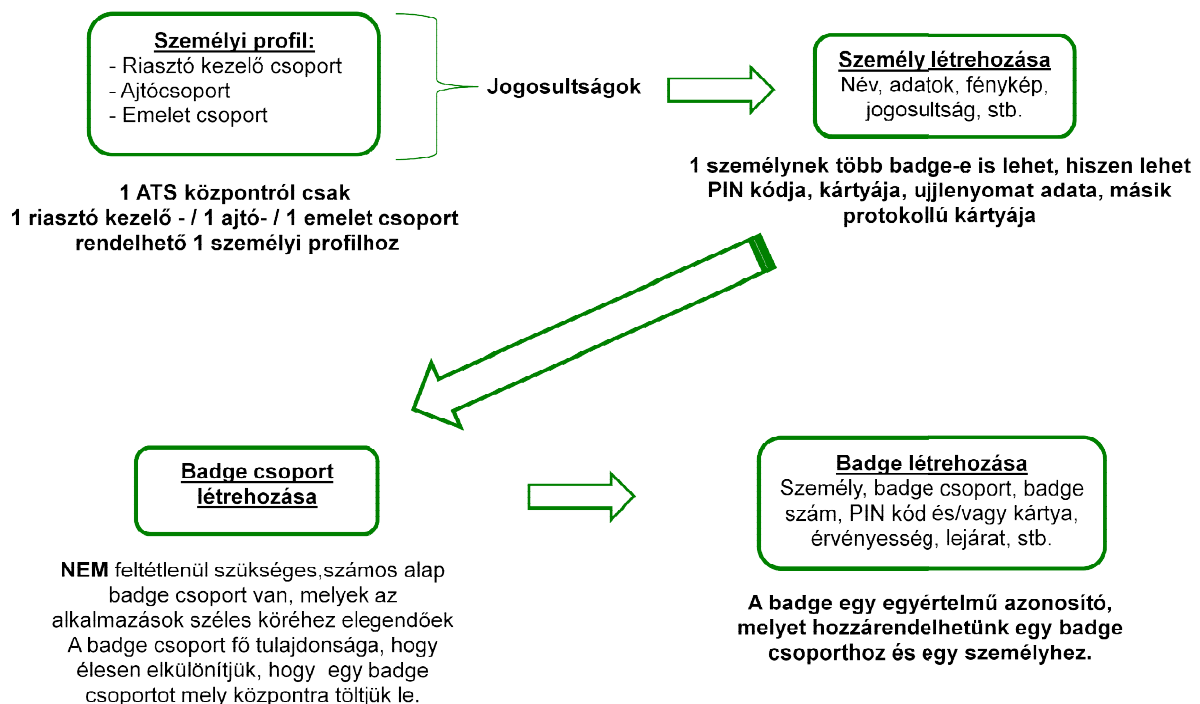


# ATS Advisor Master + Alliance

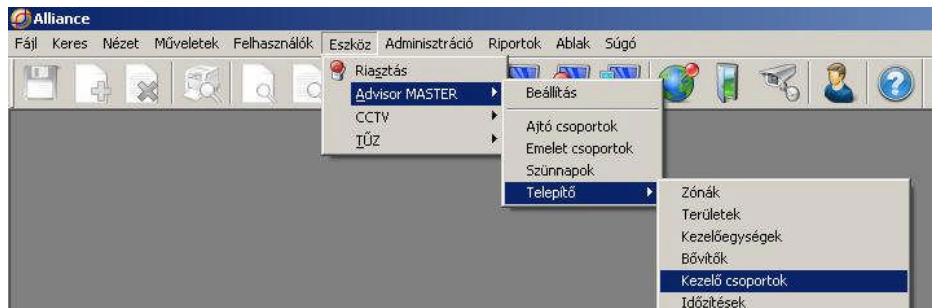
## Felhasználói PIN kód és kártya kezelési útmutató telepítőknek



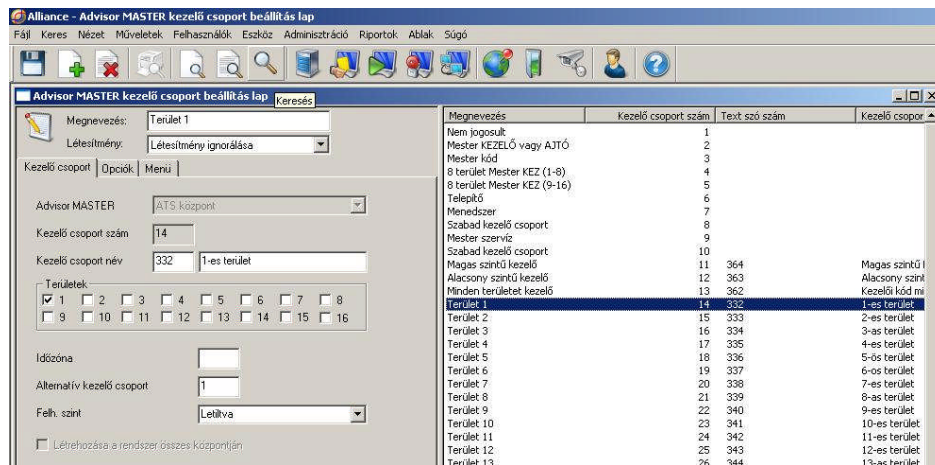
A személyeket, badge-eket, badge csoportokat, jogosultságokat létrehozhatjuk egymástól függetlenül is és később is egymáshoz rendelhetjük őket.

A **személyi profilok** vagy **jogosultságok**nál definiáljuk, hogy melyik (riasztó) kezelő csoportok, melyik ajtócsoporthoz, illetve melyik emeletcsoportok tartoznak az aktuális jogosultsághoz. Az ATS Advisor Master központok konfigurációjából adódóan, minden ATS központra egy kezelő csoport, egy ajtócsoport és egy emeletcsoport rendelhető egy jogosultságokhoz. Tehát tanácsos csoportokra osztani felhasználókat és előre megtervezni, hogy melyik csoportnak milyen jogosultságokat szeretnének adni az egyes központokon, ezek alapján pedig előre elkészíteni az egyes személyi profilokat, hogy a személy jogosultsághoz rendelésénél már csak ki kelljen választani őket a legördülő listából.

Készítsünk elsőként kezelői csoportot:



A megjelenő menüben szokás szerint a Keresés ikonra kattintva láthatjuk a jelenlegi kezelő csoportokat, központok és szám szerint csoportosítva. Az Adat hozzáadás ikonra kattintva hozhatunk létre új kezelő csoportot.



Látható, hogy – mint minden szinten – még kezelő csoport szinten is lehetséges a **létesítmény**hez rendelés.

A zónákhoz és területekhez hasonlóan a **megnevezés** (Alliance-en belüli név) és a kezelő csoport neve (ATS központra is letöltött név) akár különböző is lehet.

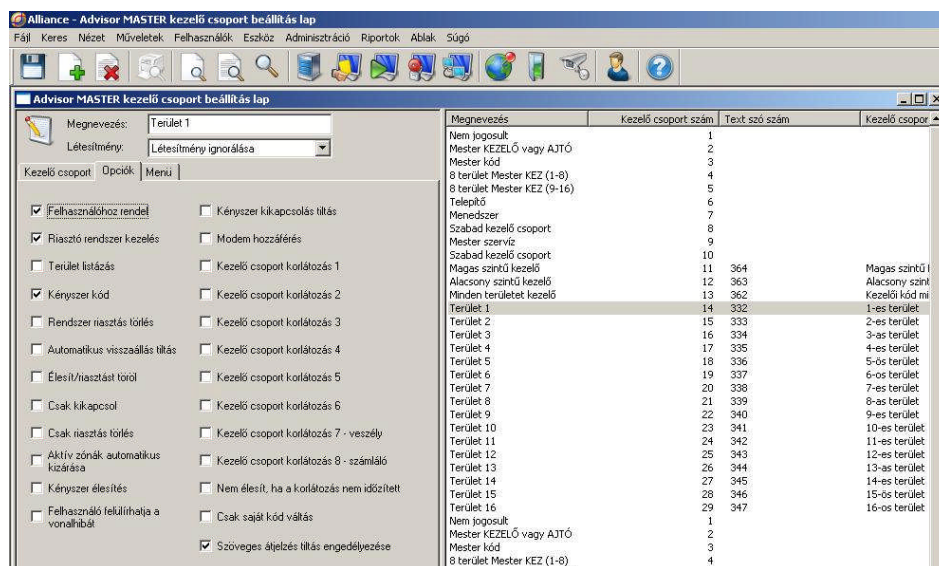
A **területek**nél egyértelműen jelölhetjük, hogy mely területek kezelését szeretnénk engedélyezni az adott csoportnak, azt, hogy hogyan lesznek képesek ezen területek kezelésére azt az opciók menüpontokban programozhatjuk be.

Az **időzóna** üresen hagyva 0-ás időzónának minősül vagyis a nap 24 órájában igaz. Az időzóna segítségével konfigurálhatjuk azt, hogy az adott riasztó kezelő jogosultság milyen időszakokban legyen érvényes. Segítségével konfigurálhatunk felhasználókat, akik például csak munkaidőben és hétköznap tudják ki- és/vagy bekapcsolni az egyes területeket.

Az **alternatív kezelő csoport**nál állíthatjuk be, hogy időzónán kívüli időben milyen másik kezelő csoport szerinti jogosultságai legyenek a kezelő csoportnak. Alapbeállítás szerint az 1-es "Nem jogosult" kezelő csoport van beállítva minden csoporthoz.

A **felhasználói szint** esetén állíthatjuk be, hogy az EN50131-es szabvány szerinti Grade2 és Grade3 szintek szerint meghatározott felülírási joggal rendelkezzenek-e az adott kezelő csoport tagjai. Az alapbeállítás a letiltva.

Amennyiben az adott kezelő csoportot minden központra szeretnénk letölteni, akkor pipáljuk be a legalsó opciót, akkor érdemes használni, ha speciális jogosultságokat konfiguráltunk és egy másik központon csak a területek konfigurációját kell csak megváltoztatni.



Az opciók fülre kattintva az alábbi opciókat rendelhetjük hozzá a kezelő csoporthoz:

**Felhasználóhoz rendelés:** ATS Advisor Master rendszerénél riasztó kezelő csoportot határozhatunk meg felhasználóknál, kezelőegységeknél/olvasóknál és kulcsos kapcsoló zónáknál. Ha ezt a kezelő csoportot felhasználóhoz is szeretnénk rendelni, akkor jelöljük be ezt az opciót.

**Riasztó rendszer kezelés:** A Kezelő csoport fülön meghatározott területeket csak akkor lesz képes élesíteni és/vagy hatástalanítani az adott kezelő csoport, ha ez az opció be van jelölve.

**Terület listázás:** Ha szeretnénk az élesítési/kikapcsolási folyamat során a kezelőegységen megjeleníteni az összes olyan területet, amelynek kezelésére a felhasználónak van jogosultsága, akkor jelöljük be ezt az opciót.

**Kényszer kód:** Felhasználók számára engedélyezi a kényszer kód használatát. [a kényszer kód kiegészítő konfigurációja elérhető az Eszköz/Advisor Master/Telepítő/Rendszer opciók/Rendszer opciók/Rendszer opciók1 fülön a Kényszer típus opciónál]

**Rendszer riasztás törlés:** Engedélyezi a kezelő csoport számára a tárolódó rendszer riasztások törlését, azok helyreállítása után. Rendszer riasztásnak minősül a bővítő szabotázs, sziréna kimenet hiba, akku hiba, átjelzés hiba, stb.

**Automatikus visszaállítás tiltás:** Kizárt zónák nem kerülnek visszaállításra a területük kikapcsolása után sem, ha ezzel a kezelő csoporttal kapcsolták ki a területet.

**Élesít/riasztást töröl:** Korlátozza a riasztó kezelést kizárólag élesítésre és riasztás törlésre. Ezzel az opcióval valósítható meg, hogy például egy ór ne tudjon kikapcsolni területeket csak élesíteni, illetve nyugtázni az onnan érkező riasztásokat. Működéséhez Riasztó rendszer kezelés opciónak szintén engedélyezve kell lennie.

