

Unica Delivery V12.1.1 起動および管理者のガイド



Contents

Chapter 1. Unica Campaign と Unica Deliver を使用したホ ステッド・メッセージング 4	システム構成の確認..... 38
でのホストメールアカウントの確立Unica..... 4	HCL Unica ホスト・サービスへのアップロードのテス ト..... 41
起動プロセスの全体像..... 4	HCL Unica ホスト・サービスからのダウンロードのテ スト..... 41
Before you begin working with Unica Deliver..... 6	ホストされたメッセージング・インターフェースへの 接続のテスト..... 41
Chapter 2. ローカルの設定HCL Unica環境Deliver 7	Chapter 6. About configuring Unica Deliver 42
確認中Deliver登録..... 7	Configuring access to additional mailing execution history..... 43
Deliver の手動登録..... 7	Configuring support for Campaign offer integration..... 44
Campaign での配信機能の有効化..... 8	Configuring support for dimension tables..... 44
表示中Deliverメニューオプション..... 8	ローカル Deliver システム・テーブルへのアクセスの構 成..... 45
Deliver システム・テーブル特性の指定..... 9	Unica Delivery 設定プロパティ 46
ローカルへのアクセスの構成Deliverシステムテー ブル..... 10	Campaign partitions partition[n] Deliver..... 46
Deliverシステムテーブルに必要なマッピン グCampaign..... 11	Campaign partitions partition[n] server internal..... 48
次の Web アプリケーションサーバーの再起動が必要で す: Campaign..... 11	Campaign partitions partition[n] Deliver contactAndResponseHistTracking..... 49
Chapter 3. メッセージサービスへの接続 12	Deliver serverComponentsAndLocations hostedServices..... 52
への接続を設定するための要件HCL Unicaホストサー ビス..... 12	Deliver partitions partition[n] hostedAccountInfo..... 53
にデータをアップロードするための要件HCL Unicaホ ステッドサービス..... 12	Deliver partitions partition[n] dataSources systemTables..... 54
接続とポートの要件..... 13	Deliver partitions partition[n] recipientListUploader..... 58
IP をホワイトリストに登録する..... 13	Deliver partitions partition[n] responseContactTracker..... 58
SFTP によるアップロード接続..... 14	Chapter 7. About utilities for Deliver 61
SFTP の構成..... 15	The RLU script..... 61
明示的 FTP によるデフォルトのアップロード接 続..... 16	Deliver レスポンスおよびコンタクトのトラッカー (RCT) スクリプト..... 62
明示的 FTP を使用したデータアップロード..... 17	The MKService_rct script..... 63
HTTP プロキシを介した接続..... 20	The configTool utility..... 64
データダウンロードの頻度とポート設定..... 25	Chapter 8. About troubleshooting Deliver 65
HCL Unica ホスト・サービスにアクセスするシステ ム・ユーザーの構成..... 26	Log files for Deliver..... 65
HCL Unica ホスト・サービスにアクセスするシス テム・ユーザーの構成..... 27	Deliver での log4j の使用..... 65
To configure addresses for connecting to HCL Unica Hosted Services..... 28	Chapter 9. メッセージ機能へのユーザーアクセスの管 理 67
配信ホスト名のIPアドレス..... 29	メール送信アクセスのためのロールとポリシーの割り 当て..... 67
ホストメールの安全な通信の構成..... 29	Platform および Campaign での役割と権限..... 67
信頼できるキーストアの生成..... 29	セキュリティ・ポリシーの仕組み..... 68
WebSphere 使用時の SSL の構成..... 31	Campaign でのメッセージ許可..... 70
WebSphere 使用時の SSL の構成..... 33	ロールと許可の使用可能化..... 71
Tomcat または JBOSS での Campaign の配置..... 35	Campaign による権限の評価方法..... 71
Chapter 4. Response and Contact Tracker の操作 36	権限の状態の定義..... 72
Response and Contact Tracker の手動操作..... 36	Campaign でのメーリングに対する許可..... 73
Response and Contact Tracker のサービスとしての追 加..... 36	
Response and Contact Tracker サービスの削除..... 37	
Chapter 5. 起動確認 38	

「デジタル資産」カテゴリの許可.....	73
文書カテゴリの許可.....	74
[メール管理] カテゴリの権限.....	75
次のメール許可Deliver.....	75
Deliverロールの割り当て.....	75
メールアドレスと短縮リンクドメインの制御.....	76
ホストメールアドレスの保守.....	77
デフォルトの送信者アドレスと表示名の構成.....	78
送信メールリストへのアクセス制御.....	79
送信メールリストへのアクセスを許可中.....	79
送信メールリストへのアクセスの拒否.....	80
送信メール一覧への制限を有効にする.....	81
About permissions for Deliver reports	81
Chapter 10. 技術情報 (問題解決).....	82
プロキシを経由してメッセージサービスに接続.....	82
SOCKS プロキシ経由で FTPS と HTTPS トラ フィックをルーティングするために必要な変 更.....	83
Chapter 11. チャネルベンダーアカウント設定の提供.....	88
Karix SMS アカウント設定.....	88
RML SMS アカウント構成.....	89
RML WhatsApp アカウント設定.....	90
Twilio SMS アカウント設定.....	90
Index.....	91

第 1 章. Unica Campaign と Unica Deliver を使用したホスティング・メッセージング

Unica Campaign を Unica Deliver と統合すると、Deliver を使用して、高度にパーソナライズされたデジタル・マーケティング・キャンペーンを行うことができます。



注: Deliver は、電子メールとともに次のチャンネルをサポートします。このガイドでは、メッセージという用語はすべてのチャンネルに適用されます。

- SMS
- WhatsApp
- プッシュ

Deliver から Unica でホストされるリソースにアクセスできるため、顧客データマートに保存されている情報に基づいて、個別にカスタマイズされたメッセージを設計、送信、および監視できます。

- Campaign で、フローチャートを使用して、メッセージ受信者のリストを作成し、各受信者のパーソナライズ・データを選択します。
- Deliver では、メッセージの設計、送信、および配信到達性に関して HCL によってホストされるリソースを使用して、デジタル・マーケティング・キャンペーンを行います。

でのホストメールアカウントの確立Unica

メッセージの定期購入を購入すると、Unica は、ユーザーの代わりにホストメールアカウントを作成し、メッセージ機能を使用するために必要なアカウント資格情報を送信します。これらの資格情報を適用し、ローカル HCL Unica アプリケーションがホストされているメール環境に安全な接続でアクセスします。

メッセージリソースにアクセスするには、有効なアカウントが必要です。Unica は、ソフトウェアサービスとして提供します。あなたの HCL Unica インストールに複数のパーティションがあり、複数のパーティションでメッセージを使用する予定です。ホストされたメールアカウントと、各パーティション用の WhatsApp と SMS 用の少なくとも 1 つのサービスプロバイダが必要です。インストール間またはパーティション間でメールアカウントを共有することはできません。

ホストされたメールアカウントの設定から、スタートアッププロセスを開始します。このプロセスは、約 90 日間続きます。要件に従って、SMS または WhatsApp を登録できます。プロセスの一般的な説明については、次のトピックを参照してください。

起動プロセスの全体像

Unica Campaign のメッセージ機能をアクティブ化して、ターゲットを絞った追跡可能なデジタル・マーケティング・キャンペーンを実施できます。Campaign では、米国およびヨーロッパのデータ・センターでホストされているリソースを介して、Unica Deliver によって提供されるメッセージ機能を使用します。E メール・リソースにアクセスするためのアカウントは、Deliver サブスクリプションに含まれています。要件に従って、WhatsApp、プッシュ、または SMS チャンネルを選択することもできます。

Unica は、ホストされた E メール・アカウントを作成した後、起動プロセスを開始します。Unica は、お客様が Deliver に精通し、メッセージ・リソースに接続し、主要なインターネット・サービス・プロバイダー (ISP) の間で正当なデジタル・マーケティング担当者としての評判を確立するのに役立ちます。

このプロセスは 3 つのフェーズで進行します。Unica Professional Services チームと Deliver Services チームが、お客様をサポートします。

Professional Services コンサルタントは、起動プロセスにおける Unica との主要な窓口です。アカウント起動プロセスが完了すると、Professional Services コンサルタントは主なサポート担当を Unica Product Support チームに移管します。

専任の Deliver Services コンサルタントが、メッセージ関連の問題に対して特別なサポートを提供します。主要インターネット・サービス・プロバイダー (ISP) の間でメッセージの評判を高めることは、デジタル・マーケティング・キャンペーンをターゲット受信者に一貫して届けるために重要です。メール配信を開始すると、EAS コンサルタントがメール配信の配信到達性パフォーマンスを確認し、メッセージの評判を徐々に構築するための最良の方法を提案します。

スタートアップのアクティビティとマイルストーン

計画

結果	担当者
メールアカウント資格情報と、E メールスタートアップワークシートを含む Welcome キットを送信します。	Unica サービスの送信
電話会議をスケジュールして、関係者すべての紹介、立ち上げスケジュールの確認、メールマーケティングの目的について説明します。	Unica プロフェッショナルサービス
メール開始ワークシートに記入して、メールドメインの要件とメール送信の予想を指定してください。	組織

メール評価の作成

結果	担当者
電話会議と E メールスタートアップワークシートで提供された情報を使用して、メールアカウントをプロビジョニングします。	Unica メール操作
主要 ISP の選択したテストアカウント宛でのメールのウォーミングアップを開始します。このフェーズが完了するまでに、約 30 日かかります。	Unica メール操作
有効化 Deliver/Unica Campaign .	あなたの組織 (以下のサポートあり)Unica)

結果	担当者
ホストされているメールリソースへのアクセスを設定します。どのデータセンターを指定するかは、EAS コンサルタントに確認してください。	あなたの組織 (以下のサポートあり)Unica)
メーリングの送信を開始します。好ましいメール評価を確立するには、最初は小さいメールを送信し、時間の経過と共に、大きくて頻度の高いメールを送信します。ISP	あなたの組織 (以下のサポートあり)Unica)
は、多くの場合、正規のものと認識できないメールアドレスからの大量のメールや頻繁なメールをブロックすることで、スパムを制限しようとしています。	
メールの量と頻度の増加に応じて、到達率の結果と評価ガイドを提供します。	Unicaサービスの送信

本番

結果	担当者
標準的な量と頻度でメールを送信します。	組織
次の連絡先に主連絡先を転送しますUnicaサポートチーム	Unicaプロフェッショナルサービス
メールの問題に関するコンサルトの約束を維持します。メールアカウントサポートを継続するには、定期的にお問い合わせください。	Unicaサービスの送信

作業を開始する前にDeliver

メッセージの起動プロセスを開始する前に、以下の点を考慮してください。

- 一部の設定では、Web アプリケーションサーバーの再起動が必要です。計画Deliverで実行される大規模なフローチャートやその他のアクティビティの妨げを避けるための構成アクティビティCampaign.
- Unicaは、立ち上げプロセス中の主連絡先ポイントとして、1人を指定するように要求します。
- 起動プロセスを開始する前に、ホストメールアカウントの資格情報を要求してください。これらの資格情報を使用して、アカウントにアクセスするようシステムを設定します。
- ネットワーク管理者に確認してください。Deliver通信時に特定のポート範囲を必要とするHCL Unica.
- 設定を変更するための適切なネットワーク許可を持っていることを確認してください。

Chapter 2. ローカルの設定HCL Unica環境Deliver

使用Deliverメッセージを送信するには、ローカルへインストールされているシステムでの変更が必要ですHCL Unica.以下のセクションで説明されているステップを実行してください。

- [Campaign での配信機能の有効化 on page 8](#)
- [Deliver の手動登録 on page 7](#)
- [Deliver システム・テーブル特性の指定 on page 9](#)
- [Deliverシステムテーブルに必要なマッピングCampaign on page 11](#)
- [ローカルへのアクセスの構成Deliverシステムテーブル on page 10](#)
- [次の Web アプリケーションサーバーの再起動が必要です: Campaign on page 11](#)

環境に複数のパーティションが含まれている場合、これらのステップをそれぞれのパーティションに対して繰り返します。Campaign使用するパーティションUnica Deliver.複数パーティションの作成と使用の詳細については、*Unica Campaign*インストールガイド。

確認中Deliver登録

Unica Deliver Unica Platformとして登録されている必要があります。確認するにはDeliverは正常に登録されました。次の設定を確認する必要があります。Platform .

1. HCL Unica にログインします。
2. **[設定]** > **[構成]** に移動します。
3. Deliver設定カテゴリ次を探します。

Unica Deliverは登録されていますPlatformのときDeliver設定プロパティ階層にカテゴリが表示されます。

What to do next

次のDeliverカテゴリはプロパティ階層に表示されません。Unica 登録方法の詳細は、*Campaign*インストールガイドDeliver手動で。

次のDeliverカテゴリを使用できます。有効Deliverにする必要があります。関数Campaign.

Deliver の手動登録

インストール・プロセス中に Deliver インストーラーが Platform システム・テーブルにアクセスできない場合は、configTool ユーティリティを実行して手動で登録する必要があります。

このタスクについて

デフォルトでは、Campaign インストーラーは Deliver を Platform システム・テーブルに自動的に登録します。ただし、Deliver は使用可能化されません。場合によっては、Campaign インストーラーは、自動的に Deliver を登録する際に Platform システム・テーブルに接続しません。

インストーラーによって Deliver が自動的に登録されない場合は、HCL Unica インストール済み環境に含まれる configTool ユーティリティを使って Deliver を手動で登録する必要があります。configTool ユーティリティは、Platform インストール済み環境の tools\bin ディレクトリーにあります。

手動で Deliver を登録するには、以下のコマンドを使用して configTool ユーティリティを実行します。

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

Deliver インストール・ディレクトリーは、Campaign インストール・ディレクトリーのサブディレクトリーです。

Campaign での配信機能の有効化

About this task

インストール Campaign の場合、インストーラはインストールも実行します。Deliver で、デフォルトのパーティションに追加しますが、有効にはしません。Deliver 機能は、有効にするまで使用できません Deliver.

有効にする Deliver 次の構成プロパティを使用して、Unica Platform .

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

有効にするには Deliver 値を yes に変更します。

What to do next

登録要件

登録中 Deliver と Unica Platform は操作する必要があります Deliver. 登録した Deliver と Platform インストール時 Unica Campaign.

有効にした後 Deliver、確認 Deliver は正しく登録されています Unica Platform. 詳しくは、[確認中 Deliver 登録 on page 7](#) を参照してください。

表示中 Deliver メニューオプション

使用する Unica Deliver の場合、システム設定を更新する必要があります。Deliver 表示 Unica Platform インターフェースを指定します。Campaign をインストールする場合、インストーラーはデフォルト区画に「配信」メニューもインストールします。Campaign インストーラーがプラットフォームシステムテーブルに接続しない場合、以下のステップを使用して、手動でそれらを構成する必要があります。必要なオプションを表示するには、システムに提供されている configTool ユーティリティを使用します。HCL Unica インストールされます。

それぞれに固有のパラメータを指定して configTool を実行する必要があります。Deliver をクリックします。configTool を実行すると、システム構成の設定が更新されます。変更を適用するには、Web アプリケーションサーバーを再起動する必要があります。ただし Deliver と共にインストールされます Campaign、メニューオプション Deliver configTool を実行して Web アプリケーションサーバーを再起動するまでは表示されません。ツールのディレクトリ Platform インストール、configTool ユーティリティは bin フォルダにあります。



Note: ファイルへのパスを指定する必要があります。DeliverインストールディレクトリをconfigToolパラメーターとして指定します。Deliver インストール・ディレクトリーは、Campaign インストール・ディレクトリーのサブディレクトリーです。

- 表示**Deliver設定**メニューの**設定**です。

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|settingsMenu" -f " Deliver_installation_ディレクトリへのフルパス\conf\deliver_op_odSettings_navigation.xml"
```

- 表示**[Deliverキャンペーン]**メニューの**メーリング**。

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|Campaign" -f " Deliver_installation_ディレクトリへのフルパス\conf\deliver_op_mailings_navigation.xml"
```

- **キャンペーンメニューにクイックビルダ**を表示します。

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu| Campaign" -f "Deliver_installation_ディレクトリのフルパス"
```

- 表示**[Deliverキャンペーン]**メニューの**文書**。

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

- 表示**[Deliver分析]**メニューの**[分析]**をクリックしてください。

```
configTool.bat -v -i -p "Affinium|suite|uiNavigation|mainMenu|Analytics" -f " Deliver_installation_ディレクトリへのフルパス\conf\deliver_op_analytics_navigation.xml"
```

メニューオプションが正常に追加されたことを確認するには、Web アプリケーションサーバーを再起動した後、ログインします。HCL Unicaをクリックし、**[設定]**、**[キャンペーン]**、**[分析]**メニューを開いて、以下を確認してください。Deliverオプションが表示されます。

Deliver システム・テーブル特性の指定

Unica Deliver では、インストール済み環境の Deliver システム・テーブルについて、タイプ、スキーマ、および JDBC 接続を説明する情報が必要です。Campaign インストール・プロセスの一環として、Campaign スキーマに Deliver システム・テーブルが作成されます。

- **「設定」 > 「構成」 > 「配信」 > 「パーティション」 > 「パーティション [n]」 > 「データソース」 > 「システム・テーブル」**に移動します。
- 以下のパラメーターの情報を確認および更新します。



注: ここでは、Campaign システム・テーブルの情報を想定しています。

データベース・タイプ

スキーマ名

jdbcBatchSize

jdbcClassName

jdbcURI

asmDataSourceForDBCredentials - UA_SYSTEM_TABLES である必要があります

- 以下の構成プロパティに必要な情報を入力します。

構成プロパティの設定について詳しく学ぶには、各プロパティの Platform オンライン・ヘルプを参照してください。

- Deliver > partitions > partition [n] < dataSources > systemTables > type
- Deliver > partitions > partition [n] < dataSources > systemTables > schemaName
- Deliver > partitions > partition [n] < dataSources > systemTables > jdbcBatchSize
- Deliver > partitions > partition [n] < dataSources > systemTables > jdbcClassName
- Deliver > partitions > partition [n] < dataSources > systemTables > jdbcURI

次にやるべきこと

構成プロパティおよび Deliver の構成の詳細については、[「Unica Deliver の構成 ページ 42」](#)を参照してください。

ローカルへのアクセスの構成Deliverシステムテーブル

Unica Deliverへのアクセス権が必要ですDeliverシステムテーブルCampaignスキーマを参照してください。Unica Delivery コンポーネントが、手動でデータベースにログインすることなく、Campaign スキーマのシステムテーブルにアクセスできるようにするには、Deliverシステムユーザーが、必要なデータベースアクセス資格情報を提供します。

About this task

データベースにアクセスするシステムユーザーは、Unica Platformクライアントデータベースをホストするデータベースのログイン資格情報を含むデータソース。Campaignスキーマを参照してください。

システムテーブル設定プロパティの詳細については、[を参照してください。Deliver | partitions | partition\[n\] | dataSources | systemTables on page 54.](#)

1. 定義したシステムユーザーを指定しますUnica Platform.次の構成プロパティを編集します。

```
Deliver > パーティション > パーティション [n] < dataSources > systemTables > asmUserForDBCredentials
```

2. 次のデータベースのログイン資格情報を指定します。CampaignスキーマとDeliverシステムテーブル。次の構成プロパティを編集します。

