Unica Journey V12.1.2 Administratorhandbuch

Contents

Chapter 1. Eine Einführung in Unica Journey..... 1
- Funktionen von Unica Journey.....1
- Vorteile von Unica Journey..... 1

Chapter 2. Unica Journey Integrationen.....3
- Eine Einführung in Unica Deliver..... 6
- Unica Deliver integration..... 7
- Kafka-Integration.....8

Chapter 3. Prozess, ein Journey zu starten und zu stoppen..... 10

Chapter 4. Journey Benutzerrollen und Berechtigungen..... 11
- Den Journey Rollen die Berechtigungen zuweisen.....11
- Rolle JourneyAdmin einem Benutzer zuweisen.....12
- JourneyUser Rolle einem Benutzer zuweisen..... 13
- Dem Benutzer eine ContactCentralAdmin Rolle zuweisen.....13

Chapter 5. Journey Interaktionsprotokollierung..... 14

Chapter 6. Journey GDPR.....15

Chapter 7. Kafka-Authentifizierung mit SSL verwenden.....17
- Konfiguration von Kafka Server, die Komponenten von Journey und Link mit SSL..... 18
  - Konfigurieren des Kafka-Servers mit SSL-Authentifizierung..... 18
  - Konfiguration von Journey Engine mit Kafka SSL.....18
  - Konfiguration von Journey web mit Kafka SSL.....19
  - Konfiguration von Unica Link Komponenten mit SSL.....19
- Konfiguration von Kafka Server, Journey und Link Komponenten mit SASL..... 19
  - Konfigurieren des Kafka Servers mit SASL-Authentifizierung..... 20
  - Konfiguration von Journey Engine mit Kafka SASL..... 20
  - Konfiguration von Journey Web mit Kafka SASL..... 20
  - Konfiguration von Unica Link Komponenten mit Kafka SASL..... 20
- Konfiguration von Kafka Server und Journey Komponenten mit SASL_SSL Konfiguration.....21
  - Konfigurieren des Kafka-Servers mit Kafka SASL_SSL.....21
  - Konfiguration von Journey Engine mit Kafka SASL_SSL.....21
  - Konfiguration von Journey Web mit Kafka SASL_SSL.....22

Chapter 8. Tomcat-Webanwendungsserver für SSL konfigurieren..... 23
- Sicherheit von Cookies.....23
  - Festlegen der Flags für SSL in Tomcat..... 23
- Konfiguration von Unica Journey mit SSL.....23

Chapter 9. Mailchimp Konfiguration..... 25

Chapter 10. Einstellungen..... 28
- Standard-E-Mail-Verbindung einrichten..... 28
- Standardverbindung für SMS einrichten.....28
- Eine Standard-CRM-Verbindung festlegen..... 29
- Standard ADTECH-Verbindung einrichten..... 29
- Standard Datenbankverbindung einrichten..... 30
- Verbindungen verwalten.....30
- REST-Integration.....33
  - Neue Integration von REST erstellen..... 33
  - Anzeigen der REST-Integrationsliste..... 34
  - Vorhandene REST-Integration ändern..... 34
  - REST-Integrationen löschen.....35
- Integration von Journey Proxy..... 35
- Entwicklertools.....36
  - API-Dokumentation..... 37

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:

- **Zielorientierte Erlebnisse**: Definieren Sie Ziele für Ihre Kundenerfahrung und passen Sie Ihre Journeys in Echtzeit an, um sie zu erreichen.
- **Orchestrierungs-Leinwand**: Erstellen und visualisieren Sie Ihre gesamte Kunden-Journey über Kanäle/ Touchpoints und Ereignisse mit einer schlanken und intuitiven Journey Leinwand.
- **Immer auf Engagement**: Vollständig automatisierte Ausführung, die mit jedem Schritt des Markeneinsatzes Ihres Kunden synchronisiert wird.
- **Einblicke in Echtzeit**: Verstehen Sie Ihr Kundenverhalten mit Einsichten, die Dinge so widerspiegeln, wie auf in ihren Journeys passieren.
- **Auswahl an 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 Daten-Framework**: 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 Markentreue**: Stärken Sie Ihre Marke folgendermaßen mit gezielten und automatisierten Journeys, die Kunden erfassen, pflegen, konvertieren und binden.
- **Verstärkte Omni Channel 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 Kundenkonversionszyklus**: 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.
- **Niedrigere 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 für die 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 Referenzverbinder gemäß Ihres Wunsches:

- **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

Task	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*.
Installieren des Unica Link Verbinders – MailChimp	Siehe *Unica Link Mailchimp Connector-Benutzerhandbuch*.
Installieren des Unica Link Verbinders – Mandrill	Siehe *Unica Link Mandrill Connector-Benutzerhandbuch*.
Installieren des Unica Link Verbinders – Twilio	Siehe *Unica Link Twilio Connector-Benutzerhandbuch*.
Installieren des Unica Link Verbinders – Salesforce	Siehe *Unica Link Salesforce Connector-Benutzerhandbuch*.

Note: HCL stellt nicht das Konto oder den Zugriff auf diese Anbieter von Bereitstellungskanälen bereit. Basierend auf Ihrer Vorgabe 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. Dies hilft auch bei der Erfassung der E-Mail-Benachrichtigungen in Echtzeit und in bei der Zielgruppenverarbeitung Journey. 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-Eintragsquelle gesendet und auf alle Journeys übertragen, die Daten aus diesen Eintragsquellen verwenden.

Weitere Informationen zur Integration von Unica Campaign und Unica Interact mit Unica Journey finden Sie in den in der folgenden Dokumentationszuordnung erwähnten Anleitungen.

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.

Sie müssen Änderungen an der Konfigurationsplattform und an Benutzerrollen und Berechtigungen vornehmen:

- Die unter den Eingabequellen angezeigten Details des Campaign-Ablaufdiagramms stammen aus mehreren Partitionen.
- Basierend auf der Partition werden die Deliver-Vorlagen in E-Mail/SMS / WhatsApp-Touchpoints angezeigt.

Table 2. Integration von Unica Campaign mit anderen HCL-Produkten

Task	**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. Unica Discover sendet Daten zum Zielgruppenschwierigkeiten an Unica Journey. Die Zielgruppendaten werden über REST-Eintragsquelle gesendet und auf alle Journeys übertragen, die Daten aus diesen Eintragsquellen verwenden. Vier Scripts werden bereitgestellt, nach der Installation von Journey müssen Sie die Scripts sofort ausführen, dadurch werden zwei Eintragsquellen und zwei Datendefinitionen mit dem Namen Discover-Eintragsquelle für den Einkaufskorb und Discover-Eintragsquelle für Formular erstellt.

DD-Name	Einkaufskorb

Beschreibung	Wenn der Kunde einen Warenkorb oder eine Reihe ausgewählter Angebote verwirft, kann dieses Ereignis ausgelöst werden.

Table 3. Attribute, die gesendet werden sollen

Name	Typ	Länge	Hinweis
E-Mail*	TEXT	200	Es ist ein Pflichtfeld.
Name	TEXT	200	
DiscoverSessionId	TEXT	50	Sitzungs-ID erkennen, um sie wieder zu verbinden.
CartId	TEXT	50	Eindeutige ID zur Identifizierung des Einkaufskorbs.
CartValue	NUMBER		
EventDateTime	TIMESTAMP		Datum und Uhrzeit des Ereignisses in UTC-Längengrad
EventType	TEXT		Ereignistyp kann CART_ABANDONED sein
CookieID	TEXT	1024	
TLT_BROWSER	TEXT	50	Browserdetails
TLT_MODEL	TEXT	50	Einheitendetails
HTTP_ACCEPT_LANGUAGE	TEXT	50	Sprache

DD-Name	Formular
Beschreibung	Wenn der Kunde ein Webformular ausfüllt, kann dieses Ereignis veröffentlicht werden.

Table 4. Attribute, die gesendet werden sollen

Name	Typ	Länge	Hinweis
E-Mail*	TEXT	200	Es ist ein Pflichtfeld.
Name	TEXT	200	
DiscoverSessionId	TEXT	50	Sitzungs-ID erkennen, um sie wieder zu verbinden.