**Csak kikapcsol:** Korlátozza a programozott területek riasztó kezelését csak kikapcsolásra. Működéséhez Riasztó rendszer kezelés opciónak szintén engedélyezve kell lennie.

**Csak riasztás törlés:** Korlátozza a programozott területek riasztó kezelését csak riasztás törlésre. Ezzel a jogosultsággal nem lehet kikapcsolni a területeket. Működéséhez Riasztó rendszer kezelés opciónak szintén engedélyezve kell lennie.

**Aktív zónák automatikus kizárása:** Élesítés esetén automatikusan kizárja az aktív zónákat. Ha nincs engedélyezve akkor a terület(ek) csak akkor élesíthetők, ha nincs aktív zónájuk vagy kényszerélesítéssel, ha az engedélyezve van.

**Kényszer élesítés:** Élesíti a területeket akkor is ha van aktív zónájuk. Ebben az esetben zóna típustól függően lehetséges, hogy azonnali riasztás történik.

**Felhasználó felülírhatja a vonalhibát:** Ha engedélyezve van ez az opció, akkor a kezelő csoport felhasználói felülírhatják a vonalhibát, ha az minden kommunikációs úton fennáll. Ez természetesen naplózásra kerül.

**Kényszer kikapcsolás tiltás:** Nem engedélyezi a terület kikapcsolását aktív zónák esetén (csak az 1-es és 11-es zóna típusok esetén használható).

**Modem hozzáférés:** A kezelő csoporttal rendelkező felhasználó számára engedélyezi modemes hozzáférés aktiválását a központhoz.

**Kezelő csoport korlátozás 1-6:** A kiválasztott területeken szigorítják a riasztó kezelést időzített kikapcsolásra vagy élesítés/riasztás törlésre. Kezelő csoportonként csak 1 korlátozás használható, de több kezelő csoport is használhatja ugyanazt a korlátozást. [kezelő csoport korlátozás kiegészítő konfigurációja elérhető az Eszköz/Advisor Master/Telepítő/Kezelő csoport korlátozások menüpontban.]

**Kezelő csoport korlátozás 7 – veszély:** úgy működik, mint az 1-es kezelő csoport korlátozás, de időzített kikapcsolás esetén vészriasztást generál, ha a terület újraélesedik. Használható őrárat ellenőrzés esetén,

ha az őrnek időről-időre be kell jelentkeznie egy adott helyen (terület kikapcsolással), ha ez nem történik meg, akkor a terület újraélesedik és a központ küldi a vészriasztást.

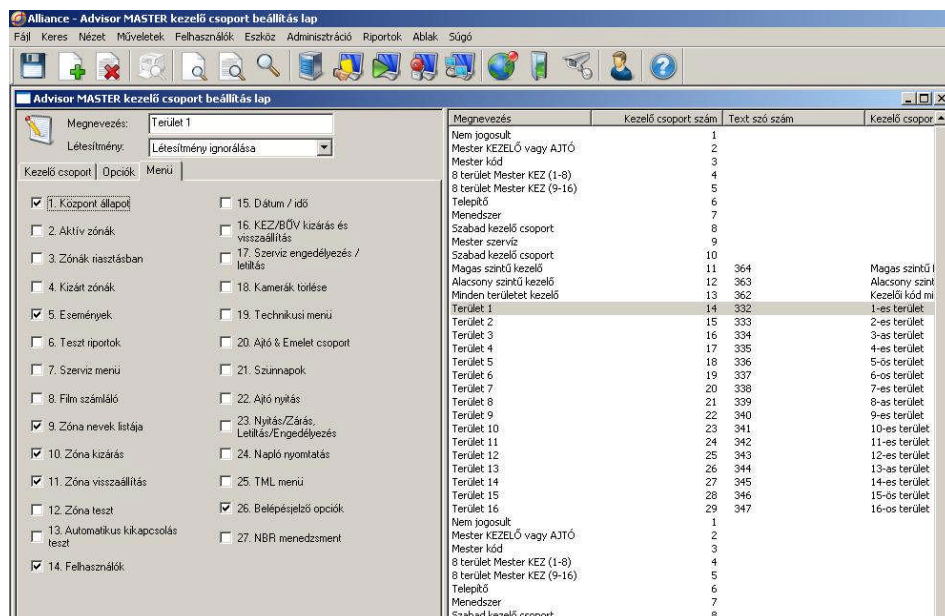
**Kezelő csoport korlátozás 8 – számláló:** úgy működik, mint az 1-es kezelő csoport korlátozás, de kikapcsoláskor elindít egy felhasználó számlálót - és növeli annak értékét. Amennyiben egy terület ezzel a kezelő csoporttal élesedik, akkor csökkenti a számlálót. A kijelző mindig kijelzi a számláló értékét. Amikor a számláló eléri a 0-át, a kezelő csoport élesíteni fogja a hozzá tartozó területeket. Az időzítések erre a korlátozásra nem működnek. Területenként a maximális felhasználó szám 255.

**Nem élesít, ha a korlátozás nem időzített:** megelőzi a kezelői csoport korlátozás területek élesítésének időzítését, ha egy felhasználó - kezelői csoport korlátozás nélkül - hatástalanítja a területet.

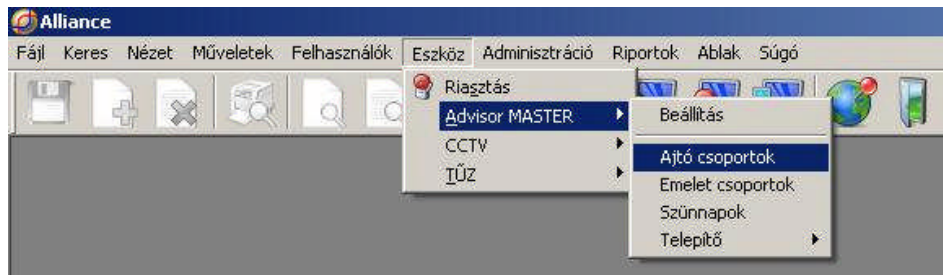
**Csak saját kód váltás:** meghatározza, hogy a felhasználó megváltoztathatja a PIN kódját a többi felhasználónak, akik ugyanezzel a kezelő csoporttal vagy annál kisebb jogosultsággal rendelkeznek vagy csak a saját PIN kódját változtathatja. [hogyan egyáltalán tudjon PIN kódot változtatni egy felhasználó kezelőről, ahhoz jogosultnak kell lennie a 14. Felhasználók menüponthoz is.]

**Szöveges átjelzés tiltás engedélyezése:** ezzel az opcióval a felhasználó jogosulttá válik, hogy törölje az aktív és jelentésre váró eseményeket hangmodulos átjelzés esetén (ez a tiltás nem vonatkozik a pánik, kényszer és rablás eseményekre). Az opció csak akkor használható, ha a felhasználó - és a kezelőegység kezelő csoportjához is egyaránt hozzá van rendelve.

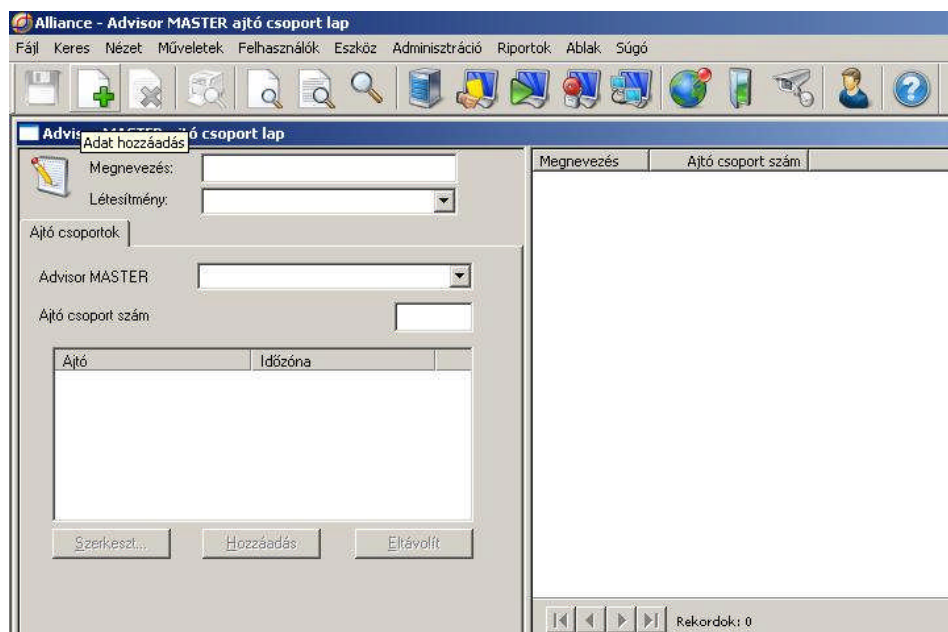
A menü fülre kattintva jelölhetjük be, hogy az adott kezelő csoport mely menüpontok kezelésére lesz alkalmas. Ha minden beállítással végeztünk a Mentés ikonnal menthetjük a változásokat.



### Ajtócsoporthoz létrehozása:



Lépünk be az Eszköz/Advisor MASTER/Ajtó csoportok menübe.



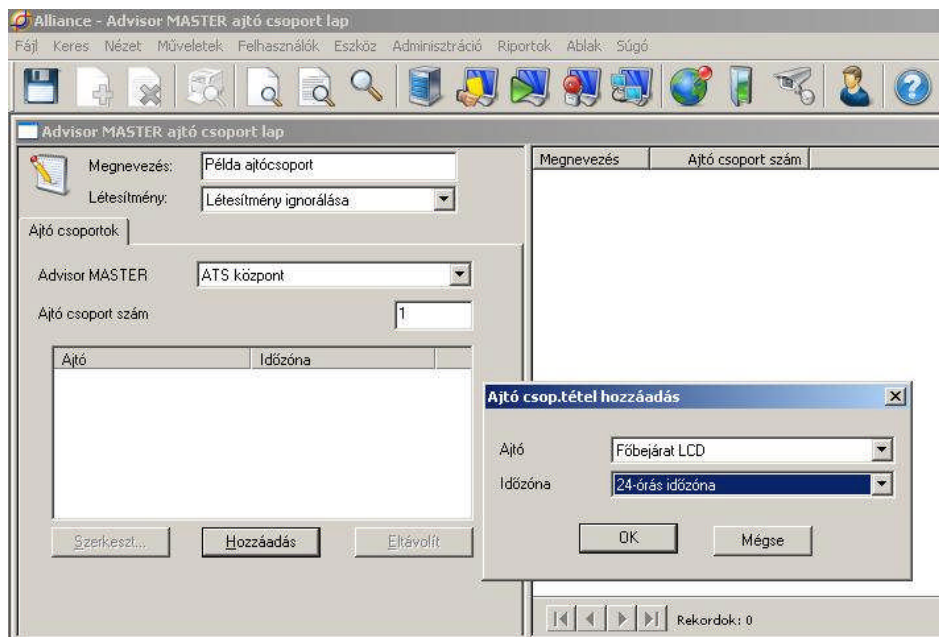
A Keresés ikonra kattintva láthatjuk a már létrehozott ajtó csoportokat, míg rögtön az “Adat létrehozás” ikonra kattintva létrehozhatunk egy újat. Kattintsunk az Adat létrehozás ikonra - rögtön látjuk, hogy aktiválódott a Mentés ikon – és adjuk meg az alábbi adatokat.

A **megnevezés** mezőben adjunk egyértelmű nevet az ajtó csoportnak.

