Ολοκλήρωση υπηρεσιών καταλόγου ενοποιημένης πρόσβασης (LDAP Server και μηχανισμός shibboleth) για πιστοποίηση των μελών της Ακαδημαϊκής και Ερευνητικής κοινότητας" και πρόσβασή τους σε διιδρυματικές εφαρμογές

Παραδοτέο: Σχεδιασμός συστήματος διαχείρισης κωδικών πρόσβασης

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

1. ΕΙΣΑΓΩΓΗ

1.1 ΑΝΤΙΚΕΙΜΕΝΟ ΚΑΙ ΔΟΜΗ ΤΟΥ ΠΑΡΑΔΟΤΕΟΥ

Το παρόν έργο παραδίδεται στο πλαίσιο της πράξης «Ολοκλήρωση υπηρεσιών καταλόγου ενοποιημένης πρόσβασης (LDAP Server και μηχανισμός shibboleth) για πιστοποίηση των μελών της Ακαδημαϊκής και Ερευνητικής κοινότητας και πρόσβασή τους σε διιδρυματικές εφαρμογές» και αφορά στην ανάπτυξη συστήματος διαχείρισης και ανάκτησης κωδικών και πολιτικών για χρήστες σε υπηρεσίες καταλόγου. Η υπηρεσία απευθύνεται στο σύνολο των εγγεγραμμένων χρηστών, στην υπηρεσία καταλόγου του ιδρύματος, τόσο στους καθηγητές , όσο και στο προσωπικό του ιδρύματος.

Κύριος στόχος της υπηρεσίας θεωρείται αφενός η αυτοματοποίηση της διαδικασίας ανάκτησης κωδικού για τους παραπάνω χρήστες, χρησιμοποιώντας εναλλακτικά κανάλια επικοινωνίας, αφετέρου η εύκολη δημιουργία και εφαρμογή πολιτικών για τους κωδικούς που επιλέγονται. Το σύστημα, μέσω της αυτοματοποίησης των παραπάνω διαδικασιών έχει σαν στόχο την αποφόρτιση των αιτημάτων προς το ανθρώπινο δυναμικό, αλλά και την επιτάχυνση της εξυπηρέτησης κάθε ανάγκης χρηστών, τέτοιας κατηγορίας.

Η παροχή της υπηρεσίας γίνεται αυτόματα σε όλους τους χρήστες που είναι εγγεγραμμένοι σε ένα ίδρυμα χωρίς την ανάγκη κάποιας ενεργοποίησης εκ μέρους τους αλλά απαιτεί την ύπαρξη δευτερευόντων στοιχείων επικοινωνίας. Αυτά τα στοιχεία εισάγονται μαζικά στο σύστημα καταλόγου ή σε δεύτερο χρόνο από τους ίδιους τους χρήστες.

Στο έγγραφο που ακολουθεί θα αναλυθούν αρχικά οι προδιαγραφές της υπηρεσίας και μετά την περιγραφή των επιλογών υλοποίησης παρουσιάζονται τα βασικά σενάρια χρήσης. Τέλος αναφέρονται αρχιτεκτονικά στοιχεία της εφαρμογής καθώς και οι δυνατότητες διαλειτουργικότητας με άλλα συστήματα της υποδομής των ιδρυμάτων.

1.2 ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

Η υπηρεσία βασίζεται στην ύπαρξη μιας υποδομής καταλόγου. Αντικειμενικός σκοπός είναι η συμβολή στην ολοκλήρωσή των παροχών προς τους χρήστες που είναι εγγεγραμμένοι στους ιδρυματικούς αυτούς καταλόγους. Η υπηρεσία καταλόγου, έχει το ρόλο του μέσου διαπίστευσης, αποτελεί όμως και τον αποδέκτη του συνόλου των ενεργειών που παρέχονται.

Δεδομένου πως δεν υπήρχε κάποια εφαρμογή που να ταιριάζει στις απαιτήσεις που τέθηκαν, έγινε υλοποίηση εκ του μηδενός. Η υλοποίησή βασίστηκε στις ακόλουθες παραμέτρους.

1.2.1 Προσδιορισμός απαιτήσεων περιφερειακών πληροφοριακών συστημάτων και εφαρμογών

Για την λειτουργία της εφαρμογής θεωρείται απαραίτητη η ύπαρξη ενός εξυπηρετητή LDAP σε λειτουργία με μια πλήρη παρουσία δεδομένων. Οποιοσδήποτε LDAPv3 εξυπηρετητής μπορεί να χρησιμοποιηθεί χωρίς πρόβλημα. Απαραίτητο για την σωστή λειτουργία είναι η ύπαρξη των κατάλληλων σχημάτων. Ως απαραίτητα σχήματα έχουν οριστεί τα *ppolicy, ExtendedAuth, SchAc, SchGrAc.* Τα παραπάνω σχήματα χρησιμοποιούνται τόσο από αυτή την εφαρμογή αλλά και από τις βοηθητικές του όλου οικοδομήματος. Η ουσιαστική χρησιμότητα τους είναι η ύπαρξη της δυνατότητας για ορισμό πολιτικής κωδικών και δευτερευόντων στοιχείων επικοινωνίας. Ως βοηθητικά μπορούν να θεωρηθούν αν είναι εγκατεστημένα και τα σχήματα eduPerson, eduOrg.

Για τη διαδικασία αποστολής SMS είναι απαραίτητη η ύπαρξη ενός SMS gateway. Ένα νέο κανάλι (10-ψήφιο long number) μπορεί να χρησιμοποιηθεί αποκλειστικά για τους σκοπούς του έργου μέσα από την υφιστάμενη πλατφόρμα SMS (ws.gunet.gr) ή διαφορετικά να αξιοποιηθεί οποιοσδήποτε SMS πάροχος εφόσον παρέχει τις κατάλληλες διεπαφές διασύνδεσης.

1.2.2 Επιλογή βασικών λειτουργιών

Η εφαρμογή έχει σαν στόχο δυο μεγάλες κατηγορίες λειτουργιών. Τις λειτουργίες που

προορίζονται προς τους **χρήστες** και τις λειτουργίες προς τους **διαχειριστές**.

Στην πρώτη περίπτωση, στους **χρήστες** δίνεται η δυνατότητα για τις παρακάτω διαδικασίες :

- Ανάκτηση κωδικού με χρήση email.
- Ανάκτηση κωδικού με χρήση sms.
- Εισαγωγή δευτερευόντων στοιχείων επικοινωνίας
- Αλλαγή κωδικού.

Στους **διαχειριστές** το πλήθος των λειτουργιών είναι πιο εκτεταμένο. Συγκεκριμένα οι λειτουργίες που ορίστηκαν σαν αναγκαίες είναι.

- Απεικόνιση λίστας χαρακτηριστικών χρηστών
- Αναφορά προβλημάτων
- Προβολή διαχειριστών
- Επιβολή πολιτικής σε χρήστες
- Αναζήτηση χρηστών και προχωρημένη αναζήτηση με βάση φίλτρα ldap
- Προβολή πολιτικών κωδικών και δημιουργία νέων
- Προβολή πληροφοριών χρήστη και αλλαγή κωδικού

1.2.3 Υλοποίηση διαχειριστικού περιβάλλοντος και περιβάλλοντος χρήστη

Μετά το πέρας του ορισμού των προδιαγραφών είναι δυνατή η υλοποίηση τόσο του διαχειριστικού τμήματος, όσο και του τμήματος της εφαρμογής που απευθύνεται στους τελικούς χρήστες. Πέρα από τις παραμέτρους υλοποίησης που ορίστηκαν ανωτέρω, ιδιαίτερη έμφαση δόθηκε στον τομέα της ασφάλειας και διαπίστευσης των χρηστών. Δεδομένης της σημασίας και κρισιμότητας των δεδομένων που βρίσκονται υπό διαχείριση, είναι υψίστης σημασίας τα άτομα με πρόσβαση στην υπηρεσία να έχουν διαπιστευτεί σωστά. Ακολούθως οι χρήστες που θεωρούνται τελικοί αποδέκτες πρέπει να διασφαλίζονται, όσον αφορά την προστασία από κακόβουλες επιθέσεις και προσπάθειες υποκλοπής κωδικών. Γι αυτό το λόγο η κυριότερη από τις επιλογές είναι η διαδικασία αναγνώρισης χρήστη και η απόδοση δικαιώματος χρήσης της λειτουργίας αρχικοποίησης κωδικού.

1.2.4 Υλοποίηση διαδικασίας εγκατάστασης εφαρμογής

Κατά τον σχεδιασμό της υπηρεσίας, κρίθηκε σκόπιμη και η υλοποίηση της διαδικασίας εγκατάστασης σαν τμήμα του διαχειριστικού της εφαρμογής. Δεδομένου πως η εφαρμογή έχει σαν αποδέκτες ένα μεγάλο σύνολο ιδρυμάτων, θεωρείται απαραίτητη η λεπτομερής καταγραφή των απαιτήσεων εγκατάστασης και η μορφοποίησή με τον κατάλληλο τρόπο ώστε η εγκατάσταση να απαιτεί την συνδρομή ενός μόνο διαχειριστή ιδρύματος. Αυτή η διαδικασία εγκατάστασης ακολούθως ενσωματώθηκε και στην λειτουργία διαχείρισης της εφαρμογής, με τέτοιο τρόπο ώστε κάθε παράμετρος να είναι προσβάσιμη μέσω του διαχειριστικού περιβάλλοντος.

Αναλυτική παρουσίαση της διαδικασίας εγκατάστασης παρέχεται στα σενάρια χρήσης της εφαρμογής.

2. ΥΛΟΠΟΙΗΣΗ ΥΠΗΡΕΣΙΑΣ – ΑΝΤΙΚΕΙΜΕΝΟ

Ο ορισμός των δικαιούχων της υπηρεσίας προηγείται της υλοποίησης, καθώς με βάση αυτόν ορίζονται τα επίπεδα πρόσβασης χρηστών. Μετά τον ορισμό των επιπέδων αυτών αναλύονται οι υπηρεσίες που διατίθενται.

2.1 ΔΙΚΑΙΟΥΧΟΙ ΥΠΗΡΕΣΙΑΣ

Η επιλογή των χρηστών που θα έχουν πρόσβαση στην υπηρεσία γίνεται καταρχάς σε λογικό επίπεδο, βάσει των αναγκών των ιδρυμάτων. Είναι αυτονόητο πως η λειτουργία ανάκτησης πρόσβασης είναι απαραίτητη για το σύνολο των χρηστών των ιδρυμάτων. Οι χρήστες αυτοί δεν διαχωρίζονται σε υποκατηγορίες, καθώς οι λειτουργίες της εφαρμογής δεν απαιτούν κάποια άλλη πληροφορία για τα άτομα που μετέχουν. Αυτό ισχύει όσον αφορά το τμήμα της εφαρμογής που απευθύνεται στο σύνολο των μη προνομιούχων χρηστών.

Το διαχειριστικό τμήμα προφανώς είναι μη προσβάσιμο από οποιονδήποτε πέρα από την κλειστή ομάδα των διαχειριστών.

Αυτή η ομάδα ορίζεται αυστηρά σε κάθε ίδρυμα και έχει δυο υποκατηγορίες:

- Τους **διαχειριστές** που έχουν πλήρη πρόσβαση στο σύστημα και έχουν δικαίωμα αλλαγής και της πολιτικής κωδικών
- τους **υποδιαχειριστές** που έχουν δυνατότητα μόνο για αλλαγές κωδικών.

Και οι δυο κατηγορίες διαχειριστών διατηρούν τα ίδια δικαιώματα στο υπόλοιπο σύνολο της εφαρμογής. Αυτό συνεπάγεται πως μπορούν να επεξεργαστούν κάθε μια από τις ιδιότητες της εγκατάστασης.

Η διάκριση των χρηστών στις τρεις κατηγορίες που αναφέρθηκαν (χρήστες, υποδιαχειριστές και διαχειριστές) γίνεται μέσω της ύπαρξης ενός χαρακτηριστικού από την υπηρεσία καταλόγου. Αυτό το χαρακτηριστικό ορίστηκε σαν το eduPersonEntitlement και οι δύο δυνατές τιμές του είναι dbadmin και

admin_password. Στην πρώτη περίπτωση το σύστημα αναγνωρίζει τον υπερδιαχειριστή, ενώ στην δεύτερη τον διαχειριστή που δύναται να αλλάξει κωδικούς αλλά όχι πολιτικές. Η απουσία αυτής της ιδιότητας αυτομάτως συνεπάγεται πως ο χρήστης είναι μη διαχειριστής και έχει δικαίωμα μόνο για χρήση της λειτουργίας ανάκτησης κωδικού.

2.2 ΥΠΗΡΕΣΙΕΣ

Οι παρεχόμενες υπηρεσίες που σχεδιάστηκαν για την εφαρμογή είναι οι εξής:

2.2.1 Ανάκτηση κωδικού

Η λειτουργία ανάκτησης κωδικού αποτελεί την βασικότερη παροχή στους χρήστες της υπηρεσίας. Οι χρήστες έχοντας ήδη εγγραφεί στην υπηρεσία καταλόγου, παρακινούνται να συμπληρώσουν δευτερεύοντα στοιχεία επικοινωνίας. Τα απαραίτητα στοιχεία στην παρούσα φάση είναι είτε μια δευτερεύουσα διεύθυνση email, είτε αριθμός κινητού τηλεφώνου. Και στις δυο περιπτώσεις τα στοιχεία αυτά χρησιμοποιούνται ώστε να αποσταλεί στον χρήστη μια μοναδική διεύθυνση εισόδου στην υπηρεσία, όπου εκεί δίνεται η δυνατότητα δημιουργίας νέου κωδικού. Σημειώνεται πως και στις δυο περιπτώσεις η αίτηση ξεκινά από τον χρήστη, μέσω της κατάλληλης φόρμας, και το δευτερεύον μέσο επικοινωνίας χρησιμοποιείται για την διασφάλιση της ταυτότητας του χρήστη. Δεν υπάρχει καμιά ουσιαστική διαφοροποίηση στη χρήση email, είτε sms, και ουσιαστικά η επιλογή του επαφίεται στην ευχέρεια του χρήστη της υπηρεσίας.

Σημειώνεται πως ανάλογα με τις επιλογές του διαχειριστή, δίνεται η δυνατότητα ενεργοποίησης ελέγχου captcha για τις αιτήσεις των χρηστών, ενώ η προσθήκη του ελέγχου για επιπλέον στοιχεία του χρήστη είναι μέσα στις υλοποιημένες δυνατότητες της εφαρμογής.

