# JB1.1 - Perché un accesso unico

**In una frase.** In ADSWnext entri una volta sola, e quello che puoi fare lo decide un livello che vale uguale in tutti i servizi.

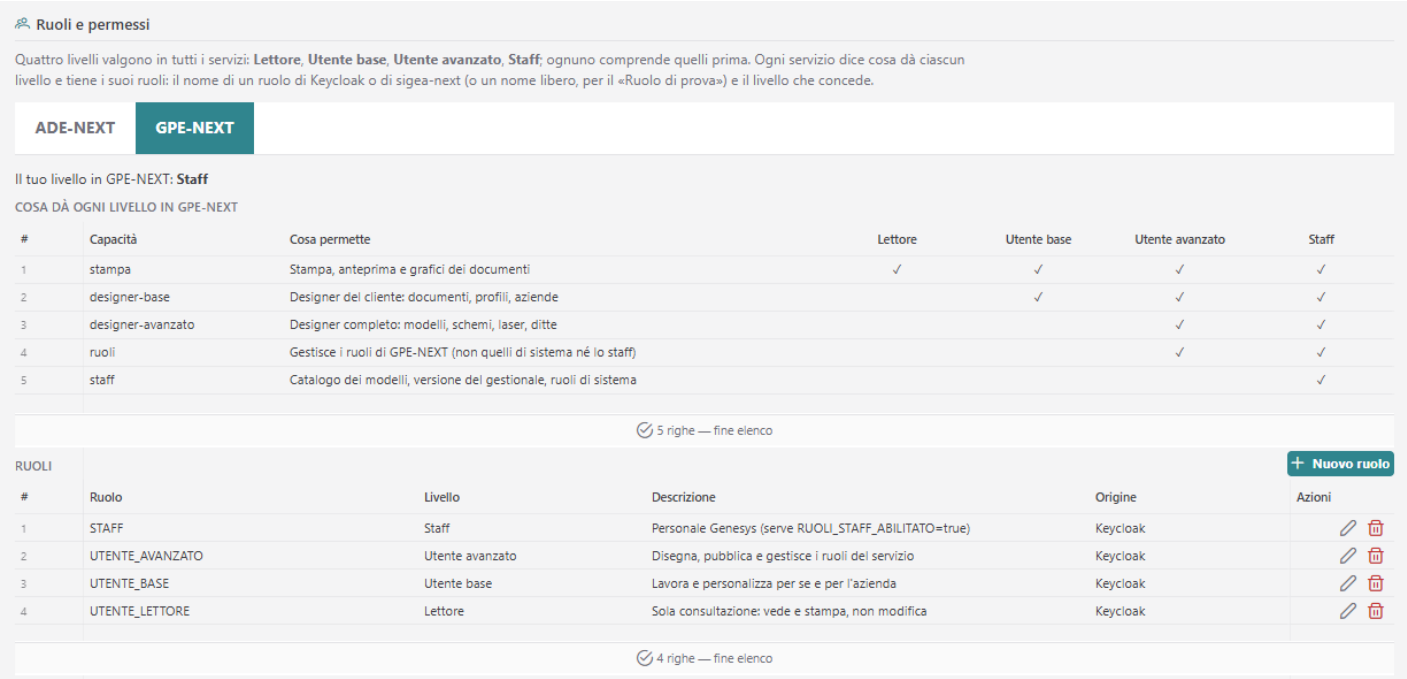
Un gestionale fatto di più programmi rischia di avere un utente per ogni programma: una password per l'ERP, una per le stampe, una per le analisi, e permessi da tenere allineati a mano. Qui non succede. Il controllo di utente e password lo fa un componente solo, l'**Accesso**. I servizi non chiedono mai una password: guardano chi sei e che livello hai.

Entri una volta dall'Accesso. Da lì in poi ogni richiesta porta con sé il tuo lasciapassare: il Gateway lo
*Entri una volta dall'Accesso. Da lì in poi ogni richiesta porta con sé il tuo lasciapassare: il Gateway lo controlla, il servizio ci legge i tuoi ruoli*

Gli utenti e i ruoli non si reinventano: sono quelli che hai già nel gestionale. L'installazione li copia nell'Accesso, senza password. Ognuno sceglie la sua al primo ingresso.

> **Cosa ci guadagni.**
> • **Un solo utente per tutto.** Con lo stesso utente e la stessa password apri le pagine nuove di SIGEAnext, le pagine storiche di SBHweb, le stampe di GPEnext e le analisi. Niente utenti doppi da creare e da ricordare.
> • **Quattro livelli uguali ovunque.** Lettore, Utente base, Utente avanzato, Staff. Chi è Lettore consulta e stampa in ogni servizio, senza regole diverse da un programma all'altro.
> • **I permessi si gestiscono in una pagina sola. Ruoli e permessi** ha una scheda per servizio: dici una volta che livello dà un ruolo del gestionale, e vale dalla richiesta successiva.

Qui sotto la pagina **Ruoli e permessi**: una scheda per servizio, in alto il tuo livello, sotto cosa dà ogni livello e i ruoli agganciati.




*La pagina Ruoli e permessi: le schede dei servizi, il tuo livello, cosa dà ogni livello e l'elenco dei ruoli. Ambiente di prova*

> **Nota.** Nelle pagine storiche l'ERP legacy/COBOL chiede ancora la sua password, con l'utente già scritto. È la stessa password: il sistema le tiene uguali. Dettagli nella pagina La pagina di accesso.

> **Per chi sviluppa.**
> • L'Accesso è Keycloak. Ogni installazione ha il suo spazio (realm), che si chiama `sigea-<codice installazione>`.
> • Il lasciapassare è un token JWT. Il Gateway ne controlla la firma; ogni servizio ne legge i ruoli.
> • Si accende con `AUTH_ENABLED=true`. Disegno: `docs/devops/auth/SSO-DISEGNO-TECNICO.md`.

---

Revisione #2
Creato 17 novembre 2026 07:56:20 da Giuseppe Anelli
Aggiornato 17 novembre 2026 09:34:06 da Genesys Software