

User Manager

Tabella dei contenuti

1. Introduzione

2. Activation

3. Profili Utente

3.1 Admin

3.2 Admin senza manager utente

3.3 Encoder

3.4 Fraud analyst

3.5 Fraud manager

3.6 Fraud viewer

3.7 Helpdesk admin

3.8 Super-codificatore

3.9 Super-codificatore senza rimborso

3.10 Visualizzatore

4. Tipi di utente

4.1 Utente di back-office (utente ADM)

4.2 Utente API

5. Gestione Utenti

5.1 Creare un nuovo utente

5.1.1 Dettagli di pre-inizializzazione

5.1.2 Dettagli utente

5.1.3 Fuso orario

5.1.4 Profilo

5.1.5 Accesso limitato all'utente

5.1.6 Utente speciale per API

5.1.7 Iritti di accesso

5.2 Gestione password

5.3 Disattivare utenti

5.4 Modifica dettagli utente

5.5 Indirizzo IP

5.5.1 Limitazioni utente dell'indirizzo IP

5.5.2 Formato e valore dell'indirizzo IP

6. Login Utente

7. Tracciamento Utenti per Transazioni

8. Sommario Autorizzazioni Utente

8.1 Profili Rilevamento frodi

1. Introduzione

All'interno di una società, esistono generalmente diversi profili con funzioni (ruoli) diverse. Un contabile, per esempio, non esegue le stesse operazioni di un codificatore di pagamento o di un integratore tecnico. Il desiderio del cliente è quello di garantire semplicemente i diritti di accesso necessari per ogni individuo che deve utilizzare il suo conto, e soprattutto tracciare quale utente ha effettuato quale operazione.

Le opzioni del Manager utente permettono di assegnare un profilo specifico ad ogni utente, conferendogli i diritti di accesso di cui ha bisogno per adempiere alla sua funzione. Il Manager utente è un servizio aggiuntivo disponibile per tutti i prodotti.

Il Manager utente permette di:

- configurare i diversi utenti all'interno di un account
- gestire il profilo e i diritti di accesso per ogni utente
- evitare errori critici dei codificatori di pagamento
- tracciare le azioni di ogni utente (numero di transazioni al giorno, per esempio)
- limitare gli utenti per visualizzare esclusivamente le proprie transazioni
- gestire facilmente i diritti di accesso per collaboratori temporanei.

È possibile accedere al Manager utente tramite "Configurazione" > "Utenti" dal menu del conto Ingenico ePayments.

2. Activation

Per impostazione predefinita, il Ingenico ePayments conto viene fornito con due utenti; l'utente PSPID di default (admin), e un utente aggiuntivo.

Se avete bisogno di più utenti, a seconda del tipo di abbonamento, è possibile attivare l'opzione nel Ingenico ePayments conto:

1. Va a "Configurazione> Abbonamento > Opzioni".
2. Cerca l'elenco delle opzioni per "User Manager up to x users" ("x" definisce il numero di utenti che si desidera creare: 5, 10, 20 ... 200)
3. Fare clic sul pulsante "Attiva".

A seconda dell'opzione avete attivato, è possibile creare altri utenti con differenti profili e configurazioni.

3. Profili Utente

I principali profili utente supportati dal Manager utente sono:

- visualizzatore
- codificatore
- super-codificatore
- super-codificatore senza rimborso
- admin senza manager utente
- admin
- helpdesk admin

3.1 Admin

Un admin ha tutti i diritti di accesso.

Ogni volta che si crea un account, si genera automaticamente anche un utente predefinito (l'UserID di questo utente predefinito è identico al PSPID); questo utente predefinito ha un profilo di admin. Naturalmente è possibile creare anche altri utenti admin.

Un utente admin è l'unico utente con i permessi per modificare la configurazione del conto.

3.2 Admin senza manager utente

L'admin senza manager utente ha gli stessi diritti di accesso dell'admin, ad eccezione del fatto che non ha accesso alle opzioni del Manager utente.

3.3 Encoder

Un codificatore può inserire un nuovo pagamento tramite il link "Nuovo pagamento" nel menu del conto o tramite DirectLink.

3.4 Fraud analyst

Un Fraud analyst consente di modificare blacklist/whitelist, verificare la valutazione delle transazioni e contestare le transazioni.

Nota: Per il funzionamento corretto di questo profilo utente, occorre selezionare "Rilevamento frodi" nei diritti di accesso utente.

3.5 Fraud manager

Un Fraud manager consente di modificare tutte le pagine di configurazione rilevamento frodi rilevanti, modificare blacklist/whitelist, verificare e contestare le transazioni, ecc.

Nota: Per il funzionamento corretto di questo profilo utente, occorre selezionare "Rilevamento frodi" nei diritti di accesso utente.

