PREMESSA

Grazie al portale dedicato potrai attribuire le tue utenze a diversi progetti, suddividerle in gruppi all'interno di un progetto per poterle fare gestire da amministratori diversi, ciascuno con i propri permessi.

Potrai comodamente importare le utenze che già gestisci e decidere se mantenere le loro credenziali attuali o cambiarle.

In Autentica le impronte delle password delle utenze verranno storicizzate in un Database apposito: grazie al fatto che le tue password non saranno più contenute nel database insieme ai dati sensibili, il tuo applicativo diventerà più sicuro e a norma GDPR.

GUIDA ALL'UTILIZZO DI AUTENTICA ADMIN

Introduzione

Autentica Admin è il portale Web che consente di gestire le credenziali delle tue utenze in diverse modalità.

Con questo portale sarai in grado di organizzare la gestione credenziali come meglio credi: potrai aggiungere i progetti (che possono essere i tuoi applicativi) di cui devi gestire le utenze e potrai creare gli amministratori ai quali desideri delegare qualche funzione in tale gestione.

Chi si registra al portale avrà il ruolo di super-amministratore, ovvero possiederà tutti i permessi possibili presenti nel portale. Il ruolo non è cedibile ad altri amministratori.

Nel caso in cui la sottoscrizione non venga rinnovata non sarà più possibile accedere all'applicativo.

Basterà rinnovare la sottoscrizione per poter ripristinare l'accesso senza alcuna perdita di dati.

Quando aggiungi i progetti potrai definirne le caratteristiche che riguardano l'autenticazione e la sicurezza delle credenziali.

All'interno del progetto selezionato potrai creare utenti o importare utenze già definite per garantire una continuità con il pregresso.

Potrai attribuire le singole utenze a dei gruppi, dei quali deciderai tu chi sarà l'amministratore e che funzioni specifiche potrà svolgere su di esso.

La struttura logico-funzionale di "Autentica Admin" è la seguente:

1. Il mio profilo (contiene i dati dell'amministratore loggato);
2. Lista progetti;
3. All'interno di ciascun progetto:
    a. Dati del progetto (password, token, SMTP, modelli email).
    b. Amministratori (funzioni abilitate in questo progetto, gruppi ad esso attribuiti).
    c. Utenti (dati utente, gruppi di appartenenza).
    d. Gruppi (elenco utenti appartenenti al gruppo, elenco gruppi e relativi amministratori assegnati).

Versioni

Quando ti registri ricorda che sottoscriverai la versione **gratuita** di “Autentica” (Autentica Cherry).

Se desideri un’altra versione basterà loggarti ed entrare nel profilo dove potrai scegliere la versione desiderata nella sezione “la tua sottoscrizione”. Se sottoscriverai una versione a pagamento ti verranno richieste informazioni di fatturazione con il consenso al trattamento di tali informazioni.

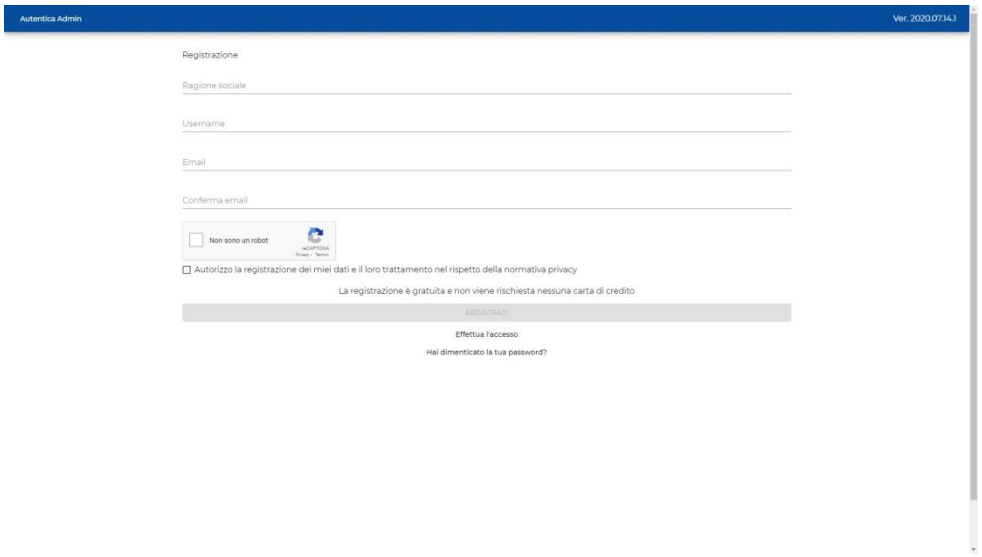
In ogni tipo di sottoscrizione, tranne quella gratuita, è prevista la possibilità di acquistare il pacchetto “2FA” che ti consente di avere l’autenticazione a due fattori nelle tue App.