2.2.2 Εισαγωγή δευτερευόντων στοιχείων επικοινωνίας

Για την χρήση της λειτουργίας ανάκτησης/δημιουργίας κωδικού αναφέρθηκε πως είναι απαραίτητη η ύπαρξη στοιχείων επικοινωνίας για τα άτομα. Αυτά τα στοιχεία κατά ένα ποσοστό εισάγονται κατά την εγγραφή του χρήστη στις υπηρεσίες καταλόγου, και εφόσον υπάρχει η έγκριση του ιδίου. Σε περιπτώσεις που τα στοιχεία αυτά δεν είναι

διαθέσιμα, είτε έχουν μεταβληθεί, οι χρήστες οφείλουν να τα ενημερώσουν. Αυτό γίνεται με την είσοδο στην υπηρεσία και την επιλογή "καταχώρηση στοιχείων". Εκεί γίνεται η εισαγωγή των απαραίτητων στοιχείων που θα χρησιμοποιηθούν σε άλλες λειτουργίες.

2.2.3 Αλλαγή κωδικού.

Στην αλλαγή κωδικού, δίνεται στον χρήστη η δυνατότητα να αλλάξει τον κωδικό που έχει εισαχθεί από αυτόν στο σύστημα. Οι ουσιαστικές διαφοροποιήσεις περιλαμβάνουν τους ελέγχους σχετικά με τις πολιτικές κωδικών, αλλά και με τον τρόπο που μπορεί το σύστημα να ζητήσει την αλλαγή του κωδικού του χρήστη, όταν δεν πληροί πλέον κάποιες από τις προϋποθέσεις των πολιτικών. Κατά τα άλλα ακολουθείται η πάγια τακτική αλλαγής κωδικών.

2.2.4 Απεικόνιση λίστας χαρακτηριστικών χρηστών.

Ο χρήστης με δικαιώματα διαχειριστή έχει την δυνατότητα της εποπτικής απεικόνισης των χαρακτηριστικών του συνόλου των δεδομένων της υπηρεσίας καταλόγου. Ουσιαστικά αυτό αποτελεί μια εικόνα της κατάστασης του συστήματος, στην οποία αναλύονται τα κυριότερα στοιχεία που έχουν σημασία για τους διαχειριστές. Αυτά αποτελούνται από μια συνολική εικόνα των χρηστών και μια εικόνα σχετικά με τα δευτερεύοντα στοιχεία επικοινωνίας τους. Επιπλέον δίνονται πληροφορίες σχετικά με το πλήθος και τις κατηγορίες των διαχειριστών. Σε όλες αυτές τις περιπτώσεις διατίθενται λεπτομέρειες, σχετικά με τις επιπλέον πληροφορίες των χρηστών και τα χαρακτηριστικά τους που έχουν σημασία για την εύρυθμη λειτουργία του συστήματος.

2.2.5 Αναφορά προβλημάτων

Στην συνολική εικόνα της κατάστασης του συστήματος, δίνεται στους διαχειριστές και μια λίστα πιθανών προβλημάτων που μπορούν να ενσκήψουν στο σύστημα. Αυτά τα προβλήματα συνήθως αναφέρονται σε χρήστες που δεν έχουν τα κατάλληλα στοιχεία, τους κατάλληλους κωδικούς, είτε ακόμα τις απαραίτητες , από το σύστημα, κλάσεις. Σε αυτές τις περιπτώσεις δίνεται δυνατότητα επιδιόρθωσης αυτών των θεμάτων.

2.2.6 Δημιουργία και επιβολή πολιτικής σε χρήστες

Σε κάθε διαχειριστή δίνεται η δυνατότητα για τη δημιουργία πολλαπλών πολιτικών ασφαλείας για τους κωδικούς που χρησιμοποιούν οι χρήστες. Αυτές οι πολιτικές περιλαμβάνουν επιλογές σχετικά με τη διάρκεια και την πολυπλοκότητα των κωδικών, επιλογές σχετικά με τις αποτυχημένες προσπάθειες εισόδου στο σύστημα καθώς και για τα δικαιώματα των χρηστών πάνω στους κωδικούς τους.

2.2.7 Αναζήτηση χρηστών και προχωρημένη αναζήτηση με βάση φίλτρα LDAP

Κάθε διαχειριστής έχει την δυνατότητα για αναζήτηση χρηστών. Αυτή η αναζήτηση μπορεί να διεκπεραιωθεί πέρα από την απλή χρήση ονομάτων και με την χρήση ldap φίλτρων, δίνοντας έτσι μια απευθείας αντιστοίχιση της εφαρμογής με την υποδομή που βασίζεται. Το αποτέλεσμα της αναζήτησης μπορεί να χρησιμοποιηθεί άμεσα για μια σειρά ενεργειών.

2.2.8 Προβολή πληροφοριών χρήστη και αλλαγή κωδικού

Κάθε εμφάνιση ονομάτων χρηστών στο σύστημα, είτε αποτελεί αποτέλεσμα αναζήτησης, είτε αναφέρεται στην λίστα χρηστών, έχει τη βοηθητική λειτουργία της εμφάνισης πληροφοριών. Οι διαχειριστές πέρα από την προβολή πληροφοριών έχουν την δυνατότητα ενεργειών πάνω στον λογαριασμό του χρήστη, αλλά και να ορίσουν υποχρεωτικές ενέργειες από πλευράς του χρήστη στην επόμενη είσοδό του.

3. ΣΕΝΑΡΙΑ ΧΡΗΣΗΣ

Ακολούθως θα αναλυθούν οι πιο συνηθισμένες περιπτώσεις χρήσης της εφαρμογής. Και σε αυτή την περίπτωση θα γίνει ένας διαχωρισμός στις δύο βασικές κατηγορίες λειτουργιών των απλών χρηστών και των διαχειριστών.

3.1 ΔΙΑΔΙΚΑΣΙΑ ΕΓΚΑΤΑΣΤΑΣΗΣ

Η διαδικασία εγκατάστασης απευθύνεται κυρίως σε διαχειριστές των συστημάτων. Παρόλα αυτά κρίνεται πως είναι απαραίτητη η παρουσίαση της, καθώς δίνει πληροφορίες και σχετικά με την διαχείριση της εφαρμογής.

Η διαδικασία εγκατάστασης ξεκινά με την αποσυμπίεση του πακέτου εγκατάστασης σε έναν φάκελο του εξυπηρετητή που είναι προσβάσιμο από το δίκτυο. Προτείνεται η αποσυμπίεση στον ριζικό κατάλογο του εξυπηρετητή ιστού.

Χρησιμοποιώντας τη διεύθυνση του εξυπηρετητή πχ http://arcanum.teixal.gr η πρώτη σελίδα που εμφανίζεται είναι η γενική σελίδα που παρέχει τις βασικές οδηγίες προτού ξεκινήσει η διαδικασία.

Εικόνα 1 - Εκκίνηση διαδικασίας εγκατάστασης

Στην παραπάνω σελίδα δίνονται βασικές πληροφορίες σχετικά με τις ρυθμίσεις του εξυπηρετητή καταλόγου. Τα βασικά προαπαιτούμενα αφορούν τα απαραίτητα σχήματα που θα πρέπει να είναι εγκατεστημένα, ώστε να υποστηρίζονται όλες οι λειτουργίες της εφαρμογής.

Παράδειγμα OpenLDAP configuration (/etc/ldap/slapd.conf)

```
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/eduorg.schema
include /etc/ldap/schema/eduperson.schema
include /etc/ldap/schema/GUPerson.schema
include /etc/ldap/schema/GUExtendedAuthentication.schema
```

Έχετε θέσει τα κατάλληλα LDAP ACLs και settings του Policy Module.

Παράδειγμα OpenLDAP configuration (/etc/ldap/slapd.conf)

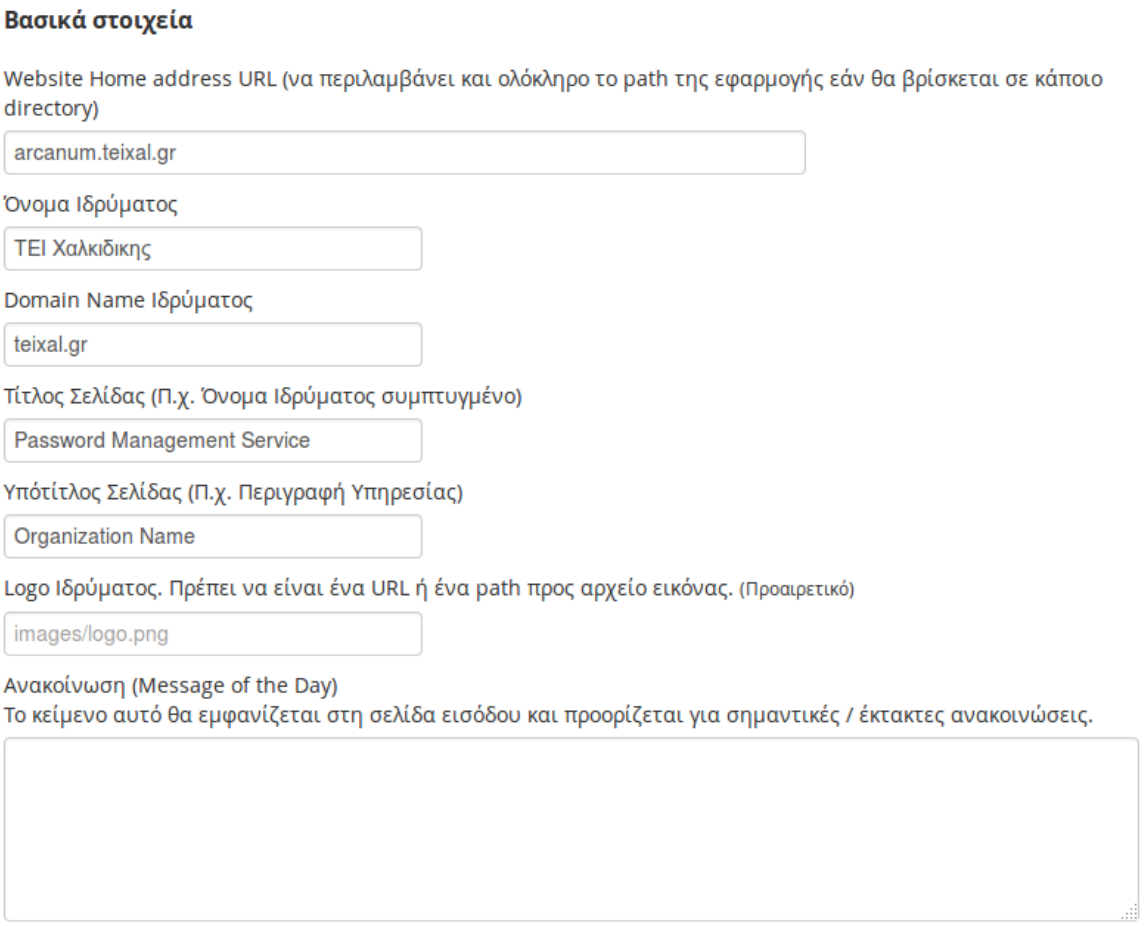
```
# Database Options

access to attrs=userPassword,shadowLastChange
        by dn="cn=manager,dc=org,dc=gr" write
        by anonymous auth
        by self write
        by * none

access to dn.base="" by * read

access to *
        by dn="cn=manager,dc=org,dc=gr" write
        by * none

overlay ppolicy
ppolicy_default "cn=students,ou=policies,dc=org,dc=gr"
ppolicy_use_lockout
ppolicy_hash_cleartext
```

Εικόνα 2 - Προαπαιτούμενα σχήματα καταλόγου

Εφόσον ο διαχειριστής θεωρεί πως ο κατάλογος πληροί όλες τις προδιαγραφές, μπορεί να συνεχίσει την εγκατάσταση. Σημειώνεται πως δεν υπάρχει σχετικός έλεγχος, καθώς τα δύο συστήματα είναι εντελώς διακριτά και δεν περαιτέρω αλληλεπίδραση μεταξύ τους πέρα από τη βασική λειτουργία της εφαρμογής (επερωτήσεις σχετικά με χρήστες).

Η εγκατάσταση που ακολουθεί χωρίζεται σε επτά βήματα, σε καθένα από τα οποία ζητούνται και διαφορετικές κατηγορίες ρυθμίσεων.

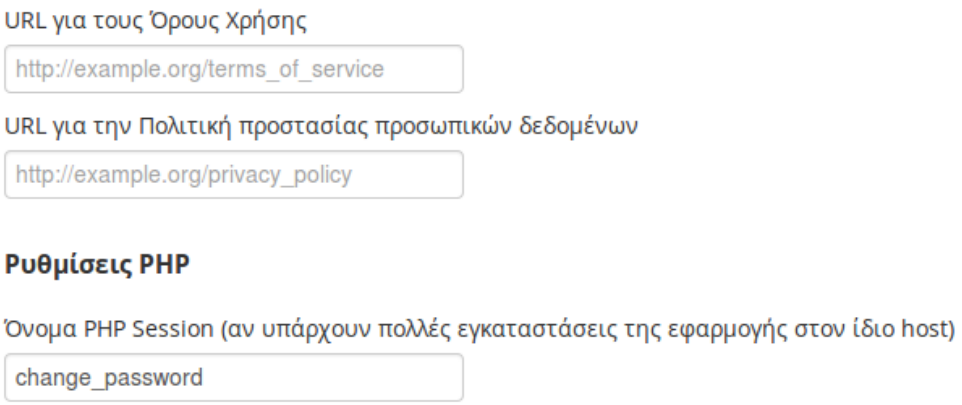
Τα βασικά στοιχεία της εφαρμογής που ζητούνται φαίνονται στην επόμενη εικόνα.



Εικόνα 3 - Βασικά στοιχεία

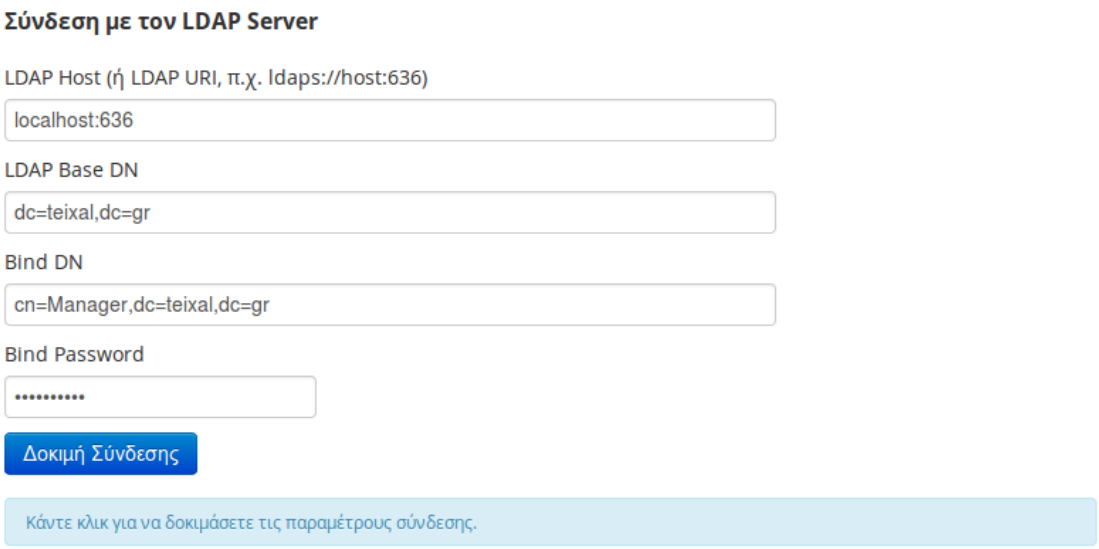
Αυτά αποτελούν κυρίως επικεφαλίδες και στοιχεία που καθορίζουν την βασική εμφάνιση της εφαρμογής.

