ESET PROTECT On-Prem

Οδηγός εγκατάστασης αναβάθμισης και μετεγκατάστασης

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

Το ESET PROTECT On-Prem 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. 17/4/2024

Σχετικά με τη βοήθεια

Αυτός ο οδηγός εγκατάστασης συντάχτηκε ως βοήθημα για την εγκατάσταση και αναβάθμιση του ESET PROTECT On-Prem και παρέχει οδηγίες για τη διαδικασία.

Για λόγους συνέπειας και για την αποτροπή σύγχυσης, η ορολογία που χρησιμοποιείται σε όλη την έκταση αυτού του οδηγού βασίζεται στα ονόματα παραμέτρων του ESET PROTECT On-Prem. Επίσης, χρησιμοποιείται ένα σύνολο συμβόλων για την επισήμανση θεμάτων ιδιαίτερου ενδιαφέροντος και σημασίας.

Οι σημειώσεις παρέχουν χρήσιμες πληροφορίες, όπως ειδικές δυνατότητες ή έναν σύνδεσμο για κάποιο σχετικό θέμα.

Αυτή η αναφορά απαιτεί την προσοχή σας και δεν θα πρέπει να την παραλείψετε. Συνήθως, παρέχει σημαντικές πληροφορίες, οι οποίες όμως δεν είναι κρίσιμης σημασίας.

Κρίσιμες πληροφορίες τις οποίες θα πρέπει να προσέξετε ιδιαίτερα. Οι προειδοποιήσεις επισημαίνονται ειδικά για να σας αποτρέψουν από δυνητικά επιβλαβή λάθη. Διαβάστε και κατανοήστε το κείμενο που έχει τοποθετηθεί σε προειδοποιητικές αγκύλες, επειδή αναφέρει πολύ ευαίσθητες ρυθμίσεις συστήματος ή κάτι επικίνδυνο.

Σενάριο παραδείγματος που περιγράφει ένα περιστατικό χρήστη που είναι σχετικό με το θέμα στο οποίο περιλαμβάνεται. Τα παραδείγματα χρησιμοποιούνται για να επεξηγήσουν πιο σύνθετα θέματα.

Σύμβαση	Έννοια
Έντονη γραφή	Ονόματα στοιχείων διασύνδεσης, όπως πλαίσια και κουμπιά επιλογών.
Πλάγια γραφή	Σύμβολα κράτησης θέσης για πληροφορίες που παρέχετε. Για παράδειγμα, το όνομα αρχείου ή η διαδρομή σημαίνει ότι πρέπει να πληκτρολογήσετε την πραγματική διαδρομή ή το όνομα του αρχείου.
`Courier New`	Δείγματα κώδικα ή εντολές.
Υπερσύνδεσμος	Παρέχει γρήγορη και εύκολη πρόσβαση σε θέματα παραπομπής ή μια εξωτερική τοποθεσία στο διαδίκτυο. Οι υπερσύνδεσμοι επισημαίνονται με μπλε χρώμα και μπορεί να έχουν υπογράμμιση.
%ProgramFiles%	Ο κατάλογος συστήματος των Windows στον οποίο αποθηκεύονται τα εγκατεστημένα προγράμματα των Windows και άλλα προγράμματα.

- Η ηλεκτρονική βοήθεια είναι η κύρια πηγή περιεχομένου βοήθειας. Η πιο πρόσφατη έκδοση της Ηλεκτρονικής βοήθειας θα εμφανίζεται αυτόματα εάν έχετε λειτουργική σύνδεση Internet. Οι σελίδες ηλεκτρονικής βοήθειας του ESET PROTECT On-Prem περιλαμβάνουν τέσσερις ενεργές καρτέλες στην επάνω κεφαλίδα πλοήγησης: Εγκατάσταση/αναβάθμιση, Διαχείριση και Ανάπτυξη εικονικής συσκευής.

- Τα θέματα σε αυτό τον οδηγό χωρίζονται σε πολλά κεφάλαια και υποκεφάλαια. Μπορείτε να βρείτε σχετικές πληροφορίες χρησιμοποιώντας το πεδίο Αναζήτηση στο επάνω μέρος.

Μόλις ανοίξετε έναν Οδηγό χρήστη από τη γραμμή πλοήγησης στο επάνω μέρος της σελίδας, η αναζήτηση θα περιοριστεί στα περιεχόμενα του συγκεκριμένου οδηγού. Για παράδειγμα, εάν ανοίξετε τον οδηγό Διαχειριστή, τα θέματα από τους οδηγούς Εγκατάσταση/Αναβάθμιση και Ανάπτυξη VA δεν θα περιλαμβάνονται στα αποτελέσματα αναζήτησης.

- 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 τύπων προβλημάτων.

- Το Φόρουμ της ESET παρέχει στους χρήστες της ESET έναν εύκολο τρόπο να λάβουν βοήθεια και να βοηθήσουν άλλους χρήστες. Μπορείτε να δημοσιεύετε οποιοδήποτε πρόβλημα ή ερώτημα που σχετίζεται με τα προϊόντα ESET.

Εγκατάσταση/αναβάθμιση/μετεγκατάσταση

το ESET PROTECT On-Prem είναι μια εφαρμογή που σας επιτρέπει να διαχειρίζεστε προϊόντα ESET σε σταθμούς εργασίας υπολογιστών-πελατών, διακομιστές και κινητές συσκευές σε ένα δικτυωμένο περιβάλλον από μία κεντρική τοποθεσία. Με το ενσωματωμένο σύστημα διαχείρισης εργασιών του ESET PROTECT On-Prem, μπορείτε να εγκαταστήσετε λύσεις ασφάλειας ESET σε απομακρυσμένους υπολογιστές και να αποκριθείτε γρήγορα σε νέα προβλήματα και ανιχνεύσεις.

Το ESET PROTECT On-Prem δεν παρέχει προστασία από κακόβουλο κώδικα μόνο του. Η προστασία του περιβάλλοντός σας εξαρτάται από την παρουσία μιας λύσης ασφάλειας ESET, όπως το ESET Endpoint Security σε σταθμούς εργασίας και κινητές συσκευές ή το ESET Server Security για το Windows σε υπολογιστές διακομιστές.

Από την έκδοση 11.0, το ESET PROTECT μετονομάστηκε σε ESET PROTECT On-Prem.

Το ESET PROTECT On-Prem είναι δομημένο με βάση δύο κύριες αρχές:

- **Κεντρική διαχείριση** - η διαμόρφωση, η διαχείριση και η παρακολούθηση ολόκληρου του δικτύου είναι δυνατή από ένα μέρος.

- **Κλιμάκωση** - το σύστημα μπορεί να αναπτυχθεί σε περιβάλλον μικρού δικτύου, καθώς και σε μεγάλες επιχειρήσεις. Το ESET PROTECT On-Prem είναι σχεδιασμένο για να εξυπηρετεί την ανάπτυξη της υποδομής σας.

Το ESET PROTECT On-Prem υποστηρίζει τη νέα γενιά προϊόντων ασφάλειας ESET, ενώ είναι συμβατό και με τα προϊόντα προηγούμενης γενιάς.

Οι σελίδες βοήθειας του ESET PROTECT On-Prem περιλαμβάνουν έναν πλήρη οδηγό εγκατάστασης και αναβάθμισης:

- Αρχιτεκτονική του ESET PROTECT On-Prem
- Διαδικασία εγκατάστασης
- Διαδικασίες αναβάθμισης
- Διαδικασίες μετεγκατάστασης
- Διαδικασίες κατάργησης εγκατάστασης
- Διαχείριση αδειών χρήσης
- Διαδικασίες ανάπτυξης και Ανάπτυξη φορέα χρησιμοποιώντας GPO ή SCCM
- Πρώτα βήματα μετά την εγκατάσταση του ESET PROTECT On-Prem
- Οδηγός διαχείρισης

Νέες δυνατότητες στο ESET PROTECT On-Prem 11.0

ESET LiveGuard Advanced αναφορά συμπεριφοράς αρχείων

Στο πλαίσιο της προετοιμασίας για την παροχή νέων, πιο αξιόπιστων αναφορών συμπεριφοράς για τους πελάτες EDR, η εταιρεία πρόσθεσε την επιλογή λήψης αναφορών συμπεριφοράς που δημιουργούνται από το ESET LiveGuard Advanced. Μάθετε περισσότερα

Μια νέα εργασία υπολογιστή-πελάτη που ελέγχει για ενημερωμένες εκδόσεις προϊόντων

Αυτή η εργασία υπολογιστή-πελάτη ελέγχει τη διαθεσιμότητα μιας νέας έκδοσης προϊόντος. Εάν βρεθεί, θα εκτελεστεί λήψη του και θα ξεκινήσει η διαδικασία εγκατάστασης. Μάθετε περισσότερα

Κανόνες ώρας για δυναμικές ομάδες

Παρουσιάζεται η επιλογή συμπερίληψης των κανόνων ώρας ως πρόσθετων κριτηρίων για πρότυπα δυναμικής ομάδας. Όταν ρυθμίζονται οι παράμετροι των κανόνων ώρας, οι υπολογιστές θα τοποθετούνται σε δυναμικές ομάδες μόνο κατά τη διάρκεια της καθορισμένης χρονικής περιόδου. Μάθετε περισσότερα

Μετονομασία προϊόντων

Το όνομα προϊόντος άλλαξε από ESET PROTECT σε ESET PROTECT On-Prem, ενώ σε αυτήν την έκδοση περιλαμβάνονται επίσης ορισμένες πρόσθετες αλλαγές που σχετίζονται με το όνομα του προϊόντος.

Άλλες βελτιώσεις και διορθώσεις σφαλμάτων

Μάθετε ποια άλλα στοιχεία έχουν βελτιωθεί στο αρχείο καταγραφής αλλαγών.

Αρχιτεκτονική

Το ESET PROTECT On-Prem είναι μια νέα γενιά ενός συστήματος απομακρυσμένης διαχείρισης.

Για να εκτελέσετε πλήρη ανάπτυξη των προϊόντων ασφαλείας της ESET, εγκαταστήστε τα ακόλουθα στοιχεία (πλατφόρμες Windows και Linux):

- ESET PROTECTΔιακομιστής
- Κονσόλα διαδικτύου ESET PROTECT
- Φορέας ESET Management

Τα ακόλουθα στοιχεία υποστήριξης είναι προαιρετικά, αλλά συνιστάται να τα εγκαταστήσετε για να διασφαλίσετε καλύτερες επιδόσεις της εφαρμογής στο δίκτυο:

- Αισθητήρας RD
- ESET Bridge Διακομιστής Μεσολάβησης HTTP
- Mobile Device Connector

Τα στοιχεία του ESET PROTECT χρησιμοποιούν πιστοποιητικά για να επικοινωνούν με το διακομιστή ESET PROTECT. Διαβάστε περισσότερα σχετικά με τα πιστοποιητικά στο ESET PROTECT On-Prem στο άρθρο της Γνωσιακής βάσης.

Επισκόπηση στοιχείων υποδομής

Ο παρακάτω πίνακας περιέχει μια επισκόπηση των στοιχείων υποδομής του ESET PROTECT και τις κύριες λειτουργίες τους:

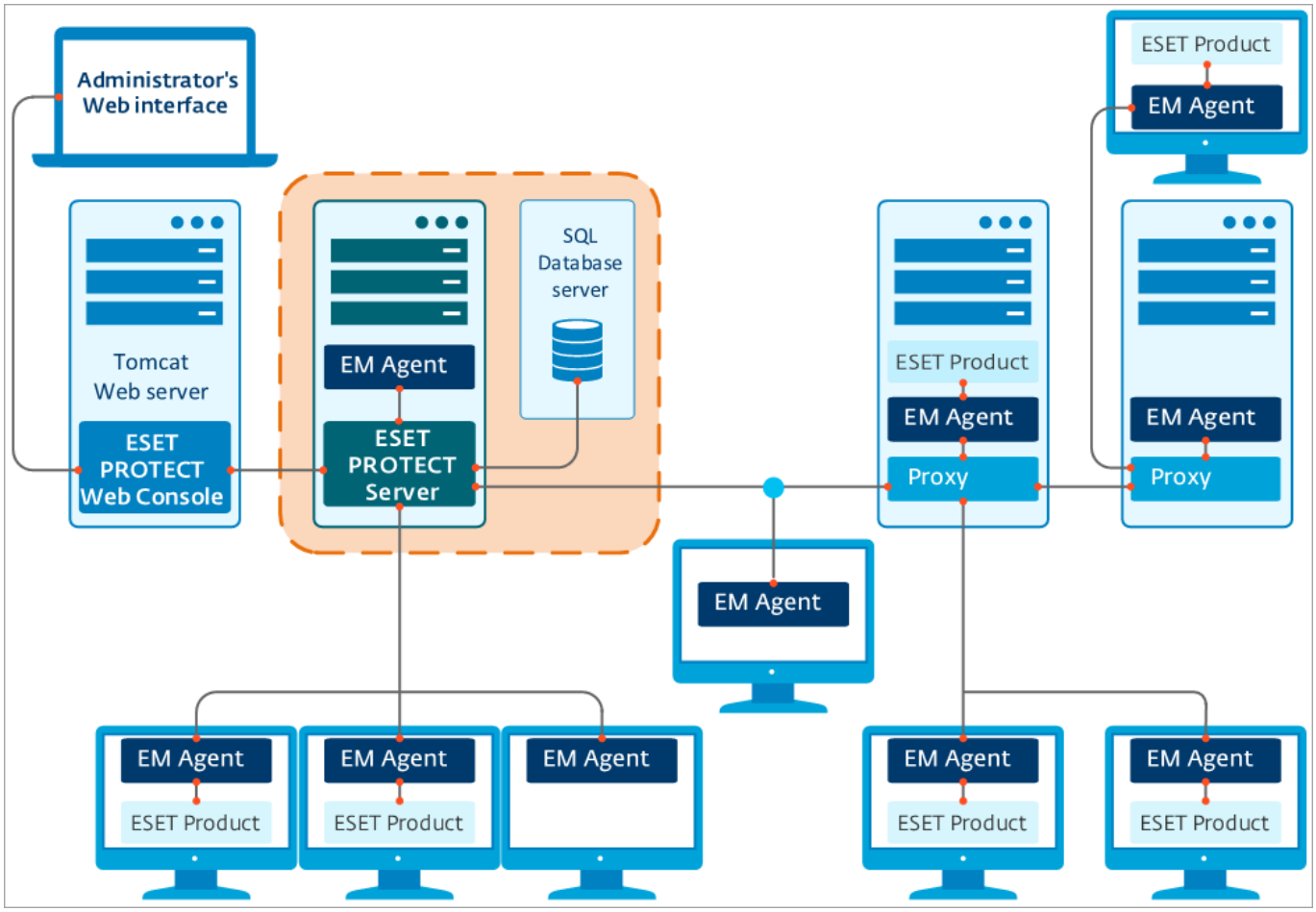
Λειτουργικότητα	ESET PROTECTΔιακομιστής	Φορέας ESET Management	Προϊόν ασφάλειας ESET	ESET Bridge Διακομιστής Μεσολάβησης HTTP	Διακομιστές ESET	Σύνδεση κινητών συσκευών
Απομακρυσμένη διαχείριση των προϊόντων ασφάλειας ESET (δημιουργία πολιτικών, εργασίες, αναφορές, κ.λπ.)	✔	x	x	x	x	x
Επικοινωνία με το διακομιστή ESET PROTECT και διαχείριση του προϊόντος ασφάλειας ESET στη συσκευή-πελάτη	x	✔	x	x	x	✔
Παροχή ενημερώσεων, επαλήθευση αδειών χρήσης	x	x	x	*	✔	x
Προσωρινή αποθήκευση και προώθηση ενημερώσεων (μηχανισμός ανίχνευσης, προγράμματα εγκατάστασης, λειτουργικές μονάδες)	x	x	**	✔	x	x
Προώθηση δικτυακής κίνησης μεταξύ του φορέα ESET Management και του διακομιστή ESET PROTECT	x	x	x	✔	x	x
Ασφάλιση της συσκευής-πελάτη	x	x	✔	x	x	x
Απομακρυσμένη διαχείριση κινητών συσκευών	x	x	x	x	x	✔

* Μόνο με αποθετήριο εκτός σύνδεσης.

** Τα προϊόντα ασφάλειας ESET δεν αποθηκεύουν προσωρινά τα προγράμματα εγκατάστασης.

Διακομιστής

Ο διακομιστής ESET PROTECT είναι η εκτελεστική εφαρμογή, η οποία επεξεργάζεται όλα τα δεδομένα που λαμβάνονται από τους υπολογιστές-πελάτες που συνδέονται με το διακομιστή (μέσω του φορέα ESET Management ή του διακομιστή μεσολάβησης HTTP). Για τη σωστή επεξεργασία των δεδομένων, ο διακομιστής απαιτεί σταθερή σύνδεση με ένα διακομιστή βάσης δεδομένων, όπου αποθηκεύονται τα δεδομένα δικτύου. Συνιστάται να εγκαταστήσετε το διακομιστή βάσης δεδομένων σε διαφορετικό υπολογιστή για να επιτύχετε καλύτερες επιδόσεις.

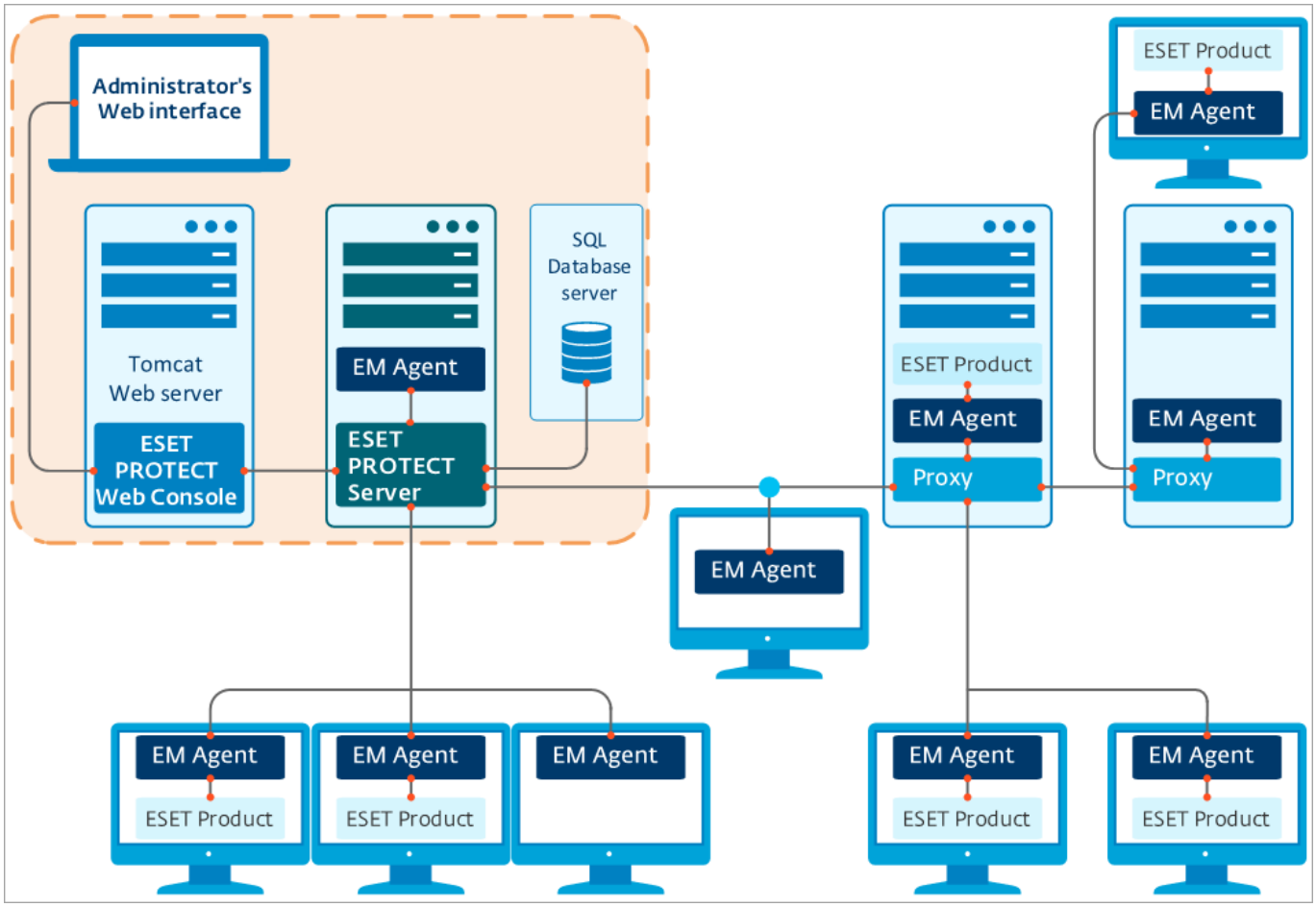


Κονσόλα διαδικτύου

Η Κονσόλα διαδικτύου ESET PROTECT είναι ένα περιβάλλον χρήστη που βασίζεται στο διαδίκτυο και σας επιτρέπει να διαχειρίζεστε τις λύσεις ασφάλειας της ESET στο περιβάλλον σας. Εμφανίζει μια επισκόπηση της κατάστασης των υπολογιστών-πελατών στο δίκτυό σας και μπορεί να χρησιμοποιηθεί για την ανάπτυξη λύσεων της ESET σε απομακρυσμένους υπολογιστές. Η πρόσβαση στην κονσόλα διαδικτύου πραγματοποιείται με χρήση του προγράμματος περιήγησης (δείτε τα υποστηριζόμενα προγράμματα περιήγησης). Εάν επιλέξετε να επιτρέψετε την πρόσβαση του διακομιστή διαδικτύου από το Internet, μπορείτε να χρησιμοποιήσετε το ESET PROTECT On-Prem σχεδόν από οποιοδήποτε μέρος και συσκευή.

Η Κονσόλα διαδικτύου χρησιμοποιεί Apache Tomcat ως διακομιστή διαδικτύου HTTP. Εάν χρησιμοποιείτε το Tomcat συνδυαστικά στο πρόγραμμα εγκατάστασης ESET ή στην Εικονική συσκευή, επιτρέπει μόνο συνδέσεις TLS 1.2 και 1.3 στην Κονσόλα διαδικτύου.

> Μπορείτε να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT σε έναν διαφορετικό υπολογιστή από τον υπολογιστή στον οποίο εκτελείται ο διακομιστής ESET PROTECT.



ESET Bridge Διακομιστής Μεσολάβησης HTTP

Μπορείτε να χρησιμοποιήσετε το ESET Bridge με το ESET PROTECT On-Prem ως υπηρεσία διακομιστή μεσολάβησης για να κάνετε τα εξής:

- Λήψη και προσωρινή μνήμη: Ενημερώσεις μονάδων ESET, πακέτα εγκατάστασης και ενημέρωσης που προωθούνται από το ESET PROTECT On-Prem (π.χ., πρόγραμμα εγκατάστασης MSI του ESET Endpoint Security), ενημερώσεις προϊόντων ασφάλειας ESET (ενημερώσεις στοιχείων και προϊόντων), αποτελέσματα του ESET LiveGuard.

- Προώθηση επικοινωνίας από τους φορείς ESET Management στο ESET PROTECT On-Prem.

Για περισσότερες λεπτομέρειες σχετικά με την εγκατάσταση και τη ρύθμιση παραμέτρων του ESET Bridge, διαβάστε την Ηλεκτρονική βοήθεια για το ESET Bridge.

Apache HTTP Proxy χρήστες
Από το ESET PROTECT On-Prem 10.0, το ESET Bridge αντικαθιστά το Apache HTTP Proxy. Το Apache HTTP Proxy έχει φθάσει σε στάδιο περιορισμένης υποστήριξης. Εάν χρησιμοποιείτε το Apache HTTP Proxy, συνιστάται η μετεγκατάσταση σε ESET Bridge.

Φορέας

Ο φορέας ESET Management είναι ένα απαραίτητο μέρος του ESET PROTECT On-Prem. Οι υπολογιστές-πελάτες δεν επικοινωνούν απευθείας με το διακομιστή του ESET PROTECT, αλλά ο φορέας είναι το

στοιχείο που διευκολύνει αυτή την επικοινωνία. Ο φορέας συλλέγει πληροφορίες από τον υπολογιστή-πελάτη και τις αποστέλλει στο διακομιστή ESET PROTECT. Εάν ο διακομιστής ESET PROTECT στείλει μια εργασία για τον υπολογιστή-πελάτη, αυτή αποστέλλεται στο φορέα, ο οποίος την στέλνει στη συνέχεια στον υπολογιστή-πελάτη. Ο φορέας ESET Management χρησιμοποιεί ένα νέο βελτιωμένο πρωτόκολλο επικοινωνίας.

Για να απλοποιηθεί η υλοποίηση της προστασίας τελικού σημείου, ο ανεξάρτητος φορέας ESET Management περιλαμβάνεται στη σουίτα ESET PROTECT On-Prem. Είναι μια απλή, έντονα αρθρωτή και ελαφριά υπηρεσία που καλύπτει όλη την επικοινωνία μεταξύ του διακομιστή ESET PROTECT και οποιουδήποτε προϊόντος της ESET ή λειτουργικό σύστημα. Αντί να επικοινωνούν απευθείας με το διακομιστή ESET PROTECT, τα προϊόντα ESET επικοινωνούν μέσω του φορέα. Οι υπολογιστές-πελάτες, στους οποίους έχει εγκατασταθεί φορέας ESET Management και μπορούν να επικοινωνούν με το διακομιστή ESET PROTECT, αναφέρονται ως «διαχειριζόμενοι». Μπορείτε να εγκαταστήσετε το φορέα σε οποιονδήποτε υπολογιστή, ανεξάρτητα εάν έχει εγκατασταθεί άλλο λογισμικό της ESET.

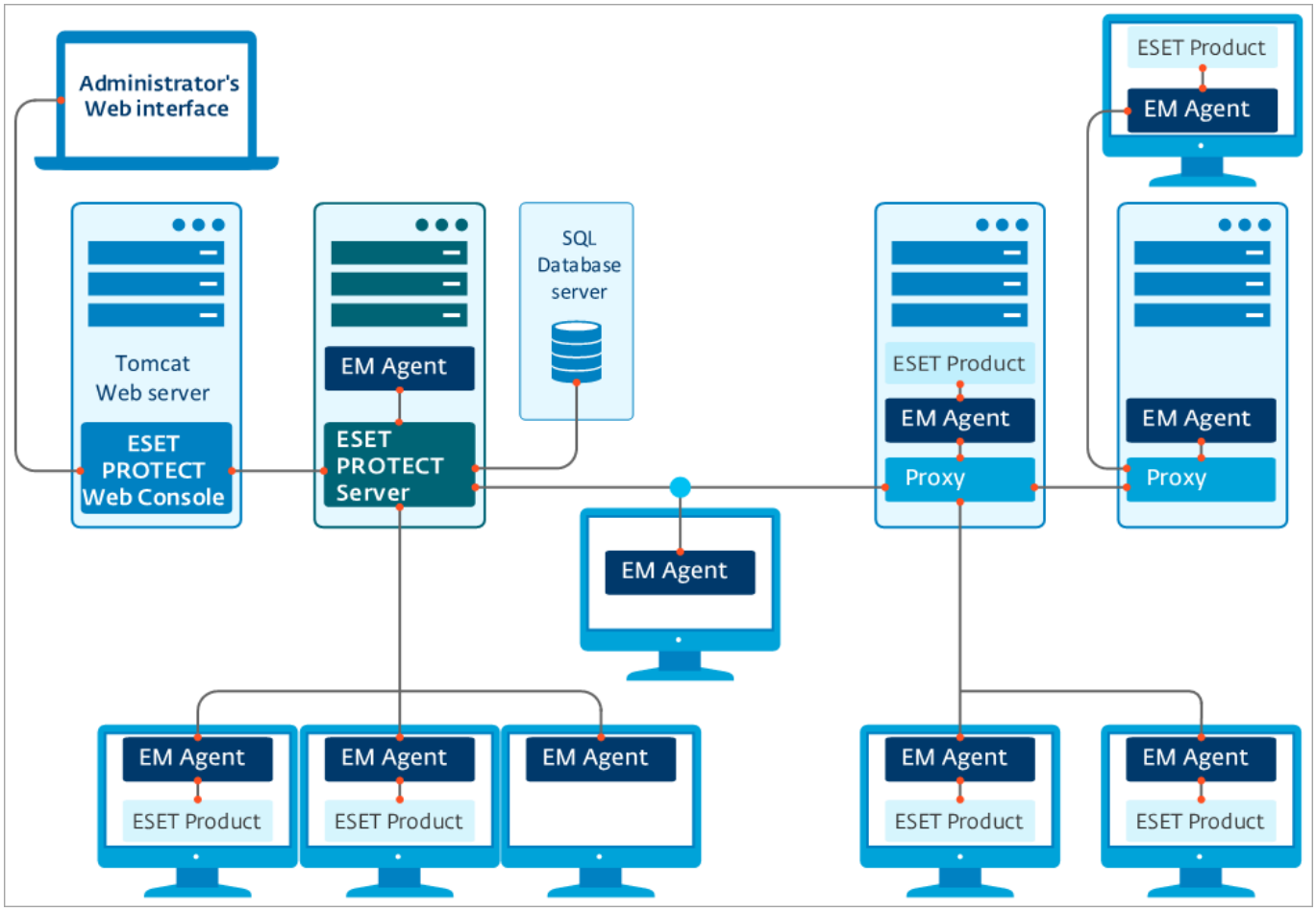
Τα οφέλη περιλαμβάνουν τα εξής:

- Εύκολη ρύθμιση – μπορείτε να αναπτύξετε τον Φορέα ως μέρος της τυπικής εταιρικής εγκατάστασης.

- Επιτόπου διαχείριση ασφάλειας – επειδή η ρύθμιση παραμέτρων του φορέα μπορεί να περιλαμβάνει την αποθήκευση πολλών σεναρίων ασφάλειας, μειώνεται σημαντικά ο χρόνος αντίδρασης μέχρι την ανίχνευση.

- Διαχείριση ασφάλειας εκτός σύνδεσης – ο φορέας μπορεί να αποκριθεί σε ένα συμβάν, ακόμα και εάν δεν είναι συνδεδεμένος με το διακομιστή ESET PROTECT.

Το πρωτόκολλο επικοινωνίας μεταξύ του φορέα και του διακομιστή ESET PROTECT δεν υποστηρίζει τον έλεγχο ταυτότητας. Οποιαδήποτε λύση διακομιστή μεσολάβησης που χρησιμοποιείται για προώθηση της επικοινωνίας του φορέα στο διακομιστή ESET PROTECT και απαιτεί έλεγχο ταυτότητας δεν θα λειτουργεί.
Εάν επιλέξετε να χρησιμοποιήσετε μια μη προεπιλεγμένη θύρα για την Κονσόλα διαδικτύου ή το φορέα, ενδέχεται να απαιτείται προσαρμογή του τείχους προστασίας. Διαφορετικά, η εγκατάσταση μπορεί να αποτύχει.



Ανιχνευτής Διασκορπισμένων Μηχανών

Ο αισθητήρας **Rogue Detection Sensor (Αισθητήρας RD)** είναι ένα εργαλείο εντοπισμού συστήματος rogue, το οποίο πραγματοποιεί αναζήτηση στο δίκτυό σας για υπολογιστές. Ο αισθητήρας είναι εύχρηστος επειδή μπορεί να εντοπίζει νέους υπολογιστές από το ESET PROTECT On-Prem χωρίς να απαιτείται χειροκίνητη αναζήτηση και προσθήκη τους. Οι υπολογιστές που εντοπίζονται τοποθετούνται και αναφέρονται αμέσως σε μια προκαθορισμένη αναφορά, η οποία σας επιτρέπει να τους μετακινήσετε σε συγκεκριμένες στατικές ομάδες και να προχωρήσετε σε εργασίες διαχείρισης.

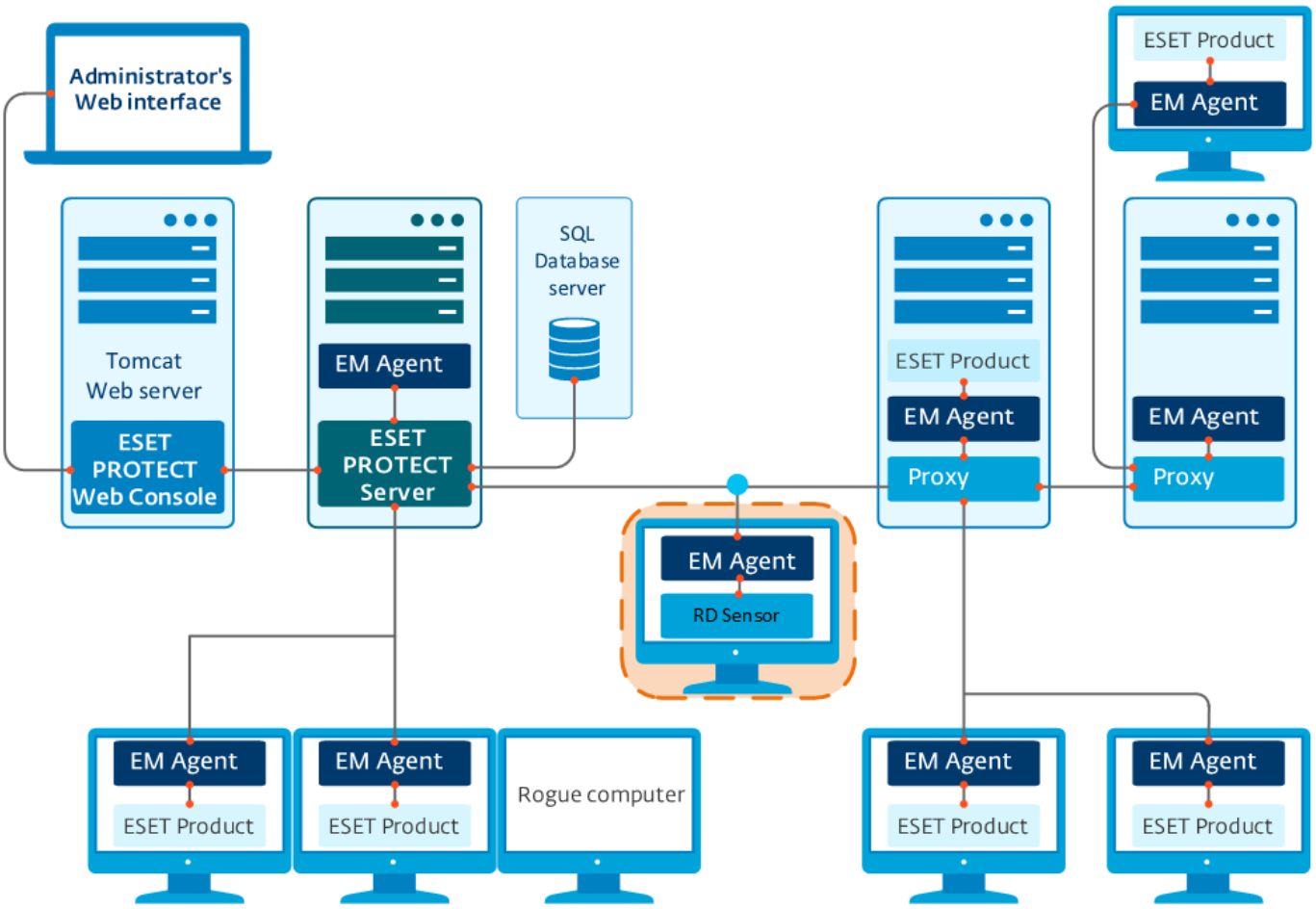
Ο αισθητήρας RD παρακολουθεί ενεργά τις εκπομπές ARP. Όταν ο αισθητήρας RD ανιχνεύει ένα νέο ενεργό στοιχείο δικτύου, ο αισθητήρας RD στέλνει μοναδικές διανομές ARP, εκτελεί τη λήψη δακτυλικών αποτυπωμάτων κεντρικού υπολογιστή (χρησιμοποιώντας διάφορες θύρες) και στέλνει πληροφορίες σχετικά με τους ανιχνευμένους υπολογιστές στον διακομιστή ESET PROTECT. Στη συνέχεια, ο διακομιστής ESET PROTECT αξιολογεί εάν οι υπολογιστές που βρέθηκαν στο δίκτυο είναι άγνωστοι στο διακομιστή ESET PROTECT ή είναι ήδη διαχειριζόμενοι.

Δεν μπορείτε να απενεργοποιήσετε τη λήψη δακτυλικών αποτυπωμάτων κεντρικού υπολογιστή, επειδή αυτή είναι η κύρια λειτουργικότητα του αισθητήρα RD.

> Εάν υπάρχουν πολλά τμήματα δικτύου, ο αισθητήρας Rogue Detection Sensor πρέπει να εγκατασταθεί ξεχωριστά σε κάθε τμήμα δικτύου για να δημιουργήσει μια ολοκληρωμένη λίστα όλων των συσκευών σε ολόκληρο το δίκτυο.

Κάθε υπολογιστής εντός της δομής του δικτύου (τομέας, LDAP, δίκτυο Windows) προστίθεται αυτόματα στη λίστα υπολογιστών του διακομιστή ESET PROTECT μέσω μιας εργασίας συγχρονισμού

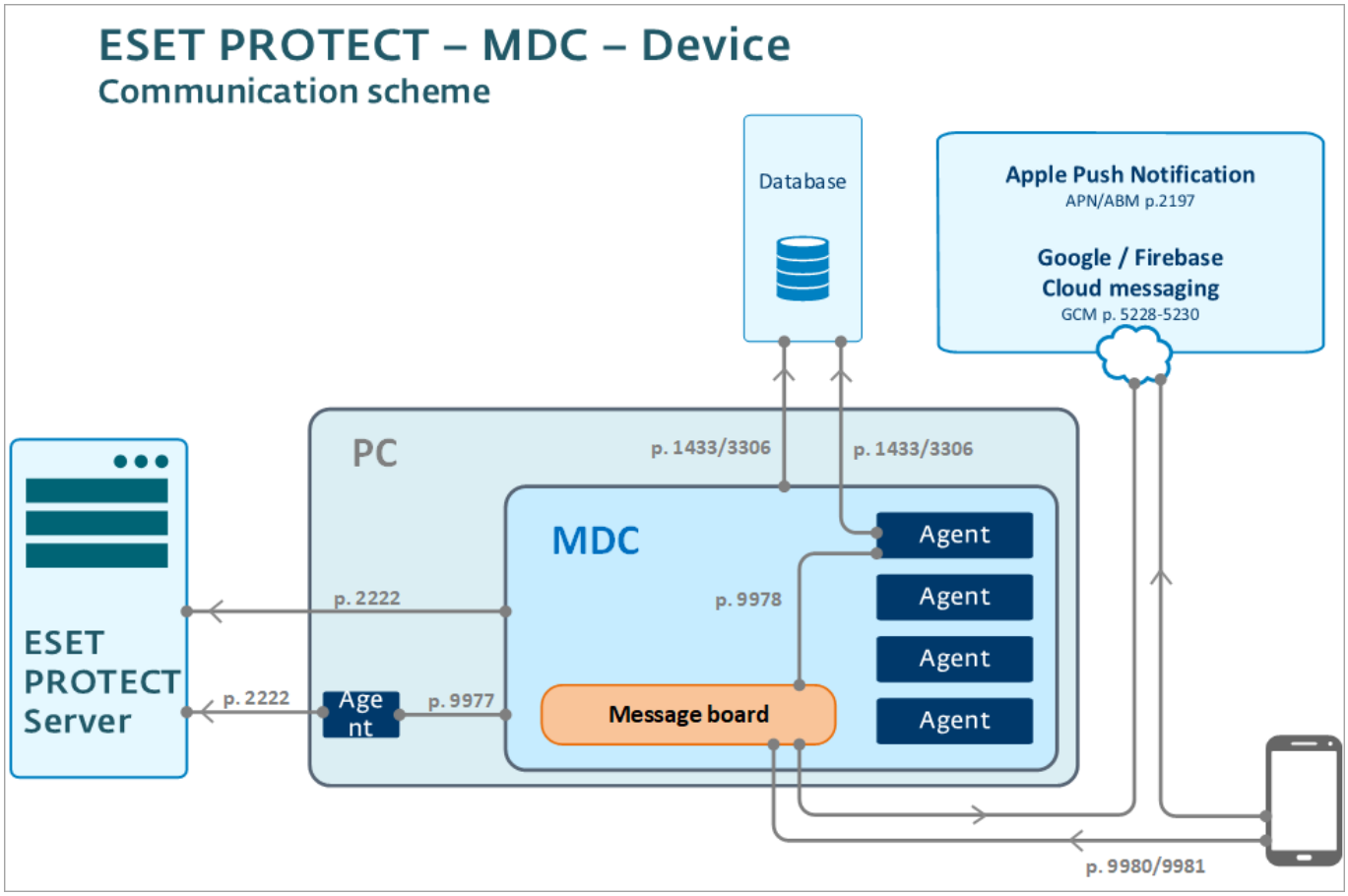
διακομιστή. Η χρήση του αισθητήρα RD είναι ένας εύχρηστος τρόπος για τον εντοπισμό υπολογιστών που δεν βρίσκονται στον τομέα ή σε άλλη δομή του δικτύου και την προσθήκη τους στο διακομιστή ESET PROTECT. Ο αισθητήρας RD απομνημονεύει τους υπολογιστές που εντοπίζονται και δεν αποστέλλει τις ίδιες πληροφορίες δύο φορές.



Σύνδεση κινητών συσκευών

Η σύνδεση κινητών συσκευών ESET PROTECT είναι ένα στοιχείο που επιτρέπει τη διαχείριση κινητών συσκευών (Android και iOS) με το ESET PROTECT On-Prem, καθώς και τη διαχείριση του ESET Endpoint Security για Android.

Το στοιχείο Διαχείριση/Σύνδεση κινητών συσκευών (Διαχείριση κινητών συσκευών/MDC) του ESET PROTECT (μόνο εσωτερικής εγκατάστασης) φτάνει στο τέλος του κύκλου ζωής τον Ιανουάριο του 2024. Διαβάστε περισσότερα. Συνιστάται η μετεγκατάσταση στο cloud διαχείρισης κινητών συσκευών.



Δείτε την εικόνα σε μεγαλύτερη

Συνιστάται να αναπτύξετε το στοιχείο MDM σε μια κεντρική συσκευή διαφορετική από τη συσκευή στην οποία φιλοξενείται ο διακομιστής ESET PROTECT.

Οι συνιστώμενες προϋποθέσεις υλικού για περίπου 80 διαχειριζόμενες κινητές συσκευές είναι:

Υλικό	Συνιστώμενη διαμόρφωση
Επεξεργαστής	4 πυρήνες, 2,5 GHz
ΜΝΉΜΗ RAM:	4 GB (συνιστάται)
HDD	100 GB

Για περισσότερες από 80 διαχειριζόμενες κινητές συσκευές, οι απαιτήσεις υλικού δεν είναι πολύ μεγαλύτερες. Ο λανθάνων χρόνος μεταξύ της αποστολής της εργασίας από το ESET PROTECT On-Prem και της εκτέλεσης της εργασίας στην κινητή συσκευή θα αυξηθεί αναλογικά με τον αριθμό των συσκευών στο περιβάλλον σας.

Ακολουθήστε τις οδηγίες εγκατάστασης του MDM για Windows (Πρόγραμμα εγκατάστασης «όλα σε ένα) ή Εγκατάσταση στοιχείων) ή Linux.

Διαφορές μεταξύ του διακομιστή μεσολάβησης HTTP ESET Bridge, του εργαλείου ειδώλου και της απευθείας συνδεσιμότητας

Η επικοινωνία του προϊόντος ESET περιλαμβάνει ενημερώσεις του μηχανισμού ανίχνευσης και των μονάδων του προγράμματος, καθώς και την ανταλλαγή δεδομένων ESET LiveGrid® (δείτε τον πίνακα

παρακάτω) και πληροφορίες άδειας χρήσης.

Το ESET PROTECT On-Prem πραγματοποιεί λήψη των πιο πρόσφατων προϊόντων για διανομή σε υπολογιστές-πελάτες από το χώρο αποθήκευσης. Μόλις ολοκληρωθεί η διανομή, το προϊόν είναι έτοιμο για ανάπτυξη στον υπολογιστή-στόχο.

Μόλις εγκατασταθεί ένα προϊόν ασφαλείας της ESET, πρέπει να ενεργοποιηθεί, δηλαδή το προϊόν πρέπει να επαληθεύσει τις πληροφορίες άδειας χρήσης στο διακομιστή αδειών χρήσης. Μετά την ενεργοποίηση, ο μηχανισμός ανίχνευσης και οι μονάδες του προγράμματος ενημερώνονται σε τακτική βάση.

Το Σύστημα πρώιμης προειδοποίησης ESET LiveGrid® βοηθά να διασφαλίζεται ότι η ESET ενημερώνεται άμεσα και διαρκώς σχετικά με νέες εισβολές, ώστε να προστατεύει γρήγορα τους πελάτες της. Το σύστημα επιτρέπει την υποβολή νέων ανιχνεύσεων στο Εργαστήριο της ESET, όπου αναλύονται και υποβάλλονται σε επεξεργασία.

Το μεγαλύτερο μέρος της κυκλοφορίας δικτύου δημιουργείται από τις ενημερώσεις μονάδων του προϊόντος. Γενικά, ένα προϊόν ασφαλείας ESET πραγματοποιεί λήψη περίπου 23,9 MB ενημερώσεων των μονάδων σε έναν μήνα.

Τα δεδομένα του ESET LiveGrid® (περίπου 22,3 MB) και το αρχείο έκδοσης ενημέρωσης (έως 11 kB) είναι τα μόνα διανεμόμενα αρχεία τα οποία δεν είναι δυνατό να αποθηκευτούν στην προσωρινή μνήμη.

Υπάρχουν δύο τύποι ενημερώσεων – οι ενημερώσεις επιπέδου και οι ενημερώσεις nano. Ανατρέξτε στο άρθρο της Γνωσιακή βάσης για περισσότερες πληροφορίες σχετικά με τους τύπους ενημερώσεων.

Υπάρχουν 2 τρόποι για να μειώσετε το φορτίο του δικτύου κατά τη διανομή ενημερώσεων σε ένα δίκτυο υπολογιστών: ο ESET Bridge Διακομιστής μεσολάβησης HTTP ή το Εργαλείο ειδώλου (διατίθεται μόνο για Windows και Linux).

> **i** Διαβάστε αυτό το άρθρο της Γνωσιακής βάσης για να ρυθμίσετε την αλυσίδα του Εργαλείου ειδώλου (ρυθμίστε τις παραμέτρους του Εργαλείου ειδώλου ώστε να λαμβάνει ενημερώσεις από ένα άλλο Εργαλείο ειδώλου).

Τύποι επικοινωνίας ESET

Τύπος επικοινωνίας	Συχνότητα επικοινωνίας	Επίπτωση στην κυκλοφορία δικτύου	Επικοινωνία προωθούμενη από διακομιστή μεσολάβησης	Επιλογή προσωρινής αποθήκευσης στο διακομιστή μεσολάβησης[1]	Επιλογή ειδώλου[2]	Επιλογή περιβάλλοντος εκτός σύνδεσης
Ανάπτυξη φορέα (Προγράμματα προώθησης/ζωντανής εγκατάστασης από το χώρο αποθήκευσης)	Μία φορά	Κατά προσέγγιση 50 MB ανά υπολογιστή-πελάτη	NAI	NAI[3]	OXI	NAI (GPO / SCCM, επεξεργασμένα προγράμματα ζωντανής εγκατάστασης)[4]
Εγκατάσταση τελικού σημείου (εγκατάσταση λογισμικού από το χώρο αποθήκευσης)	Μία φορά	Κατά προσέγγιση 100 MB ανά υπολογιστή-πελάτη	NAI	NAI[3]	OXI	NAI (GPO / SCCM, εγκατάσταση με πακέτο URL)[4]
Μονάδα μηχανισμού ανίχνευσης / Ενημέρωση μονάδας προγράμματος	6+ φορές την ημέρα	23,9 MB ανά μήνα[5]	NAI	NAI	NAI	NAI (Χωρίς σύνδεση Mirror Tool και Προσαρμοσμένο διακομιστή HTTP)[6]
Αρχείο έκδοσης ενημέρωσης update.ver	~8 φορές την ημέρα	2,6 MB ανά μήνα[7]	NAI	OXI	-	-
Ενεργοποίηση/¨Ελεγχος άδειας χρήσης	4 φορές την ημέρα	αμελητέα	NAI	OXI	OXI	NAI (Αρχεία χωρίς σύνδεση που δημιουργούνται από το ESET Business Account)[8]
ESET LiveGrid® Φήμη βασισμένη στο cloud	Επιτόπου	11 MB ανά μήνα	NAI	OXI	OXI	OXI

1.Για τις επιπτώσεις και τα πλεονεκτήματα της προσωρινής αποθήκευσης μέσω διακομιστή μεσολάβησης, ανατρέξτε στο κεφάλαιο Πότε πρέπει να ξεκινήσω να χρησιμοποιώ το ESET Bridge διακομιστή μεσολάβησης HTTP;

2.Για τις επιπτώσεις από τη χρήση ειδώλου, ανατρέξτε στο κεφάλαιο Πότε πρέπει να ξεκινήσω να χρησιμοποιώ το εργαλείο ειδώλου;

3.Μία φορά ανά εγκατάσταση / αναβάθμιση, συνιστάται να αναπτύσσετε αρχικά έναν φορέα (έναν ανά συγκεκριμένη έκδοση) / τερματικό σημείο, έτσι ώστε να αποθηκεύεται προσωρινά το πρόγραμμα εγκατάστασης.

4.Για να αναπτύξετε το φορέα ESET Management σε ένα μεγάλο δίκτυο, ανατρέξτε στο κεφάλαιο Ανάπτυξη φορέα χρησιμοποιώντας GPO και SCCM.

5.Η αρχική ενημέρωση του μηχανισμού ανίχνευσης μπορεί να είναι μεγαλύτερη από το κανονικό, ανάλογα με την ηλικία του πακέτου εγκατάστασης, επειδή θα γίνει λήψη όλων των νεότερων ενημερώσεων του μηχανισμού ανίχνευσης και των μονάδων. Συνιστούμε να πραγματοποιήσετε την εγκατάσταση σε έναν υπολογιστή-πελάτη αρχικά, και να αφήσετε να πραγματοποιηθεί ενημέρωση, έτσι ώστε να αποθηκευτούν προσωρινά οι απαιτούμενες ενημερώσεις του μηχανισμού ανίχνευσης και των μονάδων του προγράμματος.

6.Χωρίς σύνδεση Internet, το Mirror Tool δεν μπορεί να πραγματοποιήσει λήψη ενημερώσεων του μηχανισμού ανίχνευσης. Μπορείτε να χρησιμοποιήσετε το Apache Tomcat ως διακομιστή HTTP για να λαμβάνετε ενημερώσεις σε έναν κατάλογο διαθέσιμο στο Εργαλείο ειδώλου (διατίθεται μόνο για Windows και Linux).

7.Κατά τον έλεγχο για ενημερώσεις του μηχανισμού ανίχνευσης, γίνεται πάντα λήψη και ανάλυση του αρχείου *update.ver*. Από προεπιλογή, το χρονοδιάγραμμα του προϊόντος ESET Endpoint υποβάλλει ερώτημα για νέα ενημέρωση κάθε μία ώρα. Υποθέτουμε ότι ένας υπολογιστής-πελάτης είναι ενεργοποιημένος 8 ώρες την ημέρα. Το αρχείο *update.ver* περιέχει περίπου 11 kB.

8.Λήψη αρχείων άδειας χρήσης εκτός σύνδεσης από το ESET Business Account.

Δεν μπορείτε να αποθηκεύσετε στην προσωρινή μνήμη ενημερώσεις για προϊόντα των εκδόσεων 4 και 5 χρησιμοποιώντας διακομιστή μεσολάβησης HTTP ESET Bridge. Για να διανείμετε ενημερώσεις για αυτά τα προϊόντα, χρησιμοποιήστε το Εργαλείο ειδώλου.

Πότε πρέπει να ξεκινήσω να χρησιμοποιώ το ESET Bridge (Διακομιστή μεσολάβησης HTTP)

Με βάση τις δοκιμές μας, συνιστούμε να αναπτύσσετε το ESET Bridge διακομιστή μεσολάβησης HTTP εάν έχετε δίκτυο με 37 ή περισσότερους υπολογιστές.

Είναι πολύ σημαντικό για την αποτελεσματική προσωρινή αποθήκευση να έχει οριστεί σωστά η ημερομηνία και η ώρα στο διακομιστή μεσολάβησης HTTP. Οι διαφορές αρκετών λεπτών θα προκαλούσαν τη μη αποτελεσματική λειτουργία του μηχανισμού προσωρινής αποθήκευσης και τη λήψη περισσότερων αρχείων από τα απαιτούμενα.

Η ανάλυση του εύρους ζώνης δικτύου που χρησιμοποιείται αποκλειστικά από ενημερώσεις σε ένα δοκιμαστικό δίκτυο 1.000 υπολογιστών, όπου σημειώθηκαν αρκετές εγκαταστάσεις και απεγκαταστάσεις, έδειξε τα εξής:

- ένας μόνο υπολογιστής πραγματοποιεί λήψεις ενημερώσεων 23,9 MB κατά μέσο όρο το μήνα,

εάν συνδέεται απευθείας στο Internet (χωρίς να χρησιμοποιείται διακομιστής μεσολάβησης HTTP).

- Με τη χρήση διακομιστή μεσολάβησης HTTP, οι λήψεις για ολόκληρο το δίκτυο δεν ξεπερνούν συνολικά τα 900 MB το μήνα.

Ακολουθεί μια απλή σύγκριση στα ληφθέντα δεδομένα ενημερώσεων σε ένα μήνα, με χρήση απευθείας σύνδεσης στο Internet ή με τη χρήση διακομιστή μεσολάβησης HTTP σε ένα δίκτυο υπολογιστών:

Αριθμός υπολογιστών στο εταιρικό σας δίκτυο	25	36	50	100	500	1.000
Απευθείας σύνδεση στο Internet (MB/μήνα)	375	900	1.250	2.500	12.500	25.000
ESET Bridge Διακομιστής μεσολάβησης HTTP Apache (MB/μήνα)	30	50	60	150	600	900

Πότε πρέπει να ξεκινήσω να χρησιμοποιώ το Mirror Tool

Εάν έχετε περιβάλλον εκτός σύνδεσης, δηλαδή οι υπολογιστές στο δίκτυό σας δεν συνδέονται στο Internet για μεγάλο χρονικό διάστημα (μήνες ή έτος), το Εργαλείο ειδώλου (διατίθεται για Windows και Linux) είναι ο μόνος τρόπος να διανέμετε ενημερώσεις μονάδων προϊόντος, επειδή λαμβάνει όλες τις διαθέσιμες ενημερώσεις επιπέδου και Nano με κάθε νέο αίτημα ενημέρωσης, εάν υπάρχει νέα διαθέσιμη ενημέρωση.

> Διαβάστε αυτό το άρθρο της Γνωσιακής βάσης για να ρυθμίσετε την αλυσίδα του Εργαλείου ειδώλου (ρυθμίστε τις παραμέτρους του Εργαλείου ειδώλου ώστε να λαμβάνει ενημερώσεις από ένα άλλο Εργαλείο ειδώλου).

Η μεγαλύτερη διαφορά ανάμεσα στο διακομιστή μεσολάβησης HTTP ESET Bridge και στο Εργαλείο ειδώλου είναι ότι ο διακομιστής μεσολάβησης HTTP ESET Bridge πραγματοποιεί λήψη μόνο των ενημερώσεων που λείπουν (για παράδειγμα, ενημέρωση Nano 3), ενώ το Mirror Tool πραγματοποιεί λήψη όλων των διαθέσιμων ενημερώσεων επιπέδου και Nano (ή μόνο ενημερώσεων επιπέδου, εάν καθορίζεται), ανεξάρτητα από την ενημέρωση που λείπει από μια συγκεκριμένη λειτουργική μονάδα του προϊόντος.

> Οι ενημερώσεις ροής δεν είναι διαθέσιμες με το Εργαλείο ειδώλου. Συνιστάται να προτιμάτε ενημέρωση μέσω του διακομιστή μεσολάβησης HTTP ESET Bridge για ενημέρωση από είδωλο, όπου είναι δυνατόν. Ακόμα και αν ένας υπολογιστής είναι εκτός σύνδεσης, αλλά έχει πρόσβαση σε έναν άλλο υπολογιστή που είναι συνδεδεμένος στο Internet και μπορεί να εκτελέσει το ESET Bridge διακομιστή μεσολάβησης HTTP για να αποθηκεύσει προσωρινά αρχεία ενημέρωσης, επιλέξτε αυτό τον τρόπο.

Στο ίδιο δίκτυο 1.000 υπολογιστών εξετάσαμε το εργαλείο ειδώλου αντί του ESET Bridge διακομιστή μεσολάβησης HTTP. Η ανάλυση έδειξε ότι κατεβάσατε 5.500 MB ενημερώσεων μέσα σε έναν μήνα. Το μέγεθος των ενημερώσεων που λήφθηκαν δεν αυξήθηκε με την προσθήκη περισσότερων υπολογιστών στο δίκτυο. Αυτό εξακολουθεί να αποτελεί αξιοσημείωτη μείωση στο φόρτο δικτύου, σε σύγκριση με μια διαμόρφωση στην οποία οι υπολογιστές-πελάτες συνδέονται απευθείας στο Internet, αλλά η βελτίωση στις επιδόσεις δεν είναι τόσο σημαντική όσο αυτή που επιτυγχάνεται με τη χρήση

διακομιστή μεσολάβησης HTTP.

Αριθμός υπολογιστών στο εταιρικό σας δίκτυο	25	36	50	100	500	1.000
Απευθείας σύνδεση στο Internet (MB/μήνα)	375	900	1.250	2.500	12.500	25.000
Εργαλείο ειδώλου (MB/μήνα)	5.500	5.500	5.500	5.500	5.500	5.500

Ακόμη κι όταν ένα δίκτυο έχει περισσότερους από 1.000 υπολογιστές, η χρήση εύρους ζώνης που αφορά ενημερώσεις δεν αυξάνεται σημαντικά είτε με τη χρήση ESET Bridge διακομιστή μεσολάβησης HTTP είτε με τη χρήση του εργαλείου ειδώλου.

Απαιτήσεις συστήματος και διαμόρφωση μεγέθους

Το σύστημά σας πρέπει να πληροί ένα σύνολο προαπαιτούμενων υλικού, βάσης δεδομένων, δικτύου και λογισμικού για την εγκατάσταση και τη λειτουργία του ESET PROTECT On-Prem.

Υποστηριζόμενα λειτουργικά συστήματα

Οι ακόλουθες ενότητες περιγράφουν την υποστήριξη στοιχείων του ESET PROTECT για εκδόσεις λειτουργικού συστήματος Windows, Linux, macOS και κινητών συσκευών.

Windows

Ο ακόλουθος πίνακας εμφανίζει τα υποστηριζόμενα λειτουργικά συστήματα Windows για κάθε στοιχείο του ESET PROTECT:

Διαχείριση εκδόσεων και υποστήριξη του Φορέα ESET Management

Ο Φορέας ESET Management ακολουθεί τον αριθμό έκδοσης του ESET PROTECTOn-Prem και την πολιτική τέλους του κύκλου ζωής:

- Οι υποστηριζόμενες εκδόσεις του Φορέα ESET Management είναι 9.x–11.x.
- Κάθε έκδοση του Φορέα ESET Management λαμβάνει έξι μήνες πλήρους υποστήριξης και δύο χρόνια περιορισμένης υποστήριξης. Στη συνέχεια, η έκδοση μεταβαίνει στο τέλος του κύκλου ζωής.

Η πιο πρόσφατη υποστηριζόμενη έκδοση Φορέα ESET Management είναι η έκδοση 11.x. Συνιστάται η χρήση της πιο πρόσφατης έκδοσης Φορέα ESET Management για την πλήρη διαχείριση της πιο πρόσφατης έκδοσης των προϊόντων ασφαλείας ESET και των δυνατοτήτων τους. Εάν χρησιμοποιείτε παλαιότερη έκδοση του Φορέα ESET Management από την έκδοση του Διακομιστή ESET PROTECT, ορισμένες από τις πιο πρόσφατες δυνατότητες διαχείρισης ενδέχεται να μην είναι διαθέσιμες.

Το στοιχείο Διαχείριση/Σύνδεση κινητών συσκευών (Διαχείριση κινητών συσκευών/MDC) του ESET PROTECT (μόνο εσωτερικής εγκατάστασης) φτάνει στο τέλος του κύκλου ζωής τον Ιανουάριο του 2024. Διαβάστε περισσότερα. Συνιστάται η μετεγκατάσταση στο cloud διαχείρισης κινητών συσκευών.

Λειτουργικό σύστημα	Διακομιστής	Φορέας	Αισθητήρας RD	MDM

Λειτουργικό σύστημα	Διακομιστής	Φορέας	Αισθητήρας RD	MDM
Windows Server 2012 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2012 CORE x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2012 R2 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2012 R2 CORE x64	✔	9.x—10.x, 11.0	✔	✔
Windows Storage Server 2012 R2 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2016 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Storage Server 2016 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2019 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2022 x64	✔	9.x—10.x, 11.0	✔	✔
Windows Server 2022 CORE x64	✔	11.0		

Λειτουργικό σύστημα	Διακομιστής	Φορέας	Αισθητήρας RD	MDM
Windows 10 x86		9.x—10.x, 11.0	✔	
Windows 10 x64 (όλες οι επίσημες εκδόσεις)	*	9.x—10.x, 11.0	✔	*
Windows 10 σε ARM		9.x—10.x, 11.0		
Windows 11 x64	*	9.x (21H2) 10.x, 11.0 (21H2 και 22H2) 10.1, 11.0 (23H2)	✔	*
Windows 11 σε ARM		10.x, 11.0		

* Η εγκατάσταση στοιχείων του ESET PROTECT σε λειτουργικό σύστημα υπολογιστή-πελάτη ενδέχεται να μην συμφωνεί με την πολιτική αδειοδότησης της Microsoft. Ελέγξτε την πολιτική αδειοδότησης της Microsoft ή συμβουλευτείτε τον προμηθευτή λογισμικού για λεπτομέρειες. Σε περιβάλλοντα SMB/μικρών δικτύων, συνιστάται να εξετάσετε το ενδεχόμενο εγκατάστασης του ESET PROTECT On-Prem σε Linux ή σε εικονική συσκευή, ανάλογα με την περίπτωση.

Δεν υποστηρίζουμε τα παράνομα ή πειρατικά λειτουργικά συστήματα.

Μπορείτε να εκτελείτε το ESET PROTECT On-Prem σε λειτουργικό σύστημα χωρίς διακομιστή, ώστε να μη χρειάζεται ESXi. Υπάρχει η δυνατότητα να εγκαταστήσετε το VMware Player σε ένα λειτουργικό σύστημα επιφάνειας εργασίας και να αναπτύξετε την εικονική συσκευή του ESET PROTECT.

Παλαιότερα συστήματα Microsoft Windows:

- Ο φορέας ESET Management 10.x είναι η τελευταία έκδοση που υποστηρίζει Windows 7/8.x και Windows Server 2008 R2/Microsoft SBS 2011.
- Να εγκαθιστάτε πάντα το πιο πρόσφατο service pack, ιδιαίτερα σε παλαιότερα συστήματα όπως Server 2008 και Windows 7.
- Το ESET PROTECT On-Prem δεν υποστηρίζει τη διαχείριση υπολογιστών που εκτελούν Windows 7 (χωρίς SP), Widows Vista και Windows XP.

Linux

Ο ακόλουθος πίνακας εμφανίζει τα υποστηριζόμενα λειτουργικά συστήματα Linux για κάθε στοιχείο του ESET PROTECT:

Διαχείριση εκδόσεων και υποστήριξη του Φορέα ESET Management

Ο Φορέας ESET Management ακολουθεί τον αριθμό έκδοσης του ESET PROTECTOn-Prem και την πολιτική τέλους του κύκλου ζωής:

- Οι υποστηριζόμενες εκδόσεις του Φορέα ESET Management είναι 9.x–11.x.
- Κάθε έκδοση του Φορέα ESET Management λαμβάνει έξι μήνες πλήρους υποστήριξης και δύο χρόνια περιορισμένης υποστήριξης. Στη συνέχεια, η έκδοση μεταβαίνει στο τέλος του κύκλου ζωής.

Η πιο πρόσφατη υποστηριζόμενη έκδοση Φορέα ESET Management είναι η έκδοση 11.x. Συνιστάται η χρήση της πιο πρόσφατης έκδοσης Φορέα ESET Management για την πλήρη διαχείριση της πιο πρόσφατης έκδοσης των προϊόντων ασφαλείας ESET και των δυνατοτήτων τους. Εάν χρησιμοποιείτε παλαιότερη έκδοση του Φορέα ESET Management από την έκδοση του Διακομιστή ESET PROTECT, ορισμένες από τις πιο πρόσφατες δυνατότητες διαχείρισης ενδέχεται να μην είναι διαθέσιμες.

Το στοιχείο Διαχείριση/Σύνδεση κινητών συσκευών (Διαχείριση κινητών συσκευών/MDC) του ESET PROTECT (μόνο εσωτερικής εγκατάστασης) φτάνει στο τέλος του κύκλου ζωής τον Ιανουάριο του 2024. Διαβάστε περισσότερα. Συνιστάται η μετεγκατάσταση στο cloud διαχείρισης κινητών συσκευών.

Ο Φορέας ESET Management έχει δοκιμαστεί και εκτελείται στις τελευταίες δευτερεύουσες εκδόσεις των αναφερόμενων διανομών Linux.

Λειτουργικό σύστημα	Διακομιστής	Φορέας	Αισθητήρας RD	MDM
Ubuntu 18.04.1 LTS x64 Desktop	✔	9.x—10.x, 11.0	✔	✔
Ubuntu 18.04.1 LTS x64 Server	✔	9.x—10.x, 11.0	✔	✔
Ubuntu 20.04 LTS x64	✔	9.x—10.x, 11.0	✔	✔
Ubuntu 22.04 LTS x64		10.x, 11.0	✔	
Linux Mint 20		10.x, 11.0	✔	
Linux Mint 21		10.1, 11.0	✔	
RHEL Server 7 x64	✔	9.x—10.x, 11.0	✔	✔
RHEL Server 8 x64	✔*	9.x—10.x, 11.0		✔*
RHEL Server 9 x64		9.x—10.x, 11.0	✔	
CentOS 7 x64	✔	9.x—10.x, 11.0	✔	✔
SLED 15 x64		9.x—10.x, 11.0	✔	
SLES 12 x64		9.x—10.x, 11.0	✔	
SLES 15 x64		9.x—10.x, 11.0	✔	
Debian 9 x64		9.x—10.x, 11.0	✔	
Debian 10 x64	✔	9.x—10.x, 11.0	✔	✔
Debian 11 x64		9.x—10.x, 11.0	✔	
Debian 12 x64		10.1, 11.0	✔	
Oracle Linux 8		9.x—10.x, 11.0	✔	

Λειτουργικό σύστημα	Διακομιστής	Φορέας	Αισθητήρας RD	MDM
Amazon Linux 2		9.x—10.x, 11.0	✔	
Alma Linux 9		10.1, 11.0	✔	
Rocky Linux 8		10.1, 11.0		
Rocky Linux 9		10.1, 11.0		

* Το Red Hat Entreprise Linux Server 8.x δεν υποστηρίζει τη δημιουργία αναφορών *.pdf* - δείτε περισσότερες λεπτομέρειες στο θέμα Γνωστά ζητήματα του ESET PROTECT On-Prem.

macOS

Διαχείριση εκδόσεων και υποστήριξη του Φορέα ESET Management

Ο Φορέας ESET Management ακολουθεί τον αριθμό έκδοσης του ESET PROTECTOn-Prem και την πολιτική τέλους του κύκλου ζωής:

- Οι υποστηριζόμενες εκδόσεις του Φορέα ESET Management είναι 9.x–11.x.
- Κάθε έκδοση του Φορέα ESET Management λαμβάνει έξι μήνες πλήρους υποστήριξης και δύο χρόνια περιορισμένης υποστήριξης. Στη συνέχεια, η έκδοση μεταβαίνει στο τέλος του κύκλου ζωής.

Η πιο πρόσφατη υποστηριζόμενη έκδοση Φορέα ESET Management είναι η έκδοση 11.x. Συνιστάται η χρήση της πιο πρόσφατης έκδοσης Φορέα ESET Management για την πλήρη διαχείριση της πιο πρόσφατης έκδοσης των προϊόντων ασφαλείας ESET και των δυνατοτήτων τους. Εάν χρησιμοποιείτε παλαιότερη έκδοση του Φορέα ESET Management από την έκδοση του Διακομιστή ESET PROTECT, ορισμένες από τις πιο πρόσφατες δυνατότητες διαχείρισης ενδέχεται να μην είναι διαθέσιμες.

Λειτουργικό σύστημα	Φορέας
macOS Catalina (10.15)	9.x—10.x, 11.0
macOS Big Sur (11.0)	9.x—10.x, 11.0
macOS Monterey (12.0)	9.x—10.x, 11.0
macOS Ventura (13.0)	9.x—10.x, 11.0
macOS Sonoma (14.0)	10.1, 11.0

Το MacOS υποστηρίζεται μόνο ως πρόγραμμα-πελάτης. Ο Φορέας ESET Management και τα προϊόντα ESET για macOS μπορούν να εγκατασταθούν σε macOS. Ωστόσο, ο Διακομιστής ESET PROTECT δεν είναι δυνατόν να εγκατασταθεί σε macOS.

Κινητό τηλέφωνο

Το στοιχείο Διαχείριση/Σύνδεση κινητών συσκευών (Διαχείριση κινητών συσκευών/MDC) του ESET PROTECT (μόνο εσωτερικής εγκατάστασης) φτάνει στο τέλος του κύκλου ζωής τον Ιανουάριο του 2024. Διαβάστε περισσότερα. Συνιστάται η μετεγκατάσταση στο cloud διαχείρισης κινητών συσκευών.

Λειτουργικό σύστημα	EESA	Κάτοχος συσκευής EESA	MDM iOS	MDM iOS ABM
Android 6	✔			
Android 7	✔	✔		

Λειτουργικό σύστημα	EESA	Κάτοχος συσκευής EESA	MDM iOS	MDM iOS ABM
Android 8	✔	✔		
Android 9	✔	✔		
Android 10	✔	✔		
Android 11	✔	✔		
Android 12	✔	✔		
Android 13	✔	✔		
Android 14	✔	✔		
iOS 9			✔	*
iOS 10			✔	*
iOS 11			✔	*
iOS 12			✔	*
iOS 13			✔	✔
iOS 14			✔	✔
iOS 15			✔	✔
iOS 16			✔	✔
iOS 17			✔	✔
iPadOS 13			✔	✔
iPadOS 14			✔	✔
iPadOS 15			✔	✔
iPadOS 16			✔	✔
iPadOS 17			✔	✔

* Το iOS ABM είναι διαθέσιμο μόνο σε επιλεγμένες χώρες.

Συνιστάται να ενημερώνετε το λειτουργικό σύστημα της κινητής συσκευής σας με την πιο πρόσφατη έκδοση, για να λαμβάνετε σημαντικές ενημερώσεις κώδικα ασφαλείας.

Απαιτήσεις για iOS 10.3 και νεότερες εκδόσεις:

Από την έκδοση του iOS 10.3, ενδέχεται να μην θεωρείται αυτόματα αξιόπιστη μια Αρχή έκδοσης πιστοποιητικού, το οποίο είναι εγκατεστημένο ως μέρος του προφίλ εγγραφής. Για να επιλύσετε αυτό το πρόβλημα, ακολουθήστε τα παρακάτω βήματα:
a)Χρησιμοποιήστε ένα πιστοποιητικό που έχει εκδοθεί από τον εκδότη πιστοποιητικού που θεωρεί αξιόπιστο η Apple.
b)Εγκαταστήστε την αξιοπιστία πιστοποιητικών μη αυτόματα πριν από την εγγραφή. Αυτό σημαίνει ότι θα πρέπει να εγκαταστήσετε μη αυτόματα τη ριζική Αρχή έκδοσης πιστοποιητικού στην κινητή συσκευή πριν την εγγραφή και να ενεργοποιήσετε το στοιχείο ενεργοποίηση πλήρους αξιοπιστίας για το εγκατεστημένο πιστοποιητικό.

Απαιτήσεις για iOS 12:

Αναθεωρήστε τις απαιτήσεις για iOS 10.3 και νεότερες εκδόσεις.

- Η σύνδεση πρέπει να χρησιμοποιεί **TLS 1.2 ή νεότερες εκδόσεις**.
- Η σύνδεση πρέπει να χρησιμοποιεί **AES-128** ή **συμμετρική κρυπτογράφηση AES-256**. Η διαπραγματευόμενη σουίτα κρυπτογράφησης σύνδεσης TLS πρέπει να υποστηρίζει **άριστη και άμεση εμπιστευτικότητα (PFS)** μέσω **Ανταλλαγής κλειδιού Elliptic Curved Diffie-Hellman Ephemeral (ECDHE)** και πρέπει να είναι μία από τις ακόλουθες:

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

- Υπογεγραμμένη με **Κλειδί RSA** με μήκος **τουλάχιστον 2048 bit**. Ο αλγόριθμος κατακερματισμού του πιστοποιητικού πρέπει να είναι **SHA-2 με σύνοψη** (ονομάζεται και «δακτυλικό αποτύπωμα») που έχει μήκος τουλάχιστον 256 bit, (δηλαδή, **SHA-256 ή μεγαλύτερο**). Μπορείτε να δημιουργήσετε ένα πιστοποιητικό με αυτές τις απαιτήσεις στο ESET PROTECT On-Prem αφού ενεργοποιήσετε το στοιχείο Προηγμένη ασφάλεια.
- Τα πιστοποιητικά πρέπει να περιέχουν την **πλήρη αλυσίδα πιστοποιητικού, συμπεριλαμβανομένης της ριζικής αρχής έκδοσης πιστοποιητικού**. Η ριζική αρχή έκδοσης πιστοποιητικού που συμπεριλαμβάνεται στο πιστοποιητικό χρησιμοποιείται για να αποδεικνύεται αξιοπιστία με τις συσκευές και εγκαθίσταται ως μέρος του προφίλ εγγραφής MDM.

Απαιτήσεις για iOS 13:

- Η διαχείριση των κινητών συσκευών iOS 13 απαιτεί την εκπλήρωση των νέων απαιτήσεων πιστοποιητικού επικοινωνίας της Apple (MDM HTTPS). Τα πιστοποιητικά που εκδόθηκαν πριν από την 1η Ιουλίου 2019, πρέπει να πληρούν και αυτά τα κριτήρια.
- Το πιστοποιητικό HTTPS με υπογραφή του ESMC CA δεν πληροί αυτές τις απαιτήσεις.

> Συνιστάται να μην αναβαθμίσετε τις κινητές συσκευές σας σε iOS 13 εάν δεν πληρούνται οι απαιτήσεις του πιστοποιητικού επικοινωνίας της Apple. Μια τέτοια ενέργεια θα έχει ως αποτέλεσμα να σταματήσει η σύνδεση των συσκευών σας με το ESET PROTECT MDM.

- Εάν έχετε ήδη αναβαθμίσει χωρίς το κατάλληλο πιστοποιητικό και οι συσκευές σας έπαψαν να συνδέονται με το ESET PROTECT MDM, πρέπει πρώτα να αλλάξετε το τρέχον πιστοποιητικό HTTPS που χρησιμοποιείτε για την επικοινωνία με τις συσκευές iOS με το πιστοποιητικό που πληροί τις απαιτήσεις του πιστοποιητικού επικοινωνίας της Apple (MDM HTTPS) και, μετά από αυτό να εγγράψετε ξανά τις συσκευές iOS.
- Εάν δεν έχετε αναβαθμίσει σε iOS 13, βεβαιωθείτε ότι το τρέχον πιστοποιητικό MDM HTTPS που χρησιμοποιείται για επικοινωνία με τις συσκευές iOS πληροί τις απαιτήσεις του πιστοποιητικού επικοινωνίας της Apple (MDM HTTPS). Εάν το έχετε κάνει, μπορείτε να συνεχίσετε την αναβάθμιση των συσκευών iOS σε iOS 13. Εάν δεν πληροί τις απαιτήσεις, αλλάξτε το τρέχον πιστοποιητικό MDM HTTPS με το πιστοποιητικό HTTPS που πληροί τις απαιτήσεις του πιστοποιητικού επικοινωνίας της Apple (MDM HTTPS) και, στη συνέχεια, προχωρήστε στην αναβάθμιση των συσκευών iOS σε iOS 13.

Υποστηριζόμενα περιβάλλοντα παροχής

επιφάνειας εργασίας

Η παροχή επιφάνειας εργασίας διευκολύνει τη διαχείριση συσκευών και επιτρέπει ταχύτερη παράδοση επιτραπέζιων υπολογιστών σε τελικούς χρήστες.

Οι παρεχόμενες επιφάνειες εργασίας είναι κατά κανόνα φυσικές ή εικονικές. Για εικονικά περιβάλλοντα που χρησιμοποιούν λειτουργικά συστήματος ροής (υπηρεσίες παροχής Citrix), δείτε τη λίστα υποστηριζόμενων υπερεποπτών.

ESET PROTECT On-Prem υποστηρίζει:

- συστήματα με μη μόνιμους δίσκους
- περιβάλλοντα VDI
- αναγνώριση κλωνοποιημένων υπολογιστών

Υποστηριζόμενοι υπερεπόπτες και επεκτάσεις υπερεπόπτη

Υπερ-επόπτης	ESET PROTECT On-Prem	ESET Full Disk Encryption
Citrix XenServer	✔	X
Microsoft Hyper-V	✔	✔ (δεν υποστηρίζεται η ασφαλής εκκίνηση)
VMware vSphere	✔	✔ (7.0.3.00300)
VMware ESXi	✔	✔ (7.0)
VMware Workstation	✔	✔ (16.2.3)
VMware View	✔	X
Oracle VirtualBox	✔	X
VMware Fusion	? x64 X ARM	✔ (12.2.3)
Parallels	X	✔

Επέκταση υπερεπόπτη	ESET PROTECT On-Prem	ESET Full Disk Encryption
Citrix VDI-in-a-box	✔	X
Citrix XenDesktop	✔	X

Εργαλεία

(ισχύει για εικονικούς και φυσικούς υπολογιστές)

- Microsoft SCCM
- Windows Server 2012/2016/2019/2022 Server Manager
- Κέντρο διαχείρισης Windows

Διαμόρφωση μεγέθους υλικού και υποδομής

Ο υπολογιστής του διακομιστή ESET PROTECT θα πρέπει να πληροί τις συστάσεις υλικού του ακόλουθου πίνακα.

Αριθμός υπολογιστών-πελατών	ESET PROTECTΔιακομιστής + Διακομιστής βάσης δεδομένων SQL				
	Πυρήνες CPU	Ταχύτητα ρολογιού CPU (GHz)	Μνήμη RAM (GB)	Μονάδα δίσκου1	Δίσκος IOPS2
Έως 1.000	4	2.1	4	Μονός	500
5.000	8	2.1	8		1.000
10,000 3	4	2.1	16	Ξεχωριστός	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	64+		20.000

1 Μονή / Ξεχωριστή μονάδα δίσκου - Συνιστάται να εγκαταστήσετε τη βάση δεδομένων σε ξεχωριστή μονάδα δίσκου για συστήματα με περισσότερους από 10.000 υπολογιστές-πελάτες.

2 IOPS (συνολικές λειτουργίες εισόδου/εξόδου ανά δευτερόλεπτο) - ελάχιστη απαιτούμενη τιμή.

- Συνιστάται να έχετε κατά προσέγγιση 0,2 IOPS ανά συνδεδεμένο υπολογιστή-πελάτη, αλλά τουλάχιστον 500.

- Μπορείτε να ελέγξετε τα IOPS της μονάδας δίσκου σας χρησιμοποιώντας το εργαλείο diskspd. Χρησιμοποιήστε την ακόλουθη εντολή:

Αριθμός υπολογιστών-πελατών	Εντολή
Έως 5.000 υπολογιστές-πελάτες	`diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat`
Άνω των 5.000 υπολογιστών-πελατών	`diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat`

3 Ανατρέξτε στο παράδειγμα σεναρίου για περιβάλλον 10.000 υπολογιστών-πελατών.

Συστάσεις μονάδας δίσκου

Η μονάδα δίσκου είναι ο κρίσιμος παράγοντας που επηρεάζει τις επιδόσεις του ESET PROTECT On-Prem.

- Η εμφάνιση του διακομιστή SQL μπορεί να μοιράζεται πόρους με το διακομιστή ESET PROTECT για μεγιστοποίηση της χρηστικότητας και ελαχιστοποίηση των καθυστερήσεων. Εκτελέστε το διακομιστή ESET PROTECT και το διακομιστή βάσης δεδομένων σε έναν υπολογιστή για να αυξήσετε τις επιδόσεις του ESET PROTECT On-Prem.

- Οι επιδόσεις ενός διακομιστή SQL ενισχύονται εάν τοποθετήσετε τα αρχεία καταγραφής βάσης δεδομένων και συναλλαγών σε ξεχωριστές μονάδες δίσκου, κατά προτίμηση σε ξεχωριστές φυσικές μονάδες δίσκου SSD.

- Εάν έχετε μία μονάδα δίσκου, συνιστάται να χρησιμοποιήσετε μονάδα δίσκου SSD.

• Συνιστάται να χρησιμοποιήσετε αρχιτεκτονική στερεάς κατάστασης. Οι δίσκοι στερεάς κατάστασης (SSD) είναι πολύ ταχύτεροι από τον τυπικό δίσκο HDD.

• Εάν έχετε ρύθμιση παραμέτρων υψηλής μνήμης RAM, η ρύθμιση SAS με R5 είναι επαρκής. Η δοκιμασμένη ρύθμιση παραμέτρων: Δίσκοι 10x 1.2TB SAS σε R5 - ομάδα με ισοτιμία δύο σε 4+1 χωρίς επιπλέον προσωρινή μνήμη.

• Η απόδοση δεν βελτιώνεται εάν χρησιμοποιείται ένας δίσκος SSD εταιρικού επιπέδου με υψηλή τιμή IOPS.

• Η χωρητικότητα 100 GB επαρκεί για οποιονδήποτε αριθμό υπολογιστών-πελατών. Ενδέχεται να χρειάζεστε μεγαλύτερη χωρητικότητα, εάν δημιουργείτε συχνά αντίγραφα ασφαλείας της βάσης δεδομένων.

• Μη χρησιμοποιήσετε μονάδα δίσκου δικτύου, επειδή οι επιδόσεις της θα επιβραδύνουν το ESET PROTECT On-Prem.

• Εάν έχετε μια λειτουργική υποδομή αποθήκευσης πολλαπλών επιπέδων, η οποία επιτρέπει τη μετεγκατάσταση χώρου αποθήκευσης στο διαδίκτυο, συνιστάται να ξεκινήσετε με πιο αργά κοινόχρηστα επίπεδα και να παρακολουθείτε τις επιδόσεις του ESET PROTECT On-Prem. Εάν παρατηρήσετε ότι η καθυστέρηση στην ανάγνωση/εγγραφή υπερβαίνει τα 20ms, μπορείτε να εκτελέσετε μη ενοχλητική μετακίνηση στο επίπεδο αποθήκευσης που έχετε σε ένα ταχύτερο επίπεδο, για να χρησιμοποιήσετε τον πιο οικονομικό μηχανισμό backend. Μπορείτε να κάνετε το ίδιο σε έναν υπερεπόπτη (εάν χρησιμοποιείτε το ESET PROTECT On-Prem ως εικονικό υπολογιστή).

Συστάσεις μεγεθών για διάφορους αριθμούς υπολογιστών-πελατών

Παρακάτω θα βρείτε τα αποτελέσματα επιδόσεων για ένα εικονικό περιβάλλον με καθορισμένο αριθμό υπολογιστών-πελατών που λειτουργούν ένα έτος.

ℹ Η βάση δεδομένων και το ESET PROTECT On-Prem εκτελούνται σε ξεχωριστούς εικονικούς υπολογιστές με πανομοιότυπες ρυθμίσεις παραμέτρων υλικού.

Πυρήνες CPU	Ταχύτητα ρολογιού CPU (GHz)	Μνήμη RAM (GB)	Επιδόσεις		
			10.000 υπολογιστές-πελάτες	20.000 υπολογιστές-πελάτες	40.000 υπολογιστές-πελάτες
8	2.1	64	Υψηλή	Υψηλή	Κανονικό
8	2.1	32	Κανονικό	Κανονικό	Κανονικό
4	2.1	32	Κανονικό	Κανονικό	Χαμηλή
2	2.1	16	Χαμηλή	Χαμηλή	Ανεπαρκής
2	2.1	8	Πολύ χαμηλή (δεν συνιστάται)	Πολύ χαμηλή (δεν συνιστάται)	Ανεπαρκής

Συστάσεις ανάπτυξης

Βέλτιστες πρακτικές για την ανάπτυξη του ESET PROTECT On-Prem

Αριθμός υπολογιστών-πελατών	Έως 1.000	1,000–5,000	5,000–10,000	10,000–50,000	50,000–100,000	100,000+
ESET PROTECTΔιακομιστής και διακομιστής βάσης δεδομένων στον ίδιο υπολογιστή	✔	✔	✔	X	X	X
Χρήση του Microsoft SQL Express	✔	?*	X	X	X	X
Χρήση του Microsoft SQL	✔	✔	✔	✔	✔	✔
Χρήση του MySQL	✔	✔	✔	X	X	X
Χρήση της εικονικής συσκευής ESET PROTECT	✔	✔	Δεν συνιστάται	X	X	X
Χρήση διακομιστή VM	✔	✔	✔	Προαιρετική	X	X
Συνιστώμενο διάστημα σύνδεσης (κατά τη φάση ανάπτυξης)	60 δευτερόλεπτα	5 λεπτά	10 λεπτά	15 λεπτά	20 λεπτά	25 λεπτά
Συνιστώμενο διάστημα σύνδεσης (μετά την ανάπτυξη, κατά την τυπική χρήση)	10 λεπτά	10 λεπτά	20 λεπτά	30 λεπτά	40 λεπτά	60 λεπτά

* Για να αποφύγετε τη συμπλήρωση της βάσης δεδομένων του ESET PROTECT, δεν συνιστάται αυτό το σενάριο εάν χρησιμοποιείτε και το ESET Inspect On-Prem.

Διάστημα σύνδεσης

Ο διακομιστής ESET PROTECT συνδέεται στους φορείς ESET Management με χρήση μόνιμων συνδέσεων. Παρά τη μόνιμη σύνδεση, η μετάδοση δεδομένων προκύπτει μόνο μία φορά κατά τη διάρκεια του διαστήματος σύνδεσης. Για παράδειγμα, εάν το διάστημα αναπαραγωγής σε 5.000 υπολογιστές-πελάτες έχει οριστεί σε οκτώ λεπτά, υπάρχουν 5.000 μεταδόσεις σε 480 δευτερόλεπτα, 10,4 ανά δευτερόλεπτο. Βεβαιωθείτε ότι έχετε ρυθμίσει το κατάλληλο χρονικό διάστημα σύνδεσης υπολογιστή-πελάτη. Βεβαιωθείτε ότι διατηρείτε τον συνολικό αριθμό των συνδέσεων φορέα - διακομιστή κάτω από το όριο των 1.000 ανά δευτερόλεπτο, ακόμα και για ρυθμίσεις παραμέτρων υλικού υψηλών επιδόσεων.

Εάν ένας διακομιστής υπερφορτωθεί ή σημειωθεί επίθεση κακόβουλου λογισμικού (για παράδειγμα, συνδέονται 20.000 υπολογιστές-πελάτες σε έναν διακομιστή που μπορεί να εξυπηρετήσει μόνο 10.000 υπολογιστές-πελάτες ανά χρονικό διάστημα 10 λεπτών), ο διακομιστής θα παραβλέψει κάποιους από τους συνδεδεμένους υπολογιστές-πελάτες. Οι μη συνδεδεμένοι υπολογιστές θα προσπαθήσουν να συνδεθούν στο διακομιστή ESET PROTECT αργότερα.

Ένας διακομιστής (Μικρή επιχείρηση)

Για τη διαχείριση μικρών δικτύων (1.000 υπολογιστές-πελάτες ή λιγότεροι) χρησιμοποιήστε έναν υπολογιστή με διακομιστή ESET PROTECT και όλα τα στοιχεία του ESET PROTECT που είναι εγκατεστημένα σε αυτόν. Σε περιβάλλοντα SMB/μικρών δικτύων, συνιστάται να εξετάσετε το ενδεχόμενο εγκατάστασης του ESET PROTECT On-Prem σε Linux ή σε εικονική συσκευή, ανάλογα με την περίπτωση.

Απομακρυσμένοι κλάδοι με διακομιστές μεσολάβησης

Εάν οι υπολογιστές-πελάτες δεν βλέπουν απευθείας τον Διακομιστή ESET PROTECT, χρησιμοποιήστε έναν διακομιστή μεσολάβησης για να προωθήσετε την επικοινωνία των προϊόντων ESET. Ο

διακομιστής μεσολάβησης HTTP δεν συγκεντρώνει τις επικοινωνίες και δεν μειώνει την κυκλοφορία της αντιγραφής.

Υψηλή διαθεσιμότητα (Εταιρικό)

Για εταιρικά περιβάλλοντα (πάνω από 10.000 υπολογιστές-πελάτες), εξετάστε τα εξής:

• Ο αισθητήρας RD βοηθά στην αναζήτηση του δικτύου σας και τον εντοπισμό νέων υπολογιστών.

• Μπορείτε να εγκαταστήσετε τον Διακομιστή ESET PROTECT σε ένα σύμπλεγμα ανακατεύθυνσης.

• Ρυθμίστε τις παραμέτρους του Διακομιστή μεσολάβησης HTTP για μεγάλο αριθμό υπολογιστών-πελατών ή χρησιμοποιήστε περισσότερους διακομιστές μεσολάβησης.

Ρύθμιση παραμέτρων της Κονσόλας διαδικτύου για επιχειρηματικές λύσεις ή συστήματα χαμηλών επιδόσεων

Από προεπιλογή, η Κονσόλα διαδικτύου ESET PROTECT που εγκαθίσταται μέσω του προγράμματος εγκατάστασης «όλα σε ένα» για Windows διατηρεί ένα όριο μνήμης 1024 MB για το Apache Tomcat.

Μπορείτε να αλλάξετε την προεπιλεγμένη ρύθμιση παραμέτρων της Κονσόλας διαδικτύου με βάση την υποδομή σας:

• Σε επιχειρηματικό περιβάλλον, η προεπιλεγμένη ρύθμιση παραμέτρων της Κονσόλας διαδικτύου μπορεί να παρουσιάσει αστάθεια κατά την εργασία με μεγάλο αριθμό αντικειμένων. Αλλάξτε τις ρυθμίσεις Tomcat, για να αποτραπεί η εμφάνιση ελλειμμάτων μνήμης. Βεβαιωθείτε ότι το σύστημά σας έχει αρκετή μνήμη RAM (16 GB ή περισσότερα) προτού κάνετε αυτές τις αλλαγές.

• Εάν έχετε σύστημα χαμηλών επιδόσεων με περιορισμένους πόρους υλικού, μπορείτε να μειώσετε τη χρήση μνήμης από το Tomcat.

> Οι τιμές μνήμης που παρέχονται παρακάτω αποτελούν συστάσεις. Μπορείτε να προσαρμόσετε τις ρυθμίσεις μνήμης Tomcat με βάση τους πόρους υλικού σας.

Windows

1. Ανοίξτε το αρχείο *tomcat9w.exe* ή εκτελέστε την εφαρμογή `Configure Tomcat`.
2. Μεταβείτε στην καρτέλα **Java**.
3. Αλλαγή της χρήσης μνήμης:
    a. Αύξηση (επιχείρηση): Αλλάξτε τις τιμές για το στοιχείο **Αρχική συγκεντρωτική μνήμη** σε 2048 MB και για το στοιχείο **Μέγιστη συγκεντρωτική μνήμη** σε 16384 MB.
    b. Μείωση (συστήματα χαμηλών επιδόσεων): Αλλάξτε τις τιμές για το στοιχείο **Αρχική συγκεντρωτική μνήμη** σε 256 MB και για το στοιχείο **Μέγιστη συγκεντρωτική μνήμη** σε 2048 MB.
4. Επανεκκινήστε την υπηρεσία Tomcat.

LINUX και εικονική συσκευή ESET PROTECT

1.Ανοίξτε το τερματικό ως ρίζα ή χρησιμοποιήστε το `sudo`.

2.Ανοίξτε το αρχείο

a.Εικονική συσκευή ESET PROTECT / CentOS: `/etc/sysconfig/tomcat`

b.Debian: `/etc/default/tomcat9`

3.Προσθέστε την παρακάτω γραμμή στο αρχείο:

a.Αύξηση της χρήσης μνήμης (επιχείρηση): `JAVA_OPTS="-Xms2048m -Xmx16384m"`

b.Μείωση της χρήσης μνήμης (συστήματα χαμηλών επιδόσεων): `JAVA_OPTS="-Xms256m -Xmx2048m"`

4.Αποθηκεύστε το αρχείο και επανεκκινήστε την υπηρεσία Tomcat.
`service tomcat restart`

Ανάπτυξη για 10.000 υπολογιστές-πελάτες

Παρακάτω θα βρείτε τα αποτελέσματα επιδόσεων για ένα εικονικό περιβάλλον με 10.000 υπολογιστές-πελάτες με διάρκεια εκτέλεσης ενός έτους.

Ρύθμιση παραμέτρων διακομιστή υπερεπόπτη

ΣΤΟΙΧΕΙΟ	Τιμή
VMware	ESXi 6.7 Ενημέρωση 2 και νεότερες εκδόσεις (VM έκδοση 15)
Υπερ-επόπτης	VMware ESXi, 6.7.0
Λογικοί επεξεργαστές	112
Τύπος επεξεργαστή	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz

Η δοκιμή εκτελέστηκε σε αποκλειστικούς υπολογιστές
Η βάση δεδομένων και το ESET PROTECT On-Prem εκτελούνται σε ξεχωριστούς εικονικούς υπολογιστές με πανομοιότυπες ρυθμίσεις παραμέτρων υλικού.

Λογισμικό που χρησιμοποιείται σε εικονικούς υπολογιστές

ESET PROTECT On-Prem:

- Λειτουργικό σύστημα: Microsoft Windows Server 2016 Standard (64-bit)

Βάση δεδομένων:

- Διακομιστής βάσης δεδομένων: Microsoft SQL Server 2017 (RTM) Standard Edition (64-bit)
- Λειτουργικό σύστημα: Microsoft Windows Server 2016 Standard (64-bit)

Περιγραφή περιβάλλοντος του ESET PROTECT On-Prem

- 10.000 συνδεδεμένοι υπολογιστές-πελάτες
- Περίπου 2.000 δυναμικές ομάδες και 2.000 πρότυπα για δυναμικές ομάδες
- Περίπου 255 στατικές ομάδες
- 20 χρήστες
- Διάστημα σύνδεσης 15 λεπτών για τους Φορείς ESET Management
- Μετά την εκτέλεση του περιβάλλοντος για ένα έτος, το μέγεθος της βάσης δεδομένων είναι 15 GB

Πλήθος CPU	Μνήμη RAM (GB)	Επιδόσεις
8	64	Υψηλή
4	32	Κανονικό
2	16	Χαμηλή
2	8	Πολύ χαμηλή (δεν συνιστάται)

Βάση δεδομένων

Καθορίστε το διακομιστή βάσης δεδομένων και τη σύνδεση που θέλετε να χρησιμοποιήσετε κατά την εγκατάσταση του διακομιστή ESET PROTECT. Μπορείτε να χρησιμοποιήσετε έναν υπάρχοντα διακομιστή που εκτελείται στο περιβάλλον σας. Ωστόσο, θα πρέπει να πληροί τις παρακάτω απαιτήσεις.

ESET PROTECT On-Prem 11.0 Το πρόγραμμα εγκατάστασης «όλα σε ένα» εγκαθιστά το Microsoft SQL Server Express 2019 από προεπιλογή.

- Εάν χρησιμοποιείτε μια παλαιότερη έκδοση των Windows (Server 2012 ή SBS 2011), το Microsoft SQL Server Express 2014 θα εγκατασταθεί από προεπιλογή.
- Το πρόγραμμα εγκατάστασης δημιουργεί αυτόματα έναν τυχαίο κωδικό πρόσβασης για τον έλεγχο ταυτότητας της βάσης δεδομένων (που είναι αποθηκευμένη στη διαδρομή *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

Το Microsoft SQL Server Express έχει όριο μεγέθους 10 GB για κάθε σχετική βάση δεδομένων. Δεν συνιστάται η χρήση του Microsoft SQL Server Express:
- Σε εταιρικά περιβάλλοντα ή μεγάλα δίκτυα.
- Εάν θέλετε να χρησιμοποιήσετε το ESET PROTECT On-Prem με το ESET Inspect On-Prem.

Υποστηριζόμενοι διακομιστές βάσεων δεδομένων και

συνδέσεις βάσεων δεδομένων

Το ESET PROTECT On-Prem υποστηρίζει δύο τύπους διακομιστών βάσης δεδομένων: Microsoft SQL Server και MySQL.

> ⚠ Το ESET PROTECT On-Prem δεν υποστηρίζει MariaDB. Η βάση δεδομένων MariaDB είναι η προεπιλεγμένη βάση δεδομένων στα περισσότερα τρέχοντα περιβάλλοντα Linux και εγκαθίσταται όταν επιλέγετε να εγκαταστήστε το MySQL.

Υποστηριζόμενοι διακομιστές βάσης δεδομένων	Υποστηριζόμενες εκδόσεις βάσης δεδομένων	Υποστηριζόμενες συνδέσεις βάσης δεδομένων
Microsoft SQL Server	• Εκδόσεις Express και μη Express • 2014, 2016, 2017, 2019, 2022	• Διακομιστής SQL • Τοπικό πρόγραμμα-πελάτης διακομιστή SQL 10.0 • Πρόγραμμα οδήγησης ODBC για το διακομιστή SQL 11, 13, 17, 18
MySQL	• 5.6* • 5.7 • 8.0 • 8.1	Εκδόσεις προγράμματος οδήγησης MySQL ODBC: • 5.1, 5.2 • 5.3.0-5.3.10 • 8.x (8.0.x, 8.1.x)

* Το MySQL 5.6 έφτασε στο τέλος του κύκλου ζωής του τον Φεβρουάριο του 2021. Συνιστάται να αναβαθμίσετε τον διακομιστή βάσης δεδομένων MySQL στην έκδοση 5.7 και νεότερες εκδόσεις.