Il tipo di sottoscrizione potrà essere cambiato solamente dal super-amministratore.

Registrazione

Per registrarsi occorrono solo pochi dati:

- username (che può anche non essere un indirizzo e-mail);
- e-mail (obbligatoria se il campo username non è un indirizzo e-mail);

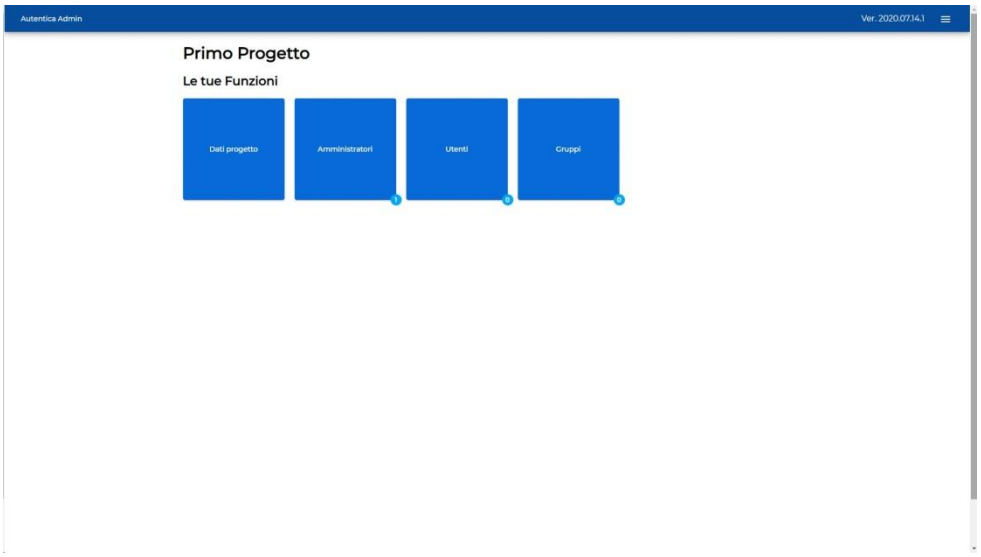


Ti verrà automaticamente spedita una password temporanea alla tua casella di posta che dovrai cambiare al primo accesso per verificare il tuo account.

Quando ti registri sarai configurato automaticamente come super-amministratore e avrai la possibilità di:

- aggiungere ed eliminare i progetti modificandone anche le impostazioni di sicurezza (password, token, modelli email, SMTP);
- gestire gli amministratori;
- gestire le utenze;
- gestire i gruppi.

È pertanto consigliabile che ad effettuare la registrazione sia la figura che possa assolvere a tutte le funzioni sopra descritte.



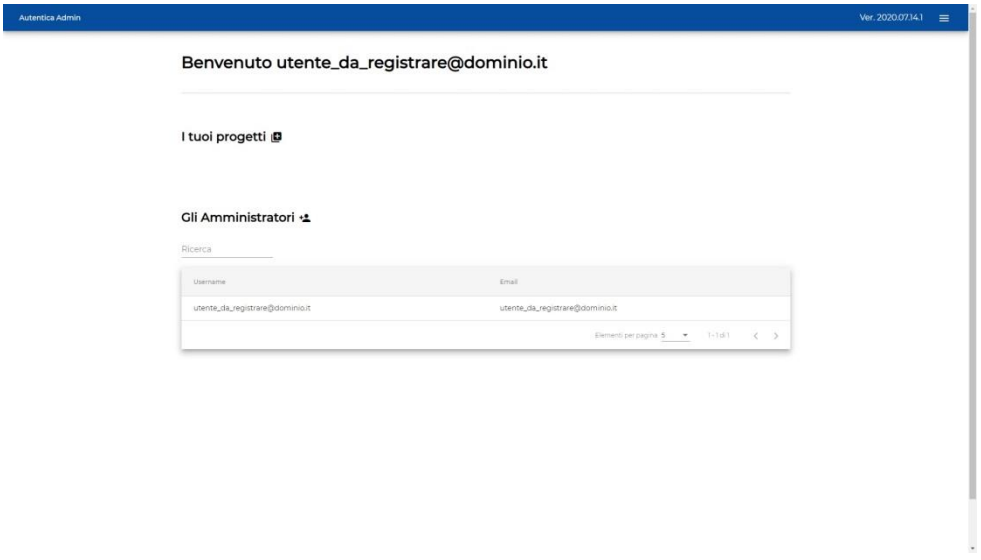
Il tuo profilo

Nel tuo profilo troverai tutte le tue informazioni e potrai modificare i dati quando lo desideri.

Nessun amministratore può variare i permessi di se stesso. Il super-amministratore possiede di default ogni permesso senza la possibilità di rimuoverlo.

