ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Ασφάλεια Πληροφοριών

«Windows Security Policies»

Τμήμα Πληροφορικής

Επικ. Καθηγητής Π. Κοτζανικολάου,
Υπ.Δρ. Β. Μάλαμας

Περιεχόμενα

Εισαγωγή

Windows Security Policies

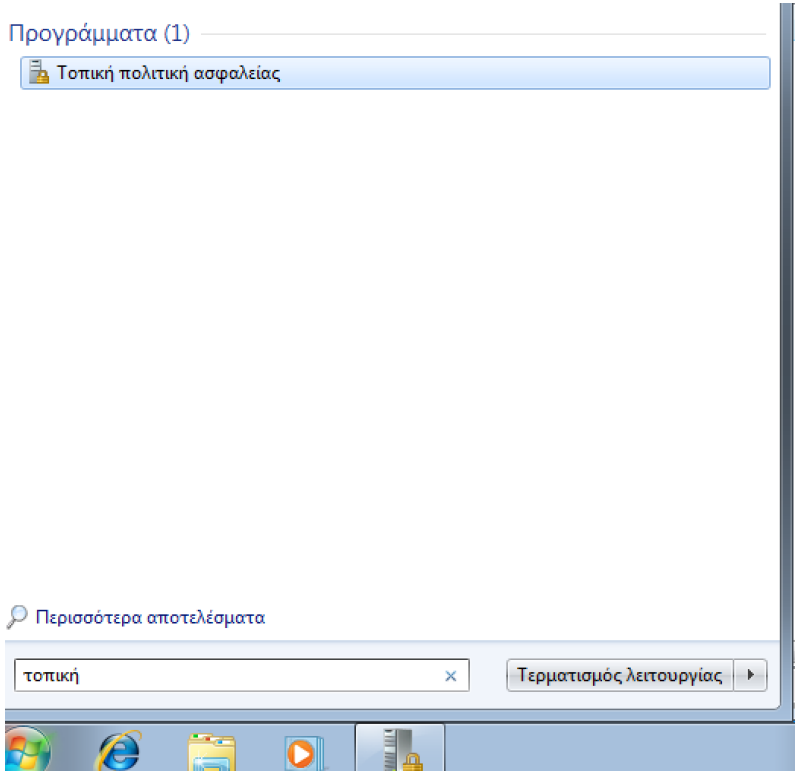
Πρόκειται για ένα πολύτιμο εργαλείο για τον έλεγχο της χρήσης και της ασφάλειας που προσφέρουν τα windows και με το οποίο μπορούμε να ρυθμίσουμε πολλές πτυχές του λειτουργικού συστήματος

Μέσα απο αυτό το εργαλείο μπορούμε να επιτρέψουμε ή να αποκλείσουμε ένα χρήστη ή μια ομάδα χρηστών απο διάφορες λειτουργίες του συστήματος.

Μπορούμε για παράδειγμα να φτιάξουμε μια πολιτική ασφάλειας που να απαγορεύει σε χρήστες να εγκαταστήσουν νέο λογισμικό ή να έχουν πρόσβαση στο διαδίκτυο ή ακόμα και να τους αποκλείσουμε απο το να εισέλθουν σε μια εφαρμογή (για παράδειγμα στον Πίνακα Ελέγχου)

