Crea il tuo ambiente Big Data in modo semplice e veloce

Isaac
No code, Just data

www.isaacbigdata.com

isaac-big-data

Indice

03 Protezione dei dati sensibili in conformità al GDPR

04 Cos'è il GDPR?

05 Crittografia del disco e di una partizione

06 Gestione dei dati personali in Isaac

07 Linee guida nei Cluster di Cassandra

08 Introduzione gestione utenti e ruoli

09 Ruoli predefiniti di Isaac

10 Associazione dei permessi in Cassandra

11 Associazione dei permessi su Isaac

12 Gestione Utenti

13 Creazione Utente

14 Modifica Utente

14 Cambio Password

14 Elimina Utente

15 Utente Operator

15 Utente Viewer

Protezione dei dati sensibili in conformità al GDPR

Questo documento ha lo scopo di definire le linee guida per la gestione delle informazioni sensibili degli utenti registrati in Isaac, al fronte della nuova normativa sulla privacy regolata dalla **GDPR/18**.

Nel documento sono descritte le funzionalità che permettono una migliore protezione, riservatezza e gestione dei dati contenuti nel software, sia per quanto riguarda i dati sensibili, sia per quanto riguarda la gestione utenti e ruoli.

Cos'è il GDPR?

Il Regolamento Generale sulla Protezione dei Dati (**GDPR 2018**) in vigore dal 25 Maggio 2018 stabilisce le nuove regole per trattare i Dati Personali all'interno della Comunità Europea e disciplinare l'esportazione dei Dati Personali al di fuori dei confini UE.

Tale regolamento (General Data Protection Regulation) definisce Dato Personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Nel rispetto del **Codice della Privacy** il nuovo Regolamento descrive in che maniera i dati personali vadano protetti ("**data protection**") e trattati in conformità con le Normative vigenti: i dati vanno trattati seguendo nuovi principi di applicazione, e il trattamento deve seguire un ciclo progettato, riconosciuto come "trattamento by design".

Crittografia del disco

La crittografia dei dischi assicura che tutti i file immagazzinati sul disco siano criptati. I file diventeranno disponibili al sistema operativo e alle applicazioni solo quando il sistema corrente sarà sbloccato da un utente fidato. Leggere settori criptati senza i permessi restituirà dati messi a caso invece dei file effettivi.
Se un disco è criptato, anche staccandolo da quel computer e collegandolo ad un altro non potremo mai estrarre i file al suo interno.
A questo proposito, il primo meccanismo di sicurezza da attivare è la cifratura del disco rigido in fase d'installazione del sistema operativo CentOS. Verrà richiesta una passphrase sia in fase d'installazione che ogni volta che si riavvia il sistema.
I vantaggi nel cifrare il disco sono i seguenti:

- Previene accessi fisici non autorizzati ai file del sistema operativo;
- Previene accessi fisici non autorizzati ai dati privati che potrebbero essere immaganizzati dal sistema.

Crittografia di una partizione

Nel caso non sia possibile eseguire la cifratura dell'intero disco, è possibile crittografare solamente una partizione del disco, in particolare la partizione in cui sono presenti i dati sensibili, ad esempio le directory contenente il Database.
In fase d'installazione del Sistema Operativo CentOs7, oppure successivamente, si può creare una nuova partizione, separata da quella contenente il sistema operativo e configurare gli applicativi in modo che i dati sensibili siano salvati in tale partizione.

Gestione dei dati personali in Isaac

Per garantire la protezione dei dati da eventuali “data breach” e nel rispetto delle nuove regole GDPR, nell’applicativo Isaac sono state seguite alcune linee guida utili allo scopo:

1

Le informazioni degli utenti registrati in Isaac sono memorizzate su più tabelle, all’interno del Database, in modo che esse non siano facilmente riconducibili all’utente stesso.

2

Le informazioni sensibili dell’utente sono state cifrate mediante l’algortimo blowfish. Le informazioni che vengono richieste ad un utente che si registra sono: Nome, Cognome ed Email e tutte queste informazioni sono salvate in modo cifrato.

3

La cancellazione di un utente, quando quest’ultimo o un amministratore la richiedesse è una cancellazione fisica e immediata. La cancellazione di un utente comporta anche la cancellazione dello stesso nel Cluster di Cassandra, di conseguenza non potrà più accedervi.