Dashboard

La home page di Autentica Admin si presenta con in alto la lista dei progetti e in basso la lista totale degli amministratori dei tuoi progetti. Il super-amministratore vedrà tutti i progetti e tutti gli amministratori.

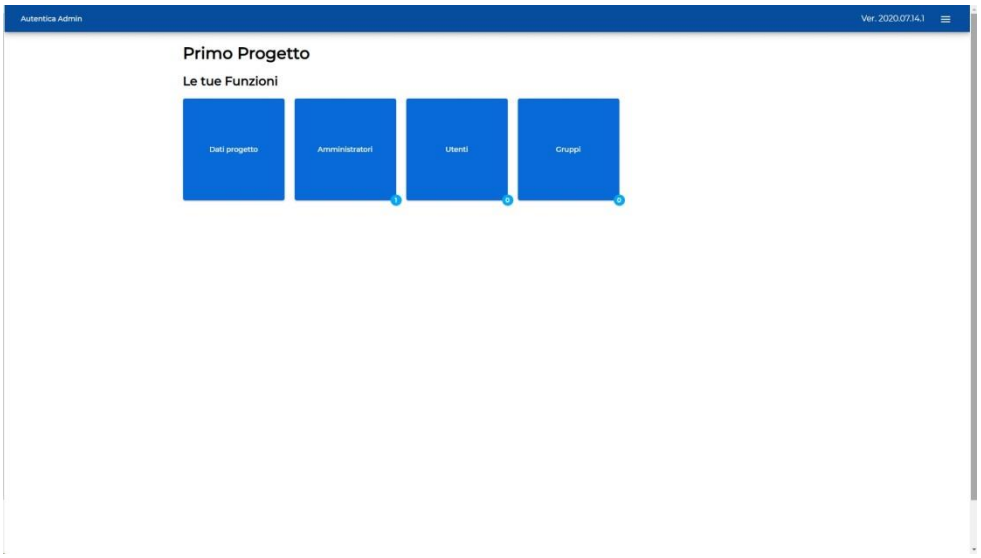


Quando un amministratore effettua il login vedrà invece la lista completa dei progetti solo se possiede i permessi necessari (gestione progetti), altrimenti vedrà i progetti ai quali è stato assegnato dal super-amministratore per svolgere qualche funzione (gestione utenti, gestione gruppi).

Se un amministratore loggato ha la gestione amministratori, vedrà la lista in basso, altrimenti non comparirà alcuna lista e potrà vedere i dati di sé stesso e i suoi permessi nella sezione Profilo.

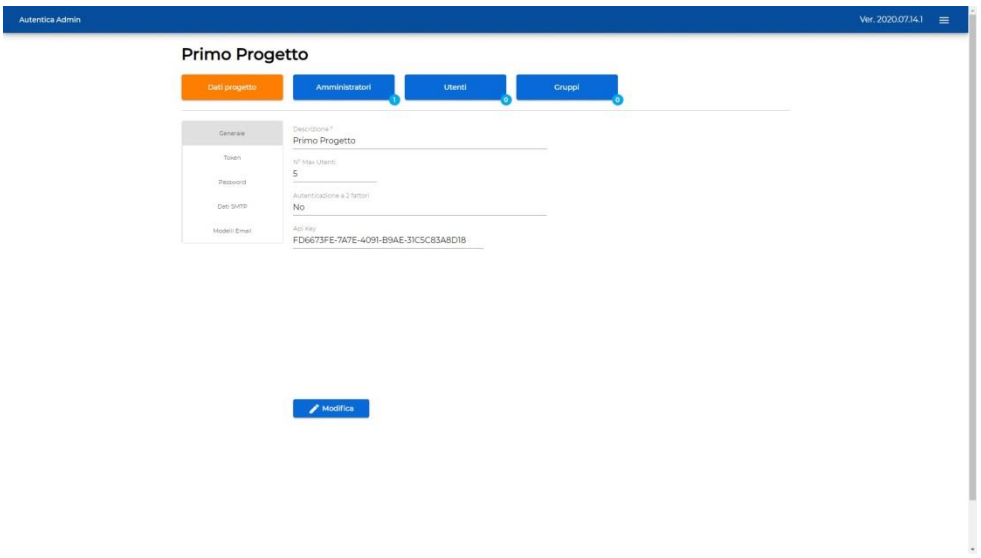
Progetti

Per prima cosa noi ti consigliamo di aggiungere i progetti.



