EPSILONNET
GROUP OF COMPANIES

ΜΙΣΘΟΔΟΣΙΑ HRM ΩΡΟΜΕΤΡΗΣΗ ESS

Νέο Σύστημα Ασφάλειας
Advanced Security Settings

Νέο Σύστημα Ασφάλειας
Advanced Security Settings

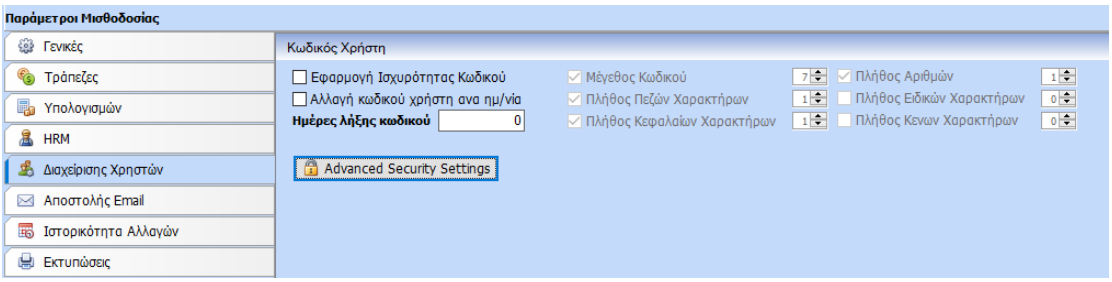
Το νέο σύστημα ασφάλειας αποτελεί μια νέα ολοκληρωμένη λύση επιβολής extra ασφάλειας και διασφάλισης συμμόρφωσης. Από την παροχή χρηστών, τη διαχείριση κωδικών πρόσβασης από τον χρήστη και την παρακολούθηση αλλαγών της υπηρεσίας καταλόγου Active Directory έως τη δυνατότητα καθολικής κρυπτογράφησης τόσο του Data Access, όσο και του Password του SQL Server, των χρηστών της εφαρμογής αλλά ακόμα και του UpdClient.

Συγκεκριμένα το νέο σύστημα παρέχει:

- MFA (Multi Factor Authentication)
- Active Directory
- Data Access με TLS Encryption
- Encryption το Password του SQL Server
- Hash + Salt encryption και PBKDF2 Encryption των Passwords των χρηστών της εφαρμογής
- Hash + Salt encryption και PBKDF2 Encryption του UpdClient

Μέσω ενός απλού και εύχρηστου περιβάλλοντος εργασίας ο Διαχειριστής (Administrator) μπορεί να ορίσει όλα εκείνα τα χαρακτηριστικά που θα του δώσουν την ολοκληρωμένη ασφαλή λειτουργία της εφαρμογής.

Πιο αναλυτικά μέσω των Παραμέτρων Προγράμματος και συγκεκριμένα την καρτέλα Διαχείρισης Χρηστών/ button Advanced Security Settings



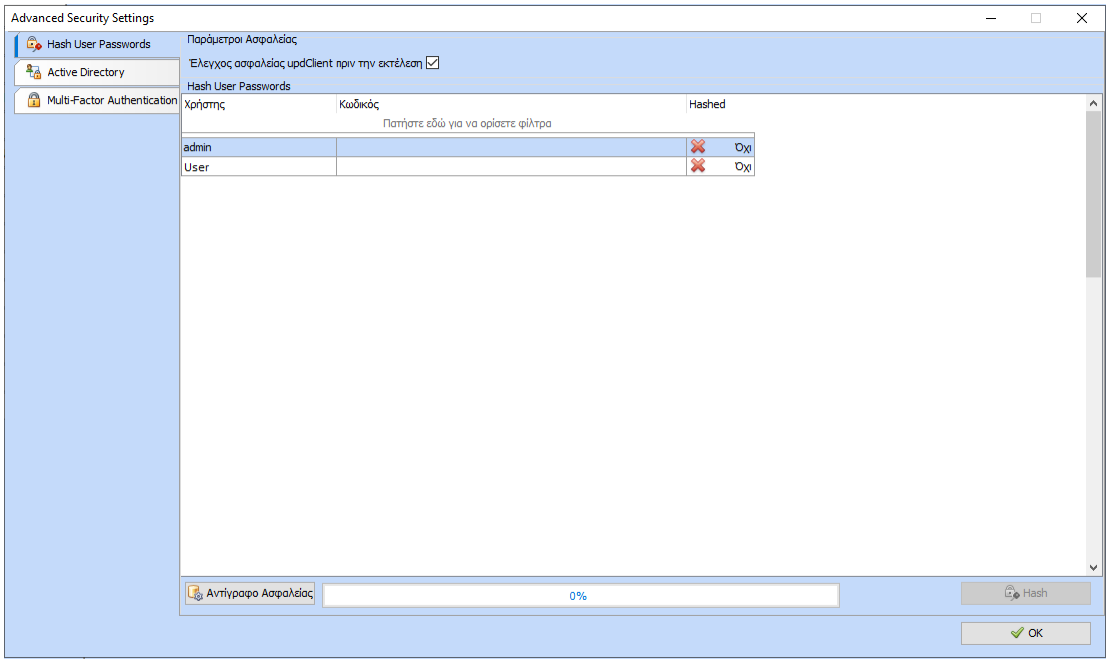
Ο Διαχειριστής μπορεί να κάνει την απαιτούμενη παραμετροποίηση προκειμένου να ολοκληρώσει την ασφαλή λειτουργία της εφαρμογής.

