HCLSoftware

Unica Deliver V12.1.1 Guide de démarrage et de l'administrateur

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.

Établissement d’un compte de messagerie hébergé avec Unica

Lorsque vous souscrivez un abonnement, Unica crée un compte de messagerie hébergée en votre nom et vous envoie les données d'identification du compte dont vous aurez besoin pour utiliser les fonctions de message. Vous appliquez ces données d’identification lorsque vous configurez vos applications HCL Unica locales pour accéder à l’environnement de messagerie hébergée via des connexions sécurisées.

Vous devez disposer d'un compte valide pour accéder aux ressources de message que Unica fournit en tant que service logiciel. Si votre installation HCL Unica inclut plusieurs partitions et que vous prévoyez d'utiliser un message dans plus d'une partition, vous avez besoin d'un compte de messagerie hébergé et d'au moins un fournisseur de services pour WhatsApp et SMS pour chaque partition. Vous ne pouvez pas partager de comptes de messagerie entre des installations ou des partitions.

L’établissement d’un compte de messagerie hébergé est le début du processus de démarrage, qui dure environ 90 jours. Vous pouvez vous abonner à SMS ou WhatsApp conformément aux exigences. Pour une description générale du processus, voir la rubrique suivante.

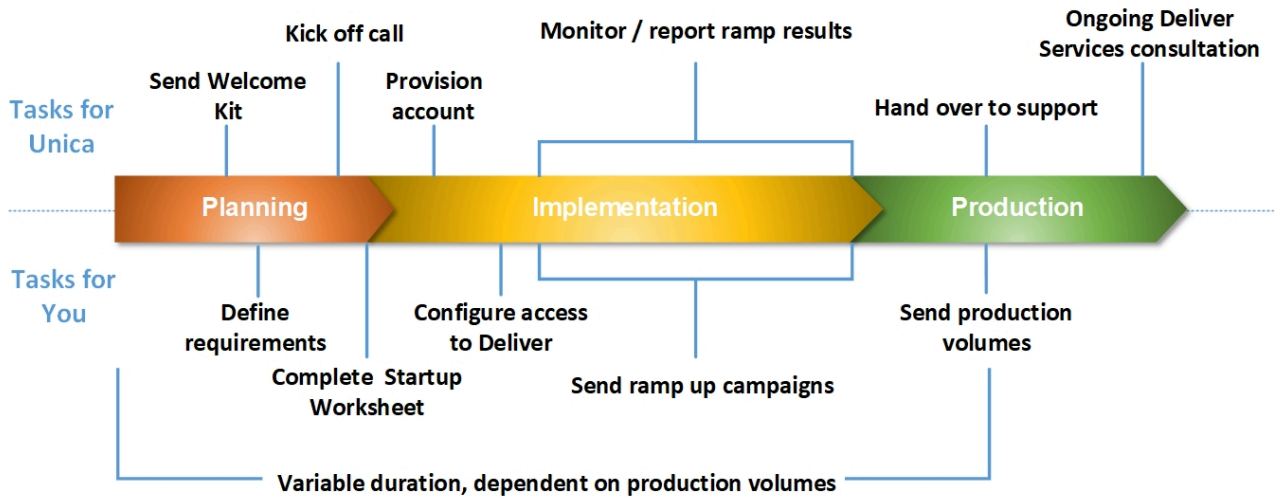
Vue d’ensemble du processus de démarrage

Vous pouvez activer les fonctions de message dans Unica Campaign pour effectuer des campagnes de marketing numérique hautement ciblées. Campaign utilise les fonctions de message fournies par Unica Deliver via des ressources

hébergées dans des centres de données aux Etats-Unis et en Europe. Un compte permettant d'accéder à ces ressources de messages électroniques est inclus avec votre abonnement Deliver. Vous pouvez également choisir les canaux WhatsApp, Push ou SMS conformément aux exigences.

Unica lance un processus de démarrage après la création de votre compte de messagerie hébergé. Unica vous aide à vous familiariser avec Deliver, à vous connecter aux ressources de message et d'établir votre réputation comme spécialiste du marketing numérique parmi les principaux fournisseurs d'accès Internet (FAI).

Le processus se déroule en trois phases. Les équipes Services professionnels Unica et Deliver Services vous guident tout au long de la procédure.



Le consultant des services professionnels est votre point de contact principal avec Unica au cours du processus de démarrage. Une fois le processus de démarrage du compte terminé, le consultant des services professionnels transfère la responsabilité du support principal à l'équipe de support du produit Unica .

Un consultant Deliver Services dédié fournit une assistance spéciale pour les problèmes liés aux messages. Il est essentiel de créer une réputation de message favorable auprès des principaux fournisseurs d'accès à Internet (FAI) pour vous assurer que vos campagnes marketing numérique atteignent les destinataires cible de manière homogène. Lorsque vous commencez à exécuter des mailings, le consultant EAS passe en revue les performances de délivrabilité du mailing et suggère les meilleures façons de développer progressivement votre réputation de message.

Activités de démarrage et jalons

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

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 volumineux ou fréquents des domaines de messagerie qu'ils ne reconnaissent pas légitimement.	Votre organisation (avec prise en charge de Unica)
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

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.

Que faire ensuite

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.

À propos de cette tâche

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

À propos de cette tâche

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`.

Que faire ensuite

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 8.

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`

Que faire ensuite

Pour plus d'informations sur ces propriétés de configuration et sur la configuration de Deliver, voir Configurations pour Unica Deliver à la page 46.

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.

À propos de cette tâche

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 58.

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.

Chapitre 3. Connexions aux services de messagerie

Pour accéder aux services de messagerie fournis par Unica, vous devez configurer une connexion entre l'installation locale de HCL Unica et HCL Unica.

Les spécialistes du marketing accèdent aux fonctions Deliver via l'interface Campaign. Si vous travaillez avec Deliver, vous devez établir une connexion Internet sécurisée et automatique que Campaign peut utiliser pour charger des listes de destinataires de message dans HCL Unica. Les composants Deliver installés avec Campaign utilisent également cette connexion pour télécharger les données de contact et de réponse dans les tables système Deliver du schéma Campaign.

Remarque : Chaque instance de Campaign requiert une connexion unique à HCL Unica. Si l'installation Campaign inclut plusieurs partitions, chaque partition nécessite un compte de messagerie hébergé distinct. Les comptes peuvent partager la connexion IP avec HCL Unica.

Toutes les communications entre HCL Unica et les services hébergés HCL Unica sont réalisées via SSL. Chaque communication depuis les services hébergés HCL Unica est une réponse à une demande provenant de l'environnement local. Les services hébergés HCL Unica ne tentent jamais d'établir une connexion avec votre réseau d'entreprise. Toutes les communications avec les services hébergés HCL Unica proviennent de derrière le pare-feu de votre entreprise.

Exigences pour la configuration de la connexion aux services hébergés HCL Unica

La configuration d'une connexion aux services hébergés HCL Unica requiert des droits d'administration et les informations relatives au compte de messagerie hébergé établi pour votre organisation.

Pour configurer une connexion de messagerie hébergée, vous devez disposer des éléments suivants.

- Nom d'utilisateur et mot de passe fournis par Unica pour le compte de messagerie hébergé
- Droits de créer ou de modifier des utilisateurs système dans Unica Platform
- Accès administratif aux propriétés de configuration conservées dans l'installation locale Unica Platform
- Accès administrateur au serveur d'applications Web sur lequel Unica Platform et Campaign sont déployés

Vous devez connaître ou être en mesure de consulter des personnes connaissant les exigences de votre entreprise en matière de sécurité des données. Avant de commencer, consultez ces procédures pour savoir comment créer la connexion nécessaire en conformité avec les restrictions de pare-feu de votre entreprise.

Vous devez vous familiariser avec la configuration des connexions sécurisées sur votre serveur d'applications Web, IBM WebSphere®, Oracle WebLogic, Apache Tomcat et JBoss.

Conditions requises pour le téléchargement des données versHCL Unica services hébergés

Une Deliver composant appelé Recipient List Uploader (RLU) fait partie de votre Unica Campaign installation. Le RLU utilise SFTP comme mécanisme préféré pour gérer le téléchargement des listes de destinataires et des métadonnées associées

vers les services hébergés HCL Unica. Il prend également en charge le FTP en mode passif en tant que mécanisme ancien mais obsolète pour les téléchargements de listes de destinataires.

Deliver utilise SFTP pour télécharger des données. Lors de l'utilisation de SFTP, la RLU initie toutes les demandes de connexion de téléchargement en tant que client local. HCL Unica les services hébergés n'initient jamais de demande de connexion à votre réseau.

Deliver prend en charge deux méthodes FTP passives, FTP explicite et FTP implicite. Le FTP explicite est la méthode utilisée par défaut pour télécharger les listes de destinataires. Pour utiliser le FTP implicite, vous devez apporter des modifications aux propriétés de configuration de Deliver.

Pour plus d'informations sur le FTP en mode passif et l'utilisation de FTP sur SSL, voir RFC959 et RFC2228.

Exigences en matière de connexion et de port

Pour communiquer avec les services hébergés HCL Unica, vous devez disposer d'une connexion à Internet. Les services hébergés HCL Unica utilisent des ports spécifiques.

L'installation locale de HCL Unica et les services hébergés de HCL Unica utilisent les ports suivants pour communiquer.

HTTPS: port 443

Port SFTP

- port 2222

Port de commande FTP:

- Explicite FTP : port 21
- FTP implicite : port 990

Ports de téléchargement de données FTP

- Centre de données américain

  FTP explicite : ports 15393 à 15443

  FTP implicite : ports 15600 à 15650

- Centre de données en Europe

  FTP explicite : ports 15393 à 15443

  FTP implicite : ports 15600 à 15650

HCL Unica Les services hébergés n'établissent jamais de connexion avec votre réseau local. Il ne répond qu'aux demandes de connexion initiées depuis l'arrière de votre pare-feu.

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
    ```

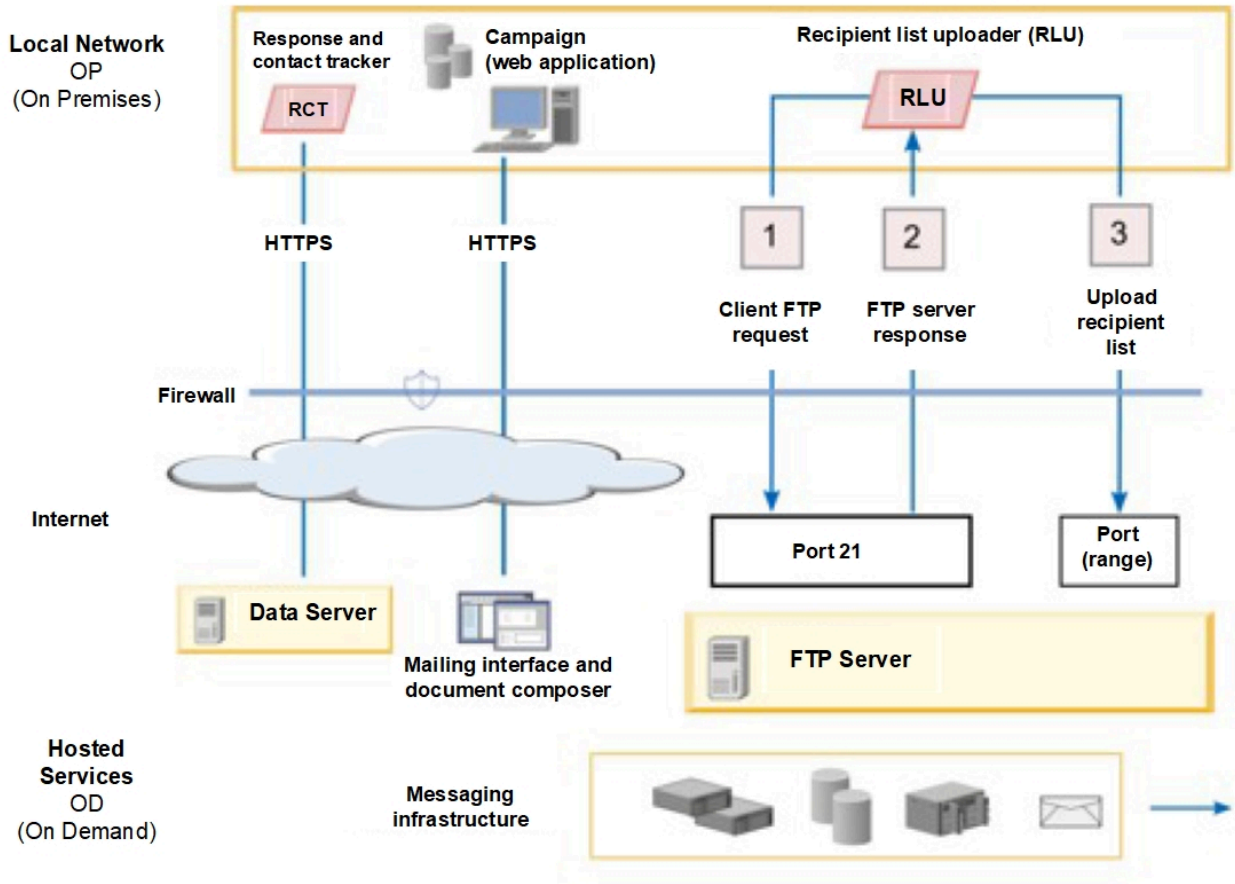
Note: Tous les chemins de fichier spécifiés ci-dessus doivent être complets, y compris le nom du fichier. Répétez les étapes 7 à 9 pour toutes les partitions, où Deliver est configuré.

Connexion de téléchargement par FTP explicite

Le télé-chargeur de liste de destinataires (RLU) utilise un protocole FTP, FTPS ou SFTP explicite lorsque le système télécharge une liste de destinataires d'e-mails. La section suivante comprend les détails de la connexion en amont par FTP et FTPS. Les méthodes FTP et FTPS sont dépréciées. La liste des destinataires est également appelée table des listes de sortie (OLT).

Le RLU établit une connexion avec les services hébergés sur HCL Unica via le port de commande FTP par défaut (port 21). Il émet une demande de cryptage de la session via SSL. Sur la connexion sécurisée, le RLU négocie avec le serveur FTP pour établir une liaison SSL distincte sur un port choisi au hasard par le RLU. Pour plus d'informations sur le FTP explicite, voir la RFC 2228.

Le schéma suivant illustre la méthode par défaut pour télécharger les données des destinataires de Campaign vers les services hébergés de HCL Unica.



Le tableau suivant décrit la séquence de connexion.

Etape	Action	La description
1	Demande initiale de connexion FTP du client	Derrière le pare-feu de l'entreprise, le RLU lance une session de téléchargement de données en utilisant FTP sur SSL explicite. Le RLU envoie la demande de connexion SSL à l'adresse des services hébergés HCL Unica. Vous devez configurer cette adresse à l'avance. Pour démarrer la session, le RLU ouvre un port choisi au hasard du côté client comme port de commande FTP. Les services hébergés sur HCL Unica acceptent les connexions de commande FTP sur le port 21.
2	Réponse du serveur FTP distant	En réponse à la demande du RLU d'une session SSL sécurisée, le serveur FTP désigne le port de données FTP à utiliser pour le téléchargement de la liste des destinataires.
5	Téléchargement de la liste des destinataires	Le RLU commence le téléchargement de la liste sur le port de données spécifié. Lorsque le téléchargement est terminé, le RLU interrompt la connexion FTP.

Pour connaître la gamme des ports de données que le serveur FTP peut spécifier, voir Exigences en matière de connexion et de port on page 14.

Configuration de la connexion FTP explicite

Aucune configuration supplémentaire n'est requise. Par défaut, RLU utilise un protocole FTP explicite.

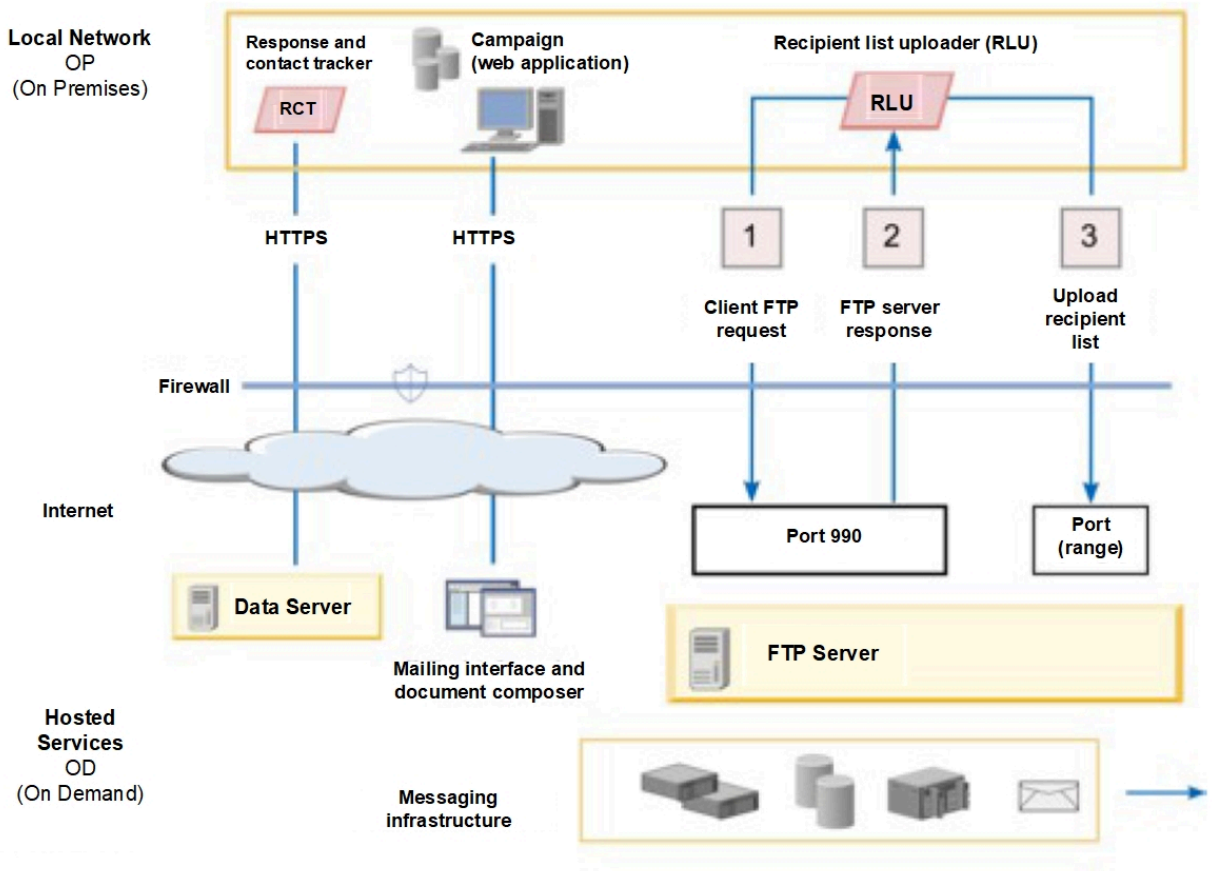
Chargement de données avec FTP implicite

Vous pouvez configurer RLU pour qu'il utilise le protocole FTP implicite pour charger les listes de destinataires de courrier électronique. Le protocole FTP implicite utilise le port 990 pour établir une connexion aux services hébergés HCL Unica.

Lorsque vous activez le protocole FTP implicite pour RLU, la session toute entière est chiffrée depuis le début. Le protocole FTP implicite est différent de la connexion via le protocole FTP explicite, où RLU demande explicitement un lien sécurisé.

Pour utiliser le protocole FTP implicite pour charger des listes de destinataires, vous devez révéler et configurer une propriété de configuration système dans les propriétés de configuration de Deliver.

Le diagramme suivant montre comment RLU charge les données des destinataires vers les services hébergés HCL Unica lorsque le système est configuré pour utiliser le protocole FTP implicite.



Le tableau suivant décrit la séquence de connexion.

Etape	Action	Description
1	Demande de connexion FTP du client initial	Derrière le pare-feu de l'entreprise, RLU lance une session de chargement de données via FTP avec chiffrement SSL. RLU envoie la demande de connexion SSL à l'adresse correspondant aux services hébergés HCL Unica. Vous devez configurer cette adresse à l'avance. Pour démarrer la session, RLU ouvre le port 990. Les services hébergés HCL Unica acceptent les connexions de commande FTP chiffrées uniquement sur le port 990.
2	Réponse du serveur FTP distant	Si les services hébergés HCL Unica reconnaissent la demande en tant que demande FTP implicite valide, le serveur FTP accepte la demande de connexion. Elle désigne

Etape	Action	Description
		le port de données FTP à utiliser pour le chargement de la liste de destinataires. Voir Exigences en matière de connexion et de port à la page 14 pour connaître la plage de ports de données que le serveur FTP peut spécifier.
3	Chargement de la liste de destinataires	RLU commence le chargement de la liste via le port de données spécifié. Une fois le chargement terminé, RLU interrompt la connexion FTP.

Accès aux paramètres de configuration pour le chargement FTP implicite

Pour configurer le système afin qu'il utilise le protocole FTP implicite pour le chargement des données, vous devez éditer les propriétés de configuration qui sont masquées par défaut. Vous exécutez un script pour afficher les propriétés.

À propos de cette tâche

Pour configurer le système afin qu'il utilise le protocole FTP implicite pour le chargement des données, rendez les propriétés de configuration suivantes visibles. Ces propriétés sont masquées par défaut.

- `Deliver > serverComponentsAndLocations > hostedServices > ftpPort`
- `Deliver > serverComponentsAndLocations > hostedServices > useFTPImplicitSSL`

Cette procédure révèle les propriétés de configuration, mais ne les configure pas. Pour activer le protocole FTP implicite, vous devez accéder à ces propriétés dans la configuration Deliver et les configurer. Pour des informations sur la configuration de ces propriétés, voir Activation du chargement FTP implicite à la page 22.

Pour afficher `ftpPort` et `useFTPImplicitSSL` dans le répertoire **Tools** de votre installation Deliver, exécutez le script `switch_config_visibility` à partir du script de ligne de commande, comme suit.

Windows™

```
\switch_config_visibility.bat -p "Affinium|Deliver|serverComponentsAndLocations|hostedServices|ftpPort" -v true

\switch_config_visibility.bat -p "Affinium|Deliver|serverComponentsAndLocations|hostedServices|useFTPImplicitSSL" -v true
```

UNIX™

```
/switch_config_visibility.sh -p "Affinium|Deliver|serverComponentsAndLocations|hostedServices|ftpPort" -v true

/switch_config_visibility.sh -p "Affinium|Deliver|serverComponentsAndLocations|hostedServices|useFTPImplicitSSL" -v true
```

Que faire ensuite

Vous devez redémarrer le serveur d'application Web pour rendre ces propriétés visibles dans la configuration Deliver.

Activation du chargement FTP implicite

Pour activer le protocole FTP implicite, vous devez mettre à jour la configuration Deliver.

Avant que tu commences

Pour effectuer cette tâche, vous devez révéler deux propriétés de configuration. Pour plus d'informations, voir Accès aux paramètres de configuration pour le chargement FTP implicite à la page 21.

