αριθμός ανιχνεύσεων που εντοπίστηκαν
- Ώρα ολοκλήρωσης
- Συνολικός χρόνος σάρωσης

Η νέα έναρξη μιας εργασίας προγραμματισμένης σάρωσης υπολογιστή παραλείπεται εάν εξακολουθεί να εκτελείται η ίδια προγραμματισμένη εργασία που εκτελέστηκε νωρίτερα. Η εργασία προγραμματισμένης σάρωσης που παραλείφθηκε θα δημιουργήσει ένα αρχείο καταγραφής σάρωσης υπολογιστή με 0 σαρωμένα αντικείμενα και κατάσταση **Η σάρωση δεν ξεκίνησε επειδή η προηγούμενη σάρωση εξακολουθούσε να εκτελείται**.

Για να βρείτε προηγούμενα αρχεία καταγραφής σάρωσης, στο κύριο παράθυρο του προγράμματος, επιλέξτε τα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής**. Στο αναπτυσσόμενο μενού, επιλέξτε **Σάρωση υπολογιστή** και κάντε διπλό κλικ στην εγγραφή που θέλετε.



> Για να μάθετε περισσότερα σχετικά με τις καταχωρίσεις «δεν είναι δυνατό το άνοιγμα», «σφάλμα κατά το άνοιγμα» ή/και «κατεστραμμένη αρχειοθήκη», ανατρέξτε στο άρθρο της Γνωσιακής βάσης της ESET.

Κάντε κλικ στο εικονίδιο ρυθμιστικού **Φιλτράρισμα** για να ανοίξετε το παράθυρο Φιλτράρισμα αρχείων καταγραφής, όπου μπορείτε να περιορίσετε την αναζήτησή σας με προσαρμοσμένα κριτήρια. Για να δείτε το μενού περιβάλλοντος, κάντε δεξί κλικ σε μια συγκεκριμένη εγγραφή αρχείου καταγραφής:

Ενέργεια	Χρήση:
Φιλτράρισμα ίδιων εγγραφών	Ενεργοποιεί το φιλτράρισμα αρχείων καταγραφής. Το αρχείο καταγραφής θα εμφανίζει μόνο εγγραφές του ίδιου τύπου με τον επιλεγμένο.
Φίλτρο	Αυτή η επιλογή ανοίγει το παράθυρο φιλτραρίσματος αρχείων καταγραφής και σας επιτρέπει να καθορίζετε κριτήρια για συγκεκριμένες εγγραφές του αρχείου καταγραφής. Συντόμευση: `Ctrl+Shift+F`
Ενεργοποίηση φίλτρου	Ενεργοποιεί τις ρυθμίσεις φιλτραρίσματος. Εάν ενεργοποιήσετε το φιλτράρισμα για πρώτη φορά, πρέπει να καθορίσετε τις ρυθμίσεις και θα ανοίξει το παράθυρο Φιλτραρίσματος αρχείων καταγραφής.
Απενεργοποίηση φίλτρου	Απενεργοποιεί το φιλτράρισμα (ίδια ενέργεια όπως κάνοντας κλικ στο διακόπτη στο κάτω μέρος).
Αντιγραφή	Αντιγράφει τις επισημασμένες εγγραφές στο πρόχειρο. Συντόμευση: `Ctrl+C`
Αντιγραφή όλων	Αντιγράφει όλες τις εγγραφές που βρίσκονται στο παράθυρο.

Ενέργεια	Χρήση:
Εξαγωγή	Εξάγει τις επισημασμένες εγγραφές στο πρόχειρο σε ένα αρχείο XML.
Εξαγωγή όλων	Αυτή η επιλογή εξάγει όλες τις εγγραφές που βρίσκονται στο παράθυρο σε ένα αρχείο XML.
Περιγραφή ανίχνευσης	Ανοίγει την Εγκυκλοπαίδεια απειλών της ESET, η οποία περιέχει λεπτομερείς πληροφορίες για τους κινδύνους και τα συμπτώματα της επισημασμένης εισβολής.

Σαρώσεις για κακόβουλο λογισμικό

Η πρόσβαση στην ενότητα **Σαρώσεις για κακόβουλο λογισμικό** πραγματοποιείται από την **Εγκατάσταση για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **Σαρώσεις για κακόβουλο λογισμικό** και παρέχει επιλογές για τον ορισμό των παραμέτρων σάρωσης. Η ενότητα αυτή περιλαμβάνει τα παρακάτω στοιχεία:

Επιλεγμένο προφίλ – Ένα συγκεκριμένο σύνολο παραμέτρων που χρησιμοποιείται από την εκτέλεση σάρωσης κατ' απαίτηση. Για να δημιουργήσετε νέο προφίλ, κάντε κλικ στο κουμπί **Επεξεργασία** δίπλα στη **Λίστα προφίλ**. Για περισσότερες λεπτομέρειες ανατρέξτε στην ενότητα Προφίλ σάρωσης.

Προορισμοί σάρωσης – Εάν θέλετε να σαρώσετε μόνο έναν συγκεκριμένο προορισμό, μπορείτε να κάνετε κλικ στο κουμπί **Επεξεργασία** δίπλα στο στοιχείο **Προορισμοί σάρωσης** και να καθορίσετε μια επιλογή από το αναπτυσσόμενο μενού, ή να επιλέξετε συγκεκριμένους προορισμούς από τη δομή φακέλων. Για περισσότερες λεπτομέρειες ανατρέξτε στην ενότητα Προορισμοί σάρωσης.

Παράμετροι ThreatSense – Σε αυτή την ενότητα βρίσκονται επιλογές Εγκατάστασης για προχωρημένους, όπως επεκτάσεις αρχείων που θέλετε να ελέγξετε, μέθοδοι ανίχνευσης που θα χρησιμοποιηθούν κ.λπ. Κάντε κλικ για να ανοίξετε μια καρτέλα με προηγμένες επιλογές σάρωσης.

Σάρωση σε κατάσταση αδράνειας

Μπορείτε να ενεργοποιήσετε τη σάρωση σε κατάσταση αδράνειας στο στοιχείο **Εγκατάσταση για προχωρημένους** στη διαδρομή **Μηχανισμός ανίχνευσης** > **Σαρώσεις για κακόβουλο λογισμικό** > **Σάρωση σε κατάσταση αδράνειας**.

Σάρωση σε κατάσταση αδράνειας

Ενεργοποιήστε το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Ενεργοποίηση σάρωσης σε κατάσταση αδράνειας** για να ενεργοποιηθεί αυτή η δυνατότητα. Όταν ο υπολογιστής βρίσκεται σε κατάσταση αδράνειας, εκτελείται μια σιωπηλή σάρωση υπολογιστή σε όλες τις τοπικές μονάδες δίσκου.

Από προεπιλογή, η σάρωση σε κατάσταση αδράνειας δεν εκτελείται όταν ο υπολογιστής (φορητός) τροφοδοτείται από μπαταρία. Μπορείτε να παρακάμψετε αυτήν τη ρύθμιση ενεργοποιώντας το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Εκτέλεση ακόμη κι αν ο υπολογιστής τροφοδοτείται από μπαταρία** στην Εγκατάσταση για προχωρημένους.

Ενεργοποιήστε το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Ενεργοποίηση καταγραφής** στην Εγκατάσταση για προχωρημένους για να καταγράφεται μια έξοδος σάρωσης υπολογιστή στην

ενότητα Αρχεία καταγραφής (από το κύριο παράθυρο του προγράμματος κάντε κλικ στο στοιχείο **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής** και, στη συνέχεια, επιλέξτε **Σάρωση υπολογιστή** από το αναπτυσσόμενο μενού **Καταγραφή**).

Ανίχνευση κατάστασης αδράνειας

Δείτε την ενότητα Ερεθίσματα ανίχνευσης σε κατάσταση αδράνειας για μια πλήρη λίστα προϋποθέσεων που πρέπει να εκπληρώνονται για να ενεργοποιηθεί η σάρωση σε κατάσταση αδράνειας.

Κάντε κλικ στη Ρύθμιση παραμέτρων μηχανισμού ThreatSense για να τροποποιήσετε τις παραμέτρους σάρωσης (για παράδειγμα, τις μεθόδους ανίχνευσης) για τη σάρωση σε κατάσταση αδράνειας.

Προφίλ σάρωσης

Υπάρχουν 4 προκαθορισμένα προφίλ σάρωσης στο ESET Internet Security:

- **Έξυπνη σάρωση** – Αυτό είναι το προεπιλεγμένο προφίλ σάρωσης για προχωρημένους. Το προφίλ έξυπνης σάρωσης χρησιμοποιεί τεχνολογία Έξυπνης βελτιστοποίησης, η οποία εξαιρεί αρχεία που βρέθηκαν καθαρά σε προηγούμενη σάρωση και δεν έχουν τροποποιηθεί μετά από αυτή τη σάρωση. Αυτό επιτρέπει μικρότερους χρόνους σάρωσης με ελάχιστη επίπτωση στην ασφάλεια του συστήματος.

- **Σάρωση μενού περιβάλλοντος** – Μπορείτε να ξεκινήσετε μια σάρωση κατ' απαίτηση οποιουδήποτε αρχείου από το μενού περιβάλλοντος. Το προφίλ Σάρωσης μενού περιβάλλοντος σάς επιτρέπει να ορίσετε μια ρύθμιση παραμέτρων σάρωσης που θα χρησιμοποιείται όταν θα ενεργοποιείτε τη σάρωση με αυτόν τον τρόπο.

- **Σάρωση σε βάθος** – Το προφίλ Σάρωσης σε βάθος δεν χρησιμοποιεί έξυπνη βελτιστοποίηση από προεπιλογή, συνεπώς δεν εξαιρείται κανένα αρχείο από τη σάρωση όταν χρησιμοποιείται αυτό το προφίλ.

- **Σάρωση υπολογιστή** – Αυτό είναι το προεπιλεγμένο προφίλ που χρησιμοποιείται στην τυπική σάρωση υπολογιστή.

Μπορείτε να αποθηκεύσετε τις παραμέτρους σάρωσης που προτιμάτε για μελλοντικές σαρώσεις. Συνιστούμε να δημιουργήσετε διαφορετικό προφίλ (με διάφορους προορισμούς σάρωσης, μεθόδους σάρωσης και άλλες παραμέτρους) για κάθε τύπο σάρωσης που πραγματοποιείτε συχνά.

Για να δημιουργήσετε νέο προφίλ, ανοίξτε το παράθυρο "Ρυθμίσεις για προχωρημένους" (F5) και επιλέξτε **Μηχανισμός ανίχνευσης** > **Σαρώσεις κακόβουλου λογισμικού** > **Σάρωση κατ' απαίτηση** > **Λίστα προφίλ**. Το παράθυρο **Διαχείριση προφίλ** περιλαμβάνει το αναπτυσσόμενο μενού **Επιλεγμένο προφίλ**, το οποίο παραθέτει τα υπάρχοντα προφίλ σάρωσης και την επιλογή να δημιουργήσετε ένα νέο. Για βοήθεια σχετικά με τη δημιουργία ενός προφίλ σάρωσης που θα ταιριάζει στις απαιτήσεις σας, ανατρέξτε στην ενότητα Ρύθμιση παραμέτρων μηχανισμού ThreatSense, για την περιγραφή κάθε παραμέτρου των ρυθμίσεων σάρωσης.

Υποθέστε ότι θέλετε να δημιουργήσετε το προσωπικό σας προφίλ σάρωσης και η διαμόρφωση της επιλογής **Σάρωση του υπολογιστή σας** σας ικανοποιεί εν μέρει, αλλά δεν θέλετε να πραγματοποιείται σάρωση προγραμμάτων συσκευασίας χρόνου εκτέλεσης ή ενδεχομένως μη ασφαλών εφαρμογών και επίσης θέλετε να εφαρμόσετε **Πάντα αποκατάσταση ανίχνευσης**. Εισαγάγετε το όνομα του νέου προφίλ στο παράθυρο **Διαχείριση προφίλ** και κάντε κλικ στο κουμπί **Προσθήκη**. Εισαγάγετε το νέο σας προφίλ από το αναπτυσσόμενο μενού **Επιλεγμένο προφίλ**, ρυθμίστε τις υπόλοιπες παραμέτρους σύμφωνα με τις απαιτήσεις σας και κάντε κλικ στο κουμπί **OK** για να αποθηκεύσετε το νέο προφίλ σας.

Προορισμοί σάρωσης

Το αναπτυσσόμενο μενού **Προορισμοί σάρωσης** σάς επιτρέπει να επιλέξετε προκαθορισμένους προορισμούς σάρωσης.

- **Σύμφωνα με τις ρυθμίσεις προφίλ** – Επιλέγει προορισμούς που καθορίζονται από το επιλεγμένο προφίλ σάρωσης.
- **Αφαιρούμενα μέσα** – Επιλέγει δισκέτες, συσκευές αποθήκευσης USB, CD/DVD.
- **Τοπικές μονάδες** – Επιλέγει όλες τις μονάδες σκληρού δίσκου του συστήματος.
- **Μονάδες δικτύου** – Επιλέγει όλες τις χαρτογραφημένες μονάδες δικτύου.
- **Προσαρμοσμένη επιλογή** – Ακυρώνει όλες τις προηγούμενες επιλογές.

Η δομή φακέλων (δέντρου) περιέχει επίσης συγκεκριμένους προορισμούς σάρωσης.

- **Λειτουργική μνήμη** – Σαρώνει όλες τις διεργασίες και τα δεδομένα που χρησιμοποιούνται αυτή τη στιγμή από τη λειτουργική μνήμη.
- **Τομείς εκκίνησης/UEFI** – Σαρώνει τους τομείς εκκίνησης και UEFI για την παρουσία κακόβουλου λογισμικού. Διαβάστε περισσότερα σχετικά με το Εργαλείο σάρωσης UEFI στο γλωσσάρι.
- **Βάση δεδομένων WMI** – Σαρώνει ολόκληρη τη βάση δεδομένων Windows Management Instrumentation WMI, όλους τους χώρους ονομάτων, όλες τις παρουσίες κλάσεων και όλες τις ιδιότητες. Αναζητά αναφορές σε μολυσμένα αρχεία ή κακόβουλο λογισμικό που είναι ενσωματωμένα ως δεδομένα.
- **Μητρώο συστήματος** – Σαρώνει ολόκληρο το μητρώο συστήματος, όλα τα κλειδιά και τα δευτερεύοντα κλειδιά. Αναζητά αναφορές σε μολυσμένα αρχεία ή κακόβουλο λογισμικό που είναι ενσωματωμένα ως δεδομένα. Κατά τον καθαρισμό των ανιχνεύσεων, η αναφορά παραμένει στο μητρώο για να διασφαλίζεται ότι δεν θα χαθούν σημαντικά δεδομένα.

Για να μεταβείτε γρήγορα σε έναν προορισμό σάρωσης (αρχείο ή φάκελο), πληκτρολογήστε τη διαδρομή του στο πεδίο κειμένου κάτω από τη δομή δέντρου. Στη διαδρομή γίνεται διάκριση πεζών-κεφαλαίων. Για να συμπεριλάβετε τον προορισμό στη σάρωση, επιλέξτε το πλαίσιο ελέγχου του στη δομή δέντρου.

Έλεγχος συνδεδεμένων συσκευών

Το ESET Internet Security παρέχει αυτόματο έλεγχο συνδεδεμένων συσκευών (CD/DVD/USB/...). Η μονάδα αυτή σάς επιτρέπει να κάνετε αποκλεισμό ή ρύθμιση εκτεταμένων φίλτρων/δικαιωμάτων και να καθορίσετε εάν ο χρήστης θα μπορεί να αποκτά πρόσβαση και να εργάζεται με μια συγκεκριμένη συσκευή. Αυτό μπορεί να είναι χρήσιμο εάν ο διαχειριστής του υπολογιστή θέλει να εμποδίσει τη χρήση συσκευών που περιέχουν ανεπιθύμητο περιεχόμενο.

Υποστηριζόμενες εξωτερικές συσκευές:

- Δίσκος αποθήκευσης (HDD, αφαιρούμενη μονάδα δίσκου USB)
- CD/DVD
- USB Εκτυπωτής
- FireWire Χώρος αποθήκευσης
- Bluetooth Συσκευή
- Συσκευή ανάγνωσης έξυπνων καρτών
- Συσκευή απεικόνισης
- Μόντεμ
- LPT/COM θύρα
- Φορητή συσκευή
- Όλοι οι τύποι συσκευών

Μπορείτε να αλλάξετε τις επιλογές του ελέγχου συνδεδεμένων συσκευών στη ρύθμιση **Ρυθμίσεις για προχωρημένους** (F5) > **Έλεγχος συνδεδεμένων συσκευών**.

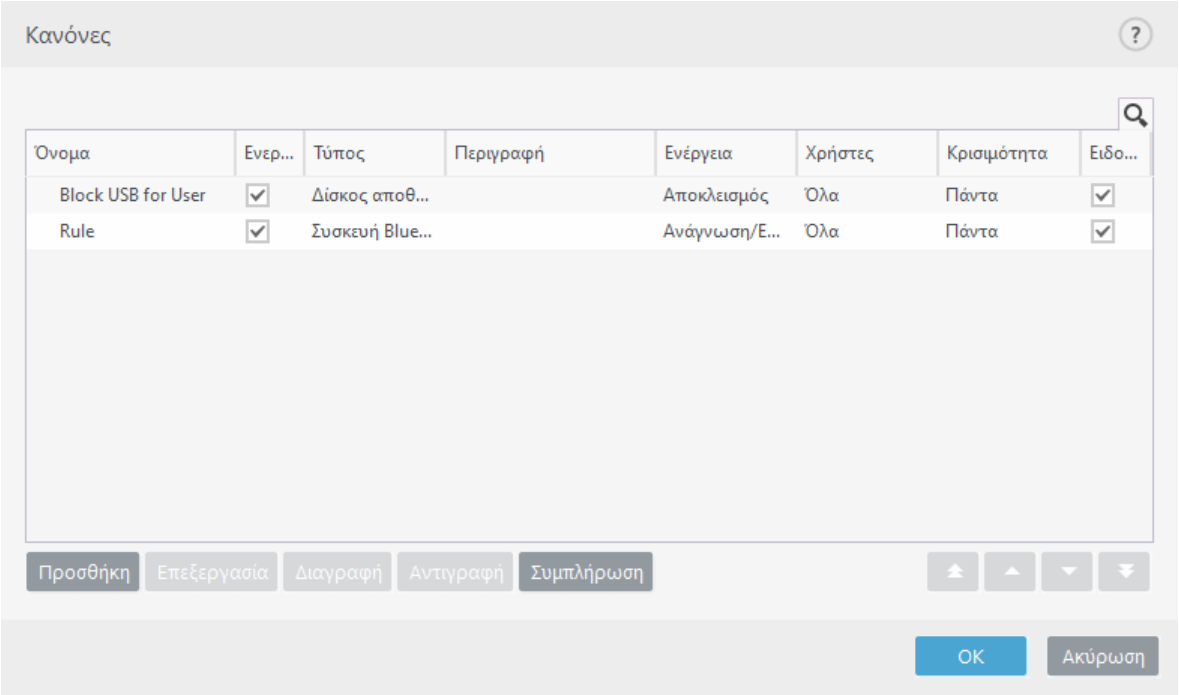
Ενεργοποιήστε το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Ενεργοποίηση ελέγχου συνδεδεμένων συσκευών** για να ενεργοποιηθεί η δυνατότητα Ελέγχου συνδεδεμένων συσκευών στο ESET Internet Security. Θα πρέπει να κάνετε επανεκκίνηση του υπολογιστή σας για να εφαρμοστεί αυτή η αλλαγή. Όταν ενεργοποιηθεί ο Έλεγχος συνδεδεμένων συσκευών, θα γίνει ενεργή η επιλογή **Κανόνες** και θα σας επιτρέπεται να ανοίξετε το παράθυρο του Επεξεργαστή κανόνων.

> Μπορείτε να δημιουργήσετε διαφορετικές ομάδες συσκευών στις οποίες να εφαρμόζονται διαφορετικοί κανόνες. Μπορείτε επίσης να δημιουργήσετε μία ομάδα για την οποία θα εφαρμόζεται ο κανόνας με δικαιώματα **Ανάγνωσης/Εγγραφής** ή **Μόνο ανάγνωσης**. Αυτό διασφαλίζει τον αποκλεισμό των μη αναγνωρισμένων συσκευών από τον έλεγχο συνδεδεμένων συσκευών, όταν αυτές συνδέονται στον υπολογιστή σας.

Εάν εισαχθεί μια συσκευή η οποία αποκλείεται από έναν υπάρχοντα κανόνα, θα εμφανιστεί ένα παράθυρο ειδοποίησης και δεν θα δοθεί πρόσβαση στη συσκευή.

Επεξεργαστής κανόνων ελέγχου συνδεδεμένων συσκευών

Το παράθυρο **Επεξεργαστής κανόνων ελέγχου συνδεδεμένων συσκευών** εμφανίζει τους υπάρχοντες κανόνες και επιτρέπει τον ακριβή έλεγχο των εξωτερικών συσκευών τις οποίες συνδέουν οι χρήστες στον υπολογιστή.



Είναι δυνατόν να επιτρέπονται ή να αποκλείονται συγκεκριμένες συσκευές ανά χρήστη ή ομάδα χρηστών και με βάση πρόσθετες παραμέτρους συσκευών που μπορούν να καθοριστούν στη διαμόρφωση κανόνων. Η λίστα κανόνων περιέχει αρκετές περιγραφές ενός κανόνα, όπως το όνομα, τον τύπο της εξωτερικής συσκευής, την ενέργεια που θα εκτελείται μετά τη σύνδεση μιας εξωτερικής συσκευής στον υπολογιστή σας και τη σοβαρότητα της καταγραφής. Δείτε επίσης το θέμα Προσθήκη κανόνων ελέγχου συνδεδεμένων συσκευών.

Κάντε κλικ στο κουμπί **Προσθήκη** ή στο κουμπί **Επεξεργασία** για να διαχειριστείτε έναν κανόνα. Κάντε κλικ στο στοιχείο **Αντιγραφή** για να δημιουργήσετε έναν νέο κανόνα με προκαθορισμένες επιλογές που θα χρησιμοποιηθούν σε έναν άλλο επιλεγμένο κανόνα. Οι συμβολοσειρές XML που εμφανίζονται όταν κάνετε κλικ σε έναν κανόνα είναι δυνατό να αντιγραφούν στο πρόχειρο, έτσι ώστε οι διαχειριστές συστημάτων να μπορούν να εξαγάγουν/εισαγάγουν αυτά τα δεδομένα και να τα χρησιμοποιήσουν.

Κάνοντας κλικ κρατώντας ταυτόχρονα πατημένο το **CTRL**, μπορείτε να επιλέξετε πολλούς κανόνες και να εφαρμόσετε ενέργειες, όπως διαγραφή ή μετακίνηση προς τα επάνω ή προς τα κάτω στη λίστα, σε όλους τους επιλεγμένους κανόνες. Το πλαίσιο ελέγχου **Ενεργό** απενεργοποιεί ή ενεργοποιεί έναν κανόνα. Αυτό μπορεί να είναι χρήσιμο εάν δεν θέλετε να διαγράψετε οριστικά έναν κανόνα, σε περίπτωση που θέλετε να τον χρησιμοποιήσετε στο μέλλον.

Ο έλεγχος επιτυγχάνεται με κανόνες οι οποίοι ταξινομούνται με τη σειρά που καθορίζει την προτεραιότητά τους, με τους κανόνες υψηλότερης προτεραιότητας να βρίσκονται στην κορυφή.

Μπορείτε να προβάλετε τις καταχωρίσεις καταγραφής από το κύριο παράθυρο του ESET Internet

Security στη θέση **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής**.

Το Αρχείο καταγραφής ελέγχου συνδεδεμένων συσκευών καταγράφει όλες τις περιπτώσεις στις οποίες ενεργοποιείται ο Έλεγχος συνδεδεμένων συσκευών.

Ανιχνευμένες συσκευές

Το κουμπί **Συμπλήρωση** παρέχει μια επισκόπηση όλων των συνδεδεμένων συσκευών με πληροφορίες όπως: τύπος συσκευής, όνομα κατασκευαστή, μοντέλο και αριθμός σειράς (εάν είναι διαθέσιμος).

Επιλέξτε μια συσκευή από τη λίστα «Ανιχνευμένες συσκευές» και κάντε κλικ στο **OK** για να προσθέσετε έναν κανόνα ελέγχου συνδεδεμένων συσκευών με προκαθορισμένες πληροφορίες (μπορείτε να προσαρμόσετε όλες τις ρυθμίσεις).

Οι συσκευές που βρίσκονται σε λειτουργία χαμηλής ισχύος (αναστολή λειτουργίας) επισημαίνονται με ένα εικονίδιο προειδοποίησης . Για να ενεργοποιήσετε το κουμπί **OK** και να προσθέσετε έναν κανόνα για αυτήν τη συσκευή:

- Επανασύνδεση της συσκευής
- Χρησιμοποιήστε τη συσκευή (για παράδειγμα, ξεκινήστε την εφαρμογή Κάμερα στα Windows για να ενεργοποιήσετε την κάμερα)

Ομάδες συσκευών

> Μια συσκευή που είναι συνδεδεμένη στον υπολογιστή σας μπορεί να αποτελεί κίνδυνο ασφαλείας.

Το παράθυρο "Ομάδες συσκευών" χωρίζεται σε δύο τμήματα. Το δεξί τμήμα του παραθύρου περιέχει μια λίστα συσκευών που ανήκουν στην αντίστοιχη ομάδα, ενώ το αριστερό τμήμα του παραθύρου περιέχει τις ομάδες που έχουν δημιουργηθεί. Επιλέξτε μια ομάδα με μια λίστα συσκευών που θέλετε να εμφανίζεται στο δεξί τμήμα.

Όταν ανοίγετε το παράθυρο "Ομάδες συσκευών" και επιλέγετε μια ομάδα, μπορείτε να προσθέσετε ή να διαγράψετε συσκευές από τη λίστα. Ένας άλλος τρόπος να προσθέσετε συσκευές στην ομάδα είναι να τις εισαγάγετε από αρχείο. Εναλλακτικά, μπορείτε να κάνετε κλικ στο κουμπί **Συμπλήρωση** και όλες οι συσκευές που είναι συνδεδεμένες στον υπολογιστή σας θα εμφανιστούν στο παράθυρο **Ανιχνευμένες συσκευές**. Επιλέξτε μια συσκευή από τη λίστα που εμφανίζεται και κάντε κλικ στο κουμπί **OK** για να προσθέσετε τη συσκευή στην ομάδα.

Στοιχεία ελέγχου

Προσθήκη – Μπορείτε να προσθέσετε μια ομάδα, πληκτρολογώντας το όνομά της, ή μια συσκευή σε μια υπάρχουσα ομάδα (προαιρετικά, μπορείτε να καθορίσετε λεπτομέρειες, όπως όνομα κατασκευαστή, μοντέλο και αριθμό σειράς) ανάλογα με το τμήμα του παραθύρου στο οποίο πατήσατε το κουμπί.

Επεξεργασία – Σας επιτρέπει να τροποποιήσετε το όνομα της επιλεγμένης ομάδας ή τις παραμέτρους της συσκευής (κατασκευαστή, όνομα, αριθμό σειράς).

Διαγραφή – Διαγράφει την επιλεγμένη ομάδα ή συσκευή ανάλογα με το τμήμα του παραθύρου στο οποίο πατήσατε το κουμπί.

Εισαγωγή – Εισάγει μια λίστα συσκευών από ένα αρχείο κειμένου. Η εισαγωγή συσκευών από ένα αρχείο κειμένου απαιτεί σωστή μορφοποίηση:

- Κάθε συσκευή εκκινεί στη νέα γραμμή.
- Για κάθε συσκευή πρέπει να υπάρχουν τα στοιχεία **Προμηθευτής**, **Μοντέλο** και **Σειριακός αριθμός**, διαχωρισμένα με κόμμα.

Ακολουθεί ένα παράδειγμα του περιεχομένου του αρχείου κειμένου:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Εξαγωγή – Εξάγει μια λίστα συσκευών σε ένα αρχείο.

Το κουμπί **Συμπλήρωση** παρέχει μια επισκόπηση όλων των συνδεδεμένων συσκευών με πληροφορίες όπως: τύπος συσκευής, όνομα κατασκευαστή, μοντέλο και αριθμός σειράς (εάν είναι διαθέσιμος).

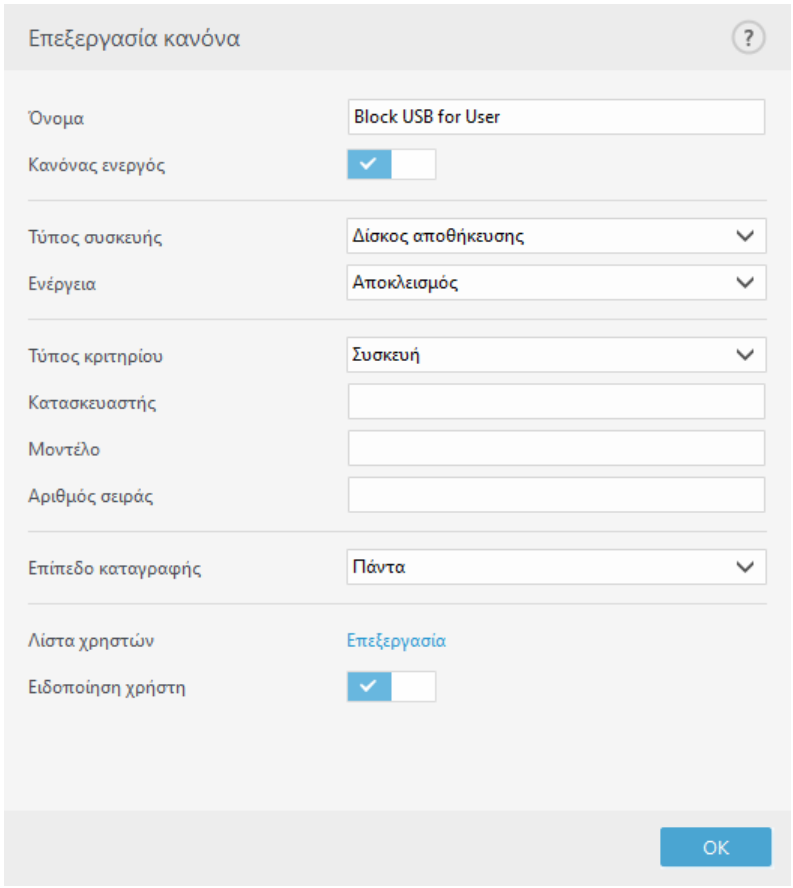
Όταν ολοκληρώσετε την επεξεργασία, κάντε κλικ στο κουμπί **OK**. Κάντε κλικ στο κουμπί **Άκυρο**, εάν θέλετε να κλείσετε το παράθυρο **Ομάδες συσκευών** χωρίς να αποθηκεύσετε τις αλλαγές.

Μπορείτε να δημιουργήσετε διαφορετικές ομάδες συσκευών στις οποίες να εφαρμόζονται διαφορετικοί κανόνες. Μπορείτε επίσης να δημιουργήσετε μία ομάδα για την οποία θα εφαρμόζεται ο κανόνας με δικαιώματα **Ανάγνωσης/Εγγραφής** ή **Μόνο ανάγνωσης**. Αυτό διασφαλίζει τον αποκλεισμό των μη αναγνωρισμένων συσκευών από τον έλεγχο συνδεδεμένων συσκευών, όταν αυτές συνδέονται στον υπολογιστή σας.

Σημειώνεται ότι δεν είναι διαθέσιμες όλες οι Ενέργειες (δικαιώματα) για όλους τους τύπους συσκευών. Εάν είναι συσκευή τύπου αποθήκευσης, και οι τέσσερις Ενέργειες είναι διαθέσιμες. Για συσκευές χωρίς αποθήκευση, υπάρχουν μόνο τρεις Ενέργειες διαθέσιμες (για παράδειγμα η ενέργεια **Μόνο ανάγνωση** δεν είναι διαθέσιμη για Bluetooth, συνεπώς για τις συσκευές Bluetooth οι διαθέσιμες ενέργειες είναι μόνο Αποδοχή, Αποκλεισμός ή Προειδοποίηση).

Προσθήκη κανόνων ελέγχου συνδεδεμένων συσκευών

Ο κανόνας ελέγχου συνδεδεμένων συσκευών καθορίζει την ενέργεια που θα εκτελεστεί όταν συνδεθεί στον υπολογιστή μια συσκευή που πληροί τα κριτήρια του κανόνα.



Εισαγάγετε μια περιγραφή του κανόνα στο πεδίο **Όνομα** για καλύτερη ταυτοποίηση. Κάντε κλικ στο ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Κανόνας ενεργός** για να απενεργοποιήσετε ή να ενεργοποιήσετε τον κανόνα. Αυτό μπορεί να είναι χρήσιμο αν δεν θέλετε να καταργήσετε οριστικά τον κανόνα.

Τύπος συσκευής

Επιλέξτε τον τύπο εξωτερικής συσκευής από το αναπτυσσόμενο μενού (Δίσκος αποθήκευσης, φορητή συσκευή, Bluetooth, FireWire κ.λπ). Πληροφορίες για τον τύπο συσκευών λαμβάνονται από το λειτουργικό σύστημα και εμφανίζονται στη Διαχείριση συσκευών του συστήματος, εφόσον υπάρχει συνδεδεμένη συσκευή στον υπολογιστή. Οι συσκευές αποθήκευσης περιλαμβάνουν τους εξωτερικούς δίσκους και τις συμβατικές συσκευές ανάγνωσης καρτών μνήμης που συνδέονται μέσω USB ή FireWire. Οι συσκευές ανάγνωσης έξυπνων καρτών περιλαμβάνουν όλες τις συσκευές ανάγνωσης έξυπνων καρτών με ενσωματωμένο ολοκληρωμένο κύκλωμα, όπως κάρτες SIM ή κάρτες ελέγχου ταυτότητας. Παραδείγματα συσκευών απεικόνισης είναι οι σαρωτές ή οι κάμερες. Επειδή οι συσκευές αυτές παρέχουν πληροφορίες μόνο σχετικά με τις ενέργειές τους και δεν παρέχουν πληροφορίες σχετικά με τους χρήστες, μπορούν να αποκλειστούν μόνο γενικά.

Ενέργεια

Η πρόσβαση σε συσκευές που δεν είναι συσκευές αποθήκευσης μπορεί να επιτρέπεται ή να αποκλείεται. Αντίθετα, οι κανόνες για τις συσκευές αποθήκευσης σάς επιτρέπουν να επιλέξετε μία από τις παρακάτω ρυθμίσεις δικαιωμάτων:

- **Ανάγνωση/Εγγραφή** – Θα επιτρέπεται πλήρης πρόσβαση στη συσκευή.
- **Αποκλεισμός** – Η πρόσβαση στη συσκευή θα αποκλειστεί.
- **Μόνο ανάγνωση** – Θα επιτρέπεται μόνο πρόσβαση ανάγνωσης στη συσκευή.

- **Προειδοποίηση** – Κάθε φορά που συνδέεται μια συσκευή, ο χρήστης θα ειδοποιείται εάν επιτρέπεται/αποκλείεται και θα δημιουργείται μια καταχώριση στο αρχείο καταγραφής. Οι συσκευές δεν απομνημονεύονται, αλλά θα εμφανίζεται μια ειδοποίηση σε κάθε επόμενη σύνδεση της ίδιας συσκευής.

Σημειώνεται ότι δεν είναι διαθέσιμες όλες οι Ενέργειες (δικαιώματα) για όλους τους τύπους συσκευών. Εάν είναι συσκευή τύπου αποθήκευσης, και οι τέσσερις Ενέργειες είναι διαθέσιμες. Για συσκευές χωρίς αποθήκευση, υπάρχουν μόνο τρεις Ενέργειες διαθέσιμες (για παράδειγμα η ενέργεια **Μόνο ανάγνωση** δεν είναι διαθέσιμη για Bluetooth, συνεπώς για τις συσκευές Bluetooth οι διαθέσιμες ενέργειες είναι μόνο Αποδοχή, Αποκλεισμός ή Προειδοποίηση).

Τύπος κριτηρίου

Επιλέξτε **Ομάδα συσκευών** ή **Συσκευή**.

Οι πρόσθετες παράμετροι που εμφανίζονται παρακάτω μπορούν να χρησιμοποιηθούν για τη ρύθμιση των κανόνων και την προσαρμογή τους στις συσκευές. Σε όλες τις παραμέτρους γίνεται διάκριση πεζών-κεφαλαίων:

- **Κατασκευαστής** – Φιλτράρισμα κατά όνομα ή ID.
- **Μοντέλο** – Το συγκεκριμένο όνομα της συσκευής.
- **Σειριακός αριθμός** – Οι εξωτερικές συσκευές έχουν συνήθως δικούς τους αριθμούς σειράς. Στην περίπτωση CD/DVD, ο αριθμός αυτός είναι ο αριθμός σειράς του συγκεκριμένου μέσου και όχι της μονάδας CD.

Εάν αυτές οι παράμετροι δεν οριστούν, ο κανόνας θα αγνοήσει αυτά τα πεδία κατά το συσχετισμό. Στις παραμέτρους φιλτραρίσματος όλων των πεδίων κειμένου δεν γίνεται διάκριση πεζών-κεφαλαίων και δεν υποστηρίζονται ειδικοί χαρακτήρες (*, ?).

Για να προβάλετε πληροφορίες σχετικά με μια συσκευή, δημιουργήστε έναν κανόνα για τον συγκεκριμένο τύπο συσκευής, συνδέστε τη συσκευή στον υπολογιστή και κατόπιν κάντε κλικ στις λεπτομέρειες της συσκευής στο Αρχείο καταγραφής ελέγχου συνδεδεμένων συσκευών.

Καταγραφή κρισιμότητας

Το ESET Internet Security αποθηκεύει όλα τα σημαντικά συμβάντα σε ένα αρχείο καταγραφής, το οποίο μπορείτε να προβάλετε απευθείας από το κύριο μενού. Κάντε κλικ στα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής** και κατόπιν επιλέξτε **Έλεγχος συνδεδεμένων συσκευών** από το αναπτυσσόμενο μενού **Καταγραφή**.

- **Πάντα** – Γίνεται καταγραφή όλων των συμβάντων.
- **Εγγραφές διαγνωστικού ελέγχου** – Καταγράφει πληροφορίες απαραίτητες για τη ρύθμιση του προγράμματος.
- **Πληροφορίες** – Καταγράφει πληροφοριακά μηνύματα, συμπεριλαμβανομένων μηνυμάτων επιτυχούς ενημέρωσης, καθώς και όλες τις παραπάνω εγγραφές.
- **Προειδοποίηση** – Καταγράφει κρίσιμα σφάλματα και προειδοποιητικά μηνύματα.

• **Καμία** – Δεν καταγράφονται εγγραφές.

Λίστα χρηστών

Οι κανόνες μπορεί να περιορίζονται σε ορισμένους χρήστες ή ομάδες χρηστών με την προσθήκη τους στη Λίστα χρηστών κάνοντας κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Λίστα χρηστών**.

• **Προσθήκη** – Ανοίγει το παράθυρο διαλόγου **Τύποι αντικειμένων: Χρήστες ή Ομάδες** που σας επιτρέπει να επιλέξετε τους χρήστες που θέλετε.

• **Κατάργηση** – Αφαιρεί τον επιλεγμένο χρήστη από το φίλτρο.

Περιορισμοί λίστας χρηστών

Στη Λίστα χρηστών δεν είναι δυνατόν να οριστούν κανόνες με συγκεκριμένους τύπους συσκευών:

- Εκτυπωτής USB
- Συσκευή Bluetooth
- Συσκευή ανάγνωσης έξυπνων καρτών
- Συσκευή απεικόνισης
- Μόντεμ
- Θύρα LPT/COM

Ειδοποίηση χρήστη – Εάν εισαχθεί μια συσκευή η οποία αποκλείεται από έναν υπάρχοντα κανόνα, θα εμφανιστεί ένα παράθυρο ειδοποίησης.

Προστασία web κάμερας

Η **Προστασία web κάμερας** σάς ενημερώνει σχετικά με τις διεργασίες και τις εφαρμογές που αποκτούν πρόσβαση στην κάμερα του υπολογιστή σας. Εάν μια εφαρμογή προσπαθήσει να αποκτήσει πρόσβαση στην κάμερά σας, θα λάβετε μια ειδοποίηση όπου μπορείτε να επιλέξετε **επιτρέπεται** ή **αποκλεισμός** της πρόσβασης. Το χρώμα του παραθύρου συναγερμού εξαρτάται από τη φήμη της εφαρμογής.

Οι επιλογές εγκατάστασης προστασίας web κάμερας μπορούν να τροποποιηθούν στη διαδρομή **Εγκατάσταση για προχωρημένους** (F5) > **Έλεγχος συνδεδεμένων συσκευών** > **Προστασία web κάμερας**.

Για να ενεργοποιήσετε τη δυνατότητα Προστασίας web κάμερας στο ESET Internet Security, ενεργοποιήστε το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Ενεργοποίηση προστασίας web κάμερας**.

Όταν ενεργοποιηθεί η Προστασία web κάμερας, θα ενεργοποιηθούν οι **Κανόνες**, επιτρέποντάς σας να ανοίξετε το παράθυρο του Επεξεργαστή κανόνων.

Για να απενεργοποιήσετε τους συναγερμούς για εφαρμογές όταν υπάρχει κανόνας και οι εφαρμογές τροποποιήθηκαν, αλλά εξακολουθούν να έχουν έγκυρη ψηφιακή υπογραφή (για παράδειγμα, μια ενημέρωση εφαρμογής), ενεργοποιήστε το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Απενεργοποίηση συναγερμών πρόσβασης web κάμερας για τροποποιημένες εφαρμογές**.

Επεξεργαστής κανόνων προστασίας κάμερας

Αυτό το παράθυρο εμφανίζει υπάρχοντες κανόνες και επιτρέπει τον έλεγχο των εφαρμογών και των διαδικασιών που αποκτούν πρόσβαση στην κάμερα του υπολογιστή σας, ανάλογα με την ενέργεια που έχετε εκτελέσει.

Είναι διαθέσιμες οι παρακάτω ενέργειες:

- **Να επιτρέπεται η πρόσβαση**
- **Αποκλεισμός πρόσβασης**

- **Ερώτηση** (Ερωτάται ο χρήστης κάθε φορά που μια εφαρμογή προσπαθεί να αποκτήσει πρόσβαση στην κάμερα)

Καταργήστε την επιλογή του πλαισίου ελέγχου στη στήλη **Ειδοποίηση** για να διακόψετε τη λήψη ειδοποιήσεων όταν μια εφαρμογή αποκτά πρόσβαση στην κάμερα.

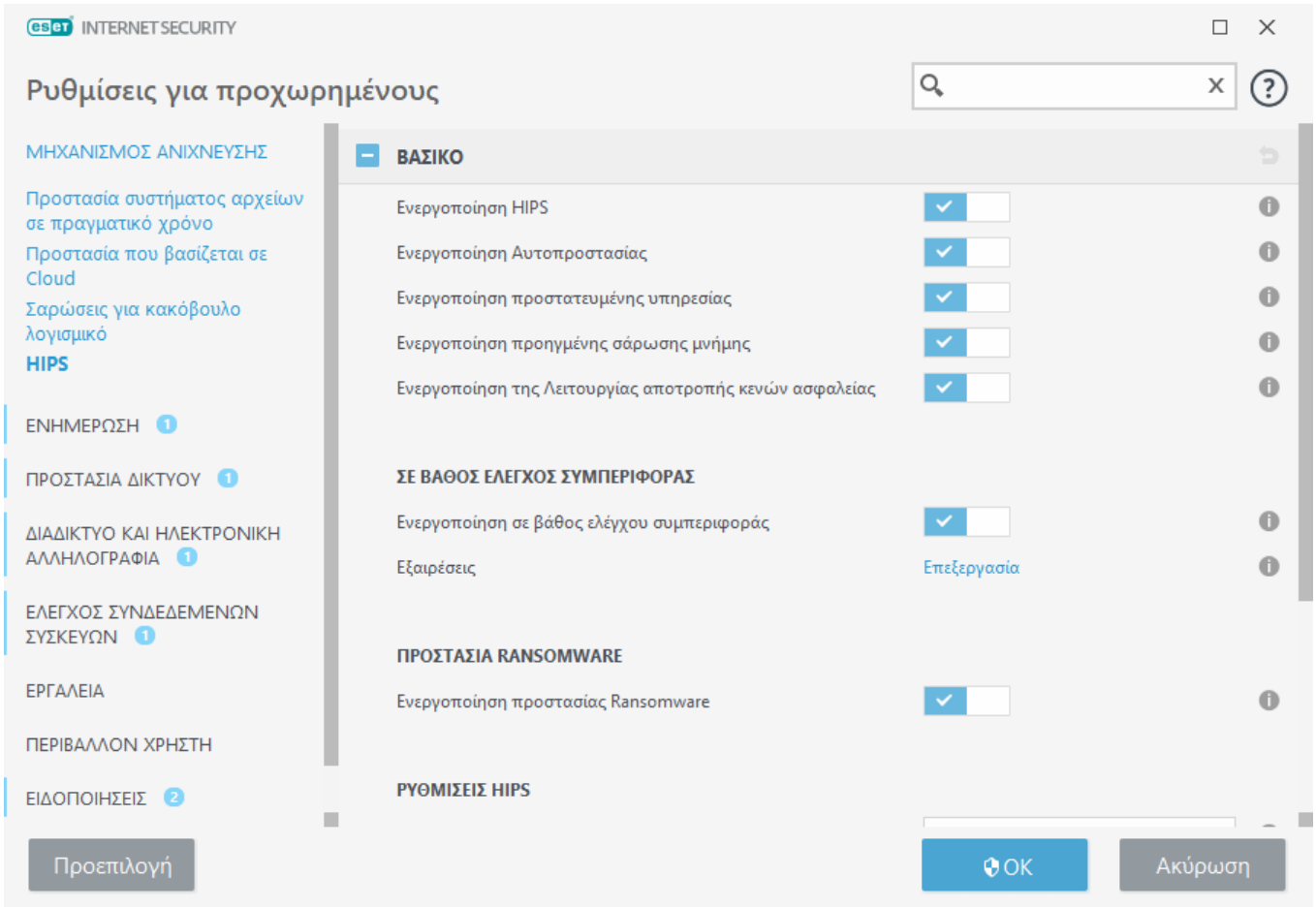
> **Εικονογραφημένες οδηγίες**
> Πώς να δημιουργήσετε και να επεξεργαστείτε κανόνες της web κάμερας στο ESET Internet Security.

Σύστημα αποτροπής απειλών με βάση (HIPS)

> Αλλαγές στις ρυθμίσεις HIPS θα πρέπει να γίνονται μόνο από πεπειραμένους χρήστες. Εσφαλμένη διαμόρφωση των ρυθμίσεων HIPS μπορεί να οδηγήσει σε αστάθεια του συστήματος.

Το **Host-based Intrusion Prevention System (HIPS)** - Σύστημα αποτροπής εισβολών από κεντρικό υπολογιστή (HIPS) προστατεύει το σύστημά σας από κακόβουλο λογισμικό και ανεπιθύμητη δραστηριότητα που επιχειρεί να επηρεάσει αρνητικά τον υπολογιστή σας. Το HIPS χρησιμοποιεί προηγμένη ανάλυση συμπεριφοράς σε συνδυασμό με δυνατότητες ανίχνευσης φιλτραρίσματος δικτύου για την παρακολούθηση των διεργασιών που εκτελούνται, αρχείων και κλειδιών μητρώου. Το HIPS είναι ξεχωριστό από την προστασία συστήματος αρχείων σε πραγματικό χρόνο και δεν είναι τείχος προστασίας - παρακολουθεί μόνο διεργασίες που εκτελούνται στο πλαίσιο του λειτουργικού συστήματος.

Οι ρυθμίσεις HIPS βρίσκονται στη θέση **Ρυθμίσεις για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **HIPS** > **Βασικές ρυθμίσεις**. Η κατάσταση HIPS (ενεργοποιημένο/απενεργοποιημένο) εμφανίζεται στο κύριο παράθυρο προγράμματος του ESET Internet Security, στη θέση **Ρυθμίσεις** > **Προστασία υπολογιστή**.



Βασικό

Ενεργοποίηση HIPS – Το HIPS ενεργοποιείται από προεπιλογή στο ESET Internet Security. Εάν απενεργοποιήσετε το HIPS θα απενεργοποιηθούν και οι υπόλοιπες δυνατότητες του HIPS, όπως η Λειτουργία αποτροπής κενών ασφαλείας.

Ενεργοποίηση αυτοπροστασίας – Το ESET Internet Security χρησιμοποιεί την ενσωματωμένη τεχνολογία **Αυτοπροστασία** ως μέρος του HIPS για να εμποδίζει το κακόβουλο λογισμικό να καταστρέψει ή να απενεργοποιήσει την προστασία antivirus και antispyware. Η αυτοπροστασία προστατεύει κρίσιμες διεργασίες του συστήματος και της ESET, κλειδιά μητρώου και αρχεία από επέμβαση.

Ενεργοποίηση προστατευμένης υπηρεσίας – ενεργοποιεί την προστασία για την Υπηρεσία ESET (ekrn.exe). Όταν η επιλογή είναι ενεργή, η υπηρεσία εκκινείται ως προστατευμένη υπηρεσία των Windows για άμυνα ενάντια σε επιθέσεις από κακόβουλο λογισμικό. Αυτή η επιλογή είναι διαθέσιμη στα Windows 8.1 και νεότερες εκδόσεις.

Ενεργοποίηση προηγμένης σάρωσης μνήμης – λειτουργεί σε συνδυασμό με τη Λειτουργία αποτροπής κενών ασφαλείας, ενισχύοντας την προστασία από κακόβουλο λογισμικό που έχει σχεδιαστεί για να αποφεύγει την ανίχνευση από προϊόντα προστασίας από κακόβουλο λογισμικό μέσω παραπλάνησης ή κρυπτογράφησης. Η Προηγμένη σάρωση μνήμης είναι ενεργοποιημένη από προεπιλογή. Διαβάστε περισσότερα για αυτό τον τύπο προστασίας στο γλωσσάρι.

Ενεργοποίηση της λειτουργίας αποτροπής κενών ασφαλείας – είναι σχεδιασμένη για να προστατεύει τύπους εφαρμογών που γίνονται συχνά αντικείμενο εκμετάλλευσης, όπως προγράμματα περιήγησης, προγράμματα ανάγνωσης εγγράφων PDF, προγράμματα-πελάτες email και στοιχεία του

MS Office. Η Λειτουργία αποτροπής κενών ασφαλείας ενεργοποιείται από προεπιλογή. Διαβάστε περισσότερα για αυτό τον τύπο προστασίας στο γλωσσάρι.

Σε βάθος έλεγχος συμπεριφοράς

Ενεργοποίηση σε βάθος ελέγχου συμπεριφοράς – άλλο ένα επίπεδο προστασίας που λειτουργεί ως μέρος της δυνατότητας HIPS. Αυτή η επέκταση του HIPS αναλύει τη συμπεριφορά όλων των προγραμμάτων που εκτελούνται στον υπολογιστή και σας προειδοποιεί εάν η συμπεριφορά της διεργασίας είναι κακόβουλη.

Οι εξαιρέσεις HIPS από τον σε βάθος έλεγχο συμπεριφοράς σάς επιτρέπουν να εξαιρείτε διεργασίες από την ανάλυση. Για να διασφαλίζεται η σάρωση όλων των διεργασιών για ενδεχόμενες απειλές, συνιστάται να δημιουργείτε εξαιρέσεις μόνο όταν είναι απολύτως απαραίτητο.

Προστασία Ransomware

Ενεργοποίηση προστασίας Ransomware – άλλο ένα επίπεδο προστασίας που λειτουργεί ως μέρος της δυνατότητας HIPS. Για να λειτουργήσει η προστασία ransomware, πρέπει να είναι ενεργοποιημένο το σύστημα φήμης ESET LiveGrid®. Διαβάστε περισσότερα σχετικά με αυτό τον τύπο προστασίας.

Ρυθμίσεις HIPS

Η **Λειτουργία φιλτραρίσματος** μπορεί να εκτελεστεί σε μία από τις ακόλουθες λειτουργίες:

Λειτουργία φιλτραρίσματος	Περιγραφή
Αυτόματη λειτουργία	Επιτρέπονται οι ενέργειες εκτός από εκείνες που αποκλείονται από προκαθορισμένους κανόνες για την προστασία του συστήματός σας.
Έξυπνη λειτουργία	Ο χρήστης θα ειδοποιείται μόνο για πολύ ύποπτα συμβάντα.
Αλληλεπιδραστική λειτουργία	Θα ζητείται από το χρήστη να επιβεβαιώνει ενέργειες.
Λειτουργία βασισμένη σε πολιτική	Αποκλείει όλες τις λειτουργίες που δεν ορίζονται από έναν συγκεκριμένο κανόνα που τις επιτρέπει.
Λειτουργία εκμάθησης	Οι λειτουργίες είναι ενεργοποιημένες και δημιουργείται ένας κανόνας μετά από κάθε λειτουργία. Οι κανόνες που δημιουργούνται σε αυτή τη λειτουργία μπορούν να προβληθούν στον επεξεργαστή **Κανόνες HIPS**, αλλά η προτεραιότητά τους είναι χαμηλότερη από την προτεραιότητα των κανόνων που δημιουργούνται μη αυτόματα ή των κανόνων που δημιουργούνται με αυτόματη λειτουργία. Εάν επιλέξετε τη **Λειτουργία εκμάθησης** από το αναπτυσσόμενο μενού **Λειτουργία φιλτραρίσματος**, θα είναι διαθέσιμη η ρύθμιση **Η λειτουργία εκμάθησης θα τερματιστεί στις**. Επιλέξτε το χρονικό διάστημα για το οποίο θέλετε να ενεργοποιηθεί η λειτουργία εκμάθησης. Η μέγιστη διάρκεια είναι 14 ημέρες. Όταν παρέλθει η καθορισμένη διάρκεια, θα σας ζητηθεί να επεξεργαστείτε τους κανόνες που δημιουργήθηκαν με το HIPS όσο βρισκόταν σε λειτουργία εκμάθησης. Μπορείτε να επιλέξετε διαφορετική λειτουργία φιλτραρίσματος ή να αναβάλετε την απόφαση και να συνεχίσετε να χρησιμοποιείτε τη λειτουργία εκμάθησης.

Η λειτουργία καθορίζεται μετά τη λήξη της λειτουργίας εκμάθησης – Επιλέξτε τη λειτουργία φιλτραρίσματος που θα χρησιμοποιηθεί μετά τη λήξη της λειτουργίας εκμάθησης. Μετά τη λήξη, η

επιλογή **Ερώτηση στο χρήστη** απαιτεί δικαιώματα διαχειριστή για να εκτελεστεί αλλαγή στη λειτουργία φιλτραρίσματος HIPS.

Το σύστημα HIPS παρακολουθεί συμβάντα μέσα στο λειτουργικό σύστημα και αντιδρά ανάλογα, με βάση κανόνες παρόμοιους με εκείνους που χρησιμοποιούνται στο τείχος προστασίας. Κάντε κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Κανόνες**, για να ανοίξετε το πρόγραμμα επεξεργασίας **Κανόνες HIPS**. Στο παράθυρο κανόνων HIPS μπορείτε να επιλέξετε, να προσθέσετε, να επεξεργαστείτε ή να καταργήσετε κανόνες. Μπορείτε να βρείτε περισσότερες λεπτομέρειες για τη δημιουργία κανόνων και τις λειτουργίες HIPS στην ενότητα Επεξεργασία κανόνα HIPS.

Αλληλεπιδραστικό παράθυρο HIPS

Το παράθυρο διαλόγου HIPS σάς επιτρέπει να δημιουργήσετε έναν κανόνα με βάση τις νέες ενέργειες που θα ανιχνεύσει το HIPS και, στη συνέχεια, να καθορίσετε τις συνθήκες υπό τις οποίες θα επιτρέπεται ή δεν θα επιτρέπεται αυτή η ενέργεια.

Οι κανόνες που δημιουργούνται από το παράθυρο ειδοποιήσεων θεωρούνται ισοδύναμοι με τους κανόνες που δημιουργούνται με μη αυτόματο τρόπο. Ένας κανόνας που έχει δημιουργηθεί από ένα παράθυρο ειδοποιήσεων μπορεί να είναι λιγότερο συγκεκριμένος από ότι ο κανόνας που ενεργοποίησε το συγκεκριμένο παράθυρο διαλόγου. Αυτό σημαίνει ότι, μετά τη δημιουργία ενός τέτοιου κανόνα στο παράθυρο διαλόγου, η ίδια λειτουργία θα μπορεί να ενεργοποιεί το ίδιο παράθυρο. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Προτεραιότητα για κανόνες HIPS.

Εάν η προεπιλεγμένη ενέργεια για έναν κανόνα καθοριστεί σε **Ερώτηση κάθε φορά**, θα εμφανίζεται ένα παράθυρο διαλόγου κάθε φορά που ενεργοποιείται ο κανόνας. Για τη λειτουργία μπορείτε να επιλέξετε **Δεν επιτρέπεται** ή **Επιτρέπεται**. Εάν δεν επιλέξετε μια ενέργεια τη δεδομένη στιγμή, η νέα ενέργεια επιλέγεται με βάση τους κανόνες.

Η επιλογή **Απομνημόνευση μέχρι το κλείσιμο της εφαρμογής** προκαλεί τη χρήση μιας ενέργειας (**Αποδοχή/Δεν επιτρέπεται**) μέχρι να προκύψει αλλαγή κανόνων ή λειτουργίας φιλτραρίσματος, ενημέρωση της μονάδας HIPS ή επανεκκίνηση του συστήματος. Ύστερα από οποιαδήποτε από αυτές τις τρεις ενέργειες, οι προσωρινοί κανόνες θα διαγράφονται.

Η επιλογή **Δημιουργία κανόνα και μόνιμη απομνημόνευση** θα δημιουργήσει έναν νέο κανόνα HIPS, ο οποίος μπορεί να τροποποιηθεί αργότερα στην ενότητα Διαχείριση κανόνων HIPS (απαιτεί δικαιώματα διαχειριστή).

Κάντε κλικ στο στοιχείο **Λεπτομέρειες** στο κάτω μέρος για να δείτε ποια εφαρμογή ενεργοποιεί τη λειτουργία, τη φήμη του αρχείου ή το είδος λειτουργίας που σας ζητείται να επιτρέψετε ή να μην επιτρέψετε.

Για να αποκτήσετε πρόσβαση στις ρυθμίσεις για τις πιο λεπτομερείς παραμέτρους κανόνων κάντε κλικ στο στοιχείο **Επιλογές για προχωρημένους**. Οι παρακάτω επιλογές είναι διαθέσιμες εάν επιλέξετε **Δημιουργία κανόνα και μόνιμη απομνημόνευση**:

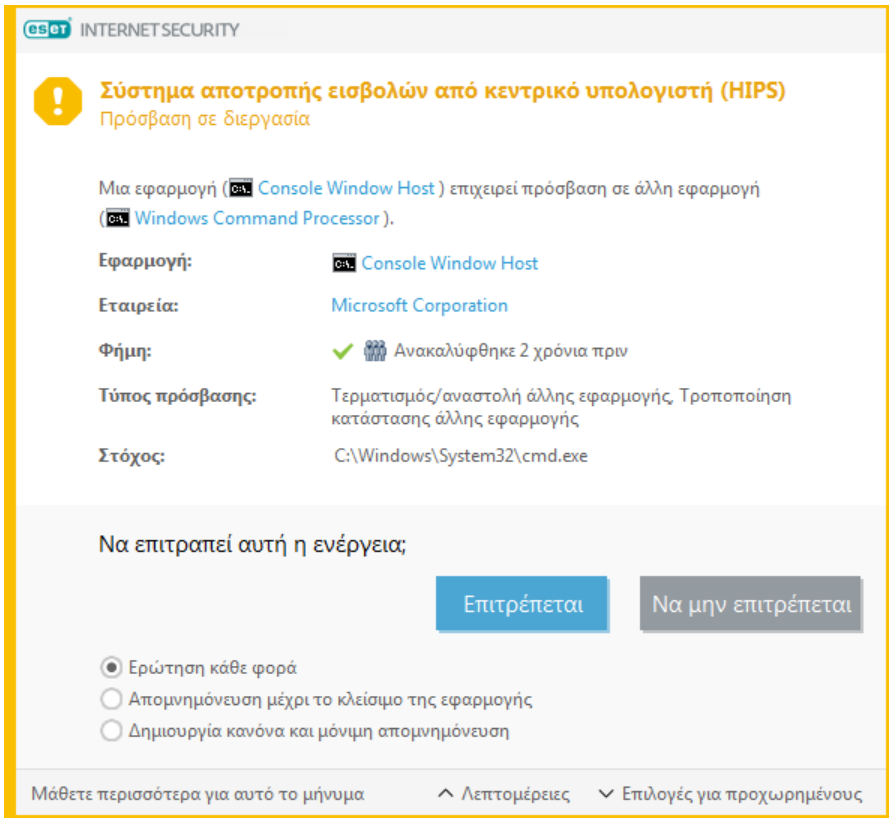
- **Δημιουργία κανόνα που ισχύει μόνο για αυτήν την εφαρμογή** – Εάν καταργήσετε την επιλογή του πλαισίου ελέγχου, ο κανόνας θα δημιουργηθεί για όλες τις εφαρμογές προέλευσης.

- **Μόνο για τη λειτουργία** – Επιλέξτε το αρχείο κανόνα/την εφαρμογή/τις λειτουργίες μητρώου. Ανατρέξτε στις περιγραφές για όλες τις λειτουργίες HIPS.

• **Μόνο για τον προορισμό** – Επιλέξτε το αρχείο κανόνα/την εφαρμογή/τους προορισμούς μητρώου.

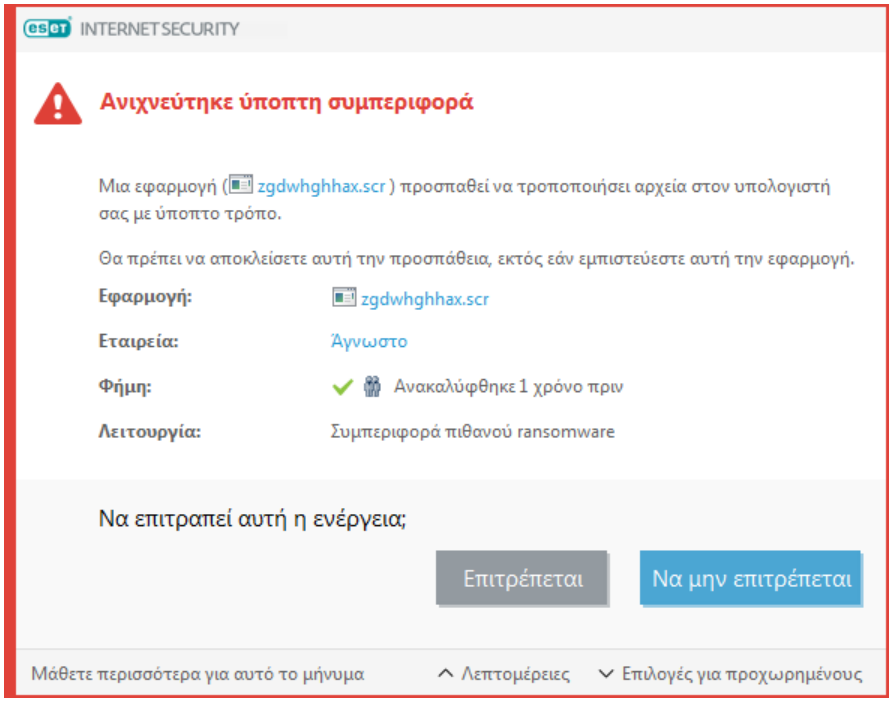
Αδιάκοπες ειδοποιήσεις HIPS;

Για να διακόψετε την εμφάνιση των ειδοποιήσεων, αλλάξτε τη λειτουργία φιλτραρίσματος σε **Αυτόματη λειτουργία** στο στοιχείο **Εγκατάσταση για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **HIPS** > **Βασικές ρυθμίσεις**.



Ανιχνεύτηκε συμπεριφορά πιθανού ransomware

Αυτό το αλληλεπιδραστικό παράθυρο θα εμφανίζεται όταν ανιχνεύεται συμπεριφορά πιθανού ransomware. Για τη λειτουργία μπορείτε να επιλέξετε **Δεν επιτρέπεται** ή **Επιτρέπεται**.



Κάντε κλικ στο στοιχείο **Λεπτομέρειες** για να δείτε συγκεκριμένες παραμέτρους ανίχνευσης. Το παράθυρο διαλόγου σάς επιτρέπει να κάνετε **Υποβολή για ανάλυση** ή **Εξαίρεση από τον εντοπισμό**.

Το ESET LiveGrid® πρέπει να έχει ενεργοποιηθεί για να λειτουργήσει σωστά η Προστασία ransomware.

Διαχείριση κανόνων HIPS

Μια λίστα κανόνων που καθορίζει ο χρήστης και προσθέτονται αυτόματα από το σύστημα HIPS. Μπορείτε να βρείτε περισσότερες λεπτομέρειες για τη δημιουργία κανόνων και τις λειτουργίες HIPS στο κεφάλαιο Ρυθμίσεις κανόνων HIPS. Επίσης, ανατρέξτε στην ενότητα Γενική αρχή του HIPS.

Στήλες

Κανόνας – Όνομα του κανόνα που καθορίζεται από το χρήστη ή επιλέγεται αυτόματα.

Ενεργός – Απενεργοποιήστε το ρυθμιστικό εάν θέλετε να διατηρήσετε τον κανόνα στη λίστα αλλά δεν θέλετε να τον χρησιμοποιήσετε.

Ενέργεια – Ο κανόνας καθορίζει μια ενέργεια – **Αποδοχή**, **Αποκλεισμός** ή **Ερώτηση** – που θα πρέπει να εκτελεστεί εάν ισχύουν οι κατάλληλες συνθήκες.

Προελεύσεις – Ο κανόνας θα χρησιμοποιείται μόνο εάν το συμβάν ενεργοποιηθεί από κάποια εφαρμογή.

Προορισμοί – Ο κανόνας θα χρησιμοποιηθεί μόνο εάν η λειτουργία σχετίζεται με ένα συγκεκριμένο αρχείο, εφαρμογή ή καταχώριση μητρώου.

Καταγραφή κρισιμότητας: – Εάν ενεργοποιήσετε αυτή την επιλογή, θα εγγραφούν πληροφορίες για αυτό τον κανόνα στο αρχείο καταγραφής HIPS.

Ειδοποίηση χρήστη – Εμφανίζεται ένα μικρό αναδυόμενο παράθυρο στην κάτω δεξιά γωνία αν ενεργοποιηθεί ένα συμβάν.

Στοιχεία ελέγχου

Προσθήκη – Δημιουργεί νέο κανόνα.

Επεξεργασία – Επιτρέπει την επεξεργασία επιλεγμένων καταχωρίσεων.

Διαγραφή – Καταργεί επιλεγμένες καταχωρίσεις.

Προτεραιότητα για τους κανόνες HIPS

Δεν υπάρχουν επιλογές για την προσαρμογή του επιπέδου προτεραιότητας των κανόνων HIPS χρησιμοποιώντας τα κουμπιά πάνω/κάτω (αναφορικά με τους Κανόνες τείχους προστασίας όπου οι κανόνες εκτελούνται από πάνω προς τα κάτω).

- Όλοι οι κανόνες που δημιουργείτε έχουν την ίδια προτεραιότητα
- Όσο πιο συγκεκριμένος είναι ένας κανόνας, τόσο υψηλότερη προτεραιότητα έχει (για παράδειγμα, ο κανόνας για μια συγκεκριμένη εφαρμογή έχει υψηλότερη προτεραιότητα σε σχέση με τον κανόνα για όλες τις εφαρμογές)
- Εσωτερικά, το HIPS περιέχει κανόνες υψηλότερης προτεραιότητας και ο χρήστης δεν έχει πρόσβαση σε αυτούς (για παράδειγμα, δεν μπορείτε να παρακάμψετε τους κανόνες αυτοπροστασίας)
- Ένας κανόνας που δημιουργείτε, ο οποίος μπορεί να παγώσει το λειτουργικό σύστημα, δεν θα εφαρμοστεί (θα έχει την χαμηλότερη προτεραιότητα)

Επεξεργασία ενός κανόνα HIPS

Δείτε πρώτα το θέμα Διαχείριση κανόνων HIPS.

Όνομα κανόνα – Όνομα του κανόνα που καθορίζεται από το χρήστη ή επιλέγεται αυτόματα.

Ενέργεια – Καθορίζει μια ενέργεια – **Αποδοχή**, **Αποκλεισμός** ή **Ερώτηση** – που θα πρέπει να εκτελεστεί εάν ισχύουν καθορισμένες συνθήκες.

Λειτουργίες που επηρεάζονται – Πρέπει να επιλέξετε τον τύπο λειτουργίας για τον οποίο θα ισχύει ο κανόνας. Ο κανόνας θα χρησιμοποιηθεί μόνο για αυτό τον τύπο λειτουργίας και για τον επιλεγμένο προορισμό.

Ενεργός – Απενεργοποιήστε αυτό το ρυθμιστικό εάν θέλετε να διατηρηθεί ο κανόνας στη λίστα αλλά να μην εφαρμόζεται.

Καταγραφή κρισιμότητας: – Εάν ενεργοποιήσετε αυτή την επιλογή, θα εγγραφούν πληροφορίες για αυτό τον κανόνα στο αρχείο καταγραφής HIPS.

Ειδοποίηση χρήστη – Εμφανίζεται ένα μικρό αναδυόμενο παράθυρο στην κάτω δεξιά γωνία εάν ενεργοποιηθεί ένα συμβάν.

Ο κανόνας αποτελείται από μέρη τα οποία περιγράφουν τις συνθήκες ενεργοποίησης αυτού του κανόνα:

Εφαρμογές προέλευσης– Ο κανόνας θα χρησιμοποιείται μόνο εάν ενεργοποιηθεί το συμβάν από αυτή ή αυτές τις εφαρμογές. Επιλέξτε **Συγκεκριμένες εφαρμογές** από το αναπτυσσόμενο μενού και κάντε κλικ στο στοιχείο **Προσθήκη** για να προσθέσετε νέα αρχεία ή μπορείτε να επιλέξετε **Όλες οι εφαρμογές** από το αναπτυσσόμενο μενού για να προσθέσετε όλες τις εφαρμογές.

Αρχεία προορισμού – Ο κανόνας θα χρησιμοποιηθεί μόνο εάν η λειτουργία σχετίζεται με αυτό τον προορισμό. Επιλέξτε **Συγκεκριμένα αρχεία** από το αναπτυσσόμενο μενού και κάντε κλικ στο στοιχείο **Προσθήκη** για να προσθέσετε νέα αρχεία ή φακέλους ή μπορείτε να επιλέξετε **Όλα τα αρχεία** από το αναπτυσσόμενο μενού για να προσθέσετε όλα τα αρχεία.

Εφαρμογές – Ο κανόνας θα χρησιμοποιηθεί μόνο εάν η λειτουργία σχετίζεται με αυτό τον προορισμό. Επιλέξτε **Συγκεκριμένες εφαρμογές** από το αναπτυσσόμενο μενού και κάντε κλικ στο στοιχείο **Προσθήκη** για να προσθέσετε νέα αρχεία ή φακέλους, ή μπορείτε να επιλέξετε **Όλες οι εφαρμογές** από το αναπτυσσόμενο μενού για να προσθέσετε όλες τις εφαρμογές.

Καταχωρίσεις μητρώου – Ο κανόνας θα χρησιμοποιηθεί μόνο εάν η λειτουργία σχετίζεται με αυτό τον προορισμό. Επιλέξτε **Συγκεκριμένες καταχωρίσεις** από το αναπτυσσόμενο μενού και κάντε κλικ στο στοιχείο **Προσθήκη** για να συμπληρώσετε τον κανόνα μη αυτόματα, ή μπορείτε να κάνετε κλικ στο στοιχείο **Άνοιγμα Επεξεργαστή Μητρώου** για να επιλέξετε ενα κλειδί από το Μητρώο. Επίσης, μπορείτε να επιλέξετε **Όλες οι καταχωρίσεις** από το αναπτυσσόμενο μενού, για να προσθέσετε όλες τις εφαρμογές.

> Ορισμένες λειτουργίες συγκεκριμένων κανόνων που είναι προκαθορισμένες από το HIPS δεν είναι δυνατόν να αποκλειστούν και επιτρέπονται από προεπιλογή. Επιπλέον, δεν παρακολουθούνται όλες οι λειτουργίες συστήματος από το HIPS. Το HIPS παρακολουθεί λειτουργίες που μπορεί να θεωρούνται μη ασφαλείς.

Περιγραφές σημαντικών λειτουργιών:

Λειτουργίες αρχείων

- **Διαγραφή αρχείου** – Η εφαρμογή ζητά άδεια για να διαγράψει το αρχείο προορισμού.

- **Εγγραφή σε αρχείο** – Η εφαρμογή ζητά άδεια για να κάνει εγγραφή στο αρχείο προορισμού.

- **Άμεση πρόσβαση στο δίσκο** – Η εφαρμογή προσπαθεί να διαβάσει από ή να γράψει στο δίσκο με μη τυπικό τρόπο, ο οποίος θα παρακάμψει συνηθισμένες διαδικασίες των Windows. Αυτό μπορεί να έχει σαν αποτέλεσμα τροποποίηση των αρχείων χωρίς την εφαρμογή αντίστοιχων κανόνων. Η λειτουργία αυτή μπορεί να προκληθεί από κακόβουλο λογισμικό που προσπαθεί να αποφύγει την ανίχνευση, από λογισμικό δημιουργίας αντιγράφων ασφαλείας που προσπαθεί να δημιουργήσει ένα ακριβές αντίγραφο δίσκου ή από μια εφαρμογή διαχείρισης διαμερισμάτων που προσπαθεί να αναδιοργανώσει τους τόμους του δίσκου.

- **Εγκατάσταση γενικού άγκιστρου** – Αναφέρεται στην κλήση της λειτουργίας SetWindowsHookExαπό τη βιβλιοθήκη MSDN.

- **Φόρτωση προγράμματος οδήγησης** – Εγκατάσταση και φόρτωση προγραμμάτων οδήγησης στο σύστημα.

Λειτουργίες εφαρμογών

• **Διόρθωση σφαλμάτων άλλης εφαρμογής** – Επισύναψη εφαρμογής διόρθωσης σφαλμάτων στη διεργασία. Κατά τη διόρθωση σφαλμάτων μιας εφαρμογής, είναι δυνατή η προβολή και η τροποποίηση πολλών λεπτομερειών της συμπεριφοράς της, καθώς και η πρόσβαση στα δεδομένα της.

• **Διακοπή συμβάντων από άλλη εφαρμογή** – Η εφαρμογή προορισμού προσπαθεί να πιάσει συμβάντα που έχουν στόχο μια συγκεκριμένη εφαρμογή (για παράδειγμα ένα πρόγραμμα καταγραφής πλήκτρων προσπαθεί να αποτυπώσει συμβάντα προγράμματος περιήγησης).

• **Τερματισμός/αναστολή άλλης εφαρμογής** – Αναστολή, συνέχιση ή τερματισμός μιας διεργασίας (η πρόσβαση μπορεί να γίνει απευθείας από το παράθυρο Εξερεύνησης διεργασιών ή Διεργασιών).

• **Έναρξη νέας εφαρμογής** – Έναρξη νέων εφαρμογών ή διεργασιών.

• **Τροποποίηση κατάστασης άλλης εφαρμογής** – Η εφαρμογή προέλευσης προσπαθεί να κάνει εγγραφή στη μνήμη των εφαρμογών προορισμού ή να εκτελέσει κώδικα για λογαριασμό της. Αυτή η λειτουργικότητα μπορεί να είναι χρήσιμη για την προστασία μιας απαραίτητης εφαρμογής αν τη διαμορφώσετε ως εφαρμογή προορισμού σε έναν κανόνα που αποκλείει τη χρήση αυτής της λειτουργίας.

Δεν είναι δυνατόν να διακοπούν λειτουργίες επεξεργασίας στην έκδοση 64-bit των Windows XP.

Λειτουργίες μητρώου

• **Τροποποίηση ρυθμίσεων εκκίνησης** – Οποιεσδήποτε αλλαγές ρυθμίσεων που καθορίζουν ποιες εφαρμογές θα εκτελούνται κατά την εκκίνηση των Windows. Αυτές βρίσκονται, για παράδειγμα, με αναζήτηση για κλειδί Run στο Μητρώο των Windows.

• **Διαγραφή από το μητρώο** – Διαγραφή ενός κλειδιού ή της τιμής μητρώου.

• **Μετονομασία κλειδιού μητρώου** – Μετονομασία κλειδιών μητρώου.

• **Τροποποίηση μητρώου** – Δημιουργία νέων τιμών κλειδιών μητρώου, αλλαγή υφιστάμενων τιμών, μετακίνηση δεδομένων στο δέντρο βάσης δεδομένων ή ρύθμιση δικαιωμάτων χρηστών ή ομάδων για κλειδιά μητρώου.

Μπορείτε να χρησιμοποιήσετε ειδικούς χαρακτήρες με ορισμένους περιορισμούς όταν εισαγάγετε έναν προορισμό. Αντί για ένα συγκεκριμένο κλειδί, μπορεί να χρησιμοποιηθεί το σύμβολο * (αστερίσκος) σε διαδρομές μητρώου. Για παράδειγμα το *HKEY_USERS*\software* μπορεί να σημαίνει *HKEY_USER\.default\software* αλλά όχι *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. Το *HKEY_LOCAL_MACHINE\system\ControlSet** δεν είναι έγκυρη διαδρομή κλειδιού μητρώου. Μια διαδρομή κλειδιού μητρώου που περιέχει * καθορίζει «αυτή τη διαδρομή, ή οποιαδήποτε διαδρομή σε οποιοδήποτε επίπεδο μετά από αυτό το σύμβολο». Αυτός είναι ο μόνος τρόπος χρήσης των ειδικών συμβόλων για αρχεία προορισμού. Πρώτα θα αξιολογηθεί το συγκεκριμένο μέρος μιας διαδρομής, μετά η διαδρομή που ακολουθεί το ειδικό σύμβολο (*).

Εάν δημιουργήσετε έναν πολύ γενικό κανόνα, θα εμφανιστεί η προειδοποίηση σχετικά με αυτό τον τύπο κανόνα.

Στο παρακάτω παράδειγμα, καταδεικνύεται πώς μπορείτε να περιορίσετε την ανεπιθύμητη συμπεριφορά μιας συγκεκριμένης εφαρμογής:

1. Ονομάστε τον κανόνα και επιλέξτε **Αποκλεισμός** (ή **Ερώτηση** εάν προτιμάτε να επιλέξετε αργότερα) από το αναπτυσσόμενο μενού **Ενέργεια**.

2. Επιλέξτε το διακόπτη που βρίσκεται δίπλα στο στοιχείο **Ειδοποίηση χρήστη** για να εμφανίζεται ειδοποίηση κάθε φορά που εφαρμόζεται ένας κανόνας.

3. Επιλέξτε τουλάχιστον μία λειτουργία στην ενότητα **Λειτουργίες που επηρεάζονται** στην οποία θα εφαρμοστεί ο κανόνας.

4. Κάντε κλικ στο στοιχείο **Επόμενο**.

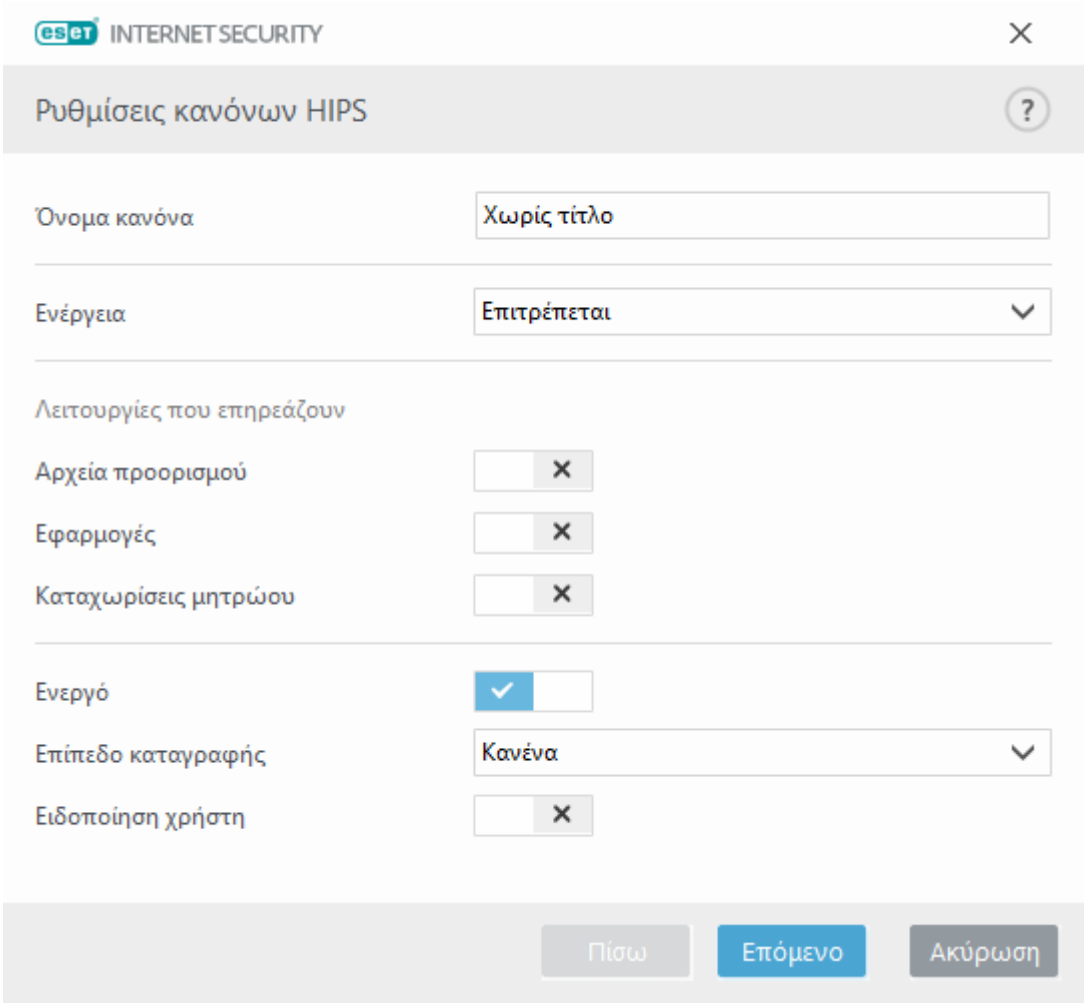
5. Στο παράθυρο **Εφαρμογές προέλευσης**, επιλέξτε **Συγκεκριμένες εφαρμογές** από το αναπτυσσόμενο μενού, για να εφαρμόσετε τον νέο κανόνα σε όλες τις εφαρμογές που επιχειρούν να πραγματοποιήσουν οποιαδήποτε από τις επιλεγμένες λειτουργίες στις εφαρμογές που καθορίσατε.

6. Κάντε κλικ στο στοιχείο **Προσθήκη** και, στη συνέχεια, στο στοιχείο **...** για να επιλέξετε μια διαδρομή σε μια συγκεκριμένη εφαρμογή, και μετά πατήστε το στοιχείο **OK**. Εάν θέλετε, προσθέστε περισσότερες εφαρμογές.
Για παράδειγμα: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Επιλέξτε τη λειτουργία **Εγγραφή σε αρχείο**.

8. Επιλέξτε το στοιχείο **Όλα τα αρχεία** από το αναπτυσσόμενο μενού. Αυτό θα αποκλείσει οποιεσδήποτε προσπάθειες εγγραφής σε οποιαδήποτε αρχεία από τις εφαρμογές που επιλέξατε στο προηγούμενο βήμα.

9. Κάντε κλικ στο κουμπί **Τέλος** για να αποθηκεύσετε τον νέο κανόνα.



Προσθήκη εφαρμογής/διαδρομής μητρώου για HIPS

Επιλέξτε μια διαδρομή εφαρμογής αρχείου κάνοντας κλικ στην επιλογή **...**. Όταν επιλέγετε έναν φάκελο, θα συμπεριληφθούν όλες οι εφαρμογές που βρίσκονται σε αυτή την τοποθεσία.

Με την επιλογή **Άνοιγμα Επεξεργαστή Μητρώου** θα εκκινήσει η επεξεργασία μητρώου των Windows (regedit). Όταν προσθέτετε μια διαδρομή μητρώου, εισαγάγετε τη σωστή τοποθεσία στο πεδίο **Τιμή**.

Παραδείγματα της διαδρομής αρχείου ή μητρώου:

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

Εγκατάσταση για προχωρημένους του HIPS

Οι ακόλουθες επιλογές είναι χρήσιμες για την εξάλειψη σφαλμάτων και την ανάλυση της συμπεριφοράς μιας εφαρμογής:

Επιτρέπεται πάντα η φόρτωση προγραμμάτων οδήγησης – Επιτρέπεται πάντα η φόρτωση

ορισμένων προγραμμάτων οδήγησης ανεξάρτητα από τη διαμόρφωση της λειτουργίας φιλτραρίσματος, εκτός εάν αποκλείονται ρητά από κάποιον κανόνα του χρήστη.

Καταγραφή όλων των αποκλεισμένων λειτουργιών - Όλες οι αποκλεισμένες λειτουργίες θα εγγραφούν στο αρχείο καταγραφής HIPS. Χρησιμοποιήστε αυτήν τη δυνατότητα μόνο κατά την αντιμετώπιση προβλημάτων ή εάν σας ζητηθεί από την Τεχνική υποστήριξη της ESET, επειδή μπορεί να δημιουργήσει ένα τεράστιο αρχείο καταγραφής και να επιβραδύνει τον υπολογιστή σας.

Ειδοποίηση όταν σημειώνονται αλλαγές στις εφαρμογές εκκίνησης – Εμφανίζει μια ειδοποίηση επιφάνειας εργασίας κάθε φορά που προστίθεται ή αφαιρείται μια εφαρμογή από την εκκίνηση του συστήματος.

Επιτρέπεται πάντα η φόρτωση προγραμμάτων οδήγησης

Επιτρέπεται πάντα η φόρτωση των προγραμμάτων οδήγησης που εμφανίζονται σε αυτήν τη λίστα, ανεξάρτητα από τη λειτουργία φιλτραρίσματος HIPS, εκτός εάν αποκλείονται ρητά από κάποιον κανόνα του χρήστη.

Προσθήκη – Δημιουργεί νέο πρόγραμμα οδήγησης.

Επεξεργασία – Επιτρέπει την επεξεργασία του επιλεγμένου προγράμματος οδήγησης.

Κατάργηση – Αφαιρεί το πρόγραμμα οδήγησης από τη λίστα.

Επαναφορά – Επαναφορτώνει ένα σύνολο προγραμμάτων οδήγησης του συστήματος.

> Κάντε κλικ στο στοιχείο **Επαναφορά** εάν δεν θέλετε να συμπεριλαμβάνονται προγράμματα οδήγησης που έχετε προσθέσει εσείς οι ίδιοι. Αυτό μπορεί να είναι χρήσιμο εάν έχετε προσθέσει διάφορα προγράμματα οδήγησης και δεν μπορείτε να τα διαγράψετε από τη λίστα.

Λειτουργία Gamer

Η λειτουργία Gamer είναι μια δυνατότητα για χρήστες που απαιτούν αδιάλειπτη χρήση του λογισμικού τους, δεν θέλουν να διακόπτονται από αναδυόμενα παράθυρα και θέλουν να ελαχιστοποιήσουν τη χρήση της μονάδας CPU. Η λειτουργία Gamer μπορεί να χρησιμοποιηθεί επίσης κατά τη διάρκεια παρουσιάσεων που δεν πρέπει να διακόπτονται από δραστηριότητα antivirus. Εάν ενεργοποιήσετε αυτήν τη δυνατότητα, απενεργοποιούνται όλα τα αναδυόμενα παράθυρα και θα διακοπεί εντελώς η δραστηριότητα του χρονοδιαγράμματος. Η προστασία συστήματος εξακολουθεί να λειτουργεί στο παρασκήνιο αλλά δεν απαιτεί καμία αλληλεπίδραση με τον χρήστη.

Μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τη λειτουργία Gamer στο κύριο παράθυρο του προγράμματος στην ενότητα **Ρυθμίσεις** > **Προστασία υπολογιστή** κάνοντας κλικ στο στοιχείο  ή στο στοιχείο  που βρίσκεται δίπλα στην επιλογή **Λειτουργία Gamer**. Η ενεργοποίηση της Λειτουργίας Gamer είναι πιθανός κίνδυνος για την ασφάλεια, για αυτό το εικονίδιο κατάστασης προστασίας στη γραμμή εργασιών θα γίνει πορτοκαλί και θα εμφανιστεί μια προειδοποίηση. Επίσης, θα δείτε αυτή την προειδοποίηση στο κύριο παράθυρο του προγράμματος, όπου εμφανίζεται η ένδειξη **Η λειτουργία Gamer ενεργοποιήθηκε** με πορτοκαλί χρώμα.

Ενεργοποιήστε το στοιχείο **Αυτόματη ενεργοποίηση λειτουργίας Gamer κατά την εκτέλεση εφαρμογών σε πλήρη οθόνη** στην ενότητα **Ρυθμίσεις για προχωρημένους** (F5) > **Εργαλεία** > **Λειτουργία Gamer** προκειμένου η λειτουργία Gamer να ξεκινά όταν εκκινείτε μια εφαρμογή σε πλήρη οθόνη και να σταματά μετά την έξοδό σας από την εφαρμογή.

Ενεργοποιήστε την **Αυτόματη απενεργοποίηση λειτουργίας Gamer ύστερα από** για να ορίσετε το χρονικό διάστημα μετά από το οποίο θα απενεργοποιείται αυτόματα η λειτουργία Gamer.

> Αν το Firewall βρίσκεται σε Αλληλεπιδραστική λειτουργία και είναι ενεργοποιημένη η Λειτουργία Gamer, μπορεί να παρουσιαστούν προβλήματα στη σύνδεση με το Διαδίκτυο. Αυτό μπορεί να αποτελέσει πρόβλημα αν ξεκινήσετε ένα παιχνίδι που συνδέεται με το Διαδίκτυο. Κανονικά, θα έπρεπε να επιβεβαιώσετε μια τέτοια ενέργεια (αν δεν έχουν καθοριστεί κανόνες ή εξαιρέσεις επικοινωνίας), αλλά στη Λειτουργία Gamer απενεργοποιείται η αλληλεπίδραση με τον χρήστη. Για να επιτρέπεται η επικοινωνία, καθορίστε έναν κανόνα επικοινωνιών για όποια εφαρμογή ενδέχεται να αντιμετωπίζει αυτό το ζήτημα ή χρησιμοποιήστε διαφορετική Λειτουργία φιλτραρίσματος στο Firewall. Να θυμάστε ότι, εάν η Λειτουργία Gamer είναι ενεργοποιημένη και μεταβείτε σε μια ιστοσελίδα ή σε μια εφαρμογή που μπορεί να αποτελεί κίνδυνο για την ασφάλεια, μπορεί να αποκλειστεί καμία επεξήγηση ή προειδοποίηση, επειδή η αλληλεπίδραση με τον χρήστη είναι απενεργοποιημένη.

Σάρωση κατά την εκκίνηση

Από προεπιλογή ο αυτόματος έλεγχος κατά την εκκίνηση θα εκτελείται κατά την εκκίνηση του συστήματος και κατά τη διάρκεια των ενημερώσεων του μηχανισμού ανίχνευσης. Αυτή η σάρωση εξαρτάται από τη Διαμόρφωση του Χρονοδιαγράμματος και των εργασιών.

Οι επιλογές σάρωσης κατά την εκκίνηση αποτελούν μέρος της εργασίας χρονοδιαγράμματος **Έλεγχος αρχείων κατά την εκκίνηση του συστήματος**. Για να τροποποιήσετε τις ρυθμίσεις της εργασίας, μεταβείτε στη θέση **Εργαλεία** > **Περισσότερα εργαλεία** > **Χρονοδιάγραμμα**, κάντε κλικ στην επιλογή **Αυτόματος έλεγχος αρχείων κατά την εκκίνηση** και κατόπιν **Επεξεργασία**. Στο τελευταίο βήμα θα εμφανιστεί το παράθυρο Αυτόματος έλεγχος αρχείων κατά την εκκίνηση (για περισσότερες λεπτομέρειες δείτε το παρακάτω κεφάλαιο).

Για λεπτομερείς οδηγίες σχετικά με τη δημιουργία εργασίας χρονοδιαγράμματος και τη διαχείριση, δείτε την ενότητα Δημιουργία νέων εργασιών.

Αυτόματος έλεγχος αρχείων κατά την εκκίνηση

Όταν δημιουργείτε μια προγραμματισμένη εργασία για τον έλεγχο αρχείων κατά την εκκίνηση του συστήματος, έχετε διάφορες επιλογές για να ρυθμίσετε τις παρακάτω παραμέτρους:

Το αναπτυσσόμενο μενού **Προορισμός σάρωσης** καθορίζει το βάθος σάρωσης για αρχεία που εκτελούνται κατά την εκκίνηση του συστήματος βάσει μυστικού πρωτοποριακού αλγόριθμου. Τα αρχεία διευθετούνται σε φθίνουσα σειρά, σύμφωνα με τα παρακάτω κριτήρια:

- **Όλα τα εγγεγραμμένα αρχεία** (σάρωση των περισσότερων αρχείων)

- **Αρχεία που χρησιμοποιούνται σπάνια**
- **Αρχεία που χρησιμοποιούνται συνήθως**
- **Αρχεία που χρησιμοποιούνται συχνά**
- **Μόνο τα αρχεία που χρησιμοποιούνται συχνότερα** (σάρωση των λιγότερων αρχείων)

Επίσης περιλαμβάνονται δύο ειδικές ομάδες:

- **Αρχεία που εκτελούνται πριν από τη σύνδεση του χρήστη** – Περιέχει αρχεία από θέσεις στις οποίες η πρόσβαση είναι δυνατή χωρίς σύνδεση του χρήστη (περιλαμβάνει όλες τις θέσεις εκκίνησης, όπως υπηρεσίες, ειδοποιήσεις σύνδεσης στα Windows, καταχωρίσεις χρονοδιαγράμματος των Windows, γνωστές βιβλιοθήκες dll κ.λπ.).

- **Αρχεία που εκτελούνται μετά τη σύνδεση του χρήστη** - Περιέχει αρχεία από θέσεις στις οποίες η πρόσβαση είναι δυνατή μόνο μετά τη σύνδεση του χρήστη (περιλαμβάνει αρχεία που εκτελούνται μόνο από συγκεκριμένο χρήστη, συνήθως αρχεία στη θέση *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Οι λίστες των αρχείων που θα σαρωθούν καθορίζονται για κάθε μία από τις παραπάνω ομάδες. Εάν επιλέξετε χαμηλότερο βάθος σάρωσης για αρχεία που εκτελούνται κατά την εκκίνηση του συστήματος, τα αρχεία που δεν έχουν σαρωθεί θα σαρωθούν κατά το άνοιγμα ή την εκτέλεση.

Προτεραιότητα σάρωσης – Το επίπεδο προτεραιότητας που χρησιμοποιείται για τον προσδιορισμό του χρόνου έναρξης σάρωσης:

- **Σε αδράνεια** – η εργασία πραγματοποιείται μόνο όταν το σύστημα βρίσκεται σε κατάσταση αδράνειας,
- **Ελάχιστη** – όταν ο φόρτος συστήματος είναι ο χαμηλότερος δυνατός,
- **Χαμηλή** – σε χαμηλό φόρτο συστήματος,
- **Κανονική** – σε μέτριο φόρτο συστήματος.

Προστασία εγγράφων

Η δυνατότητα Προστασίας εγγράφων σαρώνει τα έγγραφα του Microsoft Office προτού ανοιχτούν, καθώς και αρχεία που λαμβάνονται αυτόματα από τον Internet Explorer, όπως στοιχεία Microsoft ActiveX . Η προστασία εγγράφων παρέχει ένα επίπεδο προστασίας εκτός από την προστασία συστήματος αρχείων σε πραγματικό χρόνο και μπορεί να απενεργοποιηθεί για να ενισχυθεί η απόδοση σε συστήματα που δεν χειρίζονται μεγάλο αριθμό εγγράφων του Microsoft Office.

Για να ενεργοποιήσετε την Προστασία εγγράφων, ανοίξτε τα στοιχεία **Εγκατάσταση για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **Σαρώσεις για κακόβουλο λογισμικό** > **Προστασία εγγράφων** και κάντε κλικ στο ρυθμιστικό **Ενεργοποίηση Προστασίας εγγράφων**.

> Αυτή η δυνατότητα ενεργοποιείται από εφαρμογές που χρησιμοποιούν το Microsoft Antivirus API (για παράδειγμα, Microsoft Office 2000 και νεότερες εκδόσεις ή Microsoft Internet Explorer 5.0 και νεότερες εκδόσεις).

Εξαιρέσεις

Οι **Εξαιρέσεις** σάς επιτρέπουν να εξαιρείτε αντικείμενα από το μηχανισμό ανίχνευσης. Για να διασφαλίζεται η σάρωση όλων των αντικειμένων, συνιστάται να δημιουργείτε εξαιρέσεις μόνο όταν είναι απολύτως απαραίτητο. Οι περιπτώσεις στις οποίες μπορεί να χρειαστεί να εξαιρέσετε ένα αντικείμενο μπορεί να περιλαμβάνουν τη σάρωση καταχωρίσεων μεγάλων βάσεων δεδομένων, οι οποίες μπορεί να επιβραδύνουν τον υπολογιστή σας κατά τη σάρωση ή λογισμικό που παρουσιάζει διενέξεις με τη σάρωση.

Οι Εξαιρέσεις επιδόσεων σάς επιτρέπουν να εξαιρείτε αρχεία και φακέλους από τη σάρωση. Οι εξαιρέσεις επιδόσεων είναι χρήσιμες για την εξαίρεση σάρωσης σε επίπεδο αρχείων σε εφαρμογές παιχνιδιών ή όταν προκαλούν μη αναμενόμενη συμπεριφορά στο σύστημα ή αυξημένες επιδόσεις.

Οι Εξαιρέσεις ανίχνευσης σάς επιτρέπουν να εξαιρείτε αντικείμενα από την ανίχνευση χρησιμοποιώντας το όνομα, τη διαδρομή ή τον κατακερματισμό της ανίχνευσης. Οι εξαιρέσεις ανίχνευσης δεν εξαιρούν αρχεία και φακέλους από την σάρωση, όπως συμβαίνει με τις Εξαιρέσεις επιδόσεων. Οι εξαιρέσεις ανίχνευσης εξαιρούν αντικείμενα μόνο όταν ανιχνεύονται από τον μηχανισμό ανίχνευσης και υπάρχει ένας κατάλληλος κανόνας στη λίστα εξαιρέσεων.

Δεν πρέπει να τις συγχέετε με άλλους τύπους εξαιρέσεων:

- Εξαιρέσεις διεργασίας – Όλες οι λειτουργίες αρχείων που αποδίδονται σε διεργασίες εξαίρεσης εφαρμογών εξαιρούνται από τη σάρωση (ενδέχεται να απαιτούνται για τη βελτίωση της ταχύτητας δημιουργίας αντιγράφων ασφαλείας και διαθεσιμότητας υπηρεσίας).
- Εξαιρούμενες επεκτάσεις αρχείων
- Εξαιρέσεις HIPS
- Φίλτρο εξαίρεσης για προστασία που βασίζεται σε cloud

Εξαιρέσεις επιδόσεων

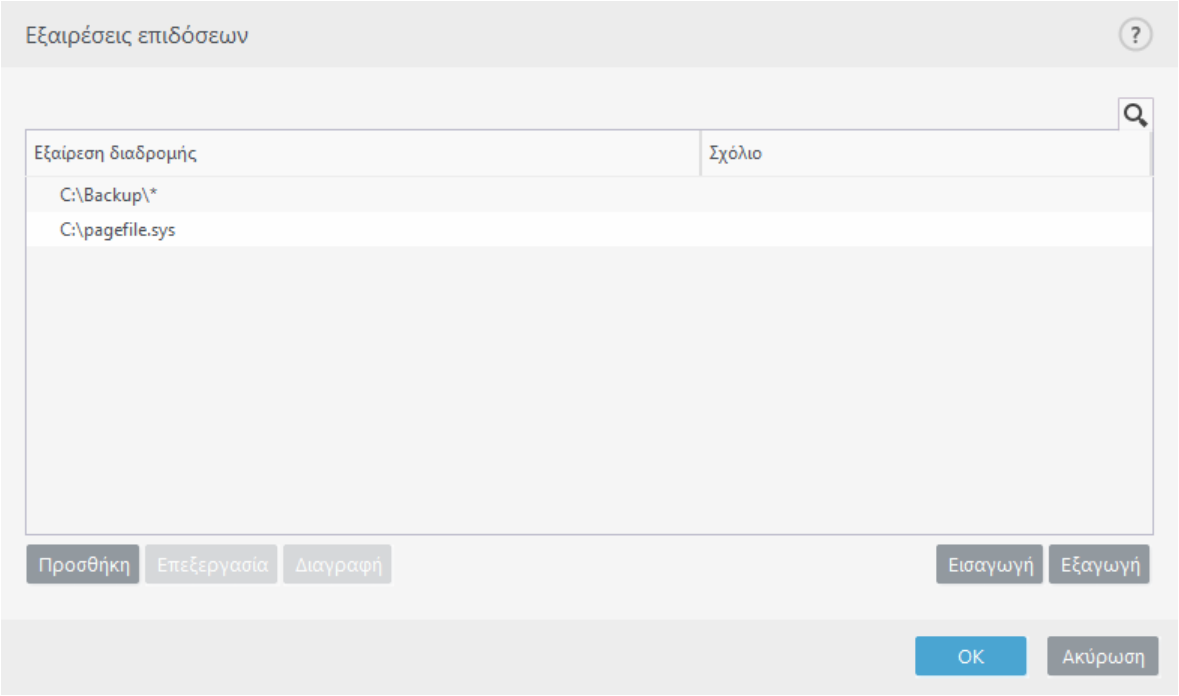
Οι εξαιρέσεις επιδόσεων σάς επιτρέπουν να εξαιρείτε αρχεία και φακέλους από τη σάρωση.

Για να διασφαλίζεται η σάρωση όλων των αντικειμένων για απειλές, συνιστάται να δημιουργείτε εξαιρέσεις μόνο όταν είναι απολύτως απαραίτητο. Ωστόσο, υπάρχουν περιπτώσεις που μπορεί να χρειάζεται να εξαιρέσετε ένα αντικείμενο, για παράδειγμα καταχωρίσεις μεγάλων βάσεων δεδομένων που θα επιβραδύνουν τον υπολογιστή σας κατά τη σάρωση ή λογισμικό που παρουσιάζει διενέξεις με τη σάρωση.

Μπορείτε να προσθέσετε αρχεία και φακέλους που θα εξαιρούνται από τη σάρωση στη λίστα εξαιρέσεων μέσω της διαδρομής **Εγκατάσταση για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **Εξαιρέσεις** > **Εξαιρέσεις επιδόσεων** > **Επεξεργασία**.

> Μη συγχέετε τα στοιχεία Εξαιρέσεις ανιχνεύσεων, Εξαιρούμενες επεκτάσεις αρχείων, Εξαιρέσεις HIPS ή Εξαιρέσεις διεργασιών.

Για να εξαιρέσετε ένα αντικείμενο (διαδρομή: αρχείο ή φάκελος) από τη σάρωση, κάντε κλικ στο στοιχείο **Προσθήκη** και εισαγάγετε την ισχύουσα διαδρομή ή επιλέξτε τη στη δομή δέντρου.



> Αν ένα αρχείο πληροί τα κριτήρια εξαίρεσης από τη σάρωση, δεν θα ανιχνευτεί μια απειλή που βρίσκεται σε αυτό το αρχείο από τη μονάδα **Προστασία συστήματος αρχείων σε πραγματικό χρόνο** ή από τη μονάδα **Σάρωση υπολογιστή**.

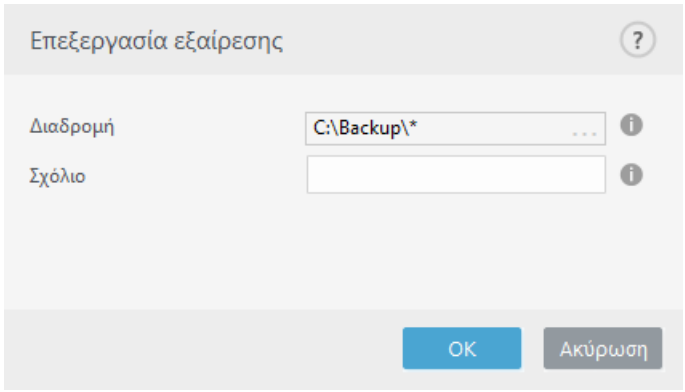
Στοιχεία ελέγχου

- **Προσθήκη** – Εξαιρεί αντικείμενα από τον εντοπισμό.
- **Επεξεργασία** – Επιτρέπει την επεξεργασία επιλεγμένων καταχωρίσεων.
- **Κατάργηση** – Καταργεί επιλεγμένες καταχωρίσεις (πατήστε CTRL + κλικ για να επιλέξετε πολλαπλές καταχωρίσεις).

Προσθήκη ή επεξεργασία εξαίρεσης επιδόσεων

Αυτό το παράθυρο διαλόγου εξαιρεί μια συγκεκριμένη διαδρομή (αρχείο ή κατάλογο) για αυτό τον υπολογιστή.

> Επιλέξτε τη διαδρομή ή εισαγάγετέ τη μη αυτόματα
> Για να επιλέξετε την κατάλληλη διαδρομή, κάντε κλικ στο στοιχείο **...** στο πεδίο **Διαδρομή**. Εάν κάνετε μη αυτόματη εισαγωγή, δείτε περισσότερα παραδείγματα μορφής εξαίρεσης παρακάτω.



Μπορείτε να χρησιμοποιήσετε ειδικούς χαρακτήρες για να εξαιρέσετε μια ομάδα αρχείων. Το αγγλικό ερωτηματικό (*?*) αντιπροσωπεύει έναν μεμονωμένο χαρακτήρα, ενώ ο αστερίσκος (***) αντιπροσωπεύει μια συμβολοσειρά που αποτελείται από κανέναν ή περισσότερους χαρακτήρες.

Μορφή εξαίρεσης

- Εάν θέλετε να εξαιρέσετε όλα τα αρχεία και τους υποφακέλους που βρίσκονται σε έναν φάκελο, πληκτρολογήστε τη διαδρομή προς τον φάκελο και χρησιμοποιήστε τη μάσκα ***
- Εάν θέλετε να εξαιρέσετε μόνο αρχεία doc, χρησιμοποιήστε τη μάσκα **.doc*
- Εάν το όνομα κάποιου εκτελέσιμου αρχείου περιέχει συγκεκριμένο αριθμό χαρακτήρων (με διάφορους χαρακτήρες) και γνωρίζετε μόνο τον πρώτο χαρακτήρα (για παράδειγμα, «D»), χρησιμοποιήστε την ακόλουθη μορφή:
D????.exe (τα Λατινικά ερωτηματικά αντικαθιστούν τους χαρακτήρες που λείπουν/είναι άγνωστοι)

Παραδείγματα:

- *C:\Tools** – Η διαδρομή πρέπει να τελειώνει με την ανάστροφη κάθετο (\) και τον αστερίσκο (*) για να υποδεικνύεται ότι πρόκειται για έναν φάκελο και ότι θα εξαιρείται το σύνολο του περιεχομένου του φακέλου (αρχεία και υποφάκελοι).
- *C:\Tools*.** – Ίδια συμπεριφορά με το *C:\Tools**
- *C:\Tools* – Ο φάκελος *Tools* δεν θα εξαιρεθεί. Από την άποψη της σάρωσης, το *Tools* μπορεί να είναι και όνομα αρχείου.
- *C:\Tools*.dat* – Αυτό θα εξαιρέσει τα αρχεία .dat στο φάκελο *Tools*.
- *C:\Tools\sg.dat* - Αυτό θα εξαιρέσει το συγκεκριμένο αρχείο που βρίσκεται σε αυτήν ακριβώς τη διαδρομή.

Μεταβλητές συστήματος σε εξαιρέσεις

Μπορείτε να χρησιμοποιήσετε μεταβλητές συστήματος όπως το %PROGRAMFILES% για να καθορίσετε εξαιρέσεις σάρωσης.

• Για να εξαιρέσετε το φάκελο «Αρχεία εφαρμογών» χρησιμοποιώντας αυτή τη μεταβλητή, χρησιμοποιήστε τη διαδρομή *%PROGRAMFILES%** (μη ξεχάσετε να προσθέσετε την ανάστροφη κάθετο και τον αστερίσκο στο τέλος της διαδρομής) όταν κάνετε προσθήκη στις εξαιρέσεις.

• Για να εξαιρέσετε όλα τα αρχεία και τους φακέλους σε έναν υποκατάλογο *%PROGRAMFILES%*, χρησιμοποιήστε τη διαδρομή *%PROGRAMFILES%*\Εξαιρούμενος_Κατάλογος*

Ανάπτυξη λίστας των υποστηριζόμενων μεταβλητών συστήματος

Οι ακόλουθες μεταβλητές μπορούν να χρησιμοποιηθούν στη μορφή εξαίρεσης διαδρομής:

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

Δεν υποστηρίζονται μεταβλητές ειδικές για το χρήστη (όπως *%TEMP%* ή *%USERPROFILE%*) ή μεταβλητές περιβάλλοντος (όπως *%PATH%*).

Οι χαρακτήρες wildcard στην μέση μιας διαδρομής δεν υποστηρίζονται

Η χρήση χαρακτήρων wildcard στη μέση μιας διαδρομής (για παράδειγμα *C:\Tools*\Data\file.dat*) μπορεί να λειτουργήσει, αλλά δεν υποστηρίζεται επίσημα για τις εξαιρέσεις επιδόσεων. Για περισσότερες πληροφορίες, ανατρέξτε στο ακόλουθο άρθρο της Γνωσιακής βάσης.

Δεν υπάρχουν περιορισμοί για τη χρήση ειδικών χαρακτήρων στο μέσο της διαδρομής όταν χρησιμοποιείτε εξαιρέσεις ανίχνευσης.

Σειρά εξαιρέσεων

• Δεν υπάρχουν επιλογές για την προσαρμογή του επιπέδου προτεραιότητας των εξαιρέσεων χρησιμοποιώντας τα κουμπιά πάνω/κάτω (αναφορικά με τους Κανόνες τείχους προστασίας όπου οι κανόνες εκτελούνται από πάνω προς τα κάτω).

• Όταν ο πρώτος κανόνας που εφαρμόζεται αντιστοιχιστεί από τη σάρωση, δεν θα αξιολογηθεί ο δεύτερος κανόνας που εφαρμόζεται.

• Όσο λιγότεροι είναι οι κανόνες, τόσο καλύτερη είναι η απόδοση της σάρωσης.

• Αποφεύγετε τη δημιουργία ταυτόχρονων κανόνων.

Μορφή εξαίρεσης διαδρομής

Μπορείτε να χρησιμοποιήσετε ειδικούς χαρακτήρες για να εξαιρέσετε μια ομάδα αρχείων. Το αγγλικό ερωτηματικό (*?*) αντιπροσωπεύει έναν μεμονωμένο χαρακτήρα, ενώ ο αστερίσκος (***) αντιπροσωπεύει μια συμβολοσειρά που αποτελείται από κανέναν ή περισσότερους χαρακτήρες.

Μορφή εξαίρεσης

• Εάν θέλετε να εξαιρέσετε όλα τα αρχεία και τους υποφακέλους που βρίσκονται σε έναν φάκελο, πληκτρολογήστε τη διαδρομή προς τον φάκελο και χρησιμοποιήστε τη μάσκα *
• Εάν θέλετε να εξαιρέσετε μόνο αρχεία doc, χρησιμοποιήστε τη μάσκα **.doc*
• Εάν το όνομα κάποιου εκτελέσιμου αρχείου περιέχει συγκεκριμένο αριθμό χαρακτήρων (με διάφορους χαρακτήρες) και γνωρίζετε μόνο τον πρώτο χαρακτήρα (για παράδειγμα, «D»), χρησιμοποιήστε την ακόλουθη μορφή:
D????.exe (τα Λατινικά ερωτηματικά αντικαθιστούν τους χαρακτήρες που λείπουν/είναι άγνωστοι)

✓ Παραδείγματα:

• *C:\Tools** – Η διαδρομή πρέπει να τελειώνει με την ανάστροφη κάθετο (\) και τον αστερίσκο (*) για να υποδεικνύεται ότι πρόκειται για έναν φάκελο και ότι θα εξαιρείται το σύνολο του περιεχομένου του φακέλου (αρχεία και υποφάκελοι).
• *C:\Tools*.** – Ίδια συμπεριφορά με το *C:\Tools**
• *C:\Tools* – Ο φάκελος *Tools* δεν θα εξαιρεθεί. Από την άποψη της σάρωσης, το *Tools* μπορεί να είναι και όνομα αρχείου.
• *C:\Tools*.dat* – Αυτό θα εξαιρέσει τα αρχεία .dat στο φάκελο *Tools*.
• *C:\Tools\sg.dat* - Αυτό θα εξαιρέσει το συγκεκριμένο αρχείο που βρίσκεται σε αυτήν ακριβώς τη διαδρομή.

Μεταβλητές συστήματος σε εξαιρέσεις

Μπορείτε να χρησιμοποιήσετε μεταβλητές συστήματος όπως το %PROGRAMFILES% για να καθορίσετε εξαιρέσεις σάρωσης.
• Για να εξαιρέσετε το φάκελο «Αρχεία εφαρμογών» χρησιμοποιώντας αυτή τη μεταβλητή, χρησιμοποιήστε τη διαδρομή *%PROGRAMFILES%** (μη ξεχάσετε να προσθέσετε την ανάστροφη κάθετο και τον αστερίσκο στο τέλος της διαδρομής) όταν κάνετε προσθήκη στις εξαιρέσεις.
• Για να εξαιρέσετε όλα τα αρχεία και τους φακέλους σε έναν υποκατάλογο *%PROGRAMFILES%*, χρησιμοποιήστε τη διαδρομή *%PROGRAMFILES%*\Εξαιρούμενος_Κατάλογος*

Ανάπτυξη λίστας των υποστηριζόμενων μεταβλητών συστήματος

Οι ακόλουθες μεταβλητές μπορούν να χρησιμοποιηθούν στη μορφή εξαίρεσης διαδρομής:

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

Δεν υποστηρίζονται μεταβλητές ειδικές για το χρήστη (όπως *%TEMP%* ή *%USERPROFILE%*) ή μεταβλητές περιβάλλοντος (όπως *%PATH%*).

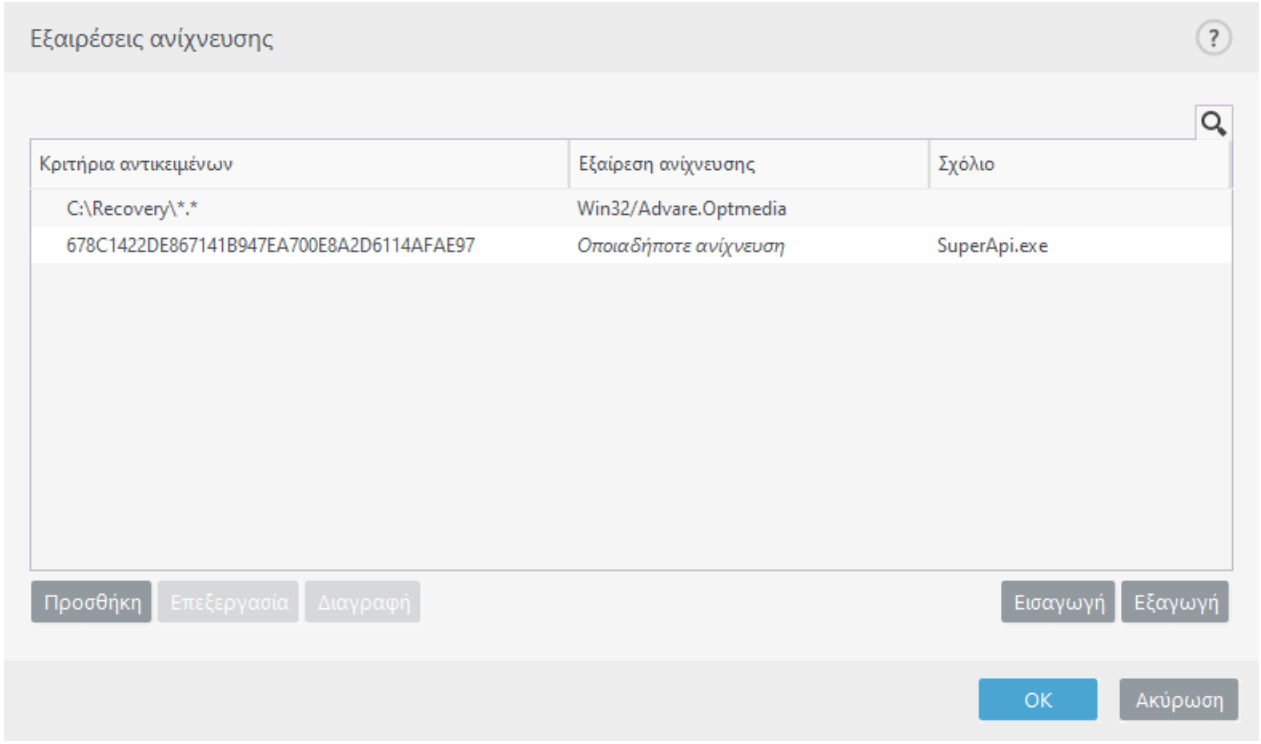
Εξαιρέσεις ανίχνευσης

Οι εξαιρέσεις ανίχνευσης σάς επιτρέπουν να εξαιρείτε αντικείμενα από την ανίχνευση φιλτράροντας το όνομα ανίχνευσης, τη διαδρομή του αντικειμένου ή τον κατακερματισμό του.

Πώς λειτουργούν οι εξαιρέσεις ανίχνευσης

Οι εξαιρέσεις ανίχνευσης δεν εξαιρούν αρχεία και φακέλους από την ανίχνευση όπως συμβαίνει με τις Εξαιρέσεις επιδόσεων. Οι εξαιρέσεις ανίχνευσης εξαιρούν αντικείμενα μόνο όταν ανιχνεύονται από τον μηχανισμό ανίχνευσης και υπάρχει ένας κατάλληλος κανόνας στη λίστα εξαιρέσεων.

Για παράδειγμα, (δείτε την πρώτη σειρά στην παρακάτω εικόνα), όταν ένα αντικείμενο ανιχνεύεται ως Win32/Adware.Optmedia και το ανιχνευμένο αρχείο είναι *C:\Recovery\file.exe*. Στη δεύτερη σειρά, κάθε αρχείο, το οποίο έχει τον κατάλληλο κατακερματισμό SHA-1, θα εξαιρείται πάντα παρά το όνομα ανίχνευσης.



Για να διασφαλίζεται ότι ανιχνεύονται όλες οι απειλές, συνιστάται η δημιουργία εξαιρέσεων ανίχνευσης μόνο όταν είναι απολύτως απαραίτητο.

Για να προσθέσετε αρχεία και φακέλους στη λίστα εξαιρέσεων, μεταβείτε στη διαδρομή **Εγκατάσταση για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **Εξαιρέσεις** > **Εξαιρέσεις ανίχνευσης** > **Επεξεργασία**.

Μη συγχέετε τα στοιχεία Εξαιρέσεις επιδόσεων, Εξαιρούμενες επεκτάσεις αρχείων, Εξαιρέσεις HIPS ή Εξαιρέσεις διεργασιών.

Για να εξαιρέσετε ένα αντικείμενο (με το όνομα ανίχνευσης ή τον κατακερματισμό του) από το μηχανισμό ανίχνευσης, κάντε κλικ στο στοιχείο **Προσθήκη**.

Για Ενδεχομένως ανεπιθύμητες εφαρμογές και Ενδεχομένως μη ασφαλείς εφαρμογές, μπορεί να δημιουργηθεί επίσης μια εξαίρεση με το όνομα ανίχνευσης:

- Στο παράθυρο συναγερμού όπου αναφέρεται η ανίχνευση (κάντε κλικ στο στοιχείο **Εμφάνιση επιλογών για προχωρημένους** και, στη συνέχεια, επιλέξτε το στοιχείο **Εξαίρεση από την ανίχνευση**).

- Από το μενού περιβάλλοντος «Αρχεία καταγραφής» χρησιμοποιώντας τον Οδηγό δημιουργίας εξαίρεσης ανίχνευσης.

• Κάντε κλικ στο στοιχείο **Εργαλεία** > **Περισσότερα εργαλεία** > **Καραντίνα**, κατόπιν κάντε δεξί κλικ στο αρχείο που απομονώθηκε στην καραντίνα και στη συνέχεια επιλέξτε **Επαναφορά και εξαίρεση από τη σάρωση** από το μενού περιβάλλοντος.

Κριτήρια αντικειμένων εξαιρέσεων ανίχνευσης

• **Διαδρομή** – Περιορίστε μια εξαίρεση ανίχνευσης για μια καθορισμένη διαδρομή (ή για οποιαδήποτε διαδρομή).

• **Όνομα ανίχνευσης** – Εάν υπάρχει όνομα ανίχνευσης δίπλα σε ένα εξαιρεθέν αρχείο, σημαίνει ότι το αρχείο εξαιρείται μόνο για τη συγκεκριμένη ανίχνευση και όχι εντελώς. Εάν αυτό το αρχείο μολυνθεί αργότερα από άλλο κακόβουλο λογισμικό, θα ανιχνευτεί.

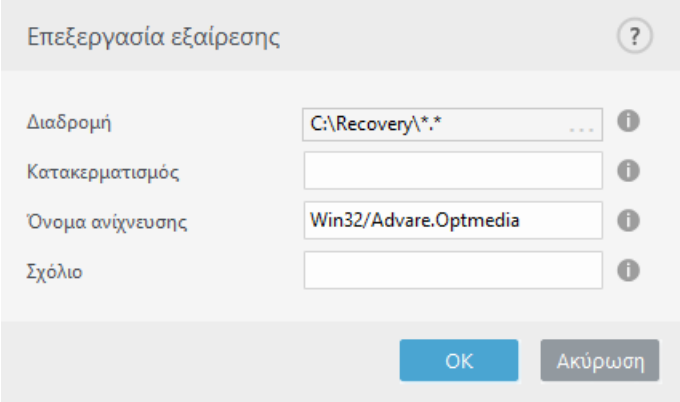
• **Κατακερματισμός** – Εξαιρεί ένα αρχείο που βασίζεται σε συγκεκριμένο κατακερματισμό SHA-1, ανεξάρτητα από τον τύπο αρχείου, τη θέση, το όνομα ή την επέκτασή του.

Προσθήκη ή Επεξεργασία εξαίρεσης ανίχνευσης

Εξαίρεση ανίχνευσης

Θα πρέπει να δοθεί ένα έγκυρο όνομα ανίχνευσης ESET. Για ένα έγκυρο όνομα ανίχνευσης, δείτε τα Αρχεία καταγραφής και, στη συνέχεια, επιλέξτε **Ανιχνεύσεις** από το αναπτυσσόμενο μενού «Αρχεία καταγραφής». Αυτό είναι χρήσιμο όταν ανιχνεύεται ένα ψευδώς θετικό δείγμα στο ESET Internet Security. Οι εξαιρέσεις για πραγματικές εισβολές είναι πολύ επικίνδυνες. Μελετήστε την εξαίρεση μόνο των επηρεαζόμενων αρχείων / καταλόγων κάνοντας κλικ στο στοιχείο **...** στο πεδίο **Διαδρομή** ή/και μόνο για προσωρινό χρονικό διάστημα. Οι εξαιρέσεις εφαρμόζονται επίσης στις Ενδεχομένως ανεπιθύμητες εφαρμογές, στις ενδεχομένως μη ασφαλείς εφαρμογές και στις ύποπτες εφαρμογές.

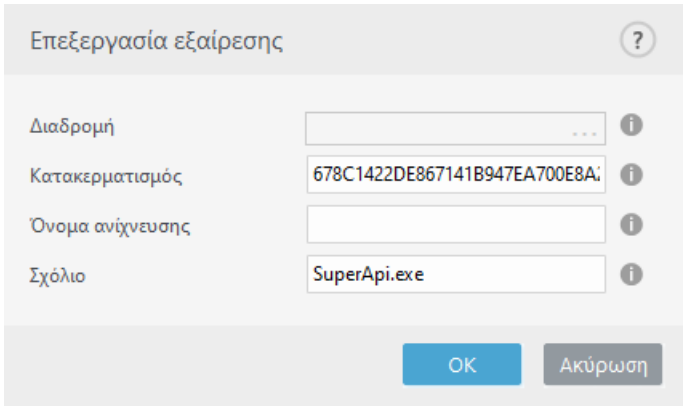
Δείτε επίσης την ενότητα Μορφή εξαίρεσης διαδρομής.



Δείτε την παρακάτω ενότητα Παράδειγμα εξαιρέσεων ανίχνευσης.

Εξαίρεση κατακερματισμού

Εξαιρεί ένα αρχείο που βασίζεται σε συγκεκριμένο κατακερματισμό SHA-1, ανεξάρτητα από τον τύπο αρχείου, τη θέση, το όνομα ή την επέκτασή του.



Εξαιρέσεις κατά όνομα ανίχνευσης

Για να εξαιρέσετε μια συγκεκριμένη ανίχνευση με το όνομά της, εισαγάγετε το έγκυρο όνομα ανίχνευσης:

Win32/Adware.Optmedia

Επίσης, μπορείτε να χρησιμοποιείτε την ακόλουθη μορφή όταν εξαιρείτε μια ανίχνευση από το παράθυρο συναγερμού του ESET Internet Security:

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

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

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

Στοιχεία ελέγχου

- **Προσθήκη** – Εξαιρεί αντικείμενα από τον εντοπισμό.
- **Επεξεργασία** – Επιτρέπει την επεξεργασία επιλεγμένων καταχωρίσεων.
- **Κατάργηση** – Καταργεί επιλεγμένες καταχωρίσεις (πατήστε CTRL + κλικ για να επιλέξετε πολλαπλές καταχωρίσεις).

Δημιουργία οδηγού εξαίρεσης ανίχνευσης

Μια εξαίρεση ανίχνευσης μπορεί να δημιουργηθεί και από το μενού περιβάλλοντος του στοιχείου Αρχεία καταγραφής (δεν είναι διαθέσιμο για ανιχνεύσεις κακόβουλου λογισμικού):

1. Στο κύριο παράθυρο του προγράμματος, κάντε κλικ στο στοιχείο **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής**.
2. Κάντε δεξί κλικ σε μια ανίχνευση στο στοιχείο **Αρχείο καταγραφής ανιχνεύσεων**.
3. Κάντε κλικ στο στοιχείο **Δημιουργία εξαίρεσης**.

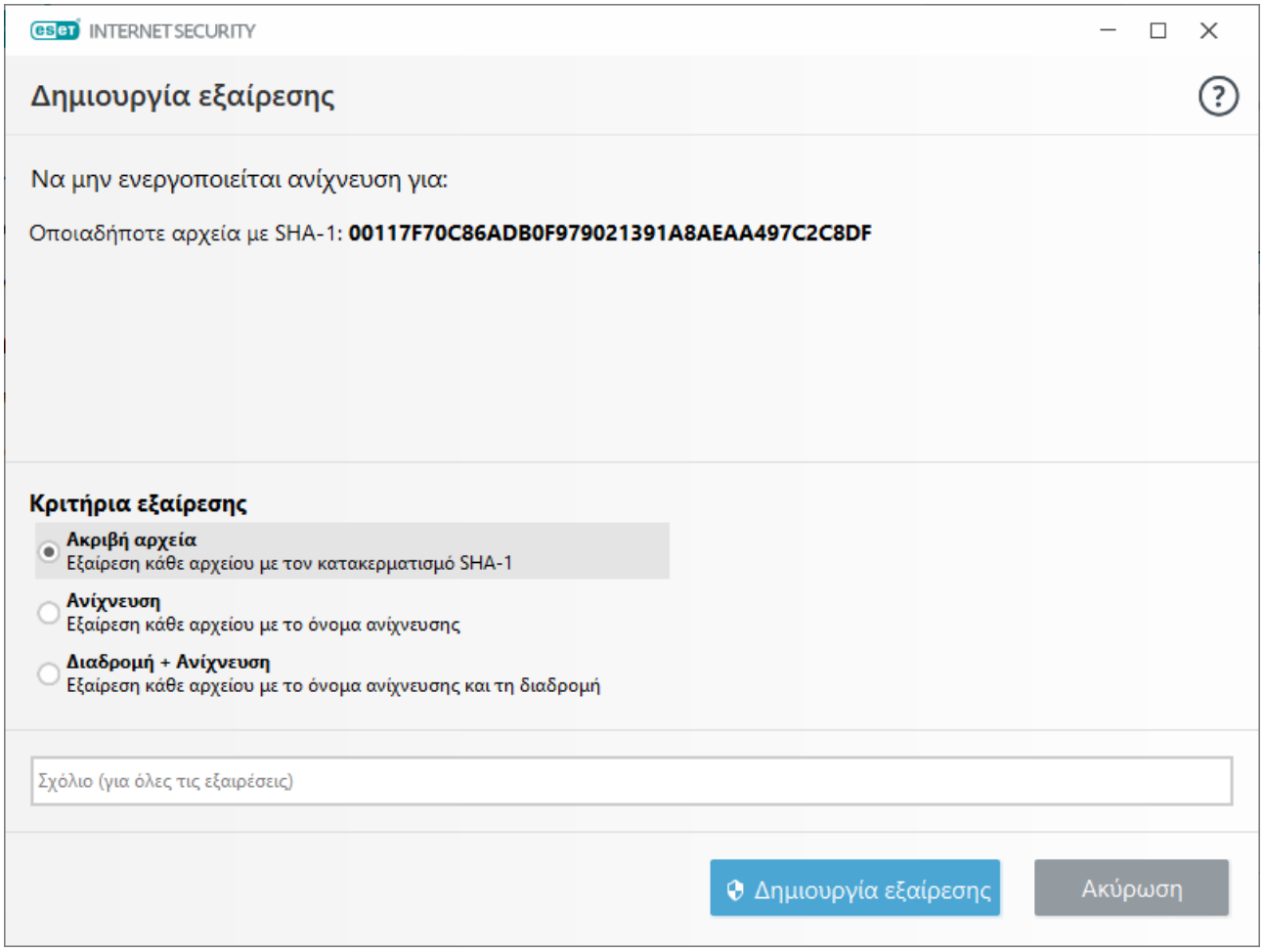
Για να εξαιρέσετε μία ή περισσότερες ανιχνεύσεις με βάση τα **Κριτήρια εξαίρεσης**, κάντε κλικ στο στοιχείο **Αλλαγή κριτηρίων**:

- **Ακριβή αρχεία** – Εξαίρεση κάθε αρχείου με τον κατακερματισμό SHA-1.
- **Ανίχνευση** – Εξαίρεση κάθε αρχείου με το όνομα ανίχνευσης.
- **Διαδρομή + Ανίχνευση** – Εξαίρεση κάθε αρχείου με το όνομα ανίχνευσης και τη διαδρομή,

συμπεριλαμβανομένου του ονόματος αρχείου (π.χ. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Η συνιστώμενη επιλογή είναι προεπιλεγμένη με βάση τον τύπο ανίχνευσης.

Προαιρετικά, μπορείτε να προσθέσετε ένα **Σχόλιο** προτού κάνετε κλικ στο στοιχείο **Δημιουργία εξαίρεσης**.



Εξαιρέσεις HIPS

Οι εξαιρέσεις σάς επιτρέπουν να εξαιρείτε διεργασίες από τον σε βάθος έλεγχο συμπεριφοράς HIPS.

Για να επεξεργαστείτε εξαιρέσεις HIPS, μεταβείτε στα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **HIPS** > **Βασικές ρυθμίσεις** > **Εξαιρέσεις** > **Επεξεργασία**.

Μη συγχέετε τα στοιχεία Εξαιρούμενες επεκτάσεις αρχείων, Εξαιρέσεις ανιχνεύσεων, Εξαιρέσεις επιδόσεων ή Εξαιρέσεις διεργασιών.

Για να εξαιρέσετε ένα αντικείμενο, κάντε κλικ στο στοιχείο **Προσθήκη** και εισαγάγετε τη διαδρομή σε ένα αντικείμενο ή επιλέξτε το στη δομή δέντρου. Επίσης, μπορείτε να πραγματοποιήσετε Επεξεργασία ή Κατάργηση επιλεγμένων καταχωρίσεων.

Παράμετροι ThreatSense

Το ThreatSense περιλαμβάνει πολλές σύνθετες μεθόδους ανίχνευσης απειλών. Αυτή η τεχνολογία είναι προληπτική, που σημαίνει ότι παρέχει επίσης προστασία κατά τα πρώτα στάδια εξάπλωσης μιας νέας απειλής. Χρησιμοποιεί ανάλυση και εξομοίωση κώδικα, γενικές δομές και υπογραφές ιών, συνδυάζοντάς τα ώστε να ενισχύει σημαντικά την ασφάλεια του συστήματος. Ο μηχανισμός σάρωσης μπορεί να ελέγχει ταυτόχρονα πολλές ροές δεδομένων, μεγιστοποιώντας την αποτελεσματικότητα και το ποσοστό ανίχνευσης. Επίσης, η τεχνολογία ThreatSense εξαλείφει με επιτυχία τις απειλές rootkit.

Οι επιλογές ρυθμίσεων του μηχανισμού ThreatSense σάς επιτρέπουν να καθορίσετε διάφορες παραμέτρους σάρωσης:

- Τύποι και επεκτάσεις αρχείων που πρόκειται να σαρωθούν
- Ο συνδυασμός διάφορων μεθόδων ανίχνευσης
- Επίπεδα καθαρισμού κ.λπ.

Για να ανοίξετε το παράθυρο ρυθμίσεων, κάντε κλικ στο κουμπί Παράμετροι **ThreatSense** στο παράθυρο "Ρυθμίσεις για προχωρημένους", για κάθε μονάδα που χρησιμοποιεί την τεχνολογία ThreatSense (δείτε παρακάτω). Τα διάφορα σενάρια ασφαλείας ενδέχεται να απαιτούν διαφορετικές διαμορφώσεις. Έχοντας αυτό υπόψη, το ThreatSense είναι δυνατό να διαμορφωθεί για τις εξής λειτουργικές μονάδες προστασίας:

- Προστασία συστήματος αρχείων σε πραγματικό χρόνο
- Σάρωση σε κατάσταση αδράνειας
- Σάρωση κατά την εκκίνηση
- Προστασία εγγράφων
- Προστασία ηλεκτρονικής αλληλογραφίας
- Προστασία πρόσβασης στο διαδίκτυο
- Σάρωση υπολογιστή

Οι παράμετροι του ThreatSense είναι ιδιαίτερα βελτιστοποιημένες για κάθε μονάδα και η τροποποίησή τους μπορεί να επηρεάσει σημαντικά τη λειτουργία του συστήματος. Για παράδειγμα, αν αλλάξετε τις παραμέτρους ώστε να πραγματοποιείται πάντοτε σάρωση για πακέτα συσκευασίας χρόνου εκτέλεσης ή η ενεργοποίηση προηγμένου ευριστικού ελέγχου στη μονάδα προστασίας συστήματος αρχείων σε πραγματικό χρόνο, αυτό θα μπορούσε να έχει ως αποτέλεσμα την καθυστέρηση του συστήματος (κανονικά, με τη χρήση αυτών των μεθόδων σαρώνονται μόνο τα αρχεία που δημιουργήθηκαν πρόσφατα). Συνιστούμε να μην αλλάζετε τις προεπιλεγμένες παραμέτρους του ThreatSense για όλες τις μονάδες εκτός από τη Σάρωση υπολογιστή.