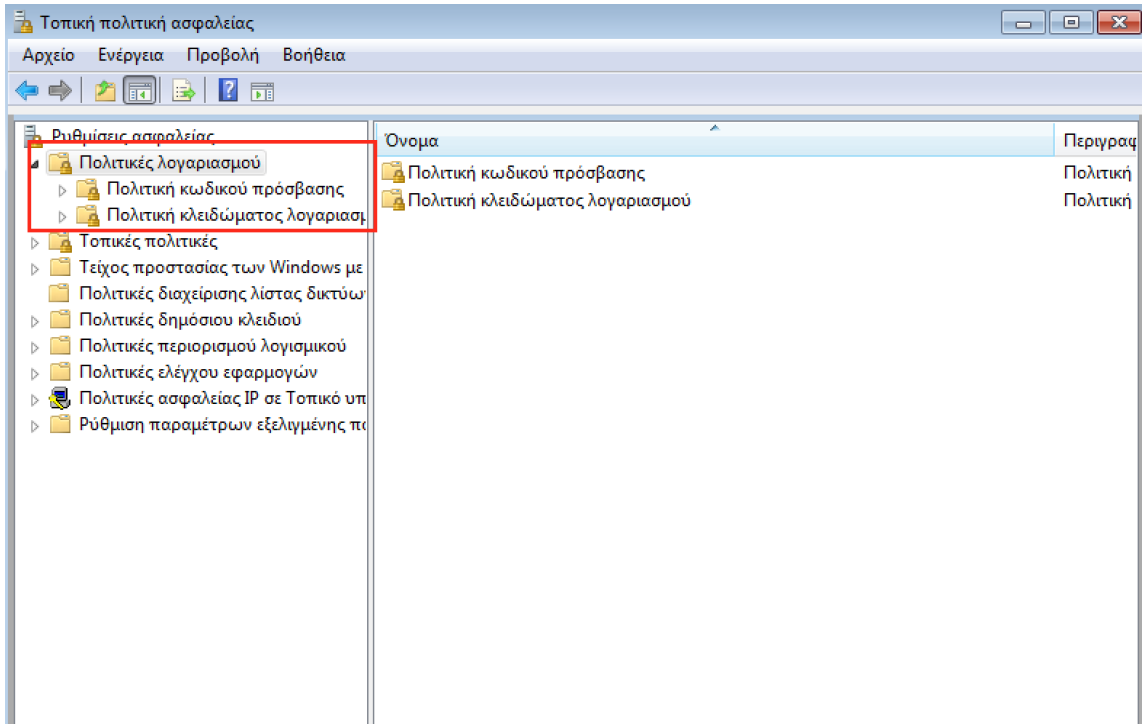
Πρόσβαση στις πολιτικές ασφάλειας

Για να εισέλθουμε στις τοπικές πολιτικές ασφάλειας πληκτρολογούμε στην αναζήτηση τοπικές πολιτικές:



Account policies (πολιτικές λογαριασμού)

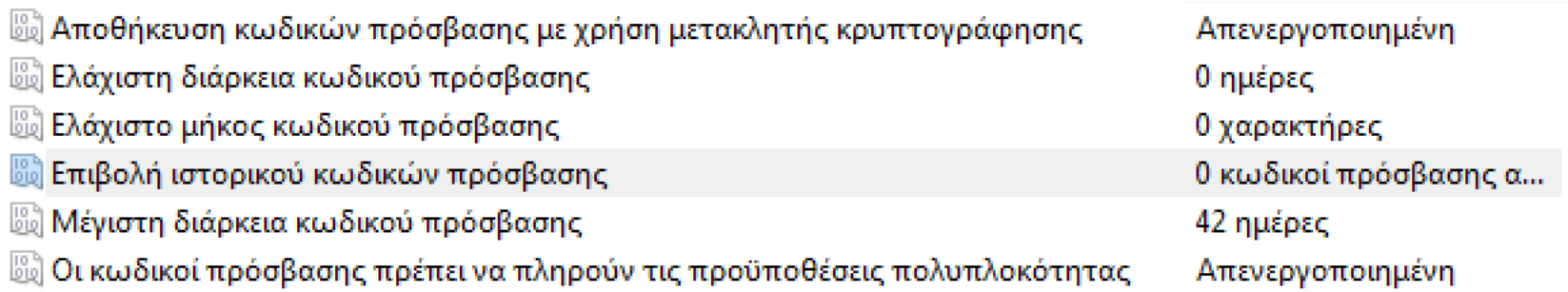
Στις πολιτικές λογαριασμού έχουμε δύο βασικές κατηγορίες την **πολιτική κωδικού πρόσβασης** και την **πολιτική κλειδώματος λογαριασμού**.



