JB4 - Per chi amministra

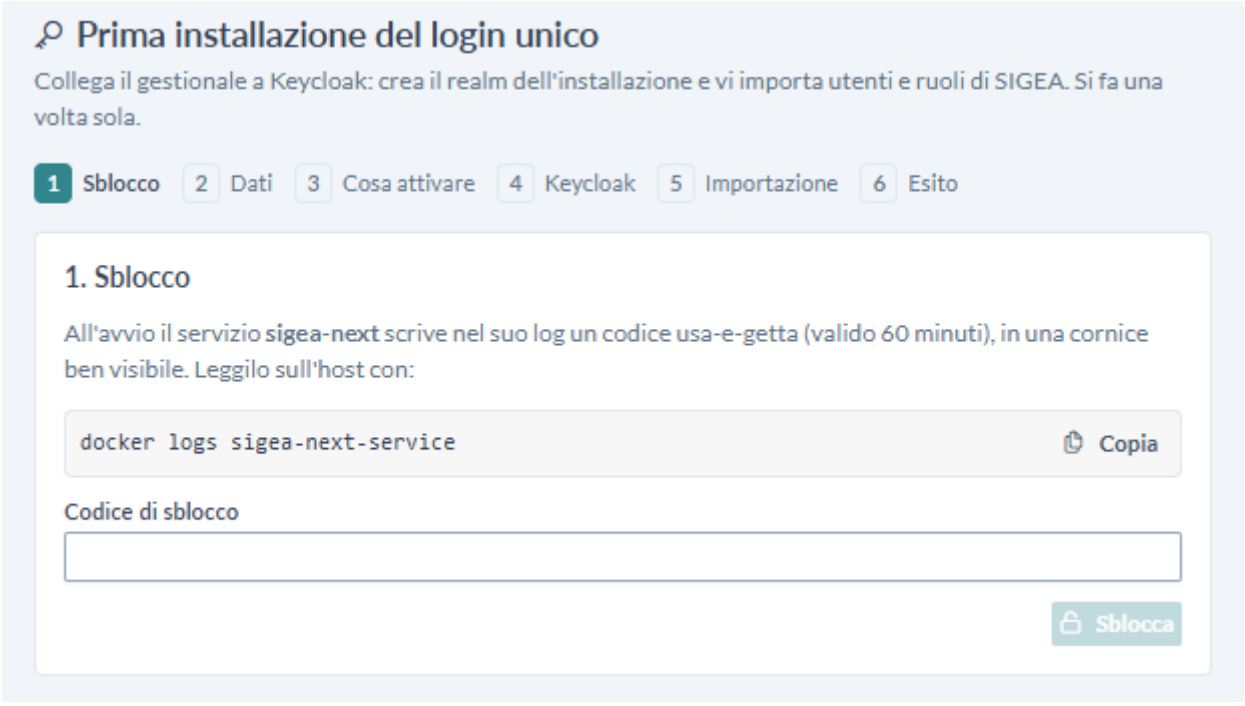
- JB4.1 - Attivare il login unico
- JB4.2 - Agganciare un servizio nuovo
- JB4.3 - Se qualcosa non va

JB4.1 - Attivare il login unico

In una frase. L'accesso unico si accende una volta per installazione, con una procedura guidata che copia utenti e ruoli dal gestionale.

Non devi creare gli utenti a mano né configurare l'Accesso voce per voce. La procedura fa tutto in sei passi, legge soltanto dal gestionale e si può rilanciare senza creare doppioni.

1. **Prepara l'installazione.** Chi installa scrive nel file d'ambiente che l'accesso è acceso, il codice dell'installazione e l'indirizzo dell'Accesso. Poi riavvia i servizi.
2. **Apri l'applicazione.** Finché l'installazione non è fatta, qualunque indirizzo apre **Prima installazione del login unico**. Nessuno entra, ma tutti vedono perché.
3. **Sblocca.** La procedura chiede un codice usa e getta, valido 60 minuti. Lo trova solo chi ha accesso al server: così un visitatore qualunque non può fare l'installazione al posto tuo.



