Unica Journey V12.1.1
Administratorhandbuch

Contents

Chapter 1. Eine Einführung in Unica Journey

Unica Journey ist eine zielbasierte Steuerungslösung zum Basteln, Ausführen und Visualisieren kontextorientierter, personalisierter und mehrstufiger Kundenerlebnisse.

Marketiers können Unica Journey verwenden, um:

- Ziele für Kundenerfahrung zu definieren
- Journeys in Echtzeit problemlos anpassen, um sie zu schaffen
- Gesamte Kunden-Journeys über Kanal/Touchpoints und Ereignisse hinweg mit einer schlanken und intuitiven Journey-Leinwand abzugleichen und zu visualisieren

Kunden-Journeys sind vollständig automatisiert und werden mit jedem Schritt des Markeneinsatzes Ihres Kunden synchronisiert. Verwenden Sie die Echtzeiteinsichten in Journey, um das Kundenverhalten mit Einsichten zu verstehen, die Dinge so widerspiegeln, wie sie in Journey passieren .

Funktionen von Unica Journey

Die Funktionen von Unica Journey lauten wie folgt:

- **Zielgesteuerte Erfahrungen**: Definieren Sie Ziele für Ihre Kundenerfahrung und passen Sie Ihre Journeys in Echtzeit an, um sie zu erreichen.
- **Orchestrierungsleinwand**: Erstellen und visualisieren Sie Ihre gesamte Kunden-Journey über Kanäle/Touchpoints und Ereignisse mit einer schlanken und intuitiven Journey Leinwand.
- **Stets aktives Engagement**: Komplett automatisierte Ausführung, die mit jedem Schritt des Markeneinsatzes Ihres Kunden synchronisiert wird.
- **Echtzeitansichten**: Verstehen Sie Ihr Kundenverhalten mit Einsichten, die Dinge so widerspiegeln, wie auf in ihren Journeys passieren.

- **Auswahl der Touchpoints**: Verarbeiten Sie direkt die nativen Touchpoints für digitale Kanäle oder erstellen Sie einen angepassten TouchPoint und orchestrieren Sie nahtlos die Journey in Ihrem Ökosystem.
- **Dynamisches Datenframework**: Flexible Datendefinition und Eintragsquellen zum Erweitern der Kunden-Journey mit kontextbezogenen Daten und Ereignissen aus mehreren Touchpoints und in verschiedenen Formattypen (Datei, API usw.)

Vorteile von Unica Journey

Im Folgenden werden die Vorteile beschrieben:Unica Journey

- **Verstärkte Markenbindung**: Stärken Sie Ihre Marke folgendermaßen mit gezielten und automatisierten Journeys, die Kunden erfassen, pflegen, konvertieren und binden.
- **Verstärkeltes Omnikanal-Engagement**: Erzielen Sie ein konsistentes Kundenerlebnis über Kanäle hinweg, in denen die native Integration für abgehende (Unica Campaign) und eingehende Engagements (Unica Interact , Unica Discover und Unica Deliver) verwendet wird.
- **Verkürzen Sie Ihren Kundenkonvertierungszyklus**: Seien Sie einen Schritt voraus und bringen Sie Ihren Kunden zu seinen Zielen mit rechtzeitigen nächstbesten Aktionen.
- **Reagieren Sie auf den Moment**: Sie werden keine Möglichkeit verpassen, zu erfahren, wo sich Ihr Kunde auf seiner Reise befindet, und ihn mit der entsprechenden Erfahrung begeistern.
- **Verringern Sie Ihre Marketing-TCO**: Reduzieren Sie Ihre Marketing-TCO mit automatisierten Strömen und Plug-und-Play-Integration in ihr MarTech-Ökosystem über ein offenes und flexibles Framework, das von Unica Link angetrieben wird.

Chapter 2. Unica Journey Integrationen

Unica Journey Ausführungssysteme für E-Mail

Unica Journey unterstützt Unica Deliver und Unica Link für den E-Mail Versand. Sie können beide zur Integration mit Journey verwenden.

Unica Journey Integration mit Unica Link

Unica Link bietet die Funktionen zur Versendung von Mitteilungen über die Kanäle E-Mail, SMS, CRM, ADTECH und JDBC. Unica Link bietet die folgenden Referenz-Connectors, um die Mitteilungen an die Kanäle E-Mail, SMS, CRM, ADTECH und JDBC zu senden.

Installieren Sie die folgenden Referenz-Connectors nach Belieben:

- **MailChimp** – für E-Mail
- **Mandrill** – für E-Mail
- **Twilio** – für SMS
- **Salesforce** – für CRM

Die Integration mit Unica Link erlaubt die Integration von Journey mit Drittanbietern nur für die Ausführungen von E-Mail, SMS, CRM, ADTECH und JDBC.

Table 1. Installation und Konfiguration von Unica Link

Aufgabe	**Dokumentation**
Installation und Konfiguration von Unica Link	Siehe *Unica LinkV12.1 Installationshandbuch*.
Installation von Unica Link Connector Anwendung für Journey	Siehe *Unica LinkV12.1 Installationshandbuch*.
Installation von Unica Link Connector – MailChimp	Siehe *Unica Link Mailchimp Connector-Benutzerhandbuch*.
Installation von Unica Link Connector – Mandrill	Siehe *Unica Link Mandrill Connector-Benutzerhandbuch*.

Table 1. Installation und Konfiguration von Unica Link (continued)

Aufgabe	Dokumentation
Installation von Unica Link Connector – Twilio	Siehe *Unica Link Twilio Connector-Benutzerhandbuch*.
Installation von Unica Link Connector – Salesforce	Siehe *Unica Link Salesforce Connector-Benutzerhandbuch*.

Note: Weder das Konto noch der Zugriff auf die Anbieter von Lieferkanälen werden von HCL bereitgestellt. Abhängig von Ihren Anforderungen können Sie die Berechtigungen oder Konten von diesen Anbietern erhalten.

Unica Journey Integration mit Unica Deliver

Unica Journey nutzt die Funktionen von Unica Deliver zu dem Versand von E-Mail Mitteilungen. Damit können die E-Mail Antworten in Echtzeit erfasst und die Journey Zielgruppe verarbeitet werden. Für weitere Informationen über die Aktivierung von Unica Deliver Integration mit Unica Journey, siehe Unica Journey Installationshandbuch.

Unica Journey Integration mit Unica Campaign und Unica Interact

Unica Journey wird nahtlos mit Unica Campaign und Unica Interact integriert. Die Zielgruppendaten über ein bestimmtes Kafka Thema werden von Unica Campaign und Unica Interact an Unica Journey gesendet. Die Zielgruppendaten werden über eine Kafka-Eingabequelle gesendet und über alle Journeys, die die Daten aus diesen Eingabequellen verbrauchen, übertragen.

Für weitere Informationen über die Integration von Unica Campaign und Unica Interact mit Unica Journey, siehe die in der folgenden Dokumentationsliste erwähnten Handbücher.

Die Daten aus mehreren Campaign Partitionen werden von Journey unterstützt.

Journey-Support-Daten aus mehreren Partitionen von Campaign.

1. Mehrfache Partitionen werden von Journey nicht unterstützt.
2. Nur die Daten aus mehrfachen Partitionen von Campaign/Interact/Deliver können von Journey verarbeitet werden. Dafür wird Journey auf einer einzelnen Partition ausgeführt.