3.6 Fraud viewer

Un Fraud viewer consente di visualizzare varie pagine di configurazione rilevamento frodi, ma non consente di apportare alcuna modifica.

Nota: Per il funzionamento corretto di questo profilo utente, occorre selezionare "Rilevamento frodi" nei diritti di accesso utente.

3.7 Helpdesk admin

Il helpdesk admin ha accesso esclusivamente alla pagina di "Gestione utenti" del conto.

Per ulteriori informazioni, consultare [panoramica permessi utenti](#) per i vari profili.

3.8 Super-codificatore

Un super-codificatore può sia inserire nuove transazioni, sia effettuare operazioni di manutenzione sulle transazioni esistenti. Egli può anche caricare file di pagamento e scaricare report delle transazioni.

3.9 Super-codificatore senza rimborso

Il super-codificatore senza rimborso ha gli stessi diritti di accesso del super-codificatore, ad eccezione del fatto che non è in grado di effettuare rimborsi o cancellare autorizzazioni. Questo profilo permette di accordare permessi per effettuare esclusivamente raccolte di dati, ma non per effettuare rimborsi o cancellare pagamenti.

3.10 Visualizzatore

Il profilo visualizzatore è il profilo ideale per un contabile. Un visualizzatore può visualizzare e richiedere report e stato delle transazioni, ma non può modificare o inserire nulla. Si tratta di un profilo di sola lettura.

4. Tipi di utente

Per questo motivo abbiamo 2 tipi di utente:

- l'utente di back-office (= l'utente ADM)
- l'utente applicativo (= l'utente API)

4.1 Utente di back-office (utente ADM)

Un utente di back-office (utente ADM) è un utente che ha accesso ai moduli di amministrazione conto (back-office) tramite pagina web.

Un utente di back-office deve modificare la propria password ogni 90 giorni. Può farlo attraverso il link "Password" nel menu del conto.

4.2 Utente API

Un utente API (Application Program Interface) è un utente disegnato specificatamente per utilizzare un'applicazione che esegue richieste automatiche di pagamento alla piattaforma (caricare/scaricare file automaticamente, richieste dirette di pagamento...).

Anche se per un utente API dei vari profili utente sono disponibili, si consiglia vivamente di configurare questo utente con il profilo "Admin". Se si vuole limitare i diritti per la manutenzione delle operazioni (rimborsi, cancellazioni, ecc), è ancora possibile modificare il profilo utente a "Encoder".

Se non siete sicuri, vi consigliamo di scegliere il profilo "Admin", altrimenti andate a [profili utenti](#) per maggiori informazioni.

Una password di utente API non deve essere modificata regolarmente; ciò è più comodo quando la password deve essere hardcoded all'interno dell'applicazione. Consigliamo di modificare ogni tanto la password.

Per modificare la password di un utente API:

1. Si selezioni il link "Utenti" nel menu del conto
2. Si utilizzi link "Cambia la password" per l'utente API in question. Si verrà reindirizzati ad una pagina in cui è possibile modificare la password. Anche alla creazione di un nuovo utente API è necessario configurare la password in tale pagina.

Per motivi di sicurezza gli utenti API non hanno diritto di accesso ai moduli di amministrazione conto, cioè non possono accedere al back-office.

5. Gestione Utenti

Dalla pagina Gestione utenti è possibile:

- creare nuovi utenti
- gestire le password degli utenti
- disattivare utenti non più attivi nell'azienda
- modificare i dettagli degli utenti.

	UserID	Status	Profile	Scope	
?	testPSPID	Active	Admin	Account	Edit Deactivate Send new password
?	testuser_API	Active	Admin	Account	Edit Deactivate
?	testuser_jim	Active	Admin	Account	Edit Deactivate Send new password

1 - 3 of 3 items

NEW USER

Il numero di utenti abilitati è visualizzato nella pagina menu Gestione utenti. Quando si raggiunge il numero massimo di utenti abilitati, il pulsante "Nuovo utente" viene disabilitato.

5.1 Creare un nuovo utente

È possibile creare un nuovo utente facendo clic sul pulsante "Nuovo utente" nella pagina Gestione utenti. È necessario compilare la maschera visualizzata per inserire un nuovo utente.

UserID	<input type="text" value="JaneS"/>	*
REFID	testPSPID	
User type	PSPID	
User's name	<input type="text" value="Jane Smith"/>	*
E-mail address	<input type="text" value="janesmith@mycompany.com"/>	*
Timezone	(GMT-06:00) Central Time (US & Canada)	
	<input checked="" type="checkbox"/> Automatically adjust to daylight saving changes	
User created by	testPSPID/testPSPID/PSPID	
Profile	Super-encoder	
Scope limited to user?	<input type="checkbox"/>	
Special user for API (no access to admin.)	<input type="checkbox"/> Related FAQ	
Access rights	<input type="checkbox"/> Fraud detection <input type="checkbox"/> Technical information <input type="checkbox"/> Payment methods	
To confirm the modification, please enter your own password	<input type="text"/>	*

5.1.1 Dettagli di pre-inizializzazione

La maschera contiene tre campi dati pre-inizializzati:

- REFID: nome dell'entità a cui è collegato l'ID utente (per es. per un merchant: il suo PSPID).