```
Deliver > パーティション > パーティション [n] < dataSources > systemTables > AMDataSourceForDBCredentials
```

Deliverシステムテーブルに必要なマッピングCampaign

マップする必要がありますDeliverシステムテーブルCampaignスキーマから対応Deliverデータベーステーブル。[Deliverシステムテーブルが**Deliver**。

Campaign, 次をマップしますDeliverシステムテーブル。

- Deliver出力リストテーブル
- Deliver出力リストのユーザーフィールドマッピングテーブル
- Deliverメーリングテーブル
- Deliverメールインスタンステーブル
- Deliverデータテーブルの列マッピングテーブル
- Deliverパーソナライゼーションフィールドマッピングテーブル
- Deliver個人設定のフィールド使用表

マッピングテーブルの詳細については、*Unica Campaign*管理者ガイド。

次の Web アプリケーションサーバーの再起動が必要です: Campaign

に変更を加えた後CampaignandDeliver設定を変更するには、ホストしている Web アプリケーションサーバーを再起動する必要がありますCampaign。

再起動の方法については、Web アプリケーションサーバーの資料を参照してください。

Chapter 3. メッセージサービスへの接続

提供するメッセージサービスにアクセスするにはUnicaの場合、ローカル間の接続を設定する必要があります。HCL UnicaインストールとHCL Unica.

マーケターのアクセスDeliver機能を介してCampaignインターフェースを指定します。使用Deliver安全な自動インターネット接続を確立する必要があります。Campaignを使用してメールのアップロードを行うには、受信者リストをHCL Unica.DeliverインストールするコンポーネントCampaignまた、この接続を使用して、連絡先と返信データをダウンロードするために使用しますDeliverシステムテーブルCampaignスキーマを参照してください。



Note: 各インスタンスCampaignへの固有の接続が必要ですHCL Unica.次のCampaignインストールに複数のパーティションが含まれています。各パーティションには個別のホストメールアカウントが必要です。これらのアカウントは、次への IP 接続を共有できます。HCL Unica .

間のすべての通信HCL UnicaandHCL Unicaホストサービスは SSL 上で実行されます。HCL Unicaからの各通信ホストサービスは、ローカル環境からの要求への応答です。HCL Unicaホストされているサービスが、会社ネットワークとの接続を開始することはありません。すべての通信HCL Unicaホストサービスが会社のファイアウォールの後ろから開始されます。

への接続を設定するための要件HCL Unicaホストサービス

への接続の構成HCL Unicaホストサービスを使用するには、管理許可と、組織用に確立されたホストメールアカウントに関する情報が必要です。

ホストメール接続を設定するには、以下が必要です。

- ユーザー名とパスワードの提供Unicaホストされているメールアカウント
- システムユーザーを作成または変更する権限Unica Platform
- ローカルインストールUnica Platformで維持される構成プロパティへの管理アクセス
- がインストールされている Web アプリケーションサーバーへの管理アクセス。Unica Platform andCampaignデプロイされています

あなたは、会社のデータセキュリティ要件を知っている、または知っている人に相談できる必要があります。開始する前に、これらの手順を確認して、会社のファイアウォールの制限に従って必要な接続を作成する方法を理解してください。

Web アプリケーションサーバーである IBM WebSphere®、Oracle WebLogic、Apache Tomcat、JBoss で信頼できる接続を構成する方法を理解する必要があります。

にデータをアップロードするための要件HCL Unicaホスレッドサービス

ADeliver受信者リストアップローダー (RLU) と呼ばれるコンポーネントは、Unica Campaignインストール。RLU は、パッシブモードの FTP を使用して、メーリングリストと関連付けられたメタデータのアップロードを管理します。HCL Unicaホストされているサービス。

Deliverパッシブ FTP を使用してデータのアップロード。パッシブ FTP を使用する場合、RLU はローカルクライアントとしてすべてのアップロード接続要求を開始します。HCL Unicaホストされているサービスがネットワークに接続要求を開始することはありません。

Delivery は、明示的 FTP と明示的 FTP の 2 つのパッシブ FTP 方法をサポートしています。明示的 FTP は、受信者リストのアップロードに使用されるデフォルトの方法です。明示的 FTP を使用するには、Deliver構成プロパティ。

パッシブモードでの FTP および FTP over SSL の使用の詳細については、RFC959 と RFC2228 を参照してください。

接続とポートの要件

通信HCL Unicaホストサービスを使用するには、インターネットへの接続が必要です。HCL Unicaホストサービスは特定のポートを使用します。

ローカルHCL UnicaインストールとHCL Unicaホストサービスは、通信に次のポートを使用します。

HTTPS: ポート 443

FTP コマンドポート:

- 明示 FTP: ポート 21
- 暗黙的 FTP: ポート 990

FTP データアップロードポート

- 米国のデータセンター

明示的 FTP: ポート 15393 から 15443

インプリシット FTP: ポート 15600 から 15650

- ヨーロッパのデータセンター

明示的 FTP: ポート 15393 から 15443

インプリシット FTP: ポート 15600 から 15650

HCL Unicaホストされているサービスがローカルネットワークとの接続を開始することはありません。ファイアウォールの後ろから開始された接続要求にのみ応答します。

IP をホワイトリストに登録する

受信者リスト (OLT) を FTP 配信サーバーにアップロードするには、キャンペーン Web が実行されているサーバーの外部 IP が、オンデマンド配信サーバー側でホワイトリストに登録されている必要があります。

次のコマンドを使用して外部 IP を取得し、オンボードチームに提供する必要があります。オンボードチームが、ユーザーのサーバーから FTP Deliverサーバーへの FTP 要求を許可する IP のホワイトリストを要求します。

- Unix システムで `curl ifconfig.me` コマンドを実行して、サーバーの外部 IP を取得します。
- Windows システムでは、`http://ifconfig.me` にアクセスして、サーバーの外部 IP を取得できます。

SFTP によるアップロード接続

受信者リスト・アップローダー (RLU) は、受信者リストを安全にアップロードするための優先メカニズムとして SFTP プロトコルを使用します。RLU は、SFTP ポート 2222 を介して HCL Unica ホスト・サービスとの接続を確立します。セキュアな接続を介して RLU は SFTP サーバーと認証の詳細をネゴシエートし、認証が成功すると受信者リストをアップロードします。

次の図は、この方法で Campaign から HCL Unica ホスト・サービスに受信者データをアップロードする様子を示しています。

「構成」ページの「ftpProtocol」(serverComponentsAndLocations -> hostedServices) の下には「SFTP」オプションがあります。

RLU は SFTP サーバーに接続し、受信者リストを SFTP サーバーにアップロードします。認証サーバーへの接続には、証明書ベースの認証が使用されます。PEM ファイルで構成された SSH 秘密鍵と known_hosts ファイルで構成された SSH RSA フィンガープリントを使用して、SFTP サーバーとの接続を確立します。Deliver パーティションごとに個別の PEM ファイルを構成できるように、Deliver アカウントごとに個別の PEM ファイルを構成する必要があります。RLU には、PEM ファイルに加えて、SSH サーバー・フィンガープリントを含む known_hosts ファイルが必要です。これは、パス `Affinium|Deliver|serverComponentsAndLocations|hostedServices`、および、RLU が known_hosts ファイル内の事前構成された SSH サーバー・フィンガープリントを必要とするかどうかを制御するフラグで、グローバルに設定されます。

認証が完了すると、受信者リストのアップロードは SFTP を使用して行われます。トリガーされる場所からの Deliver プロセス・ボックス実行に影響はありません。

`passPhrase` を使用して公開鍵または秘密鍵を生成する場合は、「`amUserForAcctCredentials`」で指定された Platform ユーザーの下に、「`SFTP_PASSPHRASE_DATASOURCE`」という名前の新しいデータソースを作成します。例えば「`asm_admin`」とし、公開鍵または秘密鍵の生成時に使用したものと同一パスワードまたは `Passphrase` をこのデータソースに指定します。データ・ソース・ログインは、任意のテキストとして言及できます。

`passPhrase` を使用して公開鍵または秘密鍵を生成しない場合は、データソースを作成しないでください。

鍵を生成するには、次の手順を行います。

SFTP 認証用の公開鍵と秘密鍵のペアを生成する手順。

1. 鍵ペアを作成する

最初の手順では、Campaign Web がインストールされているマシンに鍵ペアを作成します。Campaign Web がインストールされているマシンにログインします。コマンド・プロンプトを開いて、次のコマンドを実行します。

```
ssh-keygen
```

2. 鍵を保存する場所を指定します。

Enter キーを押すと、ホーム・ディレクトリーの .ssh ディレクトリー内にあるデフォルトの場所にファイルを保存できます。または、プロンプトの後に別のファイル名または場所を入力して Enter キーを押すことで、別のファイル名または場所を選択できます。

3. パスフレーズを作成します。

ssh-keygen からの 2 番目と最後のプロンプトでは、パスフレーズの入力を求められます。パスフレーズを使用するかどうかは、要件によって異なります。

次に例を示します。

```
[root@Host bin]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
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]#
```

公開鍵は - /root/.ssh/id_rsa.pub に保存されます。生成された公開鍵を HCL の構成サポートを通じて Deliver Dev Ops チームに提供します。

SFTP の構成

SFTP を構成するには、以下の手順を実行します。

1. コマンド・プロンプトから <Deliver_Home>/tools に移動して以下のコマンドを実行し、UI で ftpProtocol プロパティを公開します。

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

2. Platform にログインし、**【設定】 > 【構成】** に移動し、Affinium|Deliver|serverComponentsAndLocations|hostedServices の ftpProtocol に **【SFTP】** を選択します。
3. コマンド・プロンプトから <Deliver_Home>/tools に移動して以下のコマンドを実行し、UI で ftpPort プロパティを公開します。

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

- Affinium|Deliver|serverComponentsAndLocations|hostedServices の ftpPort で、ポート番号を 2222 と言及します。
- enforceKnownHostsValidation の値を false のままにし、knowHostsPath プロパティでパスを <Deliver_HOME>/Conf/known_hosts に更新します。

例: knowHostsPath - /opt/HCL/Campaign/Deliver/conf/known_hosts

```
enforceKnownHostsValidation - False
```

- オプション。known_hosts ファイルを使用している場合は、Affinium|Deliver|serverComponentsAndLocations|hostedServices の knowHostsPath プロパティで絶対パスを更新し、enforceKnownHostsValidation を true に設定します。
- プライベート証明書ファイル (id_rsa) を <DELIVER_HOME>/conf にコピーし、Affinium|Deliver|partitions|partition1|hostedAccountInfo の pemFilePath プロパティでこのプライベート証明書ファイルの絶対パスを更新します。

次に例を示します。

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

```
amDataSourceForSftpPassPhrase-- SFTP_PASSPHRASE_DATASOURCE
```

- パスフレーズを指定していた場合は、公開鍵/秘密鍵の生成時に、amUserForAcctCredentials で指定された Platform ユーザー (例: asm_admin) の下に SFTP_PASSPHRASE_DATASOURCE という名前でデータソースを作成し、公開鍵/秘密鍵の生成時に使用したものと同一パスワード/パスフレーズをこのデータソースに指定します。データソース・ログインは、任意のテキストとして言及できます。
- 公開鍵/秘密鍵の生成時にパスフレーズを指定しなかった場合は、asm_admin ユーザーまたは他のユーザーに対してこのデータソース SFTP_PASSPHRASE_DATASOURCE を作成する必要はありません。
- Campaign のアプリケーション・サーバーを再起動します。
- コマンド・プロンプトを開き、<Deliver_home>/bin に移動し、以下のように rlu を使用して SFTP 接続をテストします。

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



Note: 上記で指定したすべてのファイル・パスは、ファイル名を含めて完全である必要があります。Deliver が構成されているすべてのパーティションについて、手順 7~9 を繰り返します。

明示的 FTP によるデフォルトのアップロード接続

デフォルトでは、システムによる受信者リストのアップロード時に、受信者リストアップローダ (RLU) は明示的な FTP を使用します。受信者リストは、出力リストテーブル (OLT) とも呼ばれます。

RLUはとの接続を確立しますHCL UnicaデフォルトのFTPコマンドポート（ポート21）を介してホストされるサービス。SSLを介してセッションを暗号化する要求を発行します。安全な接続を介して、RLUはFTPサーバーとネゴシエートし、RLUによってランダムに選択されたポートを介して個別のSSLリンクを確立します。明示的FTPの詳細については、RFC2228を参照してください。

次の図は、から受信者データをアップロードするためのデフォルトの方法を示していますCampaignにHCL Unicaホステッドサービス。

次の表に、接続シーケンスを示します。

ステップ	アクション	説明
1	最初のクライアントFTP接続要求	<p>RLUは、企業ファイアウォールの背後から、明示的なSSLを介したFTPを使用してデータアップロードセッションを開始します。RLUは、SSL接続要求を次のアドレスに送信します。HCL Unicaホステッドサービス。このアドレスは事前に設定する必要があります。</p> <p>セッションを開始するために、RLUはFTPコマンドポートとしてクライアント側でランダムに選択されたポートを開きます。HCL Unicaホストされているサービスは、ポート21でFTPコマンド接続を受け入れます。</p>
2	リモートFTPサーバーの応答	<p>RLUが安全なSSLセッションを要求することに応答して、FTPサーバーは受信者リストのアップロードに使用するFTPデータポートを指定します。</p>
3	受信者リストのアップロード	<p>RLUは、指定されたデータポートでリストのアップロードを開始します。アップロードが完了すると、RLUはFTP接続をドロップします。</p>

FTPサーバーが指定できるデータポートの範囲については、を参照してください。[接続とポートの要件 on page 13](#)。

明示的 FTP 接続の構成

追加の構成は不要です。RLU は、デフォルトで明示的 FTP を使用します。

明示的 FTP を使用したデータアップロード

明示的 FTP を使用して受信者リストをアップロードするように RLU を設定できます。明示的 FTP は、ポート 990 を使用して接続を確立します。HCL Unicaホストされているサービス。

明示的 FTP 用に RLU を有効にすると、セッション全体が最初から暗号化されます。インプリシット FTP は、RLU が明示的に安全なリンクを要求する明示的な FTP での接続とは異なります。

明示的 FTP を使用して受信者リストをアップロードするには、Deliver構成プロパティ。

下の図は、RLU が受信者データをどのようにアップロードするかを示しています。HCL Unicaホストされたサービス (システムが暗黙 FTP を使用するように設定されている場合)

次の表に、接続シーケンスを示します。

ステップ	アクション	説明
1	最初のクライアントFTP接続要求	<p>RLU は、企業のファイアウォールの後ろから、SSL 上の FTP を使用してデータアップロードセッションを開始します。RLUは、SSL接続要求を次のアドレスに送信します。HCL Unicaホステッドサービス。このアドレスは事前に設定する必要があります。</p> <p>セッションを開始するために、RLU はポート 990 を開きます。HCL Unicaホストサービスは、ポート 990 で暗号化された FTP コマンド接続のみを受け入れます。</p>
2	リモートFTPサーバーの応答	<p>次の場合HCL Unicaホストされているサービスが要求を有効な暗黙的な FTP 要求として認識した場合、FTP サーバーは接続要求を受け入れます。受信者リストのアップロードに使用する FTP データポートを指定します。</p> <p>FTP サーバーが指定できるデータ ポートの範囲については、接続とポートの要件 on page 13を参照してください</p>
3	受信者リストのアップロード	<p>RLUは、指定されたデータポートでリストのアップロードを開始します。アップロードが完了すると、RLUはFTP接続をドロップします。</p>

暗黙的 FTP アップロードの設定パラメータへのアクセス

データのアップロードに明示的 FTP を使用するようにシステムを構成するには、デフォルトでは非表示になっている設定プロパティを編集する必要があります。プロパティを表示するスクリプトを実行します。

About this task

データのアップロードに明示的 FTP を使用するようにシステムを構成するには、以下の設定プロパティを表示します。これらのプロパティはデフォルトでは非表示です。

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

この手順では、構成プロパティが表示されますが、構成はしません。明示的 FTP を有効にするには、Deliver をクリックして、それらを構成します。これらのプロパティにアクセスする必要があります。[明示的 FTP アップロードの有効化 on page 19](#) これらのプロパティの構成方法については、[を参照してください](#)。

ftpPort と use FTPImplicitSSL を表示するには、Deliver インストールの **Tools** ディレクトリで、以下のようにコマンド行スクリプトから switch_config_visibility スクリプトを実行します。

Windows™

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

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

UNIX™

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

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

What to do next

これらのプロパティをウィンドウに表示するには、Web アプリケーションサーバーを再起動する必要があります。Deliver 削除します。

明示的 FTP アップロードの有効化

明示的 FTP を有効にするには、Deliver 削除します。

Before you begin

このタスクを完了するには、2 つの構成プロパティを公開する必要があります。詳しくは、「[暗黙的 FTP アップロードの設定パラメータへのアクセス on page 18](#)」を参照してください。

1. Navigate to Settings > Configuration > Deliver > serverComponentsAndLocations > hostedServices にナビゲートします
2. **[設定の編集]** をクリックします。
 - UseFTPImplicitSSL が true に設定されていることを確認します。
 - ftpPort を 990 に設定します。
3. 変更を保存します。

What to do next

変更は、Web アプリケーションサーバーを再起動して、Campaign listener:これは、すぐに実行することも、すべてのスタートアップ設定ステップが完了するまで待つこともできます。

HTTP プロキシを介した接続

会社のファイアウォールルールが、公共のインターネットとの直接通信を禁止している場合、インターネットに接続できません。HCL Unica HTTP プロキシサーバー経由。Deliverは、HTTPS と FTPS トラフィックの両方を許可する SOCKS プロキシサーバー経由の接続をサポートします。

Deliverは、SOCKS プロトコルバージョン 5 をサポートします。

次の図は、SOCKS プロキシを使用した場合のローカル環境とホスト環境間の通信を示しています。

ローカルの設置環境で SOCKS プロキシサーバーを構成します。プロキシサーバーの設定を開始する前に、以下の要件を満たしていることを確認してください。

- プロキシサーバーは SOCKS プロキシサーバーである必要があります。
- プロキシサーバーは、Deliver OD 環境。サーバーは、ホストメールアドレスで使われるデータセンター用に構成されたポートとのトラフィックを許可する必要があります。Unicaは、米国とヨーロッパにデータセンターを保守しています。
- [Deliver OP 環境は、SOCKS プロキシサーバーにアクセスできなければなりません。

SOCKS プロキシを経由する FTPS および HTTPS トラフィックのルーティングの構成

SOCKS プロキシを使用してホストされている E メールリソースにアクセスするには、Campaign をデプロイした Web アプリケーションサーバーを更新する必要があります。また、Deliver RCT と RLU。

- FTPS トラフィックの場合、以下の設定を RLU と Web アプリケーションサーバーに適用します。

設定	説明
<code>-Dhcl.unica.deliver.ftps.proxy.host = <socksHost></code>	SOCKS プロキシのホスト名または IP。
<code>-DhCL.unica.deliver.ftps.proxy.port = <socksPort></code>	SOCKS プロキシが実行されているポート。
<code>-DhCL.unica.deliver.ftps.proxy.match.hosts= <ホスト名と IP アドレスのカンマで区切られたリスト></code>	SOCKS プロキシにトラフィックをルーティングするときに使

設定	説明
	用されるホスト名と IP アドレス。アカウントで使用されているデータセンターに固有の値を指定します。

ローカル環境とホストされた環境がデータ接続を確立する場合、リモート FTP サーバーがローカル FTP クライアントに送信する IP アドレスは、 `-Dhcl.unica.deliver.ftps.proxy.match.hosts` です。

`-DhCL.unica.deliver.ftps.proxy.match.hosts` を次のいずれかの値に設定します。入力する値は、ホストメールアカウントで使用されているデータセンターによって異なります。

US データセンターのホスト名と IP アドレス:

```
-DhCL.unica.deliver.ftps.proxy.match.hosts=
FTP-em.unicadeliver.com
```

ヨーロッパデータセンターのホスト名と IP アドレス:

```
-DhCL.unica.deliver.ftps.proxy.match.hosts=
FTP-eu.unicadeliver.com
```

- HTTPS トラフィックの場合、RCT と Web アプリケーションサーバーに以下の設定を適用します。

設定	説明
<code>-DhCL.unica.deliver.https.proxy.host=<sockshost></code>	SOCKS プロキシのホスト名または IP
<code>-DhCL.unica.deliver.https.proxy.port=<socksPort></code>	SOCKS プロキシが実行されているポート

設定	説明
<code>-DhCL.unica.Deliveryr.https.proxy.type=SOCKS</code>	プロキシサーバーの種類。SOCKS プロキシサーバーを使用する必要があります。

SOCKS プロキシにアクセスするための認証の構成

SOCKS プロキシが認証を必要とする場合、アクセス資格情報を提供するように Web アプリケーションサーバー、RLU、RCT を設定する必要があります。

Web アプリケーションサーバー、RLU、RCT 用に以下を設定します。ユーザー名とパスワードの値は、プロキシに対する認証に必要な資格情報である必要があります。

```
-DhCL.unica.deliver.proxy.auth.user = <ユーザー名>
```

```
-DhCL.unica.deliver.proxy.auth.password = <パスワード>
```

SOCKS プロキシを使用するための RCT 構成

SOCKS プロキシサーバーを介して通信するには、RCT を変更する必要があります。必要な設定は、オペレーティングシステムによって異なります。

- Windows™環境の RCT の場合、以下のプロキシ引数を `Common.bat` に追加します。

`Common.bat` ファイルは、ローカル・システムの `\deliver\bin` ディレクトリーにあります。Deliver インストールされません。