Die Konfigurationsplattform, Benutzerrollen und -berechtigungen müssen geändert werden:

- Die Details von Campaign-Ablaufdiagrammen, die unter den Eingabequellen angezeigt werden, stammen aus mehreren Partitionen.
- Abhängig von der Partition werden die Vorlagen von Deliver in den Touchpoints E-Mail/SMS/WhatsApp angezeigt.

Table 2. Integration von Unica Campaign mit anderen HCL Produkten

Aufgabe	**Dokumentation**
Integration von Unica Campaign und Unica Journey	Siehe *Unica Campaign Administratorhandbuch* und *Unica CampaignBenutzerhandbuch*.
Integration von Unica Campaign und Unica Interact	Siehe *Unica Interact Administratorhandbuch*.

Unica Journey Integration mit Unica Discover

Unica Journey wird nahtlos mit Unica Discover integriert. Die Daten bezüglich der Schwierigkeiten von Zielgruppen werden von Unica Discover an Unica Journey gesendet. Die Zielgruppendaten werden über eine REST-Eingabequelle gesendet und über alle Journeys, die die Daten aus diesen Eingabequellen verbrauchen, übertragen. Es werden vier Skripte bereitgestellt. Nach der Installation von Journey müssen die Skripte sofort ausgeführt werden. Dadurch werden zwei Eingabequellen und zwei Datendefinitionen erstellt namens Eingabequelle-Discover für CART und Eingabequelle-Discover für Form.

DD Name	Einkaufskorb

Beschreibung	Dieses Ereignis wird ausgelöst, wenn der Kunde einen Warenkorb oder eine Reihe von ausgewählten Angeboten aufgibt.

Table 3. Zu übertragende Attribute

Name	Typ	Länge	Anmerkung
Email*	TEXT	200	Es ist ein Pflichtfeld.
Name	TEXT	200	
DiscoverSessionId	TEXT	50	Discover Session Id zur Rückverbindung erforderlich.
CartId	TEXT	50	Eindeutige ID zur Identifizierung des Warenkorbs.
CartValue	NUMBER		
EventDateTime	TIMESTAMP		Datum und Uhrzeit des Ereignisses in UTC-Längengrad
EventType	TEXT		Der Ereignistyp kann CART_ABANDONED sein
CookieID	TEXT	1024	
TLT_BROWSER	TEXT	50	Browser-Details
TLT_MODEL	TEXT	50	Einheitendetails

Table 3. Zu übertragende Attribute (continued)

Name	Typ	Länge	Anmerkung
HTTP_ACCEPT_LAN-GUAGE	TEXT	50	Sprache

DD Name	Formular
Beschreibung	Dieses Ereignis wird veröffentlicht, wenn der Kunde ein beliebiges Webformular ausfüllt.

Table 4. Zu übertragende Attribute

Name	Typ	Länge	Anmerkung
Email*	TEXT	200	Es ist ein Pflicht-feld.
Name	TEXT	200	
DiscoverSessionId	TEXT	50	Discover Ses-sion Id zur Rück-verbindung er-forderlich.
FormId	TEXT	50	Eindeutige ID zur Identifizierung des Formulars
FormName	TEXT	100	
EventDateTime	TIMESTAMP		Datum und Uhrzeit des Ereignisses in UTC-Längengrad
CookieID	TEXT	1024	
TLT_BROWSER	TEXT	50	Browser-Details

Table 4. Zu übertragende Attribute (continued)

Name	Typ	Länge	Anmerkung
TLT_MODEL	TEXT	50	Einheitendetails
HTTP_ACCEPT_LAN-GUAGE	TEXT	50	Sprache
EventType	TEXT		Der Ereignistyp kann FORM_SUB-MITTED oder FOR-M_ABANDONED sein

Note: Ab Fixpack 3 wird die Integrationsfunktion von Unica Journey mit Unica Discover verfügbar.

Eine Einführung in Unica Deliver

Unica Deliver ist eine webbasierte, unternehmensweite Marketingnachrichtenlösung, mit der Sie ausgehende Massennachrichten und transaktionale Nachrichtenkampagnen durchführen können. Deliver integriert sich in Unica Campaign sowie mit sicherem Erstellen und Übertragen von Nachrichten und der Verfolgung von Ressourcen, die von Unicagehostet werden.

Sie können Deliver verwenden, um personalisierte E-Mail-Kommunikation zu erstellen, zu senden und zu verfolgen. Da Deliver mit Campaigninstalliert und arbeitet, können Sie Campaign-Ablaufdiagramme verwenden, um die Empfängerinformationen exakt auszuwählen und zu segmentieren, um jede beliebige Nachrichten anzupassen.

Ihre Zielgruppe auswählen

Verwenden Sie Campaign, um Nachrichtenempfänger und Daten zu jeder Person auszuwählen, die Sie für die Personalisierung der Nachrichten verwenden können.

Mit Deliverkönnen Sie eine große Anzahl von E-Mail-Empfängern schnell und persönlich erreichen. Sie können ein Mailing aber auch so einstellen, dass es automatisch eine einzige E-Mail-Nachricht als Antwort auf eine Transaktion verschickt.

Nachricht erstellen

Der Deliver-Dokumentersteller stellt Bearbeitungswerkzeuge bereit, mit denen Sie personalisierte Nachrichteninhalte entwerfen, voransehen und veröffentlichen können. Sie können Nachrichten mit Inhalten erstellen, die Sie in den Dokumentersteller hochladen oder sie mit externen Inhalten verbinden, wenn Deliver Nachrichten erstellt und übermittelt. Deliver bietet verschiedene Möglichkeiten, Nachrichten zu entwerfen, die Inhalte abhängig von personenbezogenen Daten für jeden Empfänger konditionell anzeigen.

Nachricht verschicken und Antworten verfolgen

Abhängig von ihren Zielen können Sie planen, dass eine Nachrichtenkampagne so bald wie möglich ausgeführt wird, oder planen, dass sie später ausgeführt wird. Deliver überwacht die Nachrichtenbereitstellung und verfolgt die Empfängerantworten. Das System gibt Kontakt- und Antwortdaten an die Systemtabellen von Deliver zurück, die als Teil des Campaign-Datenbank-Schemas installiert sind.

Wie Sie loslegen

Um loszulegen, müssen Sie Campaign installieren und über ein gehostetes Nachrichtenkonto verfügen.

Systemadministratoren müssen ein gehostetes Nachrichtenkonto anfordern und mit Unica arbeiten, um sicheren Zugriff auf die fernen Nachrichten und auf Nachverfolgungssysteme zu konfigurieren. Einige Nachrichtenfunktionen stehen nur auf Anfrage gegenüber Unica zur Verfügung. Weitere Informationen zum Einrichten eines gehosteten Nachrichtenkontos und zum Konfigurieren des Zugriffs auf Unica Hosted Messaging finden Sie im Start- und Administratorhandbuch von Unica Deliver.

Unica Deliver-Integration

Um Unica Deliver mit Unica Journey zu integrieren, müssen Sie die folgenden Konfigurationen in Unica Platformvornehmen.

1. In Unica Platform navigieren Sie zu **Einstellungen > Konfiguration**.
   Die Seite **Konfigurationskategorien** wird angezeigt.
2. Wählen Sie **Journey** aus.
   Die Seite **Einstellungen für 'Journey'** wird angezeigt.
3. Wählen Sie **Einstellungen bearbeiten** aus.
   Die Seite **(Journey)** wird angezeigt.
4. Führen Sie die folgenden Schritte aus:
   a. Wählen Sie für das Feld **Deliver_Configured** die Option **Ja**aus.
   b. Klicken Sie auf **Änderungen speichern**.
5. Wählen Sie im erweiterten Journey-Knoten die Option **Deliver_Configurations**aus.
   Die Seite **Einstellungen für die 'Deliver_Configurations'** wird angezeigt.
6. Wählen Sie **Einstellungen bearbeiten** aus.
   Die Seite **(Deliver_Configurations)** wird angezeigt.
7. Führen Sie die folgenden Schritte aus:

   a. Geben Sie Werte für die folgenden Felder ein:
      - **Deliver_URL**: Die URL für Deliver konfiguriert.
      - **Deliver_Partition**: Die Partition, in der die Berechtigungsnachweise für den Zugriff auf die **Deliver_URL** gespeichert werden.

   b. Klicken Sie auf **Änderungen speichern**.