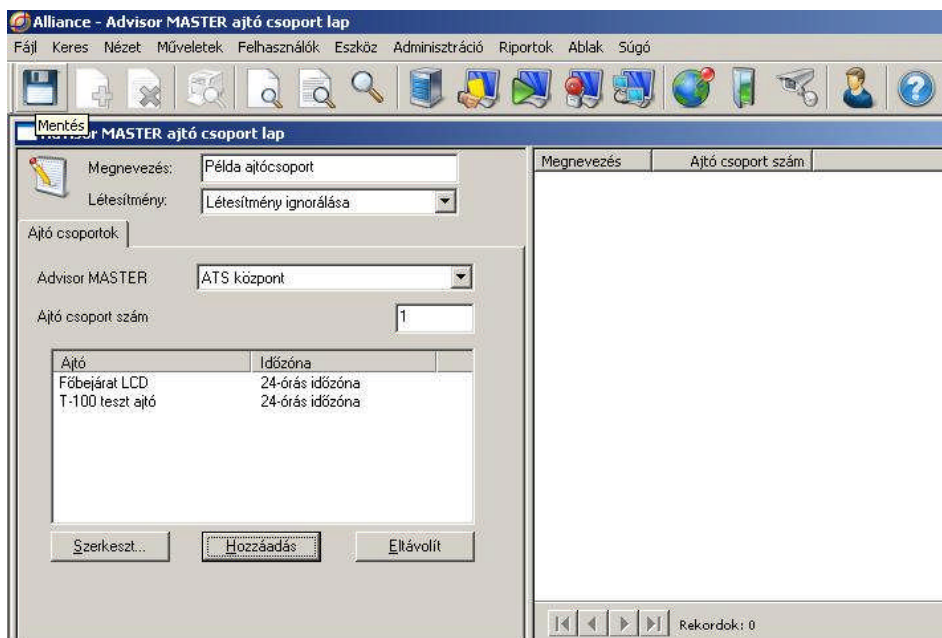
A **létesítmény** mezőben látható, hogy az ajtó csoportok esetében is lehetséges létesítményhez rendelni őket.

Az **Advisor MASTER** mezőben a legördülő menüből válasszuk ki az ATS központot, ahol az ajtó csoportunkat szeretnénk létrehozni.

Az **ajtó csoport számnál**, pedig rendeljünk hozzá egy számot az ajtó csoporthoz 1 és 128 között, ami még nem létezik az adott központon.

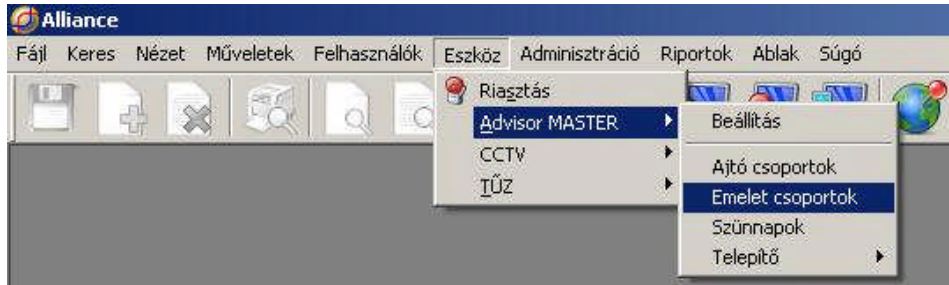


A Hozzáadás gombra kattintva megjelenik egy ablak, amiben legördülő menükben láthatjuk a rendszer ajtóit és a hozzájuk rendelhető időzónákat. Gyakorlatilag itt programozzuk be, hogy az adott ajtó csoport mely ajtókat és milyen időzónában nyithatja majd ki.



Végül a Mentés ikonra kattintva elmentjük az újonnan létrehozott ajtó csoportot.

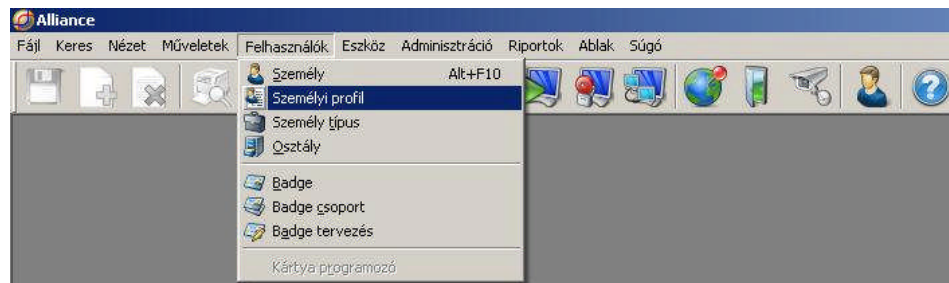
### Emelet csoport létrehozása:



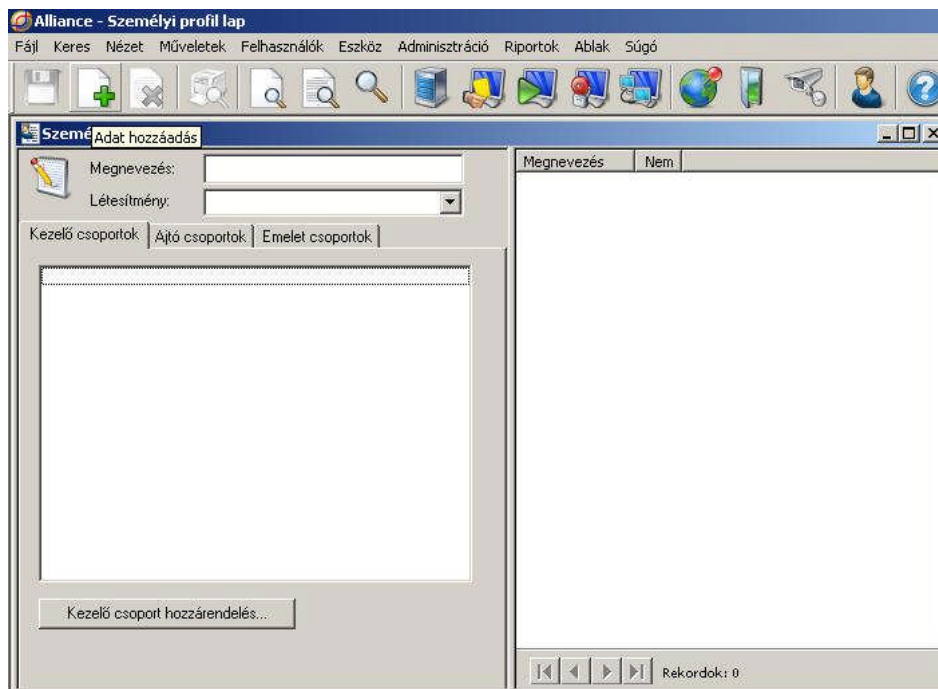
Ha vannak a rendszerünkben liftvezérlők, akkor az emelet csoportok konfigurálásához lépünk be az Eszköz/Advisor MASTER/Emelet csoportok menüpontba és ott az ajtó csoportok létrehozásával teljesen megegyező módon konfigurálhatjuk az emelet csoportokat.

Abban az esetben, ha már létrehoztuk a szükséges kezelő-, ajtó- és/vagy emelet csoportokat, akkor ezekből létrehozhatunk egy Személyi Profilt – egy személyhez rendelhető jogosultságot.

### **Jogosultság létrehozása**

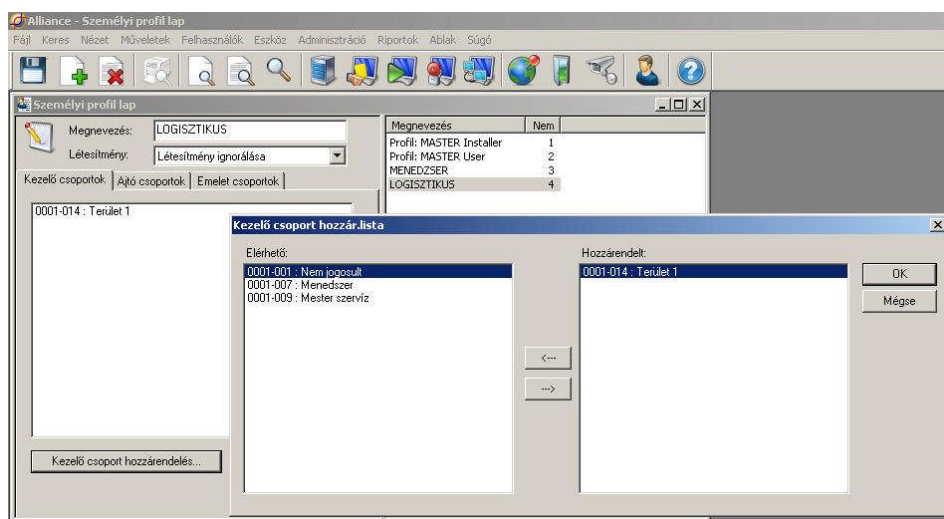


Lépünk be a Felhasználók/Személyi profil menüpontba.



A Keresés ikonra kattintva láthatjuk a már létrehozott személyi profilokat, míg az “Adat létrehozás” ikonra kattintva létrehozhatunk egy újat. Kattintsunk az Adat létrehozás ikonra - rögtön látjuk, hogy aktiválódott a Mentés ikon – és adjuk meg az alábbi adatokat.

A **megnevezés** mezőben adjunk egyértelmű nevet a jogosultságnak. Javasolt munkakör szerint kiosztani a jogosultságokat, így könnyebben nyomon követhető, hogy kinek mihez van joga.



Ezután pedig az egyes fülken lent található “Kezelő csoport hozzárendelés” vagy “Ajtó csoport hozzárendelés” vagy “Emelet csoport hozzárendelés” gombokat megnyomva a felugró ablakban a

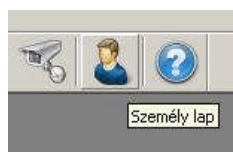
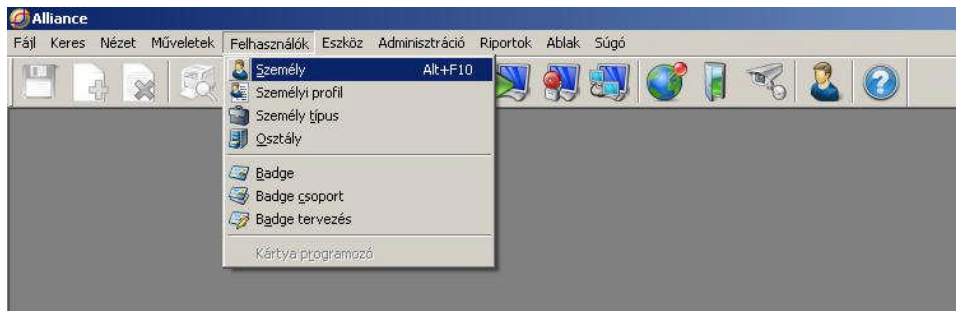
megfelelő csoportot kiválasztva és a jobbra nyílra kattintva definiáljuk, hogy az adott személyi profilhoz(jogosultsághoz) mely csoportok tartozzanak.

**MEGJEGYZÉS:** Ne feledjük, hogy egy ATS központról csak egy kezelő csoportot, egy ajtó csoportot és egy emelet csoportot rendelhetünk hozzá a személyi profilhoz. Ha pl. szeretnénk még egy ajtót hozzárendelni egy adott személyi profilhoz, akkor az ajtó csoportját kell módosítani.