Linee guida nei Cluster di Cassandra

Nei Cluster di Cassandra, la gestione dei dati sensibili è affidata agli utenti utilizzatori dell'applicativo che creano i Cluster e le relative tabelle. Si consiglia di seguire le stesse regole espresse precedentemente nella gestione dei dati personali in Isaac.

Per quanto riguarda la cifratura dei dati sensibili degli utenti, può avvenire sia a livello applicativo utilizzando la classe BlowfishUtil.java, presente nella libreria isaac-libraries-xxx.jar, richiamando i metodi encode/decode, sia utilizzando le due funzioni UDF presenti nel Database Cassandra, encrypt e decrypt.

NOTA: i dati da cifrare devono essere di tipo stringa.

Di seguito alcuni esempi di utilizzo delle due modalità di cifratura.

Esempio 1

```
String cipher_str = BlowfishUtil.encode("Mario Rossi");
char[] clear_str = BlowfishUtil.decode("a5gdbfy4hdf4fr");
```

Esempio 2

```
INSERT INTO employee (firstname, lastname, email)
VALUES (encrypt('Mario'), encrypt('Rossi'),
encrypt('m.rossi@gmail.com'));

SELECT decrypt(firstname), decrypt(lastname), decrypt(email)
FROM employee where firstname = encrypt('Mario');
```

È onere dell'utente finale quindi, richiamare tali funzionalità nel momento in cui inserisce dati sensibili e quindi "da proteggere".

Dunque, mentre in Isaac l'inserimento di un nuovo utente e la protezione dei suoi dati è implicita in quanto già gestita 'by design', nei Cluster di Cassandra invece è dipendente dall'attivazione delle misure di sicurezza (decrypt/encrypt o encode/decode messe a disposizione) dell'utente finale.

Introduzione gestione utenti e ruoli

Questo documento ha lo scopo di esporre la gestione degli utenti nell'applicativo Isaac.

Premessa sulla gestione degli utenti

In Isaac si dà la possibilità agli utenti amministratori di gestire il CRUD degli utenti. I ruoli sono invece prefissati e non è possibile crearne di nuovi.

In Cassandra è presente la possibilità di abilitare l'autenticazione e la gestione dei permessi: in Isaac questo avviene di default, poiché è importante garantire la sicurezza dei dati.

In Cassandra:

- Un utente può essere superuser (permessi massimi) o non esserlo.
- Un utente può avere un ruolo associato.
- Un ruolo può avere garantiti determinati permessi, validi su uno o più keyspace

Per avere un'integrazione completa tra Isaac e le istanze di Cassandra che vengono installate, ogni utente creato nel sistema viene creato anche in Cassandra. I ruoli, come detto, sono predefiniti e vengono creati in automatico in Cassandra al momento della creazione del Cluster.

Ruoli predefiniti di Isaac

In Isaac saranno presenti tre ruoli predefiniti e non sarà possibile modificarli, cancellarli o aggiungerne di nuovi.

Tali ruoli saranno:

Admin

Ruolo con permessi massimi sia su Cassandra che sul sistema Isaac. Gli utenti con questo ruolo, oltre ad avere la gestione completa sui dati, avranno la possibilità di operare su tutta la parte amministrativa.

Operator

Ruolo con permessi completi su dati e operazioni. Non avrà accesso alla parte amministrativa, ma potrà operare su dati, strutture dati e operazioni sul Cluster.

Viewer

Ruolo con permessi ridotti sui dati. Non avrà accesso alla parte amministrativa e non potrà effettuare operazioni su dati e Cluster, ma potrà leggere dati.

Associazione dei permessi in Cassandra

In Cassandra esistono i seguenti tipi di permessi:

- **ALTER:** permette la modifica delle strutture dati (keyspace, table, column);
- **AUTHORIZE:** permette la gestione di utenti/ruoli in Cassandra;
- **CREATE:** permette la creazione di strutture dati (keyspace, table, column);
- **DESCRIBE:** permette la visualizzazione dei ruoli
- **DROP:** permette l'eliminazione delle strutture dati (keyspace, table, column)
- **EXECUTE:** permette di effettuare letture, inserimenti e aggiornamenti sui dati
- **MODIFY:** permette di effettuare letture, inserimenti, aggiornamenti e cancellazioni sui dati
- **SELECT:** permette di effettuare letture sui dati.

Inoltre esiste l'ALL PERMISSIONS che racchiude tutti i precedenti.

