User Manager

ingenico
ePayments

Inhaltsverzeichnisses

1. Was ist der Benutzer Manager?

In einem Unternehmen existieren generell verschiedene Funktionen/Tätigkeitsprofile (Rollen). Ein Buchhalter wird bespielsweise nicht dieselben Aufgaben wie ein Datenerfasser oder ein technischer Integrator erfüllen. Ganz logisch werden Sie darum jedem einzelnen Mitarbeiter, der Ihr Konto nutzt, nur die nötigen Zugangsrechte einräumen und zudem kontrollieren, welche Aktionen welcher Benutzer veranlasst hat.

Die Option Benutzer Manager hilft Ihnen dabei, jedem Benutzer ein spezifisches Profil zuzuordnen, das ihm die zur Erfüllung seiner Aufgaben notwendigen Zugangsrechte gibt. Der Benutzer Manager ist ein für alle Produkte erhältlicher zusätzlicher Service.

Mit dem Benutzer Manager können Sie:

- Unter einem Konto mehrere Benutzer konfigurieren
- Profil und Zugangsrechte jedes Benutzers verwalten
- Kritische Fehler von Datenerfassern vermeiden
- Die Aktivitäten jedes Benutzers verfolgen (beispielsweise die Anzahl von Transaktionen pro Tag)
- Benutzern nur Leserechte für die eigenen Transaktionen gestatten
- Bequem die Zugangsrechte für vorübergehende Mitarbeiter verwalten

Sie können die Benutzer Manager zugreifen, durch Auswahl von "Konfiguration> Benutzerverwaltung" im Menü Ihres Ingenico ePayments Kontos.

2. Activation

Standardmäßig wird Ihre Ingenico ePayments Konto mit zwei Benutzer; PSPID Ihr Standard-Benutzer (admin) und eine zusätzliche Benutzer.

Wenn Sie mehrere Benutzer,-je nach Ihrem Abonnement benötigen, können Sie die Option in Ihrem Ingenico ePayments Konto zu aktivieren:

1. Gehen Sie auf "Konfiguration > Konto > Ihre Optionen".
2. Suchen Sie in der Liste der Optionen für "User Manager up to x users" ("x" definiert die Anzahl der Benutzer, die Sie erstellen möchten: 5, 10, 20 ... 200)
3. Klicken Sie auf die Schaltfläche "Aktivieren".

Abhängig von den Optionen, die Sie aktiviert haben, können Sie weitere Benutzer mit unterschiedlichen Profilen und Konfigurationen erstellen.

3. Benutzerprofile

Zu den wichtigsten Benutzerprofilen, die vom Benutzer Manager unterstützt werden, gehören:

- Betrachter
- Kodierer
- Superkodierer
- Superkodierer ohne Gutschriften
- Administrator ohne Benutzer Manager
- Administrator
- Helpdesk Admin

3.1 Administrator

Ein Administrator besitzt uneingeschränkte Zugangsrechte.

Immer wenn ein Konto angelegt wird, wird automatisch auch ein Standard-Benutzer angelegt (die UserID dieses Standard-Benutzers ist identisch mit der PSPID). Diesem Standard-Benutzer ist ein Admin-Profil zugeordnet. Sie können darüber hinaus natürlich weitere Benutzer mit Admin-Rechten anlegen.

Ein Admin-Benutzer besitzt als einziger Benutzertyp die Rechte zu Änderungen an der Konfiguration des Kontos.

3.2 Administrator ohne Benutzer Manager

Dieser Benutzertyp besitzt die gleichen Rechte wie ein Administrator mit dem Unterschied, dass er keinen Zugriff auf die Option Benutzer Manager erhält.

3.3 Kodierer

Ein Kodierer kann eine neue Zahlung über den Link "Neue Transaktion" im Kontomenü oder über DirectLink einreichen.

3.4 Betrugsanalytiker

Ein Betrugsanalytiker (Fraud analyst) kann Blacklists/Whitelists bearbeiten, das Scoring von Transaktionen einsehen und Transaktionen zu Streitfällen erheben.

Hinweis: Damit dieses Anwenderprofil korrekt funktioniert, müssen Sie in den Zugriffsrechten des Anwenders die Option „Betrugserkennung" auswählen.

