# Unica Deliver V12.1.3 Start- und Administratorhandbuch

# Contents

# Kapitel 1. Hosted Messaging mit Unica Campaign und Unica Deliver

Wenn Unica Campaign in Unica Deliver integriert wird, können Sie Deliver verwenden, um hochgradig personalisierte Digital-Marketingkampagnen durchzuführen.

**Anmerkung:** Deliver unterstützt die folgenden Kanäle zusammen mit E-Mail. In diesem Handbuch bezieht sich der Begriff Nachricht auf alle Kanäle.

- SMS
- WhatsApp
- Push-Operation

Deliver bietet Zugriff auf Ressourcen, die von Unica gehostet werden, sodass Sie individuell angepasste Nachrichten entwerfen, senden und überwachen können, die auf den in Ihrem Kunden-Datamart gespeicherten Informationen basieren.

- In Campaign können Sie Ablaufdiagramme verwenden, um Listen von Nachrichtenempfängern zu erstellen und Personalisierungsdaten für jeden Empfänger auszuwählen.
- In Deliver können Sie durch HCL gehostete Ressourcen für E-Mail-Design, -Übertragung und -Zustellung verwenden, um E-Mail-Marketingkampagnen durchzuführen.

## Einrichtung eines gehosteten Kontos mit Unica

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

Sie müssen über ein gültiges Konto verfügen, um auf die Nachrichtenressourcen zugreifen zu können, die Unica als Software-Service zur Verfügung stellt. Wenn Ihre HCL Unica Installation mehrere Partitionen umfasst und Sie Nachrichten in mehr als einer Partition verwenden möchten, benötigen Sie ein gehostetes Konto und mindestens einen Dienstanbieter für SMS, Push und Whatsapp, je nachdem, welche Dienste Sie für jede Partition benötigen. Sie können keine Konten über Installationen oder Partitionen gemeinsam nutzen.

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

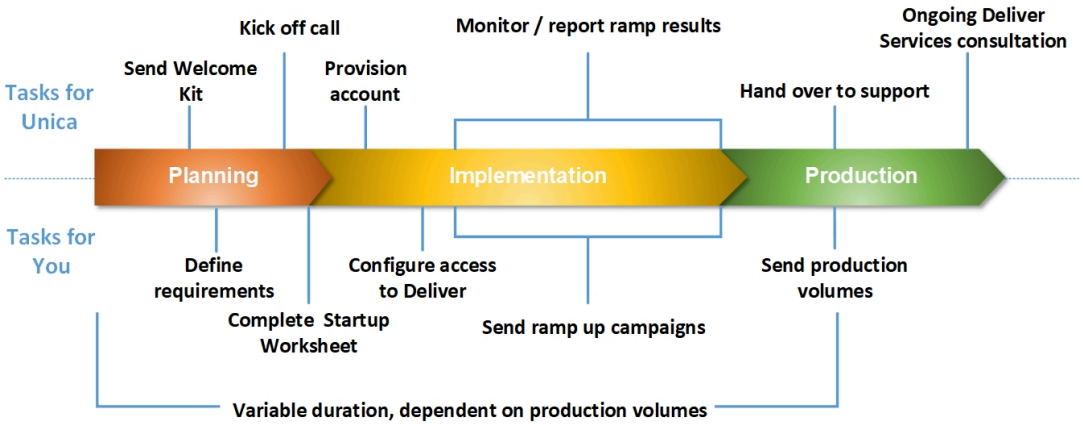
### Gesamtübersicht über den Startprozess

Sie können Nachrichtenfunktionen in Unica Campaign aktivieren, um zielgerichtete und nachverfolgbare digitale Marketingkampagnen durchzuführen. Campaign verwendet Nachrichtenfunktionen, die von Unica Deliver über

Ressourcen bereitgestellt werden, die in Rechenzentren in den USA, Indien und in Europa gehostet werden. Ein Konto für den Zugriff auf diese E-Mail-Ressourcen ist in Ihrem Deliver Abonnement enthalten. Sie können sich je nach den Anforderungen auch für die WhatsApp-, Push- oder SMS-Kanäle entscheiden.

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

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




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

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

## Startup-Aktivitäten und Meilensteine

### Planung

**Eine Auflistung der Planungsaktivitäten**

| Was geschieht? | Wer ist verantwortlich? |
|---|---|
| Senden Sie die Berechtigungsnachweise für das E-Mail-Konto und das Begrüßungskit, einschließlich des E-Mail-Startup-Arbeitsblatts. | Unica Deliver-Dienste |

| Was geschieht? | Wer ist verantwortlich? |
|---|---|
| Planen Sie eine Telefonkonferenz, um alle beteiligten Parteien einzuführen, den Startzeitplan zu überprüfen und die Ziele des E-Mail-Marketings zu verstehen. | Unica Professionelle Services |
| Füllen Sie das Arbeitsblatt E-Mail-Startup aus, um Ihre E-Mail-Domänenanforderungen und Mailingprognosen anzugeben. | Ihre Organisation |

## Bauen Sie Ihre E-Mail-Reputation auf

**Erforderliche Aktionen zur Etablierung eines günstigen Rufes für die E-Mail**

| Was geschieht? | Wer ist verantwortlich? |
|---|---|
| Stellen Sie das E-Mail-Konto unter Verwendung der Informationen bereit, die während der Telefonkonferenz und im Arbeitsblatt E-Mail-Startup bereitgestellt wurden. | Unica E-Mail-Operationen |
| Beginnen Sie die Erstellung von Mailings auf ausgewählte Testkonten mit wichtigen ISPs. Für diese Phasen sind etwa 30 Tage erforderlich. | Unica E-Mail-Operationen |
| Aktivieren Sie Deliver in Unica Campaign. | Ihr Unternehmen (mit der Unterstützung von Unica ) |
| Konfigurieren Sie den Zugriff auf gehostete-Mailressourcen. Informieren Sie sich beim EAS Consultant darüber, welches Rechenzentrum angegeben werden soll. | Ihr Unternehmen (mit der Unterstützung von Unica ) |
| Beginnen Sie mit dem Versand von Mailings. Um sich eine günstige E-Mail-Reputation aufzubauen, senden Sie zunächst kleine Mailings, gefolgt von größeren und häufigeren Mailings im Laufe der Zeit. ISPs versuchen oft, Spam zu begrenzen, indem große oder häufige Mailings von E-Mail-Domänen, die sie nicht als legitim erkennen, blockiert werden. | Ihr Unternehmen (mit der Unterstützung von Unica ) |
| Geben Sie die Zustellbarkeitsergebnisse und Hinweise zur Reputation an, während das Volumen und die Häufigkeit der Mailings allmählich zunehmen. | Unica Deliver-Dienste |

## Produktion

**Erforderliche Aktivitäten, um die gewünschten Produktionsmengen zu erreichen und zu pflegen**

| Was geschieht? | Wer ist verantwortlich? |
|---|---|
| Senden Sie Mailings mit typischem Volumen und Häufigkeit. | Ihre Organisation |
| Übertragen Sie die Verantwortung für Primärkontakt an das Unica Support-Team. | Unica Professionelle Services |
| Behalten Sie das Engagement für Konsultationen zu E-Mail-Fragen bei. Nehmen Sie regelmäßig Kontakt auf, um den E-Mail-Konto-Support fortzusetzen. | Unica Deliver-Dienste |

# Bevor Sie beginnen, Deliver

Bevor Sie mit dem Start des Messaging beginnen, sollten Sie die folgenden Punkte beachten.

- Bei einigen Konfigurationen ist ein Neustart des Anwendungsserver erforderlich. Planen Sie die Deliver-Konfigurationsaktivität, um zu vermeiden, dass große Flussdiagrammläufe und andere Aktivitäten in Campaign gestört werden.
- Unica fordert Sie auf, eine Person zu benennen, die während des Startvorgangs als primärer Kontaktpunkt dient.
- Fordern Sie die Anmeldeinformationen des gehosteten E-Mail-Kontos an, bevor Sie mit dem Startvorgang beginnen. Mit diesen Anmeldeinformationen konfigurieren Sie Ihre Systeme für den Zugriff auf das Konto.
- Informieren Sie sich bei Ihrem Netzverwaltungspersonal. Deliver erfordert bei der Kommunikation mit HCL Unica bestimmte Portbereiche.
- Bestätigen Sie, dass Sie über die entsprechenden Netzberechtigungen verfügen, um Konfigurationsänderungen vorzunehmen.

# Kapitel 2. Konfigurieren der lokalen HCL Unica Umgebung für Deliver

Die Verwendung von Deliver zum Senden der Nachrichten erfordert Änderungen in der lokalen Installation von HCL Unica. Führen Sie die in den folgenden Abschnitten beschriebenen Schritte aus.



Wenn Ihre Umgebung mehrere Partitionen enthält, wiederholen Sie diese Schritte für jede Campaign-Partition, in der Sie Unica Deliver verwenden. Weitere Informationen zum Erstellen und Arbeiten mit mehreren Partitionen finden Sie im Unica CampaignInstallationshandbuch.

## Bestätigung der Deliver-Registrierung

Unica Deliver muss bei Unica Platform registriert sein. Um zu bestätigen, dass Deliver erfolgreich registriert wurde, müssen Sie die Konfiguration für Platform überprüfen.

1. Melden Sie sich bei HCL Unica an.
2. Navigieren Sie zu **Einstellungen** > **Konfiguration**.
3. Suchen Sie nach der Konfigurationskategorie Deliver.

   Unica Deliver ist bei Platform registriert, wenn die Deliver Kategorie in der Hierarchie der Konfigurationseigenschaften angezeigt wird.

Wenn die Deliver Kategorie nicht in der Eigenschaftenhierarchie angezeigt wird, finden Sie im Unica Campaign Installationshandbuch Informationen zur manuellen Registrierung von Deliver.

Wenn die Deliver Kategorie verfügbar ist, müssen Sie die Deliver -Funktion in Campaign aktivieren.

### Deliver manuell registrieren

Falls das Installationsprogramm von Deliver während des Installationsprozesses nicht auf die Platform-Systemtabellen zugreifen kann, müssen Sie das Dienstprogramm configTool ausführen, um die Registrierung manuell durchzuführen.

Das Installationsprogramm von Campaign registriert Deliver normalerweise automatisch zusammen mit den Platform-Systemtabellen, ohne dass Deliver aktiviert wird. In einigen Situationen stellt das Campaign-Installationsprogramm keine Verbindung zu den Platform-Systemtabellen her, um Deliver automatisch zu registrieren.

Wenn das Installationsprogramm Deliver nicht automatisch registriert, müssen Sie Deliver manuell mit dem Dienstprogramm `configToolG`registrieren, das mit der Installation von HCL Unica bereitgestellt wird. Das Dienstprogramm `configTool` befindet sich im Verzeichnis `tools\bin` Ihrer Platform-Installation.

Verwenden Sie zum manuellen Registrieren von Deliver den folgenden Befehl, um das Dienstprogramm `configTool` auszuführen:

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

Das Deliver-Installationsverzeichnis ist ein Unterverzeichnis des Campaign-Installationsverzeichnisses.

# Lieferfunktionen in Campaign aktivieren

Wenn Sie Campaign installieren, wird das Installationsprogramm auch Deliver in der Standardpartitionspartition installiert, aber nicht aktiviert. Die Deliver Funktion ist erst verfügbar, wenn Sie Deliver aktivieren.

Sie aktivieren Deliver mit der folgenden Konfigurationseigenschaft in Unica Platform.

`Campaign > Partitionen > Partition[n] > Server > intern > deliverInstalled`

Ändern Sie den Wert in `Ja`, um zu Deliver aktivieren.

**Registrierungsanforderungen**

Die Registrierung von Deliver bei Unica Platform ist für die Bedienung von Deliver erforderlich. Bei der Installation von Unica Campaign können Sie Deliver bei Platform anmelden.

Bestätigen Sie nach dem aktivieren Deliver , dass Deliver ordnungsgemäß bei registriert ist Unica Platform . Details hierzu finden Sie unter Bestätigung der Deliver-Registrierung (auf Seite 10).

# DeliverMenüoptionen anzeigen

Um Unica Deliver zu verwenden, müssen Sie die Systemkonfiguration aktualisieren, damit die Menüoptionen für Deliver in der Unica Platform-Oberfläche angezeigt werden. Wenn Sie Campaign installieren, installiert das Installationsprogramm auch die Option „Menüs“ in der Standardpartitionspartition. Falls das Campaign-Installationsprogramm keine Verbindung zu den Platform-Systemtabellen herstellt, müssen Sie diese mithilfe der folgenden Schritte manuell konfigurieren. Verwenden Sie zum Anzeigen der erforderlichen Optionen das Dienstprogramm `configTool` , das mit Ihrer HCL Unica -Installation geliefert wird.

Für jede Deliver-Menüoption müssen Sie `configTool` mit bestimmten Parametern ausführen. Die Systemkonfigurationseinstellungen werden von `configTool` aktualisiert. Sie müssen den Webanwendungsserver neu starten, um die Änderungen zu übernehmen. Obwohl Deliver mit Campaign installiert ist, werden Menüoptionen für Deliver nicht angezeigt, nachdem Sie `configTool` ausgeführt und den Anwendungsserver erneut gestartet haben. Im `Tools` -Verzeichnis der Platform -Installation befindet sich das Dienstprogramm `configTool` im Ordner `bin` .

**Anmerkung:** Sie müssen einen Pfad zum Deliver Installationsverzeichnis als `configTool` -Parameter angeben. Das Deliver-Installationsverzeichnis ist ein Unterverzeichnis des Campaign-Installationsverzeichnisses.

- So zeigen Sie **Deliver Einstellungen** im Menü **Einstellungen** an.

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

- So zeigen Sie **Deliver Mailings** im Menü **Campaign** an.

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

- So zeigen Sie **Quick Builder** im **Campaign**-Menü an

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

- So zeigen Sie im Menü **DeliverCampaign Dokumente** an.

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

- So zeigen Sie **Deliver Analysen** im Menü **Analyse** an.

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

Um zu überprüfen, ob Sie die Menüoptionen erfolgreich hinzugefügt haben, melden Sie sich bei einem Neustart der Anwendungsserver bei an HCL Unica und öffnen Sie die Menüs **Einstellungen**, **Campaign**und **Analysen** , um zu überprüfen, ob die Deliver -Optionsoptionen angezeigt werden.

## Eigenschaften von Deliver-Systemtabellen angeben

Unica Deliver erfordert Informationen, die den Typ, das Schema und die JDBC-Verbindung für die Deliver Systemtabellen in Ihrer Installation beschreiben. Die Deliver-Systemtabellen werden im Rahmen des Campaign-Installationsprozesses im Campaign-Schema erstellt.

- Navigieren Sie zu **Einstellungen > Konfiguration > Bereitstellungspartitionen > Partition > [n] > Datenquellen > Systemtabellen**.
- Lesen und aktualisieren Sie die Informationen für die folgenden Parameter.

**Anmerkung:** Die Informationen zur Campaign-Systemtabelle werden hier erwartet.

Datenbanktyp

Schemaname

jdbcBatchSize

jdbcClassName

jdbcURI

ASMDataSourceFordbBerechtigungsnachweise-muss UA_SYSTEM_TABLES sein

- Geben Sie die erforderlichen Informationen in den folgenden Konfigurationseigenschaften an. Ausführliche Informationen zur Einstellung der Konfigurationseigenschaften finden Sie in der Platform-Onlinehilfe zu den einzelnen Eigenschaften.
    - `Deliver > Partitionen > Partition [n] < dataSources > Systemtabellen > type`
    - `Deliver > Partitionen > Partition [n] < dataSources > Systemtabellen > type`
    - `Deliver > Partitionen > Partition [n] < dataSources > Systemtabellen > jdbcBatchSize`
    - `Deliver > Partitionen > Partition [n] < dataSources > Systemtabellen > type`
    - `Deliver > Partitionen > Partition [n] < dataSources > Systemtabellen > type`

Weitere Informationen zu Konfigurationseigenschaften und zur Konfiguration von Deliver finden Sie unter Konfigurationen für Unica Deliver (auf Seite 45).

# Zugriff auf lokale Deliver Systemtabellen konfigurieren

Unica Deliver erfordert Zugriff auf die DeliverSystemtabellen im CampaignSchema. Damit Unica Deliver-Komponenten auf Systemtabellen im Kampagnenschema zugreifen können, ohne eine manuelle Datenbankanmeldung anzufordern, müssen Sie einen Deliver-Systembenutzer angeben, der die erforderlichen Anmeldeinformationen für den Datenbankzugriff bereitstellt.

Der Systembenutzer, der auf die Datenbank zugreift, ist einer Unica Platform Datenquelle zugeordnet, die die Anmeldeberechtigungsnachweise für die Datenbank enthält, die das Campaign Schema hostet.

Weitere Informationen zu den Konfigurationseigenschaften der Systemtabelle finden Sie unter Deliver | partitions | partition[n] | dataSources | systemTables (auf Seite 61).

1. Geben Sie den Systembenutzer an, den Sie in Unica Platform definiert haben. Bearbeiten Sie , um die folgende Konfigurationseigenschaft festzulegen:

   `Deliver > Partitionen > Partition [n] < dataSources > systemTables > asmUserForDBCredentials`

2. Geben Sie die Anmeldeinformationen für die Datenbank an, die das Campaign.Schema und die Deliver-Systemtabellen enthält. Bearbeiten Sie , um die folgende Konfigurationseigenschaft festzulegen:

   `Deliver > Partitionen > Partition [n] < dataSources > Systemtabellen > amDataSourceForDBCredentials`

# Erforderliche Zuordnung für Deliver -Systemtabellen in Campaign

Sie müssen Deliver Systemtabellen im Campaign Schema entsprechend den Deliver Datenbanktabellen zuordnen. Die Deliver -Systemtabellen haben **Deliver** den Tabellennamen.

Ordnen Sie in Campaign die folgenden Deliver-Systemtabellen zu.

- Deliver Ausgabelistentabelle.
- Deliver Ausgabeliste-Zielgruppenfeld-Zuordnungstabelle
- Deliver Mailingtabelle
- Deliver Mailinginstanztabelle
- Deliver Datentabellenspalten-Zuordnungstabelle
- Deliver Personalisierungsfeld-Zuordnungstabelle
- Deliver Personalisierungsfeld-Nutzungstabelle

Informationen zum Zuordnen von Tabellen finden Sie im Unica Campaign-Administratorhandbuch.

## Erforderlicher Neustart des Webanwendungsservers für Campaign

Nachdem Sie Änderungen an den Campaign- und Deliver-Konfigurationen vorgenommen haben, müssen Sie den Webanwendungsserver neu starten, auf dem Campaign gehostet wird.

Anweisungen zum Neustart finden Sie in der Dokumentation Ihres Webanwendungsservers.

# Chapter 3. Verbindungen zu Nachrichtendiensten

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

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

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

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

## Voraussetzungen für die Konfiguration der Verbindung zu HCL Unica gehosteten Services

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

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

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

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

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

# Konfiguration von Adressen für die Verbindung zu HCL Unica gehosteten Diensten

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

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

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

- `Deliver > serverComponentsAndLocations > hostedServices> uiHostName`

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

  Um eine Verbindung zum europäischen UnicaRechenzentrum herzustellen, ändern Sie diesen Wert in `em-eu.unicadeliver.com`.

  Um eine Verbindung zu dem Unica Rechenzentrum in Indien herzustellen, ändern Sie diesen Wert in `em-in.unicadeliver.com`

- `Deliver > serverComponentsAndLocations > hostedServices> dataHostName`

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

  Um eine Verbindung zum europäischen UnicaRechenzentrum herzustellen, ändern Sie diesen Wert in `em-eu.unicadeliver.com`.

  Um eine Verbindung zu dem Unica Rechenzentrum in Indien herzustellen, ändern Sie diesen Wert in `em-in.unicadeliver.com`

- `Deliver > serverComponentsAndLocations > hostedServices> ftpHostName`

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

  Um eine Verbindung zum europäischen UnicaRechenzentrum herzustellen, ändern Sie diesen Wert in `ftp-eu.unicadeliver.com`.

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

`ftp-in.unicadeliver.com`

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

# IP-Adresse der Hostnamen von Deliver

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

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

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

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

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

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

`ftp-in.unicadeliver.com: 192.175.4.236`

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

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

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

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

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

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

## Anforderungen bezüglich der Verbindung und des Ports

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

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

**HTTPS**: port 443

**SFTP port**: port 2222

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

## IP auf Whitelist setzen

Um die Empfängerliste (OLT) auf den FTP Deliver-Server hochzuladen, muss die externe IP des Servers, auf dem Campaign Web ausgeführt wird, auf der Serverseite von Deliver On Demand in die Whitelist aufgenommen werden.

Sie müssen die externe IP mit den folgenden Befehlen abrufen und dem Onboarding-Team zur Verfügung stellen. Das Onboarding-Team fordert Sie auf, die IP-Adresse auf die Whitelist zu setzen, damit FTP-Anforderungen von Ihrem Server an den FTP Deliver-Server zulässig sind.

- Führen Sie auf einem Unix-System den `curl ifconfig.me`-Befehl aus, um die externe IP Ihres Servers abzurufen.
- Auf Windows-System können Sie auf `http://ifconfig.me` zugreifen, um die externe IP Ihres Servers zu erhalten.

## Upload Verbindung über SFTP

Der Recipient List Uploader (RLU) verwendet das SFTP Protokoll als bevorzugten Mechanismus zum sicheren Hochladen von Empfängerlisten. Die RLU stellt eine Verbindung mit den von HCL Unica gehosteten Services über SFTP Port 2222 her. Über die sichere Verbindung handelt RLU die Authentifizierungsdetails mit dem SFTP Server aus und lädt die Empfängerliste hoch, sobald die Authentifizierung erfolgreich ist.

Das folgende Diagramm veranschaulicht diese Methode, um die Empfängerdaten von Campaign zu den HCL Unica gehosteten Services hochzuladen.

Auf der Konfigurationsseite können Sie die SFTP Option unter ftpProtocol (serverComponentsAndLocations -> hostedServices) anzeigen.

Die RLU stellt eine Verbindung zum SFTP Server her und lädt die Empfängerliste auf den SFTP Server hoch. Eine auf einem Zertifikat basierende Autorisierung wird für die Verbindung zum Autorisierungsserver verwendet. Der in der PEM Datei konfigurierte private SSH Schlüssel und der in der Datei known_hosts konfigurierte SSH RSA Fingerabdruck wird zur Verbindung mit dem SFTP Server verwendet. Die Kunden müssen eine separate PEM Datei pro Deliver Konto konfigurieren, damit sie für jede Deliver Partition separat konfiguriert werden kann. Zusätzlich zur PEM Datei benötigt RLU die Datei known_hosts, die den Fingerabdruck des SSH Servers enthält. Diese wird global unter dem folgenden Pfad `Affinium|Deliver|serverComponentsAndLocations|hostedServices` konfiguriert zusammen

mit einem Flag, um zu steuern, ob RLU einen vorkonfigurierten SSH Server Fingerabdruck in der Datei known_hosts benötigt.

Sobald die Authentifizierung erfolgt ist, werden die Empfängerlisten über SFTP hochgeladen, und es gibt keine Auswirkungen auf die Ausführung des Deliver Prozessfelds, von der aus dies ausgelöst wird.

Falls öffentliche oder private Schlüssel mit `passPhrase` generiert werden, erstellen Sie eine neue Datenquelle mit dem Namen "`SFTP_PASSPHRASE_DATASOURCE`" unter dem bei "`amUserForAcctCredentials`" angegebenen Platform-Benutzer. Beispiel: asm_admin und geben Sie dasselbe Passwort oder dieselbe `Passphrase` für diese Datenquelle an, die Sie bei der Generierung öffentlicher oder privater Schlüssel verwendet haben. Die Anmeldung der Datenquelle kann als beliebiger Text angegeben werden.

Wenn öffentliche oder private Schlüssel nicht mit `passPhrase` generiert werden, darf die Datenquelle nicht erstellt werden.

Führen Sie die folgenden Schritte aus, um die Schlüssel zu generieren.

Schritte zur Generierung von öffentlichen/privaten Schlüsselpaaren für die SFTP Authentifizierung.

1. Erstellen Sie das Schlüsselpaar

   Der erste Schritt ist die Erstellung eines Schlüsselpaares auf dem Computer, auf dem Campaign Web installiert ist. Melden Sie sich bei dem Computer an, auf dem Campaign Web installiert ist. Öffnen Sie die Eingabeaufforderung und führen Sie den folgenden Befehl aus.

   ```
   ssh-keygen
   ```

2. Geben Sie den Speicherort für die Schlüssel an.

   Sie können hier die EINGABETASTE drücken, um die Dateien am Standardspeicherort im .ssh Verzeichnis Ihres Home Verzeichnisses zu speichern. Alternativ können Sie einen anderen Dateinamen oder Speicherort auswählen, indem Sie ihn nach der Eingabeaufforderung eingeben und die EINGABETASTE drücken.

3. Erstellen Sie eine Passphrase.

   Sie werden von der zweiten und letzten Eingabeaufforderung von ssh-keygen erfordert, eine Passphrase einzugeben. Die Verwendung von einer Passphrase hängt von Ihren Anforderungen ab.

   Beispiel:

   ```
   [root@Host bin]# ssh-keygen Generierung von einem öffentlichen/privaten RSA Schlüsselpaars.
    Geben Sie die Datei ein, in der der Schlüssel gespeichert werden soll (/root/.ssh/id_rsa):
    Geben Sie eine Passphrase ein (leer für keine Passphrase): Geben Sie dieselbe Passphrase
    erneut ein: Ihre Identifikationsdaten werden in /root/.ssh/id_rsa gespeichert. Ihr öffentlicher
    Schlüssel wird in /root/.ssh/id_rsa.pub gespeichert. Der Fingerabdruck des Schlüssels lautet:
    61:ca:14:c2:7a:71:e2:aa:bd:2e:ff:25:b8:b1:fd:ac root@Host The following is the key's randomart
    image. .. . +... o +. o . oo o . o o S .. oo . . o .= + +*oEoo [root@Host bin]#
   ```

Ihr öffentlicher Schlüssel wird in `- /root/.ssh/id_rsa.pub` gespeichert. Zur Konfiguration, senden Sie den generierten öffentlichen Schlüssel über den HCL Support an das Deliver Dev Ops Team.

## Konfiguration von SFTP

Führen Sie die folgenden Schritte aus, um SFTP zu konfigurieren.

1. Führen Sie den folgenden Befehl aus, indem Sie an der Eingabeaufforderung zu `<Deliver_Home>/tools` navigieren, um die Eigenschaft ftpProtocol auf der Benutzeroberfläche anzuzeigen.

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

2. Melden Sie sich bei Platform an und navigieren Sie zu **Einstellungen > Konfiguration** und wählen Sie **SFTP** für ftpProtocol unter `Affinium|Deliver|serverComponentsAndLocations|hostedServices`.
3. Führen Sie den folgenden Befehl aus, indem Sie an der Eingabeaufforderung zu `<Deliver_Home>/tools` navigieren, um die Eigenschaft ftpPort auf der Benutzeroberfläche anzuzeigen.

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

4. Geben Sie die Portnummer `2222` für ftpPort bei `Affinium|Deliver|serverComponentsAndLocations|hostedServices` an.
5. Setzen Sie den Wert für `enforceKnownHostsValidation` auf `false` und aktualisieren Sie den Pfad als `<Deliver_HOME>/Conf/known_hosts` für die Eigenschaft `knowHostsPath`.

   Z.B.: `knowHostsPath - /opt/HCL/Campaign/Deliver/conf/known_hosts`

   `enforceKnownHostsValidation - False`

6. Diese Angabe ist optional. Falls Sie über die Datei known_hosts verfügen, aktualisieren Sie deren vollständigen Pfad für die Eigenschaft `knowHostsPath` unter `Affinium|Deliver|serverComponentsAndLocations|hostedServices` und setzen Sie `enforceKnownHostsValidation` auf `true`.
7. Kopieren Sie die private Zertifikatsdatei (id_rsa) nach `<DELIVER_HOME>/conf` und aktualisieren Sie den vollständigen Pfad für diese private Zertifikatsdatei in der Eigenschaft `pemFilePath` unter `Affinium|Deliver|partitions|partition1|hostedAccountInfo`.

   Beispiel:

   pemFilePath – `/opt/HCL/Campaign/Deliver/conf/id_rsa`

   amDataSourceForSftpPassPhrase-- `SFTP_PASSPHRASE_DATASOURCE`

8. Falls Sie bei der Generierung von öffentlicher/privater Schlüssel eine Passphrase angegeben haben, erstellen Sie eine Datenquelle mit dem Namen `SFTP_PASSPHRASE_DATASOURCE` unter dem unter `amUserForAcctCredentials` angegebenen Platform-Benutzer (Beispiel: asm_admin) und geben Sie dasselbe Passwort / dieselbe

Passphrase für diese Datenquelle an, die Sie bei der Generierung öffentlicher/privater Schlüssel verwendet haben. Die Anmeldung an die Datenquelle kann als beliebiger Text angegeben werden.

9. Falls Sie bei der Generierung öffentlicher/privater Schlüssel keine Passphrase angegeben haben, müssen Sie diese Datenquelle `SFTP_PASSPHRASE_DATASOURCE` nicht für den Benutzer asm_admin oder einen anderen Benutzer erstellen.
10. Starten Sie den App Server für Campaign neu.
11. Öffnen Sie die Eingabeaufforderung, navigieren Sie zu `<Deliver_home>/bin` und testen Sie die SFTP Verbindung mit rlu wie folgt.

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

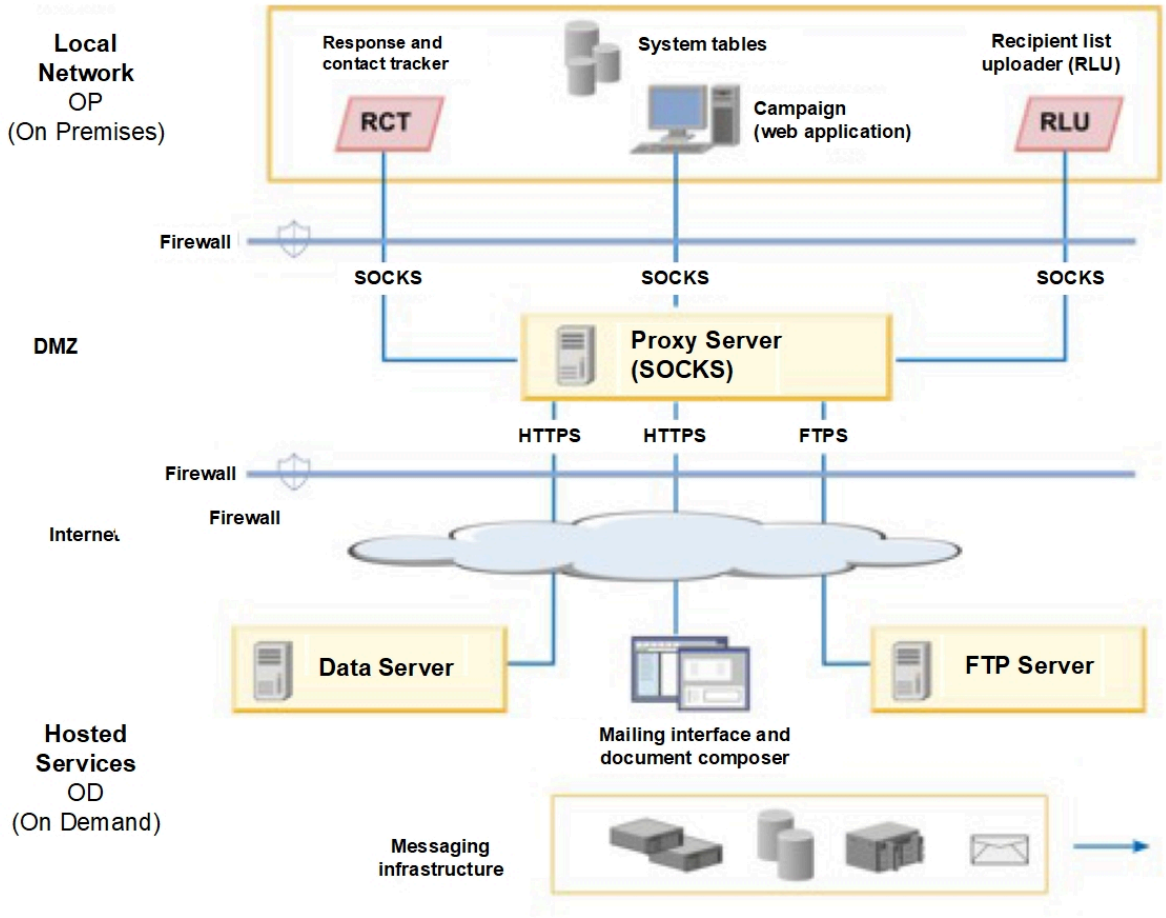
**Note:** Alle oben angegebenen Dateipfade müssen einschließlich des Dateinamens vollständig sein. Wiederholen Sie die Schritte 7 bis 9 für alle Partitionen, in denen Deliver konfiguriert ist.

## Verbindung über einen HTTP Proxy

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

Deliver unterstützt SOCKS Protokoll Version 5.