L'associazione tra ruoli e permessi sarà la seguente:

- **Admin:** ALL PERMISSIONS (ALTER, AUTHORIZE, CREATE, DESCRIBE, DROP, EXECUTE, MODIFY, SELECT)
- **Operator:** ALTER, CREATE, DROP, EXECUTE, MODIFY, SELECT
- **Viewer:** SELECT

Associazione dei permessi su Isaac

Essendo Isaac composto da varie sezioni, ognuna di esse ha dei permessi customizzati e ogni ruolo ha accesso solo a determinate funzionalità.

Sezione Amministrazione

L'associazione tra ruoli e permessi sarà la seguente:

- **Admin:** gestione completa del CRUD degli utenti. Nessun permesso sul CRUD dei ruoli.
- **Operator:** nessun permesso sull'amministrazione.
- **Viewer:** nessun permesso sull'amministrazione.

Sezione Configurazione Cluster

L'associazione tra ruoli e permessi sarà la seguente:

- **Admin:** gestione completa della configurazione del Cluster.
- **Operator:** nessun permesso sulla configurazione del Cluster.
- **Viewer:** nessun permesso sulla configurazione del Cluster.

Sezione Query Builder

L'associazione tra ruoli e permessi sarà la seguente:

- **Admin:** gestione completa del Query Builder.
- **Operator:** gestione completa del Query Builder.
- **Viewer:** accesso alle funzionalità di costruzione di SELECT e JOIN, ma non degli statement di modifica sui dati.

Sezione DB Builder

L'associazione tra ruoli e permessi sarà la seguente:

- **Admin:** gestione completa del DB Builder.
- **Operator:** Gestione completa del DB Builder.
- **Viewer:** nessun permesso sul DB Builder.

Sezione Cluster Monitor

L'associazione tra ruoli e permessi sarà la seguente:

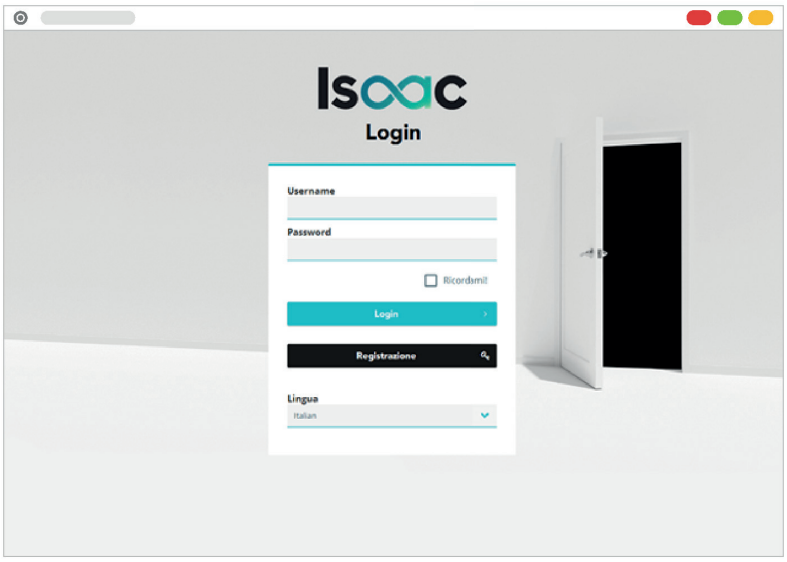
- **Admin:** gestione completa del Cluster Monitor.
- **Operator:** gestione completa del Cluster Monitor.
- **Viewer:** accesso alla visualizzazione delle statistiche relative al Cluster, ma non alle azioni sul Cluster.

Sezione Import Dati

L'associazione tra ruoli e permessi sarà la seguente:

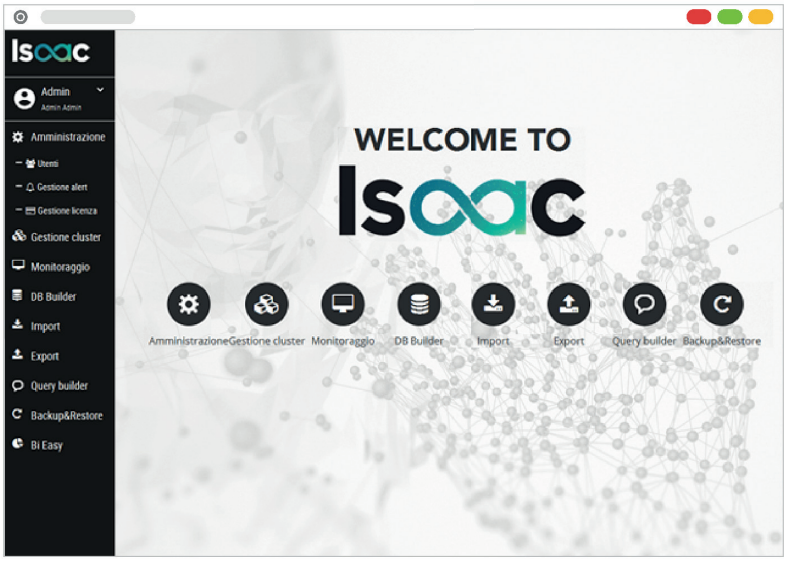
- **Admin:** gestione completa del Cluster Monitor.
- **Operator:** gestione completa del Cluster Monitor.
- **Viewer:** nessun permesso sull'Import Dati.

Gestione Utenti



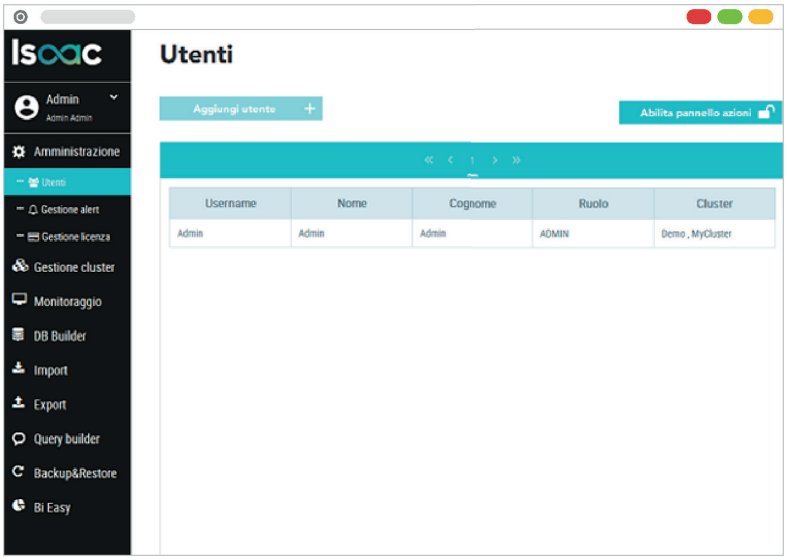
1

L'utente amministratore accede al sistema attraverso la seguente pagina di login.



2

Inserite le credenziali si visualizza la seguente pagina principale.



3

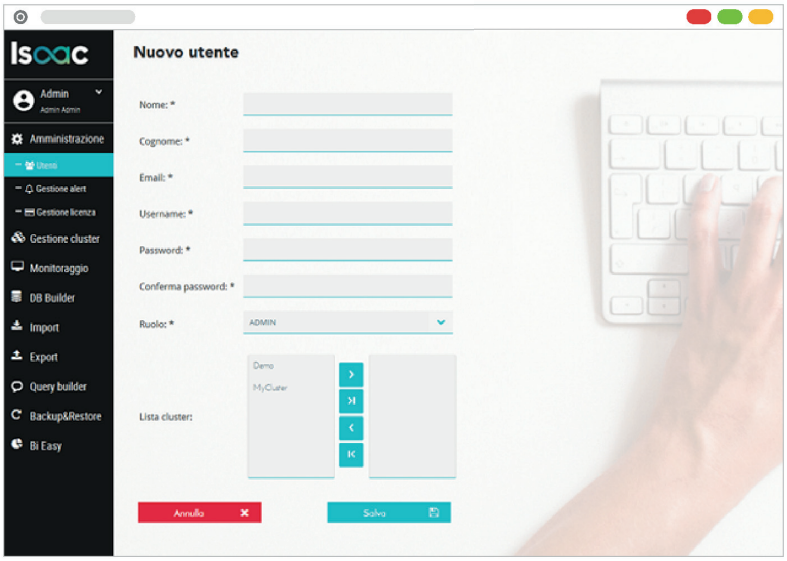
Cliccando sul menu link "**Utenti**" all'interno della sezione "**Amministrazione**", si accede alla seguente pagina in cui si visualizza la lista di tutti gli utenti presenti all'interno del sistema.

