

Indice

1. Cos'è AYCC Auth
2. Accesso alla piattaforma
 - 2.1 Schermata iniziale
 - 2.2 Accesso con Magic Link
 - 2.3 Login social e con altri Identity Providers
3. Dashboard utente
4. Pannello amministratore
 - 4.1 Gestione ruoli e permessi
 - 4.2 Gestione Identity Provider
5. Autenticazione a più fattori (2FA)
 - 5.1 Attivazione 2FA
 - 5.2 Accesso con 2FA attivo
6. Recupero e reset password
 - 6.1 Recupero password
 - 6.2 Reimpostazione
7. Personalizzazione e branding
 - 7.1 Accesso alle impostazioni
 - 7.2 Funzionalità disponibili
8. Sicurezza e privacy
9. Conclusione e feedback

1. Cos'è AYCC Auth

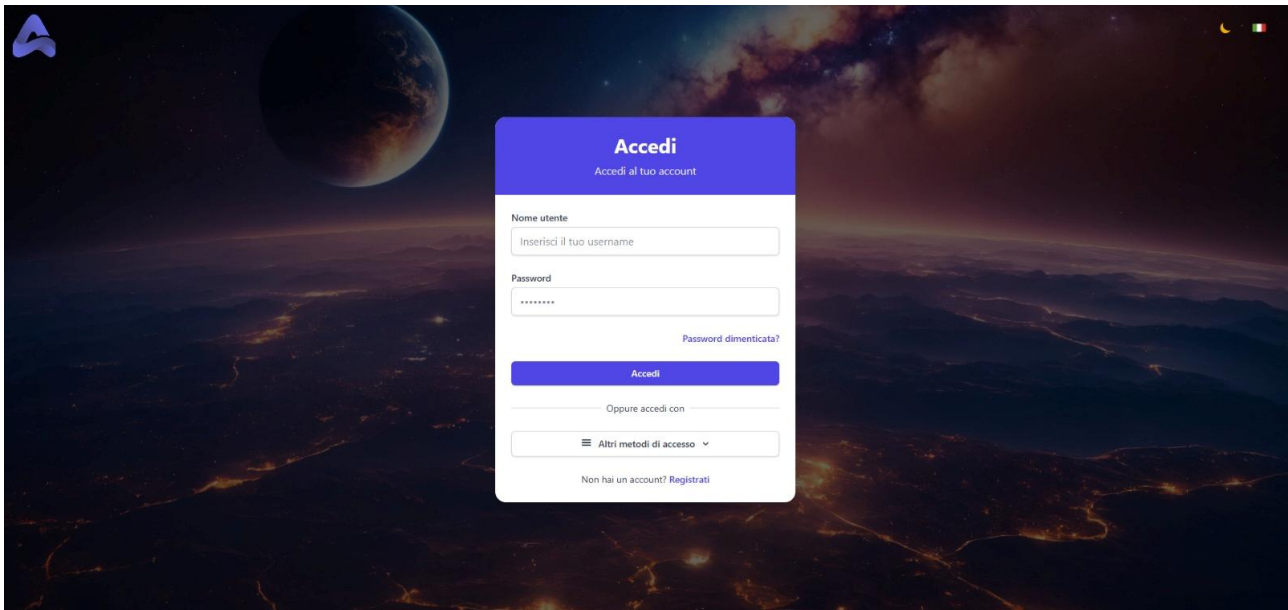
AYCC Auth è il sistema di **autenticazione e autorizzazione avanzato** integrato nella piattaforma All You Can Cloud.

Offre login tradizionale, autenticazione multifattore, accesso tramite Magic Link, login social e tramite altri Identity Providers, garantendo massima sicurezza e personalizzazione.

2. Accesso alla piattaforma

2.1 Schermata iniziale

Dalla schermata principale di AYCC Auth l'utente può effettuare l'accesso tramite nome utente e password, oppure scegliere altre modalità di autenticazione. L'interfaccia è semplice e intuitiva, con uno sfondo personalizzabile e campi ben visibili per l'inserimento delle credenziali.