- Tipo utente: tipo di entità a cui è collegato l'ID utente (per es. per un merchant: il suo "PSPID").
- Utente creato da: l'UserID dell'utente che sta creando questo nuovo utente / il suo tipo di utente / il suo REFID.

5.1.2 Dettagli utente

I dettagli utente che devono essere compilati sono:

- USERID: l'ID utente (username) per il nuovo utente (lunghezza almeno 3 e massima 20 caratteri, senza spazi o caratteri speciali).
- Nome utente: il nome completo del nuovo utente.
- Indirizzo e-mail: l'indirizzo e-mail del nuovo utente (nel caso in futuro venisse attivata una nuova password per questo utente, sarà inviata a questo indirizzo e-mail).

5.1.3 Fuso orario

Con la creazione d'utente, automaticamente verrà applicato il fuso orario del PSPID. Successivamente, l'utente può configurare il fuso orario di sua scelta.

Il fuso orario che l'utente sceglie è applicabile per tutte le pagine di back-office dove il tempo è relativo. In questo modo l'utente può anche visualizzare/scaricare operazioni e file/rapporti in proprio fuso orario preferito.

Inoltre il tempo può essere regolato automaticamente alle modifiche di risparmio di luce, selezionando la stessa opzione.

5.1.4 Profilo

Vedere [profili utente](#).

5.1.5 Accesso limitato all'utente

Queste opzioni possono essere configurate solo per i seguenti profili:

- codificatore
- super-codificatore
- super-codificatore senza rimborso

Se questa casella è abilitata, i codificatori potranno vedere ed accedere solo alle transazioni che hanno inserito/inizializzato essi stessi. Non saranno in grado di vedere/accedere a nessuna transazione inserita da altri utenti

Se questa casella è abilitata, i super-codificatori e super-codificatori senza rimborso potranno vedere, accedere ed effettuare solo operazioni di manutenzione sulle transazioni che hanno inserito/inizializzato essi stessi (ad eccezione delle operazioni di manutenzione inviate tramite caricamento di file). Non saranno in grado di vedere/accedere/effettuare operazioni di manutenzione su nessuna transazione inserita da altri utenti.

5.1.6 Utente speciale per API

Se si desidera creare un utente applicativo (utente API), è necessario abilitare questa casella. L'utente creato sarà utilizzato esclusivamente per l'accesso applicativo e non per l'accesso di back-office tramite pagina web.

5.1.7 Iritti di accesso

I diritti di accesso "rilevamento frodi", "metodi di pagamento" e "informazioni tecniche" possono essere attivata solo se le rispettive caselle sono abilitate.

Queste opzioni possono essere configurate solo per i seguenti profili:

- visualizzatore
- admin
- admin senza gestione utente

È possibile inserire le impostazioni dell'utente già immesse facendo clic sul pulsante "Crea". Se qualcuna delle informazioni è stata compilata in modo non corretto, si visualizza un messaggio di errore. L'utente appena creato non riceverà la sua prima password per e-mail, apparirà invece una schermata con la password che il nostro sistema ha creato per lui. Questa password potrà poi essere comunicata al nuovo utente.

5.2 Gestione password

È possibile inviare una nuova password ad un determinato utente facendo clic sul pulsante "Invia la nuova password". La nuova password sarà inviata all'indirizzo e-mail configurato nei dettagli utente.

Non è possibile assegnare una nuova password all'utente col cui nome si è effettuato l'accesso, o all'utente predefinito dell'account.

Se l'utente predefinito dell'account ha perso la password, può richiederne una nuova esclusivamente tramite il link "Hai dimenticato la password?" nella pagina di login. Nella pagina successiva dovrà compilare il PSPID e fare clic sul pulsante "Invia". Una mail con la nuova password sarà inviata all'indirizzo e-mail amministrativo dell'account.

Per gli utenti API non esiste un pulsante "Invia la nuova password". Per modificare la password di un utente API, è necessario utilizzare la funzione "Cambia la password". Si verrà reindirizzati ad una pagina in cui è possibile modificare la password manualmente.

Per maggiore sicurezza, puoi anche attivare o disattivare l'autenticazione a due fattori (2FA). Clicca [qui](#) per maggiori informazioni.

5.3 Disattivare utenti

È possibile impostare un utente come inattivo facendo clic sul pulsante "Disattiva" vicino all'utente. Quando un utente è inattivo egli non è autorizzato ad accedere al conto e non viene conteggiato nel numero di utenti autorizzati.