Kafka Integration

Sie müssen Kafka in Unica Platform für die Journey Knoten konfigurieren.

Zugriff auf Kafka_Configurations in Unica Platform

Führen Sie die folgenden Schritte aus, um auf Kafka_Configurations zuzugreifen:

1. Auf Unica Platform, navigieren Sie zu **Einstellungen > Konfiguration**.
2. Klappen Sie die **Journey** Knoten auf.
3. Wählen Sie die Option **Kafka_Configurations** aus.
4. Wählen Sie die Option **Einstellungen bearbeiten** aus.

Obligatorische Konfigurationen basierend auf dem Wert CommunicationMechanism

Auf der Seite **(Kafka_Configurations)** können Sie einen der folgenden Werte für das Feld CommunicationMechanism auswählen:

- NO_SASLPLAINTEXT_SSL
- SASL_PLAINTEXT
- SSL
- SASL_PLAINTEXT_SSL

Abhängig von Ihrer Auswahl sind die folgenden Felder obligatorisch:

Feldname	**NO_-SASLPLAIN TEXT_SSL**	**SASL_PLAIN TEXT**	**SSL**	**SASL_PLAIN TEXT_SSL**
KafkaBrokerURL	Ja	Ja	Ja	Ja
TopicName	Ja	Ja	Ja	Ja
sasl.mechanism		Ja		Ja
UserForKafkaData		Ja	Ja	Ja
sasl.jaas.config.data Quelle		Ja		Ja
truststore.location			Ja	Ja
truststore.password.da-ta Quelle			Ja	Ja
keystore.location			Ja	Ja
keystore.password.data Quelle			Ja	Ja

Feldname	**NO_-SASLPLAIN TEXT_SSL**	**SASL_PLAIN TEXT**	**SSL**	**SASL_PLAIN TEXT_SSL**
key.password.data-Source			Optional	Optional
ssl.endpoint.identifica-tion. algorithm			Ja	Ja

Nehmen Sie die erforderlichen Konfigurationen vor und klicken Sie auf **Änderungen speichern**.

Note: Der Festplattenspeicher ist erschöpft und der Kafka-Server wurde aufgrund der großen Kafka-Protokolldatei unerwartet abgeschaltet.

Chapter 3. Prozess, ein Journey zu starten und zu stoppen

Prozess zum Starten

1. Starten von Process Web
    a. Konfigurieren Sie Kafka und Zookeeper
        i. IP – auf der Zookeeper/Kafka läuft
        ii. PORT- Kafka (Standard 9092), Zookeeper Standardport 2181
        iii. Protokollpfad
        iv. auto.create.topic.enable = true, diese Eigenschaft sollte auf true gesetzt werden, damit das Dienstprogramm Engine-Veröffentlichen funktioniert.
    b. Starten Sie Zookeeper und warten Sie 10 Sekunden lang
    c. Starten Sie Kafka
    d. Konfigurieren Sie Journey.xml --(Siehe Doc, Doc2)
    e. Konfigurieren Sie Log4j2.xml im Ordner conf
    f. Starten Sie den Webserver (JBOSS/TOMCAT/WebSphere)
    g. Starten Sie die Journey Webanwendung
2. Starten Sie Engine
    a. Konfigurieren Sie application.properties
        i. Fügen Sie die DB-Details hinzu
        ii. Fügen Sie die Kafka Details hinzu(z.B.: spring.kafka.bootstrap-servers=127.0.0.1:9092, 127.0.0.2:9092)
            - Pfad zur Ignite Speicherung, spring.ignite.storage.path. Benutzer, über die die Engine ausgeführt wird, sollten Lese- und Schreibzugriff auf den Pfad des Ignite-Ordners haben
        iii. Konfigurieren Sie Log4j2.xml im Ordner conf
        iv. Konfigurieren Sie die Eigenschaft spring.ignite.ipFinder.List wie folgt:
            - `spring.ignite.ipFinder.List=127.0.0.1:63501,127.0.0.1:63502, 127.0.0.1:63503,127.0.0.1:63504`
        v. Starten Sie Engine (java –jar journeyEngine.jar)

Stoppen Sie den Prozess (Schritte für keinen Datenverlust)

a. Stoppen Sie den Webserver
b. Stoppen Sie die Engine (grep und kill Pid) oder verwenden Sie Director
c. Stoppen Sie Kafka
d. Stoppen Sie Zookeeper

Chapter 4. Benutzerrollen und Berechtigungen für Journey

Bevor Sie mit der Nutzung von Unica Journey beginnen, sollten Sie den Benutzern Rollen und Berechtigungen zuweisen.

Note: Jede Änderung der Konfiguration erfordert einen Neustart von Unica Journey. Weitere Informationen zu Sicherheitskonfigurationen finden Sie im *Administratorhandbuch von Unica Platform*.

Den Journey-Rollen Berechtigungen zuordnen

Bevor Sie einem Benutzer eine Rolle zuweisen, sollten Sie den verfügbaren Rollen Berechtigungen erteilen.

Journey bietet zwei Benutzerrollen:

- **Journey-Admin**
- **Journey-Benutzer**

Um Berechtigungen beiden Rollen zuzuweisen, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Unica Platform-Startseite, **Einstellungen > Benutzerrollen und Berechtigungen**.
   Die Seite **Benutzerrollen und Berechtigungen** wird angezeigt.
2. Erweitern Sie im linken Fenster **Unica Journey > partition1**.
   Die Seite **Partition1** wird angezeigt.
3. Wählen Sie **Berechtigungen zuweisen**.
   Die Seite **(Eigenschaften von Administrationsrollen)** wird angezeigt.

4. Klicken Sie auf **Berechtigungen speichern und bearbeiten**
   Die Seite **(Berechtigungen für partition1)** wird angezeigt.
5. **Anwendungen** erweitern.
6. Werte für die folgenden Felder festlegen:

Operationen	**Journey-Admin-Standardeinstellung**	**Journey-Benutzer-Standardeinstellung**
Datendefinition erstellen	Ja	Nein
Datendefinition bearbeiten	Ja	Nein
Datendefinition löschen	Ja	Nein
Eintragsquellen erstellen	Ja	Nein
Eintragsquellen bearbeiten	Ja	Nein
Eintragsquellen löschen	Ja	Nein
Journey erstellen	Ja	Ja
Journey bearbeiten	Ja	Ja
Journey löschen	Ja	Nein
Journey veröffentlichen	Ja	Ja
Journey veröffentlichen	Ja	Ja
Journey veröffentlichen	Ja	Ja
Ziel hinzufügen/ändern/löschen	Ja	Nein
Zielansicht	Ja	Ja
Einstellungen hinzufügen/ändern/löschen	Ja	Nein

Operationen	Journey-Admin-Standardeinstellung	Journey-Benutzer-Standardeinstellung
Ansicht "Einstellungen"	Ja	Ja

Note:

- Für die Rolle "**Journey-Admin**" empfehlen wir Ihnen, die Berechtigungen nicht zu reduzieren und die Standardberechtigungen beizubehalten. Standardmäßig verfügt **Journey-Admin** über alle Berechtigungen.
- Geben Sie für die **Journey-Benutzerrolle** die Berechtigungen an, die Sie für geeignet halten. Sie können dem **Journey-Benutzer** alle Berechtigungen erteilen, es wird jedoch nicht empfohlen.