Account policies (πολιτικές λογαριασμού)

πολιτική κωδικού πρόσβασης

1. **ελάχιστη διάρκεια κωδικού πρόσβασης:** Για πόσο χρονικό διάστημα θα μπορεί να χρησιμοποιείται ένας κωδικός πρόσβασης
2. **ελάχιστο μήκος κωδικού πρόσβασης:** Ορίζουμε το ελάχιστο επιτρεπτό μήκος
3. **επιβολή ιστορικού:** ώστε να αποτρέπουμε την επαναχρησιμοποίηση κωδικών
4. **μέγιστη διάρκεια:** εξασφάλιση ότι ο κωδικός αλλάζει σε συγκεκριμένα χρονικά διαστήματα
5. **πολυπλοκότητα:** δημιουργία ισχυρών κωδικών πρόσβασης



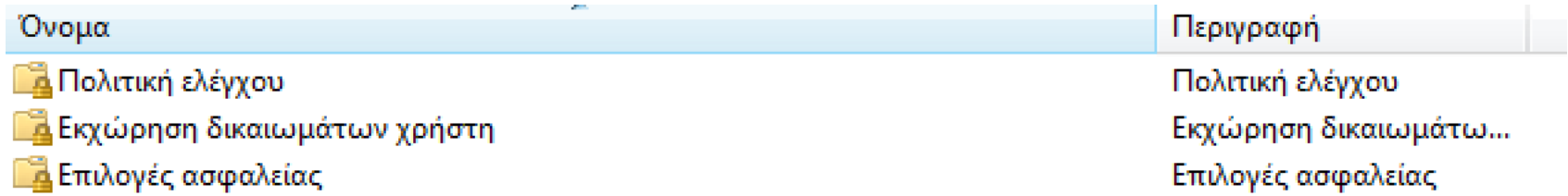
Account policies (πολιτικές λογαριασμού)

πολιτική κλειδώματος λογαριασμού

1. **επαναφορά μετρητή κλειδώματος ύστερα απο:** καθορίζει την διάρκεια κλειδώματος ύστερα απο ολοκλήρωση των επιτρεπτών προσπαθειών εισόδου
2. **κλείδωμα λογαριασμού για:** η χρονική διάρκεια για την οποία ένας λογαριασμός θα παραμείνει κλειδωμένος μετά απο αποτυχημένη προσπάθεια εισόδου
3. **όριο κλειδώματος λογαριασμου:** ο αριθμός των αποτυχημένων προσπαθειών που θα προκαλέσει κλείδωμα του λογαριασμού

Local policies (τοπικές πολιτικές)

Στις τοπικές πολιτικές έχουμε τρείς βασικές κατηγορίες την **πολιτική ελέγχου** ,την **εκχώρηση δικαιωμάτων χρήστη** και τις **επιλογές ασφάλειας**.



Local policies (τοπικές πολιτικές)