Creazione Utente

Prima di poter effettuare una creazione utente bisogna abilitare la funzionalità tramite il pulsante "Abilita Pannello azioni"

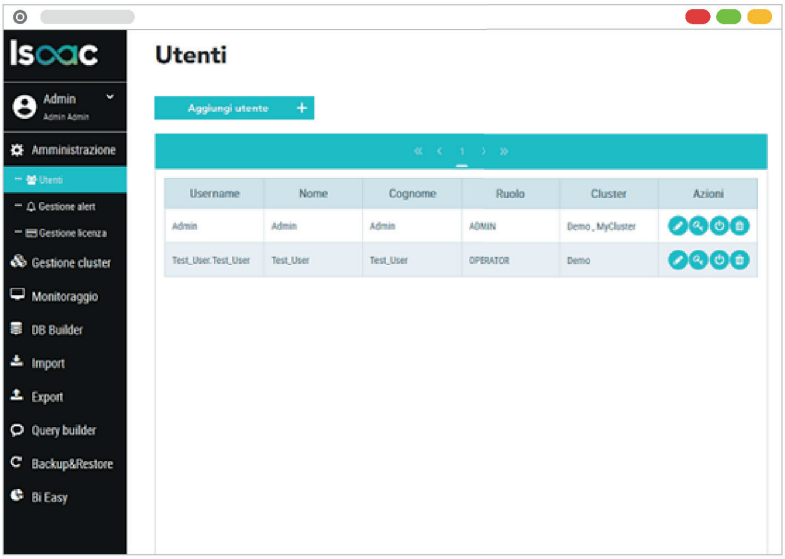
1

In generale, prima di poter effettuare una qualsiasi operazione di gestione utente, bisogna cliccare sul pulsante "**Abilita pannello azioni**" che ci porta all'apertura del pop-up della figura seguente in cui si richiede nuovamente l'inserimento della password.



2

Abilitata la funzionalità "**Aggiungi utente**" e cliccando sul pulsante stesso, si giunge alla schermata di inserimento di tutti i dati dell'utenza da creare nonché degli eventuali ruoli e lista dei Cluster da associare ad essa. I ruoli possibili da associare ad un utente sono : **Admin**, **Operator** e **Viewer** le cui potenzialità sono state esposte nei paragrafi precedenti.
Cliccando sul tasto "**Salva**" si torna alla pagina principale della lista utenti, "Annulla" ci riporta ugualmente alla tabella principale della lista utenti ma senza portare a buon fine la creazione dell'utente.



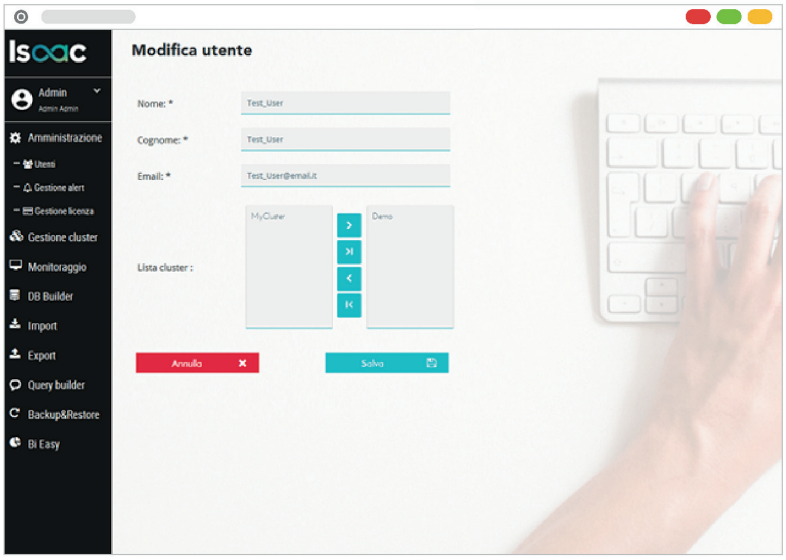
3

Creato il nuovo utente (Es:Test_User, Role:Operator) si possono effettuare su di esso le seguenti azioni: **Modifica**, **Cambio password**, **Elimina**, **Disabilita**.

Modifica Utente

Cliccando sul tasto “**Modifica**” presente sotto la colonna “**Azioni**” si giunge alla seguente pagina in cui si possono modificare i dati dell’utente selezionato.