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




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

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

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

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

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

**RLU- und Webserver-Konfigurationen für SFTP.**

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

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

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

Hostname und IP Adressen für das US Rechenzentrum:

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

ftp-em.unicadeliver.com
```

Hostname und IP Adressen für das europäische Rechenzentrum:

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

ftp-eu.unicadeliver.com
```

Hostname und IP-Adressen für das Rechenzentrum Indien:

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

ftp-in.unicadeliver.com
```

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

**Konfigurationseinstellungen für den HTTPS zu SOCKS-Proxy**

| Einstellung | Beschreibung |
|---|---|
| `-Dhcl.unica.deliver.https.proxy.host=<socksHost>` | Hostname oder IP des SOCKS Proxys |
| `-Dhcl.unica.deliver.https.proxy.port=<socksPort>` | Der Port, auf dem der SOCKS Proxy ausgeführt wird |
| `-Dhcl.unica.deliver.https.proxy.type=SOCKS` | Der Typ des Proxy Servers. Sie müssen einen SOCKS Proxyserver verwenden. |

## Konfiguration der Authentifizierung für den Zugriff auf einen SOCKS-Proxy

Wenn für Ihren SOCKS-Proxy eine Authentifizierung erforderlich ist, müssen Sie den Webanwendungsserver, die RLU und die RCT so konfigurieren, dass die Anmeldeinformationen für den Zugriff bereitgestellt werden.

Konfigurieren Sie Folgendes für den Webanwendungsserver, die RLU und den RC Die Werte für `Benutzername` und `Kennwort` müssen die Berechtigungsnachweise sein, die für die Authentifizierung mit dem Proxy erforderlich sind.

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

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

## Konfigurieren des RCT für die Verwendung eines SOCKS-Proxys

Sie müssen das RCT ändern, um über einen SOCKS-Proxyserver zu kommunizieren. Die erforderlichen Einstellungen hängen von Ihrem Betriebssystem ab.

- Fügen Sie für die RCT in Windows™-Umgebungen die folgenden Proxy-Argumente zu `common.bat` hinzu. Die Datei `Common.bat` befindet sich im Verzeichnis `\deliver\bin` Ihrer lokalen Deliver -Installation.

```
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_AUTH_USER>
-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_PASSWORD>
set RCT_JAVA_ARGS=%BASE_VM_ARGS% %RCT_MEM_ARGS%
%RCT_EXTRA_VM_ARGS% %RCT_PROXY_ARGS%
```

- Fügen Sie für die RCT in UNIX™-Umgebungen die folgenden Proxy-Argumente zu `common.sh` hinzu.
  Die `Common.sh` befindet sich im Verzeichnis `/Deliver/bin` Ihrer lokalen Deliver -Installation.

  **Anmerkung:** Ändern Sie nicht direkt `RLU.sh`, `RCT.sh`oder `setenv.sh`. Das System überschreibt die Änderungen.

```
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_AUTH_USER>
-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_PASSWORD>"
RCT_JAVA_ARGS="${BASE_VM_ARGS} ${RCT_MEM_ARGS} ${RCT_EXTRA_VM_ARGS} ${RCT_PROXY_ARGS}"
```

## Konfiguration von für die Verwendung eines SOCKS-Proxys

Sie müssen das RLU ändern, um die Kommunikation von RLU über einen SOCKS-Proxy Server zu ermöglichen. Die erforderlichen Einstellungen sind von Ihrem Betriebssystem abhängig.

- Für die RLU in Windows™ Umgebungen, fügen Sie die folgenden Proxy Argumente zu `common.bat` hinzu.
  Die Datei `common.bat` befindet sich im Verzeichnis `\deliver\bin` Ihrer lokalen Deliver Installation.

```
Setzen Sie 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= <kommagetrennte Liste von Hostnamen und IP-Adressen>

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

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

set RLU_JAVA_ARGS=%BASE_VM_ARGS% %RLU_MEM_ARGS% %RLU_EXTRA_VM_ARGS%

%RLU_PROXY_ARGS%
```

- Für die RLU in UNIX™ Umgebungen, fügen Sie die folgenden Proxy Argumente zu `common.sh` hinzu. Die Datei `common.sh` befindet sich im Verzeichnis `/deliver/bin` Ihrer lokalen Deliver Installation.

  **Note:** Ändern Sie `rlu.sh`, `rct.sh` oder `setenv.sh` nicht direkt. Das System überschreibt die Änderungen.

```
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= <kommagetrennte Liste von Hostnamen und IP-Adressen>

-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}"
```

## Konfiguration von dem Webanwendungsserver für die Verwendung eines SOCKS Proxys

Um eine Verbindung mit HCL Unica über einen SOCKS Proxy herzustellen, müssen Sie die Konfiguration des Webanwendungsservers ändern. Für Unica  WebSphere® Server, müssen Sie die generischen JVM Argumente ändern. Für Oracle Weblogic Server, müssen Sie das `SetDomainEnv` Skript ändern.

- Wenn Ihr Webanwendungsserver Unica  WebSphere® lautet, fügen Sie den generischen JVM Argumenten von WebSphere® Folgendes hinzu.

```
-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= <kommagetrennte Liste von Hostnamen und IP-Adressen>

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

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

- Wenn Ihr Webanwendungsserver Oracle Weblogic lautet, ändern Sie das `setDomainEnv` Skript. Die erforderlichen Einstellungen sind von Ihrem Betriebssystem abhängig.

  In den Windows™ Umgebungen, nehmen Sie die folgenden Änderungen vor:

```
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= <kommagetrennte Liste von Hostnamen und IP-Adressen>

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

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

  In den UNIX-™ Umgebungen, nehmen Sie die folgenden Änderungen vor:

```
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= <kommagetrennte Liste von Hostnamen und IP-Adressen>

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

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

## Daten-Download-Frequenz und Port-Einstellung

Im Rahmen Ihrer DeliverUnica -Installation wird eine Campaign-Komponente namens Response and Contact Tracker (RCT) installiert. Das RCT fordert regelmäßig E-Mail-Antworten und Verfolgungsdaten von HCL Unica an. Standardmäßig gibt das RCT alle 5 Minuten eine Datenanforderung aus.

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

## Konfigurieren eines Systembenutzers für den Zugriff auf HCL Unica Hosted Services

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

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

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

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

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

### Konfigurieren des Partitionszugriffs auf HCL Unica Hosted Services

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

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

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

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

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

## Konfigurieren des Systembenutzers, der auf HCL Unica gehostete Dienste zugreift

Deliver-Komponenten in Campaign müssen automatisch auf HCL Unica gehostete Dienste zugreifen können, ohne dass eine Anmeldung erforderlich ist. Systembenutzer, die in konfiguriert sind, Unica Platform können auf eine Datenquelle verweisen, die den erforderlichen Benutzernamen und das erforderliche Kennwort bereitstellt. Sie können die Datenquelle einem neuen Systembenutzer oder einem vorhandenen Systembenutzer hinzufügen. Um die Benutzerverwaltung zu vereinfachen, können Sie einen Systembenutzer aktualisieren, der bereits für den Zugriff auf das Campaign-Schema konfiguriert ist, sodass er auch auf HCL Unica gehostete Dienste zugreifen kann.

Um diese Aufgabe ausführen zu können, müssen Sie den Benutzernamen und das Kennwort der HCL Unica gehosteten Services kennen, die Unica Ihrem gehosteten E-Mail-Konto zugewiesen hat. Der Empfang des Benutzernamens und des Kennworts ist Teil des Benutzereinstellungsprozesses.

Sie müssen über die entsprechenden Zugriffsberechtigungen verfügen und wissen, wie Sie Systembenutzer und Datenquellen in Unica Platform erstellen können.

**Anmerkung:** Wenn Ihre Installation mehrere Partitionen enthält, müssen Sie diese Task für jede Partition ausführen. Sie können Systembenutzer nicht über Partitionen gemeinsam nutzen.

1. Erstellen Sie eine Platform Datenquellen, die den Benutzernamen und das Kennwort enthält, die für den Zugriff auf HCL Unica gehostete Services erforderlich sind. Um die besten Ergebnisse zu erzielen und die Wartung zu vereinfachen, benennen Sie diese Datenquellen UNICA_HOSTED_SERVICES. Konfigurieren Sie diese Datenquellen wie folgt.

   Geben Sie für die **Datenquellanmeldung** den Benutzernamen ein, den Sie von Unica während des Kontostarts erhalten haben.

   Geben Sie unter **Datenquellenkennwort** das Kennwort ein, das Sie beim Start des Kontos Unica erhalten haben.

2. Geben Sie die Datenquellen in der Deliver Konfiguration an. Verwenden Sie die Konfigurationseigenschaft **amDataSourceForAcctCredentials**

   Die Konfigurationseigenschaft ist bei `Deliver > Partitionen > Partition [n] > hosteRechnungstInfo > amDataSourceForAcctCredentials`.

   Standardmäßig ist die angegebene Datenquelle `UNICA_HOSTED_SERVICES`.

3. Geben Sie einen Systembenutzer für den Zugriff auf HCL Unica gehostete Services an. Sie können einen vorhandenen Benutzer angeben oder einen Benutzer erstellen. Verwenden Sie in der Deliver Konfiguration die Konfigurationseigenschaft **amUserForAcctCredentials**

   Die Konfigurationseigenschaft ist bei `Deliver > Partitionen > Partition[n] > hostedAccountInfo > amUserForAcctCredentials`.

   Standardmäßig ist der angegebene Benutzer `asm_admin`.

4. Fügen Sie die Datenquelle, die in Schritt 1 konfiguriert ist, dem in Schritt 3 angegebenen Systembenutzer hinzu.

Sie müssen den Webanwendungsserver erneut starten, damit die Änderungen wirksam werden.

# Konfigurieren einer sicheren Kommunikation für gehostete E-Mails

Die Kommunikation zwischen dem E-Mail-Vermarkter und HCL Unica gehosteten Diensten erfolgt über Secure Sockets Layer (SSL). Sie müssen die Konfiguration des Webanwendungsservers ändern, um SSL verwenden zu können. Um die erforderlichen Änderungen vorzunehmen, muss das Java™ Dienstprogramm `keytool` verwendet werden.

Das Konfigurieren der sicheren Kommunikation umfasst die folgenden Aktionen.

- Generieren Sie einen vertrauenswürdigen Schlüsselspeicher.
- Rufen Sie ein digitales Zertifikat von HCL Unica gehosteten Services ab.
- Fügen Sie den vertrauenswürdigen Schlüsselspeicher zum Webanwendungsserver hinzu.
- Importieren Sie das digitale Zertifikat für HCL Unica gehostete Dienste in den vertrauenswürdigen Schlüsselspeicher.

Die genauen Schritte und die Reihenfolge, die zum Konfigurieren von SSL erforderlich sind, hängen vom Typ und der Version des Webanwendungsservers (WebSphere®, WebLogic, Tomcat, JBOSS) ab, auf dem Sie Unica Platform und Unica Campaign bereitgestellt haben.

Für WebLogic siehe SSL bei Verwendung von WebLogic konfigurieren (auf Seite 32).

Für WebSphere® siehe SSL bei Verwendung von WebSphere konfigurieren (auf Seite 35).

## Generieren Sie einen vertrauenswürdigen Schlüsselspeicher.

Führen Sie die folgenden Schritte aus, um einen Identitätsschlüsselspeicher und einen vertrauenswürdigen Schlüsselspeicher für die Konfiguration von Unica Deliver für die Kommunikation mit HCL Unica gehosteten Diensten über SSL zu erstellen. Sie fügen die Schlüsselspeicher dem Webanwendungsserver hinzu, wenn Sie SSL konfigurieren.

In den in diesem Abschnitt enthaltenen Prozeduren werden die folgenden Beispielwerte von HCL verwendet.

- Identitätsschlüsselspeicher: `HCLUnicaClientIdentity.jks`
- Aliasname für den Identitätsschlüsselspeicher: `HCLUnicaClientIdentity`
- Passwort (`-storepass`) für den Identitätsschlüsselspeicher: `clientPwd`
- Der Sicherheitsschlüssel (`-keypass`) für den Identitätsschlüsselspeicher: `clientPwd`
- Zertifikat basierend auf dem Identitätsschlüsselspeicher: `ClientCertificate.cer`
- Vertrauenswürdiger Schlüsselspeicher: `HCLUnicaTrust.jks`
- Kennwörter (`-storePass`) für den vertrauenswürdigen Schlüsselspeicher: `-trustpwd`

Die tatsächlichen Werte, die Sie eingeben, müssen für Ihre Installation spezifisch sein.

Führen Sie das Java™ Dienstprogramm `KeyTool` in der Befehlszeile aus, um die Schritte in diesem Verfahren abzuschließen.

1. Erstellen Sie einen Identity-Keystore. Verwenden Sie den Befehl `genkey`, wie im folgenden Beispiel gezeigt.

   In diesem Beispiel wird ein Identitätsschlüsselspeicher mit dem Namen `HCLUnicaClientIdentity.jks` erstellt. Sie können einen anderen Namen für den von Ihnen erstellten Identitätsschlüsselspeicher verwenden.

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

   Beachten Sie Folgendes:

   - Sie verwenden die Werte für `Alias`, `Schlüsselspeicher`, `Keypass` und `Storepass` später in diesem Verfahren und bei der Konfiguration von SSL auf dem Webanwendungsserver.
   - Für WebSphere® müssen das`Schlüsselspeicher-Kennwort (-storePass`) und das Schlüssel-Kennwort (`-Tastenblock`) identisch sein.
   - Im definierten Namen (`-dname`) entspricht der allgemeine Name (`CN`) dem Hostnamen, der für den Zugriff auf HCL Unica gehostete Dienste verwendet wird. Wenn beispielsweise die URL

für HCL Unica gehostete Services `https://hostName.example.com:7002/unica/jsp`ist, ist die CN `HostName.example.com`. Der CN-Teil des definierten Namens ist der einzige erforderliche Teil; Organisation (`O`) und Organisationseinheit (`OU, Organization Unit`) sind nicht erforderlich.

2. Erstellen Sie ein Zertifikat auf Basis des erstellten Identitätsschlüsselspeicher. Verwenden Sie den Befehl `Export`, wie im folgenden Beispiel dargestellt.

   Das Beispiel generiert ein Zertifikat mit dem Namen `ClientCertificate.cer`. Sie können für das von Ihnen erstellte Zertifikat einen anderen Namen verwenden.

   Die Werte für `Keystore`, `Storepass` und `Alias` müssen mit den Werten übereinstimmen, die Sie für den Identitätsschlüsselspeicher angegeben haben.

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

3. Generieren Sie den vertrauenswürdigen Schlüsselspeicher. Verwenden Sie den Befehl `Import`, wie im folgenden Beispiel dargestellt.

   Das Beispiel generiert einen vertrauenswürdigen Schlüsselspeicher mit dem Namen `HCLUnicaTrust.jks`. Sie können einen anderen Namen für den von Ihnen erstellten vertrauenswürdigen Schlüsselspeicher verwenden.

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

   Geben Sie **Y** ein, wenn Sie aufgefordert werden, die Vertrauenswürdigkeit des Zertifikats zu bestätigen.

Beachten Sie die Werte, die Sie für die folgenden Variablen definiert haben. Ihre Werte können sich von den im Beispiel angegebenen Werten unterscheiden.

- `Aliasname` (im Beispiel: `HCLUnicaClientIdentity`)
- `Identitätsschlüsselspeicher` (im Beispiel: `HCLUnicaClientIdentity.jks`)
- `StorePass` (im Beispiel: `TrupPWD`) Der `Storepass` -Wert für den vertrauenswürdigen Schlüsselspeicher kann sich von dem Wert `Storepass` für den Identitätsschlüsselspeicherladen und das Zertifikat unterscheiden.
- `Schlüsselspeicher` (im Beispiel: `HCLUnicaTrust.jks`) Abhängig von Ihrem Anwendungsserver geben Sie auch den-Identität-Keystore an.

Sie legen diese installationsspezifischen Werte fest, wenn Sie SSL auf dem Anwendungsserver für Ihre HCL Unica -Installation konfigurieren.

## SSL bei Verwendung von WebLogic konfigurieren

In diesem Abschnitt werden die Schritte beschrieben, die zur Konfiguration von SSL erforderlich sind, wenn Sie HCL Unica Komponenten in Oracle WebLogic implementieren Diese Änderung ist erforderlich, damit Deliver-Komponenten, die in Campaign arbeiten, um mit den HCL Unica gehosteten Diensten über SSL zu kommunizieren.

Spezifische Anleitungen zur Navigation und zum Arbeiten mit der Oracle WebLogic-Benutzeroberfläche finden Sie in der Dokumentation der von Ihnen verwendeten Oracle WebLogic-Version.

Führen Sie die folgenden Tasks aus.

- Startscript für WebLogic ändern
- Ändern der WebLogic-Konfiguration
- Rufen Sie ein digitales Zertifikat von HCL Unica gehosteten Services ab.
- Erstellen Sie einen vertrauenswürdigen Schlüsselspeicher und importieren Sie das digitale Unica-Zertifikat

## Startscript für WebLogic ändern

Wenn Sie Campaign auf WebLogic implementiert haben, müssen Sie das Startscript für WebLogic und die Konfiguration von WebLogic für SSL ändern, damit WebLogic die sichere Kommunikation zwischen lokal installierten Deliver Komponenten und HCL Unica gehosteten Services erkennt und akzeptiert.

Fügen Sie dem JAVA_OPTIONS im Startscript von WebLogic die folgenden Argumente hinzu.

- `-Dweblogic.security.SSL.allowSmallRSAExponent=true`
- WebLogic Version 12C oder höher: `-Dweblogic.security.SSL.protocolVersion=TLS1`

  Alle vorherigen Versionen: `-Dweblogic.security.SSL.nojce=true`

## Ändern der WebLogic-Konfiguration

Sie müssen die SSL-Konfiguration in WebLogic ändern.

Verwenden Sie die WebLogic-Konsole, um die folgende Änderung in der WebLogic SSL-Konfiguration für Ihre Domäne vorzunehmen.

Ändern Sie die Einstellung zur **Überprüfung des Hostnamens** in `Keine`.

## Erhalten Sie ein Zertifikat von HCL Unica gehosteten Diensten

Um die SSL Kommunikation zu konfigurieren, müssen Sie ein digitales Zertifikat von HCL Unica herunterladen. Die Zertifikatdetails werden in einer Datei mit der Erweiterung `.cer` gespeichert, die Sie in den Schlüsselspeicher des Webanwendungsservers importieren können.

Nach Ablauf des vorhandenen SSL Zertifikat, verlieren Sie den Zugriff auf HCL Unica gehostete Dienste. Verwenden Sie dieses Verfahren, um ein neues Zertifikat herunterzuladen.

1. Melden Sie sich im Internet Explorer bei der Adresse für HCL Unica gehostete Dienste an, die für Ihr gehostetes E-Mail-Konto konfiguriert wurden.
   - Das US-Rechenzentrum finden Sie unter https://em.unicadeliver.com
   - Das europäische Rechenzentrum finden Sie unter https://em-eu.unicadeliver.com
   - Das Rechenzentrum von Indien finden Sie unter https://em-in.unicadeliver.com

   Der Anmeldeversuch führt zu einer fehlgeschlagenen Anmeldung, aber Sie können den Browser verwenden, um die Zertifikatsanforderung zu übermitteln.

2. Klicken Sie auf das Schlosssymbol und wählen Sie **Zertifikat anzeigen** aus.
3. Wählen Sie die Registerkarte Details und danach **In Datei kopieren** aus.

   Speichern Sie die Datei mit der Erweiterung `.cer` an einem Speicherort, auf den der Webanwendungsserver zugreifen kann. Die von Ihnen erstellte Datei ist das digitale Zertifikat, das Sie in den Schlüsselspeicher auf dem Webanwendungsserver einfügen.

   Speichern Sie das Zertifikat beispielsweise als `HCLHosted.cer`.

## Erstellen Sie einen vertrauenswürdigen Keystore für WebLogic und importieren Sie das Unica Zertifikat.

Für WebLogic müssen Sie einen vertrauenswürdigen Keystore erstellen, der das Unica Zertifikat akzeptiert.

Bevor Sie beginnen, verwenden Sie einen Web-Browser, um das HCL Unica digitale Zertifikat für gehostete Services herunterzuladen, und speichern Sie es als `.cer`-Datei. Das Zertifikat kann z. B. den Namen `HCLHosted.cer` haben (der Dateiname kann anders sein). Weitere Informationen finden Sie im Abschnitt Erhalten Sie ein Zertifikat von HCL Unica gehosteten Diensten (auf Seite 33).

In den in diesem Abschnitt enthaltenen Prozeduren werden die folgenden Beispielwerte von HCL verwendet.

- Identitätsschlüsselspeicher: `HCLUnicaClientIdentity.jks`
- Passwort für den Identitätsschlüsselspeicher: `clientPwd`
- Vertrauenswürdiger Schlüsselspeicher: `HCLUnicaTrust.jks`
- Passwort für den Identitätsschlüsselspeicher: `HCLUnicaHostedIdentity`
- Kennwörter (`-storePass`) für den vertrauenswürdigen Schlüsselspeicher: `trustPwd`
- Digitales Zertifikat (`-Datei`) von Unica: `HCLHosted.cer`

Die tatsächlichen Werte, die Sie eingeben, müssen für Ihre Installation spezifisch sein.

Führen Sie das Dienstprogramm Java™ `KeyTool` in der Befehlszeile aus, um die Schritte in diesem Verfahren abzuschließen.

1. Generieren Sie einen vertrauenswürdigen Schlüsselspeicher für WebLogic.
   Details hierzu finden Sie unter Generieren Sie einen vertrauenswürdigen Schlüsselspeicher. *(auf Seite 31)*.

   Sie geben das identity keystore und das trusted keystore in der WebLogic-Konfiguration an.

2. Verwenden Sie den Befehl `Import` im Dienstprogramm von `KeyTool` , um das Hosted HCL Unica Services Certificate zu dem Trusted Keystore hinzuzufügen, der in Schritt 1 erstellt wurde, wie im folgenden Beispiel dargestellt.
   Verwenden Sie das digitale Zertifikat, das Sie von Unica heruntergeladen haben.

   In diesem Verfahren definieren Sie auch einen Alias für den vertrauenswürdigen Schlüsselspeicher.

   ```
   KeyTool-Import- HCLUnicaHostedIdentity Alias/Datei < HCLHosted.cer >-Keystore <HCLUnicaTrust.jks>
   -StamePass <trustPwd>
   ```

Geben Sie **Y** ein, wenn Sie aufgefordert werden, die Vertrauenswürdigkeit des Zertifikats zu bestätigen.

3. Konfigurieren Sie in der WebLogic-Verwaltungskonsole die Schlüsselspeicher für den Server.

   Um die Konfigurationsregeln anzugeben, wählen Sie aus den verfügbaren Optionen die Option für benutzerdefinierte Identitäts- und benutzerdefinierte Vertrauensspeicher aus. Für die benutzerdefinierte Identität geben Sie den Identitätsschlüsselspeicher an. Für die benutzerdefinierte Vertrauensstellung geben Sie den vertrauenswürdigen Schlüsselspeicher an.

   Geben Sie beispielsweise in der Administrationskonsole Folgendes an (anhand der Beispielwerte aus dem vertrauenswürdigen Schlüsselspeicher, den Sie in Schritt 1 erstellt haben).

   - Für die **Identität**: Geben Sie den Identitätsschlüsselspeicher und das zugehörige Kennwort an.

     Z. B. die Option `HCLUnicaClientIdentity.jks` und `clientPwd`.

   - Für **Trust**: Geben Sie den vertrauenswürdigen Schlüsselspeicher und das zugehörige Kennwort an.

     Zum Beispiel `HCLUnicaTrust.jks` und `trustPwd`.

   Geben Sie den vollständigen Pfad zu beiden Schlüsselspeichern an.

4. Starten Sie WebLogic neu. WebLogic implementiert die Konfigurationsänderungen erst, wenn Sie den Webanwendungsserver neu starten.
5. Um die SSL-Verbindung zu testen, melden Sie sich bei Unica Campaign an und greifen Sie auf verschiedene Menüs für Nachrichtenfunktionen zu. Bestätigen Sie, dass Sie E-Mails, Landing-Pages und Mailings erstellen können.

## SSL bei Verwendung von WebSphere konfigurieren

In diesem Abschnitt werden die allgemeinen Schritte beschrieben, die zum Konfigurieren von SSL erforderlich sind, wenn Sie HCL Unica-Komponenten auf WebSphere® bereitgestellt haben. Diese Änderung ist erforderlich, damit Deliver-Komponenten, die in Campaign arbeiten, um mit den HCL Unica gehosteten Diensten über SSL zu kommunizieren.

Bevor Sie beginnen, müssen Sie den Wert für die Konfigurationseigenschaft `uihostNAME`kennen. Der Wert für `uihostNAME` ist die URL für HCL Unica gehostete Services. Details hierzu finden Sie unter Konfiguration von Adressen für die Verbindung zu HCL Unica gehosteten Diensten (auf Seite 16).

Sie müssen auf die WebSphere®-Sicherheitskonsole zugreifen, um die Einstellungen für die Verwaltung von SSL-Zertifikaten und Schlüsseln zu ändern. Diese Aufgabe erfordert einen Neustart des Campaign-Webanwendungsservers, um die Änderungen zu implementieren.

Wenn Sie Campaign auf WebSphere® bereitgestellt haben, müssen Sie die WebSphere®-Sicherheitskonfiguration ändern, um das Unterzeichnerzertifikat von HCL Unica abzurufen und dem WebSphere®-Vertrauensspeicher hinzuzufügen. Wenn Sie eine Fehlermeldung erhalten, die anzeigt, dass Ihr derzeitiges Unterzeichnerzertifikat abgelaufen ist, löschen Sie das vorhandene Zertifikat und fügen Sie ein neues ein.

Spezifische Anleitungen zur Navigation und zum Arbeiten mit der WebSphere® Benutzeroberfläche finden Sie in der Dokumentation der von Ihnen verwendeten Unica WebSphere® Version.

1. Generieren Sie einen vertrauenswürdigen Schlüsselspeicher.

   Weitere Informationen finden Sie im Abschnitt Generieren Sie einen vertrauenswürdigen Schlüsselspeicher. (auf Seite 31).

   Um SSL zu konfigurieren, müssen Sie die Werte angeben, die Sie für die folgenden Variablen definieren. Die angezeigten Werte sind nur Beispiele. Ihre Werte können anders sein.

   - `Alias`: *`UnicaClientIdentity`* (Beispiel)
   - `Keystore`: *`HCLUnicaTrust.jks`* (Beispiel)
   - `Storepass`: *`trustPwd`* (Beispiel)
2. Wählen Sie den neuen Schlüsselspeicher in der WebSphere® Sicherheitskonsole aus.

   Wenn Sie z. B. dem Beispiel in Schritt 1 gefolgt sind, wählen Sie die Option `HCLUnicaTrust.jks` aus.
3. Beziehen Sie ein Sicherheitszertifikat von HCL Unica und importieren Sie es in WebSphere®, wie in den folgenden Schritten beschrieben

   a. Navigieren Sie in der -WebSphere® Sicherheitskonsole zu **SSL-Zertifikat- und Schlüsselverwaltung** > **Schlüsselspeicher und Zertifikate> NodeDefaultTrustStore** > **Unterzeichnerzertifikate**. Wählen Sie die Option zum **Abrufen vom Port**.

   b. Konfigurieren Sie WebSphere®, um eine Testverbindung zum Abrufen des Unterzeichnerzertifikats von HCL Unica herzustellen. Geben Sie die folgenden Werte für das HCL Unica-Unterzeichnerzertifikat ein.
      - **Host** Der Wert, der für die `Deliver > serverComponentsAndLocations > hostedServices > uihostNAME`
      - **Port: 443**
      - **SSL-Konfiguration für ausgehende Verbindung** `NodeDefaultSSLSettings`
      - **Aliasname** Der Wert, den Sie für den **Host** eingegeben haben

      Wenn Sie fertig sind, WebSphere® kommuniziert mit HCL Unica Hosted Services, um die Informationen abzurufen, die zum Erstellen eines Unterzeichnerzertifikats für HCL Unica gehostete Services erforderlich sind.
4. Nachdem WebSphere® die Erstellung des Unterzeichnerzertifikats abgeschlossen hat, wählen Sie das neue Zertifikat in der Sicherheitskonsole aus.

   Der Webanwendungsserver verwendet das neue Zertifikat beim Herstellen von Verbindungen zu HCL Unica.
5. Erneut starten WebSphere®

WebSphere® implementiert die Konfigurationsänderungen erst, wenn Sie den Webanwendungsserver neu starten.

Weitere Informationen zu unterstützten WebSphere®-Versionen für die Bereitstellung von Unica-Produkten finden Sie im Dokument Empfohlene Softwareumgebungen und Mindestsystemanforderungen für jedes Produkt.

## Bereitstellung von Campaign in Tomcat oder JBOSS

Falls Campaign in Tomcat oder JBOSS bereitgestellt wird, werden keine zusätzlichen Konfigurationen in Deliver erforderlich. Sie müssen keine Zertifikate für gehostete Dienste beschaffen und konfigurieren.

# Chapter 4. Operation für Response and Contact-Tracker

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

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

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

**Unter folgenden Bedingungen ist ein Neustart von RCT erforderlich:**

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

Sie müssen Kafka in Unica Platform für RCT konfigurieren. Führen Sie die folgenden Schritte aus, um auf Kafka-Konfigurationen zuzugreifen. Für Einzelheiten zur Konfiguration von Kafka, siehe das Thema Konfigurationseigenschaften von Unica Deliver (on page 49).

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

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

Auf der Seite Kafka Konfiguration können Sie einen der folgenden Werte für das Feld CommunicationMechanism auswählen:

- NO_SASLPLAINTEXT_SSL
- SASL_PLAINTEXT
- SSL
- SASL_PLAINTEXT_SSL

Abhängig von Ihrer Auswahl sind die folgenden Felder obligatorisch:

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

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

**Schritte, um RCT zu starten:**

1. Zookeeper starten, 10 Sekunden warten

2. Kafka starten

3. RCT wie gewohnt starten

**Schritte, um RCT zu stoppen:**

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

Sie können die RCT auf eine der folgenden Arten starten.

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

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

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

# Manuelle Bedienung des Response and Contact Tracker

Um die Antwort-und Kontakttracker (RCT) manuell zu betreiben, führen Sie das `rct` Script im Verzeichnis `bin` in Ihrer Deliver-Installation aus.

- Führen Sie zum Starten der RTC das `rct` -Skript im `bin` -Verzeichnis unter Ihrer Deliver -Installation wie folgt aus.

```
rct start
```

- Führen Sie das rct-Skript wie folgt aus, um die `RCT` zu stoppen.

```
rct stop
```

Weitere Informationen zu dem Beispielscript finden Sie in Deliver Response and Contact Tracker (RCT) Skript (auf Seite 114).

## Antwort-und Kontaktverfolgung als Service hinzufügen

Sie können die Antwort- und Kontaktverfolgung (RCT) so konfigurieren, dass Sie automatisch gestartet wird, indem Sie sie als Service hinzufügen.

Registrieren Sie den RCT-Dienst, indem Sie das mit der Deliver-Software gelieferte Skript `MKService_rct` ausführen.

Führen Sie das Skript `MKService_rct -install` im Verzeichnis `bin` unter Ihrer Deliver-Installation aus, um den RCT (Response and Contact Tracker) als Dienst hinzuzufügen.

Das Verzeichnis `bin` wird als Unterverzeichnis im Campaign Installationsverzeichnis erstellt, wenn Sie die neueste Version von Unica Campaign installieren oder aktualisieren.

Führen Sie dieses Skript in UNIX™ oder Linux™ mit einem Benutzer aus, der über Root-Berechtigungen oder Berechtigungen zum Erstellen von Daemon-Prozessen verfügt.

In Windows™ lautet der Name des Dienstes **Response and Contact Tracker**.

Nachdem Sie das Skript `MKService_rct` ausgeführt haben, starten Sie die RCT manuell mit dem Skript `rct`. Sie müssen die RCT nur einmal manuell erneut starten. Nachdem Sie die RCT beim ersten Mal manuell gestartet haben, startet die RCT bei jedem Neustart des Betriebssystems des Computers, auf dem Sie die RCT installiert haben, automatisch erneut.

Nach dem Konfigurieren des RCT-Dienstes können Sie verhindern, dass der RCT automatisch gestartet wird, indem Sie das Skript `MKService_rct` mit der Option `-remove` ausführen.

## Entfernen des Antwort- und Kontaktverfolgungsdienstes

Wenn Sie den Antwort- und Kontaktverfolgungsdienst (Response and Contact Tracker - RCT) als Dienst installiert haben, wird der RCT jedes Mal neu gestartet, wenn Sie das System neu starten, auf dem Sie den RCT installiert haben.. Um zu verhindern, dass der RCT automatisch erneut gestartet wird, müssen Sie den Service für Response and Contact Tracker (RCT) entfernen.

Um die RCT als Service zu entfernen, führen Sie das `MKService_rct` Script mit der Option `-Entfernen` aus.

Führen Sie in einer Windows™-Befehlszeile in Ihrem HCL Unica-Ausgangsverzeichnis `Deliver\bin\MKService_rct.bat -remove` aus.

Führen Sie in UNIX™ oder Linux™ in Ihrem HCL Unica-Ausgangsverzeichnis `Deliver/bin/MKService_rct.sh -remove` aus.

Weitere Informationen zu dem Beispielscript finden Sie in Das Script MKService_rct (auf Seite 115).

# Kapitel 5. Startüberprüfung

Um den Zugriff auf alle gehosteten E-Mail-Funktionen sicherzustellen, testen Sie die Konfigurationen und Verbindungen für Ihre Campaign- und Deliver-Installationen, nachdem Sie Deliver aktiviert, Ihre Deliver-Installation erweitert oder die Campaign-Installation aktualisiert haben.

