Utilizzo SPID/CIE per le Scuole

MANUALE

Integrazione con il Gateway delle Identità

INDICE

INDICE DELLE FIGURE

1 INTRODUZIONE

1.1 Scopo del documento

Il presente documento è una guida pensata per supportare le scuole che vogliono permettere ai propri utenti di accedere tramite SPID e CIE nelle proprie applicazioni o portali istituzionali, utilizzando il gateway delle identità fornito dal Ministero dell'Istruzione e del Merito.

In particolare, il documento fornisce anche gli strumenti per un'integrazione tra il Gateway delle Identità con WordPress, prodotto di riferimento della comunità open source e tra i più utilizzati dalle Pubbliche Amministrazioni come menzionato su Docs Italia.

1.2 Applicabilità

La guida è rivolta alle scuole statali sede di direttivo che intendono avvalersi del Gateway delle Identità (eID-Gateway) per l'accesso con SPID e CIE all'interno delle applicazioni e siti della scuola.

2 Cos'è il Gateway delle Identità del MIM

In considerazione degli obblighi introdotti per le pubbliche amministrazioni con il Decreto-legge Semplificazione (D.L. 76/2020) convertito in legge l'11/09/2020 (120/2020), dal 28 febbraio 2021 tutte le amministrazioni devono garantire l'accesso ai servizi digitali da parte dei cittadini esclusivamente con credenziali SPID (Sistema Pubblico di Identità Digitale) o CIE (Carta d'Identità Elettronica).

In questo scenario anche le Istituzioni Scolastiche che offrono alle famiglie e agli studenti i propri servizi digitali, sono tenute a adottare le misure previste dalla norma.

Il Ministero dell'Istruzione e del Merito si è accreditato presso l'AGID come soggetto aggregatore di servizi pubblici in modalità "full", ovvero mette a disposizione delle Istituzioni scolastiche (soggetti aggregati) una piattaforma di autenticazione tramite SPID, CIE ed eIDAS attraverso il componente chiamato Gateway delle Identità o eID-Gateway. I soggetti aggregatori sono pubbliche amministrazioni o privati che offrono a terzi (soggetti aggregati) la possibilità di rendere accessibili tramite identità digitali i rispettivi servizi.

Il processo di adesione come aggregato è rivolto a tutte le Istituzioni scolastiche statali sedi di Direttivo dislocate su tutto il territorio nazionale, che vogliono integrarsi o che utilizzano fornitori di pacchetti locali che già si sono integrati con il componente eID-Gateway fornito dal Ministero dell'Istruzione e del Merito, in qualità di soggetto aggregatore.

2.1 Modalità di adesione delle scuole

L'Istituzione scolastica, tramite il proprio Dirigente scolastico, con le funzioni messe a disposizione sull'applicazione SIDI "Gestione Aggregazione Scuola", dovrà dichiarare la propria adesione come "soggetto aggregato" al Gateway delle Identità.

Aggregarsi al Gateway delle Identità, vuole dire essere riconosciuta da AGID/Ministero dell'Interno come una istituzione scolastica che andrà a usufruire di questo sistema per far accedere con SPID/CIE e permetterà, una volta aggregata al Gateway, di effettuare delle richieste di autenticazione a nome del proprio Istituto scolastico.

Inoltre, aggregandosi, il Gateway delle Identità si farà carico di tutte le operazioni burocratiche connesse con i fornitori dei servizi garantendo l'accesso ai cittadini attraverso identità digitali conformemente al Decreto-legge.

Con l'utilizzo del Gateway del Ministero dell'Istruzione e del Merito, la scuola non dovrà avviare in autonomia il processo di adesione al Sistema Pubblico di Identità Digitale risparmiando risorse in termini di adempimenti burocratici per la definizione dei rapporti con AgID e delle competenze tecnologiche e amministrative. Inoltre, grazie all'integrazione con SPID e CIE le scuole abbandonano i diversi sistemi di autenticazione gestiti localmente, risparmiando i costi derivati dal rilascio e la manutenzione delle credenziali.

3 Integrazione con il Gateway delle Identità del MIM

L'Istituzione scolastica, tramite il proprio dirigente scolastico (DS), con le funzioni messe a disposizione sull'applicazione SIDI "Gestione Aggregazione Scuola", potrà ottenere le informazioni tecniche utili alla propria applicazione o eventuale sito istituzionale per integrarsi con il Gateway delle Identità.

L'integrazione è possibile grazie all'utilizzo di un protocollo di comunicazione standard denominato OpenIDConnect che permette di autenticarsi attraverso un servizio decentralizzato.

3.1 Il protocollo di comunicazione OpenId Connect

OpenID Connect (OIDC) è un protocollo di autenticazione che permette a diverse applicazioni di verificare l'identità di un utente basandosi su un servizio di autenticazione di terze parti. È costruito sopra OAuth 2.0, che è un framework per l'autorizzazione. OAuth 2.0 elimina la necessità di condividere le credenziali con terze parti, garantendo la sicurezza e la privacy. Utilizza token di accesso per concedere l'autorizzazione specifica per l'accesso a determinate risorse.

OIDC utilizza standard di sicurezza avanzati per proteggere le informazioni degli utenti e garantire che i dati condivisi siano autentici e non manipolati. Essendo un protocollo standardizzato, permette l'interoperabilità tra diversi sistemi e piattaforme.

In sintesi, OpenID Connect è un protocollo che consente agli utenti di accedere a diverse applicazioni e servizi online utilizzando un'unica identità digitale, migliorando l'esperienza utente e aumentando la sicurezza.

L'applicazione della scuola, quindi dovrà avere un client OIDC per comunicare con il Gateway delle Identità che sarà riconosciuto tramite clientID e secret.

In questo documento verrà indicato come ottenere le credenziali per l'integrazione (clientId e secret) attraverso un'apposita funzione presente nell'applicazione SIDI "Gestione aggregazione scuole". Il prerequisito necessario è che la scuola abbia correttamente terminato la procedura di aggregazione.

Inoltre, verrà riportato un esempio di come integrare l'autenticazione SPID/CIE attraverso il Gateway delle identità all'interno di un sito wordpress.

3.2 Gestione Aggregazione Scuole - SIDI

Nell'applicazione SIDI "Gestione aggregazione scuole" la funzione di Gestione Client permette alla scuola di creare un client con protocollo OpenID Connect, necessario per l'integrazione con il Gateway delle Identità del MIM, e permettere un'autenticazione con SPID,CIE o eIDAS. Il client potrà essere creato soltanto dopo che la scuola si sia aggregata,

per tanto il bottone AGGIUNGI sarà inibito nel caso in cui quest'ultima non sia aggregata. Il client dovrà essere creato quando è la scuola stessa a gestire servizi o applicazioni che devono permettere questa tipologia di autenticazione.

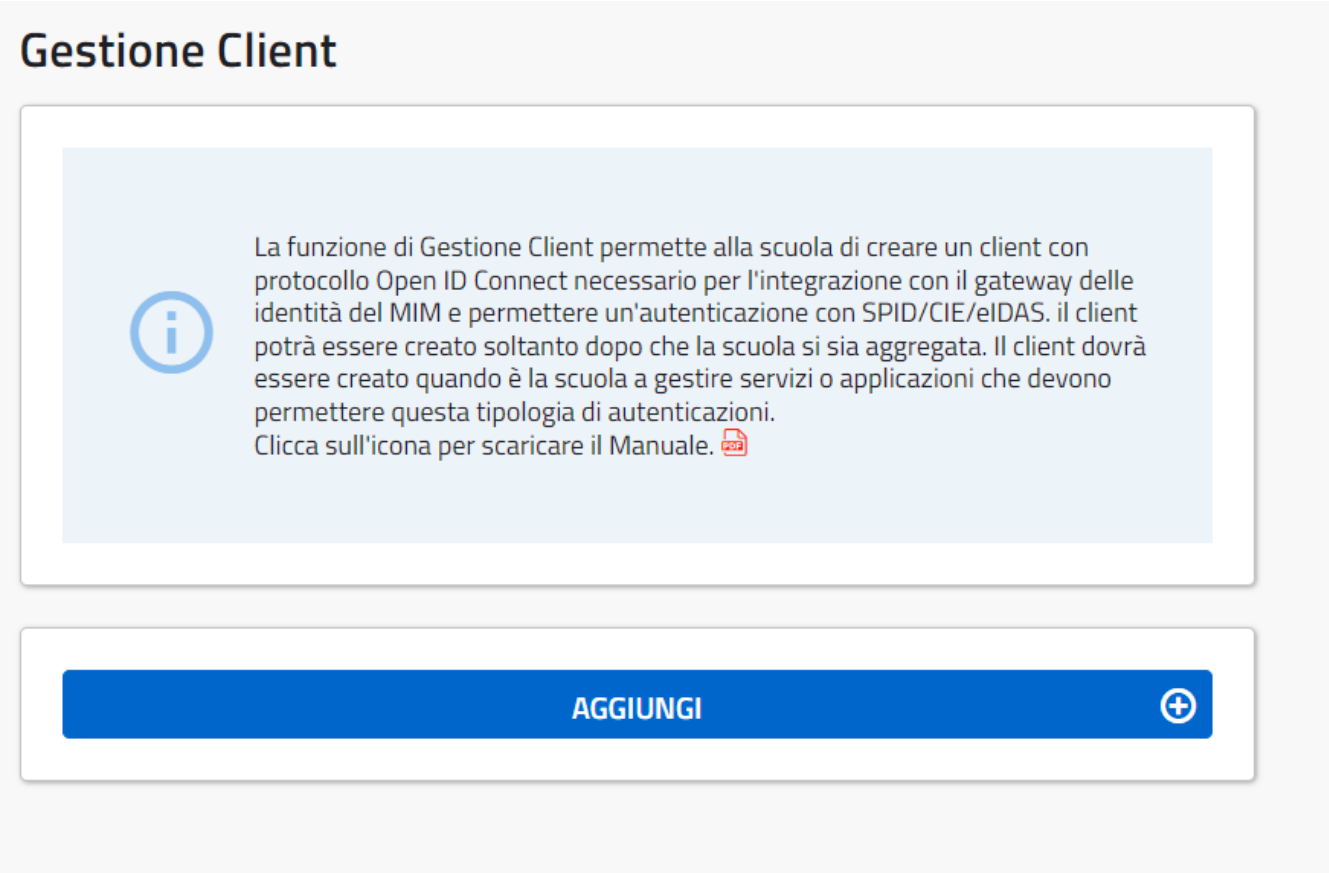

Figura 1: Gestione Client

Dopo aver cliccato sul bottone "Aggiungi" si aprirà la pagina "Inserimento Client" in cui è possibile inserire i dati del client, indicando le informazioni necessarie.

3.2.1 Registrazione Client OIDC

Attraverso la funzione di "Inserimento Client" dell'applicazione SIDI "Gestione Aggregazione Scuola", è possibile registrare un proprio client al fine di ottenere le informazioni tecniche (clientID e Secret) per comunicare con il gateway delle identità con protocollo OIDC.

3.2.1.1 Dati generali

Nella sezione Dati Generali, "Descrizione client" rappresenta il nome che si vuole dare al client che si sta per inserire, è necessario indicare anche la tipologia di accesso che si vorrà utilizzare (SPID, CIE, EIDAS).