```
set RCT_PROXY_ARGS=

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

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

-DhCL.unica.Deliveryr.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% を設定します %RCT_MEM_ARGS%

%RCT_EXTRA_VM_ARGS% %RCT_PROXY_ARGS%
```

- UNIX™環境の RCT の場合、以下のプロキシ引数を `Common.sh` に追加します。

Common.shファイルは、ローカル・システムの`/deliver/bin`ディレクトリーにあります。Deliverインストールされません。



Note: `rlu.sh`、`rct.sh`、または`setenv.sh`を直接変更しないでください。変更が上書きされます。

```
RCT_PROXY_ARGS=

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

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

-DhCL.unica.Deliveryr.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} "
```

SOCKS プロキシを使用するための RLU の設定

SOCKS プロキシサーバーを経由して通信するには RLU を変更する必要があります。必要な設定は、オペレーティングシステムによって異なります。

- Windows™環境の RLU の場合、以下のプロキシ引数を `Common.bat` に追加します。

`Common.bat`ファイルは、ローカル・システムの`\deliver\bin`ディレクトリーにあります。Deliverインストールされません。

```
RLU_PROXY_ARGS=を設定します

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

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

-DhCL.unica.deliver.https.proxy.match.hosts=<ホスト名と IP アドレスのカンマで区切られたリスト>

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

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

設定 RLU_JAVA_ARGS=%BASE_VM_ARGS% %RLU_MEM_ARGS% %RLU_EXTRA_VM_ARGS%

%RLU_PROXY_ARGS%
```

- UNIX™環境の RLU の場合、以下のプロキシ引数を `Common.sh` に追加します。

Common.shファイルは、ローカル・システムの`/deliver/bin`ディレクトリーにあります。Deliverインストールされません。



Note: `rlu.sh`、`rct.sh`、または`setenv.sh`を直接変更しないでください。変更が上書きされます。

```
RLU_PROXY_ARGS=

-DhCL.unica.deliver.ftps.proxy.host=<PROXY_HOST>

-DhCL.unica.deliver.ftps.proxy.port=<PROXY_PORT>

-DhCL.unica.deliver.ftps.proxy.match.hosts=<ホスト名と IP アドレスのカンマで区切られたリスト>

-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}"
```

SOCKS プロキシを使用するための Web アプリケーションサーバー設定

接続先HCL UnicaSOCKS プロキシを経由する場合、Web アプリケーションサーバーの設定を変更する必要があります。対象Unica WebSphere®サーバーの場合、一般 JVM 引数を変更する。Oracle Weblogic サーバーの場合は、`SetDomainEnv`スクリプトを変更します。

- Web アプリケーションサーバーがUnica WebSphere®の場合、WebSphere®の一般 JVM 引数に以下を追加します。

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

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

-DhCL.unica.Deliveryr.https.proxy.type=SOCKS

-DhCL.unica.deliver.ftps.proxy.host=<PROXY_HOST>

-DhCL.unica.deliver.ftps.proxy.port=<PROXY_PORT>

-DhCL.unica.deliver.ftps.proxy.match.hosts=<ホスト名と IP アドレスのカンマで区切られたリスト>

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

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

- Web アプリケーションサーバーが Oracle Weblogic の場合、`setDomainEnv`スクリプトを変更します。必要な設定は、オペレーティングシステムによって異なります。

Windows™環境で、以下の変更を行います。

```
Java_OPTIONS =%{JAVA_OPTIONS}

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

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

-DhCL.unica.Deliveryr.https.proxy.type=SOCKS

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

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

-DhCL.unica.deliver.https.proxy.match.hosts=<ホスト名と IP アドレスのカンマで区切られたリスト>

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

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

UNIX™環境の場合、以下の変更を行います。

```
Java_OPTIONS ='${JAVA_OPTIONS}

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

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

-DhCL.unica.Deliveryr.https.proxy.type=SOCKS

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

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

-DhCL.unica.deliver.https.proxy.match.hosts=<ホスト名と IP アドレスのカンマで区切られたリスト>

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

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

データダウンロードの頻度とポート設定

ADeliver Response and Contact Tracker (RCT) と呼ばれるコンポーネントは、ユーザーの一部としてインストールUnica Campaignされます。RCT は、定期的にメールの返信とトラッキングデータHCL Unicaを要求しています。デフォルトでは、RCT は 5 秒ごとにデータ要求を発行します。

RCT は HTTPS (HTTP over SSL) 上でデータ要求を発行します。HCL Unicaホストサービスは、ホストメールアカウントの起動プロセス中に指定したホストからのみ、ポート 443 で HTTPS 接続要求を受け入れます。

HCL Unica ホスト・サービスにアクセスするシステム・ユーザーの構成

Deliver コンポーネントは、ログイン資格情報の手動入力が必要とせずに、HCL Unica ホスト・サービスにアクセスできなければなりません。自動ログインを確立するには、Platform に、必要なアクセス資格情報を提供できるシステム・ユーザーを定義します。

ユーザー管理およびトラブルシューティングを単純にするために、既存のシステム・ユーザーがホスト・サービスおよびローカル・システム・テーブルにアクセスするように変更することができます。複数のシステムに資格情報を提供する単一のシステム・ユーザーを構成できます。例えば、Campaign システム・ユーザーの構成を変更することで、HCL Unica ホスト・サービスおよび Campaign スキーマの Deliver システム・テーブルに自動的にアクセスできる単一のユーザーを作成します。

HCL Unica ホスト・サービスにアクセスするために必要な資格情報は、ご使用のホストされたメッセージング・アカウント用に Unica から提供されるユーザー名とパスワードです。使用する資格情報は、Unica の米国のデータ・センターに接続するか、Unica がヨーロッパで保守しているデータ・センターに接続するかによって異なります。どちらのデータ・センターを使用するかを決定するには、Unica にご相談ください。

HCL Unica ホスト・サービスと通信するシステム・ユーザーの構成方法に関する具体的な情報については、「*Unica Deliver 起動および管理者ガイド*」を参照してください。

システム・ユーザーおよびデータ・ソースの作成方法に関する一般情報については、「*Unica Platform 管理者ガイド*」を参照してください。

HCL Unica ホスト・サービスへのパーティション・アクセスの構成

パーティション内の Unica Deliver コンポーネントは、HCL Unica ホスト・サービスとの通信を試みる際に、有効なログイン資格情報を自動的に提供できるようになっていなければなりません。そのためには、Platform ユーザーに HCL Unica ホスト・サービス・ログイン資格情報を追加する必要があります。このユーザーは、Deliver システム・ユーザーになります。

HCL Unica ホスト・サービス資格情報を格納するプラットフォーム・データ・ソースを、Deliver システム・ユーザーに追加できます。このユーザーは、パーティション内の Campaign システム・テーブルにアクセスするシステム・ユーザーと同じであっても構いません。

パーティションのシステム・ユーザーを構成するための手順は、Deliver の初期インストール時に、最初のパーティションを作成するために従った手順と同じです。HCL Unica ホスト・サービス・ログイン資格情報をシステム・ユーザーに追加する方法について詳しくは、「*Unica Deliver 起動および管理者ガイド*」を参照してください。

HCL Unica ホスト・サービスにアクセスするために必要な資格情報は、最初の起動プロセスで Unica から提供されるユーザー名とパスワードです。

 **重要:** 追加するパーティションごとに、個別のユーザー名およびパスワードを Unica に要求する必要があります。

HCL Unica ホスト・サービスにアクセスするシステム・ユーザーの構成

Campaign の Deliver コンポーネントは、ログインを要求することなく、HCL Unica ホスト・サービスに自動的にアクセスできる必要があります。Unica Platform で構成されているシステム・ユーザーは、必要なユーザー名とパスワードを提供するデータ・ソースを参照できます。データ・ソースは、新しいシステム・ユーザーにも、既存のシステム・ユーザーにも追加できます。ユーザー管理を簡素化するために、Campaign スキーマにアクセスするように構成済みのシステム・ユーザーを更新して、HCL Unica ホスト・サービスにもアクセスできるようにすることができます。

開始する前に

このタスクを完了するには、ホストされている E メール・アカウントに Unica が割り当てた HCL Unica ホスト・サービスのユーザー名とパスワードを知っている必要があります。ユーザー名とパスワードの受信は、アカウントの起動プロセスの一部です。

適切なアクセス権限を持っていて、Unica Platform でシステム・ユーザーとデータ・ソースを作成する方法を理解している必要があります。

このタスクについて

 **注:** インストール済み環境に複数のパーティションが含まれている場合は、パーティションごとにこのタスクを実行する必要があります。パーティション間でシステム・ユーザーを共有することはできません。

1. HCL Unica ホスト・サービスにアクセスするのに必要なユーザー名とパスワードを格納する Platform データ・ソースを作成します。最良の結果を得るため、およびメンテナンスを容易にするために、このデータ・ソースに UNICA_HOSTED_SERVICES という名前を付けます。このデータ・ソースを次のように構成します。

「データ・ソース・ログイン」で、アカウントの起動時に Unica から受け取ったユーザー名を入力します。

「データ・ソース・パスワード」で、アカウントの起動時に Unica から受け取ったパスワードを入力します。

2. Deliver 構成内のデータ・ソースを指定します。**amDataSourceForAcctCredentials** 構成プロパティを使用します。

この構成プロパティは、Deliver > partitions > partition[n] > hostedAccountInfo > **amDataSourceForAcctCredentials** にあります。

デフォルトでは、指定されたデータ・ソースは UNICA_HOSTED_SERVICES です。

3. HCL Unica ホスト・サービスにアクセスするシステム・ユーザーを指定します。既存のユーザーを指定したり、ユーザーを作成したりできます。Deliver 構成では、**amUserForAcctCredentials** 構成プロパティを使用します。

この構成プロパティは、Deliver > partitions > partition[n] > hostedAccountInfo > **amUserForAcctCredentials** にあります。

デフォルトでは、指定されたユーザーは `asm_admin` です。

4. 手順1で構成したデータ・ソースを、手順3で指定したシステム・ユーザーに追加します。

次にやるべきこと

構成の変更を有効にするには、Webアプリケーション・サーバーを再始動する必要があります。

接続アドレスの設定HCL Unicaホストサービス

に正しく接続するにはHCL Unicaホストされているサービスを使用するには、ウィンドウの設定プロパティの値としてアドレスを入力する必要があります。Deliver削除します。入力する接続アドレスは、Unica米国のデータセンターまたはUnicaヨーロッパにあるデータセンター。

Before you begin

問い合わせUnicaホストされているメールアカウントが使用しているデータセンターを確認してください。

インUnica Platform、**[設定] > [構成]**に移動します。[Deliver設定です。次の場所に移動します。Deliver構成プロパティを参照し、アカウントで使用しているデータセンターに応じて、接続設定を確認または更新します。

- 「配信」 > 「serverComponentsAndLocals」 > 「hostedServices」 > `uiHostName`

米国の Unica データセンターに接続するには、この値を `em.unicadeliver.com` に変更します。

に接続するにはUnicaヨーロッパにあるデータセンターについては、この値を次のように変更します。

`em-eu.unicadeliver.com` .

- Deliver > serverComponentsAndLocations > hostedServices> `dataHostName`

米国の Unica データセンターに接続するには、この値を `em.unicadeliver.com` に変更します。

に接続するにはUnicaヨーロッパにあるデータセンターについては、この値を次のように変更します。

`em-eu.unicadeliver.com` .

- Deliver > serverComponentsAndLocations > hostedServices> `ftpHostName`

米国の Unica データセンターに接続するには、この値を `ftp-em.unicadeliver.com` に変更します。

に接続するにはUnicaヨーロッパにあるデータセンターについては、この値を次のように変更します。

`ftp-eu.unicadeliver.com` .

What to do next

設定プロパティを変更した場合、Webアプリケーションサーバーを再起動して変更を適用してください。

配信ホスト名のIPアドレス

会社のファイアウォールでホスト名の配信用の IP アドレスをホワイトリストに載せる必要がある場合は、次の IP アドレスを使用します。

`em.unicadeliver.com`: 13.248.215.130 と 76.223.84.165

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

`FTP-em.unicadeliver.com`: 192.190.152.236

`FTP-eu.unicadeliver.com`: 192.190.153.236

ホストメールの安全な通信の構成

メールマーケターとの間の通信 HCL Unica ホストされるサービスは SSL 上で発生します。SSL を使用するには Web アプリケーションサーバー設定を変更する必要があります。Java™ `keytool` ユーティリティを使用して、必要な変更を行う必要があります。

保護された通信を構成するには、以下のアクションを含めます。

- 信頼できるキーストアを生成します。
- 次からのデジタル証明書の取得 HCL Unica ホストされているサービス。
- 信頼できるキーストアを Web アプリケーションサーバーに追加します。
- インポートする HCL Unica ホストされているサービスのデジタル証明書を信頼できるキーストアに。

SSL の設定に必要な正確なステップと順序は、デプロイした Web アプリケーションサーバーのタイプとバージョン (WebSphere®、WebLogic、Tomcat、JBOSS) によって異なります。Unica Platform and Unica Campaign。

WebSphere については、を参照してください。 [WebSphere 使用時の SSL の構成 on page 31](#) .

WebSphere® の場合は、を参照してください。 [WebSphere 使用時の SSL の構成 on page 33](#) .

信頼できるキーストアの生成

構成用の ID キーストアと信頼できるキーストアを作成するには、この手順に従います。Unica Deliver 通信先 HCL Unica SSL 上のホストされたサービス。SSL の設定時に、Web アプリケーションサーバーにキーストアを追加します。

About this task

HCL は、このセクションの手順で次のサンプル値を使用します。

- ID キーストア: `HCLUnicaClientIdentity.jks`
- ID キーストアの別名: `HCLUnicaClientIdentity`
- ID キーストアのパスワード (`-storepass`): `clientPwd`
- ID キーストアのセキュリティキー (`-keypass`): `clientPwd`
- ID キーストアに基づく証明書: `ClientCertificate.cer`

- 信頼できるキーストア: `HCLUnicaTrust.jks`
- 信頼できるキーストアのパスワード (`-storepass`): `TrustPwd`

実際に入力する値は、ご使用のシステムに固有のものである必要があります。

この手順のステップを実行するには、コマンド行からJava™ `keytool`ユーティリティを実行します。

1. ID キーストアを生成します。次の例に示すように、`genkey`コマンドを使用します。

この例では、`HCLUnicaClientIdentity.jks`という ID キーストアを作成します。作成する ID キーストアに別の名前を使用できます。

Example

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

次のことに注意してください。

- この手順の後の方、および Web アプリケーションサーバーで SSL を設定するときに、別名、キーストア、キーパス、ストアパスの値を使用します。
- WebSphere®の場合、キーストアパスワード (`-storepass`) とキーパスワード (`-keypass`) は同じである必要があります。
- 識別名 (`-dname`) で、共通名 (CN) がアクセスに使用するホスト名と同じである HCL Unicaホストされているサービス。たとえば、HCL Unicaホストされているサービスが `https://hostName.example.com:7002/unica/jsp` の場合、CN は `hostName.example.com` です。識別名の CN 部分は、必須の部分です。組織 (o) と組織単位 (ou) は必須ではありません。

2. ID キーストアに基づいて証明書を生成します。次の例に示すように、`export`コマンドを使用します。

この例では、`ClientCertificate.cer`という名前の証明書を生成します。作成する証明書に別の名前を使用できません。

`keystore`、`storepass`、および別名の値は、ID キーストアに指定した値と一致している必要があります。

Example

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

3. 信頼できるキーストアを生成します。次の例に示すように、インポートコマンドを使用します。

この例では、`HCLUnicaTrust.jks`という名前の信頼できるキーストアを生成します。作成する信頼できるキーストアに別の名前を使用できます。

Example

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

証明書を信頼するかどうかを確認するプロンプトが表示されたら、**Y**を入力します。

What to do next

以下の変数に定義した値をメモします。値は、例と異なる値であってもよいです。

- 別名(例の場合: `HCLUnicaClientIdentity`)
- ID キーストア(例: `HCLUnicaClientIdentity.jks`)
- ストアパス (例: `TrustPwd`) 信頼できるキーストアのストアパス値は、ID キーストアと証明書のストアパス値とは異なる場合があります。
- キーストア(例: `HCLUnicaTrust.jks`) Web アプリケーションサーバーによっては、ID キーストアも指定します。

これらのインストール固有の値は、システムの Web アプリケーションサーバーで SSL を構成するときに指定します。HCL Unicaインストールされます。

WebSphere 使用時の SSL の構成

このセクションでは、展開している場合に SSL を設定するために必要なステップを説明します。HCL Unica」を参照してください。この変更は、Deliver内部で動作するコンポーネントCampaign通信先HCL UnicaSSL 上のホストされたサービス。

About this task

Oracle WebLogic ユーザーインターフェースのナビゲーションと作業に関する具体的なガイダンスについては、使用している Oracle WebLogic のバージョンの文書を参照してください。

次のタスクを実行してください。

- WebLogic 起動スクリプトの変更
- WebLogic 構成の変更
- 次からのデジタル証明書の取得HCL Unicaホストサービス
- 信頼できるキーストアを作成し、Unicaデジタル証明書

WebLogic 起動スクリプトの変更

デプロイしたCampaignWebLogic では、ローカルにインストールされたサーバー間の安全な通信を WebSphere が認識し、受け入れるように、WebLogic 起動スクリプトと SSL 用の WebLogic 構成を変更する必要があります。DeliverコンポーネントとHCL Unicaホストされているサービス。

WebSphere 起動スクリプトの `Java_OPTIONS` に以下の引数を追加します。

- `-Dweblogic.security.SSL.lowSmallRSAExponent=true`
- WebLogic バージョン 12c 以上: `-Dweblogic.security.SSL.protocolVersion=TLS1`
- 以前のすべてのバージョン: `-Dweblogic.security.SSL.nojce=true`

WebLogic 構成の変更

WebLogic の SSL 構成を変更する必要があります。

WebLogic コンソールを使用して、ドメインの WebLogic SSL 構成に以下の変更を加えます。

ホスト名の検証の設定を「なし」に変更します。

証明書の取得HCL Unicaホストサービス

SSL 通信を設定するには、次の場所からデジタル証明書をダウンロードする必要があります。HCL Unica 証明書の詳細が .cer 拡張子の付いたファイルに保存されます。このファイルは、Web アプリケーションサーバーキーストアにインポートできます。

About this task

既存の SSL 証明書の有効期限が切れると、ホストされているサービスにアクセスできなくなりますHCL Unica。この手順を使用して、新規証明書をダウンロードします。

1. Internet Explorer で、次のアドレスにログインします。HCL Unicaホストメールアカウント用に設定されたホストサービスを指定します。
 - 米国のデータセンターの場合は、移動します。 <https://em.unicadeliver.com>
 - ヨーロッパのデータセンターの場合は、次の場所に移動します。 <https://em-eu.unicadeliver.com>

ログインは失敗しますが、ブラウザを使用して認証要求を送信することを許可します。

2. 鍵アイコンをクリックし、**[証明書の表示]** を選択します。
3. [詳細] タブを選択し、**[ファイルにコピー]** を選択します。

Web アプリケーションサーバーからアクセス可能な場所に、.cer 拡張子を付けてファイルを保存します。作成するファイルは、Web アプリケーションサーバーのキーストアに挿入するデジタル証明書です。

たとえば、証明書を HCLhosted.cer として保存します。

WebLogic 用に信頼されたキーストアを作成し、Unica証明書

Weblogic の場合、Unica証明書を参照してください。

Before you begin

開始する前に、Web ブラウザを使用してHCL Unicaホストされているサービスのデジタル証明書を削除して、.cerファイルとして保存してください。たとえば、証明書の名前をHCLhosted.cerにすることができます(実際のファイル名は別のものでもかまいません)。詳細は、[証明書の取得HCL Unicaホストサービス on page 32](#)を参照してください。 .

About this task

HCL は、このセクションの手順で次のサンプル値を使用します。

- ID キーストア: HCLUnicaClientIdentity.jks
- ID キーストアのパスワード: clientPwd
- 信頼できるキーストア: HCLUnicaTrust.jks
- 信頼できるキーストアの別名: HCLUnicaHostedIdentity

- 信頼できるキーストアのパスワード (-storepass): TrustPwd
- デジタル証明書 (-file) からのUnica: HCLhosted.cer

実際に入力する値は、ご使用のシステムに固有のものである必要があります。

この手順のステップを実行するには、コマンド行からJava™ keytoolユーティリティを実行します。

1. WebLogic 用に信頼されたキーストアを生成します。

詳しくは、[信頼できるキーストアの生成 on page 29](#)を参照してください。

アイデンティティキーストアと信頼できるキーストアをWebLogic 設定で指定します。

2. keytoolユーティリティのインポートコマンドを使用して、HCL Unicaホストされているサービスの証明書を、次の例に示すように、ステップ 1 で作成した信頼できるキーストアにコピーします。
ダウンロードしたデジタル証明書を使用しますUnica.

この手順では、信頼できるキーストアの別名も定義します。

Example

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

証明書を信頼するかどうかを確認するプロンプトが表示されたら、**Y**を入力します。

3. WebLogic 管理コンソールで、サーバーのキーストアを構成します。

設定ルールを指定するには、利用可能な選択肢から「カスタム ID」と「カスタム信頼キーストア」のオプションを選択します。カスタム ID の場合、ID キーストアを指定します。カスタム信頼の場合、信頼できるキーストアを指定します。

例えば、管理コンソールでは、以下を指定します (ステップ 1 で作成した信頼できるキーストアの値の例を使用)。

- **ID**: ID キーストアと関連するパスワードを指定します。

例: HCLUnicaClientIdentity.jks、clientPwdです。

- **信頼**の場合: 信頼できるキーストアと関連するパスワードを指定します。

例: HCLUnicaTrust.jks、TrustPwdです。

両方のキーストアのフルパスを指定します。

4. WebLogic を再始動します。Web アプリケーションサーバーを再起動するまで、設定の変更は実装されません。
5. SSL 接続をテストするには、次のようにログインします。Unica Campaignや、さまざまなメッセージ機能メニューにアクセスできます。メール、ランディングページ、メールを作成できることを確認します。

WebSphere 使用時の SSL の構成

このセクションでは、SSL を設定している場合に、SSL を設定するために必要な一般的なステップを説明します。HCL Unica WebSphere®上のコンポーネント.この変更は、Deliver内部で動作するコンポーネントCampaign通信先HCL UnicaSSL 上のホストされたサービス。

Before you begin

開始する前に、構成プロパティ `uiHostName` の値を知っている必要があります。 `uiHostName` の値は URL です。 HCL Unica ホストサービス。詳しくは、 [接続アドレスの設定 HCL Unica ホストサービス on page 28](#) を参照してください。

About this task

SSL 証明書と鍵管理の設定を変更するには、 WebSphere® セキュリティコンソールにアクセスする必要があります。このタスクでは、 Campaign Web アプリケーションサーバーにアクセスしてください。

展開している場合 Campaign WebSphere® の場合、次の場所から署名者証明書を取得するように WebSphere® セキュリティ構成を変更する必要があります。 HCL Unica して WebSphere® のトラストストアに追加します。現在の署名者証明書の期限が切れていることを示すエラーメッセージを受け取った場合は、現在の証明書を削除して、新規に追加してください。

WebSphere® ユーザーインターフェースのナビゲーションと操作に関する特定のガイダンスについては、特定の Unica 使用している WebSphere® のバージョン。

1. 信頼できるキーストアを生成します。

詳細は、 [信頼できるキーストアの生成 on page 29](#) を参照してください。

SSL を構成するには、以下の変数に定義した値を指定する必要があります。表示されている値は例です。これとは異なる値を指定することができます。

- 別名: `UnicaClientIdentity` (例)
- キーストア: `HCLUnicaTrust.jks` (例)
- Storepass: `TrustPwd` (例)

2. WebSphere® セキュリティコンソールで新規キーストアを選択します。

例えば、ステップ 1 の例に従った場合、 `HCLUnicaTrust.jks` を選択します。

3. セキュリティ証明書の取得先 HCL Unica 次のステップで説明するように、 WebSphere® にインポートします。

- a. WebSphere® セキュリティー・コンソールで、「 **SSL 証明書と鍵の管理** 」 > 「 **鍵ストアと証明書** 」 > 「 **NodeDefaultTrust Store** 」 > 「 **署名者証明書** 」 にナビゲートします。 **ポートから取得** するオプションを選択します。
- b. 署名者証明書を取得するためのテスト接続を確立するように WebSphere® を構成します HCL Unica 次の値を入力します。 HCL Unica 署名者証明書。
 - **ホスト** 「 `Deliver` 」 > 「 `serverComponentsAndLocations` 」 > 「 `hostedServices` 」 > 「 `uiHostName` 」 に定義されている値
 - **ポート** 443
 - **アウトバウンド接続の SSL 構成** `NodeDefaultSSLSettings`
 - **別名** ホストに入力した値

終了すると、 WebSphere® は HCL Unica に対する署名者証明書の作成に必要な情報を取得するホストされたサービス HCL Unica ホストされているサービス。

4. WebSphere®が署名者証明書の作成を完了したら、セキュリティーコンソールで新規証明書を選択します。

Web アプリケーションサーバーは、接続を確立するときに、新しい証明書を使用します。HCL Unica .

5. WebSphere の®再起動

WebSphere®は、ユーザーが Web アプリケーションサーバーを再起動するまで、設定の変更を実装しません。

Unica 製品をデプロイするためにサポートされるWebSphere®のバージョンの追加情報は、各製品の「推奨されるソフトウェア環境と最小システム要件」の文書を参照してください。

Tomcat または JBOSS での Campaign の配置

Campaign が Tomcat または JBOSS に配置されている場合、Deliver に追加の構成は必要ありません。ホスト・サービス証明書を取得して構成する必要はありません。

Chapter 4. Response and Contact Tracker の操作

Response and Contact Tracker (RCT) がローカル環境にインストールされており、かつHCL Unicaメール連絡先、メール Deliver、受信者の応答 (リンクのクリックやオープンなど) のデータを取得して処理するためのホストサービス。次からリンクトラッキングとメールDeliver通知のデータを取得するために、RCT が実行されている必要があります。HCL Unicaホストサービス。

RCT は、以下のいずれかの方法で開始できます。

- 手動で RCT を開始します。
- サービスとしての RCT を開始します

! **Important:** Deliverを最初に使用するときは、RCT を手動で開始しなければなりません。(RCT をサービスとして登録した場合でも)。

サーバーの構成プロパティ Deliverを変更したときは、RCT を再起動する必要があります。RCT は、サービスとして実行するように構成した場合でも、いつでも再起動できます。HCL Unica RCT がシャットダウンまたは再起動しても、ホストされているサービスはトラッキングデータを保存し続けます。操作を再開すると、RCT はキューに入っている情報をダウンロードします。

Response and Contact Tracker の手動操作

Response and Contact Tracker (RCT) を手動で操作するには、Deliverインストールされます。

- RCTを開始するには、Deliverを以下のようにインストールします。