Καρτέλα Hash User Passwords

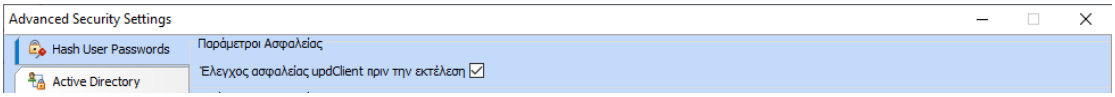
Στην συγκεκριμένη καρτέλα ο Διαχειριστής έχει την δυνατότητα να κρυπτογραφήσει με Hash + Salt encryption και PBKDF2 Encryption το Password των χρηστών της εφαρμογής της μισθοδοσίας.

Στην καρτέλα εμφανίζονται όλοι οι χρήστες της εφαρμογής με τον ήδη κρυπτογραφημένο κωδικό και με την ένδειξη αν έχει εφαρμοστεί ή όχι η νέα κρυπτογράφηση.

Πριν την εφαρμογή της νέας κρυπτογράφησης προτείνεται η δημιουργία αντιγράφου.



Στην ίδια καρτέλα ο Διαχειριστής μπορεί να ορίσει εφόσον το επιθυμεί την κρυπτογράφηση του UpdClient με Hash + Salt encryption και PBKDF2 Encryption για την αποτροπή μεσολάβησης κακόβουλου αρχείου κατά την αναβάθμιση της εφαρμογής.



Καρτέλα Active Directory

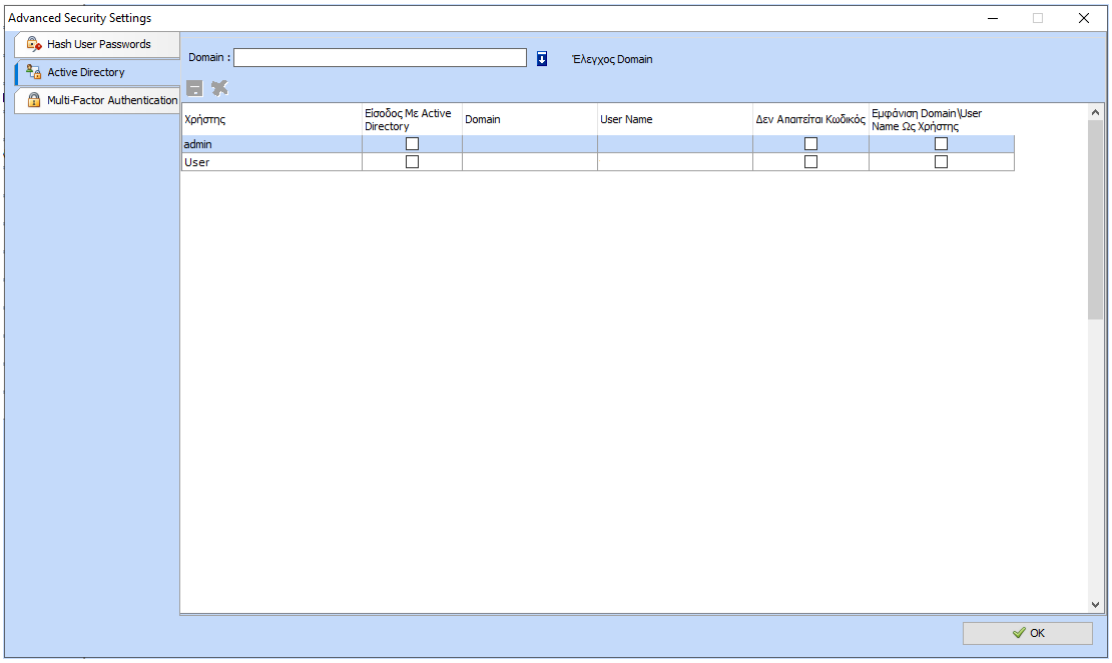
Στην συγκεκριμένη καρτέλα ο Διαχειριστής έχει την δυνατότητα διασύνδεσης των χρηστών της εφαρμογής μισθοδοσίας με τους χρήστες που ενσωματώνονται στο λειτουργικό σύστημα. Με το Active Directory καθίσταται εφικτή η μοναδική εγγραφή σε πόρους του δικτύου και στην πρόσβαση στην εφαρμογή μισθοδοσίας (Single Sign On) και βελτιώνεται η ιδιωτικότητα και ασφάλεια.