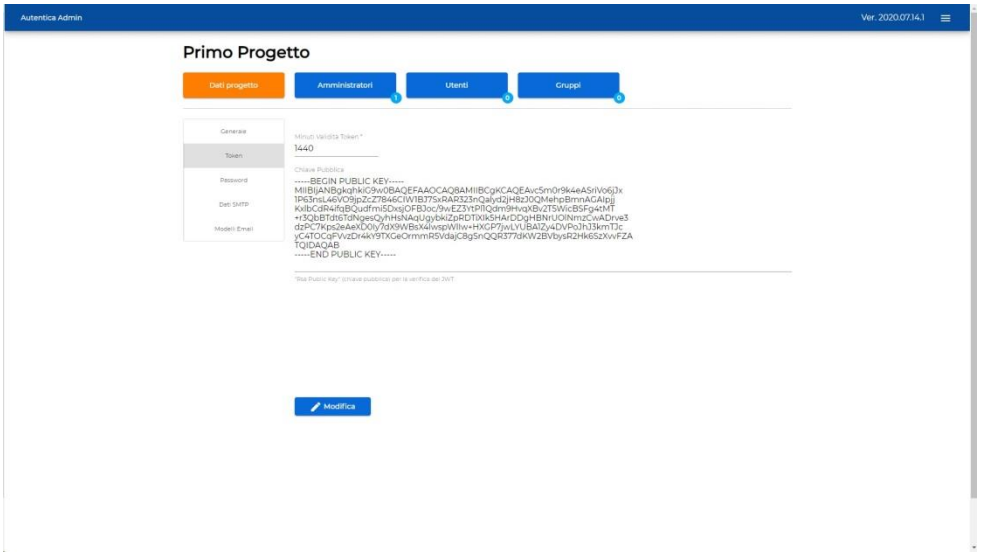
Di ciascuno di essi potrai visualizzare e gestire i seguenti dati:

- Nome progetto/descrizione progetto.
- Numero massimo di utenti (parametro legato al tipo di sottoscrizione).
- Autenticazione a 2 fattori (parametro legato al tipo di sottoscrizione).
- Api Key, il codice univoco dell'applicazione da utilizzare per le chiamate ad Autentica che potrai anche rigenerare per questioni di sicurezza.

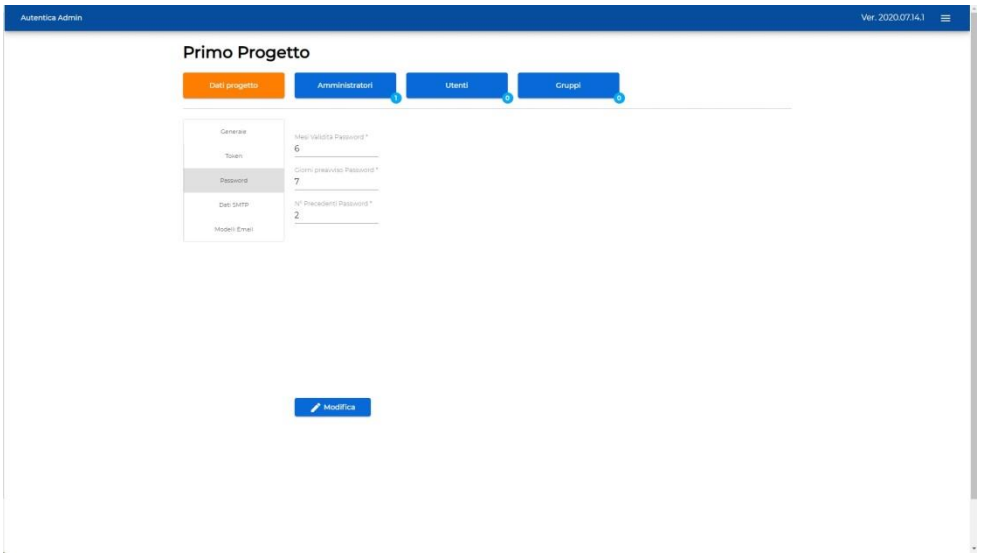


- Se si seleziona una coppia di chiavi asimmetriche generate automaticamente per la codifica/decodifica, la chiave privata di codifica sarà nota solo a GI; in alternativa puoi caricare un certificato, la cui chiave privata verrà utilizzata per la codifica (solo nelle versioni a pagamento).

- La chiave pubblica per decodificare il token.
- Minuti di validità del token.