Table 4. Attribute, die gesendet werden sollen (continued)

Name	Typ	Länge	Hinweis
FormId	TEXT	50	Eindeutige ID zur Identifizierung von Formular
FormName	TEXT	100	
EventDateTime	TIMESTAMP		Datum und Uhrzeit des Ereignisses in UTC-Längengrad
CookieID	TEXT	1024	
TLT_BROWSER	TEXT	50	Browserdetails
TLT_MODEL	TEXT	50	Einheitendetails
HTTP_ACCEPT_LANGUAGE	TEXT	50	Sprache
EventType	TEXT		Ereignistyp kann FORM_SUBMITTED, FORM_ABANDONED sein

Note: Ab Fixpack 3 ist die Unica Journey Integration mit Unica Discover Feature verfügbar.

Eine Einführung in Unica Deliver

Unica Deliver ist eine webbasierte, unternehmensweite Marketingnachrichtenlösung, die Sie verwenden können, um ausgehende Massennachrichten und transaktionale Nachrichtenkampagnen durchzuführen. Deliver integriert sich mit Unica Campaign und mit sicheren Ressourcen für Nachrichtenerstellung, -übertragung und -verfolgung, die bei Unica gehostet werden.

Sie können Deliver verwenden, um personalisierte E-Mail-Kommunikation zu erstellen, zu senden und zu verfolgen. Da Deliver mit Campaign installiert und betrieben wird, können Sie Campaign-Ablaufdiagramme verwenden, um Empfängerinformationen exakt auszuwählen und zu segmentieren, um jede Nachricht 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 Deliver können Sie eine große Anzahl von E-Mail-Clients 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 Dokumentersteller von Deliver 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 mit externen Inhalten verknüpfen, wenn Deliver Nachrichten erstellt und überträgt. Deliver bietet verschiedene Möglichkeiten, Nachrichten zu entwerfen, die Inhalte bedingt auf Basis personenbezogener Daten für jeden Empfänger anzeigen.

Nachricht verschicken und Antworten verfolgen

Abhängig von Ihren Zielen können Sie planen, dass eine Nachrichtenkampagne so bald wie möglich oder zu einem späteren Zeitpunkt ausgeführt wird.Deliver überwacht die Nachrichtenzustellung 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 *Unica Deliver-Startup- und Administratorhandbuch*.

Unica Deliver integration

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

1. Navigieren Sie in Unica Platform zu **Einstellungen > Konfiguration**.
   Result
   Die Seite **Konfigurationskategorien** wird angezeigt.
2. Wählen Sie**Journey** aus.
   Result
   Die Seite **Einstellungen für 'Journey'** wird angezeigt.
3. Wählen Sie die Option **Einstellungen bearbeiten** aus.
   Result
   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.
   Result
   Die Seite **Einstellungen für die 'Deliver_Configurations'** wird angezeigt.
6. Wählen Sie die Option **Einstellungen bearbeiten** aus.

Result

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 für Deliver konfigurierte URL.

            Note:

            i. Der Benutzer muss die TMS-URL in der Journey Konfiguration aktualisieren. Aktualisieren Sie die TMS-URL, da die SOAP-TMS URL nicht unterstützt wird, sondern nur die REST-URL. Navigieren Sie zu **Platform > Einstellungen > Konfiguration > Journey > Deliver_URL**.

            ii. Fügen Sie die Kafka Informationen im folgenden Pfad hinzu:

            Platform Einstellungen > Konfiguration > Deliver > serverComponentsAndLocations > Kafka RCT.

        - **Deliver_Partition**: Die Partition, in der die Berechtigungsnachweise für den Zugriff auf die **Deliver_URL** gespeichert werden.
        - Wenn für die Journey ein Deliver-Touchpoint konfiguriert ist, muss der Benutzer die Journey anhalten und erneut veröffentlichen, erst dann beginnen die Zielgruppen mit der Verarbeitung

    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

Um auf Kafka_Configurations zuzugreifen, führen Sie die folgenden Schritte aus:

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.