Überprüfen Sie die Konfigurationen und Verbindungen, nachdem Sie einen der folgenden Schritte ausgeführt haben.

- Deliver zum ersten Mal aktivieren
- Aktualisieren Sie Ihre Unica Campaign -Installation
- Fügen Sie eine neue Partition zur Deliver-Konfiguration hinzu, die in Unica Platform verwaltet wird.

## Bestätigung für Systemkonfigurationen

Um sicherzustellen, dass die Startvorbereitungen abgeschlossen sind, müssen Sie sicherstellen, dass die folgenden Konfigurationseigenschaften festgelegt sind und die Einstellungen den Anforderungen für Ihre Deliver und die Campaign -Installation entsprechen.

| Konfigurationseigenschaft | Einstellung |
|---|---|
| `Campaign \| Partitionen \| Partition[n] \| Deliver \| DeliverPluginJarFile` | Vollständiger Pfad zur Speicherposition der Plug-In-Datei, die als RLU (Recipient List Uploader) agiert. Geben Sie den vollständigen lokalen Verzeichnispfad im Dateisystem für den Computer ein, auf dem sich der Campaign-Webanwendungsserver befindet.<br><br>Das Unica Installationsprogramm trägt bei der Ausführung der Installation diese Einstellung automatisch für die Standardpartition ein. Für weitere Partitionen müssen Sie diese Eigenschaft manuell konfigurieren. |
| `Campaign \| Partitionen \| Partition[n] \| Server \| intern \| deliverInstalled` | Gibt an, dass Deliver installiert ist.<br><br>Setzen Sie diese Eigenschaft in jeder Partition, in der Sie Deliver aktivieren möchten, einschließlich der Standardpartition, auf **Ja**. Wenn Sie diese Eigenschaft auf **Ja** setzen, werden Deliver-Funktionen in der Campaign-Oberfläche verfügbar. |
| `Deliver \| serverComponentsAndLocations \| hostedServices \| uiHostName` | Adresse HCL Unica für die gesamte Kommunikation mit Ausnahme des Hochladens von Listen.<br><br>Die Standardeinstellung ist `em.unicadeliver.com`, für das US-Rechenzentrum. |

| Konfigurationseigenschaft | Einstellung |
|---|---|
| | Wenn Sie eine Verbindung zum Rechenzentrum in Europa herstellen, ändern Sie diesen Wert in `em-eu.unicadeliver-.com`. |
| `Deliver \| serverComponentsAndLocations \| hostedSer-vices \| dataHostName` | Die Adresse für die Verbindung, die Deliver zum Hochladen von Metadaten verwendet, die sich auf Empfängerlisten beziehen, auf HCL Unica.<br><br>Die Standardeinstellung ist `em.unicadeliver.com`, für das US-Rechenzentrum.<br><br>Wenn Sie eine Verbindung zum Rechenzentrum in Europa herstellen, ändern Sie diesen Wert in `em-eu.unicadeliver-.com`. |
| `Deliver \| serverComponentsAndLocations \| hostedSer-vices \| ftpHostName` | Die Adresse, die Deliver für das Hochladen von Empfängerlistendaten (ausgenommen Listenmetadaten) nach HCL Unica verwendet.<br><br>Die Standardeinstellung ist `FTP-em.unicadeliver.com`, für das US-Rechenzentrum.<br><br>Wenn Sie eine Verbindung zum Rechenzentrum in Europa herstellen, ändern Sie diesen Wert in `ftp-eu.unicadeliver-.com`. |
| `Deliver \| Partitionen \| Partition[n] \| hostedAc-countInfo \| amUserForAcctCredentials` | Der HCL Unica Benutzer, der auf die Datenquellen verweist, die die Berechtigungsnachweise für HCL Unica gehostete Services<br><br>Sie konfigurieren diesen Wert, wenn Sie einen Systembenutzer erstellen, der auf die von Unica gehosteten E-Mail-Ressourcen zugreift. |
| `Deliver \| Partitionen \| Partition [n] \| hostedAc-countInfo \| amDataSourceForAcctCredentials` | Die Platform-Datenquellen, die die Anmeldeberechtigungsnachweise für HCL Unica gehostete Services enthält<br><br>Sie konfigurieren diesen Wert, wenn Sie einen Systembenutzer erstellen, der auf die von Unica gehosteten E-Mail-Ressourcen zugreift. |

| Konfigurationseigenschaft | Einstellung |
|---|---|
| `Deliver \| Partitionen \| Partition[n] \| dataSources \| SystemTabellen \| Typ` | Typ der Datenbank, die die -Systemtabellen hostet.<br><br>Geben Sie den korrekten Wert für Ihre Datenbank an. |
| `Deliver \| Partitionen \| Partition[n] \| dataSources \| SystemTabellen \| schemaName` | Name des Datenbankschemas für die -Systemtabellen.<br><br>Setzen Sie den entsprechenden Schemanamen für Ihre Datenbank fest. |
| `Deliver \| Partitionen \| Partition[n] \| dataSources \| SystemTabellen \| jdbcClassName` | JDBC-Treiber für Systemtabellen.<br><br>Geben Sie den korrekten Wert für Ihre Umgebung an. |
| `Deliver \| Partitionen \| Partition[n] \| dataSources \| SystemTabellen \| jdbcURI` | JDBC-Verbindungs-URI für Systemtabellen.<br><br>Geben Sie den korrekten Wert für Ihre Umgebung an.<br><br>Geben Sie den Datenbanktyp, den Datenbanktreiber, den Host, den Port und den Datenbanknamen an. Zum Beispiel: `jdbc:oracle:thin:@yourdb.example.com:1234:DBname`<br><br>In Ihrer Datenbankdokumentation finden Sie spezifische Anweisungen zum Erstellen der JDBC-URL.<br><br>Der Wert, den Sie eingeben, muss exakt mit dem Wert übereinstimmen, der in Ihrem Campaign-Web-Server definiert ist. |
| `Deliver > Partitionen > Partition[n] < dataSources > systemTables > asmUserForDBCredentials` | Der HCL Unica Benutzer, der auf die Datenquellen verweist, die die Berechtigungsnachweise für Systemtabellen<br><br>Sie können diesen Benutzer erstellen, wenn Sie den Zugriff auf die lokalen Deliver Systemtabellen konfigurieren. |
| `Deliver \| Partitionen > partition [n] < dataSources \| systemTables \| amDataSourceForDBCredentials` | Die Platform-Datenquelle, die Anmeldeinformationen für die Datenbank enthält, die die Systemtabellen enthält.<br><br>Sie erstellen diese Datenquellen, wenn Sie einen Benutzer für den Zugriff auf die Deliver -Systemtabellen erstellen. |

# Testen von Upload auf HCL Unica gehostete Services

Führen Sie das **rlu**-Skript im Überprüfungsmodus aus, um die Fähigkeit zum Hochladen von Daten auf HCL Unica gehostete Dienste aus Ihrer lokalen Umgebung zu testen.

Führen Sie im Verzeichnis `bin` unter ihrer Deliver -Installation das Script `rlu'` auf eine der folgenden Arten aus.

- `rlu -c`
- `rlu -- überprüfen`

# Herunterladen von HCL Unica gehosteten Services testen

Führen Sie das rct-Skript im Überprüfungsmodus aus, um die Fähigkeit zum Herunterladen von Informationen von HCL Unica gehosteten Diensten zu testen.

Führen Sie im Verzeichnis `bin` unter Ihrer Deliver -Installation das `rct` -Skript wie folgt aus.

```
Überprüfung der RMA-Nummer
```

# Verbindung zur gehosteten Nachrichtenschnittstelle testen

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

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

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

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

# Kapitel 6. Konfigurationen für Unica Deliver

Die Unica Platform bietet verschiedene Konfigurationseigenschaften zur Änderung des Verhaltens und der Darstellung von Deliver. Einige Konfigurationseigenschaften werden während der Installation festgelegt. Konfigurationseigenschaften können jederzeit geändert werden.

Nachdem Sie die Konfigurationen von Campaign und Deliver geändert haben, müssen Sie den Webanwendungsserver erneut starten, auf dem sich Campaign befindet, und die Antwort- und Kontaktverfolgung (RCT) erneut starten.

| Charakteristik oder Funktion | Konfigurationseigenschaft (einschließlich Pfad) |
|---|---|
| Aktivieren oder inaktivieren Sie Deliver in der Campaign Partition.<br><br>Entsprechende Informationen finden Sie unter Campaign \| Partitionen \| Partition[n] \| Server \| intern (auf Seite 51). | `Campaign \| Partitionen \| Partition[n] \| Server \| intern` |
| Merkmale der Empfängerlisten für die E-Mail.<br><br>Entsprechende Informationen finden Sie unter Campaign \| Partitionen \| Partition[n] \| Deliver (auf Seite 49). | `Campaign \| Partitionen \| Partition[n] \| Zustellen` |
| URLs, die für die Verbindung zu HCL Unica Hosted Services erforderlich sind.<br><br>Entsprechende Informationen finden Sie unter Deliver \| serverComponentsAndLocations \| hostedServices (auf Seite 55). | `Deliver \| serverComponentsAndLocations \| hostedServices` |
| Datenbank-und Kontozugriffberechtigungsnachweise für die Verbindung zu HCL Unica gehosteten Services<br><br>Weitere Informationen finden Sie unter Deliver \| Partitionen \| Partition[n] \| hostedAccountInfo (auf Seite 60). | `Deliver \| Partitionen \| Partition[n] \| hostedAccountInfo` |
| Datenbankzugriff und Schemaeinstellungen für die Deliver -Systemtabellen. | `Deliver \| Partitionen \| Partition[n] \| dataSources \| SystemTabellen` |

| Charakteristik oder Funktion | Konfigurationseigenschaft (einschließlich Pfad) |
|---|---|
| Weitere Informationen finden Sie unter Deliver \| partitions \| partition[n] \| dataSources \| systemTables (auf Seite 61). | |
| Speicherort eines Scripts, das als Reaktion auf die Aktionen oder den Status des Uploaders der Empfängerliste ausgeführt wird. (Optional)<br><br>Weitere Informationen finden Sie unter Deliver \| Partitionen \| Partition[n] \| recipientListUploader (auf Seite 65). | `Deliver \| Partitionen \| Partition[n] \| recipientListUploader` |
| Einstellungen zum Herunterladen von Daten, die von der Antwort- und Kontaktverfolgung (RCT) verarbeitet werden.<br><br>Weitere Informationen finden Sie unter Deliver \| Partitionen \| Partition[n] \| responseContactTracker (auf Seite 65). | `Unica Deliver \| Partitionen \| Partition[n] \| responseContactTracker` |
| Betreuung der Darstellung von Listen personalisierter Daten in Deliver basierend auf Dimensionstabellen in Campaign.<br><br>Siehe Informationen zur Konfiguration von Dimensionstabellen (auf Seite 48). | `Campaign \| partitions \| partition[n]\| Deliver \| OLTDimTableSupport` |
| Unterstützung für die Verfolgung des Mailing-Ausführungsverlaufs. Weitere Informationen finden Sie unter Deliver \| Partitionen \| Partition[n] \| responseContactTracker (auf Seite 65). | `Unica Deliver \| Partitionen \| Partition[n] \| responseContactTracker`<br><br>Siehe den Parameter **enableExecutionHistoryDataTracking** . |

Weitere Informationen zu den Konfigurationseigenschaften finden Sie im Platform -Administratorhandbuch.

# Konfigurieren des Zugriffs auf den zusätzlichen Mailing-Ausführungsverlauf

Sie können anfordern, dass Unica zusätzliche Daten zum Mailingausführung bereitgestellt werden. Der Zugriff auf zusätzliche Mailing-Ausführungsverlaufsdaten ist auf Anfrage von Unica und durch Aktualisieren der Deliver-

Konfiguration möglich. Daten für den Mailing-Ausführungsverlauf werden in Ihren lokalen Deliver-Systemtabellen in der Tabelle `UACE_ExecHistory` aufgezeichnet, um abgeschlossene Mailing-Läufe zu beschreiben.

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

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

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

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

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

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

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

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

# Unterstützung bei der Campaign Angebotsintegration

Unica  Deliverunterstützt das Hinzufügen von Angeboten, die in Campaign zu einer personalisierten, in Deliver erstellten E-Mail konfiguriert sind.

Die Angebote basieren auf Angebotsvorlagen, die in Unica Campaign konfiguriert sind. Um die Integration von Angeboten in personalisierte E-Mails zu unterstützen Campaign, müssen Sie die Eigenschaft `contactAndResponSehistTracking` in der Campaign Konfiguration aktualisieren und andere Konfigurationen in Campaign abschließen.

Weitere Informationen zur Konfiguration der Unterstützung der Angebotsintegration finden Sie in den Abschnitten Deliver zur Angebotsintegration im Unica Campaign Administratorhandbuch.

# Konfigurieren der Unterstützung für Dimensionstabellen

Um bestimmte Funktionen zu nutzen, die von erweiterten Scripts für die E-Mail-Adresse bereitgestellt werden, muss die Konfigurationseigenschaft `OLTdimTablesUpPort` auf **true**gesetzt sein.

Deliver Bietet erweiterte Skripts zum Erstellen von E-Mail-Nachrichten, in denen Listen mit personalisierten Informationen angezeigt werden. Diese Listen müssen Dimensionstabellen zuordnen Campaign , die in mit einer Ausgabelistentabelle (OLT) erstellt werden, die die Empfängerliste des Empfängers definiert Die Ausgabenlistentabellen werden im Deliver Schema erstellt.

Die Konfigurationseigenschaft `OLTdimTableUpPort` steuert die Support für die Erstellung von Dimensionstabellen im Deliver Schema. Wenn der Wert für diese Eigenschaft auf ' `true`' gesetzt ist, kann ein OLT die in einer Dimensionstabelle bereitgestellten Informationen verwenden.

Gehen Sie wie folgt vor, um die Eigenschaft `OLTdimTablesupPort` zu aktualisieren.

Weitere Informationen darüber, wie Vermarkter erweiterte Skripts zum Erstellen von Datentabellen verwenden, finden Sie im Unica DeliverBenutzerhandbuch.

1. Gehen Sie zu **Einstellungen** > **Konfiguration** > **Campaign** > **Partitionen** > **Partition [n]** > **Deliver**
2. Klicken Sie auf **Einstellungen bearbeiten** und setzen Sie den Wert der `Eigenschaft OLTDimTablesUpPort` auf `true`.

# Zugriff auf lokale Deliver Systemtabellen konfigurieren

Deliver Komponenten müssen in der Lage sein, auf die Deliver -Systemtabellen im Campaign zuzugreifen. Sie müssen einen Systembenutzer erstellen und konfigurieren, der automatisch auf die Systemtabellen zugreifen kann. Der Systembenutzer, der während der Installation von konfiguriert wurde, Campaign verfügt bereits über den erforderlichen Zugriff auf das Campaign Schema.

**Anmerkung:** Wenn Ihre Installation mehrere Partitionen enthält, müssen Sie diese Task für jede Partition ausführen. Sie können Systembenutzer nicht über Partitionen gemeinsam nutzen.

Wenn Sie einen anderen Systembenutzer für den Zugriff auf die Deliver -Systemtabellen verwenden möchten, müssen Sie einen neuen Systembenutzer in Platform erstellen und eine neue Plattformdatenquelle mit Zugriff auf Campaign erstellen.

1. Geben Sie in der Deliver Konfiguration einen Systembenutzer an, der auf die Datenbank zugreift, die das Campaign-Schema hostet.

   Sie können einen neuen Benutzer erstellen oder einen vorhandenen Benutzer angeben. Der Systembenutzer, den Sie für einrichten, hat Campaign bereits Zugriff auf das Campaign-Schema.

   Verwenden Sie die Konfigurationseigenschaft `Deliver > Partitionen > Partition [n] < dataSources > Systemtabellen > asmUserForDBCredentials`.

Standardmäßig ist der angegebene Benutzer `asm_admin`.

2. Geben Sie in der Deliver Konfiguration die Datenquelle an, die so konfiguriert ist, dass sie den Benutzernamen und das Kennwort enthält, die für den Zugriff auf die Datenbank erforderlich sind, in der das Campaign Schema gehostet wird.

   Sie können die Datenquelle verwenden, die erstellt wurde, um bei der Installation von Campaign auf das Kampagnenschema zuzugreifen.

   Verwenden Sie die Konfigurationseigenschaft `Deliver > Partitionen > Partition [n] < dataSources > Systemtabellen > amDataSourceForDBCredentials`.

# Konfigurationseigenschaften von Unica Deliver

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

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

## Campaign | Partitionen | Partition[n] | Deliver

Die Eigenschaften in dieser Kategorie ermöglichen die Definition der Merkmale von Empfängerlisten und die Angabe der Speicherposition von Ressourcen, die die Listen in HCL Unica hochladen.

### DeliverPluginJarFile

**Beschreibung**

Vollständiger Pfad zur Speicherposition der Datei, die als RLU (Recipient List Uploader) agiert. Dieses Plug-in zu Campaign lädt OLT-Daten und zugehörige Metadaten zu den von Unica gehosteten fernen Services hoch. Sie müssen als Speicherposition den vollständigen lokalen Verzeichnispfad im Dateisystem des Computers angeben, der den Campaign-Webanwendungsserver hostet.

Das Unica Installationsprogramm trägt bei der Ausführung der Installation diese Einstellung automatisch für die Standardpartition ein. Für weitere Partitionen müssen Sie diese Eigenschaft manuell konfigurieren. Da es für jede Deliver-Installation nur einen RLU gibt, müssen alle Partitionen dieselbe Speicherposition für den RLU angeben.

Verändern Sie diese Einstellung nicht, es sei denn, Unica weist Sie dazu an.

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

Vollständiger lokaler Verzeichnispfad zur Installationsposition des Campaign-Web-Servers.

## defaultSeedInterval

**Beschreibung**

Die Anzahl von Nachrichten zwischen Seednachrichten, wenn `defaultSeedType` `Distribute list` lautet.

**Standardwert**

`1000`

## defaultSeedType

**Beschreibung**

Die Standardmethode, die von Deliver verwendet wird, um Anfangsadressen in eine Empfängerliste einzufügen.

**Standardwert**

`Distribute IDS`

**Gültige Werte**

- `Distribute IDS` - Verteilt IDs gleichmäßig basierend auf der Größe der Empfängerliste und der Anzahl verfügbarer Anfangsadressen und fügt Anfangsadressen in gleich großen Intervallen über die gesamte Empfängerliste hinweg ein.
- `Distribute list` Fügt die Seedadresse für jede `defaultSeedInterval`-ID in der Hauptliste ein. Fügt die gesamte Liste verfügbarer Seedadressen in festgelegten Intervallen in der gesamten Empfängerliste ein. Sie müssen das Intervall zwischen den Einfügepunkten angeben.

## oltTableNamePrefix

**Beschreibung**

Wird im generierten Schema für die Ausgabelistentabelle verwendet. Sie müssen diesen Parameter definieren.

**Standardwert**

OLT

**Gültige Werte**

Das Präfix darf höchstens acht alphanumerische Zeichen oder Unterstriche enthalten und muss mit einem Buchstaben beginnen.

## oltDimTableSupport

**Beschreibung**

Dieser Konfigurationsparameter steuert die Fähigkeit, Dimensionstabellen den Ausgabelistentabellen (OLT) im Deliver-Schema hinzuzufügen. Dimensionstabellen sind erforderlich, um erweitertes Scripting für E-Mail zum Erstellen von Datentabellen in E-Mail-Nachrichten zu verwenden.

Sie müssen diese Eigenschaft auf `True` setzen (standardmäßig ist sie `True`), damit Marketiers Dimensionstabellen erstellen können, wenn sie den Deliver-Prozess zum Definieren einer Empfängerliste verwenden. Weitere Informationen zum Erstellen von Datentabellen und zur Verwendung von erweiterten Scripts für E-Mail finden Sie im Unica Deliver-Benutzerhandbuch.

Sie müssen diese Eigenschaft auf `False` setzen, falls Sie Dimensionstabellenfelder für die Ausgabe in OLT verwenden und diese Dimensionsfelder in der Kommunikation als Personalisierungsfeld verwenden möchten.

**Standardwert**

`True`

**Gültige Werte**

True | False

## Campaign | Partitionen | Partition[n] | Server | intern

Eigenschaften in dieser Kategorie geben Integrationseinstellungen und die internalID-Grenzwerte für die ausgewählte Campaign-Partition an. Wenn Ihre Campaign-Installation aus mehreren Partitionen besteht, legen Sie diese Eigenschaften für jede Partition fest, für die sie gelten sollen.

### internalIdLowerLimit

**Konfigurationskategorie**

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

**Beschreibung**

Die Eigenschaften `internalIdUpperLimit` und `internalIdLowerLimit` beschränken die internen IDs von Campaign so, dass diese im angegebenen Bereich liegen. Beachten Sie, dass die Werte inklusiv sind: das heißt, Campaign kann sowohl die untere als auch die obere Grenzwerte verwenden.

**Standardwert**

`0` (Null)

### internalIdUpperLimit

**Konfigurationskategorie**

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

**Beschreibung**

Die Eigenschaften `internalIdUpperLimit` und `internalIdLowerLimit` beschränken die internen IDs von Campaign so, dass diese im angegebenen Bereich liegen. Die Werte sind inklusiv: das heißt, Campaign kann sowohl die untere als auch die obere Grenzwerte verwenden. Wenn Unica Collaborate installiert ist, setzen Sie den Wert auf `2147483647`.

**Standardwert**

`4294967295`

## deliverInstalled

**Konfigurationskategorie**

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

**Beschreibung**

Gibt an, dass Deliver installiert ist. Wenn Sie `Yes` auswählen, sind die Deliver-Funktionen in der Campaign-Benutzeroberfläche verfügbar.

Das Unica-Installationsprogramm setzt diesen Wert für die Standardpartition Ihrer Deliver-Installation auf `Yes`. Für weitere Partitionen, auf denen Deliver installiert ist, müssen Sie diese Eigenschaft manuell konfigurieren.

**Standardwert**

`No`

**Gültige Werte**

`Yes | No`

## Legacy_campaigns

**Konfigurationskategorie**

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

**Beschreibung**

Aktiviert für diese Partition den Zugriff auf Kampagnen, die vor der Integration von Unica Plan und Campaign erstellt wurden. Gilt nur, wenn **MO_UC_integration** auf `Yes` gesetzt ist. Veraltete Kampagnen umfassen außerdem Kampagnen, die in Campaign 7.x erstellt und mit Plan 7.x-Projekten verlinkt wurden. Weitere Informationen finden Sie im Unica Unica PlanCampaign-Integrationshandbuch.

**Standardwert**

Nein

**Gültige Werte**

Yes | No

# Campaign | Partitionen | Partition[n] | Deliver | contactAndResponseHistTracking

Verwenden Sie die Eigenschaften in dieser Kategorie, um die Deliver-Angebotsintegration mit Unica Campaign für die aktuelle Partition zu konfigurieren.

## etlEnabled

### Beschreibung

Campaign verwendet einen eigenen ETL-Prozess, um die Angebotsantwortdaten aus den Deliver-Überwachungstabellen zu extrahieren, sie umzuwandeln und in die Kontakt- und Antwortverlaufstabellen von Campaign zu laden.

Der ETL-Prozess koordiniert Informationen zwischen den erforderlichen Tabellen einschließlich `UA_UsrResponseType` (Campaign-Antworttypen) und `UA_RespTypeMapping` (Zuordnung von Antworttypen zwischen Campaign und Deliver).

Wenn Sie den Wert auf `Yes` setzen, wird sichergestellt, dass die Informationen über den Kontakt- und Antwortverlauf für Deliver-Angebote zwischen Campaign und Deliver koordiniert werden. Beispielsweise werden E-Mail-Antwortdaten in Campaign-Berichte aufgenommen.

**Anmerkung:** Damit der ETL-Prozess ausgeführt werden kann, müssen Sie zudem `Campaign | Partitionen | Partition[n] | Server | intern | DeliverInstalled` für diese Partition auf `Yes` setzen.

**Tipp:** Wenn Sie den Fortschritt des ETL-Prozesses überwachen möchten, aktivieren Sie `Campaign | Überwachung | monitorEnabledForEmessage`.

### Standardwert

`Nein`

### Gültige Werte

`Yes | No`

## runOnceADay

### Beschreibung

Gibt an, ob der ETL-Prozess nur einmal pro Tag ausgeführt werden soll.

Wenn der Wert `Yes` ist: Sie müssen eine Startzeit (**startTime**) angeben. Der ETL-Job wird dann ausgeführt, bis alle Datensätze verarbeitet sind. Der Wert für **sleepIntervalInMinutes** wird ignoriert.

Wenn der Wert `No` ist: Der ETL-Job beginnt, sobald der Campaign-Webserver startet. Der ETL-Job wird gestoppt, nachdem alle Datensätze verarbeitet wurden, und dann wartet der ETL-Job die in **sleepIntervalInMinutes** angegebene Zeit lang.

**Standardwert**

`Nein`

**Gültige Werte**

`Yes | No`

## batchSize

**Beschreibung**

Der ETL-Prozess verwendet diesen Parameter zum Abrufen von Datensätzen, die von RCT in die lokalen Deliver-Systemtabellen heruntergeladen wurden. Da hohe Werte die Leistung beeinträchtigen können, ist die Liste der verfügbaren Werte auf die nachfolgend aufgelisteten gültigen Werte beschränkt. Wenn Sie mit großen Datensatzvolumen rechnen, sollten Sie die Werte für **batchSize** und **sleepIntervalInMinutes** anpassen, um Datensätze in regelmäßigen Intervallen zu verarbeiten.

**Standardwert**

`100`

**Gültige Werte**

100 | 200 | 500 | 1000

## sleepIntervalInMinutes

**Beschreibung**

Geben Sie das Intervall zwischen ETL-Jobs in Minuten an. Diese Option legt die Wartezeit nach Abschluss eines Jobs fest. Der ETL-Prozess wartet die angegebene Zeit lang, bevor der nächste Job gestartet wird. Es können mehrere Jobs gleichzeitig ausgeführt werden, und pro Partition können mehrere ETL-Jobs vorhanden sein.

Hat **runOnceADay** den Wert `Yes`, können Sie kein Ruheintervall festlegen.

**Standardwert**

`60`

**Gültige Werte**

Positive Ganzzahlen

## startTime

**Beschreibung**

Gibt die Uhrzeit an, zu der der ETL-Job gestartet werden soll. Sie müssen das Format der englischen Ländereinstellung verwenden, um die Startzeit anzugeben.

**Standardwert**

`12:00:00 AM`

**Gültige Werte**

Eine gültige Zeit im Format `hh:mm:ss AM/PM`.

### notificationScript

**Beschreibung**

Eine optionale ausführbare Datei oder Scriptdatei, die nach dem Abschluss der einzelnen ETL-Jobs ausgeführt wird. Dies kann beispielsweise der Fall sein, wenn Sie zu Überwachungszwecken über den Erfolg oder Fehlschlag der einzelnen ETL-Jobs benachrichtigt werden wollen. Das Benachrichtigungsscript wird immer dann ausgeführt, wenn der ETL-Job für eine angegebene Partition abgeschlossen wird.

Die Parameter, die an dieses Script übergeben werden, sind fest definiert und können nicht geändert werden. Die folgenden Parameter können vom Script verwendet werden:

- etlStart: Die ETL-Startzeit in Millisekunden.
- etlEnd: Die ETL-Endzeit in Millisekunden.
- totalCHRecords: Die Gesamtzahl der verarbeiteten Kontaktdatensätze.
- totalRHRecords: Die Gesamtzahl der verarbeiteten Antwortverlaufsdatensätze.
- executionStatus: Der ETL-Ausführungsstatus mit dem Wert 1 (fehlgeschlagen) oder 0 (erfolgreich abgeschlossen).

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

Ein beliebiger gültiger Pfad, auf den der Campaign-Server mit Lese- und Schreibberechtigungen zugreifen kann. Zum Beispiel: `D:\myscripts\scriptname.exe`

## Deliver | serverComponentsAndLocations | hostedServices

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

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

## uiHostName

**Beschreibung**

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

**Standardwert**

`em.unicadeliver.com`

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

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

## dataHostName

**Beschreibung**

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

**Standardwert**

`em.unicadeliver.com`

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

## ftpHostName

**Beschreibung**

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

**Standardwert**

`ftp-em.unicadeliver.com`

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

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

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

# Deliver|serverComponentsAndLocations|Kafka|RCT

## KafkaBrokerURL

**Beschreibung**

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

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

Jede gültige Kafka-Broker-URL.

## Kommunikationmechanismus

**Beschreibung**

Gibt die Konfiguration für die Kafka Client-Authentifizierung an.

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

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

- NO_SASLPLAINTEXT_SSL
- SASL_PLAINTEXT
- SSL
- SASL_PLAINTEXT_SSL

## sasl.mechanism

**Beschreibung**

Gibt die Kafka Client-Authentifizierung an.

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

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

- SASL_PLAINTEXT
- SASL_PLAINTEXT_SSL
- SSL

### UserForKafkaDataSource

**Beschreibung**

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

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

Jeder gültige Benutzer, der auf die Kafka-Datenquelle verweist

### sasl.jaas.config.dataSource

**Beschreibung**

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

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

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

### truststore.location

**Beschreibung**

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

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

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

### truststore.password.dataSource

**Beschreibung**

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

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

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

### keystore.password.dataSource

**Beschreibung**

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

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

Datenquelle, die die Anmeldeinformationen für den Kafka-Keystore enthält

### key.password.dataSource

**Beschreibung**

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

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

Datenquelle, die die Anmeldeinformationen für den Kafka Schlüssel enthält

### ssl.endpoint.identification.algorithm

**Beschreibung**

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

**Standardwert**

leeren

**Gültige Werte**

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

### KafkaPartitionCount

**Beschreibung**

Partitionen sind der wichtigste Gleichzeitigkeitsmechanismus in Kafka. Ein Thema wird in eine oder mehrere Partitionen unterteilt, so dass Hersteller- und Verbraucherlasten skaliert werden können. Insbesondere unterstützt eine Verbrauchergruppe so viele Verbraucher wie Partitionen für ein Thema.

**Standardwert**

2

**Gültige Werte**

Anzahl der RCT-Instanz * 2

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

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

### Replicafactor

**Beschreibung**

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

**Standardwert**

1

**Gültige Werte**

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

## Deliver | Partitionen | Partition[n] | hostedAccountInfo

Definieren Sie Eigenschaften in dieser Kategorie, um Benutzerberechtigungsnachweise für die Datenbank zu definieren, die Kontoinformationen enthält, die für den Zugriff auf HCL Unica gehostete Services erforderlich sind. Die Werte, die Sie hier angeben, müssen als Benutzereinstellungen in Platform definiert werden.

### amUserForAcctCredentials

**Beschreibung**

Mit dieser Eigenschaft können Sie den Platform-Benutzer angeben, der eine Platform-Datenquelle enthält, die die für den Zugriff auf HCL Unica gehostete Services erforderlichen Kontozugangsberechtigungsnachweise angibt.

**Standardwert**

asm_admin

**Gültige Werte**

Beliebiger Platform-Benutzer.

### amDataSourceForAcctCredentials

**Beschreibung**

Verwenden Sie diese Eigenschaft, um die Platform-Datenquelle anzugeben, , die die Berechtigungsnachweise für HCL Unica gehostete Services definiert.

**Standardwert**

UNICA_HOSTED_SERVICES

**Gültige Werte**

Eine Datenquelle, die dem in `amUserForAcctCredentials` angegebenen Benutzer zugeordnet ist.

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

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

### Typ

**Beschreibung**

Typ der Datenbank, die die Deliver-Systemtabellen hostet.

**Standardwert**

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

**Gültige Werte**

- `SQLSERVER`
- `ORACLE`
- `DB2`
- `MARIADB`
- `ONEDB`

### schemaName

**Beschreibung**

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

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

**Standardwert**

dbo

### jdbcBatchSize

**Beschreibung**

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

**Standardwert**

10

**Gültige Werte**

Eine Ganzzahl größer 0.

### jdbcClassName

**Beschreibung**

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

**Standardwert**

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

### jdbcURI

**Beschreibung**

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

**Standardwert**

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

### asmUserForDBCredentials

**Beschreibung**

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

**Standardwert**

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

**Gültige Werte**

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

## amDataSourceForDBCredentials

**Beschreibung**

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

**Standardwert**

UA_SYSTEM_TABLES

**Gültige Werte**

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

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

## poolAcquireIncrement

**Beschreibung**

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

**Standardwert**

1

**Gültige Werte**

Eine Ganzzahl größer 0.

## poolIdleTestPeriod

**Beschreibung**

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

**Standardwert**

100

**Gültige Werte**

Eine Ganzzahl größer 0.

## poolMaxSize

**Beschreibung**

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

**Standardwert**

100

**Gültige Werte**

Eine Ganzzahl größer oder gleich 0.

## poolMinSize

**Beschreibung**

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

**Standardwert**

10

**Gültige Werte**

Eine Ganzzahl größer oder gleich 0.

## poolMaxStatements

**Beschreibung**

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

**Standardwert**

0

**Gültige Werte**

Eine Ganzzahl größer oder gleich 0.

## timeout

**Beschreibung**

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

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

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

**Standardwert**

100

**Gültige Werte**

Eine Ganzzahl größer oder gleich 0.