Στην καρτέλα εμφανίζονται όλοι οι χρήστες της εφαρμογής και μέσω του πεδίου «Είσοδος Με Active Directory» ο Διαχειριστής μπορεί να ορίσει τους χρήστες που επιθυμεί την παραπάνω σύνδεση. Στο πεδίο Domain πρέπει να εγγραφεί το «Domain» στο οποίο ανήκει ο χρήστης και στο πεδίο User Name το «User Name» με το οποίο συνδέεται στο λειτουργικό σύστημα.

Επιπλέον ενσωματώθηκαν οι παράμετροι «Δεν απαιτείται Κωδικός» και «Εμφάνιση Domain\ User Name Ως Χρήστης».

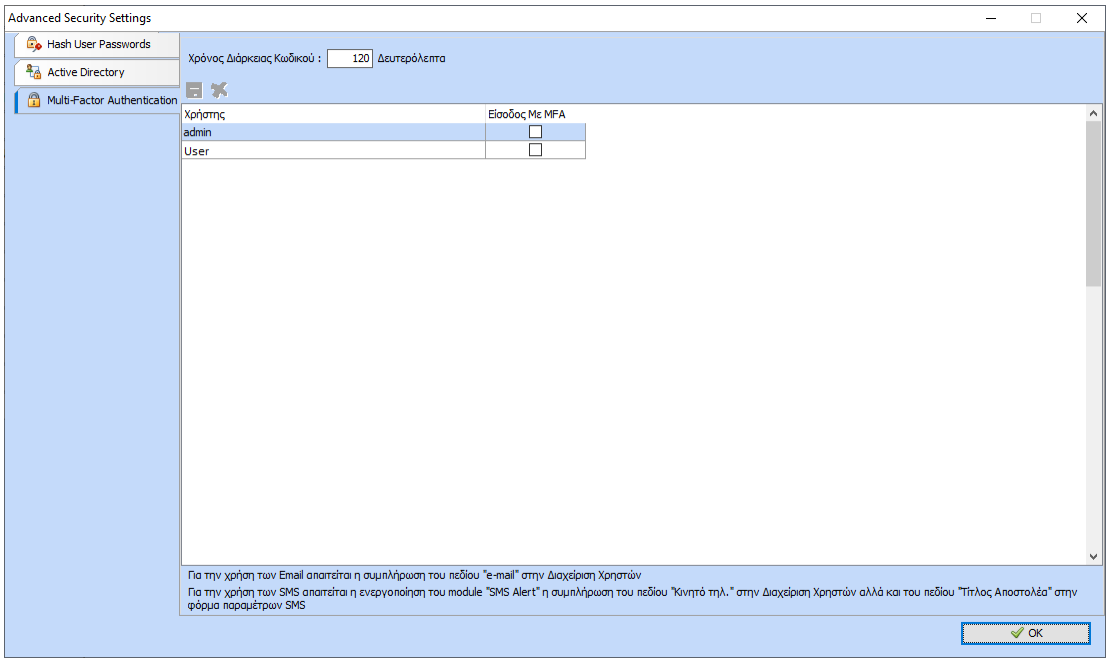
Με την 1η παράμετρο το πεδίο «Κωδικός» της εφαρμογής γίνεται ανενεργό επιτρέποντας την είσοδο χωρίς να απαιτείται η πληκτρολόγηση του Κωδικού.

Ενώ με την 2η παράμετρο, η λίστα των χρηστών που εμφανίζεται στην φόρμα εισόδου της εφαρμογής προσαρμόζεται έτσι ώστε να εμφανίζεται το όνομα του χρήστη με την μορφή Domain\UserName του λειτουργικού συστήματος.



Καρτέλα Multi Factor Authentication

Στην συγκεκριμένη καρτέλα ο Διαχειριστής έχει την δυνατότητα να ορίσει ανά χρήστη μια επιπλέον μέθοδο ηλεκτρονικής επαλήθευσης ταυτότητας του προκειμένου να συνδεθεί στην εφαρμογή.