```
rct start
```

- RCT を停止するには、次のようにrctスクリプトを実行します。

```
rct stop
```

What to do next

このスクリプトの詳細については、[を参照してください。Deliver レスポンスおよびコンタクトのトラッカー \(RCT\) スクリプト on page 62.](#)

Response and Contact Tracker のサービスとしての追加

Response and Contact Tracker (RCT) をサービスとして追加することにより、自動的に開始するように構成できます。

About this task

RCTサービスを登録します。Deliverます。

Response and Contact Tracker (RCT) をサービスとして追加するには、Deliverインストール環境の bin ディレクトリから `MKService_rct -install` スクリプトを実行します。

binディレクトリがサブディレクトリとして作成されます。Campaignインストール・ディレクトリーを最新バージョンにインストールするとき、または最新バージョンにアップグレードするときUnica Campaign。 .

UNIX™またはLinux™ では、ルート権限またはデーモンプロセスを作成する権限を持つユーザーでこのスクリプトを実行します。

Windows™では、サービスの名前は**Response&Contact Tracker**です。

What to do next

MKService_rctスクリプトを実行した後、rctスクリプトを使用して、RCTを手動で開始します。RCTを手動で再起動するのは1回のみです。RCTを最初に手動で起動した後は、RCTをインストールしたコンピューターのオペレーティングシステムを再起動するたびに、RCTは自動的に再起動します。

RCTサービスの構成後、MKService_rctスクリプトを`-remove`オプション付きで実行すると、RCTが自動的に開始しないようになります。

Response and Contact Tracker サービスの削除

Response and Contact Tracker (RCT) をサービスとしてインストールした場合、RCTは、インストールしたシステムを再起動するたびに再起動します。RCTが自動的に再起動しないようにするには、Response and Contact Tracker (RCT) サービスを削除する必要があります。

サービスとしてのRCTを削除するには、MKService_rctスクリプトを`-remove`オプションを指定して実行します。

Windows™のコマンドラインから、次のコマンドを実行します。HCL Unicaホームディレクトリで、`Delivery\bin\MKService_rct.bat -remove`を実行します。

UNIX™またはLinux™の場合、HCL Unicaホームディレクトリ。

What to do next

このスクリプトの詳細については、を参照してください。[MKService_rct スクリプト on page 63](#)

Chapter 5. 起動確認

ホストされているメールのすべての機能にアクセスできることを確認するには、設定と接続をテストしてください。Campaign and Deliver インストール 有効化した後 Deliver、展開します。Deliver インストール、またはアップグレードする Campaign インストール されます。

次のいずれかを実行した後は、設定と接続を確認してください。

- 有効 Deliver 初めて
- 現在の Unica Campaign インストール
- 次へ新規パーティションを Deliver 設定の保守追加します。Unica Platform

システム構成の確認

起動の準備が完了していることを確認するには、次の構成プロパティが設定されていること、および設定が Deliver と Campaign のインストール要件を満たしていることを確認します。

構成プロパティ	設定
<code>Campaign partitions partition[n] Deliver DeliverPluginJarFile</code>	<p>宛先リスト・アップローダー (RLU) として作動するプラグイン・ファイルの場所の絶対パスです。Campaign Web アプリケーション・サーバーをホストするコンピューターのファイル・システムにあるローカル・ディレクトリーの絶対パスを入力します。</p> <p>Unica インストーラーにより、インストーラー実行時にデフォルトのパーティション用のこの設定が自動的に取り込まれます。その他のパーティションの場合、このプロパティは手動で構成します。</p>
<code>Campaign partitions partition[n] server internal deliverInstalled</code>	<p>Deliver がインストールされていることを示します。</p> <p>デフォルト・パーティションを含め、Deliver を有効にする各パーティションで、このプロパティを「はい」に設定します。このプロパティを「はい」に設定すると、Campaign インターフェイスで Deliver 機能が使用可能になります。</p>
<code>Deliver serverComponentsAndLocations hostedServices uiHostName</code>	<p>リストのアップロードを除くすべての通信に対する HCL Unica のアドレス。</p> <p>米国のデータ・センターの場合、デフォルト設定は <code>em.unicadeliver.com</code> です。</p>

構成プロパティ

設定

Deliver | serverComponentsAndLocations |
hostedServices | dataHostName

ヨーロッパのデータ・センターに接続している場合は、この値を `em-eu.unicadeliver.com` に変更します。

インドのデータ・センターに接続している場合は、この値を `em-in.unicadeliver.com` に変更します。

受信者リストに関連するメタデータを HCL Unica にアップロードするために、Deliver が使用する接続のアドレス。

米国のデータ・センターの場合、デフォルト設定は `em.unicadeliver.com` です。

ヨーロッパのデータ・センターに接続している場合は、この値を `em-eu.unicadeliver.com` に変更します。

インドのデータ・センターに接続している場合は、この値を `em-in.unicadeliver.com` に変更します。

Deliver | serverComponentsAndLocations |
hostedServices | ftpHostName

受信者リストのデータ (リストのメタデータを除く) を HCL Unica にアップロードするために、Deliver が使用する接続のアドレス。

ホスト名については、[「接続アドレスの設定HCL Unicaホストサービス ページ 28」](#) のトピックを参照してください。

Deliver | partitions | partition[n] |
hostedAccountInfo | amUserForAcctCredentials

HCL Unica ホスト・サービスのアクセス資格情報を含むデータ・ソースを参照する HCL Unica ユーザー。

この値は、Unica によってホストされている E メール・リソースにアクセスするシステム・ユーザーを作成するときに構成します。

Deliver | partitions | partition[n] |
hostedAccountInfo | amDataSourceForAcctCredentials

HCL Unica ホスト・サービスのログイン資格情報を含む Platform データ・ソース。

この値は、Unica によってホストされている E メール・リソースにアクセスするシステム・ユーザーを作成するときに構成します。

構成プロパティ

設定

Deliver partitions partition [n] < dataSources systemTables type	システム・テーブルをホストするデータベースのタイプ。 データベースの正しい値を指定します。
Deliver partitions partition [n] < dataSources systemTables schemaName	システム・テーブルのデータベース・スキーマの名前。 データベースに適切なスキーマ名を設定します。
Deliver partitions partition [n] < dataSources systemTables jdbcClassName	システム・テーブルの JDBC ドライバー。 環境に適切な値を指定します。
Deliver partitions partition [n] < dataSources systemTables jdbcURI	システム・テーブルの JDBC 接続 URI。 環境に適切な値を指定します。 データベース・タイプ、データベース・ドライバー、ホスト、ポート、およびデータベース名を指定します。例: jdbc:oracle:thin:@yourdb.example.com:1234:DBname JDBC URL の構築方法に関する具体的な指示については、データベースのドキュメントを参照してください。 入力する値は、Campaign Web サーバーで定義されている値と完全に一致する必要があります。
Deliver partitions partition [n] < dataSources systemTables asmUserForDBCredentials	システム・テーブルのログイン資格情報を含むデータ・ソースを参照する HCL Unica ユーザー。 このユーザーは、ローカルの Deliver システム・テーブルへのアクセスを構成するときに作成します。
Deliver partitions partition [n] < dataSources systemTables asmDataSourceForDBCredentials	システム・テーブルを含むデータベースへのログイン資格情報を含む Platform データ・ソース。 このデータ・ソースは、Deliver システム・テーブルにアクセスするユーザーを作成するときに作成します。

HCL Unica ホスト・サービスへのアップロードのテスト

ローカル環境から HCL Unica ホスト・サービスにデータをアップロードできるかどうかをテストするには、チェック・モードで `r1u` スクリプトを実行します。

Deliver インストール済み環境の `bin` ディレクトリーで、以下のいずれかの方法で `r1u` スクリプトを実行します。

- `r1u -c`
- `r1u --check`

HCL Unica ホスト・サービスからのダウンロードのテスト

HCL Unica ホスト・サービスから情報をダウンロードできるかどうかをテストするには、チェック・モードで `rct` スクリプトを実行します。

Deliver インストール済み環境の `bin` ディレクトリーで、以下のように `rct` スクリプトを実行します。