> ⚠ Οι ακόλουθες εκδόσεις του προγράμματος οδήγησης MySQL ODBC δεν υποστηρίζονται:
> • 5.3.11 και νεότερες εκδόσεις 5.3.x

Απαιτήσεις υλικού διακομιστή βάσης δεδομένων

Ανατρέξτε στις οδηγίες για το υλικό και τη διαμόρφωση μεγέθους.

Συστάσεις επιδόσεων

Συνιστάται να χρησιμοποιείτε το πιο πρόσφατο υποστηριζόμενο Microsoft SQL Server ως βάση δεδομένων του ESET PROTECT, για βέλτιστες επιδόσεις. Παρόλο που το ESET PROTECT On-Prem είναι συμβατό με το MySQL, η χρήση του MySQL μπορεί να επηρεάσει αρνητικά τις επιδόσεις του συστήματος όταν εργάζεστε με μεγάλους όγκους δεδομένων, όπως πίνακες ελέγχου, ανιχνεύσεις και υπολογιστές-πελάτες. Το ίδιο υλικό με το Microsoft SQL Server μπορεί να χειριστεί πολύ περισσότερους υπολογιστές-πελάτες από ότι το MySQL.

Μπορείτε να αποφασίσετε αν θα εγκαταστήσετε έναν διακομιστή βάσης δεδομένων SQL:

- Στον ίδιο υπολογιστή με το διακομιστή ESET PROTECT.
- Στον ίδιο υπολογιστή, αλλά σε ξεχωριστό δίσκο.
- Σε έναν αποκλειστικό διακομιστή για εγκατάσταση ενός διακομιστή βάσης δεδομένων SQL.

Εάν θέλετε να διαχειρίζεστε περισσότερους από 10.000 υπολογιστές-πελάτες, συνιστούμε να χρησιμοποιήσετε έναν ή περισσότερους αποκλειστικούς υπολογιστές με δεσμευμένους πόρους.

Βάση δεδομένων	Πελάτης SMB	Εταιρικός πελάτης	Όριο υπολογιστών	Windows	Linux
Microsoft SQL Express	✔	(προαιρετικό)	5.000	✔	
Microsoft SQL Server	✔	✔	Καμιά	✔	
MySQL	✔	✔	10.000	✔	✔

Πρόσθετες πληροφορίες

ESET PROTECTO διακομιστής δεν χρησιμοποιεί ενσωματωμένο αντίγραφο ασφαλείας. Συνιστούμε οπωσδήποτε να δημιουργήσετε αντίγραφο ασφαλείας του διακομιστή βάσης δεδομένων, για να αποφύγετε απώλεια δεδομένων.

- Μην εγκαταστήσετε το SQL Server σε έναν Ελεγκτή τομέα (για παράδειγμα, Windows SBS / Essentials). Συνιστάται να εγκαταστήσετε το ESET PROTECT On-Prem σε διαφορετικό διακομιστή ή να μην επιλέξετε το στοιχείο του SQL Server Express κατά την εγκατάσταση (αυτό απαιτεί να χρησιμοποιήσετε το υπάρχον SQL ή MySQL Server για την εκτέλεση της βάσης δεδομένων ESET PROTECT).

- Εάν σκοπεύετε να χρησιμοποιήσετε τον αποκλειστικό λογαριασμό χρήστη βάσης δεδομένων που θα έχει πρόσβαση μόνο στη βάση δεδομένων ESET PROTECT, πρέπει να δημιουργήσετε ένα λογαριασμό χρήστη με συγκεκριμένα δικαιώματα πριν από την εγκατάσταση. Για περισσότερες πληροφορίες, ανατρέξτε στο κεφάλαιο Αποκλειστικός λογαριασμός χρήστη βάσης δεδομένων. Επιπλέον, θα χρειαστεί να δημιουργήσετε μια κενή βάση δεδομένων η οποία θα χρησιμοποιείται από το ESET PROTECT On-Prem.

- Δείτε τις οδηγίες για τον τρόπο εγκατάστασης και ρύθμισης παραμέτρων του MySQL για Windows και του MySQL για Linux ώστε να λειτουργούν σωστά με το ESET PROTECT On-Prem.

- Το Microsoft SQL Server σε Linux δεν υποστηρίζεται. Ωστόσο, μπορείτε να συνδέσετε το διακομιστή ESET PROTECT σε Linux με το Microsoft SQL Server σε Windows.

- Εάν εγκαταστήσετε το διακομιστή ESET PROTECT και το Microsoft SQL Server σε ξεχωριστούς υπολογιστές, μπορείτε να ενεργοποιήσετε μια κρυπτογραφημένη σύνδεση με τη βάση δεδομένων.

- Η ρύθμιση cluster της βάσης δεδομένων σε περιβάλλοντα Windows υποστηρίζεται μόνο για το Microsoft SQL Server, όχι για το MySQL.

Υποστηριζόμενες εκδόσεις των Apache Tomcat και Java

Apache Tomcat

το Apache Tomcat είναι απαραίτητο στοιχείο για τη λειτουργία της Κονσόλας διαδικτύου ESET PROTECT.

Το ESET PROTECT On-Prem υποστηρίζει μόνο Apache Tomcat 9.x (64 bit). Συνιστάται να χρησιμοποιήσετε την πιο πρόσφατη έκδοση του Apache Tomcat 9.x.

Το ESET PROTECT On-Prem δεν υποστηρίζει τις εκδόσεις alpha/beta/RC του Apache Tomcat.

Java

Το Apache Tomcat απαιτεί Java/OpenJDK 64 bit.

Εάν έχετε πολλαπλές εκδόσεις Java εγκατεστημένες στο σύστημά σας, συνιστάται να καταργήσετε την εγκατάσταση των παλαιότερων εκδόσεων Java και να διατηρήσετε μόνο την πιο πρόσφατη υποστηριζόμενη έκδοση Java.

⚠ Από τον Ιανουάριο 2019, οι δημόσιες ενημερώσεις Oracle JAVA SE 8 για επιχειρηματική, εμπορική ή παραγωγική χρήση, απαιτούν εμπορική άδεια χρήσης. Εάν δεν αγοράσετε συνδρομή JAVA SE, μπορείτε να χρησιμοποιήσετε αυτό τον οδηγό για μετάβαση σε μια εναλλακτική λύση χωρίς κόστος. Δείτε τις υποστηριζόμενες εκδόσεις του JDK.

Υποστηριζόμενα προγράμματα περιήγησης στο διαδίκτυο, προϊόντα ασφάλειας ESET και γλώσσες

Τα ακόλουθα λειτουργικά συστήματα υποστηρίζονται από το ESET PROTECT On-Prem:

- Windows, Linux και macOS

Η κονσόλα διαδικτύου ESET PROTECT μπορεί να εκτελείται στα ακόλουθα προγράμματα περιήγησης στο διαδίκτυο:

Πρόγραμμα περιήγησης στο διαδίκτυο
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

Για τη βέλτιστη εμπειρία με την κονσόλα διαδικτύου ESET PROTECT, συνιστάται να διατηρείτε τα προγράμματα περιήγησης στο διαδίκτυο ενημερωμένα.

Νεότερες εκδόσεις των προϊόντων ESET των οποίων η διαχείριση πραγματοποιείται μέσω του ESET PROTECT On-Prem 11.0

Η διαχείριση των εκδόσεων του προϊόντος ασφάλειας ESET που αναφέρονται παρακάτω είναι δυνατή με έκδοση Φορέα ESET Management 11.0 και νεότερες εκδόσεις.
Συνιστάται η χρήση της πιο πρόσφατης έκδοσης Φορέα ESET Management για την πλήρη διαχείριση της πιο πρόσφατης έκδοσης των προϊόντων ασφαλείας ESET και των δυνατοτήτων τους. Εάν χρησιμοποιείτε παλαιότερη έκδοση του Φορέα ESET Management από την έκδοση του Διακομιστή ESET PROTECT, ορισμένες από τις πιο πρόσφατες δυνατότητες διαχείρισης ενδέχεται να μην είναι διαθέσιμες.
Η διαχείριση των εκδόσεων προϊόντων ασφάλειας ESET που είναι παλαιότερες από αυτές που εμφανίζονται στον παρακάτω πίνακα δεν είναι εφικτή χρησιμοποιώντας το ESET PROTECT On-Prem 11.0.
Για περισσότερες πληροφορίες σχετικά με τη συμβατότητα, επισκεφθείτε την Πολιτική διάρκειας υποστήριξης προϊόντων της ESET για επιχειρήσεις.

Προϊόν	Έκδοση προϊόντος
ESET Endpoint Security για Windows	7.3, 8.x, 9.x, 10.x
ESET Endpoint Antivirus για Windows	7.3, 8.x, 9.x, 10.x
ESET Endpoint Security για macOS	6.10+
ESET Endpoint Antivirus για macOS	6.10+
ESET Endpoint Security για Android	3.3+
ESET Server Security για Microsoft Windows Server (πρώην ESET File Security για Microsoft Windows Server)	7.3, 8.x, 9.x, 10.x, 11.x
ESET Mail Security για Microsoft Exchange Server	7.3, 8.x, 9.x, 10.x, 11.x
ESET Security for Microsoft SharePoint Server	7.3, 8.x, 9.x, 10.x, 11.x
ESET Mail Security για IBM Domino	7.3, 8.x, 9.x, 10.x
ESET Server Security για Linux (πρώην ESET File Security για Linux)	7.2, 8.1, 9.x, 10.x
ESET Endpoint Antivirus για Linux	7.1, 8.1, 9.x, 10.x
ESET LiveGuard Advanced	
ESET Inspect Connector	1.8+
ESET Full Disk Encryption για Windows	
ESET Full Disk Encryption για macOS	

Προϊόντα που υποστηρίζουν ενεργοποίηση μέσω άδειας χρήσης συνδρομής

Προϊόν ESET	Διαθέσιμο από την έκδοση
ESET Endpoint Antivirus/Security για Windows	7.0
ESET Endpoint Antivirus/Security για macOS	6.8.x
ESET Endpoint Security για Android	2.0.158
Διαχείριση κινητών συσκευών ESET για Apple iOS	7.0

Προϊόν ESET	Διαθέσιμο από την έκδοση
ESET File Security για Microsoft Windows Server	7.0
ESET Mail Security για Microsoft Exchange	7.0
ESET File Security για Windows Server	7.0
ESET Mail Security για IBM Domino	7.0
ESET Security for Microsoft SharePoint Server	7.0
ESET File Security για Linux	7.0
ESET Endpoint Antivirus για Linux	7.0
ESET Server Security για Windows	8.0
ESET Server Security για Linux	8.1
ESET LiveGuard Advanced	
ESET Inspect On-Prem (με ESET Endpoint για Windows 7.3 και νεότερες εκδόσεις)	1.5

Υποστηριζόμενες γλώσσες

Γλώσσα	Κωδικός
Αγγλικά (Ηνωμένες Πολιτείες)	en-US
Αραβικά (Αίγυπτος)	ar-EG
Κινεζικά απλοποιημένα	zh-CN
Κινεζικά παραδοσιακά	zh-TW
Κροατικά (Κροατία)	hr-HR
Τσεχικά (Δημοκρατία της Τσεχίας)	cs-CZ
Γαλλικά (Γαλλία)	fr-FR
Γαλλικά (Καναδάς)	fr-CA
Γερμανικά (Γερμανία)	de-DE
Ελληνικά (Ελλάδα)	el-GR
Ουγγρικά (Ουγγαρία)*	hu-HU
Ινδονησιακά (Ινδονησία)*	id-ID
Ιταλικά (Ιταλία)	it-IT
Ιαπωνικά (Ιαπωνία)	ja-JP
Κορεατικά (Κορέα)	ko-KR
Πολωνικά (Πολωνία)	pl-PL
Πορτογαλικά (Βραζιλία)	pt-BR
Ρωσικά (Ρωσία)	ru-RU
Ισπανικά (Χιλή)	es-CL
Ισπανικά (Ισπανία)	es-ES
Σλοβακικά (Σλοβακία)	sk-SK
Τουρκικά (Τουρκία)	tr-TR
Ουκρανικά (Ουκρανίας)	uk-UA

* Μόνο το προϊόν είναι διαθέσιμο σε αυτή τη γλώσσα. Η ηλεκτρονική βοήθεια δεν είναι διαθέσιμη.

Δίκτυο

Εάν σημαντικό τόσο ο διακομιστής ESET PROTECT και οι υπολογιστές-πελάτες τους οποίους διαχειρίζεστε με το ESET PROTECT On-Prem να διαθέτουν λειτουργική σύνδεση στο Internet, προκειμένου να μπορούν να επικοινωνούν με το χώρο αποθήκευσης της ESET και τους διακομιστές ενεργοποίησης. Εάν προτιμάτε να μην έχετε υπολογιστές-πελάτες συνδεδεμένους απευθείας στο Internet, μπορείτε να χρησιμοποιήσετε έναν διακομιστή μεσολάβησης (διαφορετικό από τον ESET Bridge διακομιστή μεσολάβησης HTTP) για τη διευκόλυνση της επικοινωνίας μεταξύ του δικτύου σας και του Internet.

Ο διακομιστής ESET PROTECT πρέπει να είναι ορατός στους υπολογιστές-πελάτες – οι υπολογιστές-πελάτες πρέπει να μπορούν να επικοινωνούν με τον διακομιστή ESET PROTECT για να χρησιμοποιούν τις δυνατότητες απομακρυσμένης ανάπτυξης και κλήσης αφύπνισης.

Το ESET PROTECT On-Prem για Windows/Linux είναι συμβατό και με τα δύο πρωτόκολλα Internet IPv4 και IPv6. Η Εικονική συσκευή ESET PROTECT είναι συμβατή μόνο με το πρωτόκολλο IPv4.

Θύρες που χρησιμοποιούνται

Εάν το δίκτυό σας χρησιμοποιεί firewall, δείτε τη λίστα με τις θύρες επικοινωνίας δικτύου που είναι δυνατόν να χρησιμοποιούνται όταν το ESET PROTECT On-Prem και τα στοιχεία του είναι εγκατεστημένα στην υποδομή σας.

Επίπτωση στην κυκλοφορία δικτύου από την επικοινωνία του διακομιστή ESET PROTECT και του φορέα ESET Management

Οι εφαρμογές στους υπολογιστές-πελάτες δεν επικοινωνούν απευθείας με το διακομιστή ESET PROTECT. Ο φορέας ESET Management διευκολύνει αυτή την επικοινωνία. Αυτή η λύση προσφέρει πιο εύκολη διαχείριση και είναι λιγότερο απαιτητική σε σχέση με τα δεδομένα που μεταφέρονται μέσω δικτύου. Η κυκλοφορία δικτύου εξαρτάται από το διάστημα σύνδεσης του υπολογιστή-πελάτη και τους τύπους εργασιών που εκτελούνται από τους υπολογιστές-πελάτες. Ακόμα και αν δεν εκτελεστεί ή προγραμματιστεί καμία εργασία σε έναν υπολογιστή-πελάτη, ο φορέας ESET Management επικοινωνεί με το διακομιστή ESET PROTECT μία φορά σε κάθε διάστημα σύνδεσης. Κάθε σύνδεση δημιουργεί κυκλοφορία. Ανατρέξτε στον παρακάτω πίνακα για παραδείγματα κυκλοφορίας:

Τύπος ενέργειας	Κυκλοφορία σε ένα διάστημα σύνδεσης
Εργασία υπολογιστή-πελάτη: Σάρωση χωρίς καθαρισμό	4 kB
Εργασία υπολογιστή-πελάτη: Ενημέρωση μονάδων	4 kB
Εργασία υπολογιστή-πελάτη: Αίτημα αρχείου καταγραφής SysInspector	300 kB
Πολιτική Antivirus - Μέγιστη ασφάλεια	26 kB

ESET ManagementΔιάστημα αντιγραφής φορέα	Ημερήσια κυκλοφορία που δημιουργείται από έναν αδρανή φορέα ESET Management
1 λεπτό	16 MB
15 λεπτά	1 MB
30 λεπτά	0,5 MB
1 ώρα	144 kB
1 ημέρα	12 kB

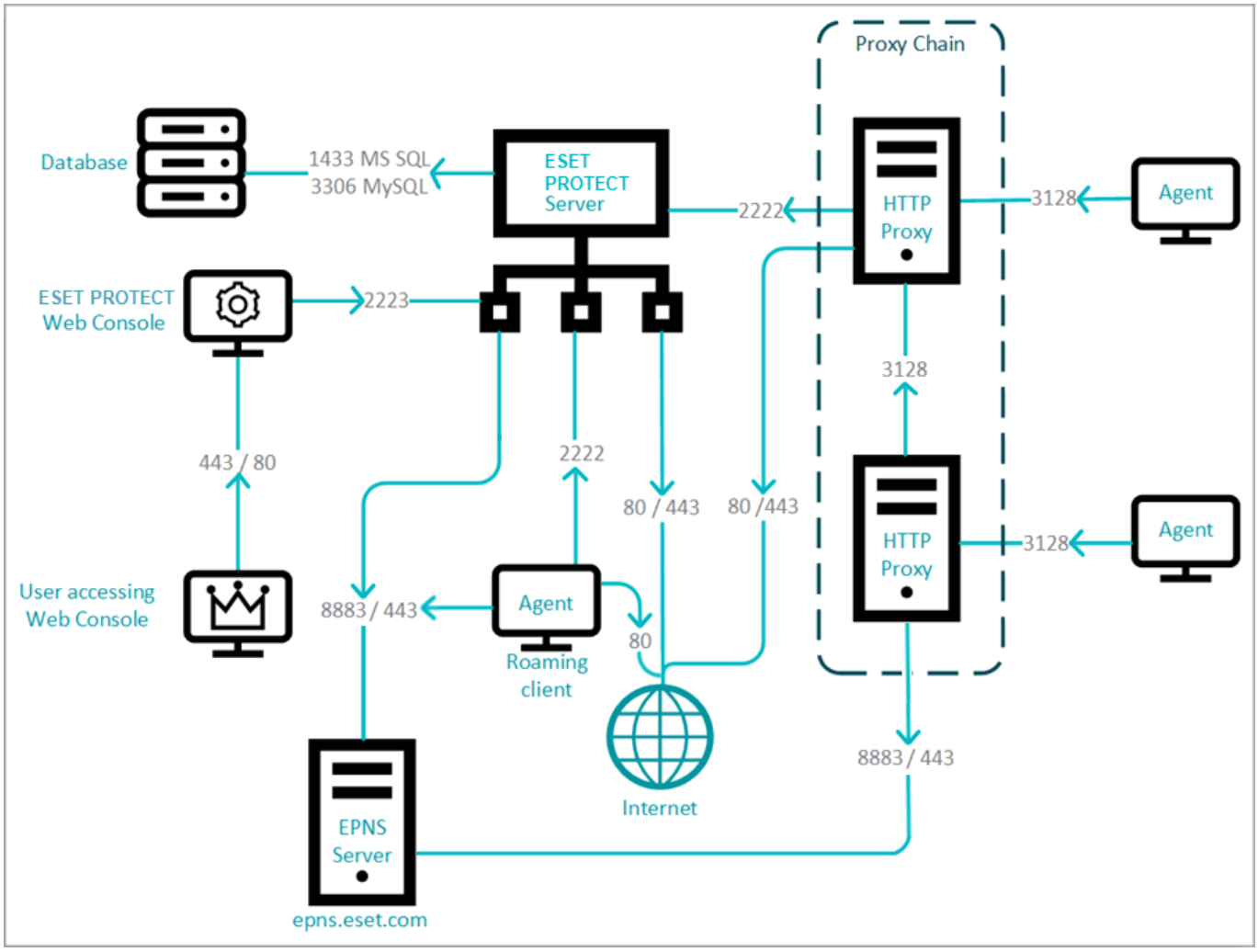
Για να εκτιμήσετε τη συνολική κυκλοφορία που δημιουργείται από τους φορείς ESET Management, χρησιμοποιήστε τον παρακάτω τύπο:

Αριθμός υπολογιστών-πελατών * (Ημερήσια κυκλοφορία αδρανούς φορέα + (Κυκλοφορία για συγκεκριμένη εργασία * ημερήσια εμφάνιση της εργασίας))

Εάν χρησιμοποιείτε το ESET Inspect On-Prem, ο ESET Inspect Connector δημιουργεί ημερήσια κυκλοφορία 2-5 MB (ποικίλει ανάλογα με τον αριθμό συμβάντων).

Θύρες που χρησιμοποιούνται

Ο διακομιστής ESET PROTECT μπορεί να εγκατασταθεί στον ίδιο υπολογιστή με τη βάση βάση δεδομένων, την κονσόλα διαδικτύου ESET PROTECT και το διακομιστή μεσολάβησης HTTP. Το παρακάτω διάγραμμα παρουσιάζει την ξεχωριστή εγκατάσταση και τις θύρες που χρησιμοποιούνται (τα βέλη υποδεικνύουν τη δικτυακή κίνηση:



Στους παρακάτω πίνακες αναγράφονται όλες οι πιθανές θύρες επικοινωνίας δικτύου που χρησιμοποιούνται όταν εγκαθίσταται το ESET PROTECT On-Prem και τα στοιχεία του στην υποδομή σας. Άλλες επικοινωνίες επιτυγχάνονται μέσω των τοπικών διεργασιών του λειτουργικού συστήματος (για παράδειγμα NetBIOS μέσω TCP/IP).

Για την ορθή λειτουργία του ESET PROTECT On-Prem, οι άλλες εφαρμογές δεν πρέπει να χρησιμοποιούν καμία από τις παρακάτω θύρες.
Βεβαιωθείτε ότι έχετε ρυθμίσεις τις παραμέτρους για οποιαδήποτε τείχη προστασίας μέσα στο δίκτυό σας, για να επιτρέπεται η επικοινωνία μέσω των θυρών που αναγράφονται παρακάτω.

Υπολογιστής-πελάτης (φορέας ESET Management) ή υπολογιστής ESET Bridge διακομιστή μεσολάβησης HTTP

Πρωτόκολλο	Θύρα	Περιγραφές
TCP	2222	Επικοινωνία μεταξύ φορέων ESET Management και του διακομιστή ESET PROTECT
TCP	80	Σύνδεση με το αποθετήριο της ESET
MQTT	8883, 443	Υπηρεσία ESET Push Notification Service - Κλήσεις αφύπνισης μεταξύ του διακομιστή ESET PROTECT και του φορέα ESET Management, η θύρα 443 είναι η θύρα ανακατεύθυνσης.
TCP	3128	Επικοινωνία με το ESET Bridge (Διακομιστής μεσολάβησης HTTP)
TCP	443	Επικοινωνία με το ESET LiveGuard Advanced (μόνο με το διακομιστή μεσολάβησης)

Φορέας ESET Management - θύρες που χρησιμοποιούνται για απομακρυσμένη ανάπτυξη σε έναν υπολογιστή προορισμού με λειτουργικό σύστημα Windows

Πρωτόκολλο	Θύρα	Περιγραφές
TCP	139	Χρήση του κοινόχρηστου πόρου ADMIN$
TCP	445	Απευθείας πρόσβαση στους κοινόχρηστους πόρους χρησιμοποιώντας TCP/IP κατά την απομακρυσμένη εγκατάσταση (μια εναλλακτική στο TCP 139)
UDP	137	Επίλυση ονόματος κατά την απομακρυσμένη εγκατάσταση
UDP	138	Αναζήτηση κατά την απομακρυσμένη εγκατάσταση

Υπολογιστής κονσόλας διαδικτύου ESET PROTECT (εάν δεν είναι ίδιος με τον υπολογιστή διακομιστή ESET PROTECT)

Πρωτόκολλο	Θύρα	Περιγραφές
TCP	2223	Επικοινωνία μεταξύ της κονσόλας διαδικτύου ESET PROTECT και του διακομιστή ESET PROTECT, χρησιμοποιείται για υποβοηθούμενη εγκατάσταση.
TCP	443/80	Εκπομπή της κονσόλας διαδικτύου από Tomcat.
TCP	443	Ροή RSS για ειδήσεις υποστήριξης: • https://era.welivesecurity.com:443 • https://support.eset.com:443/rss/news.xml

Υπολογιστής διακομιστή ESET PROTECT

Πρωτόκολλο	Θύρα	Περιγραφές
TCP	2222	Επικοινωνία μεταξύ του φορέα ESET Management και του διακομιστή ESET PROTECT
TCP	80	Σύνδεση με το αποθετήριο της ESET
MQTT	8883	Υπηρεσία ESET Push Notification Service - Κλήσεις αφύπνισης μεταξύ του διακομιστή ESET PROTECT και του φορέα ESET Management
TCP	2223	Επίλυση DNS και εναλλακτική MQTT
TCP	3128	Επικοινωνία με το ESET Bridge (Διακομιστής μεσολάβησης HTTP)
TCP	1433 (Microsoft SQL) 3306 (MySQL)	Σύνδεση με εξωτερική βάση δεδομένων (μόνο εάν η βάση δεδομένων βρίσκεται σε άλλον υπολογιστή).
TCP	389	Συγχρονισμός LDAP. Ανοίξτε αυτή τη θύρα και στον ελεγκτή AD.
UDP	88	Δελτία Kerberos (εφαρμόζεται μόνο για την εικονική συσκευή ESET PROTECT)

Αισθητήρας Rogue Detection (RD)

Πρωτόκολλο	Θύρα	Περιγραφές
TCP	22, 139	Ανίχνευση λειτουργικού συστήματος μέσω των πρωτοκόλλων SMB (TCP 139) και SSH (TCP 22).
UDP	137	Ανάλυση ονόματος κεντρικού υπολογιστή μέσω NetBIOS.

ESET PROTECT MDC machine

Πρωτόκολλο	Θύρα	Περιγραφές
TCP	9977 9978	**Εσωτερική** επικοινωνία μεταξύ της Σύνδεσης κινητών συσκευών και του φορέα ESET Management
TCP	9980	Εγγραφή κινητής συσκευής
TCP	9981	Επικοινωνία κινητών συσκευών
HTTPS	2197	Υπηρεσία Apple push notification και σχόλια (*api.push.apple.com*)
TCP	2222	Επικοινωνία (αντιγραφή) μεταξύ του φορέα ESET Management, του MDC και του διακομιστή ESET PROTECT
TCP	1433 (Microsoft SQL) 3306 (MySQL)	Σύνδεση με εξωτερική βάση δεδομένων (μόνο εάν η βάση δεδομένων βρίσκεται σε άλλον υπολογιστή)

Διαχειριζόμενη συσκευή MDM

Πρωτόκολλο	Θύρα	Περιγραφές
TCP	9980	Εγγραφή κινητής συσκευής
TCP	9981	Επικοινωνία κινητών συσκευών
TCP	5223	Εξωτερική επικοινωνία με την υπηρεσία Apple Push Notification (iOS)
TCP	443	• Μετάβαση σε Wi-Fi μόνο, όταν οι συσκευές δεν μπορούν να επικοινωνήσουν με τις υπηρεσίες APN στη θύρα 5223. (iOS) • Σύνδεση συσκευής Android σε διακομιστή GCM. • Σύνδεση με την πύλη αδειών χρήσης ESET. • ESET LiveGrid® (Android) (Εισερχόμενα: *https://i1.c.eset.com*, Εξερχόμενα: *https://i3.c.eset.com*) • Ανώνυμα στατιστικά στοιχεία προς το Εργαστήριο της ESET (Android) (*https://ts.eset.com*) • Κατηγοριοποίηση εφαρμογών που έχουν εγκατασταθεί στη συσκευή. Χρησιμοποιείται για το Application Control, εάν ορίστηκε αποκλεισμός ορισμένων κατηγοριών εφαρμογών. (Android) (*https://play.eset.com*) • Για αποστολή αίτησης υποστήριξης χρησιμοποιώντας τη λειτουργία «Αίτηση υποστήριξης» (Android) (*https://suppreq.eset.eu*)
TCP	5228 5229 5230	Αποστολή ειδοποιήσεων στην υπηρεσία Google Cloud Messaging (Android)* Αποστολή ειδοποιήσεων στην υπηρεσία Firebase Cloud Messaging (Android)*
TCP	80	• Ενημέρωση μονάδων (Android) (*http://update.eset.com*) • Χρησιμοποιείται μόνο στην έκδοση διαδικτύου. Πληροφορίες για την πιο πρόσφατη ενημέρωση έκδοσης εφαρμογής και λήψη μιας νέας έκδοσης. (Android) (*http://go.eset.eu*)

* Η υπηρεσία GCM (Google Cloud Messaging) αποσύρθηκε και καταργήθηκε από τις 11 Απριλίου 2019. Αντικαταστάθηκε από την υπηρεσία FCM (Firebase Cloud Messaging). Το MDM v7 αντικατέστησε την υπηρεσία GCM με την υπηρεσία FCM μέχρι εκείνη την ημερομηνία, οπότε χρειάζεται μόνο να επιτρέψετε την επικοινωνία για την υπηρεσία FCM.

Οι προκαθορισμένες θύρες 2222, 2223 μπορούν να αλλάξουν, εάν απαιτηθεί.

Διαδικασία εγκατάστασης

Ο οδηγός εγκατάστασης καλύπτει πολλούς τρόπους με τους οποίους μπορείτε να εγκαταστήσετε το ESET PROTECT On-Prem και προορίζεται γενικά για εταιρικούς πελάτες. Ανατρέξτε στο θέμα Εγκατάσταση «όλα σε ένα», εάν θέλετε να εγκαταστήσετε το ESET PROTECT On-Prem σε πλατφόρμα Windows για να διαχειρίζεστε μέχρι και 250 προϊόντα ESET Endpoint για Windows.
Για οδηγίες σχετικά με την αναβάθμιση της υπάρχουσας εγκατάστασης ESET PROTECT On-Prem, δείτε τις Διαδικασίες αναβάθμισης.

Τα προγράμματα εγκατάστασης ESET PROTECT διατίθενται στην ενότητα Λήψη του ESET PROTECT στον ιστότοπο της ESET. Διατίθενται σε διάφορες μορφές ώστε να υποστηρίζουν διαφορετικές μεθόδους εγκατάστασης. Από προεπιλογή, είναι επιλεγμένη η καρτέλα **Πρόγραμμα εγκατάστασης "όλα σε ένα"**. Κάντε κλικ στην κατάλληλη καρτέλα για να λάβετε ένα VA ή ένα ανεξάρτητο πρόγραμμα εγκατάστασης. Είναι διαθέσιμα τα παρακάτω στοιχεία λήψης:

- Το πακέτο προγραμμάτων εγκατάστασης «όλα-σε-ένα» ESET PROTECT On-Prem για Windows σε μορφή zip.
- Ένα είδωλο ISO που περιέχει όλα τα προγράμματα εγκατάστασης του ESET PROTECT (εκτός από τις εικονικές συσκευές ESET PROTECT).
- Των εικονικών συσκευών (αρχεία OVA). Η ανάπτυξη της εικονικής συσκευής ESET PROTECT συνιστάται για χρήστες που θέλουν να εκτελούν το ESET PROTECT On-Prem σε εικονικό περιβάλλον ή προτιμούν μια πιο απλή εγκατάσταση. Δείτε τον πλήρη οδηγό ανάπτυξης εικονικής συσκευής ESET PROTECT, για οδηγίες βήμα προς βήμα.
- Ξεχωριστά προγράμματα εγκατάστασης για κάθε στοιχείο για τις πλατφόρμες Windows και Linux.

Πρόσθετες μέθοδοι εγκατάστασης:

- Αναλυτικές οδηγίες εγκατάστασης για Linux

Από τον Νοέμβριο του 2022, η εταιρεία δεν παρέχει την Εικονική συσκευή ESET PROTECT στο Azure Marketplace. Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το ESET PROTECT (cloud) και να επιτρέπετε στην ESET να διαχειρίζεται όλα τα απαιτούμενα στοιχεία υποδομής.

Μην αλλάζετε το Όνομα υπολογιστή για τον υπολογιστή του διακομιστή ESET PROTECT μετά την εγκατάσταση. Ανατρέξτε στο θέμα Αλλαγή διεύθυνσης IP ή ονόματος κεντρικού υπολογιστή στο διακομιστή ESET PROTECT για περισσότερες πληροφορίες.

Εάν θέλετε να αποφασίσετε το είδος εγκατάστασης του ESET PROTECT On-Prem που είναι κατάλληλο για το περιβάλλον σας, δείτε τον ακόλουθο πίνακα λήψης απόφασης, ο οποίος θα σας καθοδηγήσει στην καλύτερη επιλογή: Για παράδειγμα:

- Μη χρησιμοποιείτε αργή σύνδεση Internet για το ESET PROTECT On-Prem στο cloud.
- Επιλέξτε ένα πρόγραμμα εγκατάστασης "όλα σε ένα", εάν είστε πελάτης SMB.

Δείτε επίσης το θέμα Διαμόρφωση μεγέθους υλικού και υποδομής. Μπορείτε να εγκαταστήσετε το ESET PROTECT On-Prem σε φυσικούς ή εικονικούς υπολογιστές.

Μέθοδος εγκατάστασης	Τύπος πελάτη		Μετεγκατάσταση		Περιβάλλον για εγκατάσταση ESET PROTECT On-Prem					Σύνδεση Internet		
	SMB	Εταιρικό	Ναι	Όχι	Χωρίς διακομιστή	Αποκλειστικός διακομιστής	Κοινόχρηστος διακομιστής	Πλατφόρμα εικονικού περιβάλλοντος	Διακομιστής cloud	Καμιά	Καλή	Κακή
"Όλα σε ένα" ενεργό Διακομιστής Windows	✔	✔	✔			✔	✔		✔	✔	✔	✔
"Όλα σε ένα" ενεργό Επιφάνεια εργασίας Windows	✔		✔		✔					✔	✔	✔
Εικονική συσκευή	✔		✔					✔		✔	✔	✔
Στοιχείο Linux		✔	✔			✔	✔		✔	✔	✔	✔
Στοιχείο Windows		✔	✔			✔	✔		✔	✔	✔	✔

Εγκατάσταση όλα-σε-ένα στα Windows

Μπορείτε να εγκαταστήσετε το ESET PROTECT On-Prem με αρκετούς τρόπους. Επιλέξτε τον τύπο εγκατάστασης που ταιριάζει καλύτερα στις ανάγκες και στο περιβάλλον σας. Η πιο απλή μέθοδος είναι να χρησιμοποιήσετε το πρόγραμμα εγκατάστασης «όλα-σε-ένα» του ESET PROTECT. Αυτή η μέθοδος σάς επιτρέπει να εγκαταστήσετε το ESET PROTECT On-Prem και τα στοιχεία του σε έναν μοναδικό υπολογιστή.

Η εγκατάσταση του στοιχείου σάς επιτρέπει να προσαρμόσετε την εγκατάσταση και να εγκαταστήσετε κάθε στοιχείο του ESET PROTECT σε ξεχωριστό υπολογιστή, υπό την προϋπόθεση ότι πληροί τις απαιτήσεις του συστήματος.

Μπορείτε να εγκαταστήσετε το ESET PROTECT On-Prem χρησιμοποιώντας:

- Την εγκατάσταση πακέτου «όλα-σε-ένα» του Διακομιστή ESET PROTECT, του ESET BridgeΔιακομιστή μεσολάβησης HTTP ή της Σύνδεσης κινητών συσκευών
- Ανεξάρτητα προγράμματα εγκατάστασης για στοιχεία ESET PROTECT (εγκατάσταση στοιχείων)

Τα προσαρμοσμένα σενάρια εγκατάστασης περιλαμβάνουν:

- Εγκατάσταση με προσαρμοσμένα πιστοποιητικά
- Εγκατάσταση σε σύμπλεγμα ανακατεύθυνσης

Για πολλά σενάρια εγκατάστασης, πρέπει να εγκαταστήσετε διαφορετικά στοιχεία του ESET PROTECT σε διαφορετικούς υπολογιστές ώστε να εξυπηρετούνται οι αρχιτεκτονικές δικτύου, να ικανοποιούνται οι απαιτήσεις επιδόσεων ή για άλλους λόγους. Για μεμονωμένα στοιχεία του ESET PROTECT, υπάρχουν διαθέσιμα τα ακόλουθα πακέτα εγκατάστασης:

Εγκατάσταση βασικών στοιχείων:

- ESET PROTECTΔιακομιστής
- Κονσόλα διαδικτύου ESET PROTECT – Μπορείτε να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT σε έναν διαφορετικό υπολογιστή από τον υπολογιστή στον οποίο εκτελείται ο διακομιστής ESET PROTECT.
- Ο φορέας ESET Management (πρέπει να εγκατασταθεί σε υπολογιστές-πελάτες, προαιρετικά στο διακομιστή ESET PROTECT)

Εγκατάσταση προαιρετικών στοιχείων:

- Αισθητήρας RD
- Σύνδεση κινητών συσκευών
- ESET Bridge Διακομιστής Μεσολάβησης HTTP
- Εργαλείο ειδώλου

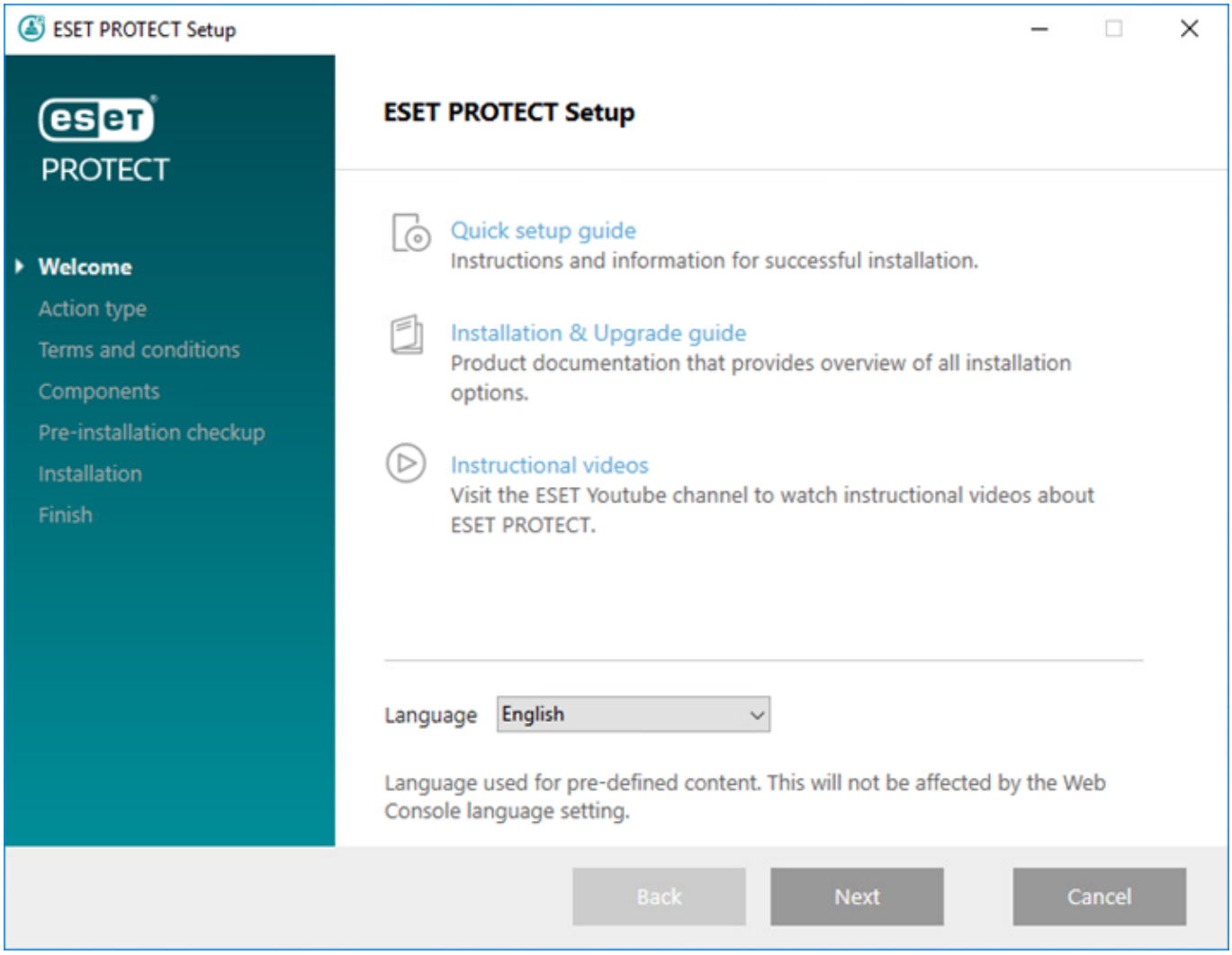
Δείτε επίσης το θέμα Εγκατάσταση όλα σε ένα του ESET PROTECT.

Για οδηγίες σχετικά με την αναβάθμιση παλαιότερης έκδοσης του ESET PROTECT On-Prem στην πιο πρόσφατη έκδοση του ESET PROTECT On-Prem 11.0, ανατρέξτε στο θέμα διαδικασίες αναβάθμισης.

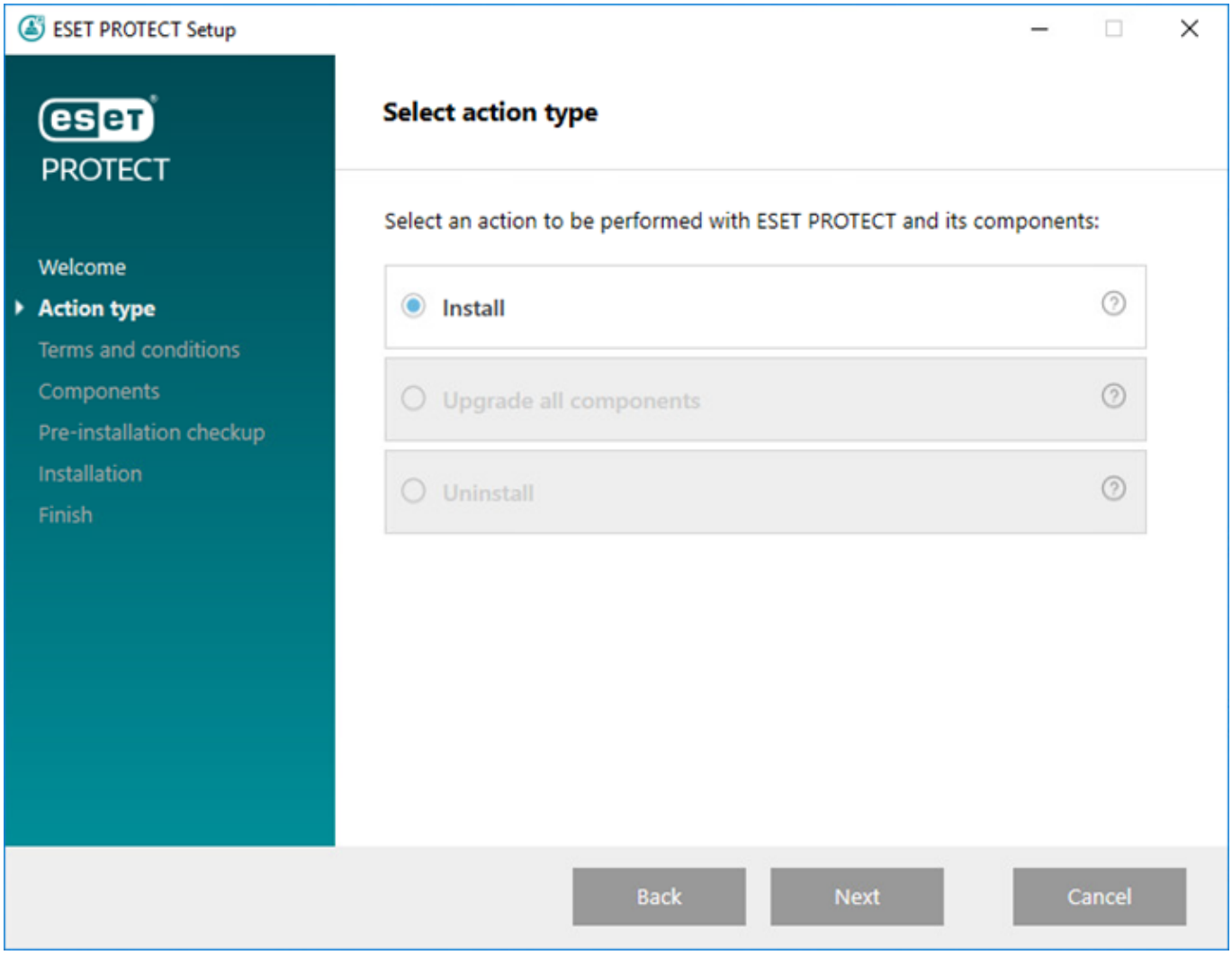
Εγκατάσταση του διακομιστή ESET PROTECT

Το πρόγραμμα εγκατάστασης ESET PROTECT «όλα-σε-ένα» είναι διαθέσιμο μόνο για λειτουργικά συστήματα Windows. Το πρόγραμμα εγκατάστασης «Όλα σε ένα» επιτρέπει την εγκατάσταση όλων των στοιχείων του ESET PROTECT χρησιμοποιώντας τον οδηγό εγκατάστασης του ESET PROTECT On-Prem.

1. Ανοίξτε το πακέτο εγκατάστασης. Στην οθόνη υποδοχής, χρησιμοποιήστε το αναπτυσσόμενο μενού **Γλώσσα** για να αλλάξετε τις ρυθμίσεις γλώσσας. Κάντε κλικ στο στοιχείο **Επόμενο** για να προχωρήσετε.



2. Επιλέξτε **Εγκατάσταση** και κάντε κλικ στο στοιχείο **Επόμενο**.



3. Επιλέξτε το πλαίσιο ελέγχου **Συμμετοχή στο πρόγραμμα βελτίωσης προϊόντος**, για να αποστέλλονται ανώνυμα δεδομένα τηλεμετρίας και αναφορές σφαλμάτων στην ESET (έκδοση και τύπος λειτουργικού συστήματος, έκδοση προϊόντος ESET και άλλες πληροφορίες ειδικά για το προϊόν). Αφού αποδεχτείτε την Άδεια Χρήσης Τελικού Χρήστη (EULA), επιλέξτε **Επόμενο**.

4. Επιλέξτε τα στοιχεία που θέλετε να εγκαταστήσετε και κάντε κλικ στο στοιχείο **Επόμενο**.

Microsoft SQL Server Express

- ESET PROTECT On-Prem 11.0 Το πρόγραμμα εγκατάστασης «όλα σε ένα» εγκαθιστά το Microsoft SQL Server Express 2019 από προεπιλογή.
oΕάν χρησιμοποιείτε μια παλαιότερη έκδοση των Windows (Server 2012 ή SBS 2011), το Microsoft SQL Server Express 2014 θα εγκατασταθεί από προεπιλογή.
oΤο πρόγραμμα εγκατάστασης δημιουργεί αυτόματα έναν τυχαίο κωδικό πρόσβασης για τον έλεγχο ταυτότητας της βάσης δεδομένων (που είναι αποθηκευμένη στη διαδρομή *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

> ⚠ Το Microsoft SQL Server Express έχει όριο μεγέθους 10 GB για κάθε σχετική βάση δεδομένων. Δεν συνιστάται η χρήση του Microsoft SQL Server Express:
> - Σε εταιρικά περιβάλλοντα ή μεγάλα δίκτυα.
> - Εάν θέλετε να χρησιμοποιήσετε το ESET PROTECT On-Prem με το ESET Inspect On-Prem.

- Εάν έχετε ήδη μια άλλη υποστηριζόμενη έκδοση του Microsoft SQL Server ή του MySQL εγκατεστημένη ή εάν σχεδιάζετε να συνδεθείτε σε διαφορετικό διακομιστή SQL Server, καταργήστε την επιλογή του πλαισίου ελέγχου δίπλα στο **Microsoft SQL Server Express**.
- Μην εγκαταστήσετε το SQL Server σε έναν Ελεγκτή τομέα (για παράδειγμα, Windows SBS / Essentials).

Συνιστάται να εγκαταστήσετε το ESET PROTECT On-Prem σε διαφορετικό διακομιστή ή να μην επιλέξετε το στοιχείο του SQL Server Express κατά την εγκατάσταση (αυτό απαιτεί να χρησιμοποιήσετε το υπάρχον SQL ή MySQL Server για την εκτέλεση της βάσης δεδομένων ESET PROTECT).

Προσθήκη προσαρμοσμένου πιστοποιητικού HTTPS για την Κονσόλα διαδικτύου

- Επιλέξτε αυτό το στοιχείο εάν θέλετε να χρησιμοποιήσετε προσαρμοσμένο πιστοποιητικό HTTPS για την Κονσόλα διαδικτύου ESET PROTECT.
- Εάν δεν ορίσετε αυτήν την επιλογή, το πρόγραμμα εγκατάστασης δημιουργεί αυτόματα ένα νέο αρχείο κλειδιών για το Tomcat (ένα πιστοποιητικό HTTPS αυτο-υπογραφής).

ESET Bridge Διακομιστής μεσολάβησης

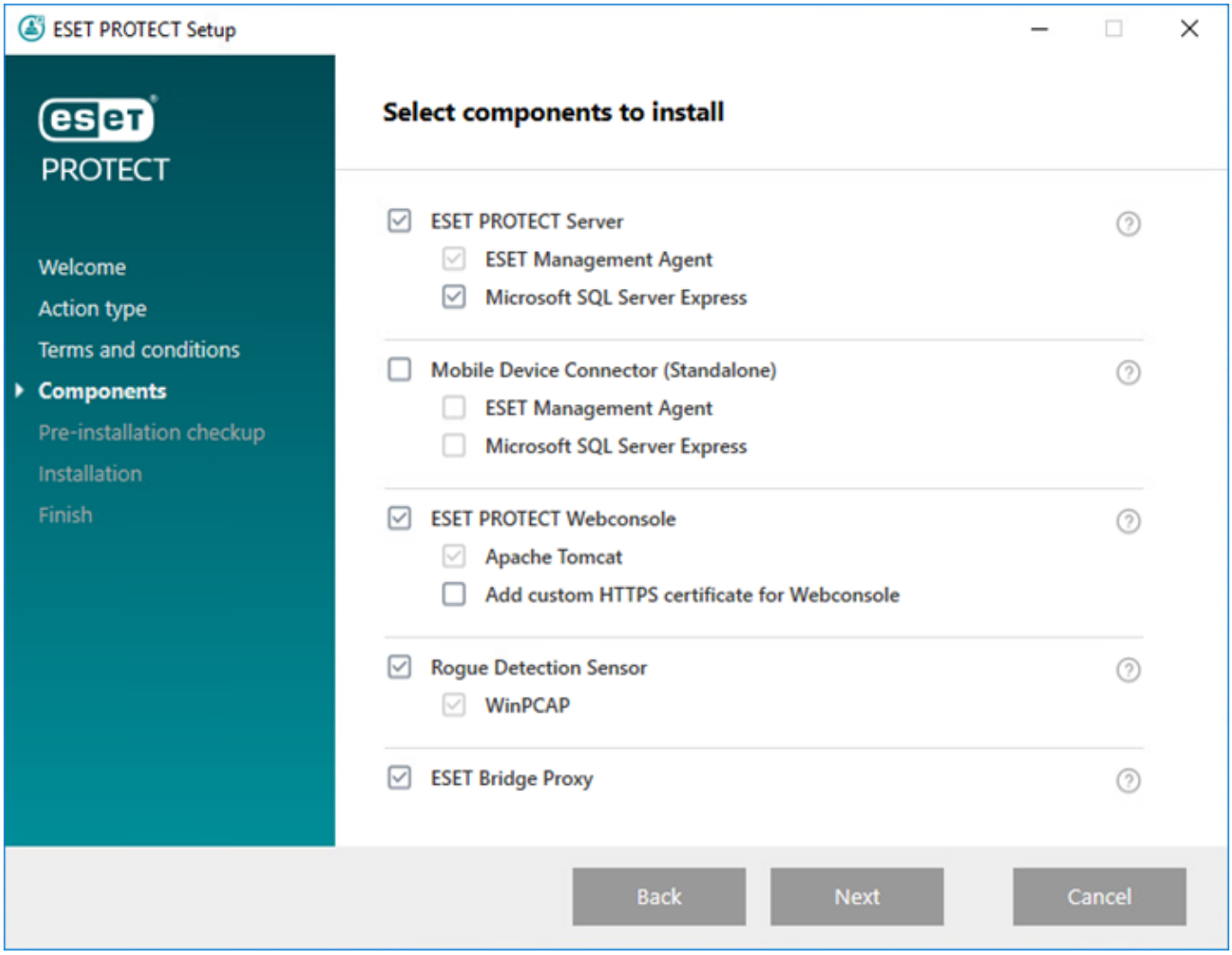
Η επιλογή **ESET Bridge Διακομιστής μεσολάβησης** προορίζεται μόνο για μικρότερα ή κεντρικά δίκτυα, χωρίς προγράμματα-πελάτη περιαγωγής. Εάν οριστεί αυτή η επιλογή, το πρόγραμμα εγκατάστασης ρυθμίζει τις παραμέτρους των υπολογιστών-πελατών για να διοχετεύεται η επικοινωνία με την ESET μέσω του διακομιστή μεσολάβησης που έχει εγκατασταθεί στον ίδιο υπολογιστή με το Διακομιστή ESET PROTECT. Αυτή η σύνδεση δεν θα λειτουργεί εάν δεν υπάρχει απευθείας ορατότητα δικτύου μεταξύ των υπολογιστών-πελατών και του διακομιστή ESET PROTECT.

- Η χρήση διακομιστή μεσολάβησης HTTP μπορεί να εξοικονομήσει μεγάλο εύρος ζώνης για δεδομένα που λαμβάνονται από το Internet και να βελτιώσει τις ταχύτητες λήψης για τις ενημερώσεις προϊόντος. Συνιστάται να επιλέξετε το πλαίσιο ελέγχου δίπλα στο **ESET Bridge διακομιστή μεσολάβησης**, εάν θέλετε να διαχειρίζεστε περισσότερους από 37 υπολογιστές μέσω του ESET PROTECT On-Prem. Μπορείτε επίσης να επιλέξετε να εγκαταστήσετε το ESET Bridge αργότερα.
- Για περισσότερες πληροφορίες, ανατρέξτε στις ενότητες ESET Bridge (Διακομιστής μεσολάβησης HTTP) και Διαφορές μεταξύ του ESET Bridge (Διακομιστής μεσολάβησης HTTP), του εργαλείου ειδώλου και της απευθείας συνδεσιμότητας.

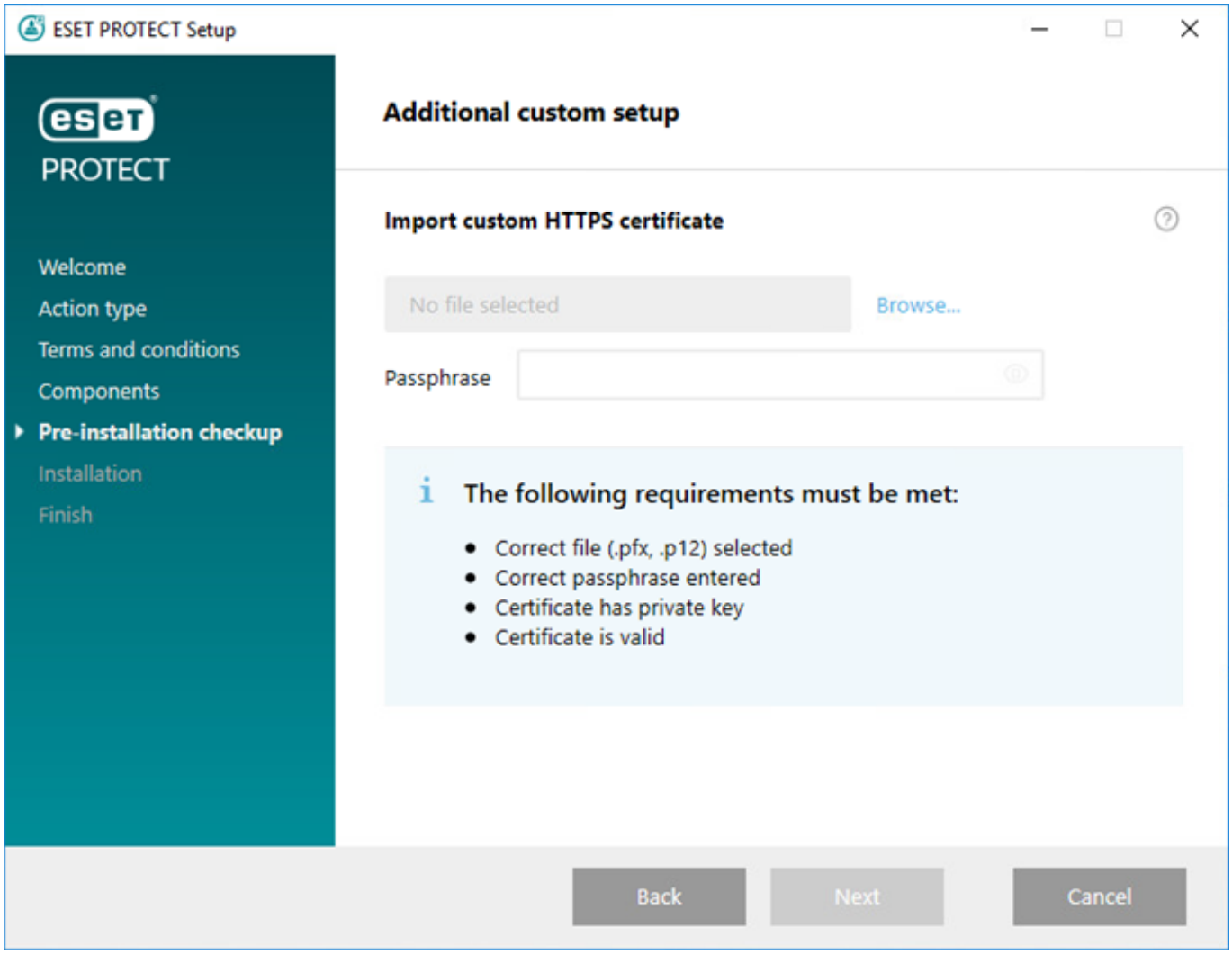
Το πρόγραμμα εγκατάστασης «όλα σε ένα» δημιουργεί προεπιλεγμένες πολιτικές για τη **Χρήση HTTP Proxy** για τον Φορέα ESET Management και τα προϊόντα ασφάλειας ESET που εφαρμόζονται στην στατική ομάδα **Όλα**. Οι πολιτικές ρυθμίζουν αυτόματα τις παραμέτρους των Φορέων ESET Management και των προϊόντων ασφάλειας ESET σε διαχειριζόμενους υπολογιστές ώστε να χρησιμοποιούν το ESET Bridge ως διακομιστή μεσολάβησης για την προσωρινή αποθήκευση πακέτων ενημερώσεων. Η προσωρινή αποθήκευση της κυκλοφορίας HTTPS είναι ενεργοποιημένη από προεπιλογή:

- Η πολιτική του ESET Bridge περιέχει το πιστοποιητικό HTTPS και το πλήκτρο εναλλαγής **Προσωρινή αποθήκευση της κυκλοφορίας HTTPS** είναι ενεργό.
- Η πολιτική **Χρήση** του **HTTP Proxy** για το ESET Endpoint για Windows περιέχει την Αρχή έκδοσης πιστοποιητικών για την προσωρινή αποθήκευση κυκλοφορίας HTTPS.

Ο κεντρικός υπολογιστής διακομιστή μεσολάβησης HTTP είναι η τοπική διεύθυνση IP του διακομιστή ESET PROTECT και η θύρα 3128. Ο έλεγχος ταυτότητας είναι απενεργοποιημένος. Μπορείτε να αντιγράψετε αυτές τις ρυθμίσεις σε άλλη πολιτική, αν θέλετε να ρυθμίσετε επιπλέον προϊόντα.



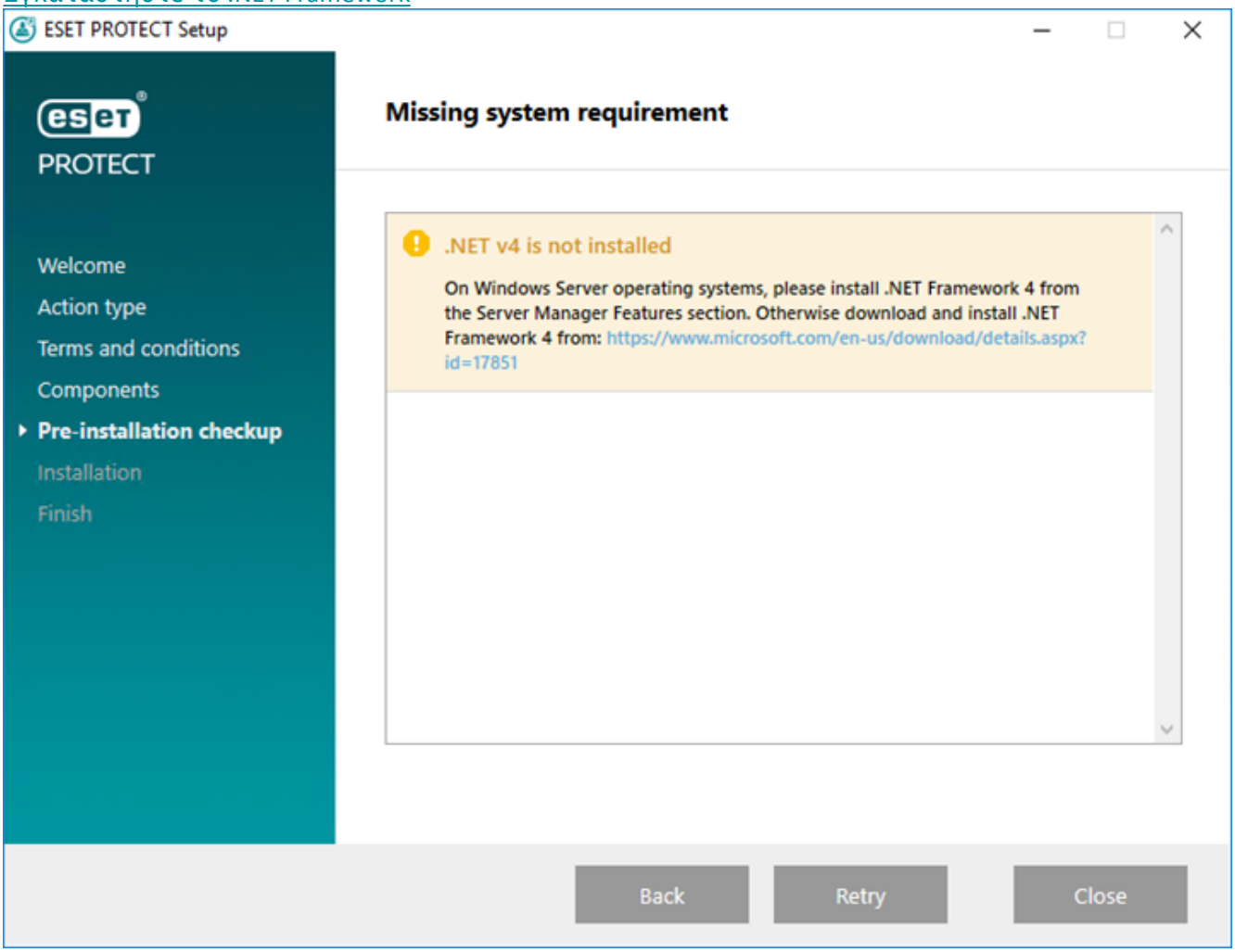
5. Εάν επιλέξετε **Προσθήκη προσαρμοσμένου πιστοποιητικού HTTPS για την Κονσόλα διαδικτύου**, κάντε κλικ στο στοιχείο **Αναζήτηση** και επιλέξτε ένα έγκυρο πιστοποιητικό (αρχείο *.pfx* ή .p12) και συμπληρώστε το πεδίο **Κωδικός πρόσβασης** (ή αφήστε το πεδίο κενό εάν δεν υπάρχει κωδικός πρόσβασης). Το πρόγραμμα εγκατάστασης θα εγκαταστήσει το πιστοποιητικό για πρόσβαση στην Κονσόλα διαδικτύου στο διακομιστή Tomcat. Κάντε κλικ στο στοιχείο **Επόμενο** για να συνεχίσετε.



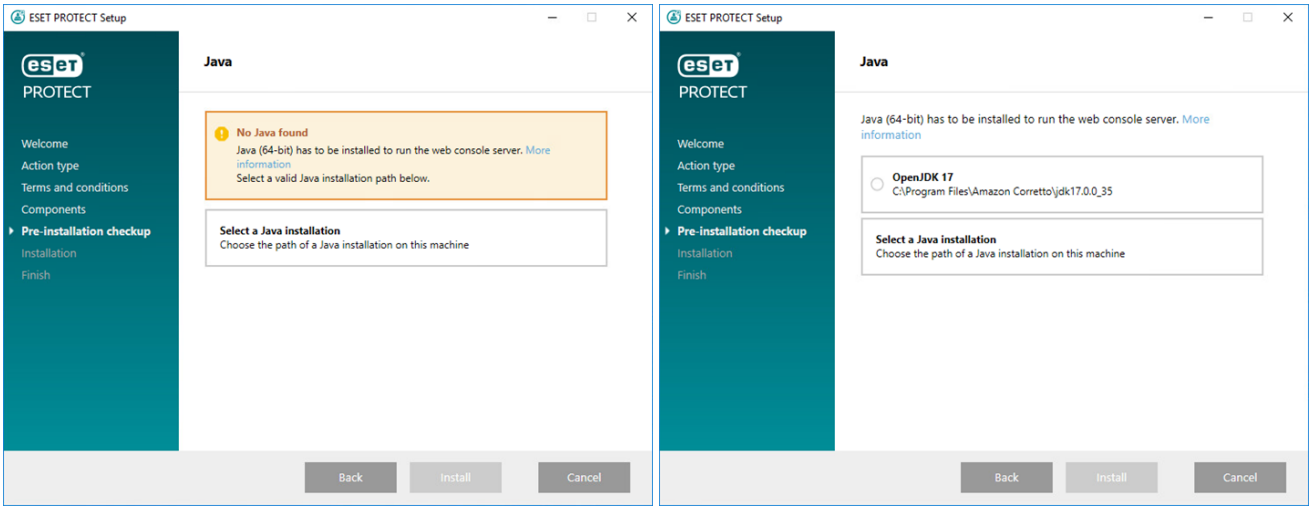
6. Εάν βρεθούν σφάλματα κατά τον έλεγχο προαπαιτούμενων, αντιμετωπίστε τα καταλλήλως. Βεβαιωθείτε ότι το σύστημά σας πληροί όλα τα προαπαιτούμενα.

Το .NET v4 δεν έχει εγκατασταθεί

Εγκαταστήστε το .NET Framework



Δεν βρέθηκε εγκατάσταση Java / Ανιχνεύτηκε Java (64-bit)



Εάν έχετε πολλαπλές εκδόσεις Java εγκατεστημένες στο σύστημά σας, συνιστάται να καταργήσετε την εγκατάσταση των παλαιότερων εκδόσεων Java και να διατηρήσετε μόνο την πιο πρόσφατη υποστηριζόμενη έκδοση Java.

> Από τον Ιανουάριο 2019, οι δημόσιες ενημερώσεις Oracle JAVA SE 8 για επιχειρηματική, εμπορική ή παραγωγική χρήση, απαιτούν εμπορική άδεια χρήσης. Εάν δεν αγοράσετε συνδρομή JAVA SE, μπορείτε να χρησιμοποιήσετε αυτό τον οδηγό για μετάβαση σε μια εναλλακτική λύση χωρίς κόστος. Δείτε τις υποστηριζόμενες εκδόσεις του JDK.

a)Για να επιλέξετε το ήδη εγκατεστημένο Java, κάντε κλικ στο στοιχείο **Επιλογή μιας εγκατάστασης Java**, επιλέξτε το φάκελο στον οποίο είναι εγκατεστημένο το Java (με έναν υποφάκελο *bin*, για παράδειγμα *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) και κάντε κλικ στο **OK**. Το πρόγραμμα εγκατάστασης θα σας ρωτήσει εάν έχετε επιλέξει μη έγκυρη διαδρομή.
b)Κάντε κλικ στο στοιχείο **Εγκατάσταση** για να συνεχίσετε ή **αλλαγή** για να αλλάξετε τη διαδρομή εγκατάστασης Java.

Οι ρυθμίσεις δεν είναι σε έγκυρη κατάσταση/Microsoft SQL Server Express

Το πρόγραμμα εγκατάστασης μπορεί να εμφανίσει αυτή την ειδοποίηση για διάφορους λόγους:
- Το πρόγραμμα εγκατάστασης είναι κατεστραμμένο. Για παράδειγμα, λείπουν ορισμένα αρχεία του προγράμματος εγκατάστασης. Πραγματοποιήστε λήψη και εκτέλεση του προγράμματος εγκατάστασης «όλα σε ένα» ξανά.
- Η διαδρομή προς το πρόγραμμα εγκατάστασης «όλα σε ένα» περιέχει ειδικούς χαρακτήρες – για παράδειγμα, γράμματα με ορθογραφικά σημάδια. Εκτελέστε το πρόγραμμα εγκατάστασης «όλα σε ένα» του ESET PROTECT από μια διαδρομή χωρίς ειδικούς χαρακτήρες.

Υπάρχουν μόνο 32 MB ελεύθερα στο δίσκο συστήματος

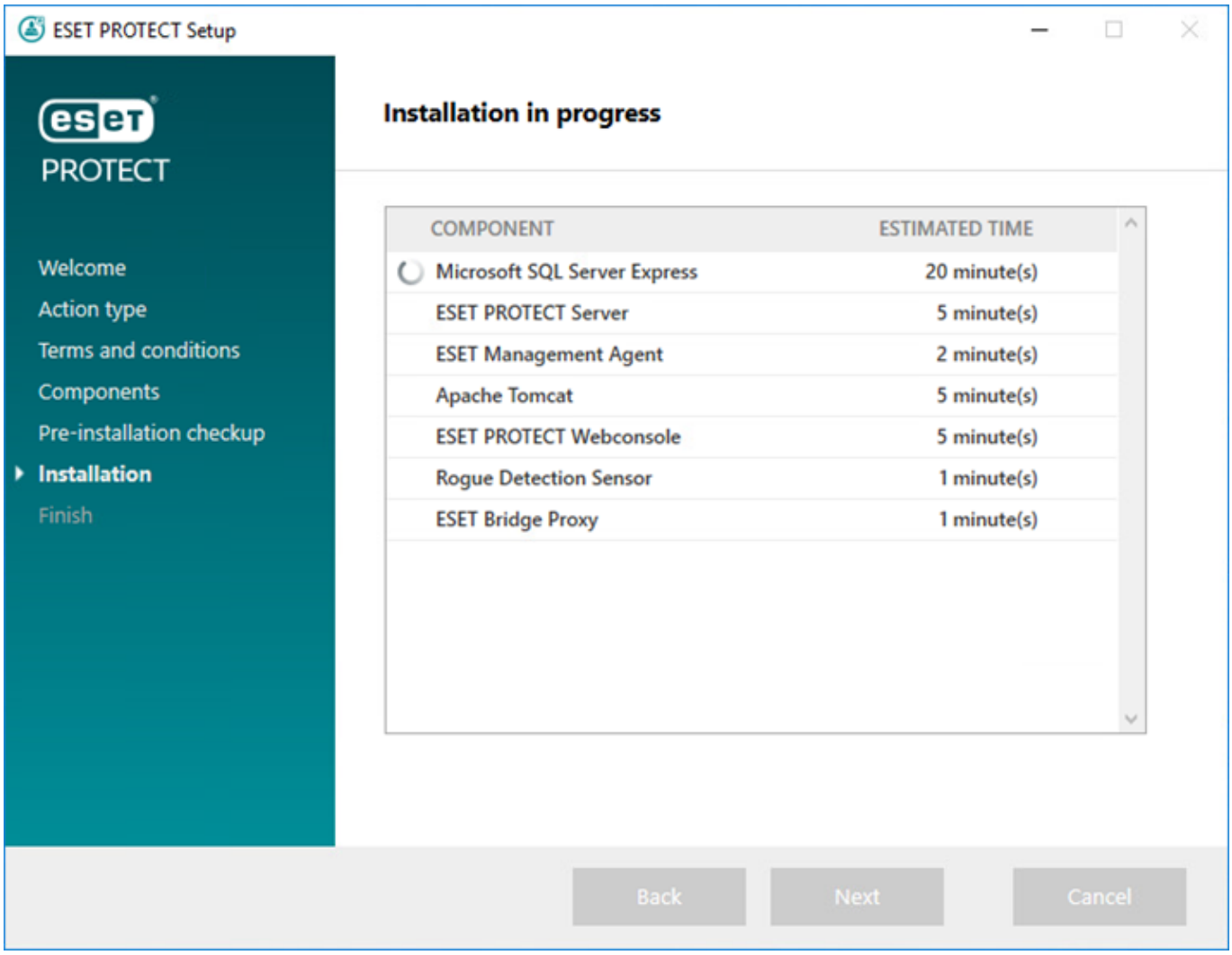
Το πρόγραμμα εγκατάστασης ενδέχεται να εμφανίσει αυτή την ειδοποίηση, εάν το σύστημά σας δεν έχει αρκετό χώρο στο δίσκο για την εγκατάσταση του ESET PROTECT On-Prem.
Για να εγκαταστήσετε το ESET PROTECT On-Prem και όλα τα στοιχεία του, πρέπει να έχετε τουλάχιστον 4.400 MB ελεύθερου χώρου στο δίσκο.

Έχει εγκατασταθεί στον υπολογιστή το ESET Remote Administrator 5.x ή παλαιότερη έκδοση, η οποία δεν επιτρέπει στο πρόγραμμα εγκατάστασης να συνεχίσει.

Μπορείτε να αναβαθμίσετε σε ESET PROTECT On-Prem 11.0 από ESET PROTECT On-Prem 9.0 και νεότερες εκδόσεις. Η απευθείας αναβάθμιση από τις εκδόσεις τέλους του κύκλου ζωής 7.2–8.x δεν έχει δοκιμαστεί και δεν υποστηρίζεται.
Εάν έχετε το ERA 5.x/6.x ή το ESMC 7.0/7.1, η άμεση αναβάθμιση σε ESET PROTECT On-Prem 11.0 δεν υποστηρίζεται – Εκτελέστε μια καθαρή εγκατάσταση του ESET PROTECT On-Prem 11.0.

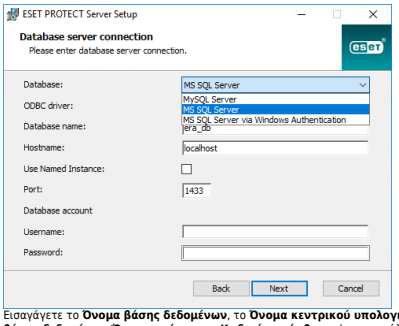
7. Όταν ολοκληρωθεί ο έλεγχος προαπαιτούμενων και το περιβάλλον σας ικανοποιεί όλες τις απαιτήσεις, θα ξεκινήσει η εγκατάσταση. Έχετε υπόψη ότι η εγκατάσταση μπορεί να διαρκέσει πάνω από μία ώρα, ανάλογα με το σύστημά σας και τη ρύθμιση παραμέτρων του δικτύου.

Όταν η εγκατάσταση βρίσκεται σε εξέλιξη, ο Οδηγός εγκατάστασης ESET PROTECT On-Prem δεν ανταποκρίνεται.



8. Εάν επιλέξατε να εγκαταστήσετε το **Microsoft SQL Server Express** στο βήμα 4, το πρόγραμμα εγκατάστασης θα εκτελέσει έναν έλεγχο σύνδεσης βάσης δεδομένων. Εάν έχετε έναν υπάρχοντα διακομιστή βάσης δεδομένων, το πρόγραμμα εγκατάστασης θα σας ζητήσει να εισαγάγετε τα στοιχεία σύνδεσης της βάσης δεδομένων σας:

Ρύθμιση παραμέτρων της σύνδεσης με το SQL/MySQL Server

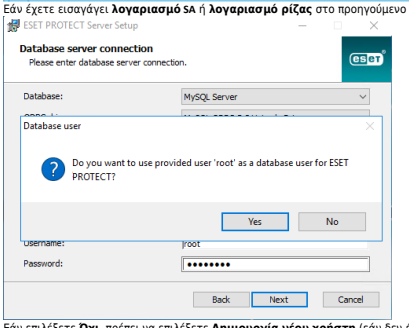


Εισαγάγετε το **Όνομα βάσης δεδομένων**, το **Όνομα κεντρικού υπολογιστή**, τον αριθμό **Θύρας** (μπορείτε να βρείτε αυτές τις πληροφορίες στη Διαχείριση διαμόρφωσης του Microsoft SQL Server) και τα στοιχεία του **Λογαριασμού διαχειριστή της βάσης δεδομένων** (**Όνομα χρήστη** και **Κωδικός πρόσβασης**) στα κατάλληλα πεδία και κατόπιν κάντε κλικ στο κουμπί **Επόμενο**. Το πρόγραμμα εγκατάστασης θα επαληθεύσει τη σύνδεση της βάσης δεδομένων. Εάν έχετε μια υπάρχουσα βάση δεδομένων (από προηγούμενη εγκατάσταση του ESET PROTECT On-Prem) στο διακομιστή βάσης δεδομένων σας, θα ανιχνευτεί. Μπορείτε να επιλέξετε **Χρήση της υπάρχουσας βάσης δεδομένων και εφαρμογή αναβάθμισης** ή **Κατάργηση της υπάρχουσας βάσης δεδομένων και εγκατάσταση νέας έκδοσης**.

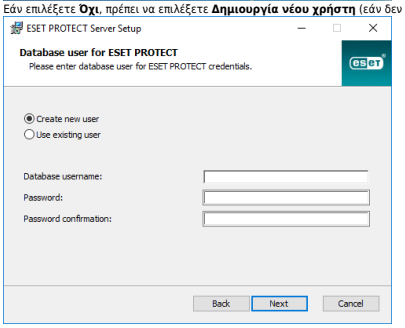
Χρήση ονόματος παρουσίας - Εάν χρησιμοποιείτε βάση δεδομένων Microsoft SQL, μπορείτε να επιλέξετε το πλαίσιο ελέγχου **Χρήση ονόματος παρουσίας** για να χρησιμοποιήσετε μια προσαρμοσμένη παρουσία βάσης δεδομένων. Μπορείτε να τη ρυθμίσετε στο πεδίο **Όνομα κεντρικού υπολογιστή** με τη μορφή *HOSTNAME\DB_INSTANCE* (για παράδειγμα, *192.168.0.10\ESMC7SQL*. Για βάση δεδομένων σε σύμπλεγμα, χρησιμοποιήστε μόνο το όνομα συμπλέγματος. Εάν ορίσετε αυτήν την επιλογή, δεν μπορείτε να αλλάξετε τη θύρα σύνδεσης της βάσης δεδομένων - το σύστημα θα χρησιμοποιεί τις προεπιλεγμένες θύρες που προσδιορίζονται από την Microsoft. Για να συνδέσετε τον Διακομιστή ESET PROTECT με τη βάση δεδομένων Microsoft SQL που είναι εγκατεστημένη σε ένα σύμπλεγμα ανακατεύθυνσης, εισαγάγετε το όνομα συμπλέγματος στο πεδίο **Όνομα κεντρικού υπολογιστή**.

> Υπάρχουν δυο επιλογές κατά την εισαγωγή των πληροφοριών για το **Λογαριασμό βάσης δεδομένων**. Μπορείτε να χρησιμοποιήσετε έναν **αποκλειστικό λογαριασμό χρήστη βάσης δεδομένων** που θα έχει πρόσβαση μόνο στη βάση δεδομένων ESET PROTECT ή μπορείτε να χρησιμοποιήσετε **Λογαριασμό SA** (Microsoft SQL) ή **λογαριασμό ρίζας** (MySQL). Εάν αποφασίσετε να χρησιμοποιήσετε αποκλειστικό λογαριασμό χρήστη, θα χρειαστεί να δημιουργήσετε αυτόν το λογαριασμό με συγκεκριμένα δικαιώματα. Για λεπτομέρειες, ανατρέξτε στο θέμα Αποκλειστικός λογαριασμός χρήστη βάσης δεδομένων. Εάν δεν σκοπεύετε να χρησιμοποιήσετε αποκλειστικό λογαριασμό χρήστη, εισαγάγετε το λογαριασμό διαχειριστή (SA ή λογαριασμό ρίζας).

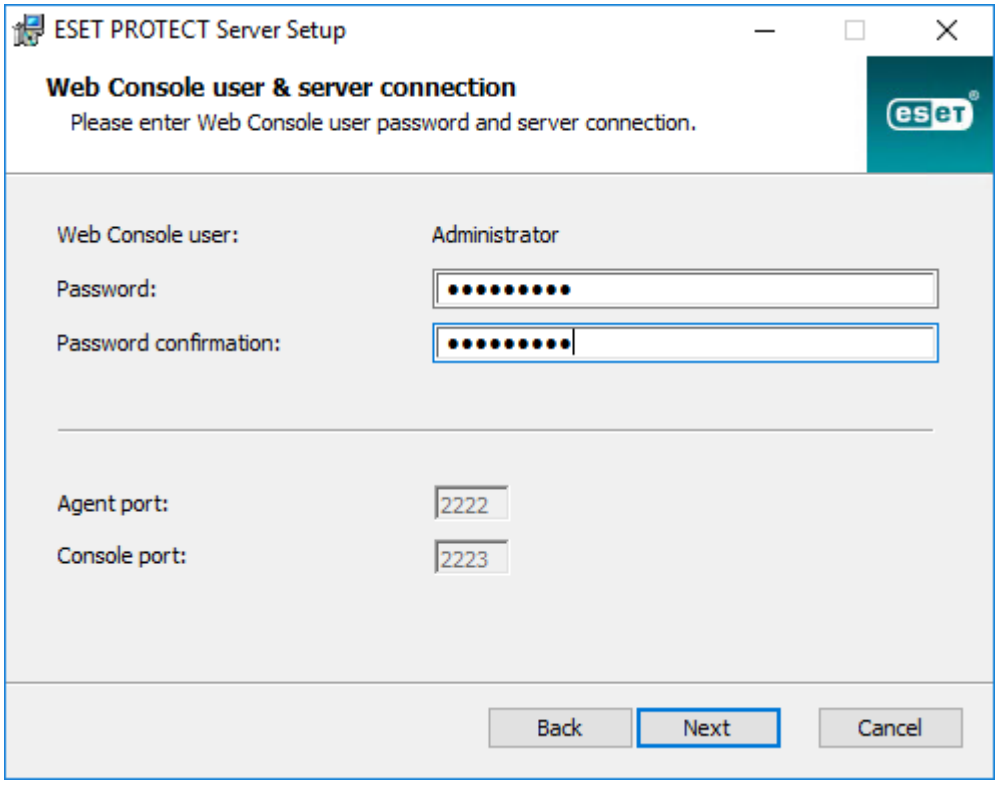
Εάν έχετε εισαγάγει **λογαριασμό SA** ή **λογαριασμό ρίζας** στο προηγούμενο παράθυρο, επιλέξτε **Ναι** για να συνεχίσετε να χρησιμοποιείτε το λογαριασμό SA/ρίζας ως το χρήστη βάσης δεδομένων για το ESET PROTECT.



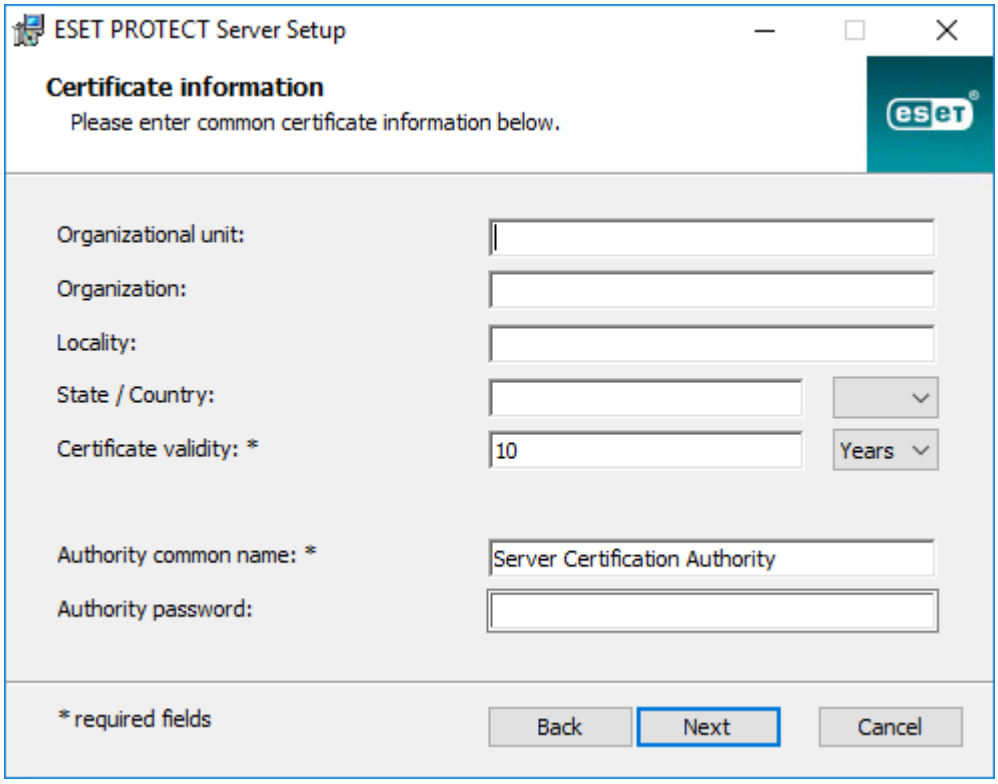
Εάν επιλέξετε **Όχι**, πρέπει να επιλέξετε **Δημιουργία νέου χρήστη** (εάν δεν έχετε ήδη δημιουργήσει) ή **Χρήση υπάρχοντος χρήστη** (εάν έχετε αποκλειστικό λογαριασμό χρήστη βάσης δεδομένων).



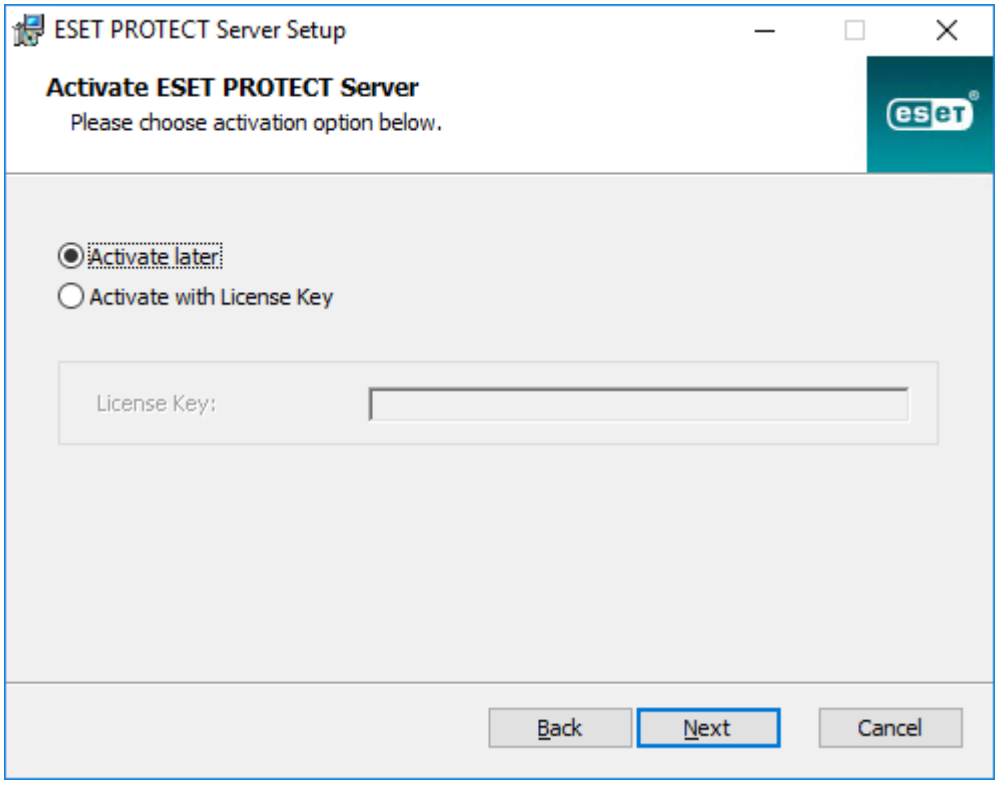
9. Το πρόγραμμα εγκατάστασης θα σας ζητήσει να εισαγάγετε έναν κωδικό πρόσβασης για τον λογαριασμό διαχειριστή της Κονσόλας διαδικτύου. Αυτός ο κωδικός πρόσβασης είναι σημαντικός, επειδή θα τον χρησιμοποιήσετε για να συνδεθείτε με την Κονσόλα διαδικτύου ESET PROTECT. Κάντε κλικ στο στοιχείο**Επόμενο**.



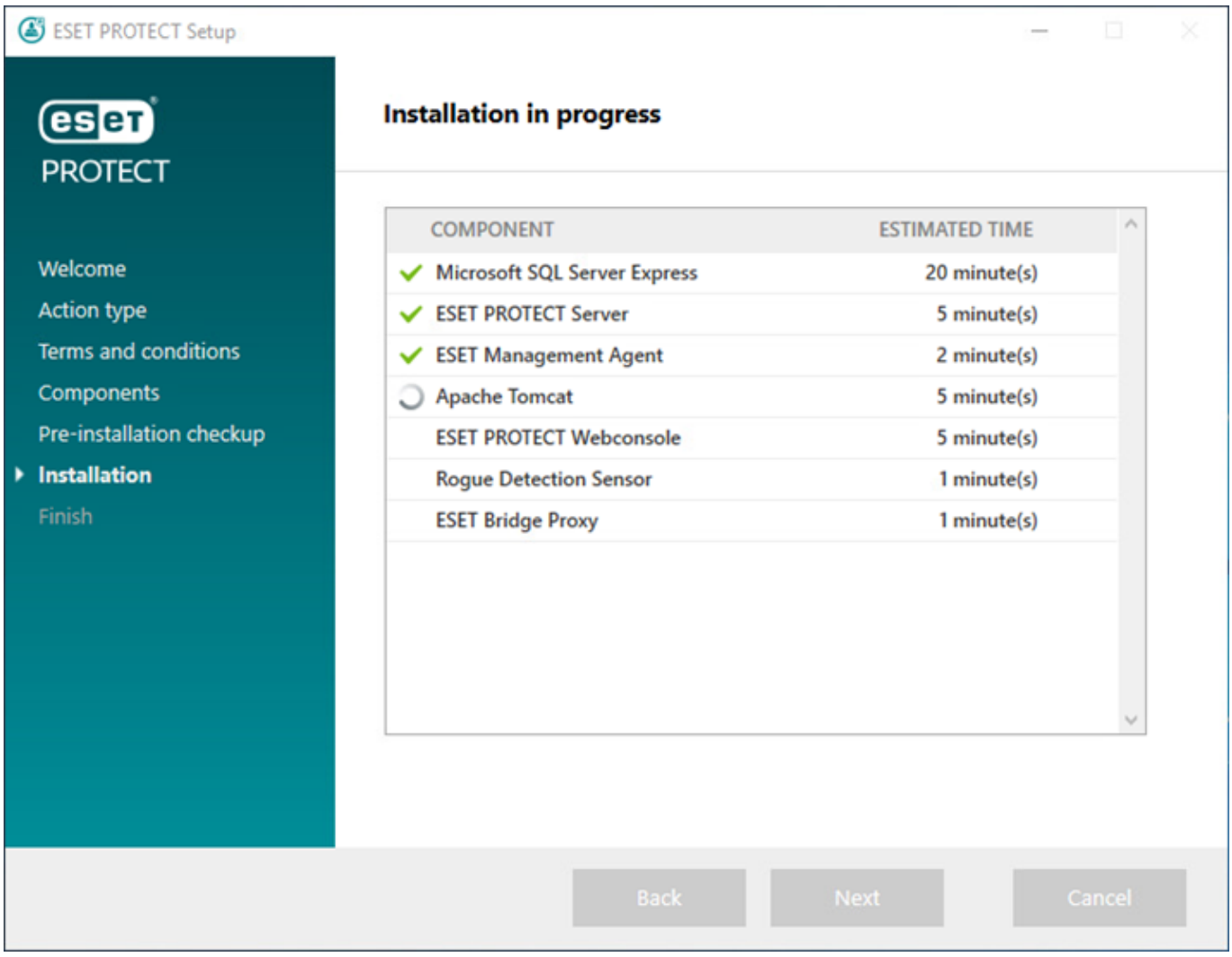
10. Αφήστε τα πεδία όπως είναι ή πληκτρολογήστε τις εταιρικές πληροφορίες σας, ώστε να εμφανίζονται στις λεπτομέρειες των πιστοποιητικών του φορέα ESET Management και του διακομιστή ESET PROTECT. Εάν επιλέξετε να εισαγάγετε κωδικό πρόσβασης στο πεδίο **Κωδικός πρόσβασης αρχής έκδοσης πιστοποιητικού**, φροντίστε να τον απομνημονεύσετε. Κάντε κλικ στο στοιχείο**Επόμενο**.



11. Εισαγάγετε ένα έγκυρο **Κλειδί άδειας χρήσης** (περιλαμβάνεται στο email νέας αγοράς που λάβατε από την ESET) και κάντε κλικ στο κουμπί **Επόμενο**. Εναλλακτικά, μπορείτε να επιλέξετε **Ενεργοποίηση αργότερα** (ανατρέξτε στο κεφάλαιο Ενεργοποίηση για πρόσθετες οδηγίες).



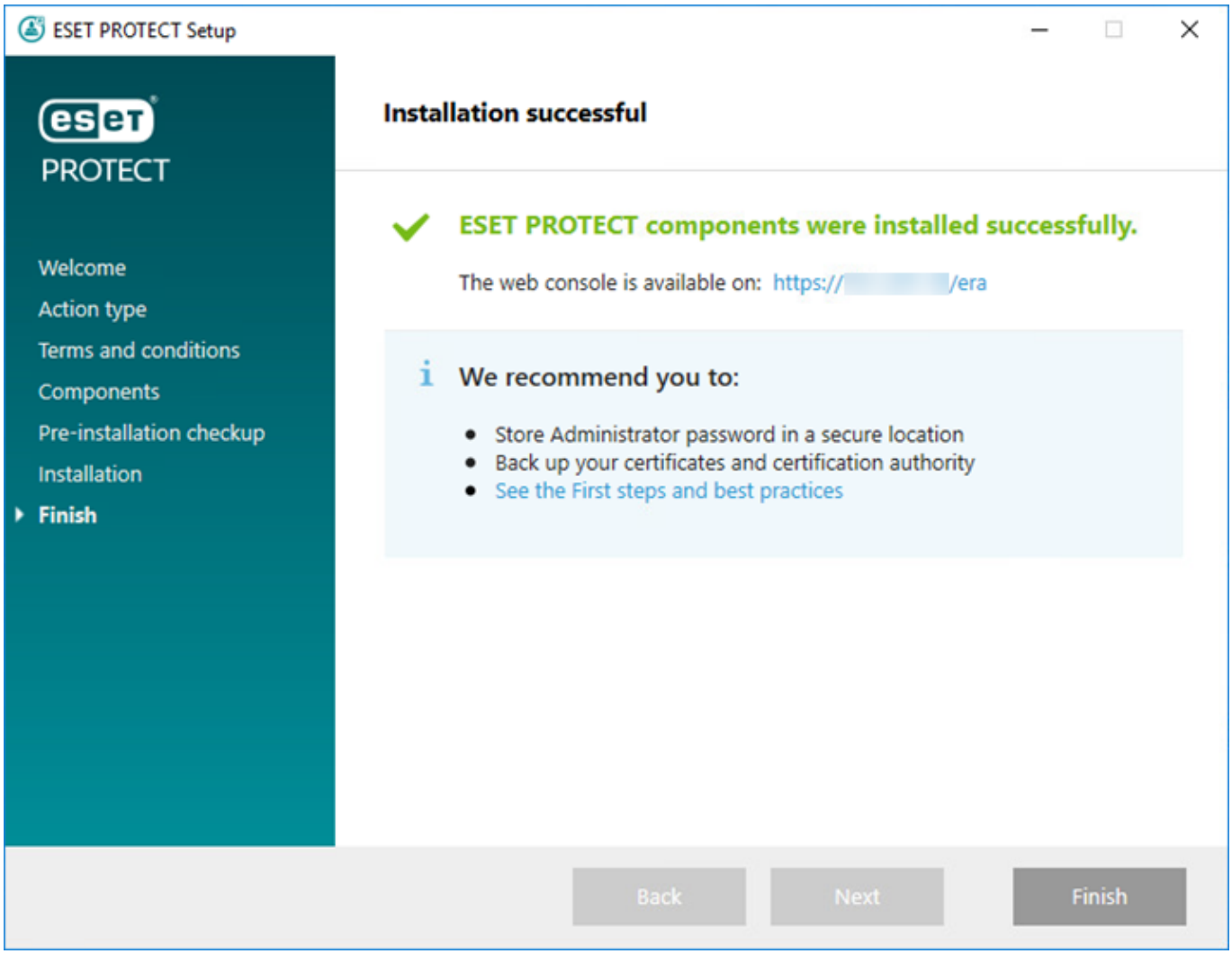
12. Θα δείτε την πρόοδο της εγκατάστασης.



13. Αν επιλέξατε την εγκατάσταση του **αισθητήρας Rogue Detection Sensor**, θα δείτε τα παράθυρα

εγκατάστασης για το πρόγραμμα οδήγησης WinPcap. Βεβαιωθείτε ότι έχετε επιλέξει το πλαίσιο ελέγχου **Αυτόματη έναρξη του προγράμματος οδήγησης WinPcap κατά την εκκίνηση**.

14. Όταν ολοκληρωθεί η εγκατάσταση, θα εμφανιστεί το μήνυμα «Τα στοιχεία του ESET PROTECT εγκαταστάθηκαν επιτυχώς» μαζί με τη διεύθυνση URL της Κονσόλας διαδικτύου ESET PROTECT. Κάντε κλικ στη διεύθυνση URL για να ανοίξετε την Κονσόλα διαδικτύου ή κάντε κλικ στο κουμπί **Τέλος**.