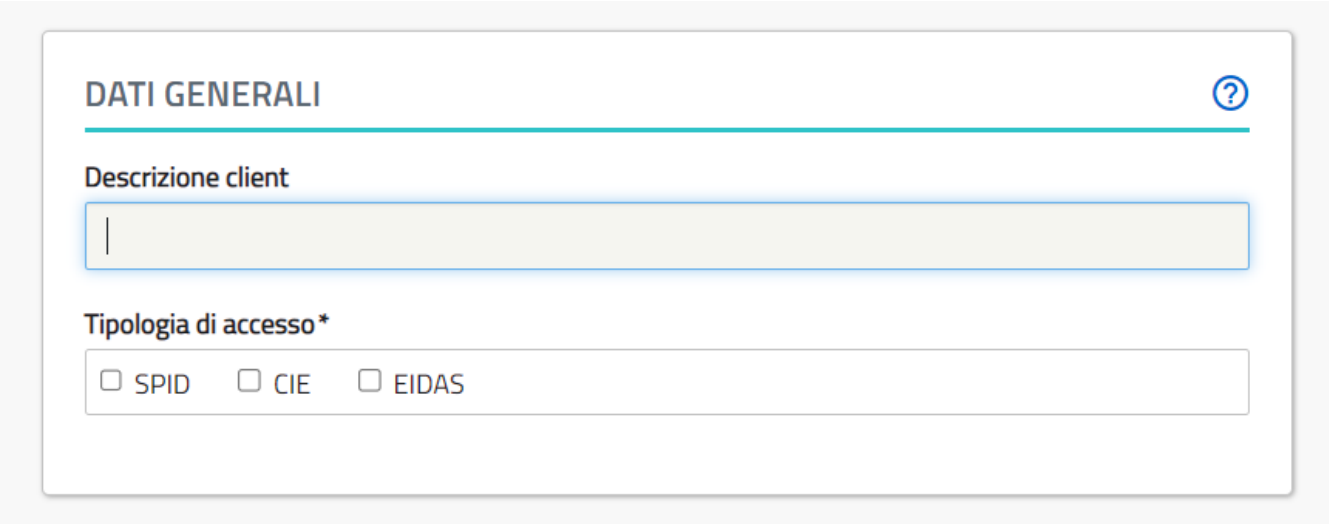

Figura 2: Inserimento Client – Dati Generali

È obbligatorio indicare almeno una tipologia di accesso tra quelle indicate.

3.2.1.2 Elenco redirect uri

In questa sezione devono essere inseriti i servizi (definiti per url) per cui il client deve garantire l'accesso agli utenti.

Si richiede quindi di inserire tutti i servizi su cui l'utente potrà accedere dopo aver effettuato l'autenticazione tramite identità digitale.

Nel caso in cui i servizi sono mascherati da un unico punto di accesso, come ad esempio un portale, inserire solamente l'url principale. L'autenticazione verrà richiesta solo per l'accesso al portale e l'utente autenticato potrà usufruire di tutti i servizi offerti.

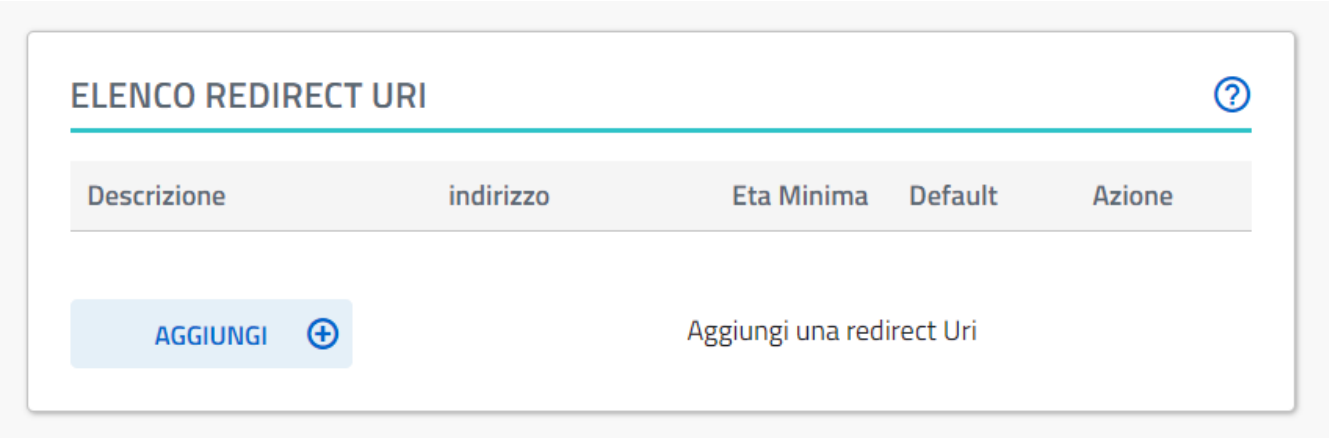

Figura 3: Inserimento Client – Redirect uri

Le redirect uri, in sostanza, rappresentano i punti di ingresso al client ai quali il gateway ridirigerà le informazioni dell'utente che ha effettuato l'accesso.

Dopo aver cliccato sul bottone aggiungi si aprirà la seguente finestra dove sarà possibile inserire i dati del servizio.

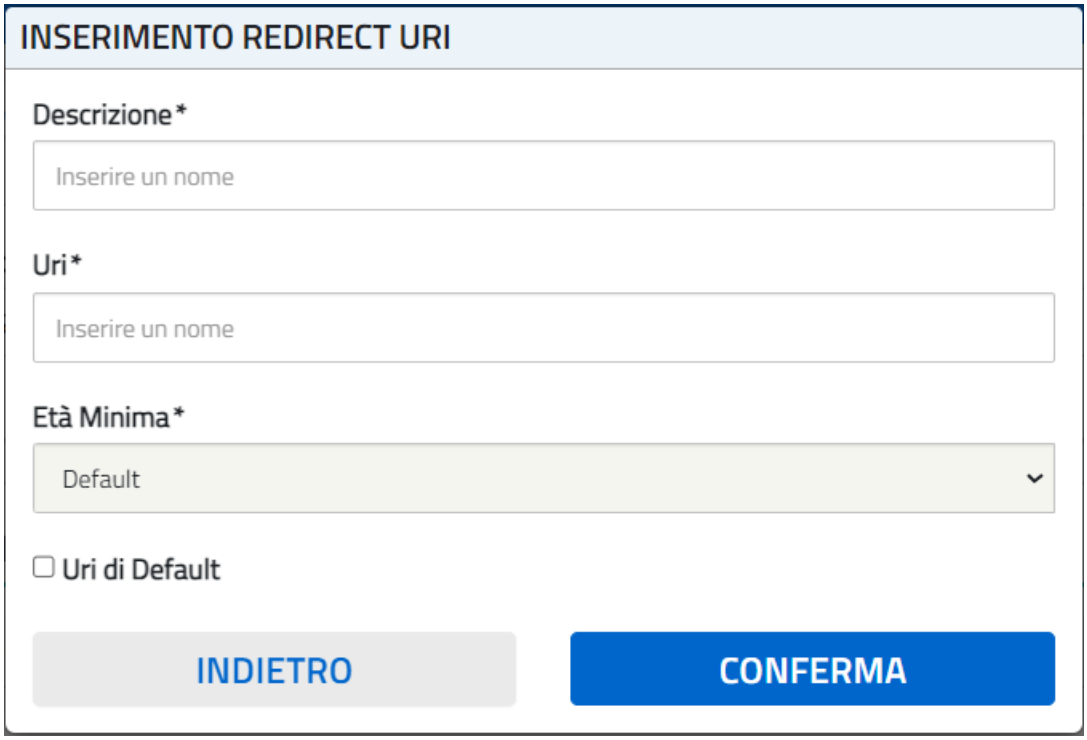

Figura 4: Inserimento Client – PopUp inserimento uri

Queste url rappresentano il servizio al quale si vuole dare l'accesso, specificando un'età minima per l'utilizzo del servizio.

3.2.1.3 Attributi

In questa sezione è possibile decidere quale set di informazioni verranno restituite dopo la fase di autenticazione.

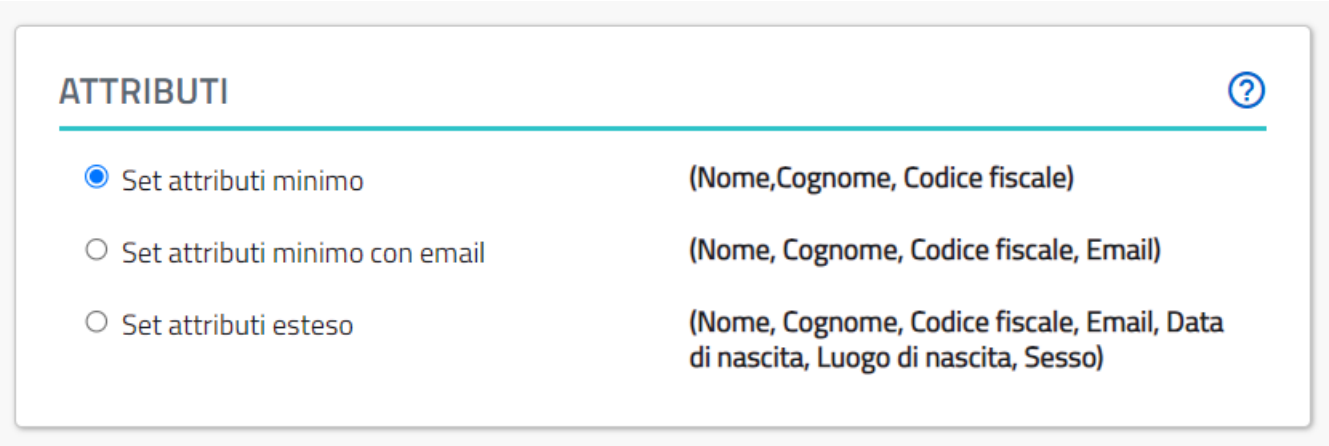

Figura 5: Inserimento Client – Attributi

Dopo aver inserito tutte le informazioni necessarie, tramite il bottone "Salva client" quest'ultimo verrà inserito e verranno visualizzate le informazioni del client necessarie per l'integrazione con il Gateway delle Identità.

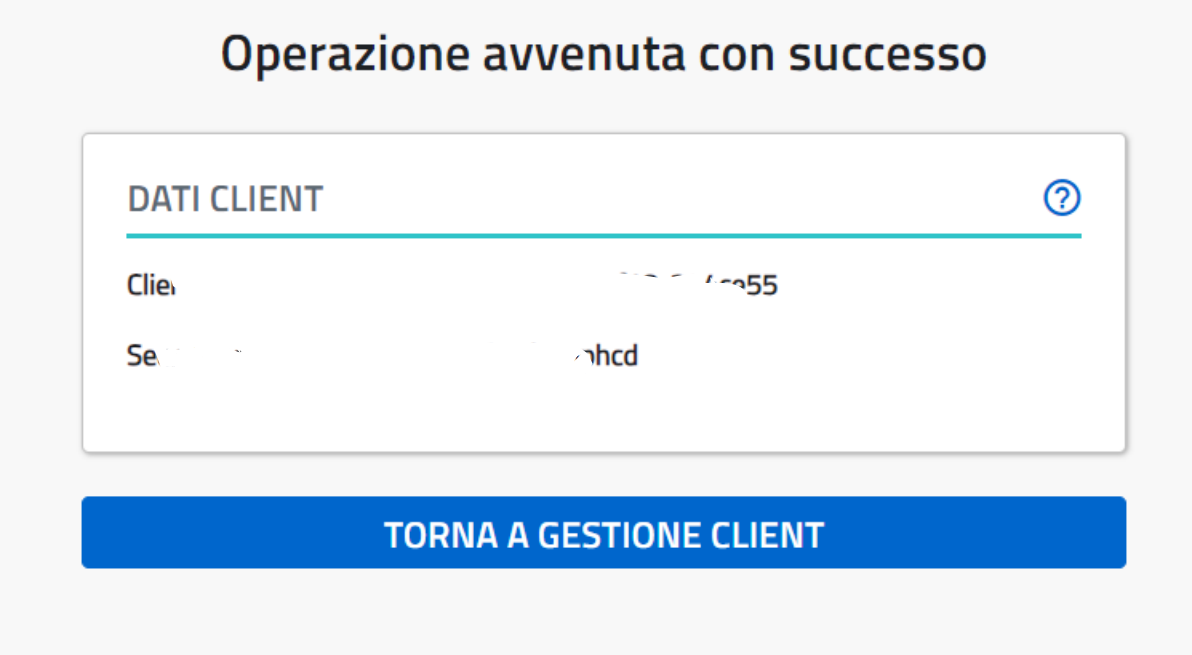

Figura 6: Inserimento Client – Dati del client

N.B. È necessario salvare le informazioni relative a client id e secret perché non saranno più visualizzabili.

Cliccando sul bottone "Torna a gestione client" verremo reindirizzati alla pagina di "Gestione client" dove troveremo l'elenco dei client inseriti.