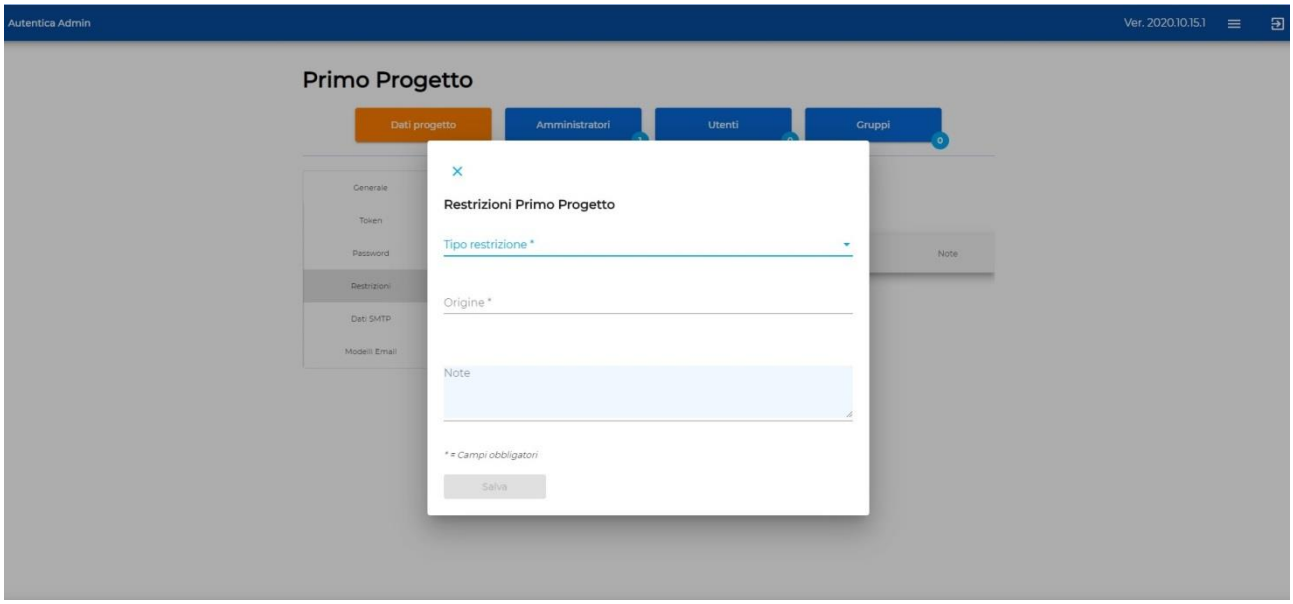
- Mesi validità password, specifica per quanti mesi saranno valide le password delle utenze di tale progetto. Ricordiamo che se le password non scadono mai, non verranno rispettate le norme GDPR in termini di sicurezza password. Il valore di default per questo campo è di 6 mesi, che è uno standard che può andare bene per la maggioranza dei casi, ma per la protezione di dati sensibili tale valore dovrebbe essere al massimo 3.
- Giorni preavviso, specifica a livello di progetto, quanti giorni prima della scadenza password dovranno essere avvisati gli utenti con una mail automatica.
- Numero precedenti password, specifica a livello di progetto quante delle ultime password già utilizzate non devono poter essere utilizzate nuovamente dall'utente.



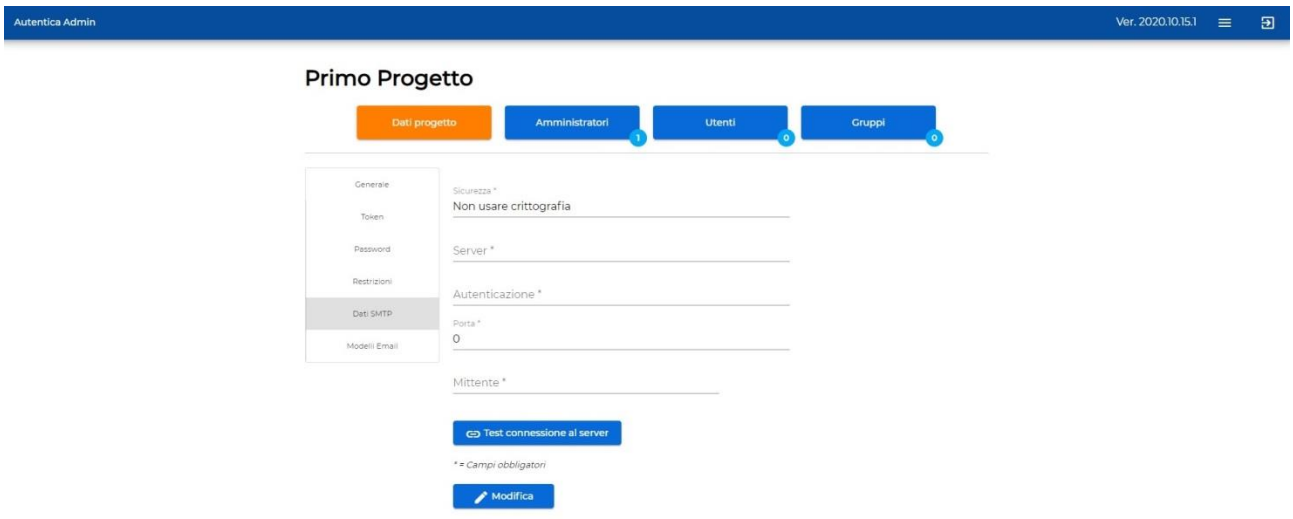
- Restrizioni, permette di inserire limitazioni di utilizzo delle chiamate ad Autentica. Le restrizioni possono essere dei seguenti tipi:
    - "Riferimento HTTP", in tal caso si specifica il dominio da cui sono accettate le chiamate (con possibilità di utilizzo del carattere * per estendere l'accettazione a tutti i domini di terzo livello);