Αντικείμενα που θα σαρωθούν

Αυτή η ενότητα σας επιτρέπει να καθορίσετε τα στοιχεία του υπολογιστή και τα αρχεία που θα σαρωθούν για εισβολές.

Λειτουργική μνήμη – Σαρώνει για απειλές που επιτίθενται στη λειτουργική μνήμη του συστήματος.

Τομείς εκκίνησης/UEFI – Σαρώνει τους τομείς εκκίνησης για την παρουσία κακόβουλου λογισμικού στην κύρια εγγραφή εκκίνησης. Διαβάστε περισσότερα για το UEFI στο γλωσσάρι.

Αρχεία ηλεκτρονικής αλληλογραφίας – Το πρόγραμμα υποστηρίζει τις παρακάτω επεκτάσεις: DBX (Outlook Express) και EML.

Αρχειοθήκες – Το πρόγραμμα υποστηρίζει τις παρακάτω επεκτάσεις: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE και πολλές άλλες.

Αρχειοθήκες αυτόματης εξαγωγής – Οι αρχειοθήκες αυτόματης εξαγωγής (SFX) είναι αρχειοθήκες που μπορούν να εξαχθούν μόνες τους.

Προγράμματα συσκευασίας χρόνου εκτέλεσης – Μετά την εκτέλεσή τους, τα προγράμματα συσκευασίας χρόνου εκτέλεσης (σε αντίθεση με τους συνήθεις τύπους αρχειοθηκών) αποσυμπιέζονται στη μνήμη. Εκτός από τα τυπικά στατικά προγράμματα συσκευασίας (UPX, yoda, ASPack, FSG, κ.λπ.), η σάρωση είναι σε θέση να αναγνωρίσει πολλούς διαφορετικούς τύπους προγραμμάτων συσκευασίας, μέσω της εξομοίωσης κώδικα.

Επιλογές σάρωσης

Επιλέξτε τις μεθόδους που θα χρησιμοποιούνται κατά τη σάρωση του συστήματος για εισβολές. Οι διαθέσιμες επιλογές είναι οι παρακάτω:

Ευριστικοί έλεγχοι – Ο ευριστικός έλεγχος είναι ένας αλγόριθμος που αναλύει την (κακόβουλη) δραστηριότητα των προγραμμάτων. Το κύριο πλεονέκτημα αυτής της τεχνολογίας είναι η ικανότητα να αναγνωρίζει κακόβουλο λογισμικό που δεν υπήρχε ή που δεν αναγνωρίστηκε από την προηγούμενη έκδοση του μηχανισμού ανίχνευσης. Το μειονέκτημα είναι η (πολύ μικρή) πιθανότητα εσφαλμένων ειδοποιήσεων.

Προηγμένοι ευριστικοί έλεγχοι/DNA υπογραφές – Οι προηγμένοι ευριστικοί έλεγχοι είναι ένας μοναδικός ευριστικός αλγόριθμος που αναπτύχθηκε από την ESET, ο οποίος έχει βελτιστοποιηθεί για την ανίχνευση worm και trojan horse υπολογιστών και έχει γραφτεί σε γλώσσες προγραμματισμού υψηλού επιπέδου. Η χρήση προηγμένων ευριστικών ελέγχων αυξάνει σημαντικά τις ικανότητες ανίχνευσης απειλών των προϊόντων ESET. Η ανίχνευση ιών μπορεί να ανιχνεύσει και να αναγνωρίσει ιούς αξιόπιστα. Με τη χρήση του συστήματος αυτόματης ενημέρωσης είναι διαθέσιμες νέες ενημερώσεις ανίχνευσης μέσα σε λίγες ώρες από την ανακάλυψη της απειλής. Το μειονέκτημα της αναγνώρισης ιών είναι ότι ανιχνεύονται μόνο ιοί που είναι γνωστοί (ή ελαφρώς τροποποιημένες εκδόσεις αυτών των ιών).

Καθαρισμός

Οι ρυθμίσεις καθαρισμού προσδιορίζουν τη συμπεριφορά του ESET Internet Security κατά τον καθαρισμό αντικειμένων. Υπάρχουν 4 επίπεδα καθαρισμού:

Οι παράμετροι ThreatSense έχουν τα ακόλουθα επίπεδα αποκατάστασης (π.χ. καθαρισμός).

Αποκατάσταση στο ESET Internet Security

Επίπεδο καθαρισμού	Περιγραφή
Πάντα αποκατάσταση ανίχνευσης	Προσπάθεια αποκατάστασης της ανίχνευσης κατά τον καθαρισμό αντικειμένων χωρίς παρέμβαση του τελικού χρήστη. Σε ορισμένες σπάνιες περιπτώσεις (για παράδειγμα, αρχεία συστήματος), εάν δεν είναι δυνατή η αποκατάσταση της ανίχνευσης, το αναφερόμενο αντικείμενο μένει στην αρχική του θέση.
Αποκατάσταση ανίχνευσης εάν είναι ασφαλές, διαφορετικά διατήρηση	Προσπάθεια αποκατάστασης της ανίχνευσης κατά τον καθαρισμό αντικειμένων χωρίς παρέμβαση του τελικού χρήστη. Σε ορισμένες περιπτώσεις (για παράδειγμα, αρχεία συστήματος ή αρχειοθήκες με καθαρά και μολυσμένα αρχεία), εάν δεν είναι δυνατή η αποκατάσταση μιας ανίχνευσης, το αναφερόμενο αντικείμενο μένει στην αρχική του θέση.
Αποκατάσταση ανίχνευσης εάν είναι ασφαλές, διαφορετικά ερώτηση	Προσπάθεια αποκατάστασης της ανίχνευσης κατά τον καθαρισμό αντικειμένων. Σε ορισμένες περιπτώσεις, εάν δεν είναι δυνατή η εκτέλεση οποιασδήποτε ενέργειας, ο τελικός χρήστης λαμβάνει έναν αλληλεπιδραστικό συναγερμό και πρέπει να επιλέξει μια ενέργεια αποκατάστασης (για παράδειγμα, κατάργηση ή παράλειψη). Αυτή η ρύθμιση συνιστάται στις περισσότερες περιπτώσεις.
Να ερωτάται πάντα ο τελικός χρήστης	Ο τελικός χρήστης λαμβάνει ένα αλληλεπιδραστικό παράθυρο κατά τον καθαρισμό αντικειμένων και πρέπει να επιλέξει μια ενέργεια αποκατάστασης (για παράδειγμα, κατάργηση ή παράβλεψη). Αυτό το επίπεδο έχει σχεδιαστεί για πιο προχωρημένους χρήστες που γνωρίζουν τα βήματα που πρέπει να ακολουθήσουν σε περίπτωση ανίχνευσης.

Εξαιρέσεις

Η επέκταση είναι το μέρος του ονόματος ενός αρχείου που διαχωρίζεται από μια τελεία. Η επέκταση καθορίζει τον τύπο και το περιεχόμενο ενός αρχείου. Αυτή η ενότητα της ρύθμισης παραμέτρων του ThreatSense σάς επιτρέπει να καθορίσετε τους τύπους αρχείων που θα σαρωθούν.

Άλλα

Όταν διαμορφώνετε τις παραμέτρους του μηχανισμού ThreatSense για κατ' απαίτηση σάρωση του υπολογιστή, είναι επίσης διαθέσιμες οι παρακάτω επιλογές στην ενότητα **Άλλα**:

Σάρωση εναλλακτικών ροών δεδομένων (ADS) – Οι εναλλακτικές ροές δεδομένων που χρησιμοποιούνται από το σύστημα αρχείων NTFS είναι συσχετισμοί αρχείων και φακέλων που είναι αόρατοι στις συνηθισμένες τεχνικές σάρωσης. Πολλές εισβολές προσπαθούν να αποφύγουν την ανίχνευση επιχειρώντας συγκάλυψη ως εναλλακτικές ροές δεδομένων.

Εκτέλεση σαρώσεων χαμηλής προτεραιότητας στο παρασκήνιο – Κάθε ακολουθία σάρωσης καταναλώνει συγκεκριμένη ποσότητα των πόρων του συστήματος. Αν εργάζεστε με προγράμματα που επιβαρύνουν τους πόρους του συστήματος, μπορείτε να ενεργοποιήσετε τη σάρωση χαμηλής προτεραιότητας στο παρασκήνιο και να εξοικονομήσετε πόρους για τις εφαρμογές σας.

Καταγραφή όλων των αντικειμένων – Το Αρχείο καταγραφής σάρωσης θα εμφανίζει όλα τα σαρωμένα αρχεία σε αρχειοθήκες αυτόματης εξαγωγής, ακόμα και εκείνα που δεν μολύνθηκαν (μπορεί να δημιουργήσει πολλά δεδομένα αρχείου καταγραφής σάρωσης και να αυξήσει το μέγεθος του αρχείου καταγραφής σάρωσης).

Ενεργοποίηση έξυπνης βελτιστοποίησης – Όταν είναι ενεργοποιημένη η Έξυπνη βελτιστοποίηση,

χρησιμοποιούνται οι πλέον βέλτιστες ρυθμίσεις για να διασφαλίζεται το πιο αποτελεσματικό επίπεδο σάρωσης, διατηρώντας ταυτόχρονα τις υψηλότερες ταχύτητες σάρωσης. Οι διάφορες μονάδες προστασίας πραγματοποιούν έξυπνη σάρωση, χρησιμοποιώντας διάφορες μεθόδους σάρωσης και εφαρμόζοντάς τις σε συγκεκριμένους τύπους αρχείων. Εάν απενεργοποιηθεί η Έξυπνη βελτιστοποίηση, εφαρμόζονται μόνο οι ρυθμίσεις που έχει ορίσει ο χρήστης στη βάση του ThreatSense των συγκεκριμένων λειτουργικών μονάδων κατά την εκτέλεση μιας σάρωσης.

Διατήρηση χρονικής σήμανσης τελευταίας πρόσβασης – Κάντε αυτή την επιλογή για να διατηρείται ο αρχικός χρόνος πρόσβασης στα σαρωμένα αρχεία αντί να ενημερώνεται (για παράδειγμα, για χρήση με συστήματα δημιουργίας αντιγράφων ασφαλείας δεδομένων).

Όρια

Η ενότητα Όρια σάς επιτρέπει να καθορίσετε το μέγιστο μέγεθος αντικειμένων και επιπέδων ένθετων αρχειοθηκών που θα σαρωθούν:

Ρυθμίσεις αντικειμένων

Μέγιστο μέγεθος αντικειμένων – Καθορίζει ένα μέγιστο μέγεθος αντικειμένων που θα σαρωθούν. Η συγκεκριμένη μονάδα antivirus θα σαρώσει στη συνέχεια μόνο αντικείμενα με μέγεθος μικρότερο από το καθορισμένο. Η επιλογή αυτή θα πρέπει να μεταβάλλεται μόνο από προχωρημένους χρήστες οι οποίοι μπορεί να έχουν ειδικούς λόγους για την εξαίρεση μεγάλων αντικειμένων από τη σάρωση. Προεπιλεγμένη τιμή: απεριόριστο.

Μέγιστος χρόνος σάρωσης για αντικείμενο (δευτ.) – Καθορίζει τη μέγιστη τιμή χρόνου για τη σάρωση αρχείων σε ένα αντικείμενο κοντέινερ (όπως μια αρχειοθήκη RAR/ZIP ή ένα email με πολλά συνημμένα). Αυτή η ρύθμιση δεν ισχύει για ανεξάρτητα αρχεία. Εάν έχει εισαχθεί μια τιμή που ορίζεται από τον χρήστη και έχει παρέλθει αυτός ο χρόνος, η σάρωση θα διακοπεί το συντομότερο δυνατόν, ανεξάρτητα αν έχει ολοκληρωθεί η σάρωση κάθε αρχείου σε ένα αντικείμενο κοντέινερ. Στην περίπτωση μιας αρχειοθήκης με μεγάλα αρχεία, η σάρωση δεν θα σταματήσει μέχρι να εξαχθεί ένα αρχείο από την αρχειοθήκη (για παράδειγμα, όταν μια μεταβλητή που ορίζεται από τον χρήστη είναι 3 δευτερόλεπτα, αλλά η εξαγωγή ενός αρχείου διαρκεί 5 δευτερόλεπτα). Τα υπόλοιπα αρχεία στην αρχειοθήκη δεν θα σαρωθούν αφού παρέλθει αυτός ο χρόνος.
Για να περιορίσετε το χρόνο σάρωσης, συμπεριλαμβανομένων των μεγαλύτερων αρχειοθηκών, χρησιμοποιήστε την επιλογή **Μέγιστο μέγεθος αντικειμένων** και **Μέγιστο μέγεθος αρχείου στην αρχειοθήκη** (δεν συνιστάται λόγω ενδεχόμενων κινδύνων ασφαλείας).
Προεπιλεγμένη τιμή: απεριόριστο.

Ρυθμίσεις σάρωσης αρχειοθηκών

Βάθος ένθεσης αρχειοθηκών – Καθορίζει το μέγιστο βάθος σάρωσης αρχειοθηκών. Προεπιλεγμένη τιμή: 10.

Μέγιστο μέγεθος αρχείου στην αρχειοθήκη – Αυτή η επιλογή σάς επιτρέπει να καθορίσετε το μέγιστο μέγεθος αρχείου για αρχεία που περιέχονται σε αρχειοθήκες (κατά την εξαγωγή τους), τα οποία πρόκειται να σαρωθούν. Η μέγιστη τιμή είναι **3 GB**.

> Δεν συνιστάται η αλλαγή των προεπιλεγμένων τιμών. Υπό κανονικές συνθήκες, δεν θα πρέπει να υπάρχει λόγος να μεταβληθούν.

Επεκτάσεις αρχείων που εξαιρούνται από τον έλεγχο

Οι εξαιρούμενες επεκτάσεις αρχείων αποτελούν μέρος των παραμέτρων του ThreatSense. Για να ρυθμίσετε τις παραμέτρους των εξαιρούμενων επεκτάσεων αρχείων, κάντε κλικ στο στοιχείο **Παράμετροι του ThreatSense** στο παράθυρο ρυθμίσεων για προχωρημένους για οποιαδήποτε λειτουργική μονάδα που χρησιμοποιεί την τεχνολογία ThreatSense.

Η επέκταση είναι το μέρος του ονόματος ενός αρχείου που διαχωρίζεται από μια τελεία. Η επέκταση καθορίζει τον τύπο και το περιεχόμενο ενός αρχείου. Αυτή η ενότητα της ρύθμισης παραμέτρων του ThreatSense σάς επιτρέπει να καθορίσετε τους τύπους αρχείων που θα σαρωθούν.

> Μη συγχέετε την επιλογή με το στοιχείο Εξαιρέσεις διεργασιών, Εξαιρέσεις HIPS ή Εξαιρέσεις αρχείων/φακέλων.

Από προεπιλογή, σαρώνονται όλα τα αρχεία. Στη λίστα αρχείων που εξαιρούνται από τη σάρωση μπορεί να προστεθεί οποιαδήποτε επέκταση.

Η εξαίρεση αρχείων είναι απαραίτητη μερικές φορές αν η σάρωση ορισμένων τύπων αρχείων εμποδίζει τη σωστή εκτέλεση του προγράμματος που χρησιμοποιεί συγκεκριμένες επεκτάσεις. Για παράδειγμα, μπορεί να είναι καλό να εξαιρούνται οι επεκτάσεις `.edb`, `.eml` και `.tmp` όταν χρησιμοποιούνται διακομιστές Microsoft Exchange.

> Για να προσθέσετε μια νέα επέκταση στη λίστα, κάντε κλικ στο στοιχείο **Προσθήκη**. Πληκτρολογήστε την επέκταση στο κενό πεδίο (για παράδειγμα tmp) και κάντε κλικ στο **ΟΚ**. Όταν επιλέγετε **Εισαγωγή πολλαπλών τιμών**, μπορείτε να προσθέσετε πολλές επεκτάσεις αρχείων διαχωρισμένες με γραμμές, κόμματα ή ερωτηματικά (για παράδειγμα, επιλέξτε **Ερωτηματικό** από το αναπτυσσόμενο μενού ως διαχωριστικό, και πληκτρολογήστε `edb;eml;tmp`).
> Μπορείτε να χρησιμοποιήσετε ένα ειδικό σύμβολο ? (Λατινικό ερωτηματικό). Το Λατινικό ερωτηματικό αντιπροσωπεύει οποιοδήποτε σύμβολο (για παράδειγμα `?db`).

> Για να μπορείτε να δείτε την ακριβή επέκταση (εάν υπάρχει) ενός αρχείου σε ένα λειτουργικό σύστημα Windows, πρέπει να καταργήσετε την επιλογή **Απόκρυψη επεκτάσεων για γνωστούς τύπους αρχείων** στη θέση **Πίνακας Ελέγχου** > **Επιλογές φακέλων** > (καρτέλα) **Προβολή** και να εφαρμόσετε αυτή την αλλαγή.

Πρόσθετες παράμετροι του ThreatSense

Για να επεξεργαστείτε αυτές τις ρυθμίσεις, μεταβείτε στα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5) > **Μηχανισμός ανίχνευσης** > **Προστασία συστήματος αρχείων σε πραγματικό χρόνο** > **Πρόσθετες παράμετροι του ThreatSense**.

Πρόσθετες παράμετροι ThreatSense για αρχεία που δημιουργήθηκαν και τροποποιήθηκαν πρόσφατα

Η πιθανότητα μόλυνσης σε αρχεία που δημιουργήθηκαν ή τροποποιήθηκαν πρόσφατα είναι συγκριτικά μεγαλύτερη από όσο στα υπάρχοντα αρχεία. Για αυτόν το λόγο, το πρόγραμμα ελέγχει

αυτά τα αρχεία με πρόσθετες παραμέτρους σάρωσης. Το ESET Internet Security χρησιμοποιεί προηγμένη ευρετική τεχνολογία, η οποία μπορεί να ανιχνεύσει νέες απειλές προτού εκδοθεί η ενημέρωση του μηχανισμού ανίχνευσης, σε συνδυασμό με μεθόδους σάρωσης που βασίζονται στην αναγνώριση ιών.

Πέρα από τα αρχεία που έχουν δημιουργηθεί πρόσφατα, εκτελείται σάρωση στις **Αρχειοθήκες αυτόματης εξαγωγής** (.sfx) και σε **Προγράμματα Packer χρόνου εκτέλεσης** (εσωτερικά συμπιεσμένα εκτελέσιμα αρχεία). Από προεπιλογή, οι αρχειοθήκες σαρώνονται μέχρι και το 10ο επίπεδο ένθεσης και ελέγχονται ανεξάρτητα από το πραγματικό τους μέγεθος. Για να τροποποιήσετε τις ρυθμίσεις σάρωσης αρχειοθηκών, απενεργοποιήστε το στοιχείο **Προεπιλεγμένες ρυθμίσεις σάρωσης αρχειοθήκης**.

Πρόσθετες παράμετροι ThreatSense για εκτελούμενα αρχεία

Προηγμένοι ευριστικοί έλεγχοι κατά την εκτέλεση αρχείων – Από προεπιλογή, χρησιμοποιούνται προηγμένοι ευριστικοί έλεγχοι κατά την εκτέλεση αρχείων. Όταν η επιλογή είναι ενεργοποιημένη, συνιστούμε οπωσδήποτε να διατηρείτε ενεργοποιημένη την Έξυπνη βελτιστοποίηση και το ESET LiveGrid®, για να περιορίσετε τον αντίκτυπο στις επιδόσεις του συστήματος.

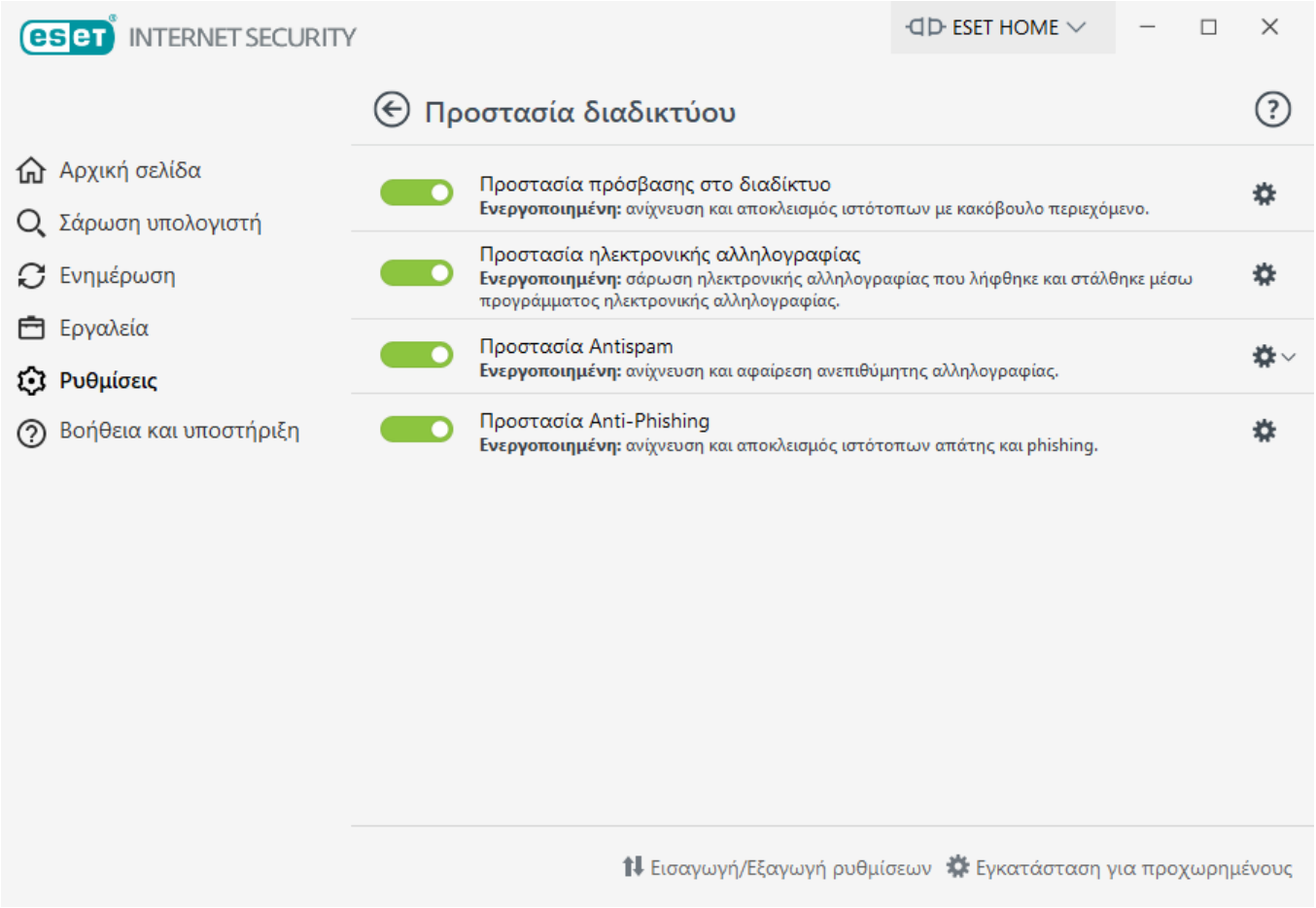
Προηγμένοι ευριστικοί έλεγχοι κατά την εκτέλεση αρχείων από αφαιρούμενα μέσα – Οι προηγμένοι ευριστικοί έλεγχοι εξομοιώνουν τον κώδικα σε ένα εικονικό περιβάλλον και αξιολογούν τη συμπεριφορά του προτού επιτραπεί η εκτέλεση του κώδικα από το αφαιρούμενο μέσο.

Προστασία διαδικτύου

Για να ρυθμίσετε τις παραμέτρους της Προστασίας διαδικτύου και ηλεκτρονικής αλληλογραφίας, κάντε κλικ στο στοιχείο **Προστασία διαδικτύου** στο παράθυρο **Ρυθμίσεις**. Από εδώ μπορείτε να αποκτήσετε πρόσβαση σε πιο λεπτομερείς ρυθμίσεις του προγράμματος.

Για να διακόψετε προσωρινά ή να απενεργοποιήσετε μεμονωμένες λειτουργικές μονάδες προστασίας, κάντε κλικ στο εικονίδιο ρυθμιστικού .

Η απενεργοποίηση των λειτουργικών μονάδων προστασίας ενδέχεται να μειώσει το επίπεδο προστασίας του υπολογιστή σας.



Κάντε κλικ στο εικονίδιο γραναζιού για να ανοίξετε το διαδίκτυο/email/Anti-Phishing/antispam στις Ρυθμίσεις για προχωρημένους.

Η συνδεσιμότητα με το διαδίκτυο είναι μια τυπική δυνατότητα για τους προσωπικούς υπολογιστές. Δυστυχώς, το Διαδίκτυο έχει γίνει το κύριο μέσο για τη μεταφορά κακόβουλου κώδικα. Για αυτό τον λόγο είναι απαραίτητο να μελετήσετε προσεκτικά τις ρυθμίσεις για την Προστασία πρόσβασης στον διαδικτύο.

Η Προστασία ηλεκτρονικής αλληλογραφίας παρέχει έλεγχο των επικοινωνιών ηλεκτρονικής αλληλογραφίας που λαμβάνονται μέσω των πρωτοκόλλων POP3(S) και IMAP(S). Χρησιμοποιώντας το πρόγραμμα προσθήκης για το πρόγραμμα-πελάτη ηλεκτρονικής αλληλογραφίας, το ESET Internet Security παρέχει έλεγχο σε όλες τις επικοινωνίες από το πρόγραμμα-πελάτη ηλεκτρονικής αλληλογραφίας που χρησιμοποιείτε.

Η Προστασία Antispam φιλτράρει ανεπιθύμητα μηνύματα ηλεκτρονικής αλληλογραφίας.

Για το στοιχείο **Προστασία Antispam**, κάντε κλικ στο εικονίδιο γραναζιού και επιλέξτε από τις ακόλουθες επιλογές:

• **Ρύθμιση παραμέτρων** – Ανοίγει προηγμένες ρυθμίσεις για την προστασία Antispam του προγράμματος-πελάτη ηλεκτρονικής αλληλογραφίας.

• **Λίστα διευθύνσεων χρήστη** (εάν έχει ενεργοποιηθεί) – Ανοίγει ένα παράθυρο διαλόγου όπου μπορείτε να προσθέσετε, να επεξεργαστείτε ή να καταργήσετε διευθύνσεις για να καθορίσετε τους κανόνες Antispam. Οι κανόνες αυτής της λίστας θα εφαρμοστούν στον τρέχοντα χρήστη.

• **Γενική λίστα διευθύνσεων** (εάν έχει ενεργοποιηθεί) – Ανοίγει ένα παράθυρο διαλόγου όπου

μπορείτε να προσθέσετε, να επεξεργαστείτε ή να καταργήσετε διευθύνσεις για να καθορίσετε τους κανόνες Antispam. Οι κανόνες αυτής της λίστας θα εφαρμοστούν σε όλους τους χρήστες.

Η Προστασία Anti-Phishing σάς επιτρέπει να αποκλείσετε ιστοσελίδες που είναι γνωστό ότι διανέμουν περιεχόμενο phishing. Συνιστάται να αφήσετε ενεργοποιημένη τη δυνατότητα Anti-Phishing.

Φιλτράρισμα πρωτοκόλλων

Η προστασία Antivirus για πρωτόκολλα εφαρμογών παρέχεται από τη μονάδα σάρωσης ThreatSense, η οποία ενσωματώνεται πλήρως με όλες τις προηγμένες τεχνικές σάρωσης για κακόβουλο λογισμικό. Το φιλτράρισμα πρωτοκόλλων λειτουργεί αυτόματα, ανεξάρτητα από το πρόγραμμα περιήγησης στο διαδίκτυο ή το πρόγραμμα-πελάτη email που χρησιμοποιείται. Για να επεξεργαστείτε ρυθμίσεις κρυπτογραφημένης επικοινωνίας (SSL/TLS), μεταβείτε στην ενότητα **Εγκατάσταση για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **SSL/TLS**.

Ενεργοποίηση φιλτραρίσματος περιεχομένου από το πρωτόκολλο εφαρμογής – Μπορεί να χρησιμοποιηθεί για την απενεργοποίηση του φιλτραρίσματος πρωτοκόλλων. Σημειώστε ότι πολλά στοιχεία του ESET Internet Security (Προστασία πρόσβασης στο διαδίκτυο, Προστασία πρωτοκόλλων ηλεκτρονικής αλληλογραφίας, Anti-Phishing, Γονικός έλεγχος) εξαρτώνται από αυτήν τη δυνατότητα και δεν λειτουργούν χωρίς αυτήν.

Εξαιρεθείσες εφαρμογές – Σας επιτρέπει να εξαιρείτε συγκεκριμένες εφαρμογές από το φιλτράρισμα πρωτοκόλλων. Χρήσιμη επιλογή όταν το φιλτράρισμα πρωτοκόλλων προκαλεί ζητήματα συμβατότητας.

Εξαιρεθείσες διευθύνσεις IP – Σας επιτρέπει να εξαιρείτε συγκεκριμένες απομακρυσμένες διευθύνσεις από το φιλτράρισμα πρωτοκόλλων. Χρήσιμη επιλογή όταν το φιλτράρισμα πρωτοκόλλων προκαλεί ζητήματα συμβατότητας.

Προσθέτει (για παράδειγμα *2001:718:1c01:16:214:22ff:fec9:ca5*).

Υποδίκτυο – Υποδίκτυο (ομάδα υπολογιστών) που καθορίζεται από μια διεύθυνση IP και μάσκα (για παράδειγμα: *2002:c0a8:6301:1::1/64*).

Παράδειγμα εξαιρούμενων διευθύνσεων IP

Διευθύνσεις IPv4 και μάσκα:

- *192.168.0.10* – Προσθέτει τη διεύθυνση IP ενός μεμονωμένου υπολογιστή για τον οποίο θα εφαρμόζεται ο κανόνας.
- *192.168.0.1* έως *192.168.0.99* – Εισαγάγετε τη διεύθυνση IP έναρξης και τη διεύθυνση IP τέλους για να καθορίσετε το εύρος διευθύνσεων IP (για πολλούς υπολογιστές) για τους οποίους θα εφαρμόζεται ο κανόνας.
- Υποδίκτυο (μια ομάδα υπολογιστών) που καθορίζεται από μια διεύθυνση IP και μάσκα. Για παράδειγμα, *255.255.255.0* είναι η μάσκα δικτύου για το πρόθεμα *192.168.1.0/24*, που σημαίνει εύρος διευθύνσεων *192.168.1.1* έως 192.168.1.254.

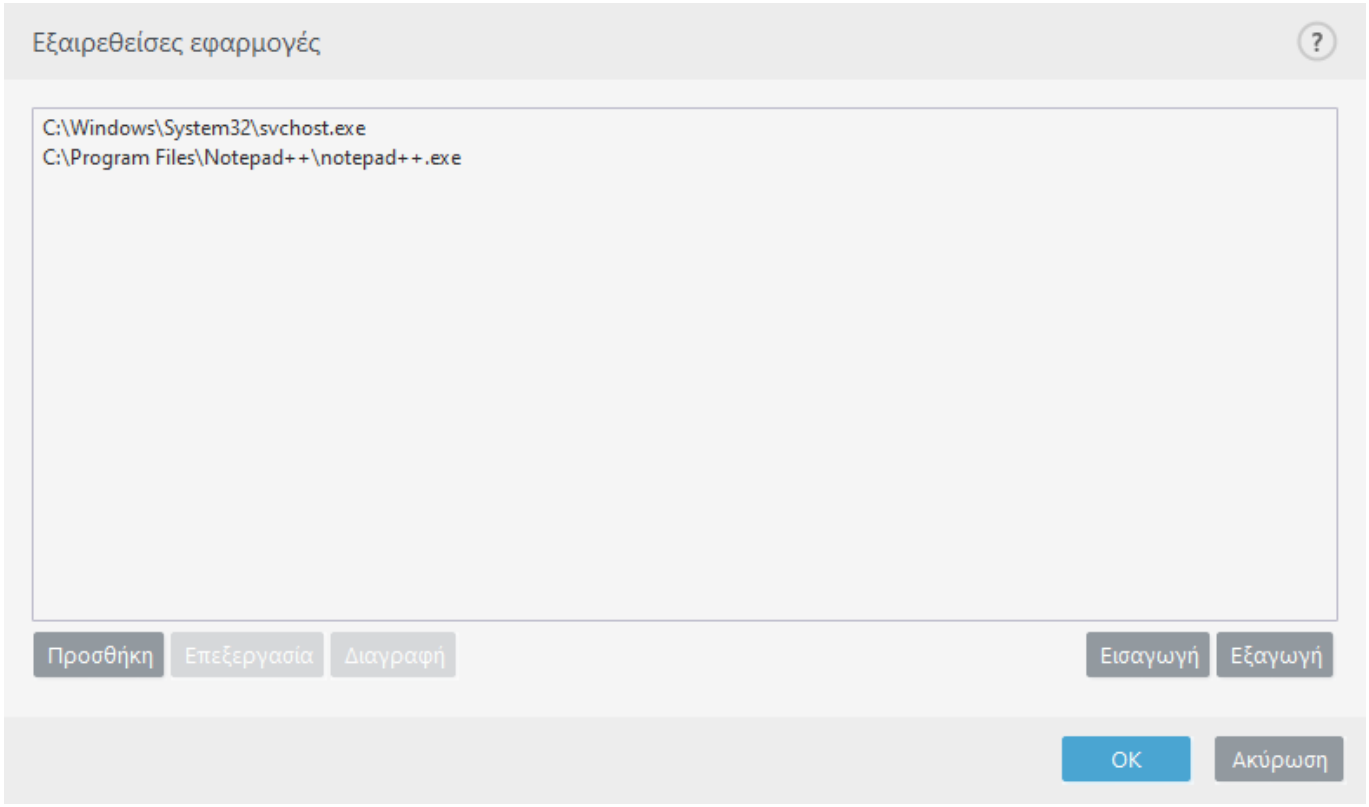
Διευθύνσεις IPv6 και μάσκα:

- *2001:718:1c01:16:214:22ff:fec9:ca5* – η διεύθυνση IPv6 ενός μεμονωμένου υπολογιστή για τον οποίο θα εφαρμόζεται ο κανόνας
- *2002:c0a8:6301:1::1/64* – η διεύθυνση IPv6 με το μήκος προθέματος 64 bit, που σημαίνει *2002:c0a8:6301:0001:0000:0000:0000:0000* έως *2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

Εξαιρεθείσες εφαρμογές

Για να εξαιρέσετε την επικοινωνία συγκεκριμένων εφαρμογών που σχετίζονται με το δίκτυο από το φιλτράρισμα περιεχομένου, επιλέξτε τις στη λίστα. Η επικοινωνία HTTP/POP3/IMAP των επιλεγμένων εφαρμογών δεν θα ελέγχεται για απειλές. Συνιστάται η επιλογή αυτή να χρησιμοποιείται μόνο για εφαρμογές που δεν λειτουργούν σωστά όταν ελέγχεται η επικοινωνία τους.

Η εκτέλεση εφαρμογών και υπηρεσιών θα είναι διαθέσιμη αυτόματα εδώ. Κάντε κλικ στο στοιχείο **Προσθήκη** για να προσθέσετε με μη αυτόματο τρόπο μια εφαρμογή η οποία δεν εμφανίζεται στη λίστα φιλτραρίσματος πρωτοκόλλων.



Εξαιρεθείσες διευθύνσεις IP

Οι καταχωρίσεις στη λίστα θα εξαιρούνται από φιλτράρισμα περιεχομένου από το πρωτόκολλο. Η επικοινωνία HTTP/POP3/IMAP από/προς τις επιλεγμένες διευθύνσεις δεν θα ελέγχεται για απειλές. Συνιστάται η επιλογή αυτή να χρησιμοποιείται μόνο για διευθύνσεις των οποίων η αξιοπιστία είναι γνωστή.

Κάντε κλικ στο κουμπί **Προσθήκη** για να εξαιρέσετε τη διεύθυνση IP, το εύρος διευθύνσεων ή το υποδίκτυο ενός απομακρυσμένου σημείου που δεν εμφανίζεται στη λίστα φιλτραρίσματος πρωτοκόλλων.

Κάντε κλικ στο κουμπί **Διαγραφή** για να καταργήσετε επιλεγμένες καταχωρίσεις από τη λίστα.

Προσθήκη διεύθυνσης IPv4

Αυτή η επιλογή σάς επιτρέπει να προσθέσετε μια διεύθυνση/εύρος διευθύνσεων/υποδίκτυο IP ενός απομακρυσμένου σημείου στο οποίο εφαρμόζεται ένας κανόνας. Το πρωτόκολλο διαδικτύου έκδοση 4 είναι το παλαιότερο αλλά εξακολουθεί να χρησιμοποιείται ευρέως.

Μοναδική διεύθυνση – Προσθέτει τη διεύθυνση IP ενός μεμονωμένου υπολογιστή για τον οποίο θα εφαρμόζεται ο κανόνας (για παράδειγμα *192.168.0.10*).

Εύρος διευθύνσεων – Εισαγάγετε τη διεύθυνση IP έναρξης και τη διεύθυνση IP τέλους για να καθορίσετε το εύρος διευθύνσεων IP (για πολλούς υπολογιστές) για τους οποίους θα εφαρμόζεται ο κανόνας (για παράδειγμα *192.168.0.1* έως *192.168.0.99*).

Υποδίκτυο – Υποδίκτυο (ομάδα υπολογιστών) που καθορίζεται από μια διεύθυνση IP και μάσκα.

Για παράδειγμα, *255.255.255.0* είναι η μάσκα δικτύου για το πρόθεμα *192.168.1.0/24*, που σημαίνει εύρος διευθύνσεων *192.168.1.1* έως 192.168.1.254.

Προσθήκη διεύθυνσης IPv6

Αυτή η επιλογή σάς επιτρέπει να προσθέσετε μια διεύθυνση/υποδίκτυο IPv6 ενός απομακρυσμένου σημείου για το οποίο εφαρμόζεται ένας κανόνας. Είναι η πιο πρόσφατη έκδοση του πρωτοκόλλου διαδικτύου και θα αντικαταστήσει την παλαιότερη έκδοση 4.

Μοναδική διεύθυνση – Προσθέτει τη διεύθυνση IP ενός μεμονωμένου υπολογιστή για τον οποίο θα εφαρμόζεται ο κανόνας (για παράδειγμα *2001:718:1c01:16:214:22ff:fec9:ca5*).

Υποδίκτυο – Υποδίκτυο (ομάδα υπολογιστών) που καθορίζεται από μια διεύθυνση IP και μάσκα (για παράδειγμα: *2002:c0a8:6301:1::1/64*).

SSL/TLS

Το ESET Internet Security είναι σε θέση να ελέγχει για απειλές σε επικοινωνίες που χρησιμοποιούν το πρωτόκολλο SSL. Μπορείτε να χρησιμοποιήσετε διάφορες λειτουργίες Φιλτράρισμα να εξετάζετε επικοινωνίες που προστατεύονται με κρυπτογράφηση SSL χρησιμοποιώντας αξιόπιστα πιστοποιητικά, άγνωστα πιστοποιητικά ή πιστοποιητικά που εξαιρούνται από τον έλεγχο επικοινωνιών που προστατεύεται με κρυπτογράφηση SSL.

Ενεργοποίηση φιλτραρίσματος πρωτοκόλλου SSL/TLS – Εάν το φιλτράρισμα πρωτοκόλλων είναι απενεργοποιημένο, το πρόγραμμα δεν θα σαρώνει επικοινωνίες σύνδεσης SSL.

η Λειτουργία φιλτραρίσματος πρωτοκόλλου SSL/TLS είναι διαθέσιμη στις παρακάτω επιλογές:

Λειτουργία φιλτραρίσματος	Περιγραφή
Αυτόματη λειτουργία	Η προεπιλεγμένη λειτουργία θα σαρώνει μόνο τις κατάλληλες εφαρμογές, όπως προγράμματα περιήγησης και προγράμματα-πελάτες ηλεκτρονικής αλληλογραφίας. Μπορείτε να την παρακάμψετε επιλέγοντας εφαρμογές οι επικοινωνίες των οποίων θα σαρώνονται.
Αλληλεπιδραστική λειτουργία	Εάν επισκεφτείτε έναν νέο ιστότοπο που προστατεύεται με σύνδεση SSL (με άγνωστο πιστοποιητικό), εμφανίζεται ένα παράθυρο διαλόγου επιλογής ενέργειας. Αυτή η λειτουργία σάς επιτρέπει να δημιουργήσετε μια λίστα πιστοποιητικών / εφαρμογών SSL που θα εξαιρούνται από τη σάρωση.
Λειτουργία πολιτικής	Λειτουργία πολιτικής – Ενεργοποιήστε αυτή την επιλογή για να σαρώνονται όλες οι επικοινωνίες που προστατεύονται με κρυπτογράφηση SSL, εκτός από τις επικοινωνίες που προστατεύονται με πιστοποιητικά τα οποία εξαιρούνται από τον έλεγχο. Αν δημιουργηθεί μια νέα επικοινωνία που χρησιμοποιεί άγνωστο, υπογεγραμμένο πιστοποιητικό, δεν θα ειδοποιηθείτε και η επικοινωνία θα φιλτραριστεί αυτόματα. Όταν αποκτάτε πρόσβαση σε ένα διακομιστή με μη αξιόπιστο πιστοποιητικό που επισημαίνεται ως αξιόπιστο (βρίσκεται στη λίστα αξιόπιστων πιστοποιητικών), επιτρέπεται η επικοινωνία με το διακομιστή και φιλτράρεται το περιεχόμενο του διαύλου επικοινωνίας.

Η **Λίστα εφαρμογών με φιλτράρισμα SSL/TLS** μπορεί να χρησιμοποιηθεί για να προσαρμόσετε τη συμπεριφορά του ESET Internet Security για συγκεκριμένες εφαρμογές

Λίστα γνωστών πιστοποιητικών – Σας επιτρέπει να προσαρμόζετε τη συμπεριφορά του ESET Internet Security για συγκεκριμένα πιστοποιητικά SSL.

Εξαίρεση επικοινωνίας με αξιόπιστους τομείς – Εάν ενεργοποιηθεί, η επικοινωνία με αξιόπιστους τομείς θα εξαιρείται από τον έλεγχο. Η αξιοπιστία των τομέων προσδιορίζεται από ενσωματωμένη λίστα.

Αποκλεισμός κρυπτογραφημένης επικοινωνίας που χρησιμοποιεί το καταργημένο πρωτόκολλο SSL v2 – Η επικοινωνία που χρησιμοποιεί παλαιότερη έκδοση του πρωτοκόλλου SSL θα αποκλείεται αυτόματα.

Πιστοποιητικό ρίζας

Προσθήκη του πιστοποιητικού ρίζας σε γνωστά προγράμματα περιήγησης – Για να λειτουργήσει σωστά η επικοινωνία SSL στα προγράμματα περιήγησης/προγράμματα-πελάτες email, είναι απαραίτητο το πιστοποιητικό ρίζας για την ESET να προστεθεί στη λίστα γνωστών πιστοποιητικών ρίζας (εκδότες). Εάν ενεργοποιήσετε αυτή την επιλογή, το ESET Internet Security θα προσθέτει αυτόματα το πιστοποιητικό ρίζας ESET SSL Filter CA στα γνωστά προγράμματα περιήγησης (για παράδειγμα Opera). Για προγράμματα περιήγησης που χρησιμοποιούν το χώρο αποθήκευσης πιστοποιητικών του συστήματος, το πιστοποιητικό προστίθεται αυτόματα. Για παράδειγμα, εκτελείται αυτόματα ρύθμιση παραμέτρων για το Firefox, ώστε να είναι αξιόπιστες οι αρχές ρίζας στο χώρο αποθήκευσης του συστήματος.

Για να εφαρμόσετε το πιστοποιητικό σε προγράμματα περιήγησης που δεν υποστηρίζονται, κάντε κλικ στα **Προβολή πιστοποιητικού** > **Λεπτομέρειες** > **Αντιγραφή σε αρχείο** και στη συνέχεια εισαγάγετε το πιστοποιητικό με μη αυτόματο τρόπο στο πρόγραμμα περιήγησης.

Εγκυρότητα πιστοποιητικού

Εάν δεν μπορεί να προσδιοριστεί η αξιοπιστία του πιστοποιητικού – Σε κάποιες περιπτώσεις, το πιστοποιητικό ιστότοπου δεν μπορεί να επαληθευτεί χρησιμοποιώντας το χώρο αποθήκευσης πιστοποιητικών TRCA (Trusted Root Certification Authorities). Κατά συνέπεια, το πιστοποιητικό υπογράφεται από κάποιον (για παράδειγμα, τον διαχειριστή ενός διακομιστή διαδικτύου ή μιας μικρής επιχείρησης) και η θεώρηση του πιστοποιητικού ως αξιόπιστου δεν αποτελεί πάντα κίνδυνο. Οι περισσότερες μεγάλες επιχειρήσεις (για παράδειγμα οι τράπεζες) χρησιμοποιούν ένα πιστοποιητικό υπογεγραμμένο από το TRCA. Εάν επιλέξετε το στοιχείο **Ερώτηση σχετικά με την εγκυρότητα του πιστοποιητικού** (ορίζεται από προεπιλογή), θα ζητηθεί από τον χρήστη να επιλέξει μια ενέργεια όταν δημιουργηθεί κρυπτογραφημένη επικοινωνία. Μπορείτε να επιλέξετε το στοιχείο **Αποκλεισμός της επικοινωνίας η οποία χρησιμοποιεί το πιστοποιητικό** για να τερματίζονται πάντα οι κρυπτογραφημένες συνδέσεις με ιστότοπους που χρησιμοποιούν μη επαληθευμένα πιστοποιητικά.

Εάν το πιστοποιητικό είναι κατεστραμμένο – Αυτό σημαίνει ότι το πιστοποιητικό έχει εσφαλμένη υπογραφή ή καταστράφηκε. Σε αυτή την περίπτωση, η ESET συνιστά να αφήσετε επιλεγμένο το στοιχείο **Αποκλεισμός της επικοινωνίας η οποία χρησιμοποιεί το πιστοποιητικό**. Εάν επιλέξετε το στοιχείο **Ερώτηση σχετικά με την εγκυρότητα του πιστοποιητικού**, θα ζητηθεί από τον χρήστη να επιλέξει μια ενέργεια όταν δημιουργηθεί κρυπτογραφημένη επικοινωνία.

> **Εικονογραφημένα παραδείγματα**
> Τα ακόλουθα άρθρα της Γνωσιακής βάσης της ESET μπορεί να είναι διαθέσιμα μόνο στα Αγγλικά:
> • Ειδοποιήσεις πιστοποιητικών στα οικιακά προϊόντα της ESET για Windows
> • Όταν πραγματοποιείται επίσκεψη σε ιστοσελίδες, εμφανίζεται το μήνυμα «Κρυπτογραφημένη δικτυακή κίνηση: Μη αξιόπιστο πιστοποιητικό»

Πιστοποιητικά

Για να λειτουργεί σωστά η επικοινωνία SSL στα προγράμματα περιήγησης/προγράμματα-πελάτες ηλεκτρονικής αλληλογραφίας, είναι απαραίτητο το πιστοποιητικό ρίζας για το ESET να προστεθεί στη

λίστα γνωστών πιστοποιητικών ρίζας (εκδότες). Θα πρέπει να ενεργοποιηθεί η επιλογή **Προσθήκη του πιστοποιητικού ρίζας σε γνωστά προγράμματα περιήγησης**. Με αυτή την επιλογή θα προστίθεται αυτόματα το πιστοποιητικό ρίζας ESET στα γνωστά προγράμματα περιήγησης (για παράδειγμα, Opera και Firefox). Για προγράμματα περιήγησης που χρησιμοποιούν τον χώρο αποθήκευσης πιστοποιητικών του συστήματος, το πιστοποιητικό προστίθεται αυτόματα (π.χ. Internet Explorer). Για να εφαρμόσετε το πιστοποιητικό σε προγράμματα περιήγησης που δεν υποστηρίζονται, κάντε κλικ στα **Προβολή πιστοποιητικού** > **Λεπτομέρειες** > **Αντιγραφή σε αρχείο** και στη συνέχεια εισαγάγετέ το με μη αυτόματο τρόπο στο πρόγραμμα περιήγησης.

Σε κάποιες περιπτώσεις, το πιστοποιητικό δεν μπορεί να επαληθευτεί χρησιμοποιώντας το χώρο αποθήκευσης πιστοποιητικών Trusted Root Certification Authorities (π.χ. VeriSign). Αυτό σημαίνει ότι το πιστοποιητικό υπογράφεται μόνο του από κάποιον (π.χ. διαχειριστής του διακομιστή Ιστού ή μια μικρή επιχείρηση) και η θεώρηση του πιστοποιητικού ως αξιόπιστο δεν αποτελεί πάντα κίνδυνο. Οι περισσότερες μεγάλες επιχειρήσεις (οι τράπεζες για παράδειγμα) χρησιμοποιούν πιστοποιητικό υπογεγραμμένο από το TRCA.

Αν επιλέξετε **Ερώτηση σχετικά με την εγκυρότητα του πιστοποιητικού** (επιλεγμένο από προεπιλογή), θα ζητηθεί από τον χρήστη να επιλέξει μια ενέργεια όταν δημιουργηθεί κρυπτογραφημένη επικοινωνία. Θα εμφανιστεί ένα παράθυρο διαλόγου επιλογής ενέργειας στο οποίο μπορείτε να αποφασίσετε να επισημάνετε το πιστοποιητικό ως αξιόπιστο ή να το εξαιρέσετε. Αν το πιστοποιητικό δεν υπάρχει στη λίστα TRCA, το παράθυρο θα είναι κόκκινο. Αν το πιστοποιητικό βρίσκεται στη λίστα TRCA, το παράθυρο θα είναι πράσινο.

Μπορείτε να επιλέξετε **Αποκλεισμός της επικοινωνίας η οποία χρησιμοποιεί το πιστοποιητικό** για να τερματίζεται πάντα μια κρυπτογραφημένη σύνδεση με τον ιστότοπο που χρησιμοποιεί μη επαληθευμένο πιστοποιητικό.

Αν το πιστοποιητικό είναι άκυρο ή καταστραμμένο, αυτό σημαίνει ότι το πιστοποιητικό έληξε ή υπογράφηκε μόνο του εσφαλμένα. Σε αυτή την περίπτωση, συνιστάται να αποκλείσετε την επικοινωνία που χρησιμοποιεί το πιστοποιητικό.

Κρυπτογραφημένη κυκλοφορία δικτύου

Εάν το σύστημά σας είναι διαμορφωμένο ώστε να χρησιμοποιεί σάρωση πρωτοκόλλου SSL, θα ανοίξει ένα παράθυρο διαλόγου που θα σάς ζητά να επιλέξετε μια ενέργεια σε δύο περιπτώσεις:

Πρώτα, εάν ένας ιστότοπος χρησιμοποιεί ένα μη επαληθεύσιμο ή μη έγκυρο πιστοποιητικό, και το ESET Internet Security είναι διαμορφωμένο να ρωτά το χρήστη σε τέτοιες περιπτώσεις (από προεπιλογή «ναι» για μη επαληθεύσιμα πιστοποιητικά, «όχι» για μη έγκυρα), σε ένα παράθυρο διαλόγου θα πρέπει να απαντήσετε **Επιτρέπεται** ή **Αποκλεισμός** για τη σύνδεση. Εάν το πιστοποιητικό δεν βρίσκεται στο Trusted Root Certification Authorities store (TRCA), θεωρείται μη αξιόπιστο.

Δεύτερον, εάν η **Λειτουργία φιλτραρίσματος πρωτοκόλλου SSL** είναι **Αλληλεπιδραστική**, ένα παράθυρο διαλόγου για κάθε ιστότοπο θα σας ρωτήσει εάν θα γίνεται **Σάρωση** ή **Παράβλεψη** της κυκλοφορίας. Ορισμένες εφαρμογές βεβαιώνουν ότι η κυκλοφορία SSL δεν τροποποιείται και δεν επιθεωρείται από κανέναν. Σε αυτές τις περιπτώσεις, το ESET Internet Security πρέπει να **παραβλέψει** την κυκλοφορία, προκειμένου να διατηρεί την εφαρμογή σε λειτουργία.

Εικονογραφημένα παραδείγματα

Τα ακόλουθα άρθρα της Γνωσιακής βάσης της ESET μπορεί να είναι διαθέσιμα μόνο στα Αγγλικά:

- Ειδοποιήσεις πιστοποιητικών στα οικιακά προϊόντα της ESET για Windows
- Όταν πραγματοποιείται επίσκεψη σε ιστοσελίδες, εμφανίζεται το μήνυμα «Κρυπτογραφημένη δικτυακή κίνηση: Μη αξιόπιστο πιστοποιητικό»

Και στις δύο περιπτώσεις, ο χρήστης μπορεί να επιλέξει την απομνημόνευση της επιλεγμένης ενέργειας. Οι ενέργειες που θέλετε να απομνημονευτούν αποθηκεύονται στη Λίστα γνωστών πιστοποιητικών.

Λίστα γνωστών πιστοποιητικών

Η **Λίστα γνωστών πιστοποιητικών** μπορεί να χρησιμοποιηθεί για την προσαρμογή της συμπεριφοράς του ESET Internet Security για συγκεκριμένα πιστοποιητικά SSL, καθώς και για την απομνημόνευση ενεργειών εάν είναι επιλεγμένη η **Αλληλεπιδραστική λειτουργία** στο **Φιλτράρισμα πρωτοκόλλου SSL/TLS**. Μπορείτε να προβάλετε και να επεξεργαστείτε τη λίστα στην ενότητα **Ρυθμίσεις για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **SSL/TLS** > **Λίστα γνωστών πιστοποιητικών**.

Το παράθυρο **Λίστα γνωστών πιστοποιητικών** αποτελείται από:

Στήλες

Όνομα – Το όνομα του πιστοποιητικού.

Εκδότης πιστοποιητικού – Το όνομα του δημιουργού του πιστοποιητικού.

Θέμα πιστοποιητικού – Το πεδίο θέματος προσδιορίζει την οντότητα που συσχετίζεται με το δημόσιο κλειδί που είναι αποθηκευμένο στο πεδίο δημόσιου κλειδιού.

Πρόσβαση – Επιλέξτε **Αποδοχή** ή **Αποκλεισμός** για την **Ενέργεια πρόσβασης**, ώστε να επιτρέπεται ή να αποκλείεται η επικοινωνία που προστατεύεται με αυτό το πιστοποιητικό, ανεξάρτητα από την αξιοπιστία του. Επιλέξτε **Αυτόματη**, για να επιτρέπετε τα αξιόπιστα πιστοποιητικά και να ερωτάται ο χρήστης για τα μη αξιόπιστα. Επιλέξτε **Ερώτηση**, για να ερωτάται πάντα ο χρήστης για το τι πρέπει να γίνει.

Σάρωση – Επιλέξτε **Σάρωση** ή **Παράβλεψη** για την **Ενέργεια σάρωσης**, για να πραγματοποιείται σάρωση ή παράβλεψη της επικοινωνίας που προστατεύεται με αυτό το πιστοποιητικό. Επιλέξτε **Αυτόματη**, για σάρωση στην αυτόματη λειτουργία και ερώτηση στην αλληλεπιδραστική λειτουργία. Επιλέξτε **Ερώτηση**, για να ερωτάται πάντα ο χρήστης για το τι πρέπει να γίνει.

Στοιχεία ελέγχου

Προσθήκη – Προσθέστε ένα νέο πιστοποιητικό και διαμορφώστε τις ρυθμίσεις του σχετικά με τις επιλογές πρόσβασης και σάρωσης.

Επεξεργασία – Επιλέξτε το πιστοποιητικό που θέλετε να διαμορφώσετε και κάντε κλικ στο κουμπί **Επεξεργασία**.

Διαγραφή – Επιλέξτε το πιστοποιητικό που θέλετε να διαγράψετε και κάντε κλικ στο κουμπί **Κατάργηση**.

OK/Ακύρωση – Κάντε κλικ στο κουμπί **OK**, εάν θέλετε να αποθηκεύσετε τις αλλαγές, ή στο κουμπί **Ακύρωση** για έξοδο χωρίς αποθήκευση των αλλαγών.

Λίστα εφαρμογών με φιλτράρισμα SSL/TLS

Η **Λίστα εφαρμογών με φιλτράρισμα SSL/TLS** μπορεί να χρησιμοποιηθεί για την προσαρμογή της συμπεριφοράς του ESET Internet Security για συγκεκριμένες εφαρμογές, καθώς και για την απομνημόνευση επιλεγμένων ενεργειών, όταν το στοιχείο **Λειτουργία φιλτραρίσματος πρωτοκόλλου SSL/TLS** έχει ρυθμιστεί σε **Αλληλεπιδραστική λειτουργία**. Μπορείτε να δείτε και να επεξεργαστείτε τη λίστα στην ενότητα **Εγκατάσταση για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **SSL/TLS** > **Λίστα εφαρμογών με φιλτράρισμα SSL/TLS**.

Το παράθυρο **Λίστα εφαρμογών με φιλτράρισμα SSL/TLS** αποτελείται από:

Στήλες

Εφαρμογή – Επιλέξτε ένα εκτελέσιμο αρχείο από το δέντρο καταλόγων, κάντε κλικ στην επιλογή **...** ή καταχωρίστε τη διαδρομή με μη αυτόματο τρόπο.

Ενέργεια σάρωσης – Επιλέξτε **Σάρωση** ή **Παράβλεψη** για να πραγματοποιείται σάρωση ή παράβλεψη της επικοινωνίας. Επιλέξτε **Αυτόματη**, για σάρωση στην αυτόματη λειτουργία και ερώτηση στην αλληλεπιδραστική λειτουργία. Επιλέξτε **Ερώτηση**, για να ερωτάται πάντα ο χρήστης για το τι πρέπει να γίνει.

Στοιχεία ελέγχου

Προσθήκη – Προσθέστε την εφαρμογή που θα φιλτράρεται.

Επεξεργασία – Επιλέξτε την εφαρμογή της οποίας τις παραμέτρους θέλετε να ρυθμίσετε και κάντε κλικ στο στοιχείο **Επεξεργασία**.

Κατάργηση – Επιλέξτε την εφαρμογή που θέλετε να καταργήσετε και κάντε κλικ στο στοιχείο **Κατάργηση**.

Εισαγωγή/Εξαγωγή – Εισαγάγετε εφαρμογές από ένα αρχείο ή αποθηκεύστε την τρέχουσα λίστα εφαρμογών σας σε ένα αρχείο.

OK/Ακύρωση – Κάντε κλικ στο κουμπί **OK**, εάν θέλετε να αποθηκεύσετε τις αλλαγές, ή στο κουμπί **Ακύρωση** για έξοδο χωρίς αποθήκευση των αλλαγών.

Προστασία ηλεκτρονικής αλληλογραφίας

Ανατρέξτε στο θέμα Ενσωμάτωση του ESET Internet Security με το πρόγραμμα ηλεκτρονικής αλληλογραφίας για να ρυθμίσετε τις παραμέτρους της ενσωμάτωσης.

Οι ρυθμίσεις του προγράμματος ηλεκτρονικής αλληλογραφίας βρίσκονται στην ενότητα **Ρυθμίσεις**

για προχωρημένους (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία ηλεκτρονικής αλληλογραφίας** > **Προγράμματα ηλεκτρονικής αλληλογραφίας**.

Προγράμματα ηλεκτρονικής αλληλογραφίας

Ενεργοποίηση προστασίας email μέσω προσθέτων προγραμμάτων πελάτη – Εάν έχει απενεργοποιηθεί, είναι ανενεργή η προστασία μέσω πρόσθετων προγραμμάτων-πελάτη email.

Αλληλογραφία που θα σαρωθεί

Επιλέξτε email για σάρωση:

- **Ληφθείσα Email**
- **Απεσταλμένη Email**
- **Αναγνωσμένη Email**
- **Τροποποιημένο Email**

> Συνιστάται να διατηρείτε ενεργή η επιλογή **Ενεργοποίηση προστασίας email μέσω προσθέτων προγραμμάτων-πελάτη**. Ακόμα κι αν δεν είναι ενεργοποιημένη η ενοποίηση, η επικοινωνία email εξακολουθεί να προστατεύεται από το Φιλτράρισμα πρωτοκόλλων (IMAP/IMAPS και POP3/POP3S).

Ενέργεια που θα πραγματοποιηθεί σε μολυσμένο μήνυμα ηλεκτρονικού ταχυδρομείου

Καμία ενέργεια – Αν είναι ενεργοποιημένη, το πρόγραμμα θα αναγνωρίσει τα μολυσμένα συνημμένα, αλλά θα αφήσει την αλληλογραφία χωρίς να προβεί σε καμία ενέργεια.

Διαγραφή αλληλογραφίας – Το πρόγραμμα θα ειδοποιήσει το χρήστη για την ή τις εισβολές και θα διαγράψει το μήνυμα.

Μετακίνηση αλληλογραφίας στο φάκελο Διαγραμμένων στοιχείων – Η μολυσμένη αλληλογραφία θα μετακινηθεί αυτόματα στο φάκελο «Διαγραμμένα».

Μετακίνηση email σε φάκελο (προεπιλεγμένη ενέργεια) – Τα μολυσμένα email θα μετακινηθούν αυτόματα στον καθορισμένο φάκελο.

Φάκελος – Καθορίστε τον προσαρμοσμένο φάκελο στον οποίο θέλετε να μετακινείται η μολυσμένη αλληλογραφία μόλις ανιχνευτεί.

Ενοποίηση προγράμματος ηλεκτρονικής αλληλογραφίας

Η ενοποίηση του ESET Internet Security με το πρόγραμμα-πελάτη ηλεκτρονικής αλληλογραφίας σας αυξάνει το επίπεδο ενεργής προστασίας κατά του κακόβουλου κώδικα σε μηνύματα ηλεκτρονικής αλληλογραφίας. Αν υποστηρίζεται το πρόγραμμα-πελάτης ηλεκτρονικής αλληλογραφίας που χρησιμοποιείτε, η ενοποίηση μπορεί να ενεργοποιηθεί στο ESET Internet Security. Μετά την ενοποίηση

με το πρόγραμμα-πελάτη ηλεκτρονικής αλληλογραφίας σας, η γραμμή εργαλείων του ESET Internet Security εισάγεται απευθείας στο πρόγραμμα-πελάτη ηλεκτρονικής αλληλογραφίας, για πιο αποτελεσματική προστασία της ηλεκτρονικής αλληλογραφίας. Οι ρυθμίσεις ενοποίησης βρίσκονται στην ενότητα **Ρυθμίσεις για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία ηλεκτρονικής αλληλογραφίας** > **Ενοποίηση προγράμματος ηλεκτρονικής αλληλογραφίας**.

Τα προγράμματα-πελάτες ηλεκτρονικής αλληλογραφίας που υποστηρίζονται αυτή τη στιγμή περιλαμβάνουν το Microsoft Outlook, το Outlook Express, το Windows Mail και το Windows Live Mail. Η προστασία ηλεκτρονικής αλληλογραφίας λειτουργεί ως πρόσθετο για αυτά τα προγράμματα. Το κύριο πλεονέκτημα της προσθήκης είναι ότι είναι ανεξάρτητη από το πρωτόκολλο που χρησιμοποιείται. Όταν το πρόγραμμα–πελάτης ηλεκτρονικής αλληλογραφίας λαμβάνει ένα κρυπτογραφημένο μήνυμα, αυτό αποκρυπτογραφείται και αποστέλλεται στη σάρωση για ιούς. Για μια πλήρη λίστα των προγραμμάτων-πελάτες ηλεκτρονικής αλληλογραφίας και των εκδόσεών τους που υποστηρίζονται, ανατρέξτε στο ακόλουθο άρθρο της Γνωσιακής βάσης της ESET.

Απενεργοποιήστε τη **Βελτιστοποίηση χειρισμού συνημμένων** και την **Επεξεργασία προγράμματος ηλεκτρονικής αλληλογραφίας για προχωρημένους** εάν αντιμετωπίσετε επιβράδυνση του συστήματος κατά την ανάκτηση email.

Γραμμή εργαλείων του Microsoft Outlook

Η προστασία Microsoft Outlook λειτουργεί ως μονάδα προσθήκης. Μετά από την εγκατάσταση του ESET Internet Security, προστίθεται αυτή η γραμμή εργαλείων που περιέχει τις επιλογές προστασίας antivirus/antispam στο Microsoft Outlook:

Ανεπιθύμητο – Επισημαίνει επιλεγμένα μηνύματα ως ανεπιθύμητα. Μετά από την επισήμανση, αποστέλλεται ένα «δακτυλικό αποτύπωμα» του μηνύματος σε έναν κεντρικό διακομιστή όπου αποθηκεύονται στοιχεία αναγνώρισης ανεπιθύμητων μηνυμάτων. Αν ο διακομιστής λάβει περισσότερα παρόμοια «δακτυλικά αποτυπώματα» από πολλούς χρήστες, το μήνυμα θα ταξινομείται ως ανεπιθύμητο στο μέλλον.

Μη ανεπιθύμητο – Επισημαίνει επιλεγμένα μηνύματα ως μη ανεπιθύμητα.

Διεύθυνση ανεπιθύμητου περιεχομένου (λίστα αποκλεισμένων διευθύνσεων, μια λίστα με ανεπιθύμητες διευθύνσεις) – Προσθέτει μια νέα διεύθυνση αποστολέα στη Λίστα αποκλεισμένων διευθύνσεων. Όλα τα μηνύματα που λαμβάνονται από τη λίστα θα ταξινομούνται αυτόματα ως ανεπιθύμητα.

> ⚠ Να προσέχετε το spoofing – την πλαστογράφηση της διεύθυνσης ενός αποστολέα σε μηνύματα ηλεκτρονικής αλληλογραφίας με στόχο την παραπλάνηση των παραληπτών ηλεκτρονικής αλληλογραφίας ώστε να διαβάσουν τα μηνύματα και να ανταποκριθούν.

Αξιόπιστη διεύθυνση (λίστα μη αποκλεισμένων διευθύνσεων, μια λίστα με αξιόπιστες διευθύνσεις) – Προσθέτει μια νέα διεύθυνση αποστολέα στη Λίστα μη αποκλεισμένων διευθύνσεων. Όλα τα μηνύματα που λαμβάνονται από διευθύνσεις που βρίσκονται στη Λίστα μη αποκλεισμένων διευθύνσεων δεν θα ταξινομούνται ποτέ αυτόματα ως ανεπιθύμητα.

ESET Internet Security – Κάντε διπλό κλικ στο εικονίδιο για να ανοίξετε το κύριο παράθυρο του ESET Internet Security.

Επανάληψη σάρωσης μηνυμάτων – Επιτρέπει την έναρξη ελέγχου ηλεκτρονικής αλληλογραφίας με μη αυτόματο τρόπο. Μπορείτε να καθορίσετε μηνύματα που θα ελεγχθούν και μπορείτε να ενεργοποιήσετε την επανάληψη σάρωσης της ληφθείσας ηλεκτρονικής αλληλογραφίας. Για περισσότερες πληροφορίες, δείτε την ενότητα Προστασία ηλεκτρονικής αλληλογραφίας.

Ρυθμίσεις σάρωσης – Εμφανίζει τις επιλογές ρυθμίσεων της ενότητας Προστασία ηλεκτρονικής αλληλογραφίας.

Ρύθμιση Antispam – Εμφανίζει τις επιλογές ρυθμίσεων της ενότητας Προστασία Antispam.

Βιβλία διευθύνσεων – Ανοίγει το παράθυρο προστασίας Antispam, όπου μπορείτε να αποκτήσετε πρόσβαση σε λίστες με εξαιρούμενες, αξιόπιστες και ανεπιθύμητες διευθύνσεις.

Γραμμή εργαλείων Outlook Express και Windows Mail

Η προστασία του Outlook Express και του Windows Mail λειτουργεί ως μονάδα προσθήκης. Μετά από την εγκατάσταση του ESET Internet Security, προστίθεται αυτή η γραμμή εργαλείων που περιέχει τις επιλογές προστασίας antivirus/antispam στο Outlook Express ή το Windows Mail:

Ανεπιθύμητο – Επισημαίνει επιλεγμένα μηνύματα ως ανεπιθύμητα. Μετά από την επισήμανση, αποστέλλεται ένα «δακτυλικό αποτύπωμα» του μηνύματος σε έναν κεντρικό διακομιστή όπου αποθηκεύονται στοιχεία αναγνώρισης ανεπιθύμητων μηνυμάτων. Αν ο διακομιστής λάβει περισσότερα παρόμοια «δακτυλικά αποτυπώματα» από πολλούς χρήστες, το μήνυμα θα ταξινομείται ως ανεπιθύμητο στο μέλλον.

Μη ανεπιθύμητο – Επισημαίνει επιλεγμένα μηνύματα ως μη ανεπιθύμητα.

Διεύθυνση ανεπιθύμητου περιεχομένου – Προσθέτει μια νέα διεύθυνση αποστολέα στη Λίστα αποκλεισμένων διευθύνσεων. Όλα τα μηνύματα που λαμβάνονται από τη λίστα θα ταξινομούνται αυτόματα ως ανεπιθύμητα.

> ⚠ Να προσέχετε το spoofing – την πλαστογράφηση της διεύθυνσης ενός αποστολέα σε μηνύματα ηλεκτρονικής αλληλογραφίας με στόχο την παραπλάνηση των παραληπτών ηλεκτρονικής αλληλογραφίας ώστε να διαβάσουν τα μηνύματα και να ανταποκριθούν.

Αξιόπιστη διεύθυνση – Προσθέτει μια νέα διεύθυνση αποστολέα στη λίστα μη αποκλεισμένων διευθύνσεων. Όλα τα μηνύματα που λαμβάνονται από διευθύνσεις που βρίσκονται στη Λίστα μη αποκλεισμένων διευθύνσεων δεν θα ταξινομούνται ποτέ αυτόματα ως ανεπιθύμητα.

ESET Internet Security – Κάντε διπλό κλικ στο εικονίδιο για να ανοίξετε το κύριο παράθυρο του ESET Internet Security.

Επανάληψη σάρωσης μηνυμάτων – Επιτρέπει την έναρξη ελέγχου ηλεκτρονικής αλληλογραφίας με μη αυτόματο τρόπο. Μπορείτε να καθορίσετε μηνύματα που θα ελεγχθούν και μπορείτε να ενεργοποιήσετε την επανάληψη σάρωσης της ληφθείσας ηλεκτρονικής αλληλογραφίας. Για περισσότερες πληροφορίες, δείτε την ενότητα Προστασία ηλεκτρονικής αλληλογραφίας.

Ρυθμίσεις σάρωσης – Εμφανίζει τις επιλογές ρυθμίσεων της ενότητας Προστασία ηλεκτρονικής αλληλογραφίας.

Ρύθμιση Antispam – Εμφανίζει τις επιλογές ρυθμίσεων της ενότητας Προστασία Antispam.

Περιβάλλον χρήστη

Προσαρμογή εμφάνισης – Η εμφάνιση της γραμμής εργαλείων μπορεί να τροποποιηθεί για το πρόγραμμα-πελάτη ηλεκτρονικής αλληλογραφίας που χρησιμοποιείτε. Καταργήστε την επιλογή για να προσαρμόσετε την εμφάνιση ανεξάρτητα από τις παραμέτρους του προγράμματος ηλεκτρονικής αλληλογραφίας.

Εμφάνιση κειμένου – Εμφανίζει περιγραφές για εικονίδια.

Κείμενο στα δεξιά – Οι περιγραφές επιλογών μετακινούνται από το κάτω μέρος στα δεξιά των εικονιδίων.

Μεγάλα εικονίδια – Εμφανίζει μεγάλα εικονίδια για επιλογές μενού.

Παράθυρο διαλόγου επιβεβαίωσης

Η ειδοποίηση αυτή εξυπηρετεί ώστε να επιβεβαιώνεται ότι ο χρήστης θέλει πραγματικά να εκτελέσει την επιλεγμένη ενέργεια, κάτι που θα πρέπει να εξαλείφει πιθανά λάθη.

Από την άλλη μεριά, το παράθυρο διαλόγου προσφέρει επίσης την επιλογή απενεργοποίησης των επιβεβαιώσεων.

Επανάληψη σάρωσης μηνυμάτων

Η γραμμή εργαλείων του ESET Internet Security που είναι ενοποιημένη στα προγράμματα-πελάτες ηλεκτρονικής αλληλογραφίας επιτρέπει στους χρήστες να καθορίσουν πολλές επιλογές για τον έλεγχο της ηλεκτρονικής αλληλογραφίας. Η επιλογή **Επανάληψη σάρωσης μηνυμάτων** προσφέρει δύο λειτουργίες σάρωσης:

Όλα τα μηνύματα στον τρέχοντα φάκελο – Σαρώνει τα μηνύματα που βρίσκονται στο φάκελο που προβάλλεται αυτή τη στιγμή.

Μόνο επιλεγμένα μηνύματα – Σαρώνει μόνο μηνύματα που επισημαίνονται από το χρήστη.

Το πλαίσιο ελέγχου **Επανάληψη σάρωσης ήδη σαρωμένων μηνυμάτων** παρέχει στον χρήστη την επιλογή να εκτελέσει κι άλλη σάρωση σε μηνύματα που έχουν σαρωθεί προηγουμένως.

Πρωτόκολλα ηλεκτρονικής αλληλογραφίας

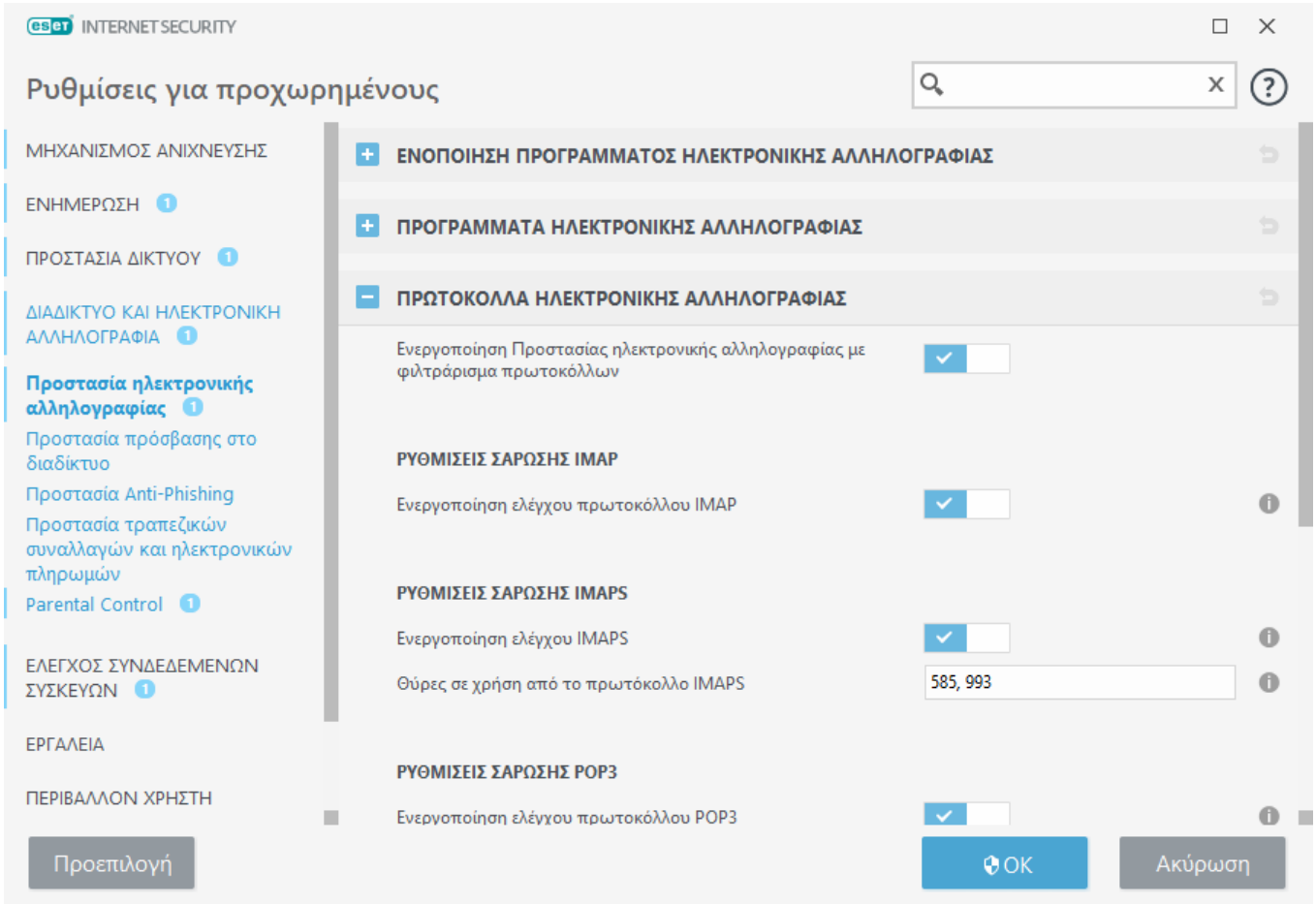
Τα πρωτόκολλα IMAP και POP3 είναι τα πιο ευρέως διαδεδομένα πρωτόκολλα που χρησιμοποιούνται για τη λήψη επικοινωνίας email σε μια εφαρμογή προγράμματος-πελάτη email. Το Internet Message Access Protocol (IMAP) είναι άλλο ένα πρωτόκολλο διαδικτύου για ανάκτηση ηλεκτρονικής αλληλογραφίας. Το IMAP έχει ορισμένα πλεονεκτήματα σε σχέση με το POP3, για παράδειγμα, μπορούν πολλά προγράμματα-πελάτες να συνδέονται ταυτόχρονα με το ίδιο γραμματοκιβώτιο και να διατηρούν πληροφορίες κατάστασης μηνυμάτων, όπως αν διαβάστηκε το μήνυμα, αν απαντήθηκε ή αν καταργήθηκε. Η λειτουργική μονάδα προστασίας που παρέχει αυτό το στοιχείο ελέγχου ξεκινά αυτόματα κατά την εκκίνηση του συστήματος και στη συνέχεια δραστηριοποιείται στη μνήμη.

Το ESET Internet Security παρέχει προστασία για αυτά τα πρωτόκολλα, ανεξάρτητα από το πρόγραμμα-πελάτη email που χρησιμοποιείται και χωρίς να απαιτείται εκ νέου ρύθμιση παραμέτρων του προγράμματος-πελάτη email. Από προεπιλογή, όλη η επικοινωνία μέσω πρωτοκόλλων POP3 και IMAP σαρώνεται, ανεξάρτητα από τους προεπιλεγμένους αριθμούς θύρας POP3/IMAP.
Το πρωτόκολλο IMAP δεν σαρώνεται. Ωστόσο, η επικοινωνία με το διακομιστή Microsoft Exchange μπορεί να σαρωθεί από τη λειτουργική μονάδα ενοποίησης σε προγράμματα-πελάτη email όπως το Microsoft Outlook.

Συνιστάται να διατηρούνται ενεργοποιημένες οι επιλογές **Ενεργοποίηση προστασίας email με φιλτράρισμα πρωτοκόλλων**. Για να ρυθμίσετε τις παραμέτρους του ελέγχου πρωτοκόλλου IMAP/IMAPS και POP3/POP3S, μεταβείτε στη διαδρομή **Ρυθμίσεις για προχωρημένους** > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία ηλεκτρονικής αλληλογραφίας** > **Πρωτόκολλα ηλεκτρονικής αλληλογραφίας**.

Το ESET Internet Security υποστηρίζει επίσης τη σάρωση πρωτοκόλλων IMAPS (585, 993) και POP3S (995), τα οποία χρησιμοποιούν έναν κρυπτογραφημένο δίαυλο για τη μεταφορά πληροφοριών μεταξύ διακομιστή και προγράμματος-πελάτη. Το ESET Internet Security ελέγχει τις επικοινωνίες που χρησιμοποιούν πρωτόκολλα SSL (Secure Socket Layer) και TLS (Transport Layer Security). Το πρόγραμμα θα σαρώνει μόνο την κυκλοφορία στη θύρες που καθορίζονται στη ρύθμιση **Θύρες που χρησιμοποιούνται από το πρωτόκολλο IMAPS/POP3S**, ανεξάρτητα από την έκδοση του λειτουργικού συστήματος. Μπορούν να προστεθούν και άλλες θύρες επικοινωνίας εάν απαιτείται. Οι πολλαπλοί αριθμοί θυρών πρέπει να διαχωρίζονται με κόμμα.

Η κρυπτογραφημένη επικοινωνία θα σαρώνεται από προεπιλογή. Για να δείτε τις ρυθμίσεις σάρωσης, ανοίξτε τα στοιχεία «Ρυθμίσεις για προχωρημένους» > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **SSL/TLS**.



Φίλτρο POP3, POP3S

Το πρωτόκολλο POP3 είναι το πιο ευρέως διαδεδομένο πρωτόκολλο που χρησιμοποιείται για τη λήψη επικοινωνίας ηλεκτρονικής αλληλογραφίας σε μια εφαρμογή προγράμματος-πελάτη ηλεκτρονικής αλληλογραφίας. Το ESET Internet Security παρέχει προστασία για αυτό το πρωτόκολλο ανεξάρτητα από το πρόγραμμα-πελάτη ηλεκτρονικής αλληλογραφίας που χρησιμοποιείται.

Η λειτουργική μονάδα προστασίας που παρέχει αυτό το στοιχείο ελέγχου ξεκινά αυτόματα κατά την εκκίνηση του συστήματος και στη συνέχεια δραστηριοποιείται στη μνήμη. Για να λειτουργεί σωστά η μονάδα, βεβαιωθείτε ότι είναι ενεργοποιημένη – ο έλεγχος πρωτοκόλλου POP3 εκτελείται αυτόματα χωρίς να απαιτείται αναδιαμόρφωση του προγράμματος-πελάτη ηλεκτρονικής αλληλογραφίας. Από προεπιλογή, σαρώνονται όλες οι επικοινωνίες στη θύρα 110, αλλά αν χρειάζεται μπορούν να προστεθούν κι άλλες θύρες επικοινωνίας. Οι πολλαπλοί αριθμοί θυρών πρέπει να διαχωρίζονται με κόμμα.

Η κρυπτογραφημένη επικοινωνία θα σαρώνεται από προεπιλογή. Για να δείτε τις ρυθμίσεις σάρωσης, ανοίξτε τα στοιχεία «Ρυθμίσεις για προχωρημένους» > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **SSL/TLS**.

Σε αυτή την ενότητα μπορείτε να διαμορφώσετε τον έλεγχο πρωτοκόλλου POP3 και POP3S.

Ενεργοποίηση ελέγχου πρωτοκόλλου POP3 – Αν είναι ενεργοποιημένο, όλη η κίνηση μέσω του POP3 παρακολουθείται για κακόβουλο λογισμικό.

Θύρες που χρησιμοποιούνται από το πρωτόκολλο POP3 – Μια λίστα θυρών που χρησιμοποιείται από το πρωτόκολλο POP3 (110 από προεπιλογή).

Το ESET Internet Security υποστηρίζει επίσης τον έλεγχο πρωτοκόλλου POP3S. Αυτός ο τύπος επικοινωνίας χρησιμοποιεί έναν κρυπτογραφημένο δίαυλο για τη μεταφορά πληροφοριών μεταξύ διακομιστή και προγράμματος-πελάτη. Το ESET Internet Security ελέγχει τις επικοινωνίες που χρησιμοποιούν μεθόδους κρυπτογράφησης SSL (Secure Socket Layer) και TLS (Transport Layer Security).

Να μη γίνεται έλεγχος πρωτοκόλλου POP3S – Οι κρυπτογραφημένες επικοινωνίες δεν θα ελέγχονται.

Χρήση πρωτοκόλλου POP3S για τον έλεγχο επιλεγμένων θυρών – Επιλέξτε για να ενεργοποιηθεί ο έλεγχος POP3S μόνο για θύρες που καθορίζονται στο στοιχείο **Θύρες που χρησιμοποιούνται από το πρωτόκολλο POP3S**.

Θύρες που χρησιμοποιούνται από το πρωτόκολλο POP3S – Μια λίστα θυρών POP3S που θα ελέγχονται (995 από προεπιλογή).

Ετικέτες email

Οι επιλογές για αυτήν τη λειτουργικότητα είναι διαθέσιμες στις **Ρυθμίσεις για προχωρημένους** > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία προγράμματος-πελάτη ηλεκτρονικής αλληλογραφίας** > **Συναγερμοί και ειδοποιήσεις**.

Όταν ελεγχθεί ένα μήνυμα ηλεκτρονικής αλληλογραφίας, μπορεί να επισυναφθεί στο μήνυμα μια ειδοποίηση με το αποτέλεσμα της σάρωσης. Μπορείτε να επιλέξετε **Επισύναψη ετικετών σε**

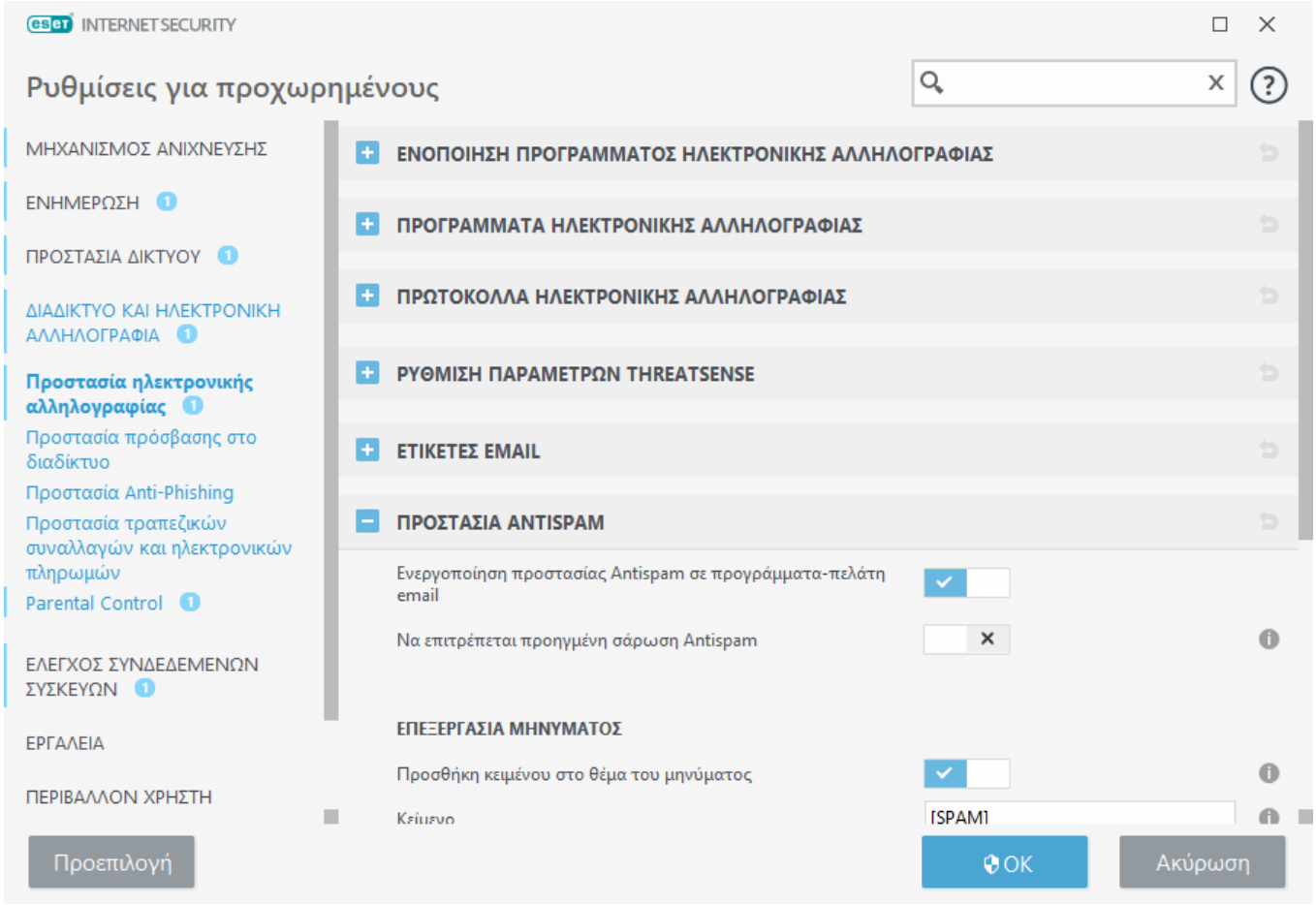
ληφθέντα και αναγνωσμένα μηνύματα email ή **Επισύναψη ετικετών σε απεσταλμένα μηνύματα**. Θα πρέπει να γνωρίζετε ότι σε σπάνιες περιπτώσεις οι ετικέτες μπορεί να παραλείπονται σε προβληματικά μηνύματα HTML ή εάν τα μηνύματα είναι παραποιημένα από κακόβουλο λογισμικό. Οι ετικέτες μπορούν να προστεθούν σε ληφθέντα και αναγνωσμένα μηνύματα, απεσταλμένα μηνύματα ή και στα δύο. Οι διαθέσιμες επιλογές είναι οι παρακάτω:

- **Ποτέ** – Δεν θα προστίθεται καμία ετικέτα.
- **Όταν παρουσιάζεται μια ανίχνευση** – Θα επισημαίνονται ως ελεγμένα μόνο μηνύματα που περιέχουν κακόβουλο λογισμικό (προεπιλογή).
- **Σε όλα τα email κατά τη σάρωση** – Το πρόγραμμα θα επισυνάπτει ετικέτες σε όλα τα σαρωμένα email.

Κείμενο που θα προστίθεται στο θέμα ανιχνευμένων μηνυμάτων email – Επεξεργαστείτε αυτό το πρότυπο αν θέλετε να τροποποιήσετε τη μορφή προθέματος του θέματος ενός μολυσμένου email. Η λειτουργία αυτή θα αντικαταστήσει το θέμα μηνύματος «Γεια σας» με την ακόλουθη μορφή: «[ανίχνευση %DETECTIONNAME%] Γεια σας». Η μεταβλητή %DETECTIONNAME% αντιπροσωπεύει την ανίχνευση.

Προστασία Antispam

Τα ανεπιθύμητα email, που ονομάζονται ανεπιθύμητα μηνύματα, αποτελούν ένα από τα μεγαλύτερα προβλήματα της ηλεκτρονικής επικοινωνίας. Τα μηνύματα spam αντιπροσωπεύουν 30 τοις εκατό του συνόλου της επικοινωνίας με ηλεκτρονική αλληλογραφία. Η προστασία Antispam προστατεύει από αυτό το πρόβλημα. Ο συνδυασμός διαφόρων αρχών ασφάλειας email που διαθέτει η λειτουργική μονάδα Antispam παρέχει ανώτερο φιλτράρισμα για να διατηρείται καθαρό το γραμματοκιβώτιο εισερχομένων σας. Για να ρυθμίσετε τις παραμέτρους της προστασίας antispam, ανοίξτε τα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία ηλεκτρονικής αλληλογραφίας** > **Προστασία Antispam**.



Για την ανίχνευση ανεπιθύμητων μηνυμάτων, μια σημαντική αρχή είναι η αναγνώριση ανεπιθύμητων email με βάση προκαθορισμένες αξιόπιστες διευθύνσεις (επιτρεπτές) και διευθύνσεις ανεπιθύμητων μηνυμάτων (αποκλεισμένες).

Η κύρια μέθοδος που χρησιμοποιείται για την ανίχνευση ανεπιθύμητων μηνυμάτων είναι η σάρωση των ιδιοτήτων του μηνύματος email. Τα ληφθέντα μηνύματα σαρώνονται για τα βασικά κριτήρια Antispam (ορισμοί μηνύματος, στατιστικοί ευριστικοί έλεγχοι, αναγνώριση αλγόριθμων ή άλλες μοναδικές μέθοδοι) και η τιμή ευρετηρίου που προκύπτει προσδιορίζει αν ένα μήνυμα είναι spam ή όχι.

Ενεργοποίηση προστασίας Antispam σε προγράμματα ηλεκτρονικής αλληλογραφίας – Όταν ενεργοποιηθεί, η Προστασία Antispam θα ενεργοποιείται αυτόματα κατά την εκκίνηση του συστήματος.

Να επιτρέπεται προηγμένη σάρωση Antispam – Θα γίνεται περιοδική λήψη πρόσθετων βάσεων δεδομένων Antispam, αυξάνοντας τις δυνατότητες Antispam για καλύτερα αποτελέσματα.

Η Προστασία Antispam του ESET Internet Security σάς επιτρέπει να ρυθμίσετε διαφορετικές παραμέτρους για τα μηνύματα.

Επεξεργασία μηνύματος

Προσθήκη κειμένου στο θέμα του μηνύματος – Επιτρέπει την προσθήκη προσαρμοσμένης συμβολοσειράς προθέματος στη γραμμή θέματος των μηνυμάτων που έχουν ταξινομηθεί ως spam. Η προεπιλογή είναι «[SPAM]».

Μετακίνηση μηνυμάτων στο φάκελο μηνυμάτων spam – Όταν είναι ενεργοποιημένη αυτή η

επιλογή τα μηνύματα spam θα μετακινούνται στον προεπιλεγμένο φάκελο ανεπιθύμητης αλληλογραφίας. Επίσης, μηνύματα αναταξινομημένα ως μη ανεπιθύμητα θα μετακινούνται στα εισερχόμενα. Όταν κάνετε δεξί κλικ σε ένα μήνυμα και επιλέξετε ESET Internet Security από το μενού περιβάλλοντος, μπορείτε να επιλέξετε μία από τις διαθέσιμες επιλογές.

Χρήση του φακέλου – Καθορίστε τον προσαρμοσμένο φάκελο στον οποίο θέλετε να μετακινείται η μολυσμένη αλληλογραφία μόλις ανιχνευτεί.

Σήμανση ανεπιθύμητων μηνυμάτων (spam) ως αναγνωσμένων – Ενεργοποιήστε αυτή την επιλογή για να επισημαίνονται αυτόματα τα μηνύματα spam ως αναγνωσμένα. Θα σας βοηθήσει να εστιάζετε την προσοχή σας στα «καθαρά» μηνύματα.

Σήμανση αναταξινομημένων μηνυμάτων ως μη αναγνωσμένων – Τα μηνύματα που ταξινομήθηκαν αρχικά ως spam, αλλά επισημάνθηκαν αργότερα ως «καθαρά» θα εμφανίζονται ως μη αναγνωσμένα.

Καταγραφή βαθμολογίας spam – Ο μηχανισμός Antispam του ESET Internet Security αντιστοιχίζει μια βαθμολογία spam σε κάθε μήνυμα που σαρώνεται. Το μήνυμα θα καταγράφεται στο αρχείο καταγραφής antispam (το κύριο παράθυρο του προγράμματος > **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής** > **Προστασία Antispam**).

- **Καμία** – Δεν θα καταγράφεται η βαθμολογία μετά τη σάρωση Antispam.
- **Αναταξινομήθηκε και επισημάνθηκε ως ανεπιθύμητο** – Επιλέξτε εάν θέλετε να καταγράφεται μια βαθμολογία spam για μηνύματα που έχουν σημανθεί ως SPAM.
- **Όλα** – Όλα τα μηνύματα θα καταγράφονται στο αρχείο καταγραφής με μια βαθμολογία spam.

Όταν κάνετε κλικ σε ένα μήνυμα στο φάκελο ανεπιθύμητης αλληλογραφίας, μπορείτε να επιλέξετε **Αναταξινόμηση επιλεγμένων μηνυμάτων ως ΜΗ ανεπιθύμητων** και το μήνυμα θα μετακινηθεί στα εισερχόμενα. Όταν κάνετε κλικ σε ένα μήνυμα στα εισερχόμενα το οποίο θεωρείτε ανεπιθύμητο, μπορείτε να επιλέξετε **Αναταξινόμηση μηνυμάτων ως ανεπιθύμητων** και το μήνυμα θα μετακινηθεί στο φάκελο ανεπιθύμητης αλληλογραφίας. Μπορείτε να επιλέξετε πολλά μηνύματα και να κάνετε ενέργειες που τα αφορούν όλα ταυτόχρονα.

Το ESET Internet Security υποστηρίζει προστασία Antispam για τις εφαρμογές Microsoft Outlook, Outlook Express, Windows Mail και Windows Live Mail.

Αποτέλεσμα επεξεργασίας διευθύνσεων

Κατά την προσθήκη νέων διευθύνσεων ή κατά την αλλαγή της ενέργειας που εκτελείται για τη διεύθυνση email, το ESET Internet Security εμφανίζει μηνύματα ειδοποίησης. Το περιεχόμενο των μηνυμάτων ειδοποίησης διαφέρει ανάλογα με την ενέργεια που προσπαθείτε να εκτελέσετε.

Επιλέξτε το πλαίσιο ελέγχου **Να μην ερωτηθώ ξανά** για να εκτελεστεί αυτόματα η ενέργεια την επόμενη φορά χωρίς την εμφάνιση του μηνύματος.

Λίστες διευθύνσεων antispam

Η δυνατότητα Antispam στο ESET Internet Security σάς επιτρέπει να διαμορφώσετε διάφορες παραμέτρους για λίστες διευθύνσεων.

Ενεργοποίηση λίστας διευθύνσεων χρήστη – Ενεργοποιήστε αυτήν την επιλογή για να ενεργοποιήσετε τη λίστα διευθύνσεων του χρήστη.

Λίστα διευθύνσεων χρήστη – Λίστα διευθύνσεων email όπου μπορείτε να προσθέσετε, να επεξεργαστείτε ή να καταργήσετε διευθύνσεις για να ορίσετε τους κανόνες antispam. Οι κανόνες αυτής της λίστας θα εφαρμοστούν στον τρέχοντα χρήστη.

Ενεργοποίηση γενικών λιστών διευθύνσεων – Ενεργοποιήστε αυτή την επιλογή για να ενεργοποιηθεί η γενική λίστα διευθύνσεων για κοινή χρήση με όλους τους χρήστες σε αυτήν τη συσκευή.

Γενική λίστα διευθύνσεων – Λίστα διευθύνσεων email όπου μπορείτε να προσθέσετε, να επεξεργαστείτε ή να καταργήσετε διευθύνσεις για να ορίσετε τους κανόνες antispam. Οι κανόνες αυτής της λίστας θα εφαρμοστούν σε όλους τους χρήστες.

Να επιτρέπεται αυτόματα και να προστίθεται στη λίστα διευθύνσεων χρήστη

Να θεωρούνται αξιόπιστες οι διευθύνσεις από αυτό το βιβλίο διευθύνσεων – Οι διευθύνσεις από τη λίστα επαφών σας θα θεωρούνται αξιόπιστες, χωρίς να προστίθενται στη λίστα διευθύνσεων χρήστη.

Προσθήκη διευθύνσεων παραληπτών από εξερχόμενα μηνύματα – Προσθέστε διευθύνσεις παραληπτών από απεσταλμένα μηνύματα στη λίστα διευθύνσεων χρήστη ως επιτρεπτές.

Προσθήκη διευθύνσεων από αναταξινομημένα μηνύματα ως ΜΗ ανεπιθύμητα – Προσθέστε διευθύνσεις αποστολέων από μηνύματα που έχουν αναταξινομηθεί ως ΜΗ ανεπιθύμητα στη λίστα διευθύνσεων χρήστη ως επιτρεπτές.

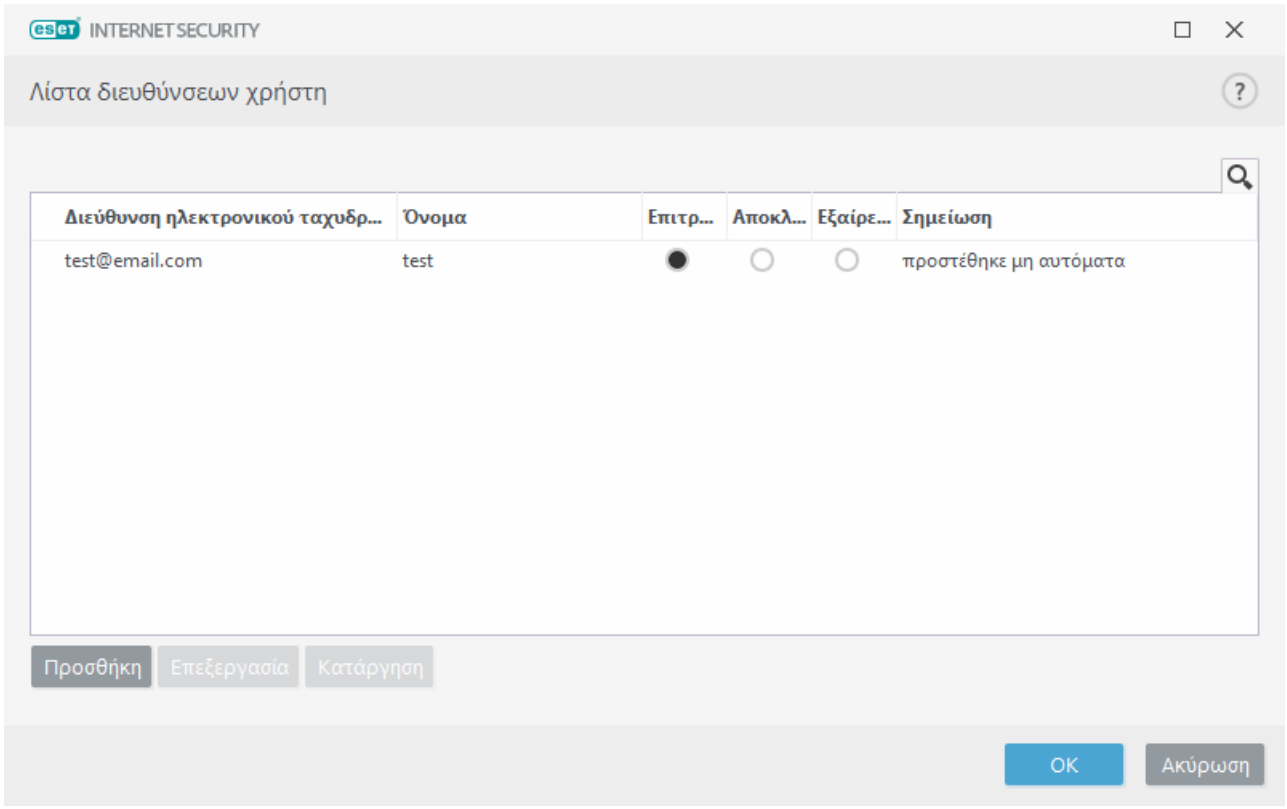
Αυτόματη προσθήκη στη λίστα διευθύνσεων χρήστη ως εξαίρεση

Προσθήκη διευθύνσεων από προσωπικούς λογαριασμούς – Προσθέστε τις διευθύνσεις σας από υπάρχοντες λογαριασμούς προγραμμάτων ηλεκτρονικής αλληλογραφίας στη λίστα διευθύνσεων χρήστη ως εξαίρεση.

Διευθύνσεις διευθύνσεων

Για να προστατευθείτε από ανεπιθύμητα email, το ESET Internet Security σάς επιτρέπει να ταξινομήσετε τις διευθύνσεις email στις λίστες διευθύνσεων.

Για να επεξεργαστείτε λίστες διευθύνσεων, ανοίξτε τα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία ηλεκτρονικής αλληλογραφίας** > **Λίστες διευθύνσεων Antispam** και κάντε κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Λίστα διευθύνσεων χρήστη** ή **Γενική λίστα διευθύνσεων**.



Στήλες

Διεύθυνση email – Διεύθυνση στην οποία θα εφαρμοστεί ο κανόνας.

Όνομα – Όνομα προσαρμοσμένου κανόνα.

Να επιτρέπεται/Αποκλεισμός/Εξαίρεση – Κουμπιά επιλογής που χρησιμοποιούνται για τον προσδιορισμό της ενέργειας που πρέπει να εκτελεστεί για τη διεύθυνση email (κάντε κλικ στο κουμπί επιλογής στην στήλη που προτιμάτε για να αλλάξετε γρήγορα την ενέργεια):

- **Να επιτρέπεται** – Διευθύνσεις που θεωρούνται ασφαλείς και από τις οποίες θέλετε να λαμβάνετε μηνύματα.
- **Αποκλεισμός** – Διευθύνσεις που θεωρούνται μη ασφαλείς/ανεπιθύμητες και από τις οποίες δεν θέλετε να λαμβάνετε μηνύματα.
- **Εξαίρεση** – Διευθύνσεις που ελέγχονται πάντα για ανεπιθύμητα μηνύματα, και οι οποίες μπορεί να είναι πλαστές και να χρησιμοποιούνται για την αποστολή ανεπιθύμητων μηνυμάτων.

Σημείωση – Πληροφορίες σχετικά με τον τρόπο που δημιουργήθηκε ο κανόνας και εάν ισχύει για ολόκληρο τον τομέα / τομείς χαμηλότερου επιπέδου.

Διαχείριση των διευθύνσεων

- **Προσθήκη** – Κάντε κλικ για να προσθέσετε έναν κανόνα για μια νέα διεύθυνση.
- **Επεξεργασία** – Επιλέξτε και κάντε κλικ για να επεξεργαστείτε έναν υπάρχοντα κανόνα.
- **Κατάργηση** – Επιλέξτε και κάντε κλικ εάν θέλετε να καταργήσετε έναν κανόνα από τη λίστα διευθύνσεων.

Προσθήκη/Επεξεργασία διεύθυνσης

Αυτό το παράθυρο σάς επιτρέπει να προσθέσετε ή να επεξεργαστείτε μια διεύθυνση που βρίσκεται στη λίστα διευθύνσεων Antispam και να ρυθμίσετε τις παραμέτρους της ενέργειας που εκτελείται:

Διεύθυνση email – Διεύθυνση στην οποία θα εφαρμοστεί ο κανόνας.

Όνομα – Όνομα προσαρμοσμένου κανόνα.

Ενέργεια – Ενέργεια που πρέπει να εκτελεστεί εάν η διεύθυνση email της επαφής ταιριάζει με τη διεύθυνση που καθορίζεται στο πεδίο **Διεύθυνση email**:

- **Να επιτρέπεται** – Διευθύνσεις που θεωρούνται ασφαλείς και από τις οποίες θέλετε να λαμβάνετε μηνύματα.

- **Αποκλεισμός** – Διευθύνσεις που θεωρούνται μη ασφαλείς/ανεπιθύμητες και από τις οποίες δεν θέλετε να λαμβάνετε μηνύματα.

- **Εξαίρεση** – Διευθύνσεις που ελέγχονται πάντα για ανεπιθύμητα μηνύματα, και οι οποίες μπορεί να είναι πλαστές και να χρησιμοποιούνται για την αποστολή ανεπιθύμητων μηνυμάτων.

Ολόκληρος ο τομέας – Κάντε αυτή την επιλογή για να εφαρμοστεί ο κανόνας σε ολόκληρο τον τομέα της επαφής (όχι μόνο στη διεύθυνση που καθορίζεται στο πεδίο **Διεύθυνση email**, αλλά σε όλες τις διευθύνσεις email στον τομέα *address.info*).

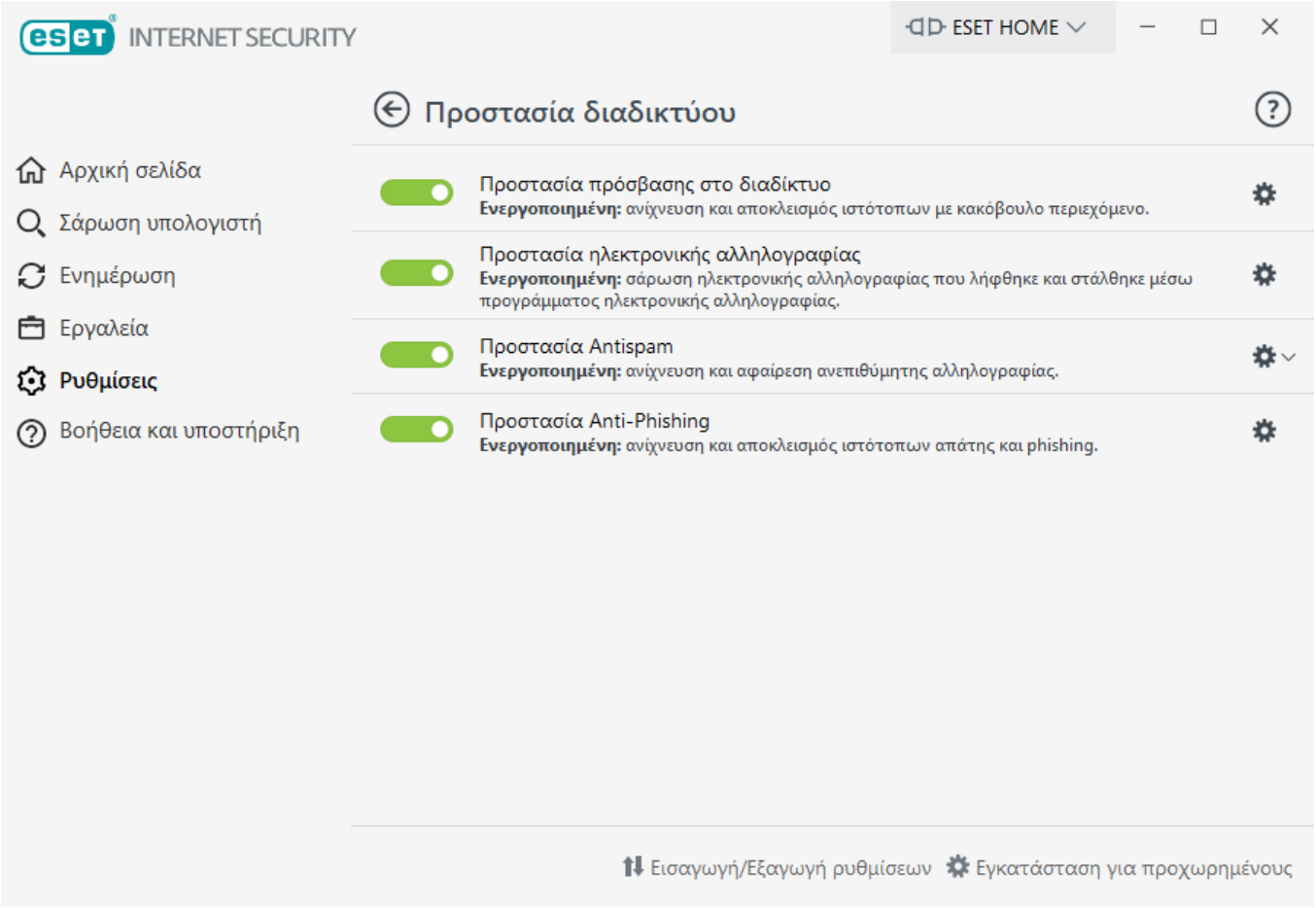
Τομείς χαμηλότερου επιπέδου – Κάντε αυτή την επιλογή για να εφαρμοστεί ο κανόνας στους τομείς χαμηλότερου επιπέδου της επαφής (Το *address.info* αντιπροσωπεύει τον τομέα, ενώ το *my.address.info* αντιπροσωπεύει έναν υποτομέα).

Προστασία πρόσβασης στο διαδίκτυο

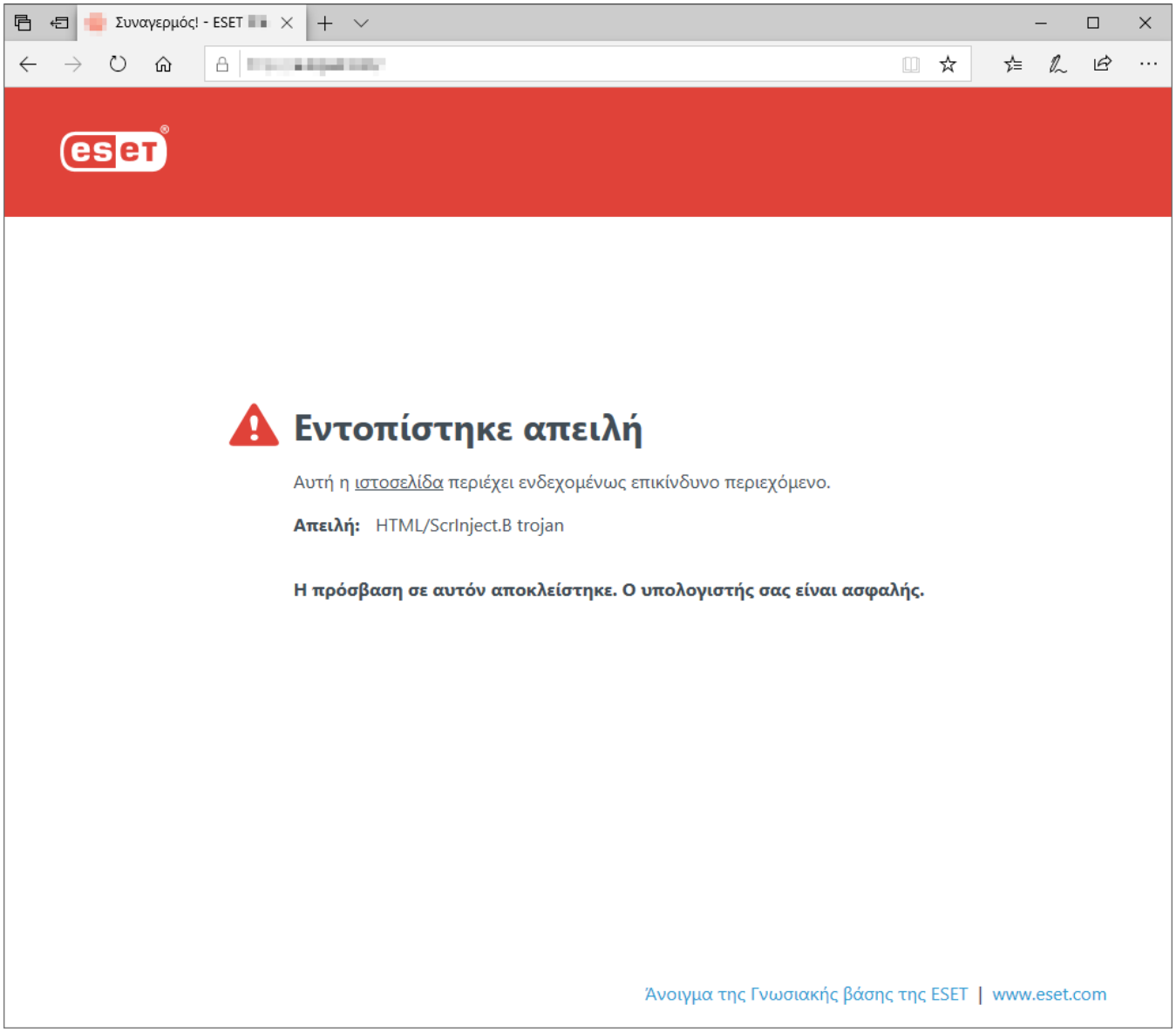
Η συνδεσιμότητα με το διαδίκτυο είναι μια τυπική δυνατότητα ενός προσωπικού υπολογιστή. Δυστυχώς, έχει γίνει επίσης το κύριο μέσο για τη μεταφορά κακόβουλου κώδικα. Η προστασία πρόσβασης στο διαδίκτυο λειτουργεί παρακολουθώντας την επικοινωνία ανάμεσα σε προγράμματα περιήγησης στο διαδίκτυο και απομακρυσμένους διακομιστές και συμμορφώνεται με τους κανόνες HTTP (Πρωτόκολλο Μεταφοράς Υπερκειμένου) και HTTPS (κρυπτογραφημένη επικοινωνία).

Η πρόσβαση σε ιστοσελίδες που είναι γνωστό ότι περιέχουν κακόβουλο περιεχόμενο αποκλείεται προτού γίνει λήψη περιεχομένου. Όλες οι άλλες ιστοσελίδες σαρώνονται με το μηχανισμό σάρωσης ThreatSense κατά τη φόρτωσή τους και αποκλείονται, εάν εντοπιστεί κακόβουλο περιεχόμενο. Η Προστασία πρόσβασης στο διαδίκτυο παρέχει δύο επίπεδα προστασίας: αποκλεισμό κατά λίστα αποκλεισμού και αποκλεισμό κατά περιεχόμενο.

Συνιστάται να ενεργοποιήσετε την Προστασία πρόσβασης στο διαδίκτυο. Η πρόσβαση σε αυτή την επιλογή επιτυγχάνεται από το κύριο παράθυρο του προγράμματος > **Ρυθμίσεις** > **Προστασία διαδικτύου** > **Προστασία πρόσβασης στο διαδίκτυο**.



Η Προστασία πρόσβασης στο διαδίκτυο θα εμφανίσει το ακόλουθο μήνυμα στο πρόγραμμα περιήγησης όταν ένας ιστότοπος έχει αποκλειστεί:



Εικονογραφημένες οδηγίες

Τα ακόλουθα άρθρα της Γνωσιακής βάσης της ESET μπορεί να είναι διαθέσιμα μόνο στα Αγγλικά:

- Εξαίρεση ενός ασφαλούς ιστότοπου από τον αποκλεισμό με την Προστασία πρόσβασης στο διαδίκτυο
- Αποκλεισμός ενός ιστότοπου χρησιμοποιώντας το ESET Internet Security

---

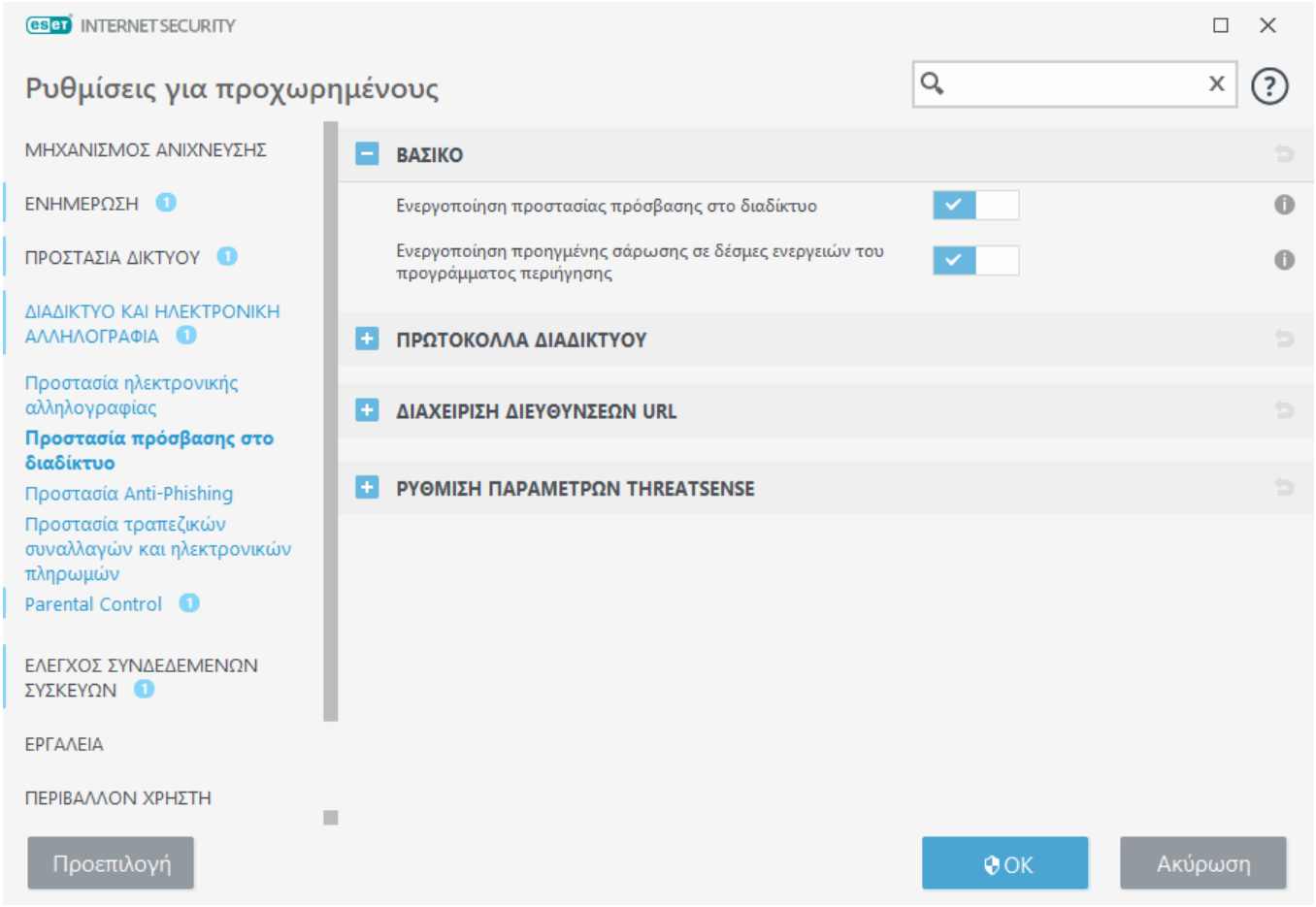
Οι παρακάτω επιλογές είναι διαθέσιμες στην ενότητα **Ρυθμίσεις για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία πρόσβασης στο διαδίκτυο**:

Βασικές ρυθμίσεις – Για να ενεργοποιήσετε ή να απενεργοποιήσετε αυτή τη λειτουργία από την Εγκατάσταση για προχωρημένους.

Πρωτόκολλα διαδικτύου – Σας επιτρέπει να ρυθμίσετε τις παραμέτρους για την παρακολούθηση αυτών των τυπικών πρωτοκόλλων, τα οποία χρησιμοποιούνται από τα περισσότερα προγράμματα περιήγησης στο διαδίκτυο.

Διαχείριση διευθύνσεων URL – Σας επιτρέπει να καθορίσετε τις διευθύνσεις URL που θα αποκλείονται, θα επιτρέπονται ή θα εξαιρούνται από τον έλεγχο.

Παράμετροι ThreatSense – Προηγμένες ρυθμίσεις σάρωσης για ιούς – σας επιτρέπει να διαμορφώνετε ρυθμίσεις όπως τύπους αντικειμένων που θα σαρωθούν (ηλεκτρονική αλληλογραφία, αρχειοθήκες κ.λπ.), μεθόδους ανίχνευσης για προστασία πρόσβασης στο διαδίκτυο κ.λπ.



Εγκατάσταση για προχωρημένους για την προστασία πρόσβασης στο διαδίκτυο

Οι παρακάτω επιλογές είναι διαθέσιμες στη διαδρομή **Εγκατάσταση για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία πρόσβασης στο διαδίκτυο** > **Βασικές ρυθμίσεις**:

Ενεργοποίηση προστασίας πρόσβασης στο διαδίκτυο – Όταν απενεργοποιείται, η Προστασία πρόσβασης στο διαδίκτυο και η Προστασία Anti-Phishing δεν θα λειτουργούν. Αυτή η επιλογή είναι διαθέσιμη μόνο όταν έχει ενεργοποιηθεί το φιλτράρισμα πρωτοκόλλων SSL/TLS.

Ενεργοποίηση προηγμένης σάρωσης σε δέσμες ενεργειών του προγράμματος περιήγησης – Όταν ενεργοποιείται, όλα τα προγράμματα JavaScript που εκτελούνται από τα προγράμματα περιήγησης στο διαδίκτυο θα ελέγχονται από το μηχανισμό ανίχνευσης.

Συνιστάται να διατηρείτε ενεργοποιημένη την προστασία πρόσβασης στο διαδίκτυο.

Πρωτόκολλα διαδικτύου

Από προεπιλογή, το ESET Internet Security είναι διαμορφωμένο ώστε να παρακολουθεί το πρωτόκολλο HTTP που χρησιμοποιείται από τα περισσότερα προγράμματα περιήγησης.

Ρυθμίσεις σάρωσης HTTP

Η κυκλοφορία HTTP παρακολουθείται πάντα σε όλες τις θύρες για όλες τις εφαρμογές.

Ρυθμίσεις σάρωσης HTTPS

Το ESET Internet Security υποστηρίζει επίσης τον έλεγχο πρωτοκόλλου HTTPS. Η επικοινωνία HTTPS χρησιμοποιεί έναν κρυπτογραφημένο δίαυλο για τη μεταφορά πληροφοριών μεταξύ διακομιστή και προγράμματος-πελάτη. Το ESET Internet Security ελέγχει την επικοινωνία που χρησιμοποιεί πρωτόκολλα SSL (Secure Socket Layer) και TLS (Transport Layer Security). Το πρόγραμμα θα σαρώνει μόνο την κυκλοφορία στις θύρες (443, 0-65535) που καθορίζονται στη ρύθμιση **Θύρες που χρησιμοποιούνται από το πρωτόκολλο HTTPS**, ανεξάρτητα από την έκδοση του λειτουργικού συστήματος.

Η κρυπτογραφημένη επικοινωνία θα σαρώνεται από προεπιλογή. Για να δείτε τις ρυθμίσεις σάρωσης, ανοίξτε τα στοιχεία «Ρυθμίσεις για προχωρημένους» > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **SSL/TLS**.

Διαχείριση διευθύνσεων URL

Η ενότητα διαχείρισης διευθύνσεων URL σάς επιτρέπει να καθορίσετε τις διευθύνσεις HTTP που θα αποκλείονται, θα επιτρέπονται ή θα εξαιρούνται από τη σάρωση περιεχομένου.

Πρέπει να ενεργοποιήσετε την επιλογή Ενεργοποίηση φιλτραρίσματος πρωτοκόλλου SSL/TLS εάν θέλετε να φιλτράρονται και διευθύνσεις HTTPS πέρα από ιστοσελίδες HTTP. Διαφορετικά, θα προστεθούν μόνο οι τομείς ιστότοπων HTTPS που έχετε επισκεφτεί, όχι η πλήρης διεύθυνση URL.

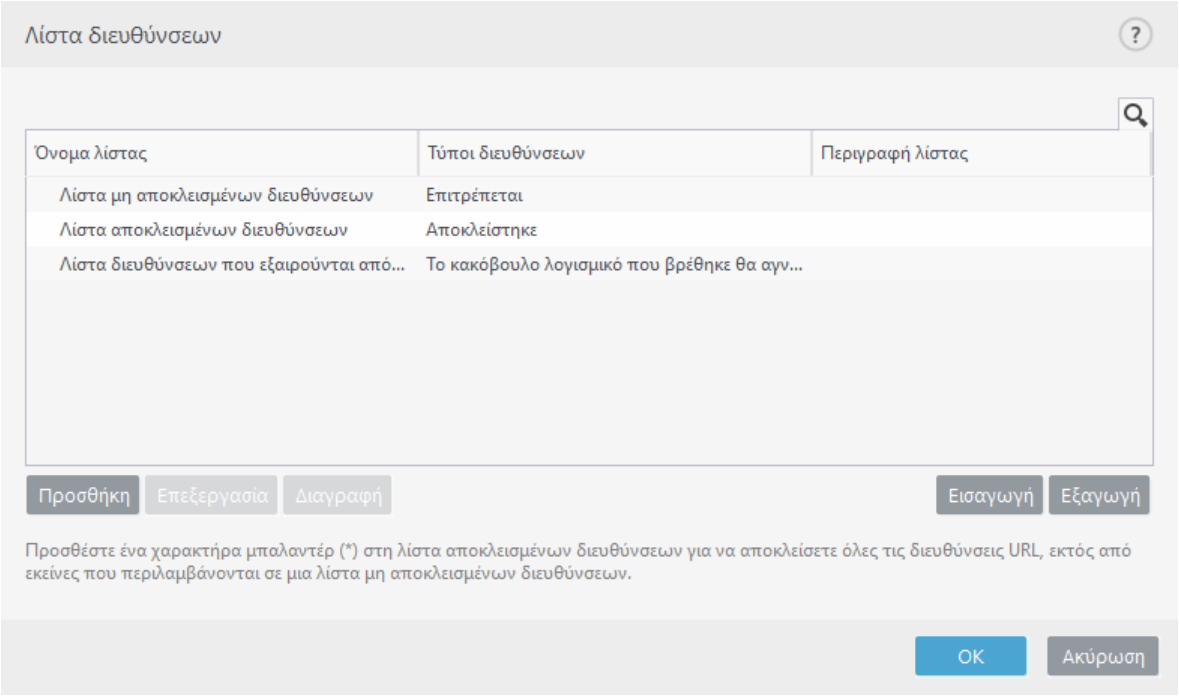
Οι ιστότοποι στη **Λίστα αποκλεισμένων διευθύνσεων** δεν θα είναι προσπελάσιμοι, εκτός εάν περιλαμβάνονται και στη **Λίστα επιτρεπτών διευθύνσεων**. Οι ιστότοποι που βρίσκονται στη **Λίστα διευθύνσεων που εξαιρούνται από τη σάρωση περιεχομένου** δεν σαρώνονται για κακόβουλο κώδικα κατά την πρόσβαση σε αυτούς.

Εάν θέλετε να αποκλείονται όλες οι διευθύνσεις HTTP εκτός από τις διευθύνσεις που εμφανίζονται στην ενεργή **Λίστα αποδεκτών διευθύνσεων**, προσθέστε αστερίσκο (*) στην ενεργή **Λίστα αποκλεισμένων διευθύνσεων**.

Δεν μπορείτε να χρησιμοποιήσετε τα ειδικά σύμβολα * (αστερίσκος) και ? (ερωτηματικό) στις λίστες. Ο αστερίσκος αντικαθιστά οποιαδήποτε συμβολοσειρά χαρακτήρων και το ερωτηματικό αντικαθιστά οποιοδήποτε σύμβολο. Χρειάζεται ιδιαίτερη προσοχή όταν καθορίζετε διευθύνσεις που θα εξαιρεθούν, επειδή η λίστα θα πρέπει να περιέχει μόνο αξιόπιστες και ασφαλείς διευθύνσεις. Παρομοίως, είναι απαραίτητο να διασφαλίζετε ότι χρησιμοποιούνται σωστά τα σύμβολα * και ? σε αυτή τη λίστα. Ανατρέξτε στο κεφάλαιο Προσθήκη διεύθυνσης HTTP/μάσκας τομέα για τον τρόπο με τον οποίο μπορείτε να αντιστοιχίσετε με ασφάλεια έναν ολόκληρο τομέα συμπεριλαμβάνοντας όλους τους δευτερεύοντες τομείς. Για να ενεργοποιήσετε τη λίστα, επιλέξτε **Εμφάνιση ενεργών**. Εάν

θέλετε να ειδοποιείστε κατά την είσοδό σας σε μια διεύθυνση από την τρέχουσα λίστα, επιλέξτε **Ειδοποίηση κατά την εφαρμογή**.

> **Αξιόπιστοι τομείς**
> Οι διευθύνσεις δεν θα φιλτράρονται εάν η ρύθμιση στη διαδρομή **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **SSL/TLS** > **Εξαίρεση επικοινωνίας με αξιόπιστους τομείς** είναι ενεργή και ο τομέας θεωρείται αξιόπιστος.



Στοιχεία ελέγχου

Προσθήκη – Δημιουργεί μια νέα λίστα πέρα από τις προκαθορισμένες. Αυτό μπορεί να είναι χρήσιμο εάν θέλετε να ξεχωρίσετε διαφορετικές ομάδες διευθύνσεων. Για παράδειγμα, μία λίστα αποκλεισμένων διευθύνσεων μπορεί να περιέχει διευθύνσεις από μια εξωτερική δημόσια λίστα αποκλεισμού, ενώ μια άλλη μπορεί να περιέχει τη δική σας λίστα αποκλεισμού, ώστε να είναι ευκολότερο να ενημερώσετε την εξωτερική λίστα, κρατώντας ταυτόχρονα τη δική σας λίστα ανέπαφη.

Επεξεργασία – Τροποποιεί υπάρχουσες λίστες. Χρησιμοποιήστε αυτή την επιλογή για να προσθέσετε ή να αφαιρέσετε διευθύνσεις.

Διαγραφή – Διαγράφει υπάρχουσες λίστες. Η επιλογή είναι διαθέσιμη μόνο για λίστες που έχουν δημιουργηθεί με την επιλογή **Προσθήκη**, όχι για τις προεπιλεγμένες λίστες.

Λίστα διευθύνσεων URL

Σε αυτή την ενότητα μπορείτε να καθορίσετε λίστες διευθύνσεων HTTP που θα αποκλείονται, θα επιτρέπονται ή θα εξαιρούνται από τον έλεγχο.

Από προεπιλογή, διατίθενται οι τρεις παρακάτω λίστες:

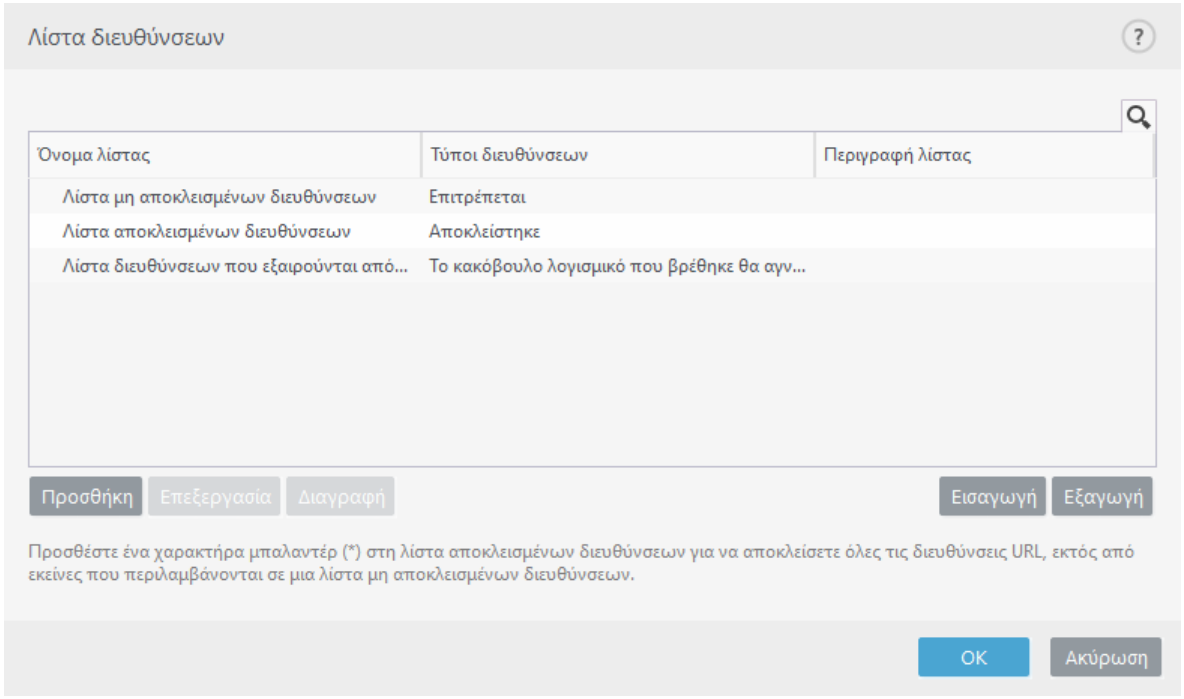
- **Λίστα διευθύνσεων που εξαιρούνται από τη σάρωση περιεχομένου** – Δεν θα εκτελείται κανένας έλεγχος για κακόβουλο κώδικα για οποιαδήποτε διεύθυνση προστίθεται σε αυτή τη

λίστα.