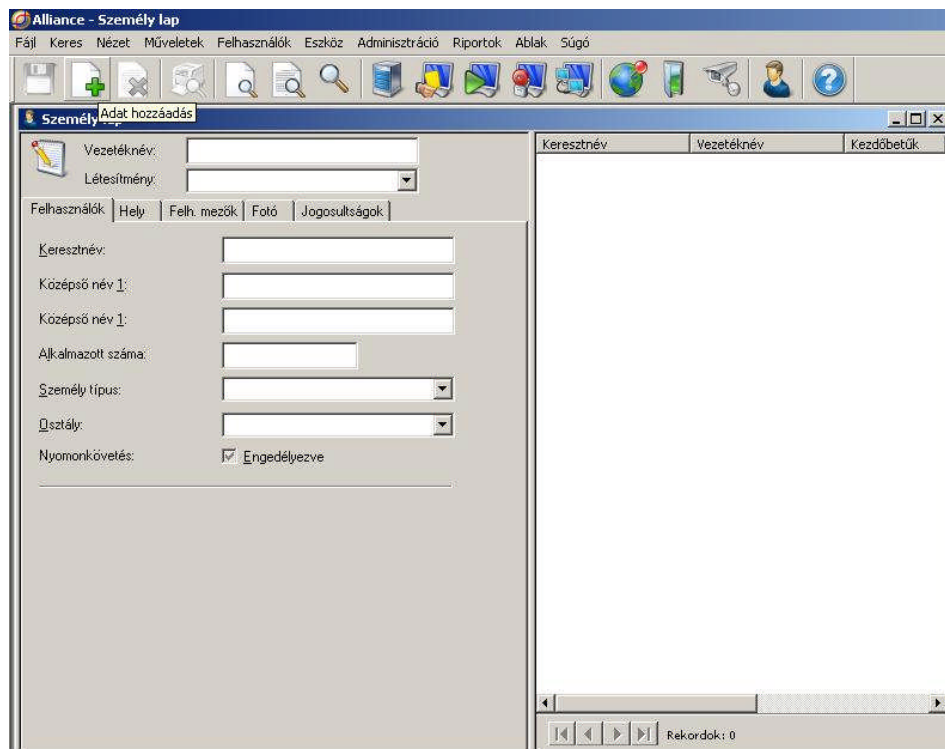
A megfelelő csoportok kiválasztása után a Mentés ikonra kattintva elmenthetjük az adott személyi profilt.

### Személy létrehozása

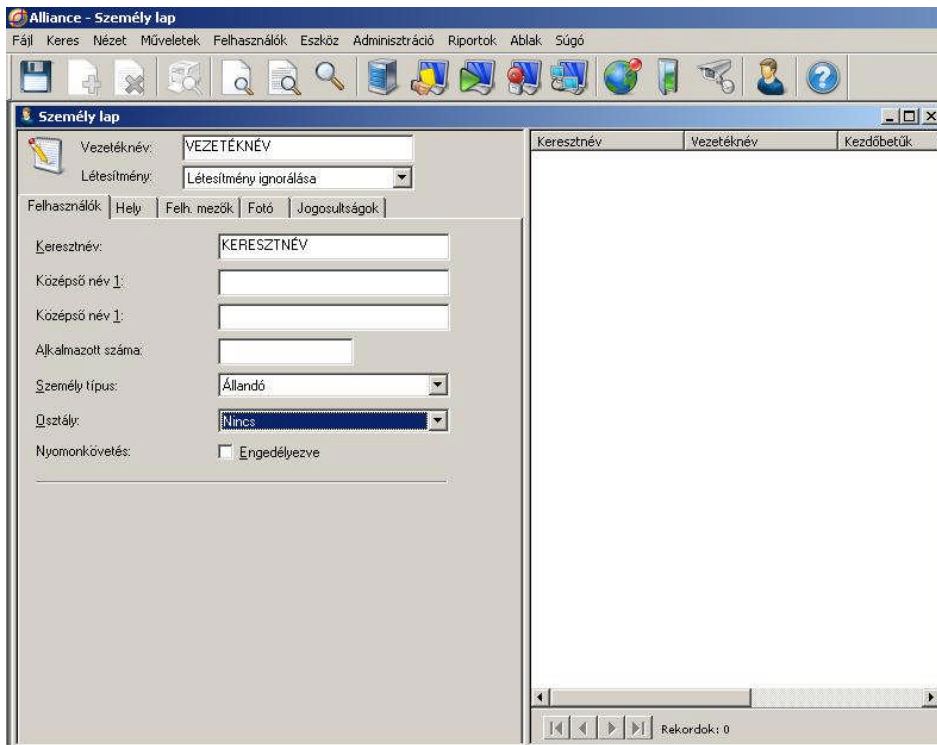
A **személy** létrehozásánál tulajdonképpen minden kívánt adatot megadhatunk a felhasználóról mielőtt badge-et rendelnénk hozzá. Fotót vagy aláírást csak a Képkezelő szoftver licenz birtokában leszünk képesek hozzáadni. Minél több adatot rögzítünk az adott személyről, annál részletesebb és árnyaltabb adatbázis építhető, később ezen adatok alapján tudjuk majd csoportosítani őket, aktivitásukat lekérdezni.



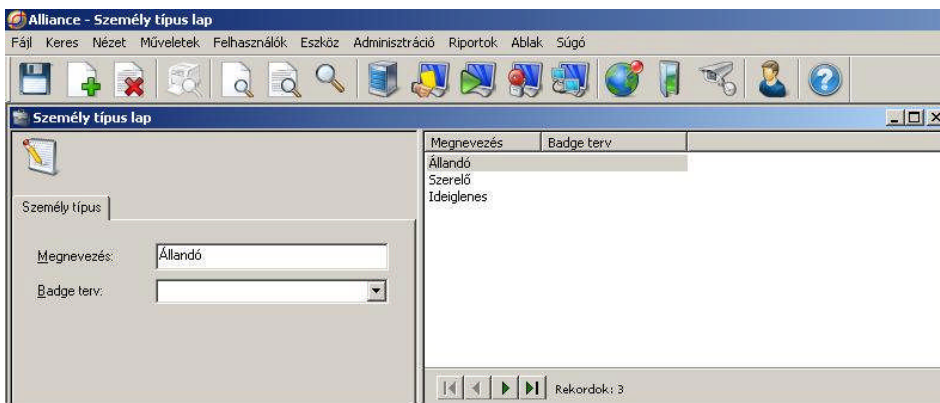
Nyissuk meg a személyi lapot a Felhasználók/Személy menüpontból vagy az eszköz soron található Személy lap ikonra kattintva.



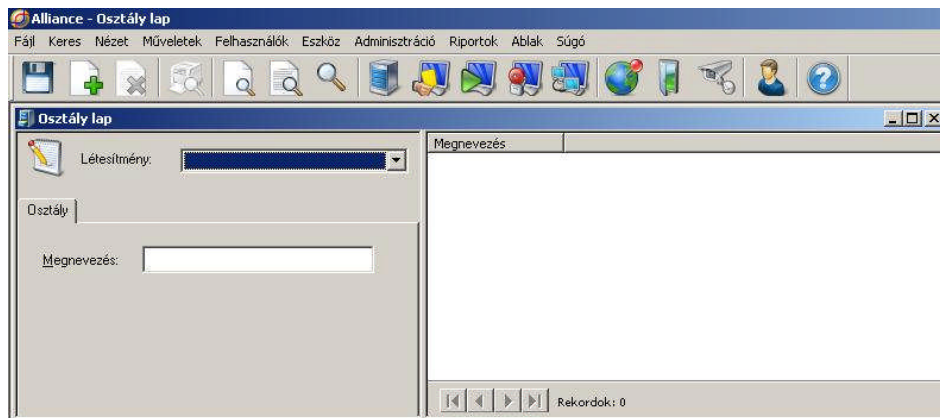
A Keresés ikonra kattintva láthatjuk a már létrehozott személyeket, míg az “Adat létrehozás” ikonra kattintva létrehozhatunk egy újat. Kattintsunk az Adat létrehozás ikonra - rögtön látjuk, hogy aktiválódott a Mentés ikon – így az adatok megadása után el is tudjuk majd menteni azokat.



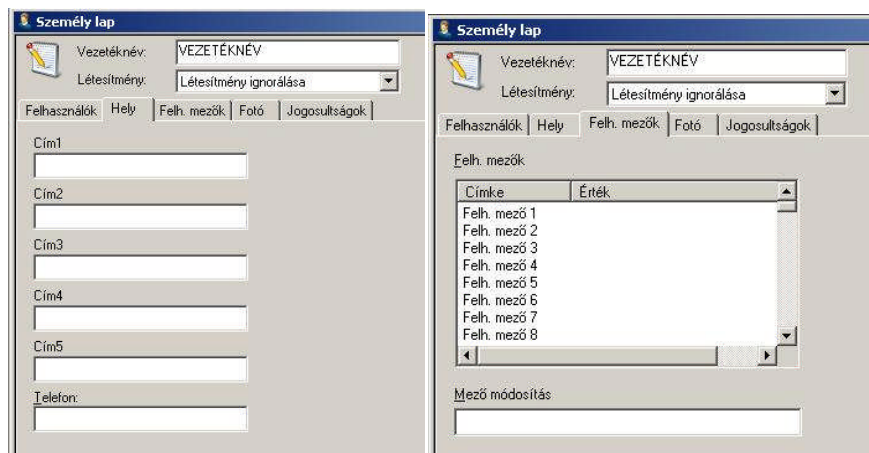
A **Felhasználók** fülön egyes adatokat értelemszerűen töltünk ki, a **személy típus** megadása kötelező. Telepítés után alpból három személy típus létezik az állandó, az ideiglenes és a szerelő. Létrehozhatunk egyedi személy típusokat is a Felhasználók/Személy típus ablakon keresztül, illetve ebben az ablakban személy típusonként akár különböző badge terveket rendelhetünk az adott személyekhez. Ilyen módon számukra egyedi kártya nyomtatható.



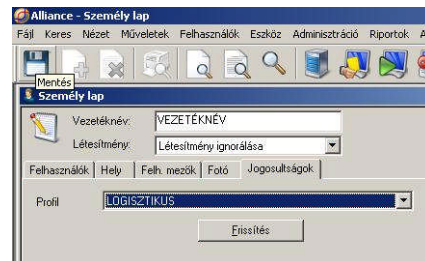
Az **osztály** mezőben a legördülő menüből válasszuk ki a személy melyik osztályon dolgozik. Ez később riport készítéseknél még jól jöhet, mint szűrési feltétel. Az egyes osztályok is létesítményhez rendelhetők.



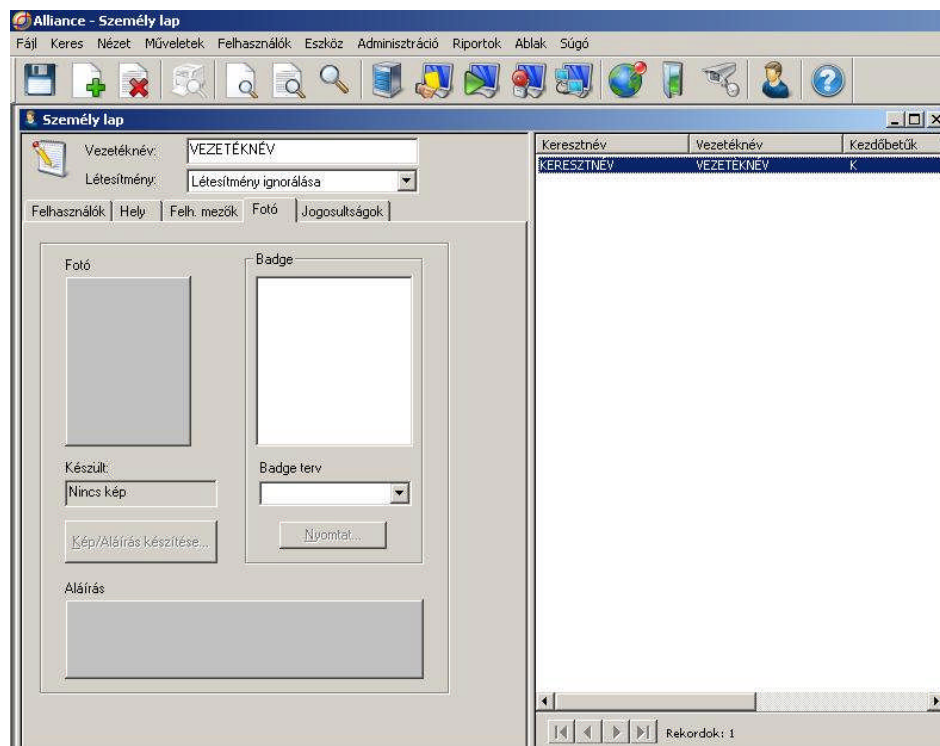
A **nyomonkövetés** engedélyezésével az illető könnyedén nyomonkövethető a Badge felügyeleti lapon, illetve négyajtós bővítők esetén külön vezérléseket is indíthatunk az ilyen személy olvastatása esetén. Eseti opció, kezdeti programozáskor nyugodtan figyelmen kívül hagyhatjuk.