πολιτική ελέγχου

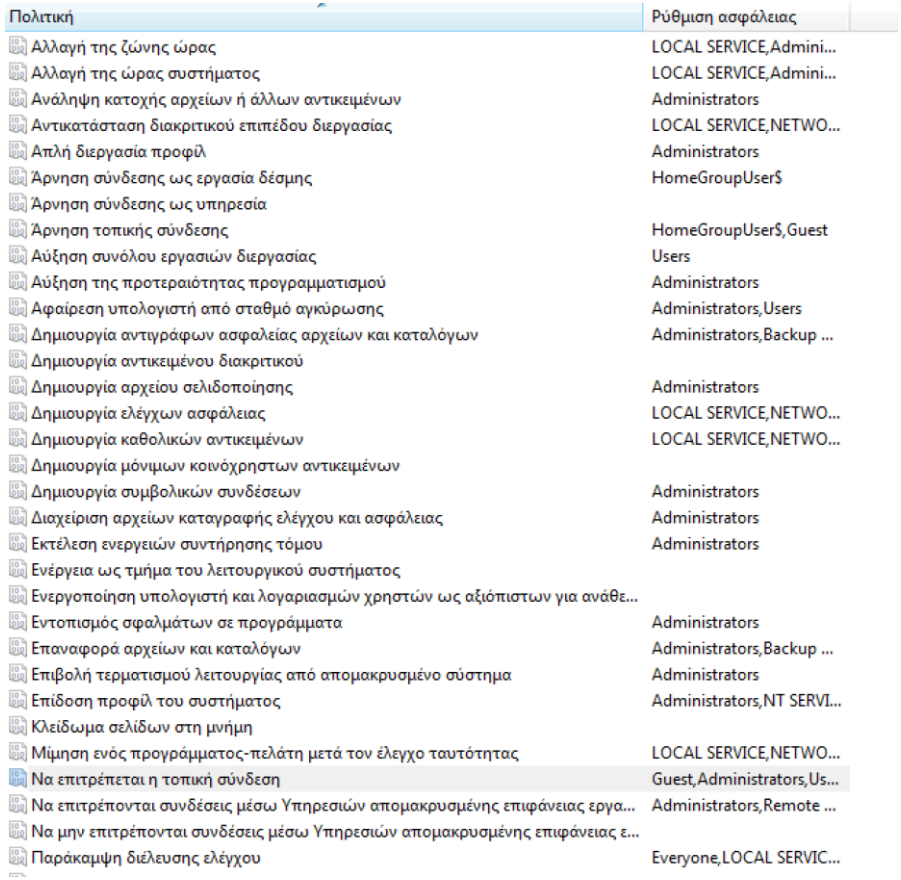
Κάθε μία απο τις παρακάτω επιλογές ελέγχει ποιά συμβάντα θα καταγράφονται στο αρχείο καταγραφής

Πολιτική	Ρύθμιση ασφάλειας
Αλλαγή της πολιτικής ελέγχου	Κανένας έλεγχος
Έλεγχος διαχείρισης των λογαριασμών	Κανένας έλεγχος
Έλεγχος παρακολούθησης διεργασίας	Κανένας έλεγχος
Έλεγχος πρόσβασης αντικειμένων	Κανένας έλεγχος
Έλεγχος πρόσβασης στην υπηρεσία καταλόγου	Κανένας έλεγχος
Έλεγχος συμβάντων σύνδεσης	Κανένας έλεγχος
Έλεγχος συμβάντων σύνδεσης λογαριασμού	Κανένας έλεγχος
Έλεγχος συμβάντων συστήματος	Κανένας έλεγχος
Έλεγχος χρήσης των δικαιωμάτων	Κανένας έλεγχος

Local policies (τοπικές πολιτικές)