• **Λίστα επιτρεπτών διευθύνσεων** – Αν είναι ενεργοποιημένη η επιλογή «Να επιτρέπεται η πρόσβαση μόνο σε διευθύνσεις HTTP στη λίστα αποδεκτών διευθύνσεων» και η λίστα αποκλεισμένων διευθύνσεων περιέχει * (που σημαίνει ότι αντιστοιχούν όλες οι διευθύνσεις), θα επιτρέπεται στο χρήστη η πρόσβαση μόνο στις διευθύνσεις που καθορίζονται σε αυτήν τη λίστα. Οι διευθύνσεις σε αυτήν τη λίστα επιτρέπονται ακόμη κι αν περιλαμβάνονται στη λίστα αποκλεισμένων διευθύνσεων.

• **Λίστα αποκλεισμένων διευθύνσεων** – Ο χρήστης δεν θα επιτρέπεται να έχει πρόσβαση στις διευθύνσεις που καθορίζονται σε αυτήν τη λίστα, εκτός εάν εμφανίζονται επίσης στη λίστα μη αποκλεισμένων διευθύνσεων.

Κάντε κλικ στο στοιχείο **Προσθήκη** για να δημιουργήσετε μια νέα λίστα. Για να διαγράψετε επιλεγμένες λίστες, κάντε κλικ στο στοιχείο **Διαγραφή**.



> **Εικονογραφημένες οδηγίες**
> Τα ακόλουθα άρθρα της Γνωσιακής βάσης της ESET μπορεί να είναι διαθέσιμα μόνο στα Αγγλικά:
> • Εξαίρεση ενός ασφαλούς ιστότοπου από τον αποκλεισμό με την Προστασία πρόσβασης στο διαδίκτυο
> • Αποτρέψτε έναν ιστότοπο χρησιμοποιώντας οικιακά προϊόντα της ESET για Windows

Για περισσότερες πληροφορίες δείτε την ενότητα Διαχείριση διευθύνσεων URL.

Δημιουργία νέας λίστας διευθύνσεων URL

Αυτή η ενότητα σάς επιτρέπει να καθορίσετε λίστες διευθύνσεων/μασκών URL που θα αποκλείονται, θα επιτρέπονται ή θα εξαιρούνται από τον έλεγχο.

Κατά τη δημιουργία νέας λίστας, οι παρακάτω επιλογές είναι διαθέσιμες για διαμόρφωση:

Τύπος λίστας διευθύνσεων – Διατίθενται τρεις τύποι λιστών:

• **Εξαιρούνται από τον έλεγχο** – Δεν θα εκτελείται κανένας έλεγχος για κακόβουλο κώδικα για οποιαδήποτε διεύθυνση προστίθεται σε αυτή τη λίστα.

• **Αποκλεισμένες** - Ο χρήστης δεν θα επιτρέπεται να έχει πρόσβαση στις διευθύνσεις που καθορίζονται σε αυτήν τη λίστα.

• **Επιτρεπτές** – Αν είναι ενεργοποιημένη η επιλογή «Να επιτρέπεται η πρόσβαση μόνο σε διευθύνσεις HTTP στη λίστα μη αποκλεισμένων διευθύνσεων» και η λίστα αποκλεισμένων διευθύνσεων περιέχει * (που σημαίνει ότι αντιστοιχούν όλες οι διευθύνσεις), θα επιτρέπεται στο χρήστη η πρόσβαση μόνο στις διευθύνσεις που καθορίζονται σε αυτήν τη λίστα. Οι διευθύνσεις σε αυτήν τη λίστα επιτρέπονται ακόμη κι αν περιλαμβάνονται στη λίστα αποκλεισμένων διευθύνσεων.

Όνομα λίστας – Καθορίστε το όνομα της λίστας. Αυτό το πεδίο θα είναι απενεργοποιημένο όταν επεξεργάζεστε μία από τις τρεις προκαθορισμένες λίστες.

Περιγραφή λίστας – Πληκτρολογήστε μια σύντομη περιγραφή για τη λίστα (προαιρετικά). Θα είναι απενεργοποιημένο όταν επεξεργάζεστε μία από τις τρεις προκαθορισμένες λίστες.

Για να ενεργοποιήσετε μια λίστα, επιλέξτε **Ενεργή λίστα** δίπλα στην αντίστοιχη λίστα. Εάν θέλετε να ειδοποιείστε όταν χρησιμοποιείται μια συγκεκριμένη λίστα για την αξιολόγηση ενός ιστότοπου HTTP που επισκέπτεστε, επιλέξτε **Ειδοποίηση όταν εφαρμόζεται**. Για παράδειγμα, θα αποστέλλεται ειδοποίηση εάν ένας ιστότοπος αποκλείεται ή επιτρέπεται επειδή συμπεριλαμβάνεται στη λίστα αποκλεισμένων ή μη αποκλεισμένων διευθύνσεων. Η ειδοποίηση θα περιέχει το όνομα της λίστας η οποία περιλαμβάνει τον συγκεκριμένο ιστότοπο.

Στοιχεία ελέγχου

Προσθήκη – Προσθέστε μια νέα διεύθυνση URL στη λίστα (εισαγάγετε πολλαπλές τιμές με διαχωριστικό).

Επεξεργασία – Τροποποιεί μια υπάρχουσα διεύθυνση στη λίστα. Η επιλογή είναι δυνατή μόνο για διευθύνσεις που έχουν δημιουργηθεί με την επιλογή **Προσθήκη**.

Κατάργηση – Διαγράφει υπάρχουσες διευθύνσεις από τη λίστα. Η επιλογή είναι δυνατή μόνο για διευθύνσεις που έχουν δημιουργηθεί με την επιλογή **Προσθήκη**.

Εισαγωγή – Εισαγάγετε ένα αρχείο με διευθύνσεις URL (διαχωρίστε τις τιμές με αλλαγή γραμμής, για παράδειγμα *.txt χρησιμοποιώντας κωδικοποίηση UTF-8).

Πώς να προσθέσετε μια μάσκα URL

Ανατρέξτε στις οδηγίες για αυτό το παράθυρο διαλόγου προτού εισαγάγετε τη διεύθυνση/μάσκα τομέα που θέλετε.

Το ESET Internet Security επιτρέπει στον χρήστη να αποκλείσει την πρόσβαση σε συγκεκριμένους ιστότοπους και να εμποδίσει το πρόγραμμα περιήγησης στο διαδίκτυο να εμφανίσει το περιεχόμενό τους. Επιπλέον, επιτρέπει στον χρήστη να καθορίσει διευθύνσεις, οι οποίες θα πρέπει να αποκλειστούν από τον έλεγχο. Αν δεν είναι γνωστό το πλήρες όνομα του απομακρυσμένου διακομιστή ή ο χρήστης θέλει να καθορίσει μια ολόκληρη ομάδα απομακρυσμένων διακομιστών, μπορούν να

χρησιμοποιηθούν οι επονομαζόμενες μάσκες για την αναγνώριση μιας τέτοιας ομάδας. Οι μάσκες περιλαμβάνουν τα σύμβολα «?» και «*»:

- χρησιμοποιήστε το ? για αντικατάσταση ενός συμβόλου
- χρησιμοποιήστε το * για αντικατάσταση μιας συμβολοσειράς κειμένου.

Για παράδειγμα το *.c?m εφαρμόζεται σε όλες τις διευθύνσεις στις οποίες το τελευταίο μέρος αρχίζει με το γράμμα c, τελειώνει με το γράμμα m και περιέχει ένα άγνωστο σύμβολο μεταξύ τους (.com, .cam, κ.λπ.)

Η αρχική ακολουθία «*.» αντιμετωπίζεται με ιδιαίτερο τρόπο, εάν χρησιμοποιείται στην αρχή του ονόματος τομέα. Πρώτον, ο χαρακτήρας wildcard * δεν αντιστοιχεί στον χαρακτήρα καθέτου («/») σε αυτή την περίπτωση. Με αυτό τον τρόπο αποφεύγεται η παράκαμψη της μάσκας, για παράδειγμα η μάσκα **.domain.com* δεν θα αντιστοιχεί στο *http://anydomain.com/anypath#.domain.com* (η προσθήκη αυτού του επιθήματος είναι δυνατή σε οποιαδήποτε διεύθυνση URL χωρίς να επηρεάζεται η λήψη). Και δεύτερον, σε αυτή την ειδική περίπτωση, το «*.» αντιστοιχεί επίσης με μια κενή συμβολοσειρά. Αυτό επιτρέπει την αντιστοίχιση ολόκληρου του τομέα, συμπεριλαμβανομένων τυχόν υποτομέων με χρήση μιας μοναδικής μάσκας. Για παράδειγμα, η μάσκα **.domain.com* αντιστοιχεί επίσης στο *http://domain.com*. Η χρήση του **domain.com* θα ήταν εσφαλμένη, καθώς θα αντιστοιχούσε επίσης στο *http://anotherdomain.com*.

Προστασία Anti-Phishing

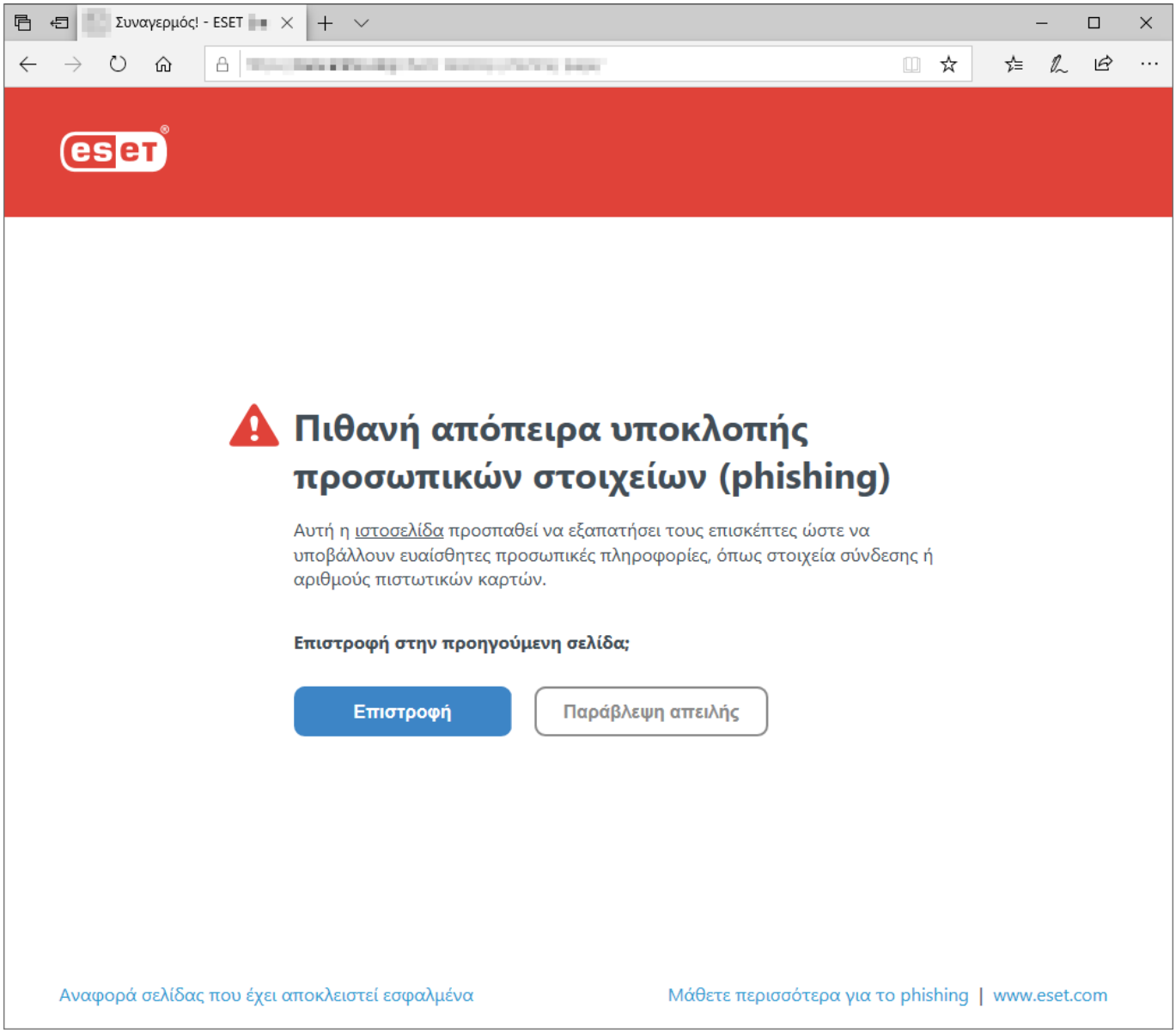
Ο όρος phishing καθορίζει μια εγκληματική δραστηριότητα που χρησιμοποιεί την κοινωνική μηχανική (τον χειρισμό χρηστών προκειμένου να εξασφαλιστούν εμπιστευτικές πληροφορίες). Το Phishing συχνά χρησιμοποιείται για πρόσβαση σε ευαίσθητα δεδομένα όπως αριθμοί τραπεζικών λογαριασμών, αριθμοί PIN και άλλα. Διαβάστε περισσότερα σχετικά με αυτήν τη δραστηριότητα στο γλωσσάρι. Το ESET Internet Security περιλαμβάνει προστασία anti-phishing, η οποία αποκλείει ιστοσελίδες που είναι γνωστό ότι διανέμουν περιεχόμενο αυτού του τύπου.

Συνιστάται να ενεργοποιήσετε τη δυνατότητα Anti-Phishing στο ESET Internet Security. Για να το κάνετε αυτό, ανοίξτε τις **Ρυθμίσεις για προχωρημένους** (F5) και μεταβείτε στο στοιχείο **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία Anti-Phishing**.

Επισκεφτείτε το άρθρο στη Γνωσιακή βάση μας για περισσότερες πληροφορίες σχετικά με την Προστασία Anti-Phishing στο ESET Internet Security.

Πρόσβαση σε έναν ιστότοπο phishing

Όταν αποκτάτε πρόσβαση σε έναν αναγνωρισμένο ιστότοπο phishing, θα εμφανιστεί το ακόλουθο παράθυρο διαλόγου στο πρόγραμμα περιήγησης. Εάν θέλετε οπωσδήποτε να αποκτήσετε πρόσβαση στον ιστότοπο, κάντε κλικ στην επιλογή **Παράβλεψη απειλής** (δεν συνιστάται).



Οι πιθανοί ιστότοποι phishing που έχουν τοποθετηθεί στη λίστα μη αποκλεισμένων διευθύνσεων λήγουν μετά από μερικές ώρες από προεπιλογή. Για να επιτρέπεται μόνιμα η πρόσβαση σε έναν ιστότοπο, χρησιμοποιήστε το εργαλείο Διαχείριση διευθύνσεων URL. Στη διαδρομή **Εγκατάσταση για προχωρημένους** (F5), **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία πρόσβασης στο διαδίκτυο** > **Διαχείριση διευθύνσεων URL** > **Λίστα διευθύνσεων** > **Επεξεργασία** προσθέστε στη λίστα τον ιστότοπο που θέλετε να επεξεργαστείτε.

Αναφορά ιστότοπου Phishing

Ο σύνδεσμος **Αναφορά** σάς επιτρέπει να αναφέρετε έναν ιστότοπο phishing/κακόβουλο ιστότοπο στην ESET για ανάλυση.

Προτού υποβάλλετε έναν ιστότοπο στην ESET, βεβαιωθείτε ότι πληροί ένα ή περισσότερα από τα παρακάτω κριτήρια:
• Ο ιστότοπος δεν ανιχνεύεται καθόλου.
• Ο ιστότοπος ανιχνεύεται εσφαλμένα ως απειλή. Σε αυτή την περίπτωση, μπορείτε να υποβάλετε Αναφορά σελίδας που έχει αποκλειστεί εσφαλμένα.

Εναλλακτικά, μπορείτε να υποβάλετε τον ιστότοπο με ηλεκτρονική αλληλογραφία. Στείλτε το μήνυμα

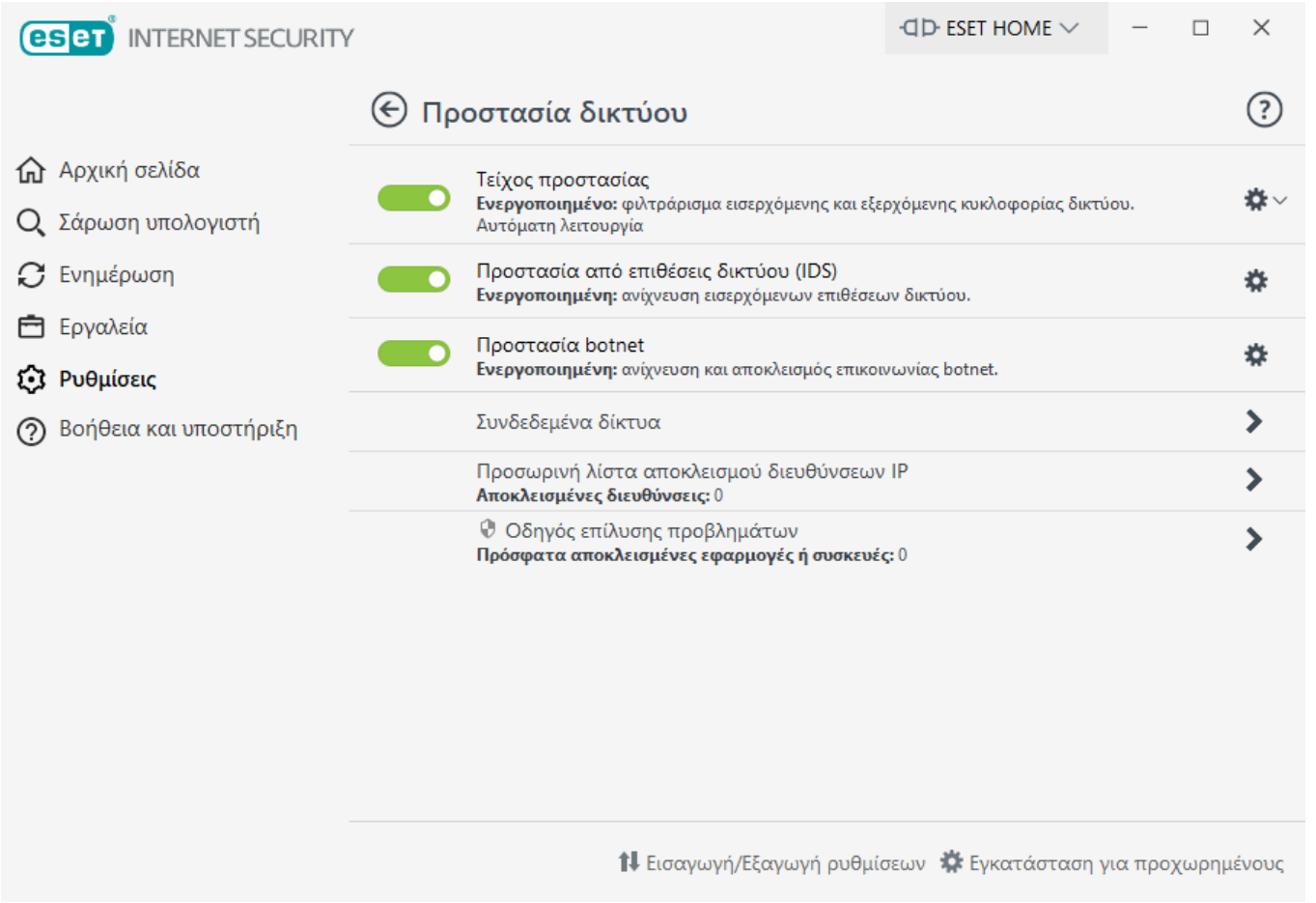
ηλεκτρονικής αλληλογραφίας στη διεύθυνση samples@eset.com. Φροντίστε να χρησιμοποιείτε ένα περιγραφικό θέμα και να περιλαμβάνετε όσο το δυνατόν περισσότερες πληροφορίες για τον ιστότοπο (π.χ. τη σελίδα από την οποία μεταφερθήκατε στον ιστότοπο, από πού μάθατε για τον ιστότοπο κ.λπ.).

Προστασία δικτύου

Η ρύθμιση παραμέτρων προστασίας δικτύου βρίσκεται στο παράθυρο **Ρυθμίσεις** στην ενότητα **Προστασία δικτύου**.

Για να διακόψετε προσωρινά ή να απενεργοποιήσετε μεμονωμένες λειτουργικές μονάδες προστασίας, κάντε κλικ στο εικονίδιο ρυθμιστικού .

Η απενεργοποίηση των λειτουργικών μονάδων προστασίας ενδέχεται να μειώσει το επίπεδο προστασίας του υπολογιστή σας.



Τείχος προστασίας – Εδώ μπορείτε να προσαρμόσετε τη λειτουργία φιλτραρίσματος για το Τείχος προστασίας της ESET. Για να αποκτήσετε πρόσβαση σε πιο λεπτομερείς ρυθμίσεις, κάντε κλικ στο γρανάζι > **Ρύθμιση παραμέτρων** και κατόπιν στο στοιχείο **Τείχος προστασίας**, ή πατήστε το πλήκτρο **F5** για να αποκτήσετε πρόσβαση στο στοιχείο Εγκατάσταση για προχωρημένους.

Ρύθμιση παραμέτρων – Ανοίγει το παράθυρο «Firewall» στις Ρυθμίσεις για προχωρημένους, όπου μπορείτε να καθορίσετε τον τρόπο με τον οποίο το firewall θα χειρίζεται την επικοινωνία δικτύου.

Παύση του τείχους προστασίας (να επιτρέπεται όλη η κίνηση) – Το αντίθετο του αποκλεισμού όλης της δικτυακής κίνησης. Εάν το επιλέξετε, απενεργοποιούνται όλες οι επιλογές

φιλτραρίσματος του Firewall και επιτρέπονται όλες οι εισερχόμενες και εξερχόμενες συνδέσεις. Κάντε κλικ στην επιλογή **Ενεργοποίηση firewall** για να ενεργοποιήσετε εκ νέου το firewall όταν το Φιλτράρισμα κυκλοφορίας δικτύου βρίσκεται σε αυτήν τη λειτουργία.

Αποκλεισμός όλης της κυκλοφορίας – Όλες οι εισερχόμενες και εξερχόμενες επικοινωνίες θα αποκλείονται από το Firewall. Χρησιμοποιείτε αυτή την επιλογή μόνο εάν υποπτεύεστε κρίσιμο κίνδυνο ασφαλείας που απαιτεί την αποσύνδεση του συστήματος από το δίκτυο. Ενώ το Φιλτράρισμα κυκλοφορίας δικτύου είναι στη λειτουργία **Αποκλεισμός όλης της κυκλοφορίας**, κάντε κλικ στην επιλογή **Διακοπή αποκλεισμού όλης της κυκλοφορίας** για να επαναφέρετε την κανονική λειτουργία του firewall.

Αυτόματη λειτουργία – (όταν είναι ενεργοποιημένη μια άλλη λειτουργία φιλτραρίσματος) – Κάντε κλικ για να αλλάξετε τη λειτουργία φιλτραρίσματος σε αυτόματη (με κανόνες καθορισμένους από το χρήστη).

Αλληλεπιδραστική λειτουργία – (όταν είναι ενεργοποιημένη μια άλλη λειτουργία φιλτραρίσματος) - Κάντε κλικ για να αλλάξετε τη λειτουργία φιλτραρίσματος σε αλληλεπιδραστική.

Προστασία από επιθέσεις δικτύου (IDS) – Αναλύει το περιεχόμενο της δικτυακής κίνησης και προστατεύει από επιθέσεις δικτύου. Οποιαδήποτε κίνηση θεωρείται επιβλαβής θα αποκλείεται. Το ESET Internet Security θα σας ειδοποιεί όταν συνδέεστε σε ένα μη προστατευμένο ασύρματο δίκτυο ή σε ένα δίκτυο με αδύναμη προστασία.

Προστασία Botnet – Εντοπίζει γρήγορα και με ακρίβεια κακόβουλο λογισμικό στο σύστημά σας.

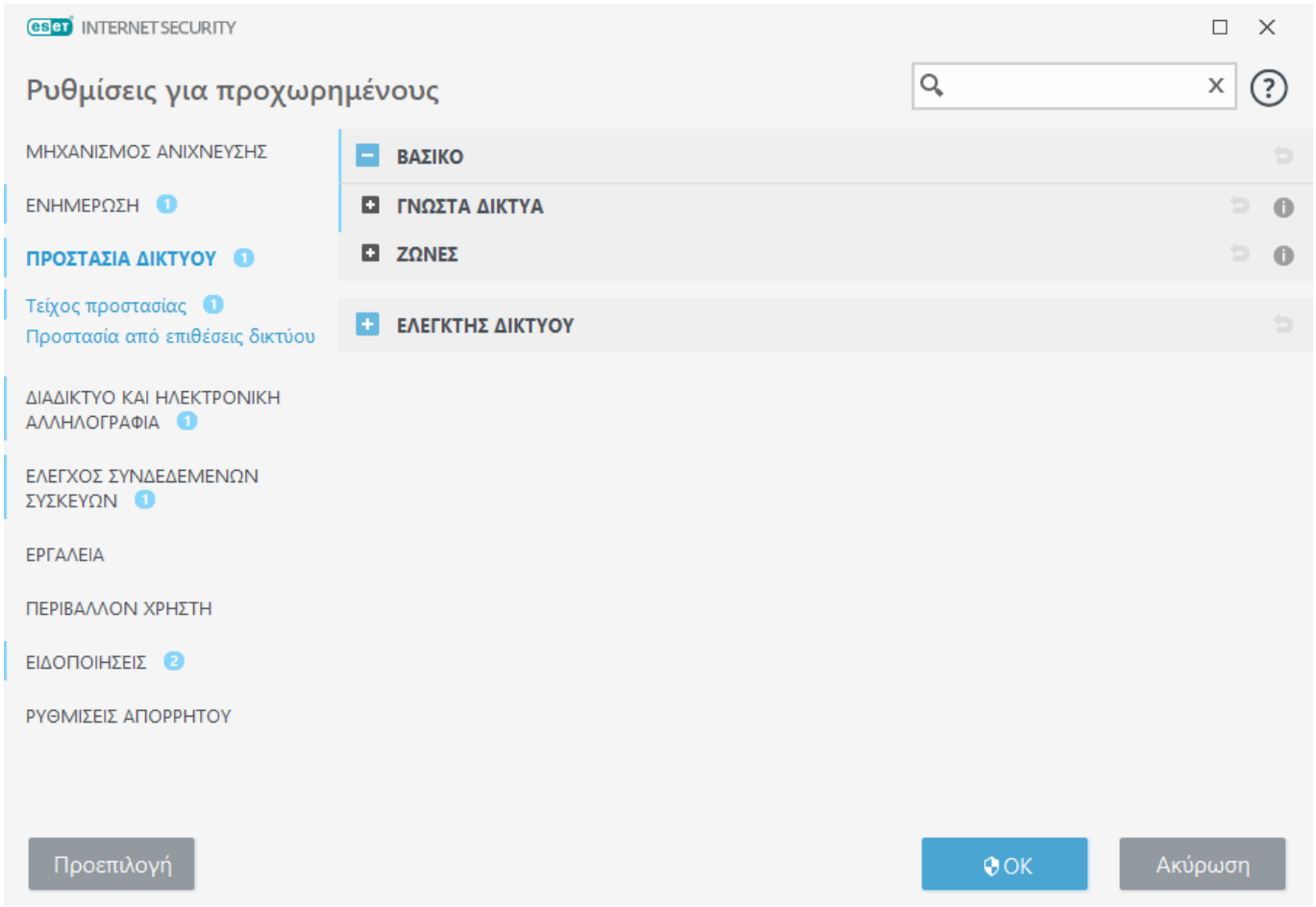
Συνδεδεμένα δίκτυα – Εμφανίζει τα δίκτυα στα οποία συνδέονται προσαρμογείς δικτύου. Αφού κάνετε κλικ στον σύνδεσμο που βρίσκεται κάτω από το όνομα δικτύου, ένα αναδυόμενο παράθυρο θα σας επιτρέψει να ρυθμίσετε τις παραμέτρους του δικτύου ως αξιόπιστου.

Προσωρινή λίστα αποκλεισμού διευθύνσεων IP – Εμφανίζει μια λίστα διευθύνσεων IP που έχουν ανιχνευτεί ως προέλευση επιθέσεων και έχουν προστεθεί στη λίστα αποκλεισμένων διευθύνσεων, ώστε να αποκλείεται η σύνδεση για συγκεκριμένο χρονικό διάστημα. Για περισσότερες πληροφορίες, κάντε κλικ σε αυτή την επιλογή και στη συνέχεια πατήστε F1.

Οδηγός επίλυσης προβλημάτων – Σας βοηθά να επιλύετε προβλήματα συνδεσιμότητας που προκαλούνται από το Τείχος προστασίας της ESET. Για περισσότερο λεπτομερείς πληροφορίες, ανατρέξτε στην ενότητα Οδηγός επίλυσης προβλημάτων.

Ρυθμίσεις για προχωρημένους της Προστασίας δικτύου

Στο κύριο παράθυρο του προγράμματος, κάντε κλικ στα στοιχεία **Ρυθμίσεις** > **Ρυθμίσεις για προχωρημένους** (F5) > **Προστασία δικτύου**.



Βασικό

Γνωστά δίκτυα

Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα Γνωστά δίκτυα.

Ζώνες

Μια ζώνη αντιπροσωπεύει μια συλλογή διευθύνσεων δικτύου οι οποίες δημιουργούν μία λογική ομάδα. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Ρύθμιση παραμέτρων ζωνών.

Ελεγκτής δικτύου

Ενεργοποίηση Ελεγκτή δικτύου

Η λειτουργία Ελεγκτής δικτύου βοηθά στην ταυτοποίηση τρωτών σημείων στο οικιακό δίκτυο, όπως οι ανοιχτές θύρες ή ένας αδύναμος κωδικός πρόσβασης δρομολογητή. Επίσης, παρέχει μια λίστα συνδεδεμένων συσκευών που είναι κατηγοριοποιημένες κατά τύπο συσκευής.

Ειδοποίηση όταν ανιχνεύονται νέες συσκευές οικιακού δικτύου

Θα ειδοποιείστε όταν ανιχνεύεται μια νέα συσκευή στο δίκτυό σας.

Γνωστά δίκτυα

Εάν χρησιμοποιείτε έναν υπολογιστή ο οποίος συνδέεται συχνά σε μη αξιόπιστα δίκτυα ή δίκτυα εκτός του αξιόπιστου (οικιακού ή εταιρικού) δικτύου σας, συνιστάται να επαληθεύετε την αξιοπιστία των νέων δικτύων με τα οποία συνδέεστε. Όταν οριστούν τα δίκτυα, το ESET Internet Security μπορεί να αναγνωρίσει τα αξιόπιστα (οικιακά ή εταιρικά) δίκτυα χρησιμοποιώντας παραμέτρους δικτύων, οι οποίες έχουν ρυθμιστεί στην **Αναγνώριση δικτύου**. Οι υπολογιστές συχνά συνδέονται σε δίκτυα με διευθύνσεις IP που είναι παρόμοιες με το αξιόπιστο δίκτυο. Σε αυτές τις περιπτώσεις, το ESET Internet Security μπορεί να θεωρήσει ένα άγνωστο δίκτυο ως αξιόπιστο (οικιακό ή εταιρικό δίκτυο). Συνιστάται να χρησιμοποιείτε το στοιχείο **Έλεγχος ταυτότητας δικτύου** για να αποφεύγετε τέτοιες καταστάσεις. Για να αποκτήσετε πρόσβαση στις ρυθμίσεις των γνωστών δικτύων, μεταβείτε στα στοιχεία **Εγκατάσταση για προχωρημένους** (F5) > **Προστασία δικτύου** > **Βασικές** > **Γνωστά δίκτυα**.

Εάν ένας προσαρμογέας δικτύου συνδέεται σε ένα δίκτυο ή εάν πραγματοποιηθεί εκ νέου ρύθμιση παραμέτρων του, το ESET Internet Security αναζητά στη λίστα γνωστών δικτύων μια εγγραφή που αντιστοιχεί στο νέο δίκτυο. Εάν η **Αναγνώριση δικτύου** και ο **Έλεγχος ταυτότητας δικτύου** (προαιρετικά) συμφωνούν, το δίκτυο θα επισημανθεί ως συνδεδεμένο σε αυτή τη διασύνδεση. Εάν δεν βρεθεί κανένα γνωστό δίκτυο, η ρύθμιση παραμέτρων της αναγνώρισης δικτύου θα δημιουργήσει μια νέα σύνδεση δικτύου, για να ταυτοποιήσει το δίκτυο την επόμενη φορά που θα συνδεθείτε σε αυτό. Από προεπιλογή, η σύνδεση με το νέο δίκτυο χρησιμοποιεί τον τύπο προστασίας που ορίζεται στις ρυθμίσεις των Windows. Το παράθυρο διαλόγου **Ανιχνεύτηκε νέα σύνδεση δικτύου** θα σας ζητήσει να επιλέξετε ανάμεσα στον τύπο προστασίας **αξιόπιστο δίκτυο**, **μη αξιόπιστο δίκτυο** ή **Χρήση ρύθμισης των Windows**. Εάν ένας προσαρμογέας δικτύου συνδεθεί με ένα γνωστό δίκτυο και το συγκεκριμένο δίκτυο επισημαίνεται ως **αξιόπιστο δίκτυο**, τα τοπικά υποδίκτυα του προσαρμογέα θα προστεθούν στη ζώνη αξιοπιστίας.

Τύπος προστασίας νέων δικτύων – Ορίστε μία από τις παρακάτω επιλογές: Για νέα δίκτυα χρησιμοποιείται από προεπιλογή το στοιχείο **Χρήση ρύθμισης των Windows**, **Ερώτηση στον χρήστη** ή **Επισήμανση ως μη αξιόπιστο**.

Το στοιχείο **Γνωστά δίκτυα** σάς επιτρέπει να διαμορφώσετε το όνομα δικτύου, την αναγνώριση δικτύου, τον τύπο προστασίας κ.λπ. Για να αποκτήσετε πρόσβαση στην Επεξεργασία γνωστών δικτύων, κάντε κλικ στο στοιχείο **Επεξεργασία**.

> Εάν επιλέξετε το στοιχείο **Χρήση ρύθμισης των Windows** δεν θα εμφανιστεί παράθυρο διαλόγου και το δίκτυο με το οποίο έχετε συνδεθεί θα επισημαίνεται αυτόματα, σύμφωνα με τις ρυθμίσεων των Windows στον υπολογιστή σας. Αυτό θα έχει ως αποτέλεσμα ορισμένες δυνατότητες (για παράδειγμα, η κοινή χρήση αρχείων και η απομακρυσμένη επιφάνεια εργασίας) να είναι προσπελάσιμες από νέα δίκτυα.

Επεξεργασία γνωστών δικτύων

Μπορείτε να διαμορφώσετε γνωστά δίκτυα μη αυτόματα στη διαδρομή **Εγκατάσταση για προχωρημένους** > **Προστασία δικτύου** > **Βασικές** > **Γνωστά δίκτυα** κάνοντας κλικ στο κουμπί **Επεξεργασία**.

Στήλες

Όνομα – Όνομα ενός γνωστού δικτύου.

Τύπος προστασίας – Δείχνει εάν το δίκτυο έχει ρυθμιστεί ως **Αξιόπιστο**, **Μη αξιόπιστο** ή **Χρήση ρυθμίσεων των Windows**.

Προφίλ τείχος προστασίας – Επιλέξτε ένα προφίλ από το αναπτυσσόμενο μενού **Εμφάνιση κανόνων που χρησιμοποιούνται στο προφίλ** για να εμφανιστεί το φίλτρο κανόνων του προφίλ.

Προφίλ ενημέρωσης – Σας επιτρέπει να εφαρμόσετε το προφίλ ενημέρωσης κατά τη σύνδεση σε αυτό το δίκτυο.

Στοιχεία ελέγχου

Προσθήκη – Δημιουργεί ένα νέο γνωστό δίκτυο.

Επεξεργασία – Κάντε κλικ για να επεξεργαστείτε ένα υπάρχον γνωστό δίκτυο.

Κατάργηση – Επιλέξτε ένα δίκτυο και κάντε κλικ στο κουμπί **Κατάργηση** για να το διαγράψετε από τη λίστα γνωστών δικτύων.

Κορυφή/Επάνω/Κάτω/Τέλος – Σας επιτρέπει να ρυθμίσετε το επίπεδο προτεραιότητας των γνωστών δικτύων (η σειρά προτεραιότητας των δικτύων ξεκινά από την κορυφή και καταλήγει στο τέλος της λίστας).

Οι ρυθμίσεις διαμόρφωσης δικτύου βρίσκονται στις παρακάτω καρτέλες:

Δίκτυο

Εδώ μπορείτε να ορίσετε το **Όνομα δικτύου** και να επιλέξετε το στοιχείο **Τύπος προστασίας** (αξιόπιστο, μη αξιόπιστο ή Χρήση ρύθμισης των Windows) για το δίκτυο. Χρησιμοποιήστε το αναπτυσσόμενο μενού **Προφίλ τείχος προστασίας** για να επιλέξετε το προφίλ για αυτό το δίκτυο. Εάν το δίκτυο χρησιμοποιεί τύπο προστασίας **αξιόπιστο**, τότε όλα τα άμεσα συνδεδεμένα υποδίκτυα θεωρούνται αξιόπιστα. Για παράδειγμα, εάν ένας προσαρμογέας δικτύου είναι συνδεδεμένος σε αυτό το δίκτυο με διεύθυνση IP 192.168.1.5 και μάσκα υποδικτύου 255.255.255.0, το υποδίκτυο 192.168.1.0/24 προστίθεται στη ζώνη αξιοπιστίας του προσαρμογέα. Εάν ο προσαρμογέας έχει περισσότερες διευθύνσεις ή υποδίκτυα, θεωρούνται όλα αξιόπιστα, ανεξάρτητα από τη διαμόρφωση **Αναγνώριση δικτύου** του γνωστού δικτύου.

Επιπλέον, οι διευθύνσεις που προστίθενται στην ενότητα **Πρόσθετες αξιόπιστες διευθύνσεις** προστίθενται πάντα στη ζώνη αξιοπιστίας των προσαρμογέων που συνδέονται σε αυτό το δίκτυο (ανεξάρτητα από τον τύπο προστασίας του δικτύου).

Ειδοποίηση σχετικά με αδύναμη κρυπτογράφηση WiFi – Το ESET Internet Security θα σας ειδοποιεί όταν συνδέεστε με ένα μη προστατευμένο ασύρματο δίκτυο ή ένα δίκτυο με αδύναμη προστασία.

Προφίλ τείχους προστασίας – Επιλέξτε το προφίλ τείχους προστασίας που χρησιμοποιείται κατά τη σύνδεση σε αυτό το δίκτυο.

Προφίλ ενημέρωσης – Επιλέξτε το προφίλ ενημέρωσης που χρησιμοποιείται κατά τη σύνδεση σε αυτό το δίκτυο.

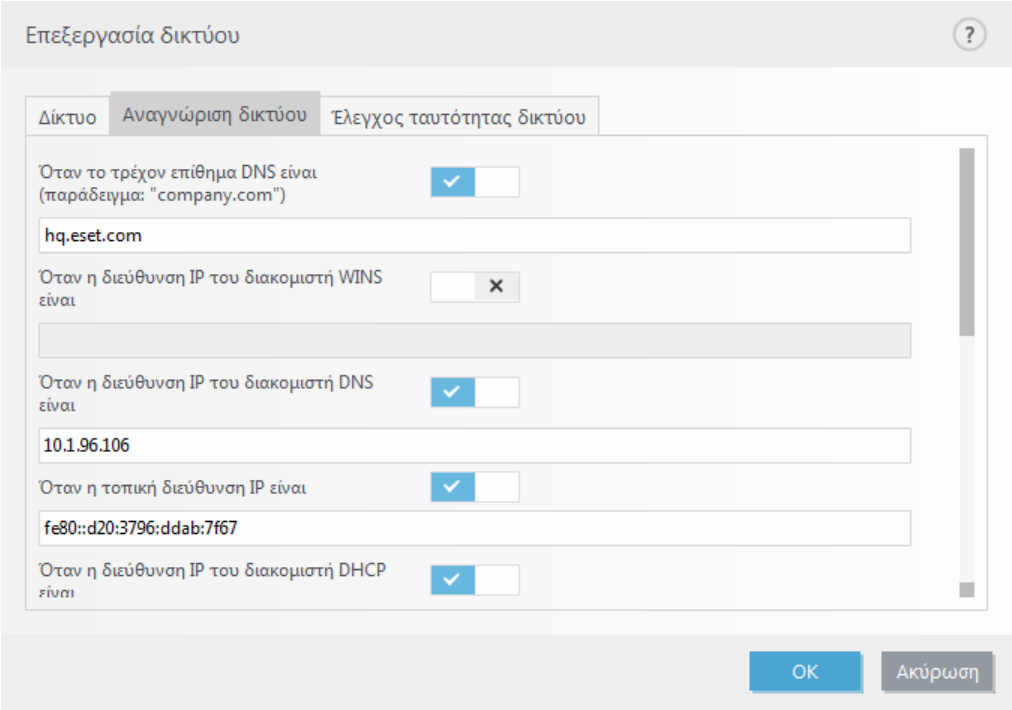
Για να επισημανθεί ένα δίκτυο ως συνδεδεμένο στη λίστα συνδεδεμένων δικτύων, πρέπει να πληρούνται οι εξής προϋποθέσεις:

• **Αναγνώριση δικτύου** – Όλες οι συμπληρωμένες παράμετροι πρέπει να ταιριάζουν με τις παραμέτρους της ενεργής σύνδεσης.

• **Έλεγχος ταυτότητας δικτύου** – Εάν έχει επιλεγεί διακομιστής ελέγχου ταυτότητας, πρέπει να πραγματοποιηθεί επιτυχής έλεγχος ταυτότητας με το διακομιστή ελέγχου ταυτότητας της ESET.

Αναγνώριση δικτύου

Η αναγνώριση δικτύου εκτελείται με βάση τις παραμέτρους του προσαρμογέα τοπικού δικτύου. Όλες οι επιλεγμένες παράμετροι συγκρίνονται με τις πραγματικές παραμέτρους των ενεργών συνδέσεων δικτύου. Επιτρέπονται οι διευθύνσεις IPv4 και IPv6.



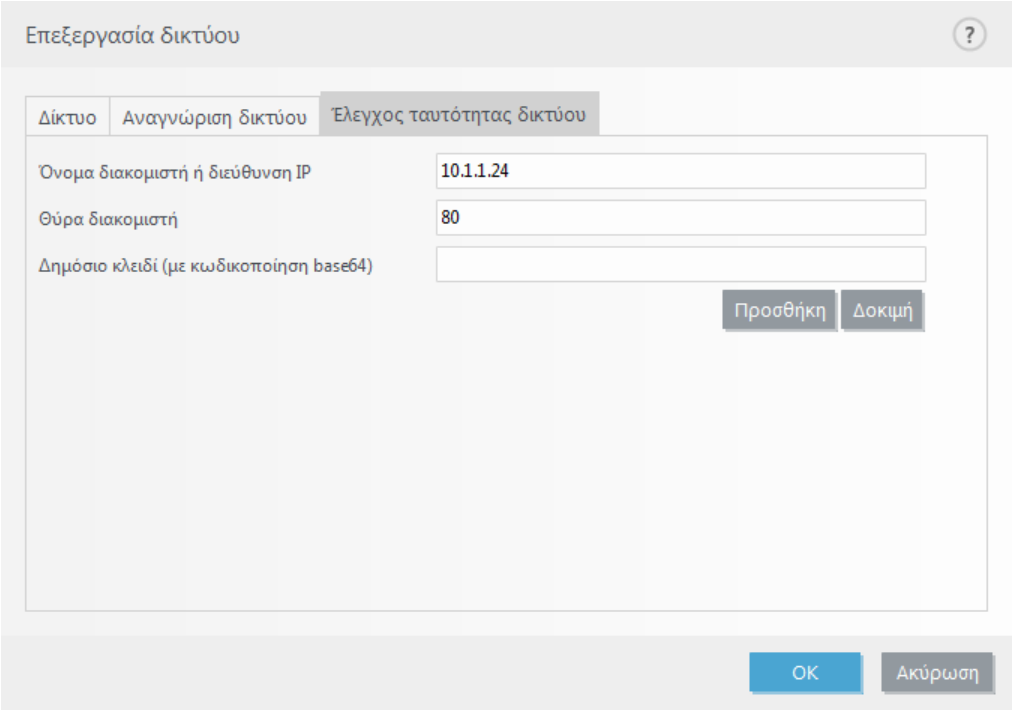
Έλεγχος ταυτότητας δικτύου

Ο έλεγχος ταυτότητας δικτύου αναζητά έναν συγκεκριμένο διακομιστή στο δίκτυο και χρησιμοποιεί ασυμμετρική κρυπτογράφηση (RSA) για τον έλεγχο ταυτότητας του συγκεκριμένου διακομιστή. Το όνομα του δικτύου για το οποίο εκτελείται έλεγχος ταυτότητας πρέπει να ταιριάζει με το όνομα ζώνης που καθορίζεται στις ρυθμίσεις του διακομιστή ελέγχου ταυτότητας. Στο όνομα γίνεται διάκριση πεζών-κεφαλαίων. Καθορίστε ένα όνομα διακομιστή, μια θύρα παρακολούθησης του διακομιστή και ένα δημόσιο κλειδί που αντιστοιχεί στο ιδιωτικό κλειδί διακομιστή (δείτε την ενότητα Έλεγχος ταυτότητας δικτύου – Διαμόρφωση διακομιστή). Το όνομα διακομιστή μπορεί να εισαχθεί με τη μορφή διεύθυνσης IP, ονόματος DNS ή NetBios και να ακολουθείται από μια διαδρομή που καθορίζει τη θέση του κλειδιού του διακομιστή (για παράδειγμα, όνομα_διακομιστή_/directory1/directory2/authentication). Μπορείτε να καθορίσετε εναλλακτικούς διακομιστές προσθέτοντάς τους στη διαδρομή, διαχωρισμένους με ερωτηματικά (;).

Κάντε λήψη του Διακομιστή ελέγχου ταυτότητας ESET.

Το δημόσιο κλειδί μπορεί να εισαχθεί χρησιμοποιώντας έναν από τους παρακάτω τύπους αρχείου:

- Κρυπτογραφημένο δημόσιο κλειδί PEM (.pem). Αυτό το κλειδί μπορεί να δημιουργηθεί χρησιμοποιώντας το Διακομιστή ελέγχου ταυτότητας της ESET (δείτε την ενότητα Έλεγχος ταυτότητας δικτύου – Διαμόρφωση διακομιστή).
- Κρυπτογραφημένο δημόσιο κλειδί
- Πιστοποιητικό δημόσιου κλειδιού (.crt)



Κάντε κλικ στο κουμπί **Δοκιμή** για να δοκιμάσετε τις ρυθμίσεις σας. Εάν ο έλεγχος ταυτότητας είναι επιτυχής, θα εμφανιστεί η ειδοποίηση Ο έλεγχος ταυτότητας του διακομιστή ήταν επιτυχής. Εάν ο έλεγχος ταυτότητας δεν έχει διαμορφωθεί σωστά, θα εμφανιστεί ένα από τα ακόλουθα μηνύματα σφάλματος:

Απέτυχε ο έλεγχος ταυτότητας διακομιστή. Η υπογραφή δεν είναι έγκυρη ή δεν αντιστοιχεί.
Η υπογραφή διακομιστή δεν ταιριάζει με το δημόσιο κλειδί που έχει εισαχθεί.

Απέτυχε ο έλεγχος ταυτότητας διακομιστή. Το όνομα δικτύου δεν αντιστοιχεί.
Το διαμορφωμένο όνομα δικτύου δεν αντιστοιχεί στο όνομα της ζώνης του διακομιστή ελέγχου ταυτότητας. Ελέγξτε και τα δυο ονόματα και βεβαιωθείτε ότι είναι ίδια.

Απέτυχε ο έλεγχος ταυτότητας διακομιστή. Ο διακομιστής δεν ανταποκρίνεται με έγκυρο τρόπο ή δεν ανταποκρίνεται καθόλου.
Δεν λαμβάνεται απόκριση εάν ο διακομιστής δεν εκτελείται ή δεν είναι προσβάσιμος. Μπορεί να ληφθεί μη έγκυρη απόκριση, εάν ένας άλλος διακομιστής HTTP εκτελείται στην καθορισμένη διεύθυνση.

Έγινε εισαγωγή μη έγκυρου κλειδιού.
Βεβαιωθείτε ότι δεν έχει καταστραφεί το αρχείο δημόσιου κλειδιού που έχετε εισαγάγει.

Έλεγχος ταυτότητας δικτύου - Διαμόρφωση διακομιστή

Η διαδικασία ελέγχου ταυτότητας μπορεί να εκτελεστεί από οποιονδήποτε υπολογιστή/διακομιστή που είναι συνδεδεμένος στο δίκτυο στο οποίο πρόκειται να γίνει έλεγχος ταυτότητας. Η εφαρμογή "Διακομιστής ελέγχου ταυτότητας" της ESET πρέπει να είναι εγκατεστημένη σε έναν υπολογιστή/διακομιστή στον οποίο η πρόσβαση είναι πάντοτε δυνατή κάθε φορά που ένας υπολογιστής-πελάτης επιχειρεί να συνδεθεί στο δίκτυο. Το αρχείο εγκατάστασης της εφαρμογής Διακομιστής ελέγχου ταυτότητας της ESET είναι διαθέσιμο για λήψη στον ιστότοπο της ESET.

Αφού εγκαταστήσετε την εφαρμογή "Διακομιστής ελέγχου ταυτότητας" της ESET, θα εμφανιστεί ένα παράθυρο διαλόγου (μπορείτε να αποκτήσετε πρόσβαση στην εφαρμογή πατώντας **Έναρξη** > **Προγράμματα** > **ESET** > **Διακομιστής ελέγχου ταυτότητας**).

Για να διαμορφώσετε το διακομιστή ελέγχου ταυτότητας, πληκτρολογήστε το όνομα ζώνης ελέγχου ταυτότητας, τη θύρα παρακολούθησης του διακομιστή (η προεπιλογή είναι 80), καθώς και τη θέση για την αποθήκευση του ζεύγους δημόσιου και ιδιωτικού κλειδιού. Κατόπιν, δημιουργήστε το δημόσιο και το ιδιωτικό κλειδί που θα χρησιμοποιηθεί στη διαδικασία ελέγχου ταυτότητας. Το ιδιωτικό κλειδί θα παραμείνει στο διακομιστή, ενώ το δημόσιο κλειδί πρέπει να εισαχθεί στην πλευρά του υπολογιστή-πελάτη στην ενότητα "Έλεγχος ταυτότητας ζώνης" κατά τη ρύθμιση μιας ζώνης στις ρυθμίσεις του firewall.

Για πιο λεπτομερείς πληροφορίες, ανατρέξτε στο παρακάτω άρθρο της Γνωσιακή βάσης της ESET.

Ρύθμιση παραμέτρων ζωνών

Η ζώνη είναι μια συλλογή διευθύνσεων δικτύου που αποτελούν μια λογική ομάδα διευθύνσεων IP και είναι χρήσιμη όταν επαναχρησιμοποιείται το ίδιο σύνολο διευθύνσεων σε πολλαπλούς κανόνες. Κάθε διεύθυνση σε μια συγκεκριμένη ομάδα αντιστοιχίζεται με παρόμοιους κανόνες που καθορίζονται κεντρικά για ολόκληρη την ομάδα. Ένα παράδειγμα μιας τέτοιας ομάδας είναι η **Ζώνη αξιοπιστίας**. Η Ζώνη αξιοπιστίας αντιπροσωπεύει μια ομάδα διευθύνσεων δικτύου που δεν αποκλείονται με κανέναν τρόπο από το τείχος προστασίας.

Για να προσθέσετε μια ζώνη αξιοπιστίας:

1. Μεταβείτε στα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5) > **Προστασία δικτύου** > **Βασικές ρυθμίσεις** > **Ζώνες**.

2. Κάντε κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Ζώνες**.

3. Κάντε κλικ στο στοιχείο **Προσθήκη**, πληκτρολογήστε ένα **Όνομα** και μια **Περιγραφή** για τη ζώνη και πληκτρολογήστε μια απομακρυσμένη διεύθυνση IP στο στοιχείο **Διεύθυνση απομακρυσμένου υπολογιστή (IPv4/IPv6, εύρος, μάσκα)**.

4. Κάντε κλικ στο στοιχείο **OK**.

Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα Ζώνες τείχους προστασίας.

Ζώνες τείχος προστασίας

Για περισσότερες πληροφορίες σχετικά με τις ζώνες, ανατρέξτε στην ενότητα Διαμόρφωση ζωνών.

Στήλες

Όνομα – Όνομα μιας ομάδας απομακρυσμένων υπολογιστών.

Διευθύνσεις IP – Οι απομακρυσμένες διευθύνσεις IP που ανήκουν σε μια ζώνη.

Στοιχεία ελέγχου

Όταν κάνετε **Προσθήκη** ή **Επεξεργασία** μιας ζώνης, τα παρακάτω πεδία γίνονται διαθέσιμα:

Όνομα – Όνομα μιας ομάδας απομακρυσμένων υπολογιστών.

Περιγραφή – Μια γενική περιγραφή της ομάδας.

Διεύθυνση απομακρυσμένου υπολογιστή (IPv4, IPv6, εύρος, μάσκα) – Σας επιτρέπει να προσθέσετε μια απομακρυσμένη διεύθυνση, εύρος διευθύνσεων ή υποδίκτυο.

Διαγραφή – Αφαιρεί μια ζώνη από τη λίστα.

Να έχετε υπόψη ότι δεν είναι δυνατή η κατάργηση προκαθορισμένων ζωνών.

Τείχος προστασίας

Το Firewall ελέγχει όλη την κυκλοφορία δικτύου προς και από το σύστημα. Αυτό επιτυγχάνεται επιτρέποντας ή αποκλείοντας μεμονωμένες συνδέσεις δικτύου με βάση καθορισμένους κανόνες φιλτραρίσματος. Παρέχει προστασία έναντι επιθέσεων από απομακρυσμένους υπολογιστές και μπορεί να αποκλείσει δυνητικά απειλητικές υπηρεσίες.

Βασικό

Ενεργοποίηση προστασίας τείχους προστασίας

Συνιστάται να διατηρείτε ενεργοποιημένη αυτήν τη δυνατότητα για να διασφαλίζεται η ασφάλεια του συστήματός σας. Όταν το firewall είναι ενεργοποιημένο, η κίνηση δικτύου σαρώνεται και προς τις δύο κατευθύνσεις.

Επιπλέον αξιολόγηση κανόνων από το Τείχος προστασίας των Windows

Στην αυτόματη λειτουργία, επιτρέπεται επίσης η εισερχόμενη κυκλοφορία που επιτρέπεται από κανόνες του Τείχους προστασίας των Windows, εκτός εάν αποκλείεται ρητά από κανόνες ESET.

Λειτουργία φιλτραρίσματος

Η συμπεριφορά του τείχους προστασίας αλλάζει ανάλογα με τη λειτουργία φιλτραρίσματος. Οι λειτουργίες φιλτραρίσματος μπορεί επίσης να επηρεάσουν το απαιτούμενο επίπεδο αλληλεπίδρασης με το χρήστη.

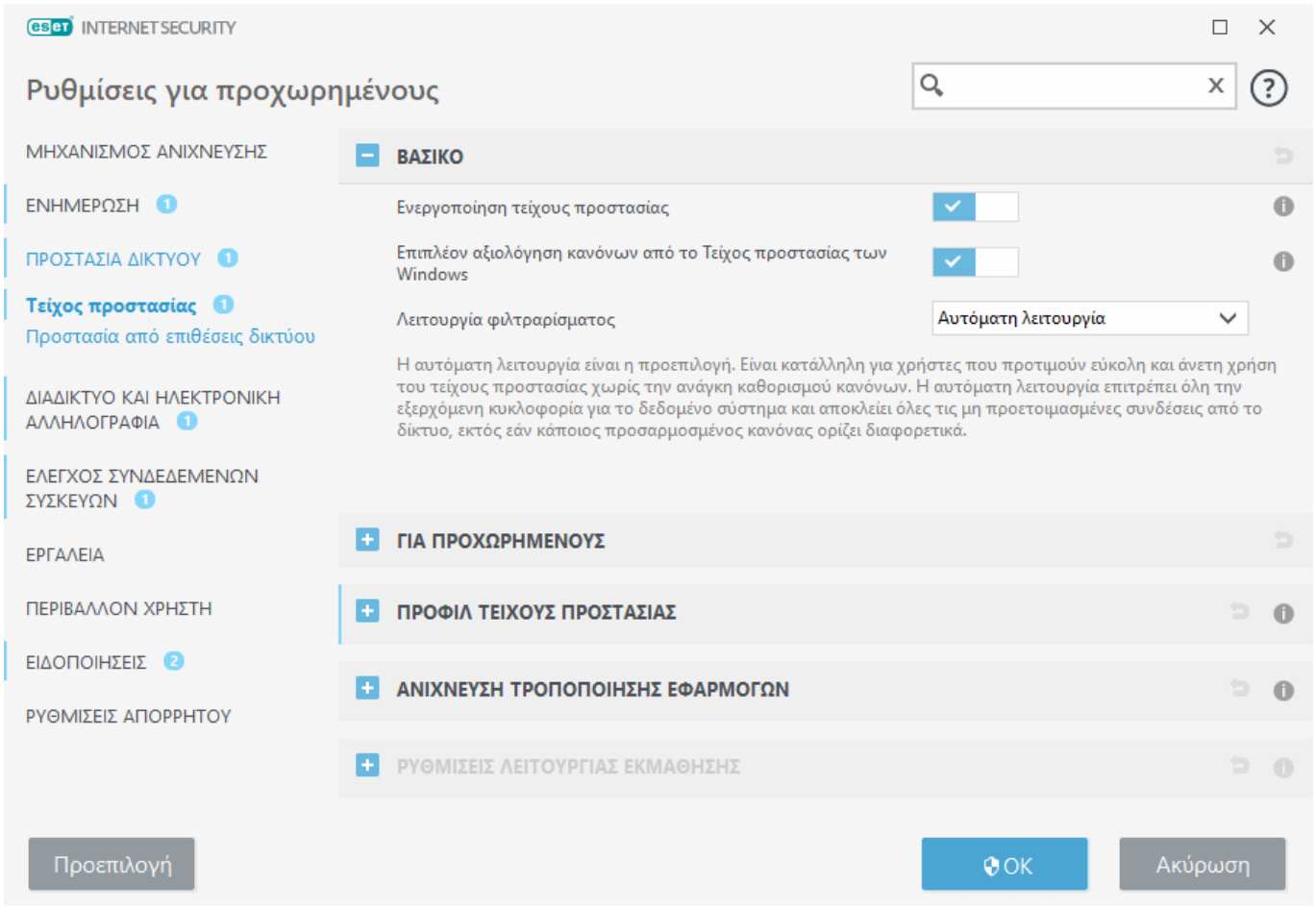
Για το Τείχος προστασίας του ESET Internet Security υπάρχουν οι εξής λειτουργίες φιλτραρίσματος:

Λειτουργία φιλτραρίσματος	Περιγραφή
Αυτόματη λειτουργία	Η προεπιλεγμένη λειτουργία. Αυτή η λειτουργία είναι κατάλληλη για χρήστες που προτιμούν την εύκολη και άνετη χρήση του τείχους προστασίας που δεν απαιτεί τον καθορισμό κανόνων. Μπορείτε να δημιουργήσετε προσαρμοσμένους κανόνες, αλλά δεν απαιτούνται στην **Αυτόματη λειτουργία**. Η αυτόματη λειτουργία επιτρέπει όλη την εξερχόμενη κίνηση για ένα συγκεκριμένο σύστημα και αποκλείει το μεγαλύτερο μέρος της εισερχόμενης κίνησης, με εξαίρεση ένα μέρος της κυκλοφορίας από τη ζώνη αξιοπιστίας (όπως περιγράφεται στην ενότητα IDS και ρυθμίσεις για προχωρημένους/Επιτρεπτές υπηρεσίες), και αποκρίσεις σε πρόσφατες εξερχόμενες επικοινωνίες.
Αλληλεπιδραστική λειτουργία	Σας επιτρέπει να δημιουργήσετε μια προσαρμοσμένη διαμόρφωση για το Firewall. Όταν ανιχνευτεί μια επικοινωνία και δεν εφαρμόζονται υπάρχοντες κανόνες σε αυτήν, θα εμφανίζεται ένα παράθυρο διαλόγου που θα αναφέρει μια άγνωστη σύνδεση. Το παράθυρο διαλόγου παρέχει την επιλογή να επιτρέπετε ή να απορρίπτετε την επικοινωνία και η απόφαση να επιτραπεί ή να απορριφθεί θα αποθηκεύεται ως νέος κανόνας για το Firewall. Εάν επιλέξετε να δημιουργήσετε έναν νέο κανόνα, όλες οι μελλοντικές συνδέσεις αυτού του τύπου θα επιτρέπονται ή θα αποκλείονται σύμφωνα με τον κανόνα.
Λειτουργία βασισμένη σε πολιτική	Αποκλείει όλες τις συνδέσεις που δεν καθορίζονται από έναν συγκεκριμένο κανόνα που τις επιτρέπει. Η λειτουργία αυτή επιτρέπει σε προχωρημένους χρήστες να καθορίσουν κανόνες που επιτρέπουν μόνο επιθυμητές και ασφαλείς συνδέσεις. Όλες οι άλλες μη καθορισμένες συνδέσεις θα αποκλείονται από το Firewall.
Λειτουργία εκμάθησης	Δημιουργεί και αποθηκεύει κανόνες αυτόματα. Η λειτουργία αυτή χρησιμοποιείται καλύτερα για την αρχική διαμόρφωση του Firewall, αλλά δεν θα πρέπει να παραμένει ενεργή για παρατεταμένα χρονικά διαστήματα. Δεν απαιτείται αλληλεπίδραση του χρήστη επειδή το ESET Internet Security αποθηκεύει τους κανόνες σύμφωνα με προκαθορισμένες παραμέτρους. Για την αποφυγή κινδύνων ασφαλείας, η λειτουργία εκμάθησης θα πρέπει να χρησιμοποιείται μόνο μέχρι να δημιουργηθούν όλοι οι κανόνες για τις απαιτούμενες επικοινωνίες.

Για προχωρημένους

Κανόνες

Η ρύθμιση κανόνων σας επιτρέπει να εμφανίσετε όλους τους κανόνες που εφαρμόζονται στην κυκλοφορία που δημιουργείται από μεμονωμένες εφαρμογές μέσα στις αξιόπιστες ζώνες και το διαδίκτυο.



Μπορείτε να δημιουργήσετε έναν κανόνα IDS εάν ένα Botnet επιτεθεί στον υπολογιστή σας. Μπορείτε να τροποποιήσετε έναν κανόνα από τη διαδρομή **Εγκατάσταση για προχωρημένους** (F5) > **Προστασία δικτύου** > **Προστασία από επιθέσεις δικτύου** > **Κανόνες IDS** κάνοντας κλικ στο στοιχείο **Επεξεργασία**.

Επιτρεπτές υπηρεσίες

Ρυθμίστε τις παραμέτρους πρόσβασης σε κοινές υπηρεσίες δικτύου που εκτελούνται στον υπολογιστή σας. Δείτε την ενότητα επιτρεπτές υπηρεσίες για περισσότερες πληροφορίες.

Προφίλ τείχος προστασίας

Μπορείτε να χρησιμοποιήσετε προφίλ τείχους προστασίας για να προσαρμόσετε τη συμπεριφορά του Τείχος προστασίας του ESET Internet Security καθορίζοντας διαφορετικά σύνολα κανόνων για διαφορετικές περιπτώσεις.

Ανίχνευση τροποποίησης εφαρμογών

Η δυνατότητα ανίχνευσης τροποποίησης εφαρμογής εμφανίζει ειδοποιήσεις εάν γίνει προσπάθεια δημιουργίας συνδέσεων από τροποποιημένες εφαρμογές, για τις οποίες υπάρχει κανόνας τείχους προστασίας.

Προφίλ τείχος προστασίας

Τα προφίλ μπορούν να χρησιμοποιηθούν για τον έλεγχο της συμπεριφοράς του Firewall του ESET Internet Security. Όταν δημιουργείτε ή επεξεργάζεστε έναν κανόνα του Firewall, μπορείτε να αντιστοιχίσετε σε αυτόν ένα συγκεκριμένο προφίλ ή να τον εφαρμόσετε σε κάθε προφίλ. Όταν ένα προφίλ είναι ενεργό σε μια διασύνδεση δικτύου, εφαρμόζονται μόνο οι καθολικοί κανόνες (κανόνες χωρίς καθορισμένο προφίλ) και οι κανόνες που έχουν αντιστοιχιστεί στο συγκεκριμένο προφίλ. Μπορείτε να δημιουργήσετε πολλά προφίλ με διαφορετικούς κανόνες αντιστοιχισμένους σε προσαρμογείς δικτύου ή σε δίκτυα, για να αλλάζετε εύκολα τη συμπεριφορά του Firewall.

Κάντε κλικ στην επιλογή **Επεξεργασία** δίπλα από τη Λίστα προφίλ, για να ανοίξετε το παράθυρο **Προφίλ Firewall** από όπου μπορείτε να επεξεργαστείτε τα προφίλ.

Μπορείτε να ρυθμίσετε έναν προσαρμογέα δικτύου, ο οποίος θα χρησιμοποιεί ένα προφίλ οι παράμετροι του οποίου έχουν ρυθμιστεί για ένα συγκεκριμένο δίκτυο, όταν ο προσαρμογέας είναι συνδεδεμένος σε αυτό το δίκτυο. Μπορείτε επίσης να αντιστοιχίσετε ένα συγκεκριμένο προφίλ που θα χρησιμοποιείται σε ένα συγκεκριμένο δίκτυο, στη διαδρομή **Ρυθμίσεις για προχωρημένους** (F5) > **Προστασία δικτύου** > **Γνωστά δίκτυα** > **Επεξεργασία**. Επιλέξτε ένα δίκτυο από τη λίστα με τα **Γνωστά δίκτυα** και κάντε κλικ στο στοιχείο **Επεξεργασία** για να αντιστοιχίσετε ένα προφίλ τείχους προστασίας στο συγκεκριμένο δίκτυο από το αναπτυσσόμενο μενού **Προφίλ τείχους προστασίας**.

Εάν αυτό το δίκτυο δεν έχει αντιστοιχισμένο προφίλ, τότε θα χρησιμοποιηθεί το προεπιλεγμένο προφίλ του προσαρμογέα. Εάν ο προσαρμογέας έχει ρυθμιστεί ώστε να μην χρησιμοποιεί το προφίλ του δικτύου, θα χρησιμοποιείται το προεπιλεγμένο προφίλ του προσαρμογέα ανεξάρτητα από το δίκτυο στο οποίο είναι συνδεδεμένος. Εάν δεν υπάρχει προφίλ για τη ρύθμιση παραμέτρων του δικτύου ή του προσαρμογέα, χρησιμοποιείται το καθολικό προεπιλεγμένο προφίλ. Για να αντιστοιχίσετε ένα προφίλ σε έναν προσαρμογέα δικτύου, επιλέξτε τον προσαρμογέα δικτύου, κάντε κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Προφίλ αντιστοιχισμένα σε προσαρμογείς δικτύου**, επεξεργαστείτε τον επιλεγμένο προσαρμογέα δικτύου και επιλέξτε το προφίλ από το αναπτυσσόμενο μενού **Προεπιλεγμένο προφίλ τείχους προστασίας**.

Όταν το Firewall κάνει εναλλαγή σε ένα άλλο προφίλ, θα εμφανιστεί μια ειδοποίηση στην κάτω δεξιά γωνία, δίπλα στο ρολόι του συστήματος.

Παράθυρο διαλόγου - Επεξεργασία προφίλ τείχους προστασίας

Εδώ μπορείτε να κάνετε **Προσθήκη**, **Επεξεργασία** ή **Κατάργηση** προφίλ. Σημειώστε ότι για να κάνετε **Επεξεργασία** ή **Κατάργηση** ενός προφίλ, πρέπει να είναι επιλεγμένο από τη λίστα στο παράθυρο **Προφίλ firewall**.

Για περισσότερες πληροφορίες, δείτε το θέμα Προφίλ firewall.

Προφίλ αντιστοιχισμένα σε προσαρμογείς

δικτύου

Εναλλάσσοντας προφίλ, μπορείτε γρήγορα να πραγματοποιήσετε πολλαπλές αλλαγές στη συμπεριφορά του τείχος προστασίας. Μπορείτε να ρυθμίσετε προσαρμοσμένους κανόνες και να τους εφαρμόσετε σε συγκεκριμένα προφίλ. Οι καταχωρίσεις προσαρμογέων δικτύου για όλους τους προσαρμογείς που βρίσκονται στον υπολογιστή προστίθενται αυτόματα στη λίστα **Προσαρμογείς δικτύου**.

Στήλες

Όνομα – Όνομα του προσαρμογέα δικτύου.

Προεπιλεγμένο προφίλ τείχος προστασίας – Το προεπιλεγμένο προφίλ χρησιμοποιείται όταν το δίκτυο στο οποίο συνδέεστε δεν έχει διαμορφωμένο προφίλ ή όταν ο προσαρμογέας δικτύου είναι ρυθμισμένος έτσι ώστε να μη χρησιμοποιεί προφίλ δικτύου.

Να προτιμάται το προφίλ δικτύου – Όταν είναι ενεργοποιημένη η επιλογή **Να προτιμάται το προφίλ firewall του συνδεδεμένου δικτύου**, ο προσαρμογέας δικτύου θα χρησιμοποιεί το προφίλ firewall που είναι αντιστοιχισμένο σε ένα συνδεδεμένο δίκτυο, όποτε αυτό είναι δυνατό.

Στοιχεία ελέγχου

Προσθήκη – Προσθέτει έναν νέο προσαρμογέα δικτύου.

Επεξεργασία – Σας επιτρέπει να επεξεργαστείτε έναν υπάρχοντα προσαρμογέα δικτύου.

Κατάργηση – Επιλέξτε έναν προσαρμογέα δικτύου και κάντε κλικ στο στοιχείο **Κατάργηση** εάν θέλετε να καταργήσετε έναν προσαρμογέα δικτύου από τη λίστα.

OK/Ακύρωση – Κάντε κλικ στο κουμπί **OK**, εάν θέλετε να αποθηκεύσετε τις αλλαγές ή στο κουμπί **Ακύρωση** για έξοδο χωρίς αποθήκευση των αλλαγών.

Διαμόρφωση και χρήση κανόνων

Οι κανόνες αντιπροσωπεύουν ένα σύνολο προϋποθέσεων που χρησιμοποιούνται για την εκτέλεση σημαντικών δοκιμών σε όλες τις συνδέσεις δικτύου και σε όλες τις ενέργειες που έχουν αντιστοιχιστεί σε αυτές τις προϋποθέσεις. Με τη χρήση των κανόνων τείχους προστασίας, μπορείτε να καθορίσετε την ενέργεια που θα πραγματοποιείται όταν δημιουργούνται διάφοροι τύποι συνδέσεων δικτύου. Για να αποκτήσετε πρόσβαση στις ρυθμίσεις κανόνων φιλτραρίσματος, μεταβείτε στα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5) > **Τείχος προστασίας** > **Για προχωρημένους**. Κάποιοι προκαθορισμένοι κανόνες συνδέονται με πλαίσια ελέγχου από τις **επιτρεπτές υπηρεσίες** (Επιλογές IDS και επιλογές για προχωρημένους) και δεν μπορούν να απενεργοποιηθούν απευθείας, παρά μόνο χρησιμοποιώντας τα αντίστοιχα πλαίσια ελέγχου.

Σε αντίθεση με την προηγούμενη έκδοση του ESET Internet Security, η σειρά προτεραιότητας των κανόνων ξεκινά από την προς το τέλος. Η ενέργεια του πρώτου κανόνα που αντιστοιχεί χρησιμοποιείται για κάθε σύνδεση δικτύου που αξιολογείται. Αυτό είναι μια σημαντική αλλαγή συμπεριφοράς σε σχέση με την προηγούμενη έκδοση, στην οποία η προτεραιότητα των κανόνων ήταν αυτόματη και οι πιο εξειδικευμένοι κανόνες είχαν μεγαλύτερη προτεραιότητα από τους γενικότερους.

Οι συνδέσεις διαιρούνται σε εισερχόμενες και εξερχόμενες συνδέσεις. Οι εισερχόμενες συνδέσεις ξεκινούν όταν ένας απομακρυσμένος υπολογιστής επιχειρεί να δημιουργήσει σύνδεση με το τοπικό σύστημα. Οι εξερχόμενες συνδέσεις λειτουργούν με τον αντίθετο τρόπο – το τοπικό σύστημα επικοινωνεί με έναν απομακρυσμένο υπολογιστή.

Αν ανιχνευτεί μια νέα άγνωστη επικοινωνία, πρέπει να μελετήσετε προσεκτικά αν θα την επιτρέψετε ή αν θα την απορρίψετε. Οι ανεπιθύμητες, μη ασφαλείς ή άγνωστες συνδέσεις αποτελούν κίνδυνο για την ασφάλεια του συστήματος. Αν δημιουργηθεί μια τέτοια σύνδεση, συνιστάται να προσέξετε ιδιαίτερα τον απομακρυσμένο υπολογιστή και την εφαρμογή που επιχειρεί να συνδεθεί με τον υπολογιστή σας. Πολλές εισβολές προσπαθούν να λάβουν και αποστείλουν τα προσωπικά σας δεδομένα ή να αποστείλουν άλλες κακόβουλες εφαρμογές σε σταθμούς εργασίας κεντρικού υπολογιστή. Το Firewall σάς επιτρέπει να ανιχνεύσετε και να τερματίσετε τέτοιες συνδέσεις.

Λίστα κανόνων τείχους προστασίας

Η λίστα κανόνων τείχους προστασίας βρίσκεται στη διαδρομή **Ρυθμίσεις για προχωρημένους** (F5) > **Προστασία δικτύου** > **Τείχος προστασίας** > **Για προχωρημένους** κάνοντας κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Κανόνες**.

Στήλες

Όνομα – Το όνομα του κανόνα.

Ενεργός – Δείχνει εάν ο κανόνας είναι ενεργοποιημένος ή απενεργοποιημένος. Το αντίστοιχο πλαίσιο ελέγχου πρέπει να είναι επιλεγμένο για να ενεργοποιήσετε έναν κανόνα.

Πρωτόκολλο – Το πρωτόκολλο για το οποίο ισχύει αυτός ο κανόνας.

Προφίλ – Δείχνει το προφίλ τείχος προστασίας για το οποίο ισχύει αυτός ο κανόνας.

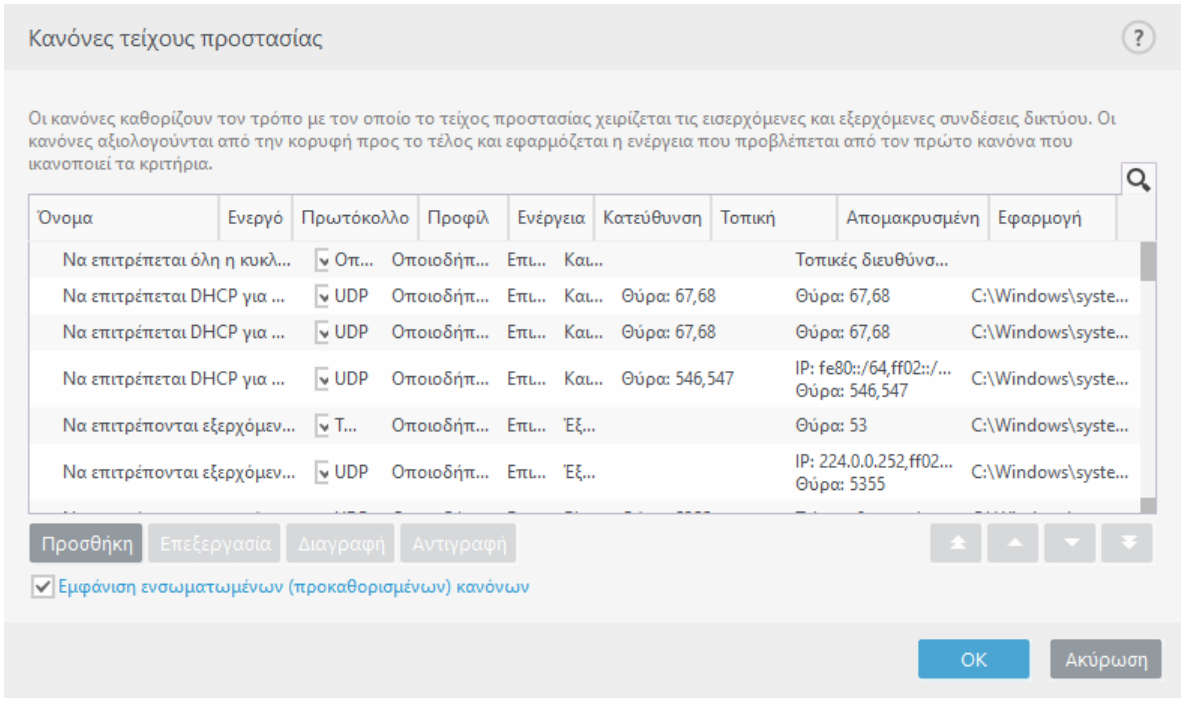
Ενέργεια – Εμφανίζει την κατάσταση της επικοινωνίας (αποκλεισμός/αποδοχή/ερώτηση).

Κατεύθυνση – Η κατεύθυνση της επικοινωνίας (εισερχόμενη/εξερχόμενη/και τα δύο).

Τοπικός – Απομακρυσμένη διεύθυνση IPv4 ή IPv6 / εύρος / υποδίκτυο και θύρα τοπικού υπολογιστή.

Απομακρυσμένος – Απομακρυσμένη διεύθυνση IPv4 ή IPv6 / εύρος / υποδίκτυο και θύρα απομακρυσμένου υπολογιστή.

Εφαρμογή – Οι εφαρμογές στις οποίες εφαρμόζεται ο κανόνας.



Στοιχεία ελέγχου

Προσθήκη – Δημιουργεί νέο κανόνα.

Επεξεργασία – Επεξεργασία ενός υπάρχοντος κανόνα.

Κατάργηση – Κατάργηση ενός υπάρχοντος κανόνα.

Αντιγραφή – Δημιουργεί αντίγραφο ενός επιλεγμένου κανόνα.

Εμφάνιση ενσωματωμένων (προκαθορισμένων) κανόνων – Κανόνες που είναι προκαθορισμένοι από το ESET Internet Security και επιτρέπουν ή απορρίπτουν συγκεκριμένες επικοινωνίες. Μπορείτε να απενεργοποιήσετε αυτούς τους κανόνες, αλλά δεν μπορείτε να διαγράψετε έναν προκαθορισμένο κανόνα.

Κορυφή/Επάνω/Κάτω/Τέλος – Σας επιτρέπει να ρυθμίσετε το επίπεδο προτεραιότητας των κανόνων (η σειρά εκτέλεσης των κανόνων ξεκινά από την κορυφή και καταλήγει στο τέλος της λίστας).

Κάντε κλικ στο εικονίδιο αναζήτησης επάνω δεξιά για να αναζητήσετε κανόνες κατά όνομα, πρωτόκολλο ή θύρα.

Προσθήκη ή επεξεργασία κανόνων τείχους προστασίας

Κάθε φορά που αλλάζουν οι παρακολουθούμενες παράμετροι απαιτείται τροποποίηση. Εάν πραγματοποιηθούν αλλαγές τέτοιες ώστε ένας κανόνας να μην εκπληρώνει τις συνθήκες και να μην είναι δυνατή η εφαρμογή της καθορισμένης ενέργειας, η δεδομένη σύνδεση ενδέχεται να απορριφθεί. Αυτό μπορεί να οδηγήσει σε προβλήματα με τη λειτουργία της εφαρμογής η οποία επηρεάζεται από κάποιον κανόνα. Ένα παράδειγμα είναι η αλλαγή της διεύθυνσης δικτύου ή του αριθμού θύρας της

απομακρυσμένης πλευράς.

> **Εικονογραφημένες οδηγίες**
> Τα ακόλουθα άρθρα της Γνωσιακής βάσης της ESET μπορεί να είναι διαθέσιμα μόνο στα Αγγλικά:
> • Άνοιγμα ή κλείσιμο (επιτρέπεται ή απορρίπτεται) μιας συγκεκριμένης θύρας στο τείχος προστασίας της ESET
> • Δημιουργία κανόνα τείχους προστασίας από τα αρχεία καταγραφής στο ESET Internet Security

Το επάνω μέρος του παραθύρου περιέχει τρεις καρτέλες:

• **Γενικά** – Καθορίστε ένα όνομα κανόνα, την κατεύθυνση της σύνδεσης, την ενέργεια (**Να επιτρέπεται**, **Να μην επιτρέπεται**, **Ερώτηση**), το πρωτόκολλο και το προφίλ στα οποία θα εφαρμόζεται ο κανόνας.

• **Τοπικά** – Εμφανίζει πληροφορίες σχετικά με την τοπική πλευρά της σύνδεσης, συμπεριλαμβανομένου του αριθμού της τοπικής θύρας ή του εύρους θυρών και του ονόματος της εφαρμογής επικοινωνίας. Επίσης σας επιτρέπει να προσθέσετε μια προκαθορισμένη ή δημιουργημένη ζώνη με εύρος διευθύνσεων IP εδώ, κάνοντας κλικ στο στοιχείο **Προσθήκη**.

• **Απομακρυσμένα** – Αυτή η καρτέλα περιέχει πληροφορίες σχετικά με την απομακρυσμένη θύρα (εύρος θυρών). Σας επιτρέπει να καθορίσετε μια λίστα απομακρυσμένων διευθύνσεων IP ή ζωνών για έναν συγκεκριμένο κανόνα. Επίσης, μπορείτε να προσθέσετε μια προκαθορισμένη ή δημιουργημένη ζώνη με εύρος διευθύνσεων IP εδώ, κάνοντας κλικ στο στοιχείο **Προσθήκη**.

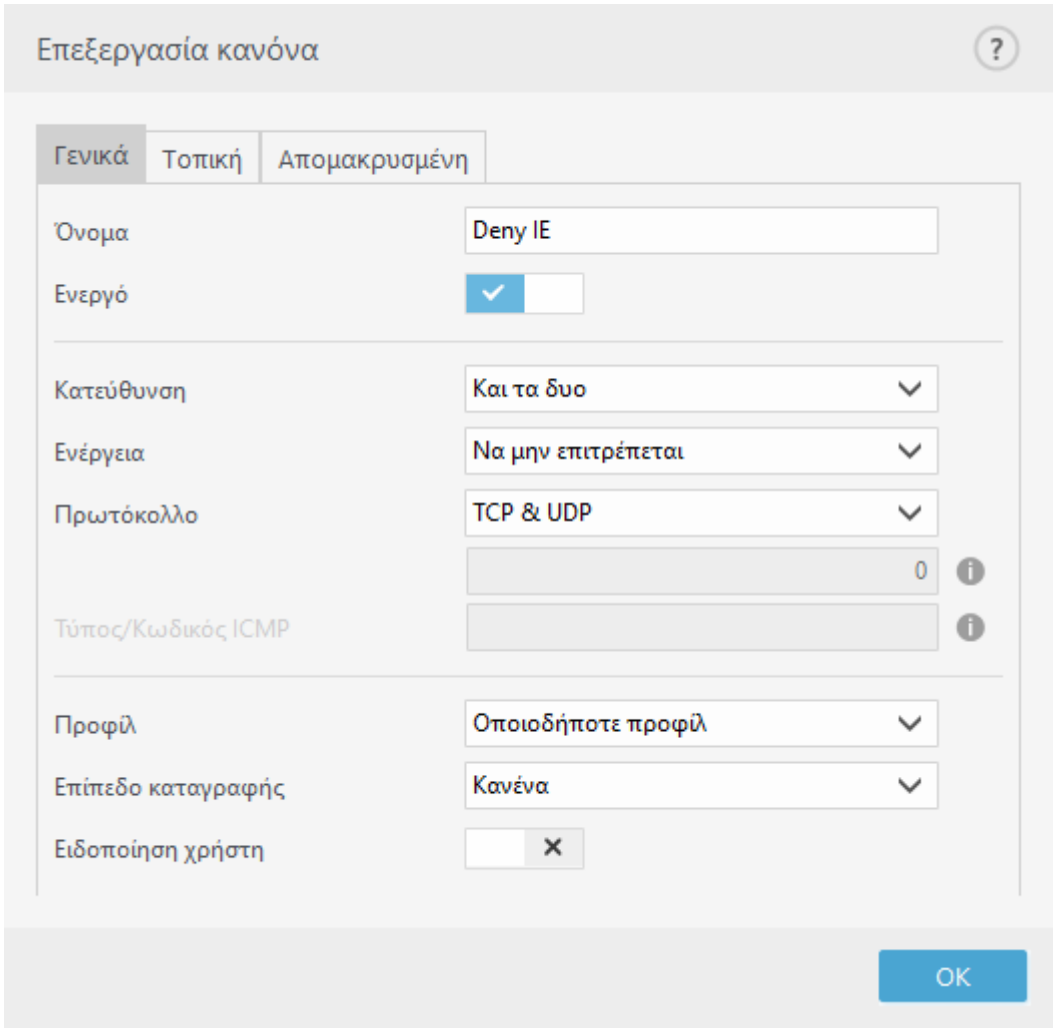
Όταν δημιουργείτε έναν νέο κανόνα, πρέπει να εισαγάγετε ένα όνομα για τον κανόνα στο πεδίο **Όνομα**. Επιλέξτε την κατεύθυνση στην οποία εφαρμόζεται ο κανόνας από το αναπτυσσόμενο μενού **Κατεύθυνση** και την ενέργεια που θα εκτελείται όταν η επικοινωνία πληροί τον κανόνα από το αναπτυσσόμενο μενού **Ενέργεια**.

Το **Πρωτόκολλο** αντιπροσωπεύει το πρωτόκολλο μεταφοράς που χρησιμοποιείται για τον κανόνα. Επιλέξτε από το αναπτυσσόμενο μενού το πρωτόκολλο που θα χρησιμοποιείται για έναν δεδομένα κανόνα.

Ο **Τύπος/Κωδικός ICMP** αντιπροσωπεύει ένα μήνυμα ICMP που προσδιορίζεται από έναν αριθμό (για παράδειγμα, το 0 αναπαριστά την "Απάντηση ηχούς").

Όλοι οι κανόνες ενεργοποιούνται για **Οποιοδήποτε προφίλ** από προεπιλογή. Εναλλακτικά, επιλέξτε ένα προσαρμοσμένο προφίλ firewall χρησιμοποιώντας το αναπτυσσόμενο μενού **Προφίλ**.

Εάν ενεργοποιήσετε το στοιχείο **Καταγραφή κρισιμότητας:**, η δραστηριότητα που συνδέεται με τον κανόνα θα καταγράφεται σε ένα αρχείο καταγραφής. Η **Ειδοποίηση χρήστη** εμφανίζει μια ειδοποίηση όταν εφαρμόζεται ο κανόνας.



Δημιουργούμε έναν νέο κανόνα για να επιτρέψουμε στο πρόγραμμα περιήγησης Firefox την πρόσβαση στο Internet / σε ιστοσελίδες τοπικού δικτύου. Σε αυτό το παράδειγμα, πρέπει να ρυθμιστούν οι εξής παράμετροι:

1.Στην καρτέλα **Γενικά**, ενεργοποιήστε την εξερχόμενη επικοινωνία μέσω του πρωτοκόλλου TCP και UDP.

2.Κάντε κλικ στην καρτέλα **Τοπικός**.

3.Επιλέξτε τη διαδρομή αρχείου του προγράμματος περιήγησης που χρησιμοποιείται κάνοντας κλικ στο **...** (για παράδειγμα *C:\Program Files\Firefox\Firefox.exe*). ΜΗΝ εισαγάγετε το όνομα της εφαρμογής.

4.Στην καρτέλα **Απομακρυσμένη**, ενεργοποιήστε τους αριθμούς θύρας 80 και 443, εάν θέλετε να επιτρέπεται η τυπική περιήγηση στο διαδίκτυο.

Έχετε υπόψη ότι η δυνατότητα τροποποίησης προκαθορισμένων κανόνων είναι περιορισμένη.

Κανόνας τείχους προστασίας - Τοπικός

Καθορίστε το όνομα της τοπικής εφαρμογής και την τοπική θύρα στην οποία θα εφαρμοστεί ο κανόνας.

Θύρα – Αριθμοί τοπικής θύρας. Εάν δεν δοθούν αριθμοί, ο κανόνας θα εφαρμόζεται σε όλες τις θύρες. Προσθέστε μία μοναδική θύρα επικοινωνίας ή ένα εύρος θυρών επικοινωνίας.

IP – Σας επιτρέπει να προσθέσετε μια απομακρυσμένη διεύθυνση, εύρος διευθύνσεων ή υποδίκτυο στο

οποίο θα εφαρμοστεί ο κανόνας. Αν δεν δοθεί τιμή, ο κανόνας θα εφαρμόζεται για όλες τις επικοινωνίες.

Ζώνες – Λίστα των ζωνών που έχουν προστεθεί.

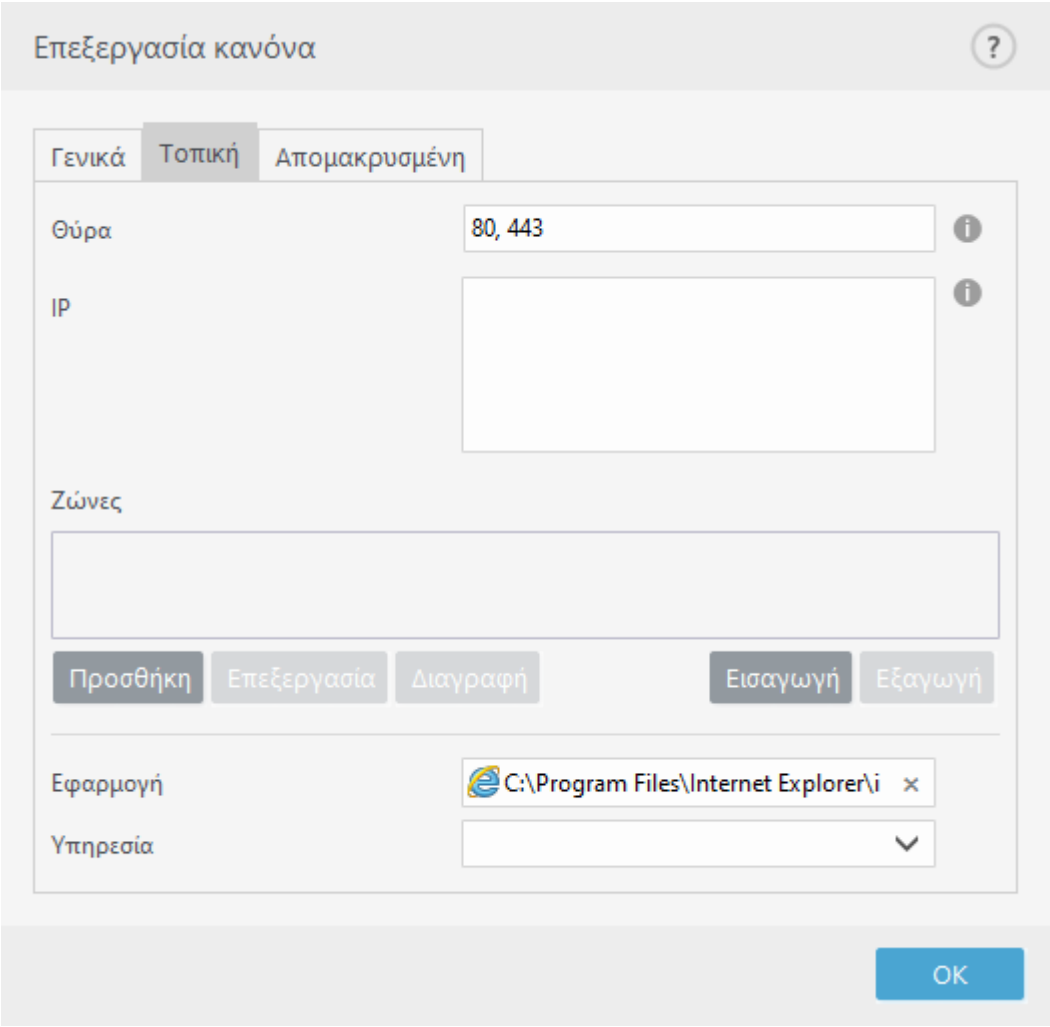
Προσθήκη – Προσθέστε μια δημιουργημένη ζώνη επιλέγοντάς την από το αναπτυσσόμενο μενού. Για να δημιουργήσετε μια ζώνη, χρησιμοποιήστε την καρτέλα Ρυθμίσεις ζώνης.

Κατάργηση – Αφαιρεί ζώνες από τη λίστα.

Εφαρμογή – Το όνομα της εφαρμογής στην οποία εφαρμόζεται ο κανόνας. Προσθέστε τη θέση της εφαρμογής στην οποία θα εφαρμόζεται ο κανόνας.

Υπηρεσία – Το αναπτυσσόμενο μενού εμφανίζει υπηρεσίες συστήματος.

> Μπορείτε να δημιουργήσετε έναν κανόνα για το είδωλό σας ο οποίος να παρέχει ενημερώσεις μέσω της θύρας 2221, επιλέγοντας για επικοινωνία την υπηρεσία EHttpSrv στο αναπτυσσόμενο μενού.



Κανόνας τείχους προστασίας -

Απομακρυσμένος

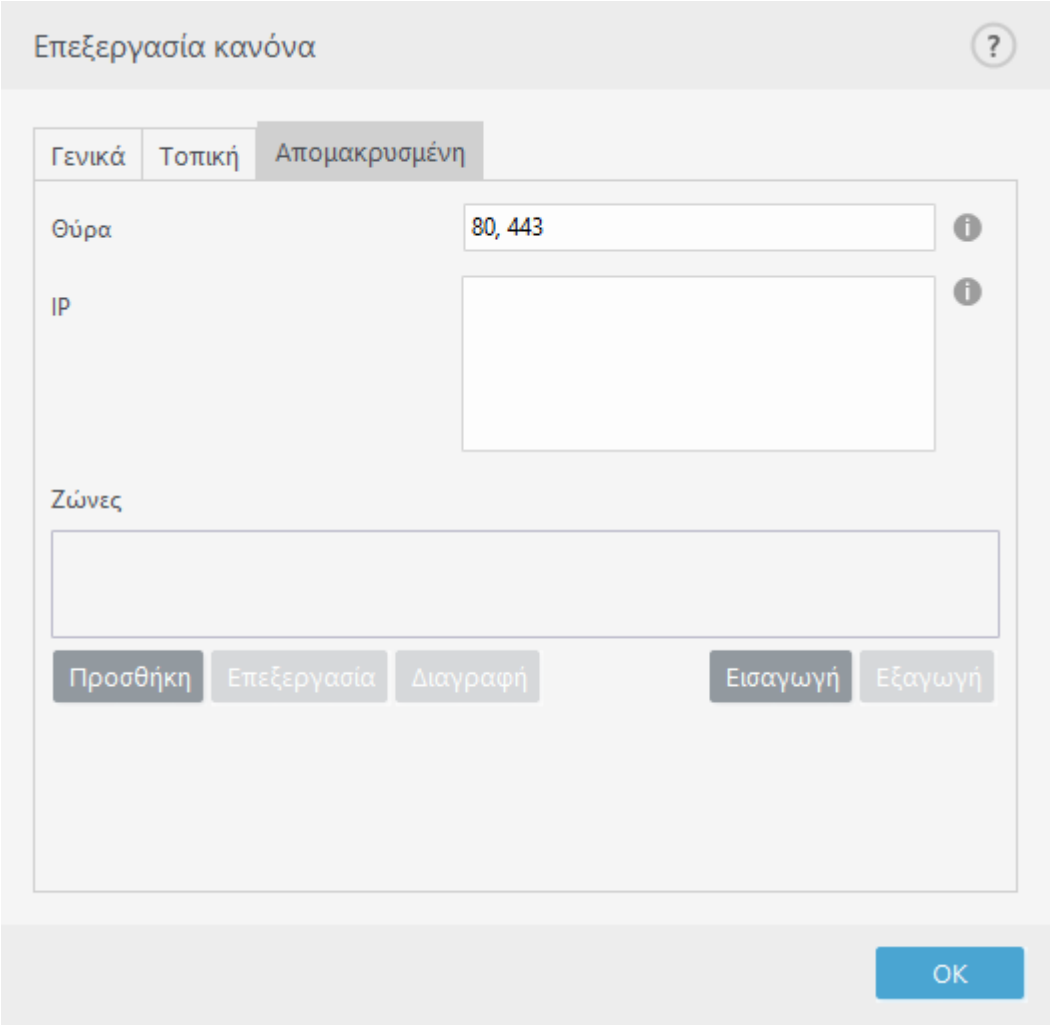
Θύρα – Αριθμοί απομακρυσμένης θύρας. Εάν δεν δοθούν αριθμοί, ο κανόνας θα εφαρμόζεται σε όλες τις θύρες. Προσθέστε μία μοναδική θύρα επικοινωνίας ή ένα εύρος θυρών επικοινωνίας.

IP – Σας επιτρέπει να προσθέσετε μια απομακρυσμένη διεύθυνση, εύρος διευθύνσεων ή υποδίκτυο. Η διεύθυνση, το εύρος/υποδίκτυο ή η απομακρυσμένη ζώνη στην οποία εφαρμόζεται ο κανόνας. Αν δεν δοθεί καμία τιμή, ο κανόνας θα εφαρμόζεται στο σύνολο της επικοινωνίας.

Ζώνες – Λίστα των ζωνών που έχουν προστεθεί.

Προσθήκη – Προσθέστε μια ζώνη επιλέγοντάς την από το αναπτυσσόμενο μενού. Για να δημιουργήσετε μια ζώνη, χρησιμοποιήστε την καρτέλα Ρυθμίσεις ζώνης.

Κατάργηση – Αφαιρεί ζώνες από τη λίστα.



Ανίχνευση τροποποίησης εφαρμογών

Η δυνατότητα ανίχνευσης τροποποίησης εφαρμογής εμφανίζει ειδοποιήσεις εάν τροποποιημένες εφαρμογές, για τις οποίες υπάρχει κανόνας τείχους προστασίας, προσπαθήσουν να δημιουργήσουν συνδέσεις. Η τροποποίηση της εφαρμογής είναι ένας μηχανισμός προσωρινής ή μόνιμης αντικατάστασης μιας αρχικής εφαρμογής από άλλη εφαρμογή με διαφορετικό εκτελέσιμο αρχείο

(προστατεύει από την κατάχρηση των κανόνων τείχους προστασίας).

Έχετε υπόψη ότι αυτή η δυνατότητα δεν έχει σκοπό να ανιχνεύει τροποποιήσεις σε οποιαδήποτε εφαρμογή γενικά. Σκοπός της είναι να αποτρέπει την κατάχρηση υφιστάμενων κανόνων του τείχος προστασίας και παρακολουθεί μόνο εφαρμογές για τις οποίες υφίστανται συγκεκριμένοι κανόνες του τείχος προστασίας.

Ενεργοποίηση ανίχνευσης τροποποιήσεων εφαρμογών – Εάν επιλεγεί, το πρόγραμμα θα παρακολουθεί τις εφαρμογές για αλλαγές (ενημερώσεις, μολύνσεις, άλλες τροποποιήσεις). Όταν μια τροποποιημένη εφαρμογή προσπαθήσει να δημιουργήσει μια σύνδεση, θα ειδοποιηθείτε από το Firewall.

Να επιτρέπεται τροποποίηση υπογεγραμμένων (αξιόπιστων) εφαρμογών – Δεν θα λαμβάνετε ειδοποίηση, εάν η εφαρμογή έχει την ίδια έγκυρη ψηφιακή υπογραφή πριν και μετά την τροποποίηση.

Λίστα εφαρμογών που εξαιρούνται από την ανίχνευση – Αυτό το παράθυρο σάς επιτρέπει να προσθέσετε ή να καταργήσετε μεμονωμένες εφαρμογές για τις οποίες επιτρέπονται τροποποιήσεις χωρίς ειδοποίηση.

Λίστα εφαρμογών που εξαιρούνται από την ανίχνευση

Το τείχος προστασίας στο ESET Internet Security ανιχνεύει αλλαγές σε εφαρμογές για τις οποίες υπάρχουν κανόνες (δείτε την ενότητα Ανίχνευση τροποποίησης εφαρμογών).

Σε ορισμένες περιπτώσεις είναι δυνατό να μη θέλετε να χρησιμοποιήσετε αυτήν τη λειτουργικότητα για κάποιες εφαρμογές, εάν θέλετε να τις εξαιρέσετε από τον έλεγχο με το τείχος προστασίας.

Προσθήκη – Ανοίγει ένα παράθυρο στο οποίο μπορείτε να επιλέξετε μια εφαρμογή για να την προσθέσετε στη λίστα εφαρμογών που εξαιρούνται από την ανίχνευση τροποποίησης. Μπορείτε να επιλέξετε από μια λίστα εφαρμογών που εκτελούνται με ανοιχτή επικοινωνία δικτύου για την οποία υπάρχει κανόνας τείχους προστασίας ή να προσθέσετε μια συγκεκριμένη εφαρμογή.

Επεξεργασία – Ανοίγει ένα παράθυρο στο οποίο μπορείτε να αλλάξετε την τοποθεσία μιας εφαρμογής, η οποία βρίσκεται στη λίστα εφαρμογών που εξαιρούνται από την ανίχνευση τροποποίησης. Μπορείτε να επιλέξετε από μια λίστα εφαρμογών που εκτελούνται με ανοιχτή επικοινωνία δικτύου για την οποία υπάρχει κανόνας τείχους προστασίας ή να αλλάξετε την τοποθεσία μη αυτόματα.

Κατάργηση – Καταργεί καταχωρίσεις από τη λίστα εφαρμογών που εξαιρούνται από την ανίχνευση τροποποίησης.

Ρυθμίσεις λειτουργίας εκμάθησης

Η Λειτουργία εκμάθησης δημιουργεί και αποθηκεύει αυτόματα έναν κανόνα για κάθε επικοινωνία που έχει δημιουργηθεί στο σύστημα. Δεν απαιτείται αλληλεπίδραση του χρήστη επειδή το ESET Internet Security αποθηκεύει τους κανόνες σύμφωνα με τις προκαθορισμένες παραμέτρους.

Η λειτουργία αυτή μπορεί να εκθέσει το σύστημά σας σε κίνδυνο και συνιστάται μόνο για την αρχική

διαμόρφωση του Firewall.

Επιλέξτε **Λειτουργία εκμάθησης** από το αναπτυσσόμενο μενού στη διαδρομή **Ρυθμίσεις για προχωρημένους**(F5) > **Firewall** > **Βασικές λειτουργίες** > **Λειτουργία φιλτραρίσματος** για να ενεργοποιήσετε τις **Επιλογές λειτουργίας εκμάθησης**. Η ενότητα αυτή περιλαμβάνει τα παρακάτω στοιχεία:

> ⚠ Όταν βρίσκεστε στη Λειτουργία εκμάθησης, το Firewall δεν φιλτράρει την επικοινωνία. Επιτρέπονται όλες οι εξερχόμενες και εισερχόμενες επικοινωνίες. Σε αυτή τη λειτουργία, ο υπολογιστής δεν προστατεύεται πλήρως από το Firewall.

Η λειτουργία καθορίζεται μετά τη λήξη της λειτουργίας εκμάθησης – Καθορίστε τη λειτουργία φιλτραρίσματος στην οποία θα επιστρέφει το Τείχος προστασίας του ESET Internet Security μετά το τέλος του χρονικού διαστήματος για τη λειτουργία εκμάθησης. Διαβάστε περισσότερα για τις λειτουργίες φιλτραρίσματος. Μετά τη λήξη λειτουργίας, η επιλογή **Ερώτηση στο χρήστη** απαιτεί δικαιώματα διαχειριστή για να εκτελεστεί μια αλλαγή στη λειτουργία φιλτραρίσματος του τείχους προστασίας.

Τύπος επικοινωνίας – Επιλέξτε ειδικές παραμέτρους δημιουργίας κανόνων για κάθε τύπο επικοινωνίας. Υπάρχουν τέσσερις τύποι επικοινωνίας:

Εισερχόμενη κυκλοφορία από τη Ζώνη αξιοπιστίας – Ένα παράδειγμα εισερχόμενης σύνδεσης από τη ζώνη αξιοπιστίας είναι ένας απομακρυσμένος υπολογιστής της ζώνης αξιοπιστίας που προσπαθεί να δημιουργήσει επικοινωνία με μια τοπική εφαρμογή που εκτελείται στον υπολογιστή σας.

Εξερχόμενη κυκλοφορία προς τη Ζώνη αξιοπιστίας – Μια τοπική εφαρμογή που προσπαθεί να δημιουργήσει σύνδεση με άλλον υπολογιστή της ζώνης αξιοπιστίας.

Εισερχόμενη κυκλοφορία διαδικτύου – Ένας απομακρυσμένος υπολογιστής προσπαθεί να επικοινωνήσει με μια εφαρμογή που εκτελείται στον υπολογιστή.

Εξερχόμενη κυκλοφορία διαδικτύου – Μια τοπική εφαρμογή προσπαθεί να δημιουργήσει σύνδεση με άλλον υπολογιστή.

Κάθε ενότητα σάς επιτρέπει να καθορίσετε παραμέτρους που θα προστεθούν σε κανόνες που δημιουργήθηκαν πρόσφατα:

Προσθήκη τοπικής θύρας – Περιλαμβάνει τον αριθμό τοπικής θύρας της επικοινωνίας δικτύου. Για εξερχόμενες επικοινωνίες δημιουργούνται συνήθως τυχαίοι αριθμοί. Για αυτό τον λόγο, συνιστάται να ενεργοποιείται αυτή η επιλογή μόνο για εισερχόμενες επικοινωνίες.

Προσθήκη εφαρμογής – Περιλαμβάνει το όνομα της τοπικής εφαρμογής. Η επιλογή αυτή είναι κατάλληλη για μελλοντικούς κανόνες επιπέδου εφαρμογής (κανόνες που καθορίζουν την επικοινωνία για μια ολόκληρη εφαρμογή). Για παράδειγμα, μπορείτε να ενεργοποιήσετε την επικοινωνία μόνο για ένα πρόγραμμα περιήγησης ή πρόγραμμα-πελάτη ηλεκτρονικής αλληλογραφίας.

Προσθήκη απομακρυσμένης θύρας – Περιλαμβάνει τον αριθμό απομακρυσμένης θύρας της επικοινωνίας δικτύου. Για παράδειγμα, μπορείτε να επιτρέπετε ή να μην επιτρέπετε μια συγκεκριμένη υπηρεσία που συσχετίζεται με έναν αριθμό τυπικής θύρας (HTTP – 80, POP3 – 110, κ.λπ.).

Προσθήκη απομακρυσμένης διεύθυνσης IP/Ζώνης αξιοπιστίας – Μια απομακρυσμένη

διεύθυνση IP ή ζώνη μπορεί να χρησιμοποιηθεί ως παράμετρος για νέους κανόνες που καθορίζουν όλες τις συνδέσεις δικτύου μεταξύ του τοπικού συστήματος και της συγκεκριμένης απομακρυσμένης διεύθυνσης/ζώνης. Η επιλογή αυτή είναι κατάλληλη αν θέλετε να ορίσετε ενέργειες για έναν συγκεκριμένο υπολογιστή ή ομάδα δικτυωμένων υπολογιστών.

Μέγιστος αριθμός διαφορετικών κανόνων για μια εφαρμογή – Αν μια εφαρμογή επικοινωνεί μέσω διαφορετικών θυρών με διάφορες διευθύνσεις IP, κ.λπ., το τείχος προστασίας σε λειτουργία εκμάθησης δημιουργεί το κατάλληλο πλήθος κανόνων για αυτή την εφαρμογή. Η επιλογή αυτή σάς επιτρέπει να περιορίζετε τον αριθμό κανόνων που μπορούν να δημιουργηθούν για μία εφαρμογή.

Προστασία από επιθέσεις δικτύου (IDS)

Η Προστασία από επιθέσεις δικτύου (IDS) βελτιώνει την ανίχνευση των καταχρήσεων για γνωστά τρωτά σημεία. Διαβάστε περισσότερα σχετικά με την Προστασία από επιθέσεις δικτύου στο γλωσσάρι.

Προστασία από επιθέσεις δικτύου (IDS) – Αναλύει το περιεχόμενο κυκλοφορίας δικτύου και προστατεύει από επιθέσεις δικτύου. Οποιαδήποτε κυκλοφορία θεωρείται βλαβερή θα αποκλείεται.

Ενεργοποίηση Προστασίας botnet – Ανιχνεύει και αποκλείει την επικοινωνία με κακόβουλους διακομιστές ελέγχου βάσει τυπικών μοτίβων, όταν ο υπολογιστής μολυνθεί και κάποιο bot επιχειρήσει να επικοινωνήσει μαζί του. Διαβάστε περισσότερα σχετικά με την Προστασία από botnet δικτύου στο γλωσσάρι.

Κανόνες IDS – Αυτή η επιλογή σας επιτρέπει να διαμορφώσετε σύνθετες επιλογές φιλτραρίσματος για την ανίχνευση πολλών τύπων εισβολών και καταχρήσεων οι οποίες θα μπορούσαν να χρησιμοποιηθούν για να βλάψουν τον υπολογιστή σας.

> **Εικονογραφημένες οδηγίες**
> Τα ακόλουθα άρθρα της Γνωσιακής βάσης της ESET μπορεί να είναι διαθέσιμα μόνο στα Αγγλικά:
> - Να εξαιρείται μια διεύθυνση IP από το IDS στο ESET Internet Security

Όλα τα σημαντικά συμβάντα που ανιχνεύονται από την προστασία δικτύου αποθηκεύονται σε ένα αρχείο καταγραφής. Για περισσότερες πληροφορίες, δείτε το αρχείο καταγραφής προστασίας δικτύου.

Προστασία από επιθέσεις

Η Προστασία από επιθέσεις εξαντλητικής δοκιμής κωδικών αποκλείει τις επιθέσεις με δοκιμές του κωδικού πρόσβασης για υπηρεσίες RDP και SMB. Η επίθεση εξαντλητικής δοκιμής κωδικών είναι μια μέθοδος ανακάλυψης ενός στοχευμένου κωδικού πρόσβασης με συστηματικές δοκιμές όλων των συνδυασμών γραμμάτων, αριθμών και συμβόλων. Για να ρυθμίσετε τις παραμέτρους της Προστασίας από επιθέσεις εξαντλητικής δοκιμής κωδικών, στο κύριο παράθυρο του προγράμματος, κάντε κλικ στα στοιχεία **Ρυθμίσεις** > **Ρυθμίσεις για προχωρημένους** (F5) > **Προστασία δικτύου** > **Προστασία δικτύου από επιθέσεις** > **Προστασία από επιθέσεις εξαντλητικής δοκιμής κωδικών**.

Ενεργοποίηση της προστασίας από επιθέσεις εξαντλητικής δοκιμής κωδικών – Το ESET

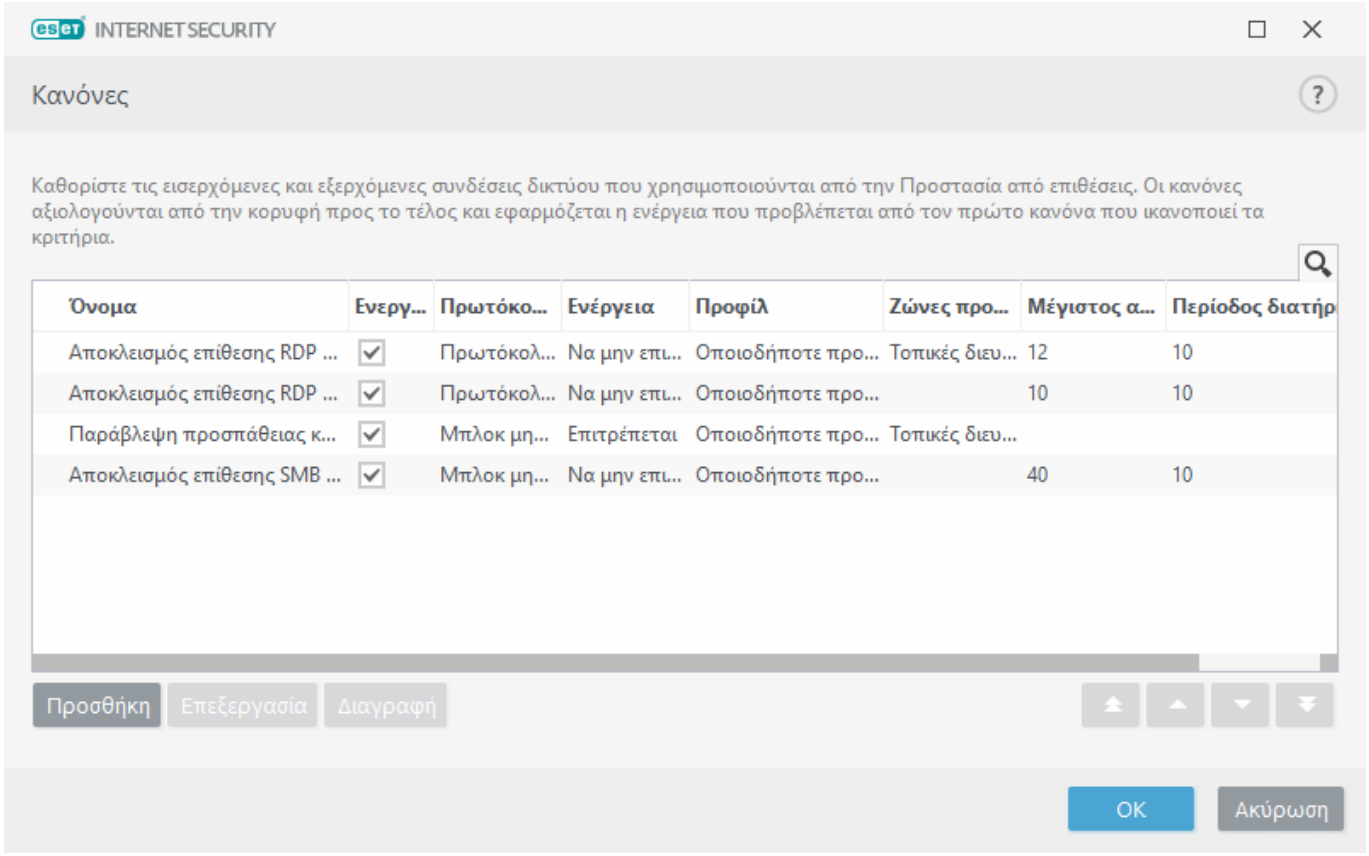
Internet Security ελέγχει το περιεχόμενο της δικτυακής κίνησης και αποκλείει τις προσπάθειες επιθέσεων με δοκιμές κωδικού πρόσβασης.

Κανόνες – Σας επιτρέπουν να δημιουργείτε, να επεξεργάζεστε και να προβάλλετε κανόνες για εισερχόμενες και εξερχόμενες συνδέσεις δικτύου. Για περισσότερες πληροφορίες, ανατρέξτε στο κεφάλαιο Κανόνες.

Κανόνες

Οι κανόνες Προστασίας από επιθέσεις εξαντλητικής δοκιμής κωδικών σάς επιτρέπουν να δημιουργείτε, να επεξεργάζεστε και να προβάλλετε κανόνες για εισερχόμενες και εξερχόμενες συνδέσεις δικτύου. Δεν είναι δυνατή η επεξεργασία ή η κατάργηση των προκαθορισμένων κανόνων.

Διαχείριση κανόνων για προστασία από επίθεση εξαντλητικής δοκιμής κωδικών



Προσθήκη – Δημιουργεί νέο κανόνα.

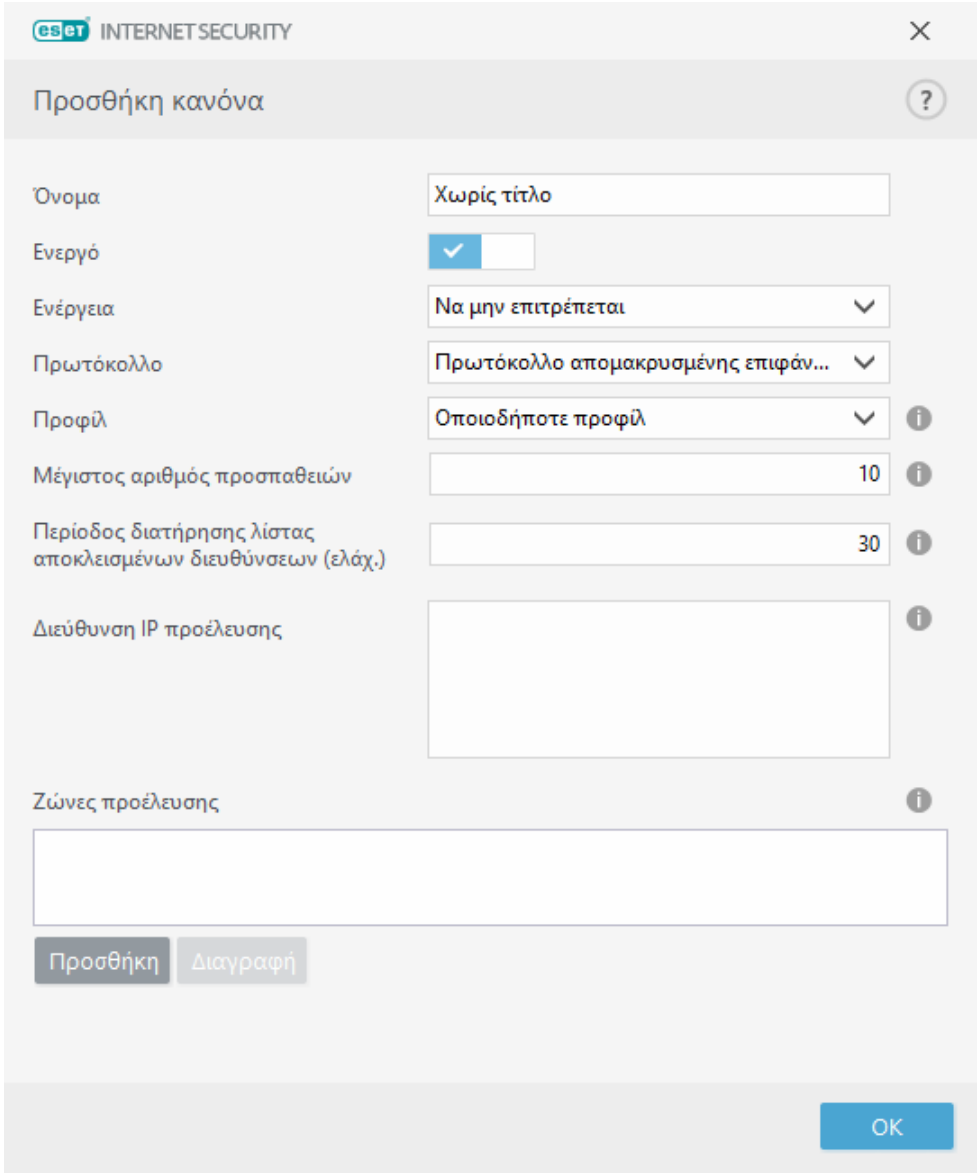
Επεξεργασία – Επεξεργασία ενός υπάρχοντος κανόνα.

Κατάργηση – Κατάργηση ενός υπάρχοντος κανόνα από τη λίστα κανόνων.

Κορυφή/Επάνω/Κάτω/Τέλος – Προσαρμόστε το επίπεδο προτεραιότητας των κανόνων.

Για να διασφαλιστεί η υψηλότερη δυνατή προστασία, εφαρμόζεται ο κανόνας αποκλεισμού με τη χαμηλότερη τιμή για το στοιχείο **Μέγιστος αριθμός προσπαθειών**, ακόμη και αν ο κανόνας βρίσκεται σε χαμηλότερο επίπεδο στη λίστα κανόνων όταν πολλοί κανόνες αποκλεισμού αντιστοιχούν στις συνθήκες ανίχνευσης.

Επεξεργαστής κανόνων



Όνομα – Το όνομα του κανόνα.

Ενεργός – Απενεργοποιήστε αυτό το ρυθμιστικό εάν θέλετε να διατηρηθεί ο κανόνας στη λίστα αλλά να μην εφαρμόζεται.

Ενέργεια – Επιλέξτε **Δεν επιτρέπεται** ή **Επιτρέπεται** για τη σύνδεση εάν πληρούνται οι ρυθμίσεις κανόνα.

Πρωτόκολλο – Το πρωτόκολλο επικοινωνίας που θα ελέγχει αυτός ο κανόνας.

Προφίλ – Για συγκεκριμένα προφίλ μπορούν να ρυθμιστούν και να εφαρμοστούν προσαρμοσμένοι κανόνες.

Μέγιστος αριθμός προσπαθειών - Ο μέγιστος αριθμός προσπαθειών επανάληψης επίθεσης που

επιτρέπεται μέχρι να αποκλειστεί η διεύθυνση IP και να προστεθεί στη Λίστα αποκλεισμένων διευθύνσεων.

Περίοδος διατήρησης λίστας αποκλεισμένων διευθύνσεων (ελάχ.) – Ρυθμίζει την ώρα κατά την οποία αφαιρείται η διεύθυνση από τη λίστα αποκλεισμένων διευθύνσεων. Η χρονική περίοδος που χρησιμοποιείται για την καταμέτρηση του αριθμού προσπαθειών έχει προκαθοριστεί σε 30 λεπτά από προεπιλογή.

Διεύθυνση IP προέλευσης – Μια λίστα με διευθύνσεις IP / εύρη / υποδίκτυα. Οι πολλαπλές διευθύνσεις πρέπει να διαχωρίζονται με κόμμα.

Ζώνες προέλευσης – Σας επιτρέπουν να προσθέσετε εδώ μια προκαθορισμένη ή δημιουργημένη ζώνη με ένα εύρος διευθύνσεων IP, κάνοντας κλικ στο στοιχείο **Προσθήκη**.

IDS κανόνες

Σε ορισμένες περιπτώσεις η Υπηρεσία ανίχνευσης εισβολής (IDS) μπορεί να ανιχνεύσει την επικοινωνία μεταξύ των δρομολογητών ή άλλων εσωτερικών συσκευών δικτύωσης ως ενδεχόμενη επίθεση. Για παράδειγμα, μπορείτε να προσθέσετε τη γνωστή ασφαλή διεύθυνση στη ζώνη «Εξαίρεση διευθύνσεων από το IDS» για να παρακάμψετε το IDS.

> **Εικονογραφημένες οδηγίες**
> Τα ακόλουθα άρθρα της Γνωσιακής βάσης της ESET μπορεί να είναι διαθέσιμα μόνο στα Αγγλικά:
> - Να εξαιρείται μια διεύθυνση IP από το IDS στο ESET Internet Security

Στήλες

- **Ανίχνευση** – Τύπος ανίχνευσης.

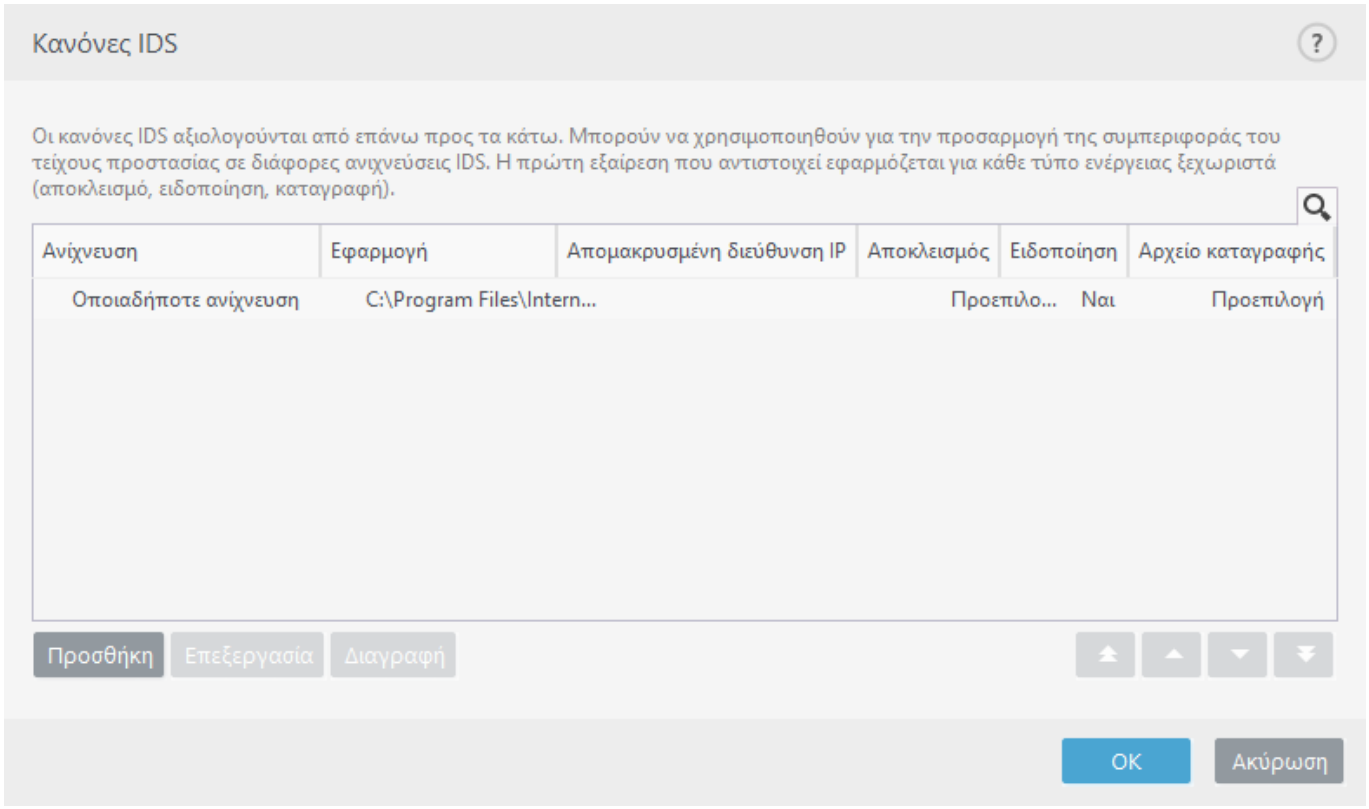
- **Εφαρμογή** – Επιλέξτε τη διαδρομή αρχείου μιας εξαιρούμενης εφαρμογής κάνοντας κλικ στο ... (για παράδειγμα C:\Program Files\Firefox\Firefox.exe). ΜΗΝ εισαγάγετε το όνομα της εφαρμογής.

- **Απομακρυσμένη IP** – Λίστα απομακρυσμένων διευθύνσεων / εύρους / υποδικτύων IPv4 ή IPv6. Οι πολλαπλές διευθύνσεις πρέπει να διαχωρίζονται με κόμμα.

- **Αποκλεισμός** – Κάθε διεργασία του συστήματος έχει τη δική της προεπιλεγμένη συμπεριφορά και αντιστοιχισμένη ενέργεια (αποκλεισμός ή αποδοχή). Για να παρακάμψετε την προεπιλεγμένη συμπεριφορά για το ESET Internet Security, μπορείτε να επιλέξετε εάν θα αποκλείεται ή θα επιτρέπεται, χρησιμοποιώντας το αναπτυσσόμενο μενού.

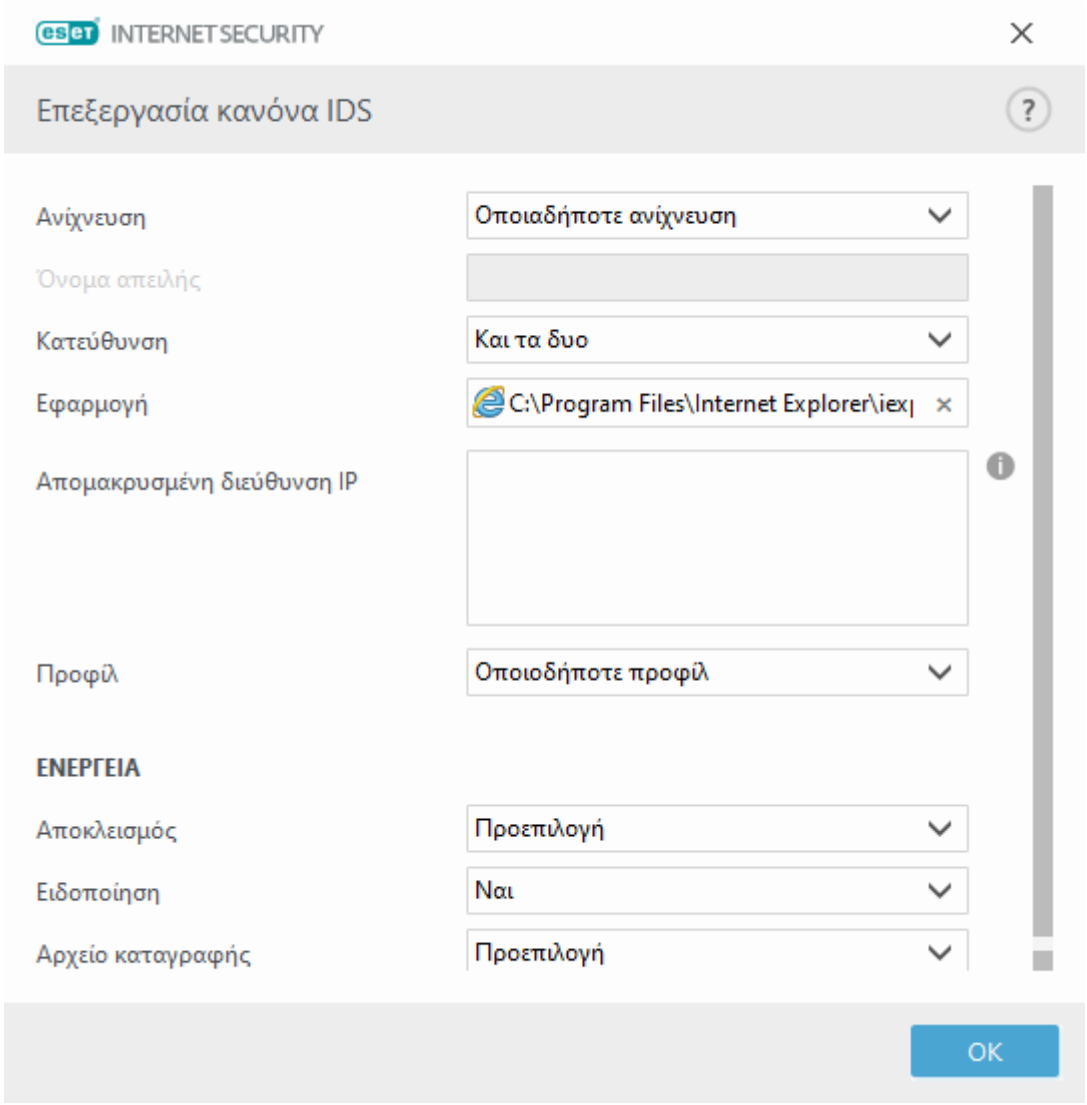
- **Ειδοποίηση** – Επιλέξτε εάν θα εμφανίζονται Ειδοποιήσεις επιφάνειας εργασίας στον υπολογιστή σας. Επιλέξτε από τις τιμές **Προεπιλογή**/**Ναι**/**Όχι**.

- **Αρχείο καταγραφής** – Καταγράφονται συμβάντα στα αρχεία καταγραφής του ESET Internet Security. Επιλέξτε από τις τιμές **Προεπιλογή**/**Ναι**/**Όχι**.



Διαχείριση κανόνων IDS

- **Προσθήκη** – Κάντε κλικ για να δημιουργήσετε έναν νέο κανόνα IDS.
- **Επεξεργασία** – Κάντε κλικ για να επεξεργαστείτε έναν υπάρχοντα κανόνα IDS.
- **Κατάργηση** – Επιλέξτε και κάντε κλικ εάν θέλετε να καταργήσετε έναν κανόνα από τη λίστα κανόνων IDS.
- **Κορυφή/Επάνω/Κάτω/Τέλος** – Σας επιτρέπει να ρυθμίσετε το επίπεδο προτεραιότητας των κανόνων (οι κανόνες αξιολογούνται από την κορυφή προς το τέλος).



Εάν θέλετε να εμφανίζεται μια ειδοποίηση και να συλλέγεται ένα αρχείο καταγραφής οποτεδήποτε προκύπτει το συμβάν:

1.Κάντε κλικ στο στοιχείο **Προσθήκη** για να προσθέσετε έναν νέο κανόνα IDS.

2.Επιλέξτε μια συγκεκριμένη ανίχνευση από το αναπτυσσόμενο μενού **Ανίχνευση**.

3.Επιλέξτε μια διαδρομή εφαρμογής κάνοντας κλικ στο στοιχείο **...** στο οποίο θέλετε να εφαρμοστεί αυτή η ειδοποίηση.

4.Να παραμείνει η **προεπιλογή** στο αναπτυσσόμενο μενού του στοιχείου **Αποκλεισμός**. Με αυτό τον τρόπο θα μεταφερθεί η προεπιλεγμένη ενέργεια που εφαρμόζεται στο ESET Internet Security.

5.Ρυθμίστε και τα δύο αναπτυσσόμενα μενού του στοιχείου **Ειδοποίηση** και **Καταγραφή** σε **Ναι**.

6.Κάντε κλικ στο στοιχείο **OK** για να αποθηκεύσετε αυτή την ειδοποίηση.

Εάν δεν θέλετε να εμφανίζεται μια επαναλαμβανόμενη ειδοποίηση, την οποία δεν θεωρείτε απειλή και είναι **Ανίχνευση** συγκεκριμένου τύπου:
1.Κάντε κλικ στο στοιχείο **Προσθήκη** για να προσθέσετε έναν νέο κανόνα IDS.
2.Επιλέξτε μια συγκεκριμένη ανίχνευση από το αναπτυσσόμενο μενού **Ανίχνευση**, για παράδειγμα **Περίοδος λειτουργίας SMB χωρίς επεκτάσεις ασφαλείας επίθεση σάρωσης θύρας TCP**.
3.Επιλέξτε **Εισερχόμενη επικοινωνία** από το αναπτυσσόμενο μενού κατεύθυνσης σε περίπτωση που προέρχεται από εισερχόμενη επικοινωνία.
4.Ρυθμίστε το αναπτυσσόμενο μενού **Ειδοποίηση** σε **Όχι**.
5.Ρυθμίστε το αναπτυσσόμενο μενού **Καταγραφή** σε **Ναι**.
6.Αφήστε το στοιχείο **Εφαρμογή** κενό.
7.Εάν η επικοινωνία δεν προέρχεται από μια συγκεκριμένη διεύθυνση IP, αφήστε το στοιχείο**Απομακρυσμένη διεύθυνση IP** κενό.
8.Κάντε κλικ στο στοιχείο **OK** για να αποθηκεύσετε αυτή την ειδοποίηση.