7. Klicken Sie nach der Bereitstellung der Berechtigungen auf **Änderungen speichern**.

Rolle JourneyAdmin einem Benutzer zuweisen

Um die **JourneyAdmin**-Rolle einem Benutzer zuzuweisen, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Marketing Platform-Startseite **Einstellungen > Benutzerrollen und Berechtigungen**.
   Die Seite **Benutzerrollen und Berechtigungen** wird angezeigt.
2. Erweitern Sie in der linken Anzeige **Unica Journey**.
3. Wählen Sie **partition1 > JourneyAdmin**aus.
   Die Seite **JourneyAdmin** wird angezeigt.
4. Wählen Sie im Abschnitt **Benutzer** einen Benutzer aus. Beispiel: `asm_admin`.
   Die Benutzerdetailseite **asm_admin (asm_admin)** wird angezeigt.
5. Wählen Sie **Rollen bearbeiten**.
   Die Seite **Rollen bearbeiten** wird angezeigt.
6. Wählen Sie in der Liste **Verfügbare Rollen** die Option **OfferAdmin (Unica- Angebot)** und klicken Sie auf die Schaltfläche **>>**, um die Rolle in die Liste **Ausgewählte Rollen** zu verschieben.
7. Klicken Sie auf **Änderungen speichern**.

JourneyUser Rolle einem Benutzer zuweisen

Um die **JourneyUser**-Rolle einem Benutzer zuzuweisen, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Marketing Platform-Startseite **Einstellungen > Benutzerrollen und Berechtigungen**.
   Die Seite **Benutzerrollen und Berechtigungen** wird angezeigt.
2. Erweitern Sie in der linken Anzeige **Unica Journey**.
3. Wählen Sie **partition1 > JourneyUser**aus.
   Die Seite **JourneyUser** wird angezeigt.
4. Wählen Sie im Abschnitt **Benutzer** einen Benutzer aus. Beispiel: `journey_example`.
   Die Benutzerdetailseite **journey_example (journey_example)** wird angezeigt.
5. Wählen Sie **Rollen bearbeiten**.
   Die Seite **Rollen bearbeiten** wird angezeigt.
6. Wählen Sie in der Liste **Verfügbare Rollen** die Option **OfferAdmin (Unica- Angebot)** und klicken Sie auf die Schaltfläche **>>**, um die Rolle in die Liste **Ausgewählte Rollen** zu verschieben.
7. Klicken Sie auf **Änderungen speichern**.

Chapter 5. Journey-Interaktionsprotokollierung

Die Interaktionsprotokollierung für Journey wird als geplanter Job ausgeführt. Die Terminierungsparameter werden in der `application.properties`-Datei der Journey-Engine festgelegt. Im Folgenden finden Sie ein Beispiel für die Einstellung:

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

Der geplante Job exportiert Daten in ein alternatives Schema, das in den `application.properties`-Dateien der Journey-Engine erneut definiert wird.

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

Bei der Interaktionsprotokollierung wird die Bewegung jedes Kontakts erfasst, der die Anwendung Journey betritt, wenn sie sich durch die einzelnen Journey bewegen, egal, ob diese veröffentlicht oder abgeschlossen sind. Auch Journeys, die publiziert, aber angehalten wurden, werden für die Interaktionsprotokollierung berücksichtigt.

Alle Touchpoints, E-Mails, SMS oder CRM werden für die Interaktionsprotokollierung berücksichtigt, da die Zielgruppendaten mithilfe der konfigurierten Integrationen über die entsprechenden Kanäle gesendet werden. Die empfangenen Antworten, die von jedem Kontakt empfangen werden, werden ebenfalls erfasst.

Log4j2

Sowohl Journey Web als auch Journey Engine verwenden den Standard für die Protokollierung. Die Datei `log4j2.xml` wird sowohl für die Journey-Web als auch für die Journey-Engine innerhalb des `conf`-Ordners im Installationsverzeichnis abgelegt.

Sowohl Journey Web als auch Journey Engine erzeugen reguläre Anwendungsprotokolle sowie Leistungsprotokolle. Bei Journey Web befindet sich die Standardposition der Protokolle innerhalb des `logs` Ordners. Für Journey Engine ist die Standardposition der

Protokolle innerhalb des `performancelogs` Ordners. Für sowohl Journey Web als auch Journey Engine werden die genannten Ordner innerhalb des Installationsverzeichnisses abgelegt.

Chapter 6. Journey DSGVO

Zugriff auf Journey DSGVO

Das DSGVO Tool kann über den Journey Anwendungsordner zugegriffen werden. Unten finden Sie den Speicherort:

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

DSGVO unterstützt > MariaDB, **MS SQL Server**, **OneDb Datenbanken** und **Oracle**

Ausführung von Journey DSGVO

Führen Sie die folgenden Schritte aus, um Journey DSGVO auszuführen:

1. Die folgenden Eigenschaften in der Datei `gdpr.properties vor` sollen geändert werden:

Eigenschaftsname	Beispielwert	Hinweise
`Journey.audience.DB-Type`	`ORACLE`	Zur Zeit wird nur Oracle von Journey unterstützt.
`Journey.audience.Db.Schema.Name`	`JourneyUser`	Name des Schemas, der in der Journey Datenbank verwendet wird.
`Journey.audience-.Field`	`email/mobileNumber`	Feldname in der Eingabe-datei `CSV`.
`Journey.audience.Csv`	`<GDPR_HOME>/sam-ple/JourneyAudi-ences.csv`	Ersetzen Sie `<GDPR_-HOME>` durch den ak-tuellen Verzeichnispfad. Dies ist die Eingabedatei `CSV` mit Datensätzen, die Sie aus Journey deak-tivieren müssen.

Eigenschaftsname	Beispielwert	Hinweise
`Journey.audience.Output`	`<GDPR_HOME>/Journey-Audiences.sql`	Der `JourneyAudiences.sql` ist der Name einer Ausgabedatei, die alle SQL Abfragen enthält, die zur Löschung aller Datensätze aus der Journey Anwendung verwendet wird. Ersetzen Sie `<GDPR_HOME>` durch den aktuellen Verzeichnispfad.
`Journey.audience.Output. FileSizeLimit`	`10`	Der Wert wird in MB angegeben. Sollte die Dateigröße den eingegebenen Wert überschreiten, werden mehrere Dateien mit den folgenden Zusätzen generiert: `JourneyAudiences_0`, `JourneyAudiences_1` usw.

2. **Note:** Falls Fehler auftreten, können Sie diese Fehler mithilfe dieser Protokolldatei verfolgen.

3. Führen Sie einen der folgenden Schritte aus, um die Datei auszuführen:
   a. Für Windows, suchen Sie die Datei `gdpr_purge.bat` und führen Sie diese aus. Z.B. wenn sich die Datei `gdpr_purge.bat` im Verzeichnis `D:\workspace\HCL_GDPR\dist\journey\` befindet, führen Sie die Datei `gdpr_purge.bat` aus.

   b. Für UNIX-basierte Systeme, suchen Sie die Datei `gdpr_purge.sh` und führen Sie diese aus. Z.B. wenn sich die Datei `gdpr_purge.sh` im Verzeichnis `\workspace\HCL_GDPR\dist\journey\` befindet, führen Sie den Befehl ./ gdpr_purge.sh aus.

