Unica Deliver V12.1.2 Startup und Administratorhandbuch

Contents

Chapitre 1. Messagerie hébergée à l'aide d'Unica Campaign et d'Unica Deliver

Lorsqu'Unica Campaign est intégré à Unica Deliver, vous pouvez utiliser Deliver pour mener des campagnes personnalisées de marketing numérique.

Remarque : Deliver prend en charge les canaux suivants, ainsi que les e-mails. Dans ce guide, le terme message s'applique à tous les canaux.

- SMS
- WhatsApp
- Push

Deliver vous donne accès à des ressources hébergées par Unica et vous permet de concevoir, envoyer et surveiller des messages personnalisés individuellement, qui sont basés sur les informations stockées dans votre magasin de données client.

- Dans Campaign, utilisez des diagrammes pour créer des listes de destinataires de message et sélectionner des données de personnalisation pour chaque destinataire.
- Dans Deliver, utilisez les ressources de conception, de transmission et de délivrabilité de message hébergées par HCL pour mener des campagnes de marketing numérique.

Einrichtung eines gehosteten Kontos mit Unica

Wenn Sie ein Nachrichten-Abonnement erwerben, wird in Ihrem Namen ein gehostetes Konto von Unica erstellt und Ihnen die Konto-Anmeldedaten gesendet, die Sie für die Verwendung von Nachrichtenfunktionen benötigen. Diese Berechtigungsnachweise werden bei der Konfiguration Ihrer lokalen HCL Unica Anwendungen für den Zugriff auf die gehostete E-Mail-Kommunikation über sichere Verbindungen verwendet.

Sie müssen über ein gültiges Konto verfügen, um auf die Nachrichtenressourcen zugreifen zu können, die Unica als Software-Service zur Verfügung stellt. Wenn Ihre HCL Unica Installation mehrere Partitionen umfasst und Sie Nachrichten in mehr als einer

Partition verwenden möchten, benötigen Sie ein gehostetes Konto und mindestens einen Dienstanbieter für SMS, Push und Whatsapp, je nachdem, welche Dienste Sie für jede Partition benötigen. Sie können keine Konten über Installationen oder Partitionen gemeinsam nutzen.

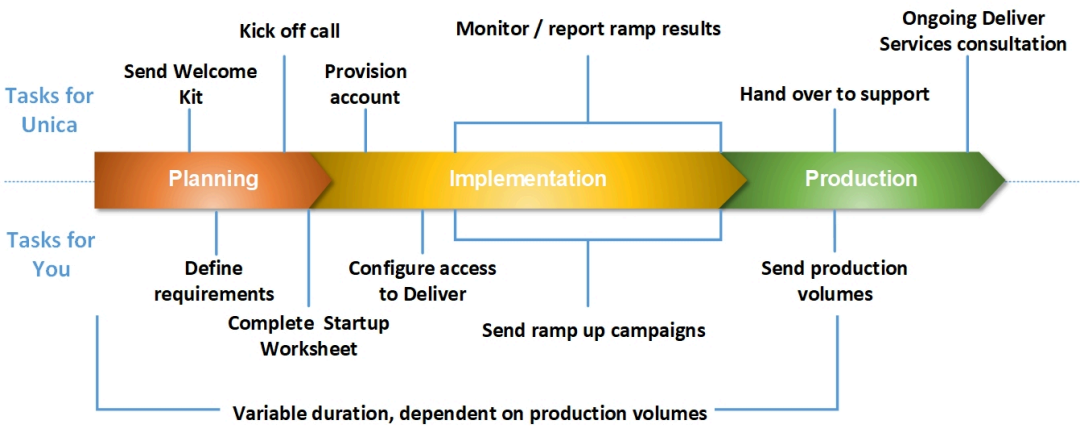
Die Einrichtung eines gehosteten Kontos ist der Anfang des Startprozesses, der etwa 90 Tage dauert. Sie können SMS, Push und Whatsapp abonnieren, je nachdem, welche Dienste Sie gemäß den Anforderungen benötigen. Eine allgemeine Beschreibung des Prozesses finden Sie im nächsten Thema.

Gesamtübersicht über den Startprozess

Sie können Nachrichtenfunktionen in Unica Campaign aktivieren, um zielgerichtete und nachverfolgbare digitale Marketingkampagnen durchzuführen. Campaign verwendet Nachrichtenfunktionen, die von Unica Deliver über Ressourcen bereitgestellt werden, die in Rechenzentren in den USA, Indien und in Europa gehostet werden. Ein Konto für den Zugriff auf diese E-Mail-Ressourcen ist in Ihrem Deliver Abonnement enthalten. Sie können sich je nach den Anforderungen auch für die WhatsApp-, Push- oder SMS-Kanäle entscheiden.

Unica startet den Startvorgang, nachdem Ihr gehostetes E-Mail-Konto erstellt wurde. Mit Unica können Sie sich mit Deliver vertraut machen, eine Verbindung zu gehosteten Nachrichtenressourcen herstellen und Ihren Ruf als legitimer Digital-Vermarkter unter führenden Internetdienstanbietern (ISPs) etablieren.

Der Prozess verläuft in drei Phasen. Die Unica Teams von Professional Services und Deliver Services führen Sie auf dem Weg durch.



Der Professional Services Consultant ist Ihr primärer Ansprechpartner beim Unica-Startprozess. Wenn der Kontenstartprozess abgeschlossen ist, überträgt der Professional Services Consultant die primäre Unterstützungsverantwortung an das Unica Produktunterstützungsteam.

Ein dedizierter Service für die Bereitstellung von Dienstleistungen bietet spezielle Unterstützung für Probleme mit der Nachrichten. Die Schaffung einer günstigen Wahrnehmung Ihrer Nachrichten bei den großen Internet Service Providern (ISPs) ist entscheidend dafür, dass Ihre digitalen Marketing-Kampagnen ihre Ziel-Empfänger konsequent erreichen. Wenn Sie mit der Ausführung von Mailings beginnen, überprüft der EAS-Berater die Zustellbarkeitsleistung des Mailings und schlägt die besten Möglichkeiten vor, um Ihren Ruf als Versender schrittweise aufzubauen.

Activités de démarrage et jalons

Planification

Liste des activités de planification

Résultat	Qui est responsable
Envoyer les données d'identification du compte de messagerie et le kit de bienvenue, y compris la feuille de calcul de démarrage de la messagerie.	Unica Services Deliver

Résultat	Qui est responsable
Planifier une conférence téléphonique afin d'introduire toutes les parties impliquées, vérifier le planning de démarrage et découvrir les objectifs de marketing par courrier électronique.	Unica Services professionnels
Compléter la feuille de calcul de démarrage de messagerie pour spécifier vos exigences de domaine de messagerie et vos projections de mailing.	Votre organisation

Créer votre réputation de messagerie

Actions requises pour établir une réputation de messagerie favorable

Résultat	Qui est responsable
Mettre à disposition le compte de messagerie à l'aide des informations fournies lors de la conférence téléphonique et dans la feuille de calcul de démarrage de messagerie.	Unica opérations de courrier électronique
Lancer des mailings préliminaires pour sélectionner des comptes de test avec les principaux FAI. Cette phase nécessite environ 30 jours.	Unica opérations de courrier électronique
Activer Deliver dans Unica Campaign.	Votre organisation (avec prise en charge de Unica)
Configurer l'accès aux ressources de messagerie hébergées. Consulter le consultant EAS pour déterminer le centre de données à spécifier.	Votre organisation (avec prise en charge de Unica)
Commencer à envoyer des mailings. Pour créer une réputation de messagerie favorable, commencez par envoyer de petits mailings, suivis, au fil du temps, par des mailings plus volumineux et plus fréquents. Les FAI essaient souvent de limiter le spam en bloquant les mailings volumi-	Votre organisation (avec prise en charge de Unica)

Résultat	Qui est responsable
neux ou fréquents des domaines de messagerie qu'ils ne reconnaissent pas légitimement.	
Fournir des résultats de délivrabilité et des conseils de réputation au fur et à mesure de l'augmentation progressive des volumes et de la fréquence de mailing.	Unica Services Deliver

Production

Activités requises pour atteindre et maintenir les volumes de production souhaités

Résultat	Qui est responsable
Envoyer des mailings à un volume et une fréquence typiques.	Votre organisation
Transférer la responsabilité du contact principal à l'équipe de support Unica.	Unica Services professionnels
Mettre à jour l'engagement pour la consultation des problèmes de messagerie. Prendre contact régulièrement pour un support de compte de messagerie continu.	Unica Services Deliver

Avant de commencer à utiliser Deliver

Avant de commencer le processus de démarrage de la messagerie, tenez compte des points suivants.

- Certaines configurations nécessitent le redémarrage du serveur d'application Web. Planifiez l'activité de configuration Deliver pour éviter toute interférence avec les exécutions de diagrammes volumineuses et d'autres activités dans Campaign.
- Unica vous invite à nommer une personne qui fera office de point de contact principal lors du processus de démarrage.

- Demandez les données d’identification du compte de messagerie hébergé avant de commencer le processus de démarrage. Vous utilisez ces données d’identification pour configurer vos systèmes afin d’accéder au compte.
- Consultez votre équipe d’administration réseau. Deliver requiert des plages de ports spécifiques lors de la communication avec HCL Unica.
- Vérifiez que vous disposez des droits réseau appropriés pour apporter des modifications à la configuration.

Chapitre 2. Configuration de l’environnement local HCL Unica pour Deliver

L'utilisation de Deliver pour envoyer des messages nécessite des modifications dans l'installation locale de HCL Unica. Suivez les étapes décrites dans les sections suivantes.

Si votre environnement contient plusieurs partitions, répétez ces étapes pour chaque partition Campaign dans laquelle vous utilisez Unica Deliver. Pour plus d'informations sur la configuration et l'utilisation de plusieurs partitions, voir le document Unica Campaign - Guide d'installation.

Confirmation de l'enregistrement de Deliver

Unica Deliver doit être enregistré auprès de Unica Platform. Pour confirmer que Deliver est enregistré correctement, vous devez examiner la configuration de Platform.

1. Connectez-vous à HCL Unica.
2. Accédez à **Paramètres** > **Configuration**.
3. Recherchez la catégorie de configuration Deliver.

   Unica Deliver est enregistré auprès de Platform lorsque la catégorie Deliver apparaît dans la hiérarchie des propriétés de configuration.

Si la catégorie Deliver n’apparaît pas dans la hiérarchie des propriétés, consultez le document Unica Campaign - Guide d’installation pour plus d’informations sur l’enregistrement manuel de Deliver.

Si la catégorie Deliver est disponible, vous devez activer les fonctions Deliver dans Campaign.

Enregistrement manuel de Deliver

Si le programme d'installation d'Deliver ne peut pas accéder aux tables système Platform pendant l'installation, vous devez exécuter l'utilitaire configTool pour l'enregistrer manuellement.

Par défaut, le programme d'installation de Campaign enregistre automatiquement Deliver avec les tables système Platform sans activer Deliver. Dans certains cas, le programme d'installation de Campaign ne se connecte pas avec les tables système Platform pour enregistrer automatiquement Deliver.

Si le programme d'installation n'enregistre pas automatiquement Deliver, vous devez enregistrer manuellement Deliver à l'aide de l'utilitaire `configTool` qui est fourni avec l'installation HCL Unica. L'utilitaire `configTool` se trouve dans le répertoire `tools\bin` de votre installation Platform.

Pour enregistrer Deliver manuellement, utilisez la commande suivante pour exécuter l'utilitaire `configTool` :

configTool -r Deliver -f "***full_path_to_Deliver_installation_directory*\conf\Deliver_configuration.xml"**

Le répertoire d'installation d'Deliver est un sous-répertoire du répertoire d'installation de Campaign.

Activer les fonctions Deliver dans Campaign

Lorsque vous installez Campaign, le programme d'installation installe également Deliver dans la partition par défaut, mais ne l'active pas. Les fonctions Deliver ne sont pas disponibles tant que vous n'avez pas activé Deliver.

Vous activez Deliver avec la propriété de configuration suivante dans Unica Platform.

`Campaign > partitions > partition[n] > server > internal > deliverInstalled`

Pour activer Deliver, remplacez la valeur par `oui`.

Exigence d'enregistrement

L'enregistrement de Deliver auprès de Unica Platform est nécessaire pour faire fonctionner Deliver. Vous enregistrez Deliver auprès de Platform lors de l'installation de Unica Campaign.

Une fois que vous avez activé Deliver, vérifiez que Deliver est correctement enregistré auprès de Unica Platform. Pour plus d'informations, voir Confirmation de l'enregistrement de Deliver (à la page 7).

Affichage des options du menu Deliver

Pour utiliser Unica Deliver, vous devez mettre à jour la configuration du système de sorte que les options de menu pour Deliver s'affichent dans l'interface Unica Platform. Lorsque vous installez Campaign, le programme d'installation installe également les menus Deliver dans la partition par défaut. Dans le cas où le programme d'installation de Campaign ne se connecte pas aux tables système de Platform, vous devez les configurer manuellement à l'aide de la procédure ci-dessous. Pour afficher les options requises, utilisez l'utilitaire `configTool` fourni avec votre installation HCL Unica.

Vous devez exécuter `configTool` avec des paramètres spécifiques pour chaque option de menu Deliver. L'exécution de `configTool` met à jour les paramètres de configuration du système. Vous devez relancer manuellement le serveur d'applications Web pour appliquer les modifications. Bien que Deliver soit installé avec Campaign, les options de menu de Deliver ne s'affichent pas avant l'exécution de `configTool` et le redémarrage du serveur d'applications Web. Dans le répertoire `tools` de l'installation Platform, l'utilitaire `configTool` est situé dans le dossier `bin`.

Remarque : Vous devez spécifier un chemin d'accès au répertoire d'installation Deliver en tant que paramètre `configTool`. Le répertoire d'installation d'Deliver est un sous-répertoire du répertoire d'installation de Campaign.

- Pour afficher les **Deliver Paramètres** dans le menu **Paramètres**.

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|
settingsMenu" -f "full_path_to_Deliver_installation_directory\conf
\deliver_op_odsettings_navigation.xml"
```

- Pour afficher les **Deliver Mailings** dans le menu **Campaign**.

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|
Campaign" -f "full_path_to_Deliver_installation_directory\conf
\deliver_op_mailings_navigation.xml"
```

- Pour afficher **Quick Builder** dans le menu **Campaign**.

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|
Campaign" -f "full_path_to_Deliver_installation_directory\conf
\deliver_op_new_documents_navigation.xml"
```

- Pour afficher les **Deliver Documents** dans le menu **Campaign**.

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|
Campaign" -f "full_path_to_Deliver_installation_directory\conf
\deliver_op_documents_navigation.xml"
```

- Pour afficher **Deliver Analytics** dans le menu **Analyse**.

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|
Analytics" -f "full_path_to_Deliver_installation_directory\conf
\deliver_op_analytics_navigation.xml"
```

Pour vérifier que vous avez correctement ajouté les options de menu, après avoir redémarré le serveur d'applications Web, connectez-vous à HCL Unica et ouvrez les menus **Paramètres**, **Campaign**et **Analytics** pour vérifier que les options Deliver s'affichent.

Spécification des caractéristiques des tables système Deliver

Unica Deliver requiert des informations qui décrivent le type, le schéma et la connexion JDBC pour les tables système Deliver de votre installation. Les tables système Deliver sont créées dans le schéma Campaign dans le cadre du processus d'installation Campaign.

- Accédez à **Paramètres > Configuration > Deliver > Partitions > Partition[n] > Sources de données > Tables système**.
- Consultez et mettez à jour les informations pour les paramètres suivants.

Remarque : Les informations de la table système Campaign sont prévues ici.

Type de base de données

Nom du schéma

jdbcBatchSize

jdbcClassName

jdbcURI

asmDataSourceForDBCredentials - doit être UA_SYSTEM_TABLES

- Fournissez les informations requises dans les propriétés de configuration suivantes. Consultez l'aide en ligne de Platform pour chaque propriété pour en savoir plus sur la définition des propriétés de configuration.
  - `Deliver > partitions > partition [n] < dataSources > systemTables > type`
  - `Deliver > partitions > partition [n] < dataSources > systemTables > schemaName`
  - `Deliver > partitions > partition [n] < dataSources > systemTables > jdbcBatchSize`
  - `Deliver > partitions > partition [n] < dataSources > systemTables > jdbcClassName`
  - `Deliver > partitions > partition [n] < dataSources > systemTables > jdbcURI`

Pour plus d'informations sur ces propriétés de configuration et sur la configuration de Deliver, voir Configurations pour Unica Deliver (à la page 54).

Configuration de l'accès aux tables système Deliver locales

Unica Deliver requiert l'accès aux tables système Deliver du schéma Campaign. Pour permettre aux composants Unica Deliver d'accéder aux tables système du schéma Campaign sans demander de connexion manuelle à la base de données, vous devez spécifier un utilisateur système Deliver pour fournir les données d'identification nécessaires pour l'accès à la base de données.

L'utilisateur système qui accède à la base de données est associé à une source de données Unica Platform qui contient les données d'identification de connexion de la base de données qui héberge le schéma Campaign.

Pour plus d'informations sur les propriétés de configuration de table système, voir Deliver | partitions | partition[n] | dataSources | systemTables (à la page 76).

1. Indiquez l'utilisateur système que vous avez défini dans Unica Platform. Modifiez la propriété de configuration suivante.

   `Deliver > partitions > partition [n] < dataSources > systemTables > asmUserForDBCredentials`
2. Spécifiez les données d'identification de connexion à la base de données qui contient le schéma Campaign et les tables système Deliver. Modifiez la propriété de configuration suivante.

   `Deliver > partitions > partition [n] < dataSources > systemTables > amDataSourceForDBCredentials`

Mappage requis pour les tables système Deliver dans Campaign

Vous devez mapper les tables système Deliver du schémaCampaign aux tables de base de données Deliver correspondantes. Les tables système Deliver ont **Deliver** dans leur nom de table.

Dans Campaign, mappez les tables système Deliver suivantes.

- Deliver Table de liste des cibles
- Deliver Table de mappage des zones d'audience des listes cible
- Deliver Table de mailing
- Deliver Table d'instance de mailing
- Deliver Table de mappage de colonnes de table de données
- Deliver Table de mappage de zones de personnalisation
- Deliver Table d'utilisation des zones de personnalisation

Pour plus d'informations sur les tables de mappage, voir le document Unica Campaign - Guide d'administration.

Redémarrage requis du serveur d'applications Web pour Campaign

Après avoir apporté des modifications aux configurations Campaign et Deliver, vous devez redémarrer le serveur d'applications Web qui héberge Campaign.

Consultez la documentation relative à votre serveur d'applications Web pour obtenir des instructions de démarrage.

Chapter 3. Verbindungen zu Nachrichtendiensten

Um auf Nachrichtendienste von Unica zuzugreifen, müssen Sie eine Verbindung zwischen der lokalen HCL Unica Installation und den HCL Unica gehosteten Diensten konfigurieren.

Marketer greifen über die Deliver-Oberfläche auf Campaign-Funktionen zu. Für die Arbeit mit Deliver müssen Sie eine sichere, automatische Internetverbindung herstellen, über die die Campaign Nachrichtenempfängerlisten nach HCL Unica gehosteten Diensten hochladen kann. Deliver Komponenten, die mit Campaign installiert wurden, verwenden diese Verbindung auch, um Kontakt- und Antwortdaten in die Deliver-Systemtabellen im Campaign-Schema herunterzuladen.

Note: Für jede Instanz von Campaign ist eine eindeutige Verbindung zu HCL Unica erforderlich. Wenn die Campaign Installation mehrere Partitionen umfasst, ist für jede Partition ein separates gehostete Konto erforderlich. Die Konten können die IP-Verbindung mit HCL Unica teilen.

Die gesamte Kommunikation zwischen HCL Unica und HCL Unica gehosteten Services erfolgt über SSL. Jede Kommunikation von HCL Unica gehosteten Services ist eine Antwort auf eine Anforderung aus der lokalen Umgebung. HCL Unica gehostete Services versuchen nie, eine Verbindung mit Ihrem Unternehmensnetzwerk zu initiieren. Die gesamte Kommunikation mit den HCL Unica gehosteten Services stammt von Ihrer Unternehmensfirewall.

Voraussetzungen für die Konfiguration der Verbindung zu HCL Unica gehosteten Services

Für die Konfiguration einer Verbindung zu HCL Unica gehosteten Services sind Administratorberechtigungen und Informationen zum gehosteten Konto für Ihr Unternehmen erforderlich.

Um eine gehostete E-Mail-Kommunikation zu konfigurieren, benötigen Sie Folgendes:

- Benutzername und Passwort von Unica für das gehostete Konto
- Berechtigungen zur Erstellung oder Änderung von Systembenutzern in der Unica Platform
- Administratorzugriff auf Konfigurationseigenschaften, die in der lokalen Unica Platform-Installation verwaltet werden
- Administratorzugriff auf den Webanwendungsserver, auf dem Unica Platform und Campaign bereitgestellt werden

Sie müssen Ihre Anforderungen an die Datensicherheit Ihres Unternehmens kennen oder in der Lage sein, sich mit Personen zu beraten, die diese kennen. Bevor Sie beginnen, lesen Sie diese Verfahren, um zu verstehen, wie Sie die erforderliche Verbindung gemäß den Firewall-Einschränkungen Ihres Unternehmens herstellen.

Sie müssen mit der Konfiguration vertrauenswürdiger Verbindungen auf Ihrem Webanwendungsserver, IBM WebSphere®, Oracle WebLogic, Apache Tomcat und JBOSS vertraut sein.

Konfiguration von Adressen für die Verbindung zu HCL Unica gehosteten Diensten

Um eine ordnungsgemäße Verbindung zu HCL Unica gehosteten Diensten zu gewährleisten müssen Sie die Adressen als Werte für die Konfigurationseigenschaften in die Deliver Konfiguration eingeben. Die eingegebenen Verbindungsadressen hängen davon ab, ob Sie eine Verbindung zum Unica-Rechenzentrum in den USA, Europa oder Indien herstellen.

Wenden Sie sich an Unica um zu bestätigen, welches Rechenzentrum von Ihrem gehosteten E-Mail Konto verwendet wird.

In Unica Platform, navigieren zu **Einstellungen > Konfiguration**. Unter der Deliver Konfiguration, navigieren Sie zu den folgenden Deliver Konfigurationseigenschaften und bestätigen oder aktualisieren Sie die Verbindungseinstellungen, je nachdem, welches Rechenzentrum Ihr Konto verwendet.

- `Deliver > serverComponentsAndLocations > hostedServices> uiHostName`

  Um eine Verbindung zum Unica Rechenzentrum in den USA herzustellen, ändern Sie diesen Wert in `em.unicadeliver.com`.

  Um eine Verbindung zum europäischen UnicaRechenzentrum herzustellen, ändern Sie diesen Wert in

  `em-eu.unicadeliver.com`.

  Um eine Verbindung zu dem Unica Rechenzentrum in Indien herzustellen, ändern Sie diesen Wert in

  `em-in.unicadeliver.com`
- `Deliver > serverComponentsAndLocations > hostedServices> dataHostName`

  Um eine Verbindung zum Unica Rechenzentrum in den USA herzustellen, ändern Sie diesen Wert in `em.unicadeliver.com`.

  Um eine Verbindung zum europäischen UnicaRechenzentrum herzustellen, ändern Sie diesen Wert in

  `em-eu.unicadeliver.com`.

  Um eine Verbindung zu dem Unica Rechenzentrum in Indien herzustellen, ändern Sie diesen Wert in

  `em-in.unicadeliver.com`
- `Deliver > serverComponentsAndLocations > hostedServices> ftpHostName`

  Um eine Verbindung zum Unica Rechenzentrum in den USA herzustellen, ändern Sie diesen Wert in `ftp-em.unicadeliver.com`.

  Um eine Verbindung zum europäischen UnicaRechenzentrum herzustellen, ändern Sie diesen Wert in

  `ftp-eu.unicadeliver.com`.

  Um eine Verbindung zu dem Unica Rechenzentrum in Indien herzustellen, ändern Sie diesen Wert in

  `ftp-in.unicadeliver.com`

Wenn Sie eine Konfigurationseigenschaft ändern, starten Sie den Webanwendungsserver neu, um die Änderungen zu übernehmen.

IP-Adresse der Hostnamen von Deliver

Wenn Sie die IP Adressen für Deliver Hostnamen auf der Firewall Ihres Unternehmens auf die Whitelist setzen möchten, verwenden Sie die folgenden IP-Adressen.

`em.unicadeliver.com`: `13.248.215.130` und `76.223.84.165`

`em-eu.unicadeliver.com`: `75.2.15.173` und `99.83.137.137`

`em-in.unicadeliver.com`: `75.2.92.153` und `99.83.224.139`

`ftp-em.unicadeliver.com`: `192.190.152.236`

`ftp-eu.unicadeliver.com`: `192.190.153.236`

`ftp-in.unicadeliver.com`: `192.175.4.236`

`tms-us.unicadeliver.com`: `13.248.172.132` und `76.223.38.158`

`tms-eu.unicadeliver.com`: `75.2.31.132` und `99.83.164.171`

`tms-in.unicadeliver.com`: `15.197.234.141` und `3.33.199.128`

Anforderungen, um die Daten zu den von HCL Unica gehosteten Services hochzuladen

Eine Deliver Komponente namens Recipient List Uploader (RLU) ist Teil Ihrer Unica Campaign Installation. Die RLU verwendet SFTP als bevorzugten Mechanismus, um das Hochladen von Empfängerlisten und den zugehörigen Metadaten an gehostete HCL Unica-Services zu verwalten.

Deliver verwendet SFTP, um die Daten hochzuladen. Bei der Verwendung von SFTP stoßt die RLU alle Verbindungsanfragen zum Hochladen als lokaler Client an. Die von HCL Unica gehosteten Services stoßen niemals eine Verbindungsanfrage an Ihr Netzwerk an.

Anforderungen bezüglich der Verbindung und des Ports

Eine Internetverbindung ist erforderlich, um mit den HCL Unica gehosteten Services zu kommunizieren. Die HCL Unica gehosteten Services verwenden bestimmte Ports.

Zur Kommunikation verwenden die lokale HCL Unica Installation und die HCL Unica gehosteten Services die folgenden Ports.

HTTPS: port 443

SFTP port: port 2222

HCL Unica Die gehosteten Services stellen niemals eine Verbindung zu Ihrem lokalen Netzwerk her. Es reagiert nur auf Verbindungsanfragen, die hinter Ihrer Firewall angestoßen werden.

Mise en liste blanche d'adresses IP

Pour charger la liste des destinataires (OLT) sur le serveur FTP Deliver, l'adresse IP externe du serveur sur lequel Campaign Web s'exécute doit figurer dans la liste blanche côté serveur Deliver On Demand.

Vous devez obtenir l'adresse IP externe à l'aide des commandes suivantes et la fournir à l'équipe d'intégration. L'équipe d'intégration demandera la mise sur liste blanche de l'adresse IP, afin que les requêtes FTP de votre serveur vers le serveur FTP Deliver soient autorisées.

- Sur un système Unix, exécutez la commande `curl ifconfig.me` pour obtenir l'adresse IP externe de votre serveur.
- Sur un système Windows, vous pouvez accéder à `http://ifconfig.me` pour obtenir l'adresse IP externe de votre serveur.

Connexion de téléchargement par SFTP

Le Recipient List Uploader (RLU) utilise le protocole SFTP comme mécanisme privilégié pour télécharger les listes de destinataires en toute sécurité. La RLU établit une connexion avec les services hébergés de HCL Unica sur le port SFTP 2222. Par le biais de la connexion

sécurisée, la RLU négocie les détails d'authentification avec le serveur SFTP et télécharge la liste des destinataires une fois l'authentification réussie.

Le schéma suivant illustre cette méthode de téléchargement des données des destinataires de Campaign vers les services hébergés de HCL Unica.

Dans la page de configuration, vous pouvez voir l'option SFTP sous ftpProtocol (serverComponentsAndLocations -> hostedServices).

La RLU se connecte au serveur SFTP et télécharge la liste des destinataires sur le serveur SFTP. Une autorisation basée sur un certificat est utilisée pour se connecter au serveur d'authentification. Il utilise la clé privée SSH configurée dans le fichier PEM et l'empreinte RSA SSH configurée dans le fichier known_hosts pour établir la connexion avec le serveur SFTP. Les clients sont tenus de configurer un fichier PEM distinct par compte Deliver, afin qu'il puisse être configuré séparément pour chaque partition Deliver. En plus du fichier PEM, RLU a besoin du fichier known_hosts contenant l'empreinte digitale du serveur SSH, qui est configuré globalement au chemin suivant `Affinium|Deliver|serverComponentsAndLocations|hostedServices`. et un drapeau pour contrôler si RLU exige une empreinte digitale de serveur SSH préconfigurée dans le fichier known_hosts.

Une fois authentifié, le téléchargement de la liste des destinataires se fait par SFTP et il n'y a pas d'impact sur l'exécution de la boîte de processus Deliver à partir de laquelle il sera déclenché.

Dans le cas où les clés publiques ou privées sont générées en utilisant la `passPhrase`, créer une nouvelle source de données avec le nom "`SFTP_PASSPHRASE_DATASOURCE`" sous l'utilisateur de la plateforme spécifié à "`amUserForAcctCredentials`". Par exemple : asm_admin et spécifiez le même mot de passe ou `Passphrase` pour cette source de données que vous avez utilisé lors de la génération des clés publiques ou privées. Le login de la source de données peut être mentionné comme n'importe quel texte.

Si les clés publiques ou privées ne sont pas générées à l'aide de `passPhrase`, la source de données ne doit pas être créée.

Pour générer des clés, effectuez les étapes suivantes.

Étapes pour générer une paire de clés publiques / privées pour l'authentification SFTP.

1. Créer la paire de clés

   La première étape consiste à créer une paire de clés sur la machine, où Campaign web est installé. Connectez-vous à la machine où Campaign web est installé. Ouvrez l'invite de commande et exécutez la commande suivante.

   `ssh-keygen`
2. Indiquez l'emplacement où enregistrer les clés.

   Vous pouvez appuyer sur ENTER ici pour enregistrer les fichiers à l'emplacement par défaut dans le répertoire .ssh de votre répertoire personnel. Vous pouvez également choisir un autre nom de fichier ou un autre emplacement en le saisissant après l'invite et en appuyant sur ENTER.
3. Créez une phrase de passe.

   La deuxième et dernière invite de ssh-keygen vous demandera de saisir une phrase de passe. Cela dépend de vos besoins, si vous voulez utiliser une phrase de passe ou non.

   Exemple :

```
[root@Host bin]# ssh-keygen Génération d'une paire de clés
 rsa publiques/privées. Entrez le fichier dans lequel vous
 souhaitez enregistrer la clé (/root/.ssh/id_rsa) : Saisir la
 phrase de passe (vide si pas de phrase de passe) : Entrez à
 nouveau la même phrase de passe : Votre identification a été
 sauvegardée dans /root/.ssh/id_rsa. Votre clé publique a été
 enregistrée dans /root/.ssh/id_rsa.pub. L'empreinte de la clé est :
 61:ca:14:c2:7a:71:e2:aa:bd:2e:ff:25:b8:b1:fd:ac root@Host Ce qui suit
 est l'image randomart de la clé. .. . +... o +. o . oo o . o o S ..
 oo . . o .= + +*oEoo [root@Host bin]#
```

Votre clé publique est enregistrée dans - `/root/.ssh/id_rsa.pub`. Envoyez la clé publique générée à l'équipe DevOps de Deliver via le support HCL pour la configuration.

Configuration de SFTP

Pour configurer SFTP, effectuez les étapes suivantes.

1. Exécutez la commande suivante en naviguant vers `<Deliver_Home>/tools` depuis l'invite de commande pour exposer la propriété ftpProtocol sur l'interface utilisateur.

   ```
   ./switch_config_visibility.sh / bat -p "Affinium|Deliver|
   serverComponentsAndLocations|hostedServices|ftpProtocol" -v true
   ```
2. Connectez-vous à la plate-forme et accédez à **Paramètres > Configuration** et sélectionnez **SFTP** pour ftpProtocol dans `Affinium|Deliver|serverComponentsAndLocations|hostedServices` .
3. Exécutez la commande suivante en naviguant vers `<Deliver_Home>/tools` depuis l'invite de commande pour exposer la propriété ftpPort sur l'interface utilisateur.

   ```
   ./switch_config_visibility.sh / bat -p "Affinium|Deliver|
   serverComponentsAndLocations|hostedServices|ftpPort" -v true
   ```
4. Mentionnez le numéro de port `2222` pour ftpPort dans `Affinium|Deliver|serverComponentsAndLocations|hostedServices`.
5. Gardez la valeur de `enforceKnownHostsValidation` à `faux`, mettez à jour le chemin comme `<Deliver_HOME>/Conf/known_hosts` pour la propriété `knowHostsPath`.

   Par exemple : `knowHostsPath - /opt/HCL/Campaign/Deliver/conf/known_hosts`

   `enforceKnownHostsValidation - Faux`
6. Facultatif. Si vous disposez du fichier known_hosts, mettez à jour son chemin complet pour la propriété `knowHostsPath` dans `Affinium|Deliver|serverComponentsAndLocations|hostedServices` et définissez `enforceKnownHostsValidation` à `vrai`.
7. Copier le fichier de certificat privé (id_rsa) dans `<DELIVER_HOME>/conf` et mettre à jour le chemin complet pour ce fichier de certificat privé dans la propriété `pemFilePath` à `Affinium|Deliver|partitions|partition1|hostedAccountInfo`.

   Exemple :

   pemFilePath - `/opt/HCL/Campagne/Deliver/conf/id_rsa`

   amDataSourceForSftpPassPhrase-- `SFTP_PASSPHRASE_DATASOURCE`

8. Si vous avez spécifié une phrase de passe lors de la génération des clés publiques/privées, créez une source de données avec le nom `SFTP_PASSPHRASE_DATASOURCE` sous l'utilisateur de la plate-forme spécifié dans `amUserForAcctCredentials` (exemple : asm_admin) et spécifiez le même mot de passe / phrase de passe à cette source de données, que vous avez utilisé lors de la génération des clés publiques/privées. Le login de la source de données peut être mentionné comme n'importe quel texte.
9. Dans le cas où vous n'avez pas spécifié de phrase de passe lors de la génération des clés publiques/privées, vous n'êtes pas obligé de créer ce datasource `SFTP_PASSPHRASE_DATASOURCE` pour l'utilisateur asm_admin ou tout autre utilisateur.
10. Redémarrez le serveur App pour la campagne.
11. Ouvrez une invite de commande, naviguez dans `<Deliver_home>/bin` et testez la connectivité SFTP en utilisant rlu , comme suit.

    ```
    rlu.sh / bat -c
    ```

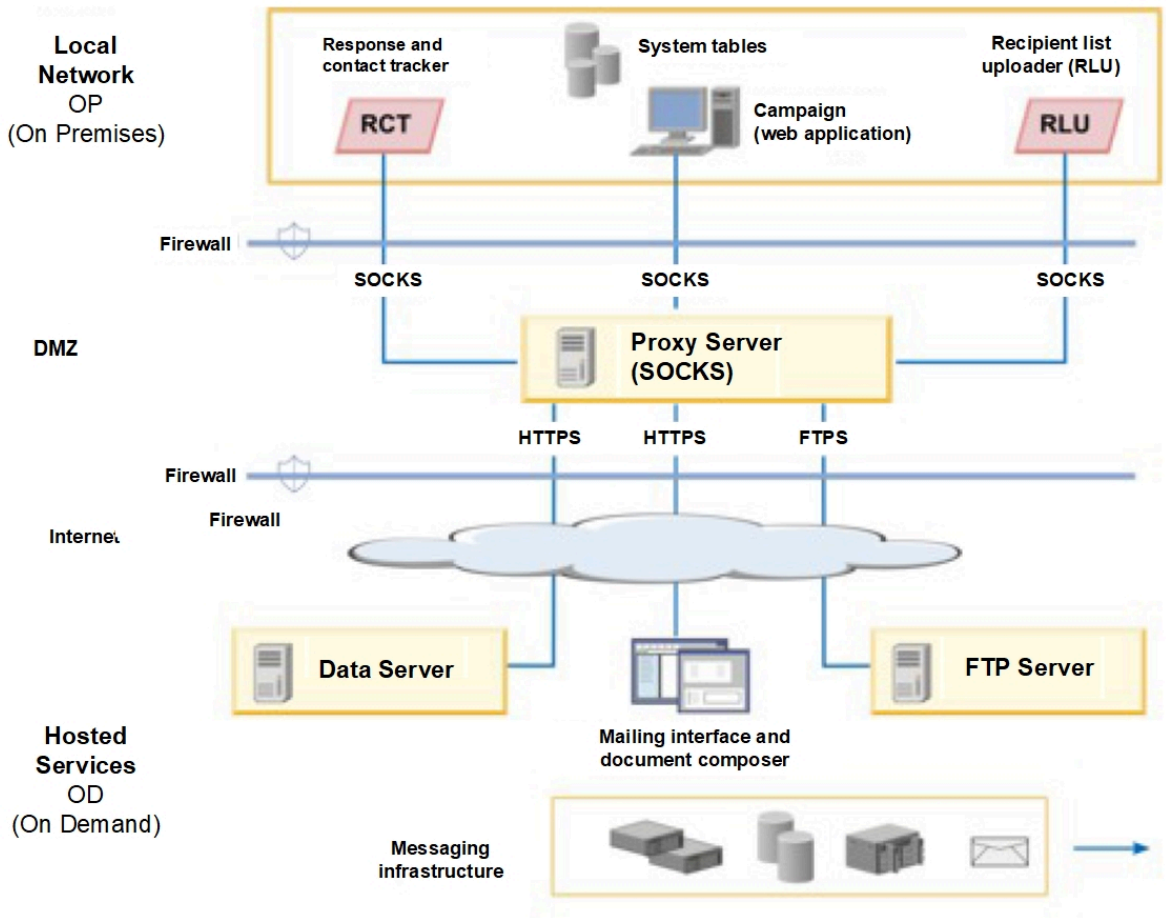
Note: Tous les chemins de fichier spécifiés ci-dessus doivent être complets, y compris le nom du fichier. Répétez les étapes 7 à 9 pour toutes les partitions, où Deliver est configuré.

Verbindung über einen HTTP Proxy

Wenn Ihre Verwaltungsvorschriften in der Regel die direkte Kommunikation mit dem öffentlichen Internet verbieten, können Sie mit HCL Unica über einen HTTP eine Verbindung herstellen. Deliver unterstützt die Verbindung über einen SOCKS-Proxy-Server, der sowohl HTTPS- als auch den SFTP-Datenverkehr zulässt.

Deliver unterstützt SOCKS Protokoll Version 5.

Das folgende Diagramm veranschaulicht die Kommunikation zwischen der lokalen und der gehosteten Umgebungen bei der Verwendung von einem SOCKS Proxy.



Sie müssen den SOCKS Proxy Server in der lokalen Vor-Ort Umgebung konfigurieren. Vor der Konfiguration des Proxy Servers, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllt haben.

- Der Proxy Server muss ein SOCKS Proxy Server sein.
- Der Proxy Server muss auf die Deliver OD Umgebung zugreifen können. Der Server muss Datenverkehr zu und von den für das Rechenzentrum konfigurierten Ports zulassen, das von Ihrem gehosteten E-Mail Konto verwendet wird. Unica besitzt Rechenzentren in den Vereinigten Staaten, Europa und Indien.
- Die Deliver OP Umgebung muss auf den SOCKS Proxy Server zugreifen können.

Konfiguration des Routings für SFTP- und HTTPS-Verkehr über einen SOCKS-Proxy

Um einen SOCKS Proxy für den Zugriff auf die gehosteten E-Mail-Ressourcen zu verwenden, müssen Sie den Webanwendungsserver aktualisieren, auf dem Sie Campaign bereitgestellt haben. Sie müssen auch die Startskripts für Deliver RCT und RLU ändern.

- Wenden Sie für SFTP-Datenverkehr die folgenden Konfigurationen auf die RLU und den Webanwendungsserver an.

RLU- und Webserver-Konfigurationen für SFTP.

Einstellung	Beschreibung
`-Dhcl.unica.deliver.ftp.proxy.host = <socksHost>`	Hostname oder IP des SOCKS Proxys.
`-Dhcl.unica.deliver.ftp.proxy.port = <socksPort>`	Der Port, auf dem der SOCKS Proxy ausgeführt wird.
`-Dhcl.unica.deliver.ftps.proxy.match.hosts= <kommagetrennte Liste von Hostnamen und IP-Adressen>`	Hostnamen und IP-Adressen, die bei der Weiterleitung des Datenverkehrs über den SOCKS Proxy verwendet werden. Geben Sie spezifische Werte für das Rechenzentrum an, das von Ihrem Konto verwendet wird.

Wenn die lokale und die gehostete Umgebung eine Datenverbindung herstellen, ist die für `-Dhcl.unica.deliver.ftps.proxy.match.hosts` angegebene IP-Adresse die IP-Adresse, die der Remote FTP-Server an den lokalen FTP-Client sendet.

Setzen Sie `-Dhcl.unica.deliver.ftps.proxy.match.hosts` auf einen der folgenden Werte. Der von Ihnen eingegebene Wert hängt von dem Rechenzentrum ab, das von Ihrem gehosteten E-Mail Konto verwendet wird.

Hostname und IP Adressen für das US Rechenzentrum:

```
-Dhcl.unica.deliver.ftps.proxy.match.hosts=

ftp-em.unicadeliver.com
```

Hostname und IP Adressen für das europäische Rechenzentrum:

```
-Dhcl.unica.deliver.ftps.proxy.match.hosts=

ftp-eu.unicadeliver.com
```

Hostname und IP-Adressen für das Rechenzentrum Indien:

```
-Dhcl.unica.deliver.ftps.proxy.match.hosts=

ftp-in.unicadeliver.com
```

- Für den HTTPS Datenverkehr, nehmen Sie die folgenden Konfigurationen für das RCT und den Webanwendungsserver an.

Konfigurationseinstellungen für den HTTPS zu SOCKS-Proxy

Einstellung	Beschreibung
`-Dhcl.unica.deliver.https.proxy.host=<socksHost>`	Hostname oder IP des SOCKS Proxys
`-Dhcl.unica.deliver.https.proxy.port=<socksPort>`	Der Port, auf dem der SOCKS Proxy ausgeführt wird

Einstellung	Beschreibung
`-Dhcl.unica.deliver.https.proxy.type=SOCKS`	Der Typ des Proxy Servers. Sie müssen einen SOCKS Proxyserver verwenden.

Configuration de l’authentification pour l’accès à un proxy SOCKS

Si votre proxy SOCKS requiert une authentification, vous devez configurer le serveur d'applications Web, RLU et RCT pour fournir les données d’identification d’accès.

Configurez les éléments suivants pour le serveur d'applications Web, RLU et RCT. Les valeurs de `nom d’utilisateur` et `mot de passe` doivent être les données d’identification requises pour l’authentification auprès du proxy.