Στην ίδια πρώτη κατηγορία εμφανίζονται και ρυθμίσεις που αφορούν πληροφορίες για τους όρους χρήσης της εφαρμογής. Τέλος ζητείται από τον διαχειριστή ένα μοναδικό όνομα για τη συνεδρία που δημιουργείται από τον εξυπηρετητή με την είσοδο κάθε χρήστη.

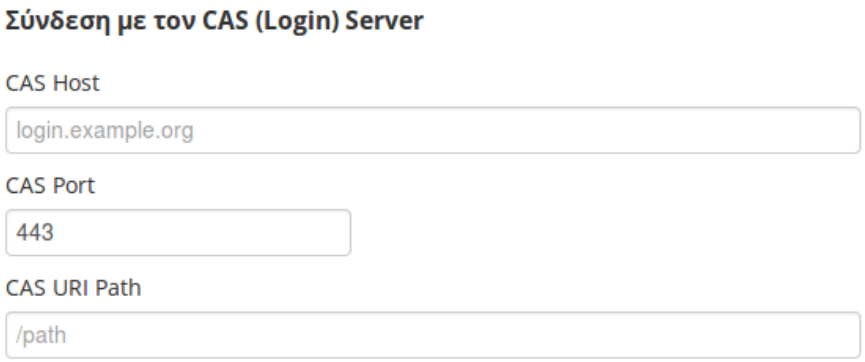


Εικόνα 4 - Όροι χρήσης και συνεδρία

Στο επόμενο στάδιο ζητούνται διαδοχικά πληροφορίες για τον εξυπηρετητή καταλόγου που χρησιμοποιείται και για τον εξυπηρετητή σύνδεσης και ταυτοποίησης.

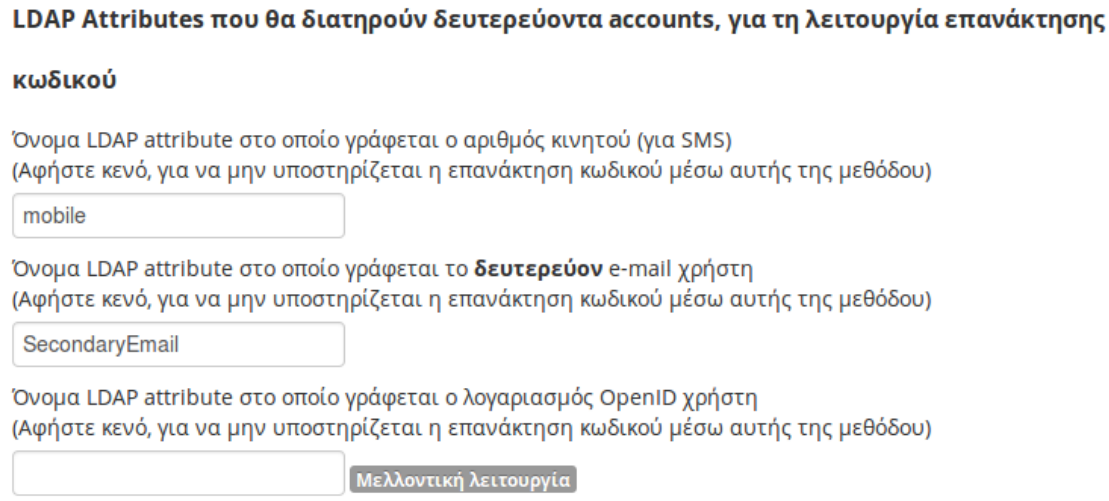


Εικόνα 5 - Ρυθμίσεις LDAP



Εικόνα 6 - Ρυθμίσεις login server

Δεδομένου πως μπορεί να υπάρχουν διαφοροποιήσεις στη σύνθεση των εξυπηρετητών καταλόγου ζητείται και μια σειρά από φίλτρα που οφείλει να γνωρίζει η εφαρμογή ώστε να γίνεται σωστά η ανάκτηση πληροφοριών χρηστών και διαχειριστών.

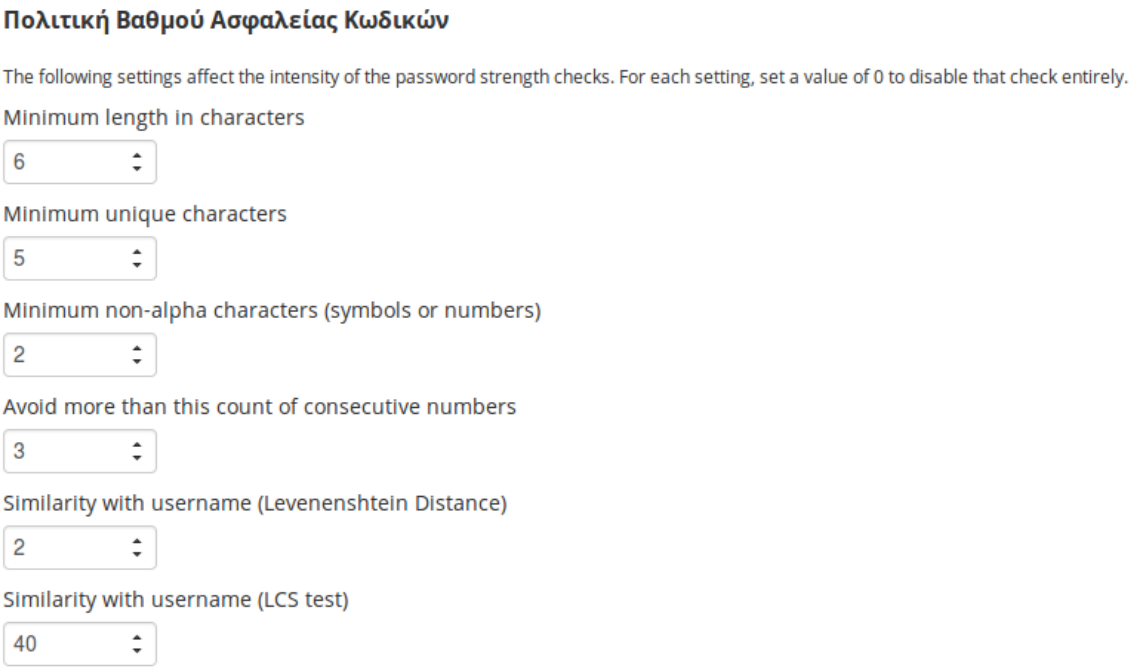


Εικόνα 7 - Απαραίτητα attributes χρηστών

Εικόνα 8 - Απαραίτητα φίλτρα ανάκτησης διαχειριστών

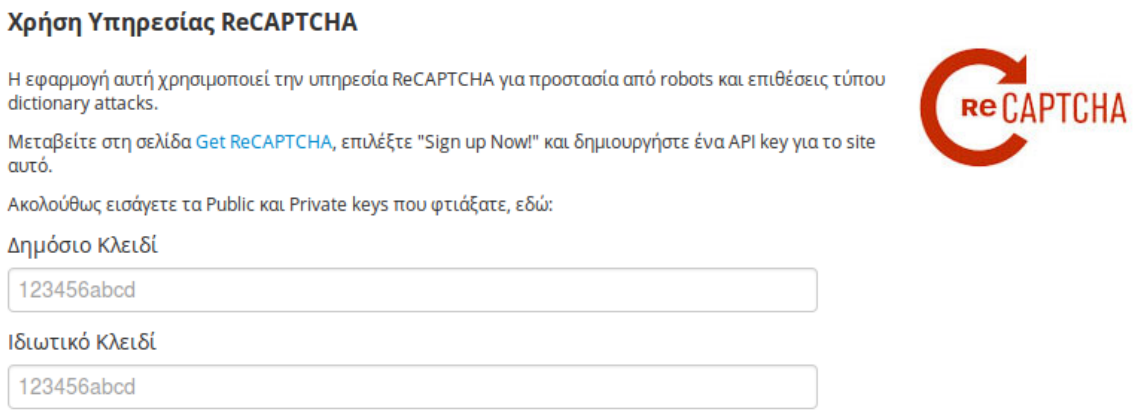
Και στις δυο παραπάνω περιπτώσεις δίνεται μια σειρά από παραδείγματα που διευκολύνουν και καθοδηγούν τον διαχειριστή.

Το επόμενο σκέλος των ερωτήσεων της διαδικασίας εγκατάστασης αφορά τους ελέγχους του βαθμού ασφαλείας των κωδικών που εισάγει ο χρήστης. Εδώ δίνεται η δυνατότητα ορισμού των παραμέτρων για κάθε ένα από τους ελέγχους που πραγματοποιούνται.



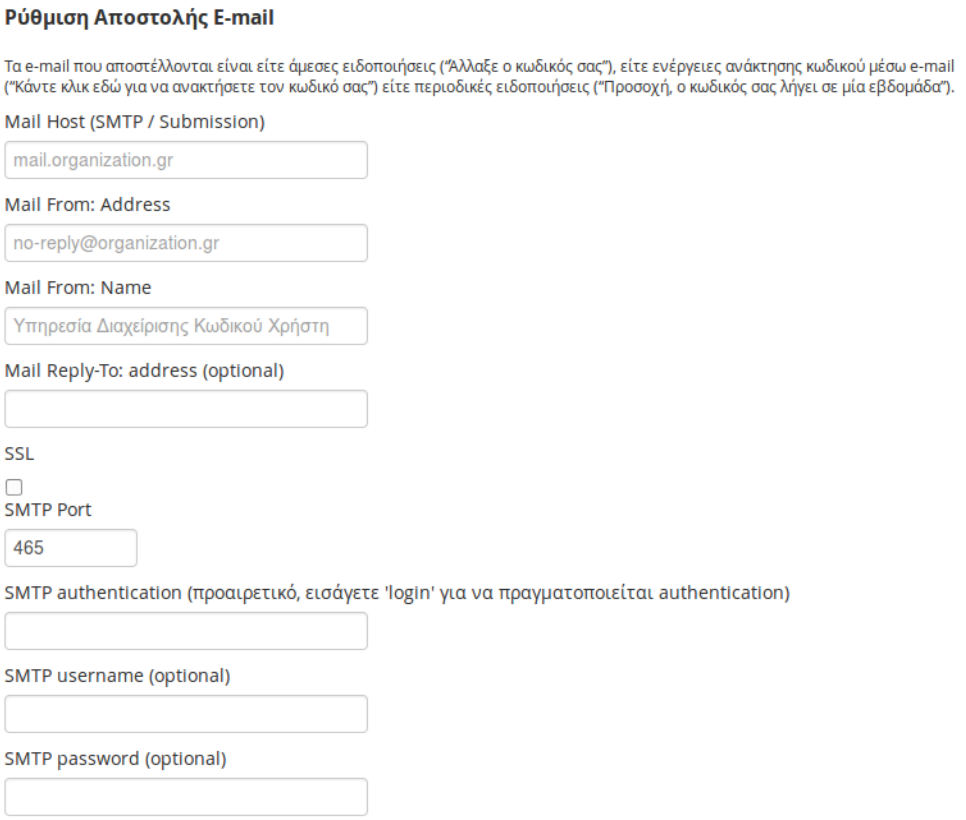
Εικόνα 9 - Πολιτική Βαθμού ασφαλείας κωδικών

Η προώθηση στην επόμενη σελίδα εμφανίζει στον διαχειριστή τη δυνατότητα ορισμού ενός κλειδιού για την υπηρεσία reCaptcha. Η υπηρεσία αυτή χρησιμοποιείται για την αποφυγή των επονομαζόμενων dictionary attacks. Σε περίπτωση που ο διαχειριστής το επιθυμεί, μπορεί απλά να παραβλέψει τη συγκεκριμένη επιλογή. Για τις ανάγκες των ιδρυμάτων, θεωρείται σκόπιμο να μην χρησιμοποιείται, για λόγους ευκολίας και απλότητας της συνολικής διαδικασίας που παρουσιάζεται στον χρήστη.



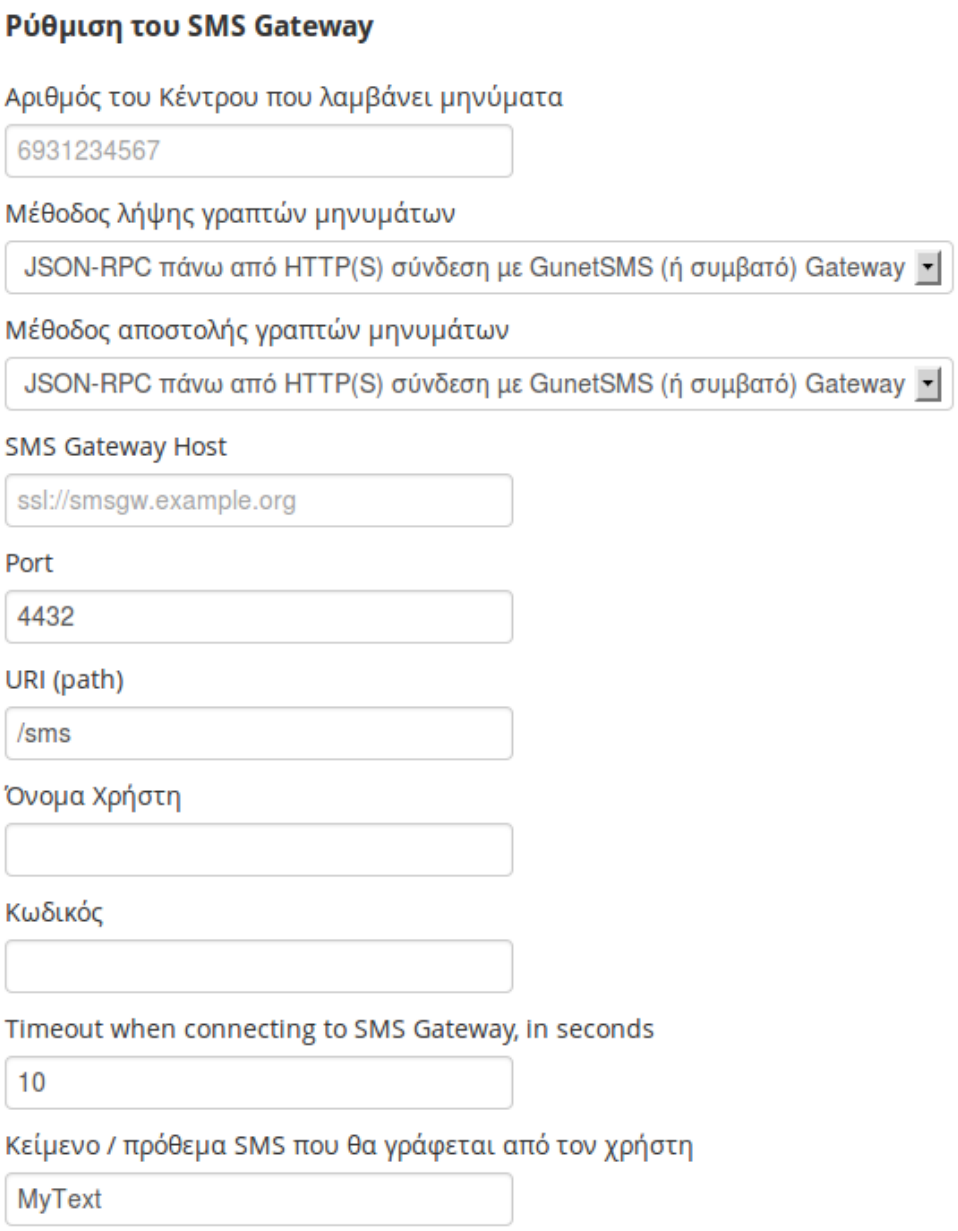
Εικόνα 10 - Υπηρεσία reCaptcha

Επόμενο στάδιο των ρυθμίσεων είναι οι ρυθμίσεις σχετικά με τον λογαριασμό email, που θα αποστέλλει μηνύματα στους χρήστες.