4. Nachdem die Datei `gdpr_purge.bat` (für Windows) oder `gdpr_purge.sh` (für Linux) ausgeführt wird, werden die Ausgabedateien *"JourneyAudiences 0"*, *"JourneyAudiences _1"*, *"JourneyAudiences _2"* usw. an dem in den obigen Schritten angegebenen Speicherort `<GDPR_HOME>` generiert. Die Anzahl der generierten Dateien hängt von der angegebenen Dateigröße ab.
5. Die Datei *"JourneyAudiences_x"* enthält Löschabfragen für Datensätze, die in JourneyAudiences.csv erwähnt werden
6. Diese Abfragen müssen bei Bedarf manuell in der Datenbank „Journey“ ausgeführt werden, damit die Datensätze aus der Tabelle journeyaudiences gelöscht werden.

Das Dienstprogramm DSGVO entfernt die Datensätze aus der folgenden Tabelle: JourneyAudiences, AudienceResponse, AudienceResponseMetaData, AudienceResponseInteraction, JourneyAudienceMilestone and JourneyAudienceGoal. Die Daten aus den jeweiligen Tabellen, in denen die aggregierten Zählungen gespeichert sind, werden jedoch nicht gelöscht. Z.B. die Tabellen wie journeyFlow, journeyAudienceFlow, JourneyGoalContactTransaction usw. Daher kommt es zu einer Abweichung der Zählung in der Benutzeroberfläche.

Mit Hilfe des DSGVO Tool wäre es dem Benutzer nicht möglich, die Kundendaten aus 'Kafka Thema veröffentlichen' oder aus den im Dateisystem verfügbaren Dateien zu löschen. Der Benutzer muss diese Daten nach Bedarf manuell löschen.

Mit Hilfe des DSGVO Tool wäre es dem Benutzer nicht möglich, die vom JDBC Connector exportierten Kundendaten zu löschen.

Chapter 7. Kafka-Authentifizierung mit SSL verwenden

Wenn Sie die Kafka-Instanz Ihres Unternehmens verwenden, können Sie für diese Instanz von Kafka konfigurierten Zertifikate verwenden. Sie müssen keine SSL-Schlüssel und -Zertifikate generieren und können die Clientzertifikate zum Konfigurieren in den Journey-Anwendungseigenschaften abrufen.

Wenn Sie nicht über die Zertifikate verfügen, können Sie eine selbst signierte Zertifizierungsstelle (CA) generieren, die lediglich ein öffentlich-privates Schlüsselpaar und ein Zertifikat ist.

Sie müssen dieselbe CA für jeden Kafka-Client und trustStore eines Vermittlers hinzufügen.

SSL-Schlüssel und Zertifikat für jeden Kafka-Vermittler generieren

Führen Sie die folgenden Schritte aus, um selbstsignierte Zertifikate für den Kafka-Server zu generieren.

Voraussetzungen

- Sie müssen über Java KeyTool und OpenSSL verfügen, um Zertifikate und trustStore generieren zu können.
- Optional können Sie anstelle von OpenSSL jedes Dienstprogramm für die SSL-Zertifikatgenerierung verwenden.

1. Um SSL zu implementieren, müssen Sie den Schlüssel und das Zertifikat für jede Maschine im Cluster generieren. Generieren Sie den Schlüssel zunächst in einem vorübergehenden Keystore, sodass Sie ihn später mit CA exportieren und signieren können.
   ```
   keytool -keystore kafka.server.keystore.jks -alias localhost -validity 365 -genkey
   ```
   - keystore: Die keystore-Datei, die das Zertifikat speichert. Die keystore-Datei enthält den privaten Schlüssel des Zertifikats. Daher muss sie sicher aufbewahrt werden.
   - validity: Die gültige Zeit des Zertifikats in Tagen.

2. Ihre Eigene CA erstellen (Zertifizierungsstelle)

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

   Die generierte CA ist lediglich ein öffentlich-privates Schlüsselpaar und Zertifikat und es ist beabsichtigt, andere Zertifikaten zu signieren.
3. Fügen Sie die generierte CA zum trustStore der Clients hinzu, damit die Clients dieser CA vertrauen können.
   - `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. Unterzeichnen Sie alle Zertifikatszeugnisse im Keystore mit der generierten CA.
   a. Zertifikat aus dem Keystore exportieren:

      ```
      keytool -keystore kafka.server.keystore.jks -alias localhost -certreq -file cert-file
      ```
5. Unterzeichnen Sie sie mit der CA.

   ```
   openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -days 365 -CAcreateserial -passin pass:<password>
   ```
6. Importieren Sie sowohl die Zertifikate der CA als auch das signierte Zertifikat in den Keystore.

   ```
   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. Erstellen Sie einen Client-Keystore und importieren Sie beide Zertifikate der CA und die signierten Zertifikate in den Keystore des Clients. Diese Clientzertifikate werden in Anwendungseigenschaften eingesetzt.

   ```
   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`

Konfigurieren des für Kafka-Servers, Journey und Link-Komponenten mit SSL

Die Serverzertifikate, die für Kafka Server und Clientzertifikate verwendet werden sollen, müssen von allen Anwendungen verwendet werden, die sich mit dem Kafka-Server verbindet, einschließlich Journey Web, Journey Engine, Unica Link – Kafka-Link oder sämtlichen anderen Tools, die Sie benötigen, um eine Verbindung zu diesem Kafka-Server herzustellen.

Führen Sie die in den folgenden Abschnitten bereitgestellten Prozeduren aus, um den Kafka-Server, Journey-Komponenten und Link-Komponenten mit SSL-Authentifizierung zu konfigurieren.

Konfigurieren des Kafka-Servers mit SSL-Authentifizierung

Sie dürfen die folgenden Serverzertifikate nur für den Kafka-Server verwenden. Teilen Sie diese Zertifikate mit den erforderlichen Maschinen und notieren Sie sich das Kennwort.

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

Aktualisieren Sie die folgenden server.properties im Konfigurationsverzeichnis des Kafka-Servers.

```
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
```

Journey-Engine mit Kafka SSL konfigurieren

Verwenden Sie die folgenden Clientzertifikate und teilen Sie diese Zertifikate mit den erforderlichen Maschinen und notieren Sie sich das Kennwort.

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

1. Aktualisieren Sie die Journey-Engine-Datei `log4j2.xml` aus dem `<JOURNEY_HOME>/Engine/conf/`-Verzeichnis. Entfernen Sie die Kommentarzeichen für die folgenden Zeichen:`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. Aktualisieren Sie das folgende `journey_engine_master.config` vom Verzeichnis `<JOURNEY_HOME>/Engine/`.
3. Aktualisieren Sie die folgenden Eigenschaftswerte.

```
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=
```

Konfigurieren von Journey-Web mit Kafka SSL

1. Die Journey-Webdatei `application.properties` aus dem `<JOURNEY_HOME>/Web/properties/`-Verzeichnis aktualisieren.
2. Aktualisieren Sie die folgenden Eigenschaftswerte.

```
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=
```

Komponente Unica Link mit SSL konfigurieren

Aktualisieren Sie die folgenden Eigenschaftswerte in der Unica Link-Installations-Datei `kafkalink.properties`.

```
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=
```

Konfigurieren des Kafka-Server, Journey und Link-Komponenten mit SASL

Führen Sie die in den folgenden Abschnitten bereitgestellten Prozeduren aus, um den Kafka-Server, Journey-Komponenten und Link-Komponenten mit SASL-Authentifizierung zu konfigurieren.

