Unica Journey
12.1 - Guide d'administration

Contents

Chapter 1. Introduction à Unica Journey

Unica Journey est une solution d'orchestration basée sur les objectifs qui permet de concevoir, d'exécuter et de visualiser des expériences client contextualisées, personnalisées, omnicanales en plusieurs étapes.

Les spécialistes du marketing peuvent utiliser Unica Journey pour :

- Définir des objectifs pour l'expérience client
- Ajuster facilement les parcours en temps réel pour les accomplir
- Concevoir et visualiser un parcours client entier sur les canaux/points de contact et les événements à l'aide d'une zone de conception de Journey élégante et intuitive

Les parcours client sont entièrement automatisés et synchronisés à chaque étape de l'engagement de marque de votre client. Utilisez les connaissances en temps réel dans Journey pour comprendre le comportement des clients grâce à des connaissances qui reflètent les expériences qui se produisent dans leur Journey.

Fonctionnalités de Unica Journey

Les fonctions de Unica Journey sont les suivantes :

- **Expériences basées sur des objectifs** : Définissez des objectifs pour votre expérience client et ajustez facilement vos parcours en temps réel pour les atteindre.
- **Zone de conception d'orchestration** : Concevez et visualisez l'intégralité du parcours client à travers les canaux, les points de contact et les événements grâce à une zone de conception de Journey élégante et intuitive.
- **Toujours l'engagement** : Une exécution totalement automatisée qui est synchronisée à chaque étape de l'engagement de votre client.
- **Connaissances en temps réel** : Comprenez le comportement des clients grâce à des connaissances qui reflètent les expériences qui se produisent dans leur parcours.

- **Choix de points de contact** : Tirez parti des points de contact natifs et orginaux pour les canaux numériques ou élaborez un point de contact personnalisé et orchestrez en toute transparence le parcours dans votre écosystème.
- **Structure de données dynamiques** : Définitions de données et sources d'entrée flexibles pour enrichir le parcours des clients à l'aide de données contextuelles et d'événements provenant de plusieurs points de contact et dans divers formats (fichier, API, etc.)

Avantages de Unica Journey

Les avantages de Unica Journey sont les suivants :

- **Meilleure fidélité à la marque** : Renforcez votre marque en suivant les parcours ciblés et automatisés qui acquièrent, accroissent, convertissent et retiennent les clients.
- **Engagement omnicanal amplifié** : Fournir une expérience client cohérente sur les canaux avec une intégration native pour les engagements sortants (Unica Campaign) et entrants (Unica Interact, Unica Discover et Unica Deliver).
- **Réduction du cycle de conversion client** : Ayez une longueur d'avance et guidez votre client vers ses objectifs avec les meilleures actions suivantes.
- **Réaction au moment présent** : Vous ne manquerez plus aucune possibilité de savoir où votre client se trouver sur son parcours et de lui faire plaisir grâce à une expérience pertinente.
- **Réduction du TCO marketing** : Réduisez votre TCO marketing grâce aux flux automatisés et à l'intégration plug and play à votre écosystème MarTech via une structure ouverte et flexible, alimentée par Unica Link.

Chapter 2. Intégrations de Unica Journey

Unica Journey moteurs d’exécution pour la messagerie

Unica Journey prend en charge Unica Deliver et Unica Link pour la distribution de courrier électronique. Vous pouvez utiliser l'un ou l'autre pour l’intégration à Journey.

Unica Journey intégration Unica Link

Unica Link fournit des fonctions permettant d’envoyer des communications entre les canaux e-mail, SMS et CRM. Unica Link fournit les connecteurs de référence suivants pour fournir des communications aux canaux de messagerie, SMS et CRM.

Installez les connecteurs de référence suivants en fonction de vos préférences :

- **MailChimp** – pour la messagerie
- **Mandrill** – pour la messagerie
- **Twilio** – pour les SMS
- **Salesforce** – pour le CRM

L’intégration avec Unica Link permet à Journey de s’intégrer à des fournisseurs tiers pour les exécutions d’e-mail, de SMS et de CRM.

Table 1. installation et configuration de Unica Link

Tâche	**Documentation**
installation et configuration de Unica Link	Voir *Unica Link V12.1 - Guide d'installation*.
Installation de l’application de connecteur Unica Link pour Journey	Voir *Unica Link V12.1 - Guide d'installation*.
Installation du connecteur Unica Link – MailChimp	Voir *Unica Link - Connecteur MailChimp - Guide d’utilisation*.
Installation du connecteur Unica Link – Mandrill	Voir *Unica Link - Connecteur Mandrill - Guide d’utilisation*.
Installation du connecteur Unica Link – Twilio	Voir le *Unica Link - Connecteur Twilio - Guide d’utilisation*.
Installation du connecteur Unica Link – Salesforce	Voir *Unica Link - Connecteur Salesforce - Guide d’utilisation*.

Note: HCL ne fournit pas le compte ou l'accès à ces fournisseurs de canaux de distribution. En fonction de vos préférences, vous pouvez obtenir les droits ou les comptes pour ces fournisseurs.

Unica Journey intégration Unica Deliver

Unica Journey utilise les fonctions de Unica Deliver pour envoyer des communications de type Courrier électronique. Cela permet également de capturer les réponses aux courriers électroniques en temps réel et à traiter le Journey de l'audience. Pour plus de détails sur l'activation de l'intégration Unica Deliver avec Unica Journey, voir Unica Journey - Guide d'installation.

Intégration **Unica Journey avec Unica Campaign et Unica Interact**

Unica Journey s'intègre en toute transparence avec Unica Campaign et Unica Interact. Unica Campaign et Unica Interact envoient des données d'audience à Unica Journey sur une rubrique Kafka spécifique. Les données d'audience sont envoyées via une source d'entrée Kafka et envoyées dans tous les parcours qui utilisent des données provenant de ces sources d'entrée.

Pour plus d'informations sur l'intégration de Unica Campaign et Unica Interact avec Unica Journey, voir les guides mentionnés dans le plan de documentation suivant.

Journey prend en charge les données provenant de plusieurs partitions de Campaign

Journey prend en charge les données provenant de plusieurs partitions de Campaign. Vous devez apporter des modifications à la plateforme de configuration, aux rôles utilisateur et aux autorisations :

- Les détails du diagramme Campaign affichés sous les sources d'entrée proviennent de plusieurs partitions.
- En fonction de la partition, les modèles Deliver s'affichent dans les points de contact e-mail/SMS/WhatsApp.

Table 2. Intégration de Unica Campaign à d'autres produits HCL

Tâche	Documentation
Intégration de Unica Campaign et Unica Journey	Voir *Unica Campaign - Guide d'administration* et *Unica Campaign - Guide d'utilisation*.
Intégration de Unica Campaign et Unica Interact	Voir *Unica Interact - Guide d'administration*.