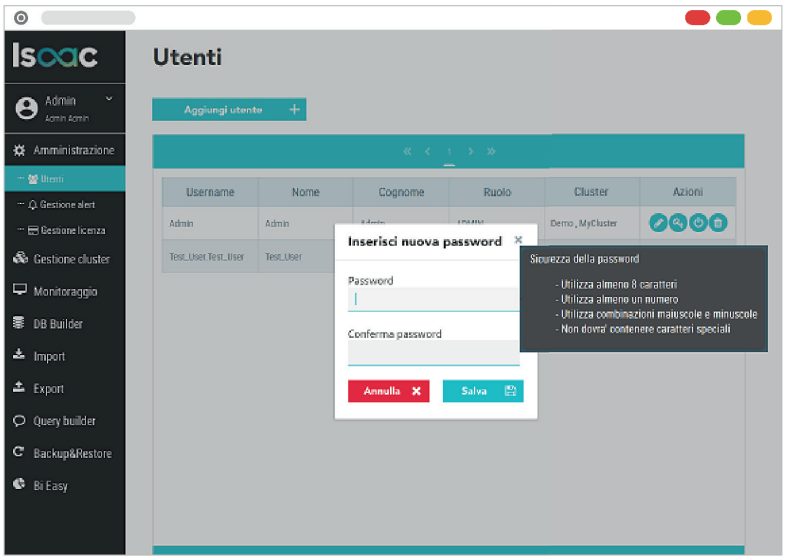
Cliccando il pulsante “**Salva**” si rendono effettive le modifiche, “**Annulla**” altrimenti.



Cambio Password

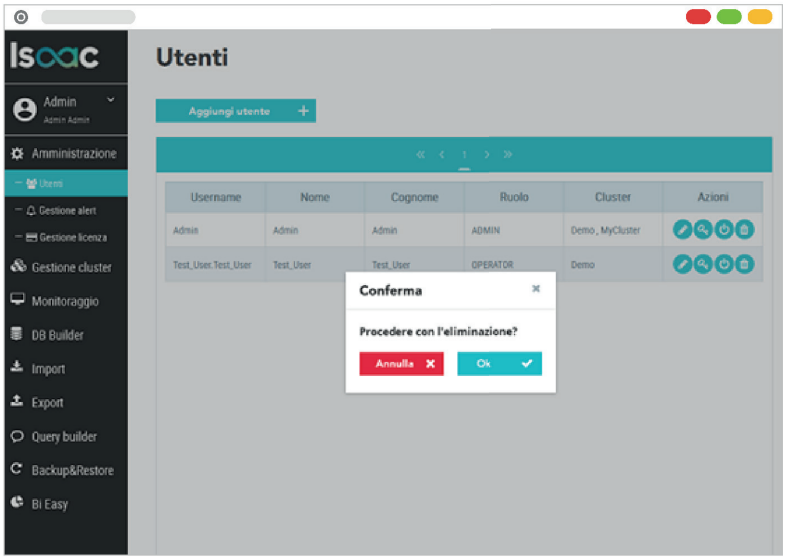
Nella tabella principale degli utenti, cliccando sul tasto “**Aggiorna Password**” sotto la colonna “**Azioni**”, in corrispondenza dell’utenza di interesse, si apre il seguente pop-up di modifica password.

Digitando i campi “**Password**” e “**Conferma passord**” e successivamente il tasto “**Salva**” si rende effettiva la modifica della password dell’utente selezionato.