Konfigurieren des Kafka-Servers mit SASL-Authentifizierung

1. Geben Sie den JVM-Parameter in `kafka-run-class.bat/sh` an.

   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% %*`

   Beispieldatei `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. Aktualisieren Sie die folgende Eigenschaftendatei vom Kafka-Server aus `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
```

Journey-Engine mit Kafka SASL konfigurieren

1. Aktualisieren Sie die Journey-Engine-Datei `log4j2.xml` aus dem `<JOURNEY_HOME>/Engine/conf/`-Verzeichnis. Entfernen Sie die Kommentarzeichen für die folgenden Zeichen:`log4j2.xml`

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

2. Aktualisieren Sie das folgende `journey_engine_master.config` vom Verzeichnis `<JOURNEY_HOME>/Engine/`. Aktualisieren Sie die folgenden Eigenschaftswerte.

```
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
```

Konfigurieren von Journey-Web mit Kafka SASL

Die Journey-Webdatei `application.properties` aus dem `<JOURNEY_HOME>/Web/properties/`-Verzeichnis aktualisieren.

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

Komponente Unica Link mit Kafka SASL konfigurieren

Aktualisieren Sie die folgenden Eigenschaftswerte in der Unica Link-Installations-Datei `kafkalink.properties`.

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

Konfigurieren des Kafka-Servers und Journey-Komponenten mit SASL_SSL-Konfiguration

Um den Kafka-Server und andere Journey-Komponenten mit SASL-Authentifizierung zu konfigurieren, führen Sie die in den folgenden Abschnitten bereitgestellten Prozeduren aus.

Note: Unica Link unterstützt keine Verbindung zum Kafka-Link mit SASL_SSL-Authentifizierung. Sie müssen entweder SASL oder SSL als Authentifizierungsmechanismus verwenden.

Konfigurieren des Kafka-Servers mit Kafka SASL_SSL

Aktualisieren Sie die folgenden server.properties im Konfigurationsverzeichnis des Kafka-Servers.

```
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
```

Journey-Engine mit Kafka SASL_SSL konfigurieren

1. Aktualisieren Sie die Journey-Engine-Datei `log4j2.xml` aus dem `<JOURNEY_HOME>/Engine/conf/`-Verzeichnis.

   Entfernen Sie die Kommentarzeichen für die folgenden Zeichen:`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}</Proper
   ty>
   <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.ident
ification.algorithm}</Property>
```

2. Aktualisieren Sie das folgende `journey_engine_master.config` vom Verzeichnis `<JOURNEY_HOME>/Engine/`.

   Aktualisieren Sie die folgenden Eigenschaftswerte.

```
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
```

Konfigurieren von Journey-Web mit Kafka SASL_SSL

Aktualisieren Sie die folgende Journey`application.properties`-Webdatei aus dem `<JOURNEY_HOME>/Web/properties/`-Verzeichnis.

```
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 8. Tomcat-Webanwendungsserver für SSL konfigurieren

Konfigurieren Sie auf jedem Anwendungsserver, auf dem eine Unica-Anwendung implementiert wird, den Webanwendungsserver so, dass die von Ihnen vorgesehenen Zertifikate genutzt werden.

Weitere Informationen zur Ausführung dieser Schritte entnehmen Sie bitte der Dokumentation Ihres Webanwendungsservers.

Sicherheit von Cookies

Einige Cookies sind im Client-Browser möglicherweise nicht angemessen gesichert. Bei ungesicherten Cookies ist die Anwendung anfällig für Man-in-the-Middle- und Session-Hijacking-Angriffe. Um dies zu verhindern, ergreifen Sie die folgenden Vorsichtsmaßnahmen.

- Erzwingen Sie stets die Verwendung von SSL, um die Gefahr zu verringern, dass Cookies bei der Übertragung abgefangen werden.
- Legen Sie im Webanwendungsserver die Flags `secure` und `httponly` für alle Cookies fest.
    - Das Flag `secure` weist den Browser an, das Cookie ausschließlich über eine HTTPS-Verbindung zu senden. Wenn Sie dieses Flag festlegen, müssen Sie in allen Anwendungen, die miteinander kommunizieren, SSL aktivieren.
    - Das Flag `httponly` verhindern den Zugriff auf Cookies über ein Script auf Clientseite.

Festlegen der Flags für SSL in Tomcat

Führen Sie die folgenden Änderungen auf dem `.xml` Server von Tomcat durch, um die Flags `secure` und `httponly` in Tomcat festzulegen.