3.5 Betrugsmanager

Ein Betrugsmanager (Fraud manager) kann alle relevanten Konfigurationsseiten für die Betrugserkennung bearbeiten, Blacklists/Whitelists bearbeiten, Transaktionen einsehen und zu Streitfällen erheben usw.

Hinweis: Damit dieses Anwenderprofil korrekt funktioniert, müssen Sie in den Zugriffsrechten des Anwenders die Option „Betrugserkennung" auswählen.

3.6 Betrugsbeobachter

Ein Betrugsbeobachter (Fraud Viewer) kann verschiedene Konfigurationsseiten für die Betrugserkennung einsehen, jedoch keine Änderungen darin vornehmen.

Hinweis:Damit dieses Anwenderprofil korrekt funktioniert, müssen Sie in den Zugriffsrechten des Anwenders die Option „Betrugserkennung" auswählen

3.7 Helpdesk-admin

Ein Helpdesk-Admin hat nur Zugriff auf die Seite "Benutzermanagement" im Konto.

Weitere Informationen finden Sie unter Benutzerberechtigungen Übersicht für die verschiedenen Profile.

3.8 Superkodierer

Ein Superkodierer kann nicht nur neue Transaktionen einreichen, sondern auch Datenpflegeaktionen bezüglich bestehender Transaktionen veranlassen. Er kann weiterhin Zahlungsdateien hochladen und Transaktionsberichte herunterladen.

3.9 Superkodierer ohne Gutschriften

Dieser Benutzertyp verfügt über die gleichen Zugangsrechte wie ein Superkodierer mit dem Unterschied, dass er keine Gutschriften veranlassen oder Autorisierungen stornieren kann. Dieses Profil erlaubt es Ihnen, Rechte für die Veranlassung von Kontobelastungen zu erteilen, ohne gleichzeitig Gutschriften oder die Löschung von Zahlungen zu gestatten.

3.10 Betrachter

Das Profil Betrachter eignet sich ideal für Buchhaltungskräfte. Ein Betrachter kann den Status von Transaktionen und Berichte anzeigen oder abrufen, aber keine Änderungen vornehmen oder Transaktionen einreichen. Es handelt sich um ein Zugangsprofil mit reinem Leserecht.

4. Benutzertypen

Wir haben darum zwei Benutzertypen vorgesehen:

- den Back-Office-Benutzer (= den ADM Benutzer)
- den applikationsgebundenen Benutzer (= den API Benutzer)

4.1 Back-Office-Benutzer (ADM User)

Ein Back-Office-Benutzer (ADM User) ist ein Benutzer, der Zugriffsrecht für das Kontoverwaltungsmodul (Back-Office) über die Website besitzt.

Ein Back-Office-Benutzer muss alle 90 Tage sein Passwort ändern. Dies kann er über den Link "Passwort" im Kontomenü tun.

4.2 API Benutzer

Ein API Benutzer (Application Program Interface) ist ein Benutzer, der speziell zur Nutzung durch eine Applikation konzipiert ist, um automatische Anfragen an die Zahlungsplattform vorzunehmen (automatisches Upload/Download von Dateien, direkte Zahlungsanfragen usw.).

Auch wenn für eine API Benutzer die verschiedenen Benutzerprofile zur Verfügung stehen, empfehlen wir Ihnen dringend, diese Benutzer mit der "Admin"-Profil konfigurieren. Wenn Sie die Rechte für die Wartung der Transaktionen (Erstattungen, Stornierungen etc.) beschränken möchten, können Sie immer noch auf "Encoder" ändern Sie den Benutzerprofil.

Wenn Sie nicht sicher sind, empfehlen wir Ihnen, den "Admin"-Profil wählen, ansonsten auf Benutzerprofile, um weitere Informationen zu gehen.

Das Passwort für einen API-Benutzer muss nicht regelmäßig geändert werden, was bequemer ist, falls das Passwort fest im Programmcode ihrer Applikation verankert ist. Wir empfehlen aber dennoch, das Passwort von Zeit zu Zeit zu ändern.

