

# Sigurnosne politike - lozinke

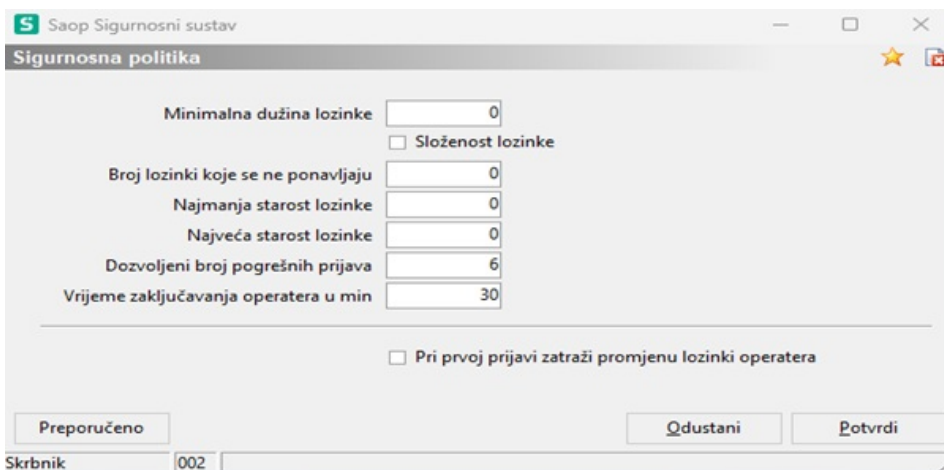
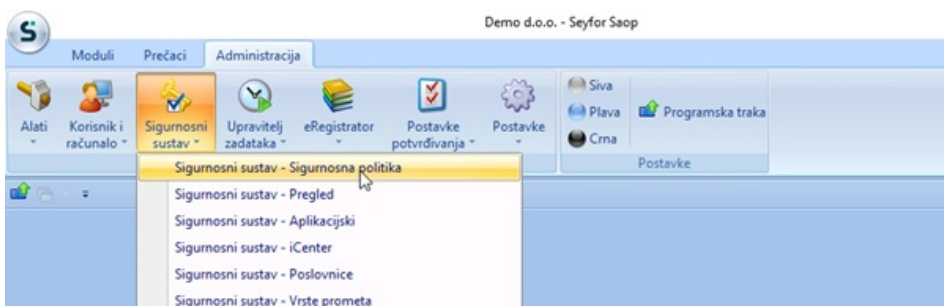
U ovom članku

Zadnja promjena 23/03/2026 12:59 pm CET | Objavljeno 10/03/2026

U Saopu je moguće postaviti sigurnosne politike lozinke koja osiguravaju sigurnost lozinke s kojom se operateri prijavljuju u program. Ukoliko sigurnosne politike nisu postavljene, operateri mogu do daljnjeg koristiti svoje lozinke.

Pristup je odobren samo administratoru putem sigurnosnog sustava na kartici *Administracija*.

Prikaz niže prikazuje zadane postavke. Jedina zadana postavka je da se nakon 6 neuspješnih pokušaja unosa lozinke prijava onemogućuje na 30 minuta. Nakon 30 minuta, ponovno je omogućena prijava s valjanom lozinkom.



- Minimalna duljina lozinke:

0 14 - gdje 0 znači da je prijava moguća bez lozinke dok najdulja moguća lozinka ima 14 znamenki.

- Složenost lozinke

Složena lozinka pokriva najmanje 3 skupine znakova. Postoje 4 skupine znakova: mala slova, velika slova, brojevi i posebni znakovi. Kao rezultat, lozinka mora imati najmanje 3 znaka.

- Broj lozinki koje se ne ponavljaju:

0 24 gdje 0 znači da nema kontrole nad ponavljanjem lozinke – stara lozinka se može unijeti kao nova. Primjerice, unos 7 znači da tek nakon 7 izmijenjenih lozinki možemo ponovno koristiti istu.