Pflichtkonfigurationen basierend auf dem Wert von 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

Basierend auf Ihrer Auswahl werden die folgenden Felder verbindlich:

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.data Quelle			Ja	Ja
keystore.location			Ja	Ja
keystore.password.data Quelle			Ja	Ja
key.password.dataSource			Optional	Optional
ssl.endpoint.identification. 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

About this task

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. Journey Benutzerrollen und Berechtigungen

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

- Den Journey Rollen die Berechtigungen zuweisen on page 11
- Rolle JourneyAdmin einem Benutzer zuweisen on page 12
- JourneyUser Rolle einem Benutzer zuweisen on page 13

Note: Im Falle von jeglichen Konfigurationsänderungen, muss Unica Journey neu gestartet werden. Für weitere Informationen über Sicherheitskonfigurationen, siehe *Unica Platform Administratorhandbuch*.

Den Journey Rollen die Berechtigungen zuweisen

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

About this task

Journey bietet zwei Benutzerrollen:

- **JourneyVerwaltung**
- **JourneyBenutzer**

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

1. Auf der Unica PlatformStartseite, wählen Sie **Einstellungen > Benutzerrollen und Berechtigungen** aus.
   Result
   Sie werden zu der Seite **Benutzerrollen und Berechtigungen** navigiert.
2. Erweitern Sie im linken Bereich **Unica Journey > partition1**.
   Result
   Die Seite **partition1** wird angezeigt.
3. Wählen Sie **Berechtigungen zuweisen** aus.
   Result
   Die Seite **(Eigenschaften von Administrationsrollen)** wird angezeigt.
4. Klicken Sie auf **Berechtigungen speichern und bearbeiten**.
   Result
   Die Seite **(Berechtigungen für partition1)** wird angezeigt.
5. Erweitern Sie **Anwendung**.
6. Werte für die folgenden Felder festlegen:

Operationen	**JourneyAdmin Standardeinstellung**	**JourneyBenutzer Standardeinstellung**
Datendefinition erstellen	Ja	Nein

Operationen	JourneyAdmin Standardeinstellung	JourneyBenutzer Standardeinstellung
Datendefinition bearbeiten	Ja	Nein
Datendefinition löschen	Ja	Nein
Eingabequellen erstellen	Ja	Nein
Eingabequellen bearbeiten	Ja	Nein
Eingabequellen löschen	Ja	Nein
Erstellen Journey	Ja	Ja
Bearbeiten Journey	Ja	Ja
Löschen Journey	Ja	Nein
Veröffentlichen Journey	Ja	Ja
Beendet Journey	Ja	Ja
Anhalten Journey	Ja	Ja
Ziel hinzufügen/ändern/löschen	Ja	Nein
Zielansicht	Ja	Ja
Einstellungen hinzufügen/ändern/löschen	Ja	Nein
Ansicht - Einstellungen	Ja	Ja

Note:

- Für die Rolle **JourneyAdmin** empfehlen wir Ihnen, die Berechtigungen nicht zu reduzieren und die Standardberechtigungen beizubehalten. Standardmäßig verfügt **JourneyAdmin** über alle Berechtigungen.
- Geben Sie für die Rolle **JourneyUser** die Berechtigungen an, die Sie für geeignet halten. Sie können dem **JourneyUser** 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**.
   Result
   Sie werden zu der Seite **Benutzerrollen und Berechtigungen** navigiert.
2. Erweitern Sie in dem linken Bereich **UnicaJourney**.

3. Wählen Sie **partition1 > JourneyAdmin** aus.
   Result
   Die Seite **JourneyAdmin** wird angezeigt.
4. Wählen Sie im Abschnitt **Benutzer** einen Benutzer aus. Zum Beispiel `asm_admin`.
   Result
   Sie werden zur Seite **asm_admin (asm_admin)** mit Benutzerdetails navigiert.
5. Wählen Sie **Rollen bearbeiten** aus.
   Result
   Sie werden zur Seite **Rollen bearbeiten** navigiert.
6. Wählen Sie in der Liste **Verfügbare Rollen** die Option **Journey Admin(Unica Journey)** 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**.
   Result
   Sie werden zu der Seite **Benutzerrollen und Berechtigungen** navigiert.
2. Erweitern Sie in dem linken Bereich **UnicaJourney**.
3. Wählen Sie **partition1 > JourneyUser** aus.
   Result
   Die Seite **JourneyUser** wird angezeigt.
4. Wählen Sie im Abschnitt **Benutzer** einen Benutzer aus. Beispiel: `journey_example`.
   Result
   Die Benutzerdetailseite **journey_example (journey_example)** wird angezeigt.
5. Wählen Sie **Rollen bearbeiten** aus.
   Result
   Sie werden zur Seite **Rollen bearbeiten** navigiert.
6. Wählen Sie in der Liste **Verfügbare Rollen** die Option **Journey User (Unica Journey)** und klicken Sie auf die Schaltfläche **>>**, um die Rolle in die Liste **Ausgewählte Rollen** zu verschieben.
7. Klicken Sie auf **Änderungen speichern**.