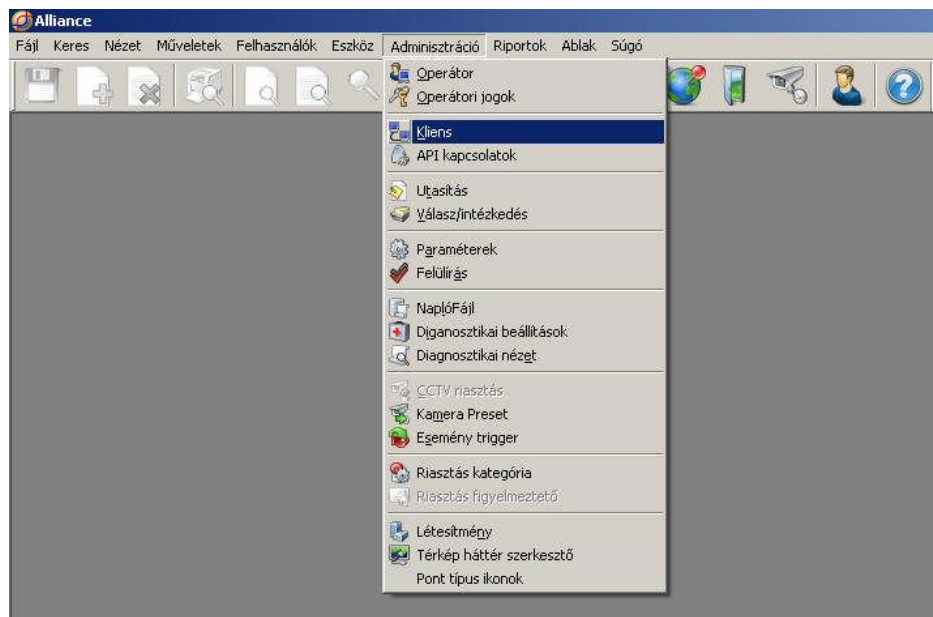
A személy lap **Hely** és **Felhasználói mezők** fülén megadhatunk több kiegészítő adatot, ezeknek ismét akkor lehet jelentősége, ha nagy felhasználói adatbázist kezelünk és szükség lehet egy-egy szűrésnél kiegészítő adatokra.



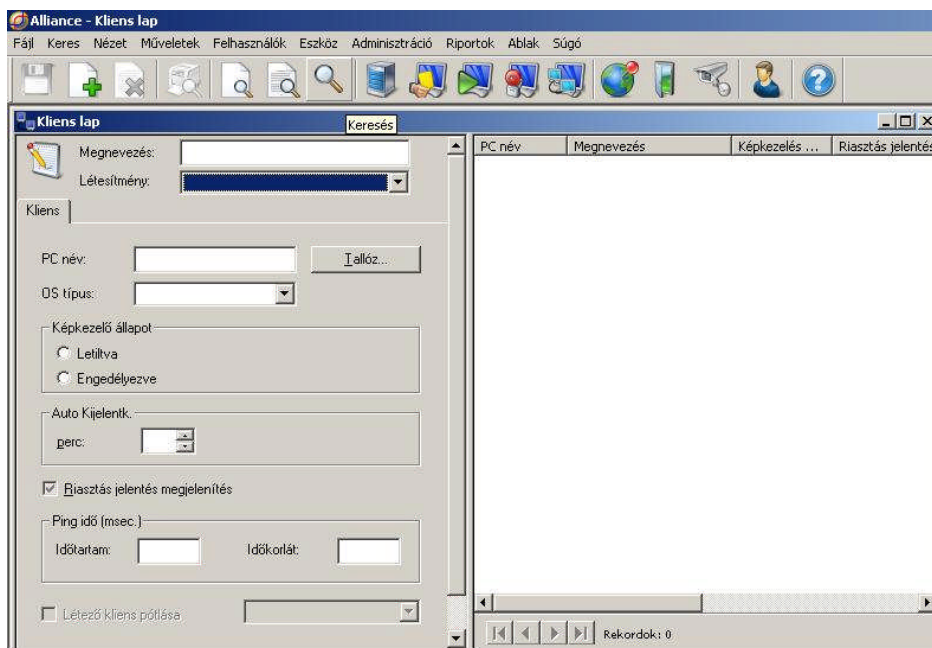
A személy lap **Jogosultságok** fülén állítható a legördülő menüből kiválasztva, hogy az adott személy milyen személyi profillal bír, vagyis milyen kezelő-, ajtó- és emelet csoportok tartoznak hozzá az egyes ATS központokon. Ha az ablak megnyitása után hoznánk létre egy új személyi profilt, akkor a Frissítés gombra kell kattintsunk, hogy megjelenjen a legördülő listában.



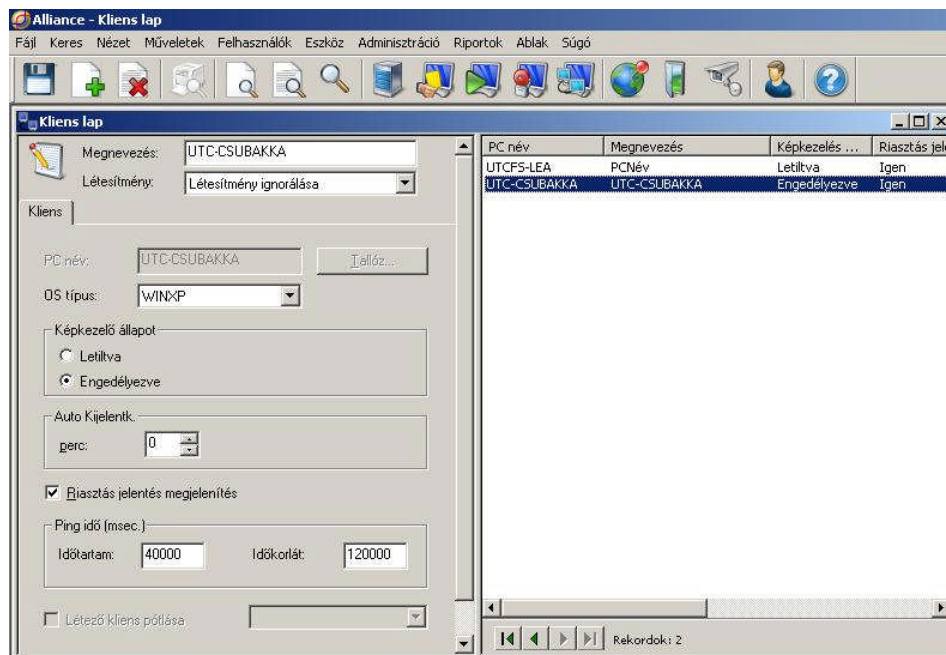
A személyi lapon a Fotó fülön tudunk képet, aláírási képet, badge tervet hozzárendelni az adott személyhez, bár képet és aláírási képet csakis akkor, ha rendelkezünk Képfeldolgozás(Imaging) licensszel.



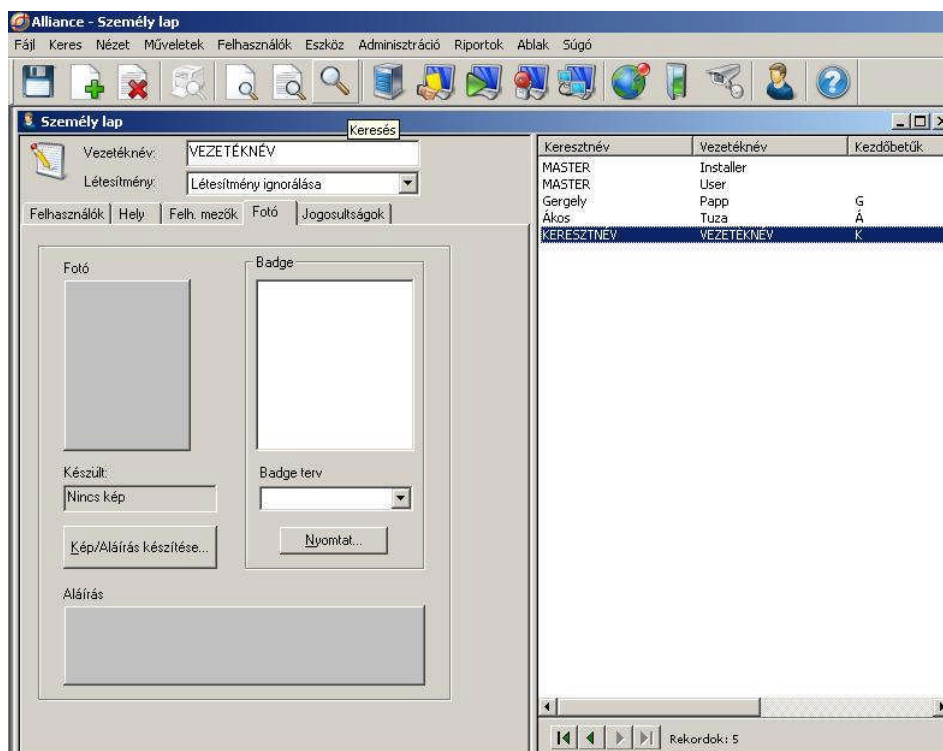
Egy rendszeren belül több kliens PC is lehet, kliensenként kell engedélyezni a Képkészítő licenst. Ezt az Adminisztráció/Kliens menüpont alatt tudjuk megtenni.



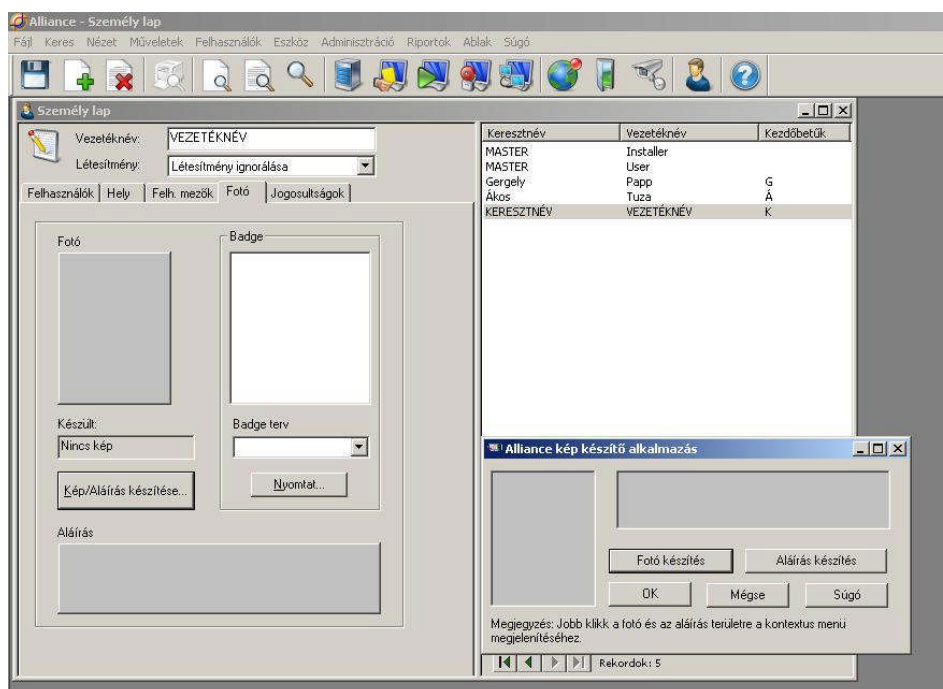
A kliens lapon kattintsunk a Keresésre, ha nem kívánunk létesítményre szűrni.