```
rct check
```

ホストされたメッセージング・インターフェースへの接続のテスト

Unica は、米国およびヨーロッパのデータ・センターからのメッセージング・インターフェースをホストします。Deliver 機能にアクセスして、ホストされたメール配信インターフェースへの接続をテストします。

HCL Unica にログインし、**「キャンペーン」**メニューから**「Deliver メール配信」**を選択します。

結果

Deliver ユーザー・インターフェースへの接続が正しく確立されると、「Deliver メール配信」ページが開き、メール配信と関連するメール配信特性のリストが表示されます。

ユーザー・インターフェースへの接続が正しく確立されていない場合は、エラーが表示されます。

第 6 章. Unica Deliver の構成

Unica Platform には、Deliver の動作と外観を変更するためのさまざまな構成プロパティが用意されています。一部の構成プロパティは、インストール時に設定されます。構成プロパティはいつでも変更できます。

Campaign または Deliver の構成を更新した後、レスポンスおよびコンタクトのトラッカー (RCT)、および Campaign をホストする Web アプリケーション・サーバーを再起動する必要があります。

特性または機能

構成プロパティ (パスを含む)

Deliver を Campaign パーティションで有効または無効にします。

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

[Campaign | partitions | partition\[n\] | server | internal](#) ページ 48 を参照してください。

E メール受信者リストの特性です。

Campaign | partitions | partition[n] | Deliver

[Campaign | partitions | partition\[n\] | Deliver](#) ページ 46 を参照してください。

HCL Unica ホスト・サービスへの接続に必要な URL です。

Deliver | serverComponentsAndLocations | hostedServices

[Deliver | serverComponentsAndLocations | hostedServices](#) ページ 52 を参照してください。

HCL Unica ホスト・サービスに接続するためのデータベースおよびアカウント・アクセス資格情報です。

Deliver | partitions | partition[n] | hostedAccountInfo

参照 [Deliver | partitions | partition\[n\] | hostedAccountInfo](#) ページ 53

Deliver システム・テーブルのデータベース・アクセスとスキーマの設定です。

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

参照 [Deliver | partitions | partition\[n\] | dataSources | systemTables](#) ページ 54

特性または機能

構成プロパティ (パスを含む)

受信者リスト・アップローダーのアクションまたは Deliver | partitions | partition[n] | recipientListUploader はステータスに応答して実行されるスクリプトの場所です。(オプション)

参照 [Deliver | partitions | partition\[n\] | recipientListUploader](#) ページ 58

レスポンスおよびコンタクトのトラッカー (RCT) Deliver | partitions | partition[n] | responseContactTracker によって処理される、データ・ダウンロードに関連する設定です。

参照 [Deliver | partitions | partition\[n\] | responseContactTracker](#) ページ 58

Campaign Campaign | partitions | partition[n] | Deliver | oltDimTableSupport のディメンション・テーブルに基づいて、Deliver でパーソナライズされたデータのリストを表示するためのサポートです。

[[ディメンション・テーブルのサポートの構成](#) ページ 44] を参照してください。

メーリング配信実行履歴を追跡するためのサポート Deliver | partitions | partition[n] | responseContactTracker です。参照 [Deliver | partitions | partition\[n\] | responseContactTracker](#) ページ 58 **enableExecutionHistoryDataTracking** パラメーターを参照してください。

構成プロパティの操作については、「[Unica Platform 管理者ガイド](#)」を参照してください。

追加メール実行履歴のアクセス設定を行う

要求できます。Unicaメール送信実行履歴に追加データを提供します。追加メール実行履歴データへのアクセスは、次の場所からの要求により可能です。Unica更新することでDeliver削除します。メール送信実行履歴のデータはローカルに記録されますDeliver^{UACE_ExecHistory}テーブル内のシステムテーブルを使用して、完了したメール送信実行を記述します。

Before you begin

追加のメール実行データをダウンロードするには、構成プロパティ `EnableExecutionHistoryDataTracking` を更新する必要があります。デフォルトでは、`enableExecutionHistoryDataTracking` はDeliver構成プロパティ。

この構成プロパティは、ローカルDeliverインストールは、`Deliver\tools`ディレクトリにある`switch_config_visibility.bat`スクリプトを実行してインストールします。追加メール実行履歴で使用できるレコードは、次のとおりです。

About this task

- メールの件名
- 差出人アドレス
- メーリングを更新したユーザー
- 文書の説明
- メールの保存日

1. 追加メール実行履歴データのアクセスを要求します。アクセス権を要求するには、HCL 技術サポートから Unica Delivery Services チームに連絡してください。
2. 更新:Deliver削除します。以下の構成プロパティを構成します。

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

enableExecutionHistoryDataTrackingをTrueに設定します。

3. UACE_ExecHistory のテーブルマッピングが正しいことを確認してください。

What to do next

照会できます。Deliverシステムテーブルを使用して、`UACE_ExecHistory`テーブルからメーリング実行情報を取得します。

Deliverに関する詳細は、システムテーブルについては、*Unia* が提供するシステムテーブルとデータディクショナリを参照してください。

Campaign プランの統合のサポート

Unica Deliverプランの追加をサポートしていますCampaign作成者用メールへDeliver.

オファーは、次で設定されたオファーテンプレートに基づいています。Unica Campaign 統合をサポートするにはCampaignカスタマイズされたメールへの提案を行うには、Campaignを指定し、他の設定を完了しますCampaign.

オファーの統合のサポートを構成する方法について詳しくは、次のトピックを参照してください。Deliver Unica Campaign 管理者ガイドの提供の統合について。

次元テーブルのサポートの構成

メール用拡張スクリプトによって提供される特定の機能をサポートするには、`oltDimTablesupport`構成プロパティをTrueに設定する必要があります。

About this task

Deliverでは、個人情報のリストを表示するメールメッセージを作成するための拡張スクリプトが提供されています。これらのリストを関連付ける必要があります: Campaignと、メールの受信者リストを定義する出力リストテーブル (OLT) を使用します。出力一覧テーブルはDeliverスキーマを参照してください。

`oltDimTablesupport` 構成プロパティは、Deliverスキーマを参照してください。このプロパティの値が`True`に設定されている場合、OLT はディメンションテーブルで提供される情報を使用できます。

`oltDimTablesupport` プロパティを更新するには、以下のステップを実行してください。

マーケターが拡張スクリプトを使用してデータテーブルを作成する方法の詳細については、次を参照してください。*Unica Deliver* ユーザーズ・ガイド。

1. 「設定」 > 「構成」 > 「キャンペーン」 > 「パーティション」 > 「パーティション[n]」 > 「配信」に移動してください。
2. 「設定の編集」をクリックし、`oltDimTablesupport` プロパティの値を`True`に設定します。

ローカル Deliver システム・テーブルへのアクセスの構成

Deliver コンポーネントは、Campaign スキーマの Deliver システム・テーブルにアクセスする必要があります。システム・テーブルに自動的にアクセスできるシステム・ユーザーを作成して構成する必要があります。Campaign のインストール時に構成されたシステム・ユーザーは、Campaign スキーマへの必要なアクセス権をすでに持っています。

このタスクについて



注: インストール済み環境に複数のパーティションが含まれている場合は、パーティションごとにこのタスクを実行する必要があります。パーティション間でシステム・ユーザーを共有することはできません。

別のシステム・ユーザーを使用して Deliver システム・テーブルにアクセスする場合は、Platform で新しいシステム・ユーザーを作成し、Campaign スキーマにアクセスできる新しいプラットフォーム・データ・ソースを作成する必要があります。

1. Deliver 構成で、Campaign スキーマをホストするデータベースにアクセスするシステム・ユーザーを指定します。

新しいユーザーを作成したり、既存のユーザーを指定したりできます。Campaign 用に設定したシステム・ユーザーは、すでに Campaign スキーマにアクセスできます。

構成プロパティ `Deliver > partitions > partition [n] < dataSources > systemTables > asmUserForDBCredentials` を使用します。

デフォルトでは、指定されたユーザーは `asm_admin` です。

2. Deliver 構成で、Campaign スキーマをホストするデータベースにアクセスするために必要なユーザー名とパスワードを含むように構成されているデータ・ソースを指定します。

Campaign のインストール時に、作成されたデータ・ソースを使用して Campaign スキーマにアクセスできます。

構成プロパティ `Deliver > partitions > partition [n] < dataSources > systemTables > amDataSourceForDBCredentials` を使用します。

Unica Delivery 設定プロパティ

プラットフォームの「設定」メニューから「配信設定」プロパティにアクセスします。配信を設定するためのプロパティは、[Campaign] と [Delivery] 設定カテゴリに含まれています。

設定プロパティにアクセスするには、**[設定] > [構成]**に移動します。設定ページには、Unica インストールで使用可能なすべての設定プロパティがリストされます。

Campaign | partitions | partition[n] | Deliver

このカテゴリのプロパティを定義することで、宛先リストの特性を定義し、HCL Unica にリストをアップロードするリソースの場所を指定します。

DeliverPluginJarFile

説明

宛先リスト・アップローダー (RLU) として作動するファイルの場所の絶対パスです。Campaign に対するこのプラグインによって、Unica がホストするリモート・サービスに OLT データと関連メタデータがアップロードされます。指定する場所は、Campaign Web アプリケーション・サーバーをホストするコンピューターのファイル・システムにあるローカル・ディレクトリーの絶対パスでなければなりません。

Unica インストーラーにより、インストーラー実行時にデフォルトのパーティション用のこの設定が自動的に取り込まれます。その他のパーティションの場合、このプロパティは手動で構成しなければなりません。Deliver のインストール済み環境ごとに RLU は 1 つしか存在しないので、すべてのパーティションに関して RLU に同じ場所を指定する必要があります。

Unica で指示されない限り、この設定は変更しないでください。

デフォルト値

デフォルト値が定義されていません。

有効な値

Campaign Web サーバーをインストールした場所のローカル・ディレクトリーの絶対パスです。

defaultSeedInterval

説明

`defaultSeedType` が `Distribute list` の場合におけるシード・メッセージ間のメッセージ数。

デフォルト値

1000

defaultSeedType**説明**

Deliver がシード・アドレスを受信者リストに挿入するために使用するデフォルトの方法です。

デフォルト値

Distribute IDS

有効な値

- `Distribute IDS` - 宛先リストのサイズと有効なシード・アドレスの数に基づいて ID を均等に配布し、シード・アドレスを宛先リスト全体で均等な間隔に挿入します。
- `Distribute list` - メイン・リストの `defaultSeedInterval ID` すべてにシード・アドレスを挿入します。宛先リストに指定の間隔で、有効なシード・アドレスのリスト全体を挿入します。挿入点の間隔を指定する必要があります。

oltTableNamePrefix**説明**

出力リスト表の生成済みスキーマで使われます。このパラメーターを定義する必要があります。

デフォルト値

OLT

有効な値

接頭部を含めることができるのは 8 文字までの英数字または下線文字で、先頭は文字でなければなりません。

oltDimTableSupport**説明**

この構成パラメーターによって制御される機能は、Deliver スキーマで作成された出力リスト表 (OLT) にディメンション表を追加する機能です。ディメンション表は、Eメールの Eメール・メッセージにデータ表を作成する拡張スクリプトを使用するのに必要となります。

マーケティング担当者が Deliver プロセスを使用して受信者リストを定義する際にディメンション表を作成できるように、このプロパティを `True` に設定する必要があります (デフォルトで `True` です)。データ・テーブルの作成と、Eメールの拡張スクリプトの処理に関して詳しくは、「Unica Deliver ユーザー・ガイド」を参照してください。

OLT で出力するためにディメンション・テーブル・フィールドを使用しており、通信でこれらのディメンション・フィールドをパーソナライズ・フィールドとして使用する場合は、このプロパティを `False` に設定する必要があります。

デフォルト値

`True`

有効な値

True | False

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

このカテゴリのプロパティは、選択された Campaign パーティションの統合設定と internalID の制限を指定します。Campaign のインストール済み環境に複数のパーティションがある場合は、反映させるパーティションごとにこれらのプロパティを設定します。

internalIdLowerLimit

構成カテゴリ

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

説明

`internalIdUpperLimit` プロパティと `internalIdLowerLimit` プロパティは、Campaign 内部 ID を指定の範囲に制限します。指定された値も範囲に含まれます。すなわち、Campaign は、上限値と下限値の両方を使用できます。

デフォルト値

0 (ゼロ)

internalIdUpperLimit

構成カテゴリ

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

説明

`internalIdUpperLimit` プロパティと `internalIdLowerLimit` プロパティは、Campaign 内部 ID を指定の範囲に制限します。指定された値も範囲に含まれます。すなわち、Campaign は、上限値と下限値の両方を使用できます。Unica Collaborate がインストールされている場合は、この値を `2147483647` に設定してください。

デフォルト値

4294967295

deliverInstalled

構成カテゴリ

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

説明

Deliver がインストールされていることを示します。「はい」を選択すると、Deliver 機能が Campaign インターフェースで使用できます。

Unica インストーラーは、Deliver インストール済み環境のデフォルトのパーティションに関してこのプロパティを「はい」に設定します。Deliver をインストールした追加パーティションについては、このプロパティを手動で構成する必要があります。

デフォルト値

いいえ

有効な値

はい | いいえ

Legacy_campaigns

構成カテゴリ

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

説明

このパーティションで、Unica Plan と Campaign が統合される前に作成されたキャンペーンへのアクセスを有効にします。**MO_UC_integration** が「はい」に設定されている場合のみ、適用されます。レガシー・キャンペーンには、Campaign 7.x で作成され、Plan 7.x プロジェクトにリンクされたキャンペーンも含まれます。詳しくは、「*Unica Unica Plan* および *Campaign* 統合ガイド」を参照してください。

デフォルト値

いいえ

有効な値

はい | いいえ

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

このカテゴリのプロパティを使用して、現行パーティションに対して Unica Campaign との Deliver オフライン統合を構成します。

etlEnabled

説明

Campaign は独自の ETL プロセスを使用して、Deliver トラッキング・テーブルから Campaign コンタクト履歴テーブルおよびレスポンス履歴テーブルへのオファー・レスポンス・データの抽出、変換、ロードを行います。

ETL プロセスは必要なテーブル全体にわたって情報を調整します。これには、`UA_UsrResponseType` (Campaign レスポンス・タイプ) および `UA_RespTypeMapping` (Campaign と Deliver の間のレスポンス・タイプのマッピング) が含まれます。

値を「はい」に設定することで、Deliver オffer・コンタクトおよびレスポンス履歴に関する情報が Campaign と Deliver の間で確実に調整されます。例えば、E メール・レスポンス・データは Campaign レポートに組み込まれます。



注: このパーティションの `Campaign | partitions | partition[n] | server | internal | DeliverInstalled` を「はい」に設定する必要もあります。そうしないと ETL プロセスが動作しません。



ヒント: ETL の進行状況を監視する場合、`Campaign | monitoring | monitorEnabledForDeliver` を有効にします。

デフォルト値

いいえ

有効な値

はい | いいえ

runOnceADay

説明

ETL プロセスを 1 日に 1 回のみ実行するかどうかを示します。

値が `Yes` の場合: `startTime` を指定する必要があります。これにより、すべてのレコードが処理されるまで ETL ジョブが実行されます。そして `sleepIntervallnMinutes` は無視されます。

値が `No` の場合: Campaign Web サーバーが始動するとすぐに ETL ジョブが開始されます。すべてのレコードの処理が完了した後、ETL ジョブは停止し、`sleepIntervallnMinutes` で指定した時間待機します。

デフォルト値

いいえ

有効な値

はい | いいえ

batchSize

説明

ETL プロセスはこのパラメーターを使用して、RCT からローカル Deliver システム・テーブルにダウンロードされたレコードを取り出します。値が大きいとパフォーマンスに影響を与える可能性があるため、使用可能な値のリストは、以下に示す有効な値に制限されています。大量のレコードを事前に予期している場合、**sleepIntervallnMinutes** とともに **batchSize** を調整して、定期的な間隔でレコードを処理するようにしてください。

デフォルト値

100

有効な値

100 | 200 | 500 | 1000

sleepIntervallnMinutes

説明

ETL ジョブ間の間隔を分単位で指定します。このオプションにより、ジョブ完了後の待機時間が決まります。ETL プロセスは、次のジョブを開始する前に、この時間待機します。複数のジョブを同期的に実行することができ、1つのパーティションに複数の ETL ジョブを置くこともできます。

runOnceADay が **Yes** の場合、スリープ間隔を設定できません。

デフォルト値

60

有効な値

正整数

startTime

説明

ETL ジョブを開始する時刻を指定します。開始時刻の指定には、英語ロケールの形式を使用する必要があります。

デフォルト値

00:00

有効な値

hh:mm:ss AM/PM という形式の、任意の有効な時刻

notificationScript

説明

ETL ジョブが実行された後に毎回実行される、オプションの実行可能ファイルまたはスクリプト・ファイル。例えば、モニター目的で、ETL ジョブが実行されるたびに、その成功または失敗が通知されるようにすることもできます。特定のパーティションの ETL ジョブが実行を完了するたびに、通知スクリプトが実行されます。

このスクリプトに渡されるパラメーターは固定されており、変更できません。スクリプトでは、以下のパラメーターを使用できます。

- etlStart: ETL の開始時刻 (ミリ秒単位)。
- etlEnd: ETL の終了時刻 (ミリ秒単位)。
- totalCHRecords: 処理されたコンタクト・レコードの総数。
- totalRHRecords: 処理されたレスポンス履歴レコードの総数。
- executionStatus: ETL の実行状況。値は 1 (失敗) または 0 (成功) のいずれか。

デフォルト値

デフォルト値が定義されていません。

有効な値

Campaign サーバーが読み取り権限または実行権限でアクセスできる任意の有効なパス。以下に例を示します。D:\myscripts\scriptname.exe

Deliver | serverComponentsAndLocations | hostedServices

HCL Unica ホスト・サービスに接続するための URL を指定するプロパティを定義します。Deliver では、受信者リストおよび受信者リストを記述したメタデータのアップロードと、ホストされた環境へ送信する一般的な通信に別々の接続が使用されます。

Unica がヨーロッパに設立したデータ・センターを通じて HCL Unica ホスト・サービスに接続する場合は、デフォルト値を変更する必要があります。接続先のデータ・センターを判別するには、Unica にお問い合わせください。

uiHostName

説明

受信者リストとそれに関連するメタデータのアップロードを除いて、Deliver が HCL Unica ホスト・サービスへのすべての通信に使用するアドレス。

デフォルト値

em.unicadeliver.com

ヨーロッパのデータ・センターに接続している場合は、この値を em-eu.unicadeliver.com に変更します。

インドのデータ・センターに接続している場合は、この値を em-in.unicadeliver.com に変更します。

dataHostName

説明

受信者リストに関連するメタデータを HCL Unica ホスト・サービスにアップロードするために、Deliver が使用するアドレス。

デフォルト値

```
em.unicadeliver.com
```

ヨーロッパのデータ・センターに接続している場合は、この値を `em-eu.unicadeliver.com` に変更します。

ftpHostName

説明

受信者リストのデータ (リストのメタデータを除く) を HCL Unica ホスト・サービスにアップロードするために、Deliver が使用するアドレス。

デフォルト値

```
ftp-em.unicadeliver.com
```

ヨーロッパのデータ・センターに接続している場合は、この値を `ftp-eu.unicadeliver.com` に変更します。

インドのデータ・センターに接続している場合は、この値を `ftp-in.unicadeliver.com` に変更します。

Deliver | partitions | partition[n] | hostedAccountInfo

このカテゴリのプロパティを定義することによって、HCL Unica ホスト・サービスへのアクセスに必要なアカウント情報を格納するデータベース用のユーザー資格情報を定義します。ここで指定する値は、Platform 内でユーザー設定として定義されている必要があります。

amUserForAcctCredentials

説明

このプロパティを使用して、HCL Unica ホスト・サービスへのアクセスに必要なアカウント・アクセス資格情報を指定する Platform データ・ソースを含んでいる Platform ユーザーを指定します。

デフォルト値

```
asm_admin
```

有効な値

任意の Platform ユーザー。

amDataSourceForAcctCredentials

説明

このプロパティを使用して、HCL Unica ホスト・サービスのログイン資格情報を定義している Platform データ・ソースを指定します。

デフォルト値

UNICA_HOSTED_SERVICES

有効な値

`amUserForAcctCredentials` の中で指定するユーザーに関連付けられているデータ・ソース。

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

このカテゴリには、ネットワーク環境内の Deliver システム・テーブルを含んでいるデータベースについて、そのスキーマ、接続設定、およびログイン資格情報を定義する構成プロパティが含まれています。

type

説明

Deliver システム・テーブルをホストするデータベースのタイプ。

デフォルト値

デフォルト値が定義されていません。このプロパティを定義することは必須です。

有効な値

- SQLSERVER
- ORACLE
- :NONE.

schemaName

説明

Deliver システム・テーブルのデータベース・スキーマの名前。これは、Campaign システム・テーブルのスキーマ名と同じです。

スクリプト内でシステム・テーブルを参照するときは、このスキーマ名を含める必要があります。

デフォルト値

dbo

jdbcBatchSize

説明

JDBC がデータベース上で一度に実行する実行要求の数。

デフォルト値

10

有効な値

0 より大きい整数。

jdbcClassName

説明

Campaign Web サーバーで定義されている、システム・テーブルの JDBC ドライバー。

デフォルト値

デフォルト値が定義されていません。このプロパティを定義することは必須です。

jdbcURI

説明

Campaign Web サーバーで定義されている、システム・テーブルの JDBC 接続 URI。

デフォルト値

デフォルト値が定義されていません。このプロパティを定義することは必須です。

asmUserForDBCredentials

説明

このプロパティを使用して、Deliver システム・テーブルへのアクセスを許可される HCL Unica ユーザーを指定します。

デフォルト値

デフォルト値が定義されていません。このプロパティを定義することは必須です。

有効な値

Platform で定義されている任意のユーザー。一般に、これは Campaign のシステム・ユーザーの名前にします。

amDataSourceForDBCredentials

説明

このプロパティを使用して、Deliver システム・テーブルを含んでいるデータベースのログイン資格情報を定義しているデータ・ソースを指定します。これは、Campaign システム・テーブルのデータ・ソースと同じものにすることができます。

デフォルト値

UA_SYSTEM_TABLES

有効な値

`asmUserForDBCredentials` で指定する HCL Unica ユーザーに関連付けられている Platform データ・ソース

このデータ・ソースは、Deliver システム・テーブルへのアクセスに使用されるデータベース・ユーザーおよび資格情報を指定します。データベース・ユーザーのデフォルト・スキーマが、システム・テーブルを含んでいるスキーマでない場合は、システム・テーブルへのアクセスに使用する JDBC 接続の中で、システム・テーブル・スキーマを指定する必要があります。

poolAcquireIncrement

説明

データベース接続プールの接続を使い尽くしたときに、Deliver がシステム・テーブル用に作成する新規接続の数。Deliver は、`poolMaxSize` で指定された数を最大値として、新規接続を作成します。

デフォルト値

1

有効な値

0 より大きい整数。

poolIdleTestPeriod

説明

Deliver で、Deliver システム・テーブルへのアイドル接続のアクティビティの有無をテストする間の待ち時間 (秒数)。

デフォルト値

100

有効な値

0 より大きい整数。

poolMaxSize

説明

Deliver がシステム・テーブルに対して作成する接続の最大数。値がゼロ (0) の場合、最大値はないということになります。

デフォルト値

100

有効な値

0 以上の整数。

poolMinSize

説明

Deliver がシステム・テーブルに対して作成する接続の最小数。

デフォルト値

10

有効な値

0 以上の整数。

poolMaxStatements

説明

Deliver で PreparedStatement キャッシュに保管される、システム・テーブルへの接続 1 つあたりの最大ステートメント数。poolMaxStatements をゼロ (0) に設定すると、ステートメント・キャッシュは無効になります。

デフォルト値

0

有効な値

0 以上の整数。

timeout

説明

Deliver で、アイドル状態のデータベース接続が除去されるまでに維持される秒数。

poolIdleTestPeriod が 0 より大きい場合、Deliver はプール内にあるチェックアウトされていないすべてのアイドル接続を、timeout 秒ごとにテストします。

`poolIdleTestPeriod` が `timeout` より大きい場合、アイドル接続は除去されます。

デフォルト値

100

有効な値

0以上の整数。

Deliver | partitions | partition[n] | recipientListUploader

この構成カテゴリーには、受信者リスト・アップローダーのアクションまたはステータスに対する応答として実行されるユーザー定義スクリプトの場所に関するオプション・プロパティーが含まれています。

pathToTriggerScript

説明

HCL Unica ホスト・サービスへの受信者リストのアップロードに対して、アクションをトリガーするスクリプトを作成できます。例えば、リストのアップロードが正常に完了したときにリスト・デザイナーに E メール・アラートを送信するスクリプトを作成できます。

このプロパティーの値を定義した場合、Deliver は受信者リスト・アップローダーに関するステータス情報を、指定された場所に渡します。このプロパティーを空白のままにした場合、Deliver は何もアクションを実行しません。

デフォルト値

デフォルト値が定義されていません。

有効な値

有効な任意のネットワーク・パス。

Deliver | partitions | partition[n] | responseContactTracker

このカテゴリーのプロパティーは、Response and Contact Tracker (RCT) の動作を指定します。RCT は、E メール・コンタクト、E メール配信、および受信者のレスポンス (例えば、リンクのクリックとオープンなど) に関するデータを取り出し、処理します。

pauseCustomerPremisesTracking

説明

Deliver は、コンタクトとレスポンスのデータを HCL Unica ホスト・サービス内のキューに保管します。このプロパティーを使用すると、RCT に HCL Unica ホスト・サービスからのデータの取得を一時的に停止するよう指示できます。トラッキングを再開すると、蓄積されたデータが RCT によりダウンロードされます。

デフォルト値

偽

有効な値

True | False

waitTimeToCheckForDataAvailability**説明**

RCT は、E メール・コンタクトまたは受信者レスポンスに関して、新規データの有無を定期的に検査します。このプロパティを使用すると、RCT が HCL Unica ホスト・サービス内の新規データの有無を検査する頻度を秒単位で指定できます。デフォルト値は 300 秒、つまり 5 分ごとです。

デフォルト値

300

有効な値

1 より大きい整数。

perfLogInterval**説明**

このプロパティを使用すると、パフォーマンス統計を RCT によってログ・ファイルに記録する頻度を指定できます。入力した値によって、ログ項目間のバッチの数が決まります。

デフォルト値

10

有効な値

0 より大きい整数。

enableSeparatePartialResponseDataTracking**説明**

このプロパティは、Deliver で、部分的な E メール・レスポンス・データをローカル Deliver インストール済み環境内のトラッキング・テーブルに転送するかどうかを決定します。

Deliver で E メール・レスポンスを正しく属性付けするには、メール配信インスタンス ID とメッセージ・シーケンス番号が必要です。enableSeparatePartialResponseDataTracking を True に設定すると、Deliver は不完全なレスポンスを別個のローカル・トラッキング・テーブルに入れます。このテーブルで、それらのレスポンスを確認するか追加の処理を行うことができます。

デフォルト値

真

有効な値

True | False

enableExecutionHistoryDataTracking

説明

このプロパティは、追加のメール配信の実行の履歴データを HCL Unica からダウンロードできるかどうかを制御します。

デフォルトで、このプロパティは追加データのダウンロードを許可しない **False** に設定されています。このプロパティを **True** に設定すると、通常は Deliver システム・テーブルに入力されないメール配信の実行に関するデータをダウンロードできるようになります。この補足情報は、メール配信やデータベース管理を自動化するために使用できます。

このプロパティは、デフォルトでは非表示になっています。この構成プロパティは、`Deliver\tools` ディレクトリーにある `switch_config_visibility.bat` スクリプトを実行することで、ローカルの Deliver インストール済み環境で表示できます。

メール配信実行の履歴データに対するアクセスは、Unica から要求することによって可能となります。追加のメール配信実行の履歴データへのアクセスを要求するには、HCL 技術サポートから Unica Deliver Services チームにお問い合わせください。

デフォルト値

偽

有効な値

True | False

Chapter 7. ユーティリティ Deliver

Deliverには、管理するために使用するいくつかのスク립トが用意されています。Deliver関数を指定します。

このセクションで説明するソフトウェアユーティリティは、さまざまな起動と管理機能に使用できます。これらのアプリケーションで使用されるソフトウェアユーティリティに加えて、Unica Platform、Unica Deliverユーティリティは固有です。Deliver管理目的にのみ使用しますDeliver削除できます。

次で使用可能なその他のユーティリティの詳細については、HCL Unicaインストールについては、「*Unica Platform*管理者ガイド」。

RLU スクリプト

RLU スクリプトを使用して、受信者リスト・アップローダー (RLU) のステータスを確認します。



注: このスクリプトを使用して RLU を開始または停止することはできません。このスクリプトは、オンプレミスのコンポーネントとオンデマンドのコンポーネント間の接続を確認するために使用してください。

RLU スクリプトは <Deliver Install Home>/bin フォルダにあります。Deliver ディレクトリーは、Campaign ディレクトリー内にあるサブディレクトリーです。

UNIX™ または Linux™ 環境では、このスクリプトを `rlu.sh` として実行します。

Windows™ では、このスクリプトをコマンド・プロンプトから `rlu.bat` として実行します。

Syntax