```
-Dhcl.unica.deliver.proxy.auth.user = <nom d'utilisateur>
```

```
-Dhcl.unica.deliver.proxy.auth.password = <mot de passe>
```

Configuration de RCT pour l’utilisation d’un proxy SOCKS

Vous devez modifier RCT afin de pouvoir communiquer via un serveur proxy SOCKS. Les paramètres requis dépendent de votre système d’exploitation.

- Pour RCT dans les environnements Windows™, ajoutez les arguments proxy suivants à `common.bat`.
  Le fichier `common.bat` se trouve dans le répertoire `\deliver\bin` de votre installation locale Deliver.

  set `RCT_PROXY_ARGS=`

  ```
  -Dhcl.unica.deliver.https.proxy.host=<HÔTE_PROXY>
  ```

  ```
  -Dhcl.unica.deliver.https.proxy.port=<PORT_PROXY>
  ```

  ```
  -Dhcl.unica.deliver.https.proxy.type=SOCKS
  ```

```
-Dhcl.unica.deliver.proxy.auth.user=<UTILISATEUR_AUTHENTIFICATION_-
PROXY>

-Dhcl.unica.deliver.proxy.auth.password=<MOT_DE_PASSE_AUTHENTIFI-
CATION_PROXY>

set RCT_JAVA_ARGS=%BASE_VM_ARGS% %RCT_MEM_ARGS%

%RCT_EXTRA_VM_ARGS% %RCT_PROXY_ARGS%
```

- Pour RCT dans les environnements UNIX™, ajoutez les arguments proxy suivants à `common.sh`.
  Le fichier `common.sh` se trouve dans le répertoire `/deliver/bin` de votre installation locale Deliver.

  Remarque : Ne modifiez pas directement `rlu.sh`, `rct.sh`ou `setenv.sh`. Le système remplace les modifications.

```
RCT_PROXY_ARGS="

-Dhcl.unica.deliver.https.proxy.host=<HÔTE_PROXY>

-Dhcl.unica.deliver.https.proxy.port=<PORT_PROXY>

-Dhcl.unica.deliver.https.proxy.type=SOCKS

-Dhcl.unica.deliver.proxy.auth.user=<UTILISATEUR_AUTHENTIFICATION_-
PROXY>

-Dhcl.unica.deliver.proxy.auth.password=<MOT_DE_PASSE_AUTHENTIFI-
CATION_PROXY>"

RCT_JAVA_ARGS="${BASE_VM_ARGS} ${RCT_MEM_ARGS} ${RCT_EXTRA_VM_ARGS}
${RCT_PROXY_ARGS}"
```

Configuration de la RLU pour utiliser un proxy SOCKS

Vous devez modifier le RLU pour qu'il communique par le biais d'un serveur proxy SOCKS. Les paramètres requis dépendent de votre système d'exploitation.

- Pour le RLU dans les environnements Windows™, ajoutez les arguments de proxy suivants à `common.bat`.
  Le fichier `common.bat` se trouve dans le répertoire `\deliver\bin` de votre installation locale Deliver.

```
fixer RLU_PROXY_ARGS=

-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.ftp.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes
et d'adresses IP séparés par des virgules>.

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUTH_USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_PASSWORD>

définir RLU_JAVA_ARGS=%BASE_VM_ARGS% %RLU_MEM_ARGS% %RLU_EXTRA_VM_-
ARGS%

%RLU_PROXY_ARGS%.
```

- Pour le RLU dans les environnements UNIX™, ajoutez les arguments de proxy suivants à `common.sh`.
  Le fichier `common.sh` se trouve dans le répertoire `/deliver/bin` de votre installation locale Deliver.

Note: Ne modifiez pas directement `rlu.sh`, `rct.sh` ou `setenv.sh`. Le système annule les modifications.

```
RLU_PROXY_ARGS="

-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.ftp.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes
et d'adresses IP séparés par des virgules>.

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUTH_USER>
```

```
-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_PASSWORD>"

RLU_JAVA_ARGS="${BASE_JAVA_ARGS} ${RLU_MEM_ARGS} ${RLU_EXTRA_VM_-
ARGS}

${RLU_PROXY_ARGS}"
```

Configuration du serveur d'applications Web pour utiliser un proxy SOCKS

Pour vous connecter à HCL Unica via un proxy SOCKS, vous devez modifier la configuration du serveur d'applications web. Pour les serveurs Unica WebSphere®, vous modifiez les arguments JVM génériques. Pour les serveurs Oracle Weblogic, vous modifiez le script `SetDomainEnv`.

- Si votre serveur d'applications web est Unica WebSphere®, ajoutez les éléments suivants aux arguments JVM génériques de WebSphere®.

  ```
  -Dhcl.unica.deliver.https.proxy.host=<PROXY_HOST>

  -Dhcl.unica.deliver.https.proxy.port=<PROXY_PORT>

  -Dhcl.unica.deliver.https.proxy.type=SOCKS

  -Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

  -Dhcl.unica.deliver.ftp.proxy.port=<PROXY_PORT>

  -Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes
  et d'adresses IP séparés par des virgules>.

  -Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUTH_USER>

  -Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_PASSWORD>
  ```

- Si votre serveur d'applications web est Oracle Weblogic, modifiez le script `setDomainEnv`. Les paramètres requis dépendent de votre système d'exploitation.

  Dans les environnements Windows™, apportez les modifications suivantes :

  ```
  JAVA_OPTIONS =%{JAVA_OPTIONS}
  ```

```
-Dhcl.unica.deliver.https.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.https.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.https.proxy.type=SOCKS

-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.ftp.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes
et d'adresses IP séparés par des virgules>.

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUTH_USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_PASSWORD>
```

Dans les environnements UNIX™, effectuez les modifications suivantes :

```
JAVA_OPTIONS = '${JAVA_OPTIONS}

-Dhcl.unica.deliver.https.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.https.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.https.proxy.type=SOCKS

-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.ftp.proxy.port=<POXY_PORT>

-Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes
et d'adresses IP séparés par des virgules>.

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUTH_USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_PASSWORD>'.
```

Daten-Download-Frequenz und Port-Einstellung

Im Rahmen Ihrer DeliverUnica -Installation wird eine Campaign-Komponente namens Response and Contact Tracker (RCT) installiert. Das RCT fordert regelmäßig E-Mail-

Antworten und Verfolgungsdaten von HCL Unica an. Standardmäßig gibt das RCT alle 5 Minuten eine Datenanforderung aus.

Das RCT gibt Datenanforderungen über HTTPS (HTTP über SSL) aus. HCL Unica gehostete Dienste akzeptieren HTTPS-Verbindungsanforderungen an Port 443 und nur von Hosts, die Sie beim Start des gehosteten E-Mail-Kontos angegeben haben.

Konfigurieren eines Systembenutzers für den Zugriff auf HCL Unica Hosted Services

Deliver Komponenten müssen auf die HCL Unica Hosted Services zugreifen können, ohne dass eine manuelle Eingabe der Anmeldeinformationen erforderlich ist. Um die automatische Anmeldung einzurichten, definieren Sie einen Systembenutzer in Platform, der die erforderlichen Zugriffsberechtigungen bereitstellen kann.

Um die Benutzeradministration und Fehlersuche zu vereinfachen, können Sie einen vorhandenen Systembenutzer ändern, damit dieser auf gehostete Services und lokale Systemtabellen zugreifen kann. Sie können einen einzelnen Systembenutzer konfigurieren, um Berechtigungsnachweise für mehrere Systeme bereitzustellen. Beispielsweise können Sie durch Ändern der Konfiguration des Campaign-Systembenutzers einen einzelnen Benutzer erstellen, der automatisch auf IBM Hosted Services und die HCL Unica-Systemtabellen im DeliverCampaign-Schema zugreifen kann.

Als Berechtigungsnachweise für den Zugriff auf HCL Unica Hosted Services werden der Benutzername und das Kennwort benötigt, die Unica für Ihr Hosted-Messaging-Konto bereitgestellt hat. Die verwendeten Anmeldeinformationen hängen davon ab, ob Sie eine Verbindung zum Unica-Rechenzentrum in den USA, Europa oder Indien herstellen. Fragen Sie bei Unica nach, welches Rechenzentrum Sie verwenden sollen.

Spezifische Informationen zur Konfiguration eines Systembenutzers für die Kommunikation mit HCL Unica Hosted Services finden Sie im Unica Deliver Initialisierungs- und Administratorhandbuch.

Allgemeine Informationen zur Erstellung von Systembenutzern und Datenquellen finden Sie im Unica Platform Administratorhandbuch.

Konfigurieren des Partitionszugriffs auf HCL Unica Hosted Services

Unica Deliver Komponenten in der Partition müssen befugt sein, automatisch gültige Berechtigungsnachweise für die Anmeldung bereitzustellen, wenn versucht wird, mit HCL Unica Hosted Services zu kommunizieren. Zu diesem Zweck müssen Sie die HCL Unica Hosted Services-Anmeldeinformationen zu einem Platform-Benutzer hinzufügen. Dieser Benutzer wird der Deliver-Systembenutzer.

Sie können dem HCL Unica-Systembenutzer die Platform-Datenquelle hinzufügen, die die Berechtigungsnachweise für Deliver Hosted Services enthält. Bei diesem Benutzer kann es sich um denselben Systembenutzer handeln, der auf die Campaign-Systemtabellen in der Partition zugreift.

Die Schritte für die Konfiguration von Systembenutzern für eine Partition sind identisch mit denen, die bei der Deliver-Erstinstallation durchgeführt werden, bei der die erste Partition erstellt wurde. Einzelheiten zum Hinzufügen von HCL Unica Hosted Services Login-Berechtigungsnachweisen für einen Systembenutzer finden Sie im Unica Deliver-Initialisierungs- und Administratorhandbuch.

Die für den Zugriff auf HCL Unica gehostete Dienste erforderlichen Anmeldeinformationen sind der Benutzername und das Kennwort, die Unica beim ersten Startvorgang angegeben hat.

Important: Für jede zusätzliche Partition müssen Sie einen eigenen Benutzernamen und ein eigenes Kennwort von Unica anfordern.

Configuration de l'utilisateur système qui accède aux services hébergés HCL Unica

Les composants Deliver dans Campaign doivent être en mesure d’accéder automatiquement aux services hébergés HCL Unica, sans demander de connexion. Les utilisateurs système configurés dans Unica Platform peuvent faire référence à une source de données qui fournit le nom d’utilisateur et le mot de passe requis. Vous pouvez ajouter la source de données à un nouvel utilisateur système ou à un utilisateur système existant. Pour simplifier l’administration des utilisateurs, vous pouvez mettre à jour un utilisateur

système déjà configuré pour accéder au schéma Campaign afin qu'il puisse également accéder aux services hébergés HCL Unica.

Pour effectuer cette tâche, vous devez connaître le nom d'utilisateur et le mot de passe des services hébergés HCL Unica, que Unica a affectés à votre compte de messagerie hébergé. La réception du nom d'utilisateur et du mot de passe fait partie du processus de démarrage de compte.

Vous devez disposer des droits d'accès appropriés et savoir comment créer des utilisateurs système et des sources de données dans Unica Platform.

Remarque : Si votre installation contient plusieurs partitions, vous devez effectuer cette tâche pour chaque partition. Vous ne pouvez pas partager les utilisateurs système entre plusieurs partitions.

1. Créez une source de données Platform pour contenir le nom d'utilisateur et le mot de passe requis pour accéder aux services hébergés HCL Unica. Pour des résultats optimaux et une plus grande facilité de maintenance, nommez cette source de données UNICA_HOSTED_SERVICES. Configurez cette source de données comme suit.

   Pour **Connexion à la source de données**, entrez le nom d'utilisateur que vous avez reçu de la part d'Unica lors du démarrage du compte.

   Pour **Mot de passe de la source de données**, entrez le mot de passe que vous avez reçu de la part d'Unica lors du démarrage du compte.
2. Indiquez la source de données dans la configuration Deliver. Utilisez la propriété de configuration **amDataSourceForAcctCredentials**.

   La propriété de configuration se trouve sous `Deliver > partitions > partition[n] > hostedAccountInfo > amDataSourceForAcctCredentials`.

   Par défaut, la source de données spécifiée est `UNICA_HOSTED_SERVICES`.
3. Spécifiez un utilisateur système pour accéder aux services hébergés HCL Unica. Vous pouvez spécifier un utilisateur existant ou créer un utilisateur. Dans la configuration Deliver, utilisez la propriété de configuration **amUserForAcctCredentials**.

La propriété de configuration se trouve sous `Deliver > partitions > partition[n] > hostedAccountInfo > **amUserForAcctCredentials**`.

Par défaut, l'utilisateur spécifié est `asm_admin`.

4. Ajoutez la source de données configurée à l'étape 1 à l'utilisateur système spécifié à l'étape 3.

Vous devez redémarrer le serveur d'applications Web pour que les changements de configuration prennent effet.

Configurer une communication sécurisée pour les e-mails hébergés

Les communications entre le spécialiste du marketing par e-mail et les services hébergés HCL Unica se produisent via Secure Sockets Layer (SSL). Vous devez modifier la configuration du serveur d'applications Web pour utiliser SSL. L'exécution des modifications requises nécessite l'utilisation de l'utilitaire Java™ `keytool`.

La configuration de la communication sécurisée implique les actions suivantes.

- Générez un magasin de clés sécurisé.
- Obtenir un certificat numérique auprès des services hébergés HCL Unica.
- Ajouter le magasin de clés sécurisé au serveur d'applications Web.
- Importer le certificat numérique des services hébergés HCL Unica dans le magasin de clés sécurisé.

Les étapes et la séquence exactes requises pour configurer SSL dépendent du type et de la version du serveur d'applications Web (WebSphere®, WebLogic, Tomcat, JBoss) sur lequel vous avez déployé Unica Platform et Unica Campaign.

Pour WebLogic, voir Configuration de SSL lors de l'utilisation de WebLogic (à la page 37).

Pour WebSphere®, voir Configuration de SSL lors de l'utilisation de WebSphere (à la page 41).

Génération d’un magasin de clés sécurisé

Suivez cette procédure pour créer un magasin de clés d’identité et un magasin de clés sécurisé afin de configurer Unica Deliver dans le but de communiquer avec les services hébergés HCL Unica via SSL. Vous ajoutez les magasins de clés au serveur d'applications Web lorsque vous configurez SSL.

HCL utilise les valeurs d'exemple ci-dessous dans les procédures contenues dans cette section.

- Magasin de clés d’identité : `HCLUnicaClientIdentity.jks`
- Alias du magasin de clés d’identité : `HCLUnicaClientIdentity`
- Mot de passe (`-storepass`) pour le magasin de clés d’identité : `clientPwd`
- La clé de sécurité (`-keypass`) pour le magasin de clés d’identité : `clientPwd`
- Certificat basé sur le magasin de clés d'identité : `ClientCertificate.cer`
- Magasin de clés sécurisé : `HCLUnicaTrust.jks`
- Mot de passe (`-storepass`) pour le magasin de clés sécurisé : `trustPwd`

Les valeurs réelles que vous entrez doivent être propres à votre installation.

Pour exécuter les étapes de cette procédure, exécutez l'utilitaire Java™ `keytool` à partir de la ligne de commande.

1. Générez un fichier de clés d'identité. Utilisez la commande `genkey`, comme illustré dans l’exemple suivant.

   L'exemple crée un magasin de clés d'identité nommé `HCLUnicaClientIdentity.jks`. Vous pouvez utiliser un nom différent pour le magasin de clés d’identité que vous créez.

   ```
   keytool -genkey -alias HCLUnicaClientIdentity -keyalg RSA -keystore
   <HCLUnicaClientIdentity.jks> -keypass <clientPwd> -validity 1000 -dname
   "CN=hostName, O=myCompany" -storepass <clientPwd>
   ```

   Prenez connaissance des informations suivantes.

- Vous utilisez les valeurs pour `alias`, `keystore`, `keypass`et `storepass` plus tard dans cette procédure et lorsque vous configurez SSL dans le serveur d'applications Web.
- Pour WebSphere®, le mot de passe du magasin de clés (`-storepass`) et le mot de passe de clé (`-keypass`) doivent être identiques.
- Dans le nom distinctif (`-dname`), le nom courant (`CN`) est le même que le nom d'hôte utlisé pour accéder aux services hébergés HCL Unica. Par exemple, si l'URL pour les services hébergés HCL Unica est `https://nomdhote.exemple.com:7002/unica/jsp`, le nom courant est `nomdhote.exemple.com`. La partie "nom courant" du nom distinctif est la seule qui soit obligatoire. Les parties "Organisation" (`O`) et "Unité organisationnelle" (`OU`) sont facultatives.

2. Générez un certificat basé sur le magasin de clés d'identité. Utilisez la commande `export`, comme illustré dans l’exemple suivant.

   L’exemple génère un certificat appelé `ClientCertificate.cer`. Vous pouvez utiliser un nom différent pour le certificat que vous créez.

   Les valeurs de `keystore`, `storepass`et `alias` doivent correspondre aux valeurs que vous avez spécifiées pour le magasin de clés d’identité.

   ```
   keytool -export -keystore <HCLUnicaClientIdentity.jks> -storepass
   <clientPwd> -alias HCLUnicaClientIdentity -file <ClientCertificate.cer>
   ```

3. Générez le magasin de clés sécurisé. Utilisez la commande `import`, comme illustré dans l’exemple suivant.

   L'exemple crée un magasin de clés sécurisé nommé `HCLUnicaTrust.jks`. Vous pouvez utiliser un nom différent pour le magasin de clés sécurisé que vous créez.

   ```
   keytool –import -alias HCLUnicaClientIdentity -file
   <ClientCertificate.cer> -keystore <HCLUnicaTrust.jks> -storepass
   <trustPwd>
   ```

   Appuyez sur la touche **Y** lorsque vous êtes invité à approuver le certificat.

Notez les valeurs que vous avez définies pour les variables suivantes. Vos valeurs peuvent être différentes des valeurs indiquées dans l’exemple.

- `alias` (dans l'exemple : `HCLUnicaClientIdentity`)
- `magasin de clés d'identité` (dans l'exemple : `HCLUnicaClientIdentity.jks`)
- `storepass` (dans l'exemple : `trustPwd`) La valeur `storepass` du magasin de clés sécurisé peut être différente de la valeur `storepass` du certificat et magasin de clés d'identité.
- `magasin de clés` (dans l'exemple : `HCLUnicaTrust.jks`) selon votre serveur d'applications Web, vous spécifiez également le magasin de clés d'identité.

Vous spécifiez ces valeurs propres à l'installation lorsque vous configurez SSL sur le serveur d'applications Web pour votre installation HCL Unica.

Configuration de SSL lors de l'utilisation de WebLogic

Cette section décrit les étapes requises pour configurer SSL si vous déployez des composants HCL Unica sur Oracle WebLogic. Cette modification est requise pour permettre aux composants Deliver qui fonctionnent dans Campaign de communiquer avec les services hébergés HCL Unica via SSL.

Pour obtenir des instructions spécifiques concernant la navigation et l'utilisation de l'interface utilisateur d'Oracle WebLogic, consultez la documentation relative à la version spécifique d'Oracle WebLogic que vous utilisez.

Effectuez les tâches suivantes.

- Modifier le script de démarrage de WebLogic
- Modifier la configuration WebLogic
- Obtenir un certificat numérique auprès des services hébergés HCL Unica
- Créer un magasin de clés sécurisé et importer le certificat numérique Unica

Modification du script de démarrage de WebLogic

Si vous avez déployé Campaign sur WebLogic, vous devez modifier le script de démarrage de WebLogic et la configuration SSL pour WebLogic afin que WebLogic détecte et accepte les communications sécurisées entre les composants Deliver installés localement et les services HCL Unica hébergés.

Ajoutez les arguments suivants à JAVA_OPTIONS dans le script de démarrage de WebLogic.

- `-Dweblogic.security.SSL.allowSmallRSAExponent=true`
- WebLogic, version 12c ou ultérieure : `-Dweblogic.security.SSL.protocolVersion=TLS1`

  Toutes les versions précédentes : `-Dweblogic.security.SSL.nojce=true`

Modifier la configuration WebLogic

Vous devez modifier la configuration SSL dans WebLogic.

Utilisez la console WebLogic pour apporter les modifications suivantes dans la configuration SSL de WebLogic pour votre domaine.

Modifiez le paramètre **Vérification du nom d'hôte** sur `Aucune`.

Obtenir un certificat à partir des services hébergés de HCL Unica

Pour configurer la communication SSL, vous devez télécharger un certificat numérique à partir de HCL Unica. Les détails du certificat sont enregistrés dans un fichier portant l'extension `.cer` que vous pouvez importer dans le keystore du serveur d'applications web.

Vous perdez l'accès aux services hébergés sur HCL Unica lorsque votre certificat SSL existant expire. Utilisez cette procédure pour télécharger un nouveau certificat.

1. Dans Internet Explorer, connectez-vous à l'adresse des services hébergés HCL Unica qui a été configurée pour votre compte de messagerie hébergé.
   - Pour le centre de données américain, allez https://em.unicadeliver.com
   - Pour le centre de données européen, allez à https://em-eu.unicadeliver.com
   - Pour le centre de données de l'Inde, allez à https://em-in.unicadeliver.com

   La tentative de connexion se solde par un échec, mais vous permet d'utiliser le navigateur pour soumettre la demande de certificat.
2. Cliquez sur l'icône de verrouillage et sélectionnez **Afficher le certificat**.
3. Sélectionnez l'onglet Détails et sélectionnez **Copier dans le fichier**.

Enregistrez le fichier avec une extension `.cer` à un emplacement accessible au serveur d'applications Web. Le fichier que vous créez est le certificat numérique que vous insérez dans le keystore du serveur d'applications web.

Par exemple, enregistrez le certificat sous le nom `HCLHosted.cer`.

Créer un magasin de clés sécurisé pour WebLogic et importer le certificat Unica

Pour WebLogic, vous devez créer un magasin de clés sécurisé qui accepte le certificat Unica.

Avant de commencer, utilisez un navigateur Web pour télécharger le certificat numérique des services hébergés HCL Unica et l'enregistrer en tant que fichier `.cer`. Par exemple, le certificat peut être nommé `HCLHosted.cer` (votre nom de fichier peut être différent). Pour des détails supplémentaires, voir Obtenir un certificat à partir des services hébergés de HCL Unica (à la page 38).

HCL utilise les valeurs d'exemple ci-dessous dans les procédures contenues dans cette section.

- Magasin de clés d'identité : `HCLUnicaClientIdentity.jks`
- Mot de passe du magasin de clés d'identité : `clientPwd`
- Magasin de clés sécurisé : `HCLUnicaTrust.jks`
- Alias pour le magasin de clés sécurisé : `HCLUnicaHostedIdentity`
- Mot de passe (`-storepass`) pour le magasin de clés sécurisé : `trustPwd`
- Certificat numérique (`-file`) fourni par Unica : `HCLHosted.cer`

Les valeurs réelles que vous entrez doivent être propres à votre installation.

Pour exécuter les étapes de cette procédure, exécutez l'utilitaire Java™ `keytool` à partir de la ligne de commande.

1. Générez un magasin de clés sécurisé pour WebLogic.
   Pour plus d'informations, voir Génération d'un magasin de clés sécurisé *(à la page 35)*.

Vous spécifiez le identity keystore et le trusted keystore dans la configuration de WebLogic.

2. Utilisez la commande `import` dans l'utilitaire `keytool` pour ajouter le certificat de services hébergés HCL Unica au magasin de clés sécurisé créé à l'étape 1, comme illustré dans l'exemple suivant.
   Utilisez le certificat numérique que vous avez téléchargé auprès d'Unica.

   Dans cette procédure, vous définissez également un alias pour le magasin de clés sécurisé.

   ```
   keytool -import -alias HCLUnicaHostedIdentity -file <HCLHosted.cer>
   -keystore <HCLUnicaTrust.jks> -storepass <trustPwd>
   ```

   Appuyez sur la touche **Y** lorsque vous êtes invité à approuver le certificat.
3. Dans la console d'administration WebLogic, configurez les magasins de clés pour le serveur.

   Pour spécifier les règles de configuration, sélectionnez l'option pour le magasin de clés d'identité et le magasin de clés sécurisé personnalisés parmi les choix disponibles. Pour Identité personnalisée, spécifiez le magasin de clés d'identité. Pour Clés de confiance personnalisées, spécifiez le magasin de clés sécurisé.

   Par exemple, dans la console d'administration, spécifiez les éléments suivants (en utilisant les valeurs d'exemple du magasin de clés sécurisé que vous avez créé à l'étape 1).

   - Pour **Identité** : spécifiez le magasin de clés d'identité et le mot de passe associé.

     Par exemple, `HCLUnicaClientIdentity.jks` et `clientPwd`.
   - Pour la **Confiance** : spécifiez le magasin de clés sécurisé et le mot de passe associé.

     Par exemple, `HCLUnicaTrust.jks` et `trustPwd`.

   Indiquez le chemin d'accès complet aux deux magasins de clés.

4. Redémarrez WebLogic. WebLogic n’implémente pas les modifications de configuration tant que vous ne redémarrez pas le serveur d'applications Web.
5. Pour tester la connexion SSL, connectez-vous à Unica Campaign et accédez à divers menus des fonctions de messagerie. Confirmez que vous pouvez créer des courriers électroniques, des pages d’arrivée et des mailings.

Configuration de SSL lors de l’utilisation de WebSphere

Cette section décrit les étapes générales requises pour configurer SSL si vous avez déployé des composants HCL Unica sur WebSphere®. Cette modification est requise pour permettre aux composants Deliver qui fonctionnent dans Campaign de communiquer avec les services hébergés HCL Unica via SSL.

Avant de commencer, vous devrez connaître la valeur de la propriété de configuration `uiHostName`. La valeur de `uiHostName` est l'URL des services hébergés HCL Unica. Pour plus d'informations, voir Konfiguration von Adressen für die Verbindung zu HCL Unica gehosteten Diensten (à la page 15).

Vous devez accéder à la console de sécurité WebSphere® pour modifier les paramètres de certificat SSL et de gestion des clés. Cette tâche nécessite un redémarrage du serveur d'applications Web Campaign pour implémenter les modifications.

Si vous avez déployé Campaign sur WebSphere®, vous devez modifier la configuration de sécurité WebSphere® pour extraire le certificat de signataire de HCL Unica et l’ajouter au magasin de confiance WebSphere®. Si vous recevez un message d’erreur indiquant que votre certificat de signataire actuel a expiré, supprimez le certificat actuel et ajoutez-en un nouveau.

Pour obtenir des instructions spécifiques concernant la navigation et l’utilisation de l'interface utilisateur WebSphere®, consultez la documentation relative à la version spécifique d'Unica WebSphere® que vous utilisez.

1. Générez un magasin de clés sécurisé.

   Pour des détails supplémentaires, voir Génération d’un magasin de clés sécurisé (à la page 35).

Pour configurer SSL, vous devez spécifier les valeurs que vous définissez pour les variables suivantes. Les valeurs affichées sont fournies uniquement à titre d'exemple. Vos valeurs peuvent être différentes.

- `alias` : *`UnicaClientIdentity`* (exemple)
- `keystore` : *`HCLUnicaTrust.jks`* (exemple)
- `storepass` : *`trustPwd`* (exemple)

2. Sélectionnez le nouveau magasin de clés dans la console de sécurité WebSphere®.

   Par exemple, si vous avez suivi l'exemple à l'étape 1, sélectionnez `HCLUnicaTrust.jks`.
3. Procurez-vous un certificat de sécurité auprès de HCL Unica et importez-le dans WebSphere®, comme décrit dans les étapes suivantes.

   a. Dans la console de sécurité WebSphere®, accédez à **Certificat SSL et gestion des clés** > **Magasins de clés et certificats** > **NodeDefaultTrustStore** > **Certificats de signataires**. Sélectionnez **Extraire d'un port**.

   b. Configurez WebSphere® pour établir une connexion de test afin d'extraire le certificat de signataire depuis HCL Unica. Entrez les valeurs suivantes pour le certificat de signataire HCL Unica.
      - **Host** La valeur définie pour `Deliver >serverComponentsAndLocations > hostedServices >uiHostName`
      - **Port** 443
      - **Configuration SSL de connexion sortante** `NodeDefaultSSLSettings`
      - **Alias** La valeur que vous avez entrée pour **Host**

      Lorsque vous avez terminé, WebSphere® communique avec les services hébergés HCL Unica afin d'extraire les informations requises pour créer un certificat de signataire pour les services hébergés HCL Unica.
4. Une fois que WebSphere® a créé le certificat de signataire, sélectionnez le nouveau certificat dans la console de sécurité.

   Le serveur d'applications Web utilise le nouveau certificat pour établir des connexions à HCL Unica.
5. Redémarrer WebSphere®

WebSphere® n’implémente pas les modifications de configuration tant que vous ne redémarrez pas le serveur d'applications Web.

Pour plus d'informations sur les versions de WebSphere® prises en charge pour déployer des produits Unica, voir le document Environnements logiciels recommandés et configuration minimum requise de chaque produit.

Déploiement de la Campaign dans Tomcat ou JBOSS

Aucune configuration supplémentaire n'est requise pour Deliver, si Campaign est déployé dans Tomcat ou JBOSS. Vous n'avez pas besoin d'obtenir et de configurer des certificats de services hébergés.

Chapter 4. Operation für Response and Contact-Tracker

Die Response and Contact Tracker (RCT) ist in Ihrer lokalen Umgebung installiert und kommuniziert mit HCL Unica Hosted Services, um Daten für E-Mail-Kommunikation, E-Mail-Benachrichtigungen und Empfängerantworten zu abrufen und zu verarbeiten, wie z. B. Links anklickt und geöffnet werden. Das RCT muss ausgeführt werden, um Link-Tracking- und E-Mail-Zustellungsbenachrichtigungsdaten von HCL Unica gehosteten Diensten abzurufen.

RCT verwendet Kafka, um Antworten unabhängig vom Download-Mechanismus zu verarbeiten. Wenn RCT zum ersten Mal ausgeführt wird, werden mehrere Kafka-Themen erstellt, falls noch nicht vorhanden. Jeder Antworttyp wird unter Verwendung eines separaten Themas pro Campaign-Partition verarbeitet. Jedes Thema hat standardmäßig zwei Kafka-Partitionen und zwei Verbraucher, was eine schnellere Antwortverarbeitung sogar mit einer einzelnen Instanz von RCT ermöglicht.

Es wird empfohlen, Kafka als gemeinsam genutzten Service auf separaten Rechnern laufen zu lassen, damit es nicht RCT-spezifisch ist und auch Nachrichten von anderen Unica-Anwendungen wie Campaign, Journeys und Interact verarbeiten kann.

Unter folgenden Bedingungen ist ein Neustart von RCT erforderlich:

1. Das Ausführungsprotokoll-Flag wird umgeschaltet
2. Kafka-Konfigurationen werden geändert
3. Kafka-Partitionen werden erhöht

Sie müssen Kafka in Unica Platform für RCT konfigurieren. Führen Sie die folgenden Schritte aus, um auf Kafka-Konfigurationen zuzugreifen. Für Einzelheiten zur Konfiguration von Kafka, siehe das Thema Konfigurationseigenschaften für Deliver (on page 59).

1. Navigieren Sie auf der Unica Platform zu **Einstellungen > Konfiguration**.
2. Klappen Sie die Deliver Knoten auf.
3. Navigieren Sie zu **Deliver|serverComponentsAndLocations|Kafka|RCT**.
4. Wählen Sie **RCT**aus.
5. Wählen Sie **Einstellungen bearbeiten** aus.

Im Folgenden sind die obligatorischen Konfigurationen basierend auf dem Wert CommunicationMechanism aufgeführt.

Auf der Seite Kafka Konfiguration 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:

Nehmen Sie die erforderlichen Konfigurationen vor und klicken Sie auf Speichern.

Note: Da die Kafka-Protokolldateien sehr groß sind, kann der Speicherplatz knapp werden und der Kafka-Server plötzlich abgeschaltet werden.

Schritte, um RCT zu starten:

1. Zookeeper starten, 10 Sekunden warten
2. Kafka starten
3. RCT wie gewohnt starten

Schritte, um RCT zu stoppen:

1. RCT stoppen
2. Kafka stoppen
3. Zookeeper stoppen

Sie können die RCT auf eine der folgenden Arten starten.

- Starten Sie die RCT manuell.
- RCT als Dienst starten

Important: Sie müssen die RCT manuell starten, wenn Sie Deliver zum ersten Mal verwenden, auch wenn Sie die RCT als Dienst registriert haben.

Sie müssen die RCT neu starten, wenn Sie Änderungen an den Konfigurationseigenschaften für Deliver vornehmen. Sie können das RCT jederzeit neu starten, auch wenn Sie es für die Ausführung als Dienst konfiguriert haben. HCL Unica Gehostete Dienste speichern weiterhin Tracking-Daten, wenn das RCT heruntergefahren oder neu gestartet wird. Wenn der Betrieb wieder aufgenommen wird, lädt der RCT die Informationen in der Warteschlange herunter.

Fonctionnement manuel du service RCT (Response and Contact Tracker)

Pour utiliser le service RCT (Response and Contact Tracker) manuellement, exécutez le script `rct` dans le répertoire `bin` de votre installation Deliver.

- Pour démarrer RCT, exécutez le script `rct` dans le répertoire `bin` de votre installation Deliver, comme suit.

  ```
  rct start
  ```
- Pour arrêter RCT, exécutez le script `rct` comme suit.