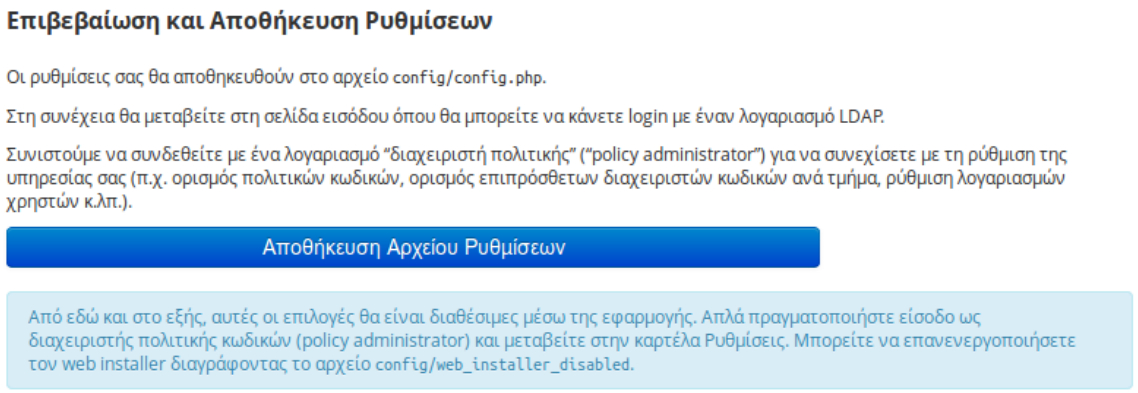
Εικόνα 11 - Ρυθμίσεις email

Τέλος ζητείται από τον υπεύθυνο εγκατάστασης μια σειρά πληροφοριών σχετικά με την υπηρεσία SMS Gateway που θα χρησιμοποιηθεί. Η υπηρεσία αυτή χρησιμοποιείται για την αποστολή και λήψη γραπτών μηνυμάτων σαν μέσο διαπίστευσης χρηστών στην αλλαγή κωδικού και κρίνεται απολύτως απαραίτητη.



Εικόνα 12 - Ρυθμίσεις SMS Gateway

Όταν αποθηκευθούν όλες οι παραπάνω πληροφορίες τότε δημιουργείται το αρχείο ρυθμίσεων και απενεργοποιείται η δυνατότητα επανεγκατάστασης.



Εικόνα 13 - Αποθήκευση ρυθμίσεων

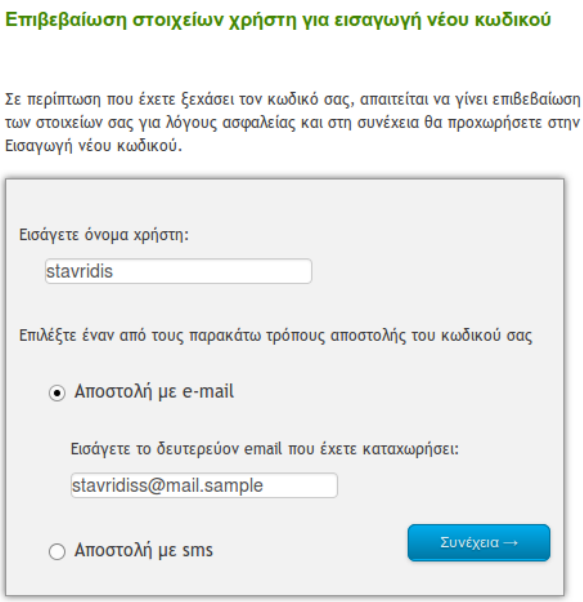
Ένα χαρακτηριστικό παράδειγμα αρχείου ρυθμίσεων παρατίθεται στο παράρτημα.

Μετά την ολοκλήρωση της εγκατάστασης, ο χρήστης προωθείται στη σελίδα εισόδου της εφαρμογής.

3.2 ΕΠΑΝΑΦΟΡΑ ΚΩΔΙΚΟΥ ΜΕ ΧΡΗΣΗ EMAIL/SMS

Η λειτουργία επαναφοράς κωδικού προηγείται οποιαδήποτε άλλης, διότι δεν απαιτεί είσοδο στην εφαρμογή. Η διαπίστευση του χρήστη επιτυγχάνεται μέσω της επιβεβαίωσης κάποιων πληροφοριών ταυτότητας και με την αξιοποίηση ενός άμεσα διαθέσιμου δευτερεύοντος καναλιού επικοινωνίας.

Ο χρήστης αρκεί να ακολουθήσει τον σύνδεσμο "*Έχω ξεχάσει τον κωδικό μου*" και θα βρεθεί στη σελίδα εισαγωγής στοιχείων. Σε αυτή τη σελίδα, χάριν ευκολίας, δεν ζητείται τίποτε άλλο πέρα από την διεύθυνση του χρήστη ή το κινητό του τηλέφωνο. Αυτή η πληροφορία επιβεβαιώνεται από την εφαρμογή, ότι αντιστοιχεί στην πραγματική πληροφορία του χρήστη και ακολούθως σε αυτό το μέσο αποστέλλεται ένας σύνδεσμος εισόδου στο σύστημα που έχει διάρκεια ζωής μίας ώρας.



Εικόνα 14 - Φόρμα επαναφοράς κωδικού

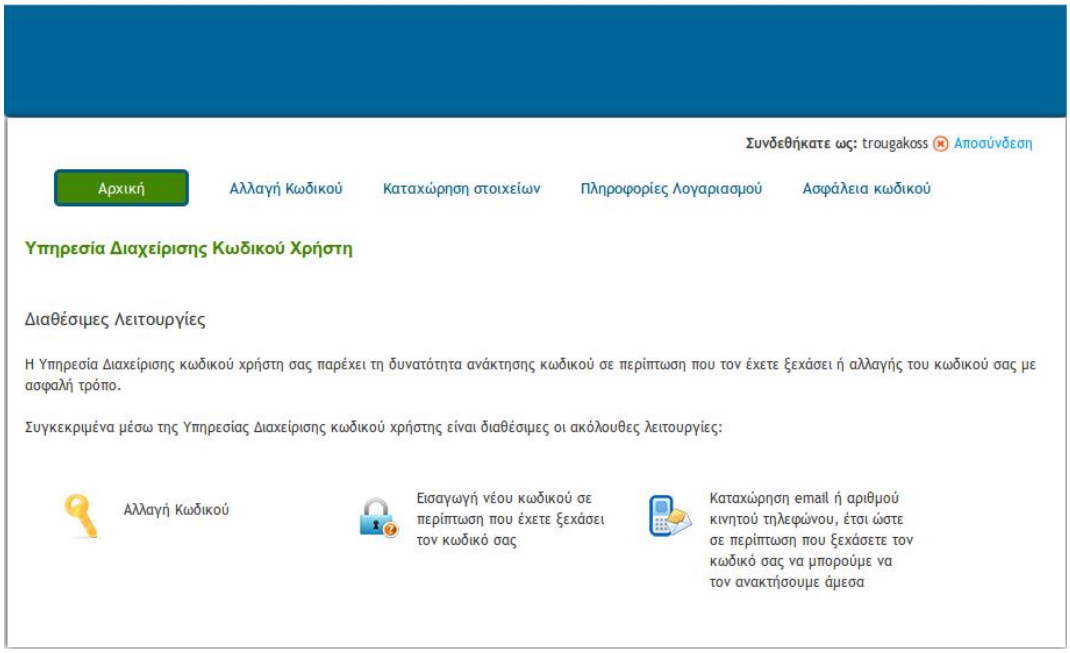
Όταν εισαχθεί ο χρήστης στην εφαρμογή, θα μπορεί να αλλάξει τον κωδικό του με την διαδικασία που αναλύεται στο επόμενο σενάριο χρήσης.

Σημειώνεται ότι απαραίτητη προϋπόθεση για τη χρήση της επαναφοράς κωδικού, είναι ο χρήστης να έχει συνδεθεί τουλάχιστον μια φορά κατά το παρελθόν σε αυτή και να έχει ορίσει τα δευτερεύοντα στοιχεία επικοινωνίας.

3.3 ΕΙΣΟΔΟΣ ΣΤΗΝ ΥΠΗΡΕΣΙΑ ΚΑΙ ΑΛΛΑΓΗ ΚΩΔΙΚΟΥ

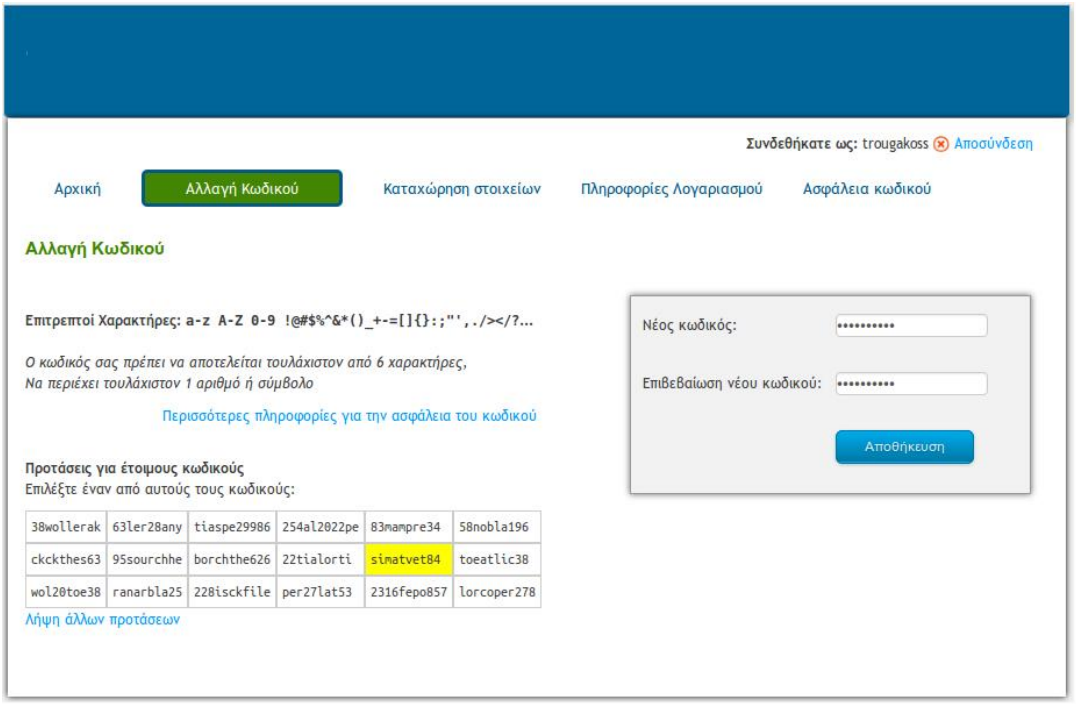
Η είσοδος στην υπηρεσία γίνεται ακολουθώντας την φόρμα εισόδου που εμφανίζεται στην πρώτη σελίδα, κατά την γνωστή διαδικασία.

Μετά την είσοδο του χρήστη, παρουσιάζεται η συνολική εικόνα της εφαρμογής, όσον αφορά το μη διαχειριστικό κομμάτι .



Εικόνα 15 - Συνολική εικόνα εφαρμογής

Σε αυτή την οθόνη ο χρήστης επιλέγει την αλλαγή κωδικού που είναι και η υπηρεσία που αναφέρεται και το αποτέλεσμα είναι η οθόνη αλλαγής κωδικού, στην οποία πέρα από την φόρμα παρέχονται και οι οδηγίες, καθώς και προτεινόμενοι κωδικοί.



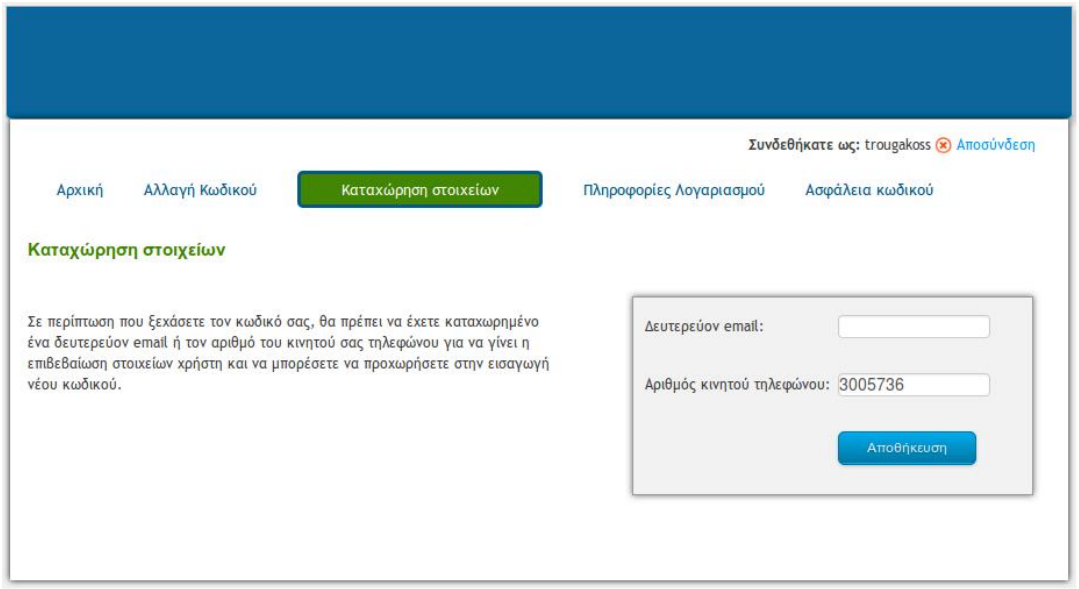
Εικόνα 16 - Αλλαγή κωδικού

Αρκεί η εισαγωγή νέου κωδικού και η αποθήκευση πραγματοποιείται, δεδομένου πως ο νέος κωδικός πληροί τις προδιαγραφές ασφάλειας της πολιτικής.