3.2.1.4 Visualizza client

Tramite il menu a tendina e cliccando "Visualizza" sarà possibile visualizzare le informazioni del client inserite precedentemente.

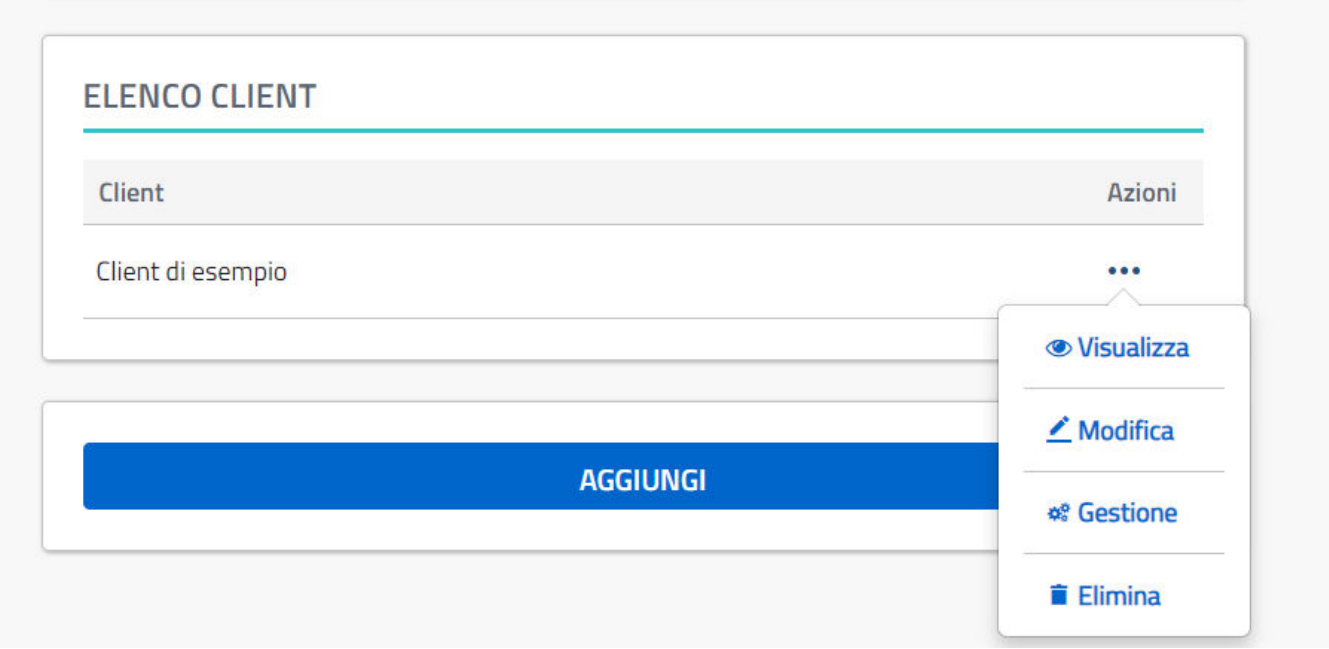

Figura 7: Elenco client inseriti

Dopo aver cliccato su "Visualizza" verrete reindirizzati nella pagina contenente le informazioni del client.

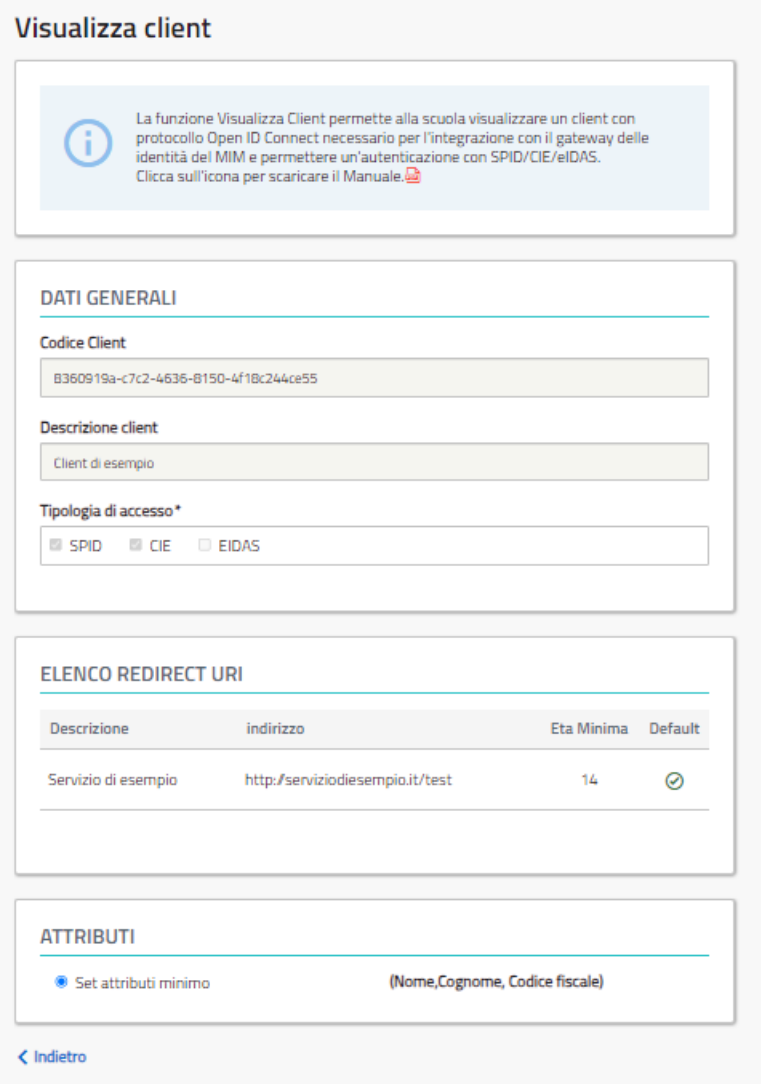

Figura 8: Visualizza Client

3.2.2 Modifica client

Tramite il menu a tendina e cliccando su "Modifica" sarà possibile modificare alcune informazioni del client.

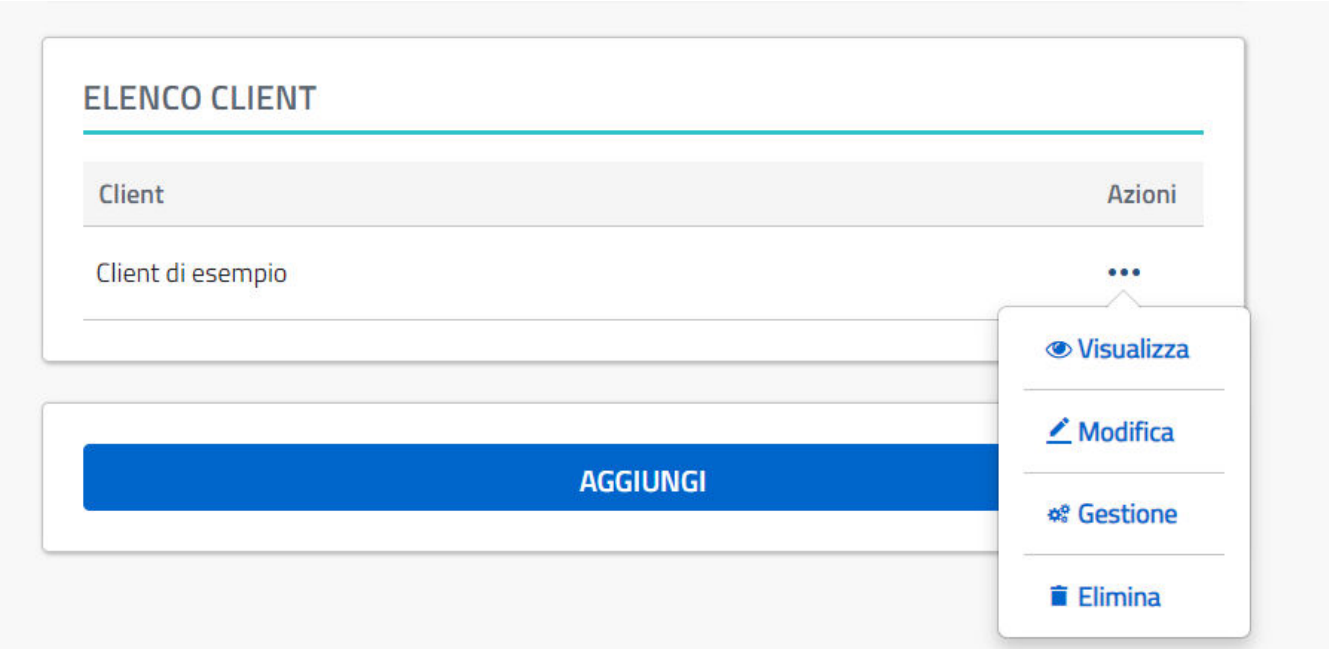

Figura 9: Modifica Client

Dopo aver cliccato su "Modifica" verrete reindirizzati nella pagina contenente le informazioni del client. In questa sezione è possibile modificare:

- la Tipologia di accesso

Figura 10: Modifica Client – Tipologia di accesso

- l'elenco delle redirect uri, aggiungendo o eliminando i servizi tramite i relativi bottoni

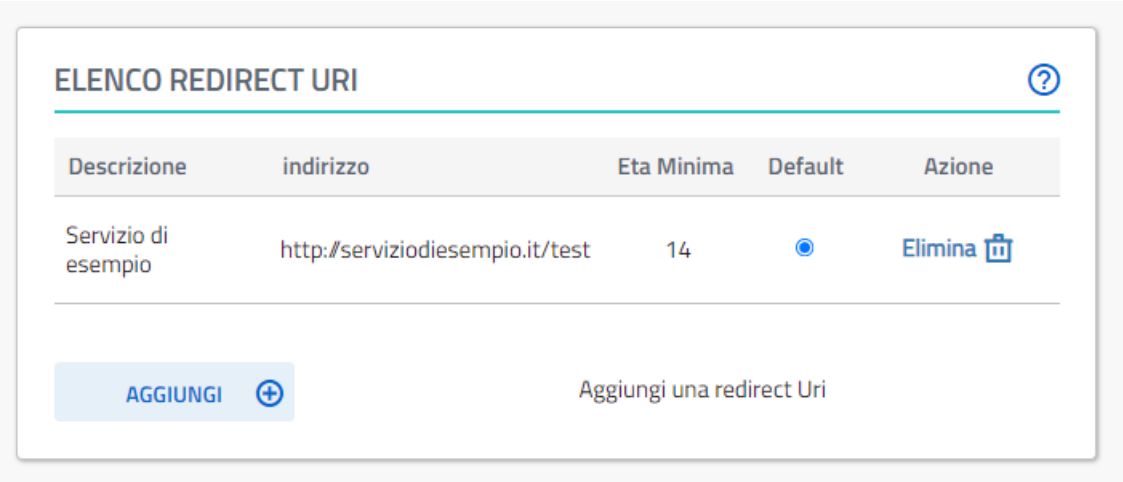

Figura 11: Modifica Client – Redirect uri

- il set di attributi

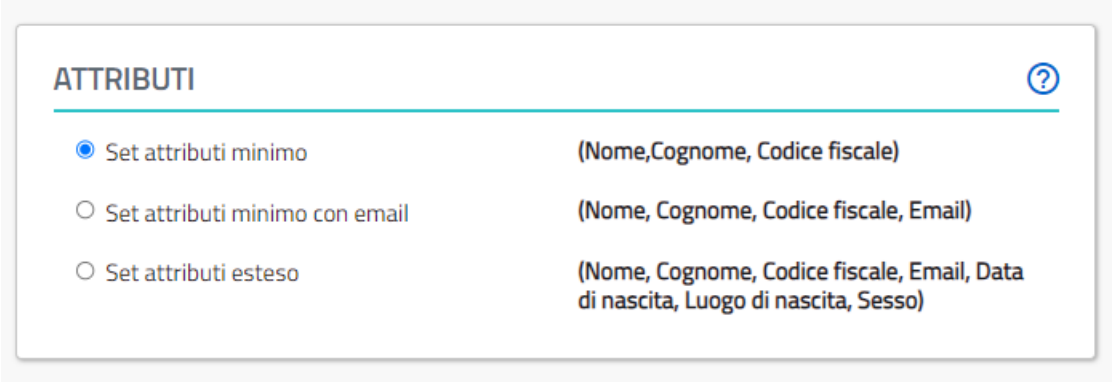

Figura 12: Modifica Client – Attributi

Tramite il bottone "Salva client" posto alla fine della pagina le modifiche apportate verranno salvate.