- "Indirizzi IP", per specificare un indirizzo IPv4 da cui sono accettate le chiamate (con possibilità di utilizzo di un intervallo per l'ultima terzina dell'indirizzo);
- "App Android", per indicare il nome del pacchetto e l'impronta del certificato della App per Android (informazioni ricavabili dal portale di pubblicazione su Play Store);
- "App iOS", per inserire l'identificatore del bundle della App per IOS.

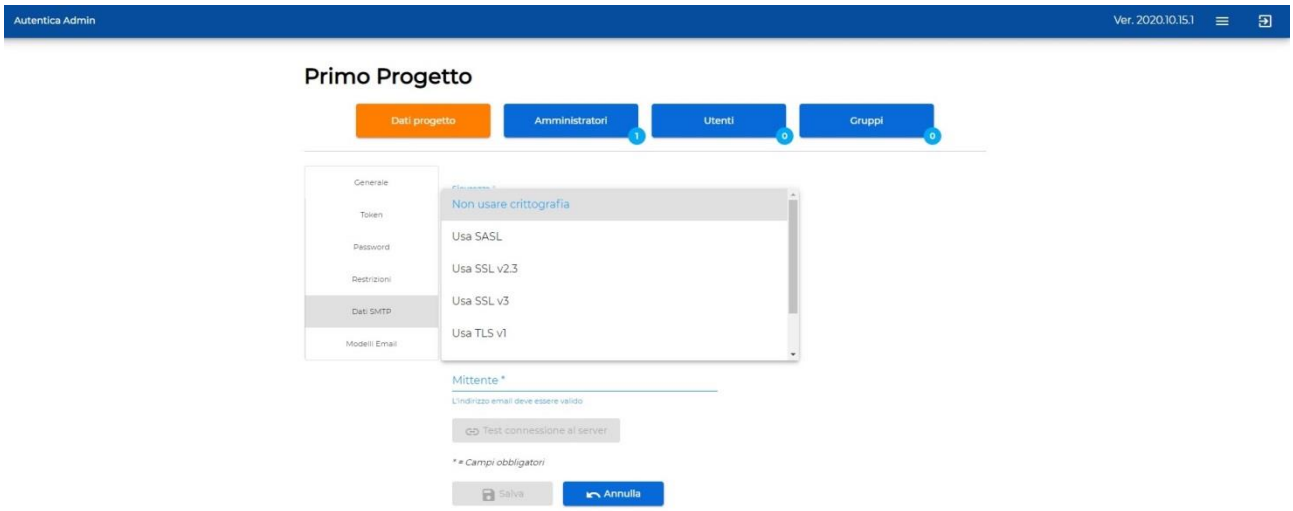
Ciascuno dei tipi di restrizione sopra elencati può essere inserito un numero di volte illimitato.



- Dati SMTP, dati del server di posta da utilizzare per le comunicazioni relative alla password. I dati sono personalizzabili; in mancanza di personalizzazione vengono utilizzate le impostazioni del server di posta di Autentica.



- Testi modelli email, testi delle email da inviare agli utenti. I modelli sono personalizzabili; in mancanza di personalizzazione vengono utilizzati i modelli standard di Autentica. Le casistiche che prevedono invio di email agli utenti sono i seguenti:
  - nuovo accesso, scadenza password, invio password temporanea, password dimenticata, modifica PIN, modifica telefono (invio otp via sms e invio otp via email), invio OTP via SMS.



È utile precisare che la personalizzazione del server di posta implica necessariamente che venga specificato il mittente dei messaggi da inviare; tale mittente deve essere un indirizzo di posta congruente con il server di posta.

Si specifica che una volta aggiunto, un progetto non potrà essere eliminato dal portale. Potrete contattarci a info@autenticazionesicura.it e a info@generazioneinformatica.it e indicare il progetto da disabilitare.

Amministratori

Nella lista in basso della dashboard sarà possibile aggiungere tutti gli amministratori che si desiderano e attribuire ad ognuno di essi i permessi desiderati:

- “gestione progetti”: consente di creare progetti e modificarne le informazioni;
- “gestione amministratori”: consente di aggiungere/rimuovere/modificare i dati degli amministratori e i loro permessi;

Non è obbligatorio selezionare una di queste due voci in quanto si può aggiungere un amministratore per dargli dei privilegi più specifici all’interno di un progetto e non in generale.