Um das Passwort eines API Benutzers zu ändern:

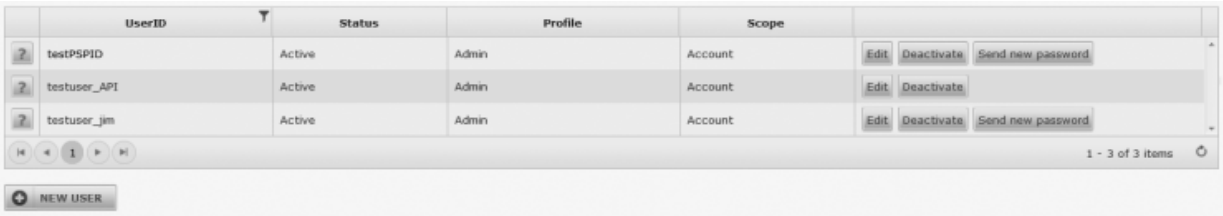
1. Klicken Sie auf "Benutzerverwaltung"
2. Klicken Sie die Schaltfläche "Passwort ändern" des betreffenden API Benutzers. Sie werden auf eine Seite umgeleitet, auf der Sie das Passwort ändern können. Auch wenn Sie einen neuen API Benutzer erstellen, werden Sie auf diese Seite geleitet.

Aus Sicherheitsgründen erhalten API-Benutzer keinen Zugang zum Kontoverwaltungsmodul, d. h. sie können sich nicht ins Back-Office einloggen.

5. Benutzerverwaltung

Auf der Seite Benutzermanagement können Sie:

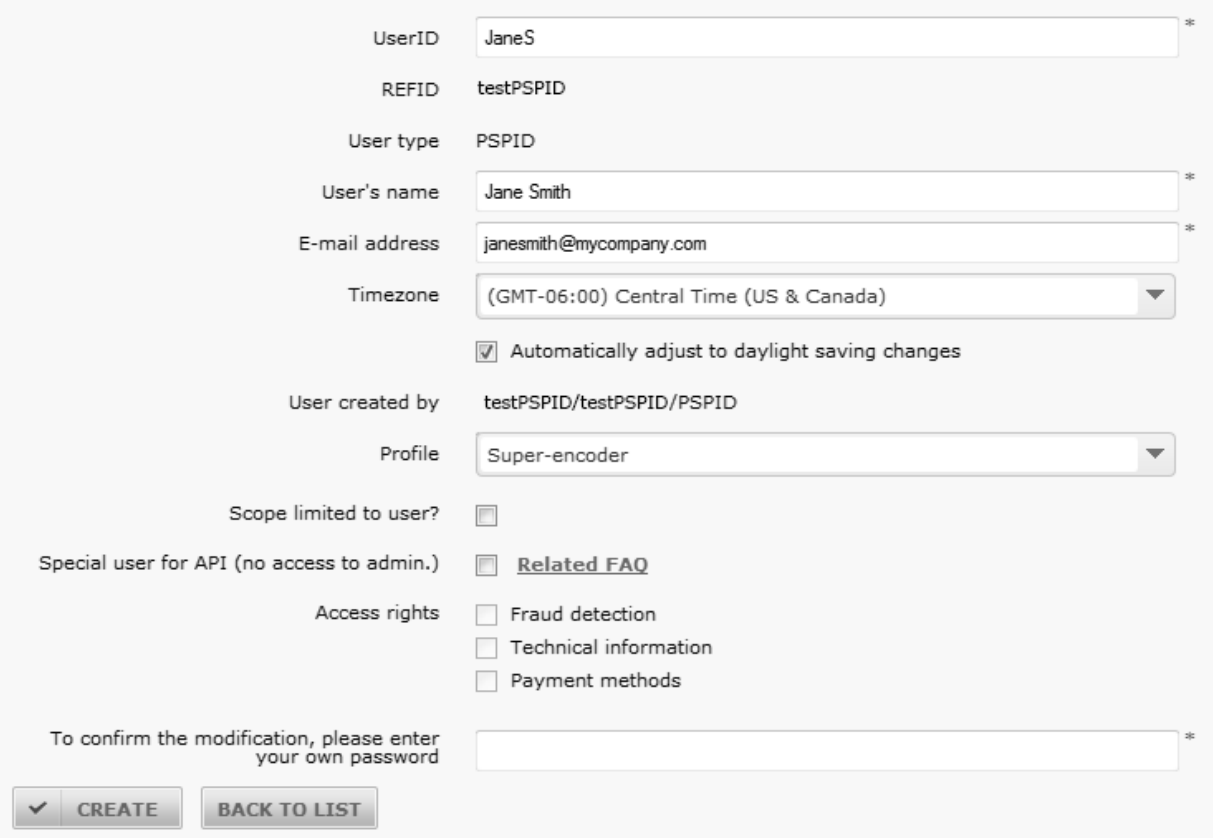
- neue Benutzer anlegen
- die Benutzerpasswörter verwalten
- nicht länger im Unternehmen aktive Benutzer deaktivieren
- Benutzerdaten bearbeiten