1. Accédez à `Paramètres > Configuration > Deliver > serverComponentsAndLocations > hostedServices`.
2. Cliquez sur **Editer des paramètres**.
    - Vérifiez que `useFTPImplicitSSL` est défini sur `true`.
    - Définissez `ftpPort` sur `990`.
3. Sauvegardez vos modifications.

Que faire ensuite

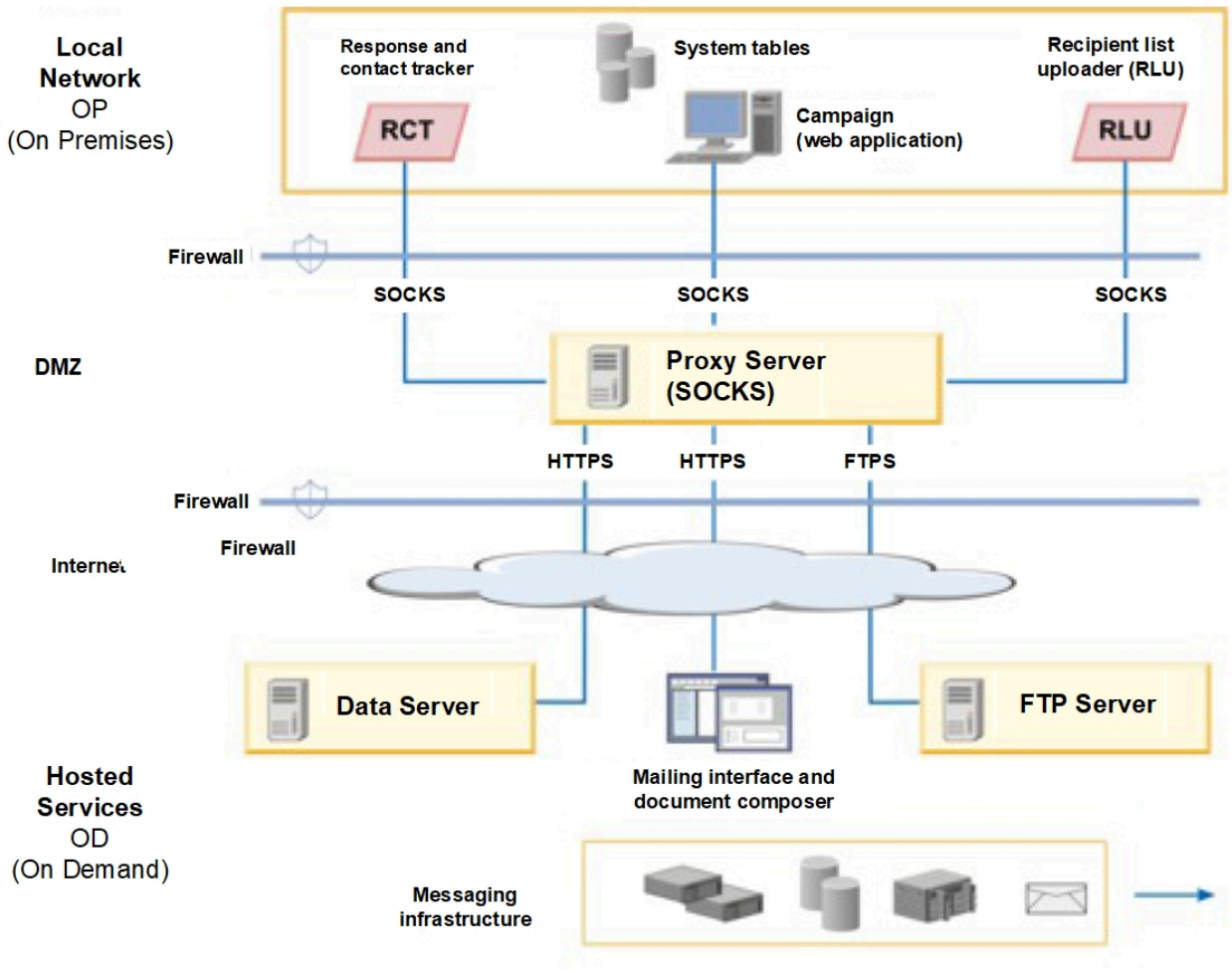
Les modifications ne prennent effet qu'après le redémarrage du serveur d'applications Web et du programme d'écoute Campaign. Vous pouvez effectuer cette opération maintenant ou attendre la fin de toutes les étapes de configuration du démarrage.

Connexion via un proxy HTTP

Si les règles de votre pare-feu d'entreprise interdisent la communication directe avec l'Internet public, vous pouvez vous connecter à HCL Unica via un serveur proxy HTTP. Deliver prend en charge la connexion via un serveur proxy SOCKS qui autorise le trafic HTTPS et FTPS.

Deliver prend en charge le protocole SOCKS version 5.

Le schéma suivant illustre la communication entre l'environnement local et l'environnement hébergé lorsque vous utilisez un proxy SOCKS.



Vous configurez le serveur proxy SOCKS dans l'environnement local sur site. Avant de commencer à configurer le serveur proxy, confirmez que vous remplissez les conditions suivantes.

- Le serveur proxy doit être un serveur proxy SOCKS.
- Le serveur proxy doit pouvoir accéder à l'environnement OD Deliver. Le serveur doit autoriser le trafic vers et depuis les ports configurés pour le centre de données utilisé par votre compte de messagerie hébergé. Unica possède des centres de données aux États-Unis, en Europe et en Inde.
- L'environnement Deliver OP doit pouvoir accéder au serveur proxy SOCKS.

Configuration du routage pour le trafic SFTP/FTPS et HTTPS via un proxy SOCKS

Pour utiliser un proxy SOCKS afin d'accéder aux ressources de messagerie hébergées, vous devez mettre à jour le serveur d'applications Web où vous avez déployé Campaign. Vous devez également modifier les scripts de démarrage pour le RCT et le RLU de Deliver.

- Pour le trafic SFTP/FTPS, appliquez les configurations suivantes à la RLU et au serveur d'applications Web.

Paramètre	Description
`-Dhcl.unica.deliver.ftp.proxy.host = <socksHost>`	Nom d'hôte ou IP du proxy SOCKS.
`-Dhcl.unica.deliver.ftp.proxy.port = <socksPort>`	Le port sur lequel le proxy SOCKS fonctionne.
`-Dhcl.unica.deliver.ftps.proxy.match.hosts= <liste séparée par des virgules de noms d'hôtes et d'adresses IP>.`	Noms d'hôtes et adresses IP qui sont utilisés lors de l'acheminement du trafic par le proxy SOCKS. Fournissez des valeurs spécifiques au centre de données utilisé par votre compte.

Lorsque les environnements local et hébergé établissent une connexion de données, l'adresse IP spécifiée pour `-Dhcl.unica.deliver.ftps.proxy.match.hosts` est l'adresse IP que le serveur FTP distant envoie au client FTP local.

Définissez `-Dhcl.unica.deliver.ftps.proxy.match.hosts` sur l'une des valeurs suivantes. La valeur que vous entrez dépend du centre de données qui est utilisé par votre compte de messagerie hébergé.

Nom d'hôte et adresses IP pour le centre de données américain :

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

ftp-em.unicadeliver.com
```

Nom d'hôte et adresses IP pour le centre de données européen :

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

ftp-eu.unicadeliver.com
```

Nom d'hôte et adresses IP pour le centre de données en Inde :

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

```
ftp-in.unicadeliver.com
```

- Pour le trafic HTTPS, appliquez les configurations suivantes au RCT et au serveur d'applications web.

Paramètre	Description
`-Dhcl.unica.deliver.https.proxy.host=<socksHost>`	Nom d'hôte ou IP du proxy SOCKS
`-Dhcl.unica.deliver.https.proxy.port=<socksPort>`	Le port sur lequel le proxy SOCKS fonctionne.
`-Dhcl.unica.deliver.https.proxy.type=SOCKS`	Le type de serveur proxy. Vous devez utiliser un serveur proxy SOCKS.

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_AUTHENTIFICATION_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_AUTHENTIFICATION_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>'.
```

Débit de téléchargement des données et paramètre de port

Un composant Deliver appelé RCT (Response and contact Tracker) est installé dans le cadre de votre installation Unica Campaign. RCT demande régulièrement des données de suivi et de réponse d'e-mail à HCL Unica. Par défaut, RCT émet une demande de données toutes les 5 secondes.

RCT émet des demandes de données sur HTTPS (HTTP sur SSL). Les services hébergés HCL Unica acceptent les demandes de connexion HTTPS sur le port 443, et uniquement à partir des hôtes que vous avez spécifiés lors du processus de démarrage du compte de messagerie hébergé.

Configuration d'un utilisateur système pour accéder aux services hébergés HCL Unica

Les composants Deliver doivent être en mesure d'accéder aux services hébergés HCL Unica sans qu'il soit nécessaire d'entrer manuellement des identifiants de connexion. Pour établir une connexion automatique, définissez un utilisateur système dans Platform qui peut fournir les données d'identification d'accès requises.

Pour simplifier l'administration des utilisateurs et le traitement des incidents, vous pouvez modifier un utilisateur système existant pour accéder aux services hébergés et aux tables système locales. Vous pouvez configurer un utilisateur système unique pour fournir des données d'identification pour plusieurs systèmes. Par exemple, en modifiant la configuration de l'utilisateur système Campaign, vous créez un utilisateur unique qui peut automatiquement accéder aux services hébergés HCL Unica et aux tables système Deliver du schéma Campaign.

Les données d'identification requises pour accéder aux services hébergés HCL Unica correspondent au nom d'utilisateur et au mot de passe fournis par Unica pour votre compte de messagerie hébergé. Les données d'identification que vous utilisez varient selon que vous connectiez au centre de données Unica des Etats-Unis ou au centre de données géré par Unica en Europe. Consultez Unica pour savoir quel centre de données vous utilisez.

Pour plus d'informations sur la configuration d'un utilisateur système pour qu'il communique avec les services hébergés HCL Unica, voir le document *Unica Deliver - Guide de démarrage et d'administration.*

pour obtenir des informations générales sur la procédure de création des utilisateurs système et des sources de données, voir le document *Unica Platform - Guide d'administration*.

Configuration de l'accès des partitions aux services hébergés HCL Unica

Les composants Unica Deliver de la partition doivent être autorisés à fournir automatiquement des identifiants de connexion valides lors d'une tentative de connexion aux services hébergés HCL Unica. Pour ce faire, vous devez ajouter les données d'identification de connexion aux services hébergés HCL Unica à un utilisateur Platform. Cet utilisateur devient l'utilisateur système Deliver.

Vous pouvez ajouter la source de données de plateforme contenant les données d'identification aux services hébergés HCL Unica à l'utilisateur système Deliver. Cet utilisateur peut être le même utilisateur système que celui qui accède aux tables système Campaign dans la partition.

Les étapes de configuration des utilisateurs système d'une partition sont identiques à celles suivies au cours de l'installation initiale de Deliver pour créer la première partition. Pour plus d'informations sur l'ajout d'identifiants de connexion aux services hébergés HCL Unica à un utilisateur système, voir le document *Unica Deliver - Guide de démarrage et d'administration* .

Les données d'identification requises pour accéder aux services hébergés HCL Unica sont le nom d'utilisateur et le mot de passe fournis par Unica lors de l'étape initiale du processus de démarrage.

Important : Pour chaque partition supplémentaire, vous devez demander un nom d'utilisateur et un mot de passe distincts à Unica.

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.

Avant que tu commences

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.

À propos de cette tâche

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.

Que faire ensuite

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

Configuration des adresses pour la connexion aux services hébergés sur HCL Unica

Pour garantir une connexion correcte aux services hébergés de HCL Unica, vous devez saisir les adresses comme valeurs des propriétés de configuration dans la configuration de Deliver. Les adresses de connexion que vous saisissez varient selon que vous vous connectez au centre de données Unica aux États-Unis ou au centre de données Unica en Europe.

Before you begin

Consultez Unica pour confirmer quel centre de données votre compte de messagerie hébergé utilise.

Sur le site Unica Platform, accédez à **Paramètres > Configuration**. Dans la configuration Deliver, accédez aux propriétés de la configuration Deliver suivantes et confirmez ou mettez à jour les paramètres de connexion, en fonction du centre de données utilisé par votre compte.

- `Deliver > serverComponentsAndLocations > hostedServices> uiHostName`

  Pour se connecter au centre de données d'Unica aux États-Unis, changez cette valeur en `em.unicadeliver.com`.

  Pour se connecter au centre de données Unica en Europe, changez cette valeur en

  `em-eu.unicadeliver.com`.

  Pour se connecter au centre de données Unica en Inde, changez cette valeur en

  `em-in.unicadeliver.com`

- `Deliver > serverComponentsAndLocations > hostedServices> dataHostName`

Pour se connecter au centre de données d'Unica aux États-Unis, changez cette valeur en `em.unicadeliver.com`.

Pour se connecter au centre de données Unica en Europe, changez cette valeur en

`em-eu.unicadeliver.com`.

Pour se connecter au centre de données Unica en Inde, changez cette valeur en

`em-in.unicadeliver.com`

- `Deliver > serverComponentsAndLocations > hostedServices> ftpHostName`

  Pour se connecter au centre de données d'Unica aux États-Unis, changez cette valeur en `ftp-em.unicadeliver.com`.

  Pour se connecter au centre de données Unica en Europe, changez cette valeur en

  `ftp-eu.unicadeliver.com`.

  Pour se connecter au centre de données Unica en Inde, changez cette valeur en

  `ftp-in.unicadeliver.com`

What to do next

Si vous modifiez une propriété de configuration, redémarrez le serveur d'applications web pour appliquer les modifications.

Adresse IP des noms d'hôtes délivrés

Si vous avez besoin d'une liste blanche d'adresses IP pour les noms d'hôtes de Deliver sur votre pare-feu d'entreprise, utilisez les adresses IP suivantes.

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

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

`em-in.unicadeliver.com : 75.2.92.153` et `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` et `76.223.38.158`

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

`tms-in.unicadeliver.com : 197.234.141` et `3.33.199.128`

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 35.

Pour WebSphere®, voir Configuration de SSL lors de l'utilisation de WebSphere à la page 38.

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.

À propos de cette tâche

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.

Exemple

```
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.

   Exemple

   ```
   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.

   Exemple

   ```
   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.

Que faire ensuite

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.

À propos de cette tâche

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.

About this task

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 que tu commences

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 36.

À propos de cette tâche

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 33.

   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.

   Exemple

   `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 que tu commences

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 Configuration des adresses pour la connexion aux services hébergés sur HCL Unica à la page 31.

À propos de cette tâche

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 33.

   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.

Chapitre 4. Fonctionnement du service RCT (Response and Contact Tracker)

Le service RCT (Response and Contact Tracker) est installé dans votre environnement local et communique avec les services hébergés HCL Unica pour extraire et traiter les données des contacts de messagerie, de distribution par courrier électronique et de réponse des destinataires, telles que les clics de lien et les ouvertures. RCT doit être en cours d'exécution pour que vous puissiez récupérer les données de suivi de lien et de notification de distribution par courrier électronique depuis les services hébergés HCL Unica.

Vous pouvez démarrer RCT de l'une des manières suivantes.

- Démarrer RCT manuellement
- Démarrer RCT en tant que service

Important : Vous devez démarrer RCT manuellement la première fois que vous utilisez Deliver, même si vous avez enregistré RCT en tant que service.

Vous devez redémarrer RCT lorsque vous apportez des modifications aux propriétés de configuration de Deliver. Vous pouvez redémarrer RCT à tout moment, même si vous l'avez configuré pour s'exécuter en tant que service. Les services hébergés HCL Unica continuent de stocker les données de suivi si RCT est arrêté ou redémarré. Lorsqu'il se remet à fonctionner, RCT télécharge les informations en file d'attente.

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
  ```

Que faire ensuite

Pour plus d'informations sur ce script, voir Script RCT (Response and Contact Tracker) d'Deliver à la page 113.

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.

À propos de cette tâche

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**.

Que faire ensuite

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`.

Que faire ensuite

Pour plus d'informations sur ce script, voir Script MKService_rct à la page 114.

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.
`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.

Propriété de configuration	Paramètre
	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. Le paramètre par défaut est `ftp-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 `ftp-eu.unicadeliver.com`.
`Deliver | partitions | partition[n] | hostedAccountInfo | amUserForAcctCredentials`	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 | amDataSourceForAcctCredentials`	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.

Propriété de configuration	Paramètre
`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.
`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. 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
```

Test de la connexion à l'interface de messagerie hébergée

Unica héberge l'interface de messagerie à partir de ses centres de données aux Etats-Unis et en Europe. Testez la connexion à l'interface de mailing hébergée en tentant d'accéder à une fonction Deliver.

Connectez-vous à HCL Unica et sélectionnez **Mailings Deliver** dans le menu **Campaign**.
Résultat

Si la connexion à l'interface utilisateur Deliver est établie correctement, la page Mailings Deliver s'ouvre et affiche la liste des mailings et des caractéristiques de mailing associées.

Si la connexion à l'interface utilisateur n'est pas correctement établie, une erreur s'affiche.

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 52.	`Campaign | partitions | partition[n] | server | internal`
Caractéristiques des listes de destinataires de courrier électronique. Voir Campaign | partitions | partition[n] | Deliver à la page 50.	`Campaign | partitions | partition[n] | Deliver`
URL requises pour la connexion aux services hébergés HCL Unica. Voir Deliver | serverComponentsAndLocations | hostedServices à la page 56.	`Deliver | serverComponentsAndLocations | hostedServices`
Identifiants d'accès de base de données et de compte pour la connexion aux services hébergés HCL Unica. Voir Deliver | partitions | partition[n] | hostedAccountInfo à la page 57	`Deliver | partitions | partition[n] | hostedAccountInfo`
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 58	`Deliver | partitions | partition[n] | dataSources | systemTables`

Caractéristique ou fonction	Propriété de configuration (y compris le chemin d'accès)
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 62	`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 62	`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. Voir Configuration de la prise en charge des tables de dimension à la page 48.	`Campaign | partitions | partition[n]| Deliver | oltDimTableSupport`
Prise en charge du suivi d'historique d'exécution de mailing. Voir Deliver | partitions | partition[n] | responseContactTracker à la page 62	`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.

Configuration de l'accès à un historique d'exécution de mailing supplémentaire

Vous pouvez demander à Unica de fournir des données supplémentaires pour l'historique d'exécution de mailing. L'accès aux données d'historique d'exécution de mailing est disponible sur demande auprès de Unica et en mettant à jour la configuration Deliver. Les données d'historique d'exécution de mailing sont enregistrées dans les tables système locales Deliver de la table `UACE_ExecHistory` pour décrire les exécutions de mailing terminées.

Avant que tu commences

Pour télécharger des données d'exécution de mailing supplémentaires, vous devez mettre à jour la propriété de configuration `enableExecutionHistoryDataTracking`. Par défaut, `enableExecutionHistoryDataTracking` n'est pas exposé dans les propriétés de configuration Deliver.

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`. Les types d'enregistrements suivants sont disponibles dans l'historique d'exécution de mailing supplémentaire.

À propos de cette tâche

- Ligne d'objet du message
- Adresse de l'expéditeur
- Utilisateur qui a mis à jour le mailing
- Description du document
- Date d'enregistrement du mailing

1. Demandez l'accès à d'autres données d'historique d'exécution de mailing. Pour demander l'accès, contactez votre équipe Unica Deliver Services via le support technique d'HCL.
2. Mettez à jour la configuration de Deliver. Configurez les propriétés de configuration suivantes.

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

   Définissez **enableExecutionHistoryDataTracking** sur **True**.
3. Vérifiez que le mappage de table pour UACE_ExecHistory est correct.

Que faire ensuite

Vous pouvez interroger les tables système Deliver afin d'extraire des informations d'exécution de mailing à partir de la table `UACE_ExecHistory`.

Pour plus d'informations sur les tables système Deliver, voir *Unica Deliver - Tables système et dictionnaire de données*.

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**.

À propos de cette tâche

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.

À propos de cette tâche

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`.

Propriétés de configuration d'Deliver

Vous accédez aux propriétés de configuration Deliver à partir du menu Paramètres dans Platform. Les propriétés de configuration de Deliver sont contenues dans les catégories de configuration Campaign et Deliver.

Pour accéder aux propriétés de configuration, sélectionnez **Paramètres > Configuration**. La page Configurations répertorie toutes les propriétés de configuration disponibles pour votre installation HCL Unica.

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

Définissez les propriétés permettant de spécifier les adresses URL utilisées pour se connecter aux services hébergés HCL Unica. Deliver utilise des connexions séparées pour transférer les listes de destinataires, les métadonnées qui décrivent ces listes ainsi que pour la communication générale avec l'environnement hébergé.

Vous devez changer les valeurs par défaut si vous vous connectez aux services hébergés HCL Unica via le centre de données implanté par Unica en Europe. Consultez Unica pour savoir à quel centre de données vous êtes connecté.

uiHostName

Description

Adresse utilisée par Deliver pour toutes les communications vers les services hébergés HCL Unica, à l'exception des listes de destinataires téléchargées et des métadonnées associées.

Valeur par défaut

`em.unicadeliver.com`

Si vous vous connectez au centre de données européen, remplacez cette valeur par `em-eu.unicadeliver.com`.

dataHostName

Description

Adresse utilisée par Deliver pour télécharger les métadonnées associées aux listes de destinataires sur les services hébergés HCL Unica.

Valeur par défaut

`em.unicadeliver.com`

Si vous vous connectez au centre de données européen, remplacez cette valeur par `em-eu.unicadeliver.com`.

ftpHostName

Description

Adresse utilisée par Deliver pour transférer les données associées aux listes de destinataires (sauf les métadonnées de la liste) sur les services hébergés HCL Unica.

Valeur par défaut

`ftp-em.unicadeliver.com`

Si vous vous connectez au centre de données européen, remplacez cette valeur par `ftp-eu.unicadeliver.com`.

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

Les propriétés de configuration de cette catégorie définissent le schéma, les paramètres de connexion et les données d'identification de connexion à la base de données qui héberge les tables système d'Deliver dans votre environnement réseau.

type

Description

Type de base de données hébergeant les tables système Deliver.

Valeur par défaut

Aucune valeur par défaut définie. Vous devez définir cette propriété.

Valeurs valides

- `SQLSERVER`
- `ORACLE`
- `DB2`

schemaName

Description

Nom du schéma de base de données pour les tables système Deliver. Ce nom de schéma est le même que celui des tables système de Campaign.

Vous devez spécifier ce nom de schéma lorsque vous référencez des tables système dans les scripts.

Valeur par défaut

dbo

jdbcBatchSize

Description

Nombre de requêtes d'exécution JDBC exécutées simultanément dans la base de données.

Valeur par défaut

10

Valeurs valides

Un nombre entier supérieur à 0.

jdbcClassName

Description

Pilote JDBC associé aux tables système, comme défini sur le serveur Web de Campaign.

Valeur par défaut

Aucune valeur par défaut définie. Vous devez définir cette propriété.

jdbcURI

Description

URI de connexion JDBC associée aux tables système, comme définie sur le serveur Web de Campaign.