## Deliver | Partitionen | Partition[n] | recipientListUploader

Diese Konfigurationskategorie enthält eine optionale Eigenschaft für die Position eines benutzerdefinierten Scripts, das als Reaktion auf die Aktionen oder den Status des Uploaders der Empfängerliste ausführt wird.

### pathToTriggerScript

**Beschreibung**

Sie können ein Script erstellen, das eine Aktion als Antwort auf das Hochladen einer Empfängerliste in HCL Unica gehosteten Services auslöst. Sie können beispielsweise ein Script erstellen, um einen E-Mail-Alert an den Listendesigner zu senden, wenn der Upload der Liste erfolgreich abgeschlossen wurde.

Wenn Sie einen Wert für diese Eigenschaft definieren, übergibt Deliver Statusinformationen zum Uploader der Empfängerliste an die angegebene Position. Deliver nimmt keine Aktion vor, wenn Sie diese Eigenschaft leer lassen.

**Standardwert**

Es ist kein Standardwert definiert.

**Gültige Werte**

Ein gültiger Netzpfad.

## Deliver | Partitionen | Partition[n] | responseContactTracker

Die Eigenschaften in dieser Kategorie geben das Verhalten für die Antwort- und Kontaktverfolgung (Response and Contact Tracker, RCT) an. Die RCT ruft Daten für E-Mail-Kontakte, E-Mail-Zustellung und Empfängerantworten, z. B. Klicks auf Links und Öffnen von Links, ab und verarbeitet diese.

### pauseCustomerPremisesTracking

**Beschreibung**

Deliver speichert Kontakt- und Antwortdaten in einer Warteschlange in HCL Unica gehosteten Services. Über diese Eigenschaft können Sie die RCT anweisen, das Abrufen von Daten von HCL Unica gehosteten Services vorübergehend zu stoppen. Wenn Sie die Verfolgung fortsetzen, werden die akkumulierten Daten von RCT heruntergeladen.

**Standardwert**

Falsch

**Gültige Werte**

True | False

### waitTimeToCheckForDataAvailability

**Beschreibung**

Die RCT prüft regelmäßig auf neue Informationen bezüglich E-Mail-Kontakten oder Empfängerantworten. Mit dieser Eigenschaft können Sie angeben, wie oft das RCT in Sekunden auf neue Daten in HCL Unica gehosteten Services prüft. Der Standardwert ist 300 Sekunden bzw. alle 5 Minuten.

**Standardwert**

300

**Gültige Werte**

Eine beliebige Ganzzahl größer 1.

### perfLogInterval

**Beschreibung**

Mit dieser Eigenschaft können Sie in Sekunden festlegen, wie oft RCT Leistungsstatistiken in einer Protokolldatei protokollieren soll. Der eingegebene Wert bestimmt die Anzahl von Blöcken zwischen Protokolleinträgen.

**Standardwert**

10

**Gültige Werte**

Eine Ganzzahl größer 0.

### enableSeparatePartialResponseDataTracking

**Beschreibung**

Diese Eigenschaft legt fest, ob Deliver partielle E-Mail-Antwortdaten an die Überwachungstabellen Ihrer lokalen Deliver-Installation weiterleitet.

Deliver benötigt zur richtigen Zuweisung von E-Mail-Antworten die Mailing-Instanz-ID und die Nachrichtensequenznummer. Wenn Sie die partielle Antwortdatenüberwachung aktivieren, verschiebt Deliver die unvollständigen Antworten in gesonderte lokale Überwachungstabellen, wo Sie sie überprüfen oder weiter bearbeiten können.

**Standardwert**

Wahr

**Gültige Werte**

True | False

## enableExecutionHistoryDataTracking

**Beschreibung**

Diese Eigenschaft steuert, ob Sie zusätzliche Protokolldaten zur Mailing-Ausführung von HCL Unica herunterladen können.

Diese Eigenschaft ist standardmäßig auf **False** festgelegt, um das Herunterladen zusätzlicher Daten zu verhindern. Wenn Sie diese Eigenschaft auf **True** festlegen, können Sie Daten zu Mailing-Ausführungen herunterladen, die normalerweise nicht in die Deliver-Systemtabellen eingegeben werden. Sie können diese ergänzenden Informationen nutzen, um das Mailing- und Datenbankmanagement zu automatisieren.

Diese Eigenschaft ist standardmäßig ausgeblendet. Sie können diese Konfigurationseigenschaft in Ihrer lokalen Deliver-Installation anzeigen. Führen Sie dazu das Script `switch_config_visibility.bat` aus, das sich im Verzeichnis `Deliver\tools` befindet.

Der Zugriff auf Protokolldaten zur Mailing-Ausführung kann bei Unica angefordert werden. Um den Zugriff auf zusätzliche Daten zu Ausführung zu beantragen, wenden Sie sich an das Unica Deliver Services Team über HCL Technical Support

**Standardwert**

Falsch

**Gültige Werte**

True | False

# Chapter 7. Konfigurationen für die Einführung von Push-Benachrichtigungen

### Einführung

Unica unterstützt Push-Benachrichtigungen mithilfe des Kumulos-SDK, das in Form eines Frameworks bereitgestellt wird, um die Integration in Ihre iOS-, Android- oder plattformübergreifende App zu erleichtern. Dieses Handbuch bietet eine Übersicht über das Einrichten Ihrer App mit in Apple Developer- und Firebase-Cloud Messaging-Konten, bevor die spezifischen Integrationsschritte für das entsprechende SDK für Ihr Projekt detailliert beschrieben werden.

Die Integration wird durch Ausführen der folgenden Schritte abgeschlossen:

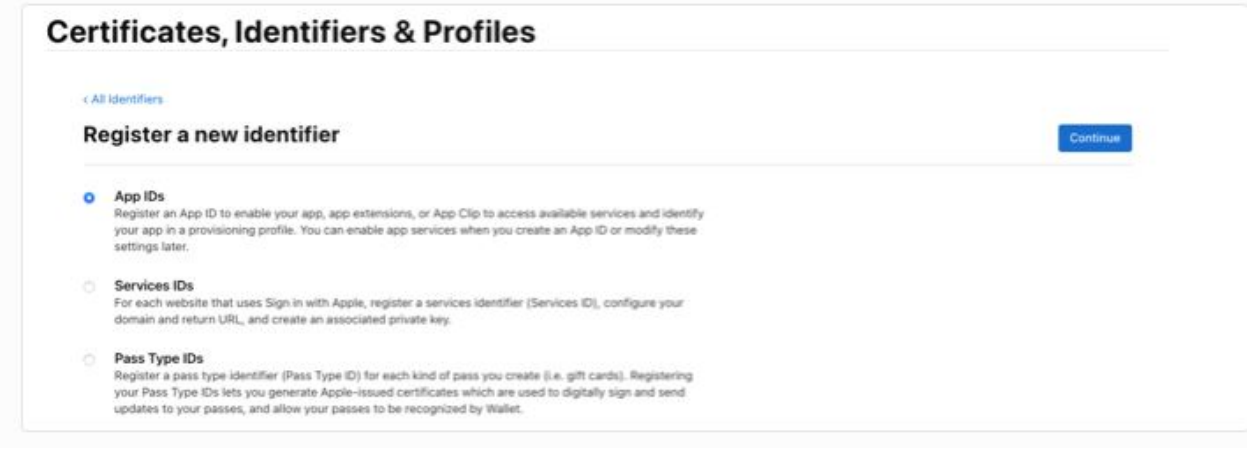
1. Konfigurieren Ihrer App in Ihrem Apple Developer-Konto
2. Konfigurieren Ihrer App in Ihrem Firebase Cloud Messaging-Konto
3. Konfigurieren Ihrer Unica-App für APNS und FCM, indem Sie die relevanten Berechtigungsnachweise angeben.
4. Wählen Sie das geeignete SDK für Ihre ausgewählte Entwicklungsplattform aus.

## Ihr Apple-Entwicklerkonto konfigurieren

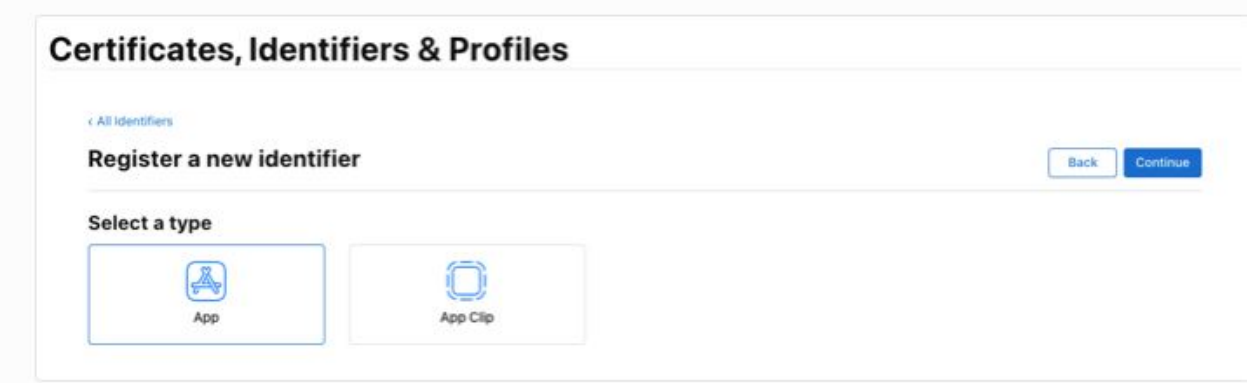
### Ihre Bundle-ID und -Funktionalität registrieren

Um Ihre App im App Store zu veröffentlichen, müssen Sie eine Bundle-ID definieren und ihre Funktionen so konfigurieren, dass Push-Benachrichtigungen und eine App-Gruppe zulässig sind.

Wählen Sie in Ihrem Apple Developer-Konto "Zertifikate, Kennungen und Profile" und dann "Kennungen" aus dem linken Menü. Klicken Sie auf das Symbol +, um Ihre neue ID zu registrieren.

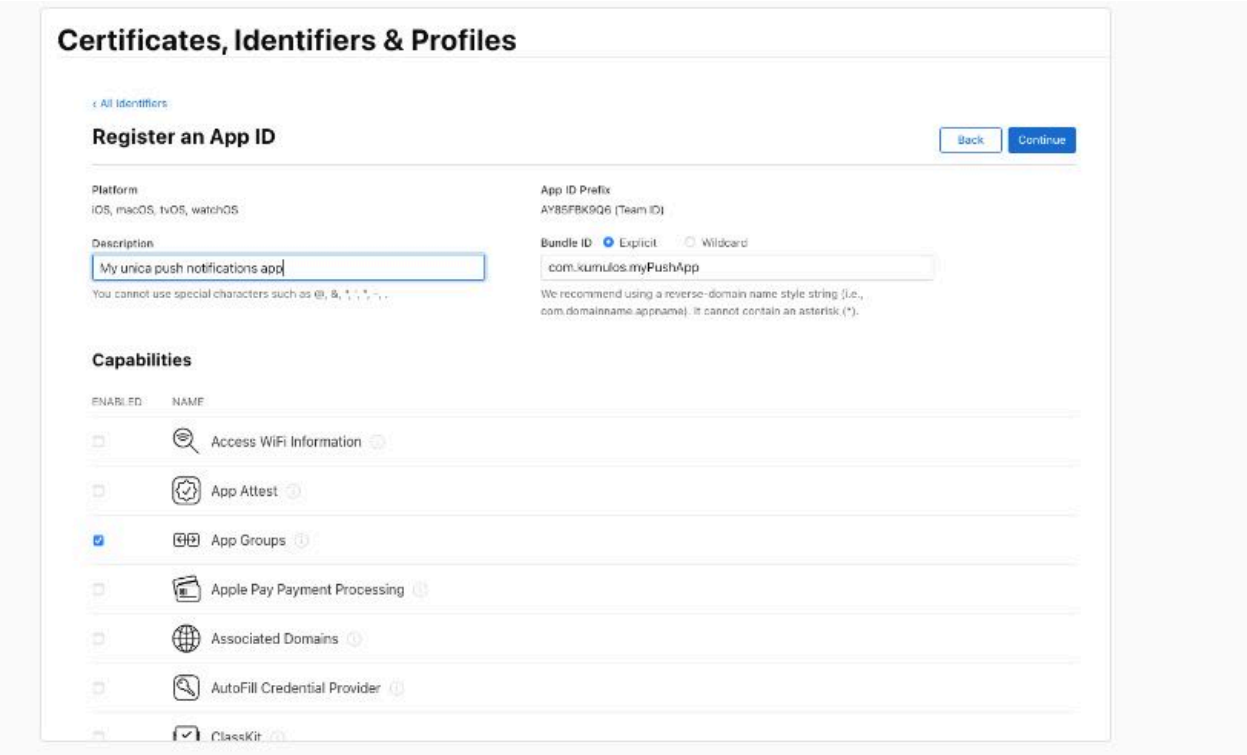



Wenn Sie aufgefordert werden, eine neue ID zu registrieren, wählen Sie die Option App-IDs aus und klicken Sie auf Weiter. Wählen Sie im zweiten Schritt den Typ App aus und klicken Sie erneut auf Weiter.




Im letzten Schritt müssen Sie Ihre Bundle-ID und Ihre Funktionalität konfigurieren. Ihre Bundle-ID entspricht in der Regel dem Standard com.[organisation name].[app name], zum Beispiel "com.kumulos.myPushApp", wählen Sie das Optionsfeld 'Explizit' aus und geben Sie Ihre vollständig qualifizierte Bundle-ID ein.

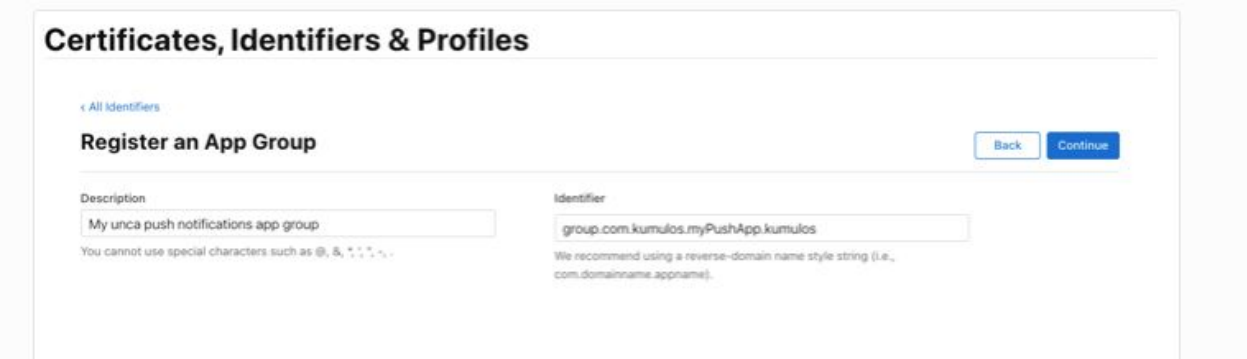
Stellen Sie im Abschnitt "Funktionalität" sicher, dass die Kontrollkästchen "App-Gruppen" und "Push-Benachrichtigungen" ausgewählt sind, und klicken Sie dann auf "Fortfahren".




Im letzten Formularschritt werden Ihre Details zur Bestätigung wiederholt. Wenn alles richtig ist, klicken Sie auf "Registrieren".

### Erstellen Sie eine App-Gruppe

Klicken Sie erneut in der Liste "Kennungen" auf das Symbol +, um eine neue Kennung zu registrieren, aktivieren Sie das Optionsfeld "App-Gruppen" und klicken Sie auf "Weiter". Ihre Kennung für die App-Gruppe muss der Konvention `group.{your.bundle.identifier}.kumulos` entsprechen. Nach unserer Beispiel-Bundle-ID lautet diese "group.com.kumulos.myPushApp.kumulos". Klicken Sie auf "Fortfahren" und klicken Sie in der letzten Anzeige, wenn alle Details richtig sind, auf "Registrieren".




### App-Gruppe mit Ihrer App-ID verknüpfen

Klicken Sie in der Liste Kennungen auf Ihre AppID, um die entsprechende Bundle-Kennung zu erhalten. Sie können die Liste auch mithilfe des Filters oben rechts nach nur App-ID-Typen filtern.

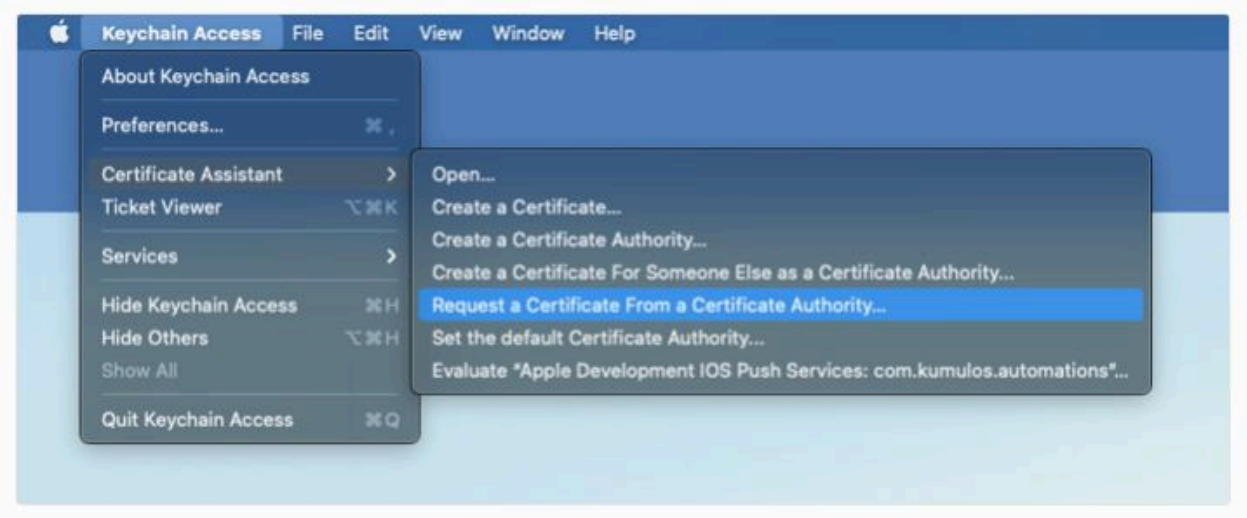
Klicken Sie im Bildschirm "AppID-Konfiguration bearbeiten" neben der Funktion "App-Gruppen" auf die Schaltfläche "Konfigurieren". Aktivieren Sie im Popup-Fenster das Kontrollkästchen neben der Gruppe, die im vorherigen Schritt mit der entsprechenden Bundle-ID erstellt wurde, und klicken Sie dann auf "Weiter", der Text neben "App-Gruppen" im Konfigurationsbildschirm sollte jetzt "Aktivierte App-Gruppen (1)" lauten. Klicken Sie auf Speichern.

### APNS-Zertifikate erstellen

Um Push-Benachrichtigungen mit Unica an iOS-Geräte zu senden, müssen Sie Zertifikate im Apple Developer Member Center erstellen, um die Berechtigungsnachweise bei Ihrer Unica App zu registrieren.

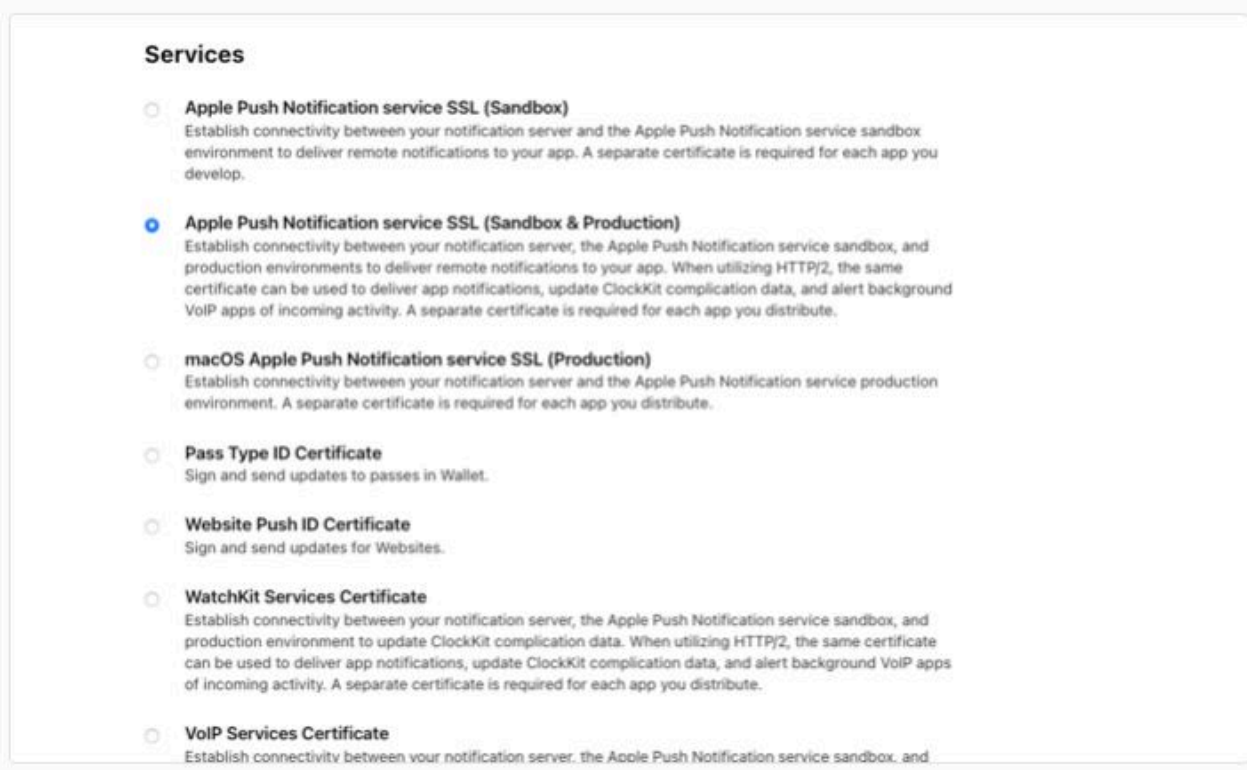
Am Ende dieses Schritts erhalten Sie eine mit Passphrasen gesicherte .p12-Datei zum Hinzufügen zur Unica-App.

Zuerst wird eine Zertifikatssignieranforderung mit Keychain Access erstellt. Greifen Sie über Ihre Symbolleiste auf das Menü Keychain Access zu und wählen Sie Zertifikatassistent, Zertifikat von einer Zertifizierungsstelle anfordern.

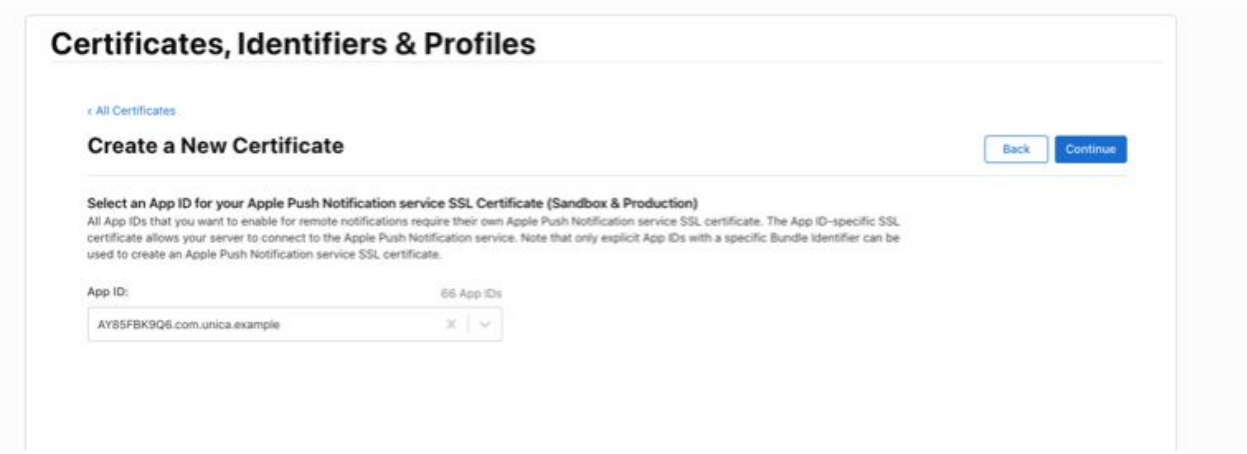



Geben Sie im Dialogfenster Ihre E-Mail-Adresse in das Feld 'Benutzer-E-Mail-Adresse' ein. Ihr Name sollte bereits im Feld 'Allgemeiner Name' angezeigt werden. Wählen Sie das Optionsfeld 'Auf Platte gespeichert' aus und klicken Sie auf 'Fortfahren'. Speichern Sie die Datei zur späteren Verwendung auf Ihrer Festplatte.

Greifen Sie als Nächstes auf Ihr Apple Developer-Konto zu und wählen Sie Zertifikate, Kennungen und Profile' im Bildschirm Zertifikate aus. Klicken Sie oben auf das blaue Pluszeichen. Scrollen Sie im Bildschirm 'Neues Zertifikat erstellen' zu 'Dienste' und wählen Sie 'Apple Push Notification Service SSL (Sandbox & Production)', klicken Sie auf Weiter.

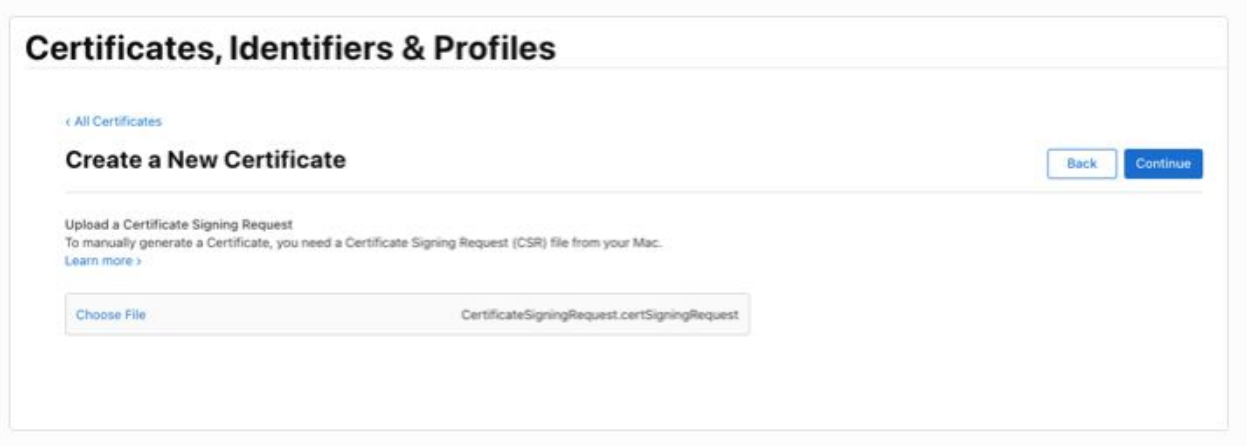



Wählen Sie in der nächsten Anzeige die App-ID aus, die während des Prozesses Erste Schritte erstellt wurde, und klicken Sie auf Weiter.




Wenn Sie aufgefordert werden, eine Zertifikatssignieranforderung hochzuladen, klicken Sie auf Datei auswählen und suchen Sie dann die

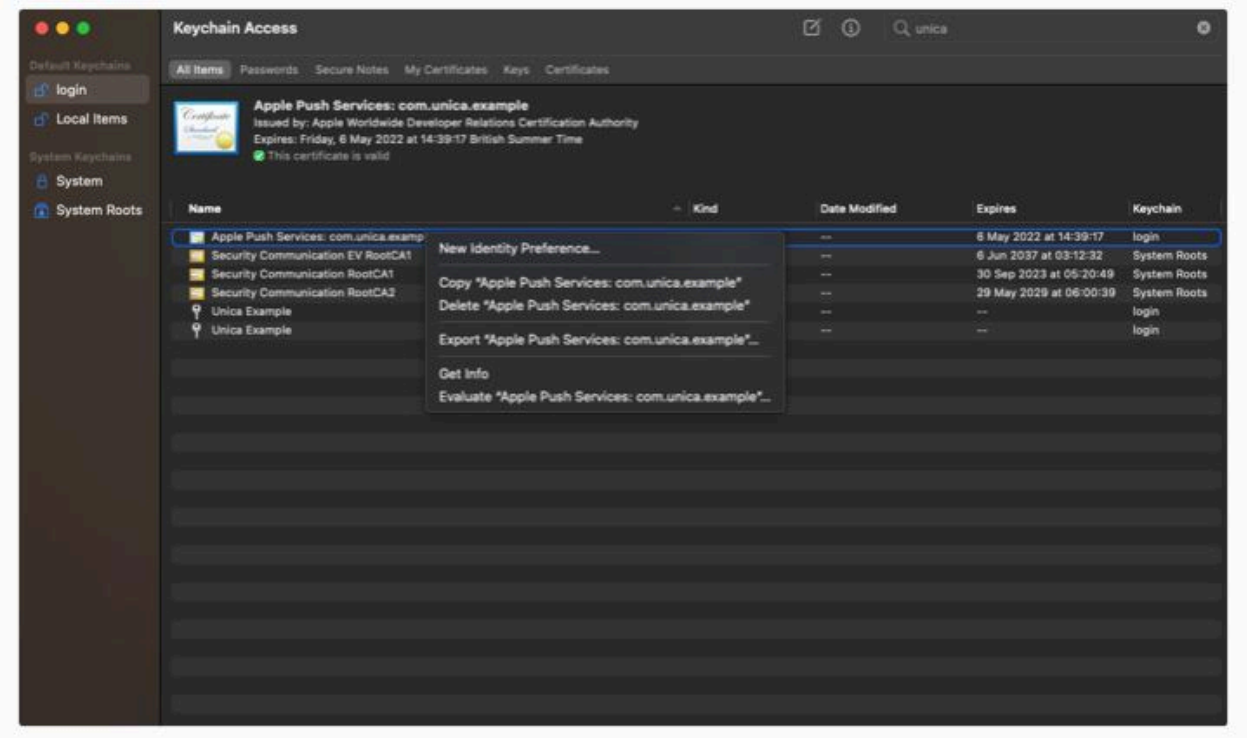
`certSigningRequest`-Datei, die zuvor erstellt wurde, klicken Sie auf Weiter.




Im letzten Schritt wird Ihnen eine Anzeige angezeigt, in der alle bisher ausgewählten Details bestätigt werden, klicken Sie auf die Schaltfläche Herunterladen.

Dadurch wird eine Datei auf Ihrer lokalen Platte gespeichert. Doppelklicken Sie auf die `.cer`-Datei, um sie zu Ihrem Keychain Access hinzuzufügen.

Sie können die Ergebnisse Ihres Schlüsselbunds mithilfe des Textfilters oben rechts filtern. Sobald Sie das Element gefunden haben, das mit der Art 'Zertifikat' mit dem Namen 'Apple Push Services [Ihre Bundle-ID]' übereinstimmt, klicken Sie mit der rechten Maustaste auf das Element und wählen Sie 'Exportieren' aus.



Stellen Sie im neuen Fenster sicher, dass das ausgewählte Dateiformat 'Personal Information Exchange (.p12)' ist, und wählen Sie eine Speicherposition für die Datei aus. Wenn Sie auf 'Speichern' klicken, sollten Sie aufgefordert werden, ein Kennwort zum Schutz der exportierten Elemente einzugeben und zu verifizieren.

Sie benötigen die Passphrase- und die .p12-Datei, um Ihr Unica App-Backend zu konfigurieren.

## Firebase Cloud-Messaging konfigurieren

Um mit Unica Nachrichten an Ihre Android-Benutzer zu senden, müssen Sie eine Firebase-App erstellen und für Firebase Cloud Messaging konfigurieren.