Unica Journey intégration à Unica Discover

Unica Journey s'intègre de manière transparente à UNICA Discover. Unica Discover envoie des données de difficultés d'audience à Unica Journey. Les données d'audience sont envoyées via une source d'entrée REST et envoyées dans tous les parcours qui utilisent des données provenant de ces sources d'entrée. Quatre scripts seront fournis. Après avoir installé Journey, vous devez exécuter les scripts immédiatement, ce qui crée deux sources d'entrée et deux définitions de données appelées source d'entrée Discover pour CART et source d'entrée Discover pour le formulaire.

Nom symbolique	Panier
Description	Lorsque le client abandonne tout type de panier ou d'ensemble d'offres sélectionnées, cet événement peut être déclenché.

Table 3. Attributs à envoyer sur

Nom	Type	Longueur	Remarque
E-mail*	TEXT	200	Cette zone est obligatoire.
Nom	TEXT	200	
DiscoverSessionId	TEXT	50	ID de session Discover requis pour le lier à nouveau.
CartId	TEXT	50	ID unique permettant d'identifier le panier.
CartValue	NUMBER		

Nom	Type	Longueur	Remarque
EventDateTime	TIMESTAMP		Date et heure de l'événement en longitude UTC
EventType	TEXT		Le type d'événement peut être CART_ABANDONED
CookieID	TEXT	1024	
TLT_BROWSER	TEXT	50	Détails du navigateur
TLT_MODEL	TEXT	50	Caractéristiques de l'unité
HTTP_ACCEPT_LANGUAGE	TEXT	50	Langue

Nom symbolique	Formulaire
Description	Lorsque le client remplit un formulaire WebForm, cet événement peut être publié.

Table 4. Attributs à envoyer sur

Nom	Type	Longueur	Remarque
E-mail*	TEXT	200	Cette zone est obligatoire.
Nom	TEXT	200	
DiscoverSessionId	TEXT	50	ID de session Discover requis pour le lier à nouveau.
FormId	TEXT	50	ID unique permettant d'identifier le formulaire
FormName	TEXT	100	
EventDateTime	TIMESTAMP		Date et heure de l'événement en longitude UTC
CookieID	TEXT	1024	

Nom	Type	Longueur	Remarque
TLT_BROWSER	TEXT	50	Détails du navigateur
TLT_MODEL	TEXT	50	Caractéristiques de l'unité
HTTP_ACCEPT_LANGUAGE	TEXT	50	Langue
EventType	TEXT		Le type d'événement peut être FORM_SUBMITTED, FORM_ABANDONED

Note: A partir du groupe de correctifs 3, la fonction d'intégration d'Unica Journey à Unica Discover est disponible.

Introduction à Unica Deliver

Unica Deliver est une solution de messages marketing à l'échelle de l'entreprise et basée sur le Web, que vous pouvez utiliser pour exécuter des campagnes d'envoi de messages en masse et de messages transactionnels. Deliver s’intègre à Unica Campaign et à des ressources de composition, de transmission et de suivi des messages sécurisées et hébergées par Unica.

Vous pouvez utiliser Deliver pour créer, envoyer et suivre des communications de type Courrier électronique personnalisées. Comme Deliver s'installe et fonctionne avec Campaign, vous pouvez utiliser des diagrammes Campaign pour sélectionner et segmenter avec précision les informations relatives aux destinataires afin de personnaliser chaque message.

Sélectionnez votre audience

Utilisez Campaign pour sélectionner les destinataires de message et les données relatives à chaque personne que vous pouvez utiliser pour personnaliser chaque message.

Deliver vous permet d’atteindre rapidement et personnellement un grand nombre de destinataires par courrier électronique. Toutefois, vous pouvez également configurer un

mailing pour envoyer automatiquement un seul message électronique en réponse à une transaction.

Créez un message

Deliver Document Composer fournit des outils d'édition que vous pouvez utiliser pour concevoir, prévisualiser et publier du contenu de message personnalisé. Vous pouvez créer des messages avec un contenu que vous chargez dans l'éditeur de message ou effectuer un lien vers du contenu externe lors de la génération et de la transmission de messages par Deliver. Deliver fournit plusieurs méthodes pour concevoir des messages qui affichent du contenu de manière conditionnelle, en fonction des données personnelles de chaque destinataire.

Envoyer le message et suivre les réponses

Selon vos objectifs, vous pouvez planifier l'exécution d'une campagne de messagerie dès que possible ou la planifier pour qu'elle s'exécute plus tard. Deliver surveille la distribution des messages et effectue le suivi des réponses des destinataires. Le système renvoie les données de contact et de réponse aux tables système Deliver installées dans le cadre du schéma de base de données Campaign.

Comment commencer

Pour commencer, vous devez installer Campaign et disposer d'un compte de messagerie hébergé.

Les administrateurs système doivent demander un compte de messagerie hébergé et travailler avec Unica pour configurer un accès sécurisé aux systèmes de messagerie et de suivi distants. Certaines fonctions de messagerie ne sont disponibles que sur demande à Unica. Pour plus d'informations sur l'établissement d'un compte de messagerie hébergée et la configuration de l'accès à la messagerie hébergée Unica, voir le document Unica Deliver - Guide de démarrage et d'administration.

Intégration Unica Deliver

Pour intégrer Unica Deliver à Unica Journey, vous devez effectuer les configurations suivantes dansUnica Platform.

1. Dans Unica Platform, accédez à **Paramètres > Configuration**.
   La page **Catégories de configuration** s'affiche.

2. Sélectionnez **Journey**.
   La page **Paramètres pour 'Journey'** s'affiche.

3. Sélectionnez **Modifier les paramètres**.
   La page **(Journey)** s'affiche.

4. Effectuez les opérations suivantes :
   a. Dans la zone **Deliver_Configured**, sélectionnez **Oui**.
   b. Cliquez sur **Enregistrer les modifications**.

5. Dans le nœud de parcours étendu, sélectionnez **Deliver_Configurations**.
   La page **Paramètres pour 'Deliver_Configurations'** s'affiche.

6. Sélectionnez **Modifier les paramètres**.
   La page **(Deliver_Configurations)** s'affiche.

7. Effectuez les opérations suivantes :

   a. Indiquez des valeurs pour les zones suivantes :
      - **Deliver_URL** : L'URL configurée pour Deliver.
      - **Deliver_Partition** : Partition dans laquelle sont stockées les données d'identification permettant d'accéder à **Deliver_URL**.

   b. Cliquez sur **Enregistrer les modifications**.

Intégration Kafka

Vous devez configurer Kafka dans Unica Platform pour le noeud Journey.

Accès à Kafka_Configurations dans Unica Platform

Pour accéder à Kafka_Configurations, procédez comme suit :

1. Dans Unica Platform, accédez à **Paramètres > Configuration**.
2. Développez le nœud **Journey**.
3. Sélectionnez **Kafka_Configurations**.
4. Sélectionnez **Modifier les paramètres**.