Valeur par défaut

Aucune valeur par défaut définie. Vous devez définir cette propriété.

asmUserForDBCredentials

Description

Employez cette propriété pour spécifier un utilisateur HCL Unica qui sera autorisé à accéder aux tables système d'Deliver.

Valeur par défaut

Aucune valeur par défaut définie. Vous devez définir cette propriété.

Valeurs valides

N'importe quel utilisateur défini dans Platform. En règle générale, il s'agit du nom de l'utilisateur système de Campaign.

amDataSourceForDBCredentials

Description

Utilisez cette propriété pour spécifier la source de données qui définit les données d'identification de connexion à la base de données qui contient les tables système d'Deliver. Cette source de données peut être la même que celle des tables système de Campaign.

Valeur par défaut

UA_SYSTEM_TABLES

Valeurs valides

Une source de données Platform associée à l'utilisateur HCL Unica que vous spécifiez dans `asmUserForDBCredentials`

La source de données spécifie l'utilisateur et les données d'identification utilisées pour accéder aux tables système d'Deliver. Si le schéma par défaut associé à l'utilisateur de la base de données ne correspond pas au schéma qui héberge les tables système, vous devez spécifier le schéma des tables système au niveau de la connexion JDBC utilisée pour accéder aux tables système.

poolAcquireIncrement

Description

Lorsque le pool de connexions de base de données n'a plus de connexions, nombre de nouvelles connexions créées par Deliver pour les tables système. Deliver crée des connexions dans la limite du nombre indiqué dans `poolMaxSize`.

Valeur par défaut

1

Valeurs valides

Un nombre entier supérieur à 0.

poolIdleTestPeriod

Description

La durée, en secondes, pendant laquelle Deliver attend avant de vérifier si chaque connexion aux tables système d'Deliver est active.

Valeur par défaut

100

Valeurs valides

Un nombre entier supérieur à 0.

poolMaxSize

Description

Nombre maximum de connexions aux tables système établies par Deliver. La valeur 0 (zéro) indique qu'il n'y a pas de limite maximum.

Valeur par défaut

100

Valeurs valides

Un nombre entier supérieur ou égal à 0.

poolMinSize

Description

Nombre minimum de connexions aux tables système établies par Deliver.

Valeur par défaut

10

Valeurs valides

Un nombre entier supérieur ou égal à 0.

poolMaxStatements

Description

Nombre maximum d'instructions enregistrées par Deliver dans la mémoire cache PrepareStatement pour chaque connexion aux tables système. Si vous définissez poolMaxStatements sur 0 (zéro), la mise en mémoire des instructions est désactivée.

Valeur par défaut

0

Valeurs valides

Un nombre entier supérieur ou égal à 0.

timeout

Description

Durée, en secondes, pendant laquelle Deliver conserve une connexion au repos avant de l'annuler.

Si `poolIdleTestPeriod` est supérieur à 0, Deliver teste toutes les connexions au repos et en pool, mais pas les connexions non contrôlées, selon l'intervalle de temps (en secondes) spécifié pour `timeout`.

Si `poolIdleTestPeriod` est supérieur à `timeout`, les connexions au repos sont annulées.

Valeur par défaut

100

Valeurs valides

Un nombre entier supérieur ou égal à 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 :

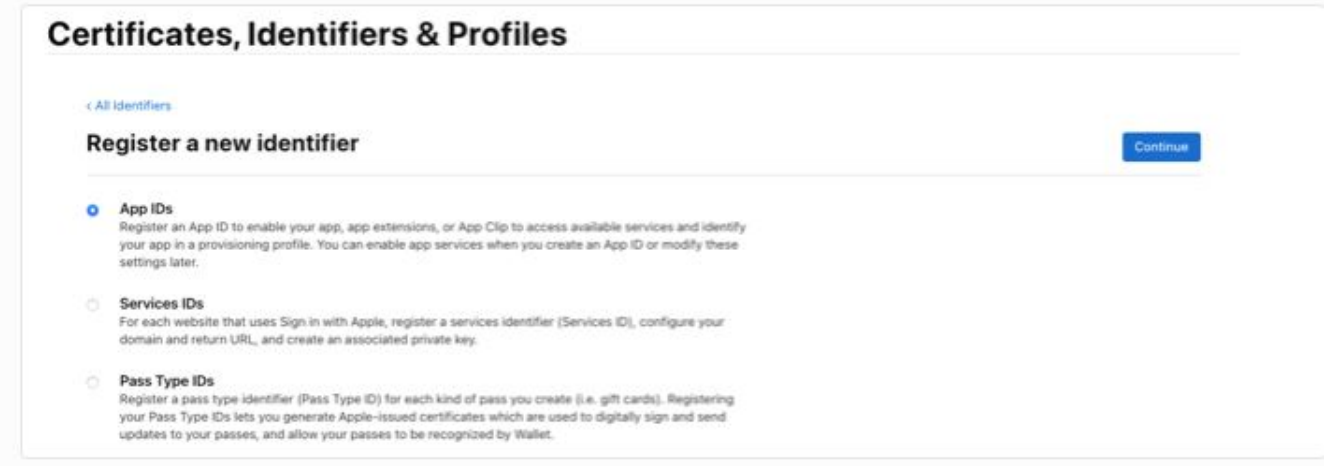
1. Configurez votre application dans votre compte Apple Developer
2. Configurez votre application dans votre compte Firebase Cloud Messaging
3. Configurez votre application Unica pour APNS et FCM en fournissant les données d'identification qui conviennent
4. Sélectionnez le SDK qui convient pour la plateforme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

Configurer votre compte Apple Developer

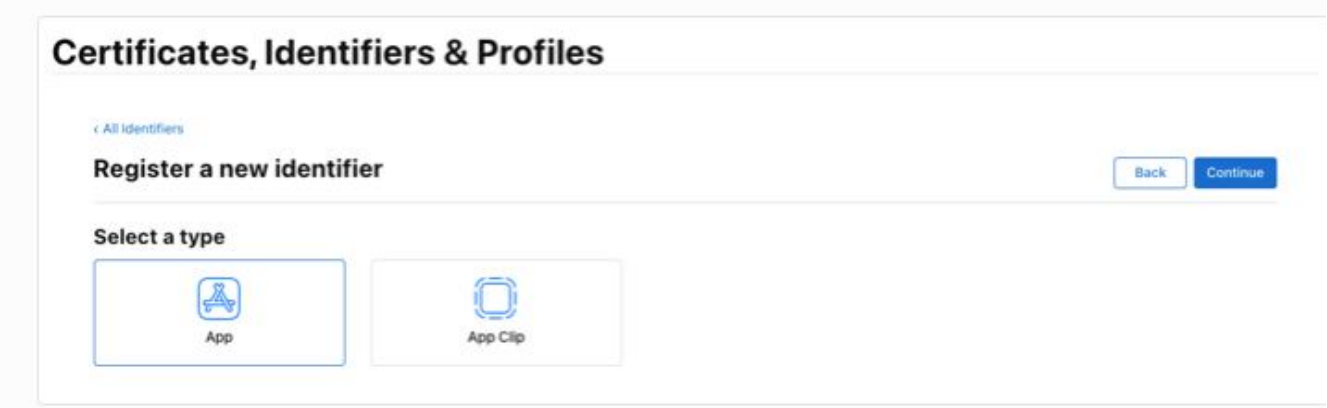
Enregistrer votre identifiant de lot et ses capacités

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.

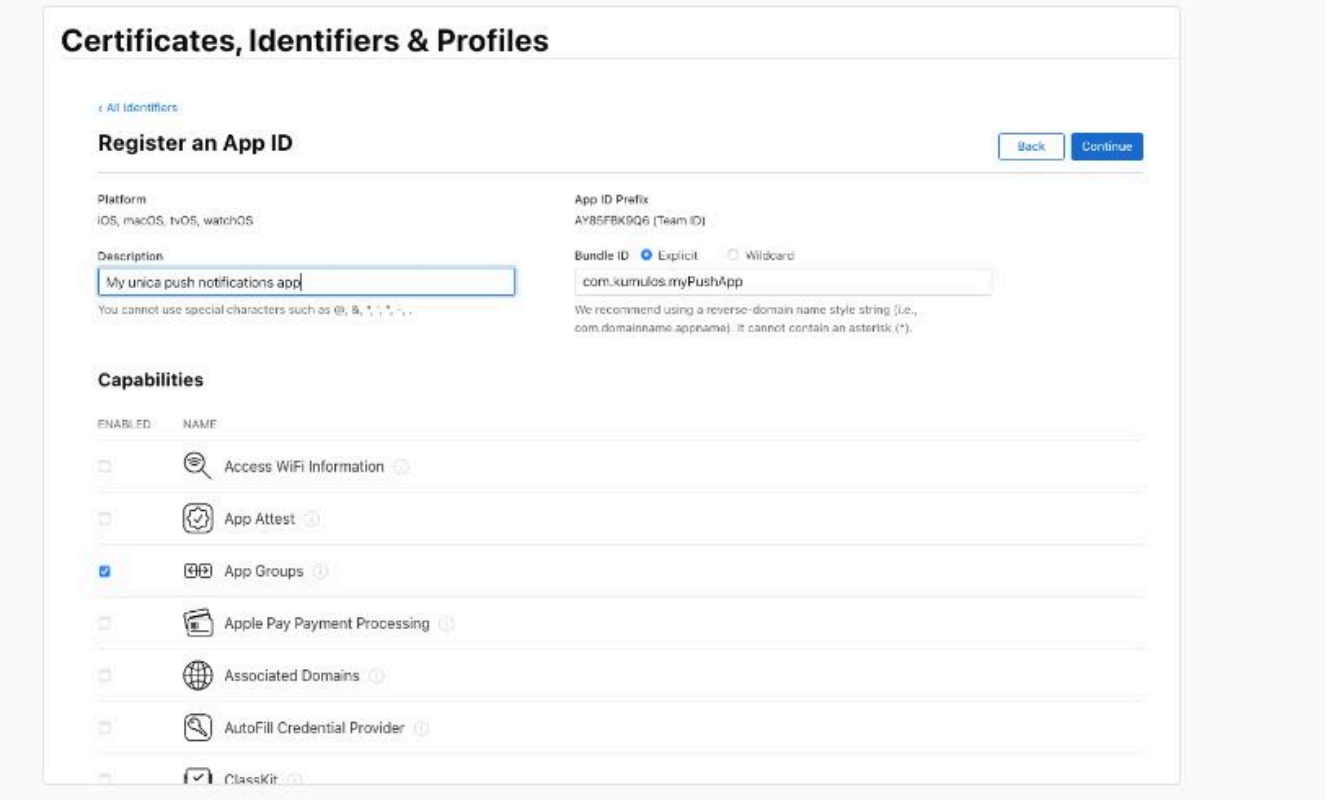


Lorsque vous êtes invité à enregistrer un nouvel identifiant, sélectionnez l'option Identifiant de l'app et cliquez sur Continuer puis, à la deuxième étape, sélectionnez le type App et cliquez à nouveau sur Continuer.



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.

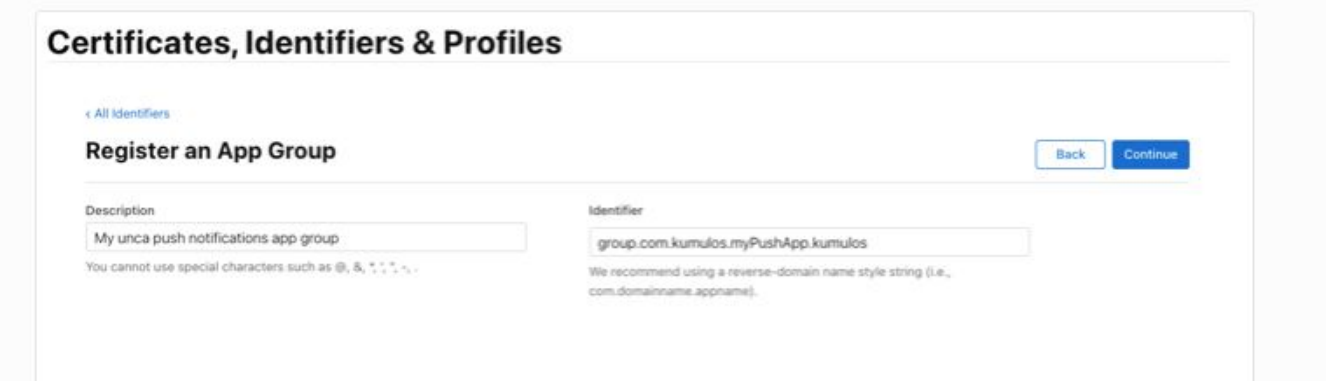
Dans la section Capacités, vérifiez que les cases « Groupes d'apps » et « Notifications push » sont cochées, puis appuyez sur Continuer.



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.

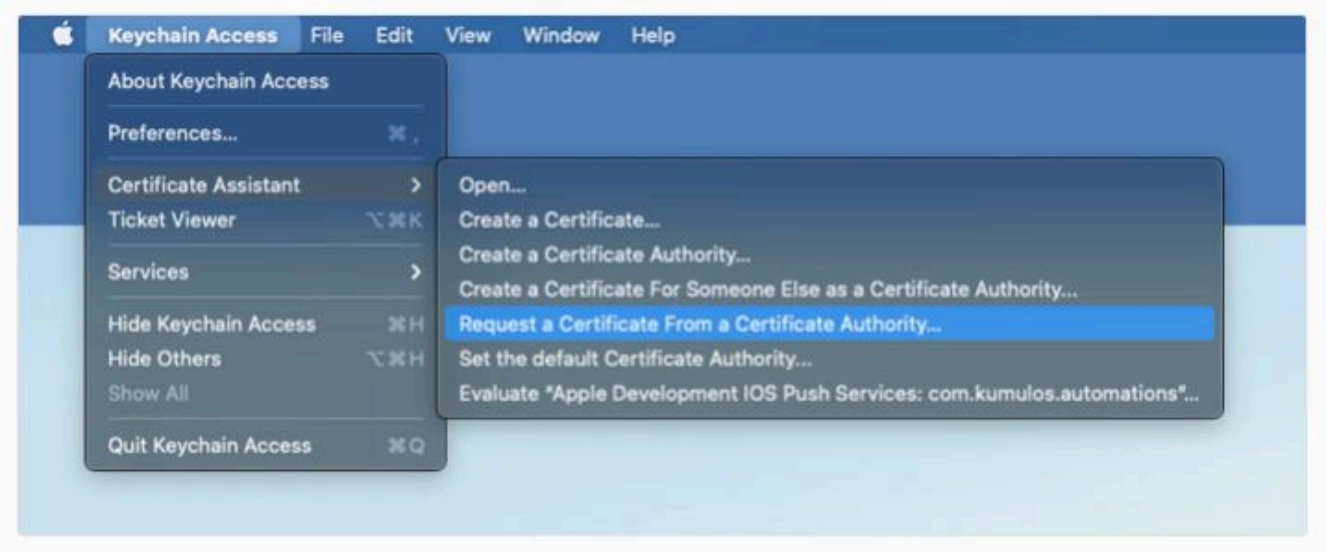
Dans l'écran « Editer la configuration de votre identifiant d'app », cliquez sur le bouton « Configurer » à côté de la capacité « Groupes d'apps ». Dans la fenêtre contextuelle, cochez la case à côté du groupe créé à l'étape précédente avec l'identifiant de lot correspondant, puis cliquez sur « Continuer ». 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

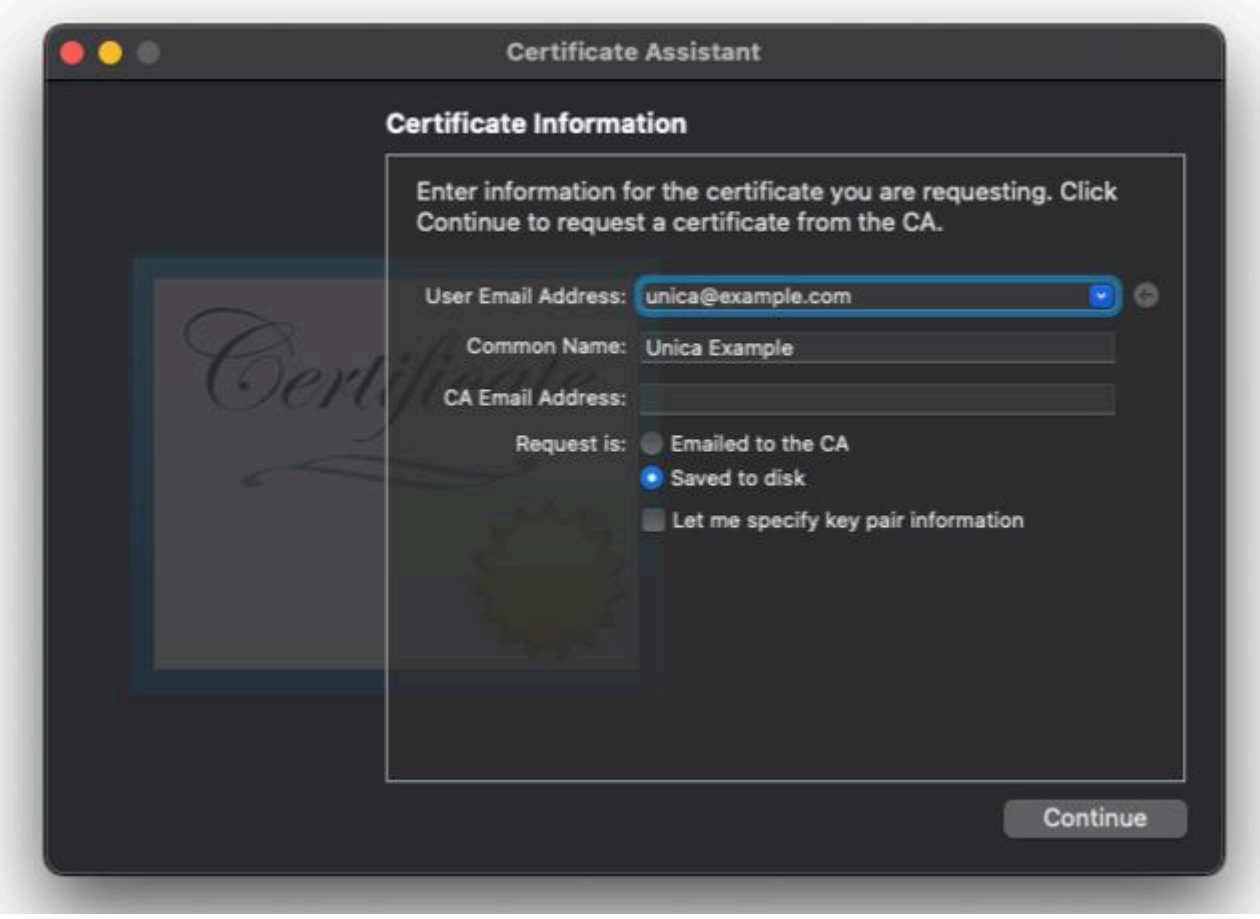
Pour envoyer des notifications Push aux périphériques iOS avec Unica, vous devrez créer des certificats dans Apple Developer Member Center afin d'enregistrer les données d'identification auprès de votre application Unica.

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

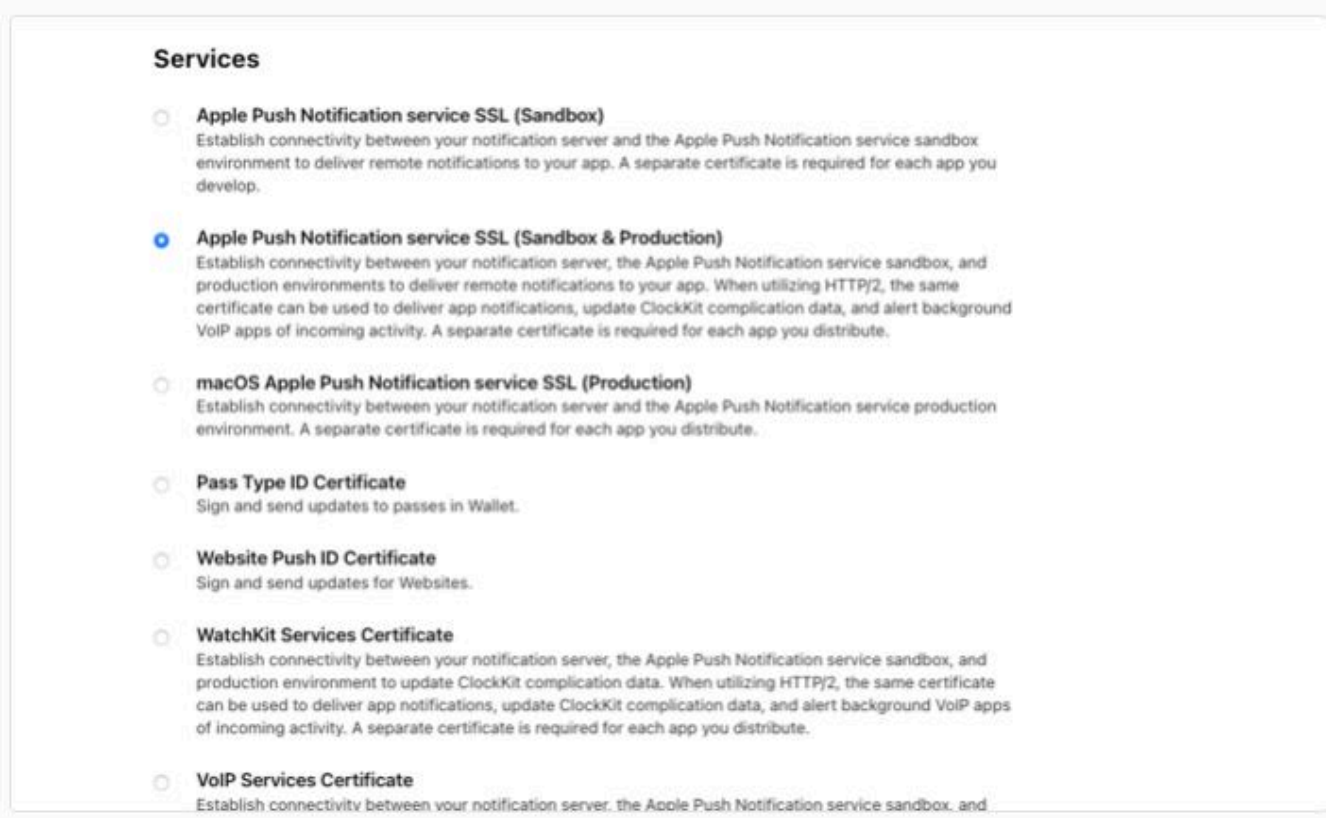
Tout d'abord, nous allons créer une demande de signature de certificat, à l'aide de Keychain Access. Accédez au menu Keychain Access depuis votre barre d'outils et sélectionnez Assistant de certificat, Demander un certificat à une autorité de certification.