  ```
  rct stop
  ```

Pour plus d'informations sur ce script, voir Deliver Response and Contact Tracker (RCT) Skript (à la page 138).

Ajout de la fonction RCT en tant que service

Vous pouvez configurer le démarrage automatique de la fonction RCT (Response and Contact Tracker) en l'ajoutant en tant que service.

Enregistrez le service RCT en exécutant le script `MKService_rct` fourni avec le logiciel Deliver.

Pour ajouter la fonction RCT (Response and Contact Tracker) en tant que service, exécutez le script `MKService_rct-install` à partir du répertoire `bin` de votre installation Deliver.

Le répertoire `bin` est créé en tant que sous-répertoire dans le répertoire d'installation Campaign lorsque vous installez ou effectuez une mise à niveau vers la version la plus récente d'Unica Campaign.

Dans UNIX™ ou Linux™, exécutez ce script avec un utilisateur qui dispose de droits root ou de droits permettant de créer des processus de démon.

Dans Windows™, le nom du service est **Response & Contact Tracker**.

Après avoir exécuté le script `MKService_rct`, lancez RCT manuellement avec le script `rct`. Vous redémarrez manuellement RCT qu'une seule fois. Une fois que vous avez démarré RCT manuellement la première fois, RCT redémarre automatiquement chaque fois que vous redémarrez le système d'exploitation de l'ordinateur sur lequel vous avez installé RCT.

Après avoir configuré le service RCT, vous pouvez empêcher le démarrage automatique de RCT en exécutant le script `MKService_rct` avec l'option `-remove`.

Suppression du service RCT (Response and Contact Tracker)

Si vous avez installé la fonction RCT (Response and Contact Tracker) en tant que service, RCT redémarre à chaque fois que vous redémarrez le système sur lequel vous avez installé RCT. Pour empêcher le redémarrage automatique de RCT, vous devez supprimer le service RCT (Response and Contact Tracker).

Pour supprimer RCT en tant que service, exécutez le script `MKService_rct` avec l'option `-remove`.

A partir d'une ligne de commande Windows™, dans votre répertoire de base HCL Unica, exécutez `Deliver\bin\MKService_rct.bat -remove`.

Sous UNIX™ ou Linux™, dans votre répertoire de base HCL Unica, exécutez `Deliver/bin/MKService_rct.sh -remove`.

Pour plus d'informations sur ce script, voir Script MKService_rct (à la page 139).

Chapitre 5. Vérification au démarrage

Pour garantir l'accès à toutes les fonctions de messagerie hébergée, testez les configurations et les connexions pour vos installations Campaign et Deliver une fois que vous avez activé Deliver, développé votre installation Deliver ou mis à niveau l'installation Campaign.

Vérifiez les configurations et les connexions après avoir effectué l'une des opérations suivantes.

- Activer Deliver pour la première fois
- Mettre à niveau votre installation Unica Campaign actuelle
- Ajouter une nouvelle partition à la configuration Deliver conservée dans Unica Platform

Confirmation pour les configurations système

Pour vous assurer que les préparatifs de démarrage sont terminés, vérifiez que les propriétés de configuration suivantes sont définies et que les paramètres répondent aux exigences de vos installations Deliver et Campaign.

Propriété de configuration	Paramètre
`Campaign | partitions | partition[n] | Deliver | DeliverPluginJarFile`	Chemin d'accès complet vers l'emplacement du fichier de plug-in qui fonctionne comme RLU (Recipient List Uploader). Entrez le chemin d'accès complet au répertoire local du système de fichiers de l'ordinateur qui héberge le serveur d'applications Web Campaign. Le programme d'installation d'Unica remplit automatiquement ce paramètre pour la partition par défaut lorsque vous l'exécuterez. Pour les autres partitions, configurez cette propriété manuellement.

Propriété de configuration	Paramètre
`Campaign | partitions | partition[n] | server | internal | deliverInstalled`	Indique qu'Deliver est installé. Affectez la valeur **Yes** à cette propriété dans chaque partition où vous souhaitez activer Deliver, y compris la partition par défaut. Lorsque vous affectez la valeur **Yes**à cette propriété, les fonctions Deliver deviennent disponibles dans l'interface Campaign.
`Deliver | serverComponentsAndLocations | hostedServices | uiHostName`	Adresse vers HCL Unica pour toutes les communications à l’exception des listes de chargement. Le paramètre par défaut est `em.unicadeliver.com`, pour le centre de données aux États-Unis. Si vous vous connectez au centre de données situé en Europe, remplacez cette valeur par `em-eu.unicadeliver.com`.
`Deliver | serverComponentsAndLocations | hostedServices | dataHostName`	Adresse de la connexion utilisée par Deliver pour charger les métadonnées associées aux listes de destinataires sur HCL Unica. Le paramètre par défaut est `em.unicadeliver.com`, pour le centre de données aux États-Unis. Si vous vous connectez au centre de données situé en Europe, remplacez cette valeur par `em-eu.unicadeliver.com`.
`Deliver | serverComponentsAndLocations | hostedServices | ftpHostName`	Adresse de la connexion utilisée par Deliver pour transférer les données associées aux listes de destinataires (sauf les métadonnées de la liste) sur HCL Unica.

Propriété de configuration	Paramètre
	Le paramètre par défaut est `ftp-em.unica-deliver.com`, pour le centre de données aux États-Unis. Si vous vous connectez au centre de données situé en Europe, remplacez cette valeur par `ftp-eu.unicadeliver.com`.
`Deliver | partitions | partition[n] | hostedAccountInfo | amUserFor-AcctCredentials`	Utilisateur HCL Unica qui fait référence à la source de données qui contient les droits d'accès aux services hébergés HCL Unica. Vous configurez cette valeur lorsque vous créez un utilisateur système pour accéder aux ressources de courrier électronique hébergées par Unica.
`Deliver | partitions | partition[n] | hostedAccountInfo | amDataSource-ForAcctCredentials`	Source de données Platform qui contient les données d'identification de connexion aux services hébergés HCL Unica. Vous configurez cette valeur lorsque vous créez un utilisateur système pour accéder aux ressources de courrier électronique hébergées par Unica.
`Deliver | partitions | partition [n] < dataSources | systemTables | type`	Type de base de données hébergeant les tables système . Indiquez la valeur correcte pour votre base de données.
`Deliver | partitions | partition [n] < dataSources | systemTables | schemaName`	Nom du schéma de base de données pour les tables système . Définissez le nom de schéma approprié pour votre base de données.

Propriété de configuration	Paramètre
`Deliver | partitions | partition [n] < dataSources | systemTables | jdbcClassName`	Pilote JDBC pour les tables système. Indiquez la valeur correcte pour votre environnement.
`Deliver | partitions | partition [n] < dataSources | systemTables | jdbcURI`	URI de connexion JDBC pour les tables système. Indiquez la valeur correcte pour votre environnement. Indiquez le type de base de données, le pilote de base de données, l'hôte, le port et le nom de la base de données. Par exemple : `jdbc:oracle:thin:@yourdb.example-.com:1234:DBname` Consultez la documentation de votre base de données pour obtenir des instructions spécifiques sur la façon de construire l'URL JDBC. La valeur que vous entrez doit correspondre exactement à la valeur définie dans votre serveur Web Campaign.
`Deliver | partitions | partition [n] < dataSources | systemTables | asmUserForDBCredentials`	Utilisateur HCL Unica qui fait référence à la source de données qui contient les données d’identification de connexion aux tables système. Vous créez cet utilisateur lorsque vous configurez l’accès aux tables système Deliver locales.
`Deliver | partitions | partition [n] < dataSources | systemTables | asmDataSourceForDBCredentials`	Source de données Platform qui contient les identifiants de connexion aux tables système.

Propriété de configuration	Paramètre
	Vous créez cette source de données lorsque vous créez un utilisateur pour accéder aux tables système Deliver.

Test de chargement vers les services hébergés HCL Unica

Pour tester la possibilité de charger des données vers les services hébergés HCL Unica depuis votre environnement local, exécutez le script **`rlu`** en mode vérification.

Dans le répertoire `bin` de votre installation Deliver, exécutez le script `rlu` de l'une des manières suivantes.

- `rlu -c`
- `rlu --check`

Test du téléchargement depuis les services hébergés HCL Unica

Pour tester la possibilité de télécharger des informations depuis les services hébergés HCL Unica, exécutez le script rct en mode vérification.

Dans le répertoire `bin` de votre installation Deliver, exécutez le script `rct` comme suit.