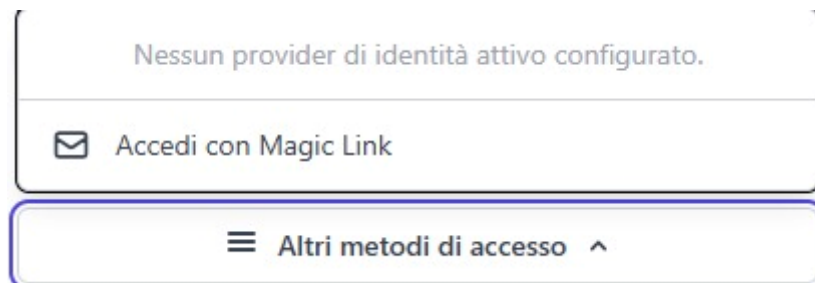


2.2 Accesso con Magic Link

AYCC Auth supporta l'autenticazione passwordless tramite Magic Link, una modalità che consente di accedere all'account semplicemente cliccando su un link ricevuto via email. Per utilizzare questa funzione:

- Nella schermata di accesso, clicca su "Altri metodi di accesso".
- Seleziona "Accedi con Magic Link".
- Inserisci il tuo indirizzo email e conferma.
- Riceverai un'email contenente un link univoco:

Cliccandolo, accederai automaticamente al tuo account senza digitare la password.



2.3 Login social e con altri Identity Providers

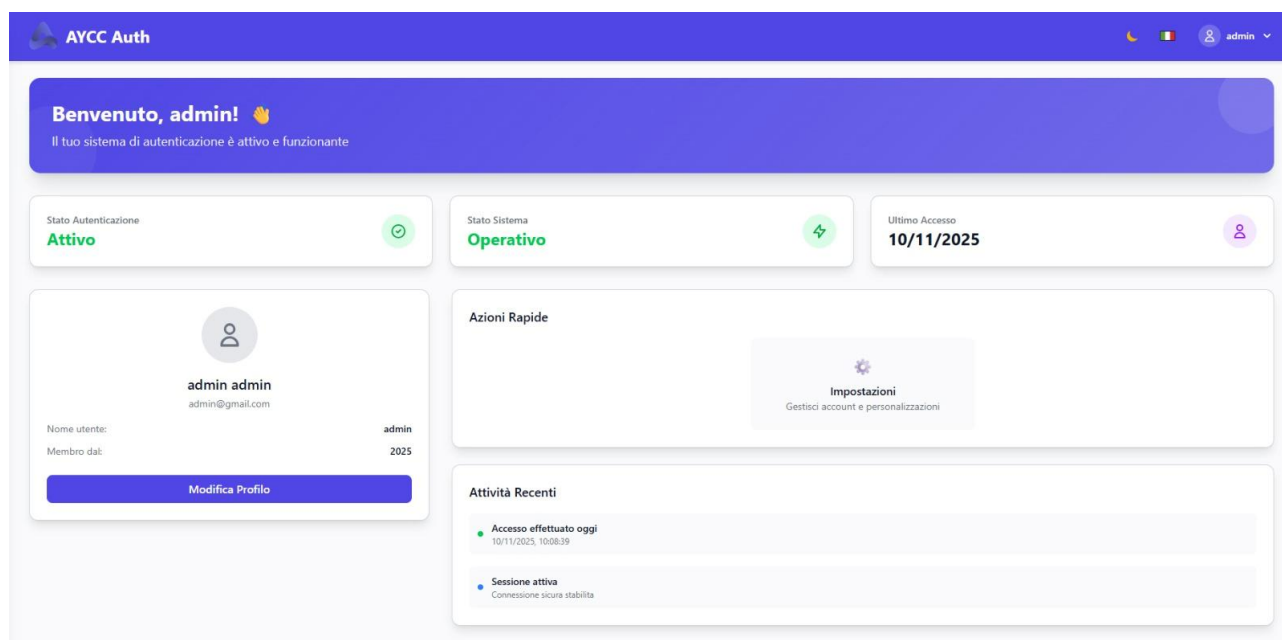
AYCC Auth consente anche l'accesso tramite provider di identità esterni, come Google, Microsoft, Facebook, o GitHub. Questa funzionalità permette agli utenti di autenticarsi con il proprio account già esistente presso uno di questi servizi.

Nota: La disponibilità di questi provider dipende dalla configurazione del sistema. Solo l'amministratore può abilitare o aggiungere nuovi provider. Per ulteriori dettagli sulla configurazione, consulta la sezione 4.2 Gestione Identity Provider.