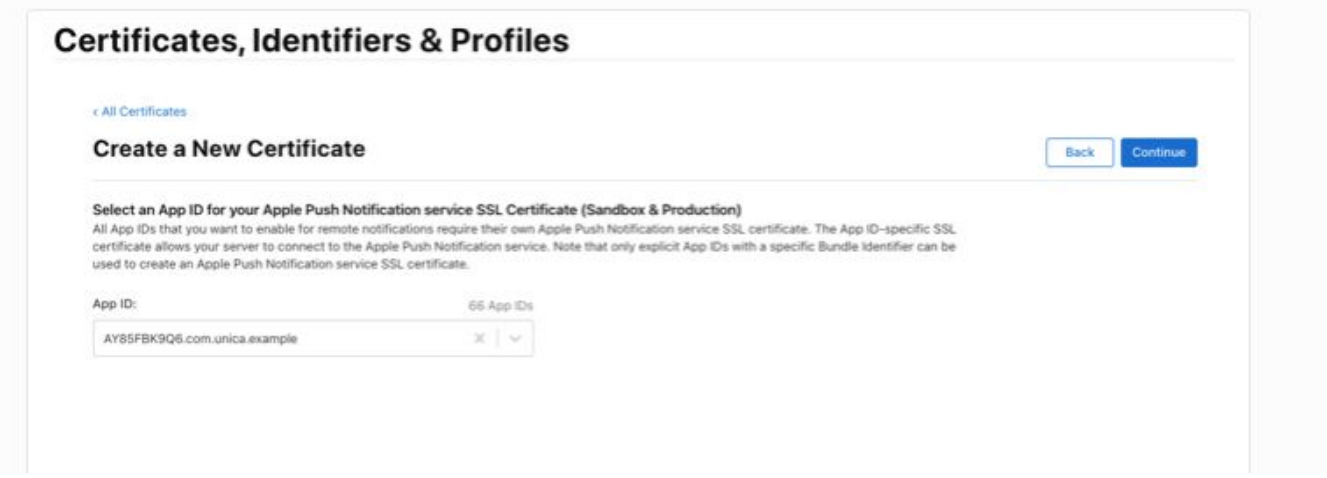
Dans la fenêtre de la boîte de dialogue, entrez votre courrier électronique dans le champ « Adresse e-mail de l'utilisateur ». Votre nom doit déjà apparaître dans le champ « Nom usuel ». Sélectionnez la case d'option 'Enregistré sur le disque' et cliquez sur 'Continuer'. Enregistrez le fichier sur votre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

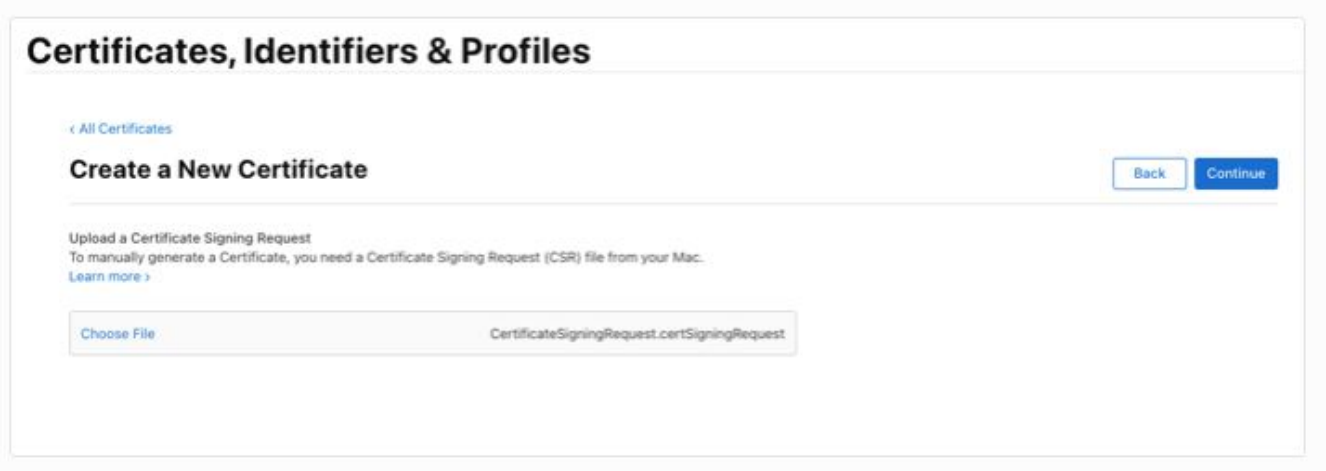


Sur l'écran suivant, sélectionnez l'identifiant d'application lors du processus de mise en route, puis cliquez sur Continuer.



Lorsque vous êtes invité à charger une demande de signature de certificat, cliquez sur Sélectionner un fichier et rechercher, puis sélectionnez le fichier

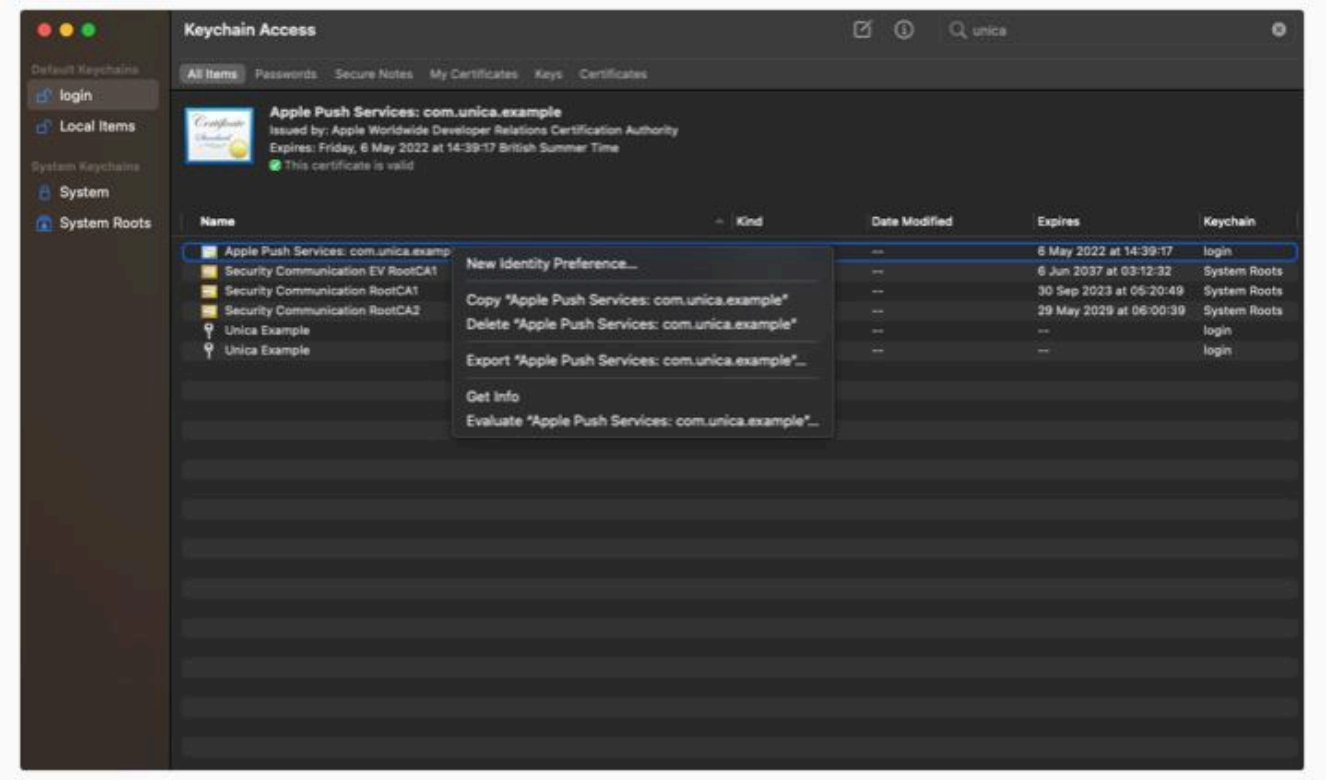
`certSigningRequest` créé précédemment et cliquez sur Continuer.



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.

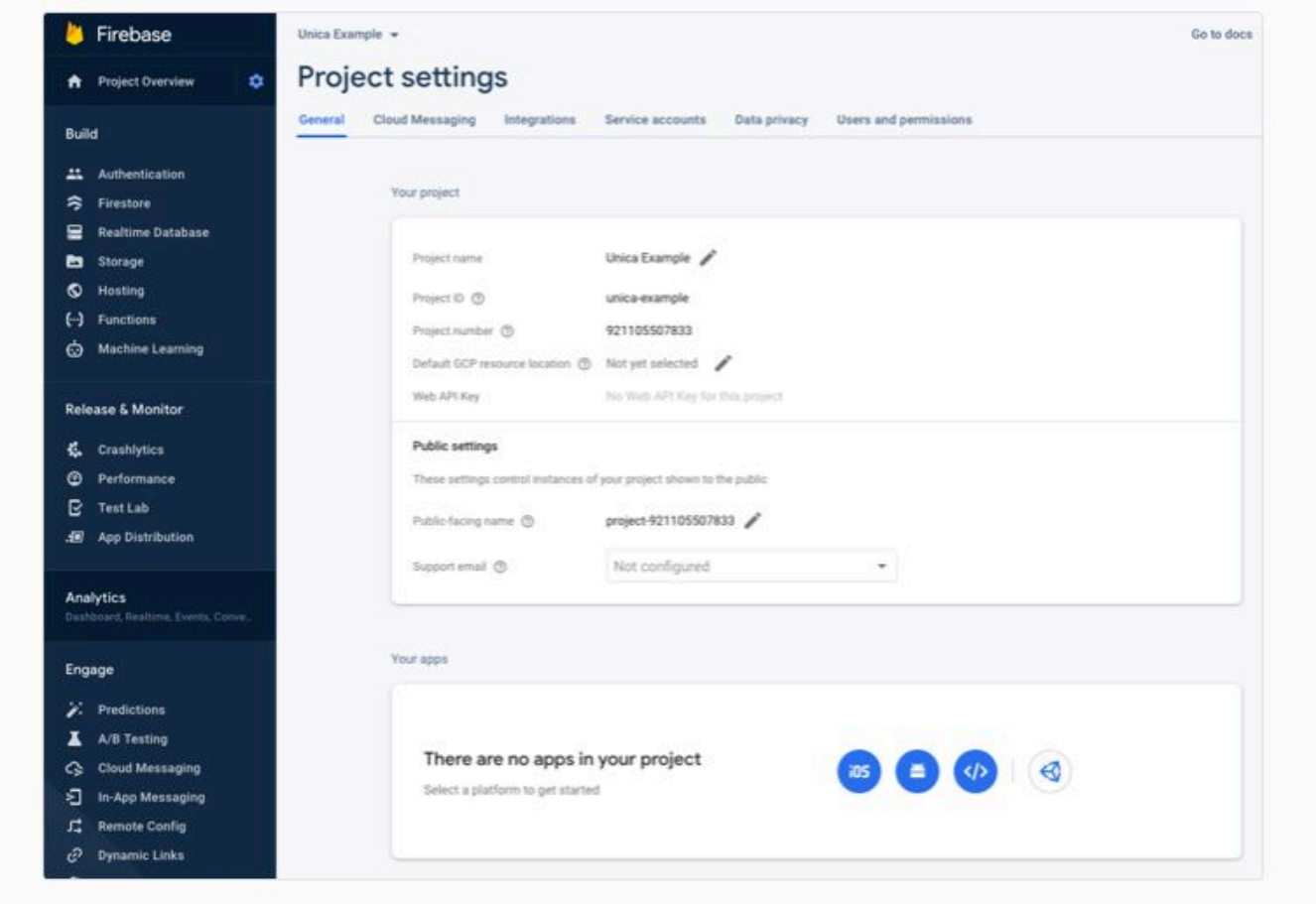
Dans cette étape, nous allons générer plusieurs artefacts utilisés pour configurer à la fois l'application Unica et votre projet d'application Android, à savoir :

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

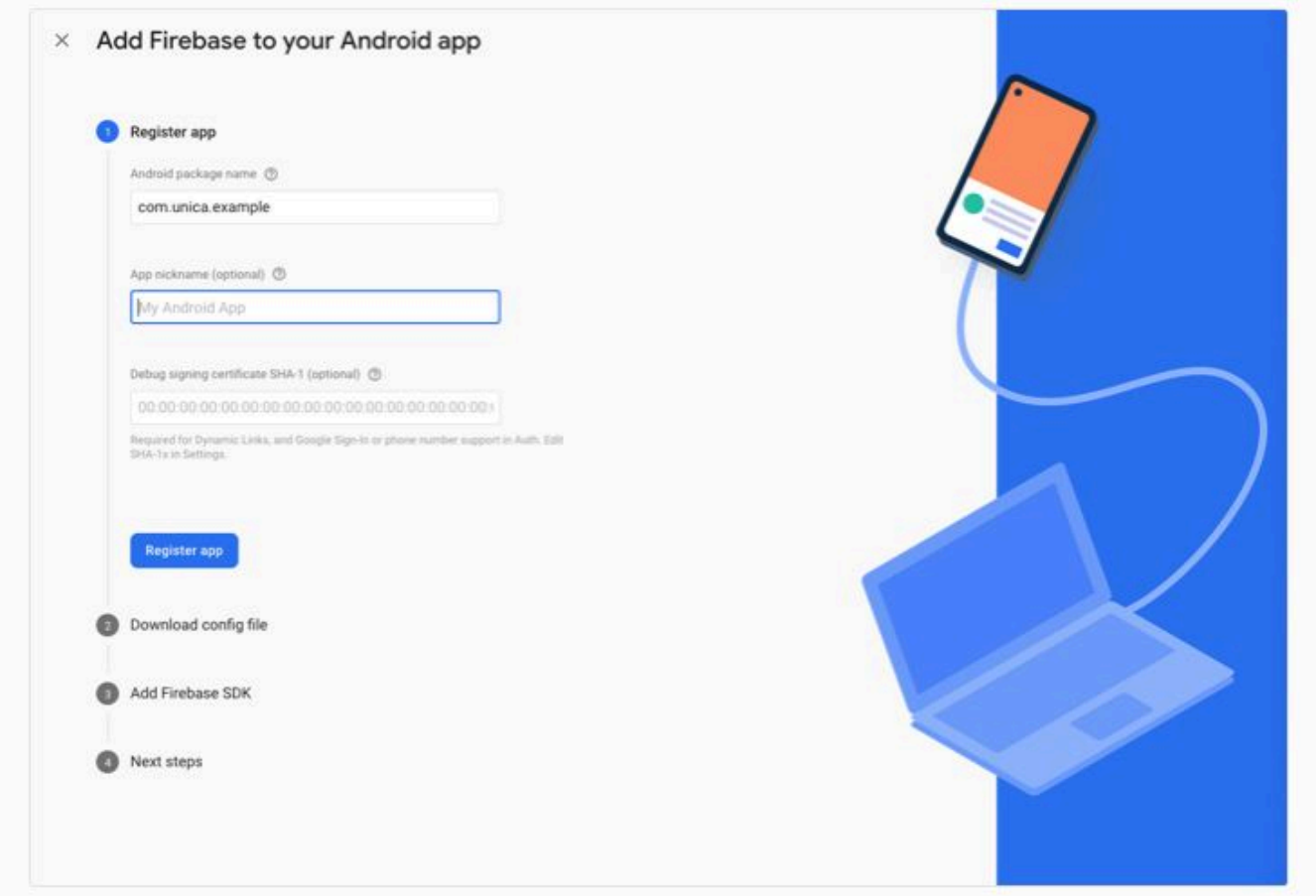
Connectez-vous d'abord à votre console Firebase, sélectionnez « Ajouter un projet » et entrez le nom de votre projet dans l'assistant. Vous pouvez choisir ou non Google Analytics pour votre projet, cela n'affectera pas l'intégration.

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'

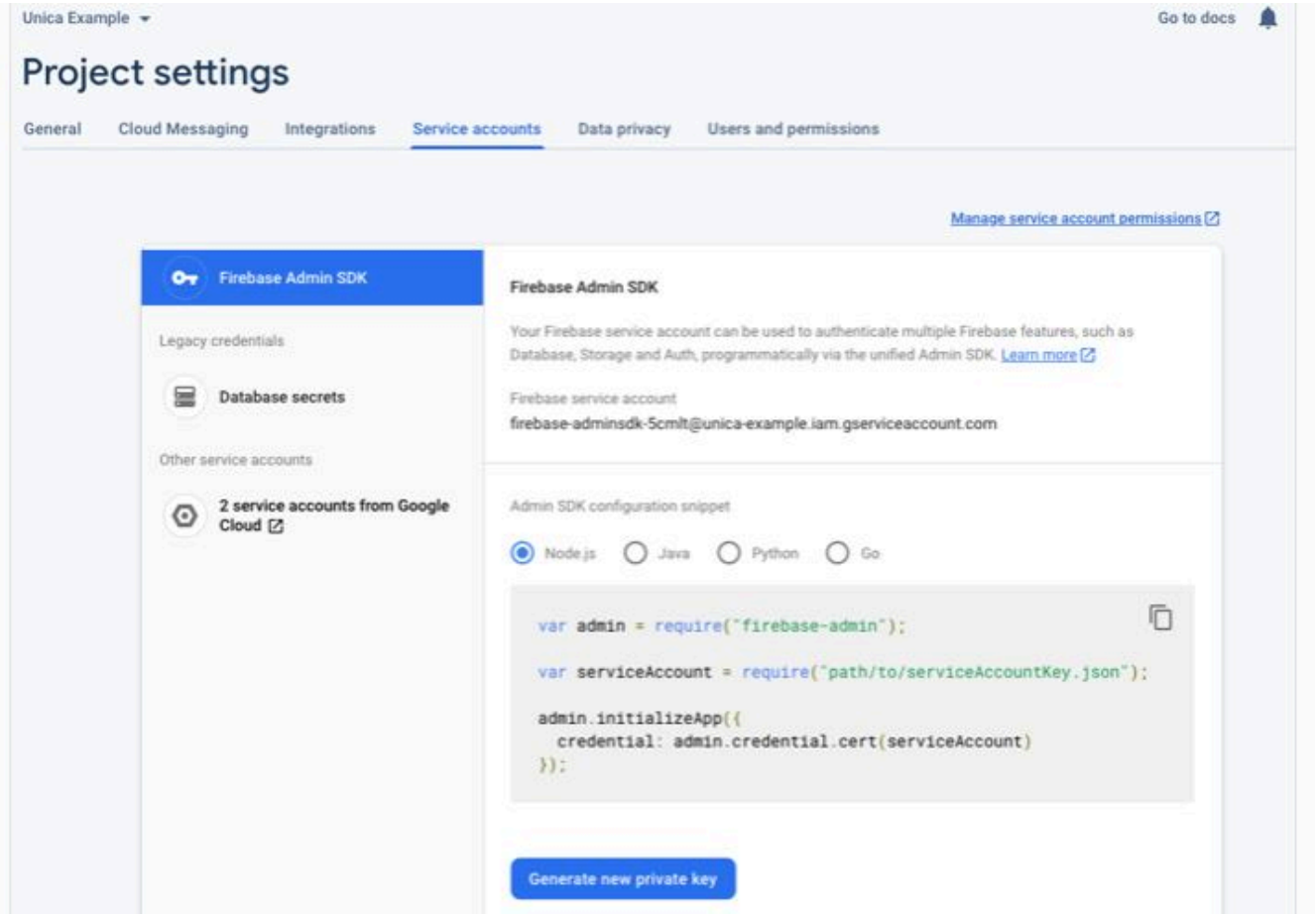


Dans l'onglet 'Général' du panneau 'Vos applications', cliquez sur l'icône pour Android. L'assistant permettant de créer l'application s'ouvre alors.



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.



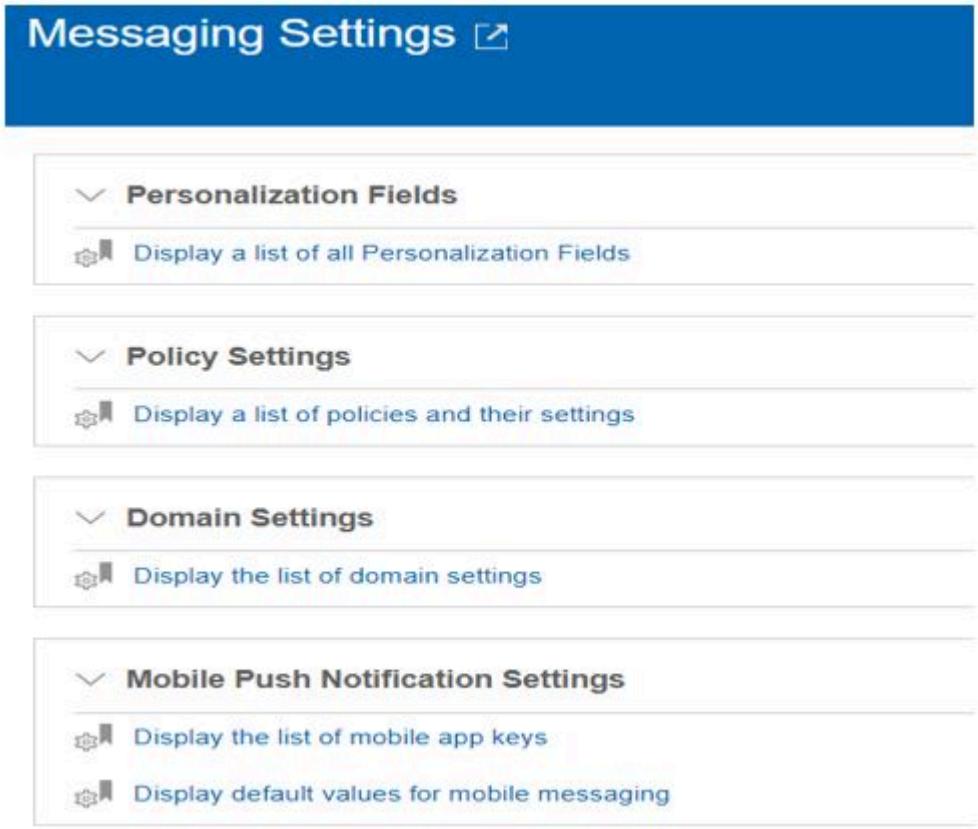
Ensuite, cliquez sur l'onglet « Comptes de service », puis sur « Générer une nouvelle clé privée ». Un fichier JSON décrivant vos données d'identification de compte sera alors téléchargé. Vous en aurez aussi besoin pour configurer votre application Unica.