3.2.3 Gestione Secret

Tramite il menu a tendina e cliccando su "Gestione" sarà possibile verificare se la secret del client corrisponde a quella indicata nell'apposito campo e rigenerarla in caso sia andata perduta o risulti non valida.

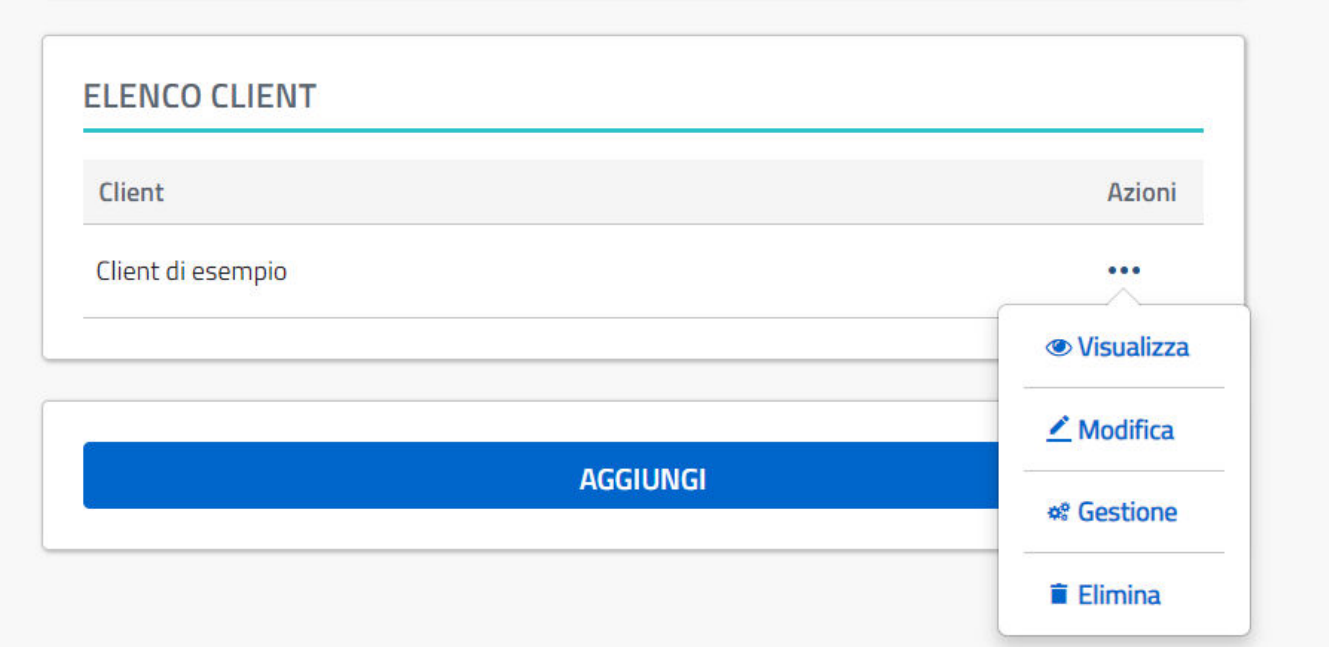

Figura 13: Gestione Client

Dopo aver cliccato su "Gestione" verrete reindirizzati nella pagina contenente le funzioni che permettono di verificare o rigenerare la secret del client.

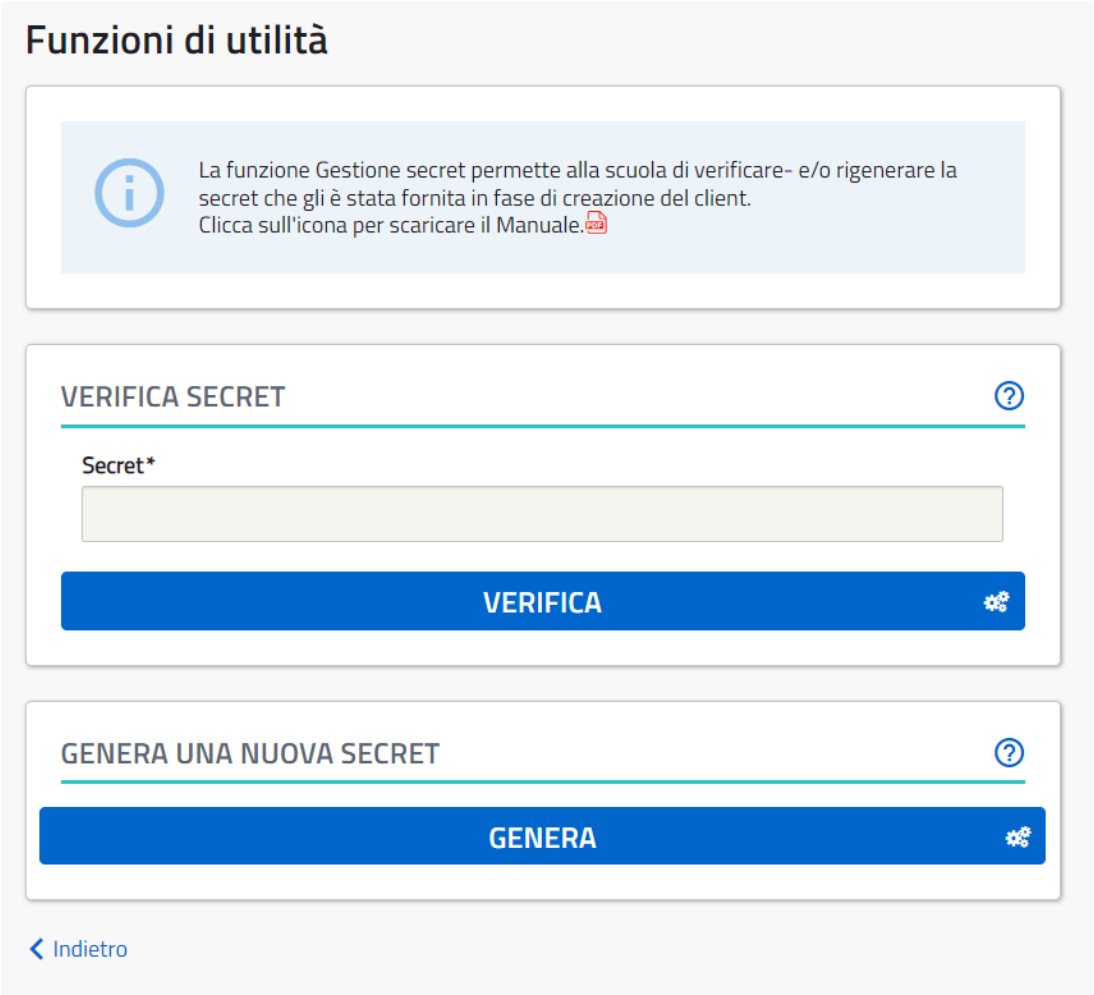

Figura 14: Gestione Client

3.2.4 Elimina client

Tramite il menu a tendina e cliccando su "Elimina" sarà possibile eliminare il client selezionato.

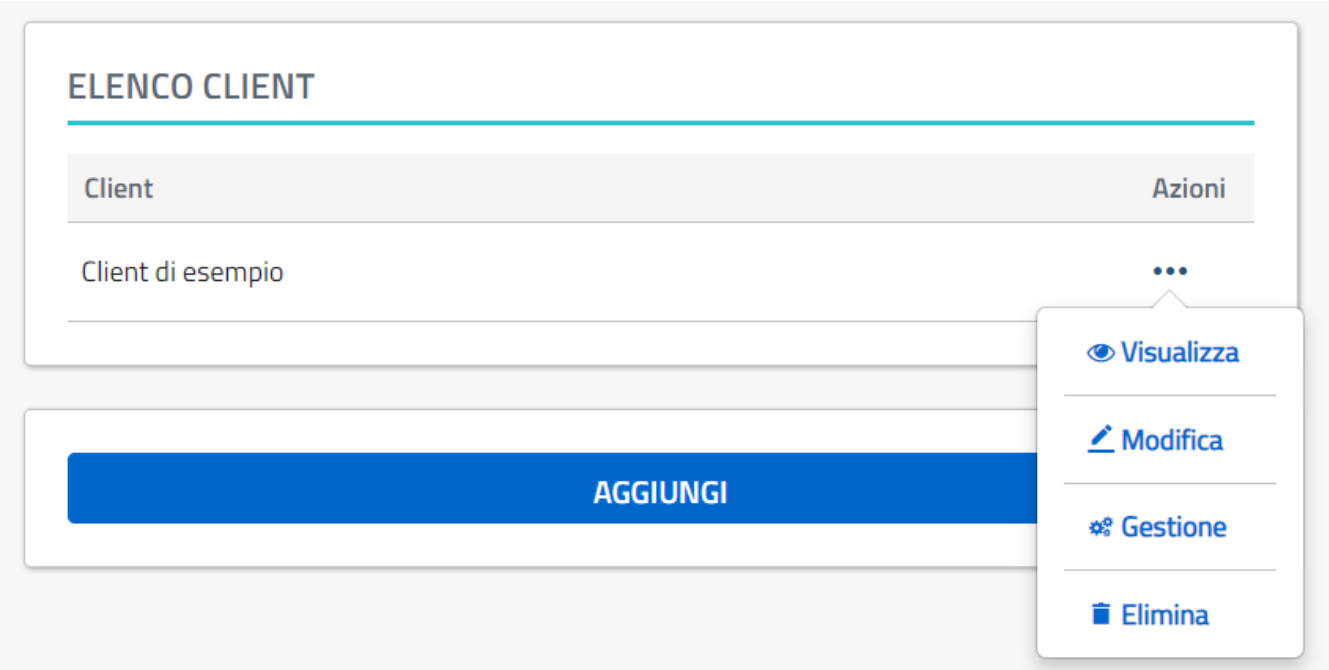

Figura 15: Elimina Client

4 Esempio di integrazione

Nei capitoli successivi verrà mostrato, a scopo di esempio, come integrare le credenziali ottenute seguendo le istruzioni del capitolo precedente**Errore. L'origine riferimento non è stata trovata.**, allo scopo di integrare l'accesso con SPID/CIE all'interno di un sito web scolastico realizzato con Design Scuole Italia.

4.1 WordPress

WordPress è un sistema di gestione di contenuti (CMS) open source e gratuito basato su PHP e MySQL. Si tratta di una interfaccia utente web-based per la creazione, la pubblicazione e l'aggiornamento di contenuti.

Rilasciato nel 2004, WordPress è diventato il CMS più utilizzato a livello globale: da allora viene costantemente aggiornato, per migliorarne facilità d'uso e funzionalità. Uno degli ultimi update ha introdotto l'editor a blocchi Gutenberg, che ha rivoluzionato l'esperienza di gestione dei contenuti per gli utenti del CMS.

L'aspetto grafico della pagina web viene definito dal tema, un template che può essere personalizzato o modificato a seconda delle esigenze. Inoltre, le funzionalità base di WordPress possono essere ampliate grazie ai plug-in, pacchetti di funzionalità che possono essere installati con facilità.

Questo semplifica la gestione dei contenuti anche da parte di chi non ha conoscenze specifiche in ambito informatico. Inoltre, l'ampia comunità di sviluppatori e utenti che gravita attorno a WordPress assicura la più ampia disponibilità di temi, plugin e supporto per la loro implementazione.

4.2 Design Scuole Italia

Design Scuole Italia è un tema WordPress per i siti delle Scuole Italiane rilasciato da Designers Italia del Team per la Trasformazione Digitale in seno alla Presidenza del Consiglio dei Ministri, in accordo con il **MIM**, nel rispetto dell'autonomia scolastica e con l'obiettivo di creare un prodotto in grado di rispondere ai principali bisogni di tutte le scuole.