Die zulässige Zahl von Benutzern wird auf der Menüseite Benutzermanagement angezeigt. Sobald die zulässige Zahl von Benutzern erreicht ist, wird die Schaltfläche "Neuer Benutzer" abgeblendet.

5.1 Neuen Benutzer anlegen

Um einen neuen Benutzer anzulegen, klicken Sie die Schaltfläche "Neuer Benutzer" auf der Seite Benutzermanagement an. Um den neuen Benutzer zu erstellen, muss das angezeigte Formular ausgefüllt werden.



5.1.1 Vorab eingetragene Daten

Das Formular enthält drei Felder mit vorab eingetragenen Daten:

- REFID: Name der Entität, mit der die UserID verknüpft ist (bei einem Händler beispielsweise dessen PSPID).
- Benutzertyp: Typ der Entität, mit der die UserID verknüpft ist (für einen Händler beispielsweise: "PSPID").
- Benutzer erstellt von: Die UserID des Benutzers, der diesen neuen Benutzer anlegt / seinen Benutzertyp / seine REFID.

5.1.2 Benutzerdaten

Folgende Benutzerdaten müssen angegeben werden:

- USERID: Die UserID (Benutzername) für den neuen Benutzer (min. 3 und max. 20 Zeichen lang, keine Leerstellen oder Sonderzeichen erlaubt).
- Benutzername: Voller Name des neuen Benutzers.
- E-Mailadresse: E-Mail-Adresse des neuen Benutzers (ein künftig ausgelöstes neues Passwort wird an diese E-Mail-Adresse gesendet).

5.1.3 Zeitzone

Mit der Schaffung eines Benutzers wird automatisch die Zeitzone des PSPID angewendet. Danach kann der Benutzer die Zeitzone seiner Wahl zu konfigurieren.

Die Zeitzone, die der Benutzer auswählt, ist für alle Back-Office-Seiten, auf denen die Zeit ist relevant. Auf diese Weise kann der Benutzer auch ansehen und Download-Transaktionen und Dateien/Berichte in seinem eigenen bevorzugten Zeitzone.

Darüber hinaus kann die Zeit automatisch auf Sommerzeit-Umstellung angepasst werden, durch die Option zu wählen.

5.1.4 Profile

Siehe Benutzerprofile.

5.1.5 Bereich auf Benutzer beschränken

Diese Optionen können nur für die folgenden Profile konfiguriert werden:

- Kodierer
- Superkodierer
- Superkodierer ohne Gutschriften

Wenn dieses Kontrollkästchen aktiviert ist, können Kodierer nur Transaktionen anzeigen und darauf zugreifen, die sie selbst eingegeben/veranlasst haben. Von anderen Benutzern eingegebene Transaktionen können sie weder anzeigen noch darauf zugreifen.

Wenn dieses Kontrollkästchen aktiviert ist, können Superkodierer und Superkodierer ohne Gutschriften nur Datenpflegeaktionen bezüglich Transaktionen anzeigen, darauf zugreifen und sie veranlassen, die sie selbst eingegeben/veranlasst haben (ausgenommen Aktionen zur Datenpflege, die per Dateiupload eingereicht werden). Aktionen zur Datenpflege bezüglich Transaktionen, die von anderen Benutzern eingegeben wurden, können sie weder anzeigen, noch darauf zugreifen oder veranlassen.