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

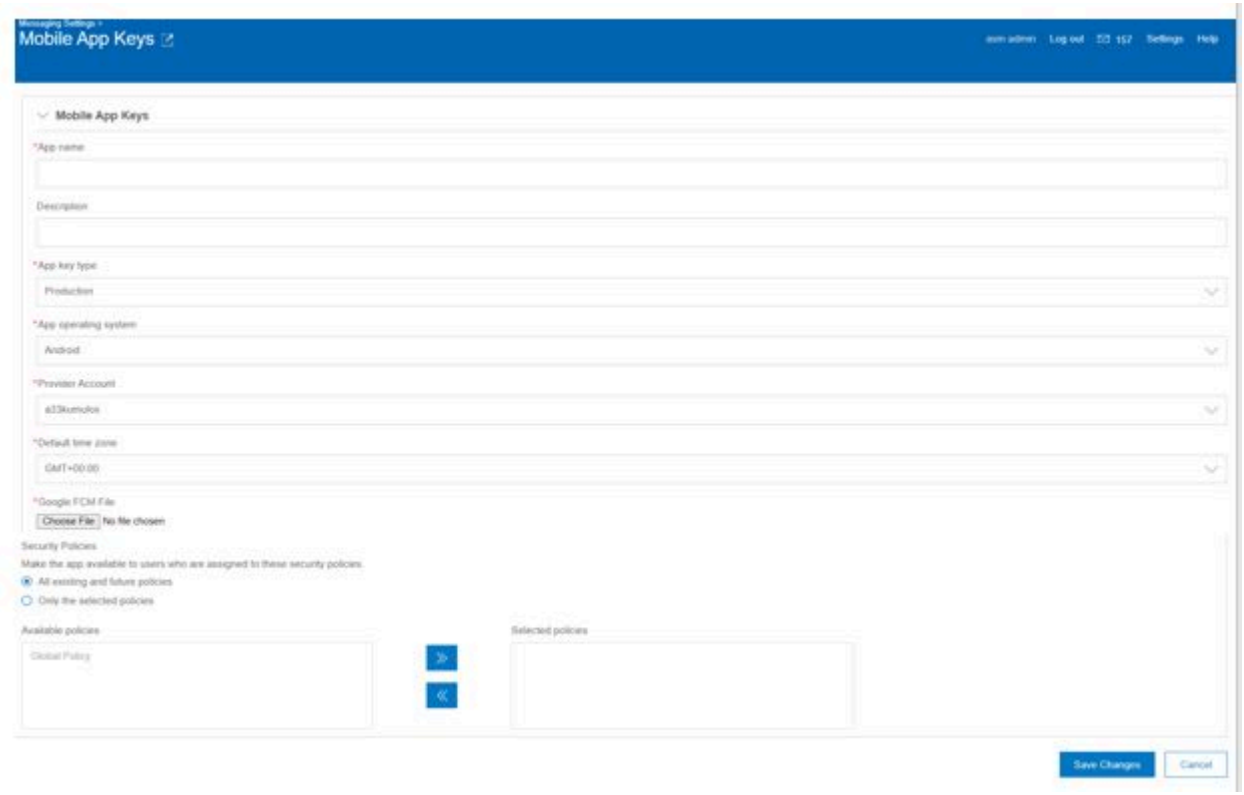
Procédez comme suit.

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 77
- Android on page 83

Multiplateforme

- React Native on page 103

iOS Swift

Introduction

Le SDK Kumulos est un projet open source hébergé sur Github et qui se trouve à l'adresse https://github.com/Kumulos/KumulosSdkSwift.

Ce guide suppose que vous avez effectué les étapes de Configurations pour l'implémentation de notifications Push mobiles on page 65 et que vous avez configuré votre identifiant, vos capacités et votre profil de mise à disposition Apple à partir de ce guide. il couvre les étapes d'intégration suivantes :

1. Intégrer le SDK et configurer votre projet pour la fonction APNS
2. Initialisation des composants SDK dans votre projet et enregistrement pour les notifications Push
3. Enregistrer l'installationID de Kumulos avec votre système dorsal pour fournir un lien entre le périphérique et les utilisateurs représentés dans le système dorsal de votre CRM pour le ciblage ultérieur des notifications.
4. Envoyez une notification Push de test à partir de votre application Unica et recevez-la sur le périphérique.
5. Crochets facultatifs pour un comportement avancé

Intégration

Les instructions d'intégration Carthage et CocoaPods sont disponibles dans le référentiel GitHub.

Mise en route de Cocoapods

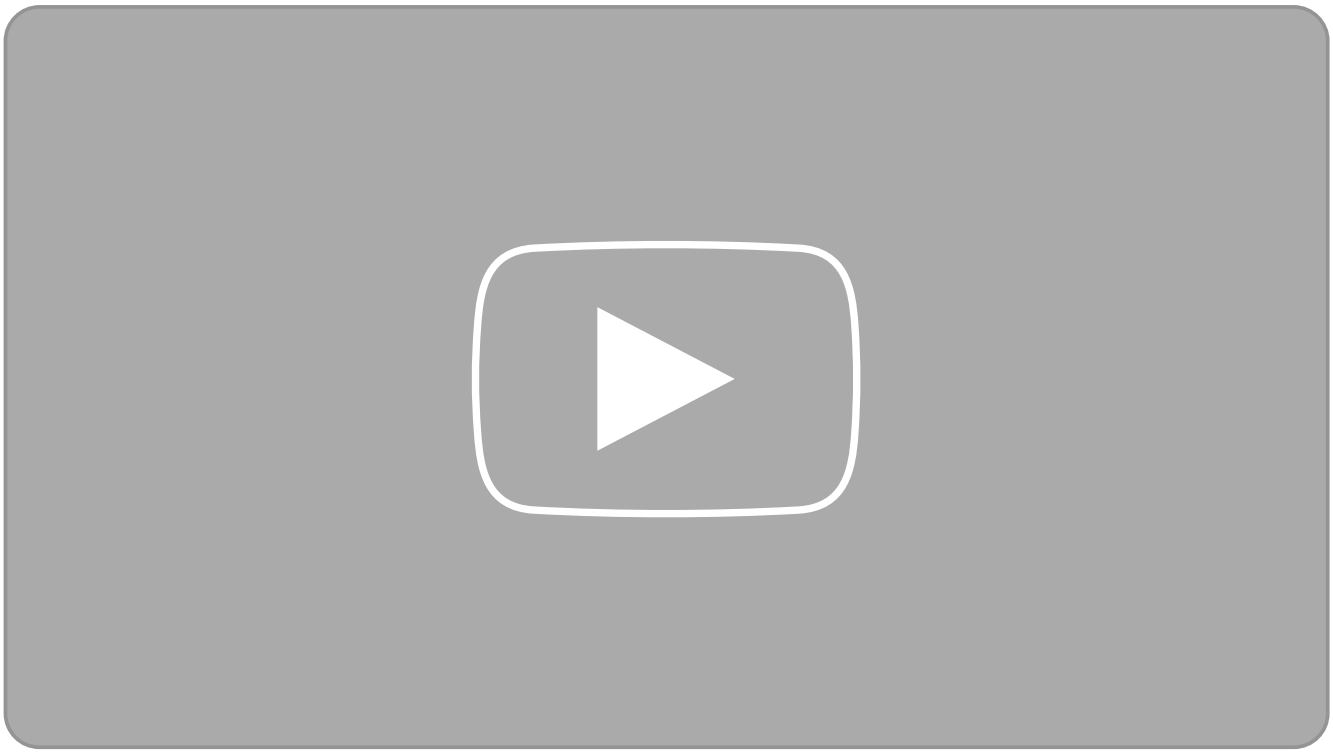
Mise en route de Carthage

Il vous suffit de suivre les instructions de votre gestionnaire de dépendances préféré pour ajouter l'infrastructure KumulosSDK au projet.

Ajouter une extension de service de notification

Pour prendre en charge toutes les fonctions d'Apple Push Notification Service, votre application doit posséder une extension de service de notification afin d'autoriser un traitement limité de la notification à sa réception, avant que le système d'exploitation ne la présente à l'utilisateur.

Il s'agit d'un second projet qui doit être ajouté à votre espace de travail, comme le montre la vidéo ci-dessous.



Si vous utilisez CocoaPods, ajoutez ce qui suit à votre fichier Podfile et exécutez `pod install`.

```
target 'KumulosNotificationServiceExtension' do
  pod 'KumulosSdkSwiftExtension', '~> 8.4.0'
end
```

Remplacez ensuite le contenu de `NotificationService.swift` par les lignes suivantes :

```
import UserNotifications
import KumulosSDKExtension

class NotificationService: UNNotificationServiceExtension {
    override func didReceive(_ request: UNNotificationRequest, withCo
        KumulosNotificationService.didReceive(request, withContentHan
    }
}
```

Les fonctions d'aide du SDK Kumulos ajouteront automatiquement des boutons et des pièces jointes d'image au contenu de la notification.

Configurer les capacités et les droits de votre application

Dans les paramètres de votre projet d'application, utilisez le bouton « + capacité » pour ajouter les fonctions Groupes d'applications, Modes d'arrière-plan et Notifications push.

Dans votre extension de notification, utilisez le bouton « + capacité » pour ajouter la fonction Groupes d'applications.

Dans les deux projets, la fonction Groupes d'applications doit être configurée pour partager le même groupe. Ce dernier doit correspondre exactement au groupe défini précédemment dans les capacité de vos identifiants.

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

Dans votre projet d'application, le mode « Notifications à distance » doit être coché pour les modes d'arrière-plan.

Tester votre configuration

A ce stade, vous pouvez tester le déploiement de votre application sur un périphérique pour vous assurer que vos droits et capacités sont configurés correctement.

Initialisation

Pour configurer le SDK pour l'utiliser, vous devez l'initialiser avec les informations d'identification de votre application. Cette procédure doit être effectuée au début du démarrage de votre application.

```
import UIKit
import KumulosSDK

@UIApplicationMain
class AppDelegate: UIResponder, UIApplicationDelegate {

  var window: UIWindow?

  func application(application: UIApplication, didFinishLaunchingWith

    let builder = KSConfigBuilder(apiKey: "your-api-key", secretKey:
    Kumulos.initialize(config: builder.build())

    // Override point for customization after application launch.
    return true
  }
}
```

Le SDK Kumulos prend automatiquement en charge les badges, les boutons et le contenu d'image. Notez toutefois qu'en raison de limitations d'iOS, les badges ne sont pas définis lorsque l'application est en avant-plan.

Enregistrement pour les notifications Push

iOS nécessite l'autorisation explicite de l'utilisateur pour recevoir des notifications. Lorsque vous jugez cela approprié, vous pouvez déclencher l'invite pour autoriser les notifications en appelant :

```
Kumulos.pushRequestDeviceToken()
```

Cet assistant invite le système d'exploitation à demander à l'utilisateur d'accepter les notifications Push avec les options badge, alerte et son.

Lorsque l'utilisateur accepte, le SDK Kumulos gère automatiquement l'enregistrement du jeton Push auprès du système dorsal de Kumulos.

Enregistrement 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 :

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

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.

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(userIdentifier: "unique-user-identif
```

Envoi d'un test

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)
    }
```

Android

Introduction

Le SDK Kumulos est un projet open source hébergé sur Github et qui se trouve à l'adresse https://github.com/Kumulos/KumulosSdkAndroid.

Ce guide suppose que vous avez effectué les étapes depuis l'Configurations pour l'implémentation de notifications Push mobiles on page 65 et que vous avez configuré votre console Firebase et votre application Unica avec les identifiants appropriés pour Cloud Messaging. Il couvre les étapes suivantes :

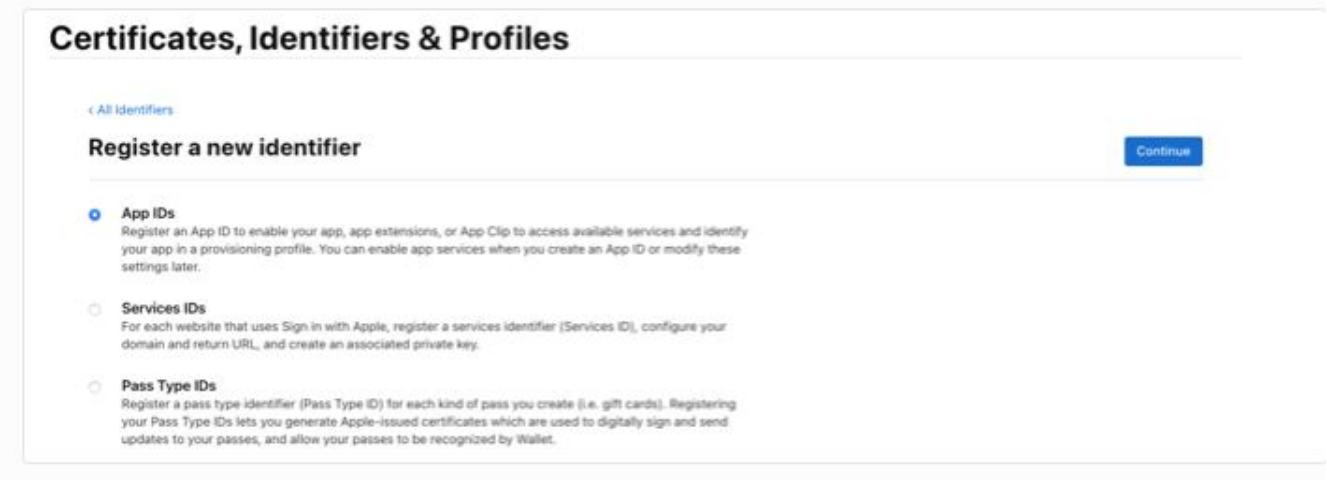
1. Intégrer le SDK et configurer votre projet.
2. Initialiser les composants du SDK au sein de votre projet et vous enregistrer pour les notifications Push.
3. Enregistrer l'installationID de Kumulos avec votre système dorsal pour fournir un lien entre le périphérique et les utilisateurs représentés dans le système dorsal de votre CRM pour le ciblage ultérieur des notifications.
4. Envoyer une notification Push de test à partir de votre application Unica et la recevoir sur le périphérique.
5. Crochets facultatifs pour un comportement avancé.

Configurer votre compte Apple Developer

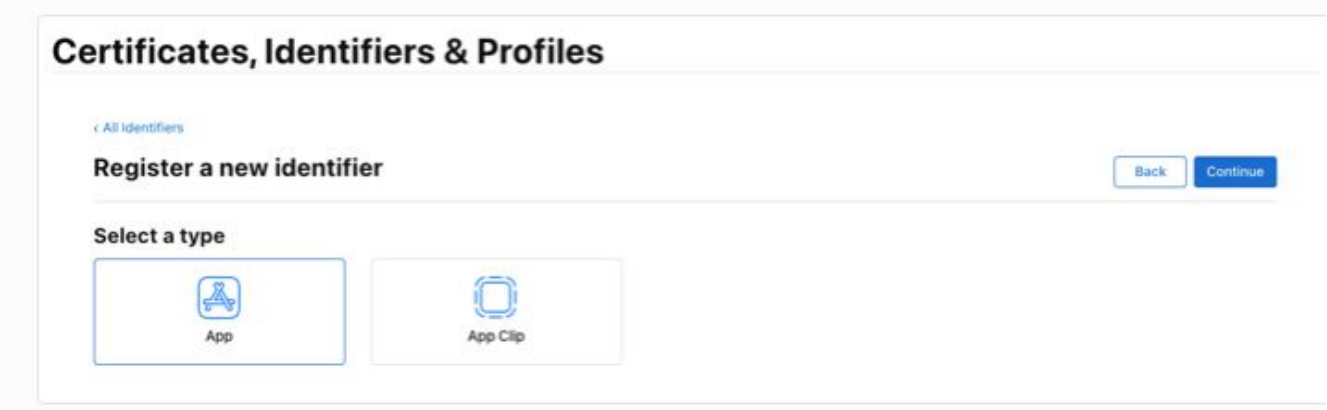
Enregistrer votre identifiant de lot et ses capacités

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.

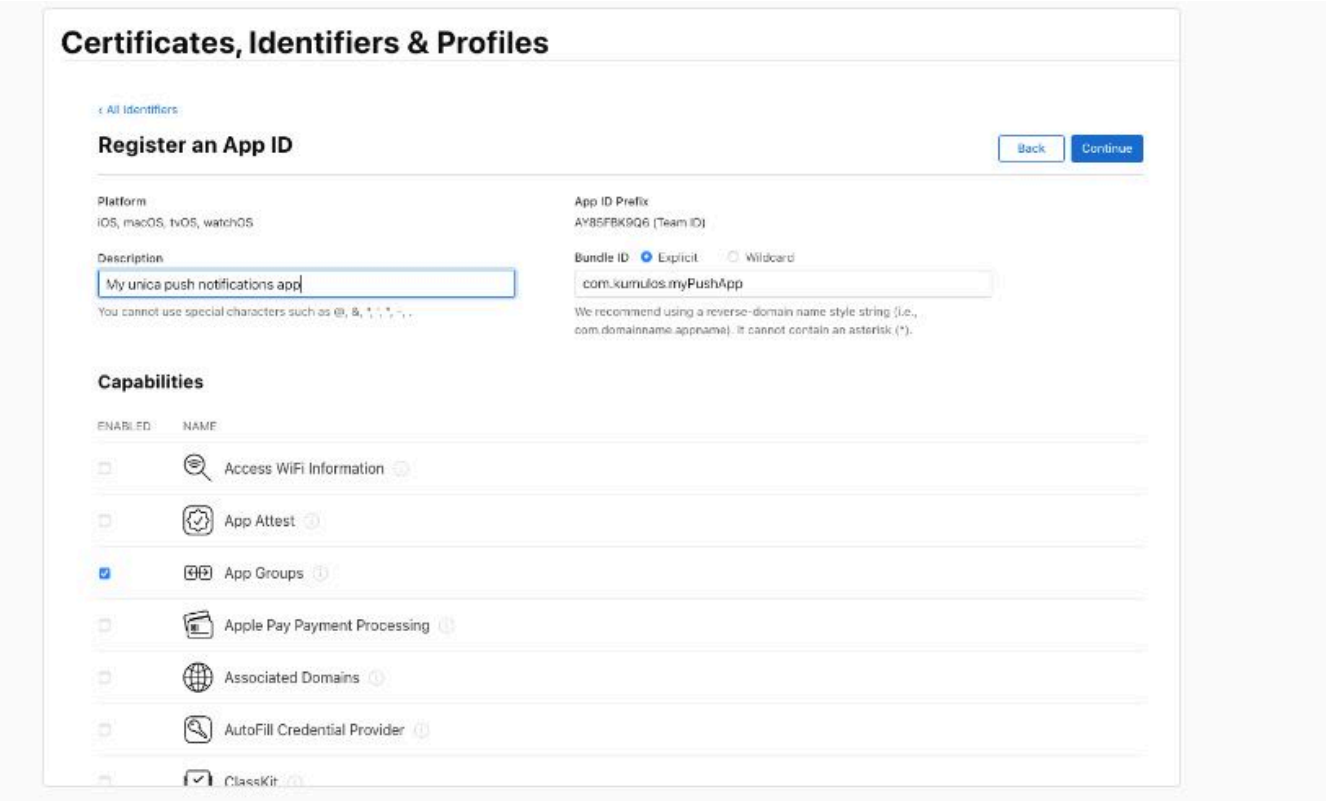


Lorsque vous êtes invité à enregistrer un nouvel identifiant, sélectionnez l'option Identifiant de l'app et cliquez sur Continuer puis, à la deuxième étape, sélectionnez le type App et cliquez à nouveau sur Continuer.



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.

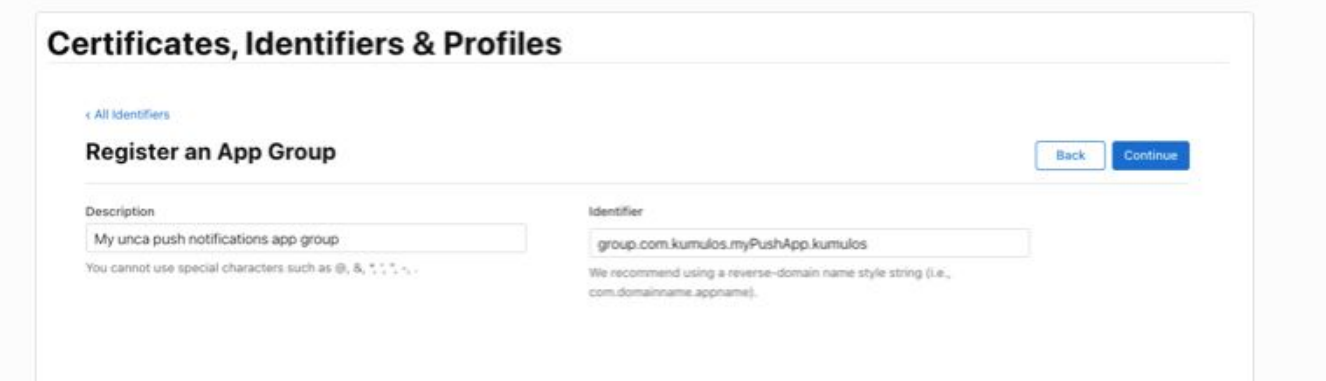
Dans la section Capacités, vérifiez que les cases « Groupes d'apps » et « Notifications push » sont cochées, puis appuyez sur Continuer.



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.