Configurations obligatoires en fonction de la valeur de CommunicationMechanism

Sur la page **(Kafka_Configurations)**, vous pouvez sélectionner l'une des valeurs suivantes pour la zone CommunicationMechanism :

- NO_SASLPLAINTEXT_SSL
- SASL_PLAINTEXT
- SSL
- SASL_PLAINTEXT_SSL

En fonction de votre sélection, les zones suivantes deviennent obligatoires :

Nom de zone	NO_SASLPLAINTEXT_SSL	SASL_PLAINTEXT	SSL	SASL_PLAINTEXT_SSL
KafkaBrokerURL	Oui	Oui	Oui	Oui
TopicName	Oui	Oui	Oui	Oui
sasl.mechanism		Oui		Oui
UserForKafkaDataSource		Oui	Oui	Oui
sasl.jaas.config.dataSource		Oui		Oui
truststore.location			Oui	Oui
truststore.password.dataSource			Oui	Oui
keystore.location			Oui	Oui
keystore.password.dataSource			Oui	Oui
key.password.dataSource			Facultatif	Facultatif
ssl.endpoint.identification.algorithm			Oui	Oui

Apportez les modifications nécessaires, puis cliquez sur **Enregistrer les modifications**

Chapter 3. Rôles utilisateur et droits d'accès Journey

Avant de commencer à utiliser Unica Journey, vous devez attribuer des rôles et des droits aux utilisateurs.

Note: Toute modification de la configuration nécessite de redémarrer Unica Journey. Pour en savoir plus sur les configurations de sécurité, consultez *Unica Platform - Guide d'administration*.

Affectation de droits aux rôles Journey

Avant d'affecter un rôle à un utilisateur, vous devez affecter des droits aux rôles disponibles.

Journey offre deux rôles utilisateur :

- **JourneyAdmin**
- **JourneyUtilisateur**

Pour affecter des droits aux deux rôles, procédez comme suit :

1. Depuis la page d'accueil de Unica Platform, sélectionnez **Paramètres > Rôles d'utilisateur et droits d'accès**.
   La page **Rôles utilisateur et droits d'accès** s'affiche.
2. Dans le panneau de gauche, développez **Unica Journey > partition1**.
   La page **partition1** s'affiche.
3. Sélectionnez **Affecter des droits d'accès**.
   La page **(Propriétés des rôles d'administration)** apparaît.

4. Cliquez sur **Droits d'enregistrement et d'édition**.
   La page **(Droits pour la partition1)** s'affiche.

5. Développez **Application**.

6. Définissez les valeurs des zones suivantes :

Opérations	JourneyParamètre par défaut de l'administrateur	JourneyParamètre par défaut de l'utilisateur
Créer une définition de données	Oui	Non
Editer la définition de données	Oui	Non
Supprimer une définition de données	Oui	Non
Créer des sources d'entrée	Oui	Non
Editer les sources d'entrée	Oui	Non
Supprimer les sources d'entrée	Oui	Non
Créer un Journey	Oui	Oui
Editer un Journey	Oui	Oui
Supprimer un Journey	Oui	Non
Publier un Journey	Oui	Oui
Terminer un Journey	Oui	Oui
Mettre en pause un Journey	Oui	Oui
Ajouter/modifier/supprimer un objectif	Oui	Non
Afficher l'objectif	Oui	Oui
Ajouter/modifier/supprimer des paramètres	Oui	Non
vue Paramètres	Oui	Oui

Note:

- Pour le rôle **JourneyAdmin**, nous vous recommandons de ne pas réduire les droits et de conserver les droits par défaut. Par défaut, **Journeyadmin** dispose de tous les droits d’accès.
- Pour le rôle **JourneyUser**, fournissez les droits que vous jugez appropriés. Vous pouvez attribuer tous les droits à **JourneyUser**, mais cela n’est pas recommandé.

7. Après avoir fourni les droits, cliquez sur **Enregistrer les modifications**.

Affectation d’un rôle JourneyAdmin à un utilisateur

Pour attribuer le rôle **JourneyAdmin** à un utilisateur, procédez comme suit :

1. Depuis la page d'accueil de Marketing Platform, sélectionnez **Paramètres > Rôles d'utilisateur et droits d'accès**.
   La page **Rôles utilisateur et droits d'accès** s'affiche.
2. Dans le panneau de gauche, développez **Unica Journey**.
3. Sélectionnez **partition1 > JourneyAdmin**.
   La page **JourneyAdmin** s’affiche.
4. Dans la section **Utilisateurs**, sélectionnez un utilisateur. Par exemple, `asm_admin`.
   La page des détails de l'utilisateur **asm_admin (asm_admin)** apparaît.
5. Sélectionnez **Editer les rôles**.
   La page **Editer les rôles** apparaît.
6. Dans la liste **Rôles disponibles**, sélectionnez **OfferAdmin (Unica Journey)**, puis cliquez sur le bouton **>>** pour déplacer le rôle dans la liste **Rôles sélectionnés**.
7. Cliquez sur **Enregistrer les modifications**.

Affectation d’un rôle JourneyUser à un utilisateur

Pour attribuer le rôle **JourneyUse** à un utilisateur, procédez comme suit :

1. Depuis la page d'accueil de Marketing Platform, sélectionnez **Paramètres > Rôles d'utilisateur et droits d'accès**.
   La page **Rôles utilisateur et droits d'accès** s'affiche.

2. Dans le panneau de gauche, développez **Unica Journey**.

3. Sélectionnez **partition1 > JourneyUser**.
   La page **JourneyUser** apparaît.

4. Dans la section **Utilisateurs**, sélectionnez un utilisateur. Par exemple, `journey_example`.
   La page des détails de l'utilisateur **journey_example (journey_example)** s'affiche.

5. Sélectionnez **Editer les rôles**.
   La page **Editer les rôles** apparaît.

6. Dans la liste **Rôles disponibles**, sélectionnez **JourneyUser (Unica Journey)**, puis cliquez sur le bouton **>>** pour déplacer le rôle dans la liste **Rôles sélectionnés**.

7. Cliquez sur **Enregistrer les modifications**.

Chapter 4. Journalisation des interactions Journey

La journalisation des interactions pour Journey est exécutée en tant que travail planifié. Les paramètres de planification sont définis dans le fichier `application.properties` de Journey Engine. Voici un exemple de paramètre :

```
engine.logging.cron=0 15 3 * * ?
```

Le travail planifié exporte les données dans un autre schéma qui est de nouveau défini dans les fichiers `application.properties` de Journey Engine.

```
journey.report.datasource.url =
journey.report.datasource.username =
journey.report.datasource.password =
journey.report.datasource.driver-class-name=
```

La journalisation des interactions capture le mouvement de tous les contacts qui entrent dans l'application Journey lors de leur déplacement dans chaque Journey, qu'ils soient publiés ou terminés. Même les parcours publiés, mais en pause sont pris en compte pour la journalisation des interactions.

Tous les points de contact, E-mail, SMS ou CRM sont pris en compte pour la journalisation des interactions lorsque les données d'audience sont envoyées à l'aide des intégrations configurées via les canaux respectifs. Les réponses reçues de chaque contact sont également capturées.