```
rct check
```

Verbindung zur gehosteten Nachrichtenschnittstelle testen

Unica Hostet die Nachrichtenschnittstelle aus den Rechenzentren in den USA, Indien und Europa. Testen Sie die Verbindung zur gehosteten Mailschnittstelle, indem Sie versuchen, auf eine Deliver Funktion zuzugreifen.

Melden Sie sich bei HCL Unica an und wählen Sie **Mailings** im Menü **Campaign** aus.

Wenn die Verbindung zur Deliver Benutzerschnittstelle ordnungsgemäß hergestellt wurde, wird die Seite „Senden von Mailings“ geöffnet und eine Auflistung der Mailings und der zugehörigen Maileigenschaften angezeigt.

Wenn die Verbindung zur Benutzerschnittstelle nicht ordnungsgemäß hergestellt wurde, wird ein Fehler angezeigt.

Chapitre 6. Configurations pour Unica Deliver

Unica Platform fournit diverses propriétés de configuration permettant de modifier le comportement et l'apparence de Deliver. Certaines propriétés de configuration sont définies lors de l'installation. Vous pouvez modifier les propriétés de configuration à tout moment.

Une fois que vous avez mis à jour les configurations Campaign et Deliver, vous devez redémarrer RCT (Response and Contact Tracker) et le serveur d'applications Web qui héberge Campaign.

Caractéristique ou fonction	Propriété de configuration (y compris le chemin d'accès)
Activez ou désactivez Deliver dans la partition Campaign. Voir Campaign | partitions | partition[n] | server | internal (à la page 62).	`Campaign | partitions | partition[n] | server | internal`
Caractéristiques des listes de destinataires de courrier électronique. Voir Campaign | partitions | partition[n] | Deliver (à la page 60).	`Campaign | partitions | partition[n] | Deliver`
URL requises pour la connexion aux services hébergés HCL Unica. Voir Deliver | serverComponentsAndLocations | hostedServices (à la page 68).	`Deliver | serverComponentsAndLocations | hostedServices`
Identifiants d'accès de base de données et de compte pour la connexion aux services hébergés HCL Unica.	`Deliver | partitions | partition[n] | hostedAccountInfo`

Caractéristique ou fonction	Propriété de configuration (y compris le chemin d'accès)
Voir Deliver | partitions | partition[n] | hostedAccountInfo (à la page 75)	
Paramètres de schéma et d'accès à la base de données pour les tables système Deliver. Voir Deliver | partitions | partition[n] | dataSources | systemTables (à la page 76)	`Deliver | partitions | partition[n] | dataSources | systemTables`
Emplacement d'un script qui s'exécute en réponse aux actions ou aux statuts de RLU (Recipient List Uploader) (facultatif). Voir Deliver | partitions | partition[n] | recipientListUploader (à la page 81)	`Deliver | partitions | partition[n] | recipientListUploader`
Paramètres liés au téléchargement de données, traités par RCT (Response and Contact Tracker). Voir Deliver | partitions | partition[n] | responseContactTracker (à la page 81)	`deliver | partitions | partition[n] | responseContactTracker`
Prise en charge de la présentation de listes de données personnalisées dans Deliver en fonction de tables de dimension dans Campaign.	`Campaign | partitions | partition[n]| Deliver | oltDimTableSupport`

Caractéristique ou fonction	Propriété de configuration (y compris le chemin d'accès)
Voir Configuration de la prise en charge des tables de dimension (à la page 58).	
Prise en charge du suivi d'historique d'exécution de mailing. Voir Deliver | partitions | partition[n] | responseContactTracker (à la page 81)	`deliver | partitions | partition[n] | responseContactTracker` Voir le paramètre **enableExecutionHistoryDataTracking**.

Pour plus d'informations sur l'utilisation des propriétés de configuration, voir le document Unica Platform - Guide d'administration.

Konfigurieren des Zugriffs auf den zusätzlichen Mailing-Ausführungsverlauf

Sie können anfordern, dass Unica zusätzliche Daten zum Mailingausführung bereitgestellt werden. Der Zugriff auf zusätzliche Mailing-Ausführungsverlaufsdaten ist auf Anfrage von Unica und durch Aktualisieren der Deliver-Konfiguration möglich. Daten für den Mailing-Ausführungsverlauf werden in Ihren lokalen Deliver-Systemtabellen in der Tabelle `UACE_ExecHistory` aufgezeichnet, um abgeschlossene Mailing-Läufe zu beschreiben.

Um zusätzliche Daten für die Mailausfuhr herunterzuladen, müssen Sie die Konfigurationseigenschaft `enabletExecutionHistorityDataTracking` aktualisieren. Standardmäßig ist `enableExecutionHistoryDataTracking` in den Deliver-Konfigurationseigenschaften nicht verfügbar.

Sie können diese Konfigurationseigenschaft in Ihrer lokalen Deliver-Installation anzeigen. Führen Sie dazu das Script `switch_config_visibility.bat` aus, das sich im Verzeichnis `emessage\tools` befindet. Die folgenden Arten von Datensätzen sind in einem zusätzlichen Mailingausführung verfügbar.

- Betreffzeile der Nachricht
- Adresse des Absenders
- Benutzer, der das Mailing aktualisiert hat
- Dokumentbeschreibung
- Mailingspeicherdatum

1. Fordern Sie Zugriff auf zusätzliche Daten der Mailingausführung an. Um den Zugriff anzustellen, wenden Sie sich an Ihr Unica Deliver Services Team über HCL Technical Support
2. Aktualisieren Sie die Deliver-Konfiguration. Konfigurieren Sie die folgende Konfigurationseigenschaft.

   ```
   Affinium|deliver|partitions|partition1|responseContactTracker| enableExecutionHistoryDataTracking
   ```

   Setzen Sie **enableExecutionHistoryDataTracking** auf **True**.

Sie können die Deliver Systemtabellen abfragen, um Mailingausführung informationen aus der Tabelle `UACE_ExecHistory` abzurufen.

Weitere Informationen zu den Deliver-Systemtabellen finden Sie in den Unica Deliver-Systemtabellen und im Datenwörterbuch.

Prise en charge de l’intégration des offres Campaign

Unica Deliver prend en charge l’ajout d’offres configurées dans Campaign à un e-mail personnalisé créé dans Deliver.

Les offres sont basées sur des modèles d’offre configurés dans Unica Campaign. Pour prendre en charge l’intégration d'offres Campaign dans un e-mail personnalisé, vous devez mettre à jour la propriété `contactAndResponseHistTracking` dans la configuration Campaign et effectuer d’autres configurations dans Campaign.

Pour plus d’informations sur la configuration de la prise en charge de l’intégration des offres, voir les rubriques relatives à l’intégration des offres Deliver dans le Guide d’administration d'Unica Campaign.

Configuration de la prise en charge des tables de dimension

Pour prendre en charge certaines fonctions fournies par les scripts de messagerie avancés, la propriété de configuration `oltDimTableSupport` doit être définie sur **True**.

Deliver fournit des scripts avancés pour créer des messages électroniques qui affichent des listes d'informations personnalisées. Ces listes nécessitent l'association de tables de dimension créées dans Campaign à une table de liste de cibles (OLT) qui définit la liste des destinataires du courrier électronique. Les tables de liste de cibles sont créées dans le schéma Deliver.

La propriété de configuration `oltDimTableSupport` contrôle la prise en charge de la création de tables de dimension dans le schéma Deliver. Lorsque la valeur de cette propriété est définie sur `True`, une table OLT peut utiliser les informations fournies dans une table de dimension.

Procédez comme suit pour mettre à jour la propriété `oltDimTableSupport`.

Pour plus d'informations sur la manière dont les spécialistes du marketing utilisent les scripts avancés pour créer des tables de données, voir le document Unica Deliver - Guide d'utilisation.

1. Accédez à **Paramètres** > **Configuration** > **Campaign** > **partitions** > **partition[n]** > **Deliver**
2. Cliquez sur **Editer les paramètres** et affectez la valeur `True` à la propriété `oltDimTableSupport`.

Configuration de l'accès aux tables système Deliver locales

Les composants Deliver doivent pouvoir accéder aux tables système Deliver du schéma Campaign. Vous devez créer et configurer un utilisateur système qui peut accéder aux tables système automatiquement. L'utilisateur système qui a été configuré lors de l'installation de Campaign dispose déjà des droits d'accès nécessaires au schéma Campaign.

Remarque : Si votre installation contient plusieurs partitions, vous devez effectuer cette tâche pour chaque partition. Vous ne pouvez pas partager les utilisateurs système entre plusieurs partitions.

Si vous souhaitez utiliser un autre utilisateur système pour accéder aux tables système Deliver, vous devez créer un nouvel utilisateur système dans Platform et créer une nouvelle source de données de plateforme avec accès au schéma Campaign.

1. Dans la configuration Deliver, spécifiez un utilisateur système qui accède à la base de données qui héberge le schéma Campaign.

   Vous pouvez créer un nouvel utilisateur ou spécifier un utilisateur existant. L'utilisateur système que vous avez configuré pour Campaign a déjà accès au schéma Campaign.

   Utilisez la propriété de configuration `Deliver > partitions > partition [n] < dataSources > systemTables > asmUserForDBCredentials`.

   Par défaut, l'utilisateur spécifié est `asm_admin`.
2. Dans la configuration Deliver, spécifiez la source de données qui est configurée pour contenir le nom d'utilisateur et le mot de passe requis pour accéder à la base de données qui héberge le schéma Campaign.

   Vous pouvez utiliser la source de données qui a été créée pour accéder au schéma Campaign lors de l'installation de Campaign.

   Utilisez la propriété de configuration `Deliver > partitions > partition [n] < dataSources > systemTables > amDataSourceForDBCredentials`.

Konfigurationseigenschaften für Deliver

Sie greifen auf die Deliver-Konfigurationseigenschaften über das Menü Einstellungen im Platform zu. Eigenschaften zum Konfigurieren von Deliver sind in den Konfigurationskategorien „Kampagne“ und "Bereitstellen" enthalten.

Um auf die Konfigurationseigenschaften zuzugreifen, navigieren Sie zu **Einstellungen > Konfigurationen**. Auf der Seite Konfigurationen werden alle verfügbaren Konfigurationseigenschaften für Ihre HCL Unica-Installation aufgelistet.

Campaign | partitions | partition[n] | Deliver

Les propriétés de cette catégorie vous permettent de définir les caractéristiques des listes de destinataires, et de préciser l'emplacement des ressources qui téléchargent les listes sur HCL Unica.

DeliverPluginJarFile

Description

Chemin d'accès complet à l'emplacement du fichier qui fait office de Chargeur des listes de destinataires (RLU). Ce plug-in d'accès à Campaign télécharge les données OLT et les métadonnées associées vers des services distants hébergés par Unica. L'emplacement que vous spécifiez doit être le chemin d'accès complet au répertoire local du système de fichiers de l'ordinateur qui héberge le serveur d'applications Web de Campaign.

Le programme d'installation d'Unica remplit automatiquement ce paramètre pour la partition par défaut lorsque vous l'exécuterez. Pour les autres partitions, vous devez configurer manuellement cette propriété. Etant donné qu'il n'y a qu'un seul RLU pour chaque installation d'Deliver, toutes les partitions doivent spécifier le même emplacement pour le RLU.

Ne changez pas ce paramètre, sauf si Unica vous le demande.

Valeur par défaut

Aucune valeur par défaut définie.

Valeurs valides

Chemin d'accès complet au répertoire local dans lequel est installé le serveur Web de Campaign.

defaultSeedInterval

Description

Nombre de messages entre les messages de valeur de départ si `defaultSeedType` est défini sur `Distribute list`.

Valeur par défaut

`1000`

defaultSeedType

Description

Méthode par défaut utilisée par Deliver pour insérer des adresses pièges dans une liste de destinataires.

Valeur par défaut

`Distribute IDS`

Valeurs valides

- `Distribution des identifiants` - distribue de manière homogène des ID en fonction de la taille de la liste des destinataires et du nombre d'adresses pièges disponibles, insère les adresses des clés à des intervalles égaux dans l'intégralité de la liste des destinataires.
- `Distribute list` : insertion d'adresses pièges pour chaque ID `defaultSeedInterval` de la liste principale. Insère toute la liste des adresses pièges disponibles à des intervalles spécifiés dans la liste des destinataires. Vous devez spécifier l'intervalle entre les points d'insertion.

oltTableNamePrefix

Description

Utilisé dans le schéma généré pour la table des listes cibles. Vous devez définir ce paramètre.

Valeur par défaut

OLT

Valeurs valides

Le préfixe ne peut pas comporter plus de 8 caractères alphanumériques ou de traits de soulignement et doit commencer par une lettre.

oltDimTableSupport

Description

Ce paramètre de configuration contrôle la capacité d'ajouter des tables de dimension aux tables des listes cibles (OLT) créées dans le schéma Deliver. Les tables de dimension sont obligatoires pour utiliser le langage de script avancé afin que les e-mails puissent créer des tableaux de données dans les messages e-mail.

Vous devez définir cette propriété sur `True` (`True` par défaut) de sorte que les spécialistes du marketing puissent créer des tables de dimension lorsqu'ils utilisent le processus Deliver pour définir une liste de destinataires. Pour plus d'informations sur la création de tables de données et l'utilisation de scripts avancés pour les e-mails, voir le Guide d'utilisation d'Unica Deliver.

Vous devez définir cette propriété sur `False`, si vous utilisez des champs de table de dimension pour la sortie dans olt et que vous souhaitez utiliser ces champs de dimension dans la communication en tant que champ de personnalisation.

Valeur par défaut

`True`

Valeurs valides

True | False

Campaign | partitions | partition[n] | server | internal

Les propriétés de cette catégorie spécifient les paramètres d'intégration et les limites d'ID interne pour la partition Campaign sélectionnée. Si votre installation de Campaign comporte plusieurs partitions, définissez ces propriétés pour chaque partition que vous souhaitez affecter.

internalIdLowerLimit

Catégorie de configuration

`Campaign|partitions|partition[n]|server|internal`

Description

Les propriétés `internalIdUpperLimit` et `internalIdLowerLimit` permettent de limiter les ID internes Campaign à une plage spécifiée. Notez que les valeurs sont inclusives : cela signifie que Campaign peut utiliser les limites supérieure et inférieure.

Valeur par défaut

`0` (zéro)

internalIdUpperLimit

Catégorie de configuration

`Campaign|partitions|partition[n]|server|internal`

Description

Les propriétés `internalIdUpperLimit` et `internalIdLowerLimit` permettent de limiter les ID internes Campaign à une plage spécifiée. Les valeurs sont inclusives : cela signifie que Campaign peut utiliser les limites supérieure et inférieure. Si Unica Collaborate est installé, définissez la valeur sur `2147483647`.

Valeur par défaut

`4294967295`

deliverInstalled

Catégorie de configuration

`Campaign|partitions|partition[n]|server|internal`

Description

Indique qu'Deliver est installé. Si vous sélectionnez `Yes`, les fonctionnalités Deliver sont disponibles dans l'interface de Campaign.

Le programme d'installation d'Unica affecte à cette propriété la valeur `Yes` pour la partition par défaut de votre installation d'Deliver. Pour les partitions

supplémentaires où vous avez installé Deliver, vous devez configurer cette propriété manuellement.

Valeur par défaut

`Non`

Valeurs valides

`Oui | Non`

Legacy_campaigns

Catégorie de configuration

`Campaign|partitions|partition[n]|server|internal`

Description

Pour cette partition, autorise l'accès aux campagnes créées avant l'intégration de Unica Plan et de Campaign. S'applique uniquement si **MO_UC_integration** a pour valeur `Yes`. Les campagnes existantes incluent également les campagnes créées dans Campaign 7.x et liées à des projets Plan 7.x. Pour plus d'informations, voir Unica Unica Plan and Campaign Integration Guide.

Valeur par défaut

Non

Valeurs valides

Oui | Non

Campaign | partitions | partition[n] | Deliver | contactAndResponseHistTracking

Utilisez les propriétés de cette catégorie pour configurer l'intégration de l'offre Deliver à Unica Campaign pour la partition en cours.

etlEnabled

Description

Campaign utilise son propre processus ETL pour extraire, transformer et charger les données de réponse à l'offre des tables de suivi Deliver dans les tables de l'historique des réponses et des contacts Campaign.

Le processus ETL coordonne les informations des tables nécessaires, y compris `UA_UsrResponseType` (types de réponse `UA_RespTypeMapping`) et Campaign (mappage de types de réponse entre Campaign et Deliver).

La définition de la valeur sur `Yes` (Oui) garantit que les informations d'historique des contacts et des réponses à l'offre Deliver sont coordonnées entre Campaign et Deliver. Par exemple, les données de réponse par courrier électronique sont incluses dans les rapportsCampaign.

Remarque : Vous devez également définir `Campaign | partitions | partition[n] | serveur | interne | DeliverInstalled` sur `Yes` (Oui) pour cette partition, faute de quoi le processus ETL ne s'exécute pas.

Conseil : Si vous souhaitez surveiller la progression du processus ETL, activez `Campaign | surveillance | monitorEnabledForDeliver`.

Valeur par défaut

`Non`

Valeurs valides

`Oui | Non`

runOnceADay

Description

Indiquez si le processus ETL doit s'exécuter une seule fois par jour.

Si la valeur est `Yes` : vous devez spécifier **startTime** ; le travail ETL s'exécute alors jusqu'à ce que tous les enregistrements soient traités et **sleepIntervalInMinutes** est ignoré.

Si la valeur est `No` : le travail ETL démarre dès que le serveur Web Campaign démarre. Le travail ETL s'arrête une fois que tous les enregistrements sont traités, puis attend le temps spécifiée par **sleepIntervalInMinutes**.

Valeur par défaut

`Non`

Valeurs valides

`Oui | Non`

batchSize

Description

Le processus ETL utilise ce paramètre pour extraire les enregistrements qui ont été téléchargés par le RCT dans les tables système Deliver locales. Etant donné que les valeurs élevées peuvent affecter les performances, la liste des valeurs disponibles est limitée aux valeurs valides indiquées ci-dessous. Si vous anticipez de grands volumes d'enregistrements, réglez **batchSize** conjointement à **sleepIntervalInMinutes** pour traiter les enregistrements à intervalles réguliers.

Valeur par défaut

`100`

Valeurs valides

100 | 200 | 500 | 1000

sleepIntervalInMinutes

Description

Spécifiez l'intervalle en minutes entre les travaux ETL. Cette option détermine le temps d'attente après la fin d'un travail. Le processus ETL attend pendant cette durée avant de démarrer le travail suivant. Plusieurs travaux peuvent s'exécuter de façon synchrone et il peut y avoir plusieurs travaux ETL par partition.

Si **runOnceADay** est `Oui`, vous ne pouvez pas définir un intervalle de veille.

Valeur par défaut

`60`

Valeurs valides

Nombres entiers positifs

startTime

Description

Indiquez une heure pour démarrer le travail ETL. Vous devez utiliser le format de paramètres régionaux anglais pour spécifier l'heure de début.

Valeur par défaut

`00:00:00`

Valeurs valides

Toute heure valide au format `hh:mm:ss AM/PM`

notificationScript

Description

Exécutable facultatif ou fichier script exécuté après chaque travail ETL effectué. Par exemple, vous pouvez demander à être averti du succès ou de l'échec de chaque travail ETL, à des fins de surveillance. Le script de notification s'exécute chaque fois que le travail ETL pour une partition donnée se termine.

Les paramètres transmis à ce script sont fixes et ne peuvent être modifiés. Les paramètres suivants peuvent être utilisés par le script :

- etlStart : heure de début d'ETL en nombre de millisecondes.
- etlEnd : heure de fin d'ETL en nombre de millisecondes.
- totalCHRecords : Nombre total d'enregistrements de contact traités.

- totalRHRecords : nombre total d'enregistrements d'historique de réponse traités.
- executionStatus : statut d'exécution d'ETL avec la valeur 1 (échoué) ou 0 (réussi).

Valeur par défaut

Aucune valeur par défaut définie.

Valeurs valides

Tout chemin valide auquel le serveur Campaign peut accéder avec les droits de lecture et d'exécution. Par exemple : `D:\myscripts\scriptname.exe`

Deliver | serverComponentsAndLocations | hostedServices

Legen Sie Eigenschaften fest, um die URLs für die Verbindung mit HCL Unica gehosteten Services anzugeben. Deliver verwendet separate Verbindungen zum Uploaden von Empfängerlisten, für Metadaten, die Empfängerlisten beschreiben, und für die allgemeine Kommunikation, die an die gehostete Umgebung gesendet wird.

Sie müssen die Standardwerte ändern, wenn Sie eine Verbindung zu HCL Unica gehosteten Services über das Rechenzentrum herstellen, das von Unica in Europa oder Indien eingerichtet wird. Wenden Sie sich bitte an Unica, um zu erfahren, mit welchem Rechenzentrum Sie verbunden sind.

uiHostName

Beschreibung

Die Adresse, die Deliver für die gesamte Kommunikation mit HCL Unica gehosteten Services verwendet, abgesehen vom Hochladen von Empfängerlisten und zugehörigen Metadaten.

Standardwert

`em.unicadeliver.com`

Wenn Sie eine Verbindung mit dem Rechenzentrum in Europa herstellen, ändern Sie diesen Wert in `em-eu.unicadeliver.com`.

Wenn Sie eine Verbindung mit dem Rechenzentrum in Indien herstellen, ändern Sie diesen Wert in `em-in.unicadeliver.com`.

dataHostName

Beschreibung

Die Adresse, die Deliver für den Upload von Metadaten verwendet, die sich auf Empfängerlisten in HCL Unica gehosteten Services beziehen.

Standardwert

`em.unicadeliver.com`

Wenn Sie eine Verbindung mit dem Rechenzentrum in Europa herstellen, ändern Sie diesen Wert in `em-eu.unicadeliver.com`.

ftpHostName

Beschreibung

Die Adresse, die Deliver für das Hochladen von Empfängerlistendaten (ausgenommen Listenmetadaten) in HCL Unica gehostete Services verwendet wird.

Standardwert

`ftp-em.unicadeliver.com`

Wenn Sie eine Verbindung zum Rechenzentrum in Europa herstellen, ändern Sie diesen Wert in `ftp-eu.unicadeliver.com`.

Wenn Sie eine Verbindung mit dem Rechenzentrum in Indien herstellen, ändern Sie diesen Wert in `em-in.unicadeliver.com`.

Wenn Sie eine Verbindung zum Rechenzentrum in Indien herstellen, ändern Sie diesen Wert in `ftp-in.unicadeliver.com`.

Deliver|serverComponentsAndLocations|Kafka|RCT

KafkaBrokerURL

Beschreibung

Verwenden Sie diese Eigenschaft, um IP und Port zu definieren, auf denen Zookeeper oder Kafka ausgeführt wird.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Jede gültige Kafka-Broker-URL.

Kommunikationmechanismus

Beschreibung

Gibt die Konfiguration für die Kafka Client-Authentifizierung an.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Auf der Seite Kafka-Konfigurationen können Sie je nach Stream-Sicherheit des Kafka-Servers Ihrer Organisation einen der folgenden Werte für das Feld CommunicationMechanism auswählen.

- NO_SASLPLAINTEXT_SSL
- SASL_PLAINTEXT
- SSL
- SASL_PLAINTEXT_SSL

sasl.mechanism

Beschreibung

Gibt die Kafka Client-Authentifizierung an.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Abhängig von den Authentifizierungskonfigurationen des Kafka-Servers können Sie einen der folgenden Werte auswählen.

- SASL_PLAINTEXT
- SASL_PLAINTEXT_SSL
- SSL

UserForKafkaDataSource

Beschreibung

Gibt den HCL Unica Benutzer an, der auf die Datenquelle verweist, die die Zugangsdaten für die Kafka-Dienste enthält. Sie können diesen Wert konfigurieren, wenn Sie einen Systembenutzer erstellen.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Jeder gültige Benutzer, der auf die Kafka-Datenquelle verweist

sasl.jaas.config.dataSource

Beschreibung

Kafka verwendet den Java Authentication and Authorization Service (JAAS) für die SASL-Konfiguration. Sie müssen JAAS-Konfigurationen für alle SASL-Authentifizierungsmechanismen bereitstellen.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Verweisen Sie auf “listener.name.sasl_ssl.plain.sasl.jaas.config” wie in kafka_home/server.properties

truststore.location

Beschreibung

Gibt den Pfad von "kafka.server.truststore.jks" an

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Pfad der Datei "kafka.server.truststore.jks", wie in kafka_home/server.properties/ssl.truststore.location erwähnt.

truststore.password.dataSource

Beschreibung

Gibt die Datenquelle von Platform an, die die Anmeldeinformationen für den Kafka-Truststore enthält. Sie können diesen Wert konfigurieren, wenn Sie einen Systembenutzer erstellen.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Pfad von "kafka.server.keystore.jks", wie in `kafka_home/server.properties/ssl.keystore.location` erwähnt.

keystore.password.dataSource

Beschreibung

Gibt die Datenquelle von Platform an, die die Anmeldeinformationen für den Kafka-Keystore enthält. Sie können diesen Wert konfigurieren, wenn Sie einen Systembenutzer erstellen.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Datenquelle, die die Anmeldeinformationen für den Kafka-Keystore enthält

key.password.dataSource

Beschreibung

Gibt die Datenquelle von Platform an, die die Anmeldeinformationen für den Kafka Schlüssel enthält. Sie können diesen Wert konfigurieren, wenn Sie einen Systembenutzer erstellen.

Standardwert

Es ist kein Standardwert definiert.

Gültige Werte

Datenquelle, die die Anmeldeinformationen für den Kafka Schlüssel enthält

ssl.endpoint.identification.algorithm

Beschreibung

Gibt den Endpunkt-Identifikationsalgorithmus an, der von Clients verwendet wird, um den Server-Hostnamen zu validieren. Deaktivieren Sie die Überprüfung des Serverhostnamens, indem Sie ssl.endpoint.identification.algorithm auf eine leere Zeichenfolge setzen.

Standardwert

leeren

Gültige Werte

Verweisen Sie auf ssl.endpoint.identification.algorithm, wie in kafka_home/server.properties erwähnt.

KafkaPartitionCount

Beschreibung

Partitionen sind der wichtigste Gleichzeitigkeitsmechanismus in Kafka. Ein Thema wird in eine oder mehrere Partitionen unterteilt, so dass Hersteller-

und Verbraucherlasten skaliert werden können. Insbesondere unterstützt eine Verbrauchergruppe so viele Verbraucher wie Partitionen für ein Thema.

Standardwert

2

Gültige Werte

Anzahl der RCT-Instanz * 2

Jede RCT-Instanz hat nur zwei Verbraucher pro Thema. Dies kann durch Vergrößerung der Kafka-Partitionen in der Konfiguration und durch Initiierung mehrerer RCT-Instanzen erhöht werden.

Ein Beispiel: Wenn es vier Kafka-Partitionen gibt, dann müssen zwei RCT-Instanzen gestartet werden. Für sechs Kafka-Partitionen müssen drei RCT-Instanzen vorhanden sein und so weiter. Jede RCT-Instanz muss auf verschiedenen Knoten ausgeführt werden. Wenn Kafka-Partitionen vergrößert werden, müssen alle RCT-Instanzen neu gestartet werden.

Replicafactor

Beschreibung

Ein Replizierungsfaktor ist die Anzahl der Kopien von Daten über mehrere Vermittler. Der Wert des Replizierungsfaktors sollte immer größer als 1 sein. Auf diese Weise wird eine Kopie der Daten in einem anderen Vermittler gespeichert, von dem aus der Benutzer auf die Daten zugreifen kann.

Standardwert

1

Gültige Werte

Die Anzahl der Kopien von Daten, die Sie bei mehreren Vermittlern aufbewahren müssen.

Deliver | partitions | partition[n] | hostedAccountInfo

Les propriétés de cette catégorie permettent de définir les données d'identification de l'utilisateur pour la base de données contenant les informations de compte nécessaires pour accéder aux services hébergés HCL Unica. Les valeurs spécifiées ici doivent être définies en tant que paramètres utilisateur dans Platform.

amUserForAcctCredentials

Description

Cette propriété permet de spécifier l'utilisateur Platform qui contient une source de données Platform définissant les données d'identification d'accès de compte requises pour accéder aux services hébergés HCL Unica.

Valeur par défaut

asm_admin

Valeurs valides

N'importe quel utilisateur Platform.

amDataSourceForAcctCredentials

Description

Utilisez cette propriété pour spécifier la source de données Platform qui définit les données d'identification de connexion pour les services hébergés HCL Unica.

Valeur par défaut

UNICA_HOSTED_SERVICES

Valeurs valides

Source de données associée à l'utilisateur spécifié dans `amUserForAcctCredentials`

Deliver | partitions | partition[n] | dataSources | systemTables

Diese Kategorie enthält Konfigurationseigenschaften, die das Schema, die Verbindungseinstellungen und die Anmeldeberechtigungsnachweise für die Datenbank definieren, die die Deliver-Systemtabellen in Ihrer Netzumgebung enthält.

Typ

Beschreibung

Typ der Datenbank, die die Deliver-Systemtabellen hostet.

Standardwert

Es ist kein Standardwert definiert. Sie müssen diese Eigenschaft definieren.

Gültige Werte

- SQLSERVER
- ORACLE
- DB2
- MARIADB
- ONEDB

schemaName

Beschreibung

Name des Datenbankschemas für die Deliver-Systemtabellen. Dieser Name ist mit dem Schemanamen für die Campaign-Systemtabellen identisch.

Sie müssen diesen Schemanamen angeben, wenn Sie in Scripts auf Systemtabellen verweisen.

Standardwert

dbo

jdbcBatchSize

Beschreibung

Die Anzahl von Ausführungsanforderungen, die JDBC in der Datenbank gleichzeitig ausführt.

Standardwert

10

Gültige Werte

Eine Ganzzahl größer 0.

jdbcClassName

Beschreibung

JDBC-Treiber für Systemtabellen anhand der Definition auf dem Campaign-Web-Server.

Standardwert

Es ist kein Standardwert definiert. Sie müssen diese Eigenschaft definieren.

jdbcURI

Beschreibung

JDBC-Verbindungs-URI für Systemtabellen anhand der Definition auf dem Campaign-Web-Server.

Standardwert

Es ist kein Standardwert definiert. Sie müssen diese Eigenschaft definieren.

asmUserForDBCredentials

Beschreibung

Verwenden Sie diese Eigenschaft, um einen HCL Unica-Benutzer anzugeben, der auf die Deliver-Systemtabellen zugreifen darf.

Standardwert

Es ist kein Standardwert definiert. Sie müssen diese Eigenschaft definieren.

Gültige Werte

Beliebiger in der Platform definierter Benutzer. Dies ist üblicherweise der Name des Systembenutzers für Campaign

amDataSourceForDBCredentials

Beschreibung

Verwenden Sie diese Eigenschaft, um die Datenquelle anzugeben, die Berechtigungsnachweise für die Datenbank definiert, die die Deliver-Systemtabellen enthält. Diese Datenquelle kann mit der Datenquelle für die Campaign-Systemtabellen identisch sein.

Standardwert

UA_SYSTEM_TABLES

Gültige Werte

Eine Platform Datenquelle, die dem in `asmUserForDBCredentials` angegebenen HCL Unica Benutzer zugeordnet ist.

Die Datenquelle gibt einen Datenbankbenutzer und Berechtigungsnachweise an, die zum Zugreifen auf die Deliver-Systemtabellen verwendet werden. Wenn das Standardschema für den Datenbankbenutzer nicht das Schema ist, das die Systemtabellen enthält, müssen Sie die Systemtabelle in den JDBC-Verbindungen angeben, die zum Zugreifen auf die Systemtabellen verwendet werden.

poolAcquireIncrement

Beschreibung

Wenn im Datenbankverbindungspool keine Verbindungen mehr verfügbar sind, ist dies die Anzahl neuer Verbindungen, die Deliver für die Systemtabellen anlegt. Deliver legt neue Verbindungen bis zu der in `poolMaxSize` angegebenen Anzahl an.

Standardwert

1

Gültige Werte

Eine Ganzzahl größer 0.

poolIdleTestPeriod

Beschreibung

Die Anzahl von Sekunden, die Deliver zwischen dem Testen von Verbindungen im Leerlauf mit den Deliver-Systemtabellen auf Aktivität wartet.

Standardwert

100

Gültige Werte

Eine Ganzzahl größer 0.

poolMaxSize

Beschreibung

Die maximale Anzahl von Verbindungen, die Deliver mit den Systemtabellen herstellt. Der Wert 0 (Null) gibt an, dass es keine maximale Anzahl gibt.

Standardwert

100

Gültige Werte

Eine Ganzzahl größer oder gleich 0.

poolMinSize

Beschreibung

Die minimale Anzahl von Verbindungen, die Deliver mit den Systemtabellen herstellt.

Standardwert

10

Gültige Werte

Eine Ganzzahl größer oder gleich 0.

poolMaxStatements

Beschreibung

Die maximale Anzahl von Anweisungen, die Deliver im PrepareStatement-Cache pro Verbindung mit den Systemtabellen speichert. Wird poolMaxStatements auf 0 (Null) gesetzt, wird das Zwischenspeichern der Anweisung inaktiviert.

Standardwert

0

Gültige Werte

Eine Ganzzahl größer oder gleich 0.

timeout

Beschreibung

Die Anzahl von Sekunden, über die Deliver eine Datenbankverbindung im Leerlauf aufrechterhält, bevor die Verbindung getrennt wird.

Wenn `poolIdleTestPeriod` größer als 0 ist, testet Deliver alle im Leerlauf und im Pool befindlichen, jedoch nicht ausgecheckten Verbindungen in einem Intervall von `timeout` Sekunden.

Wenn `poolIdleTestPeriod` größer als `timeout` ist, werden die Verbindungen im Leerlauf getrennt.

Standardwert

100

Gültige Werte

Eine Ganzzahl größer oder gleich 0.

Deliver | partitions | partition[n] | recipientListUploader

Cette catégorie de configuration comporte une propriété facultative concernant l'emplacement d'un script défini par l'utilisateur qui s'exécute en réponse aux actions ou à l'état de RLU (Recipient List Uploader - Chargeur des listes de destinataires).

pathToTriggerScript

Description

Vous pouvez créer un script qui permet de déclencher une action en réponse au transfert d'une liste de destinataires sur les services hébergés HCL Unica. Par exemple, vous pouvez créer un script pour envoyer une alerte par e-mail au concepteur de la liste lorsque le téléchargement de cette dernière est terminé.

Si vous définissez une valeur pour cette propriété, Deliver transmet des informations d'état sur RLU à l'emplacement spécifié. Deliver n'effectue aucune action si vous ne renseignez pas cette propriété.

Valeur par défaut

Aucune valeur par défaut définie.

Valeurs valides

N'importe quel chemin de réseau valide.

Deliver | partitions | partition[n] | responseContactTracker

Les propriétés de cette catégorie spécifient le comportement du Response and Contact Tracker (RCT, Suivi des réponses et des contacts). Le RCT récupère et traite les données associées aux contacts e-mail, à la réception d'e-mails et aux réponses des destinataires (par exemple, l'ouverture et la consultation de liens).

pauseCustomerPremisesTracking

Description

Deliver stocke les données de contact et de réponse dans une file d'attente des services hébergés HCL Unica. Cette propriété permet de demander à

RCT d'arrêter temporairement l'extraction des données depuis les services hébergés HCL Unica. Lorsque vous reprenez le suivi, RCT télécharge les données accumulées.

Valeur par défaut

False

Valeurs valides

True | False

waitTimeToCheckForDataAvailability

Description

Le RCT recherche régulièrement de nouvelles données relatives aux contacts e-mail ou aux réponses des destinataires. Cette propriété vous permet de spécifier la fréquence, en secondes, à laquelle RCT recherche les nouvelles données dans les services hébergés HCL Unica. La valeur par défaut est 300 secondes (toutes les 5 minutes).

Valeur par défaut

300

Valeurs valides

N'importe quel nombre entier supérieur à 1.

perfLogInterval

Description

Cette propriété vous permet de spécifier la fréquence à laquelle RCT consigne les statistiques de performances dans un fichier journal. La valeur entrée détermine le nombre de lots dans chaque entrée de journal.

Valeur par défaut

10

Valeurs valides

Un nombre entier supérieur à 0.

enableSeparatePartialResponseDataTracking

Description

Cette propriété détermine si Deliver transfère des réponses partielles par e-mail aux tables de suivi de l'installation locale Deliver.

Deliver a besoin de l'ID d'instance de mailing et du numéro de séquence de message pour affecter correctement les réponses par e-mail. Si vous activez le suivi des réponses partielles séparées, Deliver placera les réponses incomplètes dans des tables de suivi locales séparées dans lesquelles vous pourrez les modifier ou exécuter un traitement supplémentaire.

Valeur par défaut

True

Valeurs valides

True | False

enableExecutionHistoryDataTracking

Description

Cette propriété détermine si vous pouvez télécharger des données d'historique d'exécution de mailing supplémentaires à partir d'HCL Unica.

Par défaut, cette propriété a pour valeur **False** pour empêcher le chargement de données additionnelles. Quand vous affectez la valeur **True** à cette propriété, vous pouvez télécharger des données relatives à l'exécution des mailings qui ne sont généralement pas entrées dans les tables système Deliver. Vous pouvez utiliser ces informations supplémentaires pour faciliter l'automatisation de la gestion des mailings et des bases de données.

Cette propriété est masquée par défaut. Vous pouvez afficher cette propriété de configuration dans votre installation Deliver locale en exécutant le script `switch_config_visibility.bat`, situé dans le répertoire `Deliver\tools`.

L'accès aux données d'historique d'exécution des mailings est disponible sur demande chez Unica. Pour demander l'accès à d'autres données d'historique d'exécution des mailings, contactez l'équipe Unica Deliver Services via le support technique HCL.

Valeur par défaut

False

Valeurs valides

True | False

Chapter 7. Configurations pour l'implémentation de notifications Push mobiles

Introduction

Unica prend en charge les notifications Push à l'aide du SDK Kumulos, fourni sous la forme d'une infrastructure pour faciliter l'intégration à votre application iOS, Android ou multiplateforme. Ce guide fournit une présentation de la configuration de votre application au sein de vos comptes Apple Developer et Firebase Cloud Messaging avant de détailler les étapes d'intégration spécifiques pour le SDK adapté à votre projet.

L'intégration est effectuée en procédant comme suit :

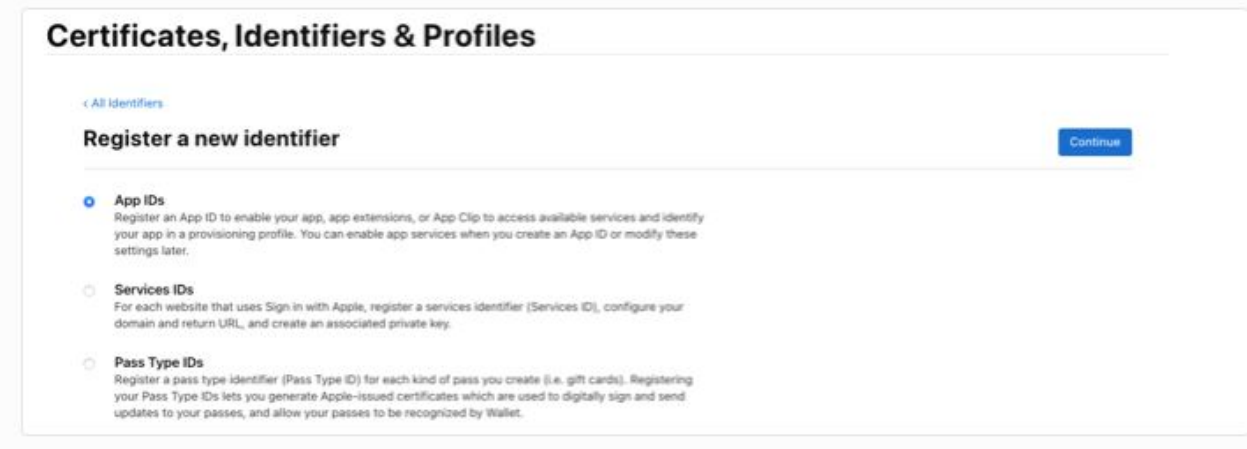
1. Configurez votre application dans votre compte Apple Developer
2. Configurez votre application dans votre compte Firebase Cloud Messaging
3. Configurez votre application Unica pour APNS et FCM en fournissant les données d'identification qui conviennent
4. Sélectionnez le SDK qui convient pour la plateforme de développement que vous avez sélectionnée

Configurer votre compte Apple Developer

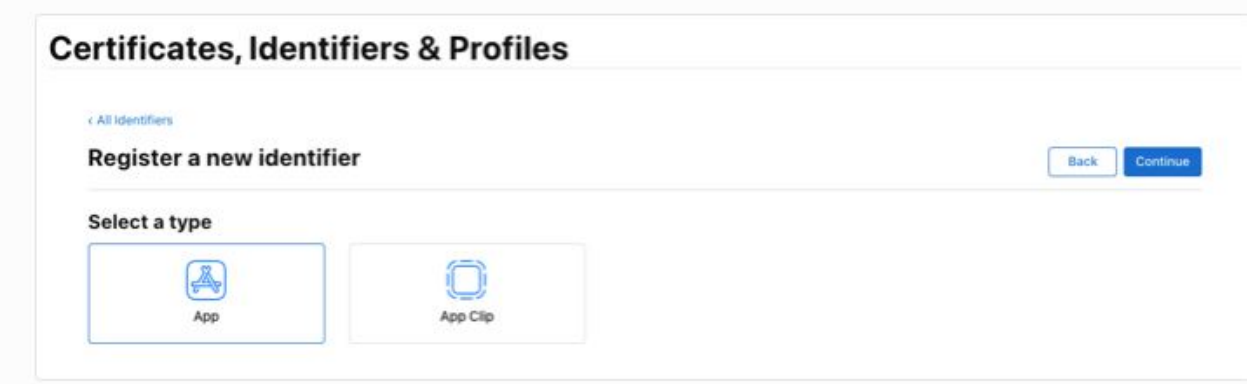
Enregistrer votre identifiant de lot et ses capacités

Pour publier votre application sur l'App Store, vous devez définir un identifiant de lot et configurer ses capacités pour autoriser les notifications push et un groupe d'applications.

Dans votre compte Apple Developer, sélectionnez « Certificats, identifiants et profils », puis « Identifiants » dans le menu de gauche. Cliquez sur l'icône + pour enregistrer votre nouvel identifiant.

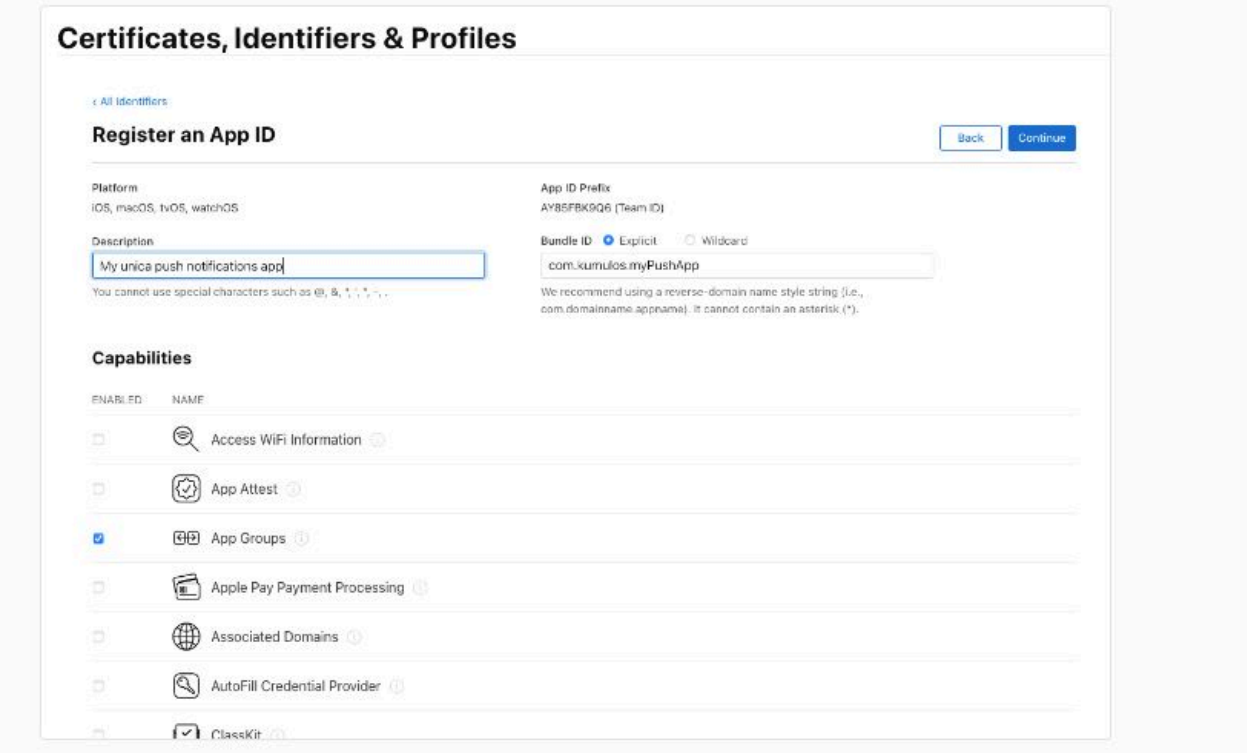


Lorsque vous êtes invité à enregistrer un nouvel identifiant, sélectionnez l'option Identifiant de l'app et cliquez sur Continuer puis, à la deuxième étape, sélectionnez le type App et cliquez à nouveau sur Continuer.



Lors de la dernière étape, vous devez configurer votre identifiant de lot et ses capacités. Votre identifiant de lot suivra généralement la norme com.[nom d'organisation].[nom de l'application] par exemple « com.kumulos.myPushApp ». Sélectionnez la case d'option 'Contenu explicite', puis entrez votre identifiant de lot qualifié complet.

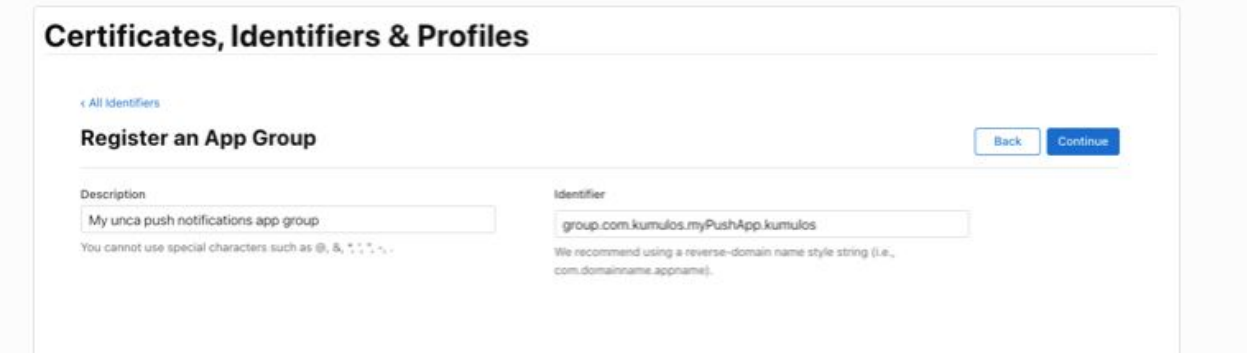
Dans la section Capacités, vérifiez que les cases « Groupes d'apps » et « Notifications push » sont cochées, puis appuyez sur Continuer.



La dernière étape de formulaire récapitulera vos informations pour les confirmer. Si tout est correct, cliquez sur « Enregistrer ».

Créer un groupe d'applications

À nouveau dans la liste Identifiants, cliquez sur l'icône + pour enregistrer un nouvel identifiant, sélectionnez le bouton d'option Groupes d'apps et cliquez sur 'Continuer'. Votre identificateur de groupe d'applications doit respecter la convention `group.{your.bundle.identifier}.kumulos`. Dans notre exemple d'identifiant de lot, il s'agit de « group.com.kumulos.myPushApp.kumulos ». Cliquez sur Continuer, et sur l'écran final si tous les détails sont corrects, cliquez sur « Enregistrer ».



Lier le groupe d'applications à votre identifiant d'application

Dans la liste Identifiants, cliquez sur votre identifiant d'application pour l'identifiant de lot qui convient. Vous pouvez également filtrer la liste pour afficher uniquement les types Identifiant d'app à l'aide du filtre en haut à droite.

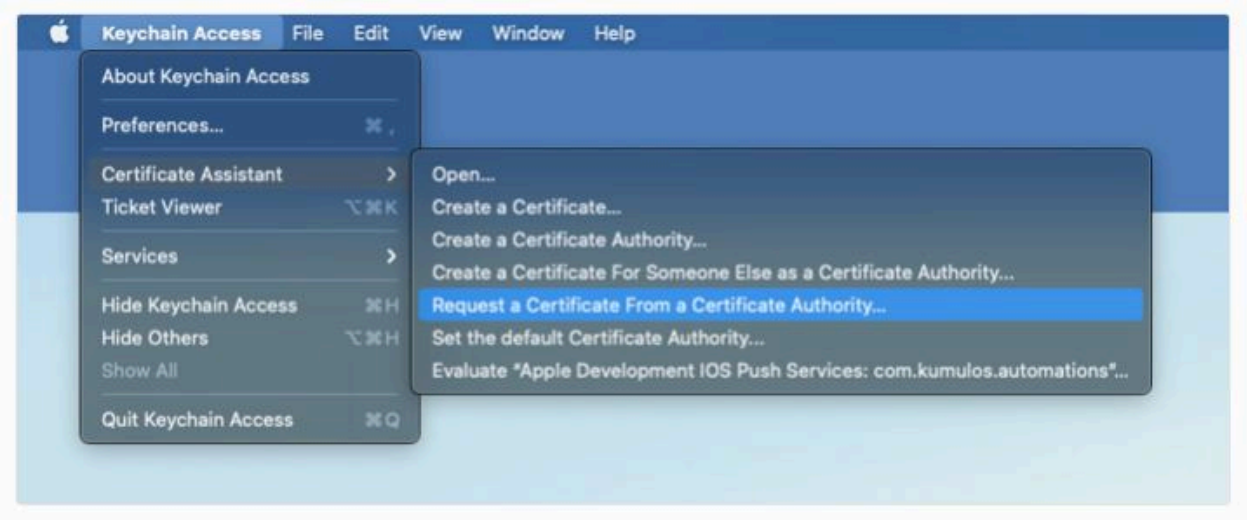
Dans l'écran « Editer la configuration de votre identifiant d'app », cliquez sur le bouton « Configurer » à côté de la capacité « Groupes d'apps ». Dans la fenêtre contextuelle, cochez la case à côté du groupe créé à l'étape précédente avec l'identifiant de lot correspondant, puis cliquez sur « Continuer ». Le texte à côté de « Groupes d'apps » dans l'écran de configuration doit maintenant être « Groupes d'apps activés (1) ». Cliquez alors sur Enregistrer.

Créer des certificats APNS

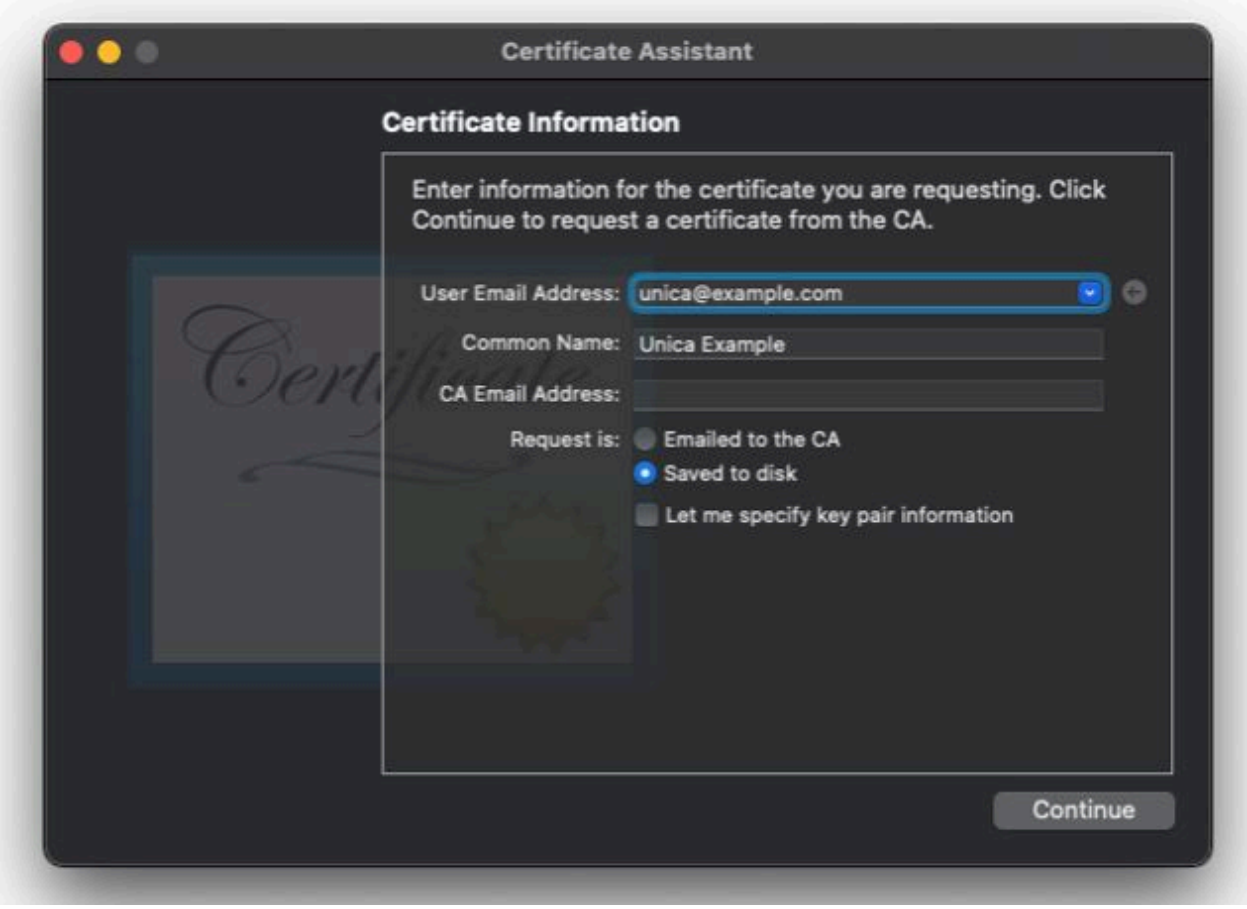
Pour envoyer des notifications Push aux périphériques iOS avec Unica, vous devrez créer des certificats dans Apple Developer Member Center afin d'enregistrer les données d'identification auprès de votre application Unica.

A la fin de cette étape, vous aurez un fichier .p12 sécurisé par mot de passe à ajouter à l'application Unica.

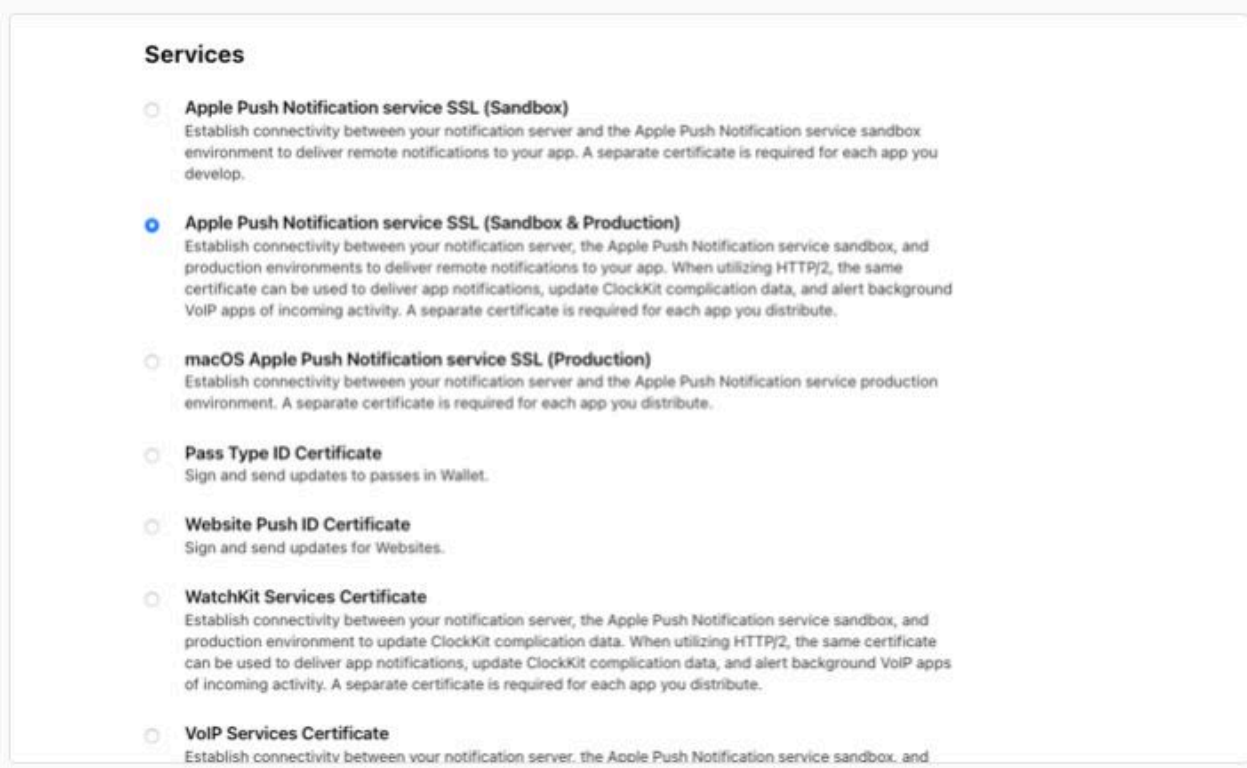
Tout d'abord, nous allons créer une demande de signature de certificat, à l'aide de Keychain Access. Accédez au menu Keychain Access depuis votre barre d'outils et sélectionnez Assistant de certificat, Demander un certificat à une autorité de certification.



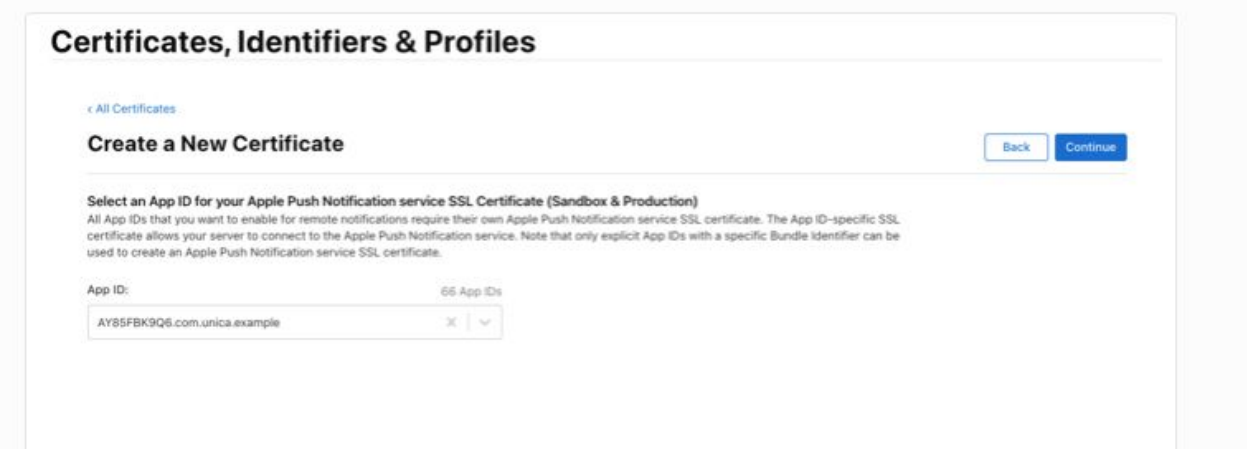
Dans la fenêtre de la boîte de dialogue, entrez votre courrier électronique dans le champ « Adresse e-mail de l'utilisateur ». Votre nom doit déjà apparaître dans le champ « Nom usuel ». Sélectionnez la case d'option 'Enregistré sur le disque' et cliquez sur 'Continuer'. Enregistrez le fichier sur votre disque pour une utilisation ultérieure.



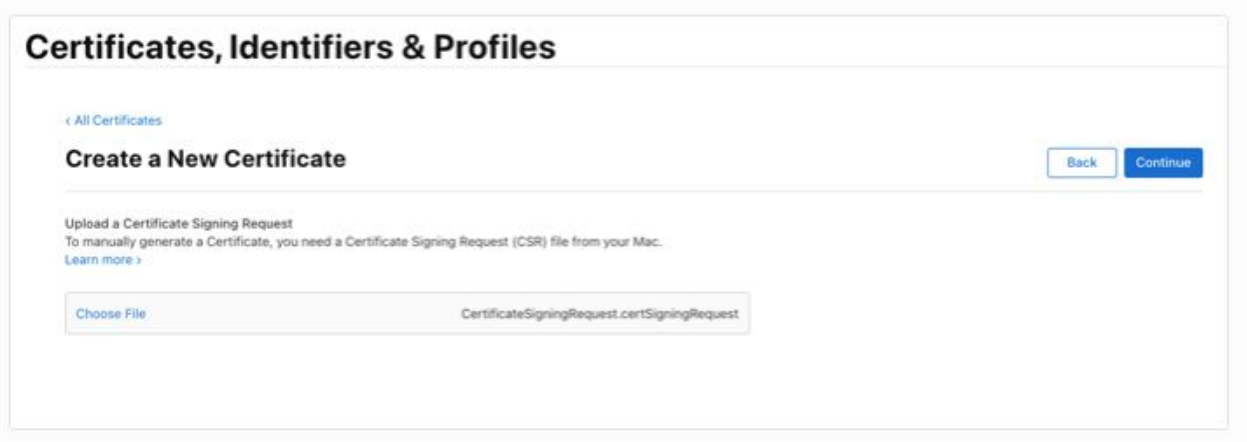
Ensuite, accédez à votre compte Apple Developer et sélectionnez « Certificats, identifiants et profils ». Sur l'écran Certificats, cliquez sur le bouton en forme de + bleu en haut de l'écran. Sur l'écran « Créer un certificat », accédez à « Services » et sélectionnez « SSL Apple Push Notification Service (Bac à sable et Production) », puis cliquez sur Continuer.



Sur l'écran suivant, sélectionnez l'identifiant d'application lors du processus de mise en route, puis cliquez sur Continuer.



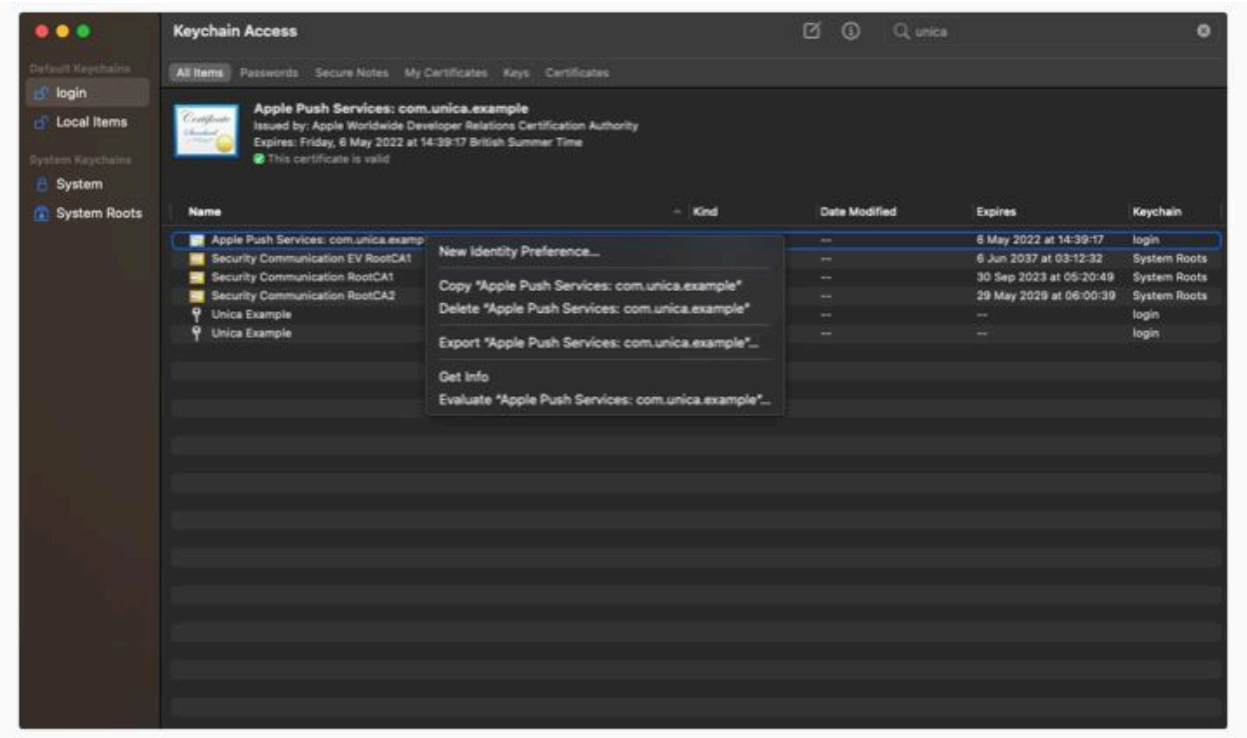
Lorsque vous êtes invité à charger une demande de signature de certificat, cliquez sur Sélectionner un fichier et rechercher, puis sélectionnez le fichier `certSigningRequest` créé précédemment et cliquez sur Continuer.



A l'étape finale, un écran vous confirmant tous les détails sélectionnés jusqu'à présent s'affiche. Cliquez ensuite sur le bouton Télécharger.

Un fichier `.cer` est alors enregistré sur votre disque local. Cliquez deux fois sur le fichier pour l'ajouter à votre Keychain Access.

Vous pouvez filtrer les résultats de votre chaîne de certificats à l'aide du filtre de texte en haut à droite. Une fois que vous avez trouvé l'élément correspondant au 'certificat' Kind avec le nom 'Apple Push Services [votre identifiant de lot]', cliquez avec le bouton droit de la souris sur l'élément et sélectionnez 'Exporter'.



Dans la nouvelle fenêtre, assurez-vous que le format de fichier sélectionné est « Personal Information Exchange (.p12) » et choisissez un emplacement pour enregistrer le fichier. Lorsque vous cliquez sur 'Enregistrer', vous devriez être invité à entrer un mot de passe pour protéger les éléments exportés. Entrez-en un et vérifiez.

Vous aurez besoin de la phrase de passe et du fichier .p12 pour configurer le système dorsal de votre application Unica.

Configurer Firebase Cloud Messaging

Pour envoyer des messages aux utilisateurs Android avec Unica, vous devez créer une application Firebase et la configurer pour Firebase Cloud Messaging.

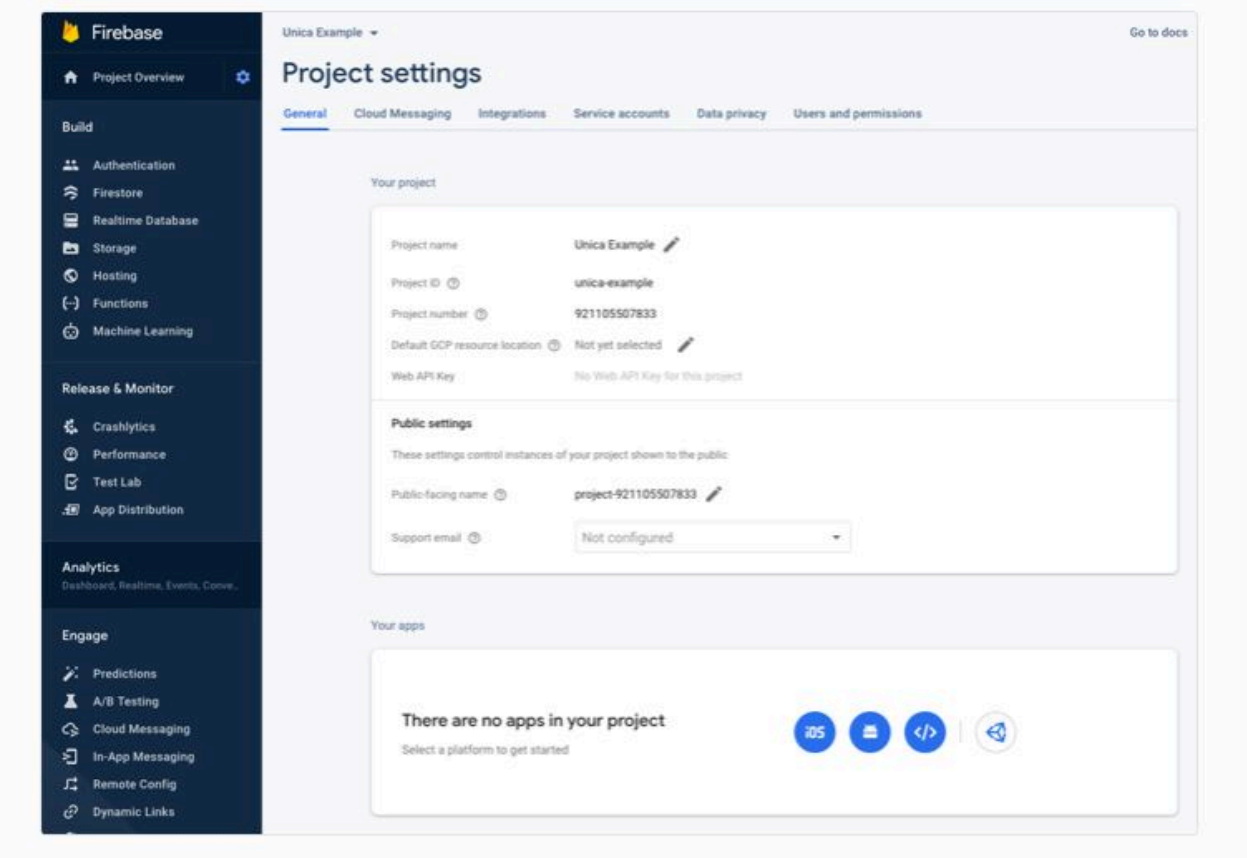
Dans cette étape, nous allons générer plusieurs artefacts utilisés pour configurer à la fois l'application Unica et votre projet d'application Android, à savoir :

- Fichier JSON Google Services
- Fichier JSON du compte Google Services
- Clé de serveur

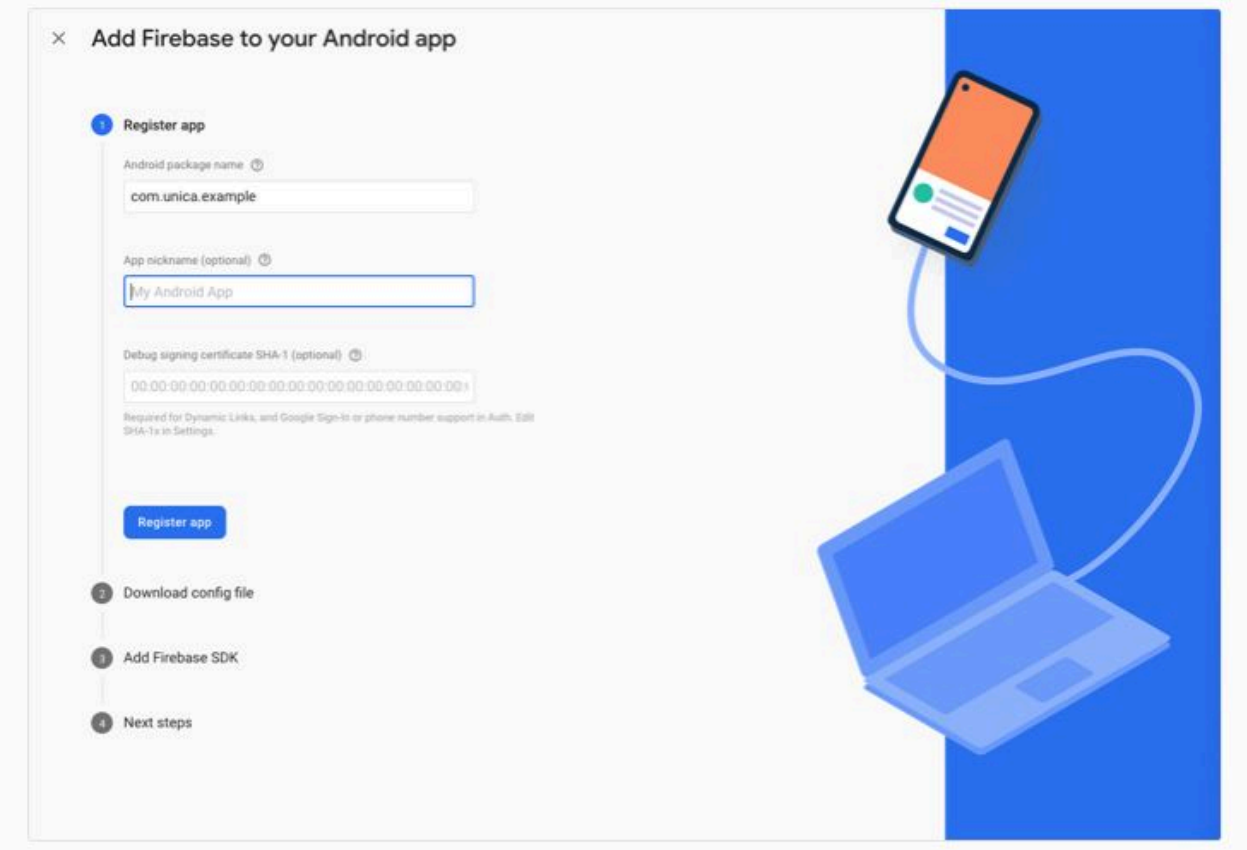
Connectez-vous d'abord à votre console Firebase, sélectionnez « Ajouter un projet » et entrez le nom de votre projet dans l'assistant. Vous pouvez choisir ou non Google Analytics pour votre projet, cela n'affectera pas l'intégration.

Enfin, la console Firebase va créer votre application. Une fois le processus de configuration terminé, cliquez sur Continuer.

Ensuite, nous allons ajouter une application Android au projet Firebase. Dans l'écran de présentation du projet, cliquez sur le rouage de configuration à côté de 'Présentation du projet', puis sur 'Paramètres du projet'

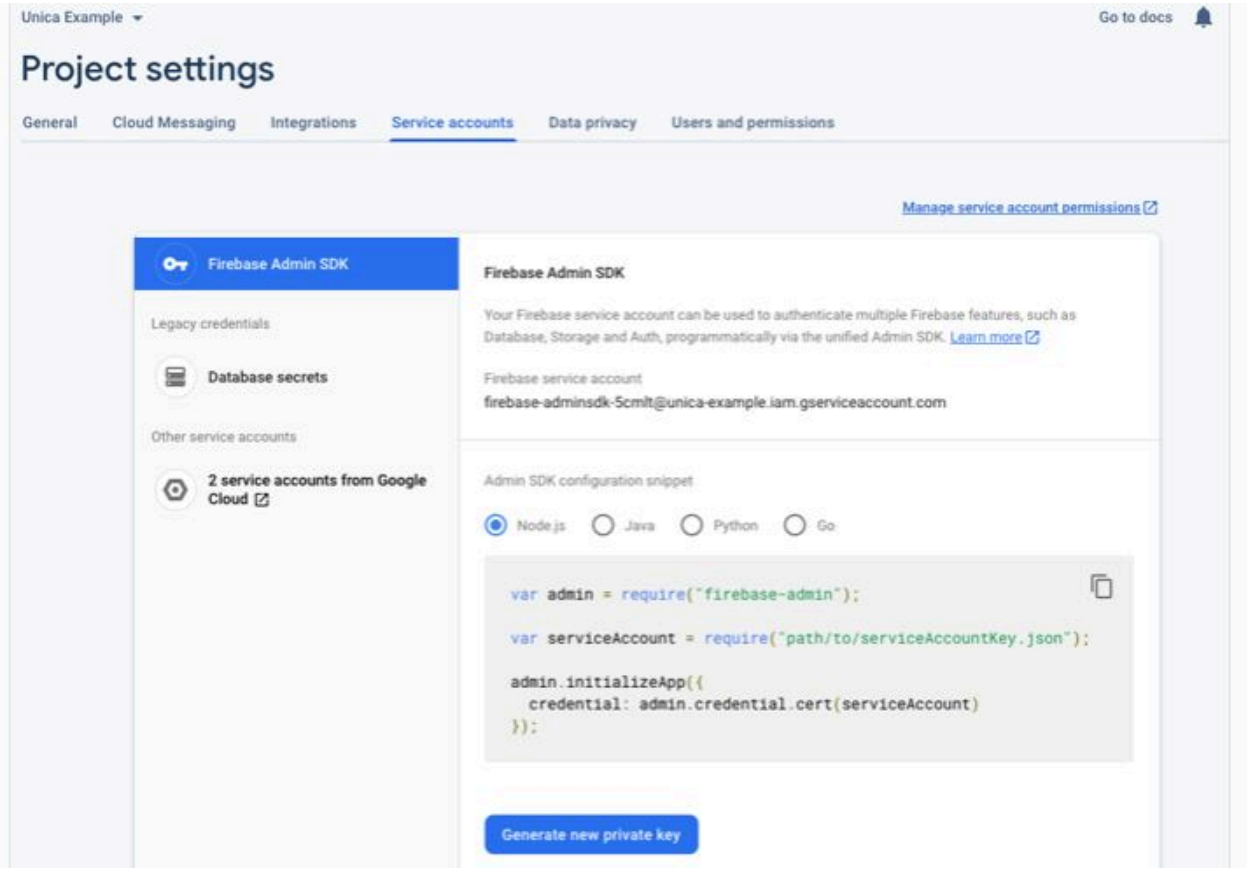


Dans l'onglet 'Général' du panneau 'Vos applications', cliquez sur l'icône pour Android. L'assistant permettant de créer l'application s'ouvre alors.



Entrez le nom du package de votre application dans la fenêtre supérieure et cliquez sur 'Enregistrer l'application'. Le JSON Google Services sera téléchargé automatiquement et utilisé ultérieurement lors de l'intégration du SDK à votre projet Android.

Sélectionnez l'onglet de messagerie cloud et copiez la clé de serveur pour pouvoir vous y référer ultérieurement. Elle sera utilisée pour configurer l'application Unica.



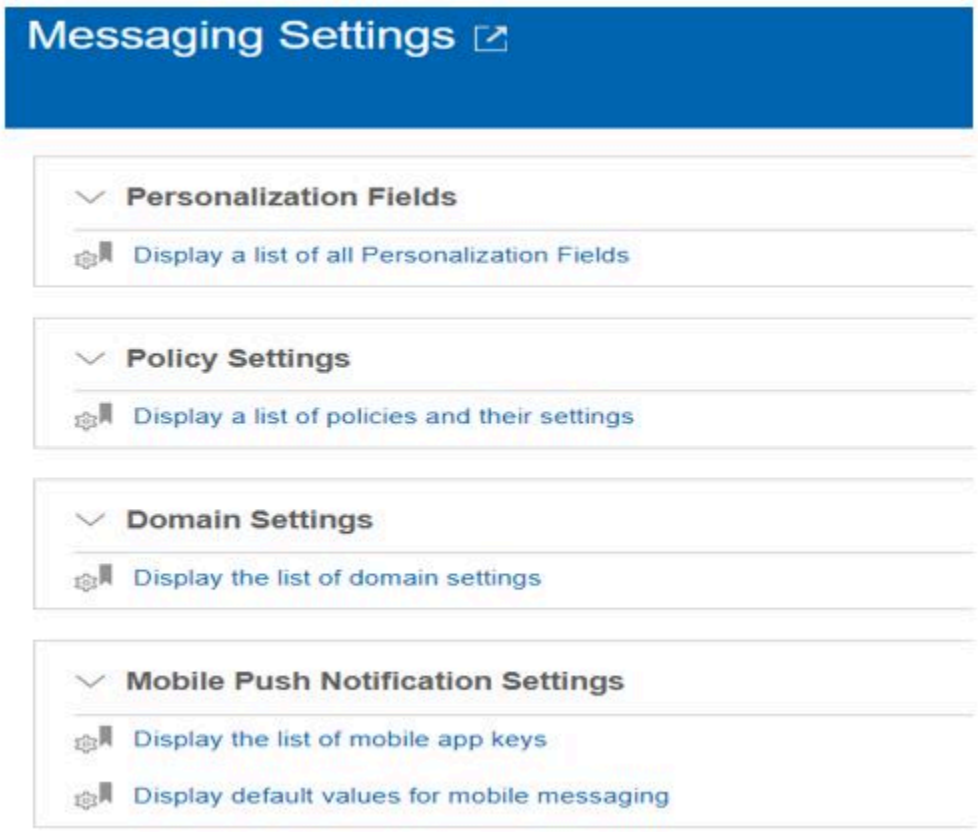
Ensuite, cliquez sur l'onglet « Comptes de service », puis sur « Générer une nouvelle clé privée ». Un fichier JSON décrivant vos données d'identification de compte sera alors téléchargé. Vous en aurez aussi besoin pour configurer votre application Unica.

Vous aurez besoin du fichier JSON des comptes du service, mais aussi de la clé de serveur pour configurer le système dorsal de votre application Unica.

Configurer votre application Unica

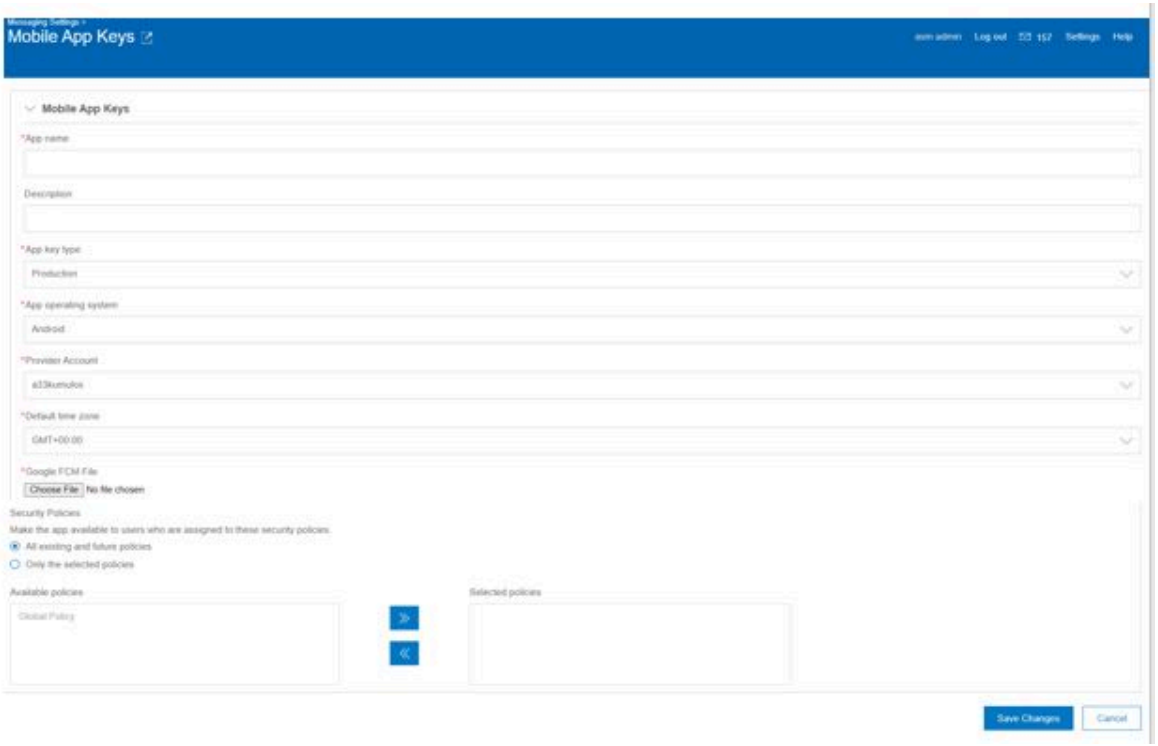
Procédez comme suit.

1. Dans **Paramètres**, sélectionnez **Paramètres de messagerie**. Vous devriez voir l'option « Paramètres de notification Push mobile » sur la page suivante. Si ce n'est pas le cas, contactez le support Unica pour activer cette option.



2. Cliquez sur **Afficher la liste des clés d'application mobile**. La page suivante s'affiche.

3. Cliquez sur **Ajouter une clé d'application mobile**. La page suivante s'affiche.



4. Remplissez le formulaire avec les valeurs appropriées.
    - Nom de l'application : Nom de l'application
    - Description : Description de l'application
    - Type de clé d'application – Le type doit être « production ».
    - Système d'exploitation de l'application : Android ou iOS. La valeur dépend des utilisateurs que vous ciblez.
    - Compte du fournisseur : Il est récupéré à partir du système dorsal Unica en fonction des comptes créés.
    - Fuseau horaire par défaut : Peut être choisi en fonction de l'emplacement.
    - Fichier FCM Google : Fournissez un fichier JSON de compte de service Google pour l'application mobile.

    Si vous choisissez IOS dans « Système d'exploitation de l'application », vous verrez ce qui suit au lieu de « Fichier FCM Google ».

- Fichier du certificat : Spécifiez le fichier p12 pour l'application iOS.
- Mot de passe du certificat : Fournissez le mot de passe du certificat p12.
- Stratégies de sécurité : Faites votre choix en fonction des stratégies à appliquer à l'application.

5. Cliquez sur **Enregistrer** pour créer l'application mobile. Vous pouvez voir l'application sur la page de liste. Le message « Réussite du chargement du fichier » fournit le statut du chargement du fichier FCM/P12, que vous avez fourni dans le formulaire.

Intégrer le SDK

Sélectionnez le SDK qui convient pour la plateforme de développement que vous avez sélectionnée

Natif

- iOS Swift *(on page 98)*
- Android *(on page 107)*

Multiplateforme

- React Native *(on page 125)*

iOS Swift

Einführung

Das Kumulos SDK ist ein Open Source-Projekt, das auf Github gehostet wird und unter https://github.com/Kumulos/KumulosSdkSwift zu finden ist.

In diesem Handbuch wird davon ausgegangen, dass Sie die Schritte aus dem Configurations pour l'implémentation de notifications Push mobiles *(on page 85)* ausgeführt und Ihren Apple Identifier, die Funktionen und das Bereitstellungsprofil in diesem Handbuch konfiguriert haben. Die folgenden Integrationsschritte werden behandelt:

1. SDK integrieren und Projekt für APNS-Funktionalität konfigurieren
2. SDK-Komponenten in Ihrem Projekt initialisieren und für Push-Benachrichtigungen registrieren
3. Registrieren der Kumulos-Installations-ID in Ihrem Backend, um eine Verbindung zwischen dem Gerät und Ihren in Ihrem CRM-Backend dargestellten Benutzern für die spätere Ausrichtung von Benachrichtigungen herzustellen.
4. Senden Sie eine Test-Push-Benachrichtigung von Ihrer Unica-App und empfangen auf dem Gerät.
5. Benutzerdefinierte Analyseereignisse
6. Optional erweitertes Verhalten für native Push Benachrichtigungen
7. Optional erweitertes Verhalten für umfangreiche In-App Nachrichten

Integration

Im GitHub-Repository sind sowohl Anweisungen zur Integration von Carthage als auch CocoaPods verfügbar.

Erste Schritte mit CocoaPods

Erste Schritte mit Carthage

Befolgen Sie einfach die Anweisungen Ihres bevorzugten Abhängigkeitsmanagers, um das KumulosSDK-Framework zum Projekt hinzuzufügen.

Benachrichtigungsserviceerweiterung hinzufügen

Um alle Funktionen des Apple Push-Benachrichtigungsdienstes zu unterstützen, muss Ihre App über eine Erweiterung für den Benachrichtigungsdienst verfügen, um eine eingeschränkte Verarbeitung der Benachrichtigung beim Empfang zu ermöglichen, bevor das Betriebssystem sie dem Benutzer präsentiert.

Dies ist ein zweites Build-Ziel, das Ihrem vorhandenen xcode-Projekt hinzugefügt wird, indem Sie zu Ihrem Projektinfobildschirm gehen und in der Fußzeile auf die Schaltfläche '+' klicken.

Wählen Sie im Popup-Fenster die Vorlage `Erweiterung des Benachrichtigungsdienstes` für Ihr neues Projekt aus und klicken Sie auf „Weiter“.

Fügen Sie im letzten Fenster einen geeigneten Namen für Ihre Erweiterung hinzu und klicken Sie auf 'Fertigstellen'.

Wenn Sie CocoaPods verwenden, fügen Sie Folgendes zu Ihrem Podfile hinzu und führen Sie `pod install` aus.

Durch die Vorlage für das Projekt wird automatisch eine Datei mit dem Namen `NotificationService.swift` erstellt, deren Inhalt durch die folgenden Zeilen ersetzt wird:

Die Kumulos SDK-Hilfsfunktionen fügen dem Benachrichtigungsinhalt automatisch Bildanhänge und Schaltflächen hinzu.

.

App-Funktionalitäten und -Berechtigungen konfigurieren

Verwenden Sie in den App-Projekteinstellungen die Schaltfläche "+ Funktionalität", um die Funktionen für App-Gruppen, Hintergrundmodi und Push-Benachrichtigungen hinzuzufügen.

Verwenden Sie in Ihrer Benachrichtigungserweiterung die Schaltfläche "+ Funktionalität", um die Funktion "App-Gruppen" hinzuzufügen.

In beiden Projekten sollte die App-Gruppen-Funktion so konfiguriert werden, dass sie dieselbe Gruppe gemeinsam nutzen kann. Dies muss genau mit der Gruppe übereinstimmen, die zuvor in Ihren Kennungsfunktionen definiert wurde.

`group.{your.bundle.identifier}.kumulos`

In Ihrem App-Projekt sollte für die Hintergrundmodi der Modus "Fernbenachrichtigungen" aktiviert sein.

Vorgehensweise zum Testen Ihrer Konfiguration

An diesem Punkt können Sie testen, ob Ihre App auf einem Gerät bereitgestellt wird, um sicherzustellen, dass Ihre Berechtigungen und Funktionen richtig konfiguriert sind.

Initialisierung (Initialization)

Um das SDK für die Verwendung zu konfigurieren, das Sie mit den Berechtigungsnachweisen Ihrer App initialisieren müssen, sollte dies zu einem früh bei Ihrem Anwendungsstart durchgeführt werden.

Das Kumulos SDK unterstützt automatisch Abzeichen, Schaltflächen und Bildinhalte. Beachten Sie jedoch, dass aufgrund von iOS-Einschränkungen keine Abzeichen festgelegt werden, wenn die App im Vordergrund steht.

Für Push-Benachrichtigungen registrieren

Für iOS ist eine explizite Benutzerberechtigung erforderlich, um Benachrichtigungen zu empfangen. Wenn Sie es für geeignet halten, können Sie die Eingabeaufforderung zum Zulassen von Benachrichtigungen auslösen, indem Sie folgendes aufrufen:

```
Kumulos.pushRequestDeviceToken()
```

Dieser Helper fordert das Betriebssystem auf, den Benutzer auf zu bitten, Push-Benachrichtigungen mit der Signalabzeichen-, Warnungs- und Tonoptionen zu akzeptieren.

Wenn der Benutzer akzeptiert, übernimmt das Kumulos SDK automatisch die Registrierung des Push-Tokens beim Kumulos-Backend.

Registieren Ihres CRM

Bei der erstmaligen Initialisierung erstellt das Kumulos SDK eine eindeutige Kennung für die App-Installation, die das SDK initialisiert hat. Diese Kennung kann später verwendet werden, um Push-Benachrichtigungen auf ein bestimmtes Gerät auszurichten.

Um diese Installations-ID abzurufen, greifen Sie einfach auf die Klassenvariable zu:

```
let installId = Kumulos.installId;
```

Sobald Sie die Installations-ID haben, können Sie sie an das CRM-Backend Ihrer App senden, um sie später für das Push-Targeting zu verwenden.

Verknüpfen Sie Ihren App-Benutzer optional mit Kumulos für das Targeting

Wenn Ihre App eine Kennung verwendet, um eindeutig zu bestimmen, welcher Benutzer bei einem Gerät angemeldet ist (z. B. eine Primärschlüssel-Ganzzahl oder UUID oder eine E-Mail-Adresse), können Sie diese Kennung für ein späteres Push-Targeting über denselben Schlüssel an Kumulos senden.

```
Kumulos.associateUserWithInstall(userIdentifier: "unique-user-identif
```

Ereignisverfolgung

Mit Kumulos können Sie benutzerdefinierte Analyse-Ereignisse verfolgen, um die Aktivitäten Ihrer Benutzer in Ihrer App zu beobachten. So können Sie das Verhalten analysieren und

die Journeys optimieren, um sicherzustellen, dass Ihre Benutzer den vollen Nutzen aus den Funktionen Ihrer App ziehen.

Um ein benutzerdefiniertes Analyseereignis zu verfolgen, verwenden Sie `Kumulos.trackEvent` wie folgt:

Jedes Ereignis und seine Eigenschaften müssen weniger als 250 KB groß sein, damit das Ereignis nachverfolgt werden kann.

Die Ereignisverfolgung ist offline verfügbar, da alle Ereignisse lokal gespeichert werden, bevor sie stapelweise im Hintergrund mit dem Server synchronisiert werden.

Eine ähnliche Methode `trackEventImmediately`startet sofort eine Ereignissynchronisation, anstatt auf das nächste Mal zu warten, wenn die App im Hintergrund läuft.

Fonctions avancées

Gestion des événements ouverts de notification

Lorsqu'un utilisateur interagit avec votre message Push, en appuyant soit sur la notification elle-même, soit sur un bouton d'action inclus, `pushOpenedHandlerBlock` sera appelé. Dans ce bloc, vous pouvez indiquer un comportement supplémentaire pour gérer les actions personnalisées.

```
let builder = KSConfigBuilder(apiKey: "your-api-key", secretKey: "you
    .setPushOpenedHandler(pushOpenedHandlerBlock: { (notification : K
        //- Inspect notification data and do work.
        if let action = notification.actionIdentifier {
            print("User pressed an action button.")
            print(action)
            print(notification.data)
        } else {
            print("Just an open event.")
        }
    })

Kumulos.initialize(config: builder.build())
```

Gestion des Push de données d'arrière-plan

Lorsque vous envoyez un Push avec l'indicateur `content-available` défini sur la notification, votre application peut être activée pour traiter la notification Push en arrière-plan, ce qui déclenche tout comportement requis dans votre application sans la lancer en avant-plan.

Si vous définissez un titre et un message, la notification sera silencieuse et rien ne sera affiché pour l'utilisateur dans le centre de notification. Toutefois, vous pouvez également fournir un titre et un message afin de déclencher le comportement, puis en notifier l'utilisateur.

L'indicateur `content-available` déclenchera le délégué d'application `application:didReceiveRemoteNotification:fetchCompletionHandler:`. A partir de là, vous pouvez inspecter la charge de la notification et effectuer toute action requise.

```
// iOS9 handler for push notifications
// iOS9+10 handler for background data pushes (content-available)
func application(_ application: UIApplication, didReceiveRemoteNotifi
        // userInfo["aps"]["content-available"] will be set to 1
        // userInfo["custom"]["a"] will contain any additional data s

        completionHandler(UIBackgroundFetchResult.noData)
    }
```

Erweiterte In-App Funktionen

In-App-Benutzerinhalte verwalten

Wenn Sie Ihre Benutzer für den Empfang von In-App-Nachrichten anmelden möchten, können Sie das SDK während der Initialisierung so konfigurieren, dass die Anmeldung explizit erfolgt, indem Sie die Strategie festlegen und dann den SDK-Helper aufrufen, um die Zustimmung zu verwalten.

Deep-Linking für In-App

Mit In-App Nachrichten können Sie über Deep-Link Aktionsschaltflächen an native Anwendungsbildschirme übergeben. Wenn sie angetippt werden, übergeben diese Schaltflächen die Kontrolle an den definierten Deep-Link-Handler, einschließlich ihrer definierten Daten-Nutzlast (konfiguriert im In-App Message Composer für die Aktionsschaltfläche).

Wenn Sie Deep-Links mit benutzerdefinierten Datennutzlasten als Teil einer In-App-Nachricht behandeln möchten, können Sie während der SDK-Initialisierung einen Handler-Block zu Ihren Konfigurationsoptionen hinzufügen.

```
let builder =KSConfigBuilder(apiKey:"your-api-key", secre
```

Verwendung des In-App-Posteingangs

In-App-Nachrichten können optional für einen späteren Abruf in einem Posteingang auf Benutzerebene gespeichert werden. So können Sie Funktionen wie Prämien oder ablaufende Gutscheine in Ihre App integrieren. Unabhängig davon, ob sie im Posteingang gespeichert sind, können maximal 50 In-Apps auf einem Gerät gespeichert werden (die ältesten Nachrichten, die diese Grenze überschreiten, werden entfernt).

Nachrichten abrufen

Um eine Nachrichtenliste aus dem Posteingang des Benutzers abzurufen und die erste in der Liste anzuzeigen, siehe das folgende Beispiel:

Als gelesen markieren

Um eine einzelne oder alle Posteingangsnachrichten als gelesen zu markieren:

Nachricht löschen

Sie können auch eine In-App-Nachricht aus dem Posteingang löschen:

Posteingang aktualisierter Handler

Um benachrichtigt zu werden, wenn sich der Posteingang ändert, können Sie einen Handler einrichten. Der Handler wird im Haupt-Thread ausgelöst, wenn eines der folgenden Ereignisse bei einer In-App mit Posteingang eintritt:

- Nachricht vom Server abgerufen
- Nachricht geöffnet
- Nachricht als gelesen markiert
- Nachricht gelöscht
- Nachricht entfernt (abgelaufen oder die Grenze der gespeicherten Nachrichten überschritten)

Sie können es wie folgt verwenden:

Eine Zusammenfassung des Posteingangs erhalten

Sie können die Zusammenfassung des Posteingangs wie folgt abrufen:

Die Methode wird asynchron ausgeführt und ruft den Haupt-Thread zurück.

Rufen Sie die Bild-URL des Posteingangselements ab

Jedem Posteingangselement kann ein Bild zugeordnet sein. `getImageUrl` gibt eine URL zum Bild mit der angegebenen Breite oder `nil` zurück, wenn kein Bild vorhanden ist.

Android

Einführung

Das Kumulos SDK ist ein Open Source-Projekt, das auf Github gehostet wird und unter https://github.com/Kumulos/KumulosSdkAndroid zu finden ist.

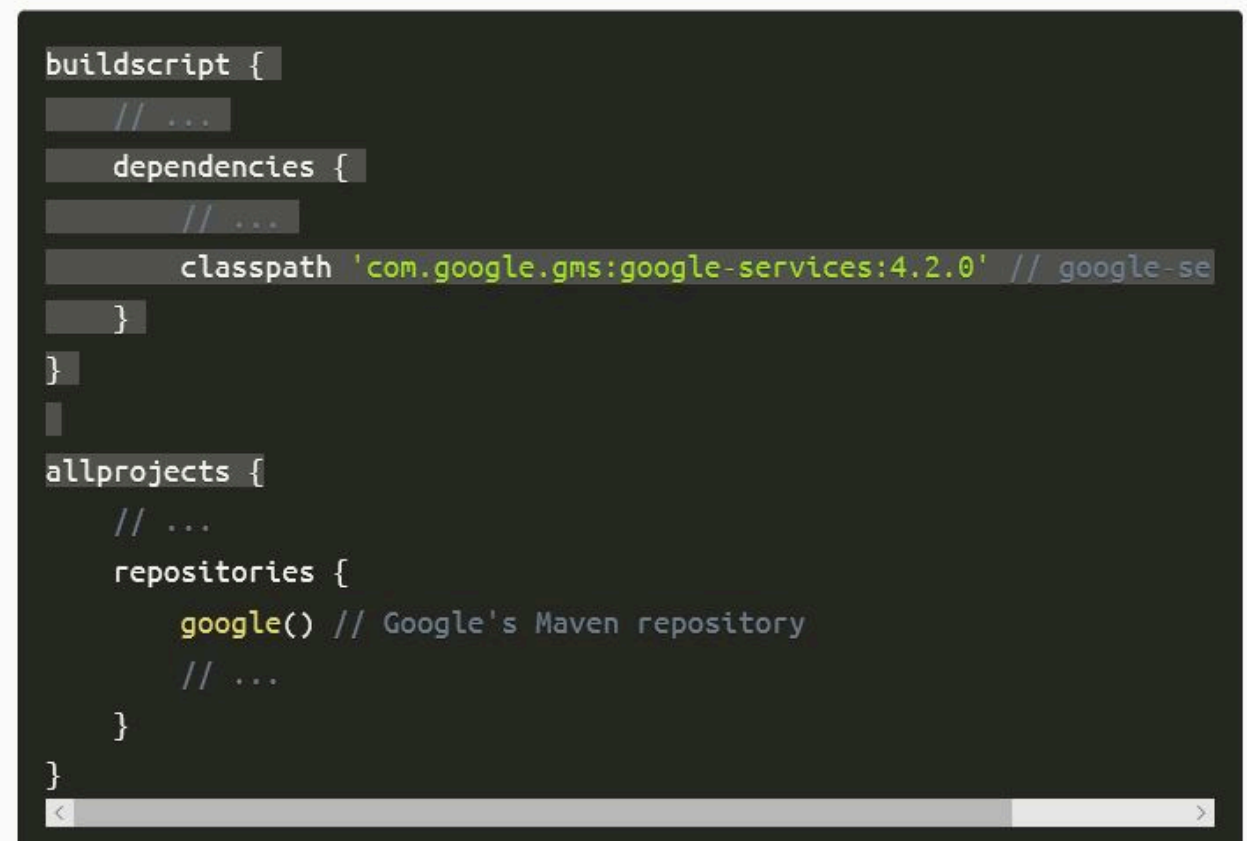
In diesem Handbuch wird davon ausgegangen, dass Sie die Schritte von Configurations pour l'implémentation de notifications Push mobiles (on page 85) aus ausgeführt und Ihre Firebase Console und Unica App mit den entsprechenden Anmeldeinformationen für Cloud Messaging konfiguriert haben. Es deckt die folgenden Schritte ab:

1. Integration des SDK und Konfiguration Ihres Projekts.
2. SDK-Komponenten in Ihrem Projekt initialisieren und für Push-Benachrichtigungen registrieren
3. Registrieren der Kumulos-Installations-ID in Ihrem Backend, um eine Verbindung zwischen dem Gerät und Ihren in Ihrem CRM-Backend dargestellten Benutzern für die spätere Ausrichtung von Benachrichtigungen herzustellen.
4. Senden Sie eine Test-Push-Benachrichtigung von Ihrer Unica-App und empfangen auf dem Gerät.
5. Benutzerdefinierte Analyseereignisse
6. Optional erweitertes Verhalten für native Push Benachrichtigungen
7. Optional erweitertes Verhalten für umfangreiche In-App Nachrichten

Integration

Firebase-Komponenten hinzufügen zu Ihrer App, wie unten gezeigt.

Stellen Sie im **root** `build.gradle`, dass das Google-Repository aktiviert ist und sich das Google Services-Plugin im Klassenpfad befindet:



```
buildscript {
    // ...
    dependencies {
        // ...
        classpath 'com.google.gms:google-services:4.2.0' // google-se
    }
}

allprojects {
    // ...
    repositories {
        google() // Google's Maven repository
        // ...
    }
}
```

Die Kumulos-Bibliotheken werden über JCenter verteilt. Um die Bibliotheken zu installieren, bearbeiten Sie die Datei `build.gradle` Ihrer App und fügen Sie Folgendes hinzu:

- In Konflikt stehende Metadatendateien vom Build ausschließen
- Kompilierungsoptionen für Quelle und Ziel deklarieren
- Kumulos-Bibliotheksabhängigkeiten hinzufügen
- Firebase-Kern-SDK hinzufügen
- Google-Services-Plug-in anwenden

Ein Beispiel für `build.gradle` ist unten zu sehen.

```
android {
    // Exclude duplicate files from the build
    packagingOptions {
        exclude 'META-INF/NOTICE'
        exclude 'META-INF/ASL2.0'
        exclude 'META-INF/LICENSE'
    }

    compileOptions {
        sourceCompatibility JavaVersion.VERSION_1_8
        targetCompatibility JavaVersion.VERSION_1_8
    }
}

apply plugin: 'com.android.application'

dependencies {
    // Kumulos debug & release libraries
    debugImplementation 'com.kumulos.android:kumulos-android-debug:11
    releaseImplementation 'com.kumulos.android:kumulos-android-releas
    implementation 'com.google.firebase:firebase-core:16.0.7'
}

// ADD THIS AT THE BOTTOM
apply plugin: 'com.google.gms.google-services'
```

Das `debugImplementation` hat die Protokollierung mit einem Tag aktiviert, das mit `com.kumulos.*` übereinstimmt. Bei der Ausführung im Debugmodus sollten die Protokollnachrichten in LogCat sichtbar sein.

Führen Sie eine Gradle-Synchronisation aus, um die Kumulos-Bibliotheken zu installieren und Ihr Projekt zu erstellen.

Standardmäßig sendet Firebase SDK Analysedaten an Google. Um dies zu deaktivieren, fügen Sie einfach

```
<meta-data android:name="firebase_analytics_collection_deactivated"
 android:value="true" />
```

zur `AndroidManifest.xml` Ihrer App hinzu

Laden Sie die Datei `google-services.json` aus den „Allgemeinen“ Einstellungen Ihrer Firebase-App herunter und fügen Sie diese Ihrem Ordner `app/` hinzu.

Jetzt können Sie den Kumulos `FirebaseMessagingService` und `PushBroadcastReceiver` zu Ihrer `AndroidManifest.xml` hinzufügen.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example">

    <!-- Optionally add the wake lock permission to stop the CPU from
    <!-- <uses-permission android:name="android.permission.WAKE_LOCK"
    <!-- Optionally add the boot completed permission to allow period
    <!-- <uses-permission android:name="android.permission.RECEIVE_BO

   <!-- Set the android:name to your custom Application class -->
    <application
        android:name=".ExampleApp"
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:supportsRtl="true"
        android:theme="@style/AppTheme">
        ...
        </application>

        ...

        <!-- Kumulos FCM handler -->
        <service android:name="com.kumulos.android.FirebaseMessagingS
            <intent-filter>
                <action android:name="com.google.firebase.MESSAGING_E
            </intent-filter>
        </service>

        <!-- Kumulos Push receiver -->
        <receiver android:name="com.kumulos.android.PushBroadcastRece
            <intent-filter>
                <action android:name="com.kumulos.push.RECEIVED" />
                <action android:name="com.kumulos.push.OPENED" />
                <action android:name="com.kumulos.push.DISMISSED" />
                <action android:name="com.kumulos.push.BUTTON_CLICKED
            </intent-filter>
        </receiver>
    </application>

</manifest>
```

Initialisierung und Registrierung für Push-Benachrichtigungen

Um das SDK zu initialisieren, empfehlen wir, die Klasse `Anwendung` in Unterklassen zu unterteilen und Kumulos in seiner `onCreate` Methode zu initialisieren.

Wenn Sie die Registrierung der Installation aufheben möchten, können Sie `Kumulos.pushUnregister(context)` verwenden.

.

Registrieren mit dem CRM

Installations-ID

Bei der erstmaligen Initialisierung erstellt das Kumulos SDK eine eindeutige Kennung für die App-Installation, die das SDK initialisiert hat. Diese Kennung kann später verwendet werden, um Push-Benachrichtigungen auf ein bestimmtes Gerät auszurichten.

Um diese Installations-ID abzurufen, greifen Sie einfach auf die Klassenvariable zu:

```
String id = com.kumulos.android.Installation.id(context);
```

Sobald Sie die Installations-ID haben, können Sie sie an das CRM-Backend Ihrer App senden, um sie später für das Push-Targeting zu verwenden.

Verknüpfen Sie Ihren App-Benutzer optional mit Kumulos für das Targeting

Wenn Ihre App eine Kennung verwendet, um eindeutig zu bestimmen, welcher Benutzer bei einem Gerät angemeldet ist (z. B. eine Primärschlüssel-Ganzzahl oder UUID oder eine E-Mail-Adresse), können Sie diese Kennung für ein späteres Push-Targeting über denselben Schlüssel an Kumulos senden.

```
Kumulos.associateUserWithInstall(context, "unique-user-identifier");
```

Erweiterte Features

Verarbeitung von Schaltflächen für Push-Aktionen

Mit Push-Nachrichten können Sie über Deep-Link-Push-Aktionsschaltflächen an native Anwendungsbildschirme übergeben. Beim Tippen übergeben diese Schaltflächen die Steuerung an den definierten Push-Aktionshandler.

Wenn Sie Deep-Links als Teil einer Push-Nachricht verarbeiten möchten, können Sie eine Klasse erstellen, die `PushActionHandlerInterface` implementiert und diese während der SDK-Initialisierung zuteilt.

```
Kumulos.setPushActionHandler(new MyPushActionHandler());
```

Eine Stub-Implementierung des Handlers kann wie folgt lauten:

```
public class MyPushActionHandler implements PushActionHandlerInterfac
    public void handle(Context context, PushMessage pushMessage, Stri
        //- actionId is the button id you set when creating the notifi
        //- Note, that when action button is clicked your app's activi
    }
}
```

Push-Standardverhalten

Standardmäßig zeigt Kumulos `PushBroadcastReceiver` eine Benachrichtigung im Benachrichtigungsbereich des Geräts an, wenn eine Inhalts-Push-Benachrichtigung empfangen wird.

Durch Antippen dieser Benachrichtigung wird die Hauptstarteraktivität Ihrer Anwendung geöffnet und die Push-Konvertierung wird für Sie verfolgt.

Ihre Hauptaktivität erhält den Push-Inhalt im Optionspaket unter der `PushMessage.EXTRAS_KEY`.

Push-Symbol ändern

Um das Symbol zu ändern, das in der Statusleiste unter Android angezeigt wird, können Sie Kumulos während der Initialisierung mit einem Drawable konfigurieren:

```
KumulosConfig config = new KumulosConfig.Builder("API_KEY", "SECRET_K
    .setPushSmallIconId(R.id.my_push_small_icon)
    .build();
Kumulos.initialize(this, config);
```

Stellen Sie sicher, dass Sie die Richtlinien für Statusleisten-Symbole einhalten, damit das Symbol auf allen Geräten korrekt wiedergegeben wird. Um Hilfe bei der Vorbereitung von Assets zu erhalten, empfehlen wir Ihnen, das Android Asset Studio zu besuchen.

Push-Verhalten anpassen

Um das Verhalten des SDK anzupassen, wenn ein Push empfangen oder auf seine Benachrichtigung getippt wird, empfehlen wir, die `PushBroadcastReceiver` zu unterklassifizieren und ihre Basismethoden zu überschreiben, je nachdem, was Sie anpassen möchten.

Beispiel für Erweiterungsklasse:

```
package com.example;

import com.kumulos.android.PushBroadcastReceiver;

public class MyPushReceiver extends PushBroadcastReceiver {

}
```

Ändern Sie unbedingt den `AndroidManifest.xml` Empfänger:

```
<receiver android:name="com.example.MyPushReceiver" android:exported=
    <intent-filter>
        <action android:name="com.kumulos.push.RECEIVED" />
        <action android:name="com.kumulos.push.OPENED" />
        <action android:name="com.kumulos.push.DISMISSED" />
        <action android:name="com.kumulos.push.BUTTON_CLICKED" />
    </intent-filter>
</receiver>
```

Gestartete Aktivität ändern

Um zu ändern, welche Aktivität gestartet wird, wenn der Benutzer eine Benachrichtigung antippt, können Sie

```
PushBroadcastReceiver#getPushOpenActivityIntent(Context, PushMessage)
```

überschreiben.

```
package com.example;

import android.content.Context;
import android.content.Intent;

import com.kumulos.android.PushBroadcastReceiver;
import com.kumulos.android.PushMessage;

public class MyPushReceiver extends PushBroadcastReceiver {

    @Override
    protected Intent getPushOpenActivityIntent(Context context, PushM
        // TODO implement your own logic here
        return super.getPushOpenActivityIntent(context, pushMessage);
    }
}
```

Das `PushMessage` Modell wird der standardmäßig nicht zum `Intent` hinzugefügt. Sie können es bei Wunsch als Zusatz hinzufügen:

```
Intent launchIntent = new Intent(context, MyActivity.class);
launchIntent.putExtra(PushMessage.EXTRAS_KEY, pushMessage);
```

Sie können `null` zurückgeben, um die Push-Konvertierung zu verfolgen, und nichts tun, wenn auf die Benachrichtigung getippt wird.