3.4 ΕΙΣΑΓΩΓΗ ΔΕΥΤΕΡΕΥΟΝΤΩΝ ΣΤΟΙΧΕΙΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ ΧΡΗΣΤΗ

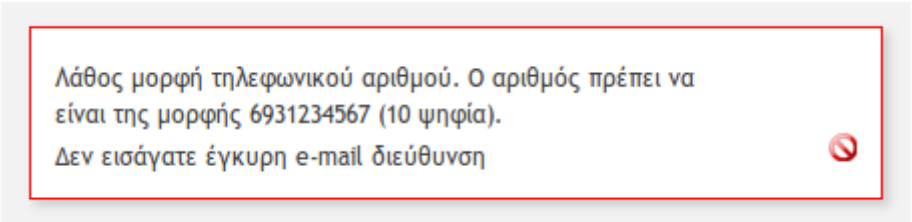
Η εισαγωγή δευτερευόντων στοιχείων επικοινωνίας του χρήστη είναι η διαδικασία της εφαρμογής που ουσιαστικά ενεργοποιεί τη χρησιμότητά της. Χωρίς αυτήν δεν μπορεί να πραγματοποιηθεί η ανάκτηση και αλλαγή κωδικού.

Η εισαγωγή στοιχείων γίνεται έχοντας εισαχθεί στην εφαρμογή και ακολουθώντας την επιλογή «Καταχώρηση στοιχείων».



Εικόνα 17 - Καταχώρηση στοιχείων

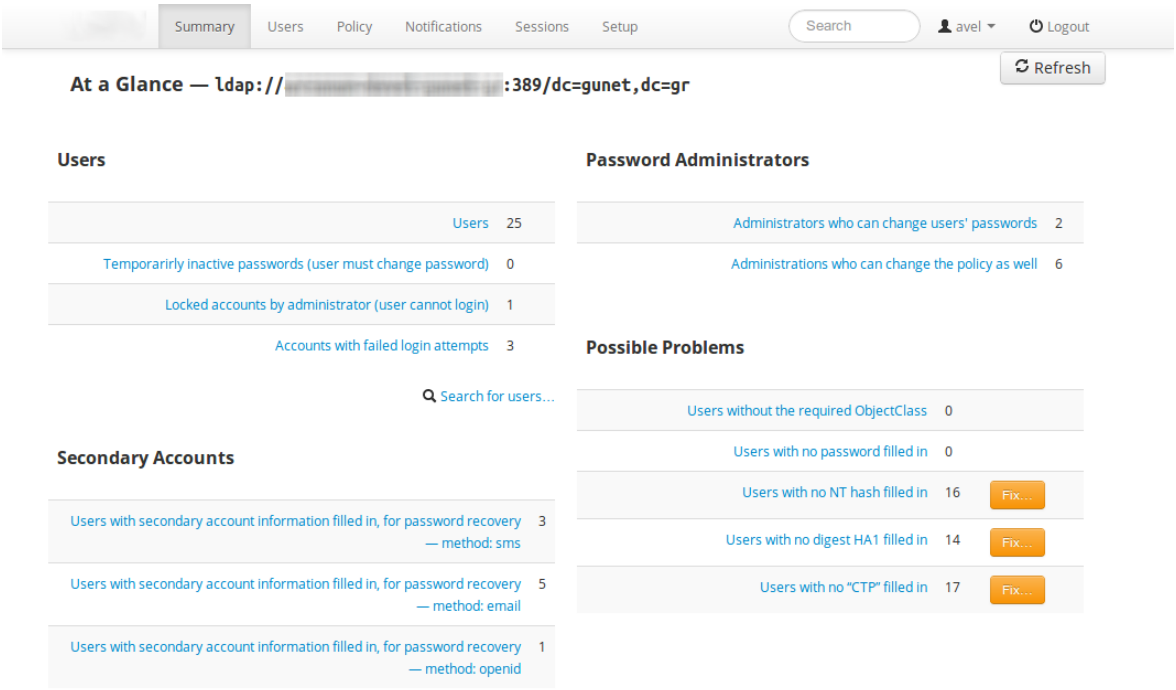
Σε κάθε περίπτωση γίνεται έλεγχος εγκυρότητας των στοιχείων που εισάγονται από τον χρήστη. Σε περίπτωση λάθους ο χρήστης ειδοποιείται και η διαδικασία σταματά.



Εικόνα 18 - Έλεγχος εγκυρότητας

3.5 ΕΙΣΑΓΩΓΗ ΔΙΑΧΕΙΡΙΣΤΗ ΚΑΙ ΠΡΟΒΟΛΗ ΣΥΝΟΨΗΣ

Στη σελίδα εισόδου στην εφαρμογή, όταν τα στοιχεία διαπίστευσης του χρήστη αντιστοιχούν σε έναν διαχειριστή του συστήματος, τότε η αρχική σελίδα της εφαρμογής διαφοροποιείται στην ακόλουθη :

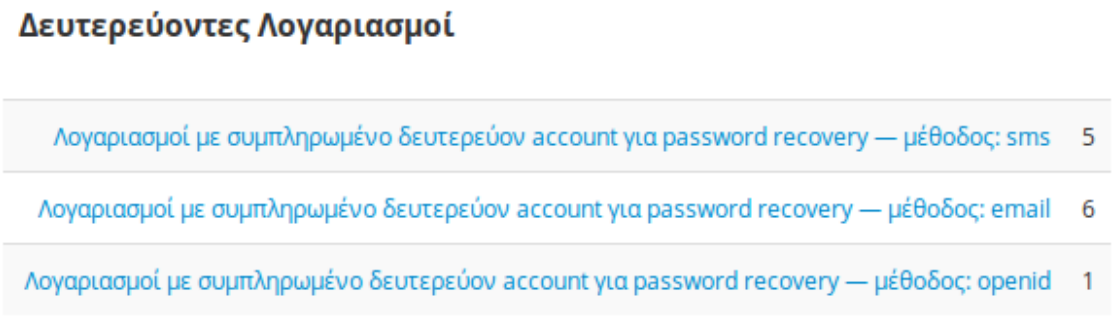


Εικόνα 19 - Αρχική σελίδα διαχειριστών

Σε αυτήν την περίπτωσή παρουσιάζονται στον διαχειριστή οι βασικές πληροφορίες χρήσης και λειτουργίας της εφαρμογής. Η συνολική εικόνα του συστήματος αποτελεί το πρώτο βήμα, πέρα από το οποίο μπορούν να πραγματοποιηθούν οι ενέργειές διαχείρισης. Σε κάθε περίπτωση εκτός από τα στοιχεία που παρουσιάζονται στο διαχειριστή, υπάρχει και ένας σύνδεσμος με αναλυτικότερες λεπτομέρειες, οπού παρουσιάζονται και οι δυνατές ενέργειες που μπορεί να εκτελέσει.

Οι κυριότερες ενέργειες για έναν διαχειριστή είναι η επιδιόρθωση στοιχείων χρηστών και ο έλεγχος σχετικά με τους δευτερεύοντες λογαριασμούς χρηστών.

Δίνεται η επιλογή της ανάκτησης μιας λίστας χρηστών που έχουν συμπληρώσει τα στοιχεία που θεωρούνται απαραίτητα για την ανάκτηση κωδικών. Αυτή η λίστα διαχωρίζεται σε τρεις κατηγορίες, ανάλογα με το είδος του δευτερεύοντος λογαριασμού που χρησιμοποιείται



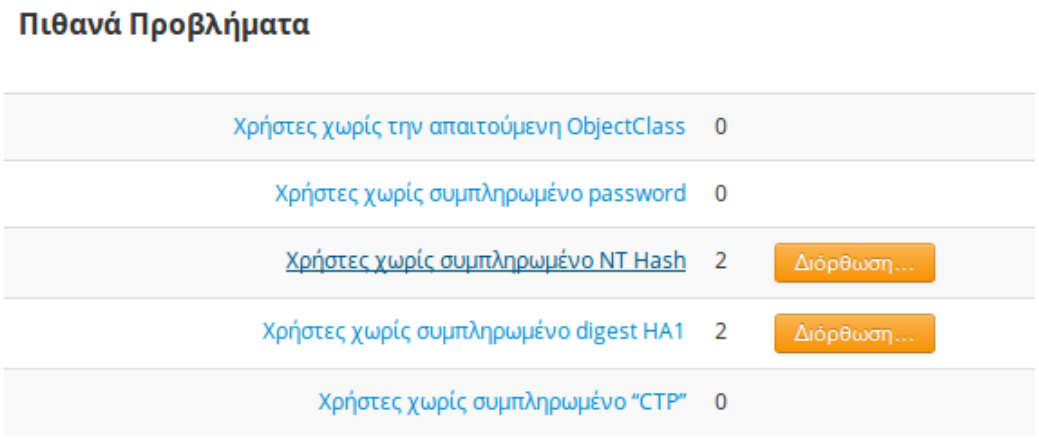
Εικόνα 20 - Δευτερεύοντες λογαριασμοί

Ακολουθώντας την πρώτη επιλογή δίνεται λίστα χρηστών και η δυνατότητα προβολής λεπτομερειών, αλλά και αλλαγής κωδικών.

Εικόνα 21 - Λίστα χρηστών με SMS

3.6 ΕΠΙΔΙΟΡΘΩΣΗ ΠΡΟΒΛΗΜΑΤΩΝ ΕΦΑΡΜΟΓΗΣ

Η επιδιόρθωση των προβλημάτων της εφαρμογής αναφέρεται σε προβλήματα που πιθανώς να υπάρχουν στις πληροφορίες και ιδιότητες των χρηστών, είτε αυτό αναφέρεται σε κλάσεις που λείπουν, είτε σε μορφές κωδικών που δεν έχουν αποθηκευθεί. Σε κάθε περίπτωση η εφαρμογή αναλαμβάνει να συμπληρώσει οποιαδήποτε παράλειψη και ο χρήστης απλά αρκεί να ακολουθήσει τον σύνδεσμο διόρθωση.

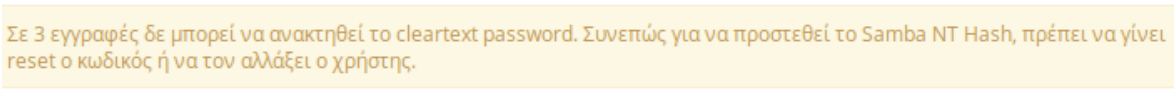


Εικόνα 22 - Λίστα πιθανών προβλημάτων

Ο σύνδεσμος "*Διόρθωση*" ενεργοποιεί την διαδικασία εισαγωγής των ελλιπών στοιχείων σε κάθε object που παρουσιάζει πρόβλημα.

Επιλέγοντας την επιδιόρθωση χρηστών που δεν έχουν συμπληρωμένο κωδικό NTHash, το σύστημα ελέγχει αν υπάρχει ο κωδικός σε απλό κείμενο.

Αν δεν υπάρχει δίνεται ένα μήνυμα λάθους, καθώς δεν είναι δυνατόν να παραχθεί κωδικός από άγνωστη πηγή, ειδάλλως δημιουργείται ο κωδικός και παρουσιάζεται στον χρήστη η εικόνα επιτυχίας.



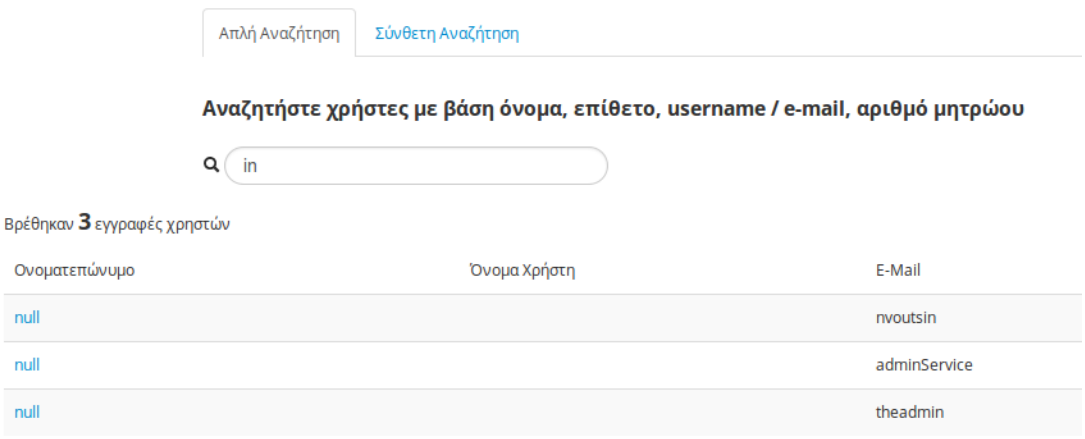
Εικόνα 23 - Αποτυχία δημιουργίας κωδικού

3.7 ΑΝΑΖΗΤΗΣΗ ΧΡΗΣΤΗ ΚΑΙ ΠΡΟΒΟΛΗ ΠΛΗΡΟΦΟΡΙΩΝ

Σε κάθε περίπτωση που ένας διαχειριστής το επιθυμεί μπορεί να αναζητήσει τις πληροφορίες ενός χρήστη.

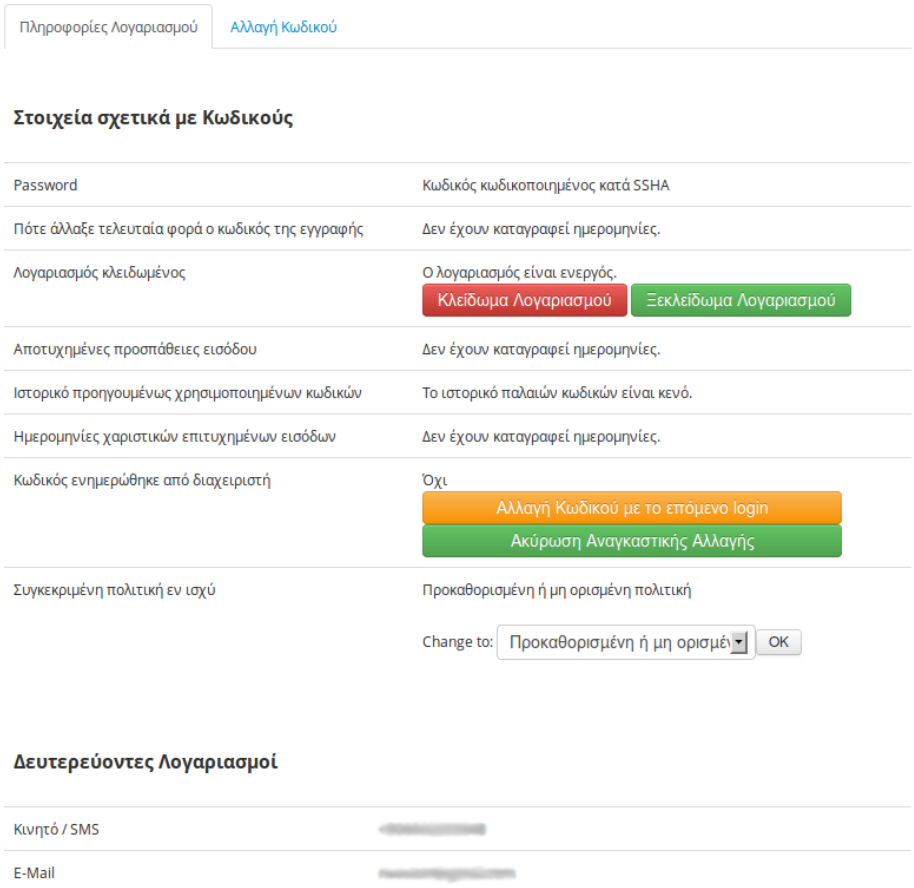
Αυτό γίνεται συμπληρώνοντας την απλή φόρμα αναζήτησής στην επιλογή χρήστες.