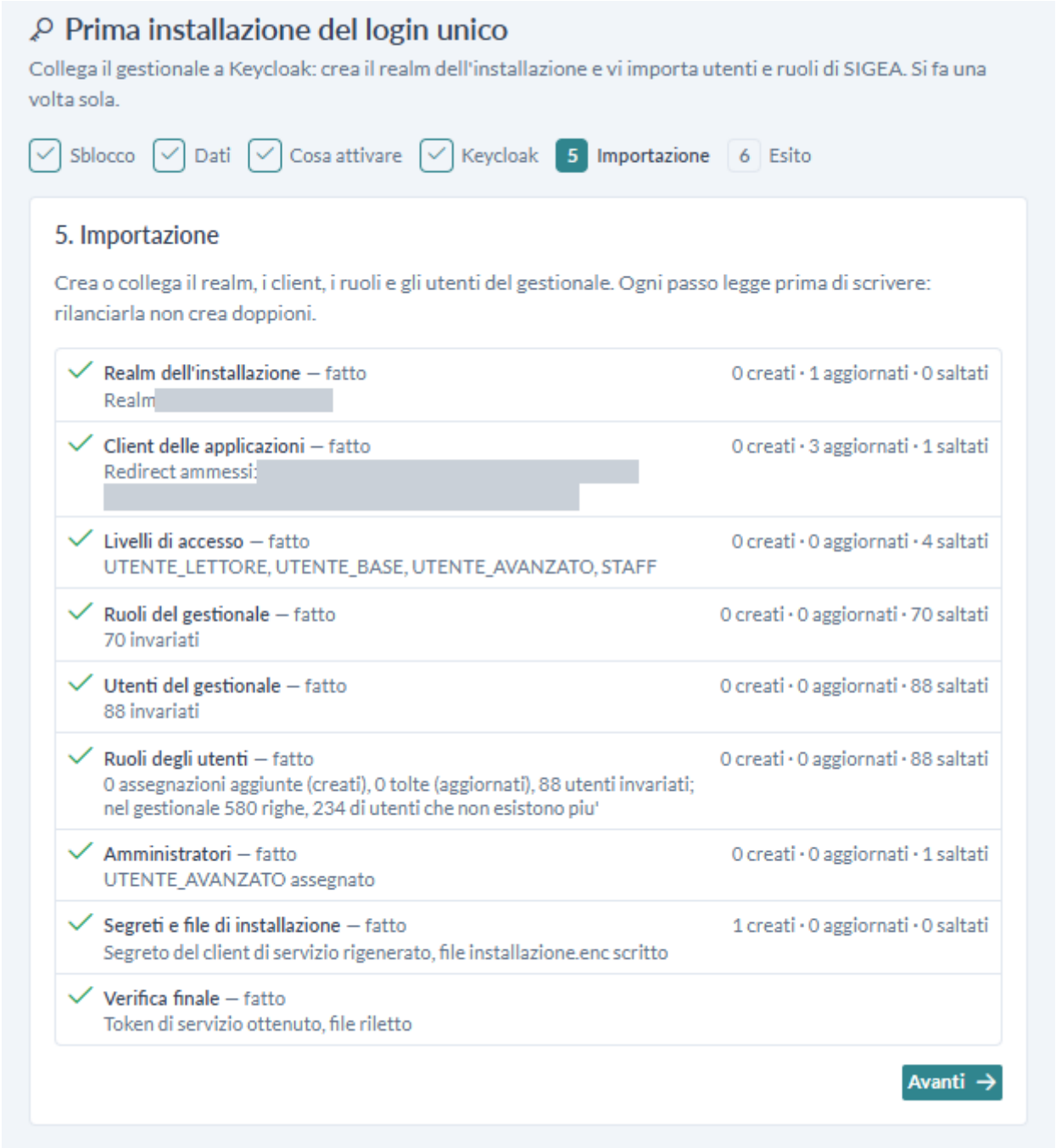
Passo 1 della procedura: il codice di sblocco, da leggere sul server

4. **Conferma i dati e scegli cosa attivare.** Il nome dell'azienda, gli utenti che saranno amministratori, e quali applicazioni usano l'accesso unico, per esempio l'ERP e le pagine storiche.



Passo 3: quali applicazioni entrano con l'accesso unico

5. **Collega l'Accesso e avvia.** Servono utente e password di un amministratore dell'Accesso: non vengono salvati. **Verifica** mostra quanti utenti e ruoli arriveranno. **Avvia** li importa.