Ο μηχανισμός ελέγχου της ταυτότητας περιλαμβάνει την αποστολή 6ψήφιου κωδικού με δύο τρόπους:

- με SMS
- με Email

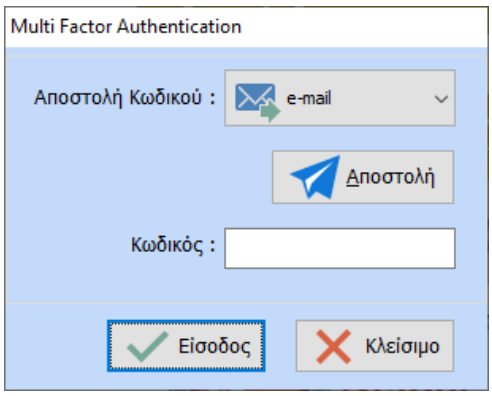
Για τον 1ο τρόπο αποστολής, με SMS, προϋποθέτει να είναι ενεργοποιημένο το module «SMS Alert». (Στην περίπτωση που δεν είναι μπορείτε να απευθυνθείτε στο τμήμα πωλήσεων).

Στην περίπτωση που είναι ενεργοποιημένο και επιθυμείτε την αποστολή του κωδικού με SMS τότε πρέπει να εισάγετε το κινητό τηλέφωνο στην καρτέλα του χρήστη στην φόρμα της Διαχείρισης Χρηστών.

Επιπλέον, πρέπει να συμπληρωθεί το πεδίο «Τίτλος Αποστολέα» στην φόρμα των Παραμέτρων SMS (από menu\Internet\SMS\Παράμετροι\Παράμετροι SMS).

Για τον 2ο τρόπο αποστολής πρέπει να συμπληρωθεί το πεδίο «e-mail» στην καρτέλα του χρήστη στην φόρμα της Διαχείρισης Χρηστών.

Εφόσον ολοκληρωθεί η παραπάνω παραμετροποίηση τότε μπαίνοντας στην εφαρμογή με τον συγκεκριμένο χρήστη εμφανίζεται η κάτωθι φόρμα εισόδου.

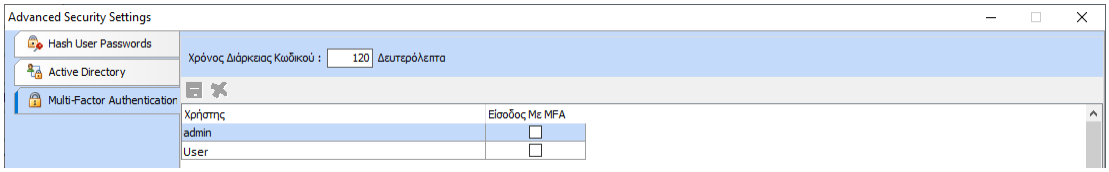


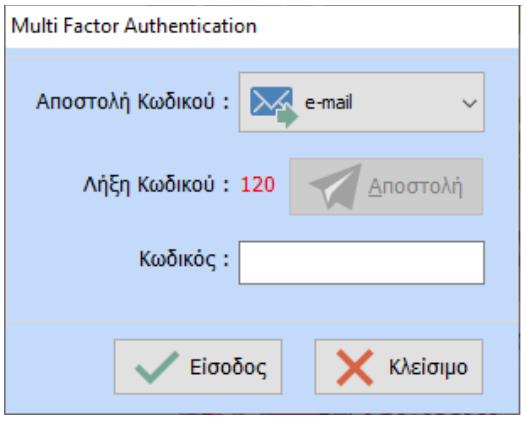
Στο πεδίο «Αποστολή Κωδικού» ο χρήστης μπορεί να επιλέξει είτε την αποστολή με 

είτε με 

.

Πατώντας το κουμπί Αποστολή ενεργοποιείται ένας counter ο οποίος αρχίζει να μετράει αντίστροφα και αφορά τον χρόνος ισχύς του κωδικού. Ο χρόνος αυτός ορίζεται μέσα στην καρτέλα Multi Factor Authentication