εκχώρηση δικαιωμάτων χρήστη

Εδώ μπορούμε να προσθέσουμε ή
να αφαιρέσουμε δικαιώματα απο τους χρήστες



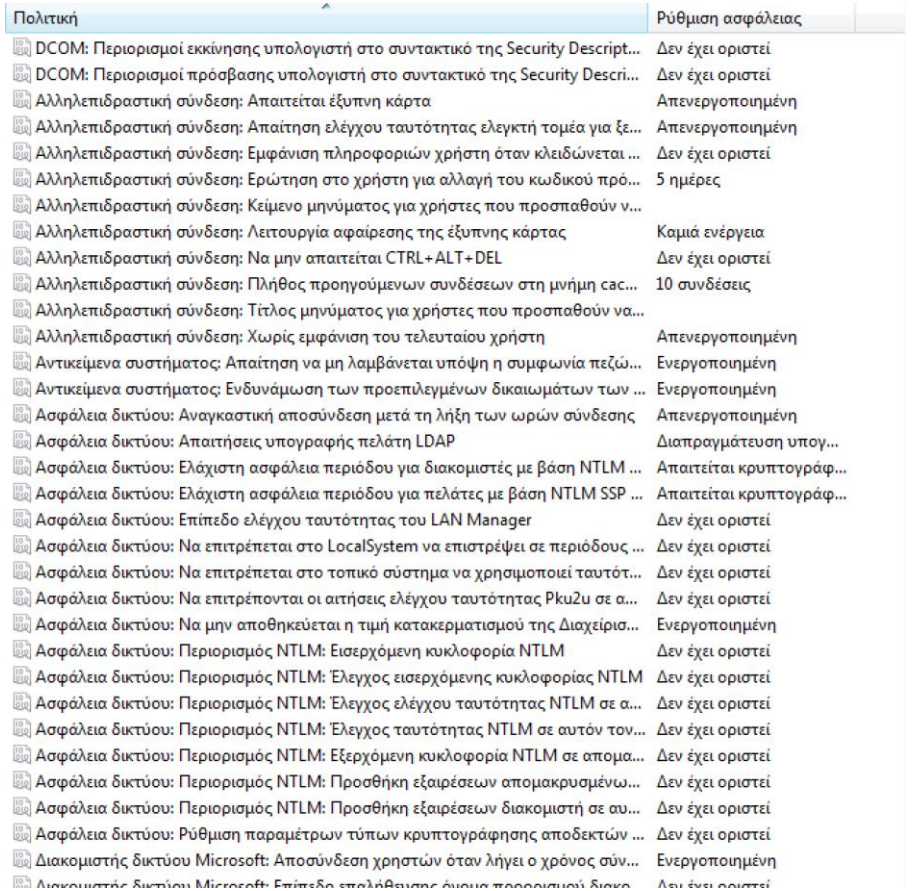
Πολιτική	Ρύθμιση ασφάλειας
Αλλαγή της ζώνης ώρας	LOCAL SERVICE,Admini...
Αλλαγή της ώρας συστήματος	LOCAL SERVICE,Admini...
Ανάληψη κατοχής αρχείων ή άλλων αντικειμένων	Administrators
Αντικατάσταση διακριτικού επιπέδου διεργασίας	LOCAL SERVICE,NETWO...
Απλή διεργασία προφίλ	Administrators
Άρνηση σύνδεσης ως εργασία δέσμης	HomeGroupUser$
Άρνηση σύνδεσης ως υπηρεσία	
Άρνηση τοπικής σύνδεσης	HomeGroupUser$,Guest
Αύξηση συνόλου εργασιών διεργασίας	Users
Αύξηση της προτεραιότητας προγραμματισμού	Administrators
Αφαίρεση υπολογιστή από σταθμό αγκύρωσης	Administrators,Users
Δημιουργία αντιγράφων ασφαλείας αρχείων και καταλόγων	Administrators,Backup ...
Δημιουργία αντικειμένου διακριτικού	
Δημιουργία αρχείου σελιδοποίησης	Administrators
Δημιουργία ελέγχων ασφάλειας	LOCAL SERVICE,NETWO...
Δημιουργία καθολικών αντικειμένων	LOCAL SERVICE,NETWO...
Δημιουργία μόνιμων κοινόχρηστων αντικειμένων	
Δημιουργία συμβολικών συνδέσεων	Administrators
Διαχείριση αρχείων καταγραφής ελέγχου και ασφάλειας	Administrators
Εκτέλεση ενεργειών συντήρησης τόμου	Administrators
Ενέργεια ως τμήμα του λειτουργικού συστήματος	
Ενεργοποίηση υπολογιστή και λογαριασμών χρηστών ως αξιόπιστων για ανάθε...	
Εντοπισμός σφαλμάτων σε προγράμματα	Administrators
Επαναφορά αρχείων και καταλόγων	Administrators,Backup ...
Επιβολή τερματισμού λειτουργίας από απομακρυσμένο σύστημα	Administrators
Επίδοση προφίλ του συστήματος	Administrators,NT SERVI...
Κλείδωμα σελίδων στη μνήμη	
Μίμηση ενός προγράμματος-πελάτη μετά τον έλεγχο ταυτότητας	LOCAL SERVICE,NETWO...
Να επιτρέπεται η τοπική σύνδεση	Guest,Administrators,Us...
Να επιτρέπονται συνδέσεις μέσω Υπηρεσιών απομακρυσμένης επιφάνειας εργα...	Administrators,Remote ...
Να μην επιτρέπονται συνδέσεις μέσω Υπηρεσιών απομακρυσμένης επιφάνειας ε...	
Παράκαμψη διέλευσης ελέγχου	Everyone,LOCAL SERVIC...