Dem Benutzer eine ContactCentralAdmin Rolle zuweisen

Der Unica Journey Administrator muss Journey Benutzern die Rolle ContactCentralAdmin zuweisen, damit sie auf Contact Central zugreifen können. Um Contact Central für Journey zu aktivieren, sollte der Wert von Contact_Central_Configured aus Platform auf „Ja“ gesetzt werden. Standardmäßig wird der Wert auf Nein eingestellt. Der Benutzer kann den gewünschten Wert Ja/Nein für Contact_Central_Configured aus dem Pfad Affinium|Journey in Platform auswählen. Für weitere Informationen, siehe *Unica Contact Central Administrationshandbuch*.

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` für beide Journey Web und Journey Engine, wird im Ordner `conf` am Installationsort 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 GDPR

Zugriff auf Journey DSGVO

Das DSGVO Tool kann über den Journey Anwendungsordner zugegriffen werden. Die Position ist wie folgt:

```
<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.DBType`	`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 Eingabedatei CSV.
`Journey.audience.Csv`	`<GDPR_HOME>/sample/JourneyAudiences.csv`	Ersetzen Sie `<GDPR_HOME>` durch den aktuellen Verzeichnispfad. Dies ist die Eingabedatei `csv` mit Datensätzen, die Sie aus Journey deaktivieren müssen.
`Journey.audience.Output`	`<GDPR_HOME>/JourneyAudiences.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 ist in MB. Sollte die Dateigröße den eingegebenen Wert überschreiten, werden mehrere Dateien mit den folgenden Zusätzen generiert: `Jour-`

Eigenschaftsname	Beispielwert	Hinweise
		neyAudiences_0, Journey-Audiences_1 usw.

2. **Note:** Wenn Fehler auftreten, können Sie ihn mit dieser Protokolldatei verfolgen.
3. Gehen Sie wie folgt vor, 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, um die Datensätze aus der Tabelle "journeyaudiences" löschen zu lassen.

Das Dienstprogramm DSGVO entfernt die Datensätze aus der folgenden Tabelle: JourneyAudiences, AudienceResponse, AudienceResponseMetaData, AudienceResponseInteraction, JourneyAudienceMilestone and JourneyAudienceGoal. Die Daten aus den entsprechenden Tabellen, in denen aggregierte Zählerstände gespeichert werden, werden jedoch nicht gelöscht. Beispielsweise 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 dem DSGVO-Tool kann der Benutzer keine Kundendaten löschen, die vom JDBC-Connector exportiert wurden.

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.
   - Gültigkeit: Die Gültigkeitsdauer 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
```

Konfiguration von Kafka Server, die Komponenten von Journey und Link mit SSL

Die Serverzertifikate, die für Kafka Server und Clientzertifikate verwendet werden sollen, müssen von allen Anwendungen verwendet werden, die sich mit dem KafkaServer 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
```

Konfiguration von Journey Engine mit Kafka SSL

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 Datei Journey Engine `log4j2.xml` aus dem Verzeichnis `<JOURNEY_HOME>/Engine/conf/`. Entfernen Sie die Kommentare für die folgenden Zeilen in `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 die Datei `journey_engine_master.config` aus dem 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=
```

Konfiguration von Journey web mit Kafka SSL

1. Aktualisieren Sie die Datei Journey Web `application.properties` aus dem Verzeichnis `<JOURNEY_HOME>/Web/properties/`.
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=
```

Konfiguration von Unica Link Komponenten mit SSL

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

```
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=
```

Konfiguration von Kafka Server, Journey und Link Komponenten mit SASL

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

Konfigurieren des Kafka Servers mit SASL-Authentifizierung

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

   Setzen Sie `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 des KafkaServers 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
   ```

Konfiguration von Journey Engine mit Kafka SASL

1. Aktualisieren Sie die Datei Journey Engine `log4j2.xml` aus dem Verzeichnis `<JOURNEY_HOME>/Engine/conf/`. Entfernen Sie die Kommentare für die folgenden Zeilen in `log4j2.xml`.