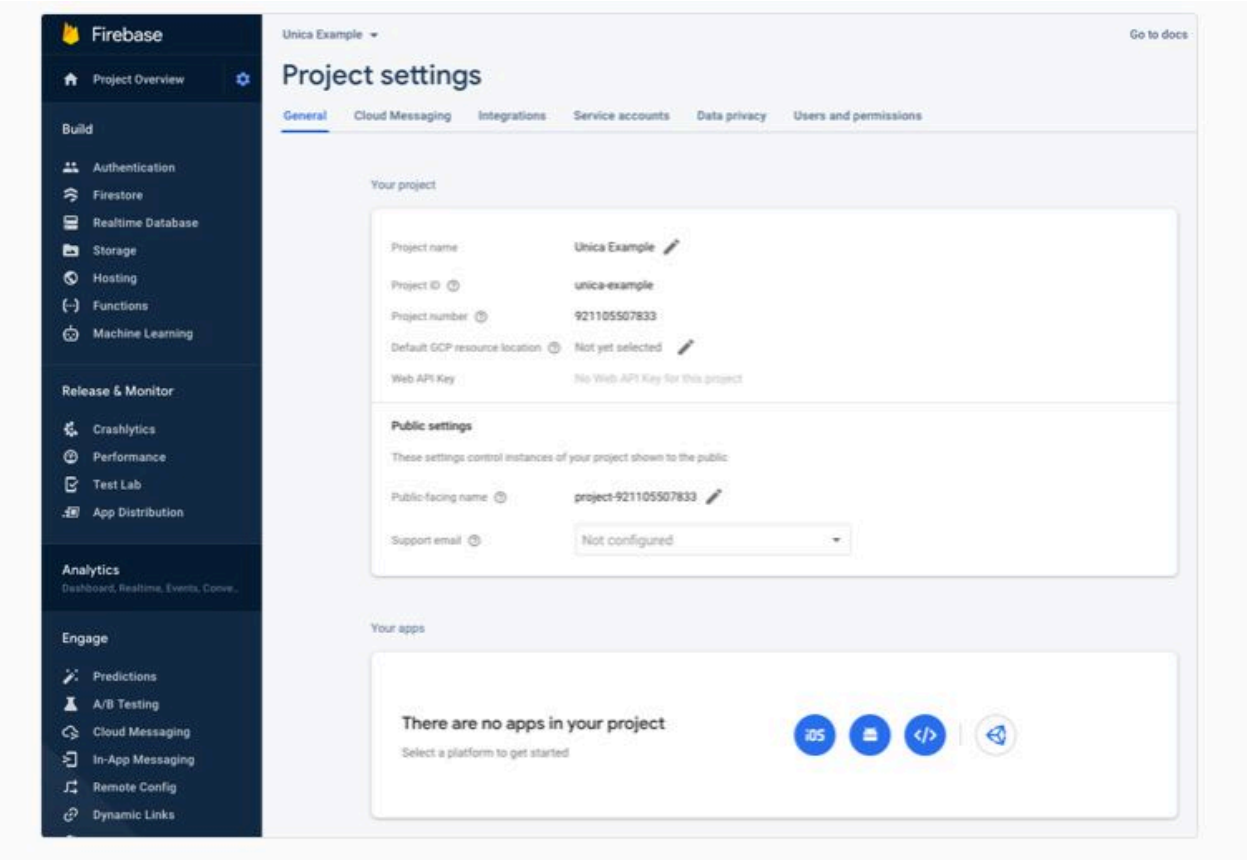
In diesem Schritt werden verschiedene Artefakte generiert, mit denen sowohl die Unica-App als auch Ihr Android-App-Projekt konfiguriert werden. Diese sind:

- JSON-Datei für Google-Dienste
- JSON-Datei für Google-Services-Account
- Serverschlüssel

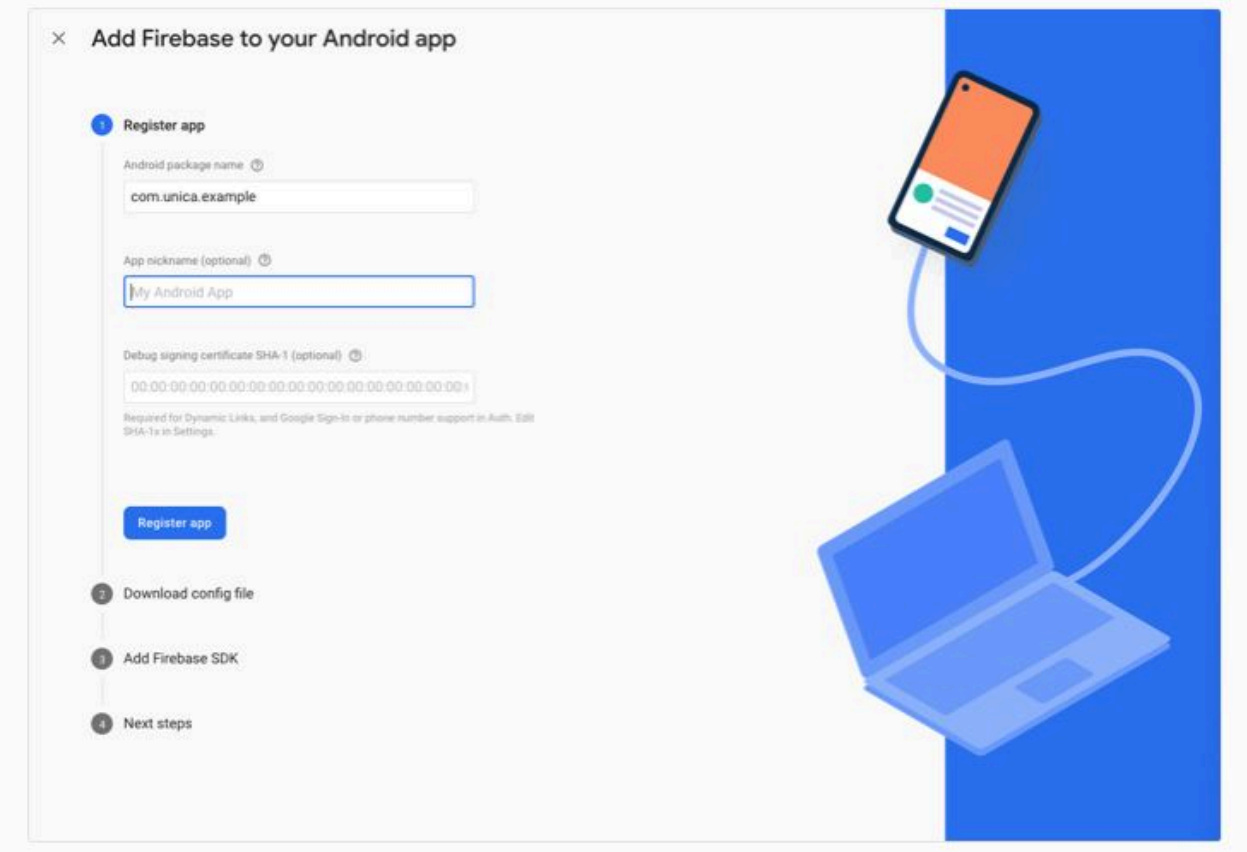
Melden Sie sich zuerst bei Ihrer Firebase-Konsole an, wählen Sie 'Projekt hinzufügen' aus und geben Sie Ihren Projektnamen im Assistenten ein. Sie können Google Analytics für Ihr Projekt aktivieren oder deaktivieren. Dies hat keine Auswirkungen auf die Integration.

Schließlich erstellt die Firebase-Konsole Ihre App, sobald der Konfigurationsprozess abgeschlossen ist, klicken Sie auf Weiter.

Als Nächstes fügen wir dem Firebase-Projekt eine Android-App hinzu. Klicken Sie im Projektübersichtsbildschirm auf das Konfigurationszahnrad neben 'Projektübersicht' und dann auf 'Projekteinstellungen'.

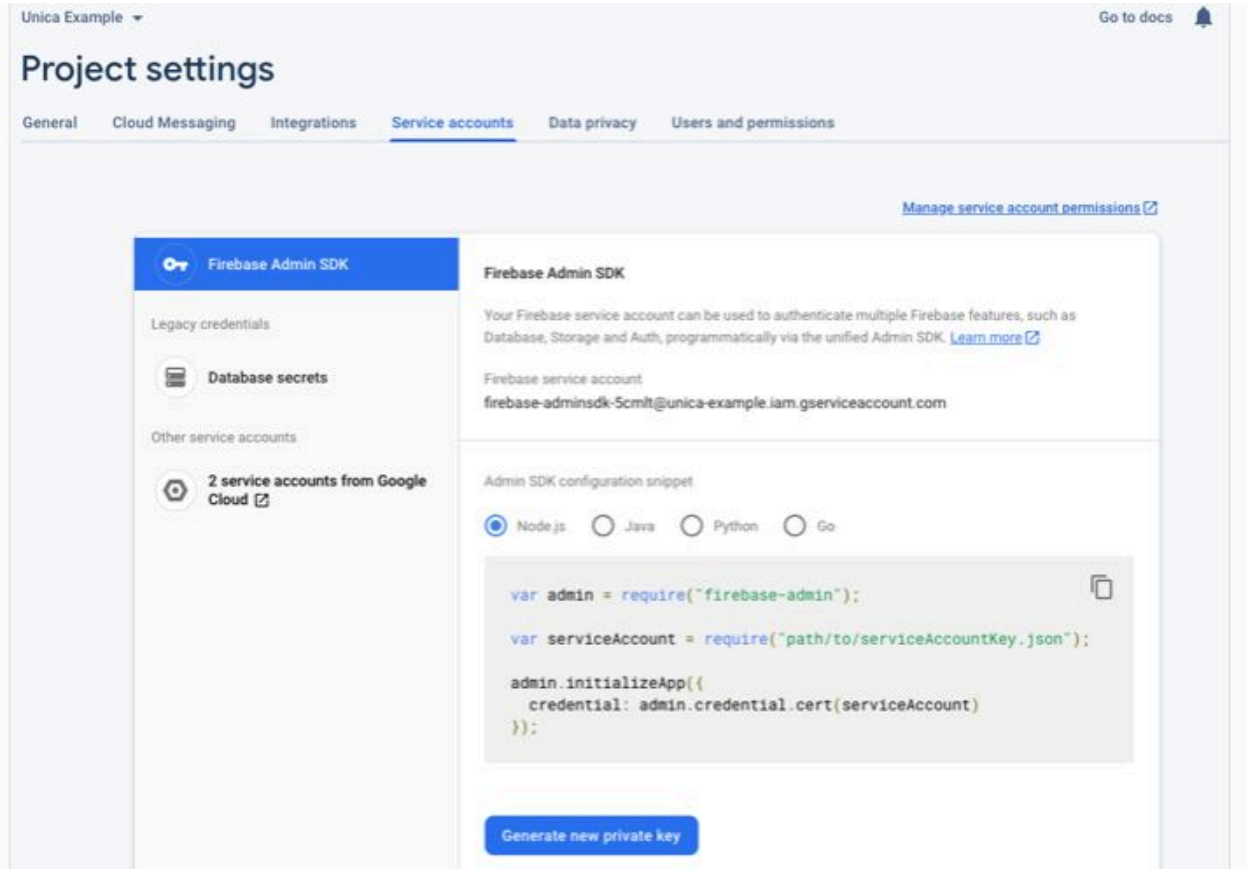



Klicken Sie auf der Registerkarte 'Allgemein' im Fenster 'Ihre Apps' auf das Symbol für Android. Dadurch wird der Assistent zum Erstellen der App geöffnet.




Geben Sie den Paketnamen Ihrer App im oberen Fenster ein und klicken Sie auf 'App registrieren'. Dadurch wird automatisch das JSON-Objekt von Google Services heruntergeladen, das später bei der SDK-Integration mit Ihrem Android-Projekt verwendet wird.

Wählen Sie die Registerkarte Cloud-Messaging aus und kopieren Sie den Serverschlüssel zur Referenzierung, um später die Unica-App zu konfigurieren.



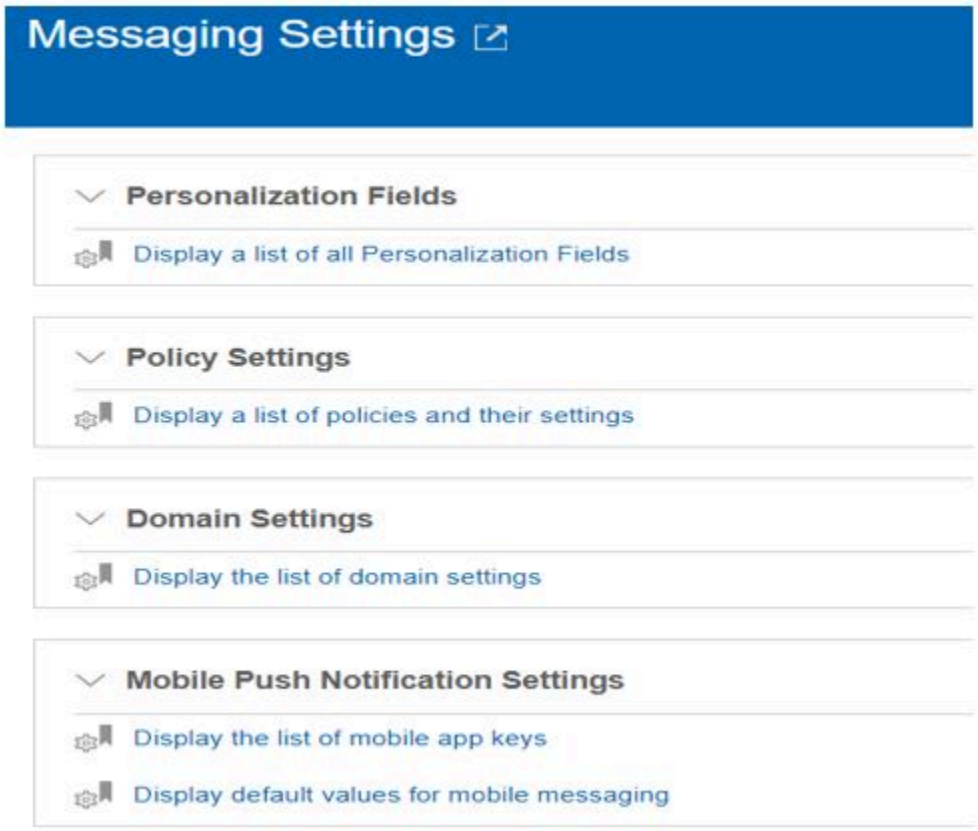

Klicken Sie anschließend auf die Registerkarte 'Service-Konten' und klicken Sie auf 'Neuen privaten Schlüssel generieren'. Dadurch wird eine JSON-Datei heruntergeladen, die Ihre Kontoberechtigungsnachweise beschreibt. Diese wird auch zum Konfigurieren Ihrer Unica-App verwendet.

Sie benötigen sowohl die JSON-Datei für Service-Konten als auch den Serverschlüssel, um Ihr Unica App-Backend zu konfigurieren.

## Konfigurieren Ihrer Unica App

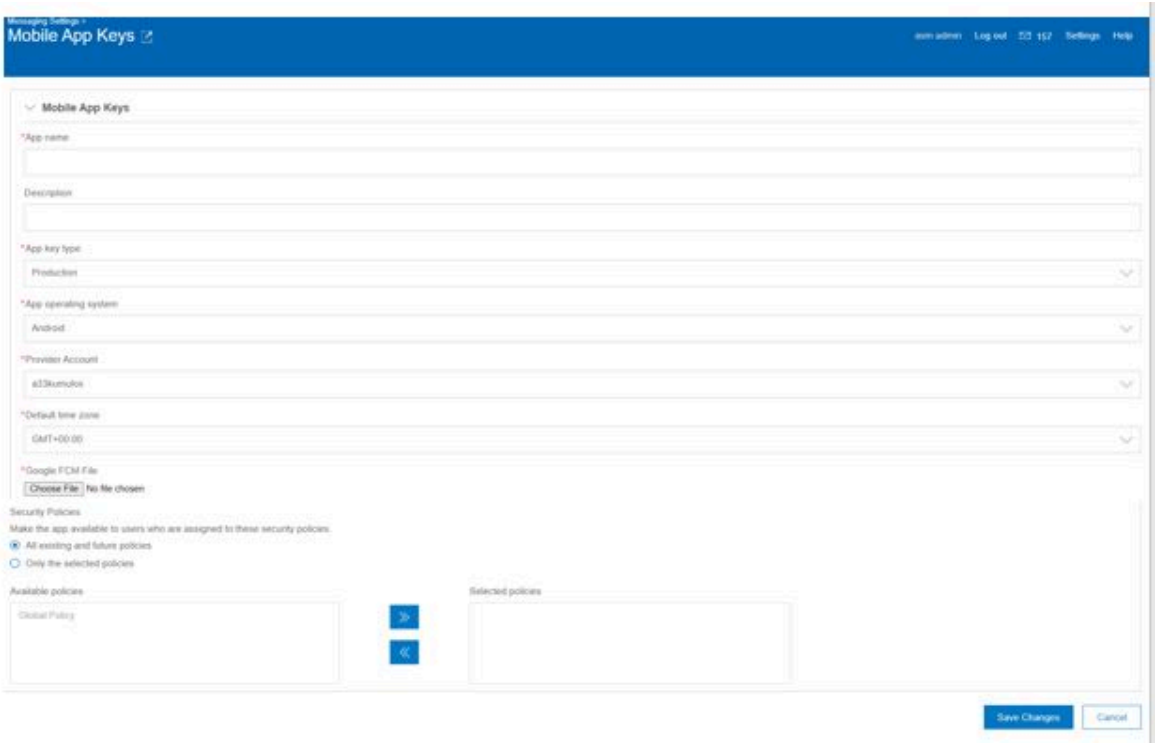
Führen Sie die folgenden Schritte aus.

1. Wählen Sie im Menü **Einstellungen** die Option **Nachrichteneinstellungen**. Die Option "Einstellungen für Mobile-Push-Benachrichtigungen" wird auf der folgenden Seite angezeigt. Wenden Sie sich andernfalls an den Unica-Support, um diese Option zu aktivieren.




2. Klicken Sie auf **Anzeige der Tasten der mobilen App anzeigen**. Die folgende Seite wird angezeigt.


3. Klicken Sie auf **einen mobilen Anwendungsschlüssel hinzufügen** . Die folgende Seite wird angezeigt.




4. Füllen Sie das Formular mit den entsprechenden Werten aus.
    - App-Name: Name der App
    - Beschreibung: Beschreibung der App
    - Schlüsseltyp der Anwendung – Der Schlüssel muss "Produktion" sein.
    - App-Betriebssystem: Android oder iOS. Dies hängt von den Zielbenutzern ab.
    - Provider-Account: Dies wird vom Unica-Backend gemäß den erstellten Konten abgerufen.
    - Standardzeitzone: Kann je nach Position ausgewählt werden.
    - Google FCM-Datei: Stellen Sie eine JSON-Datei für einen Google-Service-Account für die mobile App zur Verfügung.

Wenn Sie IOS unter 'App-Betriebssystem' auswählen, wird anstelle von 'Google FCM File' Folgendes angezeigt.


- Zertifikatsdatei: p12-Datei für iOS-App angeben.
- Kennwort für Zertifikat: Geben Sie das Kennwort für das p12-Zertifikat an.
- Sicherheitsrichtlinien: Wählen Sie die Richtlinien aus, die für die App angewendet werden sollen.

5. Klicken Sie auf **Speichern**, um die Mobile App zu erstellen. Sie können die App auf der Listenseite sehen. "Dateiupload erfolgreich" stellt den Status des FCM/P12-Dateiuploads zur Verfügung, den Sie im Formular angegeben haben.


# Integrieren von SDK

Wählen Sie das geeignete SDK für Ihre ausgewählte Entwicklungsplattform aus.

**Nativ**

- iOS Swift *(on page 80)*
- Android *(on page 87)*

**Plattformübergreifend**

- React Native *(on page 102)*

# iOS Swift

## Einführung

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

In diesem Handbuch wird davon ausgegangen, dass Sie die Schritte aus dem Konfigurationen für die Einführung von Push-Benachrichtigungen *(on page 68)* ausgeführt und Ihren Apple Identifier, die Funktionen und das Bereitstellungsprofil in diesem Handbuch konfiguriert haben. Die folgenden Integrationsschritte werden behandelt:

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

6. Optional erweitertes Verhalten für native Push Benachrichtigungen
7. Optional erweitertes Verhalten für umfangreiche In-App Nachrichten

## Integration

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

Erste Schritte mit CocoaPods

Erste Schritte mit Carthage

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

### Benachrichtigungsserviceerweiterung hinzufügen

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

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

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

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

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

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

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

.

## App-Funktionalitäten und -Berechtigungen konfigurieren

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

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

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

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

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

### Vorgehensweise zum Testen Ihrer Konfiguration

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

### Initialisierung (Initialization)

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

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

### Für Push-Benachrichtigungen registrieren

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

```
Kumulos.pushRequestDeviceToken()
```

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

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

## Registieren Ihres CRM

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

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

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

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

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

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

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

## Ereignisverfolgung

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

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

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

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

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

# Erweiterte Features

### Bearbeitung von geöffneten Benachrichtigungsereignissen

Wenn ein Benutzer mit Ihrer Push-Nachricht interagiert, indem er entweder auf die Benachrichtigung selbst oder auf eine enthaltene Aktionsschaltfläche tippt, wird das `pushOpenedHandlerBlock` aufgerufen. In diesem Block können Sie weiteres Verhalten für die Verarbeitung benutzerdefinierter Aktionen bereitstellen.

```
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())
```

### Hintergrunddaten-Push-Benachrichtigungen verarbeiten

Wenn Sie einen Push mit dem in der Benachrichtigung gesetzten `content-available`-Markierung senden, wird Ihre App aufgeweckt, um die Push-Benachrichtigung im Hintergrund zu verarbeiten. Dies löst das erforderliche Verhalten in Ihrer App aus, ohne in den Vordergrund zu treten.

Wenn Sie einen Titel und eine Nachricht festlegen, wird die Benachrichtigung stumm geschaltet und dem Benutzer im Benachrichtigungscenter wird nichts angezeigt. Sie können jedoch auch einen Titel und eine Nachricht angeben, um das Verhalten auszulösen und den Benutzer dann zu benachrichtigen.

Die `content-available`-Markierung löst den `application:didReceiveRemoteNotification:fetchCompletionHandler:`-Anwendungsdelegierten aus. Von hier aus können Sie die Nutzdaten der Benachrichtigung überprüfen und alle erforderlichen Aktionen ausführen.

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

        completionHandler(UIBackgroundFetchResult.noData)
    }
```

## Erweiterte In-App Funktionen

### In-App-Benutzerinhalte verwalten

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

### Deep-Linking für In-App

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

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

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

### Verwendung des In-App-Posteingangs

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

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

### Nachrichten abrufen

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

### Als gelesen markieren

Um eine einzelne oder alle Posteingangsnachrichten als gelesen zu markieren:

### Nachricht löschen

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

### Posteingang aktualisierter Handler

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

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

Sie können es wie folgt verwenden:

### Eine Zusammenfassung des Posteingangs erhalten

Sie können die Zusammenfassung des Posteingangs wie folgt abrufen:

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

### Rufen Sie die Bild-URL des Posteingangselements ab

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

# Android

### Einführung

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

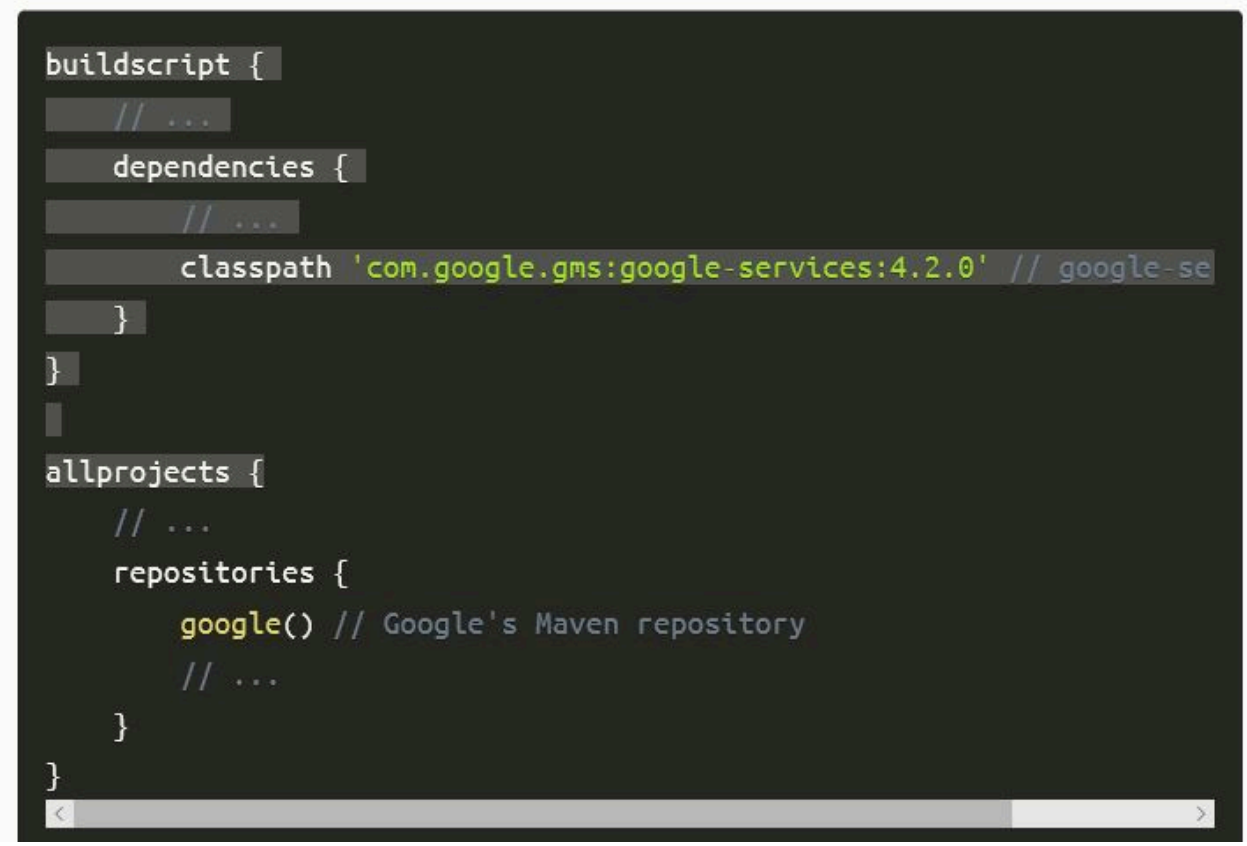
In diesem Handbuch wird davon ausgegangen, dass Sie die Schritte von Konfigurationen für die Einführung von Push-Benachrichtigungen (on page 68) aus ausgeführt und Ihre Firebase Console und Unica App mit den entsprechenden Anmeldeinformationen für Cloud Messaging konfiguriert haben. Es deckt die folgenden Schritte ab:

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

## Integration

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

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



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

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

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

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

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

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

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

apply plugin: 'com.android.application'

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

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

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

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

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

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

zur `AndroidManifest.xml` Ihrer App hinzu

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

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

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

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

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

        ...

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

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

</manifest>
```

### Initialisierung und Registrierung für Push-Benachrichtigungen

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

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

.

## Registrieren mit dem CRM

### Installations-ID

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

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

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

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

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

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

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

## Erweiterte Features

### Verarbeitung von Schaltflächen für Push-Aktionen

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

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

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

Eine Stub-Implementierung des Handlers kann wie folgt lauten:

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

### Push-Standardverhalten

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

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

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

### Push-Symbol ändern

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

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

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

### Push-Verhalten anpassen

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

Beispiel für Erweiterungsklasse:

```
package com.example;

import com.kumulos.android.PushBroadcastReceiver;

public class MyPushReceiver extends PushBroadcastReceiver {

}
```

Ändern Sie unbedingt den `AndroidManifest.xml` Empfänger:

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

### Gestartete Aktivität ändern

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

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

überschreiben.

```
package com.example;

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

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

public class MyPushReceiver extends PushBroadcastReceiver {

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

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

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

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

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

### Die Benachrichtigung anpassen

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

```
package com.example;

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

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

public class MyPushReceiver extends PushBroadcastReceiver {

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

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

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

...

notificationBuilder.setContentIntent(pendingOpenIntent);

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

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

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

...

notificationBuilder.setDeleteIntent(pendingDismissedIntent);
```

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

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

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

### Starten eines Dienstes für Hintergrunddaten-Pushs

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

```
package com.example;

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

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

public class MyPushReceiver extends PushBroadcastReceiver {

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

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

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

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

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

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

### URL-Pushes

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

### Alle Verhaltensweisen überschreiben

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

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

Darüber hinaus müssen Sie möglicherweise Verhaltensweisen implementieren für:

- Lieferverfolgung: `pushTrackDelivered(context, pushMessage)`

### Verwenden eigener `FirebaseMessagingService` mit Kumulos

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

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

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

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

## Ereignisverfolgung

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

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

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

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

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

## Erweiterte In-App Funktionen

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

### Deep-Linking für In-App

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

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

### Verwenden Sie den In_App Posteingang

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

### Nachrichten abrufen

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

### Als gelesen markieren

Um eine einzelne oder alle Posteingangsnachrichten als gelesen zu markieren:

### Nachricht löschen

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

### Posteingang aktualisierter Handler

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

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

Sie können es wie folgt verwenden:

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

### Eine Zusammenfassung des Posteingangs erhalten

Sie können die Zusammenfassung des Posteingangs wie folgt abrufen:

### Rufen Sie die Bild-URL des Posteingangselements ab

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

## Fehlerbehebung

### Proguard

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

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

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

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

# React Native

### Einführung

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

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

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

## Integration

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

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

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

Für jede Plattform sind manuelle Verknüpfungsschritte erforderlich.

### Android-Verknüpfungsschritte

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

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

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

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

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

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

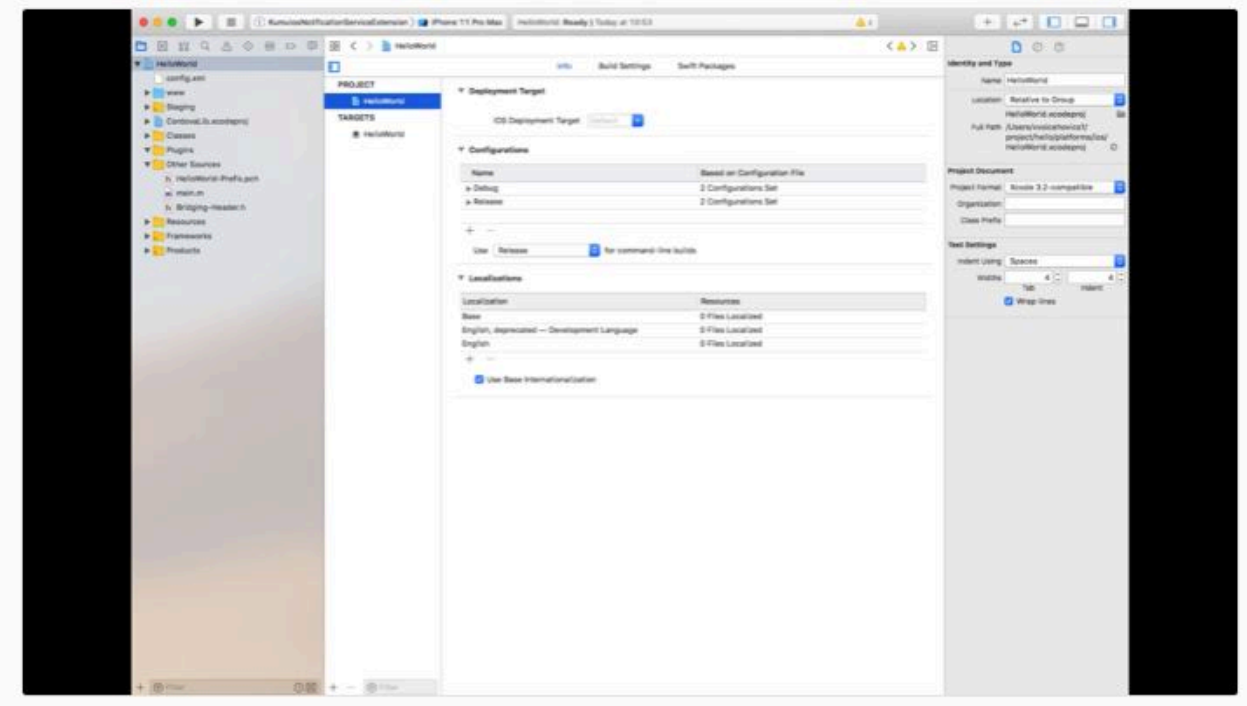
### iOS-Projektkonfiguration

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

### Benachrichtigungsserviceerweiterung hinzufügen

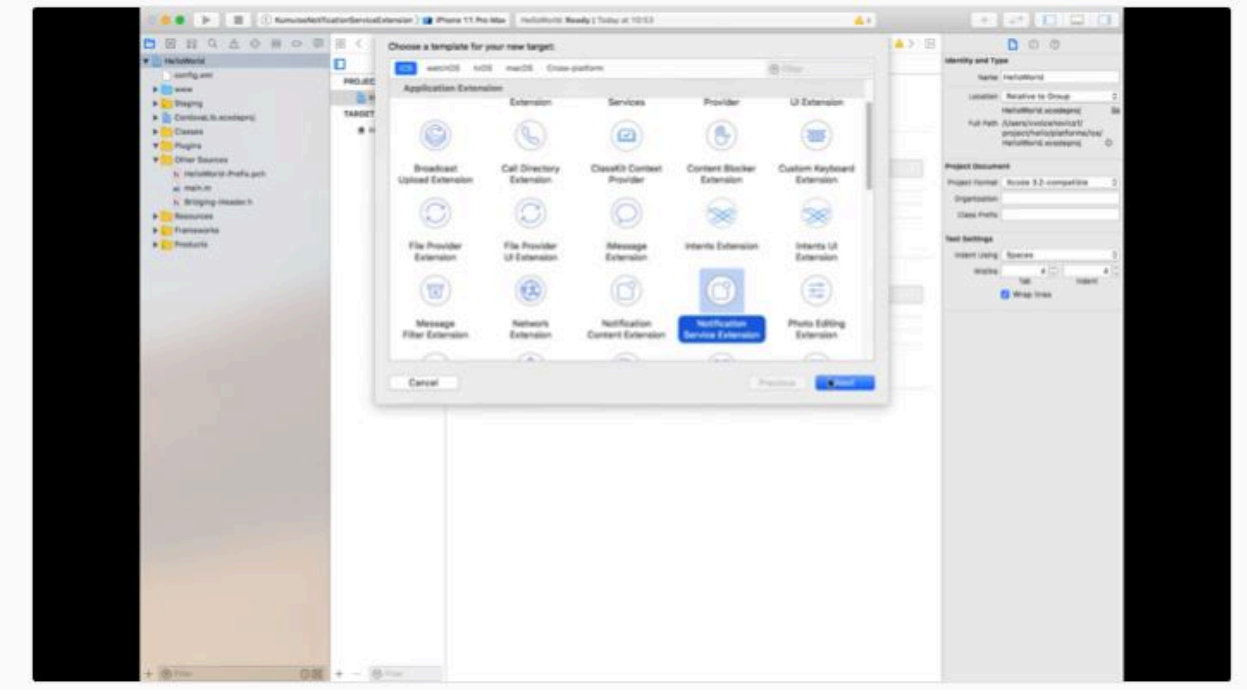
Um alle Funktionen des Apple Push-Benachrichtigungsdienstes zu unterstützen, muss Ihre App über eine Erweiterung für den Benachrichtigungsdienst verfügen, um eine eingeschränkte Verarbeitung der Benachrichtigung beim Empfang zu ermöglichen, bevor das Betriebssystem sie dem Benutzer präsentiert.