Wenn die zurückgegebene `Intent` nicht eine `Aktivität` beschreibt, wird sie ignoriert.

Die Benachrichtigung anpassen

Um die dem Benutzer angezeigte Benachrichtigung für Inhalts-Pushes anzupassen, können Sie `PushBroadcastReceiver#buildNotification(Context, PushMessage)` überschreiben.

```
package com.example;

import android.app.Notification;
import android.content.Context;

import com.kumulos.android.PushBroadcastReceiver;
import com.kumulos.android.PushMessage;

public class MyPushReceiver extends PushBroadcastReceiver {

    @Override
    protected Notification buildNotification(Context context, PushMes
        // TODO customize the notification
        return super.buildNotification(context, pushMessage);
    }
}
```

Wenn Sie die Offenen/Benachrichtigungen mit dem Broadcast-Empfänger bearbeiten möchten, stellen Sie sicher, dass Sie die Inhaltsabsichten der Benachrichtigung wie folgt einrichten:

```
PendingIntent pendingOpenIntent = PendingIntent.getBroadcast(
        context,
        pushMessage.getId(),
        openIntent,
        PendingIntent.FLAG_UPDATE_CURRENT | PendingIntent.FLAG_ONE_SH

...

notificationBuilder.setContentIntent(pendingOpenIntent);

//Similarly
Intent dismissedIntent = new Intent(PushBroadcastReceiver.ACTION_PUSH

dismissedIntent.putExtra(PushMessage.EXTRAS_KEY, pushMessage);
dismissedIntent.setPackage(context.getPackageName());

PendingIntent pendingDismissedIntent = PendingIntent.getBroadcast(
        context,
        pushMessage.getId(),
        dismissedIntent,
        PendingIntent.FLAG_UPDATE_CURRENT | PendingIntent.FLAG_ONE_SH

...

notificationBuilder.setDeleteIntent(pendingDismissedIntent);
```

Dadurch wird sichergestellt, dass die Benachrichtigungskonvertierung in Kumulos verfolgt wird.

Wenn Sie etwas anderes erreichen wollen, können Sie die Umwandlung von Push Open mit `Kumulos#pushTrackOpen(Context, int)` und das Ereignis "abgewiesen" mit `Kumulos#pushTrackDismissed(Context, int)` manuell verfolgen. Darüber hinaus müssten Sie Deep Link-Extras für In-App-Nachrichten-Deep Links hinzufügen, um weiterarbeiten zu können.

```
Kumulos.pushTrackOpen(context, pushMessage.getId());
Kumulos.pushTrackDismissed(context, pushMessage.getId());
//call in the scope of MyPushReceiver
addDeepLinkExtras(pushMessage, launchIntent);
```

Starten eines Dienstes für Hintergrunddaten-Pushs

Um einen Dienst zu starten, wenn eine Push-Benachrichtigung im Hintergrund empfangen wird, können Sie `PushBroadcastReceiver#getBackgroundPushServiceIntent` überschreiben.

```
package com.example;

import android.content.Context;
import android.content.Intent;

import com.kumulos.android.PushBroadcastReceiver;
import com.kumulos.android.PushMessage;

public class MyPushReceiver extends PushBroadcastReceiver {

    @Override
    protected Intent getBackgroundPushServiceIntent(Context context,
        // TODO implement your own logic here
        return super.getBackgroundPushServiceIntent(context, pushMess
    }
}
```

Auf diese Weise können Sie die Datenverarbeitung ohne Weiteres im Hintergrund verarbeiten, indem Sie beispielsweise einen `IntentService` starten.

Das `PushMessage` Modell wird der standardmäßig nicht zum `Intent` hinzugefügt. Sie können es bei Wunsch als Zusatz hinzufügen:

```
Intent serviceIntent = new Intent(context, MyIntentService.class);
serviceIntent.putExtra(PushMessage.EXTRAS_KEY, pushMessage);
```

Geben Sie `null` zurück, wenn Sie nichts mit der Daten-Push machen möchten.

Wenn die zurückgegebene `Intent` nicht eine `Service`beschreibt, wird sie ignoriert.

URL-Pushes

Push-Benachrichtigungen, die zum Öffnen einer URL gesendet werden, öffnen standardmäßig den Standard-Webbrowser.

Alle Verhaltensweisen überschreiben

Wenn Sie die Logik für die Verarbeitung von Push-Benachrichtigungen vollständig ersetzen möchten, können Sie `PushBroadcastReceiver#onPushReceived(Context, PushMessage)` überschreiben.

Denken Sie daran, dass Sie für alle Aspekte des Push-Prozesses verantwortlich sind, z. B. das Anzeigen einer Benachrichtigung an den Benutzer, das Verfolgen einer offenen Konvertierung mit `Kumulos#pushTrackOpen(Context, int)` und das Abweisen von Ereignissen mit `Kumulos#pushTrackDismissed(Context, int)` oder das Starten von Aktivitäten oder Diensten.

Darüber hinaus müssen Sie möglicherweise Verhaltensweisen implementieren für:

- Lieferverfolgung: `pushTrackDelivered(context, pushMessage)`

Verwenden eigener `FirebaseMessagingService` mit Kumulos

Wenn Sie FCM-Push-Benachrichtigungen bereits mit Ihrer eigenen `FirebaseMessagingService` verwenden, aber auch die Vorteile des Kumulos-Push-Dienstes nutzen möchten, können Sie die Hilfsmethoden des SDK in Ihrer eigenen Implementierung verwenden. Zum Beispiel:

```
public class MyAppFirebaseMessagingService extends com.google.firebas

    @Override
    public void onNewToken(String token) {
        // Handle token for your purposes
        // ...
        // Also pass token to Kumulos for registration
        Kumulos.pushTokenStore(this, token);
    }

    @Override
    public void onMessageReceived(RemoteMessage remoteMessage) {
        // Handle message as you wish
        // ...
        // Hand over to Kumulos if not of interest / came from the Ku
        com.kumulos.android.FirebaseMessageHandler.onMessageReceived(
    }
}
```

Ereignisverfolgung

Mit Kumulos können Sie benutzerdefinierte Analyse-Ereignisse verfolgen, um die Aktivitäten Ihrer Benutzer in Ihrer App zu beobachten. So können Sie das Verhalten analysieren und die Journeys optimieren, um sicherzustellen, dass Ihre Benutzer den vollen Nutzen aus den Funktionen Ihrer App ziehen.

Um ein benutzerdefiniertes Analyseereignis zu verfolgen, verwenden Sie `Kumulos.trackEvent` wie folgt:

Jedes Ereignis und seine Eigenschaften müssen weniger als 250 KiB groß sein, damit das Ereignis nachverfolgt werden kann.

Die Ereignisverfolgung ist offline verfügbar, da alle Ereignisse lokal gespeichert werden, bevor sie stapelweise im Hintergrund mit dem Server synchronisiert werden.

Eine ähnliche Methode `trackEventImmediately` startet sofort eine Ereignissynchronisierung, anstatt darauf zu warten, dass die App das nächste Mal in den Hintergrund läuft.

Erweiterte In-App Funktionen

Wenn Sie Ihre Benutzer für den Empfang von In-App-Nachrichten anmelden möchten, können Sie das SDK während der Initialisierung so konfigurieren, dass die Anmeldung explizit erfolgt, indem Sie die Strategie festlegen und dann den SDK-Helper aufrufen, um die Zustimmung zu verwalten.

Deep-Linking für In-App

Mit In-App Nachrichten können Sie über Deep-Link Aktionsschaltflächen an native Anwendungsbildschirme übergeben. Wenn sie angetippt werden, übergeben diese Schaltflächen die Kontrolle an den definierten Deep-Link-Handler, einschließlich ihrer definierten Daten-Nutzlast (konfiguriert im In-App Message Composer für die Aktionsschaltfläche).

Wenn Sie Deep-Links mit benutzerdefinierten Datennutzlasten als Teil einer In-App-Nachricht verarbeiten möchten, können Sie eine Klasse erstellen, die das `InAppDeepLinkHandlerInterface` implementiert, und es Ihren Konfigurationsoptionen während der SDK-Initialisierung hinzufügen:

Verwenden Sie den In_App Posteingang

In-App-Nachrichten können optional für einen späteren Abruf in einem Posteingang auf Benutzerebene gespeichert werden. So können Sie Funktionen wie Prämien oder ablaufende Gutscheine in Ihre App integrieren. Unabhängig davon, ob sie im Posteingang

gespeichert sind, können maximal 50 In-Apps auf einem Gerät gespeichert werden (die ältesten Nachrichten, die diese Grenze überschreiten, werden entfernt).

Nachrichten abrufen

Um eine Nachrichtenliste aus dem Posteingang des Benutzers abzurufen und die erste in der Liste anzuzeigen, siehe das folgende Beispiel:

Als gelesen markieren

Um eine einzelne oder alle Posteingangsnachrichten als gelesen zu markieren:

Nachricht löschen

Sie können auch eine In-App-Nachricht aus dem Posteingang löschen:

Posteingang aktualisierter Handler

Um benachrichtigt zu werden, wenn sich der Posteingang ändert, können Sie einen Handler einrichten. Der Handler wird im UI-Thread ausgelöst, wenn eines der folgenden Ereignisse bei einer In-App mit Posteingangskonfiguration eintritt:

- Nachricht vom Server abgerufen
- Nachricht geöffnet
- Nachricht als gelesen markiert
- Nachricht gelöscht
- Nachricht entfernt (abgelaufen oder die Grenze der gespeicherten Nachrichten überschritten)

Sie können es wie folgt verwenden:

Beachten Sie, dass Sie `KumulosInApp.setOnInboxUpdated(null)` ausführen können, wenn Sie nicht mehr an Posteingangs-Updates interessiert sind.

Eine Zusammenfassung des Posteingangs erhalten

Sie können die Zusammenfassung des Posteingangs wie folgt abrufen:

Rufen Sie die Bild-URL des Posteingangselements ab

Jedem Posteingangselement kann ein Bild zugeordnet sein. `getImageUrl` gibt eine URL zum Bild mit der angegebenen Breite oder `null` zurück, wenn kein Bild vorhanden ist.

Fehlerbehebung

Proguard

Wenn Sie ProGuard verwenden, um Ihren Java-Code zu optimieren, müssen Sie sicherstellen, dass Ihre Datei `proguard.cfg` das Kumulos SDK und die erforderlichen Komponenten enthält, z. B.:

```
-keep class com.google.android.gms.** { *; }
-dontwarn com.google.android.gms.
-keep class com.google.firebase.** { *; }
-dontwarn com.google.firebase.
-keep class android.support.v7.widget.** { *; }
-dontwarn android.support.v7.widget.
-keep class android.support.v4.widget.Space { *; }
-dontwarn android.support.v4.widget.Space
-keep class com.kumulos.** { *; }
-dontwarn com.kumulos.**
-keep class okhttp3.** { *;}
-dontwarn okhttp3.**
-keep class oikio.** { *;}
-dontwarn okio.**
```

Proguard reagiert auch sehr empfindlich auf UTF-8 mit Stücklistencodierung, während Android-Werkzeuge nur UTF-8 akzeptieren. Eine einfache Möglichkeit, um sicherzustellen, dass Sie nicht versehentlich UTF-8-Bytereihenfolgen in Ihrem `proguard.cfg` haben, besteht darin, vim über das Terminal wie folgt zu verwenden:

```
$ vim proguard.cfg
:set nobomb
:wq!
```

React Native

Einführung

Das Kumulos SDK ist ein Open Source-Projekt, das auf Github gehostet wird und unter https://github.com/Kumulos/KumulosSdkReactNative zu finden ist.

In diesem Handbuch wird davon ausgegangen, dass Sie die Schritte aus der Einführung ausgeführt und Ihr Projekt über das Apple Developer-Konto und die Firebase Console konfiguriert haben. Es umfasst die folgenden Schritte:

1. Integrieren des SDK und konfigurieren Ihrer Projekte für die APNS/FCM-Funktionalität.
2. SDK-Komponenten in Ihrem Projekt initialisieren und für Push-Benachrichtigungen registrieren
3. Registrieren der Kumulos-Installations-ID in Ihrem Backend, um eine Verbindung zwischen dem Gerät und Ihren in Ihrem CRM-Backend dargestellten Benutzern für die spätere Ausrichtung von Benachrichtigungen herzustellen.
4. Senden Sie eine Test-Push-Benachrichtigung von Ihrer Unica-App und empfangen auf dem Gerät.
5. Benutzerdefinierte Analyseereignisse
6. Optional erweitertes Verhalten für native Push Benachrichtigungen
7. Optional erweitertes Verhalten für umfangreiche In-App Nachrichten

Integration

Das Kumulos React Native-Modul erfordert native Funktionen und sollte daher in einem ausgeworfenen Projekt installiert werden.

Führen Sie die folgenden Befehle aus, um das Projekt zu installieren und zu verknüpfen:

```
npm install kumulos-react-native --save
pod install --project-directory=ios
```

Für jede Plattform sind manuelle Verknüpfungsschritte erforderlich.

Android-Verknüpfungsschritte

Um den Verknüpfungsprozess für Android zu vervollständigen, müssen Sie sicherstellen, dass Ihr Projekt die folgenden Versionen für Werkzeuge und Bibliotheken verwendet:

- Gradle-Plug-in v3.1.3 oder höher
- Build-Tools ab Version 23.0.3
- Unterstützungsbibliothek v27.+

Platzieren Sie das während der Einführung erstellte `google-services.json` im Android/App-Verzeichnis Ihres Projekts. Darüber hinaus müssen Sie Ihrer `android/app/build.gradle` Datei Folgendes hinzufügen:

```
android {
    // ...
    packagingOptions {
        exclude 'META-INF/NOTICE'
        exclude 'META-INF/ASL2.0'
        exclude 'META-INF/LICENSE'
    }

    dependencies {
    // Kumulos debug & release libraries
        classpath 'com.google.gms:google-services:4.2.0'
    }

    // ADD THIS AT THE BOTTOM
    apply plugin: 'com.google.gms.google-services'
}
```

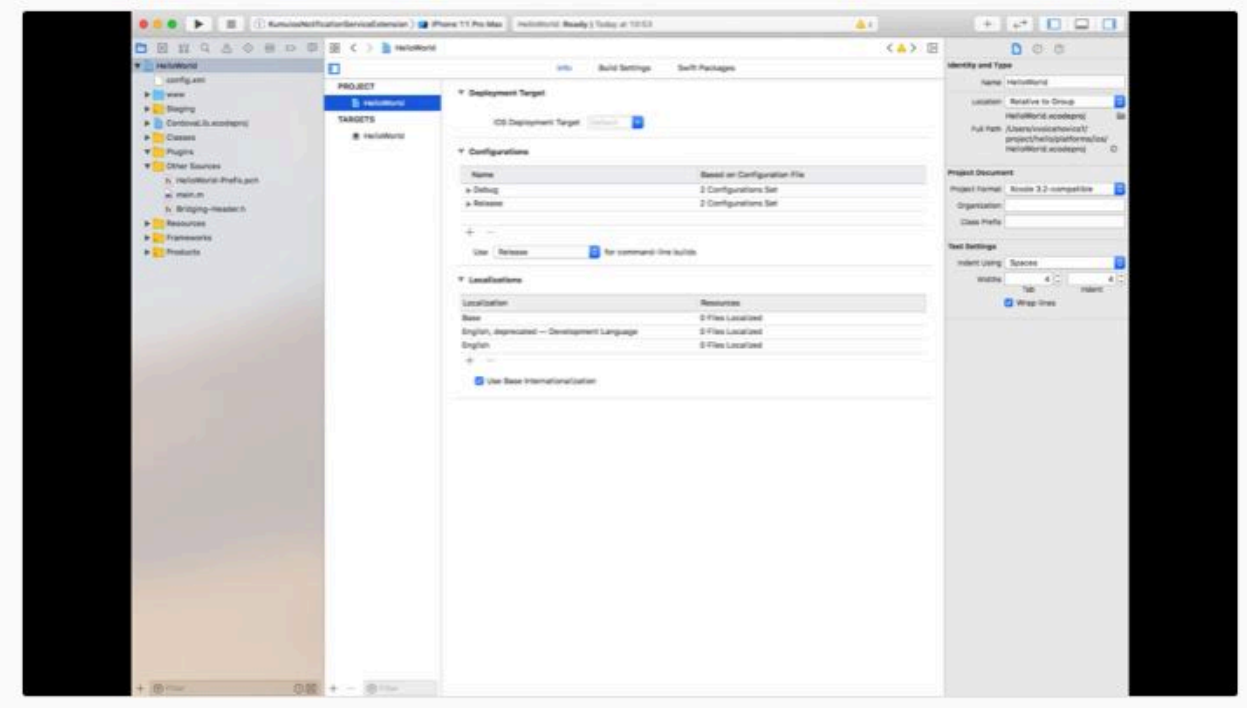
iOS-Projektkonfiguration

Die Benachrichtigung wird erweitert, wenn Sie die Benachrichtigung auf Geräten wischen, die 3D Touch unterstützen. Um diese Funktionalität zu aktivieren, müssen Sie Ihr iOS-Projekt in Xcode öffnen und Ihrer Anwendung eine Benachrichtigungsdiensterweiterung hinzufügen.

Benachrichtigungsserviceerweiterung hinzufügen

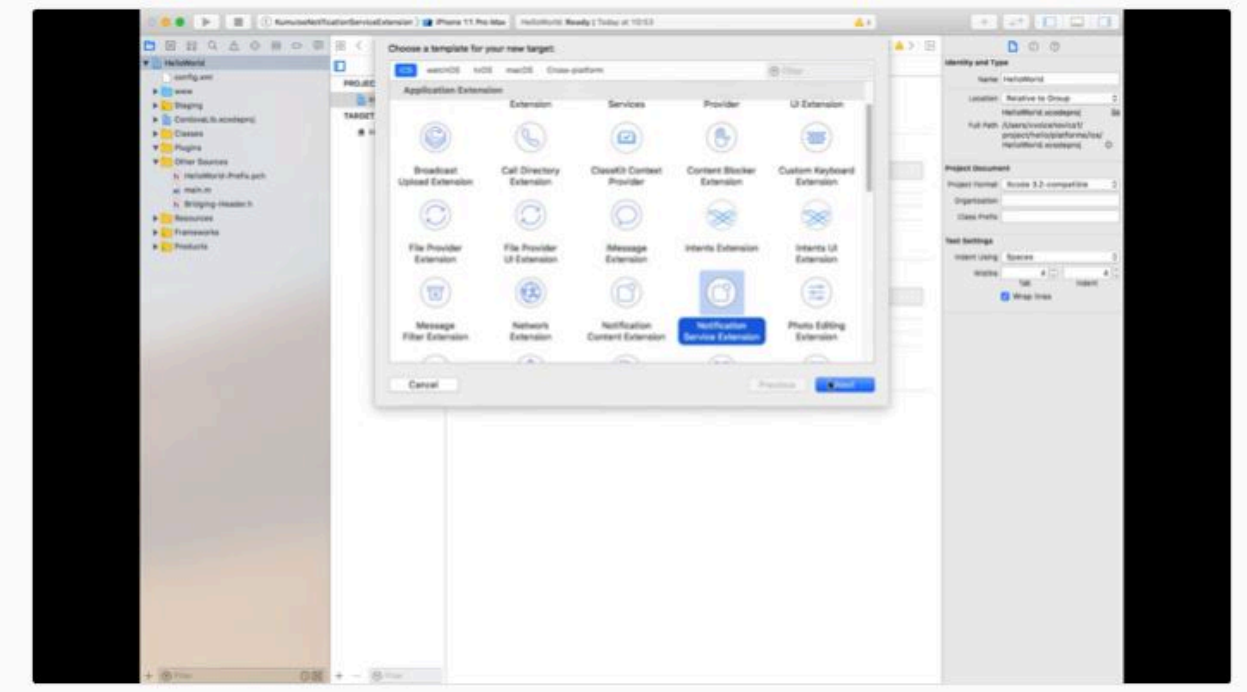
Um alle Funktionen des Apple Push-Benachrichtigungsdienstes zu unterstützen, muss Ihre App über eine Erweiterung für den Benachrichtigungsdienst verfügen, um eine eingeschränkte Verarbeitung der Benachrichtigung beim Empfang zu ermöglichen, bevor das Betriebssystem sie dem Benutzer präsentiert.

Dies ist ein zweites Build-Ziel, das Ihrem vorhandenen xcode-Projekt hinzugefügt wird, indem Sie zu Ihrem Projektinfobildschirm gehen und in der Fußzeile auf die Schaltfläche '+' klicken.

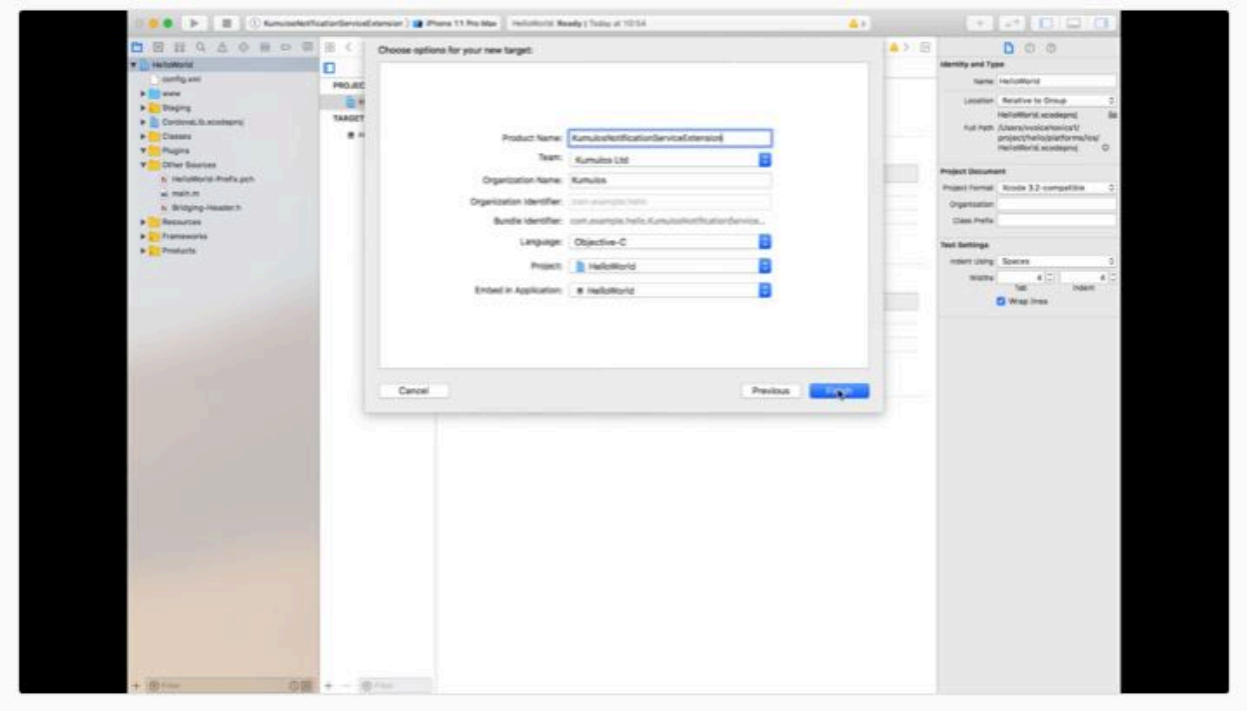


Wählen Sie im Popup-Fenster die

Die Vorlage `Benachrichtigungsservice-Erweiterung` für Ihr neues Projekt und klicken Sie auf 'Weiter'.



Fügen Sie im letzten Fenster einen geeigneten Namen für Ihre Erweiterung hinzu und klicken Sie auf 'Fertigstellen'.



Fügen Sie Folgendes zum von React Native generierten Podfile hinzu und führen Sie `pod install` aus.

```
target 'KumulosNotificationServiceExtension' do
  pod 'KumulosSdkObjectiveCExtension', '4.2.2'
end
```

Durch die Vorlage für das Projekt wird automatisch eine Datei mit dem Namen `NotificationService.m` erstellt, deren Inhalt durch die folgenden Zeilen ersetzt wird:

```
#import "NotificationService.h"
#import <KumulosSDKExtension/KumulosNotificationService.h>

@interface NotificationService ()
@end

@implementation NotificationService
- (void)didReceiveNotificationRequest:(UNNotificationRequest *)reques
   [KumulosNotificationService didReceiveNotificationRequest:request
}
@end
```

Die Kumulos SDK-Hilfsfunktionen fügen dem Benachrichtigungsinhalt automatisch Bildanhänge und Schaltflächen hinzu.

App-Funktionalitäten und -Berechtigungen konfigurieren

Verwenden Sie in den App-Projekteinstellungen die Schaltfläche "+ Funktionalität", um die Funktionen für App-Gruppen, Hintergrundmodi und Push-Benachrichtigungen hinzuzufügen.

Verwenden Sie in Ihrer Benachrichtigungserweiterung die Schaltfläche "+ Funktionalität", um die Funktion "App-Gruppen" hinzuzufügen.

In beiden Projekten sollte die App-Gruppen-Funktion so konfiguriert werden, dass sie dieselbe Gruppe gemeinsam nutzen kann. Dies muss genau mit der Gruppe übereinstimmen, die zuvor in Ihren Kennungsfunktionen definiert wurde.

`group.{your.bundle.identifier}.kumulos`

In Ihrem App-Projekt sollte für die Hintergrundmodi der Modus "Fernbenachrichtigungen" aktiviert sein.

Vorgehensweise zum Testen Ihrer Konfiguration

An diesem Punkt können Sie testen, ob Ihre App auf einem Gerät bereitgestellt wird, um sicherzustellen, dass Ihre Berechtigungen und Funktionen richtig konfiguriert sind. Stellen Sie sicher, dass die Signatur für das Erweiterungsziel ordnungsgemäß eingerichtet ist.

Initialisierung (Initialization)

Um das SDK für die Verwendung zu konfigurieren, müssen Sie es mit den API-Anmeldeinformationen Ihrer App initialisieren. Dies muss frühzeitig beim Anwendungsstart erfolgen, damit Sie mit dem Aufrufen von API-Methoden und der Verwendung von Funktionen beginnen können.

In Ihrer `App.js`:

```
import Kumulos from 'kumulos-react-native';

Kumulos.initialize({
    apiKey: 'YOUR_API_KEY',
    secretKey: 'YOUR_SECRET_KEY'
});

// When you are ready to request the push token from the user, you wo
Kumulos.pushRequestToken();
```

In Ihrer `ios/AppDelegate.mapplication:didFinishLaunchingWithOptions:` Methode:

In Ihrer `android/app/src/main/java/.../MainApplication.javaonCreate` Methode:

Enregistrement auprès de votre CRM

Lorsqu'il est initialisé pour la première fois, le SDK Kumulos crée un identifiant unique pour l'installation de l'application qui a initialisé le SDK. Cet identificateur peut être utilisé ultérieurement pour cibler les notifications Push envoyées à un périphérique spécifique.

Pour extraire cet identifiant d'installation, accédez simplement à la variable de classe :

```
const id = await Kumulos.getInstallId();
```

Une fois que vous disposez de l'identifiant d'installation, vous pouvez l'envoyer au système dorsal CRM de votre application pour qu'il soit utilisé ultérieurement pour le ciblage Push.

Association d'utilisateurs

Vous avez également la possibilité d'associer votre utilisateur d'application à Kumulos à des fins de ciblage

Si votre application utilise un identifiant pour indiquer de manière unique quel utilisateur est connecté à un périphérique (par exemple, un entier de clé primaire, un UUID ou une adresse électronique), vous pouvez envoyer cet identifiant à Kumulos pour un ciblage Push ultérieur via la même clé.

```
Kumulos.associateUserWithInstall('unique-user-identifier');
```

Ereignisverfolgung

Mit Kumulos können Sie benutzerdefinierte Analyse-Ereignisse verfolgen, um die Aktivitäten Ihrer Benutzer in Ihrer App zu beobachten. So können Sie das Verhalten analysieren und

die Journeys optimieren, um sicherzustellen, dass Ihre Benutzer den vollen Nutzen aus den Funktionen Ihrer App ziehen.

Um ein benutzerdefiniertes Analyseereignis zu verfolgen, verwenden Sie `Kumulos.trackEvent` wie folgt:

Jedes Ereignis und seine Eigenschaften müssen weniger als 250 KiB groß sein, damit das Ereignis nachverfolgt werden kann.

Die Ereignisverfolgung ist offline verfügbar, da alle Ereignisse lokal gespeichert werden, bevor sie stapelweise im Hintergrund mit dem Server synchronisiert werden.

Eine ähnliche Methode `trackEventImmediately` startet sofort eine Ereignissynchronisierung, anstatt darauf zu warten, dass die App das nächste Mal in den Hintergrund läuft.

Erweiterte In-App Funktionen

Jedes Ereignis und seine Eigenschaften müssen weniger als 250 KB groß sein, damit das Ereignis nachverfolgt werden kann.

Die Ereignisverfolgung ist offline verfügbar, da alle Ereignisse lokal gespeichert werden, bevor sie stapelweise im Hintergrund mit dem Server synchronisiert werden.

Eine ähnliche Methode `trackEventImmediately`startet sofort eine Ereignissynchronisation, anstatt auf das nächste Mal zu warten, wenn die App im Hintergrund läuft.

In Ihrer `android/app/src/main/java//MainApplication.javaonCreate` Methode:

Sobald die Konfigurationen festgelegt wurden, können Sie jetzt die Zustimmung aus der JS-Ebene verwalten:

Deep-Linking für In-App

Mit In-App Nachrichten können Sie über Deep-Link Aktionsschaltflächen an react-native Anwendungsbildschirme übergeben. Wenn sie angetippt werden, übergeben diese Schaltflächen die Kontrolle an den definierten Deep-Link-Handler, einschließlich ihrer definierten Daten-Nutzlast (konfiguriert im In-App Message Composer für die Aktionsschaltfläche).

Verwenden Sie den In_App Posteingang

In-App-Nachrichten können optional für einen späteren Abruf in einem Posteingang auf Benutzerebene gespeichert werden. So können Sie Funktionen wie Prämien oder ablaufende Gutscheine in Ihre App integrieren. Unabhängig davon, ob sie im Posteingang gespeichert sind, können maximal 50 In-Apps auf einem Gerät gespeichert werden (die ältesten Nachrichten, die diese Grenze überschreiten, werden entfernt).

Nachrichten abrufen

Um eine Nachrichtenliste aus dem Posteingang des Benutzers abzurufen und die erste in der Liste anzuzeigen, siehe das folgende Beispiel:

Als gelesen markieren

Um eine einzelne oder alle Posteingangsnachrichten als gelesen zu markieren:

Nachricht löschen

Sie können auch eine In-App-Nachricht aus dem Posteingang löschen:

Posteingang aktualisierter Handler

Um benachrichtigt zu werden, wenn sich der Posteingang ändert, können Sie einen Handler einrichten. Der Handler wird im UI-Thread ausgelöst, wenn eines der folgenden Ereignisse bei einer In-App mit Posteingangskonfiguration eintritt:

- Nachricht vom Server abgerufen
- Nachricht geöffnet
- Nachricht als gelesen markiert
- Nachricht gelöscht
- Nachricht entfernt (abgelaufen oder die Grenze der gespeicherten Nachrichten überschritten)

Sie können es wie folgt verwenden:

Beachten Sie, dass Sie `KumulosInApp.setOnInboxUpdated(null)` ausführen können, wenn Sie nicht mehr an Posteingangs-Updates interessiert sind.

Eine Zusammenfassung des Posteingangs erhalten

Sie können die Zusammenfassung des Posteingangs wie folgt abrufen:

Rufen Sie die Bild-URL des Posteingangselements ab

Jedem Posteingangselement kann ein Bild zugeordnet sein. `getImageUrl` gibt eine URL zum Bild mit der angegebenen Breite oder `null` zurück, wenn kein Bild vorhanden ist.

Fonctions avancées

Gestion des événements ouverts ou des Push de données d'arrière-plan

L'exemple de code suivant montre comment utiliser Kumulos pour gérer les notifications Push pour les liens profonds et d'autres tâches de messagerie courantes.

```
import Kumulos from 'kumulos-react-native';

Kumulos.initialize({
    apiKey: 'YOUR_API_KEY',
    secretKey: 'YOUR_SECRET_KEY',
    pushReceivedHandler: (notification) => {
        // Called when a push is received with your app in the foregr
    },
    pushOpenedHandler: (notification) => {
        // Called when a user taps on a push notification
    }
});
```

Gestion des boutons d'action de notification

Lorsqu'un utilisateur interagit avec votre message Push, le `pushOpenedHandler` défini ci-dessus est appelé. Si l'utilisateur a appuyé sur un bouton, l'objet de notification contiendra une propriété `actionId` :

```
Kumulos.initialize({
```

```
Kumulos.initialize({
    ...
    pushOpenedHandler: (notification) => {
        console.log(notification.actionId);
    },
});
```

Chapitre 8. Utilitaires pour Deliver

Deliver fournit plusieurs scripts que vous pouvez utiliser pour administrer les fonctions Deliver.

Vous pouvez utiliser les utilitaires logiciels décrits dans cette section pour une variété de fonctions de démarrage et d'administration. Outre les utilitaires logiciels utilisés avec Unica Platform, Unica Deliver utilise des utilitaires propres à Deliver et vous pouvez les utiliser uniquement pour gérer les composants Deliver.

Pour plus d'informations sur les autres utilitaires disponibles pour votre installation HCL Unica, voir le document Unica Platform - Guide d'administration.

Le script RLU

Utilisez le script RLU pour vérifier le statut du service RLU (Recipient List Uploader).

Remarque : Vous ne pouvez pas utiliser ce script pour démarrer ou arrêter le service RLU. Utilisez ce script pour vérifier la connectivité entre les composants sur site et à la demande.

Le script RLU se trouve dans le dossier `<Deliver Install Home>/bin`. Le répertoire Deliver est un sous-répertoire du répertoire Campaign.

Dans les environnements UNIX™ ou Linux™, exécutez le script en tant que `rlu.sh`.

Sous Windows™, exécutez le script à partir de l'invite de commande en tant que `rlu.bat`.

Syntaxe

```
rlu -c | --check [-h]
```

Commandes

-c, --check

Vérifiez que le service RLU est correctement configuré et qu'il est connecté à HCL Unica.

Options

-h, --help

Afficher la syntaxe du script

Exemple

Dans un environnement Linux™, pour déterminer si le service RLU est connecté aux services hébergés HCL Unica, procédez comme suit :

`rlu.sh --check`

Selon l'état de votre système, la sortie de cette commande peut se présenter comme suit :

```
Configuring Data Source [systemTables]...
Testing configuration for partition partition1
Testing connectivity for partition partition1
Testing user accessibility for partition partition1
Succeeded. List uploader config and connectivity test
succeeded for partition partition1
```

Deliver Response and Contact Tracker (RCT) Skript

Um bestehende Probleme in der vorherigen Version von RCT zu beheben, wurde die Kafka-Ebene eingeführt.

Mit diesem Script können Sie die Antwort- und Kontaktverfolgung (Response and Contact Tracker, RCT) ausführen und ihren Status überprüfen.

Dieses Script befindet sich im Verzeichnis `bin` unter Ihrer Deliver Installation. Das Verzeichnis Deliver ist ein Unterverzeichnis des Verzeichnisses Campaign.

Führen Sie das Skript in UNIX™ oder Linux™ Umgebungen als `rct.sh` aus.

Führen Sie unter Windows™ das Skript über die Befehlszeile als `rct.bat` aus.

Syntax

`rct [ starten | stoppen | prüfen ]`

Befehle

start

Startet die RCT.

stop

Stoppt die RCT

Optionen

Prüfen

Überprüfen Sie den Status der Verbindung zwischen der RCT und den HCL Unica Hosted Services.

Beispiele

- Um die RCT auf Windows™ zu starten.

  ```
  rct.bat start
  ```
- Um die RCT auf Windows™ zu stoppen.

  ```
  rct.bat stop
  ```
- In einer Linux™ Umgebung, um festzustellen, ob das RCT mit HCL Unica gehosteten Diensten verbunden ist.

  ```
  rct.sh check
  ```

  Abhängig vom Status Ihres Systems könnte die Ausgabe dieses Befehls wie folgt aussehen:

  ```
  C:\ <UNICA_HOME> \Campaign\Deliver\bin>rct check Testen von
   Konfiguration und Verbindung für Partition partition1 Erfolgreich |
   Partition: Partition1 – Konto-ID für gehostete Dienste: asm_admin
  ```

Script MKService_rct

Le script MKService_rct ajoute ou supprimer RCT (Response and Contact Tracker) en tant que service. L'ajout de RCT en tant que service redémarre RCT chaque fois que vous

redémarrez l'ordinateur sur lequel vous avez installé RCT. La suppression de RCT en tant que service empêche RCT de redémarrer automatiquement.

Ce script est situé dans le répertoire `bin` de votre installation Deliver.

Dans des environnements UNIX™ ou Linux™, exécutez `MKService_rct.sh.` avec un utilisateur qui dispose de droits root ou de droits permettant de créer des processus démons.

Sous Windows™, exécutez le script à partir de la ligne de commande sous la forme `MKService_rct.bat`.

Syntaxe

```
MKService_rct -install
```

```
MKService_rct -remove
```

Commandes

-install

Ajoute RCT en tant que service

-remove

Supprime le service RCT

Exemples

- Ajoute RCT en tant que service Windows™

  ```
  MKService_rct.bat -install
  ```
- Pour supprimer le service RCT sous UNIX™ ou Linux™.

  ```
  MKService_rct.sh -remove
  ```

configTool

Les propriétés et les valeurs de la page **Configuration** sont enregistrées dans les tables système Platform. Vous pouvez utiliser l'utilitaire `configTool` pour importer et exporter les

paramètres de la configuration dans les tables système. Pour plus d'informations, reportez-vous au document Platform - Guide d'administration.

Chapitre 9. A propos de l'identification des incidents Deliver

Unica Deliver fournit différents outils et techniques que vous pouvez utiliser pour étudier les problèmes liés à vos installations Campaign et Deliver.

Fichiers journaux pour Deliver

HCL Unica fournit plusieurs fichiers journaux que vous pouvez consulter pour surveiller votre installation Deliver et examiner les problèmes.

Fichier journal Deliver

Ce journal contient les types d'informations suivants concernant les informations téléchargées depuis les services hébergés HCL Unica. Il se trouve dans le répertoire `logs` de votre installation Deliver.

- informations générales de mailing
- ID d'instance de mailing
- données sur les clics de lien
- données sur les e-mails retournés

Fichiers temporaires Deliver

Ce répertoire contient les données en cours de chargement.

Il se trouve dans le répertoire `temp` de votre installation Deliver.

Fichiers journaux de campagne

Vous pouvez consulter les fichiers journaux dans les emplacements suivants pour obtenir des informations sur les activités liées aux mailings dans Campaign.