Με την ολοκλήρωση της αναζήτησης παρουσιάζεται μια λίστα με τα αποτελέσματα και παρουσιάζονται οι πληροφορίες του λογαριασμού των χρηστών.



Εικόνα 24 - Απλή αναζήτηση

Επιλέγοντας έναν από τους παραπάνω χρήστες γίνεται ανακατεύθυνση στην σελίδα πληροφοριών που είναι η ακόλουθη:



Εικόνα 25 - Στοιχεία χρήστη

Σε αυτή την σελίδα παρουσιάζονται οποιεσδήποτε πληροφορίες αναζητά ο διαχειριστής.

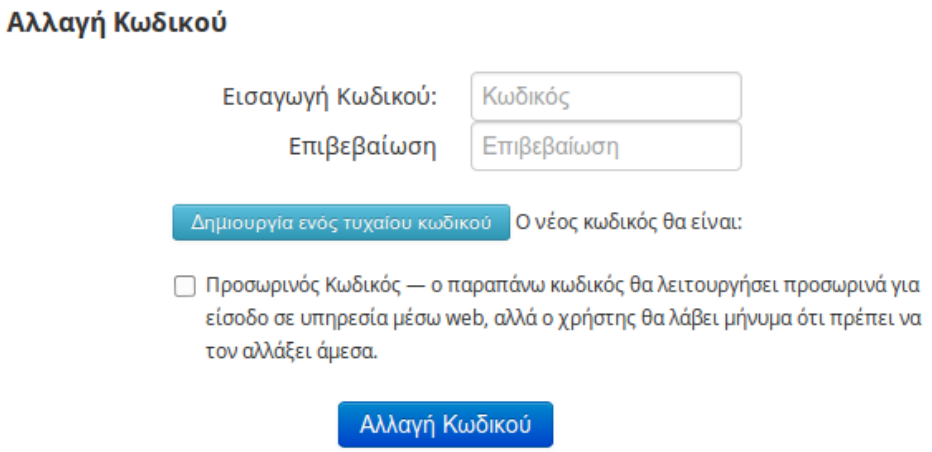
Σε αυτό το σημείο βρίσκεται η δυνατότητα για μια σειρά ενεργειών. Αυτές οι ενέργειες περιλαμβάνουν:

- ✓ την αλλαγή κωδικού
- ✓ το κλείδωμα ή ξεκλείδωμα λογαριασμού
- ✓ την αναγκαστική αλλαγή κωδικού από τον χρήστη κατά την επόμενη σύνδεσή του.

3.8 ΑΛΛΑΓΗ ΚΩΔΙΚΟΥ

Η ενέργεια της αλλαγής του κωδικού ενός χρήστη διεκπεραιώνεται με τη χρήση της φόρμας που μπορεί να ακολουθήσει ο διαχειριστής από την παραπάνω σελίδα.

Η φόρμα που θα χρησιμοποιηθεί απαιτεί απλά την δημιουργία ενός νέου κωδικού

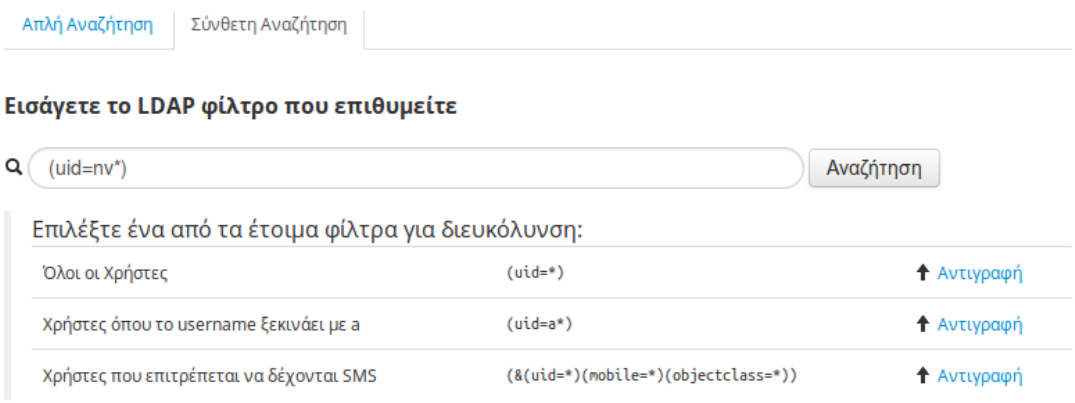


Εικόνα 26 - Αλλαγή κωδικού από διαχειριστή

Η εφαρμογή παρέχει τη διευκόλυνση για την δημιουργία κωδικού από το ίδιο το σύστημα, ενώ πολύ σημαντική είναι η ύπαρξη της λειτουργία δημιουργίας προσωρινού κωδικού. Αυτό σημαίνει ότι ο χρήστης θα αναγκαστεί στην επόμενη σύνδεση να αλλάξει τον κωδικό του, διασφαλίζοντας με αυτό τον τρόπο την ασφάλεια της σύνδεσής του στο μέλλον.

3.9 ΠΡΟΧΩΡΗΜΕΝΗ ΑΝΑΖΗΤΗΣΗ ΧΡΗΣΤΩΝ

Σε πολλές περιπτώσεις η απλή αναζήτησή δεν αρκεί για να δώσει τα αποτελέσματα που αναζητούνται. Σημειώνεται πως είναι δυνατή η χρήση του συνόλου των αποτελεσμάτων για πολλαπλές ενέργειες σε αυτά. Για το σκοπό αυτό δίνεται στο διαχειριστή η δυνατότητα χρήσης πιο σύνθετων φίλτρων αναζήτησης. Αυτά τα φίλτρα όπως προαναφέρθηκε απαιτούν μια γνώση σύνταξης ldap αναζητήσεων. Επιλέγοντας την σύνθετη αναζήτηση εμφανίζεται η κάτωθι σελίδα, στην οποία δίνονται και μια σειρά παραδειγμάτων αναζητήσεων.

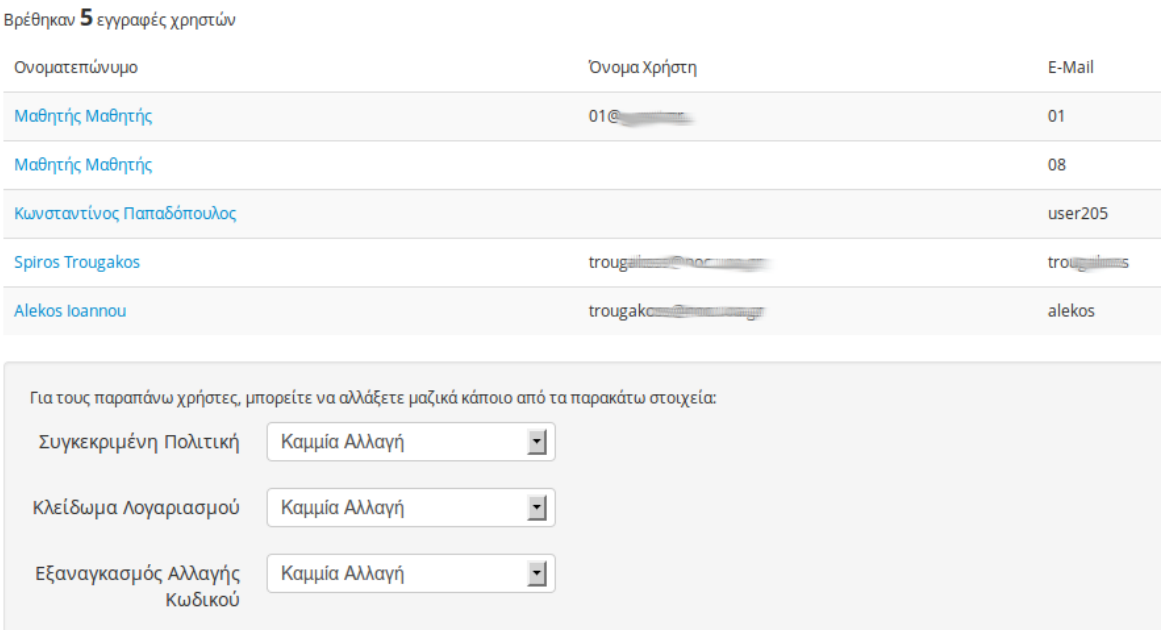


Τα αποτελέσματα είναι αντίστοιχα της απλής αναζήτησης και οι ενέργειες που μπορούν να γίνουν ακριβώς οι ίδιες.

Πιθανά φίλτρα που μπορούν να χρησιμοποιηθούν είναι τα ακόλουθα

Χρήστες που μπορούν να δέχονται SMS

`(&(uid=*)(mobile=*)(objectclass=*))` , Με αποτέλεσμα

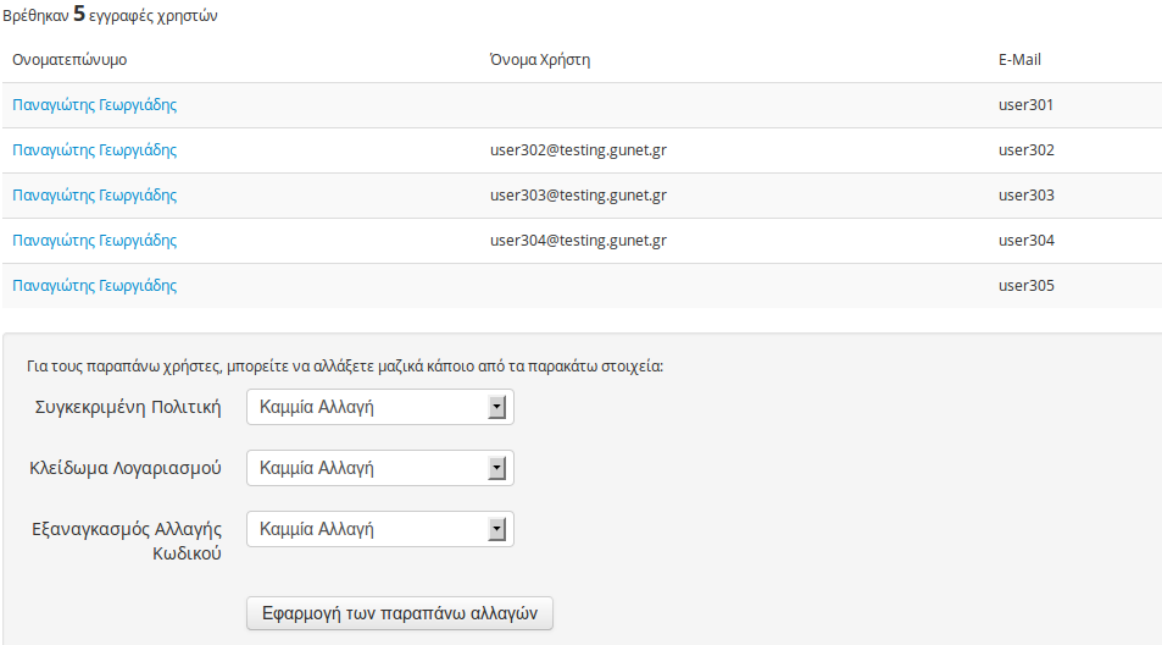


Εικόνα 27 – Χρήστες με SMS

Χρήστες που ανήκουν στο τμήμα μαθηματικών του ιδρύματος (τμήμα με αριθμό 418)

`(&(&(uid=*)(objectclass=*))(edupersonorgunitdn=ou=418,ou=units,dc=teixal,dc=gr))`

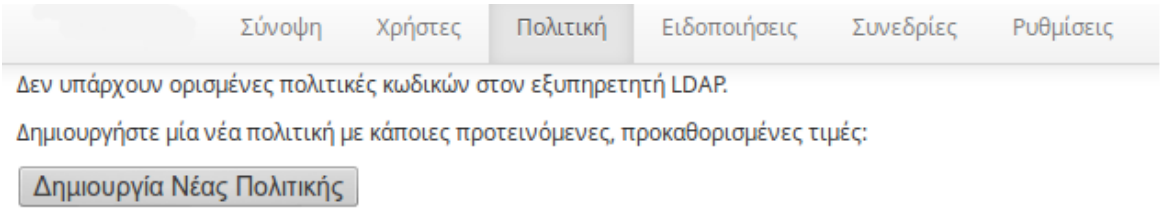
Με αποτέλεσμα



Εικόνα 28 - Χρήστες Μαθηματικού

3.10 ΔΗΜΙΟΥΡΓΙΑ – ΕΠΕΞΕΡΓΑΣΙΑ ΠΟΛΙΤΙΚΗΣ

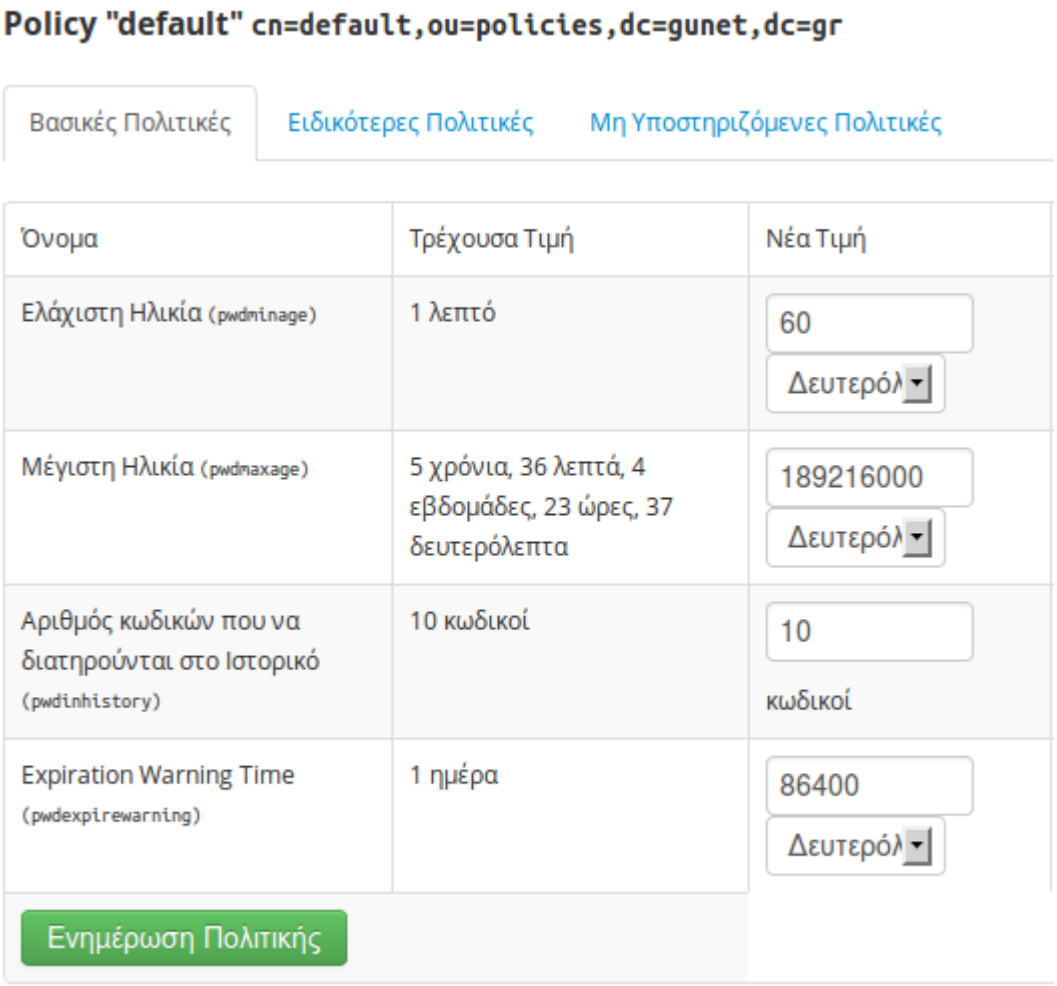
Η διαδικασία της δημιουργίας και επεξεργασίας της πολιτικής θεωρείται ο δεύτερος μεγάλος πυλώνας της εφαρμογής. Το σύστημα όταν αναγνωρίζει πως δεν υπάρχει καμιά πολιτική σχετικά με τους κωδικούς, δίνει τη δυνατότητα στον χρήστη για δημιουργία νέας πολιτικής όπως φαίνεται ακολούθως.