3. Dashboard utente

Dopo il login, l'utente visualizza la dashboard personale: un pannello riepilogativo con profilo, preferenze e notifiche. Da qui è possibile:

- Gestire il profilo utente (nome, email, lingua, tema)
- Visualizzare l'attività recente
- Compiere azioni rapide



4. Pannello amministratore

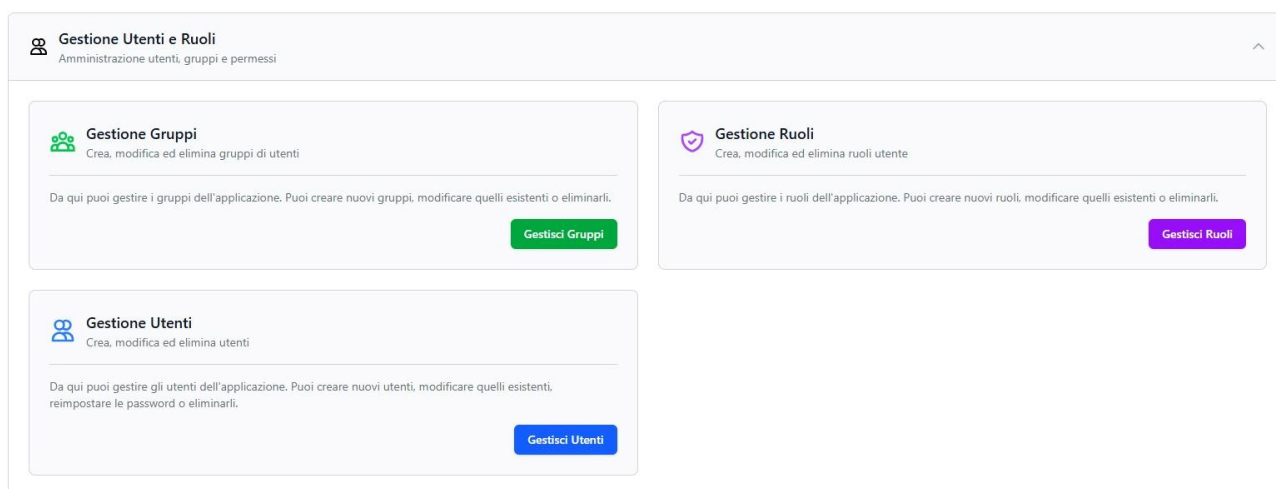
Solo gli utenti con ruolo admin hanno accesso al pannello amministratore, da cui è possibile gestire utenti, gruppi, ruoli, provider e impostazioni di branding. Per accedervi:

- Dalla schermata iniziale, clicca in alto a destra sul menu "Admin".
- Si aprirà la dashboard amministrativa, che include un pannello laterale sinistro con le varie sezioni: Amministrazione, Profilo, Password, Gruppi, Ruoli, Utenti, ecc.

4.1 Gestione ruoli e permessi

La sezione Ruoli e Permessi permette di creare, modificare o eliminare ruoli utente e di assegnare i relativi permessi. Da qui l'amministratore può strutturare il sistema di accesso, differenziando i livelli di visibilità e di azione per ciascun gruppo di utenti. Come accedere alla sezione:

- Dalla dashboard amministrativa, clicca su “Ruoli” nel pannello laterale.
- Si aprirà una schermata che permetterà di gestire ruoli, utenti e gruppi
- Cliccando su Gestione Ruoli, si potranno creare, modificare o eliminare tutti i ruoli attualmente definiti.



Funzionalità principali:

- Creazione di un nuovo ruolo: clicca su “Nuovo Ruolo”, inserisci nome e descrizione, quindi conferma con “Crea”.
- Modifica o eliminazione: tramite le icone accanto a ciascun ruolo, è possibile aggiornare i dettagli o rimuovere ruoli non più necessari.
- Associazione permessi: ogni ruolo può essere collegato a specifici permessi d'accesso a moduli o funzionalità.