```
rlu -c | --check [-h]
```

コマンド

-c、--check

RLU が正しく構成されていること、および RLU が HCL Unica に接続されていることを確認します。

オプション

-h、--help

スクリプトの構文を表示します

例

Linux™ 環境で、RLU が HCL Unica ホスト・サービスに接続されているかどうかを判別します。

```
rlu.sh --check
```

システムの状況に応じて、このコマンドの出力は以下のサンプルのような内容になる場合があります。

```
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 レスpons およびコンタクトのトラッカー (RCT) スクリプト

レスpons およびコンタクトのトラッカー (RCT) を実行し、その状況を確認するには、このスクリプトを使用します。

このスクリプトは、Deliver インストール済み環境の `bin` ディレクトリーにあります。Deliver ディレクトリーは、Campaign ディレクトリー内にあるサブディレクトリーです。

UNIX™ または Linux™ 環境では、このスクリプトを `rct.sh` として実行します。

Windows™ では、このスクリプトをコマンド・ラインから `rct.bat` として実行します。

Syntax

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

コマンド

開始

RCT を始動します。

停止

RCT を停止します。

オプション

check

RCT と HCL Unica ホスト・サービスとの接続状況を確認します。

例(X)

- Windows™ で RCT を始動するには、以下を実行します。

```
rct.bat start
```

- Windows™ で RCT を停止するには、以下を実行します。

```
rct.bat stop
```

- Linux™ 環境では、RCT が HCL Unica ホスト・サービスに接続されているかどうかを判別するには、以下を実行します。

```
rct.sh check
```

システムの状況に応じて、このコマンドの出力は以下のような内容になります。

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

MKService_rct スクリプト

MKService_rct スクリプトは、レスポンスおよびコンタクトのトラッカー (RCT) をサービスとして追加または削除します。RCT をサービスとして追加すると、RCT をインストールしたコンピューターが再始動するたびに、RCT が再始動します。サービスとしての RCT を削除すると、RCT は自動的に再始動されなくなります。

このスクリプトは、Deliver インストール済み環境の bin ディレクトリーにあります。

UNIX™ または Linux™ 環境では、root 権限またはデーモン・プロセスを作成する権限を持つユーザーとして MKService_rct.sh. を実行します。

Windows™ では、このスクリプトをコマンド・ラインから MKService_rct.bat として実行します。

Syntax

```
MKService_rct -install
```

```
MKService_rct -remove
```

コマンド

-install

RCT をサービスとして追加します。

-remove

RCT サービスを削除します。

例(X)

- RCT を Windows™ サービスとして追加するには、以下を実行します。

```
MKService_rct.bat -install
```

- UNIX™ または Linux™ で RCT サービスを削除するには、以下を実行します。

```
MKService_rct.sh -remove
```

configTool

【構成】 ページのプロパティと値は、Platform システム・テーブルに保管されます。configTool ユーティリティーを使用して、構成設定をシステム・テーブルにインポートしたり、システム・テーブルからエクスポートしたりできます。詳しくは、「Platform 管理者ガイド」を参照してください。

Chapter 8. トラブルシューティングについてDeliver

Unica Deliverには、ユーザーに関連した問題の調査に使用できるさまざまなツールと手法が用意されています。Campaign and Deliver削除できます。

Deliverログファイル

HCL Unicaでは、タスクの監視に使用できるいくつかのログファイルを提供します。Deliverインストールし、問題を調査します。

Deliverログファイル

このログには、次の場所からダウンロードされた情報に関して、次のタイプの情報が含まれます。HCL Unicaホストされているサービス。ディレクトリのlogsディレクトリにあります。Deliverインストールされます。

- 一般メーリング情報
- メールインスタンス ID
- リンククリックデータ
- 返送メールのデータ

Deliver一時ファイル

このディレクトリには、アップロードされるデータが含まれます。

次のtempディレクトリにあります。Deliverインストールされます。

Campaign ログ・ファイル

メール送信関連の情報を含むログファイルは、次の場所で確認できます。Campaign .

- Campaign\partitions\

フローチャートに含まれるDeliverプロセスからのログエントリを含む、フローチャートの実行に関連するさまざまなログファイル。

- Campaign\logs

このディレクトリには、受信者リストアップローダによるアップロード情報に関する情報が含まれるキャンペーンweb.logが含まれます。

Deliver での log4j の使用

Deliverは、Apache log4j ユーティリティを使用して、Response and Contact Tracker (RCT) と受信者リストアップローダ (RLU) の設定、デバッグ、エラー情報のログを記録します。

システムログ設定の変更については、以下を参照してください。

- log4j.xml ファイルのコメント。
- ApacheWeb サイト <https://logging.apache.org/log4j/2.x/manual/index.html>

受信者リストアップローダでの log4j の使用

コマンド行から受信者リストアップローダ (RLU) ユーティリティを実行すると、デフォルトのロガー設定が使用されます。

これらの設定を変更するには、`deliver_rlu_log4j.xml` ファイルを変更します。

ファイルのコメントの指示に従って、`deliver_rlu_log4j.xml` を変更します。HCL サポートからの提案がない限り、このファイルを変更しないでください。

RLU がフローチャートによって自動的に呼び出されるとき、RLU は CampaignWeb アプリケーションのロギング。これは、Campaign インストールディレクトリ。

Response and Contact Tracker での log4j の使用

Response and Contact Tracker (RCT) ユーティリティを実行すると、デフォルトのロガー設定が使用されます。

これらの設定を変更するには、`deliver_rct_log4j.xml` ファイルを変更します。

ファイルのコメントの指示に従って、`deliver_rct_log4j.xml` を変更します。

Chapter 9. メッセージ機能へのユーザーアクセスの管理

Campaign and Deliverによって提供されるロールと許可を使用します。Unica Platformメッセージ機能へのユーザーアクセスの制御はDeliver and Campaign . 次の権限が必要ですUnica Platform and Campaign をクリックして必要な変更を行います。また、Platformでのロールと権限の構成方法、およびCampaignセキュリティ ポリシーの定義方法についても理解しておく必要があります。

メールマーケティングキャンペーンを実施するために、メールマーケティング担当者は、次のようにアクセスします。 Deliver メール送信機能 Unica Campaign .

カスタマイズされた通信とホストされているランディングページを作成するために、マーケターはDeliver文書コンポーザー。

ロール、許可、ポリシーの設定方法に関する一般的な情報は、次のセクションを参照してください。 *Unica* でのセキュリティの管理方法を説明したPlatform「管理者ガイド」 。 Unica Platform およびUnica Campaign .

メール送信アクセスのためのロールとポリシーの割り当て

にログインするにはHCL Unicaシステムのユーザー名とパスワードを入力する際に、マーケティング担当者がメールを送信します。システムユーザーに許可されている許可によって、マーケターが次の場所のメール機能、個別に設定された通信、コンテンツにアクセスする方法が決定します。 Deliver and Campaign .

許可は、ロールに関連付けられます。 Unica Platform . のメール送信機能へのアクセスを制御するにはCampaignを使用すると、1つ以上のセキュリティポリシー内でロールを定義できます。メール機能、通信、コンテンツにアクセスするすべてのシステムユーザーには、Deliver内のロールCampaignセキュリティポリシーを参照してください。ポリシーを通じて、メール送信機能の許可を選択的に適用しますCampaign また、Deliver文書コンポーザー。

メール送信機能にアクセスするユーザーには、Deliverユーザーロールと管理者ロール。これらのロールは、Deliver使用可能なロールCampaignセキュリティポリシー。

Platform および Campaign での役割と権限

Platform および Campaign での役割は、構成可能な権限の集合です。Platform および Campaign での役割ごとに、アプリケーションへのアクセスを制御する権限を指定できます。

デフォルトの役割を使用するか、新しい役割を作成することができます。使用可能な権限のセットは、システムによって定義されており、新しい権限を作成することはできません。

役割割り当てについて

一般に、ユーザーに与える役割は、そのユーザーが HCL Unica を使用するとき組織内で実行する機能を反映した権限を持つ役割にしてください。役割は、グループに割り当てるか、個々のユーザーに割り当てることができます。グループによって役割を割り当てる利点は、役割の組み合わせをグループに割り当てることができ、後でその組み合わせを変更する場合は、複数のユーザーについて何度も変更を行う必要がなく、1 個所で変更できることです。グループによって役割を割り当てる場合は、グループにユーザーを追加または削除することによって、ユーザー・アクセスを制御します。

システムが役割を評価する方法

ユーザーが複数の役割を持つ場合、システムはそれらすべての役割をまとめたものから、権限を評価します。特定のオブジェクトに対して機能を実行する資格能力は、すべての役割から集約された権限に基づいて認可あるいは否定されます。Campaign の場合、特定のオブジェクトに対して機能を実行する資格能力は、そのオブジェクトのセキュリティー・ポリシーに基づいて認可あるいは拒否されます。

セキュリティー・ポリシーの仕組み

セキュリティー・ポリシーは、Campaign でフォルダーとオブジェクトのセキュリティーを管理する「ルール・ブック」です。ユーザーがアプリケーションで操作を実行するたびに参照されます。

独自のセキュリティー・ポリシーを作成したり、Campaign に含まれるデフォルトのグローバル・セキュリティー・ポリシーを使用したりできます。

Campaign では、セキュリティー・ポリシーはフォルダーに割り当てられます。さらに、最上位フォルダーを作成するとき、セキュリティー・ポリシーをフォルダーに適用するよう求められます。そのフォルダー内のオブジェクトやサブフォルダーは、フォルダーのセキュリティー・ポリシーを継承します。

最上位フォルダーがフォルダー内のオブジェクトのセキュリティー・ポリシーを決定するため、セキュリティー・ポリシーをオブジェクトに直接割り当てることはできません。オブジェクトのセキュリティー・ポリシーを変更するには、適切なセキュリティー・ポリシーを持つフォルダーの中、または最上位ルート・フォルダーにオブジェクトを移動する必要があります。

セキュリティー・ポリシーをユーザーに直接割り当てることもできません。セキュリティー・ポリシーに全体として割り当てられるオブジェクトやフォルダーとは異なり、ユーザーはセキュリティー・ポリシー内の役割に割り当てられます。ユーザーが実行できることを制御するために、ユーザーをセキュリティー・ポリシー内の役割に割り当てます。この方法で、これらのセキュリティー・ポリシーを使用するフォルダー内のオブジェクトへのユーザー・アクセスを制御します。

ユーザーがセキュリティー・ポリシーのどの役割にも明示的に割り当てられていない場合、そのユーザーはそのポリシーを使用する最上位フォルダーの下にフォルダーとオブジェクトを作成できません。また、そのユーザーは、そのフォルダーまたはサブフォルダー下のオブジェクトにアクセスできません。

次の図は、セキュリティー・ポリシー、フォルダー、オブジェクト、役割、およびユーザーの間の関係を示しています。

最上位の管理役割

Unica Campaign での管理役割はパーティションごとに割り当てられます。これらの役割を持つユーザーは、パーティション内の任意のオブジェクトに対して、そのオブジェクトを含むフォルダー内で使用されるセキュリティー・ポリシーに関係なく、許可された操作を実行できます。

セキュリティー・ポリシーとパーティション

セキュリティー・ポリシーは、パーティションごとに作成されます。複数のパーティション間でセキュリティー・ポリシーが共有されることはありません。

Unica Campaign の各パーティションで複数のセキュリティ・ポリシーを設定できます。

セキュリティ・ポリシーは、フォルダーおよびオブジェクトを移動またはコピーすると変更されます。

複数のセキュリティ・ポリシー間でオブジェクトとフォルダーを移動またはコピーできますが、移動/コピーを実行するユーザーは、ソースと宛先の両方のポリシーでその操作を行う権限を持っている必要があります。

元のフォルダーとは異なるセキュリティ・ポリシーに割り当てられたフォルダーにオブジェクトやフォルダーが移動/コピーされると、下位のオブジェクトやサブフォルダーのセキュリティ・ポリシーは新しいフォルダーのセキュリティ・ポリシーに自動的に変更されます。

グローバル・セキュリティ・ポリシー

Campaign には、デフォルトのグローバル・セキュリティ・ポリシーが含まれています。このポリシーは削除できず、常に適用されます。ただし、セキュリティ・スキームは次のようにカスタマイズできます。

- グローバル・ポリシーの役割と権限を、組織のニーズを満たすよう変更します。
- カスタム・ポリシーを作成し、グローバル・ポリシーではなくカスタム・ポリシーにのみユーザーを割り当てます。
- カスタムポリシーとグローバル・ポリシーの両方を使用します。

作成するカスタム・ポリシーは、グローバル・ポリシーの下にあります。独自のセキュリティ・ポリシーを作成しないこととした場合、ユーザーが Campaign で作成したフォルダーとオブジェクトに対して、デフォルトでグローバル・セキュリティ・ポリシーが適用されます。

グローバル・セキュリティ・ポリシーには、事前に定義された 6 つの役割が含まれています。事前に定義された役割を削除することはできませんが、その権限を変更することは可能です。

グローバル・セキュリティ・ポリシーで事前に定義されている役割は、次のとおりです。

- **フォルダー所有者** - ユーザーが作成したフォルダーのすべての権限が有効。すべてのユーザーがこの役割を持っています。ユーザーを割り当てる必要はありません。
- **所有者** - ユーザーが作成したオブジェクトのすべての権限が有効。すべてのユーザーがこの役割を持っています。ユーザーを割り当てる必要はありません。
- **管理** - すべての権限が有効。デフォルト・ユーザー `asm_admin` は、この役割を持っています。
- **実行** - すべての権限が有効。
- **設計** - すべてのオブジェクトに対する読み取り権限および書き込み権限。この役割は、フローチャートやセッションをスケジュールすることはできません。
- **レビュー** - 読み取り専用権限。

Deliver グローバルポリシーのロール

定義済みの文字列に加えて、Campaign ロールの場合、グローバルポリシーにいくつかのロールが含まれています Deliver。 .

グローバルポリシーには以下が含まれますDeliver削除することができます。

- **Deliver_admin** - すべてのメール送信機能、すべてのコンテンツ、すべての文書にアクセスできます。
- **Deliver_execute** - すべてのメール送信機能、すべてのコンテンツ、すべての文書にアクセスできます。
- **Deliver_design** - すべてのコンテンツ、すべての文書、ほとんどのメール送信機能にアクセスできます。ただし、実稼働メールを送信する許可は明示的に与えられません。
- **Deliver_review** - コンテンツと文書の表示のみが可能で、メーリングを操作するための許可が制限されています。メーリングを追加、編集、削除する許可は明示的には与えられていません。テストメールと実稼働メールの表示と送信が許可されます。



Note: Deliver Campaignは、デフォルトで作成されている所有者とフォルダ所有者ロールをサポートしていません。

Campaign でのメッセージ許可

Campaignは、ユーザーまたはグループに割り当てられるロールで定義された特定のアクセス許可を有効または無効にすることにより、メール機能へのユーザーアクセスを制御します。これらのロールは、1つ以上のセキュリティポリシーに関連付けられています。複数定義できます。Campaignセキュリティポリシーを開き、各ポリシーに複数のロールを割り当てます。ポリシーとロールの組み合わせごとに、特定の許可のセットを定義できます。

サンプルセキュリティシナリオを含む、セキュリティアクセス許可の管理方法の詳細については、次を参照してください。*Unica Campaign*管理者ガイド。

に対するロールと許可Unica Platformの場合、メール送信機能とコンテンツの許可を次の場所で割り当てます。Campaignセクションを次のように参照する。

1. ユーザー・ロールを定義します。

次のシステム定義ユーザーロールDeliverは、デフォルトではグローバルポリシーの下に作成されます。

また、カスタムロールを定義し、グローバルポリシーなどの定義したポリシーに追加することもできます。

2. セキュリティポリシーを定義し、ポリシーにユーザーロールを追加します。

デフォルトではグローバルポリシーが定義されています。次に対して追加ポリシーを定義できますCampaign。

3. 各ポリシーのロールに固有の許可を定義します。

追加のポリシーとカスタムロールをさまざまな許可セットで定義して、メール送信機能へのアクセスをより詳細に制御できますCampaignとDeliver文書コンポーザー。

許可、ロール、ポリシーへの変更は、ユーザーがログインしたときに適用されますHCL Unica。ユーザーにメール送信許可を割り当てまたは変更した後、変更を有効にするには、ユーザーはログアウトしてから再度ログインする必要があります。

ルールと許可の使用可能化

Unica Platformに依じてインストールの直後には、役割と許可の定義および適用に必要な管理制御がすぐに表示されない場合があります。にアクセスすると、必要なコントロールを表示することができます。Deliver DocumentComposer またはメーリングインCampaign.