Log4j2

Journey Web et Journey Engine utilisent tous les deux la norme pour la journalisation. Le fichier `log4j2.xml`, pour Journey Web et Journey Engine, est placé dans le dossier `conf` à l'emplacement d'installation.

Journey Web et Journey Engine produisent tous les deux des journaux d'application standard ainsi que des journaux de performances. Pour Journey Web, l'emplacement par défaut des journaux se trouve dans le dossier `logs`. Pour Journey Engine, l'emplacement

par défaut des journaux se trouve dans le dossier `performancelogs`. Pour Journey Web et Journey Engine, les dossiers mentionnés sont placés dans l'emplacement d'installation.

Chapter 5. Journey GDPR

Accès à Journey GDPR

Vous pouvez accéder à l'outil GDPR (RGPD) à partir du dossier de l'application Journey. L'emplacement est le suivant :

```
<Journey_Home>\Journey\tools\GDPR\
```

Le RGPD prend en charge > les bases de données MariaDB, **MS Sql server** et **OneDb**, ainsi qu'**Oracle**

Exécution de Journey GDPR

Pour exécuter Journey GDPR, procédez comme suit :

1. Modifiez les propriétés suivantes dans le fichier `gdpr.properties` :

Nom de la propriété	Valeur exemple	Notes
`Journey.audience.DBType`	`ORACLE`	Actuellement, Journey prend uniquement en charge Oracle.
`Journey.audience.Db.Schema.Name`	`JourneyUtilisateur`	Nom de schéma utilisé dans la base de données Journey.
`Journey.audience.Field`	`email/mobileNumber`	Nom de la zone dans le fichier d'entrée `CSV`.
`Journey.audience.Csv`	`<GDPR_HOME>/sample/JourneyAudiences.csv`	Remplacez `<GDPR_HOME>` par le chemin du répertoire en cours. s'agit du fichier d'entrée CSV contenant les enregistrements que vous devez exclure de Journey.
`Journey.audience.Output`	`<GDPR_HOME>/JourneyAudiences.sql`	`JourneyAudiences.sql` est le nom du fichier de

Nom de la propriété	Valeur exemple	Notes
		sortie contenant toutes les requêtes SQL utilisées pour supprimer tous les enregistrements de l'application Journey. Remplacez `<GDPR_HOME>` par le chemin du répertoire en cours.
`Journey.audience.Output.FileSizeLimit`	`10`	La valeur est exprimée en Mo. Lorsque la taille du fichier dépasse la valeur entrée, il génère plusieurs fichiers avec les suffixes suivants : `JourneyAudiences _0`, `JourneyAudiences _1`, etc.

2. **Note:** Si vous constatez des erreurs, vous pouvez les tracer à l'aide de ce fichier journal.
3. Pour exécuter le fichier, procédez comme suit :
   a. Pour Windows, localisez et exécutez le fichier `gdpr_purge.bat`. Par exemple, si le fichier `gdpr_purge.bat` se trouve à l'emplacement `D:\workspace\HCL_GDPR\dist\journey\`, exécutez le fichier `gdpr_purge.bat`.
   b. Pour les systèmes basés sur UNIX, localisez et exécutez le fichier `gdpr_purge.sh`. Par exemple, si le fichier `gdpr_purge.sh` se trouve à l'emplacement `\workspace\HCL_GDPR\dist\journey\`, exécutez la commande ./gdpr_purge.sh.
4. Après l'exécution de `gdpr_purge.bat` (pour Windows) ou `gdpr_purge.sh` (pour Linux), les fichiers de sortie *« JourneyAudiences 0 »,« JourneyAudiences _1 »,« JourneyAudiences _2 »* et ainsi de suite seront générés à l'emplacement

<GDPR_HOME> spécifié dans les étapes ci-dessus. Le nombre de fichiers générés dépendra de la taille de fichier spécifiée.

5. Le fichier *« JourneyAudiences_x »* aura des requêtes de suppression pour les enregistrements mentionnés dans JourneyAudiences.csv
6. Ces requêtes doivent être exécutées manuellement dans la base de données « Journey » si nécessaire pour que les enregistrements soient supprimés de la table journeyaudiences.

L'utilitaire RGPD supprime les enregistrements du tableau suivant : JourneyAudiences, AudienceResponse, AudienceResponseMetaData, AudienceResponseInteraction, JourneyAudienceMilestone et JourneyAudienceGoal. Toutefois, il ne supprime pas les données des tables respectives, où les sommes agrégées sont stockées. Par exemple, des tables telles que journeyFlow, journeyAudienceFlow, JourneyGoalContactTransaction, etc. Par conséquent, il y aura une non-concordance de nombres dans l'interface utilisateur.

Avec l'outil RGPD, l'utilisateur ne pourra pas supprimer les données client d'une rubrique de publication Kafka ni des fichiers disponibles sur le système de fichiers. L'utilisateur doit supprimer ces données manuellement selon ses besoins.

Avec l'outil RGPD, l'utilisateur ne pourra pas supprimer les données client exportées par le connecteur JDBC.

Chapter 6. Authentification Kafka à l'aide de SSL

Si vous utilisez l'instance Kafka de votre organisation, vous pouvez utiliser des certificats configurés pour cette instance Kafka. Vous n'êtes pas obligé de générer des certificats et des clés SSL ni d'obtenir les certificats client à configurer dans les propriétés de l'application Journey.

Si vous ne disposez pas des certificats, vous pouvez générer une autorité de certification autosignée (CA), qui est simplement une paire de clés publique-privée et un certificat.

Vous devez ajouter le même certificat de CA au fichier de clés certifiées de chaque client et courtier Kafka.

Générer une clé et un certificat SSL pour chaque courtier Kafka

Pour générer des certificats autosignés pour le serveur Kafka, procédez comme suit.

Eléments prérequis

- Vous devez disposer de Java keytool et d'OpenSSL pour générer des certificats et le fichier de clés certifiées.
- Si vous le souhaitez, vous pouvez utiliser n'importe quel utilitaire de génération de certificat SSL au lieu d'OpenSSL.

1. Pour déployer SSL, générez la clé et le certificat pour chaque machine du cluster. Générez la clé initialement dans un fichier de clés temporaire afin de pouvoir l'exporter et le signer ultérieurement à l'aide de l'autorité de certification.

   ```
   keytool -keystore kafka.server.keystore.jks -alias localhost -validity 365
   -genkey
   ```

   - keystore : Fichier de clés qui stocke le certificat. Le fichier de clés contient la clé privée du certificat ; par conséquent, il doit être conservé en toute sécurité.
   - validity: Heure valide du certificat en jours.
2. Créer votre propre autorité de certification (CA).

   ```
   openssl req -new -x509 -keyout ca-key -out ca-cert -days 365
   ```

L'autorité de certification générée est simplement une paire de clés publique-privée et un certificat, et elle est destinée à signer d'autres certificats.