Sarà possibile popolare la lista degli amministratori anche prima di aver creato i progetti e, successivamente, assegnare ciascuno di essi al progetto desiderato con i relativi permessi:

- “gestione gruppi”: consente di creare ed eliminare gruppi;
- “gestione utenti”: consente di modificare/aggiungere utenze;
- “cancellazione utenti”: consente di eliminare in forma definitiva le utenze dal DB.

Per modificare le utenze appartenenti ad un gruppo e consentire la composizione del gruppo stesso dovrai associare l’amministratore al gruppo.

Ogni amministratore può essere amministratore più gruppi.

Gruppi

Se desideri che un amministratore possa eseguire soltanto alcune funzioni su delle specifiche utenze potrai creare dei gruppi ed associarli all'amministratore. In questo modo l'amministratore, nella sezione utenti, vedrà solamente le utenze del gruppo o gruppi che può gestire.

Un utente può far parte di più gruppi.

I gruppi non hanno altro scopo che quello di garantire una gestione degli utenti diversificata da amministratore a amministratore, non sono la definizione di ruoli o gruppi nell'applicativo finale. Esistono soltanto nell'ambiente di Autentica Admin.

Nella sezione "Gruppi", se l'amministratore possiede il permesso "gestione gruppi", vedrà tutti i gruppi con la possibilità di eliminarli o crearne dei nuovi.

Se non ha il permesso "gestione gruppi" vedrà tutti i gruppi senza la possibilità di eliminarli o di crearne dei nuovi. Dei gruppi ai quali non è stato associato vedrà la lista degli utenti che li compongono e la lista degli amministratori che li amministrano. Dei gruppi di cui è amministratore vedrà l'elenco degli utenti che lo compongono e l'elenco degli amministratori che lo amministrano, con la possibilità di modificare entrambi gli elenchi.

Utenti

Le utenze possono essere create singolarmente riempiendo manualmente i campi, oppure tramite una importazione massiva delle utenze.

I dati dell'utente sono:

- ID utente: **è l'identificativo dell'utente nel vostro applicativo finale, è l'unico dato del token che vi consentirà di riconoscere l'utente loggato**;
- Attivo: è un flag che consente di capire se l'utenza è attiva o meno e consente di disattivare l'utenza;
- username: può essere una mail oppure no;
- email: obbligatoria se c'è 2FA e lo username non è un indirizzo e-mail, facoltativo in caso contrario;
- password:
    - in progetti senza la 2FA in fase di inserimento, consigliamo comunque la valorizzazione del campo e-mail; se il campo è stato valorizzato, parte una mail con la password temporanea da cambiare al primo accesso nel vostro applicativo finale. Se invece non è stato specificato alcun indirizzo email la password temporanea viene visualizzata a video e sarà compito dell'amministratore riportarla all'utente, il quale dovrà cambiare quest'ultima al primo accesso nell'applicativo finale.

      NOTA: in quest'ultimo caso si deve tener presente che viene meno il rispetto della normativa privacy in quanto l'amministratore viene a conoscenza di una password, seppur temporanea, di un'altra identità;
    - in progetti con la 2FA, in fase di inserimento, parte una mail con la password temporanea da cambiare al primo accesso nel vostro applicativo finale in quanto l'indirizzo email è obbligatorio per inserire una utenza;

- PIN: obbligatorio nel caso di 2FA e generato automaticamente e spedito alla casella postale dell'utenza finale;
- Telefono: è obbligatorio nel caso di 2FA altrimenti non è visibile, ed è modificabile solo in un momento successivo alla registrazione, quando la password temporanea è stata cambiata;
- Roles: è un campo, ad inserimento libero, che permette di indicare il ruolo o i ruoli dell'utente nell'applicativo finale;
- mesi validità: specifica per quanti mesi la password sarà valida per la singola utenza; se è valorizzato viene preso tale valore e non quello stabilito a livello di progetto; se invece è vuoto viene preso il valore a livello di progetto;
- giorni preavviso: specifica quanti giorni prima della scadenza password verrà avvisato l'utente tramite una mail (se valorizzato vale questo, se viene lasciato vuoto vale il dato a livello di progetto);
- n. precedenti password (specifica il numero delle ultime password già utilizzate che non devono poter essere utilizzate nuovamente dall'utente).

Quando si crea un utente sarà possibile anche scegliere il gruppo in cui verrà inserito. Nella lista gruppi ai quali attribuire l'utenza in fase di creazione l'amministratore vedrà quelli a cui è associato.

Se l'amministratore ha "gestione utenti" ed è assegnato almeno ad un gruppo, nella sezione "Utenti" visualizzerà gli utenti dei gruppi ad esso associati. Se invece l'amministratore ha "gestione utenti" e non è assegnato ad alcun gruppo vedrà tutti gli utenti di tutti i gruppi.