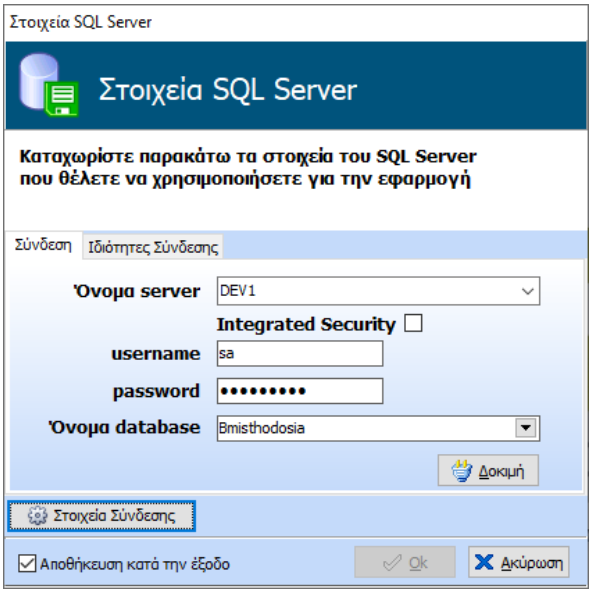


Με την αποστολή είτε Email είτε SMS καταφθάνει το μήνυμα το οποίο ενημερώνει τον χρήστη με τον κωδικό εισόδου και τον χρόνο ισχύος της διάρκειας του.

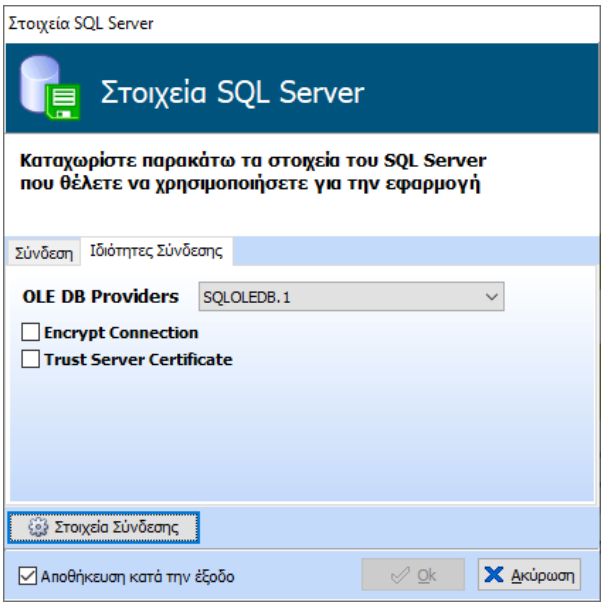
Αφού τον εισάγει στο πεδίο «Κωδικός» με το ΟΚ γίνεται η είσοδος στην εφαρμογή.

Φόρμα Σύνδεσης στην Βάση Δεδομένων

Στην συγκεκριμένη φόρμα ενσωματώθηκε το κουμπί «Στοιχεία Σύνδεσης».



Με το συγκεκριμένο κουμπί ανοίγει η καρτέλα «Ιδιότητες Σύνδεσης»

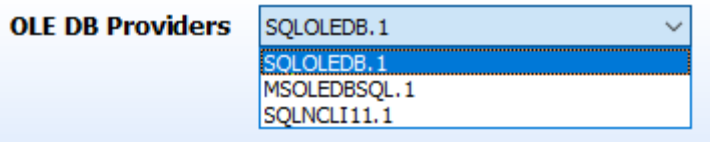


στην οποία ενσωματώθηκαν οι εξής ιδιότητες:

- OLE DB Providers
- Encrypt Connection
- Trust Server Certificate

Με την 1η ιδιότητα (**OLE DB Providers**) ο Διαχειριστής έχει την δυνατότητα να επιλέξει έναν από τους 3 OLE DB Providers που παρέχονται για SQL SERVER.

Προτεινόμενος OLE DB Driver είναι ο **MSOLEDBSQL** γιατί είναι ο πιο ασφαλής , ταχύτερος και ο μόνος που επιτρέπει την σύνδεση με «TLS SQL Server» ενώ οι υπόλοιποι drivers δεν το επιτρέπουν. Σχετικό κείμενο της Microsoft OLE DB Driver SQL Server



Με την 2η ιδιότητα (**Encrypt Connection**) ο Διαχειριστής έχει την δυνατότητα να επιλέξει αν τα δεδομένα μεταξύ Client – Server θα αποστέλλονται encrypted με TLS (Transport Layer Security).

Βασική προϋπόθεση είναι η ενεργοποίηση του TLS και στον SQL Server.

Έτσι όλα τα δεδομένα είναι encrypted διασφαλίζοντας τα από επιθέσεις man in the middle attack. Σχετικό κείμενο της Microsoft TLS SQL Server.

Με την 3η ιδιότητα (**Trust Server Certificate**) ο Διαχειριστής έχει την δυνατότητα να επιλέξει αν σε κάθε connection κατά την διαδικασία του handshake προκειμένου να διασφαλίσει encrypted connection κάνει validation του Certificate ή όχι.