Le informazioni per lo scarico e l'installazione del template scuola sono disponibili attraverso il seguente link:

https://developers.italia.it/it/software/github.com/italia/design-scuole-wordpress-theme

4.3 Client OIDC per WordPress

Dallo Store di WordPress è possibile scaricare un plugin per integrare nel proprio sito istituzionale un client OIDC.

Per fare questo è necessario accedere a WordPress utilizzando le credenziali di amministratore. Una volta effettuato l'accesso, verrà visualizzata la dashboard principale.

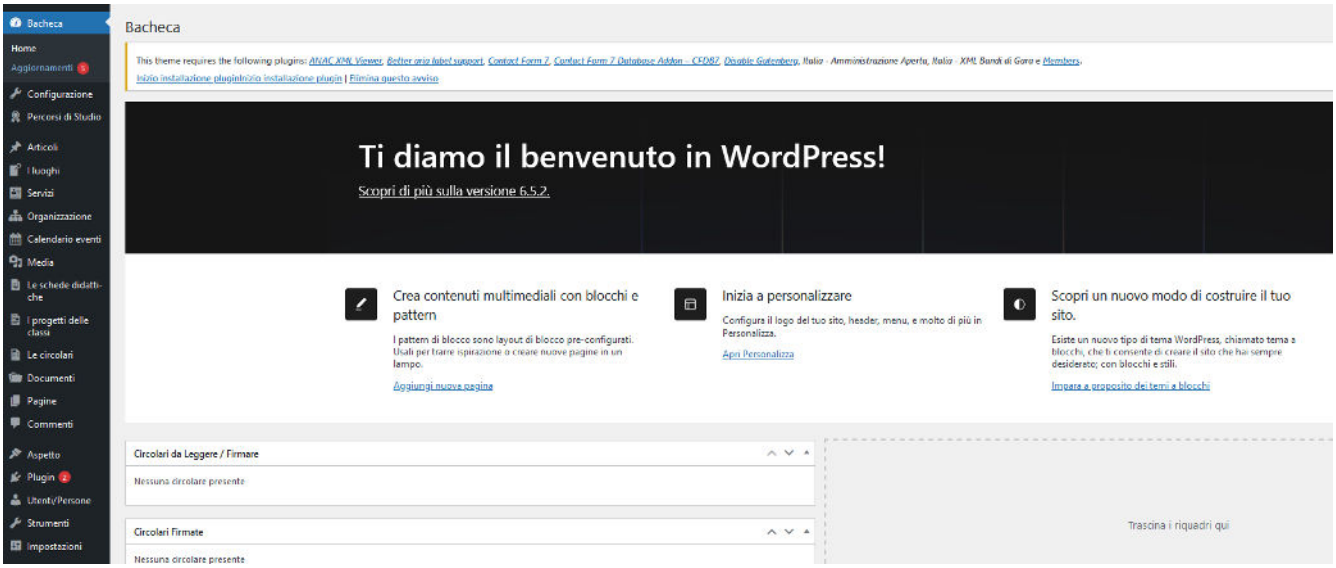

Figura 16: Dashboard principale di Wordpress

Nella barra laterale sinistra della dashboard, è presente una voce di menu chiamata "Plugin". Passando il mouse su questa voce viene visualizzato un menu a discesa, su quest'ultimo cliccare su "Aggiungi un nuovo Plugin".

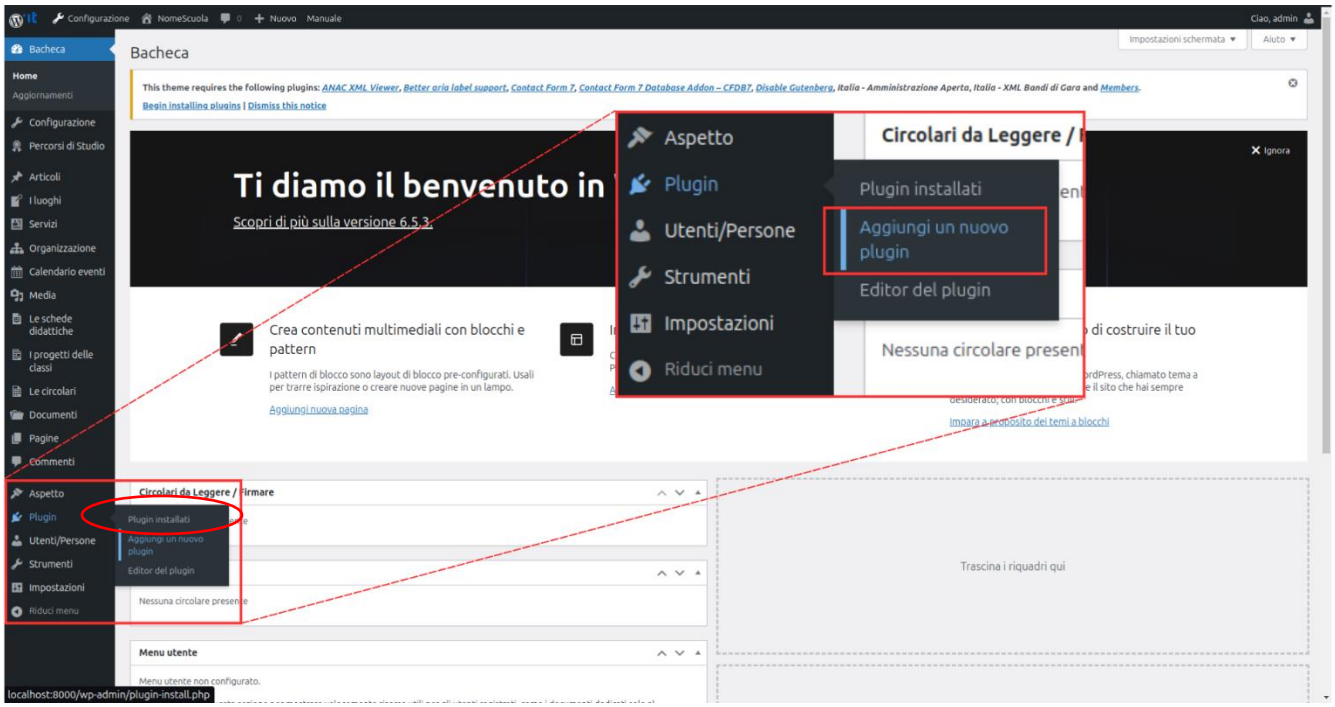

Figura 17: Aggiungi nuovo plugin

Dopo aver cliccato su "Aggiungi un nuovo plugin" ci troveremo su questa schermata:

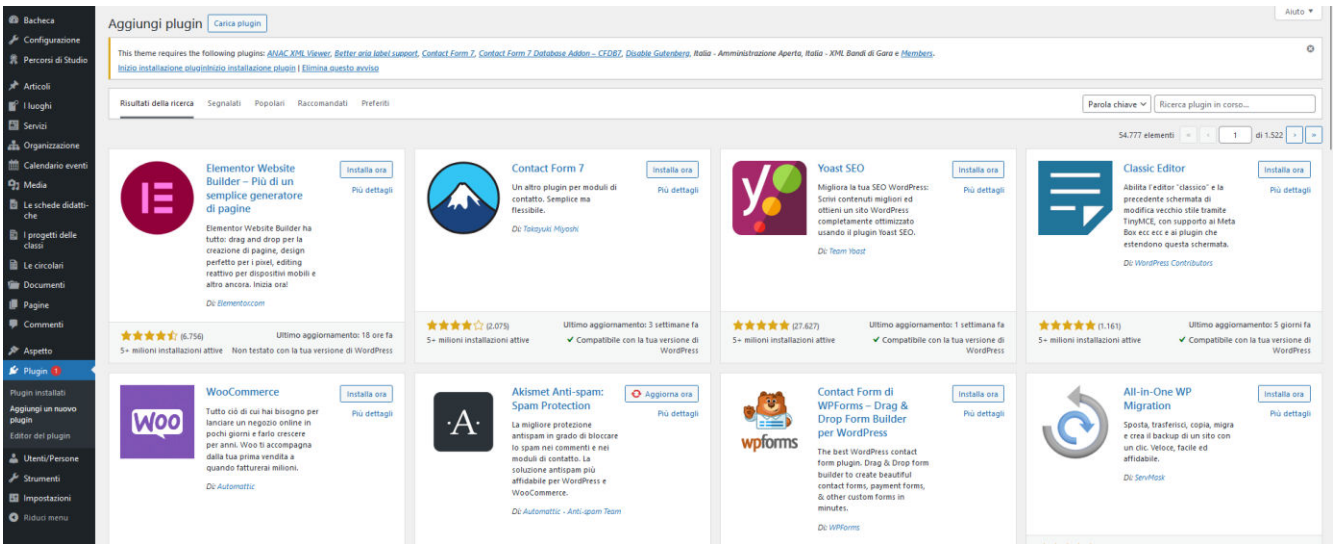

Figura 18: Pagina elenco plugin

Nel campo “Ricerca plugin” situato in alto a destra della schermata scrivere “OpenID Connect”:

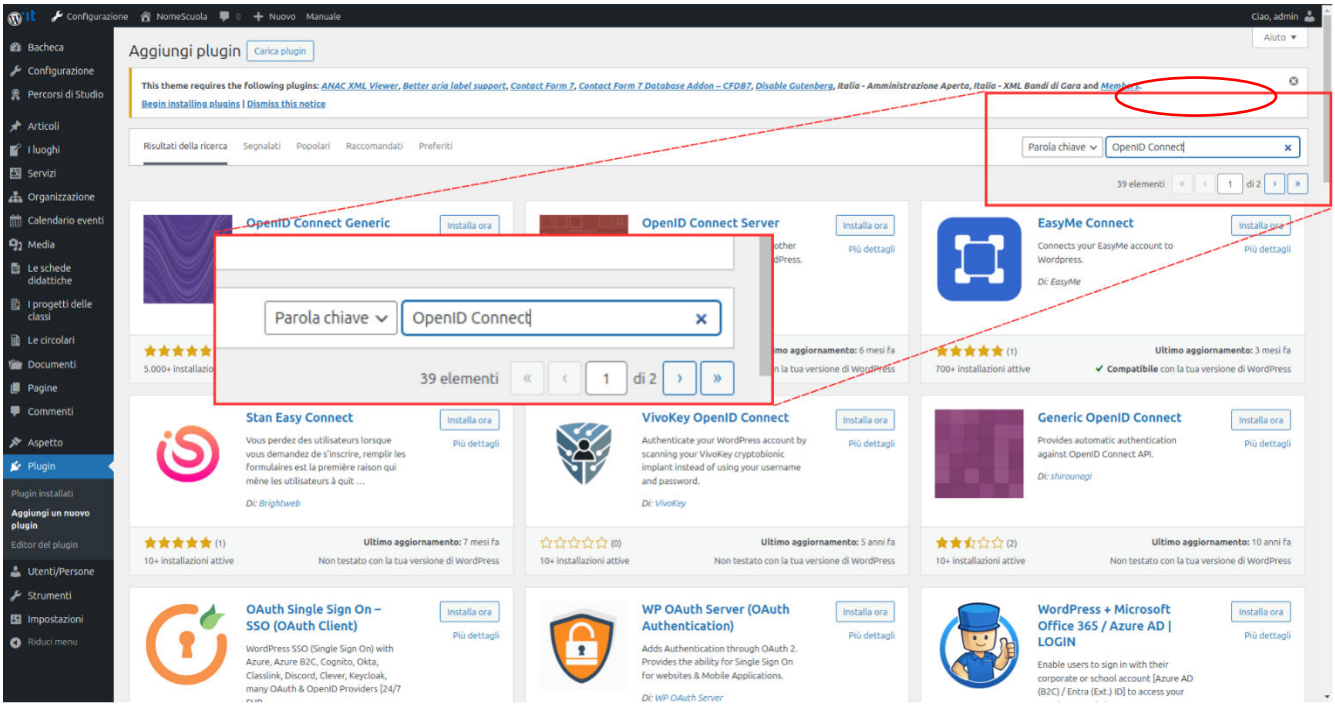

Figura 19: Ricerca plugin

Una volta effettuata la ricerca, verranno mostrati una serie di plugin. Successivamente fai clic sul pulsante “Installa ora” del plugin “OpenID Connect Generic Client” e attendere che l’installazione sia conclusa.