Αποκλείστηκε ύποπτη απειλή

Αυτή η περίπτωση μπορεί να συμβεί όταν κάποια εφαρμογή στον υπολογιστή σας προσπαθεί να μεταδώσει κακόβουλη κυκλοφορία σε άλλον υπολογιστή στο δίκτυο, εκμεταλλευόμενη ένα κενό ασφαλείας, ή ακόμη κι όταν ανιχνεύεται απόπειρα σάρωσης θυρών στο σύστημά σας.

Απειλή – Όνομα της απειλής.

Απομακρυσμένη διεύθυνση – Απομακρυσμένη διεύθυνση IP.

Επιτρέπεται – Δημιουργεί έναν κανόνα Υπηρεσίας ανίχνευσης εισβολής (IDS) χωρίς καμιά προκαθορισμένη ενέργεια για κάθε τύπο ενέργειας (αποκλεισμός, ειδοποίηση, καταγραφή).

Συνέχεια αποκλεισμού – Αποκλείει την ανιχνευμένη απειλή. Για να δημιουργήσετε έναν κανόνα IDS για αυτήν την απειλή, επιλέξτε το πλαίσιο ελέγχου **Να μην ειδοποιηθώ ξανά** και ο κανόνας θα προστεθεί χωρίς ειδοποίηση και καταγραφή.

Οι πληροφορίες που εμφανίζονται σε αυτό το παράθυρο ειδοποίησης μπορεί να διαφέρουν ανάλογα με τον τύπο της ανιχνευμένης απειλής.
Για περισσότερες πληροφορίες σχετικά με απειλές και άλλους σχετικούς όρους, ανατρέξτε στην ενότητα Τύποι απομακρυσμένων επιθέσεων ή Τύποι ανιχνεύσεων.
Για να επιλύσετε το συμβάν **Διπλότυπες διευθύνσεις IP στο δίκτυο**, ανατρέξτε στο άρθρο της Γνωσιακής βάσης της ESET.

Αντιμετώπιση προβλημάτων προστασίας δικτύου

Ο Οδηγός επίλυσης προβλημάτων σάς βοηθά να επιλύετε προβλήματα συνδεσιμότητας που προκαλούνται από το Firewall της ESET. Από το αναπτουσσόμενο μενού, επιλέξτε μια χρονική περίοδο κατά την οποία αποκλείστηκε κάποια επικοινωνία. Μια λίστα πρόσφατα αποκλεισμένων επικοινωνιών σάς παρέχει μια επισκόπηση σχετικά με τον τύπο της εφαρμογής ή της συσκευής, τη φήμη και τον συνολικό αριθμό εφαρμογών και συσκευών που αποκλείστηκαν κατά τη συγκεκριμένη χρονική περίοδο. Για περισσότερες πληροφορίες σχετικά με τος αποκλεισμό επικοινωνιών, κάντε κλικ στο στοιχείο **Λεπτομέρειες**. Το επόμενο βήμα είναι να καταργήσετε τον αποκλεισμό της εφαρμογής ή

της συσκευής στην οποία αντιμετωπίζετε προβλήματα συνδεσιμότητας.

Όταν κάνετε κλικ στο κουμπί **Κατάργηση αποκλεισμού**, θα επιτρέπεται η επικοινωνία που αποκλειόταν προηγουμένως. Εάν συνεχίζετε να αντιμετωπίζετε προβλήματα με μια εφαρμογή, ή εάν η συσκευή σας δεν λειτουργεί με τον αναμενόμενο τρόπο, κάντε κλικ στην επιλογή **Η εφαρμογή εξακολουθεί να μη λειτουργεί** και θα επιτρέπονται πλέον όλες οι επικοινωνίες που προηγουμένως αποκλείονταν για αυτήν τη συσκευή. Εάν το πρόβλημα παραμένει, επανεκκινήστε τον υπολογιστή.

Κάντε κλικ στο στοιχείο **Εμφάνιση αλλαγών** για να δείτε τους κανόνες που δημιουργήθηκαν από τον οδηγό. Επιπλέον, μπορείτε να δείτε κανόνες που δημιουργήθηκαν από τον οδηγό **Εγκατάσταση για προχωρημένους** > **Προστασία δικτύου** > **Τείχος προστασίας** > **Ρυθμίσεις για προχωρημένους** > **Κανόνες**.

Κάντε κλικ στην επιλογή **Κατάργηση αποκλεισμού άλλου** για να επιλύσετε ζητήματα επικοινωνίας με άλλες συσκευές ή εφαρμογές.

Επιτρεπτές υπηρεσίες και επιλογές για προχωρημένους

Οι επιλογές για προχωρημένους στις ενότητες Τείχος προστασίας και Προστασία από επιθέσεις δικτύου σάς επιτρέπουν να ρυθμίσετε τις παραμέτρους πρόσβασης σε ορισμένες από τις υπηρεσίες που εκτελούνται στον υπολογιστή σας από τη ζώνη αξιοπιστίας.

Μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε την ανίχνευση διαφόρων τύπων επιθέσεων και εκμεταλλεύσεων που ενδέχεται να βλάψουν τον υπολογιστή σας.

Σε ορισμένες περιπτώσεις δεν θα λάβετε ειδοποίηση απειλής για επικοινωνίες που έχουν αποκλειστεί. Συμβουλευτείτε την ενότητα Καταγραφή και δημιουργία κανόνων ή εξαιρέσεων από το αρχείο καταγραφής για οδηγίες σχετικά με την προβολή όλων των αποκλεισμένων επικοινωνιών στο αρχείο καταγραφής του τείχος προστασίας.

Η διαθεσιμότητα συγκεκριμένων επιλογών σε αυτό το παράθυρο μπορεί να διαφέρει ανάλογα με τον τύπο ή την έκδοση του προϊόντος ESET και τη μονάδα Firewall που διαθέτετε, καθώς και την έκδοση του λειτουργικού συστήματός σας.

Επιτρεπτές υπηρεσίες

Οι ρυθμίσεις σε αυτήν τη μονάδα έχουν στόχο να απλοποιήσουν τη διαμόρφωση της πρόσβασης στις υπηρεσίες αυτού του υπολογιστή από τη Ζώνη αξιοπιστίας. Πολλές από αυτές ενεργοποιούν ή απενεργοποιούν προκαθορισμένους κανόνες του τείχος προστασίας. Μπορείτε να επεξεργαστείτε τις επιτρεπτές υπηρεσίες στις **Ρυθμίσεις για προχωρημένους** (F5) > **Προστασία δικτύου** > **Τείχος προστασίας** > **Για προχωρημένους** > **Επιτρεπτές υπηρεσίες**.

- **Να επιτρέπεται η κοινή χρήση αρχείων και εκτυπωτών στη ζώνη αξιόπιστων τοποθεσιών** – Επιτρέπει σε απομακρυσμένους υπολογιστές στη ζώνη αξιοπιστίας να αποκτήσουν πρόσβαση στα αρχεία και τους εκτυπωτές κοινής χρήσης.

- **Να επιτρέπεται η δυνατότητα UPNP για υπηρεσίες συστήματος στη ζώνη αξιόπιστων τοποθεσιών** – Επιτρέπει εισερχόμενα και εξερχόμενα αιτήματα πρωτοκόλλων UPnP για υπηρεσίες συστήματος. Το UPnP (Η δυνατότητα Τοποθέτησης και Άμεσης Λειτουργίας (UPnP) γενικής χρήσης

είναι επίσης γνωστή ως Microsoft Network Discovery) χρησιμοποιείται σε λειτουργικά συστήματα Windows Vista και νεότερα.

- **Να επιτρέπεται η εισερχόμενηRPC επικοινωνία στη ζώνη αξιόπιστων τοποθεσιών** – Ενεργοποιεί συνδέσεις TCP από τη Ζώνη αξιοπιστίας, επιτρέποντας πρόσβαση στο MS RPC Portmapper και σε υπηρεσίες RPC/DCOM.

- **Να επιτρέπεται η σύνδεση απομακρυσμένης επιφάνειας εργασίας στη ζώνη αξιόπιστων τοποθεσιών** – Ενεργοποιεί συνδέσεις μέσω Πρωτοκόλλου απομακρυσμένης επιφάνειας εργασίας της Microsoft (RDP) και επιτρέπει σε υπολογιστές της Ζώνης αξιοπιστίας να αποκτήσουν πρόσβαση στον υπολογιστή σας χρησιμοποιώντας ένα πρόγραμμα που χρησιμοποιεί RDP (για παράδειγμα, Σύνδεση απομακρυσμένης επιφάνειας εργασίας).

- **Ενεργοποίηση σύνδεσης σε ομάδες πολλαπλών προορισμών (multicast) μέσω IGMP** – Επιτρέπει εισερχόμενες/εξερχόμενες ροές IGMP και εισερχόμενες ροές πολλαπλών διαύλων UDP, για παράδειγμα ροές βίντεο που δημιουργούνται από εφαρμογές που χρησιμοποιούν το πρωτόκολλο IGMP (Πρωτόκολλο ομαδικής διαχείρισης Internet).

- **Να επιτρέπεται η επικοινωνία για γεφυρωμένες συνδέσεις** – Ενεργοποιήστε αυτή την επιλογή για να αποφεύγεται ο τερματισμός των γεφυρωμένων συνδέσεων. Το δίκτυο γεφυρωμένων συνδέσεων συνδέει έναν εικονικό υπολογιστή σε ένα δίκτυο χρησιμοποιώντας τον προσαρμογέα Ethernet του κεντρικού υπολογιστή. Εάν χρησιμοποιείτε δίκτυο γεφυρωμένων συνδέσεων, ο εικονικός υπολογιστής μπορεί να αποκτήσει πρόσβαση σε άλλες συσκευές στο δίκτυο και αντίστροφα, όπως εάν ήταν φυσικός υπολογιστής στο δίκτυο.

- **Να επιτρέπεται αυτόματος εντοπισμός υπηρεσιών ιστού (WSD - Web Services Discovery) για υπηρεσίες συστήματος στη ζώνη αξιοπιστίας** – Επιτρέπει εισερχόμενα αιτήματα Web Services Discovery από Ζώνες αξιοπιστίας μέσω του firewall. Το WSD είναι το πρωτόκολλο που χρησιμοποιείται για τον εντοπισμό υπηρεσιών σε ένα τοπικό δίκτυο.

- **Να επιτρέπεται ανάλυση διευθύνσεων πολλαπλών προορισμών (multicast) στη ζώνη αξιοπιστίας (LLMNR)** – Το LLMNR (Link-local Multicast Name Resolution ή Επίλυση ονόματος πολλαπλής διανομής τοπικής σύνδεσης) είναι ένα πακέτο που βασίζεται σε πρωτόκολλο DNS και επιτρέπει σε κεντρικούς υπολογιστές IPv4 και IPv6 να εκτελούν επίλυση ονόματος για κεντρικούς υπολογιστές στην ίδια τοπική σύνδεση χωρίς να απαιτείται διακομιστής DNS ή διαμόρφωση προγράμματος-πελάτη DNS. Αυτή η επιλογή επιτρέπει εισερχόμενα αιτήματα πολλαπλής διανομής DNS από τη Ζώνη αξιοπιστίας μέσω του τείχους προστασίας.

- **Υποστήριξη Windows HomeGroup** – Ενεργοποιεί την υποστήριξη HomeGroup για Windows 7 και νεότερα λειτουργικά συστήματα. Η οικιακή ομάδα επιτρέπει την κοινή χρήση αρχείων και εκτυπωτών σε ένα οικιακό δίκτυο. Για να διαμορφώσετε ένα Homegroup, μεταβείτε στο στοιχείο **Έναρξη** > **Πίνακας ελέγχου** > **Δίκτυο και Internet** > **HomeGroup**.

Ανίχνευση εισβολής

Η ανίχνευση εισβολών παρακολουθεί την επικοινωνία δικτύου της συσκευής για κακόβουλη δραστηριότητα. Μπορείτε να επεξεργαστείτε αυτές τις ρυθμίσεις **Ρυθμίσεις για προχωρημένους** (F5) > **Προστασία δικτύου** > **Προστασία δικτύου από επιθέσεις** > **Επιλογές για προχωρημένους** > **Ανίχνευση εισβολής**.

- **ΠρωτόκολλοSMB** – Ανιχνεύει και αποκλείει διάφορα προβλήματα ασφαλείας στο πρωτόκολλο

SMB.

- **Πρωτόκολλο DCE/RPC** – Ανιχνεύει και αποκλείει διάφορα κενά ασφαλείας CVE στο σύστημα απομακρυσμένης κλήσης διαδικασίας που αναπτύχθηκε για το Περιβάλλον κατανεμημένων υπολογιστών (DCE).

- **Πρωτόκολλο RDP** – Ανιχνεύει και αποκλείει διάφορα κενά ασφαλείας CVE στο πρωτόκολλο RDP (βλ. παραπάνω).

- **Ανίχνευση επίθεσης προσβολής** ARP – Η ανίχνευση των επιθέσεων προσβολής **ARP** που ενεργοποιούνται από προσβολές μεσάζοντα ή η ανίχνευση μη εξουσιοδοτημένης παρακολούθησης στον διακόπτη του δικτύου. Το ARP (Πρωτόκολλο ανάλυσης διευθύνσεων) χρησιμοποιείται από την εφαρμογή ή τη συσκευή δικτύου για να προσδιορίσει τη διεύθυνση Ethernet.

- **TCP/UDP Ανιχνεύει επιθέσεις λογισμικού** – εφαρμογής σάρωσης θυρών που είναι σχεδιασμένο/η να εξετάζει έναν κεντρικό υπολογιστή για ανοιχτές θύρες στέλνοντας αιτήματα προγράμματος-πελάτη σε διάφορες διευθύνσεις θυρών, με στόχο να εντοπίσει ενεργές θύρες και να εκμεταλλευτεί τα κενά ασφαλείας της υπηρεσίας. Διαβάστε περισσότερα για αυτό τον τύπο εισβολής στο γλωσσάρι.

- **Αποκλεισμός μη ασφαλούς διεύθυνσης μετά την ανίχνευση της επίθεσης** – Οι διευθύνσεις IP που έχουν ανιχνευτεί ως πηγές επιθέσεων προστίθενται στη Λίστα αποκλεισμένων διευθύνσεων για να αποτρέπεται η σύνδεση για ένα ορισμένο χρονικό διάστημα.

- **Εμφάνιση ειδοποίησης μετά την ανίχνευση της επίθεσης** – Ενεργοποιεί τις ειδοποιήσεις δίσκου συστήματος στην κάτω δεξιά γωνία της οθόνης.

- **Εμφάνιση ειδοποιήσεων και για εισερχόμενες επιθέσεις σε κενά ασφαλείας** – Σας ειδοποιεί εάν ανιχνευτούν επιθέσεις σε κενά ασφαλείας ή εάν κάποια απειλή επιχειρήσει να εισβάλει στο σύστημα με αυτό τον τρόπο.

Επιθεώρηση πακέτου

Ένας τύπος ανάλυσης πακέτων που φιλτράρει τα δεδομένα που μεταφέρονται μέσω του δικτύου. Μπορείτε να επεξεργαστείτε αυτές τις ρυθμίσεις στη διαδρομή **Ρυθμίσεις για προχωρημένους** (F5) > **Προστασία δικτύου** > **Προστασία δικτύου από επιθέσεις** > **Επιλογές για προχωρημένους** > **Επιθεώρηση πακέτου**.

- **Να επιτρέπεται εισερχόμενη σύνδεση με κοινόχρηστα στοιχεία διαχείρισης σε πρωτόκολλο SMB** – Τα κοινόχρηστα αρχεία διαχείρισης είναι τα προεπιλεγμένα κοινόχρηστα αρχεία δικτύου που έχουν κοινόχρηστα διαμερίσματα σκληρού δίσκου (*C$*, *D$* κ.λπ.) στο σύστημα μαζί με το φάκελο συστήματος (ADMIN$*ADMIN$*). Η απενεργοποίηση της σύνδεσης με τα κοινόχρηστα αρχεία διαχείρισης θα πρέπει περιορίσει πολλούς κινδύνους ασφαλείας. Για παράδειγμα, το Conficker worm εκτελεί επιθέσεις σε λεξικά για να συνδεθεί με κοινόχρηστα αρχεία διαχείρισης.

- **Να μην επιτρέπονται παλαιές (μη υποστηριζόμενες) διάλεκτοι SMB** – Να μην επιτρέπονται περίοδοι λειτουργίας SMB που χρησιμοποιούν παλιά διάλεκτο SMB, η οποία δεν υποστηρίζεται από το IDS. Τα σύγχρονα λειτουργικά συστήματα των Windows υποστηρίζουν παλιές διαλέκτους SMB λόγω της συμβατότητάς τους με παλαιότερες εκδόσεις λειτουργικών συστημάτων όπως τα Windows 95. Ο εισβολέας μπορεί να χρησιμοποιήσει μια παλιά διάλεκτο σε περίοδο λειτουργίας SMB για να αποφύγει την επιθεώρηση κυκλοφορίας. Μην επιτρέπετε παλιές διαλέκτους SMB αν ο

υπολογιστής σας δεν χρειάζεται να κάνει κοινή χρήση αρχείων (ή να χρησιμοποιεί επικοινωνία SMB γενικότερα) με έναν υπολογιστή με παλιά έκδοση των Windows.

- **Να μην επιτρέπονται περίοδοι λειτουργίας SMB χωρίς εκτενή ασφάλεια** – Η εκτεταμένη ασφάλεια μπορεί να χρησιμοποιηθεί κατά τη διάρκεια της διαπραγμάτευσης της περιόδου λειτουργίας SMB για την παροχή πιο ασφαλούς μηχανισμού ελέγχου ταυτότητας από αυτόν που παρέχει ο έλεγχος ταυτότητας της Διαχείρισης προκλήσεων/αποκρίσεων LAN (LM). Το σχήμα LM θεωρείται αδύναμο και η χρήση του δεν συνιστάται.

- **Να μην επιτρέπεται το άνοιγμα εκτελέσιμων αρχείων σε διακομιστή εκτός της ζώνης αξιοπιστίας στο πρωτόκολλο SMB** – Κλείνει τη σύνδεση όταν προσπαθείτε να ανοίξετε ένα εκτελέσιμο αρχείο (.exe, .dll, ...) από έναν κοινόχρηστο φάκελο στον διακομιστή που δεν ανήκει στη ζώνη αξιοπιστίας στο Firewall. Σημειώνεται ότι η αντιγραφή εκτελέσιμων αρχείων από αξιόπιστες πηγές μπορεί να είναι νόμιμη. Σημειώστε ότι η αντιγραφή εκτελέσιμων αρχείων από αξιόπιστες πηγές μπορεί να είναι νόμιμη, ωστόσο αυτή η ανίχνευση θα πρέπει να μειώνει τους κινδύνους από το ανεπιθύμητο άνοιγμα ενός αρχείου σε κακόβουλο διακομιστή (για παράδειγμα, ενός αρχείου που ανοίγει κάνοντας κλικ σε ένα σύνδεσμο προς ένα κοινόχρηστο κακόβουλο εκτελέσιμο αρχείο).

- **Να μην επιτρέπεται έλεγχος ταυτότητας NTLM στο πρωτόκολλο SMB για σύνδεση με διακομιστή εντός/εκτός της ζώνης αξιοπιστίας** – Τα πρωτόκολλα που χρησιμοποιούν σχήματα ελέγχου ταυτότητας NTLM (και στις δύο εκδόσεις) εκτίθενται σε μια επίθεση προώθησης διαπιστευτηρίων (γνωστή ως επίθεση μεταβίβασης SMB στην περίπτωση πρωτοκόλλου SMB). Όταν δεν επιτρέπεται ο έλεγχος ταυτότητας NTLM με έναν διακομιστή εκτός της ζώνης αξιοπιστίας, αυτό θα πρέπει να μειώσει τους κινδύνους από προώθηση διαπιστευτηρίων από κάποιον κακόβουλο διακομιστή εκτός της ζώνης αξιοπιστίας. Παρομοίως, μπορείτε να μην επιτρέψετε έλεγχο ταυτότητας NTLM σε διακομιστές εντός της Ζώνης αξιοπιστίας.

- **Να επιτρέπεται επικοινωνία με την υπηρεσία Διαχείρισης λογαριασμών ασφαλείας** – Για περισσότερες πληροφορίες σχετικά με αυτή την υπηρεσία, ανατρέξτε στη σελίδα [MS-SAMR].

- **Να επιτρέπεται επικοινωνία με την υπηρεσία Τοπικής αρχής ασφαλείας** – Για περισσότερες πληροφορίες σχετικά με αυτή την υπηρεσία, ανατρέξτε στις σελίδες [MS-LSAD] και [MS-LSAT].

- **Να επιτρέπεται επικοινωνία με την υπηρεσία Απομακρυσμένου μητρώου** – Για περισσότερες πληροφορίες σχετικά με αυτή την υπηρεσία, ανατρέξτε στη σελίδα [MS-RRP].

- **Να επιτρέπεται επικοινωνία με την υπηρεσία Διαχείρισης ελέγχου υπηρεσιών** – Για περισσότερες πληροφορίες σχετικά με αυτή την υπηρεσία, ανατρέξτε στη σελίδα [MS-SCMR].

- **Να επιτρέπεται επικοινωνία με την υπηρεσία διακομιστή** – Για πληροφορίες σχετικά με αυτή την υπηρεσία, ανατρέξτε στη σελίδα [MS-SRVS].

- **Να επιτρέπεται επικοινωνία με τις άλλες υπηρεσίες** – Άλλες υπηρεσίες MSRPC.

Συνδεδεμένα δίκτυα

Εμφανίζει τα δίκτυα στα οποία συνδέονται προσαρμογείς δικτύου. Το στοιχείο **Συνδεδεμένα δίκτυα** βρίσκεται στο κύριο μενού, στην διαδρομή **Ρυθμίσεις** > **Προστασία δικτύου**. Αφού κάνετε κλικ στον σύνδεσμο κάτω από το όνομα δικτύου, θα σας ζητηθεί να επιλέξετε έναν τύπο προστασίας για το δίκτυο στο οποίο έχετε συνδεθεί.

Υπάρχουν δύο λειτουργίες προστασίας δικτύου που μπορείτε να επιλέξετε στο παράθυρο ρύθμισης παραμέτρων προστασίας δικτύου:

• **Ναι** – Για αξιόπιστο δίκτυο (οικιακό ή εταιρικό δίκτυο). Ο υπολογιστής σας και τα κοινόχρηστα αρχεία που είναι αποθηκευμένα στον υπολογιστή σας είναι ορατά σε άλλους χρήστες του δικτύου και άλλοι χρήστες έχουν πρόσβαση στους πόρους συστήματος. Συνιστάται η χρήση αυτής της ρύθμισης όταν αποκτάτε πρόσβαση σε ένα ασφαλές τοπικό δίκτυο.

• **Όχι** – Για μη αξιόπιστο δίκτυο (δημόσιο δίκτυο). Τα αρχεία και οι φάκελοι στο σύστημά σας δεν είναι κοινόχρηστα ή ορατά σε άλλους χρήστες στο δίκτυο και η κοινή χρήση των πόρων του συστήματος έχει απενεργοποιηθεί. Συνιστάται να χρησιμοποιείτε αυτή τη ρύθμιση όταν αποκτάτε πρόσβαση σε ασύρματα δίκτυα.

Κάντε κλικ στο εικονίδιο γραναζιού που βρίσκεται δίπλα σε ένα δίκτυο για να επιλέξετε από τις ακόλουθες επιλογές (για μη αξιόπιστα δίκτυα, είναι διαθέσιμη μόνο η επιλογή **Επεξεργασία δικτύου**):

• **Επεξεργασία δικτύου** – Ανοίγει το στοιχείο Επεξεργασία δικτύου.

• **Σάρωση δικτύου με τον Ελεγκτή δικτύου** – Ανοίγει ο Ελεγκτής δικτύου για την εκτέλεση σάρωσης δικτύου.

• **Επισήμανση ως «Το δίκτυό μου»** – Προσθέτει μια ετικέτα «Το δίκτυό μου» στο δίκτυο. Αυτή η ετικέτα θα εμφανίζεται δίπλα στο δίκτυο σε όλο το ESET Internet Security για καλύτερη αναγνώριση και επισκόπηση της ασφάλειας.

• **Κατάργηση της επισήμανσης ως «Το δίκτυό μου»** – Καταργεί την ετικέτα «Το δίκτυό μου». Η δυνατότητα είναι διαθέσιμη μόνο εάν το δίκτυο διαθέτει ήδη την ετικέτα.

Για να δείτε κάθε προσαρμογέα δικτύου, το αντιστοιχισμένο του προφίλ τείχους προστασίας και τη ζώνη αξιοπιστίας κάντε κλικ στο στοιχείο **Προσαρμογείς δικτύου**. Για πιο λεπτομερείς πληροφορίες, ανατρέξτε στην ενότητα Προσαρμογείς δικτύου.

Προσαρμογείς δικτύου

Το παράθυρο "Προσαρμογείς δικτύου" εμφανίζει τις παρακάτω πληροφορίες σχετικά με τους προσαρμογείς δικτύου σας:

• Όνομα προσαρμογέα δικτύου και τύπος σύνδεσης (εάν είναι ενσύρματη, εικονική κ.λπ.)

• Διεύθυνση IP με διεύθυνση MAC

• Συνδεδεμένο δίκτυο (εμφανίζει την ετικέτα «Το δίκτυό μου»)

• Διεύθυνση IP ζώνης αξιοπιστίας με υποδίκτυο

• Ενεργό προφίλ (ανατρέξτε στο θέμα Προφίλ αντιστοιχισμένα σε προσαρμογείς δικτύου)

Προσωρινή λίστα αποκλεισμού διευθύνσεων IP

Για να δείτε αν οι διευθύνσεις IP που ανιχνεύτηκαν ως προελεύσεις επιθέσεων έχουν προστεθεί στη λίστα αποκλεισμένων διευθύνσεων, ώστε να αποκλείεται η σύνδεση για συγκεκριμένο χρονικό διάστημα, από το ESET Internet Security μεταβείτε στα στοιχεία **Ρυθμίσεις** > **Προστασία δικτύου** > **Προσωρινή λίστα αποκλεισμένων διευθύνσεων IP**. Οι αποκλεισμένες διευθύνσεις IP αποκλείονται για 1 ώρα.

Στήλες

Διεύθυνση IP – εμφανίζει μια διεύθυνση IP που έχει αποκλειστεί.

Λόγος αποκλεισμού – εμφανίζει τον τύπο επίθεσης που έχει αποτραπεί από τη διεύθυνση (για παράδειγμα επίθεση Σάρωσης θύρας TCP).

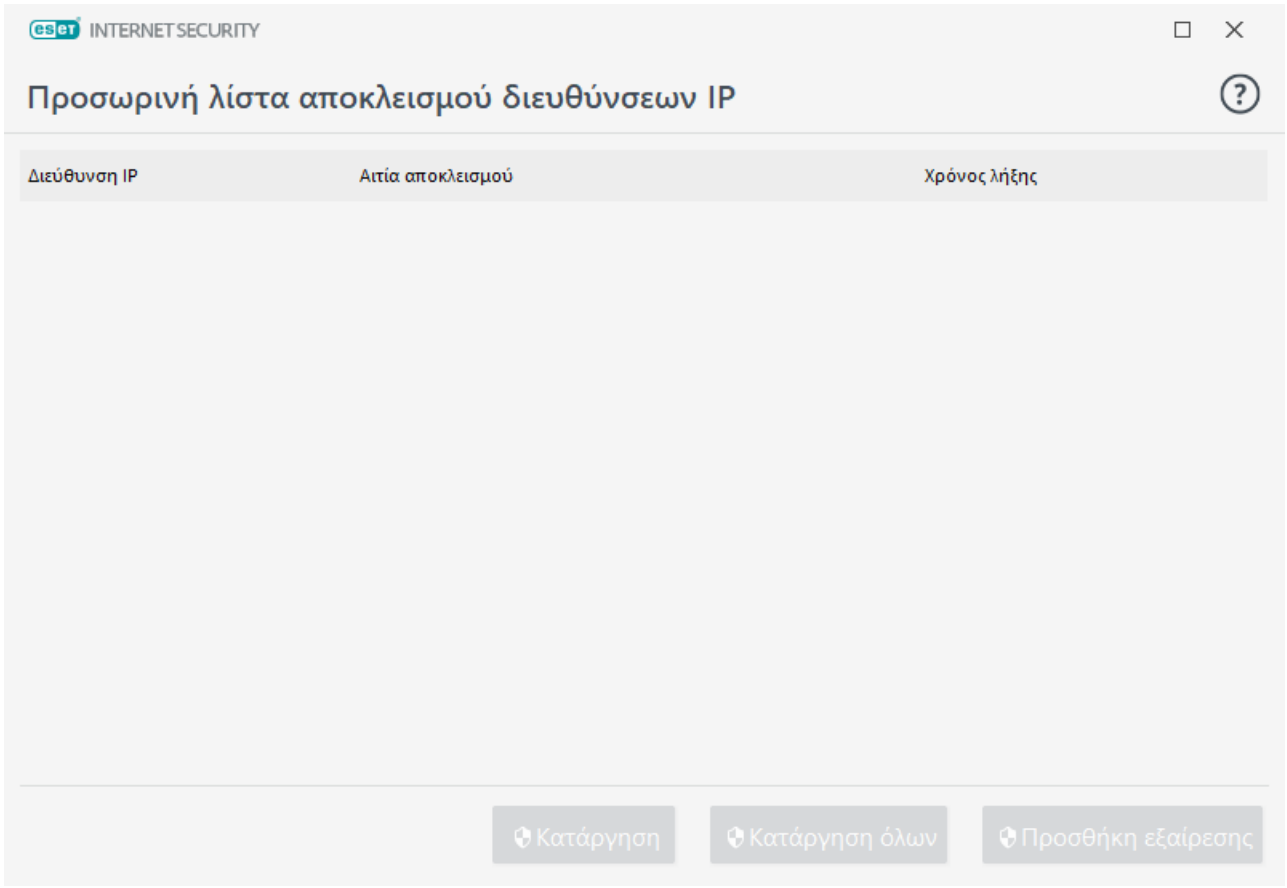
Λήξη χρονικού ορίου – εμφανίζει την ώρα και την ημερομηνία κατά την οποία θα αφαιρεθεί η διεύθυνση από τη λίστα αποκλεισμένων διευθύνσεων.

Στοιχεία ελέγχου

Κατάργηση – κάντε κλικ για να αφαιρέσετε μια διεύθυνση από τη λίστα αποκλεισμένων διευθύνσεων προτού λήξει.

Κατάργηση όλων – κάντε κλικ για να αφαιρέσετε αμέσως όλες τις διευθύνσεις από τη λίστα αποκλεισμένων διευθύνσεων.

Προσθήκη εξαίρεσης – Κάντε κλικ για να προσθέσετε μια εξαίρεση firewall στο φιλτράρισμα IDS.



Αρχείο καταγραφής προστασίας δικτύου

Η προστασία δικτύου του ESET Internet Security αποθηκεύει όλα τα σημαντικά συμβάντα σε ένα αρχείο καταγραφής, το οποίο μπορείτε να προβάλετε απευθείας από το κύριο μενού. Κάντε κλικ στο στοιχείο **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής** και κατόπιν επιλέξτε **Προστασία δικτύου** από το αναπτυσσόμενο μενού **Καταγραφή**.

Τα αρχεία καταγραφής μπορούν να χρησιμοποιηθούν για την ανίχνευση σφαλμάτων και την αποκάλυψη εισβολών στο σύστημά σας. Στα αρχεία καταγραφής προστασίας δικτύου της ESET περιλαμβάνονται τα εξής δεδομένα:

- Ημερομηνία και ώρα συμβάντος
- Όνομα συμβάντος
- Προέλευση
- Διεύθυνση δικτύου προορισμού
- Πρωτόκολλο επικοινωνίας δικτύου
- Εφαρμοζόμενος κανόνας ή όνομα απειλής worm, εάν εντοπίστηκε
- Σχετική εφαρμογή
- Χρήστης

Η λεπτομερής ανάλυση αυτών των δεδομένων μπορεί να σας βοηθήσει να εντοπίσετε απόπειρες

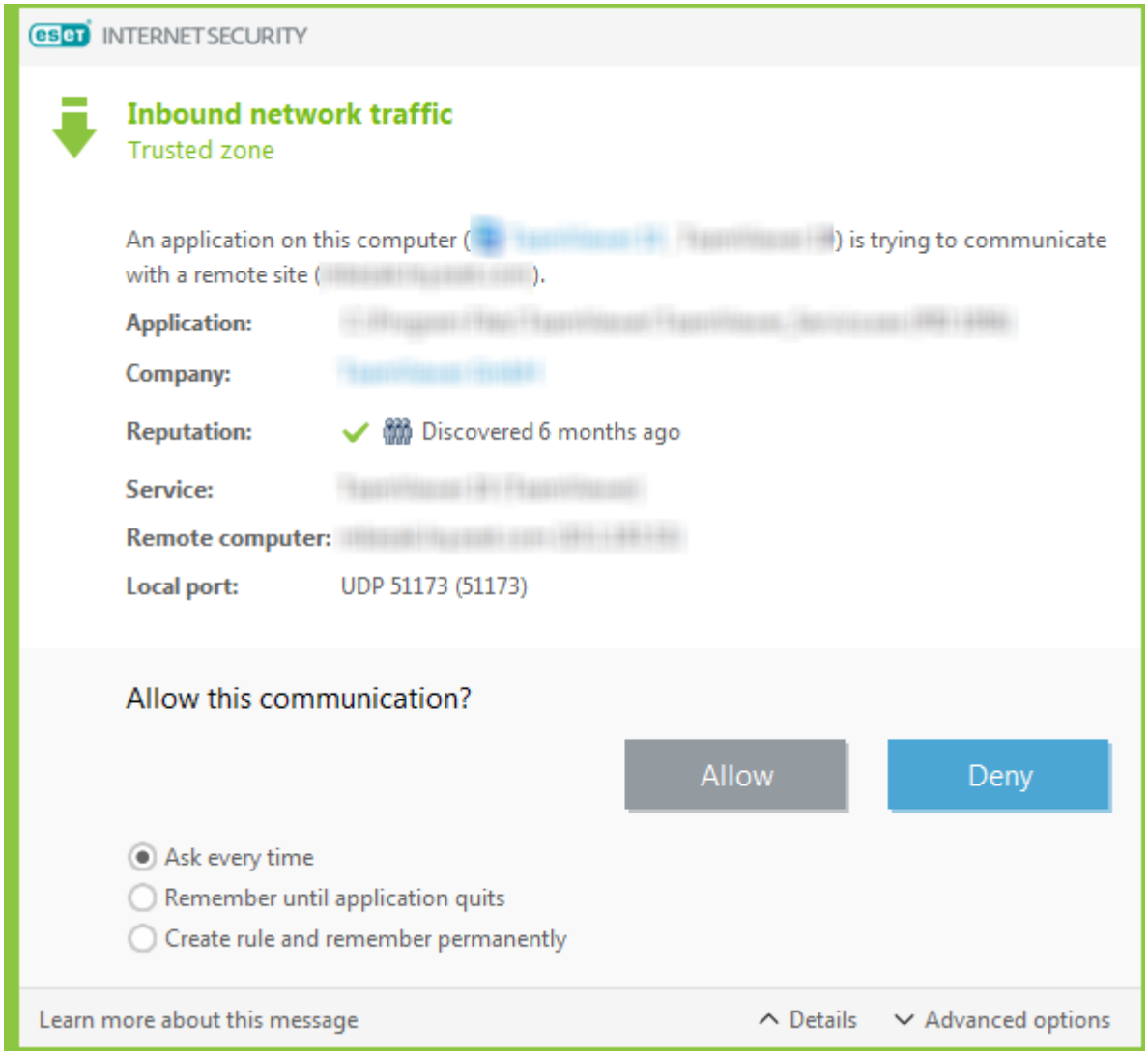
παραβίασης της ασφάλειας του συστήματός σας. Πολλοί άλλοι παράγοντες υποδεικνύουν δυνητικούς κινδύνους ασφαλείας και σας επιτρέπουν να ελαχιστοποιήσετε τις επιπτώσεις τους: συχνές συνδέσεις από άγνωστες τοποθεσίες, πολλαπλές απόπειρες δημιουργίας συνδέσεων, επικοινωνία άγνωστων εφαρμογών ή χρήση ασυνήθιστων αριθμών θυρών.

> **Εκμετάλλευση τρωτών σημείων ασφαλείας**
> Το μήνυμα της κατάχρησης τρωτών σημείων ασφαλείας καταγράφεται ακόμα και αν το συγκεκριμένο τρωτό σημείο έχει ήδη επιδιορθωθεί, αφού η προσπάθεια κατάχρησης ανιχνεύεται και αποκλείεται σε επίπεδο δικτύου προτού πραγματοποιηθεί αυτή η κατάχρηση.

Δημιουργία σύνδεσης - ανίχνευση

Το Firewall ανιχνεύει κάθε νέα σύνδεση δικτύου. Η ενεργή λειτουργία firewall προσδιορίζει τις ενέργειες που θα πραγματοποιούνται για τον νέο κανόνα. Εάν ενεργοποιηθεί η επιλογή **Αυτόματη λειτουργία** ή η επιλογή **Λειτουργία βασισμένη σε πολιτική**, το τείχος προστασίας θα πραγματοποιεί προκαθορισμένες ενέργειες χωρίς παρέμβαση του χρήστη.

Η λειτουργία **Αλληλεπιδραστική λειτουργία** ένα παράθυρο πληροφοριών στο οποίο αναφέρεται η ανίχνευση νέας σύνδεσης δικτύου, μαζί με λεπτομερείς πληροφορίες σχετικά με τη σύνδεση. Μπορείτε να επιλέξετε **Να επιτρέπεται** ή **Να μην επιτρέπεται** (να αποκλείεται) η σύνδεση. Εάν επανειλημμένα επιτρέπετε την ίδια σύνδεση στο παράθυρο διαλόγου, συνιστούμε να δημιουργήσετε έναν νέο κανόνα για τη σύνδεση. Για να το κάνετε αυτό, επιλέξτε **Δημιουργία κανόνα και μόνιμη απομνημόνευση** και αποθηκεύστε την ενέργεια ως νέο κανόνα για το Firewall. Εάν το τείχος προστασίας αναγνωρίσει την ίδια σύνδεση στο μέλλον, θα εφαρμόσει τον υφιστάμενο κανόνα χωρίς να απαιτήσει παρέμβαση του χρήστη.



Κατά τη δημιουργία νέων κανόνων, να επιτρέπετε μόνο τις συνδέσεις που γνωρίζετε ότι είναι ασφαλείς. Εάν επιτρέπονται όλες οι συνδέσεις, τότε το τείχος προστασίας δεν μπορεί να επιτύχει στο σκοπό του. Αυτές είναι οι σημαντικές παράμετροι για τις συνδέσεις:

Εφαρμογή – Εκτελέσιμη θέση αρχείου και αναγνωριστικό διεργασίας. Να μην επιτρέπετε συνδέσεις για άγνωστες εφαρμογές και διεργασίες.

Εταιρεία – Όνομα εκδότη της εφαρμογής. Κάντε κλικ στο κείμενο για να εμφανιστεί ένα πιστοποιητικό ασφαλείας για την εταιρεία.

Φήμη – Επίπεδο κινδύνου της σύνδεσης. Στις συνδέσεις αντιστοιχίζεται ένα επίπεδο κινδύνου: Αβλαβές (πράσινο), Άγνωστο (πορτοκαλί) ή Επικίνδυνο (κόκκινο), χρησιμοποιώντας μια σειρά ευριστικών κανόνων που εξετάζουν τα χαρακτηριστικά κάθε σύνδεσης, τον αριθμό χρηστών και τον χρόνο αποκάλυψης. Αυτές οι πληροφορίες συλλέγονται από την τεχνολογία ESET LiveGrid®.

Υπηρεσία – Όνομα της υπηρεσίας, εάν η εφαρμογή είναι υπηρεσία των Windows.

Απομακρυσμένος υπολογιστής – Διεύθυνση της απομακρυσμένης συσκευής. Επιτρέπονται μόνο συνδέσεις με αξιόπιστες και γνωστές διευθύνσεις.

Απομακρυσμένη θύρα – Θύρα επικοινωνίας. Η επικοινωνία σε συνήθεις θύρες (π.χ. κυκλοφορία διαδικτύου – αριθμός θύρας 80.443) μπορεί να επιτρέπεται υπό κανονικές συνθήκες.

Οι εισβολές υπολογιστών χρησιμοποιούν συχνά συνδέσεις Internet και κρυφές συνδέσεις για να μολύνουν απομακρυσμένα συστήματα. Εάν οι κανόνες ρυθμίζονται σωστά, το Firewall γίνεται ένα χρήσιμο εργαλείο για την προστασία απέναντι σε μια σειρά επιθέσεων κακόβουλου κώδικα.

Επίλυση προβλημάτων με το Τείχος προστασίας της ESET

Εάν αντιμετωπίσετε προβλήματα συνδεσιμότητας ενώ είναι εγκατεστημένο το ESET Internet Security, υπάρχουν διάφοροι τρόποι να διαπιστώσετε εάν το Τείχος προστασίας της ESET δημιουργεί το πρόβλημα. Επιπλέον, το Τείχος προστασίας της ESET μπορεί να σας βοηθήσει να δημιουργήσετε νέους κανόνες ή εξαιρέσεις για να επιλύσετε προβλήματα συνδεσιμότητας.

Ανατρέξτε στα παρακάτω θέματα για βοήθεια στην επίλυση προβλημάτων με το Τείχος προστασίας της ESET:

- Οδηγός επίλυσης προβλημάτων
- Καταγραφή και δημιουργία κανόνων ή εξαιρέσεων από το αρχείο καταγραφής
- Δημιουργία εξαιρέσεων από τις ειδοποιήσεις Firewall
- Καταγραφή για προχωρημένους προστασίας δικτύου
- Επίλυση προβλημάτων με το φιλτράρισμα πρωτοκόλλων

Οδηγός επίλυσης προβλημάτων

Ο οδηγός αντιμετώπισης προβλημάτων παρακολουθεί αθόρυβα όλες τις αποκλεισμένες συνδέσεις και σάς καθοδηγεί στη διαδικασία αντιμετώπισης προβλημάτων για τη διόρθωση ζητημάτων του firewall με συγκεκριμένες εφαρμογές ή συσκευές. Στη συνέχεια, ο οδηγός θα προτείνει ένα νέο σύνολο κανόνων που θα εφαρμοστούν εάν τους εγκρίνετε. Ο **Οδηγός επίλυσης προβλημάτων** βρίσκεται στο κύριο μενού στην ενότητα **Ρυθμίσεις** > **Προστασία δικτύου**.

Καταγραφή και δημιουργία κανόνων ή εξαιρέσεων από το αρχείο καταγραφής

Από προεπιλογή, το Τείχος προστασίας της ESET δεν καταγράφει όλες τις αποκλεισμένες συνδέσεις. Εάν θέλετε να βλέπετε ποια έχει αποκλειστεί από την Προστασία δικτύου, ενεργοποιήστε την καταγραφή στην **Εγκατάσταση για προχωρημένους** στην ενότητα **Εργαλεία** > **Διαγνωστικοί έλεγχοι** > **Καταγραφή για προχωρημένους** > **Ενεργοποίηση καταγραφής για προχωρημένους της προστασίας δικτύου**. Εάν δείτε κάτι στο αρχείο καταγραφής το οποίο δεν θέλετε να αποκλείεται από το Τείχος προστασίας, μπορείτε να δημιουργήσετε έναν κανόνα ή έναν κανόνα IDS κάνοντας δεξί κλικ στο στοιχείο και επιλέγοντας **Να μην αποκλείονται στο μέλλον παρόμοια συμβάντα**. Σημειώνεται ότι το αρχείο καταγραφής όλων των αποκλεισμένων συνδέσεων μπορεί να περιέχει χιλιάδες στοιχεία και ίσως είναι δύσκολο να βρείτε μια συγκεκριμένη σύνδεση σε αυτό το αρχείο καταγραφής. Μπορείτε να απενεργοποιήσετε την καταγραφή αφού επιλύσετε το ζήτημα.

Για περισσότερες πληροφορίες σχετικά με την καταγραφή, ανατρέξτε στο κεφάλαιο Αρχεία καταγραφής.

Χρησιμοποιείτε την καταγραφή για να δείτε τη σειρά με την οποία το Προστασία δικτύου απέκλεισε συγκεκριμένες συνδέσεις. Επιπλέον, η δυνατότητα δημιουργίας κανόνων από το αρχείο καταγραφής σάς επιτρέπει να δημιουργήσετε κανόνες που κάνουν ακριβώς αυτό που θέλετε.

Δημιουργία κανόνα από αρχείο καταγραφής

Η νέα έκδοση του ESET Internet Security σάς επιτρέπει να δημιουργήσετε έναν κανόνα από το αρχείο καταγραφής. Από το κύριο μενού, κάντε κλικ στα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής**. Επιλέξτε **Τείχος προστασίας** από το αναπτυσσόμενο μενού, κάντε δεξί κλικ στην καταχώριση καταγραφής που θέλετε και επιλέξτε **Να μην αποκλείονται στο μέλλον παρόμοια συμβάντα** από το μενού περιβάλλοντος. Ένα παράθυρο ειδοποίησης θα εμφανίσει τον νέο κανόνα.

Για να επιτρέπεται η δημιουργία νέων κανόνων από το αρχείο καταγραφής, το ESET Internet Security πρέπει να είναι διαμορφωμένο με τις εξής ρυθμίσεις:

1. Ρυθμίστε το ελάχιστο επίπεδο λεπτομερειών καταγραφής σε **Εγγραφές διαγνωστικού ελέγχου** στην ενότητα **Ρυθμίσεις για προχωρημένους** (F5) > **Εργαλεία** > **Αρχεία καταγραφής**,

2. Ενεργοποιήστε την επιλογή **Εμφάνιση ειδοποιήσεων και για εισερχόμενες επιθέσεις σε κενά ασφαλείας** στη διαδρομή **Εγκατάσταση για προχωρημένους** (F5) > **Προστασία δικτύου** > **Προστασία από επιθέσεις δικτύου** > **Επιλογές για προχωρημένους** > **Ανίχνευση εισβολής**.

Δημιουργία εξαιρέσεων από τις ειδοποιήσεις Firewall

Όταν το Τείχος προστασίας της ESET εντοπίσει κακόβουλη δραστηριότητα στο δίκτυο, εμφανίζεται ένα παράθυρο ειδοποίησης που περιγράφει το συμβάν. Αυτή η ειδοποίηση περιέχει έναν σύνδεσμο που σας επιτρέπει να μάθετε περισσότερα σχετικά με το συμβάν και να ρυθμίσετε έναν κανόνα για το συμβάν, εάν επιθυμείτε.

Εάν μια εφαρμογή ή συσκευή δικτύου δεν υλοποιεί σωστά τις προδιαγραφές δικτύου, μπορεί να ενεργοποιήσει αλλεπάλληλες ειδοποιήσεις IDS του τείχος προστασίας. Μπορείτε να δημιουργήσετε μια εξαίρεση απευθείας από την ειδοποίηση για να εμποδίσετε το Τείχος προστασίας της ESET να ανιχνεύει τη συγκεκριμένη εφαρμογή ή συσκευή.

Καταγραφή για προχωρημένους προστασίας δικτύου

Αυτή η δυνατότητα έχει σκοπό να παρέχει πιο σύνθετα αρχεία καταγραφής για την τεχνική υποστήριξη της ESET. Χρησιμοποιήστε αυτή τη δυνατότητα μόνο όταν σάς ζητείται από την τεχνική

υποστήριξη της ESET, επειδή μπορεί να δημιουργήσει ένα τεράστιο αρχείο καταγραφής και να επιβραδύνει τη λειτουργία του υπολογιστή σας.

1. Μεταβείτε στα στοιχεία **Εγκατάσταση για προχωρημένους** > **Εργαλεία** > **Διαγνωστικοί έλεγχοι** και ενεργοποιήστε το στοιχείο **Ενεργοποίηση της καταγραφής για προχωρημένους προστασίας δικτύου**.

2. Προσπαθήστε να αναπαραγάγετε το πρόβλημα που αντιμετωπίζετε.

3. Απενεργοποιήστε την Καταγραφή για προχωρημένους προστασίας δικτύου.

4. Μπορείτε να βρείτε το αρχείο καταγραφής PCAP που δημιουργήθηκε από την Καταγραφή για προχωρημένους προστασίας δικτύου στον ίδιο κατάλογο όπου ο διαγνωστικός έλεγχος δημιουργεί τα αρχεία ένδειξης σφαλμάτων μνήμης: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Επίλυση προβλημάτων με το φιλτράρισμα πρωτοκόλλων

Εάν αντιμετωπίζετε προβλήματα με το πρόγραμμα περιήγησης ή το πρόγραμμα ηλεκτρονικής αλληλογραφίας σας, το πρώτο βήμα είναι να προσδιορίσετε εάν ευθύνεται το φιλτράρισμα πρωτοκόλλων. Για να το κάνετε αυτό, δοκιμάστε να απενεργοποιήσετε προσωρινά το φιλτράρισμα πρωτοκόλλων στις Ρυθμίσεις για προχωρημένους (θυμηθείτε να το ενεργοποιήσετε ξανά μόλις τελειώσετε, διαφορετικά το πρόγραμμα περιήγησης και το πρόγραμμα ηλεκτρονικής αλληλογραφίας σας δεν θα προστατεύονται). Εάν το πρόβλημα εξαφανιστεί μετά την απενεργοποίηση, ακολουθεί μια λίστα με συνηθισμένα προβλήματα και έναν τρόπο για να τα επιλύσετε:

Προβλήματα ενημέρωσης ή προστασίας επικοινωνιών

Εάν η εφαρμογή σας δεν είναι σε θέση να ενημερωθεί ή σας πληροφορεί ότι ένας δίαυλος επικοινωνίας δεν είναι ασφαλής:

- Εάν έχετε ενεργοποιημένο το φιλτράρισμα πρωτοκόλλου SSL, δοκιμάστε να το απενεργοποιήσετε προσωρινά. Εάν αυτό βοηθά, μπορείτε να συνεχίσετε να χρησιμοποιείτε το φιλτράρισμα πρωτοκόλλου SSL και να πραγματοποιήσετε την εργασία ενημέρωσης εξαιρώντας την προβληματική επικοινωνία:
Αλλάξτε τη λειτουργία φιλτραρίσματος SSL σε Αλληλεπιδραστική. Πραγματοποιήστε ξανά την ενημέρωση. Θα πρέπει να εμφανιστεί ένα παράθυρο διαλόγου που θα σάς πληροφορεί σχετικά με κρυπτογραφημένη κυκλοφορία δικτύου. Βεβαιωθείτε ότι η εφαρμογή αντιστοιχεί σε εκείνη που προσπαθείτε να διορθώσετε και ότι το πιστοποιητικό δείχνει να προέρχεται από το διακομιστή από τον οποίο η εφαρμογή επιχειρεί να λάβει την ενημέρωση. Κατόπιν, επιλέξτε να απομνημονευτεί η ενέργεια για αυτό το πιστοποιητικό και κάντε κλικ στο κουμπί "Παράβλεψη". Εάν δεν εμφανίζονται άλλα σχετικά παράθυρα διαλόγου, μπορείτε να επαναφέρετε τη λειτουργία φιλτραρίσματος σε "Αυτόματη" και το πρόβλημα κανονικά θα πρέπει να λυθεί.

- Εάν η εφαρμογή δεν είναι πρόγραμμα περιήγησης ή ηλεκτρονικής αλληλογραφίας, μπορείτε να την εξαιρέσετε εντελώς από το φιλτράρισμα πρωτοκόλλων (εάν το κάνετε αυτό σε πρόγραμμα περιήγησης ή ηλεκτρονικής αλληλογραφίας, ίσως σάς εκθέσει σε απειλές). Όλες οι εφαρμογές των οποίων οι επικοινωνίες φιλτράρονταν στο παρελθόν θα πρέπει να βρίσκονται ήδη στη λίστα που λάβατε κατά την προσθήκη εξαιρέσεων, συνεπώς δεν χρειάζεται να προσθέσετε μη αυτόματα κάποια εφαρμογή.

Πρόβλημα πρόσβασης σε μια συσκευή του δικτύου σας

Εάν δεν είστε σε θέση να χρησιμοποιήσετε καμιά λειτουργικότητα συσκευής στο δίκτυό σας (όπως το άνοιγμα μιας ιστοσελίδας από την κάμερα ή την αναπαραγωγή βίντεο σε μια συσκευή αναπαραγωγής πολυμέσων), δοκιμάστε να προσθέσετε τις διευθύνσεις IPv4 και IPv6 της συσκευής στη λίστα εξαιρουμένων διευθύνσεων.

Προβλήματα με έναν συγκεκριμένο ιστότοπο

Μπορείτε να εξαιρέσετε συγκεκριμένους ιστότοπους από το φιλτράρισμα πρωτοκόλλων χρησιμοποιώντας τη διαχείριση διευθύνσεων URL. Για παράδειγμα, εάν δεν μπορείτε να αποκτήσετε πρόσβαση στη διεύθυνση https://www.gmail.com/intl/en/mail/help/about.html, δοκιμάστε να προσθέσετε το *gmail.com* στη λίστα εξαιρουμένων διευθύνσεων.

Σφάλμα «Εκτελούνται ακόμη ορισμένες από τις εφαρμογές που έχουν δυνατότητα εισαγωγής του πιστοποιητικού ρίζας»

Όταν ενεργοποιείτε το φιλτράρισμα πρωτοκόλλου SSL, το ESET Internet Security διασφαλίζει ότι οι εγκατεστημένες εφαρμογές εμπιστεύονται τον τρόπο με τον οποίο το πρόγραμμα φιλτράρει το πρωτόκολλο SSL, εισάγοντας ένα πιστοποιητικό στο χώρο αποθήκευσης πιστοποιητικών τους. Για ορισμένες εφαρμογές, αυτό δεν είναι δυνατό ενώ εκτελούνται. Σε αυτές τις εφαρμογές περιλαμβάνεται το Firefox και το Opera. Βεβαιωθείτε ότι καμιά από αυτές δεν εκτελείται (ο καλύτερος τρόπος είναι να ανοίξετε τη Διαχείριση Εργασιών και να βεβαιωθείτε ότι δεν εμφανίζονται τα στοιχεία firefox.exe ή opera.exe στην καρτέλα "Διεργασίες") και κατόπιν πατήστε "Επανάληψη".

Σφάλμα σχετικά με μη αξιόπιστο εκδότη ή μη έγκυρη υπογραφή

Αυτό κατά πάσα πιθανότητα σημαίνει ότι η εισαγωγή που περιγράψαμε παραπάνω έχει αποτύχει. Πρώτα βεβαιωθείτε ότι καμιά από τις προαναφερθείσες εφαρμογές δεν εκτελείται. Κατόπιν απενεργοποιήστε το φιλτράρισμα πρωτοκόλλου SSL και ενεργοποιήστε το ξανά. Με αυτό τον τρόπο θα επαναληφθεί η εισαγωγή.

> Δείτε το άρθρο της γνωσιακής βάσης για να μάθετε Πώς να διαχειρίζεστε φιλτράρισμα πρωτοκόλλων SSL/TLS στο οικιακό προϊόν ESET για Windows.

Ανιχνεύτηκε νέο δίκτυο

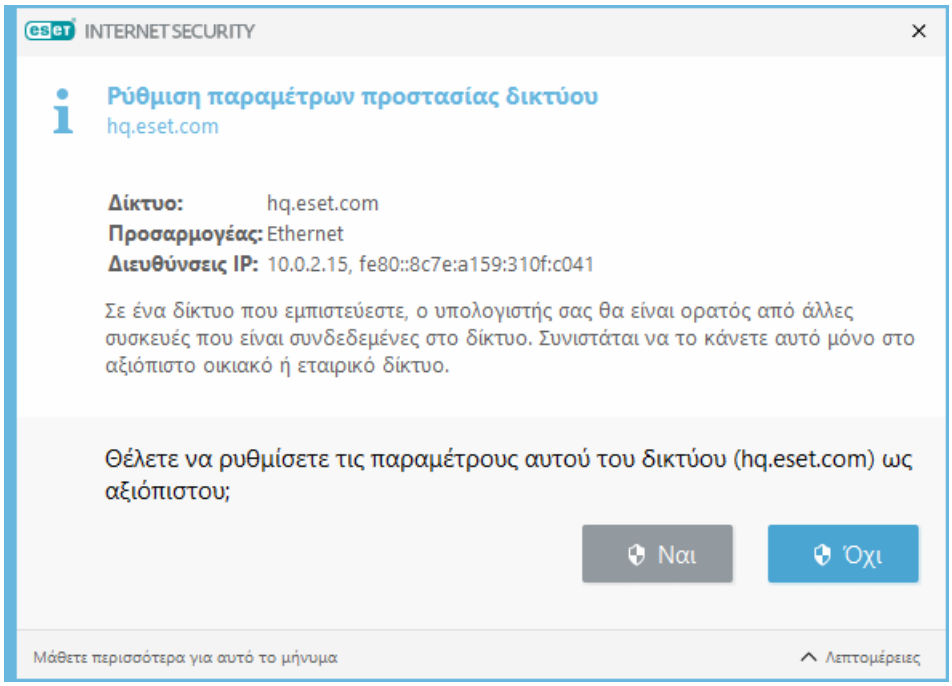
Από προεπιλογή, το ESET Internet Security χρησιμοποιεί τις ρυθμίσεις των Windows όταν ανιχνεύεται ένα νέο δίκτυο. Για να εμφανίζεται ένα παράθυρο διαλόγου όταν ανιχνεύεται ένα νέο δίκτυο, αλλάξτε τον τύπο προστασίας των νέων δικτύων στα Γνωστά δίκτυα για να ερωτάται ο χρήστης. Στη συνέχεια, εάν ανιχνευτεί ένα νέο δίκτυο, ο χρήστης μπορεί να επιλέξει το επίπεδο προστασίας. Αυτή η ρύθμιση θα εφαρμόζεται σε συνδέσεις με όλους τους απομακρυσμένους υπολογιστές από το συγκεκριμένο δίκτυο.

Υπάρχουν δύο λειτουργίες προστασίας δικτύου που μπορείτε να επιλέξετε στο παράθυρο ρύθμισης

παραμέτρων προστασίας δικτύου:

• **Ναι** – Για αξιόπιστο δίκτυο (οικιακό ή εταιρικό δίκτυο). Ο υπολογιστής σας και τα κοινόχρηστα αρχεία που είναι αποθηκευμένα στον υπολογιστή σας είναι ορατά σε άλλους χρήστες του δικτύου και άλλοι χρήστες έχουν πρόσβαση στους πόρους συστήματος. Συνιστάται η χρήση αυτής της ρύθμισης όταν αποκτάτε πρόσβαση σε ένα ασφαλές τοπικό δίκτυο.

• **Όχι** – Για μη αξιόπιστο δίκτυο (δημόσιο δίκτυο). Τα αρχεία και οι φάκελοι στο σύστημά σας δεν είναι κοινόχρηστα ή ορατά σε άλλους χρήστες στο δίκτυο και η κοινή χρήση των πόρων του συστήματος έχει απενεργοποιηθεί. Συνιστάται να χρησιμοποιείτε αυτή τη ρύθμιση όταν αποκτάτε πρόσβαση σε ασύρματα δίκτυα.



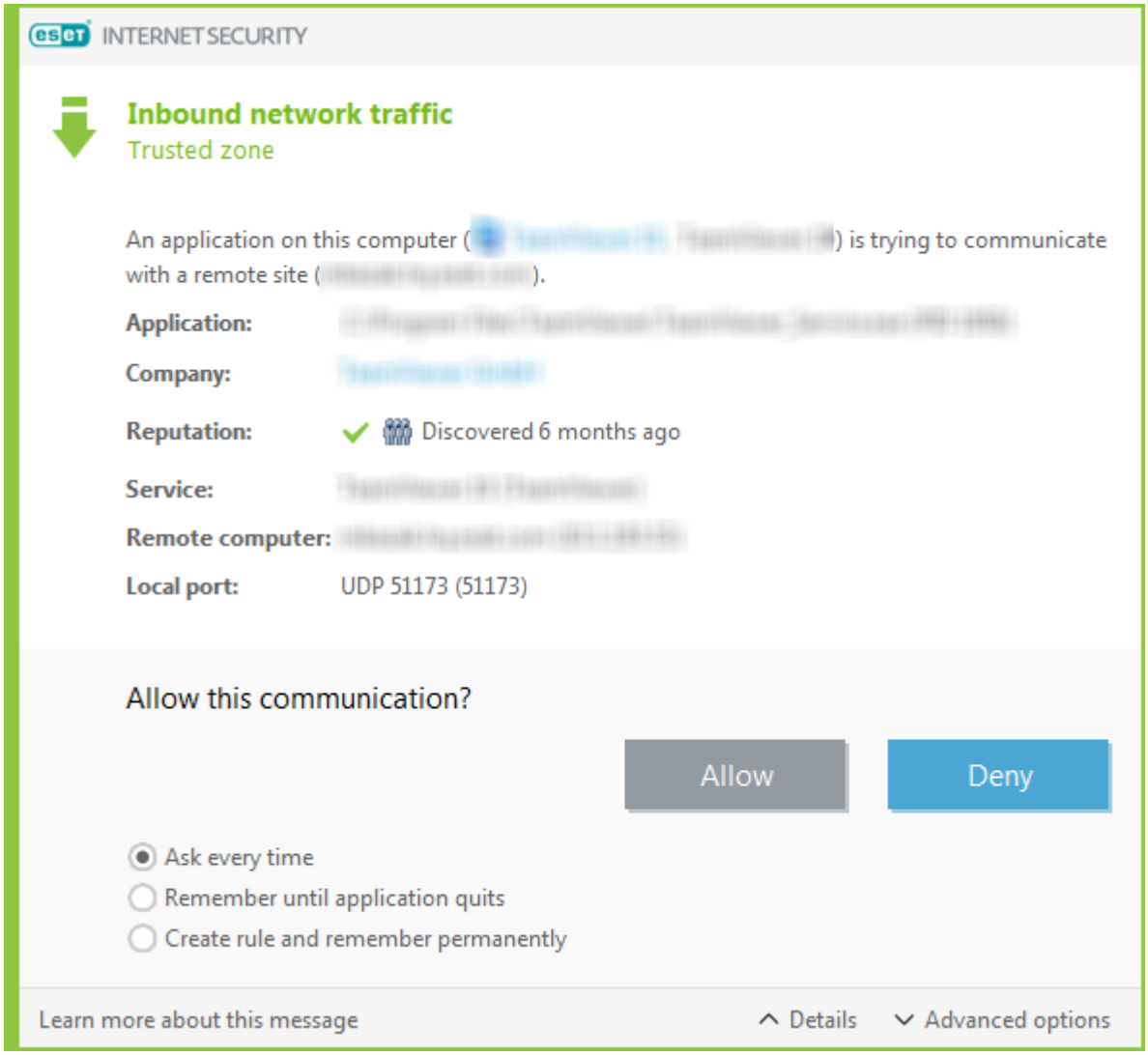
Εάν το δίκτυο έχει ρυθμιστεί ως αξιόπιστο, τα άμεσα συνδεδεμένα υποδίκτυα θεωρούνται αυτόματα αξιόπιστα.

Αλλαγή εφαρμογής

Το Firewall έχει ανιχνεύσει μια τροποποίηση σε μια εφαρμογή που χρησιμοποιείται για τη δημιουργία εξερχόμενων συνδέσεων από τον υπολογιστή σας. Είναι πιθανόν η εφαρμογή να έχει απλώς ενημερωθεί σε νέα έκδοση. Από την άλλη μεριά, η τροποποίηση μπορεί να προκλήθηκε από κακόβουλη εφαρμογή. Αν δεν γνωρίζετε κάτι για μια νόμιμη τροποποίηση, συνιστάται να απορρίψετε τη σύνδεση και να κάνετε σάρωση του υπολογιστή σας χρησιμοποιώντας την πιο πρόσφατη βάση αναγνώρισης ιών.

Αξιόπιστη εισερχόμενη επικοινωνία

Παράδειγμα μιας εισερχόμενης σύνδεσης μέσα στη ζώνη αξιοπιστίας:
Ένας απομακρυσμένος υπολογιστής μέσα από τη ζώνη αξιοπιστίας προσπαθεί να δημιουργήσει επικοινωνία με μια τοπική εφαρμογή που εκτελείται στον υπολογιστή σας.



Εφαρμογή – Η εφαρμογή με την οποία επικοινωνεί ο απομακρυσμένος υπολογιστής.

Εταιρεία – Ο εκδότης της εφαρμογής.

Φήμη – Η φήμη της εφαρμογής όπως λαμβάνεται από την τεχνολογία ESET LiveGrid®.

Υπηρεσία – Το όνομα της υπηρεσίας που εκτελείται εκείνη τη στιγμή στον υπολογιστή σας.

Απομακρυσμένος υπολογιστής – Ο απομακρυσμένος υπολογιστής που προσπαθεί να δημιουργήσει επικοινωνία με την εφαρμογή στον υπολογιστή σας.

Τοπική θύρα – Η θύρα που χρησιμοποιείται για την επικοινωνία.

Ερώτηση κάθε φορά – Εάν η προεπιλεγμένη ενέργεια για έναν κανόνα καθορίζεται σε **Ερώτηση**, θα εμφανίζεται ένα παράθυρο διαλόγου κάθε φορά που ενεργοποιείται ο κανόνας.

Απομνημόνευση μέχρι το κλείσιμο της εφαρμογής – Το ESET Internet Security θα απομνημονεύσει την επιλεγμένη ενέργεια μέχρι την επόμενη επανεκκίνηση.

Δημιουργία κανόνα και μόνιμη απομνημόνευση – Εάν ενεργοποιήσετε αυτή την επιλογή προτού επιτρέψετε ή απορρίψετε μια επικοινωνία, το ESET Internet Security θα απομνημονεύσει την ενέργεια και θα τη χρησιμοποιήσει εάν ο απομακρυσμένος υπολογιστής επικοινωνήσει ξανά με την εφαρμογή.

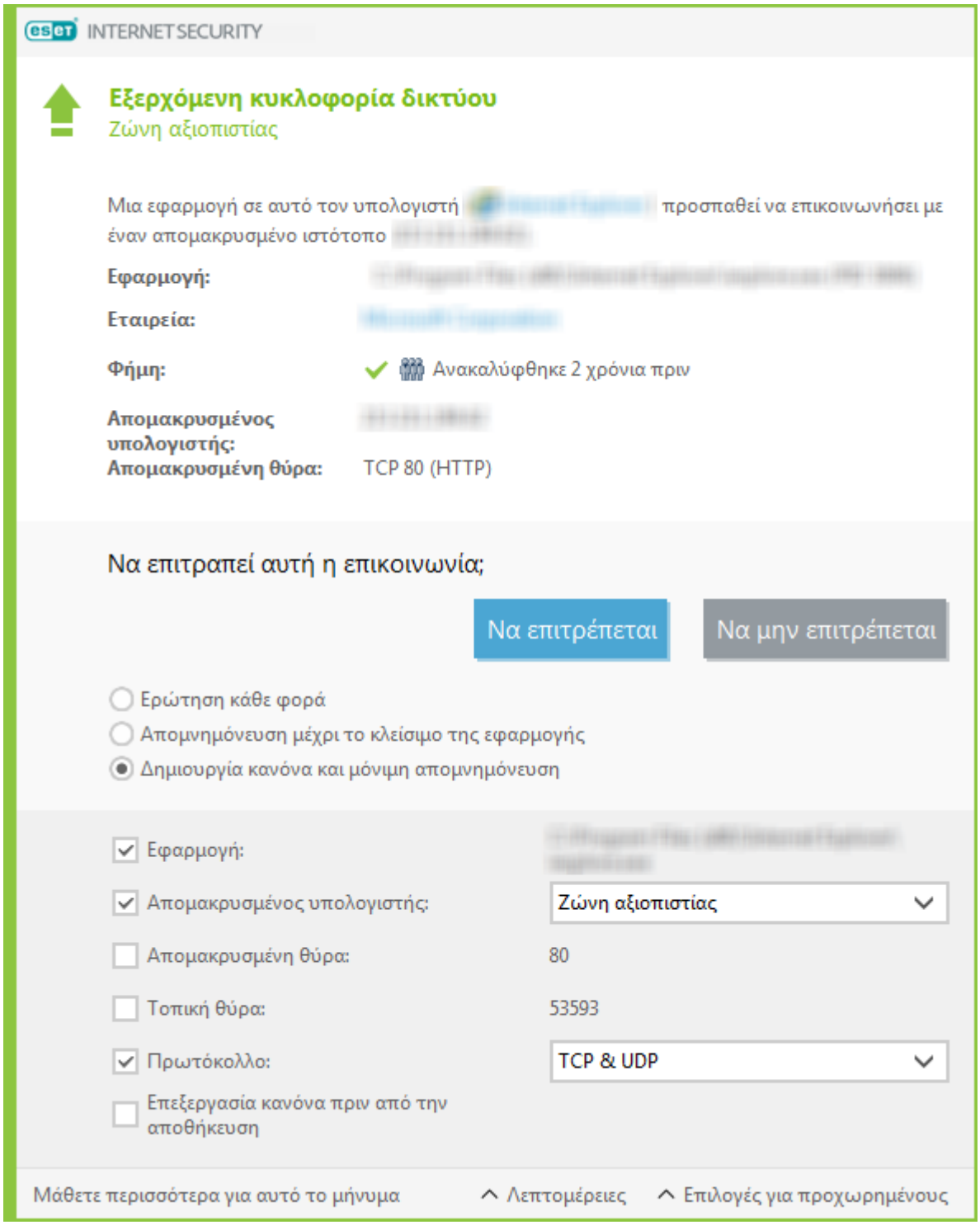
Αποδοχή – Επιτρέπει την εισερχόμενη επικοινωνία.

Δεν επιτρέπεται – Δεν επιτρέπει την εισερχόμενη επικοινωνία.

Επιλογές για προχωρημένους – Σας επιτρέπει να προσαρμόζετε τις ιδιότητες των κανόνων.

Αξιόπιστη εξερχόμενη επικοινωνία

Παράδειγμα μιας εξερχόμενης σύνδεσης μέσα στη ζώνη αξιοπιστίας:
Μια τοπική εφαρμογή που προσπαθεί να δημιουργήσει σύνδεση με άλλον υπολογιστή μέσα στο τοπικό δίκτυο ή μέσα σε ένα δίκτυο στη ζώνης αξιοπιστίας.



Εφαρμογή – Η εφαρμογή με την οποία επικοινωνεί ο απομακρυσμένος υπολογιστής.

Εταιρεία – Ο εκδότης της εφαρμογής.

Φήμη – Η φήμη της εφαρμογής όπως λαμβάνεται από την τεχνολογία ESET LiveGrid®.

Υπηρεσία – Το όνομα της υπηρεσίας που εκτελείται εκείνη τη στιγμή στον υπολογιστή σας.

Απομακρυσμένος υπολογιστής – Ο απομακρυσμένος υπολογιστής που προσπαθεί να δημιουργήσει επικοινωνία με την εφαρμογή στον υπολογιστή σας.

Τοπική θύρα – Η θύρα που χρησιμοποιείται για την επικοινωνία.

Ερώτηση κάθε φορά – Εάν η προεπιλεγμένη ενέργεια για έναν κανόνα καθορίζεται σε **Ερώτηση**, θα εμφανίζεται ένα παράθυρο διαλόγου κάθε φορά που ενεργοποιείται ο κανόνας.

Απομνημόνευση μέχρι το κλείσιμο της εφαρμογής – Το ESET Internet Security θα απομνημονεύσει την επιλεγμένη ενέργεια μέχρι την επόμενη επανεκκίνηση.

Δημιουργία κανόνα και μόνιμη απομνημόνευση – Εάν ενεργοποιήσετε αυτή την επιλογή προτού επιτρέψετε ή απορρίψετε μια επικοινωνία, το ESET Internet Security θα απομνημονεύσει την ενέργεια και θα τη χρησιμοποιήσει εάν ο απομακρυσμένος υπολογιστής επικοινωνήσει ξανά με την εφαρμογή.

Αποδοχή – Επιτρέπει την εισερχόμενη επικοινωνία.

Δεν επιτρέπεται – Δεν επιτρέπει την εισερχόμενη επικοινωνία.

Επιλογές για προχωρημένους – Σας επιτρέπει να προσαρμόζετε τις ιδιότητες των κανόνων.

Εισερχόμενη επικοινωνία

Παράδειγμα μιας εισερχόμενης σύνδεσης διαδικτύου:
Ένας απομακρυσμένος υπολογιστής προσπαθεί να επικοινωνήσει με μια εφαρμογή που εκτελείται στον υπολογιστή.

Εφαρμογή – Η εφαρμογή με την οποία επικοινωνεί ο απομακρυσμένος υπολογιστής.

Εταιρεία – Ο εκδότης της εφαρμογής.

Φήμη – Η φήμη της εφαρμογής όπως λαμβάνεται από την τεχνολογία ESET LiveGrid®.

Υπηρεσία – Το όνομα της υπηρεσίας που εκτελείται εκείνη τη στιγμή στον υπολογιστή σας.

Απομακρυσμένος υπολογιστής – Ο απομακρυσμένος υπολογιστής που προσπαθεί να δημιουργήσει επικοινωνία με την εφαρμογή στον υπολογιστή σας.

Τοπική θύρα – Η θύρα που χρησιμοποιείται για την επικοινωνία.

Ερώτηση κάθε φορά – Εάν η προεπιλεγμένη ενέργεια για έναν κανόνα καθορίζεται σε **Ερώτηση**, θα εμφανίζεται ένα παράθυρο διαλόγου κάθε φορά που ενεργοποιείται ο κανόνας.

Απομνημόνευση μέχρι το κλείσιμο της εφαρμογής – Το ESET Internet Security θα απομνημονεύσει την επιλεγμένη ενέργεια μέχρι την επόμενη επανεκκίνηση.

Δημιουργία κανόνα και μόνιμη απομνημόνευση – Εάν ενεργοποιήσετε αυτή την επιλογή προτού

επιτρέψετε ή απορρίψετε μια επικοινωνία, το ESET Internet Security θα απομνημονεύσει την ενέργεια και θα τη χρησιμοποιήσει εάν ο απομακρυσμένος υπολογιστής επικοινωνήσει ξανά με την εφαρμογή.

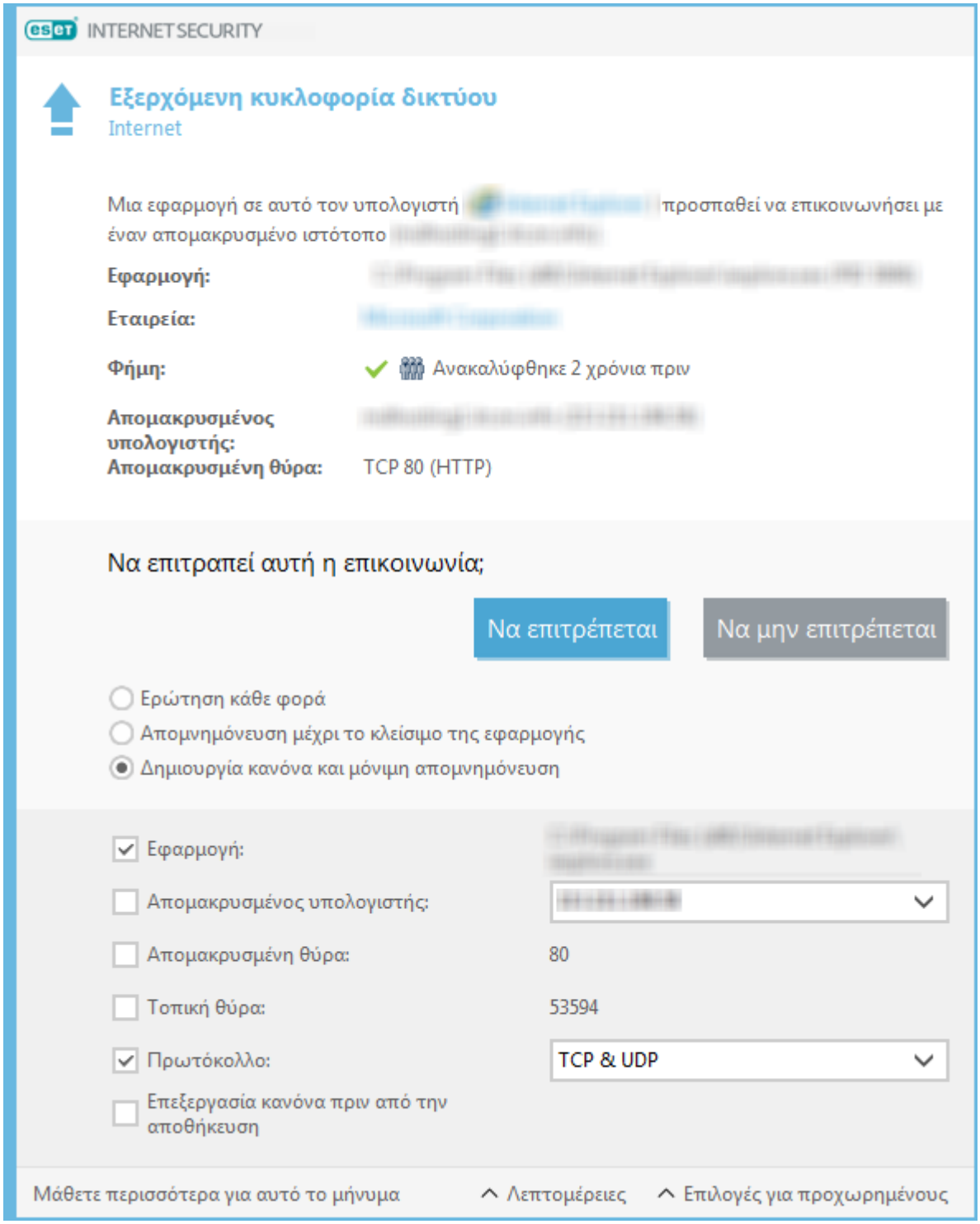
Αποδοχή – Επιτρέπει την εισερχόμενη επικοινωνία.

Δεν επιτρέπεται – Δεν επιτρέπει την εισερχόμενη επικοινωνία.

Επιλογές για προχωρημένους – Σας επιτρέπει να προσαρμόζετε τις ιδιότητες των κανόνων.

Εξερχόμενη επικοινωνία

Παράδειγμα μιας εξερχόμενης σύνδεσης διαδικτύου:
Μια τοπική εφαρμογή προσπαθεί να δημιουργήσει μια σύνδεση στο διαδίκτυο.



Εφαρμογή – Η εφαρμογή με την οποία επικοινωνεί ο απομακρυσμένος υπολογιστής.

Εταιρεία – Ο εκδότης της εφαρμογής.

Φήμη – Η φήμη της εφαρμογής όπως λαμβάνεται από την τεχνολογία ESET LiveGrid®.

Υπηρεσία – Το όνομα της υπηρεσίας που εκτελείται εκείνη τη στιγμή στον υπολογιστή σας.

Απομακρυσμένος υπολογιστής – Ο απομακρυσμένος υπολογιστής που προσπαθεί να δημιουργήσει επικοινωνία με την εφαρμογή στον υπολογιστή σας.

Τοπική θύρα – Η θύρα που χρησιμοποιείται για την επικοινωνία.

Ερώτηση κάθε φορά – Εάν η προεπιλεγμένη ενέργεια για έναν κανόνα καθορίζεται σε **Ερώτηση**, θα εμφανίζεται ένα παράθυρο διαλόγου κάθε φορά που ενεργοποιείται ο κανόνας.

Απομνημόνευση μέχρι το κλείσιμο της εφαρμογής – Το ESET Internet Security θα απομνημονεύσει την επιλεγμένη ενέργεια μέχρι την επόμενη επανεκκίνηση.

Δημιουργία κανόνα και μόνιμη απομνημόνευση – Εάν ενεργοποιήσετε αυτή την επιλογή προτού επιτρέψετε ή απορρίψετε μια επικοινωνία, το ESET Internet Security θα απομνημονεύσει την ενέργεια και θα τη χρησιμοποιήσει εάν ο απομακρυσμένος υπολογιστής επικοινωνήσει ξανά με την εφαρμογή.

Αποδοχή – Επιτρέπει την εισερχόμενη επικοινωνία.

Δεν επιτρέπεται – Δεν επιτρέπει την εισερχόμενη επικοινωνία.

Επιλογές για προχωρημένους – Σας επιτρέπει να προσαρμόζετε τις ιδιότητες των κανόνων.

Ρυθμίσεις προβολής συνδέσεων

Κάντε δεξί κλικ σε μια σύνδεση για να δείτε πρόσθετες επιλογές που περιλαμβάνουν:

Επίλυση ονομάτων κεντρικού υπολογιστή – Εάν είναι δυνατόν, εμφανίζονται όλες οι διευθύνσεις δικτύου σε μορφή DNS και όχι σε μορφή αριθμητικής διεύθυνσης IP.

Να εμφανίζονται μόνο συνδέσεις TCP – Η λίστα εμφανίζει μόνο συνδέσεις που ανήκουν στη σουίτα πρωτοκόλλων TCP.

Εμφάνιση ελεγχόμενων συνδέσεων – Επιλέξτε αυτό το στοιχείο για να εμφανίζονται μόνο συνδέσεις στις οποίες δεν έχει δημιουργηθεί επικοινωνία αυτήν τη στιγμή, αλλά για τις οποίες το σύστημα έχει ανοίξει μια θύρα και αναμένει σύνδεση.

Εμφάνιση συνδέσεων μέσα στον υπολογιστή – Επιλέξτε αυτό το στοιχείο για να εμφανίζονται μόνο συνδέσεις των οποίων η απομακρυσμένη πλευρά είναι ένα τοπικό σύστημα – ονομάζονται επίσης συνδέσεις localhost.

Ταχύτητα ανανέωσης – Επιλέξτε τη συχνότητα για ανανέωση των ενεργών συνδέσεων.

Άμεση ανανέωση – Επαναφορτώνει το παράθυρο **συνδέσεων δικτύου**.

Εργαλεία ασφαλείας

Η ρύθμιση **Εργαλεία ασφαλείας** σάς επιτρέπει να προσαρμόσετε τις ακόλουθες λειτουργικές μονάδες:

- **Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών** – Προσθέτει ένα επιπλέον επίπεδο προστασίας στο πρόγραμμα περιήγησης που έχει σχεδιαστεί για να προστατεύει τα οικονομικά δεδομένα σας κατά τη διάρκεια ηλεκτρονικών συναλλαγών. Ενεργοποιήστε το στοιχείο **Προστασία όλων των προγραμμάτων περιήγησης** ώστε όλα τα υποστηριζόμενα προγράμματα περιήγησης να εκκινούν σε ασφαλή λειτουργία. Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών.

• **Γονικός έλεγχος** – Η λειτουργική μονάδα Γονικός έλεγχος προστατεύει τα παιδιά σας αποτρέποντας ακατάλληλο ή επιβλαβές περιεχόμενο στο Internet.

• **Anti-Theft** – Ενεργοποιήστε το Anti-Theft για να προστατέψετε τον υπολογιστή σας σε περίπτωση απώλειας ή κλοπής.

Προστασία τραπεζικών πληρωμών

Η Προστασία τραπεζικών πληρωμών είναι ένα πρόσθετο επίπεδο προστασίας που έχει σχεδιαστεί για να προστατεύει τα οικονομικά δεδομένα σας κατά τη διάρκεια ηλεκτρονικών συναλλαγών.

Στις περισσότερες περιπτώσεις, μόλις επισκεφτείτε έναν γνωστό ιστότοπο τραπεζικών συναλλαγών, εκκινεί το ασφαλές πρόγραμμα περιήγησης για την Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών στο τρέχον πρόγραμμα περιήγησης.

Ορίστε μία από τις ακόλουθες επιλογές ρύθμισης παραμέτρων συμπεριφοράς του ασφαλούς προγράμματος περιήγησης:

• **Προστασία όλων των προγραμμάτων περιήγησης** - Εάν ενεργοποιηθεί, όλα τα υποστηριζόμενα προγράμματα περιήγησης εκκινούν σε ασφαλή λειτουργία. Αυτό σας επιτρέπει να περιηγηθείτε στο διαδίκτυο, να αποκτήσετε πρόσβαση σε τραπεζικές συναλλαγές στο διαδίκτυο και να πραγματοποιήσετε ηλεκτρονικές αγορές και συναλλαγές σε ένα παράθυρο ασφαλούς προγράμματος περιήγησης χωρίς ανακατεύθυνση.

• **Ανακατεύθυνση ιστότοπων** (προεπιλογή) - Ιστότοποι από μια λίστα προστατευμένων ιστότοπων και εσωτερική λίστα τραπεζικών συναλλαγών στο διαδίκτυο ανακατευθύνουν στο ασφαλές πρόγραμμα περιήγησης. Μπορείτε να επιλέξετε το πρόγραμμα περιήγησης (τυπικό ή ασφαλές) που θα ανοίξει.

• Οι δύο προηγούμενες επιλογές είναι απενεργοποιημένες - Για να αποκτήσετε πρόσβαση σε ένα ασφαλές πρόγραμμα περιήγησης στο ESET Internet Security, κάντε κλικ στα στοιχεία **Εργαλεία** > **Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών** ή κάντε κλικ στο εικονίδιο της επιφάνειας εργασίας **Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών**. Το πρόγραμμα περιήγησης που έχει ρυθμιστεί ως προεπιλεγμένο στα Windows εκκινεί σε ασφαλή λειτουργία.

Για να ρυθμίσετε τις παραμέτρους της συμπεριφοράς του ασφαλούς προγράμματος περιήγησης, ανατρέξτε στο θέμα Ρυθμίσεις για προχωρημένους της Προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών. Για να ενεργοποιήσετε τη δυνατότητα «Προστασία όλων των προγραμμάτων περιήγησης» στο ESET Internet Security, κάντε κλικ στο στοιχείο **Ρυθμίσεις** > **Εργαλεία ασφαλείας** και ενεργοποιήστε το ρυθμιστικό **Προστασία όλων των προγραμμάτων περιήγησης**.

Η χρήση κρυπτογραφημένης επικοινωνίας HTTPS είναι απαραίτητη για την πραγματοποίηση προστατευόμενης περιήγησης. Τα παρακάτω προγράμματα περιήγησης υποστηρίζουν την Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών:

• Internet Explorer 8.0.0.0+

• Microsoft Edge 83.0.0.0+

• Google Chrome 64.0.0.0+

- Firefox 24.0.0.0+

Για περισσότερες λεπτομέρειες σχετικά με τις δυνατότητες προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών, ανατρέξτε στο άρθρο της Γνωσιακής βάσης της ESET που είναι διαθέσιμο στα Αγγλικά και αρκετές άλλες γλώσσες:

- Πώς μπορώ να χρησιμοποιήσω την προστασία τραπεζικών πληρωμών της ESET;
- Ενεργοποίηση ή απενεργοποίηση της Προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών ESET για έναν συγκεκριμένο ιστότοπο
- Παύση ή απενεργοποίηση της Προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών της ESET σε οικιακά προϊόντα για Windows
- Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών της ESET –συνήθη σφάλματα
- Γλωσσάρι της ESET | Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών

Ρυθμίσεις για προχωρημένους για την Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών

Αυτή η ρύθμιση είναι διαθέσιμη στην ενότητα **Εγκατάσταση για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών**.

Βασικό

Ενεργοποίηση προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών – Μόλις ενεργοποιηθεί η επιλογή Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών, θα γίνει ενεργή η λίστα προστατευόμενων ιστότοπων, η οποία σάς επιτρέπει να επεξεργαστείτε τη λίστα Προστατευόμενων ιστότοπων.

Προστασία προγράμματος περιήγησης

Προστασία όλων των προγραμμάτων περιήγησης – Ενεργοποιήστε αυτή την επιλογή για να εκκινούν όλα τα υποστηριζόμενα προγράμματα περιήγησης σε ασφαλή λειτουργία.

Λειτουργία εγκατάστασης επεκτάσεων – Από το αναπτυσσόμενο μενού, μπορείτε να επιλέξετε τις επεκτάσεις των οποίων η εγκατάσταση θα επιτρέπεται σε ένα πρόγραμμα περιήγησης που προστατεύεται από την ESET: Η αλλαγή της λειτουργίας εγκατάστασης επεκτάσεων δεν επηρεάζει τις επεκτάσεις του προγράμματος περιήγησης που έχουν εγκατασταθεί προηγουμένως:

- **Απαραίτητες επεκτάσεις** – Μόνο οι πιο απαραίτητες επεκτάσεις που αναπτύχθηκαν από έναν συγκεκριμένο κατασκευαστή προγράμματος περιήγησης.
- **Όλες οι επεκτάσεις** – Όλες οι επεκτάσεις που υποστηρίζονται από ένα συγκεκριμένο πρόγραμμα περιήγησης.

Ανακατεύθυνση ιστότοπων

Ενεργοποίηση ανακατεύθυνσης προστατευόμενων ιστότοπων – Εάν ενεργοποιηθεί η λειτουργία, οι ιστότοποι από τη λίστα προστατευόμενων ιστότοπων και την εσωτερική λίστα ιστότοπων τραπεζικών συναλλαγών μέσω Internet θα ανακατευθύνονται στο ασφαλές πρόγραμμα περιήγησης.

Προστατευόμενοι ιστότοποι –- Μια λίστα ιστότοπων για τους οποίους μπορείτε να επιλέξετε το πρόγραμμα περιήγησης (κανονικό ή ασφαλές) με το οποίο θα ανοίγουν. Στο πλαίσιο του προγράμματος περιήγησης θα εμφανίζεται ένα λογότυπο της ESET που θα δηλώνει ότι η ασφαλής περιήγηση είναι ενεργή. Για να επεξεργαστείτε τη λίστα, ανατρέξτε στο θέμα Προστατευμένοι ιστότοποι.

Ασφαλές πρόγραμμα περιήγησης

Ενεργοποίηση βελτιωμένης προστασίας μνήμης – Εάν ενεργοποιηθεί η λειτουργία, η μνήμη του ασφαλούς προγράμματος περιήγησης θα προστατεύεται από τον έλεγχο από άλλες διεργασίες.

Ενεργοποίηση της προστασίας πληκτρολογίου – Εάν ενεργοποιηθεί, οι πληροφορίες που εισάγονται μέσω πληκτρολογίου σε ασφαλές πρόγραμμα περιήγησης θα είναι κρυφές για τις άλλες εφαρμογές. Αυτό αυξάνει την προστασία από προγράμματα καταγραφής χειρισμών πληκτρολογίου (keyloggers).

Πράσινο πλαίσιο του προγράμματος περιήγησης - Εάν απενεργοποιηθεί, η ενημερωτική ειδοποίηση εντός του προγράμματος περιήγησης και το πράσινο πλαίσιο γύρω από το πρόγραμμα περιήγησης θα εμφανιστούν στιγμιαία κατά την εκκίνηση του προγράμματος περιήγησης και στη συνέχεια θα εξαφανιστούν.

Προστατευόμενοι ιστότοποι

Τα ESET Internet Security περιλαμβάνουν μια ενσωματωμένη λίστα προκαθορισμένων ιστότοπων που ενεργοποιούν το άνοιγμα ενός Ασφαλούς προγράμματος περιήγησης. Μπορείτε να προσθέσετε έναν ιστότοπο ή να επεξεργαστείτε τη λίστα ιστότοπων στη ρύθμιση παραμέτρων του προϊόντος.

Μπορείτε να δείτε και να επεξεργαστείτε τη λίστα **Προστατευόμενοι ιστότοποι** στην ενότητα **Εγκατάσταση για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών** > **Βασικές ρυθμίσεις** > **Προστατευόμενοι ιστότοποι** > **Επεξεργασία**. Το παράθυρο αποτελείται από:

Στήλες

Ιστότοπος – Προστατευόμενος ιστότοπος.

Ασφαλές πρόγραμμα περιήγησης – Το λογότυπο ESET θα εμφανίζεται στο πλαίσιο του προγράμματος περιήγησης κατά τη διάρκεια της ασφαλούς περιήγησης.

Να γίνεται ερώτηση – Όταν είναι ενεργοποιημένο, θα εμφανίζεται ένα παράθυρο διαλόγου με επιλογές περιήγησης κάθε φορά που επισκέπτεστε έναν προστατευόμενο ιστότοπο. Το ESET Internet Security μπορεί να απομνημονεύσει την ενέργειά σας ή μπορείτε να επιλέξετε μη αυτόματα τον τρόπο με τον οποίο θα συνεχίσετε.

Κανονικό πρόγραμμα περιήγησης – Ενεργοποιήστε αυτή την επιλογή για να συνεχίσετε μια τραπεζική συναλλαγή χωρίς πρόσθετη ασφάλεια.

Στοιχεία ελέγχου

Προσθήκη – Σας επιτρέπει να προσθέσετε έναν ιστότοπο στη λίστα γνωστών ιστότοπων.

Επεξεργασία – Σας επιτρέπει να επεξεργαστείτε τις επιλεγμένες καταχωρίσεις.

Διαγραφή – Καταργεί επιλεγμένες καταχωρίσεις.

Εισαγωγή/Εξαγωγή - Σας επιτρέπει να εξαγάγετε τη λίστα προστατευμένων ιστότοπων και να την εισαγάγετε σε μια νέα συσκευή.

Ειδοποίηση εντός του προγράμματος περιήγησης

Το ασφαλές πρόγραμμα περιήγησης σάς ενημερώνει για την τρέχουσα κατάστασή του μέσω ειδοποιήσεων εντός του προγράμματος περιήγησης και μέσω του χρώματος του πλαισίου του προγράμματος περιήγησης.

Οι ειδοποιήσεις εντός του προγράμματος περιήγησης εμφανίζονται στην καρτέλα στη δεξιά πλευρά.

Για να αναπτύξετε την ειδοποίηση εντός του προγράμματος περιήγησης, κάντε κλικ στο εικονίδιο της ESET. Για να ελαχιστοποιήσετε την ειδοποίηση, κάντε κλικ στο κείμενο της ειδοποίησης. Για να απορρίψετε την ειδοποίηση, κάντε κλικ στο εικονίδιο κλεισίματος.

Ειδοποιήσεις εντός του προγράμματος περιήγησης

Τύπος ειδοποίησης	Κατάσταση
Ενημερωτική ειδοποίηση και πράσινο πλαίσιο προγράμματος περιήγησης	Η μέγιστη προστασία διασφαλίζεται και η ειδοποίηση εντός του προγράμματος περιήγησης ελαχιστοποιείται από προεπιλογή. Αναπτύξτε την ειδοποίηση εντός του προγράμματος περιήγησης για να εμφανίζονται οι επιλογές ρύθμισης παραμέτρων: • **Απόκρυψη του πράσινου πλαισίου του προγράμματος περιήγησης** – Επιλέξτε το πλαίσιο ελέγχου για να αποκρύψετε το πράσινο πλαίσιο που περιβάλλει το πρόγραμμα περιήγησης όταν απορρίπτεται η ειδοποίηση. Μπορείτε να απενεργοποιήσετε μόνιμα την ενημερωτική ειδοποίηση εντός του προγράμματος περιήγησης και το πράσινο πλαίσιο που περιβάλλει το πρόγραμμα περιήγησης στην οθόνη Ρυθμίσεις για προχωρημένους για την Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών. • **Ρυθμίσεις** – Ανοίγει τις ρυθμίσεις για τα Εργαλεία ασφαλείας.

Τύπος ειδοποίησης	Κατάσταση
Προειδοποίηση και πορτοκαλί πλαίσιο προγράμματος περιήγησης	Το ασφαλές πρόγραμμα περιήγησης απαιτεί την προσοχή σας για ένα μη κρίσιμο ζήτημα. Για περισσότερες πληροφορίες σχετικά με το ζήτημα ή μια λύση, ακολουθήστε τις οδηγίες στην ειδοποίηση εντός του προγράμματος περιήγησης.
Συναγερμός ασφάλειας και κόκκινο πλαίσιο προγράμματος περιήγησης	Το πρόγραμμα περιήγησης δεν προστατεύεται από την Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών της ESET. Πραγματοποιήστε επανεκκίνηση του προγράμματος περιήγησης για να διασφαλίσετε ότι η προστασία είναι ενεργή. Για να επιλύσετε μια διένεξη με αρχεία που έχουν φορτωθεί στο πρόγραμμα περιήγησης, επικοινωνήστε με την Τεχνική υποστήριξη της ESET ακολουθώντας τις οδηγίες στο άρθρο της Γνωσιακής βάσης.

Γονικός έλεγχος

Η μονάδα Γονικού ελέγχου σάς επιτρέπει να διαμορφώνετε ρυθμίσεις γονικού ελέγχου, οι οποίες παρέχουν στους γονείς αυτοματοποιημένα εργαλεία με τα οποία προστατεύουν τα παιδιά και καθορίζουν περιορισμούς για συσκευές και υπηρεσίες. Στόχος είναι να μην επιτρέπεται στα παιδιά και τους εφήβους η πρόσβαση σε σελίδες με ακατάλληλο ή επιβλαβές περιεχόμενο.

Ο Γονικός έλεγχος σάς επιτρέπει να αποκλείετε ιστοσελίδες που ενδέχεται να περιέχουν ενδεχομένως προσβλητικό περιεχόμενο. Επιπλέον, οι γονείς μπορούν να εμποδίζουν την πρόσβαση σε περισσότερες από 40 προκαθορισμένες κατηγορίες ιστότοπων και περισσότερες από 140 υποκατηγορίες.

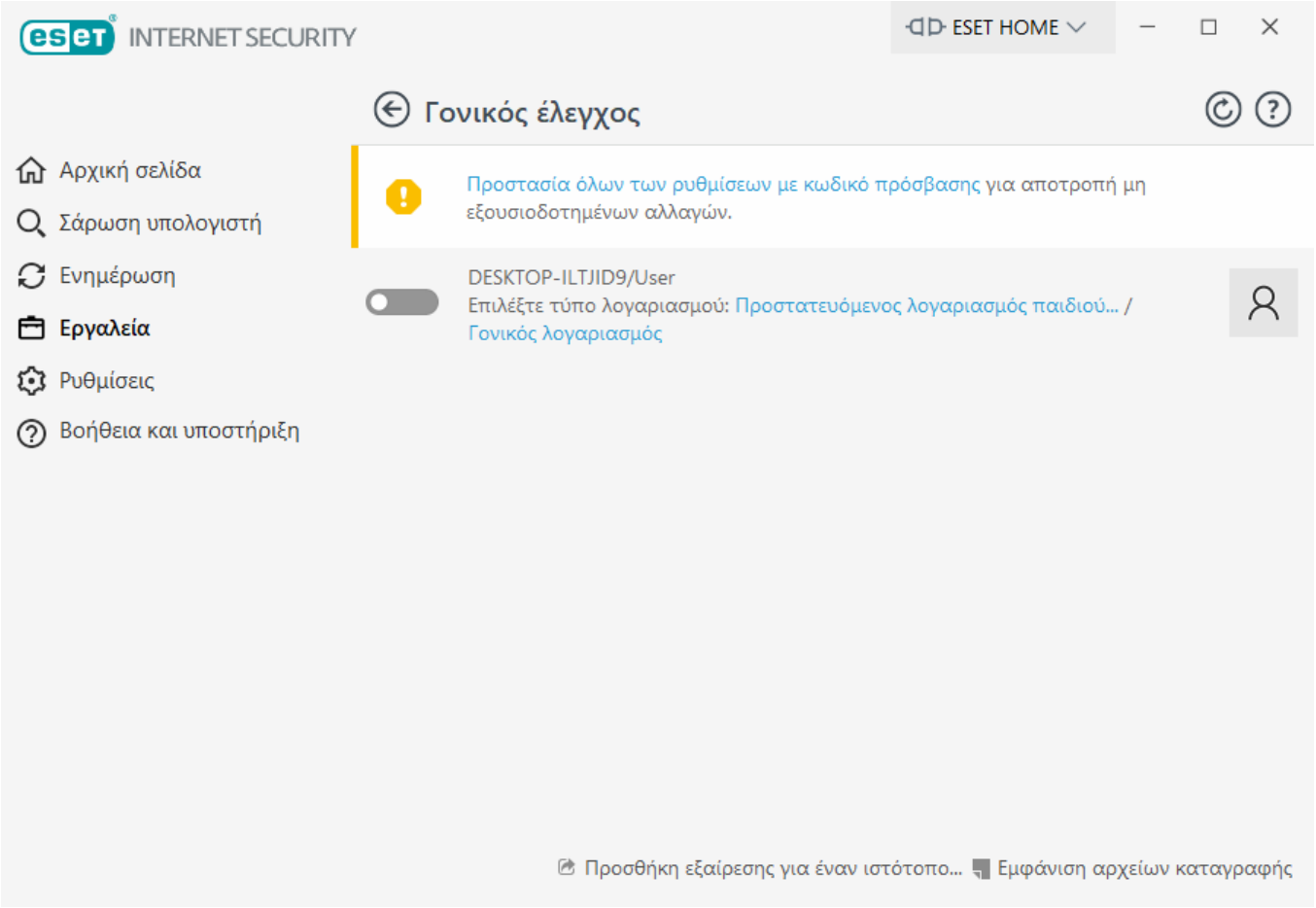
Για να ενεργοποίησετε τον Γονικό έλεγχο για ένα συγκεκριμένο λογαριασμό χρήστη, ακολουθήστε τα παρακάτω βήματα:

1. Ο Γονικός έλεγχος είναι απενεργοποιημένος από προεπιλογή στο ESET Internet Security. Υπάρχουν δύο μέθοδοι για την ενεργοποίηση του Γονικού ελέγχου:

   • Κάντε κλικ στο στοιχείο  στη θέση **Ρυθμίσεις** > **Εργαλεία ασφαλείας** > **Γονικός έλεγχος** από το κύριο παράθυρο του προγράμματος και αλλάξτε την κατάσταση του Γονικού ελέγχου σε ενεργό.

   • Πιέστε το πλήκτρο F5 για να αποκτήσετε πρόσβαση στη δομή **Εγκατάσταση για προχωρημένους**, μεταβείτε στο στοιχείο **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Γονικός έλεγχος** και, στη συνέχεια, ενεργοποιήστε το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Ενεργοποίηση Γονικού ελέγχου**.

2. Κάντε κλικ στα στοιχεία **Ρυθμίσεις** > **Εργαλεία ασφαλείας** > **Γονικός έλεγχος** από το κύριο παράθυρο του προγράμματος. Παρόλο που εμφανίζεται η ένδειξη **Ενεργοποιημένο** δίπλα από το στοιχείο **Γονικός έλεγχος**, πρέπει να ρυθμίσετε τις παραμέτρους για τον γονικό έλεγχο για το λογαριασμό που επιθυμείτε κάνοντας κλικ στο σύμβολο βέλους και στη συνέχεια επιλέγοντας στο επόμενο παράθυρο **Προστατευόμενος λογαριασμός παιδιού** ή **Γονικός λογαριασμός**. Στο επόμενο παράθυρο επιλέξτε την ημερομηνία γέννησης, για να προσδιοριστεί το επίπεδο πρόσβασης και οι συνιστώμενες ιστοσελίδες που είναι κατάλληλες για την ηλικία. Ο Γονικός έλεγχος θα είναι τώρα ενεργός για τον καθορισμένο λογαριασμό χρήστη. Κάντε κλικ στο στοιχείο **Αποκλεισμένο περιεχόμενο και ρυθμίσεις** κάτω από το όνομα λογαριασμού για να προσαρμόσετε τις κατηγορίες που θέλετε να επιτρέπονται ή να αποκλείονται στην καρτέλα Κατηγορίες. Για να επιτρέπονται ή να αποκλείονται προσαρμοσμένες ιστοσελίδες που δεν αντιστοιχούν σε μια κατηγορία, κάντε κλικ στην καρτέλα Εξαιρέσεις.



Εάν μεταβείτε στη θέση **Ρυθμίσεις** > **Εργαλεία ασφαλείας** > **Γονικός έλεγχος** από το κύριο παράθυρο του ESET Internet Security, θα δείτε ότι το κύριο παράθυρο περιέχει τα εξής στοιχεία:

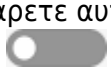
Λογαριασμοί χρηστών των Windows

Εάν έχετε δημιουργήσει έναν ρόλο για έναν υπάρχοντα λογαριασμό, θα εμφανίζεται εδώ. Κάντε κλικ στο ρυθμιστικό έτσι ώστε να εμφανιστεί ένα πράσινο σημάδι ελέγχου δίπλα στον Γονικό έλεγχο για τον λογαριασμό. Στον ενεργό λογαριασμό, κάντε κλικ στο στοιχείο Αποκλεισμένο περιεχόμενο και ρυθμίσεις για να δείτε τη λίστα επιτρεπόμενων κατηγοριών ιστοσελίδων για αυτόν το λογαριασμό και των αποκλεισμένων και μη αποκλεισμένων ιστοσελίδων.

Για να δημιουργήσετε έναν νέο λογαριασμό (για παράδειγμα για ένα παιδί), χρησιμοποιήστε τις ακόλουθες οδηγίες βήμα-βήμα για Windows 7 ή Windows Vista:
1.Ανοίξτε το στοιχείο **Λογαριασμοί χρηστών** κάνοντας κλικ στο κουμπί **Έναρξη** (βρίσκεται στην κάτω αριστερή πλευρά της επιφάνειας εργασίας), κάντε κλικ στο στοιχείο **Πίνακας ελέγχου** και μετά στο στοιχείο **Λογαριασμοί χρηστών**.
2.Κάντε κλικ στο στοιχείο **Διαχείριση λογαριασμού χρήστη**. Αν σας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση, πληκτρολογήστε τον κωδικό πρόσβασης και επιβεβαιώστε.
3.Κάντε κλικ στην επιλογή **Δημιουργία νέου λογαριασμού**.
4.Πληκτρολογήστε το όνομα που θέλετε να δώσετε στον λογαριασμό χρήστη, κάντε κλικ σε έναν τύπο λογαριασμού και μετά στο στοιχείο **Δημιουργία λογαριασμού**.
5.Ανοίξτε ξανά το παράθυρο Γονικού ελέγχου κάνοντας πάλι κλικ από το κύριο παράθυρο προγράμματος του ESET Internet Security στη διαδρομή **Ρυθμίσεις** > **Εργαλεία ασφαλείας** > **Γονικός έλεγχος** και κάντε κλικ στο σύμβολο βέλους.

Το κάτω μέρος του παραθύρου περιέχει

Προσθήκη εξαίρεσης για έναν ιστότοπο – Ο συγκεκριμένος ιστότοπος μπορεί να επιτραπεί ή να αποκλειστεί ανάλογα με τις προτιμήσεις σας για κάθε γονικό λογαριασμό ξεχωριστά.

Εμφάνιση αρχείων καταγραφής – Με αυτή την επιλογή εμφανίζεται ένα λεπτομερές αρχείο καταγραφής της δραστηριότητας Γονικού ελέγχου (αποκλεισμένες σελίδες, ο λογαριασμός για τον οποίο αποκλείστηκε η σελίδα, η κατηγορία κ.λπ.). Επίσης μπορείτε να φιλτράρετε αυτό το αρχείο καταγραφής με βάση τα κριτήρια που επιλέγετε κάνοντας κλικ στο στοιχείο  **Φιλτράρισμα**.

Γονικός έλεγχος

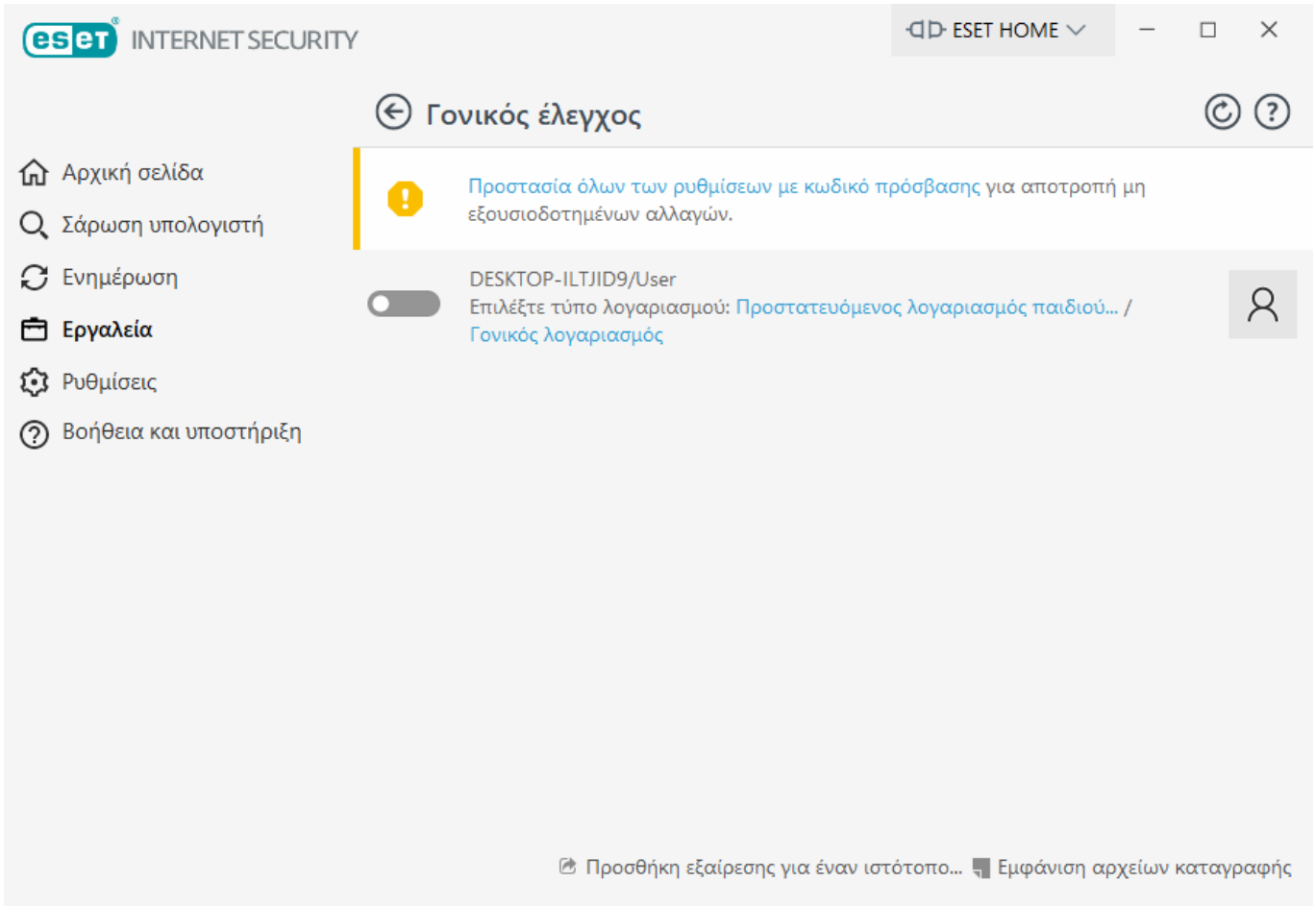
Μετά την απενεργοποίηση του Γονικού ελέγχου, εμφανίζεται ένα παράθυρο **Απενεργοποίηση γονικού ελέγχου**. Εδώ μπορείτε να ορίσετε το χρονικό διάστημα για το οποίο θα είναι απενεργοποιημένη η προστασία. Η επιλογή τότε αλλάζει σε **Σε παύση** ή **Οριστικά απενεργοποιημένο**.

Είναι σημαντικό να προστατεύετε τις ρυθμίσεις στο ESET Internet Security με κωδικό πρόσβασης. Αυτός ο κωδικός πρόσβασης μπορεί να ρυθμιστεί στην ενότητα Ρύθμιση πρόσβασης. Εάν δεν έχει καθοριστεί κωδικός πρόσβασης, θα εμφανιστεί η ακόλουθη προειδοποίηση – **Προστασία όλων των ρυθμίσεων με κωδικό πρόσβασης** για αποτροπή μη εξουσιοδοτημένων αλλαγών. Οι περιορισμοί που ορίζονται στον Γονικό έλεγχο επηρεάζουν μόνο τους τυπικούς λογαριασμούς χρηστών. Επειδή ο Διαχειριστής μπορεί να παρακάμψει κάθε περιορισμό δεν θα επηρεαστεί καθόλου.

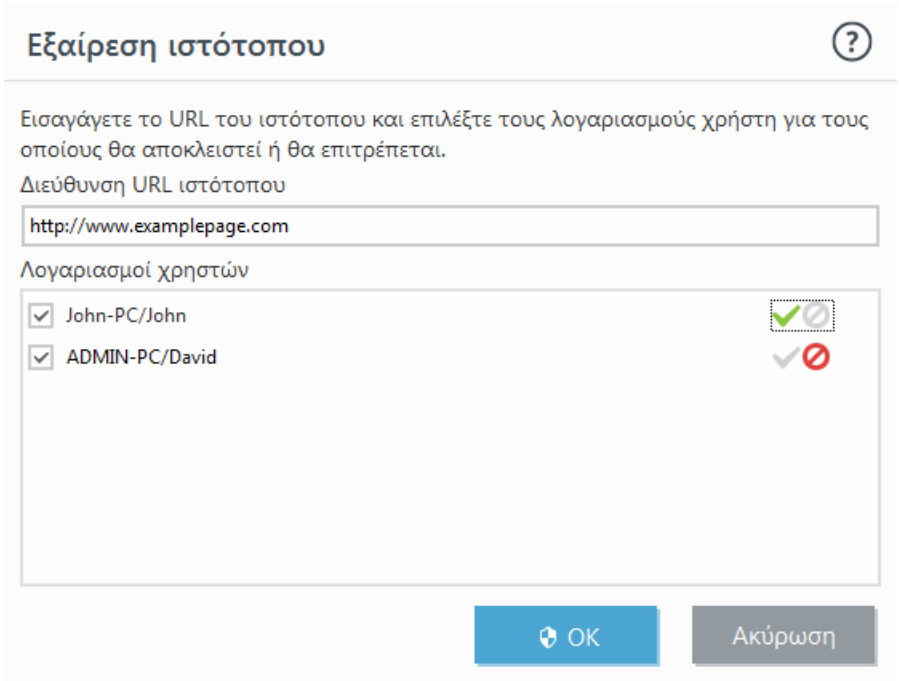
> Για να λειτουργήσει σωστά, ο Γονικός έλεγχος απαιτεί να είναι ενεργό το Φιλτράρισμα περιεχομένου από το πρωτόκολλο εφαρμογής, ο Έλεγχος πρωτοκόλλου HTTP και το Firewall. Όλες αυτές οι λειτουργικότητες είναι ενεργοποιημένες από προεπιλογή.

Εξαιρέσεις ιστότοπων

Για να προσθέσετε μια εξαίρεση σε έναν ιστότοπο, κάντε κλικ στα στοιχεία **Ρύθμιση** > **Εργαλεία ασφάλειας** > **Γονικός έλεγχος** και, στη συνέχεια, κάντε κλικ στο στοιχείο **Προσθήκη εξαίρεσης για έναν ιστότοπο**.

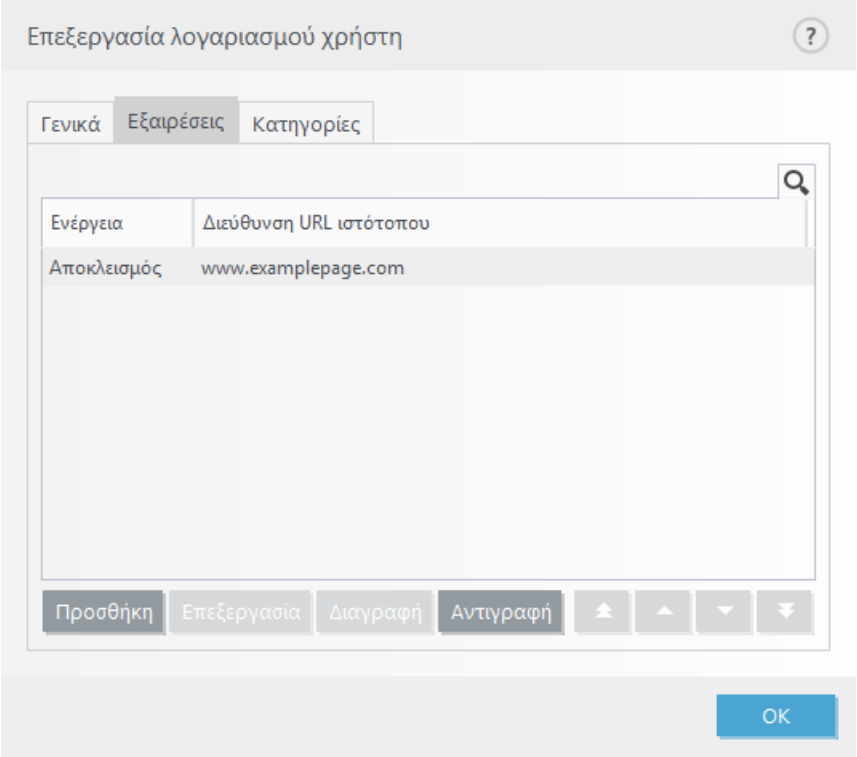


Εισαγάγετε μια διεύθυνση URL στο πεδίο **URL ιστότοπου**, επιλέξτε ✔ (επιτρέπεται) ή ⊘ (αποκλεισμός) για κάθε συγκεκριμένο λογαριασμό χρήστη και, στη συνέχεια, κάντε κλικ στο **OK** για να τον προσθέσετε στη λίστα.



Για να διαγράψετε μια διεύθυνση URL από τη λίστα, κάντε κλικ στο στοιχείο **Ρυθμίσεις** > **Εργαλεία ασφαλείας** > **Γονικός έλεγχος**, επιλέξτε **Αποκλεισμένο περιεχόμενο και ρυθμίσεις** κάτω από το λογαριασμό χρήστη που θέλετε, κάντε κλικ στην καρτέλα **Εξαίρεση**, επιλέξτε την εξαίρεση και, στη

συνέχεια, κάντε κλικ στην επιλογή **Κατάργηση**.



Στη λίστα διευθύνσεων URL, δεν είναι δυνατή η χρήση των ειδικών συμβόλων * (αστερίσκος) και ? (ερωτηματικό). Για παράδειγμα, οι διευθύνσεων ιστοσελίδων με πολλαπλούς τομείς ανώτατου επιπέδου (top-level domain ή TLD) πρέπει να εισάγονται μη αυτόματα (examplepage.com*examplepage.com*, *examplepage.sk*examplepage.sk κ.λπ.). Όταν προσθέτετε έναν τομέα στη λίστα, όλο το περιεχόμενο που βρίσκεται σε αυτόν τον τομέα και σε όλους δευτερεύοντες τομείς (για παράδειγμα, sub.examplepage.com*sub.examplepage.com*) θα αποκλείεται ή θα επιτρέπεται ανάλογα με την ενέργεια που επιλέγετε για την αντίστοιχη διεύθυνση URL.

Ο αποκλεισμός ή η αποδοχή μιας συγκεκριμένης ιστοσελίδας μπορεί να είναι πιο ακριβής από τον αποκλεισμό ή την αποδοχή μιας κατηγορίας ιστοσελίδων. Απαιτείται προσοχή όταν αλλάζετε αυτές τις ρυθμίσεις και προσθέτετε μια κατηγορία/ιστοσελίδα στη λίστα.

Λογαριασμοί χρηστών

Αυτή η ρύθμιση είναι διαθέσιμη στο στοιχείο **Εγκατάσταση για προχωρημένους** (F5) > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Γονικός έλεγχος** > **Λογαριασμοί χρηστών** > **Επεξεργασία**.

Σε αυτή την ενότητα μπορείτε να συσχετίσετε λογαριασμούς χρηστών των Windows που χρησιμοποιούνται από τον γονικό έλεγχο με συγκεκριμένους χρήστες, για να περιορίσετε την πρόσβασή τους σε ακατάλληλο ή επιβλαβές περιεχόμενο στο διαδίκτυο.

Στήλες

Λογαριασμός των Windows – Το όνομα του χρήστη.

Ενεργό – Όταν είναι ενεργοποιημένο, ενεργοποιούνται οι γονικοί έλεγχοι για έναν συγκεκριμένο λογαριασμό χρήστη.

Τομέας – Το όνομα του τομέα στον οποίο ανήκει ένας χρήστης.

Ημερομηνία γέννησης – Η ηλικία του χρήστη στον οποίο ανήκει αυτός ο λογαριασμός.

Στοιχεία ελέγχου

Προσθήκη – Εμφανίζεται το παράθυρο διαλόγου Εργασία με λογαριασμούς χρηστών.

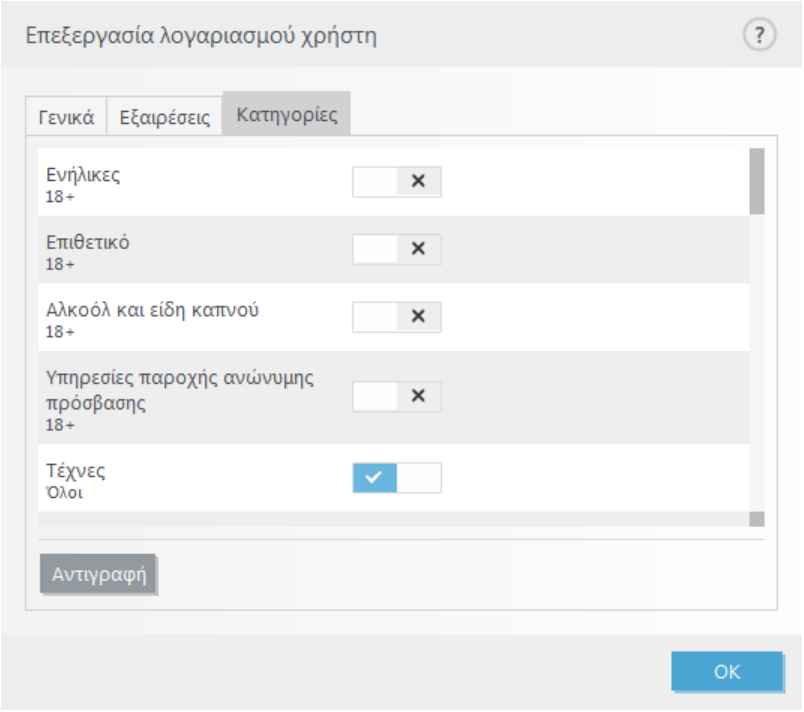
Επεξεργασία – Η επιλογή αυτή σάς επιτρέπει να επεξεργαστείτε τους επιλεγμένους λογαριασμούς.

Διαγραφή – Διαγράφει τον επιλεγμένο λογαριασμό.

Ανανέωση – Εάν έχετε προσθέσει λογαριασμό χρήστη, το ESET Internet Security μπορεί να ανανεώσει τη λίστα λογαριασμών χρηστών χωρίς να χρειάζεται να ανοίξει ξανά αυτό το παράθυρο.

Κατηγορίες

Επιλέξτε το πλαίσιο ελέγχου στη στήλη **Ενεργό** που βρίσκεται δίπλα σε μια κατηγορία, για να επιτρέπεται αυτή η κατηγορία. Εάν αφήσετε το πλαίσιο ελέγχου άδειο, η κατηγορία δεν θα επιτρέπεται για τον συγκεκριμένο λογαριασμό.



Παρακάτω παρατίθενται ορισμένα παραδείγματα κατηγοριών (ομάδων) τις οποίες μπορεί να γνωρίζουν οι χρήστες:

• **Διάφορα** – Συνήθως ιδιωτικές (τοπικές) διευθύνσεις IP όπως intranet, 127.0.0.0/8, 192.168.0.0/16, κ.λπ. Όταν λαμβάνετε κωδικό σφάλματος 403 ή 404, ο ιστότοπος θα αντιστοιχεί επίσης σε αυτή την κατηγορία.

• **Δεν έχει επιλυθεί** – Αυτή η κατηγορία περιλαμβάνει ιστοσελίδες που δεν έχουν επιλυθεί εξαιτίας σφάλματος κατά τη σύνδεση με το μηχανισμό βάσης δεδομένων του Γονικού ελέγχου.

• **Δεν έχει κατηγοριοποιηθεί** – Άγνωστες ιστοσελίδες που δεν βρίσκονται ακόμα στη βάση δεδομένων Γονικού ελέγχου.

• **Δυναμικές** – Ιστοσελίδες που ανακατευθύνουν σε άλλες σελίδες σε άλλους ιστότοπους.

Εργασία με λογαριασμούς χρηστών

Το παράθυρο διαθέτει τρεις καρτέλες:

Γενικά

Κάντε κλικ στη γραμμή ρυθμιστικού που βρίσκεται δίπλα στο στοιχείο **Ενεργοποίηση** για να ενεργοποιήσετε τον Γονικό έλεγχο για τον λογαριασμό Windows που θα επιλεχτεί παρακάτω.

Πρώτα κάντε κλικ στο στοιχείο **Επιλογή**, για να επιλέξετε έναν λογαριασμό Windows από τον υπολογιστή σας. Οι περιορισμοί που ορίζονται στον γονικό έλεγχο επηρεάζουν μόνο τους τυπικούς λογαριασμούς των Windows. Οι λογαριασμοί διαχειριστών μπορούν να παρακάμπτουν τυχόν περιορισμούς.

Εάν ο λογαριασμός χρησιμοποιείται από γονέα, επιλέξτε **Γονικός λογαριασμός**.

Ρυθμίστε την **Ημερομηνία γέννησης παιδιού** για τον λογαριασμό, για να προσδιοριστεί το επίπεδο πρόσβασης και για να ρυθμίσετε κανόνες πρόσβασης για ιστοσελίδες κατάλληλες για την επιλεγμένη ηλικία.

Καταγραφή κρισιμότητας

Το ESET Internet Security αποθηκεύει όλα τα σημαντικά συμβάντα σε ένα αρχείο καταγραφής, το οποίο μπορείτε να προβάλετε απευθείας από το κύριο μενού. Κάντε κλικ στα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής** και κατόπιν επιλέξτε **Γονικός έλεγχος** από το αναπτυσσόμενο μενού **Καταγραφή**.

• **Εγγραφές διαγνωστικού ελέγχου** – Καταγράφει πληροφορίες απαραίτητες για τη ρύθμιση του προγράμματος.

• **Πληροφορίες** – Καταγράφει ενημερωτικά μηνύματα, συμπεριλαμβανομένων μη αποκλεισμένων και αποκλεισμένων εξαιρέσεων, καθώς και όλων των παραπάνω εγγραφών.

• **Προειδοποίηση** – Καταγράφει κρίσιμα σφάλματα και προειδοποιητικά μηνύματα.

• **Καμία** – Δεν καταγράφονται εγγραφές.

Εξαιρέσεις

Η δημιουργία εξαίρεσης μπορεί να επιτρέπει ή να απαγορεύει την πρόσβαση ενός χρήστη σε ιστότοπους που δεν βρίσκονται στις λίστα εξαιρέσεων. Αυτό είναι χρήσιμο εάν θέλετε να ελέγχετε την πρόσβαση σε συγκεκριμένους ιστότοπους αντί να χρησιμοποιείτε κατηγορίες. Οι εξαιρέσεις που δημιουργήθηκαν για έναν λογαριασμό μπορούν να αντιγραφούν και να χρησιμοποιηθούν για κάποιον άλλο λογαριασμό. Αυτό μπορεί να είναι χρήσιμο όταν θέλετε να δημιουργήσετε πανομοιότυπους κανόνες για παιδιά παρόμοιας ηλικίας.

Κάντε κλικ στο στοιχείο **Προσθήκη** για να δημιουργήσετε μια νέα εξαίρεση. Καθορίστε την **Ενέργεια** (για παράδειγμα, **Αποκλεισμός**) χρησιμοποιώντας το αναπτυσσόμενο μενού, πληκτρολογήστε τη **Διεύθυνση URL ιστότοπου** στην οποία θα εφαρμόζεται αυτή η εξαίρεση και

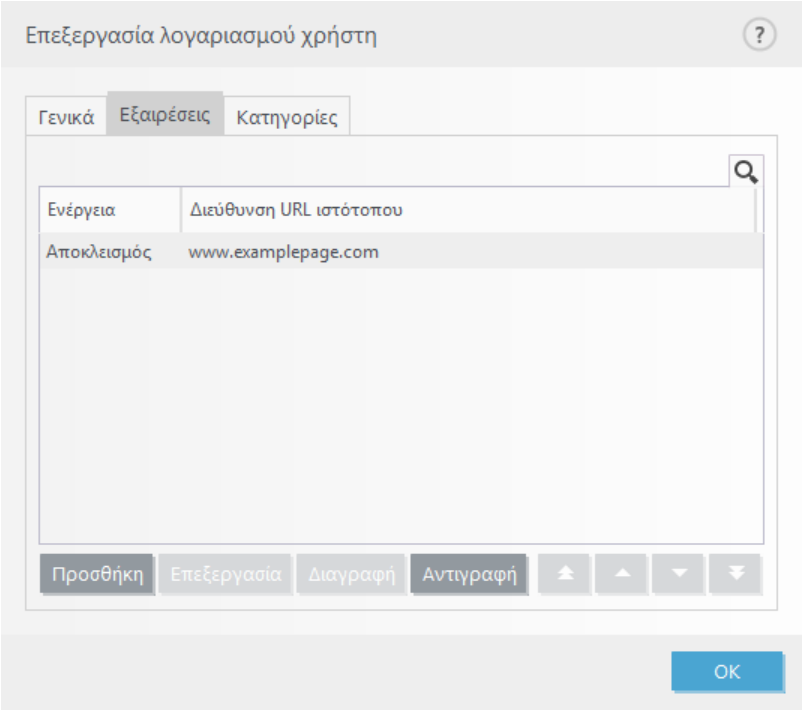
κατόπιν κάντε κλικ στο κουμπί **OK**. Η εξαίρεση θα προστεθεί στη λίστα υπαρχουσών εξαιρέσεων και θα εμφανίζεται η κατάστασή της.

Προσθήκη – Δημιουργεί μια νέα εξαίρεση.

Επεξεργασία – Μπορείτε να επεξεργαστείτε τη **Διεύθυνση URL ιστότοπου** ή την **Ενέργεια** της επιλεγμένης εξαίρεσης.

Κατάργηση – Αφαιρεί την επιλεγμένη εξαίρεση.

Αντιγραφή – Επιλέξτε από το αναπτυσσόμενο μενού έναν χρήστη από τον οποίο θέλετε να αντιγράψετε μια δημιουργημένη εξαίρεση.

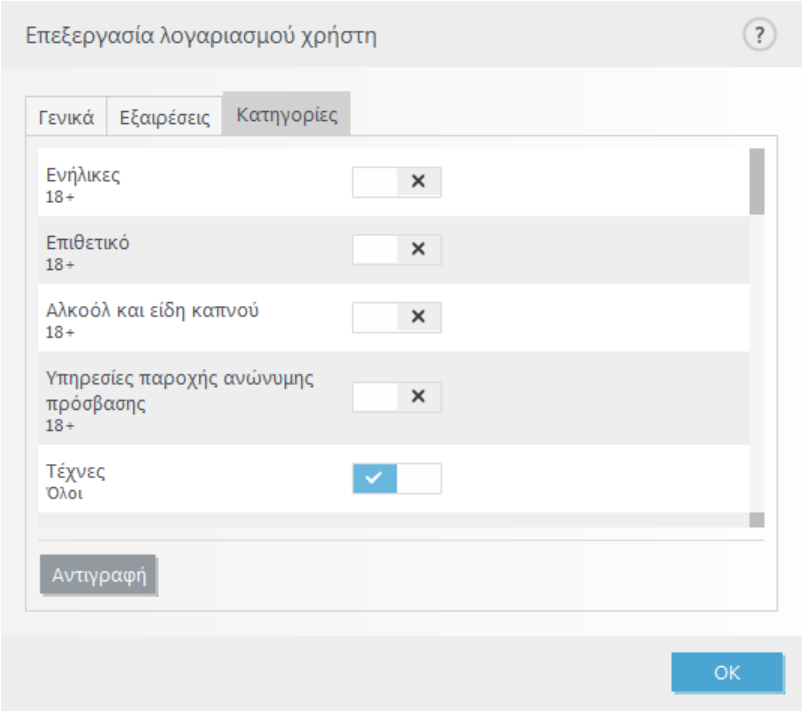


Οι εξαιρέσεις που καθορίζονται υπερισχύουν των κατηγοριών που καθορίζονται για τους επιλεγμένους λογαριασμούς. Για παράδειγμα, εάν ο λογαριασμός έχει αποκλεισμένη την κατηγορία **Ειδήσεις**, αλλά έχετε καθορίσει μια ιστοσελίδα ειδήσεων ως επιτρεπτή εξαίρεση, ο λογαριασμός θα μπορεί να έχει πρόσβαση στην ιστοσελίδα που επιτρέπετε. Μπορείτε να δείτε τις αλλαγές που έχουν πραγματοποιηθεί εδώ στην ενότητα Εξαιρέσεις.

Κατηγορίες

Στην καρτέλα **Κατηγορίες**, μπορείτε να ορίσετε τις γενικές κατηγορίες των ιστότοπων που θέλετε να αποκλείσετε ή να επιτρέψετε για κάθε λογαριασμό. Επιλέξτε το πλαίσιο ελέγχου που βρίσκεται δίπλα σε μια κατηγορία, για να επιτρέπεται η κατηγορία αυτή. Εάν αφήσετε το πλαίσιο ελέγχου κενό, η κατηγορία δεν θα επιτρέπεται για τον συγκεκριμένο λογαριασμό.

Αντιγραφή – Σας επιτρέπει να αντιγράψετε μια λίστα αποκλεισμένων ή επιτρεπόμενων κατηγοριών από έναν υπάρχοντα τροποποιημένο λογαριασμό.



Αντιγραφή εξαίρεσης από τον χρήστη

Επιλέξτε από το αναπτυσσόμενο μενού έναν χρήστη από τον οποίο θέλετε να αντιγράψετε μια δημιουργημένη εξαίρεση.

Αντιγραφή κατηγοριών από λογαριασμό

Σας επιτρέπει να αντιγράψετε μια λίστα αποκλεισμένων ή επιτρεπόμενων κατηγοριών από έναν υπάρχοντα τροποποιημένο λογαριασμό.

Ενεργοποίηση Γονικού ελέγχου

Η επιλογή **Ενεργοποίηση γονικού ελέγχου** ενσωματώνει τον Γονικό έλεγχο στο ESET Internet Security. Θα εμφανιστεί η ενότητα Γονικός έλεγχος στο κύριο παράθυρο στην περιοχή **Ρυθμίσεις** > **Εργαλεία ασφαλείας** > **Γονικός έλεγχος**.