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

2. Aktualisieren Sie die Datei `journey_engine_master.config` aus dem 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
   ```

Konfiguration von Journey Web mit Kafka SASL

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

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

Konfiguration von Unica Link Komponenten mit Kafka SASL

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

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

Konfiguration von Kafka Server und Journey Komponenten mit SASL_SSL Konfiguration

Zur Konfiguration von Kafka Server und anderen Journey-Komponenten mit SASL-Authentifizierung müssen Sie die in den folgenden Abschnitten bereitgestellten Prozeduren ausführen.

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
```

Konfiguration von Journey Engine mit Kafka SASL_SSL

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

   Entfernen Sie die Kommentare für die folgenden Zeilen in `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}</Prope
   rty>
   ```

2. Aktualisieren Sie die folgende `journey_engine_master.config` aus dem 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
   ```

Konfiguration von Journey Web mit Kafka SASL_SSL

Aktualisieren Sie die folgende Datei Journey Web `application.properties` aus dem Verzeichnis `<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 8. Tomcat-Webanwendungsserver für SSL konfigurieren

Konfigurieren Sie auf jedem Anwendungsserver, auf dem eine UnicaAnwendung 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.

About this task

```
<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>
```

Konfiguration von Unica Journey mit SSL

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

About this task

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.

   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.
   - *`Domäne`* ist Ihre Unternehmensdomäne, in der IhreUnica Produkte installiert sind
   - *`SSL_Port`* ist der SSL-Port im Anwendungsserver, auf dem Unica Journey bereitgestellt wurde

   Beachten Sie das `https` in der URL.

Chapter 9. Mailchimp Konfiguration

Konfiguration von Mailchimp als externe Quelle mit Journey.

About this task

Navigieren Sie zur **Unica Platform > Einstellungen > Konfiguration**

Auf der Seite Konfigurationskategorien, navigieren Sie zu **Journey > Integration > dataSources**.

Um eine Journey-Datenquelle hinzufügen

1. Klicken Sie auf **Systemkonfigurationsvorlagen**
   Result
   Die Seite **Systemkonfigurationsvorlagen** wird angezeigt.
2. Geben Sie die folgenden Informationen an:
   - **Neuer Kategoriename**: <Journey>
   - **systemIdentifier**: Journey
   - **userCredentials**: Standardbenutzer
   - **defaultUserCredentials**: asm_Admin
   - **dataSourceNameForCredentials**: <JOURNEY_DS_1>
   - **AdditionalParameters**:
   - **event-publisher-service.kafka.topics**: CIFINTEGRATION
   - **event-publisher-service.kafka.topics.CIFINTEGRATION.value.format**: Json
3. Klicken Sie auf **Speichern**.
4. Klappen Sie den Journey-Knoten aus und klicken Sie auf **httpGateway**
   Result
   Die Seite **Einstellungen für „httpGateway“** wird angezeigt.
5. Geben Sie die folgenden Informationen an:

   baseUrl : http:<hostname>:<port>/journey
6. Klicken Sie auf den Link **Kafka Konfiguration** und fügen Sie die folgenden Informationen hinzu

   Bootstrap Server (durch Kommas getrennte Liste von Hosts): <Kafkahost>:<port>

   z.B. <IP ODER Hostname>:9092

Um eine Mailchimp Datenquelle hinzufügen

1. Klicken Sie auf **Systemkonfigurationsvorlagen**
   Result
   Die Seite **Systemkonfigurationsvorlagen** wird angezeigt.
2. Geben Sie die folgenden Informationen an:
   - **Neuer Kategoriename**: <Mailchimp>
   - **systemIdentifier** : Mailchimp
   - **userCredentials**: Standardbenutzer