Passo 5: l'importazione, con quante cose sono state create o aggiornate. Indirizzi coperti

6. **Vai al login.** Da qui ogni utente fa il suo primo accesso e sceglie la password.

L'importazione crea lo spazio dell'installazione, i quattro livelli, tutti i ruoli e tutti gli utenti del gestionale. Gli utenti arrivano senza password: quelle del gestionale non vengono lette né copiate.

> **Nota.** Per tornare indietro basta spegnere l'accesso nel file d'ambiente e riavviare: tutto torna com'era e quello che è stato importato resta dov'è.

> **Attenzione.** Un utente creato nel gestionale dopo l'importazione non entra finché non si riallinea. Per portare un'installazione già fatta allo stato di oggi c'è **Assesta l'installazione**, nella stessa voce di menu di **Ruoli e permessi**.

Per chi sviluppa.

• Variabili: `AUTH_ENABLED=true`, `SIGEA_INSTALLAZIONE`, `KEYCLOAK_BASE_URL`, `KEYCLOAK_INTERNAL_URL`, `SIGEA_SETUP_KEY`, `SSO_REDIRECT_ORIGINS`; per le pagine storiche `SBH_SSO_MODE=on`. Registro: `docs/devops/ENVIRONMENT.md`.

• Il codice di sblocco è nel log di SIGEAnext. L'esito finisce nel file cifrato `installazione.enc`.

• Una installazione per cliente: `docs/devops/auth/SSO-PER-INSTALLAZIONE.md`.

Per approfondire.

• Login unico con Keycloak: `docs/guide/amministrazione/login-unico-keycloak/README.md`

JB4.2 - Agganciare un servizio nuovo

In una frase. Un servizio nuovo entra nell'accesso unico rispettando poche regole fisse: da quel momento compare da solo nella pagina Ruoli e permessi, con gli stessi quattro livelli.

ADSWnext cresce un servizio alla volta. Se ognuno inventasse i suoi utenti e i suoi permessi, in pochi mesi si tornerebbe al punto di partenza. Con un contratto unico chi amministra non deve imparare niente di nuovo: trova una scheda in più, fatta come le altre.

Oggi sono agganciati ADEnext, GPEnext e SIGEAnext, che usa gli stessi agganci di ADEnext. L'Assistente dei dati non lo è ancora.

Cosa deve fare un servizio per entrare:

1. **Stare dietro il Gateway.** Le richieste arrivano solo da lì, già controllate. Il servizio non chiede password e non ne conserva.
2. **Leggere i ruoli nello stesso modo degli altri.** Dal lasciapassare prende tutti i ruoli della persona e li traduce in un livello con le stesse regole: vale il più alto, lo Staff conta solo dove è acceso.
3. **Dichiarare cosa concede.** Un elenco di capacità, ognuna con il livello minimo che serve. È ciò che la pagina mostra con le spunte.
4. **Tenere la sua tabella dei ruoli**, con i quattro livelli già pronti.
5. **Rispondere alle stesse domande.** Quali ruoli conosci, cosa dà ogni livello, che livello ha chi sta chiedendo. Sono uguali in ogni servizio.
6. **Farsi elencare.** Una riga nel registro dei servizi dell'applicazione. La pagina **Ruoli e permessi** e il **Ruolo di prova** lo trovano da soli; se è spento lo mostrano spento, con il motivo.

Un test uguale in tutti i servizi controlla che le regole diano gli stessi risultati ovunque.

> **Attenzione.** Un servizio non deve mai decidere guardando il nome di un ruolo scritto nel codice. Decide sulle sue capacità: è questo che permette a chi amministra di cambiare i permessi senza toccare il programma.

> **Per chi sviluppa.**
> • Non c'è una libreria comune: i file sono gemelli e si copiano cambiando solo il `package` (`Livello`, `Capacita`, `Origine`, `RegoleRuoli`, `RuoliException`, più il proprio `CapacitaServizio`).
> • Contratto: `GET /ruoli`, `GET /ruoli/livelli`, `GET /me/permessi`, e `/admin/ruoli` per chi ha la capacità `ruoli`. Il Gateway antepone `/api/<servizio>`.