About this task

[Campaignグローバル ポリシーに次の権限がすべて表示されない場合は、次の手順を実行します。

- 「キャンペーン」カテゴリのメールの許可
- [デジタルアセット] カテゴリのコンテンツライブラリに対する許可
- 許可Deliver文書カテゴリ内の文書

1. HCL Unica にログインします。

複数のユーザーが設定されている場合は、最も制限された権限を持つユーザーとしてログインします。たとえば、表示権限のみを持つユーザーとしてログインします。

2. 「**キャンペーン**」 > 「文書の**配信**」にナビゲートして、Document Composer にアクセスします。

DocumentComposer のロードが完了するまで待ちます。

3. 「**設定**」 > 「**ユーザーの役割と許可**」 > 「**キャンペーン**」 > 「**パーティション [n]**」 > 「**グローバル・ポリシー**」にナビゲートしてください。

プロンプトが表示されたら、Document Composer を終了することを確認してページを閉じます。

4. [**ロールの追加と権限の割り当て**] をクリックします。次のDeliverロールが表示されます。

- delivery_admin
- Delivery_execute
- Delivery_design
- Delivery_review

5. [**保存**] と [**アクセス権を編集**] をクリックします。

メール送信の許可は、「キャンペーン」、「デジタル資産」、「文書」カテゴリに表示されます。

使用可能な特定の許可の詳細については、以下のトピックを参照してください。

Campaign による権限の評価方法

ユーザーがタスクを実行するか、オブジェクトへのアクセスを試みると、Campaign は以下のステップを実行します。

1. グローバル・セキュリティー・ポリシー内でユーザーが所属するすべてのグループおよび役割を識別します。

ユーザーは、1つまたは複数の役割に属することができ、役割に属さないこともできます。ユーザーはオブジェクトを所有している場合には所有者役割に属します。オブジェクトが置かれているフォルダーを所有している場合にはフォルダー所有者役割に属します。

ユーザーは、(直接的に、またはその役割に割り当てられているグループに属しているために) その他の特定の役割に明確に割り当てられている場合のみ、その役割に属します。

2. アクセス中のオブジェクトが、カスタム定義ポリシーに割り当てられているかどうかを識別します。割り当てられていれば、システムはそのカスタム・ポリシー内でユーザーが属するすべてのグループと役割を識別します。
3. ステップ 1 および 2 の結果に基づいて、ユーザーが属するすべての役割の権限を集約します。この複合ロールを使用して、システムはアクションの権限を次のように評価します。
 - a. このアクションの権限が **「拒否」** に設定された役割がある場合は、以下のようにして権限を集約します。
 - i. グローバル・ポリシー、1つのカスタム・ポリシーがあり、カスタム・ポリシー役割で権限が DENIED に設定されているとします。この場合は、カスタム・ポリシー役割の権限の DENIAL が、グローバル・ポリシー役割に割り当てられた権限よりも優先されます。
 - ii. グローバル・ポリシー、2つ以上のカスタム・ポリシーがあり、いずれかのカスタム・ポリシー役割で権限が DENIED に設定されていて、他のカスタム・ポリシー役割では同じ権限が GRANTED に設定されているとします。この場合は、カスタム・ポリシーの権限の GRANT が、カスタム・ポリシーの権限の DENIAL よりも優先されます。
 - b. 対象のアクションに関して **「拒否」** 権限を持つ役割がない場合、そのアクションに関して **「許可」** 権限を持つ役割があるかどうかを判別するために検査されます。その役割がある場合、ユーザーはそのアクションを実行できます。
 - c. a と b のどちらも当てはまらない場合、ユーザーは権限を拒否されます。

カスタム・ポリシーが 1 つの場合の例

グローバル・ポリシーの下にカスタム・ポリシー CustomPolicyA が 1 つあるとします。CustomPolicyA には CustomPolicyARole があり、その「追加/編集」の Campaign 権限が DENIED に設定されています。

CustomPolicyARole を割り当てられた UserA について考えてみましょう。この場合は、CustomPolicyARole の「追加/編集」の Campaign 権限の DENIAL が、グローバル・ポリシー役割に割り当てられた権限よりも優先されます。そのため、「追加/編集」の Campaign オブジェクトは UserA には表示されません。

カスタム・ポリシーが 2 つある場合の例

グローバル・ポリシーの下に 2 つのカスタム・ポリシー CustomPolicyA および CustomPolicyB があるとします。CustomPolicyA と CustomPolicyB の両方には、それぞれ CustomPolicyARole と CustomPolicyBRole があります。CustomPolicyARole では、「追加/編集」の Campaign 権限が GRANTED に設定されています。CustomPolicyBRole では、「追加/編集」の Campaign 権限が DENIED に設定されています。

UserA には CustomPolicyARole および CustomPolicyBRole の両方が割り当てられています。CustomPolicyARole の「追加/編集」の権限の GRANT が、CustomPolicyBRole の権限の DENIAL より優先されます。そのため、「追加/編集」の Campaign オブジェクトは UserA に表示されます。

権限の状態の定義

それぞれの役割について、どの権限を認可するか、認可しないか、または拒否するかを指定することができます。これらの権限は、「設定」 > 「ユーザーの役割と権限」 ページで設定します。

これらの状態には以下の意味があります。

- **「付与済み」** - チェック・マーク で示されます。ユーザーのその他の役割で明示的に権限が否定されない限り、この特定の機能を実行する権限が明示的に認可されます。
- **「拒否済み」** - 「X」 で示されます。ユーザーの他の役割で権限が認可されているかどうかに関係なく、この特定の機能を実行する権限が明示的に拒否されます。
- **「付与されていません」** - 円 で示されます。特定の機能を実行する権限を明示的に認可または拒否しません。ユーザーの役割のいずれかでこの権限が明示的に認可されていない場合、ユーザーはこの機能を実行することはできません。

Campaign でのメーリングに対する許可

Campaign、ユーザーが作成、構成、実行、監視Deliverメーリング (オン)Deliverメーリングタブ。宛先は別のタブで管理します。

次の権限は、Deliverメール タブへのユーザー アクセスを制御します。これらのファイルは **[キャンペーン]** カテゴリにあります。

権限	説明
メーリングの表示	ユーザーにDeliver件名を指定します。ユーザーは、メールアドレスを編集または変更することはできません。
メーリングの編集	ユーザーがキャンペーンのDeliverメールタブを設定または変更できるようにします。
メーリングの削除	ユーザーがDeliverメールを送信しています。
メーリングの追加	キャンペーンにメーリングの作成をユーザーに許可します。
実稼働メールの送信	メーリングの実行の開始、トランザクション E メール用のメーリングの有効化、またはメーリングの実行のスケジュールをユーザーに許可します。 実稼働メールには、多くのメッセージを含めることができます。E メールは、そのメーリングに関連付けられた受信者リストで実稼働受信者として指定されたすべての個人に送信されます。
テスト実行の実行	メーリングのテスト実行の開始をユーザーに許可します。 通常、テストメールには数件のメールが送信されます。テスト実行中、メールは、メーリングに関連付けられた受信者リストでテスト受信者として識別されたすべてのアドレスに送信されます。

「デジタル資産」カテゴリの許可

デジタル資産許可は、コンテンツ要素へのユーザーアクセスを制御しますDeliverコンテンツライブラリ、およびそれらが保存されているフォルダとサブフォルダへ移動します。

コンテンツライブラリは、ユーザーがデータベースで作成した通信で使用されるコンテンツ要素 (デジタル資産とも呼ばれます) のリポジトリです。Deliver文書コンポーザー。

権限	説明
ビュー-Deliverデジタル資産	ユーザーがコンテンツエレメントを開いて、プロパティを表示したり、個人用連絡に追加できるコンテンツのプレビューを行うことを許可します。
Deliverコンテンツライブラリに次の新規デジタルアセットを作成します	コンテンツ要素の作成とコンテンツライブラリに追加することをユーザーに許可します。
Deliverコンテンツライブラリに次の既存のデジタル資産を編集します。	ユーザーが既存のコンテンツ要素を開いて編集することを許可します。
Deliverコンテンツライブラリに次からデジタル資産を削除します。	コンテンツライブラリからコンテンツ要素を削除することをユーザーに許可します。
フォルダからフォルダへのデジタルアセットの移動	コンテンツライブラリ内でコンテンツ要素を移動することをユーザーに許可します。コンテンツ要素を移動するには、移動元のフォルダと移動先のフォルダにこの許可を割り当てる必要があります。

文書カテゴリの許可

文書カテゴリのアクセス権は、個人用通信を作成、編集、管理するためのユーザーアクセスを制御します。Deliver文書コンポーザー。

権限	説明
ビュー-Deliver文書	メールの作成に使用される文書の参照をユーザーに許可する、受信ボックスプッシュ通知、ホストされているランディングページを指定します。
新規作成Deliver文書	新規の個人用連絡先を作成することをユーザーに許可します。
既存を編集(_E)Deliver文書	既存の個人用連絡先の変更をユーザーに許可します。
削除(_D)Deliver文書	カスタマイズされた連絡の削除をユーザーに許可します。
公開Deliver文書、公開インターネットでコンテンツを使用可能	カスタマイズされた連絡を公開することをユーザーに許可します。 連絡を公開すると、文書と追加されたすべてのコンテンツをメールで使用できるようになります。Deliverを参照してください。
コピー-Deliverフォルダから別の文書へ	コンテンツライブラリのフォルダ間で個人用通信をコピーすることをユーザーに許可します。

権限	説明
	連絡をコピーするには、この許可をソースフォルダと宛先フォルダに割り当てる必要があります。
移動Deliverフォルダから別の文書へ	個人用連絡先をコンテンツライブラリ内のフォルダから別のフォルダに移動することをユーザーに許可します。 連絡を移動するには、この許可をソースと宛先のフォルダに割り当てる必要があります。

[メール管理] カテゴリの権限

[メール管理] カテゴリのアクセス権は、Campaignグローバルポリシーが提供Deliverさまざまなメッセージドメインとメッセージ機能へのユーザーアクセスを制御する設定へのアクセス権を持つ管理者。

管理者は、Deliver設定ウィンドウ。たとえば、管理者は、ユーザーが通信エディタで作成されたメールの送信者:ドメインとして選択できるメールアドレスのリストを制限できます。「ポリシーの設定」セクションは、適切な許可がCampaignグローバルポリシー。

管理者は、モバイルアプリケーションを次の場所に登録するための管理インターフェースへのアクセスも制御できます。Deliverまた、ロケーショントリガー配信で使用するロケーションを設定します。管理ページへのリンクは、Deliver「設定」ページの「モバイル通知設定」セクションに表示されます。Deliver[設定] ページの [モバイル通知設定] セクションを表示するには、ホスト型メッセージングアカウントでモバイルメッセージングを有効にする必要があります。

権限	説明
ドメインの設定	Deliver「設定」ページの「ポリシー設定」セクションへのアクセスを制御します。メールアドレスを設定する権限が管理者のロールに付与されていない場合、管理者は [ポリシー設定] セクションを表示できません。この許可は、短縮リンクドメインを管理する場合にも必要です。

次のメール許可Deliver

Unica Deliver[メール] タブCampaignの外部のメール機能へのアクセスを制御しますを以下の事前定義セキュリティロールを通じて使用します。

- Delivery_Admin
- Delivery_user

ユーザーがアクセスするには、両方のロールが必要ですDeliverはじめます。

Deliverロールの割り当て

次へのフルアクセスをユーザーに提供するにはDeliverメール機能、定義済みのDeliverロールをユーザーに追加します。

1. インUnica Platformから、「設定」 > 「ユーザーロールと許可」 > 「配信」 > パーティション [n] > 「Deliver_admin」にナビゲートします。
2. **[ユーザーの割り当て]**をクリックします。
3. 使用可能なユーザーのリストからユーザーを選択します。「追加」をクリックして、ユーザーにロールを割り当てます。
4. Deliver_user ロールについて、ステップ 1 から 3 を繰り返します。
5. 変更を保存します。

メールアドレスと短縮リンクドメインの制御

要求に応じて、Unicaホストメールアドレスのメールアドレスを設定します。Unicaでは、ドメインを割り当てることもできます。では、マーケターがさまざまなタイプのメッセージ内に短縮リンクを作成するために使用します。適切な許可を持つシステム管理者は、マーケターが使用できるメッセージドメインを制御します。

About this task

ビジネス要件によっては、特定のマーケターが利用できるメッセージドメインのリストを制限したい場合があります。Deliver管理者は、Document Composer でフォルダに適用されるセキュリティポリシーを使用して、使用可能なドメインのリストを制限します。マーケティング担当者がEメールを作成および編集する機能は、連絡が含まれるフォルダに適用されるセキュリティポリシーによって異なります。

Deliver適切な権限を持つ管理者は、次のことを行うメールアドレスのリストを制御できます。Deliverユーザーはメールを送信者:ドメインとして使用できます。管理者は、短縮リンクを使用する通信を設定するときにマーケターに表示される短縮リンクドメインのリストを制御することもできます。たとえば、マーケターがソーシャル共有リンクをマーケティングメッセージに追加するときに、利用可能な短縮リンクドメインを指定できます。

Deliver管理者は、**[ポリシー設定]**ページを使用して、特定のメッセージドメインの使用許可を付与します。「**ポリシー設定**」ページへのアクセスは、Campaign グローバルポリシーによって付与されるメール管理許可によって制御されます。適切な権限を持つ管理者のみが、**[ポリシー設定]**ページからメールアドレスへのアクセスを制限できます。

1. **[設定]**メニューの**[メール設定]**を選択します。

Result

適切な管理許可を持っている場合、**[ポリシーの設定]** セクションが表示されます。Deliver設定ページ。

2. **[ポリシーと設定のリストの表示]**をクリックします。

Result

システムに設定されているセキュリティポリシーのリストDeliverインストールが表示されます。

3. メッセージドメインアクセスを制御したいシステムユーザーに関連付けられたセキュリティポリシーをクリックします。

[ドメイン] セクションに、ホストメッセージアカウント用に設定されているメールアドレスが表示されます。

[短縮リンクドメイン] セクションには、ホストメッセージアカウント用に設定された短縮リンクドメインが表示されます。

- いずれかのセクションで、**[すべてのドメインを使用]** をクリックして、ポリシーに関連付けられたユーザーに、次の条件が設定されたすべてのメールドメインの使用を許可します。Unicaホストメールアカウント用に設定されています。

このオプションはデフォルトです。

- **特定のドメインを選択するには、[特定のドメインを使用]** をクリックします。



Note: **[特定のドメインを使用]** を選択した場合、ホストメッセージアカウントの新規メールドメインまたは短縮リンクドメインを登録するときに、ドメイン許可を更新する必要があります。新しいドメインの許可は、自動的に割り当てられません。

Results

このセキュリティポリシーに関連付けられたユーザーには、選択したメールドメインのみが、メールの送信者アドレスのオプションとして表示されます。短縮リンクを必要とする通信の場合、マーケターは、ユーザーが選択した短縮リンクのドメインのみを選択できます。

新規設定の保存後、Document Composer は、マーケティング担当者が使用できるドメインオプションを更新します。

方法の詳細Deliverマーケターは、連絡の作成と管理、を参照してください。 *UnicaDeliver* ユーザーズ・ガイド。

ホストメールドメインの保守

メールメッセージを送信するには、少なくとも1つのメールドメインを登録する必要がありますUnica。メッセージの到達率を改善するには、Unicaは、世界中の主要なインターネットサービスプロバイダ (ISP) と共に協力してドメインのメール評価を確立し、維持することができます。次のコマンドで複数のメールドメインを設定できますUnica。

メールにヘッダーを設定すると、システムによって送信者アドレスに登録済みのメールドメインが設定されますUnica。を使用して複数のメールドメインを設定する場合Unicaの場合、使用可能なドメインがドロップダウンリストに表示されます。システム管理者は、メール担当者が選択または変更できるメールドメインを制御できます。

要求できます。Unicaホストされたメッセージアカウント用に設定されたメールドメインを追加または削除します。後Unicaが変更を完了すると、使用可能なメールドメインのリストが更新されます。変更は、次回メール通信を作成または編集したときに、使用可能なメールドメインのリストに反映されます。



Note: アカウントのメールドメインを変更しても、変更要求前に作成していたメールは更新されません。以前に作成された連絡のメールドメインを変更するには、メール連絡を再度開いて、メールドメインの選択を更新する必要があります。

でのメールドメインの登録方法の詳細についてUnica、参照 *HCL Unica* メール のドメイン名オプション。

メールドメインに関連する変更を要求するには、HCL 技術サポートから Unica Delivery Services チームに連絡してください。

デフォルトの送信者アドレスと表示名の構成

登録しているメールアドレスごとUnicaでは、デフォルトのメールアドレスとデフォルトのわかりやすい名前を定義できます。送信するメールの送信者:アドレスとして、メールアドレスまたはわかりやすい名前とメールアドレスの組み合わせが表示されます。

About this task

管理者は、デフォルトの送信者名と表示名をドメイン設定ページで設定できます。ドメイン設定はDeliver設定インターフェース。[ドメイン設定] ページへのアクセスは、以下を介して付与されるメール管理権限によって制御されます。Campaignグローバルポリシー。適切な権限を持つ管理者のみが、[ポリシー設定] ページからメールアドレスへのアクセスを制限できます。

1. **[設定] > [配信設定]**に移動します。「ドメイン設定」セクションで、「ドメイン設定のリストの**表示**」をクリックします。

[ドメイン設定] ページには、ホストメールアドレスに登録されているメールアドレスに関連付けられたデフォルトの表示名とメールアドレスがリストされます。リストには、変更を許可されたユーザー許可のドメインのみが含まれます。

「デフォルト」列は、表示名、アドレス、新規メールのデフォルトの送信者アドレスとして表示されるドメインの組み合わせを示します。

2. **[編集]** をクリックします。。「ドメイン設定の編集」ウィンドウが開きます。

[ドメイン名] 列に、使用可能なメールアドレスのリストが表示されます。すべてのドメインに対して、以下を実行できます。

- [送信者] 列に、リストのメールアドレスのデフォルトとして表示するわかりやすい名前を入力します。
- [送信者アドレス] 列に、リストのメールアドレスのデフォルトとして表示するメールアドレスのローカル部分を入力します。

3. 必要に応じて、「デフォルト」列で、新規メールのデフォルトの送信者アドレスとして表示される表示名アドレスとドメインの組み合わせを1つ選択します。

デフォルトを選択しない場合、リストの最初のドメインを使用して、新規メールのデフォルトの送信者アドレスが作成されます。

4. 変更を保存します。

Results

新しいアドレス設定は、作成するすべての新規メールに適用されます。この設定によって、以前に作成されたEメール通信のアドレス情報は変更されません。以前のメール連絡を更新するには、それぞれの連絡を再度開いて変更する必要があります。

送信メールリストへのアクセス制御

Deliverから送信されたメールのリストを提供します。Deliver環境に表示されます。リストにはメッセージ設定へのリンクが含まれているため、セキュリティ計画によって、リストへのアクセスを制限する必要がある場合があります。

About this task

メッセージのリストは「**メッセージの概要**」ページに表示されます。デフォルトでは、Campaign and Deliver environment は送信メッセージのリストを参照できます。ただし、アクセス制限を有効にした場合、特定のユーザーに、リストを含むページを開くためのメニューオプションを表示することを防止できます。

送信メッセージリストへのアクセスを制限すると、Campaignインストールされます。あなたのCampaignインストールに複数のパーティションが含まれる場合、各パーティションで個別にユーザー許可を更新して、リストにアクセスする許可を明示的に許可または拒否する必要があります。

送信メッセージリストにアクセスできるユーザーを制御するには、ユーザー許可とシステム設定を変更するための一連のタスクが必要です。

タスク	詳細情報
メッセージのリストにアクセスできるユーザーを識別します。最初に、すべてのユーザーにアクセスが許可されます。	送信メールリストへのアクセスを許可中 on page 79
メッセージリストへのアクセスを許可されないユーザーを特定します。	送信メールリストへのアクセスの拒否 on page 80
アクセス制限を有効にします。	送信メール一覧への制限を有効にする on page 81

Results

これらのタスクを完了した場合、メールリストへのアクセス権を明示的に付与した役割を持つユーザーにのみ、「**キャンペーン**」メニューの「**メッセージオーバービュー**」オプションが表示されます。

送信メールリストへのアクセスを許可中

送信メッセージのリストへのアクセスを制限する場合、リストにアクセスする必要があるユーザーに、アクセスを許可する必要があります。

About this task

ユーザーは、[**キャンペーン**]メニューの[**メッセージ概要**]リンクをクリックして、送信メッセージのリストにアクセスします。すべての送信メールのリストへのアクセス権をユーザーに許可するには、「メールの**概要**」リンクを表示する権限が明示的に付与された最上位の管理ロールをユーザーに割り当てます。