5.1.6 Spezieller Benutzer für API

Wenn Sie einen applikationsgebundenen Benutzer (API Benutzer) anlegen wollen, müssen Sie dieses Kontrollkästchen aktivieren. Der von Ihnen angelegte Benutzer wird nur für applikationsgebundenen Zugang genutzt und nicht für den Back-Office-Zugang über die Website.

5.1.7 Spezieller Zugriff

Die Betrugserkennung, Zahlungsmethoden und Technische Informationen Zugriffsrechte können aktiviert werden, wenn Sie die entsprechenden Kontrollkästchen aktivieren.

Diese Optionen können nur für die folgenden Profile konfiguriert werden:

- Betrachter
- Administrator

- Administrator ohne Benutzer Manager

Um die eingegebenen Benutzereinstellungen zu aktivieren, klicken Sie die Schaltfläche "Erstellen" an. Sollte eine der Angaben falsch eingetragen sein, erscheint eine Fehlermeldung. Der neue Benutzer bekommt das neue Passwort nicht per E-Mail zugeschickt. Stattdessen erscheint am Bildschirm ein Fenster mit dem von unserem System für den Benutzer erzeugten Passwort. Dieses Passwort kann dann dem neuen Benutzer mitgeteilt werden.

5.2 Passwortverwaltung

Um einem bestimmten Benutzer ein neues Passwort zu schicken, klicken Sie die Schaltfläche "Neues passwort senden" an. Das neue Passwort wird an die in den Benutzerdaten angegebene E-Mail-Adresse gesendet.

Sie können kein neues Passwort an den Benutzer vergeben, unter dem Sie selbst angemeldet sind, und auch nicht an den Standard-Benutzer des Kontos.

Wenn der Standard-Benutzer des Kontos sein Passwort verloren hat, kann er ein neues Passwort nur über den Link "Passwort vergessen?" auf der Anmeldeseite anfordern. Auf der nachfolgenden Seite gibt er seine PSPID ein und klickt auf die Schaltfläche "Abschicken". An die E-Mail-Adresse des Administrators des betreffenden Kontos wird dann eine E-Mail mit dem neuen Passwort gesendet.

Für API Benutzer gibt es keine "Neues Passwort senden" Schaltfläche. Um das Passwort eines API Benutzers zu ändern, nutzen Sie bitte die "Passwort ändern" Schaltfläche. Sie werden auf eine Seite umgeleitet, auf der Sie das Passwort manuell ändern können

5.3 Benutzer deaktivieren

Um einen Benutzer zu deaktivieren, klicken Sie die Schaltfläche "Deaktivieren" neben dem betreffenden Benutzer an. Sobald ein Benutzer deaktiviert ist, kann er sich nicht mehr beim Konto anmelden und wird bei der zulässigen Zahl von Benutzern nicht mehr berücksichtig.

Um eine komplette Liste der Benutzer (aktive und inaktive) anzuzeigen, klicken Sie die Schaltfläche "Inaktive Benutzer anzeigen" an.

Zur Einhaltung der PCI-Vorschriften und aus Sicherheitsgründen ist es weder Ihnen noch uns erlaubt, Benutzer zu löschen.

5.4 Benutzerdaten bearbeiten

Um die Daten eines bestimmten Benutzers zu bearbeiten, klicken Sie die Schaltfläche "Ändern" neben dem betreffenden Benutzer an. Wenn es sich hierbei um den Standard-Benutzer des Kontos handelt, können nur Name und E-Mail-Adresse geändert werden.

5.5 IP-Adresse

Zum Schutz vor unerlaubtem Zugriff auf die Back-Office-Händlerkonten können die Benutzer einer bestimmten IP-Adresse (oder Liste mit IP-Adressen) Zugang gewähren, indem die Adresse(n) in dem IP-Adressfeld registriert wird/werden.

Die Benutzer müssen sich mit ihrem Konto anmelden, um dieses Feld konfigurieren zu können. Das IP-Adressfeld befindet sich in Anmeldezugriff unter der Registerkarte *Configuration* > *Users* (Konfiguration > Benutzer).