Εν συνεχεία η επιλογή δημιουργίας νέας πολιτικής, ουσιαστικά αρχικοποιεί την προεπιλεγμένη πολιτική του συστήματος. Αυτό είναι ουσιαστικά το εναρκτήριο βήμα για την επεξεργασία της πολιτικής.

Στην επεξεργασία ο χρήστης μπορεί να θέσει τιμές στα πεδία που απαρτίζουν την πολιτική, όπως η ελάχιστη ηλικία κωδικού, αριθμός κωδικών στο ιστορικό και ούτω καθεξής.

Ένα υποσύνολο των διαθέσιμων επιλογών φαίνεται στην επόμενη οθόνη:



3.11 ΕΠΙΠΛΕΟΝ ΔΙΑΧΕΙΡΙΣΤΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ

Πέρα από τις βασικές ενέργειες που μπορεί να κάνει ένας διαχειριστής, με στόχο την διαχείριση κωδικών, στο σύστημα δίνονται και μια σειρά ενεργειών υποστηρικτικών της ίδιας της εφαρμογής.

Αυτές αφορούν την τροποποίηση των ρυθμίσεων της εφαρμογής, τη διαχείριση των ατόμων με δικαιώματα διαχειριστή, τη διαχείριση των ανοιχτών συνδέσεων, καθώς και την ενεργοποίηση και παραμετροποίηση των ειδοποιήσεων που μπορεί να στείλει το σύστημα προς τους χρήστες.

3.11.1 Ρυθμίσεις εφαρμογής

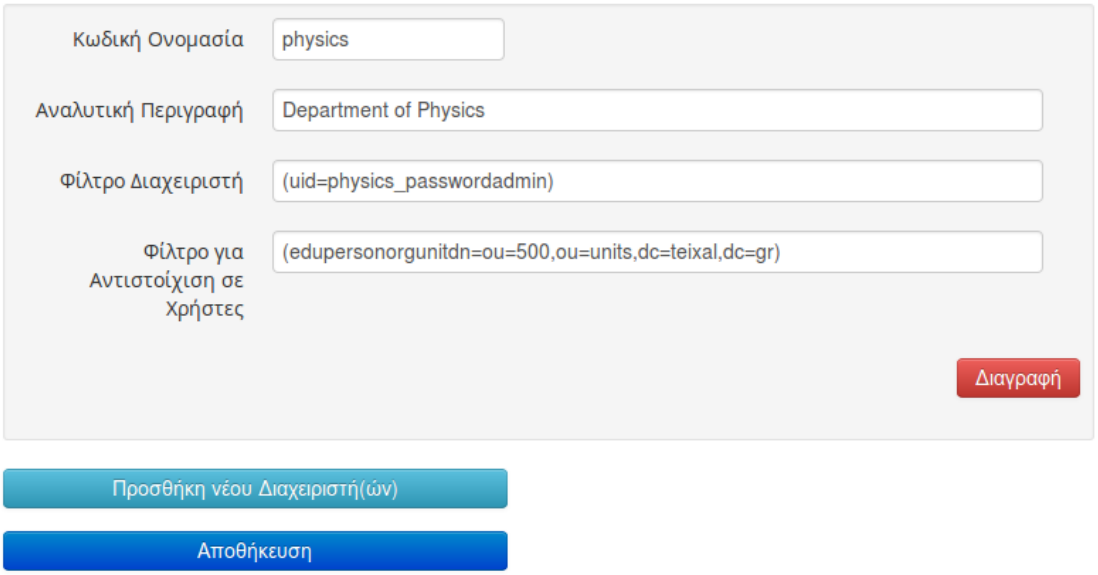
Το περιβάλλον στο οποίο ο χρήστης μπορεί να μεταβάλει τις ρυθμίσεις της εφαρμογής είναι ίδιο με το αντίστοιχο που παρουσιάζεται στην διαδικασία εγκατάστασης,. Στον χρήστη παρουσιάζεται η ομαδοποίηση των ρυθμίσεων όπως είχε πρωτοεμφανιστεί με την προσθήκη μιας κατηγορίας διαχείρισης κωδικών

Εικόνα 29 - Ρυθμίσεις εφαρμογής

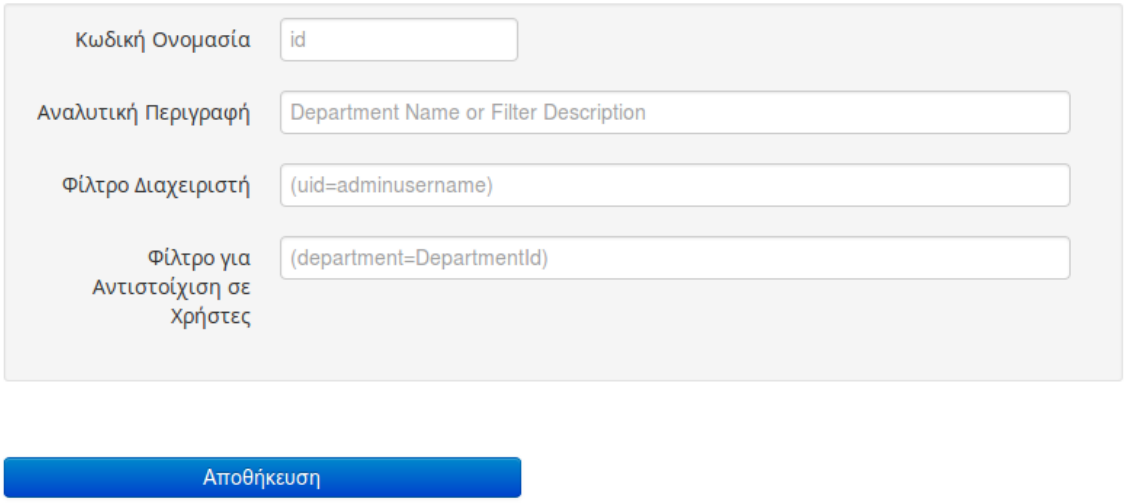
3.11.2 Προσθήκη διαχειριστών

Το σύστημα υποστηρίζει δυο κατηγορίες διαχειριστών, τους διαχειριστές κωδικών και τους διαχειριστές πολιτικής, Ειδικά για τους διαχειριστές κωδικών υπάρχει πρόβλεψη προσθήκης αυτών μέσα από το διαχειριστικό περιβάλλον.

Με την επιλογή της αντίστοιχης ρύθμισης στο διαχειριστικό, ο χρήστης (υπερδιαχειριστής) μπορεί να δει μια λίστα αυτών και αν προσθέσει ή να διαγράψει αν το επιθυμεί.



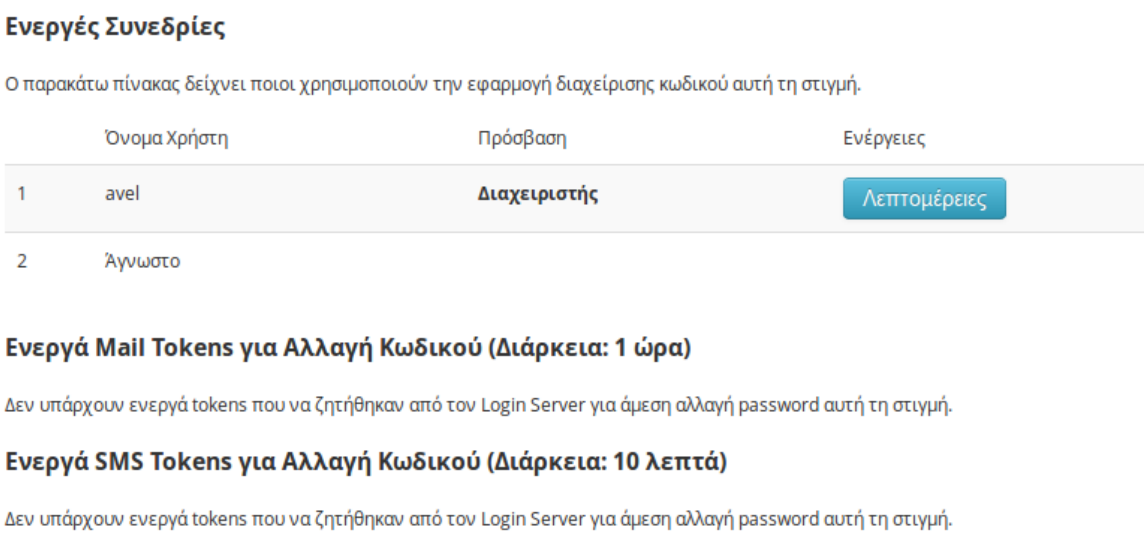
Εικόνα 30 - Προβολή διαχειριστών κωδικών



Εικόνα 31 - Προσθήκη διαχειριστή κωδικών

3.11.3 Συνεδρίες

Συχνά είναι απαραίτητο, κυρίως για λόγους ασφαλείας, να παρουσιάζεται μια λίστα των ατόμων που χρησιμοποιούν την εφαρμογή. Αυτό μπορεί να γίνει επιλέγοντας το μενού Συνεδρίες. Εκεί παρουσιάζεται μια λίστα των ατόμων που είναι συνδεδεμένοι στην εφαρμογή, αλλά δίνεται και μια εικόνα τον προσωρινών κωδικών που έχουν εκδοθεί ώστε να μπορέσουν οι χρήστες να αλλάξουν κωδικό.