Anti-Theft

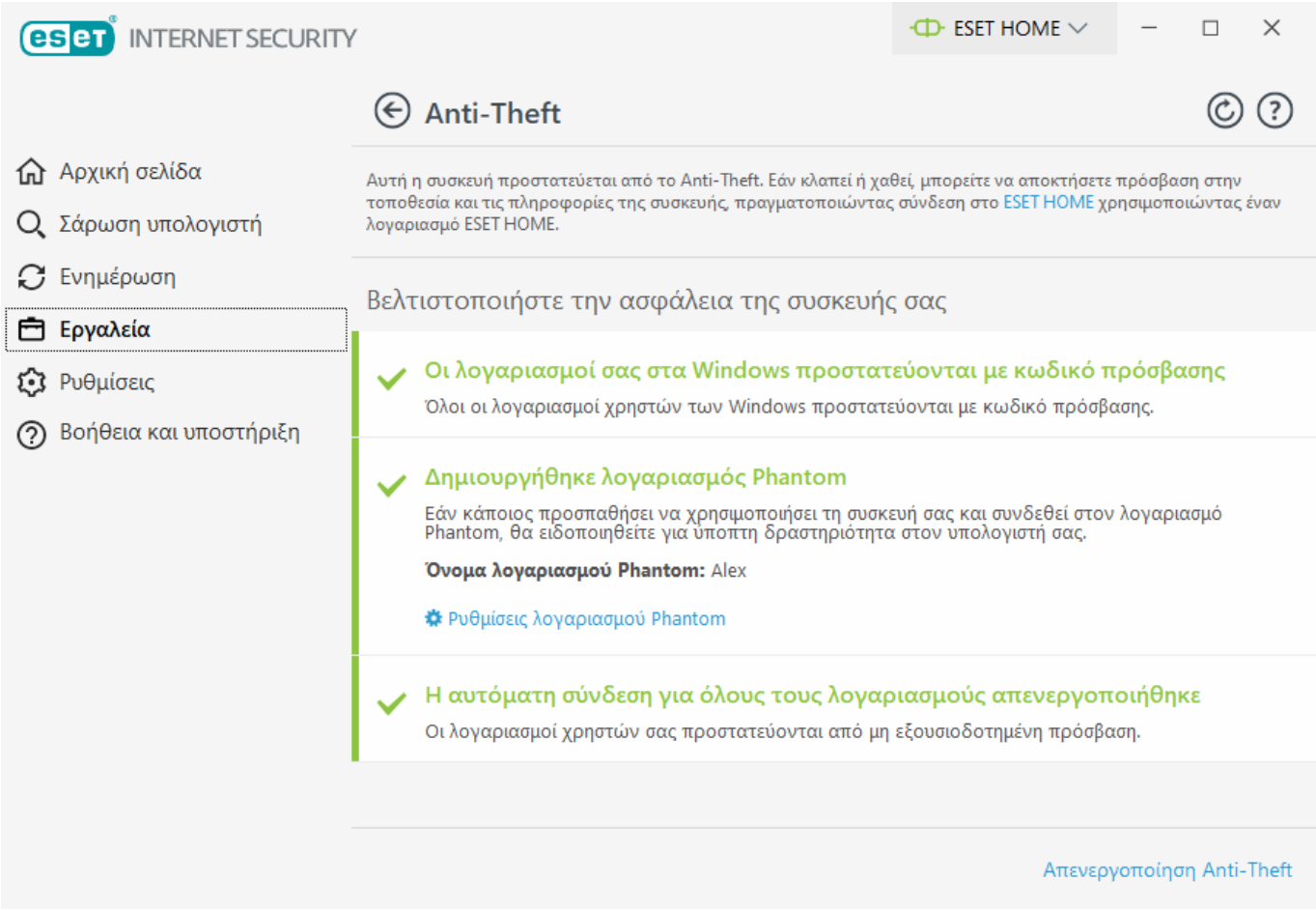
Οι προσωπικές συσκευές κινδυνεύουν διαρκώς με απώλεια ή κλοπή κατά τις καθημερινές μας μετακινήσεις από το σπίτι στο γραφείο και σε άλλους δημόσιους χώρους. Το Anti-Theft είναι μια δυνατότητα που επεκτείνει την ασφάλεια σε επίπεδο χρήστη σε περίπτωση που μια συσκευή χαθεί ή κλαπεί. Το Anti-Theft σάς επιτρέπει να παρακολουθείτε τη χρήση της συσκευής και να εντοπίζετε τη χαμένη συσκευή χρησιμοποιώντας τον εντοπισμό μέσω της διεύθυνσης IP στο ESET HOME, βοηθώντας σας έτσι να ανακτήσετε τη συσκευή σας και να προστατέψετε τα δεδομένα προσωπικού χαρακτήρα.

Με τη χρήση σύγχρονων τεχνολογιών, όπως αναζήτηση γεωγραφικών διευθύνσεων, καταγραφή εικόνων με την ενσωματωμένη κάμερα, προστασία λογαριασμών χρήστη και παρακολούθηση συσκευών, η μονάδα Anti-Theft μπορεί να βοηθήσει εσάς και τις αρχές να εντοπίσουν τον υπολογιστή

ή τη συσκευή σας εάν έχει χαθεί ή κλαπεί. Στο ESET HOME, μπορείτε να δείτε τις δραστηριότητες που πραγματοποιούνται στον υπολογιστή ή στη συσκευή σας.

Για να μάθετε περισσότερα σχετικά με το Anti-Theft στο ESET HOME, ανατρέξτε στην Ηλεκτρονική βοήθεια του ESET HOME.

Αφού ενεργοποιήσετε το Anti-Theft, μπορείτε να βελτιστοποιήσετε την ασφάλεια της συσκευής σας από το κύριο παράθυρο του προγράμματος > **Εργαλεία** > **Anti-Theft**.



Επιλογές βελτιστοποίησης

Δεν δημιουργήθηκε λογαριασμός Phantom

Η δημιουργία ενός λογαριασμού Phantom αυξάνει την πιθανότητα εντοπισμού μιας χαμένης ή κλεμμένης συσκευής. Εάν επισημάνετε τη συσκευή σας ως χαμένη, το Anti-Theft θα αποκλείσει την πρόσβαση στους ενεργούς λογαριασμούς χρήστη σας για να προστατεύσει τα ευαίσθητα δεδομένα σας. Όποιος επιχειρήσει να χρησιμοποιήσει τη συσκευή θα επιτρέπεται να χρησιμοποιεί μόνο τον λογαριασμό Phantom. Ο λογαριασμός Phantom είναι μια μορφή λογαριασμού επισκέπτη με περιορισμένα δικαιώματα. Θα χρησιμοποιείται ως προεπιλεγμένος λογαριασμός συστήματος μέχρι να επισημανθεί η συσκευή σας ως ανακτηθείσα – εμποδίζοντας οποιονδήποτε να συνδεθεί σε άλλους λογαριασμούς χρήστη ή να αποκτήσει πρόσβαση στα δεδομένα του χρήστη.

Κάθε φορά που κάποιος συνδέεται στον λογαριασμό Phantom όταν ο υπολογιστής βρίσκεται σε κανονική κατάσταση, θα σας αποστέλλεται με email μια ειδοποίηση με πληροφορίες σχετικά με ύποπτη δραστηριότητα στον υπολογιστή σας. Αφού λάβετε την ειδοποίηση με email, μπορείτε να αποφασίσετε εάν θέλετε να επισημάνετε τον υπολογιστή ως χαμένο.

Για να δημιουργήσετε έναν λογαριασμό Phantom, κάντε κλικ στο στοιχείο **Δημιουργία λογαριασμού Phantom**, πληκτρολογήστε το **Όνομα λογαριασμού Phantom** στο πεδίο κειμένου και κάντε κλικ στο στοιχείο **Δημιουργία**.

Όταν δημιουργήσετε τον λογαριασμό Phantom, κάντε κλικ στο στοιχείο **Ρυθμίσεις λογαριασμού Phantom** για να μετονομάσετε ή να καταργήσετε τον λογαριασμό.

Προστασία κωδικών πρόσβασης λογαριασμών Windows

Ο λογαριασμός χρήστη σας δεν προστατεύεται με κωδικό πρόσβασης. Θα λάβετε αυτήν την προειδοποίηση βελτιστοποίησης εάν τουλάχιστον ένας λογαριασμός χρήστη δεν προστατεύεται με κωδικό πρόσβασης. Η δημιουργία κωδικού πρόσβασης για όλους τους χρήστες (εκτός από τον **λογαριασμό Phantom**) στον υπολογιστή θα επιλύσει αυτό το ζήτημα.

Για να δημιουργήσετε έναν κωδικό πρόσβασης για τον λογαριασμό χρήστη, κάντε κλικ στο στοιχείο **Διαχείριση λογαριασμών Windows** και αλλάξτε τον κωδικό πρόσβασης ή ακολουθήστε τις παρακάτω οδηγίες:

1. Πατήστε τα πλήκτρα CTRL+Alt+Delete στο πληκτρολόγιό σας.
2. Κάντε κλικ στο στοιχείο **Αλλαγή κωδικού πρόσβασης**.
3. Αφήστε κενό το πεδίο **Παλιός κωδικός πρόσβασης**.
4. Πληκτρολογήστε τον κωδικό πρόσβασης στα πεδία **Νέος κωδικός πρόσβασης** και **Επιβεβαίωση κωδικού πρόσβασης** και πατήστε το πλήκτρο **Enter**.

Αυτόματη σύνδεση για λογαριασμούς Windows

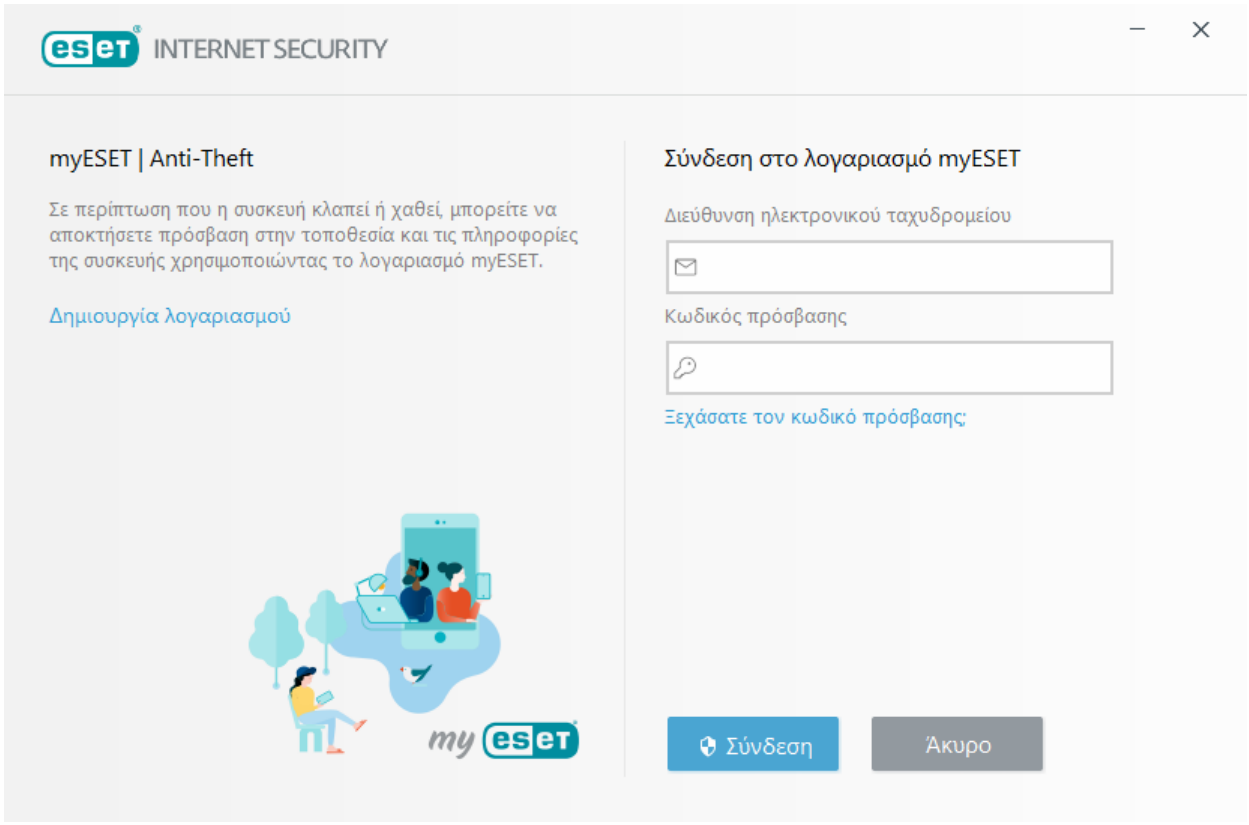
Στον λογαριασμό χρήστη σας έχει ενεργοποιηθεί η αυτόματη σύνδεση. Επομένως, ο λογαριασμός σας δεν προστατεύεται από μη εξουσιοδοτημένη πρόσβαση. Θα λάβετε αυτήν την προειδοποίηση βελτιστοποίησης εάν έχει ενεργοποιηθεί η αυτόματη σύνδεση σε έναν τουλάχιστον λογαριασμό χρήστη. Κάντε κλικ στο στοιχείο **Απενεργοποίηση αυτόματης σύνδεσης** για να επιλύσετε αυτό το ζήτημα βελτιστοποίησης.

Η αυτόματη σύνδεση για τον λογαριασμό Phantom ενεργοποιήθηκε

Η αυτόματη σύνδεση ενεργοποιήθηκε για τον **Λογαριασμό Phantom** στη συσκευή σας. Όταν η συσκευή βρίσκεται σε κανονική κατάσταση, συνιστάται να μην χρησιμοποιείτε αυτόματη σύνδεση, επειδή μπορεί να προκαλέσει προβλήματα πρόσβασης στον πραγματικό λογαριασμό χρήστη σας ή να αποστέλλει ψευδείς συναγερμούς σχετικά με την κατάσταση «χαμένος» του υπολογιστή σας. Κάντε κλικ στο στοιχείο **Απενεργοποίηση αυτόματης σύνδεσης** για να επιλύσετε αυτό το ζήτημα βελτιστοποίησης.

Σύνδεση στον λογαριασμό σας στο ESET HOME

Για να ενεργοποιήσετε/απενεργοποιήσετε το Anti-Theft και να αποκτήσετε πρόσβαση στην τοποθεσία της συσκευής και τις πληροφορίες στο ESET HOME, συνδεθείτε στον λογαριασμό σας στο ESET HOME.



Υπάρχουν πολλές διαθέσιμες μέθοδοι σύνδεσης στον λογαριασμό σας στο ESET HOME:

• **Χρήση της διεύθυνσης email και του κωδικού πρόσβασης στο ESET HOME** - Πληκτρολογήστε τη **Διεύθυνση email** και τον **Κωδικό πρόσβασης** που χρησιμοποιήσατε για να δημιουργήσετε τον λογαριασμό σας στο ESET HOME και κάντε κλικ στο στοιχείο **Σύνδεση**.

• **Χρήση του λογαριασμού σας στο Google/AppleID** – Κάντε κλικ στο στοιχείο **Συνέχεια με Google** ή **Συνέχεια με Apple** και συνδεθείτε στον κατάλληλο λογαριασμό. Μετά από επιτυχημένη σύνδεση, θα μεταφερθείτε στην ιστοσελίδα επιβεβαίωσης του ESET HOME. Για να συνεχίσετε, επιστρέψτε στο παράθυρο του προϊόντος ESET. Για περισσότερες πληροφορίες σχετικά με τη σύνδεση μέσω λογαριασμού Google/AppleID, ανατρέξτε στις οδηγίες στο θέμα Ηλεκτρονική βοήθεια του ESET HOME.

• **Σάρωση κωδικού QR** – Κάντε κλικ στην επιλογή **Σάρωση κωδικού QR** για να εμφανίσετε τον κωδικό QR. Ανοίξτε την εφαρμογή για κινητά ESET HOME και σαρώστε τον κωδικό QR ή στρέψτε την κάμερα της συσκευής σας στον κωδικό QR. Για περισσότερες πληροφορίες, ανατρέξτε στις οδηγίες της Ηλεκτρονικής βοήθειας του ESET HOME.

⚠ Η σύνδεση απέτυχε - συνήθη σφάλματα.

Εάν δεν έχετε λογαριασμό στο ESET HOME, κάντε κλικ στο στοιχείο **Δημιουργία λογαριασμού** για να εγγραφείτε ή δείτε τις οδηγίες στην Ηλεκτρονική βοήθεια του ESET HOME.
Εάν ξεχάσατε τον κωδικό πρόσβασής σας, κάντε κλικ στο στοιχείο **Ξέχασα τον κωδικό πρόσβασης** και ακολουθήστε τα βήματα στην οθόνη ή δείτε τις οδηγίες στην Ηλεκτρονική βοήθεια του ESET HOME.

Το Anti-Theft δεν υποστηρίζει το Microsoft Windows Home Server.

Ορισμός ονόματος συσκευής

Το πεδίο **Όνομα συσκευής** αντιπροσωπεύει το όνομα του υπολογιστή (της συσκευής) σας, το οποίο θα εμφανίζεται ως αναγνωριστικό σε όλες τις υπηρεσίες του ESET HOME. Το όνομα υπολογιστή του υπολογιστή σας χρησιμοποιείται από προεπιλογή. Πληκτρολογήστε το όνομα της συσκευής ή χρησιμοποιήστε το προεπιλεγμένο και κάντε κλικ στο στοιχείο **Συνέχεια**.

Anti-Theft ενεργό/ανενεργό

Αυτό το παράθυρο περιέχει ένα μήνυμα επιβεβαίωσης όταν ενεργοποιείτε/απενεργοποιείτε το Anti-Theft:

• Ενεργό – Η συσκευή σας προστατεύεται πλέον από το Anti-Theft και μπορείτε να διαχειριστείτε την ασφάλειά της απομακρυσμένα στην πύλη ESET HOME χρησιμοποιώντας τον λογαριασμό σας.

• Ανενεργό – Το Anti-Theft απενεργοποιήθηκε σε αυτήν τη συσκευή και όλα τα δεδομένα που σχετίζονται με το <%ESET_ANTTHEFT%> για αυτήν τη συσκευή θα καταργηθούν από την πύλη ESET HOME.

Η προσθήκη νέας συσκευής απέτυχε

Λάβατε ένα μήνυμα σφάλματος κατά την ενεργοποίηση του Anti-Theft.

Τα πιο συνηθισμένα σενάρια είναι:

• Σφάλμα σύνδεσης στο ESET HOME

• Δεν υπάρχει συνδεσιμότητα Internet (ή δεν λειτουργεί το Internet εκείνη τη στιγμή)

Εάν δεν μπορείτε να επιλύσετε το ζήτημα, επικοινωνήστε με την Τεχνική υποστήριξη της ESET.

Ενημέρωση του προγράμματος

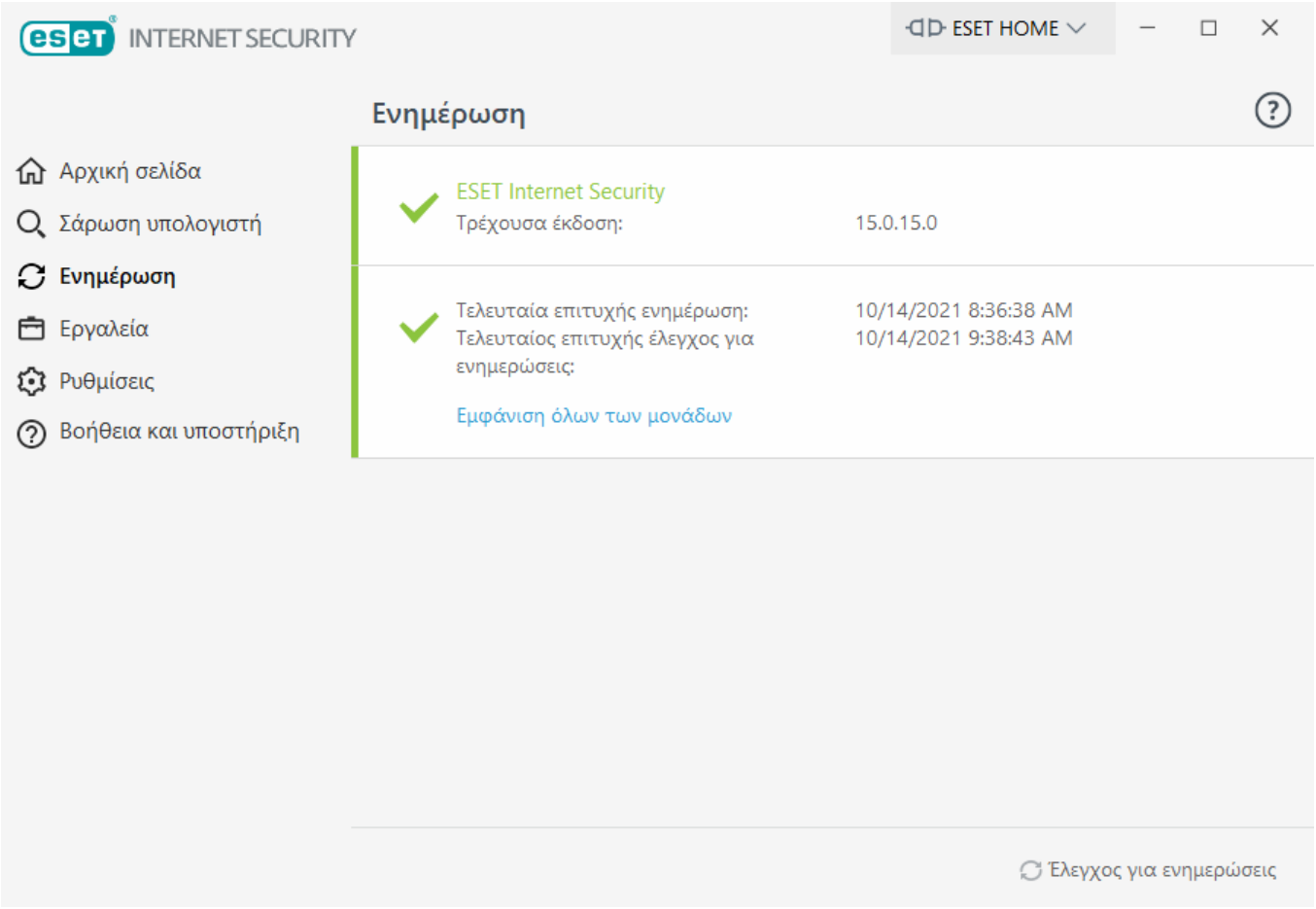
Η τακτική ενημέρωση του ESET Internet Security είναι η καλύτερη μέθοδος για να διασφαλίσετε μέγιστο επίπεδο ασφάλειας στον υπολογιστή σας. Η μονάδα Ενημέρωσης διασφαλίζει ότι είναι πάντα ενημερωμένες οι μονάδες προγράμματος και τα στοιχεία συστήματος.

Εάν κάνετε κλικ στο στοιχείο **Ενημέρωση** στο κύριο παράθυρο του προγράμματος, μπορείτε να δείτε την τρέχουσα κατάσταση ενημέρωσης που συμπεριλαμβάνει την ημερομηνία και την ώρα της τελευταίας επιτυχημένης ενημέρωσης, καθώς και αν χρειάζεται ενημέρωση.

Εκτός από τις αυτόματες ενημερώσεις, μπορείτε να κάνετε κλικ στο στοιχείο **Έλεγχος για ενημερώσεις** για να ενεργοποιήσετε μια μη αυτόματη ενημέρωση. Η τακτική ενημέρωση των μονάδων και των στοιχείων προγράμματος είναι σημαντικός παράγοντας για τη διατήρηση πλήρους προστασίας έναντι κακόβουλου κώδικα. Προσέξτε τη διαμόρφωση και τη λειτουργία των λειτουργικών μονάδων του προϊόντος. Για να λαμβάνετε ενημερώσεις, πρέπει να ενεργοποιήσετε το προϊόν σας χρησιμοποιώντας το Κλειδί άδειας χρήσης. Εάν δεν το είχατε κάνει κατά την εγκατάσταση, θα πρέπει να εισαγάγετε το κλειδί άδειας χρήσης για να ενεργοποιήσετε το προϊόν

σας προκειμένου να αποκτήσετε πρόσβαση στους διακομιστές ενημέρωσης της ESET κατά την ενημέρωση.

Το κλειδί άδειας χρήσης σας στάλθηκε μέσω email από την ESET μετά την αγορά του ESET Internet Security.



Τρέχουσα έκδοση – Εμφανίζει τον αριθμό της τρέχουσας έκδοσης του προϊόντος που έχετε εγκαταστήσει.

Τελευταία επιτυχής ενημέρωση – Εμφανίζει την ημερομηνία της τελευταίας επιτυχούς ενημέρωσης. Εάν δεν βλέπετε μια πρόσφατη ημερομηνία, οι μονάδες του προϊόντος που έχετε μπορεί να μην είναι πρόσφατες.

Τελευταίος επιτυχής έλεγχος για ενημερώσεις – Εμφανίζει την ημερομηνία του τελευταίου επιτυχούς ελέγχου για ενημερώσεις.

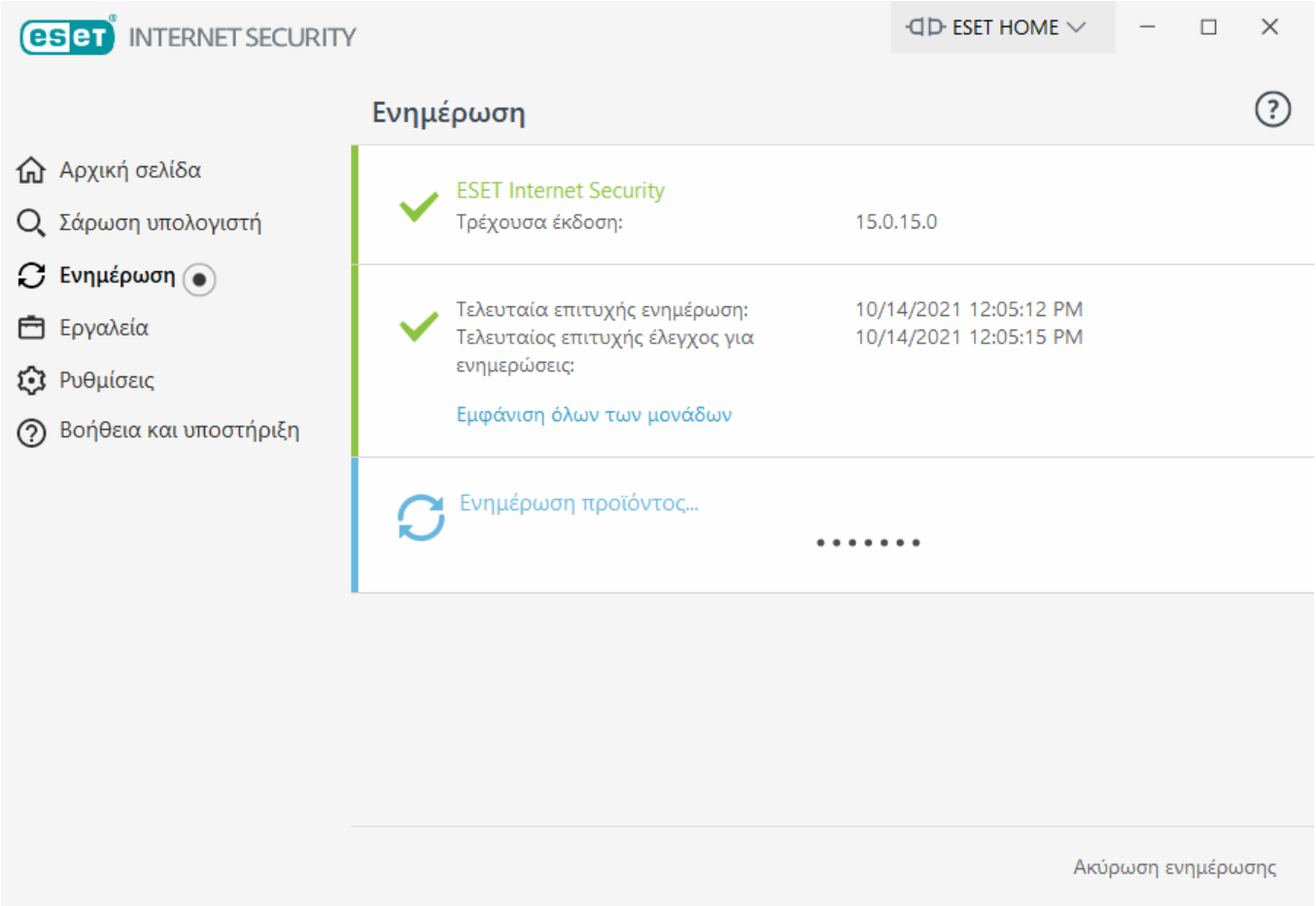
Εμφάνιση όλων των μονάδων – Εμφανίζει τη λίστα εγκατεστημένων μονάδων του προγράμματος.

Κάντε κλικ στο στοιχείο **Έλεγχος για ενημερώσεις** για να ανιχνεύσετε την πιο πρόσφατη έκδοση του ESET Internet Security.

Διεργασία ενημέρωσης

Η λήψη ξεκινά μόλις κάνετε κλικ στην επιλογή **Έλεγχος για ενημερώσεις**. Θα εμφανιστεί μια

γραμμή προόδου της λήψης και ο χρόνος που υπολείπεται για τη λήψη. Για να διακόψετε την ενημέρωση, κάντε κλικ στην **Ακύρωση ενημέρωσης**.



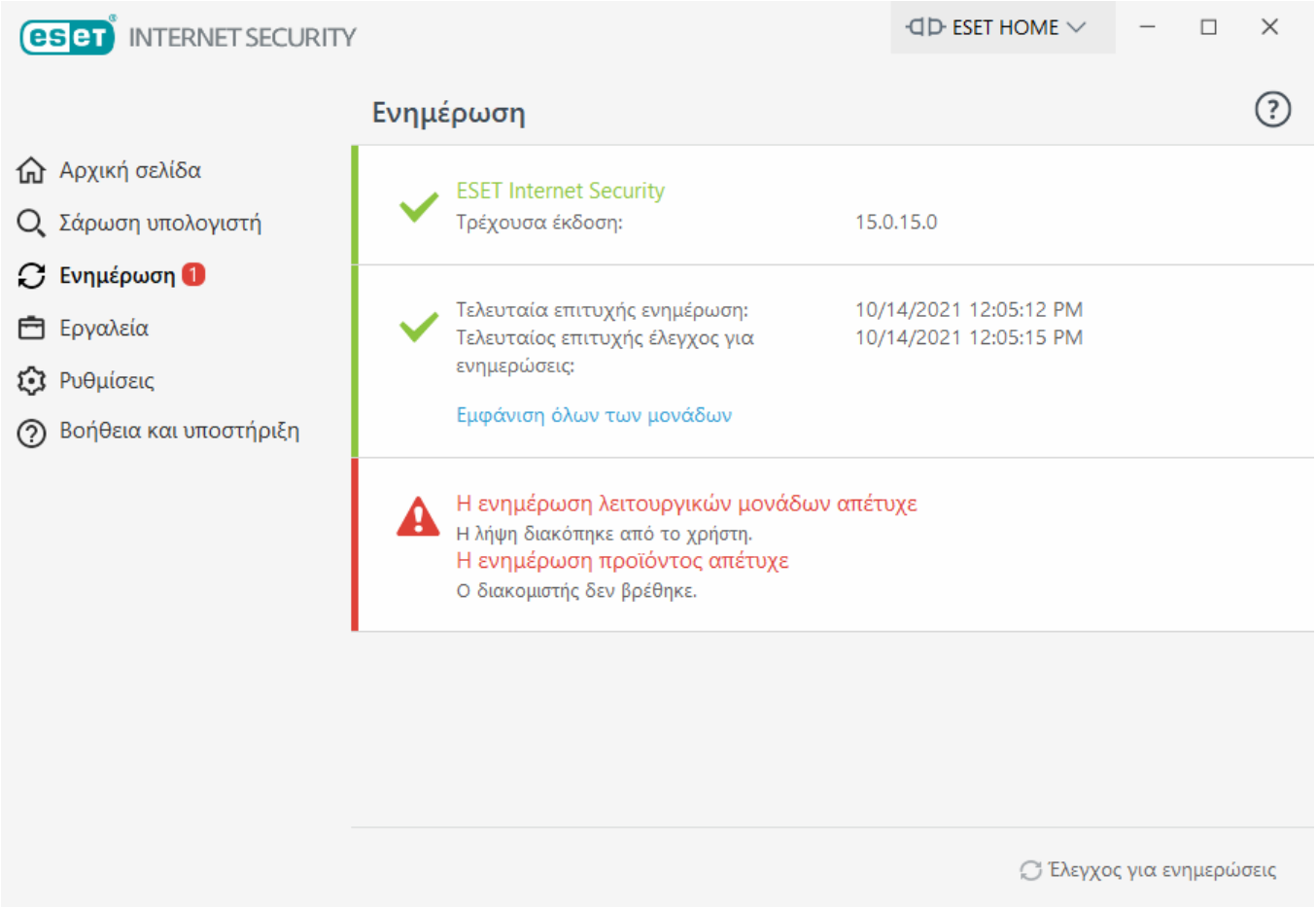
Υπό κανονικές συνθήκες, θα δείτε το πράσινο σημάδι ελέγχου στο παράθυρο **Ενημέρωση** που υποδεικνύει ότι το πρόγραμμα είναι ενημερωμένο. Εάν δεν δείτε το πράσινο σημάδι ελέγχου, το πρόγραμμα δεν είναι ενημερωμένο και είναι πιο ευάλωτο σε μόλυνση. Ενημερώστε τις λειτουργικές μονάδες του προγράμματος το συντομότερο δυνατόν.

Μη επιτυχής ενημέρωση

Εάν λάβετε ένα μήνυμα αποτυχίας ενημέρωσης των λειτουργικών μονάδων του προγράμματος, αυτό μπορεί να προκαλείται από τα παρακάτω ζητήματα:

1. **Μη έγκυρη άδεια χρήσης** – Η άδεια χρήσης που χρησιμοποιήθηκε για ενεργοποίηση δεν είναι έγκυρη ή έληξε. Στο κύριο παράθυρο προγράμματος, κάντε κλικ στα στοιχεία **Βοήθεια και υποστήριξη** > **Αλλαγή άδειας χρήσης** και εισαγάγετε ένα νέο κλειδί άδειας χρήσης.

2. **Παρουσιάστηκε σφάλμα κατά τη λήψη των αρχείων ενημέρωσης** – Αυτό μπορεί να οφείλεται σε εσφαλμένες Ρυθμίσεις σύνδεσης διαδικτύου. Συνιστάται να ελέγξετε τη συνδεσιμότητα του Διαδικτύου (ανοίγοντας οποιονδήποτε ιστότοπο στο πρόγραμμα περιήγησης στον ιστό). Αν δεν ανοίξει ο ιστότοπος, είναι πιθανόν να μην έχει δημιουργηθεί σύνδεση στο Διαδίκτυο ή να υπάρχουν προβλήματα συνδεσιμότητας με τον υπολογιστή σας. Ελέγξτε με την υπηρεσία παροχής υπηρεσιών διαδικτύου (ISP) αν δεν έχετε ενεργή σύνδεση Διαδικτύου.



Συνιστάται να κάνετε επανεκκίνηση του υπολογιστή σας μετά από επιτυχημένη ενημέρωση του ESET Internet Security σε νεότερη έκδοση, για να διασφαλίσετε ότι ενημερώθηκαν σωστά όλες οι λειτουργικές μονάδες του προγράμματος. Δεν είναι απαραίτητο να κάνετε επανεκκίνηση του υπολογιστή σας μετά από τακτικές ενημερώσεις των λειτουργικών μονάδων.

Για περισσότερες πληροφορίες, επισκεφτείτε την ενότητα Αντιμετώπιση προβλημάτων με το μήνυμα «Αποτυχία ενημέρωσης των λειτουργικών μονάδων».

Ρυθμίσεις ενημέρωσης

Οι επιλογές ρυθμίσεων ενημέρωσης είναι διαθέσιμες στη δομή **Ρυθμίσεις για προχωρημένους** (F5) στην ενότητα **Ενημέρωση** > **Βασικές ρυθμίσεις**. Αυτή η ενότητα καθορίζει πληροφορίες προέλευσης ενημερώσεων, όπως οι διακομιστές ενημέρωσης που χρησιμοποιούνται και τα δεδομένα ελέγχου ταυτότητας για αυτούς τους διακομιστές.

Βασικό

Το προφίλ ενημέρωσης που χρησιμοποιείται αυτή τη στιγμή (εκτός εάν έχει ρυθμιστεί κάποιο συγκεκριμένο στη διαδρομή **Ρυθμίσεις για προχωρημένους** > **Firewall** > **Γνωστά δίκτυα**) εμφανίζεται στο αναπτυσσόμενο μενού **Επιλογή προεπιλεγμένου προφίλ ενημέρωσης**.

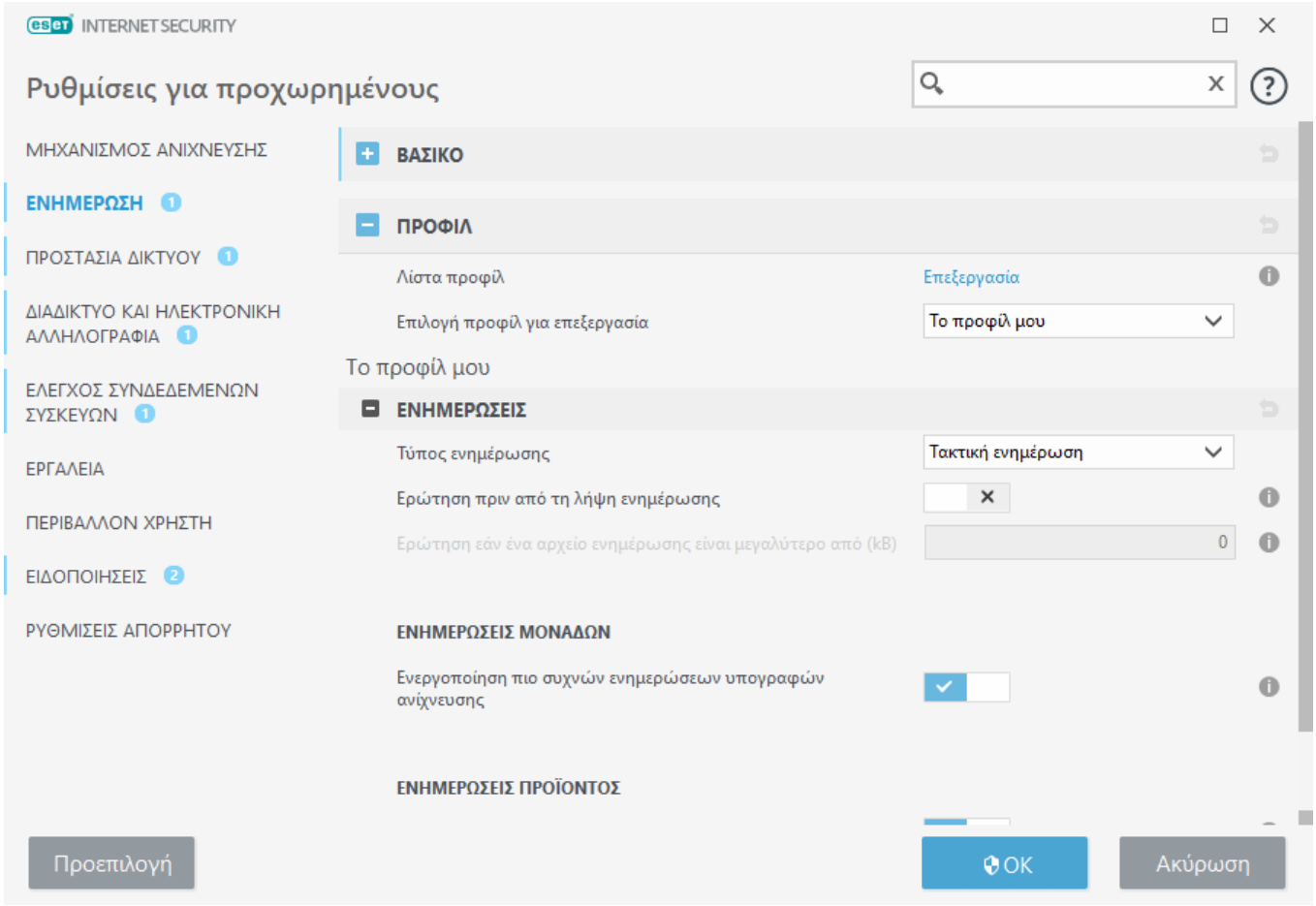
Για να δημιουργήσετε ένα νέο προφίλ, ανατρέξτε στην ενότητα Προφίλ ενημέρωσης.

Αυτόματη εναλλαγή προφίλ – Σας επιτρέπει να αλλάξετε το προφίλ για ένα συγκεκριμένο δίκτυο.

Εάν αντιμετωπίζετε δυσκολίες κατά την προσπάθεια λήψης ενημερώσεων του μηχανισμού ανίχνευσης ή των λειτουργικών μονάδων, κάντε κλικ στην επιλογή **Καθαρισμός** για να εκκαθαρίσετε τα προσωρινά αρχεία ενημέρωσης/την προσωρινή μνήμη.

Επαναφορά μονάδας

Αν υποπτεύεστε ότι μια νέα ενημέρωση του μηχανισμού ανίχνευσης ή/και των μονάδων του προγράμματος μπορεί να είναι ασταθής ή κατεστραμμένη, μπορείτε να επιστρέψετε στην προηγούμενη έκδοση και να απενεργοποιήσετε τις ενημερώσεις για συγκεκριμένο χρονικό διάστημα.



Για να γίνεται σωστά η λήψη των ενημερώσεων είναι απαραίτητο να συμπληρώνετε σωστά τις παραμέτρους ενημέρωσης. Εάν χρησιμοποιείτε τείχος προστασίας, βεβαιωθείτε ότι το πρόγραμμα ESET επιτρέπεται να επικοινωνεί με το διαδίκτυο (για παράδειγμα, επικοινωνία HTTP).

Προφίλ

Μπορείτε να δημιουργήσετε προφίλ ενημέρωσης για διάφορες διαμορφώσεις και εργασίες ενημέρωσης. Η δημιουργία προφίλ ενημέρωσης είναι ιδιαίτερα χρήσιμη για τους χρήστες φορητών υπολογιστών που χρειάζονται ένα εναλλακτικό προφίλ για τις ιδιότητες σύνδεσης στο Internet, τις οποίες αλλάζουν τακτικά.

Το αναπτυσσόμενο μενού **Επιλογή προφίλ για επεξεργασία** εμφανίζει το τρέχον επιλεγμένο προφίλ και είναι καθορισμένο στη ρύθμιση **Το προφίλ μου** από προεπιλογή. Για να δημιουργήσετε νέο προφίλ, κάντε κλικ στο στοιχείο **Επεξεργασία** δίπλα στη **Λίστα προφίλ**, πληκτρολογήστε το **Όνομα προφίλ** που θέλετε και κατόπιν κάντε κλικ στο στοιχείο **Προσθήκη**.

Ενημερώσεις

Από προεπιλογή, η ρύθμιση του μενού **Τύπος ενημέρωσης** ορίζεται σε **Τακτική ενημέρωση**, για να διασφαλιστεί ότι η λήψη των αρχείων ενημέρωσης θα γίνεται αυτόματα από τον διακομιστή της ESET με τη λιγότερη κίνηση δικτύου. Οι ενημερώσεις προέκδοσης (η επιλογή **Ενημέρωση προέκδοσης**) είναι ενημερώσεις που έχουν περάσει από ενδελεχείς εσωτερικές δοκιμές και θα είναι σύντομα διαθέσιμες στο κοινό. Μπορείτε να ωφεληθείτε από την ενεργοποίηση των ενημερώσεων προέκδοσης, αφού θα έχετε πρόσβαση στις πιο πρόσφατες μεθόδους ανίχνευσης και τις διορθώσεις. Ωστόσο, οι ενημερώσεις προέκδοσης μπορεί να μην είναι αρκετά σταθερές πάντα και ΔΕΝ ΠΡΕΠΕΙ να χρησιμοποιούνται σε διακομιστές παραγωγής και σταθμούς εργασίας όπου απαιτείται μέγιστη διαθεσιμότητα και σταθερότητα.

Ερώτηση πριν από τη λήψη ενημέρωσης – Το πρόγραμμα θα εμφανίζει μια ειδοποίηση, όπου μπορείτε να επιλέξετε την επιβεβαίωση ή απόρριψη των λήψεων αρχείων ενημέρωσης.

Ερώτηση εάν το μέγεθος ενός αρχείου ενημέρωσης είναι μεγαλύτερο από (kB) – Το πρόγραμμα θα εμφανίζει ένα παράθυρο διαλόγου επιβεβαίωσης εάν το μέγεθος του αρχείου ενημέρωσης είναι μεγαλύτερο από την καθορισμένη τιμή. Εάν το μέγεθος του αρχείου ενημέρωσης έχει ρυθμιστεί σε 0 kB, το πρόγραμμα θα εμφανίζει πάντα ένα παράθυρο διαλόγου επιβεβαίωσης.

Απενεργοποίηση ειδοποίησης σχετικά με επιτυχείς ενημερώσεις – Απενεργοποιεί τις ειδοποιήσεις της περιοχής ειδοποιήσεων στην κάτω δεξιά γωνία της οθόνης. Είναι χρήσιμο να επιλέξετε αυτό το στοιχείο, εάν εκτελείτε μια εφαρμογή πλήρους οθόνης ή ένα παιχνίδι. Σημειώστε ότι η λειτουργία Gamer απενεργοποιεί όλες τις ειδοποιήσεις.

Ενημερώσεις μονάδας

Ενεργοποίηση συχνότερων ενημερώσεων της βάσης αναγνώρισης ιών – Η βάση αναγνώρισης ιών θα ενημερώνεται κατά πιο μικρά χρονικά διαστήματα. Η απενεργοποίηση αυτής της ρύθμισης μπορεί να επηρεάσει αρνητικά το ποσοστό ανίχνευσης.

Ενημερώσεις προϊόντος

Ενημερώσεις δυνατοτήτων εφαρμογής – Αυτόματη εγκατάσταση νέων εκδόσεων του ESET Internet Security.

Επιλογές σύνδεσης

Για να χρησιμοποιήσετε έναν διακομιστή μεσολάβησης για τη λήψη ενημερώσεων, ανατρέξτε στην ενότητα Επιλογές σύνδεσης.

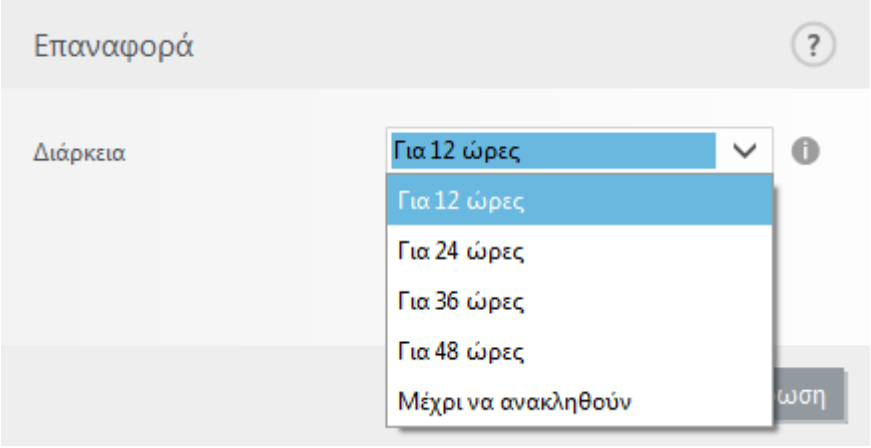
Επιστροφή ενημέρωσης σε προηγούμενη έκδοση

Εάν υποπτεύεστε ότι μια νέα ενημέρωση του μηχανισμού ανίχνευσης ή οι μονάδες προγράμματος μπορεί να είναι ασταθείς ή κατεστραμμένες, μπορείτε να επιστρέψετε στην προηγούμενη έκδοση και να απενεργοποιήσετε προσωρινά τις ενημερώσεις. Εναλλακτικά, μπορείτε να ενεργοποιήσετε ενημερώσεις που απενεργοποιήθηκαν προηγουμένως αν τις είχατε αναβάλει επ' αόριστον.

Το ESET Internet Security καταγράφει στιγμιότυπα του μηχανισμού ανίχνευσης και των μονάδων προγράμματος για χρήση με τη δυνατότητα επαναφοράς. Για να δημιουργήσετε στιγμιότυπα βάσης δεδομένων ιών, διατηρήστε ενεργοποιημένο το στοιχείο **Δημιουργία στιγμιότυπων των λειτουργικών μονάδων**. Εάν έχει ενεργοποιηθεί το στοιχείο **Δημιουργία στιγμιότυπων των λειτουργικών μονάδων**, το πρώτο στιγμιότυπο δημιουργείται κατά την πρώτη ενημέρωση. Το επόμενο δημιουργείται μετά από 48 ώρες. Το πεδίο **Αριθμός τοπικά αποθηκευμένων στιγμιότυπων** καθορίζει τον αριθμό των αποθηκευμένων στιγμιότυπων του μηχανισμού ανίχνευσης.

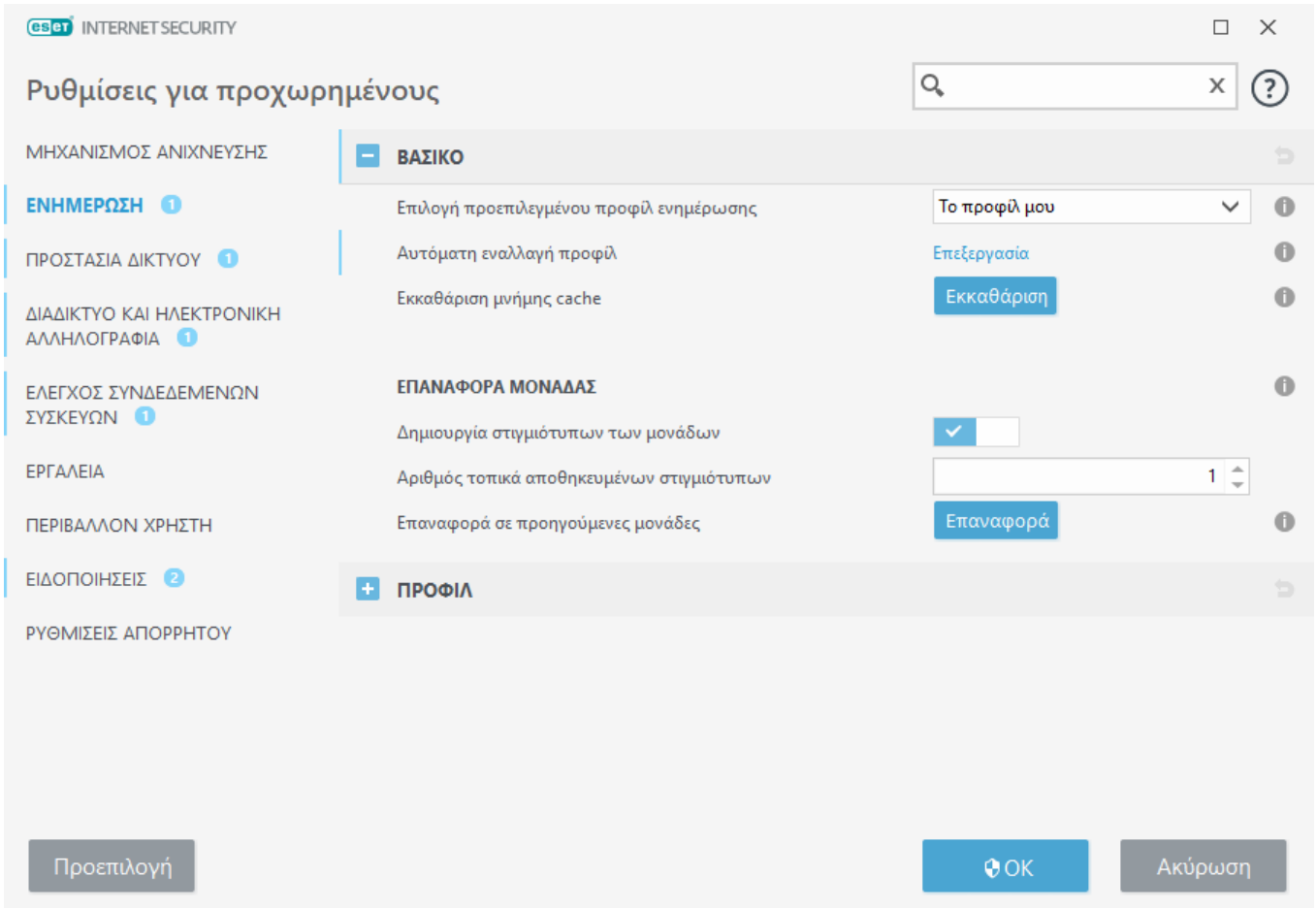
Όταν συμπληρωθεί ο μέγιστος αριθμός στιγμιότυπων (π.χ. τρία), το παλαιότερο στιγμιότυπο αντικαθίσταται από ένα νέο στιγμιότυπο κάθε 48 ώρες. Το ESET Internet Security πραγματοποιεί επαναφορά σε προηγούμενη έκδοση του μηχανισμού ανίχνευσης και των εκδόσεων ενημερώσεων της μονάδας προγράμματος στο παλαιότερο στιγμιότυπο.

Εάν κάνετε κλικ στην επιλογή **Επαναφορά** (**Ρυθμίσεις για προχωρημένους** (F5) > **Ενημέρωση** > **Βασικές ρυθμίσεις**), θα πρέπει να επιλέξετε ένα χρονικό διάστημα από το αναπτυσσόμενο μενού **Διάρκεια** που αντιπροσωπεύει το χρονικό διάστημα κατά το οποίο θα γίνει παύση των ενημερώσεων του μηχανισμού ανίχνευσης και των μονάδων προγράμματος.



Επιλέξτε το στοιχείο **Μέχρι να ακυρωθεί** για να αναβάλλετε επ' αόριστον τις τακτικές ενημερώσεις μέχρι να κάνετε επαναφορά της λειτουργικότητας ενημέρωσης μη αυτόματα. Η ESET δεν συνιστά αυτή την επιλογή, επειδή αποτελεί ενδεχόμενο κίνδυνο για την ασφάλεια.

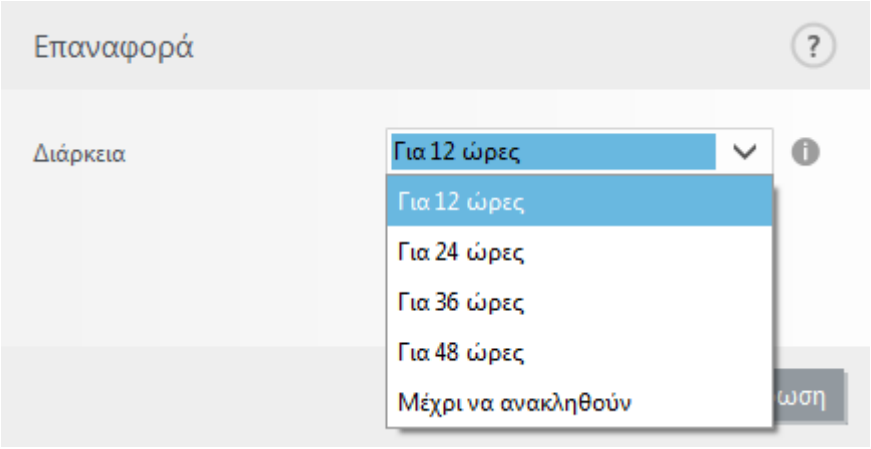
Αν εκτελεστεί επαναφορά, το κουμπί **Επαναφορά** θα αλλάξει σε **Να επιτρέπονται ενημερώσεις**. Δεν θα επιτρέπονται ενημερώσεις για το χρονικό διάστημα που έχει επιλεγεί από το αναπτυσσόμενο μενού **Αναστολή ενημερώσεων**. Η έκδοση του μηχανισμού ανίχνευσης υποβιβάζεται στην παλαιότερη διαθέσιμη και αποθηκεύεται ως στιγμιότυπο στο τοπικό σύστημα αρχείων του υπολογιστή.



Αν υποθέσουμε ότι ο πιο πρόσφατος αριθμός έκδοσης του μηχανισμού ανίχνευσης είναι 22700, οι αριθμοί έκδοσης 22698 και 22696 αποθηκεύονται ως στιγμιότυπα του μηχανισμού ανίχνευσης. Σημειώνεται ότι η έκδοση 22697 δεν είναι διαθέσιμη. Σε αυτό το παράδειγμα, ο υπολογιστής ήταν απενεργοποιημένος κατά τη διάρκεια της ενημέρωσης έκδοσης 22697 και μια πιο πρόσφατη ενημέρωση ήταν διαθέσιμη πριν από τη λήψη της ενημέρωσης έκδοσης 22697. Εάν το πεδίο **Αριθμός τοπικά αποθηκευμένων στιγμιότυπων** είναι δύο και κάνετε κλικ στο κουμπί **Επαναφορά**, ο μηχανισμός ανίχνευσης (συμπεριλαμβανομένων των μονάδων προγράμματος) επαναφέρεται στον αριθμό έκδοσης 22696. Αυτή η διαδικασία μπορεί να διαρκέσει αρκετά λεπτά. Βεβαιωθείτε ότι η έκδοση του μηχανισμού ανίχνευσης έχει υποβαθμιστεί στην οθόνη Ενημέρωση.

Χρονικό διάστημα επαναφοράς

Εάν κάνετε κλικ στην επιλογή **Επαναφορά** (**Ρυθμίσεις για προχωρημένους** (F5) > **Ενημέρωση** > **Βασικές ρυθμίσεις**), θα πρέπει να επιλέξετε ένα χρονικό διάστημα από το αναπτυσσόμενο μενού **Διάρκεια** που αντιπροσωπεύει το χρονικό διάστημα κατά το οποίο θα γίνει παύση των ενημερώσεων του μηχανισμού ανίχνευσης και των μονάδων προγράμματος.



Επιλέξτε το στοιχείο **Μέχρι να ακυρωθεί** για να αναβάλλετε επ' αόριστον τις τακτικές ενημερώσεις μέχρι να κάνετε επαναφορά της λειτουργικότητας ενημέρωσης μη αυτόματα. Η ESET δεν συνιστά αυτή την επιλογή, επειδή αποτελεί ενδεχόμενο κίνδυνο για την ασφάλεια.

Ενημερώσεις προϊόντος

Η ενότητα **Ενημερώσεις προϊόντος** σάς επιτρέπει να εγκαθιστάτε αυτόματα ενημερώσεις νέων δυνατοτήτων όταν είναι διαθέσιμες.

Οι ενημερώσεις δυνατοτήτων εφαρμογής προσφέρουν νέες δυνατότητες ή αλλάζουν αυτές που υπάρχουν ήδη από προηγούμενες εκδόσεις. Μπορεί να εκτελείται αυτόματα χωρίς παρέμβαση του χρήστη ή μπορείτε να επιλέξετε να λαμβάνετε ειδοποιήσεις. Μετά την εγκατάσταση μιας ενημέρωσης δυνατοτήτων εφαρμογής, μπορεί να απαιτείται επανεκκίνηση του υπολογιστή.

Ενημερώσεις δυνατοτήτων εφαρμογής – Εάν ενεργοποιηθεί, οι ενημερώσεις δυνατοτήτων εφαρμογής θα εκτελούνται αυτόματα.

Επιλογές σύνδεσης

Για να αποκτήσετε πρόσβαση στις επιλογές ρυθμίσεων διακομιστή μεσολάβησης για ένα συγκεκριμένο προφίλ ενημερώσεων, κάντε κλικ στο στοιχείο **Ενημέρωση** στη δομή **Εγκατάσταση για προχωρημένους** (F5) και, στη συνέχεια, κάντε κλικ στις επιλογές **Προφίλ** > **Ενημερώσεις** > **Επιλογές σύνδεσης**. Κάντε κλικ στο αναπτυσσόμενο μενού **Λειτουργία μεσολάβησης** και επιλέξτε μία από τις τρεις παρακάτω επιλογές:

- Να μην χρησιμοποιείται διακομιστής μεσολάβησης
- Σύνδεση μέσω διακομιστή μεσολάβησης
- Χρήση καθολικών ρυθμίσεων διακομιστή μεσολάβησης

Επιλέξτε **Χρήση καθολικών ρυθμίσεων διακομιστή μεσολάβησης** για να χρησιμοποιούνται οι επιλογές διαμόρφωσης διακομιστή μεσολάβησης που έχουν καθοριστεί ήδη στον κλάδο **Εργαλεία** > **Διακομιστής μεσολάβησης** του δέντρου ρυθμίσεων για προχωρημένους.

Επιλέξτε **Να μην χρησιμοποιείται διακομιστής μεσολάβησης** για να καθορίσετε ότι δεν θα χρησιμοποιείται κανένας διακομιστής μεσολάβησης για την ενημέρωση του ESET Internet Security.

Η επιλογή **Σύνδεση μέσω διακομιστή μεσολάβησης** θα πρέπει να οριστεί αν:

• Χρησιμοποιείται διαφορετικός διακομιστής μεσολάβησης από εκείνον που ορίζεται στα **Εργαλεία** > **Διακομιστής μεσολάβησης** για την ενημέρωση του ESET Internet Security. Σε αυτήν τη διαμόρφωση, οι πληροφορίες για τον νέο διακομιστή μεσολάβησης θα πρέπει να καθορίζονται στη διεύθυνση του στοιχείου **Διακομιστής μεσολάβησης**, στη **Θύρα** επικοινωνίας (3128 από προεπιλογή) και στα στοιχεία **Όνομα χρήστη** και **Κωδικός πρόσβασης** για το διακομιστή μεσολάβησης, εάν απαιτείται.

• Οι ρυθμίσεις διακομιστή μεσολάβησης δεν ρυθμίζονται καθολικά, αλλά το ESET Internet Security θα συνδέεται με έναν διακομιστή μεσολάβησης για ενημερώσεις.
• Ο υπολογιστής σας είναι συνδεδεμένος στο Διαδίκτυο μέσω διακομιστή μεσολάβησης. Οι ρυθμίσεις λαμβάνονται από τον Internet Explorer κατά την εγκατάσταση του προγράμματος, αλλά αν αλλάξουν στη συνέχεια (π.χ. αν αλλάξετε πάροχο υπηρεσιών διαδικτύου), βεβαιωθείτε ότι οι ρυθμίσεις διακομιστή μεσολάβησης, που αναγράφονται σε αυτό το παράθυρο, είναι σωστές. Διαφορετικά, το πρόγραμμα δεν θα μπορεί να συνδεθεί με τους διακομιστές ενημέρωσης.

Η προεπιλεγμένη ρύθμιση για τον διακομιστή μεσολάβησης είναι **Χρήση καθολικών ρυθμίσεων διακομιστή μεσολάβησης**.

Χρήση απευθείας σύνδεσης εάν δεν υπάρχει διαθέσιμος διακομιστής μεσολάβησης – Εάν η επικοινωνία με το διακομιστή μεσολάβησης δεν είναι δυνατή, ο διακομιστής μεσολάβησης θα παρακάμπτεται.

Τα πεδία **Όνομα χρήστη** και **Κωδικός πρόσβασης** σε αυτή την ενότητα είναι ειδικά για το διακομιστή μεσολάβησης. Συμπληρώστε αυτά τα πεδία μόνο αν απαιτείται όνομα χρήστη και κωδικός πρόσβασης για να αποκτήσετε πρόσβαση στο διακομιστή μεσολάβησης. Αυτά τα πεδία θα πρέπει να συμπληρώνονται μόνο αν γνωρίζετε ότι απαιτείται κωδικός πρόσβασης για να αποκτήσετε πρόσβαση στο Internet μέσω διακομιστή μεσολάβησης.

Πώς να δημιουργήσετε εργασίες ενημέρωσης

Μπορείτε να ενεργοποιήσετε ενημερώσεις μη αυτόματα, κάνοντας κλικ στην επιλογή **Έλεγχος για ενημερώσεις** στο κύριο παράθυρο που εμφανίζεται αφού επιλέξετε **Ενημέρωση** από το κύριο μενού.

Οι ενημερώσεις είναι δυνατό επίσης να εκτελούνται ως προγραμματισμένες εργασίες. Για να διαμορφώσετε μια προγραμματισμένη εργασία, κάντε κλικ στις επιλογές **Εργαλεία** > **Περισσότερα εργαλεία** > **Προγραμματισμός εργασιών**. Από προεπιλογή, οι παρακάτω εργασίες είναι ενεργοποιημένες στο ESET Internet Security:

- **Τακτική αυτόματη ενημέρωση**
- **Αυτόματη ενημέρωση μετά τη σύνδεση μέσω τηλεφώνου**
- **Αυτόματη ενημέρωση μετά τη σύνδεση χρήστη**

Κάθε εργασία ενημέρωσης μπορεί να τροποποιηθεί ανάλογα με τις ανάγκες σας. Πέρα από τις προεπιλεγμένες εργασίες ενημέρωσης, μπορείτε να δημιουργήσετε νέες εργασίες ενημέρωσης με διαμόρφωση καθορισμένη από το χρήστη. Για περισσότερες πληροφορίες σχετικά με τη δημιουργία και τη διαμόρφωση εργασιών ενημέρωσης, ανατρέξτε στην ενότητα Χρονοδιάγραμμα εργασιών.

Παράθυρο διαλόγου - Απαιτείται επανεκκίνηση

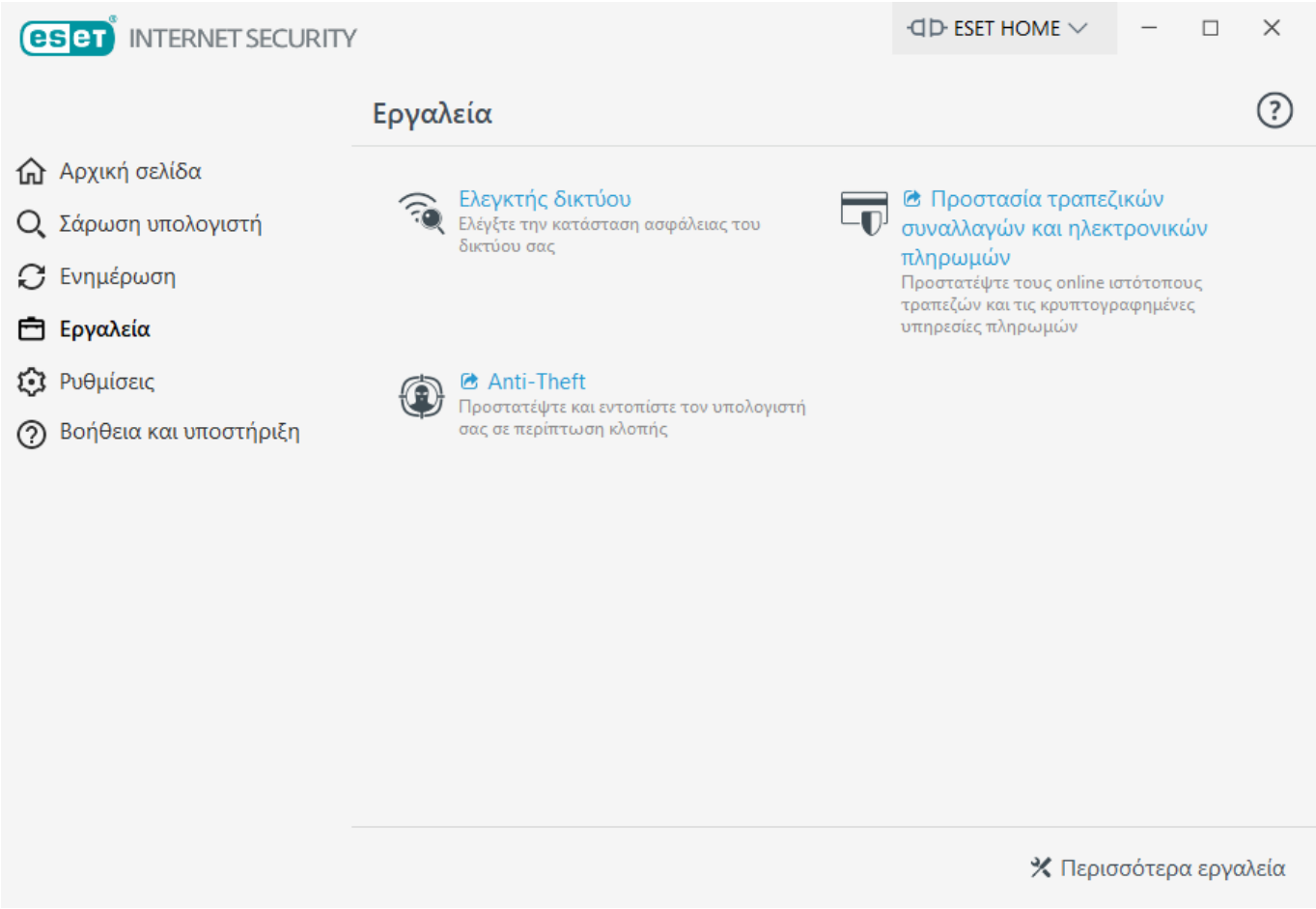
Απαιτείται επανεκκίνηση του υπολογιστή μετά την ενημέρωση του ESET Internet Security σε νέα έκδοση. Εκδίδονται νέες εκδόσεις του ESET Internet Security για την υλοποίηση βελτιώσεων ή τη διόρθωση ζητημάτων τα οποία δεν μπορούν να επιλυθούν από αυτόματες ενημερώσεις των μονάδων προγράμματος.

Η νέα έκδοση του ESET Internet Security μπορεί να εγκατασταθεί αυτόματα, με βάση τις ρυθμίσεις ενημέρωσης του προγράμματος ή μη αυτόματα κάνοντας λήψη και εγκατάσταση μιας νεότερης έκδοσης επάνω στην προηγούμενη.

Κάντε κλικ στο στοιχείο **Επανεκκίνηση τώρα** για να επανεκκινήσετε τον υπολογιστή σας. Εάν σκοπεύετε να επανεκκινήσετε τον υπολογιστή σας αργότερα, κάντε κλικ στο στοιχείο **Υπενθύμιση αργότερα**. Αργότερα, μπορείτε να επανεκκινήσετε τον υπολογιστή σας μη αυτόματα από την ενότητα **Αρχική σελίδα** στο κύριο παράθυρο του προγράμματος.

Εργαλεία

Το μενού **Εργαλεία** περιλαμβάνει μονάδες που βοηθούν να απλοποιηθεί η διαχείριση του προγράμματος και προσφέρει πρόσθετες επιλογές για προχωρημένους χρήστες.



Ελεγκτής δικτύου – Μειώστε τον κίνδυνο ζητημάτων ασφάλειας όταν συνδέεστε σε ένα δίκτυο.

Για περισσότερες πληροφορίες, δείτε την ενότητα Ελεγκτής δικτύου.

 **Προστασία τραπεζικών πληρωμών** – Το ESET Internet Security προστατεύει τους αριθμούς των πιστωτικών σας καρτών και άλλα ευαίσθητα προσωπικά δεδομένα καθώς χρησιμοποιείτε ιστότοπους τραπεζικών συναλλαγών ή διαδικτυακών πληρωμών. Θα ανοίγει ένα ασφαλές πρόγραμμα περιήγησης το οποίο θα παρέχει ασφαλέστερες τραπεζικές συναλλαγές.

 **Anti-Theft** – Εντοπίζει και βοηθά να βρείτε τη χαμένη συσκευή σας σε περίπτωση απώλειας ή κλοπής.

Κάντε κλικ στο θέμα Περισσότερα εργαλεία για να εμφανιστούν άλλα εργαλεία που προστατεύουν τον υπολογιστή σας (όπως η Καραντίνα).

Ελεγκτής δικτύου

Ο Ελεγκτής δικτύου μπορεί να σας βοηθήσει στην ταυτοποίηση τρωτών σημείων στο αξιόπιστο (οικιακό ή εταιρικό) δίκτυό σας (π.χ., ανοιχτές θύρες ή ένας αδύναμος κωδικός πρόσβασης δρομολογητή). Επίσης, παρέχει μια λίστα συνδεδεμένων συσκευών που είναι κατηγοριοποιημένες κατά τύπο συσκευής (π.χ., εκτυπωτής, δρομολογητής, κινητή συσκευή κ.λπ.) για να βλέπετε ποια είναι συνδεδεμένη στο δίκτυό σας (π.χ., κονσόλα παιχνιδιών, IoT ή άλλες έξυπνες οικιακές συσκευές).

Ο Ελεγκτής δικτύου σάς βοηθά στην ταυτοποίηση των τρωτών σημείων του δρομολογητή και αυξάνει το επίπεδο προστασίας όταν συνδέεστε σε ξένο δίκτυο.

Ο Ελεγκτής δικτύου δεν πραγματοποιεί εκ νέου ρύθμιση παραμέτρων του δρομολογητή. Αυτές τις αλλαγές πρέπει να τις κάνετε μόνοι σας χρησιμοποιώντας την εξειδικευμένη διασύνδεση του δρομολογητή σας. Οι οικιακοί δρομολογητές μπορεί να είναι πολύ ευάλωτοι σε κακόβουλο λογισμικό που χρησιμοποιείται για την εκκίνηση κατανεμημένων επιθέσεων άρνησης υπηρεσιών (DDoS). Εάν ο χρήστης δεν έχει αλλάξει τον κωδικό πρόσβασης του δρομολογητή από τον προεπιλεγμένο, είναι εύκολο για τους χάκερ να τον μαντέψουν και να συνδεθούν στον δρομολογητή σας για να ρυθμίσουν τις παραμέτρους του ξανά ή να θέσουν σε κίνδυνο το δίκτυό σας.

> ⚠ Συνιστάται να δημιουργήσετε έναν ισχυρό κωδικό πρόσβασης με αρκετά μεγάλο μήκος, ο οποίος θα περιλαμβάνει αριθμούς, σύμβολα ή κεφαλαία γράμματα. Για να ενισχύσετε ακόμα περισσότερο τον κωδικό πρόσβασης, χρησιμοποιήστε ποικιλία διαφορετικών τύπων χαρακτήρων.

Εάν το δίκτυο με το οποίο είστε συνδεδεμένοι έχει ρυθμιστεί ως αξιόπιστο, μπορείτε να επισημάνετε το δίκτυο ως «Το δίκτυό μου». Κάντε κλικ στην επιλογή **Επισήμανση ως «Το δίκτυό μου»** για να προσθέσετε μια ετικέτα «Το δίκτυό μου» στο δίκτυο. Αυτή η ετικέτα θα εμφανίζεται δίπλα στο δίκτυο σε όλο το ESET Internet Security για καλύτερη αναγνώριση και επισκόπηση της ασφάλειας. Κάντε κλικ στο στοιχείο **Κατάργηση επισήμανσης ως «Το δίκτυό μου»** για να καταργήσετε την ετικέτα.

Κάθε συσκευή που είναι συνδεδεμένη στο δίκτυό σας εμφανίζεται με τις βασικές πληροφορίες σε μια προβολή λίστας. Κάντε κλικ στη συγκεκριμένη συσκευή για να επεξεργαστείτε τη συσκευή ή για να προβάλετε λεπτομερείς πληροφορίες σχετικά με τη συσκευή.

Το αναπτυσσόμενο μενού **Δίκτυα** σάς επιτρέπει να φιλτράρετε συσκευές με βάση τα ακόλουθα κριτήρια:

- Συσκευές συνδεδεμένες με συγκεκριμένο δίκτυο
- Συσκευές συνδεδεμένες με **όλα τα δίκτυα**
- Μη κατηγοριοποιημένες συσκευές

Για να εμφανίζονται όλες οι συνδεδεμένες συσκευές σε προβολή ραντάρ, κάντε κλικ στο εικονίδιο ραντάρ  . Μετακινήστε τον δρομέα επάνω από το εικονίδιο μιας συσκευής για να δείτε βασικές πληροφορίες, όπως το όνομα δικτύου και την ημερομηνία που εντοπίστηκε τελευταία φορά.

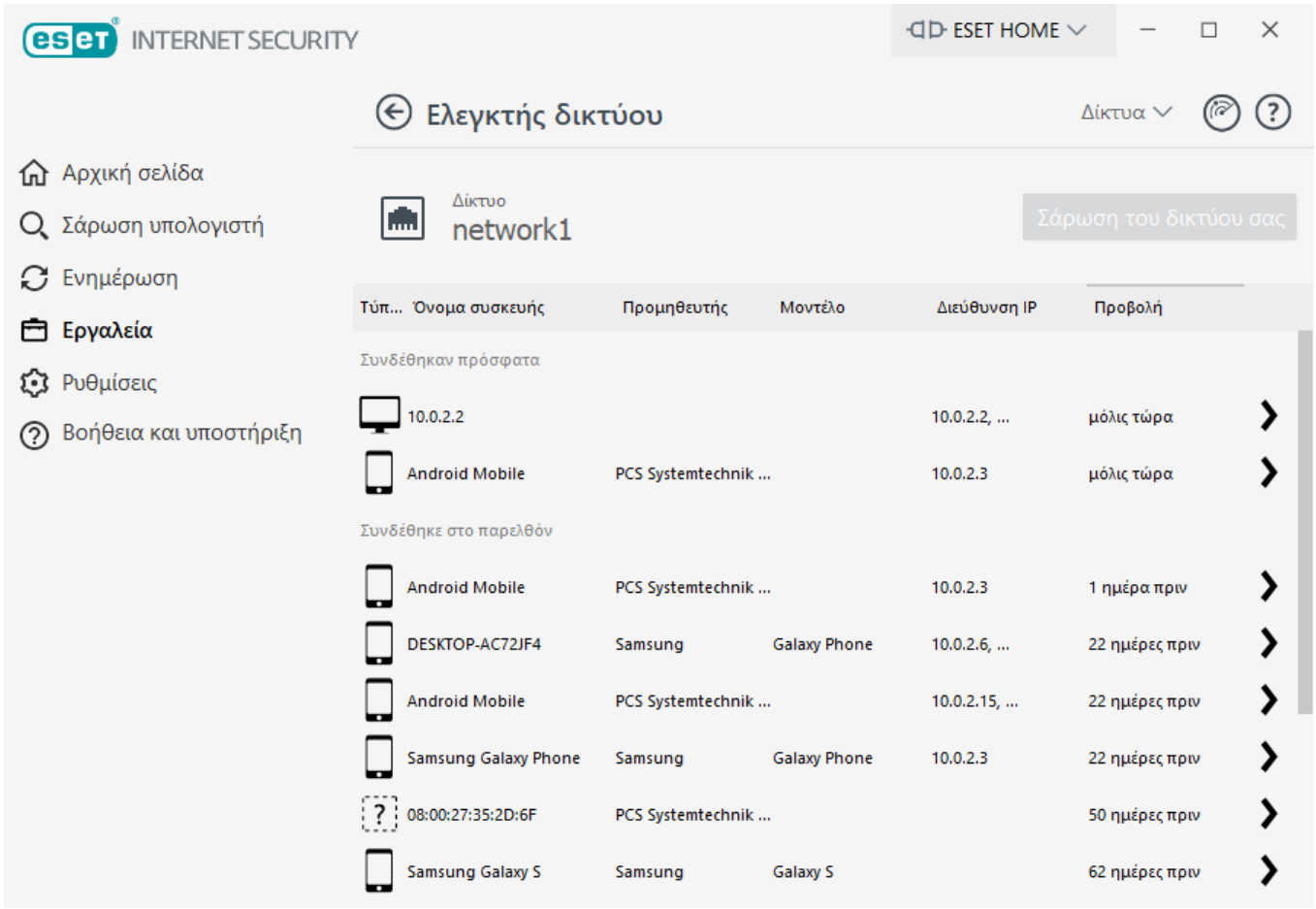
Κάντε κλικ στο εικονίδιο της συσκευής για να επεξεργαστείτε τη συσκευή ή για να δείτε λεπτομερείς πληροφορίες για τη συσκευή. Οι συσκευές που συνδέθηκαν πρόσφατα εμφανίζονται πιο κοντά στον δρομολογητή, ώστε να μπορείτε να τις εντοπίσετε πιο εύκολα.

Κάντε κλικ στο στοιχείο **Σάρωση του δικτύου σας** για να εκτελέσετε μη αυτόματα μια σάρωση του δικτύου με το οποίο είστε συνδεδεμένοι αυτή τη στιγμή. Το στοιχείο **Σάρωση του δικτύου σας** είναι διαθέσιμο μόνο για ένα αξιόπιστο δίκτυο. Ανατρέξτε στην ενότητα Γνωστά δίκτυα για να ελέγξετε ή να επεξεργαστείτε τις ρυθμίσεις δικτύου σας.

Μπορείτε να επιλέξτε από τις εξής επιλογές σάρωσης:

- Σάρωση όλων
- Σάρωση μόνο του δρομολογητή
- Σάρωση μόνο των συσκευών

> Να εκτελείτε σαρώσεις δικτύου μόνο σε αξιόπιστο δίκτυο. Εάν το κάνετε σε μη αξιόπιστα δίκτυα, θα πρέπει να γνωρίζετε ότι υπάρχει δυνητικός κίνδυνος.



Όταν ολοκληρωθεί η σάρωση, θα εμφανιστεί μια ειδοποίηση με έναν σύνδεσμο προς τις βασικές πληροφορίες για τη συσκευή ή μπορείτε να κάνετε διπλό κλικ στην ύποπτη συσκευή σε προβολή λίστας ή ραντάρ. Κάντε κλικ στην **Αντιμετώπιση προβλημάτων** για να δείτε τις επικοινωνίες που αποκλείστηκαν πρόσφατα. Περισσότερες πληροφορίες για την αντιμετώπιση προβλημάτων του Τείχους προστασίας.

Υπάρχουν δύο τύποι ειδοποιήσεων που εμφανίζονται από τη λειτουργική μονάδα Ελεγκτή δικτύου:

- **Νέα συσκευή συνδέθηκε στο δίκτυο** – Εμφανίζεται εάν μια συσκευή, που δεν έχει εντοπιστεί προηγουμένως, συνδεθεί με το δίκτυο ενώ είναι συνδεδεμένος ο χρήστης.

- **Βρέθηκαν νέες συσκευές δικτύου** – Εμφανίζεται εάν ξανασυνδεθείτε στο αξιόπιστο δίκτυό σας και υπάρχει τώρα μια συσκευή που δεν είχε εντοπιστεί προηγουμένως.

Και οι δύο τύποι ειδοποίησης σάς ενημερώνουν εάν κάποια μη εξουσιοδοτημένη συσκευή προσπαθεί να συνδεθεί με το δίκτυό σας. Κάντε κλικ στο στοιχείο **προβολή συσκευής** για να εμφανιστούν οι λεπτομέρειες της συσκευής.

Τι σημαίνουν τα εικονίδια στις συσκευές στον Ελεγκτή δικτύου;

	Το κίτρινο εικονίδιο με το αστέρι υποδεικνύει συσκευές που είναι νέες στο δίκτυο ή που έχουν ανιχνευτεί από την ESET για πρώτη φορά.
	Το κίτρινο εικονίδιο προσοχής υποδεικνύει ότι ο δρομολογητής σας μπορεί να παρουσιάζει τρωτά σημεία. Κάντε κλικ στο εικονίδιο στο προϊόν σας για πιο λεπτομερείς πληροφορίες σχετικά με το ζήτημα.

	Το κόκκινο εικονίδιο προειδοποίησης υποδεικνύει συσκευές, ότι ο δρομολογητής σας παρουσιάζει τρωτά σημεία και ότι ενδέχεται να έχουν μολυνθεί. Κάντε κλικ στο εικονίδιο στο προϊόν σας για πιο λεπτομερείς πληροφορίες σχετικά με το ζήτημα.
	Το μπλε εικονίδιο μπορεί να εμφανίζεται όταν το προϊόν ESET έχει πρόσθετες πληροφορίες για το δρομολογητή σας, αλλά δεν απαιτεί άμεσα προσοχή, επειδή δεν υπάρχουν κίνδυνοι ασφαλείας. Κάντε κλικ στο εικονίδιο στο προϊόν σας για πιο λεπτομερείς πληροφορίες.

Συσκευή δικτύου στον Ελεγκτή δικτύου

Εδώ μπορείτε να βρείτε λεπτομερείς πληροφορίες σχετικά με τη συσκευή, όπως οι παρακάτω:

- Όνομα συσκευής
- Τύπος συσκευής
- Τελευταία εμφάνιση
- Όνομα δικτύου
- Διεύθυνση IP
- Διεύθυνση MAC
- Λειτουργικά συστήματα

Το εικονίδιο μολυβιού υποδεικνύει ότι μπορείτε να τροποποιήσετε το όνομα ή τον τύπο της συσκευής.

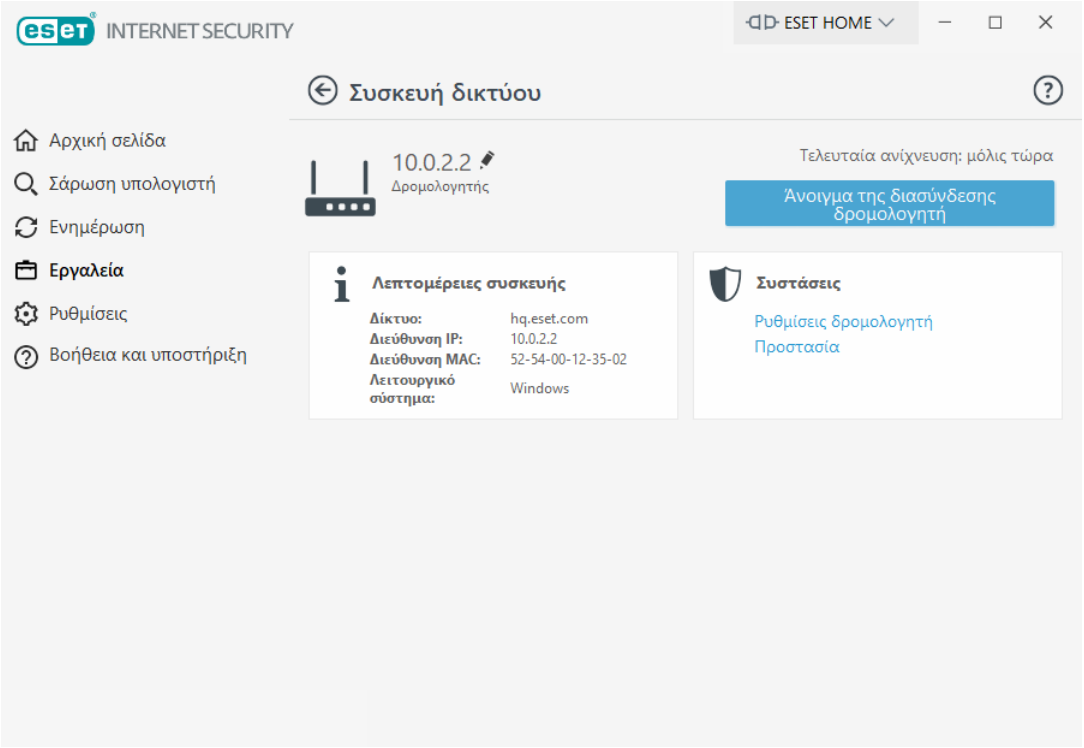
Κατάργηση από το ιστορικό – καταργήστε τη συσκευή από τη λίστα συσκευών. Αυτή η επιλογή είναι διαθέσιμη μόνο για συσκευές που δεν είναι συνδεδεμένες στο δίκτυό σας αυτήν τη στιγμή.

Για κάθε τύπο συσκευής, είναι διαθέσιμες οι παρακάτω ενέργειες:

Δρομολογητής

Ρυθμίσεις δρομολογητή – Αποκτήστε πρόσβαση στις ρυθμίσεις του δρομολογητή από τη διασύνδεση διαδικτύου ή την εφαρμογή για κινητές συσκευές ή κάντε κλικ στο στοιχείο **Άνοιγμα της διασύνδεσης δρομολογητή**. Εάν διαθέτετε έναν δρομολογητή που παρέχεται από τον πάροχο υπηρεσιών διαδικτύου, ενδέχεται να χρειαστεί να επικοινωνήσετε με την τεχνική υποστήριξη του παρόχου υπηρεσιών διαδικτύου ή τον κατασκευαστή του δρομολογητή για να επιλύσετε ζητήματα ασφαλείας που έχουν ανιχνευτεί. Να ακολουθείτε πάντα τις κατάλληλες προφυλάξεις ασφαλείας, όπως υποδεικνύεται στον οδηγό χρήστη του δρομολογητή σας.

Προστασία – Για να προστατέψετε το δρομολογητή και το δίκτυό σας από επιθέσεις κυβερνοασφάλειας, ακολουθήστε τις παρακάτω βασικές συστάσεις.

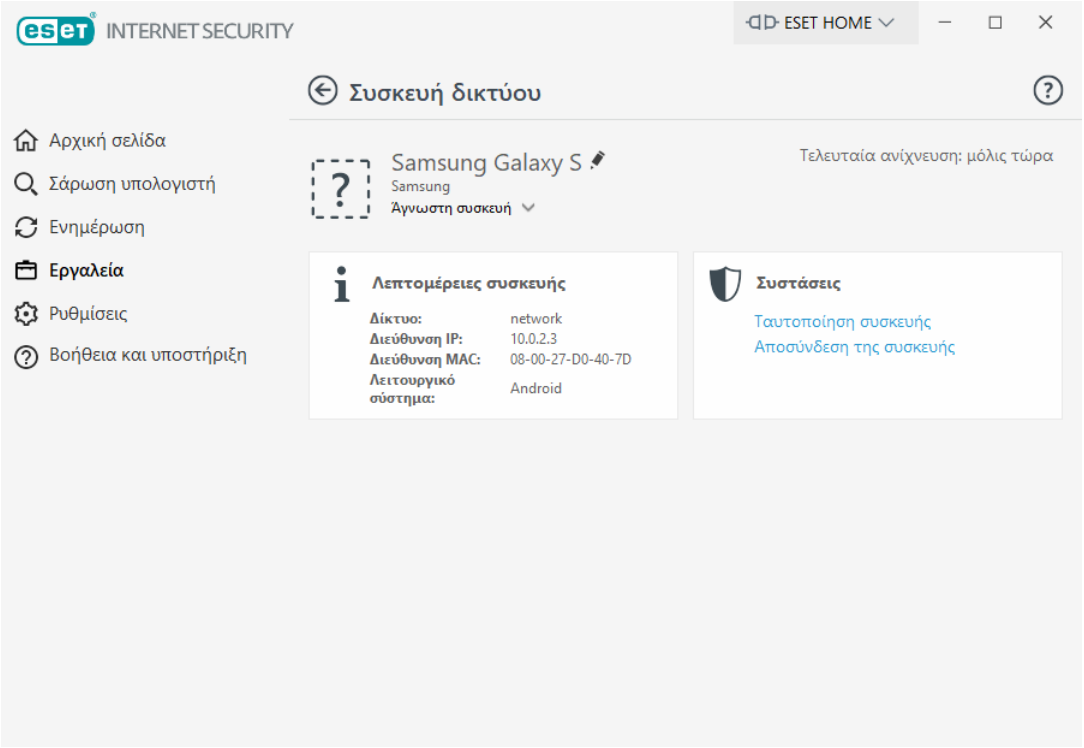


Συσκευή δικτύου

Ταυτοποίηση συσκευής – Εάν δεν είστε βέβαιοι σχετικά με τη συσκευή που είναι συνδεδεμένη με το δίκτυό σας, ελέγξτε το όνομα του προμηθευτή ή του κατασκευαστή κάτω από το όνομα της συσκευής. Αυτό μπορεί να σας βοηθήσει να ταυτοποιήσετε τον τύπο συσκευής. Μπορείτε να αλλάξετε το όνομα της συσκευής για μελλοντική αναφορά.

Αποσύνδεση της συσκευής – Εάν δεν είστε βέβαιοι ότι μια συνδεδεμένη συσκευή είναι ασφαλής για το δίκτυο ή τις συσκευές σας, διαχειριστείτε την πρόσβαση δικτύου για αυτήν τη συσκευή στις ρυθμίσεις δρομολογητή σας ή αλλάξτε τον κωδικό πρόσβασης στο δίκτυό σας.

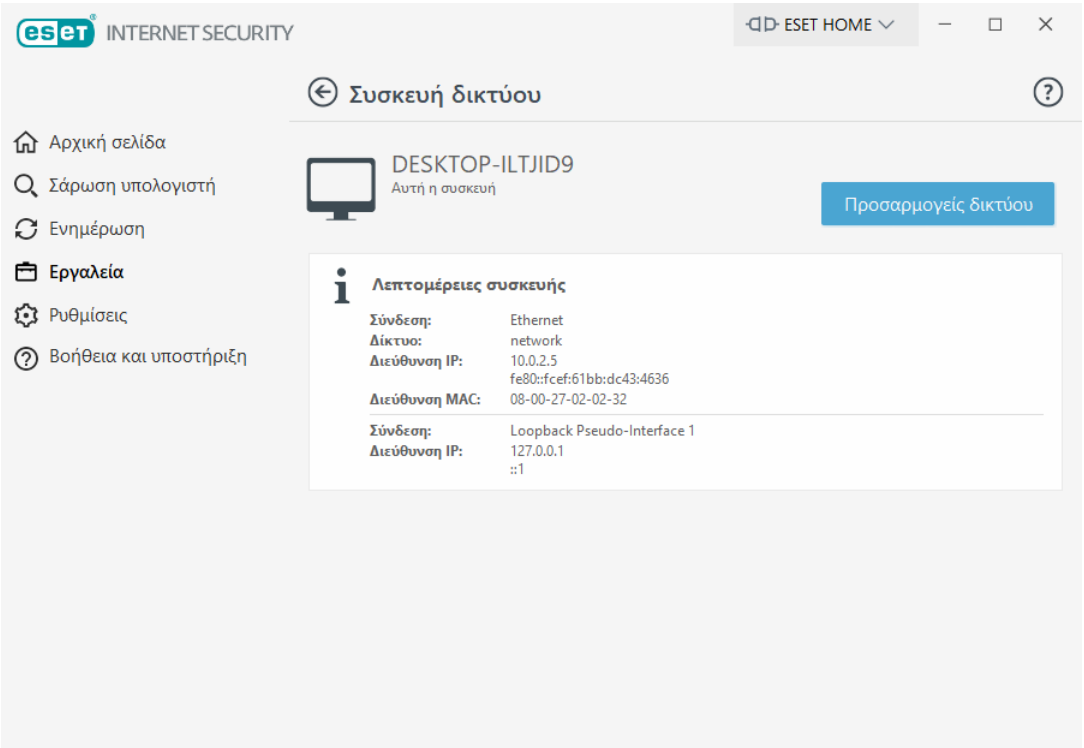
Προστασία – Για να προστατέψετε τη συσκευή σας από επιθέσεις και κακόβουλο λογισμικό, εγκαταστήστε την προστασία κυβερνοασφάλειας στη συσκευή σας και διατηρείτε πάντα ενημερωμένο το λειτουργικό σύστημα και το εγκατεστημένο λογισμικό. Για να παραμείνετε προστατευμένοι, μη συνδέεστε σε μη ασφαλή δίκτυα Wi-Fi.



Αυτή η συσκευή

Αυτή η συσκευή αντιπροσωπεύει τον υπολογιστή σας στο δίκτυο.

Προσαρμογείς δικτύου – Εμφανίζει πληροφορίες για τους προσαρμογείς δικτύου σας.



Ειδοποιήσεις | Ελεγκτής δικτύου

Ακολουθούν αρκετές ειδοποιήσεις οι οποίες μπορεί να εμφανιστούν όταν το ESET Internet Security ανιχνεύει κάποιο ζήτημα τρωτού σημείου στο δρομολογητή σας. Κάθε ειδοποίηση περιέχει μια σύντομη περιγραφή και παρέχει κάποια λύση ή βήματα που θα πρέπει να εκτελεστούν για να ελαχιστοποιηθεί ο κίνδυνος τρωτού σημείου στο δρομολογητή σας. Εάν δεν είστε εξοικειωμένοι με τις αλλαγές του δρομολογητή σας, συνιστάται να επικοινωνήσετε με τον κατασκευαστή του δρομολογητή ή τον πάροχο υπηρεσιών διαδικτύου.

Βρέθηκαν δυνητικά τρωτά σημεία
Ο δρομολογητής σας μπορεί να περιέχει γνωστά τρωτά σημεία που θα μπορούσαν να τον καταστήσουν εύκολο στόχο επίθεσης και εκμετάλλευσης. Ενημερώστε το υλικολογισμικό του δρομολογητή σας.

Βρέθηκε τρωτό σημείο
Ο δρομολογητής σας περιέχει γνωστά τρωτά σημεία που τον καθιστούν εύκολο στόχο επίθεσης και εκμετάλλευσης. Ενημερώστε το υλικολογισμικό του δρομολογητή σας.

Εντοπίστηκε απειλή
Ο δρομολογητής σας έχει μολυνθεί από κακόβουλο λογισμικό. Επανεκκινήστε το δρομολογητή σας και επαναλάβετε τη σάρωση.

Ασθενής κωδικός πρόσβασης δρομολογητή
Ο κωδικός πρόσβασης στο δρομολογητή σας είναι αδύναμος και μπορεί εύκολα κάποιος να τον μαντέψει. Αλλάξτε τον κωδικό πρόσβασης στο δρομολογητή σας.

Κακόβουλη ανακατεύθυνση δικτύου
Η κυκλοφορία σας στο Internet φαίνεται να ανακατευθύνεται σε κακόβουλους ιστότοπους. Αυτό μπορεί να σημαίνει ότι ο δρομολογητής σας έχει παραβιαστεί. Αλλάξτε τη ρύθμιση διακομιστή DNS στο δρομολογητή σας.

Άνοιγμα υπηρεσιών δικτύου
Ο δρομολογητής σας εκτελεί υπηρεσίες δικτύου, τις οποίες ενδέχεται κάποιοι να εκμεταλλευτούν. Αυτό μπορεί να οφείλεται σε κακή διαμόρφωση ή στο ότι ο δρομολογητής σας έχει παραβιαστεί. Ελέγξτε τη διαμόρφωση του δρομολογητή σας.

Ευαίσθητες πληροφορίες ανοιχτού δικτύου
Ο δρομολογητής σας εκτελεί ευαίσθητες υπηρεσίες δικτύου, τις οποίες ενδέχεται κάποιοι να εκμεταλλευτούν. Αυτό μπορεί να οφείλεται σε κακή διαμόρφωση ή στο ότι ο δρομολογητής σας έχει παραβιαστεί. Ελέγξτε τη διαμόρφωση του δρομολογητή σας.

Μη ενημερωμένο υλικολογισμικό
Το υλικολογισμικό στο δρομολογητή σας δεν είναι ενημερωμένο και ίσως περιέχει τρωτά σημεία. Ενημερώστε το υλικολογισμικό στο δρομολογητή σας.

Κακόβουλη ρύθμιση δρομολογητή
Αυτός ο διακομιστής DNS που χρησιμοποιείται από το δρομολογητή σας είναι κακόβουλος και μπορεί να σας κατευθύνει σε επικίνδυνους ιστότοπους. Αυτό μπορεί να σημαίνει ότι ο δρομολογητής σας έχει παραβιαστεί. Αλλάξτε τη ρύθμιση διακομιστή DNS στο δρομολογητή σας.

Υπηρεσίες δικτύου
Ο δρομολογητής σας εκτελεί συνηθισμένες υπηρεσίες δικτύου. Αυτές οι υπηρεσίες είναι απαραίτητες για το δίκτυο και είναι μάλλον ασφαλείς. Ελέγξτε τη διαμόρφωση του δρομολογητή σας.

Εργαλεία στο ESET Internet Security

Το μενού **Εργαλεία** περιλαμβάνει μονάδες που βοηθούν να απλοποιηθεί η διαχείριση του προγράμματος και προσφέρει πρόσθετες επιλογές για προχωρημένους χρήστες. Αυτά τα εργαλεία είναι ορατά μόνο αν κάνετε κλικ στην επιλογή **Περισσότερα εργαλεία** στην κάτω δεξιά γωνία.

Το μενού αυτό περιλαμβάνει τα παρακάτω εργαλεία:

 Αρχεία καταγραφής

 Αναφορά ασφαλείας

 Εκτελούμενες διεργασίες (αν είναι ενεργοποιημένη η δυνατότητα ESET LiveGrid® στο ESET Internet Security)

 Συνδέσεις δικτύου (εάν το Firewall είναι ενεργοποιημένο στο ESET Internet Security)

 ESET SysInspector

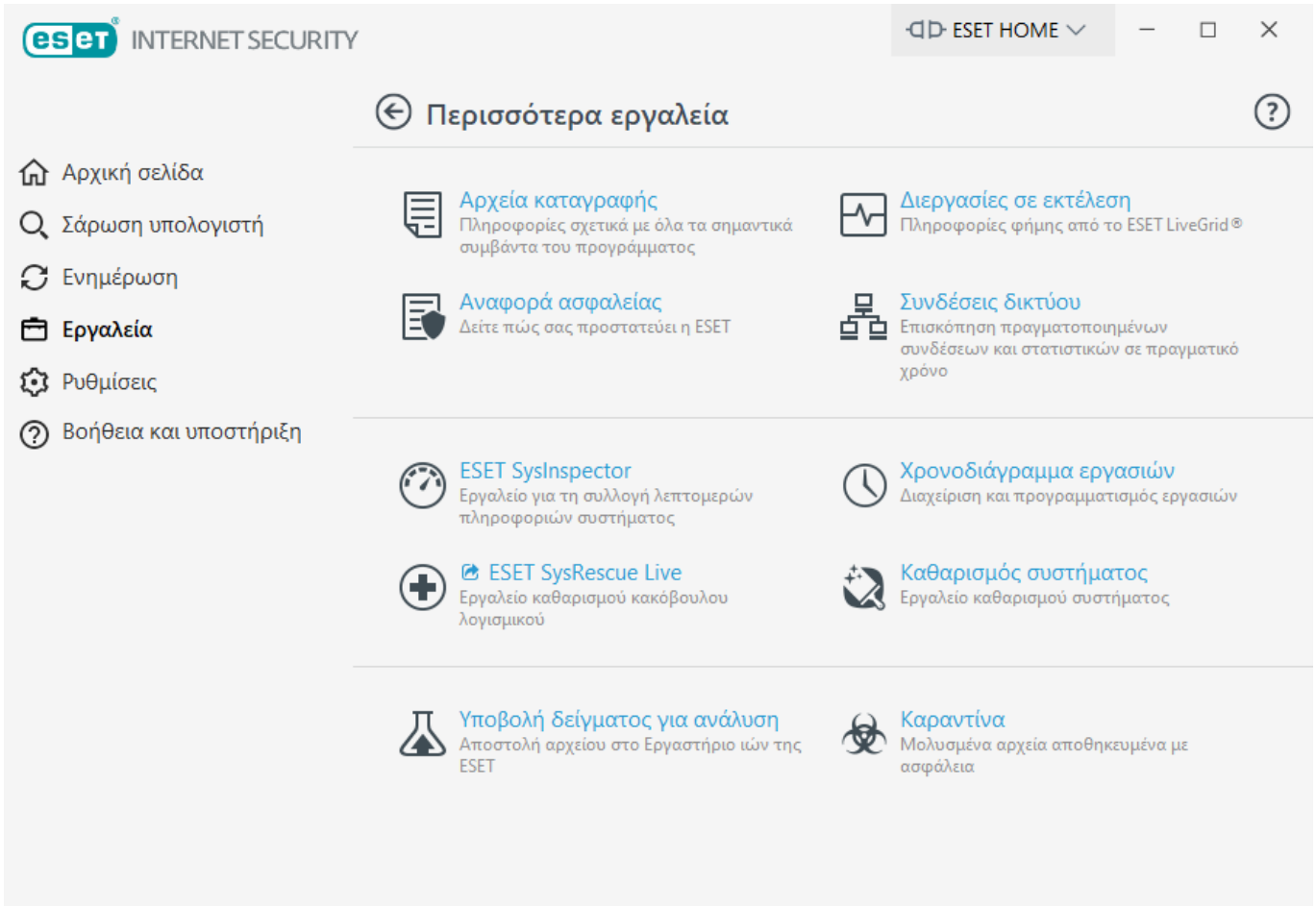
 ESET SysRescue Live – Σας ανακατευθύνει στον ιστότοπο ESET SysRescue Live, όπου μπορείτε να κάνετε λήψη της εικόνας CD/DVD ESET SysRescue Live.iso.

 Προγραμματισμός εργασιών

 Καθαρισμός συστήματος – Σας βοηθά να επαναφέρετε τον υπολογιστή σας σε κατάσταση χρήσης μετά από τον καθαρισμό της απειλής.

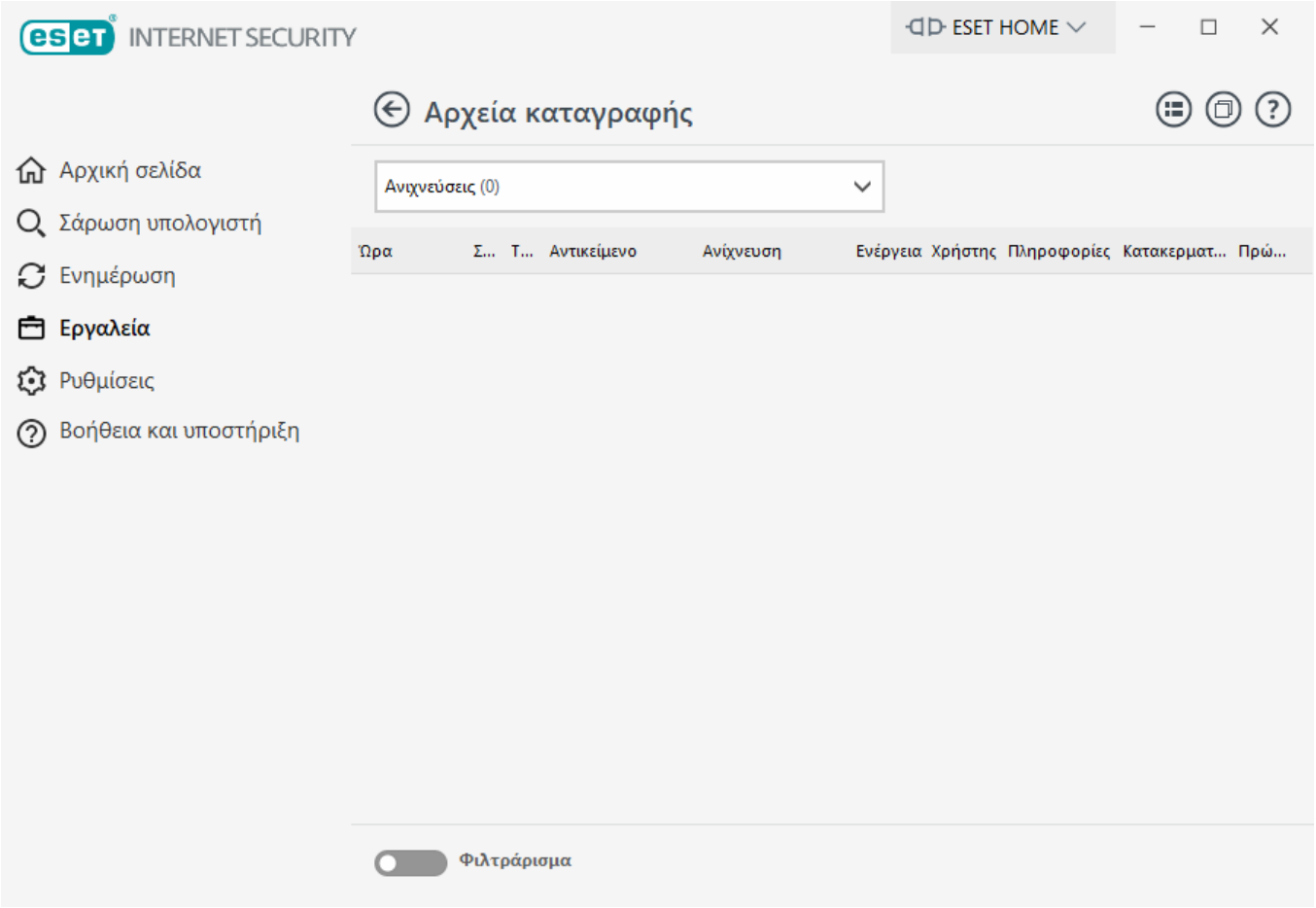
 Υποβολή δείγματος για ανάλυση – Σας επιτρέπει να υποβάλετε ένα ύποπτο αρχείο για ανάλυση στο Εργαστήριο ερευνών της ESET (ενδέχεται να μην είναι διαθέσιμο με βάση τη ρύθμιση παραμέτρων του ESET LiveGrid®).

 Καραντίνα



Αρχεία καταγραφής

Τα αρχεία καταγραφής περιέχουν πληροφορίες για σημαντικά συμβάντα του προγράμματος που έχουν προκύψει και παρέχουν μια επισκόπηση των απειλών που ανιχνεύτηκαν. Η καταγραφή είναι σημαντικό μέρος της ανάλυσης συστήματος, της ανίχνευσης απειλών και της αντιμετώπισης προβλημάτων. Η καταγραφή εκτελείται ενεργά στο παρασκήνιο χωρίς αλληλεπίδραση του χρήστη. Οι πληροφορίες καταγράφονται με βάση τις τρέχουσες ρυθμίσεις λεπτομερειών καταγραφής. Είναι δυνατόν να δείτε μηνύματα κειμένου και αρχεία καταγραφής απευθείας από το περιβάλλον του ESET Internet Security, καθώς και να αρχειοθετήσετε αρχεία καταγραφής.



Η πρόσβαση στα αρχεία καταγραφής είναι δυνατή από το κύριο παράθυρο του προγράμματος κάνοντας κλικ στα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής**. Επιλέξτε τον τύπο αρχείου καταγραφής που θέλετε από το αναπτυσσόμενο μενού **Καταγραφή**. Είναι διαθέσιμα τα παρακάτω αρχεία καταγραφής:

• **Ανιχνεύσεις** – Αυτό το αρχείο καταγραφής προσφέρει λεπτομερείς πληροφορίες για ανιχνεύσεις και εισβολές που ανιχνεύτηκαν από το ESET Internet Security. Οι πληροφορίες του αρχείου καταγραφής περιλαμβάνουν τον χρόνο ανίχνευσης, τον τύπο σάρωσης, τον τύπο αντικειμένου, την τοποθεσία αντικειμένου, το όνομα της ανίχνευσης, την ενέργεια που εκτελέστηκε, το όνομα του χρήστη που ήταν συνδεδεμένος όταν ανιχνεύτηκε η εισβολή, τον κατακερματισμό και την πρώτη εμφάνιση. Οι εισβολές που δεν καθαρίστηκαν επισημαίνονται πάντα με κόκκινο κείμενο σε ανοιχτό κόκκινο φόντο. Οι εισβολές που καθαρίστηκαν επισημαίνονται με κίτρινο κείμενο σε λευκό φόντο. Οι PUA ή ενδεχομένως μη ασφαλείς εφαρμογές που δεν καθαρίστηκαν επισημαίνονται με κίτρινο κείμενο σε λευκό φόντο.

• **Συμβάντα** – Στο αρχείο καταγραφής συμβάντων καταγράφονται όλες οι σημαντικές ενέργειες που εκτελούνται από το ESET Internet Security. Το αρχείο καταγραφής συμβάντων περιέχει πληροφορίες για συμβάντα και σφάλματα που έχουν προκύψει στο πρόγραμμα Είναι σχεδιασμένο για να λύνουν προβλήματα οι διαχειριστές συστήματος και οι χρήστες. Συχνά οι πληροφορίες που βρίσκονται εδώ μπορεί να σας βοηθήσουν να βρείτε λύση σε ένα πρόβλημα που παρουσιάζει το πρόγραμμα.

• **Σάρωση υπολογιστή** – Τα αποτελέσματα όλων των προηγούμενων σαρώσεων εμφανίζονται σε αυτό το παράθυρο. Κάθε γραμμή αντιστοιχεί σε έναν έλεγχο του υπολογιστή. Κάντε διπλό κλικ σε οποιαδήποτε καταχώριση για να δείτε λεπτομέρειες της επιλεγμένης σάρωσης.

• **HIPS** – Περιέχει εγγραφές συγκεκριμένων κανόνων HIPS που επισημαίνονται για καταγραφή. Το

πρωτόκολλο εμφανίζει την εφαρμογή που ενεργοποίησε τη λειτουργία, το αποτέλεσμα (αν επιτράπηκε ή απαγορεύτηκε ο κανόνας) και το όνομα του κανόνα.

• **Προστασία δικτύου** – Το αρχείο καταγραφής προστασίας δικτύου εμφανίζει όλες τις απομακρυσμένες επιθέσεις που ανιχνεύτηκαν από το Τείχος προστασίας, την Προστασία από επιθέσεις δικτύου (IDS) και την Προστασία από botnet. Εδώ θα βρείτε πληροφορίες για οποιαδήποτε επίθεση έγινε στον υπολογιστή σας. Στη στήλη Συμβάν αναγράφονται οι επιθέσεις που ανιχνεύτηκαν. Στη στήλη Προέλευση αναγράφονται περισσότερες πληροφορίες για τον εισβολέα. Η στήλη Πρωτόκολλο περιλαμβάνει το πρωτόκολλο επικοινωνίας που χρησιμοποιήθηκε για την επίθεση. Η ανάλυση του αρχείου καταγραφής προστασίας δικτύου μπορεί να σας βοηθήσει να ανιχνεύσετε έγκαιρα προσπάθειες εισβολής στο σύστημα, ώστε να εμποδίσετε τη μη εξουσιοδοτημένη πρόσβαση στο σύστημά σας. Για περισσότερες πληροφορίες σχετικά με επιθέσεις δικτύου, δείτε τις Επιλογές IDS και επιλογές για προχωρημένους.

• **Φιλτραρισμένοι ιστότοποι** – Αυτή η λίστα είναι χρήσιμη αν θέλετε να δείτε μια λίστα με ιστότοπους που αποκλείστηκαν από την Προστασία πρόσβασης στον διαδικτύο ή τη λειτουργία Γονικός έλεγχος. Κάθε καταγραφή περιλαμβάνει την ώρα, τη διεύθυνση URL, το χρήστη και την εφαρμογή που δημιούργησε μια σύνδεση με έναν συγκεκριμένο ιστότοπο.

• **Προστασία Antispam** – Περιέχει εγγραφές που σχετίζονται με μηνύματα ηλεκτρονικής αλληλογραφίας που επισημάνθηκαν ως ανεπιθύμητα.

• **Γονικός έλεγχος** – Εμφανίζει ιστοσελίδες που αποκλείστηκαν ή επιτράπηκαν από τον Γονικό έλεγχο. Η στήλη Τύπος αντιστοίχισης και Τιμές αντιστοίχισης εξηγεί πώς εφαρμόστηκαν οι κανόνες φιλτραρίσματος.

• **Έλεγχος συνδεδεμένων συσκευών** – Περιέχει εγγραφές αφαιρούμενων μέσων ή συσκευών που συνδέθηκαν με τον υπολογιστή. Στο αρχείο καταγραφής θα εγγραφούν μόνο συσκευές με αντίστοιχους κανόνες Ελέγχου συνδεδεμένων συσκευών. Αν ο κανόνας δεν αντιστοιχεί σε μια συνδεδεμένη συσκευή, δεν θα δημιουργηθεί εγγραφή για συνδεδεμένη συσκευή. Μπορείτε, επίσης, να δείτε λεπτομέρειες όπως ο τύπος συσκευής, ο αριθμός σειράς, το όνομα του κατασκευαστή και το μέγεθος του μέσου (αν είναι διαθέσιμο).

• **Προστασία κάμερας** – Περιέχει εγγραφές για εφαρμογές που αποκλείστηκαν από την προστασία κάμερας.

Επιλέξτε τα περιεχόμενα οποιουδήποτε αρχείου καταγραφής και πιέστε **CTRL + C** για να τα αντιγράψετε στο πρόχειρο. Κρατήστε πατημένο το πλήκτρο **CTRL** ή **SHIFT** για να επιλέξετε πολλές καταχωρίσεις.

Κάντε κλικ στο στοιχείο **Φιλτράρισμα** για να ανοίξετε το παράθυρο Φιλτράρισμα αρχείων καταγραφής, όπου μπορείτε να καθορίσετε τα κριτήρια φιλτραρίσματος.

Κάντε δεξί κλικ σε μια συγκεκριμένη εγγραφή για να ανοίξει το μενού περιβάλλοντος. Στο μενού περιβάλλοντος είναι διαθέσιμες οι ακόλουθες επιλογές:

• **Εμφάνιση** – Εμφανίζει σε νέο παράθυρο πιο λεπτομερείς πληροφορίες σχετικά με το επιλεγμένο αρχείο καταγραφής.

• **Φιλτράρισμα ίδιων εγγραφών** – Μετά την ενεργοποίηση αυτού του φίλτρου, θα βλέπετε μόνο εγγραφές ίδιου τύπου (διαγνωστικοί έλεγχοι, προειδοποιήσεις κ.λπ.).

• **Φίλτρο** – Όταν κάνετε κλικ σε αυτή την επιλογή, το παράθυρο Φιλτράρισμα αρχείων

καταγραφής θα σας επιτρέψει να καθορίσετε κριτήρια φιλτραρίσματος για συγκεκριμένες καταχωρίσεις του αρχείου καταγραφής.

• **Ενεργοποίηση φίλτρου** – Ενεργοποιεί τις ρυθμίσεις φιλτραρίσματος.

• **Απενεργοποίηση φίλτρου** – Εκκαθαρίζει όλες τις ρυθμίσεις φίλτρου (όπως περιγράφεται παραπάνω).

• **Αντιγραφή/Αντιγραφή όλων** – Αντιγράφει πληροφορίες σχετικά με τις επιλεγμένες εγγραφές στο παράθυρο.

• **Κατάργηση/Κατάργηση όλων** – Καταργεί τις επιλεγμένες εγγραφές ή όλες τις εγγραφές που εμφανίζονται. Αυτή η ενέργεια απαιτεί δικαιώματα διαχειριστή.

• **Εξαγωγή/Εξαγωγή όλων** – Εξάγει πληροφορίες σχετικά με τις επιλεγμένες εγγραφές ή όλες τις εγγραφές σε μορφή XML.

• **Εύρεση/Εύρεση επόμενου/Εύρεση προηγούμενου** – Αφού κάνετε κλικ σε αυτήν την επιλογή, μπορείτε να καθορίσετε τα κριτήρια φιλτραρίσματος για να επισημάνετε τη συγκεκριμένη καταχώρηση χρησιμοποιώντας το παράθυρο «Φιλτράρισμα αρχείων καταγραφής».

• **Περιγραφή ανίχνευσης** – Ανοίγει την Εγκυκλοπαίδεια απειλών της ESET, η οποία περιέχει λεπτομερείς πληροφορίες για τους κινδύνους και τα συμπτώματα της καταγεγραμμένης εισβολής.

• **Δημιουργία εξαίρεσης** – Δημιουργεί μια νέα Εξαίρεση ανίχνευσης χρησιμοποιώντας έναν οδηγό (δεν είναι διαθέσιμο για ανιχνεύσεις κακόβουλου λογισμικού).

Φιλτράρισμα αρχείων καταγραφής

Κάντε κλικ στο στοιχείο **Φιλτράρισμα** στη διαδρομή **Εργαλεία** > **Περισσότερα εργαλεία** > **Αρχεία καταγραφής** για τον καθορισμό των κριτηρίων φιλτραρίσματος.

Η δυνατότητα φιλτραρίσματος αρχείων καταγραφής θα σας βοηθήσει να βρείτε πληροφορίες που αναζητάτε, ιδιαίτερα εάν υπάρχουν πολλές καταχωρίσεις. Σας επιτρέπει να περιορίσετε τον αριθμό καταχωρίσεων αρχείων καταγραφής, για παράδειγμα εάν αναζητάτε έναν συγκεκριμένο τύπο συμβάντος, κατάστασης ή χρονικού διαστήματος. Μπορείτε να φιλτράρετε τις καταχωρίσεις αρχείων καταγραφής καθορίζοντας ορισμένες επιλογές αναζήτησης και έτσι θα εμφανιστούν στο παράθυρο «Αρχεία καταγραφής» μόνο αρχεία που είναι σχετικά (σύμφωνα με αυτές τις επιλογές αναζήτησης).

Πληκτρολογήστε τη λέξη κλειδί που αναζητάτε στο πεδίο **Εύρεση κειμένου**. Χρησιμοποιήστε το αναπτυσσόμενο μενού **Αναζήτηση σε στήλες** για να περιορίσετε την αναζήτησή σας. Επιλέξτε μία ή περισσότερες καταχωρίσεις από το αναπτυσσόμενο μενού **Τύποι καταχωρίσεων αρχείων καταγραφής**. Καθορίστε το στοιχείο **Χρονική περίοδος** για το οποίο θέλετε να εμφανιστούν αποτελέσματα. Επίσης, μπορείτε να χρησιμοποιήσετε περισσότερες επιλογές αναζήτησης, όπως **Αντιστοίχιση μόνο ολόκληρων λέξεων** ή **Διάκριση πεζών-κεφαλαίων**.

Εύρεση κειμένου

Πληκτρολογήστε μια συμβολοσειρά (λέξη ή μέρος μιας λέξης). Θα εμφανιστούν μόνο οι καταχωρίσεις που περιέχουν αυτή τη συμβολοσειρά. Οι άλλες καταχωρίσεις θα παραλειφθούν.

Αναζήτηση σε στήλες

Επιλέξτε τις στήλες που θα λαμβάνονται υπόψη κατά την αναζήτηση. Μπορείτε να επιλέξετε μία ή περισσότερες στήλες που θα χρησιμοποιηθούν για την αναζήτηση.

Τύποι εγγραφών

Επιλέξτε έναν ή περισσότερους τύπους καταχωρίσεων αρχείων καταγραφής από το αναπτυσσόμενο μενού:

• **Εγγραφές διαγνωστικού ελέγχου** – Καταγράφει πληροφορίες απαραίτητες για τη ρύθμιση του προγράμματος και όλες τις παραπάνω εγγραφές.

• **Εγγραφές πληροφοριών** – Καταγράφει πληροφοριακά μηνύματα, συμπεριλαμβανομένων μηνυμάτων επιτυχούς ενημέρωσης, καθώς και όλες τις παραπάνω εγγραφές.

• **Προειδοποιήσεις** – Καταγράφει κρίσιμα σφάλματα και προειδοποιητικά μηνύματα.

• **Σφάλματα** – Καταγράφονται σφάλματα όπως «Σφάλμα κατά τη λήψη του αρχείου» και κρίσιμα σφάλματα.

• **Κρίσιμες προειδοποιήσεις** – Καταγράφει μόνο κρίσιμα σφάλματα (σφάλμα κατά την έναρξη της προστασίας Antivirus

Χρονική περίοδος

Καθορίστε το χρονικό διάστημα για το οποίο θέλετε να εμφανιστούν αποτελέσματα.

• **Δεν καθορίζεται** (προεπιλογή) - Δεν γίνεται αναζήτηση μέσα σε μια χρονική περίοδο. Η αναζήτηση γίνεται σε ολόκληρο το αρχείο καταγραφής.

• **Τελευταία ημέρα**

• **Τελευταία εβδομάδα**

• **Τελευταίος μήνας**

• **Χρονική περίοδος** - Μπορείτε να καθορίσετε την ακριβή χρονική περίοδο (Από: και Έως:) για να φιλτράρετε μόνο τις καταχωρίσεις της καθορισμένης χρονικής περιόδου.

Αντιστοίχιση μόνο ολόκληρων λέξεων

Χρησιμοποιήστε αυτό το πλαίσιο ελέγχου εάν θέλετε να κάνετε αναζήτηση για ολόκληρες λέξεις για πιο ακριβή αποτελέσματα.

Διάκριση πεζών-κεφαλαίων

Ενεργοποιήστε αυτή την επιλογή εάν θεωρείτε σημαντική τη χρήση κεφαλαίων ή πεζών γραμμάτων κατά το φιλτράρισμα. Όταν διαμορφώσετε τις επιλογές φιλτραρίσματος/αναζήτησης, κάντε κλικ στο στοιχείο **OK** για να εμφανιστούν οι φιλτραρισμένες καταχωρίσεις αρχείων καταγραφής ή το στοιχείο **Εύρεση** για να ξεκινήσει η αναζήτηση. Τα αρχεία καταγραφής αναζητούνται από πάνω προς τα κάτω, ξεκινώντας από την τρέχουσα θέση σας (την καταχώριση που επισημαίνεται). Η αναζήτηση διακόπτεται όταν εντοπιστεί η πρώτη καταχώριση που αντιστοιχεί. Πατήστε το πλήκτρο **F3** για αναζήτηση της επόμενης καταχώρισης ή κάντε δεξί κλικ και επιλέξτε **Εύρεση** για

να περιορίσετε τις επιλογές αναζήτησης.

Διαμόρφωση καταγραφής

Στη διαμόρφωση Καταγραφής του ESET Internet Security παρέχεται πρόσβαση από το κύριο παράθυρο του προγράμματος. Κάντε κλικ στο κουμπί **Ρυθμίσεις** > **Εγκατάσταση για προχωρημένους** > **Εργαλεία** > **Αρχεία καταγραφής**. Η ενότητα καταγραφής χρησιμοποιείται για τον καθορισμό του τρόπου διαχείρισης των αρχείων καταγραφής. Το πρόγραμμα διαγράφει αυτόματα παλαιότερες καταγραφές για να εξοικονομεί χώρο στο σκληρό δίσκο. Μπορείτε να καθορίσετε τις παρακάτω επιλογές για τα αρχεία καταγραφής:

Ελάχιστο επίπεδο λεπτομερειών καταγραφής – Καθορίζει το ελάχιστο επίπεδο λεπτομερειών των συμβάντων που θα καταγράφονται.

- **Εγγραφές διαγνωστικού ελέγχου** – Καταγράφει πληροφορίες απαραίτητες για τη ρύθμιση του προγράμματος και όλες τις παραπάνω εγγραφές.
- **Εγγραφές πληροφοριών** – Καταγράφει πληροφοριακά μηνύματα, συμπεριλαμβανομένων μηνυμάτων επιτυχούς ενημέρωσης, καθώς και όλες τις παραπάνω εγγραφές.
- **Προειδοποιήσεις** – Καταγράφει κρίσιμα σφάλματα και προειδοποιητικά μηνύματα.
- **Σφάλματα** – Καταγράφονται σφάλματα όπως «Σφάλμα κατά τη λήψη του αρχείου» και κρίσιμα σφάλματα.
- **Κρίσιμες προειδοποιήσεις** – Καταγράφει μόνο κρίσιμα σφάλματα (σφάλμα κατά την έναρξη της προστασίας Antivirus, Firewallκ.λπ...).

> Όλες οι αποκλεισμένες συνδέσεις θα καταγράφονται όταν επιλέγετε το επίπεδο λεπτομερειών "Διαγνωστικοί έλεγχοι".

Οι καταχωρίσεις καταγραφής που είναι παλαιότερες από τον καθορισμένο αριθμό ημερών στο πεδίο **Αυτόματη διαγραφή εγγραφών παλιότερων από (ημέρες)** θα διαγράφονται αυτόματα.

Αυτόματη βελτιστοποίηση εγγραφών – Αν επιλεχτεί, τα αρχεία καταγραφής θα ανασυγκροτούνται αυτόματα αν το ποσοστό είναι υψηλότερο από την τιμή που καθορίζεται στο πεδίο **Εάν ο αριθμός των μη χρησιμοποιούμενων εγγραφών υπερβαίνει (%)**.

Κάντε κλικ στο στοιχείο **Βελτιστοποίηση** για να αρχίσει η ανασυγκρότηση των αρχείων καταγραφής. Όλες οι κενές καταχωρίσεις καταγραφής αφαιρούνται κατά τη διάρκεια αυτής της διεργασίας, η οποία βελτιώνει την απόδοση και την ταχύτητα επεξεργασίας των καταγραφών. Η βελτίωση αυτή παρατηρείται ειδικά αν τα αρχεία καταγραφής περιέχουν μεγάλο αριθμό καταχωρίσεων.

Η επιλογή **Ενεργοποίηση πρωτοκόλλου κειμένου** επιτρέπει την αποθήκευση καταγραφών σε άλλη μορφή αρχείου ξεχωριστά από τα Αρχεία καταγραφής:

- **Κατάλογος προορισμού** – Ο κατάλογος στον οποίο θα αποθηκεύονται αρχεία καταγραφής (ισχύει μόνο για αρχεία κειμένου/CSV). Κάθε ενότητα καταγραφής θα έχει το δικό της αρχείο με προκαθορισμένο όνομα (για παράδειγμα, virlog.txt για την ενότητα **Ανιχνεύσεις** των αρχείων καταγραφής, εάν χρησιμοποιείτε μορφή απλού κειμένου για την αποθήκευση καταγραφών).

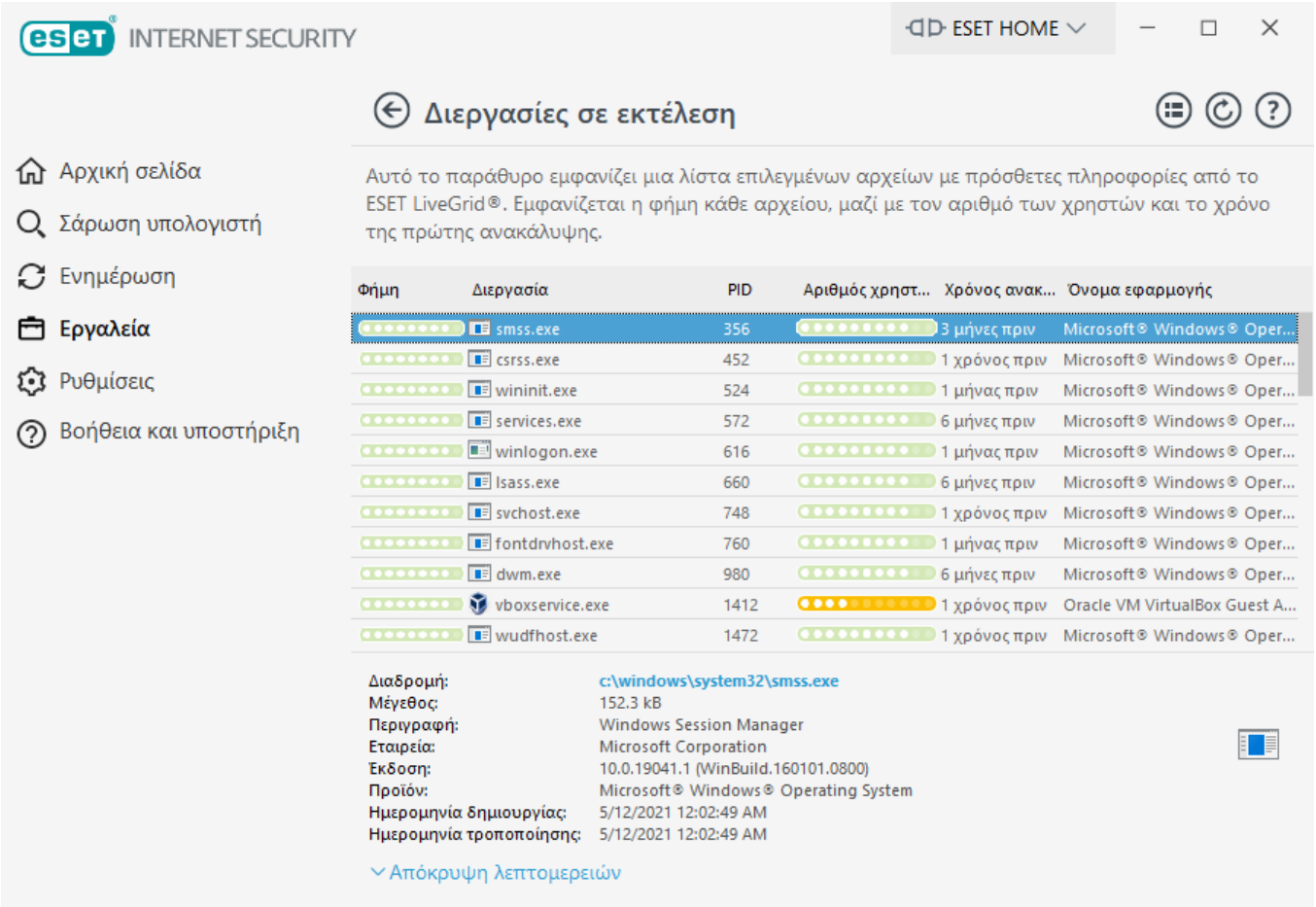
• **Τύπος** – Εάν επιλέξετε τη μορφή αρχείου **Κείμενο**, οι καταγραφές θα αποθηκεύονται σε αρχείο κειμένου, ενώ τα δεδομένα θα διαχωρίζονται μεταξύ τους με στηλοθέτες (χαρακτήρες tab). Το ίδιο ισχύει για τη μορφή αρχείων **CSV** (αρχείο τιμών διαχωρισμένων με κόμματα). Εάν επιλέξετε **Συμβάν**, οι καταγραφές θα αποθηκεύονται στην Καταγραφή συμβάντων των Windows (μπορείτε να την προβάλετε χρησιμοποιώντας το Πρόγραμμα προβολής συμβάντων στον Πίνακα Ελέγχου) και όχι σε αρχείο.

• **Διαγραφή όλων των αρχείων καταγραφής** – Διαγράφει όλα τα αποθηκευμένα αρχεία καταγραφής που είναι επιλεγμένα στο αναπτυσσόμενο μενού **Τύπος**. Θα εμφανιστεί ειδοποίηση σχετικά με την επιτυχή διαγραφή των αρχείων καταγραφής.

Για την ταχύτερη επίλυση ζητημάτων, η ESET μπορεί να σας ζητήσει να παράσχετε αρχεία καταγραφής από τον υπολογιστή σας. Η ESET Log Collector σάς διευκολύνει να συλλέξετε τις απαραίτητες πληροφορίες. Για περισσότερες πληροφορίες σχετικά με το ESET Log Collector, επισκεφτείτε το σχετικό άρθρο της Γνωσιακής βάσης της ESET.

Εκτελούμενες διεργασίες

Οι εκτελούμενες διεργασίες εμφανίζουν τα προγράμματα ή διεργασίες που εκτελούνται στον υπολογιστή σας και ενημερώνουν αμέσως και διαρκώς την ESET σχετικά με νέες εισβολές. Το ESET Internet Security παρέχει λεπτομερείς πληροφορίες για τις διεργασίες σε εκτέλεση για να προστατεύει τους χρήστες με την τεχνολογία ESET LiveGrid®.



Φήμη – Στις περισσότερες περιπτώσεις, το ESET Internet Security και η τεχνολογία ESET LiveGrid® αντιστοιχίζουν επίπεδα κινδύνου σε αντικείμενα (αρχεία, διεργασίες, κλειδιά μητρώου, κ.λπ.)

χρησιμοποιώντας μια σειρά ευριστικών κανόνων που εξετάζουν τα χαρακτηριστικά κάθε αντικειμένου και στη συνέχεια ζυγίζουν την πιθανότητα κακόβουλης δραστηριότητας. Με βάση αυτούς τους ευριστικούς ελέγχους, τα αντικείμενα αντιστοιχίζονται σε ένα επίπεδο κινδύνου από 1 – Αβλαβές (πράσινο) έως 9 – Επικίνδυνο (κόκκινο).