- Najmanja starost lozinke:

0 998 – koliko dana nakon promjene ne možemo ponovno promijeniti lozinku odnosno kada najranije možemo ponovno promijeniti lozinku. 0- znači da lozinku možemo odmah promijeniti. Kontrola je postavljena tako da spriječi da u jednom danu promijenimo lozinku 7 puta te se vratimo na staru.

- Najveća starost lozinke:

0 999 – kada trebamo promijeniti lozinku odnosno koliko dana vrijedi jedna lozinka. 0 znači da nikada ne tražimo promjenu lozinke dok 999 znači da se lozinka mora promijeniti nakon 999 dana.

- Dozvoljen broj pogrešnih prijavi:

0 99 gdje 0 znači da ne postoji kontrola pogrešnih unosa.

- Vrijeme zaključavanja operatera u min:

0 99 gdje 0 znači da nema zaključavanja. Operatera možemo zaključati da se ne može prijaviti na najviše 99 minuta. U tom slučaju ni administrator ne može otključati operatera ranije.

- Pri prvoj prijavi zatraži promjenu lozinki operatera:

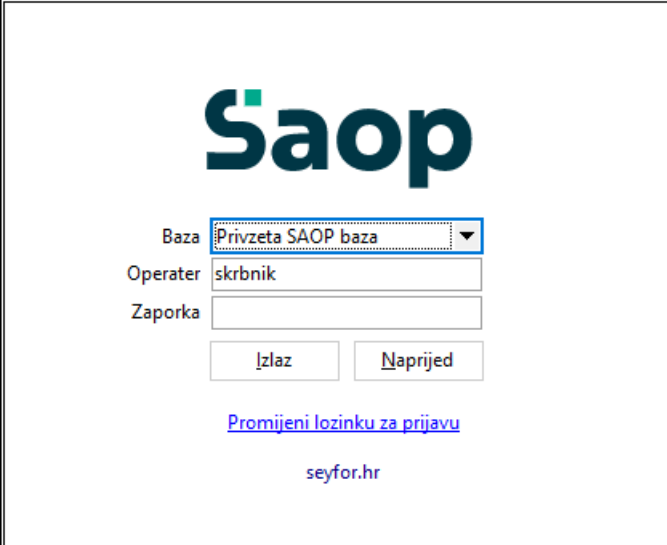
Ako je označeno ovo polje, operater će morati promijeniti lozinku pri prvoj prijavi u skladu s postavljenom sigurnosnom politikom.

Ako administrator sustava nije upoznat sa sigurnosnim politikama lozinke, preko polja Preporučeno može dobiti prijedlog lozinke. Niže je prikaz pravila prema preporučenoj sigurnosnoj politici:

- 1 Lozinka ima najmanje 8 znakova
- 2 Lozinka se mora sastojati od najmanje tri skupine znakova
- 3 Tek nakon šest promjena lozinke možemo ponovno koristiti istu.
- 4 Ako je nova lozinka postavljena danas, može se ponovno zamijeniti tek sutra.
- 5 Nakon 90 dana sustav će zatražiti od operatera da promijeni lozinku.
- 6 Operater će biti blokiran nakon 6 neuspješnih pokušaja prijave.
- 7 Nakon 6 neuspješnih pokušaja prijave, operater će biti blokiran na 30 minuta.
- 8 Nakon postavljanja sigurnosne politike, operateri će biti prisiljeni promijeniti lozinku.

Ako označimo funkcionalnost  *Zatražite promjenu lozinke operatera pri prvoj prijavi*, nakon prijave u sustav otvorit će se dodatni prozor za operatera, gdje će postaviti novu lozinku.

Nakon unosa lozinke te odabirom polja *Naprijed*, otvorit će se novi prozor za postavljanje nove lozinke u skladu s postavljenim sigurnosnim politikama.



**Saop**

Baza

Operater

Zaporka

[Promijeni lozinku za prijavu](#)

seyfor.hr