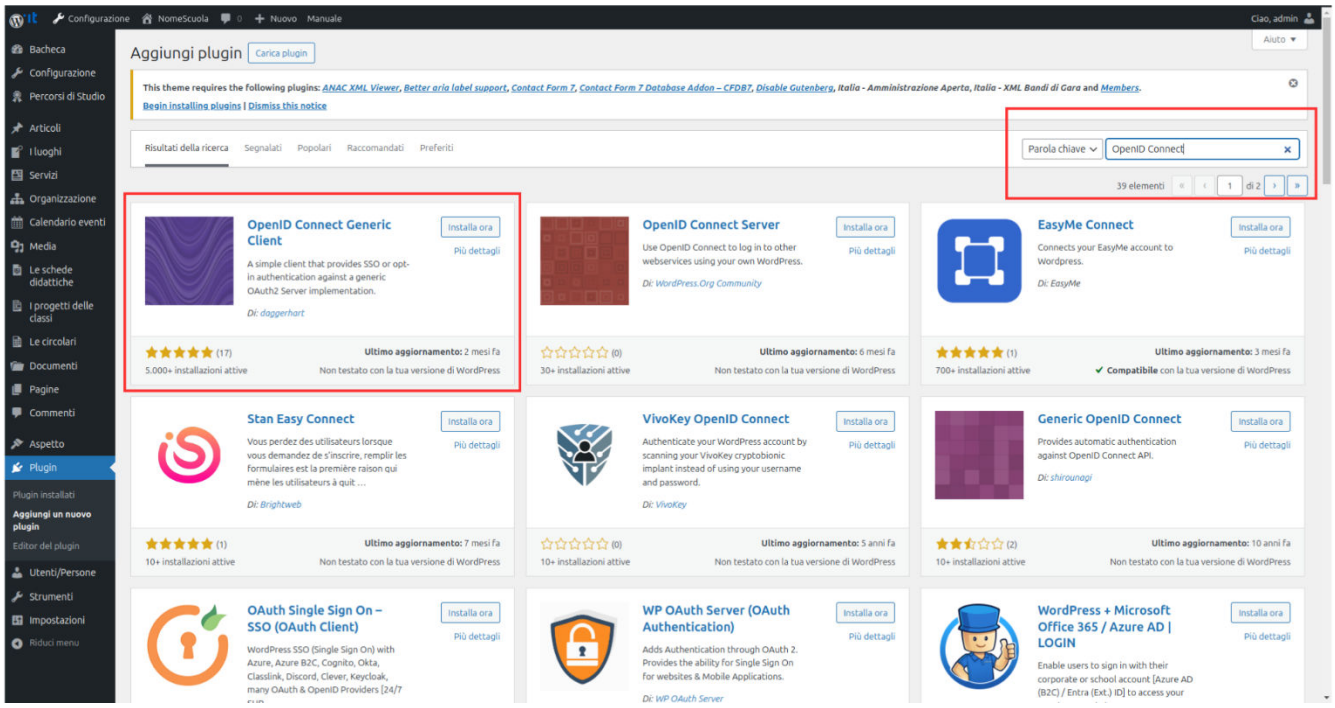

Figura 20: Selezione plugin

Dopo aver cliccato, aspettiamo che il plugin venga installato. Dopo l'installazione cliccare sullo stesso bottone che avrà preso il nome di "Attiva"

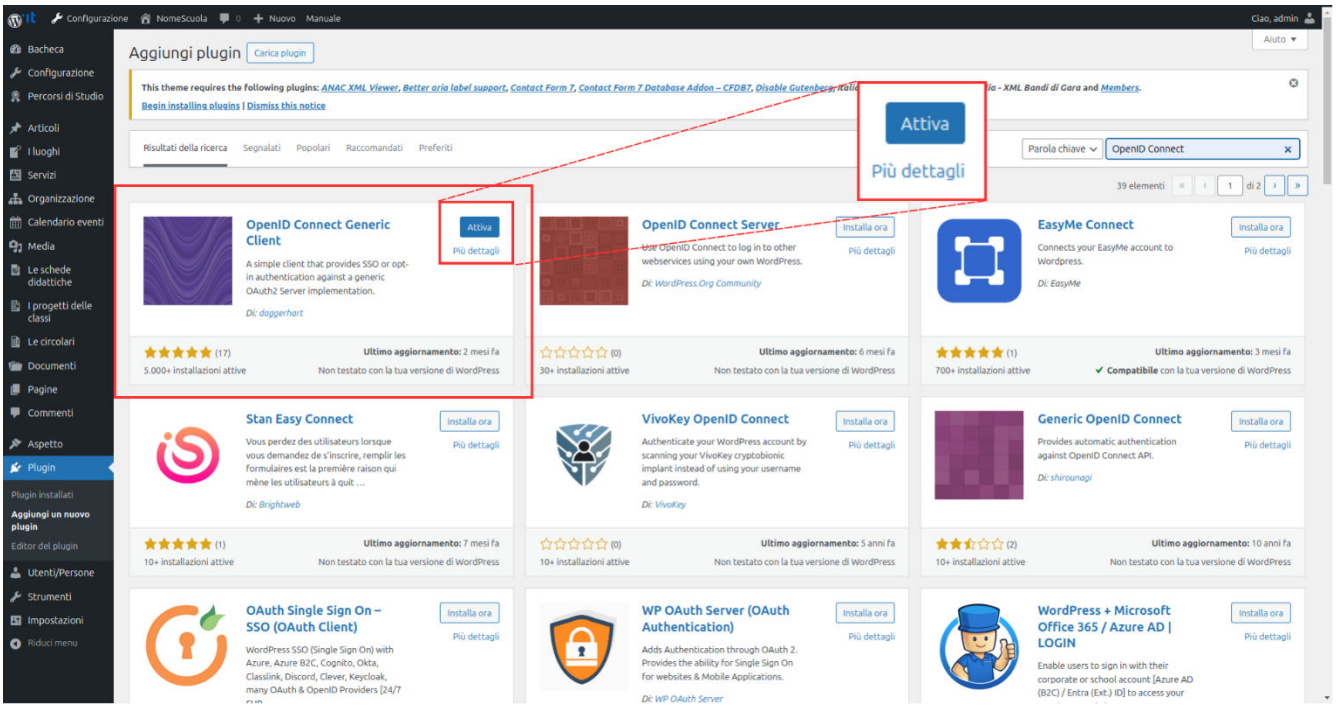

Figura 21: Attivazione plugin

Una volta attivato il plugin è necessario cliccare sul pulsante “Refresh Now” che comparirà nella parte superiore della finestra.

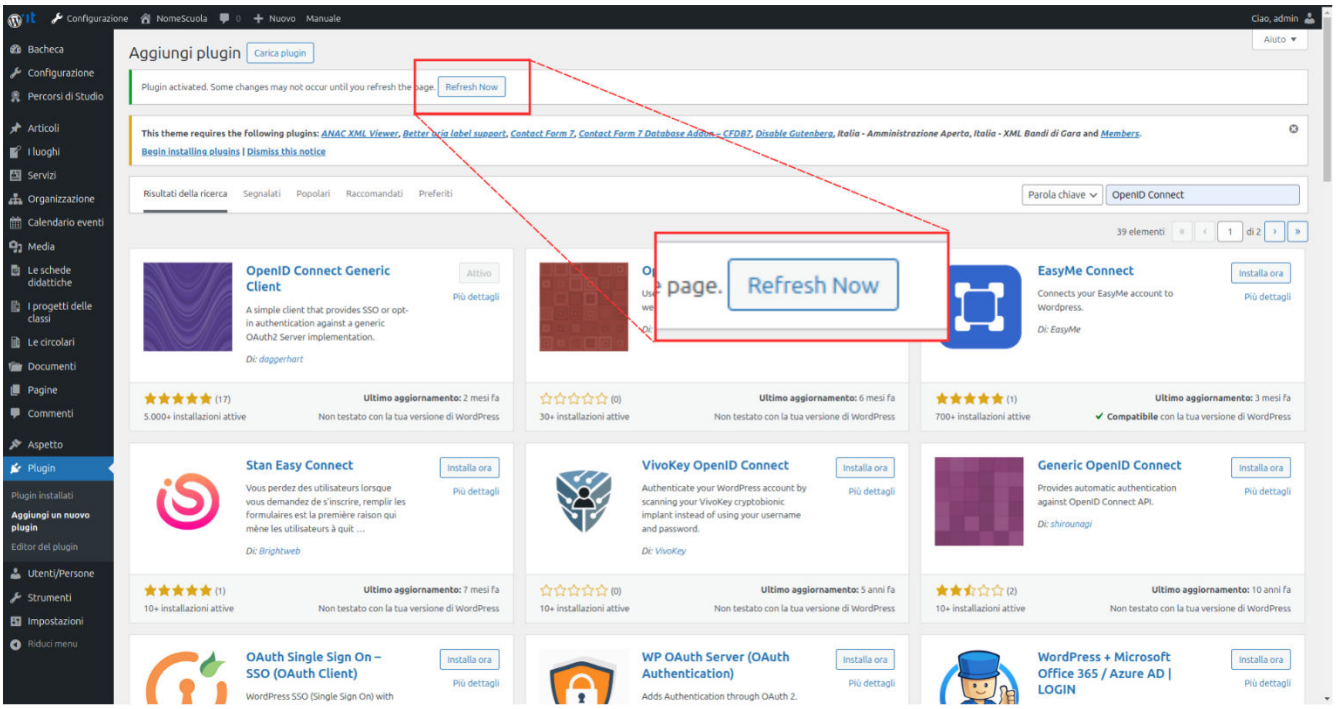

Figura 22: Aggiornamento finestra

Dopo aver aggiornato la pagina, nella sezione “Impostazioni”, in basso a sinistra nella barra laterale, clicca su “OpenID Connect Client”.

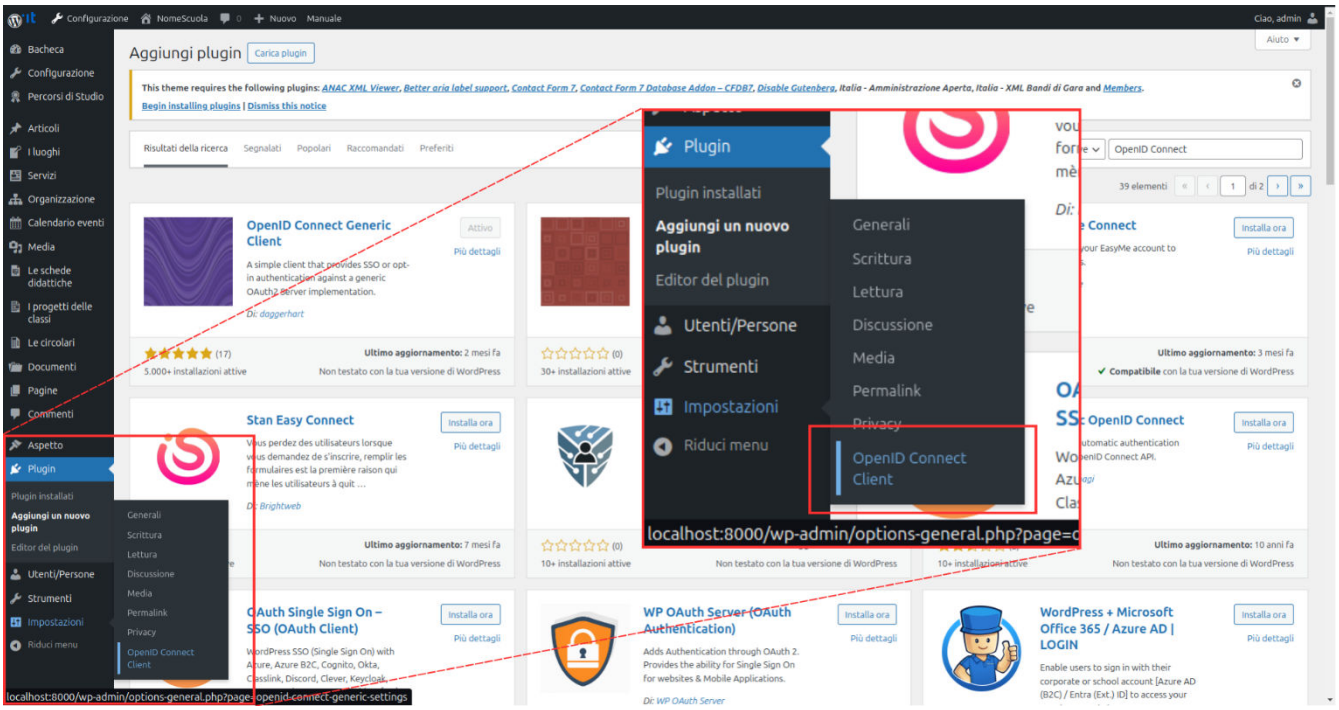

Figura 23: Accesso alla configurazione del plugin

A questo punto ci troveremo nella pagina di configurazione del plugin.