デフォルトの最上位のロールには、**Admin**、**実行**、**設計**、**レビュー**が含まれます。最上位のロールを通じて付与した権限は、パーティション内のすべてのオブジェクトに適用されます。

1. 「設定」 > 「ユーザーロールと許可」 > 「キャンペーン」 > 「partition (n)」に移動します。
2. **[保存]** と **[アクセス権を編集]** をクリックします。
パーティションの許可のリストが開きます。使用可能な最上位のロールが、ページの上部にリストされています。
3. **[管理]** セクションで、すべてのロールに**[メーリングリストページの表示]**権限を明示的に付与します。

Results

送信メッセージリストのアクセス制限を有効にすると、「**[メーリングリストページの表示]**」権限が明示的に付与されているロールを持つユーザーは、**[キャンペーン]** メニューに**[メッセージの概要]** リンクが表示されます。

What to do next

送信メッセージリストへのアクセスを拒否するロールを作成します。

送信メールリストへのアクセスの拒否

送信メッセージリストへのアクセスを制限する場合、リストへのアクセスを許可されないユーザーに対して、具体的にアクセスを拒否する必要があります。

About this task

ユーザーは、**[キャンペーン]** メニューの**[メッセージ概要]** リンクをクリックして、送信メッセージのリストにアクセスします。「メールの**[概要]**」リンクを表示する権限を明示的に拒否されている最上位の管理ロールをユーザーに割り当てると、ユーザーがすべての送信メールのリストにアクセスできないようにすることができます。

デフォルトの最上位のロールには、**Admin**、**実行**、**設計**、**レビュー**が含まれます。最上位のロールを通じて付与した権限は、パーティション内のすべてのオブジェクトに適用されます。デフォルトの最上位のロールを補完する新規の最上位のロールを作成できます。新しいロールでは、特定の許可を許可または拒否できます。

1. 「設定」 > 「ユーザーロールと許可」 > 「キャンペーン」 > 「partition (n)」に移動します。パーティション <n> ページが開きます。
2. **[ロールの追加]** をクリックします。ロールに名前を割り当て、簡単な説明を入力します。変更を保存してパーティション <n> ページに戻ります。
3. 送信メールのリストへのアクセスを拒否するには、新規ロールを設定します。
 - a. **[ロールの追加と権限の割り当て]** をクリックします。「**管理ロールのプロパティ**」ページが開きます。新規ロールがロールのリストに表示されます。
 - b. **[保存]** と **[アクセス権を編集]** をクリックします。
パーティションの許可のリストが、各ロールの各許可の状態を示す選択アイコンのマトリックスとして表示されます。新規ロールは、マトリックスの上部にある他の最上位のロールの横に表示されます。
 - c. **[管理]** セクションで、新しいロールに対する**[メーリングリストページの表示]**権限を明示的に拒否します。変更を保存します。
4. メーリングリストページにアクセスさせないユーザーに、新規ロールを割り当てます。

- a. **[設定]** > **[ユーザー]** に移動します。送信メッセージリストへのアクセスを禁止するユーザーを選択します。
- b. **[ロールの編集]** をクリックします。前のステップで作成した新規ロール (アクセスを拒否するように設定されたロール) が、**利用可能なロール** のリストに表示されます。
- c. 新規のロールを **[使用可能なロール]** から **[ロール]** に移動します。変更を保存します。

Results

送信メールリストのアクセス制限を有効にした場合、新規ロールを割り当てられたユーザーには [メールの**概要**] リンクを表示できません。

What to do next

設定を更新して、送信メールリストのアクセス制限を有効にしてください。

送信メール一覧への制限を有効にする

ユーザーは、**[キャンペーン]** メニューの **[メッセージ概要]** オプションから送信メッセージのリストにアクセスします。送信メッセージのリストへのアクセスを制限する場合、「セキュリティ機能 ID」プロパティによってこのメニューオプションの表示が制御され、送信メッセージリストへのアクセスが制御されます。

About this task

送信メッセージのリストへのアクセスを制限するには、Platform削除します。このプロパティは、Campaignインストールされます。

セキュリティ機能 ID に正しい値を設定した場合、「メーリングリストページの表示」許可を明示的に許可するロールを持つユーザーのみが、「**メッセージ概要**」オプションを使用できます。「メーリングリストページの表示」権限が拒否されているロールまたは付与されていないロールを持つユーザーには、「**メッセージの概要**」オプションは表示されません。

1. **[設定]** > **[構成]** > **[プラットフォーム]** > **[プラットフォーム間ナビゲーション]** > **[メインナビゲーションメニュー]** > **[キャンペーン]** > **[メーリングの配信]** に移動します。「**メーリングの配信**」をクリックして、設定を表示します。
2. **[設定の編集]** をクリックします。
3. 「**セキュリティ機能 ID**」フィールドに、7000を入力します。変更を保存します。

設定の変更結果を確認するには、システムからログアウトし、再度ログインします。

Results

送信メールリストにアクセスするためのメール**概要**リンクが表示されます。

レポート Deliver の許可

ユーザー権限によって、レポートを表示 Deliver できるかどうかが決まります。

標準へのアクセス権の設定方法について Deliver レポートの詳細については、レポートとセキュリティに関する『*Unica Insights Reports* インストール/設定ガイド』のセクションを参照してください。

Chapter 10. 技術情報 (問題解決)

問題 (要約)

Unica Campaign と共にインストールされる Deliver コンポーネントを使用し、個人化されたマーケティングメッセージを送信するには、ローカルの Campaign インストール済み環境を、HCL がホストするリモートメッセージリソースに接続する必要があります。このセクションでは、会社のファイアウォールルールによってホスト環境との直接通信が禁止されている場合に、そのような接続を設定する方法を説明します。

問題の解決

ホストされている E メールリソース環境との一般的な通信

次の図は、オンプレミス (OP) 環境とオンデマンド (OD) 環境間の通信の標準的な設定を示しています。

ローカルの Deliver OP 環境は、HTTPS と FTP (明示的 FTP) または FTP (黙示的 FTP) を使用して、Deliver OD 環境との外部通信を必要とします。このセクションでは、明示的 FTP と黙示的 FTP の両方を示すために FTPS という用語を使用します。

OP 環境に、Campaign をデプロイした Web アプリケーションサーバー (IBM WebSphere または Oracle WebLogic のいずれか) が含まれています。Campaign は、OD 環境でホストされる E メールリソースと通信する Deliver コンポーネント (RCT および RLU) をホストします。

Response and Contact Tracker (RCT) は、OD 環境から応答データをダウンロードします。

応答リストアップローダ (RLU) は、メーリングリストやその他の必要なメーリングデータを OD 環境にアップロードします。

Unica Deliver がインストールされているマシンが OD 環境と直接通信できない場合、Deliver は SOCKS プロキシ経由でホストされている OD リソースとの通信をサポートします。

プロキシを経由してメッセージサービスに接続

次の図は、SOCKS プロキシを使用した場合の OP 環境と OD 環境間の通信を示しています。SOCKS プロキシはローカルの「オンプレミス」環境で設定されていることに注意してください。

プロキシオプションを有効にする前に、以下の点を確認してください。

- プロキシサーバーは SOCKS プロキシです。
- プロキシサーバーは Delivery OD 環境にアクセスでき、ホストメールアカウントが使用する HCL データセンターで設定されたポートとのトラフィックを許可します。
- Delivery OP 環境がプロキシにアクセスできる方法で SOCKS プロキシをインストールしている必要があります。

SOCKS プロキシ経由で FTPS と HTTPS トラフィックをルーティングするために必要な変更

SOCKS プロキシを使用して HCL がホストする E メールリソースにアクセスするには、Campaign をデプロイした Web アプリケーションと、RCT と RLU を配信の開始スクリプトを変更する必要があります。

FTPS の変更

FTPS トラフィックの場合、以下の設定を RLU と Web アプリケーションサーバーに適用します。

- `- Dhcl.unica.deliver.ftp.proxy.host = <socksHost>`
- `- Dhcl.unica.deliver.ftp.proxy.port = <socksPort>`
- `- Dhcl.unica.deliver.ftp.proxy.match.hosts = <ホスト名と IP アドレスのカンマで区切られたリスト>`

successhost は SOCKS プロキシのホスト名または IP です。

SOCKS ポートは SOCKS プロキシが実行されているポートです。

`-Dhcl.unica.deliver.ftp.proxy.match.hosts` は、SOCKS プロキシを経由してトラフィックをルーティングするときに使用されるホスト名と IP に一致します

`-DhCL.unica.deliver.ftp.proxy.match.hosts` に対して指定された IP アドレスです。データ転送中に、ホスト OD 環境の FTP サーバーがローカル OP 環境の FTP クライアントに FTPS プロトコルの一部として送信する IP アドレスです。 .

`-DhCL.unica.deliver.ftp.proxy.match.hosts` を次のいずれかの値に設定します。(ホストメールアカウントで使用されているデータセンターによって異なります)

米国のデータセンター: `-DhCL.unica.deliver.ftp.proxy.match.hosts=ftp-em.unicadeliver.com`

デモ環境: `-DhCL.unica.deliver.ftp.proxy.match.hosts=1SS.212.8.162`

ヨーロッパのデータセンター: `-DhCL.unica.deliver.ftp.proxy.match.hosts=ftp-eu.unicadeliver.com`

HTTPS 用の変更

HTTPS トラフィックの場合、RCT と Web アプリケーションサーバーに以下の設定を適用します。

`-DhCL.unica.deliver.https.proxy.host= <sockshost>`

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

`-DhCL.unica.Deliveryr.https.proxy.type=SOCKS`

successhost は SOCKS プロキシのホスト名または IP です。

SOCKS ポートは SOCKS プロキシが実行されているポートです。

SOCKS プロキシを使用するときの認証要件

SOCKS プロキシが認証を必要とする場合、Web アプリケーションサーバー、RLU と RCT を以下を設定します。

- `-DhCL.unica.deliver.proxy.auth.user = <ユーザー名>`
- `-DhCL.unica.deliver.proxy.auth.password = <パスワード>`

ユーザー名とパスワードは、プロキシに対する認証に必要な資格情報です。

SOCKS プロキシを使用して RCT を設定するには

SOCKS プロキシを介して動作するように RCT を構成します。オペレーティングシステムに応じた手順に従います。

Windows 環境での RCT の場合

ローカルの Delivery インストール済み環境の `//deliver/bin` ディレクトリーにある `Common.bat` に、以下のプロキシ引数を追加します。

```
set RCT_PROXY_ARGS=  
  
-DhCL.unica.deliver.https.proxy.host=<PROXY_HOST>  
  
-DhCL.unica.deliver.https.proxy.port=<PROXY_PORT>  
  
-DhCL.unica.Deliveryr.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
```

UNIX 環境の RCT の場合

以下のプロキシ引数をローカルの Delivery インストールの `\\deliver\bin` ディレクトリーの `Common.sh` に追加します。



Note: `rlu.sh.rct.sh` または `setenv.sh` は上書きされるため、直接変更しないでください。

```
RCT_PROXY_ARGS="  
  
-DhCL.unica.deliver.https.proxy.host=<PROXY_HOST>  
  
-DhCL.unica.deliver.https.proxy.port=<PROXY_PORT>  
  
-DhCL.unica.Deliveryr.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}"
```

SOCKS プロキシを使用して RLU を設定するには

SOCKS プロキシを介して機能するように RLU を構成するには、オペレーティングシステムに応じた手順に従います。

Windows 環境での RLU の場合

ローカルの Deliver インストール済み環境の `//deliver/bin` ディレクトリーにある `common.bat` に、以下のプロキシ引数を追加します。

```
set RLU_PROXY_ARGS=

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

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

-Dhcl.unica.deliver.https.proxy.match.hosts=<comma separated list of host names and IP addresses>

-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>

-DhCL.unica.deliver.proxy.auth.password=<PROXY_AUIH_PASSWORD>

設定 RLU_JAVA_ARGS=%BASE_VM_ARGS% %RLU_MEM_ARGS% %RLU_EXTRA_VM_ARGS%
%RLU_PROXY_ARGS%
```

UNIX 環境の RLU の場合

以下のプロキシ引数をローカルの Delivery インストールの `\deliver\bin` ディレクトリーにある `Common.sh` に追加します。



Note: `rlu.sh`、`rct.sh` または `setenv.sh` は上書きされるため、直接変更しないでください。

```
RLU プロキシARGS=

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

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

-Dhcl.unica.deliver.https.proxy.match.hosts=<comma separated list of host names and IP addresses>

-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} "
```

WebSphere 設定の変更

WebSphere の一般的な JVM 引数に以下を追加します (スクリーンショットを参照):

```
-DhCL.unica.deliver.https.proxy.host=<PROXY_HOST>  
  
-DhCL.unica.deliver.https.proxy.port=<PROXY_PORT>  
  
-Dhcl.unica.deliver.bhttps.proxy.type=SOCKS  
  
-DhCL.unica.deliver.ftps.proxy.host=<PROXY_HOST>  
  
-DhCL.unica.deliver.ftps.proxy.port=<PROXY_PORT>  
  
-Dhcl.unica.deliver.ftps.proxy.match.hosts=<comma separated list of host names and IP addresses>  
  
-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>  
  
-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_ PASSWORD>
```

Oracle WebLogic 構成の変更

WebSphere の場合は、スクリプトを変更します。

Windows 環境の場合

```
Java_OPTIONS=%(JAVA_OPTIONS)  
  
-DhCL.unica.deliver.https.proxy.host=<PROXY_HOST>  
  
-DhCL.unica.deliver.https.proxy.port=<PROXY_PORT>  
  
-Dhcl.unica.deliver.bhttps.proxy.type=SOCKS  
  
-DhCL.unica.deliver.ftps.proxy.host=<PROXY_HOST>  
  
-DhCL.unica.deliver.ftps.proxy.port=<PROXY_PORT>  
  
-Dhcl.unica.deliver.ftps.proxy.match.hosts=<comma separated list of host names and IP addresses>  
  
-Dhcl.unica.deliver.proxy.auth.user=<PROXY_AUIH USER>  
  
-Dhcl.unica.deliver.proxy.auth.password=<PROXY_AUTH_ PASSWORD>%
```

UNIX 環境の場合

```
Java_OPTIONS='(JAVA_OPTIONS)
```

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

```
-DhCL.unica.deliver.https.proxy.port=<PROXY_PORT>
```

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

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

```
-DhCL.unica.deliver.https.proxy.port=<PROXY_PORT>
```

```
-Dhcl.unica.deliver.https.proxy.match.hosts=<comma separated list of host names and IP addresses>
```

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

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

Chapter 11. チャネルベンダーアカウント設定の提供

Delivery は、メールのほかに、送信チャネルとして SMS、WhatsApp、プッシュをサポートします。Delivery は、メールのほかに、送信チャネルとして SMS、WhatsApp、プッシュをサポートします。SMS はさまざまなベンダーのサポートが提供しています。そのため、お客様は、地域とコストの側面に基づいて SMS パートナーを選択することができます。顧客が SMS または WhatsApp メッセージを特定のベンダーを使用することを決定するたびに、HCL はその顧客と連携し、彼がスムーズに配信できるオンボードを行うように要求しました。このプロセスの一部として、各ベンダーに顧客アカウントが作成されます。このアカウントにより、配信者がその顧客の代わりにメッセージを送信したり、ユーザーからの応答を処理したりできます。

配信は、次のチャネルをサポートしています。

- Karix ベンダーを使用した SMS
- RML ベンダーを使用する SMS (紹介と再販業者タイプのライセンスの両方)
- RML ベンダーを使用した WhatsApp
- ベンダーとして Kumos を使用したプッシュ
- Twilio SMS

次の文書では、これらのチャネルごとのステップを説明します。これらのステップは、オンボードプロセスの一部として、顧客アカウントごとに実行する必要があります。

Karix SMS アカウント設定

以下のステップを実行して、顧客の Karix SMS アカウントを Deliver で動作するように構成します。

1. Karix コンソール (www.karix.solutions) にログインし、ダッシュボードの [API キー] ボタンをクリックして API キーを作成し、[配信] で設定を行います。
2. 右上隅の[自分のアカウントを開く]リストの下で、[個人情報の編集] オプションを選択し、Karix アカウント用に構成された送信者 ID を [配信] に設定します。
3. ステップ 1 で作成した API キーとステップ 2 でメモした Sender ID をアカウントに設定します。
4. Karix コンソールにコールバック URL を設定します。

- 米国のデータセンターの場合: <https://smsin-us.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=karix&dmy=1>
- EU データセンターの場合: <https://smsin-eu.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=karix&dmy=1>



Note: Deliver でアカウントを構成したら、上の URL の <アカウント> を配信プロビジョニングチームから提供されたアカウント名に置換する必要があります。

RML SMS アカウント構成

顧客の RML SMS アカウントが配信を使用するには、以下の設定を行う必要があります。

RML アカウントオンボード

- RML チームと協力して、顧客の場所に基づいて、インドまたは世界各国用の SMS アカウントを作成する必要があります。
- senderid は RML で設定され、お客様が提供する必要があります。
- また、SMS テンプレートは、ターゲットの SMS 送信場所に基づいて、ホワイトリストに登録する必要があります。たとえば、アメリカとカナダには事前承認テンプレートが必要です。

RML には地域に基づいて異なるログイン URL があり、アカウント作成メールの一部として RML 側から提供されます。例: インドと世界のデータセンターの URL

- インドのアカウント: <https://ems.rmlconnect.net/>
- グローバルアカウント: <https://client.rmlconnect.net/login>

次のステップを実行します。

1. 上記の URL に従って RML Console にログインし、**[ユーティリティ] > [DMR プッシュ URL]** に移動します。



Note: アカウントのプロビジョニング中にこのメニューを追加するように RML に要求する必要があります。

2. RML コンソールでコールバック URL を設定します。

- 米国のデータセンターの場合: <https://smsin-us.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=RML>
- EU データセンターの場合: <https://smsin-eu.unicadeliver.com/deliversmsib/sms?partition=<account>&provider=RML>



Note: Deliver でアカウントを構成したら、上の URL の <アカウント> を配信プロビジョニングチームから提供されたアカウント名に置換する必要があります。

RML WhatsApp アカウント設定

About this task

WhatsApp 機能 (RML 提供) がプロビジョニングされたお客様は、以下の構成ステップを実行する必要があります。

1. WhatsApp 用の確認済みの Facebook Business Manager アカウント設定を作成します。RML チームが、必要に応じて Facebook Business Manager アカウントを設定するようにお客様をサポートします。
2. RML で WhatsApp アカウントを作成します。Facebook Business Manager アカウントの確認が完了した後、RML はこのアカウントを作成します。
3. WhatsApp で承認されたメールテンプレートを作成します。RML チームはお客様と協力して、必要な形式のメッセージテンプレートを準備し、お客様の承認を取得します。
4. RML が承認済みテンプレートを顧客に提供したら、顧客は[新規] > [WhatsAppコンテンツ] メニュー項目を使用して、それらをメッセージ配信エディターにアップロードする必要があります。WhatsApp はテンプレートの承認後の変更を許可していないため、すべての詳細は承認されたテンプレートに従って正確に提供する必要があります。
5. RML WhatsApp アカウントにコールバック URL を設定します。このためには、以下の URL を RML に提供する必要があります。これは、whatsapp メッセージ送信レポートのコールバック URL として設定できるようにします。

<https://smsin-us.unicadeliver.com/delivermsib/wa/<アカウント>>

Twilio SMS アカウント設定

About this task

顧客の Twilio SMS アカウントを配信と使用するには、以下の設定が必要です-

1. Twilio コンソール (<https://www.twilio.com/console>) にログインし、SMS 用のプロジェクトを作成します。このプロジェクトの ACCOUNT SID と AUTH TOKEN をコピーします。
2. <https://www.twilio.com/console/sms/services> でこのアカウントのメッセージサービス ID を作成し、後で使用するためにそのメッセージサービス ID をコピーしてください。
3. Twilio オンボードチームと協力してアカウントをアップグレードし、任意の携帯電話番号に確実に SMS を送信できるようにしてください。体験版アカウントは、番号に SMS を送信する前に、その番号をホワイトリストに登録する必要があります。

Index

Special Characters

ユーティリティー
configTool 64

C

configTool 64
configTool ユーティリティー 64