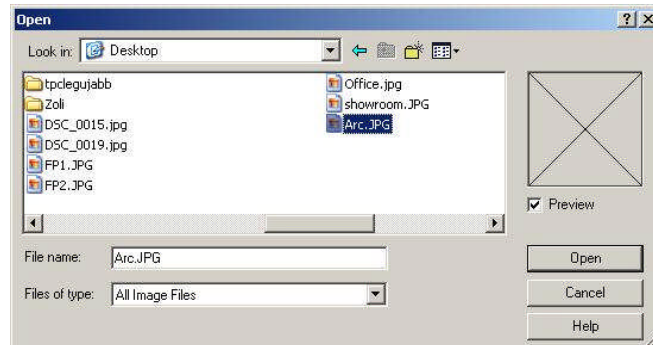
Láthatjuk, hogy a mostani példánkban két kliens létezik, az egyik az UTCFS-LEA szerveren, a másik az UTC-CSUBAKKA kliens gépen. Viszont csak egy Képkészítő licenszünk van, így ha szeretném azt a UTC-CSUBAKKA gépen használni, akkor minden más kliensen le kell tiltanom a Képkészítő állapotot és a UTC-CSUBAKKÁN engedélyeznem kell. Természetesen ahhoz, hogy ténylegesen használni tudjam a Képkészítőt egy Alliance kliens gépen, ahhoz előzetesen telepíteni kell a Képkészítő kiegészítő csomagot, esetünkben ez a telepítés már megtörtént. Minden kliens változtatás után mentek, majd bezárom az ablakot.



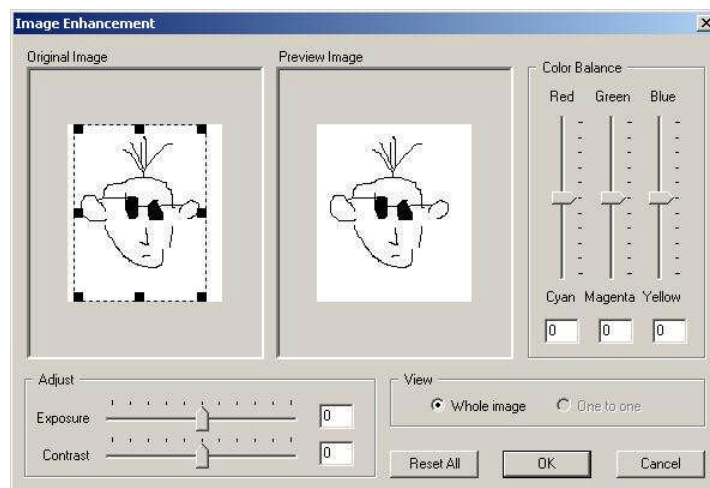
Amint újraindítottuk az Alliance-et, a Személy lap/Fotó fülön a „Kép/Aláírás készítése...” gomb aktívvá vált, így már lehetséges kép és aláírás készítése. Nyomjuk meg ezt a gombot.



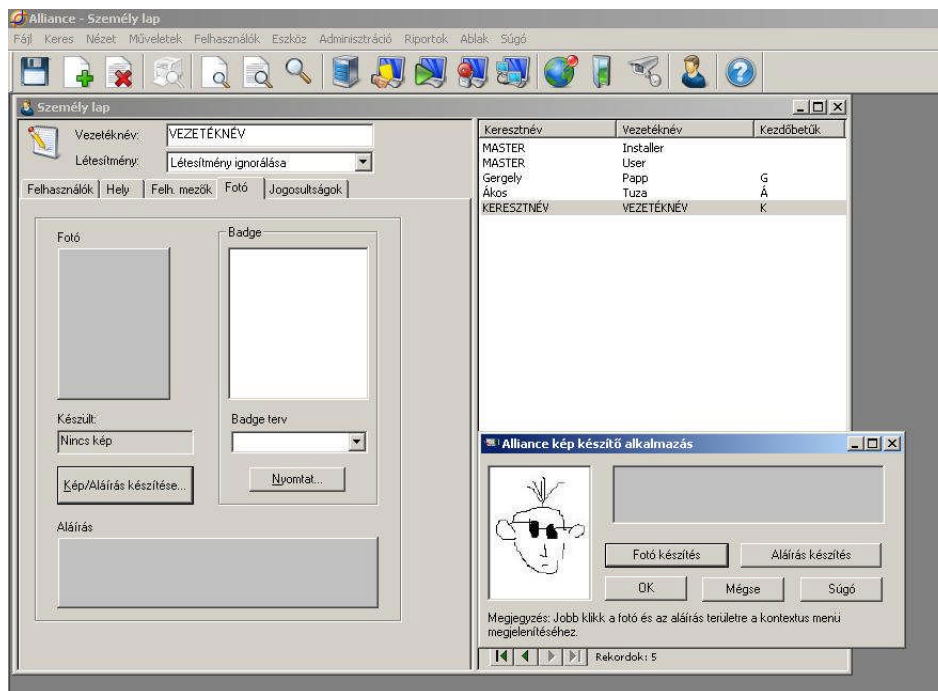
Majd nyomjuk meg a Fotó készítés gombot.



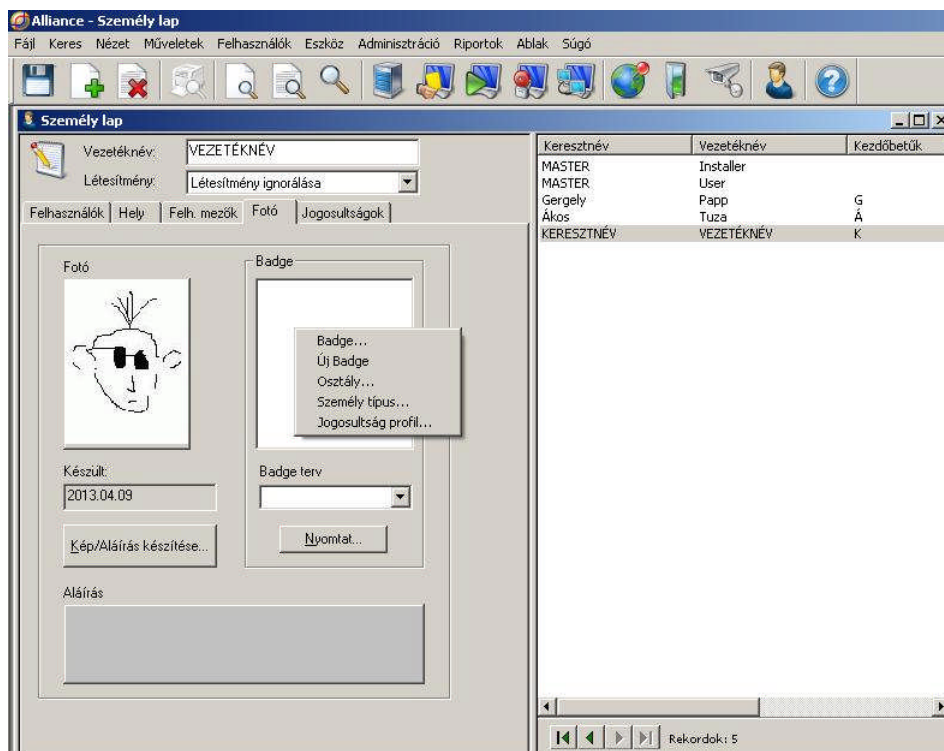
Tallózzuk ki a személyhez tartozó igazolványképet, jelöljük ki, majd nyomjuk meg az „Open” gombot.



A következő ablakban pontosan középre igazíthatjuk az arcképet, állíthatunk rajta színegyensúlyt, kontrasztot és megvilágítást. Ha ezt befejeztük nyomjunk „OK”-ét.



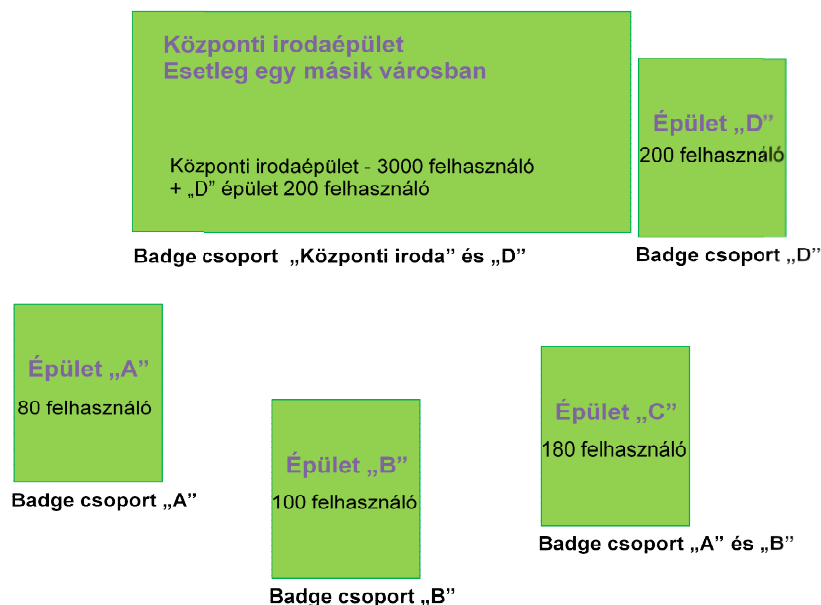
Ismét visszatértünk a kiinduló kép és aláírás beviteli részhez, ha szeretnénk itt még aláírás képet is rendelhetünk a személyhez, ha elegendő az igazolványkép, akkor nyomjunk OK-ét.



Láthatjuk, hogy az Alliance beemelte a személy igazolványképét az adatbázisba. Az üres Badge mezőben láthatjuk a jelenleg a személyhez rendelt badge-eket, amennyiben még nem volna badge hozzárendelve, akkor jobb egér gombbal kattintva (a személy lap füleinek bármelyik részére) választhatunk számos ide vonatkozó menüpont közül. Így hozzárendelhetünk egy már létező badge-et, vagy létrehozhatunk egy teljesen újat, illetve egyéb tulajdonságait tudjuk módosítani.

### **Badge csoport létrehozása (NEM kötelező)**

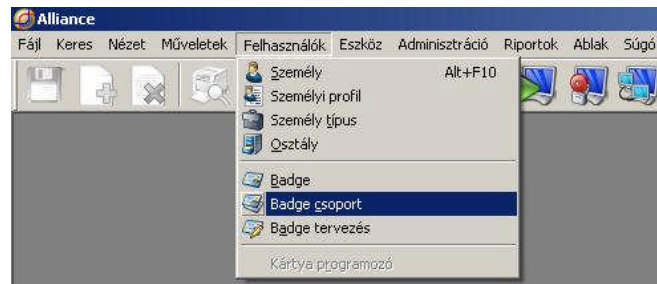
A badge csoport segít az Alliance szoftvernek abban, hogy tudja mely badge-eket kell letölteni melyik ATS központra. A badge csoportok a Központ vezérlés lap/Szerkesztés/Badge csoportok menüponthoz kapcsolódnak. Minden újonnan létrehozott központ alapbeállítás szerint rendelkezni fog az alap badge csoportokkal.