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

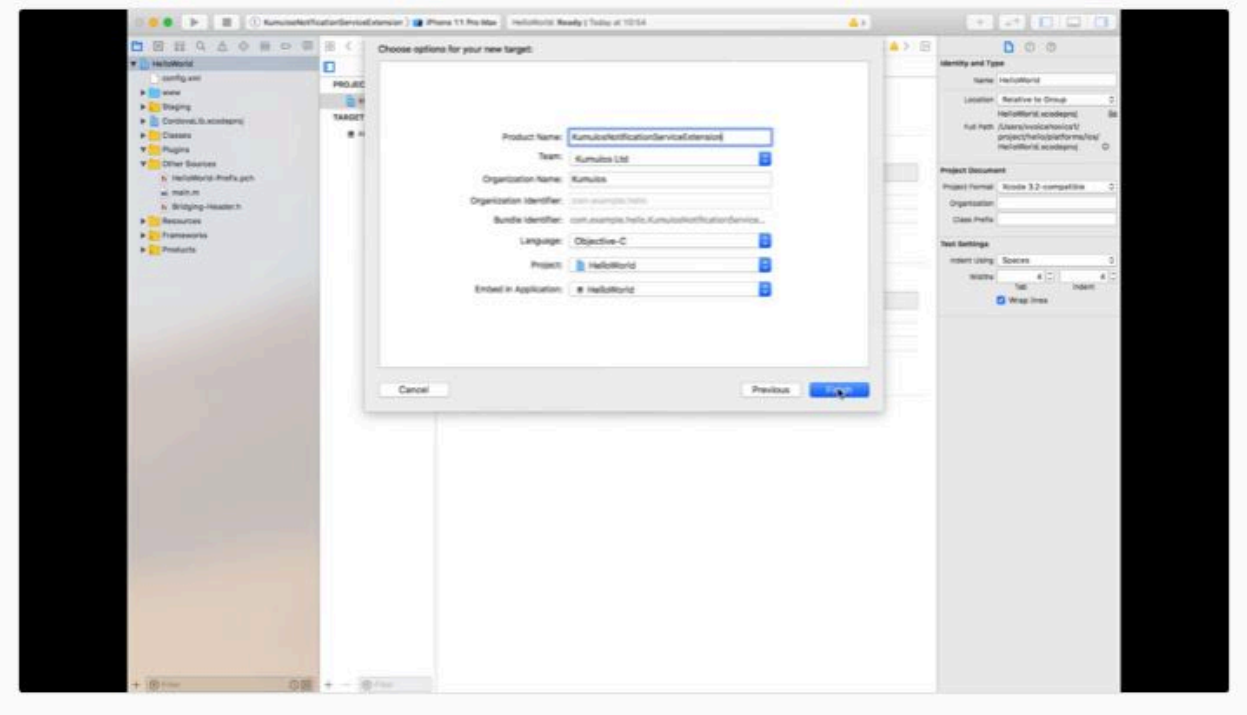


Wählen Sie im Popup-Fenster die

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



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




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

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

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

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

@interface NotificationService ()
@end

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

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

### App-Funktionalitäten und -Berechtigungen konfigurieren

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

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

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

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

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

### Vorgehensweise zum Testen Ihrer Konfiguration

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

## Initialisierung (Initialization)

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

In Ihrer `App.js`:

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

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

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

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

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

## Registrieren mit dem CRM

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

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

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

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

## Benutzerzuordnung

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

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

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

## Ereignisverfolgung

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

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

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

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

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

## Erweiterte In-App Funktionen

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

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

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

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

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

### Deep-Linking für In-App

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

### Verwenden Sie den In_App Posteingang

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

### Nachrichten abrufen

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

### Als gelesen markieren

Um eine einzelne oder alle Posteingangsnachrichten als gelesen zu markieren:

### Nachricht löschen

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

### Posteingang aktualisierter Handler

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

- Nachricht vom Server abgerufen
- Nachricht geöffnet

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

Sie können es wie folgt verwenden:

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

### Eine Zusammenfassung des Posteingangs erhalten

Sie können die Zusammenfassung des Posteingangs wie folgt abrufen:

### Rufen Sie die Bild-URL des Posteingangselements ab

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

## Erweiterte Features

### Offene Ereignisse oder Hintergrunddaten-Push-Benachrichtigungen verarbeiten

Der folgende Beispielcode zeigt die Verwendung von Kumulos zur Handhabung von Push-Benachrichtigungen für Deep Linking und andere allgemeine Nachrichten-Tasks.

```
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
    }
});
```

### Schaltflächen für Benachrichtigungsaktionen handhaben

Wenn ein Benutzer mit Ihrer Push-Nachricht interagiert, wird die oben definierte `pushOpenedHandler` aufgerufen. Wenn auf eine Schaltfläche getippt wurde, enthält das Benachrichtigungsobjekt eine `actionId`-Eigenschaft:

```
Kumulos.initialize({
```

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

# Kapitel 8. Dienstprogramme für Deliver

Deliver bietet mehrere Scripts, die Sie für die Verwaltung von Deliver -Aufgaben verwenden.

Sie können die in diesem Abschnitt beschriebenen Software-Dienstprogramme für eine Vielzahl von Start- und Verwaltungsfunktionen verwenden. Zusätzlich zu den mit Unica Platform verwendeten Software-Dienstprogrammen sind die von Unica Deliver verwendeten Dienstprogramme spezifisch für Deliver und Sie verwenden sie nur zum Verwalten von Deliver-Komponenten.

Weitere Informationen zu anderen Dienstprogrammen, die für Ihre HCL Unica-Installation verfügbar sind, finden Sie im Unica PlatformAdministratorhandbuch.

## Das RLU Skript

Prüfen Sie das Script RLU, um den Status des Uploaders der Empfängerliste (RLU) zu prüfen.

**Anmerkung:** Sie können dieses Script nicht zum Starten oder Stoppen der RLU verwenden. Verwenden Sie dieses Skript, um die Konnektivität zwischen „vor Ort“ und lokale Komponenten zu überprüfen.

Das RLU-Skript befindet sich im Ordner `<Deliver Install Home>/bin`. Das Verzeichnis Deliver ist ein Unterverzeichnis des Verzeichnisses Campaign.

Führen Sie in UNIX™- oder Linux™-Umgebungen das Script als `rct.sh`aus.

Führen Sie in Windows™ das Skript an der Eingabeaufforderung als `rlu.bat` aus.

### Syntax

```
RLU-c | --Prüfen [-h]
```

### Befehle

**-c, --überprüfen**

Prüfen Sie, ob die Sicherheitskontrolle korrekt konfiguriert ist und mit HCL Unica verbunden ist.

### Optionen

**-h,--Hilfe**

Syntax für das Script anzeigen

### Beispiel

Bestimmen Sie in einer Linux™-Umgebung, ob die RLU mit HCL Unica gehosteten Diensten verbunden ist.

```
RLU.sh--prüfen
```

Abhängig vom Status Ihres Systems könnte die Ausgabe dieses Befehls wie folgt aussehen:

```
Configuring Data Source [systemTables]...
Testing configuration for partition partition1
Testing connectivity for partition partition1
Testing user accessibility for partition partition1
Succeeded. List uploader config and connectivity test
succeeded for partition partition1
```

# Deliver Response and Contact Tracker (RCT) Skript

Um bestehende Probleme in der vorherigen Version von RCT zu beheben, wurde die Kafka-Ebene eingeführt.

Mit diesem Script können Sie die Antwort- und Kontaktverfolgung (Response and Contact Tracker, RCT) ausführen und ihren Status überprüfen.

Dieses Script befindet sich im Verzeichnis `bin` unter Ihrer Deliver Installation. Das Verzeichnis Deliver ist ein Unterverzeichnis des Verzeichnisses Campaign.

Führen Sie das Skript in UNIX™ oder Linux™ Umgebungen als `rct.sh` aus.

Führen Sie unter Windows™ das Skript über die Befehlszeile als `rct.bat` aus.

## Syntax

```
rct [ starten | stoppen | prüfen ]
```

## Befehle

**start**

Startet die RCT.

**stop**

Stoppt die RCT

## Optionen

**Prüfen**

Überprüfen Sie den Status der Verbindung zwischen der RCT und den HCL Unica Hosted Services.

## Beispiele

- Um die RCT auf Windows™ zu starten.

  ```
  rct.bat start
  ```

- Um die RCT auf Windows™ zu stoppen.

  ```
  rct.bat stop
  ```

- In einer Linux™ Umgebung, um festzustellen, ob das RCT mit HCL Unica gehosteten Diensten verbunden ist.

  ```
  rct.sh check
  ```

  Abhängig vom Status Ihres Systems könnte die Ausgabe dieses Befehls wie folgt aussehen:

  ```
  C:\ <UNICA_HOME> \Campaign\Deliver\bin>rct check Testen von Konfiguration und Verbindung für Partition
   partition1 Erfolgreich | Partition: Partition1 – Konto-ID für gehostete Dienste: asm_admin
  ```

# Das Script MKService_rct

Durch das Script "MKService_rct" wird die Antwort- und Kontaktverfolgung (Response and Contact Tracker, RCT) als ein Service hinzugefügt oder entfernt. Wenn Sie die RCT als Service hinzufügen, wird die RCT bei jedem Neustart des Computers, auf dem Sie die RCT installiert haben, automatisch gestartet. Wenn Sie die RCT als Service entfernen, wird der automatische Neustart der RCT verhindert.

Dieses Script befindet sich im Verzeichnis `bin` unter Ihrer Deliver-Installation.

Führen Sie in UNIX™ oder Linux™-Umgebungen `MKService_rct.sh.` mit einem Benutzer aus, der über Root-Berechtigungen verfügt oder berechtigt ist, Daemon-Prozesse zu erstellen.

Führen Sie in Windows™ das Script von der Befehlszeile aus als `MKService_rct.bat`aus.

## Syntax

```
MKService_rct -install

MKService_rct -remove
```

## Befehle

**-install**

Fügt die RCT als Service hinzu.

**-remove**

Entfernt den RCT-Service.

## Beispiele

- Um den RCT als Windows™-Service hinzuzufügen.

  ```
  MKService_rct.bat -install
  ```

- Um den RCT-Service auf UNIX™ oder Linux™ zu entfernen.

```
MKService_rct.sh -remove
```

# configTool

Die Eigenschaften und Werte auf der Seite **Konfiguration** werden in den Platform-Systemtabellen gespeichert. Sie können das Dienstprogramm `configTool` verwenden, um Konfigurationseinstellungen aus den Systemtabellen zu importieren oder exportieren. Weitere Informationen finden Sie im Platform Administratorhandbuch.

# Kapitel 9. Informationen zur Fehlerbehebung Deliver

Unica Deliver stellt verschiedene Tools und Techniken bereit, mit denen Sie Probleme in Bezug auf Ihre Campaign und Deliver-Installationen untersuchen können.

## Protokolldateien für Deliver

HCL Unica bietet mehrere Protokolldateien, die Sie überprüfen können, um Ihre Deliver-Installation zu überwachen und Probleme zu untersuchen.

### Deliver-Protokolldatei

Dieses Protokoll enthält die folgenden Arten von Informationen zu den Informationen, die von HCL Unica gehosteten Services heruntergeladen wurden. Befindet sich im `Protokoll`verzeichnis unter Ihrer Deliver-Installation.

- allgemeine Mailing-Informationen
- ID der Mailinstanz
- Klicken Sie auf Daten
- Daten für abgeprallte E-Mails

### Temporäre Deliver Dateien

Dieses Verzeichnis enthält die Daten, die hochgeladen werden.

Befindet sich im `temp` Verzeichnis unter Ihrer Deliver-Installation.

### Campaign-Protokolldateien

Sie können Protokolldateien an den folgenden Speicherorten auf Informationen zu Mailing-bezogenen Aktivitäten in Campaign überprüfen.

- `Campaign\partitions\<partitionN>\logs`

  Verschiedene Protokolldateien, die sich auf Ablaufdiagrammausführungen beziehen, einschließlich Protokolleinträgen aus jedem im Ablaufdiagramm enthaltenen Lieferprozess.

- `Campaign\Protokolle`

  Dieses Verzeichnis enthält `campaignweb.log`, das Informationen zur Uploadaktivität enthält, die vom Uploader der Empfängerliste ausgeführt wird.

## Log4j mit Deliver verwenden

Deliver Verwendet das Dienstprogramm Apache log4j zum Protokollieren von Konfigurations-, Debugging- und Fehlerinformationen in Bezug auf die Antwort- und Kontaktverfolgung (RCT) und den Empfängerlistenuploader (RLU).

Informationen zum Ändern der Systemprotokolleinstellungen finden Sie unter:

- Den Anmerkungen in der Datei log4j.xml.
- Der Dokumentation zu log4j auf der Apache-Website: https://logging.apache.org/log4j/2.x/manual/index.html

### Log4j mit dem Uploader der Empfängerliste verwenden

Wenn Sie das RLU-Dienstprogramm (Recipient List Uploader) über die Befehlszeile ausführen, werden die Standardeinstellungen für den Logger verwendet.

Um diese Einstellungen zu ändern, ändern Sie die Datei `deliver_rlu_log4j.xml`.

Ändern Sie `deliver_rlu_log4j.xml` gemäß den Anweisungen in dieser Datei. Sie dürfen diese Datei nur ändern, wenn Sie von der HCL-Support vorgeschlagen wird.

Wenn die RLU automatisch von einem Flussdiagramm aufgerufen wird, verwendet sie die Protokollierung der Campaign-Webanwendung, die `campaign_log4j.xml` in Ihrem Campaign-Installationsverzeichnis konfiguriert ist.

### Verwenden von log4j mit der Antwort- und Kontaktverfolgung

Wenn Sie das Dienstprogramm „Response and Contact Tracker (RCT)“ ausführen, werden die Standardeinstellungen für den Logger verwendet.

Um diese Einstellungen zu ändern, ändern Sie die Datei `deliver_rct_log4j.xml`.

Ändern Sie `deliver_rct_log4j.xml` gemäß den Kommentaren in dieser Datei.

## Zielseite

Falls nach der Erstellung einer bestimmten Zielseite, unerwartete oder keine Werte in der Tabelle UCC_RESPONSEATTR für eines der Formularfelder angezeigt werden, führen Sie zur Lösung die folgenden Schritte aus

.

1. Öffnen Sie den Nachrichteneditor und suchen Sie die Zielseite.

2. Klicken Sie mit der rechten Maustaste auf **Inhalt bearbeiten**, klicken Sie auf die Registerkarte **Link**, wählen Sie das in der Dropdown-Liste „Formular absenden (optional)“ definierte Formular aus, und klicken Sie auf **OK**.

3. Speichern Sie und veröffentlichen Sie die Zielseite.

4. Senden Sie die Mail erneut. Dadurch wird sichergestellt, dass alle Formularfeldwerte in der Tabelle UCC_RESPONSEATTR für die Zielseite hinzugefügt werden.

**Note:**

Diese Schritte sind im Schnellentwurfsmuster nicht erforderlich.

# Kapitel 10. Verwaltung des Benutzerzugriffs auf Nachrichtennachrichtenfunktionen

Campaign und Deliver verwenden Sie Rollen und Berechtigungen von Unica Platform, um den Benutzerzugriff auf Nachrichtenfunktionen in Deliver und Campaign zu steuern. Sie müssen über Berechtigungen in verfügen Unica Platform und Campaign die erforderlichen Änderungen vornehmen. Sie müssen auch mit dem Konfigurieren von Rollen und Berechtigungen im Platform und dem Definieren von Sicherheitsrichtlinien für Campaign vertraut sein.

Um E-Mail-Marketingkampagnen durchzuführen, greifen E-Mail-Marketer auf Deliver Mailing-Funktionen in Unica Campaign zu.

Um personalisierte Kommunikation und gehostete Zielseiten zu erstellen, arbeiten Marketer mit Funktionen und Inhalten im Deliver Dokumentkomponisten.

Allgemeine Informationen zum Konfigurieren von Rollen, Berechtigungen und Richtlinien finden Sie in den Abschnitten des Unica PlatformAdministratorhandbuchs, in denen beschrieben wird, wie die Sicherheit in Unica Platform und Unica Campaign verwaltet wird.

## Rollen- und Richtlinienzuweisung für Mailingzugriff

Um sich beim HCL Unica-System anzumelden, geben Marketer eines Systems einen Systembenutzernamen und ein Kennwort ein. Die Berechtigungen, die dem Systembenutzer erteilt werden, bestimmen, wie der Marketer auf Mailfunktionen, personalisierte Kommunikation und Inhalte in Deliver und Campaign zugreifen kann.

Berechtigungen sind Rollen zugeordnet, die in Unica Platform definiert sind. Um den Zugriff auf Mailfunktionen in Campaign zu steuern, können Sie Rollen innerhalb einer oder mehrerer Sicherheitsrichtlinienstrategien definieren. Allen Systembenutzern, die auf Mailing Features, Kommunikation und Inhalt zugreifen, muss eine Deliver Rolle innerhalb einer Campaign Sicherheitsrichtlinie zugewiesen werden. Über die Richtlinie müssen Sie die Berechtigungen für das Mailing von Features in Campaign und die Kommunikation und den Inhalt im Deliver Dokumentkomponisten selektiv anwenden.

Benutzern, die auf Mailingfunktionen zugreifen, müssen auch die Deliver-Benutzer- und Administratorrollen zugewiesen werden. Diese Rollen sind von den in Campaign-Sicherheitsrichtlinien verfügbaren Deliver-Rollen getrennt.

### Rollen und Berechtigungen in Platform und Campaign

Rollen in Platform und Campaign sind eine konfigurierbare Sammlung von Berechtigungen. Sie können für jede Rolle in Platform und Campaign Berechtigungen festlegen, mit denen der Zugriff auf die Anwendung gesteuert wird.

Sie können die Standardrollen verwenden oder neue Rollen erstellen. Die verfügbaren Berechtigungen werden vom System definiert; Sie können keine neue Berechtigung erstellen.

### Informationen über Rollenzuordnungen

Normalerweise werden Benutzer mit den Berechtigungen ausgestattet, die den Funktionen entsprechen, die dieser in der Organisation ausführt, wenn er HCL Unica verwendet. Sie können Rollen an Gruppen oder an einzelne Benutzer zuordnen. Der Vorteil der Rollenzuordnung nach Gruppe besteht darin, dass Sie eine Kombination aus Rollen der Gruppe zuordnen können. Wenn Sie an dieser Kombination zu einem späteren Zeitpunkt etwas ändern möchten, können Sie dies in einem Mal tun und müssen diesen Vorgang nicht mehrmals für verschiedene Benutzer ausführen. Wenn Sie Rollen nach Gruppe zuordnen, können Sie Benutzer den Gruppen hinzufügen oder sie daraus entfernen, um den Benutzerzugriff zu steuern.

### Auswertung von Rollen

Wenn ein Benutzer über mehrere Rollen verfügt, wertet das System die Berechtigungen aus all diesen Rollen zusammen aus. Die Möglichkeit eines Benutzers, eine Funktion für ein bestimmtes Objekt auszuführen, wird dann entsprechend der aggregierten Berechtigungen aus allen Rollen gewährt oder verweigert. Im Fall von Campaign wird die Möglichkeit, eine Funktion für ein bestimmtes Objekt auszuführen, auf der Grundlage der Sicherheitsrichtlinie des Objekts gewährt oder verweigert.

## Funktionsweise von Sicherheitsrichtlinien

Sicherheitsrichtlinien sind die "Regelbücher", mit denen die Sicherheit in Ordnern und Objekten in Campaign geregelt wird. Sie werden jedes Mal zu Rate gezogen, wenn ein Benutzer in der Anwendung eine Aktion durchführt.

Sie können eigene Sicherheitsrichtlinien erstellen oder die globale Standardsicherheitsrichtlinie verwenden, die in Campaign verfügbar ist.

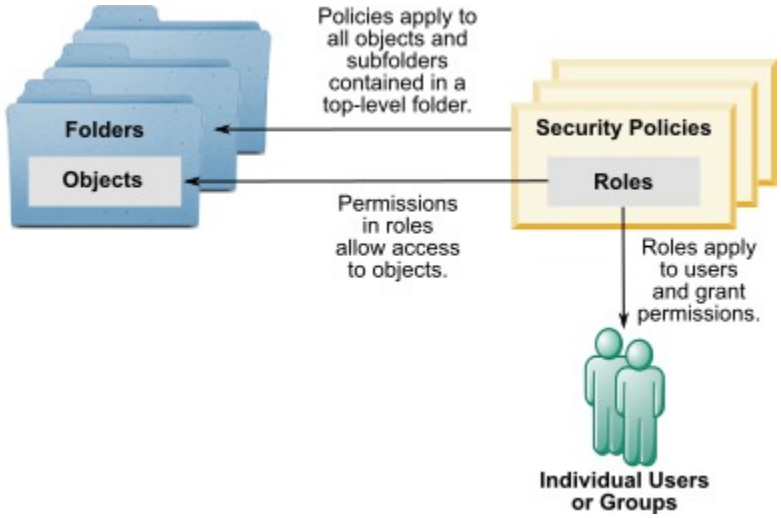
In Campaign werden Sicherheitsrichtlinien Ordnern zugeordnet. Wenn Sie einen Ordner der höchsten Ebene erstellen, müssen Sie eine Sicherheitsrichtlinie auf den Folder anwenden. Alle Objekte oder Unterordner innerhalb dieses Ordners übernehmen die Sicherheitsrichtlinie des Ordners.

Da der Ordner der höchsten Ebene die Sicherheitsrichtlinie für die Objekte im Ordner bestimmt, können Sie Objekten nicht direkt eine Sicherheitsrichtlinie zuordnen. Um die Sicherheitsrichtlinie eines Objekts zu ändern, müssen Sie das Objekt in einen Ordner mit der gewünschten Sicherheitsrichtlinie oder in den Stammordner der obersten Ebene verschieben.

Sie können eine Sicherheitsrichtlinie auch nicht direkt einem Benutzer zuordnen. Anders als bei Objekten und Ordnern, die Sicherheitsrichtlinien insgesamt zugeordnet sind, werden Benutzer Rollen innerhalb von Sicherheitsrichtlinien zugeordnet. Um die Aktivitäten von Benutzern zu steuern, ordnen Sie die Benutzer Rollen innerhalb der Sicherheitsrichtlinien zu. Auf diese Weise steuern Sie den Zugriff von Benutzern auf Objekte innerhalb von Ordnern, die diese Sicherheitsrichtlinien verwenden.

Wenn ein Benutzer nicht explizit mindestens einer Rolle in einer Sicherheitsrichtlinie zugeordnet wird, kann dieser Benutzer unter einem Ordner auf höchster Ebene, der diese Richtlinie verwendet, keine Ordner und Objekte erstellen. Zudem hat dieser Benutzer keinen Zugriff auf Objekte unter diesem Ordner oder seinen Unterordnern.

Im folgenden Diagramm wird die Beziehung zwischen Sicherheitsrichtlinien, Ordnern, Objekten, Rollen und Benutzern dargestellt.




### Verwaltungsrollen auf höchster Ebene

Jeder Partition sind in Unica Campaign Verwaltungsrollen zugeordnet. Benutzer mit diesen Rollen können die zulässigen Aktionen bei allen Objekten in der Partition durchführen, unabhängig von der Sicherheitsrichtlinie, die in den Ordnern mit den Objekten verwendet wird.

### Sicherheitsrichtlinien und Partitionen

Sicherheitsrichtlinien werden pro Partition erstellt. Sie können nicht partitionsübergreifend gemeinsam genutzt werden.

Jede Partition in Unica Campaign kann über mehrere Sicherheitsrichtlinien verfügen.

### Änderungen von Sicherheitsrichtlinien bei Verschieben oder Kopieren von Ordnern und Objekten

Objekte und Ordner können zwischen verschiedenen Richtlinien verschoben oder kopiert werden. Der Benutzer, der die Aktion ausführt muss jedoch über Berechtigungen hierfür verfügen – sowohl in der Quell- als auch in der Zielrichtlinie.

Nachdem ein Objekt oder Ordner in einen Ordner verschoben oder kopiert wurde, der von seiner Quelle einer anderen Sicherheitsrichtlinie zugeordnet wurde, wird die Sicherheitsrichtlinie der Objekte der unteren Ebene oder der Unterordner automatisch zur Sicherheitsrichtlinie der neuen Ordner umgeändert.

## Globale Sicherheitsrichtlinie

Campaign umfasst eine globale Standardsicherheitsrichtlinie. Sie können diese Richtlinie nicht löschen; sie gilt immer. Sie können Ihr Sicherheitsschema jedoch wie folgt anpassen.

- Ändern Sie die Rollen und Berechtigungen in der globalen Richtlinie, um sie an die Bedürfnisse Ihres Unternehmens anzupassen.
- Erstellen Sie benutzerdefinierte Richtlinien und ordnen Sie Benutzer nicht der globalen Richtlinie, sondern nur Ihren benutzerdefinierten Richtlinien zu.
- Verwenden Sie benutzerdefinierte Richtlinien und die globale Richtlinie.

Alle von Ihnen erstellten benutzerdefinierten Richtlinien sind unter der globalen Richtlinie vorhanden. Wenn Sie keine eigenen Sicherheitsrichtlinien erstellen möchten, wird die globale Sicherheitsrichtlinie standardmäßig auf die Ordner und Objekte angewendet, die Benutzer in Campaign erstellen.

Die globale Sicherheitsrichtlinie enthält sechs vordefinierte Rollen. Sie können die vordefinierten Rollen zwar nicht löschen, Sie können aber ihre Berechtigungen ändern.

Zu den vordefinierten Rollen in der globalen Sicherheitsrichtlinie zählen:

- **Folder Owner** - Alle Berechtigungen, die für die von einem Benutzer erstellten Ordner aktiviert wurden. Alle Benutzer verfügen über diese Rolle; Sie müssen ihr keine Benutzer zuordnen.
- **Owner** - Alle Berechtigungen, die für die von einem Benutzer erstellten Objekte aktiviert wurden. Alle Benutzer verfügen über diese Rolle; Sie müssen ihr keine Benutzer zuordnen.
- **Admin** - Alle Berechtigungen sind aktiviert. Der Standardbenutzer `asm_admin` hat diese Rolle.
- **Execute** - Alle Berechtigungen sind aktiviert.
- **Design** - Lese- und Schreibberechtigungen für alle Objekte. Mit dieser Rolle können keine Ablaufdiagramme oder Sitzungen geplant werden.
- **Review** - Leseberechtigungen.

## Deliver Rollen in der globalen Richtlinie

Zusätzlich zu den vordefinierten Campaign Rollen umfasst die globale Richtlinie mehrere Rollen, die spezifisch für Deliver sind.

Die globale Richtlinie umfasst die folgenden Deliver Rollen.

- **Deliver_admin** kann auf alle Mailfunktionen, den gesamten Inhalt und alle Dokumente zugreifen.
- **Deliver_execute** kann auf alle Mailfunktionen, den gesamten Inhalt und alle Dokumente zugreifen.
- **Deliver_design** kann auf alle Inhalte, alle Dokumente und die meisten Mailfunktionen zugreifen. Es wird jedoch explizit keine Berechtigung zum Senden von Produktionsmailings erteilt.
- **Deliver_review** kann nur Inhalte und Dokumente anzeigen und verfügt über eingeschränkte Berechtigungen für die Arbeit mit Mailings. Es wird explizit nicht die Berechtigung zum Hinzufügen, Bearbeiten oder Löschen von Mailings vergeben. Es ist zulässig, Test- und Produktionsmailings anzuzeigen und zu versenden.

**Anmerkung:** Deliver unterstützt nicht die Rollen für Eigentümer und Ordnereigentümer, die standardmäßig für Campaign erstellt wurden.

# Nachrichtenberechtigungen in Campaign

Campaign Steuert den Benutzerzugriff auf Mailingfunktionen, indem bestimmte Berechtigungen aktiviert oder deaktiviert werden, die in Rollen definiert sind, die einem Benutzer oder einer Gruppe zugewiesen sind. Diese Rollen sind einer oder mehreren Sicherheitsrichtlinienstrategien zugeordnet. Sie können mehrere Campaign Sicherheitsrichtlinien definieren und jeder Richtlinie mehrere Rollen zuweisen. Jede Kombination aus Richtlinien und Rollen kann eine bestimmte Berechtigungsgruppe definieren.

Weitere Informationen zur Vorgehensweise bei der Verwaltung von Sicherheitsberechtigungen, einschließlich Mustersicherheitsszenarios, finden Sie im Unica Campaign-Administratorhandbuchs.

Unter Rollen und Berechtigungen für Unica Platform können Sie die Benutzerberechtigungen für Mailfunktionen und -Inhalte im Campaign Abschnitt wie folgt zuweisen.

1. Definieren Sie Benutzerrollen.

   Systemdefinierte Benutzerrollen für Deliver werden standardmäßig in der globalen Richtlinie erstellt.

   Sie können auch benutzerdefinierte Rollen definieren und sie zur globalen Richtlinie oder zu anderen von Ihnen definierten Richtlinien hinzufügen.

2. Definieren Sie Sicherheitsregeln und fügen Sie den Regeln Benutzerrollen hinzu.

   Die globale Richtlinie ist standardmäßig definiert. Sie können zusätzliche Datenschutzrichtlinien für Campaign definieren.

3. Definieren Sie für jede Rolle in jeder Richtlinie bestimmte Berechtigungen.

   Sie können zusätzliche Datenschutzrichtlinien und benutzerdefinierte Rollen mit verschiedenen Berechtigungsgruppen definieren, um den Zugriff auf Mailfunktionen in Campaign und den Deliver Dokumentkomponisten zu kontrollieren.

Änderungen an Berechtigungen, Rollen und- Datenschutzrichtlinien werden angewendet, wenn sich der Benutzer bei HCL Unica anmeldet. Nachdem Sie die Mailberechtigungen für einen Benutzer zugeordnet oder geändert haben, muss sich der Benutzer abmelden und sich anschließend wieder anmelden, damit die Änderungen beachtet werden.

## Rollen und Berechtigungen zur Verfügung stellen

Abhängig von Ihrer Unica Platform Installation sind die Verwaltungssteuerelemente, die zum Definieren und Anwenden von Rollen und Berechtigungen erforderlich sind, möglicherweise nicht sofort sichtbar. Sie können die erforderlichen Steuerelemente sichtbar machen, indem Sie auf den Deliver Dokumentkomponisten oder ein Mailing in Campaign zugreifen.

Führen Sie die folgende Prozedur aus, wenn Sie nicht alle folgenden Berechtigungen in der Campaign globalen Richtlinie sehen.

- Berechtigungen für Mailings in der Kampagnenkategorie
- Berechtigungen für die Inhaltsbibliothek in der digitalen Assets-Kategorie
- Berechtigungen für Deliver Dokumente in der Dokumente-Kategorie

1. Melden Sie sich bei HCL Unica an.

   Wenn Sie mehrere Benutzer konfiguriert haben, melden Sie sich als Benutzer mit den eingeschränktesten Berechtigungen an. Melden Sie sich beispielsweise als Benutzer mit nur Ansichtsberechtigungen an.

2. Navigieren Sie zu **Campaign** > **Deliver Dokumente** für den Zugriff auf den Dokumentkomponisten.

   Warten Sie, bis der Dokumentkomponist das Laden beendet hat.

3. Navigieren Sie zu **Einstellungen** > **Benutzerrollen und Berechtigungen** > **Kampagne** > **Partition [n]** > **Globale Richtlinie**

   Bestätigen Sie bei einer Aufforderung, dass Sie den Dokumentkomponisten verlassen möchten, indem Sie die Seite verlassen.

4. Klicken Sie auf **Rollen hinzufügen und Berechtigungen zuweisen**. Die folgenden Deliver Rollen sind sichtbar.
   - deliver_admin
   - deliver_execute
   - deliver_design
   - deliver_review
5. Klicken Sie auf **Berechtigungen speichern und bearbeiten**.

   Die Mailberechtigungen sind in den Kategorien Kampagne, digitale Assets und Dokumente sichtbar.

   Weitere Informationen zu den verfügbaren Berechtigungen finden Sie in den folgenden Abschnitten.

## Evaluierung von Berechtigungen in Campaign

Wenn ein Benutzer eine Aufgabe ausführt oder versucht, auf ein Objekt zuzugreifen, werden in Campaign folgende Schritte ausgeführt.

1. Bestimmen aller Gruppen und Rollen, denen ein Benutzer innerhalb der globalen Sicherheitsrichtlinie angehört.

   Benutzer können einer, mehreren oder keiner Rolle angehören. Benutzer gehören der Rolle "Owner" an, wenn sie ein Objekt besitzen; sie gehören der Rolle "Folder Owner" an, wenn sie den Ordner besitzen, in dem sich ein Objekt befindet.

   Benutzer gehören nur dann anderen Rollen an, wenn Sie diesen Rollen eindeutig zugeordnet wurden (entweder direkt oder aufgrund der Zugehörigkeit ihrer Gruppe zu dieser Rolle).