3. Ajoutez l'autorité de certification générée au fichier de clés sécurisées des clients afin que les clients puissent faire confiance à cette autorité de certification.
   - `keytool -keystore kafka.server.truststore.jks -alias CARoot -import -file ca-cert`
   - `keytool -keystore kafka.client.truststore.jks -alias CARoot -import -file ca-cert`
4. Signez tous les certificats dans le fichier de clés avec l'autorité de certification générée.
   a. Exportez le certificat depuis le fichier de clés :

      ```
      keytool -keystore kafka.server.keystore.jks -alias localhost -certreq -file cert-file
      ```
5. Signez-le auprès de l'autorité de certification.

   ```
   openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -days 365 -CAcreateserial -passin pass:<password>
   ```
6. Importez les certificats de l'autorité de certification et le certificat signé dans le fichier de clés.

   ```
   keytool -keystore kafka.server.keystore.jks -alias CARoot -import -file ca-cert
   ```

   ```
   keytool -keystore kafka.server.keystore.jks -alias localhost -import -file cert-signed
   ```
7. Créez le fichier de clés du client et importez les deux certificats de l'autorité de certification et les certificats signés dans le fichier de clés du client. Ces certificats client seront utilisés dans les propriétés de l'application.

   ```
   keytool -keystore kafka.client.keystore.jks -alias localhost -validity 365 -genkey
   ```

   ```
   keytool -keystore kafka.client.keystore.jks -alias localhost -certreq -file cert-file
   ```

   ```
   openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -days 365 -CAcreateserial -passin pass:<password>
   ```

```
keytool -keystore kafka.client.keystore.jks -alias CARoot -import -file
ca-cert
```

```
keytool -keystore kafka.client.keystore.jks -alias localhost -import -file
cert-signed
```

Configuration des composants du serveur Kafka, de Journey et de Link avec SSL

Les certificats de serveur à utiliser pour le serveur Kafka et les certificats client doivent être utilisés par toute application qui se connecte au serveur Kafka, notamment Journey Web, Journey Engine, Unica Link – Kafka-Link ou tout autre outil dont vous avez besoin pour vous connecter à ce serveur Kafka.

Pour configurer les composants du serveur Kafka, de Journey et de Link avec l'authentification SSL, exécutez les procédures fournies dans les sections suivantes.

Configuration du serveur Kafka avec l'authentification SSL

Vous devez utiliser les certificats de serveur suivants pour le serveur Kafka uniquement. Partagez ces certificats sur les machines requises et prenez note du mot de passe.

- `kafka.server.keystore.jks`
- `Kafka.server.truststore.jks`

Mettez à jour le fichier server.properties suivant dans le répertoire de configuration du serveur Kafka.

```
listeners=SSL://<KAFKA_HOST>:<KAFKA_PORT>
ssl.keystore.location=/PATH/kafka.server.keystore.jks
ssl.keystore.password= password
ssl.key.password= password
ssl.truststore.location= /PATH/kafka.server.truststore.jks
ssl.truststore.password= password
ssl.endpoint.identification.algorithm=
```

```
ssl.client.auth=required
security.inter.broker.protocol=SSL
```

Configurer Journey Engine avec Kafka SSL

Utilisez les certificats client suivants et partagez ces certificats sur les machines requises et prenez note du mot de passe.

- `Kafka.client.keystore.jks`
- `kafka.client.truststore.jks`

1. Mettez à jour le fichier `log4j2.xml` JourneyEngine à partir du répertoire `<JOURNEY_HOME>/Engine/conf/`. Supprimer les commentaires des lignes suivantes dans `log4j2.xml`.

   ```
   <Property name="security.protocol" >${sys:security.protocol}</
   Property>
   <Property name="ssl.truststore.location">
   ${sys:ssl.truststore.location}</Property>
   <Property name="ssl.truststore.password">
   ${sys:ssl.truststore.password}</Property>
   <Property name="ssl.keystore.location">${sys:ssl.keystore.location}</
   Property>
   <Property name="ssl.keystore.password">${sys:ssl.keystore.password}</
   Property>
   <Property name="ssl.key.password">${sys:ssl.key.password}</Property>
   <Property name="ssl.endpoint.identification.algorithm">
   ${sys:ssl.endpoint.identification.algorithm}</Property>
   ```

2. Mettez à jour l'élément `journey_engine_master.config` depuis le répertoire `<JOURNEY_HOME>/Engine/`.
3. Mettez à jour les valeurs de propriété suivantes.

   ```
   kafka.security.enabled=Y
   ```

```
kafka.security.protocols.enabled=SSL
security.protocol=SSL
ssl.truststore.location= /PATH/kafka.client.truststore.jks
ssl.truststore.password=<ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION
TOOL>
ssl.keystore.location= /PATH/kafka.client.keystore.jks
ssl.keystore.password=<ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION TOOL>
ssl.key.password=<ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION TOOL>
ssl.endpoint.identification.algorithm=
```

Configuration de Journey Web avec Kafka SSL

1. Mettez à jour le fichier `application.properties` Journey Web à partir du répertoire `<JOURNEY_HOME>/Web/properties/`.
2. Mettez à jour les valeurs de propriété suivantes.

```
kafka.security.enabled=Y
kafka.security.protocols.enabled=SSL
ssl.truststore.location= /PATH/kafka.client.truststore.jks
ssl.truststore.password= <ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION
TOOL>
ssl.keystore.location= /PATH/kafka.client.keystore.jks
ssl.keystore.password= <ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION
TOOL>
ssl.key.password= <ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION TOOL>
ssl.endpoint.identification.algorithm=
```

Configuration du composant Unica Link avec SSL

Mettez à jour les valeurs de propriété suivantes dans le fichier `kafkalink.properties` des installations Unica Link.

```
security.ssl=true
security.protocol=SSL
```

```
ssl.truststore.location= /PATH/kafka.client.truststore.jks
ssl.truststore.password=password
security.authentication=username
ssl.keystore.location= /PATH/kafka.client.keystore.jks
ssl.keystore.password=password
ssl.key.password=passwordssl.endpoint.identification.algorithm=
```

Configuration des composants du serveur Kafka, de Journey et de Link avec SASL

Pour configurer les composants du serveur Kafka, de Journey et de Link avec l'authentification SASL, exécutez les procédures fournies dans les sections suivantes.