- `Campaign\partitions\<partitionN>\logs`

  Divers fichiers journaux liés aux exécutions de diagrammes, y compris les entrées de journal provenant de tout processus Deliver contenu dans le diagramme.

- `Campaign\logs`

  Ce répertoire contient `campaignweb.log` qui contient des informations sur l'activité de chargement effectuée par RLU.

Utilisation de log4j avec Deliver

Deliver utilise l'utilitaire Apache log4j pour la configuration de la journalisation, le débogage et les informations d'erreur liées aux services RCT (Response and contact Tracker) et RLU (Recipient List Uploader).

Pour plus d'informations sur la modification des paramètres du journal système, voir :

- Les commentaires dans le fichier log4j.xml.
- La documentation log4j sur le site Web Apache : https://logging.apache.org/log4j/2.x/manual/index.html

Utilisation de log4j avec RLU (Recipient List Uploader)

Lorsque vous exécutez l'utilitaire RLU (Recipient List Uploader) à partir de la ligne de commande, il utilise les paramètres de journal par défaut.

Pour modifier ces paramètres, vous devez modifier le fichier `deliver_rlu_log4j.xml`.

Modifiez `deliver_rlu_log4j.xml` selon les instructions des commentaires de ce fichier. Vous ne devez pas modifier ce fichier sauf si le support HCL vous demande de le faire.

Lorsque RLU est appelé automatiquement par un diagramme, il utilise la journalisation de l'application Web Campaign, qui est configurée dans `campaign_log4j.xml` dans votre répertoire d'installation Campaign.

Utilisation de log4j avec RCT (Response and Contact Tracker)

Lorsque vous exécutez l'utilitaire RCT (Response and Contact Tracker), il utilise les paramètres de journal par défaut.

Pour modifier ces paramètres, vous devez modifier le fichier `deliver_rct_log4j.xml`.

Modifiez `deliver_rct_log4j.xml` selon les instructions des commentaires de ce fichier.

Zielseite

Falls nach der Erstellung einer bestimmten Zielseite, unerwartete oder keine Werte in der Tabelle UCC_RESPONSEATTR für eines der Formularfelder angezeigt werden, führen Sie zur Lösung die folgenden Schritte aus

.

1. Öffnen Sie den Nachrichteneditor und suchen Sie die Zielseite.

2. Klicken Sie mit der rechten Maustaste auf **Inhalt bearbeiten**, klicken Sie auf die Registerkarte **Link**, wählen Sie das in der Dropdown-Liste „Formular absenden (optional)“ definierte Formular aus, und klicken Sie auf **OK**.

3. Speichern Sie und veröffentlichen Sie die Zielseite.

4. Senden Sie die Mail erneut. Dadurch wird sichergestellt, dass alle Formularfeldwerte in der Tabelle UCC_RESPONSEATTR für die Zielseite hinzugefügt werden.

Note:

Diese Schritte sind im Schnellentwurfsmuster nicht erforderlich.

Chapitre 10. Gestion de l’accès des utilisateurs aux fonctions de messagerie

Campaignet Deliver utilisent les rôles et les autorisations fournis par Unica Platform pour contrôler l’accès des utilisateurs aux fonctions de messagerie dans Deliver et Campaign. Vous devez disposer des droits dans Unica Platform et Campaign pour apporter les modifications requises. Vous devez également être familiarisé avec la configuration des rôles et des droits d’accès dans Platform et avec la définition des stratégies de sécurité pour Campaign.

Pour mener des campagnes de marketing par courrier électronique, les spécialistes du marketing par courrier électronique accèdent aux fonctions de mailing Deliver dans Unica Campaign.

Pour créer des communications et des pages d’arrivée hébergées personnalisés, les spécialistes du marketing travaillent avec des fonctions et du contenu de Deliver Document Composer.

Pour des informations générales sur la configuration des rôles, des droits d’accès et des stratégies, voir les sections du document Unica Platform - Guide d’administration qui décrivent comment gérer la sécurité dans Unica Platform et Unica Campaign.

Affectation de rôle et de stratégie pour l’accès aux mailings

Pour se connecter au système HCL Unica, les spécialistes du marketing par courrier électronique entrent un nom d’utilisateur et un mot de passe système. Les droits accordés à l’utilisateur système déterminent la manière dont le spécialiste du marketing peut accéder aux fonctions de mailing, aux communications personnalisées et au contenu dans Deliver et Campaign.

Les droits sont associés aux rôles définis dans Unica Platform. Pour contrôler l’accès aux fonctions de mailing dans Campaign, vous pouvez définir des rôles dans une ou plusieurs stratégies de sécurité. Tous les utilisateurs du système qui accèdent aux fonctions de mailing, aux communications et au contenu doivent posséder un rôle Deliver au sein d'une stratégie de sécurité Campaign. Grâce à la stratégie, vous appliquez de manière sélective

des droits d’accès aux fonctions de mailing dans Campaign et aux communications et au contenu de Deliver Document Composer.

Les utilisateurs qui accèdent aux fonctions de mailing doivent également disposer de rôles utilisateur et admin Deliver. Ces rôles sont distincts des rôles Deliver disponibles dans les stratégies de sécurité Campaign.

Rôles et droits d'accès de Platform et Campaign

Dans Platform et Campaign, les rôles constituent une collection configurable de droits d'accès. Dans Platform et Campaign, vous pouvez, pour chaque rôle, spécifier des droits d'accès à l'application.

Vous pouvez utiliser les rôles par défaut ou en créer de nouveaux. L'ensemble des droits d'accès disponibles est défini par le système, vous ne pouvez pas en créer vous-même.

A propos de l'affectation de rôles

En règle générale, vous devez affecter aux utilisateurs des rôles dont les droits d'accès correspondent tâches réalisées par les utilisateurs dans votre organisation lorsqu'ils utilisent HCL Unica. Vous pouvez affecter des rôles à un groupe ou à un utilisateur en particulier. L'affectation de rôles à des groupes permet d'affecter une combinaison de rôles au groupe. Par la suite, si vous souhaitez changer cette combinaison, vous pouvez le faire en une seule fois, sans répéter l'opération pour chaque utilisateur. Lorsque vous affectez des rôles à un groupe, vous ajoutez et supprimez des utilisateurs de vos groupes pour gérer l'accès utilisateur.

Evaluation des rôles par le système

Si un utilisateur dispose de plusieurs rôles, le système évalue les droits d'accès de l'ensemble de ces rôles. L'utilisateur est alors autorisé ou non à accomplir une fonction sur un objet particulier en fonction des droits d'accès agrégés de tous les rôles. Dans le cas de Campaign, l'utilisateur est autorisé ou non à accomplir une fonction sur un objet particulier en fonction de la politique de sécurité de l'objet.

Fonctionnement des règles de sécurité

Les règles de sécurité sont les règles qui régissent la sécurité des dossiers et des objets dans Campaign. Elles sont consultées chaque fois qu'un utilisateur exécute une action dans l'application.

Vous pouvez créer vos propres stratégies de sécurité ou utiliser la stratégie de sécurité globale par défaut incluse dans Campaign.

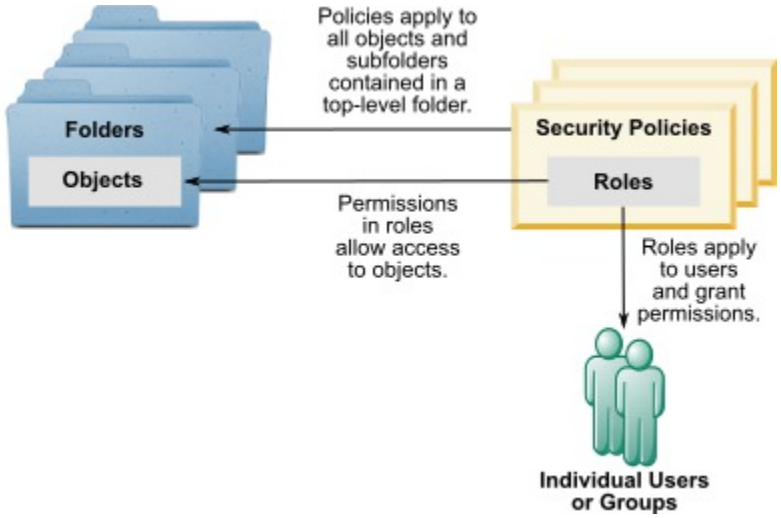
Dans Campaign, des règles de sécurité sont affectées aux dossiers. Lorsque vous créez un dossier de niveau supérieur, vous devez appliquer une règle de sécurité au dossier. Les objets ou les sous-dossiers dans le dossier héritent de la règle de sécurité du dossier.

Comme le dossier de niveau supérieur détermine la règle de sécurité des objets dans le dossier, vous ne pouvez pas affecter une règle de sécurité directement aux objets. Pour changer la stratégie de sécurité d'un objet, vous devez déplacer l'objet dans un dossier doté de la stratégie de sécurité souhaitée ou dans le dossier racine de niveau supérieur.

Vous pouvez également affecter directement une règle de sécurité à un utilisateur. Contrairement aux objets et aux dossiers, qui sont affectés à des règles de sécurité globalement, les utilisateurs sont affectés à des rôles dans les règles de sécurité. Pour contrôler les actions que les utilisateurs peuvent exécuter, vous affectez les utilisateurs à des rôles dans des règles de sécurité. Ainsi, vous contrôlez l'accès des utilisateurs aux objets dans les dossiers qui utilisent ces règles de sécurité.

Si un utilisateur n'est pas affecté explicitement à au moins un rôle dans une règle de sécurité, l'utilisateur ne peut pas créer de dossiers et d'objets sous un dossier de niveau supérieur qui utilise la règle, et l'utilisateur ne peut pas accéder aux objets du dossier et de ses sous-dossiers.

Le diagramme suivant montre la relation entre les règles de sécurité, les dossiers, les objets, les rôles et les utilisateurs.



Rôles administratifs de niveau supérieur

Des rôles administratifs dans Unica Campaign sont affectés pour chaque partition. Les utilisateurs avec ces rôles peuvent exécuter les actions autorisées sur n'importe quels objets dans la partition, quelle que soit la règle de sécurité utilisée dans les dossiers qui contiennent les objets.

Règles de sécurité et partitions

Les stratégies de sécurité sont créées pour chaque partition. Chaque partition est dotée d'une stratégie de sécurité qui lui est propre.

Chaque partition dans Unica Campaign peut avoir plusieurs règles de sécurité.

Une règle de sécurité change lorsque des dossiers et des objets sont déplacés ou copiés.

Il est possible de copier ou déplacer les objets et dossiers d'une stratégie de sécurité à l'autre, mais l'utilisateur qui exécute cette opération doit posséder les droits d'accès appropriés, à la fois dans la stratégie source et dans la stratégie cible.

Après le déplacement ou la copie d'un dossier vers un dossier affecté d'une règle de sécurité différente de sa source, la règle de sécurité des objets de niveau inférieur est remplacée automatiquement par la règle de sécurité du nouveau dossier.

Stratégie de sécurité globale

Campaign contient une règle de sécurité globale par défaut. Vous ne pouvez pas supprimer cette règle. Elle est toujours appliquée. Cependant, vous pouvez personnaliser le schéma de sécurité comme suit.

- Modifiez les rôles et les droits dans la règle de sécurité globale en fonction des besoins de votre entreprise.
- Créez des règles personnalisées et affectez des utilisateurs uniquement aux règles personnalisées, mais pas à la règle globale.
- Utilisez les règles personnalisées et la règle globale.

Les règles personnalisées que vous créez existent sous la règle globale. Si vous décidez de ne pas créer vos propres règles de sécurité, la règle de sécurité globale est appliquée par défaut aux dossiers et aux objets que les utilisateurs créent dans Campaign.

La règle de sécurité globale contient six rôles prédéfinis. Vous ne pouvez pas supprimer ces rôles, mais vous pouvez modifier leurs droits.

Les rôles prédéfinis dans la règle de sécurité globale sont :

- **Propriétaire de dossier** : tous les droits activés pour les dossiers créés par un utilisateur. Tous les utilisateurs doivent avoir ce rôle. Il n'est pas nécessaire de lui affecter des utilisateurs.
- **Propriétaire** : tous les droits activés pour les objets que créés par un utilisateur. Tous les utilisateurs doivent avoir ce rôle ; il n'est pas nécessaire de lui affecter des utilisateurs.
- **Admin** - Tous les droits d'accès sont activés. L'utilisateur par défaut `asm_admin` a ce rôle.
- **Exécuter** : tous les droits activés.
- **Concevoir** : droits de lecture et d'écriture sur tous les objets. Ce rôle ne peut pas planifier des diagrammes ni des sessions.
- **Réviser** : droits de lecture seulement.

Deliver rôles dans la stratégie globale

En plus des rôles Campaign prédéfinis, la stratégie globale inclut plusieurs rôles propres à Deliver.

La stratégie globale inclut les rôles Deliver suivants.

- **Deliver_admin** - Capable d’accéder à toutes les fonctions de mailing, à l’ensemble du contenu et à tous les documents.
- **Deliver_execute** - Capable d’accéder à toutes les fonctions de mailing, à l’ensemble du contenu et à tous les documents.
- **Deliver_design** - Capable d’accéder à l'ensemble du contenu, à tous les documents et à la plupart des fonctions de mailing. Toutefois, il n’est pas explicitement autorisé à envoyer des mailings de production.
- **Deliver_review** - Capable d'afficher uniquement le contenu et les documents et dispose de droits limités pour l’utilisation des mailings. L’autorisation d’ajouter, d’éditer ou de supprimer des mailings lui est explicitement refusée. Il est autorisé à afficher et à envoyer des mailings de test et de production.

Remarque : Deliver ne prend pas en charge les rôles Propriétaire et Propriétaire de dossier créés par défaut pour Campaign.

Droits de messagerie dans Campaign

Campaign contrôle l’accès des utilisateurs aux fonctions de mailing en activant ou en désactivant des droits spécifiques définis dans les rôles affectés à un utilisateur ou à un groupe. Ces rôles sont associés à une ou plusieurs stratégies de sécurité. Vous pouvez définir plusieurs stratégies de sécurité Campaign et affecter plusieurs rôles à chaque stratégie. Chaque combinaison stratégie/rôle peut définir un ensemble spécifique de droits d’accès.

Pour plus d’informations sur la gestion des droits de sécurité, y compris des exemples de scénarios de sécurité, voir le document Unica Campaign - Guide d’administration.

Sous Rôles et droits d'accès pour Unica Platform, vous attribuez des droits d'accès utilisateur pour les fonctions de mailing et le contenu dans la section Campaign, comme suit.

1. Définissez les rôles utilisateur.

   Les rôles utilisateur définis par le système pour Deliver sont créés par défaut sous la stratégie globale.

   Vous pouvez également définir des rôles personnalisés et les ajouter à la stratégie globale ou à d’autres stratégies que vous définissez.
2. Définissez des stratégies de sécurité et ajoutez des rôles utilisateur aux stratégies.

   La stratégie globale est définie par défaut. Vous pouvez définir des stratégies supplémentaires pour Campaign.
3. Définissez des droits spécifiques pour chaque rôle dans chaque stratégie.

   Vous pouvez définir des stratégies et des rôles personnalisés supplémentaires avec différents ensembles de droits pour mieux contrôler l’accès aux fonctions de mailing dans Campaign et Deliver Document Composer.

Les modifications apportées aux droits, rôles et stratégies sont appliquées lorsque l’utilisateur se connecte à HCL Unica. Une fois que vous avez affecté ou modifié des droits de mailing pour un utilisateur, ce dernier doit se déconnecter, puis se reconnecter pour que les modifications soient prises en compte.

Rendre des rôles et des droits d’accès disponibles

En fonction de votre installation Unica Platform, les contrôles d’administration requis pour définir et appliquer des rôles et des droits peuvent ne seront peut-être pas immédiatement visibles. Vous pouvez rendre les contrôles nécessaires visibles en accédant à Deliver Document Composer ou à un mailing dans Campaign.

Effectuez la procédure suivante si vous ne voyez pas tous les droits d’accès suivants dans la stratégie globale Campaign.

- Droits d’accès aux mailings dans la catégorie Campagnes
- Droits d’accès pour la bibliothèque de contenu dans la catégorie Ressources numériques
- Droits d’accès aux documents Deliver dans la catégorie Documents

1. Connectez-vous à HCL Unica.

   Si plusieurs utilisateurs sont configurés, connectez-vous en tant qu’utilisateur doté des droits les plus limités. Par exemple, connectez-vous en tant qu’utilisateur ayant uniquement des droits de consultation.
2. Accédez à **Campaign** > **Documents Deliver** pour accéder à Document Composer.

   Attendez la fin du chargement de Document Composer.
3. Accédez à **Paramètres** > **Rôles utilisateur et droits d'accès** > **Campaign** > **partition(n)** > **Stratégie globale**

   Lorsque vous y êtes invité, confirmez que vous souhaitez quitter Document Composer en quittant la page.
4. Cliquez sur **Ajouter des rôles et affecter des droits d'accès**. Les rôles Deliver suivants sont visibles.
   - deliver_admin
   - deliver_execute
   - deliver_design
   - deliver_review
5. Cliquez sur **Enregistrer et éditer droits d'accès**.

   Les droits de mailing sont visibles dans les catégories Campagnes, Ressources numériques et Documents.

   Pour plus d’informations sur les droits d’accès spécifiques disponibles, voir les rubriques suivantes.

Evaluation des droits d'accès par Campaign

Lorsqu'un utilisateur accomplit une tâche ou tente d'accéder à un objet, Campaign exécute les actions ci-après.

1. Identifie tous les groupes et rôles auxquels l'utilisateur fait partie dans la stratégie de sécurité globale.

   Un utilisateur peut appartenir à un ou plusieurs rôles, ou n'appartenir à aucun rôle. Un utilisateur est associé au rôle Propriétaire s'il possède un objet. Il est associé au rôle Propriétaire de dossier s'il est propriétaire du dossier où se trouve l'objet.

   Un utilisateur appartient à d'autres rôles uniquement s'il a été affecté spécifiquement à ces rôles (de manière directe ou parce qu'il appartient à un groupe auquel ce rôle a été affecté).
2. Le système détermine si l'objet auquel l'utilisateur tente d'accéder est affecté à une stratégie personnalisée. Dans l'affirmative, le système identifie tous les groupes et rôles auxquels l'utilisateur appartient dans cette stratégie personnalisée.
3. Agrège les droits d'accès de tous les rôles auxquels appartient l'utilisateur, suivant les résultats des étapes 1 et 2. A l'aide de ce rôle composite, le système évalue les droits d'accès comme suit :
   a. Si le droit d'accès d'un rôle est **Refusé** pour cette action, les droits sont agrégés comme suit :
      i. Prenons le cas d'une politique globale et d'une politique personnalisée avec un droit d'accès REFUSE pour le rôle de politique personnalisée. Alors, tout droit d'accès REFUSE pour le rôle de politique personnalisée prévaut sur les droits d'accès affectés au rôle de politique globale.
      ii. Prenons maintenant le cas d'une politique globale et de 2 politiques personnalisées ou plus, avec un droit d'accès REFUSE pour l'un des rôles de politique personnalisée et le même droit d'accès AUTORISE pour l'autre rôle de politique personnalisée. Alors, tout droit d'accès AUTORISE prévaut sur le droit REFUSE de la politique personnalisée.
   b. Si aucun rôle n'a le droit d'accès **Refusé** pour cette action, le système vérifie si l'un des rôles est doté du droit d'accès **Autorisé** pour cette action. Si tel est le cas, l'utilisateur est autorisé à exécuter l'action.
   c. Si aucune de ces deux propositions n'est vraie, l'utilisateur n'est pas autorisé à réaliser l'action.

Exemple dans le cadre d'une politique personnalisée

Prenons le cas d'une politique personnalisée dans le cadre d'une politique globale : PolitiquePersonnaliséeA. PolitiquePersonnaliséeA présente le rôle RôlePolitiquePersonnaliséeA, lui-même doté du droit d'accès REFUSE pour l'action Ajouter/Editer une campagne.

Prenons l'UtilisateurA, qui dispose du rôle RôlePolitiquePersonnaliséeA. Un droit d'accès REFUSE pour l'action Ajouter/Editer une campagne pour le rôle RôlePolitiquePersonnaliséeA prévaut sur les droits d'accès affectés au rôle de politique globale. Par conséquent, les objets Ajouter/Editer une campagne ne sont pas visibles à l'UtilisateurA.

Exemple dans le cadre de deux politiques personnalisées

Prenons le cas de deux politiques personnalisées dans le cadre d'une politique globale : PolitiquePersonnaliséeA et PolitiquePersonnaliséeB. Ces deux politiques présentent les rôles RôlePolitiquePersonnaliséeA et RôlePolitiquePersonnaliséeB, respectivement. RôlePolitiquePersonnaliséeA dispose du droit d'accès AUTORISE pour l'action Ajouter/Editer une campagne. RôlePolitiquePersonnaliséeB dispose du droit d'accès REFUSE pour cette même action.

Les rôles RôlePolitiquePersonnaliséeA et RôlePolitiquePersonnaliséeB sont affectés à l'UtilisateurA. Le droit d'accès AUTORISE affecté à l'action Ajouter/Editer du rôle RôlePolitiquePersonnaliséeA prévaut sur le droit d'accès REFUSE du rôle RôlePolitiquePersonnaliséeB. Par conséquent, les objets Ajouter/Editer une campagne sont visibles à l'UtilisateurA.

Définition des états des droits d'accès

Pour chaque rôle, vous pouvez spécifier les droits d'accès accordés, non accordés ou refusés. Vous définissez ces droits d'accès sur la page **Paramètres > Rôles utilisateur et autorisations**.

Les états qui suivent ont les significations indiquées :

- **Accordé** - signalé par une coche  . Autorise de façon explicite l'exécution de cette fonction particulière tant qu'aucun autre rôle de l'utilisateur ne refuse explicitement le droit d'accès.
- **Refusé** - signalé par un "X"  . Refuse de façon explicite l'exécution de cette fonction particulière, sans tenir compte d'autres rôles de l'utilisateur susceptibles d'autoriser le droit d'accès.
- **Non accordé** : signalé par un cercle  . N'autorise, ni ne refuse de façon explicite l'exécution d'une fonction particulière. Si le droit d'accès n'est pas accordé de façon explicite par l'un des rôles de l'utilisateur, l'utilisateur n'est pas autorisé à exécuter cette fonction.

Droits d’accès aux mailings dans Campaign

Dans Campaign, vous créez, configurez, exécutez et surveillez les mailings Deliver à l’aide de commandes dans les onglets de mailing Deliver. Vous gérez chaque mailing dans un onglet distinct.

Les droits suivants permettent de contrôler l’accès des utilisateurs aux onglets de mailing Deliver. Ils se trouvent dans la catégorie **Campagnes**.

Droit	Description
Vue des mailings	Permet à un utilisateur d’afficher un onglet de mailing Deliver dans une campagne. L’utilisateur ne peut pas éditer ni modifier le mailing.
Editer des mailings	Permet à un utilisateur de configurer ou de modifier un onglet de mailing Deliver dans une campagne.
Supprimer des mailings	Permet à un utilisateur de supprimer un mailing Deliver d’une campagne.
Ajouter des mailings	Permet à un utilisateur de créer un mailing dans une campagne.

Droit	Description
Envoyer un mailing en production	Permet à un utilisateur de lancer une exécution en production du mailing, d’activer les e-mails transactionnels pour un mailing ou de planifier une exécution de mailing en production. Les mailings de production peuvent inclure de nombreux messages. Les messages électroniques sont envoyés à chaque personne identifiée comme destinataire de production dans la liste de destinataires associée au mailing.
Lancer une exécution en mode test	Permet à un utilisateur de lancer une exécution de test du mailing. Les mailings de test impliquent généralement quelques messages. Lors d’une exécution de test, un message électronique est envoyé à chaque adresse identifiée en tant que destinataire de test dans la liste de destinataires associée au mailing.

Droits d’accès pour la catégorie Ressources numériques

Les droits d’accès aux ressources numériques contrôlent l’accès des utilisateurs aux éléments de contenu dans la bibliothèque de contenu Deliver et aux dossiers et sous-dossiers dans lesquels ils sont stockés.

La bibliothèque de contenu est un référentiel pour les éléments de contenu (également appelés ressources numériques) utilisés dans les communications créées par les utilisateurs dans Deliver Document Composer.

Droits	Description
Afficher des ressources numériques Deliver	Permet à un utilisateur d’ouvrir des éléments de contenu pour afficher les propriétés et de prévisualiser le contenu pouvant être ajouté à une communication personnalisée.
Créer des ressources numériques dans la	Permet à un utilisateur de créer un élément de contenu et de l’ajouter à la bibliothèque de contenu.

Droits	Description
bibliothèque de contenu Deliver	
Editer les ressources numériques existantes dans la bibliothèque de contenu Deliver	Permet à un utilisateur d’ouvrir et de modifier des éléments de contenu existants.
Supprimer des ressources numériques de la bibliothèque de contenu Deliver	Permet à un utilisateur de supprimer un élément de contenu de la bibliothèque de contenu.
Déplacer des ressources numériques d’un dossier à un autre	Permet à un utilisateur de déplacer des éléments de contenu au sein de la bibliothèque de contenu. Le déplacement d’un élément de contenu nécessite l’affectation de ce droit au dossier source et au dossier de destination.

Droits d’accès pour la catégorie Documents

Les droits de la catégorie **Documents** contrôlent l’accès des utilisateurs pour créer, éditer et gérer des communications personnalisées dans Deliver Document Composer.

Droits	Description
Afficher des documents Deliver	Permet à un utilisateur d’afficher un document utilisé pour créer un e-mail, une notification push de boîte de réception ou une page d’arrivée hébergée.
Créer des documents Deliver	Permet à un utilisateur de créer une nouvelle communication personnalisée.

Droits	Description
Editer les documents Deliver existants	Permet à un utilisateur de modifier une communication personnalisée existante.
Supprimer des documents Deliver	Permet à un utilisateur de supprimer une communication personnalisée.
Publier le document Deliver, en rendant le contenu disponible sur l'Internet public	Permet à un utilisateur de publier une communication personnalisée. La publication d’une communication rend le document et tous les contenus ajoutés disponibles pour une utilisation dans un mailing Deliver.
Copier des documents Deliver d'un dossier à un autre	Permet à un utilisateur de copier une communication personnalisée entre des dossiers de la bibliothèque de contenu. La copie d’une communication nécessite l’affectation de ce droit au dossier source et au dossier de destination.
Déplacer des documents Deliver d’un dossier à un autre	Permet à un utilisateur de déplacer une communication personnalisée d'un dossier vers un autre dossier de la bibliothèque de contenu. Le déplacement d’une communication nécessite l’affectation de ce droit au dossier source et au dossier de destination.

Droits d’accès pour la catégorie Administration d'e-mail

Les autorisations de la catégorie Administration d'e-mail de la stratégie globale Campaign fournissent aux administrateurs Deliver l’accès aux paramètres qui contrôlent l’accès des utilisateurs aux différents domaines et fonctions de messagerie.

Les administrateurs affectent l’accès au domaine et aux fonctions dans la section Paramètres de stratégie de la fenêtre Paramètres Deliver. Par exemple, l’administrateur peut restreindre la liste des domaines de messagerie qu’un utilisateur peut sélectionner en tant que domaine **De :** dans une communication de type Courrier électronique créée dans

l’éditeur de communication. La section Paramètres de stratégie ne s’affiche pas, sauf si les droits appropriés sont explicitement accordés à l’administrateur dans la stratégie globale Campaign.

Les administrateurs peuvent également contrôler l’accès aux interfaces d’administration pour enregistrer les applications mobiles auprès de Deliver et pour configurer des emplacements à utiliser avec la distribution déclenchée en fonction de l'emplacement. Les liens vers les pages d’administration apparaissent dans la section Paramètres de notification mobile de la page Paramètres Deliver. La messagerie mobile doit être activée pour que le compte de messagerie hébergé affiche la section Paramètres de notification mobile de la page Paramètres Deliver.

Droits	Description
Configurer les domaines	Contrôle l’accès à la section Paramètres de stratégie de la page Paramètres Deliver. Si le rôle de l’administrateur n’est pas autorisé à configurer les domaines de messagerie, l’administrateur ne peut pas voir la section Paramètres de stratégie. Cette autorisation est également requise pour administrer les domaines de liens courts.

Droits de messagerie pour Deliver

Unica Deliver contrôle l’accès aux fonctions de mailing en dehors de l’onglet de mailing dans Campaign via les rôles de sécurité prédéfinis suivants.

- `Deliver_admin`
- `Deliver_user`

Les utilisateurs doivent disposer des deux rôles pour accéder aux fonctions de mailing Deliver.

Affectation de rôles Deliver

Pour fournir à un utilisateur un accès complet aux fonctions de mailing Deliver, affectez les rôles Deliver prédéfinis à l’utilisateur.

1. Dans Unica Platform, accédez à `Paramètres > Rôles d'utilisateur et droits d'accès > Deliver > partition [n] > Deliver_admin`.
2. Cliquez sur **Affectation d'utilisateurs**.
3. Sélectionnez l'utilisateur dans la liste des utilisateurs disponibles. Cliquez sur **Ajouter** pour affecter le rôle à l’utilisateur.
4. Répétez les étapes 1 à 3 pour le rôle `Deliver_user`.
5. Enregistrez les modifications.

Contrôle des domaines de messagerie et des domaines de liens courts

Sur demande, Unica configure un ou plusieurs domaines de messagerie pour votre compte de messagerie hébergé. Unica peut également affecter des domaines utilisés par les spécialistes du marketing pour créer des liens courts dans différents types de messages. Les administrateurs système disposant des droits appropriés contrôlent les domaines de messagerie qui sont disponibles pour les spécialistes du marketing.

En fonction de vos besoins métier, il peut être souhaitable de limiter la liste des domaines de messagerie qui sont disponibles pour des spécialistes du marketing spécifiques. Les administrateurs Deliver restreignent la liste des domaines disponibles via des stratégies de sécurité appliquées aux dossiers dans Document Composer. La capacité des spécialistes du marketing à créer et à éditer des communications de type Courrier électronique dépend de la stratégie de sécurité appliquée au dossier contenant la communication.

Les administrateurs Deliver disposant des droits appropriés peuvent contrôler la liste des domaines de messagerie que les utilisateurs Deliver peuvent utiliser en tant que domaine **De :** dans les communications de type Courrier électronique. Les administrateurs peuvent également contrôler la liste des domaines de liens courts présentée aux spécialistes du marketing lorsqu’ils configurent des communications qui utilisent des liens courts.

Par exemple, vous pouvez indiquer les domaines de liens courts disponibles lorsque les spécialistes du marketing ajoutent un lien de partage social à des messages marketing.

Les administrateurs Deliver utilisent la page **Paramètres de politique** pour accorder des droits d’utilisation de domaines de messagerie spécifiques. L’accès à la page **Paramètres de politique** est contrôlé par les droits d’administration de courrier électronique accordés via la stratégie globale de Campaign. Seuls les administrateurs disposant des droits appropriés peuvent limiter l’accès aux domaines de messagerie via la page **Paramètres de politique**.

1. Dans le menu **Paramètres**, sélectionnez **Paramètres de messagerie**.
   Si vous disposez des droits d’administration appropriés, la section Paramètres de politique s’affiche sur la page Paramètres Deliver.
2. Cliquez sur **Afficher une liste de stratégies et leurs paramètres**.
   Une liste des stratégies de sécurité configurées pour votre installation Deliver s’affiche.
3. Cliquez sur une stratégie de sécurité associée à l’utilisateur système dont vous souhaitez contrôler l’accès au domaine de messagerie.

   La section Domaines affiche les domaines de messagerie configurés pour votre compte de messagerie hébergé.

   La section Domaines de liens courts affiche les domaines de liens courts configurés pour votre compte de messagerie hébergé.

   - Dans l’une ou l’autre section, cliquez sur **Utiliser tous les domaines** pour autoriser les utilisateurs associés à la politique à utiliser l’un des domaines de messagerie Unica configurés pour votre compte de messagerie hébergé.

     Cette option représente la valeur par défaut.
   - Cliquez sur **Utiliser des domaines spécifiques** pour sélectionner des domaines spécifiques.

     Remarque : Si vous sélectionnez **Utiliser des domaines spécifiques**, vous devez mettre à jour les droits d’accès au domaine lorsque vous

enregistrez un nouveau domaine de messagerie ou de liens courts pour votre compte de messagerie hébergé. Le système n’affecte pas automatiquement les droits d’accès pour le nouveau domaine.

Pour les utilisateurs associés à la stratégie de sécurité, seuls les domaines de messagerie sélectionnés apparaissent en tant qu’option pour l'adresse **De :** dans les communications de type Courrier électronique. Pour les communications nécessitant des liens courts, les spécialistes du marketing peuvent uniquement choisir parmi les domaines de liens cours spécifiques que vous sélectionnez.

Une fois que vous avez sauvegardé les nouveaux paramètres, Document Composer met à jour les options de domaine disponibles pour les spécialistes du marketing.

Pour plus d’informations sur la façon dont les spécialistes du marketing Deliver créent et gèrent des communications, voir le document Unica Deliver - Guide d’utilisation.

Maintenance des domaines de messagerie hébergés

Pour envoyer des messages électroniques, vous devez enregistrer au moins un domaine de messagerie auprès d'Unica. Pour améliorer la délivrabilité des messages, Unica collabore avec vous afin d’établir et de gérer la réputation de messagerie du domaine avec les principaux fournisseurs d'accès à Internet (FAI) dans le monde entier. Vous pouvez établir plusieurs domaines de messagerie auprès d'Unica.

Lorsque vous configurez l’en-tête dans une communication de type Courrier électronique, le système renseigne l’adresse De avec le domaine de messagerie que vous avez enregistré auprès d'Unica. Si vous établissez plusieurs domaines de messagerie avec Unica, les domaines disponibles s’affichent dans une liste déroulante. Les administrateurs système peuvent contrôler les domaines de messagerie que les spécialistes du marketing par e-mail peuvent sélectionner ou modifier.

Vous pouvez demander à Unica d’ajouter ou de supprimer des domaines de messagerie établis pour votre compte de messagerie hébergée. Une fois qu'Unica a effectué la modification, le système met à jour la liste des domaines de messagerie disponibles. La modification est reflétée dans la liste des domaines de messagerie disponibles lors de la prochaine création ou modification d’une communication de type Courrier électronique.

Remarque : Les modifications apportées au domaine de messagerie pour votre compte ne mettent pas à jour les communications de type Courrier électronique que vous avez créées avant la demande de modification. Pour modifier le domaine de messagerie d’une communication créée précédemment, vous devez rouvrir la communication de type Courrier électronique et mettre à jour la sélection du domaine de messagerie.

Pour plus d’informations sur l’enregistrement d’un domaine de messagerie auprès d'Unica, voir HCL Unica - Options de nom de domaine pour les e-mails.

Pour demander des modifications liées à vos domaines de messagerie, contactez l'équipe Unica Deliver Services via le support technique HCL.

Configuration de l’adresse d’expéditeur et des noms d’affichage par défaut

Pour chaque domaine de messagerie que vous avez enregistré auprès de Unica, vous pouvez définir une adresse électronique par défaut et un nom convivial par défaut. La combinaison de l’adresse électronique ou du nom convivial et du domaine de messagerie apparaît en tant qu'adresse De : pour les messages électroniques que vous envoyez.

Les administrateurs peuvent configurer les noms d’expéditeur et d’affichage par défaut dans la page Paramètres de domaine. Les paramètres de domaine font partie de l'interface de paramètres Deliver. L’accès à la page Paramètres de domaine est contrôlé par les droits d’administration de courrier électronique accordés par le biais de la stratégie Campaign globale. Seuls les administrateurs disposant des droits appropriés peuvent limiter l’accès aux domaines de messagerie via la page Paramètres de politique.

1. Accédez à **Paramètres** > **Paramètres Deliver**. Dans la section Paramètres de domaine, cliquez sur **Afficher** la liste des paramètres de domaine.

   La page Paramètres de domaine répertorie les noms d’affichage et les adresses électroniques par défaut associés aux domaines de messagerie enregistrés dans

votre compte de messagerie hébergé. La liste inclut uniquement les domaines que vos droits d’utilisateur vous permettent de modifier.

La colonne Par défaut indique la combinaison de nom d’affichage, adresse et domaine qui apparaît en tant qu’adresse par défaut pour les nouvelles communications de type Courrier électronique.

2. Cliquez sur **Editer**  . La fenêtre Editer les paramètres de domaine apparaît.

   La colonne Nom de domaine répertorie les domaines de messagerie disponibles. Vous pouvez effectuer les opérations suivantes pour n'importe lequel des domaines.

   - Dans la colonne Nom d'affichage De, entrez un nom convivial qui s’affichera par défaut pour un domaine de messagerie dans la liste.
   - Dans la colonne Adresse De, entrez la partie locale de l’adresse électronique à afficher par défaut pour un domaine de messagerie dans la liste.
3. Si vous le souhaitez, dans la colonne Par défaut, sélectionnez une combinaison d’adresse, nom d’affichage et domaine à afficher comme adresse par défaut pour les nouvelles communications de type Courrier électronique.

   Si vous ne sélectionnez pas de valeur par défaut, le système utilise le premier domaine de la liste pour créer l’adresse De par défaut pour les nouvelles communications de type Courrier électronique.
4. Enregistrez les modifications.

Les nouveaux paramètres d’adresse s’appliquent à toutes les nouvelles communications de type Courrier électronique que vous créez. Les paramètres ne modifient pas les informations d’adresse pour les communications de type Courrier électronique que vous avez créées précédemment. Pour mettre à jour les communications de type Courrier électronique précédentes, vous devez rouvrir et modifier chaque communication.

Contrôle de l’accès à la liste des messages envoyés

Deliver fournit une liste des messages qui ont été envoyés depuis votre environnement Deliver. Etant donné que la liste inclut des liens vers des configurations de messagerie, vos plans de sécurité peuvent nécessiter une restriction de l’accès à la liste.

La liste des messages est présentée sur la page **Présentation des messages**. Par défaut, tous les utilisateurs de votre environnement Campaign et Deliver peuvent voir la liste des messages envoyés. Toutefois, lorsque vous activez la restriction d’accès, vous pouvez empêcher des utilisateurs spécifiques de voir l’option de menu permettant d’ouvrir la page contenant la liste.

La restriction de l’accès à la liste des messages envoyés affecte toutes les partitions de votre installation Campaign. Si votre installation Campaign inclut plusieurs partitions, vous devez mettre à jour les droits utilisateur séparément dans chaque partition pour accorder ou refuser explicitement le droit d'accéder à la liste.

Le contrôle des personnes pouvant accéder à la liste des messages envoyés nécessite une série de tâches pour modifier les droits utilisateur et la configuration système.

Tâche	Informations complémentaires
Identifiez les utilisateurs qui peuvent accéder à la liste des messages. Tout d’abord, tous les utilisateurs disposent d’un accès.	Octroi de l’accès à la liste des messages envoyés *(à la page 165)*
Identifiez les utilisateurs qui ne sont pas autorisés à accéder à la liste des messages.	Refus de l’accès à la liste des messages envoyés *(à la page 166)*
Activez la restriction d'accès.	Activation de la restriction pour la liste des messages envoyés *(à la page 168)*

Lorsque vous effectuez ces tâches, l’option de **Présentation des messages** du menu **Campaign** n’est visible que pour les utilisateurs ayant des rôles qui accordent explicitement des droits d’accès à la liste des mailings.