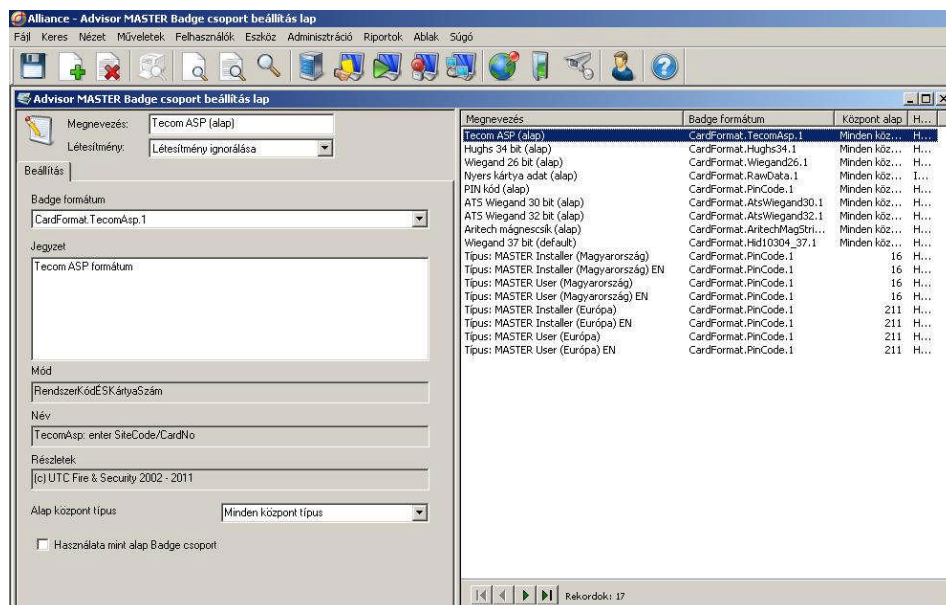
Új badge csoportot létrehozni akkor szükséges, ha egy több központos rendszerben egy vagy több központ viszonylag kevés elérhető felhasználóval bír. Hogyha a rendszerben minden központ ugyanazt a badge group-ot használná, akkor a kevesebb felhasználóval rendelkező kisebb központ hamar megtelne.

A megoldás az, hogy létrehozunk egy újabb badge csoportot azon felhasználók számára, akik a kis központot használják, ezt a badge csoportot hozzárendeljük a kis központhoz és minden más – nem szükséges - badge csoportot letörlünk róla.

Badge csoport létrehozásához lépünk be a Felhasználók/Badge csoport menüpontba.



A Keresés ikonra kattintva láthatjuk a már meglévő Badge csoportokat.

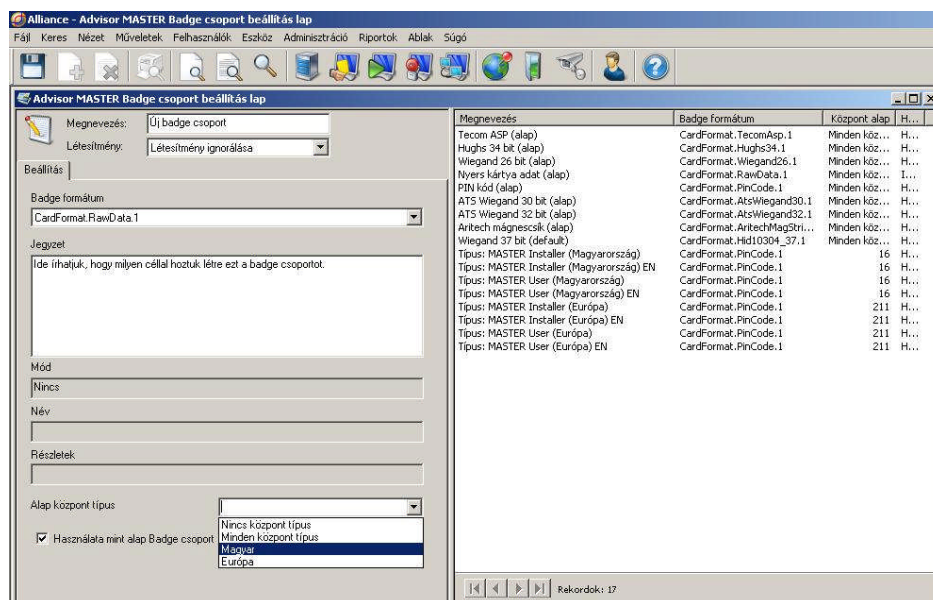


Az Adat hozzáadás ikonra kattintva pedig létrehozhatunk egy új badge csoportot. A megnevezésben adjunk nevet neki, létesítményhez is rendelhetjük, majd válasszuk ki a badge formátumát. A badge formátum az alábbi kártyaformátumok közül lehet valamelyik:

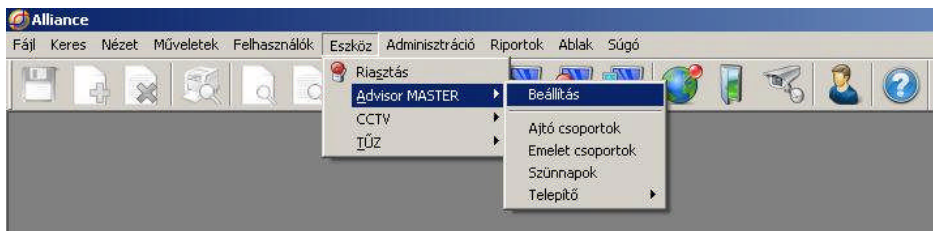
|                  |                                                                   |
|------------------|-------------------------------------------------------------------|
| <b>TecomASP</b>  | <b>ATS HITAG II programozott kártyák esetén</b>                   |
| Hughes34         | 34-bites Hughes formátumú kártyák esetén                          |
| AtsWiegand30     | 30-bites wiegand formátumú kártyák esetén                         |
| Wiegand26        | 26-bites wiegand formátumú kártyák esetén                         |
| AtsWiegand32     | 32-bites wiegand formátumú kártyák esetén                         |
| Hid10304_37      | 37-bites wiegand formátumú kártyák esetén                         |
| AritechMagStripe | Aritech mágneskód olvasók esetén                                  |
| HidC1000         | HID C1000 formátumú kártyák esetén                                |
| <b>RawData</b>   | <b>IUM-módban nyers kártya adat esetén, vagy nem programozott</b> |
|                  | <b>ATS HITAG II</b>                                               |
| <b>PinCode</b>   | <b>Csak PIN kód használata esetén</b>                             |

A leggyakrabban használt kártyaformátumok vastagon vannak kiemelve. Különösen az utolsó két formátum az, ami leginkább használt, hiszen az IUM-módba kapcsolt központok bármilyen wiegand formátumot képesek nyers kártyaadatként továbbítani, ilyen módon a RawData egyfajta univerzálisan használható formátum. A PIN kód, pedig nyilvánvalóan csak behatolásjelző rendszereknél gyakran használatos. A példánkban is az új badge csoport formátumaként nyers kártya adatot (RawData) adtunk meg. A badge létrehozásakor, ehhez a kártya formátumhoz tudunk még PIN kódot is rendelni. A jegyzet ablakban tudunk egyéb megjegyzést fűzni az adott csoporthoz, illetve az ablak alján kiválaszthatjuk, hogy mely alap központ esetén legyen alap Badge csoportként használva ez a csoport. Ez azt jelenti, hogy így egy újonnan létrehozott magyar nyelvű ATS központ esetén a rendszer automatikusan hozzá fogja rendelni ezt a csoportot is.

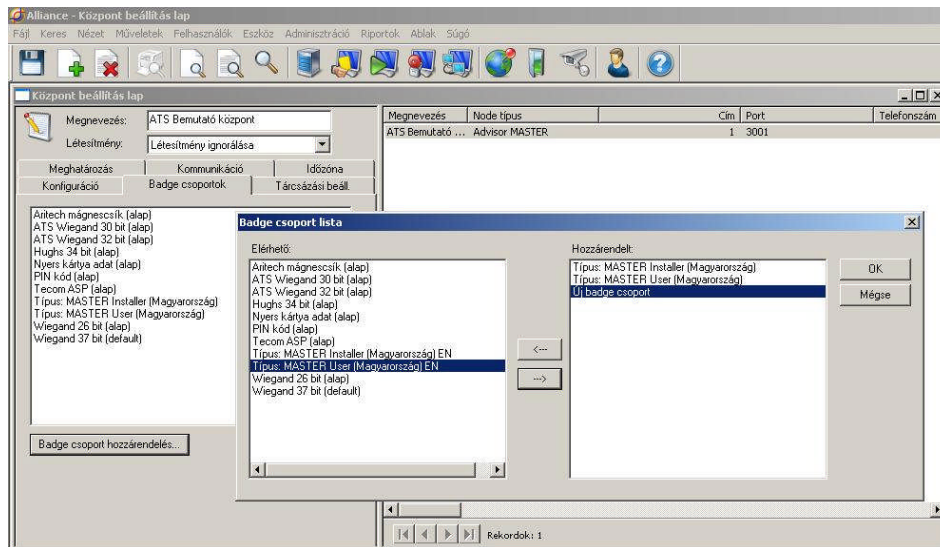
Ha minden adatot megadtunk kattintsunk a Mentés ikonra.



Ahhoz, hogy létrehozott badge csoportot hozzárendelhessük egy adott ATS központhoz lépünk be az Eszköz/Advisor MASTER/Beállítások menüpontba.

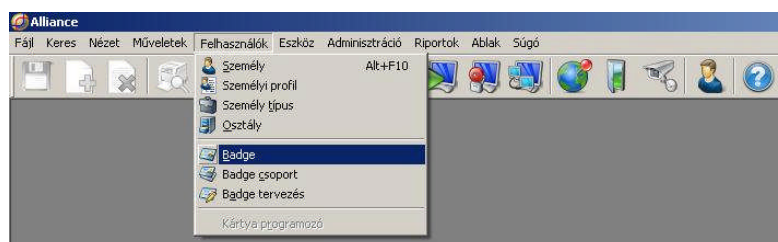


Itt a Keresés ikonra kattintva kiválasztjuk azt a központot, amihez szeretnénk új badge csoportot rendelni, majd megnyitjuk a Badge csoportok fület, ahol az ablak lenti részén megnyomjuk a „Badge csoport hozzárendelés...” gombot. A megjelenő Badge csoport lista ablakban bal oldalon az „Elérhető” badge csoportok közül kijelölve az Új badge csoportot a középen található jobbra nyílat megnyomva áttesszük a „Hozzárendelt” badge csoportok közé, ahonnan a balra nyíl segítségével kivehetjük a nemkívánatos csoportokat. A Mentés ikonra kattintva elmenthetjük az új állapotot.

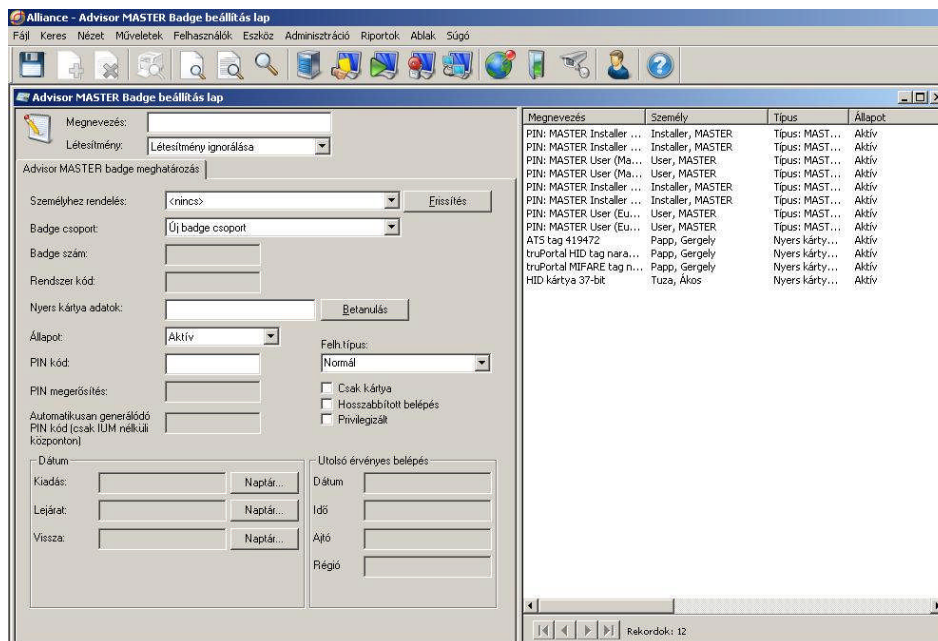


## Badge létrehozása

Badge létrehozásához lépünk be a Felhasználók/Badge menüpontba:



Itt a Keresés ikonra kattintva láthatjuk a már létrehozott badge-eket, az Adat hozzáadás ikonra kattintva pedig újat hozhatunk létre, nyomjuk meg tehát ezt a gombot, így az alábbi ablakot kell lássuk:



| Megnevezés                | Személy           | Típus           | Állapot |
|---------------------------|-------------------|-----------------|---------|
| PIN: MASTER Installer ... | Installer, MASTER | Típus: MAST...  | Aktív   |
| PIN: MASTER Installer ... | Installer, MASTER | Típus: MAST...  | Aktív   |
| PIN: MASTER User (Ma...   | User, MASTER      | Típus: MAST...  | Aktív   |
| PIN: MASTER User (Ma...   | User, MASTER      | Típus: MAST...  | Aktív   |
| PIN: MASTER Installer ... | Installer, MASTER | Típus: MAST...  | Aktív   |
| PIN: MASTER Installer ... | Installer, MASTER | Típus: MAST...  | Aktív   |
| PIN: MASTER User (Eu...   | User, MASTER      | Típus: MAST...  | Aktív   |
| PIN: MASTER User (Eu...   | User, MASTER      | Típus: MAST...  | Aktív   |
| ATS tag 419472            | Papp, Gergely     | Nyers kártya... | Aktív   |
| truPortal HID tag nára... | Papp, Gergely     | Nyers kártya... | Aktív   |
| HID kártya 37-bit         | Tuza, Ákos        | Nyers kártya... | Aktív   |

A **megnevezés** mezőben egyedi nevet adhatunk a badgenek, a **létesítmény** mezőben pedig létesítményhez rendelhetjük.