- **defaultUserCredentials**: asm_Admin
- **dataSourceNameForCredentials** : <Mailchimp_DS>

3. Klicken Sie auf **Speichern**.
4. Klappen Sie den Mailchimp-Knoten aus und klicken Sie auf **httpGateway**

   Result

   Die Seite **Einstellungen für „httpGateway“** wird angezeigt.
5. Geben Sie die folgenden Informationen an:
   baseUrl : https://<MailchimpHostname>/<Version>/

   Der Benutzer muss diese Datenquellen in Journey hinzufügen. Der Benutzer muss folgende Informationen sammeln:

   a. Benutzer-ID und Passwort der Journey-Datenquelle. Navigieren Sie zu den **Journey Anwendung > Einstellungen > Rest**, erstellen Sie entweder eine neue Rest-Integration oder verwenden Sie eine vorhandene Rest-Integration. Kopieren Sie clientid und Client Secret.
   b. Benutzer-ID und Passwort der Mailchimp-Datenquelle. Melden Sie sich bei der Mailchimp-Anwendung an und navigieren Sie zu **Profil > Zusätzliche > API-Schlüssel**. Holen Sie sich die API-Schlüssel und der Name der Spalte Benutzer lautet "Benutzer".

      In Mailchimp a/c die URL **Webhook hinzufügen** URL wie folgt:
https://<AssetpickerHostname>:<Port>/asset-viewer/api/AssetPicker/webhook/Mailchimp/events/webhook_listener

   Navigieren Sie zu **Platform Einstellungen > Benutzer**

   Klicken Sie auf **Benötigter Benutzer** z.B. asm_Admin

   Klicken Sie auf den Link **Datenquellen bearbeiten** und fügen Sie die folgenden Datenquellen hinzu

   Mailchimp_DS - Benutzer: <user> und Passwort <API key>

   JOURNEY_DS_1 - Benutzer: <clientid> und Passwort <Client Secret>

   Navigieren Sie zu Unica Platform > Einstellungen > Konfiguration > Unica Platform > Sicherheit > API Management > Unica Content Integration

   Klicken Sie auf **API Konfigurationsvorlage** und fügen Sie die folgenden Informationen hinzu
   - **Neuer Kategoriename**: <Mailchimp>
   - **API URI** : /webhook/Mailchimp/events/*
   - **Authentifizierung für API-Zugriff erforderlich** – nicht ausgewählt

   Klicken Sie auf **Speichern**

   Nachdem Sie diese Schritte ausgeführt haben, wird Mailchimp als externe Quelle in Journey hinzugefügt.

   Note:

   Wenn der Benutzer die externe Quelle in Journey konfiguriert, muss die folgende Eigenschaft auf False gesetzt werden. Dies ermöglicht es, die Daten aus einer externen Quelle zu erhalten, die in den Einstellungen für die Daten-Nicht-duplizierung von Journey als signifikantes Feld konfiguriert ist

<rule-enabled>false</rule-enabled>

\<JourneyEngine>\conf\data-validation-rules.xml

Note: Zur Konfiguration der externen Quelle muss der Benutzer die Unica Asset Picker Komponente bei der Installation/Upgrade von Unica Platform als Voraussetzung installieren.

Chapter 10. 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.

About this task

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

1. Wählen Sie  **> Link > E-Mail** aus.
   Result
   Die **E-Mail** Seite wird angezeigt.
2. Aus der Liste **Verfügbare Verbindungen**, wählen Sie 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.

About this task

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

1. Wählen Sie  **> Link > SMS** aus.
   Result
   Die Seite **SMS** wird angezeigt.
2. Aus der Liste **Verfügbare Verbindungen**, wählen Sie 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:

- *<Pluszeichen><Landesvorwahl><10-stellige Telefonnummer>* - `+15403241212` .
- *<Pluszeichen> <Landesvorwahl <(Ortsvorwahl)> <dreistellige Zahl><vierstellige Zahl>* - `+1 (540) 324 1212` .
- *<Pluszeichen>-<Landesvorwahl>-<Ortsvorwahl>-<dreistellige Nummer>-<vierstellige Nummer>* - `+1-540-324-1212` .
- *<Pluszeichen> <Landesvorwahl>-<Ortsvorwahl>-<dreistellige Nummer>-<vierstellige Nummer>* - `+1 540-324-1212` .