Local policies (τοπικές πολιτικές)

<u>επιλογές ασφάλειας</u>

Ρύθμιση επιλογών ασφάλειας τόσο σε επίπεδο δικτύου όσο και σε επίπεδο χρηστών

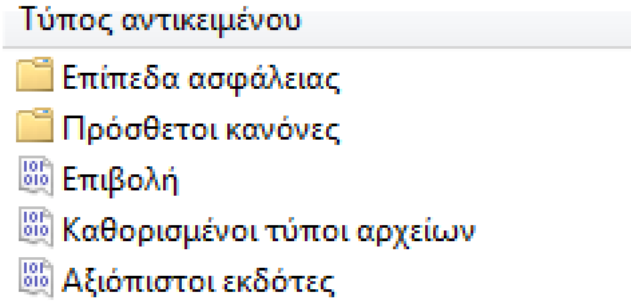
Επιλογές ασφάλειας και σε επίπεδο λειτουργικού



Πολιτική	Ρύθμιση ασφάλειας
DCOM: Περιορισμοί εκκίνησης υπολογιστή στο συντακτικό της Security Descript...	Δεν έχει οριστεί
DCOM: Περιορισμοί πρόσβασης υπολογιστή στο συντακτικό της Security Descri...	Δεν έχει οριστεί
Αλληλεπιδραστική σύνδεση: Απαιτείται έξυπνη κάρτα	Απενεργοποιημένη
Αλληλεπιδραστική σύνδεση: Απαίτηση ελέγχου ταυτότητας ελεγκτή τομέα για ξε...	Απενεργοποιημένη
Αλληλεπιδραστική σύνδεση: Εμφάνιση πληροφοριών χρήστη όταν κλειδώνεται ...	Δεν έχει οριστεί
Αλληλεπιδραστική σύνδεση: Ερώτηση στο χρήστη για αλλαγή του κωδικού πρό...	5 ημέρες
Αλληλεπιδραστική σύνδεση: Κείμενο μηνύματος για χρήστες που προσπαθούν ν...	
Αλληλεπιδραστική σύνδεση: Λειτουργία αφαίρεσης της έξυπνης κάρτας	Καμιά ενέργεια
Αλληλεπιδραστική σύνδεση: Να μην απαιτείται CTRL+ALT+DEL	Δεν έχει οριστεί
Αλληλεπιδραστική σύνδεση: Πλήθος προηγούμενων συνδέσεων στη μνήμη cac...	10 συνδέσεις
Αλληλεπιδραστική σύνδεση: Τίτλος μηνύματος για χρήστες που προσπαθούν να...	
Αλληλεπιδραστική σύνδεση: Χωρίς εμφάνιση του τελευταίου χρήστη	Απενεργοποιημένη
Αντικείμενα συστήματος: Απαίτηση να μη λαμβάνεται υπόψη η συμφωνία πεζώ...	Ενεργοποιημένη
Αντικείμενα συστήματος: Ενδυνάμωση των προεπιλεγμένων δικαιωμάτων των ...	Ενεργοποιημένη
Ασφάλεια δικτύου: Αναγκαστική αποσύνδεση μετά τη λήξη των ωρών σύνδεσης	Απενεργοποιημένη
Ασφάλεια δικτύου: Απαιτήσεις υπογραφής πελάτη LDAP	Διαπραγμάτευση υπογ...