Configuration du serveur Kafka avec l'authentification SASL

1. Spécifiez le paramètre JVM dans `kafka-run-class.bat/sh`.

   set `JAVA_OPTS=%JAVA_OPTS%`

   `-Djava.security.auth.login.config=/PATH/kafka_server_jaas.conf`

   `set COMMAND=%JAVA% %JAVA_OPTS% %KAFKA_HEAP_OPTS%`

   `%KAFKA_JVM_PERFORMANCE_OPTS% %KAFKA_JMX_OPTS% %KAFKA_LOG4J_OPTS% -cp`

   `"%CLASSPATH%" %KAFKA_OPTS% %*`

   Exemple de fichier `jaas.config` :

   ```
   KafkaServer {
      org.apache.kafka.common.security.plain.PlainLoginModule required
      username="admin"
      password="admin-secret"
      user_admin="admin-secret"
      user_alice="alice-secret";
   };
   ```

```
KafkaClient {
  org.apache.kafka.common.security.plain.PlainLoginModule required
  username="alice"
  password="alice-secret";
};
```

2. Mettez à jour le fichier de propriétés du serveur Kafka suivant à partir de `KAFKA_SERVER/config/server.properties`.

```
listeners=SASL_PLAINTEXT:// <KAFKA_HOST>:<KAFKA_PORT>
security.inter.broker.protocol=SASL_PLAINTEXT
sasl.mechanism.inter.broker.protocol=PLAIN
sasl.enabled.mechanisms=PLAIN
```

Configurer Journey Engine avec Kafka SASL

1. Mettez à jour le fichier `log4j2.xml` JourneyEngine à partir du répertoire `<JOURNEY_HOME>/Engine/conf/`. Supprimer les commentaires des lignes suivantes dans `log4j2.xml`.

```
#<!-- Kafka SASL configuration -->
<Property name="security.protocol">${sys:security.protocol}</Property>
<Property name="sasl.mechanism">${sys:sasl.mechanism}</Property>
```

2. Mettez à jour l'élément `journey_engine_master.config` depuis le répertoire `<JOURNEY_HOME>/Engine/`. Mettez à jour les valeurs de propriété suivantes.

```
kafka.security.enabled=Y
kafka.security.protocols.enabled=SASL_PLAINTEXT#
security.protocol=SASL_PLAINTEXT
sasl.mechanism=PLAIN
java.security.auth.login.config=./kafka_client_jaas.conf
```

Configuration de Journey Web avec Kafka SASL

Mettez à jour le fichier `application.properties` Journey Web à partir du répertoire `<JOURNEY_HOME>/Web/properties/`.

```
kafka.security.enabled=Y
kafka.security.protocols.enabled=SASL_PLAINTEXT
#java.security.auth.login.config=/PATH/kafka_client_jaas.conf
```

Configuration du composant Unica Link avec Kafka SASL

Mettez à jour les valeurs de propriété suivantes dans le fichier `kafkalink.properties` des installations Unica Link.

```
security.sasl =true
security.protocol=SASL_PLAINTEXT
security.sasl.auth.login.config =/PATH/kafka_client_jaas.conf
sasl.mechanism=PLAIN
```

Configuration de composants du serveur Kafka et de Journey avec la configuration SASL_SSL

Pour configurer les composants du serveur Kafka ainsi que d'autres composants Journey avec l'authentification SASL, suivez les procédures décrites dans les sections suivantes.

Note: Unica Link ne prend pas en charge la connexion à Kafka-Link à l'aide du mécanisme d'authentification SASL_SSL. Vous devez utiliser un mécanisme d'authentification SASL ou SSL.

Configuration du serveur Kafka avec Kafka SASL_SSL

Mettez à jour le fichier server.properties comme suit dans le répertoire de configuration du serveur Kafka.

```
listeners=SASL_SSL:// <KAFKA_HOST>:<KAFKA_PORT>
```

```
security.inter.broker.protocol=SASL_PLAINTEXT
sasl.mechanism.inter.broker.protocol=PLAIN
sasl.enabled.mechanisms=PLAIN
ssl.keystore.location=/PATH/kafka.server.keystore.jks
ssl.keystore.password=password
ssl.key.password= password
ssl.truststore.location=/PATH/kafka.server.truststore.jks
ssl.truststore.password= password
ssl.endpoint.identification.algorithm=
ssl.client.auth=required
security.inter.broker.protocol=SSL
```

Configuration de Journey Engine avec Kafka SASL_SSL

1. Mettez à jour le fichier `log4j2.xml` JourneyEngine à partir du répertoire `<JOURNEY_HOME>/Engine/conf/`.

   Supprimer les commentaires des lignes suivantes dans `log4j2.xml`.

   ```
   <Property name="sasl.mechanism">${sys:sasl.mechanism}</Property>
   <Property name="security.protocol" >${sys:security.protocol}</
   Property>
   <Property name="ssl.truststore.location" >
   ${sys:ssl.truststore.location}</Property>
   <Property name="ssl.truststore.password">
   ${sys:ssl.truststore.password}</Property>
   <Property name="ssl.keystore.location">${sys:ssl.keystore.location}</
   Property>
   <Property name="ssl.keystore.password">${sys:ssl.keystore.password}</
   Property>
   <Property name="ssl.key.password">${sys:ssl.key.password}</Property>
   <Property name="ssl.endpoint.identification.algorithm">
   ${sys:ssl.endpoint.identification.algorithm}</Property>
   ```

2. Mettez à jour l'élément `journey_engine_master.config` depuis le répertoire `<JOURNEY_HOME>/Engine/`.

   Mettez à jour les valeurs de propriété suivantes.

```
kafka.security.enabled=Y
kafka.security.protocols.enabled=SASL_SSL
ssl.truststore.location=/PATH/kafka.client.truststore.jks
ssl.truststore.password=<ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION
 TOOL>
ssl.keystore.location=/PATH/kafka.client.keystore.jks
ssl.keystore.password=<ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION TOOL>
ssl.key.password=<ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION TOOL>
ssl.endpoint.identification.algorithm=
java.security.auth.login.config=/PATH/kafka_client_jaas.conf
```

Configuration de Journey Web avec Kafka SASL_SSL

Mettez à jour le fichier `application.properties` Journey Web à partir du répertoire `<JOURNEY_HOME>/Web/properties/`.

```
kafka.security.enabled=Y
kafka.security.protocols.enabled=SASL_SSL
ssl.truststore.location=/PATH/kafka.client.truststore.jks
ssl.truststore.password=<ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION TOOL>
ssl.keystore.location=/PATH/kafka.client.keystore.jks
ssl.keystore.password=<ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION TOOL>
ssl.key.password=<ENCYPTED PASSWORD WITH JOURNEY ENCRYPTION TOOL>
ssl.endpoint.identification.algorithm=
java.security.auth.login.config=/PATH/kafka_client_jaas.conf
```

Chapter 7. Configuration des serveurs d'applications Web TomCat pour le protocole SSL

Pour tous les serveurs d'applications sur lesquels une application Unica est déployée, vous devez configurer le serveur d'applications Web pour qu'il utilise les certificats que vous avez décidé d'employer.

Pour plus d'informations sur l'exécution de ces procédures, consultez la documentation du serveur d'applications Web.

Mise en oeuvre de la sécurité des cookies

Certains cookies peuvent ne pas être sécurisés correctement dans le navigateur client. Ne pas sécuriser les cookies rend l'application vulnérable à l'interposition (man in the middle) et aux attaques de piratage de session. Pour résoudre ce problème, prenez les précautions suivantes.