5.5.1 Nutzerbeschränkungen bei IP-Adresse

Benutzer können sich nicht mit der Back-Office verbinden, wenn sich ihre IP-Adresse nicht in dem definierten Bereich befindet.
Wenn allerdings das IP-Adressfeld leer gelassen wird, gibt es keine IP-Einschränkungen zur Back-Office.
Die IP-Adresse des Administrators, der den IP-Bereich konfiguriert, muss sich ebenfalls in dem definierten Bereich befinden. Andernfalls erhält der Administrator eine Fehlermeldung und die IP-Adresse wird nicht gespeichert.

5.5.2 IP-Adressformat und -Wert

Außerdem muss ein striktes IP-Adressformat befolgt werden:
- CIDR-konform, z.B.: 212.166.204.28/32.
- Ist maximal 512 Zeichen lang

- Wenn Sie mehrere IP-Adressen registrieren möchten, müssen Sie diese durch Semikolons trennen.

6. Anmeldung als Benutzer

Um sich als Benutzer anzumelden, müssen Sie das Anmeldeformular mit den drei folgenden Feldern verwenden: "UserID", "PSPID" und "Passwort".

Erscheint das Anmeldeformular mit zwei Feldern (PSPID, Passwort), können Sie auf das Formular mit drei Feldern umschalten, indem Sie die Schaltfläche "User login" neben dem Anmeldeformular anklicken.

7. Benutzertransaktionen Verfolgen

Zu den Zahlungsdaten einer Transaktion gehört auch das Feld "Kodiert von". Dieses Feld enthält UserID/PSPID/Benutzertyp des Benutzers, der die Transaktion erfasst hat. Dieses Feld ist nicht sichtbar für Benutzer, die in den Benutzerdaten mit Bereich auf Benutzer beschränken konfiguriert wurden.
Um alle von einem bestimmten Benutzer erfassten Transaktionen anzuzeigen, wählen Sie in den erweiterten Auswahlkriterien für "Finanzielle Historie" bzw. "Transaktionsansicht" den Benutzer aus der Drop-down-Liste ‘Kodiert von’.

8. Benutzerrechte im Überblick

R = read (Anzeigen), W = write (Ändern/Einreichen), **fett** = muss in den Benutzerdaten konfiguriert werden.

	Betrachter	**Kodierer**	**Super-kodierer**	**Superkodierer ohne Gutschriften**	**Helpdesk Admin**	**Admin**	**Administrator ohne Benutzer Manager**
Konto Kontaktdaten Sprachen/URL /Währungen	R	R	R	R		R W	R W
Konto Subscription/ Optionen						R W	R W
Konto Rechnungsdaten						R	R
Zahlungsmethoden	**R**					**R W**	**R W**
Benutzerverwaltung					R W	R W	
Support	R W	R W	R W	R W	R W	R W	R W
Technische Informationen	**R**					**R W**	**R W**
Fehlerprotokolle	R	R	R	R	R	R	R
Betrugserkennung	**R**					**R W**	**R W**
Finanzielle Historie	R	R	R W	R W		R W	R W
Neue Transaktion		R W	R W	R W		R W	R W
Transaktionsansicht	R	R	R W	R W		R W	R W
Batchupload			R W	R W		R W	R W
Batchübersicht			R W	R W		R W	R W
Reporting	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 Benutzerprofile für die Betrugserkennungsmodul

Hinweis: Für diese Benutzerprofile, um richtig funktionieren Sie müssen dazu den "Fraud Detection" Checkbox in die Zugriffsrechte des Benutzers zu überprüfen.

R = read (Anzeigen), W = write (Ändern/Einreichen).

	Betrugsbeobachter	Betrugsanalytiker	Betrugsmanager
Betrugserkennung	R	R W	R
Betrugserkennung: Konfiguration der FDMA & Risikolisten	R	R W	R
Betrugserkennung: Konfiguration 3-D Secure	R	R W	R
Betrugserkennung: Blacklists/Whitelists	R W	R W	R
Scoring Details Seite	R	R	R
Scoring Details Seite: Fill Dispute + Blacklists/Whitelists	R W	R W	-
Score Details Seite: Bewertung Transaktionen	R W	R W	-