```
<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/PlatformClientIdenti
ty.jks" keystorePass="password" >     </Connector>
```

Unica Journey mit SSL konfigurieren

Um Unica Journey für die Nutzung mit SSL zu konfigurieren, müssen Sie einige Konfigurationseigenschaften festlegen. Nutzen Sie für Ihre Installation von Unica Journeysowie für die durch SSL zu sichernde Kommunikation die in diesem Abschnitt beschriebenen geeigneten Verfahren.

Wenn Sie auf Ihre Unica-Installation über eine gesicherte Verbindung zugreifen und wenn Sie wie in den nachfolgenden Verfahren beschrieben Navigationseigenschaften für Anwendungen festlegen, müssen Sie `https` und die Nummer des gesicherten Ports in der URL verwenden. Der standardmäßige SSL-Port ist`8443` für Tomcat.

Mit dieser Prozedur können Sie SSL in Journey konfigurieren

1. Melden Sie sich in Unica an und klicken Sie auf **Einstellungen > Konfiguration**.
2. Setzen Sie den Wert von der Eigenschaft `Affinium | Journey | Navigation` auf die Unica Journey-URL.

   Zum Beispiel: `https://`*`host.domain:SSL_port`*`/unica`

   Dabei gilt Folgendes:

   - *`host`* ist der Name oder die IP-Adresse des Computers, auf dem Unica Journey installiert ist
   - *`domain`* ist die Unternehmensdomäne, in der Ihre Unica-Produkte installiert sind
   - *`SSL_Port`* ist der SSL-Port auf dem Webanwendungsserver, auf dem Unica Journey bereitgestellt wurde

   Beachten Sie das `https` in der URL.

Chapter 9. Einstellungen

Verwenden Sie das Menü Einstellungen, um die Journey Integrationen wie E-Mail-Verbinder, SMS-Verbinder, CRM-Verbinder und REST-Integrationen zu verwalten.

Standard-E-Mail-Verbindung einrichten

Wenn Sie über mehrere Verbinder mit Unica Link zum Senden einer E-Mail verfügen, können Sie die Standardverbindung für die E-Mail im Menü **Einstellungen** festlegen.

Führen Sie die folgenden Schritte aus, um eine Standard-E-Mail-Verbindung zu erstellen:

1. Wählen Sie  **> Link > E-Mail** aus.
   Die **E-Mail**-Seite wird angezeigt.
2. Wählen Sie in der Liste **Verfügbare Verbindungen** eine Verbindung aus.
   Die verfügbaren Verbindungen umfassen Mandrill, MailChimp usw.
3. Klicken Sie auf **Speichern**.
   Sie können auch eine vorhandene Verbindung abwählen und auf **Speichern** klicken. Dies stellt sicher, dass keine Standardverbindung bestimmt wurde.

Standardverbindung für SMS einrichten

Wenn Sie über mehrere Verbinder mit Unica Link zum Senden einer SMS verfügen, können Sie die Standardverbindung für die SMS im Menü **Einstellungen** festlegen.

Führen Sie die folgenden Schritte aus, um eine Standard-SMS-Verbindung zu erstellen:

1. Wählen Sie  **> Link > SMS** aus.
   Die Seite **SMS** wird angezeigt.
2. Wählen Sie in der Liste **Verfügbare Verbindungen** eine Verbindung aus.

Note:

Die Telefonnummern sollten gemäß der Spezifikation des Bereitstellungskanals erwähnt werden. Journey sendet die Telefonnummer im gleichen Format an den Bereitstellungskanal. Beispiel: In Bezug auf Twilio Connection lautet das Telefonnummernformat, das mit Journey unterstützt wird, wie folgt:

- *<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`.

Egal, welches Format der Telefonnummer Sie angeben, Unica Journey speichert die Nummer im folgenden Format: <plus sign><country-code><10-digit phone number>. Beispiel: Wenn Sie eine Telefonnummer als `+ 1 540-324-1212`angeben, speichert Unica Journey die Telefonnummer unter `+15403241212`.

Wenn Sie Twilio als Standardverbindung für SMS auswählen, werden Telefonnummern nur im folgenden Format akzeptiert: *<plus sign><country-code><10-digit phone number>*. Beispiel: `+15403241212`.

3. Klicken Sie auf **Speichern**.

Eine Standard-CRM-Verbindung festlegen

Wenn Sie über mehrere CRM-Verbindungen verfügen, können Sie die standardmäßige CRM-Verbindung im Menü **Einstellungen** festlegen.

Führen Sie die folgenden Schritte aus, um eine Standard-CRM-Verbindung zu erstellen:

1. Wählen Sie  **> Link > CRM** aus.
   Die **CRM**-Seite wird angezeigt.

2. Wählen Sie in der Liste **Verfügbare Verbindungen** eine Verbindung aus.
3. Klicken Sie auf **Speichern**.

Einrichtung von einer standardmäßigen ADTECH Verbindung

Gibt es mehrere ADTECH Verbindungen, können Sie die standardmäßige ADTECH Verbindung unter dem Menü **Einstellungen** festlegen.

Führen Sie die folgenden Schritte aus, um eine standardmäßige ADTECH Verbindung einzurichten:

1. Wählen Sie  **> Link > ADTECH** aus
   Die Seite **ADTECH** wird angezeigt
2. Aus der Liste **Verfügbare Verbindungen**, wählen Sie eine Verbindung aus.
3. Klicken Sie auf **Speichern**.

Einrichtung von einer standardmäßigen Datenbank Verbindung

Gibt es mehrere Datenbank Verbindungen, können Sie die standardmäßige Datenbank Verbindung unter dem Menü **Einstellungen** festlegen.

Führen Sie die folgenden Schritte aus, um eine standardmäßige Datenbank Verbindung einzurichten:

1. Wählen Sie  **> Link > Datenbank** aus
   Die Seite **Datenbank** wird angezeigt
2. Aus der Liste **Verfügbare Verbindungen**, wählen Sie eine Verbindung aus.
3. Klicken Sie auf **Speichern**.

Verbindungen verwalten

Sie können Unica Link-Verbindungen über dieses Menü verwalten.

Sie können eine Verbindung mit Unica Link-Verbindern wie MailChimp, Mandrill, Salesforce und Twilio erstellen. Sie können alle vorhandenen Verbindungen im Fenster **vorhandene Verbindungen** (n) anzeigen, wobei n die Anzahl der Verbindungen ist.

1. Führen Sie die folgenden Schritte aus, um eine Mailchimp-Verbindung zu erstellen:

    a. Wählen Sie  **> Link > Verbindungen verwalten > Neue erstellen** aus. Die Seite **Neue Verbindung erstellen** wird angezeigt.

    b. Geben Sie Werte für die folgenden Felder ein:
        - **Name** - Obligatorisch
        - **Beschreibung** - Optional

    c. Klicken Sie auf **Weiter**.

    d. Wählen Sie in der Anzeige **Verbindung auswählen MailChimp** aus.

    e. Stellen Sie im Feld **Verbindungseinstellungen** Werte für die folgenden Pflichtfelder bereit:

    Note: Weitere Informationen zu den Feldern und zu den zu erstellenden Werten finden Sie im *Unica LinkMailChimp-Verbinder-Benutzerhandbuch*.

        - **Basis-URL**
        - **Benutzer-ID**
        - **API-Schlüssel**
        - **Häufigkeit von Aktivitätsabrufen**
        - **Aktivitätsabruf-Einheiten**

    f. Klicken Sie auf **Testen**, um die Verbindung zu testen. Wenn die angegebenen Werte richtig sind, wird eine Erfolgsmeldung angezeigt. Wenn die angegebenen Werte falsch sind, wird eine Fehlermeldung angezeigt.

g. Um die Verbindung zu speichern, klicken Sie auf **Speichern**.
Die neue Verbindung wird erfolgreich gespeichert und wird im Fenster **Vorhandene Verbindungen** angezeigt.

2. Führen Sie die folgenden Schritte aus, um eine Mandrill-Verbindung zu erstellen:

a. Wählen Sie  **> Link > Verbindungen verwalten > Neue erstellen** aus.
Die Seite **Neue Verbindung erstellen** wird angezeigt.

b. Geben Sie Werte für die folgenden Felder ein:
- **Name** - Obligatorisch
- **Beschreibung** - Optional

c. Klicken Sie auf **Weiter**.

d. Wählen Sie in der Anzeige **Verbindung auswählen** die Option **Mandrill** aus.

e. Stellen Sie im Feld **Verbindungseinstellungen** Werte für die folgenden Pflichtfelder bereit:

Note: Informationen zu den Feldern und den einzutragenden Werten finden Sie im *Unica LinkMandrill-Benutzerhandbuch*.

- **API-Schlüssel**
- **Häufigkeit von Aktivitätsabrufen**
- **Aktivitätsabruf-Einheiten**

f. Klicken Sie auf **Testen**, um die Verbindung zu testen. Wenn die angegebenen Werte richtig sind, wird eine Erfolgsmeldung angezeigt. Wenn die angegebenen Werte falsch sind, wird eine Fehlermeldung angezeigt.