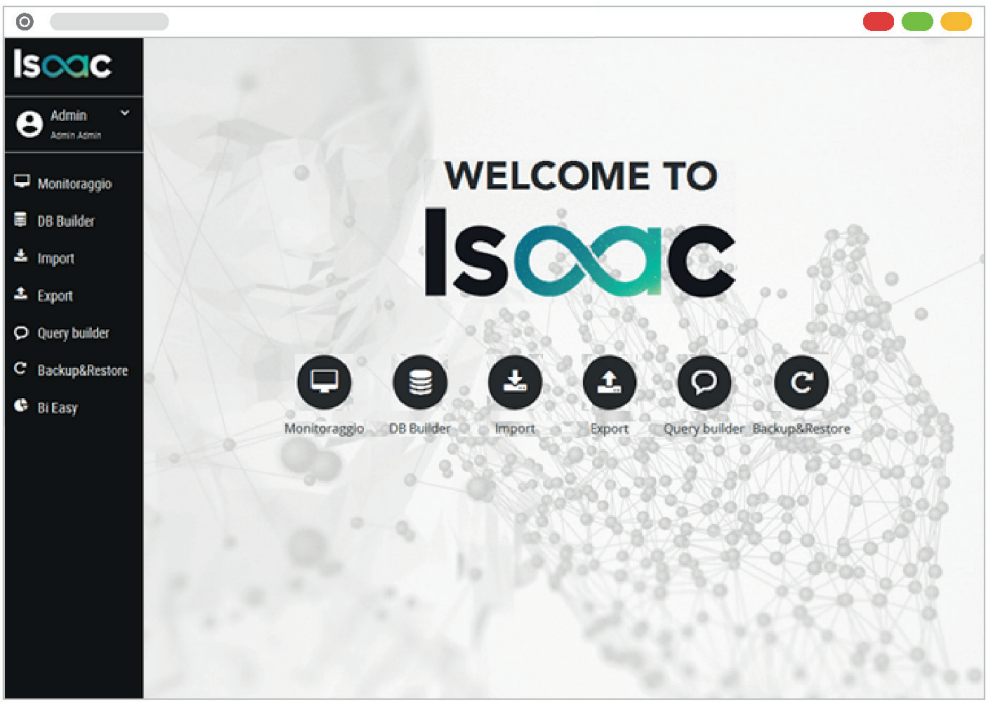
Elimina Utente

Infine, è possibile eliminare definitivamente un utente cliccando sul pulsante “**Elimina**” presente sotto la colonna “**Azioni**” in corrispondenza dell’utente selezionato.



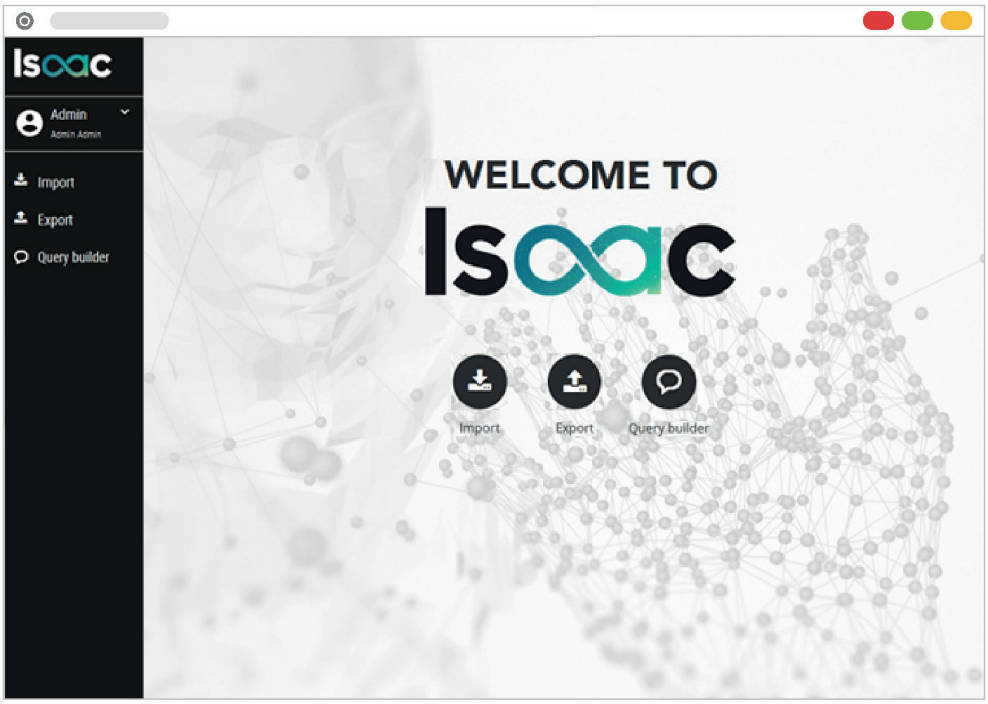
Utente Operator

Un utente con ruolo "**Operator**" entrando nell'applicazione visualizza le seguenti voci di menu:



Utente Viewer

Un utente con ruolo "**Viewer**" visualizza invece un range più ristretto di operazioni come mostra la figura seguente:



Scopri come Isaac può aiutarti a creare il tuo ambiente Big Data in modo semplice e veloce.

www.isaacbigdata.com

isaac-big-data