Role Management



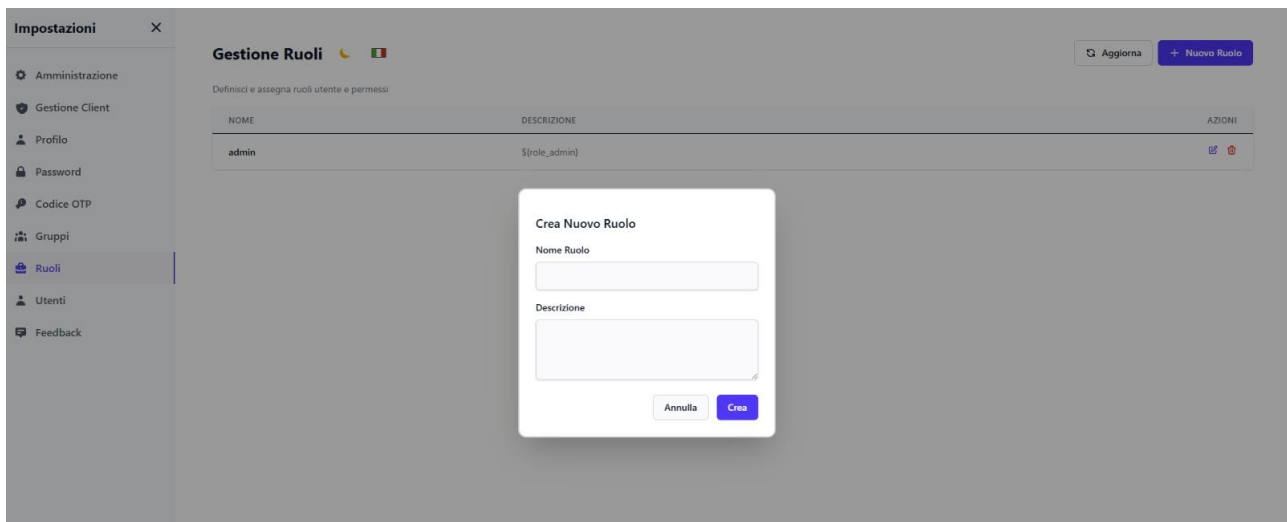
Gestione Ruoli 🌙 🇮🇹

🔄 Aggiorna

+ Nuovo Ruolo

Definisci e assegna ruoli utente e permessi

NOME	DESCRIZIONE	AZIONI
admin	`\${role_admin}`	 



4.2 Gestione Identity Provider

Questa sezione consente all'amministratore di aggiungere o modificare provider esterni per il login (Google, Microsoft, Facebook ecc.) Come accedere:

- Dalla dashboard amministrativa, clicca su "Amministrazione" nel pannello laterale.
- Una volta aperta la schermata, clicca su "Identity Provider".
- Seleziona "Aggiungi Provider" per aprire il modulo di configurazione.

Configurazione:

- Seleziona il tipo di provider dal menu a tendina.
- Inserisci le credenziali richieste (Client ID e Client Secret).
- Attiva il provider selezionando l'opzione "Abilitata".
- Salva la configurazione cliccando su "Aggiungi".

5. Autenticazione a più fattori (2FA)

AYCC Auth offre la possibilità di abilitare la verifica in due passaggi (2FA) per una maggiore sicurezza.

5.1 Attivazione 2FA

L'attivazione dell'autenticazione a due fattori è gestita a livello di organizzazione dall'amministratore. Per abilitare la 2FA per l'organizzazione:

- Accedi al Pannello Amministratore.
- Clicca su Amministrazione nel menu laterale sinistro.
- Seleziona Configurazione sistema.

- Attiva l'opzione Autenticazione a due fattori.

Una volta abilitata la 2FA per l'organizzazione, gli utenti vedranno un prompt di configurazione al successivo accesso. Ogni utente può tuttavia scegliere di saltare questo passaggio cliccando su "Salta questo passaggio" e accedere senza inserire l'OTP. Se in seguito l'utente decide di attivare la 2FA:

- Accede al proprio profilo personale.
- Clicca su Codice OTP nel menu laterale sinistro (la struttura è simile a quella del pannello admin, ma con meno opzioni).
- Segue le istruzioni per configurare il codice OTP:
- Scansiona il QR Code visualizzato.
- Inserisce il codice temporaneo generato dall'app di autenticazione per completare la verifica.

Una volta confermata, l'autenticazione a due fattori sarà attiva per tutti i futuri accessi.

5.2 Accesso con 2FA attivo

Al login, l'utente inserisce il codice OTP generato dall'app Authenticator. Se il codice è corretto, l'accesso viene completato. In caso contrario, verrà mostrato un messaggio di errore e sarà necessario ripetere l'operazione.

6. Recupero e reset password

6.1 Recupero password

- Dalla schermata di login, clicca su "Password dimenticata?".
- Inserisci l'indirizzo email associato all'account.
- AYCC Auth invia un'email con un link temporaneo di reset.
- Clicca il link entro il tempo limite (configurabile dall'amministratore).
- Verrai reindirizzato ad una pagina sicura per impostare una nuova password.

6.2 Reimpostazione

Dopo aver cliccato il link, inserire una nuova password sicura.