- Appliquez l'utilisation de SSL en permanence afin de réduire le risque d'interception des cookies sur la connexion.
- Dans le serveur d'applications Web, définissez les indicateurs `secure` et `httponly` sur tous les cookies.
    - L'indicateur `secure` indique au navigateur d'envoyer le cookie uniquement une connexion HTTPS. Vous devez activer SSL sur toutes les applications qui communiquent entre elles si vous définissez cet indicateur.
    - L'indicateur `httponly` empêche l'accès des cookies via un script côté client.

Configuration des indicateurs SSL dans Tomcat

Pour configurer les indicateurs `secure` et `httponly` dans Tomcat, procédez aux modifications suivantes sur le serveur `.xml` de Tomcat.

```
<Connector port="7003"
 protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true" scheme="https" acceptCount="100"
 clientAuth="false"
disableUploadTimeout="true" enableLookups="false" secure="true"
 sslProtocol="TLS" keystoreFile="/opt/v12.1/v12.1.0.1.1/Campaign/SSL_NEW/
PlatformClientIdentity.jks" keystorePass="password" >     </Connector>
```

Configurer Unica Journey avec SSL

Pour configurer Unica Journey afin qu'il utilise le protocole SSL, vous devez définir certaines propriétés de configuration. Suivez les procédures décrites dans cette section, relatives à l'installation de Unica Journey et aux communications que vous souhaitez sécuriser au moyen du protocole SSL.

Si vous accédez à l'installation de Unica via une connexion sécurisée, et si vous définissez des propriétés de navigation telles que décrites dans les procédures suivantes, vous devrez utiliser `https` et le numéro de port sécurisé dans l'URL. Le port SSL par défaut est`8443` pour Tomcat.

Cette procédure permet de configurer Journey avec SSL

1. Connectez-vous à Unica, puis cliquez sur **Paramètres > Configuration**.
2. Définissez la valeur de la propriété `Affinium | Journey | navigation` sur l'URL de Unica Journey.

   Par exemple : `https://`*`host.domain:SSL_port`*`/unica`

   où :

   - *`host`* est le nom ou l'adresse IP de la machine sur laquelle Unica Journey est installé.
   - *`domain`* désigne le domaine de la société dans lequel les produits Unica sont installés.

- *SSL_Port* désigne le port SSL dans le serveur d'applications sur lequel Unica Journey est déployé.

Notez que l'URL commence par `https`.

Chapter 8. Paramètres

Utilisez le menu Paramètres pour gérer les intégrations Journey, telles que les connecteurs de messagerie, les connecteurs SMS, les connexions CRM et les intégrations REST.

Définition d’une connexion de messagerie par défaut

Si vous disposez de plusieurs connecteurs à Unica Link pour envoyer un e-mail, vous pouvez choisir la connexion par défaut dans le menu **Paramètres**.

Pour définir une connexion de messagerie par défaut, procédez comme suit :

1. Sélectionnez  **> Link > E-mail** .
   La page **E-mail** s'affiche.
2. Dans la liste **Connexions disponibles**, sélectionnez une connexion.
   La connexion disponible inclut Mandrill, MailChimp, etc.
3. Cliquez sur **Sauvegarder**.
   Vous pouvez également désélectionner une connexion existante et cliquer sur **Enregistrer**. Cela permet de s’assurer qu’aucune connexion par défaut n’est définie.

Définition d’une connexion SMS par défaut

Si vous disposez de plusieurs connecteurs à Unica Link pour envoyer un SMS, vous pouvez choisir la connexion SMS par défaut dans le menu **Paramètres**.

Pour définir une connexion SMS par défaut, procédez comme suit :

1. Sélectionnez  **> Link > SMS** .
   The **SMS** page appears.
2. Dans la liste **Connexions disponibles**, sélectionnez une connexion.

Note:

Les formats de numéro de téléphone doivent être mentionnés conformément à la spécification du canal de distribution. Journey enverra le numéro de téléphone au même format au canal de distribution. Par exemple, le format de numéro de téléphone dans une connexion Twilio prise en charge avec Journey est le suivant :

- *<plus sign><country-code><10-digit phone number>* - `+15403241212`.
- *<plus sign> <country-code <(area-code)> <three-digit number><four-digit number>* - `+1 (540) 324 1212`.
- *<plus sign>-<country-code>-<area-code>-<three-digit number>-<four-digit number>* - `+1-540-324-1212`.
- *<plus sign> <country-code>-<area-code>-<three-digit number>-<four-digit number>* - `+1 540-324-1212`.

Quel que soit le format de numéro de téléphone que vous fournissez, Unica Journey enregistre le numéro au format suivant : <plus sign><country-code><10-digit phone number>. Par exemple, si vous indiquez un numéro de téléphone en tant que `+ 1 540-324-1212`, Unica Journey stocke le numéro de téléphone en tant que `+15403241212`.

Si vous sélectionnez Twilio comme connexion SMS par défaut, les numéros de téléphone seront acceptés uniquement au format suivant : *<plus sign><country-code><10-digit phone number>*. Par exemple, `+15403241212`.

3. Cliquez sur **Sauvegarder**.

Définition d'une connexion CRM par défaut

Si vous disposez de plusieurs connexions CRM, vous pouvez spécifier la connexion CRM par défaut dans le menu **Paramètres**.

Pour définir une connexion CRM par défaut, procédez comme suit :

1. Sélectionnez  **> Link > CRM** .

La page **CRM** s'affiche.

2. Dans la liste **Connexions disponibles**, sélectionnez une connexion.

3. Cliquez sur **Sauvegarder**.

Gérer les connexions

Vous pouvez gérer les connections Unica Link à partir de ce menu.

Vous pouvez créer une connexion avec des connecteurs Unica Link tels que MailChimp, Mandrill, Salesforce et Twilio. Vous pouvez afficher toutes les connexions existantes dans le panneau **Connexions existantes** (n), où n correspond au nombre de connexions.

1. Pour créer une connexion MailChimp, procédez comme suit :

   a. Sélectionnez  **> Link > Gérer les connexions > Créer**.
   La page **Créer une connexion** s'affiche.

   b. Indiquez des valeurs pour les zones suivantes :
      - **Nom** - Obligatoire
      - **Description** - Facultatif

   c. Cliquez sur **Suivant**.

   d. Dans le panneau **Choisir une connexion**, sélectionnez **MailChimp**.

   e. Dans la section **Propriétés de connexion**, fournissez des valeurs pour les zones obligatoires suivantes :

   Note: Pour connaître les zones et les valeurs à insérer, voir *Unica Link - Connecteur MailChimp - Guide d'utilisation*.

      - **Adresse URL de base**
      - **ID utilisateur**
      - **Clé d'API**

- **Fréquence d’extraction d'activité**
- **Unités d’extraction d’activité**

f. Cliquez sur **Tester** pour tester la connexion. Si les valeurs fournies sont correctes, un message de réussite s’affiche. Si les valeurs fournies sont incorrectes, un message d’erreur s’affiche.

g. Pour enregistrer la connexion, cliquez sur **Enregistrer**.
La nouvelle connexion est correctement enregistrée et apparaît dans le panneau **Connexions existantes**.