4.4 Configurazione client OIDC Wordpress

Per procedere alla configurazione del plugin è necessario riempire alcuni campi della seguente pagina.

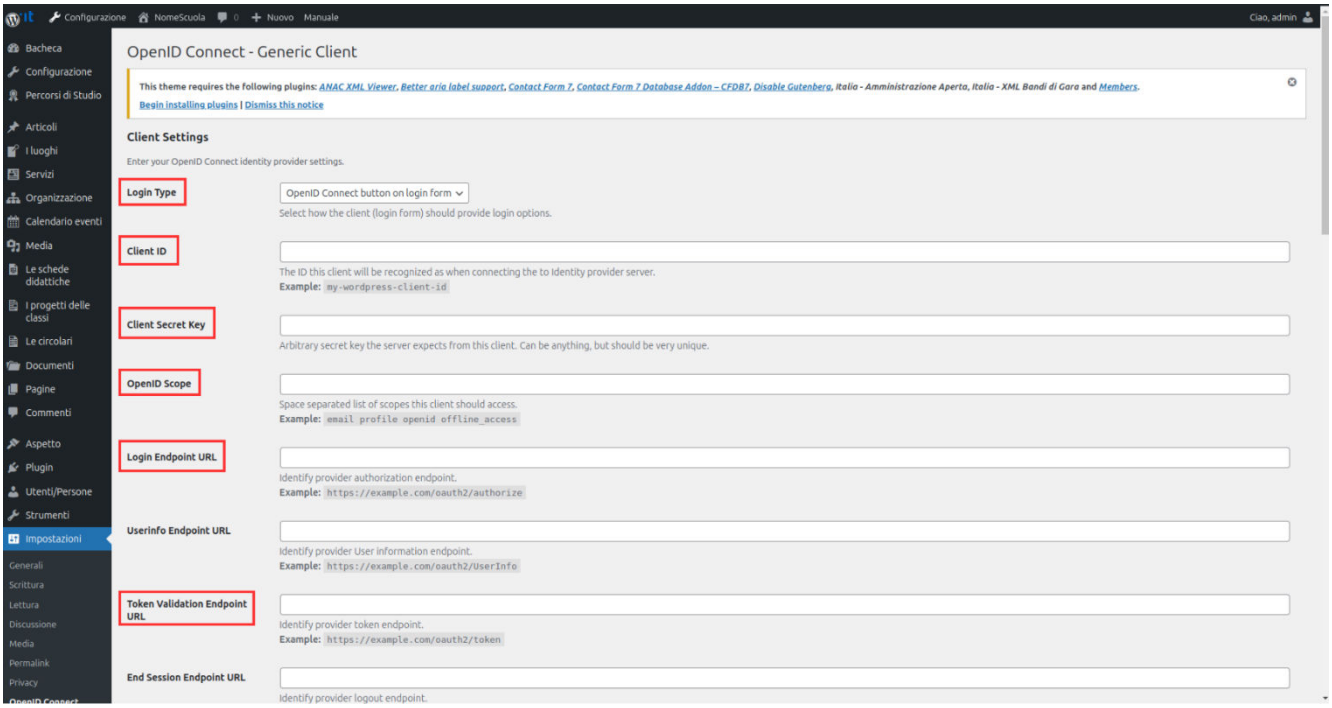

Figura 24: Pagina di configurazione del plugin - 1

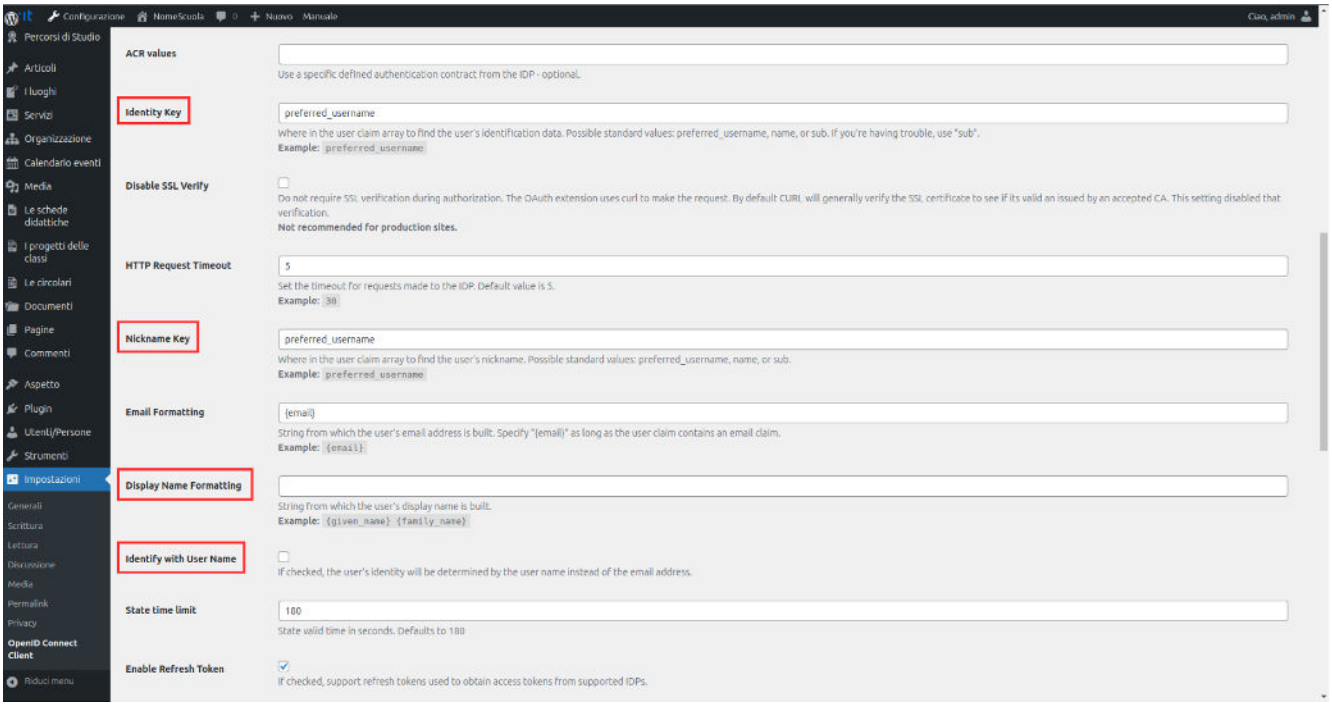

Figura 25: Pagina di configurazione del plugin - 2

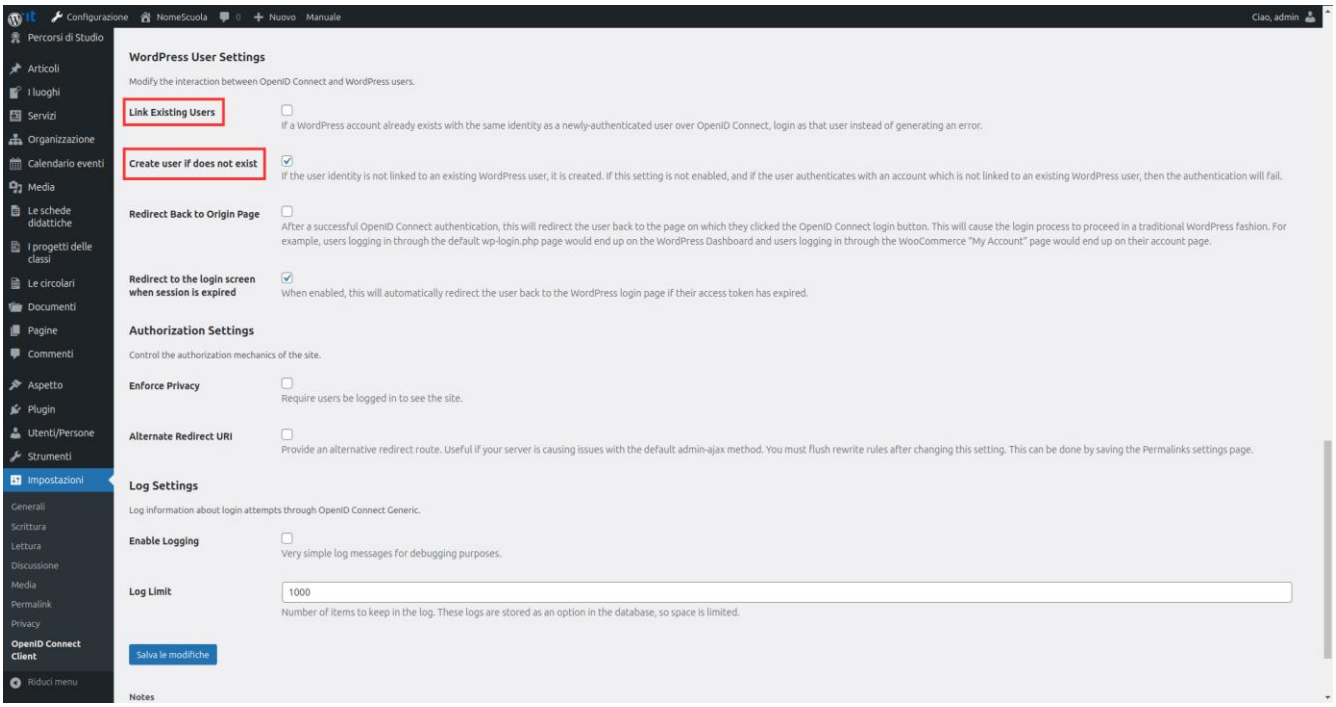

Figura 26: Pagina di configurazione del plugin - 3

I seguenti campi definiscono il comportamento di Wordpress durante e dopo la procedura di autenticazione OpenID Connect, in particolare i campi sottolineati sono quelli che definiscono come viene creato un utente su Wordpress a seguito di una corretta autenticazione, qualora quell'utente non esistesse già sulla piattaforma.

- **Client ID**: corrisponde all'ID che è stato fornito al termine della registrazione del client tramite la funzione "Gestione Client" fornito come client Id;
- **Client Secret Key**: corrisponde alla secret che è stata fornita al termine della registrazione del client tramite la funzione "Gestione Client";
- **OpenID Scope**: inserire i seguenti valori "iam openid gateway";
- **Login Endpoint URL**: inserire https://eid.istruzione.it/eid-gateway-oidc/oauth2/authorize ;
- **Token Validation Endpoint URL**: inserire https://eid.istruzione.it/eid-gateway-oidc/oauth2/token ;
- **Identity Key**: questo campo indica il "nome utente" che verrà assegnato al nuovo utente, si consiglia caldamente di utilizzare il valore "sub" corrispondente al codice fiscale, un altro valore disponibile è "preferred_username" ovvero lo username con il quale l'utente viene riconosciuto durante la procedura di OpenID Connect;
- **Nickname Key**: questo campo indica il nickname che verrà assegnato al nuovo utente, si consiglia caldamente di utilizzare il valore "sub" corrispondente al codice fiscale, a differenza del campo Identity Key questo non presenta la possibilità di inserire come valore "preferred_username";

- **Display Name Formatting**: questo campo corrisponde al "nome pubblico da visualizzare", ovvero il nome che verrà mostrato agli altri utenti, si consiglia di utilizzare "{given_name} {family_name}" corrispondente alla combinazione di nome e cognome, qualora si volesse associare solo il nome o solo il cognome utilizzare rispettivamente "{given_name}" o "{family_name}";
- **Identify with User Name**: determina come viene identificato l'utente, se attraverso l'e-mail o attraverso il nome utente, si consiglia di spuntare l'opzione per attivare l'identificazione attraverso nome utente;
- **Link Existing Users**: determina come Wordpress riconosce se un utente che accede attraverso OpenID Connect è già registrato sulla piattaforma oppure deve essere registrato, si consiglia caldamente di spuntare quest'opzione al fine di non registrare ogni volta gli utenti che fanno accesso attraverso OpenID Connect;
- **Create user if does not exist**: se spuntata permette agli utenti che non sono registrati sulla piattaforma di essere registrati, se non attiva gli utenti che non sono registrati non potranno fare accesso alla piattaforma; pertanto, si consiglia caldamente di spuntare quest'opzione.