Διεργασία – Το όνομα της εικόνας του προγράμματος ή της διεργασίας που εκτελείται αυτήν τη στιγμή στον υπολογιστή σας. Μπορείτε επίσης να χρησιμοποιήσετε τη Διαχείριση εργασιών των Windows για να δείτε όλες τις διεργασίες που εκτελούνται στον υπολογιστή σας. Για να ανοίξετε τη διαχείριση εργασιών, κάντε δεξί κλικ σε μια κενή περιοχή στη γραμμή εργασιών και στη συνέχεια κάντε κλικ στην επιλογή **Διαχείριση εργασιών** ή πατήστε **Ctrl**+**Shift**+**Esc** στο πληκτρολόγιό σας.

> Οι γνωστές εφαρμογές που επισημαίνονται ως Αβλαβής (πράσινο) είναι σίγουρα καθαρές (λίστα μη αποκλεισμένων) και θα εξαιρούνται από τη σάρωση για βελτίωση των επιδόσεων.

PID – Ο αναγνωριστικός αριθμός διεργασίας μπορεί να χρησιμοποιηθεί ως παράμετρος σε διάφορες κλήσεις λειτουργιών, όπως η προσαρμογή της προτεραιότητας της διεργασίας.

Αριθμός χρηστών – Ο αριθμός χρηστών που χρησιμοποιούν μια συγκεκριμένη εφαρμογή. Αυτές οι πληροφορίες συλλέγονται από την τεχνολογία ESET LiveGrid®.

Χρόνος ανακάλυψης – Το χρονικό διάστημα από την ανακάλυψη της εφαρμογής από την τεχνολογία ESET LiveGrid®.

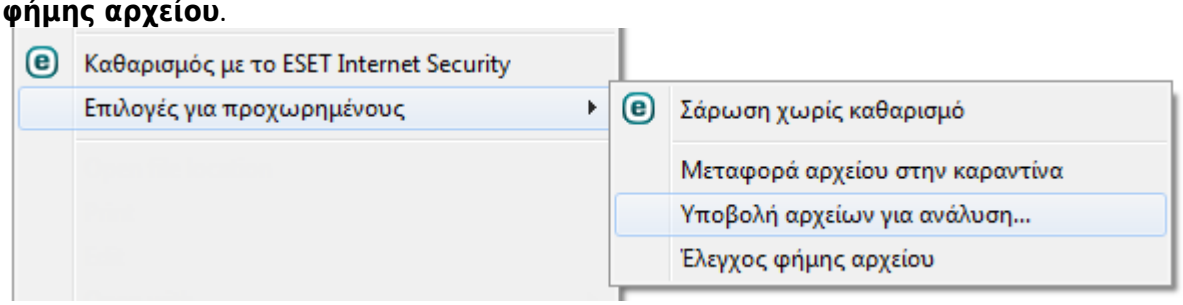
> Μια εφαρμογή που επισημαίνεται ως Άγνωστη (πορτοκαλί) δεν είναι απαραίτητα κακόβουλο λογισμικό. Συνήθως, είναι απλώς μια νεότερη εφαρμογή. Αν δεν είστε βέβαιοι για το αρχείο, μπορείτε να υποβάλλετε το αρχείο για ανάλυση στο Εργαστήριο ιών της ESET. Αν αποδειχτεί ότι το αρχείο είναι κακόβουλη εφαρμογή, η ανίχνευσή του θα προστεθεί σε μια μελλοντική ενημέρωση.

Όνομα εφαρμογής – Το συγκεκριμένο όνομα ενός προγράμματος ή μιας διεργασίας.

Κάντε κλικ σε μια εφαρμογή για να εμφανιστούν οι ακόλουθες λεπτομέρειες της συγκεκριμένης εφαρμογής:

- **Διαδρομή** – Η θέση μιας εφαρμογής στον υπολογιστή σας.
- **Μέγεθος** – Το μέγεθος αρχείου σε kB (kilobyte) ή MB (megabyte).
- **Περιγραφή** – Τα χαρακτηριστικά του αρχείου με βάση την περιγραφή από το λειτουργικό σύστημα.
- **Εταιρεία** – Το όνομα του προμηθευτή ή της εφαρμογής.
- **Έκδοση** – Πληροφορίες από τον εκδότη της εφαρμογής.
- **Προϊόν** – Το όνομα της εφαρμογής ή/και το όνομα της επιχείρησης.
- **Δημιουργήθηκε/Τροποποιήθηκε** – Η ημερομηνία και η ώρα της δημιουργίας (τροποποίησης).

Επίσης, μπορείτε να ελέγξετε τη φήμη των αρχείων που δεν ενεργούν ως εκτελούμενα προγράμματα/εκτελούμενες διεργασίες. Για να το κάνετε αυτό, κάντε δεξί κλικ σε αυτά σε ένα πρόγραμμα εξερεύνησης αρχείων και επιλέξτε **Επιλογές για προχωρημένους** > **Έλεγχος φήμης αρχείου**.



Αναφορά ασφαλείας

Αυτή η λειτουργία παρέχει μια επισκόπηση των στατιστικών στοιχείων για τις ακόλουθες κατηγορίες:

• **Αποκλεισμένες ιστοσελίδες** – Εμφανίζει τον αριθμό αποκλεισμένων ιστοσελίδων (διευθύνσεις URL στη λίστα αποκλεισμένων διευθύνσεων για PUA, phishing, παραβιασμένο δρομολογητή, διεύθυνση IP ή πιστοποιητικό).

• **Μολυσμένα αντικείμενα email που ανιχνεύτηκαν** – Εμφανίζει τον αριθμό μολυσμένων αντικειμένων email που ανιχνεύτηκαν.

• **Ιστοσελίδες στον Γονικό έλεγχο που αποκλείστηκαν** – Εμφανίζει τον αριθμό αποκλεισμένων ιστοσελίδων στον Γονικό έλεγχο.

• **PUA που ανιχνεύτηκαν** – Εμφανίζει τον αριθμό Ενδεχομένως ανεπιθύμητων εφαρμογών (PUA).

• **Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου που ανιχνεύτηκαν** – Εμφανίζει τον αριθμό ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου που ανιχνεύτηκαν.

• **Πρόσβαση σε κάμερα διαδικτύου που αποκλείστηκε** – Εμφανίζει τον αριθμό προσπαθειών πρόσβασης σε κάμερα διαδικτύου που αποκλείστηκαν.

• **Συνδέσεις σε τραπεζικές συναλλαγές μέσω Internet που προστατεύτηκαν** – Εμφανίζει τον αριθμό προστατευμένων προσπαθειών πρόσβασης σε ιστότοπους μέσω της δυνατότητας Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών.

• **Έγγραφα που ελέγχθηκαν** – Εμφανίζει τον αριθμό σαρωμένων αντικειμένων εγγράφων.

• **Εφαρμογές που σαρώθηκαν** – Εμφανίζει τον αριθμό σαρωμένων εκτελέσιμων αντικειμένων.

• **Άλλα αντικείμενα που ελέγχθηκαν** – Εμφανίζει τον αριθμό άλλων σαρωμένων αντικειμένων.

• **Αντικείμενα ιστοσελίδων που σαρώθηκαν** – Εμφανίζει τον αριθμό σαρωμένων αντικειμένων ιστοσελίδων.

• **Αντικείμενα μηνυμάτων ηλεκτρονικού ταχυδρομείου που σαρώθηκαν** – Εμφανίζει τον αριθμό σαρωμένων αντικειμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

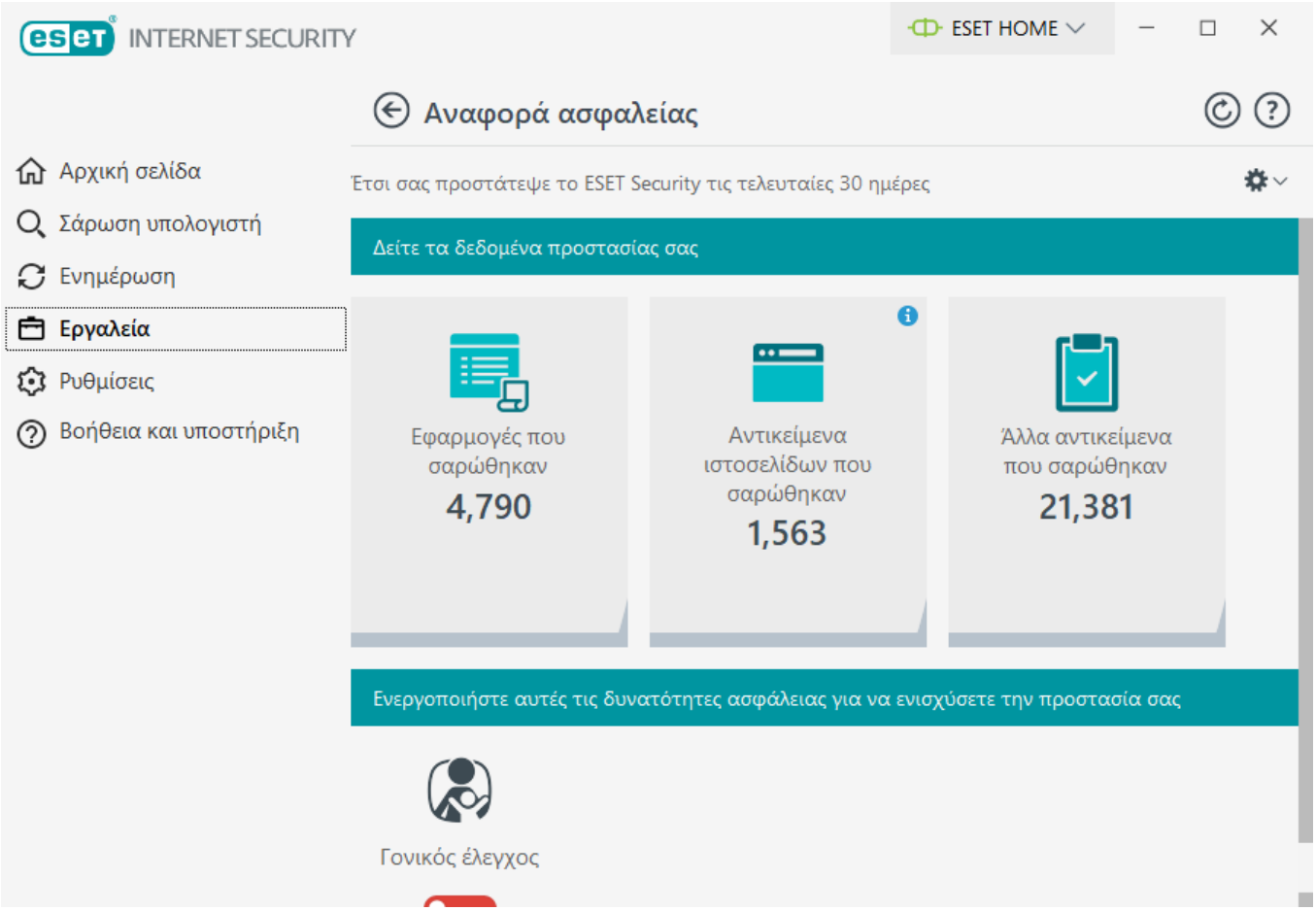
Η σειρά αυτών των κατηγοριών βασίζεται στην αριθμητική τιμή από την υψηλότερη στη χαμηλότερη. Οι κατηγορίες με μηδενική τιμή δεν εμφανίζονται. Κάντε κλικ στο στοιχείο «**Εμφάνιση περισσότερων**» για να αναπτύξετε και να εμφανίσετε κρυφές κατηγορίες.

Το τελευταίο μέρος της αναφοράς ασφαλείας προσφέρει τη δυνατότητα να ενεργοποιήσετε τις ακόλουθες λειτουργίες:

- Γονικός έλεγχος
- Anti-Theft

Εάν ενεργοποιηθεί η δυνατότητα, δεν εμφανίζεται πλέον ως μη λειτουργική στην αναφορά ασφαλείας.

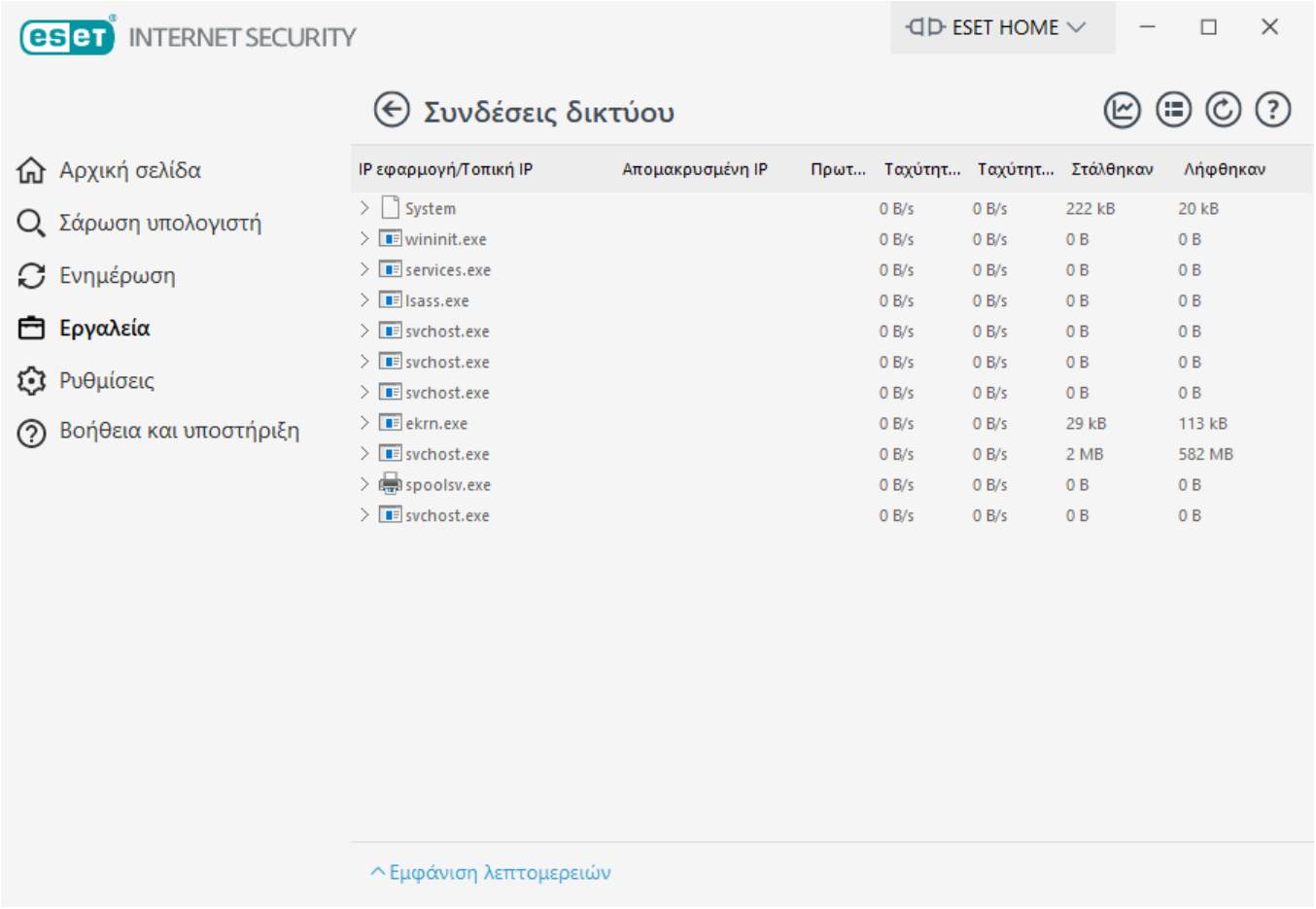
Κάντε κλικ στο γρανάζι στην επάνω δεξιά γωνία για **Ενεργοποίηση/Απενεργοποίηση ειδοποιήσεων αναφοράς ασφαλείας** ή επιλέξτε εάν τα δεδομένα θα εμφανίζονται για τις τελευταίες 30 ημέρες ή από την ενεργοποίηση του προϊόντος. Εάν το ESET Internet Security εγκαταστάθηκε πριν από λιγότερες από 30 ημέρες, τότε μπορεί να επιλεγεί μόνο ο αριθμός ημερών από την εγκατάσταση. Η περίοδος 30 ημερών ρυθμίζεται από προεπιλογή.



Η **Επαναφορά δεδομένων** εκκαθαρίζει όλα τα στατιστικά στοιχεία και καταργεί τα υπάρχοντα δεδομένα για την αναφορά ασφαλείας. Αυτή η ενέργεια πρέπει να επιβεβαιωθεί, εκτός από την περίπτωση που έχετε καταργήσει την επιλογή **Ερώτηση πριν από την επαναφορά των στατιστικών** στη διαδρομή **Ρυθμίσεις για προχωρημένους** > **Ειδοποιήσεις** > **Αλληλεπιδραστικοί συναγερμοί** > **Μηνύματα επιβεβαίωσης** > **Επεξεργασία**.

Συνδέσεις δικτύου

Στην ενότητα Συνδέσεων δικτύου, μπορείτε να δείτε μια λίστα με συνδέσεις που είναι ενεργές και εκκρεμούν. Αυτό σάς βοηθά να ελέγχετε όλες τις εφαρμογές που δημιουργούν εξερχόμενες συνδέσεις.



Κάντε κλικ στο εικονίδιο γραφήματος για να ανοίξετε τη Δραστηριότητα δικτύου.

Η πρώτη γραμμή εμφανίζει το όνομα της εφαρμογής και την ταχύτητα μεταφοράς δεδομένων της. Για να δείτε τη λίστα συνδέσεων που πραγματοποιήθηκαν από την εφαρμογή (καθώς και πιο λεπτομερείς πληροφορίες), κάντε κλικ στο στοιχείο **>**.

Στήλες

IP εφαρμογή/Τοπική IP – Όνομα της εφαρμογής, τοπικές διευθύνσεις IP και θύρες επικοινωνίας.

Απομακρυσμένη IP – Διεύθυνση IP και αριθμός θύρας του συγκεκριμένου απομακρυσμένου υπολογιστή.

Πρωτόκολλο – Πρωτόκολλο μεταφοράς που χρησιμοποιείται.

Ταχύτητα αποστολής/Ταχύτητα λήψης – Η τρέχουσα ταχύτητα εξερχόμενων και εισερχόμενων δεδομένων.

Σταλθηκάν/Λήφθηκαν – Όγκος δεδομένων που ανταλλάχτηκαν στο πλαίσιο της σύνδεσης.

Εμφάνιση λεπτομερειών – Κάντε αυτή την επιλογή για να εμφανιστούν λεπτομερείς πληροφορίες για την επιλεγμένη σύνδεση.

Κάντε δεξί κλικ σε μια σύνδεση για να δείτε πρόσθετες επιλογές που περιλαμβάνουν:

Επίλυση ονομάτων κεντρικού υπολογιστή – Εάν είναι δυνατόν, εμφανίζονται όλες οι διευθύνσεις δικτύου σε μορφή DNS και όχι σε μορφή αριθμητικής διεύθυνσης IP.

Να εμφανίζονται μόνο συνδέσεις TCP – Η λίστα εμφανίζει μόνο συνδέσεις που ανήκουν στη σουίτα πρωτοκόλλων TCP.

Εμφάνιση ελεγχόμενων συνδέσεων – Επιλέξτε αυτό το στοιχείο για να εμφανίζονται μόνο συνδέσεις στις οποίες δεν έχει δημιουργηθεί επικοινωνία αυτήν τη στιγμή, αλλά για τις οποίες το σύστημα έχει ανοίξει μια θύρα και αναμένει σύνδεση.

Εμφάνιση συνδέσεων μέσα στον υπολογιστή – Επιλέξτε αυτό το στοιχείο για να εμφανίζονται μόνο συνδέσεις των οποίων η απομακρυσμένη πλευρά είναι ένα τοπικό σύστημα – ονομάζονται επίσης συνδέσεις localhost.

Ταχύτητα ανανέωσης – Επιλέξτε τη συχνότητα για ανανέωση των ενεργών συνδέσεων.

Άμεση ανανέωση – Επαναφορτώνει το παράθυρο **συνδέσεων δικτύου**.

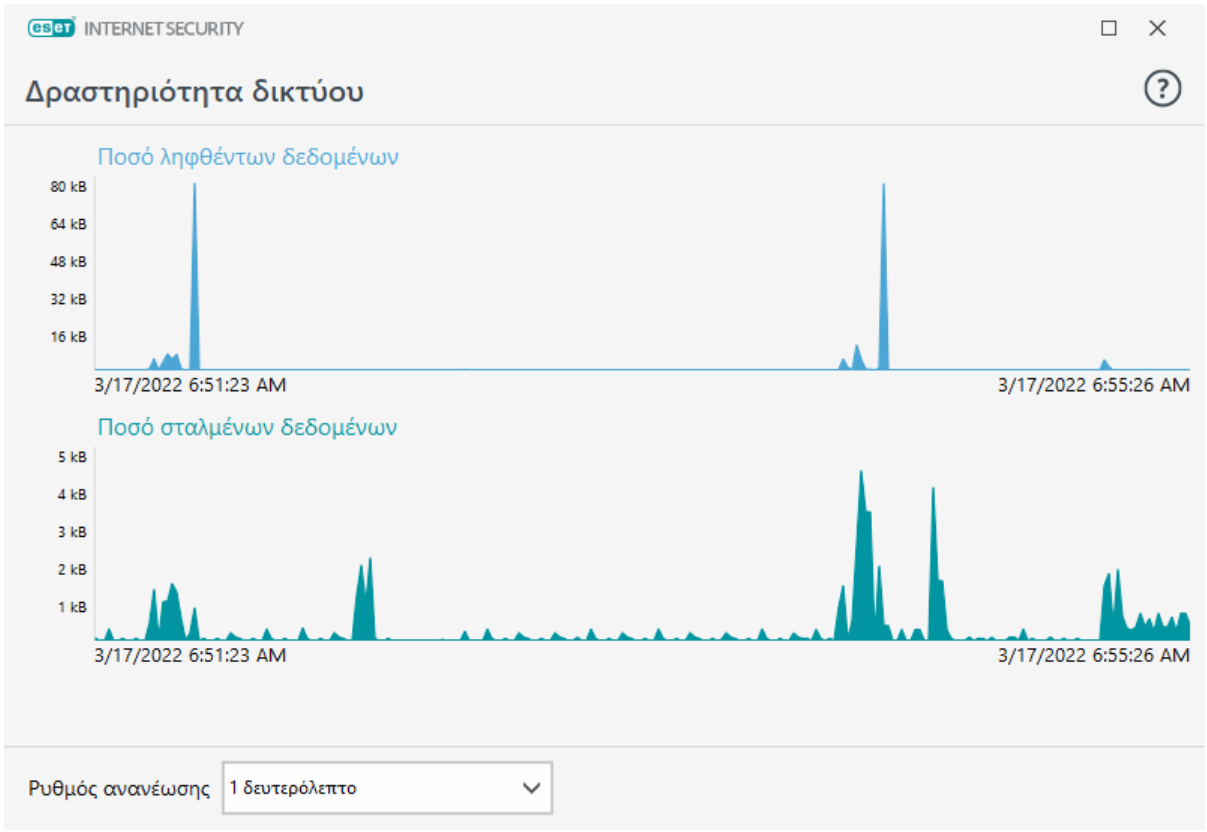
Οι παρακάτω επιλογές είναι διαθέσιμες μόνο εφόσον κάνετε κλικ σε μια εφαρμογή ή διεργασία, και όχι σε μια ενεργή σύνδεση:

Να μην επιτραπεί προσωρινά η επικοινωνία για τη διεργασία – Απορρίπτει τις τρέχουσες συνδέσεις για μια συγκεκριμένη εφαρμογή. Αν δημιουργηθεί μια νέα σύνδεση, το firewall χρησιμοποιεί έναν προκαθορισμένο κανόνα. Στην ενότητα Διαμόρφωση και χρήση κανόνων μπορείτε να βρείτε μια περιγραφή για τις ρυθμίσεις.

Να επιτραπεί προσωρινά η επικοινωνία για τη διεργασία – Επιτρέπει τις τρέχουσες συνδέσεις για μια συγκεκριμένη εφαρμογή. Αν δημιουργηθεί μια νέα σύνδεση, το firewall χρησιμοποιεί έναν προκαθορισμένο κανόνα. Στην ενότητα Διαμόρφωση και χρήση κανόνων μπορείτε να βρείτε μια περιγραφή για τις ρυθμίσεις.

Δραστηριότητα δικτύου

Για να δείτε την τρέχουσα **Δραστηριότητα δικτύου** σε μορφή γραφήματος, κάντε κλικ στα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Συνδέσεις δικτύου** και κάντε κλικ στο εικονίδιο γραφήματος . Στο κάτω μέρος του γραφήματος υπάρχει μια λωρίδα χρόνου που καταγράφει τη δραστηριότητα του δικτύου σε πραγματικό χρόνο με βάση το επιλεγμένο χρονικό διάστημα. Για να αλλάξετε το χρονικό διάστημα, επιλέξτε την κατάλληλη τιμή από το αναπτυσσόμενο μενού **Ρυθμός ανανέωσης**.



Οι διαθέσιμες επιλογές είναι οι παρακάτω:

- **1 δευτερόλεπτο** – Το γράφημα ανανεώνεται κάθε δευτερόλεπτο και η λωρίδα χρόνου καλύπτει τα τελευταία 4 λεπτά.
- **1 λεπτό (τελευταίες 24 ώρες)** – Το γράφημα ανανεώνεται κάθε λεπτό και η λωρίδα χρόνου καλύπτει τις τελευταίες 24 ώρες.
- **1 ώρα (τελευταίος μήνας)** – Το γράφημα ανανεώνεται κάθε ώρα και η λωρίδα χρόνου καλύπτει τον τελευταίο μήνα.

Ο κατακόρυφος άξονας του γραφήματος αντιπροσωπεύει τον όγκο των δεδομένων που λαμβάνονται ή αποστέλλονται. Τοποθετήστε το ποντίκι σας πάνω από το γράφημα για να δείτε τον ακριβή όγκο των δεδομένων που λάβατε/αποστείλατε σε μια συγκεκριμένη στιγμή.

ESET SysInspector

Το ESET SysInspector είναι μια εφαρμογή που ελέγχει σε βάθος τον υπολογιστή σας και συλλέγει λεπτομερείς πληροφορίες για στοιχεία του συστήματος, όπως προγράμματα οδήγησης και εφαρμογές, συνδέσεις δικτύου ή σημαντικές εγγραφές μητρώου και αξιολογεί το επίπεδο κινδύνου του κάθε στοιχείου. Οι πληροφορίες αυτές βοηθούν να προσδιοριστεί η αιτία ύποπτης συμπεριφοράς του συστήματος που μπορεί να οφείλεται σε ασυμβατότητα του λογισμικού ή του υλικού ή μόλυνση από κακόβουλο λογισμικό. Για να μάθετε πώς να χρησιμοποιείτε το ESET SysInspector, ανατρέξτε στην Ηλεκτρονική βοήθεια του ESET SysInspector.

Το παράθυρο του ESET SysInspector εμφανίζει τις ακόλουθες πληροφορίες σχετικά με τα αρχεία καταγραφής:

- **Ώρα** – Η ώρα δημιουργίας του αρχείου καταγραφής.

- **Σχόλιο** – Ένα σύντομο σχόλιο.
- **Χρήστης** – Το όνομα του χρήστη που δημιούργησε το αρχείο καταγραφής.
- **Κατάσταση** – Η κατάσταση της δημιουργίας του αρχείου καταγραφής.

Είναι διαθέσιμες οι παρακάτω ενέργειες:

- **Εμφάνιση** – Ανοίγει το επιλεγμένο αρχείο καταγραφής στο ESET SysInspector. Μπορείτε επίσης να κάνετε δεξί κλικ σε ένα αρχείο καταγραφής και να επιλέξετε **Εμφάνιση** από το μενού περιβάλλοντος.
- **Σύγκριση** – Συγκρίνει δύο υπάρχοντα αρχεία καταγραφής.
- **Δημιουργία** – Δημιουργεί ένα νέο αρχείο καταγραφής. Περιμένετε μέχρι να δημιουργηθεί το ESET SysInspector (κατάσταση **Δημιουργήθηκε**) προτού επιχειρήσετε να αποκτήσετε πρόσβαση στο αρχείο καταγραφής.
- **Διαγραφή** – Αφαιρεί τα επιλεγμένα αρχεία καταγραφής από τη λίστα.

Όταν επιλέγετε ένα ή περισσότερα αρχεία καταγραφής, στο μενού περιβάλλοντος είναι διαθέσιμες οι ακόλουθες επιλογές:

- **Εμφάνιση** – Ανοίγει το επιλεγμένο αρχείο καταγραφής στο ESET SysInspector (ίδια λειτουργία όπως κάνοντας διπλό κλικ σε ένα αρχείο καταγραφής).
- **Σύγκριση** – Συγκρίνει δύο υπάρχοντα αρχεία καταγραφής.
- **Δημιουργία** – Δημιουργεί ένα νέο αρχείο καταγραφής. Περιμένετε μέχρι να δημιουργηθεί το ESET SysInspector (κατάσταση **Δημιουργήθηκε**) προτού επιχειρήσετε να αποκτήσετε πρόσβαση στο αρχείο καταγραφής.
- **Διαγραφή** – Αφαιρεί τα επιλεγμένα αρχεία καταγραφής από τη λίστα.
- **Διαγραφή όλων** – Διαγράφει όλα τα αρχεία καταγραφής.
- **Εξαγωγή** – Κάνει εξαγωγή του αρχείου καταγραφής σε ένα αρχείο .xml ή συμπιεσμένο αρχείο .xml. Το αρχείο καταγραφής εξάγεται στο C:\ProgramData\ESET\ESET Security\SysInspector.

Χρονοδιάγραμμα εργασιών

Το Χρονοδιάγραμμα εργασιών διαχειρίζεται και εκκινεί προγραμματισμένες εργασίες με προκαθορισμένη διαμόρφωση και ιδιότητες.

Η πρόσβαση στον Προγραμματισμό εργασιών είναι δυνατή από το κύριο παράθυρο του ESET Internet Security κάνοντας κλικ στα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Προγραμματισμός εργασιών**. Το **Χρονοδιάγραμμα εργασιών** περιέχει μια λίστα με όλες τις προγραμματισμένες εργασίες και τις ιδιότητες διαμόρφωσης όπως η προκαθορισμένη ημερομηνία, η ώρα και το προφίλ σάρωσης που χρησιμοποιείται.

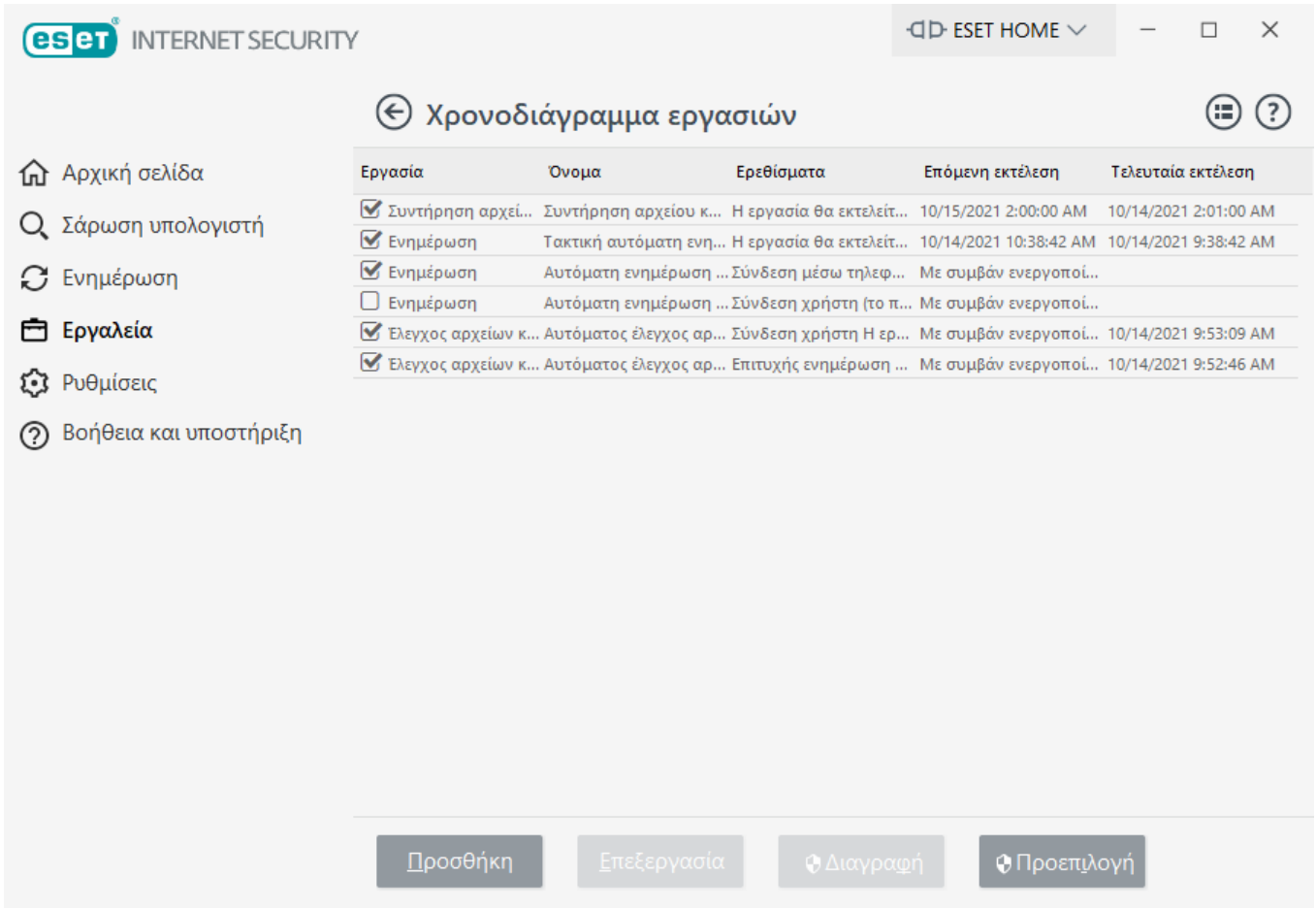
Το Χρονοδιάγραμμα εξυπηρετεί στον προγραμματισμό των ακόλουθων εργασιών: ενημέρωση μονάδων, εργασία σάρωσης, έλεγχος αρχείου εκκίνησης συστήματος και συντήρηση αρχείου

καταγραφής. Μπορείτε να προσθέσετε ή να διαγράψετε εργασίες απευθείας από το κύριο παράθυρο του Χρονοδιαγράμματος (κάντε κλικ στο στοιχείο **Προσθήκη εργασίας** ή **Διαγραφή** στο κάτω μέρος). Μπορείτε να επαναφέρετε τη λίστα προγραμματισμένων εργασιών στην προεπιλογή και να διαγράψετε όλες τις αλλαγές κάνοντας κλικ στο στοιχείο **Προεπιλογή**. Κάντε δεξί κλικ οπουδήποτε στο παράθυρο του Χρονοδιαγράμματος εργασιών για να εκτελέσετε τις ακόλουθες ενέργειες: εμφάνιση λεπτομερών πληροφοριών, εκτέλεση της εργασίας άμεσα, προσθήκη νέας εργασίας και διαγραφή υπάρχουσας εργασίας. Χρησιμοποιήστε τα πλαίσια ελέγχου στην αρχή κάθε καταχώρισης για να ενεργοποιήσετε/απενεργοποιήσετε τις εργασίες.

Από προεπιλογή, στο **Χρονοδιάγραμμα εργασιών** εμφανίζονται οι ακόλουθες προγραμματισμένες εργασίες:

- **Συντήρηση αρχείου καταγραφής**
- **Τακτική αυτόματη ενημέρωση**
- **Αυτόματη ενημέρωση μετά τη σύνδεση μέσω τηλεφώνου**
- **Αυτόματη ενημέρωση μετά τη σύνδεση χρήστη**
- **Αυτόματος έλεγχος αρχείων κατά την εκκίνηση** (μετά από σύνδεση του χρήστη)
- **Αυτόματος έλεγχος αρχείων κατά την εκκίνηση** (μετά από επιτυχημένη ενημέρωση του μηχανισμού ανίχνευσης)

Για να επεξεργαστείτε τη διαμόρφωση μιας υπάρχουσας προγραμματισμένης εργασίας (προεπιλεγμένης και καθορισμένης από τον χρήστη), κάντε δεξί κλικ στην εργασία και κλικ στο στοιχείο **Επεξεργασία** ή επιλέξτε την εργασία που θέλετε να τροποποιήσετε και κάντε κλικ στο στοιχείο **Επεξεργασία**.



Προσθήκη νέας εργασίας

1. Κάντε κλικ στο στοιχείο **Προσθήκη εργασίας** στο κάτω μέρος του παραθύρου.

2. Πληκτρολογήστε ένα όνομα για την εργασία.

3. Επιλέξτε την εργασία που θέλετε από το αναπτυσσόμενο μενού:

• **Εκτέλεση εξωτερικής εφαρμογής** – Προγραμματίζει την εκτέλεση μιας εξωτερικής εφαρμογής.

• **Συντήρηση αρχείου καταγραφής** - Τα αρχεία καταγραφής περιέχουν επίσης υπολείμματα από διαγραμμένες εγγραφές. Αυτή η εργασία βελτιστοποιεί σε τακτική βάση τις εγγραφές στα αρχεία καταγραφής, ώστε να λειτουργούν πιο αποτελεσματικά.

• **Έλεγχος αρχείων κατά την εκκίνηση του συστήματος** – Ελέγχει τα αρχεία που επιτρέπεται να εκτελούνται κατά την εκκίνηση του συστήματος ή τη σύνδεση του χρήστη.

• **Δημιουργία στιγμιότυπου κατάστασης του υπολογιστή** – Δημιουργεί ένα στιγμιότυπο ESET SysInspector του υπολογιστή – συγκεντρώνει λεπτομερείς πληροφορίες σχετικά με στοιχεία του συστήματος (π.χ. προγράμματα οδήγησης, εφαρμογές) και αξιολογεί το επίπεδο κινδύνου για κάθε στοιχείο.

• **Σάρωση υπολογιστή κατ' απαίτηση** – Πραγματοποιεί σάρωση αρχείων και φακέλων στον υπολογιστή σας.

• **Ενημέρωση** – Προγραμματίζει μια εργασία ενημέρωσης εκτελώντας ενημέρωση στις

μονάδες.

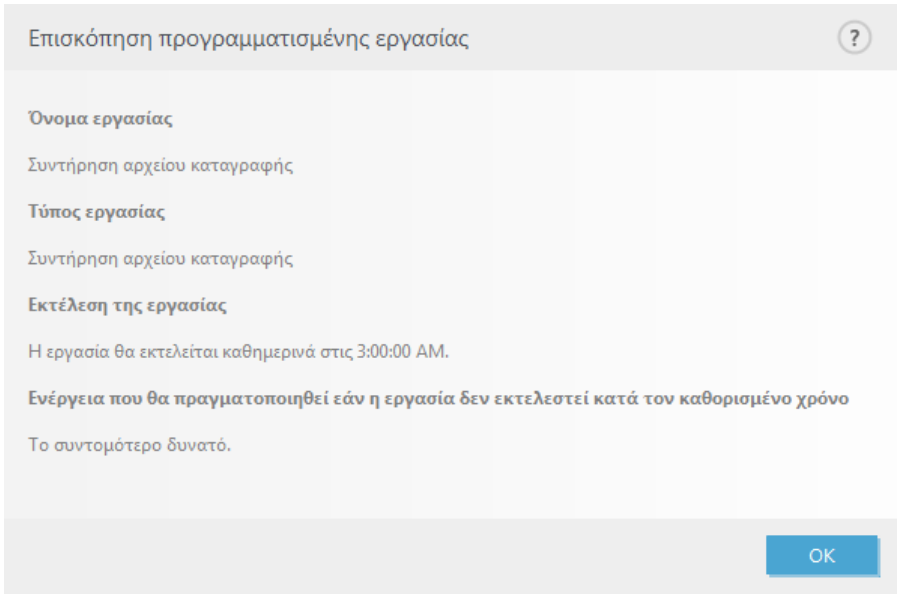
4. Κάντε κλικ στο ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Ενεργό** για να ενεργοποιήσετε την εργασία (μπορείτε να το κάνετε αργότερα επιλέγοντας/καταργώντας την επιλογή του αντίστοιχου πλαισίου ελέγχου στη λίστα προγραμματισμένων εργασιών), κάντε κλικ στο στοιχείο **Επόμενο** και καθορίστε μία από τις επιλογές χρόνου:

- **Μία φορά** – Η εργασία θα εκτελεστεί κατά την προκαθορισμένη ημερομηνία και ώρα.
- **Επανειλημμένα** – Η εργασία θα εκτελείται στο καθορισμένο χρονικό διάστημα.
- **Καθημερινά** – Η εργασία θα εκτελείται επανειλημμένα κάθε μέρα στην προκαθορισμένη ώρα.
- **Εβδομαδιαία** – Η εργασία θα εκτελείται κατά την επιλεγμένη ημέρα και ώρα.
- **Ενεργοποίηση συμβάντος** – Η εργασία θα εκτελείται μετά από ένα καθορισμένο συμβάν.

5. Επιλέξτε **Παράλειψη της εργασίας κατά τη λειτουργία με μπαταρία**, για να ελαχιστοποιήσετε την κατανάλωση πόρων συστήματος όταν χρησιμοποιείτε φορητό υπολογιστή που τροφοδοτείται με μπαταρία. Η εργασία θα εκτελείται την ημέρα και ώρα που καθορίζεται στα πεδία **Εκτέλεση εργασίας**. Αν δεν ήταν δυνατόν να εκτελεστεί η εργασία κατά την προκαθορισμένη ώρα, μπορείτε να καθορίσετε πότε θα εκτελείται ξανά:

- **Την επόμενη προγραμματισμένη φορά**
- **Το συντομότερο δυνατό**
- **Αμέσως, εάν ο χρόνος από την τελευταία εκτέλεση υπερβαίνει τις (ώρες)** – Αντιπροσωπεύει το χρονικό διάστημα που έχει παρέλθει από την πρώτη εκτέλεση της εργασίας που παραλείφθηκε. Σε περίπτωση υπέρβασης αυτού του χρόνου, η εργασία θα εκτελεστεί αμέσως. Ρυθμίστε την ώρα χρησιμοποιώντας το παρακάτω κουμπί αυξομείωσης.

Για να προβάλετε τις λεπτομέρειες μιας προγραμματισμένης εργασίας, κάντε δεξί κλικ επάνω της και επιλέξτε **Εμφάνιση λεπτομερειών εργασίας**.



Επιλογές προγραμματισμένων σαρώσεων

Σε αυτό το παράθυρο μπορείτε να καθορίσετε προηγμένες επιλογές για μια προγραμματισμένη εργασία σάρωσης υπολογιστή.

Για να εκτελέσετε μια σάρωση χωρίς καμία ενέργεια καθαρισμού, κάντε κλικ στο στοιχείο **Ρυθμίσεις για προχωρημένους** και επιλέξτε **Σάρωση χωρίς καθαρισμό**. Το ιστορικό σάρωσης αποθηκεύεται στο αρχείο καταγραφής σάρωσης.

Όταν είναι επιλεγμένο το στοιχείο **Παράβλεψη εξαιρέσεων**, τα αρχεία με επεκτάσεις που προηγουμένως εξαιρούνταν από τη σάρωση θα σαρώνονται χωρίς εξαίρεση.

Εάν χρησιμοποιήσετε το αναπτυσσόμενο μενού, μπορείτε να ρυθμίσετε μια ενέργεια που θα πραγματοποιείται αυτόματα μετά την ολοκλήρωση μιας σάρωσης:

- **Καμιά ενέργεια** – Μετά την ολοκλήρωση της σάρωσης δεν θα πραγματοποιηθεί καμιά ενέργεια.

- **Τερματισμός λειτουργίας** – Η λειτουργία του υπολογιστή τερματίζεται όταν ολοκληρωθεί η σάρωση.

- **Επανεκκίνηση** – Κλείνει όλα τα ανοιχτά προγράμματα και επανεκκινεί τον υπολογιστή όταν ολοκληρωθεί η σάρωση.

- **Επανεκκίνηση εάν απαιτείται** - Ο υπολογιστής πραγματοποιεί επανεκκίνηση μόνο εάν απαιτείται για να ολοκληρωθεί ο καθαρισμός των ανιχνευμένων απειλών.

- **Επιβολή επανεκκίνησης** - Επιβάλει το κλείσιμο όλων των ανοιχτών προγραμμάτων χωρίς να περιμένει την αλληλεπίδραση του χρήστη και επανεκκινεί τον υπολογιστή μετά την ολοκλήρωση μιας σάρωσης.

- **Επιβολή επανεκκίνησης, εάν χρειάζεται** - Ο υπολογιστής πραγματοποιεί επανεκκίνηση μόνο εάν απαιτείται για να ολοκληρωθεί ο καθαρισμός των ανιχνευμένων απειλών.

- **Αναστολή λειτουργίας** – Αποθηκεύει την περίοδο λειτουργίας σας και θέτει τον υπολογιστή σε κατάσταση χαμηλής κατανάλωσης, έτσι ώστε να μπορείτε γρήγορα να συνεχίσετε την εργασία σας.

- **Αδρανοποίηση** – Αποτυπώνει οτιδήποτε εκτελείται στη μνήμη RAM και το μετακινεί σε ένα ειδικό αρχείο στον σκληρό δίσκο. Η λειτουργία του υπολογιστή τερματίζεται, αλλά θα συνεχίσει από την προηγούμενη κατάσταση την επόμενη φορά που θα τον ξεκινήσετε.

Οι ενέργειες **Αναστολή λειτουργίας** ή **Αδρανοποίηση** είναι διαθέσιμες ανάλογα με τις ρυθμίσεις του λειτουργικού συστήματος «Ενέργεια και αναστολή λειτουργίας» ή τις δυνατότητες του υπολογιστή/φορητού υπολογιστή σας. Έχετε υπόψη ότι, ακόμη και σε κατάσταση αναστολής λειτουργίας, ο υπολογιστής εξακολουθεί να λειτουργεί. Συνεχίζει να εκτελεί βασικές λειτουργίες και να καταναλώνει ρεύμα όταν τροφοδοτείται με μπαταρία. Για να εξοικονομήσετε τη διάρκεια ζωής της μπαταρίας, για παράδειγμα όταν ταξιδεύετε μακριά από το γραφείο, συνιστάται να χρησιμοποιείτε την επιλογή «Αδρανοποίηση».

Επιλέξτε **Δεν είναι δυνατή η ακύρωση της σάρωσης** για να μην επιτρέπετε σε χρήστες με περιορισμένα δικαιώματα τη δυνατότητα να διακόπτουν ενέργειες μετά τη σάρωση.

Επιλέξτε **Μπορεί να γίνει παύση της σάρωσης από το χρήστη για (λεπτά)**, εάν θέλετε να επιτρέπετε σε χρήστες με περιορισμένα δικαιώματα να πραγματοποιούν παύση του υπολογιστή για μια καθορισμένη χρονική περίοδο.

Δείτε επίσης το θέμα Εξέλιξη σάρωσης.

Επισκόπηση προγραμματισμένης εργασίας

Αυτό το παράθυρο διαλόγου εμφανίζει λεπτομερείς πληροφορίες για την επιλεγμένη προγραμματισμένη εργασία, όταν κάνετε διπλό κλικ σε μια προσαρμοσμένη εργασία ή δεξί κλικ σε μια προσαρμοσμένη εργασία στο χρονοδιάγραμμα και επιλέξετε **Εμφάνιση λεπτομερειών εργασίας**.

Λεπτομέρειες εργασίας

Πληκτρολογήστε το **Όνομα εργασίας**, ορίστε μία επιλογή στο στοιχείο **Τύπος εργασίας** και, στη συνέχεια, κάντε κλικ στο στοιχείο **Επόμενο**:

- **Εκτέλεση εξωτερικής εφαρμογής** – Προγραμματίζει την εκτέλεση μιας εξωτερικής εφαρμογής.
- **Συντήρηση αρχείου καταγραφής** - Τα αρχεία καταγραφής περιέχουν επίσης υπολείμματα από διαγραμμένες εγγραφές. Αυτή η εργασία βελτιστοποιεί σε τακτική βάση τις εγγραφές στα αρχεία καταγραφής, ώστε να λειτουργούν πιο αποτελεσματικά.
- **Έλεγχος αρχείων κατά την εκκίνηση του συστήματος** – Ελέγχει τα αρχεία που επιτρέπεται να εκτελούνται κατά την εκκίνηση του συστήματος ή τη σύνδεση του χρήστη.
- **Δημιουργία στιγμιότυπου κατάστασης του υπολογιστή** – Δημιουργεί ένα στιγμιότυπο ESET SysInspector του υπολογιστή – συγκεντρώνει λεπτομερείς πληροφορίες σχετικά με στοιχεία του συστήματος (π.χ. προγράμματα οδήγησης, εφαρμογές) και αξιολογεί το επίπεδο κινδύνου για κάθε στοιχείο.
- **Σάρωση υπολογιστή κατ' απαίτηση** – Πραγματοποιεί σάρωση αρχείων και φακέλων στον υπολογιστή σας.
- **Ενημέρωση** – Προγραμματίζει μια εργασία ενημέρωσης εκτελώντας ενημέρωση στις μονάδες.

Χρόνος εργασίας

Η εργασία θα εκτελείται επανειλημμένα κατά το καθορισμένο χρονικό διάστημα. Επιλέξτε μία από τις επιλογές χρόνου:

- **Μία φορά** – Η εργασία θα εκτελεστεί μόνο μία φορά, κατά την προκαθορισμένη ημερομηνία και ώρα.
- **Επανειλημμένα** – Η εργασία θα εκτελείται στο καθορισμένο χρονικό διάστημα (σε ώρες).

• **Καθημερινά** – Η εργασία θα εκτελείται κάθε μέρα στην προκαθορισμένη ώρα.

• **Εβδομαδιαία** – Η εργασία θα εκτελείται μία ή περισσότερες φορές την εβδομάδα, κατά τις επιλεγμένες ημέρες και ώρες.

• **Με συμβάν ενεργοποίησης** – Η εργασία θα πραγματοποιείται ύστερα από ένα καθορισμένο συμβάν.

Παράλειψη της εργασίας κατά τη λειτουργία με μπαταρία – Εάν ο υπολογιστής σας τροφοδοτείται με μπαταρία τη στιγμή κατά την οποία είναι προγραμματισμένη η έναρξη μιας εργασίας, η εργασία δεν θα ξεκινήσει. Αυτό ισχύει επίσης για υπολογιστές που τροφοδοτούνται με UPS.

Χρόνος εργασίας - Μία φορά

Εκτέλεση εργασίας – Η καθορισμένη εργασία θα εκτελείται μόνο μία φορά κατά την προκαθορισμένη ημερομηνία και ώρα.

Χρόνος εργασίας - Καθημερινά

Η εργασία θα εκτελείται κάθε μέρα στην προκαθορισμένη ώρα.

Χρόνος εργασίας - Εβδομαδιαίως

Η εργασία θα εκτελείται επανειλημμένως κάθε εβδομάδα κατά τις επιλεγμένες ημέρες και ώρες.

Χρόνος εργασίας - Ενεργοποίηση από συμβάν

Η εργασία θα ενεργοποιηθεί από ένα από τα παρακάτω συμβάντα:

- **Κάθε φορά που ξεκινά ο υπολογιστής**
- **Την πρώτη φορά που ξεκινά ο υπολογιστής κάθε μέρα**
- **Σύνδεση μέσω τηλεφώνου στο Internet/VPN**
- **Επιτυχής ενημέρωση μονάδας**
- **Επιτυχής ενημέρωση προϊόντος**
- **Σύνδεση χρήστη**
- **Ανίχνευση απειλής**

Όταν προγραμματίζετε μια εργασία που ενεργοποιείται από συμβάν, μπορείτε να καθορίσετε το ελάχιστο διάστημα μεταξύ δύο ολοκληρώσεων της εργασίας. Για παράδειγμα, αν συνδέεστε στον

υπολογιστή σας πολλές φορές την ημέρα, επιλέξτε 24 ώρες για να εκτελείται η εργασία μόνο κατά την πρώτη σύνδεση της ημέρας και μετά την επόμενη ημέρα.

Παράλειψη εργασίας

Μια εργασία μπορεί να παραλειφθεί όταν ο υπολογιστής τροφοδοτείται με μπαταρία ή είναι σβηστός. Από τις παρακάτω επιλογές, επιλέξτε πότε θα εκτελείται μια εργασία και κάντε κλικ στο κουμπί **Επόμενο**:

• **Στην επόμενη προγραμματισμένη φορά** – Η εργασία θα εκτελεστεί εάν ο υπολογιστής είναι ενεργοποιημένος την επόμενη προγραμματισμένη ώρα.

• **Το συντομότερο δυνατό** – Η εργασία θα εκτελεστεί όταν ενεργοποιηθεί ο υπολογιστής.

• **Αμέσως, εάν ο χρόνος από την τελευταία προγραμματισμένη εκτέλεση υπερβαίνει τις (ώρες)** – Αντιπροσωπεύει το χρονικό διάστημα που έχει παρέλθει από την πρώτη εκτέλεση της εργασίας που παραλείφθηκε. Σε περίπτωση υπέρβασης αυτού του χρόνου, η εργασία θα εκτελεστεί αμέσως.

Αμέσως, εάν ο χρόνος από την τελευταία προγραμματισμένη εκτέλεση υπερβαίνει τις (ώρες) – παραδείγματα

Μια εργασία παραδείγματος έχει ρυθμιστεί να εκτελείται επανειλημμένα κάθε ώρα. Η επιλογή **Αμέσως, εάν ο χρόνος από την τελευταία προγραμματισμένη εκτέλεση υπερβαίνει τις (ώρες)** ορίζεται και ο χρόνος υπέρβασης ορίζεται σε δύο ώρες. Η εργασία εκτελείται στις 13:00 και όταν ολοκληρωθεί ο υπολογιστής μεταβαίνει σε κατάσταση αναστολής λειτουργίας:

• Ο υπολογιστής ενεργοποιείται στις 15:30. Η πρώτη εκτέλεση της εργασίας που παραλείφθηκε ήταν στις 14:00. Έχουν παρέλθει μόνο 1,5 ώρες από τις 14:00, οπότε η εργασία θα εκτελεστεί στις 16:00.

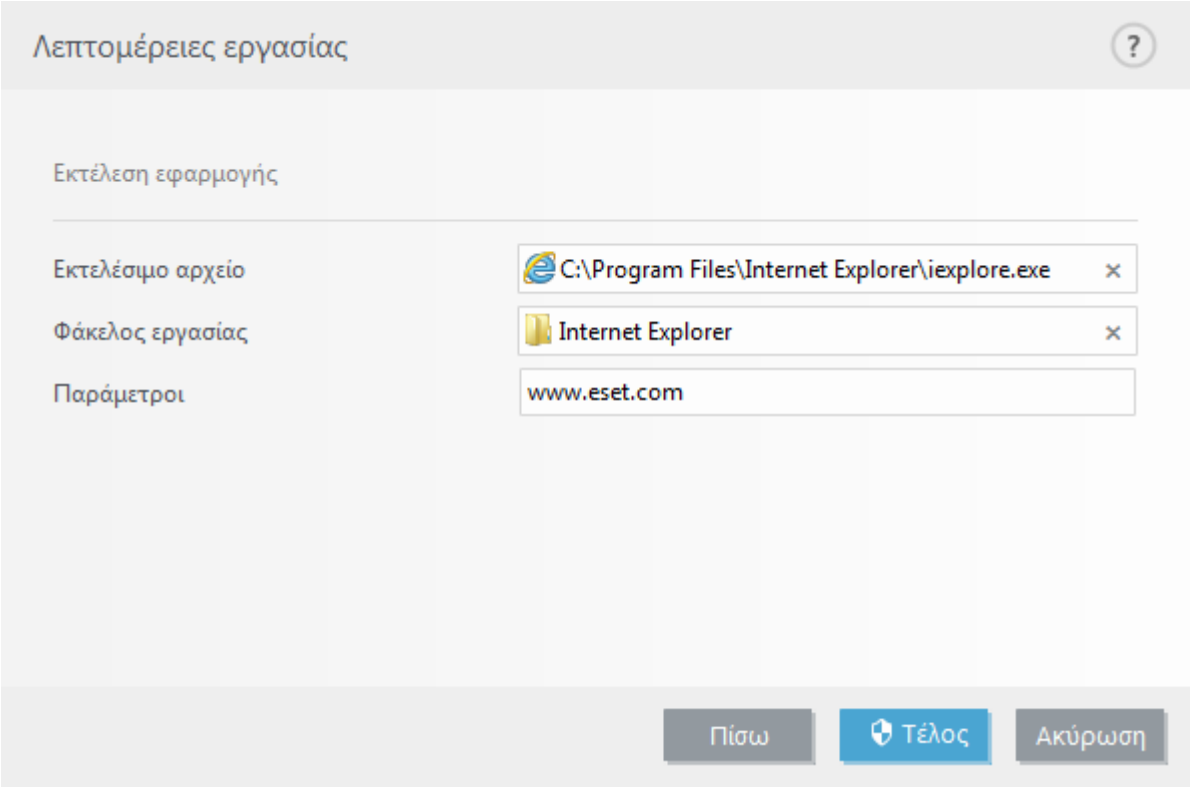
• Ο υπολογιστής ενεργοποιείται στις 16:30. Η πρώτη εκτέλεση της εργασίας που παραλείφθηκε ήταν στις 14:00. Έχουν παρέλθει δυόμιση ώρες από τις 14:00, οπότε η εργασία θα εκτελεστεί αμέσως.

Λεπτομέρειες εργασίας - Ενημέρωση

Αν θέλετε να ενημερώνετε το πρόγραμμα από δύο διακομιστές ενημέρωσης, τότε πρέπει να δημιουργήσετε δύο διαφορετικά προφίλ ενημέρωσης. Αν το πρώτο αποτύχει στη λήψη αρχείων ενημέρωσης, τότε το πρόγραμμα κάνει αυτόματα εναλλαγή στο δεύτερο. Αυτό είναι κατάλληλο για τους φορητούς υπολογιστές, για παράδειγμα, οι οποίοι ενημερώνονται κανονικά από έναν τοπικό διακομιστή ενημέρωσης LAN, αλλά οι κάτοχοί τους συχνά συνδέονται στο διαδίκτυο χρησιμοποιώντας άλλα δίκτυα. Έτσι, αν αποτύχει το πρώτο προφίλ, το δεύτερο θα κάνει αυτόματα λήψη των αρχείων ενημέρωσης από τους διακομιστές ενημέρωσης της ESET.

Λεπτομέρειες εργασίας - Εκτέλεση εφαρμογής

Αυτή η εργασία προγραμματίζει την εκτέλεση μιας εξωτερικής εφαρμογής.



Εκτελέσιμο αρχείο – Επιλέξτε ένα εκτελέσιμο αρχείο από το δέντρο καταλόγων, κάντε κλικ στην επιλογή **...** ή καταχωρίστε τη διαδρομή με μη αυτόματο τρόπο.

Φάκελος εργασίας – Καθορίστε τον κατάλογο εργασίας της εξωτερικής εφαρμογής. Όλα τα προσωρινά αρχεία του επιλεγμένου **Εκτελέσιμου αρχείου** θα δημιουργηθούν μέσα σε αυτό τον κατάλογο.

Παράμετροι – Παράμετροι γραμμής εντολών για την εφαρμογή (προαιρετικά).

Κάντε κλικ στο στοιχείο **Τέλος** για εφαρμογή της εργασίας.

Καθαρισμός συστήματος

Ο καθαρισμός συστήματος είναι ένα εργαλείο που σας βοηθά να επαναφέρετε τον υπολογιστή σας σε κατάσταση χρήσης μετά τον καθαρισμό μιας απειλής. Το κακόβουλο λογισμικό μπορεί να απενεργοποιήσει βοηθητικά προγράμματα του συστήματος, όπως τον Επεξεργαστή μητρώου, τη Διαχείριση εργασιών ή τις Ενημερώσεις των Windows. Ο καθαρισμός συστήματος επαναφέρει τις προεπιλεγμένες τιμές και ρυθμίσεις για ένα συγκεκριμένο σύστημα με ένα μόνο κλικ.

Ο καθαρισμός συστήματος αναφέρει ζητήματα από πέντε κατηγορίες ρυθμίσεων:

- **Ρυθμίσεις ασφαλείας**: αλλαγές σε ρυθμίσεις που μπορεί να προκαλέσουν αυξημένη ευπάθεια του υπολογιστή, όπως το Windows Update
- **Ρυθμίσεις συστήματος**: αλλαγές στις ρυθμίσεις συστήματος που μπορούν να αλλάξουν τη συμπεριφορά του υπολογιστή σας, όπως οι συσχετίσεις αρχείων
- **Εμφάνιση συστήματος**: ρυθμίσεις που επηρεάζουν την εμφάνιση του συστήματός σας, όπως την ταπετσαρία της επιφάνειας εργασίας σας

- **Απενεργοποιημένες δυνατότητες**: σημαντικές δυνατότητες και εφαρμογές που μπορεί να είναι απενεργοποιημένες

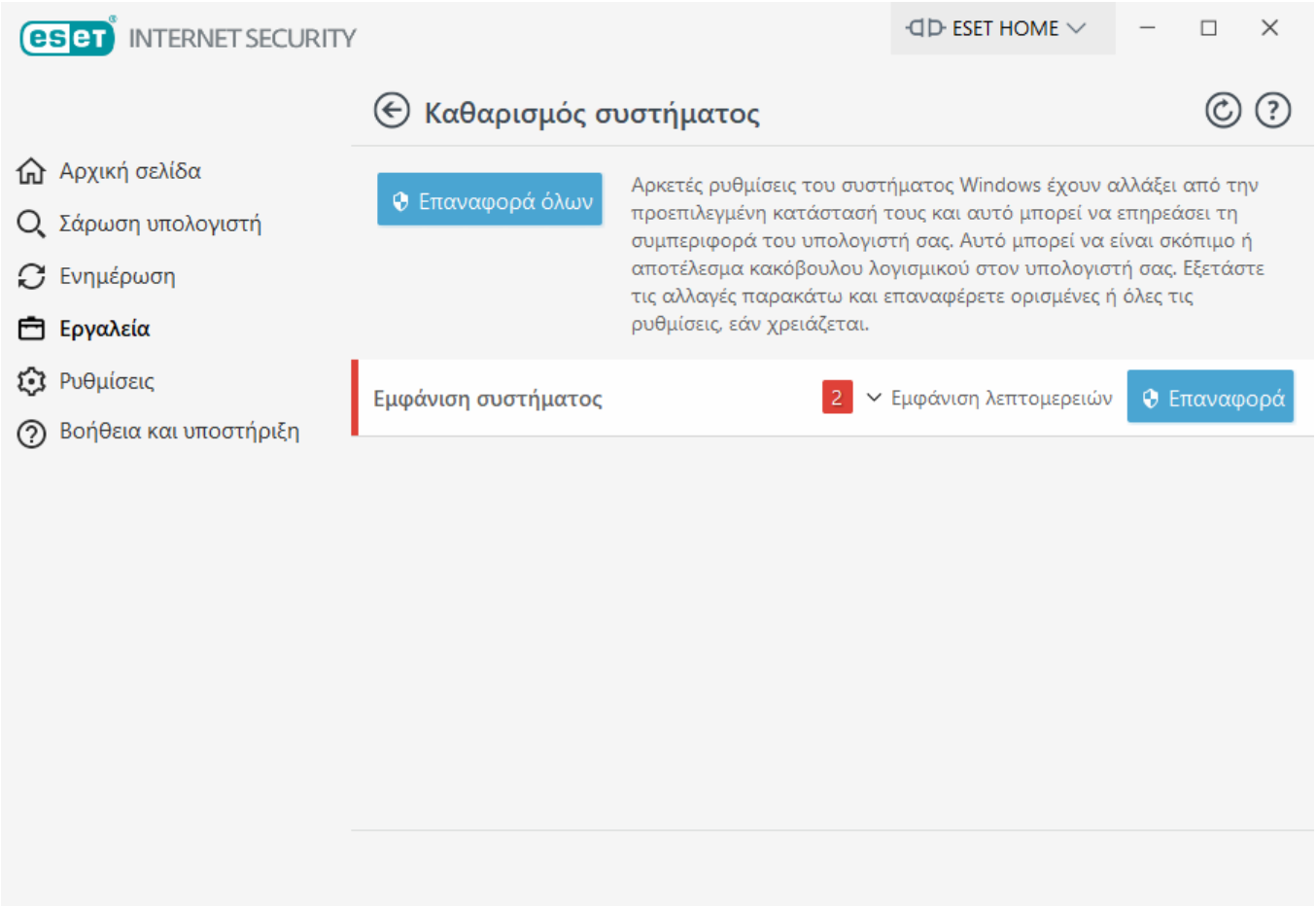
- **Επαναφορά συστήματος των Windows**: ρυθμίσεις για τη δυνατότητα "Επαναφορά συστήματος των Windows", η οποία σάς επιτρέπει να επαναφέρετε το σύστημά σας σε προηγούμενη κατάσταση

Μπορείτε να ζητήσετε καθαρισμό συστήματος:

- όταν βρεθεί μια απειλή

- όταν ένας χρήστης κάνει κλικ στην επιλογή **Επαναφορά**

Μπορείτε να αναθεωρήσετε τις αλλαγές και να πραγματοποιήσετε επαναφορά ρυθμίσεων, εάν χρειάζεται.



Οι ενέργειες στον καθαρισμό συστήματος μπορούν να εκτελεστούν μόνο από έναν χρήστη με δικαιώματα Διαχειριστή.

ESET SysRescue Live

Το ESET SysRescue Live είναι ένα δωρεάν βοηθητικό πρόγραμμα που σας επιτρέπει να δημιουργήσετε ένα CD/DVD ή μονάδα USB διάσωσης με δυνατότητα εκκίνησης. Μπορείτε να εκκινήσετε έναν μολυσμένο υπολογιστή από το μέσο διάσωσης για να κάνετε σάρωση για κακόβουλο λογισμικό και να καθαρίσετε μολυσμένα αρχεία.

Το κύριο πλεονέκτημα του ESET SysRescue Live είναι το γεγονός ότι εκτελείται ανεξάρτητα από το

λειτουργικό σύστημα του κεντρικού υπολογιστή, αλλά με απευθείας πρόσβαση στο δίσκο και στο σύστημα αρχείων. Αυτό καθιστά εφικτή την αφαίρεση απειλών, οι οποίες υπό κανονικές συνθήκες λειτουργίας ενδέχεται να μην ήταν δυνατόν να διαγραφούν (για παράδειγμα, όταν εκτελείται το λειτουργικό σύστημα κ.λπ.).

- Ηλεκτρονική βοήθεια για το ESET SysRescue Live

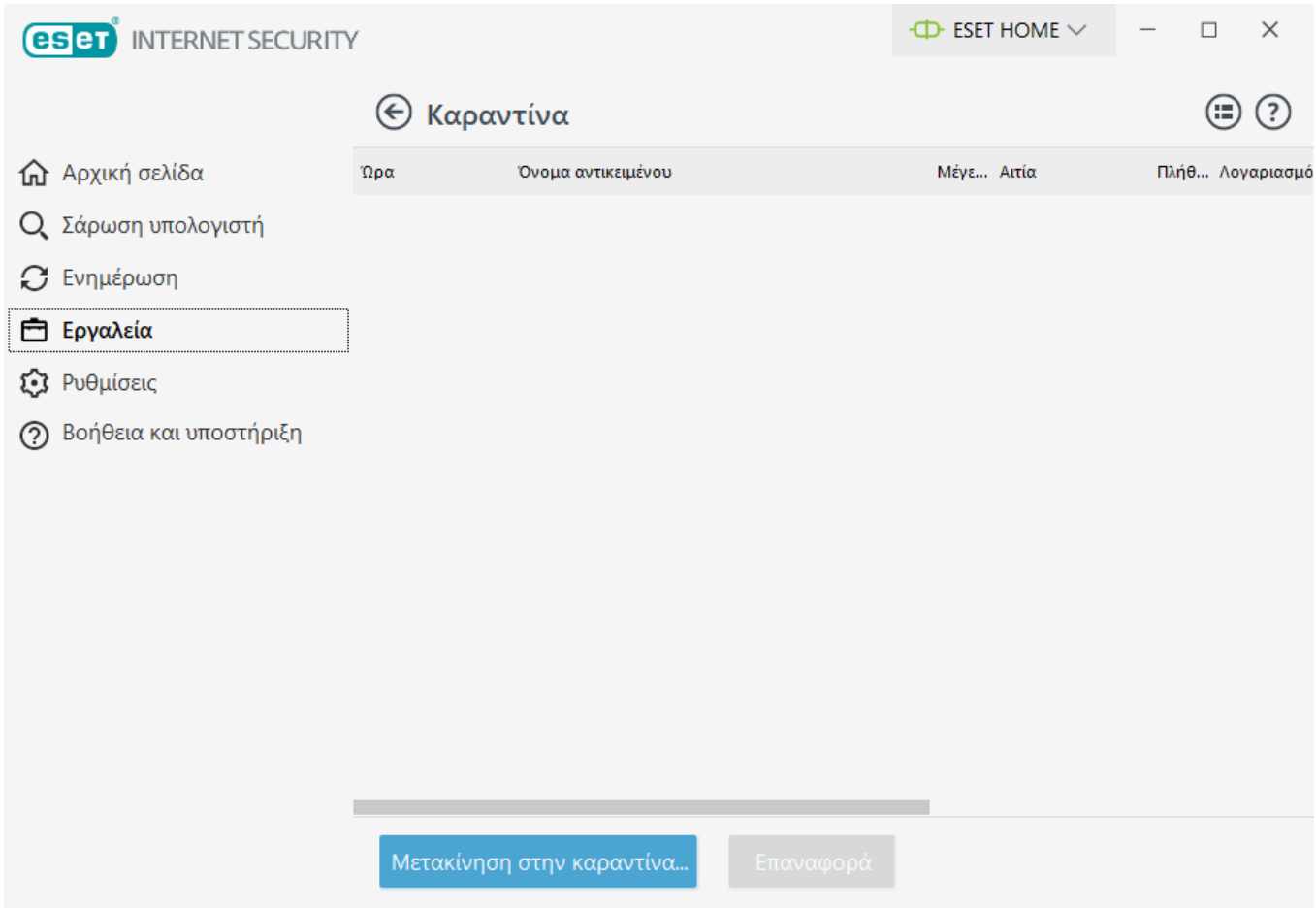
Καραντίνα

Η κύρια λειτουργία της καραντίνας είναι η ασφαλής αποθήκευση των αναφερόμενων αντικειμένων (όπως κακόβουλο λογισμικό, μολυσμένα αρχεία ή ενδεχομένως ανεπιθύμητες εφαρμογές).

Η πρόσβαση στην καραντίνα είναι δυνατή από το κύριο παράθυρο του ESET Internet Security κάνοντας κλικ στα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Καραντίνα**.

Τα αρχεία που είναι αποθηκευμένα στο φάκελο καραντίνας μπορούν να προβληθούν σε έναν πίνακα που εμφανίζει:

- την ημερομηνία και την ώρα που τοποθετήθηκαν σε καραντίνα,
- τη διαδρομή προς την αρχική θέση του αρχείου,
- το μέγεθός τους σε byte,
- αιτιολογία (για παράδειγμα, αντικείμενο που προστέθηκε από το χρήστη),
- και έναν αριθμό ανιχνεύσεων (για παράδειγμα, διπλοτύπων ανιχνεύσεων του ίδιου αρχείου ή εάν πρόκειται για αρχειοθήκη που περιέχει πολλαπλές εισβολές).



Τοποθέτηση αρχείων σε καραντίνα

Το ESET Internet Security τοποθετεί αυτόματα σε καραντίνα τα καταργημένα αρχεία (εάν δεν έχετε ακυρώσει αυτήν την επιλογή στο παράθυρο συναγερμού).

Πρόσθετα αρχεία θα πρέπει να τοποθετούνται σε καραντίνα εάν:

a.δεν μπορούν να καθαριστούν,

b.εάν δεν είναι ασφαλής ή δεν συνιστάται η κατάργησή τους,

c.εάν ανιχνεύονται ψευδώς από το ESET Internet Security,

d.ή εάν ένα αρχείο συμπεριφέρεται ύποπτα, αλλά δεν ανιχνεύεται από τη σάρωση.

Για να τοποθετήσετε ένα αρχείο στην καραντίνα, έχετε πολλές επιλογές:

a.Χρησιμοποιήστε τη δυνατότητα μεταφοράς και απόθεσης για να τοποθετήσετε μη αυτόματα ένα αρχείο στην καραντίνα, κάνοντας κλικ στο αρχείο, μετακινώντας το δείκτη του ποντικιού στην επισημασμένη περιοχή ενώ κρατάτε πατημένο το κουμπί του ποντικιού και, στη συνέχεια, ελευθερώνοντάς το. Μετά από αυτό, η εφαρμογή μετακινείται στο προσκήνιο.

b.Κάντε δεξί κλικ στο αρχείο > κάντε κλικ στο στοιχείο **Επιλογές για προχωρημένους** > **Αρχείο στην καραντίνα**.

c.Κάντε κλικ στο στοιχείο **Μετακίνηση στην καραντίνα** από το παράθυρο **Καραντίνα**.

d.Μπορείτε επίσης να χρησιμοποιήσετε το μενού περιβάλλοντος για αυτό το σκοπό. Κάντε δεξί κλικ στο παράθυρο **Καραντίνα** και επιλέξτε **Καραντίνα**.

Επαναφορά από την καραντίνα

Επίσης, μπορεί να γίνει επαναφορά των αρχείων που βρίσκονται στην καραντίνα στην αρχική τους θέση:

• Για αυτό το σκοπό, χρησιμοποιήστε τη δυνατότητα **Επαναφορά**, η οποία είναι διαθέσιμη από το μενού περιβάλλοντος, κάνοντας δεξί κλικ σε ένα συγκεκριμένο αρχείο που βρίσκεται στην Καραντίνα.

• Εάν ένα αρχείο έχει επισημανθεί ως ενδεχομένως ανεπιθύμητη εφαρμογή, ενεργοποιείται η επιλογή **Επαναφορά και εξαίρεση από τη σάρωση**. Ανατρέξτε επίσης στην ενότητα Εξαιρέσεις.

• Το μενού περιβάλλοντος προσφέρει επίσης την επιλογή **Επαναφορά σε**, η οποία σάς επιτρέπει να επαναφέρετε ένα αρχείο σε μια τοποθεσία διαφορετική από εκείνη από την οποία καταργήθηκε.

• Η λειτουργία επαναφοράς δεν είναι διαθέσιμη σε ορισμένες περιπτώσεις, για παράδειγμα, για αρχεία που βρίσκονται σε κοινόχρηστο δίκτυο με δικαίωμα μόνο για ανάγνωση.

Κατάργηση από την Καραντίνα

Κάντε δεξί κλικ σε ένα συγκεκριμένο στοιχείο και επιλέξτε **Κατάργηση από την καραντίνα**, ή επιλέξτε το στοιχείο που θέλετε να καταργήσετε και πατήστε το πλήκτρο **Delete** στο πληκτρολόγιό σας. Μπορείτε επίσης να επιλέξετε πολλά στοιχεία ταυτόχρονα και να τα καταργήσετε όλα μαζί. Τα καταργημένα στοιχεία θα αφαιρεθούν οριστικά από τη συσκευή σας και από την καραντίνα.

Υποβολή ενός αρχείου από την Καραντίνα

Εάν έχετε τοποθετήσει στην καραντίνα ένα ύποπτο αρχείο, το οποίο δεν ανιχνεύτηκε από το πρόγραμμα ή εάν ένα αρχείο προσδιορίστηκε εσφαλμένα ως μολυσμένο (για παράδειγμα, με ευριστική ανάλυση του κώδικα) και στη συνέχεια τοποθετήθηκε στην καραντίνα, αποστείλετε το δείγμα για ανάλυση στο Εργαστήριο ερευνών της ESET. Για να υποβάλετε ένα αρχείο, κάντε δεξί κλικ στο αρχείο και επιλέξτε **Υποβολή για ανάλυση** από το μενού περιβάλλοντος.

Περιγραφή ανίχνευσης

Κάντε δεξί κλικ σε ένα στοιχείο και στην επιλογή **Περιγραφή ανίχνευσης** για να ανοίξει η Εγκυκλοπαίδεια απειλών της ESET, η οποία περιέχει λεπτομερείς πληροφορίες για τους κινδύνους και τα συμπτώματα της καταγεγραμμένης εισβολής.

> **Εικονογραφημένες οδηγίες**
> Τα ακόλουθα άρθρα της Γνωσιακής βάσης της ESET μπορεί να είναι διαθέσιμα μόνο στα Αγγλικά:
> • Επαναφορά ενός αρχείου στην καραντίνα στο ESET Internet Security
> • Κατάργηση ενός αρχείου στην καραντίνα στο ESET Internet Security
> • Το προϊόν της ESET με ειδοποίησε σχετικά με μια ανίχνευση — τι πρέπει να κάνω;

Η μεταφορά στην καραντίνα απέτυχε

Οι λόγοι για τους οποίους δεν είναι δυνατή η μετακίνηση συγκεκριμένων αρχείων στην Καραντίνα είναι οι ακόλουθοι:

- **Δεν έχετε δικαιώματα ανάγνωσης** – αυτό σημαίνει ότι δεν μπορείτε να προβάλετε το περιεχόμενο ενός αρχείου.
- **Δεν έχετε δικαιώματα εγγραφής** – αυτό σημαίνει ότι δεν μπορείτε να τροποποιήσετε το περιεχόμενο του αρχείου, δηλ. να προσθέσετε νέο περιεχόμενο ή να καταργήσετε το υπάρχον περιεχόμενο.
- **Το αρχείο που προσπαθείτε να θέσετε στην καραντίνα, είναι πολύ μεγάλο** – Πρέπει να μειώσετε το μέγεθος του αρχείου.

Εάν εμφανιστεί ένα μήνυμα σφάλματος «Η καραντίνα απέτυχε», κάντε κλικ στο στοιχείο **Περισσότερες πληροφορίες**. Θα εμφανιστεί το παράθυρο με τη λίστα σφαλμάτων καραντίνας και θα δείτε το όνομα του αρχείου και το λόγο για τον οποίο το αρχείο δεν μπορεί να τεθεί σε καραντίνα.

Διακομιστής μεσολάβησης

Σε μεγάλα δίκτυα LAN, η επικοινωνία ανάμεσα στον υπολογιστή σας και στο διαδίκτυο μπορεί να γίνει μέσω διακομιστή μεσολάβησης. Χρησιμοποιώντας αυτήν τη διαμόρφωση, πρέπει να οριστούν οι ακόλουθες ρυθμίσεις. Διαφορετικά, το πρόγραμμα δεν θα μπορεί να ενημερώνεται αυτόματα. Στο ESET Internet Security, υπάρχει ρύθμιση διακομιστή μεσολάβησης από δύο διαφορετικές ενότητες στη δομή "Ρυθμίσεις για προχωρημένους".

Πρώτον, οι ρυθμίσεις διακομιστή μεσολάβησης μπορούν να διαμορφωθούν στις **Ρυθμίσεις για προχωρημένους** στο στοιχείο **Εργαλεία** > **Διακομιστής μεσολάβησης**. Ο καθορισμός του διακομιστή μεσολάβησης σε αυτό το επίπεδο προσδιορίζει τις γενικές ρυθμίσεις διακομιστή μεσολάβησης στο σύνολο του ESET Internet Security. Οι παράμετροι που ορίζονται εδώ θα χρησιμοποιούνται από όλες τις μονάδες που απαιτούν σύνδεση με το διαδίκτυο.

Για να καθορίσετε ρυθμίσεις διακομιστή μεσολάβησης για αυτό το επίπεδο, επιλέξτε **Χρήση διακομιστή μεσολάβησης** και εισαγάγετε τη διεύθυνση του διακομιστή μεσολάβησης στο πεδίο **Διακομιστής μεσολάβησης**, μαζί με τον αριθμό θύρας του διακομιστή μεσολάβησης στο πεδίο **Θύρα**.

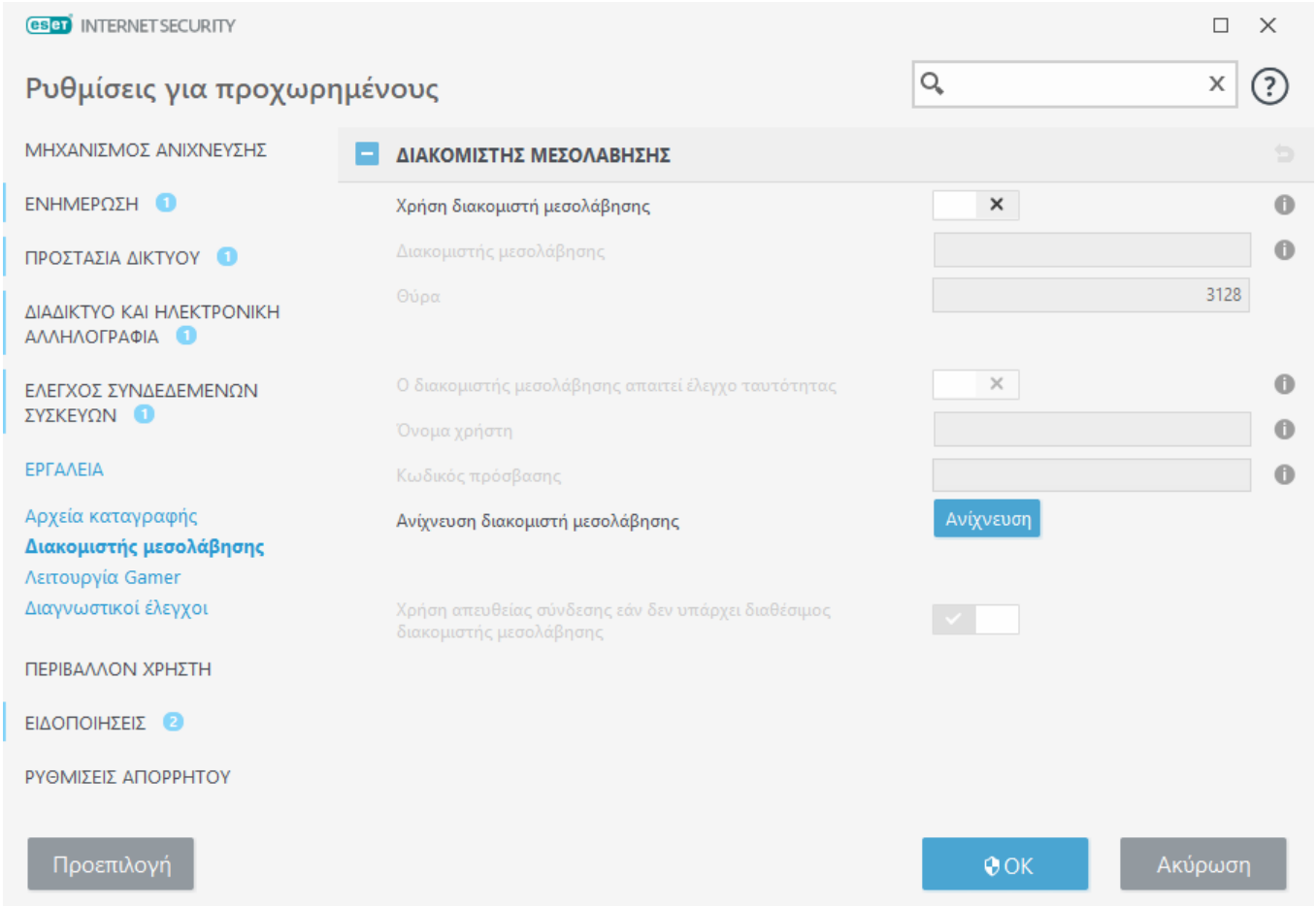
Αν η επικοινωνία με το διακομιστή μεσολάβησης απαιτεί έλεγχο ταυτότητας, επιλέξτε **Ο διακομιστής μεσολάβησης απαιτεί έλεγχο ταυτότητας** και εισαγάγετε ένα έγκυρο όνομα χρήστη και κωδικό πρόσβασης στα αντίστοιχα πεδία **Όνομα χρήστη** και **Κωδικός πρόσβασης**. Κάντε κλικ στο στοιχείο **Ανίχνευση διακομιστή μεσολάβησης** για αυτόματη ανίχνευση και συμπλήρωση των ρυθμίσεων του διακομιστή μεσολάβησης. Θα αντιγραφούν οι παράμετροι που καθορίζονται στις Επιλογές Internet για το Internet Explorer ή το Google Chrome.

> Πρέπει να πληκτρολογήσετε οι ίδιοι το όνομα χρήστη και τον κωδικό πρόσβασης στις ρυθμίσεις **Διακομιστής μεσολάβησης**.

Χρήση απευθείας σύνδεσης εάν δεν υπάρχει διαθέσιμος διακομιστής μεσολάβησης – Εάν το ESET Internet Security έχει διαμορφωθεί έτσι ώστε να συνδέεται μέσω διακομιστή μεσολάβησης και η επικοινωνία με το διακομιστή μεσολάβησης δεν είναι δυνατή, το ESET Internet Security θα παρακάμπτει

το διακομιστή μεσολάβησης και θα επικοινωνεί απευθείας με τους διακομιστές της ESET.

Μπορείτε επίσης να διαμορφώσετε τις ρυθμίσεις του διακομιστή μεσολάβησης μέσα από τις "Προηγμένες ρυθμίσεις ενημέρωσης" (**Ρυθμίσεις για προχωρημένους** > **Ενημέρωση** > **Προφίλ** > **Ενημερώσεις** > **Επιλογές σύνδεσης** επιλέγοντας **Σύνδεση μέσω διακομιστή μεσολάβησης** από το αναπτυσσόμενο μενού **Λειτουργία διακομιστή μεσολάβησης**). Η ρύθμιση αυτή εφαρμόζεται για το συγκεκριμένο προφίλ ενημέρωσης και συνιστάται για φορητούς υπολογιστές που λαμβάνουν συχνά ενημερώσεις αναγνώρισης ιών από απομακρυσμένες τοποθεσίες. Για περισσότερες λεπτομέρειες σχετικά με αυτήν τη ρύθμιση, ανατρέξτε στο κεφάλαιο Προηγμένες ρυθμίσεις ενημέρωσης.



Επιλογή δείγματος για ανάλυση

Εάν εντοπίσετε ένα ύποπτο αρχείο στον υπολογιστή σας ή έναν ύποπτο ιστότοπο στο διαδίκτυο, μπορείτε να το υποβάλετε στο Εργαστήριο ερευνών της ESET για ανάλυση (ενδέχεται να μην είναι διαθέσιμο βάσει της ρύθμισης παραμέτρων του ESET LiveGrid®).

Προτού υποβάλετε δείγματα στην ESET

Μην υποβάλετε ένα δείγμα εάν δεν πληροί τουλάχιστον ένα από τα ακόλουθα κριτήρια:

- Το δείγμα δεν ανιχνεύτηκε καθόλου από το προϊόν της ESET
- Το δείγμα ανιχνεύεται εσφαλμένα ως απειλή
- Δεν αποδεχόμαστε τα προσωπικά αρχεία σας (που θα θέλατε να σαρώσει η ESET για κακόβουλο λογισμικό) ως δείγματα (το Εργαστήριο ερευνών της ESET δεν εκτελεί σαρώσεις κατ' απαίτηση για τους χρήστες)
- Χρησιμοποιήστε μια γραμμή περιγραφής του θέματος και συμπεριλάβετε όσο το δυνατόν περισσότερες πληροφορίες για το αρχείο (για παράδειγμα, στιγμιότυπο οθόνης ή τον ιστότοπο από τον οποίο το λάβατε).

Μπορείτε να στείλετε μια υποβολή δείγματος (ένα αρχείο ή έναν ιστότοπο) στην ESET για ανάλυση χρησιμοποιώντας μία από τις παρακάτω μεθόδους:

1. Χρησιμοποιήστε τη φόρμα υποβολής δείγματος στο προϊόν σας. Βρίσκεται στη διαδρομή **Εργαλεία** > **Περισσότερα εργαλεία** > **Υποβολή δείγματος για ανάλυση**. Το μέγιστο μέγεθος ενός υποβληθέντος δείγματος είναι 256MB.

2. Εναλλακτικά, μπορείτε να υποβάλετε το αρχείο με email. Αν προτιμάτε αυτή την επιλογή, συμπιέστε το ή τα αρχεία με το WinRAR/WinZIP, προστατέψτε το αρχείο με τον κωδικό πρόσβασης «infected» και στείλτε το στη διεύθυνση samples@eset.com.

3. Για να αναφέρετε ανεπιθύμητα μηνύματα ή ψευδώς θετικά ανεπιθύμητα μηνύματα ή ιστότοπους που έχουν κατηγοριοποιηθεί εσφαλμένα από τη μονάδα Γονικού ελέγχου, ανατρέξτε στο άρθρο της Γνωσιακής βάσης της ESET.

Στη φόρμα **Επιλογή δείγματος για ανάλυση**, επιλέξτε από το αναπτυσσόμενο μενού **Λόγος υποβολής του δείγματος** την περιγραφή που ταιριάζει καλύτερα στο σκοπό του μηνύματός σας:

- Ύποπτο αρχείο
- Ύποπτος ιστότοπος (ένας ιστότοπος που έχει μολυνθεί από οποιοδήποτε κακόβουλο λογισμικό),
- Ιστότοπος με εσφαλμένη σήμανση
- Αρχείο με εσφαλμένη σήμανση (αρχείο που έχει ανιχνευτεί ως μόλυνση αλλά δεν είναι μολυσμένο),
- Άλλο

Αρχείο/Ιστότοπος – Η διαδρομή για το αρχείο ή ο ιστότοπος που θέλετε να υποβάλλετε.

Email επικοινωνίας – Αυτό το email επικοινωνίας αποστέλλεται μαζί με ύποπτα αρχεία στην ESET και μπορεί να χρησιμοποιηθεί για επικοινωνία μαζί σας αν απαιτούνται περισσότερες πληροφορίες για την ανάλυση. Η εισαγωγή email επικοινωνίας είναι προαιρετική. Επιλέξτε **Ανώνυμη υποβολή** για να το αφήσετε κενό.

> **Ενδέχεται να μη λάβετε απάντηση από την ESET**
> Δεν θα λάβετε απάντηση από την ESET παρά μόνο αν απαιτούνται περισσότερες πληροφορίες. Οι διακομιστές μας λαμβάνουν κάθε μέρα δεκάδες χιλιάδες αρχεία και είναι αδύνατον να δίνεται απάντηση σε όλες οι υποβολές.
> Αν αποδειχτεί ότι το αρχείο είναι κακόβουλη εφαρμογή ή ιστότοπος, η ανίχνευσή του θα προστεθεί σε μια μελλοντική ενημέρωση της ESET.

Επιλογή δείγματος για ανάλυση - Ύποπτο αρχείο

Ενδείξεις και συμπτώματα μόλυνσης από κακόβουλο λογισμικό – Εισαγάγετε μια περιγραφή της συμπεριφοράς του ύποπτου αρχείου που παρατηρείτε στον υπολογιστή σας.

Προέλευση αρχείου (διεύθυνση URL ή προμηθευτής) – Πληκτρολογήστε μια προέλευση του αρχείου (πηγή) και πώς βρήκατε αυτό το αρχείο.

Σημειώσεις και πρόσθετες πληροφορίες – Εδώ μπορείτε να εισαγάγετε πρόσθετες πληροφορίες ή μια περιγραφή που θα βοηθήσει κατά την επεξεργασία αναγνώρισης του ύποπτου αρχείου.

> Η πρώτη παράμετρος – **Ενδείξεις και συμπτώματα μόλυνσης από κακόβουλο λογισμικό** – είναι απαραίτητη, αλλά η παροχή πρόσθετων πληροφοριών θα βοηθήσει σημαντικά τα εργαστήριά μας στη διαδικασία αναγνώρισης και την επεξεργασία των δειγμάτων.

Επιλογή δείγματος για ανάλυση - Ύποπτος ιστότοπος

Επιλέξτε ένα από τα παρακάτω από το αναπτυσσόμενο μενού **Ποιο είναι το πρόβλημα με αυτόν τον ιστότοπο**:

- **Μολυσμένος** – Ένας ιστότοπος που περιέχει ιούς ή άλλο κακόβουλο λογισμικό που διανέμεται με διάφορες μεθόδους.

- **Phishing** – Συχνά χρησιμοποιείται για πρόσβαση σε ευαίσθητα δεδομένα όπως αριθμοί τραπεζικών λογαριασμών, αριθμοί PIN και άλλα. Διαβάστε περισσότερα για αυτό τον τύπο εισβολής στο γλωσσάρι.

- **Απάτη** – Ένας παραπλανητικός ή απατηλός ιστότοπος, ιδιαίτερα για να βγάλει γρήγορα κέρδη.

- Επιλέξτε **Άλλα** αν οι προαναφερθείσες επιλογές δεν περιγράφουν τον ιστότοπο που πρόκειται να υποβάλλετε.

Σημειώσεις και πρόσθετες πληροφορίες – Εδώ μπορείτε να εισαγάγετε πρόσθετες πληροφορίες ή μια περιγραφή που θα βοηθήσει κατά την ανάλυση του ύποπτου ιστότοπου.

Επιλογή δείγματος για ανάλυση - Ψευδώς θετικό αρχείο

Θα θέλαμε να υποβάλετε αρχεία που ανιχνεύονται ως μόλυνση αλλά δεν είναι μολυσμένα για να βελτιώσουμε το μηχανισμό antivirus και antispyware και για να βοηθήσουμε στην προστασία άλλων ατόμων. Ο εσφαλμένος αποκλεισμός (FP) μπορεί να προκύψει όταν το μοτίβο ενός αρχείου αντιστοιχεί στο ίδιο μοτίβο που περιέχεται σε έναν μηχανισμό ανίχνευσης.

Όνομα και έκδοση εφαρμογής – Ο τίτλος και η έκδοση του προγράμματος (για παράδειγμα ο αριθμός, το ψευδώνυμο ή το κωδικό όνομα).

Προέλευση αρχείου (διεύθυνση URL ή προμηθευτής) – Εισαγάγετε μια προέλευση του αρχείου (πηγή) και σημειώστε πώς βρήκατε αυτό το αρχείο.

Σκοπός της εφαρμογής – Η γενική περιγραφή της εφαρμογής, ο τύπος μιας εφαρμογής (π.χ. πρόγραμμα περιήγησης, πρόγραμμα αναπαραγωγής μέσων, ...) και η λειτουργικότητά της.

Σημειώσεις και πρόσθετες πληροφορίες – Εδώ μπορείτε να προσθέσετε επιπλέον πληροφορίες ή περιγραφές που θα βοηθήσουν κατά την επεξεργασία του ύποπτου αρχείου.

> Οι πρώτες τρεις παράμετροι απαιτούνται για την αναγνώριση νόμιμων εφαρμογών και για να είναι δυνατή η διάκρισή τους από τον κακόβουλο κώδικα. Η παροχή πρόσθετων πληροφοριών θα βοηθήσει σημαντικά τα εργαστήριά μας στη διαδικασία αναγνώρισης και την επεξεργασία των δειγμάτων.

Επιλογή δείγματος για ανάλυση - Ψευδώς θετικός ιστότοπος

Θα θέλαμε να υποβάλλετε ιστότοπους που έχουν ανιχνευτεί ως μολυσμένοι, απατηλοί ή phishing χωρίς να είναι. Ο εσφαλμένος αποκλεισμός (FP) μπορεί να προκύψει όταν το μοτίβο ενός αρχείου αντιστοιχεί στο ίδιο μοτίβο που περιέχεται σε έναν μηχανισμό ανίχνευσης. Υποβάλλετε αυτό τον ιστότοπο για να βελτιώσετε τον μηχανισμό μας antivirus και anti-phishing, και για να βοηθήσετε στην προστασία άλλων ατόμων.

Σημειώσεις και πρόσθετες πληροφορίες – Εδώ μπορείτε να προσθέσετε επιπλέον πληροφορίες ή περιγραφές που θα βοηθήσουν κατά την επεξεργασία του ύποπτου ιστότοπου.

Επιλογή δείγματος για ανάλυση - Άλλο

Χρησιμοποιήστε αυτή τη φόρμα αν δεν μπορεί να κατηγοριοποιηθεί το αρχείο ως ΄**Ύποπτο αρχείο** ή ως **Εσφαλμένος αποκλεισμός**.

Λόγος υποβολής του αρχείου – Εισαγάγετε μια λεπτομερή περιγραφή και την αιτία για την οποία στέλνετε το αρχείο.

Microsoft Windows® Update

Η δυνατότητα ενημέρωσης των Windows είναι ένα σημαντικό στοιχείο προστασίας των χρηστών από κακόβουλο λογισμικό. Για αυτό τον λόγο, είναι σημαντικό να κάνετε εγκατάσταση των ενημερώσεων των Microsoft Windows μόλις είναι διαθέσιμες. Το ESET Internet Security σάς ειδοποιεί για τις ενημερώσεις που λείπουν, σύμφωνα με το επίπεδο που καθορίζετε. Είναι διαθέσιμα τα παρακάτω επίπεδα:

- **Καμία ενημέρωση** – Δεν θα προσφέρεται καμία ενημέρωση συστήματος για λήψη.
- **Προαιρετικές ενημερώσεις** – Οι ενημερώσεις που έχουν επισημανθεί ως χαμηλής προτεραιότητας και ανώτερες θα προσφέρονται για λήψη.
- **Συνιστώμενες ενημερώσεις** – Οι ενημερώσεις που έχουν επισημανθεί ως συνήθεις και ανώτερες θα προσφέρονται για λήψη.
- **Σημαντικές ενημερώσεις** – Οι ενημερώσεις που έχουν επισημανθεί ως σημαντικές και ανώτερες θα προσφέρονται για λήψη.
- **Κρίσιμες ενημερώσεις** – Θα προσφέρονται για λήψη μόνο οι κρίσιμες ενημερώσεις.

Κάντε κλικ στο **OK** για να αποθηκεύσετε τις αλλαγές. Θα εμφανιστεί το παράθυρο Ενημερώσεων συστήματος μετά από την επαλήθευση της κατάστασης με τον διακομιστή ενημερώσεων. Αντίστοιχα, οι πληροφορίες ενημέρωσης συστήματος μπορεί να μην είναι αμέσως διαθέσιμες μετά την αποθήκευση των αλλαγών.

Παράθυρο διαλόγου - Ενημερώσεις συστήματος

Εάν υπάρχουν κάποιες ενημερώσεις διαθέσιμες για το λειτουργικό σύστημά σας, το παράθυρο αρχικής οθόνης του ESET Internet Security εμφανίζει την ειδοποίηση. Κάντε κλικ στο στοιχείο **Περισσότερες πληροφορίες** για να ανοίξετε το παράθυρο ενημερώσεων συστήματος.

Το παράθυρο "Ενημερώσεις συστήματος" εμφανίζει τη λίστα των διαθέσιμων ενημερώσεων που είναι έτοιμες για λήψη και εγκατάσταση. Ο τύπος ενημέρωσης εμφανίζεται δίπλα στο όνομα της ενημέρωσης.

Κάντε διπλό κλικ σε οποιαδήποτε σειρά ενημέρωσης για να εμφανιστεί το παράθυρο Πληροφορίες ενημέρωσης με πρόσθετες πληροφορίες.

Κάντε κλικ στην επιλογή **Εκτέλεση ενημέρωσης συστήματος** για να ξεκινήσει η λήψη και η εγκατάσταση ενημερώσεων του λειτουργικού συστήματος.

Πληροφορίες ενημέρωσης

Πληροφορίες σχετικά με τις ενημερώσεις των Windows. Το όνομα και ο αριθμός της ενημέρωσης εμφανίζονται στο επάνω μέρος του παραθύρου και ακολουθούνται από την προτεραιότητα και μια περιγραφή του προβλήματος που επιλύεται με την ενημέρωση.

Περιβάλλον χρήστη

Για να ρυθμίσετε τις παραμέτρους της συμπεριφοράς του γραφικού περιβάλλοντος χρήστη (GUI) του προγράμματος, στο κύριο παράθυρο του προγράμματος, κάντε κλικ στα στοιχεία **Ρύθμιση** > **Ρυθμίσεις για προχωρημένους** (F5) > **Περιβάλλον χρήστη**.

Μπορείτε να ρυθμίσετε την οπτική εμφάνιση και τα εφέ του προγράμματος στην οθόνη των Ρυθμίσεων για προχωρημένους Στοιχεία περιβάλλοντος χρήστη.

Για τη μέγιστη προστασία από το λογισμικό ασφάλειας, μπορείτε να αποτρέψετε την κατάργηση εγκατάστασης και οποιεσδήποτε μη εξουσιοδοτημένες αλλαγές προστατεύοντας τις ρυθμίσεις με έναν κωδικό πρόσβασης, χρησιμοποιώντας το εργαλείο Ρύθμιση πρόσβασης.

> Για να ρυθμίσετε τις παραμέτρους της συμπεριφοράς των ειδοποιήσεων συστήματος, των συναγερμών ανίχνευσης και των καταστάσεων εφαρμογής, ανατρέξτε στην ενότητα Ειδοποιήσεις.

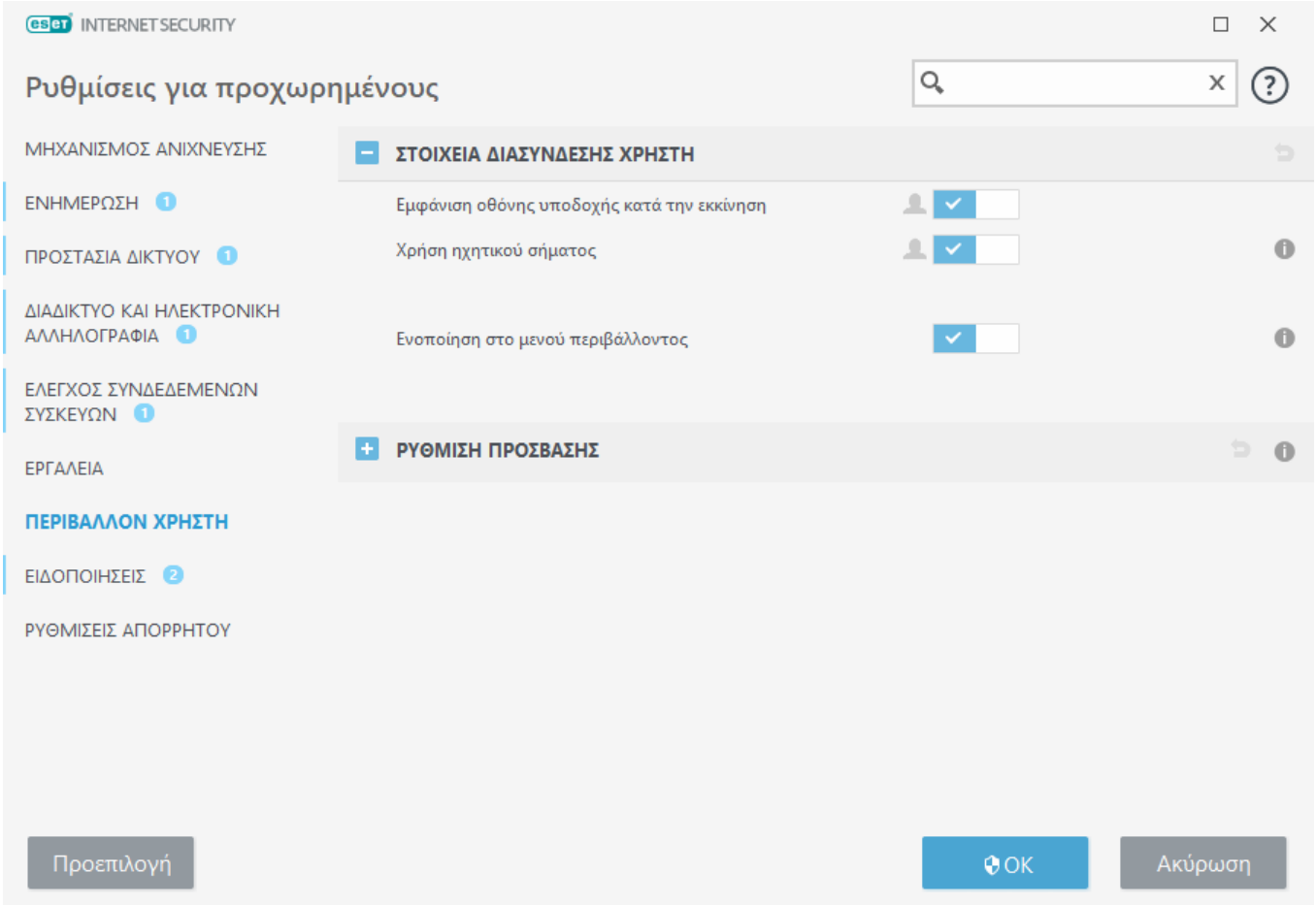
Στοιχεία διασύνδεσης χρήστη

Οι επιλογές διαμόρφωσης της διασύνδεσης χρήστη στο ESET Internet Security σάς επιτρέπουν να προσαρμόσετε το περιβάλλον εργασίας ώστε να εκπληρώνει τις ανάγκες σας. Αυτές οι επιλογές διαμόρφωσης βρίσκονται στη διαδρομή **Ρυθμίσεις για προχωρημένους** (F5) > **Διασύνδεση χρήστη** > **Στοιχεία διασύνδεσης χρήστη**.

Αν θέλετε να απενεργοποιήσετε την οθόνη υποδοχής του ESET Internet Security, καταργήστε την επιλογή **Εμφάνιση οθόνης υποδοχής κατά την εκκίνηση**.

Χρήση ηχητικού σήματος – Το ESET Internet Security αναπαράγει έναν ήχο όταν προκύπτουν σημαντικά συμβάντα κατά τη διάρκεια μιας σάρωσης, για παράδειγμα όταν ανακαλύπτεται μια απειλή ή όταν ολοκληρωθεί μια σάρωση.

Ενοποίηση στο μενού περιβάλλοντος – Ενοποιήστε τα στοιχεία ελέγχου του ESET Internet Security στο μενού περιβάλλοντος.



Ρύθμιση πρόσβασης

Οι ρυθμίσεις του ESET Internet Security αποτελούν κρίσιμο μέρος της πολιτικής ασφαλείας σας. Οι μη εξουσιοδοτημένες τροποποιήσεις μπορούν δυνητικά να θέσουν σε κίνδυνο τη σταθερότητα και την προστασία του συστήματός σας. Για να αποφεύγονται μη εξουσιοδοτημένες τροποποιήσεις, μπορείτε να προστατέψετε με κωδικό πρόσβασης τις παραμέτρους εγκατάστασης και κατάργησης εγκατάστασης του ESET Internet Security.

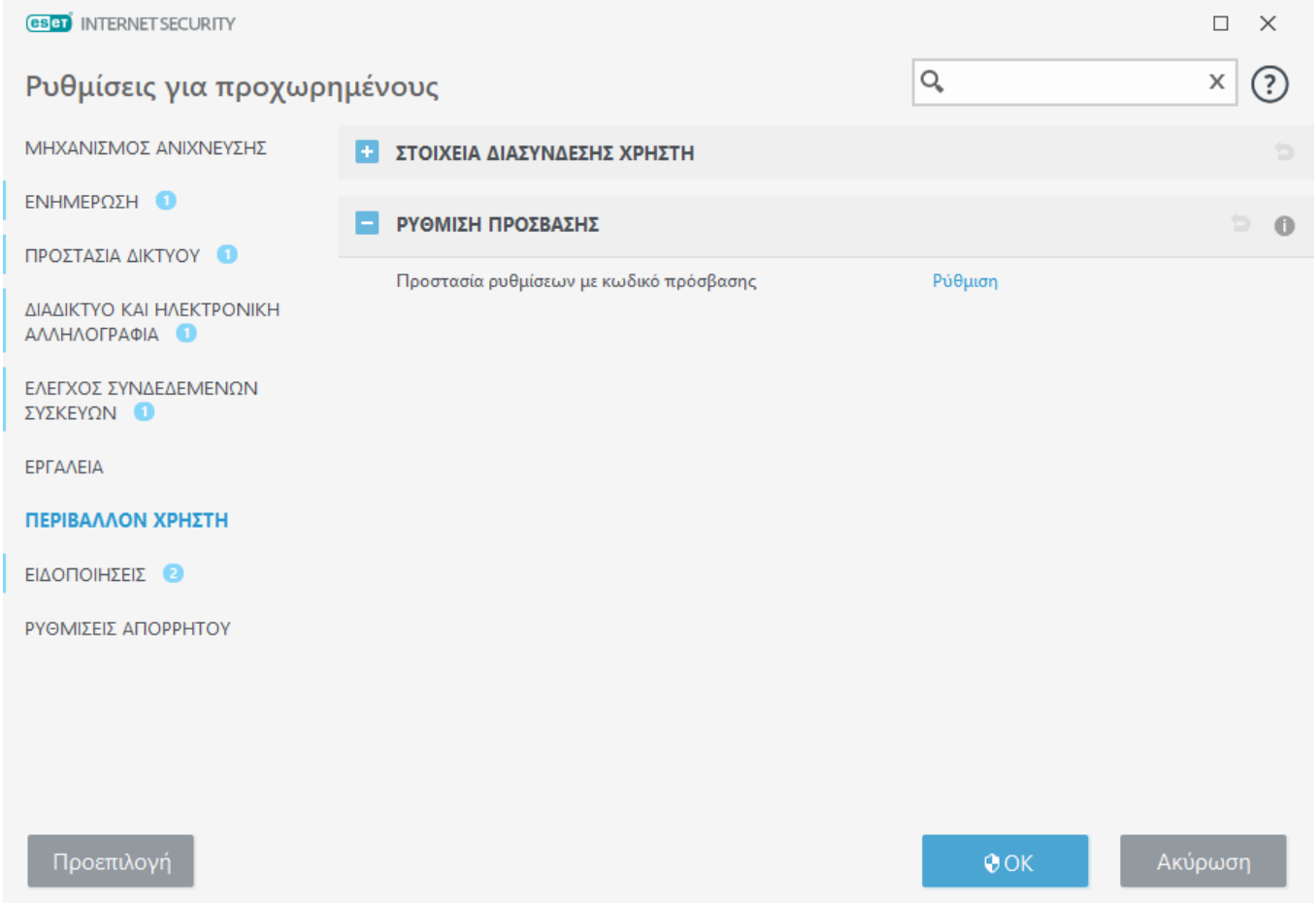
Για να ρυθμίσετε έναν κωδικό πρόσβασης για την προστασία των παραμέτρων εγκατάστασης και κατάργησης εγκατάστασης του ESET Internet Security, κάντε κλικ στην επιλογή **Ρύθμιση** που βρίσκεται δίπλα στο στοιχείο **Προστασία ρυθμίσεων με κωδικό πρόσβασης**.

Εάν θέλετε να αποκτήσετε πρόσβαση στις Ρυθμίσεις για προχωρημένους, εμφανίζεται το παράθυρο για την εισαγωγή του κωδικού πρόσβασης. Εάν ξεχάσετε ή χάσετε τον κωδικό πρόσβασής σας, κάντε κλικ στην παρακάτω επιλογή **Επαναφορά κωδικού πρόσβασης** και εισαγάγετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου που χρησιμοποιήσατε για την εγγραφή της άδειας χρήσης. Η ESET θα σας στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου με τον κωδικό επαλήθευσης και οδηγίες σχετικά με τον τρόπο επαναφοράς του κωδικού πρόσβασής σας.

- Πώς να ξεκλειδώσετε τις Ρυθμίσεις για προχωρημένους

Για να αλλάξετε τον κωδικό πρόσβασής σας, κάντε κλικ στο στοιχείο **Αλλαγή κωδικού πρόσβασης** που βρίσκεται δίπλα στο στοιχείο **Προστασία ρυθμίσεων με κωδικό πρόσβασης**.

Για να καταργήσετε τον κωδικό πρόσβασής σας, κάντε κλικ στο στοιχείο **Κατάργηση** που βρίσκεται δίπλα στο στοιχείο **Προστασία ρυθμίσεων με κωδικό πρόσβασης**.



Κωδικός πρόσβασης για Εγκατάσταση για προχωρημένους

Για την προστασία της εγκατάστασης για προχωρημένους του ESET Internet Security, προκειμένου να αποφεύγεται η μη εξουσιοδοτημένη τροποποίηση, πρέπει να ρυθμιστεί νέος κωδικός πρόσβασης.

Εάν θέλετε να αλλάξετε έναν υπάρχοντα κωδικό πρόσβασης:

1. Πληκτρολογήστε τον παλιό κωδικό πρόσβασης στο πεδίο **Παλιός κωδικός πρόσβασης**.

2. Εισαγάγετε τον νέο κωδικό πρόσβασης στα πεδία **Νέος κωδικός πρόσβασης** και **Επιβεβαίωση κωδικού πρόσβασης**.

3. Κάντε κλικ στο στοιχείο **OK**.

Αυτός ο κωδικός πρόσβασης θα απαιτείται για οποιεσδήποτε μελλοντικές τροποποιήσεις του ESET Internet Security.

Εάν ξεχάσετε τον κωδικό πρόσβασής σας, μπορεί να γίνει επαναφορά της πρόσβασης στις ρυθμίσεις για προχωρημένους χρησιμοποιώντας τη μέθοδο «Επαναφορά κωδικού πρόσβασης».

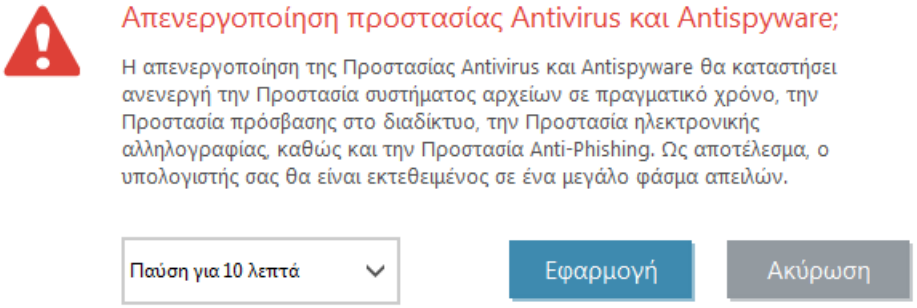
Για να ανακτήσετε το χαμένο κλειδί άδειας χρήσης της ESET, την ημερομηνία λήξης της άδειας χρήσης σας ή άλλες πληροφορίες άδειας χρήσης για το ESET Internet Security, ανατρέξτε στο άρθρο της Γνωσιακής Βάσης.

Εικονίδιο περιοχής ειδοποιήσεων

Ορισμένες από τις πιο σημαντικές επιλογές ρυθμίσεων και δυνατότητες διατίθενται κάνοντας δεξί κλικ στο εικονίδιο της γραμμής ειδοποιήσεων .

Παύση προστασίας – Εμφανίζει το παράθυρο διαλόγου επιβεβαίωσης που απενεργοποιεί το στοιχείο Μηχανισμός ανίχνευσης, το οποίο προφυλάσσει από κακόβουλες επιθέσεις κατά του συστήματος ελέγχοντας την επικοινωνία αρχείων, διαδικτύου και email.

Το αναπτυσσόμενο μενού **Χρονικό διάστημα** αντιπροσωπεύει τη χρονική περίοδο για την οποία θα απενεργοποιηθεί η προστασία.



Παύση του τείχος προστασίας (να επιτρέπεται όλη η κυκλοφορία) – Πραγματοποιεί εναλλαγή του τείχος προστασίας σε ανενεργή κατάσταση. Ανατρέξτε στην ενότητα Δίκτυο για περισσότερες πληροφορίες.

Αποκλεισμός όλης της κυκλοφορίας δικτύου – Αποκλείει κάθε είδους κυκλοφορία δικτύου. Μπορείτε να την ενεργοποιήσετε ξανά κάνοντας κλικ στην επιλογή **Διακοπή αποκλεισμού όλης της κυκλοφορίας δικτύου**.

Ρυθμίσεις για προχωρημένους – Επιλέξτε αυτό το στοιχείο για να ανοίξετε τη δομή **Ρυθμίσεις για προχωρημένους**. Υπάρχουν κι άλλοι τρόποι για να ανοίξετε τις Ρυθμίσεις για προχωρημένους, όπως να πατήσετε το πλήκτρο F5 ή να πλοηγηθείτε στα στοιχεία **Ρυθμίσεις** > **Ρυθμίσεις για προχωρημένους**.

Αρχεία καταγραφής – Τα Αρχεία καταγραφής περιέχουν πληροφορίες για σημαντικά συμβάντα του προγράμματος που έχουν προκύψει και παρέχουν μια επισκόπηση των ανιχνεύσεων.

Άνοιγμα του ESET Internet Security – Ανοίγει το κύριο παράθυρο του προγράμματος ESET Internet Security από το εικονίδιο του δίσκου.

Επαναφορά διάταξης παραθύρου – Επαναφέρει το παράθυρο του ESET Internet Security στο προεπιλεγμένο μέγεθος και τη θέση του στην οθόνη.

Έλεγχος για ενημερώσεις – Ξεκινά την ενημέρωση του μηχανισμού ανίχνευσης (ο οποίος ονομαζόταν παλαιότερα «βάση αναγνώρισης ιών») για να διασφαλίζεται το επίπεδο προστασίας του χρήστη έναντι κακόβουλου κώδικα.

Σχετικά με – Παρέχει πληροφορίες συστήματος, λεπτομέρειες σχετικά με την έκδοση του ESET Internet Security που είναι εγκατεστημένη και τις εγκατεστημένες μονάδες του προγράμματος. Εδώ μπορείτε να βρείτε επίσης την ημερομηνία λήξης της άδειας χρήσης και πληροφορίες για το λειτουργικό σύστημα και τους πόρους του συστήματος.

Υποστήριξη ανάγνωσης οθόνης

Το ESET Internet Security μπορεί να χρησιμοποιηθεί μαζί με προγράμματα ανάγνωσης οθόνης ώστε να επιτρέπεται σε χρήστες της ESET με μειωμένη όραση να πλοηγηθούν στο προϊόν ή να ρυθμίσουν τις παραμέτρους. Υποστηρίζονται τα ακόλουθα προγράμματα ανάγνωσης οθόνης (JAWS, NVDA, Narrator).

Για να διασφαλίσετε ότι το λογισμικό ανάγνωσης οθόνης μπορεί να έχει σωστή πρόσβαση στο γραφικό περιβάλλον χρήστη του ESET Internet Security, ακολουθήστε τις οδηγίες στο άρθρο της Γνωσιακής βάσης.

Βοήθεια και υποστήριξη

Το ESET Internet Security περιέχει εργαλεία επίλυσης προβλημάτων και πληροφορίες υποστήριξης που θα σας βοηθήσουν να επιλύσετε προβλήματα που μπορεί να αντιμετωπίσετε.

Άδεια χρήσης

- **Αντιμετώπιση προβλημάτων αδειών χρήσης** – Κάντε κλικ σε αυτόν τον σύνδεσμο για να βρείτε λύσεις για προβλήματα με την ενεργοποίηση ή την αλλαγή άδειας χρήσης.

- **Αλλαγή άδειας χρήσης** – Κάντε κλικ για να ανοίξετε το παράθυρο ενεργοποίησης και να ενεργοποιήσετε το προϊόν σας. Εάν η συσκευή σας είναι συνδεδεμένη στο ESET HOME, επιλέξτε μια άδεια χρήσης από το λογαριασμό σας στο ESET HOME ή προσθέστε μια νέα.

Εγκατεστημένο προϊόν

- What's New – Κάντε κλικ σε αυτό το στοιχείο για να ανοίξει το παράθυρο πληροφοριών σχετικά με τις νέες και βελτιωμένες δυνατότητες.

- **Σχετικά με το ESET Internet Security** – Εμφανίζει πληροφορίες για το αντίγραφο του ESET Internet Security που χρησιμοποιείτε.

- **Αντιμετώπιση προβλημάτων προϊόντος** - Κάντε κλικ σε αυτόν τον σύνδεσμο για να βρείτε λύσεις στα προβλήματα που προκύπτουν πιο συχνά.

- **Αλλαγή προϊόντος** – Κάντε κλικ για να δείτε εάν μπορείτε να αλλάξετε το ESET Internet Security με μια διαφορετική σειρά προϊόντων με την τρέχουσα άδεια χρήσης.

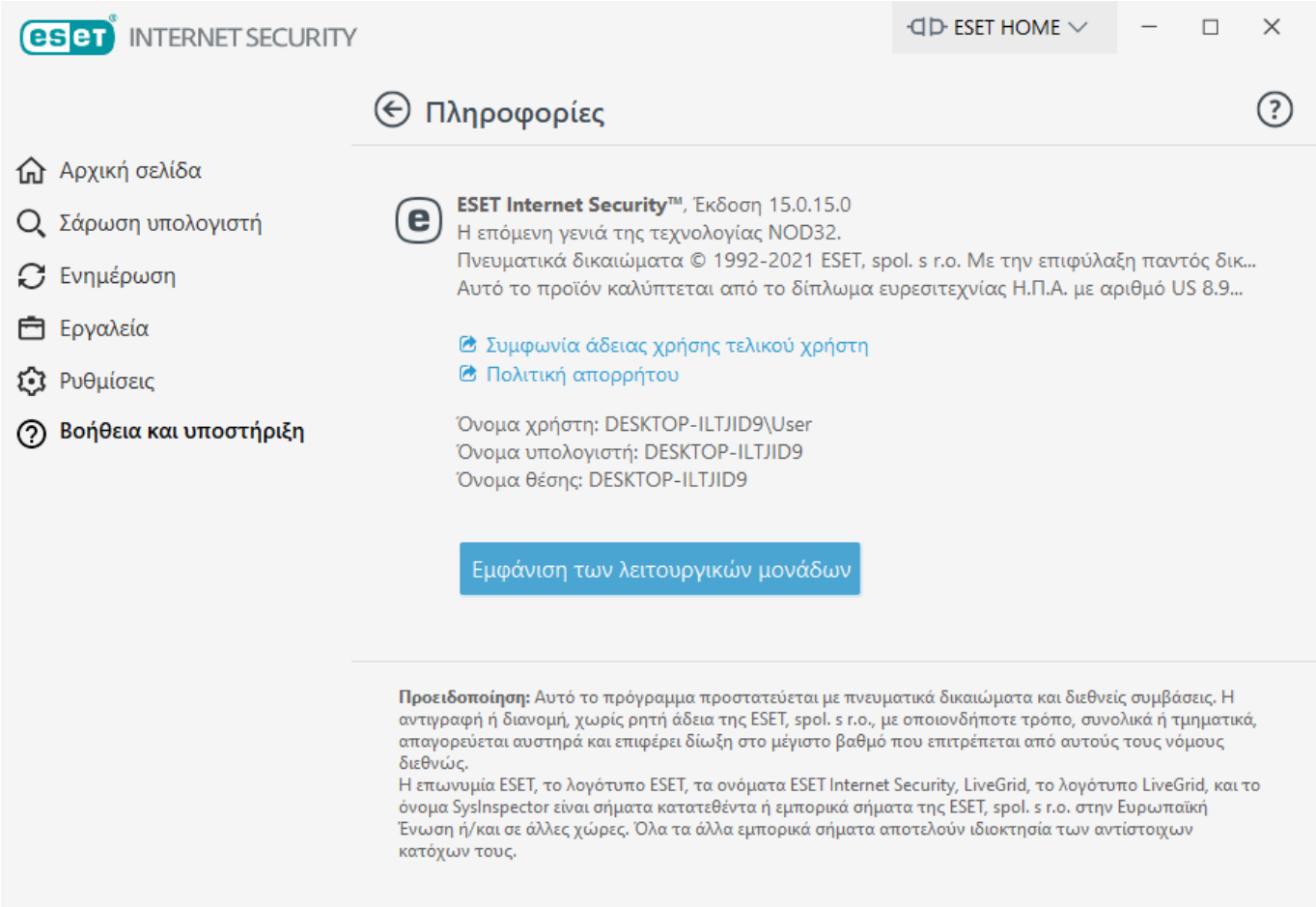
Σελίδα βοήθειας – Κάντε κλικ σε αυτόν το σύνδεσμο για να εκκινήσουν οι σελίδες βοήθειας του ESET Internet Security.

Τεχνική υποστήριξη

Γνωσιακή βάση – Η Γνωσιακή βάση της ESET περιέχει απαντήσεις στις πιο συχνές ερωτήσεις, καθώς και συνιστώμενες λύσεις για διάφορα θέματα. Η Γνωσιακή βάση ενημερώνεται τακτικά από τους ειδικούς τεχνικούς της ESET και είναι το πιο ισχυρό εργαλείο για την επίλυση διαφόρων προβλημάτων.

Σχετικά με το ESET Internet Security

Αυτό το παράθυρο παρέχει λεπτομέρειες σχετικά με την εγκατεστημένη έκδοση του ESET Internet Security και τον υπολογιστή σας.



Κάντε κλικ στο στοιχείο **Εμφάνιση λειτουργικών μονάδων** για να δείτε πληροφορίες σχετικά με τη λίστα των φορτωμένων λειτουργικών μονάδων προγράμματος.

• Μπορείτε να αντιγράψετε στο πρόχειρο πληροφορίες σχετικά με τις λειτουργικές μονάδες κάνοντας κλικ στην επιλογή **Αντιγραφή**. Αυτό μπορεί να είναι χρήσιμο κατά την αντιμετώπιση προβλημάτων ή κατά τη επικοινωνία με την Τεχνική υποστήριξη.

• Κάντε κλικ στο στοιχείο **Μηχανισμός ανίχνευσης** στο παράθυρο «Λειτουργικές μονάδες» για να ανοίξει το Ραντάρ ιών ESET, το οποίο περιέχει πληροφορίες σχετικά με κάθε έκδοση του Μηχανισμού ανίχνευσης ESET.

Νέα από την ESET

Σε αυτό το παράθυρο, το ESET Internet Security σάς ενημερώνει τακτικά σχετικά με τα νέα της ESET.

Η ανταλλαγή μηνυμάτων μέσα από το προϊόν σχεδιάστηκε για να ενημερώνει τους χρήστες σχετικά με τα νέα της ESET και άλλες επικοινωνίες. Η αποστολή μηνυμάτων προώθησης απαιτεί τη συγκατάθεση του χρήστη. Συνεπώς, τα μηνύματα μάρκετινγκ δεν αποστέλλονται στο χρήστη από προεπιλογή (εμφανίζεται ως Λατινικό ερωτηματικό). Εάν ενεργοποιήσετε αυτή την επιλογή, συμφωνείτε να λαμβάνετε μηνύματα προώθησης της ESET. Εάν δεν σας ενδιαφέρει να λαμβάνετε υλικό προώθησης της ESET, απενεργοποιήστε την επιλογή **Εμφάνιση μηνυμάτων προώθησης**.

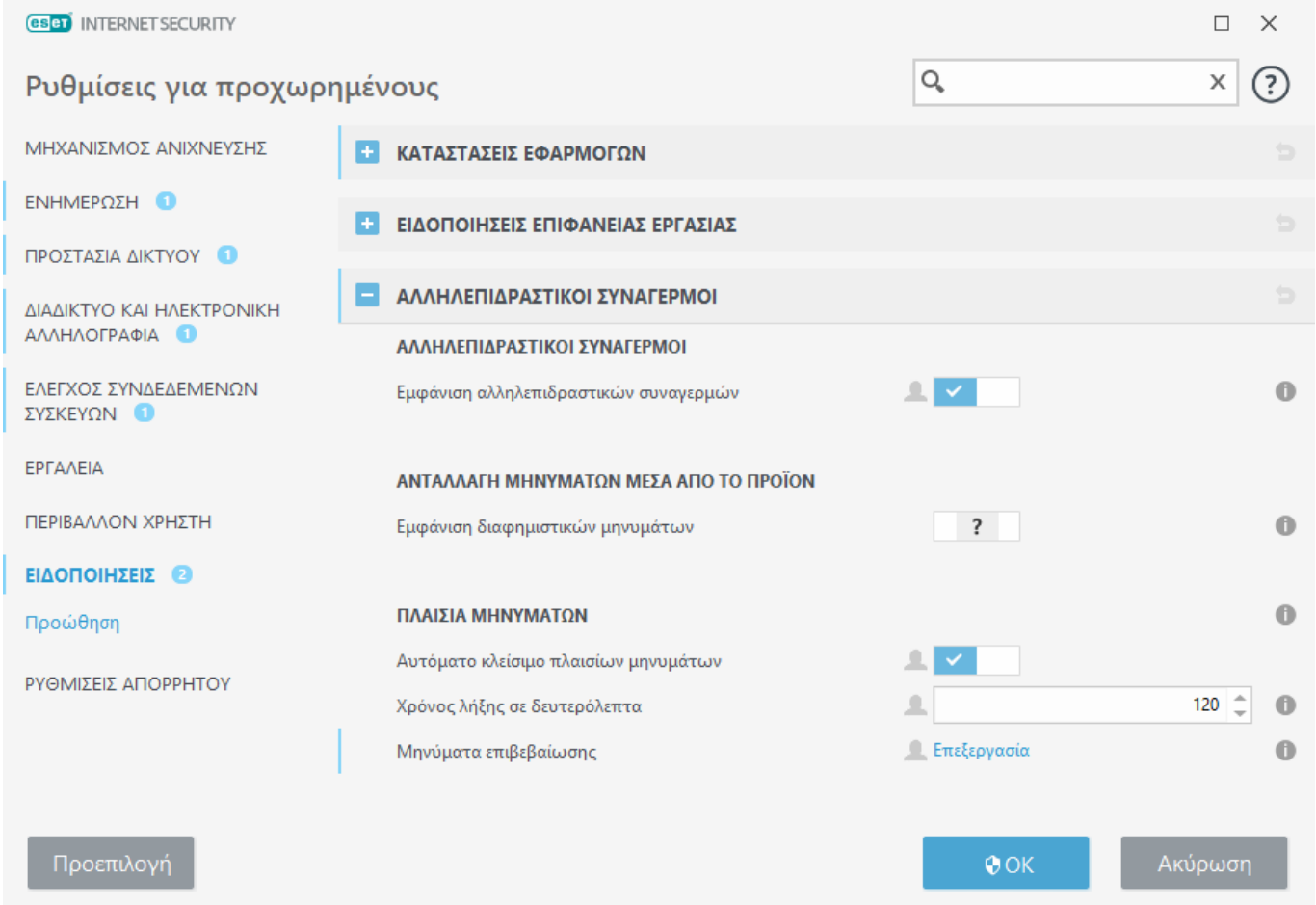
Για να ενεργοποιήσετε ή να απενεργοποιήσετε τη λήψη μηνυμάτων προώθησης μέσω αναδυόμενου παραθύρου, ακολουθήστε τις παρακάτω οδηγίες.

1. Ανοίξτε το κύριο παράθυρο του προϊόντος ESET.

2. Πατήστε το πλήκτρο **F5** για να αποκτήσετε πρόσβαση στο στοιχείο **Εγκατάσταση για προχωρημένους**.

3. Κάντε κλικ στο στοιχείο **Ειδοποιήσεις** > **Αλληλεπιδραστικοί συναγερμοί**.

4. Τροποποιήστε την επιλογή **Εμφάνιση μηνυμάτων προώθησης**.



Υποβολή δεδομένων διαμόρφωσης συστήματος

Προκειμένου να παρέχει όσο το δυνατό πιο γρήγορη και σωστή βοήθεια, η ESET απαιτεί πληροφορίες σχετικά με τη διαμόρφωση του ESET Internet Security, λεπτομερείς πληροφορίες συστήματος και εκτελούμενων διεργασιών (αρχείο καταγραφής ESET SysInspector) και δεδομένα μητρώου. Η ESET θα χρησιμοποιήσει αυτά τα δεδομένα με αποκλειστικό σκοπό να παρέχει τεχνική βοήθεια στον πελάτη.

Κατά την υποβολή της φόρμας διαδικτύου, τα δεδομένα διαμόρφωσης του συστήματός σας υποβάλλονται στην ESET. Επιλέξτε **Να αποστέλλονται πάντοτε αυτές οι πληροφορίες** εάν θέλετε να απομνημονευτεί η ενέργεια για αυτήν τη διαδικασία. Για να υποβάλετε τη φόρμα χωρίς να αποστέλλονται δεδομένα, κάντε κλικ στην επιλογή **Να μην αποστέλλονται δεδομένα** και μπορείτε να επικοινωνήσετε με την Τεχνική υποστήριξη της ESET χρησιμοποιώντας την ηλεκτρονική φόρμα υποστήριξης.

Μπορείτε επίσης να διαμορφώσετε αυτήν τη ρύθμιση στη θέση **Εγκατάσταση για προχωρημένους** > **Εργαλεία** > **Διαγνωστικοί έλεγχοι** > Τεχνική υποστήριξη.

Εάν έχετε αποφασίσει να υποβάλετε δεδομένα συστήματος, απαιτείται να συμπληρώσετε και να υποβάλετε τη φόρμα διαδικτύου, διαφορετικά το αίτημά σας δεν θα δημιουργηθεί και τα δεδομένα συστήματος που υποβάλλετε θα χαθούν.

Τεχνική υποστήριξη

Στο κύριο παράθυρο του προγράμματος, κάντε κλικ στο στοιχείο **Βοήθεια και υποστήριξη** > **Τεχνική υποστήριξη**.

Επικοινωνία με την Τεχνική υποστήριξη

Υποβολή αιτήματος υποστήριξης – Εάν δεν μπορείτε να βρείτε απάντηση στο πρόβλημά σας, μπορείτε να χρησιμοποιήσετε αυτήν τη φόρμα που βρίσκεται στον ιστότοπο της ESET, για να επικοινωνήσετε γρήγορα με το τμήμα Τεχνικής υποστήριξης της ESET. Με βάση τις ρυθμίσεις σας, εμφανίζεται το παράθυρο Υποβολή δεδομένων ρύθμισης παραμέτρων συστήματος πριν από τη συμπλήρωση της διαδικτυακής φόρμας.

Λήψη πληροφοριών για την Τεχνική υποστήριξη

Λεπτομέρειες για την Τεχνική υποστήριξη – Όταν σας ζητηθεί, μπορείτε να αντιγράψετε και να αποστείλετε πληροφορίες στην Τεχνική υποστήριξη της ESET (όπως τα στοιχεία της άδειας χρήσης, το όνομα του προϊόντος, την έκδοση του προϊόντος, το λειτουργικό σύστημα και πληροφορίες του υπολογιστή).

ESET Log Collector – Συνδέεται με το άρθρο της Γνωσιακής βάσης της ESET, όπου μπορείτε να πραγματοποιήσετε λήψη της εφαρμογής ESET Log Collector που συλλέγει αυτόματα πληροφορίες και αρχεία καταγραφής από τον υπολογιστή, προκειμένου να βοηθήσει στην ταχύτερη επίλυση ζητημάτων. Για περισσότερες πληροφορίες, κάντε κλικ στον ηλεκτρονικό οδηγό χρήστη του ESET Log Collector.