Εάν η εγκατάσταση δεν είναι επιτυχής:

• Μελετήστε τα αρχεία καταγραφής εγκατάστασης του πακέτου εγκατάστασης «όλα-σε-ένα». Ο κατάλογος των αρχείων καταγραφής είναι ίδιος με αυτόν από τον οποίο εκτελείται το πρόγραμμα εγκατάστασης «όλα-σε-ένα», για παράδειγμα:
`C:\Users\Administrator\Downloads\x64\logs\`

• Ανατρέξτε στο κεφάλαιο Αντιμετώπιση προβλημάτων για πρόσθετα βήματα επίλυσης του ζητήματος.

Εγκατάσταση Σύνδεσης κινητών συσκευών

ESET PROTECT (ανεξάρτητη)

Το στοιχείο Διαχείριση/Σύνδεση κινητών συσκευών (Διαχείριση κινητών συσκευών/MDC) του ESET PROTECT (μόνο εσωτερικής εγκατάστασης) φτάνει στο τέλος του κύκλου ζωής τον Ιανουάριο του 2024. Διαβάστε περισσότερα. Συνιστάται η μετεγκατάσταση στο cloud διαχείρισης κινητών συσκευών.

Για να εγκαταστήσετε τη Σύνδεση κινητών συσκευών ως ανεξάρτητο εργαλείο σε διαφορετικό υπολογιστή από τον διακομιστή ESET PROTECT, ακολουθήστε τα εξής βήματα.

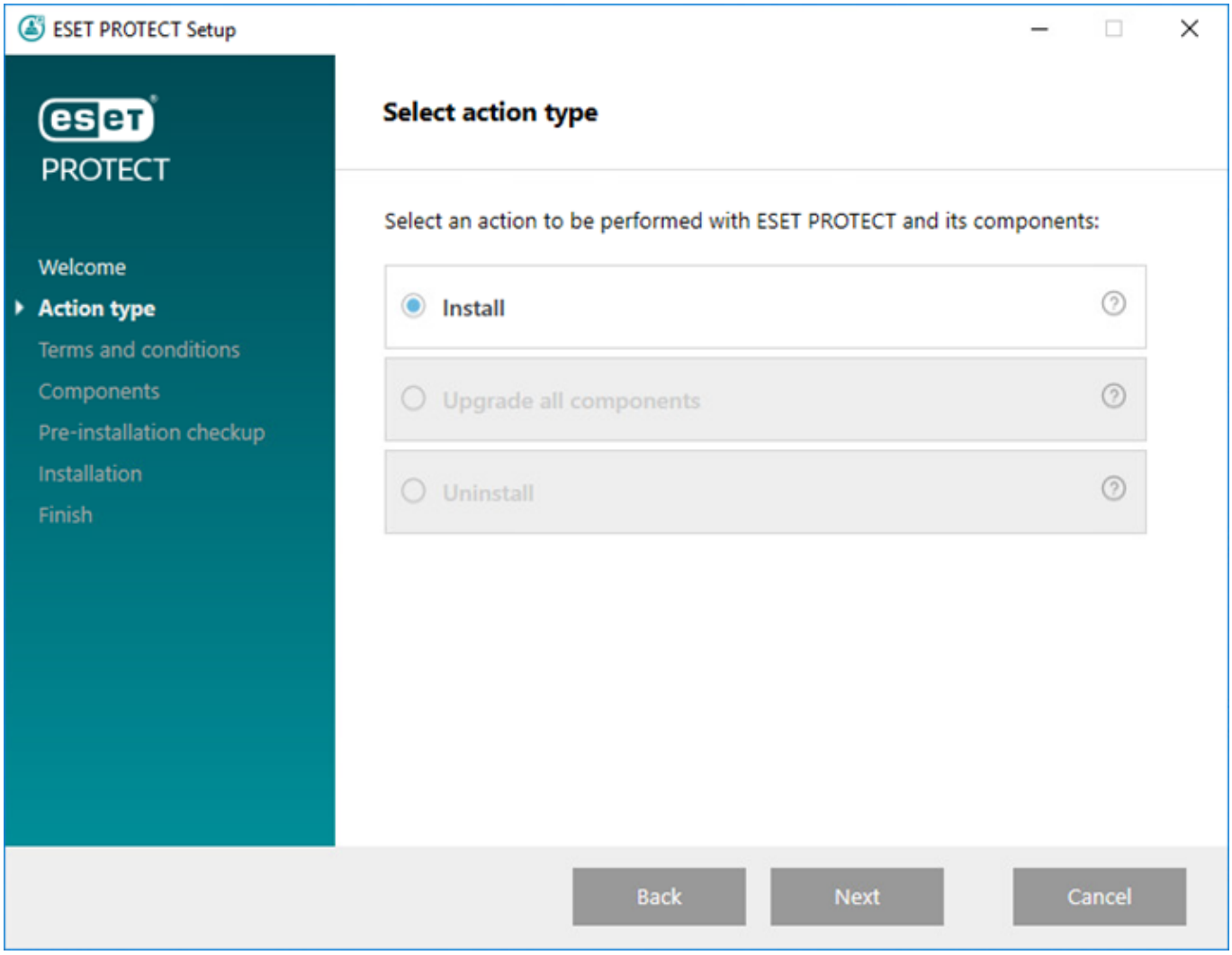
Η Σύνδεση κινητών συσκευών πρέπει να είναι προσβάσιμη από το Internet, έτσι ώστε η διαχείριση των κινητών συσκευών να είναι δυνατή ανά πάσα στιγμή, ανεξάρτητα από την τοποθεσία στην οποία βρίσκονται.

Λάβετε υπόψη ότι η κινητή συσκευή επικοινωνεί με τη σύνδεση κινητών συσκευών, η οποία επηρεάζει αναπόφευκτα τη χρήση των δεδομένων κινητής τηλεφωνίας. Αυτό εφαρμόζεται ιδιαίτερα στην περιαγωγή.

Ακολουθήστε τα παρακάτω βήματα για να εγκαταστήσετε τη Σύνδεση κινητών συσκευών σε λειτουργικό σύστημα Windows:

1. Διαβάστε πρώτα τα προαπαιτούμενα και βεβαιωθείτε ότι ικανοποιούνται όλα.

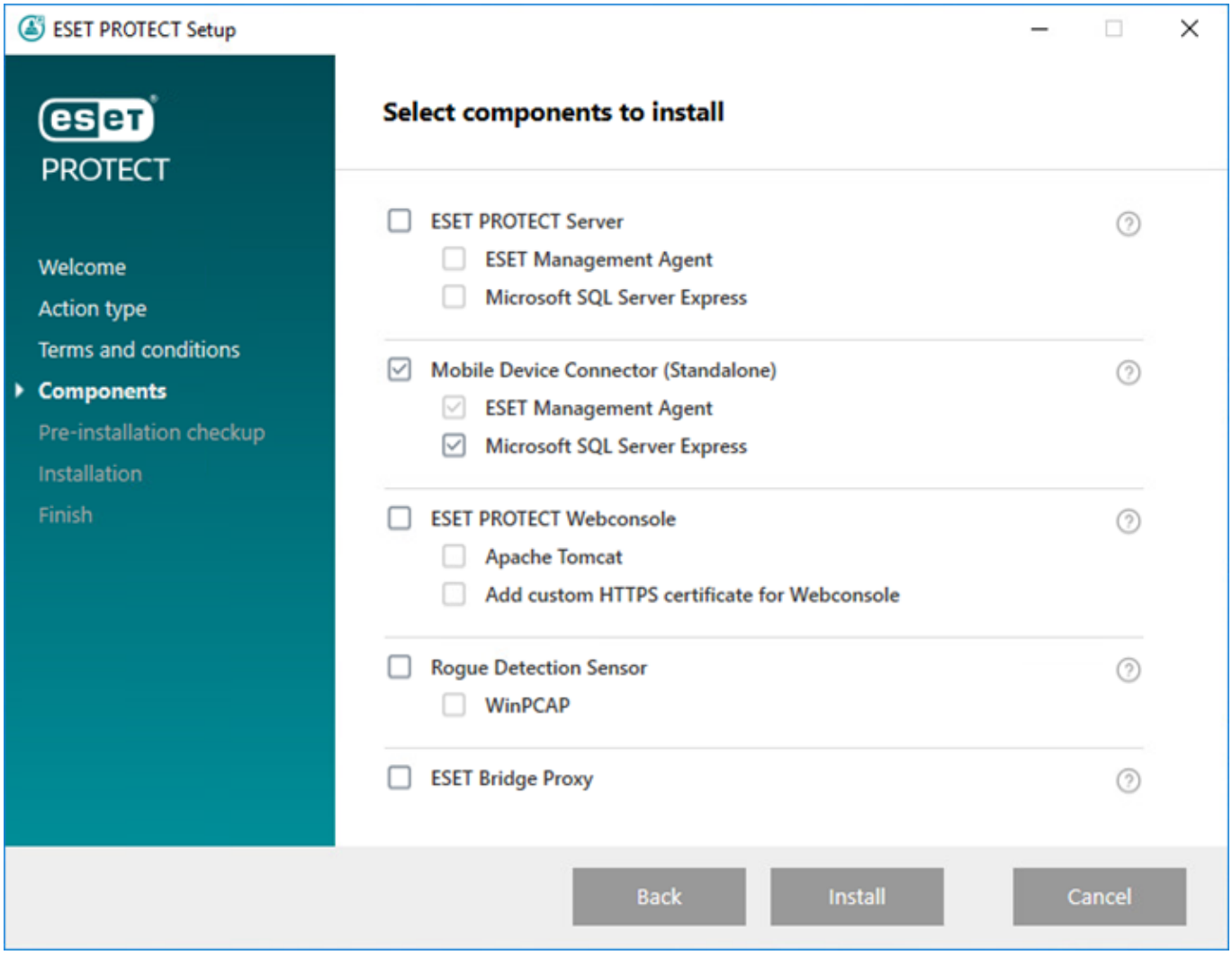
2. Κάντε διπλό κλικ στο πακέτο εγκατάστασης για να το ανοίξετε, επιλέξτε **Εγκατάσταση** και κάντε κλικ στο κουμπί **Επόμενο**.



3. Επιλέξτε το πλαίσιο ελέγχου **Συμμετοχή στο πρόγραμμα βελτίωσης προϊόντος**, για να αποστέλλονται ανώνυμα δεδομένα τηλεμετρίας και αναφορές σφαλμάτων στην ESET (έκδοση και τύπος λειτουργικού συστήματος, έκδοση προϊόντος ESET και άλλες πληροφορίες ειδικά για το προϊόν).

4. Αφού αποδεχτείτε την Άδεια Χρήσης Τελικού Χρήστη (EULA), επιλέξτε **Επόμενο**.

5. Επιλέξτε μόνο το πλαίσιο ελέγχου που βρίσκεται δίπλα στο στοιχείο **Mobile Device Connector (Ανεξάρτητο)**. Η Σύνδεση κινητών συσκευών ESET PROTECT On-Prem απαιτεί **βάση δεδομένων** για λειτουργία. Επιλέξτε **Microsoft SQL Server Express**, αν θέλετε να εγκαταστήσετε τη βάση δεδομένων ή αφήστε το πλαίσιο ελέγχου κενό. Αν θέλετε να συνδεθείτε σε μια υπάρχουσα βάση δεδομένων, θα έχετε την επιλογή να το κάνετε αυτό κατά τη διάρκεια της εγκατάστασης. Κάντε κλικ στην επιλογή **Εγκατάσταση**, για να συνεχίσετε με την εγκατάσταση.



6. Αν εγκαταστήσατε τη βάση δεδομένων στο πλαίσιο αυτής της εγκατάστασης στο βήμα 5, η βάση δεδομένων θα εγκατασταθεί τώρα αυτόματα και θα μπορείτε να μεταβείτε απευθείας στο βήμα 8. Αν επιλέξετε να μην εγκαταστήσετε βάση δεδομένων στο βήμα 5, θα σας ζητηθεί να συνδέσετε το στοιχείο MDM στην υπάρχουσα βάση δεδομένων σας.

> Μπορείτε να χρησιμοποιήσετε τον ίδιο διακομιστή βάσης δεδομένων που χρησιμοποιείτε για τη βάση δεδομένων ESET PROTECT, ωστόσο συνιστάται να χρησιμοποιήσετε διαφορετικό διακομιστή βάσης δεδομένων, αν σκοπεύετε να εγγράψετε περισσότερες από 80 κινητές συσκευές.

7. Το πρόγραμμα εγκατάστασης πρέπει να συνδέσει μια υπάρχουσα βάση δεδομένων η οποία θα χρησιμοποιείται από τη Σύνδεση κινητών συσκευών. Καθορίστε τα παρακάτω στοιχεία σύνδεσης:

- **Βάση δεδομένων**: MySQL Server/MS SQL Server/MS SQL Server via Windows Authentication

- **Πρόγραμμα οδήγησης ODBC**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/MySQL ODBC 8.1 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server

- **Όνομα βάσης δεδομένων**: Συνιστάται να χρησιμοποιήσετε το προκαθορισμένο όνομα ή να το αλλάξετε, εάν απαιτείται.

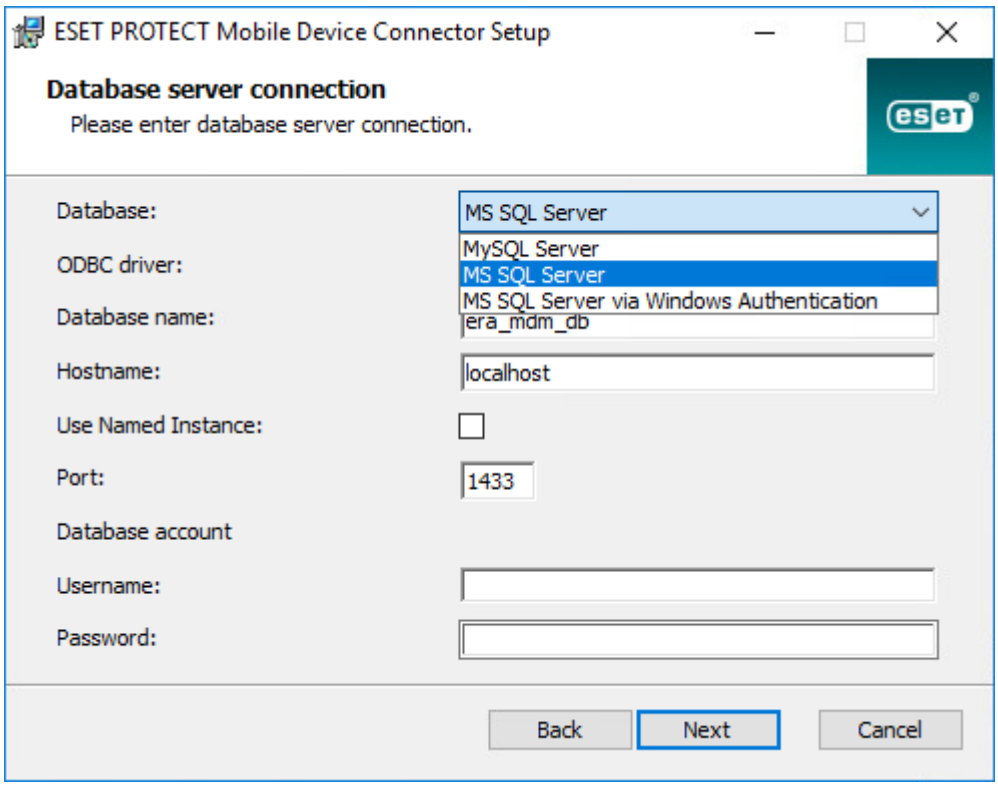
- **Όνομα κεντρικού υπολογιστή**: όνομα κεντρικού υπολογιστή ή διεύθυνση IP του διακομιστή

βάσης δεδομένων σας

• **Θύρα**: χρησιμοποιείται για σύνδεση με το διακομιστή βάσης δεδομένων

• **Όνομα χρήστη/Κωδικός πρόσβασης** του λογαριασμού διαχειριστή βάσης δεδομένων

• **Χρήση ονόματος παρουσίας** - Εάν χρησιμοποιείτε βάση δεδομένων Microsoft SQL, μπορείτε να επιλέξετε το πλαίσιο ελέγχου **Χρήση ονόματος παρουσίας** για να χρησιμοποιήσετε μια προσαρμοσμένη παρουσία βάσης δεδομένων. Μπορείτε να τη ρυθμίσετε στο πεδίο **Όνομα κεντρικού υπολογιστή** με τη μορφή *HOSTNAME\DB_INSTANCE* (για παράδειγμα, *192.168.0.10\ESMC7SQL*. Για βάση δεδομένων σε σύμπλεγμα, χρησιμοποιήστε μόνο το όνομα συμπλέγματος. Εάν ορίσετε αυτήν την επιλογή, δεν μπορείτε να αλλάξετε τη θύρα σύνδεσης της βάσης δεδομένων - το σύστημα θα χρησιμοποιεί τις προεπιλεγμένες θύρες που προσδιορίζονται από την Microsoft. Για να συνδέσετε τον Διακομιστή ESET PROTECT με τη βάση δεδομένων Microsoft SQL που είναι εγκατεστημένη σε ένα σύμπλεγμα ανακατεύθυνσης, εισαγάγετε το όνομα συμπλέγματος στο πεδίο **Όνομα κεντρικού υπολογιστή**.



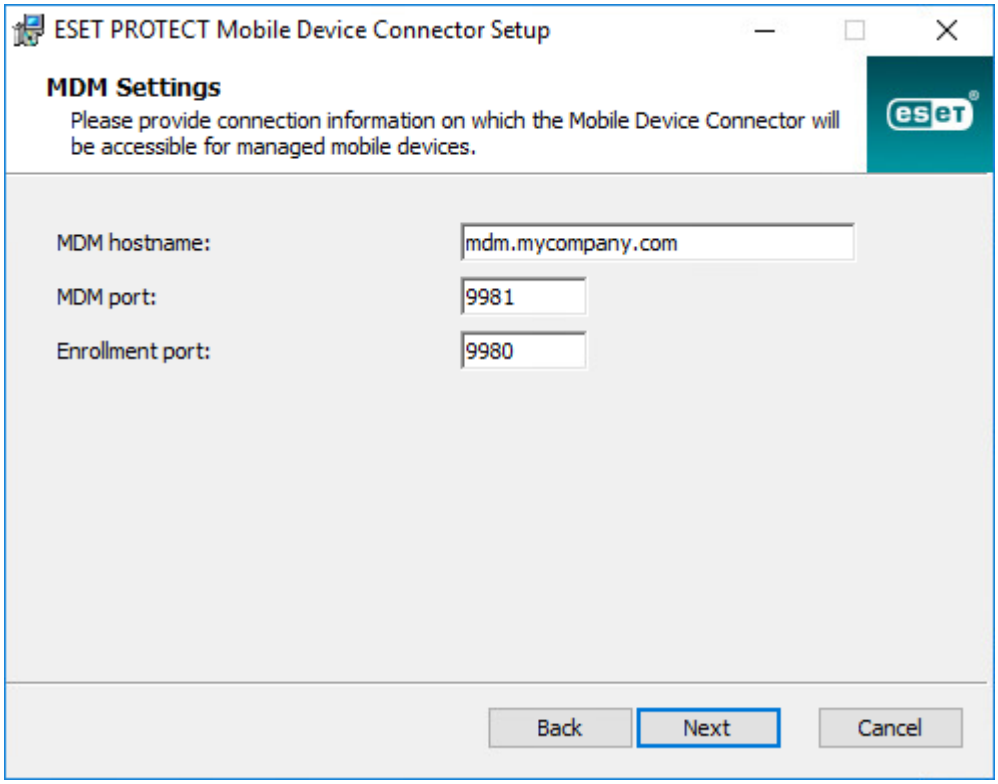
8. Εάν η σύνδεση ήταν επιτυχής, θα σας ζητηθεί να επαληθεύσετε ότι θέλετε να χρησιμοποιήσετε τον παρεχόμενο χρήστη ως χρήστη βάσης δεδομένων για το MDM ESET PROTECT.

9. Μετά την επιτυχή εγκατάσταση της νέας βάσης δεδομένων ή την επιτυχή σύνδεση του προγράμματος εγκατάστασης στην υπάρχουσα βάση δεδομένων, μπορείτε να συνεχίσετε με την εγκατάσταση του MDM. Καθορίστε το **Όνομα κεντρικού υπολογιστή MDM**: αυτό είναι ο δημόσιος τομέας ή η δημόσια διεύθυνση IP του διακομιστή MDM ο οποίος είναι προσβάσιμος από τις κινητές συσκευές μέσω διαδικτύου.

Το όνομα κεντρικού υπολογιστή MDM πρέπει να εισαχθεί με την ίδια μορφή που εμφανίζεται στο **πιστοποιητικό διακομιστή HTTPS**, διαφορετικά η κινητή συσκευή iOS θα αρνηθεί να εγκαταστήσει το προφίλ MDM. Για παράδειγμα, εάν υπάρχει διεύθυνση IP καθορισμένη στο πιστοποιητικό HTTPS, πληκτρολογήστε αυτήν τη διεύθυνση IP στο πεδίο **Όνομα κεντρικού υπολογιστή MDM**. Σε περίπτωση που καθορίζεται FQDN (π.χ., `mdm.mycompany.com`) στο

πιστοποιητικό HTTPS, εισαγάγετε αυτό το FQDN στο πεδίο **Όνομα κεντρικού υπολογιστή MDM**. Επίσης, εάν χρησιμοποιείται ειδικός χαρακτήρας * (π.χ. `*.mycompany.com`) στο πιστοποιητικό HTTPS, μπορείτε να χρησιμοποιήσετε το `mdm.mycompany.com` στο πεδίο **Όνομα κεντρικού υπολογιστή MDM**.

Να είστε πολύ προσεκτικοί όταν συμπληρώνετε το πεδίο **Όνομα κεντρικού υπολογιστή MDM** σε αυτό το βήμα της εγκατάστασης. Αν οι πληροφορίες είναι εσφαλμένες ή σε λάθος μορφή, η σύνδεση MDM δεν θα λειτουργεί σωστά και ο μοναδικός τρόπος διόρθωσής της θα είναι η εγκατάσταση του στοιχείου.



10. Στο επόμενο βήμα, επαληθεύστε τη σύνδεση στη βάση δεδομένων κάνοντας κλικ στο κουμπί **Επόμενο**.

11. Συνδέστε τη σύνδεση MDM στον διακομιστή ESET PROTECT. Συμπληρώστε τα πεδία **Κεντρικός υπολογιστής διακομιστή** και **Θύρα διακομιστή** που απαιτούνται για τη σύνδεση στον διακομιστή ESET PROTECT και επιλέξτε είτε **Εγκατάσταση με υποβοήθηση διακομιστή** είτε **Εγκατάσταση χωρίς σύνδεση**, για να συνεχίσετε:

• **Εγκατάσταση με υποβοήθηση διακομιστή** - Θα πρέπει να παράσχετε τα διαπιστευτήρια διαχειριστή της κονσόλας διαδικτύου ESET PROTECT και το πρόγραμμα εγκατάστασης θα κατεβάσει αυτόματα τα απαιτούμενα πιστοποιητικά. Επίσης, ελέγξτε τα δικαιώματα που απαιτούνται για εγκατάσταση υποβοηθούμενη από το διακομιστή.

1.Εισαγάγετε τα στοιχεία **Κεντρικός υπολογιστής διακομιστή** - όνομα ή διεύθυνση IP του διακομιστή ESET PROTECT και **Θύρα κονσόλας διαδικτύου** (αφήστε την προεπιλεγμένη θύρα 2223, εάν δεν χρησιμοποιείτε προσαρμοσμένη θύρα). Επίσης, συμπληρώστε τα διαπιστευτήρια λογαριασμού διαχειριστή της κονσόλας διαδικτύου - **Όνομα χρήστη/Κωδικός πρόσβασης**.

2.Όταν σας ζητηθεί να αποδεχτείτε το πιστοποιητικό, επιλέξτε **Ναι**. Συνεχίστε στο βήμα 11.

• **Εγκατάσταση χωρίς σύνδεση** - Θα πρέπει να παράσχετε ένα Πιστοποιητικό διακομιστή μεσολάβησης και μια Αρχή έκδοσης πιστοποιητικών που μπορείτε να εξαγάγετε από το ESET PROTECT On-Prem. Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το προσαρμοσμένο πιστοποιητικό και την κατάλληλη αρχή έκδοσης πιστοποιητικών.

1.Κάντε κλικ στην **Αναζήτηση** δίπλα στο ομότιμο πιστοποιητικό και μεταβείτε στην τοποθεσία του **ομότιμου πιστοποιητικού** σας (αυτό είναι το πιστοποιητικό διακομιστή μεσολάβησης που έχετε εξαγάγει από το ESET PROTECT On-Prem). Αφήστε κενό το πεδίο κειμένου **Κωδικός πρόσβασης πιστοποιητικού** επειδή αυτό το πιστοποιητικό δεν απαιτεί κωδικό πρόσβασης.

2.Επαναλάβετε τη διαδικασία για την αρχή έκδοσης πιστοποιητικών και συνεχίστε στο βήμα 11.

Σε περίπτωση που χρησιμοποιείτε προσαρμοσμένα πιστοποιητικά με το ESET PROTECT On-Prem (αντί των προεπιλεγμένων που δημιουργήθηκαν αυτόματα κατά την εγκατάσταση του ESET PROTECT On-Prem), θα πρέπει να χρησιμοποιήσετε αυτά όταν σας ζητηθεί να καθορίσετε πιστοποιητικό διακομιστή μεσολάβησης.

12. Καθορίστε έναν φάκελο προορισμού για τη Σύνδεση κινητών συσκευών (συνιστάται να χρησιμοποιήσετε τον προεπιλεγμένο φάκελο) και κατόπιν κάντε κλικ στα κουμπιά **Επόμενο** > **Εγκατάσταση**.

Μετά την ολοκλήρωση της εγκατάστασης του MDM, θα σας ζητηθεί η εγκατάσταση φορέα. Κάντε κλικ στο κουμπί **Επόμενο** για να ξεκινήσετε την εγκατάσταση, αποδεχτείτε το EULA, εάν συμφωνείτε, και ακολουθήστε τα εξής βήματα:

1. Εισαγάγετε τα στοιχεία **Κεντρικός υπολογιστής διακομιστή** (όνομα κεντρικού υπολογιστή ή διεύθυνση IP του διακομιστή ESET PROTECT) και **Θύρα διακομιστή** (η προεπιλεγμένη θύρα είναι 2222 - εάν χρησιμοποιείτε διαφορετική θύρα, τότε αντικαταστήστε την προεπιλεγμένη θύρα με τον προσαρμοσμένο αριθμό θύρας).

Βεβαιωθείτε ότι ο **Κεντρικός υπολογιστής διακομιστή** αντιστοιχεί σε μία τουλάχιστον από τις τιμές (υπό ιδανικές συνθήκες με το FQDN) που καθορίζονται στο πεδίο **Κεντρικός υπολογιστής** του στοιχείου **Πιστοποιητικό διακομιστή**. Διαφορετικά θα προκύψει σφάλμα που θα αναφέρει 'Το πιστοποιητικό διακομιστή που λήφθηκε δεν είναι έγκυρο'. Η μόνη εξαίρεση είναι σε περίπτωση που υπάρχει ειδικός χαρακτήρας (*) στο πεδίο κεντρικού υπολογιστή του πιστοποιητικού διακομιστή, πράγμα που σημαίνει ότι θα λειτουργήσει με οποιονδήποτε **Κεντρικό υπολογιστή διακομιστή**.

2. Εάν χρησιμοποιείτε διακομιστή μεσολάβησης, επιλέξτε το πλαίσιο ελέγχου **Χρήση διακομιστή μεσολάβησης**. Εάν επιλεγεί, το πρόγραμμα εγκατάστασης θα συνεχίσει με **εγκατάσταση χωρίς σύνδεση**.

Αυτή η ρύθμιση διακομιστή μεσολάβησης χρησιμοποιείται μόνο για (αντιγραφή) μεταξύ φορέα ESET Management και διακομιστή ESET PROTECT, όχι για αποθήκευση των ενημερώσεων στην προσωρινή μνήμη.
• **Όνομα κεντρικού υπολογιστή διακομιστή μεσολάβησης**: όνομα κεντρικού υπολογιστή ή διεύθυνση IP του υπολογιστή του διακομιστή μεσολάβησης HTTP.
• **Θύρα διακομιστή μεσολάβησης**: η προεπιλεγμένη τιμή είναι 3128.
• **Όνομα χρήστη**, **Κωδικός πρόσβασης**: εισαγάγετε τα διαπιστευτήρια που χρησιμοποιούνται από τον διακομιστή μεσολάβησης, αν χρησιμοποιείται έλεγχος ταυτότητας.
Μπορείτε να αλλάξετε τις ρυθμίσεις διακομιστή μεσολάβησης αργότερα στην πολιτική. Ο διακομιστής μεσολάβησης πρέπει να είναι εγκατεστημένος, για να μπορείτε να διαμορφώσετε μια σύνδεση φορέα - διακομιστή μέσω διακομιστή μεσολάβησης.

3. Επιλέξτε μία από τις ακόλουθες επιλογές εγκατάστασης και ακολουθήστε τα βήματα από την κατάλληλη ενότητα παρακάτω:

Εγκατάσταση με υποβοήθηση διακομιστή - θα πρέπει να δώσετε τα διαπιστευτήρια διαχειριστή της κονσόλας διαδικτύου ESET PROTECT (το πρόγραμμα εγκατάστασης θα λάβει αυτόματα τα απαιτούμενα πιστοποιητικά).

Εγκατάσταση χωρίς σύνδεση - Θα πρέπει να παράσχετε ένα Πιστοποιητικό φορέα και μια Αρχή έκδοσης πιστοποιητικού, τα οποία μπορείτε να εξαγάγετε από το ESET PROTECT On-Prem. Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το προσαρμοσμένο πιστοποιητικό σας.

• Για να συνεχίσετε την **εγκατάσταση φορέα με υποβοήθηση διακομιστή** ακολουθήστε τα εξής βήματα:

1. Εισαγάγετε το όνομα κεντρικού υπολογιστή ή τη διεύθυνση IP της Κονσόλας διαδικτύου ESET PROTECT (ίδια με του διακομιστή ESET PROTECT) στο πεδίο **Κεντρικός υπολογιστής διακομιστή**. Αφήστε τη ρύθμιση του στοιχείου **Θύρα κονσόλας διαδικτύου** στην προεπιλεγμένη θύρα 2223, εάν δεν χρησιμοποιείτε προσαρμοσμένη θύρα. Επίσης, εισαγάγετε τα διαπιστευτήρια του λογαριασμού της Κονσόλας διαδικτύου στα πεδία **Όνομα χρήστη και Κωδικός πρόσβασης**. Για να συνδεθείτε ως χρήστης τομέα, επιλέξτε το πλαίσιο ελέγχου που βρίσκεται δίπλα στο στοιχείο **Σύνδεση στον τομέα**.

• Βεβαιωθείτε ότι ο **Κεντρικός υπολογιστής διακομιστή** αντιστοιχεί σε μία τουλάχιστον από τις τιμές (υπό ιδανικές συνθήκες με το FQDN) που καθορίζονται στο πεδίο **Κεντρικός υπολογιστής** του στοιχείου **Πιστοποιητικό διακομιστή**. Διαφορετικά θα προκύψει σφάλμα που θα αναφέρει 'Το πιστοποιητικό διακομιστή που λήφθηκε δεν είναι έγκυρο'. Η μόνη εξαίρεση είναι σε περίπτωση που υπάρχει ειδικός χαρακτήρας (*) στο πεδίο κεντρικού υπολογιστή του πιστοποιητικού διακομιστή, πράγμα που σημαίνει ότι θα λειτουργήσει με οποιονδήποτε **Κεντρικό υπολογιστή διακομιστή**.
• Δεν μπορείτε να χρησιμοποιήσετε έναν χρήστη με έλεγχο ταυτότητας δύο παραγόντων για εγκαταστάσεις με υποβοήθηση του διακομιστή.

2. Όταν ερωτηθείτε εάν θέλετε να αποδεχτείτε το πιστοποιητικό, επιλέξτε **Ναι'**.

3. Επιλέξτε το στοιχείο **Να μη δημιουργηθεί υπολογιστής (ο υπολογιστής θα δημιουργηθεί αυτόματα κατά την πρώτη σύνδεση)** ή **Επιλογή προσαρμοσμένης στατικής ομάδας**. Εάν επιλέξετε **Επιλογή προσαρμοσμένης στατικής ομάδας** θα μπορείτε να επιλέξετε από μια λίστα υφιστάμενων στατικών ομάδων στο ESET PROTECT On-Prem. Ο υπολογιστής θα προστεθεί στην ομάδα που επιλέξατε.

4. Καθορίστε έναν φάκελο προορισμού για το φορέα ESET Management (συνιστάται να

χρησιμοποιήσετε την προεπιλεγμένη τοποθεσία), επιλέξτε **Επόμενο** και στη συνέχεια **Εγκατάσταση**.

- Για να συνεχίσετε την **εγκατάσταση φορέα χωρίς σύνδεση** ακολουθήστε τα εξής βήματα:

1. Εάν επιλέξατε **Χρήση διακομιστή μεσολάβησης** στο προηγούμενο βήμα, συμπληρώστε το **Όνομα κεντρικού υπολογιστή διακομιστή μεσολάβησης**, τη **Θύρα διακομιστή μεσολάβησης** (η προεπιλεγμένη θύρα είναι 3128), το **Όνομα χρήστη** και τον **Κωδικό πρόσβασης** και κάντε κλικ στο στοιχείο **Επόμενο**.

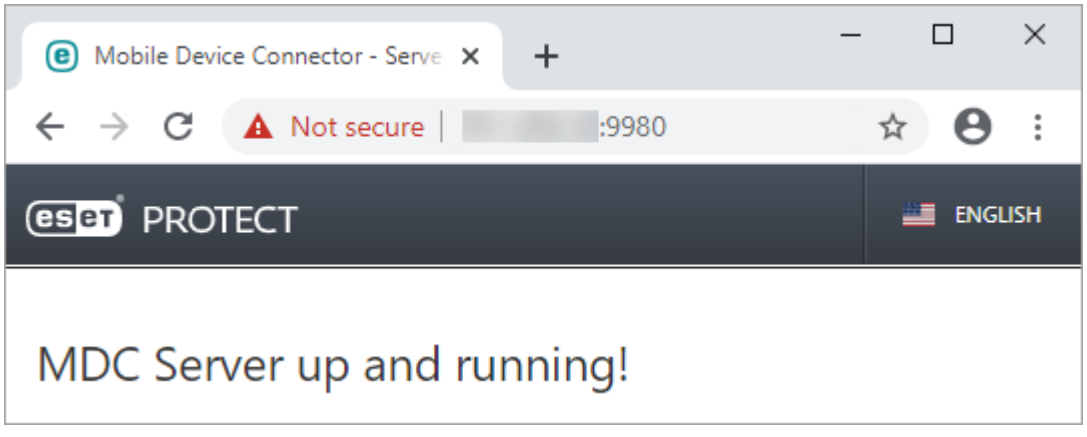
2. Κάντε κλικ στην **Αναζήτηση** και πλοηγηθείτε στην τοποθεσία του ομότιμου πιστοποιητικού σας (αυτό είναι το πιστοποιητικό φορέα που είχατε εξαγάγει από το ESET PROTECT On-Prem). Αφήστε κενό το πεδίο κειμένου **Κωδικός πρόσβασης πιστοποιητικού** επειδή αυτό το πιστοποιητικό δεν απαιτεί κωδικό πρόσβασης. Δεν χρειάζεται να κάνετε αναζήτηση για **Αρχή έκδοσης πιστοποιητικού** - αφήστε αυτό το πεδίο κενό.

> **i** Εάν χρησιμοποιείτε ένα προσαρμοσμένο πιστοποιητικό με το ESET PROTECT On-Prem (αντί των προεπιλεγμένων που δημιουργήθηκαν αυτόματα κατά την εγκατάσταση του ESET PROTECT On-Prem), χρησιμοποιήστε αναλόγως τα προσαρμοσμένα πιστοποιητικά σας.

> **⚠** Ο κωδικός πρόσβασης του πιστοποιητικού δεν πρέπει να περιέχει τους ακόλουθους χαρακτήρες: " \ Αυτοί οι χαρακτήρες προκαλούν κρίσιμο σφάλμα κατά την αρχικοποίηση του φορέα.

3. Επιλέξτε **Επόμενο** για να εγκαταστήσετε τον προεπιλεγμένο φάκελο ή **Αλλαγή** για να επιλέξετε άλλον φάκελο (συνιστάται να χρησιμοποιήσετε την προεπιλεγμένη τοποθεσία).

Μετά την ολοκλήρωση της εγκατάστασης, ελέγξτε εάν εκτελείται σωστά η Σύνδεση κινητών συσκευών ανοίγοντας τη διεύθυνση *https://*όνομα-κεντρικού-υπολογιστή-*mdm:*θύρα-εγγραφής (για παράδειγμα *https://mdm.company.com:9980*) στο πρόγραμμα περιήγησης ή από μια κινητή συσκευή. Εάν η εγκατάσταση ήταν επιτυχής, θα δείτε το ακόλουθο μήνυμα:



Τώρα μπορείτε να ενεργοποιήσετε το MDM από το ESET PROTECT On-Prem.

Εγκατάσταση στοιχείου στα Windows

Για πολλά σενάρια εγκατάστασης, πρέπει να εγκαταστήσετε διαφορετικά στοιχεία του ESET PROTECT σε διαφορετικούς υπολογιστές ώστε να εξυπηρετούνται οι αρχιτεκτονικές δικτύου, να ικανοποιούνται οι απαιτήσεις επιδόσεων ή για άλλους λόγους. Για μεμονωμένα στοιχεία του ESET PROTECT, υπάρχουν διαθέσιμα τα ακόλουθα πακέτα εγκατάστασης:

Εγκατάσταση βασικών στοιχείων:

- ESET PROTECTΔιακομιστής

- Κονσόλα διαδικτύου ESET PROTECT – Μπορείτε να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT σε έναν διαφορετικό υπολογιστή από τον υπολογιστή στον οποίο εκτελείται ο διακομιστής ESET PROTECT.

- Ο φορέας ESET Management (πρέπει να εγκατασταθεί σε υπολογιστές-πελάτες, προαιρετικά στο διακομιστή ESET PROTECT)

Εγκατάσταση προαιρετικών στοιχείων:

- Αισθητήρας RD

- Σύνδεση κινητών συσκευών

- ESET Bridge Διακομιστής Μεσολάβησης HTTP

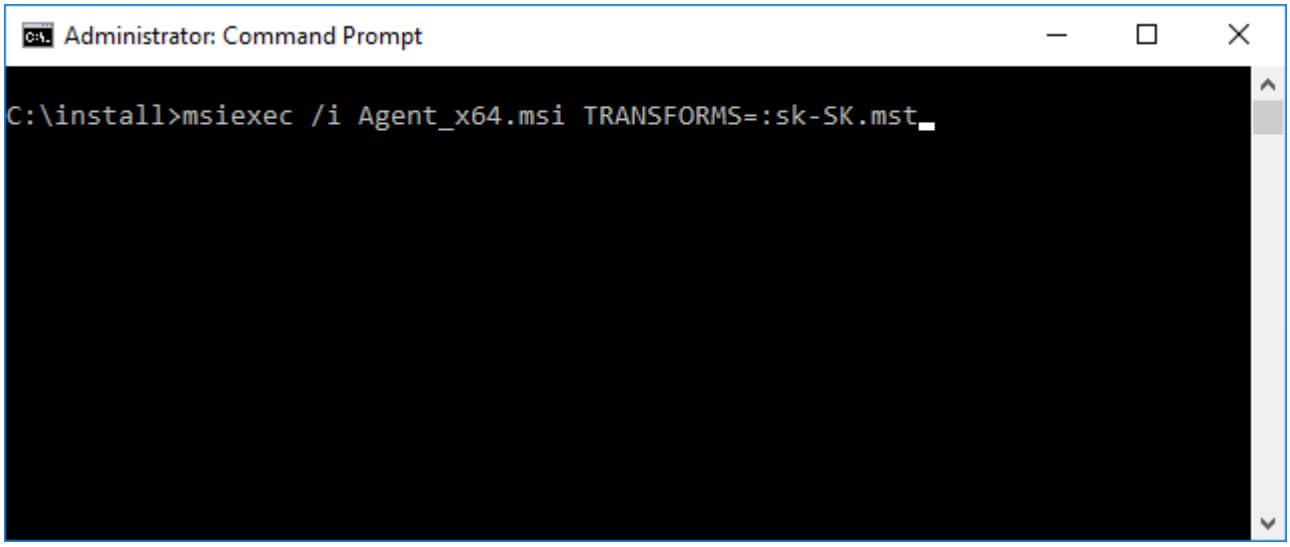
- Εργαλείο ειδώλου

Δείτε επίσης το θέμα Εγκατάσταση όλα σε ένα του ESET PROTECT.

Για οδηγίες σχετικά με την αναβάθμιση παλαιότερης έκδοσης του ESET PROTECT On-Prem στην πιο πρόσφατη έκδοση του ESET PROTECT On-Prem 11.0, ανατρέξτε στο θέμα διαδικασίες αναβάθμισης.

Εάν θέλετε να εκτελέσετε την εγκατάσταση στην τοπική γλώσσα σας, πρέπει να εκκινήσετε το πρόγραμμα εγκατάστασης MSI του συγκεκριμένου στοιχείου ESET PROTECT μέσω της γραμμής εντολών.

Ακολουθεί ένα παράδειγμα για τον τρόπο που μπορείτε να εκτελέσετε την εγκατάσταση στη Σλοβακική γλώσσα:



Για να επιλέξετε τη γλώσσα στην οποία θέλετε να εκτελέσετε το πρόγραμμα εγκατάστασης, καθορίστε την αντίστοιχη παράμετρο TRANSFORMS (Μεταμόρφωση) σύμφωνα με τον παρακάτω πίνακα:

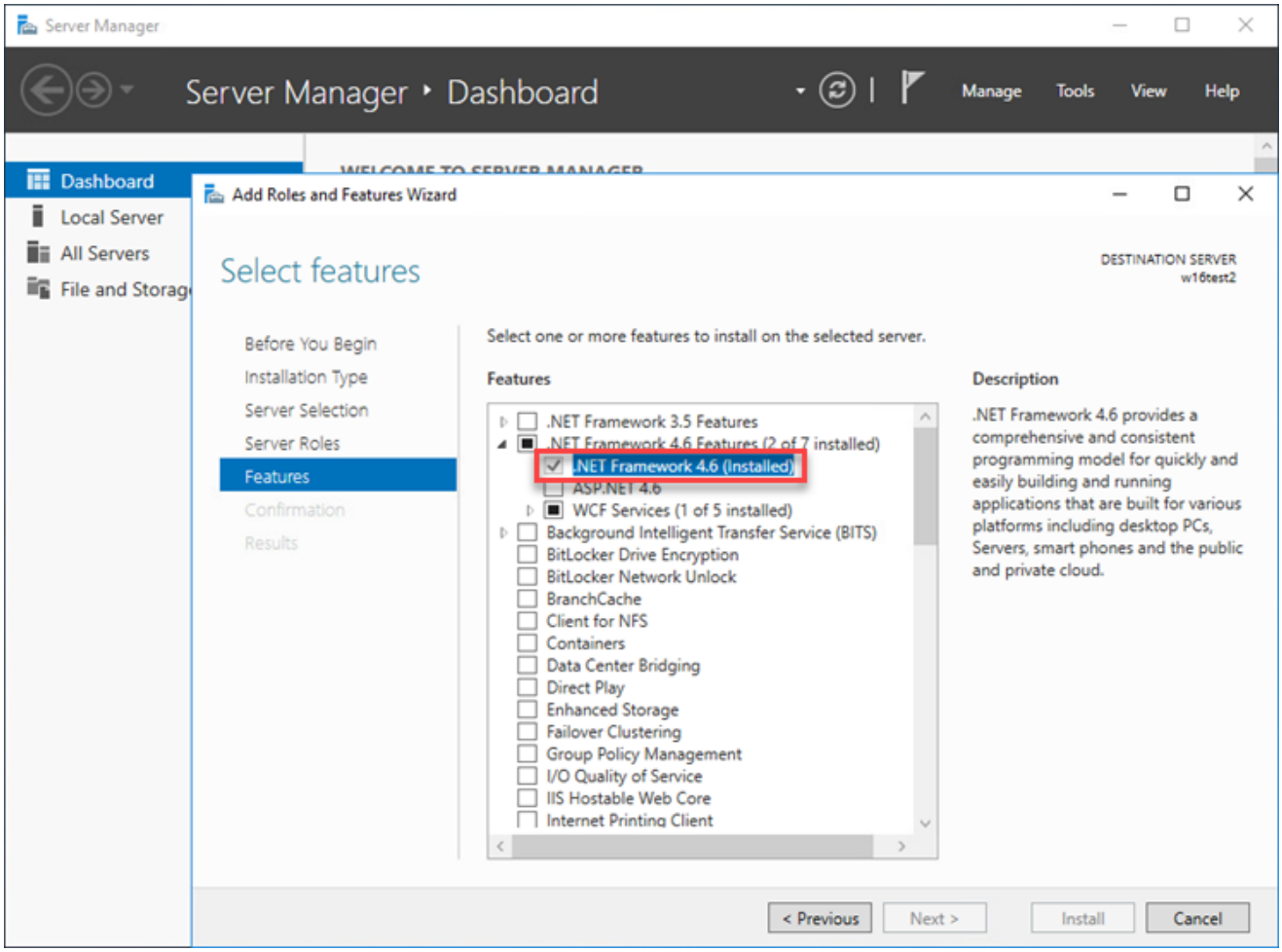
Γλώσσα	Κωδικός
Αγγλικά (Ηνωμένες Πολιτείες)	en-US
Αραβικά (Αίγυπτος)	ar-EG
Κινεζικά απλοποιημένα	zh-CN
Κινεζικά παραδοσιακά	zh-TW
Κροατικά (Κροατία)	hr-HR
Τσεχικά (Δημοκρατία της Τσεχίας)	cs-CZ
Γαλλικά (Γαλλία)	fr-FR
Γαλλικά (Καναδάς)	fr-CA
Γερμανικά (Γερμανία)	de-DE
Ελληνικά (Ελλάδα)	el-GR
Ουγγρικά (Ουγγαρία)*	hu-HU
Ινδονησιακά (Ινδονησία)*	id-ID
Ιταλικά (Ιταλία)	it-IT
Ιαπωνικά (Ιαπωνία)	ja-JP
Κορεατικά (Κορέα)	ko-KR
Πολωνικά (Πολωνία)	pl-PL
Πορτογαλικά (Βραζιλία)	pt-BR
Ρωσικά (Ρωσία)	ru-RU
Ισπανικά (Χιλή)	es-CL
Ισπανικά (Ισπανία)	es-ES
Σλοβακικά (Σλοβακία)	sk-SK
Τουρκικά (Τουρκία)	tr-TR
Ουκρανικά (Ουκρανίας)	uk-UA

* Μόνο το προϊόν είναι διαθέσιμο σε αυτή τη γλώσσα. Η ηλεκτρονική βοήθεια δεν είναι διαθέσιμη.

Εγκατάσταση διακομιστή – Windows

Προαπαιτούμενα

- Πρέπει να υπάρχει έγκυρο κλειδί άδειας χρήσης.
- Πρέπει να υπάρχει ένα υποστηριζόμενο λειτουργικό σύστημα Windows.
- Οι απαιτούμενες θύρες πρέπει να είναι ανοιχτές και διαθέσιμες – δείτε την πλήρη λίστα των θυρών εδώ.
- Ο υποστηριζόμενος διακομιστής βάσης δεδομένων και η σύνδεση (Microsoft SQL Server ή MySQL) εγκαθίστανται και εκτελούνται. Συνιστάται να αναθεωρήσετε τις λεπτομέρειες της ρύθμισης παραμέτρων του διακομιστή βάσης δεδομένων (Microsoft SQL Server ή MySQL), για να ρυθμιστούν σωστά οι παράμετροι της βάσης δεδομένων για χρήση με το ESET PROTECT On-Prem. Διαβάστε το άρθρο της Γνωσιακής βάσης για να ρυθμίσετε τη βάση δεδομένων και τον χρήστη βάσης δεδομένων για το Microsoft SQL και το MySQL.
- Η κονσόλα διαδικτύου ESET PROTECT εγκαταστάθηκε για τη διαχείριση του διακομιστή ESET PROTECT.
- Η εγκατάσταση του Microsoft SQL Server Express απαιτεί το Microsoft .NET Framework 4. Μπορείτε να το εγκαταστήσετε χρησιμοποιώντας το στοιχείο **Οδηγός προσθήκης ρόλων και δυνατοτήτων**:



Εγκατάσταση

Για να εγκαταστήσετε το στοιχείο διακομιστή ESET PROTECT σε Windows, ακολουθήστε τα παρακάτω βήματα:

Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης που αναφέρονται παραπάνω.

1. Επισκεφτείτε την ενότητα λήψεων του ESET PROTECT για λήψη ενός ανεξάρτητου προγράμματος εγκατάστασης για αυτό το στοιχείο του ESET PROTECT (*server_x64.msi*).

2. Εκτελέστε το πρόγραμμα εγκατάστασης του διακομιστή ESET PROTECT και αποδεχτείτε το EULA, εάν συμφωνείτε.

3. Επιλέξτε το πλαίσιο ελέγχου **Συμμετοχή στο πρόγραμμα βελτίωσης προϊόντος**, για να αποστέλλονται ανώνυμα δεδομένα τηλεμετρίας και αναφορές σφαλμάτων στην ESET (έκδοση και τύπος λειτουργικού συστήματος, έκδοση προϊόντος ESET και άλλες πληροφορίες ειδικά για το προϊόν).

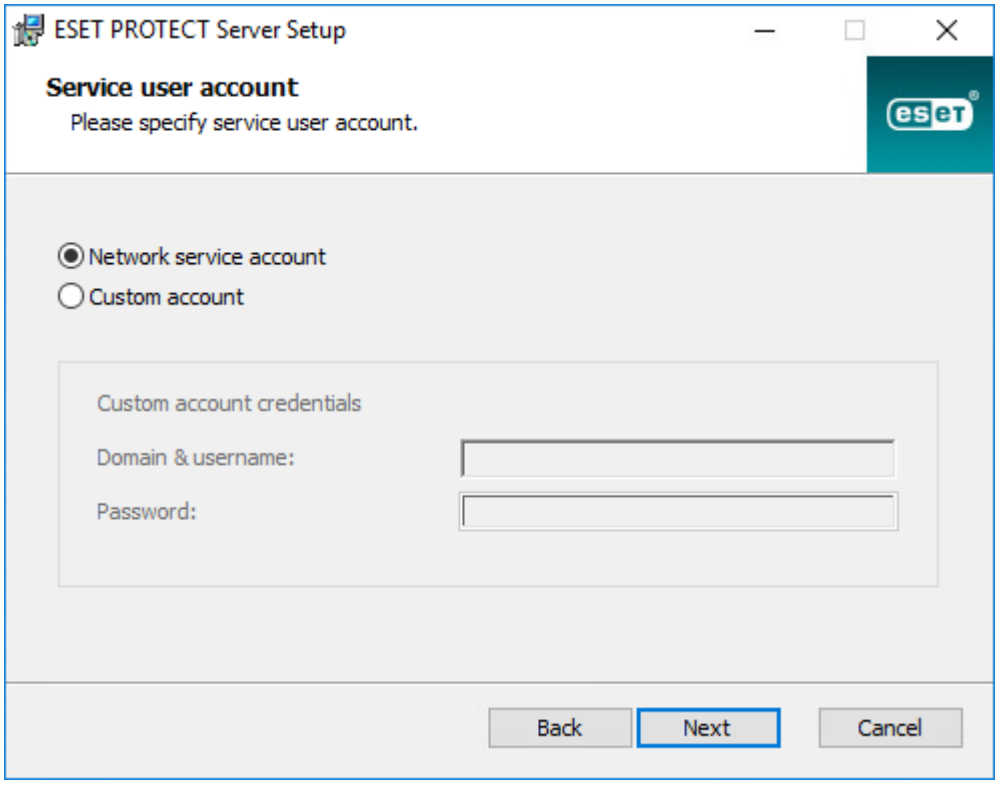
4. Αφήστε κενό το πλαίσιο ελέγχου δίπλα στο στοιχείο **Αυτή είναι εγκατάσταση συμπλέγματος** και κάντε κλικ στο κουμπί **Επόμενο**. Πρόκειται για εγκατάσταση συμπλέγματος;

Εάν εγκαθιστάτε διακομιστή ESET PROTECT σε σύμπλεγμα ανακατεύθυνσης, επιλέξτε το πλαίσιο ελέγχου δίπλα στο στοιχείο **Αυτή είναι εγκατάσταση συμπλέγματος**. Καθορίστε την **Προσαρμοσμένη διαδρομή δεδομένων εφαρμογής** που θα οδηγεί στον κοινόχρηστο χώρο αποθήκευσης του συμπλέγματος. Τα δεδομένα πρέπει να αποθηκευτούν σε μία τοποθεσία στην οποία έχουν πρόσβαση όλοι οι κόμβοι που περιλαμβάνονται στο σύμπλεγμα.

5. Επιλέξτε το στοιχείο **Λογαριασμός χρήστη υπηρεσίας**. Αυτός ο λογαριασμός θα χρησιμοποιηθεί για την εκτέλεση της υπηρεσίας διακομιστή του ESET PROTECT. Είναι διαθέσιμες οι παρακάτω επιλογές:

- **Λογαριασμός υπηρεσίας δικτύου** - Ενεργοποιήστε αυτή την επιλογή εάν δεν χρησιμοποιείτε τομέα.

- **Προσαρμοσμένος λογαριασμός**: δώστε τα διαπιστευτήρια χρήστη τομέα: ΤΟΜΕΑΣ\ΟΝΟΜΑ ΧΡΗΣΤΗ και κωδικός πρόσβασης.



6. Συνδεθείτε σε μια βάση δεδομένων. Εδώ αποθηκεύονται όλα τα δεδομένα, (κωδικός πρόσβασης της κονσόλας διαδικτύου ESET PROTECT, τα αρχεία καταγραφής του υπολογιστή-πελάτη, κ.λπ.):

• **Βάση δεδομένων**: MySQL Server/MS SQL Server/MS SQL Server via Windows Authentication

• **Πρόγραμμα οδήγησης ODBC**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/MySQL ODBC 8.1 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server

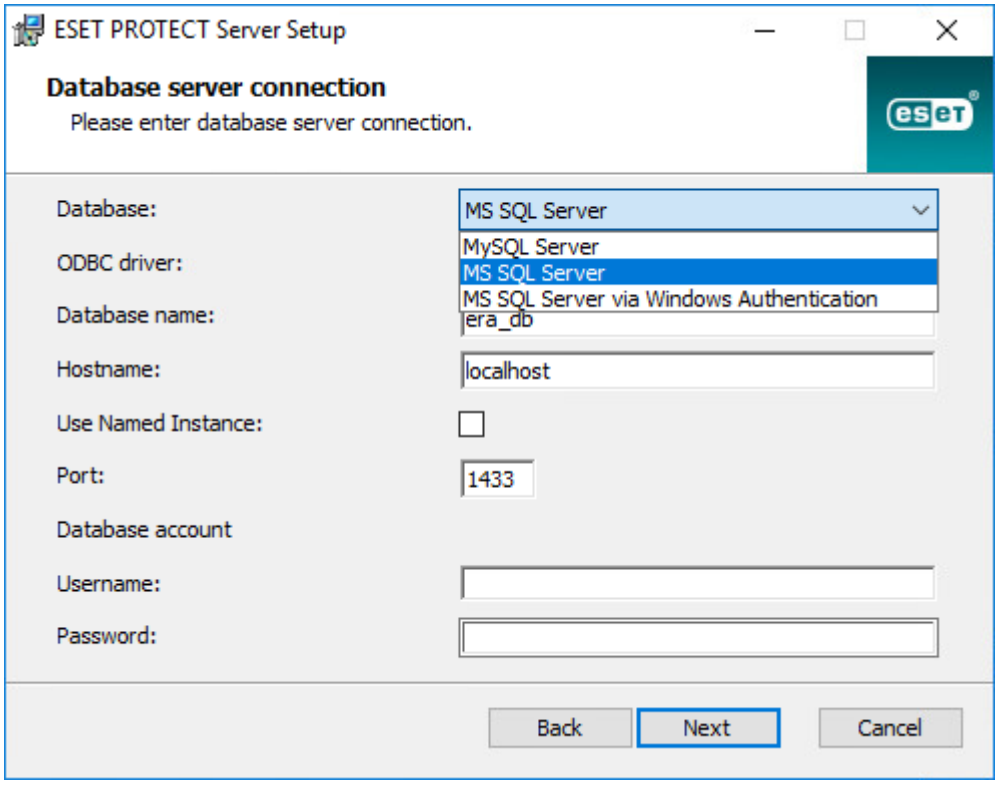
• **Όνομα βάσης δεδομένων**: Συνιστάται να χρησιμοποιήσετε το προκαθορισμένο όνομα ή να το αλλάξετε, εάν απαιτείται.

• **Όνομα κεντρικού υπολογιστή**: όνομα κεντρικού υπολογιστή ή διεύθυνση IP του διακομιστή βάσης δεδομένων σας

• **Θύρα**: χρησιμοποιείται για σύνδεση με το διακομιστή βάσης δεδομένων

• **Όνομα χρήστη/Κωδικός πρόσβασης** του λογαριασμού διαχειριστή βάσης δεδομένων

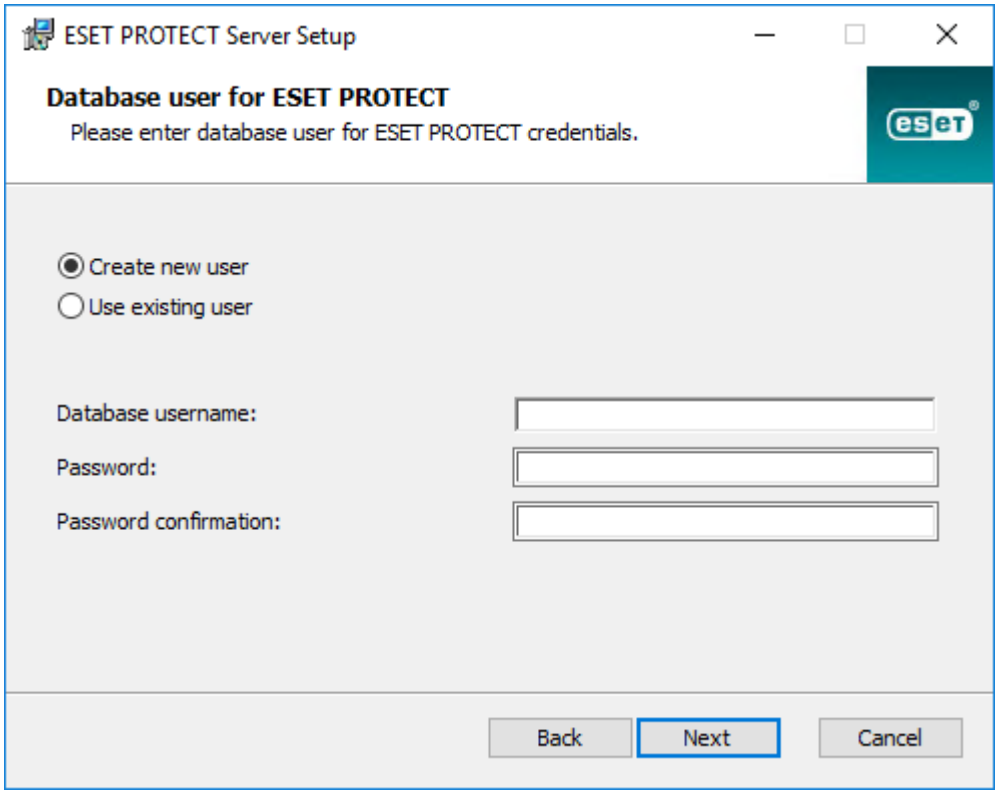
• **Χρήση ονόματος παρουσίας** - Εάν χρησιμοποιείτε βάση δεδομένων Microsoft SQL, μπορείτε να επιλέξετε το πλαίσιο ελέγχου **Χρήση ονόματος παρουσίας** για να χρησιμοποιήσετε μια προσαρμοσμένη παρουσία βάσης δεδομένων. Μπορείτε να τη ρυθμίσετε στο πεδίο **Όνομα κεντρικού υπολογιστή** με τη μορφή *HOSTNAME\DB_INSTANCE* (για παράδειγμα, *192.168.0.10\ESMC7SQL*. Για βάση δεδομένων σε σύμπλεγμα, χρησιμοποιήστε μόνο το όνομα συμπλέγματος. Εάν ορίσετε αυτήν την επιλογή, δεν μπορείτε να αλλάξετε τη θύρα σύνδεσης της βάσης δεδομένων - το σύστημα θα χρησιμοποιεί τις προεπιλεγμένες θύρες που προσδιορίζονται από την Microsoft. Για να συνδέσετε τον Διακομιστή ESET PROTECT με τη βάση δεδομένων Microsoft SQL που είναι εγκατεστημένη σε ένα σύμπλεγμα ανακατεύθυνσης, εισαγάγετε το όνομα συμπλέγματος στο πεδίο **Όνομα κεντρικού υπολογιστή**.



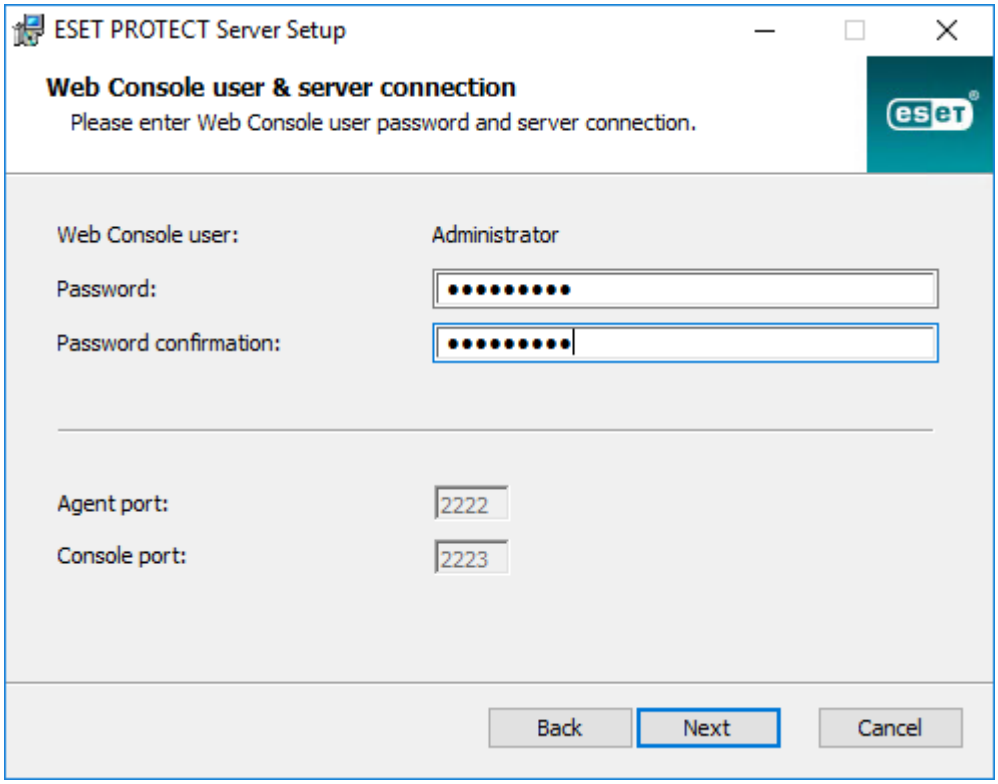
Ο διακομιστής ESET PROTECT αποθηκεύει μεγάλα μπλοκ δεδομένων στη βάση δεδομένων. Συνεπώς, είναι απαραίτητο να ρυθμιστούν οι παράμετροι του MySQL, έτσι ώστε να αποδέχεται μεγάλα πακέτα, προκειμένου να λειτουργεί σωστά το ESET PROTECT On-Prem.

Αυτό το βήμα θα επαληθεύσει τη σύνδεσή σας με τη βάση δεδομένων. Εάν η σύνδεση είναι καλή, προχωρήστε στο επόμενο βήμα.

7. Επιλέξτε ένα χρήστη για το ESET PROTECT On-Prem, ο οποίος έχει πρόσβαση στη βάση δεδομένων. Μπορείτε να χρησιμοποιήσετε έναν υπάρχοντα χρήστη ή μπορεί να δημιουργήσει έναν χρήστη η ρύθμιση.



8. Εισαγάγετε έναν κωδικό πρόσβασης για την πρόσβαση στην **Κονσόλα διαδικτύου**.



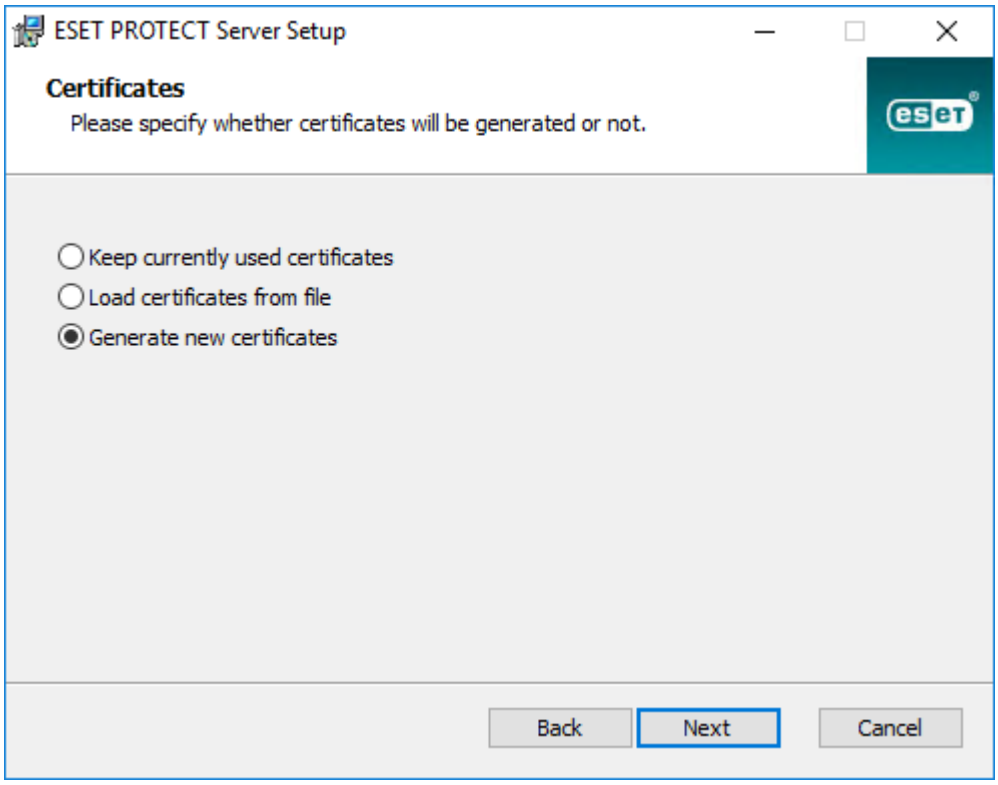
9. Το ESET PROTECT On-Prem χρησιμοποιεί πιστοποιητικά για την επικοινωνία υπολογιστή-πελάτη με το διακομιστή. Επιλέξτε μία από τις παρακάτω επιλογές:

• **Διατήρηση πιστοποιητικών που χρησιμοποιούνται αυτή τη στιγμή** - Αυτή η επιλογή είναι διαθέσιμη μόνο εάν η βάση δεδομένων χρησιμοποιούνταν ήδη με άλλον διακομιστή ESET PROTECT προηγουμένως.

• **Φόρτωση πιστοποιητικών από αρχείο** - Επιλέξτε το υπάρχον πιστοποιητικό διακομιστή και

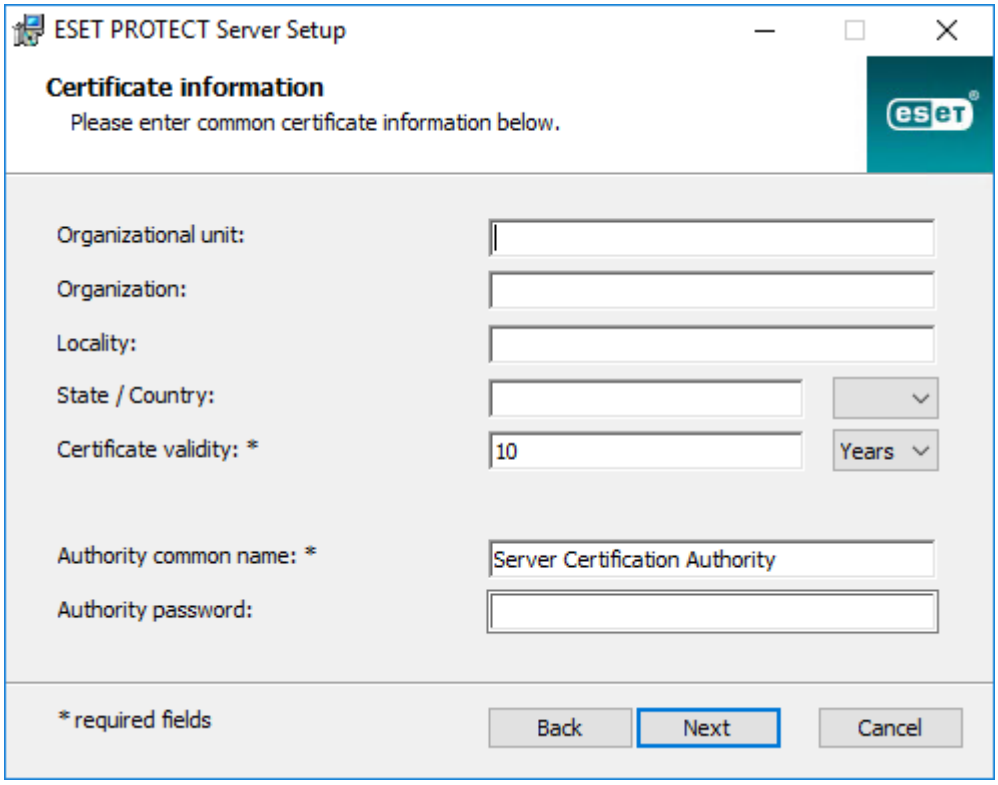
την αρχή έκδοσης πιστοποιητικού.

• **Δημιουργία νέων πιστοποιητικών** - Το πρόγραμμα εγκατάστασης δημιουργεί νέα πιστοποιητικά.



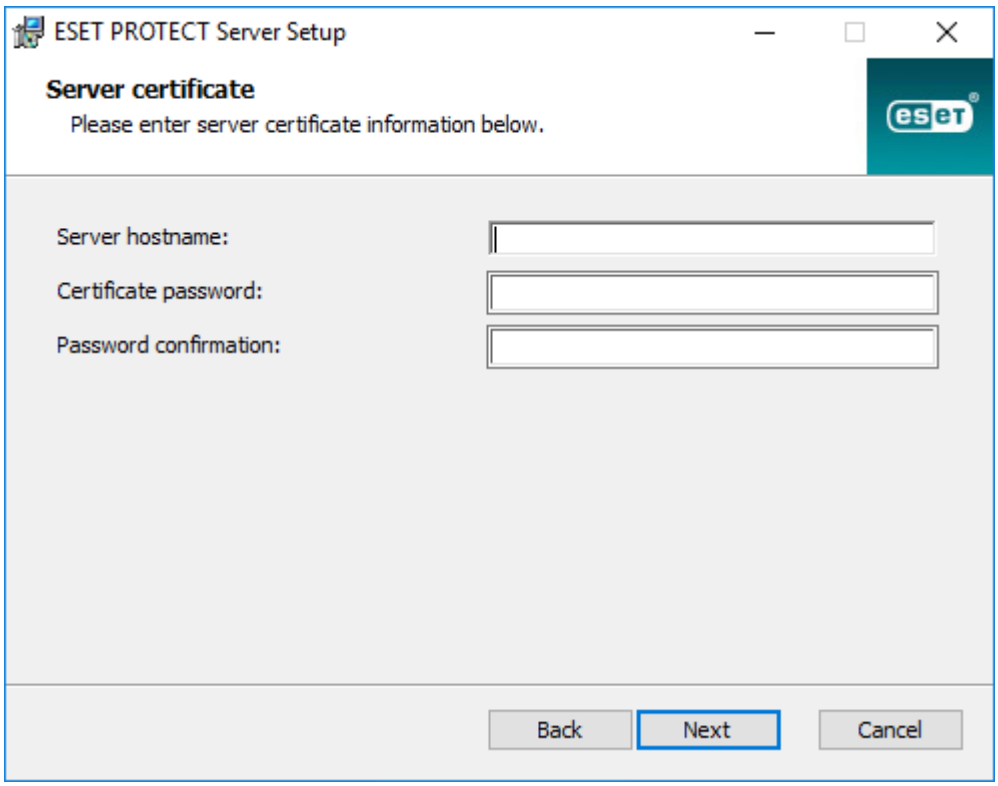
10. Ακολουθήστε αυτό το βήμα εάν είχατε ενεργοποιήσει την επιλογή **Δημιουργία νέων πιστοποιητικών** στο προηγούμενο βήμα.

a)Καθορίστε πρόσθετες πληροφορίες σχετικά με τα πιστοποιητικά (προαιρετικά). Εάν συμπληρώσετε το στοιχείο **Κωδικός πρόσβασης αρχής έκδοσης πιστοποιητικού**, φροντίστε να τον απομνημονεύσετε.

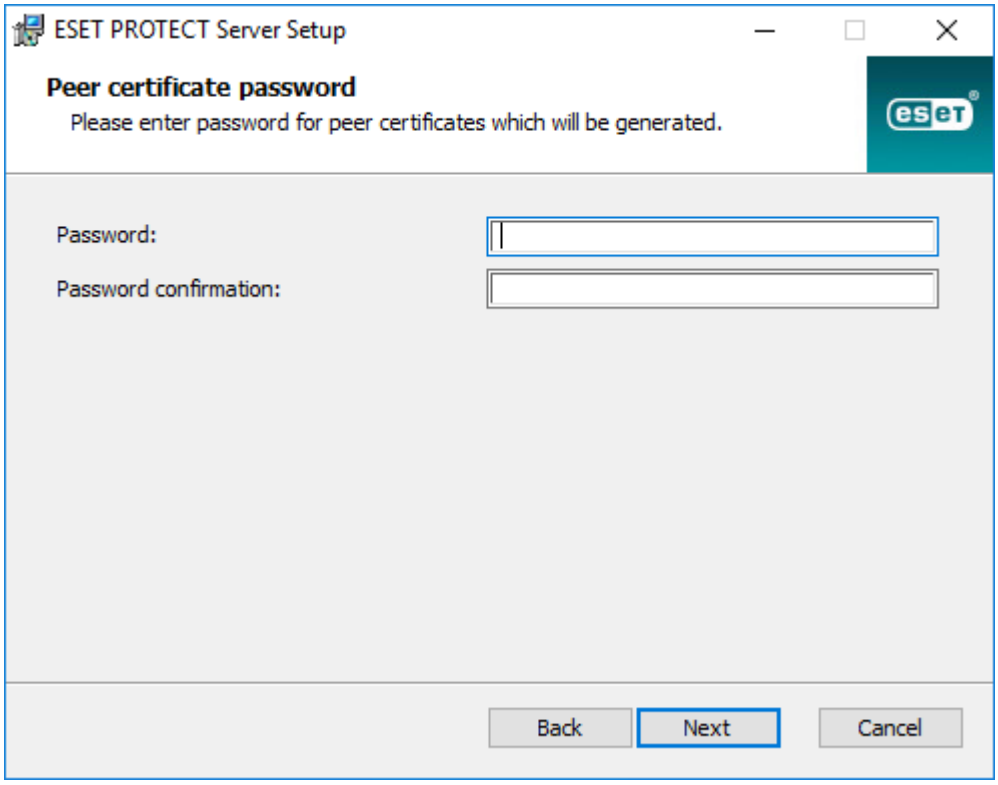


b)Στο πεδίο **Πιστοποιητικό διακομιστή**, πληκτρολογήστε το **Όνομα κεντρικού υπολογιστή διακομιστή** και συμπληρώστε το στοιχείο **Κωδικός πρόσβασης πιστοποιητικού** (προαιρετικά).

Το **Όνομα κεντρικού υπολογιστή διακομιστή** στο πιστοποιητικό διακομιστή δεν πρέπει να περιέχει καμία από τις ακόλουθες λέξεις κλειδιά: `server`, `proxy`, `agent`.

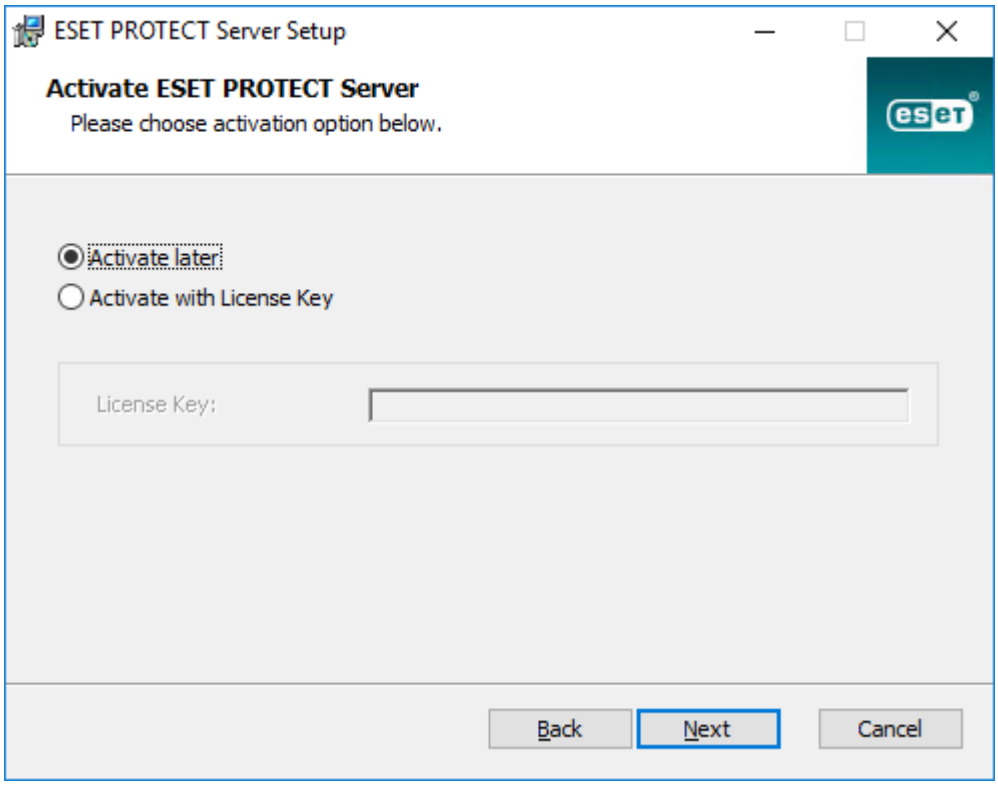


c)Στο πεδίο **Κωδικός πρόσβασης ομότιμου πιστοποιητικού**, πληκτρολογήστε τον κωδικό πρόσβασης για τα ομότιμα πιστοποιητικά του φορέα και του διακομιστή μεσολάβησης.



11. Η ρύθμιση μπορεί να εκτελέσει μια αρχική εργασία συγχρονισμού στατικής ομάδας. Επιλέξτε τη μέθοδο (**Να μη γίνει συγχρονισμός**, **Συγχρονισμός με το δίκτυο των Windows**, **Συγχρονισμός με το Active Directory**) και κάντε κλικ στο **Επόμενο**.

12. Εισαγάγετε ένα έγκυρο Κλειδί άδειας χρήσης ή επιλέξτε **Ενεργοποίηση αργότερα**.



13. Επιβεβαιώστε ή αλλάξτε το φάκελο εγκατάστασης για το διακομιστή και κάντε κλικ στο **Επόμενο**.

14. Κάντε κλικ στο στοιχείο **Εγκατάσταση** για να εγκαταστήσετε το διακομιστή ESET PROTECT.

Όταν ολοκληρώσετε την εγκατάσταση του διακομιστή ESET PROTECT, μπορείτε να εγκαταστήσετε τον φορέα ESET Management στον ίδιο υπολογιστή (προαιρετικά) για να ενεργοποιήσετε τη διαχείριση του διακομιστή με τον ίδιο τρόπο που διαχειρίζεστε έναν υπολογιστή-πελάτη.

Απαιτήσεις Microsoft SQL Server

Πρέπει να ικανοποιούνται οι ακόλουθες απαιτήσεις για το Microsoft SQL Server:

• Εγκαταστήστε μια υποστηριζόμενη έκδοση του Microsoft SQL Server. Κατά την εγκατάσταση, επιλέξτε έλεγχο ταυτότητας με **Μεικτή λειτουργία**.

• Εάν είναι ήδη εγκατεστημένο το Microsoft SQL Server, ρυθμίστε τον έλεγχο ταυτότητας σε **Μεικτή λειτουργία (Έλεγχος ταυτότητας SQL Server και έλεγχος ταυτότητας Windows)**. Για να το κάνετε αυτό, ακολουθήστε τις οδηγίες σε αυτό το άρθρο της Γνωσιακής βάσης. Εάν θέλετε να χρησιμοποιείται ο **Έλεγχος ταυτότητας Windows** για τη σύνδεση στο Microsoft SQL Server, ακολουθήστε τα βήματα σε αυτό το άρθρο της Γνωσιακής βάσης.

• Θα πρέπει να επιτρέπονται συνδέσεις TCP/IP με το SQL Server. Για να το κάνετε αυτό, ακολουθήστε τις οδηγίες σε αυτό το άρθρο της Γνωσιακής βάσης από το μέρος **II. Να επιτρέπονται συνδέσεις TCP/IP με τη βάση δεδομένων SQL**.

• Για τη ρύθμιση παραμέτρων, διαχείριση και διανομή του Microsoft SQL Server (βάσεις δεδομένων και χρήστες), πραγματοποιήστε λήψη του SQL Server Management Studio (SSMS).
• Μην εγκαταστήσετε το SQL Server σε έναν Ελεγκτή τομέα (για παράδειγμα, Windows SBS / Essentials). Συνιστάται να εγκαταστήσετε το ESET PROTECT On-Prem σε διαφορετικό διακομιστή ή να μην επιλέξετε το στοιχείο του SQL Server Express κατά την εγκατάσταση (αυτό απαιτεί να χρησιμοποιήσετε το υπάρχον SQL ή MySQL Server για την εκτέλεση της βάσης δεδομένων ESET PROTECT).

Εγκατάσταση και διαμόρφωση του MySQL Server

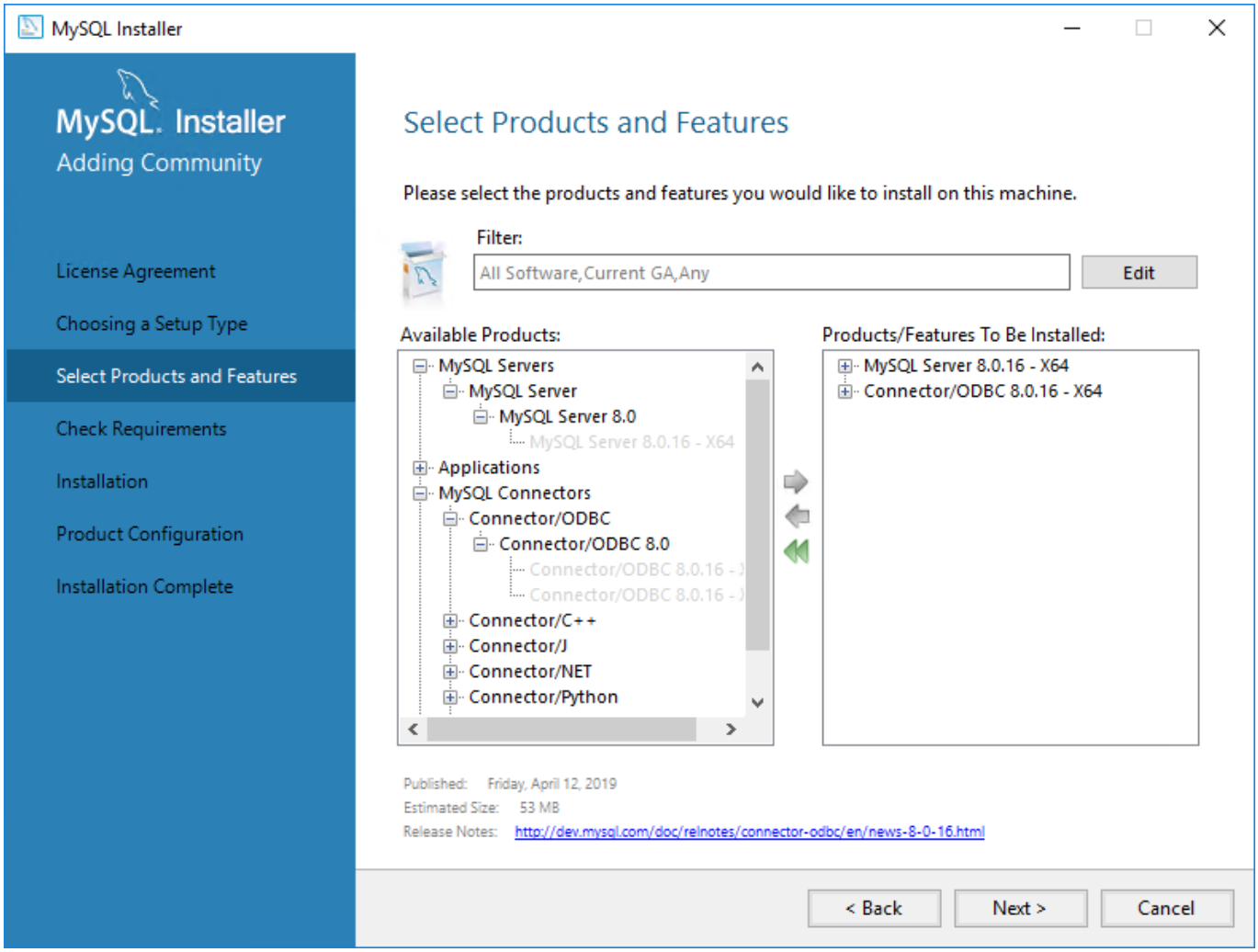
Εγκατάσταση

Βεβαιωθείτε ότι έχετε εγκαταστήσει μια υποστηριζόμενη έκδοση του διακομιστή MySQL και της σύνδεσης ODBC.

1. Κάντε λήψη του προγράμματος εγκατάστασης Windows MySQL 8 από τη διεύθυνση https://dev.mysql.com/downloads/installer/ και εκτελέστε το.

2. Επιλέξτε το πλαίσιο ελέγχου **Αποδέχομαι τους όρους άδειας χρήσης** και κάντε κλικ στο κουμπί **Επόμενο**.

3. Κατά τη ρύθμιση της εγκατάστασης, επιλέξτε **Προσαρμοσμένη** και **Διακομιστής MySQL Server** και **Σύνδεση/ODBC** για να εκτελέσετε την εγκατάσταση. Βεβαιωθείτε ότι η Σύνδεση ODBC αντιστοιχεί στα bit του εγκατεστημένου διακομιστή MySQL Server (x86 ή x64).



4. Κάντε κλικ στο στοιχείο **Επόμενο** και επιλέξτε **Εκτέλεση** για να εγκαταστήσετε το MySQL και το ODBC Connector.

5. Κάντε κλικ στο στοιχείο**Επόμενο**. Στο στοιχείο **Υψηλή διαθεσιμότητα**, επιλέξτε **Ανεξάρτητο MySQL Server / Κλασική αντιγραφή MySQL** και κάντε κλικ στο στοιχείο **Επόμενο**.

6. Στο στοιχείο **Τύπος και δικτύωση**, επιλέξτε το στοιχείο **Υπολογιστής διακομιστή** από το αναπτυσσόμενο μενού **Τύπος ρύθμισης παραμέτρων** και κάντε κλικ στο στοιχείο **Επόμενο**.

7. Στο στοιχείο **Μέθοδος ελέγχου ταυτότητας**, κάντε τη συνιστώμενη επιλογή **Χρήση ισχυρής κρυπτογράφησης κωδικού πρόσβασης για έλεγχο ταυτότητας** και κάντε κλικ στο στοιχείο **Επόμενο**.

8. Στο στοιχείο **Λογαριασμοί και Ρόλοι**, πληκτρολογήστε δύο φορές τις πληροφορίες του στοιχείου **Ριζικός κωδικός πρόσβασης MySQL**. Συνιστάται επίσης να δημιουργήσετε έναν αποκλειστικό λογαριασμό χρήστη βάσης δεδομένων.

9. Στο στοιχείο **Υπηρεσία των Windows**, διατηρήστε τις προκαθορισμένες τιμές και κάντε κλικ στο στοιχείο **Επόμενο**.

10. Κάντε κλικ στο στοιχείο **Εκτέλεση** και περιμένετε μέχρι να ολοκληρωθεί η εγκατάσταση του διακομιστή MySQL. Κάντε κλικ στα στοιχεία **Τέλος**, **Επόμενο** και **Τέλος** για να κλείσετε το παράθυρο εγκατάστασης.

Διαμόρφωση

1. Ανοίξτε το παρακάτω αρχείο σε ένα πρόγραμμα επεξεργασίας κειμένου:

C:\ProgramData\MySQL\MySQL Server 8.0\my.ini

2. Βρείτε να επεξεργαστείτε ή επισυνάψτε την παρακάτω διαμόρφωση στην ενότητα `[mysqld]` του αρχείου *my.ini*:

- Δημιουργήστε την ενότητα `[mysqld]` εάν δεν υπάρχει στο αρχείο.
- Εάν οι παράμετροι δεν υπάρχουν στο αρχείο, προσθέστε τις στην ενότητα `[mysqld]`.
- Για να προσδιορίσετε την έκδοση MySQL, εκτελέστε την εντολή: `mysql --version`

Παράμετρος	Σχόλια και συνιστώμενες τιμές	έκδοση MySQL
`max_allowed_packet=33M`		Όλες οι υποστηριζόμενες εκδόσεις.
`log_bin_trust_function_creators=1`	Εναλλακτικά, μπορείτε να απενεργοποιήσετε τη δυαδική καταγραφή: `log_bin=0`	8.x
`innodb_log_file_size=100M` `innodb_log_files_in_group=2`	Ο πολλαπλασιασμός των τιμών αυτών των δύο παραμέτρων πρέπει να είναι τουλάχιστον **200**. Η ελάχιστη τιμή για την παράμετρο `innodb_log_files_in_group` είναι **2** και η μέγιστη τιμή είναι **100** - η τιμή πρέπει να είναι ακέραιος αριθμός).	8.x 5.7 5.6.22 (και νεότερες εκδόσεις 5.6.x)
`innodb_log_file_size=200M`	Ρυθμίστε την τιμή τουλάχιστον σε **200M**, αλλά όχι μεγαλύτερη από **3000M**.	5.6.20 και 5.6.21

3. Αποθηκεύστε και κλείστε το αρχείο *my.ini*.

4. Ανοίξτε τη γραμμή εντολής και εισαγάγετε τις παρακάτω εντολές για να επανεκκινήσετε το διακομιστή MySQL και να εφαρμόσετε τη διαμόρφωση (το όνομα της διεργασίας εξαρτάται από την έκδοση του MySQL: 8.0 = mysql80 κ.λπ.):

```
net stop mysql80
net start mysql80
```

5. Εισαγάγετε την ακόλουθη εντολή στη γραμμή εντολών για να ελέγξετε εάν εκτελείται ο διακομιστής MySQL:

```
sc query mysql80
```

Αποκλειστικός λογαριασμός χρήστη βάσης δεδομένων

Εάν δεν θέλετε να χρησιμοποιήσετε **λογαριασμό SA** (Microsoft SQL) ή **λογαριασμό ρίζας** (MySQL), μπορείτε να δημιουργήσετε έναν **αποκλειστικό λογαριασμό χρήστη βάσης δεδομένων**. Αυτός ο αποκλειστικός λογαριασμός χρήστη θα χρησιμοποιείται μόνο για την πρόσβαση στη βάση δεδομένων ESET PROTECT. Συνιστούμε να δημιουργήσετε έναν αποκλειστικό λογαριασμό χρήστη βάσης δεδομένων

μέσα στο διακομιστή βάσης δεδομένων προτού ξεκινήσετε την εγκατάσταση του ESET PROTECT On-Prem. Επίσης, θα χρειαστεί να δημιουργήσετε μια κενή βάση δεδομένων στην οποία το ESET PROTECT On-Prem θα έχει πρόσβαση χρησιμοποιώντας αυτό τον αποκλειστικό λογαριασμό χρήστη.

Υπάρχει ένα ελάχιστο σύνολο δικαιωμάτων που πρέπει να εκχωρηθούν σε έναν αποκλειστικό λογαριασμό χρήστη βάσης δεδομένων:

- Δικαιώματα χρήστη MySQL: `ALTER`, `ALTER ROUTINE`, `CREATE`, `CREATE ROUTINE`, `CREATE TEMPORARY TABLES`, `CREATE VIEW`, `DELETE`, `DROP`, `EXECUTE`, `INDEX`, `INSERT`, `LOCK TABLES`, `SELECT`, `UPDATE`, `TRIGGER`. - για περισσότερες πληροφορίες σχετικά με τα δικαιώματα MySQL, ανατρέξτε στη σελίδα http://dev.mysql.com/doc/refman/8.0/en/grant.html.

- Ρόλοι επιπέδου βάσης δεδομένων Microsoft SQL Server: Ο χρήστης της βάσης δεδομένων ESET PROTECT πρέπει να είναι μέλος του ρόλου βάσης δεδομένων db_owner. Για περισσότερες πληροφορίες σχετικά με τους Ρόλους Microsoft SQL Server επιπέδου βάσης δεδομένων, ανατρέξτε στη σελίδα https://msdn.microsoft.com/en-us/library/ms189121%28v=sql.100%29.aspx

Μπορείτε να βρείτε λεπτομερείς οδηγίες για τη ρύθμιση της βάσης δεδομένων και του λογαριασμού χρήστη τόσο για το Microsoft SQL όσο και για το MySQL στο σχετικό άρθρο της Γνωσιακής βάσης.

Εγκατάσταση φορέα – Windows

Διαθέσιμες μέθοδοι

Υπάρχουν διάφορες διαθέσιμες μέθοδοι εγκατάστασης και ανάπτυξης για την εγκατάσταση του φορέα ESET Management σε σταθμούς εργασίας Windows:

Μέθοδος	Τεκμηρίωση	Περιγραφή
Εγκατάσταση με βάση το γραφικό περιβάλλον χρήστη από το πρόγραμμα εγκατάστασης *.msi*	• Αυτό το κεφάλαιο • KB	• Η **τυπική** μέθοδος εγκατάστασης. • Αυτή η μέθοδος μπορεί να εκτελεστεί ως εγκατάσταση με υποβοήθηση διακομιστή ή εκτός σύνδεσης. • Χρησιμοποιήστε αυτή τη μέθοδο εάν πραγματοποιείτε εγκατάσταση φορέα σε υπολογιστή διακομιστή ESET PROTECT.
ESET Remote Deployment Tool	• Ηλεκτρονική βοήθεια	• Συνιστάται για μαζική ανάπτυξη σε τοπικό δίκτυο. • Μπορεί να χρησιμοποιηθεί για την ανάπτυξη του προγράμματος εγκατάστασης «Όλα-σε-ένα» (Φορέας + προϊόν ασφάλειας ESET)
Πρόγραμμα εγκατάστασης φορέα «Όλα σε ένα»	• Δημιουργία προγράμματος εγκατάστασης φορέα "όλα σε ένα" • KB	• Το πρόγραμμα εγκατάστασης μπορεί να περιλαμβάνει επίσης ένα προϊόν ασφάλειας και ενσωματωμένη πολιτική. • Το μέγεθος του προγράμματος εγκατάστασης είναι αρκετές εκατοντάδες MB.
Δέσμη ενεργειών προγράμματος εγκατάστασης φορέα	• Δημιουργία προγράμματος εγκατάστασης δέσμης ενεργειών φορέα • KB	• Το πρόγραμμα εγκατάστασης είναι μια εκτελέσιμη δέσμη ενεργειών. Έχει μικρό μέγεθος αλλά χρειάζεται πρόσβαση στην τοποθεσία του προγράμματος εγκατάστασης *.msi*. • Μπορείτε να επεξεργαστείτε τη δέσμη ενεργειών για να χρησιμοποιήσετε ένα τοπικό πρόγραμμα εγκατάστασης και διακομιστή μεσολάβησης HTTP.
Ανάπτυξη SCCM και GPO	• SCCM • GPO • KB	• Μέθοδος απομακρυσμένης μαζικής ανάπτυξης για προχωρημένους. • Με χρήση ενός μικρού αρχείου *.ini*.
Εργασία διακομιστή - Ανάπτυξη φορέα	• Ηλεκτρονική βοήθεια • KB	• Μια εναλλακτική στα SCCM και GPO. • Δεν είναι εφικτό μέσω του διακομιστή μεσολάβησης HTTP. • Εκτελείται από το διακομιστή ESET PROTECT από την κονσόλα διαδικτύου ESET PROTECT. • Χρησιμοποιήστε αυτήν τη μέθοδο για να αναπτύξετε τον φορέα ESET Management στους υπολογιστές που συγχρονίζονται από το Active Directory.

Το πρωτόκολλο επικοινωνίας μεταξύ του φορέα και του διακομιστή ESET PROTECT δεν υποστηρίζει τον έλεγχο ταυτότητας. Οποιαδήποτε λύση διακομιστή μεσολάβησης που χρησιμοποιείται για προώθηση της επικοινωνίας του φορέα στο διακομιστή ESET PROTECT και απαιτεί έλεγχο ταυτότητας δεν θα λειτουργεί.
Εάν επιλέξετε να χρησιμοποιήσετε μια μη προεπιλεγμένη θύρα για την Κονσόλα διαδικτύου ή το φορέα, ενδέχεται να απαιτείται προσαρμογή του τείχους προστασίας. Διαφορετικά, η εγκατάσταση μπορεί να αποτύχει.

Εγκατάσταση με βάση το γραφικό περιβάλλον χρήστη

Ακολουθήστε τα παρακάτω βήματα για να εγκαταστήσετε το στοιχείο φορέα ESET Management τοπικά σε Windows:

1. Επισκεφτείτε την ενότητα λήψεων του ESET PROTECT για λήψη ενός ανεξάρτητου προγράμματος εγκατάστασης για αυτό το στοιχείο του ESET PROTECT (*agent_x86.msi* ή *agent_x64.msi*ή *agent_arm64.msi*).