Per visualizzare l'elenco completo di utenti (sia attivi che inattivi) fare clic sul pulsante "Mostra utenti inattivi".

Per una compatibilità PCI e per ragioni di sicurezza voi/noi non siamo autorizzati a cancellare degli utenti.

5.4 Modifica dettagli utente

Per modificare i dettagli di un utente specifico fare clic sul pulsante "Modifica" vicino a quell'utente. Nel caso dell'utente predefinito dell'account è possibile modificare esclusivamente il nome e l'indirizzo e-mail.

5.5 Indirizzo IP

Per proteggere gli account dell'esercente del Back Office dall'accesso non autorizzato, gli utenti possono concedere l'accesso a uno specifico indirizzo IP (oppure a un elenco di indirizzi IP) registrando uno o più indirizzi nel campo dell'indirizzo IP.

Gli utenti devono accedere con il loro account per configurare il campo. Il campo dell'indirizzo IP si trova nella sezione di accesso della scheda Configurazione > Utenti.

5.5.1 Limitazioni utente dell'indirizzo IP

Gli utenti non si possono collegare al Back Office se l'indirizzo IP non rientra nell'intervallo definito.

Se il campo dell'indirizzo IP rimane vuoto, tuttavia, non esistono limitazioni di IP per il Back Office.

L'intervallo definito deve includere anche l'indirizzo IP dell'amministratore che configura l'intervallo IP. L'amministratore altrimenti riceve un messaggio d'errore e l'indirizzo IP non viene salvato.

5.5.2 Formato e valore dell'indirizzo IP

Occorre rispettare rigorosamente il formato dell'indirizzo IP:

- Deve essere conforme a CIDR, ad esempio: 212.166.204.28/32.
- Non deve contenere più di 512 caratteri
- Se si desidera registrare diversi indirizzi IP, è necessario separarli con punto e virgola.

6. Login Utente

Per accedere come utente è necessario usare la maschera di login con i seguenti tre campi: "UserID", "PSPID" e "password".

Se si visualizza la maschera di login con due campi (PSPID, password), è possibile passare alla maschera di login con tre campi facendo clic sul pulsante "Login utente" vicino alla maschera di login.

7. Tracciamento Utenti per Transazioni

I dettagli di pagamento di una transazione comprendono il campo "Codificato da". Questo campo contiene l'ID utente/PSPID/tipo di utente di colui che ha codificato la transazione. Questo campo non è visibile per gli utenti che sono stati configurati con un [Accesso limitato all'utente](#) nei dettagli utente.

Per visualizzare tutte le transazioni codificate da un utente specifico selezionare l'utente dall'elenco a discesa (chiamato "Codificato da") nei criteri di selezione avanzata di "Storia finanziaria" e "Visualizza le transazioni".

8. Sommario Autorizzazioni Utente

R = rosso (diritti a visualizzare), W = scrivere (diritto a modificare/inserire), bold = deve essere configurato nei dettagli utente.							
	Visualizza-tore	Codifica-tore	Super-Codifica-tore	Super-Codifica-tore e senza rimborso	Helpdesk Admin	Admin	Admin senza manager utente
Info contatto account lingue/URL /valuta	R	R	R	R		R W	R W
Account Abbonamento/opzioni						R W	R W
Info fatturazione account						R	R
Mezzo di pagamento	R					R W	R W
Utenti					R W	R W	
Aiuto	R W	R W	R W	R W	R W	R W	R W
Informazioni tecniche	R					R W	R W
Log di errore	R	R	R	R	R	R	R
Modulo rilevamento frodi	R					R W	R W
Storia finanziaria	R	R	R W	R W		R W	R W
Nuovo pagamento		R W	R W	R W		R W	R W
Visualizza le transazione	R	R	R W	R W		R W	R W
Nuovo file			R W	R W		R W	R W
Visualizza i file			R W	R W		R W	R W
Rapporto elettronico	R W	R W	R W	R W	R W	R W	R W
Alias Manager	R	R	R	R		R W	R W

8.1 Profili Rilevamento frodi

Nota: Per questi profili utente per funzionare correttamente, è necessario spuntare la casella "rilevamento frode" nei diritti di accesso dell'utente.

R = read (rosso, diritti a visualizzare), W = write (scrivere, diritto a modificare/inserire).

User Manager

	Fraud analyst	Fraud manager	Fraud viewer
Pagina di rilevamento delle frodi	R	R W	R
Pagina di rilevamento delle frodi: FDMA configuration & risk lists	R	R W	R
Pagina di rilevamento delle frodi: 3-D Secure configuration	R	R W	R
Pagina di rilevamento delle frodi: Blacklists/Whitelists	R W	R W	R
Scoring details page	R	R	R
Scoring details page: fill dispute + Blacklists/Whitelists	R W	R W	-
Score details page: review transactions	R W	R W	-