Ενεργοποιήστε το στοιχείο **Ενεργοποίηση προηγμένης καταγραφής** για να δημιουργήσετε προηγμένες καταγραφές για όλες τις διαθέσιμες δυνατότητες, ώστε να βοηθήσετε τους προγραμματιστές να διαγνώσουν και να επιλύσουν προβλήματα. Το ελάχιστο επίπεδο λεπτομερειών καταγραφής ρυθμίζεται σε **Διαγνωστικό** επίπεδο. Η προηγμένη καταγραφή θα απενεργοποιείται αυτόματα μετά από δύο ώρες, εκτός εάν τη σταματήσετε νωρίτερα κάνοντας κλικ στο στοιχείο **Διακοπή προηγμένης καταγραφής**. Όταν δημιουργηθούν όλα τα αρχεία καταγραφής, το παράθυρο ειδοποίησης εμφανίζεται και παρέχει άμεση πρόσβαση στο φάκελο «Διαγνωστικός έλεγχος" με τα αρχεία καταγραφής που δημιουργήθηκαν.

Ειδοποιήσεις

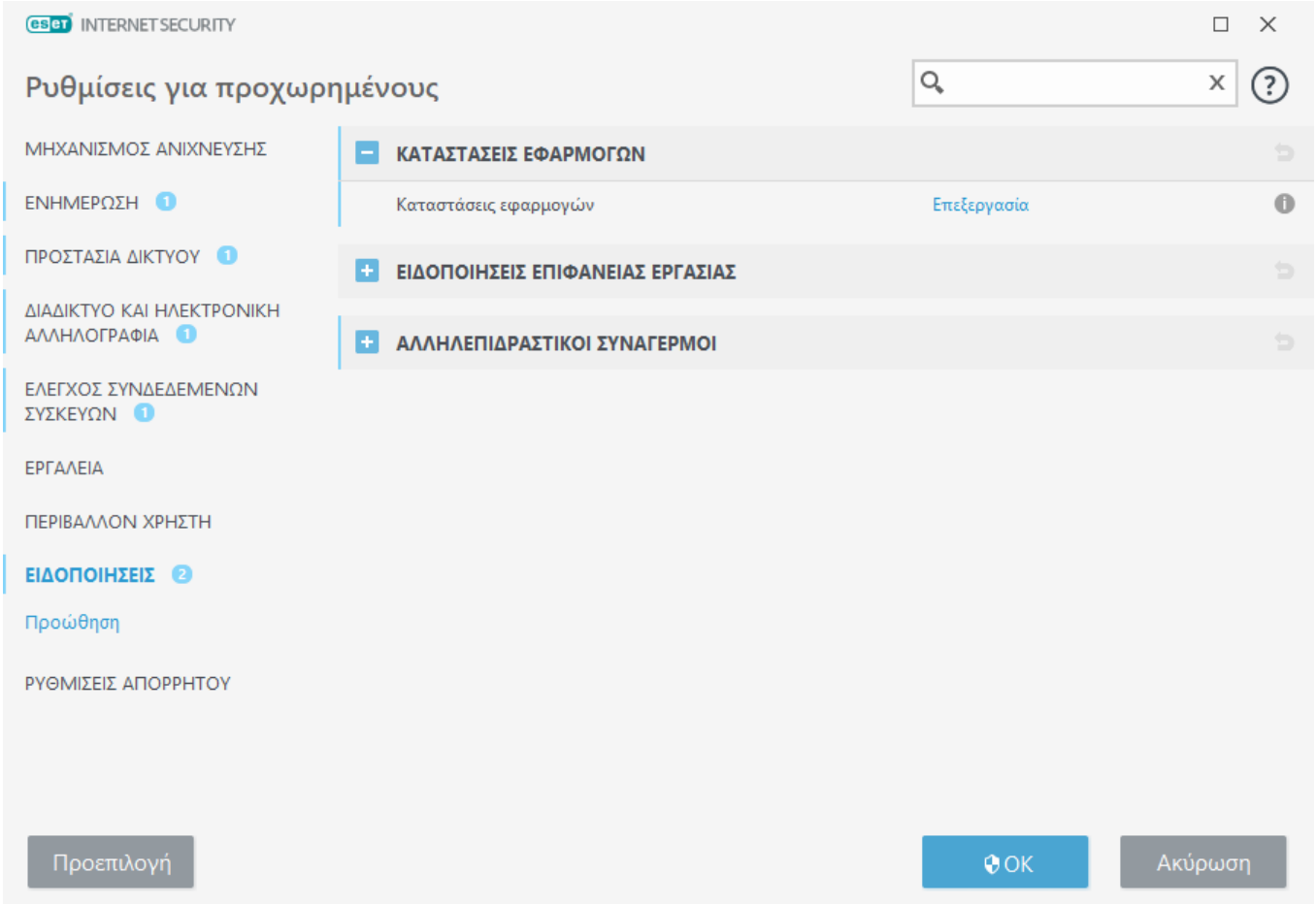
Για να διαχειριστείτε τις ειδοποιήσεις του ESET Internet Security, μεταβείτε στα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5). > **Ειδοποιήσεις** Μπορείτε να ρυθμίσετε τις παραμέτρους των ακόλουθων τύπων ειδοποιήσεων: Μπορείτε να ρυθμίσετε τις παραμέτρους των ακόλουθων τύπων ειδοποιήσεων:

- Καταστάσεις εφαρμογής – Ειδοποιήσεις που εμφανίζονται στην αρχική ενότητα του κύριου παραθύρου του προγράμματος.
- Ειδοποιήσεις επιφάνειας εργασίας – Μικρά αναδυόμενα παράθυρα που βρίσκονται δίπλα στη

γραμμή εργασιών του συστήματος.

• Αλληλεπιδραστικοί συναγερμοί – Παράθυρα συναγερμών και πλαίσια μηνυμάτων που απαιτούν αλληλεπίδραση από τον χρήστη.

• Προώθηση (Ειδοποιήσεις ηλεκτρονικού ταχυδρομείου) – Οι ειδοποιήσεις email αποστέλλονται στην καθορισμένη διεύθυνση email.



Καταστάσεις εφαρμογών

Καταστάσεις εφαρμογής - Κάντε κλικ στο στοιχείο **Επεξεργασία** για να επιλέξετε τις καταστάσεις εφαρμογής που θα εμφανίζονται στην αρχική ενότητα του κύριου παραθύρου προγράμματος.

Παράθυρο διαλόγου - Καταστάσεις εφαρμογής

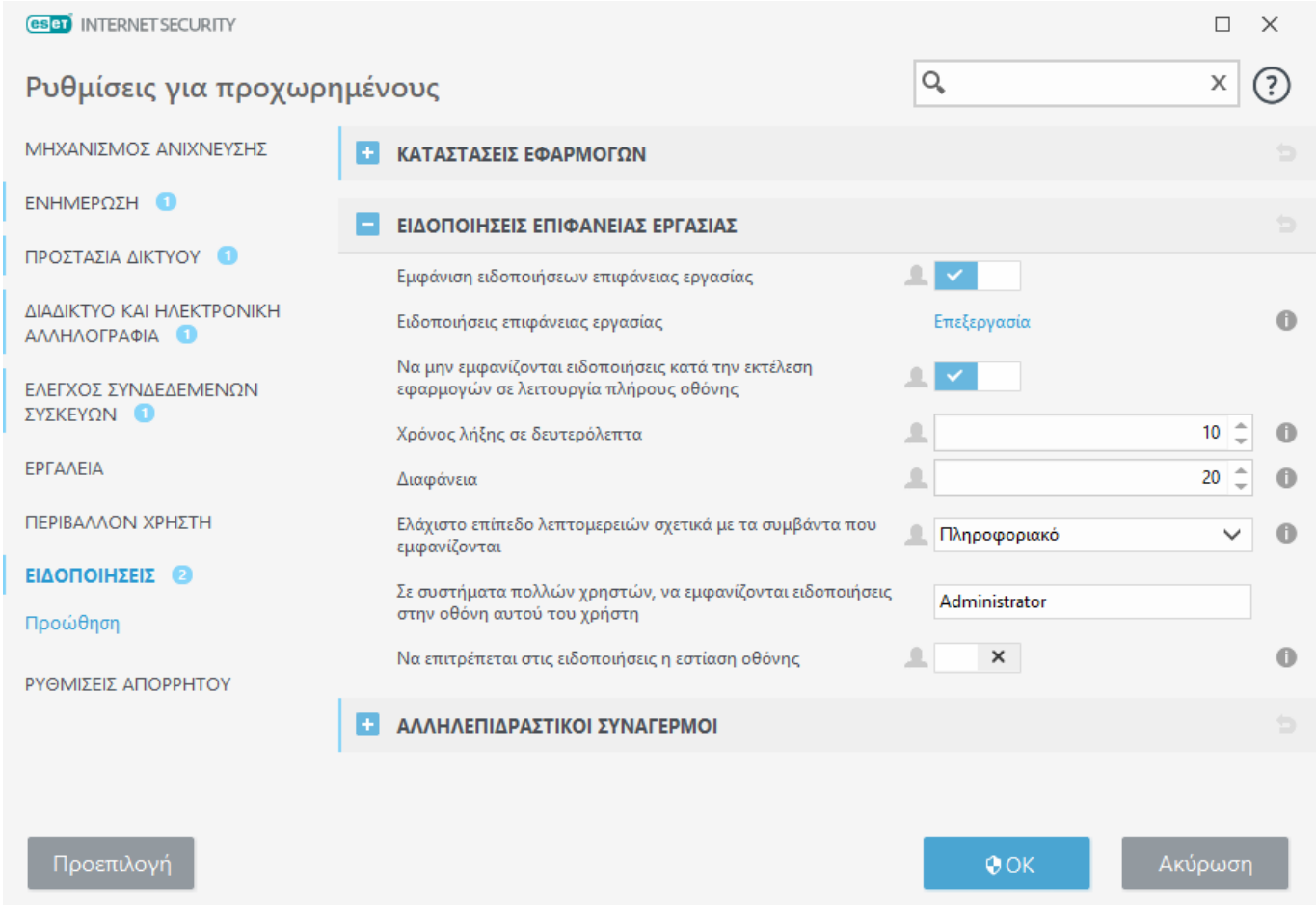
Σε αυτό το παράθυρο διαλόγου, μπορείτε να επιλέξετε τις καταστάσεις εφαρμογής που θα εμφανίζονται. Για παράδειγμα, όταν τίθεται σε παύση η προστασία Antivirus και Antispyware ή ενεργοποιείται η λειτουργία Gamer.

Επίσης, θα εμφανίζεται η κατάσταση εφαρμογής εάν το προϊόν σας δεν έχει ενεργοποιηθεί ή εάν

έληξε η άδεια χρήσης.

Ειδοποιήσεις επιφάνειας εργασίας

Οι ειδοποιήσεις επιφάνειας εργασίας επισημαίνονται από ένα μικρό αναδυόμενο παράθυρο δίπλα στη γραμμή εργασιών του συστήματος. Από προεπιλογή, αυτό εμφανίζεται για 10 δευτερόλεπτα και, στη συνέχεια, εξαφανίζεται αργά. Οι ειδοποιήσεις περιλαμβάνουν επιτυχημένες ενημερώσεις προϊόντων, νέες συσκευές που συνδέονται, ολοκλήρωση εργασιών σάρωσης για ιούς ή νέες απειλές που εντοπίστηκαν.



Εμφάνιση ειδοποιήσεων στην επιφάνεια εργασίας – Συνιστάται να διατηρείτε αυτή την επιλογή ενεργή, έτσι ώστε το προϊόν να μπορεί να σας ειδοποιεί όταν προκύπτει ένα νέο συμβάν.

Ειδοποιήσεις επιφάνειας εργασίας – Κάντε κλικ στο στοιχείο **Επεξεργασία** για να ενεργοποιήσετε ή να απενεργοποιήσετε συγκεκριμένες Ειδοποιήσεις επιφάνειας εργασίας.

Να μην εμφανίζονται ειδοποιήσεις κατά την εκτέλεση εφαρμογών σε λειτουργία πλήρους οθόνης – Καταστέλλονται όλες οι μη αλληλεπιδραστικές ειδοποιήσεις σε λειτουργία πλήρους οθόνης.

Χρόνος λήξης σε δευτερόλεπτα – Ρυθμίστε τη διάρκεια ορατότητας της ειδοποίησης. Η τιμή πρέπει να είναι μεταξύ 3-30 δευτερολέπτων.

Διαφάνεια – Ρυθμίστε το ποσοστό διαφάνειας της ειδοποίησης. Το υποστηριζόμενο εύρος είναι 0 (χωρίς διαφάνεια) έως 80 (πολύ υψηλή διαφάνεια).

Ελάχιστο επίπεδο λεπτομερειών σχετικά με τα συμβάντα που εμφανίζονται – Ρυθμίστε το αρχικό επίπεδο σοβαρότητας των ειδοποιήσεων που θα εμφανίζεται. Από το αναπτυσσόμενο μενού, επιλέξτε μία από τις ακόλουθες επιλογές:

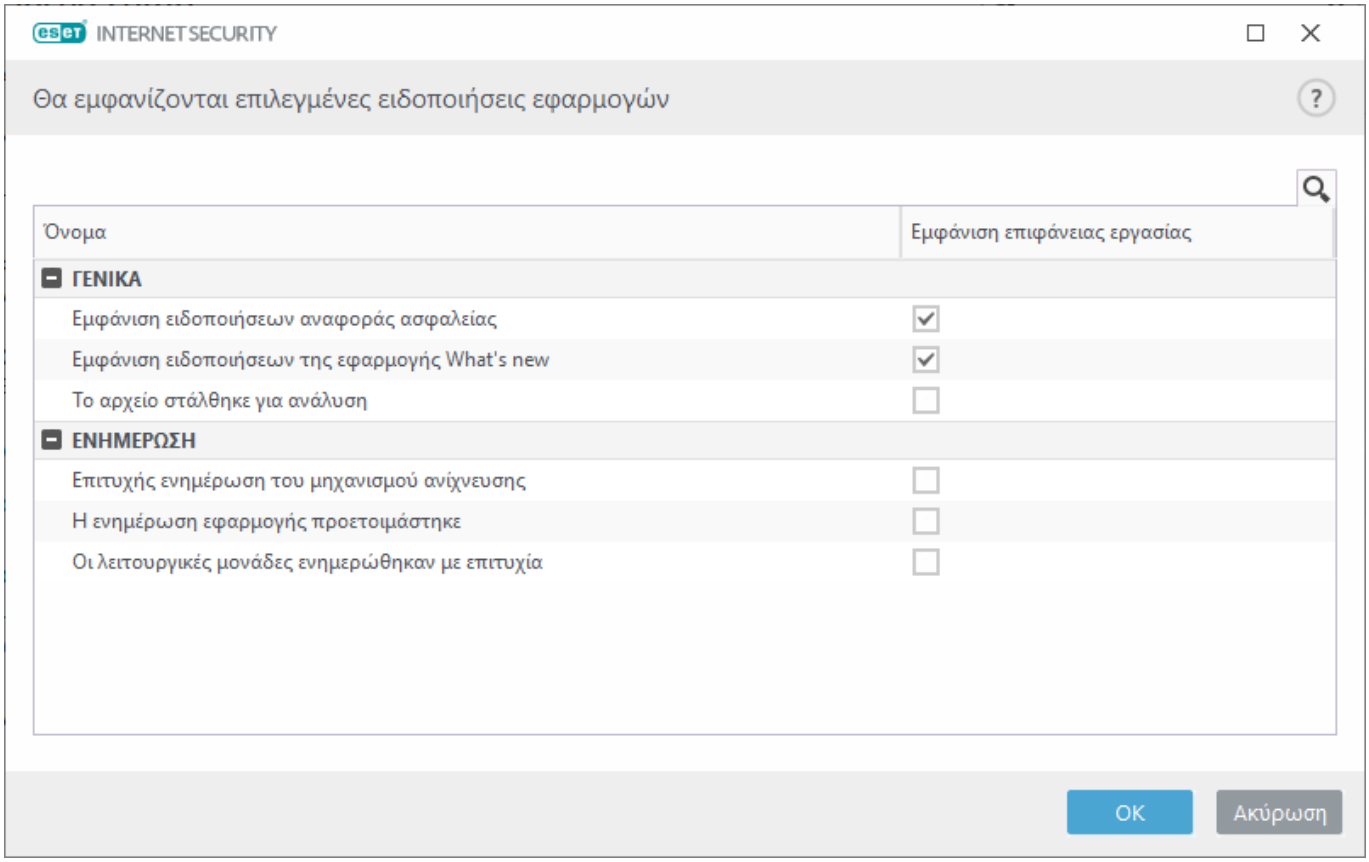
- **Εγγραφές διαγνωστικού ελέγχου** – Εμφανίζει πληροφορίες που είναι απαραίτητες για τη ρύθμιση του προγράμματος και όλες τις παραπάνω εγγραφές.
- **Εγγραφές πληροφοριών** – Εμφανίζει πληροφοριακά μηνύματα, όπως μη τυπικά συμβάντα δικτύου, συμπεριλαμβανομένων μηνυμάτων επιτυχούς ενημέρωσης, καθώς και όλες τις παραπάνω εγγραφές.
- **Προειδοποιήσεις** – Εμφανίζει προειδοποιητικά μηνύματα, σφάλματα και κρίσιμα σφάλματα (για παράδειγμα, το Antistealth δεν εκτελείται σωστά ή η ενημέρωση απέτυχε).
- **Σφάλματα** – Εμφανίζει σφάλματα (για παράδειγμα, η προστασία εγγράφου δεν ξεκίνησε) και κρίσιμα σφάλματα.
- **Κρίσιμες προειδοποιήσεις** – Εμφανίζει μόνο κρίσιμα σφάλματα (σφάλμα κατά την έναρξη της προστασίας Antivirus ή μολυσμένο σύστημα, κ.λπ.).

Σε συστήματα πολλών χρηστών, να εμφανίζονται ειδοποιήσεις στην οθόνη αυτού του χρήστη – Επιτρέπει σε επιλεγμένους λογαριασμούς να λαμβάνουν ειδοποιήσεις επιφάνειας εργασίας. Για παράδειγμα, εάν δεν χρησιμοποιείτε τον λογαριασμό διαχειριστή, πληκτρολογήστε το πλήρες όνομα λογαριασμού και οι ειδοποιήσεις επιφάνειας εργασίας θα εμφανίζονται για τον συγκεκριμένο λογαριασμό. Μόνον ένας λογαριασμός χρήστη μπορεί να λαμβάνει τις ειδοποιήσεις επιφάνειας εργασίας.

Να επιτρέπεται στις ειδοποιήσεις να εστιάζουν στην οθόνη – Επιτρέπει στις ειδοποιήσεις να εστιάζουν στην οθόνη και να είναι προσπελάσιμες από το μενού **ALT + Tab**.

Λίστα ειδοποιήσεων επιφάνειας εργασίας

Για να προσαρμόσετε την ορατότητα των ειδοποιήσεων επιφάνειας εργασίας (που εμφανίζονται κάτω δεξιά στην οθόνη), μεταβείτε στα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5), **Ειδοποιήσεις** > **Ειδοποιήσεις επιφάνειας εργασίας**. Κάντε κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Ειδοποιήσεις επιφάνειας εργασίας** και επιλέξτε το κατάλληλο πλαίσιο ελέγχου **Εμφάνιση**.



Γενικά

Εμφάνιση ειδοποιήσεων αναφοράς ασφαλείας – Θα λαμβάνετε μια ειδοποίηση όταν δημιουργείται μια νέα Αναφορά ασφαλείας.

Εμφάνιση ειδοποιήσεων της εφαρμογής What's new – Ειδοποιήσεις για όλες τις νέες και βελτιωμένες δυνατότητες της πιο πρόσφατης έκδοσης του προϊόντος.

Το αρχείο στάλθηκε για ανάλυση - Θα λαμβάνετε μια ειδοποίηση κάθε φορά που το ESET Internet Security θα στέλνει ένα αρχείο για ανάλυση.

Ενημέρωση

Η ενημέρωση εφαρμογής είναι έτοιμη – Θα λαμβάνετε μια ειδοποίηση όταν θα είναι έτοιμη ενημέρωση για μια νέα έκδοση του ESET Internet Security.

Ο Μηχανισμός ανίχνευσης ενημερώθηκε με επιτυχία - Θα λαμβάνετε μια ειδοποίηση όταν το προϊόν ενημερώνει τις λειτουργικές μονάδες του Μηχανισμού ανίχνευσης.

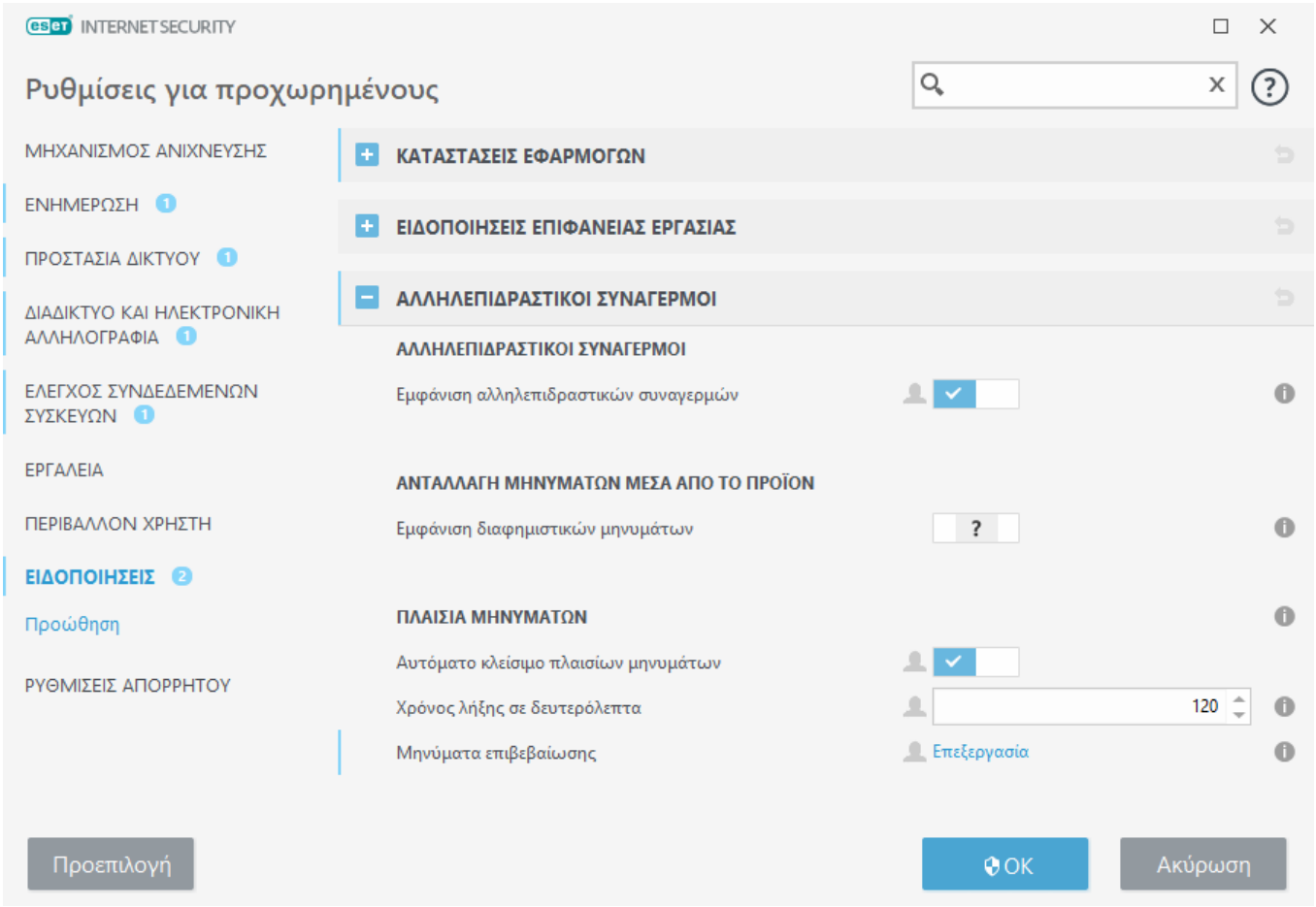
Οι λειτουργικές μονάδες ενημερώθηκαν με επιτυχία - Θα λαμβάνετε μια ειδοποίηση όταν το προϊόν ενημερώνει τα στοιχεία του προγράμματος.

Για να ορίσετε γενικές ρυθμίσεις για τις Ειδοποιήσεις επιφάνειας εργασίας, για παράδειγμα, για πόσο χρονικό διάστημα θα εμφανίζεται το μήνυμα ή το ελάχιστο επίπεδο λεπτομερειών των συμβάντων που θα εμφανίζεται, δείτε τις Ειδοποιήσεις επιφάνειας εργασίας στη διαδρομή **Εγκατάσταση για προχωρημένους** (F5) > **Ειδοποιήσεις**.

Αλληλεπιδραστικοί συναγερμοί

Αναζητάτε πληροφορίες για συνήθεις συναγερμούς και ειδοποιήσεις;
- Εντοπίστηκε απειλή
- Η διεύθυνση έχει αποκλειστεί
- Το προϊόν δεν έχει ενεργοποιηθεί
- Αλλαγή σε προϊόν με περισσότερες δυνατότητες
- Αλλαγή σε προϊόν με λιγότερες δυνατότητες
- Υπάρχει διαθέσιμη ενημέρωση
- Οι πληροφορίες ενημέρωσης δεν είναι συνεπείς
- Αντιμετώπιση προβλημάτων με το μήνυμα «Αποτυχία ενημέρωσης των λειτουργικών μονάδων»
- Επίλυση σφαλμάτων ενημέρωσης λειτουργικών μονάδων
- Αποκλείστηκε απειλή δικτύου
- Ανάκληση πιστοποιητικού ιστότοπου

Η ενότητα **Αλληλεπιδραστικοί συναγερμοί** στη διαδρομή **Ρυθμίσεις για προχωρημένους** (F5) > **Ειδοποιήσεις** σάς επιτρέπει να ρυθμίσετε τις παραμέτρους για τον χειρισμό των πλαισίων μηνυμάτων και των αλληλεπιδραστικών συναγερμών για ανιχνεύσεις, όπου απαιτείται απόφαση από έναν χρήστη (για παράδειγμα, ενδεχόμενος ιστότοπος phishing), από το ESET Internet Security.



Αλληλεπιδραστικοί συναγερμοί

Η απενεργοποίηση του στοιχείου **Εμφάνιση αλληλεπιδραστικών συναγερμών** αποκρύπτει όλα τα παράθυρα συναγερμών και τα πλαίσια διαλόγου εντός του προγράμματος περιήγησης, και είναι κατάλληλη μόνο για περιορισμένο αριθμό ειδικών καταστάσεων. Η ESET συνιστά αυτή η επιλογή να

παραμένει ενεργοποιημένη.

Ανταλλαγή μηνυμάτων μέσα από το προϊόν

Η ανταλλαγή μηνυμάτων μέσα από το προϊόν σχεδιάστηκε για να ενημερώνει τους χρήστες σχετικά με τα νέα της ESET και άλλες επικοινωνίες. Η αποστολή μηνυμάτων προώθησης απαιτεί τη συγκατάθεση του χρήστη. Συνεπώς, τα μηνύματα μάρκετινγκ δεν αποστέλλονται στο χρήστη από προεπιλογή (εμφανίζεται ως Λατινικό ερωτηματικό). Εάν ενεργοποιήσετε αυτή την επιλογή, συμφωνείτε να λαμβάνετε μηνύματα προώθησης της ESET. Εάν δεν σας ενδιαφέρει να λαμβάνετε υλικό προώθησης της ESET, απενεργοποιήστε την επιλογή **Εμφάνιση μηνυμάτων προώθησης**.

Πλαίσια μηνυμάτων

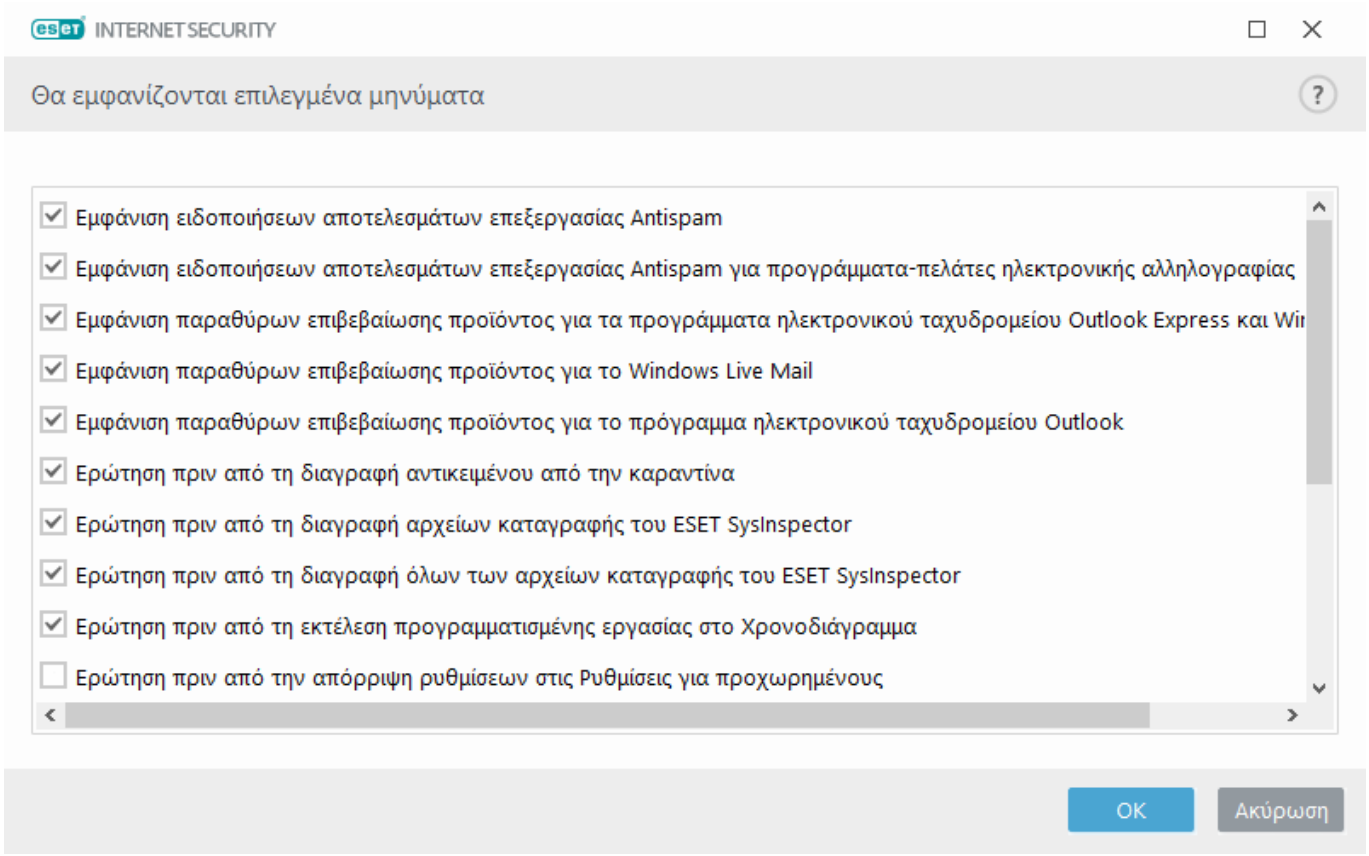
Για να κλείνουν αυτόματα τα πλαίσια μηνυμάτων μετά από συγκεκριμένο χρονικό διάστημα, επιλέξτε **Αυτόματο κλείσιμο πλαισίων μηνυμάτων**. Εάν δεν κλείσουν μη αυτόματα, τα παράθυρα συναγερμών κλείνουν αυτόματα μετά από την πάροδο του καθορισμένου χρονικού διαστήματος.

Χρόνος λήξης σε δευτερόλεπτα – Ρυθμίζει τη διάρκεια ορατότητας του συναγερμού. Η τιμή πρέπει να είναι μεταξύ 10-999 δευτερόλεπτα.

Μηνύματα επιβεβαίωσης – Κάντε κλικ στο στοιχείο **Επεξεργασία** για να εμφανιστεί μια λίστα μηνυμάτων επιβεβαίωσης για τα οποία μπορείτε να επιλέξετε εάν θα εμφανίζονται ή όχι.

Μηνύματα επιβεβαίωσης

Για να προσαρμόσετε τα μηνύματα επιβεβαίωσης, μεταβείτε στα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5) > **Ειδοποιήσεις** > **Αλληλεπιδραστικοί συναγερμοί** και κάντε κλικ στο στοιχείο **Επεξεργασία** που βρίσκεται δίπλα στο στοιχείο **Μηνύματα επιβεβαίωσης**.



Αυτό το παράθυρο εμφανίζει μηνύματα επιβεβαίωσης που το ESET Internet Security θα εμφανίζει πριν από την πραγματοποίηση κάθε ενέργειας. Επιλέξτε ή καταργήστε την επιλογή του πλαισίου ελέγχου δίπλα σε κάθε μήνυμα επιβεβαίωσης, για να επιτρέψετε ή να απενεργοποιήσετε την εμφάνιση του αντίστοιχου μηνύματος.

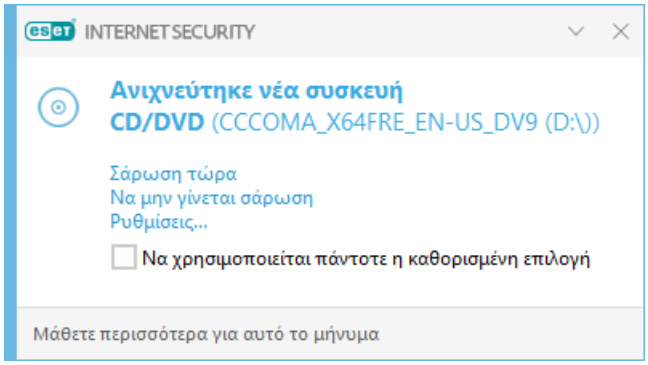
Μάθετε περισσότερα σχετικά με τη συγκεκριμένη δυνατότητα που σχετίζεται με τα μηνύματα επιβεβαίωσης:

- Ερώτηση πριν από τη διαγραφή αρχείων καταγραφής του ESET SysInspector
- Ερώτηση πριν από τη διαγραφή όλων των αρχείων καταγραφής του ESET SysInspector
- Ερώτηση πριν από τη διαγραφή αντικειμένου από την καραντίνα
- Ερώτηση πριν από την απόρριψη ρυθμίσεων στις Ρυθμίσεις για προχωρημένους
- Ερώτηση πριν το κλείσιμο ενός παραθύρου συναγερμού μην έχοντας καθαρίσει όλες τις ανιχνευμένες απειλές
- Ερώτηση πριν από την κατάργηση μιας εγγραφής από αρχείο καταγραφής
- Ερώτηση πριν από την κατάργηση προγραμματισμένης εργασίας στο Χρονοδιάγραμμα
- Ερώτηση πριν από την κατάργηση όλων των εγγραφών του αρχείου καταγραφής
- Ερώτηση πριν από την επαναφορά των στατιστικών
- Ερώτηση πριν από την επαναφορά αντικειμένου από την καραντίνα
- Ερώτηση πριν από την επαναφορά αντικειμένων από την καραντίνα και την εξαίρεσή τους από τη σάρωση
- Ερώτηση πριν από τη εκτέλεση προγραμματισμένης εργασίας στο Χρονοδιάγραμμα
- Εμφάνιση ειδοποιήσεων αποτελεσμάτων επεξεργασίας Antispam
- Εμφάνιση ειδοποιήσεων αποτελεσμάτων επεξεργασίας Antispam για προγράμματα-πελάτες ηλεκτρονικής αλληλογραφίας
- Εμφάνιση παραθύρων επιβεβαίωσης προϊόντος για τα προγράμματα ηλεκτρονικού ταχυδρομείου Outlook Express και Windows Mail
- Εμφάνιση παραθύρων επιβεβαίωσης προϊόντος για το Windows Live Mail
- Εμφάνιση παραθύρων επιβεβαίωσης προϊόντος για το πρόγραμμα ηλεκτρονικού ταχυδρομείου Outlook

Αφαιρούμενα μέσα

Το ESET Internet Security παρέχει αυτόματη σάρωση αφαιρούμενων μέσων (CD/DVD/USB/...) κατά την εισαγωγή σε έναν υπολογιστή. Αυτό μπορεί να είναι χρήσιμο αν ο διαχειριστής του υπολογιστή θέλει να εμποδίζει τους χρήστες να χρησιμοποιούν αφαιρούμενα μέσα με ανεπιθύμητο περιεχόμενο.

Όταν εισάγετε ένα αφαιρούμενο μέσο και η επιλογή **Εμφάνιση επιλογών σάρωσης** έχει οριστεί στο ESET Internet Security, εμφανίζεται το παρακάτω παράθυρο διαλόγου:



Επιλογές για αυτό το παράθυρο διαλόγου:

- **Σάρωση τώρα** – Θα ξεκινήσει η σάρωση του αφαιρούμενου μέσου.
- **Να μη γίνεται σάρωση** – Τα αφαιρούμενα μέσα δεν θα σαρωθούν.
- **Ρυθμίσεις** – Ανοίγει την ενότητα **Εγκατάσταση για προχωρημένους**.
- **Να χρησιμοποιείται πάντοτε η καθορισμένη επιλογή** – Όταν επιλέγετε αυτό το στοιχείο, θα πραγματοποιείται η ίδια ενέργεια κάθε φορά που εισάγεται ένα αφαιρούμενο μέσο.

Επιπλέον, το ESET Internet Security διαθέτει τη λειτουργικότητα "Έλεγχος συνδεδεμένων συσκευών", η οποία σάς επιτρέπει να καθορίζετε κανόνες για τη χρήση εξωτερικών συσκευών σε έναν υπολογιστή. Περισσότερες λεπτομέρειες για τον Έλεγχο συνδεδεμένων συσκευών μπορείτε να βρείτε στην ενότητα Έλεγχος συνδεδεμένων συσκευών.

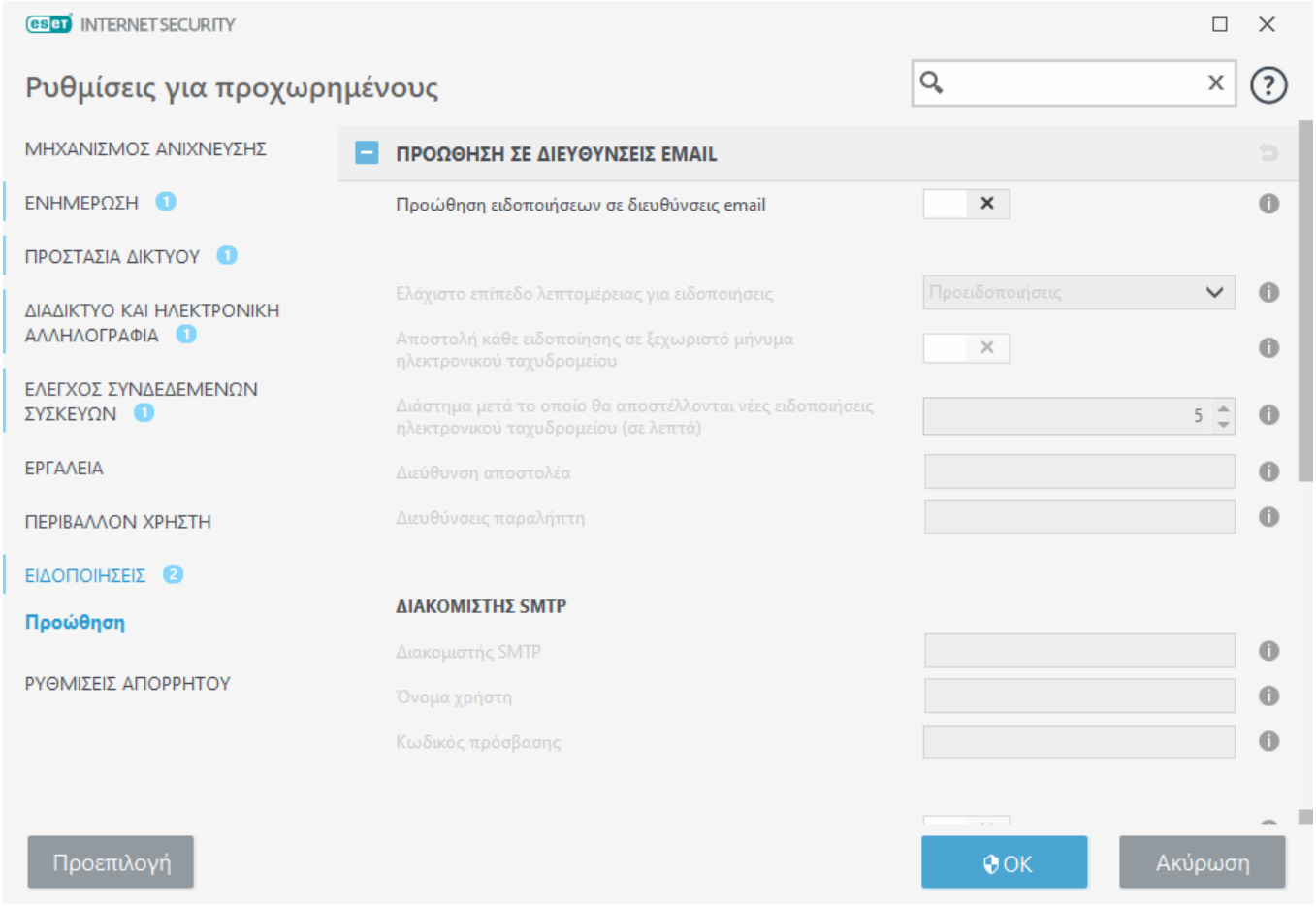
Για να αποκτήσετε πρόσβαση στις ρυθμίσεις για σάρωση αφαιρούμενων μέσων, μεταβείτε στη διαδρομή Εγκατάσταση για προχωρημένους (**F5**) > **Μηχανισμός ανίχνευσης** > **Σαρώσεις για κακόβουλο λογισμικό** > **Αφαιρούμενα μέσα**.

Ενέργεια μετά την εισαγωγή αφαιρούμενων μέσων – Επιλέξτε την προεπιλεγμένη ενέργεια που θα εκτελείται όταν εισάγεται στον υπολογιστή μια συσκευή αφαιρούμενου μέσου (CD/DVD/USB). Επιλέξτε την ενέργεια που θέλετε κατά την εισαγωγή ενός αφαιρούμενου μέσου σε έναν υπολογιστή:

- **Να μη γίνεται σάρωση** – Δεν θα εκτελείται καμιά ενέργεια και το παράθυρο **Ανιχνεύτηκε νέα συσκευή** δεν θα ανοίγει.
- **Αυτόματη σάρωση συσκευών** – Θα εκτελείται σάρωση υπολογιστή των αφαιρούμενων μέσων που έχουν εισαχθεί.
- **Εμφάνιση επιλογών σάρωσης** – Ανοίγει την ενότητα με τις ρυθμίσεις **αφαιρούμενων μέσων**.

Προώθηση

Το ESET Internet Security μπορεί να αποστέλλει αυτόματα ειδοποιήσεις μέσω email, εάν προκύψει κάποιο συμβάν με το επιλεγμένο επίπεδο λεπτομερειών. Μεταβείτε στα στοιχεία **Ρυθμίσεις για προχωρημένους** (F5) > **Ειδοποιήσεις** > **Προώθηση** και ενεργοποιήστε το στοιχείο **Προώθηση ειδοποιήσεων σε διευθύνσεις email** για να ενεργοποιήσετε την αποστολή ειδοποιήσεων μέσω email.



Από το αναπτυσσόμενο μενού **Ελάχιστο επίπεδο λεπτομέρειας για ειδοποιήσεις**, μπορείτε να επιλέξετε το αρχικό επίπεδο σοβαρότητας των συναγερμών που θα αποστέλλονται.

- **Εγγραφές διαγνωστικού ελέγχου** – Καταγράφει πληροφορίες απαραίτητες για τη ρύθμιση του προγράμματος και όλες τις παραπάνω εγγραφές.

- **Εγγραφές πληροφοριών** – Καταγράφει πληροφοριακά μηνύματα όπως μη τυπικά συμβάντα δικτύου, συμπεριλαμβανομένων μηνυμάτων επιτυχούς ενημέρωσης, καθώς και όλες τις παραπάνω εγγραφές.

- **Προειδοποιήσεις** – Καταγράφει κρίσιμα σφάλματα και προειδοποιητικά μηνύματα (π.χ. το Anti-Stealth δεν λειτουργεί σωστά ή η ενημέρωση απέτυχε).

- **Σφάλματα** – Καταγράφονται σφάλματα (η Προστασία εγγράφων δεν ξεκίνησε) και κρίσιμα σφάλματα.

- **Κρίσιμες προειδοποιήσεις** – Καταγράφει μόνο κρίσιμα σφάλματα (για παράδειγμα, Σφάλμα κατά την εκκίνηση της προστασίας Antivirus ή Βρέθηκε απειλή).

Αποστολή κάθε ειδοποίησης σε ξεχωριστό email – Εάν ενεργοποιηθεί αυτή η επιλογή, ο παραλήπτης θα λαμβάνει νέο email για κάθε ειδοποίηση. Αυτό ενδέχεται να έχει ως αποτέλεσμα ο παραλήπτης να λαμβάνει πολλά email σε σύντομο χρονικό διάστημα.

Διάστημα μετά το οποίο θα αποστέλλονται νέες ειδοποιήσεις ηλεκτρονικού ταχυδρομείου (σε λεπτά) – Διάστημα (σε λεπτά) μετά το οποίο θα αποστέλλονται νέες ειδοποιήσεις στη διεύθυνση ηλεκτρονικού ταχυδρομείου. Εάν ρυθμίσετε αυτή την τιμή σε 0, οι ειδοποιήσεις θα αποστέλλονται αμέσως.

Διεύθυνση αποστολέα – Καθορίστε τη διεύθυνση του αποστολέα που θα εμφανίζεται στην κεφαλίδα των μηνυμάτων ειδοποίησης.

Διευθύνσεις παραληπτών – Καθορίστε τις διευθύνσεις παραληπτών που θα εμφανίζονται στην κεφαλίδα των email ειδοποίησης. Υποστηρίζονται πολλαπλές τιμές. Χρησιμοποιήστε το ερωτηματικό ως διαχωριστικό.

διακομιστής SMTP

Διακομιστής **SMTP** – Ο διακομιστής SMTP που χρησιμοποιείται για την αποστολή ειδοποιήσεων (για παράδειγμα, για το smtp.provider.com:587, η προκαθορισμένη θύρα είναι 25).

οι διακομιστές SMTP με κρυπτογράφηση TLS υποστηρίζονται από το ESET Internet Security.

Όνομα χρήστη και **κωδικός πρόσβασης** – Εάν ο διακομιστής SMTP απαιτεί έλεγχο ταυτότητας, αυτά τα πεδία πρέπει να συμπληρώνονται με έγκυρο όνομα χρήστη και κωδικό πρόσβασης για την πρόσβαση στο διακομιστή SMTP.

Ενεργοποίηση TLS – Secure Alert και ειδοποιήσεις με χρήση κρυπτογράφησης TLS.

Δοκιμή σύνδεσης SMTP – Ένα δοκιμαστικό email θα σταλεί στη διεύθυνση email του παραλήπτη. Πρέπει να συμπληρωθεί ο διακομιστής SMTP, το όνομα χρήστη, ο κωδικός πρόσβασης, η διεύθυνση του αποστολέα και η διεύθυνση του παραλήπτη.

Μορφή μηνύματος

Οι επικοινωνίες μεταξύ του προγράμματος και ενός απομακρυσμένου χρήστη ή διαχειριστή συστήματος εκτελούνται μέσω email ή μηνυμάτων LAN (χρησιμοποιώντας την υπηρεσία ανταλλαγής μηνυμάτων των Windows). Το στοιχείο **Χρήση προεπιλεγμένης μορφής μηνύματος** για τα μηνύματα συναγερμού και ειδοποιήσεων θα είναι βέλτιστη για τις περισσότερες καταστάσεις. Σε ορισμένες περιπτώσεις, ενδέχεται να χρειαστεί να αλλάξετε τη μορφή μηνύματος των μηνυμάτων συμβάντων.

Μορφή μηνυμάτων συμβάντων – Η μορφή των μηνυμάτων συμβάντων που εμφανίζονται σε απομακρυσμένους υπολογιστές.

Μορφή προειδοποιητικών μηνυμάτων απειλών – Τα μηνύματα συναγερμού και ειδοποίησης έχουν προκαθορισμένη προεπιλεγμένη μορφή. Η ESET συνιστά να διατηρήσετε την προκαθορισμένη μορφή. Ωστόσο, υπό ορισμένες συνθήκες (για παράδειγμα, εάν έχετε αυτοματοποιημένο σύστημα επεξεργασίας email), μπορεί να χρειαστεί να αλλάξετε τη μορφή μηνύματος.

Σύνολο χαρακτήρων – Μετατρέπει ένα μήνυμα email στην κωδικοποίηση χαρακτήρων ANSI βάσει

των τοπικών ρυθμίσεων των Windows (π.χ. windows-1250, Unicode (UTF-8), ACSII 7-bit ή Ιαπωνικά (ISO-2022-JP)). Ως αποτέλεσμα, το "á" θα αλλάξει σε "a" και ένα άγνωστο σύμβολο σε "?").

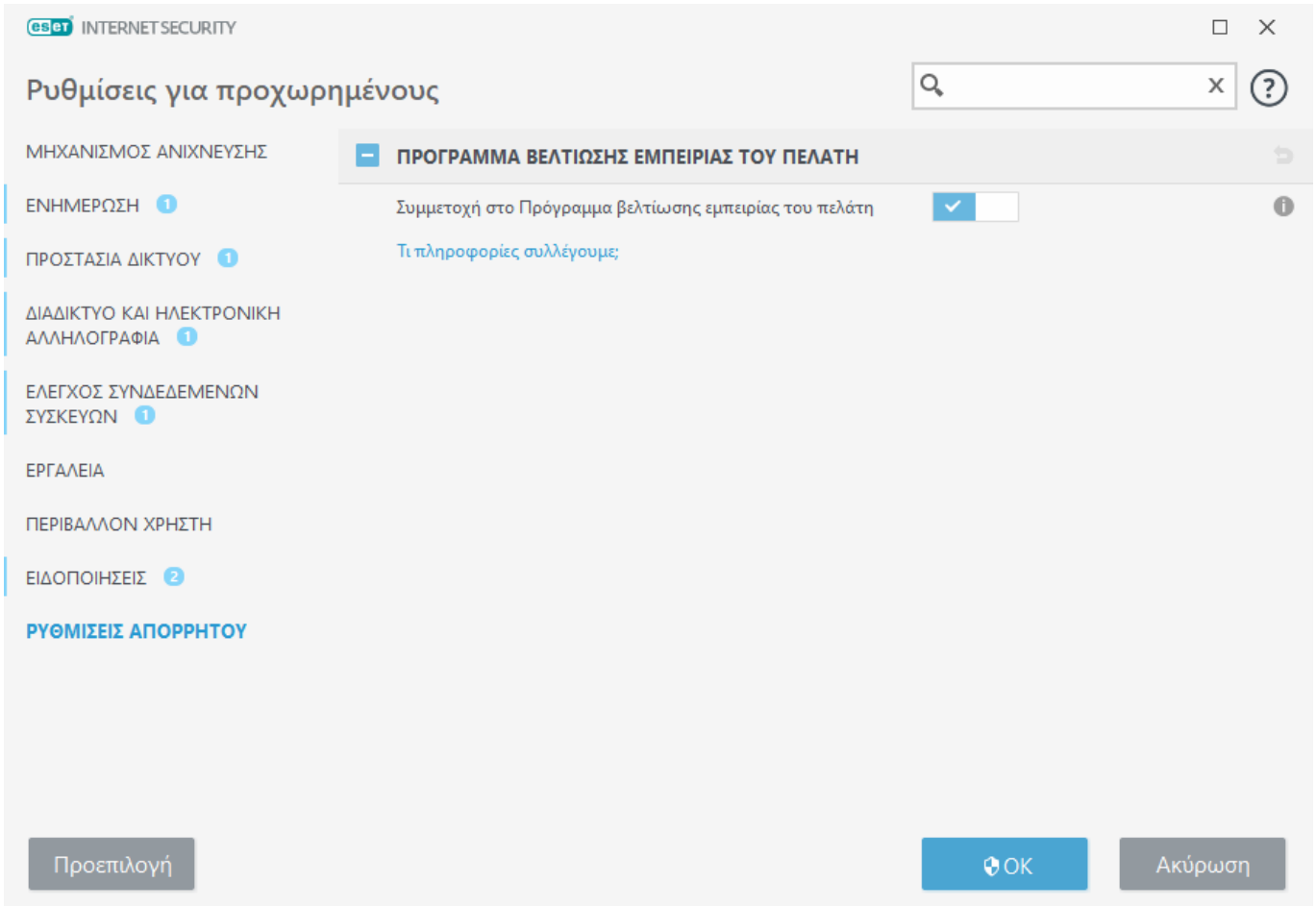
Χρήση κωδικοποίησης εκτυπώσιμης μορφής – Η προέλευση του μηνύματος ηλεκτρονικής αλληλογραφίας θα κωδικοποιηθεί με εκτυπώσιμη μορφή (QP), η οποία χρησιμοποιεί χαρακτήρες ASCII και μπορεί να μεταδώσει σωστά ειδικούς τοπικούς χαρακτήρες μέσω ηλεκτρονικής αλληλογραφίας σε μορφή 8-bit (áéíóú).

- **%TimeStamp%** – Ημερομηνία και ώρα του συμβάντος
- **%Scanner%** – Η σχετική μονάδα
- **%ComputerName%** – Όνομα του υπολογιστή όπου προέκυψε ο συναγερμός
- **%ProgramName%** – Πρόγραμμα που δημιούργησε το συναγερμό
- **%InfectedObject%** – Όνομα του μολυσμένου αρχείου, μηνύματος κ.λπ.
- **%VirusName%** – Αναγνώριση της μόλυνσης
- **%Action%** – Ενέργεια που λαμβάνεται για την εισβολή
- **%ErrorDescription%** – Περιγραφή συμβάντος που δεν σχετίζεται με ιό

Οι λέξεις-κλειδιά keywords **%InfectedObject%** και **%VirusName%** χρησιμοποιούνται μόνο σε μηνύματα προειδοποίησης απειλής, ενώ η λέξη-κλειδί **%ErrorDescription%** χρησιμοποιείται μόνο σε μηνύματα συμβάντος.

Ρυθμίσεις απορρήτου

Στο παράθυρο του κύριου προγράμματος, κάντε κλικ στα στοιχεία **Ρυθμίσεις** > **Ρυθμίσεις για προχωρημένους** (F5) > **Ρυθμίσεις απορρήτου**.



Πρόγραμμα βελτίωσης εμπειρίας του πελάτη

Ενεργοποιήστε το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Συμμετοχή στο Πρόγραμμα βελτίωσης εμπειρίας του πελάτη** για να συμμετάσχετε στο Πρόγραμμα βελτίωσης εμπειρίας του πελάτη. Με τη συμμετοχή σας παρέχετε στην ESET ανώνυμες πληροφορίες σχετικά με τη χρήση των προϊόντων της ESET. Τα δεδομένα που συλλέγονται θα βοηθήσουν την εταιρεία να βελτιώσει την εμπειρία σας και δεν θα κοινοποιηθούν ποτέ σε τρίτους. Τι πληροφορίες συλλέγουμε;

Προφίλ

Η Διαχείριση προφίλ χρησιμοποιείται σε δύο σημεία στο ESET Internet Security – στην ενότητα **Σάρωση υπολογιστή κατ' απαίτηση** και στην ενότητα **Ενημέρωση**.

Σάρωση υπολογιστή

Υπάρχουν 4 προκαθορισμένα προφίλ σάρωσης στο ESET Internet Security:

- **Έξυπνη σάρωση** – Αυτό είναι το προεπιλεγμένο προφίλ σάρωσης για προχωρημένους. Το προφίλ έξυπνης σάρωσης χρησιμοποιεί τεχνολογία Έξυπνης βελτιστοποίησης, η οποία εξαιρεί αρχεία που βρέθηκαν καθαρά σε προηγούμενη σάρωση και δεν έχουν τροποποιηθεί μετά από αυτή τη σάρωση. Αυτό επιτρέπει μικρότερους χρόνους σάρωσης με ελάχιστη επίπτωση στην ασφάλεια του συστήματος.

- **Σάρωση μενού περιβάλλοντος** – Μπορείτε να ξεκινήσετε μια σάρωση κατ' απαίτηση οποιουδήποτε αρχείου από το μενού περιβάλλοντος. Το προφίλ Σάρωσης μενού περιβάλλοντος

σάς επιτρέπει να ορίσετε μια ρύθμιση παραμέτρων σάρωσης που θα χρησιμοποιείται όταν θα ενεργοποιείτε τη σάρωση με αυτόν τον τρόπο.

• **Σάρωση σε βάθος** – Το προφίλ Σάρωσης σε βάθος δεν χρησιμοποιεί έξυπνη βελτιστοποίηση από προεπιλογή, συνεπώς δεν εξαιρείται κανένα αρχείο από τη σάρωση όταν χρησιμοποιείται αυτό το προφίλ.

• **Σάρωση υπολογιστή** – Αυτό είναι το προεπιλεγμένο προφίλ που χρησιμοποιείται στην τυπική σάρωση υπολογιστή.

Μπορείτε να αποθηκεύσετε τις παραμέτρους σάρωσης που προτιμάτε για μελλοντικές σαρώσεις. Συνιστούμε να δημιουργήσετε διαφορετικό προφίλ (με διάφορους προορισμούς σάρωσης, μεθόδους σάρωσης και άλλες παραμέτρους) για κάθε τύπο σάρωσης που πραγματοποιείτε συχνά.

Για να δημιουργήσετε νέο προφίλ, ανοίξτε το παράθυρο "Ρυθμίσεις για προχωρημένους" (F5) και επιλέξτε **Μηχανισμός ανίχνευσης** > **Σαρώσεις κακόβουλου λογισμικού** > **Σάρωση κατ' απαίτηση** > **Λίστα προφίλ**. Το παράθυρο **Διαχείριση προφίλ** περιλαμβάνει το αναπτυσσόμενο μενού **Επιλεγμένο προφίλ**, το οποίο παραθέτει τα υπάρχοντα προφίλ σάρωσης και την επιλογή να δημιουργήσετε ένα νέο. Για βοήθεια σχετικά με τη δημιουργία ενός προφίλ σάρωσης που θα ταιριάζει στις απαιτήσεις σας, ανατρέξτε στην ενότητα Ρύθμιση παραμέτρων μηχανισμού ThreatSense, για την περιγραφή κάθε παραμέτρου των ρυθμίσεων σάρωσης.

Υποθέστε ότι θέλετε να δημιουργήσετε το προσωπικό σας προφίλ σάρωσης και η διαμόρφωση της επιλογής **Σάρωση του υπολογιστή σας** σας ικανοποιεί εν μέρει, αλλά δεν θέλετε να πραγματοποιείται σάρωση προγραμμάτων συσκευασίας χρόνου εκτέλεσης ή ενδεχομένως μη ασφαλών εφαρμογών και επίσης θέλετε να εφαρμόσετε **Πάντα αποκατάσταση ανίχνευσης**. Εισαγάγετε το όνομα του νέου προφίλ στο παράθυρο **Διαχείριση προφίλ** και κάντε κλικ στο κουμπί **Προσθήκη**. Εισαγάγετε το νέο σας προφίλ από το αναπτυσσόμενο μενού **Επιλεγμένο προφίλ**, ρυθμίστε τις υπόλοιπες παραμέτρους σύμφωνα με τις απαιτήσεις σας και κάντε κλικ στο κουμπί **ΟΚ** για να αποθηκεύσετε το νέο προφίλ σας.

Ενημέρωση

Η επεξεργασία προφίλ στην ενότητα Ρυθμίσεων ενημέρωσης επιτρέπει στους χρήστες να δημιουργήσουν νέα προφίλ ενημέρωσης. Δημιουργήστε και χρησιμοποιήστε τα δικά σας προσαρμοσμένα προφίλ (εκτός από το προεπιλεγμένο **Το προφίλ μου**) μόνο αν ο υπολογιστής σας χρησιμοποιεί πολλά μέσα για να συνδεθεί σε διακομιστές ενημέρωσης.

Για παράδειγμα, ένας φορητός υπολογιστής που συνδέεται συνήθως με έναν τοπικό διακομιστή (Είδωλο) στο τοπικό δίκτυο, αλλά κάνει λήψη ενημερώσεων απευθείας από τους διακομιστές ενημέρωσης της ESET όταν αποσυνδέεται από το τοπικό δίκτυο (επιχειρηματικό ταξίδι) μπορεί να χρησιμοποιεί δύο προφίλ: το πρώτο για σύνδεση με τον τοπικό διακομιστή, και το δεύτερο για σύνδεση με τους διακομιστές της ESET. Όταν διαμορφωθούν αυτά τα προφίλ, πλοηγηθείτε στα στοιχεία **Εργαλεία** > **Χρονοδιάγραμμα εργασιών** και επεξεργαστείτε τις παραμέτρους εργασιών ενημέρωσης. Καθορίστε ένα προφίλ ως κύριο και το άλλο ως δευτερεύον.

Προφίλ ενημέρωσης – Το τρέχον προφίλ ενημέρωσης που χρησιμοποιείται. Για να το αλλάξετε, επιλέξτε ένα προφίλ από το αναπτυσσόμενο μενού.

Λίστα προφίλ – Δημιουργήστε νέα ή καταργήστε υπάρχοντα προφίλ ενημέρωσης.

Συντομεύσεις πληκτρολογίου

Για καλύτερη πλοήγηση στο ESET Internet Security, μπορείτε να χρησιμοποιείτε τις ακόλουθες συντομεύσεις πληκτρολογίου:

Συντομεύσεις πληκτρολογίου	Ενέργεια
F1	ανοίγει τις σελίδες βοήθειας
F5	ανοίγει τις Ρυθμίσεις για προχωρημένους
Επάνω βέλος / Κάτω βέλος	περιήγηση σε στοιχεία του αναπτυσσόμενου μενού
TAB	μετακίνηση στο επόμενο στοιχείο του γραφικού περιβάλλοντος χρήστη σε ένα παράθυρο
Shift+TAB	μετακίνηση στο προηγούμενο στοιχείο του γραφικού περιβάλλοντος χρήστη σε ένα παράθυρο
ESC	κλείνει το ενεργό παράθυρο διαλόγου
Ctrl+U	εμφανίζει πληροφορίες σχετικά με την άδεια χρήσης ESET και τον υπολογιστή σας (λεπτομέρειες για την Τεχνική υποστήριξη)
Ctrl+R	κάνει επαναφορά του παραθύρου του προϊόντος στο προεπιλεγμένο μέγεθος και τη θέση στην οθόνη
ALT + Αριστερό βέλος	πλοήγηση προς τα πίσω
ALT + Δεξί βέλος	πλοήγηση προς τα εμπρός
ALT+Home	πλοήγηση στην αρχική σελίδα

Μπορείτε επίσης να χρησιμοποιήσετε τα κουμπιά του ποντικιού για πλοήγηση προς τα πίσω ή προς τα εμπρός.

Διαγνωστικοί έλεγχοι

Οι διαγνωστικοί έλεγχοι παρέχουν αρχεία ένδειξης σφαλμάτων εφαρμογής για διεργασίες ESET (για παράδειγμα, το ekrn). Εάν διακοπεί η λειτουργία μιας εφαρμογής, θα δημιουργηθεί ένα αρχείο ένδειξης σφαλμάτων. Αυτό μπορεί να βοηθήσει τους προγραμματιστές να εντοπίσουν και να διορθώσουν διάφορα προβλήματα του ESET Internet Security.

Κάντε κλικ στο αναπτυσσόμενο μενού δίπλα στο στοιχείο **Τύπος αρχείου ένδειξης σφαλμάτων** και επιλέξτε μία από τις τρεις διαθέσιμες επιλογές:

- Επιλέξτε **Απενεργοποίηση** για να απενεργοποιήσετε αυτήν τη δυνατότητα.

- **Αρχείο ένδειξης μικρών σφαλμάτων** (Προεπιλογή) – Καταγράφει το μικρότερο σύνολο χρήσιμων πληροφοριών που μπορεί να βοηθήσει να προσδιοριστεί ο λόγος για τον οποίο η λειτουργία της εφαρμογής διακόπηκε με μη αναμενόμενο τρόπο. Αυτό το είδος αρχείου ένδειξης σφαλμάτων μπορεί να είναι χρήσιμο όταν ο διαθέσιμος χώρος δεν επαρκεί. Ωστόσο, λόγω των περιορισμένων πληροφοριών που περιλαμβάνονται, τα σφάλματα που δεν προκλήθηκαν άμεσα από το νήμα που εκτελούνταν την ώρα που παρουσιάστηκε το πρόβλημα μπορεί να μην αποκαλυφθούν στην ανάλυση αυτού του αρχείου.

- **Πλήρεις** – Καταγράφει όλα τα περιεχόμενα της μνήμης του συστήματος όταν διακοπεί η

λειτουργία της εφαρμογής με μη αναμενόμενο τρόπο. Το πλήρες αρχείο ένδειξης σφαλμάτων μπορεί να περιέχει δεδομένα από διεργασίες που εκτελούνταν όταν συλλέχτηκε το αρχείο ένδειξης σφαλμάτων μνήμης.

Κατάλογος προορισμού – Ο κατάλογος στον οποίο θα δημιουργηθεί το αρχείο ένδειξης σφαλμάτων κατά τη διάρκεια του σφάλματος.

Άνοιγμα φακέλου διαγνωστικών ελέγχων – Κάντε κλικ στο κουμπί **Άνοιγμα** για να ανοίξετε αυτό τον κατάλογο σε ένα νέο παράθυρο της Εξερεύνησης των *Windows*.

Δημιουργία αρχείου ένδειξης σφαλμάτων διαγνωστικού ελέγχου – Κάντε κλικ στο στοιχείο **Δημιουργία** για να δημιουργήσετε αρχεία ένδειξης σφαλμάτων διαγνωστικού ελέγχου στο στοιχείο **Κατάλογος προορισμού**.

Καταγραφή για προχωρημένους

Ενεργοποίηση καταγραφής για προχωρημένους σε μηνύματα μάρκετινγκ – Καταγραφή όλων των συμβάντων που σχετίζονται με μηνύματα μάρκετινγκ εντός του προϊόντος.

Ενεργοποίηση προηγμένης καταγραφής μηχανισμού Antispam – Καταγράφει όλα τα συμβάντα που προκύπτουν κατά τη σάρωση antispam. Αυτό μπορεί να βοηθήσει τους προγραμματιστές να διαγνώσουν και να διορθώσουν προβλήματα που σχετίζονται με το μηχανισμό Antispam της ESET.

Ενεργοποίηση προηγμένης καταγραφής μηχανισμού Anti-Theft – Καταγραφή όλων των συμβάντων που προκύπτουν στην προστασία Anti-Theft για να επιτρέπεται η διάγνωση και η επίλυση προβλημάτων.

Ενεργοποίηση καταγραφής για προχωρημένους της Προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών – Καταγραφή όλων των συμβάντων που προκύπτουν στην Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών.

Ενεργοποίηση καταγραφής για προχωρημένους της σάρωσης υπολογιστή – Καταγραφή όλων των συμβάντων που προκύπτουν κατά τη σάρωση αρχείων και φακέλων με τη Σάρωση υπολογιστή.

Ενεργοποίηση Προηγμένης καταγραφής ελέγχου συνδεδεμένων συσκευών – Καταγράφει όλα τα συμβάντα που προκύπτουν κατά τον έλεγχο συνδεδεμένων συσκευών. Αυτό μπορεί να βοηθήσει τους προγραμματιστές να διαγνώσουν και να διορθώσουν προβλήματα που σχετίζονται με τον έλεγχο συνδεδεμένων συσκευών.

Ενεργοποίηση καταγραφής για προχωρημένους του Direct Cloud – Καταγραφή όλων των συμβάντων που προκύπτουν στο ESET LiveGrid®. Αυτό μπορεί να βοηθήσει τους προγραμματιστές να διαγνώσουν και να διορθώσουν προβλήματα που σχετίζονται με το ESET LiveGrid®.

Ενεργοποίηση Καταγραφή για προχωρημένους της Προστασίας εγγράφων – Καταγράψτε όλα τα συμβάντα που προκύπτουν στην Προστασία εγγράφων, για να επιτρέπεται η διάγνωση και η επίλυση προβλημάτων.

Ενεργοποίηση καταγραφής για προχωρημένους της Προστασίας ηλεκτρονικής αλληλογραφίας – Καταγράφει όλα τα συμβάντα που προκύπτουν στην Προστασία ηλεκτρονικής αλληλογραφίας και στο πρόσθετο της Προστασίας ηλεκτρονικής αλληλογραφίας για να επιτρέπεται η διάγνωση και η επίλυση προβλημάτων.

Ενεργοποίηση καταγραφής για προχωρημένους του πυρήνα – Καταγραφή όλων των συμβάντων που σημειώνονται στον πυρήνα ESET (ekrn).

Ενεργοποίηση προηγμένης καταγραφής αδειών χρήσης – Καταγραφή όλης της επικοινωνίας του προϊόντος με την ενεργοποίηση της ESET ή τους διακομιστές ESET License Manager.

Ενεργοποίηση παρακολούθησης μνήμης – Καταγραφή όλων των συμβάντων που θα βοηθήσουν τους προγραμματιστές να διαγνώσουν διαρροές μνήμης.

Ενεργοποίηση προηγμένης καταγραφής προστασίας δικτύου – Καταγράφει όλα τα δεδομένα δικτύου που περνούν από το Τείχος προστασίας σε μορφή PCAP για να βοηθήσει τους προγραμματιστές να διαγνώσουν και να διορθώσουν προβλήματα που σχετίζονται με το Τείχος προστασίας.

Ενεργοποίηση καταγραφής για προχωρημένους του λειτουργικού συστήματος – Καταγραφή πρόσθετων πληροφοριών για το λειτουργικό σύστημα, όπως οι εκτελούμενες διεργασίες, η δραστηριότητα του CPU και οι λειτουργίες δίσκου. Αυτό μπορεί να βοηθήσει τους προγραμματιστές να διαγνώσουν και να επιδιορθώσουν προβλήματα που σχετίζονται με το προϊόν ESET που εκτελείται στο λειτουργικό σύστημά σας.

Ενεργοποίηση προηγμένης καταγραφής Γονικού ελέγχου – Καταγράφει όλα τα συμβάντα που προκύπτουν κατά το γονικό έλεγχο. Αυτό μπορεί να βοηθήσει τους προγραμματιστές να διαγνώσουν και να διορθώσουν προβλήματα που σχετίζονται με το γονικό έλεγχο.

Ενεργοποίηση προηγμένης καταγραφής Φιλτραρίσματος πρωτοκόλλων – Καταγράφει όλα τα δεδομένα που περνούν από το Φιλτράρισμα πρωτοκόλλων σε μορφή PCAP για να βοηθήσει τους προγραμματιστές να διαγνώσουν και να διορθώσουν προβλήματα που σχετίζονται με το Φιλτράρισμα πρωτοκόλλων.

Ενεργοποίηση καταγραφής για προχωρημένους της προώθησης μηνυμάτων – Καταγραφή όλων των συμβάντων που σημειώνονται κατά τη διάρκεια της προώθησης μηνυμάτων.

Ενεργοποίηση καταγραφής για προχωρημένους της προστασίας συστήματος αρχείων σε πραγματικό χρόνο – Καταγραφή όλων των συμβάντων που σημειώνονται κατά τη σάρωση αρχείων και φακέλων με την Προστασία συστήματος αρχείων σε πραγματικό χρόνο.

Ενεργοποίηση προηγμένης καταγραφής μηχανισμού ενημέρωσης – Καταγράφει όλα τα συμβάντα που προκύπτουν κατά τη διαδικασία ενημέρωσης. Αυτό βοηθά τους προγραμματιστές να διαγνώσουν και να διορθώσουν προβλήματα που σχετίζονται με το μηχανισμό ενημέρωσης.

Τα αρχεία καταγραφής βρίσκονται στη διαδρομή *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Τεχνική υποστήριξη

Όταν επικοινωνείτε με την Τεχνική υποστήριξη της ESET από το ESET Internet Security, μπορείτε να υποβάλετε δεδομένα ρύθμισης παραμέτρων συστήματος. Επιλέξτε **Υποβολή πάντα** από το αναπτυσσόμενο μενού **Υποβολή δεδομένων ρύθμισης παραμέτρων συστήματος** για να υποβάλετε αυτόματα τα δεδομένα ή επιλέξτε **Ερώτηση πριν από την υποβολή** για να ερωτηθείτε πριν από την υποβολή δεδομένων.

Ρυθμίσεις εισαγωγής και εξαγωγής

Μπορείτε να εισάγετε ή να εξάγετε το προσαρμοσμένο αρχείο διαμόρφωσης .xml του ESET Internet Security από το μενού **Ρυθμίσεις**.

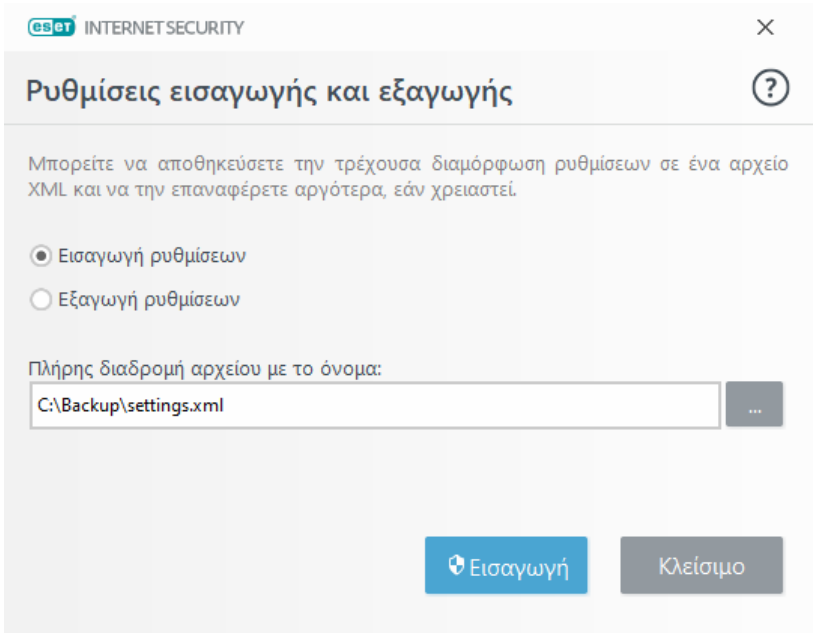
> **Εικονογραφημένες οδηγίες**
> Ανατρέξτε στο θέμα Εισαγωγή ή εξαγωγή ρυθμίσεων ρύθμισης παραμέτρων της ESET χρησιμοποιώντας ένα αρχείο .xml, για εικονογραφημένες οδηγίες που είναι διαθέσιμες στα Αγγλικά και σε αρκετές άλλες γλώσσες.

Η εισαγωγή και η εξαγωγή αρχείων ρύθμισης παραμέτρων είναι χρήσιμες, εάν χρειάζεται να δημιουργήσετε αντίγραφο ασφαλείας της τρέχουσας ρύθμισης παραμέτρων του ESET Internet Security για χρήση αργότερα. Η επιλογή εξαγωγής ρυθμίσεων είναι επίσης βολική, εάν θέλετε να χρησιμοποιήσετε την προτιμώμενη ρύθμιση παραμέτρων σας σε πολλαπλά συστήματα. Μπορείτε να εισαγάγετε ένα αρχείο .xml για να μεταφέρετε αυτές τις ρυθμίσεις.

Η εισαγωγή μιας ρύθμισης παραμέτρων είναι πολύ εύκολη. Στο κύριο παράθυρο του προγράμματος, κάντε κλικ στα στοιχεία **Ρυθμίσεις** > **Ρυθμίσεις εισαγωγής/εξαγωγής** και επιλέξτε **Ρυθμίσεις εισαγωγής**. Πληκτρολογήστε το όνομα του αρχείου ρύθμισης παραμέτρων ή κάντε κλικ στο κουμπί **...** για να αναζητήσετε το αρχείο ρύθμισης παραμέτρων που θέλετε να εισαγάγετε.

Για να εξαγάγετε μια ρύθμιση παραμέτρων, στο παράθυρο του κύριου προγράμματος, κάντε κλικ στα στοιχεία **Ρυθμίσεις** > **Ρυθμίσεις εισαγωγής/εξαγωγής**. Επιλέξτε **Εξαγωγή ρυθμίσεων** και πληκτρολογήστε την πλήρη διαδρομή αρχείου με το όνομα. Κάντε κλικ στο στοιχείο **...** για να μεταβείτε σε μια θέση στον υπολογιστή σας για να αποθηκεύσετε το αρχείο ρύθμισης παραμέτρων.

> Ενδέχεται να προκύψει σφάλμα κατά την εξαγωγή των ρυθμίσεων αν δεν έχετε επαρκή δικαιώματα για εγγραφή του αρχείου εξαγωγής στον καθορισμένο κατάλογο.



Επαναφορά όλων των ρυθμίσεων στην τρέχουσα ενότητα

Κάντε κλικ στο καμπυλωτό βέλος για επαναφορά όλων των ρυθμίσεων στην τρέχουσα ενότητα στις προεπιλεγμένες ρυθμίσεις που καθορίζονται από την ESET.

Σημειώνεται ότι όσες αλλαγές πραγματοποιήσατε θα χαθούν μόλις κάνετε κλικ στην επιλογή **Επαναφορά στην προεπιλογή**.

Επαναφορά περιεχομένων πινάκων – Όταν ενεργοποιείται αυτή η επιλογή, χάνονται οι κανόνες, οι εργασίες ή τα προφίλ τα οποία προστέθηκαν αυτόματα ή μη αυτόματα.

Δείτε επίσης Ρυθμίσεις εισαγωγής και εξαγωγής.

Επαναφορά προεπιλεγμένων ρυθμίσεων

Κάντε κλικ στο στοιχείο **Προεπιλογή** στην **Ρυθμίσεις για προχωρημένους** (F5) για να γίνει επαναφορά όλων των ρυθμίσεων του προγράμματος, για όλες τις λειτουργικές μονάδες. Αυτό θα έχει ως αποτέλεσμα την επαναφορά στην κατάσταση που θα είχαν ύστερα από μια νέα εγκατάσταση.

Δείτε επίσης Ρυθμίσεις εισαγωγής και εξαγωγής.

Σφάλμα κατά την αποθήκευση της διαμόρφωσης

Αυτό το μήνυμα σφάλματος υποδεικνύει ότι οι ρυθμίσεις δεν αποθηκεύτηκαν σωστά λόγω σφάλματος.

Αυτό σημαίνει συνήθως ότι ο χρήστης που προσπάθησε να τροποποιήσει τις παραμέτρους του προγράμματος:

• έχει ανεπαρκή δικαιώματα πρόσβασης ή δεν έχει τα απαραίτητα δικαιώματα λειτουργικού συστήματος που απαιτούνται για να τροποποιεί αρχεία ρύθμισης παραμέτρων και το μητρώο του συστήματος.
> Για να εκτελεστούν οι επιθυμητές τροποποιήσεις, πρέπει να συνδεθεί ο διαχειριστής συστήματος.

• έχει ενεργοποιήσει πρόσφατα τη Λειτουργία εκμάθησης στο HIPS ή στο Τείχος προστασίας και προσπάθησε να πραγματοποιήσει αλλαγές στην Εγκατάσταση για προχωρημένους.
> Για να αποθηκευτεί η ρύθμιση παραμέτρων και να αποφευχθεί σύγκρουση της ρύθμισης παραμέτρων, κλείστε την Εγκατάσταση για προχωρημένους χωρίς αποθήκευση και προσπαθήστε να πραγματοποιήσετε ξανά τις επιθυμητές αλλαγές.

Η δεύτερη πιο συνηθισμένη αιτία μπορεί να είναι ότι το πρόγραμμα δεν λειτουργεί πλέον σωστά, έχει καταστραφεί και πρέπει κατά συνέπεια να εγκατασταθεί ξανά.

Σαρωτής γραμμής εντολών

Η μονάδα antivirus του ESET Internet Security μπορεί να ξεκινήσει μέσω της γραμμής εντολών – με μη αυτόματο τρόπο (με την εντολή «ecls») ή με ένα αρχείο δέσμης («bat»).

Χρήση σάρωσης γραμμής εντολών ESET:

```
ecls [OPTIONS..] FILES..
```

Οι ακόλουθες παράμετροι και διακόπτες μπορούν να χρησιμοποιούνται κατά την εκτέλεση της σάρωσης κατ' απαίτηση από τη γραμμή εντολών:

Επιλογές

/base-dir=ΦΑΚΕΛΟΣ	φόρτωση λειτουργικών μονάδων από ΦΑΚΕΛΟ
/quar-dir=ΦΑΚΕΛΟΣ	ΦΑΚΕΛΟΣ καραντίνας
/exclude=ΜΑΣΚΑ	να εξαιρούνται από τη σάρωση τα αρχεία που ταιριάζουν με τη ΜΑΣΚΑ
/subdir	σάρωση υποφακέλων (προεπιλογή)
/no-subdir	να μην γίνεται σάρωση υποφακέλων
/max-subdir-level=ΕΠΙΠΕΔΟ	μέγιστο δευτερεύον επίπεδο φακέλων μέσα στους φακέλους που θα σαρωθούν
/symlink	να ακολουθούνται συμβολικοί σύνδεσμοι (προεπιλογή)
/no-symlink	παράβλεψη συμβολικών συνδέσμων
/ads	σάρωση ADS (προεπιλογή)
/no-ads	να μην γίνεται σάρωση ADS
/log-file=ΑΡΧΕΙΟ	καταγραφή εξόδου σε ΑΡΧΕΙΟ
/log-rewrite	αντικατάσταση αρχείου εξόδου (προεπιλογή – επισύναψη)
/log-console	καταγραφή εξόδου στην κονσόλα (προεπιλογή)
/no-log-console	να μην γίνεται καταγραφή της εξόδου στην κονσόλα
/log-all	να γίνεται επίσης καταγραφή των καθαρών αρχείων
/no-log-all	να μην γίνεται καταγραφή των καθαρών αρχείων (προεπιλογή)
/aind	εμφάνιση ένδειξης δραστηριότητας
/auto	σάρωση και αυτόματος καθαρισμός όλων των τοπικών δίσκων

Επιλογές σάρωσης

/files	σάρωση αρχείων (προεπιλογή)
/no-files	να μην γίνεται σάρωση αρχείων
/memory	σάρωση μνήμης
/boots	σάρωση τομέων εκκίνησης
/no-boots	να μην γίνεται σάρωση τομέων εκκίνησης (προεπιλογή)
/arch	σάρωση αρχειοθηκών (προεπιλογή)
/no-arch	να μην γίνεται σάρωση αρχειοθηκών

/max-obj-size=ΜΕΓΕΘΟΣ	μόνο σάρωση αρχείων μικρότερων από ΜΕΓΕΘΟΣ megabyte (προεπιλογή 0 = απεριόριστο)
/max-arch-level=ΕΠΙΠΕΔΟ	μέγιστο δευτερεύον επίπεδο αρχειοθηκών μέσα σε αρχειοθήκες (ένθετες αρχειοθήκες) για σάρωση
/scan-timeout=ΟΡΙΟ	σάρωση αρχειοθηκών για ΟΡΙΟ δευτερόλεπτα κατά μέγιστο
/max-arch-size=ΜΕΓΕΘΟΣ	να γίνεται σάρωση μόνο των αρχείων σε μια αρχειοθήκη που είναι μικρότερα από ΜΕΓΕΘΟΣ (προεπιλογή 0=απεριόριστο)
/max-sfx-size=ΜΕΓΕΘΟΣ	μόνο σάρωση των αρχείων σε αρχειοθήκη αυτόματης εξαγωγής που είναι μικρότερα από ΜΕΓΕΘΟΣ megabyte (προεπιλογή 0 = απεριόριστο)
/mail	σάρωση αρχείων ηλεκτρονικής αλληλογραφίας (προεπιλογή)
/no-mail	να μην γίνεται σάρωση αρχείων ηλεκτρονικής αλληλογραφίας
/mailbox	σάρωση γραμματοκιβωτίων (προεπιλογή)
/no-mailbox	να μην γίνεται σάρωση γραμματοκιβωτίων
/sfx	σάρωση αρχειοθηκών αυτόματης εξαγωγής (προεπιλογή)
/no-sfx	να μην γίνεται σάρωση αρχειοθηκών αυτόματης εξαγωγής
/rtp	σάρωση προγραμμάτων συσκευασίας χρόνου εκτέλεσης (προεπιλογή)
/no-rtp	να μην γίνεται σάρωση προγραμμάτων συσκευασίας χρόνου εκτέλεσης
/unsafe	σάρωση για ενδεχομένως μη ασφαλείς εφαρμογές
/no-unsafe	να μην γίνεται σάρωση για ενδεχομένως μη ασφαλείς εφαρμογές (προεπιλογή)
/unwanted	σάρωση για ενδεχομένως ανεπιθύμητες εφαρμογές
/no-unwanted	να μην γίνεται σάρωση για ενδεχομένως ανεπιθύμητες εφαρμογές (προεπιλογή)
/suspicious	σάρωση για ύποπτες εφαρμογές (προεπιλογή)
/no-suspicious	να μην γίνεται σάρωση για ύποπτες εφαρμογές
/pattern	χρήση υπογραφών (προεπιλογή)
/no-pattern	να μην γίνεται χρήση υπογραφών
/heur	ενεργοποίηση ευριστικού ελέγχου (προεπιλογή)
/no-heur	απενεργοποίηση ευριστικού ελέγχου
/adv-heur	ενεργοποίηση προηγμένου ευριστικού ελέγχου (προεπιλογή)
/no-adv-heur	απενεργοποίηση προηγμένου ευριστικού ελέγχου
/ext-exclude=ΕΠΕΚΤΑΣΕΙΣ	να εξαιρούνται από τη σάρωση οι ΕΠΕΚΤΑΣΕΙΣ αρχείων που διαχωρίζονται με ερωτηματικό

/clean-mode=ΛΕΙΤΟΥΡΓΙΑ	χρησιμοποιείτε τη ΛΕΙΤΟΥΡΓΙΑ καθαρισμού για μολυσμένα αντικείμενα Οι διαθέσιμες επιλογές είναι οι παρακάτω: • none (προεπιλογή) – Δεν θα πραγματοποιηθεί αυτόματος καθαρισμός. • standard – Το ecls.exe θα επιχειρήσει να καθαρίσει ή να διαγράψει αυτόματα τα μολυσμένα αρχεία. • αυστηρή – Το ecls.exe θα επιχειρήσει να καθαρίσει ή να διαγράψει αυτόματα όλα τα μολυσμένα αρχεία χωρίς παρέμβαση του χρήστη (δεν θα σας ζητείται να επιβεβαιώσετε τη διαγραφή αρχείων). • ενδελεχής – Το ecls.exe θα διαγράφει αρχεία χωρίς να επιχειρεί να τα καθαρίσει, ανεξάρτητα από το είδος των αρχείων. • διαγραφή – Το ecls.exe θα διαγράφει αρχεία χωρίς να επιχειρεί να τα καθαρίσει, αλλά δεν θα διαγράφει ευαίσθητα αρχεία όπως αρχεία συστήματος των Windows.
/quarantine	αντιγραφή μολυσμένων αρχείων (εάν έχουν καθαριστεί) στην Καραντίνα (συμπληρώνει την ενέργεια που πραγματοποιείται κατά τον καθαρισμό)
/no-quarantine	να μην γίνεται αντιγραφή των μολυσμένων αρχείων στην Καραντίνα

Γενικές επιλογές

/help	εμφάνιση βοήθειας και κλείσιμο
/version	εμφάνιση πληροφοριών έκδοσης και κλείσιμο
/preserve-time	διατήρηση χρονικής σήμανσης τελευταίας πρόσβασης

Κωδικοί εξόδου

0	δεν βρέθηκε απειλή
1	βρέθηκε απειλή και καθαρίστηκε
10	δεν ήταν δυνατό να σαρωθούν ορισμένα αρχεία (ίσως είναι απειλές)
50	εντοπίστηκε απειλή
100	σφάλμα

Οι κωδικοί εξόδου που είναι μεγαλύτεροι από 100 σημαίνουν ότι το αρχείο δεν σαρώθηκε και, συνεπώς, ίσως είναι μολυσμένο.

ESET CMD

Πρόκειται για μια δυνατότητα η οποία ενεργοποιεί προηγμένες εντολές ecmd. Σας επιτρέπει να εξάγετε και να εισάγετε ρυθμίσεις χρησιμοποιώντας τη γραμμή εντολών (ecmd.exe). Μέχρι τώρα, ήταν δυνατή η εξαγωγή ρυθμίσεων μόνο με χρήση του γραφικού περιβάλλοντος. Η διαμόρφωση του ESET Internet Security μπορεί να εξαχθεί σε αρχείο *.xml*.

Αφού ενεργοποιήσετε το ESET CMD, υπάρχουν δύο διαθέσιμες μέθοδοι εξουσιοδότησης:

• **Καμία** – Καμία εξουσιοδότηση. Δεν συνιστάται η χρήση αυτής της μεθόδου, επειδή επιτρέπει την εισαγωγή οποιασδήποτε μη υπογεγραμμένης διαμόρφωσης, κάτι που αποτελεί ενδεχόμενο κίνδυνο.

• **Κωδικός πρόσβασης ρυθμίσεων για προχωρημένους** – απαιτείται κωδικός πρόσβασης για να εισαγάγετε μια διαμόρφωση από ένα αρχείο .xml.xml. Αυτό το αρχείο πρέπει να είναι υπογεγραμμένο (δείτε την ενότητα υπογραφής αρχείου διαμόρφωσης .xml παρακάτω). Ο κωδικός πρόσβασης που καθορίζεται στη Ρύθμιση πρόσβασης πρέπει να παρέχεται πριν την εισαγωγή της νέας διαμόρφωσης. Εάν η Ρύθμιση πρόσβασης δεν είναι ενεργοποιημένη, ο κωδικός πρόσβασης δεν αντιστοιχεί ή το αρχείο διαμόρφωσης .xml δεν είναι υπογεγραμμένο, δεν πραγματοποιείται η εισαγωγή της διαμόρφωσης.

Μόλις ενεργοποιηθεί το ESET CMD, μπορείτε να χρησιμοποιήσετε τη γραμμή εντολών για την εξαγωγή ή εισαγωγή των διαμορφώσεων του ESET Internet Security. Μπορείτε να το κάνετε μη αυτόματα ή να δημιουργήσετε μια δέσμη ενεργειών για να αυτοματοποιήσετε τη διαδικασία.

Για να χρησιμοποιήσετε προηγμένες εντολές ecmd, θα πρέπει να τις εκτελέσετε με προνόμια διαχειριστή ή να ανοίξετε τη Γραμμή εντολών των Windows (cmd) με την επιλογή **Εκτέλεση ως διαχειριστής**. Διαφορετικά, θα λάβετε το μήνυμα **Error executing command**. Επίσης, κατά την εξαγωγή μιας διαμόρφωσης, πρέπει να υπάρχει ο φάκελος προορισμού. Η εντολή εξαγωγής εξακολουθεί να λειτουργεί και όταν έχει απενεργοποιηθεί η ρύθμιση ESET CMD.

Εντολή εξαγωγής ρυθμίσεων:
```
ecmd /getcfg c:\config\settings.xml
```

Εντολή εισαγωγής ρυθμίσεων:
```
ecmd /setcfg c:\config\settings.xml
```

Οι προηγμένες εντολές ecmd είναι δυνατό να εκτελούνται μόνο τοπικά.

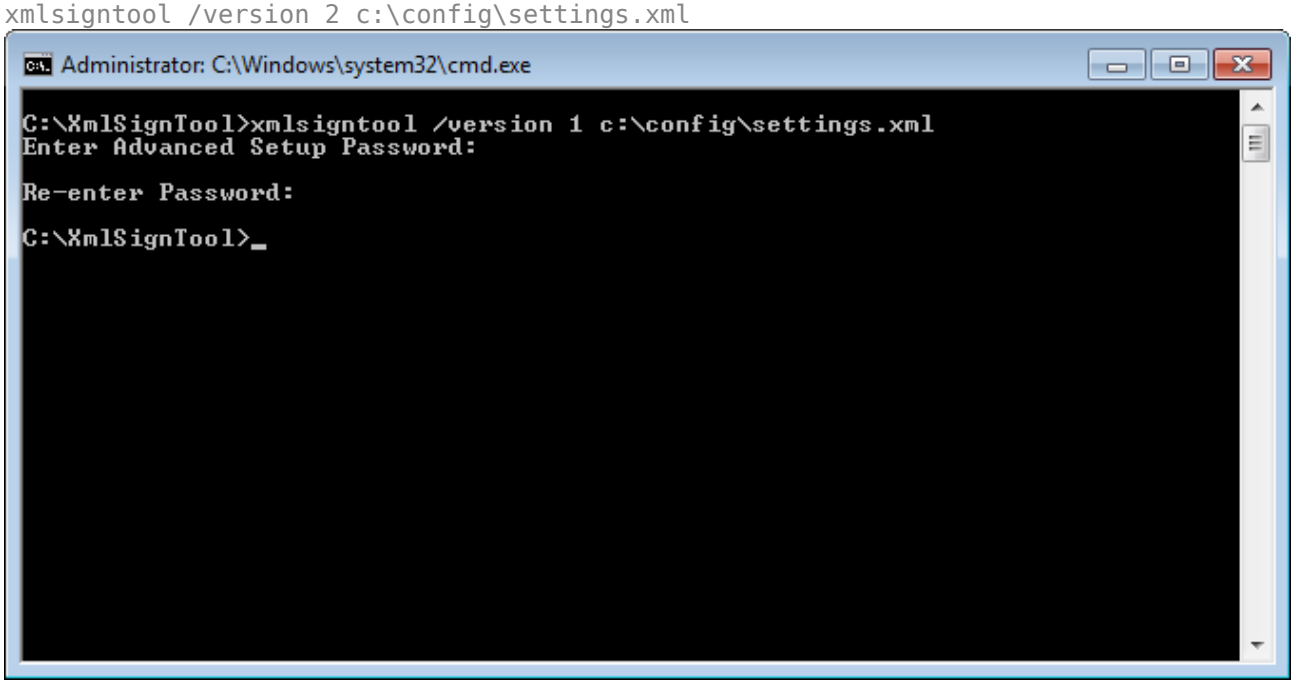
Υπογραφή αρχείου διαμόρφωσης *.xml*:

1. Κάντε λήψη του εκτελέσιμου αρχείου XmlSignTool.
2. Ανοίξτε τη Γραμμή εντολών των Windows (cmd) με την επιλογή **Εκτέλεση ως διαχειριστής**.
3. Πλοηγηθείτε στην τοποθεσία αποθήκευσης του `xmlsigntool.exe`
4. Εκτελέστε μια εντολή για την υπογραφή του αρχείου διαμόρφωσης *.xml*, με τη μορφή:
```
xmlsigntool /version 1|2 <xml_file_path>
```

Η τιμή της παραμέτρου `/version` εξαρτάται από την έκδοση του ESET Internet Security που διαθέτετε. Χρησιμοποιήστε το `/version 1` για παλαιότερες εκδόσεις του ESET Internet Security από την έκδοση 11.1. Χρησιμοποιήστε το `/version 2` για την τρέχουσα έκδοση του ESET Internet Security.

5. Εισαγάγετε δύο φορές τον κωδικό πρόσβασης για τις Ρυθμίσεις για προχωρημένους, όταν σας ζητηθεί από το XmlSignTool. Το αρχείο διαμόρφωσης *.xml* είναι πλέον υπογεγραμμένο και μπορεί να χρησιμοποιηθεί για εισαγωγή μιας άλλης εμφάνισης του ESET Internet Security με το ESET CMD χρησιμοποιώντας τη μέθοδο εξουσιοδότησης κωδικού πρόσβασης.

Εντολή υπογραφής αρχείου διαμόρφωσης εξαγωγής:
`xmlsigntool /version 2 c:\config\settings.xml`



Εάν ο κωδικός πρόσβασης για τις Ρυθμίσεις για προχωρημένους άλλαξε και θέλετε να εισαγάγετε μια διαμόρφωση που υπογράφηκε προηγουμένως με παλιό κωδικό πρόσβασης, πρέπει να υπογράψετε το αρχείο διαμόρφωσης *.xml* ξανά με τον τρέχοντα κωδικό πρόσβασης. Αυτό σάς επιτρέπει να χρησιμοποιήσετε ένα παλαιότερο αρχείο διαμόρφωσης χωρίς να το εξαγάγετε πριν από την εισαγωγή σε άλλον υπολογιστή που εκτελεί το ESET Internet Security.

Η ενεργοποίηση του ESET CMD χωρίς εξουσιοδότηση δεν συνιστάται, καθώς αυτό θα επιτρέψει την εισαγωγή οποιασδήποτε μη υπογεγραμμένης διαμόρφωσης. Καθορίστε τον κωδικό πρόσβασης στη θέση **Ρυθμίσεις για προχωρημένους** > **Περιβάλλον χρήστη** > **Ρύθμιση πρόσβασης**, για να αποτρέψετε τυχόν τροποποίηση από μη εξουσιοδοτημένους χρήστες.

Ανίχνευση κατάστασης αδράνειας

Οι ρυθμίσεις εντοπισμού σε κατάσταση αδράνειας μπορούν να διαμορφωθούν στο στοιχείο **Εγκατάσταση για προχωρημένους** στην ενότητα **Μηχανισμός ανίχνευσης** > **Σαρώσεις για κακόβουλο λογισμικό** > **Σάρωση σε κατάσταση αδράνειας** > **Ανίχνευση κατάστασης αδράνειας**. Οι ρυθμίσεις αυτές καθορίζουν ένα ερέθισμα για Σάρωση σε κατάσταση αδράνειας:

- **Απενεργοποίηση οθόνης ή προστασίας οθόνης**
- **Κλείδωμα υπολογιστή**
- **Αποσύνδεση χρήστη**

Χρησιμοποιήστε τα ρυθμιστικά για κάθε αντίστοιχη κατάσταση, για να ενεργοποιήσετε ή να απενεργοποιήσετε τα διάφορα ερεθίσματα ανίχνευσης σε κατάσταση αδράνειας.

Συχνές ερωτήσεις

Παρακάτω μπορείτε να βρείτε μερικές από τις πιο συχνές ερωτήσεις και τα προβλήματα που αντιμετωπίζονται. Κάντε κλικ στον τίτλο θέματος για να βρείτε τρόπους να επιλύσετε το πρόβλημα:

- Πώς να ενημερώσετε το ESET Internet Security
- Πώς να αφαιρέσετε έναν ιό από τον υπολογιστή σας
- Πώς να επιτρέπεται η επικοινωνία για μια συγκεκριμένη εφαρμογή
- Πώς να ενεργοποιείτε τον Γονικό έλεγχο για έναν λογαριασμό
- Πώς να δημιουργήσετε μια νέα εργασία στο Χρονοδιάγραμμα εργασιών
- Πώς να προγραμματίσετε μια εργασία σάρωσης (εβδομαδιαία)
- Πώς να επιλύσετε το σφάλμα «Η Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών δεν ήταν δυνατόν να ανακατευθυνθεί στην ιστοσελίδα που ζητήθηκε»
- Πώς να ξεκλειδώσετε τις Ρυθμίσεις για προχωρημένους
- Πώς να επιλύσετε την απενεργοποίηση του προϊόντος από το ESET HOME

Εάν το πρόβλημα που αντιμετωπίζετε δεν περιλαμβάνεται στην παραπάνω λίστα, δοκιμάστε μια αναζήτηση στις σελίδες Ηλεκτρονικής βοήθειας του ESET Internet Security.

Εάν δεν μπορείτε να βρείτε μια λύση στο πρόβλημα/ερώτημα στην Ηλεκτρονική βοήθεια του ESET Internet Security, μπορείτε να επισκεφτείτε τη Γνωσιακή βάση της ESET στο διαδίκτυο, η οποία ενημερώνεται τακτικά. Παρακάτω παρατίθενται σύνδεσμοι με τα πιο δημοφιλή άρθρα της Γνωσιακής βάσης:

- Πώς μπορώ να ανανεώσω την άδεια χρήσης μου;
- Έλαβα ένα σφάλμα ενεργοποίησης κατά την εγκατάσταση του προϊόντος ESET. Τι σημαίνει αυτό;
- Ενεργοποίηση του οικιακού προϊόντος ESET Windows χρησιμοποιώντας το όνομα χρήστη, τον κωδικό πρόσβασης ή το κλειδί άδειας χρήσης
- Κατάργηση εγκατάστασης ή επανεγκατάσταση του οικιακού προϊόντος ESET
- Έλαβα ένα μήνυμα ότι τελείωσε πρόωρα η εγκατάσταση του ESET
- Τι πρέπει να κάνω μετά από την ανανέωση της άδειάς μου; (Οικιακοί χρήστες)
- Τι θα συμβεί αν αλλάξω τη διεύθυνση ηλεκτρονικής αλληλογραφίας που χρησιμοποιώ;
- Μεταφορά του προϊόντος ESET σε έναν νέο υπολογιστή ή συσκευή
- Πώς μπορώ να εκκινήσω τα Windows σε Ασφαλή λειτουργία ή Ασφαλή λειτουργία με δυνατότητα λειτουργίας δικτύου

- Εξαίρεση ενός ασφαλούς ιστότοπου από τον αποκλεισμό
- Να επιτρέπεται η πρόσβαση για λογισμικό ανάγνωσης οθόνης στο γραφικό περιβάλλον χρήστη της ESET

Εάν χρειαστεί, μπορείτε να επικοινωνήσετε με την Τεχνική υποστήριξη για να υποβάλετε ερωτήσεις ή προβλήματα.

Πώς να ενημερώσετε το ESET Internet Security

Η ενημέρωση του ESET Internet Security μπορεί να εκτελείται με μη αυτόματο τρόπο ή αυτόματα. Για να ενεργοποιήσετε την ενημέρωση, κάντε κλικ στο στοιχείο **Ενημέρωση** στο κύριο παράθυρο του προγράμματος και, στη συνέχεια, κάντε κλικ στο στοιχείο **Έλεγχος για ενημερώσεις**.

Οι προεπιλεγμένες ρυθμίσεις εγκατάστασης δημιουργούν μια εργασία αυτόματης ενημέρωσης που εκτελείται σε ωριαία βάση. Αν θέλετε να αλλάξετε το χρονικό διάστημα, πλοηγηθείτε στο στοιχείο **Εργαλεία** > **Χρονοδιάγραμμα**.

Πώς να αφαιρέσετε έναν ιό από τον υπολογιστή σας

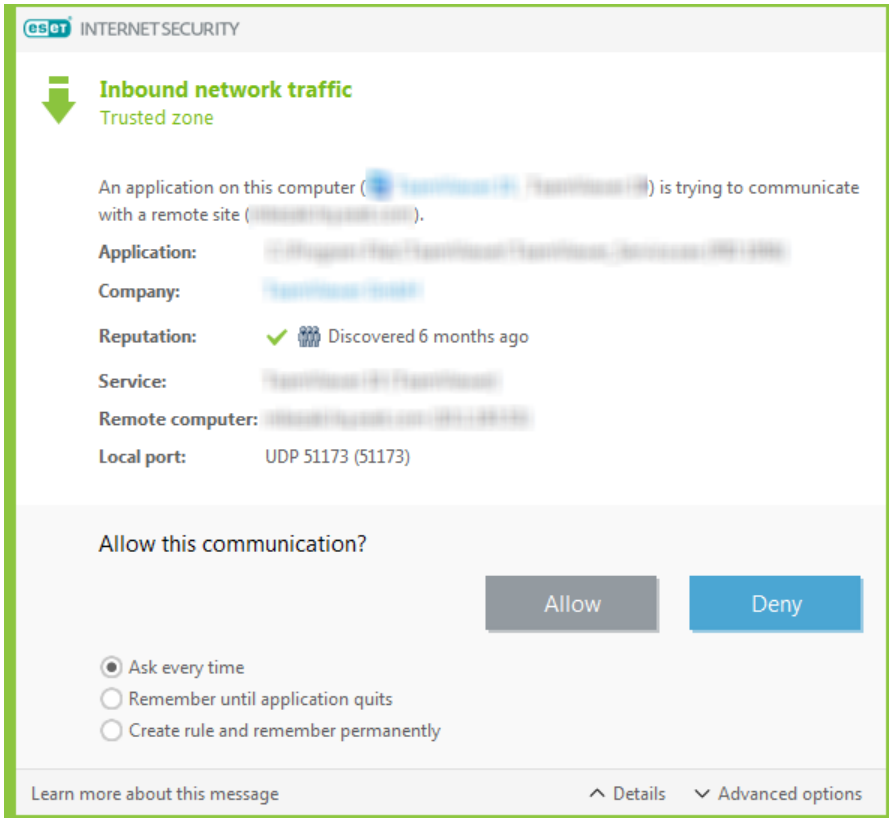
Αν ο υπολογιστής σας παρουσιάζει συμπτώματα μόλυνσης από κακόβουλο λογισμικό, π.χ. είναι πιο αργός, συχνά «παγώνει», συνιστάται να κάνετε τα ακόλουθα:

1. Στο κύριο παράθυρο του προγράμματος, κάντε κλικ στην επιλογή **Σάρωση υπολογιστή**.
2. Κάντε κλικ στο στοιχείο **Σάρωση του υπολογιστή σας** για να αρχίσει η σάρωση του συστήματός σας.
3. Όταν ολοκληρωθεί η σάρωση, κάντε μια ανασκόπηση στο αρχείο καταγραφής με τον αριθμό των σαρωμένων, μολυσμένων και καθαρισμένων αρχείων.
4. Αν επιθυμείτε να σαρώσετε μόνο ένα συγκεκριμένο μέρος του δίσκου σας, κάντε κλικ στην επιλογή **Προσαρμοσμένη σάρωση** και επιλέξτε τους προορισμούς που θέλετε να σαρωθούν για ιούς.

Για πρόσθετες πληροφορίες, ανατρέξτε στο άρθρο της Γνωσιακής βάσης της ESET που ενημερώνεται τακτικά.

Πώς να επιτρέπεται η επικοινωνία για μια συγκεκριμένη εφαρμογή

Αν έχει ανιχνευτεί μια νέα σύνδεση σε αλληλεπιδραστική λειτουργία και δεν υπάρχει αντίστοιχος κανόνας, θα σας ζητηθεί να επιτρέψετε ή να μην επιτρέψετε τη σύνδεση. Αν θέλετε το ESET Internet Security να εκτελεί την ίδια ενέργεια κάθε φορά που προσπαθεί η εφαρμογή να δημιουργήσει σύνδεση, επιλέξτε το πλαίσιο ελέγχου **Απομνημόνευση ενέργειας**.



Στη ρύθμιση του Τείχους προστασίας, μπορείτε να δημιουργήσετε νέους κανόνες Τείχους προστασίας για εφαρμογές προτού ανιχνευτούν από το ESET Internet Security. Ανοίξτε το κύριο παράθυρο του προγράμματος και επιλέξτε τα στοιχεία > **Ρυθμίσεις** > **Προστασία δικτύου** > Κάντε κλικ στο εικονίδιο ⚙ που βρίσκεται δίπλα στο στοιχείο **Τείχος προστασίας** > **Ρύθμιση παραμέτρων** > **Για προχωρημένους** > **Κανόνες** > **Επεξεργασία**.

Κάντε κλικ στο κουμπί **Προσθήκη** και στην καρτέλα **Γενικά**, εισαγάγετε το όνομα, την κατεύθυνση και το πρωτόκολλο επικοινωνίας για τον κανόνα. Αυτό το παράθυρο σάς επιτρέπει να καθορίσετε την ενέργεια που θα εκτελείται όταν εφαρμόζεται ο κανόνας.

Εισαγάγετε τη διαδρομή στο εκτελέσιμο αρχείο της εφαρμογής και στην τοπική θύρα επικοινωνίας στην καρτέλα **Τοπικά**. Κάντε κλικ στην καρτέλα **Απομακρυσμένα** για να εισαγάγετε την απομακρυσμένη διεύθυνση και θύρα (αν εφαρμόζεται). Ο κανόνας που μόλις δημιουργήσατε θα εφαρμοστεί μόλις προσπαθήσει η εφαρμογή να επικοινωνήσει ξανά.

Πώς να ενεργοποιείτε τον Γονικό έλεγχο για έναν λογαριασμό

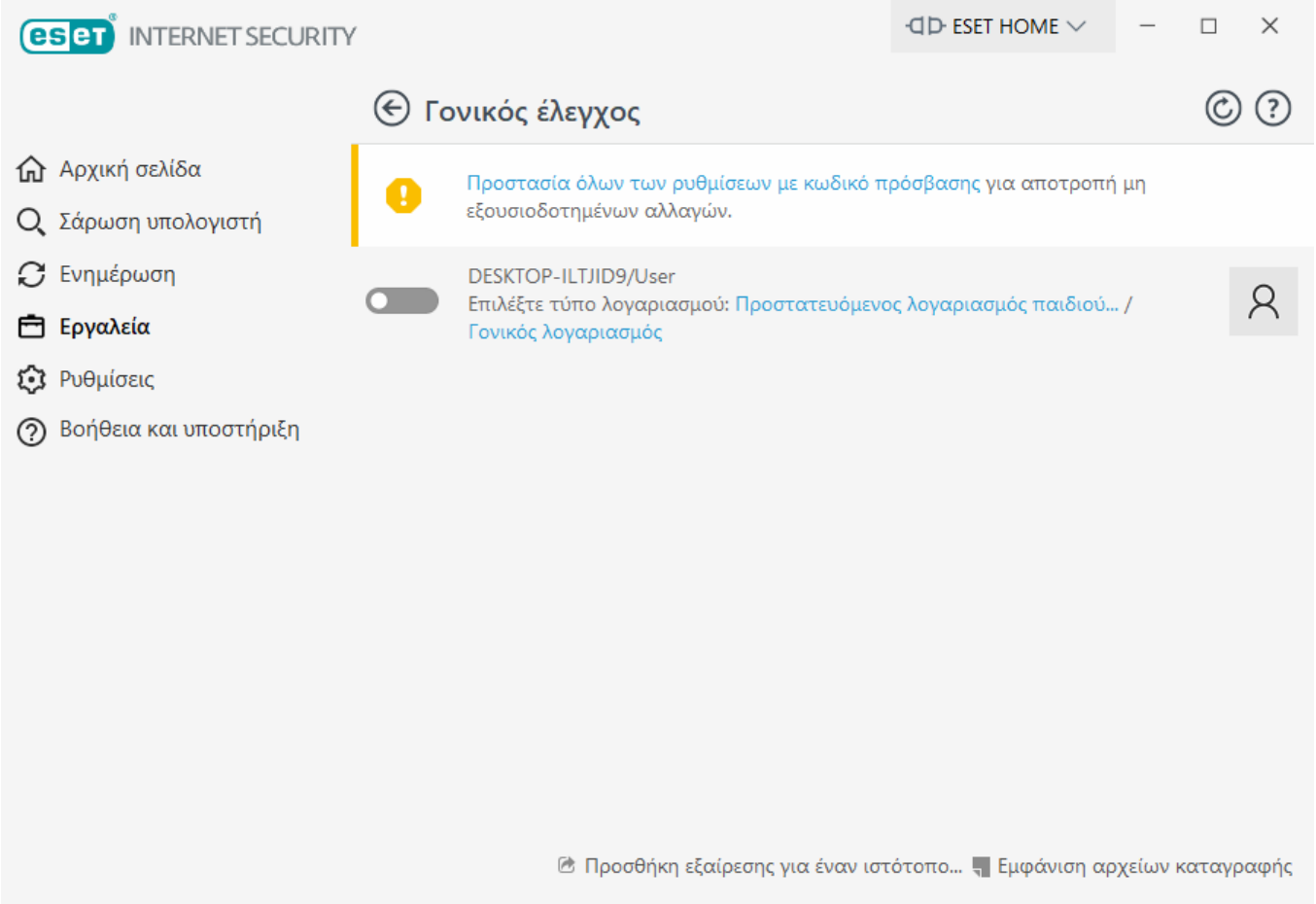
Για να ενεργοποίησετε τον Γονικό έλεγχο για ένα συγκεκριμένο λογαριασμό χρήστη, ακολουθήστε τα παρακάτω βήματα:

1. Ο Γονικός έλεγχος είναι απενεργοποιημένος από προεπιλογή στο ESET Internet Security. Υπάρχουν δύο μέθοδοι για την ενεργοποίηση του Γονικού ελέγχου:

   • Κάντε κλικ στο στοιχείο στη θέση **Ρυθμίσεις** > **Εργαλεία ασφαλείας** > **Γονικός έλεγχος** από το κύριο παράθυρο του προγράμματος και αλλάξτε την κατάσταση του Γονικού ελέγχου σε ενεργό.

• Πιέστε το πλήκτρο F5 για να αποκτήσετε πρόσβαση στη δομή **Εγκατάσταση για προχωρημένους**, μεταβείτε στο στοιχείο **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Γονικός έλεγχος** και, στη συνέχεια, ενεργοποιήστε το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Ενεργοποίηση Γονικού ελέγχου**.

2. Κάντε κλικ στα στοιχεία **Ρυθμίσεις** > **Εργαλεία ασφαλείας** > **Γονικός έλεγχος** από το κύριο παράθυρο του προγράμματος. Παρόλο που εμφανίζεται η ένδειξη **Ενεργοποιημένο** δίπλα από το στοιχείο **Γονικός έλεγχος**, πρέπει να ρυθμίσετε τις παραμέτρους για τον γονικό έλεγχο για το λογαριασμό που επιθυμείτε κάνοντας κλικ στο σύμβολο βέλους και στη συνέχεια επιλέγοντας στο επόμενο παράθυρο **Προστατευόμενος λογαριασμός παιδιού** ή **Γονικός λογαριασμός**. Στο επόμενο παράθυρο επιλέξτε την ημερομηνία γέννησης, για να προσδιοριστεί το επίπεδο πρόσβασης και οι συνιστώμενες ιστοσελίδες που είναι κατάλληλες για την ηλικία. Ο Γονικός έλεγχος θα είναι τώρα ενεργός για τον καθορισμένο λογαριασμό χρήστη. Κάντε κλικ στο στοιχείο **Αποκλεισμένο περιεχόμενο και ρυθμίσεις** κάτω από το όνομα λογαριασμού για να προσαρμόσετε τις κατηγορίες που θέλετε να επιτρέπονται ή να αποκλείονται στην καρτέλα Κατηγορίες. Για να επιτρέπονται ή να αποκλείονται προσαρμοσμένες ιστοσελίδες που δεν αντιστοιχούν σε μια κατηγορία, κάντε κλικ στην καρτέλα Εξαιρέσεις.



Πώς να δημιουργήσετε μια νέα εργασία στο Χρονοδιάγραμμα εργασιών

Για να δημιουργήσετε μια νέα εργασία στην ενότητα **Εργαλεία** > **Περισσότερα εργαλεία** > **Χρονοδιάγραμμα**, κάντε κλικ στην επιλογή **Προσθήκη** ή δεξί κλικ και επιλέξτε **Προσθήκη...** από το μενού περιβάλλοντος. Διατίθενται πέντε τύποι προγραμματισμένων εργασιών:

• **Εκτέλεση εξωτερικής εφαρμογής** – Προγραμματίζει την εκτέλεση μιας εξωτερικής εφαρμογής.

• **Συντήρηση αρχείου καταγραφής** – Τα αρχεία καταγραφής περιέχουν επίσης υπολείμματα από διαγραμμένες εγγραφές. Αυτή η εργασία βελτιστοποιεί σε τακτική βάση τις εγγραφές στα αρχεία καταγραφής, ώστε να λειτουργούν πιο αποτελεσματικά.

• **Έλεγχος αρχείων κατά την εκκίνηση του συστήματος** – Ελέγχει τα αρχεία που επιτρέπεται να εκτελούνται κατά την εκκίνηση του συστήματος ή τη σύνδεση του χρήστη.

• **Δημιουργία στιγμιότυπου κατάστασης του υπολογιστή** – Δημιουργεί ένα στιγμιότυπο ESET SysInspector του υπολογιστή – συγκεντρώνει λεπτομερείς πληροφορίες σχετικά με στοιχεία του συστήματος (π.χ. προγράμματα οδήγησης, εφαρμογές) και αξιολογεί το επίπεδο κινδύνου για κάθε στοιχείο.

• **Σάρωση υπολογιστή κατ' απαίτηση** – Πραγματοποιεί σάρωση αρχείων και φακέλων στον υπολογιστή σας.

• **Ενημέρωση** – Προγραμματίζει μια εργασία ενημέρωσης εκτελώντας ενημέρωση στις μονάδες.

Καθώς η **Ενημέρωση** είναι μία από τις προγραμματισμένες εργασίες που πραγματοποιούνται συχνότερα, παρακάτω θα σας εξηγήσουμε τον τρόπο με τον οποίο μπορείτε να προσθέσετε μια νέα εργασία ενημέρωσης:

Από το αναπτυσσόμενο μενού **Προγραμματισμένη εργασία**, επιλέξτε **Ενημέρωση**. Συμπληρώστε το όνομα της εργασίας στο πεδίο **Όνομα εργασίας** και κάντε κλικ στο κουμπί **Επόμενο**. Επιλέξτε τη συχνότητα της εργασίας. Οι διαθέσιμες επιλογές είναι οι παρακάτω: **Μία φορά**, **Επανειλημμένα**, **Καθημερινά**, **Εβδομαδιαία** και **Με συμβάν ενεργοποίησης**. Επιλέξτε **Παράλειψη της εργασίας κατά τη λειτουργία με μπαταρία**, για να ελαχιστοποιήσετε την κατανάλωση πόρων συστήματος όταν χρησιμοποιείτε φορητό υπολογιστή που τροφοδοτείται με μπαταρία. Η εργασία θα εκτελείται την ημέρα και ώρα που καθορίζεται στα πεδία **Εκτέλεση εργασίας**. Κατόπιν, καθορίστε την ενέργεια που θα πραγματοποιείται εάν δεν είναι δυνατή η πραγματοποίηση της εργασίας ή η ολοκλήρωσή της στον προγραμματισμένο χρόνο. Είναι διαθέσιμες οι παρακάτω επιλογές:

• **Την επόμενη προγραμματισμένη φορά**

• **Το συντομότερο δυνατό**

• **Αμέσως, εάν ο χρόνος από την τελευταία εκτέλεση υπερβαίνει μια καθορισμένη τιμή** (μπορείτε να καθορίσετε το διάστημα χρησιμοποιώντας το πλαίσιο κύλισης **Χρόνος από την τελευταία εκτέλεση (ώρες)**)

Στο επόμενο βήμα, εμφανίζεται ένα παράθυρο με πληροφορίες σχετικά με την τρέχουσα προγραμματισμένη εργασία. Κάντε κλικ στο κουμπί **Τέλος** όταν ολοκληρώσετε τις αλλαγές.

Θα εμφανιστεί ένα παράθυρο διαλόγου το οποίο θα σας επιτρέπει να επιλέξετε τα προφίλ που θα χρησιμοποιούνται για την προγραμματισμένη εργασία. Εδώ μπορείτε να καθορίσετε το κύριο και το εναλλακτικό προφίλ. Το εναλλακτικό προφίλ θα χρησιμοποιείται όταν η εργασία δεν θα είναι δυνατό να ολοκληρωθεί με το κύριο προφίλ. Επιβεβαιώστε τις ρυθμίσεις σας κάνοντας κλικ στο κουμπί **Τέλος** και η νέα προγραμματισμένη εργασία θα προστεθεί στη λίστα με τις τρέχουσες προγραμματισμένες εργασίες.

Πώς να προγραμματίσετε μια εβδομαδιαία εργασία σάρωσης

Για να προγραμματίσετε μια τακτική εργασία, ανοίξτε το κύριο παράθυρο του προγράμματος και κάντε κλικ στα στοιχεία **Εργαλεία** > **Περισσότερα εργαλεία** > **Προγραμματισμός εργασιών**. Παρακάτω θα βρείτε έναν σύντομο οδηγό σχετικά με τον τρόπο που μπορείτε να προγραμματίσετε μια εργασία που θα σαρώνει τις τοπικές μονάδες δίσκου σας κάθε εβδομάδα. Ανατρέξτε στο άρθρο της Γνωσιακής βάσης για πιο λεπτομερείς οδηγίες.

Για να προγραμματίσετε μια εργασία σάρωσης:

1. Κάντε κλικ στο στοιχείο **Προσθήκη** στην κύρια οθόνη του Χρονοδιαγράμματος.

2. Εισαγάγετε ένα όνομα για την εργασία και επιλέξτε το στοιχείο **Σάρωση υπολογιστή κατ' απαίτηση** από το αναπτυσσόμενο μενού **Τύπος εργασίας**.

3. Επιλέξτε **Εβδομαδιαίως** για τη συχνότητα της εργασίας.

4. Καθορίστε την ημέρα και την ώρα εκτέλεσης της εργασίας.

5. Επιλέξτε **Εκτέλεση της εργασίας όσο το δυνατό συντομότερα** για να πραγματοποιηθεί η εργασία αργότερα, εάν η προγραμματισμένη εργασία δεν εκτελεστεί για οποιονδήποτε λόγο (για παράδειγμα, εάν ο υπολογιστής είναι απενεργοποιημένος).

6. Ελέγξτε την περίληψη της προγραμματισμένης εργασίας και κάντε κλικ στο στοιχείο **Τέλος**.

7. Από το αναπτυσσόμενο μενού **Προορισμοί**, επιλέξτε **Τοπικές μονάδες**.

8. Κάντε κλικ στο στοιχείο **Τέλος** για εφαρμογή της εργασίας.

Πώς να επιλύσετε το σφάλμα «Η Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών δεν ήταν δυνατόν να ανακατευθυνθεί στη ιστοσελίδα που ζητήθηκε»

Χρησιμοποιήστε την επιλογή «Προστασία όλων των προγραμμάτων περιήγησης» αντί για ανακατεύθυνση στον ιστότοπο

Από προεπιλογή, η Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών ξεκινά στο πρόγραμμα περιήγησης που χρησιμοποιείται αυτήν τη στιγμή μετά την επίσκεψη σε γνωστό ιστότοπο τραπεζικών συναλλαγών. Αντί για ανακατεύθυνση στον ιστότοπο, μπορείτε να χρησιμοποιήσετε την επιλογή «Προστασία όλων των προγραμμάτων περιήγησης» για να ξεκινήσετε όλα τα υποστηριζόμενα προγράμματα περιήγησης σε ασφαλή λειτουργία. Αυτό σάς επιτρέπει να περιηγηθείτε στο διαδίκτυο, να αποκτήσετε πρόσβαση σε τραπεζικές συναλλαγές μέσω Internet και να πραγματοποιήσετε ηλεκτρονικές συναλλαγές χωρίς ανακατεύθυνση σε ένα παράθυρο ασφαλούς προγράμματος περιήγησης.

Για να χρησιμοποιήσετε την επιλογή Προστασίας όλων των προγραμμάτων περιήγησης, ανοίξτε το κύριο παράθυρο του προγράμματος, μεταβείτε στα στοιχεία **Ρυθμίσεις** > **Εργαλεία ασφαλείας** και ενεργοποιήστε το ρυθμιστικό που βρίσκεται δίπλα στο στοιχείο **Προστασία όλων των προγραμμάτων περιήγησης**.

Για να επιλυθεί το σφάλμα ανακατεύθυνσης στον ιστότοπο, ακολουθήστε τις παρακάτω οδηγίες:

Αφού ολοκληρώσετε το κάθε βήμα, ελέγξτε εάν λειτουργεί η «Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών»

Εάν εξακολουθεί να μη λειτουργεί το παράθυρο του προγράμματος περιήγησης, ολοκληρώστε το επόμενο βήμα μέχρι να λειτουργήσει ξανά.

1. Πραγματοποιήστε επανεκκίνηση του υπολογιστή σας.

2. Βεβαιωθείτε ότι χρησιμοποιείτε την πιο πρόσφατη έκδοση του λειτουργικού συστήματος Windows και του ESET Internet Security: Αναβάθμιση των οικιακών προϊόντων της ESET για Windows στην πιο πρόσφατη έκδοση.

3. Ενδέχεται να υπάρχει σύγκρουση με το λογισμικό ασφάλειας άλλων κατασκευαστών, με το VPN ή με το τείχος προστασίας που χρησιμοποιείτε. Απενεργοποιήστε προσωρινά ή καταργήστε την εγκατάσταση αυτού του λογισμικού.

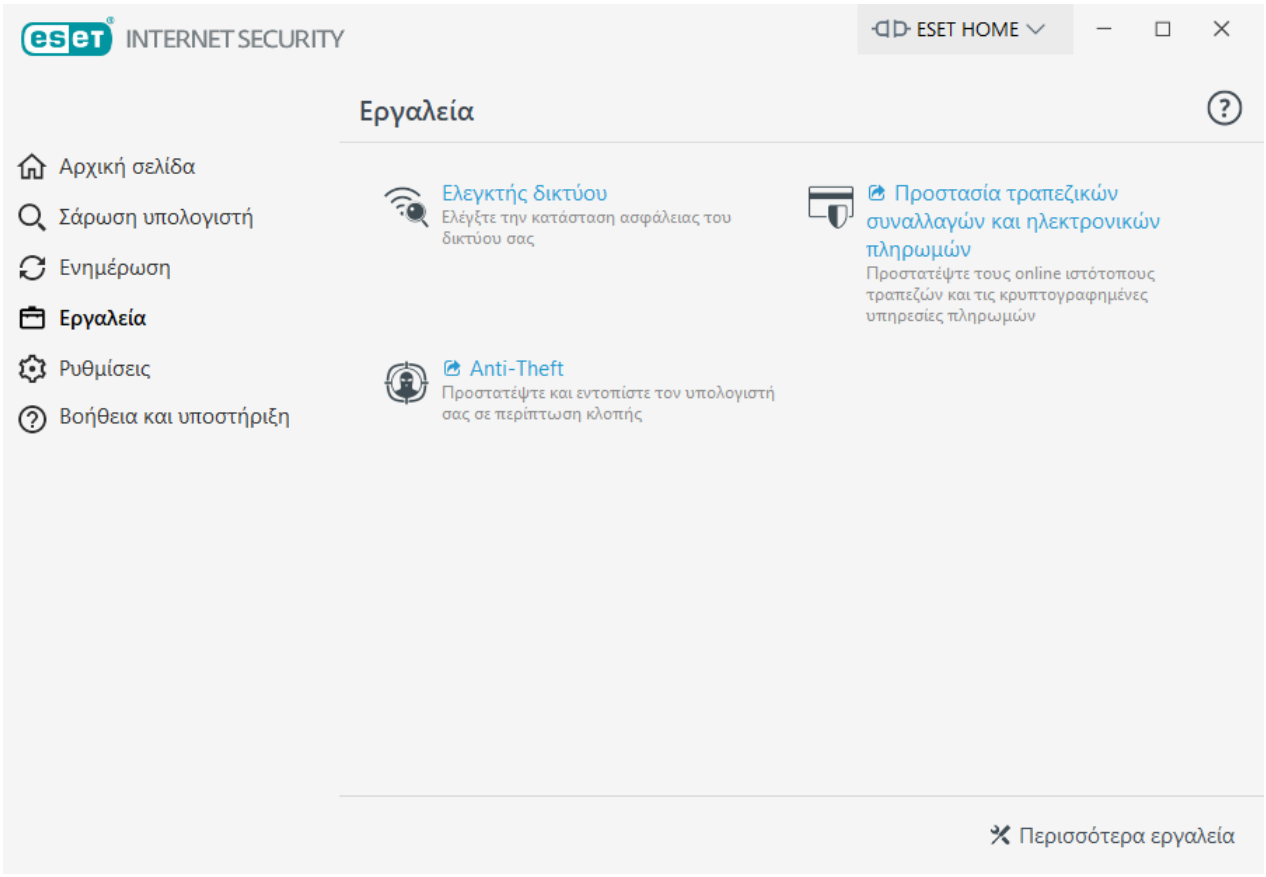
4. Απενεργοποιήστε όλες τις επεκτάσεις άλλων κατασκευαστών στο πρόγραμμα περιήγησης.

5. Εκκαθαρίστε την προσωρινή μνήμη του προγράμματος περιήγησης. Πώς μπορώ να κάνω εκκαθάριση της προσωρινής μνήμης του Firefox ή εκκαθάριση της προσωρινής μνήμης του Google Chrome στο πρόγραμμα περιήγησής μου;

6. Βεβαιωθείτε ότι το προεπιλεγμένο πρόγραμμα περιήγησης δεν έχει εξαιρεθεί στη διαδρομή **Εγκατάσταση για προχωρημένους** > **Διαδίκτυο και ηλεκτρονική αλληλογραφία** > **Φιλτράρισμα πρωτοκόλλων** > **Αποκλεισμένες εφαρμογές**. Αποκτήστε πρόσβαση στην Εγκατάσταση για προχωρημένους.

7. Εάν δεν αναβαθμίσατε το προϊόν ESET στα προηγούμενα βήματα, καταργήστε την εγκατάσταση και εγκαταστήστε ξανά το προϊόν ESET. Επανεκκινήστε τον υπολογιστή σας μετά την εγκατάσταση.

8. Εάν το πρόβλημα παραμένει, μπορείτε να ενεργοποιήσετε την επιλογή «Προστασία όλων των προγραμμάτων περιήγησης» ή να αποκτήσετε πρόσβαση στο ασφαλές πρόγραμμα περιήγησης από το κύριο παράθυρο του προγράμματος > **Εργαλεία** > **Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών**.



Η Προστασία τραπεζικών πληρωμών είναι ένα πρόσθετο επίπεδο προστασίας που έχει σχεδιαστεί για να προστατεύει τα οικονομικά δεδομένα σας κατά τη διάρκεια ηλεκτρονικών συναλλαγών.

Στις περισσότερες περιπτώσεις, μόλις επισκεφτείτε έναν γνωστό ιστότοπο τραπεζικών συναλλαγών, εκκινεί το ασφαλές πρόγραμμα περιήγησης για την Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών στο τρέχον πρόγραμμα περιήγησης.

Ορίστε μία από τις ακόλουθες επιλογές ρύθμισης παραμέτρων συμπεριφοράς του ασφαλούς προγράμματος περιήγησης:

• **Προστασία όλων των προγραμμάτων περιήγησης** - Εάν ενεργοποιηθεί, όλα τα υποστηριζόμενα προγράμματα περιήγησης εκκινούν σε ασφαλή λειτουργία. Αυτό σας επιτρέπει να περιηγηθείτε στο διαδίκτυο, να αποκτήσετε πρόσβαση σε τραπεζικές συναλλαγές στο διαδίκτυο και να πραγματοποιήσετε ηλεκτρονικές αγορές και συναλλαγές σε ένα παράθυρο ασφαλούς προγράμματος περιήγησης χωρίς ανακατεύθυνση.

• **Ανακατεύθυνση ιστότοπων** (προεπιλογή) - Ιστότοποι από μια λίστα προστατευμένων ιστότοπων και εσωτερική λίστα τραπεζικών συναλλαγών στο διαδίκτυο ανακατευθύνουν στο ασφαλές πρόγραμμα περιήγησης. Μπορείτε να επιλέξετε το πρόγραμμα περιήγησης (τυπικό ή ασφαλές) που θα ανοίξει.

• Οι δύο προηγούμενες επιλογές είναι απενεργοποιημένες - Για να αποκτήσετε πρόσβαση σε ένα ασφαλές πρόγραμμα περιήγησης στο ESET Internet Security, κάντε κλικ στα στοιχεία **Εργαλεία** > **Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών** ή κάντε κλικ στο εικονίδιο της επιφάνειας εργασίας **Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών**. Το πρόγραμμα περιήγησης που έχει ρυθμιστεί ως προεπιλεγμένο

στα Windows εκκινεί σε ασφαλή λειτουργία.

Για να ρυθμίσετε τις παραμέτρους της συμπεριφοράς του ασφαλούς προγράμματος περιήγησης, ανατρέξτε στο θέμα Ρυθμίσεις για προχωρημένους της Προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών. Για να ενεργοποιήσετε τη δυνατότητα «Προστασία όλων των προγραμμάτων περιήγησης» στο ESET Internet Security, κάντε κλικ στο στοιχείο **Ρυθμίσεις** > **Εργαλεία ασφαλείας** και ενεργοποιήστε το ρυθμιστικό **Προστασία όλων των προγραμμάτων περιήγησης**.

Η χρήση κρυπτογραφημένης επικοινωνίας HTTPS είναι απαραίτητη για την πραγματοποίηση προστατευόμενης περιήγησης. Τα παρακάτω προγράμματα περιήγησης υποστηρίζουν την Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών:

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

Για περισσότερες λεπτομέρειες σχετικά με τις δυνατότητες προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών, ανατρέξτε στο άρθρο της Γνωσιακής βάσης της ESET που είναι διαθέσιμο στα Αγγλικά και αρκετές άλλες γλώσσες:

- Πώς μπορώ να χρησιμοποιήσω την προστασία τραπεζικών πληρωμών της ESET;
- Ενεργοποίηση ή απενεργοποίηση της Προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών ESET για έναν συγκεκριμένο ιστότοπο
- Παύση ή απενεργοποίηση της Προστασίας τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών της ESET σε οικιακά προϊόντα για Windows
- Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών της ESET –συνήθη σφάλματα
- Γλωσσάρι της ESET | Προστασία τραπεζικών συναλλαγών και ηλεκτρονικών πληρωμών

Εάν εξακολουθείτε να μην μπορείτε να επιλύσετε το πρόβλημα, επικοινωνήστε με email με την Τεχνική υποστήριξη της ESET.

Πώς να ξεκλειδώσετε τις Ρυθμίσεις για προχωρημένους με προστασία με κωδικό πρόσβασης

Εάν θέλετε να αποκτήσετε πρόσβαση στην προστατευμένη Εγκατάσταση για προχωρημένους, εμφανίζεται το παράθυρο για την εισαγωγή του κωδικού πρόσβασης. Εάν ξεχάσετε ή χάσετε τον κωδικό πρόσβασής σας, κάντε κλικ στο στοιχείο **Επαναφορά κωδικού πρόσβασης** και πληκτρολογήστε τη διεύθυνση email που χρησιμοποιήσατε για την εγγραφή της άδειας χρήσης. Η ESET θα σας στείλει ένα email με τον κωδικό επαλήθευσης. Πληκτρολογήστε τον κωδικό επαλήθευσης και,

στη συνέχεια, γράψτε και επιβεβαιώστε τον νέο κωδικό πρόσβασης. Ο κωδικός επαλήθευσης είναι έγκυρος για επτά ημέρες.

Επαναφορά κωδικού πρόσβασης μέσω του λογαριασμού ESET HOME – Χρησιμοποιήστε αυτήν την επιλογή εάν η άδεια χρήσης που χρησιμοποιήθηκε για ενεργοποίηση συσχετίζεται με τον λογαριασμό σας στο ESET HOME. Πληκτρολογήστε τη διεύθυνση email που χρησιμοποιείτε για να συνδεθείτε στον λογαριασμό σας στο ESET HOME.

Εάν δεν μπορείτε να θυμηθείτε τη διεύθυνση email σας ή αντιμετωπίζετε δυσκολίες με την επαναφορά του κωδικού πρόσβασης, κάντε κλικ στο στοιχείο **Επικοινωνία με την Τεχνική υποστήριξη**. Θα ανακατευθυνθείτε στον ιστότοπο της ESET για να επικοινωνήσετε με το τμήμα Τεχνικής Υποστήριξης.