2. Εκτελέστε το πρόγραμμα εγκατάστασης του φορέα ESET Management και αποδεχτείτε το EULA, εάν συμφωνείτε.

3. Επιλέξτε το πλαίσιο ελέγχου **Συμμετοχή στο πρόγραμμα βελτίωσης προϊόντος**, για να αποστέλλονται ανώνυμα δεδομένα τηλεμετρίας και αναφορές σφαλμάτων στην ESET (έκδοση και τύπος λειτουργικού συστήματος, έκδοση προϊόντος ESET και άλλες πληροφορίες ειδικά για το προϊόν).

4. Εισαγάγετε τα στοιχεία **Κεντρικός υπολογιστής διακομιστή** (όνομα κεντρικού υπολογιστή ή διεύθυνση IP του διακομιστή ESET PROTECT) και **Θύρα διακομιστή** (η προεπιλεγμένη θύρα είναι 2222 - εάν χρησιμοποιείτε διαφορετική θύρα, τότε αντικαταστήστε την προεπιλεγμένη θύρα με τον προσαρμοσμένο αριθμό θύρας).

Βεβαιωθείτε ότι ο **Κεντρικός υπολογιστής διακομιστή** αντιστοιχεί σε μία τουλάχιστον από τις τιμές (υπό ιδανικές συνθήκες με το FQDN) που καθορίζονται στο πεδίο **Κεντρικός υπολογιστής** του στοιχείου **Πιστοποιητικό διακομιστή**. Διαφορετικά θα προκύψει σφάλμα που θα αναφέρει 'Το πιστοποιητικό διακομιστή που λήφθηκε δεν είναι έγκυρο'. Με τη χρήση του ειδικού χαρακτήρα (*) στο πεδίο «Κεντρικός υπολογιστής πιστοποιητικού διακομιστή», το πιστοποιητικό θα μπορεί να λειτουργήσει με οποιονδήποτε **Κεντρικό υπολογιστή διακομιστή**.

5. Εάν χρησιμοποιείτε διακομιστή μεσολάβησης για σύνδεση φορέα - διακομιστή, επιλέξτε το πλαίσιο ελέγχου δίπλα στην επιλογή **Χρήση διακομιστή μεσολάβησης**. Εάν επιλεγεί, το πρόγραμμα εγκατάστασης θα συνεχίσει με εγκατάσταση χωρίς σύνδεση.

Αυτή η ρύθμιση διακομιστή μεσολάβησης χρησιμοποιείται μόνο για (αντιγραφή) μεταξύ φορέα ESET Management και διακομιστή ESET PROTECT, όχι για αποθήκευση των ενημερώσεων στην προσωρινή μνήμη.
• **Όνομα κεντρικού υπολογιστή διακομιστή μεσολάβησης**: όνομα κεντρικού υπολογιστή ή διεύθυνση IP του υπολογιστή του διακομιστή μεσολάβησης HTTP.
• **Θύρα διακομιστή μεσολάβησης**: η προεπιλεγμένη τιμή είναι 3128.
• **Όνομα χρήστη**, **Κωδικός πρόσβασης**: εισαγάγετε τα διαπιστευτήρια που χρησιμοποιούνται από τον διακομιστή μεσολάβησης, αν χρησιμοποιείται έλεγχος ταυτότητας.
Μπορείτε να αλλάξετε τις ρυθμίσεις διακομιστή μεσολάβησης αργότερα στην πολιτική. Ο διακομιστής μεσολάβησης πρέπει να είναι εγκατεστημένος, για να μπορείτε να διαμορφώσετε μια σύνδεση φορέα - διακομιστή μέσω διακομιστή μεσολάβησης.

6. Επιλέξτε μία από τις ακόλουθες επιλογές εγκατάστασης και ακολουθήστε τα βήματα από την κατάλληλη ενότητα παρακάτω:

- Εγκατάσταση με υποβοήθηση διακομιστή - Θα πρέπει να δώσετε τα διαπιστευτήρια διαχειριστή της κονσόλας διαδικτύου ESET PROTECT. Το πρόγραμμα εγκατάστασης θα λάβει αυτόματα τα απαιτούμενα πιστοποιητικά.

Δεν μπορείτε να χρησιμοποιήσετε έναν χρήστη με έλεγχο ταυτότητας δύο παραγόντων για εγκαταστάσεις με υποβοήθηση του διακομιστή.

- Εγκατάσταση χωρίς σύνδεση - Θα πρέπει να παράσχετε ένα Πιστοποιητικό φορέα και μια Αρχή έκδοσης πιστοποιητικού. Μπορείτε να εξαγάγετε και τα δύο από το ESET PROTECT On-Prem. Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το προσαρμοσμένο πιστοποιητικό σας.

Εγκατάσταση από τη γραμμή εντολών

Το πρόγραμμα εγκατάστασης *MSI* μπορεί να εκτελεστεί τοπικά ή απομακρυσμένα. Κάντε λήψη του Φορέα ESET Management από τον ιστότοπο της ESET.

Παράμετρος	Περιγραφή και επιτρεπόμενες τιμές
P_HOSTNAME=	Όνομα κεντρικού υπολογιστή ή διεύθυνση IP του διακομιστή ESET PROTECT.
P_PORT=	Θύρα διακομιστή για σύνδεση με το φορέα (προαιρετικά, εάν δεν καθοριστεί, χρησιμοποιείται η προεπιλεγμένη θύρα 2222).
P_CERT_PATH=	Διαδρομή για το Πιστοποιητικό φορέα σε μορφή Base64 στο αρχείο *.txt* (που εξάγεται από την κονσόλα διαδικτύου ESET PROTECT).
P_CERT_AUTH_PATH=	Διαδρομή για την Αρχή έκδοσης πιστοποιητικού σε μορφή Base64 στο αρχείο *.txt* (που εξάγεται από την κονσόλα διαδικτύου ESET PROTECT).
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	**YES**. Χρησιμοποιήστε αυτή την παράμετρο όταν αναφέρεστε στο Πιστοποιητικό φορέα και στην Αρχή έκδοσης πιστοποιητικού που είναι αποθηκευμένη στα αρχεία *.txt*.
P_CERT_PASSWORD=	Χρησιμοποιήστε αυτή την παράμετρο για να παράσχετε έναν κωδικό πρόσβασης για το Πιστοποιητικό φορέα.
P_CERT_CONTENT=	Συμβολοσειρά για το Πιστοποιητικό φορέα σε μορφή Base64 (που εξάγεται από την κονσόλα διαδικτύου ESET PROTECT).
P_CERT_AUTH_CONTENT=	Συμβολοσειρά για την Αρχή έκδοσης πιστοποιητικού σε μορφή Base64 (που εξάγεται από την κονσόλα διαδικτύου ESET PROTECT).
PASSWORD=	Κωδικός πρόσβασης για την κατάργηση εγκατάστασης ενός φορέα που προστατεύεται με κωδικό πρόσβασης.
P_ENABLE_TELEMETRY=	**0** - ανενεργό (προεπιλογή), **1** - ενεργό. Αποστολή αναφορών διακοπής λειτουργίας και δεδομένων τηλεμετρίας στην ESET (προαιρετική παράμετρος).
P_INSTALL_MODE_EULA_ONLY=	**1**. Χρησιμοποιήστε αυτή την παράμετρο για ημι-αθόρυβη εγκατάσταση φορέα ESET Management. Μπορείτε να δείτε το παράθυρο της Εγκατάστασης φορέα και θα σας ζητηθεί να αποδεχτείτε τη Συμφωνία Άδειας Χρήσης Τελικού Χρήστη και να ενεργοποιήσετε/απενεργοποιήσετε τα δεδομένα τηλεμετρίας (εάν καθοριστεί, παραβλέπεται η παράμετρος P_ENABLE_TELEMETRY). Άλλες ρυθμίσεις εγκατάστασης φορέα λαμβάνονται από τις παραμέτρους γραμμής εντολών. Μπορείτε να δείτε την ολοκλήρωση της διεργασίας «Εγκατάσταση φορέα».
P_USE_PROXY=	**1**. Χρησιμοποιήστε αυτή την παράμετρο για να ενεργοποιήσετε τη χρήση του διακομιστή μεσολάβησης HTTP (ο οποίος είναι ήδη εγκατεστημένος στο δίκτυό σας) για αντιγραφή μεταξύ του Φορέα ESET Management και του Διακομιστή ESET PROTECT (όχι για προσωρινή αποθήκευση ενημερώσεων).
P_PROXY_HTTP_HOSTNAME=	Όνομα κεντρικού υπολογιστή ή διεύθυνση IP του διακομιστή μεσολάβησης HTTP.
P_PROXY_HTTP_PORT=	Θύρα διακομιστή μεσολάβησης HTTP για σύνδεση με το Φορέα.

Παραδείγματα εγκατάστασης από τη γραμμή εντολών

Αντικαταστήστε τον πορτοκαλί κώδικα παρακάτω, όπως απαιτείται.

- Αθόρυβη εγκατάσταση (παράμετρος `/q`) με σύνδεση προεπιλεγμένης θύρας, ενεργοποιημένα δεδομένα τηλεμετρίας και πιστοποιητικό φορέα και Αρχή έκδοσης πιστοποιητικού αποθηκευμένα στα αρχεία:

```
Agent_x64.msi /q P_HOSTNAME=10.20.30.40 P_ENABLE_TELEMETRY=1 P_CERT_PATH=C:\Users\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

- Αθόρυβη εγκατάσταση με παρεχόμενες συμβολοσειρές για το πιστοποιητικό φορέα και για την Αρχή έκδοσης πιστοποιητικού, και κωδικό πρόσβασης πιστοποιητικού φορέα και παραμέτρους διακομιστή μεσολάβησης HTTP:

```
Agent_x64.msi /q P_HOSTNAME=protect_server_name P_ENABLE_TELEMETRY=1 P_CERT_CONTENT=CJfXtf1kZqlZKAl9P48HymBHa3CkW P_CERT_PASSWORD=abcd1234EFGH P_CERT_AUTH_CONTENT=45hvkpqayzjJZhSY8qswDQYJKoZIhvc P_USE_PROXY=1 P_PROXY_HTTP_HOSTNAME=proxy_server P_PROXY_HTTP_PORT=3128
```

- Ημι-αθόρυβη εγκατάσταση:

```
Agent_x64.msi P_INSTALL_MODE_EULA_ONLY=1 P_HOSTNAME=10.20.30.40 P_CERT_PATH=C:\Users
```

\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES

Εγκατάσταση φορέα με υποβοήθηση διακομιστή

Για να συνεχίσετε την **εγκατάσταση φορέα με υποβοήθηση διακομιστή** ακολουθήστε τα εξής βήματα:

1. Εισαγάγετε το όνομα κεντρικού υπολογιστή ή τη διεύθυνση IP της Κονσόλας διαδικτύου ESET PROTECT (ίδια με του διακομιστή ESET PROTECT) στο πεδίο **Κεντρικός υπολογιστής διακομιστή**. Αφήστε τη ρύθμιση του στοιχείου **Θύρα κονσόλας διαδικτύου** στην προεπιλεγμένη θύρα 2223, εάν δεν χρησιμοποιείτε προσαρμοσμένη θύρα. Επίσης, εισαγάγετε τα διαπιστευτήρια του λογαριασμού της Κονσόλας διαδικτύου στα πεδία **Όνομα χρήστη και Κωδικός πρόσβασης**. Για να συνδεθείτε ως χρήστης τομέα, επιλέξτε το πλαίσιο ελέγχου που βρίσκεται δίπλα στο στοιχείο **Σύνδεση στον τομέα**.

> • Βεβαιωθείτε ότι ο **Κεντρικός υπολογιστής διακομιστή** αντιστοιχεί σε μία τουλάχιστον από τις τιμές (υπό ιδανικές συνθήκες με το FQDN) που καθορίζονται στο πεδίο **Κεντρικός υπολογιστής** του στοιχείου **Πιστοποιητικό διακομιστή**. Διαφορετικά θα προκύψει σφάλμα που θα αναφέρει 'Το πιστοποιητικό διακομιστή που λήφθηκε δεν είναι έγκυρο'. Η μόνη εξαίρεση είναι σε περίπτωση που υπάρχει ειδικός χαρακτήρας (*) στο πεδίο κεντρικού υπολογιστή του πιστοποιητικού διακομιστή, πράγμα που σημαίνει ότι θα λειτουργήσει με οποιονδήποτε **Κεντρικό υπολογιστή διακομιστή**.
> • Δεν μπορείτε να χρησιμοποιήσετε έναν χρήστη με έλεγχο ταυτότητας δύο παραγόντων για εγκαταστάσεις με υποβοήθηση του διακομιστή.

2. Όταν ερωτηθείτε εάν θέλετε να αποδεχτείτε το πιστοποιητικό, επιλέξτε **Ναι'**.

3. Επιλέξτε το στοιχείο **Να μη δημιουργηθεί υπολογιστής (ο υπολογιστής θα δημιουργηθεί αυτόματα κατά την πρώτη σύνδεση)** ή **Επιλογή προσαρμοσμένης στατικής ομάδας**. Εάν επιλέξετε **Επιλογή προσαρμοσμένης στατικής ομάδας** θα μπορείτε να επιλέξετε από μια λίστα υφιστάμενων στατικών ομάδων στο ESET PROTECT On-Prem. Ο υπολογιστής θα προστεθεί στην ομάδα που επιλέξατε.

4. Καθορίστε έναν φάκελο προορισμού για το φορέα ESET Management (συνιστάται να χρησιμοποιήσετε την προεπιλεγμένη τοποθεσία), επιλέξτε **Επόμενο** και στη συνέχεια **Εγκατάσταση**.

Εγκατάσταση φορέα χωρίς σύνδεση

Για να συνεχίσετε την **εγκατάσταση φορέα χωρίς σύνδεση** ακολουθήστε τα εξής βήματα:

1. Εάν επιλέξατε **Χρήση διακομιστή μεσολάβησης** στο προηγούμενο βήμα, συμπληρώστε το **Όνομα κεντρικού υπολογιστή διακομιστή μεσολάβησης**, τη **Θύρα διακομιστή μεσολάβησης** (η προεπιλεγμένη θύρα είναι 3128), το **Όνομα χρήστη** και τον **Κωδικό πρόσβασης** και κάντε κλικ στο στοιχείο **Επόμενο**.

2. Κάντε κλικ στην **Αναζήτηση** και πλοηγηθείτε στην τοποθεσία του ομότιμου πιστοποιητικού σας

(αυτό είναι το πιστοποιητικό φορέα που είχατε εξαγάγει από το ESET PROTECT On-Prem). Αφήστε κενό το πεδίο κειμένου **Κωδικός πρόσβασης πιστοποιητικού** επειδή αυτό το πιστοποιητικό δεν απαιτεί κωδικό πρόσβασης. Δεν χρειάζεται να κάνετε αναζήτηση για **Αρχή έκδοσης πιστοποιητικού** - αφήστε αυτό το πεδίο κενό.

Εάν χρησιμοποιείτε ένα προσαρμοσμένο πιστοποιητικό με το ESET PROTECT On-Prem (αντί των προεπιλεγμένων που δημιουργήθηκαν αυτόματα κατά την εγκατάσταση του ESET PROTECT On-Prem), χρησιμοποιήστε αναλόγως τα προσαρμοσμένα πιστοποιητικά σας.

Ο κωδικός πρόσβασης του πιστοποιητικού δεν πρέπει να περιέχει τους ακόλουθους χαρακτήρες: " \ Αυτοί οι χαρακτήρες προκαλούν κρίσιμο σφάλμα κατά την αρχικοποίηση του φορέα.

3. Επιλέξτε **Επόμενο** για να εγκαταστήσετε τον προεπιλεγμένο φάκελο ή **Αλλαγή** για να επιλέξετε άλλον φάκελο (συνιστάται να χρησιμοποιήσετε την προεπιλεγμένη τοποθεσία).

ESET Remote Deployment Tool

Το ESET Remote Deployment Tool είναι ένας εύχρηστος τρόπος για να διανείμετε το πακέτο προγράμματος εγκατάστασης που δημιουργήθηκε από το ESET PROTECT On-Prem για να αναπτύξετε το φορέα ESET Management και τα προϊόντα ασφάλειας ESET απομακρυσμένα σε υπολογιστές μέσα σε ένα δίκτυο.

Το ESET Remote Deployment Tool είναι διαθέσιμο δωρεάν στον ιστότοπο της ESET ως ανεξάρτητο στοιχείο του ESET PROTECT On-Prem. Το εργαλείο ανάπτυξης προορίζεται κυρίως για ανάπτυξη σε μικρά και μεσαία δίκτυα και εκτελείται με δικαιώματα διαχειριστή.

Το ESET Remote Deployment Tool προορίζεται αποκλειστικά για την ανάπτυξη του Φορέα ESET Management μόνο σε υπολογιστές-πελάτες με υποστηριζόμενα λειτουργικά συστήματα Microsoft Windows.

Για περισσότερες λεπτομέρειες σχετικά με τα προαπαιτούμενα και τη χρήση του εργαλείου, ανατρέξτε στο κεφάλαιο ESET Remote Deployment Tool.

Εγκατάσταση Κονσόλας διαδικτύου – Windows

Μπορείτε να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT σε Windows με δύο τρόπους:

- Συνιστάται η χρήση του προγράμματος εγκατάστασης «όλα σε ένα»
- Οι προχωρημένοι χρήστες μπορούν να εκτελέσουν μη αυτόματη εγκατάσταση

Μπορείτε να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT σε έναν διαφορετικό υπολογιστή από τον υπολογιστή στον οποίο εκτελείται ο διακομιστής ESET PROTECT.

Εγκατάσταση της Κονσόλας διαδικτύου χρησιμοποιώντας το πρόγραμμα εγκατάστασης «όλα σε ένα»

Προαπαιτούμενα

- Ο διακομιστής ESET PROTECT εγκαταστάθηκε.

Μπορείτε να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT σε έναν διαφορετικό υπολογιστή από τον υπολογιστή στον οποίο εκτελείται ο διακομιστής ESET PROTECT. Αυτή η διαδικασία απαιτεί πρόσθετα βήματα.

- το Apache Tomcat είναι απαραίτητο στοιχείο για τη λειτουργία της Κονσόλας διαδικτύου ESET PROTECT.

- Το Apache Tomcat απαιτεί Java/OpenJDK 64 bit. Εάν έχετε πολλαπλές εκδόσεις Java εγκατεστημένες στο σύστημά σας, συνιστάται να καταργήσετε την εγκατάσταση των παλαιότερων εκδόσεων Java και να διατηρήσετε μόνο την πιο πρόσφατη υποστηριζόμενη έκδοση Java.

Από τον Ιανουάριο 2019, οι δημόσιες ενημερώσεις Oracle JAVA SE 8 για επιχειρηματική, εμπορική ή παραγωγική χρήση, απαιτούν εμπορική άδεια χρήσης. Εάν δεν αγοράσετε συνδρομή JAVA SE, μπορείτε να χρησιμοποιήσετε αυτό τον οδηγό για μετάβαση σε μια εναλλακτική λύση χωρίς κόστος. Δείτε τις υποστηριζόμενες εκδόσεις του JDK.

Εγκατάσταση

Για να εγκαταστήσετε το στοιχείο της Κονσόλας διαδικτύου ESET PROTECT σε Windows χρησιμοποιώντας το πρόγραμμα εγκατάστασης «όλα σε ένα»:

Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης που αναφέρονται παραπάνω.

1. Πραγματοποιήστε λήψη του προγράμματος εγκατάστασης «όλα σε ένα» του ESET PROTECT από τον ιστότοπο της ESET και αποσυμπιέστε το αρχείο λήψης.

2. Εάν θέλετε να εγκαταστήσετε την πιο πρόσφατη έκδοση του Apache Tomcat και το πρόγραμμα εγκατάστασης «όλα σε ένα» περιέχει μια παλαιότερη έκδοση του Apache Tomcat (αυτό το βήμα είναι προαιρετικό - προχωρήστε στο βήμα 4, εάν δεν χρειάζεστε την πιο πρόσφατη έκδοση του Apache Tomcat):

   a. Ανοίξτε το φάκελο *x64* και μεταβείτε στο φάκελο *installers*.

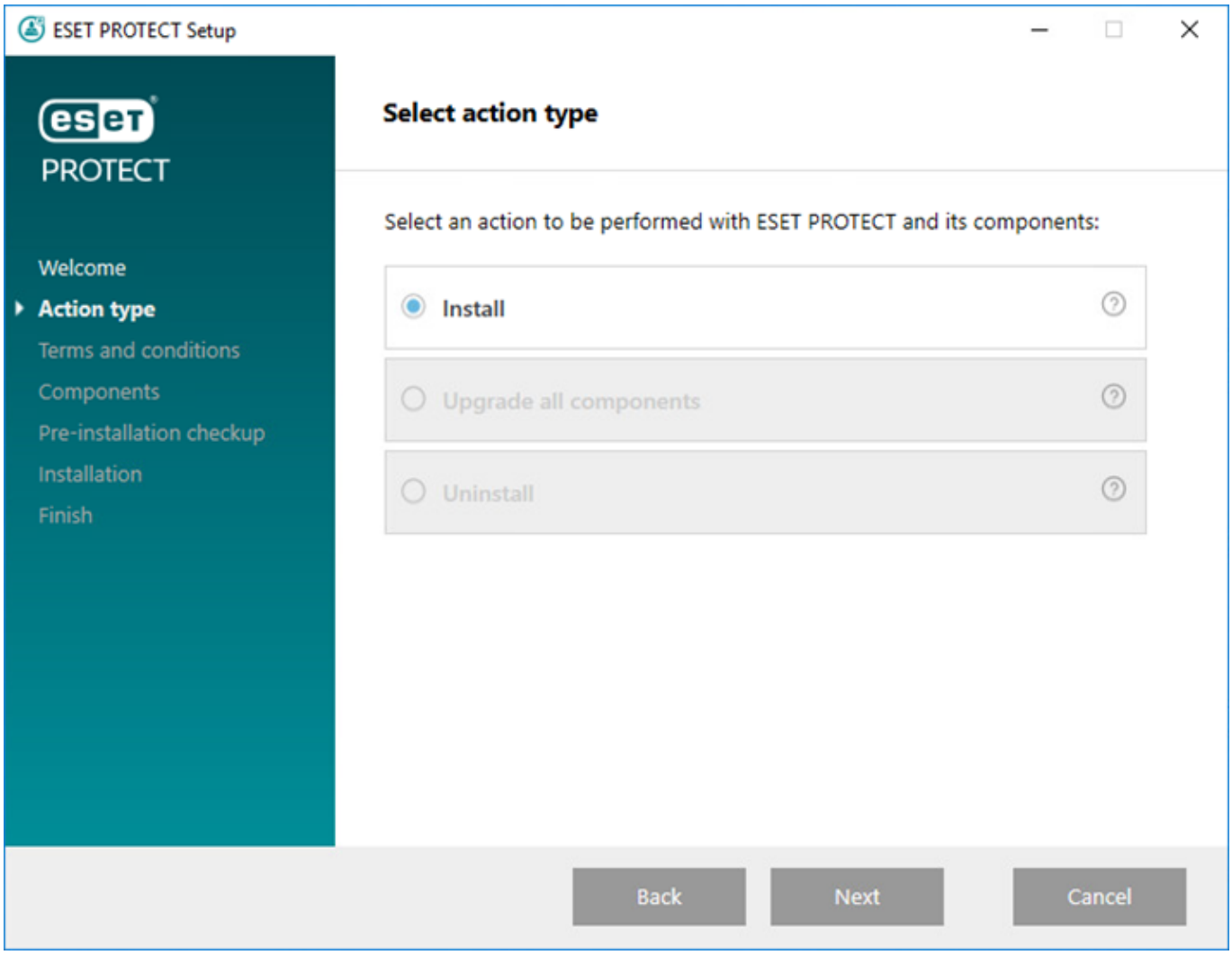
   b. Καταργήστε το αρχείο *apache-tomcat-9.0.x-windows-x64.zip* που βρίσκεται στο φάκελο *installers*.

   c. Πραγματοποιήστε λήψη του συμπιεσμένου πακέτου Apache Tomcat 9 για Windows 64 bit.

   d. Μετακινήστε το συμπιεσμένο πακέτο λήψης στο φάκελο *installers*.

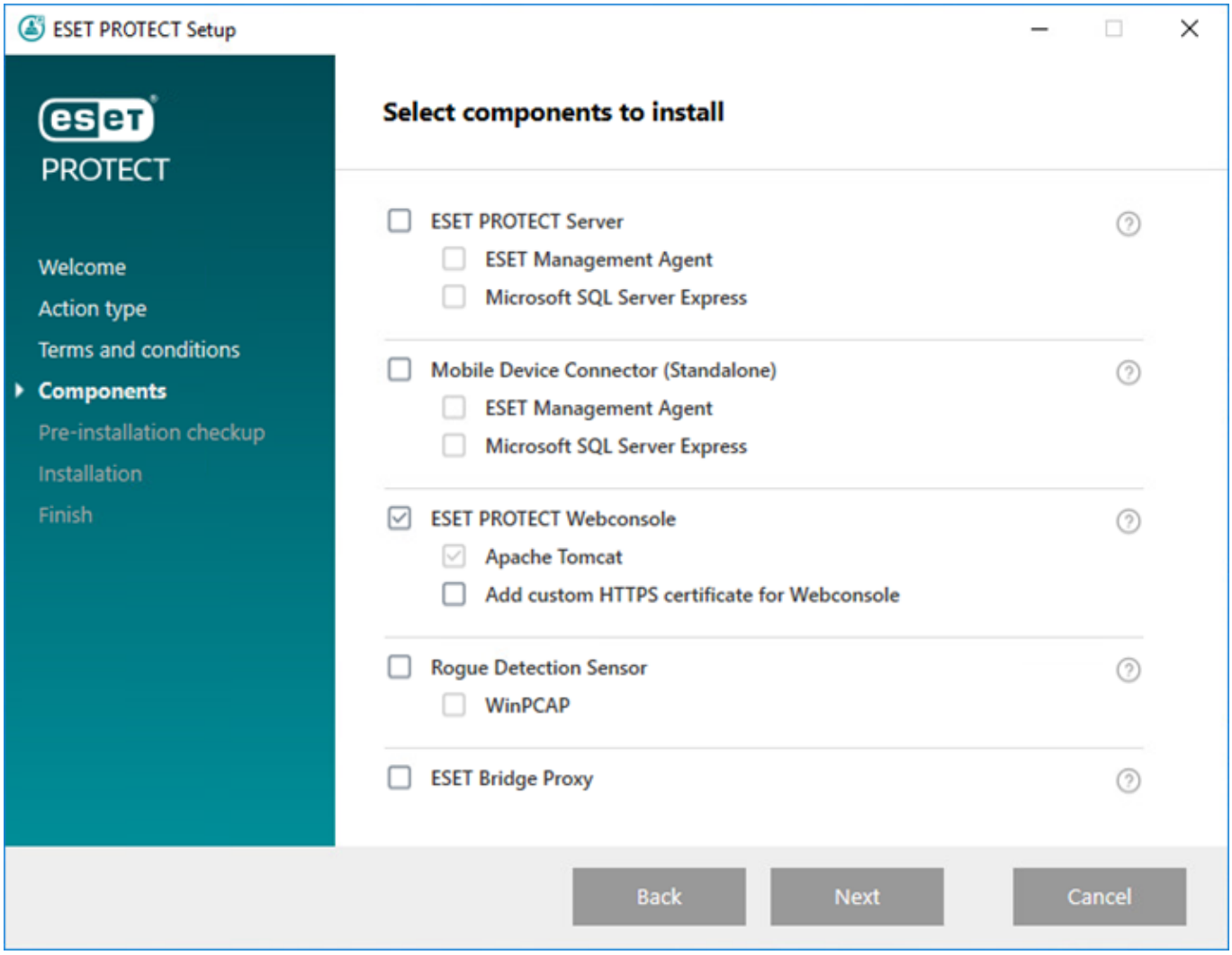
3. Για να εκκινήσετε το πρόγραμμα εγκατάστασης «όλα σε ένα», κάντε διπλό κλικ στο αρχείο *Setup.exe* και κάντε κλικ στο στοιχείο **Επόμενο** στην οθόνη **Υποδοχή**.

4. Επιλέξτε **Εγκατάσταση** και κάντε κλικ στο στοιχείο **Επόμενο**.



5. Αφού αποδεχτείτε την Άδεια Χρήσης Τελικού Χρήστη (EULA), επιλέξτε **Επόμενο**.

6. Στο στοιχείο **Επιλογή στοιχείων για εγκατάσταση**, επιλέξτε μόνο το πλαίσιο ελέγχου Κονσόλα διαδικτύου **ESET PROTECT** και κάντε κλικ στο στοιχείο **Επόμενο**.

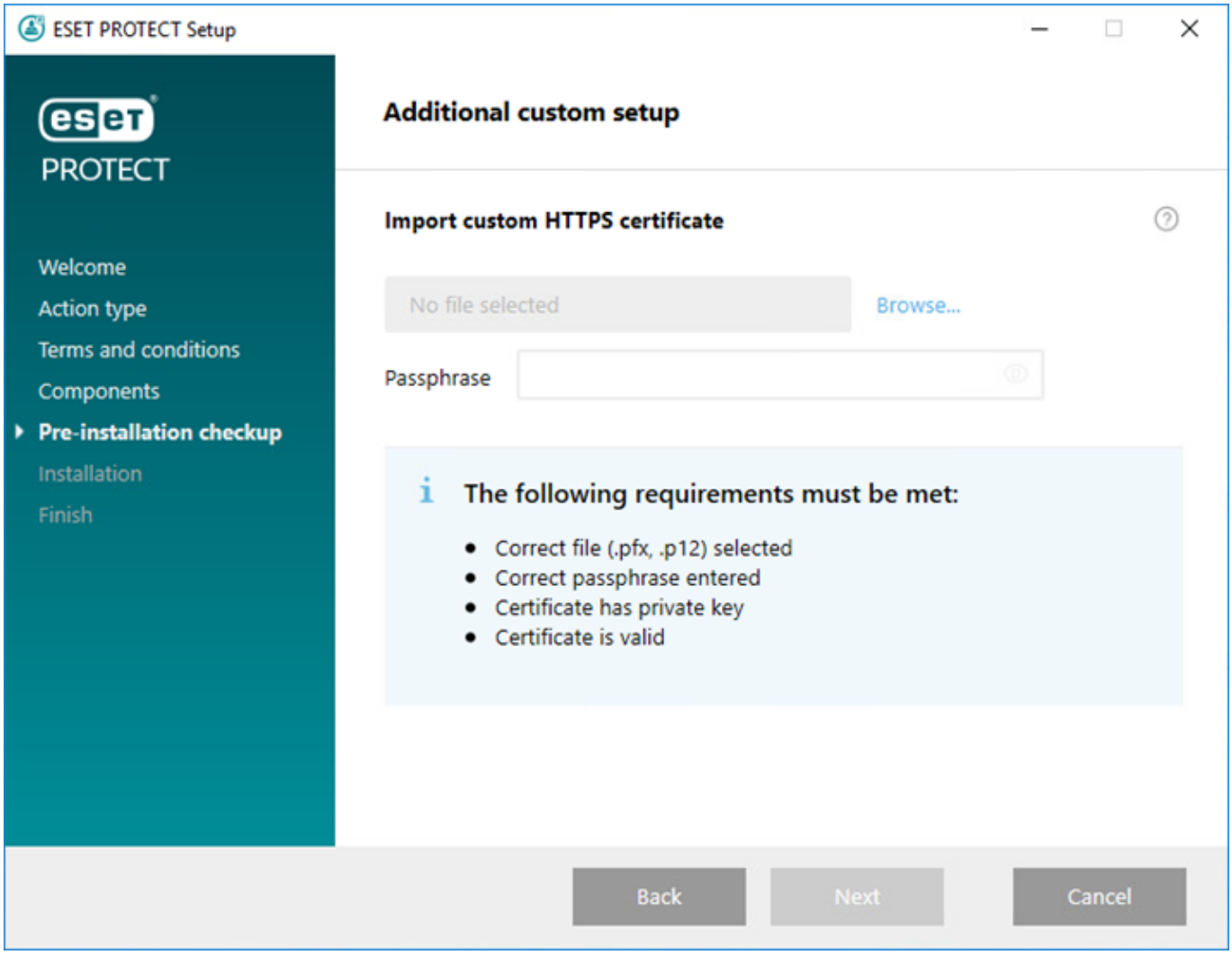


Προαιρετικά, επιλέξτε το πλαίσιο ελέγχου **Προσθήκη προσαρμοσμένου πιστοποιητικού HTTPS για την κονσόλα διαδικτύου**.

- Επιλέξτε αυτό το στοιχείο εάν θέλετε να χρησιμοποιήσετε προσαρμοσμένο πιστοποιητικό HTTPS για την Κονσόλα διαδικτύου ESET PROTECT.

- Εάν δεν ορίσετε αυτήν την επιλογή, το πρόγραμμα εγκατάστασης δημιουργεί αυτόματα ένα νέο αρχείο κλειδιών για το Tomcat (ένα πιστοποιητικό HTTPS αυτο-υπογραφής).

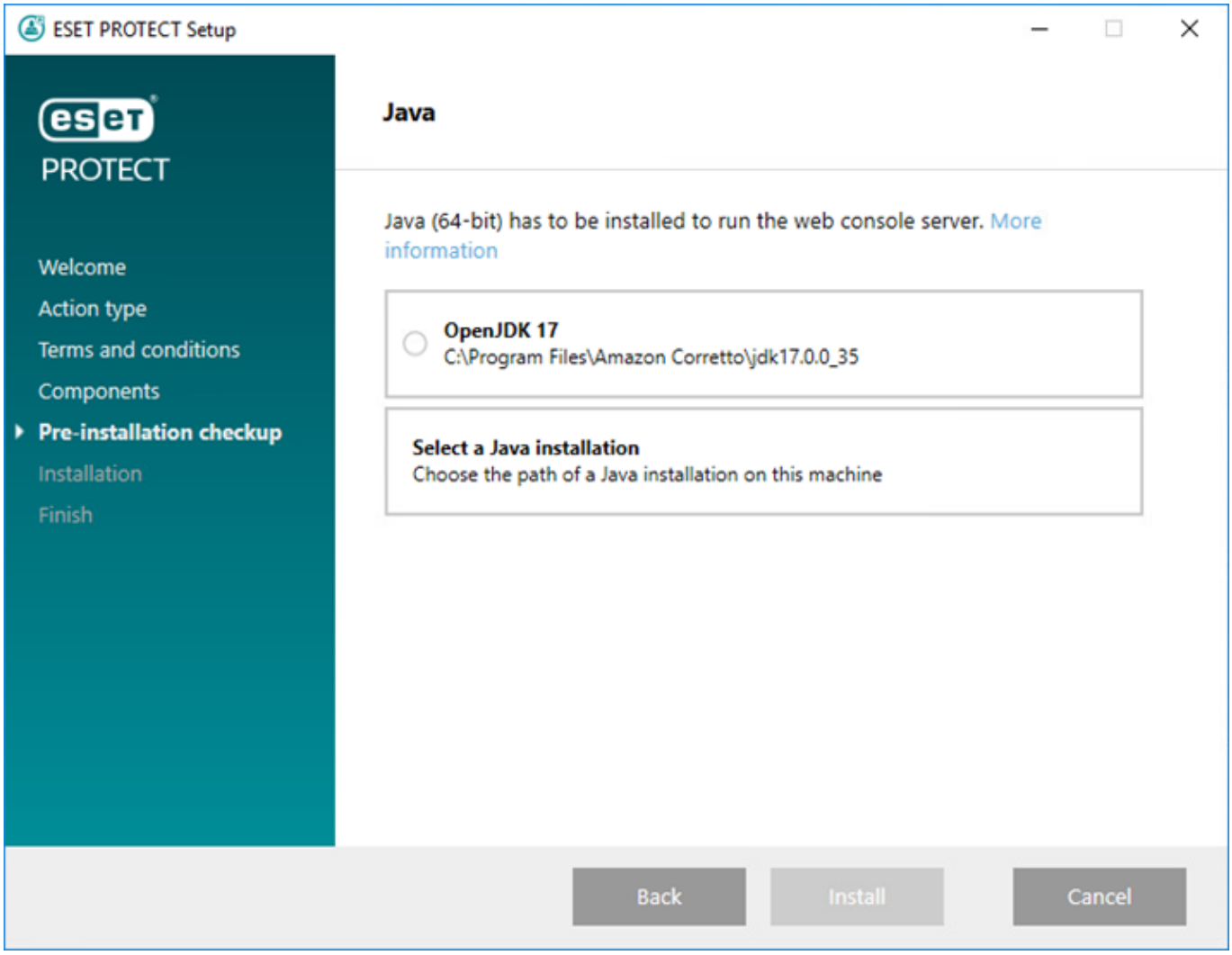
- Εάν επιλέξετε **Προσθήκη προσαρμοσμένου πιστοποιητικού HTTPS για την Κονσόλα διαδικτύου**, κάντε κλικ στο στοιχείο **Αναζήτηση** και επιλέξτε ένα έγκυρο πιστοποιητικό (αρχείο *.pfx* ή .p12) και συμπληρώστε το πεδίο **Κωδικός πρόσβασης** (ή αφήστε το πεδίο κενό εάν δεν υπάρχει κωδικός πρόσβασης). Το πρόγραμμα εγκατάστασης θα εγκαταστήσει το πιστοποιητικό για πρόσβαση στην Κονσόλα διαδικτύου στο διακομιστή Tomcat. Κάντε κλικ στο στοιχείο **Επόμενο** για να συνεχίσετε.



7. Επιλέξτε μια εγκατάσταση Java στον υπολογιστή. Επαληθεύστε ότι χρησιμοποιείτε την πιο πρόσφατη έκδοση του Java/OpenJDK.

a)Για να επιλέξετε το ήδη εγκατεστημένο Java, κάντε κλικ στο στοιχείο **Επιλογή μιας εγκατάστασης Java**, επιλέξτε το φάκελο στον οποίο είναι εγκατεστημένο το Java (με έναν υποφάκελο *bin*, για παράδειγμα *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) και κάντε κλικ στο **OK**. Το πρόγραμμα εγκατάστασης θα σας ρωτήσει εάν έχετε επιλέξει μη έγκυρη διαδρομή.

b)Κάντε κλικ στο στοιχείο **Εγκατάσταση** για να συνεχίσετε ή **αλλαγή** για να αλλάξετε τη διαδρομή εγκατάστασης Java.



8. Όταν ολοκληρωθεί η εγκατάσταση, κάντε κλικ στο στοιχείο **Τέλος**.

Εάν εγκαταστήσατε την κονσόλα διαδικτύου ESET PROTECT σε διαφορετικό υπολογιστή από το διακομιστή ESET PROTECT, εκτελέστε αυτά τα πρόσθετα βήματα, για να ενεργοποιήσετε την επικοινωνία μεταξύ της κονσόλας διαδικτύου ESET PROTECT και του διακομιστή ESET PROTECT:
a)Διακόψτε την υπηρεσία Apache TomcatTomcat. Μεταβείτε στα στοιχεία **Έναρξη** > **Υπηρεσίες** > κάντε δεξί κλικ στην υπηρεσία Apache Tomcat και επιλέξτε **Διακοπή**.
b)Εκτελέστε το Σημειωματάριο ως Διαχειριστής και επεξεργαστείτε το *C:\Program Files\Apache Software Foundation\[Tomcat* φάκελος *]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)Βρείτε το `server_address=localhost`.
d)Αντικαταστήστε το `localhost` με τη διεύθυνση IP του διακομιστή ESET PROTECT και αποθηκεύστε το αρχείο.
e) Εκκινήστε την υπηρεσία Apache Tomcat: Μεταβείτε στα στοιχεία **Έναρξη** > **Υπηρεσίες** > κάντε δεξί κλικ στην υπηρεσία Apache Tomcat και επιλέξτε **Έναρξη**.

9. Ανοίξτε την Κονσόλα διαδικτύου ESET PROTECT σε ένα υποστηριζόμενο πρόγραμμα περιήγησης: Θα εμφανιστεί μια οθόνη σύνδεσης.

- Από τον υπολογιστή που φιλοξενεί την Κονσόλα διαδικτύου ESET PROTECT: *https://localhost/era*

- Από οποιονδήποτε υπολογιστή με πρόσβαση στο Internet στην Κονσόλα διαδικτύου ESET PROTECT (αντικαταστήστε το στοιχείο *IP_ADDRESS_OR_HOSTNAME* με τη διεύθυνση IP ή το όνομα κεντρικού υπολογιστή της Κονσόλας διαδικτύου ESET PROTECT): *https://IP_ADDRESS_OR_HOSTNAME/era*

Δείτε επίσης την πρόσθετη ρύθμιση παραμέτρων της Κονσόλας διαδικτύου για εταιρικές λύσεις ή συστήματα χαμηλών επιδόσεων.

Μη αυτόματη εγκατάσταση της Κονσόλας διαδικτύου

Η μη αυτόματη εγκατάσταση της Κονσόλας διαδικτύου ESET PROTECT είναι μια διαδικασία για προχωρημένους. Συνιστάται να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT χρησιμοποιώντας το πρόγραμμα εγκατάστασης «όλα σε ένα».

Προαπαιτούμενα

- Ο διακομιστής ESET PROTECT εγκαταστάθηκε.

Μπορείτε να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT σε έναν διαφορετικό υπολογιστή από τον υπολογιστή στον οποίο εκτελείται ο διακομιστής ESET PROTECT. Αυτή η διαδικασία απαιτεί πρόσθετα βήματα.

- το Apache Tomcat είναι απαραίτητο στοιχείο για τη λειτουργία της Κονσόλας διαδικτύου ESET PROTECT. Εγκατάσταση του Apache Tomcat:

  a)Πραγματοποιήστε λήψη της πιο πρόσφατης υποστηριζόμενης έκδοσης του αρχείου προγράμματος εγκατάστασης του Apache Tomcat (32-bit/64-bit Windows Service Installer) *apache-tomcat-[].exe* από τη διεύθυνση https://tomcat.apache.org.

  b)Εκτελέστε το πρόγραμμα εγκατάστασης.

  c)Κατά την εγκατάσταση, επιλέξτε τη διαδρομή προς το Java (γονικός φάκελος των φακέλων Java *bin* και *lib*) και επιλέξτε το πλαίσιο ελέγχου **Run Apache Tomcat**.

  d)Μετά την εγκατάσταση, βεβαιωθείτε ότι εκτελείται η υπηρεσία Apache Tomcat και ότι ο τύπος εκκίνησης έχει ρυθμιστεί σε **Αυτόματη** (στο **services.msc**).

- Το Apache Tomcat απαιτεί Java/OpenJDK 64 bit. Εάν έχετε πολλαπλές εκδόσεις Java εγκατεστημένες στο σύστημά σας, συνιστάται να καταργήσετε την εγκατάσταση των παλαιότερων εκδόσεων Java και να διατηρήσετε μόνο την πιο πρόσφατη υποστηριζόμενη έκδοση Java.

Από τον Ιανουάριο 2019, οι δημόσιες ενημερώσεις Oracle JAVA SE 8 για επιχειρηματική, εμπορική ή παραγωγική χρήση, απαιτούν εμπορική άδεια χρήσης. Εάν δεν αγοράσετε συνδρομή JAVA SE, μπορείτε να χρησιμοποιήσετε αυτό τον οδηγό για μετάβαση σε μια εναλλακτική λύση χωρίς κόστος. Δείτε τις υποστηριζόμενες εκδόσεις του JDK.

Εγκατάσταση

Για να εγκαταστήσετε το στοιχείο κονσόλας διαδικτύου ESET PROTECT στα Windows, ακολουθήστε τα παρακάτω βήματα:

Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης που αναφέρονται παραπάνω.

1. Επισκεφτείτε την ενότητα λήψεων του ESET PROTECT για λήψη ενός ανεξάρτητου προγράμματος εγκατάστασης για αυτό το στοιχείο του ESET PROTECT (Κονσόλα διαδικτύου αρχείο *era.war*).

2. Αντιγράψτε το αρχείο *era.war* στο φάκελο εφαρμογών ιστού του Apache Tomcat:

C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]\webapps*

3. Το Apache Tomcat εξάγει αυτόματα το αρχείο *era.war* στον φάκελο *era* και εγκαθιστά την Κονσόλα διαδικτύου ESET PROTECT. Περιμένετε λίγα λεπτά μέχρι να ολοκληρωθεί η εξαγωγή. Εάν δεν πραγματοποιηθεί η εξαγωγή, ακολουθήστε τα βήματα αντιμετώπισης προβλημάτων.

4. Εάν εγκαταστήσατε την Κονσόλα διαδικτύου ESET PROTECT στον ίδιο υπολογιστή με το διακομιστή ESET PROTECT, επανεκκινήστε την υπηρεσία Apache Tomcat. Μεταβείτε στα στοιχεία **Έναρξη** > **Υπηρεσίες** > κάντε δεξί κλικ στην υπηρεσία Apache Tomcat και επιλέξτε **Διακοπή**. Κάντε κλικ στο στοιχείο Stop, περιμένετε 30 δευτερόλεπτα και κατόπιν κάντε κλικ στο στοιχείο **Start**.

Εάν εγκαταστήσατε την κονσόλα διαδικτύου ESET PROTECT σε διαφορετικό υπολογιστή από το διακομιστή ESET PROTECT, εκτελέστε αυτά τα πρόσθετα βήματα, για να ενεργοποιήσετε την επικοινωνία μεταξύ της κονσόλας διαδικτύου ESET PROTECT και του διακομιστή ESET PROTECT:
a)Διακόψτε την υπηρεσία Apache TomcatTomcat. Μεταβείτε στα στοιχεία **Έναρξη** > **Υπηρεσίες** > κάντε δεξί κλικ στην υπηρεσία Apache Tomcat και επιλέξτε **Διακοπή**.
b)Εκτελέστε το Σημειωματάριο ως Διαχειριστής και επεξεργαστείτε το *C:\Program Files\Apache Software Foundation\[Tomcat* φάκελος *]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)Βρείτε το `server_address=localhost`.
d)Αντικαταστήστε το `localhost` με τη διεύθυνση IP του διακομιστή ESET PROTECT και αποθηκεύστε το αρχείο.
e) Εκκινήστε την υπηρεσία Apache Tomcat: Μεταβείτε στα στοιχεία **Έναρξη** > **Υπηρεσίες** > κάντε δεξί κλικ στην υπηρεσία Apache Tomcat και επιλέξτε **Έναρξη**.

5. Ανοίξτε την Κονσόλα διαδικτύου ESET PROTECT σε ένα υποστηριζόμενο πρόγραμμα περιήγησης για να δείτε μια οθόνη σύνδεσης:

- Από τον υπολογιστή που φιλοξενεί την Κονσόλα διαδικτύου ESET PROTECT:
  http://localhost:8080/era

- Από οποιονδήποτε υπολογιστή με πρόσβαση στο Internet στην Κονσόλα διαδικτύου ESET PROTECT (αντικαταστήστε το στοιχείο *IP_ADDRESS_OR_HOSTNAME* με τη διεύθυνση IP ή το όνομα κεντρικού υπολογιστή της Κονσόλας διαδικτύου ESET PROTECT):
  http://IP_ADDRESS_OR_HOSTNAME:8080/era

6. Ρύθμιση παραμέτρων της Κονσόλας διαδικτύου μετά την εγκατάσταση:

- Η προεπιλεγμένη θύρα HTTP ορίζεται σε 8080 κατά τη μη αυτόματη εγκατάσταση του Apache Tomcat. Συνιστάται να ρυθμίσετε μια σύνδεση HTTPS για το Apache Tomcat.

- Δείτε επίσης την πρόσθετη ρύθμιση παραμέτρων της Κονσόλας διαδικτύου για εταιρικές λύσεις ή συστήματα χαμηλών επιδόσεων.

Εγκατάσταση αισθητήρα RD Sensor – Windows

Προαπαιτούμενα

- WinPcap – χρησιμοποιήστε την πιο πρόσφατη έκδοση του WinPcap (4.1.0 και νεότερες εκδόσεις)
- Θα πρέπει να έχει γίνει σωστή ρύθμιση παραμέτρων του δικτύου (να είναι ανοιχτές οικατάλληλες θύρες, να μην αποκλείεται η εισερχόμενη επικοινωνία από τείχος προστασίας, κ.λπ.)
- Να είναι δυνατή η επικοινωνία με τον διακομιστή ESET PROTECT
- Ο φορέας ESET Management πρέπει να είναι εγκατεστημένος στον τοπικό υπολογιστή, για να υποστηρίζει πλήρως όλες τις λειτουργίες του προγράμματος

> Εάν υπάρχουν πολλά τμήματα δικτύου, ο αισθητήρας Rogue Detection Sensor πρέπει να εγκατασταθεί ξεχωριστά σε κάθε τμήμα δικτύου για να δημιουργήσει μια ολοκληρωμένη λίστα όλων των συσκευών σε ολόκληρο το δίκτυο.

Εγκατάσταση

Για να εγκαταστήστε το στοιχείο αισθητήρα RD Sensor σε Windows, ακολουθήστε τα παρακάτω βήματα:

> Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης που αναφέρονται παραπάνω.

1. Επισκεφτείτε την ενότητα λήψεων του ESET PROTECT για λήψη ενός ανεξάρτητου προγράμματος εγκατάστασης για αυτό το στοιχείο του ESET PROTECT (*rdsensor_x86.msi* ή *rdsensor_x64.msi*).

2. Κάντε διπλό κλικ στο αρχείο του προγράμματος εγκατάστασης του αισθητήρα RD Sensor για να αρχίσει η εγκατάσταση.

3. Αποδεχτείτε την Άδεια χρήσης τελικού χρήστη (EULA) και κάντε κλικ στην επιλογή **Επόμενο**.

4. Επιλέξτε το πλαίσιο ελέγχου **Συμμετοχή στο πρόγραμμα βελτίωσης προϊόντος**, για να αποστέλλονται ανώνυμα δεδομένα τηλεμετρίας και αναφορές σφαλμάτων στην ESET (έκδοση και τύπος λειτουργικού συστήματος, έκδοση προϊόντος ESET και άλλες πληροφορίες ειδικά για το προϊόν).

5. Επιλέξτε τη θέση εγκατάστασης για τον αισθητήρα RD Sensor και κάντε κλικ στα στοιχεία **Επόμενο** > **Εγκατάσταση**.

6. Το ESET Rogue Detection Sensor θα εκκινήσει μετά την ολοκλήρωση της εγκατάστασης.

Μπορείτε να βρείτε το αρχείο καταγραφής του Rogue Detection Sensor στα αρχεία καταγραφής: *C:\ProgramData\ESET\Rogue Detection Sensor\Logs*

Εργαλείο ειδώλου - Windows

Είστε χρήστης Linux;

Το εργαλείο ειδώλου είναι απαραίτητο για τις ενημερώσεις του μηχανισμού ανίχνευσης χωρίς σύνδεση. Εάν οι υπολογιστές-πελάτες σας δεν έχουν σύνδεση στο Internet και χρειάζονται ενημερώσεις του μηχανισμού ανίχνευσης, μπορείτε να χρησιμοποιήσετε το εργαλείο ειδώλου για να λαμβάνετε αρχεία ενημέρωσης από τους διακομιστές ενημέρωσης της ESET και να τα αποθηκεύετε τοπικά.

Το Εργαλείο ειδώλου έχει τις εξής λειτουργίες:
• Ενημερώσεις μονάδων – Πραγματοποιεί λήψη ενημερώσεων του μηχανισμού ανίχνευσης και άλλων μονάδων προγράμματος, αλλά όχι αυτόματες ενημερώσεις (uPCU).
• Δημιουργία αποθετηρίου – Μπορεί να δημιουργήσει ένα πλήρες αποθετήριο χωρίς σύνδεση, το οποίο συμπεριλαμβάνει αυτόματες ενημερώσεις (uPCU).
Το εργαλείο ειδώλου δεν πραγματοποιεί λήψη δεδομένων του ESET LiveGrid®.

Προαπαιτούμενα

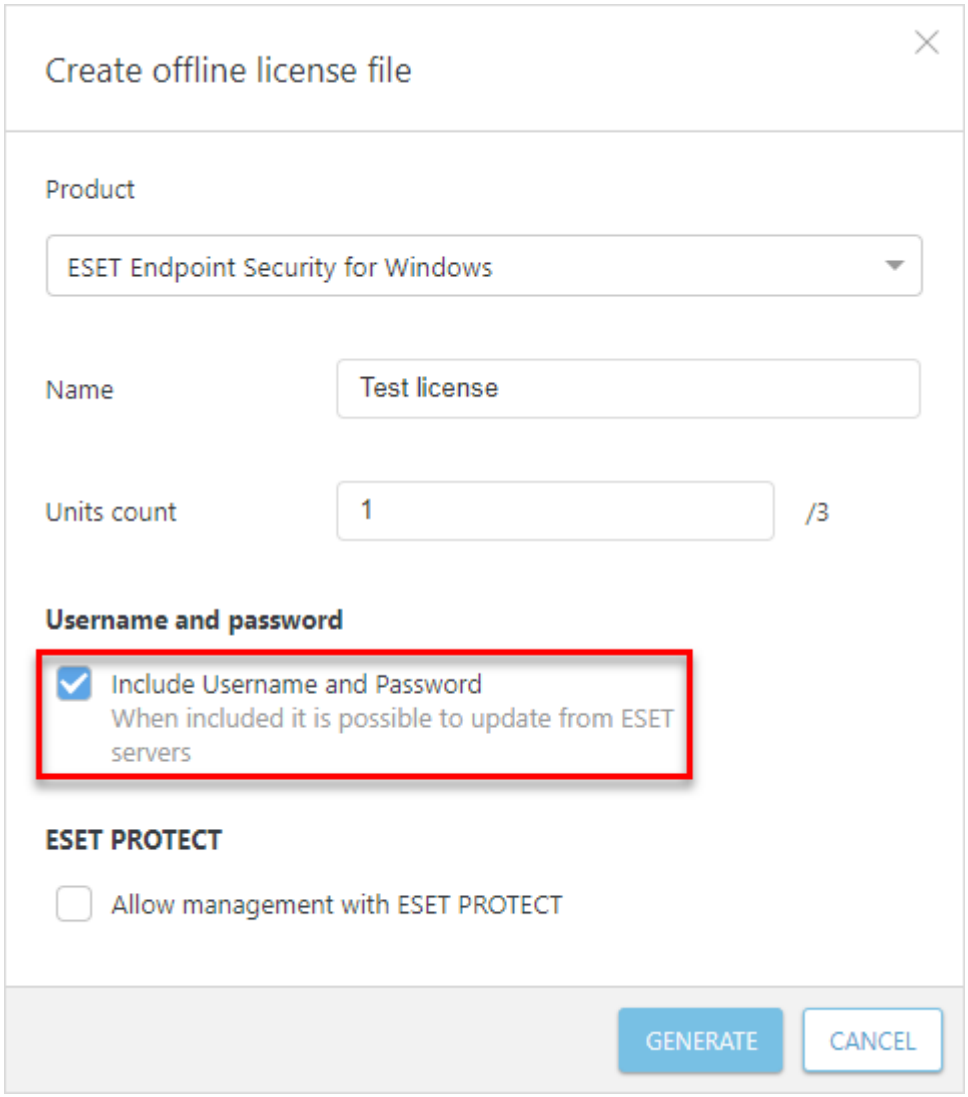
Το εργαλείο ειδώλου δε υποστηρίζει Windows XP και Windows Server 2003.

• Ο φάκελος προορισμού πρέπει να είναι διαθέσιμος για κοινή χρήση, με υπηρεσία Samba/Windows ή HTTP/FTP, ανάλογα με τον τρόπο πρόσβασης που θέλετε για τις ενημερώσεις.

oΠροϊόντα ασφάλειας ESET για Windows - Μπορείτε να τα ενημερώνετε απομακρυσμένα χρησιμοποιώντας HTTP ή έναν κοινόχρηστο φάκελο.

oΠροϊόντα ασφάλειας ESET για Linux/macOS - Μπορείτε να τα ενημερώνετε απομακρυσμένα χρησιμοποιώντας μόνο HTTP. Εάν χρησιμοποιείτε έναν κοινόχρηστο φάκελο, πρέπει να βρίσκεται στον ίδιο υπολογιστή με το προϊόν ασφάλειας ESET.

• Πρέπει να έχετε ένα έγκυρο αρχείο άδειας χρήσης εκτός σύνδεσης που περιλαμβάνει όνομα χρήστη και κωδικό πρόσβασης. Κατά τη δημιουργία ενός αρχείου άδειας χρήσης, βεβαιωθείτε ότι έχετε επιλέξει το πλαίσιο ελέγχου που βρίσκεται δίπλα από το στοιχείο **Συμπερίληψη ονόματος χρήστη και κωδικού πρόσβασης**. Επίσης, πρέπει να πληκτρολογήσετε ένα **Όνομα** της άδειας χρήσης. Για την ενεργοποίηση του εργαλείου ειδώλου και τη δημιουργία του ειδώλου ενημέρωσης απαιτείται αρχείο άδειας χρήσης εκτός σύνδεσης.



- Προτού εκτελέσετε το εργαλείο ειδώλου, πρέπει να εγκαταστήσετε τα ακόλουθα πακέτα:
- Visual C++ Redistributable for Visual Studio 2010
- Visual C++ 2015 Redistributable x86

Πώς να χρησιμοποιήσετε το εργαλείο ειδώλου

1.Πραγματοποιήστε λήψη του εργαλείου ειδώλου από τη σελίδα λήψεων της ESET (ενότητα **Ανεξάρτητα προγράμματα εγκατάστασης**).

2.Αποσυμπιέστε τον ληφθέντα αρχειοθήκη.

3.Ανοίξτε τη γραμμή εντολής και πλοηγηθείτε στο φάκελο με το αρχείο *MirrorTool.exe*.

4.Εκτελέστε την παρακάτω εντολή για να προβάλετε όλες τις διαθέσιμες παραμέτρους για το Εργαλείο ειδώλου και την έκδοσή του:

```
MirrorTool.exe --help
```

```
C:\Users\                    >MirrorTool.exe --help
Mirror Tool v1.0.1294.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights
reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Σε όλα τα φίλτρα γίνεται διάκριση πεζών-κεφαλαίων.

Μπορείτε να χρησιμοποιήσετε τις παραμέτρους για να δημιουργήσετε το είδωλο του αποθετηρίου ή το είδωλο των μονάδων:

Παράμετροι για το είδωλο του αποθετηρίου και για το είδωλο των μονάδων

--proxyHost
--proxyPort
--proxyUsername
--proxyPassword
--help

Παράμετροι ειδικά για το αποθετήριο

--repositoryServer
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

Παράμετροι ειδικά για τις μονάδες

--mirrorType
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

Παράμετρος	Περιγραφή
`--updateServer`	Το Mirror Tool δημιουργεί μια δομή φακέλων που είναι διαφορετική από αυτή του ειδώλου του τερματικού. Κάθε φάκελος διατηρεί αρχεία ενημέρωσης για μια ομάδα προϊόντων. ⚠ Πρέπει να καθορίσετε τον πλήρη σύνδεσμο του διακομιστή ενημέρωσης (πλήρη διαδρομή στον σωστό φάκελο) στις ρυθμίσεις ενημέρωσης του προϊόντος που χρησιμοποιεί το είδωλο.
`--offlineLicenseFilename`	Πρέπει να καθορίσετε μια διαδρομή προς το αρχείο άδειας χρήσης εκτός σύνδεσης (όπως αναφέρεται παραπάνω).
`--mirrorOnlyLevelUpdates`	Δεν απαιτείται όρισμα. Εάν οριστεί, θα γίνει λήψη μόνο ενημερώσεων επιπέδου (δεν θα γίνει λήψη nano ενημερώσεων). Διαβάστε περισσότερα σχετικά με τους τύπους ενημερώσεων στο άρθρο της Γνωσιακής βάσης.
`--mirrorFileFormat`	⚠ Πριν χρησιμοποιήσετε την παράμετρο `--mirrorFileFormat`, βεβαιωθείτε ότι το περιβάλλον σας δεν περιέχει παλαιότερες (6.5 και παλαιότερες) και νεότερες (6.6. και νεότερες) εκδόσεις προϊόντων ασφαλείας της ESET. Η εσφαλμένη χρήση αυτής της παραμέτρου ενδέχεται να οδηγήσει σε εσφαλμένες ενημερώσεις των προϊόντων ασφαλείας της ESET. Μπορείτε να καθορίσετε τον τύπο αρχείων ενημέρωσης που θα ληφθούν. Πιθανές τιμές (με διάκριση πεζών-κεφαλαίων): • `dat` - Χρησιμοποιήστε αυτή την τιμή εάν έχετε περιβάλλον μόνο με προϊόντα ασφαλείας ESET εκδόσεις 6.5 και παλαιότερες. • `dll` - Χρησιμοποιήστε αυτή την τιμή εάν έχετε περιβάλλον μόνο με προϊόντα ασφαλείας ESET εκδόσεις 6.6 και νεότερες. Η παράμετρος παραβλέπεται κατά τη δημιουργία ενός ειδώλου για προϊόντα παλαιού τύπου (`ep4`, `ep5`).
`--compatibilityVersion`	Αυτή η προαιρετική παράμετρος εφαρμόζεται στο εργαλείο ειδώλου που διανέμεται με το ESET PROTECT On-Prem 8.1 και νεότερες εκδόσεις. Το εργαλείο ειδώλου θα πραγματοποιήσει λήψη αρχείων ενημέρωσης που είναι συμβατά με την έκδοση αποθετηρίου του ESET PROTECT On-Prem που καθορίζετε στο όρισμα της παραμέτρου σε μορφή `x.x` ή `x.x.x.x`, για παράδειγμα: `--compatibilityVersion 11.0` ή `--compatibilityVersion 8.1.13.0`. Η παράμετρος `--compatibilityVersion` εξαιρεί τις αυτόματες ενημερώσεις (uPCU) από το είδωλο. Εάν χρειάζεστε τις αυτόματες ενημερώσεις (uPCU) στο περιβάλλον σας και θέλετε να μειώσετε το μέγεθος του ειδώλου, χρησιμοποιήστε την παράμετρο `--filterFilePath`.

ℹ Για να μειώσετε την ποσότητα δεδομένων που λαμβάνονται από το αποθετήριο της ESET, συνιστάται να χρησιμοποιήσετε τις νέες παραμέτρους στο Εργαλείο ειδώλου που διανέμεται με το ESET PROTECT On-Prem 9: `--filterFilePath` και `--dryRun`:
1.Δημιουργήστε ένα φίλτρο σε μορφή *JSON* (δείτε τη διαδρομή `--filterFilePath` παρακάτω).
2.Εκτελέστε μια δοκιμαστική εκτέλεση του Εργαλείου ειδώλου με την παράμετρο `--dryRun` (δείτε παρακάτω) και προσαρμόστε το φίλτρο όπως απαιτείται.
3.Εκτελέστε το Εργαλείο ειδώλου με την παράμετρο `--filterFilePath` και το καθορισμένο φίλτρο λήψης, μαζί με τις παραμέτρους `--intermediateRepositoryDirectory` και `--outputRepositoryDirectory`.
4.Εκτελείτε το Εργαλείο ειδώλου τακτικά, ώστε να χρησιμοποιείτε πάντα τα πιο πρόσφατα προγράμματα εγκατάστασης.

Παράμετρος	Περιγραφή

`--filterFilePath`	Χρησιμοποιήστε αυτήν την προαιρετική παράμετρο για να φιλτράρετε προϊόντα ασφάλειας ESET με βάση ένα αρχείο κειμένου σε μορφή *JSON*, το οποίο τοποθετείται στον ίδιο φάκελο με το εργαλείο ειδώλου, για παράδειγμα: `--filterFilePath filter.txt`)
	Περιγραφή ρύθμισης παραμέτρων φίλτρου:
	Η μορφή του αρχείου ρύθμισης παραμέτρων για φιλτράρισμα προϊόντος είναι *JSON* με την ακόλουθη δομή:
	• ριζικό αντικείμενο *JSON*:
	o`use_legacy` (boolean, προαιρετικά) - εάν επιλεχτεί προσδιορισμός «true» (αληθές), θα συμπεριληφθούν προϊόντα παλαιού τύπου.
	o`defaults` (αντικείμενο *JSON*, προαιρετικά) - ορίζει τις ιδιότητες φίλτρου που θα εφαρμοστούν σε όλα τα προϊόντα.
	■`languages` (λίστα) - Καθορίστε τους κωδικούς γλώσσας ISO των γλωσσών που θα συμπεριληφθούν, για παράδειγμα, για Γαλλικά πληκτρολογήστε `"fr_FR"`. Άλλοι κωδικοί γλωσσών περιλαμβάνονται στον παρακάτω πίνακα. Για να επιλέξετε περισσότερες γλώσσες, διαχωρίστε τες με κόμμα και διάστημα, για παράδειγμα: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (κατάλογος) – πλατφόρμες που θα συμπεριληφθούν (`["x64", "x86", "arm64"]`).
	⚠ Χρησιμοποιήστε το φίλτρο `platforms` με προσοχή. Για παράδειγμα, εάν το Εργαλείο ειδώλου πραγματοποιήσει λήψη μόνο προγραμμάτων εγκατάστασης 64 bit και υπάρχουν υπολογιστές 32 bit στην υποδομή σας, τα προϊόντα ασφάλειας ESET 64 bit δεν θα εγκατασταθούν σε υπολογιστές 32 bit.
	
	■`os_types` (κατάλογος) – Τύποι λειτουργικού συστήματος που θα συμπεριληφθούν (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (λίστα αντικειμένων JSON, προαιρετικά) - φίλτρα που θα εφαρμοστούν σε συγκεκριμένα προϊόντα - παράκαμψη της παραμέτρου `defaults` για συγκεκριμένα προϊόντα. Τα αντικείμενα έχουν τις ακόλουθες ιδιότητες:
	■`app_id` (συμβολοσειρά) - απαιτείται εάν δεν έχει καθοριστεί η παράμετρος `name`.
	■`name` (συμβολοσειρά), απαιτείται εάν δεν έχει καθοριστεί η παράμετρος `app_id`.
	■`version` (συμβολοσειρά) - καθορίζει την έκδοση ή το εύρος εκδόσεων που θα συμπεριληφθούν.
	■`languages` (λίστα) - κωδικοί γλώσσας ISO των γλωσσών που θα συμπεριληφθούν (δείτε τον παρακάτω πίνακα).
	■`platforms` (κατάλογος) – πλατφόρμες που θα συμπεριληφθούν (`["x64", "x86", "arm64"]`).
	■`os_types` (κατάλογος) – Τύποι λειτουργικού συστήματος που θα συμπεριληφθούν (`["windows"]`, `["linux"]`, `["mac"]`).
	ℹ Για να προσδιορίσετε τις κατάλληλες τιμές για τα πεδία, εκτελέστε το Εργαλείο ειδώλου σε δοκιμαστική λειτουργία και βρείτε το σχετικό προϊόν στο αρχείο CSV που δημιουργήθηκε.
	Περιγραφές μορφής συμβολοσειράς έκδοσης
	Όλοι οι αριθμοί έκδοσης αποτελούνται από τέσσερις αριθμούς διαχωρισμένους με κουκκίδες (για παράδειγμα, `7.1.0.0`). Μπορείτε να καθορίσετε λιγότερους αριθμούς κατά τη σύνταξη φίλτρων έκδοσης (για παράδειγμα `7.1`) και οι υπόλοιποι αριθμοί θα είναι μηδέν (το `7.1` ισούται με το `7.1.0.0`).
	Η συμβολοσειρά έκδοσης μπορεί να έχει μία από τις δύο ακόλουθες μορφές:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oΕπιλέγει εκδόσεις μεγαλύτερες/μικρότερες από ή ίσες/μικρότερες από ή ίσες/ίσες με την καθορισμένη έκδοση.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oΕπιλέγει εκδόσεις που είναι μεγαλύτερες από ή ίσες με το χαμηλότερο όριο και μικρότερες από ή ίσες με το υψηλότερο όριο.
	Οι συγκρίσεις γίνονται αριθμητικά σε κάθε τμήμα του αριθμού έκδοσης, από αριστερά προς τα δεξιά.
	Παράδειγμα JSON
	✓
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0–8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	Η παράμετρος `--filterFilePath` αντικαθιστά τις παραμέτρους `--languageFilterForRepository`, `--productFilterForRepository` και `--downloadLegacyForRepository` που χρησιμοποιούνται στις παλαιότερες εκδόσεις του Εργαλείου ειδώλου (που κυκλοφόρησαν με το ESET PROTECT On-Prem 8.x).

Παράμετρος	Περιγραφή
`--dryRun`	Όταν χρησιμοποιείτε αυτήν την προαιρετική παράμετρο, το εργαλείο ειδώλου δεν θα πραγματοποιήσει λήψη κανενός αρχείου, αλλά θα δημιουργήσει ένα αρχείο *.csv* στο οποίο θα καταγράφονται όλα τα πακέτα που θα ληφθούν. Μπορείτε να χρησιμοποιήσετε αυτήν την παράμετρο χωρίς τις υποχρεωτικές παραμέτρους `--intermediateRepositoryDirectory` και `--outputRepositoryDirectory`, για παράδειγμα: • Windows: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv` • Linux: `sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv` ℹ Ορισμένα προγράμματα εγκατάστασης της ESET δεν έχουν συγκεκριμένη γλώσσα (με κώδικα γλώσσας `multilang`) και το Εργαλείο ειδώλου θα τα καταχωρίσει στο αρχείο *.csv* ακόμα και αν καθορίσετε `γλώσσες` στην παράμετρο `--filterFilePath`. Εάν χρησιμοποιείτε την παράμετρο `--dryRun` καθώς επίσης και τις παραμέτρους `--intermediateRepositoryDirectory --outputRepositoryDirectory`, το εργαλείο ειδώλου δεν εκκαθαρίζει το *outputRepositoryDirectory*.
`--listUpdatableProducts`	Καταγράψτε σε λίστα όλα τα προϊόντα ESET για τα οποία μπορεί το Mirror Tool να λαμβάνει ενημερώσεις μονάδων (εκτός αν χρησιμοποιείται η παράμετρος `--excludedProducts`). Η παράμετρος είναι διαθέσιμη από τις εκδόσεις Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

Δομή φακέλου του Mirror Tool

Από προεπιλογή, εάν δεν καθορίσετε την παράμετρο `--updateServer`, το Mirror Tool δημιουργεί αυτήν τη δομή φακέλου στον διακομιστή HTTP:

> **Να μην χρησιμοποιείται διακομιστής ειδώλου μόνο HTTP**
> Βεβαιωθείτε ότι ο τοπικός διακομιστής ειδώλου χρησιμοποιεί πρωτόκολλα HTTP και HTTPS ή μόνο HTTPS. Εάν ο διακομιστής ειδώλου χρησιμοποιεί μόνο HTTP, δεν μπορείτε να χρησιμοποιήσετε την εργασία υπολογιστή-πελάτη «Εγκατάσταση λογισμικού», επειδή δεν είναι δυνατή η ανάκτηση της Συμφωνίας Άδειας Χρήσης Τελικού Χρήστη του προϊόντος ασφάλειας ESET από έναν διακομιστή HTTP.

Προεπιλεγμένοι φάκελοι του Mirror Tool	Προϊόν ασφάλειας ESET	Διακομιστής ενημέρωσης (σύμφωνα με την τοποθεσία ρίζας του διακομιστή HTTP)
mirror/eset_upd/era6	ESET PROTECT On-Prem (όλες οι εκδόσεις)	Για να ενημερώσετε το ESET PROTECT On-Prem 11.0 από το είδωλο, ρυθμίστε τον διακομιστή ενημέρωσης σε *http://your_server_address/mirror/eset_upd/era6*
mirror/eset_upd/ep[έκδοση]	ESET Endpoint Antivirus/Security έκδοση 6.x (και νεότερες εκδόσεις) για Windows. Κάθε κύρια έκδοση έχει το φάκελό της, για παράδειγμα *ep10* για την έκδοση 10.x.	*http://your_server_address/mirror/eset_upd/ep10* (ένα παράδειγμα για την έκδοση 10.x)
mirror/eset_upd/v5	ESET Endpoint Antivirus/Security έκδοση 5.x για Windows	*http://your_server_address/mirror/eset_upd/v5*

Προϊόντα ασφάλειας ESET Linux/macOS

Πρέπει να καθορίσετε την παράμετρο `--updateServer` και να δημιουργήσετε πρόσθετους φακέλους για να ενημερώσετε τα προϊόντα ασφάλειας ESET για Linux/macOS από το είδωλο HTTP (βλ. παρακάτω).

--updateServer	Πρόσθετος φάκελος του Mirror Tool	Προϊόν ασφάλειας ESET	Διακομιστής ενημέρωσης (σύμφωνα με την τοποθεσία ρίζας του διακομιστή HTTP)
http://update.eset.com/eset_upd/businesslinux	*mirror/eset_upd/*BusinessLinux	ESET Endpoint Antivirus για Linux	*http://your_server_address/mirror/eset_upd/BusinessLinux*
http://update.eset.com/eset_upd/serverlinux	*mirror/eset_upd/*LinuxServer	ESET Server Security για Linux	*http://your_server_address/mirror/eset_upd/LinuxServer*
http://update.eset.com/eset_upd/businessmac	*mirror/eset_upd/*BusinessMac	ESET Endpoint Security; έκδοση 7.x+ για macOS	*http://your_server_address/mirror/eset_upd/BusinessMac*
http://update.eset.com/eset_mobile/eesa	*mirror/eset_upd/*EndpointAndroid	ESET Endpoint Security for Android	*http://your_server_address/mirror/eset_upd/EndpointAndroid*

[Πίνακας κωδικών γλώσσας]

Για να δημιουργήσετε ένα είδωλο, εκτελέστε το εργαλείο ειδώλου με τις ελάχιστες απαιτούμενες παραμέτρους τουλάχιστον. Ακολουθεί ένα παράδειγμα:

```
MirrorTool.exe --mirrorType regular ^
--intermediateUpdateDirectory c:\temp\mirrorTemp ^
--offlineLicenseFilename c:\temp\offline.lf ^
--outputDirectory c:\temp\mirror
```

Ακολουθεί ένα παράδειγμα πιο προηγμένης ρύθμισης παραμέτρων για ένα αποθετήριο εκτός σύνδεσης με επιλεγμένα προϊόντα, γλώσσες και ενεργοποιημένη λήψη αρχείων παλαιού τύπου, τα οποία καθορίζονται στο αρχείο *filter.txt* (δείτε το παράδειγμα περιεχομένων του αρχείου στις λεπτομέρειες της παραμέτρου `--filterFilePath` παραπάνω):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory c:\temp\repoTemp ^
--outputRepositoryDirectory c:\temp\repository ^
--filterFilePath filter.txt
```

Εργαλείο ειδώλου και ρυθμίσεις ενημέρωσης

• Για να αυτοματοποιήσετε τις λήψεις για ενημερώσεις λειτουργικών μονάδων, μπορείτε να δημιουργήσετε ένα χρονοδιάγραμμα για την εκτέλεση του Εργαλείου ειδώλου. Για να το κάνετε αυτό, ανοίξτε την Κονσόλα διαδικτύου και πλοηγηθείτε στα στοιχεία **Εργασίες υπολογιστή-πελάτη** > **Λειτουργικό σύστημα** > **Εκτέλεση εντολής. Επιλέξτε Γραμμή εντολής που θα εκτελεστεί** (συμπεριλαμβανομένης μιας διαδρομής προς το αρχείο *MirrorTool.exe*) και ένα εύλογο ερέθισμα (όπως μια έκφραση CRON για κάθε ώρα 0 0 * * * ? *). Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το Χρονοδιάγραμμα εργασιών των Windows ή το `Cron` σε Linux.

• Για να διαμορφώσετε τις ενημερώσεις σε έναν ή περισσότερους υπολογιστές-πελάτες, δημιουργήστε μια νέα πολιτική και διαμορφώστε το **Διακομιστή ενημέρωσης** για να κατευθύνει στη διεύθυνση ειδώλου ή τον κοινόχρηστο φάκελό σας.

Εάν χρησιμοποιείτε έναν διακομιστή ειδώλου HTTPS, πρέπει να εισαγάγετε το πιστοποιητικό του στον αξιόπιστο ριζικό αποθηκευτικό χώρο στον υπολογιστή-πελάτη. Ανατρέξτε στο θέμα Εγκατάσταση του αξιόπιστου πιστοποιητικού ρίζας στα Windows.

Διαβάστε αυτό το άρθρο της Γνωσιακής βάσης για να ρυθμίσετε την αλυσίδα του Εργαλείου ειδώλου (ρυθμίστε τις παραμέτρους του Εργαλείου ειδώλου ώστε να λαμβάνει ενημερώσεις από ένα άλλο Εργαλείο ειδώλου).

Εγκατάσταση Σύνδεσης κινητών συσκευών – Windows

Το στοιχείο Διαχείριση/Σύνδεση κινητών συσκευών (Διαχείριση κινητών συσκευών/MDC) του ESET PROTECT (μόνο εσωτερικής εγκατάστασης) φτάνει στο τέλος του κύκλου ζωής τον Ιανουάριο του 2024. Διαβάστε περισσότερα. Συνιστάται η μετεγκατάσταση στο cloud διαχείρισης κινητών συσκευών.

Η Σύνδεση κινητών συσκευών πρέπει να είναι προσβάσιμη από το Internet, έτσι ώστε η διαχείριση των κινητών συσκευών να είναι δυνατή ανά πάσα στιγμή, ανεξάρτητα από την τοποθεσία στην οποία βρίσκονται.

Συνιστάται να αναπτύξετε το στοιχείο MDM σε μια κεντρική συσκευή διαφορετική από τη συσκευή στην οποία φιλοξενείται ο διακομιστής ESET PROTECT.

Ακολουθήστε τα παρακάτω βήματα για να εγκαταστήσετε το στοιχείο Mobile Device Connector για διακομιστή ESET PROTECT σε Windows:

Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης.

1. Επισκεφτείτε την ενότητα λήψεων του ESET PROTECT για λήψη ενός ανεξάρτητου προγράμματος εγκατάστασης για αυτό το στοιχείο του ESET PROTECT (*mdmcore_x64.msi*).

2. Εκτελέστε το πρόγραμμα εγκατάστασης για τη Σύνδεση κινητών συσκευών και αποδεχτείτε την EULA, εάν συμφωνείτε.

3. Κάντε κλικ στο στοιχείο **Αναζήτηση**, πλοηγηθείτε στην τοποθεσία του πιστοποιητικού SSL για

επικοινωνία μέσω HTTPS, πληκτρολογήστε τον κωδικό πρόσβασης για αυτό το πιστοποιητικό.

4. Καθορίστε το **Όνομα κεντρικού υπολογιστή MDM**: αυτό είναι ο δημόσιος τομέας ή η δημόσια διεύθυνση IP του διακομιστή MDM ο οποίος είναι προσβάσιμος από τις κινητές συσκευές μέσω διαδικτύου.

Το όνομα κεντρικού υπολογιστή MDM πρέπει να εισαχθεί με την ίδια μορφή που καθορίζεται στο **πιστοποιητικό διακομιστή HTTPS**, διαφορετικά η κινητή συσκευή iOS θα αρνηθεί να εγκαταστήσει το προφίλ MDM. Για παράδειγμα, εάν υπάρχει διεύθυνση IP καθορισμένη στο πιστοποιητικό HTTPS, πληκτρολογήστε αυτήν τη διεύθυνση IP στο πεδίο **Όνομα κεντρικού υπολογιστή MDM**. Σε περίπτωση που καθορίζεται FQDN (π.χ., `mdm.mycompany.com`) στο πιστοποιητικό HTTPS, εισαγάγετε αυτό το FQDN στο πεδίο **Όνομα κεντρικού υπολογιστή MDM**. Επίσης, εάν χρησιμοποιείται ειδικός χαρακτήρας * (π.χ. `*.mycompany.com`) στο πιστοποιητικό HTTPS, μπορείτε να χρησιμοποιήσετε το `mdm.mycompany.com` στο πεδίο **Όνομα κεντρικού υπολογιστή MDM**.

5. Το πρόγραμμα εγκατάστασης πρέπει να συνδέσει μια υπάρχουσα βάση δεδομένων η οποία θα χρησιμοποιείται από τη Σύνδεση κινητών συσκευών. Καθορίστε τα παρακάτω στοιχεία σύνδεσης:

- **Βάση δεδομένων**: MySQL Server/MS SQL Server/MS SQL Server via Windows Authentication

- **Πρόγραμμα οδήγησης ODBC**: MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/MySQL ODBC 8.1 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server

- **Όνομα βάσης δεδομένων**: Συνιστάται να χρησιμοποιήσετε το προκαθορισμένο όνομα ή να το αλλάξετε, εάν απαιτείται.

- **Όνομα κεντρικού υπολογιστή**: όνομα κεντρικού υπολογιστή ή διεύθυνση IP του διακομιστή βάσης δεδομένων σας

- **Θύρα**: χρησιμοποιείται για σύνδεση με το διακομιστή βάσης δεδομένων

- **Όνομα χρήστη/Κωδικός πρόσβασης** του λογαριασμού διαχειριστή βάσης δεδομένων

- **Χρήση ονόματος παρουσίας** - Εάν χρησιμοποιείτε βάση δεδομένων Microsoft SQL, μπορείτε να επιλέξετε το πλαίσιο ελέγχου **Χρήση ονόματος παρουσίας** για να χρησιμοποιήσετε μια προσαρμοσμένη παρουσία βάσης δεδομένων. Μπορείτε να τη ρυθμίσετε στο πεδίο **Όνομα κεντρικού υπολογιστή** με τη μορφή *HOSTNAME**DB_INSTANCE* (για παράδειγμα, *192.168.0.10**ESMC7SQL*. Για βάση δεδομένων σε σύμπλεγμα, χρησιμοποιήστε μόνο το όνομα συμπλέγματος. Εάν ορίσετε αυτήν την επιλογή, δεν μπορείτε να αλλάξετε τη θύρα σύνδεσης της βάσης δεδομένων - το σύστημα θα χρησιμοποιεί τις προεπιλεγμένες θύρες που προσδιορίζονται από την Microsoft. Για να συνδέσετε τον Διακομιστή ESET PROTECT με τη βάση δεδομένων Microsoft SQL που είναι εγκατεστημένη σε ένα σύμπλεγμα ανακατεύθυνσης, εισαγάγετε το όνομα συμπλέγματος στο πεδίο **Όνομα κεντρικού υπολογιστή**.

Μπορείτε να χρησιμοποιήσετε τον ίδιο διακομιστή βάσης δεδομένων που χρησιμοποιείτε για τη βάση δεδομένων ESET PROTECT, ωστόσο συνιστάται να χρησιμοποιήσετε διαφορετικό διακομιστή βάσης δεδομένων, αν σκοπεύετε να εγγράψετε περισσότερες από 80 κινητές συσκευές.

6. Καθορίστε χρήστη για τη βάση δεδομένων της Σύνδεσης κινητών συσκευών που μόλις δημιουργήθηκε. Μπορείτε να κάνετε **Δημιουργία νέου χρήστη** ή **Χρήση υπάρχοντος χρήστη**

βάσης δεδομένων. Πληκτρολογήστε τον κωδικό πρόσβασης για το χρήστη βάσης δεδομένων.

7. Εισαγάγετε τα στοιχεία **Κεντρικός υπολογιστής διακομιστή** (όνομα ή διεύθυνση IP του διακομιστή ESET PROTECT) και **Θύρα διακομιστή** (η προεπιλεγμένη θύρα είναι 2222, εάν χρησιμοποιείτε διαφορετική θύρα, τότε αντικαταστήστε την προεπιλεγμένη θύρα με τον προσαρμοσμένο αριθμό θύρας σας).

8. Συνδέστε τη σύνδεση MDM στον διακομιστή ESET PROTECT. Συμπληρώστε τα πεδία **Κεντρικός υπολογιστής διακομιστή** και **Θύρα διακομιστή** που απαιτούνται για τη σύνδεση στον διακομιστή ESET PROTECT και επιλέξτε είτε **Εγκατάσταση με υποβοήθηση διακομιστή** είτε **Εγκατάσταση χωρίς σύνδεση**, για να συνεχίσετε:

- **Εγκατάσταση με υποβοήθηση διακομιστή** - Θα πρέπει να παράσχετε τα διαπιστευτήρια διαχειριστή της κονσόλας διαδικτύου ESET PROTECT και το πρόγραμμα εγκατάστασης θα κατεβάσει αυτόματα τα απαιτούμενα πιστοποιητικά. Επίσης, ελέγξτε τα δικαιώματα που απαιτούνται για εγκατάσταση υποβοηθούμενη από το διακομιστή.

    1.Εισαγάγετε τα στοιχεία **Κεντρικός υπολογιστής διακομιστή** - όνομα ή διεύθυνση IP του διακομιστή ESET PROTECT και **Θύρα κονσόλας διαδικτύου** (αφήστε την προεπιλεγμένη θύρα 2223, εάν δεν χρησιμοποιείτε προσαρμοσμένη θύρα). Επίσης, συμπληρώστε τα διαπιστευτήρια λογαριασμού διαχειριστή της κονσόλας διαδικτύου - **Όνομα χρήστη/Κωδικός πρόσβασης**.

    2.Όταν σας ζητηθεί να αποδεχτείτε το πιστοποιητικό, επιλέξτε **Ναι**. Συνεχίστε στο βήμα 10.

- **Εγκατάσταση χωρίς σύνδεση** - Θα πρέπει να παράσχετε ένα **Πιστοποιητικό διακομιστή μεσολάβησης** και μια **Αρχή έκδοσης πιστοποιητικών** που μπορείτε να εξαγάγετε από το ESET PROTECT On-Prem. Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το προσαρμοσμένο πιστοποιητικό και την κατάλληλη αρχή έκδοσης πιστοποιητικών.

    1.Κάντε κλικ στην **Αναζήτηση** δίπλα στο ομότιμο πιστοποιητικό και μεταβείτε στην τοποθεσία του **ομότιμου πιστοποιητικού** σας (αυτό είναι το πιστοποιητικό διακομιστή μεσολάβησης που έχετε εξαγάγει από το ESET PROTECT On-Prem). Αφήστε κενό το πεδίο κειμένου **Κωδικός πρόσβασης πιστοποιητικού** επειδή αυτό το πιστοποιητικό δεν απαιτεί κωδικό πρόσβασης.

    2.Επαναλάβετε τη διαδικασία για την αρχή έκδοσης πιστοποιητικών και συνεχίστε στο βήμα 10.

> **i** Σε περίπτωση που χρησιμοποιείτε προσαρμοσμένα πιστοποιητικά με το ESET PROTECT On-Prem (αντί των προεπιλεγμένων που δημιουργήθηκαν αυτόματα κατά την εγκατάσταση του ESET PROTECT On-Prem), θα πρέπει να χρησιμοποιήσετε αυτά όταν σας ζητηθεί να καθορίσετε πιστοποιητικό διακομιστή μεσολάβησης.

9. Καθορίστε έναν φάκελο προορισμού για τη Σύνδεση κινητών συσκευών (συνιστάται να χρησιμοποιήσετε τον προεπιλεγμένο φάκελο), επιλέξτε **Επόμενο** και, στη συνέχεια, **Εγκατάσταση**.

10. Μετά την ολοκλήρωση της εγκατάστασης, ελέγξτε εάν εκτελείται σωστά το Mobile Device Connector ανοίγοντας τη διεύθυνση *https://your-mdm-hostname:enrollment-port* (για παράδειγμα *https://mdm.company.com:9980*) στο πρόγραμμα περιήγησής σας ή από μια κινητή συσκευή. Εάν η εγκατάσταση ήταν επιτυχής, θα δείτε το ακόλουθο μήνυμα: MDM - Ο διακομιστής είναι

ενεργοποιημένος και εκτελείται!

11. Τώρα μπορείτε να ενεργοποιήσετε το MDM από το ESET PROTECT On-Prem.

Προαπαιτούμενα Σύνδεσης κινητών συσκευών

Εάν αλλάξει η θύρα ή το όνομα κεντρικού υπολογιστή για το διακομιστή MDM, πρέπει να εγγραφούν εκ νέου όλες οι κινητές συσκευές.
Για αυτό το λόγο, συνιστάται να ρυθμίσετε ένα αποκλειστικό όνομα κεντρικού υπολογιστή για το διακομιστή MDM, έτσι ώστε εάν χρειαστεί ποτέ να αλλάξετε την κεντρική συσκευή του διακομιστή MDM, θα μπορείτε να το κάνετε με εκ νέου αντιστοίχιση της διεύθυνσης IP της νέας κεντρικής συσκευής με το όνομα κεντρικού υπολογιστή MDM στις ρυθμίσεις DNS.

Για την εγκατάσταση της σύνδεσης κινητών συσκευών σε λειτουργικό σύστημα Windows, πρέπει να πληρούνται τα παρακάτω προαπαιτούμενα:

- Δημόσια διεύθυνση IP/όνομα κεντρικού υπολογιστή ή δημόσιος τομέας προσβάσιμα από το διαδίκτυο.

Εάν πρέπει να αλλάξετε το όνομα κεντρικού υπολογιστή του διακομιστή MDM, θα πρέπει να πραγματοποιήσετε εγκατάσταση επιδιόρθωσης για το στοιχείο MDC. Εάν αλλάξετε το όνομα κεντρικού υπολογιστή του διακομιστή MDM, θα πρέπει να εισαγάγετε ένα νέο **πιστοποιητικό διακομιστή HTTPS** που θα περιλαμβάνει το νέο όνομα κεντρικού υπολογιστή, προκειμένου το MDM να συνεχίσει να λειτουργεί σωστά.

- Θύρες ανοιχτές και διαθέσιμες - δείτε την πλήρη λίστα θυρών εδώ. Συνιστάται να χρησιμοποιήσετε τις προεπιλεγμένες θύρες 9981 και 9980. Ωστόσο, μπορείτε να τις αλλάξετε στο αρχείο διαμόρφωσης του διακομιστή MDM, εάν χρειάζεται. Βεβαιωθείτε ότι οι κινητές συσκευές είναι σε θέση να συνδεθούν μέσω των καθορισμένων θυρών. Για να γίνει αυτό, αλλάξτε τις ρυθμίσεις firewall ή/και δικτύου (εάν εφαρμόζεται). Διαβάστε περισσότερα για την αρχιτεκτονική MDM.

- Ρυθμίσεις τείχους προστασίας - όταν εγκαθιστάτε τη Σύνδεση κινητών συσκευών σε λειτουργικά συστήματα χωρίς διακομιστή, όπως τα Windows 7 (μόνο για σκοπούς αξιολόγησης), βεβαιωθείτε ότι επιτρέπονται οι θύρες επικοινωνίας δημιουργώντας κανόνες τείχους προστασίας για:

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, θύρα TCP 9980

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, θύρα TCP 9981

C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, θύρα TCP 2222

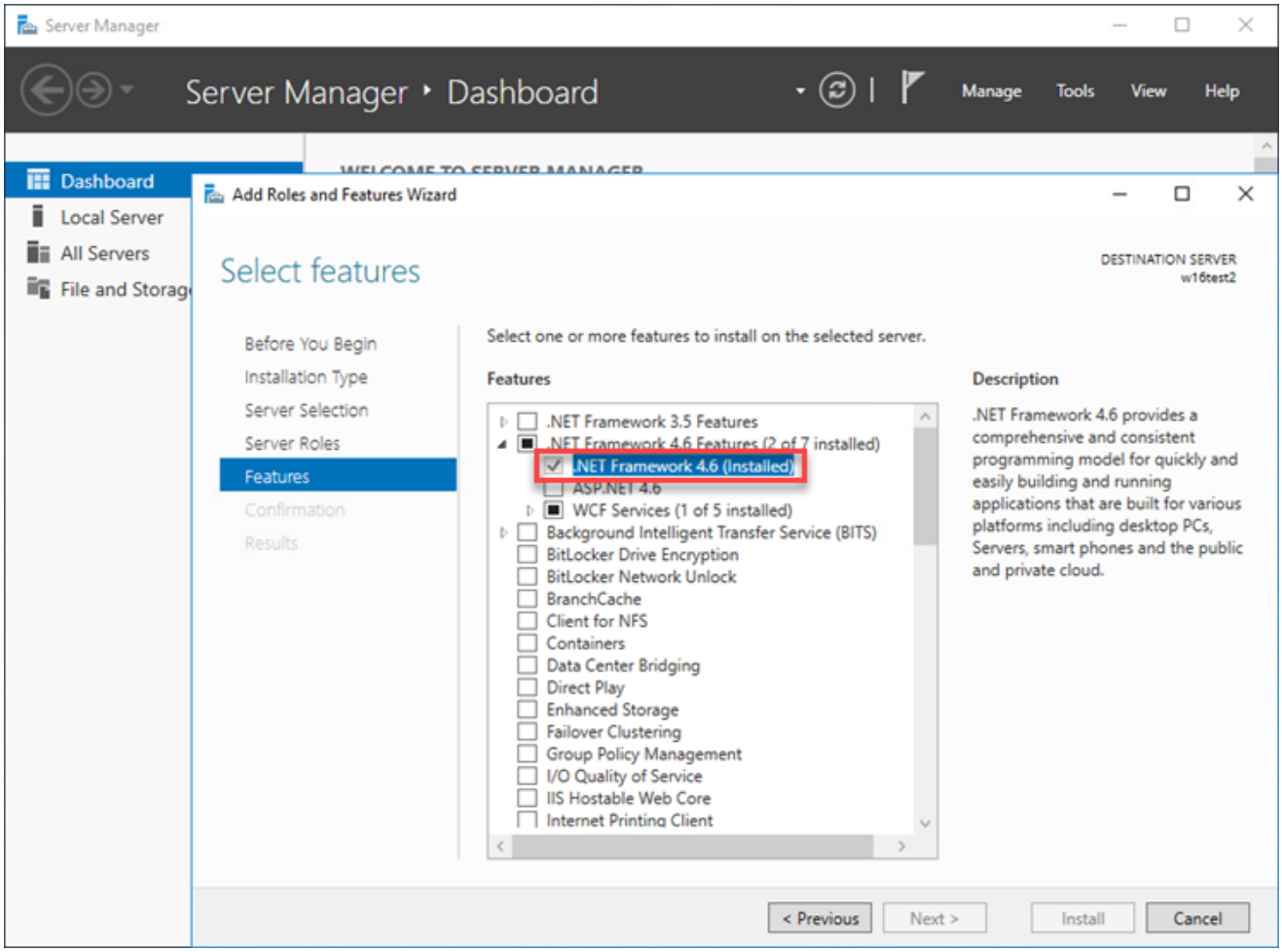
Οι πραγματικές διαδρομές προς τα αρχεία *.exe* ενδέχεται να διαφέρουν, ανάλογα με το σημείο στο οποίο εγκαθίστανται τα στοιχεία ESET PROTECT στο λειτουργικό σύστημα του υπολογιστή-πελάτη.

- Να έχει ήδη εγκατασταθεί και διαμορφωθεί ένας διακομιστής βάσης δεδομένων. Βεβαιωθείτε

ότι ικανοποιούνται οι απαιτήσεις Microsoft SQL ή MySQL.

• Η χρήση RAM της σύνδεσης MDM είναι βελτιστοποιημένη ώστε να μπορούν να εκτελούνται ταυτόχρονα έως και 48 διεργασίες «MDMCore Module ESET PROTECT» και, εάν ο χρήστης συνδέσει περισσότερες συσκευές, οι διεργασίες να αλλάζουν περιοδικά για κάθε συσκευή που χρειάζεται τη δεδομένη στιγμή τους πόρους.

• Η εγκατάσταση του Microsoft SQL Server Express απαιτεί το Microsoft .NET Framework 4. Μπορείτε να το εγκαταστήσετε χρησιμοποιώντας το στοιχείο **Οδηγός προσθήκης ρόλων και δυνατοτήτων**:



Απαιτήσεις πιστοποιητικού

• Θα χρειαστείτε ένα **Πιστοποιητικό SSL** σε μορφή *.pfx*για ασφαλή επικοινωνία μέσω HTTPS. Συνιστάται να χρησιμοποιήσετε ένα πιστοποιητικό που παρέχεται από μια Αρχή έκδοσης πιστοποιητικού άλλου κατασκευαστή. Τα αυτο-υπογεγραμμένα πιστοποιητικά (που περιλαμβάνουν πιστοποιητικά που υπογράφονται από την Αρχή έκδοσης πιστοποιητικού του ESET PROTECT On-Prem δεν συνιστώνται, επειδή δεν επιτρέπουν όλες οι κινητές συσκευές στους χρήστες να αποδέχονται αυτο-υπογεγραμμένα πιστοποιητικά.

• Θα πρέπει να έχετε πιστοποιητικό υπογεγραμμένο από την αρχή έκδοσης πιστοποιητικού και το αντίστοιχο ιδιωτικό κλειδί, και να χρησιμοποιήσετε τις τυπικές διαδικασίες (χρησιμοποιώντας συνήθως OpenSSL) για να συγχωνεύσετε αυτά τα δύο σε ένα αρχείο *.pfx*:

```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out
httpsCredentials.pfx
```

Αυτή είναι η τυπική διαδικασία για τους περισσότερους διακομιστές που χρησιμοποιούν πιστοποιητικά SSL.

• Για Εγκατάσταση χωρίς σύνδεση, θα χρειαστείτε επίσης ένα ομότιμο πιστοποιητικό (το **Πιστοποιητικό φορέα** το οποίο μπορείτε να εξαγάγετε από το ESET PROTECT On-Prem). Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το προσαρμοσμένο πιστοποιητικό με το ESET PROTECT On-Prem.

Ενεργοποίηση Σύνδεσης κινητών συσκευών

Μετά από την εγκατάσταση της σύνδεσης κινητών συσκευών, πρέπει να την ενεργοποιήσετε με μια άδεια χρήσης ESET τερματικού, επιχείρησης ή γραφείου:

1.Προσθέστε την άδεια χρήσης ESET Endpoint, Business ή Office στη Διαχείριση αδειών χρήσης του ESET PROTECT On-Prem.

2.Ενεργοποιήστε το Mobile Device Connector χρησιμοποιώντας μια εργασία υπολογιστή-πελάτη Ενεργοποίησης προϊόντος. Αυτή η διαδικασία είναι η ίδια όπως όταν ενεργοποιείτε οποιοδήποτε προϊόν της ESET σε υπολογιστή-πελάτη. Σε αυτή την περίπτωση, η Σύνδεση κινητών συσκευών είναι ο υπολογιστής-πελάτης.

Λειτουργικότητα αδειοδότησης MDM iOS

Καθώς η ESET δεν παρέχει κάποια εφαρμογή στο κατάστημα Apple App Store, η Σύνδεση κινητών συσκευών αποθηκεύει όλα τα στοιχεία αδειοδότησης για συσκευές iOS.

Οι άδειες χρήσης προορίζονται ανά συσκευή και μπορούν να ενεργοποιηθούν με εργασία ενεργοποίησης προϊόντος (όπως και οι συσκευές Android).

Οι άδειες χρήσης iOS μπορούν να απενεργοποιηθούν με τους εξής τρόπους:

- Κατάργηση της συσκευής από τη διαχείριση μέσω εργασίας διακοπής διαχείρισης
- Κατάργηση εγκατάστασης του MDC μέσω της επιλογής **Κατάργηση βάσης δεδομένων**
- Απενεργοποίηση με άλλους τρόπους (απενεργοποίηση του ESET PROTECT On-Prem ή του EBA)

Επειδή το MDC επικοινωνεί με τους διακομιστές αδειοδότησης της ESET για λογαριασμός των συσκευών iOS, η πύλη EBA αντικατοπτρίζει την κατάσταση του MDC και όχι την κατάσταση μεμονωμένων συσκευών. Οι τρέχουσες πληροφορίες συσκευών είναι πάντα διαθέσιμες στην Κονσόλα διαδικτύου του ESET PROTECT.

Οι συσκευές που δεν είναι ενεργοποιημένες ή οι συσκευές με ληγμένες άδειες χρήσης θα εμφανίζουν μια κόκκινη κατάσταση προστασίας και το μήνυμα «Το προϊόν δεν έχει ενεργοποιηθεί». Αυτές οι συσκευές θα αρνηθούν να χειρίζονται εργασίες, να καθορίζουν πολιτικές και να παραδίδουν μη κρίσιμα αρχεία καταγραφής.

Κατά την εγκατάσταση του MDM, εάν έχει επιλεγεί η ρύθμιση **Να μην καταργηθεί η βάση δεδομένων**, οι άδειες χρήσης που χρησιμοποιούνται δεν θα είναι απενεργοποιημένες. Αυτές οι άδειες χρήσης μπορούν να επαναχρησιμοποιηθούν εάν το MDM επανεγκατασταθεί σε αυτήν τη βάση

δεδομένων, καταργηθεί μέσω του ESET PROTECT On-Prem ή μέσω απενεργοποίησης του EBA. Κατά τη μεταφορά σε άλλο διακομιστή MDM, θα χρειαστεί να πραγματοποιήσετε ξανά την εργασία ενεργοποίησης προϊόντος.

Απαιτήσεις πιστοποιητικού HTTPS

Για να εγγράψετε μια κινητή συσκευή στη Σύνδεση κινητών συσκευών ESET, βεβαιωθείτε ότι ο διακομιστής HTTPS επιστρέφει την πλήρη αλυσίδα πιστοποιητικού.

Για να λειτουργεί σωστά το πιστοποιητικό, πρέπει να ικανοποιούνται οι εξής απαιτήσεις:

- Το πιστοποιητικό HTTPS (κοντέινερ pkcs#12/pfx) πρέπει να περιέχει την πλήρη αλυσίδα πιστοποιητικού, συμπεριλαμβανομένης της ριζικής αρχής έκδοσης πιστοποιητικού.
- Το πιστοποιητικό πρέπει να είναι έγκυρο κατά το απαιτούμενο διάστημα (ισχύς από / ισχύς μέχρι).
- Το **CommonName** ή τα **subjectAltNames** πρέπει να συμφωνούν με το όνομα κεντρικού υπολογιστή MDM.

Εάν το **Όνομα κεντρικού υπολογιστή MDM** είναι, για παράδειγμα, hostname.mdm.domain.com, το πιστοποιητικό σας μπορεί να περιέχει ονόματα όπως:
- hostname.mdm.domain.com
- *.mdm.domain.com

Αλλά όχι ονόματα όπως:
- *
- *.com
- *.domain.com

Βασικά, το « * » δεν μπορεί να αντικαταστήσει την τελεία. Αυτή η συμπεριφορά επιβεβαιώνεται για τον τρόπο με τον οποίο το iOS δέχεται τα πιστοποιητικά για το MDM.

Σημειώνεται ότι ορισμένες συσκευές λαμβάνουν υπόψη την τρέχουσα ζώνη ώρας όταν ελέγχουν την εγκυρότητα του πιστοποιητικού, ενώ άλλες συσκευές δεν το κάνουν. Αποφύγετε δυνητικά προβλήματα δίνοντας στο πιστοποιητικό εγκυρότητα για μία ή δύο ημέρες πριν από την τρέχουσα ημερομηνία.

Αποθετήριο χωρίς σύνδεση – Windows

Μπορείτε να χρησιμοποιήσετε το εργαλείο ειδώλου για να δημιουργήσετε ένα αποθετήριο εκτός σύνδεσης (σε Windows). Συνήθως, αυτό χρειάζεται για κλειστά δίκτυα υπολογιστών ή δίκτυα με περιορισμένη πρόσβαση στο Internet. Το εργαλείο ειδώλου μπορεί να χρησιμοποιηθεί για την κλωνοποίηση του χώρου αποθήκευσης ESET σε έναν τοπικό φάκελο. Αυτός ο κλωνοποιημένος χώρος αποθήκευσης μπορεί να μετακινηθεί στη συνέχεια (για παράδειγμα, με μια εξωτερική μονάδα δίσκου) σε μια τοποθεσία στο κλειστό δίκτυο. Μπορείτε να αντιγράψετε το αποθετήριο σε μια ασφαλή θέση στο τοπικό δίκτυο και να τον καταστήσετε διαθέσιμο μέσω διακομιστή HTTP (π.χ. ESET Bridge).

Για να ενημερώσετε το χώρο αποθήκευσης χωρίς σύνδεση, εκτελέστε την ίδια εντολή με τις ίδιες παραμέτρους που χρησιμοποιούνται για τη δημιουργία του χώρου αποθήκευσης χωρίς σύνδεση. Τα προηγούμενα δεδομένα στον ενδιάμεσο φάκελο θα ξαναχρησιμοποιηθούν. Θα ληφθούν μόνο τα μη ενημερωμένα αρχεία.

Έχετε υπόψη ότι το μέγεθος του αποθετηρίου μεγαλώνει και ο ενδιάμεσος κατάλογος θα έχει το ίδιο μέγεθος. Βεβαιωθείτε ότι έχετε ελεύθερο χώρο τουλάχιστον **1.2 TB** προτού ξεκινήσετε αυτήν τη διαδικασία.

Βέλτιστες πρακτικές

Ανατρέξτε επίσης στο άρθρο της Γνωσιακής βάσης της ESET Βέλτιστες πρακτικές για τη χρήση του ESET PROTECT On-Prem σε ένα περιβάλλον χωρίς σύνδεση.

Παραδείγματα σεναρίων για τα Windows

I. Δημιουργία κλώνου του χώρου αποθήκευσης

1. Κάντε λήψη του εργαλείου ειδώλου.

2. Εξαγάγετε το εργαλείο ειδώλου από το αρχείο *.zip* που λάβατε.

3. Προετοιμάστε (δημιουργήστε) φακέλους για:

   - τα ενδιάμεσα αρχεία
   - τον τελικό χώρο αποθήκευσης

4. Ανοίξτε μια γραμμή εντολής και αλλάξτε τον κατάλογο στο φάκελο όπου έχετε εξαγάγει το εργαλείο ειδώλου (εντολή `cd`).

5. Εκτελέστε την παρακάτω εντολή (αλλάξτε τους ενδιάμεσους καταλόγους και τον κατάλογο του τελικού χώρου αποθήκευσης στους αντίστοιχους φακέλους από το βήμα 3):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory C:\Intermediary ^
--outputRepositoryDirectory C:\Repository
```

6. Αφού αντιγράψετε το χώρο αποθήκευσης στο φάκελο `outputRepositoryDirectory`, μετακινήστε το φάκελο και τα περιεχόμενά του σε άλλον υπολογιστή, από τον οποίο έχετε πρόσβαση στο κλειστό σας δίκτυο.