2. Bestimmen, ob das Objekt, auf das zugegriffen wird, einer benutzerdefinierten Richtlinie angehört. Wenn das der Fall ist, werden vom System alle Gruppen und Rollen angegeben, denen ein Benutzer innerhalb dieser benutzerdefinierten Richtlinie angehört.
3. Fasst die Berechtigungen für alle Rollen zusammen, denen der Benutzer angehört, basierend auf Ergebnissen der Schritte 1 und 2. Anhand der zusammengefassten Rolle prüft das System die Berechtigungen für die Aktion wie folgt:
    a. Wenn Rollen die Berechtigung **Verweigert** für diese Aktion haben, werden die Berechtigungen wie folgt zusammengefasst:
        i. Angenommen, Sie haben eine globale Richtlinie, eine benutzerdefinierte Richtlinie und eine VERWEIGERTE Berechtigung für die benutzerdefinierte Richtlinienrolle. In diesem Fall hat die VERWEIGERUNG der Berechtigung für die benutzerdefinierte Richtlinienrolle Vorrang vor Berechtigungen, die der globalen Richtlinienrolle zugeordnet sind.
        ii. Angenommen, Sie haben eine globale Richtlinie, zwei oder mehr benutzerdefinierte Richtlinien, eine VERWEIGERTE Berechtigung für eine der benutzerdefinierten Richtlinienrollen und die gleiche ERTEILTE Berechtigung für die andere benutzerdefinierte Richtlinienrolle. In diesem Fall hat die ERTEILUNG der Berechtigung für die benutzerdefinierte Richtlinie Vorrang vor der VERWEIGERUNG der Berechtigung für die benutzerdefinierte Richtlinie.
    b. Wenn keine Rollen die Berechtigung **Verweigert** für diese Aktion haben, wird geprüft, ob Rollen die Berechtigung **Erteilt** für diese Aktion haben. Falls ja, kann der Benutzer die Aktion ausführen.
    c. Wenn weder A noch B zutreffen, wird dem Benutzer die Berechtigung verweigert.

### Beispiel für eine benutzerdefinierte Richtlinie

Angenommen, Sie haben eine benutzerdefinierte Richtlinie unter der globalen Richtlinie: BenutzerdefinierteRichtlinieA. Die BenutzerdefinierteRichtlinieA hat die BenutzerdefinierteRichtlinienrolleA mit einer VERWEIGERTEN Berechtigung zum Hinzufügen/Bearbeiten von Kampagnen.

Angenommen, BenutzerA wurde die BenutzerdefinierteRichtlinienrolleA zugeordnet. Die VERWEIGERUNG der Berechtigung zum Hinzufügen/Bearbeiten von Kampagnen für die BenutzerdefinierteRichtlinienrolleA hat Vorrang vor Berechtigungen, die der globalen Richtlinienrolle zugeordnet sind. Dementsprechend sind die Objekte zum Hinzufügen/Bearbeiten von Kampagnen für BenutzerA nicht sichtbar.

### Beispiel für zwei benutzerdefinierte Richtlinien

Betrachten Sie zwei benutzerdefinierte Richtlinien unter Globale Richtlinie: CustomPolicyA und CustomPolicyB. Sowohl die BenutzerdefinierteRichtlinieA als auch die BenutzerdefinierteRichtlinieB haben die Rollen BenutzerdefinierteRichtlinienrolleA bzw. BenutzerdefinierteRichtlinienrolleB. Die BenutzerdefinierteRichtlinienrolleA hat eine ERTEILTE Berechtigung zum Hinzufügen/Bearbeiten von Kampagnen. Die BenutzerdefinierteRichtlinienrolleB hat eine VERWEIGERTE Berechtigung zum Hinzufügen/Bearbeiten von Kampagnen.

BenutzerA sind sowohl die BenutzerdefinierteRichtlinienrolleA als auch die BenutzerdefinierteRichtlinienrolleB zugeordnet. In diesem Fall hat die ERTEILUNG der Berechtigung für die BenutzerdefinierteRichtlinienrolleA Vorrang vor der VERWEIGERUNG der Berechtigung für die BenutzerdefinierteRichtlinienrolleB. Dementsprechend sind die Objekte zum Hinzufügen/Bearbeiten von Kampagnen für BenutzerA sichtbar.

## Definitionen von Berechtigungsstatus

Für jede Rolle können Sie festlegen, welche Berechtigungen gewährt, nicht gewährt oder verweigert werden. Diese Berechtigungen legen Sie auf der Seite **Einstellungen > Benutzerrollen und Berechtigungen** fest.

Die Status haben die folgende Bedeutung.

- **Gewährt** - gekennzeichnet durch ein Häkchen  . Berechtigungen werden explizit gewährt, um diese bestimmte Funktion auszuführen, solange keine der anderen Rollen des Benutzers die Berechtigung verweigert.
- **Verweigert** - gekennzeichnet durch ein "X"  . Berechtigungen zum Ausführen dieser Funktion werden explizit verweigert, unabhängig von den anderen Rollen des Benutzers, die die Berechtigung gewähren.
- **Nicht gewährt** - gekennzeichnet durch einen Kreis  . Berechtigungen werden weder explizit gewährt noch verweigert, um eine bestimmte Funktion auszuführen. Wenn diese Berechtigung nicht explizit durch eine der Benutzerrollen gewährt wird, ist der Benutzer nicht berechtigt, diese Funktion durchzuführen.

## Berechtigungen für Mailings in Campaign

In Campaign erstellen, konfigurieren, führen und überwachen Sie Deliver Mailings mit Steuerelementen auf den Deliver Registerkarten für das Mailing. Sie verwalten jedes Mailing auf einer separaten Registerkarte.

Die folgenden Berechtigungen steuern den Benutzerzugriff auf die Deliver Registerkarten für das Mailing. Sie befinden sich in der Kategorie **Kampagne**.

| Berechtigung | Beschreibung |
|---|---|
| Mailings anzeigen | Ermöglicht es einem Benutzer, eine Deliver Registerkarte „Mailing“ in einer Kampagne anzuzeigen. Der Benutzer kann das Mailing nicht bearbeiten oder ändern. |
| Mailings bearbeiten | Ermöglicht es einem Benutzer, eine Registerkarte Deliver Mailing in einer Kampagne zu konfigurieren oder zu ändern. |
| Mailings löschen | Ermöglicht es einem Benutzer, ein Deliver Mailing aus einer Kampagne zu entfernen. |
| Mailings hinzufügen | Ermöglicht es einem Benutzer, ein Mailing in einer Kampagne zu erstellen. |
| Produktions-Mailing senden | Ermöglicht es einem Benutzer, eine Produktion des Mailing zu starten, ein Mailing für Transaktions-E-Mail zu aktivieren oder eine Ausführung des Mailing für eine Produktion zu planen.<br><br>Die Produktion von Ausgaben kann viele Nachrichten enthalten. E-Mail-Nachrichten werden an jede Person gesendet, die als Produktionsempfänger in der Empfängerliste angegeben ist, die dem Mailing zugeordnet ist. |
| Testlauf ausführen | Ermöglicht es einem Benutzer, einen Testlauf des Mailings zu starten. |

| Berechtigung | Beschreibung |
|---|---|
| | Testmailings sind in der Regel mit einigen Nachrichten verbunden. Während eines Testlaufs wird eine E-Mail-Nachricht an jede Adresse gesendet, die als Testempfänger in der Empfängerliste angegeben ist, die mit dem Mailing verbunden ist. |

## Berechtigungen für die Digitale Assets-Kategorie

Die Berechtigungen für digitale Assets steuern den Benutzerzugriff auf Inhaltselemente in der Deliver Inhaltsbibliothek sowie auf Ordner und Unterordner, in denen Sie gespeichert werden.

Die Inhaltsbibliothek ist eine Repository für Inhaltselemente (auch als digitale Assets bezeichnet), die in der Kommunikation eingesetzt werden, die Benutzer im Deliver Dokumentkomponisten erstellen.

| Berechtigungen | Beschreibung |
|---|---|
| Deliver Digitale Assets anzeigen | Ermöglicht es einem Benutzer, Inhaltselemente zum Anzeigen von Eigenschaften zu öffnen und den Inhalt, der zu einer personalisierten Kommunikation hinzugefügt werden kann, zur Vorschau anzuzeigen. |
| Erstellen Sie neue digitale Assets in der Deliver-Inhaltsbibliothek | Ermöglicht es einem Benutzer, ein Inhaltselement zu erstellen und es der Inhaltsbibliothek hinzuzufügen. |
| Bearbeiten Sie vorhandene digitale Assets in der Deliver-Inhaltsbibliothek | Ermöglicht es einem Benutzer, vorhandene Inhaltselemente zu öffnen und zu bearbeiten. |
| Löschen Sie digitale Assets aus der Deliver-Inhaltsbibliothek | Ermöglicht es einem Benutzer, ein Inhaltselement aus der Inhaltsbibliothek zu entfernen. |
| Digitale Assets von einem Ordner in einen anderen verschieben | Ermöglicht es einem Benutzer, Inhaltselemente innerhalb der Inhaltsbibliothek zu verschieben. Um ein Inhaltselement zu verschieben, müssen Sie die Berechtigungen für den Quell- und Zielordner zuweisen. |

## Berechtigungen für die Kategorie „Dokumente“

Die Berechtigungen in der Kategorie **Dokumente** steuern den Benutzerzugriff auf die Erstellung, Bearbeitung und Verwaltung personalisierter Kommunikationen im Deliver Dokumentkomponisten.

| Berechtigungen | Beschreibung |
|---|---|
| DeliverDokumente anzeigen | Ermöglicht es einem Benutzer, ein Dokument anzuzeigen, das zum Erstellen einer E-Mail , einer Mailanzeigebenachrichtigung oder einer gehosteten Landing-Page verwendet wird. |

| Berechtigungen | Beschreibung |
|---|---|
| Neue DeliverDokumente erstellen | Ermöglicht es einem Benutzer, eine neue personalisierte Kommunikation zu erstellen. |
| Vorhandene Deliver-Dokumente bearbeiten | Ermöglicht es einem Benutzer, eine vorhandene personalisierte Kommunikation zu ändern. |
| DeliverDokumente löschen | Ermöglicht es einem Benutzer, eine personalisierte Kommunikation zu entfernen. |
| Veröffentlichen Sie Deliver-Dokumente und stellen Sie Inhalte im öffentlichen Internet zur Verfügung | Ermöglicht es einem Benutzer, eine personalisierte Kommunikation zu veröffentlichen.<br>Durch das Publizieren einer Kommunikation werden das Dokument und alle hinzugefügten Inhalte zur Verwendung in einem Deliver Mailing verfügbar. |
| Kopieren Sie Deliver-Dokumente von einem Ordner in einen anderen | Ermöglicht es einem Benutzer, eine personalisierte Kommunikation zwischen Ordnern in der Inhaltsbibliothek zu kopieren.<br>Um eine Kommunikation zu kopieren, müssen Sie den Quell- und Zielordnern diese Berechtigung zuweisen. |
| DeliverDokumente von einem Ordner in einen anderen verschieben | Ermöglicht es einem Benutzer, eine personalisierte Kommunikation von einem Ordner in einen anderen Ordner in der Inhaltsbibliothek zu verschieben.<br>Wenn Sie eine Kommunikation verschieben, müssen Sie den Quell- und Zielordnern diese Berechtigung zuweisen. |

## Berechtigungen für die Kategorie E-Mail-Verwaltung

Mit den Berechtigungen in der Kategorie „E-Mail-Verwaltung“ der globalen CampaignRichtlinie erhalten Deliver-Administratoren Zugriff auf Einstellungen, die den Benutzerzugriff auf verschiedene Messaging-Domänen und Messaging-Funktionen steuern.

Administratoren weisen Domäne und Funktionszugriff im Abschnitt „Einstellungen“ des Deliver -Einstellungsfensters zu. Beispielsweise kann der Administrator die Liste der E-Mail-Domänen einschränken, die ein Benutzer in einer E-Mail-Kommunikation, die im Kommunikationseditor erstellt wird, als **Von:** -Domäne auswählen kann. Der Abschnitt Richtlinieneinstellungen wird nur angezeigt, wenn dem Administrator in der globalen Campaign Richtlinie ausdrücklich die entsprechende Berechtigung erteilt wurde.

Administratoren können auch den Zugriff auf Verwaltungsschnittstellen steuern, um mobile Apps bei Deliver zu registrieren und Standorte für die Verwendung mit standortgesteuerter Zustellung zu konfigurieren. Links zu den Verwaltungsseiten werden im Abschnitt Einstellungen für mobile Benachrichtigungen auf der Seite Deliver Einstellungen angezeigt. Mobile Messaging muss aktiviert sein, damit das gehostete Messaging-Konto den Abschnitt Einstellungen für mobile Benachrichtigungen auf der Seite Deliver-Einstellungen anzeigen kann.

| Berechtigungen | Beschreibung |
|---|---|
| Domänen konfigurieren | Steuert den Zugriff auf den Abschnitt Richtlinieneinstellungen auf der Seite Deliver-Einstellungen. Wenn die Rolle des Administrators nicht die Berechtigung zum Konfigurieren von Maildomänen erhält, kann der Administrator den Abschnitt „Richtlinieneinstellungen“ nicht anzeigen. Diese Berechtigung ist auch erforderlich, um Kurzlinkdomänen zu verwalten. |

# Nachrichtenberechtigungen für Deliver

Unica Deliver steuert den Zugriff auf Mailfunktionen außerhalb der Registerkarte „Mailing“ in Campaign über die folgenden vordefinierten Sicherheitsrollen.

- `deliver_admin`
- `Deliver_user`

Benutzer müssen beide Rollen haben, um Zugriff auf Deliver Mailfunktionen zu haben.

## Deliver-Rollen zuweisen

Um einem Benutzer vollen Zugriff auf Deliver Mailing-Funktionen zu gewähren, weisen Sie dem Benutzer die vordefinierten Deliver-Rollen zu.

1. Navigieren Sie in Unica Platform zu `Einstellungen > Benutzerrollen und Berechtigungen > Deliver > Partition [n] > Deliver_Admin`.
2. Klicken Sie auf **Benutzer zuweisen**.
3. Wählen Sie den Benutzer aus der Liste der verfügbaren Benutzer aus. Klicken Sie auf **Hinzufügen**, um dem Benutzer die Rolle zuzuordnen.
4. Wiederholen Sie die Schritte 1-3 für die Rolle `Deliver_user`.
5. Speichern Sie die Änderungen.

# Domänen und Kurzlinkdomänen steuern

Auf Anfrage konfiguriert Unica eine oder mehrere Maildomänen für Ihr gehostete E-Mail-Konto. Unica kann auch Domänen zuweisen, die Marketer für die Erstellung verkürzter Links in verschiedenen Arten von Nachrichten verwenden. Systemadministratoren mit entsprechenden Berechtigungen steuern die Nachrichtendomänen, die Markern zur Verfügung stehen.

Abhängig von Ihren Geschäftsanforderungen ist es möglicherweise wünschenswert, die von bestimmten Marketern verfügbare Auflistung von Nachrichtendomänen einzuschränken. Deliver Administratoren schränken die Auflistung verfügbarer Domänen durch Sicherheitsrichtlinienstrategien ein, die auf Ordner im Dokumentkomponisten angewendet werden. Die Möglichkeit für Marketer, E-Mail-Kommunikationen zu erstellen und zu bearbeiten, hängt von der Sicherheitsrichtlinie ab, die auf den Ordner angewendet wird, der die Kommunikation enthält.

Deliver Administratoren, die über entsprechende Berechtigungen verfügen, können die von Benutzern zu verwendende Auflistung von Maildomänen unter Deliver**Von:** Domäne in der E-Mail-Kommunikation verwenden. Administratoren können auch die Liste der Kurzlinkdomänen steuern, die Marketer bei der Konfiguration von Kommunikationen, die verkürzte Links verwenden, präsentiert werden. Beispielsweise können Sie angeben, welche Kurzlinkdomänen verfügbar sind, wenn Marketer Marketingnachrichten einen Link zum Teilen in sozialen Medien hinzufügen.

Deliver Administratoren verwenden die Seite **Richtlinieneinstellungen**, um Berechtigungen für die Verwendung bestimmter Nachrichtendatenbankdomänen zu erteilen. Der Zugriff auf die Seite **Richtlinieneinstellungen** wird durch die Benutzerverwaltungsberechtigungen gesteuert, die über die globale Campaign-Richtlinie erteilt werden. Nur Administratoren, die über die entsprechenden Berechtigungen verfügen, können den Zugriff auf Maildomänen über die Seite **Richtlinieneinstellungen** einschränken.

1. Wählen Sie im Menü **Einstellungen** die Option **Nachrichteneinstellungen**.
   Wenn Sie über die entsprechenden Administratorberechtigungen verfügen, wird der Abschnitt "Richtlinieneinstellungen" auf der Deliver Seite Einstellungen angezeigt.
2. Klicken Sie auf **eine Auflistung der Datenschutzrichtlinien und deren Einstellungen anzeigen**.
   Eine für Ihre Deliver Installation konfigurierte Sicherheitsrichtlinienliste wird angezeigt.
3. Klicken Sie auf eine Sicherheitsrichtlinie, die dem Systembenutzer zugeordnet ist, dessen Nachrichtendomänenzugriff Sie steuern möchten.

   Im Abschnitt Domänen werden die E-Mail-Domänen angezeigt, die für Ihr gehostetes Nachrichten-Konto konfiguriert sind.

   Im Abschnitt „Kurzlinkdomänen“ werden die Kurzlinkdomänen angezeigt, die für Ihr gehostete Nachrichtenkonto konfiguriert sind.

   - Klicken Sie in beiden Abschnitten auf **alle Domänen verwenden** , um Benutzern, die der Richtlinie zugeordnet sind, die Verwendung einer der von Unica für Ihr gehosteten E-Mail-Konto konfigurierten Maildomänen zu erteilen.

     Diese Option ist die Standardoption.
   - Klicken Sie auf **Bestimmte Domänen verwenden**, um bestimmte Domänen auszuwählen.

     **Anmerkung:** Wenn Sie **bestimmte Domänen verwenden**auswählen, müssen Sie die Domänenberechtigungen aktualisieren, wenn Sie eine neue E-Mail-Adresse oder eine kurze Domäne für Ihr gehostetes Nachrichtenkonto registrieren. Das System ordnet keine Berechtigungen für die neue Domäne automatisch zu.

Für die Benutzer, die der Sicherheitsrichtlinie zugeordnet sind, werden nur die ausgewählten Maildomänen als Option für das **Von:** angezeigt Adresse in der E-Mail-Kommunikation. Für Kommunikationen, für die verkürzte Links erforderlich sind, können Marketer nur in den von Ihnen ausgewählten Kurzlinkdomänen wählen.

Nach dem Speichern der neuen Einstellungen aktualisiert der Dokumentkomponist die Domäne, die Marketern zur Verfügung stehen.

Weitere Informationen zum Erstellen und Verwalten von Kommunikation durch Deliver-Marketer finden Sie im Unica DeliverBenutzerhandbuch.

### Wartung von gehosteten Maildomänen

Zum Senden von E-Mail-Nachrichten müssen Sie mindestens eine E-Mail Domäne mit Unica registrieren. Um die Zustellbarkeit von Nachrichten zu verbessern, arbeitet Unica mit Ihnen zusammen, um die E-Mail-Reputation der Domain bei führenden Internet Service Providern (ISPs) auf der ganzen Welt herzustellen und aufrechtzuerhalten. Sie können mit Unica mehrere E-Mail-Domänen einrichten.

Wenn Sie den Header in einer E-Mail-Kommunikation konfigurieren, füllt das System die Absenderadresse mit der E-Mail-Domäne, die Sie bei Unica registriert haben. Wenn Sie mit Unica mehrere E-Mail-Domänen einrichten, werden die verfügbaren Domänen in einer Dropdown-Liste angezeigt. Systemadministratoren können die E-Mail-Domänen steuern, die E-Mail-Marketer auswählen oder ändern können.

Sie können anfordern, dass Unica E-Mail-Domänen hinzufügt oder löscht, die für Ihr gehostetes Messaging-Konto eingerichtet wurden. Nachdem Unica die Änderung abgeschlossen hat, aktualisiert das System die Liste der verfügbaren E-Mail-Domänen Die Änderung wird in der Liste der verfügbaren E-Mail-Domänen angezeigt, wenn Sie das nächste Mal eine E-Mail-Kommunikation erstellen oder bearbeiten.

**Anmerkung:** E-Mail-Domänenänderungen für Ihr Konto aktualisieren nicht die E-Mail-Kommunikation, die Sie vor der Änderungsanforderung erstellt haben. Um die E-Mail-Domäne für eine zuvor erstellte Kommunikation zu ändern, müssen Sie die E-Mail-Kommunikation erneut öffnen und die Auswahl der E-Mail-Domäne aktualisieren.

Weitere Informationen zum Registrieren einer E-Mail-Domäne bei Unica finden Sie unter HCL UnicaDomänennamenoptionen für E-Mail.

Um Änderungen in Bezug auf Ihre E-Mail-Domänen anzufordern, wenden Sie sich über den technischen Support von HCL an das Unica Deliver Services-Team.

## Konfigurieren der Standardabsenderadresse und der Anzeigenamen

Für jede E-Mail-Domain, die Sie bei Unica registriert haben, können Sie eine Standard-E-Mail-Adresse und einen Standard-Anzeigenamen definieren. Die Kombination aus E-Mail-Adresse oder freundlichem Namen und der E-Mail-Domäne wird als Absender angezeigt: Adresse für die E-Mail-Nachrichten, die Sie senden.

Administratoren können den Standardabsender konfigurieren und Namen auf der Seite „Domäneneinstellungen“ anzeigen. Die Domäneneinstellungen sind Teil der Deliver -Einstellungen-Schnittstelle. Der Zugriff auf die Seite „Domäneneinstellungen“ wird durch die E-Mail-Verwaltungsberechtigungen gesteuert, die über die globale Campaign-Richtlinie erteilt werden. Nur Administratoren, die über die entsprechenden Berechtigungen verfügen, können den Zugriff auf Maildomänen über die Seite Richtlinieneinstellungen einschränken.

1. Wechseln Sie zu **Einstellungen** > **Deliver Einstellungen**. Klicken Sie im Abschnitt Domäneneinstellungen auf **Liste der Domäneneinstellungen anzeigen**.

   Auf der Seite Domäneneinstellungen werden die Standardanzeigenamen und E-Mail-Adressen aufgelistet, die den Maildomänen des gehosteten Benutzerkontos zugeordnet sind. Die Liste enthält nur die Domänen, die von ihren Benutzerberechtigungen geändert werden können.

   Die Standardspalte gibt die Kombination aus Anzeigename, Adresse und Domäne an, die als Standardeinstellung für die neue E-Mail-Kommunikation in der Von-Adresse erscheint.

2. Klicken Sie auf **Bearbeiten**  . Das Fenster „Domäneneinstellungen bearbeiten“ wird geöffnet.

   In der Spalte „Domänenname“ werden die verfügbaren Maildomänen aufgelistet. Sie können für jede der Domänen Folgendes tun.

   - Geben Sie in der Spalte Von-Anzeigename einen Anzeigenamen ein, der als Standard für eine E-Mail-Domäne in der Liste angezeigt wird.
   - Geben Sie in der Spalte Von-Adresse den lokalen Teil der E-Mail-Adresse ein, der als Standard für eine E-Mail-Domäne in der Liste angezeigt werden soll.

3. Wählen Sie optional in der Standardspalte eine Kombination aus Anzeigename und Domäne aus, die als Standardadresse für neue E-Mail-Kommunikation angezeigt werden soll.

   Wenn Sie keinen Standardwert auswählen, verwendet das System die erste Domäne in der Liste, um die Standard-Absenderadresse für die neue E-Mail-Kommunikation zu erstellen.

4. Speichern Sie die Änderungen.

Die neuen Adresseinstellungen gelten für alle neuen E-Mail-Kommunikationen, die Sie erstellen. Die Einstellungen ändern nicht die Adressinformationen für die zuvor erstellte E-Mail-Kommunikation. Um frühere E-Mail-Kommunikationen zu aktualisieren, müssen Sie jede Kommunikation erneut öffnen und ändern.

# Zugriff auf die Auflistung der gesendeten Nachrichten steuern

Deliver stellt eine Liste mit Nachrichten zur Verfügung, die aus Ihrer Deliver-Umgebung gesendet wurden. Da die Auflistung Links zu Nachrichtenkonfigurationen enthält, könnten Ihre Sicherheitspläne möglicherweise dazu führen, dass Sie den Zugriff auf die Liste einschränken.

Die Liste der Nachrichten wird auf der Seite **Nachrichtenübersicht** angezeigt. Standardmäßig können alle Benutzer in Ihrer Campaign- und Deliver-Umgebung die Liste der gesendeten Nachrichten anzeigen. Wenn Sie jedoch die Zugriffseinschränkung aktivieren, können Sie verhindern, dass bestimmte Benutzer die Menüoption sehen, um die Seite zu öffnen, die die Liste enthält.

Das Einschränken des Zugriffs auf die Liste der gesendeten Nachrichten wirkt sich auf alle Partitionen in Ihrer Campaign-Installation aus. Wenn Ihre Campaign Installation mehrere Partitionen umfasst, müssen Sie die Benutzerberechtigungen in jeder Partition gesondert aktualisieren, um die Berechtigung zum Zugriff auf die Liste explizit zu erteilen oder zu verweigern.

Um zu steuern, wer auf die Liste der gesendeten Nachrichten zugreifen kann, sind eine Reihe von Aufgaben erforderlich, um die Benutzerberechtigungen und die Systemkonfiguration zu ändern.

| Task | Weitere Informationen |
|---|---|
| Identifizieren Sie Benutzer, die auf die Nachrichtenliste zugreifen können. Zunächst erhalten alle Benutzer Zugriff. | Zugriff auf die Liste der gesendeten Nachrichten gewähren *(auf Seite 133)* |
| Identifizieren Sie Benutzer, die nicht auf die Nachrichtenliste zugreifen dürfen. | Zugriff auf die Auflistung der gesendeten Nachrichten verweigern *(auf Seite 134)* |
| Aktivieren Sie die Zugriffseinschränkung. | Beschränkung auf die Liste der gesendeten Nachrichten ermöglichen *(auf Seite 135)* |

Wenn Sie diese Aufgaben ausführen, ist die Option **Nachrichtenübersicht** im Menü **Kampagne** nur für Benutzer mit Rollen sichtbar, die explizit die Berechtigung zum Zugriff auf die Mailingliste erteilen.

## Zugriff auf die Liste der gesendeten Nachrichten gewähren

Wenn Sie den Zugriff auf die Liste der gesendeten Nachrichten einschränken, müssen Sie speziell Benutzern Zugriff gewähren, die auf die Liste zugreifen müssen.

Benutzer greifen auf die Auflistung gesendeten Nachrichten zu, indem Sie im Menü **Campaign** auf den **Nachrichtenübersichtsink** klicken. Sie können einem Benutzer Zugriff auf die Liste aller gesendeten Nachrichten erteilen, indem Sie dem Benutzer eine Verwaltungsrolle auf höchster Ebene zuweisen, die explizit die Berechtigung erhält, den **Nachrichtenübersichtslink** anzuzeigen.

Die Standardrollen der obersten Ebene umfassen **Admin**, **Ausführen**, **Design**und **Überprüfung**. Berechtigungen, die Sie über die Rollen der obersten Ebene erteilen, gelten für alle Objekte in der Partition.

1. Wechseln Sie zu `Settings > User Roles and Permissions > Campaign > partition (n)`.
2. Klicken Sie auf **Berechtigungen speichern und bearbeiten**.
   Eine Berechtigungsliste für die Partition wird geöffnet. Die verfügbaren Rollen der obersten Ebene werden oben in der Seite aufgelistet.
3. Gewähren Sie im Abschnitt **Verwaltung** jeder Rolle explizit die Berechtigung **Mailinglistenseite anzeigen**.

Wenn Sie Zugriffsbeschränkungen für die Liste der gesendeten Nachrichten aktivieren, können Benutzer mit Rollen, denen ausdrücklich die Berechtigung **Mailinglistenseite anzeigen** erteilt wurde, den Link **Nachrichtenübersicht** im Menü **Kampagne** anzeigen.

Erstellen Sie eine Rolle, um den Zugriff auf die Auflistung der gesendeten Nachrichten zu verweigern.

## Zugriff auf die Auflistung der gesendeten Nachrichten verweigern

Wenn Sie den Zugriff auf die Liste der gesendeten Nachrichten einschränken, müssen Sie Benutzern, die nicht auf die Liste zugreifen dürfen, ausdrücklich den Zugriff verweigern.

Benutzer greifen auf die Auflistung gesendeten Nachrichten zu, indem Sie im Menü **Campaign** auf den **Nachrichtenübersichtsink** klicken. Sie können verhindern, dass ein Benutzer auf die Liste aller gesendeten Nachrichten zugreift, indem Sie dem Benutzer eine Verwaltungsrolle auf oberster Ebene zuweisen, der ausdrücklich die Berechtigung zum Anzeigen des Links **Nachrichtenübersicht** verweigert wird.

Die Standardrollen der obersten Ebene umfassen **Admin**, **Ausführen**, **Design**und **Überprüfung**. Berechtigungen, die Sie über die Rollen der obersten Ebene erteilen, gelten für alle Objekte in der Partition. Sie können neue Rollen der obersten Ebene erstellen, um die Standardrollen der obersten Ebene zu ergänzen. Die neuen Rollen können bestimmte Berechtigungen erteilen oder verweigern.

1. Gehen Sie zu **Einstellungen> Benutzerrollen und Berechtigungen> Kampagne> Partition (n)**. Die Seite **Partition <n>** wird geöffnet.
2. Klicken Sie auf **Rolle hinzufügen.** Weisen Sie der Rolle einen Namen zu und geben Sie eine kurze Beschreibung ein. Speichern Sie die Änderungen und kehren Sie zur Seite **Partition <n>** zurück.
3. Konfigurieren Sie die neue Rolle, um den Zugriff auf die Auflistung der gesendeten Mailings zu verweigern.

    a. Klicken Sie auf **Rollen hinzufügen und Berechtigungen zuweisen**. Die Seite **Eigenschaften von Administrationsrollen** wird angezeigt. Die neue Rolle wird in der Liste der Rollen angezeigt.

    b. Klicken Sie auf **Berechtigungen speichern und bearbeiten**.
    Eine Liste der Berechtigungen für die Partition wird als Matrix von Auswahlsymbolen angezeigt, die den Status jeder Berechtigung für jede Rolle angeben. Die neue Rolle wird neben den anderen Rollen der obersten Ebene oben in der Matrix angezeigt.

    c. Verweigern Sie im Abschnitt **Verwaltung** explizit die Berechtigung **Mailinglistenseite anzeigen** für die neue Rolle. Speichern Sie die Änderungen.

4. Weisen Sie die neue Rolle den Benutzern zu, die nicht auf die Mailinglistenseite zugreifen können sollen.
    a. Wechseln Sie zu **Einstellungen** > **Benutzer**. Wählen Sie den Benutzer aus, den Sie beim Zugriff auf die Liste der gesendeten Nachrichten verhindern möchten.
    b. Klicken Sie auf **Rollen bearbeiten**. Die neue Rolle, die Sie im vorherigen Schritt erstellt haben (eine Rolle, die zum Verweigern des Zugriffs konfiguriert ist), wird unter **verfügbar Rollen**angezeigt.
    c. Verschieben Sie die neue Rolle aus **verfügbar Rollen** zu **Rollen**. Speichern Sie die Änderungen.

Wenn Sie Zugriffsbeschränkungen für die Liste der gesendeten Nachrichten aktivieren, kann ein Benutzer, dem die neue Rolle zugewiesen wurde, den Link **Nachrichtenübersicht** nicht sehen.

Aktualisieren Sie die Konfiguration, um Zugriffsbeschränkungen für die zugesandten Nachrichten zu ermöglichen.

### Beschränkung auf die Liste der gesendeten Nachrichten ermöglichen

Benutzer greifen über die Option **Nachrichtenübersicht** im Menü **Kampagne** auf die Liste der gesendeten Nachrichten zu. Wenn Sie den Zugriff auf die Auflistung der gesendeten Nachrichten einschränken, steuert die ID der Sicherheitsfunktionsfunktion die Anzeige dieser Menüoption und steuert deshalb den Zugriff auf die Auflistung der gesendeten Nachrichten.

Um den Zugriff auf die Auflistung der gesendeten Nachrichten einzuschränken, müssen Sie die Eigenschaft für die Sicherheitsfunktion-ID in der Platform Konfiguration aktualisieren. Diese Eigenschaft gilt für alle Partitionen in Ihrer Campaign -Installation.

Wenn Sie die ID der Sicherheitsfunktion mit dem korrekten Wert ausfüllen, steht die **Nachrichtenübersichtsoption** nur den Benutzern mit einer Rolle zur Verfügung, die explizit die Berechtigung für die Mailingliste der Anzeige erteilt. Benutzer mit Rollen, bei denen die Berechtigung für die Seite Mailingliste anzeigen entweder verweigert wurde oder nicht gewährt wird, können die **Nachrichtenübersichtsoption** nicht sehen.

1. Wechseln Sie zu **Einstellungen** > **Konfiguration** > **Platform** > **Platformweite Navigation** > **Hauptnavigationsmenü** > **Campaign** > **Mailings liefern**. Klicken Sie auf **Deliver Mailings**, um die Konfigurationseinstellungen anzuzeigen.
2. Klicken Sie auf **Einstellungen bearbeiten**.
3. Geben Sie im Feld **Sicherheitsfunktions-ID**`7000`ein. Speichern Sie die Änderungen.