• Test di contratto: `RuoliContrattoTest`. Registro: `SERVIZI_CON_RUOLI` in `frontend/shell/src/shared/auth/ruolo-prova.ts`.
• Passi completi: `docs/guide/sviluppo/ruoli-centrali/README.md`. Rotte e sicurezza del Gateway: `.claude/skills/gateway-auth/SKILL.md`.

Per approfondire.
• Login unico con Keycloak: `docs/guide/amministrazione/login-unico-keycloak/README.md`
• Integrazione Autenticazione JWT Angular + API Gateway: `docs/guide/sviluppo/GUIDA-AUTENTICAZIONE-JWT.md`

JB4.3 - Se qualcosa non va

In una frase. I problemi più comuni con l'accesso e i permessi, cosa vuol dire ciascuno e cosa fare.

Vedo questo	Faccio questo
«Utente o password attuale non corretti» al primo accesso	Scrivi l'utente e la password che usi oggi nel gestionale, non quella nuova
Conferma resta spento	Una regola della password non è rispettata: guarda quali non sono verdi
«Troppi tentativi: riprova fra un minuto»	Aspetta un minuto e riprova con calma
Non entro più dopo vari errori	Dopo cinque errori sei fermo 15 minuti. Aspetta, o chiedi **Sblocca** a chi amministra
Non ricordo la password	**Password dimenticata?** nella pagina di accesso. Il collegamento vale 15 minuti
L'email non arriva	Guarda nella posta indesiderata. Se manca, chiedi una password provvisoria
«rivolgiti all'amministratore» dopo Password dimenticata	Il sistema non può cambiarti la password da solo: la reimposta chi amministra
La password ha più di 12 caratteri	Non si può usare: sceglila da 10 a 12
Le pagine storiche chiedono ancora la password	È previsto: l'utente è già scritto, scrivi la stessa password
«Il login unico non è raggiungibile»	L'Accesso è spento. Avvisa chi amministra; se compare, usa **Continua col login del gestionale**
«Non hai i permessi»	Ti serve un livello più alto. Chiedi a chi gestisce i ruoli
Un pulsante è spento	Fermati sopra con il mouse: il suggerimento dice quale livello serve
Una scheda di Ruoli e permessi è **spento**	Quel servizio non risponde. Leggi il motivo e premi **Riprova**
Ho dato un ruolo ma non cambia niente	Controlla la scheda: il ruolo vale solo nel servizio dove lo hai agganciato
Un utente nuovo non riesce a entrare	Non è ancora stato copiato dal gestionale: serve un riallineamento
Si apre «Prima installazione del login unico»	L'accesso è acceso ma l'installazione non è fatta: la completa chi amministra

Parole da sapere

- **Accesso.** Il componente che controlla utente e password. Uno solo per tutta ADSWnext.
- **Lasciapassare.** La prova che sei entrato. Viaggia con ogni richiesta e contiene i tuoi ruoli.
- **Ruolo.** Un gruppo a cui appartieni nel gestionale, per esempio «amministrazione».
- **Livello.** Uno dei quattro gradi: Lettore, Utente base, Utente avanzato, Staff.
- **Capacità.** Una cosa che un servizio permette di fare, legata a un livello minimo.
- **Primo accesso.** Il modulo dove scegli la tua password, una volta sola.
- **Password provvisoria.** Una password generata dal sistema, da cambiare al primo ingresso.
- **Deposito.** La password del gestionale custodita cifrata, che permette di cambiare le due password insieme.
- **Ruolo di prova.** Il selettore degli ambienti di prova per vedere l'applicazione con un altro ruolo.
- **Staff.** Il livello del personale Genesys. Conta solo dove è acceso.

> **Per chi sviluppa.**
> • Lasciapassare = token JWT; Accesso = Keycloak; lo spazio di un'installazione = realm.
> • Le azioni su utenti e password si trovano nei registri con il marcatore `[UTENTI-PASSWORD]`.
> • Se l'Accesso non risponde nelle pagine storiche: `SBH_SSO_FALLBACK` decide se si può entrare lo stesso.
> • Disegno completo: `docs/devops/auth/SSO-DISEGNO-TECNICO.md` e `docs/devops/auth/AUTENTICAZIONE.md`.