II. Ρύθμιση διακομιστή HTTP

1. Θα πρέπει να εκτελείται διακομιστής HTTP στον υπολογιστή που έχει πρόσβαση στο κλειστό δίκτυο. Μπορείτε να χρησιμοποιήσετε:

   - Τον διακομιστή μεσολάβησης ESET Bridge από τον ιστότοπο λήψεων της ESET (για αυτό το σενάριο)
   - έναν διαφορετικό διακομιστή HTTP

2. Εγκατάσταση του διακομιστή μεσολάβησης ESET Bridge.

III. Εκτέλεση του χώρου αποθήκευσης χωρίς σύνδεση

1. Μεταβείτε στη διαδρομή *C:\Program Files\ESET\Bridge* και ανοίξτε το αρχείο *pkgid* χρησιμοποιώντας ένα απλό πρόγραμμα επεξεργασίας κειμένου. Αλλάξτε τη ρύθμιση `http_proxy_settings_static_content_enabled` σε `true` για να ενεργοποιήσετε τον διακομιστή αποθετηρίου χωρίς σύνδεση. Αποθηκεύστε τις αλλαγές και κλείστε το αρχείο *pkgid*.

2. Αντιγράψτε το αποθετήριο του οποίου πραγματοποιήθηκε λήψη στο βήμα 6 (παραπάνω ενότητα I.) στον κατάλογο διακομιστή αποθετηρίου εκτός σύνδεσης:

• Ο προεπιλεγμένος κατάλογος διακομιστή αποθετηρίου εκτός σύνδεσης βρίσκεται στη διαδρομή *C:\ProgramData\ESET\Bridge\OfflineRepository* με τα κατάλληλα δικαιώματα πρόσβασης.

• Για να χρησιμοποιήσετε έναν προσαρμοσμένο κατάλογο, δημιουργήστε έναν νέο φάκελο για το αποθετήριο χωρίς σύνδεση (για παράδειγμα, *C:\Repository*). Στο αρχείο *pkgid*, αντικαταστήστε τη γραμμή `"http_proxy_settings_offline_repository_dirPath": "%DATADIR%\\OfflineRepository"` με τη γραμμή `"http_proxy_settings_offline_repository_dirPath": "C:\\Repository"`. Ο χρήστης NETWORK SERVICE χρειάζεται πλήρη δικαιώματα πρόσβασης στον κατάλογο.

3. Επανεκκινήστε την υπηρεσία ESET Bridge χρησιμοποιώντας τις εντολές της γραμμής εντολών: `net stop "EsetBridge"` και `net start "EsetBridge"`. Πρέπει να επανεκκινείτε την υπηρεσία μόνο μετά την αλλαγή του αρχείου *pkgid* – η επανεκκίνηση της υπηρεσίας δεν είναι απαραίτητη όταν αλλάζουν διαγράφονται ή προστίθενται τα δεδομένα του αποθετηρίου.

4. Το αποθετήριο χωρίς σύνδεση εκτελείται στη διεύθυνση *http://YourIPaddress:4449* (για παράδειγμα, *http://10.1.1.10:4449*).

5. Ρυθμίστε τη νέα διεύθυνση αποθετηρίου χρησιμοποιώντας την Κονσόλα διαδικτύου ESET PROTECT:

a.Διακομιστής ESET PROTECT - Κάντε κλικ στα στοιχεία **Περισσότερα** > **PPυθμίσεις** > **Ρυθμίσεις για προχωρημένους** > **Αποθετήριο** και εισαγάγετε τη διεύθυνση αποθετηρίου χωρίς σύνδεση στο πεδίο **Διακομιστής.**

b.Φορείς ESET Management - Κάντε κλικ στις **Πολιτικές**, κάντε κλικ στην Πολιτική φορέα > **Επεξεργασία** > **Ρυθμίσεις** > **Ρυθμίσεις για προχωρημένους** > **Αποθετήριο** > εισαγάγετε τη διεύθυνση αποθετηρίου χωρίς σύνδεση στο πεδίο **Διακομιστής.**

c.Προϊόντα ESET Endpoint (για Windows) - Κάντε κλικ στις **Πολιτικές**, κάντε κλικ στην πολιτική **ESET Endpoint για Windows** > **Επεξεργασία** > **Ρυθμίσεις** > **Ενημέρωση** > **Προφίλ** > **Ενημερώσεις** > **Ενημερώσεις λειτουργικών μονάδων** > εισαγάγετε τη διεύθυνση αποθετηρίου χωρίς σύνδεση στο πεδίο **Προσαρμοσμένος διακομιστής**.

Cluster ανακατεύθυνσης – WIndows

Παρακάτω αναφέρονται τα βήματα υψηλού επιπέδου που απαιτούνται για την εγκατάσταση του ESET PROTECT On-Prem σε ένα περιβάλλον συμπλέγματος ανακατεύθυνσης.

Δείτε επίσης αυτό το άρθρο της Γνωσιακής βάσης σχετικά με την εγκατάσταση συμπλεγμάτων του διακομιστή ESET PROTECT.

1. Δημιουργήστε ένα σύμπλεγμα ανακατεύθυνσης με κοινόχρηστο δίσκο:

- Οδηγίες για τη δημιουργία cluster στο Windows Server 2016 και 2019
- Οδηγίες για τη δημιουργία cluster ανακατεύθυνσης στο Windows Server 2012 και 2012 R2

2. Στον **Οδηγό δημιουργίας συμπλέγματος**, εισαγάγετε το επιθυμητό όνομα κεντρικού υπολογιστή (καθορίστε εσείς ένα) και τη διεύθυνση IP.

3. Μεταφέρετε τον κοινόχρηστο δίσκο του συμπλέγματος στον κόμβο 1 και εγκαταστήστε το διακομιστή ESET PROTECT χρησιμοποιώντας το ανεξάρτητο πρόγραμμα εγκατάστασης στον κόμβο 1. Βεβαιωθείτε ότι το στοιχείο **Αυτή είναι εγκατάσταση συμπλέγματος** είναι επιλεγμένο κατά την εγκατάσταση και επιλέξτε τον κοινόχρηστο δίσκο ως μονάδα αποθήκευσης δεδομένων εφαρμογής. Καθορίστε ένα όνομα κεντρικού υπολογιστή και εισαγάγετέ το για το πιστοποιητικό διακομιστή του ESET PROTECT Server δίπλα στα προσυμπληρωμένα ονόματα κεντρικού υπολογιστή. Απομνημονεύστε αυτό το όνομα κεντρικού υπολογιστή και χρησιμοποιήστε το στο βήμα 6, κατά τη δημιουργία του ρόλου διακομιστή ESET PROTECT στη Διαχείριση συμπλέγματος.

4. Διακόψτε το ESET PROTECT Server στον κόμβο 1, μεταφέρετε τον κοινόχρηστο δίσκο στον κόμβο 2 και εγκαταστήστε το διακομιστή ESET PROTECT χρησιμοποιώντας το ανεξάρτητο πρόγραμμα εγκατάστασης στον κόμβο 2. Βεβαιωθείτε ότι το στοιχείο **Αυτή είναι εγκατάσταση συμπλέγματος** είναι επιλεγμένο κατά την εγκατάσταση. Επιλέξτε τον κοινόχρηστο δίσκο ως αποθηκευτικό χώρο δεδομένων της εφαρμογής. Διατηρήστε τις πληροφορίες σύνδεσης και πιστοποιητικών της βάσης δεδομένων ως έχουν (όπως διαμορφώθηκαν κατά την εγκατάσταση του ESET PROTECT Server στον κόμβο 1).

5. Διαμορφώστε το firewall ώστε να επιτρέπει εισερχόμενες συνδέσεις σε όλες τις θύρες που χρησιμοποιούνται από το ESET PROTECT Server.

6. Στη διαχείριση διαμόρφωσης συμπλέγματος, δημιουργήστε και ξεκινήστε έναν ρόλο (**Διαμόρφωση ρόλου** > **Επιλογή ρόλου** > **Γενική υπηρεσία**) για την υπηρεσία διακομιστή ESET PROTECT. Επιλέξτε την υπηρεσία **Διακομιστής ESET PROTECT** από τη λίστα διαθέσιμων υπηρεσιών. Είναι πολύ σημαντικό να χρησιμοποιήσετε το ίδιο όνομα κεντρικού υπολογιστή για το ρόλο με αυτό που χρησιμοποιήθηκε στο βήμα 3 για το πιστοποιητικό διακομιστή.

7. Εγκαταστήστε το φορέα ESET Management σε όλους τους κόμβους του συμπλέγματος χρησιμοποιώντας το ανεξάρτητο πρόγραμμα εγκατάστασης. Στις οθόνες **Διαμόρφωση φορέα** και **Σύνδεση με το διακομιστή ESET PROTECT** χρησιμοποιήστε το όνομα κεντρικού υπολογιστή που χρησιμοποιήσατε στο βήμα 6. Αποθηκεύστε τα δεδομένα του φορέα στον τοπικό κόμβο (όχι στο δίσκο του cluster).

8. Ο διακομιστής διαδικτύου (Apache Tomcat) δεν υποστηρίζεται σε cluster, συνεπώς θα πρέπει να τον εγκαταστήσετε σε δίσκο που δεν ανήκει σε cluster ή σε διαφορετικό υπολογιστή:

a. Εγκαταστήστε την Κονσόλα διαδικτύου σε ξεχωριστό υπολογιστή και ρυθμίστε τις παραμέτρους της σωστά για να συνδέεται με το διακομιστή ESET PROTECT με ρόλο cluster.

b. εντοπίστε το αρχείο διαμόρφωσής της στη διαδρομή: *C:\Program Files\Apache Software Foundation\[Tomcat* φάκελος *]\webapps\era\WEB-*

INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

c.Ανοίξτε το αρχείο στο Σημειωματάριο ή σε άλλο επεξεργαστή απλού κειμένου. Στη γραμμή της παραμέτρου `server_address=localhost` αντικαταστήστε το «localhost» με τη διεύθυνση IP ή το όνομα κεντρικού υπολογιστή του ρόλου cluster του διακομιστή ESET PROTECT.

Εγκατάσταση στοιχείου στο Linux

Στα περισσότερα σενάρια εγκατάστασης, πρέπει να εγκαταστήσετε διαφορετικά στοιχεία του ESET PROTECT σε διαφορετικούς υπολογιστές ώστε να εξυπηρετούνται οι διαφορετικές αρχιτεκτονικές δικτύου, να πληρούνται οι απαιτήσεις επιδόσεων ή για άλλους λόγους.

Ακολουθήστε τις οδηγίες βήμα προς βήμα για την εγκατάσταση του ESET PROTECT On-Prem.

Εγκατάσταση βασικών στοιχείων:

- ESET PROTECTΔιακομιστής
- Κονσόλα διαδικτύου ESET PROTECT – Μπορείτε να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT σε έναν διαφορετικό υπολογιστή από τον υπολογιστή στον οποίο εκτελείται ο διακομιστής ESET PROTECT.
- Φορέας ESET Management
- ένας διακομιστής βάσης δεδομένων

Εγκατάσταση προαιρετικών στοιχείων:

- Αισθητήρας RD
- Σύνδεση κινητών συσκευών
- ESET Bridge Διακομιστής Μεσολάβησης HTTP
- Εργαλείο ειδώλου

Για να αναβαθμίσετε το ESET PROTECT On-Prem για Linux στην πιο πρόσφατη έκδοση, ανατρέξτε στο κεφάλαιο Εργασία αναβάθμισης στοιχείων ή στο σχετικό άρθρο της Γνωσιακής βάσης.

Εγκατάσταση βήμα προς βήμα του ESET PROTECT On-Prem σε σύστημα Linux

Σε αυτό το σενάριο εγκατάστασης θα προσομοιώσουμε την εγκατάσταση του διακομιστή ESET PROTECT και της κονσόλας διαδικτύου ESET PROTECT βήμα προς βήμα. Θα προσομοιώσουμε την εγκατάσταση με χρήση MySQL.

Οδηγίες εγκατάστασης για επιλεγμένες διανομές Linux

Μπορείτε να ακολουθήσετε τα άρθρα της Γνωσιακής βάσης με οδηγίες ειδικά για τη διανομή:

- CentOS 7
- Debian 10
- SUSE Linux Enterprise Server (SLES)

Πριν από την εγκατάσταση

1. Επαληθεύστε ότι ο διακομιστής βάσης δεδομένων υπάρχει στο δίκτυό σας και βεβαιωθείτε ότι έχετε πρόσβαση σε αυτόν στον τοπικό/απομακρυσμένο διακομιστή σας. Εάν δεν έχει εγκατασταθεί διακομιστής βάσης δεδομένων, εγκαταστήστε και ρυθμίστε τις παραμέτρους σε έναν νέο.

2. Πραγματοποιήστε λήψη των ανεξάρτητων στοιχείων του ESET PROTECT για Linux (Φορέα, Διακομιστή, Κονσόλα διαδικτύου). Μπορείτε να βρείτε αυτά τα αρχεία εγκατάστασης στην κατηγορία Ανεξάρτητα προγράμματα εγκατάστασης του ESET PROTECT που είναι διαθέσιμα στον ιστότοπο της ESET.

Διαδικασία εγκατάστασης

Πρέπει να μπορείτε να χρησιμοποιήσετε την εντολή `sudo` ή δικαιώματα `root` για να ολοκληρώσετε την εγκατάσταση.

1. Εγκαταστήστε τα απαιτούμενα πακέτα για το διακομιστή ESET PROTECT.

2. Διαμορφώστε τη σύνδεση με το διακομιστή MySQL, όπως περιγράφεται στο θέμα Διαμόρφωση MySQL.

3. Επιβεβαίωση της ρύθμισης παραμέτρων του προγράμματος οδήγησης MySQL ODBC. Ανατρέξτε στην ενότητα Εγκατάσταση και ρύθμιση παραμέτρων ODBC) για περισσότερες πληροφορίες.

4. Προσαρμόστε τις παραμέτρους εγκατάστασης και εκτελέστε την εγκατάσταση διακομιστή ESET PROTECT. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Εγκατάσταση διακομιστή - Linux.

5. Εγκαταστήστε τα απαιτούμενα πακέτα Java και Tomcat και εγκαταστήστε την κονσόλα διαδικτύου ESET PROTECT. Εάν αντιμετωπίσετε προβλήματα με τη σύνδεση HTTPS στην κονσόλα διαδικτύου ESET PROTECT, ανατρέξτε στο θέμα Ρυθμίσεις της σύνδεσης HTTPS/SSL.

6. Εγκαταστήστε το φορέα ESET Management στον υπολογιστή του διακομιστή.

Συνιστάται να καταργήσετε εντολές που περιέχουν ευαίσθητα δεδομένα (για παράδειγμα, έναν κωδικό πρόσβασης) από το ιστορικό της γραμμής εντολών:
1.Εκτελέστε το στοιχείο `history` για να δείτε τη λίστα όλων των εντολών στο ιστορικό.
2.Εκτελέστε το στοιχείο `history -d line_number` (καθορίστε τον αριθμό γραμμής της εντολής). Εναλλακτικά, εκτελέστε το στοιχείο `history -c` για να καταργήσετε ολόκληρο το ιστορικό της γραμμής εντολών.

Εγκατάσταση και διαμόρφωση MySQL

Εγκατάσταση

> Βεβαιωθείτε ότι έχετε εγκαταστήσει μια υποστηριζόμενη έκδοση του διακομιστή MySQL και της σύνδεσης ODBC.

Εάν έχετε ήδη εγκαταστήσει και διαμορφώσει το MySQL, προχωρήστε στη Διαμόρφωση.

1. Προσθήκη του αποθετηρίου MySQL:

Debian, Ubuntu	Εκτελέστε τις ακόλουθες εντολές στο τερματικό:
	`a)wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb`
	`b)sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb`
	Μπορείτε να επιλέξετε τις εκδόσεις των στοιχείων που θέλετε να εγκαταστήσετε κατά την εγκατάσταση του πακέτου. Συνιστάται να ορίσετε τις προεπιλογές. Δείτε επίσης Προσθήκη του χώρου αποθήκευσης MySQL APT

CentOS, Red Hat	Προσθήκη του χώρου αποθήκευσης MySQL Yum
SUSE Linux Enterprise Server	Προσθήκη του χώρου αποθήκευσης MySQL SLES

2. Ενημερώστε την προσωρινή μνήμη του τοπικού αποθετηρίου:

Debian, Ubuntu	`sudo apt-get update`
CentOS, Red Hat	`sudo yum update`
SUSE Linux Enterprise Server	`sudo zypper update`

3. Η εγκατάσταση του MySQL διαφέρει ανάλογα με τη διανομή Linux και την έκδοση που χρησιμοποιείται:

Linux **διανομή:**	MySQL **Εντολή εγκατάστασης διακομιστή:**	MySQL **Προηγμένη εγκατάσταση διακομιστή:**
Debian, Ubuntu	`sudo apt-get install mysql-server`	Installing MySQL from Source with the MySQL APT Repository
CentOS, Red Hat	`sudo yum install mysql-community-server`	Installing MySQL on Linux Using the MySQL Yum Repository
SUSE Linux Enterprise Server	`sudo zypper install mysql-community-server`	Steps for a Fresh Installation of MySQL

Λήψη του MySQL Community Server για μη αυτόματη εγκατάσταση.

Διαμόρφωση

1. Ανοίξτε το αρχείο ρύθμισης παραμέτρων *my.cnf* σε ένα πρόγραμμα επεξεργασίας κειμένου:

```
sudo nano /etc/my.cnf
```

Εάν το αρχείο δεν υπάρχει, δοκιμάστε το `/etc/mysql/my.cnf` ή το `/etc/my.cnf.d/community-mysql-server.cnf` ή το `/etc/mysql/mysql.conf.d/mysqld.cnf`.

2. Βρείτε την παρακάτω διαμόρφωση στην ενότητα `[mysqld]` του αρχείου *my.cnf* και επεξεργαστείτε τις τιμές.

- Δημιουργήστε την ενότητα `[mysqld]` εάν δεν υπάρχει στο αρχείο.
- Εάν οι παράμετροι δεν υπάρχουν στο αρχείο, προσθέστε τις στην ενότητα `[mysqld]`.
- Για να προσδιορίσετε την έκδοση MySQL, εκτελέστε την εντολή: `mysql --version`

Παράμετρος	Σχόλια και συνιστώμενες τιμές	έκδοση MySQL
`max_allowed_packet=33M`		Όλες οι υποστηριζόμενες εκδόσεις.
`log_bin_trust_function_creators=1`	Εναλλακτικά, μπορείτε να απενεργοποιήσετε τη δυαδική καταγραφή: `log_bin=0`	8.x
`innodb_log_file_size=100M` `innodb_log_files_in_group=2`	Ο πολλαπλασιασμός των τιμών αυτών των δύο παραμέτρων πρέπει να είναι τουλάχιστον **200**. Η ελάχιστη τιμή για την παράμετρο `innodb_log_files_in_group` είναι **2** και η μέγιστη τιμή είναι **100** - η τιμή πρέπει να είναι ακέραιος αριθμός).	8.x 5.7 5.6.22 (και νεότερες εκδόσεις 5.6.x)
`innodb_log_file_size=200M`	Ρυθμίστε την τιμή τουλάχιστον σε **200M**, αλλά όχι μεγαλύτερη από **3000M**.	5.6.20 και 5.6.21

3. Πατήστε **CTRL + X** και πληκτρολογήστε **Y** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το αρχείο.

4. Επανεκκινήστε τον διακομιστή MySQL και εφαρμόστε τη ρύθμιση παραμέτρων (σε ορισμένες περιπτώσεις, το όνομα της υπηρεσίας είναι `mysqld`):

```
sudo systemctl restart mysql
```

5. Ρυθμίστε τα δικαιώματα και τον κωδικό πρόσβασης του MySQL (αυτό το βήμα είναι προαιρετικό και ενδέχεται να μην λειτουργήσει σε κάποιες διανομές Linux):

a)Αποκαλύψτε τον προσωρινό κωδικό πρόσβασης MySQL: `sudo grep 'temporary password' /var/log/mysql/mysqld.log`

b)Αντιγράψτε και αποθηκεύστε τον κωδικό πρόσβασης.

c)Ρυθμίστε έναν νέο κωδικό πρόσβασης ακολουθώντας μία από τις παρακάτω επιλογές:

• Εκτελέστε την εντολή `/usr/bin/mysql_secure_installation` και πληκτρολογήστε τον προσωρινό κωδικό πρόσβασης. Στη συνέχεια, θα σας ζητηθεί να δημιουργήσετε έναν νέο κωδικό πρόσβασης.

• Εκτελέστε την εντολή `mysql -u root -p` και πληκτρολογήστε τον προσωρινό κωδικό πρόσβασης. Εκτελέστε την εντολή `ALTER USER 'root'@'localhost' IDENTIFIED BY 'strong_new_password';` για να αλλάξετε τον ριζικό κωδικό πρόσβασης (αντικαταστήστε το `strong_new_password` με τον κωδικό πρόσβασής σας) και πληκτρολογήστε `Quit`.

Ανατρέξτε επίσης στο θέμα Βελτίωση ασφάλειας της εγκατάστασης του MySQL στο Εγχειρίδιο αναφοράς MySQL.

6. Βεβαιωθείτε ότι εκτελείται η υπηρεσία του διακομιστή MySQL:

```
sudo systemctl status mysql
```

Εγκατάσταση και διαμόρφωση ODBC

Βεβαιωθείτε ότι έχετε εγκαταστήσει μια υποστηριζόμενη έκδοση του διακομιστή MySQL και της σύνδεσης ODBC.

Μπορείτε να εγκαταστήσετε το πρόγραμμα οδήγησης Microsoft ODBC (έκδοση 13 και νεότερες εκδόσεις) για να συνδέσετε το διακομιστή ESET PROTECT σε Linux με το Microsoft SQL Server σε Windows. Για περισσότερες πληροφορίες, επισκεφτείτε αυτό το άρθρο της Γνωσιακής βάσης.

Εγκαταστήστε το πρόγραμμα οδήγησης ODBC του MySQL χρησιμοποιώντας το τερματικό. Ακολουθήστε τα βήματα για τη διανομή Linux:

- Debian, Ubuntu
- CentOS 7
- Άλλες υποστηριζόμενες διανομές Linux

Debian, Ubuntu

1. Εγκαταστήστε τα προγράμματα οδήγησης unixODBC:

```
sudo apt-get install unixodbc
```

2. Λήψη της σύνδεσης ODBC:

Ubuntu 16	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz`
Ubuntu 18	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz`
Ubuntu 20	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz`
Debian 10	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-debian10-x86-64bit.tar.gz`

- Βεβαιωθείτε ότι έχετε επιλέξει και λάβει την έκδοση που είναι συμβατή με τη διανομή και την έκδοση Linux που διαθέτετε.
- Μπορείτε να πραγματοποιήσετε λήψη της σύνδεσης ODBC για το MySQL από τον επίσημο ιστότοπο του MySQL.

3. Αποσυμπιέστε την αρχειοθήκη του προγράμματος οδήγησης ODBC (το όνομα του πακέτου αλλάζει ανάλογα με τον σύνδεσμο που χρησιμοποιείται):

```
gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz
```

4. Πραγματοποιήστε εξαγωγή του προγράμματος οδήγησης ODBC (το όνομα του πακέτου αλλάζει ανάλογα με τον σύνδεσμο που χρησιμοποιείται):

```
tar xvf mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar
```

5. Μεταβείτε στον φάκελο του προγράμματος οδήγησης ODBC (το όνομα του πακέτου αλλάζει ανάλογα με τον σύνδεσμο που χρησιμοποιείται):

```
cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit
```

6. Αντιγράψτε τα αρχεία του προγράμματος οδήγησης ODBC:

```
sudo cp bin/* /usr/local/bin
sudo cp lib/* /usr/local/lib
```

7. Εγγράψτε το πρόγραμμα οδήγησης για το ODBC.

- Για νέες εκδόσεις του Linux όπως το Ubuntu 20.x, συνιστάται να χρησιμοποιήσετε το πρόγραμμα οδήγησης Unicode, βήμα α).

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t
"Driver=/usr/local/lib/libmyodbc8w.so"
```

- Για άλλα συστήματα ή όταν το πρόγραμμα οδήγησης Unicode δεν λειτουργεί, χρησιμοποιήστε αυτή την εντολή:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t
"Driver=/usr/local/lib/libmyodbc8a.so"
```

8. Λίστα εγκατεστημένων προγραμμάτων οδήγησης:

```
sudo myodbc-installer -d -l
```

Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα: https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html.

CentOS 7

1. Εγκαταστήστε τα προγράμματα οδήγησης unixODBC:

```
sudo yum install unixODBC -y
```

2. Λήψη της σύνδεσης ODBC:

```
wget
https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-1.el7.x86_64.rpm
```

- Μην εγκαταστήσετε τη σύνδεση ODBC χρησιμοποιώντας YUM – θα εγκαταστήσει την πιο πρόσφατη, μη συμβατή έκδοση.
- Βεβαιωθείτε ότι έχετε επιλέξει και λάβει την έκδοση που είναι συμβατή με τη διανομή και την έκδοση Linux που διαθέτετε.
- Μπορείτε να πραγματοποιήσετε λήψη της σύνδεσης ODBC για το MySQL από τον επίσημο ιστότοπο του MySQL.

3. Εγκατάσταση του διακομιστή ODBC:

```
sudo rpm -ivh mysql-connector-odbc-8.0.17-1.e17.x86_64.rpm --nodeps
```

4. Ρυθμίστε το πρόγραμμα οδήγησης ODBC:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0.17" -t
"Driver=/usr/lib64/libmyodbc8w.so"
```

5. Λίστα εγκατεστημένων προγραμμάτων οδήγησης:

```
sudo myodbc-installer -d -l
```

Άλλες υποστηριζόμενες διανομές Linux

⚠ • Βεβαιωθείτε ότι έχετε επιλέξει και λάβει την έκδοση που είναι συμβατή με τη διανομή και την έκδοση Linux που διαθέτετε.
• Μπορείτε να πραγματοποιήσετε λήψη της σύνδεσης ODBC για το MySQL από τον επίσημο ιστότοπο του MySQL.

1. Ακολουθήστε αυτές τις οδηγίες για να εγκαταστήσετε το πρόγραμμα οδήγησης ODBC:

• **SUSE Linux Enterprise Server**: `sudo zypper install unixODBC`. Ανατρέξτε επίσης στη διεύθυνση https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-rpm.html

• Εγκατάσταση σύνδεσης/ODBC από δυαδική διανομή Tarball

2. Εκτελέστε την ακόλουθη εντολή για να ανοίξετε το αρχείο *odbcinst.ini* σε πρόγραμμα επεξεργασίας κειμένου:

```
sudo nano /etc/odbcinst.ini
```

ή `sudo nano/etc/unixODBC/odbcinst.ini`

3. Αντιγράψτε την ακόλουθη διαμόρφωση στο αρχείο *odbcinst.ini* (βεβαιωθείτε ότι οι διαδρομές για το **Driver** οδήγησης και τις **Setup** είναι σωστές) και κατόπιν αποθηκεύστε και κλείστε το αρχείο:

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

Το Πρόγραμμα οδήγησης μπορεί να βρίσκεται σε διαφορετική θέση για κάποιες διανομές. Μπορείτε να βρείτε το αρχείο χρησιμοποιώντας την παρακάτω εντολή:

```
sudo find /usr -iname "*libmyodbc*"
```

4. Ενημερώστε τα αρχεία διαμόρφωσης που ελέγχουν την πρόσβαση ODBC στους διακομιστές βάσεων δεδομένων στον τρέχοντα κεντρικό υπολογιστή εκτελώντας την παρακάτω εντολή:

```
sudo odbcinst -i -d -f /etc/odbcinst.ini
```

ή `sudo odbcinst -i -d -f /etc/unixODBC/odbcinst.ini`

Εγκατάσταση διακομιστή - Linux

Οδηγίες εγκατάστασης για επιλεγμένες διανομές Linux
Μπορείτε να ακολουθήσετε τα άρθρα της Γνωσιακής βάσης με οδηγίες ειδικά για τη διανομή:
- CentOS 7
- Debian 10
- SUSE Linux Enterprise Server (SLES)

Εγκατάσταση

Ακολουθήστε τα παρακάτω βήματα για να εγκαταστήσετε το στοιχείο διακομιστή ESET PROTECT σε Linux χρησιμοποιώντας μια εντολή τερματικού:

Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης.

1. Πραγματοποιήστε λήψη του στοιχείου διακομιστή ESET PROTECT:

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server
-linux-x86_64.sh
```

2. Καταστήστε το αρχείο λήψης εκτελέσιμο:

```
chmod +x server-linux-x86_64.sh
```

3. Μπορείτε να προετοιμάσετε μια δέσμη ενεργειών εγκατάστασης και, στη συνέχεια, να την εκτελέσετε χρησιμοποιώντας το `sudo`.

Εκτελέστε τη δέσμη ενεργειών εγκατάστασης στο παρακάτω παράδειγμα (Οι νέες γραμμές διαχωρίζονται με «\» για αντιγραφή ολόκληρης της εντολής στο τερματικό):

```
sudo ./server-linux-x86_64.sh \
--skip-license \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-hostname=localhost \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=password \
--server-root-password=password \
--db-user-username=root \
--db-user-password=password \
--cert-hostname="hostname, IP, FQDN"
```

Μπορείτε να τροποποιήσετε τα ακόλουθα χαρακτηριστικά:

Χαρακτηριστικό	Περιγραφή	Απαιτείται
`--uninstall`	Καταργεί την εγκατάσταση του προϊόντος.	-

Χαρακτηριστικό	Περιγραφή	Απαιτείται
`--keep-database`	Η βάση δεδομένων δεν θα καταργηθεί κατά την κατάργηση της εγκατάστασης.	-
`--locale`	Το αναγνωριστικό τοποθεσίας (LCID) του εγκατεστημένου διακομιστή (η προεπιλεγμένη τιμή είναι `en_US`). Δείτε τις υποστηριζόμενες γλώσσες για διαθέσιμες επιλογές. Εάν δεν καθορίσετε τις ρυθμίσεις `--locale`, ο Διακομιστής ESET PROTECT θα εγκατασταθεί στην Αγγλική γλώσσα. ESET PROTECT On-Prem Μπορείτε να ρυθμίσετε μια γλώσσα για κάθε περίοδο λειτουργίας της κονσόλας διαδικτύου ESET PROTECT. Δεν θα αλλάξουν όλα τα στοιχεία της Κονσόλας διαδικτύου μετά την αλλαγή γλώσσας. Ορισμένα από τα στοιχεία (προεπιλεγμένοι πίνακες ελέγχου, πολιτικές, εργασίες κ.λπ.) δημιουργούνται κατά την εγκατάσταση του ESET PROTECT On-Prem και η γλώσσα τους δεν μπορεί να αλλάξει.	Ναι
`--skip-license`	Η εγκατάσταση δεν θα ζητήσει από το χρήστη επιβεβαίωση της συμφωνίας άδειας χρήσης.	-
`--skip-cert`	Παραλείψτε τη δημιουργία πιστοποιητικών (χρησιμοποιήστε την παράμετρο `--server-cert-path`).	-
`--license-key`	Κλειδί άδειας χρήσης ESET. Μπορείτε να παράσχετε το κλειδί άδειας χρήσης αργότερα.	-
`--server-port`	Θύρα διακομιστή ESET PROTECT (η προεπιλεγμένη τιμή είναι `2222`).	-
`--console-port`	Θύρα της Κονσόλας διαδικτύουESET PROTECT (η προεπιλεγμένη τιμή είναι `2223`)	-
`--server-root-password`	Κωδικός πρόσβασης για σύνδεση του χρήστη «Διαχειριστής» στην κονσόλα διαδικτύου. Το μήκος του πρέπει να είναι τουλάχιστον 8 χαρακτήρες.	Ναι
`--db-type`	Ο τύπος βάσης δεδομένων που θα χρησιμοποιηθεί (πιθανές τιμές: `"MySQL Server"`, `"MS SQL Server"`). Το Microsoft SQL Server σε Linux δεν υποστηρίζεται. Ωστόσο, μπορείτε να συνδέσετε το διακομιστή ESET PROTECT σε Linux με το Microsoft SQL Server σε Windows.	-
`--db-driver`	Πρόγραμμα οδήγησης ODBC που θα χρησιμοποιηθεί για τη σύνδεση με τη βάση δεδομένων (η εντολή `odbcinst -q -d` παρέχει μια λίστα διαθέσιμων προγραμμάτων οδήγησης. Χρησιμοποιήστε ένα από αυτά τα προγράμματα οδήγησης, για παράδειγμα: `--db-driver="MySQL ODBC 8.0 Driver"`, `--db-driver="MySQL ODBC 8.0 Unicode Driver"` ή το `--db-driver="MySQL ODBC 8.0.17"`).	Ναι
`--db-hostname`	Όνομα υπολογιστή ή διεύθυνση IP του διακομιστή βάσης δεδομένων. Η κατονομαζόμενη εμφάνιση βάσης δεδομένων δεν υποστηρίζεται.	Ναι

Χαρακτηριστικό	Περιγραφή	Απαιτείται
`--db-port`	Θύρα του διακομιστή βάσης δεδομένων (η προεπιλεγμένη τιμή είναι `3306`).	Ναι
`--db-name`	Όνομα της βάσης δεδομένων διακομιστή ESET PROTECT (η προεπιλεγμένη τιμή είναι `era_db`).	-
`--db-admin-username`	Όνομα χρήστη διαχειριστή βάσης δεδομένων (χρησιμοποιείται από την εγκατάσταση για τη δημιουργία και τροποποίηση της βάσης δεδομένων). Μπορείτε να παραλείψετε αυτή την παράμετρο, εάν έχει προηγουμένως δημιουργηθεί χρήστης της βάσης δεδομένων που καθορίζεται στις παραμέτρους `--db-user-username` και `--db-user-password`	Ναι
`--db-admin-password`	Κωδικός πρόσβασης διαχειριστή βάσης δεδομένων. Μπορείτε να παραλείψετε αυτή την παράμετρο εάν έχει προηγουμένως δημιουργηθεί χρήστης της βάσης δεδομένων που καθορίζεται από τις παραμέτρους `--db-user-username` και `--db-user-password`	Ναι
`--db-user-username`	Όνομα χρήστη του χρήστη της βάσης δεδομένων του διακομιστή ESET PROTECT (χρησιμοποιείται από το διακομιστή ESET PROTECT για τη σύνδεση στη βάση δεδομένων). Το μήκος δεν πρέπει να υπερβαίνει τους 16 χαρακτήρες.	Ναι
`--db-user-password`	Κωδικός πρόσβασης χρήστη της βάσης δεδομένων του διακομιστή ESET PROTECT	Ναι
`--cert-hostname`	Περιέχει όλα τα πιθανά ονόματα ή/και τη διεύθυνση IP του υπολογιστή στον οποίο είναι εγκατεστημένος ο διακομιστής ESET PROTECT. Η τιμή πρέπει να αντιστοιχεί στο όνομα διακομιστή που καθορίζεται στο πιστοποιητικό φορέα που προσπαθεί να συνδεθεί με τον διακομιστή.	Ναι
`--server-cert-path`	Διαδρομή προς το ομότιμο πιστοποιητικό (χρησιμοποιήστε αυτή την επιλογή εάν καθορίσατε και `--skip-cert`)	-
`--server-cert-password`	Κωδικός πρόσβασης του ομότιμου πιστοποιητικού διακομιστή	-
`--agent-cert-password`	Κωδικός πρόσβασης του ομότιμου πιστοποιητικού φορέα	-
`--cert-auth-password`	Κωδικός πρόσβασης αρχής έκδοσης πιστοποιητικού	-
`--cert-auth-path`	Διαδρομή προς το αρχείο αρχής έκδοσης πιστοποιητικού του διακομιστή	-
`--cert-auth-common-name`	Κοινό όνομα αρχής έκδοσης πιστοποιητικού (χρησιμοποιήστε `""`)	-
`--cert-organizational-unit`	-	-
`--cert-organization`	-	-
`--cert-locality`	-	-
`--cert-state`	-	-
`--cert-country`	-	-

Χαρακτηριστικό	Περιγραφή	Απαιτείται
`--cert-validity`	Εγκυρότητα πιστοποιητικού σε ημέρες ή έτη (καθορίστε την στο όρισμα `--cert-validity-unit`)	-
`--cert-validity-unit`	Μονάδα για την εγκυρότητα του πιστοποιητικού. Οι πιθανές τιμές είναι «Έτη» ή «Ημέρες» (η προεπιλεγμένη τιμή είναι `Years`)	-
`--ad-server`	Διακομιστής Active Directory	-
`--ad-user-name`	Όνομα του χρήστη που έχει δικαιώματα αναζήτησης στο δίκτυο AD	-
`--ad-user-password`	Κωδικός πρόσβασης χρήστη του Active Directory	-
`--ad-cdn-include`	Διαδρομή δέντρου του Active Directory, για την οποία θα γίνει συγχρονισμός. Χρησιμοποιήστε κενά εισαγωγικά "" για συγχρονισμό ολόκληρου του δέντρου	-
`--enable-imp-program`	Ενεργοποιήστε το Πρόγραμμα βελτίωσης προϊόντος.	-
`--disable-imp-program`	Απενεργοποιήστε το Πρόγραμμα βελτίωσης προϊόντος.	-

Συνιστάται να καταργήσετε εντολές που περιέχουν ευαίσθητα δεδομένα (για παράδειγμα, έναν κωδικό πρόσβασης) από το ιστορικό της γραμμής εντολών:
1.Εκτελέστε το στοιχείο `history` για να δείτε τη λίστα όλων των εντολών στο ιστορικό.
2.Εκτελέστε το στοιχείο `history -d line_number` (καθορίστε τον αριθμό γραμμής της εντολής). Εναλλακτικά, εκτελέστε το στοιχείο `history -c` για να καταργήσετε ολόκληρο το ιστορικό της γραμμής εντολών.

4. Η εγκατάσταση θα σας ρωτήσει εάν θέλετε να συμμετάσχετε στο Πρόγραμμα βελτίωσης προϊόντος. Πατήστε **N** εάν συμφωνείτε να αποστέλλονται αναφορές διακοπής λειτουργίας και δεδομένα τηλεμετρίας στην ESET ή πατήστε **O** για να μην αποστέλλονται καθόλου δεδομένα.

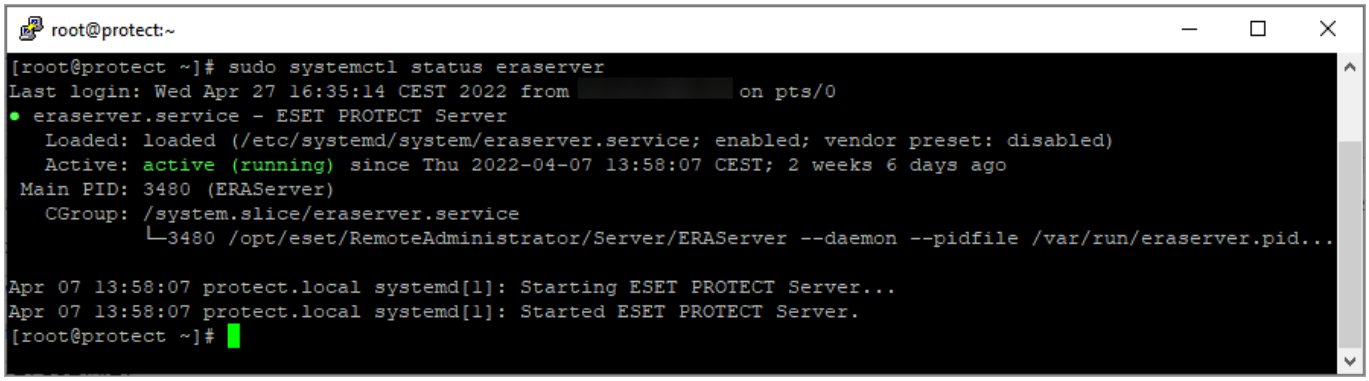
5. Ο διακομιστής ESET PROTECT και η υπηρεσία `eraserver` θα εγκατασταθούν στην παρακάτω τοποθεσία:

/opt/eset/RemoteAdministrator/Server

Η εγκατάσταση ενδέχεται να τερματιστεί με την ένδειξη **SELinux policy... failure**. Μπορείτε να αγνοήσετε την ένδειξη εάν δεν χρησιμοποιείτε το SELinux.

6. Μετά την εγκατάσταση, βεβαιωθείτε ότι εκτελείται η υπηρεσία διακομιστή ESET PROTECT χρησιμοποιώντας την εντολή που εμφανίζεται παρακάτω:

```
sudo systemctl status eraserver
```



Αρχείο καταγραφής προγράμματος εγκατάστασης

Το αρχείο καταγραφής του προγράμματος εγκατάστασης μπορεί να είναι χρήσιμο για την αντιμετώπιση προβλημάτων και μπορείτε να το βρείτε στα Αρχεία καταγραφής.

Προαπαιτούμενα διακομιστή - Linux

Βεβαιωθείτε ότι πληρούνται τα ακόλουθα προαπαιτούμενα για την εγκατάσταση του διακομιστή ESET PROTECT σε Linux:

- Πρέπει να υπάρχει έγκυρη άδεια χρήσης.
- Πρέπει να υπάρχει ένα υποστηριζόμενο λειτουργικό σύστημα Linux.
- Οι απαιτούμενες θύρες πρέπει να είναι ανοιχτές και διαθέσιμες – δείτε την πλήρη λίστα των θυρών εδώ.
- Πρέπει να είναι εγκατεστημένος ένας διακομιστής βάσης δεδομένων και να έχει διαμορφωθεί με ριζικό λογαριασμό. Δεν χρειάζεται να δημιουργηθεί λογαριασμός χρήστη πριν την εγκατάσταση. Το πρόγραμμα εγκατάστασης μπορεί να δημιουργήσει το λογαριασμό. Το Microsoft SQL Server σε Linux δεν υποστηρίζεται. Ωστόσο, μπορείτε να συνδέσετε το διακομιστή ESET PROTECT σε Linux με το Microsoft SQL Server σε Windows.

> Ο διακομιστής ESET PROTECT αποθηκεύει μεγάλα μπλοκ δεδομένων στη βάση δεδομένων. Ρύθμιση παραμέτρων του MySQL για να αποδέχεται μεγάλο μέγεθος πακέτου ώστε να εκτελείται σωστά το ESET PROTECT On-Prem.

- **Πρόγραμμα οδήγησης ODBC** - Το πρόγραμμα οδήγησης ODBC χρησιμοποιείται για τη δημιουργία σύνδεσης με το διακομιστή βάσης δεδομένων (MySQL).
- Ρυθμίστε το αρχείο εγκατάστασης διακομιστή ως εκτελέσιμο χρησιμοποιώντας την εντολή τερματικού:

```
chmod +x server-linux-x86_64.sh
```

- Συνιστάται να **χρησιμοποιήσετε την πιο πρόσφατη έκδοση του OpenSSL1.1.1**. Ο φορέας ESET Management υποστηρίζει επίσης OpenSSL 3.x. Η ελάχιστη υποστηριζόμενη έκδοση του OpenSSL για Linux είναι openssl-1.0.1e-30. Σε ένα σύστημα, μπορεί να είναι ταυτόχρονα εγκατεστημένες περισσότερες εκδόσεις του OpenSSL. Στο σύστημά σας πρέπει να υπάρχει τουλάχιστον μία υποστηριζόμενη έκδοση.

oΧρησιμοποιήστε την εντολή `openssl version` για να εμφανιστεί η τρέχουσα προεπιλεγμένη έκδοση.

oΜπορείτε να δείτε σε λίστα όλες τις εκδόσεις του OpenSSL που υπάρχουν στο σύστημά σας. Δείτε τις καταλήξεις των ονομάτων αρχείων που αναγράφονται στη λίστα χρησιμοποιώντας την εντολή `sudo find / -iname *libcrypto.so*`

oΜπορείτε να ελέγξετε εάν ο υπολογιστής-πελάτης Linux είναι συμβατός χρησιμοποιώντας την ακόλουθη εντολή: `openssl s_client -connect google.com:443 -tls1_2`

OpenSSL 3.x υποστήριξη

- Ο Φορέας ESET Management υποστηρίζει OpenSSL 3.x.
- Ο διακομιστής/η διαχείριση κινητών συσκευών ESET PROTECT δεν υποστηρίζει τοπικά το OpenSSL 3.x, αλλά μπορείτε να ενεργοποιήσετε την υποστήριξη OpenSSL 3.x για το ESET PROTECT On-Prem.

- **Xvfb** - Απαιτείται για σωστή εκτύπωση αναφορών (Δημιουργία αναφοράς) σε συστήματα διακομιστή Linux χωρίς γραφικό περιβάλλον χρήστη.

- **Xauth** - Το πακέτο εγκαθίσταται μαζί με το **xvfb**. Πρέπει να εγκαταστήσετε το **xauth** εάν δεν εγκαταστήσετε το **xvfb**.

- **cifs-utils** - Απαιτείται για σωστή ανάπτυξη του φορέα σε λειτουργικό σύστημα Windows.

- **Βιβλιοθήκες Qt4 WebKit** - Χρησιμοποιείται για την εκτύπωση αναφορών σε μορφή PDF και PS (πρέπει να είναι έκδοση 4.8, όχι 5). Όλες οι άλλες εξαρτήσεις του Qt4 θα εγκατασταθούν αυτόματα. Εάν το πακέτο δεν είναι διαθέσιμο στο αποθετήριο του λειτουργικού συστήματός σας, μπορείτε να το μεταγλωττίσετε μόνοι σας σε έναν υπολογιστή προορισμού ή να το εγκαταστήσετε από αποθετήριο άλλου κατασκευαστή (για παράδειγμα, τα αποθετήρια EPEL): Οδηγίες CentOS 7, οδηγίες Ubuntu 20.04.

- **kinit + klist** – Το Kerberos χρησιμοποιείται για έλεγχο ταυτότητας ενός χρήστη τομέα κατά τη σύνδεση και την εργασία συγχρονισμού του Active Directory. Βεβαιωθείτε ότι έχετε ρυθμίσει σωστά τις παραμέτρους του Kerberos (*/etc/krb5.conf*). Το ESET PROTECT On-Prem υποστηρίζει συγχρονισμό με πολλαπλούς τομείς.

- **ldapsearch** - Χρησιμοποιείται στην εργασία συγχρονισμού AD και για σκοπούς εξουσιοδότησης.

- **snmptrap** – Προαιρετικά, χρησιμοποιείται για την αποστολή παγιδεύσεων SNMP. Επίσης, το SNMP απαιτεί διαμόρφωση.

- **Πακέτο SELinux devel** - Χρησιμοποιείται κατά την εγκατάσταση προϊόντων για τη δημιουργία μονάδων πολιτικής SELinux. Αυτό απαιτείται μόνο σε συστήματα με ενεργοποίηση του SELinux (CentOS, RHEL). Το SELinux μπορεί να προκαλέσει προβλήματα με άλλες εφαρμογές. Δεν απαιτείται για το διακομιστή ESET PROTECT.

- **lshw** - Εγκαταστήστε το πακέτο `lshw` στον υπολογιστή-πελάτη/διακομιστή Linux ώστε ο Φορέας ESET Management να αναφέρει σωστά το απόθεμα υλικού.

Ο παρακάτω πίνακας περιέχει τις κατάλληλες εντολές τερματικού για κάθε πακέτο που περιγράφεται παραπάνω για διάφορες διανομές Linux (εκτελέστε τις εντολές ως `sudo` ή `root`):

Πακέτο	Διανομές Debian και Ubuntu	Διανομές CentOS και Red Hat
Πρόγραμμα οδήγησης ODBC	Δείτε το θέμα Εγκατάσταση και ρύθμιση παραμέτρων ODBC.	Δείτε το θέμα Εγκατάσταση και ρύθμιση παραμέτρων ODBC.
OpenSSL	`apt-get install openssl`	`yum install openssl -y`
xvfb	`apt-get install xvfb`	`yum install xorg-x11-server-Xvfb -y`
cifs-utils	`apt-get install cifs-utils`	`yum install cifs-utils`

Qt4 WebKit libraries	`apt-get install libqtwebkit4`
	Δείτε τις οδηγίες για Ubuntu 20.04.
		Το Qt4 WebKit δεν είναι το τυπικό αποθετήριο του CentOS. Εγκαταστήστε αυτά τα πακέτα:
		`yum install -y epel-release`
		`yum install qtwebkit-devel`
		Εναλλακτικά, μπορείτε να εγκαταστήσετε το πακέτο από τα αποθετήρια Fedora.

kinit + klist - προαιρετικά (απαιτείται για την υπηρεσία Active Directory)	`apt-get install krb5-user`	`yum install krb5-workstation`
ldapsearch	`apt-get install ldap-utils libsasl2-modules-gssapi-mit`	`yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap -y`
snmptrap	`apt-get install snmp`	`yum install net-snmp-utils net-snmp`
Πακέτο ανάπτυξης SELinux (προαιρετικό - δεν απαιτείται για το διακομιστή ESET PROTECT. Το SELinux μπορεί να προκαλέσει προβλήματα με άλλες εφαρμογές.)	`apt-get install selinux-policy-dev`	`yum install policycoreutils-devel`
samba (προαιρετικό, απαραίτητο μόνο για απομακρυσμένη ανάπτυξη)	`apt-get install samba`	`yum install samba samba-winbind-clients`
lshw	`apt-get install -y lshw`	`yum install -y lshw`

Εγκατάσταση φορέα - Linux

Προαπαιτούμενα

- Συνιστάται να **χρησιμοποιήσετε την πιο πρόσφατη έκδοση του OpenSSL1.1.1**. Ο φορέας ESET Management υποστηρίζει επίσης OpenSSL 3.x. Η ελάχιστη υποστηριζόμενη έκδοση του OpenSSL για Linux είναι openssl-1.0.1e-30. Σε ένα σύστημα, μπορεί να είναι ταυτόχρονα εγκατεστημένες περισσότερες εκδόσεις του OpenSSL. Στο σύστημά σας πρέπει να υπάρχει τουλάχιστον μία υποστηριζόμενη έκδοση.

  - Χρησιμοποιήστε την εντολή `openssl version` για να εμφανιστεί η τρέχουσα προεπιλεγμένη έκδοση.

  - Μπορείτε να δείτε σε λίστα όλες τις εκδόσεις του OpenSSL που υπάρχουν στο σύστημά σας. Δείτε τις καταλήξεις των ονομάτων αρχείων που αναγράφονται στη λίστα χρησιμοποιώντας την εντολή `sudo find / -iname *libcrypto.so*`

  - Μπορείτε να ελέγξετε εάν ο υπολογιστής-πελάτης Linux είναι συμβατός χρησιμοποιώντας την ακόλουθη εντολή: `openssl s_client -connect google.com:443 -tls1_2`

> **OpenSSL 3.x υποστήριξη**
> - Ο Φορέας ESET Management υποστηρίζει OpenSSL 3.x.
> - Ο διακομιστής/η διαχείριση κινητών συσκευών ESET PROTECT δεν υποστηρίζει τοπικά το OpenSSL 3.x, αλλά μπορείτε να ενεργοποιήσετε την υποστήριξη OpenSSL 3.x για το ESET PROTECT On-Prem.

- Εγκαταστήστε το πακέτο `lshw` στον υπολογιστή-πελάτη/διακομιστή Linux ώστε ο Φορέας ESET

Management να αναφέρει σωστά το απόθεμα υλικού.

Διανομή Linux	Εντολή τερματικού
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`
OpenSUSE	`sudo zypper install lshw`

- Για το Linux CentOS, συνιστάται η εγκατάσταση του πακέτου `policycoreutils-devel`. Εκτελέστε την εντολή για να εγκαταστήστε το πακέτο:

```
yum install policycoreutils-devel
```

- Εγκατάσταση φορέα με υποβοήθηση διακομιστή:

  oΟ υπολογιστής διακομιστή πρέπει να είναι προσπελάσιμος από το δίκτυο και να έχει εγκατεστημένο το διακομιστή ESET PROTECT και την Κονσόλα διαδικτύου ESET PROTECT

- Εγκατάσταση φορέα χωρίς σύνδεση:

  oΟ υπολογιστής διακομιστή πρέπει να είναι προσπελάσιμος από το δίκτυο και να έχει εγκατεστημένο το διακομιστή ESET PROTECT.

  oΠρέπει να υπάρχει πιστοποιητικό για τον φορέα.

  oΠρέπει να υπάρχει αρχείο δημόσιου κλειδιού διακομιστή από την αρχή έκδοσης πιστοποιητικών.

Εγκατάσταση

Ακολουθήστε τα παρακάτω βήματα για να εγκαταστήσετε το στοιχείο του φορέα ESET Management σε Linux χρησιμοποιώντας μια εντολή τερματικού:

Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης που αναφέρονται παραπάνω.

1. Πραγματοποιήστε λήψη της δέσμης ενεργειών εγκατάστασης φορέα:

```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent-linux-x86_64.sh
```

2. Καταστήστε το αρχείο εκτελέσιμο:

```
chmod +x agent-linux-x86_64.sh
```

3. Εκτελέστε τη δέσμη ενεργειών εγκατάστασης στο παρακάτω παράδειγμα (Οι νέες γραμμές διαχωρίζονται με «\» για αντιγραφή ολόκληρης της εντολής στο τερματικό):

Για περισσότερες λεπτομέρειες ανατρέξτε στην παρακάτω ενότητα Παράμετροι.

Εγκατάσταση με υποβοήθηση διακομιστή:

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.0.1 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

Εγκατάσταση χωρίς σύνδεση:

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222
```

Συνιστάται να καταργήσετε εντολές που περιέχουν ευαίσθητα δεδομένα (για παράδειγμα, έναν κωδικό πρόσβασης) από το ιστορικό της γραμμής εντολών:
1.Εκτελέστε το στοιχείο `history` για να δείτε τη λίστα όλων των εντολών στο ιστορικό.
2.Εκτελέστε το στοιχείο `history -d line_number` (καθορίστε τον αριθμό γραμμής της εντολής). Εναλλακτικά, εκτελέστε το στοιχείο `history -c` για να καταργήσετε ολόκληρο το ιστορικό της γραμμής εντολών.

4. Όταν σας ζητηθεί, πατήστε το πλήκτρο **y** για να αποδεχτείτε το πιστοποιητικό. Μπορείτε να αγνοήσετε τυχόν σφάλματα σχετικά με την ένδειξη SELinux που επιστρέφει το πρόγραμμα εγκατάστασης.

5. Μετά την εγκατάσταση, βεβαιωθείτε ότι εκτελείται η υπηρεσία φορέα ESET Management:

```
sudo systemctl status eraagent
```

6. Ρυθμίστε την υπηρεσία **eraagent** για να ξεκινά κατά την εκκίνηση: `sudo systemctl enable eraagent`

Αρχείο καταγραφής προγράμματος εγκατάστασης

Το αρχείο καταγραφής του προγράμματος εγκατάστασης μπορεί να είναι χρήσιμο για την αντιμετώπιση προβλημάτων. Μπορείτε να το βρείτε στα αρχεία καταγραφής.

Παράμετροι

Η σύνδεση με το διακομιστή ESET PROTECT επιλύεται χρησιμοποιώντας τις παραμέτρους --hostname και --port (η θύρα δεν χρησιμοποιείται όταν παρέχεται μια εγγραφή SRV). Πιθανές μορφές σύνδεσης.

• **Όνομα κεντρικού υπολογιστή** και **θύρα**
• **Διεύθυνση IPv4** και **θύρα**
• **Διεύθυνση IPv6** και **θύρα**
• Εγγραφή υπηρεσίας (εγγραφή SRV) - Για να διαμορφωθεί η εγγραφή πόρου DNS στο Linux, ο υπολογιστής πρέπει να βρίσκεται σε έναν τομέα με διακομιστή DNS σε λειτουργία. Δείτε την ενότητα Εγγραφή πόρου DNS. Η εγγραφή SRV πρέπει να αρχίζει με το πρόθεμα "_NAME._tcp" όπου το 'NAME' αντιπροσωπεύει το προσαρμοσμένο όνομα (για παράδειγμα, "era").

Χαρακτηριστικό	Περιγραφή	Απαιτείται
`--hostname`	Όνομα κεντρικού υπολογιστή ή διεύθυνση IP του διακομιστή ESET PROTECT για σύνδεση.	Ναι
`--port`	Θύρα διακομιστή ESET PROTECT (η προεπιλεγμένη τιμή είναι `2222`).	Ναι
`--cert-path`	Τοπική διαδρομή προς το αρχείο πιστοποιητικού φορέα (περισσότερα σχετικά με το πιστοποιητικό).	Ναι (χωρίς σύνδεση)
`--cert-auth-path`	Διαδρομή προς το αρχείο αρχής έκδοσης πιστοποιητικών του διακομιστή (περισσότερα σχετικά με την αρχή έκδοσης).	Ναι (χωρίς σύνδεση)
`--cert-password`	Κωδικός πρόσβασης πιστοποιητικού φορέα.	Ναι (χωρίς σύνδεση)
`--cert-auth-password`	Κωδικός πρόσβασης αρχής έκδοσης πιστοποιητικού.	Ναι (εάν χρησιμοποιείται)
`--skip-license`	Η εγκατάσταση δεν θα ζητήσει από το χρήστη επιβεβαίωση της συμφωνίας άδειας χρήσης.	Όχι
`--cert-content`	Περιεχόμενο με κωδικοποίηση Base64 του πιστοποιητικού δημόσιου κλειδιού με κωδικοποίηση PKCS12 μαζί με το ιδιωτικό κλειδί που χρησιμοποιούνται για τη ρύθμιση των διαύλων ασφαλούς επικοινωνίας με το διακομιστή και τους φορείς. Χρησιμοποιήστε μόνο μία από τις επιλογές `--cert-path` ή `--cert-content`.	Όχι
`--cert-auth-content`	Περιεχόμενο με κωδικοποίηση Base64 του πιστοποιητικού ιδιωτικού κλειδιού αρχής έκδοσης πιστοποιητικού με κωδικοποίηση DER που χρησιμοποιείται για την επαλήθευση απομακρυσμένων ομότιμων (διακομιστής μεσολάβησης ή διακομιστής). Χρησιμοποιήστε μόνο μία από τις επιλογές `--cert-auth-path` ή `--cert-auth-content`.	Όχι
`--webconsole-hostname`	Όνομα κεντρικού υπολογιστή ή διεύθυνση IP που χρησιμοποιείται από την Κονσόλα διαδικτύου για σύνδεση με τον διακομιστή (εάν μείνει κενό, το πρόγραμμα εγκατάστασης θα αντιγράψει την τιμή από τον «κεντρικό υπολογιστή»).	Όχι
`--webconsole-port`	Θύρα που χρησιμοποιείται από την κονσόλα διαδικτύου για σύνδεση με το διακομιστή (η προεπιλεγμένη τιμή είναι `2223`).	Όχι
`--webconsole-user`	Όνομα χρήστη που χρησιμοποιείται από την κονσόλα διαδικτύου για σύνδεση με το διακομιστή (η προεπιλεγμένη τιμή είναι `Administrator`). Δεν μπορείτε να χρησιμοποιήσετε έναν χρήστη με έλεγχο ταυτότητας δύο παραγόντων για εγκαταστάσεις με υποβοήθηση του διακομιστή.	Όχι
`--webconsole-password`	Κωδικός πρόσβασης που χρησιμοποιείται από την Κονσόλα διαδικτύου για σύνδεση με το διακομιστή.	Ναι (με υποβοήθηση του διακομιστή)
`--proxy-hostname`	Όνομα κεντρικού υπολογιστή διακομιστή μεσολάβησης HTTP. Χρησιμοποιήστε αυτή την παράμετρο για να ενεργοποιήσετε τη χρήση του διακομιστή μεσολάβησης HTTP (ο οποίος είναι ήδη εγκατεστημένος στο δίκτυό σας) για αντιγραφή μεταξύ του Φορέα ESET Management και του Διακομιστή ESET PROTECT (όχι για προσωρινή αποθήκευση ενημερώσεων).	Εάν χρησιμοποιείται διακομιστής μεσολάβησης
`--proxy-port`	Θύρα διακομιστή μεσολάβησης HTTP για σύνδεση με το διακομιστή.	Εάν χρησιμοποιείται διακομιστής μεσολάβησης
`--enable-imp-program`	Ενεργοποιήστε το Πρόγραμμα βελτίωσης προϊόντος.	Όχι
`--disable-imp-program`	Απενεργοποιήστε το Πρόγραμμα βελτίωσης προϊόντος.	Όχι

Σύνδεση και πιστοποιητικά

• Πρέπει να δοθεί η **Σύνδεση με το διακομιστή ESET PROTECT**: `--hostname`, `--port` (η θύρα δεν απαιτείται, εάν παρέχεται η εγγραφή υπηρεσίας, η προεπιλεγμένη τιμή θύρας είναι `2222`)

• Δώστε αυτές τις πληροφορίες σύνδεσης για **Εγκατάσταση με υποβοήθηση διακομιστή**: `--webconsole-port, --webconsole-user, --webconsole-password`

• Δώστε πληροφορίες πιστοποιητικού για **Εγκατάσταση χωρίς σύνδεση**: `--cert-path`, `--cert-password`. Οι παράμετροι εγκατάστασης `--cert-path` και `--cert-auth-path` απαιτούν αρχεία πιστοποιητικών (*.pfx* και *.der*), τα οποία μπορείτε να εξαγάγετε από την Κονσόλα διαδικτύου ESET PROTECT. (Διαβάστε πώς μπορείτε να εξαγάγετε το αρχείο .pfx και το αρχείο.der.)

Παράμετροι τύπου κωδικού πρόσβασης

Οι παράμετροι τύπου κωδικού πρόσβασης μπορούν να δοθούν ως μεταβλητές περιβάλλοντος, αρχεία, ανάγνωση από το `stdin` ή ως απλό κείμενο. Δηλαδή:

`--password=env:SECRET_PASSWORD` όπου το `SECRET_PASSWORD` είναι μια μεταβλητή περιβάλλοντος με κωδικό πρόσβασης

`--password=file:/opt/secret` όπου η πρώτη γραμμή του κανονικού αρχείου `/opt/secret` περιέχει τον κωδικό πρόσβασής σας

`--password=stdin` δίνει οδηγίες στο πρόγραμμα εγκατάστασης να διαβάσει τον κωδικό πρόσβασης από τυπική είσοδο

Το `--password="pass:PASSWORD"` είναι ίσο με το `--password="PASSWORD"` και είναι υποχρεωτικό, εάν ο πραγματικός κωδικός πρόσβασης είναι `"stdin"` (τυπική είσοδος) ή μια συμβολοσειρά που αρχίζει με `"env:"`, `"file:"` ή `"pass:"`

Ο κωδικός πρόσβασης του πιστοποιητικού δεν πρέπει να περιέχει τους ακόλουθους χαρακτήρες: `"` `\` Αυτοί οι χαρακτήρες προκαλούν κρίσιμο σφάλμα κατά την αρχικοποίηση του φορέα.

Σύνδεση διακομιστή μεσολάβησης HTTP

Εάν χρησιμοποιείτε διακομιστή μεσολάβησης HTTP για αντιγραφή μεταξύ του Φορέα ESET Management και του Διακομιστή ESET PROTECT (όχι για προσωρινή αποθήκευση ενημερώσεων), μπορείτε να καθορίσετε τις παραμέτρους σύνδεσης στα στοιχεία `--proxy-hostname` και `--proxy-port`.

Παράδειγμα - εγκατάσταση φορέα με σύνδεση διακομιστή μεσολάβησης HTTP

```
./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222 \
--proxy-hostname=10.1.180.3 \
--proxy-port=3333 \
```

Το πρωτόκολλο επικοινωνίας μεταξύ του φορέα και του διακομιστή ESET PROTECT δεν υποστηρίζει τον έλεγχο ταυτότητας. Οποιαδήποτε λύση διακομιστή μεσολάβησης που χρησιμοποιείται για προώθηση της επικοινωνίας του φορέα στο διακομιστή ESET PROTECT και απαιτεί έλεγχο ταυτότητας δεν θα λειτουργεί.
Εάν επιλέξετε να χρησιμοποιήσετε μια μη προεπιλεγμένη θύρα για την Κονσόλα διαδικτύου ή το φορέα, ενδέχεται να απαιτείται προσαρμογή του τείχους προστασίας. Διαφορετικά, η εγκατάσταση μπορεί να αποτύχει.

Εγκατάσταση αναβάθμισης και επιδιόρθωσης του Φορέα σε Linux

Εάν εκτελείτε την εγκατάσταση φορέα μη αυτόματα σε ένα σύστημα που έχει ήδη εγκατασταθεί ο φορέας, μπορεί να προκύψουν τα ακόλουθα σενάρια:

- **Αναβάθμιση** - Εκτέλεση μιας νεότερης έκδοσης του προγράμματος εγκατάστασης.

  oΕγκατάσταση με υποβοήθηση διακομιστή - η εφαρμογή αναβαθμίζεται, αλλά θα εξακολουθεί να χρησιμοποιεί προηγούμενα πιστοποιητικά.

  oΕγκατάσταση εκτός σύνδεσης - η εφαρμογή αναβαθμίζεται, αλλά θα χρησιμοποιούνται νέα πιστοποιητικά.

- **Επιδιόρθωση** - Εκτέλεση της ίδιας έκδοσης του προγράμματος εγκατάστασης. Μπορείτε να χρησιμοποιήσετε αυτήν την επιλογή για να μετεγκαταστήσετε τον φορέα σε διαφορετικό διακομιστή ESET PROTECT.

  oΕγκατάσταση με υποβοήθηση διακομιστή - γίνεται επανεγκατάσταση της εφαρμογής και θα διαθέτει τα τρέχοντα πιστοποιητικά από το διακομιστή ESET PROTECT (ορίζονται από την παράμετρο `hostname`).

  oΕγκατάσταση εκτός σύνδεσης – γίνεται επανεγκατάσταση της εφαρμογής και χρησιμοποιούνται νέα πιστοποιητικά.

Εάν κάνετε μετεγκατάσταση φορέα από παλαιότερο διακομιστή σε διαφορετικό νεότερο διακομιστή ESET PROTECT μη αυτόματα, και χρησιμοποιείτε εγκατάσταση με υποβοήθηση διακομιστή, εκτελέστε την εντολή εγκατάστασης δύο φορές. Η πρώτη θα αναβαθμίσει τον φορέα και η δεύτερη θα λάβει τα νέα πιστοποιητικά, έτσι ώστε ο φορέας να μπορεί να συνδεθεί με τον διακομιστή ESET PROTECT.

Εγκατάσταση κονσόλας διαδικτύου - Linux

Ακολουθήστε αυτά τα βήματα για να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT:

Μπορείτε να εγκαταστήσετε την Κονσόλα διαδικτύου ESET PROTECT σε έναν διαφορετικό υπολογιστή από τον υπολογιστή στον οποίο εκτελείται ο διακομιστής ESET PROTECT. Αυτή η διαδικασία απαιτεί πρόσθετα βήματα.

1. Εγκαταστήστε τα πακέτα Apache Tomcat και Java.

Τα παρακάτω παραδείγματα ονομάτων πακέτων μπορεί να διαφέρουν από τα πακέτα στο αποθετήριο διανομής Linux. Το προεπιλεγμένο αποθετήριο της διανομής Linux που διαθέτετε ενδέχεται να μην περιέχει την πιο πρόσφατη υποστηριζόμενη έκδοση του Apache Tomcat και της Java.

Διανομή Linux	Εντολές τερματικού
Διανομές Debian και Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
Διανομές CentOS και Red Hat	`yum update` `yum install java-17-openjdk tomcat`
SUSE Linux	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

2. Πραγματοποιήστε λήψη του αρχείου της κονσόλας διαδικτύου (*era.war*):

```
wget https://download.eset.com/com/eset/apps/business/era/webconsole/latest/era.war
```

3. Αντιγράψτε το αρχείο *era.war* στο φάκελο Tomcat:

Debian, Ubuntu	`sudo cp era.war /var/lib/tomcat9/webapps/`
CentOS, Red Hat	`sudo cp era.war /var/lib/tomcat/webapps/`
SUSE Linux Enterprise Server	`sudo cp era.war /usr/share/tomcat/webapps/`

4. Επανεκκινήστε την υπηρεσία Tomcat για να αναπτύξετε το αρχείο *era.war*:

Debian, Ubuntu	`sudo systemctl restart tomcat9`
CentOS, Red Hat	`sudo systemctl restart tomcat`
SUSE Linux Enterprise Server	`sudo systemctl restart tomcat`

5. Βεβαιωθείτε ότι ο φάκελος *era* υπάρχει στον φάκελο Tomcat:

Debian, Ubuntu	`ls /var/lib/tomcat9/webapps`
CentOS, Red Hat	`ls /var/lib/tomcat/webapps`
SUSE Linux Enterprise Server	`ls /usr/share/tomcat/webapps`

Η έξοδος πρέπει να έχει την εξής εμφάνιση: `era era.war`

6. Ρυθμίστε την υπηρεσία Tomcat για να ξεκινά κατά την εκκίνηση: `sudo systemctl enable tomcat` (ή `tomcat9` με βάση το όνομα της υπηρεσίας)

7. Εάν εγκαταστήσατε την κονσόλα διαδικτύου ESET PROTECT σε διαφορετικό υπολογιστή από το διακομιστή ESET PROTECT, εκτελέστε αυτά τα πρόσθετα βήματα, για να ενεργοποιήσετε την επικοινωνία μεταξύ της κονσόλας διαδικτύου ESET PROTECT και του διακομιστή ESET PROTECT:

a)Διακόψτε την υπηρεσία Tomcat: `sudo systemctl stop tomcat`

b)Επεξεργαστείτε το αρχείο *EraWebServerConfig.properties*:

```
sudo nano /var/lib/tomcat/webapps/era/WEB-
INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.prop
erties
```

Αν το αρχείο *EraWebServerConfig.properties* δεν βρίσκεται στην παραπάνω διαδρομή, μπορείτε να χρησιμοποιήσετε την παρακάτω εντολή, για να βρείτε το αρχείο στο σύστημά σας:

```
find / -iname "EraWebServerConfig.properties"
```

c)Βρείτε το `server_address=localhost`

d)Αντικαταστήστε το `localhost` με τη διεύθυνση IP του διακομιστή ESET PROTECT και αποθηκεύστε το αρχείο.

e)Επανεκκινήστε την υπηρεσία Tomcat: `sudo systemctl restart tomcat` (ή `tomcat9` με βάση το όνομα της υπηρεσίας)

f)Ρυθμίστε την υπηρεσία Tomcat για να ξεκινά κατά την εκκίνηση: `sudo systemctl enable tomcat` (ή `tomcat9` με βάση το όνομα της υπηρεσίας)

8. Ανοίξτε την Κονσόλα διαδικτύου ESET PROTECT σε ένα υποστηριζόμενο πρόγραμμα περιήγησης για να δείτε μια οθόνη σύνδεσης:

• Από τον υπολογιστή που φιλοξενεί την Κονσόλα διαδικτύου ESET PROTECT: *http://localhost:8080/era*

• Από οποιονδήποτε υπολογιστή με πρόσβαση στο Internet στην Κονσόλα διαδικτύου ESET PROTECT (αντικαταστήστε το στοιχείο *IP_ADDRESS_OR_HOSTNAME* με τη διεύθυνση IP ή το όνομα κεντρικού υπολογιστή της Κονσόλας διαδικτύου ESET PROTECT): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

9. Ρύθμιση παραμέτρων της Κονσόλας διαδικτύου μετά την εγκατάσταση:

• Η προεπιλεγμένη θύρα HTTP ορίζεται σε 8080 κατά τη μη αυτόματη εγκατάσταση του Apache Tomcat. Συνιστάται να ρυθμίσετε μια σύνδεση HTTPS για το Apache Tomcat.

• Δείτε επίσης την πρόσθετη ρύθμιση παραμέτρων της Κονσόλας διαδικτύου για εταιρικές λύσεις ή συστήματα χαμηλών επιδόσεων.

Εγκατάσταση αισθητήρα rogue detection sensor – Linux

Προαπαιτούμενα

• Μπορεί να γίνει αναζήτηση στο δίκτυο (οι θύρες είναι ανοιχτές, το firewall δεν αποκλείει εισερχόμενη επικοινωνία, κ.λπ.).

• Η πρόσβαση στον υπολογιστή διακομιστή ESET PROTECT είναι εφικτή.

• Ο φορέας ESET Management πρέπει να είναι εγκατεστημένος στον τοπικό υπολογιστή, για να

υποστηρίζει πλήρως όλες τις λειτουργίες του προγράμματος

Εάν υπάρχουν πολλά τμήματα δικτύου, ο αισθητήρας Rogue Detection Sensor πρέπει να εγκατασταθεί ξεχωριστά σε κάθε τμήμα δικτύου για να δημιουργήσει μια ολοκληρωμένη λίστα όλων των συσκευών σε ολόκληρο το δίκτυο.

Εγκατάσταση

Ακολουθήστε τα παρακάτω βήματα για να εγκαταστήσετε το στοιχείο αισθητήρα RD Sensor σε Linux χρησιμοποιώντας μια εντολή τερματικού:

Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης που αναφέρονται παραπάνω.

1. Επισκεφτείτε την ενότητα λήψεων του ESET PROTECT για λήψη ενός ανεξάρτητου προγράμματος εγκατάστασης για αυτό το στοιχείο του ESET PROTECT (*rdsensor-linux-i386.sh* ή *rdsensor-linux-x86_64.sh*).

2. Ρυθμίστε το αρχείο εγκατάστασης του αισθητήρα RD Sensor ως εκτελέσιμο αρχείο: `chmod +x rdsensor-linux-x86_64.sh`

3. Χρησιμοποιήστε την ακόλουθη εντολή για να εκτελέσετε το αρχείο εγκατάστασης ως sudo:

```
sudo ./rdsensor-linux-x86_64.sh
```

4. Διαβάστε τη Συμφωνία Άδειας Χρήσης Τελικού Χρήστη. Χρησιμοποιήστε το **πλήκτρο διαστήματος** για να προχωρήσετε στην επόμενη σελίδα της EULA.
Το πρόγραμμα εγκατάστασης θα σας ζητήσει να καθορίσετε εάν αποδέχεστε τη συμφωνία. Πατήστε το πλήκτρο **Y** στο πληκτρολόγιο εάν συμφωνείτε. Διαφορετικά, πατήστε το πλήκτρο **N**.

5. Πατήστε **N** εάν συμφωνείτε να συμμετάσχετε στο Πρόγραμμα βελτίωσης προϊόντος. Διαφορετικά, πατήστε το πλήκτρο **N**.

6. Το ESET Rogue Detection Sensor θα εκκινήσει μετά την ολοκλήρωση της εγκατάστασης.

7. Για να δείτε εάν ήταν επιτυχής η εγκατάσταση, επαληθεύσετε ότι η υπηρεσία λειτουργεί εκτελώντας την παρακάτω εντολή:

```
sudo systemctl status rdsensor
```

Μπορείτε να βρείτε το αρχείο καταγραφής του Rogue Detection Sensor στα αρχεία καταγραφής: */var/log/eset/RogueDetectionSensor/trace.log*

Εγκατάσταση Σύνδεσης κινητών συσκευών - Linux

Το στοιχείο Διαχείριση/Σύνδεση κινητών συσκευών (Διαχείριση κινητών συσκευών/MDC) του ESET PROTECT (μόνο εσωτερικής εγκατάστασης) φτάνει στο τέλος του κύκλου ζωής τον Ιανουάριο του 2024. Διαβάστε περισσότερα. Συνιστάται η μετεγκατάσταση στο cloud διαχείρισης κινητών συσκευών.

Μπορείτε να εγκαταστήσετε τη Σύνδεση κινητών συσκευών σε διαφορετικό διακομιστή από εκείνον στον οποίο εκτελείται ο διακομιστής ESET PROTECT. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε αυτό το σενάριο εγκατάστασης για να υπάρχει πρόσβαση στο Mobile Device Connector από το Internet για να γίνεται πάντα διαχείριση των κινητών συσκευών του χρήστη.

Ακολουθήστε τα παρακάτω βήματα για να εγκαταστήσετε το στοιχείο Mobile Device Connector σε Linux χρησιμοποιώντας μια εντολή τερματικού:

Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης.

1. Πραγματοποιήστε λήψη της δέσμης ενεργειών εγκατάστασης του Mobile Device Connector:

```
wget https://download.eset.com/com/eset/apps/business/era/mdm/latest/mdmcore-linux-x86_64.sh
```

2. Εκτελέστε τη δέσμη ενεργειών εγκατάστασης στο παρακάτω παράδειγμα (Οι νέες γραμμές διαχωρίζονται με «\» για αντιγραφή ολόκληρης της εντολής στο τερματικό):

```
sudo ./mdmcore-linux-x86_64.sh \
--https-cert-path="full_path/proxycert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

Για μια πλήρη λίστα των διαθέσιμων παραμέτρων (εκτύπωση μηνύματος βοήθειας), χρησιμοποιήστε το:

```
--help
```

Συνιστάται να καταργήσετε εντολές που περιέχουν ευαίσθητα δεδομένα (για παράδειγμα, έναν κωδικό πρόσβασης) από το ιστορικό της γραμμής εντολών:
1.Εκτελέστε το στοιχείο `history` για να δείτε τη λίστα όλων των εντολών στο ιστορικό.
2.Εκτελέστε το στοιχείο `history -d line_number` (καθορίστε τον αριθμό γραμμής της εντολής). Εναλλακτικά, εκτελέστε το στοιχείο `history -c` για να καταργήσετε ολόκληρο το ιστορικό της γραμμής εντολών.

Απαιτούμενες παράμετροι εντολής εγκατάστασης

Υπάρχουν πολλές προαιρετικές παράμετροι εγκατάστασης, αλλά ορισμένες είναι απαραίτητες:

- Ομότιμο πιστοποιητικό - Υπάρχουν δύο μέθοδοι για να εξασφαλίσετε το Ομότιμο πιστοποιητικό

του ESET PROTECT On-Prem:

• **Εγκατάσταση με υποβοήθηση διακομιστή** - Θα πρέπει να δώσετε τα στοιχεία σύνδεσης διαχειριστή της Κονσόλας διαδικτύου ESET PROTECT (το πρόγραμμα εγκατάστασης θα λάβει αυτόματα τα απαιτούμενα πιστοποιητικά).

• **Εγκατάσταση χωρίς σύνδεση** - Θα πρέπει να παράσχετε ένα ομότιμο πιστοποιητικό (το πιστοποιητικό διακομιστή μεσολάβησης το οποίο μπορείτε να εξαγάγετε από το ESET PROTECT On-Prem). Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το προσαρμοσμένο πιστοποιητικό σας.

οΓια **Εγκατάσταση με υποβοήθηση διακομιστή** θα πρέπει να συμπεριλαμβάνεται τουλάχιστον το:

```
--webconsole-password=
```

οΓια **Εγκατάσταση χωρίς σύνδεση** να συμπεριλαμβάνεται το:

```
--cert-path=
--cert-password=
```

(Το προεπιλεγμένο πιστοποιητικό Φορέα που δημιουργήθηκε κατά τη διάρκεια της εγκατάστασης του Διακομιστή ESET PROTECT δεν χρειάζεται κωδικό πρόσβασης.)

- Πιστοποιητικό HTTPS (διακομιστή μεσολάβησης):

  οΕάν έχετε ήδη ένα πιστοποιητικό HTTPS:

  ```
  --https-cert-path=
  --https-cert-password=
  ```

  οΓια να δημιουργήσετε ένα νέο πιστοποιητικό HTTPS:

  ```
  --https-cert-generate
  --mdm-hostname=
  ```

- Σύνδεση με το διακομιστή ESET PROTECT (όνομα ή διεύθυνση IP):

  ```
  --hostname=
  ```

- Σύνδεση βάσης δεδομένων:

oΓια μια βάση δεδομένων MySQL θα πρέπει να περιλαμβάνονται τα εξής:

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

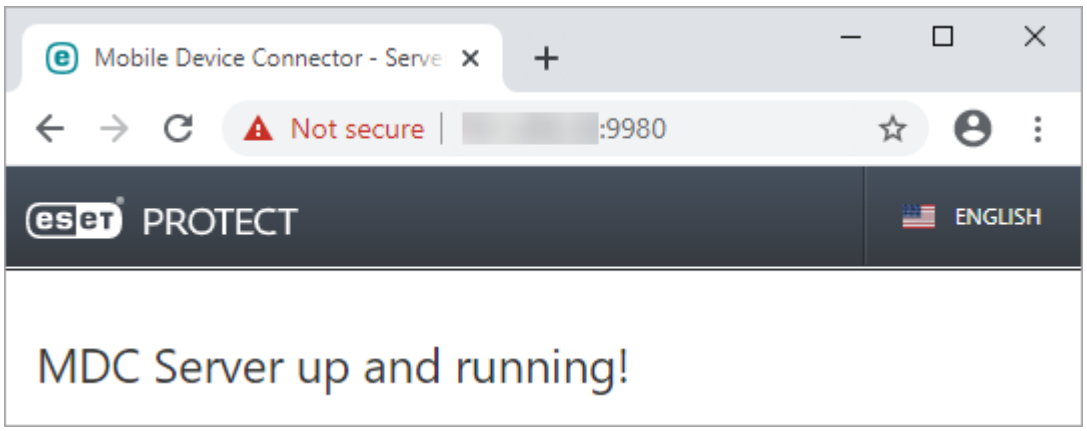
oΓια μια βάση δεδομένων Microsoft SQL θα πρέπει να περιλαμβάνονται τα εξής:

```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Αρχείο καταγραφής προγράμματος εγκατάστασης

Το αρχείο καταγραφής του προγράμματος εγκατάστασης μπορεί να είναι χρήσιμο για την αντιμετώπιση προβλημάτων και μπορείτε να το βρείτε στα Αρχεία καταγραφής.

Μετά την ολοκλήρωση της εγκατάστασης, ελέγξτε εάν εκτελείται σωστά η σύνδεση κινητών συσκευών ανοίγοντας τη διεύθυνση *https://*όνομα-κεντρικού-υπολογιστή-*mdm:*θύρα-εγγραφής (για παράδειγμα *https://eramdm:9980*) στο πρόγραμμα περιήγησης. Εάν η εγκατάσταση ήταν επιτυχής, θα δείτε το ακόλουθο μήνυμα:



Επίσης, μπορείτε να χρησιμοποιήσετε αυτή τη διεύθυνση URL για να ελέγξετε τη διαθεσιμότητα του διακομιστή της σύνδεσης κινητών συσκευών από το Internet (εάν έχει διαμορφωθεί με τέτοιο τρόπο), εάν την επισκεφτείτε από μια κινητή συσκευή. Εάν δεν μπορείτε να συνδεθείτε με τη σελίδα, ελέγξτε το firewall και τη διαμόρφωση της υποδομής δικτύου σας.

Προαπαιτούμενα Σύνδεσης κινητών

συσκευών - Linux

Για την εγκατάσταση της σύνδεσης κινητών συσκευών σε λειτουργικό σύστημα Linux, πρέπει να πληρούνται τα παρακάτω προαπαιτούμενα:

- Πρέπει να είναι ήδη εγκατεστημένος και διαμορφωμένος ένας διακομιστής βάσης δεδομένων με ριζικό λογαριασμό (δεν χρειάζεται να δημιουργηθεί λογαριασμός χρήστη πριν από την εγκατάσταση, μπορεί να τον δημιουργήσει το πρόγραμμα εγκατάστασης).
- Να είναι εγκατεστημένο στον υπολογιστή ένα πρόγραμμα οδήγησης ODBC για τη σύνδεση με το διακομιστή βάσης δεδομένων (MySQL / Microsoft SQL). Δείτε το κεφάλαιο Εγκατάσταση και ρύθμιση παραμέτρων ODBC.

> Θα πρέπει να χρησιμοποιήσετε το πακέτο `unixODBC_23` (όχι το προεπιλεγμένο πακέτο `unixODBC`) για να συνδεθεί ο MDC με τη βάση δεδομένων MySQL χωρίς προβλήματα. Αυτό ισχύει ιδιαίτερα για το SUSE Linux.

> Συνιστάται να αναπτύξετε το στοιχείο MDM σε μια κεντρική συσκευή διαφορετική από τη συσκευή στην οποία φιλοξενείται ο διακομιστής ESET PROTECT.

- Πρέπει να ρυθμιστεί το αρχείο εγκατάστασης MDMCore ως εκτελέσιμο.

```
chmod +x mdmcore-linux-x86_64.sh
```

- Μετά την εγκατάσταση, επαληθεύστε ότι εκτελείται η υπηρεσία MDMCore.

```
sudo systemctl status eramdmcore
```

- Συνιστάται να **χρησιμοποιήσετε την πιο πρόσφατη έκδοση του OpenSSL1.1.1**. Ο φορέας ESET Management υποστηρίζει επίσης OpenSSL 3.x. Η ελάχιστη υποστηριζόμενη έκδοση του OpenSSL για Linux είναι openssl-1.0.1e-30. Σε ένα σύστημα, μπορεί να είναι ταυτόχρονα εγκατεστημένες περισσότερες εκδόσεις του OpenSSL. Στο σύστημά σας πρέπει να υπάρχει τουλάχιστον μία υποστηριζόμενη έκδοση.

  oΧρησιμοποιήστε την εντολή `openssl version` για να εμφανιστεί η τρέχουσα προεπιλεγμένη έκδοση.

  oΜπορείτε να δείτε σε λίστα όλες τις εκδόσεις του OpenSSL που υπάρχουν στο σύστημά σας. Δείτε τις καταλήξεις των ονομάτων αρχείων που αναγράφονται στη λίστα χρησιμοποιώντας την εντολή `sudo find / -iname *libcrypto.so*`

  oΜπορείτε να ελέγξετε εάν ο υπολογιστής-πελάτης Linux είναι συμβατός χρησιμοποιώντας την ακόλουθη εντολή: `openssl s_client -connect google.com:443 -tls1_2`

> **OpenSSL 3.x υποστήριξη**
> - Ο Φορέας ESET Management υποστηρίζει OpenSSL 3.x.
> - Ο διακομιστής/η διαχείριση κινητών συσκευών ESET PROTECT δεν υποστηρίζει τοπικά το OpenSSL 3.x, αλλά μπορείτε να ενεργοποιήσετε την υποστήριξη OpenSSL 3.x για το ESET PROTECT On-Prem.

Εάν η βάση δεδομένων MDM στο MySQL είναι πολύ μεγάλη (χιλιάδες συσκευές), η προεπιλεγμένη τιμή `innodb_buffer_pool_size` είναι πολύ μικρή. Για περισσότερες πληροφορίες σχετικά με τη βελτιστοποίηση της βάσης δεδομένων, ανατρέξτε στη διεύθυνση: https://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html

Απαιτήσεις πιστοποιητικού

• Θα χρειαστείτε ένα **Πιστοποιητικό SSL** σε μορφή *.pfx*για ασφαλή επικοινωνία μέσω HTTPS. Συνιστάται να χρησιμοποιήσετε ένα πιστοποιητικό που παρέχεται από μια Αρχή έκδοσης πιστοποιητικού άλλου κατασκευαστή. Τα αυτο-υπογεγραμμένα πιστοποιητικά (που περιλαμβάνουν πιστοποιητικά που υπογράφονται από την Αρχή έκδοσης πιστοποιητικού του ESET PROTECT On-Prem δεν συνιστώνται, επειδή δεν επιτρέπουν όλες οι κινητές συσκευές στους χρήστες να αποδέχονται αυτο-υπογεγραμμένα πιστοποιητικά.

• Θα πρέπει να έχετε πιστοποιητικό υπογεγραμμένο από την αρχή έκδοσης πιστοποιητικού και το αντίστοιχο ιδιωτικό κλειδί, και να χρησιμοποιήσετε τις τυπικές διαδικασίες (χρησιμοποιώντας συνήθως OpenSSL) για να συγχωνεύσετε αυτά τα δύο σε ένα αρχείο *.pfx*:
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`
Αυτή είναι η τυπική διαδικασία για τους περισσότερους διακομιστές που χρησιμοποιούν πιστοποιητικά SSL.

• Για Εγκατάσταση χωρίς σύνδεση, θα χρειαστείτε επίσης ένα ομότιμο πιστοποιητικό (το **Πιστοποιητικό φορέα** το οποίο μπορείτε να εξαγάγετε από το ESET PROTECT On-Prem). Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το προσαρμοσμένο πιστοποιητικό με το ESET PROTECT On-Prem.

Εργαλείο ειδώλου - Linux

Είστε χρήστης των Windows;

Το εργαλείο ειδώλου είναι απαραίτητο για τις ενημερώσεις του μηχανισμού ανίχνευσης χωρίς σύνδεση. Εάν οι υπολογιστές-πελάτες σας δεν έχουν σύνδεση στο Internet και χρειάζονται ενημερώσεις του μηχανισμού ανίχνευσης, μπορείτε να χρησιμοποιήσετε το εργαλείο ειδώλου για να λαμβάνετε αρχεία ενημέρωσης από τους διακομιστές ενημέρωσης της ESET και να τα αποθηκεύετε τοπικά.

Το Εργαλείο ειδώλου έχει τις εξής λειτουργίες:
• Ενημερώσεις μονάδων – Πραγματοποιεί λήψη ενημερώσεων του μηχανισμού ανίχνευσης και άλλων μονάδων προγράμματος, αλλά όχι αυτόματες ενημερώσεις (uPCU).
• Δημιουργία αποθετηρίου – Μπορεί να δημιουργήσει ένα πλήρες αποθετήριο χωρίς σύνδεση, το οποίο συμπεριλαμβάνει αυτόματες ενημερώσεις (uPCU).
Το εργαλείο ειδώλου δεν πραγματοποιεί λήψη δεδομένων του ESET LiveGrid®.

Προαπαιτούμενα

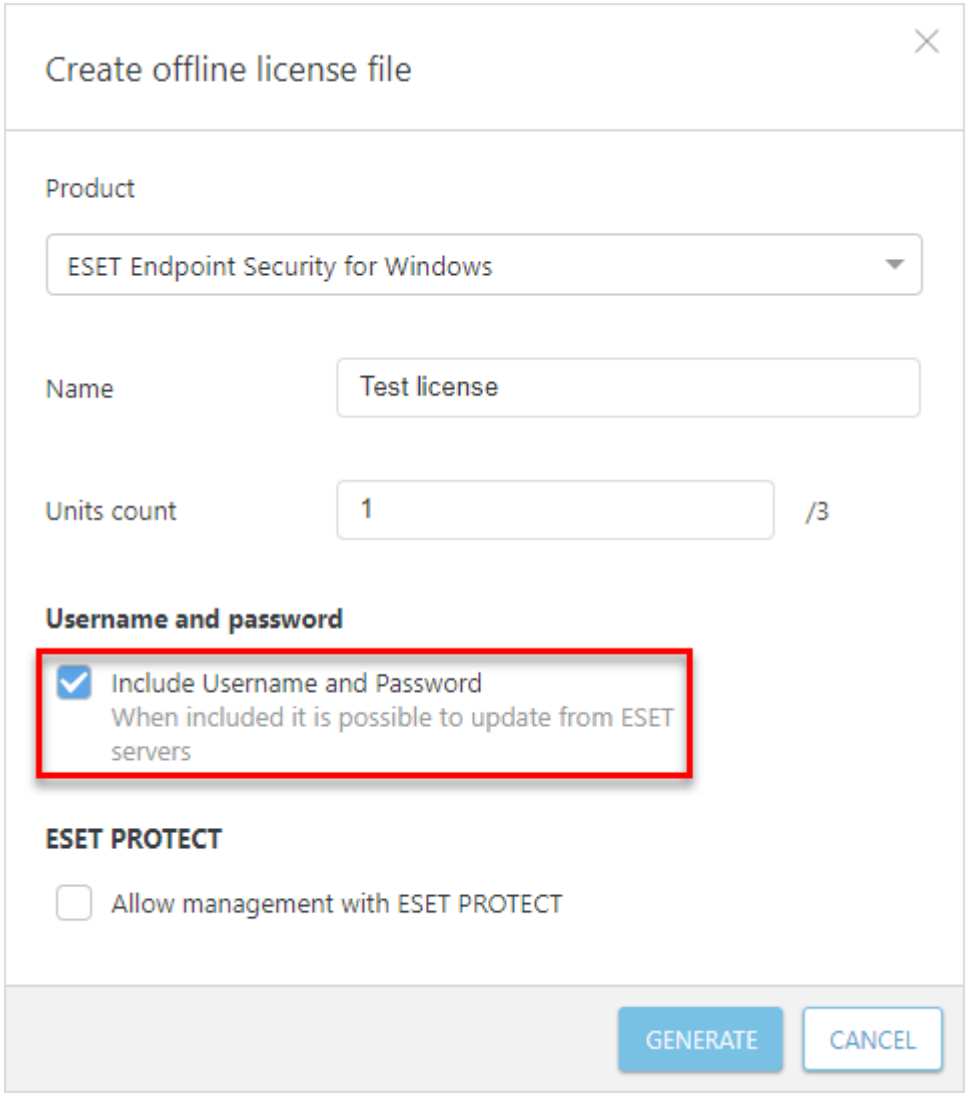
• Το αποθετήριο όπου δημιουργείται το είδωλο πρέπει να έχει δικαιώματα ανάγνωσης και εκτέλεσης για όλους τους χρήστες. Εκτελέστε αυτήν την εντολή ως χρήστης με δικαιώματα για να εκχωρήσετε το δικαίωμα: `chmod 755 mirror/folder/path` (αντικαταστήστε τη διαδρομή `mirror/folder/path` με τη διαδρομή του φακέλου ειδώλου).

• Ο φάκελος προορισμού πρέπει να είναι διαθέσιμος για κοινή χρήση, με υπηρεσία Samba/Windows ή HTTP/FTP, ανάλογα με τον τρόπο πρόσβασης που θέλετε για τις ενημερώσεις.

oΠροϊόντα ασφάλειας ESET για Windows - Μπορείτε να τα ενημερώνετε απομακρυσμένα χρησιμοποιώντας HTTP ή έναν κοινόχρηστο φάκελο.

oΠροϊόντα ασφάλειας ESET για Linux/macOS - Μπορείτε να τα ενημερώνετε απομακρυσμένα χρησιμοποιώντας μόνο HTTP. Εάν χρησιμοποιείτε έναν κοινόχρηστο φάκελο, πρέπει να βρίσκεται στον ίδιο υπολογιστή με το προϊόν ασφάλειας ESET.

• Πρέπει να έχετε ένα έγκυρο αρχείο άδειας χρήσης εκτός σύνδεσης που περιλαμβάνει όνομα χρήστη και κωδικό πρόσβασης. Κατά τη δημιουργία ενός αρχείου άδειας χρήσης, βεβαιωθείτε ότι έχετε επιλέξει το πλαίσιο ελέγχου που βρίσκεται δίπλα από το στοιχείο **Συμπερίληψη ονόματος χρήστη και κωδικού πρόσβασης**. Επίσης, πρέπει να πληκτρολογήσετε ένα **Όνομα** της άδειας χρήσης. Για την ενεργοποίηση του εργαλείου ειδώλου και τη δημιουργία του ειδώλου ενημέρωσης απαιτείται αρχείο άδειας χρήσης εκτός σύνδεσης.



Πώς να χρησιμοποιήσετε το εργαλείο ειδώλου

1.Πραγματοποιήστε λήψη του εργαλείου ειδώλου από τη σελίδα λήψεων της ESET (ενότητα **Ανεξάρτητα προγράμματα εγκατάστασης**).

2.Αποσυμπιέστε τον ληφθέντα αρχειοθήκη.

3.Ανοίξτε το τερματικό στον φάκελο με το αρχείο *MirrorTool* και κάντε το αρχείο εκτελέσιμο:

```
chmod +x MirrorTool
```

4.Εκτελέστε την παρακάτω εντολή για να προβάλετε όλες τις διαθέσιμες παραμέτρους για το Εργαλείο ειδώλου και την έκδοσή του:

```
./MirrorTool --help
```

```
root@ubuntu:/home/user/Desktop/x86_64/x86_64# ./MirrorTool --help
Mirror Tool v1.0.2226.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Σε όλα τα φίλτρα γίνεται διάκριση πεζών-κεφαλαίων.