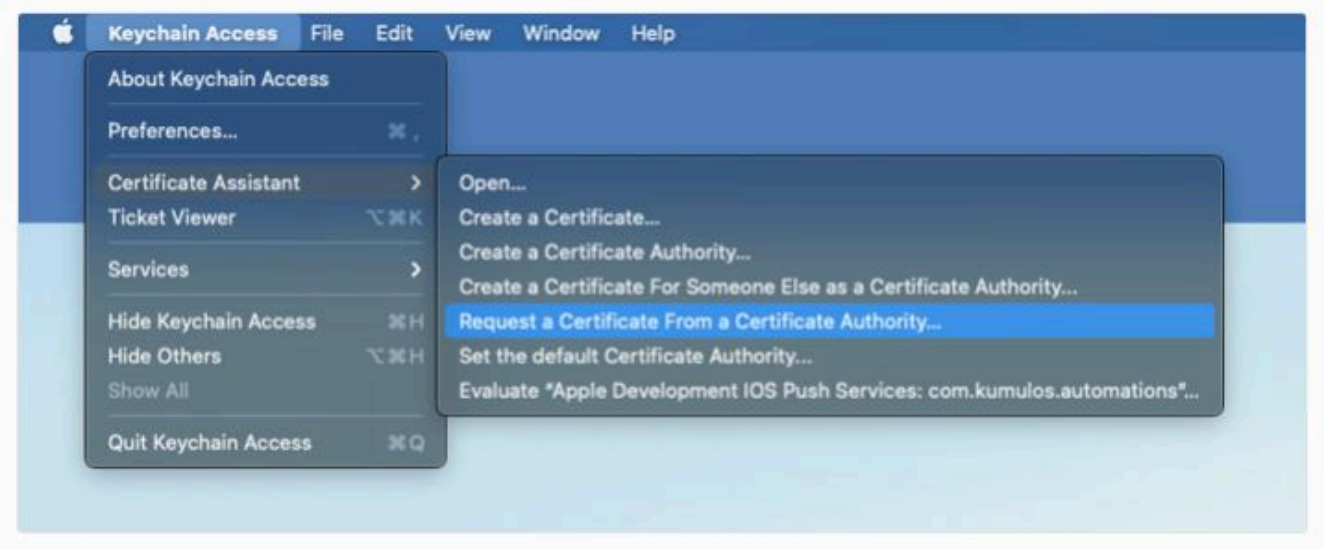
Dans l'écran « Editer la configuration de votre identifiant d'app », cliquez sur le bouton « Configurer » à côté de la capacité « Groupes d'apps ». Dans la fenêtre contextuelle, cochez la case à côté du groupe créé à l'étape précédente avec l'identifiant de lot correspondant, puis cliquez sur « Continuer ». 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

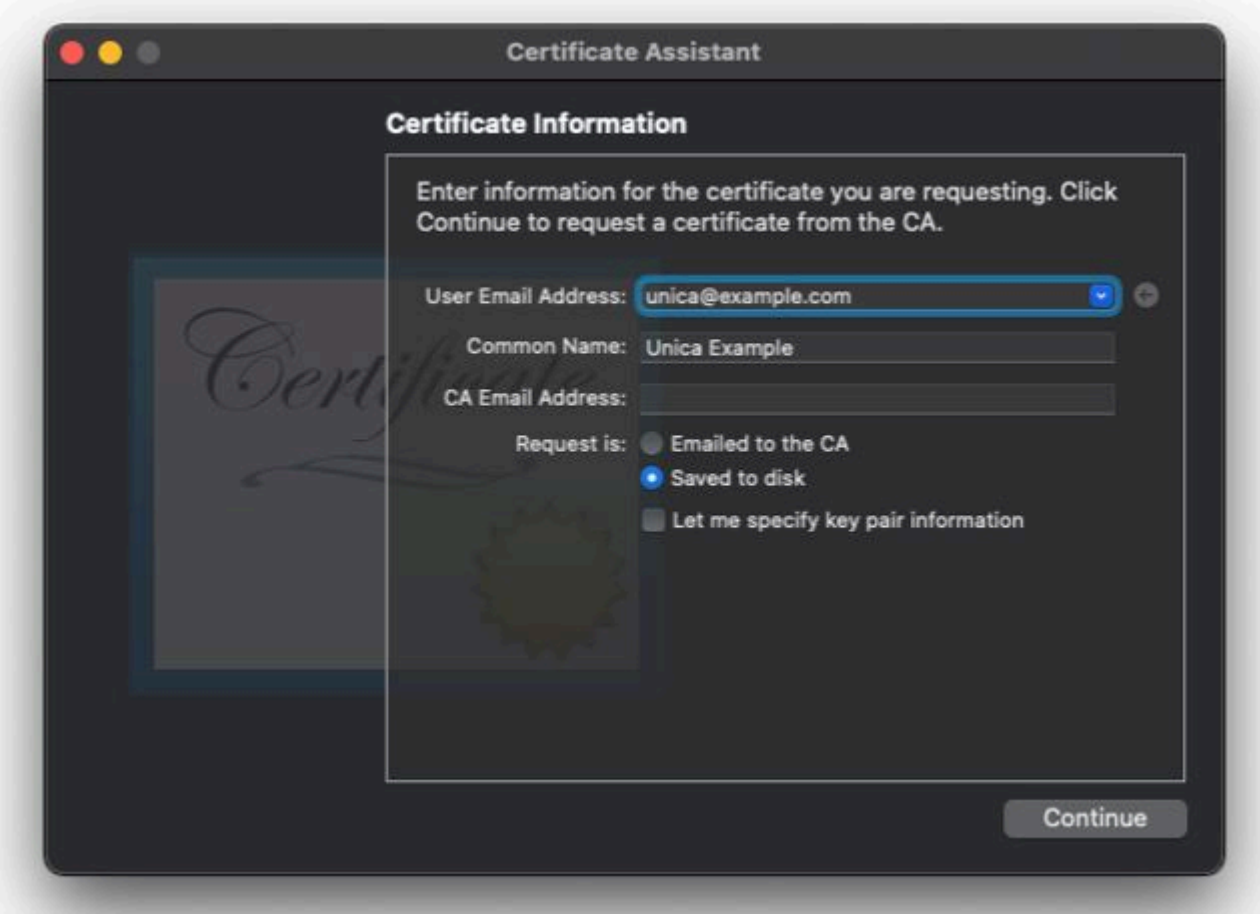
Pour envoyer des notifications Push aux périphériques iOS avec Unica, vous devrez créer des certificats dans Apple Developer Member Center afin d'enregistrer les données d'identification auprès de votre application Unica.

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

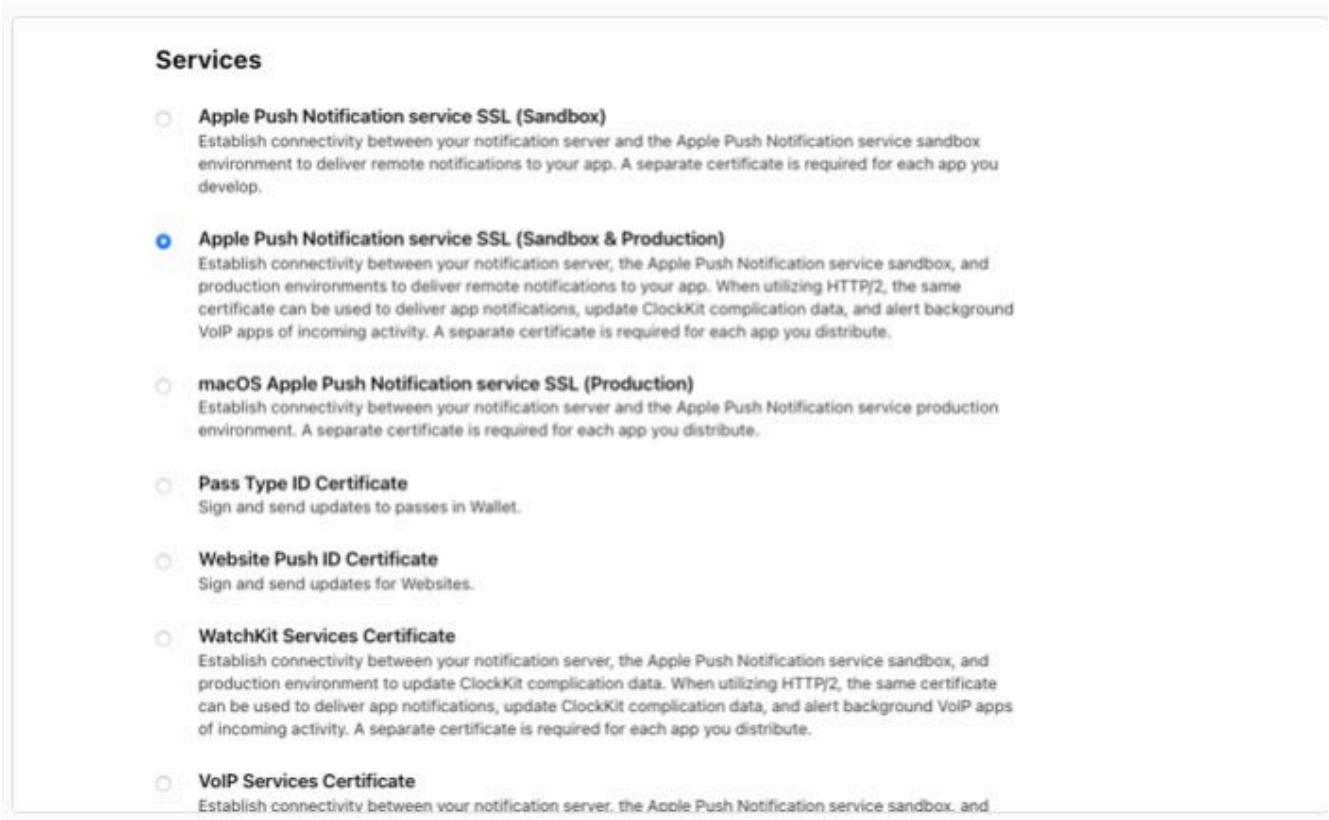
Tout d'abord, nous allons créer une demande de signature de certificat, à l'aide de Keychain Access. Accédez au menu Keychain Access depuis votre barre d'outils et sélectionnez Assistant de certificat, Demander un certificat à une autorité de certification.



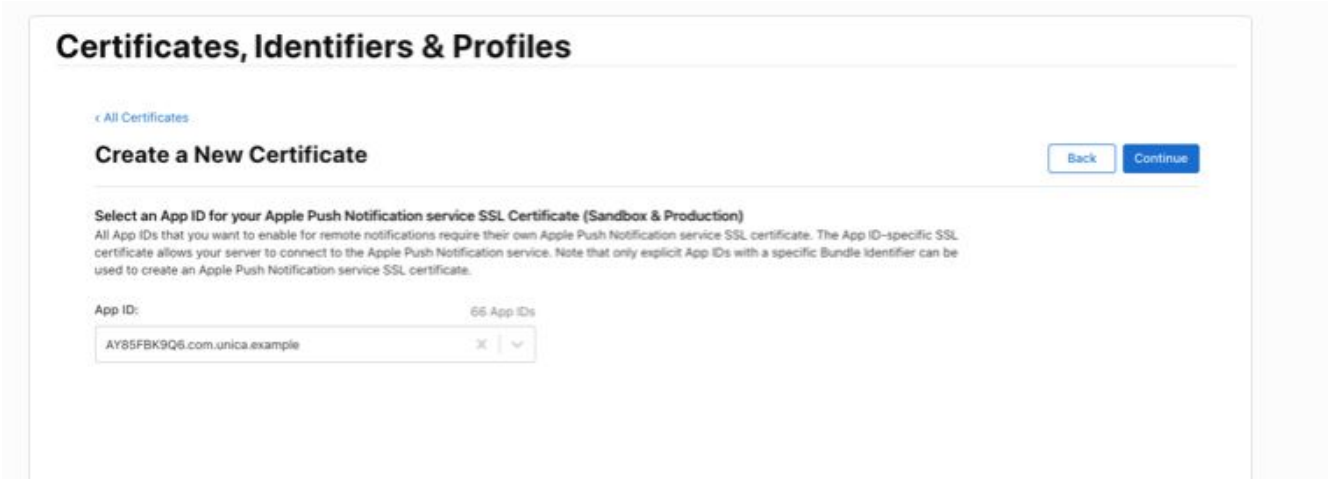
Dans la fenêtre de la boîte de dialogue, entrez votre courrier électronique dans le champ « Adresse e-mail de l'utilisateur ». Votre nom doit déjà apparaître dans le champ « Nom usuel ». Sélectionnez la case d'option 'Enregistré sur le disque' et cliquez sur 'Continuer'. Enregistrez le fichier sur votre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

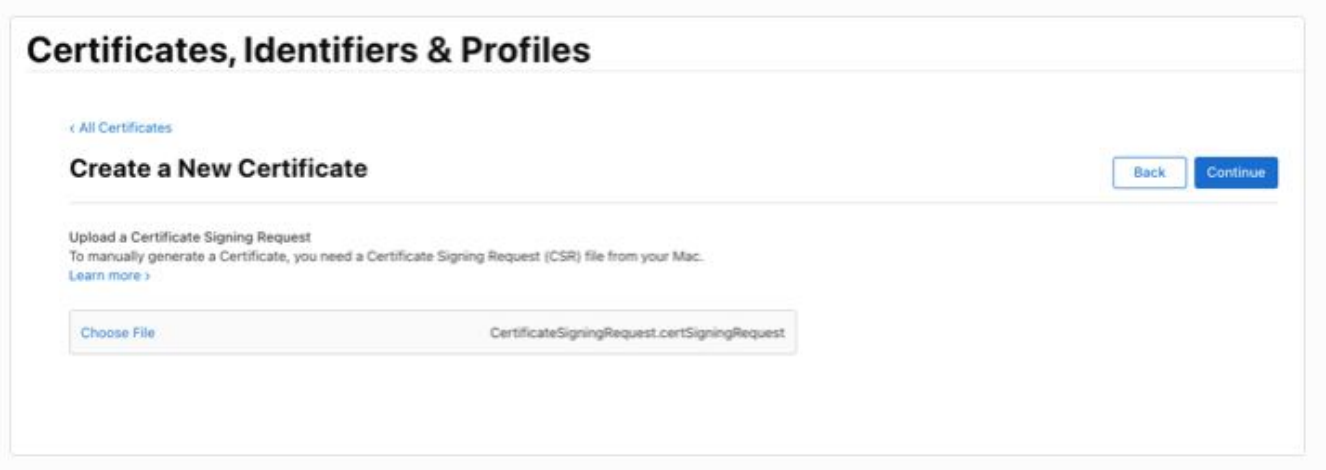


Sur l'écran suivant, sélectionnez l'identifiant d'application lors du processus de mise en route, puis cliquez sur Continuer.



Lorsque vous êtes invité à charger une demande de signature de certificat, cliquez sur Sélectionner un fichier et rechercher, puis sélectionnez le fichier

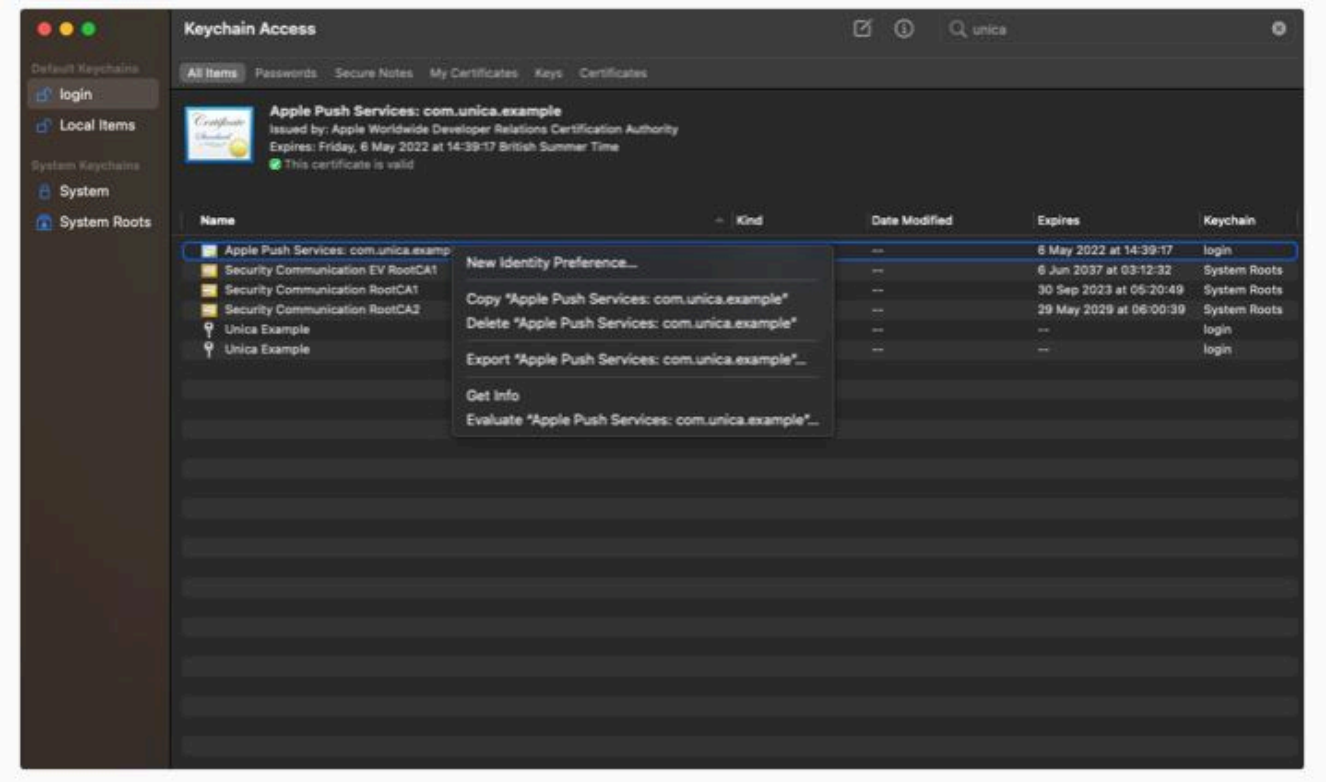
`certSigningRequest` créé précédemment et cliquez sur Continuer.



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.

Intégration

Ajoutez les composants Firebase à votre application comme indiqué ci-dessous.

Dans la **racine**`build.gradle`, assurez-vous que le référentiel Google est activé et que le plug-in google-services se trouve dans le chemin d'accès aux classes :

Les bibliothèques Kumulos sont distribuées via JCenter. Pour installer les bibliothèques, éditez le fichier `build.gradle` de votre application pour ajouter ce qui suit :

- Exclure de la génération les fichiers de métadonnées conflictuels
- Déclarer les options de compilation source et cible
- Ajouter les dépendances de bibliothèque Kumulos

- Ajouter le SDK de base Firebase
- Appliquer le plug-in google-services

Vous trouverez ci-dessous un exemple de `build.gradle`.

```
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'
```

La journalisation sera activée pour `debugImplementation` avec une balise `com.kumulos.*` correspondante. Lors de l'exécution en mode débogage, les messages du journal doivent être visibles dans LogCat.

Exécutez une synchronisation Gradle pour installer les bibliothèques Kumulos et générer votre projet.

Par défaut, le SDK Firebase enverra des données d'analyse à Google. Pour désactiver cela, ajoutez simplement

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

au fichier de votre application `AndroidManifest.xml`

Téléchargez le fichier `google-services.json` à partir des paramètres 'Général' de votre application Firebase et ajoutez-le à votre dossier `app/`.

A présent, vous pouvez ajouter `FirebaseMessagingService` et `PushBroadcastReceiver` de Kumulos à votre `AndroidManifest.xml`.

```
<?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>
```

Initialisation et enregistrement pour les notifications Push

Pour initialiser le SDK, nous recommandons de sous-classer la classe `Application` et d'initialiser Kumulos dans sa méthode `onCreate`.

```java
package com.example;

import android.app.Application;
import com.kumulos.android.Kumulos;
import com.kumulos.android.KumulosConfig;

public class ExampleApp extends Application {

    @Override
    public void onCreate() {
        super.onCreate();

        KumulosConfig config = new KumulosConfig.Builder("YOUR_API_KE
        Kumulos.initialize(this, config);

        Kumulos.pushRegister(context);
    }
}
```

Si vous souhaitez désenregistrer l'installation, vous pouvez utiliser `Kumulos.pushUnregister(context)`.

.

Enregistrement auprès de votre CRM

Identifiant d'installation

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 :

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

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.

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(context, "unique-user-identifier");
```

Fonctions avancées

Gestion des boutons d'action Push

Les messages Push vous permettent de passer la main aux écrans d'application natifs via des boutons d'action Push de lien profond. Lorsque l'utilisateur appuie dessus, ces boutons passent le contrôle au gestionnaire d'action Push défini.

Si vous souhaitez gérer les liens profonds dans le cadre d'un message Push, vous pouvez créer une classe qui implémente `PushActionHandlerInterface` et l'affecte lors de l'initialisation du SDK.

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

Le stub du gestionnaire pourrait être implémenté comme suit :

```
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
    }
}
```

Comportement Push par défaut

Par défaut, Kumulos `PushBroadcastReceiver` affiche une notification dans la zone de notification du périphérique lorsqu'une notification Push de contenu est reçue.

L'appui sur cette notification ouvrira l'activité principale du lanceur de votre application et suivra la conversion Push ouverte pour vous.

Votre activité principale recevra le contenu Push dans son groupement d'options sous `PushMessage.EXTRAS_KEY`.

Modification de l'icône Push

Pour modifier l'icône affichée dans la barre d'état sur Android, vous pouvez configurer Kumulos avec un Drawable au moment de l'initialisation :

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

Assurez-vous que vous respectez les consignes relatives à l'icône de la barre d'état afin que l'icône s'affiche correctement sur tous les périphériques. Pour obtenir de l'aide sur la préparation des ressources, nous vous suggérons d'utiliser Android Asset Studio.

Personnalisation de comportement Push

Pour personnaliser le comportement du SDK lorsqu'un Push est reçu ou que l'utilisateur appuie sur sa notification, nous vous suggérons de sous-classer `PushBroadcastReceiver` et de modifier ses méthodes de base en fonction de ce que vous souhaitez personnaliser.

Exemple de classe d'extension :

```
package com.example;

import com.kumulos.android.PushBroadcastReceiver;

public class MyPushReceiver extends PushBroadcastReceiver {

}
```

Veillez à modifier le récepteur `AndroidManifest.xml` :

```
<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>
```

Modification de l'activité lancée

Pour modifier l'activité lancée lorsque l'utilisateur appuie sur une notification, vous pouvez remplacer

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

.

```java
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);
    }
}
```

Le modèle `PushMessage` ne sera pas ajouté au `Intent` par défaut, c'est à vous de l'ajouter en tant qu'élément supplémentaire si vous le souhaitez :

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

Vous pouvez retourner `null` pour suivre la conversion Push et ne rien faire lorsque l'utilisateur appuie sur la notification.

Si le `Intent` renvoyé ne décrit pas une `Activity`, il sera ignoré

Personnalisation de la notification

Pour personnaliser la notification affichée pour l'utilisateur pour les notifications Push de contenu, vous pouvez remplacer `PushBroadcastReceiver#buildNotification(Context, PushMessage)`.

```
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);
    }
}
```

Si vous souhaitez gérer l'ouverture/le rejet avec le récepteur de diffusion, assurez-vous de configurer les intentions de contenu de la notification comme suit :

```
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);
```

Cela permet de s'assurer que la conversion de la notification est suivie dans Kumulos.

Si vous souhaitez faire autre chose, vous pouvez suivre manuellement la conversion Push ouverte à l'aide de `Kumulos#pushTrackOpen(Context, int)` et suivre l'événement de rejet à l'aide de `Kumulos#pushTrackDismissed(Context, int)`. En outre, vous devrez ajouter des suppléments de lien profond pour que les liens profonds des messages dans l'application continuent de fonctionner.

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

Lancement d'un service pour les Push de données d'arrière-plan

Pour lancer un service lorsqu'un Push de données d'arrière-plan est reçu, vous pouvez remplacer `PushBroadcastReceiver#getBackgroundPushServiceIntent`.

```
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
    }
}
```

Cela vous permet facilement de gérer le traitement des données en arrière-plan en lançant un `IntentService` par exemple.

Le modèle `PushMessage` ne sera pas ajouté au `Intent` par défaut, c'est à vous de l'ajouter en tant qu'élément supplémentaire si vous le souhaitez :

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

Renvoyez `null` si vous ne souhaitez rien faire avec le Push de données.

Si le `Intent` renvoyé ne décrit pas un `Service`, il sera ignoré

Push d'URL

Les notifications Push envoyées pour ouvrir une URL détecteront, par défaut, l'ouverture du Push si l'utilisateur appuie sur la notification, puis ouvre le navigateur Internet par défaut.

Remplacement de tous les comportements

Si vous souhaitez remplacer complètement la logique de gestion des Push, vous pouvez remplacer `PushBroadcastReceiver#onPushReceived(Context, PushMessage)`.

Gardez à l'esprit que vous serez responsable de tous les aspects du processus Push, tels que l'affichage d'une notification pour l'utilisateur, le suivi d'une conversion ouverte à l'aide de `Kumulos#pushTrackOpen(Context, int)` et d'événements de rejet à l'aide de `Kumulos#pushTrackDismissed(Context, int)`, ou le lancement d'activités ou de services.

En outre, vous devrez peut-être implémenter des comportements pour les événements suivants :

- Le suivi de la distribution : `pushTrackDelivered(context, pushMessage)`

Utilisation de votre propre `FirebaseMessagingService` avec Kumulos

Si vous utilisez déjà les notifications push FCM avec votre propre `FirebaseMessagingService`, mais que vous souhaitez également bénéficier des avantages du service Push de Kumulos, vous pouvez utiliser les méthodes d'aide du SDK dans votre propre implémentation. Par exemple :

```
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(
    }
}
```

Identification des incidents

Proguard

Si vous utilisez ProGuard pour optimiser votre code de Java, vous devez vous assurer que votre fichier `proguard.cfg` inclut le SDK Kumulos et les composants requis. Exemple :

```
-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 est également très sensible au codage UTF-8 avec BOM, alors que les outils Android accepteront *uniquement* le codage UTF-8. Par conséquent, pour vous assurer facilement que vous ne disposez pas d'indicateurs d'ordre des octets UTF-8 dans votre fichier `proguard.cfg`, utilisez vim dans le terminal comme suit :

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

React Native

Introduction

Le SDK Kumulos est un projet open source hébergé sur Github et qui se trouve à l'adresse https://github.com/Kumulos/KumulosSdkReactNative.