g. Um die Verbindung zu speichern, klicken Sie auf **Speichern**.
Die neue Verbindung wird erfolgreich gespeichert und wird im Fenster **Vorhandene Verbindungen** angezeigt.

3. Führen Sie die folgenden Schritte aus, um eine Salesforce-Verbindung zu erstellen:

a. Wählen Sie  **> Link > Verbindungen verwalten > Neue erstellen** aus.
Die Seite **Neue Verbindung erstellen** wird angezeigt.

b. Geben Sie Werte für die folgenden Felder ein:
- **Name** - Obligatorisch
- **Beschreibung** - Optional

c. Klicken Sie auf **Weiter**.

d. Wählen Sie in der Anzeige **Verbindung auswählen Salesforce**aus.

e. Stellen Sie im Feld **Verbindungseinstellungen** Werte für die folgenden Pflichtfelder bereit:

Note: Weitere Informationen zu den Feldern und zu den zu erstellenden Werten finden Sie im *Unica LinkSalesforce-Benutzerhandbuch*.

- **Instanz-URL**
- **Zugriffstoken:**
- **Version**

f. Klicken Sie auf **Testen**, um die Verbindung zu testen. Wenn die angegebenen Werte richtig sind, wird eine Erfolgsmeldung angezeigt. Wenn die angegebenen Werte falsch sind, wird eine Fehlermeldung angezeigt.

g. Um die Verbindung zu speichern, klicken Sie auf **Speichern**.
Die neue Verbindung wird erfolgreich gespeichert und wird im Fenster **Vorhandene Verbindungen** angezeigt.

4. Führen Sie die folgenden Schritte aus, um eine Twilio-Verbindung zu erstellen:

a. Wählen Sie  **> Link > Verbindungen verwalten > Neue erstellen** aus.
Die Seite **Neue Verbindung erstellen** wird angezeigt.

b. Geben Sie Werte für die folgenden Felder ein:

- **Name** - Obligatorisch
- **Beschreibung** - Optional

c. Klicken Sie auf **Weiter**.

d. Wählen Sie in der Anzeige **Verbindung auswählen** die Option **Twilio**aus.

e. Stellen Sie im Feld **Verbindungseinstellungen** Werte für die folgenden Pflichtfelder bereit:

Note: Informationen zu den Feldern und den einzutragenden Werten finden Sie im *Unica LinkTwilio-Benutzerhandbuch*.

- **Basis-URL**
- **Account SID**
- **Authentifizierungstoken**
- **Von Nummer**
- **Wiederholungsintervall**
- **Wiederholungsversuche**

f. Klicken Sie auf **Testen**, um die Verbindung zu testen. Wenn die angegebenen Werte richtig sind, wird eine Erfolgsmeldung angezeigt. Wenn die angegebenen Werte falsch sind, wird eine Fehlermeldung angezeigt.

g. Um die Verbindung zu speichern, klicken Sie auf **Speichern**.
Die neue Verbindung wird erfolgreich gespeichert und wird im Fenster **Vorhandene Verbindungen** angezeigt.

REST-Integration

REST-Schlüssel werden für die Anmeldung von Drittanbietern bei der Anwendung genutzt. Sie können ein Paar mit Schlüsselwert generieren und mit dem Schlüsselwertpaar können Sie sich bei Journey unter Verwendung von Anwendungen von Drittanbietern anmelden.

Neue Integration von REST erstellen

Führen Sie die folgenden Schritte aus, um ein neues REST-Integrationsschlüsselpaar zu erstellen:

1.  **> REST** auswählen.
   Die Seite **REST** wird angezeigt.
2. Klicken Sie auf **+ REST-Integration**.
   Die Seite **Neue REST-Integration** wird angezeigt.
3. Geben Sie Werte für die folgenden Felder ein:
   - **Anwendungsname** - Obligatorisch.
   - **Beschreibung** - Optional
4. Klicken Sie auf **Schlüssel generieren**.
   Das System generiert eine **ClientID** und ein **clientSecret**.
5. Verwenden Sie die Schaltleiste, um den **Status** in `aktiv` oder `inaktiv`zu ändern.
   Standardmäßig ist der **Status** `aktiv`.
6. Um die REST-Integration zu speichern, klicken Sie auf **Speichern**.
   Um Zielgruppendaten an Journey zu senden , befolgen Sie die Details, die in der REST-Eingangsquelle für die Konfiguration des REST-Endpunktes erwähnt wurden. Verwenden Sie die Daten zu **ClientID** und **clientSecret**, die Sie beim Ausführen von Schritt (4) erhalten haben, um den REST-Endpunkt bei der Eintragsquelle zu konfigurieren.

Anzeigen der REST-Integrationsliste

Unica Journey verwaltet eine Liste von erstellten REST-Integrationen.

Um REST-Integrationen anzuzeigen, führen Sie die folgenden Schritte aus:

1.  **> REST** auswählen.
   Die Seite **REST** wird angezeigt.
2. Führen Sie eine der folgenden Operationen aus:

a. Um die REST-Integrationen in aufsteigender Reihenfolge oder absteigender Reihenfolge im Feld 'Name' anzuzeigen, klicken Sie auf **Name**.
b. Um die REST-Integrationen in aufsteigender Reihenfolge oder absteigender Reihenfolge im Feld 'Beschreibung' anzuzeigen, klicken Sie auf **Beschreibung**.

Vorhandene REST-Integration ändern

Sie können nur die Beschreibung und den Status einer vorhandenen REST-Integration ändern.

Um vorhandene REST-Integrationen zu ändern, führen Sie die folgenden Schritte aus:

1.  **> REST** auswählen.
   Die Seite **REST** wird angezeigt.
2. Zur Änderung einer REST-Integration können Sie entweder:
   - die gewünschte REST-Integration aus der Liste auswählen
   - Auswählen **>** 

   Die Seite **REST-Integration aktualisieren** wird angezeigt.
3. Sie können nur die folgenden Felder aktualisieren:
   - **Beschreibung:**
   - **Status**
4. Klicken Sie auf **Speichern**, um die Änderungen oder Modifikationen zu speichern.

REST-Integrationen löschen

Sie können nur inaktive REST-Integrationen löschen, die nicht mehr verwendet oder benötigt werden.

Informationen zum Ändern des Status eines REST-Integrationseintrags finden Sie unter Vorhandene REST-Integration ändern (on page 45).

Um vorhandene inaktive REST-Integrationen zu entfernen, führen Sie die folgenden Schritte aus:

1.  **> REST** auswählen.
   Die Seite **REST** wird angezeigt.
2. Führen Sie einen der folgenden Schritte aus:
   - Um eine REST-Integration zu löschen, wählen Sie **>**  hinter der REST-Integration in der Liste aus.
   - Um mehrere REST-Integrationen zu löschen, wählen Sie die Kontrollkästchen vor den REST-Integrationen aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
3. Ein Bestätigungsfeld wird angezeigt. Klicken Sie auf **OK**, um den Löschvorgang fortzusetzen.

Integration von Journey Proxy

Der Proxy Server wurde in Journey Web- und Engine-Projekte integriert. Dies ermöglicht es dem Benutzer, die Sicherheit zu erhöhen und den Anwendungsserver hinter den Proxy Servern zu halten. Der Proxy Server kommuniziert mit den Servern von Deliver, Link und Platform.

Journey Web – Kommuniziert mit den Servern von Deliver, Link und Platform, um die Konfigurationsdetails abzurufen und gleichzeitig den E-Mail/SMS/AdTech Point in Journey zu integrieren.

Journey Engine – Verwendet einen Proxy zur Kommunikation mit den Servern von Deliver/Link, um die Details von E-Mail/SMS/Adtech an Endserver zu senden.

Von Journey Web unterstützter Proxy

1. SOCKS
2. HTTP
3. HTTPS

Von Journey Engine unterstützter Proxy

1. HTTP

Note: Die SOCKS- und HTTPS-Proxys werden nicht von SOAP (Apache Axis2), das von Engine zur Kommunikation mit Deliver verwendet wird, unterstüzt.

Zu konfigurierende Eigenschaft für Engine in der Datei 'Engine application.properties'.

- journey.proxy.type=NONE
- spring.proxy.host=[IP]
- spring.proxy.port=[PORT]
- spring.proxy.username=[username]
- spring.proxy.password=[password]

Zu konfigurierende Eigenschaft für Web in der Datei 'Web application.properties'

- journey.proxy.type=NONE
- spring.proxy.host=[IP]
- spring.proxy.port=[PORT]
- spring.proxy.username=[username]
- spring.proxy.password=[password]
- server.use-forward-headers=true

Note: Der Standardwert der Eigenschaft journey.proxy.type beträgt NONE. Wird der Wert auf NONE gesetzt, wird der Proxy deaktiviert.

Entwicklertools

Zeigt die Liste der Entwicklertools an.

API-Dokumentation

Der Benutzer kann die Liste der REST-APIs für Journey finden.