Μπορείτε να χρησιμοποιήσετε τις παραμέτρους για να δημιουργήσετε το είδωλο του αποθετηρίου ή το είδωλο των μονάδων:

Παράμετροι για το είδωλο του αποθετηρίου και για το είδωλο των μονάδων

--proxyHost
--proxyPort
--proxyUsername
--proxyPassword
--help

Παράμετροι ειδικά για το αποθετήριο

--repositoryServer
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

Παράμετροι ειδικά για τις μονάδες

--mirrorType
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

Παράμετρος	Περιγραφή
--updateServer	Το Mirror Tool δημιουργεί μια δομή φακέλων που είναι διαφορετική από αυτή του ειδώλου του τερματικού. Κάθε φάκελος διατηρεί αρχεία ενημέρωσης για μια ομάδα προϊόντων. ⚠ Πρέπει να καθορίσετε τον πλήρη σύνδεσμο του διακομιστή ενημέρωσης (πλήρη διαδρομή στον σωστό φάκελο) στις ρυθμίσεις ενημέρωσης του προϊόντος που χρησιμοποιεί το είδωλο.
--offlineLicenseFilename	Πρέπει να καθορίσετε μια διαδρομή προς το αρχείο άδειας χρήσης εκτός σύνδεσης (όπως αναφέρεται παραπάνω).

Παράμετρος	Περιγραφή
`--mirrorOnlyLevelUpdates`	Δεν απαιτείται όρισμα. Εάν οριστεί, θα γίνει λήψη μόνο ενημερώσεων επιπέδου (δεν θα γίνει λήψη nano ενημερώσεων). Διαβάστε περισσότερα σχετικά με τους τύπους ενημερώσεων στο άρθρο της Γνωσιακής βάσης.
`--mirrorFileFormat`	⚠ Πριν χρησιμοποιήσετε την παράμετρο `--mirrorFileFormat`, βεβαιωθείτε ότι το περιβάλλον σας δεν περιέχει παλαιότερες (6.5 και παλαιότερες) και νεότερες (6.6. και νεότερες) εκδόσεις προϊόντων ασφαλείας της ESET. Η εσφαλμένη χρήση αυτής της παραμέτρου ενδέχεται να οδηγήσει σε εσφαλμένες ενημερώσεις των προϊόντων ασφαλείας της ESET. Μπορείτε να καθορίσετε τον τύπο αρχείων ενημέρωσης που θα ληφθούν. Πιθανές τιμές (με διάκριση πεζών-κεφαλαίων): • `dat` - Χρησιμοποιήστε αυτή την τιμή εάν έχετε περιβάλλον μόνο με προϊόντα ασφαλείας ESET εκδόσεις 6.5 και παλαιότερες. • `dll` - Χρησιμοποιήστε αυτή την τιμή εάν έχετε περιβάλλον μόνο με προϊόντα ασφαλείας ESET εκδόσεις 6.6 και νεότερες. Η παράμετρος παραβλέπεται κατά τη δημιουργία ενός ειδώλου για προϊόντα παλαιού τύπου (`ep4`, `ep5`).
`--compatibilityVersion`	Αυτή η προαιρετική παράμετρος εφαρμόζεται στο εργαλείο ειδώλου που διανέμεται με το ESET PROTECT On-Prem 8.1 και νεότερες εκδόσεις. Το εργαλείο ειδώλου θα πραγματοποιήσει λήψη αρχείων ενημέρωσης που είναι συμβατά με την έκδοση αποθετηρίου του ESET PROTECT On-Prem που καθορίζετε στο όρισμα της παραμέτρου σε μορφή `x.x` ή `x.x.x.x`, για παράδειγμα: `--compatibilityVersion 11.0` ή `--compatibilityVersion 8.1.13.0`. Η παράμετρος `--compatibilityVersion` εξαιρεί τις αυτόματες ενημερώσεις (uPCU) από το είδωλο. Εάν χρειάζεστε τις αυτόματες ενημερώσεις (uPCU) στο περιβάλλον σας και θέλετε να μειώσετε το μέγεθος του ειδώλου, χρησιμοποιήστε την παράμετρο `--filterFilePath`.

ℹ Για να μειώσετε την ποσότητα δεδομένων που λαμβάνονται από το αποθετήριο της ESET, συνιστάται να χρησιμοποιήσετε τις νέες παραμέτρους στο Εργαλείο ειδώλου που διανέμεται με το ESET PROTECT On-Prem 9: `--filterFilePath` και `--dryRun`:
1.Δημιουργήστε ένα φίλτρο σε μορφή *JSON* (δείτε τη διαδρομή `--filterFilePath` παρακάτω).
2.Εκτελέστε μια δοκιμαστική εκτέλεση του Εργαλείου ειδώλου με την παράμετρο `--dryRun` (δείτε παρακάτω) και προσαρμόστε το φίλτρο όπως απαιτείται.
3.Εκτελέστε το Εργαλείο ειδώλου με την παράμετρο `--filterFilePath` και το καθορισμένο φίλτρο λήψης, μαζί με τις παραμέτρους `--intermediateRepositoryDirectory` και `--outputRepositoryDirectory`.
4.Εκτελείτε το Εργαλείο ειδώλου τακτικά, ώστε να χρησιμοποιείτε πάντα τα πιο πρόσφατα προγράμματα εγκατάστασης.

Παράμετρος	Περιγραφή

`--filterFilePath`	Χρησιμοποιήστε αυτήν την προαιρετική παράμετρο για να φιλτράρετε προϊόντα ασφάλειας ESET με βάση ένα αρχείο κειμένου σε μορφή *JSON*, το οποίο τοποθετείται στον ίδιο φάκελο με το εργαλείο ειδώλου, για παράδειγμα: `--filterFilePath filter.txt`)
	Περιγραφή ρύθμισης παραμέτρων φίλτρου:
	Η μορφή του αρχείου ρύθμισης παραμέτρων για φιλτράρισμα προϊόντος είναι *JSON* με την ακόλουθη δομή:
	• ριζικό αντικείμενο *JSON*:
	o`use_legacy` (boolean, προαιρετικά) - εάν επιλεχτεί προσδιορισμός «true» (αληθές), θα συμπεριληφθούν προϊόντα παλαιού τύπου.
	o`defaults` (αντικείμενο *JSON*, προαιρετικά) - ορίζει τις ιδιότητες φίλτρου που θα εφαρμοστούν σε όλα τα προϊόντα.
	■`languages` (λίστα) - Καθορίστε τους κωδικούς γλώσσας ISO των γλωσσών που θα συμπεριληφθούν, για παράδειγμα, για Γαλλικά πληκτρολογήστε `"fr_FR"`. Άλλοι κωδικοί γλωσσών περιλαμβάνονται στον παρακάτω πίνακα. Για να επιλέξετε περισσότερες γλώσσες, διαχωρίστε τες με κόμμα και διάστημα, για παράδειγμα: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (κατάλογος) – πλατφόρμες που θα συμπεριληφθούν (`["x64", "x86", "arm64"]`).
	⚠ Χρησιμοποιήστε το φίλτρο `platforms` με προσοχή. Για παράδειγμα, εάν το Εργαλείο ειδώλου πραγματοποιήσει λήψη μόνο προγραμμάτων εγκατάστασης 64 bit και υπάρχουν υπολογιστές 32 bit στην υποδομή σας, τα προϊόντα ασφάλειας ESET 64 bit δεν θα εγκατασταθούν σε υπολογιστές 32 bit.
	■`os_types` (κατάλογος) – Τύποι λειτουργικού συστήματος που θα συμπεριληφθούν (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (λίστα αντικειμένων JSON, προαιρετικά) - φίλτρα που θα εφαρμοστούν σε συγκεκριμένα προϊόντα - παράκαμψη της παραμέτρου `defaults` για συγκεκριμένα προϊόντα. Τα αντικείμενα έχουν τις ακόλουθες ιδιότητες:
	■`app_id` (συμβολοσειρά) - απαιτείται εάν δεν έχει καθοριστεί η παράμετρος `name`.
	■`name` (συμβολοσειρά), απαιτείται εάν δεν έχει καθοριστεί η παράμετρος `app_id`.
	■`version` (συμβολοσειρά) - καθορίζει την έκδοση ή το εύρος εκδόσεων που θα συμπεριληφθούν.
	■`languages` (λίστα) - κωδικοί γλώσσας ISO των γλωσσών που θα συμπεριληφθούν (δείτε τον παρακάτω πίνακα).
	■`platforms` (κατάλογος) – πλατφόρμες που θα συμπεριληφθούν (`["x64", "x86", "arm64"]`).
	■`os_types` (κατάλογος) – Τύποι λειτουργικού συστήματος που θα συμπεριληφθούν (`["windows"]`, `["linux"]`, `["mac"]`).
	ℹ Για να προσδιορίσετε τις κατάλληλες τιμές για τα πεδία, εκτελέστε το Εργαλείο ειδώλου σε δοκιμαστική λειτουργία και βρείτε το σχετικό προϊόν στο αρχείο CSV που δημιουργήθηκε.
	Περιγραφές μορφής συμβολοσειράς έκδοσης
	Όλοι οι αριθμοί έκδοσης αποτελούνται από τέσσερις αριθμούς διαχωρισμένους με κουκκίδες (για παράδειγμα, `7.1.0.0`). Μπορείτε να καθορίσετε λιγότερους αριθμούς κατά τη σύνταξη φίλτρων έκδοσης (για παράδειγμα `7.1`) και οι υπόλοιποι αριθμοί θα είναι μηδέν (το `7.1` ισούται με το `7.1.0.0`).
	Η συμβολοσειρά έκδοσης μπορεί να έχει μία από τις δύο ακόλουθες μορφές:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oΕπιλέγει εκδόσεις μεγαλύτερες/μικρότερες από ή ίσες/μικρότερες από ή ίσες/ίσες με την καθορισμένη έκδοση.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oΕπιλέγει εκδόσεις που είναι μεγαλύτερες από ή ίσες με το χαμηλότερο όριο και μικρότερες από ή ίσες με το υψηλότερο όριο.
	Οι συγκρίσεις γίνονται αριθμητικά σε κάθε τμήμα του αριθμού έκδοσης, από αριστερά προς τα δεξιά.
	Παράδειγμα JSON
	✓
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0–8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	Η παράμετρος `--filterFilePath` αντικαθιστά τις παραμέτρους `--languageFilterForRepository`, `--productFilterForRepository` και `--downloadLegacyForRepository` που χρησιμοποιούνται στις παλαιότερες εκδόσεις του Εργαλείου ειδώλου (που κυκλοφόρησαν με το ESET PROTECT On-Prem 8.x).

Παράμετρος	Περιγραφή
`--dryRun`	Όταν χρησιμοποιείτε αυτήν την προαιρετική παράμετρο, το εργαλείο ειδώλου δεν θα πραγματοποιήσει λήψη κανενός αρχείου, αλλά θα δημιουργήσει ένα αρχείο *.csv* στο οποίο θα καταγράφονται όλα τα πακέτα που θα ληφθούν. Μπορείτε να χρησιμοποιήσετε αυτήν την παράμετρο χωρίς τις υποχρεωτικές παραμέτρους `--intermediateRepositoryDirectory` και `--outputRepositoryDirectory`, για παράδειγμα: • Windows: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv` • Linux: `sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv` ℹ Ορισμένα προγράμματα εγκατάστασης της ESET δεν έχουν συγκεκριμένη γλώσσα (με κώδικα γλώσσας `multilang`) και το Εργαλείο ειδώλου θα τα καταχωρίσει στο αρχείο *.csv* ακόμα και αν καθορίσετε `γλώσσες` στην παράμετρο `--filterFilePath`. Εάν χρησιμοποιείτε την παράμετρο `--dryRun` καθώς επίσης και τις παραμέτρους `--intermediateRepositoryDirectory --outputRepositoryDirectory`, το εργαλείο ειδώλου δεν εκκαθαρίζει το *outputRepositoryDirectory*.
`--listUpdatableProducts`	Καταγράψτε σε λίστα όλα τα προϊόντα ESET για τα οποία μπορεί το Mirror Tool να λαμβάνει ενημερώσεις μονάδων (εκτός αν χρησιμοποιείται η παράμετρος `--excludedProducts`). Η παράμετρος είναι διαθέσιμη από τις εκδόσεις Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

Δομή φακέλου του Mirror Tool

Από προεπιλογή, εάν δεν καθορίσετε την παράμετρο `--updateServer`, το Mirror Tool δημιουργεί αυτήν τη δομή φακέλου στον διακομιστή HTTP:

> **Να μην χρησιμοποιείται διακομιστής ειδώλου μόνο HTTP**
> Βεβαιωθείτε ότι ο τοπικός διακομιστής ειδώλου χρησιμοποιεί πρωτόκολλα HTTP και HTTPS ή μόνο HTTPS. Εάν ο διακομιστής ειδώλου χρησιμοποιεί μόνο HTTP, δεν μπορείτε να χρησιμοποιήσετε την εργασία υπολογιστή-πελάτη «Εγκατάσταση λογισμικού», επειδή δεν είναι δυνατή η ανάκτηση της Συμφωνίας Άδειας Χρήσης Τελικού Χρήστη του προϊόντος ασφάλειας ESET από έναν διακομιστή HTTP.

Προεπιλεγμένοι φάκελοι του Mirror Tool	Προϊόν ασφάλειας ESET	Διακομιστής ενημέρωσης (σύμφωνα με την τοποθεσία ρίζας του διακομιστή HTTP)
mirror/eset_upd/era6	ESET PROTECT On-Prem (όλες οι εκδόσεις)	Για να ενημερώσετε το ESET PROTECT On-Prem 11.0 από το είδωλο, ρυθμίστε τον διακομιστή ενημέρωσης σε *http://your_server_address/mirror/eset_upd/era6*
mirror/eset_upd/ep[έκδοση]	ESET Endpoint Antivirus/Security έκδοση 6.x (και νεότερες εκδόσεις) για Windows. Κάθε κύρια έκδοση έχει το φάκελό της, για παράδειγμα *ep10* για την έκδοση 10.x.	*http://your_server_address/mirror/eset_upd/ep10* (ένα παράδειγμα για την έκδοση 10.x)
mirror/eset_upd/v5	ESET Endpoint Antivirus/Security έκδοση 5.x για Windows	*http://your_server_address/mirror/eset_upd/v5*

Προϊόντα ασφάλειας ESET Linux/macOS

Πρέπει να καθορίσετε την παράμετρο `--updateServer` και να δημιουργήσετε πρόσθετους φακέλους για να ενημερώσετε τα προϊόντα ασφάλειας ESET για Linux/macOS από το είδωλο HTTP (βλ. παρακάτω).

--updateServer	Πρόσθετος φάκελος του Mirror Tool	Προϊόν ασφάλειας ESET	Διακομιστής ενημέρωσης (σύμφωνα με την τοποθεσία ρίζας του διακομιστή HTTP)
http://update.eset.com/eset_upd/businesslinux	*mirror/eset_upd/*BusinessLinux	ESET Endpoint Antivirus για Linux	*http://your_server_address/mirror/eset_upd/BusinessLinux*
http://update.eset.com/eset_upd/serverlinux	*mirror/eset_upd/*LinuxServer	ESET Server Security για Linux	*http://your_server_address/mirror/eset_upd/LinuxServer*
http://update.eset.com/eset_upd/businessmac	*mirror/eset_upd/*BusinessMac	ESET Endpoint Security; έκδοση 7.x+ για macOS	*http://your_server_address/mirror/eset_upd/BusinessMac*
http://update.eset.com/eset_mobile/eesa	*mirror/eset_upd/*EndpointAndroid	ESET Endpoint Security for Android	*http://your_server_address/mirror/eset_upd/EndpointAndroid*

Πίνακας κωδικών γλώσσας

Για να δημιουργήσετε ένα είδωλο, εκτελέστε το εργαλείο ειδώλου με τις ελάχιστες απαιτούμενες παραμέτρους τουλάχιστον. Ακολουθεί ένα παράδειγμα:

```
sudo ./MirrorTool --mirrorType regular \

--intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp \

--offlineLicenseFilename /tmp/mirrorTool/offline.lf \

--outputDirectory /tmp/mirrorTool/mirror
```

Ακολουθεί ένα παράδειγμα πιο προηγμένης ρύθμισης παραμέτρων για ένα αποθετήριο εκτός σύνδεσης με επιλεγμένα προϊόντα, γλώσσες και ενεργοποιημένη λήψη αρχείων παλαιού τύπου, τα οποία καθορίζονται στο αρχείο *filter.txt* (δείτε το παράδειγμα περιεχομένων του αρχείου στις λεπτομέρειες της παραμέτρου `--filterFilePath` παραπάνω):

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \

--intermediateRepositoryDirectory /tmp/repoTemp \

--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \

--filterFilePath filter.txt
```

Συνιστάται να καταργήσετε εντολές που περιέχουν ευαίσθητα δεδομένα (για παράδειγμα, έναν κωδικό πρόσβασης) από το ιστορικό της γραμμής εντολών:
1.Εκτελέστε το στοιχείο `history` για να δείτε τη λίστα όλων των εντολών στο ιστορικό.
2.Εκτελέστε το στοιχείο `history -d line_number` (καθορίστε τον αριθμό γραμμής της εντολής). Εναλλακτικά, εκτελέστε το στοιχείο `history -c` για να καταργήσετε ολόκληρο το ιστορικό της γραμμής εντολών.

Εργαλείο ειδώλου και ρυθμίσεις ενημέρωσης

• Για να αυτοματοποιήσετε τις λήψεις για ενημερώσεις λειτουργικών μονάδων, μπορείτε να δημιουργήσετε ένα χρονοδιάγραμμα για την εκτέλεση του Εργαλείου ειδώλου. Για να το κάνετε αυτό, ανοίξτε την Κονσόλα διαδικτύου και πλοηγηθείτε στα στοιχεία **Εργασίες υπολογιστή-πελάτη** > **Λειτουργικό σύστημα** > **Εκτέλεση εντολής. Επιλέξτε Γραμμή εντολής που θα εκτελεστεί** (συμπεριλαμβανομένης μιας διαδρομής προς το αρχείο *MirrorTool.exe*) και ένα εύλογο ερέθισμα (όπως μια έκφραση CRON για κάθε ώρα 0 0 * * * ? *). Εναλλακτικά, μπορείτε να χρησιμοποιήσετε το Χρονοδιάγραμμα εργασιών των Windows ή το `Cron` σε Linux.

• Για να διαμορφώσετε τις ενημερώσεις σε έναν ή περισσότερους υπολογιστές-πελάτες, δημιουργήστε μια νέα πολιτική και διαμορφώστε το **Διακομιστή ενημέρωσης** για να κατευθύνει στη διεύθυνση ειδώλου ή τον κοινόχρηστο φάκελό σας.

Εγκατάσταση στοιχείου στο macOS

Στα περισσότερα σενάρια εγκατάστασης, πρέπει να εγκαταστήσετε διαφορετικά στοιχεία του ESET PROTECT σε διαφορετικούς υπολογιστές ώστε να εξυπηρετούνται οι διαφορετικές αρχιτεκτονικές δικτύου, να πληρούνται οι απαιτήσεις επιδόσεων ή για άλλους λόγους.

Το MacOS υποστηρίζεται μόνο ως πρόγραμμα-πελάτης. Ο Φορέας ESET Management και τα προϊόντα ESET για macOS μπορούν να εγκατασταθούν σε macOS. Ωστόσο, ο Διακομιστής ESET PROTECT δεν είναι δυνατόν να εγκατασταθεί σε macOS.

Εγκατάσταση φορέα - macOS

Μπορείτε να εγκαταστήσετε τον φορέα ESET Management σε macOS με δύο τρόπους:

• Απομακρυσμένη – Χρήση της εργασίας διακομιστή **Ανάπτυξη φορέα**. Εάν αντιμετωπίσετε προβλήματα κατά την απομακρυσμένη ανάπτυξη του Φορέα ESET Management (η εργασία διακομιστή **Ανάπτυξη φορέα** ολοκληρώνεται με κατάσταση «Απέτυχε») ανατρέξτε στην Αντιμετώπιση προβλημάτων Ανάπτυξης φορέα.

• Τοπικά – Δείτε τις παρακάτω οδηγίες.

Προαπαιτούμενα

• Ο ESET PROTECTΔιακομιστής και η ESET PROTECTΚονσόλα διαδικτύου είναι εγκατεστημένα (σε υπολογιστή διακομιστή).

• Έχει δημιουργηθεί πιστοποιητικό φορέα και έχει προετοιμαστεί στον τοπικό δίσκο σας.

- Έχει προετοιμαστεί μια Αρχή έκδοσης πιστοποιητικών στον τοπικό δίσκο σας (απαιτείται μόνο για μη υπογεγραμμένα πιστοποιητικά).

Εγκατάσταση

Ακολουθήστε τα παρακάτω βήματα για να εγκαταστήσετε το στοιχείο φορέα ESET Management τοπικά σε macOS:

Βεβαιωθείτε ότι πληρούνται όλα τα προαπαιτούμενα εγκατάστασης που αναφέρονται παραπάνω.

1. Λάβετε το αρχείο εγκατάστασης (ανεξάρτητο πρόγραμμα εγκατάστασης φορέα *.dmg*) από τον ιστότοπο λήψεων της ESET ή από τον διαχειριστή του συστήματος.

2. Κάντε διπλό κλικ στο αρχείο *Agent-MacOSX-x86_64.dmg* και, στη συνέχεια, κάντε διπλό κλικ στο αρχείο *.pkg* για να ξεκινήσει η εγκατάσταση.

3. Συνεχίστε με την εγκατάσταση. Όταν ερωτηθείτε, πληκτρολογήστε τα δεδομένα του στοιχείου **Σύνδεση διακομιστή**:

- **Όνομα κεντρικού υπολογιστή διακομιστή**: όνομα κεντρικού υπολογιστή ή διεύθυνση IP του διακομιστή ESET PROTECT
- **Θύρα διακομιστή**: θύρα για επικοινωνία φορέα - διακομιστή, η προεπιλογή είναι 2222.
- **Χρήση διακομιστή μεσολάβησης**: κάντε κλικ αν θέλετε να χρησιμοποιήσετε διακομιστή μεσολάβησης HTTP για σύνδεση φορέα - διακομιστή.

Αυτή η ρύθμιση διακομιστή μεσολάβησης χρησιμοποιείται μόνο για (αντιγραφή) μεταξύ φορέα ESET Management και διακομιστή ESET PROTECT, όχι για αποθήκευση των ενημερώσεων στην προσωρινή μνήμη.
- **Όνομα κεντρικού υπολογιστή διακομιστή μεσολάβησης**: όνομα κεντρικού υπολογιστή ή διεύθυνση IP του υπολογιστή του διακομιστή μεσολάβησης HTTP.
- **Θύρα διακομιστή μεσολάβησης**: η προεπιλεγμένη τιμή είναι 3128.
- **Όνομα χρήστη**, **Κωδικός πρόσβασης**: εισαγάγετε τα διαπιστευτήρια που χρησιμοποιούνται από τον διακομιστή μεσολάβησης, αν χρησιμοποιείται έλεγχος ταυτότητας.

Μπορείτε να αλλάξετε τις ρυθμίσεις διακομιστή μεσολάβησης αργότερα στην πολιτική. Ο διακομιστής μεσολάβησης πρέπει να είναι εγκατεστημένος, για να μπορείτε να διαμορφώσετε μια σύνδεση φορέα - διακομιστή μέσω διακομιστή μεσολάβησης.

4. Επιλέξτε ένα ομότιμο πιστοποιητικό και έναν κωδικό πρόσβασης για αυτό το πιστοποιητικό. Προαιρετικά, μπορείτε να προσθέσετε μια αρχή έκδοσης πιστοποιητικού.

Ο κωδικός πρόσβασης του πιστοποιητικού δεν πρέπει να περιέχει τους ακόλουθους χαρακτήρες: " \ Αυτοί οι χαρακτήρες προκαλούν κρίσιμο σφάλμα κατά την αρχικοποίηση του φορέα.

5. Ελέγξτε την τοποθεσία εγκατάστασης και κάντε κλικ στο στοιχείο **Εγκατάσταση**. Ο Φορέας θα εγκατασταθεί στον υπολογιστή σας.

6. Ενεργοποίηση πλήρους πρόσβασης στον δίσκο για τον Φορέα ESET Management:

Τοπικά:

a)Ανοίξτε τα στοιχεία **Προτιμήσεις συστήματος** > **Ασφάλεια και Απόρρητο** > **Απόρρητο**.

b)Ξεκλειδώστε τις ρυθμίσεις στην κάτω αριστερή γωνία.

c)Κάντε κλικ στο στοιχείο **Πλήρης πρόσβαση στον δίσκο**.

d)Κάντε κλικ στα στοιχεία **+** > **Εφαρμογή** > **ESET** > **Άνοιγμα** και προσθέστε τον Φορέα ESET Management στη λίστα εφαρμογών στον φάκελο **Πλήρης πρόσβαση στον δίσκο**.

e)Κλειδώστε τις ρυθμίσεις στην κάτω αριστερή γωνία.

Απομακρυσμένα:

a)Κατεβάστε το αρχείο ρύθμισης παραμέτρων .plist.

b)Δημιουργήστε δύο UUID με ένα πρόγραμμα δημιουργίας UUID της επιλογής σας και χρησιμοποιήστε ένα πρόγραμμα επεξεργασίας κειμένου για να αντικαταστήσετε τις συμβολοσειρές με το κείμενο. Εισαγάγετε τα UUID 1 και UUID 2 στο προφίλ ρύθμισης παραμέτρων που έχετε λάβει.

c)Αναπτύξτε το αρχείο προφίλ ρυθμίσεων παραμέτρων .plist χρησιμοποιώντας τον διακομιστή διαχείρισης κινητών συσκευών. Ο υπολογιστής σας πρέπει να εγγραφεί στον διακομιστή διαχείρισης κινητών συσκευών για να αναπτυχθούν προφίλ ρύθμισης παραμέτρων σε υπολογιστές.

7. Ο υπολογιστής με τον εγκατεστημένο φορέα θα εμφανιστεί στην κονσόλα διαδικτύου ESET PROTECT και μπορείτε να τον διαχειριστείτε χρησιμοποιώντας το ESET PROTECT On-Prem.

Αντιμετώπιση προβλημάτων κατά την εγκατάσταση του Φορέα

Βεβαιωθείτε ότι εκτελείται ο φορέας: Κάντε κλικ στο στοιχείο **Μετάβαση** > **Βοηθητικά προγράμματα** και, στη συνέχεια, κάντε διπλό κλικ στο στοιχείο **Παρακολούθηση δραστηριότητας**. Κάντε κλικ στην καρτέλα **Ενέργεια** ή στην καρτέλα **CPU** και εντοπίστε τη διεργασία που ονομάζεται **ERAAgent**.

Το αρχείο καταγραφής του φορέα ESET Management βρίσκεται στην παρακάτω διαδρομή:

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

Το πρωτόκολλο επικοινωνίας μεταξύ του φορέα και του διακομιστή ESET PROTECT δεν υποστηρίζει τον έλεγχο ταυτότητας. Οποιαδήποτε λύση διακομιστή μεσολάβησης που χρησιμοποιείται για προώθηση της επικοινωνίας του φορέα στο διακομιστή ESET PROTECT και απαιτεί έλεγχο ταυτότητας δεν θα λειτουργεί.
Εάν επιλέξετε να χρησιμοποιήσετε μια μη προεπιλεγμένη θύρα για την Κονσόλα διαδικτύου ή το φορέα, ενδέχεται να απαιτείται προσαρμογή του τείχους προστασίας. Διαφορετικά, η εγκατάσταση μπορεί να αποτύχει.

Είδωλο ISO

Το αρχείο ειδώλου ISO είναι μία από τις μορφές με τις οποίες μπορείτε να κάνετε λήψη (κατηγορία προγραμμάτων εγκατάστασης όλα-σε-ένα) των προγραμμάτων εγκατάστασης του ESET PROTECT. Το είδωλο ISO περιέχει τα ακόλουθα:

- Πακέτο εγκατάστασης ESET PROTECT
- Ξεχωριστά προγράμματα εγκατάστασης για κάθε στοιχείο

Το είδωλο ISO είναι χρήσιμο εάν θέλετε να διατηρήσετε όλα τα προγράμματα εγκατάστασης του ESET PROTECT σε ένα μέρος. Επίσης, εξαλείφει την ανάγκη λήψης των προγραμμάτων εγκατάστασης από τον ιστότοπο της ESET κάθε φορά που θέλετε να εκτελέσετε την εγκατάσταση. Επιπλέον, το είδωλο ISO είναι χρήσιμο εάν θέλετε να εγκαταστήσετε το ESET PROTECT On-Prem σε έναν εικονικό υπολογιστή.

Εγγραφή υπηρεσίας DNS

Για να ρυθμίσετε μια εγγραφή πόρου DNS:

1.Στο διακομιστή DNS (ο διακομιστής DNS στον ελεγκτή τομέα σας), πλοηγηθείτε στα στοιχεία **Πίνακας ελέγχου** > **Εργαλεία διαχείρισης**.

2.Επιλέξτε την τιμή DNS.

3.Στη διαχείριση DNS, επιλέξτε _tcp από ένα δέντρο και δημιουργήστε μια νέα εγγραφή για την **Τοποθεσία υπηρεσίας (SRV)**.

4.Εισαγάγετε το όνομα υπηρεσίας στο πεδίο **Υπηρεσία** σύμφωνα με τους τυπικούς κανόνες DNS, πληκτρολογήστε μια κάτω παύλα (_) μπροστά από το όνομα υπηρεσίας (χρησιμοποιείστε το δικό σας όνομα υπηρεσίας, για παράδειγμα **_era**).

5.Εισαγάγετε το πρωτόκολλο tcp στο πεδίο **Πρωτόκολλο** με την ακόλουθη μορφή:_tcp.

6.Εισαγάγετε τη θύρα 2222 στο πεδίο **Αριθμός θύρας**.

7.Εισαγάγετε το πλήρως προσδιορισμένο όνομα τομέα (FQDN) του διακομιστή ESET PROTECT στο πεδίο **Κεντρικός υπολογιστής που προσφέρει αυτή την υπηρεσία**.

8.Κάντε κλικ στα κουμπιά **OK** > **Τέλος** για να αποθηκεύσετε την εγγραφή. Η εγγραφή θα εμφανιστεί στη λίστα.

Για να επαληθεύσετε την εγγραφή DNS:

1.Συνδεθείτε με οποιονδήποτε υπολογιστή στον τομέα σας και ανοίξτε μια γραμμή εντολής (cmd.exe).

2.Πληκτρολογήστε `nslookup` στη γραμμή εντολής και πατήστε **Enter**.

3.Πληκτρολογήστε `set querytype=srv` και πατήστε **Enter**.

4.Πληκτρολογήστε `_era._tcp.domain.name` και πατήστε **Enter**. Η τοποθεσία της υπηρεσίας εμφανίζεται σωστά.

> Μη ξεχάσετε να αλλάξετε την τιμή του στοιχείου "Κεντρικός υπολογιστής που προσφέρει αυτή την υπηρεσία": στο FQDN του νέου διακομιστή σας, εάν εγκαταστήσετε το διακομιστή ESET PROTECT σε διαφορετικό υπολογιστή.

Σενάριο εγκατάστασης εκτός σύνδεσης για το ESET PROTECT On-Prem

Για να εγκαταστήσετε το ESET PROTECT On-Prem και τα στοιχεία του σε περιβάλλοντα χωρίς πρόσβαση στο Internet, ακολουθήστε τις οδηγίες εγκατάστασης υψηλού επιπέδου (με το ESET PROTECT On-Prem εγκατεστημένο σε Windows).

Σε έναν υπολογιστή με σύνδεση στο Internet

1. Δημιουργήστε έναν φάκελο δικτύου κοινής χρήσης.

2. Πραγματοποιήστε λήψη των ακόλουθων προγραμμάτων εγκατάστασης στον φάκελο κοινής χρήσης:

- ESET PROTECT Πρόγραμμα εγκατάστασης "all in one"
- Ένα υποστηριζόμενο πακέτο JDK (απαιτείται για την Κονσόλα διαδικτύου).
- Πρόγραμμα ζωντανής εγκατάστασης φορέα ESET Management
- Προγράμματα εγκατάστασης προϊόντων ασφάλειας ESET (για παράδειγμα, ESET Endpoint Security)

Σε έναν υπολογιστή με Windows χωρίς σύνδεση στο διαδίκτυο που βρίσκεται στο ίδιο τοπικό δίκτυο

1. Αντιγράψτε τα προγράμματα εγκατάστασης από τον φάκελο δικτύου κοινής χρήσης σε έναν υπολογιστή με Windows χωρίς σύνδεση στο διαδίκτυο, στον οποίο θέλετε να εγκαταστήσετε το ESET PROTECT On-Prem.

2. Εγκαταστήστε το πακέτο JDK.

3. Εγκαταστήστε το ESET PROTECT On-Prem στα Windows χρησιμοποιώντας το πρόγραμμα εγκατάστασης «Όλα σε ένα». Επιλέξτε το στοιχείο **Ενεργοποίηση αργότερα** κατά τη διάρκεια της εγκατάστασης.

4. Ενεργοποιήστε το ESET PROTECT On-Prem με μια άδεια χρήσης εκτός σύνδεσης.

5. Αναπτύξτε τον Φορέα ESET Management σε υπολογιστές στο περιβάλλον χωρίς σύνδεση μέσω του Δέσμη ενεργειών προγράμματος εγκατάστασης φορέα. Τροποποιήστε τη δέσμη ενεργειών εγκατάστασης για να χρησιμοποιήσετε τη νέα διεύθυνση URL, ώστε να αποκτήσετε πρόσβαση στο

πακέτο εγκατάστασης φορέα από τον φάκελο δικτύου κοινής χρήσης.

6. Αναπτύξτε τα προϊόντα ασφάλειας ESET σε σταθμούς εργασίας χρησιμοποιώντας μια εργασία Εγκατάστασης λογισμικού. Επιλέξτε το στοιχείο **<Choose package>** και δώστε μια προσαρμοσμένη διεύθυνση URL για το πακέτο εγκατάστασης από το τοπικό αποθετήριο.

7. Ενεργοποίηση διαχειριζόμενων τερματικών με άδεια χρήσης χωρίς σύνδεση.

8. Απενεργοποιήστε το ESET LiveGrid®.

Συνιστάται να διατηρείτε ενημερωμένη την υποδομή ESET εκτός σύνδεσης χρησιμοποιώντας ένα τοπικό αποθετήριο ενημερώσεων. Ενημερώνετε τακτικά τις λειτουργικές μονάδες του προϊόντος ασφάλειας ESET. Εάν δεν ενημερώνονται οι λειτουργικές μονάδες, η Κονσόλα διαδικτύου ESET PROTECT επισημαίνει με σημαία τους υπολογιστές με την ένδειξη **Μη ενημερωμένο**. Για να επιβληθεί σίγαση σε αυτή την προειδοποίηση της Κονσόλας διαδικτύου, κάντε κλικ στον υπολογιστή στη λίστα και επιλέξτε **Σίγαση** από το μενού περιβάλλοντος.

Για οδηγίες σχετικά με την αναβάθμιση του ESET PROTECT On-Prem, δείτε την ενότητα Αναβάθμιση στοιχείων ESET PROTECT σε περιβάλλον εκτός σύνδεσης.

Διαδικασίες αναβάθμισης

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορείτε να αναβαθμίσετε τον διακομιστή ESET PROTECT και άλλα στοιχεία του ESET PROTECT. Δείτε επίσης το θέμα διαδικασίες μετεγκατάστασης και επανεγκατάστασης.

Βεβαιωθείτε ότι έχετε ένα υποστηριζόμενο λειτουργικό σύστημα προτού αναβαθμίσετε στο ESET PROTECT On-Prem 11.0.
Συνιστάται να δημιουργήσετε αντίγραφα ασφαλείας της βάσης δεδομένων ESET PROTECT πριν από την αναβάθμιση.
Εάν έχετε εγκαταστήσει μια παλαιότερη μη υποστηριζόμενη βάση δεδομένων (MySQL 5.5 ή Microsoft SQL 2008/2012), αναβαθμίστε τη βάση δεδομένων σας σε μια συμβατή έκδοση βάσης δεδομένων προτού αναβαθμίσετε το διακομιστή ESET PROTECT.

Αναβάθμιση από ERA 5.x/6.5 ή ESMC 7.x

Μπορείτε να αναβαθμίσετε σε ESET PROTECT On-Prem 11.0 από ESET PROTECT On-Prem 9.0 και νεότερες εκδόσεις. Η απευθείας αναβάθμιση από τις εκδόσεις τέλους του κύκλου ζωής 7.2–8.x δεν έχει δοκιμαστεί και δεν υποστηρίζεται.

Εάν έχετε το ERA 5.x/6.x ή το ESMC 7.0/7.1, η άμεση αναβάθμιση σε ESET PROTECT On-Prem 11.0 δεν υποστηρίζεται – Εκτελέστε μια καθαρή εγκατάσταση του ESET PROTECT On-Prem 11.0.

Αναβάθμιση από παλαιότερη έκδοση του ESET PROTECT On-Prem στο ESET PROTECT On-Prem 11.0

Μπορείτε να αναβαθμίσετε σε ESET PROTECT On-Prem 11.0 από ESET PROTECT On-Prem 9.0 και νεότερες εκδόσεις. Η απευθείας αναβάθμιση από τις εκδόσεις τέλους του κύκλου ζωής 7.2–8.x δεν έχει δοκιμαστεί και δεν υποστηρίζεται.

Επιλέξτε μία από τις διαδικασίες αναβάθμισης:

Διαδικασίες αναβάθμισης	Λειτουργικό σύστημα	Σχόλιο
Εργασία αναβάθμισης στοιχείων στην Κονσόλα διαδικτύου	Windows/Linux	
ESET PROTECT On-Prem 11.0Πρόγραμμα εγκατάστασης "all in one"	Windows	Το Πρόγραμμα εγκατάστασης «Όλα σε ένα» είναι η συνιστώμενη επιλογή αναβάθμισης, εάν η υπάρχουσα εγκατάσταση εκτελέστηκε μέσω του Προγράμματος εγκατάστασης «Όλα σε ένα» (έχετε προεπιλεγμένες εγκαταστάσεις της βάσης δεδομένων Microsoft SQL και του Apache Tomcat).
Μη αυτόματη αναβάθμιση βάσει στοιχείων	Linux	Οδηγίες Linux για προχωρημένους χρήστες.
Αναβάθμιση της εικονικής συσκευής ESET PROTECT	(Εικονική συσκευή) Linux	

Για να αναζητήσετε την έκδοση του κάθε στοιχείου ESET PROTECT που εκτελείται, επαληθεύστε την έκδοση του διακομιστή ESET PROTECT. Μεταβείτε στη σελίδα Σχετικά στην Κονσόλα διαδικτύου ESET PROTECT και δείτε τη λίστα με όλες τις εκδόσεις των στοιχείων του ESET PROTECT.

Εργασία αναβάθμισης στοιχείων ESET PROTECT

Συστάσεις πριν την αναβάθμιση

Για την αναβάθμιση της υποδομής ESET PROTECT, συνιστάται να χρησιμοποιείτε την εργασία ESET PROTECT Αναβάθμιση στοιχείων που διατίθεται στην Κονσόλα διαδικτύου ESET PROTECT. Εξετάστε προσεκτικά τις οδηγίες που παρέχονται εδώ, πριν την αναβάθμιση.

Εάν αποτύχει η αναβάθμιση στοιχείων σε έναν υπολογιστή που εκτελεί το διακομιστή ή την κονσόλα διαδικτύου ESET PROTECT, ενδέχεται να μην μπορείτε να συνδεθείτε απομακρυσμένα με την κονσόλα διαδικτύου. Συνιστάται να διαμορφώσετε τη φυσική πρόσβαση στον υπολογιστή διακομιστή, προτού εκτελέσετε αυτή την αναβάθμιση. Εάν δεν μπορείτε να διευθετήσετε τη φυσική πρόσβαση στον υπολογιστή, βεβαιωθείτε ότι μπορείτε να συνδεθείτε με αυτόν με δικαιώματα διαχείρισης, χρησιμοποιώντας απομακρυσμένη επιφάνεια εργασίας. Συνιστάται να δημιουργήσετε αντίγραφα ασφαλείας των βάσεων δεδομένων του διακομιστή ESET PROTECT και της Σύνδεσης κινητών συσκευών, προτού εκτελέσετε αυτή τη λειτουργία. Για να δημιουργήσετε αντίγραφο ασφαλείας της εικονικής συσκευής σας, δημιουργήστε ένα στιγμιότυπο ή κλώνο του εικονικού υπολογιστή σας.

Κάνετε αναβάθμιση από παλαιότερη έκδοση της εικονικής συσκευής ESET PROTECT;

Η εμφάνιση του διακομιστή ESET PROTECT είναι εγκατεστημένη σε cluster ανακατεύθυνσης;

Εάν η εμφάνιση του διακομιστή ESET PROTECT είναι εγκατεστημένη σε σύμπλεγμα ανακατεύθυνσης, πρέπει να αναβαθμίσετε το στοιχείο διακομιστή ESET PROTECT χειροκίνητα σε κάθε κόμβο του συμπλέγματος. Μετά την αναβάθμιση του διακομιστή ESET PROTECT, εκτελέστε την Εργασία αναβάθμισης στοιχείων για να αναβαθμίσετε την υπόλοιπη υποδομή σας (για παράδειγμα, τους φορείς ESET Management σε υπολογιστές-πελάτες).

Μπορείτε να αναβαθμίσετε σε ESET PROTECT On-Prem 11.0 από ESET PROTECT On-Prem 9.0 και νεότερες εκδόσεις. Η απευθείας αναβάθμιση από τις εκδόσεις τέλους του κύκλου ζωής 7.2–8.x δεν έχει δοκιμαστεί και δεν υποστηρίζεται.
Το ESET PROTECT On-Prem σάς ενημερώνει αυτόματα όταν είναι διαθέσιμη νέα έκδοση του διακομιστή ESET PROTECT.
Δημιουργήστε αντίγραφα ασφαλείας των ακόλουθων δεδομένων προτού εκτελέσετε την αναβάθμιση:
• Όλα τα πιστοποιητικά σας (Αρχή έκδοσης πιστοποιητικών, Πιστοποιητικό διακομιστή, Πιστοποιητικό φορέα)
• Εξαγάγετε τα Πιστοποιητικά Αρχής έκδοσης πιστοποιητικού από έναν παλιό διακομιστή ESET PROTECT σε ένα αρχείο *.der* και αποθηκεύστε σε εξωτερική μνήμη.
• Εξαγάγετε τα Ομότιμα πιστοποιητικά (για το φορέα ESET Management, το διακομιστή ESET PROTECT) και το αρχείο ιδιωτικού κλειδιού *.pfx* από έναν παλιό διακομιστή ESET PROTECT και αποθηκεύστε σε εξωτερική μνήμη.
• Τη βάση δεδομένων ESET PROTECT. Εάν έχετε εγκαταστήσει μια παλαιότερη μη υποστηριζόμενη βάση δεδομένων (MySQL 5.5 ή Microsoft SQL 2008/2012), αναβαθμίστε τη βάση δεδομένων σας σε μια συμβατή έκδοση βάσης δεδομένων προτού αναβαθμίσετε το διακομιστή ESET PROTECT.
Βεβαιωθείτε ότι έχετε ένα υποστηριζόμενο λειτουργικό σύστημα προτού αναβαθμίσετε στο ESET PROTECT On-Prem 11.0.
Για να αναβαθμίσετε τα προϊόντα ασφάλειας ESET, εκτελέστε την Εργασία εγκατάστασης λογισμικού χρησιμοποιώντας το πιο πρόσφατο πακέτο εγκατάστασης για να εγκαταστήσετε την πιο πρόσφατη έκδοση στο υπάρχον προϊόν.

Συνιστώμενη διαδικασία αναβάθμισης

1. Αναβάθμιση του Διακομιστή ESET PROTECT - Επιλέξτε μόνο τον υπολογιστή με το διακομιστή ESET PROTECT ως προορισμό για την εργασία **Αναβάθμιση στοιχείων του ESET PROTECT**.

2. Επιλέξτε ορισμένους υπολογιστές-πελάτες (ως δοκιμαστικό δείγμα - τουλάχιστον έναν υπολογιστή-πελάτη από κάθε λειτουργικό σύστημα και αντιστοιχία bit) και εκτελέστε σε αυτούς την εργασία **Αναβάθμιση στοιχείων του ESET PROTECT**.

Συνιστάται να χρησιμοποιήσετε ESET Bridge Διακομιστή μεσολάβησης HTTP (ή οποιονδήποτε άλλο διάφανο διακομιστή μεσολάβησης διαδικτύου με ενεργοποιημένη προσωρινή μνήμη) για να περιορίσετε το φορτίο του δικτύου. Οι δοκιμαστικοί υπολογιστές-πελάτες θα ενεργοποιήσουν τη λήψη/προσωρινή αποθήκευση των προγραμμάτων εγκατάστασης. Την επόμενη φορά που θα εκτελεστεί η εργασία, τα προγράμματα εγκατάστασης θα διανεμηθούν στους υπολογιστές-πελάτες απευθείας από την προσωρινή μνήμη.

3. Αφού συνδεθούν επιτυχώς οι υπολογιστές με αναβαθμισμένο Φορέα ESET Management στο Διακομιστή ESET PROTECT, προχωρήστε με την αναβάθμιση των υπόλοιπων υπολογιστών-πελατών.

Για να αναβαθμίσετε τους Φορείς ESET Management σε όλους τους διαχειριζόμενους υπολογιστές του δικτύου, επιλέξτε τη στατική ομάδα **Όλα** ως προορισμό για την εργασία **Αναβάθμιση στοιχείων του ESET PROTECT**. Η εργασία θα παραλείψει υπολογιστές που εκτελούν ήδη τον πιο πρόσφατο Φορέα ESET Management.
Το ESET PROTECT On-Prem υποστηρίζει την αυτόματη αναβάθμιση Φορέων ESET Management σε διαχειριζόμενους υπολογιστές.

Στοιχεία που αναβαθμίζονται αυτόματα:

- ESET PROTECTΔιακομιστής

- Φορέας ESET Management

- Κονσόλα διαδικτύου ESET PROTECT - εφαρμόζεται μόνο εάν το Apache Tomcat εγκαταστάθηκε στον προεπιλεγμένο φάκελο εγκατάστασής του τόσο στη διανομή Windows όσο και στη Linux, συμπεριλαμβανομένης της εικονικής συσκευής ESET PROTECT (για παράδειγμα: */var/lib/tomcat8/webapps/*, */var/lib/tomcat7/webapps/*, */var/lib/tomcat/webapps/*).

Περιορισμοί αναβάθμισης της Κονσόλας διαδικτύου

- Το Apache Tomcat δεν αναβαθμίζεται κατά την αναβάθμιση της κονσόλας διαδικτύου ESET PROTECT μέσω της εργασίας «Αναβάθμιση στοιχείων».
- Η αναβάθμιση της κονσόλας διαδικτύου ESET PROTECT δεν λειτουργεί εάν το Apache Tomcat εγκαταστάθηκε σε προσαρμοσμένη τοποθεσία.
- Εάν είναι εγκατεστημένη μια προσαρμοσμένη έκδοση του Apache Tomcat (μη αυτόματη εγκατάσταση της υπηρεσίας Tomcat), δεν υποστηρίζεται η επακόλουθη αναβάθμιση της Κονσόλας διαδικτύου ESET PROTECT μέσω του προγράμματος εγκατάστασης «όλα σε ένα» ή μέσω της εργασίας αναβάθμισης στοιχείων.

- ESET PROTECT Mobile Device Connector

Στοιχεία που απαιτούν μη αυτόματη αναβάθμιση:

Στοιχεία ESET

- ESET Rogue Detection Sensor - Χρησιμοποιήστε την Εργασία εγκατάστασης λογισμικού για την αναβάθμιση. Εναλλακτικά, εγκαταστήστε την πιο πρόσφατη έκδοση σε παλαιότερη έκδοση (ακολουθήστε τις οδηγίες εγκατάστασης για Windows ή Linux). Εάν εγκαταστήσατε τον αισθητήρα RD με μια παλαιότερη έκδοση του ESET PROTECT On-Prem, δεν χρειάζεται να τον αναβαθμίσετε, επειδή δεν υπάρχουν νέες εκδόσεις του αισθητήρα RD.

Στοιχεία τρίτων

Εκτός από τα στοιχεία ESET, το ESET PROTECT On-Prem χρησιμοποιεί στοιχεία άλλων κατασκευαστών που απαιτούν μη αυτόματη αναβάθμιση.

Στην Κονσόλα διαδικτύου ESET PROTECT, κάντε κλικ στο στοιχείο **Γρήγοροι σύνδεσμοι** > **Στοιχεία διακομιστή** για να δείτε στοιχεία άλλων κατασκευαστών για τα οποία υπάρχει διαθέσιμη νεότερη έκδοση.

- Συνιστάται να εγκαταστήσετε την πιο πρόσφατη έκδοση των στοιχείων άλλων κατασκευαστών το συντομότερο δυνατό. Η πιο πρόσφατη διαθέσιμη έκδοση ενδέχεται να διαφέρει ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείται για την εκτέλεση του διακομιστή ESET PROTECT.
- Η εικονική συσκευή ESET PROTECT δεν αναφέρει τις διαθέσιμες αναβαθμίσεις για στοιχεία άλλων κατασκευαστών.

Η Κονσόλα διαδικτύου ESET PROTECT συνιστά αναβάθμιση για εκδόσεις παλαιότερες από αυτές που αναγράφονται παρακάτω:

Στοιχείο τρίτων:	Έκδοση:	Σημειώσεις:	Οδηγίες αναβάθμισης
Microsoft SQL Server	2019 (δομή 15.0.4335.1)	Προσδιορίστε την έκδοση σας και την έκδοση του μηχανισμού βάσης δεδομένων SQL Server και εγκαταστήστε την πιο πρόσφατη αθροιστική ενημέρωση.	Διακομιστής βάσης δεδομένων
MySQL	8.0.0.0	Κάντε κλικ στο στοιχείο **Βοήθεια** > **Σχετικά** στην Κονσόλα διαδικτύου ESET PROTECT για να δείτε την εγκατεστημένη έκδοση της βάσης δεδομένων.	Διακομιστής βάσης δεδομένων
Λειτουργικό σύστημα	Windows Server 2016	Το ESET PROTECT On-Prem δεν αναφέρει τις διαθέσιμες ενημερώσεις για Linux.	Λειτουργικό σύστημα
Apache Tomcat	9.0.82	Προσδιορίστε την εγκατεστημένη έκδοση του Apache Tomcat: • Windows – Μεταβείτε στην ενότητα *C:\Program Files\Apache Software Foundation\[Tomcat* φάκελος *]* και ανοίξτε το αρχείο *RELEASE-NOTES* σε ένα πρόγραμμα επεξεργασίας κειμένου για να ελέγξετε τον αριθμό έκδοσης. • Linux – Εκτελέστε την εντολή τερματικού: `tomcat version`	Apache Tomcat
Java	17.0	Προσδιορίστε την εγκατεστημένη έκδοση του Java: • Windows – Ανοίξτε τη γραμμή εντολών και εκτελέστε το: `java -version` • Linux – Εκτελέστε την εντολή τερματικού: `java -version`	Περιβάλλον χρόνου εκτέλεσης Java
Apache HTTP Proxy	-	**Apache HTTP Proxy χρήστες** Από το ESET PROTECT On-Prem 10.0, το ESET Bridge αντικαθιστά το Apache HTTP Proxy. Το Apache HTTP Proxy έχει φθάσει σε στάδιο περιορισμένης υποστήριξης. Εάν χρησιμοποιείτε το Apache HTTP Proxy, συνιστάται η μετεγκατάσταση σε ESET Bridge.	Μετεγκατάσταση σε ESET Bridge

Το στοιχείο Διαχείριση/Σύνδεση κινητών συσκευών (Διαχείριση κινητών συσκευών/MDC) του ESET PROTECT (μόνο εσωτερικής εγκατάστασης) φτάνει στο τέλος του κύκλου ζωής τον Ιανουάριο του 2024. Διαβάστε περισσότερα. Συνιστάται η μετεγκατάσταση στο cloud διαχείρισης κινητών συσκευών.

Αντιμετώπιση προβλημάτων

• Επαληθεύστε ότι μπορείτε να αποκτήσετε πρόσβαση στο χώρο αποθήκευσης ESET PROTECT On-Prem από έναν αναβαθμισμένο υπολογιστή.

• Εάν υπάρχει τουλάχιστον ένα στοιχείο που έχει ήδη αναβαθμιστεί στη νεότερη έκδοση, η επανεκτέλεση της εργασίας αναβάθμισης στοιχείων του ESET PROTECT δεν θα λειτουργήσει.

• Εάν η Κονσόλα διαδικτύου ESET PROTECT δεν φορτώνεται ή εμφανίζεται σφάλμα κατά τη

σύνδεση, δείτε το θέμα Αντιμετώπιση προβλημάτων της Κονσόλας διαδικτύου.

• Εάν δεν υπάρχει σαφής λόγος για την αποτυχία ενημέρωσης, αναβαθμίστε τα στοιχεία μη αυτόματα. Δείτε τις οδηγίες για Windows ή Linux.

• Ανατρέξτε στις γενικές πληροφορίες αντιμετώπισης προβλημάτων για περισσότερες προτάσεις επίλυσης ζητημάτων αναβάθμισης.

Για την αναβάθμιση, χρησιμοποιήστε το πρόγραμμα εγκατάστασης «Όλα σε ένα» του ESET PROTECT On-Prem 11.0

Χρησιμοποιήστε το πρόγραμμα εγκατάστασης «Όλα σε ένα» του ESET PROTECT On-Prem 11.0 για να αναβαθμίσετε μια παλαιότερη έκδοση του ESET PROTECT On-Prem στην πιο πρόσφατη έκδοση του ESET PROTECT On-Prem 11.0.

Το Πρόγραμμα εγκατάστασης «Όλα σε ένα» είναι η συνιστώμενη επιλογή αναβάθμισης, εάν η υπάρχουσα εγκατάσταση εκτελέστηκε μέσω του Προγράμματος εγκατάστασης «Όλα σε ένα» (έχετε προεπιλεγμένες εγκαταστάσεις της βάσης δεδομένων Microsoft SQL και του Apache Tomcat).

ESET PROTECT On-Prem 11.0 Το πρόγραμμα εγκατάστασης «όλα σε ένα» εγκαθιστά το Microsoft SQL Server Express 2019 από προεπιλογή.

oΕάν χρησιμοποιείτε μια παλαιότερη έκδοση των Windows (Server 2012 ή SBS 2011), το Microsoft SQL Server Express 2014 θα εγκατασταθεί από προεπιλογή.

oΤο πρόγραμμα εγκατάστασης δημιουργεί αυτόματα έναν τυχαίο κωδικό πρόσβασης για τον έλεγχο ταυτότητας της βάσης δεδομένων (που είναι αποθηκευμένη στη διαδρομή *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

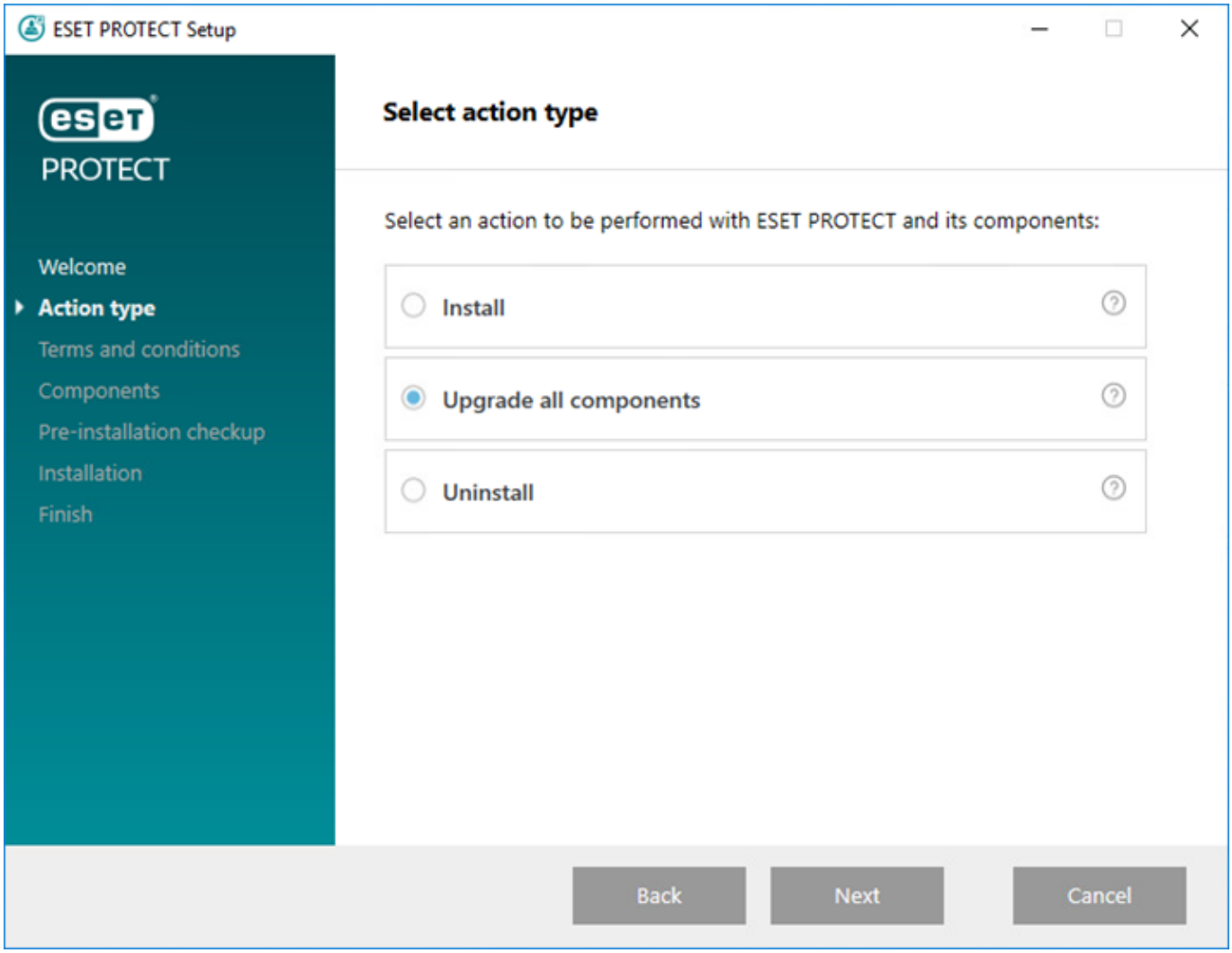
⚠ Το Microsoft SQL Server Express έχει όριο μεγέθους 10 GB για κάθε σχετική βάση δεδομένων. Δεν συνιστάται η χρήση του Microsoft SQL Server Express:
- Σε εταιρικά περιβάλλοντα ή μεγάλα δίκτυα.
- Εάν θέλετε να χρησιμοποιήσετε το ESET PROTECT On-Prem με το ESET Inspect On-Prem.

Μπορείτε να αναβαθμίσετε σε ESET PROTECT On-Prem 11.0 από ESET PROTECT On-Prem 9.0 και νεότερες εκδόσεις. Η απευθείας αναβάθμιση από τις εκδόσεις τέλους του κύκλου ζωής 7.2–8.x δεν έχει δοκιμαστεί και δεν υποστηρίζεται.
Δημιουργήστε αντίγραφα ασφαλείας των ακόλουθων δεδομένων προτού εκτελέσετε την αναβάθμιση:
• Όλα τα πιστοποιητικά σας (Αρχή έκδοσης πιστοποιητικών, Πιστοποιητικό διακομιστή, Πιστοποιητικό φορέα)
• Εξαγάγετε τα Πιστοποιητικά Αρχής έκδοσης πιστοποιητικού από έναν παλιό διακομιστή ESET PROTECT σε ένα αρχείο *.der* και αποθηκεύστε σε εξωτερική μνήμη.
• Εξαγάγετε τα Ομότιμα πιστοποιητικά (για το φορέα ESET Management, το διακομιστή ESET PROTECT) και το αρχείο ιδιωτικού κλειδιού *.pfx* από έναν παλιό διακομιστή ESET PROTECT και αποθηκεύστε σε εξωτερική μνήμη.
• Τη βάση δεδομένων ESET PROTECT. Εάν έχετε εγκαταστήσει μια παλαιότερη μη υποστηριζόμενη βάση δεδομένων (MySQL 5.5 ή Microsoft SQL 2008/2012), αναβαθμίστε τη βάση δεδομένων σας σε μια συμβατή έκδοση βάσης δεδομένων προτού αναβαθμίσετε το διακομιστή ESET PROTECT.
Βεβαιωθείτε ότι έχετε ένα υποστηριζόμενο λειτουργικό σύστημα προτού αναβαθμίσετε στο ESET PROTECT On-Prem 11.0.

1.Εκτελέστε το αρχείο *Setup.exe*.

2.Επιλέξτε τη γλώσσα και κάντε κλικ στο στοιχείο **Επόμενο**.

3.Επιλέξτε **Αναβάθμιση όλων των στοιχείων** και κάντε κλικ στο στοιχείο **Επόμενο**.



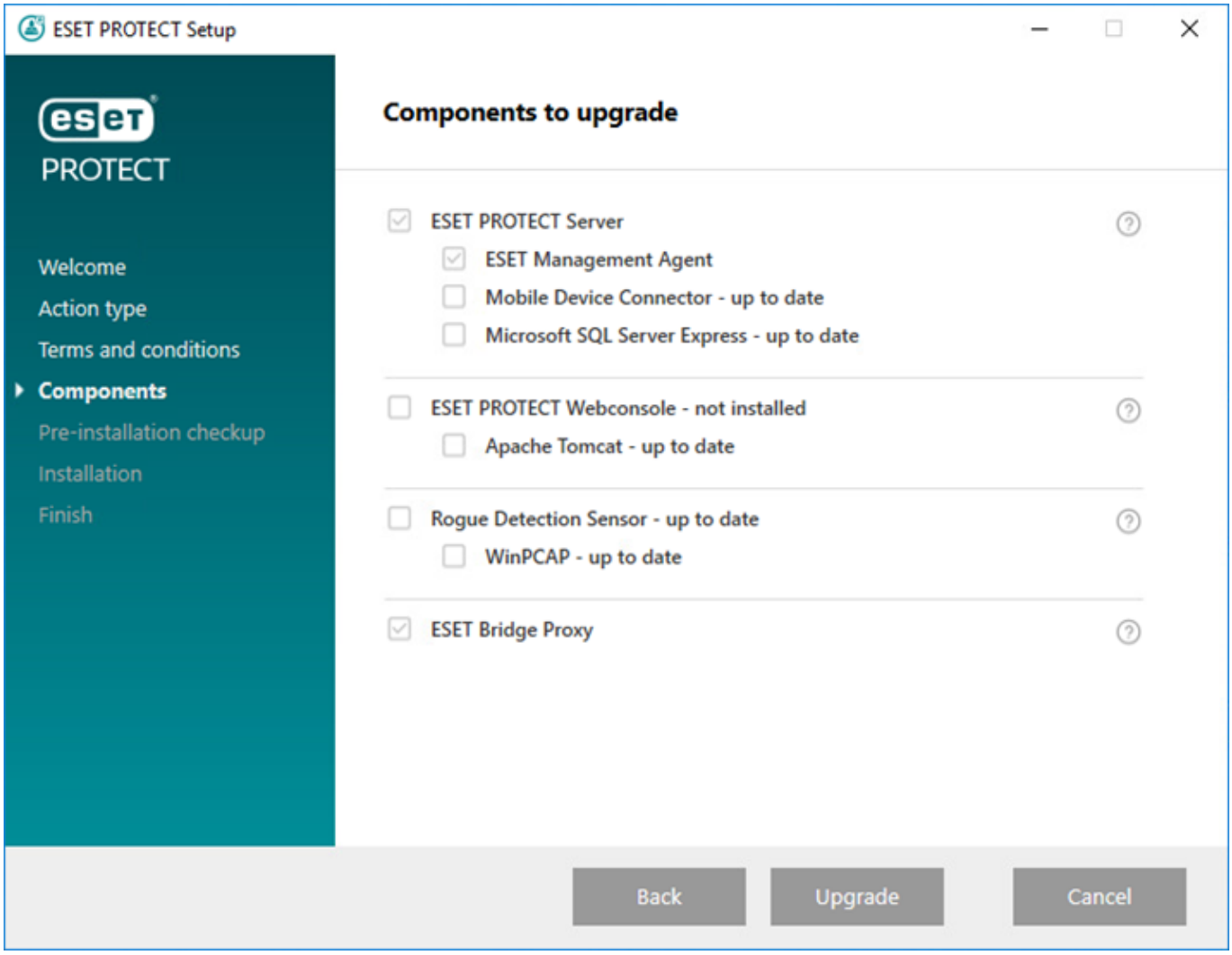
4.Διαβάστε τη **Συμφωνία Άδειας Χρήσης Τελικού Χρήστη**, αποδεχτείτε την και κάντε κλικ στο στοιχείο **Επόμενο**.

5.Στα **Στοιχεία**, αναθεωρήστε τα στοιχεία του ESET PROTECT που μπορούν να αναβαθμιστούν και κάντε κλικ στο στοιχείο **Επόμενο**.

Περιορισμοί αναβάθμισης του Apache Tomcat και της Κονσόλας διαδικτύου

- Εάν είναι εγκατεστημένη μια προσαρμοσμένη έκδοση του Apache Tomcat (μη αυτόματη εγκατάσταση της υπηρεσίας Tomcat), δεν υποστηρίζεται η επακόλουθη αναβάθμιση της Κονσόλας διαδικτύου ESET PROTECT μέσω του προγράμματος εγκατάστασης «όλα σε ένα» ή μέσω της εργασίας αναβάθμισης στοιχείων.
- Η αναβάθμιση του Apache Tomcat θα καταργήσει το φάκελο *era* που βρίσκεται στο *C:\Program Files\Apache Software Foundation\[Tomcat* φάκελος *]\webapps*. Εάν χρησιμοποιείτε το φάκελο *era* για να αποθηκεύετε πρόσθετα δεδομένα, βεβαιωθείτε ότι έχετε δημιουργήσει αντίγραφα ασφαλείας των δεδομένων πριν την αναβάθμιση.
- Εάν χρησιμοποιηθεί η επιλογή « *C:\Program Files\Apache Software Foundation\[Tomcat* φάκελος *]\webapps* περιέχει πρόσθετα δεδομένα (εκτός από το *era* και τους φακέλους *ROOT*), η αναβάθμιση Apache Tomcat δεν θα πραγματοποιηθεί και θα αναβαθμιστεί μόνο η κονσόλα διαδικτύου.
- Η αναβάθμιση της Κονσόλας διαδικτύου και του Apache Tomcat εκκαθαρίζει τα αρχεία βοήθειας εκτός σύνδεσης. Εάν χρησιμοποιήσατε βοήθεια εκτός σύνδεσης με μια παλαιότερη έκδοση του ESET PROTECT On-Prem, δημιουργήστε την ξανά για το ESET PROTECT On-Prem 11.0 μετά την αναβάθμιση, για να διασφαλίσετε ότι έχετε την πιο πρόσφατη βοήθεια εκτός σύνδεσης που αντιστοιχεί στην έκδοση του ESET PROTECT On-Prem που διαθέτετε.

Εάν εκτελέσετε το πρόγραμμα εγκατάστασης «Όλα σε ένα» σε έναν υπολογιστή Windows στον οποίο έχει εγκατασταθεί το Apache HTTP Proxy, το πρόγραμμα εγκατάστασης θα καταργήσει την εγκατάσταση του Apache HTTP Proxy αυτόματα και θα εγκαταστήσει το ESET Bridge.



6.Ακολουθήστε το στοιχείο **Έλεγχος πριν από την εγκατάσταση** για να βεβαιωθείτε ότι το σύστημά σας πληροί όλα τα προαπαιτούμενα.

7.Κάντε κλικ στο στοιχείο **Αναβάθμιση** για να ξεκινήσετε την αναβάθμιση του ESET PROTECT On-Prem. Η αναβάθμιση ενδέχεται να διαρκέσει κάποιο χρονικό διάστημα, ανάλογα με το σύστημα και τη ρύθμιση παραμέτρων του δικτύου σας.

8.Όταν ολοκληρωθεί η αναβάθμιση, κάντε κλικ στο στοιχείο **Τέλος**.

Εάν η Κονσόλα διαδικτύου ESET PROTECT δεν φορτώνεται ή εμφανίζεται σφάλμα κατά τη σύνδεση, δείτε το θέμα Αντιμετώπιση προβλημάτων της Κονσόλας διαδικτύου.

Μετά την αναβάθμιση του ESET PROTECT On-Prem, αναβαθμίστε τον Φορέα ESET Management στους διαχειριζόμενους υπολογιστές χρησιμοποιώντας την Εργασία αναβάθμισης στοιχείων. Το ESET PROTECT On-Prem υποστηρίζει την αυτόματη αναβάθμιση Φορέων ESET Management σε διαχειριζόμενους υπολογιστές.

Δημιουργία αντιγράφων ασφαλείας/αναβάθμιση διακομιστή βάσης

δεδομένων

Το ESET PROTECT On-Prem χρησιμοποιεί μια βάση δεδομένων για την αποθήκευση των δεδομένων υπολογιστών-πελατών. Στα ακόλουθα κεφάλαια περιγράφεται η δημιουργία αντιγράφων ασφαλείας και η αναβάθμιση του διακομιστή ESET PROTECT ή της βάσης δεδομένων MDM:

- Εάν δεν έχετε διαμορφώσει μια βάση δεδομένων για χρήση με το διακομιστή ESET PROTECT, το **Microsoft SQL Server Express** συμπεριλαμβάνεται στο πρόγραμμα εγκατάστασης. ESET PROTECT On-Prem 11.0 Το πρόγραμμα εγκατάστασης «όλα σε ένα» εγκαθιστά το Microsoft SQL Server Express 2019 από προεπιλογή.

  οΕάν χρησιμοποιείτε μια παλαιότερη έκδοση των Windows (Server 2012 ή SBS 2011), το Microsoft SQL Server Express 2014 θα εγκατασταθεί από προεπιλογή.

  οΤο πρόγραμμα εγκατάστασης δημιουργεί αυτόματα έναν τυχαίο κωδικό πρόσβασης για τον έλεγχο ταυτότητας της βάσης δεδομένων (που είναι αποθηκευμένη στη διαδρομή *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

> ⚠ Το Microsoft SQL Server Express έχει όριο μεγέθους 10 GB για κάθε σχετική βάση δεδομένων. Δεν συνιστάται η χρήση του Microsoft SQL Server Express:
> - Σε εταιρικά περιβάλλοντα ή μεγάλα δίκτυα.
> - Εάν θέλετε να χρησιμοποιήσετε το ESET PROTECT On-Prem με το ESET Inspect On-Prem.

- Εάν έχετε εγκαταστήσει μια παλαιότερη μη υποστηριζόμενη βάση δεδομένων (MySQL 5.5 ή Microsoft SQL 2008/2012), αναβαθμίστε τη βάση δεδομένων σας σε μια συμβατή έκδοση βάσης δεδομένων προτού αναβαθμίσετε το διακομιστή ESET PROTECT.

Δείτε επίσης το θέμα Μετεγκατάσταση της βάσης δεδομένων του ESET PROTECT.

Πρέπει να ικανοποιούνται οι ακόλουθες απαιτήσεις για το Microsoft SQL Server:

- Εγκαταστήστε μια υποστηριζόμενη έκδοση του Microsoft SQL Server. Κατά την εγκατάσταση, επιλέξτε έλεγχο ταυτότητας με **Μεικτή λειτουργία**.

- Εάν είναι ήδη εγκατεστημένο το Microsoft SQL Server, ρυθμίστε τον έλεγχο ταυτότητας σε **Μεικτή λειτουργία (Έλεγχος ταυτότητας SQL Server και έλεγχος ταυτότητας Windows)**. Για να το κάνετε αυτό, ακολουθήστε τις οδηγίες σε αυτό το άρθρο της Γνωσιακής βάσης. Εάν θέλετε να χρησιμοποιείται ο **Έλεγχος ταυτότητας Windows** για τη σύνδεση στο Microsoft SQL Server, ακολουθήστε τα βήματα σε αυτό το άρθρο της Γνωσιακής βάσης.

- Θα πρέπει να επιτρέπονται συνδέσεις TCP/IP με το SQL Server. Για να το κάνετε αυτό, ακολουθήστε τις οδηγίες σε αυτό το άρθρο της Γνωσιακής βάσης από το μέρος **II. Να επιτρέπονται συνδέσεις TCP/IP με τη βάση δεδομένων SQL**.

- Για τη ρύθμιση παραμέτρων, διαχείριση και διανομή του Microsoft SQL Server (βάσεις δεδομένων και χρήστες), πραγματοποιήστε λήψη του SQL Server Management Studio (SSMS).
- Μην εγκαταστήσετε το SQL Server σε έναν Ελεγκτή τομέα (για παράδειγμα, Windows SBS / Essentials). Συνιστάται να εγκαταστήσετε το ESET PROTECT On-Prem σε διαφορετικό διακομιστή ή να μην επιλέξετε το στοιχείο του SQL Server Express κατά την εγκατάσταση (αυτό απαιτεί να χρησιμοποιήσετε το υπάρχον SQL ή MySQL Server για την εκτέλεση της βάσης δεδομένων ESET PROTECT).

Δημιουργία αντιγράφων ασφαλείας και επαναφορά του διακομιστή βάσης δεδομένων

Όλες οι πληροφορίες και οι ρυθμίσεις του ESET PROTECT On-Prem αποθηκεύονται στη βάση δεδομένων. Συνιστάται να δημιουργείτε τακτικά αντίγραφα ασφαλείας της βάσης δεδομένων για να αποτρέπεται η απώλεια δεδομένων. Μπορείτε να χρησιμοποιήσετε το αντίγραφο ασφαλείας αργότερα κατά τη μετεγκατάσταση του ESET PROTECT On-Prem σε έναν νέο διακομιστή. Ανατρέξτε παρακάτω στην κατάλληλη ενότητα για τη βάση δεδομένων σας:

- Τα ονόματα των βάσεων δεδομένων και των αρχείων καταγραφής παραμένουν ίδια, ακόμα και μετά την αλλαγή του ονόματος του προϊόντος από ESET Security Management Center σε ESET PROTECT On-Prem.
- Εάν χρησιμοποιείτε εικονική συσκευή ESET PROTECT, ακολουθήστε τις οδηγίες δημιουργίας αντιγράφων ασφαλείας της βάσης δεδομένων εικονικής συσκευής.

Παραδείγματα δημιουργίας αντιγράφων ασφαλείας Microsoft SQL

Για να δημιουργήσετε αντίγραφο ασφαλείας για μια βάση δεδομένων Microsoft SQL σε ένα αρχείο, ακολουθήστε το παρακάτω παράδειγμα:

Αυτά τα παραδείγματα προορίζονται για χρήση με τις προεπιλεγμένες ρυθμίσεις (για παράδειγμα, προεπιλεγμένο όνομα και προεπιλεγμένες ρυθμίσεις σύνδεσης της βάσης δεδομένων). Η δέσμη ενεργειών του αντιγράφου ασφαλείας σας θα πρέπει να προσαρμοστεί ώστε να αντικατοπτρίζει τυχόν αλλαγές που έχετε πραγματοποιήσει στις προεπιλεγμένες ρυθμίσεις.
Πρέπει να έχετε επαρκή δικαιώματα για να εκτελέσετε τις παρακάτω εντολές. Εάν δεν χρησιμοποιείτε έναν τοπικό λογαριασμό χρήστη διαχειριστή, πρέπει να αλλάξετε τη διαδρομή του αντιγράφου ασφαλείας, για παράδειγμα σε *'C:\USERS\PUBLIC\BACKUPFILE'*.

Αντίγραφο ασφαλείας βάσης δεδομένων μίας χρήσης

Εκτελέστε αυτή την εντολή σε μια γραμμή εντολών των Windows για να δημιουργήσετε αντίγραφο ασφαλείας σε ένα αρχείο με το όνομα **BACKUPFILE**:

```
SQLCMD -S HOST\ERASQL -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

Σε αυτό το παράδειγμα, η παράμετρος **HOST** δηλώνει τη διεύθυνση IP ή το όνομα κεντρικού υπολογιστή, ενώ η παράμετρος **ERASQL** δηλώνει το όνομα της εμφάνισης του διακομιστή Microsoft SQL. Μπορείτε να εγκαταστήστε τον διακομιστή ESET PROTECT σε μια παρουσία SQL με προσαρμοσμένο όνομα (όταν χρησιμοποιείται βάση δεδομένων Microsoft SQL). Τροποποιήστε τις δέσμες ενεργειών αντιγράφου ασφαλείας σε αυτό το σενάριο.

Τακτικό αντίγραφο ασφαλείας βάσης δεδομένων με δέσμη ενεργειών SQL

Επιλέξτε μία από τις παρακάτω δέσμες ενεργειών SQL:

a)Δημιουργήστε τακτικά αντίγραφα ασφαλείας και αποθηκεύστε τα με βάση την ημερομηνία δημιουργίας τους:

```
@ECHO OFF


SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

  WITH NOFORMAT,INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHE
CKSUM, STATS=10"


REN BACKUPFILE BACKUPFILE-
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b)Επισυνάψτε το αντίγραφο ασφαλείας σε ένα αρχείο:

```
@ECHO OFF


SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

   WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR,
 CHECKSUM, STATS=10"
```

Επαναφορά του Microsoft SQL

Για να επαναφέρετε μια βάση δεδομένων Microsoft SQL από ένα αρχείο, ακολουθήστε το παρακάτω παράδειγμα:

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

Αντίγραφο ασφαλείας MySQL

Για να δημιουργήσετε αντίγραφο ασφαλείας για μια βάση δεδομένων MySQL σε ένα αρχείο,

ακολουθήστε το παρακάτω παράδειγμα:

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -
p DBNAME -r BACKUPFILE
```

Σε αυτό το παράδειγμα, η παράμετρος **HOST** δηλώνει τη διεύθυνση IP ή το όνομα κεντρικού υπολογιστή του διακομιστή MySQL, η παράμετρος **ROOTLOGIN** δηλώνει το λογαριασμό ρίζας του διακομιστή MySQL και η παράμετρος **DBNAME** δηλώνει το όνομα της βάσης δεδομένων ESET PROTECT.

Επαναφορά MySQL

Για να επαναφέρετε μια βάση δεδομένων MySQL από ένα αρχείο, ακολουθήστε το παρακάτω παράδειγμα:

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

Για περισσότερες πληροφορίες σχετικά με τη δημιουργία αντιγράφων ασφαλείας του Microsoft SQL Server, επισκεφτείτε τον ιστότοπο Microsoft technet. Για περισσότερες πληροφορίες σχετικά με τη δημιουργία αντιγράφων ασφαλείας του MySQL Server, επισκεφτείτε τον ιστότοπο τεκμηρίωσης του MySQL.

Αναβάθμιση διακομιστή βάσης δεδομένων

Ακολουθήστε τις οδηγίες παρακάτω για να αναβαθμίσετε μια υπάρχουσα παρουσία του διακομιστή βάσης δεδομένων σε νεότερη έκδοση για χρήση με τη βάση δεδομένων του διακομιστή ESET PROTECT:

1. Διακοπή όλων των υπηρεσιών διακομιστή ESET PROTECT που εκτελούνται για τη σύνδεση με το διακομιστή βάσης δεδομένων τον οποίο θα αναβαθμίσετε. Επιπρόσθετα, διακόψτε οποιεσδήποτε άλλες εφαρμογές που μπορεί να συνδέονται με την παρουσία του διακομιστή της βάσης δεδομένων.

2. Δημιουργήστε αντίγραφα ασφαλείας όλων των σχετικών βάσεων δεδομένων, προτού προχωρήσετε.

3. Εκτελέστε την αναβάθμιση του διακομιστή βάσης δεδομένων:

SQL Server (Windows):

- Ακολουθήστε το άρθρο της Γνωσιακής βάσης για την αναβάθμιση της βάσης δεδομένων Microsoft SQL Express στην πιο πρόσφατη έκδοση.
- Εναλλακτικά, ακολουθώντας τις οδηγίες του κατασκευαστή της βάσης δεδομένων: https://msdn.microsoft.com/en-us/library/bb677622.aspx.
- Το Microsoft SQL Server σε Linux δεν υποστηρίζεται. Ωστόσο, μπορείτε να συνδέσετε το διακομιστή ESET PROTECT σε Linux με το Microsoft SQL Server σε Windows.

MySQL Server (Windows και Linux):

- Αναβάθμιση από MySQL 5.6 στην έκδοση 5.7
- Αναβάθμιση από MySQL 5.7 στην έκδοση 8

4. Έναρξη όλων των υπηρεσιών διακομιστή ESET PROTECT και έλεγχος των αρχείων καταγραφής παρακολούθησης για να επαληθεύσετε επαληθευτεί ότι λειτουργεί σωστά η σύνδεση της βάσης δεδομένων.

Αναβάθμιση του ESET PROTECT On-Prem που έχει εγκατασταθεί σε Σύμπλεγμα ανακατεύθυνσης σε Windows

Εάν ο Διακομιστής ESET PROTECT έχει εγκατασταθεί σε περιβάλλον συμπλέγματος ανακατεύθυνσης σε Windows, ακολουθήστε τα παρακάτω βήματα για να αναβαθμίσετε στην πιο πρόσφατη έκδοση του ESET PROTECT On-Prem:

Βεβαιωθείτε ότι έχετε ένα υποστηριζόμενο λειτουργικό σύστημα.

1. Διακόψτε το ρόλο συμπλέγματος του διακομιστή ESET PROTECT στη Διαχείριση συμπλέγματος. Βεβαιωθείτε ότι η υπηρεσία (**ESET Security Management Center Server** ή **ESET PROTECT Server**) έχει διακοπεί σε όλους τους κόμβους του cluster.

2. Μεταφέρετε τον κοινόχρηστο δίσκο του cluster στον κόμβο 1 και αναβαθμίστε το στοιχείο Διακομιστή μη αυτόματα εκτελώντας το πιο πρόσφατο πρόγραμμα εγκατάστασης *.msi*, όπως στην περίπτωση της εγκατάστασης στοιχείου.

3. Μόλις ολοκληρωθεί η εγκατάσταση (αναβάθμιση), βεβαιωθείτε ότι η υπηρεσία **ESET PROTECT Server** έχει διακοπεί.

4. Μεταφέρετε τον κοινόχρηστο δίσκο του cluster στον κόμβο 2 και αναβαθμίστε το στοιχείο Διακομιστή με τον ίδιο τρόπο όπως στο βήμα 2.

5. Μόλις ενημερωθεί ο διακομιστής ESET PROTECT σε όλους τους κόμβους του συμπλέγματος, **ξεκινήστε το ρόλο διακομιστή ESET PROTECT** στη Διαχείριση συμπλέγματος.

6. Αναβαθμίστε το φορέα ESET Management μη αυτόματα εκτελώντας το πιο πρόσφατο πρόγραμμα εγκατάστασης *.msi* σε όλους του κόμβους του συμπλέγματος.

7. Στην κονσόλα διαδικτύου ESET PROTECT ελέγξτε εάν οι εκδόσεις φορέα και διακομιστή για όλους τους κόμβους αναφέρουν την πιο πρόσφατη έκδοση στην οποία κάνατε αναβάθμιση.

Αναβάθμιση του Apache Tomcat

το Apache Tomcat είναι απαραίτητο στοιχείο για τη λειτουργία της Κονσόλας διαδικτύου ESET PROTECT.

Εάν κάνετε αναβάθμιση σε μια πιο πρόσφατη έκδοση του ESET PROTECT On-Prem, ή εάν δεν έχετε αναβαθμίσει το Apache Tomcat για μεγάλη χρονικπη περίοδο, θα πρέπει να εξετάσετε το ενδεχόμενο

να αναβαθμίσετε το Apache Tomcat στην πιο πρόσφατη έκδοση. Η συνεχής ενημέρωση των δημόσιων υπηρεσιών, συμπεριλαμβανομένου του Apache Tomcat και των εξαρτήσεών του μειώνει τους κινδύνους ασφαλείας στο περιβάλλον σας.

Για να αναβαθμίσετε το Apache Tomcat, ακολουθήστε τις οδηγίες:

- Οδηγίες των Windows (το πιο πρόσφατο Πρόγραμμα εγκατάστασης «Όλα σε ένα» ESET PROTECT) - Αυτή είναι η συνιστώμενη επιλογή αναβάθμισης, εάν η υπάρχουσα εγκατάσταση του Apache Tomcat εκτελέστηκε μέσω του Προγράμματος εγκατάστασης «Όλα σε ένα».

- Οδηγίες για Windows (μη αυτόματα εγκατάσταση) - Αναβαθμίστε το Apache Tomcat μη αυτόματα εάν εκτελέσατε την υπάρχουσα εγκατάσταση του Apache Tomcat μη αυτόματα ή εάν δεν έχετε το πιο πρόσφατο Πρόγραμμα εγκατάστασης «Όλα σε ένα» του ESET PROTECT.

- Οδηγίες για Linux

Αναβάθμιση του Apache Tomcat χρησιμοποιώντας το Πρόγραμμα εγκατάστασης «όλα-σε-ένα» (Windows)

το Apache Tomcat είναι απαραίτητο στοιχείο για τη λειτουργία της Κονσόλας διαδικτύου ESET PROTECT. Χρησιμοποιήστε αυτήν τη μέθοδο για να αναβαθμίσετε το Apache Tomcat χρησιμοποιώντας το πιο πρόσφατο Πρόγραμμα εγκατάστασης «Όλα σε ένα» ESET PROTECT On-Prem 11.0. Αυτή είναι η συνιστώμενη επιλογή αναβάθμισης, εάν η υπάρχουσα εγκατάσταση του Apache Tomcat εκτελέστηκε μέσω του Προγράμματος εγκατάστασης «Όλα σε ένα». Εναλλακτικά, μπορείτε να κάνετε αναβάθμιση του Apache Tomcat μη αυτόματα.

Πριν από την αναβάθμιση

Δημιουργήστε αντίγραφα ασφαλείας για τα παρακάτω αρχεία:

C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]\.keystore*
C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]\conf\server.xml*
C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*

Εάν χρησιμοποιείτε προσαρμοσμένο χώρο αποθήκευσης πιστοποιητικών SSL στο φάκελο *Tomcat*, δημιουργήστε αντίγραφο ασφαλείας και για το πιστοποιητικό.

Περιορισμοί αναβάθμισης του Apache Tomcat και της Κονσόλας διαδικτύου

- Εάν είναι εγκατεστημένη μια προσαρμοσμένη έκδοση του Apache Tomcat (μη αυτόματη εγκατάσταση της υπηρεσίας Tomcat), δεν υποστηρίζεται η επακόλουθη αναβάθμιση της Κονσόλας διαδικτύου ESET PROTECT μέσω του προγράμματος εγκατάστασης «όλα σε ένα» ή μέσω της εργασίας αναβάθμισης στοιχείων.
- Η αναβάθμιση του Apache Tomcat θα καταργήσει το φάκελο *era* που βρίσκεται στο *C:\Program Files\Apache Software Foundation\[Tomcat* φάκελος *]\webapps*. Εάν χρησιμοποιείτε το φάκελο *era* για να αποθηκεύετε πρόσθετα δεδομένα, βεβαιωθείτε ότι έχετε δημιουργήσει αντίγραφα ασφαλείας των δεδομένων πριν την αναβάθμιση.
- Εάν χρησιμοποιηθεί η επιλογή « *C:\Program Files\Apache Software Foundation\[Tomcat* φάκελος *]\webapps* περιέχει πρόσθετα δεδομένα (εκτός από το *era* και τους φακέλους *ROOT*), η αναβάθμιση Apache Tomcat δεν θα πραγματοποιηθεί και θα αναβαθμιστεί μόνο η κονσόλα διαδικτύου.
- Η αναβάθμιση της Κονσόλας διαδικτύου και του Apache Tomcat εκκαθαρίζει τα αρχεία βοήθειας εκτός σύνδεσης. Εάν χρησιμοποιήσατε βοήθεια εκτός σύνδεσης με μια παλαιότερη έκδοση του ESET PROTECT On-Prem, δημιουργήστε την ξανά για το ESET PROTECT On-Prem 11.0 μετά την αναβάθμιση, για να διασφαλίσετε ότι έχετε την πιο πρόσφατη βοήθεια εκτός σύνδεσης που αντιστοιχεί στην έκδοση του ESET PROTECT On-Prem που διαθέτετε.

Διαδικασίες αναβάθμισης

1. Πραγματοποιήστε λήψη του προγράμματος εγκατάστασης «όλα σε ένα» του ESET PROTECT από τον ιστότοπο της ESET και αποσυμπιέστε το αρχείο λήψης.

2. Εάν θέλετε να εγκαταστήσετε την πιο πρόσφατη έκδοση του Apache Tomcat και το πρόγραμμα εγκατάστασης «όλα σε ένα» περιέχει μια παλαιότερη έκδοση του Apache Tomcat (αυτό το βήμα είναι προαιρετικό - προχωρήστε στο βήμα 4, εάν δεν χρειάζεστε την πιο πρόσφατη έκδοση του Apache Tomcat):

   a. Ανοίξτε το φάκελο *x64* και μεταβείτε στο φάκελο *installers*.

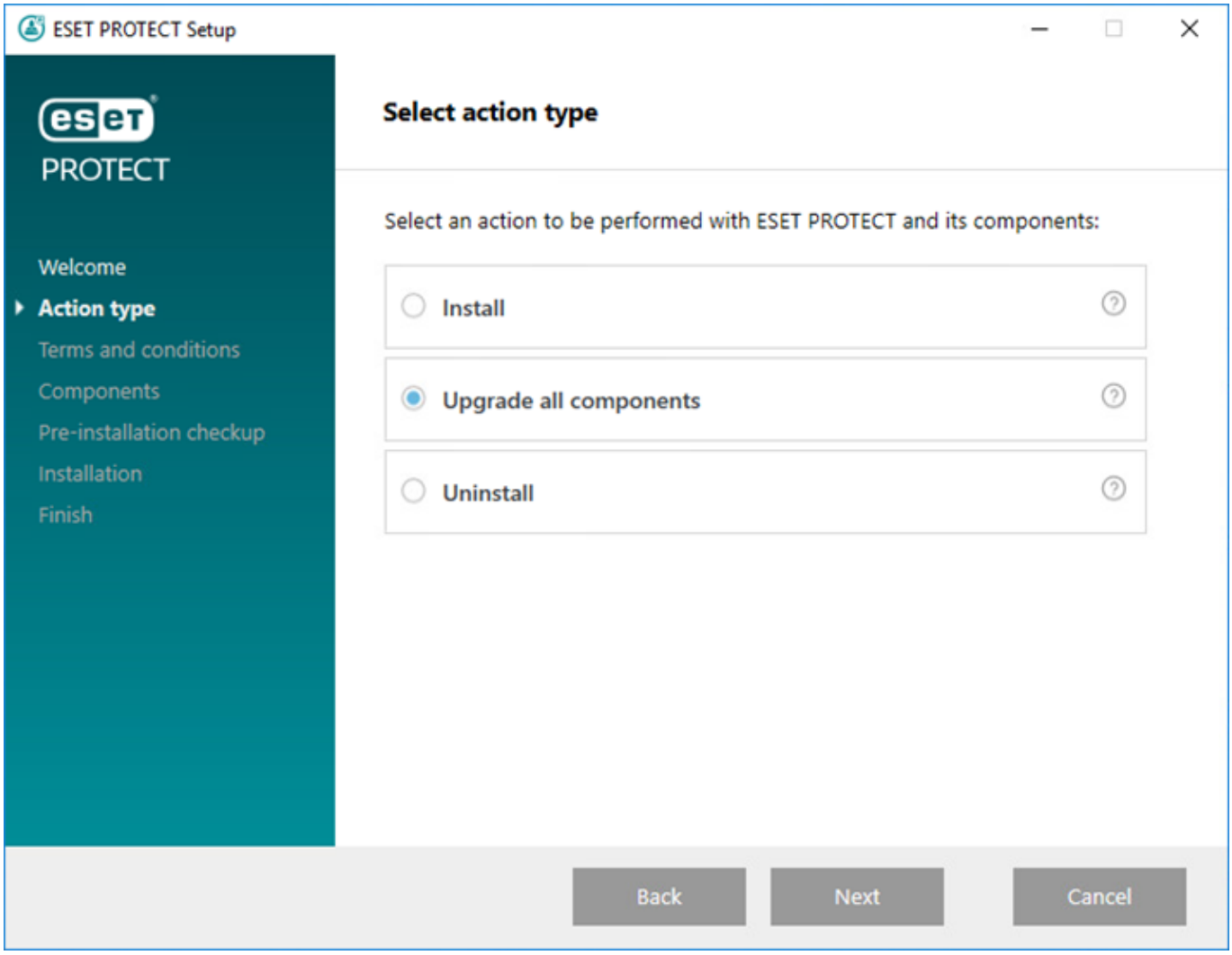
   b. Καταργήστε το αρχείο *apache-tomcat-9.0.x-windows-x64.zip* που βρίσκεται στο φάκελο *installers*.

   c. Πραγματοποιήστε λήψη του συμπιεσμένου πακέτου Apache Tomcat 9 για Windows 64 bit.

   d. Μετακινήστε το συμπιεσμένο πακέτο λήψης στο φάκελο *installers*.