Ce guide suppose que vous avez effectué les étapes de l'introduction et que vous avez configuré votre projet via le compte Apple Developer et la console Firebase. Il abordera les étapes suivantes :

1. Intégrez le SDK et configurez vos projets pour la fonction APNS/FCM.
2. Initialisation des composants du SDK dans votre projet et enregistrement pour les notifications Push.
3. Enregistrement de l'installationID de Kumulos avec votre système dorsal pour fournir un lien entre le périphérique et les utilisateurs représentés dans le système dorsal de votre CRM pour le ciblage ultérieur des notifications.
4. Envoi d'une notification Push de test à partir de votre application Unica et réception de celle-ci sur le périphérique.
5. Crochets facultatifs pour un comportement avancé.

Intégration

Le module React Native Kumulos requiert des fonctionnalités natives et doit donc être installé dans un projet éjecté.

Pour installer et lier le projet, exécutez les commandes suivantes :

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

Des étapes de liaison manuelle sont requises pour chaque plateforme.

Etapes de liaison Android

Pour effectuer le processus de liaison pour Android, vous devez vous assurer que votre projet utilise les versions suivantes pour les outils et les bibliothèques :

- Plug-in Gradle 3.1.3 ou version ultérieure
- Outils de génération 23.0.3 ou version ultérieure
- Bibliothèque de support 27 ou version ultérieure

Placez le fichier `google-services.json` créé lors de l'introduction dans le répertoire android/app de votre projet. En outre, vous devez ajouter ce qui suit à votre fichier `android/app/build.gradle` :

```
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'
}
```

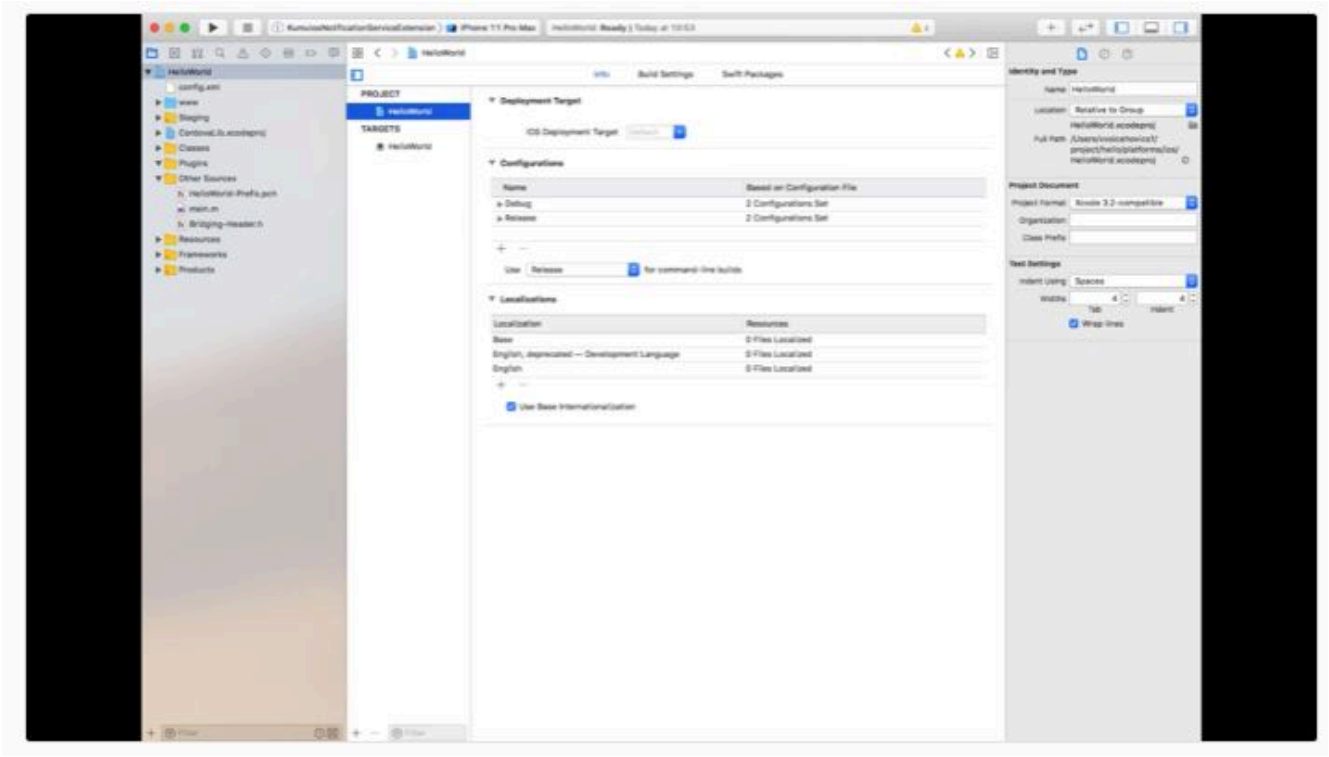
Configuration de projet iOS

La notification se développera lors du balayage sur celle-ci sur les périphériques compatibles avec la fonctionnalité 3D Touch. Pour activer cette fonctionnalité, vous devez ouvrir votre projet iOS dans Xcode et ajouter une extension de service de notification à votre application.

Ajouter une extension de service de notification

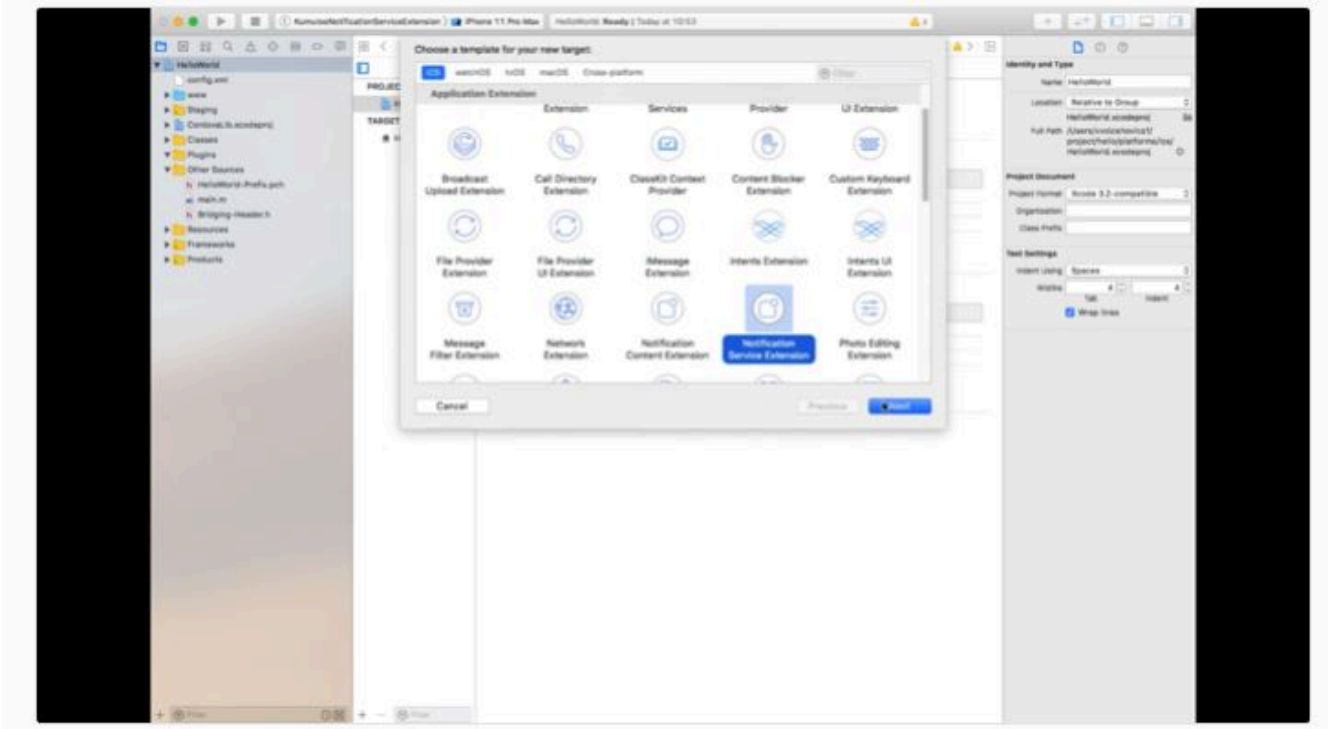
Pour prendre en charge toutes les fonctions d'Apple Push Notification Service, votre application doit posséder une extension de service de notification afin d'autoriser un traitement limité de la notification à sa réception, avant que le système d'exploitation ne la présente à l'utilisateur.

Il s'agit d'une deuxième cible de génération, qui est ajoutée à votre projet xcode existant en allant à l'écran d'informations de votre projet et en cliquant sur le bouton '+' en bas de l'écran.

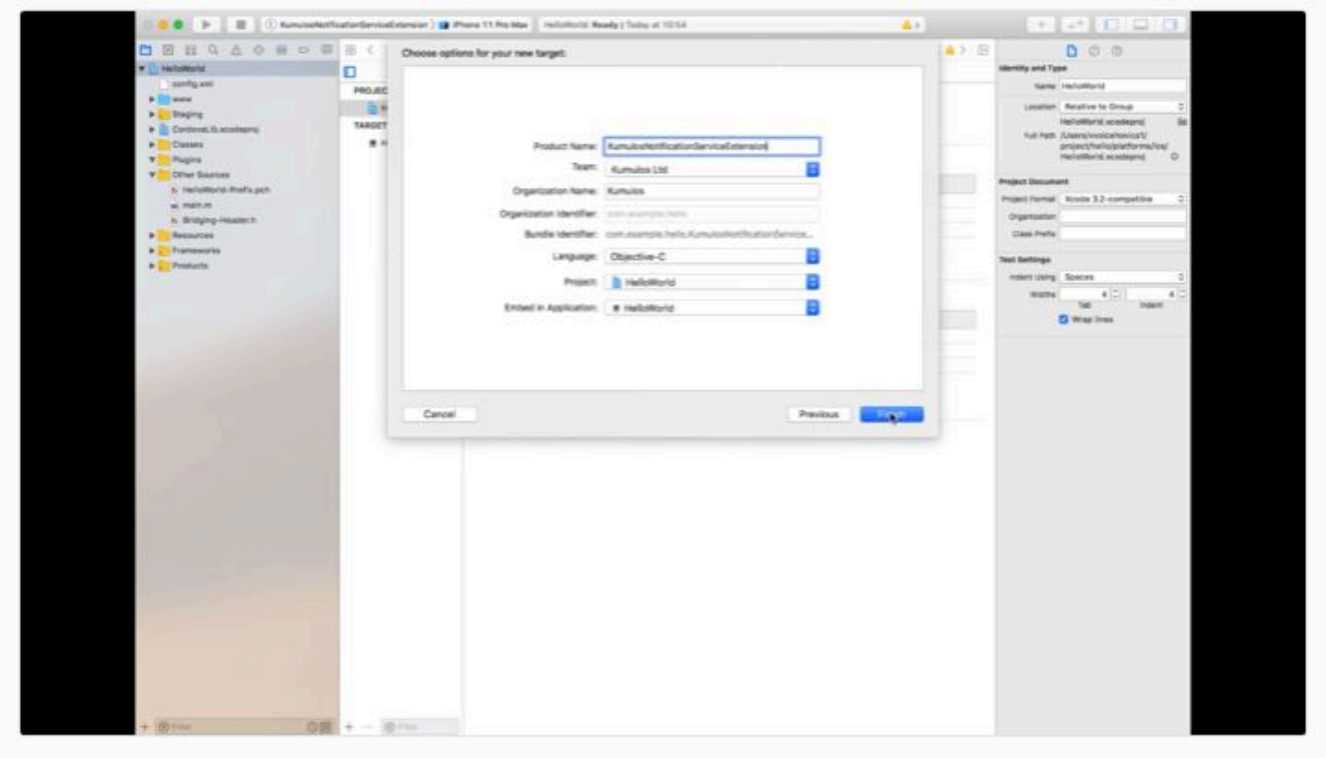


Dans la fenêtre contextuelle, sélectionnez le modèle

`Notification Service Extension` pour votre nouveau projet et cliquez sur 'Suivant'.



Dans la fenêtre finale, ajoutez un nom approprié pour votre extension et cliquez sur 'Terminer'.



Ajoutez ce qui suit au fichier Podfile généré par React Native et exécutez `pod install`.

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

Le modèle du projet aura créé automatiquement un fichier nommé `NotificationService.m`. Remplacez son contenu par les lignes suivantes :

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

@interface NotificationService ()
@end

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

Les fonctions d'aide du SDK Kumulos ajouteront automatiquement des boutons et des pièces jointes d'image au contenu de la notification.

Configurer les capacités et les droits de votre application

Dans les paramètres de votre projet d'application, utilisez le bouton « + capacité » pour ajouter les fonctions Groupes d'applications, Modes d'arrière-plan et Notifications push.

Dans votre extension de notification, utilisez le bouton « + capacité » pour ajouter la fonction Groupes d'applications.

Dans les deux projets, la fonction Groupes d'applications doit être configurée pour partager le même groupe. Ce dernier doit correspondre exactement au groupe défini précédemment dans les capacité de vos identifiants.

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

Dans votre projet d'application, le mode « Notifications à distance » doit être coché pour les modes d'arrière-plan.

Tester votre configuration

A ce stade, vous pouvez tester le déploiement de votre application sur un périphérique pour vous assurer que vos droits et capacités sont configurés correctement. Veillez à configurer correctement la connexion pour la cible d'extension.

Initialisation

Pour configurer le SDK afin de l'utiliser, vous devez l'initialiser avec les données d'identification d'API de votre application. Cette procédure doit être effectuée au début du démarrage de votre application afin que vous puissiez commencer à appeler des méthodes API et à utiliser des fonctionnalités.

Dans votre `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();
```

Dans votre méthode `ios/AppDelegate.mapplication:didFinishLaunchingWithOptions:` :

```
#import <KumulosReactNative/KumulosReactNative.h>
...
KSConfig* kumulosConfig = [KSConfig
    configWithAPIKey:@"YOUR_API_KEY"
    andSecretKey:@"YOUR_SECRET_KEY"];

[KumulosReactNative initializeWithConfig:kumulosConfig];
```

Dans votre méthode `android/app/src/main/java/.../MainApplication.javaonCreate` :

```
import com.kumulos.android.KumulosConfig;
import com.kumulos.reactnative.KumulosReactNative;
...
KumulosConfig.Builder kumulosConfig = new KumulosConfig.Builder("YOUR
KumulosReactNative.initialize(this, kumulosConfig);
```

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');
```

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
```

Script RCT (Response and Contact Tracker) d'Deliver

Utilisez ce script pour exécuter et vérifier le statut de l'RCT (Response and Contact Tracker).

Ce script est situé dans le répertoire `bin` de votre installation Deliver. Le répertoire Deliver est un sous-répertoire du répertoire Campaign.

Dans les environnements UNIX™ ou Linux™ exécutez le script sous la forme `rct.sh`.

Sous Windows™, exécutez le script à partir de la ligne de commande sous la forme `rct.bat`.

Syntaxe

```
rct [ start | stop | check ]
```

Commandes

démarrer

Démarre RCT.

stop

Arrête RCT.

Options

vérification

Vérifiez le statut de la connexion entre RCT et les services hébergés HCL Unica.

Exemples

- Pour démarrer RCT sous Windows™.

  ```
  rct.bat start
  ```

- Pour démarrer RCT sous Windows™.

  ```
  rct.bat stop
  ```

- Dans un environnement Linux™, pour déterminer si RCT est connecté aux services hébergés HCL Unica, procédez comme suit :

  ```
  rct.sh check
  ```

  Selon l'état de votre système, la sortie de cette commande peut se présenter comme suit :

  ```
  C:\<UNICA_HOME>\Campaign\Deliver\bin>rct check
  Testing config and connectivity for partition partition1
  Succeeded | Partition: partition1 - Hosted Services Account ID:
  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.

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.

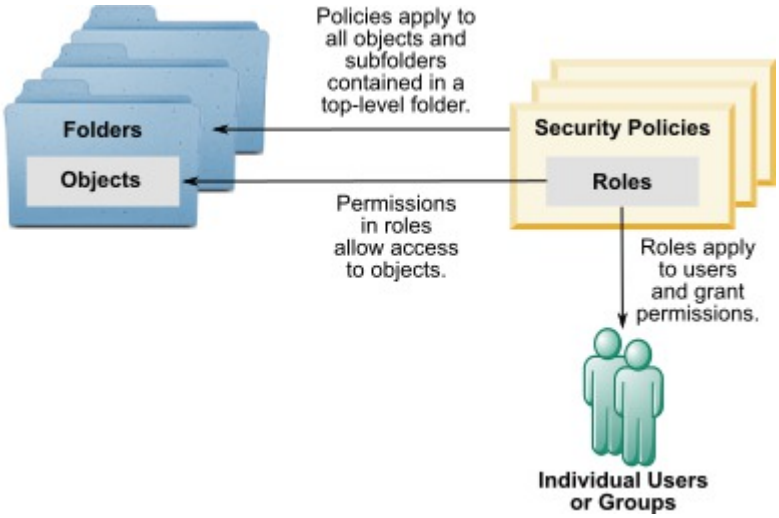
Dans Campaign, des règles de sécurité sont affectées aux dossiers. Lorsque vous créez un dossier de niveau supérieur, vous devez appliquer une règle de sécurité au dossier. Les objets ou les sous-dossiers dans le dossier héritent de la règle de sécurité du dossier.

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.

À propos de cette tâche

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.
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 bibliothèque de contenu Deliver	Permet à un utilisateur de créer un élément de contenu et de l’ajouter à la bibliothèque de contenu.
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.
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.

Droits	Description
	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.

À propos de cette tâche

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**.
   Résultat
   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**.
   Résultat
   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.

Résultats

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.

À propos de cette tâche

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.

Résultats

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.

À propos de cette tâche

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 132
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 133
Activez la restriction d'accès.	Activation de la restriction pour la liste des messages envoyés à la page 134

Résultats

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.

À propos de cette tâche

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.

Résultats

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**.

Que faire ensuite

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.

À propos de cette tâche

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.

Résultats

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**.

Que faire ensuite

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.

À propos de cette tâche

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.

Résultats

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. Note technique (traitement des incidents)

Problème (extrait)

Pour utiliser les composants Deliver installés avec Unica Campaign et envoyer des messages marketing personnalisés, vous devez connecter l'installation locale de Campaign aux ressources de messagerie distantes hébergées par HCL. Cette section explique comment configurer une telle connexion lorsque vos règles de pare-feu d’entreprise interdisent la communication directe avec l’environnement hébergé.

Résolution du problème

Communication type avec l’environnement de ressources de messagerie hébergées

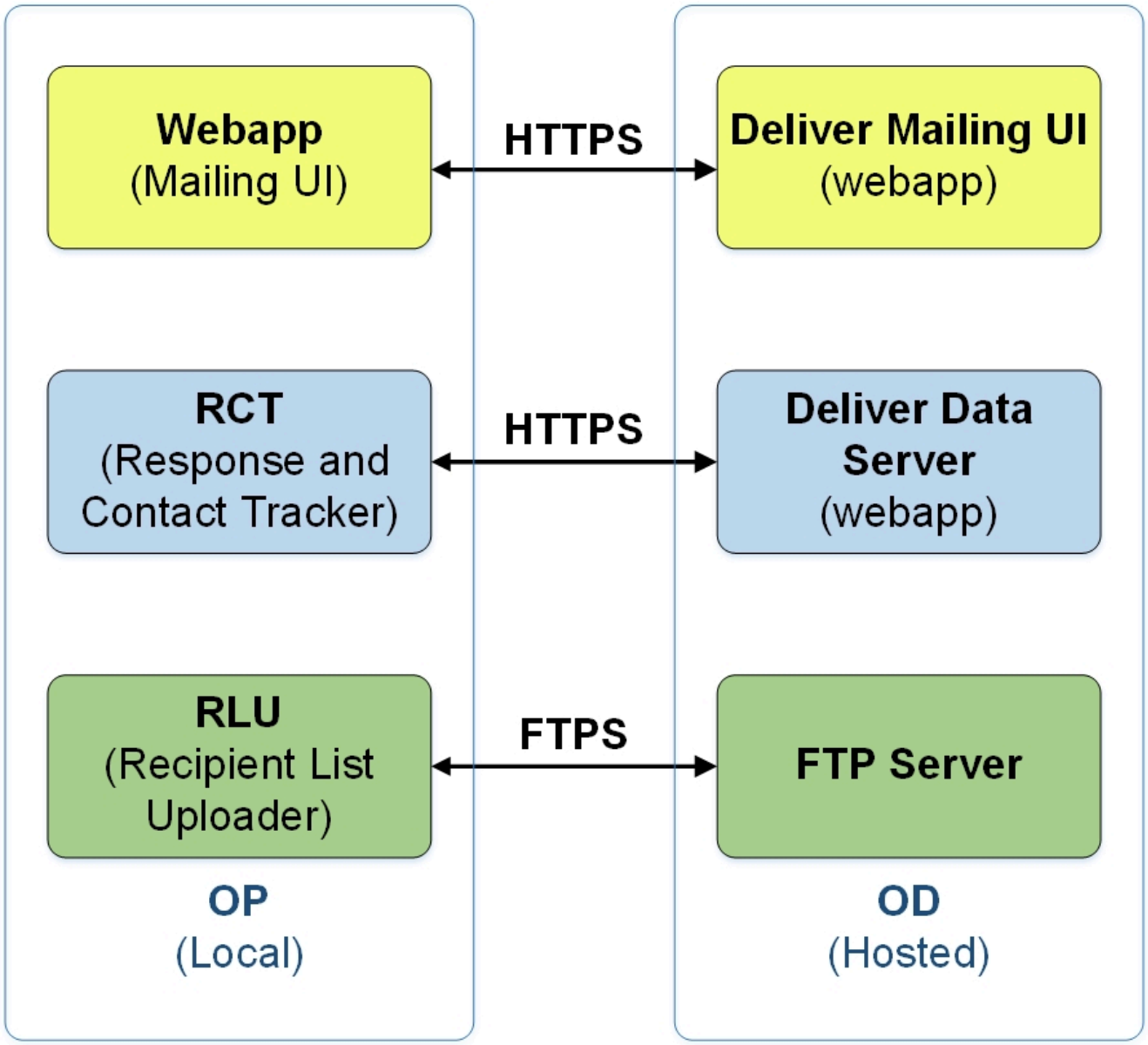
Le diagramme suivant illustre la configuration standard pour la communication entre l’environnement sur site (OP) et l’environnement à la demande (OD).