   Melden Sie sich vom System ab und erneut an, um die Ergebnisse der Konfigurationsänderung anzuzeigen.

Nur Benutzer mit Rollen, die explizit die Berechtigung zum Anzeigen der Mailingliste erteilen, können den **Nachrichtenübersicht Link** anzeigen, um auf die Liste der gesendeten Nachrichten zuzugreifen.

## Berechtigungen für Deliver Berichte

Ihre Benutzerberechtigungen bestimmen Ihre Fähigkeit, Deliver Berichte anzuzeigen.

Informationen zum Festlegen von Berechtigungen für den Zugriff auf Standard- Deliver-Berichte finden Sie im Abschnitt Unica Insights Berichte Installations- und Konfigurationshandbuch für Berichterstattung und Sicherheit.

# Chapter 11. Technische Hinweise (Fehlerbehebung)

## Problem (Kurzfassung)

Um die mit der Unica Campaign installierten Deliver-Komponenten zu verwenden und personalisierte Marketingnachrichten zu senden, müssen Sie die lokale Campaign-Installation mit fernen, von der HCL gehosteten Nachrichten-Ressourcen verbinden. In diesem Abschnitt wird beschrieben, wie Sie eine solche Verbindung konfigurieren, wenn Ihre Firewall-Regeln des Unternehmens eine direkte Kommunikation mit der gehosteten Umgebung verbieten.

## Fehlerbehebung

**Typische Kommunikation mit der gehosteten Umgebung für E-Mail-Ressourcen**

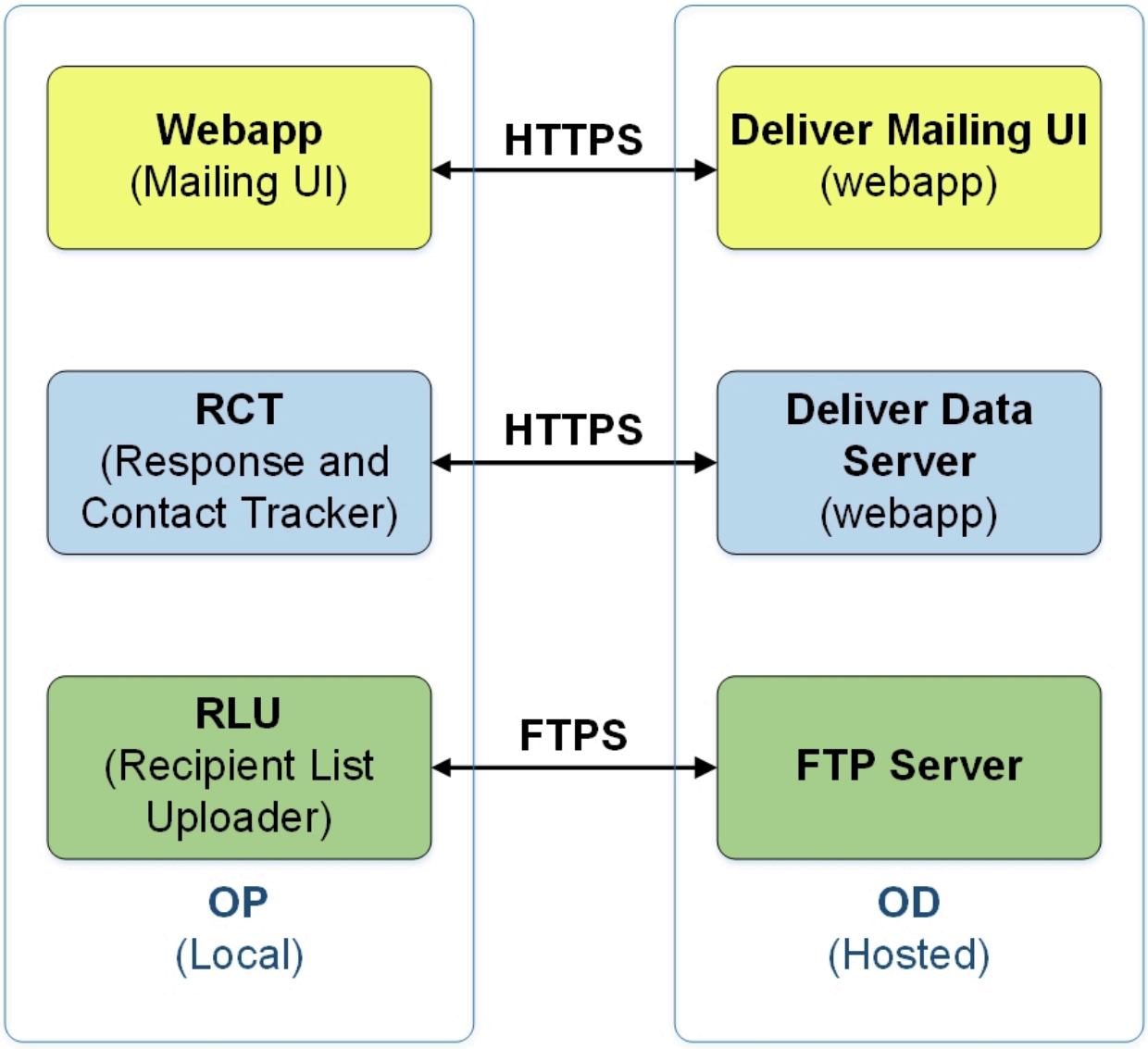
Das folgende Diagramm veranschaulicht die Standardkonfiguration für die Kommunikation zwischen der On Premises (OP)-Umgebung und der On Demand (OD)-Umgebung.

Die lokale Deliver OP Umgebung benötigt eine externe Kommunikation mit der Deliver OD Umgebung über HTTPS und SFTP.

Die OP-Umgebung enthält einen Webanwendungsserver (entweder IBM WebSphere oder Oracle WebLogic), auf dem Sie Campaign implementiert haben. Campaign hostet die Deliver-Komponenten (RCT und RLU), die mit den gehosteten E-Mail-Ressourcen in der OD-Umgebung kommunizieren.

Der Response and Contact Tracker (RCT) lädt Antwortdaten aus der OD-Umgebung.

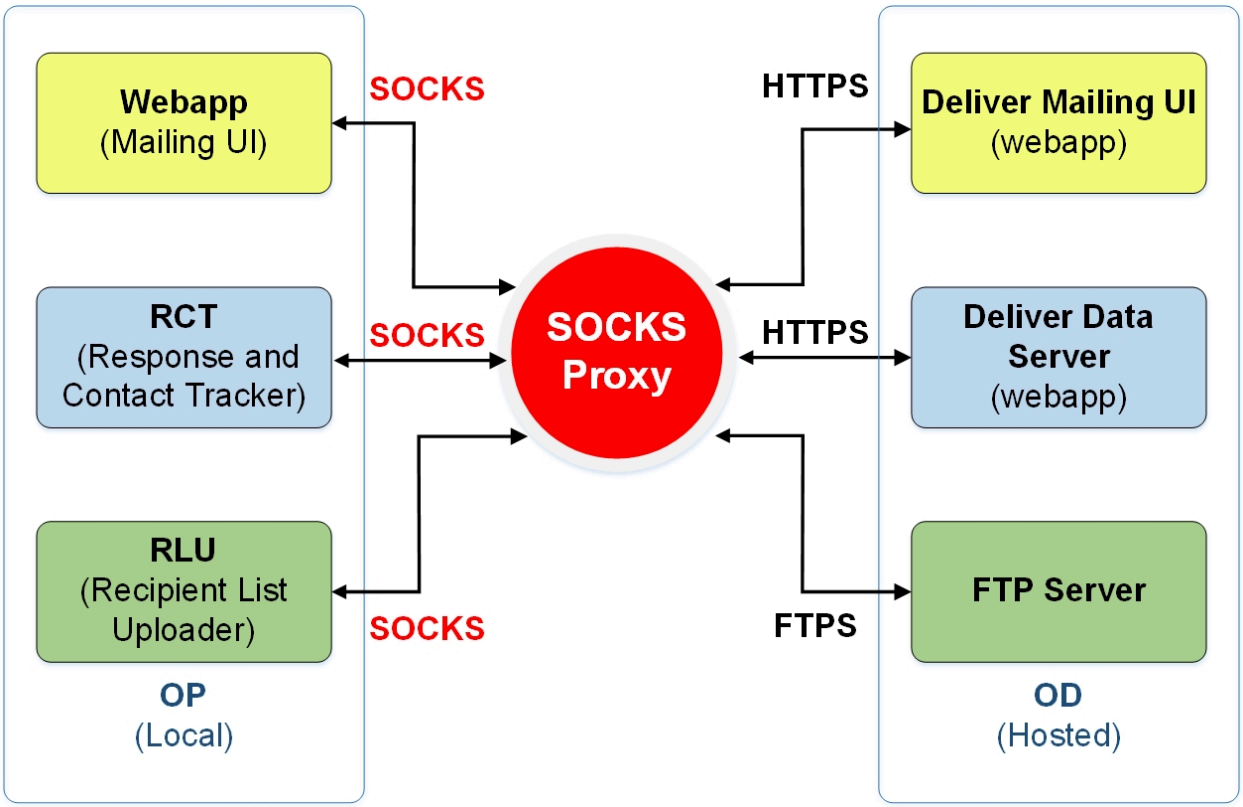
Der Response List Uploader (RLU) lädt Mailinglisten und andere erforderliche Mailingdaten in die OD-Umgebung hoch.




Wenn das System, auf dem Unica Deliver installiert ist, nicht direkt mit der OD-Umgebung kommunizieren kann, unterstützt Deliver die Kommunikation mit den gehosteten OD-Ressourcen über einen SOCKS-Proxy.

## Verbinden mit Nachrichtendiensten über einen Proxy

Das folgende Diagramm veranschaulicht die Kommunikation zwischen der OP- und OD-Umgebung, wenn ein SOCKS-Proxy verwendet wird. Beachten Sie, dass der SOCKS-Proxy in der lokalen Umgebung "On Premises" konfiguriert wird.




Überprüfen Sie die folgenden Punkte, bevor Sie die Proxy-Einstellungen aktivieren.

- Der Proxy-Server ist ein SOCKS-Proxy.
- Der Proxy-Server kann auf die Deliver-OD-Umgebung zugreifen und den Datenverkehr zu und von den Ports ermöglichen, die im HCL-Datenzentrum konfiguriert sind und von Ihrem gehosteten E-Mail-Konto verwendet werden.
- Sie haben den SOCKS-Proxy so installiert, dass der Zugriff der Deliver OP-Umgebung auf den Proxy erfolgen kann.

## Erforderliche Änderungen für die Weiterleitung von SFTP- und HTTPS-Datenverkehr durch einen SOCKS-Proxy

Um einen SOCKS-Proxy für den Zugriff auf von der HCL gehostete E-Mail-Ressourcen zu verwenden, müssen Sie Änderungen an der Webanwendung, in der Sie die Campaign bereitgestellt haben, und an den Startskripten für die Deliver RCT und RLU vornehmen.

### Änderungen für SFTP vornehmen

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

- `- Dhcl.unica.deliver.ftp.proxy.host = <socksHost>`
- `- Dhcl.unica.deliver.ftp.proxy.port = <socksPort>`
- `- Dhcl.unica.deliver.ftps.proxy.match.hosts = <eine durch Komma getrennte Liste von Hostnamen und IP Adressen>`

socksHost ist der Hostname oder die IP des SOCKS Proxys.

socksPort ist der Port, auf dem der SOCKS Proxy ausgeführt wird.

`-Dhcl.unica.deliver.ftps.proxy.match.hosts` stimmt mit Hostnamen und IP Adressen überein, die bei der Weiterleitung des Datenverkehrs über den SOCKS Proxy verwendet werden.

Die für `-Dhcl.unica.deliver.ftps.proxy.match.hosts` angegebene IP Adresse ist die IP Adresse, die der FTP-Server in der gehosteten OD-Umgebung als Teil des SFTP-Protokolls bei der Datenübertragung an den FTP-Client in der lokalen OP-Umgebung sendet.

Setzen Sie `-Dhcl.unica.deliver.ftps.proxy.match.hosts` auf einen der folgenden Werte (abhängig vom Rechenzentrum, das von Ihrem gehosteten E-Mail Konto verwendet wird).

US Rechenzentrum: `-Dhcl.unica.deliver.ftps.proxy.match.hosts=ftp-em.unicadeliver.com`

Rechenzentrum Indien: `-Dhcl.unica.deliver.ftps.proxy.match.hosts=ftp-in.unicadeliver.com`

Europäisches Rechenzentrum: `-Dhcl.unica.deliver.ftps.proxy.match.hosts=ftp-eu.unicadeliver.com`

### Änderungen für HTTPS vornehmen

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

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

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

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

socksHost ist der Hostname oder die IP des SOCKS Proxys.

socksPort ist der Port, auf dem der SOCKS Proxy ausgeführt wird.

### Authentifizierungsanforderungen bei Verwendung eines SOCKS Proxys

Sollte Ihr SOCKS Proxy eine Authentifizierung erfordern, konfigurieren Sie Folgendes für die Webanwendungsserver, RLU und RCT.

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

Dabei sind Benutzername und Passwort die Anmeldedaten, die für die Authentifizierung gegenüber dem Proxy erforderlich sind.

## So konfigurieren Sie die RCT mithilfe eines SOCKS-Proxy

Konfigurieren Sie die RCT für die Arbeit durch einen SOCKS-Proxy, befolgen Sie die Prozedur für Ihr Betriebssystem.

### Für die RTC in der Windows-Umgebung

Fügen Sie die folgenden Proxyargumente zu `common.bat,` im `//deliver/bin`-Verzeichnis Ihrer lokalen Deliver-Installation ein.

```
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
```

### Für die RCT in UNIX-Umgebungen

Fügen Sie die folgenden Proxyargumente zu `common.sh` im `\\deliver\bin`-Verzeichnis Ihrer lokalen Deliver-Installation ein.

**Note:** Nehmen Sie keine Änderungen direkt an `rlu.sh.rct.sh` oder `setenv.sh` weil sie überschrieben werden.

```
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}"
```

## Konfiguration von RLU mit einem SOCKS Proxy

Um die RLU so zu konfigurieren, dass sie über einen SOCKS-Proxy funktioniert, befolgen Sie das Verfahren für Ihr Betriebssystem.

### Für die RLU in der Windows Umgebung

Fügen Sie die folgenden Proxy Argumente zu common.bat hinzu, die sich im Verzeichnis `//deliver/bin` Ihrer lokalen Deliver Installation befindet.

```
Setzen Sie 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= <kommagetrennte Liste von Hostnamen und IP-Adressen>

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

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

set RLU_JAVA_ARGS=%BASE_VM_ARGS% %RLU_MEM_ARGS% %RLU_EXTRA_VM_ARGS%

%RLU_PROXY_ARGS%
```

### Für die RLU in UNIX Umgebungen

Fügen Sie die folgenden Proxy Argumente zu common.sh hinzu, die sich im Verzeichnis `\\deliver\bin` Ihrer lokalen Deliver Installation befindet.

**Note:** Nehmen Sie keine direkten Änderungen an `rlu.sh.rct.sh` oder `setenv.sh` vor, da diese überschrieben werden.

```
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= <kommagetrennte Liste von Hostnamen und IP-Adressen>

-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}"
```

## Änderungen an der WebSphere Konfiguration

Fügen Sie Folgendes zu den generischen WebSphere JVM Argumenten hinzu (siehe Screenshot):

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

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

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

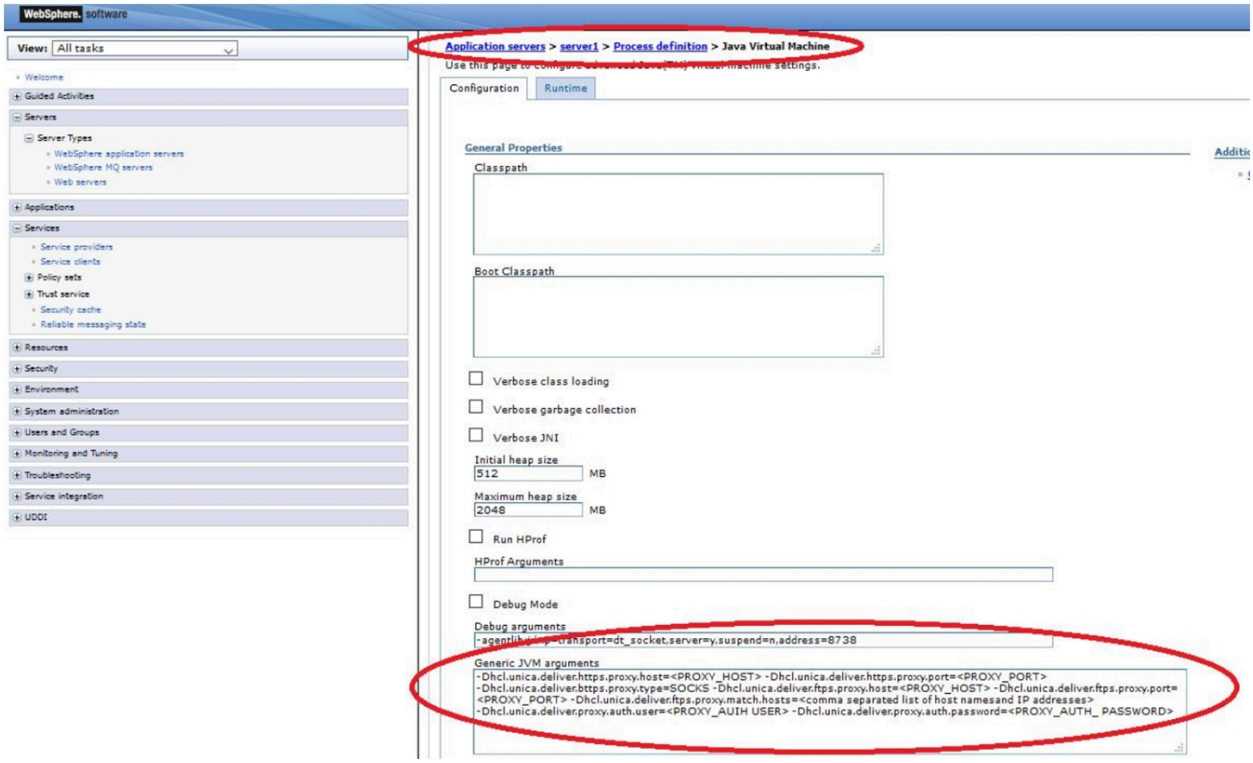
```
-Dhcl.unica.deliver.ftp.proxy.host=<PROXY_HOST>
```

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

```
-Dhcl.unica.deliver.ftps.proxy.match.hosts= <kommagetrennte Liste von Hostnamen und IP-Adressen>
```

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

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




## Änderungen an der Oracle WebLogic Konfiguration

Ändern Sie das Skript für WebLogic.

In Windows Umgebung

```
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= <kommagetrennte Liste von Hostnamen und IP-Adressen>

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_ PASSWORD>%
```

### In UNIX Umgebungen

```
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= <kommagetrennte Liste von Hostnamen und IP-Adressen>

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

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

# Chapter 12. Konfiguration des Deliver Vertriebskanalkontos

Deliver unterstützt SMS, WhatsApp und Push als Zustellungskanäle, neben E-Mail. Deliver unterstützt SMS, WhatsApp und Push als Zustellungskanäle, neben E-Mail. SMS werden durch verschiedene Anbieter unterstützt, sodass der Kunde basierend auf geografischen und Kostenaspekten einen SMS-Partner auswählen kann. Wenn ein Kunde sich entscheidet, einen bestimmten Lieferanten für SMS- oder WhatsApp-Nachrichten zu verwenden, arbeitet HCL mit dem Kunden und dem ausgewählten Lieferanten zusammen, um ein problemloses Onboarding auf Deliver zu ermöglichen. Im Rahmen dieses Prozesses wird das Konto des Kunden mit jedem Lieferanten erstellt. Dieses Konto ermöglicht es Deliver, Nachrichten im Namen dieses Kunden zu senden und Antworten von Benutzern zu verarbeiten.

Deliver unterstützt die folgenden Kanäle.

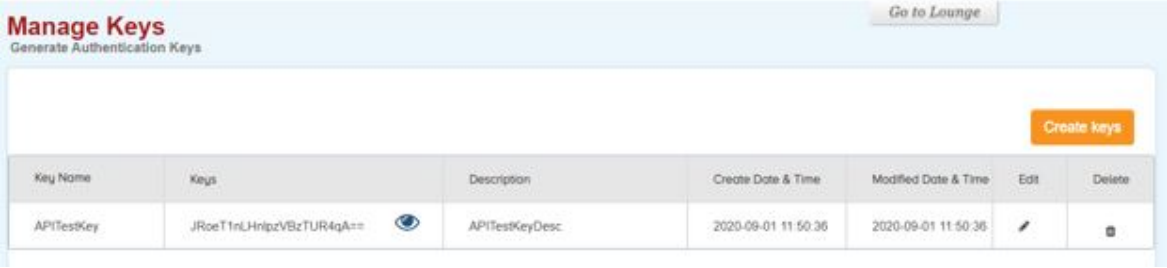
- SMS mit Lieferant Karix
- SMS mit RML-Lieferant (Sowohl für Empfehlungs- als auch für Wiederverkäufer-Lizenzen)
- Whatsapp mit RML-Lieferant
- Push mit Kumulos als Lieferant

Das folgende Dokument erklärt die Schritte für jeden dieser Kanäle. Diese Schritte müssen von oder für jedes Kundenkonto im Rahmen des Onboarding-Prozesses ausgeführt werden.

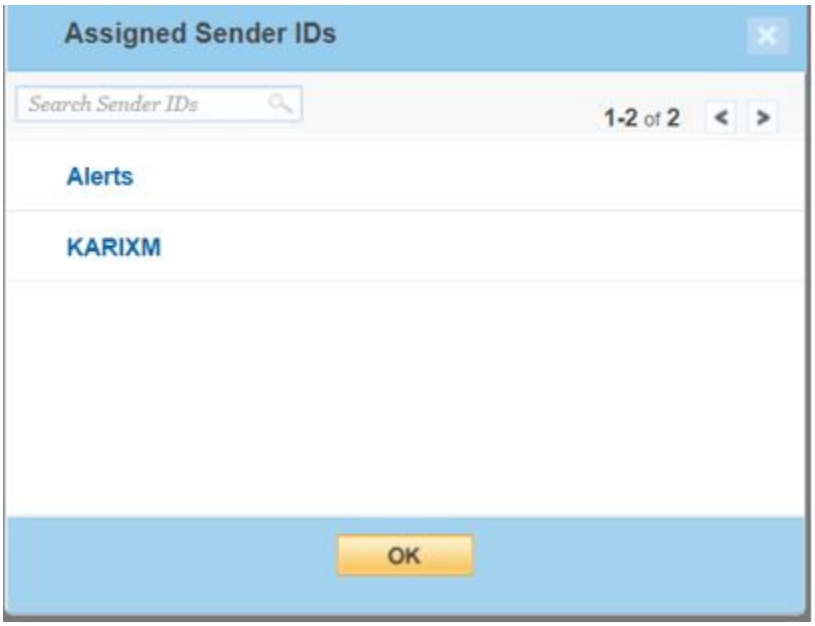
## Karix SMS Kontokonfiguration

Führen Sie die folgenden Schritte aus, um das Karix SMS-Konto des Kunden so zu konfigurieren, dass es mit Deliver funktioniert.

1. Melden Sie sich bei Karix Console (www.karix.solutions) an und klicken Sie die Schaltfläche API-Schlüssel im Dashboard, um einen API-Schlüssel zu erstellen und mit Deliver zu konfigurieren.

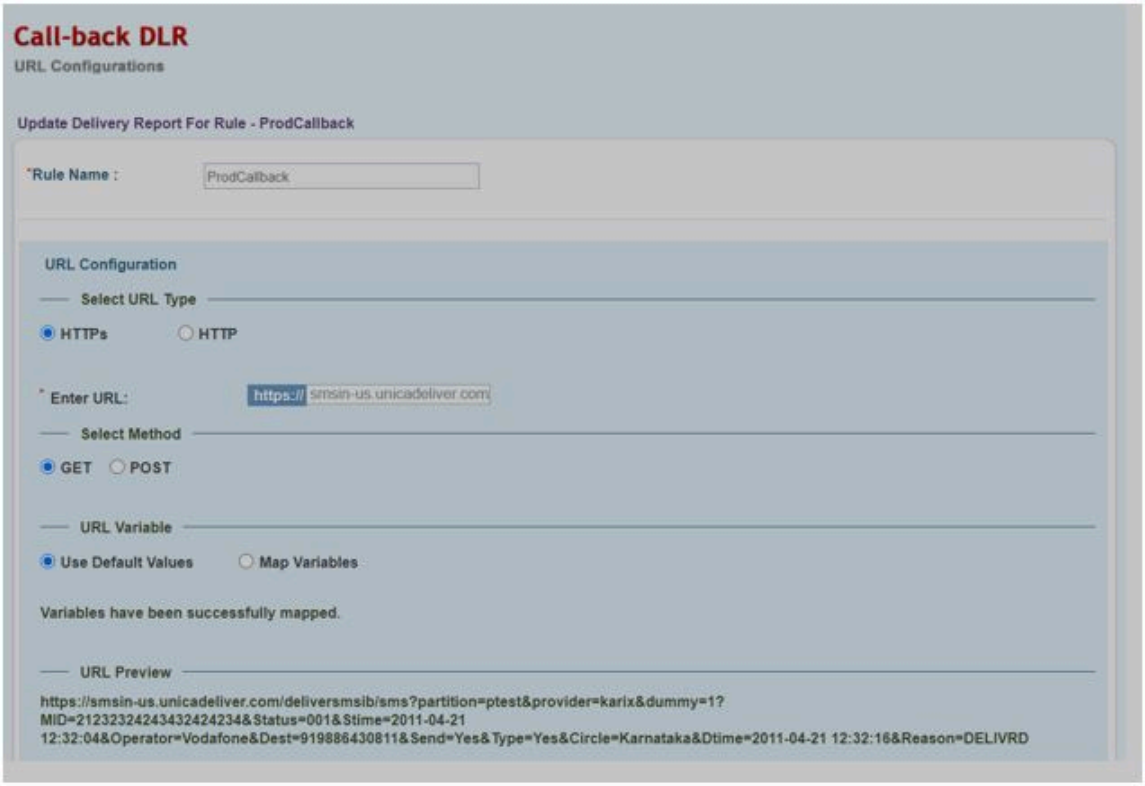



2. Wählen Sie in der rechten oberen Ecke unter der Liste " **Mein Konto öffnen** " die Option **Meine info bearbeiten** aus und notieren Sie sich die für Ihr Karix-Konto konfigurierte Absender-ID, um sie in Deliver zu konfigurieren.




3. Geben Sie den in Schritt 1 erstellten API-Schlüssel und die in Schritt 2 angegebene Absender-ID an, damit sie im Konto konfiguriert werden kann.
4. Legen Sie die Callback-URL in der Karix-Konsole fest.
    - Für das US-Rechenzentrum: https://smsin-us.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=karix&dummy=1
    - Für das EU Rechenzentrum: https://smsin-eu.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=karix&dummy=1
    - Für Indien: https://smsin-in.unicadeliver.com/deliversmsib/sms?partition=%3Caccount%3E&provider=karix&dummy=1

**Note:** Sobald das Konto in Deliver konfiguriert ist, muss <account> in der obigen URL durch den vom Deliver Provisioning Team bereitgestellten Kontonamen ersetzt werden.




# RML SMS Kontokonfiguration

Das RML-SMS-Konto des Kunden muss über die folgenden Konfigurationen verfügen, damit es mit Deliver funktioniert.

**RML-Konto Einbindung**

- Sie müssen mit RML Team arbeiten, um ein SMS Konto für Indien oder eine weltweite Position basierend auf der Position des Kunden zu erstellen.
- Die SenderID muss vom von RML konfigurierten Kunden bereitgestellt werden.
- SMS-Vorlagen müssen auch auf der Grundlage des Zielortes für den SMS-Versand in eine Whitelist aufgenommen werden. Zum Beispiel:
    - Indische Kunden müssen dem Deliver Services Team die Principal Entity ID (PE ID) zur Verfügung stellen und die auf der DLT-Plattform registrierten Vorlagen gemäß den Anweisungen im Benutzerhandbuch konfigurieren.
    - Für die USA und Kanada sind vorab genehmigte Vorlagen erforderlich.

RML verfügt über verschiedene Anmelde-URLs basierend auf der Region, die sie als Teil der E-Mail-Kontoerstellung von ihrer Seite bereitstellen. Beispiel: URLs für Indien und weltweite Rechenzentren

- Konto Indien: https://ems.rmlconnect.net/
- Weltweites Konto: https://client.rmlconnect.net/login

Führen Sie die folgenden Schritte aus.

1. Melden Sie sich gemäß den obigen URLs bei der RML-Konsole an und navigieren Sie zu **Dienstprogramme > DLR Push URL**.

   **Note:** Sie müssen RML auffordern, dieses Menü bei der Bereitstellung des Kontos hinzuzufügen.

2. Legen Sie die Callback-URL in der RML-Konsole fest.

   - Für das US-Rechenzentrum: https://smsin-us.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=RML
   - Für das EU Rechenzentrum: https://smsin-eu.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=RML
   - Für das Rechenzentrum-Indien: https://smsin-in.unicadeliver.com/deliversmsib/sms?partition=%3Caccount%3E&provider=RML&dummy=1

   **Note:** Sobald das Konto in Deliver konfiguriert ist, muss <account> in der obigen URL durch den vom Deliver Provisioning Team bereitgestellten Kontonamen ersetzt werden.

### Einrichten von bidirektionalen SMS-Antworten mit RML

Deliver unterstützt bidirektionale SMS Antworten (Beispiel: STOP Anforderungen) mit RML seit v12.1.1. Bidirektionale SMS erfordert eine Absender-ID, die die von RML auf Anfrage bereitgestellten Antworten unterstützt.

RML unterstützt entweder dedizierte oder gemeinsam genutzte Funktionscodes. Für gemeinsam genutzte Funktionscodes muss der Benutzer den Markennamen an den Nachrichtenanfang setzen (Beispiel: HCL STOP), damit RML die Anfrage korrekt an Deliver delegieren kann. Es gibt keine solche Anforderung für einen dedizierten Funktionscode (Beispiel: Der Benutzer kann nur mit STOP antworten) und RML wird die Antwort korrekt dem erforderlichen Deliver-Konto zuordnen.

Damit RML Antworten an die richtige prod-Umgebung und das richtige Kundenkonto liefern kann, muss die Webhook URL für eingehende Antworten in der freigegebenen/zugewiesenen Absender-ID des Kunden wie folgt konfiguriert werden.

- Für das US-Rechenzentrum: https://smsin-us.unicadeliver.com/deliversmsib/mo/<account>?provider=RML
- Für das EU Rechenzentrum: https://smsin-eu.unicadeliver.com/deliversmsib/mo/<account>?provider=RML
- Für das Rechenzentrum Indien: https://smsin-in.unicadeliver.com/deliversmsib/mo/<account>?provider=RML

**Note:** <Konto> in der obigen URL muss durch den vom Deliver Services-Team bereitgestellten Kontonamen ersetzt werden, sobald das Konto in Deliver konfiguriert ist.

## RML WhatsApp-Kontokonfiguration

Die Kunden, die mit der Funktion WhatsApp ausgestattet sind (bereitgestellt von RML), müssen die folgenden Schritte für die Konfiguration ausführen.

1. Erstellen Sie ein verifiziertes Facebook Business Manager-Konto, das für WhatsApp eingerichtet ist. Das RML-Team führt Kunden dazu, das Konto von Facebook Business Manager nach Bedarf zu konfigurieren.
2. Erstellen Sie ein WhatsApp-Konto mit RML. RML erstellt dieses Konto, nachdem die Überprüfung des Facebook Business Manager-Kontos abgeschlossen ist.
3. Erstellen von Nachrichtenvorlagen, die von WhatsApp genehmigt wurden. Das RML Team wird mit Kunden arbeiten, um Nachrichtenvorlagen im erforderlichen Format vorzubereiten und sie vom Kunden zu genehmigen.
4. Sobald RML den Kunden freigegebene Vorlagen zur Verfügung stellt, müssen sie diese über den Menüpunkt **Neu > WhatsApp** Inhalt in den Deliver Message Editor hochladen. Alle Details müssen genau wie in der genehmigten Vorlage angegeben werden, da WhatsApp nach der Genehmigung keine Änderungen an der Vorlage zulässt.
5. Konfigurieren Sie die Callback-URL im RML-WhatsApp-Konto. Hierzu müssen Sie RML die unten stehende URL bereitstellen, damit diese als Callback URL für WhatsApp-Nachrichten-Deliver Berichte konfiguriert werden kann.
    - Für das US Rechenzentrum: https://smsin-us.unicadeliver.com/deliversmsib/wa/ <account>
    - Für das EU Rechenzentren: https://smsin-eu.unicadeliver.com/deliversmsib/wa/ <account>
    - Für das Rechenzentrum Indien: https://smsin-in.unicadeliver.com/deliversmsib/wa/ <account>

      **Note:** <Konto> in der obigen URL muss durch den vom Deliver Services-Team bereitgestellten Kontonamen ersetzt werden, sobald das Konto in Deliver konfiguriert ist.

# Index