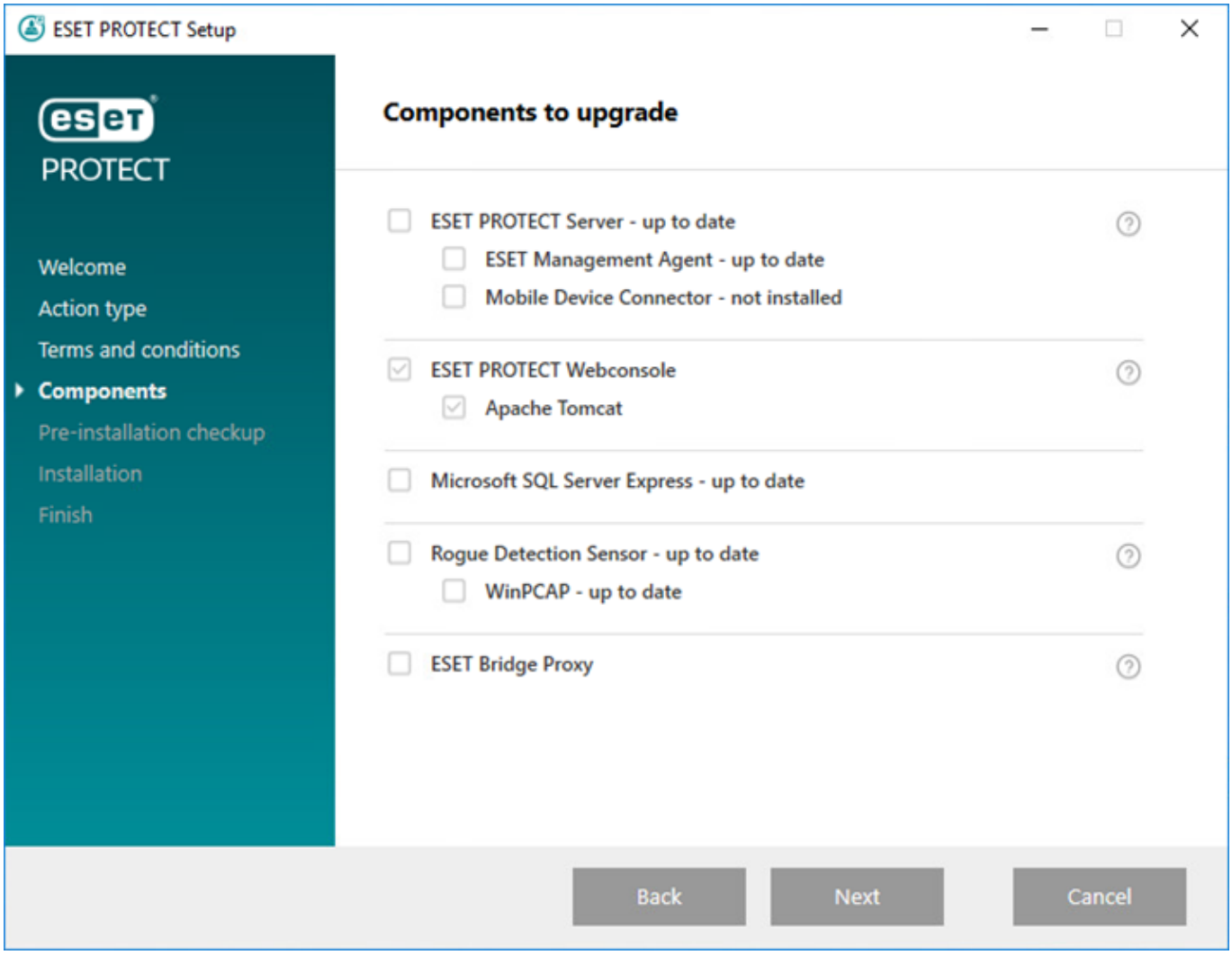
3. Για να εκκινήσετε το πρόγραμμα εγκατάστασης «όλα σε ένα», κάντε διπλό κλικ στο αρχείο *Setup.exe* και κάντε κλικ στο στοιχείο **Επόμενο** στην οθόνη **Υποδοχή**.

4. Επιλέξτε **Αναβάθμιση όλων των στοιχείων** και κάντε κλικ στο στοιχείο **Επόμενο**.



5. Αφού αποδεχτείτε την Άδεια Χρήσης Τελικού Χρήστη (EULA), επιλέξτε **Επόμενο**.

6. Το Πρόγραμμα εγκατάστασης «όλα-σε-ένα» ανιχνεύει αυτόματα εάν είναι διαθέσιμη η αναβάθμιση: υπάρχουν πλαίσια ελέγχου δίπλα στα στοιχεία του ESET PROTECT που μπορούν να αναβαθμιστούν. Κάντε κλικ στο στοιχείο**Επόμενο**.



7. Επιλέξτε μια εγκατάσταση Java στον υπολογιστή. Το Apache Tomcat απαιτεί Java/OpenJDK 64 bit. Εάν έχετε πολλαπλές εκδόσεις Java εγκατεστημένες στο σύστημά σας, συνιστάται να καταργήσετε την εγκατάσταση των παλαιότερων εκδόσεων Java και να διατηρήσετε μόνο την πιο πρόσφατη υποστηριζόμενη έκδοση Java.

⚠ Από τον Ιανουάριο 2019, οι δημόσιες ενημερώσεις Oracle JAVA SE 8 για επιχειρηματική, εμπορική ή παραγωγική χρήση, απαιτούν εμπορική άδεια χρήσης. Εάν δεν αγοράσετε συνδρομή JAVA SE, μπορείτε να χρησιμοποιήσετε αυτό τον οδηγό για μετάβαση σε μια εναλλακτική λύση χωρίς κόστος. Δείτε τις υποστηριζόμενες εκδόσεις του JDK.

8. Κάντε κλικ στο στοιχείο **Αναβάθμιση** για να ολοκληρώσετε την αναβάθμιση και μετά κάντε κλικ στο στοιχείο **Τέλος**.

9. Εάν εγκαταστήσατε την κονσόλα διαδικτύου σε διαφορετικό υπολογιστή από τον υπολογιστή όπου είναι εγκατεστημένος ο διακομιστής ESET PROTECT:

a. Διακόψτε την υπηρεσία Apache TomcatTomcat. Μεταβείτε στα στοιχεία **Έναρξη** > **Υπηρεσίες** > κάντε δεξί κλικ στην υπηρεσία Apache Tomcat και επιλέξτε **Διακοπή**.

b.Επαναφέρετε το αρχείο *EraWebServerConfig.properties* (από το βήμα 1) στην αρχική του θέση.

c. Εκκινήστε την υπηρεσία Apache Tomcat: Μεταβείτε στα στοιχεία **Έναρξη** > **Υπηρεσίες** > κάντε δεξί κλικ στην υπηρεσία Apache Tomcat και επιλέξτε **Έναρξη**.

10. Συνδεθείτε στην Κονσόλα διαδικτύου ESET PROTECT και επαληθεύστε ότι η Κονσόλα διαδικτύου φορτώνεται σωστά.

Δείτε επίσης την πρόσθετη ρύθμιση παραμέτρων της Κονσόλας διαδικτύου για εταιρικές λύσεις ή συστήματα χαμηλών επιδόσεων.

Αντιμετώπιση προβλημάτων

Εάν αποτύχει η αναβάθμιση του Apache Tomcat, καταργήστε την εγκατάσταση του Apache Tomcat και, στη συνέχεια, εγκαταστήστε το ξανά και εφαρμόστε τη ρύθμιση παραμέτρων από το βήμα 1.

Αναβάθμιση του Apache Tomcat μη αυτόματα (Windows)

το Apache Tomcat είναι απαραίτητο στοιχείο για τη λειτουργία της Κονσόλας διαδικτύου ESET PROTECT. Αναβαθμίστε το Apache Tomcat μη αυτόματα εάν εκτελέσατε την υπάρχουσα εγκατάσταση του Apache Tomcat μη αυτόματα ή εάν δεν έχετε το πιο πρόσφατο Πρόγραμμα εγκατάστασης «Όλα σε ένα» του ESET PROTECT.

Εάν είναι εγκατεστημένη μια προσαρμοσμένη έκδοση του Apache Tomcat (μη αυτόματη εγκατάσταση της υπηρεσίας Tomcat), δεν υποστηρίζεται η επακόλουθη αναβάθμιση της Κονσόλας διαδικτύου ESET PROTECT μέσω του προγράμματος εγκατάστασης «όλα σε ένα» ή μέσω της εργασίας αναβάθμισης στοιχείων.

Πριν από την αναβάθμιση

- Το Apache Tomcat απαιτεί Java/OpenJDK 64 bit. Εάν έχετε πολλαπλές εκδόσεις Java εγκατεστημένες στο σύστημά σας, συνιστάται να καταργήσετε την εγκατάσταση των παλαιότερων εκδόσεων Java και να διατηρήσετε μόνο την πιο πρόσφατη υποστηριζόμενη έκδοση Java.

Από τον Ιανουάριο 2019, οι δημόσιες ενημερώσεις Oracle JAVA SE 8 για επιχειρηματική, εμπορική ή παραγωγική χρήση, απαιτούν εμπορική άδεια χρήσης. Εάν δεν αγοράσετε συνδρομή JAVA SE, μπορείτε να χρησιμοποιήσετε αυτό τον οδηγό για μετάβαση σε μια εναλλακτική λύση χωρίς κόστος. Δείτε τις υποστηριζόμενες εκδόσεις του JDK.

- Ελέγξτε ποια έκδοση του Apache χρησιμοποιείται εκείνη τη στιγμή.

  a.Μεταβείτε στο φάκελο εγκατάστασης του Apache Tomcat:
  C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]*

  b.Ανοίξτε το αρχείο RELEASE-NOTES σε ένα πρόγραμμα επεξεργασίας κειμένου και ελέγξτε τον αριθμό έκδοσης (για παράδειγμα 9.0.34).

  c.Εάν υπάρχει διαθέσιμη νεότερη υποστηριζόμενη έκδοση, εκτελέστε αναβάθμιση.

Διαδικασίες αναβάθμισης

1. Διακόψτε την υπηρεσία Apache TomcatTomcat. Μεταβείτε στα στοιχεία **Έναρξη** > **Υπηρεσίες** >

κάντε δεξί κλικ στην υπηρεσία Apache Tomcat και επιλέξτε **Διακοπή**.

Κλείστε το αρχείο *Tomcat7w.exe* εάν εκτελείται στην περιοχή ειδοποιήσεων των Windows.

2. Δημιουργήστε αντίγραφα ασφαλείας για τα παρακάτω αρχεία:

C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]\.keystore*
C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]\conf\server.xml*
C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*

Εάν χρησιμοποιείτε προσαρμοσμένο χώρο αποθήκευσης πιστοποιητικών SSL στο φάκελο *Tomcat*, δημιουργήστε αντίγραφο ασφαλείας και για το πιστοποιητικό.

3. Καταργήστε την τρέχουσα εγκατάσταση του Apache Tomcat.

4. Διαγράψτε τον παρακάτω φάκελο εάν εξακολουθεί να υπάρχει στο σύστημά σας:

C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]*

5. Πραγματοποιήστε λήψη της πιο πρόσφατης υποστηριζόμενης έκδοσης του αρχείου προγράμματος εγκατάστασης του Apache Tomcat (32-bit/64-bit Windows Service Installer) `apache-tomcat-[].exe` από τη διεύθυνση https://tomcat.apache.org.

6. Εγκαταστήστε τη νεότερη έκδοση του Apache Tomcat που λάβατε.

• Εάν έχετε εγκαταστήσει περισσότερες εκδόσεις Java, επιλέξτε τη διαδρομή προς την πιο πρόσφατη έκδοση Java κατά τη διάρκεια της εγκατάστασης.

• Όταν ολοκληρωθεί η εγκατάσταση, καταργήστε την επιλογή του πλαισίου ελέγχου που βρίσκεται δίπλα στο στοιχείο **Εκτέλεση Apache Tomcat**.

7. Κάντε επαναφορά των στοιχείων *.keystore server.xml* και των προσαρμοσμένων πιστοποιητικών στις αρχικές τοποθεσίες τους.

8. Ανοίξτε το αρχείο *server.xml* και βεβαιωθείτε ότι η διαδρομή *keystoreFile* είναι σωστή (ενημερώστε τη διαδρομή εάν αναβαθμίσατε σε ανώτερη κύρια έκδοση του Apache Tomcat):

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat φάκελος *]\.keystore"*

9. Βεβαιωθείτε ότι η ρύθμιση παραμέτρων της σύνδεσης HTTPS για το Apache Tomcat για την Κονσόλα διαδικτύου ESET PROTECT έχει εκτελεστεί σωστά.

10. Αναπτύξτε την κονσόλα διαδικτύου ESET PROTECT (Εγκατάσταση Κονσόλας διαδικτύου - Windows).

11. Επαναφέρετε το *EraWebServerConfig.properties* στην αρχική του θέση.

12. Εκτελέστε το Apache Tomcat και καθορίστε τη σωστή εικονική μηχανή Java:

a.Μεταβείτε στο φάκελο *C:\Program Files\Apache Software Foundation\[Tomcat* φάκελος *]\bin* και εκτελέστε το *Tomcat9w.exe*.

b.Στην καρτέλα **Γενικά**, ρυθμίστε το στοιχείο **Τύπος έναρξης** σε **Αυτόματα** και πατήστε **Έναρξη**.

c.Κάντε κλικ στην καρτέλα **Java**, καταργήστε την επιλογή του στοιχείου **Χρήση προεπιλογής** και βεβαιωθείτε ότι ο **Εικονικός υπολογιστής Java** περιλαμβάνει τη διαδρομή στο αρχείο *jvm.dll* (δείτε τις εικονογραφημένες οδηγίες στη Γνωσιακή βάση) και μετά κάντε κλικ στο **OK**.

13. Συνδεθείτε στην Κονσόλα διαδικτύου ESET PROTECT και επαληθεύστε ότι η Κονσόλα διαδικτύου φορτώνεται σωστά.

Δείτε επίσης την πρόσθετη ρύθμιση παραμέτρων της Κονσόλας διαδικτύου για εταιρικές λύσεις ή συστήματα χαμηλών επιδόσεων.

Αντιμετώπιση προβλημάτων

- Εάν η ρύθμιση της σύνδεσης HTTPS για το Apache Tomcat δεν ήταν επιτυχής, μπορείτε να παραλείψετε αυτό το βήμα και να χρησιμοποιήσετε προσωρινά σύνδεση HTTP.

- Εάν η αναβάθμιση του Apache Tomcat αποτύχει, εγκαταστήστε την αρχική έκδοση και εφαρμόστε τη ρύθμιση παραμέτρων από το βήμα 2.

- Η αναβάθμιση της Κονσόλας διαδικτύου και του Apache Tomcat εκκαθαρίζει τα αρχεία βοήθειας εκτός σύνδεσης. Εάν χρησιμοποιήσατε βοήθεια εκτός σύνδεσης με μια παλαιότερη έκδοση του ESET PROTECT On-Prem, δημιουργήστε την ξανά για το ESET PROTECT On-Prem 11.0 μετά την αναβάθμιση, για να διασφαλίσετε ότι έχετε την πιο πρόσφατη βοήθεια εκτός σύνδεσης που αντιστοιχεί στην έκδοση του ESET PROTECT On-Prem που διαθέτετε.

Αναβάθμιση του Apache Tomcat και Java (Linux).

το Apache Tomcat είναι απαραίτητο στοιχείο για τη λειτουργία της Κονσόλας διαδικτύου ESET PROTECT.

Πριν από την αναβάθμιση

1. Εκτελέστε την ακόλουθη εντολή για να δείτε την εγκατεστημένη έκδοση του Apache Tomcat (σε ορισμένες περιπτώσεις, το όνομα του φακέλου είναι `tomcat7` ή `tomcat8`):

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. Εάν είναι διαθέσιμη νεότερη έκδοση:

a.Βεβαιωθείτε ότι νεότερη έκδοση υποστηρίζεται.

b.Δημιουργήστε αντίγραφα ασφαλείας του αρχείου ρύθμισης παραμέτρων του Tomcat */etc/tomcat7/server.xml*.

Διαδικασίες αναβάθμισης

1. Εκτελέστε την ακόλουθη εντολή για να διακόψετε την υπηρεσία Apache Tomcat (σε ορισμένες περιπτώσεις, το όνομα της υπηρεσίας είναι `tomcat7`):

```
sudo systemctl stop tomcat
```

2. Αναβάθμιση του Apache Tomcat και Java.

> Τα παρακάτω παραδείγματα ονομάτων πακέτων μπορεί να διαφέρουν από τα πακέτα στο αποθετήριο διανομής Linux. Το προεπιλεγμένο αποθετήριο της διανομής Linux που διαθέτετε ενδέχεται να μην περιέχει την πιο πρόσφατη υποστηριζόμενη έκδοση του Apache Tomcat και της Java.

Διανομή Linux	Εντολές τερματικού
Διανομές Debian και Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
Διανομές CentOS και Red Hat	`yum update` `yum install java-17-openjdk tomcat`
SUSE Linux	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

3. Αντικαταστήστε το αρχείο */etc/tomcat9/server.xml* με το αρχείο *server.xml* από αντίγραφο ασφαλείας.

4. Ανοίξτε το αρχείο *server.xml* και βεβαιωθείτε ότι η διαδρομή *keystoreFile* είναι σωστή.

5. Βεβαιωθείτε ότι η ρύθμιση παραμέτρων της σύνδεσης HTTPS για το Apache Tomcat έχει εκτελεστεί σωστά.

Δείτε επίσης την πρόσθετη ρύθμιση παραμέτρων της Κονσόλας διαδικτύου για εταιρικές λύσεις ή συστήματα χαμηλών επιδόσεων.

6. Εάν έχετε αναβαθμίσει τη Java, ακολουθήστε τα παρακάτω βήματα για να ρυθμίσετε τις παραμέτρους του Apache Tomcat για να χρησιμοποιήσετε το πιο πρόσφατο πακέτο Java που είναι εγκατεστημένο στο σύστημά σας:

a.Μεταβείτε στον φάκελο ρύθμισης παραμέτρων του Apache Tomcat:

```
cd /usr/share/tomcat/conf/
```

b.Ανοίξτε το αρχείο *tomcat.conf* σε ένα πρόγραμμα επεξεργασίας κειμένου:

```
nano tomcat.conf
```

c.Ενημερώστε τη διαδρομή προς το πιο πρόσφατα εγκατεστημένο πακέτο Java στη μεταβλητή `JAVA_HOME` (η διαδρομή διαφέρει ανάλογα με το πακέτο Java που έχει εγκατασταθεί στο σύστημά σας):

```
JAVA_HOME="/usr/lib/jvm/jre-11-openjdk"
```

d.Αποθηκεύστε και κλείστε το αρχείο: Πατήστε **CTRL+X** και, στη συνέχεια, πατήστε **Y** και **ENTER**.

e.Κάντε επανεκκίνηση της υπηρεσίας **tomcat**:

```
sudo systemctl restart tomcat
```

f.Εκτελέστε την παρακάτω εντολή για να επαληθεύσετε το πακέτο Java που χρησιμοποιείται από το Apache Tomcat:

```
sudo systemctl status tomcat
```

Μετά την αναβάθμιση του Apache Tomcat σε νεότερη κύρια έκδοση (για παράδειγμα, Apache Tomcat έκδοση 7.x σε 9.x):
1.Αναπτύξτε την κονσόλα διαδικτύου ESET PROTECT ξανά (δείτε την ενότητα Εγκατάσταση Κονσόλας διαδικτύου ESET PROTECT - Linux)
2.Χρησιμοποιήστε ξανά το *%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties* για να διατηρήσετε οποιεσδήποτε προσαρμοσμένες ρυθμίσεις στην κονσόλα διαδικτύου ESET PROTECT.
Η αναβάθμιση της Κονσόλας διαδικτύου και του Apache Tomcat εκκαθαρίζει τα αρχεία βοήθειας εκτός σύνδεσης. Εάν χρησιμοποιήσατε βοήθεια εκτός σύνδεσης με μια παλαιότερη έκδοση του ESET PROTECT On-Prem, δημιουργήστε την ξανά για το ESET PROTECT On-Prem 11.0 μετά την αναβάθμιση, για να διασφαλίσετε ότι έχετε την πιο πρόσφατη βοήθεια εκτός σύνδεσης που αντιστοιχεί στην έκδοση του ESET PROTECT On-Prem που διαθέτετε.

Διαδικασίες μετεγκατάστασης και επανεγκατάστασης

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορείτε να αναβαθμίσετε, να μετεγκαταστήσετε και να επανεγκαταστήσετε το διακομιστή ESET PROTECT και άλλα στοιχεία ESET PROTECT:

- Μετεγκατάσταση ή επανεγκατάσταση του ESET PROTECT On-Prem 11.0 από έναν διακομιστή σε άλλον.

Για να πραγματοποιήσετε μετεγκατάσταση από έναν διακομιστή ESET PROTECT σε νέο υπολογιστή διακομιστή, εξαγάγετε/δημιουργήσετε αντίγραφα ασφαλείας όλων των Αρχών έκδοσης πιστοποιητικού, καθώς και του Πιστοποιητικού διακομιστή ESET PROTECT. Διαφορετικά, δεν θα μπορεί να επικοινωνήσει κανένα από τα στοιχεία του ESET PROTECTμε τον νέο διακομιστή ESET PROTECT.

- μετεγκατάσταση βάσης δεδομένων ESET PROTECT
- Μετεγκατάσταση του MDM
- Αλλαγή της διεύθυνσης IP ή του ονόματος κεντρικού υπολογιστή σε έναν διακομιστή ESET PROTECT

Ανατρέξτε στο θέμα διαδικασίες αναβάθμισης.

Μετεγκατάσταση από ένα διακομιστή σε άλλον

Υπάρχουν πολλοί τρόποι να μετεγκαταστήσετε το ESET PROTECT On-Prem από έναν διακομιστή σε έναν άλλο (αυτά τα σενάρια μπορούν να χρησιμοποιηθούν κατά την επανεγκατάσταση του διακομιστή ESET PROTECT):

- Καθαρή εγκατάσταση - ίδια διεύθυνση IP - Η νέα εγκατάσταση δεν χρησιμοποιεί την προηγούμενη βάση δεδομένων από τον παλιό διακομιστή ESET PROTECT, αλλά διατηρεί την αρχική διεύθυνση IP.

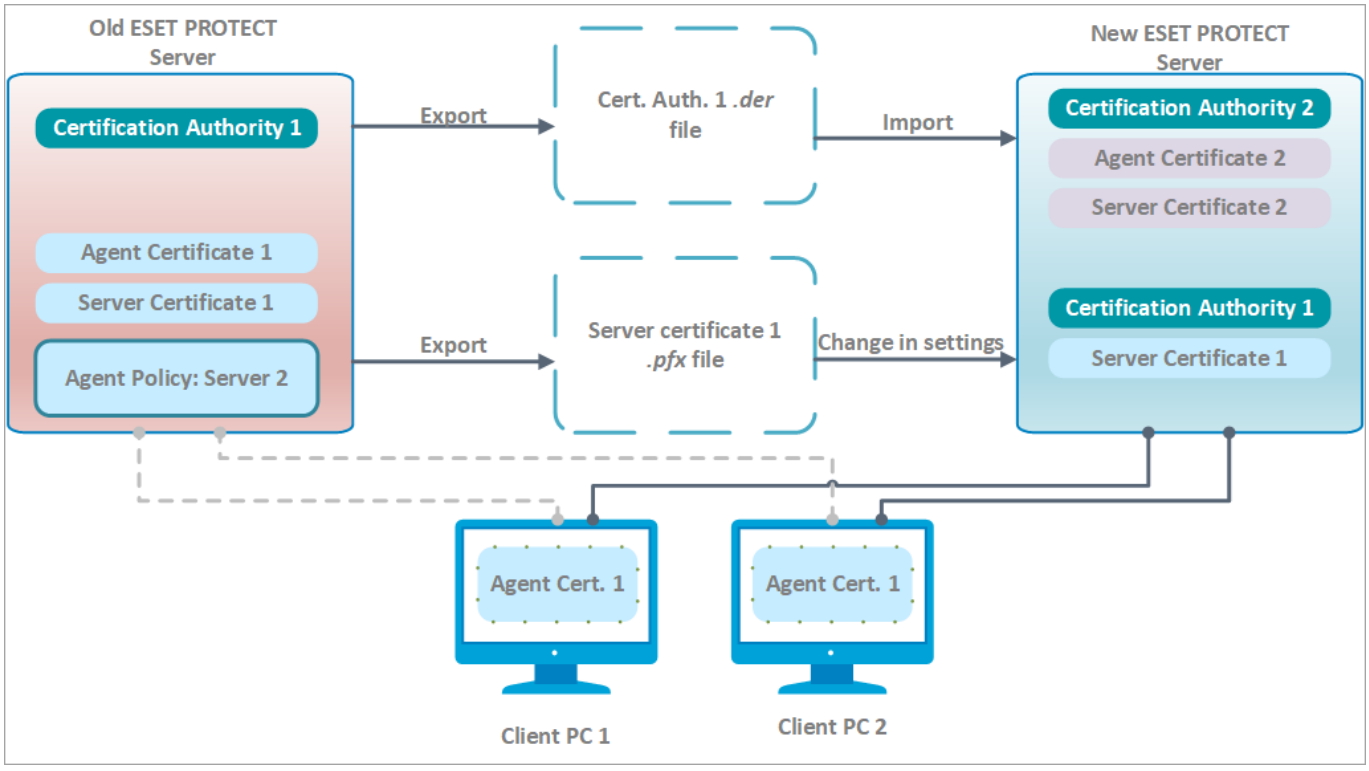
- Καθαρή εγκατάσταση - διαφορετική διεύθυνση IP (άρθρο της Γνωσιακής βάσης) - Η νέα εγκατάσταση δεν χρησιμοποιεί την προηγούμενη βάση δεδομένων από τον παλιό διακομιστή ESET PROTECT και έχει διαφορετική διεύθυνση IP.

- Μετεγκατεστημένη βάση δεδομένων - ίδια/διαφορετική διεύθυνση IP - Η μετεγκατάσταση βάσεων δεδομένων μπορεί να εκτελεστεί μόνο ανάμεσα σε δυο όμοιες βάσεις δεδομένων (από MySQL σε MySQL ή από Microsoft SQL σε Microsoft SQL) και δυο όμοιες εκδόσεις του ESET PROTECT On-Prem.

Καθαρή εγκατάσταση - ίδια διεύθυνση IP

Ο σκοπός αυτής της διαδικασίας είναι να εγκαταστήσει μια εντελώς νέα εμφάνιση του διακομιστή ESET PROTECT που δεν χρησιμοποιεί την προηγούμενη βάση δεδομένων. Ο νέος διακομιστής ESET PROTECT θα έχει **την ίδια διεύθυνση IP/όνομα κεντρικού υπολογιστή** όπως ο προηγούμενος διακομιστής, αλλά δεν θα χρησιμοποιεί τη βάση δεδομένων από τον παλιό διακομιστή ESET PROTECT.

Σύμφωνα με τις παρακάτω οδηγίες απαιτείται να εκτελείται ο παλιός Διακομιστής ESET PROTECT με μια προσπελάσιμη Κονσόλα διαδικτύου. Εάν δεν είναι δυνατή η πρόσβαση στον παλιό Διακομιστή ESET PROTECT:
1. Εγκαταστήστε τον διακομιστή/το MDM ESET PROTECT χρησιμοποιώντας την εγκατάσταση πακέτου «όλα σε ένα» (Windows) ή επιλέξτε άλλη μέθοδο εγκατάστασης (μη αυτόματη εγκατάσταση στα Windows, Linux ή εικονική συσκευή).
2. Συνδεθείτε στην Κονσόλα διαδικτύου ESET PROTECT.
3. Προσθέστε υπολογιστές-πελάτες στην υποδομή του ESET PROTECT και αναπτύξτε τον Φορέα ESET Management τοπικά ή απομακρυσμένα.



Δείτε την εικόνα σε μεγαλύτερη

I. Στον τρέχοντα (παλιό) διακομιστή ESET PROTECT:

Εάν διαχειρίζεστε συσκευές που έχουν κρυπτογραφηθεί με το ESET Full Disk Encryption, ακολουθήστε τα εξής βήματα για να αποφύγετε την απώλεια δεδομένων ανάκτησης.
1.Πριν τη μετεγκατάσταση – Μεταβείτε στο στοιχείο **Επισκόπηση κατάστασης** > **Κρυπτογράφηση**. Εδώ μπορείτε να κάνετε **Εξαγωγή** στα τρέχοντα **Δεδομένα ανάκτησης ESET Full Disk Encryption**.
2.Μετά τη μετεγκατάσταση – Πρέπει να κάνετε **Εισαγωγή** στο στοιχείο **Δεδομένα ανάκτησης ESET Full Disk Encryption** στη νέα κονσόλα διαχείρισης.
Εάν δεν μπορείτε να εκτελέσετε αυτά τα βήματα, πρέπει να αποκρυπτογραφήσετε τις διαχειριζόμενες συσκευές πριν τη μετεγκατάσταση. Μετά τη μετεγκατάσταση, μπορείτε να κρυπτογραφήσετε τις διαχειριζόμενες συσκευές από την ESET PROTECT Κονσόλα διαδικτύου.

1. Εξαγάγετε ένα πιστοποιητικά διακομιστή από τον τρέχοντα διακομιστή ESET PROTECT και αποθηκεύστε το στον εξωτερικό χώρο αποθήκευσης.

   • Εξαγάγετε όλα τα πιστοποιητικά Αρχής έκδοσης πιστοποιητικών (CA) από το διακομιστή ESET PROTECT και αποθηκεύστε κάθε πιστοποιητικό CA ως αρχείο *.der*.

   • Εξαγάγετε το πιστοποιητικό διακομιστή από το διακομιστή ESET PROTECT σε ένα αρχείο *.pfx*. Το εξηγμένο *.pfx* θα περιλαμβάνει, επίσης, ένα ιδιωτικό κλειδί.

2. Διακόψτε την υπηρεσία του διακομιστή ESET PROTECT.

3. Απενεργοποιήστε τον υπολογιστή του διακομιστή ESET PROTECT.

Μη καταργήσετε την εγκατάσταση/αποσύρετε ακόμη τον παλιό σας διακομιστή ESET PROTECT.

II. Στον νέο διακομιστή ESET PROTECT:

Για να χρησιμοποιήσετε έναν νέο διακομιστή ESET PROTECT με την ίδια διεύθυνση IP, βεβαιωθείτε ότι η ρύθμιση παραμέτρων του δικτύου στον νέο σας διακομιστή ESET PROTECT (**Διεύθυνση IP, FQDN, Όνομα υπολογιστή, Εγγραφή DNS SRV**) συμφωνεί με τη ρύθμιση παραμέτρων του παλιού σας διακομιστή ESET PROTECT.

1. Εγκαταστήστε τον διακομιστή/το MDM ESET PROTECT χρησιμοποιώντας την εγκατάσταση πακέτου «όλα σε ένα» (Windows) ή επιλέξτε άλλη μέθοδο εγκατάστασης (μη αυτόματη εγκατάσταση στα Windows, Linux ή εικονική συσκευή).

2. Συνδεθείτε στην Κονσόλα διαδικτύου ESET PROTECT.

3. Εισαγάγετε όλες τις αρχές έκδοσης πιστοποιητικών που έχετε εξαγάγει από τον παλιό διακομιστή ESET PROTECT. Για να το κάνετε αυτό, ακολουθήστε τις οδηγίες για την εισαγωγή δημόσιου κλειδιού.

4. Αλλάξτε το πιστοποιητικό του διακομιστή ESET PROTECT στις **Περισσότερα** > Ρυθμίσεις διακομιστή για να χρησιμοποιήσετε το πιστοποιητικό από τον παλιό διακομιστή ESET PROTECT.

5. Εισαγάγετε όλες τις απαιτούμενες άδειες χρήσης ESET στο ESET PROTECT On-Prem.

6. Επανεκκινήστε την υπηρεσία διακομιστή ESET PROTECT. Για λεπτομέρειες, δείτε το άρθρο της

Γνωσιακής βάσης.

Μετά από ένα ή δύο Διαστήματα σύνδεσης Φορέα, οι υπολογιστές-πελάτες θα πρέπει να συνδέονται με τον νέο Διακομιστή ESET PROTECT χρησιμοποιώντας το αρχικό τους πιστοποιητικό Φορέα ESET Management, το οποίο επαληθεύεται από την Αρχή έκδοσης πιστοποιητικών που έχει εισαχθεί από τον παλιό Διακομιστή ESET PROTECT. Εάν οι υπολογιστές-πελάτες δεν μπορούν να συνδεθούν, ανατρέξτε στο κεφάλαιο Προβλήματα μετά την αναβάθμιση/μετεγκατάσταση του διακομιστή ESET PROTECT.

Κατά την προσθήκη νέων υπολογιστών-πελατών, χρησιμοποιήστε μια νέα Αρχή έκδοσης πιστοποιητικών για να υπογράψετε τα πιστοποιητικά φορέα. Αυτό γίνεται επειδή δεν είναι δυνατό να χρησιμοποιηθεί μια εισηγμένη Αρχή έκδοσης για την υπογραφή νέων ομότιμων πιστοποιητικών - αυτή μπορεί να χρησιμοποιηθεί μόνο για τον έλεγχο ταυτότητας των φορέων ESET Management σε υπολογιστές-πελάτες που έχουν μετεγκατασταθεί.

III. Κατάργηση εγκατάστασης παλιού διακομιστή/MDM ESET PROTECT:

Εφόσον όλα λειτουργούν κανονικά με τον νέο σας διακομιστή ESET PROTECT, αποσύρετε προσεκτικά τον παλιό διακομιστή/το παλιό MDM ESET PROTECT ακολουθώντας τις οδηγίες βήμα προς βήμα.

Μετεγκατεστημένη βάση δεδομένων - ίδια/διαφορετική διεύθυνση IP

Σκοπός αυτής της διαδικασίας είναι η εγκατάσταση μιας εντελώς νέας εμφάνισης του διακομιστή ERA ESET PROTECT και η **διατήρηση της υπάρχουσας βάσης δεδομένων ERAESET PROTECT**, συμπεριλαμβανομένων των υπαρχόντων υπολογιστών-πελατών. Ο νέος διακομιστής ESET PROTECT θα έχει **την ίδια ή διαφορετική διεύθυνση IP** και η βάση δεδομένων του παλιού διακομιστή ESET PROTECT θα εισαχθεί στον υπολογιστή του νέου διακομιστή πριν από την εγκατάσταση.

- Η Μετεγκατάσταση βάσεων δεδομένων υποστηρίζεται μόνο ανάμεσα σε ταυτόσημες βάσεις δεδομένων (από MySQL σε MySQL ή από Microsoft SQL σε Microsoft SQL).
- Όταν μετεγκαθιστάτε μια βάση δεδομένων, η μετεγκατάσταση πρέπει να γίνεται ανάμεσα σε εμφανίσεις ίδιας έκδοσης του ESET PROTECT On-Prem. Ανατρέξτε στο άρθρο της Γνωσιακής βάσης για οδηγίες σχετικά με τον τρόπο προσδιορισμού της έκδοσης των στοιχείων ESET PROTECT. Αφού ολοκληρώσετε τη μετεγκατάσταση της βάσης δεδομένων, μπορείτε να πραγματοποιήσετε αναβάθμιση, εάν χρειάζεται, για να αποκτήσετε την πιο πρόσφατη έκδοση του ESET PROTECT On-Prem.

I. Στον τρέχοντα (παλιό) διακομιστή ESET PROTECT:

Η μετεγκατάσταση σε διαφορετική διεύθυνση IP συνιστάται μόνο για προχωρημένους χρήστες. Εάν ο νέος διακομιστής ESET PROTECT έχει **διαφορετική διεύθυνση IP**, εκτελέστε αυτά τα πρόσθετα βήματα στον τρέχοντα (παλιό) διακομιστή ESET PROTECT:
a)Δημιουργήστε ένα νέο πιστοποιητικό διακομιστή ESET PROTECT με πληροφορίες σύνδεσης για τον νέο διακομιστή ESET PROTECT. Αφήστε την προεπιλεγμένη τιμή (ένας αστερίσκος) στο πεδίο **Κεντρικός υπολογιστής** για να επιτρέπεται η διανομή αυτού του πιστοποιητικού χωρίς συσχετισμό σε συγκεκριμένο όνομα DNS ή διεύθυνση IP.
b)Δημιουργήστε μια πολιτική για να καθορίσετε τη διεύθυνση IP του νέου διακομιστή ESET PROTECT και εκχωρήστε την σε όλους τους υπολογιστές. Περιμένετε να διανεμηθεί η πολιτική σε όλους τους υπολογιστές-πελάτες (οι υπολογιστές θα σταματήσουν να αναφέρονται καθώς λαμβάνουν τις πληροφορίες για τον νέο διακομιστή).

1. Διακόψτε την υπηρεσία του διακομιστή ESET PROTECT.

2. Εξαγάγετε τη βάση δεδομένων του ESET PROTECT ή δημιουργήστε αντίγραφο ασφαλείας της.

3. Απενεργοποιήστε τον υπολογιστή του τρέχοντος διακομιστή ESET PROTECT (προαιρετικά, εάν ο νέος διακομιστής έχει διαφορετική διεύθυνση IP).

Μη καταργήσετε την εγκατάσταση/αποσύρετε ακόμη τον παλιό σας διακομιστή ESET PROTECT.

II. Στον νέο διακομιστή ESET PROTECT:

Για να χρησιμοποιήσετε έναν νέο διακομιστή ESET PROTECT με την ίδια διεύθυνση IP, βεβαιωθείτε ότι η ρύθμιση παραμέτρων του δικτύου στον νέο σας διακομιστή ESET PROTECT (**Διεύθυνση IP, FQDN, Όνομα υπολογιστή, Εγγραφή DNS SRV**) συμφωνεί με τη ρύθμιση παραμέτρων του παλιού σας διακομιστή ESET PROTECT.

1. Εγκαταστήστε/Ανοίξτε μια υποστηριζόμενη βάση δεδομένων ESET PROTECT.

2. Εισαγάγετε/Επαναφέρετε τη βάση δεδομένων ESET PROTECT από τον παλιό σας διακομιστή ESET PROTECT.

3. Εγκαταστήστε τον διακομιστή/το MDM ESET PROTECT χρησιμοποιώντας την εγκατάσταση πακέτου «όλα σε ένα» (Windows) ή επιλέξτε άλλη μέθοδο εγκατάστασης (μη αυτόματη εγκατάσταση στα Windows, Linux ή εικονική συσκευή). Καθορίστε τις ρυθμίσεις σύνδεσης της βάσης δεδομένων σας κατά την εγκατάσταση του διακομιστή ESET PROTECT.

4. Συνδεθείτε στην Κονσόλα διαδικτύου ESET PROTECT.

5. Μεταβείτε στα στοιχεία **Περισσότερα** > **Ρυθμίσεις** > **Σύνδεση**. Κάντε κλικ στα στοιχεία **Αλλαγή πιστοποιητικού** > **Άνοιγμα λίστας πιστοποιητικών** και επιλέξτε το **Πιστοποιητικό διακομιστή** του παλιού διακομιστή ESET PROTECT και κάντε κλικ στο κουμπί **OK** δύο φορές.

6. Κάντε επανεκκίνηση της υπηρεσίας διακομιστή ESET PROTECT.

7. Συνδεθείτε στην Κονσόλα διαδικτύου ESET PROTECT και κάντε κλικ στο στοιχείο **Υπολογιστές**.

Μετά από ένα ή δύο Διαστήματα σύνδεσης φορέα, οι υπολογιστές-πελάτες θα πρέπει να συνδέονται στον νέο Διακομιστή ESET PROTECT χρησιμοποιώντας το αρχικό πιστοποιητικό Φορέα ESET Management. Εάν οι υπολογιστές-πελάτες δεν μπορούν να συνδεθούν, ανατρέξτε στο κεφάλαιο Προβλήματα μετά την αναβάθμιση/μετεγκατάσταση του διακομιστή ESET PROTECT.

III. Κατάργηση εγκατάστασης παλιού διακομιστή/MDM ESET PROTECT:

Εφόσον όλα λειτουργούν κανονικά με τον νέο σας διακομιστή ESET PROTECT, αποσύρετε προσεκτικά τον παλιό διακομιστή/το παλιό MDM ESET PROTECT ακολουθώντας τις οδηγίες βήμα προς βήμα.

ESET PROTECTμετεγκατάσταση βάσης δεδομένων

Αυτές οι οδηγίες εφαρμόζονται μόνο στη μετεγκατάσταση της βάσης δεδομένων ESET PROTECT μεταξύ διαφορετικών εμφανίσεων του διακομιστή SQL Server (αυτό εφαρμόζεται, επίσης, κατά τη μετεγκατάσταση σε διαφορετική έκδοση του διακομιστή SQL Server ή κατά τη μετεγκατάσταση σε διακομιστή SQL Server που φιλοξενείται σε διαφορετικό υπολογιστή):

- Διαδικασία μετεγκατάστασης για το Microsoft SQL Server
- Διαδικασία μετεγκατάστασης για το MySQL Server

Διαδικασία μετεγκατάστασης για το Microsoft SQL Server

Αυτή η διαδικασία μετεγκατάστασης είναι ίδια για το **Microsof SQL Server** και το **Microsoft SQL Server Express**.

Για πρόσθετες πληροφορίες, ανατρέξτε στο ακόλουθο άρθρο της Γνωσιακής βάσης της Microsoft: https://msdn.microsoft.com/en-us/library/ms189624.aspx.

Προαπαιτούμενα

• Πρέπει να εγκατασταθούν εμφανίσεις SQL Server προέλευσης και προορισμού. Μπορούν να φιλοξενούνται σε διαφορετικούς υπολογιστές.

• Η εμφάνιση SQL Server προορισμού πρέπει να έχει τουλάχιστον την ίδια έκδοση με την εμφάνιση προέλευσης. Δεν υποστηρίζεται η υποβάθμιση!

• Πρέπει να είναι εγκατεστημένο το **SQL Server Management Studio**. Εάν οι εμφανίσεις του SQL Server βρίσκονται σε διαφορετικούς υπολογιστές, πρέπει να υπάρχει και στους δύο.

Μετεγκατάσταση με το SQL Server Management Studio.

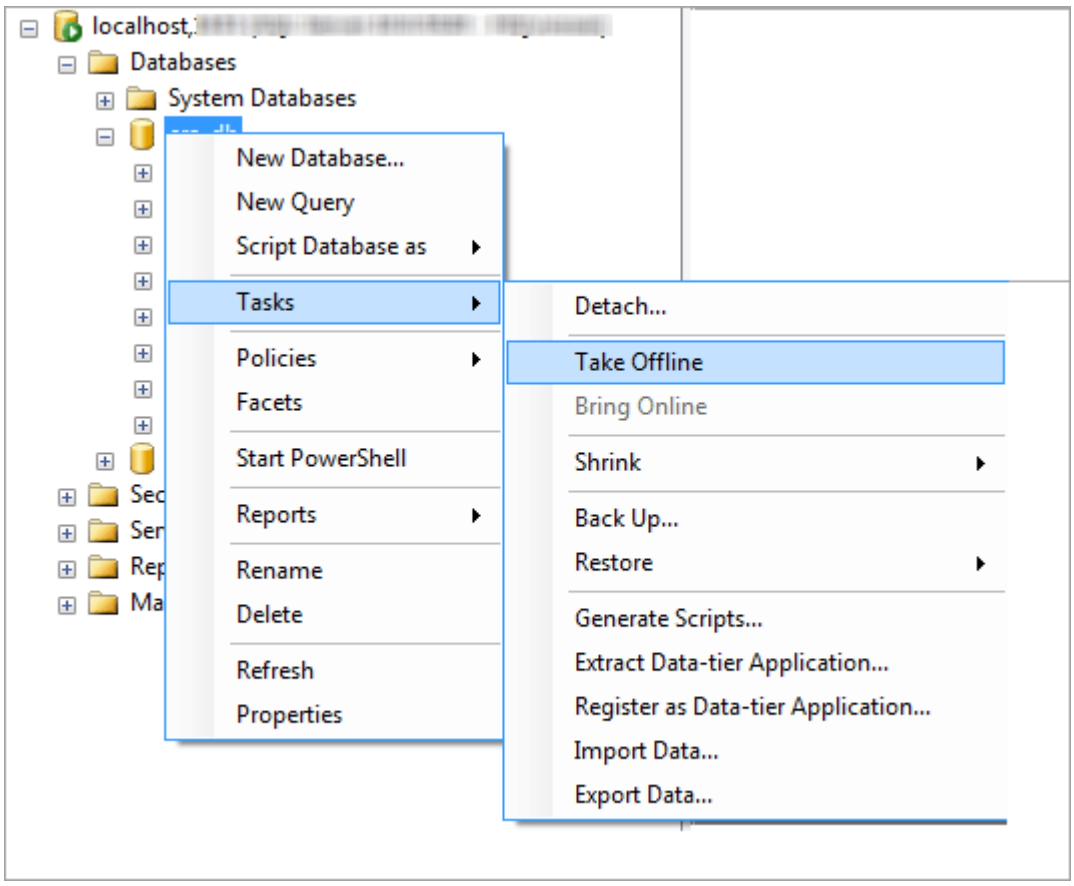
1. Διακόψτε την υπηρεσία του διακομιστή ESET PROTECT ή την υπηρεσία MDM του ESET PROTECT.

⚠ Μη εκκινήσετε το διακομιστή ESET PROTECT ή το ESET PROTECT MDM προτού ολοκληρώσετε όλα τα παρακάτω βήματα.

2. Συνδεθείτε στην εμφάνιση του SQL Server προέλευσης μέσω του SQL Server Management Studio.

3. Επιλέξτε Δημιουργία για ένα πλήρες αντίγραφο ασφαλείας βάσης δεδομένων της βάσης δεδομένων που θα μετεγκατασταθεί. Συνιστάται να καθορίσετε ένα νέο όνομα συνόλου αντιγράφων ασφαλείας. Διαφορετικά, εάν έχει ήδη χρησιμοποιηθεί το σύνολο αντιγράφων ασφαλείας, το νέο αντίγραφο ασφαλείας θα προσαρτηθεί σε αυτό με αποτέλεσμα να προκύψει χωρίς λόγο ένα μεγάλο αρχείο αντιγράφου ασφαλείας.

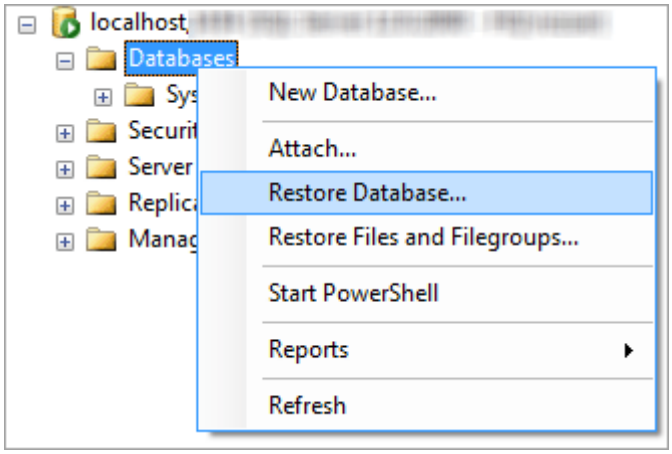
4. Μεταβείτε στη βάση δεδομένων προέλευσης χωρίς σύνδεση, επιλέξτε **Εργασίες** > **Μετάβαση χωρίς σύνδεση**.



5. Αντιγραφή του αρχείου αντιγράφου ασφαλείας (*.bak*) που δημιουργήσατε στο βήμα 3 σε μια τοποθεσία στην οποία υπάρχει πρόσβαση από την εμφάνιση SQL Server προορισμού. Ενδέχεται να χρειαστεί να επεξεργαστείτε τα δικαιώματα πρόσβασης για το αρχείο αντιγράφου ασφαλείας βάσης δεδομένων.

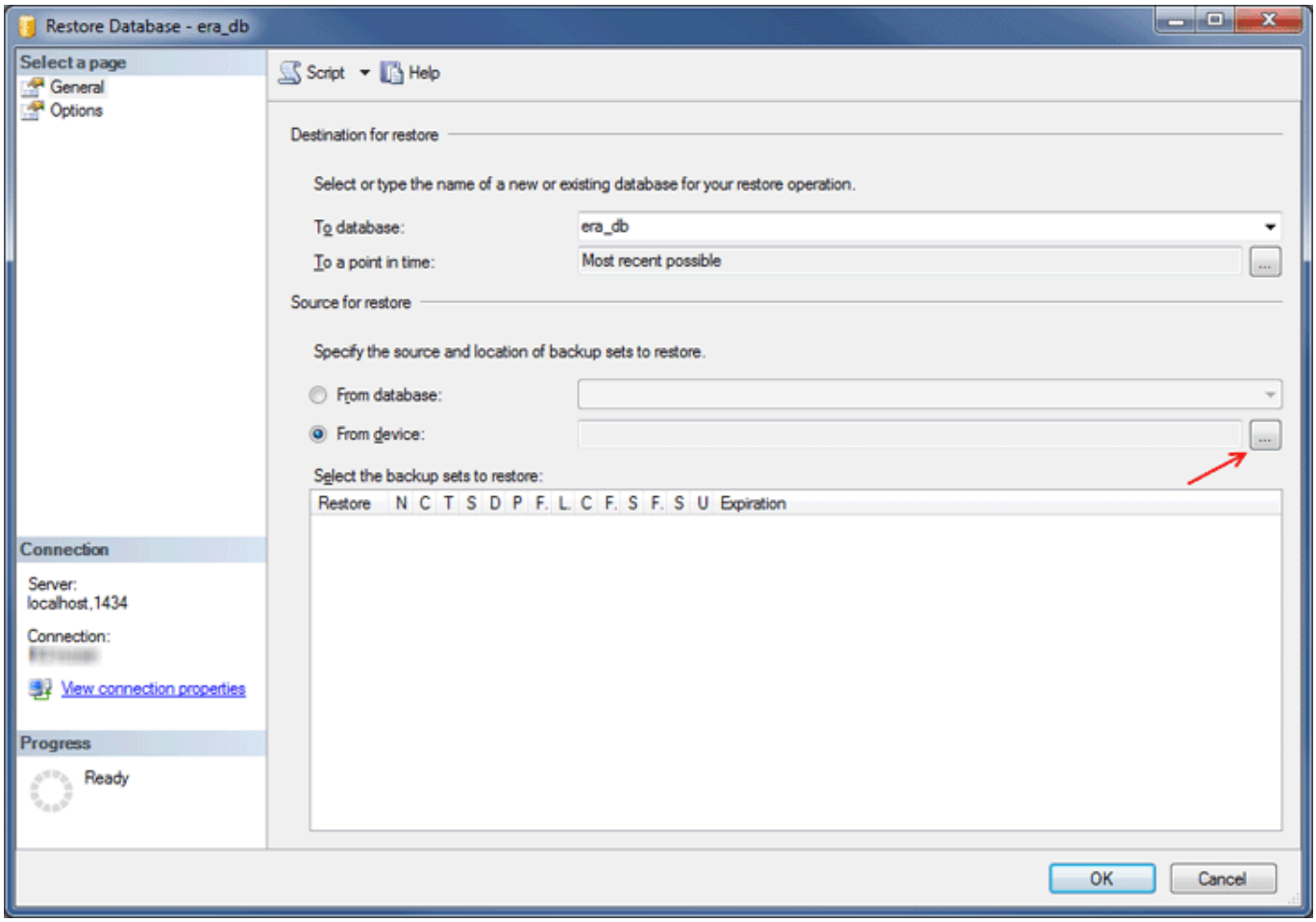
6. Συνδεθείτε στην εμφάνιση του SQL Server προορισμού με το SQL Server Management Studio.

7. Κάντε επαναφορά της βάσης δεδομένων σας στην εμφάνιση SQL Server προορισμού.



8. Πληκτρολογήστε ένα όνομα για τη νέα βάση δεδομένων σας στο πεδίο **Προς βάση δεδομένων**. Μπορείτε να χρησιμοποιήσετε το ίδιο όνομα με την παλιά βάση δεδομένων σας, εάν θέλετε.

9. Επιλέξτε 'Από συσκευή' στην περιοχή **Καθορισμός της προέλευσης και της τοποθεσίας των συνόλων αντιγράφων ασφαλείας για επαναφορά** και, στη συνέχεια, κάντε κλικ στο ... .



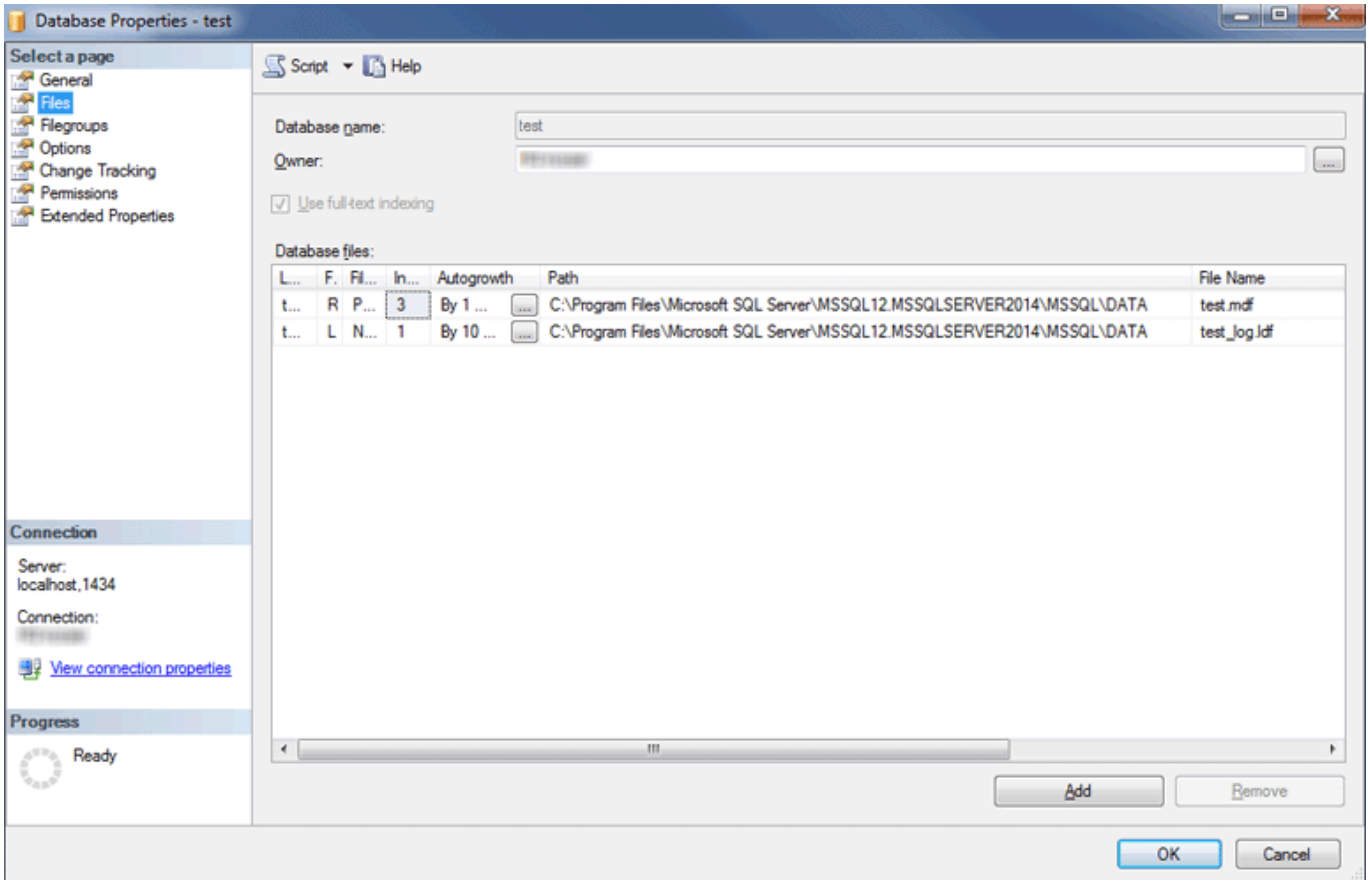
10. Κάντε κλικ στην **Προσθήκη, πλοηγηθείτε στο αρχείο αντιγράφου ασφαλείας και μετά ανοίξτε το**.

11. Επιλέξτε το πιο πρόσφατο αντίγραφο ασφαλείας για επαναφορά (το σύνολο αντιγράφων ασφαλείας μπορεί να περιέχει πολλά αντίγραφα ασφαλείας).

12. Κάντε κλικ στη σελίδα **Επιλογές** του οδηγού επαναφοράς. Προαιρετικά, επιλέξτε **Αντικατάσταση υπάρχουσας βάσης δεδομένων** και βεβαιωθείτε ότι οι τοποθεσίες

επαναφοράς για τη βάση δεδομένων (*.mdf*) και για το αρχείο καταγραφής (*.ldf*) είναι σωστές. Εάν αφήσετε αμετάβλητες τις προεπιλεγμένες τιμές, θα χρησιμοποιηθούν οι διαδρομές από το διακομιστή SQL προέλευσης, για αυτό ελέγξτε αυτές τις τιμές.

• Εάν δεν είστε βέβαιοι για το σημείο που αποθηκεύονται τα αρχεία βάσης δεδομένων στην εμφάνιση του SQL Server προορισμού, κάντε δεξί κλικ σε μια υπάρχουσα βάση δεδομένων, επιλέξτε **ιδιότητες** και κάντε κλικ στην καρτέλα **Αρχεία**. Ο κατάλογος στον οποίο είναι αποθηκευμένη η βάση δεδομένων εμφανίζεται στη στήλη **Διαδρομή** του πίνακα που εμφανίζεται παρακάτω.

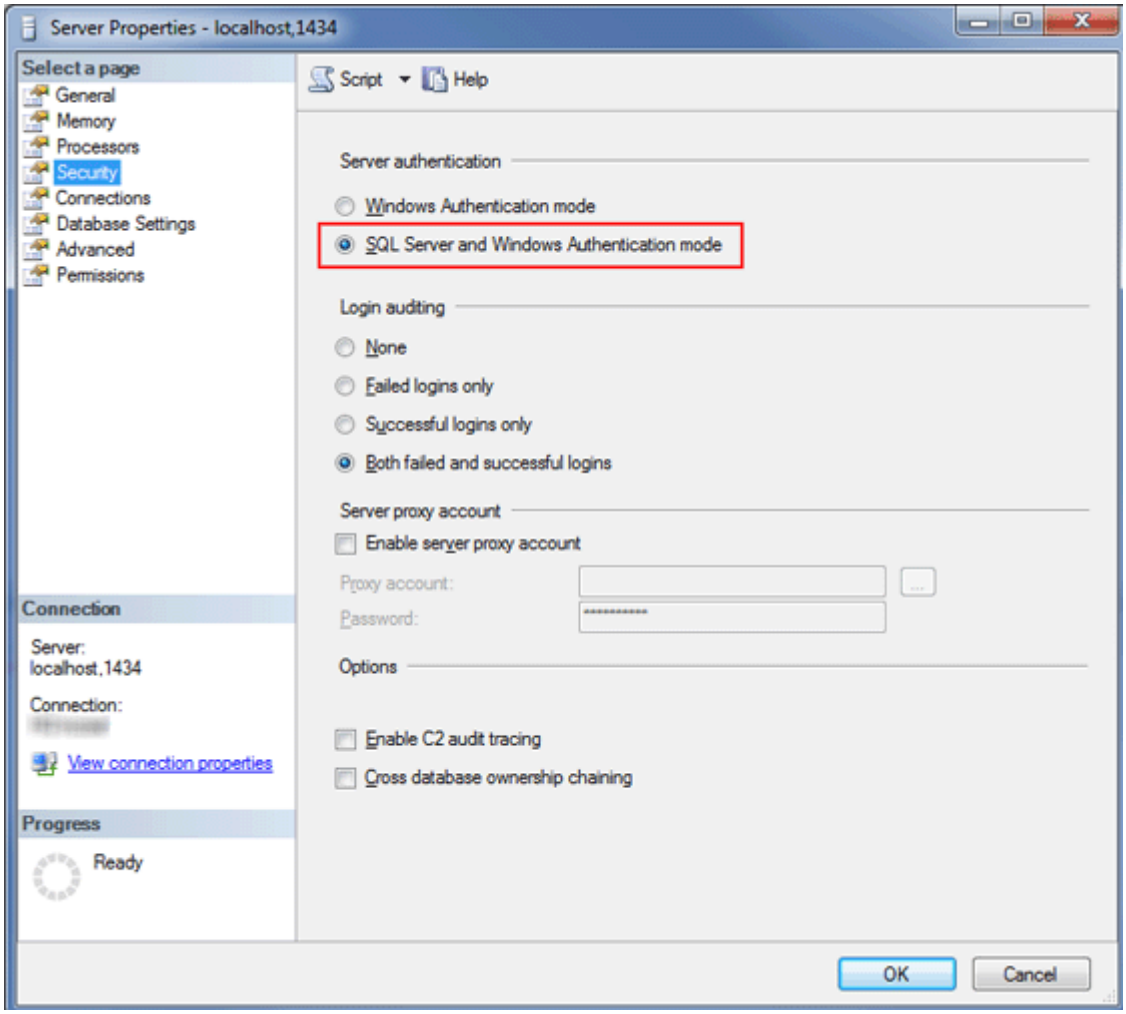


13. Κάντε κλικ στο **OK** στο παράθυρο του οδηγού επαναφοράς.

14. Κάντε δεξί κλικ στη βάση δεδομένων **era_db**, επιλέξτε **Νέο ερώτημα** και εκτελέστε το παρακάτω ερώτημα για να καταργηθούν τα περιεχόμενα του πίνακα **tbl_authentication_certificate** (διαφορετικά οι φορείς μπορεί να μη συνδέονται με τον νέο διακομιστή):

```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. Βεβαιωθείτε ότι στον νέο διακομιστή βάσης δεδομένων έχει επιλεγεί **Ενεργοποίηση ελέγχου ταυτότητας SQL Server**. Κάντε δεξί κλικ στο διακομιστή και επιλέξτε **Ιδιότητες**. Πλοηγηθείτε στην **Ασφάλεια** και επαληθεύστε ότι είναι επιλεγμένη η **λειτουργία ελέγχου ταυτότητας SQL Server** και Windows.



16. Δημιουργήστε μια νέα σύνδεσης SQL Server (για διακομιστή ESET PROTECT/MDM ESET PROTECT) στον SQL Server προορισμού με το στοιχείο **Έλεγχος ταυτότητας SQL Server** και αντιστοιχίστε τη σύνδεση σε έναν χρήστη στη επαναφερθείσα βάση δεδομένων.

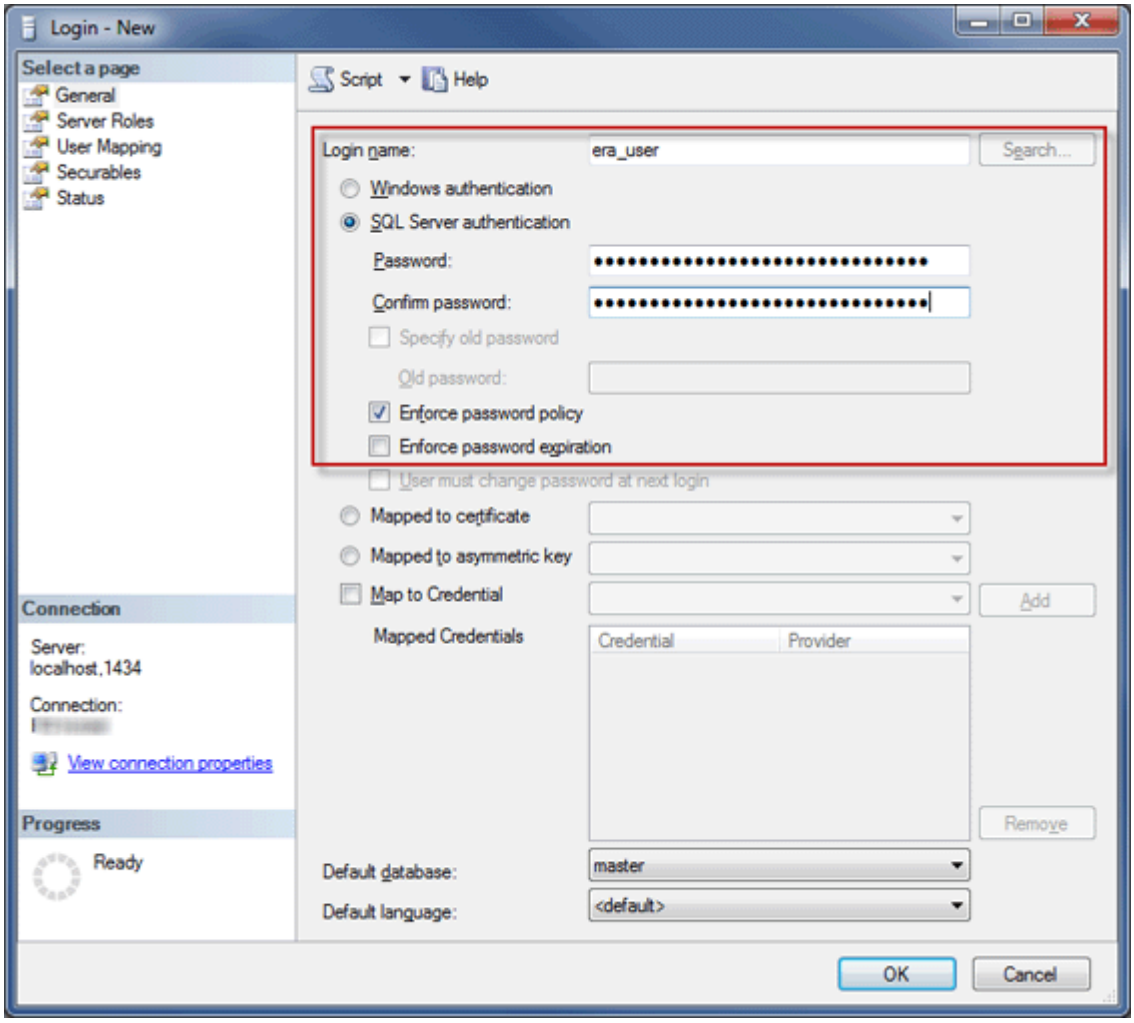
- Μην επιβάλλετε τη λήξη του κωδικού πρόσβασης!

- Συνιστώμενοι χαρακτήρες για ονόματα χρήστη: Πεζά γράμματα ASCII, αριθμοί και χαρακτήρας κάτω παύλας «_»

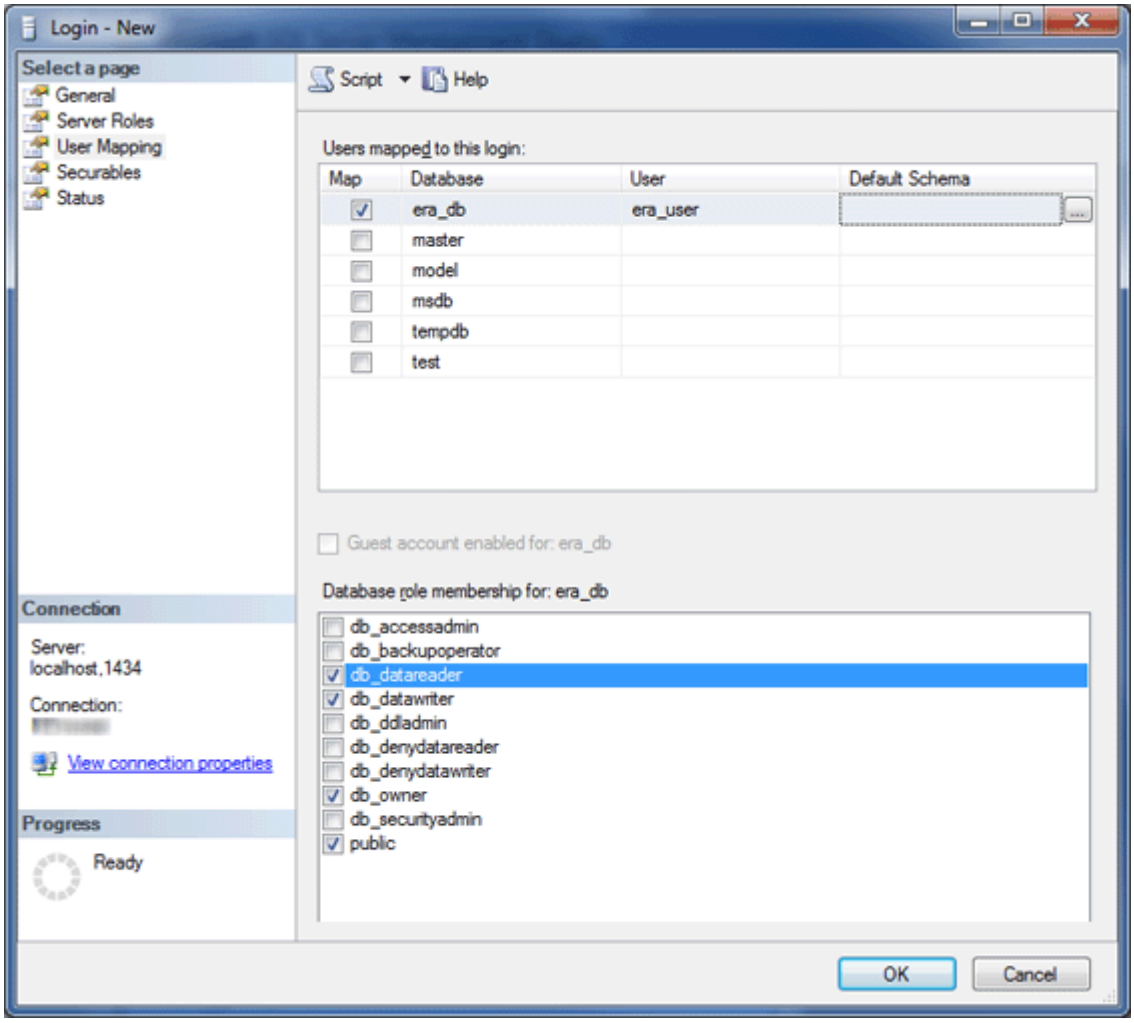
- Συνιστώμενοι χαρακτήρες για κωδικούς πρόσβασης: ΜΟΝΟ χαρακτήρες ASCII, που συμπεριλαμβάνουν κεφαλαία και πεζά γράμματα ASCII, αριθμούς, διαστήματα, ειδικούς χαρακτήρες

- Μη χρησιμοποιείτε χαρακτήρες που δεν είναι ASCII, αγκύλες {} ή @

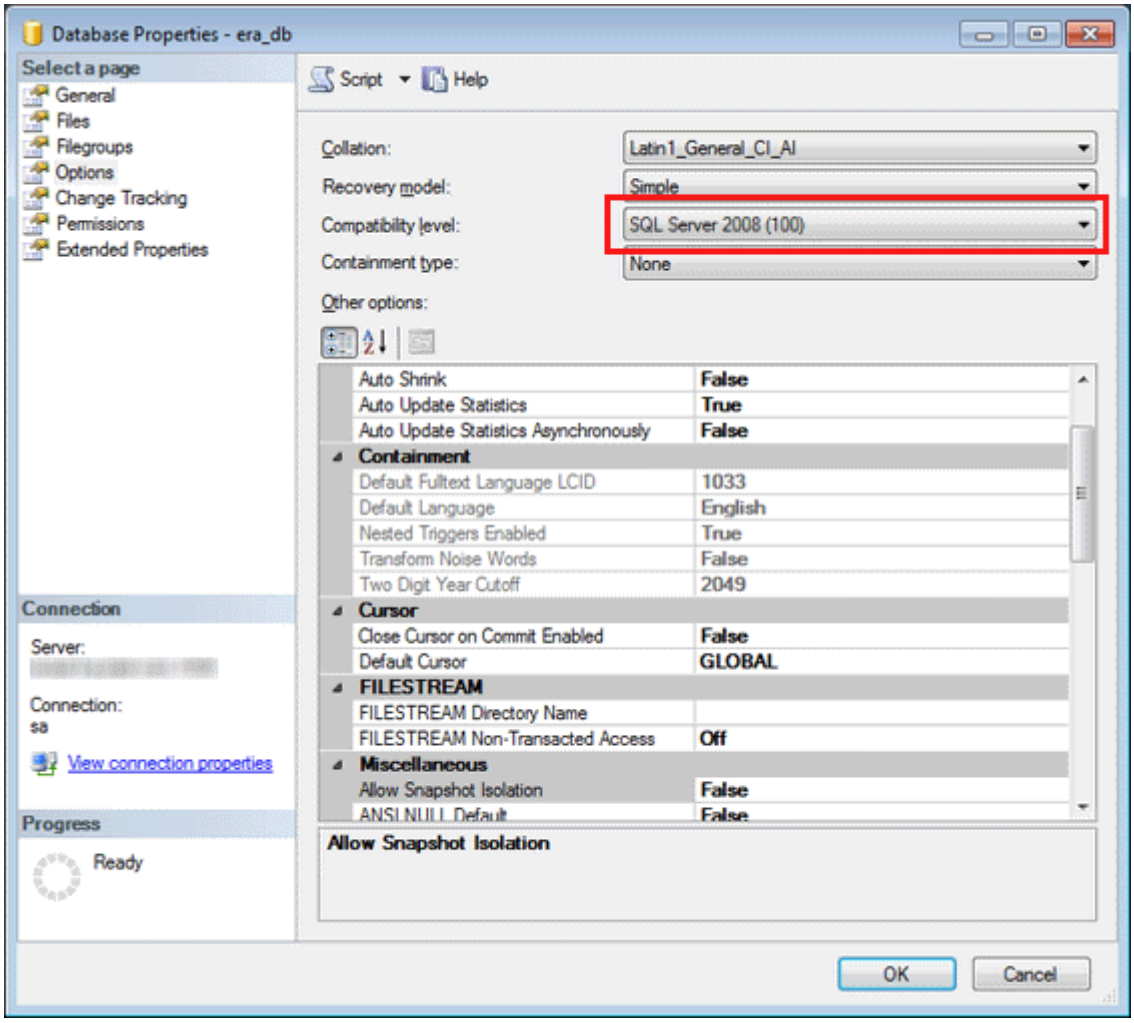
- Σημειώστε ότι εάν δεν ακολουθήσετε τις παραπάνω συστάσεις χαρακτήρων, μπορεί να αντιμετωπίσετε προβλήματα συνδεσιμότητας της βάσης δεδομένων ή θα πρέπει να πραγματοποιήσετε διαφυγή των ειδικών χαρακτήρων σε επόμενα βήματα, κατά την τροποποίηση της συμβολοσειράς σύνδεσης της βάσης δεδομένων. Οι κανόνες διαφυγής χαρακτήρων δεν περιλαμβάνονται σε αυτό το έγγραφο.



17. Χαρτογραφήστε τη σύνδεση με ένα χρήστη στη βάση δεδομένων προορισμού. Στην καρτέλα **χαρτογραφήσεων χρήστη**, βεβαιωθείτε ότι ο χρήστης βάσης δεδομένων έχει τους εξής ρόλους: **db_datareader**, **db_datawriter**, **db_owner**.

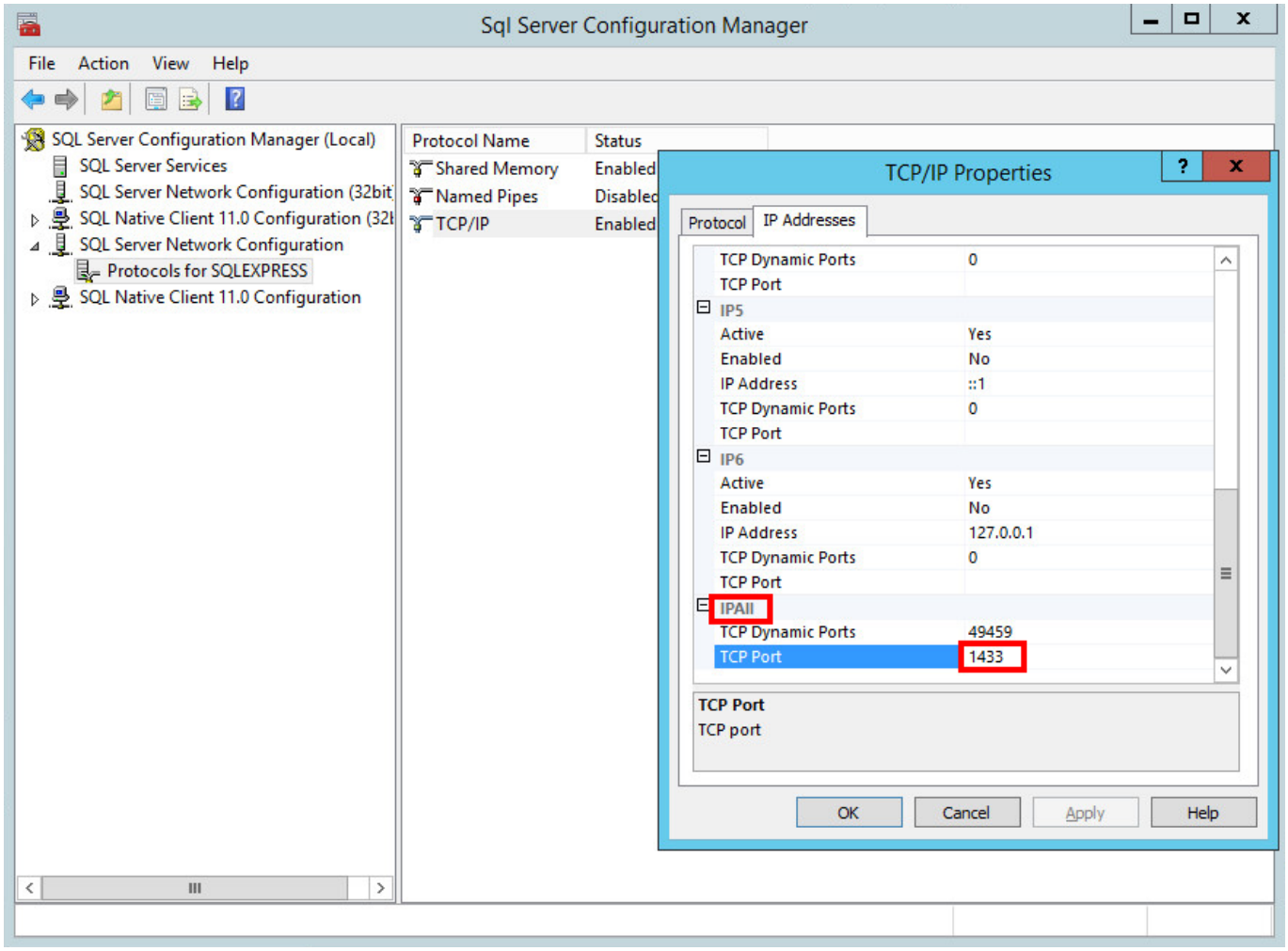


18. Για να ενεργοποιηθούν οι πιο πρόσφατες δυνατότητες του διακομιστή βάσης δεδομένων, αλλάξτε το **Επίπεδο συμβατότητας** της βάσης δεδομένων επαναφοράς στο πιο πρόσφατο. Κάντε δεξί κλικ στη νέα βάση δεδομένων και ανοίξτε τις **Ιδιότητες** της βάσης δεδομένων.



> Το SQL Server Management Studio δεν μπορεί να ορίζει επίπεδα συμβατότητας που είναι πιο πρόσφατα από την έκδοση που χρησιμοποιείται. Για παράδειγμα, το SQL Server Management Studio 2014 δεν μπορεί να ορίσει επίπεδο συμβατότητας για το SQL Server 2019.

19. Βεβαιωθείτε ότι το πρωτόκολλο σύνδεσης **TCP/IP** είναι **ενεργοποιημένο** για το στοιχείο "db_instance_name"(π.χ. SQLEXPRESS ή MSSQLSERVER) και ότι η **θύρα** TCP/IP έχει οριστεί στην τιμή **1433**. Για να το κάνετε αυτό, ανοίξτε το **Διαχείριση διαμόρφωσης του Sql Server**, μεταβείτε στο στοιχείο **Διαμόρφωση δικτύου SQL Server** > **Πρωτόκολλα για db_instance_name**, κάντε δεξί κλικ στο στοιχείο **TCP/IP** και επιλέξτε **Ενεργοποιημένο**. Κάντε διπλό κλικ στο στοιχείο **TCP/IP**, μεταβείτε στην καρτέλα **Πρωτόκολλα**, κάντε κύλιση προς τα κάτω στο στοιχείο **IPAll** και, στο πεδίο **Θύρα TCP**, πληκτρολογήστε 1433. Κάντε κλικ στο **OK** και επανεκκινήστε την υπηρεσία **SQL Server**.



20. Συνδέστε το διακομιστή ESET PROTECT ή το MDM με τη βάση δεδομένων.

Διαδικασία μετεγκατάστασης για το MySQL Server

Προαπαιτούμενα

• Πρέπει να εγκατασταθούν εμφανίσεις SQL Server προέλευσης και προορισμού. Μπορούν να φιλοξενούνται σε διαφορετικούς υπολογιστές.

• Τα εργαλεία MySQL πρέπει να είναι διαθέσιμα σε τουλάχιστον έναν από τους υπολογιστές (υπολογιστής-πελάτης `mysqldump` και mysql).

Χρήσιμοι σύνδεσμοι

- https://dev.mysql.com/doc/refman/8.0/en/copying-databases.html
- https://dev.mysql.com/doc/refman/8.0/en/mysqldump.html
- https://dev.mysql.com/doc/refman/8.0/en/mysql.html

Διαδικασία μετεγκατάστασης

Στις εντολές, τα αρχεία διαμόρφωσης ή τις δηλώσεις SQL παρακάτω, να αντικαθιστάτε πάντα τα εξής:
• Το **SRCHOST** με τη διεύθυνση του διακομιστή βάσης δεδομένων προέλευσης
• Το **SRCROOTLOGIN** με τη σύνδεση χρήστη ρίζας του διακομιστή MySQL προέλευσης
• Το **SRCDBNAME** με το όνομα της βάσης δεδομένων ESET PROTECT προέλευσης, για την οποία θα δημιουργηθεί αντίγραφο ασφαλείας
• Το **BACKUPFILE** με τη διαδρομή προς το αρχείο στο οποίο θα αποθηκευτεί το αντίγραφο ασφαλείας
• Το **TARGETROOTLOGIN** με τη σύνδεση χρήστη ρίζας του διακομιστή MySQL προορισμού
• Το **TARGETHOST** με τη διεύθυνση του διακομιστή βάσης δεδομένων προορισμού
• Το **TARGETDBNAME** με το όνομα της βάσης δεδομένων ESET PROTECT προορισμού (μετά τη μετεγκατάσταση)
• Το **TARGETLOGIN** με το όνομα σύνδεσης του χρήστη της νέας βάσης δεδομένων ESET PROTECT στο διακομιστή βάσης δεδομένων προορισμού
• Το **TARGETPASSWD** με τον κωδικό πρόσβασης του χρήστη της νέας βάσης δεδομένων ESET PROTECT στο διακομιστή βάσης δεδομένων προορισμού

Δεν είναι απαραίτητο να εκτελέσετε τις παρακάτω δηλώσεις SQL μέσω της γραμμής εντολών. Εάν υπάρχει διαθέσιμο εργαλείο γραφικού περιβάλλοντος χρήστη, μπορείτε να χρησιμοποιήσετε μια εφαρμογή που γνωρίζετε ήδη.

1. Διακόψτε τις υπηρεσίες διακομιστή/MDM ESET PROTECT.

2. Δημιουργία πλήρους αντιγράφου ασφαλείας βάσης δεδομένων της βάσης δεδομένων ESET PROTECT προέλευσης (η βάση δεδομένων που σκοπεύετε να μετεγκαταστήσετε):

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -
u SRCROOTLOGIN -p SRCDBNAME > BACKUPFILE
```

3. Προετοιμασία μιας κενής βάσης δεδομένων στο διακομιστή MySQL προορισμού:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE DATABASE TARGETDBNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

Σε συστήματα Linux, χρησιμοποιήστε το χαρακτήρα αποστρόφου ' αντί για τα εισαγωγικά ".

4. Επαναφορά της βάσης δεδομένων στο διακομιστή MySQL προορισμού στην κενή βάση δεδομένων που προετοιμάσατε προηγουμένως:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDBNAME < BACKUPFILE
```

5. Δημιουργία ενός χρήστη βάσης δεδομένων ESET PROTECT στο διακομιστή MySQL προορισμού:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

Συνιστώμενοι χαρακτήρες για το **TARGETLOGIN**:

- Πεζά γράμματα ASCII, αριθμοί και κάτω παύλα «_»

Συνιστώμενοι χαρακτήρες για το **TARGETPASSWD**:

- Μόνο χαρακτήρες ASCII, που συμπεριλαμβάνουν κεφαλαία και πεζά γράμματα ASCII, αριθμούς, διαστήματα και ειδικούς χαρακτήρες
- Μη χρησιμοποιείτε χαρακτήρες που δεν είναι ASCII, αγκύλες {} ή @

Σημειώστε ότι εάν δεν ακολουθήσετε τις παραπάνω συστάσεις χαρακτήρων, μπορεί να αντιμετωπίσετε προβλήματα συνδεσιμότητας της βάσης δεδομένων ή θα πρέπει να πραγματοποιήσετε διαφυγή των ειδικών χαρακτήρων σε επόμενα βήματα, κατά την τροποποίηση της συμβολοσειράς σύνδεσης της βάσης δεδομένων. Οι κανόνες διαφυγής χαρακτήρων δεν περιλαμβάνονται σε αυτό το έγγραφο.

6. Χορήγηση κατάλληλων δικαιωμάτων πρόσβασης στο χρήστη της βάσης δεδομένων ESET PROTECT στο διακομιστή MySQL προορισμού:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=GRANT ALL ON TARGETDBNAME.* TO TARGETLOGIN;"
```

> Σε συστήματα Linux, χρησιμοποιήστε το χαρακτήρα αποστρόφου ' αντί για τα εισαγωγικά ".