L’environnement local OP Deliver requiert une communication externe avec l’environnement OD Deliver utilisant HTTPS et FTPes (FTP explicite) ou FTPs (FTP implicite). Cette section utilise le terme FTPS pour faire référence à un protocole FTP explicite et implicite.

L’environnement OP inclut un serveur d'application Web (IBM WebSphere ou Oracle WebLogic) sur lequel vous avez déployé Campaign. Campaign héberge les composants Deliver (RCT et RLU) qui communiquent avec les ressources de messagerie hébergée dans l’environnement OD.

Le service RCT (Response and Contact Tracker) télécharge les données de réponse de l’environnement OD.

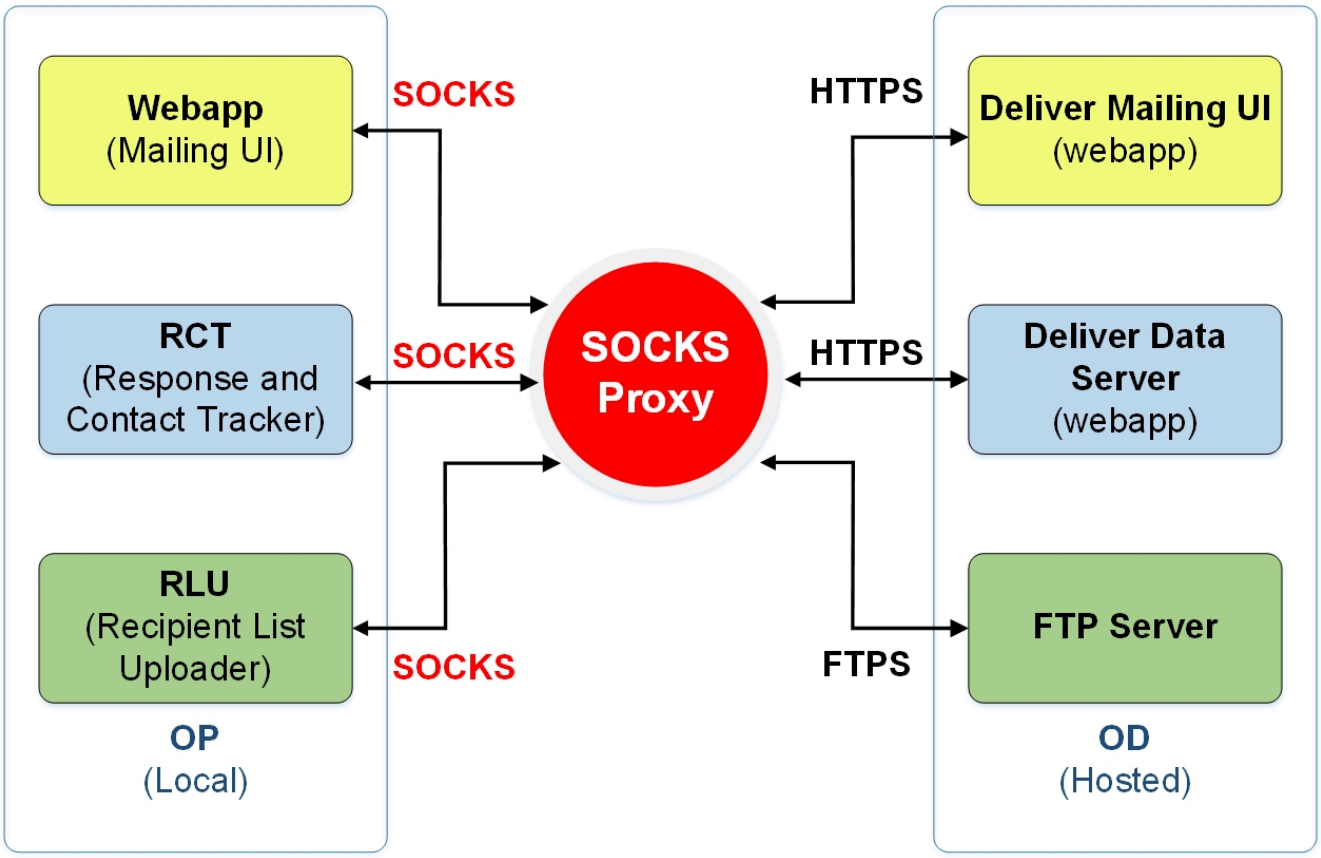
Le service RLU (Response List Uploader) télécharge les listes de diffusion et d’autres données de mailing requises dans l’environnement OD.



Lorsque la machine sur laquelle Unica Deliver est installé ne peut pas communiquer directement avec l'environnement OD, Deliver prend en charge la communication avec les ressources OD hébergées via un proxy SOCKS.

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.

Modifications requises pour le routage du trafic SFTP/FTPS et HTTPS à travers un proxy SOCKS

Pour utiliser un proxy SOCKS afin d'accéder aux ressources de messagerie hébergées par HCL, vous devez apporter des modifications à l'application Web dans laquelle vous avez déployé Campaign et aux scripts de démarrage du RCT et du RLU de Deliver.

Effectuer des modifications pour SFTP/FTPS

Pour le trafic SFTP/FTPS, appliquez les configurations suivantes à la RLU et au serveur d'applications Web.

- `- Dhcl.unica.deliver.ftp.proxy.host = <socksHost>`
- `- Dhcl.unica.deliver.ftp.proxy.port = <socksPort>`
- `- Dhcl.unica.deliver.ftps.proxy.match.hosts = <liste séparée par des virgules de noms d'hôtes et d'adresses IP>.`

socksHost est le nom d'hôte ou l'IP du proxy SOCKS.

socksPort est le port sur lequel le proxy SOCKS fonctionne.

`-Dhcl.unica.deliver.ftps.proxy.match.hosts` correspond aux noms d'hôtes et aux IP utilisés lors du routage du trafic via le proxy SOCKS.

L'adresse IP spécifiée pour `-Dhcl.unica.deliver.ftps.proxy.match.hosts` est l'adresse IP que le serveur FTP dans l'environnement OD hébergé envoie au client FTP dans l'environnement OP local dans le cadre du protocole SFTP/FTPS pendant le transfert de données.

Définissez `-Dhcl.unica.deliver.ftps.proxy.match.hosts` à l'une des valeurs suivantes (dépend du centre de données utilisé par votre compte de messagerie hébergé).

Centre de données américain : `-Dhcl.unica.deliver.ftps.proxy.match.hosts=ftp-em.unicadeliver.com`

Centre de données en Inde : `-Dhcl.unica.deliver.ftps.proxy.match.hosts=ftp-in.unicadeliver.com`

Centre de données européen : `-Dhcl.unica.deliver.ftps.proxy.match.hosts=ftp-eu.unicadeliver.com`

Apporter des modifications pour HTTPS

Pour le trafic HTTPS, appliquez les configurations suivantes au RCT et au serveur d'applications web.

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

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

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

socksHost est le nom d'hôte ou l'IP du proxy SOCKS.

socksPort est le port sur lequel le proxy SOCKS fonctionne.

Exigences d'authentification lors de l'utilisation d'un proxy SOCKS

Si votre proxy SOCKS requiert une authentification, configurez les éléments suivants pour les serveurs d'applications web, RLU et RCT.

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

Où le nom d'utilisateur et le mot de passe sont les informations d'identification requises pour s'authentifier auprès du proxy.

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
```

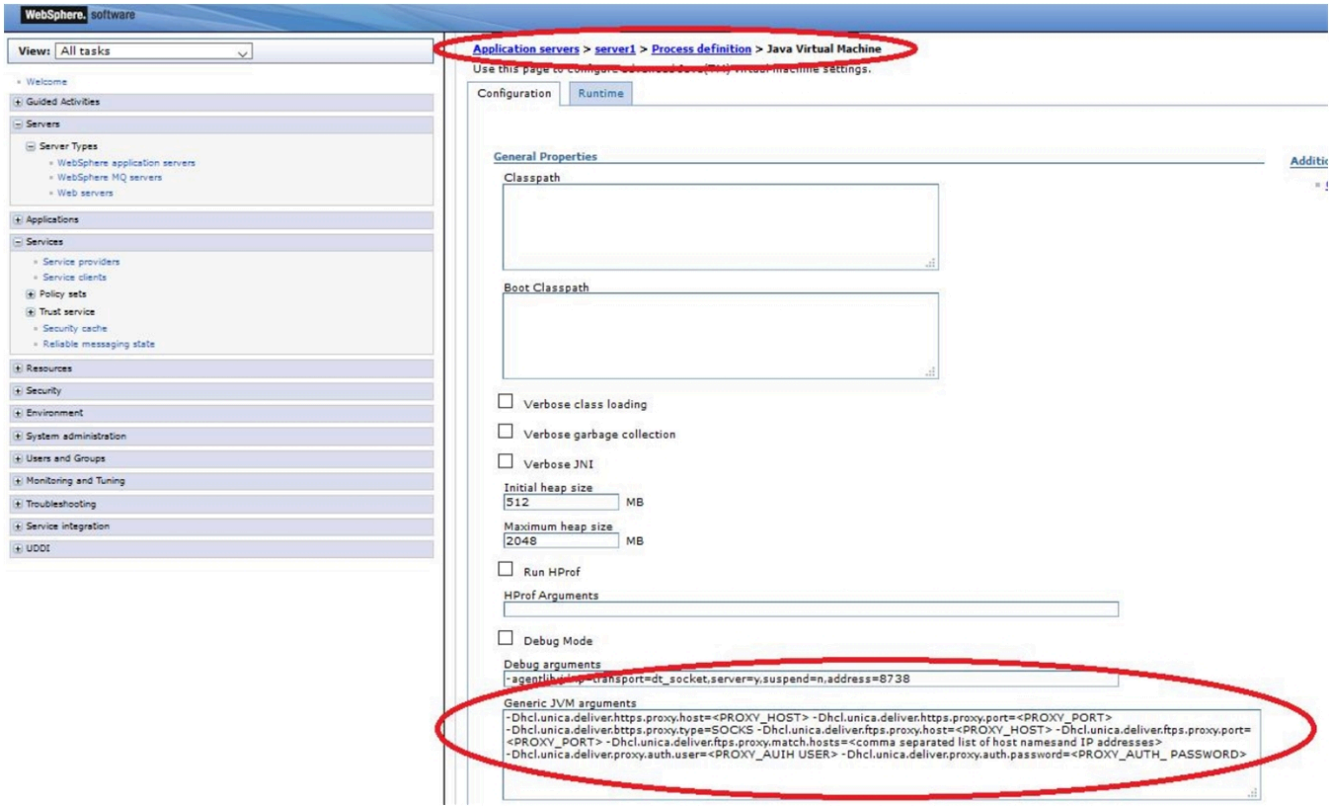
```
-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>
```

```
-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. Configuration du compte du fournisseur de canal Deliver

Deliver prend en charge les SMS, WhatsApp et Push en tant que canaux de distribution en plus des e-mails. Deliver prend en charge les SMS, WhatsApp et Push en tant que canaux de distribution en plus des e-mails. Les SMS sont pris en charge à l'aide de différents fournisseurs, de sorte que le client a le choix de sélectionner un partenaire SMS en fonction des aspects géographiques et de coût. Chaque fois qu'un client décide d'utiliser un fournisseur spécifique pour les messages SMS ou WhatsApp, HCL collabore avec le client et le fournisseur requis pour intégrer ce dernier sans heurts à Deliver. Dans le cadre de ce processus, le compte du client est créé avec chaque fournisseur. Ce compte permet à Deliver d'envoyer des messages au nom de ce client et de traiter les réponses des utilisateurs.

Deliver prend en charge les canaux suivants.

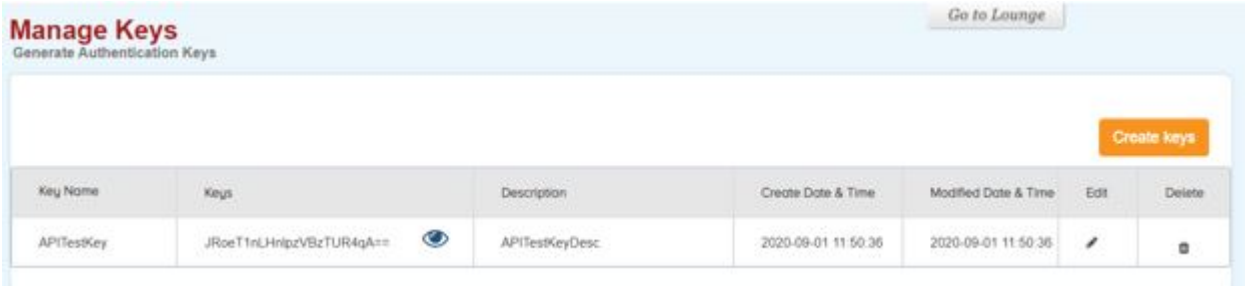
- SMS à l'aide du fournisseur Karix
- SMS à l'aide du fournisseur RML (pour les types de licence de renvoi et de revendeur)
- WhatsApp à l'aide du fournisseur RML
- Push à l'aide du fournisseur Kumulos
- SMS Twilio

Le document suivant explique ces étapes pour chacun de ces canaux. Ces étapes doivent être effectuées par ou pour chaque compte client dans le cadre du processus d'intégration.

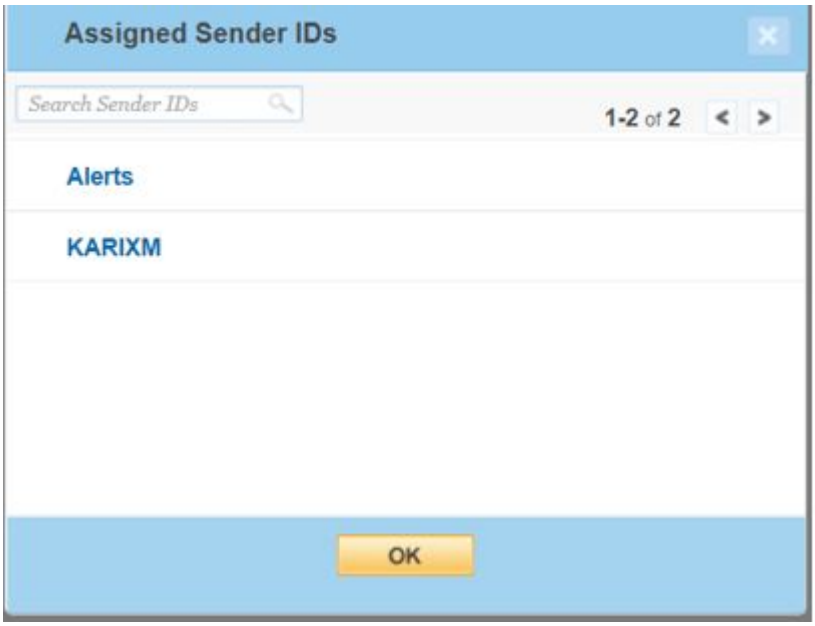
Configuration du compte SMS Karix

Procédez comme suit pour configurer le compte SMS Karix du client pour qu'il fonctionne avec Deliver.

1. Connectez-vous à la console Karix (www.karix.solutions) et cliquez sur le bouton Clés d'API du tableau de bord pour créer une clé d'API et la configurer avec Deliver.



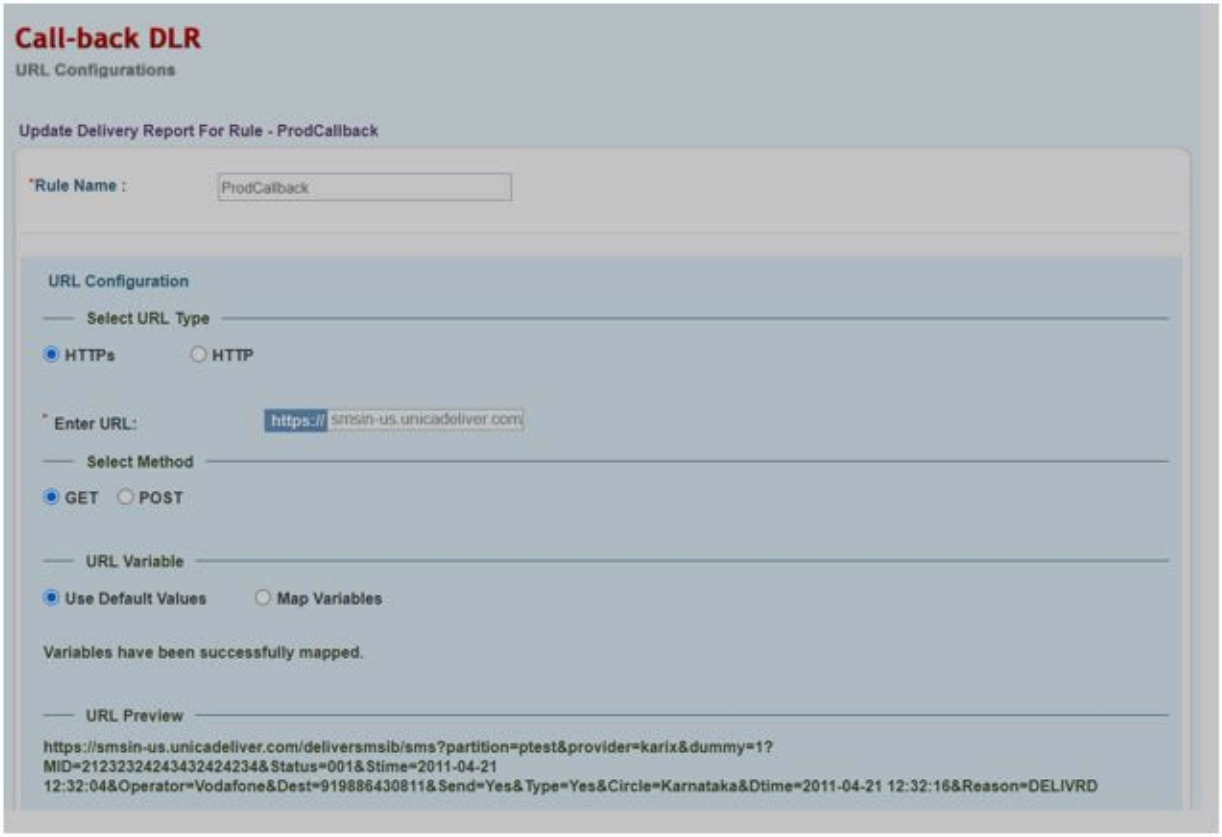
2. Dans l'angle supérieur droit, sous la liste **Ouvrir mon compte**, sélectionnez l'option **Modifier mes informations** et notez l'ID de l'expéditeur configuré pour votre compte Karix afin à configurer dans Deliver.



3. Indiquez la clé d'API créée à l'étape 1 et l'ID de l'expéditeur noté à l'étape 2 pour qu'elle soit configurée dans le compte.
4. Définissez l'URL de rappel dans la console Karix.

- Pour le centre de données des Etats-Unis : https://smsin-us.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=karix&dummy=1
- Pour le centre de données de l'UE : https://smsin-eu.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=karix&dummy=1

Note: Une fois que le compte est configuré dans Deliver, la valeur <account> dans l'URL ci-dessus doit être remplacée par le nom du compte fourni par l'équipe de mise à disposition de Deliver.



Configuration du compte SMS RML

Le compte SMS RML du client doit disposer des configurations suivantes pour fonctionner avec Deliver.

Intégration de compte RML

- Vous devez travailler avec l'équipe RML pour créer un compte SMS pour l'Inde ou le monde en fonction de l'emplacement du client.
- L'élément SenderId doit être fourni par le client configuré par RML.
- Les modèles SMS doivent également être inclus dans la liste blanche en fonction du lieu d'envoi de SMS cible. Par exemple, les modèles pré-approuvés requis pour les Etats-Unis et le Canada.

RML dispose de différentes URL de connexion en fonction de l'emplacement géographique, qu'il fournit dans le cadre de la création de compte par courrier électronique de son côté. Par exemple, les URL pour les centres de données Inde et Monde

- Compte Inde : https://ems.rmlconnect.net/
- Compte Monde : https://client.rmlconnect.net/login

Effectuez les opérations suivantes :

1. Connectez-vous à la console RML en suivant les URL ci-dessus et accédez à **Utilitaires > URL d'envoi Push DLR**.

   Note: Vous devez demander à RML d'ajouter ce menu lors de la mise à disposition du compte.

2. Définissez l'URL de rappel dans la console RML.

   - Pour le centre de données des Etats-Unis : https://smsin-us.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=RML
   - Pour le centre de données de l'UE : https://smsin-eu.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=RML

   Note: Une fois que le compte est configuré dans Deliver, la valeur <account> dans l'URL ci-dessus doit être remplacée par le nom du compte fourni par l'équipe de mise à disposition de Deliver.

Configuration de compte RML WhatsApp

About this task

Les clients qui sont mis à disposition à l'aide de la fonction WhatsApp (fournie par RML) doivent effectuer les étapes suivantes pour la configuration.

1. Créez une configuration de compte Facebook Business Manager vérifiée pour WhatsApp. L'équipe RML va guider les clients afin de configurer le compte Facebook Business Manager selon les besoins.
2. Créez un compte WhatsApp avec RML. RML va créer ce compte une fois que la vérification du compte Facebook Business Manager sera terminée.
3. Créez des modèles de message approuvés par WhatsApp. L'équipe RML va travailler avec les clients afin de préparer des modèles de message au format requis et de les faire approuver par le client.
4. Une fois que RML fournit des modèles approuvés aux clients, ils doivent les charger dans l'éditeur de message Deliver à l'aide de la nouvelle option de menu de contenu **Nouveau > WhatsApp**. Tous les détails doivent être fournis exactement en fonction du modèle approuvé, car WhatsApp ne permet pas de modifier l'approbation de publication de modèle.
5. Configurez une URL de rappel dans le compte RML WhatsApp. Pour cela, vous devez fournir l'URL ci-dessous à RML afin de pouvoir la configurer en tant qu'URL de rappel pour les rapports de distribution des messages WhatsApp.

https://smsin-us.unicadeliver.com/deliversmsib/wa/<account>

Configuration du compte SMS Twilio

About this task

Le compte SMS Twilio du client doit disposer des configurations suivantes pour fonctionner avec Deliver.

1. Connectez-vous à la console Twilio (https://www.twilio.com/console) et créez un projet pour SMS. Copiez SID DE COMPTE et JETON D'AUTHENTIFICATION pour ce projet.
2. Créez un ID de service de messagerie pour ce compte à l'adresse l'https://www.twilio.com/console/sms/services et copiez son ID de service de messagerie pour une utilisation ultérieure.
3. Travaillez avec l'équipe d'intégration Twilio pour mettre à niveau le compte afin de garantir l'envoi de SMS à n'importe quel numéro de mobile. Les comptes d'essai doivent mettre un numéro sur liste blanche avant de pouvoir lui envoyer des SMS.

Index