Unabhängig vom Format der Telefonnummer, die Sie angeben, speichert Unica Journey die Nummer in folgendem Format: *<Pluszeichen><Landesvorwahl><10-stellige Telefonnummer>*. Wenn Sie beispielsweise die Telefonnummer `+1 540-324-1212` angeben, speichert Unica Journey die Telefonnummer als `+15403241212`.

Wenn Sie Twilio als Standard-SMS-Verbindung auswählen, werden nur Telefonnummern in folgendem Format akzeptiert: *<Pluszeichen><Ländercode><10-stellige Telefonnummer>*. z.B. `+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.

About this task

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

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

Standard ADTECH-Verbindung einrichten

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

About this task

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

1. Wählen Sie  **> Link > ADTECH** aus
   Result
   Die Seite **ADTECH** wird angezeigt

2. Aus der Liste **Verfügbare Verbindungen**, wählen Sie eine Verbindung aus.
3. Klicken Sie auf **Speichern**.

Standard Datenbankverbindung einrichten

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

About this task

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

1. Wählen Sie  **> Link > Datenbank** aus

   Result

   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.

About this task

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 beträgt.

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

   a. Wählen Sie  **> Link > Verbindungen verwalten > Neu erstellen** aus.

   Result

   Die Seite **Neue Verbindung erstellen** wird angezeigt.

   b. Geben Sie Werte für die folgenden Felder ein:
      - **Name** - Pflichtfeld
      - **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**.
Result
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 > Neu erstellen** aus.
Result
Die Seite **Neue Verbindung erstellen** wird angezeigt.

b. Geben Sie Werte für die folgenden Felder ein:
- **Name** - Pflichtfeld
- **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**.
Result
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 > Neu erstellen** aus.
Result
Die Seite **Neue Verbindung erstellen** wird angezeigt.

b. Geben Sie Werte für die folgenden Felder ein:
- **Name** - Pflichtfeld
- **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**.
Result
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 > Neu erstellen** aus.
Result
Die Seite **Neue Verbindung erstellen** wird angezeigt.

b. Geben Sie Werte für die folgenden Felder ein:

- **Name** - Pflichtfeld
- **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**
- **Konto SID**
- **Auth Token**
- **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**.
Result
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. Wählen Sie  **> REST** aus.
Result
Die Seite **REST** wird angezeigt.
2. Klicken Sie auf **+ REST Integration**.
Result
Die Seite **Neue REST-Integration** wird angezeigt.

3. Geben Sie Werte für die folgenden Felder ein:
    - **Anwendungsname** - Pflichtfeld.
    - **Beschreibung** - Optional.
4. Klicken Sie auf **Schlüssel generieren**.

   Result

   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.

About this task

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

1. Wählen Sie  **> REST** aus.

   Result

   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.

About this task

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

1. Wählen Sie  **> REST** aus.

   Result

   Die Seite **REST** wird angezeigt.
2. Zur Änderung einer REST-Integration können Sie entweder:

   Choose from:

- die gewünschte REST-Integration aus der Liste auswählen
- Auswählen > 

Result

Die Seite **REST-Integration aktualisieren** wird angezeigt.

3. Sie können nur die folgenden Felder aktualisieren:

   Choose from:

   - **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.

Before you begin

Informationen zum Ändern des Status eines REST-Integrationseintrags finden Sie unter Vorhandene REST-Integration ändern on page 34.

About this task

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

1. Wählen Sie  **> REST** aus.

   Result

   Die Seite **REST** wird angezeigt.

2. Führen Sie einen der folgenden Schritte aus:

   Choose from:

   - 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.

Einstellungen des Journey Engine-Verbindungspools

- journey.datasource.maxpool.size=[MAX_POOL_SIZE] – Größe des DB-Verbindungspools festlegen
- journey.datasource.minIdle.size=[MIN_IDLE_SIZE] – legt die Größe der minimalen Leerlaufverbindungen fest

Entwicklertools

Zeigt die Liste der Entwicklertools an.

API-Dokumentation

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