7. Καταργήστε τα περιεχόμενα του πίνακα **tbl_authentication_certificate** (διαφορετικά οι φορείς μπορεί να μη συνδέονται με τον νέο διακομιστή):

```
 mysql --host TARGETHOST -u root -p "--
execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. Συνδέστε το διακομιστή ESET PROTECT ή το MDM με τη βάση δεδομένων.

Συνδέστε το διακομιστή ESET PROTECT ή το MDM με μια βάση δεδομένων

Ακολουθήστε τα παρακάτω βήματα στον υπολογιστή στον οποίο έχει εγκατασταθεί ο διακομιστής ESET PROTECT ή το MDM ESET PROTECT για να τον συνδέσετε με μια βάση δεδομένων.

1. Διακόψτε την υπηρεσία διακομιστή/MDM ESET PROTECT.

2. Βρείτε το αρχείο *startupconfiguration.ini*

   - Windows:

Διακομιστής :

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configurati
on\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configurat
ion\startupconfiguration.ini
```

- Linux:

Διακομιστής :

```
/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

MDMCore:

```
/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini
```

3. Αλλάξτε τη συμβολοσειρά σύνδεσης βάσης δεδομένων στο αρχείο *startupconfiguration.ini* του διακομιστή/MDM ESET PROTECT

oΡυθμίστε τη διεύθυνση και τη θύρα του νέου διακομιστή βάσης δεδομένων.

oΡυθμίστε νέο όνομα χρήστη και κωδικό πρόσβασης για το ESET PROTECT στη συμβολοσειρά σύνδεσης.

Το τελικό αποτέλεσμα θα πρέπει να φαίνεται ως εξής:

- Microsoft SQL:

```
DatabaseType=MSSQLOdbc

DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pw
d={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

- MySQL:

```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port
=3306;User=TARGETLOGIN;
Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

Στην παραπάνω ρύθμιση παραμέτρων, να γίνεται πάντα αντικατάσταση στα εξής:
• Το **TARGETHOST** με τη διεύθυνση του διακομιστή βάσης δεδομένων προορισμού
• Το **TARGETDBNAME** με το όνομα της βάσης δεδομένων ESET PROTECT προορισμού (μετά τη μετεγκατάσταση)
• Το **TARGETLOGIN** με το όνομα σύνδεσης του χρήστη της νέας βάσης δεδομένων ESET PROTECT στο διακομιστή βάσης δεδομένων προορισμού
• Το **TARGETPASSWD** με τον κωδικό πρόσβασης του χρήστη της νέας βάσης δεδομένων ESET PROTECT στο διακομιστή βάσης δεδομένων προορισμού

4. Εκκινήστε το διακομιστή ESET PROTECT ή το MDM ESET PROTECT και επαληθεύστε ότι η υπηρεσία εκτελείται σωστά.

Μετεγκατάσταση του MDM

Το στοιχείο Διαχείριση/Σύνδεση κινητών συσκευών (Διαχείριση κινητών συσκευών/MDC) του ESET PROTECT (μόνο εσωτερικής εγκατάστασης) φτάνει στο τέλος του κύκλου ζωής τον Ιανουάριο του 2024. Διαβάστε περισσότερα. Συνιστάται η μετεγκατάσταση στο cloud διαχείρισης κινητών συσκευών.

Για να μετεγκαταστήσετε τη διαχείριση κινητών συσκευών (εσωτερικής εγκατάστασης) από έναν διακομιστή σε έναν άλλο διακομιστή, ακολουθήστε τις παρακάτω οδηγίες.

Μετεγκατάσταση της διαχείρισης κινητών συσκευών από έναν διακομιστή σε έναν άλλο διακομιστή (εσωτερικής εγκατάστασης)

Σκοπός αυτής της διαδικασίας είναι η μετεγκατάσταση της υπάρχουσας εμφάνισης του MDM ESET PROTECT και η **διατήρηση της υπάρχουσας βάσης δεδομένων MDM ESET PROTECT**, συμπεριλαμβανομένων των εγγεγραμμένων κινητών συσκευών. Το μετεγκατεστημένο MDM ESET PROTECT θα έχει **την ίδια διεύθυνση IP/το ίδιο όνομα κεντρικού υπολογιστή** με το παλιό MDM ESET PROTECT και η βάση δεδομένων του παλιού MDM ESET PROTECT θα εισαχθεί στον κεντρικό υπολογιστή του νέου MDM πριν από την εγκατάσταση.

• Η Μετεγκατάσταση βάσεων δεδομένων υποστηρίζεται μόνο ανάμεσα σε ταυτόσημες βάσεις δεδομένων (από MySQL σε MySQL ή από Microsoft SQL σε Microsoft SQL).
• Όταν μετεγκαθιστάτε μια βάση δεδομένων, η μετεγκατάσταση πρέπει να γίνεται ανάμεσα σε εμφανίσεις ίδιας έκδοσης του ESET PROTECT On-Prem. Ανατρέξτε στο άρθρο της Γνωσιακής βάσης για οδηγίες σχετικά με τον τρόπο προσδιορισμού της έκδοσης των στοιχείων ESET PROTECT. Αφού ολοκληρώσετε τη μετεγκατάσταση της βάσης δεδομένων, μπορείτε να πραγματοποιήσετε αναβάθμιση, εάν χρειάζεται, για να αποκτήσετε την πιο πρόσφατη έκδοση του ESET PROTECT On-Prem.

I. Στον τρέχοντα (παλιό) διακομιστή MDM ESET PROTECT:

1. Δημιουργήστε ένα αντίγραφο ασφαλείας της ρύθμισης παραμέτρων MDM.

a)Στο στοιχείο **Υπολογιστές** κάντε κλικ στο στοιχείο «Διακομιστής MDM» και επιλέξτε **Λεπτομέρειες**.

b)Κάντε κλικ στο στοιχείο **Ρύθμιση παραμέτρων** > **Αίτημα ρύθμισης παραμέτρων**. Ενδέχεται να χρειαστεί να περιμένετε λίγο (ανάλογα με το χρονικό διάστημα σύνδεσης του Φορέα σας) μέχρι να δημιουργηθεί η ρύθμιση παραμέτρων που ζητήθηκε.

c)Κάντε κλικ στο **ESET PROTECT Mobile Device Connector** και επιλέξτε το στοιχείο **Άνοιγμα ρύθμισης παραμέτρων**.

d)Εξαγάγετε τα παρακάτω στοιχεία από τη ρύθμιση παραμέτρων στον εξωτερικό χώρο αποθήκευσης:

- Το ακριβές όνομα κεντρικού υπολογιστή του διακομιστή MDM.
- Ομότιμα πιστοποιητικά - Το αρχείο *.pfx* που θα εξαγάγετε θα περιλαμβάνει το ιδιωτικό κλειδί.

> Εάν εκτελείτε τον διακομιστή MDM ESET PROTECT σε Linux, πρέπει να εξαγάγετε το πιστοποιητικό HTTPS από την πολιτική ρύθμισης παραμέτρων MDM:
> I.Κάντε κλικ στο στοιχείο **Προβολή** που βρίσκεται δίπλα στο στοιχείο **Πιστοποιητικό HTTPS**.
> II.Κάντε κλικ στο στοιχείο **Λήψη** και πραγματοποιήστε λήψη του πιστοποιητικού HTTPS σε μορφή PFX.

e)Εξαγάγετε και τα ακόλουθα πιστοποιητικά και σύμβολα, εάν υπάρχουν:

- Το πιστοποιητικό υπογραφής προφίλ εγγραφής.
- Ένα πιστοποιητικό APNS (εξαγωγή τόσο του πιστοποιητικού APNS όσο και του ιδιωτικού κλειδιού APNS).
- Σύμβολο εξουσιοδότησης Apple Business Manager (ABM).

2. Διακόψτε την υπηρεσία MDM ESET PROTECT.

3. Εξαγάγετε/δημιουργήστε αντίγραφα ασφαλείας για τη βάση δεδομένων MDM ESET PROTECT.

4. Απενεργοποιήστε τον τρέχοντα υπολογιστή του MDM ESET PROTECT.

> Μη καταργήσετε την εγκατάσταση/αποσύρετε ακόμη το παλιό MDM ESET PROTECT.

II. Στον νέο διακομιστή MDM ESET PROTECT:

> Βεβαιωθείτε ότι η διαμόρφωση δικτύου στον νέο σας διακομιστή MDM ESET PROTECT (το όνομα κεντρικού υπολογιστή που εξαγάγατε από τη διαμόρφωση του «παλιού» διακομιστή MDM) συμφωνεί με τη διαμόρφωση του παλιού MDM ESET PROTECT.

1. Εγκαταστήστε/εκκινήστε μια υποστηριζόμενη ESET PROTECT βάση δεδομένων MDM.

2. Εισαγάγετε/επαναφέρετε τη βάση δεδομένων MDM ESET PROTECT από το παλιό MDM ESET PROTECT.

3. Εγκαταστήστε τον διακομιστή/το MDM ESET PROTECT χρησιμοποιώντας την εγκατάσταση

πακέτου «όλα σε ένα» (Windows) ή επιλέξτε άλλη μέθοδο εγκατάστασης (μη αυτόματη εγκατάσταση στα Windows, Linux ή εικονική συσκευή). Καθορίστε τις ρυθμίσεις σύνδεσης της βάσης δεδομένων σας κατά την εγκατάσταση του MDM ESET PROTECT.

Κατά την εγκατάσταση του ESET PROTECT MDM σε Linux, χρησιμοποιήστε το πιστοποιητικό HTTPS από το αντίγραφο ασφαλείας σας.

4. Συνδεθείτε στην κονσόλα διαδικτύου του ESET PROTECT.

5. Κάντε επανεκκίνηση της υπηρεσίας ESET PROTECT.

Οι διαχειριζόμενες κινητές συσκευές θα πρέπει τώρα να συνδέονται στον νέο διακομιστή MDM ESET PROTECT με τη χρήση του αρχικού τους πιστοποιητικού.

III. Κατάργηση εγκατάστασης παλιού διακομιστή/MDM ESET PROTECT:

Εφόσον όλα λειτουργούν κανονικά με τον νέο σας διακομιστή ESET PROTECT, αποσύρετε προσεκτικά τον παλιό διακομιστή/το παλιό MDM ESET PROTECT ακολουθώντας τις οδηγίες βήμα προς βήμα.

Αλλαγή διεύθυνσης IP ή ονόματος κεντρικού υπολογιστή στο διακομιστή ESET PROTECT μετά από μετεγκατάσταση

Για να αλλάξετε μια διεύθυνση IP ή όνομα κεντρικού υπολογιστή στο διακομιστή ESET PROTECT, ακολουθήστε τα εξής βήματα:

1. Εάν το πιστοποιητικό του διακομιστή ESET PROTECT περιέχει μια συγκεκριμένη διεύθυνση IP ή/και όνομα κεντρικού υπολογιστή, δημιουργήστε ένα νέο πιστοποιητικό διακομιστή και συμπεριλάβετε τη νέα διεύθυνση IP ή το νέο όνομα κεντρικού υπολογιστή. Ωστόσο, εάν υπάρχει ειδικός χαρακτήρας (*) στο πεδίο κεντρικού υπολογιστή του πιστοποιητικού διακομιστή, **μεταβείτε στο βήμα 2**. Εάν όχι, δημιουργήστε νέο πιστοποιητικό διακομιστή προσθέτοντας τη νέα διεύθυνση IP ή το νέο όνομα κεντρικού υπολογιστή διαχωρισμένα με κόμμα, συμπεριλαμβάνοντας επίσης την προηγούμενη διεύθυνση IP και όνομα κεντρικού υπολογιστή.

2. Υπογράψτε το νέο πιστοποιητικό διακομιστή χρησιμοποιώντας την Αρχή έκδοσης πιστοποιητικών του διακομιστή ESET PROTECT.

3. Δημιουργήστε μια πολιτική αλλάζοντας τις συνδέσεις υπολογιστή-πελάτη με τη νέα διεύθυνση IP ή το νέο όνομα κεντρικού υπολογιστή (κατά προτίμηση με τη διεύθυνση IP), αλλά συμπεριλάβετε και μια δεύτερη (εναλλακτική) σύνδεση με την παλιά διεύθυνση IP ή το παλιό όνομα κεντρικού υπολογιστή, για να δώσετε στο Φορέα ESET Management τη δυνατότητα να συνδέεται και στους δυο διακομιστές. Για περισσότερες λεπτομέρειες, ανατρέξτε στην ενότητα Δημιουργία πολιτικής για τη σύνδεση των φορέων ESET Management με τον νέο διακομιστή ESET PROTECT.

4. Εφαρμόστε αυτή την πολιτική στους υπολογιστές-πελάτες σας και επιτρέψτε στους Φορείς ESET Management να την αντιγράψουν. Ακόμη κι αν η πολιτική ανακατευθύνει τους υπολογιστές-

πελάτες στον νέο σας διακομιστή (ο οποίος δεν εκτελείται), οι Φορείς ESET Management θα χρησιμοποιούν τις εναλλακτικές πληροφορίες διακομιστή για να πραγματοποιηθεί σύνδεση με την αρχική διεύθυνση IP.

5. Ρυθμίστε το νέο πιστοποιητικό διακομιστή στη διαδρομή Περισσότερα > Ρυθμίσεις.

6. Επανεκκινήστε την υπηρεσία του διακομιστή ESET PROTECT και αλλάξτε τη διεύθυνση IP ή το όνομα κεντρικού υπολογιστή.

Ανατρέξτε στο σχετικό άρθρο της Γνωσιακής βάσης για εικονογραφημένες οδηγίες αλλαγής της διεύθυνσης του διακομιστή ESET PROTECT.

Κατάργηση εγκατάστασης του διακομιστή ESET PROTECT και των στοιχείων του

Επιλέξτε ένα από τα παρακάτω κεφάλαια για να καταργήσετε την εγκατάσταση του Διακομιστή ESET PROTECT και των στοιχείων του:

- Κατάργηση εγκατάστασης του Φορέα ESET Management
- Windows - Κατάργηση εγκατάστασης του διακομιστή ESET PROTECT και των στοιχείων του
- Linux - Αναβάθμιση, επανεγκατάσταση ή κατάργηση εγκατάστασης στοιχείων του ESET PROTECT
- macOS - Κατάργηση εγκατάστασης του φορέα ESET Management και του προϊόντος ESET Endpoint
- Παροπλίστε τον παλιό διακομιστή ESET PROTECT/MDM μετά τη μετεγκατάσταση σε άλλον διακομιστή

Κατάργηση εγκατάστασης του Φορέα ESET Management

Μπορείτε να καταργήσετε την εγκατάσταση του φορέα ESET Management με διάφορους τρόπους.

Απομακρυσμένη κατάργηση εγκατάστασης με την κονσόλα διαδικτύου ESET PROTECT

1. Συνδεθείτε στην κονσόλα διαδικτύου ESET PROTECT.

2. Από το πλαίσιο **Υπολογιστές**, επιλέξτε έναν υπολογιστή από τον οποίο θέλετε να καταργήσετε το φορέα ESET Management και κάντε κλικ στο στοιχείο **Νέα εργασία**.

Εναλλακτικά, επιλέξτε πολλούς υπολογιστές ταυτόχρονα επιλέγοντας τα αντίστοιχα πλαίσια ελέγχου και κατόπιν κάντε κλικ στα στοιχεία **Υπολογιστής** > **Εργασίες** > **Νέα εργασία**.

3. Πληκτρολογήστε ένα **Όνομα** για την εργασία.

4. Από το αναπτυσσόμενο μενού **Κατηγορία εργασίας**, επιλέξτε **ESET PROTECT On-Prem**.

5. Από το αναπτυσσόμενο μενού **Εργασία**, επιλέξτε Διακοπή διαχείρισης (Κατάργηση εγκατάστασης φορέα ESET Management).

Όταν καταργήσετε την εγκατάσταση του Φορέα ESET Management από τον υπολογιστή-πελάτη, η διαχείριση της συσκευής δεν γίνεται πλέον από το ESET PROTECT On-Prem:
• Το προϊόν ασφάλειας ESET μπορεί να διατηρήσει ορισμένες ρυθμίσεις μετά την κατάργηση εγκατάστασης του Φορέα ESET Management.
• Εάν ο Φορέας ESET Management προστατεύεται με κωδικό πρόσβασης, πρέπει να συμπληρώσετε τον κωδικό πρόσβασης για να πραγματοποιήσετε κατάργηση εγκατάστασης, επιδιόρθωση ή αναβάθμιση (με αλλαγές). Προτού καταργήσετε τη συσκευή από τη διαχείριση, συνιστάται να κάνετε επαναφορά ορισμένων ρυθμίσεων που δεν θέλετε να διατηρήσετε (για παράδειγμα, προστασία κωδικού πρόσβασης) στις προεπιλεγμένες ρυθμίσεις, χρησιμοποιώντας μια πολιτική.
• Όλες οι εργασίες που εκτελούνται στο φορέα θα εγκαταλειφθούν. Η κατάσταση εκτέλεσης **Εκτελείται**, **Ολοκληρώθηκε** ή **Αποτυχία** αυτής της εργασίας μπορεί να μην εμφανιστεί με ακρίβεια στην κονσόλα διαδικτύου ESET PROTECT ανάλογα με την αντιγραφή.
• Μετά την κατάργηση της εγκατάστασης του φορέα, μπορείτε να διαχειριστείτε το προϊόν ασφάλειας μέσω του ενσωματωμένου EGUI ή του eShell.

6. Εξετάστε την **Περίληψη** της εργασίας και κάντε κλικ στο κουμπί '**Τέλος**'.

7. Κάντε κλικ στο στοιχείο Δημιουργία ερεθίσματος, για να καθορίσετε πότε θα πρέπει να εκτελείται αυτή η εργασία υπολογιστή-πελάτη και σε ποια στοιχεία στην επιλογή **Προορισμοί**.

Τοπική κατάργηση εγκατάστασης - Windows

Δείτε επίσης τις οδηγίες για την τοπική κατάργηση εγκατάστασης του Φορέα ESET Management σε Linux ή macOS.
Για την αντιμετώπιση προβλημάτων κατά την κατάργηση εγκατάστασης του Φορέα, ανατρέξτε στο θέμα Αντιμετώπιση προβλημάτων κατά την κατάργηση εγκατάστασης του Φορέα ESET Management.

1. Συνδεθείτε στον τερματικό υπολογιστή όπου θέλετε να καταργήσετε το φορέα ESET Management (για παράδειγμα, μέσω RDP).

2. Μεταβείτε στη θέση **Πίνακας Ελέγχου** > **Προγράμματα και δυνατότητες** και κάντε διπλό κλικ στο στοιχείο **Φορέας ESET Management**.

3. Κάντε κλικ στο κουμπί **Επόμενο** > **Κατάργηση** και ακολουθήστε τις οδηγίες κατάργησης εγκατάστασης.

Εάν έχετε καθορίσει κωδικό πρόσβασης χρησιμοποιώντας μια πολιτική για τους φορείς ESET Management, έχετε τις ακόλουθες επιλογές:
• Θα χρειαστεί να πληκτρολογήσετε τον κωδικό πρόσβασης κατά την κατάργηση εγκατάστασης.
• Καταργήστε πρώτα την αντιστοίχιση αυτής της πολιτικής προτού καταργήσετε την εγκατάσταση του φορέα ESET Management.
• Αναπτύξτε εκ νέου το φορέα ESET Management επάνω από έναν υπάρχοντα φορέα που προστατεύεται με κωδικό πρόσβασης (ένα άρθρο της Γνωσιακής βάσης).

Windows - Κατάργηση εγκατάστασης του διακομιστή ESET PROTECT και των στοιχείων του

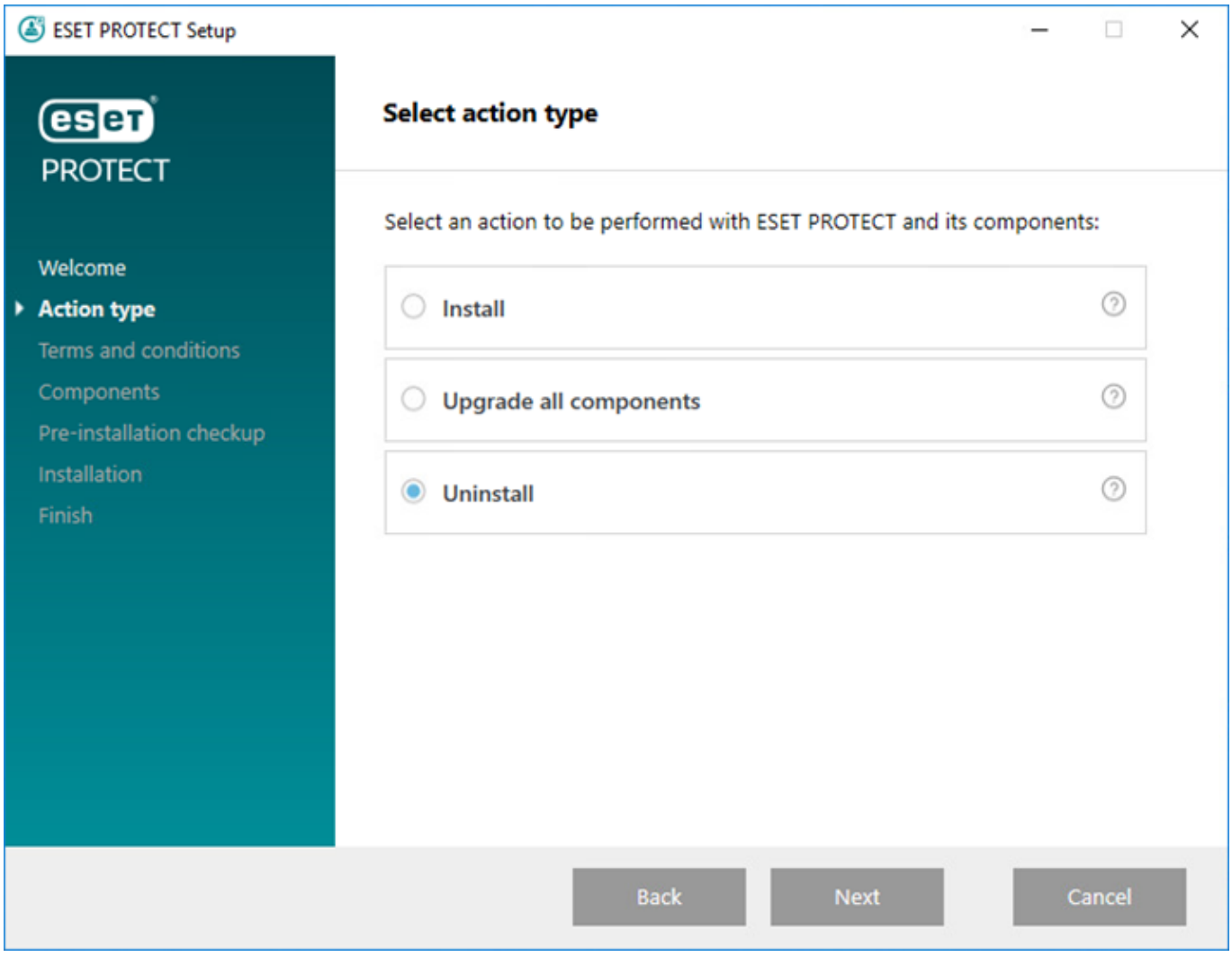
Πριν από την κατάργηση εγκατάστασης του ESET PROTECT On-Prem, καταργήστε την εγκατάσταση των Φορέων σε διαχειριζόμενους υπολογιστές.
Προτού καταργήσετε τη Σύνδεση κινητών συσκευών, διαβάστε το κεφάλαιο Λειτουργικότητα αδειοδότησης MDM iOS.

Ακολουθήστε αυτά τα βήματα για να καταργήσετε την εγκατάσταση του Διακομιστή ESET PROTECT και των στοιχείων του στα Windows:

1. Πραγματοποιήστε λήψη του Προγράμματος εγκατάστασης «Όλα σε ένα» του ESET PROTECT και αποσυμπιέστε το πακέτο.

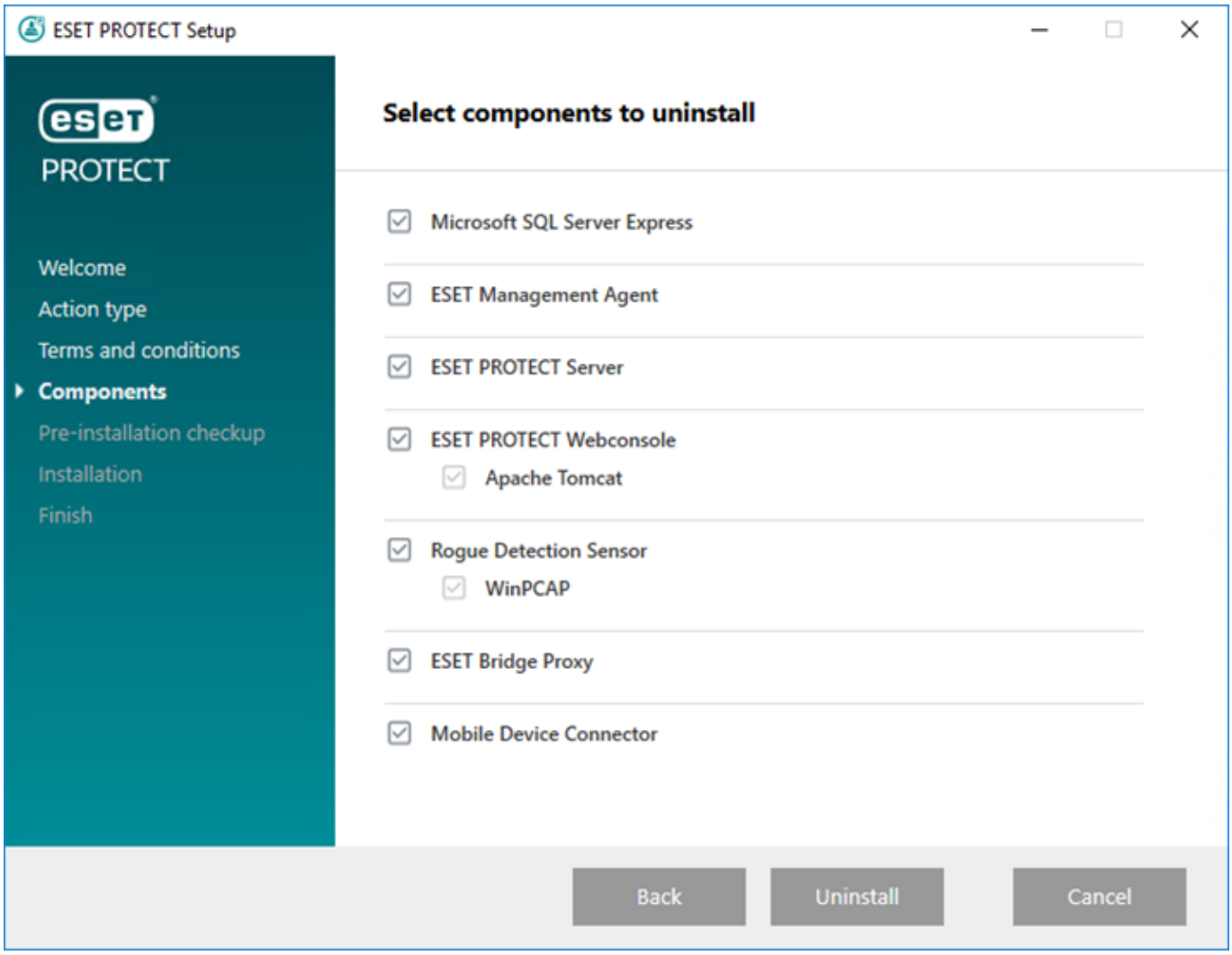
2. Εκτελέστε το αρχείο *Setup.exe*. Μπορείτε να επιλέξετε τη **Γλώσσα** από το αναπτυσσόμενο μενού. Κάντε κλικ στο στοιχείο**Επόμενο**.

3. Επιλέξτε **Απεγκατάσταση** και κάντε κλικ στο στοιχείο **Επόμενο**.



4. Αποδεχτείτε την Άδεια χρήσης τελικού χρήστη (EULA) και κάντε κλικ στην επιλογή **Επόμενο**.

5. Επιλέξτε το ή τα στοιχεία που θέλετε να απεγκαταστήσετε και κάντε κλικ στο στοιχείο **Απεγκατάσταση**.



6. Ίσως απαιτείται επανεκκίνηση του υπολογιστή, προκειμένου να ολοκληρωθεί η κατάργηση ορισμένων στοιχείων.

Δείτε επίσης Παροπλίστε τον παλιό διακομιστή ESET PROTECT On-Prem/MDM μετά τη μετεγκατάσταση σε άλλον διακομιστή.

Linux - Αναβάθμιση, επανεγκατάσταση ή κατάργηση εγκατάστασης στοιχείων του ESET PROTECT

Εάν θέλετε να επανεγκαταστήσετε ή να αναβαθμίσετε σε πιο πρόσφατη έκδοση, εκτελέστε ξανά τη δέσμη ενεργειών εγκατάστασης.

Για να καταργήσετε την εγκατάσταση ενός στοιχείου (σε αυτή την περίπτωση του Διακομιστή ESET PROTECT), εκτελέστε το πρόγραμμα εγκατάστασης με την παράμετρο `--uninstall`, όπως φαίνεται

παρακάτω:

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

Εάν θέλετε να καταργήσετε την εγκατάσταση άλλου στοιχείου, χρησιμοποιήστε το κατάλληλο όνομα πακέτου στην εντολή. Για παράδειγμα, φορέας ESET Management:

```
sudo ./agent-linux-x86_64.sh --uninstall
```

Τα αρχεία διαμόρφωσης και βάσης δεδομένων θα καταργηθούν κατά την κατάργηση της εγκατάστασης. Για να διατηρήσετε τα αρχεία βάσης δεδομένων, δημιουργήστε ένα αρχείο τοποθέτησης SQL της βάσης δεδομένων ή χρησιμοποιήστε την παράμετρο `--keep-database`.

Μετά την κατάργηση της εγκατάστασης, επαληθεύστε εάν

- διαγράφηκε η υπηρεσία `eraserver`.
- διαγράφηκε ο φάκελος `/etc/opt/eset/RemoteAdministrator/Server/`.

Συνιστάται να δημιουργήσετε ένα αντίγραφο ασφαλείας του αρχείου τοποθέτησης της βάσης δεδομένων προτού καταργήσετε την εγκατάσταση, σε περίπτωση που χρειαστεί να κάνετε επαναφορά των δεδομένων σας.
Για περισσότερες πληροφορίες σχετικά με την επανεγκατάσταση του Φορέα, ανατρέξτε στο σχετικό κεφάλαιο.
Για την αντιμετώπιση προβλημάτων κατά την κατάργηση εγκατάστασης του Φορέα, ανατρέξτε στο θέμα Αντιμετώπιση προβλημάτων κατά την κατάργηση εγκατάστασης του Φορέα ESET Management.

macOS - Κατάργηση εγκατάστασης του φορέα ESET Management και του προϊόντος ESET Endpoint

Καταργήστε την εγκατάσταση του φορέα ESET Management και του προϊόντος ESET Endpoint τοπικά ή απομακρυσμένα μέσω του ESET PROTECT On-Prem.

Μπορείτε να βρείτε πιο λεπτομερείς οδηγίες για την τοπική κατάργηση εγκατάστασης του φορέα ESET Management και του προϊόντος ESET Endpoint στο άρθρο της Γνωσιακής βάσης.

Εάν θέλετε να καταργήσετε την εγκατάσταση του προϊόντος ESET Endpoint απομακρυσμένα, βεβαιωθείτε ότι το κάνετε πριν καταργήσετε την εγκατάσταση του φορέα ESET Management.

Κατάργηση εγκατάστασης του φορέα ESET Management τοπικά

1. Κάντε κλικ στην επιλογή **Εύρεση** για να ανοίξετε ένα νέο παράθυρο **Εύρεση**.

2. Κάντε κλικ στην επιλογή **Εφαρμογές** > πατήστε παρατεταμένα το πλήκτρο **CTRL** > κάντε κλικ στην επιλογή **Φορέας ESET Management** > επιλέξτε **Εμφάνιση περιεχομένων πακέτου** από το

μενού περιβάλλοντος.

3. Μεταβείτε στα στοιχεία **Περιεχόμενα** > **Δέσμες ενεργειών** και κάντε διπλό κλικ στην εντολή **Uninstaller.command** για να εκτελέσετε το πρόγραμμα κατάργησης εγκατάστασης.

4. Πληκτρολογήστε τον κωδικό πρόσβασης διαχειριστή και πατήστε το πλήκτρο **Enter** εάν σας ζητηθεί να εισαγάγετε κωδικό πρόσβασης.

5. Όταν καταργηθεί η εγκατάσταση του φορέα ESET Management, θα δείτε το μήνυμα **Η διεργασία ολοκληρώθηκε**.

Κατάργηση εγκατάστασης του φορέα ESET Management τοπικά μέσω τερματικού

1. Ανοίξτε τα στοιχεία **Εύρεση** > **Εφαρμογές** > **Βοηθητικά προγράμματα** > **Τερματικό**.

2. Πληκτρολογήστε τον ακόλουθο κωδικό και πατήστε το πλήκτρο **Enter**:

```
sudo /Applications/ESET\ Management\ Agent.app/Contents/Scripts/Uninstall.command ;
 exit;
```

3. Πληκτρολογήστε τον κωδικό πρόσβασης διαχειριστή και πατήστε το πλήκτρο **Enter** εάν σας ζητηθεί να εισαγάγετε κωδικό πρόσβασης.

4. Όταν καταργηθεί η εγκατάσταση του φορέα ESET Management, θα δείτε το μήνυμα **Η διεργασία ολοκληρώθηκε**.

Κατάργηση της εγκατάστασης του φορέα ESET Management απομακρυσμένα μέσω του ESET PROTECT On-Prem

Στην ενότητα **Υπολογιστές**, κάντε κλικ στον υπολογιστή-πελάτη macOS και επιλέξτε **Κατάργηση** για να καταργήσετε την εγκατάσταση του φορέα ESET Management και καταργήστε τον υπολογιστή από τη διαχείριση.

Για την αντιμετώπιση προβλημάτων κατά την κατάργηση εγκατάστασης του Φορέα, ανατρέξτε στο θέμα Αντιμετώπιση προβλημάτων κατά την κατάργηση εγκατάστασης του Φορέα ESET Management.

Κατάργηση εγκατάστασης του προϊόντος ESET Endpoint τοπικά

1. Κάντε κλικ στην επιλογή **Εύρεση** για να ανοίξετε ένα νέο παράθυρο **Εύρεση**.

2. Κάντε κλικ στο στοιχείο **Εφαρμογές** > πατήστε παρατεταμένα το πλήκτρο **CTRL** > κάντε κλικ στην επιλογή **ESET Endpoint Security** ή **ESET Endpoint Antivirus** > επιλέξτε **Εμφάνιση περιεχομένων πακέτου** από το μενού περιβάλλοντος.

3. Μεταβείτε στα στοιχεία **Περιεχόμενα** > **Βοηθοί** και κάντε διπλό κλικ στο στοιχείο **Uninstaller.app** για να εκτελέσετε το πρόγραμμα κατάργησης εγκατάστασης.

4. Κάντε κλικ στο στοιχείο **Κατάργηση εγκατάστασης**.

5. Πληκτρολογήστε τον κωδικό πρόσβασης διαχειριστή και κάντε κλικ στο **OK**, εάν σας ζητηθεί να εισαγάγετε έναν κωδικό πρόσβασης.

6. Όταν καταργηθεί η εγκατάσταση του ESET Endpoint Security ή του ESET Endpoint Antivirus, θα εμφανιστεί το μήνυμα **Η κατάργηση εγκατάστασης ήταν επιτυχής**. Κάντε κλικ στο κουμπί **Κλείσιμο**.

Κατάργηση εγκατάστασης του προϊόντος ESET Endpoint τοπικά μέσω τερματικού

1. Ανοίξτε τα στοιχεία **Εύρεση** > **Εφαρμογές** > **Βοηθητικά προγράμματα** > **Τερματικό**.

2. Πληκτρολογήστε τον ακόλουθο κωδικό και πατήστε το πλήκτρο **Enter**:

- Απεγκατάσταση ESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app
/Contents/Scripts/uninstall.sh
```

- Απεγκατάσταση ESET Endpoint Security:

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/Helpers/Uninstaller.app/
Contents/Scripts/uninstall.sh
```

3. Πληκτρολογήστε τον κωδικό πρόσβασης διαχειριστή και πατήστε το πλήκτρο **Enter** εάν σας ζητηθεί να εισαγάγετε κωδικό πρόσβασης.

4. Όταν καταργηθεί η εγκατάσταση του προϊόντος ESET Endpoint, θα δείτε το μήνυμα **Η διεργασία ολοκληρώθηκε**.

Κατάργηση εγκατάστασης του προϊόντος ESET Endpoint απομακρυσμένα μέσω του ESET PROTECT On-Prem

Για να καταργήσετε την εγκατάσταση του Φορέα ESET Management απομακρυσμένα μέσω του ESET PROTECT On-Prem, μπορείτε να χρησιμοποιήσετε μία από τις παρακάτω επιλογές:

- Στην ενότητα **Υπολογιστές**, κάντε κλικ στον υπολογιστή-πελάτη macOS, επιλέξτε **Λεπτομέρειες** > **Εγκατεστημένες εφαρμογές** > επιλέξτε **ESET Endpoint Security** ή **ESET Endpoint Antivirus** και κάντε κλικ στο κουμπί **Κατάργηση εγκατάστασης**.

- Χρησιμοποιήστε την εργασία **Κατάργηση εγκατάστασης λογισμικού**.

Παροπλίστε τον παλιό διακομιστή ESET PROTECT/MDM μετά τη μετεγκατάσταση σε άλλον διακομιστή

Βεβαιωθείτε ότι ο νέος διακομιστής/το νέο MDM ESET PROTECT εκτελείται και οι υπολογιστές-πελάτες και κινητές συσκευές συνδέονται σωστά στο νέο ESET PROTECT On-Prem.

Μετά τη μετεγκατάσταση σε άλλον διακομιστή, όταν αποσύρετε τον παλιό διακομιστή ESET PROTECT/MDM, έχετε τις εξής επιλογές:

I.**Διατήρηση του λειτουργικού συστήματος υπολογιστή διακομιστή και χρησιμοποίηση εκ νέου**

1. Διακόψτε την παλαιά υπηρεσία του διακομιστή ESET PROTECT.

2. Καταργήστε (`DROP DATABASE`) την παλιά εμφάνιση βάσης δεδομένων διακομιστή ESET PROTECT (Microsoft SQL ή MySQL).

Εάν έχετε μετεγκαταστήσει τη βάση δεδομένων στο νέο Διακομιστή ESET PROTECT, φροντίστε να καταργήσετε τη βάση δεδομένων στον παλιό Διακομιστή ESET PROTECT πριν την κατάργηση της εγκατάστασης για να αποτρέψετε την κατάργηση του συσχετισμού (την κατάργηση) των αδειών χρήσης από τη νέα βάση δεδομένων του Διακομιστή ESET PROTECT.

3. Καταργήστε την εγκατάσταση του παλιού διακομιστή ESET PROTECT On-Prem/MDM και όλων των στοιχείων του (συμπεριλαμβανομένου του φορέα ESET Management, του ανιχνευτή Rogue Detection Sensor, του MDM κ.λπ.):

   - Κατάργηση εγκατάστασης του ESET PROTECT On-Prem – Windows
   - Κατάργηση εγκατάστασης του ESET PROTECT On-Prem - Linux

Μη καταργήσετε την εγκατάσταση της βάσης δεδομένων σας, εάν υπάρχει άλλο λογισμικό που εξαρτάται από αυτήν.

4. Σχεδιάστε επανεκκίνηση του λειτουργικού συστήματος του διακομιστή σας μετά την κατάργηση εγκατάστασης

II.**Διατήρηση του υπολογιστή διακομιστή**

Ο ευκολότερος τρόπος για να καταργήσετε το ESET PROTECT On-Prem/MDM είναι να μορφοποιήσετε το δίσκο στον οποίο είναι εγκατεστημένο.

Αυτή η ενέργεια θα διαγράψει τα πάντα στο δίσκο, συμπεριλαμβανομένου του λειτουργικού συστήματος.

Αντιμετώπιση προβλημάτων

Καθώς το ESET PROTECT On-Prem είναι ένα σύνθετο προϊόν που χρησιμοποιεί διάφορα εργαλεία άλλων κατασκευαστών και υποστηρίζει πολλές πλατφόρμες λειτουργικών συστημάτων, υπάρχει περίπτωση να προκύψουν ζητήματα τα οποία απαιτούν επίλυση.

Η τεκμηρίωση της ESET περιλαμβάνει διάφορες μεθόδους για την αντιμετώπιση προβλημάτων του ESET PROTECT On-Prem. Ανατρέξτε στις Απαντήσεις σε συνήθη ζητήματα εγκατάστασης για να επιλύσετε ορισμένα συνήθη ζητήματα με το ESET PROTECT On-Prem. Δείτε επίσης τα γνωστά ζητήματα για τα προϊόντα της ESET για επιχειρήσεις.

Δεν μπορείτε να επιλύσετε κάποιο ζήτημα;

- Κάθε στοιχείο του ESET PROTECT έχει ένα αρχείο καταγραφής και μπορείτε να ρυθμίσετε τις παραμέτρους του ώστε να είναι περισσότερο ή λιγότερο λεπτομερές. Μελετήστε τα αρχεία καταγραφής για να εντοπίσετε σφάλματα τα οποία ενδεχομένως εξηγούν το ζήτημα που αντιμετωπίζετε.

- Το επίπεδο λεπτομερειών στην καταγραφή κάθε στοιχείου ρυθμίζεται στην πολιτική του > **Παρακολούθηση επιπέδου λεπτομέρειας καταγραφής** - Ρυθμίστε το επίπεδο λεπτομέρειας καταγραφής που προσδιορίζει το επίπεδο πληροφοριών που θα συλλέγονται και θα καταγράφονται, από **Παρακολούθηση** (πληροφοριακά) έως **Ανεπανόρθωτο σφάλμα** (πολύ σημαντικές κρίσιμες πληροφορίες). Η πολιτική πρέπει να εφαρμοστεί στη συσκευή για να ισχύει.

  oΠολιτική φορέα ESET Management - Για να ενεργοποιήσετε πλήρη καταγραφή του Φορέα ESET Management στο αρχείο *trace.log*, δημιουργήστε ένα κενό αρχείο με το όνομα *traceAll* χωρίς επέκταση, στον ίδιο φάκελο με ένα αρχείο *trace.log* και, στη συνέχεια, κάντε επανεκκίνηση του υπολογιστή (για να γίνει επανεκκίνηση της υπηρεσίας Φορέα ESET Management).

  oESET Bridge πολιτική

  oΠολιτική του ESET Mobile Device Connector - Η πολιτική πρέπει να εφαρμοστεί στη συσκευή για να ισχύει. Δείτε επίσης το θέμα Αντιμετώπιση προβλημάτων MDM.

  oΗ λεπτομέρεια καταγραφής για τον διακομιστή ESET PROTECT βρίσκεται στις Ρυθμίσεις.

- Εάν δεν είστε σε θέση να επιλύσετε το ζήτημα, μπορείτε να επισκεφτείτε την Ομάδα συζήτησης ασφάλειας ESET και να συμβουλευτείτε την κοινότητα ESET για πληροφορίες σχετικά με ζητήματα που αντιμετωπίζετε.

- Όταν επικοινωνείτε με την Τεχνική Υποστήριξη της ESET, ενδέχεται να σας ζητηθεί να συλλέξετε αρχεία καταγραφής χρησιμοποιώντας το ESET Log Collector ή το Εργαλείο διαγνωστικού ελέγχου. Συνιστούμε οπωσδήποτε να συμπεριλαμβάνετε αρχεία καταγραφής όταν επικοινωνείτε με το τμήμα υποστήριξης, για να επιταχύνετε την επεξεργασία του αιτήματός σας από την εξυπηρέτηση πελατών.

Αναβάθμιση στοιχείων ESET PROTECT σε περιβάλλον εκτός σύνδεσης

Ακολουθήστε τα παρακάτω βήματα για να αναβαθμίσετε τα στοιχεία ESET PROTECT και τα προϊόντα ESET Endpoint χωρίς πρόσβαση στο Internet:

Η χρήση της εργασίας αναβάθμισης στοιχείων για ένα περιβάλλον χωρίς σύνδεση, είναι εφικτή εάν πληρούνται οι ακόλουθες συνθήκες:
- Υπάρχει διαθέσιμος χώρος αποθήκευσης χωρίς σύνδεση.
- Η τοποθεσία του χώρου αποθήκευσης για το φορέα ESET Management διαμορφώνεται χρησιμοποιώντας μια πολιτική σε μια προσπελάσιμη τοποθεσία.

Εκτελέστε πρώτα αναβάθμιση του διακομιστή ESET PROTECT και της Κονσόλας διαδικτύου:

1. Ελέγξτε την έκδοση της κονσόλας διαχείρισης ESET που εκτελείται στον διακομιστή.

2. Πραγματοποιήστε λήψη του πιο πρόσφατου προγράμματος εγκατάστασης «Όλα σε ένα» για Windows ή τα πιο πρόσφατα ανεξάρτητα προγράμματα εγκατάστασης στοιχείων του ESET PROTECT για Linux από τον ιστότοπο λήψεων της ESET.

3. Εκτελέστε πρώτα αναβάθμιση του διακομιστή ESET PROTECT και της ESET PROTECT Κονσόλας διαδικτύου:

   - Windows - Αναβάθμιση με χρήση του Προγράμματος εγκατάστασης «Όλα σε ένα»
   - Linux - Μη αυτόματη αναβάθμιση βάσει στοιχείων

Η αναβάθμιση της Κονσόλας διαδικτύου και του Apache Tomcat εκκαθαρίζει τα αρχεία βοήθειας εκτός σύνδεσης. Εάν χρησιμοποιήσατε βοήθεια εκτός σύνδεσης με μια παλαιότερη έκδοση του ESET PROTECT On-Prem, δημιουργήστε την ξανά για το ESET PROTECT On-Prem 11.0 μετά την αναβάθμιση, για να διασφαλίσετε ότι έχετε την πιο πρόσφατη βοήθεια εκτός σύνδεσης που αντιστοιχεί στην έκδοση του ESET PROTECT On-Prem που διαθέτετε.

Συνεχίστε με την αναβάθμιση των τερματικών προϊόντων ESET εκτός σύνδεσης

1. Δείτε ποια προϊόντα ESET είναι εγκατεστημένα στους υπολογιστές-πελάτες: Ανοίξτε την Κονσόλα διαδικτύου ESET PROTECT και πλοηγηθείτε στα στοιχεία **Πίνακας ελέγχου** > **Εφαρμογές ESET**.

2. Βεβαιωθείτε ότι έχετε τις πιο πρόσφατες εκδόσεις των προϊόντων ESET Endpoint.

3. Λάβετε προγράμματα εγκατάστασης από τον Ιστότοπο λήψεων της ESET στον τοπικό χώρο αποθήκευσης που διαμορφώθηκε κατά την εγκατάσταση χωρίς σύνδεση.

4. Εκτελέστε μια εργασία εγκατάστασης λογισμικού από την κονσόλα διαδικτύου ESET PROTECT.

Απαντήσεις σε συνήθη ζητήματα εγκατάστασης

Αναπτύξτε την ενότητα για τα μηνύματα σφάλματος που θέλετε να επιλύσετε:

ESET PROTECTΔιακομιστής

Η υπηρεσία διακομιστή ESET PROTECT δεν ξεκινά:

Κατεστραμμένη εγκατάσταση

- Αυτό μπορεί να συμβεί επειδή λείπουν κλειδιά μητρώου, λείπουν αρχεία ή τα δικαιώματα αρχείων δεν είναι έγκυρα.
- Το πρόγραμμα εγκατάστασης ESET όλα-σε-ένα έχει το δικό του αρχείο καταγραφής. Όταν εγκαθιστάτε οι ίδιοι ένα στοιχείο, χρησιμοποιήστε τη μέθοδο Καταγραφή MSI.

Η θύρα ακρόασης χρησιμοποιείται ήδη (κυρίως 2222 και 2223)

Χρησιμοποιήστε την κατάλληλη εντολή για το λειτουργικό σας σύστημα:

- Windows:

```
netstat -an | find "2222"
netstat -an | find "2223"
```

- Linux:

```
netstat | grep 2222
netstat | grep 2223
```

Η βάση δεδομένων δεν λειτουργεί ή δεν είναι προσβάσιμη

- Microsoft SQL Server: Βεβαιωθείτε ότι η θύρα 1433 είναι διαθέσιμη στο διακομιστή βάσης δεδομένων ή προσπαθήστε να συνδεθείτε στο SQL Server Management Studio
- MySQL: Βεβαιωθείτε ότι η θύρα 3306 είναι διαθέσιμη στο διακομιστή βάσης δεδομένων ή προσπαθήστε να συνδεθείτε στη διασύνδεση της βάσης δεδομένων σας (για παράδειγμα, χρησιμοποιώντας τη διασύνδεση γραμμής εντολών MySQL ή το `phpmyadmin`)

Κατεστραμμένη βάση δεδομένων

Εμφανίζονται πολλά σφάλματα SQL στο αρχείο καταγραφής του διακομιστή ESET PROTECT. Συνιστούμε να επαναφέρετε τη βάση δεδομένων από ένα αντίγραφο ασφαλείας. Εάν δεν υπάρχει αντίγραφο ασφαλείας, εγκαταστήστε εκ νέου το ESET PROTECT On-Prem.

Ανεπαρκείς πόροι συστήματος (RAM, χώρος στο δίσκο)

Εξετάστε τις εκτελούμενες διεργασίες και τις επιδόσεις του συστήματος:

- Χρήστες Windows: Εκτελέστε και μελετήστε τις πληροφορίες στη Διαχείριση εργασιών ή στο Πρόγραμμα προβολής συμβάντων
- Χρήστες Linux: Εκτελέστε μία από τις ακόλουθες εντολές:

`df -h` (για να εξετάσετε τις πληροφορίες χώρου στο δίσκο)
`cat /proc/meminfo` (για να εξετάσετε τις πληροφορίες χώρου στη μνήμη)
`dmesg` (για να εξετάσετε τη λειτουργικότητα του συστήματος Linux)

Σφάλμα με τη σύνδεση ODBC κατά την εγκατάσταση του διακομιστή ESET PROTECT

```
Error: (Error 65533) ODBC connector compatibility check failed.
Please install ODBC driver with support for multi-threading.
```

Επανεγκαταστήστε μια έκδοση προγράμματος οδήγησης ODBC που υποστηρίζει πολλαπλά νήματα ή διαμορφώστε εκ νέου το *odbcinst.ini* όπως περιγράφεται στην ενότητα διαμόρφωσης ODBC.

Σφάλμα με σύνδεση βάσης δεδομένων κατά την εγκατάσταση του διακομιστή ESET PROTECT

Η εγκατάσταση του διακομιστή ESET PROTECT ολοκληρώνεται με το παρακάτω γενικό μήνυμα σφάλματος:

```
The database server is not configured correctly.
Please check the documentation and reconfigure the database server as needed.
```

Μήνυμα σφάλματος από το αρχείο καταγραφής εγκατάστασης:

```
Error: Execution test of long statement failed with exception:
CMysqlCodeTokenExecutor: CheckVariableInnodbLogFileSize:
Server variables innodb_log_file_size*innodb_log_files_in_group
value 100663296 is too low.
```

Βεβαιωθείτε ότι η διαμόρφωση του προγράμματος οδήγησης της βάσης δεδομένων σας συμφωνεί με την περιγραφή στην ενότητα διαμόρφωσης ODBC.

Αντιμετώπιση προβλημάτων κατά την κατάργηση εγκατάστασης του Φορέα ESET Management

• Ανατρέξτε στα αρχεία καταγραφής για το φορέα ESET Management.
• Μπορείτε να καταργήσετε την εγκατάσταση του φορέα ESET Management χρησιμοποιώντας το εργαλείο κατάργησης εγκατάστασης ESET ή μια μη τυπική μέθοδο (όπως διαγραφή αρχείων, κατάργηση της υπηρεσίας του φορέα ESET Management και των αντίστοιχων καταχωρίσεων μητρώου). Ωστόσο, αυτή η μέθοδος δεν θα είναι δυνατή εάν υπάρχει τερματικό προϊόν ESET στον ίδιο υπολογιστή, επειδή θα είναι ενεργοποιημένη η Αυτοπροστασία.
• Εμφανίζεται το μήνυμα "The database cannot be upgraded. Please remove the product first." (Δεν είναι δυνατή η αναβάθμιση της βάσης δεδομένων. Καταργήστε πρώτα την εγκατάσταση του προϊόντος.) κατά την κατάργηση εγκατάστασης του Φορέα - Επιδιορθώστε τον Φορέα ESET Management:
1.Κάντε κλικ στο στοιχείο **Πίνακας Ελέγχου** > **Προγράμματα και δυνατότητες** και διπλό κλικ στο στοιχείο **Φορέας ESET Management**.
2.Κάντε κλικ στο κουμπί **Επόμενο** > **Επιδιόρθωση** και ακολουθήστε τις οδηγίες.
Όλοι οι δυνατοί τρόποι κατάργησης της εγκατάστασης του φορέα ESET Management περιγράφονται στην ενότητα «Κατάργηση εγκατάστασης».

Παρουσιάστηκε κωδικός σφάλματος 1603 κατά την εγκατάσταση του φορέα

Αυτό το σφάλμα μπορεί να προκύψει όταν τα αρχεία του προγράμματος εγκατάστασης δεν βρίσκονται στον τοπικό δίσκο. Για να διορθώσετε το πρόβλημα, αντιγράψτε τα αρχεία του προγράμματος εγκατάστασης στον τοπικό κατάλογο και εκτελέστε ξανά την εγκατάσταση. Εάν τα αρχεία βρίσκονται ήδη στον τοπικό κατάλογο ή εάν το πρόβλημα παραμένει, ακολουθήστε τις σχετικές οδηγίες της Γνωσιακής βάσης.

Κατά την εγκατάσταση του Φορέα σε Linux εμφανίζεται μήνυμα σφάλματος

Μήνυμα σφάλματος:

```
Checking certificate ... failed
Error checking peer certificate: NOT_REGULAR_FILE
```

Η πιθανή αιτία αυτού του σφάλματος είναι εσφαλμένο όνομα αρχείου στην εντολή εγκατάστασης. Στη κονσόλα γίνεται διάκριση πεζών-κεφαλαίων. Για παράδειγμα, το `Agent.pfx` δεν είναι ίδιο με το `agent.pfx`.

Ο Φορέας ESET Management δεν είναι δυνατόν να συνδεθεί με τον διακομιστή ESET PROTECT

Ανατρέξτε στο θέμα Αντιμετώπιση προβλημάτων σύνδεσης φορέα και το άρθρο της Γνωσιακής βάσης.

Η δέσμη ενεργειών του προγράμματος εγκατάστασης του φορέα πραγματοποίησε έξοδο με τον κωδικό 30

Χρησιμοποιείτε τη δέσμη ενεργειών του προγράμματος εγκατάστασης του φορέα με μια προσαρμοσμένη τοποθεσία προγράμματος εγκατάστασης και παραλείψατε να επεξεργαστείτε σωστά τη δέσμη ενεργειών. Αναθεωρήστε τη σελίδα βοήθειας και προσπαθήστε ξανά.

Κονσόλα διαδικτύου

ESET BridgeΔιακομιστής Μεσολάβησης HTTP -

Αισθητήρας ESET Rogue Detection Sensor

Γιατί καταγράφεται συνεχώς το ακόλουθο μήνυμα σφάλματος στο trace.log του αισθητήρα ESET Rogue Detector;

```
Information: CPCAPDeviceSniffer [Thread 764]:
CPCAPDeviceSniffer on rpcap://\Device\NPF_
{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} throwed error:
Device open failed with error:Error opening adapter:
The system cannot find the device specified. (20)
```

Πρόκειται για πρόβλημα με το WinPcap. Διακόψτε την υπηρεσία του αισθητήρα ESET Rogue Detector Sensor, επανεγκαταστήστε την πιο πρόσφατη έκδοση του WinPcap (τουλάχιστον 4.1.0) και επανεκκινήστε την υπηρεσία του αισθητήρα ESET Rogue Detector Sensor.

Linux

Λείπει η εξάρτηση libQtWebKit στο CentOS Linux

Εάν εμφανίζεται το παρακάτω μήνυμα:

```
Error: CReportPrinterModule [Thread 7f5f4c7b8700]:
ReportPrinter: ReportPrinterTool exited with:
/opt/eset/RemoteAdministrator/Server//ReportPrinterTool:
error while loading shared libraries: libQtWebKit.so.4:
cannot open shared object file: No such file or directory [code:127]
```

ακολουθήστε τις οδηγίες στο άρθρο της Γνωσιακής βάσης.

Η εγκατάσταση του διακομιστή ESET PROTECT στο CentOS 7 απέτυχε

Εάν εμφανίζεται το παρακάτω μήνυμα:

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

Το ζήτημα ίσως οφείλεται σε ρυθμίσεις περιβάλλοντος/τοπικές ρυθμίσεις. Θα μπορούσε να βοηθήσει η εκτέλεση της παρακάτω εντολής πριν από τη δέσμη ενεργειών του προγράμματος εγκατάστασης του διακομιστή:

```
export LC_ALL="en_US.UTF-8"
```

Microsoft SQL Server

Κωδικός σφάλματος -2068052081 κατά την εγκατάσταση του Microsoft SQL Server.

Επανεκκινήστε τον υπολογιστή σας και εκτελέστε ξανά τη ρύθμιση. Εάν το πρόβλημα επιμείνει, καταργήστε την εγκατάσταση του τοπικού προγράμματος-πελάτη SQL Server και εκτελέστε ξανά την εγκατάσταση. Εάν αυτό δεν επιλύσει το πρόβλημα, καταργήστε την εγκατάσταση όλων των προϊόντων Microsoft SQL Server, επανεκκινήστε τον υπολογιστή σας και εκτελέστε ξανά την εγκατάσταση.

Κωδικός σφάλματος -2067922943 κατά την εγκατάσταση του Microsoft SQL Server.

Βεβαιωθείτε ότι το σύστημά σας ικανοποιεί τις απαιτήσεις βάσης δεδομένων για το ESET PROTECT On-Prem.

Κωδικός σφάλματος -2067922934 κατά την εγκατάσταση του Microsoft SQL Server.

Βεβαιωθείτε ότι έχετε τα σωστά δικαιώματα λογαριασμού χρήστη.

Η κονσόλα διαδικτύου εμφανίζει την ένδειξη "Απέτυχε η φόρτωση δεδομένων".

Το Microsoft SQL Server προσπαθεί να χρησιμοποιήσει όσο το δυνατόν περισσότερο χώρο στο δίσκο για αρχεία καταγραφής συναλλαγών. Εάν θέλετε να το καθαρίσετε αυτό, επισκεφτείτε τον επίσημο ιστότοπο της Microsoft.

Κωδικός σφάλματος -2067919934 κατά την εγκατάσταση του Microsoft SQL Server.

Βεβαιωθείτε ότι όλα τα προηγούμενα βήματα έχουν ολοκληρωθεί με επιτυχία. Αυτό το σφάλμα προκαλείται λόγω κακής διαμόρφωσης ορισμένων αρχείων συστήματος. Επανεκκινήστε τον υπολογιστή σας και εκτελέστε ξανά την εγκατάσταση.

Αρχεία καταγραφής

Κάθε στοιχείο ESET PROTECT πραγματοποιεί καταγραφή. Τα στοιχεία ESET PROTECT εγγράφουν πληροφορίες σχετικά με συγκεκριμένα συμβάντα σε αρχεία καταγραφής. Η θέση των αρχείων καταγραφής ποικίλλει ανάλογα με το στοιχείο. Ακολουθεί μια λίστα με τις θέσεις των αρχείων καταγραφής:

Windows

ESET PROTECT στοιχεία	Τοποθεσία αρχείων καταγραφής
ESET PROTECTΔιακομιστής	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*
Φορέας ESET Management	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* Ανατρέξτε επίσης στην ενότητα Αντιμετώπιση προβλημάτων σύνδεσης φορέα.
ESET PROTECTΚονσόλα διαδικτύου και Apache Tomcat	*C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs* Ανατρέξτε επίσης στη διεύθυνση https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Σύνδεση κινητών συσκευών	*C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs* Δείτε επίσης το θέμα Αντιμετώπιση προβλημάτων MDM.
Ανιχνευτής Διασκορπισμένων Μηχανών	*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*

ESET PROTECT στοιχεία	Τοποθεσία αρχείων καταγραφής
ESET Bridge (Διακομιστής Μεσολάβησης HTTP)	Δείτε το θέμα Ηλεκτρονική βοήθεια για το ESET Bridge.

> Ο φάκελος *C:\ProgramData* είναι κρυφός από προεπιλογή. Για να εμφανίσετε το φάκελο:
> 1.Επιλέξτε **Έναρξη** > **Πίνακας Ελέγχου** > **Επιλογές φακέλων** > **Προβολή**.
> 2.Επιλέξτε **Εμφάνιση κρυφών αρχείων, φακέλων και μονάδων δίσκου** και κάντε κλικ στο κουμπί **OK**.

Linux

ESET PROTECT στοιχεία	Τοποθεσία αρχείων καταγραφής
ESET PROTECTΔιακομιστής	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/EraServerInstaller.log*
Φορέας ESET Management	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
Σύνδεση κινητών συσκευών	*/var/log/eset/RemoteAdministrator/MDMCore/* */var/log/eset/RemoteAdministrator/MDMCore/Proxy/* Δείτε επίσης το θέμα Αντιμετώπιση προβλημάτων MDM.
ESET Bridge (Διακομιστής Μεσολάβησης HTTP)	Δείτε το θέμα Ηλεκτρονική βοήθεια για το ESET Bridge.
ESET PROTECTΚονσόλα διαδικτύου και Apache Tomcat	*/var/log/tomcat/* Ανατρέξτε επίσης στη διεύθυνση https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Αισθητήρας RD ESET	*/var/log/eset/RogueDetectionSensor/*

Εικονική συσκευή ESET PROTECT

ESET PROTECT στοιχεία	Τοποθεσία αρχείων καταγραφής
Διαμόρφωση VA ESET PROTECT	*/root/appliance-configuration-log.txt*
ESET PROTECTΔιακομιστής	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log*
ESET Bridge (Διακομιστής Μεσολάβησης HTTP)	Δείτε το θέμα Ηλεκτρονική βοήθεια για το ESET Bridge.

macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

Εργαλείο διαγνωστικού ελέγχου

Το εργαλείο διαγνωστικού ελέγχου αποτελεί μέρος όλων των στοιχείων του ESET PROTECT. Χρησιμοποιείται για τη συλλογή και συσκευασία των αρχείων καταγραφής, τα οποία μπορούν να χρησιμοποιηθούν από εκπροσώπους τεχνικής υποστήριξης και προγραμματιστές για την επίλυση προβλημάτων με τα στοιχεία του προϊόντος.

Θέση εργαλείου διαγνωστικού ελέγχου

Windows

Φάκελος *C:\Program Files\ESET\RemoteAdministrator*[προϊόν] **Diagnostic.exe**.

Linux

Στον εξής κατάλογο στο διακομιστή: */opt/eset/RemoteAdministrator/*[προϊόν]/, υπάρχει ένα εκτελέσιμο αρχείο **Diagnostic[προϊόν]** (μία λέξη, για παράδειγμα, **DiagnosticServer**, **DiagnosticAgent**)

Χρήση (Linux)

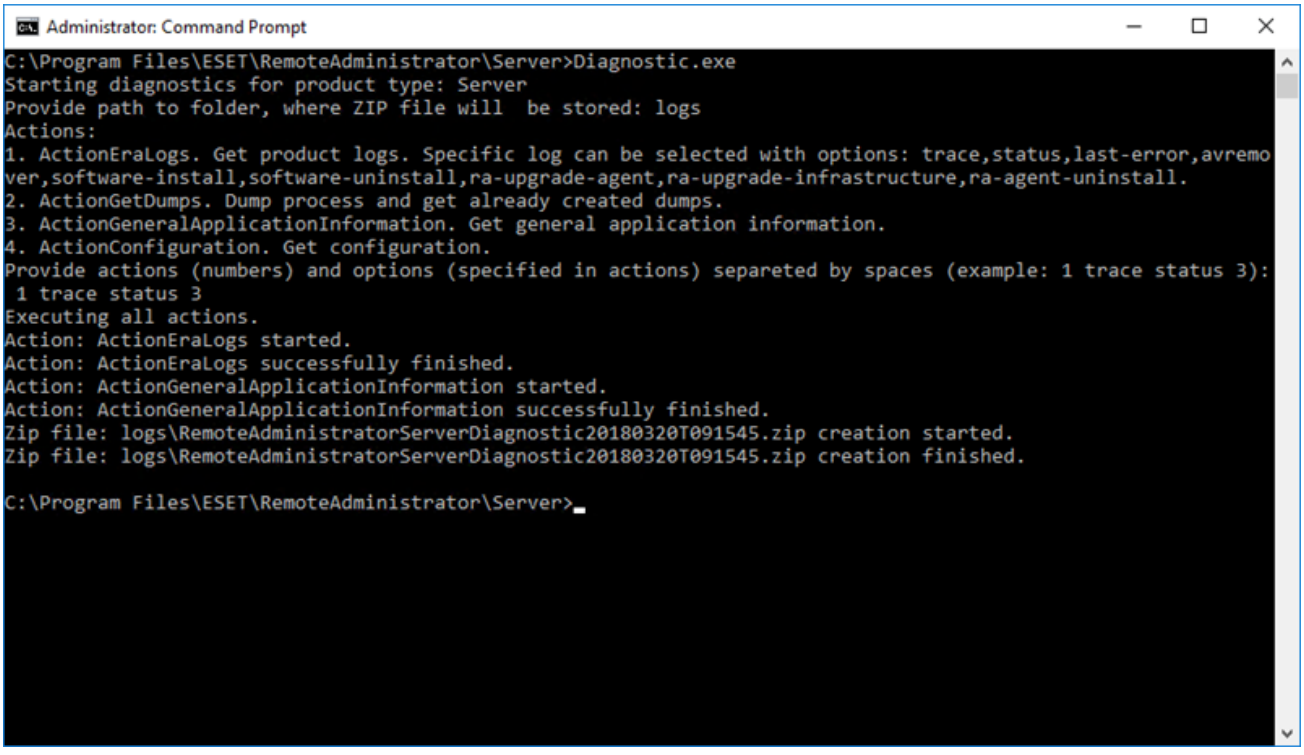
Εκτελέστε το εκτελέσιμο αρχείο διαγνωστικών ελέγχων στο τερματικό ως ρίζα και ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.

Χρήση (Windows)

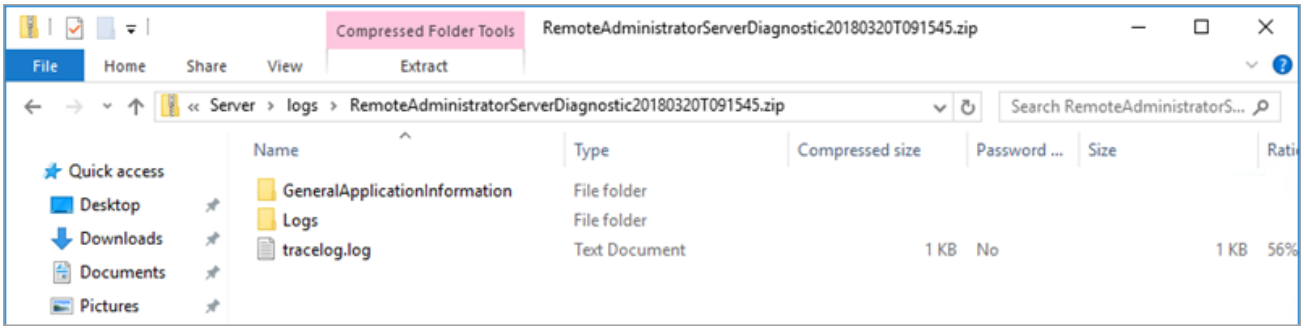
1. Εκτελέστε το εργαλείο χρησιμοποιώντας τη γραμμή εντολών.

2. Εισαγάγετε τη θέση στην οποία θα αποθηκευτούν τα αρχεία καταγραφής (στο παράδειγμά μας, "logs") και πατήστε **Enter**.

3. Εισαγάγετε τις πληροφορίες που θέλετε να συγκεντρώσετε (στο παράδειγμά μας, `1 trace status 3`). Ανατρέξτε στην ενότητα **Ενέργειες** παρακάτω για περισσότερες πληροφορίες.



4. Μόλις ολοκληρωθεί η διαδικασία, μπορείτε να βρείτε τα αρχεία καταγραφής συμπιεσμένα σε ένα αρχείο *.zip* στον κατάλογο «**logs**», στη θέση όπου βρίσκεται το εργαλείο διαγνωστικού ελέγχου.



Ενέργειες

- **ActionEraLogs** - Δημιουργείται ένας φάκελος αρχείων καταγραφής, στον οποίο αποθηκεύονται όλα τα αρχεία καταγραφής. Για να καθορίσετε μόνο συγκεκριμένα αρχεία καταγραφής, χρησιμοποιήστε ένα κενό διάστημα για να διαχωρίσετε κάθε αρχείο.

- **ActionGetDumps** - Δημιουργείται ένας νέος φάκελος. Γενικά, ένα αρχείο αποτύπωσης διεργασίας δημιουργείται εάν ανιχνευτεί κάποιο πρόβλημα. Εάν εντοπιστεί κάποιο σοβαρό πρόβλημα, δημιουργείται από το σύστημα ένα αρχείο τοποθέτησης. Για να το ελέγξετε οι ίδιοι, μεταβείτε στο φάκελο %temp% (στα Windows) ή στο φάκελο /tmp/ (στο Linux) και εισαγάγετε ένα αρχείο dmp.

ℹ Πρέπει να εκτελείται η υπηρεσία στοιχείου (Agent, Server, RD Sensor,).

- **ActionGeneralApplicationInformation** - Δημιουργείται ο φάκελος GeneralApplicationInformation και μέσα του δημιουργείται το αρχείο *GeneralApplicationInformation.txt*. Αυτό το αρχείο περιέχει πληροφορίες κειμένου που συμπεριλαμβάνουν το όνομα προϊόντος και την έκδοση του προϊόντος που είναι εγκατεστημένο εκείνη τη στιγμή.

- **ActionConfiguration** - Δημιουργείται ένας φάκελος διαμόρφωσης στον οποίο αποθηκεύεται το αρχείο storage.lua.

Προβλήματα μετά την αναβάθμιση/μετεγκατάσταση του διακομιστή ESET PROTECT

Εάν δεν μπορείτε να εκκινήσετε την υπηρεσία διακομιστή ESET PROTECT επειδή η εγκατάσταση είναι κατεστραμμένη και υπάρχουν άγνωστα μηνύματα σφαλμάτων στα αρχεία καταγραφής, πραγματοποιήστε επιδιόρθωση ακολουθώντας τα παρακάτω βήματα:

⚠ Συνιστούμε να δημιουργήσετε αντίγραφα ασφαλείας του διακομιστή βάσης δεδομένων προτού ξεκινήσετε την επιδιόρθωση.

1. Μεταβείτε στη θέση **Έναρξη** > **Πίνακας Ελέγχου** > **Προγράμματα και δυνατότητες** και κάντε διπλό κλικ στο στοιχείο **Διακομιστής ESET PROTECT**.

2. Επιλέξτε **Επιδιόρθωση** και κάντε κλικ στο κουμπί **Επόμενο**.

3. Χρησιμοποιήστε ξανά τις υπάρχουσες ρυθμίσεις σύνδεσης βάσης δεδομένων και κάντε κλικ στο κουμπί **Επόμενο**. Επιλέξτε **Ναι εάν σας ζητηθεί επιβεβαίωση**. Μπορείτε να βρείτε τις πληροφορίες σύνδεσης στη βάση δεδομένων εδώ: *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*

4. Επιλέξτε **Χρήση κωδικού πρόσβασης που είναι ήδη αποθηκευμένος στη βάση δεδομένων** και κάντε κλικ στο κουμπί **Επόμενο**.

5. Επιλέξτε **Διατήρηση πιστοποιητικών που χρησιμοποιούνται αυτήν τη στιγμή** και κάντε κλικ στο κουμπί **Επόμενο**.

6. Ενεργοποιήστε τον Διακομιστή ESET PROTECT με ένα έγκυρο κλειδί άδειας χρήσης ή επιλέξτε **Ενεργοποίηση αργότερα** (ανατρέξτε στο θέμα Διαχείριση αδειών χρήσης για πρόσθετες οδηγίες) και κάντε κλικ στο στοιχείο **Επόμενο**.

7. Κάντε κλικ στο κουμπί **Επιδιόρθωση**.

8. Συνδεθείτε ξανά στην Κονσόλα διαδικτύου και ελέγξτε εάν όλα είναι εντάξει.

Άλλα σενάρια αντιμετώπισης πτοβλημάτων:

Ο διακομιστής ESET PROTECT δεν λειτουργεί, αλλά υπάρχει αντίγραφο ασφαλείας της βάσης δεδομένων:

1. Επαναφέρετε το αντίγραφο ασφαλείας της βάσης δεδομένων.

2. Επαληθεύστε ότι ο νέος υπολογιστής χρησιμοποιεί την ίδια διεύθυνση IP ή όνομα κεντρικού υπολογιστή όπως και η προηγούμενη εγκατάσταση, για να διασφαλίσετε ότι οι φορείς θα συνδέονται.

3. Επιδιορθώστε τον διακομιστή ESET PROTECT και χρησιμοποιήστε τη βάση δεδομένων που επαναφέρατε.

Ο διακομιστής ESET PROTECT δεν λειτουργεί. αλλά έχετε εξαγάγει από αυτόν το πιστοποιητικό διακομιστή και την Αρχή έκδοσης πιστοποιητικών:

1. Επαληθεύστε ότι ο νέος υπολογιστής χρησιμοποιεί την ίδια διεύθυνση IP ή όνομα κεντρικού υπολογιστή όπως και η προηγούμενη εγκατάσταση, για να διασφαλίσετε ότι οι φορείς θα συνδέονται.

2. Επιδιορθώστε τον διακομιστή ESET PROTECT χρησιμοποιώντας αντίγραφα ασφαλείας πιστοποιητικών (κατά την επιδιόρθωση, επιλέξτε **Φόρτωση πιστοποιητικών από αρχείο** και ακολουθήστε τις οδηγίες).

Ο διακομιστής ESET PROTECT δεν λειτουργεί και δεν έχετε αντίγραφο ασφαλείας της βάσης δεδομένων ούτε πιστοποιητικό διακομιστή και Αρχή έκδοσης πιστοποιητικών ESET PROTECT:

1. Επιδιορθώστε τον διακομιστή ESET PROTECT.

2. Επιδιορθώστε τους φορείς ESET Management χρησιμοποιώντας μία από τις παρακάτω μεθόδους:

- Δέσμη ενεργειών προγράμματος εγκατάστασης φορέα
- Απομακρυσμένη ανάπτυξη (αυτό απαιτεί να απενεργοποιήσετε το firewall στους υπολογιστές προορισμού)
- Πρόγραμμα μη αυτόματης εγκατάστασης στοιχείου φορέα

Καταγραφή MSI

Αυτή είναι χρήσιμη εάν δεν είστε σε θέση να εγκαταστήσετε σωστά ένα στοιχείο ESET PROTECT στα Windows, για παράδειγμα το φορέα ESET Management:

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

ESET PROTECT On-Prem API

Το ESET PROTECT ServerApi (*ServerApi.dll*) είναι ένα περιβάλλον χρήστη προγραμματισμού εφαρμογών, ένα σύνολο λειτουργιών και εργαλείων για τη δημιουργία προσαρμοσμένων εφαρμογών λογισμικού, ώστε να πληρούν τις ανάγκες και τις ειδικές προδιαγραφές σας. Με τη χρήση του ServerApi, η εφαρμογή σας μπορεί να παρέχει προσαρμοσμένη διασύνδεση, λειτουργικότητα και λειτουργίες που θα κάνατε κανονικά μέσω της κονσόλας διαδικτύου ESET PROTECT, όπως η διαχείριση του ESET PROTECT On-Prem, η δημιουργία και λήψη αναφορών, κ.λπ.

Για περισσότερες πληροφορίες και παραδείγματα σε γλώσσα C, και για μια λίστα των διαθέσιμων μηνυμάτων JSON, ανατρέξτε στο ακόλουθο θέμα ηλεκτρονικής βοήθειας:

ESET PROTECT On-Prem 11.0 API

Συχνές ερωτήσεις

Γιατί εγκαθιστούμε Java σε διακομιστή; Δεν δημιουργεί αυτό κίνδυνο ασφάλειας; Η πλειονότητα των εταιρειών ασφάλειας και των πλαισίων ασφάλειας συνιστούν την απεγκατάσταση

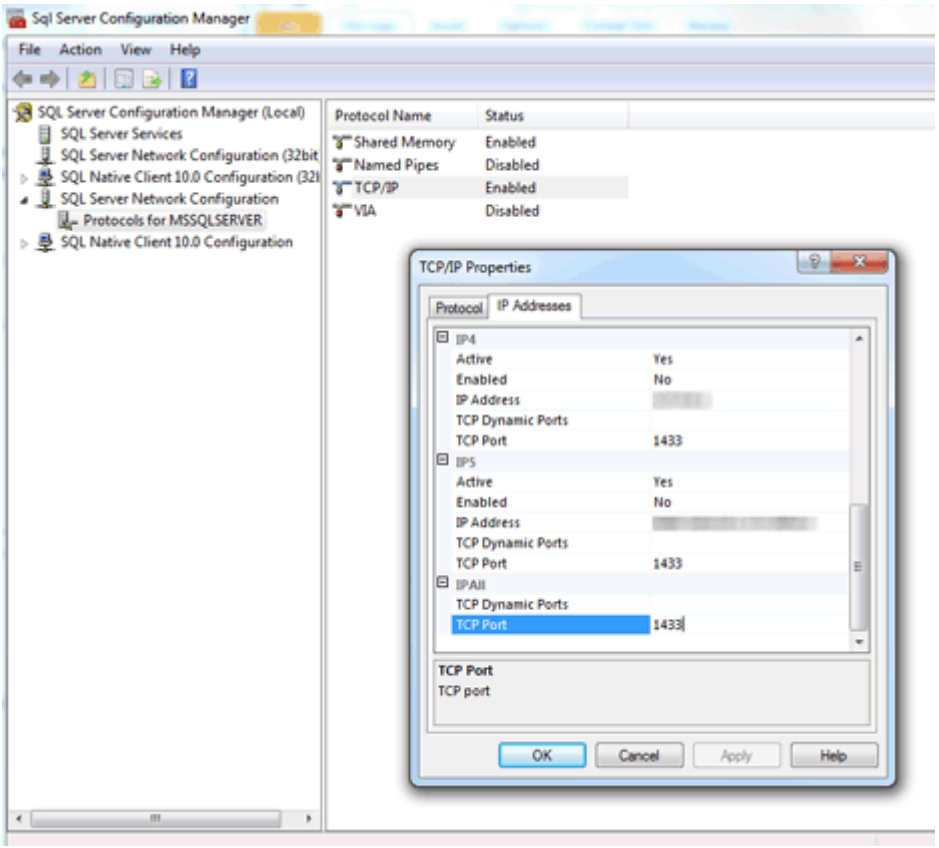
της Java από υπολογιστές, και ειδικά από τους διακομιστές.

Η κονσόλα διαδικτύου ESET PROTECT απαιτεί Java/OpenJDK για να λειτουργήσει. Η Java είναι ένα βιομηχανικό πρότυπο για κονσόλες βασισμένες στον ιστό και όλες οι γνωστές κονσόλες διαδικτύου χρησιμοποιούν Java και διακομιστή ιστού (Apache Tomcat) για τη λειτουργία τους. Η Java είναι απαραίτητη για την υποστήριξη διακομιστών διαδικτύου πολλαπλής πλατφόρμας. Μπορείτε να εγκαταστήσετε έναν διακομιστή διαδικτύου σε έναν αποκλειστικό υπολογιστή για λόγους ασφαλείας.

Από τον Ιανουάριο 2019, οι δημόσιες ενημερώσεις Oracle JAVA SE 8 για επιχειρηματική, εμπορική ή παραγωγική χρήση, απαιτούν εμπορική άδεια χρήσης. Εάν δεν αγοράσετε συνδρομή JAVA SE, μπορείτε να χρησιμοποιήσετε αυτό τον οδηγό για μετάβαση σε μια εναλλακτική λύση χωρίς κόστος. Δείτε τις υποστηριζόμενες εκδόσεις του JDK.

Πώς μπορώ να προσδιορίσω ποια θύρα χρησιμοποιείται από το διακομιστή SQL Server;

Υπάρχουν πολλοί τρόποι για να προσδιορίσετε τη θύρα που χρησιμοποιείται από το SQL Server. Μπορείτε να λάβετε το πιο ακριβές αποτέλεσμα μέσω της Διαχείρισης διαμόρφωσης του SQL Server. Δείτε την παρακάτω εικόνα για ένα παράδειγμα του σημείου που μπορείτε να εντοπίσετε αυτές τις πληροφορίες στη διαχείριση διαμόρφωσης SQL:



Μετά την εγκατάσταση του SQL Server Express (συμπεριλαμβάνεται στο πακέτο ESET PROTECT On-Prem) στο Windows Server 2012, δεν φαίνεται να γίνεται παρακολούθηση σε μια τυπική θύρα SQL. Η παρακολούθηση γίνεται πιθανότατα σε μια διαφορετική θύρα από την προεπιλεγμένη θύρα 1433.

Πώς μπορώ να διαμορφώσω το MySQL ώστε να αποδέχεται μεγάλο μέγεθος πακέτου;

Δείτε την εγκατάσταση και τη διαμόρφωση του MySQL για Windows ή Linux.

Εάν εγκαταστήσω μόνος/η το SQL, πώς πρέπει να δημιουργήσω μια βάση δεδομένων για το ESET PROTECT On-Prem;

Δεν χρειάζεται. Δημιουργείται μια βάση δεδομένων από το πρόγραμμα εγκατάστασης *Server.msi* και όχι από το πρόγραμμα εγκατάστασης του ESET PROTECT. Το πρόγραμμα εγκατάστασης του ESET PROTECT συμπεριλαμβάνεται για να απλοποιήσει τα βήματα, εγκαθιστά το διακομιστή SQL Server και κατόπιν η βάση δεδομένων δημιουργείται από το πρόγραμμα εγκατάστασης *Server.msi*.

Μπορεί το Πρόγραμμα εγκατάστασης ESET PROTECT On-Prem να δημιουργήσει μια νέα βάση δεδομένων για λογαριασμό μου σε μια υπάρχουσα εγκατάσταση του Microsoft SQL Server, εάν παράσχω τις κατάλληλες λεπτομέρειες και τα διαπιστευτήρια του Microsoft SQL Server; Θα ήταν πολύ χρήσιμο, εάν το πρόγραμμα εγκατάστασης υποστήριζε διάφορες εκδόσεις του διακομιστή SQL Server (2014, 2019, κ.λπ.).

Η βάση δεδομένων δημιουργείται από το *Server.msi*. Συνεπώς ναι, μπορεί να δημιουργήσει μια βάση δεδομένων ESET PROTECT για λογαριασμό σας σε μεμονωμένες εγκατεστημένες εμφανίσεις του SQL Server. Οι υποστηριζόμενες εκδόσεις του Microsoft SQL Server είναι η 2014 και οι νεότερες εκδόσεις.

ESET PROTECT On-Prem 11.0 Το πρόγραμμα εγκατάστασης «όλα σε ένα» εγκαθιστά το Microsoft SQL Server Express 2019 από προεπιλογή.

- Εάν χρησιμοποιείτε μια παλαιότερη έκδοση των Windows (Server 2012 ή SBS 2011), το Microsoft SQL Server Express 2014 θα εγκατασταθεί από προεπιλογή.
- Το πρόγραμμα εγκατάστασης δημιουργεί αυτόματα έναν τυχαίο κωδικό πρόσβασης για τον έλεγχο ταυτότητας της βάσης δεδομένων (που είναι αποθηκευμένη στη διαδρομή

%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini).

Το Microsoft SQL Server Express έχει όριο μεγέθους 10 GB για κάθε σχετική βάση δεδομένων. Δεν συνιστάται η χρήση του Microsoft SQL Server Express:
- Σε εταιρικά περιβάλλοντα ή μεγάλα δίκτυα.
- Εάν θέλετε να χρησιμοποιήσετε το ESET PROTECT On-Prem με το ESET Inspect On-Prem.

Εάν γίνεται εγκατάσταση σε υπάρχον πρόγραμμα SQL Server, θα πρέπει να χρησιμοποιείται από το SQL Server από προεπιλογή η ενσωματωμένη λειτουργία ελέγχου ταυτότητας των Windows;

Όχι, επειδή η λειτουργία ελέγχου ταυτότητας των Windows μπορεί να απενεργοποιηθεί στο SQL Server και ο μόνος τρόπος για σύνδεση είναι η χρήση του ελέγχου ταυτότητας SQL Server Authentication (εισαγωγή ονόματος χρήστη και κωδικού πρόσβασης). Κατά την εγκατάσταση του διακομιστή ESET PROTECT, απαιτείται έλεγχος ταυτότητας μεικτής λειτουργίας (έλεγχος ταυτότητας διακομιστή SQL και έλεγχος ταυτότητας Windows). Εάν γίνεται χειροκίνητη εγκατάσταση του SQL Server, συνιστάται να δημιουργήσετε έναν ριζικό κωδικό πρόσβασης (ο ριζικός χρήστης ονομάζεται «sa», που σημαίνει security admin (διαχειριστής ασφάλειας)) και να τον αποθηκεύσετε σε ασφαλές σημείο για μελλοντική χρήση. Ο ριζικός κωδικός πρόσβασης μπορεί να απαιτηθεί κατά την αναβάθμιση του διακομιστή ESET PROTECT. Μπορείτε να ρυθμίσετε τον Έλεγχο ταυτότητας Windows μετά την εγκατάσταση του διακομιστή ESET PROTECT.

Μπορώ να χρησιμοποιήσω MariaDB αντί του MySQL;

Όχι, το MariaDB δεν υποστηρίζεται. Βεβαιωθείτε ότι έχετε εγκαταστήσει μια υποστηριζόμενη έκδοση του διακομιστή MySQL και της σύνδεσης ODBC. Ανατρέξτε στο κεφάλαιο Εγκατάσταση και ρύθμιση παραμέτρων του MySQL.

Έπρεπε να εγκαταστήσω το Microsoft .NET Framework 4 όπως μου υπέδειξε το πρόγραμμα εγκατάστασης του ESET PROTECT On-Prem (http://www.microsoft.com/en-us/download/details.aspx?id=17851),

αλλά δεν λειτουργεί σε νέα εγκατάσταση του Windows Server 2012 R2 με SP1.

Δεν είναι δυνατή η χρήση αυτού του προγράμματος εγκατάστασης σε Windows Server 2012 λόγω πολιτικής ασφαλείας του Windows Server 2012. Το Microsoft .NET Framework πρέπει να εγκαθίσταται μέσω του στοιχείου **Οδηγός ρόλων και δυνατοτήτων**.

Είναι πολύ δύσκολο να διακρίνω εάν εκτελείται η εγκατάσταση του SQL Server. Πώς μπορώ να καταλάβω τι συμβαίνει εάν η εγκατάσταση διαρκεί περισσότερο από 10 λεπτά;

Η εγκατάσταση του SQL Server μπορεί να διαρκέσει μέχρι και 1 ώρα, σε σπάνιες περιπτώσεις. Ο χρόνος εγκατάστασης εξαρτάται από τις επιδόσεις του συστήματος.

Πώς μπορώ να κάνω επαναφορά του κωδικού πρόσβασης διαχειριστή για την κονσόλα διαδικτύου (που εισάγεται κατά τη ρύθμιση);

Μπορείτε να κάνετε επαναφορά του κωδικού πρόσβασης με εκτέλεση του προγράμματος εγκατάστασης του διακομιστή και επιλέγοντας **Επιδιόρθωση**. Έχετε υπόψη ότι μπορεί να απαιτείται ο κωδικός πρόσβασης για την πρόσβαση στη βάση δεδομένων ESET PROTECT, εάν δεν χρησιμοποιήσατε έλεγχο ταυτότητας των Windows κατά τη δημιουργία της βάσης δεδομένων.

- Απαιτείται προσοχή επειδή ορισμένες επιλογές επιδιόρθωσης ενδέχεται να καταργήσουν αποθηκευμένα δεδομένα.
- Η επαναφορά κωδικού πρόσβασης απενεργοποιεί το 2FA.

Κατά την εισαγωγή ενός αρχείου που περιέχει μια λίστα υπολογιστών για προσθήκη στο ESET PROTECT On-Prem, ποια είναι η μορφή που απαιτείται για το αρχείο;

Η μορφή είναι οι ακόλουθες γραμμές:

All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX

Το απαιτούμενο όνομα της ριζικής ομάδας είναι **Όλα**.

Μπορεί να χρησιμοποιηθεί IIS αντί για Apache Tomcat; Μπορεί να χρησιμοποιηθεί άλλος διακομιστής HTTP;

Το IIS είναι διακομιστής HTTP. Η κονσόλα διαδικτύου απαιτεί κοντέινερ Java servlet (όπως το Apache Tomcat) για να λειτουργήσει και δεν επαρκεί ο διακομιστής HTTP. Έχουν εντοπιστεί λύσεις σχετικά με τον τρόπο αλλαγής του IIS σε κοντέινερ Java servlet, αλλά γενικά, δεν υποστηρίζεται.

> Δεν χρησιμοποιούμε διακομιστή Apache HTTP, χρησιμοποιούμε Apache Tomcat, που είναι διαφορετικό προϊόν.

Το ESET PROTECT On-Prem έχει περιβάλλον γραμμής εντολών;

Ναι, διαθέτει το ESET PROTECT On-Prem ServerApi.

Μπορώ να εγκαταστήσω το ESET PROTECT On-Prem σε ελεγκτή τομέα;

Μην εγκαταστήσετε το SQL Server σε έναν Ελεγκτή τομέα (για παράδειγμα, Windows SBS / Essentials). Συνιστάται να εγκαταστήσετε το ESET PROTECT On-Prem σε διαφορετικό διακομιστή ή να μην επιλέξετε το στοιχείο του SQL Server Express κατά την εγκατάσταση (αυτό απαιτεί να χρησιμοποιήσετε το υπάρχον SQL ή MySQL Server για την εκτέλεση της βάσης δεδομένων ESET PROTECT).

Η εγκατάσταση διακομιστή ESET PROTECT θα ανιχνεύσει εάν είναι ήδη εγκατεστημένο το SQL στο σύστημα; Τι θα συμβεί

εάν το ανιχνεύσει; Τι συμβαίνει με το MySQL;

Το ESET PROTECT On-Prem θα ελέγξει εάν εκτελείται το SQL σε ένα σύστημα, σε περίπτωση που χρησιμοποιείτε τον οδηγό εγκατάστασης και έχετε επιλέξτε SQL express για εγκατάσταση. Σε περίπτωση που εκτελείται ήδη SQL σε ένα σύστημα, ο οδηγός θα εμφανίσει μια ειδοποίηση για απεγκατάσταση του υπάρχοντος SQL και στη συνέχεια θα εκτελέσει ξανά την εγκατάσταση ή θα εγκαταστήσει το ESET PROTECT On-Prem χωρίς το SQL Express. Δείτε τις απαιτήσεις βάσης δεδομένων για το ESET PROTECT On-Prem.

Πού μπορώ να βρω ένα στοιχείο του ESET PROTECT αντιστοιχισμένο σύμφωνα με την έκδοση κυκλοφορίας του;

Ανατρέξτε στο σχετικό άρθρο της Γνωσιακής βάσης.

Πώς μπορώ να κάνω αναβάθμιση του ESET PROTECT On-Prem στην πιο πρόσφατη έκδοση;

Ανατρέξτε στο θέμα διαδικασίες αναβάθμισης.

Πώς μπορώ να ενημερώσω ένα σύστημα χωρίς σύνδεση στο διαδίκτυο;

Χρησιμοποιώντας ESET Bridge διακομιστή μεσολάβησης HTTP σε έναν υπολογιστή που μπορεί να συνδεθεί με τους διακομιστές ενημέρωσης της ESET (όπου αποθηκεύονται προσωρινά τα αρχεία ενημέρωσης) και κατευθύνοντας τα τερματικά στο συγκεκριμένο διακομιστή μεσολάβησης HTTP σε ένα τοπικό δίκτυο. Εάν ο διακομιστής σας δεν έχει σύνδεση στο Internet, μπορείτε να ενεργοποιήσετε τη δυνατότητα ειδώλου στο προϊόν τελικού σημείου σε έναν υπολογιστή, να χρησιμοποιήσετε μια μονάδα δίσκου USB για την παράδοση των αρχεία ενημερώσεων σε αυτό τον υπολογιστή και να διαμορφώσετε όλους τους άλλους υπολογιστές εκτός σύνδεσης ώστε να τον χρησιμοποιούν ως διακομιστή ενημέρωσης.

Για λεπτομέρειες σχετικά με την πραγματοποίηση εγκατάσταση χωρίς σύνδεση, ακολουθήστε αυτές τις οδηγίες.

Πώς μπορώ να επανεγκαταστήσω τον Διακομιστή ESET PROTECT και να τον συνδέσω με έναν υπάρχοντα διακομιστή SQL, εάν ο διακομιστής SQL ρυθμίστηκε αυτόματα από την αρχική εγκατάσταση του ESET PROTECT On-Prem;

Εάν εγκαθιστάτε τη νέα εμφάνιση του διακομιστή ESET PROTECT χρησιμοποιώντας τον ίδιο λογαριασμό χρήστη (για παράδειγμα, έναν λογαριασμό διαχειριστή τομέα) με τον οποίο εγκαταστήσατε τον αρχικό διακομιστή ESET PROTECT, μπορείτε να χρησιμοποιήσετε το στοιχείο **MS SQL Server μέσω ελέγχου ταυτότητας Windows**.

Πώς μπορώ να διορθώσω προβλήματα με το συγχρονισμό του Active Directory στο Linux;

Βεβαιωθείτε ότι το όνομα τομέα σας έχει εισαχθεί με κεφαλαία γράμματα (`administrator@TEST.LOCAL` αντί `administrator@test.local`).

Υπάρχει τρόπος να χρησιμοποιήσω τον πόρο του δικού μου δικτύου (όπως κοινή χρήση SMB) αντί για το χώρο αποθήκευσης;

Μπορείτε να επιλέξετε να παράσχετε απευθείας τη διεύθυνση URL στην οποία βρίσκεται το πακέτο. Εάν χρησιμοποιείτε κοινόχρηστο αρχείο, καθορίστε το με την παρακάτω μορφή: file:// ακολουθούμενο από την πλήρη διαδρομή δικτύου προς το αρχείο, για παράδειγμα:

file://\\eraserver\install\ees_nt64_ENU.msi

Πώς μπορώ να επαναφέρω ή να αλλάξω τον κωδικό πρόσβασής μου;

Υπό ιδανικές συνθήκες, ο λογαριασμός διαχειριστή θα πρέπει να χρησιμοποιείται μόνο για τη δημιουργία λογαριασμών για μεμονωμένους διαχειριστές. Αφού δημιουργηθούν οι λογαριασμοί διαχειριστή, ο κωδικός πρόσβασης διαχειριστή θα πρέπει να αποθηκευτεί και δεν θα πρέπει να

χρησιμοποιείται ο λογαριασμός διαχειριστή. Αυτή η πρακτική επιτρέπει ο λογαριασμός διαχειριστή να χρησιμοποιείται μόνο για την επαναφορά κωδικών πρόσβασης/στοιχείων λογαριασμού.

Πώς να επαναφέρετε τον κωδικό πρόσβασης ενός ενσωματωμένου λογαριασμού διαχειριστή ESET PROTECT On-Prem:

1.Ανοίξτε το στοιχείο **Προγράμματα και δυνατότητες** (εκτελέστε το αρχείο appwiz.cpl), εντοπίστε το διακομιστή ESET PROTECT και κάντε δεξί κλικ.

2.Επιλέξτε **Αλλαγή** από το μενού περιβάλλοντος.

3.Επιλέξτε **Επιδιόρθωση**.

4.Καθορίστε τα στοιχεία σύνδεσης της βάσης δεδομένων.

5.Επιλέξτε **Χρήση της υπάρχουσας βάσης δεδομένων**.

6.Καταργήστε την επιλογή του πλαισίου ελέγχου **Χρήση κωδικού πρόσβασης που είναι ήδη αποθηκευμένος στη βάση δεδομένων** και εισαγάγετε νέο κωδικό πρόσβασης.

7.Συνδεθείτε στην κονσόλα διαδικτύου ESET PROTECT με τον νέο κωδικό πρόσβασης.

i Συνιστάται ιδιαίτερα να δημιουργήσετε οπωσδήποτε πρόσθετους λογαριασμούς με συγκεκριμένα δικαιώματα πρόσβασης, βάσει των αρμοδιοτήτων του λογαριασμού που θέλετε να παράσχετε.

Πώς μπορώ να αλλάξω τις θύρες του διακομιστή ESET PROTECT και της κονσόλας διαδικτύου ESET PROTECT;

Είναι απαραίτητο να αλλάξετε τη θύρα στη διαμόρφωση του διακομιστή διαδικτύου για να επιτρέπονται συνδέσεις διακομιστή διαδικτύου στη νέα θύρα. Για να το κάνετε αυτό, ακολουθήστε τα παρακάτω βήματα:

1. Τερματίστε τη λειτουργία του διακομιστή διαδικτύου.

2. Τροποποιήστε τη θύρα στη διαμόρφωση του διακομιστή διαδικτύου.

   a)Ανοίξτε το αρχείο *webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*

   b)Ρυθμίστε τον νέο αριθμό θύρας, για παράδειγμα,`server_port=44591`)

3. Ξεκινήστε ξανά το διακομιστή διαδικτύου.

Μπορώ να αναβαθμίσω από το ERA5.x/6.x ή το ESMC7.x απευθείας στο ESET PROTECT On-Prem 11.0 μέσω του προγράμματος εγκατάστασης «όλα σε ένα»;

Μπορείτε να αναβαθμίσετε σε ESET PROTECT On-Prem 11.0 από ESET PROTECT On-Prem 9.0 και νεότερες εκδόσεις. Η απευθείας αναβάθμιση από τις εκδόσεις τέλους του κύκλου ζωής 7.2–8.x δεν έχει δοκιμαστεί και δεν υποστηρίζεται.

Εάν έχετε το ERA 5.x/6.x ή το ESMC 7.0/7.1, η άμεση αναβάθμιση σε ESET PROTECT On-Prem 11.0 δεν υποστηρίζεται – Εκτελέστε μια καθαρή εγκατάσταση του ESET PROTECT On-Prem 11.0.

Λαμβάνω μηνύματα σφάλματος ή αντιμετωπίζω προβλήματα με το ESET PROTECT On-Prem. Τι πρέπει να κάνω;

Ανατρέξτε στο κεφάλαιο Συχνές ερωτήσεις αντιμετώπισης προβλημάτων.

Συμφωνία άδειας 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 τη λειτουργία του Λογισμικού και για την ενημέρωση και αναβάθμιση του Λογισμικού. Ο Πάροχος θα δικαιούται να εκδίδει 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_business. 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.

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

Προώθηση των πληροφοριών στον Πάροχο. Εφαρμόζονται πρόσθετες διατάξεις στην Προώθηση των πληροφοριών στον Πάροχο ως ακολούθως:

Το Λογισμικό περιέχει λειτουργίες οι οποίες συλλέγουν δεδομένα σχετικά με τη διαδικασία εγκατάστασης, τον υπολογιστή ή/και την πλατφόρμα στην οποία έχει εγκατασταθεί το Λογισμικό, πληροφορίες σχετικά με τις δυνατότητες και τη λειτουργικότητα του Λογισμικού, καθώς και πληροφορίες σχετικά με διαχειριζόμενες συσκευές (στο εξής «Πληροφορίες»), και στη συνέχεια τις αποστέλλει στον Πάροχο. Οι Πληροφορίες μπορεί να περιλαμβάνουν δεδομένα (συμπεριλαμβανομένων προσωπικών δεδομένων που έχουν αποκτηθεί τυχαία ή κατά λάθος) σχετικά με τις διαχειριζόμενες συσκευές. Με την ενεργοποίηση αυτής της λειτουργίας του λογισμικού, ο πάροχος μπορεί να συλλέγει και να επεξεργάζεται πληροφορίες, όπως καθορίζεται στην Πολιτική Απορρήτου και σύμφωνα με τους σχετικούς νομικούς κανονισμούς.

Το Λογισμικό απαιτεί την εγκατάσταση ενός στοιχείου στον διαχειριζόμενο υπολογιστή, το οποίο επιτρέπει τη μεταφορά πληροφοριών μεταξύ του διαχειριζόμενου υπολογιστή και του λογισμικού απομακρυσμένης διαχείρισης. Οι πληροφορίες οι οποίες υπόκεινται σε μεταφορά περιέχουν δεδομένα διαχείρισης, όπως πληροφορίες υλικού και λογισμικού του διαχειριζόμενου υπολογιστή και οδηγίες διαχείρισης από το λογισμικό απομακρυσμένης διαχείρισης. Άλλο περιεχόμενο δεδομένων που μεταφέρεται από τον διαχειριζόμενο υπολογιστή θα προσδιορίζεται από τις ρυθμίσεις του λογισμικού που έχει εγκατασταθεί στον διαχειριζόμενο υπολογιστή. Το περιεχόμενο οδηγιών από το λογισμικό διαχείρισης θα προσδιορίζεται από τις ρυθμίσεις του λογισμικού απομακρυσμένης διαχείρισης.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Πολιτική απορρήτου

Η ESET, spol. s r. o., με έδρα στη διεύθυνση Einsteinova 24, 851 01 Μπρατισλάβα, Δημοκρατία της Σλοβακίας, εγγεγραμμένη στο Εμπορικό Μητρώο δικαιοδοσίας του Πρώτου Πρωτοδικείου της Μπρατισλάβα, ενότητα Sro, με αριθμό 3586/B, Αριθμός μητρώου επιχειρήσεων: 31333532, ως Συλλογέας δεδομένων (εφεξής «ESET» ή «εταιρεία») επιθυμεί διαφάνεια σε ό,τι αφορά την επεξεργασία των προσωπικών δεδομένων και του απορρήτου των πελατών της. Για να επιτευχθεί αυτός ο στόχος, η εταιρεία δημοσιεύει την παρούσα Πολιτική Απορρήτου με αποκλειστικό σκοπό την ενημέρωση του πελάτη (εφεξής «Τελικός χρήστης» ή «χρήστης») σχετικά με τα ακόλουθα θέματα:

- Επεξεργασία προσωπικών δεδομένων,
- Εμπιστευτικότητα δεδομένων,
- Δικαιώματα του υποκειμένου δεδομένων.

Επεξεργασία προσωπικών δεδομένων

Οι υπηρεσίες που παρέχονται από την ESET, οι οποίες υλοποιούνται στο προϊόν, παρέχονται σύμφωνα με τους όρους χρήσης της Συμφωνίας Άδειας Χρήσης Τελικού Χρήστη (εφεξής «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 EULA και στην τεκμηρίωση προϊόντος, όπως η υπηρεσία ενημέρωσης/αναβάθμισης, το ESET LiveGrid®, η προστασία κατά της κατάχρησης δεδομένων, η υποστήριξη, κ.λπ. Για να λειτουργούν όλες αυτές οι υπηρεσίες, η εταιρεία πρέπει να συλλέγει τις ακόλουθες πληροφορίες:

• Η διαχείριση των προϊόντων ESET Security απαιτεί και αποθηκεύονται τοπικά πληροφορίες όπως το αναγνωριστικό θέσης και το όνομα, το όνομα προϊόντος, τις πληροφορίες άδειας χρήσης, τις πληροφορίες ενεργοποίησης και λήξης, τις πληροφορίες υλικού και λογισμικού που αφορούν τον διαχειριζόμενο υπολογιστή στον οποίο έχει εγκατασταθεί το προϊόν ESET Security. Αρχεία καταγραφής που αφορούν δραστηριότητες διαχειριζόμενων προϊόντων και συσκευών ESET Security συλλέγονται και είναι διαθέσιμα ώστε να διευκολύνεται η διαχείριση και η εποπτεία δυνατοτήτων και υπηρεσιών χωρίς αυτοματοποιημένη υποβολή στην ESET.

• Πληροφορίες που αφορούν τη διεργασία εγκατάστασης, όπως την πλατφόρμα στην οποία εγκαθίσταται το προϊόν και πληροφορίες σχετικά με τις λειτουργίες και τη λειτουργικότητα των προϊόντων, όπως το δακτυλικό αποτύπωμα υλικού, τα αναγνωριστικά εγκατάστασης, τα αρχεία ένδειξης σφαλμάτων, τα αναγνωριστικά άδειας χρήσης, τη διεύθυνση IP, τη διεύθυνση MAC, τις ρυθμίσεις διαμόρφωσης του προϊόντος, οι οποίες μπορεί να συμπεριλαμβάνουν επίσης διαχειριζόμενες συσκευές.

• Πληροφορίες αδειοδότησης όπως το αναγνωριστικό άδειας χρήσης και προσωπικά δεδομένα όπως το όνομα, το επίθετο, η διεύθυνση, η διεύθυνση ηλεκτρονικού ταχυδρομείου απαιτούνται για σκοπούς τιμολόγησης, επαλήθευσης της γνησιότητας της άδειας χρήσης και για την παροχή των υπηρεσιών της εταιρείας.

• Για την υπηρεσία υποστήριξης απαιτούνται στοιχεία επικοινωνίας και δεδομένα που περιέχονται στα αιτήματα υποστήριξης του χρήστη. Ανάλογα με τον τρόπο που θα επιλέξει ο χρήστης να επικοινωνήσει με την εταιρεία, η εταιρεία μπορεί να συλλέξει τη διεύθυνση ηλεκτρονικού

ταχυδρομείου, το τηλέφωνο, τις πληροφορίες άδειας χρήσης, τα στοιχεία του προϊόντος και την περιγραφή της υπόθεσης υποστήριξης του χρήστη. Ενδέχεται να ζητηθεί από το χρήστη να παράσχει στην εταιρεία και άλλες πληροφορίες για να διευκολυνθεί η υπηρεσία της υποστήριξης, όπως αρχεία καταγραφής που έχουν δημιουργηθεί.

• Τα δεδομένα που αφορούν τη χρήση της υπηρεσίας μας είναι απολύτως ανώνυμα μέχρι το τέλος της περιόδου λειτουργίας. Μετά το τέλος της περιόδου λειτουργίας δεν αποθηκεύονται προσωπικές πληροφορίες ταυτοποίησης.

Εμπιστευτικότητα δεδομένων

Η ESET είναι μια εταιρεία που δραστηριοποιείται σε όλο τον κόσμο μέσω των θυγατρικών της ή συνεργατών της, ως μέρος του δικτύου διανομής, σέρβις και υποστήριξης. Οι πληροφορίες που επεξεργάζεται η ESET ενδέχεται να μεταφερθούν σε ή από θυγατρικές ή συνεργάτες της για την εκτέλεση της Συμφωνίας Άδειας Χρήσης Τελικού Χρήστη, όπως η παροχή υπηρεσιών ή η υποστήριξη ή η τιμολόγηση. Ανάλογα με την τοποθεσία και την υπηρεσία που επιλέγει να χρησιμοποιήσει ο χρήστης, η εταιρεία ενδέχεται να χρειαστεί να μεταφέρει τα δεδομένα του σε χώρα στην οποία δεν ισχύει η απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής. Ακόμα και σε αυτή την περίπτωση, κάθε μεταφορά πληροφοριών υπόκειται στη νομοθεσία προστασίας δεδομένων και πραγματοποιείται μόνο εφόσον απαιτείται. Οι Τυπικοί συμβατικοί όροι, οι Δεσμευτικοί εταιρικοί κανόνες ή άλλες κατάλληλες εξασφαλίσεις πρέπει να δημιουργούνται χωρίς καμία εξαίρεση.

Η εταιρεία κάνει κάθε προσπάθεια για να αποτρέπει την αποθήκευση δεδομένων για διάστημα μεγαλύτερο από αυτό που απαιτείται ενόσω παρέχονται υπηρεσίες σύμφωνα με τη Συμφωνία Άδειας Χρήσης Τελικού Χρήστη. Το διάστημα διατήρησης δεδομένων της εταιρείας μπορεί να είναι μεγαλύτερο από την εγκυρότητα της άδειας χρήσης του χρήστη, ώστε να έχει ο χρήστης το χρόνο να πραγματοποιήσει την ανανέωση εύκολα και άνετα. Ελαχιστοποιημένα στατιστικά με ψευδώνυμα και άλλα δεδομένα από το ESET LiveGrid® ενδέχεται να υποβληθούν σε περαιτέρω επεξεργασία για στατιστικούς σκοπούς.

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 δυνατή προσπάθεια για να διασφαλίζει διαρκώς την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την αντοχή 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 εποπτεύουσα αρχή, καθώς και τα υποκείμενα των δεδομένων. Ως υποκείμενο δεδομένων, ο χρήστης έχει το δικαίωμα να υποβάλλει καταγγελία σε μια εποπτεύουσα αρχή.

Δικαιώματα του υποκειμένου δεδομένων

Η ESET υπόκειται στους κανονισμούς της νομοθεσίας της Σλοβακίας και δεσμεύεται από τη νομοθεσία περί προστασίας δεδομένων της Ευρωπαϊκής Ένωσης. Υπό την αίρεση των προϋποθέσεων που ορίζονται από την ισχύουσα νομοθεσία περί προστασίας δεδομένων, ο χρήστης έχει τα ακόλουθα δικαιώματα ως υποκείμενο των δεδομένων:

• το δικαίωμα να ζητήσει από την ESET πρόσβαση στα προσωπικά δεδομένα του,

• το δικαίωμα επανόρθωσης των προσωπικών δεδομένων του εάν είναι ανακριβή (ο χρήστης έχει επίσης το δικαίωμα να ζητήσει να συμπληρωθούν τα ατελή προσωπικά δεδομένα),

• το δικαίωμα να ζητήσει διαγραφή των προσωπικών δεδομένων του,

- το δικαίωμα να ζητήσει περιορισμό της επεξεργασίας των προσωπικών δεδομένων του,
- το δικαίωμα ένστασης στην επεξεργασία
- το δικαίωμα υποβολής παραπόνου, καθώς και
- το δικαίωμα στη φορητότητα δεδομένων.

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