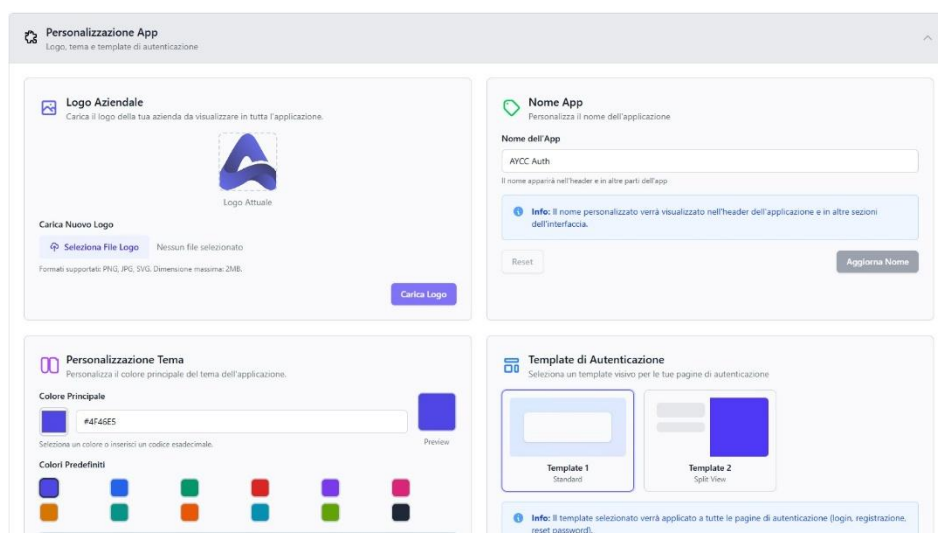
7. Personalizzazione e branding

AYCC Auth consente di personalizzare l'interfaccia dell'App con l'identità visiva e il branding della propria organizzazione. Solo gli utenti con ruolo admin possono accedere a queste impostazioni e modificare l'aspetto grafico e tematico dell'interfaccia. L'admin può:

- Caricare il logo aziendale
- Scegliere il tema (chiaro/scuro)
- Personalizzare i colori principali dell'interfaccia
- Impostare la lingua predefinita

7.1 Accesso alle impostazioni

- Dalla schermata iniziale, clicca in alto a destra sul menu "Admin".
- Nella dashboard amministrativa, seleziona "Amministrazione" dal pannello laterale sinistro.
- All'interno della sezione "Amministrazione", apri il menu "Personalizzazione App".



7.2 Funzionalità disponibili

Dalla schermata di personalizzazione è possibile configurare i seguenti elementi:

- Logo aziendale: carica il logo dell'organizzazione nei formati PNG, JPG o SVG. Il logo verrà visualizzato nelle schermate di login e nella barra superiore dell'interfaccia.
- Nome applicazione: definisci il nome che verrà mostrato nella schermata di accesso e nelle email di notifica.
- Tema e colori: seleziona il tema grafico preferito (chiaro o scuro) e personalizza i colori principali tramite codice esadecimale o palette predefinita. Le modifiche vengono applicate in tempo reale nell'anteprima.
- Layout e template di autenticazione: scegli tra layout disponibili, come Standard o Split View, per modificare l'aspetto delle schermate di login e registrazione.

- Lingua dell'interfaccia: imposta la lingua predefinita dell'applicazione (italiano o inglese). Gli utenti potranno comunque selezionare la propria lingua personale dal profilo.

8. Sicurezza e privacy

- Tutte le comunicazioni avvengono su HTTPS
- Dati sensibili criptati con algoritmi AES e bcrypt
- Sessioni gestite tramite JWT e Refresh Token

9. Conclusione e feedback

AYCC Auth è una soluzione completa e intuitiva per la gestione sicura dell'accesso e dell'identità digitale. Progettato per offrire un'esperienza fluida, personalizzabile e conforme agli standard di sicurezza, permette di amministrare utenti, ruoli e provider in modo semplice e centralizzato. Con AYCC Auth, tutto è più semplice. Questa guida è in costante evoluzione: con il rilascio pubblico dell'applicazione, AYCC raccoglierà feedback dagli utenti e dagli amministratori di sistema per migliorare le funzionalità e la documentazione. Le domande più frequenti e i suggerimenti più utili verranno integrati nelle prossime versioni della User Guide, con l'obiettivo di rendere il supporto sempre più completo e aggiornato.