A **személyhez rendelés** mezőben kiválaszthatjuk azt a személyt, akit ez a badge fog azonosítani, ha a badge még nem volna senkihez sem rendelve, akkor itt azt kell lássuk, hogy „<nincs>”. Ha egy éppen most létrehozott személy még nem szerepelne a legördülő listában, akkor a „Frissítés” gombra kattintva orvosolhatjuk ezt.

A **badge csoport** mezőben kiválaszthatjuk, hogy ez a badge melyik csoporthoz tartozzon, ezzel azt, hogy melyik ATS központokra legyen letöltve.

A **badge szám** mezőben ATS programozott kártyák esetén a felhasználó számát kell megadni, ezt nem programozott kártyák esetén NE töltsük ki!

A **rendszer kód** mezőben ATS programozott kártyák esetén a rendszer kódot adjuk meg, nem programozott kártyák esetén NE töltsük ki!

A **nyers kártya adatok** nem programozott kártyák esetén használatosak, amennyiben előre konfigurált betanító olvasók is vannak a rendszerben (Adminisztráció/Paraméterek/Badge betanítás/Badge betanító eszközök), akkor a „Betanulás” gombra kattintva kiválasztható a nyers kártya adat az adott olvasón való olvastatás után.

Másik megoldás lehet, hogy a Badge felügyelet lapról az új (ismeretlen) kártya olvastatása után jobb klikkel a „Nyers kártya adat másolása vágólappra” opciót választjuk és aztán visszatérve a badge lapra ismét jobb klikkel bemásoljuk a nyers kártya adatokat.

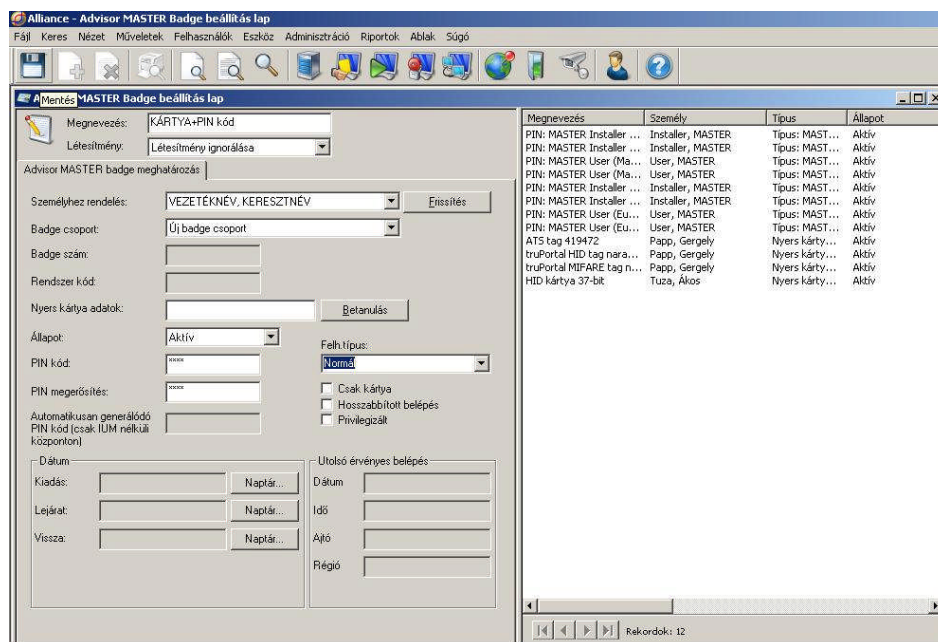
Az **állapot** mezőben a badge aktuális állapotát láthatjuk, értelemszerűen létrehozáskor ez **Aktív**, ami azt jelenti, hogy hozzá van rendelve egy személyhez és lehet használni belépéshez/riasztó kezeléshez.

A **Lejárt** állapot azt jelenti, hogy a badge nem veszett el, de le lett tiltva valamilyen oknál fogva és nem lehet belépéshez/riasztó kezeléshez használni. Pl. előfordulhat, hogy egy badge csak egy adott ideig érvényes, ha az letelik, akkor „lejárt” állapotba kerül.

Az **Elveszett** állapot, azt jelenti, hogy a badge elveszteként lett jelentve és nem használható belépéshez/riasztó kezeléshez.

Az **Érvénytelen** állapot pedig az, hogy a badge éppen nincsen személyhez rendelve és nem használható. Ilyen lehet például egy előre létrehozott kártya, amit majd egyszer a jövőben fogunk személyhez rendelni.

Csak érvénytelen badge törölhető. De a **badge-ek törlése nem ajánlott**, mert utólag lehet, hogy ez nehezségeket okoz. Pl. programozott kártyák esetén, ha letörlünk egy kártyát, ami elveszett, akkor idővel újra írhatjuk ugyanazt a kártyát, ezzel duplikáljuk az elveszett kártyát és ha valaki megtalálja a régit, akkor ugyanolyan jogokkal használhatja, mint az újat, ez pedig komoly biztonsági rést jelent. A legegyszerűbb ökölszabály tehát, hogy biztonsági okokból badge-et sose töröljünk az adatbázisból.



**Adviser MASTER badge meghatározás**

Megnevezés: KÁRTYA+PIN kód  
 Létesítmény: Létesítmény ignorálása

Adviser MASTER badge meghatározás:

Személyhez rendelés: VEZETÉKNÉV, KERESZTNÉV

Badge csoport: Új badge csoport

Badge szám:

Rendszer kód:

Nyers kártya adatok:

Állapot: Aktív

PIN kód:

PIN megerősítés:

Automatikusan generálódó PIN kód (csak IUM nélküli központok):

Felh. típus:

☐ Csak kártya  
☐ Hosszabbított belépés  
☐ Privilegiált

Dátum:

Utolsó érvényes belépés:

Kiadás:

Lejárat:

Vissza:

Idő:

Ajtó:

Régió:

| Megnevezés                | Személy           | Típus           | Állapot |
|---------------------------|-------------------|-----------------|---------|
| PIN: MASTER Installer ... | Installer, MASTER | Típus: MAST...  | Aktív   |
| PIN: MASTER Installer ... | Installer, MASTER | Típus: MAST...  | Aktív   |
| PIN: MASTER User (Ma...   | User, MASTER      | Típus: MAST...  | Aktív   |
| PIN: MASTER User (Ma...   | User, MASTER      | Típus: MAST...  | Aktív   |
| PIN: MASTER Installer ... | Installer, MASTER | Típus: MAST...  | Aktív   |
| PIN: MASTER Installer ... | Installer, MASTER | Típus: MAST...  | Aktív   |
| PIN: MASTER User (Eu...   | User, MASTER      | Típus: MAST...  | Aktív   |
| PIN: MASTER User (Eu...   | User, MASTER      | Típus: MAST...  | Aktív   |
| ATS tag 419472            | Papp, Gergely     | Nyers kártya... | Aktív   |
| truPortal HID tag nara... | Papp, Gergely     | Nyers kártya... | Aktív   |
| truPortal MIFARE tag n... | Papp, Gergely     | Nyers kártya... | Aktív   |
| HID kártya 37-bit         | Tuzsa, Ákos       | Nyers kártya... | Aktív   |

Rekordok: 12

A **PIN kód** mezőben adjuk meg a badge-hez tartozó PIN kódot, ha van ilyen, ha nincs, akkor pipáljuk ki a „Csak kártya” opciót. A PIN kódot a PIN megerősítés mezőben újra meg kell adni.

Az **Automatikusan generálódó PIN kód** opció csak bizonyos firmware verziójú központokon működik, több felhasználó együttes megadása esetén érdemes használni.

A **Dátum** mezőben a **Kiadás** mellett található „Naptár...” gombra kattintva kiválaszthatjuk azt a jövőbeli dátumot, amittől ez a badge érvényes állapotú lesz és letöltésre kerül a (badge csoportnak megfelelő) ATS

központokra. Mentés előtt győződjünk meg arról, hogy a badge állapota érvénytelen, hiszen csak így lesz érvénytelen a kiadási dátumig.

A **Lejárat** mellett található „Naptár...” gombra kattintva állíthatjuk be azt a jövőbeli dátumot, amikor az Alliance a badge állapotát érvénytelenre változtatja és letölti a megfelelő ATS központokra.

A **Vissza** dátum pusztán egy többletinformációs mező, melyben rögzíthetjük, hogy egy felhasználó mikor adta vissza az azonosítóját. Ennek a dátumnak a megadása nem indít semmilyen letöltést az ATS központ felé.

Az **Utolsó érvényes belépés** mezőben látható az adott badge utolsó érvényes használata. Ez az adat jól használható a badge aktivitásának mutatójaként. Gyakran használják pl. két hétnél régebben nem használt badge-ek kiszűrésére, ami felhívhatja a figyelmet a rendszer esetleges biztonsági réseire.

A **Felhasználó típus** mezőben az alábbi lehetőségek közül választhatunk:

- **Normál** – normál működésű felhasználó.
- **Kettős felügyelet** – négyajtós bővítő esetén használható opció, mely szerint két kettős felügyelet típusú felhasználó szükséges egy érvényes belépéshez és/vagy riasztó kezeléshez.
- **Őr** – négyajtós bővítő esetén használható opció, biztonsági őrhöz rendelhetjük. Ez a kártya csak vendég típusú kártyával együtt képes érvényes kártya használatra, önmagában nem működőképes, kísérő kártyaként is ismert.
- **Vendég** – négyajtós bővítő esetén használható opció, vendég felhasználókhöz rendelhetjük, csak az őr típusú kártyával együtt képes érvényes kártya használatra, önmagában nem működőképes.
- **Nagy biztonságú felhasználó** – négyajtós bővítő esetén használható opció, előre definiált nagy biztonságú régiók esetén, csak akkor léphetnek be normál felhasználók az adott régióba, ha megfelelő számú nagy biztonságú felhasználó tartózkodik már a régióban. Ezzel az opcióval jelölhetünk ki egy felhasználót nagy biztonságú felhasználóvá.

A **Csak kártya** opció esetén a badge-hez tartozó PIN kód érvénytelenné válik, ha nincs ilyen, akkor nem is lehet hozzáadni, amíg az opció aktív.

A **Hosszabbított belépés** opció négyajtós bővítő esetén használható, az így jelölt felhasználók számára hosszabb idő áll rendelkezésre az ajtón való áthaladásra. Mozgásukban korlátozott felhasználók számára javasolt.

A **Privilegizált** opció segítségével az adott azonosító képes felülmúlni az anti-passback szigorításokat.