Ασφάλεια δικτύου: Ελάχιστη ασφάλεια περιόδου για διακομιστές με βάση NTLM ...	Απαιτείται κρυπτογράφ...
Ασφάλεια δικτύου: Ελάχιστη ασφάλεια περιόδου για πελάτες με βάση NTLM SSP ...	Απαιτείται κρυπτογράφ...
Ασφάλεια δικτύου: Επίπεδο ελέγχου ταυτότητας του LAN Manager	Δεν έχει οριστεί
Ασφάλεια δικτύου: Να επιτρέπεται στο LocalSystem να επιστρέψει σε περιόδους ...	Δεν έχει οριστεί
Ασφάλεια δικτύου: Να επιτρέπεται στο τοπικό σύστημα να χρησιμοποιεί ταυτότ...	Δεν έχει οριστεί
Ασφάλεια δικτύου: Να επιτρέπονται οι αιτήσεις ελέγχου ταυτότητας Pku2u σε α...	Δεν έχει οριστεί
Ασφάλεια δικτύου: Να μην αποθηκεύεται η τιμή κατακερματισμού της Διαχείρισ...	Ενεργοποιημένη
Ασφάλεια δικτύου: Περιορισμός NTLM: Εισερχόμενη κυκλοφορία NTLM	Δεν έχει οριστεί
Ασφάλεια δικτύου: Περιορισμός NTLM: Έλεγχος εισερχόμενης κυκλοφορίας NTLM	Δεν έχει οριστεί
Ασφάλεια δικτύου: Περιορισμός NTLM: Έλεγχος ελέγχου ταυτότητας NTLM σε α...	Δεν έχει οριστεί
Ασφάλεια δικτύου: Περιορισμός NTLM: Έλεγχος ταυτότητας NTLM σε αυτόν τον...	Δεν έχει οριστεί
Ασφάλεια δικτύου: Περιορισμός NTLM: Εξερχόμενη κυκλοφορία NTLM σε απομα...	Δεν έχει οριστεί
Ασφάλεια δικτύου: Περιορισμός NTLM: Προσθήκη εξαιρέσεων απομακρυσμένω...	Δεν έχει οριστεί
Ασφάλεια δικτύου: Περιορισμός NTLM: Προσθήκη εξαιρέσεων διακομιστή σε αυ...	Δεν έχει οριστεί
Ασφάλεια δικτύου: Ρύθμιση παραμέτρων τύπων κρυπτογράφησης αποδεκτών ...	Δεν έχει οριστεί
Διακομιστής δικτύου Microsoft: Αποσύνδεση χρηστών όταν λήγει ο χρόνος σύν...	Ενεργοποιημένη
Διακομιστής δικτύου Microsoft: Επίπεδο επαλήθευσης όνομα προορισμού διακο...	Δεν έχει οριστεί