Octroi de l’accès à la liste des messages envoyés

Si vous restreignez l’accès à la liste des messages envoyés, vous devez accorder spécifiquement l’accès aux utilisateurs qui doivent accéder à la liste.

Les utilisateurs accèdent à la liste des messages envoyés en cliquant sur le lien **Présentation des messages** dans le menu **Campaign**. Vous pouvez accorder à un utilisateur l’accès à la liste de tous les messages envoyés en lui affectant un rôle d’administration de niveau supérieur qui est explicitement autorisé à afficher le lien **Présentation des messages**.

Les rôles de niveau supérieur par défaut incluent **Admin**, **Execute**, **Design**et **Review**. Les droits accordés via les rôles de niveau supérieur s’appliquent à tous les objets de la partition.

1. Accédez à `Settings > User Roles and Permissions > Campaign > partition (n)`.
2. Cliquez sur **Enregistrer et éditer droits d'accès**.
   Une liste des droits d’accès pour la partition s’ouvre. Les rôles de niveau supérieur disponibles sont répertoriés dans la partie supérieure de la page.
3. Dans la section **Administration**, accordez explicitement le droit **Afficher la page de liste de diffusion** à chaque rôle.

Lorsque vous activez les restrictions d’accès pour la liste des messages envoyés, les utilisateurs dont les rôles sont explicitement autorisés à **Afficher la page de liste de diffusion** peuvent voir le lien **Présentation des messages** dans le menu **Campaign**.

Créez un rôle pour refuser l’accès à la liste des messages envoyés.

Refus de l’accès à la liste des messages envoyés

Si vous restreignez l’accès à la liste des messages envoyés, vous devez spécifiquement refuser l’accès aux utilisateurs qui ne doivent pas être autorisés à accéder à la liste.

Les utilisateurs accèdent à la liste des messages envoyés en cliquant sur le lien **Présentation des messages** dans le menu **Campaign**. Vous pouvez empêcher un utilisateur d’accéder à la liste de tous les messages envoyés en lui affectant un rôle d’administration de niveau supérieur pour lequel l'autorisation d'affichage du lien **Présentation des messages** a été explicitement refusée.

Les rôles de niveau supérieur par défaut incluent **Admin**, **Execute**, **Design**et **Review**.
Les droits accordés via les rôles de niveau supérieur s’appliquent à tous les objets de la partition. Vous pouvez créer de nouveaux rôles de niveau supérieur afin de compléter les rôles de niveau supérieur par défaut. Les nouveaux rôles peuvent accorder ou refuser des droits d’accès spécifiques.

1. Accédez à **Paramètres** > **Rôles utilisateur et droits d'accès** > **Campaign** > **partition(n)**. La page **partition <n>** s’ouvre.
2. Cliquez sur **Ajouter rôle**. Affectez un nom et une courte description au rôle. Sauvegardez les modifications et revenez à la page **partition <n>**.
3. Configurez le nouveau rôle pour refuser l’accès à la liste des mailings envoyés.

    a. Cliquez sur **Ajouter des rôles et affecter des droits d'accès**. La page **Propriétés des rôles d'administration** s'ouvre. Le nouveau rôle s'affiche dans la liste des rôles.

    b. Cliquez sur **Enregistrer et éditer droits d'accès**.
    Une liste de droits d’accès pour la partition s’affiche sous la forme d’une matrice d’icônes de sélection indiquant l’état de chaque droit pour chaque rôle. Le nouveau rôle s’affiche à côté des autres rôles de niveau supérieur dans la partie supérieure de la matrice.

    c. Dans la section **Administration**, refusez explicitement l’autorisation **Afficher la page de liste de diffusion** pour le nouveau rôle. Enregistrez les modifications.
4. Affectez le nouveau rôle aux utilisateurs que vous souhaitez empêcher d’accéder à la page de liste de diffusion.
    a. Accédez à **Paramètres** > **Utilisateurs**. Sélectionnez l’utilisateur que vous souhaitez empêcher d’accéder à la liste des messages envoyés.
    b. Cliquez sur **Editer les rôles**. Le nouveau rôle que vous avez créé à l’étape précédente (un rôle configuré pour refuser l’accès) apparaît dans la liste **Rôles disponibles**.
    c. Déplacez le nouveau rôle de la liste **Rôles disponibles** vers la liste **Rôles**. Enregistrez les modifications.

Lorsque vous activez les restrictions d’accès pour la liste des messages envoyés, un utilisateur auquel le nouveau rôle a été affecté ne peut pas voir le lien **Présentation des messages**.

Mettez à jour la configuration pour activer les restrictions d’accès pour la liste des messages envoyés.

Activation de la restriction pour la liste des messages envoyés

Les utilisateurs accèdent à la liste des messages envoyés via l’option **Présentation des messages** du menu **Campaign**. Si vous restreignez l’accès à la liste des messages envoyés, la propriété Identifiant de la fonction de sécurité contrôle l’affichage de cette option de menu et, par conséquent, contrôle l’accès à la liste des messages envoyés.

Pour restreindre l’accès à la liste des messages envoyés, vous devez mettre à jour la propriété Identifiant de la fonction de sécurité dans la configuration Platform. Cette propriété s’applique à toutes les partitions de votre installation Campaign.

Lorsque vous remplissez l'identifiant de la fonction de sécurité avec la valeur correcte, l’option **Présentation des messages** n’est disponible que pour les utilisateurs disposant d’un rôle qui accorde explicitement l’autorisation Afficher la page de liste de diffusion Les utilisateurs avec des rôles pour lesquels le droit Afficher la page de liste de diffusion est refusé ou non octroyé ne peuvent pas voir l’option **Présentation des messages**.

1. Accédez à **Paramètres** > **Configuration** > **Plateforme** > **Navigation à l'échelle de la plateforme** > **Menu principal de navigation** > **Campaign** > **Mailings Deliver**. Cliquez sur **Mailings Deliver** pour afficher les paramètres de configuration.
2. Cliquez sur **Editer des paramètres**.
3. Dans la zone **Identifiant de la fonction de sécurité**, entrez `7000`. Enregistrez les modifications.

   Pour voir les résultats de la modification de la configuration, déconnectez-vous du système et reconnectez-vous.

Seuls les utilisateurs ayant des rôles qui accordent explicitement l’autorisation Afficher la page de liste de diffusion peuvent voir le lien **Présentation des messages** permettant d'accéder à la liste des messages envoyés.

Droits pour les rapports Deliver

Vos droits utilisateur déterminent votre capacité à afficher des rapports Deliver.

Pour plus d'informations sur la définition des droits d'accès aux rapports Deliver standard, voir la section consacrée à la génération de rapports et à la sécurité du document Unica Insights - Guide d'installation et de configuration de rapports.

Chapter 11. Technische Hinweise (Fehlerbehebung)

Problem (Kurzfassung)

Um die mit der Unica Campaign installierten Deliver-Komponenten zu verwenden und personalisierte Marketingnachrichten zu senden, müssen Sie die lokale Campaign-Installation mit fernen, von der HCL gehosteten Nachrichten-Ressourcen verbinden. In diesem Abschnitt wird beschrieben, wie Sie eine solche Verbindung konfigurieren, wenn Ihre Firewall-Regeln des Unternehmens eine direkte Kommunikation mit der gehosteten Umgebung verbieten.

Fehlerbehebung

Typische Kommunikation mit der gehosteten Umgebung für E-Mail-Ressourcen

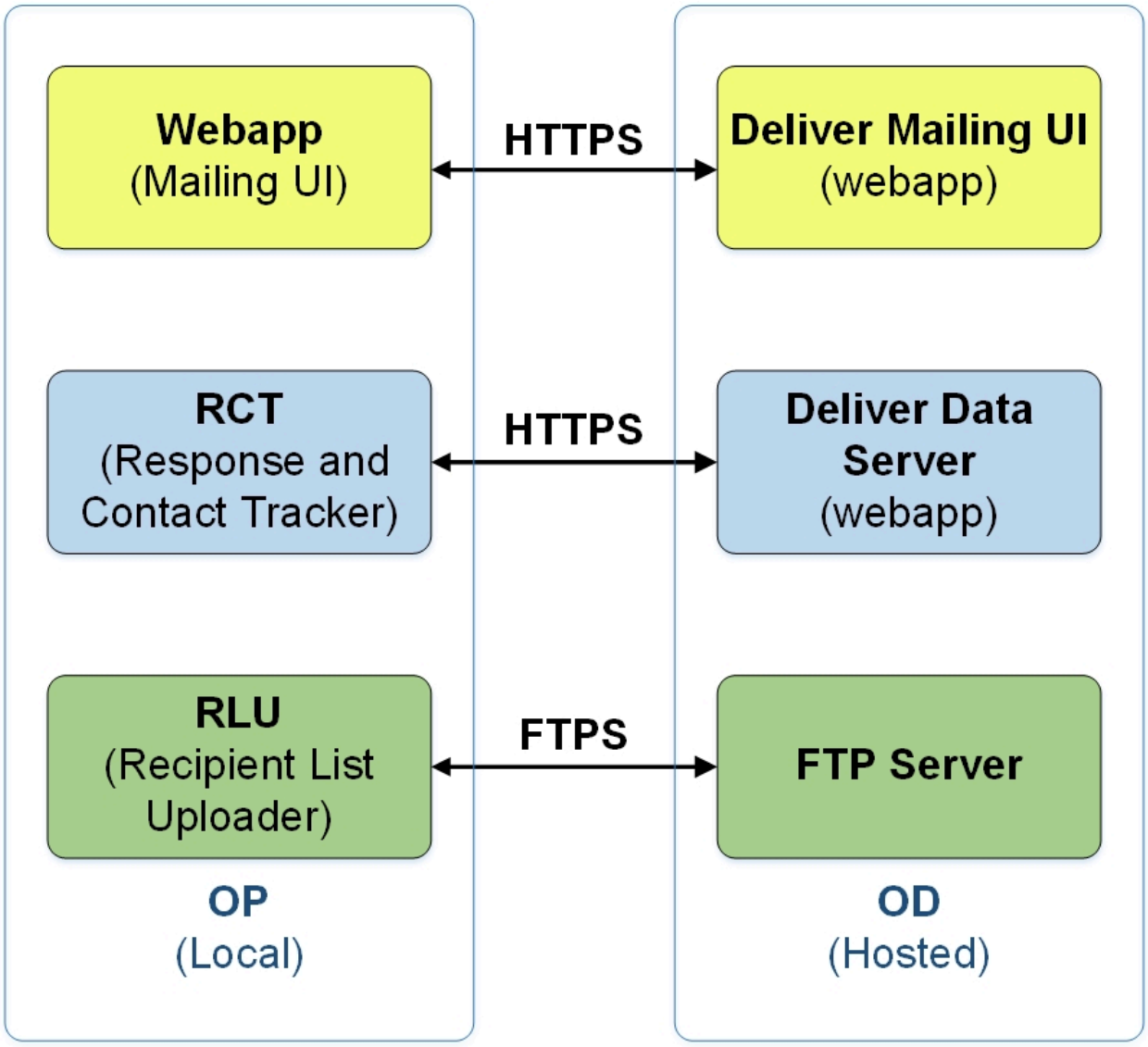
Das folgende Diagramm veranschaulicht die Standardkonfiguration für die Kommunikation zwischen der On Premises (OP)-Umgebung und der On Demand (OD)-Umgebung.

Die lokale Deliver OP Umgebung benötigt eine externe Kommunikation mit der Deliver OD Umgebung über HTTPS und SFTP.

Die OP-Umgebung enthält einen Webanwendungsserver (entweder IBM WebSphere oder Oracle WebLogic), auf dem Sie Campaign implementiert haben. Campaign hostet die Deliver-Komponenten (RCT und RLU), die mit den gehosteten E-Mail-Ressourcen in der OD-Umgebung kommunizieren.

Der Response and Contact Tracker (RCT) lädt Antwortdaten aus der OD-Umgebung.

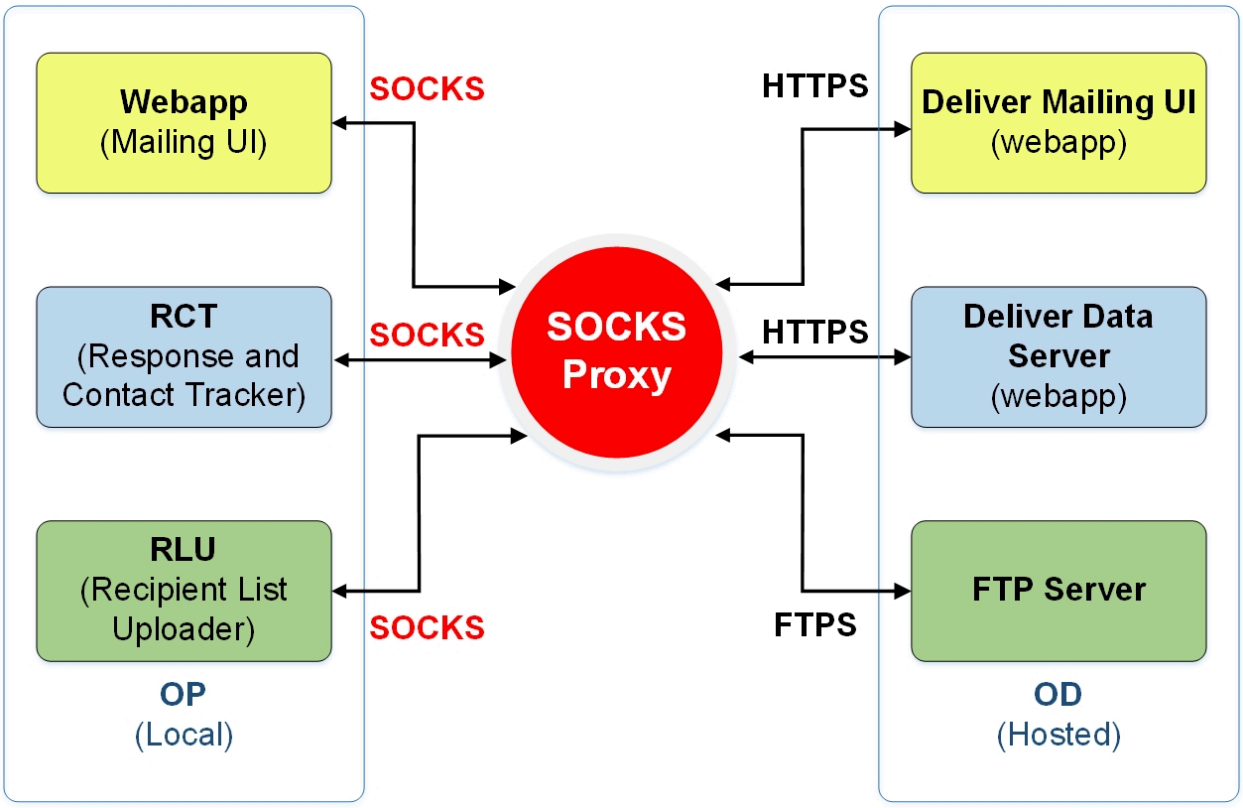
Der Response List Uploader (RLU) lädt Mailinglisten und andere erforderliche Mailingdaten in die OD-Umgebung hoch.



Wenn das System, auf dem Unica Deliver installiert ist, nicht direkt mit der OD-Umgebung kommunizieren kann, unterstützt Deliver die Kommunikation mit den gehosteten OD-Ressourcen über einen SOCKS-Proxy.

Connexion aux services de messagerie via un proxy

Le diagramme suivant illustre la communication entre les environnements OP et OD lors de l'utilisation d'un proxy SOCKS. Notez que le proxy SOCKS est configuré sur l'environnement local "sur site".



Vérifiez les points suivants avant d'activer les options de proxy.

- Le serveur proxy est un proxy SOCKS.
- Le serveur proxy peut accéder à l'environnement OD Deliver et autorise le trafic vers et depuis les ports configurés dans le centre de données HCL utilisé par votre compte de messagerie hébergé.
- Vous avez installé le proxy SOCKS de manière à ce que l'environnement OP Deliver puisse accéder au proxy.

Erforderliche Änderungen für die Weiterleitung von SFTP- und HTTPS-Datenverkehr durch einen SOCKS-Proxy

Um einen SOCKS-Proxy für den Zugriff auf von der HCL gehostete E-Mail-Ressourcen zu verwenden, müssen Sie Änderungen an der Webanwendung, in der Sie die Campaign bereitgestellt haben, und an den Startskripten für die Deliver RCT und RLU vornehmen.

Änderungen für SFTP vornehmen

Wenden Sie für SFTP-Datenverkehr die folgenden Konfigurationen auf die RLU und den Webanwendungsserver an.

- `- Dhcl.unica.deliver.ftp.proxy.host = <socksHost>`
- `- Dhcl.unica.deliver.ftp.proxy.port = <socksPort>`
- `- Dhcl.unica.deliver.ftps.proxy.match.hosts = <eine durch Komma getrennte Liste von Hostnamen und IP Adressen>`

socksHost ist der Hostname oder die IP des SOCKS Proxys.

socksPort ist der Port, auf dem der SOCKS Proxy ausgeführt wird.

`-Dhcl.unica.deliver.ftps.proxy.match.hosts` stimmt mit Hostnamen und IP Adressen überein, die bei der Weiterleitung des Datenverkehrs über den SOCKS Proxy verwendet werden.

Die für `-Dhcl.unica.deliver.ftps.proxy.match.hosts` angegebene IP Adresse ist die IP Adresse, die der FTP-Server in der gehosteten OD-Umgebung als Teil des SFTP-Protokolls bei der Datenübertragung an den FTP-Client in der lokalen OP-Umgebung sendet.

Setzen Sie `-Dhcl.unica.deliver.ftps.proxy.match.hosts` auf einen der folgenden Werte (abhängig vom Rechenzentrum, das von Ihrem gehosteten E-Mail Konto verwendet wird).

US Rechenzentrum: `-Dhcl.unica.deliver.ftps.proxy.match.hosts=ftp-em.unicadeliver.com`

Rechenzentrum Indien: `-Dhcl.unica.deliver.ftps.proxy.match.hosts=ftp-in.unicadeliver.com`

Europäisches Rechenzentrum: `-Dhcl.unica.deliver.ftps.proxy.match.hosts=ftp-eu.unicadeliver.com`

Änderungen für HTTPS vornehmen

Für den HTTPS Datenverkehr, nehmen Sie die folgenden Konfigurationen für das RCT und den Webanwendungsserver an.

`-Dhcl.unica.deliver.https.proxy.host= <socksHost>`

```
-Dhcl.unica.deliver.https.proxy.port= <socksPort>

-Dhcl.unica.deliver.https.proxy.type=SOCKS
```

socksHost ist der Hostname oder die IP des SOCKS Proxys.

socksPort ist der Port, auf dem der SOCKS Proxy ausgeführt wird.

Authentifizierungsanforderungen bei Verwendung eines SOCKS Proxys

Sollte Ihr SOCKS Proxy eine Authentifizierung erfordern, konfigurieren Sie Folgendes für die Webanwendungsserver, RLU und RCT.

- `-Dhcl.unica.deliver.proxy.auth.user = <Benutzername>`
- `-Dhcl.unica.deliver.proxy.auth.password = <Passwort>`

Dabei sind Benutzername und Passwort die Anmeldedaten, die für die Authentifizierung gegenüber dem Proxy erforderlich sind.

Pour configurer RCT à l'aide d'un proxy SOCKS

Configurez RCT pour qu'il fonctionne via un proxy SOCKS, suivez la procédure correspondant à votre système d'exploitation.

Pour RCT dans l'environnement Windows

Ajoutez les arguments de proxy suivants à `common.bat,` situé dans le répertoire `//deliver/bin` de votre installation Deliver locale.

```
set RCT PROXY ARGS=

-Dhcl.unica.deliver.https.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.https.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.https.proxy.type=SOCKS

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUIH_PASSWORD>

set RCT_JAVA_ARGS=%BASE<em>_VM_ARGS% %RCT_MEM_ARGS%

%RCT_EXTRA_VM_ARGS% %RCT_PROXY_ARGS
```

Pour RCT dans les environnements UNIX

Ajoutez les arguments de proxy suivants à `common.sh` situé dans le répertoire `\\deliver \bin` de votre installation Deliver locale.

Note: N'apportez pas de modifications directement à `rlu.sh.rct.sh` ou `setenv.sh`, car elles seront remplacées.

```
RCT PROXY ARGS="

-Dhcl.unica.deliver.https.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.https.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.https.proxy.type=SOCKS

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUIH_PASSWORD>

RCT_JAVA_ARGS="${BASE_VM_ARGS} ${RCT_MEM_ARGS} ${RCT_EXTRA_VM_ARGS}

${RCT_PROXY_ARGS}"
```

Pour configurer RLU en utilisant un proxy SOCKS

Pour configurer le RLU afin qu'il fonctionne via un proxy SOCKS, suivez la procédure correspondant à votre système d'exploitation.

Pour le RLU dans l'environnement Windows

Ajoutez les arguments proxy suivants au fichier common.bat situé dans le répertoire `// deliver/bin` de votre installation locale de Deliver.

```
set RLU PROXY ARGS=.

-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.ftp.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes et

d'adresses IP séparés par des virgules>.
```

```
-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUIH_PASSWORD>

définir RLU_JAVA_ARGS=%BASE_VM_ARGS% %RLU_MEM_ARGS% %RLU_EXTRA_VM_ARGS%

%RLU_PROXY_ARGS%.
```

Pour le RLU dans les environnements UNIX

Ajoutez les arguments proxy suivants au fichier common.sh, situé dans le répertoire `\ \deliver\bin` de votre installation locale de Deliver.

Note: Ne faites pas de changements directement dans `rlu.sh.rct.sh` ou `setenv.sh` car ils seront remplacés.

```
RLU PROXY ARGS=

-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.ftp.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes et

d'adresses IP séparés par des virgules>.

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUIH_PASSWORD>

RLU_JAVA_ARGS="${BASE_VM_ARGS} ${%RLU_MEM_ARGS%} ${%RLU_EXTRA_VM_ARGS%}

${RLU_PROXY_ARGS}"
```

Modifications de la configuration de WebSphere

Ajoutez les éléments suivants aux arguments de la JVM générique de WebSphere (voir la capture d'écran) :

```
-Dhcl.unica.deliver.https.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.https.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.bttps.proxy.type=SOCKS
```

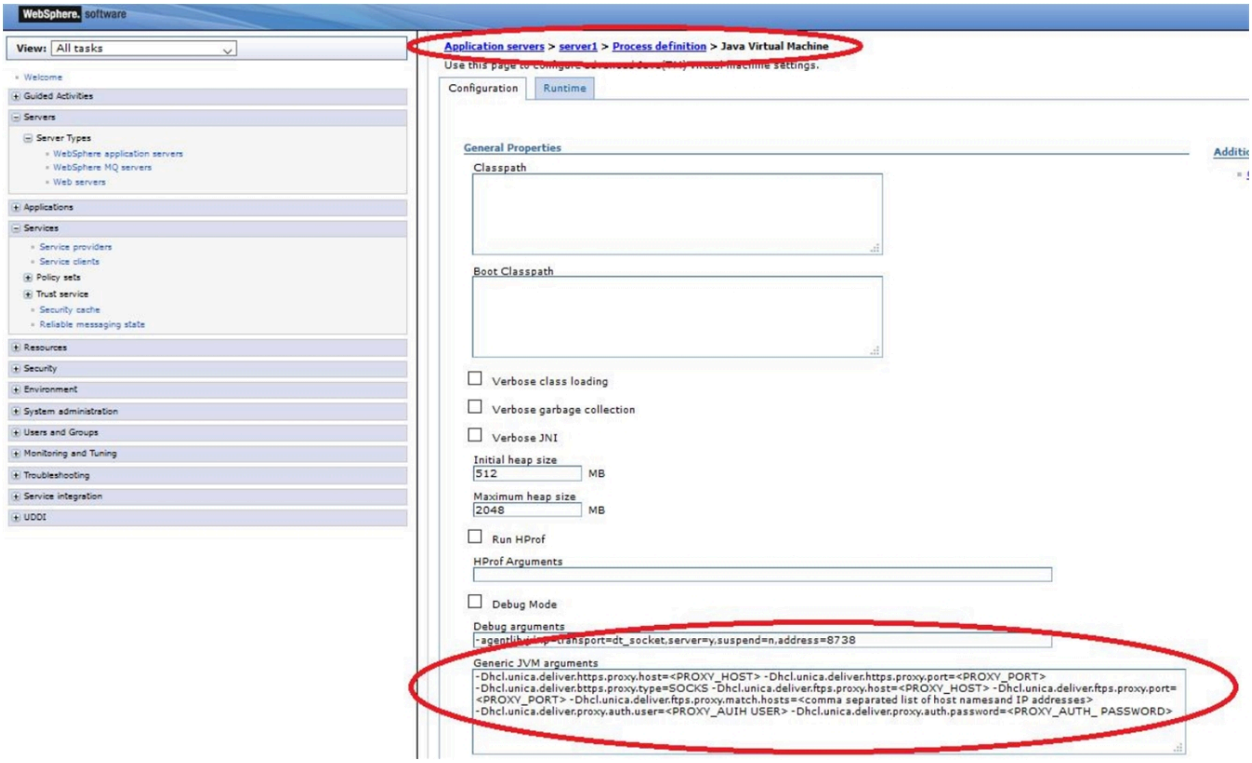
```
-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.ftp.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes et
d'adresses IP séparés par des virgules>.

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_ PASSWORD>
```



Modifications de la configuration d'Oracle WebLogic

Pour WebLogic, modifiez le script.

Dans l'environnement Windows

```
JAVA_OPTIONS=%(JAVA_OPTIONS)

-Dhcl.unica.deliver.https.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.https.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.bttps.proxy.type=SOCKS
```

```
-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.ftp.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes et
d'adresses IP séparés par des virgules>.

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_ PASSWORD>%.
```

Dans les environnements UNIX

```
JAVA_OPTIONS='(JAVA_OPTIONS)

-Dhcl.unica.deliver.https.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.https.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.bttps.proxy.type=SOCKS

-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>

-Dhcl.unica.deliver.ftp.proxy.port=<PROXY_PORT>

-Dhcl.unica.deliver.ftps.proxy.match.hosts=<liste de noms d'hôtes et
d'adresses IP séparés par des virgules>.

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_ PASSWORD>'.
```

Chapter 12. Konfiguration des Deliver Vertriebskanalkontos

Deliver unterstützt SMS, WhatsApp und Push als Zustellungskanäle, neben E-Mail. Deliver unterstützt SMS, WhatsApp und Push als Zustellungskanäle, neben E-Mail. SMS werden durch verschiedene Anbieter unterstützt, sodass der Kunde basierend auf geografischen und Kostenaspekten einen SMS-Partner auswählen kann. Wenn ein Kunde sich entscheidet, einen bestimmten Lieferanten für SMS- oder WhatsApp-Nachrichten zu verwenden, arbeitet HCL mit dem Kunden und dem ausgewählten Lieferanten zusammen, um ein problemloses Onboarding auf Deliver zu ermöglichen. Im Rahmen dieses Prozesses wird das Konto des Kunden mit jedem Lieferanten erstellt. Dieses Konto ermöglicht es Deliver, Nachrichten im Namen dieses Kunden zu senden und Antworten von Benutzern zu verarbeiten.

Deliver unterstützt die folgenden Kanäle.

- SMS mit Lieferant Karix
- SMS mit RML-Lieferant (Sowohl für Empfehlungs- als auch für Wiederverkäufer-Lizenzen)
- Whatsapp mit RML-Lieferant
- Push mit Kumulos als Lieferant

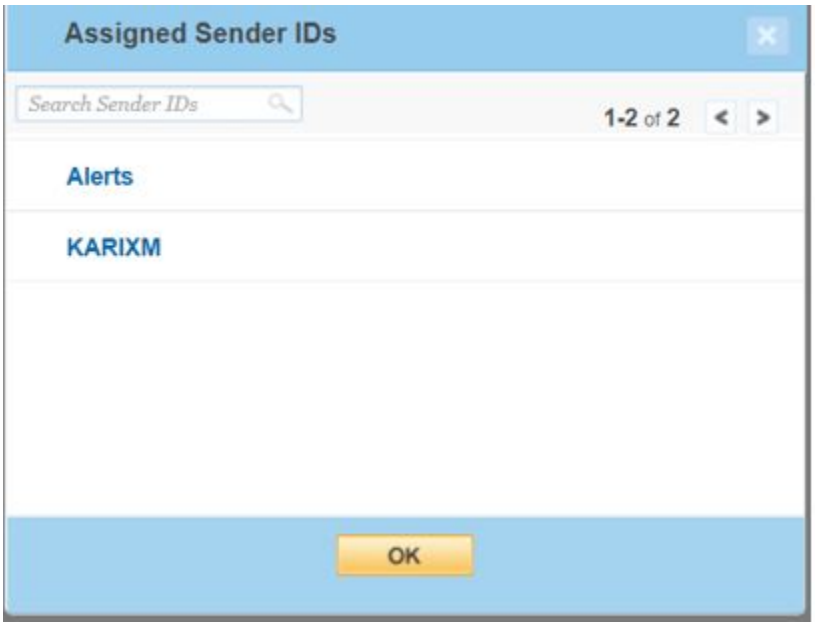
Das folgende Dokument erklärt die Schritte für jeden dieser Kanäle. Diese Schritte müssen von oder für jedes Kundenkonto im Rahmen des Onboarding-Prozesses ausgeführt werden.

Karix SMS Kontokonfiguration

Führen Sie die folgenden Schritte aus, um das Karix SMS-Konto des Kunden so zu konfigurieren, dass es mit Deliver funktioniert.

1. Melden Sie sich bei Karix Console (www.karix.solutions) an und klicken Sie die Schaltfläche API-Schlüssel im Dashboard, um einen API-Schlüssel zu erstellen und mit Deliver zu konfigurieren.

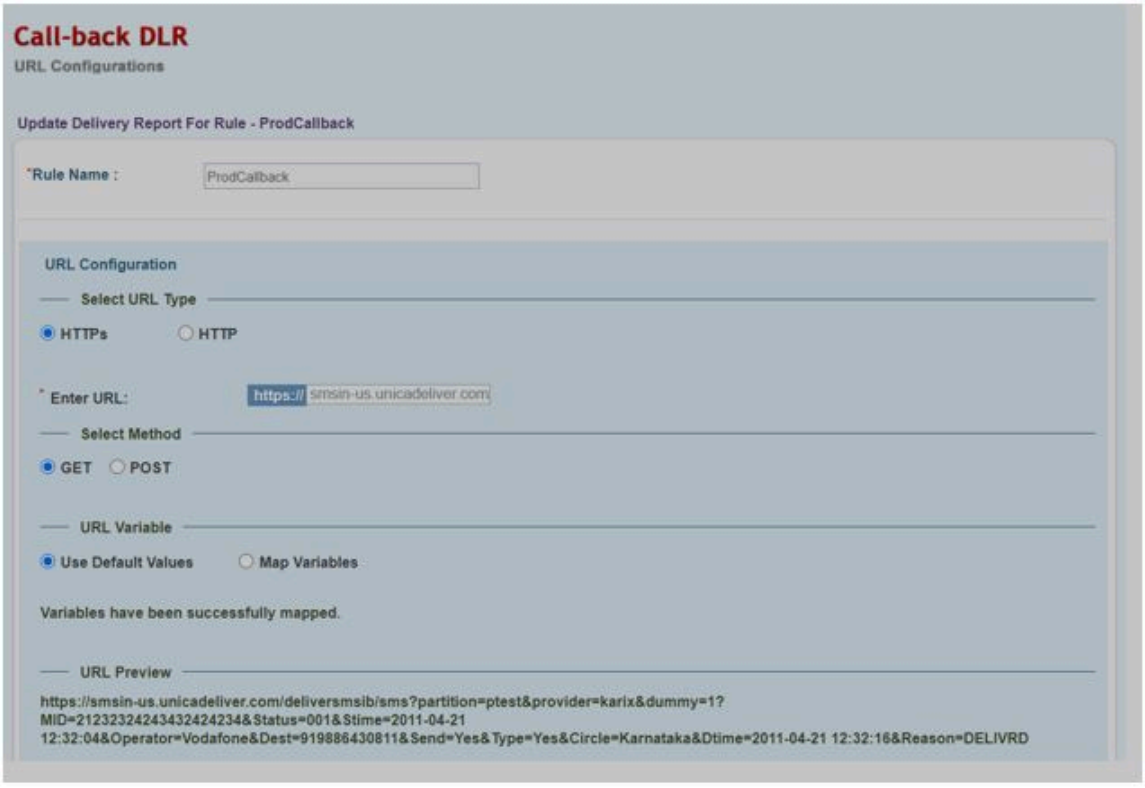
2. Wählen Sie in der rechten oberen Ecke unter der Liste " **Mein Konto öffnen** " die Option **Meine info bearbeiten** aus und notieren Sie sich die für Ihr Karix-Konto konfigurierte Absender-ID, um sie in Deliver zu konfigurieren.



3. Geben Sie den in Schritt 1 erstellten API-Schlüssel und die in Schritt 2 angegebene Absender-ID an, damit sie im Konto konfiguriert werden kann.
4. Legen Sie die Callback-URL in der Karix-Konsole fest.

- Für das US-Rechenzentrum: https://smsin-us.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=karix&dummy=1
- Für das EU Rechenzentrum: https://smsin-eu.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=karix&dummy=1
- Für Indien: https://smsin-in.unicadeliver.com/deliversmsib/sms?partition=%3Caccount%3E&provider=karix&dummy=1

Note: Sobald das Konto in Deliver konfiguriert ist, muss <account> in der obigen URL durch den vom Deliver Provisioning Team bereitgestellten Kontonamen ersetzt werden.



RML SMS Kontokonfiguration

Das RML-SMS-Konto des Kunden muss über die folgenden Konfigurationen verfügen, damit es mit Deliver funktioniert.

RML-Konto Einbindung

- Sie müssen mit RML Team arbeiten, um ein SMS Konto für Indien oder eine weltweite Position basierend auf der Position des Kunden zu erstellen.
- Die SenderID muss vom von RML konfigurierten Kunden bereitgestellt werden.
- SMS-Vorlagen müssen auch auf der Grundlage des Zielortes für den SMS-Versand in eine Whitelist aufgenommen werden. Zum Beispiel:
    - Indische Kunden müssen dem Deliver Services Team die Principal Entity ID (PE ID) zur Verfügung stellen und die auf der DLT-Plattform registrierten Vorlagen gemäß den Anweisungen im Benutzerhandbuch konfigurieren.
    - Für die USA und Kanada sind vorab genehmigte Vorlagen erforderlich.

RML verfügt über verschiedene Anmelde-URLs basierend auf der Region, die sie als Teil der E-Mail-Kontoerstellung von ihrer Seite bereitstellen. Beispiel: URLs für Indien und weltweite Rechenzentren

- Konto Indien: https://ems.rmlconnect.net/
- Weltweites Konto: https://client.rmlconnect.net/login

Führen Sie die folgenden Schritte aus.

1. Melden Sie sich gemäß den obigen URLs bei der RML-Konsole an und navigieren Sie zu **Dienstprogramme > DLR Push URL**.

    Note: Sie müssen RML auffordern, dieses Menü bei der Bereitstellung des Kontos hinzuzufügen.

2. Legen Sie die Callback-URL in der RML-Konsole fest.

- Für das US-Rechenzentrum: https://smsin-us.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=RML
- Für das EU Rechenzentrum: https://smsin-eu.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=RML
- Für das Rechenzentrum-Indien: https://smsin-in.unicadeliver.com/deliversmsib/sms?partition=%3Caccount%3E&provider=RML&dummy=1

Note: Sobald das Konto in Deliver konfiguriert ist, muss <account> in der obigen URL durch den vom Deliver Provisioning Team bereitgestellten Kontonamen ersetzt werden.

Einrichten von bidirektionalen SMS-Antworten mit RML

Deliver unterstützt bidirektionale SMS Antworten (Beispiel: STOP Anforderungen) mit RML seit v12.1.1. Bidirektionale SMS erfordert eine Absender-ID, die die von RML auf Anfrage bereitgestellten Antworten unterstützt.

RML unterstützt entweder dedizierte oder gemeinsam genutzte Funktionscodes. Für gemeinsam genutzte Funktionscodes muss der Benutzer den Markennamen an den Nachrichtenanfang setzen (Beispiel: HCL STOP), damit RML die Anfrage korrekt an Deliver delegieren kann. Es gibt keine solche Anforderung für einen dedizierten Funktionscode (Beispiel: Der Benutzer kann nur mit STOP antworten) und RML wird die Antwort korrekt dem erforderlichen Deliver-Konto zuordnen.

Damit RML Antworten an die richtige prod-Umgebung und das richtige Kundenkonto liefern kann, muss die Webhook URL für eingehende Antworten in der freigegebenen/zugewiesenen Absender-ID des Kunden wie folgt konfiguriert werden.

- Für das US-Rechenzentrum: https://smsin-us.unicadeliver.com/deliversmsib/mo/<account>?provider=RML
- Für das EU Rechenzentrum: https://smsin-eu.unicadeliver.com/deliversmsib/mo/<account>?provider=RML
- Für das Rechenzentrum Indien: https://smsin-in.unicadeliver.com/deliversmsib/mo/<account>?provider=RML

Note: <Konto> in der obigen URL muss durch den vom Deliver Services-Team bereitgestellten Kontonamen ersetzt werden, sobald das Konto in Deliver konfiguriert ist.

RML WhatsApp-Kontokonfiguration

Die Kunden, die mit der Funktion WhatsApp ausgestattet sind (bereitgestellt von RML), müssen die folgenden Schritte für die Konfiguration ausführen.

1. Erstellen Sie ein verifiziertes Facebook Business Manager-Konto, das für WhatsApp eingerichtet ist. Das RML-Team führt Kunden dazu, das Konto von Facebook Business Manager nach Bedarf zu konfigurieren.
2. Erstellen Sie ein WhatsApp-Konto mit RML. RML erstellt dieses Konto, nachdem die Überprüfung des Facebook Business Manager-Kontos abgeschlossen ist.
3. Erstellen von Nachrichtenvorlagen, die von WhatsApp genehmigt wurden. Das RML Team wird mit Kunden arbeiten, um Nachrichtenvorlagen im erforderlichen Format vorzubereiten und sie vom Kunden zu genehmigen.
4. Sobald RML den Kunden freigegebene Vorlagen zur Verfügung stellt, müssen sie diese über den Menüpunkt **Neu > WhatsApp** Inhalt in den Deliver Message Editor hochladen. Alle Details müssen genau wie in der genehmigten Vorlage angegeben werden, da WhatsApp nach der Genehmigung keine Änderungen an der Vorlage zulässt.
5. Konfigurieren Sie die Callback-URL im RML-WhatsApp-Konto. Hierzu müssen Sie RML die unten stehende URL bereitstellen, damit diese als Callback URL für WhatsApp-Nachrichten-Deliver Berichte konfiguriert werden kann.
    - Für das US Rechenzentrum: https://smsin-us.unicadeliver.com/deliversmsib/wa/ <account>
    - Für das EU Rechenzentren: https://smsin-eu.unicadeliver.com/deliversmsib/wa/ <account>

- Für das Rechenzentrum Indien: https://smsin-in.unicadeliver.com/deliversmsib/wa/ <account>

Note: <Konto> in der obigen URL muss durch den vom Deliver Services-Team bereitgestellten Kontonamen ersetzt werden, sobald das Konto in Deliver konfiguriert ist.

Index