2. Pour créer une connexion Mandrill, procédez comme suit :

a. Sélectionnez  **> Link > Gérer les connexions > Créer**.
La page **Créer une connexion** s'affiche.

b. Indiquez des valeurs pour les zones suivantes :
- **Nom** - Obligatoire
- **Description** - Facultatif

c. Cliquez sur **Suivant**.

d. Dans le panneau **Choisir une connexion**, sélectionnez **Mandrill**.

e. Dans la section **Propriétés de connexion**, fournissez des valeurs pour les zones obligatoires suivantes :

Note: Pour connaître les zones et les valeurs à insérer, voir *Unica Link Mandrill - Guide d'utilisation*.

- **Clé d'API**
- **Fréquence d’extraction d'activité**
- **Unités d’extraction d’activité**

f. Cliquez sur **Tester** pour tester la connexion. Si les valeurs fournies sont correctes, un message de réussite s’affiche. Si les valeurs fournies sont incorrectes, un message d’erreur s’affiche.

g. Pour enregistrer la connexion, cliquez sur **Enregistrer**.
La nouvelle connexion est correctement enregistrée et apparaît dans le panneau **Connexions existantes**.

3. Pour créer une connexion Salesforce, procédez comme suit :

a. Sélectionnez  **> Link > Gérer les connexions > Créer**.
La page **Créer une connexion** s'affiche.

b. Indiquez des valeurs pour les zones suivantes :
- **Nom** - Obligatoire
- **Description** - Facultatif

c. Cliquez sur **Suivant**.

d. Dans le panneau **Choisir une connexion**, sélectionnez **Salesforce**.

e. Dans la section **Propriétés de connexion**, fournissez des valeurs pour les zones obligatoires suivantes :

Note: Pour connaître les zones et les valeurs à insérer, voir *Unica LinkSalesforce - Guide d'utilisation*.

- **URL d'instance**
- **Jeton d'accès**
- **Version**

f. Cliquez sur **Tester** pour tester la connexion. Si les valeurs fournies sont correctes, un message de réussite s'affiche. Si les valeurs fournies sont incorrectes, un message d'erreur s'affiche.

g. Pour enregistrer la connexion, cliquez sur **Enregistrer**.
La nouvelle connexion est correctement enregistrée et apparaît dans le panneau **Connexions existantes**.

4. Pour créer une connexion Twilio, procédez comme suit :

a. Sélectionnez  **> Link > Gérer les connexions > Créer**.
La page **Créer une connexion** s'affiche.

b. Indiquez des valeurs pour les zones suivantes :
   - **Nom** - Obligatoire
   - **Description** - Facultatif

c. Cliquez sur **Suivant**.

d. Dans le panneau **Choisir une connexion**, sélectionnez **Twilio**.

e. Dans la section **Propriétés de connexion**, fournissez des valeurs pour les zones obligatoires suivantes :

   Note: Pour connaître les zones et les valeurs à insérer, voir *Unica Link Twilio - Guide d'utilisation*.

   - **Adresse URL de base**
   - **SID de compte**
   - **Jeton d'authentification**
   - **Numéro de début**
   - **Intervalle entre les nouvelles tentatives**
   - **Tentatives de relance**

f. Cliquez sur **Tester** pour tester la connexion. Si les valeurs fournies sont correctes, un message de réussite s’affiche. Si les valeurs fournies sont incorrectes, un message d’erreur s’affiche.

g. Pour enregistrer la connexion, cliquez sur **Enregistrer**.
La nouvelle connexion est correctement enregistrée et apparaît dans le panneau **Connexions existantes**.

Intégration REST

Les clés REST sont utilisées pour la connexion tierce à l'application. Vous pouvez générer une paire clé-valeur et à l'aide de la paire clé-valeur, vous pouvez vous connecter à Journey à l'aide d'applications tierces.

Création d'une nouvelle intégration REST

Pour créer une paire de clés pour l'intégration REST, procédez comme suit :

1. Sélectionnez  **> REST** .
   La page **REST** s'affiche.
2. Cliquez sur **+ Intégration REST**.
   La page **Nouvelle intégration REST** s'affiche.
3. Indiquez des valeurs pour les zones suivantes :
   - **Nom de l'application** - Obligatoire
   - **Description** - Facultatif.
4. Cliquez sur **Générer des clés**.
   Le système génère **ClientID** et **ClientSecret**.
5. Utilisez la barre de basculement pour modifier le **Statut** en `Actif` ou `Inactif`. Par défaut, le **Statut** est `Actif`.
6. Pour sauvegarder l'intégration REST, cliquez sur **Enregistrer**.
   Pour envoyer des données d'audience à Journey, suivez les informations mentionnées dans la source d'entrée REST utilisée pour configurer le nœud final REST. Utilisez les **ClientID** et **ClientSecret**, que vous avez reçus lors de l'exécution de l'étape (4), pour configurer le nœud final REST sur la source d'entrée.

Affichage de la liste des intégrations REST

Unica Journey gère la liste des intégrations REST créées.

Pour afficher une liste des intégrations REST, procédez comme suit :

1. Sélectionnez  **> REST** .
   La page **REST** s'affiche.
2. Effectuez l'une des opérations suivantes :
   a. Pour afficher la liste des intégrations REST dans l'ordre croissant ou décroissant de la zone Nom, cliquez sur **Nom**.
   b. Pour afficher la liste des intégrations REST dans l'ordre croissant ou décroissant de la zone Description, cliquez sur **Description**.

Modification d'une intégration REST existante

Vous pouvez uniquement modifier la description et le statut d'une intégration REST existante.

Pour modifier une intégration REST existante, procédez comme suit :

1. Sélectionnez  **> REST** .
   La page **REST** s'affiche.
2. Pour modifier une intégration REST, vous pouvez soit :
   • Sélectionner l'intégration REST requise dans la liste.
   • sélectionner 
   La page **Mettre à jour l'intégration REST** s'affiche.
3. Vous ne pouvez mettre à jour que les zones suivantes :
   • **Description**
   • **Statut**
4. Pour sauvegarder les changements ou les modifications, cliquez sur **Enregistrer**.

Suppression d'intégrations REST

Vous ne pouvez supprimer que les intégrations REST inactives qui ne sont plus utilisées ni nécessaires.

Pour modifier le statut d'une entrée d'intégration REST, voir Modification d'une intégration REST existante (on page 40).

Pour supprimer les intégrations REST inactives existantes, procédez comme suit :

1. Sélectionnez  **> REST** .
   La page **REST** s'affiche.
2. Exécutez l'une des étapes ci-après :
   - Pour supprimer une intégration REST, sélectionnez **>**  suivant l'intégration REST dans la liste.
   - Pour supprimer plusieurs intégrations REST, dans la liste, cochez les cases situées en regard des intégrations REST que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Ok** pour procéder à la suppression.