Nella sezione "utenti" è presente il pulsante "Carica" che permette di inserire le utenze con l'upload di un file caricando le impronte delle password in corso di validità. Questo permette di non dover resettare le password a tutti gli utenti e di non spedire email a ogni utente in fase di importazione.

I dati da inserire nel file di caricamento utenti saranno:
- Id Utente: obbligatorio;
- Username: obbligatorio;
- e-mail: obbligatorio se c'è 2FA, facoltativo in caso contrario;
- n. telefono obbligatorio se c'è 2FA, facoltativo in caso contrario;
- impronta della password: obbligatoria, impronta in formato SHA256 della chiave utilizzata per il login;
- impronta del PIN: facoltativo, impronta in formato SHA256 del PIN.

In tale funzione si accettano solo impronte di password: ci solleviamo da ogni tipo di responsabilità in materia di "sicurezza password" in quanto non siamo in grado di verificare il rispetto della normativa GDPR avendo solamente l'impronta.
In questo caso assumiamo che l'amministratore abbia caricato l'email e il telefono delle utenze solamente dopo aver ricevuto una certificazione di essi da parte degli utenti; in tale caricamento esso è il solo responsabile del rispetto della sicurezza e della normativa privacy.

Approfondimento privilegi

Gestione Progetti

Permette di creare, eliminare, modificare i dati di un progetto.

Se un amministratore ha GESTIONE_PROGETTI valorizzato, vede tutti i progetti nella dashboard; all'interno del singolo progetto potrà modificare i dati di esso.

Se non ha GESTIONE_PROGETTI nella dashboard vede quelli a cui è stato abbinato; all'interno del singolo progetto non vedrà la scheda "dati progetto".

Gestione Amministratori

Lista amministratori nella dashboard

Se mi loggo come super-amministratore vedo ogni amministratore con la possibilità di cambiarne mail e permessi, mentre di me stesso potrò cambiare l'indirizzo email soltanto. Potrò anche creare amministratori e eliminarli.

Se mi loggo come amministratore con il permesso "gestione amministratore" vedrò ogni amministratore e potrò cambiarne l'indirizzo email e i permessi, mentre di me stesso potrò cambiare solo l'indirizzo email. Potrò anche creare ed eliminare amministratori.

Non è obbligatorio selezionare un flag di abilitazione sull'amministratore in questa lista perché potrebbe non essere abilitato alla gestione progetti e amministratori ma essere abilitato a qualche funzione all'interno di un progetto.

Se mi loggo come amministratore che non ha la "gestione amministratori" non vedrò la lista amministratori. Di me stesso vedrò i dati nel profilo e potrò modificare solo l'indirizzo email.

Lista amministratori dentro i progetti

Dentro ogni progetto è presente la scheda Amministratori che è visibile solamente a chi ha il permesso "gestione amministratori". Chi ha la "gestione amministratori" vede tutti gli amministratori di cui può cambiare i permessi (relativi al progetto). Vede anche sé stesso ma in sola lettura.

Gestione Utenti

Permette di modificare i dati degli utenti e di aggiungerne dei nuovi.

Se ho la "gestione utenti" vedo la scheda "Utenti" dentro al progetto.

Se ho la "gestione utenti" e amministro almeno un gruppo posso modificare e vedere gli utenti di quel/i gruppo/i.

Se ho la "gestione utenti" e non amministro almeno un gruppo posso vedere e modificare tutti gli utenti.

Se non ho la "gestione utenti" e amministro almeno un gruppo posso comporre quel/i gruppo/i ma non posso modificarne gli utenti in quanto non vedrò neppure la scheda "Utenti".

Se non ho la “gestione utenti” e non amministro alcun gruppo non vedrò alcun utente e non potrò comporre alcun gruppo.

Gestione Gruppi

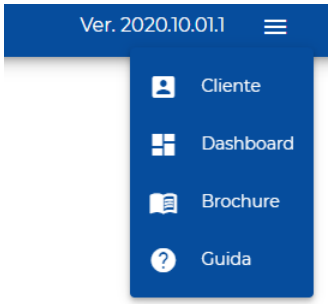
Permette di creare ed eliminare i gruppi.

Quando creo un gruppo automaticamente sono amministratore di esso e posso comporlo.

Per aggiungere amministratori al gruppo devo avere la “gestione gruppi” e la “gestione amministratori”.

Documentazione per sviluppatori

La documentazione tecnica rivolta agli sviluppatori, con l’elenco completo delle chiamate e dei parametri, è disponibile direttamente in Autentica Admin col menu Guida.



Nella Guida è possibile trovare un’introduzione alle tecniche usate da Autentica, l'elenco di tutte le funzioni richiamabili con parametri, codici di errori ed esempi di utilizzo, e due componenti funzionanti e scaricabili che sono utilizzabili così come sono o possono essere esplorati a titolo esemplificativo.