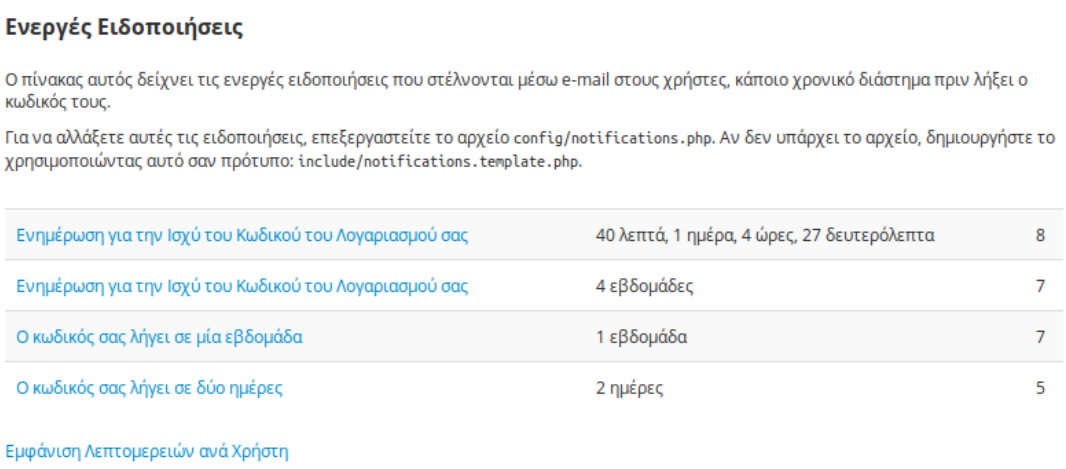


Εικόνα 32 - Λίστα ενεργών συνδέσεων

3.11.4 Ειδοποιήσεις

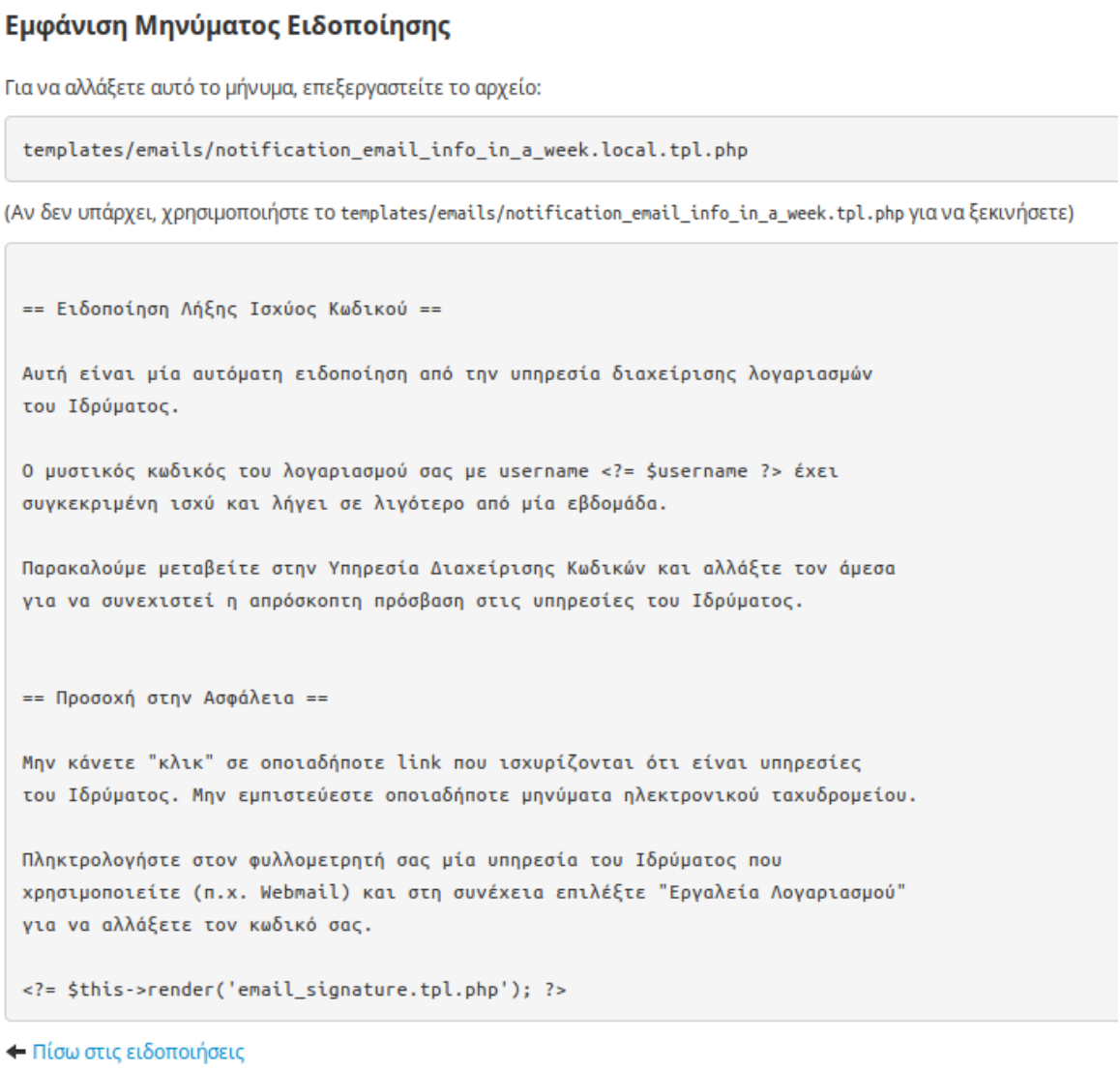
Οι ειδοποιήσεις που μπορεί να στείλει η εφαρμογή αποτελεί ένα σημαντικό κομμάτι που μπορεί να βοηθήσει στην σωστή χρήση του συστήματος. Υπάρχουν πέντε διαφορετικές κατηγορίες ειδοποιήςεων που αποστέλλονται και ο διαχειριστής μπορεί να τις δει από την επιλογή *ΕΙΔΟΠΟΙΗΣΕΙΣ* .

Σημειώνεται πως για να επεξεργαστεί κανείς τις ειδοποιήσεις θα πρέπει αν γίνει απευθείας μετατροπή των πηγαίων αρχείων και του αρχείου ρυθμίσεων αυτού (notifications.php)



Εικόνα 33 - Λίστα ειδοποιήσεων

Παραθέτουμε και ένα παράδειγμα αρχείου ειδοποιήσεων, όπως αυτό εμφανίζεται στον χρήστη, μέσα στην εφαρμογή, Όπως και στην περίπτωση των ρυθμίσεων, για να αλλαχτούν οι παράμετροι αυτού, θα πρέπει να γίνει τροποποίηση του πηγαίου αρχείου.



Εικόνα 34 - Εμφάνιση μηνύματος ειδοποίησης

Τα παραπάνω σενάρια χρήσης δείχνουν μια αρχική εικόνα των λειτουργιών του συστήματος. Είναι αυτονόητο πως οι ανάγκες χρήσης της εφαρμογής μπορούν να οδηγήσουν σε πιο σύνθετες καταστάσεις

4. ΤΕΧΝΙΚΑ – ΑΡΧΙΤΕΚΤΟΝΙΚΑ ΣΤΟΙΧΕΙΑ

4.1 ΛΟΓΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Στο αρχιτεκτονικό κομμάτι, η εφαρμογή απαρτίζεται από δυο λογικά επίπεδα. Αυτά τα επίπεδα ουσιαστικά αντικατοπτρίζουν τα επίπεδα πρόσβασης των χρηστών και μετουσιώνονται σε δύο διακριτές υποεφαρμογές.

Η πρώτη κατηγορία αναφέρεται στο διαχειριστικό κομμάτι της εφαρμογής και απαρτίζεται από όλες τις ενέργειες που γίνονται εκ μέρους των διαχειριστών με αποδέκτες τους χρήστες. Η δεύτερη κατηγορία είναι οι ενέργειες που γίνονται από την πλευρά των απλών χρηστών, διαπιστευμένων ή μη, με αποδέκτες τους ιδίους. Και οι δυο υποεφαρμογές καταλήγουν σε ένα κοινό επίπεδο επικοινωνίας με τις υποδομές καταλόγου.

Σε προγραμματιστικό επίπεδο η εφαρμογή διατηρεί την συνηθισμένη πρακτική του διαχωρισμού του λογικού τμήματος της εφαρμογής, από την παρουσίαση. Αυτό διεκπεραιώνεται με την χρήση μιας σειράς προτύπων που διατηρούν πλήρως την ανεξαρτησία τους από την υποκείμενη λογική επεξεργασία των δεδομένων.

4.2 ΦΥΣΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Σε φυσικό επίπεδο η εφαρμογή απαιτεί απλά την ύπαρξη ενός εξυπηρετητή, ο οποίος παρέχει την πλήρη απαιτούμενη λειτουργικότητα. Δεν υπάρχει καμιά απαίτηση για δευτερεύουσα εγκατάσταση καθώς δεν παρατηρείται η ύπαρξη φόρτου. Σε κάθε περίπτωση δίνεται η δυνατότητα για χρήση πολλαπλών εξυπηρετητών για την διαχείριση φόρτου, σε συστημικό επίπεδο, χωρίς την ανάγκη σχετικής παραμετροποίησης της εφαρμογής.

4.3 ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

Η εφαρμογή έχει τρία διακριτά κανάλια επικοινωνίας.

4.3.1 Διεπαφή με εξωτερικά συστήματα

Το ένα κανάλι επικοινωνίας αποτελεί την βασική λειτουργία της εφαρμογής και δημιουργείται με έναν LDAP server. Σε αυτόν γίνονται όλες οι ενέργειες διαχειριστικές ή μη και χωρίς αυτόν δεν νοείται η ύπαρξη της εφαρμογής.

4.3.2 Διεπαφή με το σύστημα διαπίστευσης

Το δεύτερο κανάλι επικοινωνίας είναι με την υποδομή του Single Sign On. Η υποδομή αυτή δίνει την δυνατότητα για διαπίστευση των χρηστών μέσω αυτού του συστήματος που παρέχει ασφάλεια και όχι με την απευθείας χρήση του LDAP.

4.3.3 Διεπαφή με σύστημα αποστολής μηνυμάτων.

Το τρίτο κανάλι επικοινωνίας αναφέρεται στη χρήση των υπηρεσιών SMS. Στην συγκεκριμένη υλοποίηση προτιμάται η χρήση των json RPC διεπαφών, παρόλα αυτά υπάρχει πρόβλεψη για χρήση οποιαδήποτε υποδομής SMS.

Η χρήση των SMS δίνει ένα επιπλέον επίπεδο λειτουργικότητας για την εφαρμογή, παρόλα αυτά η χρήση της μπορεί να γίνει και χωρίς αυτό, απλά με την παράλειψη της λειτουργίας επαναφοράς κωδικού με SMS και τη διατήρηση της επαναφοράς κωδικού με email

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο πλαίσιο του έργου, υλοποιήθηκε μια εφαρμογή η οποία χρησιμοποιώντας τις κατάλληλες υποδομές SSO, LDAP, και SMS, εξαλείφει την ανάγκη ύπαρξης ανθρωπίνου παράγοντα στις διαδικασίες ανάκτησης πρόσβασης σε λογαριασμούς χρηστών. Μεγάλη σημασία δόθηκε στην επικοινωνία της εφαρμογής με τα διάφορα υποσυστήματα και τις περιφερειακές εφαρμογές, ενώ πολύ σημαντική θεωρείται η δυνατότητα για μαζικές ενέργειες πάνω σε μια κατηγορία χρηστών.

Ιδιαίτερη προσοχή θα πρέπει να δοθεί στη συνολική υποδομή και διάταξη των μονάδων που εξυπηρετεί η εφαρμογή, καθώς χωρίς την ύπαρξη της διάταξης που έχει σχεδιαστεί, χάνεται η διασφάλιση της απρόσκοπτης λειτουργίας.

Στόχος της εφαρμογής είναι και παραμένει η εξυπηρέτηση του τελικού χρήστη και αυτό επιτυγχάνεται απόλυτα στο σύνολο των εγκαταστάσεων.

6. ΠΑΡΑΡΤΗΜΑ

6.1 ΑΡΧΕΙΟ ΡΥΘΜΙΣΕΩΝ

```
<?php

return array (

  'institution_name' => 'ΤΕΙ Χαλκιδικής',

  'institution_domain' => 'teixal.gr',

  'website_home' => 'http://Arcanum.teixal.gr/',

  'terms_link' => '',

  'privacy_policy_link' => '',

  'ldap' =>

  array (

    'host' => 'ldap://ldap.teixal.gr:389',

    'basedn' => 'dc=teixal,dc=gr',

    'bind' => 'cn=manager,dc=teixal,dc=gr',

    'password' => 'xxxxxx',

    'secondary_accounts' =>

    array (

      'sms' => 'mobile',

      'email' => 'GUAccountSecondaryMail',

      'openid' => 'GUAccountSecondaryOpenID',

    ),

    'filter' =>

    array (
```

```
      'user' => '(&(uid=%s)(objectclass=guperson))',
      'user_receivesms' => '(&(objectclass=guperson)(mobile=%s)(uid=*))',
      'admin_password' => '(&(uid=%s)(edupersonentitlement=admin_password))',
      'admin_policy' => '(&(uid=%s)(edupersonentitlement=dbadmin))',
    ),
    'servertype' => '',
    'restrictfilters' =>
    array (
      0 =>
      array (
        'id' => 'students418',
        'description' => 'Department of Mathematics',
        'adminfilter' => '(uid=passwordadmin)',
        'apply' => '(edupersonorgunitdn=ou=418,ou=units,dc=teixal,dc=gr)',
      ),
      1 =>
      array (
        'id' => 'physics',
        'description' => 'Department of Physics',
        'adminfilter' => '(uid=physics_passwordadmin)',
        'apply'                                                    =>
'(edupersonorgunitdn=ou=500,ou=units,dc=teixal,dc=gr)',
      ),
    ),
    'passwordHash' => 'ssha',
```

```
    'pwdpolicydraft10' => false,
    'passwordAttribute' => 'userPassword',
    'sambaNtAttribute' => 'sambaNtPassword',
    'ctpAttribute' => 'GUCtp',
    'ctpKey' => xxxxxxxxxxxxxxx',
    'actpAttribute' => '',
    'otpInitKeyAttribute' => '',
    'otpBackupPasswordsAttribute' => '',
    'digestha1Attribute' => 'gudigestha1',
    'digestRealm' => teixal.gr',
  ),
  'cas' =>
  array (
    'host' => 'sso.teixal.gr',
    'port' => 443,
    'uri' => '',
  ),
  'session_name' => 'arcanum1',
  'locale' =>
  array (
    'default_language' => 'el_GR',
  ),
  'title' => 'TEI Χαλκιδικης',
  'subtitle' => 'Εφαρμογή Διαχείρισης Κωδικού - Δοκιμαστική Εγκατάσταση',
  'motd' => '<p>This is an Arcanum Development Installation.</p>',
```

```
'admin' =>
array (
  'perform_strength_checks' => true,
  'summary_attrs' =>
  array (
    0 => 'cn',
    1 => 'uid',
    2 => 'mail',
  ),
  'show_attrs' =>
  array (
    0 => 'cn',
    1 => 'uid',
    2 => 'title',
    3 => 'mail',
  ),
),
'password_strength_policy' =>
array (
  'PW_CHECK_LEVENSHTEIN' => '2',
  'PW_CHECK_MIN_LEN' => '6',
  'PW_CHECK_MIN_UNIQ' => '5',
  'PW_CHECK_MIN_LCS' => '40',
  'PW_CHECK_MIN_NON_ALPHA' => '2',
  'PW_MIN_CONSECUTIVE_NUMBERS' => '2',
```

```
),
'recaptcha' =>
array (
  'pubkey' => 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx',
  'privkey' => 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx',
),
'mail' =>
array (
  'host' => 'relay.teixal.gr',
  'from' => 'noreply@teixal.gr',
  'fromComment' => 'Teixal Account Services',
  'replyto' => '',
  'smtp' =>
  array (
    'ssl' => '',
    'port' => 25,
    'auth' => '',
    'username' => '',
    'password' => '',
  ),
),
'sms_operator_number' => '6944444444',
'smsgw' =>
array (
  'sender' => 'jsonrpc',
```

```
    'receiver' => 'jsonrpc',
    'institution' => '',
    'host' => 'https://ws.xxxxx.gr',
    'port' => '443',
    'uri' => '/?service=sms&key=xxxxxxxxxxxxxxxx',
    'username' => '',
    'password' => '',
    'tout_con' => 10,
    'prefix' => 'xxPASS',
    'ip_receive' =>
    array ( 'xxx.xxx.xxx.xxx',
    ),
  ),
  'login_servers' =>
  array (
  ),
  'timezone' => 'Europe/Athens',
  'devel' =>
  array (
```

```
    'simulate_sms' => false,
    'allow_all_captcha' => true,
    'email_cc' => 'admin@noc.teixal.gr',
  ),
);
```

6.2 ΡΥΘΜΙΣΕΙΣ ΕΙΔΟΠΟΙΗΣΕΩΝ

```
<?php
/**
 * Default template configuration for password expiry notifications / reminders.
 *
 * Time cheat sheet
* #      300   5 M               #    604800   1 W
* #     2700  45 M               #   1814400   3 W
* #     3600   1 H               #   2419200   1 M
* #    54000  15 H               #  14515200   6 M
* #    86400   1 D               #  26611200  11 M
 * @package arcanum
 */


return array(
    array(
        'id' => 'info_in_a_year',
       'subject' => _("Information about the Expiration of your Password"),
        'seconds_to_expiry' => 29030400, // 1 year
        'method' => 'email',
        'message' => 'notification_email_info_in_a_year',
    ),
    array(
        'id' => 'info_in_a_month',
       'subject' => _("Information about the Expiration of your Password"),
        'seconds_to_expiry' => 2419200, // month
```

```
        'method' => 'email',
        'message' => 'notification_email_info_in_a_month',
    ),
    array(
        'id' => 'info_in_a_week',
       'subject' => sprintf( _("Your password expires in %s"), _("a week") ),
        'seconds_to_expiry' => 604800, // 1 week
        'method' => 'email',
        'message' => 'notification_email_info_in_a_week',
    ),
    array(
        'id' => 'info_in_two_days',
       'subject' => sprintf( _("Your password expires in %s"), _("two days") ),
        'seconds_to_expiry' => 86400*2, // 2 days
        'method' => 'email',
        'message' => 'notification_email_info_in_two_days',
    ),
);
```