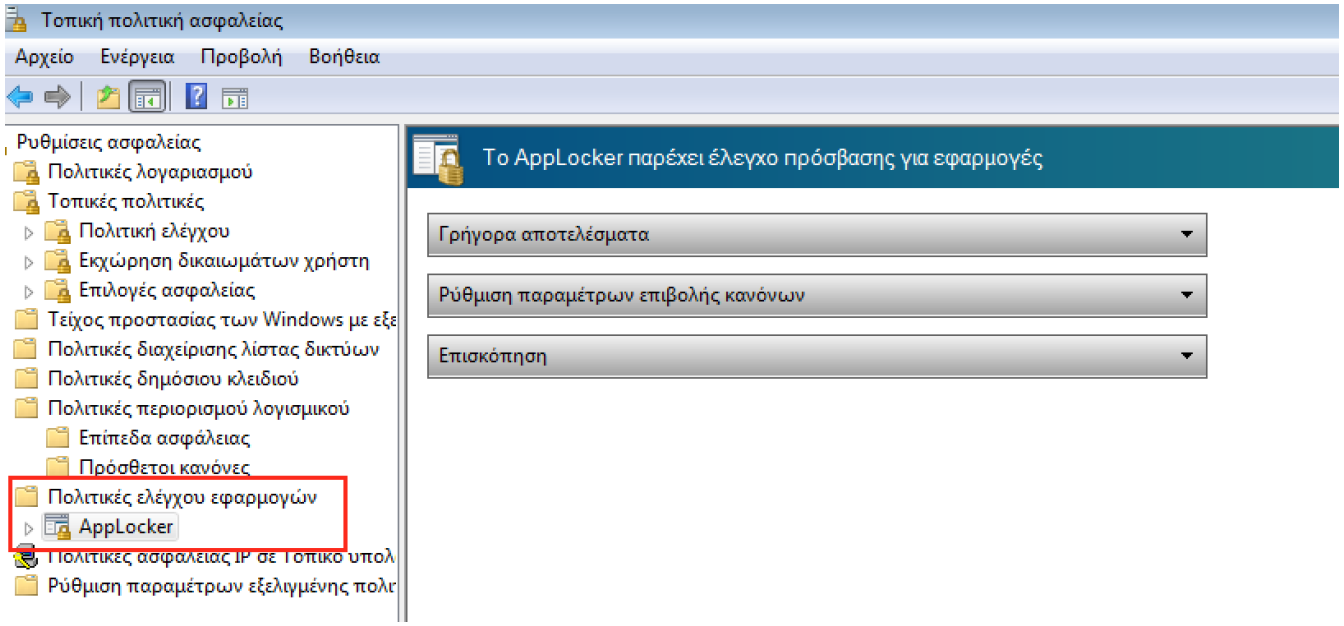
Software restrictions policies (κανόνες περιορισμού λογισμικού)

Στους κανόνες περιορισμού λογισμικού μπορούμε να ορίσουμε τα **επίπεδα ασφάλειας**, να θέσουμε **πρόσθετους κανόνες**, να καθορίσουμε τους **επιτρεπόμενους τύπους αρχείων** που θα μπορούν να εκτελούνται καθώς και τους **εκδότες που θεωρούνται αξιόπιστοι**.



Application control policies (πολιτικές ελέγχου εφαρμογών)

Στις πολιτικές ελέγχου εφαρμογών μπορούμε να ενεργοποιήσουμε το AppLocker.
Με το AppLocker μπορούμε να ελέγξουμε ποιές εφαρμογές μπορεί να επιτρέπεται στους χρήστες να εκτελέσουν, ποιοί χρήστες θα έχουν το δικαίωμα να εγκαθιστούν νέες εφαρμογές, ποιές εκδόσεις εφαρμογών θα επιτρέπονται.



Advanced Audit policy(ρύθμιση παραμέτρων εξελιγμένης πολιτικής ελέγχου)

Η καταγραφή των ενεργειών που γίνονται στο σύστημα σε συνδυασμό με την συμπεριφορά των χρηστών είναι ένας σημαντικός τομέας στην ασφάλεια των συστημάτων.

Η συγκεκριμένη πολιτκή δίνει την δυνατότητα να ελέγξουμε τις πολιτικές ελέγχου, να αναγνωρίσουμε επιχειρούμενες ή επιτυχημένες επιθέσεις στο δίκτυο και στους πόρους καθώς και να ελέγξουμε την διαχείριση των πόρων του συστήματος