Al termine dell'inserimento dati cliccare il bottone "Salva le modifiche" per salvare la configurazione.

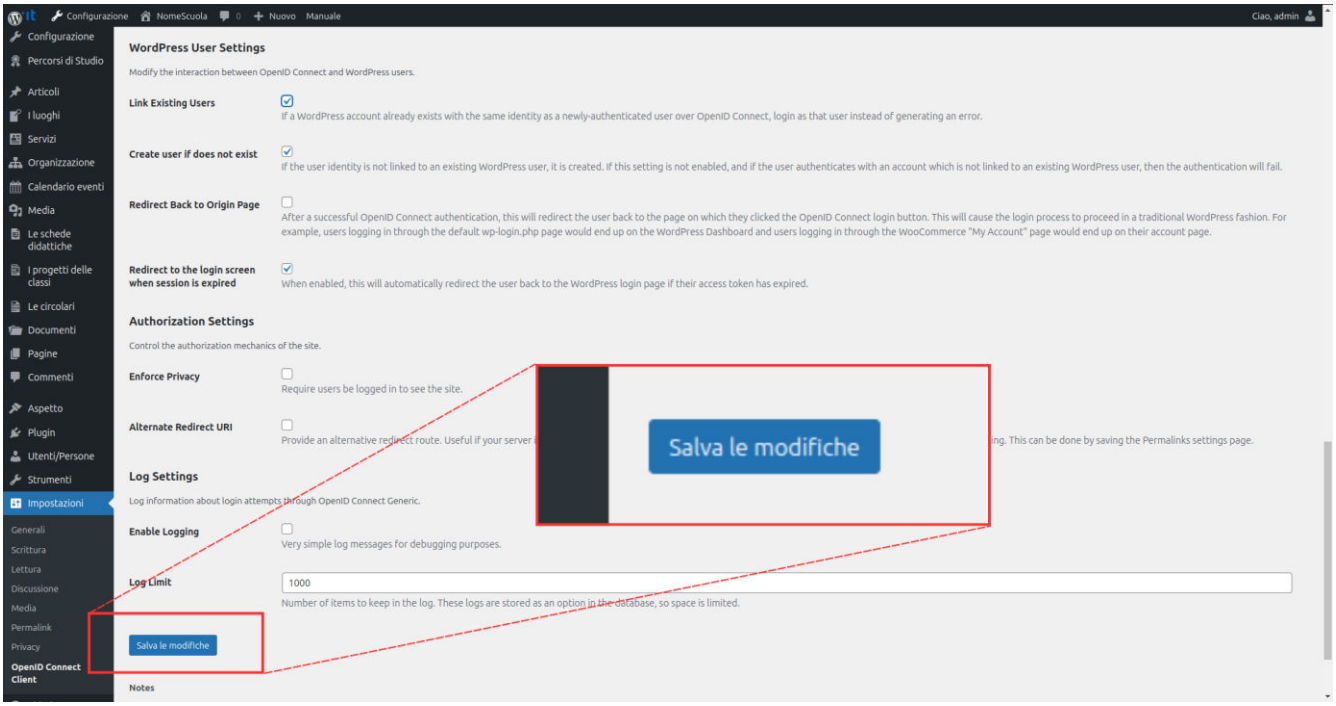

Figura 27: Salvataggio impostazioni plugin

4.5 Accesso al sito tramite il Gateway delle Identità

Una volta terminata la configurazione del plugin è possibile eseguire l'accesso a WordPress tramite il Gateway delle identità.

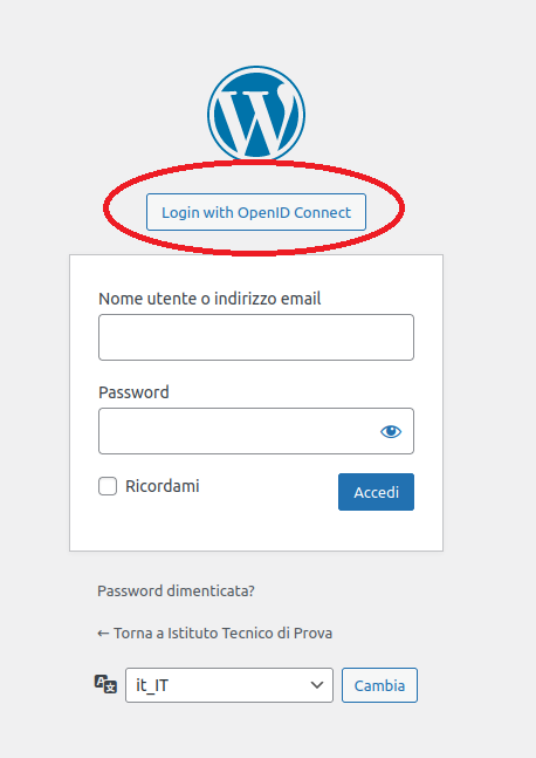

Figura 28: Pagina di accesso WordPress

Cliccando sul pulsante "Login with OpenID Connect" l'utente verrà indirizzato sulla pagina di autenticazione del Gateway delle Identità.

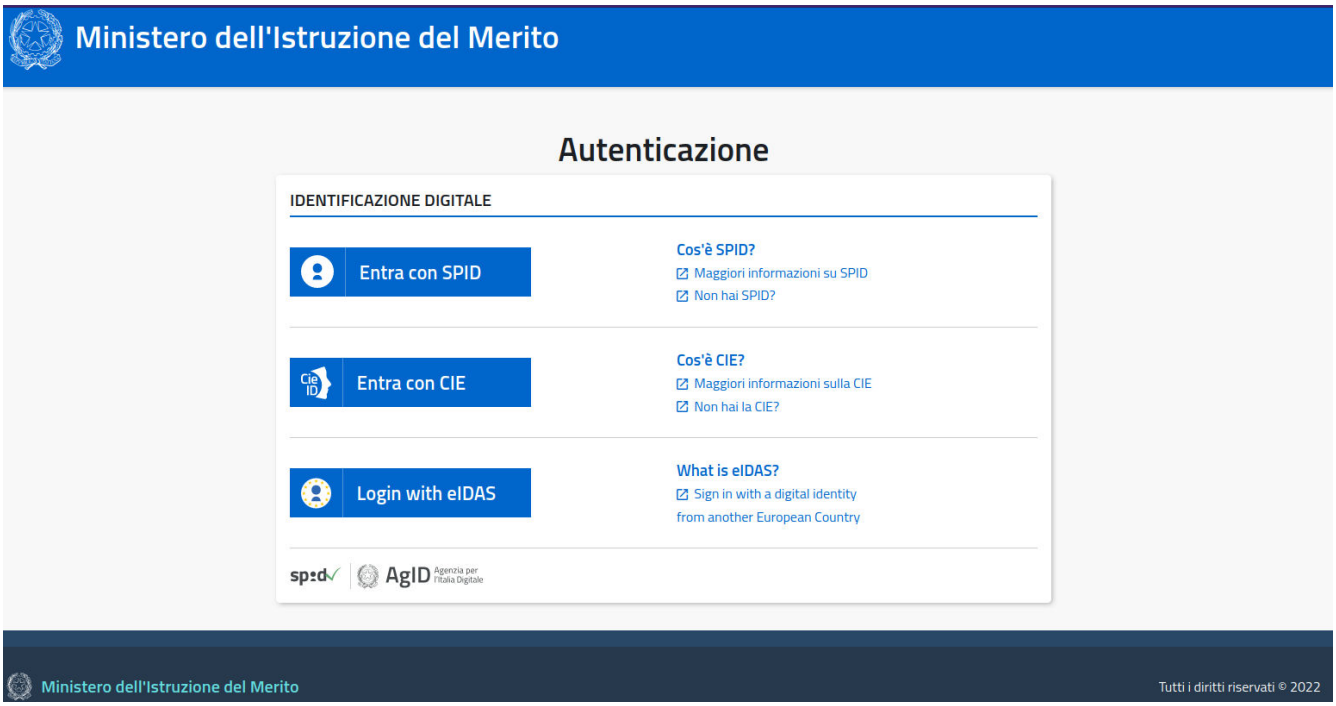

Figura 29: Autenticazione

Da questa pagina è possibile selezionare il tipo di accesso desiderato.

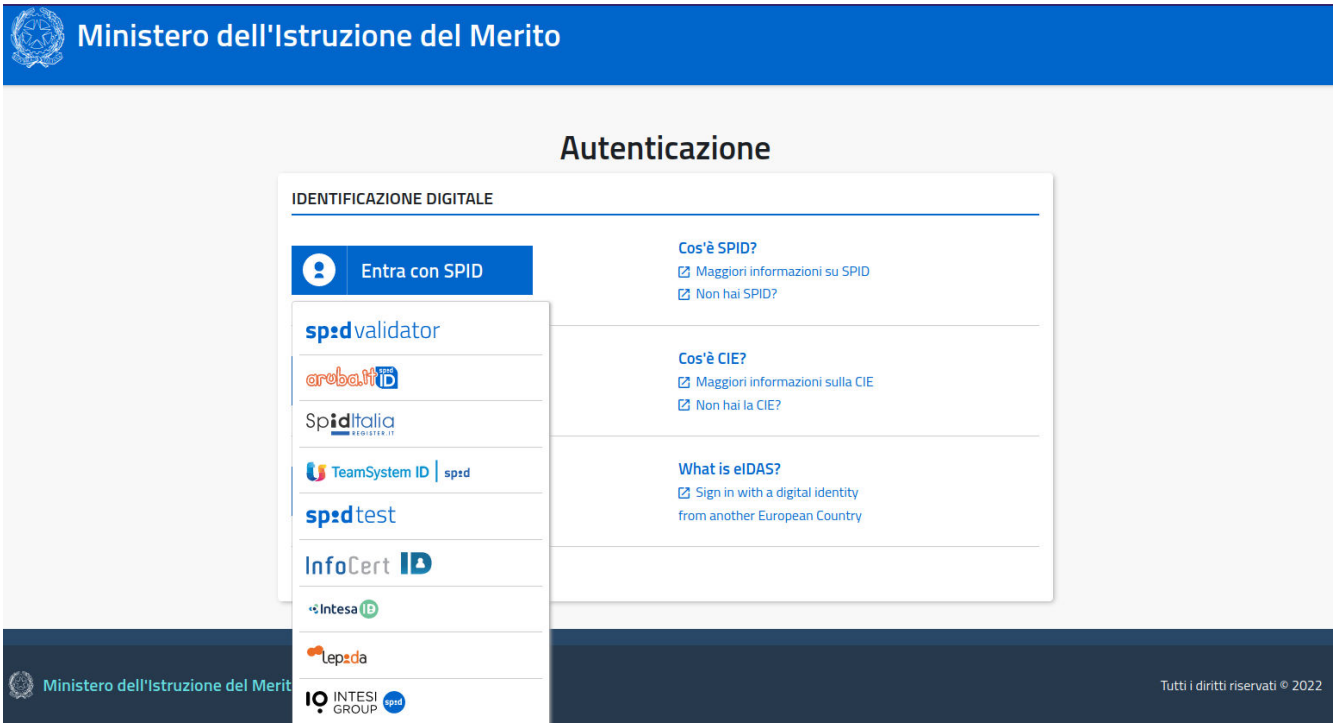

Figura 30: Selezione del provider

Una volta eseguita la procedura di login (SPID, CIE o EIDAS) l'utente verrà indirizzato sulla pagina di dashboard di WordPress come utente autenticato.

Figura 31: Dashboard WordPress utente autenticato