

Biztonsági funkciók

Rendszerünkben a biztonsági megoldások két szintje elérhető. A minden előfizetéshez automatikusan hozzátartozó **alapszintű funkciók**, valamint az előfizetésekhez külön aktiválható **emelt szintű funkciók**.

Az alapszint biztosítja:

- Napjaink standard szintű biztonsági követelményeit.
- A rosszindulatú kísérletek elleni védelmet.
- A biztonsági események nyomomonkövethetőségét.
- A home office és távoli munkavégzés kockázatának csökkentését.
- A tudatosabb, szabályozott, biztonságosabb felhasználói magatartást.
- A beépített automatizmusokat a biztonsági munkatársak feladatának könnyítésére.

Az emelt szint ezek mellett lehetővé teszi:

- Hogy minden legyen személyre szabható és az egyedi vállalati igényekhez állítható legyen.
- Hogy megkülönböztethetők legyenek a különböző szerepköröknél alkalmazott biztonsági beállítások.
- Hogy a biztonsági beállítások az ágazati szabványokhoz, rendeletekhez legyenek igazíthatók.
- Hogy a manapság kiemelten fontos kétfaktoros hitelesítés elérhető legyen az előfizetőnek.

A két szinten elérhető megoldásokat, funkciókra lebontva mutatja be az alábbi táblázat. Az emeltszintű funkciók paramétereit a szolgáltatás igénybevétele esetén nem az előfizető állítja be, hanem saját rendszerünkben kollégáink határozzák meg a kért értékeket.

Funkciók	Alapszintű megoldások	Emeltszintű megoldások
Jelszóparaméterek	• A minimum hossz 8 karakter • Kötelező kis és nagybetű, szám használta • Az utolsó megadott jelszó nem használható	• Személyre szabható a jelszó hossza és komplexitása (pl. kötelező speciális karakter) • Beállítható, hány korábbi jelszó nem használható • Beállítható minimum és maximum érvényesség
Jelszócsere	• Minden jelszóváltásnál kötelező az előző jelszó megadása	• Minimum érvényesség esetén a felhasználó nem cserélhet a megadott számú nap előtt • Maximum érvényesség esetén a felhasználó a megadott számú nap után köteles váltani
Státusz kezelés	• Egy órán belül öt sikertelen belépési kísérlet blokkolja a felhasználót. • A blokkolás 30 perc után automatikusan feloldódik • A felhasználó csak a felületet nem éri el, mellékei aktívak maradnak	• Személyre szabható a sikertelen kísérletek száma és a blokkolás időtartama • Az automatikus feloldás kapcsolható

Funkciók	Alapszintű megoldások	Emeltszintű megoldások
Felhasználó státuszváltás	· A felhasználó az aktív és a blokkolt státusz mellett tiltott státuszba is kerülhet · A tiltott státusz meghatározott napnyi inaktivitás után automatikusan életbe lép. · Az adminisztrátorok manuálisan letilthatnak és aktiválhatnak felhasználókat, a blokkolt felhasználókat pedig maguk is aktiválhatják vagy tilthatják.	
Felhasználói aktivitás megjelenítése	· Az adminisztrátorok láthatják a felhasználó minden aktivitási előzményét a jelszóváltásoktól a sikeres vagy sikertelen belépési kísérleteken át a blokkolásokig. · A felhasználók maguk is látják az belépés előtti utolsó aktivitásukat	
Munkamenet kezelés	· A felhasználói munkamenet maximum 168 óra, ezt követően újra be kell jelentkezni. · Az inaktív felhasználókat 30 perc után automatikusan kilépteti a rendszer	· A munkamenet és az inaktivitás hossza személyre szabható (Kivéve a Call Center modul esetén: az operátori felület megnyitása a beállításokatt felülírva tartja meg a munkamenet maximum hosszát. - Id. CC MODUL)
Captcha	· A rendszer minden bejelentkezést és jelszóváltást megelőzően felhasználói hitelesítést végez · A felhasználóknak semmilyen művelet nem kell elvégeznie · Google szabvány szerint kerülnek a bot programok kiszűrésre	
Kétfaktoros hitelesítés		· A rendszer minden bejelentkezést és jelszóváltást megelőzően felhasználói hitelesítést végez · A felhasználóknak semmilyen művelet nem kell elvégeznie · Google szabvány szerint kerülnek a bot programok kiszűrésre

Funkciók	Alapszintű megoldások	Emeltszintű megoldások
Felhasználói szintek megkülönböztetése		- Beállítható erősebb jelszókezelés, státusz kezelés és kétfaktoros hitelesítés külön, bizonyos jogosultsági szintek számára – ld. JOGOSULTSÁGOK Példák: - Általános felhasználók számára a kötelező jelszó 8 karakter, kis és nagy betű, valamint számok. Csak új eszköz esetén kér második faktort a rendszer. - Admin jogosultság esetén a minimum karakterszám 12, és kötelező egy speciális karakter. Minden belépés esetén kér második faktort a rendszer.