Δημιουργία κωδικού για την Τεχνική υποστήριξη – Αυτή η επιλογή δημιουργεί έναν κωδικό για την Τεχνική υποστήριξη. Αντιγράψτε τον κωδικό που παρέχεται από την Τεχνική υποστήριξη και κάντε κλικ στο στοιχείο **Έχω κωδικό επαλήθευσης**. Πληκτρολογήστε τον κωδικό επαλήθευσης και, στη συνέχεια, γράψτε και επιβεβαιώστε τον νέο κωδικό πρόσβασης. Ο κωδικός επαλήθευσης είναι έγκυρος για επτά ημέρες.

Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα Ξεκλείδωμα του κωδικού ρυθμίσεων στα οικιακά προϊόντα της ESET για Windows.

Πώς να επιλύσετε την απενεργοποίηση του προϊόντος από το ESET HOME

Το προϊόν δεν έχει ενεργοποιηθεί

Αυτό το μήνυμα σφάλματος εμφανίζεται όταν ο κάτοχος της άδειας χρήσης απενεργοποιεί το ESET Internet Security από την πύλη ESET HOME ή εάν διακοπεί η κοινή χρήση της άδειας χρήσης με το λογαριασμό σας στο ESET HOME. Για να επιλύσετε αυτό το ζήτημα:

- Κάντε κλικ στο στοιχείο **Ενεργοποίηση** και χρησιμοποιήστε μία από τις μεθόδους ενεργοποίησης για να ενεργοποιήσετε το ESET Internet Security.

- Επικοινωνήστε με τον κάτοχο της άδειας χρήσης και ενημερώστε ότι το ESET Internet Security απενεργοποιήθηκε από τον κάτοχο της άδειας χρήσης ή ότι διακόπηκε η κοινή χρήση της άδειας χρήσης. Ο κάτοχος μπορεί να επιλύσει το πρόβλημα στην ESET HOME.

Το προϊόν απενεργοποιήθηκε, η συσκευή αποσυνδέθηκε

Αυτό το μήνυμα σφάλματος εμφανίζεται μετά την κατάργηση μιας συσκευής από την ESET HOME. Για να επιλύσετε αυτό το ζήτημα:

- Κάντε κλικ στο στοιχείο **Ενεργοποίηση** και χρησιμοποιήστε μία από τις μεθόδους ενεργοποίησης για να ενεργοποιήσετε το ESET Internet Security.

- Επικοινωνήστε με τον κάτοχο της άδειας χρήσης και ενημερώστε ότι το ESET Internet Security απενεργοποιήθηκε και ότι η συσκευή αποσυνδέθηκε από το ESET HOME.

• Εάν είστε ο κάτοχος της άδειας χρήσης και δεν γνωρίζετε αυτές τις αλλαγές, ελέγξτε τη ροή δραστηριότητας της ESET HOME. Εάν εντοπίσετε οποιαδήποτε ύποπτη δραστηριότητα, αλλάξτε τον κωδικό πρόσβασης του λογαριασμού σας στο ESET HOME και επικοινωνήστε με την Τεχνική υποστήριξη της ESET.

Το προϊόν απενεργοποιήθηκε, η συσκευή αποσυνδέθηκε

Αυτό το μήνυμα σφάλματος εμφανίζεται μετά την κατάργηση μιας συσκευής από την ESET HOME. Για να επιλύσετε αυτό το ζήτημα:

• Κάντε κλικ στο στοιχείο **Ενεργοποίηση** και χρησιμοποιήστε μία από τις μεθόδους ενεργοποίησης για να ενεργοποιήσετε το ESET Internet Security.

• Επικοινωνήστε με τον κάτοχο της άδειας χρήσης και ενημερώστε ότι το ESET Internet Security απενεργοποιήθηκε και ότι η συσκευή αποσυνδέθηκε από το ESET HOME.

• Εάν είστε ο κάτοχος της άδειας χρήσης και δεν γνωρίζετε αυτές τις αλλαγές, ελέγξτε τη ροή δραστηριότητας της ESET HOME. Εάν εντοπίσετε οποιαδήποτε ύποπτη δραστηριότητα, αλλάξτε τον κωδικό πρόσβασης του λογαριασμού σας στο ESET HOME και επικοινωνήστε με την Τεχνική υποστήριξη της ESET.

Το προϊόν δεν έχει ενεργοποιηθεί

Αυτό το μήνυμα σφάλματος εμφανίζεται όταν ο κάτοχος της άδειας χρήσης απενεργοποιεί το ESET Internet Security από την πύλη ESET HOME ή εάν διακοπεί η κοινή χρήση της άδειας χρήσης με το λογαριασμό σας στο ESET HOME. Για να επιλύσετε αυτό το ζήτημα:

• Κάντε κλικ στο στοιχείο **Ενεργοποίηση** και χρησιμοποιήστε μία από τις μεθόδους ενεργοποίησης για να ενεργοποιήσετε το ESET Internet Security.

• Επικοινωνήστε με τον κάτοχο της άδειας χρήσης και ενημερώστε ότι το ESET Internet Security απενεργοποιήθηκε από τον κάτοχο της άδειας χρήσης ή ότι διακόπηκε η κοινή χρήση της άδειας χρήσης. Ο κάτοχος μπορεί να επιλύσει το πρόβλημα στην ESET HOME.

Πρόγραμμα βελτίωσης εμπειρίας του πελάτη

Με τη συμμετοχή σας στο Πρόγραμμα βελτίωσης εμπειρίας του πελάτη παρέχετε στην ESET ανώνυμες πληροφορίες σχετικά με τη χρήση των προϊόντων της. Περισσότερες πληροφορίες σχετικά με την επεξεργασία δεδομένων είναι διαθέσιμες στην Πολιτική απορρήτου.

Η συγκατάθεσή σας

Η συμμετοχή στο πρόγραμμα είναι εθελοντική και απαιτεί τη συγκατάθεσή σας. Στη συνέχεια, η συμμετοχή σας είναι παθητική. Αυτό σημαίνει ότι δεν χρειάζεται να κάνετε κάτι άλλο. Μπορείτε να ανακαλέσετε τη συγκατάθεσή σας αλλάζοντας τις ρυθμίσεις προϊόντος ανά πάσα στιγμή. Με αυτό τον τρόπο δεν θα επιτρέπεται πλέον στην εταιρεία να επεξεργαστεί περαιτέρω τα ανώνυμα δεδομένα

σας.

Μπορείτε να ανακαλέσετε τη συγκατάθεσή σας αλλάζοντας τις ρυθμίσεις προϊόντος ανά πάσα στιγμή

- Αλλαγή των ρυθμίσεων του Προγράμματος βελτίωσης εμπειρίας του πελάτη στα οικιακά προϊόντα της ESET για Windows

Τι είδους πληροφορίες συλλέγουμε;

Δεδομένα σχετικά με την αλληλεπίδραση με το προϊόν

Με αυτές οι πληροφορίες μαθαίνουμε περισσότερα για τον τρόπο που χρησιμοποιούνται τα προϊόντα μας. Χάρη σε αυτές τις πληροφορίες, γνωρίζουμε για παράδειγμα ποιες λειτουργικότητες χρησιμοποιούνται συχνά, ποιες ρυθμίσεις τροποποιούν οι χρήστες ή πόση ώρα αναλώνουν στη χρήση του προϊόντος.

Δεδομένα σχετικά με τις συσκευές

Συλλέγουμε αυτές τις πληροφορίες για να κατανοήσουμε πού και σε ποιες συσκευές χρησιμοποιούνται τα προϊόντα μας. Τυπικά παραδείγματα είναι το μοντέλο συσκευής, η χώρα, η έκδοση και η ονομασία του λειτουργικού συστήματος.

Δεδομένα διαγνωστικού ελέγχου σφαλμάτων

Επίσης, συλλέγονται πληροφορίες σχετικά με τα περιστατικά σφάλματος και διακοπής λειτουργίας. Για παράδειγμα, ποιο σφάλμα προέκυψε και τις ενέργειες που οδήγησαν σε αυτό.

Γιατί συλλέγουμε αυτές τις πληροφορίες;

Αυτές οι ανώνυμες πληροφορίες μάς επιτρέπουν να βελτιώσουμε τα προϊόντα μας για τους χρήστες μας. Μας βοηθούν να βελτιώνουμε τη σχετικότητα των προϊόντων μας και να γίνονται όσο το δυνατόν πιο εύκολα στη χρήση και χωρίς σφάλματα.

Ποιος ελέγχει αυτές τις πληροφορίες;

Η ESET, spol. s r.o. είναι ο μοναδικός ελεγκτής των δεδομένων που συλλέγονται στο πλαίσιο του προγράμματος. Οι πληροφορίες αυτές δεν κοινοποιούνται σε τρίτους.

Άδεια Χρήσης Τελικού Χρήστη

Ισχύει από 19 Οκτωβρίου 2021.

ΣΗΜΑΝΤΙΚΟ: Διαβάστε προσεκτικά τους όρους και τις προϋποθέσεις εφαρμογής του προϊόντος που ορίζονται παρακάτω πριν κάνετε λήψη, εγκατάσταση, αντιγραφή ή χρήση **ΜΕ ΤΗ ΛΗΨΗ, ΕΓΚΑΤΑΣΤΑΣΗ, ΑΝΤΙΓΡΑΦΗ Η ΧΡΗΣΗ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΔΗΛΩΝΕΤΕ ΤΗ ΣΥΓΚΑΤΑΘΕΣΗ ΣΑΣ ΣΕ ΑΥΤΟΥΣ ΤΟΥΣ ΟΡΟΥΣ ΚΑΙ ΤΙΣ ΠΡΟΫΠΟΘΕΣΕΙΣ ΚΑΙ ΑΝΑΓΝΩΡΙΖΕΤΕ ΤΗΝ ΠΟΛΙΤΙΚΗ ΑΠΟΡΡΗΤΟΥ.**

Συμφωνία Άδειας Χρήσης Τελικού Χρήστη

Σύμφωνα με τους όρους της Συμφωνίας Άδειας Χρήσης Τελικού Χρήστη («Συμφωνία») που εκτελέστηκε από και ανάμεσα στην ESET, spol. s r. o., με έδρα στη διεύθυνση Einsteinova 24, 85101 Bratislava, Slovak Republic, εγγεγραμμένη στο Εμπορικό Μητρώο δικαιοδοσίας του Πρώτου Πρωτοδικείου της Μπρατισλάβας, ενότητα Sro, με αριθμό 3586/B, Αριθμός μητρώου επιχειρήσεων: 31333532 («ESET» ή «ο Πάροχος») και τον χρήστη, φυσικό ή νομικό πρόσωπο (ο «Χρήστης» ή ο «Τελικός χρήστης»), ο χρήστης δικαιούται να χρησιμοποιεί το Λογισμικό που ορίζεται στο Άρθρο 1 της παρούσας Συμφωνίας. Το Λογισμικό που ορίζεται στο Άρθρο 1 αυτής της Συμφωνίας μπορεί να αποθηκευτεί σε φορέα δεδομένων, να αποσταλεί μέσω ηλεκτρονικού ταχυδρομείου, να ληφθεί από το Διαδίκτυο, να ληφθεί από τους διακομιστές του Παρόχου ή να αποκτηθεί από άλλες πηγές, σύμφωνα με τους όρους και τις προϋποθέσεις που καθορίζονται παρακάτω.

ΤΟ ΠΑΡΟΝ ΕΙΝΑΙ ΜΙΑ ΣΥΜΦΩΝΙΑ ΣΧΕΤΙΚΑ ΜΕ ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΤΕΛΙΚΟΥ ΧΡΗΣΤΗ ΚΑΙ ΔΕΝ ΑΠΟΤΕΛΕΙ ΣΥΜΦΩΝΙΑ ΓΙΑ ΠΩΛΗΣΗ. Ο Πάροχος εξακολουθεί να έχει την ιδιοκτησία του αντιγράφου του Λογισμικού και του φυσικού μέσου που περιέχεται στο πακέτο πώλησης και οποιαδήποτε άλλα αντίγραφα τα οποία εξουσιοδοτείται να δημιουργήσει ο Τελικός χρήστης σύμφωνα με την παρούσα Συμφωνία.

Εάν ο χρήστης κάνει κλικ στην επιλογή «Συμφωνώ» ή «Συμφωνώ...» κατά την εγκατάσταση, λήψη, αντιγραφή ή χρήση του Λογισμικού, συμφωνεί με τους όρους και τις προϋποθέσεις της παρούσας Συμφωνίας και της Πολιτικής απορρήτου. Εάν ο χρήστης δεν συμφωνεί με όλους τους όρους και τις προϋποθέσεις της παρούσας Συμφωνίας ή/και της Πολιτικής απορρήτου, πρέπει να κάνει αμέσως κλικ στην επιλογή ακύρωσης, να ακυρώσει την εγκατάσταση ή τη λήψη, ή να καταστρέψει ή να επιστρέψει το λογισμικό, το μέσο εγκατάστασης, τη συνοδευτική τεκμηρίωση και την απόδειξη πώλησης στον Πάροχο ή στο σημείο μεταπώλησης από το οποίο προμηθεύτηκε το Λογισμικό.

ΒΕΒΑΙΩΝΕΤΕ ΟΤΙ Η ΧΡΗΣΗ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΕΚ ΜΕΡΟΥΣ ΣΑΣ ΔΗΛΩΝΕΙ ΟΤΙ ΕΧΕΤΕ ΔΙΑΒΑΣΕΙ ΤΗΝ ΠΑΡΟΥΣΑ ΣΥΜΦΩΝΙΑ, ΤΗΝ ΚΑΤΑΝΟΕΙΤΕ ΚΑΙ ΑΠΟΔΕΧΕΣΤΕ ΟΤΙ ΔΕΣΜΕΥΕΣΤΕ ΑΠΟ ΤΟΥΣ ΟΡΟΥΣ ΚΑΙ ΤΙΣ ΠΡΟΫΠΟΘΕΣΕΙΣ ΤΗΣ.

1. **Λογισμικό**. Ο όρος "Λογισμικό", όπως χρησιμοποιείται στην παρούσα Συμφωνία, σημαίνει: (i) το πρόγραμμα υπολογιστή που συνοδεύεται από αυτήν τη Συμφωνία και όλα τα στοιχεία του, (ii) όλα τα περιεχόμενα των δίσκων, CD-ROM, DVD, μηνυμάτων ηλεκτρονικού ταχυδρομείου και οποιαδήποτε συνημμένα, ή άλλα μέσα με τα οποία παρέχεται η παρούσα Συμφωνία, συμπεριλαμβανομένης της μορφής του αντικειμενικού κώδικα του Λογισμικού που παρέχεται σε φορέα δεδομένων, μέσω ηλεκτρονικού ταχυδρομείου ή με λήψη μέσω του Διαδικτύου, (iii) οποιαδήποτε σχετικά επεξηγηματικά έγγραφα υλικά και οποιαδήποτε άλλη πιθανή τεκμηρίωση που σχετίζεται με το Λογισμικό, κυρίως οποιαδήποτε περιγραφή του Λογισμικού, των προδιαγραφών του, οποιαδήποτε περιγραφή των ιδιοτήτων ή της λειτουργίας του Λογισμικού, οποιαδήποτε περιγραφή του λειτουργικού περιβάλλοντος στο οποίο χρησιμοποιείται το Λογισμικό, οδηγίες για τη χρήση ή εγκατάσταση του Λογισμικού ή οποιαδήποτε περιγραφή σχετικά με τη χρήση του Λογισμικού («Τεκμηρίωση»), (iv) αντίγραφα του Λογισμικού, ενημερώσεις για πιθανά σφάλματα στο Λογισμικό, προσθήκες στο Λογισμικό, επεκτάσεις στο Λογισμικό, τροποποιημένες εκδόσεις του Λογισμικού και ενημερώσεις στοιχείων του Λογισμικού, αν υπάρχουν, που έχουν αδειοδοτηθεί σε εσάς από τον Πάροχο σύμφωνα με το Άρθρο 3 της παρούσας Συμφωνίας. Το Λογισμικό θα παρέχεται αποκλειστικά στη μορφή του εκτελέσιμου κώδικα αντικειμένου.

2. **Εγκατάσταση, Υπολογιστής και ένα Κλειδί άδειας χρήσης**. Το Λογισμικό, το οποίο παρέχεται σε φορέα δεδομένων, αποστέλλεται μέσω ηλεκτρονικού ταχυδρομείου, λαμβάνεται από το διαδίκτυο, λαμβάνεται από διακομιστές του Παρόχου ή αποκτάται από άλλες πηγές, απαιτεί εγκατάσταση. Πρέπει να εγκαταστήσετε το Λογισμικό σε σωστά διαμορφωμένο υπολογιστή, ο οποίος ικανοποιεί τουλάχιστον τις απαιτήσεις που ορίζονται στην Τεκμηρίωση. Ο τρόπος εγκατάστασης περιγράφεται στην Τεκμηρίωση. Δεν επιτρέπεται η εγκατάσταση προγραμμάτων ή υλικού, τα οποία θα μπορούσαν

να επηρεάσουν αρνητικά το Λογισμικό, στον υπολογιστή στον οποίο εγκαθιστάτε το Λογισμικό. Υπολογιστής σημαίνει το υλικό, συμπεριλαμβανομένων ενδεικτικά των προσωπικών υπολογιστών, φορητών υπολογιστών, σταθμών εργασίας, υπολογιστών χειρός, smartphone, ηλεκτρονικών συσκευών χειρός ή άλλων ηλεκτρονικών συσκευών για τις οποίες σχεδιάστηκε το Λογισμικό, στις οποίες θα εγκατασταθεί ή/και χρησιμοποιηθεί. Κλειδί άδειας χρήσης σημαίνει τη μοναδική ακολουθία συμβόλων, γραμμάτων, αριθμών ή ειδικών ενδείξεων που παρέχονται στον Τελικό χρήστη ώστε να επιτρέπεται η νόμιμη χρήση του Λογισμικού, η συγκεκριμένη έκδοση ή παράταση της διάρκειας της Άδειας χρήσης σύμφωνα με την παρούσα Συμφωνία.

3. **Άδεια χρήσης**. Με την προϋπόθεση ότι έχετε συμφωνήσει με τους όρους της παρούσας Συμφωνίας και ότι συμμορφώνεστε με όλους τους όρους και τις προϋποθέσεις που ορίζονται στο παρόν, ο Πάροχος σάς χορηγεί τα ακόλουθα δικαιώματα («η Άδεια χρήσης»):

α) **Εγκατάσταση και χρήση.** Θα έχετε μη αποκλειστικό, μη μεταβιβάσιμο δικαίωμα να εγκαταστήσετε το Λογισμικό στο σκληρό δίσκο υπολογιστή ή άλλου μόνιμου μέσου αποθήκευσης, εγκατάστασης και αποθήκευσης δεδομένων του Λογισμικού στη μνήμη ενός συστήματος υπολογιστή και να υλοποιήσετε, να αποθηκεύσετε και να προβάλετε το Λογισμικό.

β) **Ορισμός του αριθμού αδειών χρήσης.** Το δικαίωμα χρήσης του Λογισμικού θα περιορίζεται από τον αριθμό Τελικών χρηστών. Ένας Τελικός χρήστης θα θεωρείται ότι αναφέρεται στα παρακάτω: (i) εγκατάσταση του Λογισμικού σε ένα σύστημα υπολογιστή, ή (ii) αν ο βαθμός μιας άδειας χρήσης περιορίζεται στον αριθμό γραμματοκιβωτίων, τότε ένας Τελικός χρήστης θα θεωρείται ότι αναφέρεται σε έναν χρήστη υπολογιστή που αποδέχεται ηλεκτρονικό ταχυδρομείο μέσω ενός Φορέα Χρηστών Αλληλογραφίας (Mail User Agent) («ο MUA»). Αν ο MUA αποδέχεται ηλεκτρονικό ταχυδρομείο και στη συνέχεια το διανέμει αυτόματα σε πολλούς χρήστες, τότε ο αριθμός Τελικών χρηστών θα προσδιορίζεται σύμφωνα με τον πραγματικό αριθμό χρηστών για τους οποίους διανέμεται το ηλεκτρονικό ταχυδρομείο. Αν ένας διακομιστής αλληλογραφίας εκτελεί τη λειτουργία πύλης αλληλογραφίας, ο αριθμός Τελικών χρηστών θα ισούται με τον αριθμό χρηστών του διακομιστή αλληλογραφίας στους οποίους παρέχει υπηρεσίες η συγκεκριμένη πύλη. Αν ένας ακαθόριστος αριθμός διευθύνσεων ηλεκτρονικού ταχυδρομείου κατευθύνονται και γίνονται αποδεκτές από ένα χρήστη (π.χ. μέσω ψευδωνύμων) και τα μηνύματα δεν διανέμονται αυτόματα από την εφαρμογή-πελάτη σε μεγαλύτερο αριθμό χρηστών, θα απαιτείται μία Άδεια χρήσης για έναν υπολογιστή. Δεν πρέπει να χρησιμοποιείτε την ίδια Άδεια χρήσης ταυτόχρονα σε περισσότερους από έναν υπολογιστή. Ο Τελικός χρήστης δικαιούται να εισαγάγει το Κλειδί άδειας χρήσης στο Λογισμικό μόνο στο βαθμό κατά τον οποίο έχει δικαίωμα χρήσης του Λογισμικού σύμφωνα με τον περιορισμό που προκύπτει από τον αριθμό Αδειών χρήσης που του έχουν χορηγηθεί από τον Πάροχο. Το Κλειδί άδειας χρήσης θεωρείται εμπιστευτικό. Ο χρήστης δεν πρέπει να κοινοποιεί την Άδεια χρήσης σε τρίτους ή να επιτρέπει σε τρίτους να χρησιμοποιούν το Κλειδί άδειας χρήσης, παρά μόνο εφόσον επιτρέπεται από την παρούσα Συμφωνία ή τον Πάροχο. Εάν το Κλειδί άδειας χρήσης υποστεί παραβίαση, ειδοποιήστε αμέσως τον Πάροχο.

γ) **Οικιακή/Εταιρική έκδοση (Home/Business Edition).** Η Οικιακή έκδοση (Home Edition) του Λογισμικού θα χρησιμοποιείται αποκλειστικά σε ιδιωτικό ή/και μη εμπορικό περιβάλλον μόνο για οικιακή και οικογενειακή χρήση. Η Εταιρική έκδοση (Business Edition) του Λογισμικού πρέπει να αποκτάται για χρήση σε εμπορικό περιβάλλον, καθώς και για χρήση του Λογισμικού σε διακομιστές αλληλογραφίας, δρομολογητές αλληλογραφίας, πύλες αλληλογραφίας ή πύλες διαδικτύου.

δ) **Διάρκεια της Άδειας χρήσης.** Το δικαίωμά σας στη χρήση του Λογισμικού είναι χρονικά περιορισμένο.

ε) **Λογισμικό OEM.** Το Λογισμικό που ταξινομείται ως «OEM» θα περιορίζεται στον υπολογιστή με τον οποίο το προμηθεύτηκε ο χρήστης. Δεν μπορεί να μεταβιβαστεί σε διαφορετικό υπολογιστή.

στ) **Λογισμικό NFR, TRIAL.** Το λογισμικό που ταξινομείται ως «Όχι προς πώληση», NFR ή TRIAL δεν μπορεί να αντιστοιχιστεί για πληρωμή και πρέπει να χρησιμοποιείται μόνο για επίδειξη ή δοκιμή των λειτουργιών του Λογισμικού.

ζ) **Λήξη της Άδειας χρήσης.** Η Άδεια χρήσης θα λήξει αυτόματα στο τέλος του χρονικού διαστήματος για το οποίο χορηγήθηκε. Αν παραλείψετε να συμμορφωθείτε με οποιαδήποτε από τις διατάξεις αυτής της Συμφωνίας, ο Πάροχος θα δικαιούται να αποχωρήσει από τη Συμφωνία, με επιφύλαξη για οποιαδήποτε δικαίωμα ή νομική αποκατάσταση που έχει ο Πάροχος σε τέτοια ενδεχόμενο. Σε περίπτωση ακύρωσης της Άδειας χρήσης, πρέπει αμέσως να διαγράψετε, να καταστρέψετε ή να επιστρέψετε με δικά σας έξοδα το Λογισμικό και όλα τα αντίγραφα ασφαλείας στην ESET ή στο σημείο μεταπώλησης από το οποίο προμηθευτήκατε το Λογισμικό. Μετά τη λήξη της Άδειας χρήσης, ο Πάροχος θα δικαιούται επίσης να ακυρώσει το δικαίωμα του Τελικού χρήστη να χρησιμοποιεί τις λειτουργίες του Λογισμικού, οι οποίες απαιτούν σύνδεση στους διακομιστές του Παρόχου ή σε διακομιστές τρίτων.

4. **Λειτουργίες με συλλογή δεδομένων και απαιτήσεις σύνδεσης στο Internet.** Το Λογισμικό, για να λειτουργεί σωστά, απαιτεί σύνδεση στο διαδίκτυο και πρέπει να συνδέεται σε τακτά χρονικά διαστήματα με τους διακομιστές του Παρόχου ή διακομιστές τρίτων και την ισχύουσα συλλογή δεδομένων σύμφωνα με την Πολιτική Απορρήτου. Η σύνδεση στο διαδίκτυο και η ισχύουσα συλλογή δεδομένων είναι απαραίτητες για τις ακόλουθες λειτουργίες του Λογισμικού:

α) **Ενημερώσεις του Λογισμικού.** Ο Πάροχος θα δικαιούται να εκδίδει από καιρού εις καιρόν ενημερώσεις ή αναβαθμίσεις του Λογισμικού («Ενημερώσεις»), αλλά δεν θα υποχρεούται να παρέχει Ενημερώσεις. Η λειτουργία αυτή ενεργοποιείται από τις τυπικές ρυθμίσεις του Λογισμικού και, συνεπώς, οι Ενημερώσεις εγκαθίστανται αυτόματα, εκτός αν ο Τελικός χρήστης έχει απενεργοποιήσει την αυτόματη εγκατάσταση Ενημερώσεων. Για την παροχή Ενημερώσεων, απαιτείται η επαλήθευση ελέγχου ταυτότητας της Άδειας χρήσης, συμπεριλαμβανομένων πληροφοριών για τον υπολογιστή ή/και την πλατφόρμα στην οποία έχει εγκατασταθεί το Λογισμικό, σύμφωνα με την Πολιτική απορρήτου.

Η παροχή οποιωνδήποτε Ενημερώσεων ενδέχεται να υπόκειται στην Πολιτική Τέλους κύκλου ζωής («Πολιτική Τέλους κύκλου ζωής»), η οποία είναι διαθέσιμη στη διεύθυνση https://go.eset.com/eol_home. Δεν θα παρέχεται καμία Ενημέρωση, εφόσον επέλθει η ημερομηνία Τέλους κύκλου ζωής, όπως ορίζεται στην Πολιτική Τέλους κύκλου ζωής, του Λογισμικού ή οποιασδήποτε από τις δυνατότητές του.

β) **Προώθηση των εισβολών και πληροφοριών στον Πάροχο.** Το Λογισμικό περιέχει λειτουργίες οι οποίες συλλέγουν δείγματα ιών και άλλων επιβλαβών προγραμμάτων, καθώς και ύποπτων, προβληματικών, πιθανώς ανεπιθύμητων ή μη ασφαλών αντικειμένων όπως αρχεία, διευθύνσεις URL, πακέτα IP ή πλαίσια ethernet («Εισβολές») και στη συνέχεια τα αποστέλλει στον Πάροχο, συμπεριλαμβανομένων, ενδεικτικά, πληροφοριών σχετικά με τη διαδικασία εγκατάστασης, τον Υπολογιστή ή/και την πλατφόρμα στην οποία έχει εγκατασταθεί το Λογισμικό και πληροφορίες σχετικά με τις δυνατότητες και τη λειτουργικότητα του Λογισμικού («Πληροφορίες»). Οι Πληροφορίες και οι Εισβολές μπορεί να περιέχουν δεδομένα (συμπεριλαμβανομένων προσωπικών δεδομένων που έχουν αποκτηθεί τυχαία ή κατά λάθος) σχετικά με τον Τελικό χρήστη ή άλλους χρήστες του υπολογιστή στον οποίο είναι εγκατεστημένο το Λογισμικό, καθώς και αρχεία προσβεβλημένα από Εισβολές μαζί με τα σχετικά μεταδεδομένα τους.

Οι Πληροφορίες και οι Εισβολές είναι δυνατό να συλλέγονται με τις εξής λειτουργίες του Λογισμικού:

i. Η λειτουργία του συστήματος LiveGrid Reputation System περιλαμβάνει τη συλλογή και την αποστολή στον Πάροχο τμημάτων κώδικα που σχετίζονται με Εισβολές. Αυτή η λειτουργία ενεργοποιείται στις

τυπικές ρυθμίσεις του Λογισμικού.

ii. Η λειτουργία LiveGrid Feedback System περιλαμβάνει τη συλλογή και την αποστολή Εισβολών στον Πάροχο, μαζί με τα σχετικά μεταδεδομένα και τις Πληροφορίες. Αυτή η λειτουργία μπορεί να ενεργοποιηθεί από τον Τελικό Χρήστη κατά τη διαδικασία εγκατάστασης του Λογισμικού.

Ο Πάροχος θα χρησιμοποιεί τις Πληροφορίες και τις Εισβολές που έχει λάβει μόνο για το σκοπό ανάλυσης και έρευνας για τις Εισβολές, βελτίωση του Λογισμικού και επαλήθευση της γνησιότητας της Άδειας χρήσης και θα λαμβάνει τα κατάλληλα μέτρα για να διασφαλίζει ότι οι Εισβολές και οι Πληροφορίες που λαμβάνει παραμένουν εμπιστευτικές. Με την ενεργοποίηση αυτής της λειτουργίας του Λογισμικού, ο Πάροχος μπορεί να συλλέγει και να επεξεργάζεται Εισβολές και Πληροφορίες, όπως καθορίζεται στην Πολιτική Απορρήτου και σύμφωνα με τους σχετικούς νομικούς κανονισμούς. Μπορείτε να απενεργοποιήσετε αυτές τις λειτουργίες οποιαδήποτε στιγμή.

Για το σκοπό αυτής της Συμφωνίας, είναι απαραίτητη η συλλογή, επεξεργασία και αποθήκευση δεδομένων που επιτρέπουν στον Πάροχο να σας ταυτοποιήσει, σύμφωνα με την Πολιτική Απορρήτου. Με το παρόν συμφωνείτε ο Πάροχος να ελέγχει, χρησιμοποιώντας δικά του μέσα, αν χρησιμοποιείτε το Λογισμικό σύμφωνα με τις διατάξεις αυτής της Συμφωνίας. Με το παρόν συμφωνείτε ότι για το σκοπό αυτής της Συμφωνίας απαιτείται η μεταφορά των δεδομένων σας, κατά την επικοινωνία μεταξύ του Λογισμικού και των συστημάτων υπολογιστή του Παρόχου ή των επιχειρηματικών συνεργατών του, ως μέρος του δικτύου διανομής και υποστήριξης του Παρόχου για να διασφαλίζεται η λειτουργικότητα του Λογισμικού και η εξουσιοδότηση της χρήσης του Λογισμικού και για την προστασία των δικαιωμάτων του Παρόχου.

Μετά την συνομολόγηση αυτής της Συμφωνίας, ο Πάροχος ή οποιοιδήποτε από τους συνεργάτες του, ως μέρος του δικτύου διανομής και υποστήριξης του Παρόχου, θα δικαιούνται να μεταβιβάσουν, να επεξεργαστούν και να αποθηκεύσουν ουσιώδη δεδομένα που σας ταυτοποιούν, για σκοπούς τιμολόγησης και εκτέλεσης αυτής της Συμφωνίας και για μετάδοση ειδοποιήσεων στον υπολογιστή σας.

Λεπτομέρειες σχετικά με το απόρρητο και την προστασία των προσωπικών δεδομένων και τα δικαιώματά σας ως αντικείμενο δεδομένων βρίσκονται στην Πολιτική Απορρήτου, η οποία είναι διαθέσιμη στον ιστότοπο του Παρόχου και προσπελάσιμη απευθείας από τη διαδικασία εγκατάστασης. Μπορείτε, επίσης, να επισκεφτείτε τον ιστότοπο από την ενότητα βοήθειας του Λογισμικού.

5. **Άσκηση δικαιωμάτων του Τελικού χρήστη**. Πρέπει να ασκείτε τα δικαιώματα Τελικού χρήστη αυτοπροσώπως ή μέσω των υπαλλήλων σας. Δικαιούστε να χρησιμοποιείτε το Λογισμικό μόνο για να διασφαλίζετε τις λειτουργίες σας και να προστατεύετε τους υπολογιστές ή τα συστήματα υπολογιστή για τα οποία έχετε προμηθευτεί Άδεια χρήσης.

6. **Περιορισμοί δικαιωμάτων.** Απαγορεύεται η αντιγραφή, διανομή, εξαγωγή στοιχείων ή δημιουργία παράγωγων έργων του Λογισμικού. Όταν χρησιμοποιείτε το Λογισμικό υποχρεούστε να συμμορφώνεστε με τους παρακάτω περιορισμούς:

α) Μπορείτε να δημιουργήσετε ένα αντίγραφο του Λογισμικού σε ένα μέσο μόνιμης αποθήκευσης ως αντίγραφο ασφαλείας αρχειοθέτησης, εφόσον το αντίγραφο ασφαλείας αρχειοθέτησης δεν είναι εγκατεστημένο ή δεν χρησιμοποιείται σε οποιονδήποτε υπολογιστή. Οποιαδήποτε άλλα αντίγραφα του Λογισμικού που δημιουργείτε αποτελούν αθέτηση της παρούσας Συμφωνίας.

β) Δεν έχετε δικαίωμα χρήσης, τροποποίησης, ερμηνείας, αναπαραγωγής του Λογισμικού ή μεταβίβασης δικαιωμάτων χρήσης του Λογισμικού ή αντιγράφων του Λογισμικού με οποιονδήποτε

τρόπο πέραν όσων προβλέπονται στην παρούσα Συμφωνία.

γ) Δεν έχετε δικαίωμα πώλησης, υπεκχώρησης, εκμίσθωσης ή ενοικίασης ή δανεισμού του Λογισμικού ή χρήσης του Λογισμικού για την παροχή εμπορικών υπηρεσιών.

δ) Δεν έχετε δικαίωμα αποσυμπίλησης, αντίστροφης ανάλυσης ή αποσυγκρότησης του Λογισμικού ή προσπάθειας ανακάλυψης του πηγαίου κώδικα του Λογισμικού με άλλο τρόπο, παρά μόνο στο βαθμό που ο περιορισμός αυτός απαγορεύεται ρητά από το νόμο.

ε) Συμφωνείτε ότι θα χρησιμοποιείτε το Λογισμικό μόνο με τρόπο που συμμορφώνεται με το σύνολο της ισχύουσας νομοθεσίας στη δικαιοδοσία στην οποία χρησιμοποιείτε το Λογισμικό, που περιλαμβάνει, χωρίς περιορισμό, τους ισχύοντες περιορισμούς που αφορούν τα πνευματικά δικαιώματα και άλλα δικαιώματα πνευματικής ιδιοκτησίας.

στ) Συμφωνείτε ότι θα χρησιμοποιείτε το Λογισμικό και τις λειτουργίες του μόνο με τρόπο που δεν περιορίζει τις πιθανότητες πρόσβασης σε αυτές τις υπηρεσίες από άλλους Τελικούς χρήστες. Ο Πάροχος διατηρεί το δικαίωμα να περιορίζει το εύρος των υπηρεσιών που παρέχονται σε μεμονωμένους Τελικούς χρήστες, για να επιτρέπεται η χρήση των υπηρεσιών στον μεγαλύτερο δυνατό αριθμό Τελικών χρηστών. Ο περιορισμός του εύρους υπηρεσιών θα σημαίνει επίσης πλήρη τερματισμό της δυνατότητας χρήσης οποιασδήποτε από τις λειτουργίες του Λογισμικού και διαγραφή Δεδομένων και Πληροφοριών στους διακομιστές του Παρόχου ή διακομιστές τρίτων που σχετίζονται με μια συγκεκριμένη λειτουργία του Λογισμικού.

ζ) Συμφωνείτε να μη προβαίνετε σε δραστηριότητες που περιλαμβάνουν τη χρήση του Κλειδιού άδειας χρήσης, οι οποίες αντιβαίνουν στους όρους αυτής της Συμφωνίας ή οδηγούν στην παροχή του Κλειδιού άδειας χρήσης σε οποιοδήποτε άτομο που δεν δικαιούται να χρησιμοποιεί το Λογισμικό, όπως η μεταβίβαση χρησιμοποιημένου ή μη χρησιμοποιημένου Κλειδιού άδειας χρήσης με οποιαδήποτε μορφή, καθώς και μη εξουσιοδοτημένη αντιγραφή ή διανομή αντιγραμμένων ή δημιουργημένων Κλειδιών άδειας χρήσης ή χρήσης του Λογισμικού ως αποτέλεσμα της χρήσης ενός Κλειδιού άδειας χρήσης που λαμβάνεται από την προέλευση και όχι από τον Πάροχο.

7. **Πνευματικά δικαιώματα**. Το Λογισμικό και όλα τα δικαιώματά του, χωρίς περιορισμό, συμπεριλαμβανομένων δικαιωμάτων ιδιοκτησίας και δικαιωμάτων πνευματικής ιδιοκτησίας σε αυτό ανήκουν στην ESET ή/και τους αδειοδότες της. Τα δικαιώματα προστατεύονται από διατάξεις διεθνών συνθηκών και από το σύνολο των λοιπών ισχυόντων εθνικών νόμων της χώρας στην οποία χρησιμοποιείται το Λογισμικό. Η δομή, η οργάνωση και ο κώδικας του Λογισμικού είναι πολύτιμα εμπορικά μυστικά και εμπιστευτικές πληροφορίες της ESET ή/και των αδειοδοτών της. Απαγορεύεται η αντιγραφή του Λογισμικού, παρά μόνο στο βαθμό που ορίζεται στο Άρθρο 6, παρ. α. Οποιαδήποτε αντίγραφα τα οποία επιτρέπεται να δημιουργήσετε σύμφωνα με αυτή τη Συμφωνία πρέπει να περιέχουν τις ίδιες ειδοποιήσεις πνευματικών δικαιωμάτων και άλλων δικαιωμάτων ιδιοκτησίας που εμφανίζονται στο Λογισμικό. Αν προβείτε σε αποσυμπίληση, αντίστροφη ανάλυση, αποσυγκρότηση ή άλλη προσπάθεια να ανακαλύψετε τον πηγαίο κώδικα του Λογισμικού, παραβιάζοντας τις διατάξεις της παρούσας Συμφωνίας, συμφωνείτε δια του παρόντος ότι οποιεσδήποτε πληροφορίες που προκύπτουν με αυτό τον τρόπο θα θεωρείται αυτόματα και ανέκκλητα ότι μεταβιβάζονται και κατέχονται πλήρως από τον Πάροχο, από τη στιγμή κατά την οποία δημιουργήθηκαν αυτές οι πληροφορίες, παρά τα δικαιώματα του Παρόχου σε σχέση με την αθέτηση της παρούσας Συμφωνίας.

8. **Επιφύλαξη δικαιωμάτων**. Δια του παρόντος ο Πάροχος διατηρεί όλα τα δικαιώματα στο Λογισμικό, με εξαίρεση τα δικαιώματα που χορηγούνται ρητά σύμφωνα με τους όρους αυτής της Συμφωνίας σε σας ως Τελικό χρήστη του Λογισμικού.

9. **Εκδόσεις πολλαπλών γλωσσών, λογισμικό διπλού μέσου, πολλαπλά αντίγραφα**. Σε

περίπτωση που το Λογισμικό υποστηρίζει πολλαπλές πλατφόρμες ή γλώσσες, ή αν λάβατε πολλαπλά αντίγραφα του Λογισμικού, μπορείτε να χρησιμοποιείτε το Λογισμικό μόνο για τον αριθμό συστημάτων υπολογιστή και για τις εκδόσεις για τις οποίες έχετε λάβει Άδεια χρήσης. Απαγορεύεται η πώληση, ενοικίαση, εκμίσθωση, υπεκχώρηση ή μεταβίβαση εκδόσεων ή αντιγράφων του Λογισμικού που δεν χρησιμοποιείτε.

10. **Έναρξη και λήξη της Συμφωνίας.** Η παρούσα Συμφωνία τίθεται σε ισχύ από την ημερομηνία που συμφωνείτε με τους όρους αυτής της Συμφωνίας. Μπορείτε να τερματίσετε αυτή τη Συμφωνία οποτεδήποτε με μόνιμη απεγκατάσταση, καταστροφή και επιστροφή, με δικά σας έξοδα, του Λογισμικού, όλων των αντιγράφων ασφαλείας και όλων των σχετικών υλικών που παρέχονται από τον Πάροχο ή τους συνεργάτες του. Το δικαίωμα του χρήστη να χρησιμοποιεί το Λογισμικό και οποιεσδήποτε από τις δυνατότητές του ενδέχεται να υπόκειται στην Πολιτική Τέλους κύκλου ζωής. Όταν επέλθει η ημερομηνία Τέλους κύκλου ζωής του Λογισμικού ή οποιωνδήποτε από τις δυνατότητές του, η οποία ορίζεται στην Πολιτική Τέλους κύκλου ζωής, θα τερματιστεί το δικαίωμα του χρήστη να χρησιμοποιεί το Λογισμικό. Ανεξάρτητα από τον τρόπο λήξης αυτής της Συμφωνίας, θα εξακολουθήσουν να εφαρμόζονται για απεριόριστο χρονικό διάστημα οι διατάξεις των Άρθρων 7, 8, 11, 13, 19 και 21.

11. **ΔΗΛΩΣΕΙΣ ΤΕΛΙΚΟΥ ΧΡΗΣΤΗ**. ΩΣ ΤΕΛΙΚΟΣ ΧΡΗΣΤΗΣ ΑΠΟΔΕΧΕΣΤΕ ΟΤΙ ΤΟ ΛΟΓΙΣΜΙΚΟ ΠΑΡΕΧΕΤΑΙ «ΩΣ ΕΧΕΙ», ΧΩΡΙΣ ΕΓΓΥΗΣΗ ΚΑΝΕΝΟΣ ΕΙΔΟΥΣ, ΡΗΤΗ Ή ΣΙΩΠΗΡΗ, ΚΑΙ ΣΤΟ ΜΕΓΙΣΤΟ ΒΑΘΜΟ ΠΟΥ ΕΠΙΤΡΕΠΕΤΑΙ ΑΠΟ ΤΗΝ ΙΣΧΥΟΥΣΑ ΝΟΜΟΘΕΣΙΑ. ΟΥΤΕ Ο ΠΑΡΟΧΟΣ, ΟΙ ΑΔΕΙΟΔΟΤΕΣ ΤΟΥ Ή ΟΙ ΘΥΓΑΤΡΙΚΕΣ ΤΟΥ, ΟΥΤΕ ΟΙ ΚΑΤΟΧΟΙ ΤΩΝ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΠΑΡΕΧΟΥΝ ΥΠΟΣΧΕΣΕΙΣ Ή ΕΓΓΥΗΣΕΙΣ, ΡΗΤΕΣ Ή ΣΙΩΠΗΡΕΣ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΩΝ ΕΝΔΕΙΚΤΙΚΑ ΤΩΝ ΕΓΓΥΗΣΕΩΝ ΕΜΠΟΡΕΥΣΙΜΟΤΗΤΑΣ Ή ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ ΓΙΑ ΣΥΓΚΕΚΡΙΜΕΝΟ ΣΚΟΠΟ Ή ΟΤΙ ΤΟ ΛΟΓΙΣΜΙΚΟ ΔΕΝ ΘΑ ΠΑΡΑΒΙΑΖΕΙ ΤΥΧΟΝ ΕΥΡΕΣΙΤΕΧΝΙΕΣ, ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ, ΕΜΠΟΡΙΚΑ ΣΗΜΑΤΑ Ή ΑΛΛΑ ΔΙΚΑΙΩΜΑΤΑ ΤΡΙΤΩΝ. ΔΕΝ ΠΑΡΕΧΕΤΑΙ ΚΑΜΙΑ ΕΓΓΥΗΣΗ ΑΠΟ ΤΟΝ ΠΑΡΟΧΟ Ή ΑΠΟ ΟΠΟΙΟΔΗΠΟΤΕ ΑΛΛΟ ΜΕΡΟΣ ΟΤΙ ΟΙ ΛΕΙΤΟΥΡΓΙΕΣ ΠΟΥ ΠΕΡΙΕΧΟΝΤΑΙ ΣΤΟ ΛΟΓΙΣΜΙΚΟ ΘΑ ΙΚΑΝΟΠΟΙΟΥΝ ΤΙΣ ΑΠΑΙΤΗΣΕΙΣ ΣΑΣ Ή ΟΤΙ Η ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΘΑ ΕΙΝΑΙ ΑΔΙΑΛΕΙΠΤΗ ΚΑΙ ΧΩΡΙΣ ΣΦΑΛΜΑΤΑ. ΑΝΑΛΑΜΒΑΝΕΤΕ ΠΛΗΡΩΣ ΤΗΝ ΕΥΘΥΝΗ ΚΑΙ ΤΟΝ ΚΙΝΔΥΝΟ ΓΙΑ ΤΗΝ ΕΠΙΛΟΓΗ ΚΑΙ ΧΡΗΣΗ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΓΙΑ ΝΑ ΕΠΙΤΥΧΕΤΕ ΤΑ ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΟΥ ΕΠΙΘΥΜΕΙΤΕ ΚΑΙ ΓΙΑ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ, ΧΡΗΣΗ ΚΑΙ ΤΑ ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΟΥ ΠΡΟΚΥΠΤΟΥΝ ΑΠΟ ΑΥΤΗ.

12. **Απουσία άλλων υποχρεώσεων**. Αυτή η Συμφωνία δεν δημιουργεί υποχρεώσεις εκ μέρους του Παρόχου και τους αδειοδότες τους, εκτός από εκείνες που ορίζονται ειδικά στο παρόν.

13. **ΠΕΡΙΟΡΙΣΜΕΝΗ ΕΥΘΥΝΗ**. ΣΤΟ ΜΕΓΙΣΤΟ ΒΑΘΜΟ ΠΟΥ ΕΠΙΤΡΕΠΕΙ Η ΙΣΧΥΟΥΣΑ ΝΟΜΟΘΕΣΙΑ, ΣΕ ΚΑΜΙΑ ΠΕΡΙΠΤΩΣΗ Ο ΠΑΡΟΧΟΣ, ΟΙ ΥΠΑΛΛΗΛΟΙ Ή ΟΙ ΑΔΕΙΟΔΟΤΕΣ ΤΟΥ ΔΕΝ ΕΥΘΥΝΟΝΤΑΙ ΓΙΑ ΤΥΧΟΝ ΑΠΩΛΕΙΑ ΚΕΡΔΩΝ, ΕΣΟΔΩΝ, ΠΩΛΗΣΕΩΝ, ΔΕΔΟΜΕΝΩΝ Ή ΕΞΟΔΩΝ ΠΡΟΜΗΘΕΙΑΣ ΠΡΟΪΟΝΤΩΝ Ή ΥΠΗΡΕΣΙΩΝ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ, ΒΛΑΒΗ ΠΕΡΙΟΥΣΙΑΣ, ΤΡΑΥΜΑΤΙΣΜΟ, ΔΙΑΚΟΠΗ ΕΜΠΟΡΙΚΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ, ΑΠΩΛΕΙΑ ΕΠΑΓΓΕΛΜΑΤΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ Ή ΟΠΟΙΑΔΗΠΟΤΕ ΕΙΔΙΚΗ, ΑΜΕΣΗ, ΕΜΜΕΣΗ, ΣΥΜΠΤΩΜΑΤΙΚΗ, ΟΙΚΟΝΟΜΙΚΗ, ΑΣΦΑΛΙΣΤΙΚΗ, ΠΟΙΝΙΚΗ, ΕΙΔΙΚΗ Ή ΣΥΝΕΠΑΓΟΜΕΝΗ ΒΛΑΒΗ, ΑΝΕΞΑΡΤΗΤΑ ΑΠΟ ΤΗΝ ΑΙΤΙΑ, ΕΙΤΕ ΠΡΟΚΥΠΤΕΙ ΑΠΟ ΣΥΜΒΑΣΗ, ΑΔΙΚΟΠΡΑΞΙΑ, ΑΜΕΛΕΙΑ Ή ΑΛΛΗ ΕΡΜΗΝΕΙΑ ΕΥΘΥΝΗΣ, ΠΟΥ ΠΡΟΚΥΠΤΕΙ ΑΠΟ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ, ΤΗ ΧΡΗΣΗ Ή ΤΗΝ ΑΔΥΝΑΜΙΑ ΧΡΗΣΗΣ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ, ΑΚΟΜΗ ΚΙ ΑΝ Ο ΠΑΡΟΧΟΣ Ή ΟΙ ΑΔΕΙΟΔΟΤΕΣ ΤΟΥ Ή ΟΙ ΘΥΓΑΤΡΙΚΕΣ ΤΟΥ ΕΧΟΥΝ ΕΝΗΜΕΡΩΘΕΙ ΓΙΑ ΤΗΝ ΠΙΘΑΝΟΤΗΤΑ ΤΕΤΟΙΩΝ ΒΛΑΒΩΝ. ΕΠΕΙΔΗ ΟΡΙΣΜΕΝΕΣ ΧΩΡΕΣ ΚΑΙ ΔΙΚΑΙΟΔΟΣΙΕΣ ΔΕΝ ΕΠΙΤΡΕΠΟΥΝ ΤΗΝ ΕΞΑΙΡΕΣΗ ΤΗΣ ΕΥΘΥΝΗΣ, ΑΛΛΑ ΕΝΔΕΧΕΤΑΙ ΝΑ ΕΠΙΤΡΕΠΟΥΝ ΠΕΡΙΟΡΙΣΜΟ ΤΗΣ ΕΥΘΥΝΗΣ, ΣΕ ΑΥΤΕΣ ΤΙΣ ΠΕΡΙΠΤΩΣΕΙΣ, Η ΕΥΘΥΝΗ ΤΟΥ ΠΑΡΟΧΟΥ, ΤΩΝ ΥΠΑΛΛΗΛΩΝ Ή ΤΩΝ ΑΔΕΙΟΔΟΤΩΝ Ή ΤΩΝ ΘΥΓΑΤΡΙΚΩΝ ΤΟΥ ΠΕΡΙΟΡΙΖΕΤΑΙ ΣΤΟ ΠΟΣΟ ΠΟΥ ΠΛΗΡΩΣΑΤΕ ΓΙΑ ΤΗΝ ΑΔΕΙΑ ΧΡΗΣΗΣ.

14. Κανένα μέρος αυτής της Συμφωνίας δεν βλάπτει τα νομοθετημένα δικαιώματα οποιουδήποτε συμβαλλόμενου που ενεργεί ως καταναλωτής αν αυτά παραβιάζονται.

15. **Τεχνική υποστήριξη**. Η ESET ή οι τρίτοι εντεταλμένοι της ESET θα παρέχουν τεχνική υποστήριξη κατά τη διακριτική τους ευχέρεια, χωρίς καμία εγγύηση ή υπόσχεση. Δεν θα παρέχεται καμία τεχνική υποστήριξη, εφόσον επέλθει η ημερομηνία Τέλους κύκλου ζωής, που ορίζεται στην Πολιτική Τέλους κύκλου ζωής, του Λογισμικού ή οποιασδήποτε από τις δυνατότητές του. Ο Τελικός χρήστης θα υποχρεούται να διατηρεί αντίγραφα ασφαλείας όλων των υπαρχόντων δεδομένων, μέσων λογισμικού και προγραμμάτων πριν από την παροχή τεχνικής υποστήριξης. Η ESET ή/και τρίτοι εντεταλμένοι της ESET δεν αποδέχονται ευθύνη για βλάβη ή απώλεια δεδομένων, ιδιοκτησίας, λογισμικού ή υλικού ή απώλεια εσόδων εξαιτίας της παροχής τεχνικής υποστήριξης. Η ESET ή/και τρίτοι εντεταλμένοι της ESET διατηρούν το δικαίωμα να αποφασίζουν αν η επίλυση του προβλήματος υπερβαίνει το εύρος της τεχνικής υποστήριξης. Η ESET διατηρεί το δικαίωμα να αρνηθεί, να αναστείλει ή να τερματίσει την παροχή τεχνικής υποστήριξης κατά τη διακριτική της ευχέρεια. Για το σκοπό παροχής τεχνικής υποστήριξης, ενδέχεται να απαιτούνται Στοιχεία άδειας χρήσης, Πληροφορίες και άλλα δεδομένα, σύμφωνα με την Πολιτική Απορρήτου.

16. **Μεταβίβαση της Άδειας χρήσης**. Το Λογισμικό μπορεί να μεταφερθεί από ένα σύστημα υπολογιστή σε άλλο, εκτός αν αυτό αντιβαίνει στους όρους της Συμφωνίας. Αν δεν αντιβαίνει στους όρους της Συμφωνίας, ο Τελικός χρήστης θα δικαιούται να μεταφέρει μόνιμα την Άδεια χρήσης και όλα τα δικαιώματα που συνεπάγεται η παρούσα Συμφωνία σε άλλον Τελικό χρήστη μόνο με την συγκατάθεση του Παρόχου, υπό την προϋπόθεση ότι (i) ο αρχικός Τελικός χρήστης δεν διατηρεί κανένα αντίγραφο του Λογισμικού, (ii) η μεταβίβαση των δικαιωμάτων πρέπει να είναι άμεση, δηλ. από τον αρχικό Τελικό χρήστη στον νέο Τελικό χρήστη, (iii) ο νέος Τελικός χρήστης πρέπει να αναλάβει όλα τα δικαιώματα και τις υποχρεώσεις που επιβάλλονται στον αρχικό Τελικό χρήστη σύμφωνα με τους όρους αυτής της Συμφωνίας, (iv) ο αρχικός Τελικός χρήστης πρέπει να παράσχει στον νέο Τελικό χρήστη την τεκμηρίωση που επιτρέπει την επαλήθευση της γνησιότητας του Λογισμικού όπως καθορίζεται στο Άρθρο 17.

17. **Επαλήθευση της γνησιότητας του Λογισμικού.** Ο Τελικός χρήστης μπορεί να επιδείξει το δικαίωμα χρήσης του Λογισμικού με έναν από τους παρακάτω τρόπους: (i) μέσω ενός πιστοποιητικού άδειας χρήσης που εκδίδεται από τον Πάροχο ή τρίτο διορισμένο από τον Πάροχο, (ii) μέσω γραπτής συμφωνίας άδειας χρήσης, εάν συνομολογήθηκε τέτοια συμφωνία, (iii) μέσω της υποβολής μηνύματος ηλεκτρονικού ταχυδρομείου που στάλθηκε από τον Πάροχο και το οποίο περιέχει λεπτομέρειες αδειοδότησης (όνομα χρήστη και κωδικό πρόσβασης). Για το σκοπό επαλήθευσης της γνησιότητας του Λογισμικού, ενδέχεται να απαιτούνται Στοιχεία άδειας χρήσης και δεδομένα ταυτοποίησης Τελικού χρήστη, σύμφωνα με την Πολιτική Απορρήτου.

18. **Αδειοδότηση για δημόσιες αρχές και την Κυβέρνηση των Η.Π.Α.**. Το Λογισμικό θα παρέχεται σε δημόσιες αρχές, συμπεριλαμβανομένης της Κυβέρνησης των Ηνωμένων Πολιτειών, με τα δικαιώματα και τους περιορισμούς άδειας χρήσης που περιγράφονται σε αυτή τη Συμφωνία.

19. **Συμμόρφωση με τον έλεγχο εμπορίου**.

α) Απαγορεύεται η άμεση ή έμμεση εξαγωγή, επανεξαγωγή, μεταβίβαση ή άλλη διάθεση του Λογισμικού σε οποιοδήποτε πρόσωπο ή η χρήση του με οποιονδήποτε τρόπο ή η συμμετοχή σε οποιαδήποτε ενέργεια η οποία μπορεί να έχει σαν αποτέλεσμα να παραβιάσει ή να υποστεί αρνητικές επιπτώσεις η ESET ή οι εταιρείες συμμετοχών της, οι θυγατρικές της και οι θυγατρικές οποιωνδήποτε από τις εταιρείες συμμετοχών της, καθώς και οι οντότητες που ελέγχονται από τις εταιρείες συμμετοχών της («Συγγενείς εταιρείες») σύμφωνα με τη νομοθεσία περί ελέγχου εμπορίου, η οποία περιλαμβάνει

i. οποιουσδήποτε νόμους οι οποίοι ελέγχουν, περιορίζουν ή επιβάλλουν απαιτήσεις αδειοδότησης στην εξαγωγή, επανεξαγωγή ή μεταβίβαση αγαθών, λογισμικού, τεχνολογίας ή υπηρεσιών, που εκδίδονται ή υιοθετούνται από οποιαδήποτε κυβέρνηση, κράτος ή ρυθμιστική αρχή των Ηνωμένων Πολιτειών

Αμερικής, της Σιγκαπούρης, του Ηνωμένου Βασιλείου, της Ευρωπαϊκής Ένωσης ή οποιουδήποτε από τα κράτη μέλη της ή οποιασδήποτε χώρας στην οποία πρόκειται να εκτελεστούν οι υποχρεώσεις της Συμφωνίας ή στην οποία συστάθηκε ή λειτουργεί η ESET ή οποιεσδήποτε από τις Συγγενείς εταιρείες της και

ii. οποιεσδήποτε οικονομικές, χρηματοοικονομικές, εμπορικές ή άλλες κυρώσεις, περιορισμούς, εμπάργκο, αποκλεισμό εισαγωγών ή εξαγωγών, απαγόρευση μεταβίβασης χρημάτων ή περιουσιακών στοιχείων ή παροχής υπηρεσιών ή ισοδύναμο μέτρο που επιβάλλεται από οποιαδήποτε κυβέρνηση, κράτος ή ρυθμιστική αρχή των Ηνωμένων Πολιτειών Αμερικής, της Σιγκαπούρης, του Ηνωμένου Βασιλείου, της Ευρωπαϊκής Ένωσης ή οποιουδήποτε από τα κράτη μέλη της ή οποιασδήποτε χώρας στην οποία πρόκειται να εκτελεστούν οι υποχρεώσεις της Συμφωνίας ή στην οποία συστάθηκε ή λειτουργεί η ESET ή οποιεσδήποτε από τις Συγγενείς εταιρείες της («Νομοθεσία κυρώσεων»).

(νομικές ενέργειες που αναφέρονται στα παραπάνω σημεία i και ii. συλλογικά ως «Νομοθεσία περί ελέγχου εμπορίου»).

β) Η ESET θα έχει το δικαίωμα να αναστέλλει τις υποχρεώσεις της σύμφωνα με τους παρόντες Όρους ή να τερματίζει τους παρόντες Όρους με άμεση ισχύ σε περίπτωση που:

i. Η ESET προσδιορίσει ότι, κατά την εύλογη άποψή της, ο Χρήστης έχει παραβιάσει ή είναι πιθανόν να παραβιάσει τη διάταξη του Άρθρου 19 παρ. α της Συμφωνίας, ή

ii. Ο Τελικός χρήστης ή/και το λογισμικό υπόκεινται στη νομοθεσία περί ελέγχου εμπορίου και, κατά συνέπεια, η ESET προσδιορίσει ότι, κατά την εύλογη άποψή της, η συνέχιση της εκτέλεσης των υποχρεώσεών της σύμφωνα με το Συμφωνητικό μπορεί να έχει σαν αποτέλεσμα η ESET ή οι Συγγενείς εταιρείες της να παραβιάζουν ή να υποστούν αρνητικές συνέπειες σύμφωνα με τη νομοθεσία περί ελέγχου εμπορίου.

γ) Κανένα μέρος του Συμφωνητικού δεν προορίζεται και κανένα μέρος δεν θα πρέπει να ερμηνεύεται ότι παρακινεί ή απαιτεί από τον συμβαλλόμενο να ενεργεί ή να αποφεύγει να ενεργήσει (ή να συμφωνεί να ενεργήσει ή να αποφύγει να ενεργήσει) με οποιονδήποτε τρόπο ο οποίος είναι ασυνεπής, επιφέρει ποινή η απαγορεύεται σύμφωνα με οποιαδήποτε ισχύουσα νομοθεσία περί ελέγχου εμπορίου.

20. **Γνωστοποιήσεις**. Όλες οι γνωστοποιήσεις και επιστροφές του Λογισμικού και της Τεκμηρίωσης πρέπει να παραδίδονται στη διεύθυνση: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, με επιφύλαξη ως προς το δικαίωμα της ESET να επικοινωνεί στον χρήστη οποιεσδήποτε μεταβολές στην παρούσα Συμφωνία, στις Πολιτικές απορρήτου, στην Πολιτική Τέλους κύκλου ζωής και στην Τεκμηρίωση σύμφωνα με το άρθρο 22 της Συμφωνίας. Η ESET ενδέχεται να αποστείλει στον χρήστη email, ειδοποιήσεις εντός εφαρμογής μέσω του Λογισμικού ή να δημοσιεύσει την επικοινωνία στον ιστότοπό της. Ο χρήστης συμφωνεί να λαμβάνει επικοινωνίες νομικού χαρακτήρα από την ESET σε ηλεκτρονική μορφή, όπως οποιεσδήποτε επικοινωνίες σχετικά με αλλαγές στους Όρους, στους Ειδικούς όρους ή στις Πολιτικές απορρήτου, οποιαδήποτε πρόταση/αποδοχή σύμβασης ή προσκλήσεις για αντιμετώπιση ζητημάτων, ειδοποιήσεις ή άλλες επικοινωνίες νομικού χαρακτήρα. Αυτή η ηλεκτρονική επικοινωνία θα θεωρείται ότι λαμβάνεται εγγράφως, εκτός εάν απαιτείται ειδικά διαφορετική μορφή επικοινωνίας από την ισχύουσα νομοθεσία.

21. **Ισχύον δίκαιο**. Αυτή η Συμφωνία θα διέπεται από και θα ερμηνεύεται σύμφωνα με τους νόμους της Δημοκρατίας της Σλοβακίας. Ο Τελικός χρήστης και ο Πάροχος συμφωνούν δια του παρόντος ότι δεν θα ισχύουν οι αρχές αμφισβητούμενων διατάξεων και της Σύμβασης των Ηνωμένων Εθνών περί Συμβολαίων για τη διεθνή πώληση αγαθών. Συμφωνείτε ρητά ότι οποιεσδήποτε διαφωνίες ή αξιώσεις που απορρέουν από αυτή τη Συμφωνία σε σχέση με τον Πάροχο ή οποιεσδήποτε διαφωνίες ή αξιώσεις που σχετίζονται με τη χρήση του Λογισμικού θα επιλύονται από το Περιφερειακό δικαστήριο της

Μπρατισλάβα I και συμφωνείτε ρητά στην άσκηση δικαιοδοσίας από το συγκεκριμένο δικαστήριο.

22. **Γενικές διατάξεις**. Εάν οποιαδήποτε από τις διατάξεις της παρούσας Συμφωνίας είναι άκυρη ή μη εφαρμόσιμη, αυτό δεν θα επηρεάζει την εγκυρότητα των άλλων υπόλοιπων διατάξεων της Συμφωνίας, οι οποίες θα παραμείνουν έγκυρες και εφαρμοστέες σύμφωνα με τις προϋποθέσεις που διατυπώνονται στο παρόν έγγραφο. Η παρούσα Συμφωνία εκτελέστηκε στα Αγγλικά. Σε περίπτωση κατά την οποία οποιαδήποτε μετάφραση της Συμφωνίας δημιουργείται για ευκολία ή για οποιονδήποτε άλλο σκοπό ή σε περίπτωση ασυμφωνίας μεταξύ των γλωσσικών εκδόσεων της παρούσας Συμφωνίας, υπερισχύει η έκδοση στα Αγγλικά.

Η ESET διατηρεί το δικαίωμα να επιφέρει αλλαγές στο Λογισμικό, καθώς και να αναθεωρεί όρους της παρούσας Συμφωνίας, των Παραρτημάτων, των Προσθηκών της, της Πολιτικής απορρήτου, της Πολιτικής Τέλους κύκλου ζωής και της Τεκμηρίωσης ή οποιουδήποτε μέρους αυτών ανά πάσα στιγμή, ενημερώνοντας το σχετικό έγγραφο (i) ώστε να αντανακλά τις αλλαγές στο Λογισμικό ή στον τρόπο με τον οποίο δραστηριοποιείται η ESET, (ii) για νομικούς, κανονιστικούς λόγους ή για λόγους ασφαλείας ή (iii) για την αποτροπή κατάχρησης ή βλάβης. Ο χρήστης θα ειδοποιηθεί σχετικά με οποιαδήποτε αναθεώρηση της Συμφωνίας μέσω email, ειδοποίησης εντός της εφαρμογής ή άλλο ηλεκτρονικό μέσο. Εάν ο χρήστης διαφωνεί με τις προτεινόμενες αλλαγές στη Συμφωνία, μπορεί να την καταγγείλει σύμφωνα με το Άρθρο 10 εντός 30 ημερών από την παραλαβή της ειδοποίησης της αλλαγής. Εάν ο χρήστης δεν καταγγείλει τη Συμφωνία εντός αυτού του χρονικού ορίου, θα θεωρηθεί ότι οι προτεινόμενες αλλαγές έχουν γίνει αποδεκτές και θα ισχύουν για τον χρήστη από την ημέρα παραλαβής της ειδοποίησης της αλλαγής.

Το παρόν αποτελεί το σύνολο της Συμφωνίας μεταξύ του Παρόχου και Εσάς σε σχέση με το Λογισμικό και αντικαθιστά οποιεσδήποτε προηγούμενες υποσχέσεις, συζητήσεις, δεσμεύσεις, επικοινωνίες ή διαφήμιση που σχετίζεται με το Λογισμικό.

ΠΡΟΣΘΗΚΗ ΣΤΗ ΣΥΜΦΩΝΙΑ

Αξιολόγηση ασφάλειας συσκευών συνδεδεμένων στο δίκτυο. Εφαρμόζονται πρόσθετες διατάξεις στην Αξιολόγηση ασφάλειας συσκευών συνδεδεμένων στο δίκτυο ως ακολούθως:

Το Λογισμικό περιέχει μια λειτουργία για τον έλεγχο της ασφάλειας του τοπικού δικτύου του τελικού χρήστη και της ασφάλειας των συσκευών που βρίσκονται στο τοπικό δίκτυο, το οποίο απαιτεί το όνομα του τοπικού δικτύου και πληροφορίες για τις συσκευές στο τοπικό δίκτυο, όπως η εμφάνιση, ο τύπος, το όνομα, η διεύθυνση IP και η διεύθυνση MAC της συσκευής στο τοπικό δίκτυο σε σχέση με τις πληροφορίες άδειας χρήσης. Οι πληροφορίες περιλαμβάνουν επίσης τον τύπο ασύρματης ασφάλειας και τον τύπο ασύρματης κρυπτογράφησης για συσκευές δρομολογητή. Αυτή η λειτουργία μπορεί να παρέχει επίσης πληροφορίες που αφορούν τη διαθεσιμότητα της λύσης λογισμικού ασφάλειας για την εξασφάλιση των συσκευών στο τοπικό δίκτυο.

Προστασία κατά της κατάχρησης δεδομένων. Εφαρμόζονται πρόσθετες διατάξεις στην Προστασία κατά της κατάχρησης δεδομένων ως ακολούθως:

Το Λογισμικό περιέχει μια λειτουργία που εμποδίζει την απώλεια ή κατάχρηση κρίσιμων δεδομένων που συνδέονται άμεσα με την κλοπή υπολογιστή. Η λειτουργία αυτή είναι απενεργοποιημένη σύμφωνα με τις προεπιλεγμένες ρυθμίσεις του Λογισμικού. Για να ενεργοποιηθεί πρέπει να δημιουργηθεί ο λογαριασμός ESET HOME, μέσω του οποίου η λειτουργία ενεργοποιεί τη συλλογή δεδομένων στην περίπτωση κλοπής του υπολογιστή. Εάν ενεργοποιήσετε αυτήν τη λειτουργία του Λογισμικού, θα συλλέγονται και θα αποστέλλονται δεδομένα σχετικά με τον κλαπέντα υπολογιστή στον Πάροχο, τα οποία μπορεί να περιλαμβάνουν δεδομένα για την τοποθεσία δικτύου του υπολογιστή, δεδομένα για το περιεχόμενο που εμφανίζεται στην οθόνη του υπολογιστή, δεδομένα για τη διαμόρφωση του

υπολογιστή ή/και δεδομένα που καταγράφονται με κάμερα που είναι συνδεδεμένη με τον υπολογιστή (εφεξής «Δεδομένα»). Ο Τελικός χρήστης θα δικαιούται να χρησιμοποιεί τα Δεδομένα που λαμβάνονται με αυτή τη λειτουργία και παρέχονται αποκλειστικά μέσω του Λογαριασμού ESET HOME για την αποκατάσταση μιας ανεπιθύμητης κατάστασης που προκλήθηκε από κλοπή υπολογιστή. Αποκλειστικά για το σκοπό αυτής της λειτουργίας, ο Πάροχος θα επεξεργάζεται τα Δεδομένα όπως ορίζεται στην Πολιτική Απορρήτου και σύμφωνα με τους σχετικούς νομικούς κανονισμούς. Ο Πάροχος θα επιτρέπει στον Τελικό χρήστη να αποκτήσει πρόσβαση στα Δεδομένα για το χρονικό διάστημα που απαιτείται για να επιτύχει το σκοπό για τον οποίο λήφθηκαν τα δεδομένα, το οποίο δεν μπορεί να υπερβαίνει την περίοδο διατήρησης που καθορίζεται στην Πολιτική Απορρήτου. Η προστασία από κατάχρηση δεδομένων θα χρησιμοποιείται αποκλειστικά με υπολογιστές και λογαριασμούς στους οποίους ο Τελικός χρήστης έχει νόμιμη πρόσβαση. Οποιαδήποτε παράνομη χρήση θα αναφέρεται στην αρμόδια αρχή. Ο Πάροχος θα συμμορφώνεται με τους σχετικούς νόμους και θα βοηθά τις αστυνομικές και δικαστικές αρχές σε περίπτωση κατάχρησης. Συμφωνείτε και αποδέχεστε ότι είστε υπεύθυνοι για τη φύλαξη του κωδικού πρόσβασης για πρόσβαση στο λογαριασμό ESET HOME και συμφωνείτε ότι δεν θα αποκαλύψετε τον κωδικό πρόσβασής σας σε κανέναν τρίτο. Ο Τελικός χρήστης είναι υπεύθυνος για οποιαδήποτε δραστηριότητα με τη χρήση της λειτουργίας Προστασίας από κατάχρηση δεδομένων (Protection Against Misuse of Data) και του λογαριασμού ESET HOME, εξουσιοδοτημένη ή μη. Εάν ο Λογαριασμός ESET HOME υποστεί παραβίαση, ειδοποιήστε αμέσως τον Πάροχο. Εφαρμόζονται πρόσθετες διατάξεις για την Προστασία κατά της κατάχρησης δεδομένων αποκλειστικά για τους τελικούς χρήστες των προϊόντων ESET Internet Security και ESET Smart Security Premium.

ESET Secure Data. Εφαρμόζονται πρόσθετες διατάξεις στο ESET Secure Data ως ακολούθως:

1. Ορισμοί. Σε αυτές τις πρόσθετες διατάξεις στο ESET Secure Data, οι παρακάτω λέξεις έχουν την αντίστοιχη σημασία:

α) «Πληροφορίες» οποιεσδήποτε πληροφορίες ή δεδομένα, τα οποία κρυπτογραφούνται ή αποκρυπτογραφούνται με χρήση του λογισμικού,

β) «Προϊόντα» το λογισμικό και η τεκμηρίωση του ESET Secure Data,

γ) «ESET Secure Data» το λογισμικό που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση ηλεκτρονικών δεδομένων,

Όλες οι αναφορές στον πληθυντικό θα περιλαμβάνουν επίσης τον ενικό και όλες οι αναφορές στο αρσενικό γένος θα περιλαμβάνουν επίσης το θηλυκό και το ουδέτερο γένος και αντίστροφα. Οι λέξεις χωρίς συγκεκριμένο ορισμό θα χρησιμοποιούνται σύμφωνα με τους ορισμούς που παρέχονται στη Συμφωνία.

2. Πρόσθετη δήλωση Τελικού Χρήστη. Συμφωνείτε και αποδέχεστε ότι:

α) η προστασία και η φύλαξη των πληροφοριών σας και δημιουργία αντιγράφων ασφαλείας αυτών των πληροφοριών αποτελεί δική σας ευθύνη,

β) θα πρέπει να δημιουργείτε πλήρη αντίγραφα ασφαλείας για όλες τις πληροφορίες και τα δεδομένα σας (συμπεριλαμβανομένων, ενδεικτικά, όλων τω κρίσιμων πληροφοριών και δεδομένων) στον υπολογιστή σας πριν από την εγκατάσταση του ESET Secure Data,

γ) πρέπει να διατηρείτε ασφαλές αρχείο των κωδικών πρόσβασης ή άλλων πληροφοριών που χρησιμοποιούνται για τη ρύθμιση και τη χρήση του ESET Secure Data, καθώς επίσης και να δημιουργείτε αντίγραφα ασφαλείας όλων των κλειδιών κρυπτογράφησης, κωδικών άδειας χρήσης,

αρχείων κλειδιών και άλλων δεδομένων που δημιουργούνται σε ξεχωριστά μέσα αποθήκευσης,

δ) είστε υπεύθυνοι για τη χρήση των Προϊόντων. Ο Πάροχος δεν φέρει καμιά ευθύνη για τυχόν απώλεια, αξίωση ή βλάβη που προκύπτει ως αποτέλεσμα οποιασδήποτε μη εξουσιοδοτημένης ή λανθασμένης κρυπτογράφησης ή αποκρυπτογράφησης πληροφοριών ή άλλων δεδομένων, ανεξάρτητα από τη θέση και τον τρόπο με τον οποία αποθηκεύονται οι πληροφορίες ή τα δεδομένα αυτά,

ε) παρόλο που ο Πάροχος έχει λάβει όλα τα εύλογα μέτρα για τη διαφύλαξη της ακεραιότητας και της ασφάλειας του ESET Secure Data, τα προϊόντα (ή οποιαδήποτε από τα προϊόντα) δεν πρέπει να χρησιμοποιούνται σε οποιαδήποτε περιοχή που εξαρτάται από επίπεδο ασφάλειας χωρίς αστοχίες ή σε περιοχές δυνητικά επιβλαβείς ή επικίνδυνες, συμπεριλαμβανομένων, ενδεικτικά, πυρηνικών εγκαταστάσεων, συστημάτων πλοήγησης, ελέγχου ή επικοινωνίας αεροσκαφών, οπλικών και αμυντικών συστημάτων και συστημάτων παρακολούθησης και υποστήριξης ασθενών,

στ) αποτελεί ευθύνη του Τελικού Χρήστη να εξασφαλίζει ότι το επίπεδο ασφάλειας και κρυπτογράφησης που παρέχεται από το προϊόντα είναι επαρκές για τις απαιτήσεις του,

ζ) είστε υπεύθυνοι για τη χρήση των Προϊόντων ή οποιωνδήποτε προϊόντων, διασφαλίζοντας, ενδεικτικά, ότι η χρήση αυτή συμμορφώνεται με το σύνολο της ισχύουσας νομοθεσίας και των κανονισμών της Δημοκρατίας της Σλοβακίας ή της αντίστοιχης χώρας, περιοχής ή κράτους όπου χρησιμοποιούνται τα προϊόντα. Πρέπει να διασφαλίζετε πριν από οποιαδήποτε χρήση των προϊόντων ότι δεν παραβιάζονται εμπορικοί περιορισμοί (στη Δημοκρατία της Σλοβακίας ή στην αντίστοιχη χώρα),

η) Το ESET Secure Data μπορεί να επικοινωνεί κατά διαστήματα με τους διακομιστές του Παρόχου, προκειμένου να ελέγξει πληροφορίες άδειας χρήσης, διαθέσιμες ενημερώσεις κώδικα, service pack και άλλες ενημερώσεις που είναι δυνατό να βελτιώσουν, να διορθώσουν, να τροποποιήσουν ή να αναβαθμίσουν τη λειτουργία του ESET Secure Data. Το λογισμικό είναι δυνατό να αποστέλλει γενικές πληροφορίες συστήματος σχετικά με τη λειτουργία του, σύμφωνα με την Πολιτική Απορρήτου.

θ) Ο Πάροχος δεν φέρει καμιά ευθύνη για τυχόν απώλεια, βλάβη, δαπάνη ή αξίωση που προκύπτει ως αποτέλεσμα απώλειας, κλοπής, παραβίασης, βλάβης ή καταστροφής κωδικών πρόσβασης, πληροφοριών διαμόρφωσης, κλειδιών κρυπτογράφησης, κωδικών ενεργοποίησης άδειας χρήσης και άλλων δεδομένων που δημιουργούνται ή αποθηκεύονται κατά τη χρήση του λογισμικού.

Εφαρμόζονται πρόσθετες διατάξεις για το ESET Secure Data αποκλειστικά για τους τελικούς χρήστες του ESET Smart Security Premium.

Password Manager Λογισμικό. Εφαρμόζονται πρόσθετες διατάξεις στο Λογισμικό Password Manager ως ακολούθως:

1. Πρόσθετη δήλωση Τελικού Χρήστη. Συμφωνείτε και αποδέχεστε ότι απαγορεύεται:

α) η χρήση του λογισμικού Password Manager για κρίσιμες εφαρμογές οι οποίες ενέχουν κινδύνους για την ανθρώπινη ζωή ή περιουσία. Κατανοείτε ότι το λογισμικό Password Manager δεν είναι σχεδιασμένο για τέτοιους σκοπούς και ότι η μη ενδεδειγμένη χρήση του σε αυτές τις περιπτώσεις μπορεί να οδηγήσει σε θάνατο, τραυματισμό ή σε καταστροφή περιουσίας ή περιβαλλοντική καταστροφή, για τις οποίες ο Πάροχος δεν είναι υπεύθυνος.

ΤΟ ΛΟΓΙΣΜΙΚΟ PASSWORD MANAGER ΔΕΝ ΕΝΑΙ ΣΧΕΔΙΑΣΜΕΝΟ ΚΑΙ ΔΕΝ ΠΡΟΟΡΙΖΕΤΑΙ Ή ΑΔΕΙΟΔΟΤΕΙΤΑΙ ΓΙΑ ΧΡΗΣΗ ΣΕ ΕΠΙΚΙΝΔΥΝΑ ΠΕΡΙΒΑΛΛΟΝΤΑ ΠΟΥ ΑΠΑΙΤΟΥΝ ΕΛΕΓΧΟ ΑΣΦΑΛΟΥΣ ΛΕΙΤΟΥΡΓΙΑΣ ΟΠΩΣ, ΕΝΔΕΙΚΤΙΚΑ, ΓΙΑ ΤΟ ΣΧΕΔΙΑΣΜΟ, ΚΑΤΑΣΚΕΥΗ, ΣΥΝΤΗΡΗΣΗ Ή ΛΕΙΤΟΥΡΓΙΑ ΠΥΡΗΝΙΚΩΝ

ΕΓΚΑΤΑΣΤΑΣΕΩΝ, ΣΥΣΤΗΜΑΤΩΝ ΠΛΟΗΓΗΣΗΣ Ή ΕΠΙΚΟΙΝΩΝΙΑΣ ΑΕΡΟΣΚΑΦΩΝ, ΣΥΣΤΗΜΑΤΩΝ ΕΝΑΕΡΙΑΣ ΚΥΚΛΟΦΟΡΙΑΣ, ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΣΤΗΡΙΞΗΣ ΑΣΘΕΝΩΝ Ή ΟΠΛΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ. Ο ΠΑΡΟΧΟΣ ΑΠΟΠΟΙΕΙΤΑΙ ΟΠΟΙΑΔΗΠΟΤΕ ΡΗΤΗ Ή ΕΜΜΕΣΗ ΕΓΓΥΗΣΗ ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ ΓΙΑ ΤΕΤΟΙΟΥΣ ΣΚΟΠΟΥΣ.

β) η χρήση του λογισμικού Password Manager με τρόπο που παραβιάζει την παρούσα συμφωνία ή τους νόμους της Δημοκρατίας της Σλοβακίας ή της χώρας δικαιοδοσίας σας. Ειδικότερα, απαγορεύεται η χρήση του λογισμικού Password Manager για την πραγματοποίηση ή προώθηση παράνομων δραστηριοτήτων, όπως την αποστολή δεδομένων βλαβερού περιεχομένου ή περιεχομένου που μπορεί να χρησιμοποιηθεί για παράνομες δραστηριότητες ή που παραβιάζει με οποιονδήποτε τρόπο τη νομοθεσία ή τα δικαιώματα τρίτων (συμπεριλαμβανομένων δικαιωμάτων πνευματικής ιδιοκτησίας), όπως, ενδεικτικά, απόπειρες απόκτησης πρόσβασης σε λογαριασμούς στον Χώρο αποθήκευσης (για τους σκοπούς αυτών των πρόσθετων όρων για το Λογισμικό Password Manager, ο όρος «Χώρος αποθήκευσης» αναφέρεται στον χώρο αποθήκευσης δεδομένων τον οποίο διαχειρίζεται ο Πάροχος ή κάποιος τρίτος, ανεξάρτητος από τον Πάροχο και τον χρήστη, για τον σκοπό του συγχρονισμού και της δημιουργίας αντιγράφων ασφαλείας των δεδομένων του χρήστη) ή σε λογαριασμούς και δεδομένα χρηστών άλλων χρηστών του λογισμικού Password Manager ή του Χώρου αποθήκευσης. Εάν παραβιάσετε οποιαδήποτε από αυτές τις διατάξεις, ο Πάροχος δικαιούται να τερματίσει αμέσως την παρούσα συμφωνία και να μεταφέρει σε εσάς τα έξοδα τυχόν απαραίτητης αποκατάστασης, καθώς και να λάβει τα αναγκαία μέτρα για να εμποδίσει την περαιτέρω χρήση του λογισμικού Password Manager εκ μέρους σας, χωρίς τη δυνατότητα επιστροφής χρημάτων.

2. ΠΕΡΙΟΡΙΣΜΕΝΗ ΕΥΘΥΝΗ. ΤΟ ΛΟΓΙΣΜΙΚΟ PASSWORD MANAGER ΠΑΡΕΧΕΤΑΙ "ΩΣ ΕΧΕΙ". ΔΕΝ ΥΠΑΡΧΕΙ ΡΗΤΗ Ή ΕΜΜΕΣΗ ΕΓΓΥΗΣΗ ΟΠΟΙΟΥΔΗΠΟΤΕ ΕΙΔΟΥΣ. ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΤΟ ΛΟΓΙΣΜΙΚΟ ΜΕ ΔΙΚΗ ΣΑΣ ΕΥΘΥΝΗ. Ο ΚΑΤΑΣΚΕΥΑΣΤΗΣ ΔΕΝ ΦΕΡΕΙ ΚΑΜΙΑ ΕΥΘΥΝΗ ΓΙΑ ΑΠΩΛΕΙΑ ΔΕΔΟΜΕΝΩΝ, ΒΛΑΒΕΣ, ΠΕΡΙΟΡΙΣΜΟ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ ΥΠΗΡΕΣΙΑΣ ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΩΝ ΤΥΧΟΝ ΔΕΔΟΜΕΝΩΝ ΠΟΥ ΑΠΟΣΤΕΛΛΟΝΤΑΙ ΑΠΟ ΤΟ ΛΟΓΙΣΜΙΚΟ PASSWORD MANAGER ΣΕ ΕΞΩΤΕΡΙΚΟ ΧΩΡΟ ΑΠΟΘΗΚΕΥΣΗΣ ΓΙΑ ΤΟ ΣΚΟΠΟ ΤΟΥ ΣΥΓΧΡΟΝΙΣΜΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΗ ΔΗΜΙΟΥΡΓΙΑ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ. Η ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕ ΧΡΗΣΗ ΤΟΥ PASSWORD MANAGER ΔΕΝ ΣΥΝΕΠΑΓΕΤΑΙ ΚΑΜΙΑ ΕΥΘΥΝΗ ΤΟΥ ΠΑΑΡΟΧΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ ΑΥΤΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ. ΣΥΜΦΩΝΕΙΤΕ ΡΗΤΩΣ ΟΤΙ ΤΑ ΔΕΔΟΜΕΝΑ ΠΟΥ ΛΑΜΒΑΝΟΝΤΑΙ, ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ, ΚΡΥΠΤΟΓΡΑΦΟΥΝΤΑΙ, ΑΠΟΘΗΚΕΥΟΝΤΑΙ, ΣΥΓΧΡΟΝΙΖΟΝΤΑΙ Ή ΑΠΟΣΤΕΛΛΟΝΤΑΙ ΜΕΣΩ ΤΟΥ PASSWORD MANAGER ΜΠΟΡΟΥΝ ΕΠΙΣΗΣ ΝΑ ΑΠΟΘΗΚΕΥΟΝΤΑΙ ΣΕ ΔΙΑΚΟΜΙΣΤΕΣ ΤΡΙΤΩΝ (ΙΣΧΥΕΙ ΜΟΝΟ ΓΙΑ ΤΗ ΧΡΗΣΗ ΤΟΥ PASSWORD MANAGER ΟΠΟΥ ΕΧΟΥΝ ΕΝΕΡΓΟΠΟΙΗΘΕΙ ΟΙ ΥΠΗΡΕΣΙΕΣ ΣΥΓΧΡΟΝΙΣΜΟΥ ΚΑΙ ΔΗΜΙΟΥΡΓΙΑΣ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ). ΕΑΝ Ο ΠΑΡΟΧΟΣ, ΚΑΤΑ ΤΗ ΔΙΑΚΡΙΤΙΚΗ ΤΟΥ ΕΥΧΕΡΕΙΑ, ΕΠΙΛΕΞΕΙ ΝΑ ΧΡΗΣΙΜΟΠΟΙΗΣΕΙ ΧΩΡΟ ΑΠΟΘΗΚΕΥΣΗΣ, ΙΣΤΟΤΟΠΟ, ΠΥΛΗ, ΔΙΑΚΟΜΙΣΤΗ Ή ΥΠΗΡΕΣΙΑ, Ο ΠΑΡΟΧΟΣ ΔΕΝ ΕΙΝΑΙ ΥΠΕΥΘΥΝΟΣ ΓΙΑ ΤΗΝ ΠΟΙΟΤΗΤΑ, ΤΗΝ ΑΣΦΑΛΕΙΑ Ή ΤΗ ΔΙΑΘΕΣΙΜΟΤΗΤΑ ΤΗΣ ΑΝΤΙΣΤΟΙΧΗΣ ΥΠΗΡΕΣΙΑΣ ΚΑΙ ΔΕΝ ΦΕΡΕΙ ΚΑΜΙΑ ΕΥΘΥΝΗ ΑΠΕΝΑΝΤΙ ΣΑΣ ΓΙΑ ΤΥΧΟΝ ΠΑΡΑΒΙΑΣΗ ΣΤΜΦΩΝΙΑΣ Η ΝΟΜΙΚΩΝ ΥΠΟΧΡΕΩΣΕΩΝ ΑΠΟ ΤΟ ΤΡΙΤΟ ΜΕΡΟΣ, ΟΥΤΕ ΓΙΑ ΒΛΑΒΕΣ, ΑΠΩΛΕΙΑ ΚΕΡΔΩΝ, ΖΗΜΙΑ ΟΙΚΟΝΟΜΙΚΗ Ή ΜΗ, Ή ΑΛΛΕΣ ΑΠΩΛΕΙΕΣ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΗ ΧΡΗΣΗ ΤΗΣ ΣΥΣΚΕΥΗΣ. Ο ΠΑΡΟΧΟΣ ΔΕΝ ΕΙΝΑΙ ΥΠΕΥΘΥΝΟΣ ΓΙΑ ΤΟ ΠΕΡΙΕΧΟΜΕΝΟ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΟΥ ΛΑΜΒΑΝΟΝΤΑΙ, ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ, ΚΡΥΠΤΟΓΡΑΦΟΥΝΤΑΙ, ΑΠΟΘΗΚΕΥΟΝΤΑΙ, ΣΥΓΧΡΟΝΙΖΟΝΤΑΙ Ή ΑΠΟΣΤΕΛΛΟΝΤΑΙ ΜΕΣΩ ΤΟΥ PASSWORD Ή ΒΡΙΣΚΟΝΤΑΙ ΣΤΟ ΧΩΡΟ ΑΠΟΘΗΚΕΥΣΗΣ. ΑΝΑΓΝΩΡΙΖΕΤΕ ΟΤΙ Ο ΠΑΡΟΧΟΣ ΔΕΝ ΕΧΕΙ ΠΡΟΣΒΑΣΗ ΣΤΟ ΠΕΡΙΕΧΟΜΕΝΟ ΤΩΝ ΑΠΟΘΗΚΕΥΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΕΝ ΕΙΝΑΙ ΣΕ ΘΕΣΗ ΝΑ ΤΟ ΠΑΡΑΚΟΛΟΥΘΕΙ Ή ΝΑ ΚΑΤΑΡΓΗΣΕΙ ΒΛΑΒΕΡΟ Ή ΠΑΡΑΝΟΜΟ ΠΕΡΙΕΧΟΜΕΝΟ.

Ο Πάροχος κατέχει όλα τα δικαιώματα για βελτιώσεις, αναβαθμίσεις και διορθώσεις που σχετίζονται με το λογισμικό Password MANAGER ("Βελτιώσεις") ακόμη και στην περίπτωση που τέτοιες βελτιώσεις έχουν δημιουργηθεί με βάση σχόλια, ιδέες ή προτάσεις που έχετε υποβάλει σε οποιαδήποτε μορφή. Δεν έχετε δικαίωμα αποζημίωσης, συμπεριλαμβανομένων τυχόν δικαιωμάτων πνευματικής ιδιοκτησίας σε σχέση με τις εν λόγω Βελτιώσεις.

Ο ΠΑΡΟΧΟΣ ΚΑΙ ΟΙ ΑΔΕΙΟΔΟΤΕΣ ΔΕΝ ΦΕΡΟΥΝ ΚΑΜΙΑ ΕΥΘΥΝΗ ΑΠΕΝΑΝΤΙ ΣΑΣ ΣΧΕΤΙΚΑ ΜΕ ΑΞΙΩΣΕΙΣ ΟΠΟΙΟΥΔΗΠΟΤΕ ΕΙΔΟΥΣ ΟΙ ΟΠΟΙΕΣ ΠΡΟΚΥΠΤΟΥΝ ΑΠΟ Η ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΗ ΧΡΗΣΗ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ PASSWORD MANAGER ΑΠΟ ΣΑΣ Η ΑΠΟ ΤΡΙΤΟΥΣ, ΜΕ ΤΗ ΧΡΗΣΗ Η ΜΗ ΧΡΗΣΗ ΟΠΟΙΟΔΗΠΟΤΕ ΜΕΣΑΖΟΝΤΑ Η ΜΕΤΑΠΩΛΗΤΗ, Η ΜΕ ΤΗΝ ΠΩΛΗΣΗ Η ΤΗΝ ΑΓΟΡΑ ΟΠΟΙΟΥΔΗΠΟΤΕ ΤΙΤΛΟΥ, ΑΝΕΞΑΡΤΗΤΑ ΑΠΟ ΤΗ ΝΟΜΙΚΗ ΘΕΩΡΗΣΗ ΣΤΗΝ ΟΠΟΙΑ ΒΑΣΙΖΟΝΤΑΙ ΑΥΤΕΣ ΟΙ ΑΞΙΩΣΕΙΣ.

Ο ΠΑΡΟΧΟΣ ΚΑΙ ΟΙ ΑΔΕΙΟΔΟΤΕΣ ΔΕΝ ΦΕΡΟΥΝ ΚΑΜΙΑ ΕΥΘΥΝΗ ΑΠΕΝΑΝΤΙ ΣΑΣ ΓΙΑ ΤΥΧΟΝ ΑΜΕΣΕΣ, ΕΙΔΙΚΕΣ, ΕΜΜΕΣΕΣ Ή ΣΥΜΠΤΩΜΑΤΙΚΕΣ ΒΛΑΒΕΣ ΠΟΥ ΠΡΟΚΥΠΤΟΥΝ ΑΠΟ Ή ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΛΟΓΙΣΜΙΚΟ ΤΡΙΤΩΝ, ΔΕΔΟΜΕΝΑ Η ΠΡΟΣΒΑΣΗ ΤΩΝ ΟΠΟΙΩΝ ΠΡΑΓΜΑΤΟΠΟΙΕΙΤΑΙ ΜΕΣΩ ΤΟΥ PASSWORD MANAGER, ΤΗΝ ΕΚ ΜΕΡΟΥΣ ΣΑΣ ΧΡΗΣΗ Ή ΑΔΥΝΑΜΙΑ ΧΡΗΣΗΣ Ή ΠΡΟΣΒΑΣΗΣ ΤΟΥ PASSWORD MANAGER, Ή ΔΕΔΟΜΕΝΑ ΠΟΥ ΠΑΡΕΧΟΝΤΑΙ ΜΕΣΩ ΤΟΥ PASSWORD MANAGER, ΑΝΕΞΑΡΤΗΤΑ ΑΠΟ ΤΗ ΝΟΜΙΚΗ ΘΕΩΡΗΣΗ ΣΤΗΝ ΟΠΟΙΑ ΒΑΣΙΖΟΝΤΑΙ ΟΙ ΑΞΙΩΣΕΙΣ ΑΥΤΕΣ. ΟΙ ΖΗΜΙΕΣ ΠΟΥ ΑΠΟΚΛΕΙΟΝΤΑΙ ΑΠΟ ΑΥΤΗ ΤΗΝ ΠΑΡΑΓΡΑΦΟ ΠΕΡΙΛΑΜΒΑΝΟΥΝ, ΕΝΔΕΙΚΤΙΚΑ, ΑΠΩΛΕΙΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΕΡΔΩΝ, ΤΡΑΥΜΑΤΙΣΜΟ Ή ΚΑΤΑΣΤΡΟΦΗ ΠΕΡΙΟΥΣΙΑΣ, ΔΙΑΚΟΠΗ ΕΠΙΧΕΙΡΗΜΑΤΙΚΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ, ΑΠΩΛΕΙΑ ΕΠΑΓΓΕΛΜΑΤΙΚΩΝ Ή ΠΡΟΣΩΠΙΚΩΝ ΠΛΗΡΟΦΟΡΙΩΝ. ΟΡΙΣΜΕΝΑ ΔΙΚΑΣΤΗΡΙΑ ΔΕΝ ΕΠΙΤΡΕΠΟΥΝ ΤΟΝ ΠΕΡΙΟΡΙΣΜΟ ΤΩΝ ΣΥΜΠΤΩΜΑΤΙΚΩΝ Ή ΣΥΝΕΠΑΓΟΜΕΝΩΝ ΒΛΑΒΩΝ, ΣΥΝΕΠΩΣ ΑΥΤΟΣ Ο ΠΕΡΙΟΡΙΣΜΟΣ ΕΝΔΕΧΕΤΑΙ ΝΑ ΜΗΝ ΙΣΧΥΕΙ ΓΙΑ ΣΑΣ. ΣΤΗΝ ΠΕΡΙΠΤΩΣΗ ΑΥΤΗ, Η ΕΚΤΑΣΗ ΤΗΣ ΕΥΘΥΝΗΣ ΤΟΥ ΠΑΡΟΧΟΥ ΘΑ ΕΙΝΑΙ Η ΕΛΑΧΙΣΤΗ ΠΟΥ ΠΡΟΒΛΕΠΕΤΑΙ ΑΠΟ ΤΗΝ ΙΣΧΟΥΣΑ ΝΟΜΟΘΕΣΙΑ.

ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ ΠΟΥ ΠΑΡΕΧΟΝΤΑΙ ΜΕΣΩ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ PASSWORD MANAGER, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΩΝ ΤΙΜΩΝ ΜΕΤΟΧΩΝ, ΑΝΑΛΥΣΕΩΝ, ΠΛΗΡΟΦΟΡΙΩΝ ΑΓΟΡΑΣ, ΕΙΔΗΣΕΩΝ ΚΑΙ ΟΙΚΟΝΟΜΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΕΝΔΕΧΕΤΑΙ ΝΑ ΕΡΧΟΝΤΑΙ ΜΕ ΚΑΘΥΣΤΕΡΗΣΗ, ΝΑ ΕΙΝΑΙ ΑΝΑΚΡΙΒΕΙΣ Ή ΝΑ ΠΕΡΙΕΧΟΥΝ ΛΑΘΗ Ή ΠΑΡΑΛΕΙΨΕΙΣ. Ο ΠΑΡΟΧΟΣ ΚΑΙ ΟΙ ΑΔΕΙΟΔΟΤΕΣ ΔΕΝ ΦΕΡΟΥΝ ΚΑΜΙΑ ΕΥΘΥΝΗ ΣΧΕΤΙΚΑ ΜΕ ΤΑ ΠΑΡΑΠΑΝΩ. Ο ΠΑΡΟΧΟΣ ΕΧΕΙ ΤΟ ΔΙΚΑΙΩΜΑ ΝΑ ΤΡΟΠΟΠΟΙΗΣΕΙ Ή ΝΑ ΔΙΑΚΟΨΕΙ ΟΠΟΙΑΔΗΠΟΤΕ ΠΤΥΧΗ Ή ΔΥΝΑΤΟΤΗΤΑ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ PASSWORD MANAGER Ή ΤΗ ΧΡΗΣΗ ΟΛΩΝ Ή ΟΡΙΣΜΕΝΩΝ ΔΥΝΑΤΟΤΗΤΩΝ Ή ΤΕΧΝΟΛΟΓΙΩΝ ΤΟΥ PASSWORD MANAGER ΟΠΟΙΑΔΗΠΟΤΕ ΣΤΙΓΜΗ ΧΩΡΙΣ ΠΡΟΗΓΟΥΜΕΝΗ ΕΙΔΟΠΟΙΗΣΗ.

ΕΑΝ ΟΙ ΔΙΑΤΑΞΕΙΣ ΣΕ ΑΥΤΟ ΤΟ ΑΡΘΡΟ ΑΚΥΡΩΘΟΥΝ ΓΙΑ ΟΠΟΙΟΝΔΗΠΟΤΕ ΛΟΓΟ Ή ΕΑΝ Ο ΠΑΡΟΧΟΣ ΚΡΙΘΕΙ ΥΠΕΥΘΥΝΟΣ ΓΙΑ ΑΠΩΛΕΙΕΣ, ΒΛΑΒΕΣ Κ.ΛΠ., ΥΠΟ ΤΗΝ ΙΣΧΥΟΥΣΑ ΝΟΜΟΘΕΣΙΑ, ΤΑ ΜΕΡΗ ΣΥΜΦΩΝΟΥΝ ΟΤΙ Η ΕΥΘΥΝΗ ΤΟΥ ΠΑΡΟΧΟΥ ΠΡΟΣ ΕΣΑΣ ΠΕΡΙΟΡΙΖΕΤΑΙ ΣΤΟ ΣΥΝΟΛΙΚΟ ΠΟΣΟ ΠΟΥ ΚΑΤΑΒΑΛΑΤΕ ΓΙΑ ΤΗΝ ΑΓΟΡΑ ΤΗΣ ΑΔΕΙΑΣ ΧΡΗΣΗΣ.

ΣΥΜΦΩΝΕΙΤΕ ΟΤΙ Ο ΠΑΡΟΧΟΣ ΚΑΙ ΟΙ ΥΠΑΛΛΗΛΟΙ ΤΟΥ, ΟΙ ΑΝΤΙΠΡΟΣΩΠΟΙ ΤΟΥ, ΟΙ ΘΥΓΑΤΡΙΚΕΣ ΤΟΥ ΚΑΙ ΑΛΛΟΙ ΣΥΝΕΡΓΑΤΕΣ ΤΟΥ ΔΕΝ ΦΕΡΟΥΝ ΚΑΜΙΑ ΕΥΘΥΝΗ ΑΠΕΝΑΝΤΙ ΣΕ ΟΠΟΙΟΝΔΗΠΟΤΕ (ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΩΝ ΚΑΤΟΧΩΝ ΤΗΣ ΣΥΣΚΕΥΗΣ Ή ΤΡΙΤΩΝ ΤΩΝ ΟΠΟΙΩΝ ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΕΠΗΡΕΑΖΟΝΤΑΙ ΑΠΟ ΤΑ ΔΕΟΜΕΝΑ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΣΤΟ ΛΟΓΙΣΜΙΚΟ PASSWORD MANAGER Ή ΣΤΟ ΜΕΣΟ ΑΠΟΘΗΚΕΥΣΗΣ) ΣΧΕΤΙΚΑ ΜΕ ΑΞΙΩΣΕΙΣ, ΑΠΩΛΕΙΕΣ, ΔΑΠΑΝΕΣ Ή ΧΡΕΩΣΕΙΣ ΜΕ ΤΙΣ ΟΠΟΙΕΣ ΕΝΔΕΧΟΜΕΝΩΣ ΕΠΙΒΑΡΥΘΝΟΥΝ ΤΑ ΜΕΡΗ ΑΥΤΑ ΩΣ ΣΥΝΕΠΕΙΑ ΤΗΣ ΧΡΗΣΗΣ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ PASSWORD MANAGER.

3. Δεδομένα στο λογισμικό Password Manager. Εκτός εάν επιλέξετε διαφορετικά και ρητώς, όλα τα δεδομένα που φυλάσσονται σε βάση δεδομένων του λογισμικού Password Manager αποθηκεύονται σε κρυπτογραφημένη μορφή στον υπολογιστή σας ή σε άλλη συσκευή αποθήκευσης που καθορίζετε εσείς. Κατανοείτε ότι, σε περίπτωση διαγραφής ή βλάβης της βάσης δεδομένων ή άλλων αρχείων του λογισμικού Password Manager, όλα τα δεδομένα που περιέχονται εκεί θα χαθούν οριστικά, και επίσης κατανοείτε και αποδέχεστε το ενδεχόμενο μιας τέτοιας απώλειας. Το γεγονός ότι τα προσωπικά σας δεδομένα αποθηκεύονται σε κρυπτογραφημένη μορφή στον υπολογιστή δεν συνεπάγεται ότι οι πληροφορίες δεν είναι δυνατό να κλαπούν ή να παραβιαστούν από κάποιον που ανακαλύπτει τον κύριο κωδικό πρόσβασης ή αποκτά πρόσβαση στη συσκευή ενεργοποίησης που ορίζεται από τον πελάτη για το άνοιγμα της βάσης δεδομένων. Είστε υπεύθυνοι για την ασφάλεια όλων των μεθόδων πρόσβασης.

4. Μετάδοση προσωπικών δεδομένων στον Πάροχο ή στο Χώρο αποθήκευσης. Εάν το επιλέξετε, και αποκλειστικά για τον έγκαιρο συγχρονισμό και τη δημιουργία αντιγράφων ασφαλείας των δεδομένων, το λογισμικό Password Manager μεταδίδει ή αποστέλλει προσωπικά δεδομένα από τη βάση δεδομένων του Password Manager - δηλαδή κωδικούς πρόσβασης, στοιχεία σύνδεσης, Λογαριασμούς και Ταυτότητες - μέσω διαδικτύου στο Χώρο αποθήκευσης. Τα δεδομένα μεταδίδονται αποκλειστικά σε κρυπτογραφημένη μορφή. Η χρήση του Password Manager για τη συμπλήρωση κωδικών πρόσβασης, στοιχείων σύνδεσης ή άλλων δεδομένων σε ηλεκτρονικές φόρμες μπορεί να απαιτεί τη μετάδοση πληροφοριών μέσω διαδικτύου στον ιστότοπο που καθορίζετε. Αυτή η μετάδοση δεδομένων δεν εκκινείται από το Password Manager και συνεπώς ο Πάροχος δεν είναι υπεύθυνος για την ασφάλεια τέτοιων συναλλαγών με ιστότοπους που υποστηρίζονται από άλλους παρόχους. Οποιαδήποτε συναλλαγή μέσω διαδικτύου, είτε σε συνδυασμο με το Password Manager είτε όχι, πραγματοποιείται με δική σας ευθύνη και είστε αποκλειστικά υπύθυνοι για τυχόν βλάβη στον υπολογιστή σας ή απώλεια δεδομένων που προκύπτει από τη λήψη ή/και τη χρήση του υλικού ή της υπηρεσίας. Για την ελαχιστοποίηση του κινδύνου απώλειας σημαντικών δεδομένων, ο Πάροχος συνιστά στους πελάτες να δημιουργούν τακτικά αντίγραφα ασφαλείας της βάσης δεδομένων και άλλων ευαίσθητων αρχείων σε εξωτερικές μονάδες δίσκου. Ο Πάροχος δεν είναι σε θέση να σας παράσχει οποιαδήποτε βοήθεια για την ανάκτηση χαμένων ή κατεστραμμένων δεδομένων. Εάν ο Πάροχος παρέχει υπηρεσίες δημιουργίας αντιγράφων ασφαλείας για τα αρχεία βάσης δεδομένων του χρήστη σε περίπτωση καταστροφής ή διαγραφής των αρχείων στους υπολογιστές των χρηστών, αυτή η υπηρεσία παρέχεται χωρίς εγγύηση και δεν συνεπάγεται καμιά ευθύνη από την πλευρά του Παρόχου προς εσάς.

Με τη χρήση του λογισμικού Password Manager, συμφωνείτε ότι το λογισμικό είναι δυνατό να επικοινωνεί κατά διαστήματα με τους διακομιστές του Παρόχου, προκειμένου να ελέγξει πληροφορίες άδειας χρήσης, διαθέσιμες ενημερώσεις κώδικα, service pack και άλλες ενημερώσεις που είναι δυνατό να βελτιώσουν, να διορθώσουν, να τροποποιήσουν ή να αναβαθμίσουν τη λειτουργία του Password Manager. Το λογισμικό είναι δυνατό να αποστέλλει γενικές πληροφορίες συστήματος σχετικά με τη λειτουργία του Password Manager, σύμφωνα με την Πολιτική Απορρήτου.

5. Κατάργηση εγκατάστασης πληροφορίες and instructions. Εάν υπάρχουν πληροφορίες που θα θέλατε να διατηρήσετε από τη βάση δεδομένων, πρέπει να τις εξαγάγετε πριν από την κατάργηση εγκατάστασης του λογισμικού Password Manager.

Εφαρμόζονται πρόσθετες διατάξεις για το Λογισμικό Password Manager αποκλειστικά για τους τελικούς χρήστες του ESET Smart Security Premium.

ESET LiveGuard. Εφαρμόζονται πρόσθετες διατάξεις στο ESET LiveGuard ως ακολούθως:

Το Λογισμικό περιέχει μια λειτουργία για πρόσθετη ανάλυση των αρχείων που υποβάλλονται από τον τελικό χρήστη. Ο Πάροχος θα χρησιμοποιεί τα αρχεία που υποβάλλονται από τον τελικό χρήστη και τα αποτελέσματα της ανάλυσης μόνο σε συμμόρφωση με την Πολιτική απορρήτου και τους σχετικούς νομικούς κανονισμούς.

Εφαρμόζονται πρόσθετες διατάξεις για το ESET LiveGuard αποκλειστικά για τους τελικούς χρήστες του ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Πολιτική απορρήτου

Η προστασία δεδομένων προσωπικού χαρακτήρα είναι ιδιαίτερα σημαντική για την ESET, spol. s r. o., με έδρα στη διεύθυνση Einsteinova 24, 851 01 Bratislava, Slovak Republic, εγγεγραμμένη στο Εμπορικό

Μητρώο δικαιοδοσίας του Πρώτου Πρωτοδικείου της Μπρατισλάβα, ενότητα Sro, με αριθμό 3586/B, Αριθμός μητρώου επιχειρήσεων: 31333532 ως Υπεύθυνο Επεξεργασίας Δεδομένων («ESET» ή «η εταιρεία»). Η εταιρεία επιθυμεί να συμμορφώνεται με την απαίτηση διαφάνειας, όπως έχει τυποποιηθεί νομικά σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων («ΓΚΠΔ») της ΕΕ. Για να επιτευχθεί αυτός ο στόχος, η εταιρεία δημοσιεύει την παρούσα Πολιτική απορρήτου με αποκλειστικό σκοπό την ενημέρωση του πελάτη («Τελικός χρήστης» ή «χρήστης») ως υποκειμένου των δεδομένων σχετικά με τα ακόλουθα θέματα για τα δεδομένα προσωπικού χαρακτήρα:

- Νομικό έρεισμα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα,
- Κοινή χρήση δεδομένων και Εμπιστευτικότητα,
- Ασφάλεια δεδομένων,
- Τα δικαιώματα του χρήστη ως υποκειμένου των δεδομένων,
- Επεξεργασία των δεδομένων προσωπικού χαρακτήρα
- Πληροφορίες επικοινωνίας.

Νομικό έρεισμα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Υπάρχουν μόνο λίγα νομικά ερείσματα για την επεξεργασία δεδομένων, η οποία χρησιμοποιείται από την εταιρεία σύμφωνα με το σχετικό νομοθετικό πλαίσιο που αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα στην ESET είναι απαραίτητη κυρίως για τη Συμφωνία Άδειας Χρήσης Τελικού Χρήστη («Συμφωνία Άδειας Χρήσης Τελικού Χρήστη») με τον Τελικό χρήστη (Άρθρο 6, παρ. 1, στοιχείο β, του ΓΚΠΔ), η οποία εφαρμόζεται για την παροχή των προϊόντων και των υπηρεσιών της ESET, εκτός εάν αναφέρεται ρητά κάτι άλλο, π.χ.:

- Το νομικό έρεισμα του έννομου συμφέροντος (Άρθρο 6, παρ. 1, στοιχείο στ, του ΓΚΠΔ) επιτρέπει στην εταιρεία να επεξεργάζεται δεδομένα σχετικά με τον τρόπο με τον οποίο οι πελάτες της χρησιμοποιούν τις Υπηρεσίες και την ικανοποίησή τους, ώστε να παρέχονται στους χρήστες η καλύτερη προστασία, υποστήριξη και εμπειρία που μπορεί να προσφέρει η εταιρεία. Ακόμα και η εμπορική προώθηση αναγνωρίζεται από την ισχύουσα νομοθεσία ως έννομο συμφέρον, συνεπώς η εταιρεία στηρίζεται συνήθως σε αυτήν για την επικοινωνία εμπορικής προώθησης με τους πελάτες της.

- Συγκατάθεση, (Άρθρο 6, παρ. 1, στοιχείο α, του ΓΚΠΔ) την οποία ενδέχεται να ζητήσει η εταιρεία από τον χρήστη σε ειδικές περιπτώσεις, εάν θεωρεί η εταιρεία ότι αυτό το νομικό έρεισμα είναι το καταλληλότερο ή εάν απαιτείται από τον νόμο.

- Συμμόρφωση με μια νομική υποχρέωση (Άρθρο 6, παρ. 1, στοιχείο γ, του ΓΚΠΔ), π.χ. καθορισμός απαιτήσεων για ηλεκτρονική επικοινωνία, διατήρηση για παραστατικά τιμολόγησης ή χρέωσης.

Κοινή χρήση δεδομένων και εμπιστευτικότητα

Η εταιρεία δεν κάνει κοινή χρήση των δεδομένων του χρήστη με τρίτους. Ωστόσο, η ESET είναι μια εταιρεία που δραστηριοποιείται σε όλο τον κόσμο μέσω των θυγατρικών εταιρειών ή των συνεργατών της, ως μέρος του δικτύου πωλήσεων, σέρβις και υποστήριξης. Οι πληροφορίες αδειών

χρήσης, χρέωσης και τεχνικής υποστήριξης που επεξεργάζεται η ESET ενδέχεται να μεταφερθούν σε ή από θυγατρικές ή συνεργάτες της για τον σκοπό εκτέλεσης της Συμφωνίας Άδειας Χρήσης Τελικού Χρήστη, όπως η παροχή υπηρεσιών ή η υποστήριξη.

Η ESET προτιμά να επεξεργάζεται τα δεδομένα της στην Ευρωπαϊκή Ένωση (ΕΕ). Ωστόσο, ανάλογα με την τοποθεσία του χρήστη (χρήση των προϊόντων ή/και των υπηρεσιών της εταιρείας εκτός της ΕΕ) ή/και την υπηρεσία που επιλέγει, ενδέχεται να απαιτηθεί η μεταφορά των δεδομένων του χρήστη σε χώρα εκτός της ΕΕ. Για παράδειγμα, η εταιρεία χρησιμοποιεί υπηρεσίες τρίτων σε σχέση με το υπολογιστικό cloud. Σε αυτές τις περιπτώσεις, η εταιρεία επιλέγει προσεκτικά τους παρόχους υπηρεσιών και διασφαλίζει ένα κατάλληλο επίπεδο προστασίας δεδομένων μέσω συμβατικών, καθώς και τεχνικών και οργανωτικών μέτρων. Κατά κανόνα, η εταιρεία συμφωνεί επί των τυποποιημένων συμβατικών ρητρών της ΕΕ, εάν είναι απαραίτητο, με συμπληρωματικούς συμβατικούς κανονισμούς.

Για ορισμένες χώρες εκτός της ΕΕ, όπως το Ηνωμένο Βασίλειο και η Ελβετία, η ΕΕ έχει ήδη καθορίσει ένα αντίστοιχο επίπεδο προστασίας των δεδομένων. Λόγω του αντίστοιχου επιπέδου προστασίας των δεδομένων, η μεταφορά δεδομένων σε αυτές τις χώρες δεν απαιτεί ειδική εξουσιοδότηση ή συμφωνία.

Ασφάλεια δεδομένων

Η ESET υλοποιεί κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ένα επίπεδο ασφάλειας, το οποία είναι κατάλληλο για τους ενδεχόμενους κινδύνους. Η εταιρεία καταβάλλει κάθε προσπάθεια για να διασφαλίζει διαρκώς την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την ανθεκτικότητα των συστημάτων επεξεργασίας και των υπηρεσιών. Ωστόσο, σε περίπτωση παραβίασης δεδομένων που έχει ως αποτέλεσμα κάποιον κίνδυνο για τα δικαιώματα και τις ελευθερίες του χρήστη, η εταιρεία είναι πρόθυμη να ειδοποιήσει την αντίστοιχη εποπτική αρχή, καθώς και τους επηρεαζόμενους Τελικούς χρήστες ως υποκείμενα των δεδομένων.

Δικαιώματα του υποκειμένου δεδομένων

Τα δικαιώματα κάθε Τελικού χρήστη έχουν σημασία και η εταιρεία επιθυμεί να ενημερώσει τον χρήστη ότι η ESET εγγυάται τα ακόλουθα δικαιώματα σε όλους τους Τελικούς χρήστες (από οποιαδήποτε χώρα εντός ή εκτός ΕΕ). Για να ασκήσει ο χρήστης τα δικαιώματα του ως υποκείμενο των δεδομένων, μπορεί να επικοινωνήσει με την εταιρεία μέσω φόρμας υποστήριξης ή μέσω email στη διεύθυνση dpo@eset.sk. Για σκοπούς ταυτοποίησης, η εταιρεία ζητά από τον χρήστη τις ακόλουθες πληροφορίες: Όνομα, διεύθυνση email και - εάν υπάρχει - κλειδί άδειας χρήσης ή αριθμό πελάτη και εταιρική σχέση. Ο χρήστης δεν θα πρέπει να αποστέλλει στην εταιρεία οποιαδήποτε άλλα δεδομένα προσωπικού χαρακτήρα, όπως την ημερομηνία γέννησης. Η εταιρεία θα ήθελε να επισημάνει ότι για να είναι σε θέση να επεξεργαστεί το αίτημα του χρήστη, καθώς και για σκοπούς ταυτοποίησης, θα επεξεργαστεί τα δεδομένα προσωπικού χαρακτήρα του χρήστη.

Δικαίωμα ανάκλησης της συγκατάθεσης. Το δικαίωμα ανάκλησης της συγκατάθεσης εφαρμόζεται στην περίπτωση επεξεργασίας που βασίζεται μόνο στη συγκατάθεση. Εάν η εταιρεία επεξεργαστεί τα δεδομένα προσωπικού χαρακτήρα του χρήστη με βάση η συγκατάθεσή του, ο χρήστης έχει το δικαίωμα να ανακαλέσει τη συγκατάθεση ανά πάσα στιγμή χωρίς αιτιολογία. Η ανάκληση της συγκατάθεσης του χρήστη ισχύει μόνο μελλοντικά και δεν επηρεάζει τη νομιμότητα των δεδομένων που υποβλήθηκαν σε επεξεργασία πριν από την ανάκληση.

Δικαίωμα ένστασης. Το δικαίωμα ένστασης έναντι της επεξεργασίας εφαρμόζεται στην περίπτωση επεξεργασίας που βασίζεται στο έννομο συμφέρον της ESET ή κάποιου τρίτου. Εάν η εταιρεία επεξεργαστεί τα δεδομένα προσωπικού χαρακτήρα του χρήστη για να προστατέψει ένα έννομο

συμφέρον, ο χρήστης ως υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει ένσταση έναντι του έννομου συμφέροντος που κατονομάζεται από την εταιρεία και έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του ανά πάσα στιγμή. Η ένσταση του χρήστη ισχύει μόνο μελλοντικά και δεν επηρεάζει τη νομιμότητα των δεδομένων που υποβλήθηκαν σε επεξεργασία πριν από την ένσταση. Εάν η εταιρεία επεξεργαστεί τα δεδομένα προσωπικού χαρακτήρα του χρήστη για σκοπούς άμεσης εμπορικής προώθησης, τότε ο χρήστης δεν απαιτείται να αιτιολογήσει την ένστασή του. Αυτό ισχύει επίσης στην περίπτωση δημιουργίας προφίλ, στο βαθμό που συνδέεται με την εν λόγω άμεση εμπορική προώθηση. Σε όλες τις άλλες περιπτώσεις, η εταιρεία ζητά από τον χρήστη μια σύντομη ενημέρωση σχετικά με τα παράπονά του κατά του έννομου συμφέροντος της ESET για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα του χρήστη.

Σημειώνεται ότι σε ορισμένες περιπτώσεις, παρά την ανάκληση της συγκατάθεσης εκ μέρους του χρήστη, η εταιρεία δικαιούται να προβεί σε περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα του χρήστη βάσει άλλου νομικού ερείσματος, για παράδειγμα, για την εκτέλεση μιας σύμβασης.

Δικαίωμα πρόσβασης. Ως υποκείμενο των δεδομένων, ο χρήστης έχει το δικαίωμα να λαμβάνει πληροφορίες ανά πάσα στιγμή σχετικά με τα δεδομένα του που αποθηκεύονται από την ESET δωρεάν.

Δικαίωμα επανόρθωσης. Εάν η εταιρεία επεξεργαστεί ακούσια λανθασμένα δεδομένα προσωπικού χαρακτήρα που αφορούν τον χρήστη, ο χρήστης έχει το δικαίωμα να ζητήσει τη διόρθωσή τους.

Δικαίωμα διαγραφής και Δικαίωμα περιορισμού της επεξεργασίας. Ως υποκείμενο των δεδομένων, ο χρήστης έχει το δικαίωμα να ζητήσει τη διαγραφή ή τον περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα του. Εάν η εταιρεία επεξεργαστεί τα δεδομένα προσωπικού χαρακτήρα του χρήστη, για παράδειγμα, με τη συγκατάθεσή του και ο χρήστης ανακαλέσει τη συγκατάθεση, και δεν υπάρχει άλλο νομικό έρεισμα, π.χ. μια σύμβαση, η εταιρεία θα καταργήσει αμέσως τα δεδομένα προσωπικού χαρακτήρα του χρήστη. Τα δεδομένα προσωπικού χαρακτήρα του χρήστη θα καταργηθούν επίσης στο τέλος της περιόδου διατήρησης της εταιρείας, όταν δεν θα είναι πλέον απαραίτητα για τους σκοπούς που αναφέρονται για αυτά.

Εάν η εταιρεία χρησιμοποιήσει τα δεδομένα προσωπικού χαρακτήρα του χρήστη με αποκλειστικό σκοπό την άμεση εμπορική προώθηση και ο χρήστης έχει ανακαλέσει τη συγκατάθεσή του ή έχει υποβάλει ένσταση έναντι του έννομου συμφέροντος της ESET, η εταιρεία θα περιορίσει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στον βαθμό που θα συμπεριλαμβάνονται τα στοιχεία επικοινωνίας του χρήστη στην εσωτερική λίστα αποκλεισμένων διευθύνσεων της εταιρείας, προκειμένου να αποφεύγεται η ανεπιθύμητη επικοινωνία. Διαφορετικά, τα δεδομένα προσωπικού χαρακτήρα του χρήστη θα καταργηθούν.

Σημειώνεται ότι ενδέχεται να απαιτηθεί η αποθήκευση των δεδομένων του χρήστη από την εταιρεία μέχρι τη λήξη των υποχρεώσεων και των περιόδων διατήρησης που ορίζονται από τον νομοθέτη ή τις εποπτικές αρχές. Οι υποχρεώσεις και οι περίοδοι διατήρησης μπορεί να απορρέουν επίσης από τη νομοθεσία της Σλοβακίας. Στη συνέχεια, τα αντίστοιχα δεδομένα θα καταργούνται τακτικά.

Το δικαίωμα στη φορητότητα δεδομένων. Η εταιρεία είναι πρόθυμη να παράσχει στον χρήστη, ως υποκείμενο των δεδομένων, τα δεδομένα προσωπικού χαρακτήρα που έχει επεξεργαστεί η ESET σε μορφή xls.

Δικαίωμα υποβολής καταγγελίας. Ως υποκείμενο των δεδομένων, ο χρήστης έχει το δικαίωμα να υποβάλλει καταγγελία ανά πάσα στιγμή σε μια εποπτική αρχή. Η ESET υπόκειται στους κανονισμούς της νομοθεσίας της Σλοβακίας και δεσμεύεται από τη νομοθεσία περί προστασίας δεδομένων της Ευρωπαϊκής Ένωσης. Η αρμόδια εποπτική αρχή δεδομένων είναι το Γραφείο Προστασίας Δεδομένων

Προσωπικού Χαρακτήρα της Δημοκρατίας της Σλοβακίας, το οποίο βρίσκεται στη διεύθυνση Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Επεξεργασία των δεδομένων προσωπικού χαρακτήρα

Οι υπηρεσίες που παρέχονται από την ESET, οι οποίες υλοποιούνται στο προϊόν της εταιρείας, παρέχονται σύμφωνα με τους όρους χρήσης της EULA, αλλά ορισμένες ενδέχεται να απαιτούν ιδιαίτερη προσοχή. Η εταιρεία θέλει να παράσχει στο χρήστη περισσότερες λεπτομέρειες σχετικά με τη συλλογή δεδομένων που συνδέεται με την παροχή των υπηρεσιών μας. Η εταιρεία παρέχει διάφορες υπηρεσίες που περιγράφονται στην Συμφωνία Άδειας Χρήσης Τελικού Χρήστη και στην τεκμηρίωση. Για να λειτουργούν όλες αυτές οι υπηρεσίες, η εταιρεία πρέπει να συλλέγει τις ακόλουθες πληροφορίες:

Δεδομένα αδειών χρήσης και χρέωσης. Το όνομα, η διεύθυνση email, το κλειδί άδειας χρήσης και (εάν εφαρμόζεται) η διεύθυνση, τα δεδομένα εταιρικής σχέσης και πληρωμών συλλέγονται και υποβάλλονται σε επεξεργασία από την ESET, προκειμένου να διευκολυνθεί η ενεργοποίηση της άδειας χρήσης, η παράδοση του κλειδιού άδειας χρήσης, οι υπενθυμίσεις σχετικά με τη λήξη, τα αιτήματα υποστήριξης, η επαλήθευση γνησιότητας της άδειας χρήσης, η παροχή των υπηρεσιών της εταιρείας και άλλες ειδοποιήσεις, συμπεριλαμβανομένων μηνυμάτων εμπορικής προώθησης, σύμφωνα με την ισχύουσα νομοθεσία ή τη συγκατάθεση του χρήστη. Η ESET υποχρεούται νομικά να διατηρεί τα στοιχεία χρέωσης για περίοδο 10 ετών, ωστόσο οι πληροφορίες άδειας χρήσης θα ανωνυμοποιούνται το αργότερο 12 μήνες μετά τη λήξη της άδειας χρήσης.

Ενημέρωση και άλλα στατιστικά στοιχεία. Οι επεξεργασμένες πληροφορίες περιλαμβάνουν πληροφόρηση που αφορά τη διεργασία εγκατάστασης και τον υπολογιστή του χρήστη, όπως η πλατφόρμα στην οποία έχει εγκατασταθεί το προϊόν της εταιρείας και πληροφορίες σχετικά με τις λειτουργίες και τη λειτουργικότητα των προϊόντων της εταιρείας, όπως το λειτουργικό σύστημα, πληροφορίες για το υλικό, τα αναγνωριστικά εγκατάστασης, τα αναγνωριστικά άδειας χρήσης, τη διεύθυνση IP, τη διεύθυνση MAC, τις ρυθμίσεις για τη ρύθμιση παραμέτρων του προϊόντος. Οι πληροφορίες αυτές υποβάλλονται σε επεξεργασία για το σκοπό παροχής υπηρεσιών ενημέρωσης και αναβάθμισης, και για το σκοπό συντήρησης, ασφάλειας και βελτίωσης της υποδομής παρασκηνίου.

Αυτές οι πληροφορίες τηρούνται ξεχωριστά από τις πληροφορίες ταυτοποίησης που απαιτούνται για τους σκοπούς της άδειας χρήσης και της χρέωσης, επειδή δεν απαιτούν την ταυτοποίηση του Τελικού χρήστη. Η περίοδος διατήρησης είναι μέχρι 4 έτη.

Σύστημα φήμης ESET LiveGrid®. Οι κατακερματισμοί μονής κατεύθυνσης που σχετίζονται με εισβολή υποβάλλονται σε επεξεργασία για τους σκοπούς του Συστήματος φήμης ESET LiveGrid®, το οποίο βελτιώνει την αποτελεσματικότητα των λύσεων της εταιρείας κατά του κακόβουλου λογισμικού, συγκρίνοντας σαρωμένα αρχεία με μια βάση δεδομένων με λίστα μη αποκλεισμένων και λίστα αποκλεισμένων στοιχείων στο cloud. Ο Τελικός χρήστης δεν ταυτοποιείται κατά τη διάρκεια αυτής της διαδικασίας.

Σύστημα ανατροφοδότησης ESET LiveGrid®. Ύποπτα δείγματα και μεταδεδομένα από το πεδίο ως μέρος του συστήματος σχολίων ESET LiveGrid®, το οποίο επιτρέπει στην ESET να αντιδρά αμέσως στις ανάγκες των τελικών χρηστών και ενημερώνει την εταιρεία για τις πιο πρόσφατες απειλές. Η εταιρεία στηρίζεται στους χρήστες για την αποστολή

- Εισβολών, όπως δυνητικά δείγματα ιών και άλλων κακόβουλων προγραμμάτων και ύποπτων, προβληματικών, ενδεχομένως ανεπιθύμητων ή μη ασφαλών αντικειμένων, όπως εκτελέσιμα αρχεία, μηνύματα email που αναφέρονται από τους χρήστες ως ανεπιθύμητα ή επισημαίνονται από το

προϊόν,

- Πληροφορίες που αφορούν τη χρήση του Internet, όπως η διεύθυνση IP και γεωγραφικές πληροφορίες, τα πακέτα IP, οι διευθύνσεις URL και τα πλαίσια ethernet,

- Αρχεία ένδειξης σφαλμάτων διακοπής λειτουργίας και πληροφορίες που περιέχονται εκεί.

Η εταιρεία δεν επιθυμεί να συλλέγει δεδομένα του χρήστη πέρα από αυτό πλαίσιο, αλλά μερικές φορές είναι αδύνατον να αποφευχθεί. Δεδομένα που συλλέγονται κατά λάθος μπορεί να συμπεριλαμβάνονται στο ίδιο το κακόβουλο λογισμικό (συλλέγονται χωρίς να το γνωρίζει ή να το έχει εγκρίνει ο χρήστης) ή ως μέρος ονομάτων αρχείων ή διευθύνσεων URL και η εταιρεία δεν έχει πρόθεση να αποτελούν μέρος των συστημάτων της ή να τα επεξεργαστεί για το σκοπό που δηλώνεται σε αυτή την Πολιτική Απορρήτου.

Όλες οι πληροφορίες που λαμβάνονται και υποβάλλονται σε επεξεργασία μέσω του Συστήματος ανατροφοδότησης ESET LiveGrid® προορίζονται για χρήση χωρίς ταυτοποίηση του Τελικού χρήστη.

Αξιολόγηση ασφάλειας συσκευών συνδεδεμένων στο δίκτυο. Για την παροχή της λειτουργίας αξιολόγησης της ασφάλειας, η εταιρεία επεξεργάζεται το όνομα του τοπικού δικτύου και πληροφορίες για τις συσκευές στο τοπικό δίκτυο, όπως η παρουσία, ο τύπος, το όνομα, η διεύθυνση IP και η διεύθυνση MAC της συσκευής στο τοπικό δίκτυο του χρήστη σε σχέση με τις πληροφορίες άδειας χρήσης. Οι πληροφορίες περιλαμβάνουν επίσης τον τύπο ασύρματης ασφάλειας και τον τύπο ασύρματης κρυπτογράφησης για συσκευές δρομολογητή. Οι πληροφορίες άδειας χρήσης που ταυτοποιούν τον Τελικό χρήστη θα ανωνυμοποιούνται το αργότερο 12 μήνες μετά τη λήξη της άδειας χρήσης.

Τεχνική υποστήριξη. Τα στοιχεία επικοινωνίας και οι πληροφορίες της άδειας χρήσης, καθώς και τα δεδομένα που περιέχονται στα αιτήματα υποστήριξης του χρήστη, ενδέχεται να απαιτούνται για την υπηρεσία υποστήριξης. Ανάλογα με το δίαυλο επικοινωνίας που θα επιλέξει ο χρήστης για να επικοινωνήσει με την εταιρεία, η εταιρεία μπορεί να συλλέξει τη διεύθυνση ηλεκτρονικού ταχυδρομείου, τον αριθμό τηλεφώνου, τις πληροφορίες άδειας χρήσης, τα στοιχεία προϊόντος και την περιγραφή του περιστατικού υποστήριξης του χρήστη. Ενδέχεται να ζητηθεί από το χρήστη να παράσχει στην εταιρεία και άλλες πληροφορίες για να διευκολυνθεί η υπηρεσία της υποστήριξης. Τα δεδομένα που υποβάλλονται σε επεξεργασία για τεχνική υποστήριξη αποθηκεύονται για 4 χρόνια.

Προστασία κατά της κατάχρησης δεδομένων. Εάν ο Λογαριασμός ESET HOME στη διεύθυνση https://home.eset.com δημιουργηθεί και η λειτουργία ενεργοποιηθεί από τον Τελικό χρήστη σε σχέση με την κλοπή του υπολογιστή, θα συλλεχθούν και θα υποβληθούν σε επεξεργασία οι ακόλουθες πληροφορίες: τα δεδομένα τοποθεσίας, στιγμιότυπα οθόνης, τα δεδομένα σχετικά με τη ρύθμιση παραμέτρων του υπολογιστή και δεδομένα που καταγράφηκαν από την κάμερα του υπολογιστή. Τα δεδομένα που συλλέγονται αποθηκεύονται στους διακομιστές της εταιρείας ή στους διακομιστές των παρόχων υπηρεσιών της εταιρείας, με περίοδο διατήρησης 3 μηνών.

Password Manager. Εάν ο χρήστης επιλέξει να ενεργοποιήσει τη λειτουργία Password Manager, τα δεδομένα που σχετίζονται με τα στοιχεία σύνδεσης του χρήστη αποθηκεύονται σε κρυπτογραφημένη μορφή μόνο στον υπολογιστή του χρήστη ή σε άλλη καθορισμένη συσκευή. Εάν ο χρήστης ενεργοποιήσει την υπηρεσία συγχρονισμού, τα κρυπτογραφημένα δεδομένα αποθηκεύονται στους διακομιστές της εταιρείας ή σε διακομιστές των παρόχων υπηρεσιών της εταιρείας, ώστε να διασφαλίζεται η παροχή της υπηρεσίας. Τόσο η ESET όσο και ο πάροχος υπηρεσιών δεν έχουν πρόσβαση στα κρυπτογραφημένα δεδομένα. Το κλειδί για την αποκρυπτογράφηση των δεδομένων το έχει μόνο ο χρήστης. Τα δεδομένα θα καταργηθούν μετά την απενεργοποίηση της λειτουργίας.

ESET LiveGuard. Εάν ο χρήστης επιλέξει να ενεργοποιήσει τη λειτουργία ESET LiveGuard, απαιτείται η υποβολή δειγμάτων, όπως αρχεία προκαθορισμένα και επιλεγμένα από τον Τελικό χρήστη. Τα δείγματα που επιλέγει ο χρήστης για την απομακρυσμένη ανάλυση θα αποσταλούν στην υπηρεσία ESET και το αποτέλεσμα της ανάλυσης θα αποσταλούν στον υπολογιστή του χρήστη. Οποιαδήποτε ύποπτα δείγματα υποβάλλονται σε επεξεργασία με τον τρόπο των πληροφοριών που συλλέγονται από το Σύστημα ανατροφοδότησης ESET LiveGrid®.

Πρόγραμμα βελτίωσης εμπειρίας του πελάτη. Εάν επιλέξατε να ενεργοποιήσετε το Πρόγραμμα βελτίωσης εμπειρίας του πελάτη , οι ανώνυμες πληροφορίες τηλεμετρίας που σχετίζονται με τη χρήση των προϊόντων της εταιρείας θα συλλέγονται και θα χρησιμοποιούνται, με βάση τη συγκατάθεση του χρήστη.

Σημειώνεται ότι εάν το άτομο που χρησιμοποιεί τα προϊόντα και τις υπηρεσίες της εταιρείας δεν είναι ο Τελικός χρήστης που έχει αγοράσει το προϊόν ή την υπηρεσία και έχει συνομολογήσει τη Συμφωνία Άδειας Χρήσης Τελικού Χρήστη με την εταιρεία, (π.χ. ένας υπάλληλος του Τελικού χρήστη, ένα μέλος της οικογένειας ή κάποιο άτομο που εξουσιοδοτείται με άλλον τρόπο από τον Τελικό χρήστη για να χρησιμοποιεί το προϊόν ή την υπηρεσία, σε συμμόρφωση με τη Συμφωνία Άδειας Χρήσης Τελικού Χρήστη, η επεξεργασία των δεδομένων διενεργείται με βάση το έννομο συμφέρον της ESET με την έννοια του Άρθρου 6, παρ. 1, στοιχείο στ, του ΓΚΠΔ, ώστε να επιτρέπεται στον χρήστη που έχει εξουσιοδοτηθεί από τον Τελικό χρήστη να χρησιμοποιεί τα προϊόντα και τις υπηρεσίες που παρέχονται από την εταιρεία, σύμφωνα με τη Συμφωνία Άδειας Χρήσης Τελικού Χρήστη.

Πληροφορίες επικοινωνίας

Εάν ο χρήστης επιθυμεί να ασκήσει το δικαίωμά του ως υποκείμενο δεδομένων ή σε περίπτωση που υπάρχουν ερωτήσεις ή ανησυχίες, μπορεί να αποστείλει μήνυμα στη διεύθυνση:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk