Siebel

Marketing Installation and Administration Guide

September 2026

Siebel
Marketing Installation and Administration Guide

September 2026

F87461-09

Copyright © 1994, 2025, Oracle and/or its affiliates.

Author: Sukanya Mishra

Contents

Get Help i

1 What's New in This Release 1

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 26.9 Update 1
What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 26.8 Update 1
What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 26.7 Update 1
What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 25.11 Update 2
What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 24.9 Update 2
What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 22.4 Update 3
What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 21.10 Update 3
What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 21.5 Update 3

2 Installing and Administering Siebel Marketing 5

Installing and Administering Siebel Marketing 5
Installing Siebel Marketing 5
Installing Marketing Contact List Import Using PL/SQL 6
Enabling and Synchronizing Marketing Server Components 9
Activating and Configuring Marketing Workflow Processes 11
Activating and Registering Tasks for Marketing Activities 15
Updating Marketing Connection Settings 15
Enabling Automatic Responses for Opportunities and Orders 20
About the Marketing Approval Process 21
Configuring the Marketing Approval Values 21
Load Balancing and Global Deployment of Siebel Marketing 23
About Marketing Responsibilities and Access Groups 24
Creating Marketing Seed Data 28
Configuring Social Sharing Communities for Email Treatments 29
Guidelines for Testing the Marketing Module in an Integrated Environment 30
Monitoring Marketing System Tasks 33

3 Creating Source Code and Vendor Profiles 35

Creating Source Code and Vendor Profiles 35

About Source Codes 35
Creating Source Code Formats 36
Setting Up Vendor Profiles 38

4 Designing Marketing Campaign Load Formats 41

Designing Marketing Campaign Load Formats 41
Creating and Testing Campaign Load Formats 41
About Marketing Integration Objects 51

5 Installing and Configuring Siebel Email Marketing 61

Installing and Configuring Siebel Email Marketing 61
About Siebel Email Marketing 61
About Installing and Configuring Siebel Email Marketing 65
Architecture of Siebel Email Marketing 67
Requirements for Installing Email Marketing 68
Installing the Email Marketing Server 72
Roadmap for Configuring Email Marketing Daemons 77
Process of Configuring the Email Sending Daemon 78
Process of Configuring the Bounce Handler Daemon 85
Process of Configuring the Click Through Daemon 91
Encrypting Trackable URLs and Response Forms for Email Marketing 95
Configuring Email Marketing Components for HTTPS Communications 96
(Optional) Enabling TLS for Communications Between the Email Sending Daemon and the SMTP Server 98
(Optional) Verifying Email Marketing Component Configuration 99
Process of Testing the Email Marketing Components with Siebel Marketing 100
Administering Email Marketing 103
Configuring the Status of Email Addresses 114
Implementing Spam Scoring of Email Templates Using SpamAssassin 115
Authentication Mechanism of Email Marketing Server 117

6 Setting Up Web Marketing 119

Setting Up Web Marketing 119
About Siebel Web Marketing 119
About Web Marketing Web Site Visitors 119
Setting Up Siebel Web Marketing 121

7 Segmentation Migration Utility 137
Siebel Segmentation Migration Utility 137
Overview of the Siebel Segmentation Migration Utility 137
Prerequisites to Using the Siebel Segmentation Migration Utility 138
Prepare to Run the Siebel Segmentation Migration Utility 139
Run the Segmentation Migration Utility and Review the Results 142
Architecture of the Migration 144
Limitations of the Migration 147
Incremental Migration for Large Campaign Sets 147
Troubleshooting the Migration Results 148

8 Siebel CRM Integration with Oracle Unity 151
Siebel CRM Integration with Oracle Unity 151
Overview of Integration 151
Data Loading Process 151
Initial Setup and Configuration 153
Driver Parameters for the Siebel - Unity Data Export Engine 153
Defining Search Categories and Adding Categories to the Engine 156
About the CSV File Format 156
Troubleshooting the Siebel CRM Integration with Oracle Unity 157

9 Advanced Marketing Information for Administrators 159
Advanced Marketing Information for Administrators 159
Field Names for Marketing Integration Components 159
Extending Column Data to Promote Prospects to Contacts 171

10 Assigning Character Sets for the Email Marketing Server 173
Assigning Character Sets for the Email Marketing Server 173
Working with Character Sets for Email Marketing Servers 173

11 Logical Entity Relationships 185
Logical Entity Relationships 185
Logical Entity Relationships for Marketing Objects 185

12 Email Marketing Configuration Properties 187
Email Marketing Configuration Properties 187

New and Changed Properties in the esd.properties Configuration File 187
New and Changed Properties in the ctd.properties Configuration File 188
New and Changed Properties in the bhd.properties Configuration File 189

Get Help

Preface

This preface introduces information sources that can help you use the application and this guide.

Using Oracle Applications

To find guides for Oracle Applications, go to the Oracle Help Center at *https://docs.oracle.com/*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the *Oracle Accessibility Program website*.

Contacting Oracle

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit *My Oracle Support* or visit *Accessible Oracle Support* if you are hearing impaired.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an email to: *oracle_fusion_applications_help_ww_grp@oracle.com*.

1 What's New in This Release

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 26.9 Update

The following information lists the changes in this revision of the documentation to support this release of the software.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 26.9 Update

Topic	Description
Prepare the WSD Database	New topic. Explains the procedure for a new Web Survey Daemon (WSD) installation.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 26.8 Update

The following information lists the changes in this revision of the documentation to support this release of the software.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 26.8 Update

Topic	Description
Installing the Email Marketing Server	New topic. Explains the latest MDE installer workflow.
OCI Authentication Parameters	New topic. This topic describes changes to improve security by moving sensitive authentication data out of UI maintained driver parameters.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 26.7 Update

The following information lists the changes in this revision of the documentation to support this release of the software.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 26.7 Update

Topic	Description
Siebel Segmentation Migration Utility	New chapter. This chapter describes how to configure, run, and troubleshoot the Segmentation Migration Utility for migrating Siebel Marketing segmentation artifacts to Analysis-based artifacts in Oracle Analytics Server (OAS).
Installing the Email Marketing Server	Modified topic. This topic describes how to install the Email Marketing Server and the Email Marketing daemon components

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 25.11 Update

The following information lists the changes in this revision of the documentation to support this release of the software.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 25.11 Update

Topic	Description
Connecting Siebel Server to Business Intelligence Presentation Server	Modified topic. Describes how to integrate Oracle Analytics Server (OAS) with Siebel Marketing.
Confirming Host and Symbolic URL for the Marketing Module	Modified topic. Updated with new Name field values.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 24.9 Update

The following information lists the changes in this revision of the documentation to support this release of the software.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 24.9 Update

Topic	Description
Authentication Mechanism of Email Marketing Server	New topic. Addresses the issue of missing AUTH PLAIN mechanism used by major SMTP servers, it also provides a way to make use of OCI Email delivery Service for email campaign.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 22.4 Update

The following information lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
(Optional) Enabling TLS for Communications Between the Email Sending Daemon and the SMTP Server	New topic. You can now enable Transport Layer Security (TLS) for communications between the Email Sending Daemon and the SMTP server.
New and Changed Properties in the esd.properties Configuration File	Modified topic. The esd.smtp.starttls property has been added to the list of new properties in the esd.properties file.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 21.10 Update

The following information lists the changes in this revision of the documentation to support this release of the software.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 21.10 Update

Topic	Description
Siebel CRM Integration with Oracle Unity	New chapter. The Siebel CRM integration with Oracle Unity Customer Data Platform, which is also referred to here as Oracle Unity, is available as of Siebel CRM 21.10 Update.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 21.5 Update

The following information lists the changes in this revision of the documentation to support this release of the software.

What's New in Siebel Marketing Installation and Administration Guide, Siebel CRM 21.5 Update

Topic	Description
Encrypting Trackable URLs and Response Forms for Email Marketing	New topic. As of Siebel CRM 21.5 Update, Siebel eMarketing allows administrators to encrypt trackable URLs and response forms (Subscribe and Unsubscribe forms).

2 Installing and Administering Siebel Marketing

Installing and Administering Siebel Marketing

This chapter describes how to install and administer Oracle's Siebel Marketing product. It includes the following topics:

- *Installing Siebel Marketing*
- *Installing Marketing Contact List Import Using PL/SQL*
- *Enabling and Synchronizing Marketing Server Components*
- *Activating and Configuring Marketing Workflow Processes*
- *Activating and Registering Tasks for Marketing Activities*
- *Updating Marketing Connection Settings*
- *Enabling Automatic Responses for Opportunities and Orders*
- *About the Marketing Approval Process*
- *Configuring the Marketing Approval Values*
- *Load Balancing and Global Deployment of Siebel Marketing*
- *About Marketing Responsibilities and Access Groups*
- *Creating Marketing Seed Data*
- *Configuring Social Sharing Communities for Email Treatments*
- *Guidelines for Testing the Marketing Module in an Integrated Environment*
- *Monitoring Marketing System Tasks*

Installing Siebel Marketing

A Siebel Marketing installation has two main parts. You can install the following parts in any sequence:

- (Required) The Siebel Marketing operational application, including the Siebel Server.

  For more information about installing Siebel Server components, see *Siebel Installation Guide* . If you are upgrading an existing Marketing installation, see *Siebel Database Upgrade Guide* .
- (Optional) Oracle Business Intelligence Server components that provide segmentation and list generation capabilities. These components are referred to as the Marketing module. For more information about installing the Marketing module, see *Oracle Marketing Segmentation Guide* .

Installing Marketing Contact List Import Using PL/SQL

The following topics contain information about how to install and implement Marketing Contact List Import using PL/SQL.

Note: You must have installed the Siebel Database Server before you can implement this feature. For more information, see *Siebel Database Upgrade Guide* on the *Siebel Bookshelf* .

Preinstallation Tasks

Note the following important information before you install this feature:

- Make sure that the List Import Service Manager component for the Marketing Server component group has been enabled. For more information, see *Enabling Component Groups for Siebel Marketing*.
- The Mktg Master DB Import Process workflow process must have been enabled. For more information, see *Activating and Configuring Marketing Workflow Processes*.
- You must have installed the Siebel Database Server. For more information, see *Siebel Installation Guide* .

Setting System Preferences to Enable Contact List Import Using PL/SQL

Use the following procedure to set system preferences.

To set the system preferences

1. Navigate to Administration - Application, then System Preferences, and query for the MktgEnableDBImport and MktgIsDBOracle system preferences.
2. Make sure that the System Preference value is set to Y for both system preferences. If it is not, set the value to Y and log into the Siebel Marketing application again.

Activating the Mktg Master DB Import Process Workflow

Use the following procedure to activate the Mktg Master DB Import Process workflow.

To activate the Mktg Master DB Import Process workflow

Make sure the Mktg Master DB Import Process Workflow Process is active. For more information on how to activate Workflow Processes, see *Siebel Business Process Framework: Workflow Guide* .

Editing the CallPLSQL Business Service

Use the following procedure to edit the CallPLSQL business service.

To edit the CallPLSQL business service

1. Query for the CallPLSQL business service and click on the Business Service Server Script node.
2. Within the CallPLSQL business service, edit its script attribute as shown in the following example:

```
function CallPLSQL(Inputs, Outputs)
 {var vImptJobId;
 var cmdString;
 vImptJobId = Inputs.GetProperty("ImportJobId");
 Clib.sprintf(cmdString, "<absolute path of the sqlplus.exe file on the Siebel Server> <DB table owner
 username>/<DB table owner password>@<database table owner> @<absolute path of callplsql.sql file> %s",
 vImptJobId);
 Clib.system(cmdString);
 return (ContinueOperation);
 }
```

3. Edit the line highlighted in bold text to point to the:
   - sqlplus executable on the Siebel Server
   - User name (the name of the table owner) and password (the password of the database table owner)
   - @local_SID (database name in the .ini file) of the database you are connected to
   - The location of the callplsql.sql script

   For example, on a Solaris environment, the line would look like:

   ```
   /u01/app/oracle/product/11.2.0.3/dbhome_1/bin/sqlplus ORAPERF/ORAPERF@ORAPERF @/home/oracle/
   siebel/81114_23044_app4/siebsrvr/temp/callplsql.sql
   ```

   Where

   ```
   /u01/app/oracle/product/11.2.0.3/dbhome_1/bin/sqlplus
   ```

   is the path of the sqlplus executable

   ORAPERF/ORAPERF@ORAPERF are the connection credentials and

   @/home/oracle/siebel/81114_23044_app4/siebsrvr/temp/callplsql.sql is the path of the callplsql.sql script

   The callplsql.sql file is located in the <build folder>/ses>/dbsrvr/oracle/ and <build folder>/ses/siebsvr/sqltempl/ folders.

   > **Note:** The sqlplus executable is usually located in the ORACLE_HOME/bin folder where ORACLE_HOME is your environment variable that points to the Oracle home directory.

   For example, on the Linux platform:

   ```
   Clib.sprintf(cmdString,
   ```

```
"<absolute path of the sqlplus.exe on the siebel server> <DB table owner username>/<DB table owner
 password>@<database table owner> @<absolute path of mktg_listimp_callplsql.sql file> %s", vImptJobId);
```

The path to the callplsql.sql script is <absolute path to mktg_listimp_callplsql.sql>

In Siebel Tools, it would look like:

```
function CallPLSQL(Inputs, Outputs)
 {var vImptJobId;
 var cmdString;
 vImptJobId = Inputs.GetProperty("ImportJobId");
 Clib.sprintf(cmdString, "<absolute path of the sqlplus.exe file on the Siebel Server> <DB table owner
 username>/<DB table owner password>@<database table owner> @<absolute path of callplsql.sql file> %s",
 vImptJobId);
 Clib.system(cmdString);
 return (ContinueOperation);
 }
```

4. When you have finished editing the script attribute, deploy the business service to the Siebel runtime repository.

Creating the Database Directory and Uploading the File to the Database Server

Use the following procedure to create the IMPORT DIR database directory.

To create the IMPORT DIR database directory

1. On the database server, create a database directory using the following command:

```
SQL> CREATE OR REPLACE DIRECTORY IMPORT_DIR AS <DIR_PATH>';
```

For example: `CREATE OR REPLACE DIRECTORY IMPORT_DIR AS '/TMP';`

```
SQL> GRANT READ,WRITE ON DIRECTORY 'IMPORT_DIR' TO PUBLIC;
```

2. Verify that you have read/write permission for the IMPORTDIR database directory.
3. Upload the .txt file that contains the contact records to the folder on the database server that is mapped to the MPORT_DIR database directory (designated as '/TMP' in Step 1).
4. Give the IMPORT_DIR (/TMP) read/write permission for the TBLO user (the database table owner).
5. Give all the attached files read/write permission.
6. Grant CREATE/DROP table privileges for the database table owner.

Creating the PL/SQL Package on the Database Server Manually

1. Navigate to the /build/ses/dbsrvr/oracle folder, and untar the MktgListImportPkg.tar file to that directory.
2. Use the instructions in the Readme.txt file to manually create the PL/SQL package on the database server.

3. When the package has been successfully created on the database, navigate to the folder with the untarred folder and look for the mktg_listimp_pkg_body.log and mktg_listimp_pkg_spec.log files. If the file contains errors (such as TNS entry not valid… and so on), rerun the executable.

   If the mktg_listimp_pkg_body.log file contains the "Warning: Package Body created with compilation errors" error message, check with your administrator.

Importing a Contact List Using PL/SQL

1. Navigate to Administration Marketing, Import, and then Job Setup and create a new Import Job for Contact Import.
2. Set the following values to enable the Database Import button:
   - Main Object: Contact
   - Source Type: Text File
   - Import Mode: Import new records
   - File Selection: Use exact file name
   - Data Type: Comma Separated OR Other Delimiter like (|)
   - File Name: Click on the file browser and select the file that you uploaded to the database directory.
3. Navigate to Data Mapping, and specify the mapping, required fields, and exact match fields.
4. Click the Database Import button to import the contacts.
5. Navigate to Sitemap > Contacts > All Contacts, query for the imported contacts, and verify that they display.

Enabling the New List Import Functionality

When you have created the package, you need to enable the contacts list functionality. Use the following procedure to enable the new contacts list import functionality.

To enable the contacts list import functionality

1. Within the Siebel application, navigate to Administration - Application, then System Preferences.
2. Navigate to the MktgIsDBOracle and MktgEnableDBImport system preferences, and set the value to Y for each preference. The default value for these preferences is N.

Enabling and Synchronizing Marketing Server Components

During Siebel Server installation and configuration, you must enable the server components required by Siebel Marketing. Check the status of Siebel Server component groups using the Component Groups view in the Administration - Server Configuration screen. The Component Groups view is a list of installed Siebel Enterprise Server component groups with their associated components, servers, and tasks. For more information about enabling component groups, see *Siebel Installation Guide* and *Siebel System Administration Guide* .

Enabling Component Groups for Siebel Marketing

You must make sure component groups are enabled. The server assigned to the selected component group appears in the Servers view tab.

To enable component groups

1. Navigate to the Administration - Server Configuration screen, Enterprises, and then the Component Groups view.
2. In the Enterprise Servers list, select the appropriate server.
3. In the Enterprise Component Groups list, verify the required component groups have been enabled by performing the following steps:
   a. Locate each of the required component groups using the following table as a guide.
   b. Identify optional server components you might need to enable from the following list:
      - Assignment Manager. Used for campaign member assignment.
      - Data Quality Manager. Identifies duplicate contacts, accounts, and prospects when importing lists.
   c. If the Enable State field does not contain the value Enabled, select the component group, click the menu button, and choose Enable Component Group.

Group Name	Components	Description
CommMgmt	• Communications Outbound Manager • Communications Session Manager • Communications Configuration Manager	Communications Management. Delivers outbound mobile and fax offers for campaigns.
Enterprise Application Integration	EAI Object Manager	Transfers data between the Siebel database and other corporate data sources.
MktgOM	• Marketing Obj Mgr • eMarketing Obj Mgr • eEvents Obj Mgr	Marketing Component Group. Supports the user interface and business objects for the Marketing application.
Marketing Server	• List Import Service Manager	Used for Contact List Import Using PL/SQL
System	• Siebel Connection Broker • Server Manager • Server Request Broker	Supports general server management.
SystemAux	• Server Request Processor • File System Manager • Server Tables Cleanup	Supports management of auxiliary server components.
Workflow	• Workflow Process Manager • Workflow Process Batch Manager	Executes required marketing workflow processes.

Group Name	Components	Description
	• Workflow Action Agent • Workflow Recovery Manager • Workflow Monitor Agent • Generate Triggers	

Synchronizing Component Groups

After enabling server component groups, you must synchronize (enable) the server configuration.

To synchronize component groups

1. Navigate to the Administration - Server Configuration screen, Enterprises, and then the Component Groups view.
2. In the Enterprise Servers list, select the appropriate server.
3. Click the Synchronize view tab and click Synchronize.

You do not have to select any components in this view. The synchronization task can take a few minutes.

Stopping and Restarting Siebel Server

Siebel Server must be restarted each time synchronization occurs.

To restart Siebel Server process using Microsoft Windows

1. In the Microsoft Windows Control Panel, click the Services icon to open the Services window.
2. Locate Siebel Server and click Stop.
3. Click Start.

For details on stopping and restarting the Siebel Server system service on UNIX, see *Siebel System Administration Guide* .

Activating and Configuring Marketing Workflow Processes

The Siebel Marketing application uses a group of workflow processes to support various functions. This topic describes how to activate those workflow processes, and how to configure the Marketing Campaign Load workflow process.

Activating Workflow Processes

Before you can use Siebel Marketing, you must activate the workflow processes it requires.

To activate a workflow process

1. Before attempting to use Siebel Marketing, make sure that you activate version zero (0) of every workflow in the following table.

   Follow the instructions for deploying and activating workflows in *Siebel Business Process Framework: Workflow Guide* . When activated, the workflow process Status field contains a value of Active.
2. Restart the Workflow Process Manager Component or Siebel Server.

Workflow Name	Group	Description
Analytics Data Load	Marketing	Loads data through EAI for Customer Synchronization or Analytics Data Load requests.
Business Rules Workflow	Marketing	Invokes lead rules.
Campaign Copy	Marketing	Applies a campaign template.
Email Marketing - Forward to Friend	Marketing	Sends new emails to forward recipients.
Email Marketing - Update Status	Marketing	Updates the delivery status of an email offer.
Event Stage Execution Workflow	Marketing	Performs the scheduled execution of an event stage.
Generate Source Code	Marketing	Generates source codes for a campaign.
Import Marketing Contact	Marketing	Subprocess for Marketing Campaign Load.
Lead To Opty Conversion	Marketing	Converts a lead to an opportunity.
List Export	Marketing	Requests list files to be generated by the Marketing module.
List Export (Internal)	Marketing	Generates list files for sending email offers using basic mode.
List Purge	Marketing	Purges prospects from an internal list.
Marketing Approval Process	Marketing	Routes marketing approval items.
Marketing Campaign Launch	Marketing	Starts one or more campaign waves.
Marketing Campaign Load	Marketing	Loads segment or list members into a campaign.
Marketing Create Lead	Marketing	Creates leads.

Workflow Name	Group	Description
Marketing Create Response	Marketing	Creates responses.
Marketing Stage Execution	Marketing	Scheduled execution of a program stage.
Marketing Wave Launch	Marketing	Subprocess for Marketing Campaign Launch.
Mktg Import - Account Process	Marketing	Allows multi-threaded batch import of accounts from an external file to core Siebel CRM tables. This workflow is invoked from the Mktg Master Import Process workflow.
Mktg Import - Contact Process	Marketing	Allows multi-threaded batch import of contacts from an external file to core Siebel CRM tables. This workflow is invoked from the Mktg Master Import Process workflow.
Mktg Import File Processing	Marketing	Processes files for import. This workflow is invoked from the Mktg Master Import Process workflow.
Mktg Import - Lead Process	Marketing	Allows multi-threaded batch import of leads from an external file to core CRM tables. This workflow is invoked from the Mktg Master Import Process workflow.
Mktg Import - Prospect Process	Marketing	Allows multi-threaded batch import of prospects from an external file to core CRM tables. This workflow is invoked from the Mktg Master Import Process workflow.
Mktg Import - Response Process	Marketing	Allows multi-threaded batch import of responses from an external file to core Siebel CRM tables. This workflow is invoked from the Mktg Master Import Process workflow.
Mktg Master DB Import Process	Marketing	Required for Contact List Import using PL/SQL.
Mktg Master Import Process	Marketing	This workflow is the entry point for processing all import objects. The workflow launches processes by reading job details.
Post-Launch Custom Workflow	Marketing Custom Workflows	This is the custom workflow for post-launch tasks which can be executed immediately after launching a campaign. You can customize this workflow to add your own validation or business logic.

Workflow Name	Group	Description
Post-Load Custom Workflow	Marketing Custom Workflows	This is the custom workflow for post-load tasks which can be executed immediately after loading a campaign. You can customize this workflow to add your own validation or business logic.
Pre-Load Custom Workflow	Marketing Custom Workflows	This is the custom workflow for pre-load tasks which can be executed before the Campaign Load process. You can customize this workflow to add your own validation or business logic.
Program Copy	Marketing	Applies a program template.
Program Prioritization Workflow	Marketing	Manages cross-program prioritization while executing event triggers.
Promote Prospect (Many)	Marketing	Promotes multiple prospects to contacts.
Promote Prospect (Single)	Marketing	Promotes a single prospect to a contact.
Purge Staging Process	Marketing	Purges the staging tables used for the import process.
Response To Lead Conversion	Marketing	Converts a response to a lead.
Response To Opty Conversion	Marketing	Converts a response to an opportunity.

Configuring the Marketing Campaign Load Workflow Process

The Marketing Campaign Load workflow process is used to load a segment or list of target members into a campaign. After member information is loaded, the campaign can then be launched. Campaigns can either be launched all at once, in which case the campaign offer is distributed to all campaign target members at the same time, or it can be launched in waves, that is, at set distribution periods. When member records are loaded into a campaign, they are stamped with wave identifiers to indicate the campaign wave to which they are assigned.

To optimize the time it takes for campaigns to load, target member records are loaded in parallel. In addition, member records are updated with wave IDs in batches, instead of each record being updated sequentially.

You can configure the number of contacts to be included in each wave ID update batch, thereby allowing you to specify the value that is most appropriate for your implementation. To do this, you must configure the Marketing Campaign Load workflow process as described in the following procedure.

To configure the Marketing Campaign Load workflow process

1. In Siebel Tools, navigate to the Workflow Processes Object List Editor.
2. In the Workflow Processes list, query for the Marketing Campaign Load workflow process.

3. Select the Marketing Campaign Load record, then display the Properties Window by navigating to the Tools menu, choosing View, Windows, and then the Properties Window menu item.
4. Enter a value for the Bulk Update Batch Size input parameter.

   The default value is 10,000.

   The Bulk Update Batch Size parameter determines the number of contacts that are included in each batch of records that are updated with a wave ID at a time. When specifying a value for this parameter, consider both the size of the campaign and the database resources available.

   Each batch of records is processed sequentially.

Activating and Registering Tasks for Marketing Activities

Siebel Marketing includes tasks that streamline the procedures for creating and updating email treatments and landing sites. For information on using the Task UI application, see *Siebel Fundamentals* . To use these tasks, you must activate and assign privileges for the following tasks:

- Email Treatment: Create
- Email Treatment: Update
- Landing Site Create or Update
- Mktg Landing Site Task Based UI

For information about activating and assigning access privileges for tasks, see *Siebel Business Process Framework: Task UI Guide* .

Updating Marketing Connection Settings

After you complete the Oracle Business Intelligence installation, perform the following tasks:

- *Connecting Siebel Server to Business Intelligence Presentation Server*
- *Confirming Host and Symbolic URL for the Marketing Module*
- *Creating Permissions*
- *Setting Up the Marketing File System*
- *Setting Universal Time Option*

Connecting Siebel Server to Business Intelligence Presentation Server

For segmentation and list generation, you must connect the Siebel Marketing operational application on the Enterprise Siebel Server to Oracle Business Intelligence Presentation Server. To connect to Oracle Business Intelligence Presentation Server, you must change the User ID and Password fields to the default login for the Oracle Business

Intelligence Presentation Server that you plan to use. This login is the user ID that is used to authenticate requests to the Marketing module.

You must perform this setup to make sure that Siebel Server can communicate to Oracle Business Intelligence Server during program and campaign design, campaign load, list generation, and campaign launch. For example, when a user submits a request for campaign load or list generation, the requests to the Marketing module use this login for impersonation when the user's password is unavailable.

Impersonation is used to authenticate a user, allowing access to Oracle Business Intelligence Presentation Server when the user's password is unavailable. The default login is used to authenticate and create a session, and then the login ID is changed to the user ID of the person who submitted the request. Impersonation is essential to enforce appropriate visibility to Oracle Business Intelligence Web catalog objects, Business Intelligence metadata, and actual user data from various data sources, based on the User ID of the person who submitted the request.

Note: Passwords are encrypted for new server records. To encrypt the password for existing server records, select the record and reenter the password.

To change the user ID and password to the Oracle Business Intelligence Presentation Server login

1. Log in to the Marketing application as the administrator.
2. Navigate to the Administration - Marketing screen, then the Servers view.
3. In the Servers list, query for Default Analytics Web Server in the Name field.
   The Type field must be Siebel Analytics Web Server.
4. Navigate to the Detail list applet.
5. In the Detail list applet, click Authentication Service (SAWSessionServiceSoap) and perform the following steps:
   a. In the Outbound Web Services view, in the Service Ports list, change the first part of the address (default value is CHANGEME) to match the server name and domain of your Oracle Business Intelligence Presentation Server running the Marketing module.
      The address needs to be the full path name. For example, if your Marketing Server is named MarketingServer1, the full address for the JobManagementService is the following:
      `http://MarketingServer1/analytics-ws/saw.dll?SoapImpl=nQSessionService`
   b. Click the back button in the browser window.
6. In the Detail list applet, click Catalog Service (WebCatalogServiceSoap) and perform the following steps:
   a. In the Outbound Web Services view, in the Service Ports list, change the first part of the address (default value is CHANGEME) to match the server name and domain of your Siebel Business Intelligence Presentation Server running the Marketing module.
   b. Click the back button in the browser window.
7. In the Detail list applet, click Job Execution Service (JobManagementServiceSoap) and perform the following steps:
   Example:
   `http://MarketingServer1/analytics-ws/saw.dll?SoapImpl=webCatalogService`
   a. In the Outbound Web Services view, in the Service Ports list, change the first part of the address (default value is CHANGEME) to match the server name and domain of your Business Intelligence Presentation Server running the Marketing module.

b. Click the back button in the browser window.

```
http://MarketingServer1/analytics-ws/saw.dll?SoapImpl=jobManagementService
```

8. In the Detail list applet, click Analysis Export Views Service (AnalysisExportViewsServiceSoap) and perform the following steps:

   a. In the Outbound Web Services view, in the Service Ports list, change the first part of the address (default value is CHANGEME) to match the server name and domain of your Business Intelligence Presentation Server running the Marketing module.

      Example:
      ```
      http://MarketingServer1/analytics-ws/saw.dll?SoapImpl=analysisExportViewsService
      ```

   b. Click the back button in the browser window.

9. In the Detail list applet, click Xml View Service (XmlViewServiceSoap) and perform the following steps:

   a. In the Outbound Web Services view, in the Service Ports list, change the first part of the address (default value is CHANGEME) to match the server name and domain of your Business Intelligence Presentation Server running the Marketing module.

      Example:
      ```
      http://MarketingServer1/analytics-ws/saw.dll?SoapImpl=xmlViewService
      ```

   b. Click the back button in the browser window.

10. In the Detail list applet, click Report Editing Service (ReportEditingServiceSoap) and perform the following steps:

    a. In the Outbound Web Services view, in the Service Ports list, change the first part of the address (default value is CHANGEME) to match the server name and domain of your Business Intelligence Presentation Server running the Marketing module.

       Example:
       ```
       http://MarketingServer1/analytics-ws/saw.dll?SoapImpl=reportService
       ```

    b. Click the back button in the browser window.

11. Click Clear Cache.

    Restarting Siebel Server is not required for this change to be effective.

    Note: Both binary and repository upgrade is needed.

Confirming Host and Symbolic URL for the Marketing Module

Perform this task so that users can display the Segment Designer and Segment Tree Designer in the Segments screen tab and the List Format Designer in the Administration - Marketing screen tab.

To confirm the host and symbolic URL for the Marketing module

1. Log in to the Marketing application as the administrator.
2. Navigate to the Administration - Integration screen, then the WI Symbolic URL List view.
3. In the Administration - Integration screen, from the visibility filter, select Host Administration.

4. In the Host Administration list, query for NQHOST in the Virtual Name field and verify that a record appears where the Name field is [AnalyticsServerName].
5. In the Name field, change [AnalyticsServerName] to the Business Intelligence Presentation Server name that you plan to use.

   CAUTION: Be sure to change the Name column, not the Virtual Name column. Also, make sure that you have not included brackets in the name.

   Tip: This server name must be unique. For example, if you assign a server name to your Business Intelligence Presentation Server and try to use the same server name for Siebel Intelligence Dashboards, you receive a unique name error. To prevent this, you can append the domain to the server name (for example, server.example.com) or use the IP address in place of the name.

6. From the visibility filter, select Symbolic URL Administration.
7. In the Symbolic URL Administration list, query for Marketing Segmentation in the Web Application name field, and verify that records with the following Name field values appear:
   - MarketingEditListFormat
   - MarketingEditSegment
   - MarketingEditSegmentTree
   - MarketingListFormatsEntry
   - MarketingSegmentsEntry
   - MarketingSegmentTreesEntry
   - MarketingEditAnalysis
   - MarketingEditAnalysisCollection
8. Navigate to the Symbolic URL Arguments list, and verify that each Web application resulting from your query in the previous step has the correct nqUser and nqPassword argument.

   For each Web application, perform one of the following steps:

   a. To allow users to connect using their own username and login, perform the following steps:
      - In the Symbolic URL Arguments list, set the nqUser argument ArgumentType to Command and Argument Value to UseSiebelLoginId.
      - Set the nqPassword argument so that ArgumentType is set to Command and Argument Value to UseSiebelLoginPassword.

   b. In the Symbolic URL Arguments list, to connect using a fixed username and login for all users, perform the following steps:
      - Set the nqUser argument so that ArgumentType is set to Constant and Argument Value to the shared login for the Marketing module.
      - Set the nqPassword argument so that ArgumentType is set to Constant and Argument Value to the shared password for the Marketing module.

Note: After changing settings for any Web service or symbolic URLs, be sure to log out of the browser session and log in again for the changes to take effect.

Creating Permissions

In Oracle Business Intelligence Presentation Server, grant marketing permissions to the marketing administrators. For more information, see the Oracle Business Intelligence Enterprise Edition documentation.

Setting Up the Marketing File System

To prevent problems with campaign loading, make sure that the Business Intelligence Presentation Server service and Siebel Server service are running on an admin account that has read and write access to the directories used by the Marketing File System. In Windows, these services default to running under the local system account, which cannot access the Marketing File System because it is not a recognized user across the network.

For segmentation and list generation, access to the Marketing File System is shared between Siebel Server and Business Intelligence Presentation Server. If Siebel Server and Business Intelligence Presentation Server are installed on a combination of UNIX and Microsoft Windows operating systems (heterogeneous environment), then the Marketing File System must be configured for sharing in different environments.

Enable File Sharing in Mixed Environments

Siebel Marketing can be installed and operated in environments that use a combination of UNIX and Windows operating systems, but with some restrictions. The server components that use the Marketing File System must be on the same operating system. If they are not, then the difference in path name syntax prevents them from finding files. Business Intelligence Presentation Server must have visibility and write permissions to the Marketing File System. In a mixed (heterogeneous) environment, you might have to run a third-party application such as Samba to access the Marketing File System on different platforms.

Business Intelligence Presentation Server uses the MarketingFileSystem parameter to identify the location to which it writes out generated list files. This parameter on the Business Intelligence Presentation Server points to the same path as the Marketing File System parameter on the Marketing Component Group. However, the path syntax must correspond to the platform on which Business Intelligence Presentation Server is running.

For example, suppose you have the following configuration:

- Siebel Server and the Marketing File System run on UNIX. The Marketing File System is located at **`/export/home/filesystem`** on Siebel Server (sdcn1125s031).
- Business Intelligence Presentation Server is running on MS Windows.

You could export this file system path to be visible on MS Windows by running a third-party application such as Samba on the UNIX computer. In this example, the parameters would be set as shown in the following list:

- The Marketing File System parameter on Siebel Server could be set to **`/export/home/filesystem`**.
- The MarketingFileSystem configuration parameter on Business Intelligence Presentation Server must be set to **`\\`** *server* **`\export\home\filesystem`**.

The Communications and Workflow server components must run on the same operating system. If the Communications server component and the Workflow server component are not on the same operating system, you must change the Marketing File System server parameter for the Communications Outbound Manager server component. This allows the workflow process manager component to use the path syntax that corresponds to the operating system on which the Communication Outbound Manager is running.

Setting Universal Time Option

The time zone of the operating system on the Siebel Server computer can be set to any zone. However, the time must be synchronized with the database server. For example, if the time on the database server is 10:00 PM GMT, the Siebel Server computer would show a time of 2:00 PM (PST) or 4:00 PM (CST). To compensate for Siebel Servers and a database that are in different time zones, the Universal Time Option parameter is enabled to specify that server tasks are submitted in reference to a Universal Time. You must set this option to TRUE when deploying your Siebel application globally because global deployments typically have some Siebel Servers in a different time zone from the Siebel transactional database. If your implementation does not span time zones, this setting is optional. For more information, see *Siebel Global Deployment Guide* .

Note: If your Marketing Server requests do not run and remain in Queued status, then you might have a UTC issue. Repeat each step in this task to verify your settings.

To set the universal time option

1. Navigate to the Administration - Application screen, then the System Preference view.
2. In the System Preference Name field, query for Universal Time Coordinated, and perform one of the following steps:
   - To use the universal time option, in the System Preference Value field, set the value to TRUE.
   - To disable the universal time option, in the System Preference Value field, set the value to FALSE.
3. Verify that the operating system Clock and Time Zone on the Database Server computer is set to (GMT) Greenwich Mean Time.
4. Synchronize the time on the Siebel Server computer with the time on the database server computer.
5. Restart Siebel Server to make your change effective.

Enabling Automatic Responses for Opportunities and Orders

Responses can be created automatically when you associate a campaign with an order, associate a campaign as a source for an opportunity, or create an opportunity using the Create Oppty button in the Campaign screen. By default, the user properties for automatic response creation are disabled.

To allow automatic response creation in the Orders, Opportunities, and Campaigns screens, perform the following tasks in Siebel Tools:

- **Orders screen.** Set the User property Create Auto Response Service to Y in the Order Entry - Orders business component. When you enable this service, a response is created for the primary contact for the order whenever a campaign is associated with the order.
- **Opportunity screen**. Set the User property Create Auto Response Service to Y in the Opportunity business component. When you enable this service, a response is created for one of the opportunity contacts whenever a campaign is associated as a source with the opportunity.
- **Campaigns screen, Contacts and Prospects view tab.** Enable the Create Oppty button in this view tab by setting the User property Create Auto Response Service to Y in the Opportunity business component. When

you enable this service, a response is created automatically whenever the user clicks the Create Oppty button in the Campaign screen.

About the Marketing Approval Process

Siebel Marketing provides the ability to submit a variety of marketing items for review and approval using the Marketing approval process. Marketing plans, budget requests, programs, campaigns, event plans, and offers can be submitted from one employee to another by changing the Approval Status field on any of these objects.

The approval process is integrated with the Universal Inbox, so that marketing items that are submitted for review or approval, also appear in the Universal Inbox for the user who sent or received the item.

In the standard configuration, a change in the approval status opens a dialog box so the user can select the recipient employee and add a comment. When the user clicks Send, the Marketing Approval Process workflow creates a Universal Inbox Item task for the recipient employee and updates the approval history with the approval status value and any comments made by the recipient.

The business components for which the approval process is enabled are as follows:

- Campaign
- Direct Mail Offer
- Direct Sales Offer
- eEvents Parent Event
- Email Offer
- Fax Offer
- Indirect Offer
- Marketing Budget Requests
- Marketing Fund
- Marketing Plans
- Offer
- Phone Offer
- Program Container
- Web Offer
- Mobile Offer

Configuring the Marketing Approval Values

The standard Siebel Marketing configuration provides the following lists of values (LOVs) for the Marketing approval process:

- **Approval Status.** The values from this LOV appear in the Approval Status field that appears in the Marketing Plans, Budget Requests, Programs, Campaigns, Event Plans, and Offers screens.

- **Action.** The values from this LOV appear in the Action field in the Universal Inbox applets and the Approval view tab of the Marketing Plans, Budget Requests, Programs, Campaigns, Event Plans, and Offers screens. Action values are automatically mapped to Approval Status values. For example, when a user chooses an Approval Status value of Needs Revision in one record the Action value is updated to Request Revision in the corresponding Universal Inbox record.

The following table shows the preconfigured mapping for these values.

Approval Status	Action	Description
(blank)	Not Yet Submitted	This field is blank until a value is selected.
Approved	Approve	Approval Last Point. No further action is required by user.
Declined	Decline	Approval Last Point. No further action is required by user.
Needs Revision	Request Revision	Requires action by the user until an Approval Last Point is selected.
Submitted	Submit	Requires action by the user until an Approval Last Point is selected.

If required, you can add to the list of values using the Administration - Data screen. If you add a value that you intend to be an Approval Last Point, you must identify the new value as an Approval Last Point in Siebel Tools. These tasks are described in the following topics:

- *Adding a New Approval Value and Mapping the LOVs*
- *Identifying a New Approval Last Point Value*
- *Disabling the Approval Dialog Box*

Adding a New Approval Value and Mapping the LOVs

You can add a new approval value to the approval status and action LOVs by performing the steps in the following procedure.

To add a new approval value and map the LOVs

1. Navigate to the Administration - Data screen, then the List of Values view.
2. In the List of Values list, query for the MKTG_PLAN_APPR_TYPE list of values and perform the following steps:
   a. Click New and complete the fields.
   b. You must complete the Display Name, Language Name, and Order fields, and then select the Active flag.

   > **Note:** Use a unique value in the Order column in this list. This controls the sequence that the items appear in the list.

3. Query for the MKTG_UINBOX_ACTION_TYPE list of values and perform the following steps:
   a. Click New and complete the fields.

b. You must complete the Display Name, Language Name, and Order fields, and then select the Active flag.

Note: Set the order value in this list to control the sequence that the item appears in the list.

Identifying a New Approval Last Point Value

The following procedure describes how to identify a new Approval Last Point value.

To identify a new Approval Last Point value

1. Log in to Siebel Tools and query for the business component for each marketing approval item.
2. For each business component, select the Business Component User Properties.
3. Select the Approval Last Point user property.
4. Add the new value to the comma separated list.

CAUTION: Do not change the existing values (Declined and Approved). You must insert your value *your_new_value* as an additional value.

Disabling the Approval Dialog Box

If your organization does not need the Approval dialog box to appear when the Approval Status changes, you can disable it by performing the steps in the following procedure.

To disable the Approval dialog box

1. Log in to Siebel Tools.
2. Find the base Business Component for which you need to disable the popup.
3. Select the Business Component User Properties.
4. Select the Show Approval Popup user property and change the value to No.

Load Balancing and Global Deployment of Siebel Marketing

For information about load balancing server requests within the Siebel Enterprise, see *Siebel Installation Guide* and *Siebel System Administration Guide* . For information about global deployment, see also *Siebel Global Deployment Guide* .

Isolating Marketing Workflow Processes

Marketing workflow processes can be resource intensive during peak usage or large jobs. You might need to isolate marketing-related workflows from other workflow requests in the Enterprise by directing marketing requests to a specific instance of the Workflow Process Manager. If you need to do this for marketing workflow processes, you must

replicate the Workflow Process Manager component and change the enterprise parameter so that it points to the new component.

To create a new Marketing workflow process manager component

1. Navigate to the Administration - Server Configuration screen, Enterprises, then the Component Definitions view.
2. In the Component Definitions list, query for the Workflow Process Manager component.
3. From the list menu, choose Copy Record.
4. For the copied component, enter a new component name such as Workflow Process Manager - Mktg in the Name field.
5. Enter a new alias such as WfProcMgrMktg in the Alias field.
6. Change the Enable State field to Enable.
7. In the Enterprises screen, select the Parameters view.
8. In the Enterprise Parameters list, query for the parameter named Marketing Workflow Process Manager.
9. In the Value field, change the value to the alias name of the new component that you just created.
   For example if the component name is Workflow Process Manager - Mktg and the alias name is WfProcMgrMktg, then the enterprise parameter name is WfProcMgrMktg.

About Marketing Responsibilities and Access Groups

This topic contains the following information:

- *About Marketing Responsibilities*
- *Modifying Privileges for Marketing Access Groups*
- *Creating a New Marketing Access Group*
- *Assigning Marketing Users to Access Groups*

About Marketing Responsibilities

Siebel CRM provides a set of Marketing responsibilities that contain the full set of active views. These responsibilities are divided into core responsibilities and add-on responsibilities.

- **Core responsibilities.** Base user responsibilities that serve as a starting point for any Marketing user. Typically, a user has only one core Marketing responsibility from this list. The following is a list of core responsibilities:
  - Campaign Administrator
  - Campaign Agent
  - Events Manager
  - Marketing Executive
  - Marketing Planning Manager
- **Add-on responsibilities.** Support additional modules that certain users might need depending on their job description. These responsibilities are intended to be added to a core responsibility. They do not include common screens such as Accounts and Contacts because a core responsibility provides these screens. Because these are added to core responsibilities, you can assign a user multiple add-on responsibilities.
  The following is a list of add-on responsibilities:

- Marketing Admin
- Marketing Business Intelligence User
- Marketing Program Manager
- Segmentation User
- Web Marketing User

The Segmentation User responsibility is used for Business Intelligence integration. Any user who needs to access the Segment Designer or List Format designer must have this responsibility. Also, make sure that the same responsibility is associated to the segmentation catalog and other marketing server metadata in the Business Intelligence repository.

> **Tip:** If you create custom views, you can choose to create new add-on responsibilities for these views, instead of adding these views to the standard responsibilities. During future upgrades, this helps you identify custom views that you created.

Modifying Privileges for Marketing Access Groups

Siebel Marketing restricts the use of some buttons in the user interface (and their underlying methods) to those users assigned to Marketing access groups. This makes sure that unauthorized users cannot perform functions that they are not trained to perform. Marketing Access Groups can be used to restrict use of any button or menu item on any applet.

Siebel Marketing provides the following preconfigured access groups:

- Marketing Administrators
- Marketing Managers
- Marketing Users

The following information lists the functionality available to each access group.

Functionality	Marketing Administrators	Marketing Managers	Marketing Users
Analytics Data Load (Activate and Deactivate)	Yes	No	No
Generate Output List	Yes	Yes	Yes
Generate Source Code	Yes	Yes	No
Launch Campaign	Yes	Yes	Yes
Launch Wave	Yes	Yes	Yes
Load Campaign	Yes	Yes	Yes
Load History Applet, Delete Record	Yes	No	No

Functionality	Marketing Administrators	Marketing Managers	Marketing Users
Purge Load	Yes	No	No
Run Assignment Manager	Yes	No	No
Save As Template	Yes	Yes	No
Suspend Wave	Yes	Yes	Yes
System Task List Applet, Delete Record	Yes	No	No
Test Offer	Yes	Yes	Yes

To modify the Marketing access privileges for an applet

1. Log in to Siebel Tools.
2. In the Object Explorer, select Applets.
3. Select the applet, such as Campaign Execution Status List Applet, for which you need to modify access.
4. In the Applet User Properties, in the Marketing Access Group user property, add or delete access groups. Use the following syntax for each user property entry:

Name	Value
Marketing Access Group *n*	"*method name*", "*access group 1*", "*access group 2*", and so on

Note: N is an integer such as 0, 1, 2, and so on, for each method to be restricted.

For example, the Campaign Execution Status List Applet has the user properties shown in the following table in the standard repository.

Name	Value
Marketing Access Group 0	"PromptPurgeLoad", "Marketing Administrators"
Marketing Access Group 1	"PromptSuspendWave", "Marketing Administrators", "Marketing Managers"
Marketing Access Group 2	"PromptLaunchWave", "Marketing Administrators", "Marketing Managers"

5. To add or remove an access group for a specific method, add or remove the access group name from the comma separated list in the user properties.

Creating a New Marketing Access Group

If required, you can create additional access groups for your organization as described in the following procedure.

To create a new Marketing access group

1. Navigate to the Administration - Groups screen, then the Access Groups view.
2. In the Access Groups list, click New.
3. In the new record, enter an Access Group name and, from the Type list, select Access Group.
4. Review the applets in the application for which you need to enable or disable a button, menu item, or other control that invokes a method.
5. For each applet, modify the applet user properties to refer to the new access group.

Assigning Marketing Users to Access Groups

You must perform this setup task to make sure your Marketing users have access to the appropriate functionality. You assign the users to access groups based on the position of each user. For more information about access groups, see *Siebel Security Guide* .

To assign Marketing users to access groups

1. Navigate to the Administration - Group screen, then the Access Groups view.
2. In the Access Groups list, in the Name field, query for Marketing*.

   Note: At least two access groups (Marketing Administrators and Marketing Managers) appear.

3. In the Access Groups list, select Marketing Administrators.
4. In the Party list, add the positions for your administrators.

   For example, Siebel Administrator and Marketing Administrator positions.
5. In the Access Groups list, select Marketing Managers.
6. In the Party list, add the positions for your marketing managers.

   For example, Marketing Analysts, Program Managers, and so on.

   Note: You must add positions as access group members, not User List or Organization.

7. Restart the client for this change to be effective.

Creating Marketing Seed Data

After you install the Marketing application, there are some optional seed data that can be created to support various business processes. This topic contains the following tasks:

- *Creating Marketing Regions*
- *Creating Marketing Activity Templates*
- *Creating and Using Marketing Activity Plans*

Creating Marketing Regions

Marketing regions provide a way to organize the marketing plans and tactics in your organization. Additionally, using regions can generate more detailed Marketing reports and rollups in Oracle Business Intelligence Publisher.

You can define marketing regions according to any set of parent child relationships that you require. Although there is no limit to the number of layers you can create in your hierarchy, marketing Business Intelligence only supports a hierarchy that is a maximum of 10 layers deep. You can implement a marketing region hierarchy by making one region the child of another region. The following example shows a simple regional hierarchy:

- Worldwide
  - North America
  - EMEA
  - Latin America
  - Asia Pacific

To create marketing regions

1. Navigate to the Administration - Location screen, then the Regions view.
2. In the Regions list, create a new record.
3. Enter the Region name and description.
4. Be sure to set the Type as Marketing Region.
5. If this region is a child of another region, select the Parent Region in the Parent Region field.
6. Save the record.
7. Repeat step 2 through step 6 for each region in the hierarchy.

Creating Marketing Activity Templates

Activity Templates provide a convenient way for users to quickly assign a set of milestones and activities to a program or campaign. For instructions about how to create activity templates, see *Siebel Applications Administration Guide* . For instructions about updating Activity Templates from prior releases, see the activity plan topic in *Siebel Database Upgrade Guide* .

> **Note:** When you create Marketing activity templates, be sure to set the type of the template to the name of the main marketing business components, for example Program Container and Campaign.

Creating and Using Marketing Activity Plans

Activity Plans associate preconfigured planning and milestone activities and tasks with a template (activity plan). Users can assign the templates to marketing programs and campaigns. This creates one or more activities that are associated with a campaign or a program.

Note: Activities are not created for contact records that are loaded into a campaign.

Activity Plans can be designed to help you plan the marketing program or campaign or execute it. Before you link an activity plan to your campaign, you must create activity templates or customize existing templates to reflect your business process and needs. Use templates to define a generic set of activities that can be reused.

For example, a marketing department production manager can design an activity plan template called Direct Mail that contains regularly scheduled campaign planning activities (meetings with creative or budgetary staff) and start tasks (such as generating an export list according to segmentation criteria). Using the Campaign Activity Plans view the manager can associate the activity plan template to the current campaign and then assign resources, define priorities and status and so on to each predefined task, adding comments where necessary.

If your marketing program or campaign has a combination of planning and start activities, you can create two activity plans, one for planning and one for execution tasks, and assign them both to the program or campaign.

Configuring Social Sharing Communities for Email Treatments

Siebel Marketing provides functionality that allows you to use social media channels to complement and enhance your marketing campaigns. There are two aspects to this functionality:

- Social media channels can be integrated into marketing campaigns. When defining email treatments for a campaign, you can choose to embed Social Sharing URLs in the email treatment. Inserting a Social Sharing URL in an email treatment allows customers who are targeted in the campaign to share the URL with their social networks directly from the email offer.
- Siebel Marketing can be integrated with Oracle Social Relationship Management cloud services using the CreateLeads Web service and the GetCampaigns Web service. These Web services allow you to capture leads for a campaign based on an individual's social interactions, to capture social media post data for the new leads, and to make Siebel Marketing campaign data available to Oracle Social Relationship Management.

For information on the CreateLeads and GetCampaigns Web services, see *Siebel CRM Web Services Reference* .

You can configure the communities to which users can share URLs from email treatments by adding new communities or deleting existing communities, as described in the following procedure.

To configure social sharing communities in email treatments

1. Navigate to the plugin.js file in the `eapps/webeditor/plugins/mergefieldsblock` directory.
2. Using a text editor, open the plugin.js file and edit it as appropriate to either remove or add social networking sites.

By default, customers can share Social Sharing URLs with the following social communities:

- Facebook©
- Twitter©
- LinkedIn©
- Tumblr©
- Pinterest©
- GooglePlus©
- Blogger©
- MySpace©
- Delicious©

For information on using Social Sharing URLs in email treatments, see the chapter on creating and using offers and treatments in *Siebel Marketing User Guide* .

Guidelines for Testing the Marketing Module in an Integrated Environment

To deploy the Marketing module for segmentation and list generation, you must install, configure, and test your integrated environment.

- **Installation.** You must install the following products:
  - Oracle Business Intelligence Presentation Server and Oracle Business Intelligence Server. For more information, see *Oracle Business Intelligence Platform Installation and Configuration Guide*.
  - Siebel Enterprise Server. For more information, see *Siebel Installation Guide* .
- **Configuration.** After installing, you must configure segmentation metadata, list export metadata, and create example list formats. For information about configuring segmentation and list export metadata, see the Oracle Business Intelligence Enterprise Edition documentation.
- **Testing.** Test the Marketing application and module as follows:
  - After installing the Marketing application and Marketing module, conduct a system test to verify that all components are correctly activated.
  - After you install and configure Siebel Marketing and create segmentation metadata, test campaign load.

The following topics describe tasks that help you test a Marketing integrated environment:

- *Testing the Symbolic URL*
- *Testing the Web Services Integration*
- *Testing Navigation Links to the Segment Designer Page*
- *Testing the Campaign Load*

Testing the Symbolic URL

The following procedure describes how to verify that the Symbolic URL is configured correctly.

To test the Symbolic URL integration

1. In Siebel Marketing, click the Segments screen tab.
2. In the Segments screen, click the Segment Designer link.
   If the Segment Designer page does not appear, perform step 5.
3. In the Segments screen, click the Segment Tree Designer link.
   If the Segment Tree Designer page does not appear, perform step 5.
4. Navigate to the Administration - Marketing screen, then the List Formats view.
   If the List Format Designer page does not appear, perform step 5.
5. If any of the previous steps do not obtain the specified results or you receive an error, navigate to the Administration - Integration screen, then the WI Symbolic URL List view and check the Host Administration settings.

Testing the Web Services Integration

The following procedure describes how to test the Web services integration.

To test the Web Services integration

1. In Siebel Marketing, click the Segments screen tab.
2. In the Segments screen, click the Segment Designer link.
3. In the Segment Designer, create a test segment and save the segment in the Web Catalog.
   For more information about creating segments, see *Siebel Marketing User Guide* .
4. Navigate to the Campaign screen and perform the following steps:
   a. In the My Campaigns list, click New.
   b. In the record, enter a campaign name, and save the record.
   c. Click the Campaign name and click the Design view tab.
5. In the Design view, perform the following steps:
   a. Click the Segments/Lists link.
   b. In the Segments/Lists list, click Add Segment.
   c. In the Previously Used Segments dialog box, click Choose a new Segment.
   d. In the next Previously Used Segments dialog box, click the Folder Location select button to display the following folders in the Oracle Business Intelligence Web Catalog:
      - Your user name
      - Shared
6. If you receive an error, perform the following steps:
   a. Navigate to the Administration - Marketing screen, then the Servers view.
   b. Verify the following values:

- The Marketing Server definition has the correct Authentication user and password.
- All three Web Services have the correct Business Intelligence Presentation Server name in the address.

Testing Navigation Links to the Segment Designer Page

The following procedure describes how to verify that links to the Segment Designer page are correct.

To test navigation links to the Segment Designer page

1. Navigate to the Campaigns screen.
2. In the My Campaigns list, click the name of your test campaign.
3. In the Campaign Details form, click the Design view tab.
4. In the Design view, click the Segments/Lists link.
5. Add a segment to associate it with a campaign.
6. Click the name of the segment.
   The Segment Designer appears with your segment open for editing.
7. If you receive an error, verify the following:
   a. Navigate to the Administration - Marketing screen, then the Servers view, and verify that the Marketing Server definition has three parameters for the navigation views.
   b. Log in to an Business Intelligence URL directly, and verify that the segment request exists and can be opened successfully.

Testing the Campaign Load

The following procedure describes how to test the campaign load process.

To test the campaign load

1. In Siebel Marketing, click the Segments screen tab and perform the following steps:
   a. In the Segments screen, click the Segment Designer link.
   b. In the Segment Designer, create a test segment and save the segment in the Web Catalog.
      For more information about creating segments, see *Siebel Marketing User Guide* .
   c. Click the Advanced Options tab and verify that a valid Campaign Load List Format is associated with the segment.
2. Navigate to the Campaign screen and create a test campaign by performing the following steps:
   a. In the My Campaigns list, click New.
   b. In the record, enter a campaign name, and save the record.
   c. Click the Campaign name and click the Design view tab.
3. In the Design tab, perform the following steps:
   a. Click the Offers link.
   b. In the Offers list, click New.

c. In the Add Offer dialog box, choose a test offer and click OK.
d. In the Treatments list at the end of the view, click New.
e. In the Pick Treatment list, choose a test treatment.

4. In the Design view, perform the following steps:

a. Click the Segments/Lists link.
b. In the Segments/Lists list, click Add Segment.
c. In the Previously Used Segments dialog box, click Choose a new Segment.
d. Locate and select your test segment.

5. Click OK twice to associate the segment with the campaign.

   In the Allocation matrix, a check box appears for each treatment you associated in step 3.

a. Check the check box.
b. Click Save.

6. In the Campaign form, click Menu and choose Load Campaign.
7. In the Load Campaign dialog box, click OK to submit the load request.
8. Click the Execute view tab and select the System Tasks link.
9. In the System Tasks list, verify that the campaign loads successfully.

Monitoring Marketing System Tasks

The Marketing Application provides a set of views so users and administrators can monitor the progress of any marketing-specific server process. Each marketing-specific job is referred to as a system task. The following table contains a list of where to locate these jobs.

Location	Purpose
Navigate to the Administration - Marketing screen, then the System Tasks view.	Displays marketing system tasks for all users, including import tasks.
Navigate to the Campaign Management screen, Execute, and then the System Tasks view.	Displays marketing system tasks for the selected campaign.
Navigate to the Administration - Marketing screen, then the Import view.	Displays import jobs and their status.
Navigate to the Programs screen, Execute, and then the System Tasks view.	Displays marketing system tasks for the selected program and related campaigns.

Each system task provides high-level logging details that track the successful completion or any errors in each major step of the task. Because the task log is intended to be used by all users, the System Task view does not provide low-level logging details.

If an administrative user needs further details on a marketing task, each step in the task log provides the Siebel Server name, log file (indicating the server component), and Task ID. The administrator can use this information to locate the log file or the logging details under Server Administration.

For Siebel Marketing, system tasks display information for the following tasks:

- Analytics Data Load
- Campaign Launch
- Campaign Load
- Generate Source Codes
- List Export
- List Import
- Stage Execution
- Wave Launch

If you get the error message `Unable to connect to gateway server` when starting a Siebel Marketing task, then you might have the Docked parameter in the CFG file set to TRUE. To correct the problem, quit Siebel Marketing, set the Docked parameter to FALSE, and restart.

3 Creating Source Code and Vendor Profiles

Creating Source Code and Vendor Profiles

This chapter describes how to create source codes and vendor profiles. It includes the following topics:

- *About Source Codes*
- *Creating Source Code Formats*
- *Setting Up Vendor Profiles*

About Source Codes

Siebel Marketing uses source code capabilities with exported lists, for proper campaign tracking and reporting. The source code format can include encoded information about each customer or prospect based on any business component field. You can also define and maintain multiple formats for use in different campaign scenarios. After you start the campaign, the source codes assigned to each customer can be captured as part of the response and decoded for closed-loop tracking.

Siebel Marketing supports the assignment of source codes to each contact in a campaign. A source code appears to the customer as a seemingly indecipherable mix of alphanumeric characters that typically can be found on a mailer. Marketers, however, can gather a wealth of information about the demographic makeup of the consumer responding to an offer, as well as the particulars of the marketing campaign that delivered the promotion, by decoding the source code.

In a typical scenario, a customer contacts a company's call center to place an order for merchandise or ask questions about an item advertised in a catalog. During the first few minutes of the call, the representative asks the customer to read the code that appears on the catalog's label or order form. Depending on the information received, the call center representative can be authorized to present to the customer a better offer on the merchandise than the one in the catalog.

The call center representative can also capture the customer's source code to make sure that the marketing organization can make the link that this customer is responding to a direct marketing campaign.

In Siebel Marketing, a unique source code is assigned to a marketing program element each time an element is created. Marketing program elements include program, stages, segments, campaigns, and waves.

> **Note:** When marketing programs, segments, and campaigns are created, Siebel Marketing assigns a unique source code value to new program stages, segments, and campaigns. Although the stage or campaign's name might be duplicated, the source code field is the actual identifier. If you change the assigned source code to something more meaningful to you, make sure it is a unique value.

These individual source code components are concatenated and grouped according to the sequence and format that you specify in the Source Code Formats view to help you track your marketing program and analyze response to campaigns and offers. The source code format can contain up to 75 characters and can optionally include other tracking information.

When you load a campaign or generate source codes manually, the source code for each contact is assembled, based on the characteristics associated with the target contact in the marketing program. For example, the source code for a contact who is in Segment 1 and is in the first wave of Campaign 1 can be different from the source code for a contact who is in Segment 3 and the second wave of Campaign 1.

In addition, you can tailor the contact information that is generated for the distribution list to suit your business requirements. At minimum, a list has a contact's name or some other identifier and a source code. It can also contain an address (if you are mailing to the contact), phone number (if you are calling the contact), email address, account number, and so on.

Creating Source Code Formats

The Source Code Formats view defines a source code format, specifies the individual components that are included, and determines how these components are arranged or sequenced. After creating a source code format, you can use the source code in the following ways:

- Include in an export list.
- Embed as a personalization element in an email offer.
- As input in the customer-facing Web Marketing home page (in the applet named *Do you have another offer?*).
- As a direct input to a response from any of the Response views.

The Source Code Formats list shows available source code formats. The All Components list displays details of the source code format selected in the list and is used to create the structure of the source code grouping, or format. The All Components list contains the computed length of each source code (maximum of 75 characters).

By clicking Move Up or Move Down, you can rearrange components in the format. If you delete components (for example, component 2 and component 4 of 5), click the menu button and choose Resequence to reorder the remaining components before saving the record.

Creating Source Code Formats

The following procedure describes how to create source code formats.

To create source code formats

1. Navigate to the Administration - Marketing screen, then the Source Code Formats view.
2. In the Source Code Formats list, create a new record.
3. Enter a name and a description for the Source Code Format.
4. When you save the source code format, the new format appears in the Source Code Formats list.

Defining Source Code Format Components

The following procedure describes how to define source code formats.

To define source code format components

1. Navigate to the Administration - Marketing screen, then the Source Code Formats view.
2. In the Source Code Formats list, select a source code format.

3. In the All Components list, create a new record.
4. Complete the fields for the component, using the following information as a guide.

Field	Description
Attribute	Shows the available fields from the business component. For a list of available business components, see the Type row in this table. The Attribute MLOV (Multiple List of Values) column in the Source Code formats view records the language-independent code for each Attribute. The language independent code must exactly match the field name in Siebel Tools. Do not attempt to add extension fields that exceed 30 characters. The displayed value is limited to 75 characters.
Constant Value	Specifies an optional constant value to be inserted in the source code. This is editable only when the Type field is set to Constant.
Default Value	Inserted when the input value is NULL. You can provide a default value for any source code component. For example, if you included Campaign Member Country, you could insert a value for any members with no Country in their profile.
Sequence	Sequence determines the position of the code component in the source code format. Sequence is automatically set when source code components are added to the format. Use Move Up, Move Down or Resequence to adjust the order.
Type	The Type field shows the business component used as the source of the field. The supported components are Campaign, Campaign Member, Offer, Program, Segment, Stage, and Wave. When you select one of these types, you must also select the Attribute. The Type field also supports inserting a Constant, Numeric Sequence, or Alphanumeric Sequence. You cannot use both a Numeric Sequence and an Alphanumeric Sequence in the same source code. o Constant. A fixed value that is the same for all campaign members. You can have more than one constant in the source code format. For example, you can use a constant to insert a spacing character such as a hyphen (-). o Numeric Sequence. Inserts a running count in the source code for each campaign member in a campaign wave. The value uses a standard integer sequence of 1,2,3...9,10,11....N. o Alphanumeric Sequence. Similar to Numeric Sequence, except that the values include integers and letters of the alphabet. For example, 1,2,3....9,A,B,C.....,X,Y,Z,10,11, and so on. The source code generator adds a prefix of zeros (0) to the numeric sequence and alphanumeric sequence based on the width of the field. For example, if the width is 4, the values are 0001, 0002, 0003, and so on.
Width	The width of the source code component is automatically added. However, you can change the width. The maximum width for the entire source code format is 75 characters. The following is a list of examples:

Field	Description
	○ If the source code width for a component is 16 characters and you specify 6 as the width in this field, the individual source code for the component is truncated to the first six characters. ○ If the component's code has a width of 10 characters, and you specify 20 as the width, 10 blank spaces appear in your source code format.

5. Save the component.

   Note: To add more components, repeat Step 3 through Step 5, one row at a time.

6. Adjust the sequence of the components by clicking Move Up and Move Down.

   To reorder deleted components before saving the changes, click the menu button and choose Resequence.

Setting Up Vendor Profiles

Vendors are external partners that receive lists of target contacts when you start a campaign. Your campaign strategy might call for vendors such as call centers, fulfillment centers, and printers to split lists of contacts. Some customers would receive a telephone call, others a direct mail offer, and a third group would receive promotion samples.

Use the Vendors view to create a library of vendor profiles for your marketing programs. Vendors include telemarketers, fulfillment houses, and any other company you retain to help you with campaign distribution.

Vendor Tasks

When you start a marketing campaign, the generated output list is sent to the specified vendor using the vendor's preferred distribution method and communications protocol (File Transfer Protocol, email, and so on).

Before creating a vendor record, make sure the following tasks have been performed:

- **Create Export List Formats.** Determine what format the vendor prefers for the generated distribution lists. For example, does the vendor want the list to contain a header or does the vendor prefer ASCII (default) or fixed-width output? Then, create an output file layout tailored to the vendor's preferences.

  You are asked to provide the default export list format when creating the vendor profile. For more information, see *Oracle Marketing Segmentation Guide*.

- **Determine Distribution Method and Create Distribution Profile.** As you are creating the vendor record, you must select a distribution method and a distribution (communications) profile for the method. Set up distribution profiles that reflect each vendor's requirements.

  For example, if your vendor prefers to receive list files using File Transfer Protocol (FTP), you would set up a communications profile for that vendor containing information about HostName, IP Address, Password, and so

on. Communications profiles are set up using the Communications Administration screen's Communications Drivers and Profiles view.
If the list files are sent to the vendor attached to email, set up a communications profile for email, and verify that the vendor contact has provided an email address. For more details, see *Defining Distribution Profiles for Vendors*.
If someone in your marketing department receives the distribution list, rather than an outside vendor, a vendor record and communications profile that includes the team member's email address must be set up.

Defining Vendors

Use the following procedure to set up profiles for the third-party vendors who receive the distribution list of contacts. If your marketing department is the list recipient, set up a vendor profile using the marketing department contact as the vendor.

To define vendors and assign list distribution methods

1. Navigate to the Administration - Marketing screen, then the Vendors view.
2. In the Vendors list, create a new record.
3. Complete the fields for the vendor definition, using the following table as a guide, and save the record.

> **Note:** If one vendor can handle multiple list formats, such as a direct mail format and a telWeb Marketing format, create separate vendor profiles for each type. For example, the profiles can be named Ace Fulfillment: Direct Mail, and Ace Fulfillment: TelWeb Marketing.

Field	Comment
Contact Name	Select the contact name, if it exists. If the contact does not appear in the list, add the relevant information using the All Contacts list. By default, the server looks for the email address in the EMAIL_ADDR column of the S_CONTACT table. If you store the email address in a different column, see *Siebel CTI Administration Guide* to configure the Recipient Email Address field.
Distribution Method	Choose the method that describes how the distribution list is sent to the vendor.
Distribution Profile	Choose from the list of predefined distribution profiles. Distribution Profiles are defined using the Administration - Communications screen, then the Communications Drivers and Profiles view.
Email Address	The email address for the vendor is populated if it was defined for the selected vendor contact. You cannot add the email address in this view. If you plan to send a generated list to the vendor using email, you must add the email address for the contact in the All Contacts or My Contacts view.

Defining Distribution Profiles for Vendors

Use the Communication Administration screen's Drivers and Profiles view to define communications profiles for email, fax, and FTP distribution of lists to vendors. Output file layouts and vendor profiles must be defined for all types of lists. If you are using email or FTP, you must also define Email Address, Distribution Method, and Distribution Profile in the Vendor profile. For more information about using delivery profiles, see *Siebel Marketing User Guide* .

Siebel Marketing provides default drivers in its library that can be modified for use when sending files to a vendor. An administrator can create distribution profiles for each of these driver types that override the default parameters for that driver. For more information about communications drivers and profiles, see *Siebel CTI Administration Guide* .

4 Designing Marketing Campaign Load Formats

Designing Marketing Campaign Load Formats

This chapter describes how to design marketing campaign load formats. It includes the following topics:

- *Creating and Testing Campaign Load Formats*
- *About Marketing Integration Objects*

Creating and Testing Campaign Load Formats

Campaign load formats define the way campaign-related data is copied from a marketing data source into the Siebel transactional database for launching a campaign. You must define campaign load formats for your marketing data sources before you can use Siebel Enterprise Application Integration (EAI) technology to import this information. For example, contact information such as first and last name, phone number, and email address can be brought into the Siebel database during campaign load only if you define campaign load formats for this data. The Campaign Load workflow process is used to manage the load process.

For information about creating a campaign load format for the Siebel Data Warehouse, see *Examples of Recommended Campaign Load Mappings*.

This topic contains the following information:

- *Creating Campaign Load Formats*
- *Example of Creating a Response Load Format*
- *Example of Creating a Lead Load Format*
- *Testing Campaign Load Formats*

Creating Campaign Load Formats

Before you begin creating campaign load formats, make sure the subject area in the Business Intelligence Administration Tool includes the required fields to load new customers and execute your campaigns. For example, if you are loading contact data, you must verify that the Subject Area used for the Campaign Load Format includes Contact First Name, Middle Name, Last Name, and so on. For more information about creating Subject Areas for list formats, see the Oracle Business Intelligence Enterprise Edition documentation.

Creating campaign load formats requires that you complete the following tasks:

- *Creating a Campaign Load Format and Adding Columns*
- *Enabling System Data Expressions for Required Columns*
- *Assigning Integration IDs*
- *Requalifying List Results Against Original Criteria*

- *Setting Options, Headers, and Footers for Campaign Load Formats*

Creating a Campaign Load Format and Adding Columns

Campaign load formats have columns that are always required, regardless of the type of customer data being loaded, for example, contacts, accounts, or prospects. The following procedure describes how to create a campaign load format and add columns to the format.

To create a campaign load format and add columns

1. Using one of the following methods, navigate to the List Designer start page:
    - In the Siebel Marketing application, navigate to the Administration - Marketing screen, then the List Formats view.
    - If you log in to the Marketing module directly, click the Marketing screen tab and then click Create a List Format.
2. From the list of Subject Areas on the right, select a subject area that includes the required columns for your campaign load format.

    Subject areas are available for this purpose, including the following:

    - Campaign Load - Contacts
    - Campaign Load - Accounts
    - Campaign Load - Prospects

    > **Note:** Your administrator might have added additional subject areas.

3. Expand the folders in the selection panel and click each column name to add it to the format.
4. Verify that you have included the required columns for each integration object and integration component, based on the type of party being loaded (contacts, accounts, or prospects).

    > **Note:** The column label must exactly match the field name of the integration component in the Siebel runtime repository. For information about required integration component fields, see *Enabling and Synchronizing Marketing Server Components* and *Field Names for Marketing Integration Components*.

    a. To rename a column label that does not exactly match the field name of the integration component, click the properties button.
    b. Select the Custom Headings option.

    If you use one of the standard subject areas listed in Step 2, then the column names match the field names in the integration components in the Siebel enterprise application.

    c. Enter the necessary table and column heading.

    The table heading must match the integration component name and the column heading must match the field name.

5. Select the following required columns to add them to the campaign load format:
   a. From the Contact folder, add the Person UId column.
   b. From the Campaign Contact folder, add the following columns: Campaign Id, Segment Id, Load Number, Token Number, Scalability Batch Number, and Treatment Id.

      Note: The Treatment Id column is an external key, and is now a required column. Depending on your upgrade history and system configuration, your current list formats might not include this column. If this is the case, add a System Data Expression for Treatment Id to the Business Intelligence Web configuration files (see *Oracle Marketing Segmentation Guide*) and add this expression as a column to your Campaign Load list formats (see *Creating and Testing Campaign Load Formats*).

The following table shows the mappings used in the preconfigured reports.

Type of Party	Key	Party Id	Map to this Column Id
Contacts	Key 1	Contact Id	Contact.ROW_ID
Accounts	Key 1	Contact Id	Contact.ROW_ID
Accounts	Key 2	Account Id	Account.ROW_ID
Prospects	Key 3	Prospect Id	Prospect.ROW_ID

Enabling System Data Expressions for Required Columns

Several of the Campaign Contact columns required for the campaign load format must be populated with values that are determined by the list generation process at run time. To accomplish this, you set up the Campaign Contact columns to use system data expressions. The following procedure describes this task.

To enable system data expressions for required columns

1. Click the properties button on the Campaign Contact column.
2. In the dialog box, first click the Custom Headings check box.

   This makes sure the table and column name are not changed when you modify the formula in the next step.
3. Clear the current formula from the Column Formula box.
4. Place your cursor in the Column Formula box, then click the Available System Data link.
5. Select the appropriate system data expression from the values in the following table.

Column	Corresponding System Data Expression
Campaign Id	Campaign Id
Load Number	Load Number
Scalability Batch Number	Email Batch Number

Column	Corresponding System Data Expression
Segment Id	Segment Id
Token Number	Token Number
Treatment Id	Treatment Id

The expression is added to the formula. For example, the Campaign ID column would show the following formula:

```
@{campaignID}{0}
```

Note: If you get an error message in the Formula dialog box, then ignore the error.

6. Click OK.

Assigning Integration IDs

Every campaign load format requires an integration ID, referred to as Key 1, that supplies the enterprise-wide ID representing that customer. For example, most corporate data warehouses already have unique customer IDs assigned as the enterprise customer ID. Campaign load expects this column to be included in the campaign history. The following procedure describes how to set up the campaign load format integration ID.

To assign integration IDs

1. Choose the Column from the Subject Area that provides the Integration ID for the Contacts Target Level.
2. Select the column in the far pane.
3. Click the formula button in the column.
4. Check the Custom Headings box.
5. Delete the existing formula and replace it with the appropriate value from the table in *Creating a Campaign Load Format and Adding Columns*.
6. Click OK.

Requalifying List Results Against Original Criteria

The following procedure describes how to requalify list results against original criteria. The members of the campaign load file must be evaluated against the segment criteria when generating the campaign load file. This option limits the information in the list file only to members of the segment, and any Qualified List Items constrained on the segment tree. There is no need to reload the campaign because it picks up the changes in the people who are added to the segment when the campaign is launched.

To requalify list results against original criteria

1. In the Columns view, in the Filters pane, select the following check box:

   Re-qualify list results against original segment criteria
2. The following line is automatically added to the filter criteria:

Re-qualified against original segment criteria

Setting Options, Headers, and Footers for Campaign Load Formats

The following procedure describes how to set options, headers, and footers for campaign load formats. In the header, you can add an integration object name but you must not add a system data expression.

To set options, headers, and footers for campaign load formats

1. Click the Options tab and select the options in the following table.

Attribute	Option
Purpose	Campaign Load
(choose format)	Delimited File
End of Field Delimiter	Comma
Text Qualifier	""
Max # Records	1000

2. Click the Headers and Footers tab.
3. Enter the integration object name to load, using the following format (example also shown):

Format	Example
# integration object name #	# Marketing Contact #

> **Note:** You must not add additional text or a system data expression to the header. Additionally, do not press enter at the end of the second line. For EAI formatting, there must not be an end-of-line character at the end of the header.

4. Verify your campaign load format by previewing some sample contents of the list format.

   For instructions about how to preview a list format, see *Oracle Marketing Segmentation Guide*.
5. When you obtain the expected results, click the save icon to save your work.

About Siebel Contact and Campaign History Tables

When you load a campaign, the Campaign Load workflow process modifies data in the Siebel database after the Contact a integration component is mapped and the campaign load mapping data is modified.

- **Contacts table (S_CONTACT).** The Contacts table stores contact-level information.
- **Campaign History table (S_CAMP_CON).** The Campaign History table contains the history of contacts who qualify for campaigns, as well as the Campaigns ID, Segment ID, Wave Number, and so on.

If you include optional integration component fields such as Account or Contact Address in the campaign load format, other tables are updated with data according to the integration fields that are mapped.

For every record that qualifies for a campaign, the Campaign Load process uses the Contact component user key to determine if the contact record exists. The following table contains the table update rules.

Siebel Contact Record	S_CONTACT	S_CAMP_CON
Exists	Update existing record	Insert new record
Does not exist	Insert new record	Insert new record

Note: If you use the Marketing Contact integration object, the lookup uses the User Key fields for Contacts and Accounts. The illustration in *About the Marketing Contact Integration Object* shows the integration components for the Marketing Contact integration object. If you use the Marketing Person integration object, the lookup only requires the Campaign Id, Load Number, Token Number, Contact Id, or Prospect Id to confirm that the person is present in the transaction database.

Example of Configuring Campaign Load Format for Control Groups, Allocation Limits, and Stage Funneling

Campaign load formats support the use of control groups, allocation limits, and stage funneling. For more information on these features, see *Siebel Marketing User Guide* .

This topic gives an example of how to create campaign load formats for control groups, allocation limits, and stage funneling. You can use this feature differently, depending on your business model.

To create a campaign load format that supports control groups, allocation limits, and stage funneling

1. Navigate to the Administration - Marketing screen, then the List Formats view, and open the Campaign Load - Contacts Example list format.
2. Add a new column that uniquely identifies a target in the target level and change the formula to RANK([key column]). For example, in the Campaign Load - Contact and Prospect Example list format, the column has the following properties:
    - Table Heading: Contact
    - Column Heading: RANK ROW_WID
    - Column Formula: RANK(Contact.ROW_WID)

- Hide: Yes

3. Add another column to the list form.
4. Change the Column Formula to use the previous Rank column to calculate control group flag based on a system variable called controlGroupPct. For example, in the Campaign Load - Contact and Prospect Example list format, the column has the following properties:
   - Table heading: Campaign Contact
   - Column Heading: Control Group Flag
   - Column Formula: CASE WHEN (RANK(Contact.ROW_WID) - TRUNCATE(RANK(Contact.ROW_WID)*@{controlGroupPct}{0}/100,0)*100/@{controlGroupPct}{0}) < 1 THEN 'Y' ELSE 'N' END
   - Hide: No
5. Add a filter to restrict the query count according to constraining stage wave Ids and the percentage allocation limit. For example, in the Campaign Load - Contact and Prospect Example list format, the filter is:

```
Re-qualified against original segment criteria

AND '@{constrainingStageFlag}{N}' = 'N' OR "Campaign Contact"."Load Wave Id" IN
(@{constrainingWaveID}{'0'})

AND '@{pctAllocationFlag}{N}' = 'N' OR (RANK(Contact.ROW_WID) -
TRUNCATE(RANK(Contact.ROW_WID)*@{allocationLimit}{1000000}/100,0)*100/
@{allocationLimit}{1000000}) < 1

AND '@{pctAllocationFlag}{N}' = 'Y' OR RANK(Contact.ROW_WID) <=
@{allocationLimit}{1000000}
```

Example of Creating a Response Load Format

The response list format creates responses from the program flow. It can be stored in the My Data Load Format or Shared Data Load Format folders. This topic gives an example how to create a response load format based on the Analytics Data Load - Responses sample list format. You can use this feature differently, depending on your business model.

To create a response load format

1. Navigate to the Administration - Marketing screen, then the List Formats view, and open the Analytics Data Load - Responses sample list format.
2. Create new columns and map the column headers to the integration objects, using the following table as a guide.

Table Heading	Column Heading	Column Formula
Response	Id	'NOID'
Response	Response Type	'@{responseType}{}'
Response	Treatment Id	'@{treatmentID}{}'

Table Heading	Column Heading	Column Formula
Response	Description	'@{description}{}'
Response	PR_CON_ID	"- Contact Profile"."Contact Id"
Response	PRSP_CON_ID	"- Contact Profile"."Prospect Id"
Response	ACCNT_ID	"- Contact Profile"."Account Id"
Response	SRC_ID	'@{campaignID}{}'
Response	Response Value	'@{responseValue}{}'
Response	Response Cost	'@{responseCost}{}'
Response	Response Cost Currency Code	'@{responseCostCurrencyCode}{}'
Response	Score	'@{score}{}'

3. Add a filter to restrict the query count based on constraining stage wave Ids. For example:

```
Re-qualified against original segment criteria
AND ' '@{constrainingStageFlag}{N}'= 'N' OR "Campaign History (Transaction
Database)"."Campaign Load Wave Id" IN (@{constrainingWaveID}{'0'})
```

4. Set the header and footer to match the object name “Response”.
5. Set the Purpose attributes. For example:
    - Purpose: Analytics Data Load
    - Delimited
    - Max# Records: 1000

Example of Creating a Lead Load Format

The response list format creates leads from the program flow. It can be stored in the My Data Load Format or Shared Data Load Format folders. This topic gives an example how to create a lead load format based on the Analytics Data Load - Leads sample list format. You can use this feature differently, depending on your business model.

To create a lead load format

1. Navigate to the Administration - Marketing screen, then the List Formats view, and open the Analytics Data Load - Leads sample list format.
2. Create new columns and map the column headers to the integration objects, using the following table as a guide.

Table Heading	Column Heading	Column Formula
Lead	Id	'NOID'
Lead	Lead Status	'@{leadStatus}{}'
Lead	Treatment Id	'@{treatmentID}{}'
Lead	Description	'@{description}{}'
Lead	Contact Id	"- Contact Profile"."Contact Id"
Lead	Prospect Id	"- Contact Profile"."Prospect Id"
Lead	Account Id	"- Contact Profile"."Account Id"
Lead	Source Id	'@{campaignID}{}'
Lead	Division Owner	'@{divisionID}{}'
Lead	Quality	'@{leadQuality}{}'
Lead	Lead Score	'@{score}{}'
Lead	Primary Partner Id	'@{partnerID}{}'
Lead	Calc Lookback Days	'@{leadLookbackDays}{}'
Lead	Calc Product Id	'@{productID}{}'
Lead Product	Product Id	'@{productID}{}'

Table Heading	Column Heading	Column Formula
Lead Position	Position Id	'@{positionID}{}'

3. Add a filter to restrict the query count based on constraining stage wave IDs. For example:

```
"Re-qualified against original segment criteria
"AND ' '@{constrainingStageFlag}{N}'= 'N' OR "Campaign History (Transaction
Database)"."Campaign Load Wave Id" IN (@{constrainingWaveID}{'0'})
```

4. Set the header and footer to match the object name Mktg Prog Lead Dedup.
5. Set the Purpose attributes. For example:
   - Purpose: Analytics Data Load
   - Delimited
   - Max# Records: 1000

Testing Campaign Load Formats

To verify that you have created a valid campaign load format, it is recommended that you build a test campaign and test segment.

To test your campaign load mapping

1. Verify that you have included the minimum required fields for each integration component.

   For more information, see *About Marketing Integration Objects*.
2. Confirm that the Campaign Load Format includes the required columns for all formats:
   - Campaign Id
   - Segment Id
   - Load Number
   - Batch Number
   - Token Number
   - Treatment Id
3. Confirm that the parent integration component is mapped for every child component. For example, if you included Account Address fields, make sure that you also included Account Name and Location.
4. Create a test segment using the Segment Designer. For the segment, go to the Advanced Options tab and change the Campaign Load List Format to use your new Campaign Load Format. Save the segment.
5. Create a new campaign under the Campaigns screen tab.
6. In the Design tab, perform the following steps:
   a. Click the Offers link.
   b. In the Offers list, click New.
   c. In the Add Offer dialog box, choose a test offer and click OK.
   d. In the Treatments list, click New.

e. In the Pick Treatment list, choose a test treatment.

7. Navigate to the Design screen, then the Segments/Lists view for the Campaign, and click Add Segment to choose your test segment.

   a. Click the Segments/Lists link.
   b. In the Segments/Lists list, click Add Segment.
   c. In the Previously Used Segments dialog box, click Choose a new Segment.
   d. Locate and select your test segment.

      In the Allocation matrix, a check box will appear for the treatments you associated in Step 6.
   e. Check the check box and click Save.
8. Click the menu on the upper form for the campaign and choose 'Load Campaign'. In the dialog box, confirm the load time and click OK to submit.
9. Navigate to the Execute screen, then the System Tasks view to monitor whether the Campaign Load task successfully completed. Investigate any error messages that appear in the Task Log.
10. After the load completes successfully, validate that the data loaded matches the expected information.

    a. While your campaign is still selected, navigate to All Contacts/Prospects across Organizations and query for the campaign members for that Load Number. Optionally, export these rows to a file using the Export menu command.
    b. Navigate to the Administration - Marketing screen, Marketing Server Admin, and then the Manage Marketing Jobs view. Find the Marketing Job that you generated with the type WriteListFiles. Open the details link and find the network path to the file that was generated.
    c. Compare the contents of the file and the data that was loaded into your campaign to confirm that the data was complete and correct.
11. Make any changes required to the Campaign Load Format using the List Format Designer. Be sure to save any changes to the Format.
12. When completed, purge the load history by performing the following steps:

    a. Navigate to the Campaigns screen and click the campaign.
    b. In the Execute tab, click Suspend Wave.

       Note: You must suspend the waves in the load before you can purge a load.

    c. In the Execution Status view, click Purge Load, and then delete your test campaign.

About Marketing Integration Objects

For each campaign load format, you must select only one of the following integration objects:

- **Marketing Contact integration object.** If any campaign contact names do not exist within the Siebel transactional database, you must use the Marketing Contact integration object. It provides the field mappings necessary to import new contacts and accounts. For more information, see *About the Marketing Contact Integration Object*.
- **Marketing Prospect integration object.** If any prospect names from your target segment do not exist within the Siebel transactional database, you must use the Marketing Prospect integration object. It provides the field mappings necessary to import new prospects. For more information, see *About the Marketing Prospect Integration Object*.

- **Marketing Person integration object.** If your campaign contacts and prospects exist within the Siebel transactional database prior to loading any campaigns, then you can also use the Marketing Person integration object. Typically, this configuration occurs for installations that use the Siebel Data Warehouse populated from the Siebel transactional database and that do not introduce new customers into the Siebel Data Warehouse from other sources. Because the contact and prospect field information is already recorded, to load the campaign in this configuration, you only need to map the Contact and Prospect IDs between the data warehouse and Siebel transactional database. For more information, see *About the Marketing Person Integration Object*.
- **Marketing Lead integration object.** If any leads for a particular campaign do not exist within the Siebel transactional database, you must use the Marketing Lead integration object. It provides the field mappings necessary to import new leads. For more information, see *About the Marketing Lead Integration Object*.
- **Marketing Response integration object.** If any inferred responses for a particular campaign do not exist within the Siebel transactional database, you must use the Marketing Response integration object. It provides the field mappings necessary to import new inferred responses. For more information, see *About the Marketing Response Integration Object*.

Siebel Marketing does not provide an integration object that can insert new contacts and prospects simultaneously in the same load.

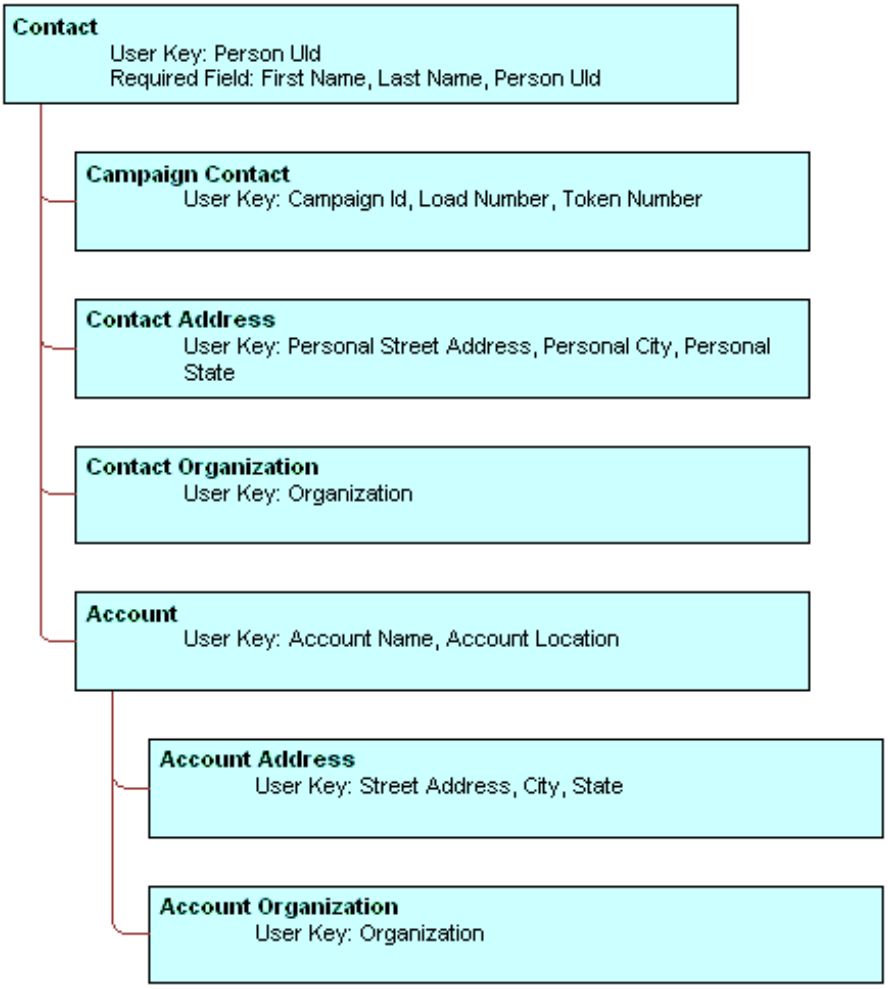
This topic contains the following information:

- *About the Marketing Contact Integration Object*
- *About the Marketing Prospect Integration Object*
- *About the Marketing Person Integration Object*
- *About the Marketing Lead Integration Object*
- *About the Marketing Response Integration Object*
- *Examples of Recommended Campaign Load Mappings*

About the Marketing Contact Integration Object

The Marketing Contact integration object provides field mappings to typical contact- and account-related information from the external data sources. The predefined integration object, Marketing Contact, defines the information that is exchanged between the external data source and Siebel Marketing, using EAI technology. For more information about EAI, see *Overview: Siebel Enterprise Application Integration* . For a list of fields for the Marketing Contact integration object, see *Field Names for Marketing Integration Components*.

The following figure shows the integration components for the Marketing Contact integration object. Required fields apply when a new contact is inserted into the Siebel transactional database.



During campaign load, integration component User Keys determine if a record already exists in the component (for the given values) and if the record is unique. Required fields cannot be a null value for the new record.

The following table describes the Marketing Contact integration components.

Component	Comment
Account	Maps account information associated with the contact.
Account Address	Maps the account address.
Account Organization	Maps information about the account's organization.
Campaign Contact	Maps campaign history-level information such as campaign Id, load number, wave number, contact Id, prospect Id, account Id, and the keys that bind contacts with their unique IDs in the data warehouse.
Contact	Maps contact-level information such as the contact's name, telephone number, email address, and so on.

Component	Comment
Contact Address	Maps the contact's address information.
Contact Organization	The Contact Organization component maps information about the contact organization.

Mapping Rules for the Marketing Contact Integration Components

Using contact information for campaign load requires the following integration components:

- **Contact.** Includes information such as contact first name, contact last name, and so on.
- **Campaign Contact.** Fields must be mapped in the campaign load report. Mapping includes the required campaign load columns and the keys that store unique IDs from the data warehouse for the party (contacts, prospects, or accounts) being loaded.

Use the following rules when mapping components:

- A parent integration component must be mapped before mapping a child component. For example, the Account Address component cannot be mapped unless Account is mapped.
- User Key fields must be mapped for each integration component if one or more fields for the component is mapped.
- Required fields must be mapped for each integration component if one or more fields for the component are mapped.
- Make sure that the campaign load format includes a column indicating the organization in which the contact and account data must be loaded.

Sample Mappings for Contact Key Components

The combination of keys that are mapped in the campaign load report depend upon the target levels that you use.

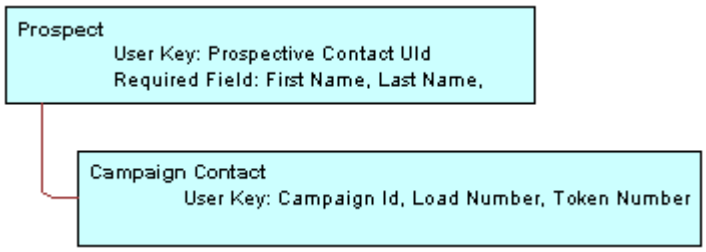
The following table describes examples of Key mappings for sample target levels.

Target Level	Key Mapping
Contacts	Key 1
Accounts	Key 2
Prospects	Key 3
Households	Key 4

About the Marketing Prospect Integration Object

The Marketing Prospect integration object provides field mappings to typical prospect information from marketing data source(s). The required fields are fields that cannot be a null value for the new record.

The following figure shows the integration components for the Marketing Prospect integration object. Required fields apply when a new prospect is inserted into the Siebel transactional database.



For a list of fields for the Marketing Prospect integration object, see *Field Names for Marketing Integration Components*.

The following table describes the Marketing Prospect Integration components.

Component	Comment
Campaign Contact	Maps campaign history-level information. • User Key: Campaign Id, Load Number, and Token Number
Prospect	Maps prospect information. • User Key: Prospect Contact UId • Required fields: First Name, Last Name, and Prospective Contact UId

Note: Required fields apply when a new contact is inserted into the Siebel transactional database.

Mapping Rules for the Marketing Prospect Integration Components

Using prospect information for a campaign load requires the following integration components:

- **Prospect.** Includes information such as prospect first name, prospect last name, and so on.
- **Campaign Contact.** Fields must be mapped in the campaign load report. Mapping includes the required campaign load columns and the keys that store unique IDs from the data warehouse for the prospects being loaded.

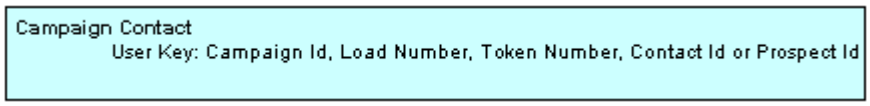
About the Marketing Person Integration Object

Most deployments of the Siebel Marketing application use the Marketing Contact integration object for loading campaign data. The Marketing Contact integration object is most commonly used because it supports inserting new contact and account names into the transaction database. In contrast, the Marketing Person integration object only supports inserting new records into the Campaign History table for contacts or prospects that already exist in the transaction database.

When all the customer data resides in the Siebel transaction database, the load process can avoid inserting new customers and improve the load time. The Marketing Person integration object supports this simple lookup load process.

Only use the Marketing Person integration object when all target contacts, accounts and prospects in the campaign already exist in the transaction database. The only required mapping is between the Row ID from the Contact and Prospect tables in the Siebel transactional database and the external data source, typically the Siebel Data Warehouse. For a list of fields for the Marketing Person integration object, see *Field Names for Marketing Integration Components*.

The following figure shows the integration components for the Marketing Person integration object. Required fields apply when a new campaign contact record is inserted into the Siebel transactional database.



The following table describes the integration component for the Marketing Person integration object.

Component	Comment
Campaign Contact	Maps the required campaign history columns and keys that store the unique IDs from the data warehouse for the party being loaded. User Key: Campaign Id, Load Number, Token Number, and one or more of the following: • Contact Id • Prospect Id

Mapping Rules for the Marketing Person Integration Components

When creating a campaign load mapping using the Marketing Person integration object, use the following guidelines:

- The Contact Id and Prospect Id values imported from the external data source must match the Row IDs for the Contact or Prospect in the contact or prospect tables.
- If all incoming target names are contacts, then mapping the Prospect Id is not required. Alternatively, you could use the Marketing Contact integration object. If all incoming target names are prospects, then you do not need to use Contact Id. If the target list includes both contacts and prospects, then both fields are required.

About the Marketing Lead Integration Object

The Marketing Lead integration object provides field mappings to typical lead-related information from external data sources. The Mktg Prog Lead Dedup integration object defines the information that is exchanged between the external data source and Siebel Marketing, using EAI technology.

The following table describes the integration components for the Lead integration object.

Component	Description
Lead	Defines all the primary attributes of the entity lead. User Key: Id
Lead Organization	Defines the Organization attributes associated with the lead.

Component	Description
	User Key: Organization Id
Lead Position	Defines attributes of Position associated with the lead. User Key: Position Id
Lead Product	Defines attributes of Products associated with the lead. User Key: Product Id

Note: During lead creation, the user keys in each integration component determine if a record already exists in the component (for the given values) and if the record is unique.

About the Marketing Response Integration Object

The Marketing Response integration object provides field mappings to typical response-related information from external data sources. The response integration object defines the information that is exchanged between the external data source and Siebel Marketing, using EAI technology.

The following table describes the integration components for the Response integration object.

Component	Description
Response	Defines all the primary attributes of the response. User Keys: • Mod Key (Modification Key) • Id • Description
Related Organization	Defines the attributes of products associated with the response. User Key: Mod Key (Modification Key)
Response Log	Defines survey-related attributes for the response. User Key: Question Text, Answer Text

Note: During response creation, the user keys in each integration component determine if a record already exists in the component (for the given values) and if the record is unique.

Examples of Recommended Campaign Load Mappings

Campaign Load Mappings depend on the following:

- **The data source.** The data source includes Siebel Data Warehouse, Siebel transactional database, or a data source other than Siebel applications.
- **The data elements required to be imported.** These elements include Contact fields, Account fields, Contact address, and so on.
- **Contact qualification.** Determine if new contacts or existing contacts qualify for a campaign.
- **Presence of contacts and prospects in the Siebel database.** Determine if all contacts and prospects are already present in the contact and prospect tables in the Siebel database.

This topic contains descriptions of mappings with the name of the sample campaign load format report in which the recommended mappings appear. You can find the examples listed in the following topics in the Siebel File System: Shared Campaign Load Formats/Marketing/Example List Formats.

Examples of Mappings to the Siebel Data Warehouse

These mappings are applicable when campaigns are run against Siebel Data Warehouse.

- **Recommended Mappings for Existing Contacts And Prospects.** See the following sample campaign load format report:

  Campaign Load - Contacts and Prospects Example
- **Recommended Mappings for Existing Accounts.** See the following sample campaign load format report:

  Campaign Load - Existing Accounts

Examples of Mappings to the Siebel Database

The mappings shown in the following reports are applicable when campaigns are run on Oracle's Siebel database.

- **Recommended Mappings for Contacts And Prospects.** See the following sample campaign load format report:

  Campaign Load - Contacts and Prospects Example
- **Recommended Mappings for Accounts.** See the following sample campaign load format report:

  Campaign Load - Existing Accounts

Examples of Mapping to a Non-Siebel Database

The mappings shown in the following reports are applicable when campaigns are run on a non-Siebel database.

- **Recommended Mappings for New Contacts.** This is for cases where some of the contacts being loaded for the campaign do not exist in the Siebel database. See the following sample campaign load format:

  Campaign Load Contacts - Example
- **Recommended Mappings for New Accounts.** This is for cases where some of the accounts being loaded for the campaign do not exist in the Siebel database. See the following sample campaign load format:

Campaign Load Accounts - Example

- **Recommended Mappings for New Prospects.** This is for cases where some of the prospects being loaded for the campaign do not exist in the Siebel database. See the following sample campaign load format:

  Campaign Load Prospects - Example

5 Installing and Configuring Siebel Email Marketing

Installing and Configuring Siebel Email Marketing

This chapter describes how to install and configure Siebel Email Marketing. It includes the following topics:

- *Overview of Siebel Email Marketing*
- *Overview of Installing and Configuring Siebel Email Marketing*
- *Architecture of Siebel Email Marketing*
- *Requirements for Installing Email Marketing*
- *Installing the Email Marketing Server*
- *Roadmap for Configuring Email Marketing Daemons*
- *Process of Configuring the Email Sending Daemon*
- *Process of Configuring the Bounce Handler Daemon*
- *Process of Configuring the Click Through Daemon*
- *Encrypting Trackable URLs and Response Forms for Email Marketing*
- *Configuring Email Marketing Components for HTTPS Communications*
- *(Optional) Enabling TLS for Communications Between the Email Sending Daemon and the SMTP Server*
- *(Optional) Verifying Email Marketing Component Configuration*
- *Process of Testing the Email Marketing Components with Siebel Marketing*
- *Administering Email Marketing*
- *Configuring the Status of Email Addresses*
- *Implementing Spam Scoring of Email Templates Using Spam Assassin*
- *Authentication Mechanism of Email Marketing Server*

About Siebel Email Marketing

The Siebel Email Marketing Server is a combination of components designed to support high volume, personalized, email messages and to track email bounces and click-through responses.

The Siebel Email Marketing Server consists of the following three components. Each has its own installer that's separate from the Siebel Marketing Server installer.

- **Email Sending Daemon (ESD)** Assembles each outbound email message for a campaign using the email template (HTML or text) and the recipient list, and then sends each message to your company's outbound Mail Transfer Agent (MTA) for delivery.
- **Bounce Handler Daemon (BHD)** Tracks email messages that can't be delivered, parses the returned email messages, and records the cause of the bounce.

- **Click Through Daemon (CTD)** Tracks clicks made by the email recipient on any Siebel-supported links included in the email template.

Example of Email Delivery

A good understanding of email delivery is helpful in understanding the key principles and items presented in the following topics. The provided example is a simplified description of the email delivery process and describes one email being sent.

When you send thousands or millions of emails, the process becomes complex. Siebel Email Marketing is designed to address the issues associated with sending a large volume of emails.

When an email is sent by person A to person B, an attempt is made to deliver the email. The first step in the process occurs when users click Send in their email client. The email client tries to initiate a connection to an email server.

> **Note:** This email server is often called a Mail Transfer Agent (MTA) because of its function or a Simple Mail Transfer Protocol (SMTP) Server because of the protocol it uses.

When the client has a connection to an MTA, the MTA and the client communicate using the SMTP. The following are important parts of this communication:

- One critical piece of this communication involves the transfer of the email message to the MTA.
- Another piece of this communication is the passing of the sender's email address. This email address is often referred to as the SMTP envelope from (or sender) address. The use of the term envelope represents the email content as a letter and the SMTP communication as the envelope used to carry the letter.

If the recipient of the email (person B) has a mailbox on this server, then the server drops the email in the box and the job is done. If person B is on another domain, then the MTA executes a Domain Name Service (DNS) lookup to find the address of another Mail Transfer Agent to communicate with. Another SMTP conversation occurs and the second MTA receives the message and delivers it to the mailbox for person. When it's in person B's mailbox, the recipient can retrieve it using another protocol such as Post Office Protocol (POP) and read the message in an email application.

About Bounce Codes

Unexpected issues can occur during the email delivery process. For example, the domain of the recipient can be unreachable or not exist at all. In this case, an error message or bounce is created by the Mail Transfer Agent that identifies the problem, and the bounce is returned to the sender of the message. The sender’s email address is called the From Address of the SMTP envelope.

Another problem might be that the domain has been found but the user doesn't exist on that domain. Again, a bounce is created and sent back to the sender of the original message. Both of these are examples of hard bounces. This means that not only was the email unable to be delivered but that it can never be delivered.

Another type of bounce is a soft bounce, which means that although the email couldn't be delivered now, but it might be possible to deliver the message in the future. Here are some bounce codes:

Bounce Code	Description
Address Moved	The recipient has changed the email address and the new address is available. This type of bounce occurs rarely.

Bounce Code	Description
Bad Sender	The email address is bad: either the address is formatted incorrectly (unlikely) or there's no such user.
Last Resort	The bounce parser couldn't determine the type of bounce, but it has the name of the original recipient.
Mailbox Problem	The email address exists, but the mailbox is full or temporarily locked. This type of bounce occurs rarely.
Message Too Large	The message size exceeds the recipient's allowable limit.
Network Problem	Because of network problems, the MTA is unable to connect to either the receiving Mail Server or some other necessary server (such as a company's LDAP server). This type of bounce occurs rarely.
Protocol Problem	The receiving Mail Server doesn't work with the version of SMTP the MTA uses. This type of bounce occurs rarely.
Security Problem	The receiving Mail Server doesn't allow email from your domain. This can occur when the receiving Mail Server blocks domains of known or suspected spammers.
System Problem	The receiving email server is having technical problems and can't accept mail right now.
Unparsable	The bounce parser couldn't classify the bounce message into any other category.

Note: If a recipient has activated a vacation mail response, then a vacation code is generated when an email is delivered. However, a vacation code is an auto-reply message code, not an error code.

For more information on bounce codes and the status of email addressees, see *About Creating Classification Rules for Bounce Messages* and *Configuring the Status of Email Addresses*.

Frequently Used Terms for Email Marketing

The following table contains abbreviations and terms frequently used in Email Marketing.

Term	Definition
BHD	Bounce Handler Daemon. Processes asynchronous bounced email (bounces that don't occur in the SMTP communications between the Email Sending Daemon and the Mail Transfer Agent).
Bounce	An email that's returned due to a temporary or permanent error condition. There are hard bounces and soft bounces as described in the following list:

Term	Definition
	• Hard bounce. The email wasn't delivered and can never be delivered. For example, if the email address is invalid. • Soft bounce. The email can't be delivered because of a temporary problem such as a full mailbox and can be delivered when the problem no longer exists.
CTD	Click Through Daemon. Handles the following customer actions: • Unsubscribe and Subscribe so contacts can opt in or opt out of email lists. • Forward to a Friend provides method for capturing new email addresses. • Trackable URLs track customer clicks on an embedded link in an email. • Read Receipts logs message opens.
Daemon	A program that's not called explicitly, but is dormant waiting for an action or event to activate it.
DNS	Domain Name System. Created to provide a way to translate domain names to their corresponding IP addresses. The DNS server maintains a list of domain names and IP addresses and each request is pointed to the correct corresponding IP address.
DMZ	Demilitarized Zone. A section of your corporate network that acts like a neutral zone or buffer between your internal network and the Internet. It's created by placing one firewall between the outside (internet) and web servers, and a second firewall between the web servers and your internal network. External users can access servers in the neutral zone, but not servers on the internal network. The servers in the DMZ handle incoming and outgoing traffic.
DNS groups	DNS domain names are categorized into groups called a record and each record is given a special name such as MX or A. • MX (type of record). Specifies a domain name which can receive and possibly relay emails. This domain probably contains a server hosting an MTA. • A (type of record). Maps a domain name to an IP address.
ESD	Email Sending Daemon. Manages the following tasks: • Email Construction and Personalization. • Delivery of outbound email to Mail Transfer Agents. • Synchronous bounced email. Bounces that occur in the SMTP conversation between the Email Sending Daemon and the MTA.
MTA	Mail Transfer Agent. A program responsible for receiving, routing, and delivering email messages. MTAs receive email messages and recipient addresses from local users and remote hosts, perform alias creation and forwarding functions, and deliver the messages to their destinations. An MTA is sometimes called a Mail Transport Agent, a mail router, an Internet mailer, or a mail server program. Commonly used MTAs include sendmail, qmail, and Exim.
SMTP	Simple Mail Transport Protocol. Used to move each email over the internet.
SOAP	Simple Object Access Protocol. The use of XML and HTTP to access services, objects, and servers in a platform-independent manner. For more information about SOAP, see the *Developer's Guide for Oracle Analytics Cloud: Introduction to Oracle Analytics Web Service*.

Term	Definition
WSD	Web Survey Daemon. Resides in the DMZ and supports web landing sites and surveys without the need for SmartScript.

About Installing and Configuring Siebel Email Marketing

Each of the Siebel Email Marketing Server's three components has its own installer and is separate from the Siebel Marketing Server installer. The installation media for the three Email Marketing Server components are distributed together on media separate from the Siebel Enterprise installation media.

The topic in this section describes some of the issues to consider when installing the different components of Siebel Email Marketing. The Email Marketing components can reside outside the firewall, with ports opened for SOAP (HTTP) and networked file system access through the firewall. Alternatively, the Email Marketing components can reside inside the firewall with ports 80 and 25 opened on the firewall (or proxies) or relays put in place.

These components talk to the Siebel Marketing Object Manager using SOAP. For more information about the Siebel Java Data Bean, see the *Siebel Transports and Interfaces: Siebel Enterprise Application Integration* guide.

Note: web.xml Updates From 26.8, web.xml is updated to align with Servlet 3.0 schema requirements by replacing legacy DOCTYPE declarations with the Servlet 3.0 XSD-based root element using version="3.0". When the HTTPS is enabled, add the secure setting under session-config in the web.xml file for the ESD, CTD and WSD component. Remove this setting when HTTP is used.

Example for HTTPS:

```
<session-config>
 <cookie-config>
 <secure>true</secure>
 </cookie-config>
</session-config>
```

Note: Do not add the secure setting for HTTP configurations.

Email Sending Daemon

The Email Sending Daemon (ESD) assembles an email to be sent to a list or segment of contacts and prospects and delivers each email to the corporate outbound Mail Transfer Agents. Assembly includes adding headers in front of the email message content and merging personalized data into the message content.

The Email Sending Daemon listens on port 8090 for SOAP requests from the Siebel Marketing Server. A SOAP request includes the file name of the email message content, the email message headers, and the Marketing Server subwave contacts and prospects list (containing mail merge data). These files are found in the Marketing File System which is commonly a networked directory accessible to the Email Sending Daemon. The Email Sending Daemon must be able to communicate with one or more outbound Mail Transfer Agents to send mailings over the internet. The Email Sending

Daemon must be able to tell the Marketing Server when it has completed a subwave as well as deliver details of email address errors that occurred while it communicated using Simple Mail Transfer Protocol to the Mail Transfer Agents (called synchronous bounces).

The most common placement for the Email Sending Daemon is within the corporate network, behind the DMZ. However, the Email Sending Daemon component can be placed inside the DMZ or outside the firewall, if there's a port opened to connect to the Siebel Marketing Server using SOAP and the networked Marketing File System.

Bounce Handler Daemon

Typically, the Bounce Handler Daemon (BHD) receives and processes bounced mail on port 25 (the default SMTP port).

Email messages that have bounced appear similar to regular email, though their email message content and headers probably have noticeable differences in content. For a bounced email to be returned to the Bounce Handler Daemon, the original email must have a usable return address (the SMTP envelope from address). The correct SMTP envelope From Address is generated for you using the Bounce Handler Daemon's domain name (supplied by you when you configure the Email Marketing Server).

The recommended approach is to place the Bounce Handler Daemon computer in the DMZ. However, some network support technicians can choose to place the Bounce Handler Daemon behind an inbound Mail Transfer Agent. The approach that you choose depends on the configuration of your network, DMZ, existing inbound Mail Transfer Agent, and firewall. The following example describes a typical approach.

You might have a domain name of example.com and an inbound Mail Transfer Agent (in this example mail.example.com) for mail to that domain. The Mail Transfer Agent mail.example.com currently routes email successfully to computers in the internal network. It might be in the DMZ with a special hole for port 25 traffic or straddling the outer firewall with one NIC in the DMZ and the other NIC on the Internet. The Bounce Handler Daemon might be running inside the DMZ, with an internal-only hostname such as example-host.internal.example.com.

In this example, you would choose a Bounce Handler Daemon hostname such as bounces.example.com that is not already used by external DNS and then perform the following steps:

- Configure the Bounce Handler Daemon to use this hostname.
- Add a DNS MX record for this hostname to an internal DNS server that can be contacted by the inbound Mail Transfer Agent (mail.example.com).
- Add this hostname to the Internet DNS servers as a hostname with an IP address for the inbound Mail Transfer Agent.

Because the Internet DNS MX records for bounce.example.com point to the inbound Mail Transfer Agent, bounced email for the Bounce Handler Daemon is sent there first. Mail.example.com must be configured to relay the mail for bounces.example.com to the Bounce Handler Daemon using the internal DNS server for the correct internal IP address.

Organizations often create IP numbers that cannot be directly reached from outside their enterprise. For example, IP numbers starting with 10.* or 192.168.* are only available inside the enterprise. Similarly, organizations often have hostnames, such as my-machine.corp.example.com, that are only visible inside the company network. If you use an IP address or hostname that is only available inside your company network for your Bounce Handler Daemon hostname, then Mail Transfer Agents outside your network cannot connect to the Bounce Handler Daemon. Therefore, the Bounce Handler Daemon server must be available, directly or indirectly, from outside your network.

Click Through Daemon

The Click Through Daemon (CTD) listens on port 8060 for HTTP requests (Clickthrough, Message Open, Forward to a Friend and un-subscription and subscription requests). This component can be placed in the DMZ, inside or outside the firewall, if a port is opened that allows it to connect to the Siebel Marketing Server using SOAP protocol. Web proxy servers can be used to route the HTTP requests to the Click Through Daemon server.

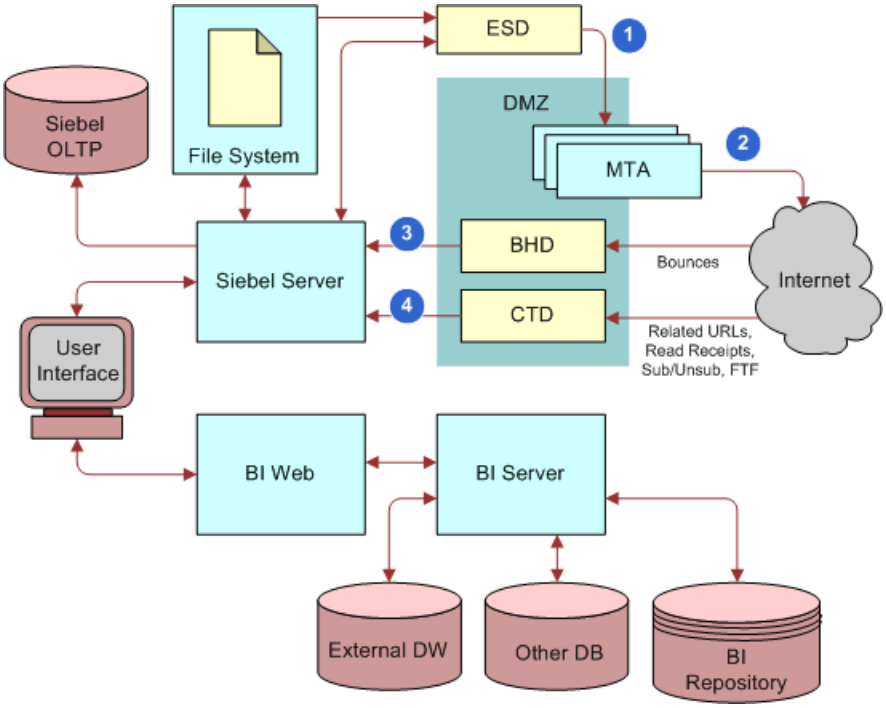
Architecture of Siebel Email Marketing

An example of a typical architectural structure for Siebel Email Marketing components is shown in the following image. The Email Marketing components interact with Siebel Marketing as follows:

1. The Email Sending Daemon, located in the corporate network, listens for requests from the Siebel Marketing Server, then assembles each outbound email message for a campaign, and sends it to the Mail Transfer Agent for delivery.

   For more detailed information on how the Email Sending Daemon interacts with Siebel Marketing, see *Email Sending Daemon Integration and Workflow*.
2. The Mail Transfer Agent receives the email messages and forwards them to their destinations.
3. The Bounce Handler Daemon, located in the DMZ, tracks email messages that cannot be delivered and records the reason why the message cannot be delivered.
4. The Click Through Daemon, located in the DMZ, tracks clicks made by email recipients on links included in the email template that are supported by Siebel Marketing.

If Siebel Email Marketing components lose connectivity to the Siebel Server, then they queue all data and continue to function. After the connection is reestablished, queued data is processed.



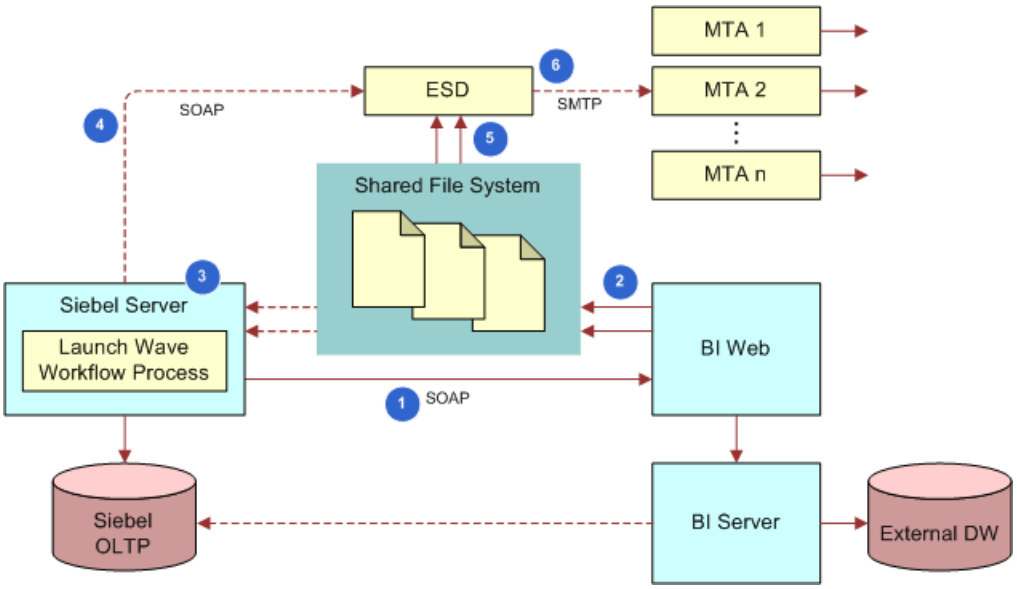
Email Sending Daemon Integration and Workflow

The following figure shows a more detailed view of the Siebel Email Sending Daemon, its interrelationship with Siebel Marketing, and the outbound flow of work within this architecture. The following steps correspond with the numbers in the figure:

1. A workflow is launched to generate list files for each batch (subwave).

   If Basic email personalization mode is implemented, then the Siebel Server generates the list files.

   If Advanced email personalization mode is implemented, then the workflow calls Business Intelligence Web to generate a list that is formatted for email personalization, then Business Intelligence Presentation Server generates the list files.
2. The workflow waits until files are returned.
3. Workflow launches a subprocess for each file and then notifies the Email Sending Daemon of the location of each file.
4. The Email Sending Daemon retrieves each subwave list of Prospects and Contacts.
5. The Email Sending Daemon sends email to the Prospects and Contacts in each subwave list.



Requirements for Installing Email Marketing

Before installing Email Marketing, you must perform the following tasks:

- *Configuring Basic and Advanced Email Personalization*
- *Removing an Existing Version of the Email Marketing Daemons*
- *Installing the Java Runtime Environment*
- *Verifying That the Object Manager Is Enabled and Running*

Configuring Basic and Advanced Email Personalization

Your application can be configured to use one of two methods for email merge fields:

- **Basic.** The Basic mode is used when your organization has not licensed or deployed the marketing segmentation module, or if your requirements do not call for advanced merge fields. This option uses a fixed set of merge fields based on the available fields in the campaign recipient business component. In this mode, the email list is generated directly from the business component and delivered to the Email Sending Daemon for sending the email messages.
- **Advanced.** The Advanced mode is only available if your organization has deployed the marketing segmentation module. This option provides a flexible set of merge fields based on data from any data source or table accessed by the Oracle Business Intelligence repository. The merge fields are determined by the fields in the Personalization Format (Email Server list format) that you select for the email offer.

Configuring Basic Email Personalization Mode

To configure basic email personalization mode, perform the steps in the following procedure.

To configure basic email personalization mode

1. Navigate to the Administration - Server Configuration screen, then the Servers view.
2. Select a server.
3. In the Components tab, query for the Marketing component.
4. Click the Parameters tab for this object manager.
5. Query for the Email Personalization Format parameter.
6. Make sure the Value field is set to any value other than a path name. For example, set it to Default Merge Fields. Using a nonpath name as a value allows Basic Personalization.

Configuring Advanced Email Personalization Mode

The advanced personalization mode requires that you install the Marketing Module for segmentation and list generation and configure the required marketing metadata for list export. Perform the following steps to set up advanced email personalization.

To configure advanced email personalization mode

1. Configure the marketing metadata for list generation. For instructions, see the Oracle Business Intelligence Enterprise Edition documentation.
2. Create one or more Email Server List Formats in the List Format Designer. For instructions, see *Oracle Marketing Segmentation Guide*.
3. Designate one of the list formats as the default Email Personalization format for the Siebel Marketing application by performing the steps in the following procedure. This set of merge fields populates for any new email offers that are created.
    a. Navigate to the Administration - Server Configuration screen, Servers, and then the Components view.
    b. In the components list, query for the Marketing (ENU) component.
    c. Click the Parameters view tab.
    d. In the Component Parameters list, query for the Email Personalization Format parameter.

       The initial value is Default Merge Fields.
    e. To change the default system email list format to another email list format, enter the full Web catalog path in the Value on Restart column. For example:

```
/shared/Marketing/Example List Formats/Advanced Merge Fields
```

f. If the catalog path is too long to enter in the parameter column, then you might need to shorten the folder and list format name in the Business Intelligence Web catalog.

Removing an Existing Version of the Email Marketing Daemons

If you have an existing version of the Email Sending Daemon, Bounce Handler Daemon, and Click Through Daemon, then you must remove them before proceeding with this install. The following procedures describe this task for a Windows and UNIX environment.

Removing Existing Email Marketing Daemons on a Windows Server

To remove existing Email Marketing daemons on a Windows server, perform the steps in the following procedure.

To remove existing Email Marketing daemons on a Windows Server

1. From the Start menu, choose Settings, Control Panel, Administrative Tools, and then Services.
2. Stop the services for Email Marketing daemons.
   a. Right-click the Email Sending Demon service and select Stop.
   b. Right-click the Bounce Handler Demon service and select Stop.
   c. Right-click the Click Through Demon service and select Stop.
3. Locate the directory where the Email Marketing Server components were installed and remove all the files and directories of each components.

> **Note:** After the uninstall, some files that could cause problems for the new installation might remain. Deleting files in these directories makes sure that the new installation does not inherit outdated information.

Removing Existing Email Marketing Daemons on a UNIX Server

To remove existing Email Marketing daemons on a UNIX Server, perform the steps in the following procedure.

To remove existing Email Marketing daemons on a UNIX server

1. Log in as root.

   The Root user has the rights to install and remove applications.
2. To remove the Email Sending Daemon program, perform the following steps:
   a. Navigate to the directory where the Email Sending Daemon program was installed and, if it is running, then stop the Email Sending Daemon using the following command:

      ```
      ./tomcat-ctl.sh stop
      ```

   b. Navigate to the parent directory where the Email Sending Daemon program was installed and remove the Email Sending Daemon program directory using the following command:

      ```
      rm -rf esd
      ```

3. To remove the Bounce Handler Daemon program, perform the following steps:
   a. Navigate to the directory where the Bounce Handler Daemon program was installed and, if it is running, then stop the Bounce Handler Daemon using the following command:

      ```
      ./bin/bhd-ctl.sh stop
      ```

   b. Navigate to the parent directory where the Bounce Handler Daemon program was installed and remove the Bounce Handler Daemon program directory using the following command:

      ```
      rm -rf bhd
      ```

4. To remove the Click Through Daemon program, perform the following steps:
   a. Navigate to the directory where the Click Through Daemon program was installed and, if it is running, then stop the Click Through Daemon using the following command:

      ```
      ./tomcat-ctl.sh stop
      ```

   b. Navigate to the parent directory where the Click Through Daemon program was installed and remove the Click Through Daemon program directory using the following command:

      ```
      rm -rf ctd
      ```

Installing the Java Runtime Environment

Install the appropriate maintenance release of the Java Runtime Environment (JRE).

Note: Ensure that there are no spaces in the JRE installation path.

Note: Platform, database, and other certifications for Siebel are found on My Oracle Support. For help searching for certifications, see *How to Check the Certification Matrix in the New My Oracle Support Site* (KB871388).

Verifying That the Object Manager Is Enabled and Running

The object manager component (such as Marketing) to which you connect must be enabled and running on the Siebel Server. To verify this, perform the following task.

To verify that the Object Manager component is enabled and running

1. Log in to the Siebel Server.
2. Navigate to the Administration - Server Configuration screen, Servers, and then the Components view.
3. Query for the alias name, and make sure the component has a status of Online or Running.

   For example, the Marketing component for the English language version has an alias name of SMObjMgr_enu.

Installing the Email Marketing Server

You use the Email Marketing Daemon installation program to install the Email Marketing Server. This program is part of the Siebel Enterprise Installation media.

You can find installers for all platforms and Siebel Email Marketing daemons on the installation media. The daemons include:

- Email Sending Daemon (ESD)
- Bounce Handler Daemon (BHD)
- Click Through Daemon (CTD)

Note: When you install these on a Microsoft Windows platform, the components must be installed on a drive with enough space to handle the size of the log files.

To install Email Marketing, navigate to the `mde` folder in the appropriate operating system folder.

Follow these steps:

1. In the `mde` folder, launch the installation program:
   - Windows: `runInstaller.bat`
   - AIX or Linux: `runInstaller.sh`
2. Select the correct installation directory and select **Next**.
3. Select all required Email Marketing daemon components that you want to install on the machine.
4. Select **Next**.
5. Select **Install**.

Install EMS Components Using the MDE Installer

Email Marketing Server (EMS) is installed by using the MDE installer. The MDE installer is available for Windows, Linux, and AIX, and supports graphical installations. A separate JDK or JRE installation is not required: the installer installs the JRE required by EMS as part of the installation.

Use the MDE installer to install one or more EMS components. The installer provides the following component selections.

Installer selection	Default selection	Purpose
Siebel Email Marketing - BHD	Selected	Bounce Handler Daemon
Siebel Email Marketing - CTD	Selected	Click Through Daemon
Siebel Email Marketing - ESD	Selected	Email Sending Daemon
Siebel Email Marketing - WSD	Selected	Web Survey Daemon

Install EMS in Graphical Mode

1. After downloading the EMS installer, open the folder for the appropriate operating system (Windows, Linux, or AIX), then open the mde folder.
2. Start the installer by running runInstaller.bat on Windows or ./runInstaller.sh on Linux or AIX. The command opens the installer GUI
3. Enter the EMS home location where the selected components, configuration files, and bundled JRE will be installed. For an upgrade, select the existing installation path from the list or click Browse to locate it.
4. Click Next. The component selection page lists the four EMS components. All components and their configuration options are selected by default. Select one or more components to install; uncheck the checkbox for any component that you do not want to install.
5. Click Next. For each selected ESD, CTD, and WSD component, enter the configuration values shown in the following table. BHD does not require these port and certificate-store values.

Configuration Fields

The installer writes the values to the configuration files identified in the following table.

Installer field	Purpose	Configuration file(s)
HTTPS Redirect Port	HTTPS connector port and HTTP-to-HTTPS redirect target.	<EMS_HOME>/<component>/conf/server.xml (ESD, CTD, and WSD) <EMS_HOME>/wsd/webapps/websurveys/WEB-INF/conf/axis2.xml (WSD only)
HTTP Connection Port	Port used by the HTTP connector.	<EMS_HOME>/<component>/conf/server.xml (ESD, CTD, and WSD) <EMS_HOME>/wsd/webapps/websurveys/WEB-INF/conf/axis2.xml (WSD only)
Shutdown Port	Tomcat shutdown listener port.	<EMS_HOME>/<component>/conf/server.xml (ESD, CTD, and WSD)
Keystore Location	Full path to the server certificate keystore used for HTTPS.	<EMS_HOME>/<component>/conf/server.xml (ESD, CTD, and WSD)
Keystore Password	Password for the server certificate keystore.	<EMS_HOME>/<component>/conf/server.xml (ESD, CTD, and WSD)
Truststore Location	Full path to the truststore used for client-certificate validation when configured.	<EMS_HOME>/<component>/conf/server.xml (ESD, CTD, and WSD)

Installer field	Purpose	Configuration file(s)
Truststore Password	Password for the truststore.	<EMS_HOME>/<component>/conf/server.xml (ESD, CTD, and WSD)

> **Note: If configuration is skipped.** If you skip configuration for a component, the installer does not replace the listed template variables. Before starting the component, manually replace these variables in <EMS_HOME>/<component>/conf/server.xml for ESD, CTD, and WSD. For WSD, also replace $HTTP_CONNECTOR_PORT and $HTTPS_REDIRECT_PORT in <EMS_HOME>/wsd/webapps/websurveys/WEB-INF/conf/axis2.xml.

6. Ensure that the HTTP, HTTPS, and shutdown port numbers are valid (from 1 through 65535), unique, and available for use.
7. Enter valid port numbers from 1 through 65535. The HTTP, HTTPS, and shutdown ports must be unique and available for use.
8. After entering the values, review the selected options on the Summary page. To save a response file for a future silent installation, click Save Response File.
9. Click Install. The installer installs the selected components and the required JRE.

   When installation completes, click Next. The installer displays the installer log file name and path; review this log if an error occurs during installation.
10. Click Close to exit the installer.

UNIX prerequisite. The UNIX MDE installer requires a graphical user interface. A VNC session is one supported way to make that interface available on a remote UNIX host.

Windows service note. On Windows, the installer creates a Windows Service entry for each installed component. After confirming the component configuration, open Windows Services and start the required component service.

Uninstall EMS

1. Navigate to the EMS installation directory, then open the uninstall folder.
2. Run uninstaller.exe on Windows or ./uninstaller.sh on Linux or AIX.
3. Follow the prompts to uninstall all installed EMS components.

Windows service note. On Windows, the uninstaller removes the Windows Service entries for the installed EMS components.

Install EMS in Silent Mode

Create a response file before starting a silent installation. The response file records the EMS home location, installation type, selected components, and release version.

Run the silent installer

On Windows, run the following command from the mde folder:

```
runInstaller.bat -silent -responseFile <response_file_path>
```

On Linux or AIX, run the equivalent command from the mde folder:

```
./runInstaller.sh -silent -responseFile <response_file_path>
```

Response file format:

With Configuration:

```
SIEBEL_HOME_LOCATION=<PATH WHERE EMS SHOULD BE INSTALLED>
INSTALLATION_TYPE=<FRESH OR UPGRADE>
SELECTED_COMPONENTS=<COMMA-SEPARATED LIST OF COMPONENTS TO INSTALL>
SELECTED_CONFIGURATION_COMPONENTS=<COMMA-SEPARATED LIST OF COMPONENTS TO CONFIGURE>
POST_INSTALLATION_PERFORMED="NO"
VERSION=<VERSION NUMBER>
[Siebel Email Marketing - CTD Configuration]
HTTPS_REDIRECT_PORT=<HTTPS_REDIRECT_PORT>
HTTP_CONNECTION_PORT=<HTTP_CONNECTION_PORT>
SHUTDOWN_PORT=< SHUTDOWN_PORT>
KEYSTORE_LOCATION=<KEYSTORE_LOCATION>
KEYSTORE_PASSWORD=<ENCRYPTED KEYSTORE_PASSWORD>
TRUSTSTORE_LOCATION=<TRUSTSTORE_LOCATION>
TRUSTSTORE_PASSWORD==<ENCRYPTED TRUSTSTORE_PASSWORD>
[Siebel Email Marketing - ESD Configuration]
HTTPS_REDIRECT_PORT=<HTTPS_REDIRECT_PORT>
HTTP_CONNECTION_PORT=<HTTP_CONNECTION_PORT>
SHUTDOWN_PORT=< SHUTDOWN_PORT>
KEYSTORE_LOCATION=<KEYSTORE_LOCATION>
KEYSTORE_PASSWORD=<ENCRYPTED KEYSTORE_PASSWORD>
TRUSTSTORE_LOCATION=<TRUSTSTORE_LOCATION>
TRUSTSTORE_PASSWORD==<ENCRYPTED TRUSTSTORE_PASSWORD>
[Siebel Email Marketing - WSD Configuration]
HTTPS_REDIRECT_PORT=<HTTPS_REDIRECT_PORT>
HTTP_CONNECTION_PORT=<HTTP_CONNECTION_PORT>
SHUTDOWN_PORT=< SHUTDOWN_PORT>
KEYSTORE_LOCATION=<KEYSTORE_LOCATION>
KEYSTORE_PASSWORD=<ENCRYPTED KEYSTORE_PASSWORD>
TRUSTSTORE_LOCATION=<TRUSTSTORE_LOCATION>
TRUSTSTORE_PASSWORD==<ENCRYPTED TRUSTSTORE_PASSWORD>
```

Without Configuration:

```
SIEBEL_HOME_LOCATION=<PATH WHERE EMS SHOULD BE INSTALLED>
INSTALLATION_TYPE=<FRESH OR UPGRADE>
SELECTED_COMPONENTS=<COMMA-SEPARATED LIST OF COMPONENTS TO INSTALL>
POST_INSTALLATION_PERFORMED="NO"
VERSION=<VERSION NUMBER>
```

Use the following valid values:

- INSTALLATION_TYPE: Fresh or Upgrade.
- SELECTED_COMPONENTS: Siebel Email Marketing - BHD; Siebel Email Marketing – CTD, Siebel Email Marketing – ESD, or Siebel Email Marketing - WSD.
- SELECTED_CONFIGURATION_COMPONENTS: Siebel Email Marketing - CTD Configuration, Siebel Email Marketing - ESD Configuration, Siebel Email Marketing – WSD Configuration
- When selecting more than one component, separate the component names with commas.
- VERSION: the release version of the EMS installer being used.

Response file examples:

New installation with all four components with no configuration:

```
SIEBEL_HOME_LOCATION="C:\EMS_25.6"
INSTALLATION_TYPE="Fresh"
SELECTED_COMPONENTS="Siebel Email Marketing - BHD,Siebel Email Marketing - CTD,Siebel Email Marketing -
 ESD,Siebel Email Marketing - WSD"
POST_INSTALLATION_PERFORMED="NO"
VERSION="25.6.0.0.0"
```

Example for New installation with configuration CTD and ESD:

```
[Installation Details]
INSTALLATION_TYPE="Fresh"
SIEBEL_HOME_LOCATION="C:\EMS_26_8"
SELECTED_COMPONENTS="Siebel Email Marketing - CTD,Siebel Email Marketing - ESD"
SELECTED_CONFIGURATION_COMPONENTS="Siebel Email Marketing - CTD ,Siebel Email Marketing - ESD"
[Siebel Email Marketing - CTD Configuration]
HTTPS_REDIRECT_PORT=6000
HTTP_CONNECTION_PORT=6001
SHUTDOWN_PORT=6002
KEYSTORE_LOCATION=C:/EMS_26_8
KEYSTORE_PASSWORD=aEdDWStVLy9CMUFCRExHalE0OTFtWHc2cERKVUFJRlNkTnZEMGxJK1ZFNnB6WStWUjdQTzlnPT1TRk9TV09IZEM5TnJuWU5SZG
TRUSTSTORE_LOCATION=C:/EMS_26_8
TRUSTSTORE_PASSWORD=aEdDWStVLy9CMUFCRExHalE0OTFtWHc2cERKVUFJRlNkTnZEMGxJK1ZFNnB6WStWUjdQTzlnPT1TRk9TV09IZEM5TnJuWU5S
[Siebel Email Marketing - ESD Configuration]
HTTPS_REDIRECT_PORT=5000
HTTP_CONNECTION_PORT=5001
SHUTDOWN_PORT=5002
KEYSTORE_LOCATION=C:/EMS_26_8
KEYSTORE_PASSWORD=aEdDWStVLy9CMUFCRExHalE0OTFtWHc2cERKVUFJRlNkTnZEMGxJK1ZFNnB6WStWUjdQTzlnPT1TRk9TV09IZEM5TnJuWU5SZG
TRUSTSTORE_LOCATION=C:/EMS_26_8
TRUSTSTORE_PASSWORD=aEdDWStVLy9CMUFCRExHalE0OTFtWHc2cERKVUFJRlNkTnZEMGxJK1ZFNnB6WStWUjdQTzlnPT1TRk9TV09IZEM5TnJuWU5S
```

Note: You can run the following command to generate the encrypted password. Open command prompt and run the following. Java should be part of the class path.

```
<build_location>\mde\ext\jlib>java -jar EncryptString.jar <passwordtext>
```

Default HTTPS Configuration for Email Sending Daemon, Click Through Daemon and Web Survey Daemon

If you do not select the configuration option during installation, you must manually replace the following template variables with the appropriate values in the files listed in the table under *Configuration Fields* in *Install EMS Components Using the MDE Installer*.

Configuration Fields: $HTTP_CONNECTOR_PORT, $HTTPS_REDIRECT_PORT, $SHUTDOWN_PORT, $KEYSTORE_FILE_VALUE, $KEYSTORE_PASSWORD, $TRUSTSTORE_FILE_VALUE, and $TRUSTSTORE_PASSWORD.

For WSD, they must also update $HTTP_CONNECTOR_PORT and $HTTPS_REDIRECT_PORT in axis2.xml.

Updated Configuration Files

- For ESD, CTD, and WSD, the installer updates conf/server.xml with the supplied port and certificate-store values.
- For WSD only, the installer also updates webapps/websurveys/WEB-INF/conf/axis2.xml with the supplied HTTP and HTTPS transport receiver ports.

Import the Siebel Web Server CA Certificate

When an EMS component must trust the certificate authority used by the Siebel Web server, import the Siebel Web Server CA certificate file into the keystore created for that component.

Run the keytool command from the bin directory of the JRE bundled with EMS. The bundled JRE is located under the EMS home directory.

Run the keytool command

Windows:

```
<EMS_HOME>\jre\bin\keytool -import -alias <alias_name> -file <certificate_file_name> -keystore
<name of the keystore with path> -storepass <keystore_password>
```

UNIX:

```
<EMS_HOME>/jre/bin/keytool -import -alias <alias_name> -file <certificate_file_name> -keystore
<name of the keystore with path> -storepass <keystore_password>
```

Definations:

- <alias_name> is the name used to identify the imported certificate; use a meaningful, unique alias for the EMS host.
- <certificate_file_name> is the certificate authority certificate file provided for the Siebel Web server.
- <name of the keystore with path> is the full path and name of the keystore file.
- <keystore_password> is the password for that keystore file.

Validation Checklist

- The selected EMS components installed successfully and start without configuration errors.
- Each applicable conf/server.xml file contains the intended HTTP, HTTPS, shutdown, keystore, and truststore values.
- For WSD, webapps/websurveys/WEB-INF/conf/axis2.xml contains the intended HTTP and HTTPS transport receiver ports.
- No unresolved placeholders, such as $HTTPS_REDIRECT_PORT, $HTTP_CONNECTOR_PORT, $SHUTDOWN_PORT, $KEYSTORE_FILE_VALUE, $KEYSTORE_PASSWORD, $TRUSTSTORE_FILE_VALUE and $TRUSTSTORE_PASSWORD remain in the deployed configuration files.
- The EMS flow operates successfully through the configured HTTPS endpoints.

Roadmap for Configuring Email Marketing Daemons

This topic contains the information that you need to configure Email Marketing Server and the Siebel Marketing application so that they can communicate with each other. To configure the Email Marketing daemons, perform the following tasks and processes:

- *Identifying the Web Service Endpoint URL*
- *Process of Configuring the Email Sending Daemon*
- *Process of Configuring the Bounce Handler Daemon*
- *Process of Configuring the Click Through Daemon*
- *Configuring Email Marketing Components for HTTPS Communications*
- *(Optional) Enabling TLS for Communications Between the Email Sending Daemon and the SMTP Server*

Before You Begin

Many of the configuration values you must specify for the Email Marketing daemons are specified in the properties file for the component, for example, the URL used to connect the Email Sending Daemon to Siebel Marketing, the location of the Siebel File System, and various other parameters that control the behavior of the Email Marketing components.

The component properties files, esd.properties, bhd.properties, and ctd.properties, are located in the *ESD_root*, *BHD_root*, and *CTD_root* installation directories, respectively. For additional information about the properties files, see *New and Changed Properties in the esd.properties Configuration File*.

Identifying the Web Service Endpoint URL

The Email Marketing components use the Web service endpoint URL to connect with Siebel Marketing. This topic describes how to identify the Web service endpoint URL. You require the URL when configuring each of the Email Marketing daemons.

This task is a step in *Roadmap for Configuring Email Marketing Daemons*.

To identify the Web services endpoint URL

1. Log in to Siebel Server.
2. Navigate to the Administration - Web Services screen, then the Inbound Web Services view.
3. In the Name field, query for the WebMarketing Web service.
4. In the Service Ports applet, copy the contents of the Address field.

> **Note:** If the Web services endpoint URL uses the HTTPS protocol, then you must configure the Email Marketing components for HTTPS communications with Siebel Marketing, as described in *Configuring Email Marketing Components for HTTPS Communications*.

Process of Configuring the Email Sending Daemon

This topic contains the configuration tasks you need to perform so that the Marketing application can communicate with the Email Sending Daemon. Additionally, you must configure the Email Sending Daemon to read files from the Marketing File System and communicate with the outbound Mail Transfer Agents. During these tasks, you have an opportunity to verify that the Email Sending Daemon has been correctly installed and configured. For information about this test, see *Process of Testing the Email Marketing Components with Siebel Marketing*.

This process is a step in *Roadmap for Configuring Email Marketing Daemons*.

> **CAUTION:** During this process, do not start the Email Sending Daemon until told to do so. If you do accidentally start it, then stop it immediately before proceeding.

To configure the Email Sending Daemon to connect to the Marketing Server, perform the following tasks:

1. *Identifying the Outbound Mail Transfer Agents for the Email Sending Daemon*
2. *Configuring the Email Sending Daemon to Access the Marketing File System*

3. *Configuring the SOAP Communications Port*
4. *Configuring Web Services Properties for the Email Sending Daemon*
5. *Verifying the Email Sending Daemon Installation*
6. *Configuring the Marketing Application to Connect to the Email Sending Daemon*
7. *Configuring the Email Address Headers for the Email Marketing Server*

Identifying the Outbound Mail Transfer Agents for the Email Sending Daemon

The Email Sending Daemon (ESD) must have one or more outbound Mail Transfer Agents (MTAs) to deliver the email over the Internet. If you specify multiple MTAs, then the ESD uses the additional MTAs as backups. In the esd.properties file, you specify the names of your MTAs. When the ESD starts, it uses the first MTA on the list. When an MTA fails, the ESD uses the next MTA on the list. To use the first MTA again, you must restart the ESD, usually by rebooting the server.

This task is a step in *Process of Configuring the Email Sending Daemon*.

To identify the outbound Mail Transfer Agent for ESD

1. Determine the hostname of the outbound Mail Transfer Agent.
2. Open the esd.properties file in a text editor such as WordPad (Windows) or vi (UNIX).
3. Locate the string esd.mailServers.
4. In the string esd.mailServers, replace "CHANGE_ME" with the hostname of the outbound Mail Transfer Agent. If there is more than one, then separate them with commas.
5. Save your changes.

Configuring the Email Sending Daemon to Access the Marketing File System

The Email Sending Daemon needs to access the Siebel Marketing File System to load the email message content (generated from the email offers and attachments) and the subwaves of contacts and prospects generated for a campaign wave. This topic describes how to configure the Email Sending Daemon to access the Siebel Marketing File System.

This task is a step in *Process of Configuring the Email Sending Daemon*.

Configuring the Email Sending Daemon to Access the Marketing File System on a Windows Server

The following procedure describes how to configure the Email Sending Daemon to access the Marketing File System on a Windows Server.

To configure the ESD to access the Marketing File System on a Windows Server

1. Log in to Siebel Server.
2. Navigate to the Administration - Server Configuration screen, Servers, and then the Parameters view.
3. Query for Marketing File System.

   Write down the value of this parameter to use later in this task.
4. Identify the Windows share name for this directory.

Write down this name to use later in this task.

5. Open the esd.properties file with a text editor, such as WordPad.
6. In the string esd.mountPoint, replace "CHANGE_ME" with the following path, using the share name determined in Step 4:

   `\\\\siebel_server_hostname\\marketing_file_system_share_name`

   Use two backslashes for each standard single backslash when defining this path. For example, `c:\Windows` is `c:\\Windows`.

   > **CAUTION:** If the Marketing File System is on the same server as the Email Sending Daemon, then use the complete path to the Marketing File System instead of the share name to avoid potential permission issues.

7. Save your changes to the esd.properties file.

Configuring the Email Sending Daemon to Access the Marketing File System on UNIX

The following procedure describes how to configure the Email Sending Daemon to access the Marketing File System on a UNIX server.

To configure the ESD to access the Marketing File System on a UNIX Server

1. Log in to Siebel Server.
2. Navigate to the Administration - Server Configuration screen, Servers, and then the Parameters view.
3. Query for Marketing File System.

   Write down the value of this parameter to use later in this task.
4. Determine if this directory is exported through NFS. If it is not, then export it.
5. Open the esd.properties file with a text editor, such as vi.
6. On the Email Sending Daemon server, make sure the Marketing File System is NFS mounted. If it is not, then mount it at this time.

   Write down the full path name of the mounted Marketing File System to use later in this task.
7. In the string esd.mountPoint, at the end of the string, add the Marketing File System NFS mount directory.
8. Save your changes to the esd.properties file.

Configuring the SOAP Communications Port

The Marketing application on Siebel Server communicates with the Email Sending Daemon using the SOAP protocol, which uses HTTP requests. You must configure the Email Sending Daemon to listen for these HTTP requests on a specific port. This task is described in the following procedure.

This task is a step in *Process of Configuring the Email Sending Daemon*.

To configure the SOAP communications port

1. Consider what port number you want to use to service the SOAP commands (HTTP requests) on the Email Sending Daemon.

Because this HTTP server does not service standard HTTP requests such as Web pages, any port can be used (even the default of 8090). Write down the port number you decide to use.

2. At the following location, open the server.xml file in a text editor:

   ```
   esd_installation_directory\config\server.xml
   ```

3. Locate the XML tag Connector by searching for the following phrase:

   ```
   Define a non-SSL Coyote HTTP/1.1 Connector
   ```

4. Identify the value of the port attribute and, if necessary, change it to the value you chose in Step 1.

   The default value is 8090.

5. Save the change.

   You need this port number again in a subsequent task.

Configuring Web Services Properties for the Email Sending Daemon

You can configure the Web services properties for the Email Sending Daemon by changing the properties in the esd.properties file.

This task is a step in *Process of Configuring the Email Sending Daemon*.

To configure the Web services properties for the Email Sending Daemon

1. Navigate to the esd.properties file in the *ESD_root* installation directory.
2. Open the esd.properties file in a text editor.
3. Change the Web services properties in the esd.properties file as indicated in the following table.

Property	Description
Web Service URL	esd.handler.webservice.url=CHANGE_ME Replace CHANGE_ME with the URL obtained in *Identifying the Web Service Endpoint URL*.
Web Service username	esd.handler.webservice.username=CHANGE_ME Replace CHANGE_ME with the Administration user name.
Web Service password	esd.handler.webservice.password=CHANGE_ME Replace CHANGE_ME with the Administration user password.

4. (Optional) If you choose to encrypt the Web service username and password using the JMangle algorithm, then set the JAR_PATH environment variable in the jmangle.bat file. The jmangle.bat file is located in the *ESD_root* `/bin` directory.

   Make sure that the value you specify for the JAR_PATH reflects the directory structure of the *ESD_root* `/bin` directory. For example:

   ```
   JAR_PATH=../common/lib/Siebel.jar;../common/lib/common.jar
   ```

Note: If the Web services endpoint URL uses the HTTPS protocol, then you must configure the Email Marketing components for HTTPS communications with Siebel Marketing as described in *Configuring Email Marketing Components for HTTPS Communications*. If you want to enable Transport Layer Security (TLS) for communications between the Email Sending Daemon and the Simple Mail Transfer Protocol (SMTP) server, follow the instructions in *(Optional) Enabling TLS for Communications Between the Email Sending Daemon and the SMTP Server*.

Verifying the Email Sending Daemon Installation

At this point, you can test the installation of the Email Sending Daemon. To verify that the installation was successful, you start the Email Sending Daemon and then perform several verification steps. For information about testing how the Email Marketing components and the Marketing application work together, see *Process of Testing the Email Marketing Components with Siebel Marketing*.

This task is a step in *Process of Configuring the Email Sending Daemon*.

Starting the Email Sending Daemon on a Windows Server

The following procedure describes how to start the Email Sending Daemon on a Windows server.

To start the Email Sending Daemon on a Windows Server

1. From the Start menu, choose Settings and then the Control Panel menu item.
2. In Control Panel, choose Administrative Tools and then Services.
3. Right-click the Email Sending Daemon service and select Start.

Starting the Email Sending Daemon on a UNIX Server

The following procedure describes how to start the Email Sending Daemon on a UNIX server.

To start the Email Sending Daemon on a UNIX server

1. Open a window and navigate to the Email Sending Daemon install directory.
2. Enter and run the following command:

   ```
   ./tomcat-ctl.sh start &
   ```

3. Optionally, you can enter and run the following commands:

```
./tomcat-ctl.sh start &; tail -f logs/esd.log
```

> **Note:** The first command (`./tomcat-ctl.sh start &`) launches the daemon. The second command (`tail -f logs/esd.log`) displays output to the esd log as it is running without generating a read lock on the file. A read lock would prevent these commands from working.

Verifying the Email Sending Daemon Installation

The following procedure describes how to verify the Email Sending Daemon installation.

To verify the Email Sending Daemon installation

1. Open the esd_InstallLog.log file located in the esd installation directory and read the summary at the start of the file.

   Make sure it says that the installation was successful with no warnings or errors. If there are warnings or errors, then you must identify the cause and fix the error.
2. Verify that the Email Sending Daemon Windows Service or UNIX process runs and stays running without an error message.
3. Verify that a esd.log file exists in the following directory:

   ***esd installation directory*\logs\esd.log**
4. Verify that the following text is in the esd.log file:

   ```
   INFO OnPremiseAppListener ESD is licensed.
   ```
5. Make sure there are no ERROR or WARN level messages in the esd.log file.
6. Confirm that the Email Sending Daemon Web container is running.

   > **Note:** You need the port number that you obtained in *Configuring the SOAP Communications Port*.

   Verify that you can open the following Web page without error using Internet Explorer:

   http://*email_sending_daemon_server_hostname*:*email_sending_daemon_soap_port*/esd/soaprpc

Configuring the Marketing Application to Connect to the Email Sending Daemon

This topic describes how to set up the Marketing application to connect to the Email Sending Daemon.

This task is a step in *Process of Configuring the Email Sending Daemon*.

To configure the Marketing application to connect to the Email Sending Daemon

1. Open Internet Explorer and navigate to the Siebel Marketing Server login screen. For example:

   http://*marketing server hostname*/marketing_enu

2. Log in as the server administrator.
3. Navigate to the Administration - Web Services screen, and then the Outbound Web Services view.
4. In the Outbound Web Services list, in the Name field, query for SendMailingService.
5. In the Service Ports list, in the SendMailing record, perform the following steps:
    a. Obtain the Web Port Id identified in *Configuring the SOAP Communications Port*.
    b. In Address field, change the URL using the following syntax:

    ```
    http://esd server hostname:esd web port/esd/soaprpc
    ```

6. Click Clear Cache.
7. Navigate to the Administration - Marketing screen, and then the Servers view.
8. In the Servers list, in the Name field, query for Email Marketing Server.
9. In the parameters list, locate the Email Sending Daemon (ESD) parameter, and verify that the Outbound Web Service Port field contains SendMailing.

Configuring the Email Address Headers for the Email Marketing Server

This topic describes how to configure the From and Reply-To headers for outbound email sent using the Email Sending Daemon.

This task is a step in *Process of Configuring the Email Sending Daemon*.

To configure the From Address and Reply-To Address for the Email Marketing Server

1. Navigate to the Administration - Marketing screen, and then the Servers view.
2. In the Servers list, in the Name field, query for Email Marketing Server.
3. In the parameters list, in the Value field, update the values as shown in the following table.

Parameter Type	Value
From Address (From header)	*email address* An address to use as the From header for outgoing emails.
Reply To Address (Reply-To header)	*email address* An address to use as the Reply-To header for outgoing emails.

Process of Configuring the Bounce Handler Daemon

The Bounce Handler Daemon notifies the Marketing Component Group that it has processed asynchronous bounces and needs to pass these bounce details to the Marketing Component Group. This topic contains the information that you need to configure the Bounce Handler Daemon to communicate with the Marketing Component Group.

This process is a step in *Roadmap for Configuring Email Marketing Daemons*.

To configure the Bounce Handler Daemon, perform the following tasks:

- *Verifying the Bounce Handler Daemon Installation*
- *Configuring the Bounce Address of the SMTP Envelope*
- *Configuring Web Services Properties for the Bounce Handler Daemon*
- Review *About Creating Classification Rules for Bounce Messages*
- *Configuring How the Bounce Handler Daemon Classifies Bounce Messages*

Note: During this process, do not start the Bounce Handler Daemon until told to do so. If you do accidentally start it, then stop it immediately before proceeding.

Verifying the Bounce Handler Daemon Installation

To verify that the Bounce Handler Daemon installation was successful, you start the Bounce Handler Daemon and then perform installation tests. This topic describes these tasks. For information about testing how the Email Marketing components and the Marketing Component Group work together, see *Process of Testing the Email Marketing Components with Siebel Marketing*.

This task is a step in *Process of Configuring the Bounce Handler Daemon*.

Starting the Bounce Handler Daemon on a Windows Server

To start the Bounce Handler Daemon on a Windows server, perform the steps in the following procedure.

To start the Bounce Handler Daemon on a Windows Server

1. From the Start menu, choose Settings and then the Control Panel menu item.
2. In Control Panel, choose Administrative Tools and then Services.
3. Right-click the bhd service and select Start.

Starting the Bounce Handler Daemon on a UNIX Server

To start the Bounce Handler Daemon on a UNIX server, perform the steps in the following procedure.

To start the Bounce Handler Daemon on a UNIX server

1. Open a window and navigate to the Bounce Handler Daemon install directory.
2. Enter and run the following command:

   ```
   ./bin/bhd-ctl.sh start &
   ```

3. Optionally, you can enter and run the following commands:

```
./bin/bhd-ctl.sh start &; tail -f bhd.log
```

The first command (./bin/bhd-ctl.sh start &) launches the daemon. The second command (tail -f bhd.log) displays output to the bhd log as it is running without generating a read lock on the file. A read lock would prevent these commands from working.

Verifying the Bounce Handler Daemon Installation

To verify the Bounce Handler Daemon installation, perform the steps in the following procedure.

To verify the Bounce Handler Daemon installation

1. Verify that the Bounce Handler Daemon Windows Service or UNIX process is running and stays running without an error message.
2. Open the bhd_InstallLog.log file (found in the *bhd installation directory*) and read the Summary at the start of the file. Make sure it says that the installation was successful with no warnings or errors. If there are warnings or errors, then you must identify the cause and fix the error.
3. Verify that a bhd.log file exists in the following directory:

   ***bhd installation directory*\logs\bhd.log**
4. Verify that the following text is in the bhd.log file:

   INFO OnPremiseMain BHD is licensed.
5. Make sure there are no ERROR or WARN level messages in the bhd.log file.
6. From a command prompt window, telnet to the Bounce Handler Daemon SMTP port (25) (for example, telnet bhd.example.com 25), wait for a greeting, and then enter the word quit and press ENTER. Your telnet session then ends.

Configuring the Bounce Address of the SMTP Envelope

This topic describes how to configure the hostname that you use to create the bounce address of the SMTP envelope. This bounce address is the email address that receives bounced emails. The hostname you use as the bounce address is the host name of the Bounce Handler Daemon.

This task is a step in *Process of Configuring the Bounce Handler Daemon*.

To configure the SMTP envelope bounce address

1. Navigate to the Siebel Marketing login screen at http://*marketing application hostname*/marketing_enu
2. Log in as the server administrator.
3. Navigate to the Administration - Marketing screen and then the Servers view.
4. In the Servers list, in the Name field, query for Email Marketing Server.
5. In the parameters list, in the Value field, update the values as shown in the following table.

Parameter Type	Value
Bounce Handler Daemon (BHD)	*bhd server hostname*

Parameter Type	Value

Configuring Web Services Properties for the Bounce Handler Daemon

You can configure the Web Services properties for the BHD by changing the properties in the bhd.properties file. This topic describes this task.

This task is a step in *Process of Configuring the Bounce Handler Daemon*.

To configure Web services properties for the Bounce Handler Daemon

1. Navigate to the bhd.properties file in the *BHD_root* installation directory.
2. Open the bhd.properties file in a text editor such as WordPad (Windows) or vi (UNIX).
3. Change the Web services properties in the bhd.properties file as indicated in the following table.

Property	Description
Web Service URL	bhd.webservice.url=CHANGE_ME Replace CHANGE_ME with the URL obtained in *Identifying the Web Service Endpoint URL*.
Web Service username	bhd.webservice.username=CHANGE_ME Replace CHANGE_ME with the Administration user name.
Web Service password	bhd.webservice.password=CHANGE_ME Replace CHANGE_ME with the Administration user password.

4. (Optional) If you choose to encrypt the Web service username and password using the JMangle algorithm, then set the JAR_PATH environment variable in the jmangle.bat file. The jmangle.bat file is located in the *BHD_root* `/bin` directory.

   Make sure that the value you specify for the JAR_PATH reflects the directory structure of the *BHD_root* `/bin` directory. For example:

   ```
   ../lib/Siebel.jar;../lib/common.jar
   ```

Note: If the Web services endpoint URL uses the HTTPS protocol, then you must configure the Email Marketing components for HTTPS communications with Siebel Marketing as described in *Configuring Email Marketing Components for HTTPS Communications*.

About Creating Classification Rules for Bounce Messages

You can extend the Bounce Handler Daemon's ability to recognize different categories and types of bounces by creating rules that specify how values in the delivery status notification messages received for undelivered emails are to be classified. You create new bounce classification rules in the following files, which are located in the *bhd_install_home* `/config` directory:

- **customDCBounceConfig.** Used to define rules for classifying bounce messages by matching specified string values in the Diagnostic Code entry of the delivery status notification message
- **customFromBounceConfig.** Used to define rules for classifying bounce messages by matching specified string values in the From header of the delivery status notification message
- **customSubjectBounceConfig.** Used to define rules for classifying bounce messages by matching specified string values in the Subject header of the delivery status notification message

You can create as many bounce message classification rules as required for your Siebel Marketing environment. If you create custom classification rules, then bounce messages are classified using these custom rules. If you choose not to create custom classification rules, or if the Email Marketing Server cannot find a match for an undelivered email in the custom classification rules you create, then bounce messages are classified using standard Siebel Marketing functionality.

Note that you cannot customize the following Bounce Handler Daemon processing functionality:

- If the delivery status notification message for an undelivered email contains a Diagnostic Code entry, then entries in the customFromBounceConfig and customSubjectBounceConfig files are not processed.
  If the delivery status notification message does not contain a Diagnostic Code entry, then entries in the customFromBounceConfig file take precedence over entries in the customSubjectBounceConfig file.
- If the delivery status notification message for an undelivered email contains a From header which includes a value equal to MAILER-DAEMON, then entries in the customFromBounceConfig and customSubjectBounceConfig files are not processed.
- If the delivery status notification message for an undelivered email contains an Action field which includes a value equal to Failed, then entries in the customFromBounceConfig and customSubjectBounceConfig files are not processed.

Configuring How the Bounce Handler Daemon Classifies Bounce Messages

You can configure how the Bounce Handler Daemon classifies bounce messages by defining custom classification rules. This topic describes how to perform this configuration task. For information about the files used to define custom classification rules, see *About Creating Classification Rules for Bounce Messages*.

This task is a step in *Process of Configuring the Bounce Handler Daemon*.

The following procedure describes how to create custom rules for classifying bounce messages.

> **Note:** The Bounce Handler Daemon processes classification rules in the order in which they appear in a custom*xx*BounceConfig file and, when it encounters a match for a bounce, it does not evaluate rules defined further down in the file. Therefore, enter classification rules in a custom*xx*BounceConfig file in order of importance.

To define classification rules for bounce messages

1. Navigate to the *bhd_install_home* `/config` directory.
2. Using a text editor, edit the appropriate custom*xx*BounceConfig file.

   The file you edit will vary according to whether you want to create a classification rule by matching values in the Diagnostic Code entry, or the From header, or the Subject header of the delivery status notification message for the undelivered email. For additional information about the custom*xx*BounceConfig files, see *About Creating Classification Rules for Bounce Messages*.
3. To create a classification rule by matching string values in the Diagnostic Code entry of the delivery status notification message, add the entries shown in the following table to the customDCBounceConfig file.

Parameter	Value
DIAGNOSTICCODEDATA=	The diagnostic code you want to match. Either enter the exact string you want to match, or enter the value in the form of a regular expression. For information on regular expression notation, see the Java 2 Platform Standard Edition 5.0 API Specification at *http://docs.oracle.com/javase/1.5.0/docs/api/java/util/regex/Pattern.html#sum* Information on regular expressions is also available at *http://www.vogella.com/articles/JavaRegularExpressions/article.html*
CODE=	The value you want to assign bounce messages that contain the diagnostic code specified in the DIAGNOSTICCODEDATA parameter.
HARD=	Enter either Yes or No to indicate whether or not bounce messages that include the diagnostic code specified in the DIAGNOSTICCODEDATA parameter are to be classified as hard bounces. A hard bounce refers to an email that cannot ever be delivered. A soft bounce refers to an email that cannot be delivered at present, but that can possibly be delivered in the future.

For example, you might want to classify bounce messages that include the following diagnostic code:

```
Diagnostic-Code: smtp; 5.4.7 - Delivery expired (message too old) 421-'4.7.0
[TS01] Messages from 155.91.38.221 temporarily deferred due to user complaints -
4.16.55.1; see http://postmaster.yahoo.com/421-ts01.html' (delivery attempts: 1)
```

To assign these bounce messages a code of MAILBOX_CUSTOMSTATE, and to classify them as soft bounces, enter the following values:

```
DIAGNOSTICCODEDATA=.*5\\.4\\.7.*
CODE=MAILBOX_CUSTOMSTATE
HARD=no
```

4. To create a classification rule by matching string values in the From header of the delivery status notification message, add the entries shown in the following table to the customFromBounceConfig file.

Parameter	Value
FROMDATA=	The string value in the From header that you want to match. Either enter the exact string to match, or enter the value in the form of a regular expression. See Step 3 for information on regular expressions.
CODE=	The code you want to assign bounce messages that contain the specified string in the From header.
HARD=	Enter either Yes or No to indicate whether or not bounce messages that include the specified string are to be classified as hard bounces.

For example, to classify bounce messages returned from a specific Mail Transfer Agent as hard bounces, and to assign them a code of BAD_ADDRESS, enter the following values:

```
FROMDATA=.*name_of_mailer.*
CODE=BAD_ADDRESS
HARD=yes
```

5. To create a classification rule by matching string values in the Subject header of the delivery status notification, add the entries in the following table to the customSubjectBounceConfig file.

Parameter	Value
SUBJECTDATA=	The string value in the Subject header that you want to match. Either enter the exact string to match, or enter the value in the form of a regular expression. See Step 3 for information on regular expressions.
CODE=	The code you want to assign bounce messages that contain the specified string in the Subject header.
HARD=	Enter either Yes or No to indicate whether or not bounce messages that include the specified string are to be classified as hard bounces.

For example, to classify bounce messages that contain the string VACATION in the Subject header as soft bounces, and to assign them a code of AUTO_REPLY, enter the following values:

```
SUBJECTDATA= (?i).*VACATION.*
CODE=AUTO_REPLY
HARD=no
```

Note: In the SUBJECTDATA field, the values (?i) indicate that the match is case-insensitive.

6. If you create custom bounce codes for the CODE parameter, you must also add the new code value to the Siebel BOUNCE_REASON_CODE Lists of Values (LOV).

   For information about customizing Siebel CRM LOVs, see *Siebel Applications Administration Guide* .
7. After creating a custom rule, stop and restart the Bounce Handler Daemon for the rule to take effect.

Process of Configuring the Click Through Daemon

This topic contains the information that you need to configure the Click Through Daemon to communicate with the Marketing Component Group. The Click Through Daemon needs to pass the server details about the HTTP requests it has serviced (Tracked URLs, Forward To Friend, and so on) to the Marketing Component Group.

This process is a step in *Roadmap for Configuring Email Marketing Daemons*.

To configure the Click Through Daemon to connect to the Marketing Component Group, perform the following tasks:

- *Configuring the Click Through Daemon HTTP Server Port*
- *Verifying the Click Through Daemon Installation*
- *Configuring the Click Through Daemon, Web Marketing, and Events Base URLs*
- *Configuring Web Services Properties for the Click Through Daemon*

CAUTION: During this process, do not start the Click Through Daemon until told to do so. If you do accidentally start it, then stop it immediately before proceeding.

Configuring the Click Through Daemon HTTP Server Port

Personalization elements sent in emails to contacts and prospects that the Click Through Daemon services (for example, Track Message Open, Tracked URLs, and so on) must be able to issue HTTP requests to the Click Through Daemon. You must configure your firewalls or DMZ to service these requests and the Email Sending Daemon to listen for these HTTP requests on a specific port. This topic describes this task.

This task is a step in *Process of Configuring the Click Through Daemon*.

To configure the Click Through Daemon HTTP server port

1. Identify the port number to use to service HTTP requests on the Click Through Daemon and write it down for use in subsequent tasks.
2. Configure your firewall to properly service these requests over this port.
3. Open the server.xml file in the *ctd_installation_directory*\`conf` directory with a text editor.
4. Search for the following phrase:

   ```
   Define a non-SSL Coyote HTTP/1.1 Connector
   ```
5. Search for the XML tag Connector using the following phrase:

   ```
   Find the value of the port attribute
   ```

   By default this value is 8060. If you chose a different port number to service HTTP requests on the Click Through Daemon, then change the port attribute value and save the file.

Verifying the Click Through Daemon Installation

To verify the Click Through Daemon installation was successful, you start the Click Through Daemon and then perform the installation test. For information about testing how the Email Marketing components and the Marketing Component Group work together, see *Process of Testing the Email Marketing Components with Siebel Marketing*.

This task is a step in *Process of Configuring the Click Through Daemon*.

Starting the Click Through Daemon on a Windows Server

The following procedure describes how to start the Click Through Daemon on a Windows server.

To start the Click Through Daemon on a Windows Server

1. From the Start menu, choose Settings and then the Control Panel menu item.
2. In Control Panel, choose Administrative Tools and then Services.
3. Right-click the ctd service and select Start.

Starting the Click Through Daemon on a UNIX Server

The following procedure describes how to start the Click Through Daemon on a UNIX server.

To start the Click Through Daemon on a UNIX server

1. Open a window and navigate to the Click Through Daemon install directory.
2. Enter and run the following command:

   ```
   ./tomcat-ctl.sh start &
   ```

3. Optionally, you can enter and run the following commands:

   ```
   ./tomcat-ctl.sh start &; tail -f logs/ctd.log
   ```

   > **Note:** The first command (`./tomcat-ctl.sh start &`) launches the daemon. The second command (`tail -f logs/ctd.log`) displays output to the ctd log as it is running without generating a read lock on the file. A read lock would prevent the tail command from working.

Verifying the Click Through Daemon Installation

The following procedure describes how to verify the Click Through Daemon installation.

To verify the Click Through Daemon installation

1. Verify that the Click Through Daemon MS Windows service or UNIX process runs and stays running without an error message.
2. Open the ctd_InstallLog.log file in the ctd installation directory and read the Summary at the start of the file.

   Make sure it says that the installation was successful with no warnings or errors. If there are warnings or errors, then you must identify the cause and fix the error.
3. Verify that a ctd.log file exists in the directory `ctd_installation_directory\logs`.
4. Verify that the following text is in the ctd.log file:

```
INFO OnPremiseAppListener CTD is licensed.
```

5. Make sure there are no ERROR or WARN level messages in the ctd.log file.
6. Confirm that the Click Through Daemon Web container is running.

   Note: To do this, you need the port number that you obtained in *Configuring the Click Through Daemon HTTP Server Port*.

7. Verify that you can open the following Web page without an error using Internet Explorer

   `http://Click_Through_Daemon_server_hostname:Click_Through_Daemon_http_port/ctd/soaprpc`

Configuring the Click Through Daemon, Web Marketing, and Events Base URLs

This topic describes how to configure the base URLs for URLs sent in email campaigns. The following are the sets of base URLs that can be generated:

- Click Through Daemon base URL (used for Tracked URLs, Forward To Friend, and so on)
- Web Marketing base URL
- Events base URL

This task is a step in *Process of Configuring the Click Through Daemon*.

To configure base URLs for email campaigns

1. Navigate to the Siebel Marketing Server login screen at http://*marketing application hostname*/marketing_enu
2. Log in as the server administrator.
3. Navigate to the Administration - Marketing screen and then the Servers view.
4. In the Servers list, in the Name field, query for Email Marketing Server.
5. In the parameters list, in the Value field, update the values as shown in the following table.

Parameter Type	Value
Click Through Daemon (CTD)	`http://Click Through Daemon server hostname:port number`

Web Server	*URL for Web Marketing;URL for Events*
	
	For example:
	
	`http://hostname/emarketing_enu;`
	
	`http://`

Parameter Type	Value
	hostname **/eevents_enu**

Configuring Web Services Properties for the Click Through Daemon

You can configure the Web Services properties for the CTD by changing the properties in the ctd.properties file, located in the *CTD_root_installation* directory.

This task is a step in *Process of Configuring the Click Through Daemon*.

To configure Web services properties for the Click Through Daemon

1. Navigate to the ctd.properties file in the *CTD_root_installation* directory.
2. Open the ctd.properties file in a text editor.
3. Change the Web services properties in the ctd.properties file as indicated in the following table.

Property	Description
Web Service URL	ctd.webservice.url=CHANGE_ME Replace CHANGE_ME with the URL obtained in *Identifying the Web Service Endpoint URL*.
Web Service username	ctd.webservice.username=CHANGE_ME Replace CHANGE_ME with the Administration user name.
Web Service password	ctd.webservice.password=CHANGE_ME Replace CHANGE_ME with the Administration user password.

4. (Optional) If you choose to encrypt the Web service username and password using the JMangle algorithm, then set the JAR_PATH environment variable in the jmangle.bat file. The jmangle.bat file is located in the *CTD_root* **/bin** directory.

   Make sure that the value you specify for the JAR_PATH reflects the directory structure of the *CTD_root* **/bin** directory. For example:

   ```
   JAR_PATH=../common/lib/Siebel.jar;../common/lib/common.jar
   ```

Note: If the Web services endpoint URL uses the HTTPS protocol, then you must configure the Email Marketing components for HTTPS communications with Siebel Marketing as described in *Configuring Email Marketing Components for HTTPS Communications*.

Encrypting Trackable URLs and Response Forms for Email Marketing

As of Siebel CRM 21.5 Update, Siebel eMarketing allows administrators to encrypt trackable URLs and response forms (Subscribe and Unsubscribe forms).

Note: This feature requires that you have installed Siebel CRM 21.5 Update or later and that you run the RepositoryUpdate utility after installation. The Encryption user property is not available in prior releases. For full functionality, both Siebel EMS and Siebel CRM (Siebel eMarketing application) require installation to version 21.5 or later.

There are two scenarios for this feature:

- **URLs in emails.** URLs that are sent as a part of emails are encrypted by Email Sending Daemon (ESD) and will be decrypted by Click Through Daemon (CTD) when the URL is clicked. If you install Siebel EMS 21.5 or later, then URLs sent in the email are encrypted and decrypted.
- **URLs in Siebel eMarketing offers.** URLs that are seen on the eMarketing Offers screen are encrypted by Siebel CRM and decrypted by CTD when the URL is clicked. For the URLs in Siebel eMarketing to be encrypted and decrypted, both Siebel EMS and Siebel CRM must be updated to 21.5 or later, and the Siebel Repository must be updated.

  The behavior of this feature depends on the version of the installed software and the setting of the user property Encryption. To enable this feature for Siebel eMarketing, set this user property on the Web Offer business component to Y. By default, the value is set to N. When the value is N, the behavior is the same as it is in releases prior to Siebel CRM 21.5 Update.

The following table describes different behaviors for the encryption feature, with different versions of Siebel EMS and Siebel CRM (Siebel eMarketing application).

Installed Software	Encryption User Property	Feature Available in Siebel EMS	Feature Available in Siebel eMarketing
Siebel EMS 21.5 or later Siebel CRM 21.5 or later	Y	Available. The encryption feature is enabled for Siebel EMS.	Available. The encryption feature is enabled for Siebel eMarketing URLs.
Siebel EMS 21.5 or later Siebel CRM 21.5 or later	N	Available. The encryption feature is enabled for Siebel EMS.	Not available. Siebel eMarketing URLs work without encryption.

Installed Software	Encryption User Property	Feature Available in Siebel EMS	Feature Available in Siebel eMarketing
Prior to Siebel EMS 21.5 Siebel CRM 21.5 or later	Y	Not available.	Not available.
Prior to Siebel EMS 21.5 Siebel CRM 21.5 or later	N	Not available.	Not available. Siebel eMarketing URLs work without encryption.
Siebel EMS 21.5 or later Prior to Siebel CRM 21.5	Property not available	Available. The encryption feature is enabled for Siebel EMS.	Not available. Siebel eMarketing URLs work without encryption.
Prior to Siebel EMS 21.5 Prior to Siebel CRM 21.5	Property not available	Not available.	Not available.

Configuring Email Marketing Components for HTTPS Communications

This topic describes how to configure the Email Marketing Server components to support communications with Siebel Marketing using the HTTPS protocol.

This task is a step in *Roadmap for Configuring Email Marketing Daemons*.

If the Siebel Web server has been configured to use SSL or TLS encryption for communications with Web clients (HTTPS protocol), and if the Web service endpoint URL that the Email Marketing components use to connect with Siebel Marketing uses HTTPS, then you must perform the following tasks:

- Import the certificate file used by the Siebel Web server onto the computer on which you installed the Email Marketing components.
- Configure the Windows services or UNIX shell scripts used to start the Email Marketing Server components for HTTPS.

The procedures in this topic describe how to perform these tasks in a Windows environment and in a UNIX environment.

Configuring the Email Marketing Server to Use HTTPS on UNIX

The following procedure describes how to configure Email Marketing Server components for HTTPS communications on a UNIX environment.

1. On the computer on which you installed the Email Sending Daemon, create a keystore file for the CA certificate used by the Siebel Web server using a program such as Java keytool.

   For example, create a keystore file named cacerts.
2. On the computer on which the Email Sending Daemon is installed, verify that the `JAVA_HOME` variable is set to the installation directory of the JRE environment that's being used by the Email Sending Daemon, and verify that the PATH variable includes the `JAVA_HOME/bin` folder.

   > **Note:** The Siebel Web server certificate file must be imported in the `lib\security` folder of the Java Runtime Environment (JRE) environment being used by the Email Marketing Server daemons. For information, see *Installing the Java Runtime Environment*.

3. Import the Siebel Web server CA certificate file into the keystore file you created in Step 1 using the following command:

   ```
   keytool -import -alias hostname
     -file certificate_file_name -keystore
   keystore_name -storepass keystore_password
   ```

   where:

   - *hostname* is the name of the Email Sending Daemon host computer.
   - *certificate_file_name* is the name of the certificate file.
   - *keystore_name* is the name of the keystore file you created in Step 1.
   - *keystore_password* is the keystore file password.

   If you not specify the full path to the keystore file, the file is created in the user home folder.
4. (Optional) If the Click Through Daemon is installed on a different computer to the Email Sending Daemon, create a keystore file and import the Siebel Web server certificate into the keystore file on the Click Through Daemon computer.

   To perform these tasks, follow the instructions in Step 1 through Step 3, substituting references to the Email Sending Daemon with the Click Through Daemon.
5. (Optional) If the Bounce Handler Daemon is installed on a different computer to the Email Sending Daemon, create a keystore file and import the Siebel Web server certificate into the keystore file on the Bounce Handler Daemon computer.

   To perform these tasks, follow the instructions in Step 1 through Step 3, substituting references to the Email Sending Daemon with the Bounce Handler Daemon.
6. When configuring the Web services properties for Email Sending Daemon, Click Through Daemon, and Bounce Handler Daemon, make sure that the URL specified for the `component.handler.webservice.url` parameter points to a Siebel Inbound Web service that uses HTTPS.

For additional information on this task, see the following:

- *Configuring Web Services Properties for the Email Sending Daemon*
- *Configuring Web Services Properties for the Bounce Handler Daemon*
- *Configuring Web Services Properties for the Click Through Daemon*

Configuring the Email Marketing Server to Use HTTPS on Microsoft Windows

The following procedure describes how to configure Email Marketing Server components for HTTPS communications on a Microsoft Windows environment.

To configure the Email Marketing Server to Use HTTPS on Windows

1. On the computer on which you installed the Email Sending Daemon, create a keystore file for the CA certificate file used by the Siebel Web server using a program such as Java keytool.

   For example, create a keystore file named cacerts.jks.
2. Import the Siebel Web server certificate file into the `lib\security` folder of the Java Runtime Environment (JRE) being used by the Email Marketing Server daemons as described in Steps 2 and 3 in *Configuring the Email Marketing Server to Use HTTPS on UNIX* .
3. (Optional) If the Click Through Daemon is installed on a different computer to the Email Sending Daemon, create a keystore file and import the Siebel Web server certificate into the keystore file on the Click Through Daemon computer.

   To perform these tasks, follow the instructions in Steps 1 through 3 in *Configuring the Email Marketing Server to Use HTTPS on UNIX*, substituting references to the Email Sending Daemon with the Click Through Daemon.
4. (Optional) If the Bounce Handler Daemon is installed on a different computer to the Email Sending Daemon, create a keystore file and import the Siebel Web server certificate into the keystore file on the Bounce Handler Daemon computer.

   To perform these tasks, follow the instructions in Steps 1 through 3 in *Configuring the Email Marketing Server to Use HTTPS on UNIX* , substituting references to the Email Sending Daemon with the Bounce Handler Daemon.
5. When configuring the Web services properties for Email Sending Daemon, Click Through Daemon, and Bounce Handler Daemon, make sure that the URL specified for the `component.handler.webservice.url` parameter points to a Siebel Inbound Web service that uses HTTPS

(Optional) Enabling TLS for Communications Between the Email Sending Daemon and the SMTP Server

If you want to enable Transport Layer Security (TLS) for communications between the Email Sending Daemon (ESD) and the Simple Mail Transfer Protocol (SMTP) server, then perform the steps in the following procedure.

This task is a step in *Roadmap for Configuring Email Marketing Daemons*.

To enable TLS for communications between the ESD and the SMTP server

1. Navigate to the esd.properties file in the *ESD_root* installation directory.
2. Open the esd.properties file in a text editor.
3. Locate the SMTP talker configuration options section in the file.
4. Set the esd.smtp.starttls property to True.

(Optional) Verifying Email Marketing Component Configuration

After you have installed and configured the Email Marketing components, you can optionally use the Email Marketing configuration check utility provided with Siebel Marketing to verify your configuration. The Email Marketing configuration check performs tests to verify that the Email Sending Daemon, the Bounce Handler Daemon, and the Click Through Daemon components are correctly setup and functioning.

To use the Email Marketing configuration check utility, run the end2end.jar file for each component, as described in the following procedure.

To verify Email Marketing component configuration

1. Start the ESD, the CTD, and the BHD components as Windows services.
2. To start the Email Marketing configuration check, run the following command from the command line for each of the ESD, BHD, and CTD components in turn:

   ```
   java -DpropertyFile=component_property_file_path -jar component-end2end.jar_path
   ```

   where:

   - *component_property_file_path* is the full path to the component's property file.
   - *component*- `end2end.jar` *_path* is the full path to the end2end.jar file for the component, which is located in the *component_root*\webapps*component*\WEB-INF\lib directory.

   The following is an example of the command to run for the Email Sending Daemon:

   ```
   java -DpropertyFile=D:\programs\esd\esd.properties -jar D:\Program
   Files\esd\webapps\esd\WEB-INF\lib\esd-end2end.jar
   ```

The following table shows some of the tests performed by the Email Marketing configuration check for each component.

Component	Conditions Verified by the Configuration Check Utility
Email Sending Daemon	• A connect string to the Siebel Marketing Server is provided. • The ESD can connect to the Siebel Marketing Server. • Validates the ESD license with the Siebel Marketing Server.

Component	Conditions Verified by the Configuration Check Utility
	• Verifies that Mail Transfer Agent information is provided. • Checks ESD connectivity to the Mail Transfer Agent. • Checks that the ESD has write permission to the **\mailings** directory. • Checks that the ESD has write permission to the **\state_dir** directory. • Verifies that a mount point directory exists. • Checks that the ESD has read permission to the mount point directory.
Click Through Daemon	• A connect string to the Siebel Marketing Server is provided. • The CTD can connect to the Siebel Marketing Server. • Validates the CTD license with the Siebel Marketing Server. • Checks that the CTD has write permission to the **`ueue** directory. • Checks that the CTD has write permission to the **\Queue\** *Message_Open* subdirectory. • Checks that the CTD has write permission to the **`ueue** *Click* subdirectory. • Checks that the CTD has write permission to the **`ueue***List_unsubscribe* subdirectory.
Bounce Handler Daemon	• A connect string to the Siebel Marketing Server is provided. • The BHD can connect to the Siebel Marketing Server. • Validates the BHD license with the Siebel Marketing Server.

Process of Testing the Email Marketing Components with Siebel Marketing

This topic describes how to test all the Email Marketing components and the Siebel Marketing application together as a complete product. This test involves sending a test email to three or more test contacts. The content of the test email template must include links to test the Click Through Daemon, the Web Marketing Server, and the Events server. Make sure at least two of the contacts are invalid email addresses, one within the corporate domain, and one outside the corporate domain. These test bounce handling and bounce detail communications for the Email Sending Daemon and the Bounce Handler Daemon. Additionally, send email to at least one email account that you can access outside of your corporate network. This tests your Email Sending Daemon, DNS alterations, and corporate firewall configurations.

To perform this comprehensive test of the Email Marketing components, perform the following tasks:

1. *Creating the Test Email Template*
2. *Sending the Test Email Template to Test Contacts*
3. *Confirming That Tests Function as Expected*

Creating the Test Email Template

Create a test email template as described in the following procedure.

This task is a step in *Process of Testing the Email Marketing Components with Siebel Marketing*.

To create the test email template

- Create a test email template to verify your Email Marketing components are correctly installed and configured. For information about creating an email template, see *Siebel Marketing User Guide* .

  When you create the test email template, make sure you add a One-Click Unsub Response Form, a Web Offer link, and an Event link.

  > **Note:** Because this email is sent over the Internet, it is recommended that you add text that announces that this is a test email, offers your apologies if someone unintended receives it, and provides information so the recipients can contact you.

Sending the Test Email Template to Test Contacts

Send the test email template as described in the following procedure.

This task is a step in *Process of Testing the Email Marketing Components with Siebel Marketing*.

To send the test email template

1. Determine the contacts to whom the test email template is sent, create an email offer from it, and send it to these contacts.

   Whether you use a list or a segment to generate your target contacts for this test, make sure the following three contact types are included:

   - **Invalid contact email address within the corporate domain.** This tests communication from the Email Sending Daemon to the Marketing Component Group. The Email Sending Daemon reports synchronous bounces to the Marketing Component Group. An invalid email address within the corporate domain generates a synchronous bounce from the Mail Transfer Agent.

     > **Note:** The administrator must make sure that the Mail Transfer Agent is configured to handle synchronous bounces and confirm that the contact's email address generates a synchronous bounce. This is desirable even if the Mail Transfer Agent is normally not configured to handle synchronous bounces. The reason for this is to make sure that if the normal Mail Transfer Agent configuration changes and starts performing synchronous bounces, then your server can properly record them. After testing, the administrator can return the Mail Transfer Agent to its normal configuration.

   - **Invalid contact email address outside of the corporate domain.** This tests the corporate firewall and Internet DNS configuration of the Bounce Handler Daemon. This also tests communication between the Bounce Handler Daemon and the Marketing Component Group. An invalid email address for a domain other than the corporate domain generates an asynchronous bounce. The Bounce Handler Daemon must be able to receive bounced emails, process bounced emails, and send the bounce details to the Marketing Component Group.

     Be aware that some email domains (such as aol.com) do not generate bounces. Also, be aware that email bounces are not guaranteed to be returned. It can take some research to determine whether the problem is actually the Bounce Handler Daemon or one of a number issues not related to the installation and configuration of the Email Marketing components.

- **Valid contact email address for an email account accessible outside of the corporate firewall.** This tests the corporate firewall and Internet DNS configuration with the Click Through Daemon, Web Server, and Event Server. This tests communication between the Click Through Daemon and the Marketing Server. The email sent to a valid contact contains a One-Click Unsub Response Form, a Web Offer link, and an Event link. The tester must access this account and email from a computer outside the corporate firewall to correctly execute this test.

2. Launch a campaign using a list or segment including the described types of contacts.
3. Monitor the campaign to make sure that it succeeds without any errors. One example of an error is an error message in the log containing the word SOAP. This indicates that the Siebel Marketing application is not correctly configured to communicate with the Email Sending Daemon.

Confirming That Tests Function as Expected

Perform the tests in this topic to confirm that the Siebel Marketing application performed as expected.

This task is a step in *Process of Testing the Email Marketing Components with Siebel Marketing*.

To confirm that tests function as expected

1. Test an email offer sent to a valid contact email address as follows:

   a. Verify that the email offer was received. Find a computer that is outside of the corporate network and has access to the valid contact's email account. Then you must access that account from the computer that is outside of the corporate network.

      Results of test. If the email offer is received, then you have confirmed the following results:

      - The Marketing Server communicates with the Email Sending Daemon.
      - The Email Sending Daemon can access the email message content and subwaves from the Marketing File System.
      - The Email Sending Daemon can send email to email accounts outside of the corporate domain using the corporate Mail Transfer Agents.
      - The email message From and Reply-To headers are correct.

   b. Click the One Click Unsub link in the email.

      A Web page that is hosted by the Click Through Daemon appears with the message, You have been unsubscribed!

      Results of test. This message confirms that you correctly configured the Click Through Daemon for the corporate firewall and it has been properly added to the Internet DNS records. Additionally, this confirms that the Marketing application has been correctly configured with the base URL for the Click Through Daemon.

   c. Click the One Click Unsub link in the email for the Web Offer link and the Event link.

      Results of test. The Web Server and Event Server base URLs are properly configured within the Marketing application.

2. Verify campaign details:

   a. Synchronous bounce reported. Navigate to the All Contacts/Prospects Across Organizations applet for the test campaign. Verify that the invalid contact with an email address within the corporate domain is identified as a bounce.

Results of test. The Email Sending Daemon is able to communicate with the Marketing application and can report synchronous bounces.

> **Note:** You might need to add the Email Bounce Type and Email Bounce Reason Code columns to the visible columns shown in this applet.

b. Asynchronous bounce reported. Navigate to the Campaign Contact/Prospect Applet-Admin applet for the test campaign. Verify that the invalid contact with an email address outside of the corporate domain is identified as a bounce.

   Results of test. The Bounce Handler Daemon can receive bounces sent from outside of the company firewall. This means the Bounce Handler Daemon's hostname is correctly configured in the Internet DNS records. The Bounce Handler Daemon is able to communicate with the Marketing Component Group and can report asynchronous bounces. The Marketing application has been correctly configured to use the Bounce Handler's hostname as the SMTP envelope from address.

c. One Click Unsub recorded. Navigate to the Campaign Response List applet and verify that the valid contact's email address is entered here with a Response Type of One Click Unsub.

   Results of test. The Click Through Daemon can communicate with the Marketing Component Group and update the Siebel transactional database with information that it collects when an email recipient clicks on a link that it monitors.

Administering Email Marketing

This topic describes the on-going administration tasks that you perform to monitor and maintain Siebel Email Marketing after it is installed and configured. The administration tasks include the following:

- *Monitoring Email Sending Daemon Jobs Using the Jobs Console*
- *Prioritizing Email Sending Daemon Jobs*
- *Limiting Maximum Throughput Rate for the Email Sending Daemon*
- *Disabling SMTP Command Pipelining*
- *About Email Marketing Log Files*
- *Configuring Email Marketing Server Logging*
- *Setting Up Administrator Alerts for Email Marketing*
- *Setting Up Automatic Failover for the Email Sending Daemon*

Monitoring Email Sending Daemon Jobs Using the Jobs Console

The Email Marketing Server Jobs console provides an interface that allows administrators to view and control email jobs currently being processed by the Email Sending Daemon. The Jobs console is provided as a Java Server Page (JSP); to access the console, perform the steps in the following procedure.

To monitor Email Sending Daemon jobs using the Jobs console

1. Define the username and password that are to be used to access the Jobs console in the tomcat-users.xml configuration file, which is located in the *ESD_root* `/conf` directory.
2. Navigate to the Jobs console at the following URL:

http://*ESD_hostname*:*port*/esd/jobMonitor.jsp

where:

- *ESD_hostname* is the host name of the Email Sending Daemon.
- *port* is the port number of the Jobs console (default is 8090).

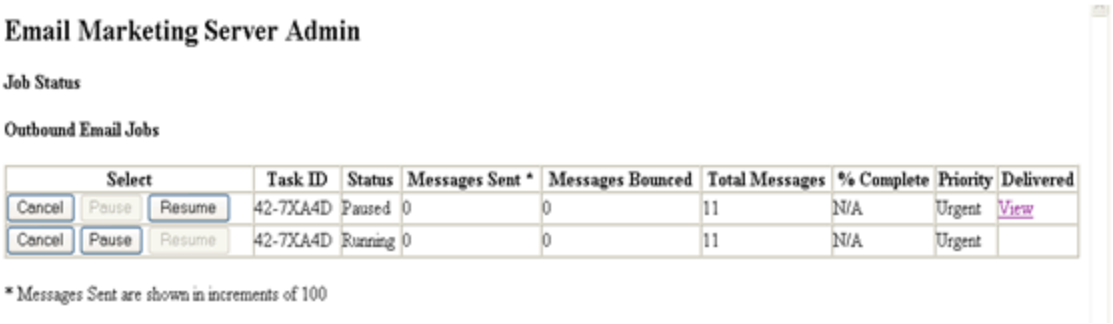
The port number of the Jobs console is the same as the port number used by the Email Sending Daemon. If you have changed the default port number used by the Email Sending Daemon (8090), then use the same port number to access the Jobs console.

3. Enter the username and password you defined in Step 1 to log in to the Jobs console.

The following figure shows the Jobs console, which displays all active and incomplete jobs being processed by the Email Sending Daemon.

You can use the Jobs console to Pause, Resume, and Cancel jobs. Clicking the Pause button suspends a job with a status of In Progress; clicking the Resume button resumes a Paused job; and clicking the Cancel button cancels the job and removes it from the console.

If you click the hyperlink in the Delivered column of the console, then a list of all the email addresses to which emails have been sent is displayed.



Email Marketing Server Admin

Job Status

Outbound Email Jobs

Select	Task ID	Status	Messages Sent *	Messages Bounced	Total Messages	% Complete	Priority	Delivered
Cancel Pause Resume	42-7XA4D	Paused	0	0	11	N/A	Urgent	View
Cancel Pause Resume	42-7XA4D	Running	0	0	11	N/A	Urgent	

* Messages Sent are shown in increments of 100

To monitor email jobs in the buffer queue, navigate to the *component_root* `/ queueDir` directory, where *component_root* is the installation directory of the Email Sending Daemon, the Bounce Handler Daemon, or the Click Through Daemon.

Prioritizing Email Sending Daemon Jobs

In Siebel Marketing, the priority level that you specify for a campaign also determines the priority that is assigned to email jobs associated with the campaign. As a result, email jobs for critical campaigns are executed before jobs for less critical campaigns. The priority levels that can be chosen for a campaign and, therefore, for associated email jobs are: 1-Urgent, 2-High, 3-Medium, or 4-Low.

In general, the Email Sending Daemon suspends processing of a lower priority job if a higher priority job enters the processing queue. However, in some circumstances, it is more efficient to continue processing the lower priority job, for example, if the low-priority email job has only a few recipients and the high-priority job has thousands.

To accommodate these circumstances, you can determine a priority threshold for email jobs. The priority threshold is the number of recipients that an email job must have in order that its priority level is always maintained. For example, if you specify a value of 50, then email jobs with fewer than 50 recipients are always assigned a priority of High by the Email Sending Daemon, even if the priority initially specified for the campaign is 3-Medium, or 4-Low.

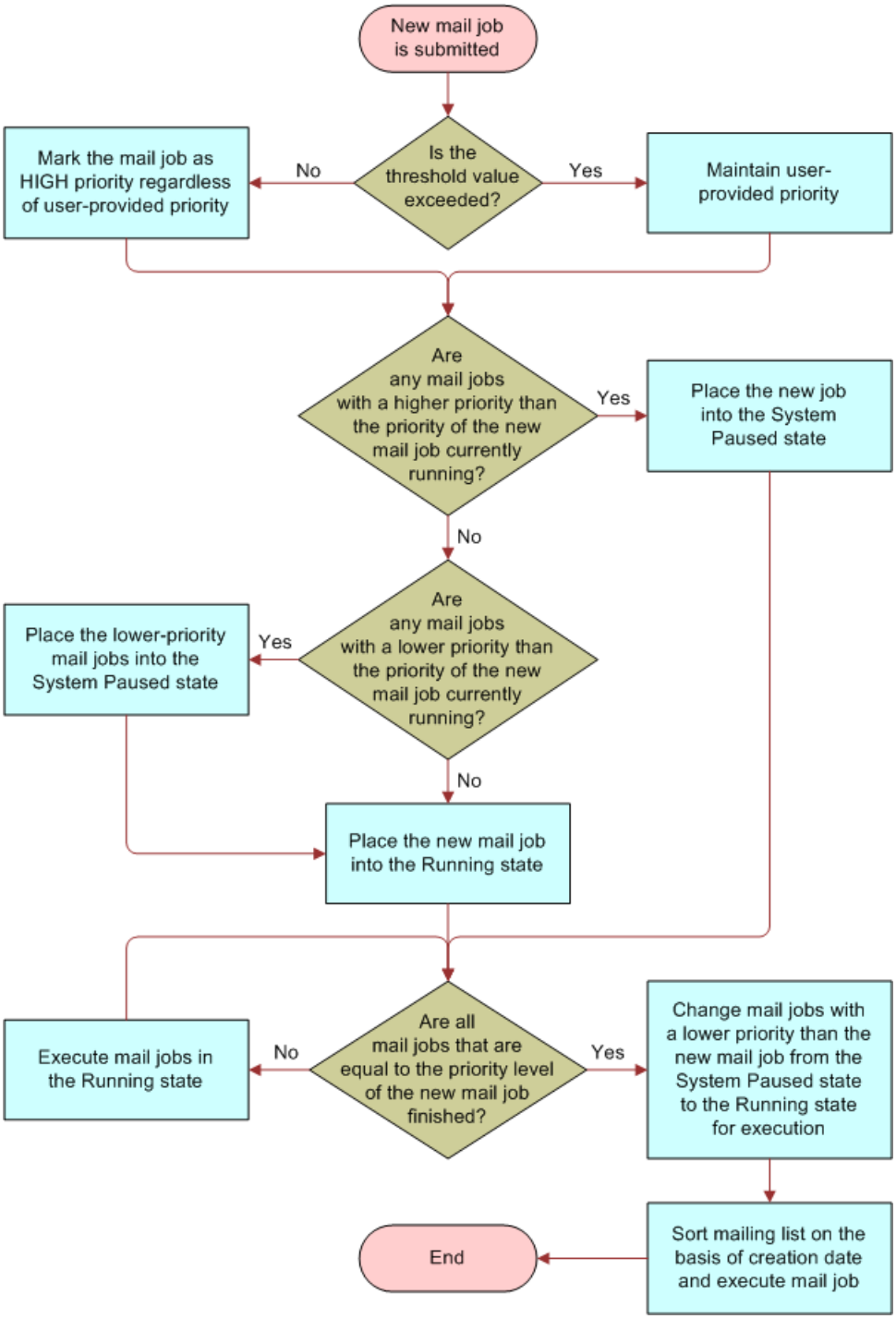
The following procedure describes how to set the priority threshold for Email Sending Daemon jobs.

To set the priority threshold for Email Sending Daemon jobs

1. Navigate to the esd.properties file in the *ESD_root* installation directory.
2. Open the esd.properties file in a text editor.
3. Set the value of the esd.priorityThreshold parameter to an appropriate value.

   The default value is 5001, indicating that the priority assigned to any email job with more than 5001 recipients is not to be overridden by the Email Sending Daemon.

The following figure shows the job prioritization workflow.



Whenever a new mail job is submitted, the steps in the job prioritization workflow are as follows:

1. Is the threshold value exceeded?
    - If yes, then maintain the user-provided priority.
    - If no, then mark the mail job as high priority regardless of the user-provided priority.

2. Are any mail jobs with a higher priority than the priority of the new mail job currently running?
   - If yes, then place the new job into the System Paused state and proceed to Step 4.
   - If no, then proceed to Step 3.
3. Are any mail jobs with a lower priority than the priority of the new mail job currently running?
   - If yes, then place the lower-priority mail jobs into the System Paused state.
   - If no, then place the new mail job into the Running state.
4. Are all mail jobs that are equal to the priority level of the new mail job finished?
   - If yes, then:
     - Change mail jobs with a lower priority than the new mail job from the System Paused state to the Running state for execution.
     - Sort mailing list on the basis of creation date and execute mail job.
   - If no, then execute mail jobs in the Running state.

Limiting Maximum Throughput Rate for the Email Sending Daemon

You can limit the number of emails that the Email Sending Daemon sends to your company's outbound Mail Transfer Agent (MTA) each second in order to avoid delays resulting from the MTA being overburdened. This topic describes how to limit the maximum throughput rate, specified in messages per second, for the Email Sending Daemon.

To set a maximum throughput rate

1. Navigate to the esd.properties file in the *ESD_root* installation directory.
2. Open the esd.properties file in a text editor.
3. Set the esd.smtp.throttleVal property to one of the following values:
   - **-1 (High, no throttle).** Sends emails at the highest rate possible. This is the default setting.
   - **250-350 (Medium).** Sends emails at the rate of this setting, per second.
   - **250-50 (Low).** Sends emails at the rate of this setting, per second.

Disabling SMTP Command Pipelining

The Email Sending Daemon implements SMTP command pipelining by default. SMTP command pipelining allows the Email Sending Daemon to send multiple emails to the Mail Transfer Agent at a time, without having to wait for a response to each individual email.

Pipelining significantly improves the performance of email communications. However, it can result in an email being sent to the same recipient more than once in certain circumstances. When processing a group of emails, the Mail Transfer Agent returns an error if any problem arises during the email sending process, even if the email has been successfully delivered to some of the recipients. If the group of emails are then resent, then some individuals might receive the email a second time. If you want to make sure this situation never occurs, then disable SMTP pipelining as described in this topic.

To disable SMTP command pipelining

1. Navigate to the esd.properties file in the *ESD_root* installation directory.
2. Open the esd.properties file in a text editor.
3. Locate the SMTP talker configuration options section in the file.
4. Set the esd.smtp.suppressPipelining property to True.

About Email Marketing Log Files

This topic describes the log files that are generated by the Email Marketing Server during processing. These log files provide detailed information about the processes that have been run and list any errors that occurred. This topic also lists other files which can provide important information that can help you to troubleshoot email processing, or to improve the performance of the Email Marketing Server.

Email Marketing Log Files

The main log files generated for the ESD, CTD, and BHD components are as follows:

- esd.log
- ctd.log
- bhd.log

Review these files, which are located in the logs folder of the main installation directory for each component, if errors occur during email processing. These files contain logger debug statements for the relevant component.

The Email Marketing components also generate important information in the log files shown in the following table. These files can provide useful information about email processing problems that are not caused by individual Email Marketing components.

Log File	Description
failure.log	Logs Queue Reader failures.
stderr.log	Logs any error stack that is not handled by an Email Marketing component.
stdout.log	Logs any output that is not explicitly directed to the Email Marketing component log files.
commons-daemon.log (ESD and CTD components only)	Contains errors generated by the Apache Tomcat application server.
SiebelBounceHandlingDaemon.log (BHD component only)	Contains information and errors generated by Commons Daemon.

Files to Review When Troubleshooting Campaign Wave Processing

This topic describes files, other than log files, that are generated during Email Marketing processing which can provide useful troubleshooting information.

Email Files

When you launch a Siebel Marketing campaign including an email offer that is sent to recipients, Siebel Marketing generates a list of recipients file and an email .MIME file, both of which are processed by the Email Sending Daemon. The list of recipients file and the .MIME file can provide useful information when troubleshooting errors in campaign wave processing. The files are located in the following directories:

- .MIME file: *Siebel_File_System* **\Marketing\EmailOfferContent**
- List of recipients file: *Siebel_File_System* **\Marketing** *wave_list*

  where *wave_list* is the list of recipients for a wave.

Job Files

When the Email Sending Daemon processes a campaign wave, a directory is created for each job that is processed as part of the wave in the **ESD_root \state_dir\mailings** directory. For example:

```
ESD_root
\state_dir\mailings\00000001

ESD_root
\state_dir\mailings\00000002
```

Within each **\0000000** *n* job directory, the following files are created for the job:

- Delivered.txt: Lists all recipients to whom emails were successfully delivered.
- Recipientsxxx.txt: Lists all recipients to whom emails were sent.
- Retry*xxx*.txt: Lists all recipients to whom emails were re-sent.
- State0.txt: Lists the status of the job.

Review these files if errors occur when the Email Sending Daemon runs a job.

Related Topic

Configuring Email Marketing Server Logging

Configuring Email Marketing Server Logging

This topic describes how to configure the type and amount of information that is logged by the Email Marketing Server.

The Email Marketing Server components are Java based applications that use the standard logging library for Java, log4j2, to control the logging behavior for the esd.log, ctd.log, and bhd.log files. You can configure the information that is written to each of the main component log files by editing the log4j2.properties configuration file for each component. This task is described in the following procedure.

To configure Email Marketing Server logging

1. Using a text editor, open the log4j2.properties file for the component for which you want to configure logging. The log4j2.properties file is located in the lib folder of the main installation directory for each of the ESD, CTD, and BHD components.
2. The Email Marketing Server logs information for specific SMPT classes, and logging levels are set for each SMTP class.
   For example, the following line in the log4j2.properties file records details in the log file of each individual to whom an email was successfully delivered:

   ```
   log4j.logger.com.siebel.sem.smtp.MailingState=DEBUG
   ```

   In the previous command, `smtp.MailingState` is the SMTP class that is logged and DEBUG is the log level. If you choose, you can enable logging for all SMTP classes by adding the following line to the end of the log4j2.properties file for a component:

   ```
   log4j.logger.com.siebel.sem.smtp=DEBUG
   ```

3. To change the amount of information that is logged for a class, navigate to the statement in the log4j2.properties file that enables logging for the class, then set the logging level to one of the following values, where DEBUG3 generates the maximum amount of information in the log file and FATAL generates the minimum amount of information:
   - Trace
   - All
   - DEBUG
   - INFO
   - WARN
   - ERROR
   - FATAL
   - OFF

   In general, set log levels to DEBUG only when you are running the Email Marketing Server for debugging purposes. Running a component with DEBUG levels of logging can impact the performance of the component.
4. To configure the size of the component log files, and the number of archived log files maintained by the Email Marketing Server, edit the log4j2.properties file to specify values for the following parameters:
   - ```
     #appender.rolling.policies.time.type = TimeBasedTriggeringPolicy
     #appender.rolling.policies.time.interval = 2
     #appender.rolling.policies.time.modulate = true
     ```
   - ```
     appender.rolling2.policies.size.type = SizeBasedTriggeringPolicy
     appender.rolling2.policies.size.size=1MB
     appender.rolling2.strategy.type = DefaultRolloverStrategy
     appender.rolling2.strategy.max = 5
     ```
5. To archive the component log files based on the time interval, edit the log4j2.properties file and configure the parameters as follows:
   - ```
     appender.rolling.policies.time.type = TimeBasedTriggeringPolicy
     appender.rolling.policies.time.interval = 2
     appender.rolling.policies.time.modulate = true
     ```
     ```

```
#appender.rolling2.policies.size.type = SizeBasedTriggeringPolicy
#appender.rolling2.policies.size.size=1MB
#appender.rolling2.strategy.type = DefaultRolloverStrategy
#appender.rolling2.strategy.max = 5
```

For additional information on logging, see *Setting Up Administrator Alerts for Email Marketing* and *About Email Marketing Log Files*.

Setting Up Administrator Alerts for Email Marketing

This topic describes how to configure the Email Marketing Server to send email alerts to the administrator if the Email Marketing components malfunction.

To enable administrator alerts for a component, you must set the relevant properties in the log4j2.properties file for the component. Each of the abnormality conditions that generates an alert is defined in the log4j2.properties file for a particular package or class, as is the alert level. For example, the following condition triggers an Error alert when an error occurs in the OnPremiseAppListener class:

Note: The `rollinguniquenumber` will be the incremental value of the highest value used in the file.

```
logger.rolling<rollinguniquenumber>.name = com.siebel.sem.esd.integrated.OnPremiseAppListener
logger.rolling<rollinguniquenumber>.level = ERROR
logger.rolling<rollinguniquenumber>.additivity = false
logger.rolling<rollinguniquenumber>.appenderRef.rolling.ref = RollingFile
```

By default, the following predefined abnormality conditions trigger an alert for an Email Marketing Server component:

- Component is unable to communicate with the Marketing server
- Component is restarted
- Component failed to write to the queue
- Component is not licensed
- Component is unable to communicate with the MTA

Alert levels can be set to the following values: INFO, DEBUG, TRACE, WARNING, ERROR, or FATAL. The Email Marketing Server generates alerts for the ERROR level and above, but you can configure the alert level for each SMTP class.

The following procedure describes how to enable administrator alerts.

To configure administrator alerts

1. To send administrator alerts for either the ESD, the BHD, or the CTD components, navigate to the log4j2.properties file in the component installation directory for the daemon you want to configure.
2. Locate the # IT Alerts settings section of the file.

3. Uncomment the parameters shown in the following table, then enter values similar to those shown.

   Note: To send alerts from all three daemons, you must update these parameters in the log4j2.properties file of each component.

Property	Description
appender.smtp.from= CHANGE_ME	Defines the From Address that is used to generate the alerts.
appender.smtp.Host=CHANGE_ME	Defines the SMTP host name that is used to send the alerts. This SMTP host must be different to the MTA's SMTP that is used to send marketing emails.
appender.smtp.to= CHANGE_ME	Defines the recipient of the alerts.

4. Stop and restart the relevant component for the changes to the log4j2.properties file to take effect.

Setting Up Automatic Failover for the Email Sending Daemon

Use the following procedure to designate a backup instance of the Email Sending Daemon.

To set up automatic failover for ESD

1. Install the ESD in two separate directories (for example, ESD1 and ESD2).
2. Configure ESD1 with the default port of 8080 and the default AJP port of 8009.
3. Open the `conf/server.xml` file and uncomment the section that starts with following line:

```
<Cluster className="org.apache.catalina.cluster.tcp.SimpleTcpCluster"
…….
</Cluster>
```

4. Make changes on cluster configuration based on the information mentioned in the link below:

   https://tomcat.apache.org/tomcat-9.0-doc/cluster-howto.html#Cluster_Basics

5. Configure ESD2 as follows:

   a. In the `conf/server.xml` file, change the port to any other number (for example, 9090).
   b. Modify the HTTP/1.1 Connector port parameter:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 9090 -->
 <Connector port="9090" ……..
```

   c. In the `conf/server.xml` file, change the AJP port to any port number other than 8009.
   d. Modify the AJP 1.3 Connector port parameter (for example, 9009):

```
<!-- Define an AJP 1.3 Connector on port 9009-->
```

```
<Connector port="9009" …..
```

e. If ESD1 and ESD2 are running on the same computer or server, then you must open the install-win32-service.bat file (located in the ESD_root installation directory) and change the value of the **Dcom.sun.management.jmxremote.port parameter, Service Name and Description**.

   Port number can be given any value other than default value of 8096.

f. Open the `conf/server.xml` file and uncomment the section that starts with following line:

```
<Cluster className="org.apache.catalina.cluster.tcp.SimpleTcpCluster"
…….
</Cluster>
```

g. Make changes on cluster configuration based on the information mentioned in the link below:

   https://tomcat.apache.org/tomcat-9.0-doc/cluster-howto.html#Cluster_Basics

h. In the Cluster section, change Receiver, `tcpListenPort` property to a value other than 4001, so that ESD2 will be identified as a unique cluster node. (for example, Update tcpListenPort to 4002).

6. The current status of each instance of the ESD must be available to the other instance for automatic failover to occur. For this to happen, share the job status directory of each ESD instance with the other instance.

   The job status directory is created when you install the ESD at `esd_root\state_dir`. For each job that is submitted to ESD, a directory is created in the `state_dir\mailings` directory that contains a file named state0.txt.

   The state0.txt file stores the status of the job. In order to share the job directory, update property name `esd.stateDirectory` in `esd.properties` file for both instances by giving a shared path. This path should be accessible by both the instances.

   > **Note:** If both esd are in the same machine, you can give absolute path of state_dir. Example, `esd.stateDirectory= c:\\ems\\esd\\state_dir`.

7. Make sure you have installed Apache 2.2.3 Web server.
8. Download JK 1.2 Binary for the operating system you are using from *https://archive.apache.org/dist/tomcat/tomcat-connectors/jk/*.

   For example, if you are using windows u can download tomcat-connectors-1.2.32-windows-i386-httpd-2.2.x from *https://archive.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/windows/*.
9. Unzip connector zip file and place mod_jk.so in <root_dir>\Apache Software Foundation\Apache2.2\modules directory.

   If tomcat-connectors contains, mod_jk.so file name with the version number. Example, mod_jk-apache-2.2.3.so then rename the file to mod_jk.so before placing it under Apache2.2\modules directory.
10. Modify the `apache conf/ workers.properties` file by registering both ESD nodes as worker nodes, and registering ESD1 as ACTIVE and ESD2 as HOT STAND BY. If the `workers.properties` file is not present, create one based on the given example and modify the value appropriately:

```
# The advanced router LB worker
worker.list=loadbalancer
# Define a worker using ajp13
worker.worker1.port=ESD1_AJP_PORT_NUMBER(8009)
worker.worker1.host=ESD1_IP_ADDRESS
worker.worker1.type=ajp13
worker.worker1.redirect=worker2
# Define another worker using ajp13
worker.worker2.port= ESD1_AJP_PORT_NUMBER(9009)
worker.worker2.host= ESD2_IP_ADDRESS
```

```
worker.worker2.type=ajp13
# Disable worker2 for all requests except failover, hot stand by
worker.worker2.activation=disabled
# Define the LB worker
worker.loadbalancer.type=lb
worker.loadbalancer.balance_workers=worker1,worker2
```

11. Configure the Apache Web server and use the Apache URL as the ESD SOAP URL. Apache will act as a load balancer for both ESD nodes. Modify the `apache conf/httpd.conf` file and register the entry for the ESD URL as follows:

```
# Load mod_jk module
LoadModule jk_module modules/mod_jk.so
JkWorkersFile <point to workers.properties which suppose to be same location as
httpd.conf>#
Where to put jk logs
JkLogFile <modjk log file path>
# Set the jk log level [debug/error/info]
JkLogLevel error
# Select the log format
JkLogStampFormat "[%a %b %d %H:%M:%S %Y] "
# JkOptions indicate to send SSL KEY SIZE,
JkOptions +ForwardKeySize +ForwardURICompat -ForwardDirectories
# JkRequestLogFormat set the request format
JkRequestLogFormat "%w %V %T"
# Send esd soap request to worker named worker1
JkMount /esd/soaprpc loadbalancer
JkMount /esd/* loadbalancer
```

12. Start the ESD and the Apache Web server in the following sequence:
    a. ESD1 Node
    b. ESD2 Node
    c. Apache (load balancer)
13. Use the Apache URL as the ESD SOAP URL in the Marketing delivery profile:

```
http://apache_ip:apache_port/esd/soaprpc
```

Configuring the Status of Email Addresses

This topic describes how to configure the status of email addresses.

You can configure the circumstances in which the status of a contact's email address is set to Bad Address or Undeliverable in the EMAIL_STATUS_CD field. The email address for a contact is set to a status of Bad Address if the number of hard bounces logged for the address exceeds a defined threshold and is set to a status of Undeliverable if the number of soft bounces logged for the email address exceeds a defined threshold. To configure the value of this threshold, perform the steps in the following procedure.

To configure how the email address status is determined

1. Navigate to the Administration - Business Process screen, Workflow Policies, and then the Policies view.
2. In the Policies list, query for the Update Contact Email Status object in the Workflow Object field.
3. Select either the Update Contact Email Hard Bounce Status policy or the Update Contact Email Soft Bounce Status policy.
4. Navigate to the Conditions list, then enter a number in the Value field, for example, 10.

The number you enter becomes the threshold used to determine when a contact's email address is assigned a status of Bad Address (hard bounces) or Undeliverable (soft bounces).

Implementing Spam Scoring of Email Templates Using SpamAssassin

This topic describes how to configure Email Marketing to integrate with SpamAssassin so that users can generate spam scores for email treatment templates before they are used in a campaign.

Generating a spam score for an email treatment template allows Siebel Marketing users to assess whether the emails generated using the template are likely to be classified as spam and be rejected by recipient's spam filters. If the email template generates a high spam score, then users can then modify the email template content until it passes the spam scoring test.

Siebel Marketing uses Apache SpamAssassin, an open source product released under the Apache License 2.0, to run the spam scoring test. SpamAssassin provides an API for an email sending component, in this case, the Email Sending Daemon, to test an email message against the scoring system and report any potential problems.

After spam scoring is enabled, when a user clicks the Verify and Preview button on the email editor to preview an email template message, spam scoring data for the email is displayed, including content analysis details and descriptions, as shown in the following image. The user can then manually correct any issues and preview the email template again to re-score the content.

```
Spam: True ; 15.3 / 6.3
Content analysis details:   (15.3 points, 6.3 required)
-0.0 NO_RELAYS              Informational: message was not relayed via SMTP
 2.5 MISSING_HB_SEP         Missing blank line between message header and body
 0.2 MISSING_HEADERS        Missing To: header
 3.4 URIBL_JP_SURBL         Contains an URL listed in the JP SURBL blocklist
                            [URIs: deferrt.com]
 1.5 URIBL_WS_SURBL         Contains an URL listed in the WS SURBL blocklist
                            [URIs: deferrt.com]
 2.6 URIBL_OB_SURBL         Contains an URL listed in the OB SURBL blocklist
                            [URIs: deferrt.com]
 3.6 URIBL_SC_SURBL         Contains an URL listed in the SC SURBL blocklist
                            [URIs: deferrt.com]
 1.3 MISSING_SUBJECT        Missing Subject: header
-0.0 NO_RECEIVED            Informational: message has no Received headers
 0.1 TO_CC_NONE             No To: or Cc: header
```

Siebel Marketing does not embed Spam Assassin, but the Email Sending Daemon can be connected to a Spam Assassin instance. This involves installing the Spam Assassin application, then configuring the Email Sending Daemon to connect to the SpamAssassin service as described in the following procedure.

To implement spam scoring of email templates using SpamAssassin

1. Download and install SpamAssassin from the Apache SpamAssassin Web site at

   http://spamassassin.apache.org/
2. Extract the files from the zip file you downloaded into a folder named SpamAssassin.

3. Start the SpamAssassin server using one of the following procedures:

   - If the Email Sending Daemon and SpamAssassin are running on the same computer, then open a command prompt Window and enter the following command to start the SpamAssassin server:

     ```
     spamd -d
     ```

     By default, the spamd -d command accepts connections only from the local system. For example:

     ```
     C:\SpamAssassin >spamd.exe
     ```

   - If the Email Sending Daemon and SpamAssassin are located on different computers, then use the following command at the DOS prompt to start SpamAssassin:

     ```
     spamd -d -i listen_ip_address -A allowed_hosts
     ```

     where:

     - *listen_ip_address* is the address on which SpamAssassin is to listen.
     - *allowed_hosts* is a list of the IP addresses authorized to connect to this SpamAssassin instance.

     For example, enter the following (in this example, 0.0.0.0 indicates that SpamAssassin is to listen on all IP addresses):

     ```
     C:\SpamAssassin >spamd.exe -D -i 0.0.0.0 -A ESD_Machine_I.P
     ```

4. You must now connect the Email Sending Daemon to the SpamAssassin Server by editing properties in the esd.properties file as follows:

   a. Navigate to the esd.properties file in the *ESD_root* installation directory.
   b. Open the esd.properties file in a text editor.
   c. Locate the SpamAssassin Server Setup section of the file, then add values for the parameters shown in the following table.

Parameter	Value
esd.spamServer	Enter the host name of the SpamAssassin server. Specifying a value for this parameter enables the spam scoring feature. If you do not want to enable spam scoring, then leave the value of this parameter as esd.spamServer=CHANGE_ME.
esd.spamPort	The port number used by SpamAssassin. The default is 783.
esd.reportSpamErrors	Set this parameter to true so that SpamAssassin error messages are displayed to the user, for example, if an error occurs connecting to the SpamAssassin server.

Parameter	Value

Authentication Mechanism of Email Marketing Server

Siebel Email Marketing server only supports AUTH-LOGIN authentication mechanism, changes are made to introduce AUTH PLAIN authentication mechanism in Email sending daemon (ESD) of EMS.

Our implementation addresses the issue of missing AUTH PLAIN mechanism used by major SMTP servers, Also it provides a way to make use of OCI Email delivery Service for email campaign.

Caveat for Using OCI Email delivery service

You should be able to send the email for email campaign however you won't be able to get the delivery status of the email sent. Call status may show false positive in case of failure in "Campaign Load Wave Contact/Prospect List Applet?, under Campaign view.

Following are the scenarios and AUTH mechanism picked:

1. When SMTP server supports only AUTH-PLAIN, AUTH-PLAIN will be used for authentication.
2. When SMTP server supports only AUTH-LOGIN, AUTH-LOGIN will be used for authentication.
3. When SMTP server supports both AUTH-LOGIN & AUTH-PLAIN, AUTH-LOGIN will be used for authentication.

6 Setting Up Web Marketing

Setting Up Web Marketing

This chapter describes how to set up Web Marketing. It includes the following topics:

- *About Siebel Web Marketing*
- *About Web Marketing Web Site Visitors*
- *Setting Up Siebel Web Marketing*

About Siebel Web Marketing

Oracle's Siebel Web Marketing is an optional Siebel Marketing module that provides you with the tools and templates to manage and execute Web-based marketing. It provides the Web site visitor a method of viewing a Web offer, downloading literature, and using preconfigured Web response forms to request more information or ask you to contact them by telephone.

A Web Survey Daemon resides in the DMZ and supports Web landing sites and surveys without the need for SmartScript. For information on how to create Web landing sites and surveys, see *Siebel Marketing User Guide* .

Siebel Web Marketing Web sites can be deployed in more than one language. For information about deploying Siebel applications in a multilingual environment, see *Siebel Global Deployment Guide* .

About Web Marketing Web Site Visitors

A Web site visitor can navigate to the Web Marketing home page by typing the URL or by clicking a link on another Web page. At this point, the user is an anonymous visitor and can choose to register, log in (if they have an existing user name and password), or continue to navigate anonymously. When the anonymous visitor arrives at the Web Marketing home page, the default campaign offers and the details for the first offer in the Featured Offers list appear. If the visitor registers or logs in, the visitor sees other campaign offers for which they are eligible. For more information about default offers and default campaigns, see the description of featured offers in *Siebel Marketing User Guide* .

If a contact logs in using the contact's user ID and password, any responses generated by this customer are tagged with the customer's account ID and with the associated campaign ID. For information about setting up users, see *Setting Up Default Responsibilities and Users for Web Marketing*.

Web site visitors can also navigate to the Web Marketing site by clicking on an embedded URL from within an email offer. Only contacts or prospects receive these offers. When an email contact or email prospect clicks an embedded URL, the Web Offer page for this offer appears. Any responses to the offer from this contact or prospect are tagged with the associated campaign ID and offer ID, so marketers can track response rates for specific campaigns. For a list of responses that are captured, see *Response Management*.

How Visitors Access the Web Marketing Home Page

Visitors access the Web Marketing home page in the following ways:

- **Anonymous visitor.** Any visitor can enter the Web Marketing URL into a Web browser and navigate to your Web Marketing home page. This visitor sees no personalized Welcome message and responses are not captured when the visitor clicks a Recommended Product link or downloads literature. An anonymous visitor can create a product information or call response by clicking on the Send Product Information or Request a Call link in the Offers page or Information page. The profile information that the anonymous visitor enters creates a prospect record that is associated with the responses.
- **Email contact.** When a contact clicks an embedded link in an email, your Web Marketing home page appears and the Contact Id is set in an anonymous session. At this point, the email contact is not logged in. The contact must be a registered contact and must log in to access profile information in the My Accounts link or to perform any other tasks that require the contact to be a registered contact. The email contact can generate responses by clicking a Recommended Product link, downloading literature, or requesting product information or a telephone call.

  In the Web Marketing home page, the contact can log in. After logging in, the email contact becomes a logged-in contact.

  If an email contact clicks the My Accounts link during an anonymous session, the User Login (user registration) view appears, requiring the anonymous visitor to log in before continuing.
- **Email prospect.** When a prospect clicks an embedded link in an email, your Web Marketing home page appears and the Prospect Id is set in an anonymous session. At this point, the email prospect is not logged in. The prospect must become a registered contact and must log in to access profile information in the My Accounts link or to perform any other tasks that require the prospect to be a registered contact. The email prospect can generate responses by clicking a Recommended Product link, downloading literature, or requesting product information or a telephone call.

  In the Web Marketing home page, the email prospect must register as a new contact before the prospect can log in. In the User Login view, the email prospect can enter a user ID and password or click the New User link to register as a new contact and obtain a user ID and password.

  In the User Login view, the User Login (user registration) view appears, requiring the anonymous visitor to log in or to register as a new user before continuing. When registration is complete, the prospect is converted to a new logged-in contact. However, the original email prospect's responses are not associated with the new contact record. After logging in, the email prospect becomes a logged-in contact.

  > **Note:** If an email prospect clicks the My Accounts link during an anonymous session, the User Login (user registration) view appears, requiring the anonymous visitor to log in or to register as a new user before continuing.

- **Logged-in contact.** This contact has access to the My Account link and can perform all other tasks that a registered contact is eligible to perform. The logged-in contact can generate responses by clicking a Recommended Product link, downloading literature, or by requesting product information or a telephone call. These responses are associated with the contact record in the Siebel database.

Setting Up Siebel Web Marketing

This topic describes how to set up Siebel Web Marketing. It includes information about customizing the user interface, controlling user access, setting up responsibilities, and managing default campaigns and offers.

Before Siebel Web Marketing can be used, certain setup tasks must be performed. These include:

- *Installing Web Marketing*
- *Installing the Web Survey Daemon*
- *Configuring the Web Survey Daemon*
- *Controlling User Access to the Web Marketing Web Site*
- *Setting Up Default Responsibilities and Users for Web Marketing*
- *Setting Up a Default Campaign and Default Offer*
- *Using Siebel Personalization with Web Marketing*
- *Customizing the Web Marketing User Interface*

Installing Web Marketing

Before you install and use Web Marketing, you must install the following:

- **Siebel Web Engine.** To deploy information about the Web and customer applications, you must install the Siebel Web Engine and the components on which it depends. These include a Web server, Siebel Gateway, Siebel Server, and Siebel Application Interface. For information about installing Siebel components, see *Siebel Installation Guide* .
- **Siebel Applications.** To perform administrative tasks such as server administration, creating Web offers, and managing marketing activities, you must install a Siebel employee application such as Siebel eSales and add the Siebel Web Marketing license key. For information about setting up your Siebel employee application, see the appropriate administration guide, for example, *Siebel eSales Administration Guide* .

  Siebel Web Marketing. An add-on module to Siebel Marketing, Siebel Web Marketing requires the Web Marketing Object Manager component, which is part of the Marketing Component Group. For information about installing Siebel Marketing, see *Installing and Administering Siebel Marketing* and *Siebel Installation Guide* .

Installing the Web Survey Daemon

The Web Survey Daemon (WSD) resides in the DMZ and supports Web landing sites and surveys without the need for SmartScript. For information on how to create Web landing sites and surveys, see *Siebel Marketing User Guide*.

This topic contains the information that you need to install the Web Survey Daemon. Before installing the Web Survey Daemon, make sure that you have completed the installation requirements:

- Java Runtime Environment (JRE)
- Oracle Database, MS SQL Server, or DB2 database, with JDBC drivers

Note: The Oracle JDBC driver is included with WSD. For Microsoft SQL Server and IBM Db2, users must obtain the appropriate JDBC driver from the database vendor and add the driver JAR to `WSD_HOME\webapps\websurveys\WEB-INF\lib` before starting WSD.

Installing the Web Survey Daemon on Windows

The following procedure describes how to install the Web Survey Daemon on a Windows server.

To install the Web Survey Daemon on Windows

1. On a Windows server, run the Web Survey Daemon installation program, wsd_install.exe.
2. In the Installation dialog box, review the information, and then click Next.
3. In the Choose Java Virtual Machine dialog box, select the JRE that you installed in *Requirements for Installing Email Marketing*, and then click Next.

   Note: Make sure that you choose the correct JRE. Selecting the wrong JRE will not properly start the Daemon.

4. In the Choose Install Folder dialog box, choose the Web Survey Daemon installation directory, and then click Next.
5. Review the Pre-Installation Summary dialog box, and then click Install.
6. In the Install Complete dialog box, verify the information, and then click Done.
7. Create a Windows service file for stopping and starting the Siebel Web Survey Daemon as follows:
   a. Navigate to the directory where you installed the Web Survey Daemon in Step 4.
   b. Locate the install-win32-service.bat file, then double-click the file.

      The Web Survey Daemon service file is created in the Windows services list.
8. From the Start menu, choose Programs, Administrative Tools, and then the Services menu item.
9. Start the Siebel Web Survey Daemon service.
10. Verify that the Apache Welcome page is displayed when you access the server where the Web Survey Daemon has been installed.

Installing the Web Survey Daemon on UNIX

The following procedure describes how to install the Web Survey Daemon on a UNIX server.

To install the Web Survey Daemon on UNIX

1. On a UNIX server, perform the following steps:
   a. Make an installation directory named wsd using the following command:

      ```
      mkdir wsd
      ```

   b. Copy the Web Survey Daemon installation program from the installation media to the directory that you created.
   c. In the Web Survey Daemon installation directory, run the Web Survey Daemon installation program.
2. In the WSD installation directory, open the tomcat-ctl.sh file and, after the line `#Execute the bundled (integrated) tomcat,`add the following:

   ```
   # get the name of this program
   JAVA_HOME=/usr/jre1.5.0_06
   export JAVA_HOME
   ```

3. Before the text, `# get the name of this program`, add the following line:
   `PROGNAME=`basename $0``
4. In the bin directory for the WSD installation, open the setenv.sh file and make sure the path provided for configuration directory is correct. For example:

   ```
   CATALINA_OPTS="-Dwebsurvey.configDir=/export/home/qa7/wsd/webapps/websurveys/config"
   ```

5. Use the `CHMOD 777 *` command to grant Read, Write, and Execute permissions to all the files in the WSD directory.
6. Configure the WSD. For details, see *Configuring the Web Survey Daemon*.

Configuring the Web Survey Daemon

This topic describes the tasks you must perform to configure the Web Survey Daemon after it is installed. After configuring the WSD, you must also configure the outbound Web service in Siebel Marketing for the Web Survey Daemon. It includes the following topics:

- *Prepare the WSD Database*
- *Configuring the Web Survey Daemon*
- *Configuring the Web Survey Outbound Web Service*

Prepare the WSD Database

This procedure is used for a new Web Survey Daemon (WSD) installation.

To prepare the WSD database:

- Prepare an empty database or schema before running a WSD database creation script.
- Do not run a creation script against an existing WSD schema or a schema that contains objects from an incomplete installation.
- The database creation script creates two WSD accounts.
- Select a distinct password for each account that complies with your organization's password policy.

Credential	Purpose	Value used during database preparation
Database owner	Connects the database client and creates the WSD schema objects	Database password
WSD system	Signs in to the WSD administration application	Encrypted WSD password
WSD SiebelSystem	Authenticates WSD communication with Siebel Marketing	Encrypted WSD password

- Retain the clear passwords in an approved credential store. You need the clear system password to sign in to WSD and the clear SiebelSystem password when you configure the Web Survey outbound Web service.

> **Note:** Do not enter an encrypted value in a WSD or Siebel application password field.

Generate the Encrypted WSD Passwords

The WSD database creation scripts require values generated by OccamCrypto. Run the following command separately for the selected system and SiebelSystem passwords:

```
java -cp "<WSD_WEBAPP_ROOT>/WEB-INF/lib/occam-crypto.jar" com.siebel.occam.security.OccamCrypto
encrypt <password>
```

Replace <WSD_WEBAPP_ROOT> with the installed WSD Web application directory and <password> with the applicable clear password. Copy only the encrypted value printed by the command. Keep the two outputs identified by account so that each value is entered at the correct database-script prompt.

The command receives the clear password as a command-line argument. Run it from an approved administrative session and protect command history, process information, terminal output, and copied values according to your organization's credential-handling requirements. Treat the encrypted output as a credential.

Database Requirements

The following table describes the database requirements:

Database	Requirements
Oracle Database	An empty WSD schema, its schema-owner credentials, and SQL*Plus
Microsoft SQL Server	An empty WSD database, a table-owner SQL login with the required object-creation privileges, Windows PowerShell 5.1 or later, Microsoft ODBC Driver 18 for SQL Server, and sqlcmd on PATH
IBM Db2	An empty WSD schema, an authorized database user, the COMM_SPACE table space, and IBM CLPPlus in interactive mode; do not use classic Db2 CLP

Prepare an Oracle Database

To prepare an Oracle Database for WSD:

1. Create an empty WSD schema and grant its owner the privileges required to create the WSD schema objects.
2. Start SQL*Plus as the WSD schema owner. Omit the password from the command line:
   ```
   sqlplus -L <WSD_SCHEMA_USER>@<CONNECT_IDENTIFIER>
   Enter password: <database_owner_password>
   ```
3. At the SQL*Plus prompt, run the installed database creation script:
4. At each protected prompt, paste only the encrypted value generated for the named account, and then press Enter. The value is not displayed.
5. Confirm that the database creation script executed successfully and review the session for errors before exiting.

Prepare a Microsoft SQL Server Database

You need to use the Windows PowerShell launcher script to run communicatorSqlServer.sql.

To prepare a SQL Server database for WSD:

1. Create an empty WSD database. Prepare a table-owner SQL login with the required object-creation privileges and set its default schema to the schema in which the WSD objects will be created.
2. Open Windows PowerShell 5.1 or later and change to the installed WSD SQL directory:
   ```
   Set-Location "<WSD_HOME>\sql"
   ```
3. Run the launcher with the SQL Server endpoint, empty database, table-owner login, and expected table-owner schema:

```
.\runCommunicatorSqlServer.ps1 `
-Server "tcp:<SQL_SERVER>,<PORT>" `
-Database "<WSD_DATABASE>" `
-TableOwnerUser "<TABLE_OWNER_LOGIN>" `
-TableOwner "<TABLE_OWNER_SCHEMA>"
```

4. At the hidden prompts, enter the table-owner database password and the two encrypted WSD values in the following order:
   - encrypted password for system;
   - encrypted password for SiebelSystem.
5. Confirm that the launcher reports WSD SQL Server bootstrap completed successfully. and returns exit code 0.

The launcher verifies the selected database and the table-owner's default schema and stops if it finds an existing WSD table. Certificate validation is enabled by default. If the server certificate has been reviewed but its issuing authority is not trusted by the Windows host, add -TrustServerCertificate. This option accepts the server certificate without validating its certificate chain and must be used only in accordance with your organization's security policy.

Prepare an IBM Db2 Database

The Db2 database creation script uses CLPPlus protected prompts and substitution variables. Run it with IBM CLPPlus in interactive mode, not with classic Db2 CLP.

To prepare a Db2 database for WSD:

1. Create an empty WSD schema and confirm that the target database contains a usable COMM_SPACE table space.
2. Start CLPPlus as the authorized database user:
   ```
   clpplus <DB_USER>@<DB_HOST>:<PORT>/<DATABASE>
   Enter password: <database_owner_password>
   ```
3. Confirm that the connected user, database, and current schema are the intended WSD targets.
4. At the CLPPlus prompt, run the installed database creation script:
   ```
   SQL> @<WSD_HOME>/sql/communicatorDB2.DDL
   Enter encrypted password for WSD system:
   Enter encrypted password for WSD SiebelSystem:
   ```
5. Confirm that the query returns one row for system in organization 1 and one row for SiebelSystem in organization 2.

   Do not select or record the PASSWORD column.
6. After WSD starts, sign in as system with its selected clear password. Use the selected clear SiebelSystem password when configuring the Web Survey outbound Web service.

Verify the Database Preparation

To verify the database preparation, after the database creation script completes:

1. Review the complete client output and confirm that it contains no database errors.
2. While connected as an authorized database user, run the following query:
   ```
   SELECT LOGIN, ORG_ID
   FROM COMMON_USER
   WHERE (LOGIN = 'system' AND ORG_ID = 1)
   OR (LOGIN = 'SiebelSystem' AND ORG_ID = 2);
   ```
3. Confirm that the query returns one row for system in organization 1 and one row for SiebelSystem in organization 2. Do not select or record the PASSWORD column.
4. After the WSD starts, sign in as system with its selected clear password.

Use the selected clear SiebelSystem password when configuring the Web Survey outbound Web service.

Troubleshoot WSD Database Preparation

To troubleshoot WSD database preparation:

Symptom	Resolution
Java reports that OccamCrypto cannot be found or loaded	Confirm that Java is available and that <WSD_WEBAPP_ROOT>/WEB-INF/lib/occam-crypto.jar exists. Retain any additional class-path entries required by the installed WSD delivery.
A required database client is not found	Install and configure SQL*Plus for Oracle Database, sqlcmd and Microsoft ODBC Driver 18 for SQL Server, or IBM CLPPlus for Db2. Confirm that the required executable is available on PATH.
An encrypted-password prompt rejects the value	Generate the value again for the intended account. Supply a single-line value of no more than 100 characters. Do not enter a blank value, CHANGE_ME, or a value containing internal whitespace. Leading and trailing whitespace from copying and pasting is removed.
Nothing appears when a password is typed or pasted	The database scripts and SQL Server launcher use hidden prompts. The absence of displayed characters is expected. Enter or paste the value once and press Enter.
The database client cannot connect	Verify the host, port, database or service name, database-owner login, password, and network access. Confirm that the connected owner and current schema are the intended WSD targets.
SQL Server reports a database or table-owner schema mismatch	Verify Database, TableOwnerUser, and TableOwner. The table-owner login's default schema must match TableOwner.
SQL Server reports that the certificate chain is not trusted	Configure the Windows host to trust the issuing authority. Use -TrustServerCertificate only after the certificate has been reviewed and organizational policy permits bypassing certificate-chain validation.
Db2 reports an error involving ACCEPT, HIDE, or an & variable	Confirm that the script is running in interactive IBM CLPPlus. Classic Db2 CLP does not support the required prompt and substitution behavior.
Db2 reports that COMM_SPACE is undefined or unavailable	Have the Db2 administrator create or make available the required COMM_SPACE table space, and then retry against an empty schema.
The script reports that an object already exists	Stop the procedure. Verify that the selected schema is intended for a new WSD installation. Do not run the script over existing WSD objects.
A database error occurs after table creation begins	The schema can be partially created. Use your approved database cleanup or restore procedure to return to an empty schema before retrying. Do not rerun the creation script over partial objects.

Configuring the Web Survey Daemon

Perform the steps in the following procedure to configure the WSD.

Configure the Web Survey Daemon

1. Prepare the WSD database and create the WSD schema objects. For instructions for Oracle Database, Microsoft SQL Server, or IBM Db2, see *Prepare the WSD Database*.

2. In the webservey.properties file located at `WSD_HOME \webapps\websurveys\config`, define the parameters shown in the following table.

> **Note:** Do not use either encrypted WSD account value for this parameter. The database owner password is used by WSD to connect to the database; the system and SiebelSystem passwords authenticate their respective WSD accounts.

Parameter	Value
db.driver	Set db.driver to the driver class for the WSD database: For Oracle database: `com.siebel.sem.jdbc.oracle.OracleDriver` For Microsoft SQLServer database: `com.siebel.sem.jdbc.sqlserver.SQLServerDriver` For IBM DB2 database: `com.siebel.sem.jdbc.db2.DB2Driver`
db.WEBSURVEY.password	*WSD database user's password* **Note:** The password must be encrypted. To encrypt strings, make sure occam-crypto.jar is in the classpath. At the command line, type: `java com.siebel.occam.security.OccamCrypto encrypt string.` Use the output to make entries in the properties file.
db.WEBSURVEY.url	Make sure the database URL is set for the appropriate database type. Sample URLs are provided in the configuration file.
db.WEBSURVEY.user	*WSD database* user
DEFAULT_RESPONSE_DAEMON_ SLEEP_TIME	Sleep time in milliseconds for the response processor daemon.
QueueFlushInterval	Interval in milliseconds that the response processor is invoked.
QueueMaxSize	Max Queue size after which the response processor is invoked.
SIEBEL_PASSWORD	Siebel Password for response Web Service call.
SIEBEL_URL	Siebel endpoint URL for response processing.

Parameter	Value
SIEBEL_USERNAME	Siebel Username for response Web Service call.
survey.baseURL	*MachineName:port*/websurveys
WebSurveyHandlerClassName	oracle.apps.sem.wsd.runtime.queueing.MBQQueueHandler
WebSurveyProcessorClassName	oracle.apps.sem.wsd.response.ResponseDataProcessor
WebSurveyQueueDirectory	Directory where the queue files will be written. The default directory is **`WSD_home_directory\webapps\websurveys'ueueing`**. You can specify a different location if you choose.

3. (Optional) Configure advanced settings in the websurveys.properties file.

Parameter	Value
systemCache.active	This is an optional but recommended system cache setting to activate the WSD's object cache. Default is true.
systemCache.maxSize	This is an optional system cache setting to specify the maximum number of Java objects to keep in the Web survey's cache. Default is 9216.
systemCache.maxAge	This is an optional system cache setting to specify the maximum age (in milliseconds) of objects in the cache. Default is 3,600,000 (one hour).
systemCache.cleanFrequency	This is an optional system cache setting to specify how often (in milliseconds) the cache is cleaned. Default is 300,000 (5 minutes).
respondentCache.active	This is an optional (but highly recommended) respondent cache setting to activate the Web survey's object cache. Default is true.
respondentCache.maxSize	This is an optional respondent cache setting to specify the maximum number of respondents' answers that will be kept in the Web survey's cache. Default is 1024.
respondentCache.maxAge	This is an optional respondent cache setting to specify the maximum age (in milliseconds) of objects in the cache. Default is 1,200,000 (20 minutes).

Parameter	Value
respondentCache.cleanFrequency	This is an optional respondent cache setting to specify how often (in milliseconds) the cache is cleaned. Default is 60,000 (1 minute).
SOCKET_TIMEOUT	This is a response processor setting that adjusts the timeout of the network socket used to communicate with the response import Web Service. It prevents a socket timeout from occurring when the import Web Service needs more time to process the responses (due to resource issues or the batch size). Default is 300,000 ms.

4. (Optional) If you are running the WSD in a load-balanced, multi-server configuration, list the base URLs of each computer in your configuration in the Multi-Server Settings section of the websurveys.properties file. These URLs go directly to the individual computers, bypassing whatever load balancing facility you are using. Be sure to include the application context path (typically /websurvey). For example:

```
#server.1 = http://websurvey01.example.com/websurvey
#server.2 = http://websurvey02.example.com/websurvey
#server.3 = http://websurvey03.example.com/websurvey
```

5. On a Windows server, start the Siebel Web Survey Daemon service.
6. On a UNIX server, enter and run the following command:

```
./tomcat-ctl.sh start
```

Configuring the Web Survey Outbound Web Service

Perform the steps in the following procedure to configure the Web Survey outbound Web service for the WSD.

Configure the Web Survey Outbound Web Service for the WSD

1. Navigate to the Administration - Web Services screen, and then the Outbound Web Services view.
2. Configure the IP address and port for the Web Survey outbound Web service to point to the appropriate computer name and port where the WSD is running. For example:

```
http://MachineName:8088/websurveys/services/WebSurveyWebService?wsdl
```

3. Configure the Web Survey Daemon server record with the WSD Web service credential:
   a. Navigate to the **Administration** > **Marketing screen** and then the **Servers view**.
   b. Query for **Web Survey Daemon**.
   c. Use `SiebelSystem` as the user name. Enter the clear SiebelSystem password selected during *Preparing the WSD Database*, and then save the record.

   Whenever the SiebelSystem password is changed in WSD, update the Web Survey Daemon server record with the same clear password before resuming Web Survey service operations.
4. (Optional) If the default port 8080 is unavailable, you can change the port by doing the following:

   a. Navigate to `%CATALINA_HOME%\conf` and open the server.xml file.
   b. Edit the port number in the following section:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
```

```
<Connector port="< your port No.>" maxHttpHeaderSize="8192"
```

c. Restart Apache Tomcat server.

Controlling User Access to the Web Marketing Web Site

You can perform some of the following tasks to control user access in your Siebel Web Marketing Web site:

- Using external authentication using LDAP (Lightweight Directory Access Protocol)

  LDAP is an Internet protocol that email programs use to look up contact information from a server.
- Creating database users for LDAP to use in database access
- Defining visibility for views and products
- Assigning a proxy employee
- Creating users through registration or user administration
- Associating users with accounts
- Allowing various levels of access such as Anonymous, Implicit login, and Explicit login
- Customizing access to home and login pages

  For more information, see about the New User link in *Siebel Marketing User Guide* .
- Using single-sign on functionality
- Allowing another application to log in
- Adding fields to registration forms

For more information about controlling user access, see *Siebel Security Guide* .

Setting Up Default Responsibilities and Users for Web Marketing

Responsibilities control which views the users can display. The views to which a user has access determines the links and page tabs that the user sees. For example, if a user has a responsibility that does not permit access to the Credit Cards view, no Credit Cards link appears in the My Settings view. If no views within a business object are visible, the page tab that maps to that business object is not visible.

The responsibilities predefined for Siebel Web Marketing include:

- **Web Anonymous User.** Grants view visibility to anonymous users such as anonymous visitors, email prospects, and email contacts. For more information about these user enters, see *About Web Marketing Web Site Visitors*. This responsibility allows the user to access views that do not have the Requires_Explicit_Login flags set to TRUE in Siebel Tools. For more information, see *Siebel Tools Online Help* .
- **Web Registered User.** End user in a business-to-consumer model such as logged-in contact. For more information about these user types, see *About Web Marketing Web Site Visitors*. This user has registered and is recognized by the Siebel Marketing application either through his or her login, or because the user enters the site by clicking an embedded link in an email offer.
- **Web Corporate User.** End user in a business-to-business model. A Web corporate user is associated with an account and must be authorized by the Web Delegated Customer Administrator to access the site. An administrator can add new Web corporate users.

For more information about setting up and managing responsibilities, see *Siebel Security Guide* .

Setting Up a Default Campaign and Default Offer

Assigning a default campaign and offer is part of the Web Marketing setup process. An offer associated with the default campaign can be designated as the default offer. The default campaign and default offer determine which offers are presented to the customer during his or her Web Marketing session. These offers appear in addition to any targeted offers such as an embedded link in an email offer. For more information about configuring default offers and default campaigns, see *Siebel Marketing User Guide* .

Using Siebel Personalization with Web Marketing

Siebel Personalization delivers personalized content and offers to a customer profile, needs, interests, and history. Personalized content includes greeting users by name, presenting them with content targeted to their needs and interests, and showing them recommended products and offers based on their needs and history.

Using Siebel Personalization, you can define rules to show and hide content dynamically during a user's experience with Siebel Web Marketing. Personalization deployment rules can depend on data such as user's profile information, date ranges, company information, products and services they already purchased or reviewed, and specific session information.

The home page in Siebel Web Marketing includes the salutation applet. It typically includes a personal greeting but it can be configured to deliver targeted content such as product promotions, announcements, birthday greetings, and offer updates. The home page also contains a list of recommended products and featured offers, both of which can be personalized based on user-specific information. Conditional expressions can be used to hide applets under certain conditions.

You manage personalization in the Personalization Administration screen in your Siebel application. For information about administering personalization, see *Siebel Personalization Administration Guide* .

Customizing the Web Marketing User Interface

The product provides a set of Web templates and cascading style sheets (CSS) to create the look and feel of an Oracle Siebel application. Customers can create their own look and feel by modifying corporate logos, colors, and fonts in the style sheets and Web templates. When modifying these elements, make sure you save a backup copy in case you need to restore the original files.

Note: These elements are not automatically upgraded during the upgrade process.

The Siebel Web architecture uses the Siebel Application Interface to dynamically generate HTML pages from the configuration information in the Siebel runtime repository.

To customize the Web Marketing User Interface, perform the following tasks:

- *Modifying Web Templates*
- *Implementing Web Marketing without Frames*

- *Full-Text Search*
- *Response Management*

If you are using Web Offers with a custom Web site rather than the prebuilt Siebel microsite, do not use the standard response types such as Downloads, Request Unsubscribe, Web Survey, and so on. These response types do not work because they generate Siebel specific URLs that do not function without additional scripting. An easier solution is to use Trackable URLs for your links.

Modifying Web Templates

A Web template defines the layout and formatting elements of the user interface (UI), such as views, applets, and controls. You associate these UI elements with the templates in Siebel Tools. The associated information is stored in the Siebel runtime repository. For example, you might have a View object with three applets. You associate a View Template with the view, and map each applet to a placeholder in that template. The advantage of this approach is that the UI objects in the repository are not hard-coded in individual templates. As a result, a number of View objects can share the same template if they share the same layout. The same process and design applies to Applet objects.

The three primary templates types are Container, View and Applet. The final HTML pages created by the Siebel Application Interface places the applet in the view and the view in the container. Siebel CRM provides numerous applet and view templates with the product. They can be viewed in Tools, but are edited in an external editor. For information about the physical user interface layer, see *Siebel Tools Online Help* .

The following is a list of some modifications available to change the look and feel of your Web site:

- Modifying Views and Applets
- Modifying Web Templates
- Changing colors
- Modifying behavior caused by clicking a button
- Adding or removing applets
- Changing controls
- Making fields in a form appear

For more information about customizing the user interface, see *Siebel Tools Online Help* .

Implementing Web Marketing without Frames

Customer and partner applications use HTML frames for compatibility when running in browser-based applications. HTML frames create portions of the browser window that can navigate independently of the rest of the window. For example, you can place the navigation elements in one frame and content in another frame. You can navigate the content while the navigation elements remain in a fixed location.

Customer and partner applications can be implemented without using frames. Before choosing this method, consider the following limitation. In an unframed application, all UI elements exist in the same window. Therefore, the contents list might move off the page as a user navigates down. For example, if the user navigates down to review content, the navigation elements might not be visible.

Full-Text Search

Siebel Search for Customers is a subset of the Siebel Search product. Users can scan database tables and documents for pertinent information. Siebel Search is included with every license of an Oracle Siebel application. For information about Siebel Search and Siebel Search for Customers, see *Siebel Search Administration Guide* .

Response Management

Siebel Web Marketing captures a series of responses during a customer interaction. Siebel Web Marketing supports automatic capture of the following responses:

- Clicked on Web Offer. Captured when the recipient clicks the embedded link for a Web offer in an email offer.
- Clicked on Product URL. Captured when the recipient clicks the embedded link for the product in an email or Web offer.
- Clicked on Web Survey. Captured when the recipient clicks the embedded link for the Web survey in an email or Web offer.
- Completed Web Survey. Captured when the recipient submits his or her survey responses, after clicking the embedded link in an email. To view the response, navigate to the Responses screen.
- Downloaded Info or File. Captured when the recipient clicks the embedded link for the document that is downloaded in a Web offer.
- Requested Unsubscribe. Captured when the recipient submits his or her subscription preference updates after clicking the embedded link in the email offer. In addition to the response, the contact profile is updated.
- Requested call back. Captured when the recipient submits his or her request after clicking the embedded link in an email or Web offer.
- Requested more info. Captured when the recipient submits his or her request after clicking the embedded link in an email or Web offer.
- Submitted Source Code. Captured when a contact or prospect enters a source code and offer code in the Do you have Another Offer form in the Offers page.

Preconfigured Values for the COMM_RESPONSE_TYPE LOV

The following table shows the list of values for the COMM_RESPONSE_TYPE LOV that are seeded in the preconfigured Marketing product.

Note: The values that either trigger specialized logic or are automatically set by various features of the Siebel Marketing application must not be changed or deleted.

Values	Values Triggering Specialized Logic or Automatically Set
Language-Independent Code	Clicked on Product URL Clicked on Web Offer Clicked on Web Survey Completed Web Survey Downloaded info or file(s) Email Bounceback Email Reply
Rejected	Requested Unsubscribe Requested Call Back

Values	Values Triggering Specialized Logic or Automatically Set
	Requested More Info Respondent Purchased
Respondent Unreachable	Response Created Opportunity Read Receipt
Unclassified Response	None
No Interest	None
Respondent Interested	None
Accepted Invitation	None
Declined Invitation	None
Gave Referral	None
Requested Further Engagement	Submitted Source Code Clicked on URL
Attended	None
Cancelled	None
Confirmed	None
Invited	None
No Show	None
Pending	None
Waitlisted	None
Walk-in	Clicked on Event URL Forward to Friend Unsubscribe from List Subscribe to List One Click Unsubscribe

Values	Values Triggering Specialized Logic or Automatically Set
	Confirm Unsubscribe from List Confirm Subscribe to List

Additional responses and Siebel events can be captured through configuration. For more information, see event tracking topics in *Siebel Tools Online Help* .

Overriding Delete Protection for Phone and Web Offers

Active offers of type Phone or Web cannot be deleted by default. This prevents users from deleting offers that are in progress. You can override this delete protection at your own risk.

To override deletion protection for phone and Web offers

1. Start Siebel Tools.
2. Locate the Phone Offer or Web Offer Business Components.
3. Set the No Delete Protection user property to Y.

7 Segmentation Migration Utility

Siebel Segmentation Migration Utility

This chapter describes how to configure, run, and validate the Siebel Segmentation Migration Utility.

Here are the topics:

- *Overview of the Siebel Segmentation Migration Utility*
- *Prerequisites to Using the Siebel Segmentation Migration Utility*
- *Prepare to Run the Siebel Segmentation Migration Utility*
- *Run the Segmentation Migration Utility and Review the Results*
- *Architecture of the Migration*
- *Limitations of the Migration*
- *Incremental Migration for Large Campaign Sets*
- *Troubleshooting the Migration Results*

Overview of the Siebel Segmentation Migration Utility

The Siebel Segmentation Migration Utility migrates Siebel Marketing segmentation artifacts to analysis-based artifacts in Oracle Analytics Server (OAS). Then, it updates Siebel Marketing campaign references to use the migrated artifacts.

> **Note:** The Siebel Segmentation Migration Utility is separate from the existing Siebel Migration application. The utility delivered for this specific segmentation migration is named `mktg-seg-migration` and it's used specifically for Siebel Marketing segmentation migration.

The segmentation migration utility:

- Converts Segments to Analysis Artifacts.
- Converts Segment Trees to Analysis Collections.
- Converts List Export artifacts to Analysis Export artifacts when they're associated with migrated campaigns.
- Discovers eligible Siebel Marketing campaigns and their associated segmentation artifacts through Siebel REST APIs.
- Creates migrated OAS catalog artifacts by using the `M_` naming convention and links the generated analysis-based artifacts back to Siebel Marketing campaigns.
- Supports scoped migration through `siebel.campaign.searchspec`. If no search specification is provided, the application evaluates all eligible campaigns returned by Siebel.
- Provides application logs, audit logs, per-campaign status, and a command-line run summary for validation and troubleshooting.

Prerequisites to Using the Siebel Segmentation Migration Utility

Before configuring the Siebel Segmentation Migration Utility, ensure that you've done the prerequisites:

- *Import Certificates into a Truststore*
- *Prepare the OAS Repository Metadata File*
- *Enable Dynamic IO for Siebel REST Access*
- *Prepare the Repository File and Convert It to XML*

Import Certificates into a Truststore

Import both Siebel and OAS certificate chains into one shared truststore, for example `migration-truststore.jks`, and point `TRUSTSTORE_PATH` to that file.

Windows example:

```
keytool -importcert -alias siebel -file C:\path\to\siebel.cer
 -keystore C:\path\to\migration-truststore.jks -storepass <pwd> -noprompt
 keytool -importcert -alias oas -file C:\path\to\oas.cer -keystore
 C:\path\to\migration-truststore.jks -storepass <pwd> -noprompt
```

Linux example:

```
keytool -importcert -alias siebel -file /path/to/siebel.cer
 -keystore /path/to/migration-truststore.jks -storepass '<pwd>' -noprompt keytool -importcert
 -alias oas -file /path/to/oas.cer -keystore /path/to/migration-truststore.jks
 -storepass '<pwd>' -noprompt
```

Also see: *The keytool Command*

Prepare the OAS Repository Metadata File

Before configuring the segmentation migration utility, prepare the OAS repository metadata file. The segmentation migration utility uses this file to identify target levels and qualifying-key columns, such as `ROW_ID`.

See *Managing Metadata Repositories for Oracle Analytics Server* for more information.

Enable Dynamic IO for Siebel REST Access

Enable Dynamic IO for Siebel REST access and grant REST access to these business objects:

- Marketing Segment
- Mktg List Format

See *Supporting RESTful Access to Siebel Business Objects Dynamically* for more details.

Prepare the Repository File and Convert It to XML

If the Oracle BI Repository File (RPD) file isn't already available, download the active OAS repository file using Oracle's `downloadrpd` command.

The command is run through `datamodel.sh` on Linux or `datamodel.cmd` on Windows.

Use the target OAS or OBIEE RPD that contains the Siebel Marketing segmentation metadata. Siebel's segmentation migration utility doesn't migrate or remodel the RPD. It reads and filters the metadata required to generate the migrated Analysis and Analysis Collection artifacts, including target levels and qualifying-key columns such as `ROW_ID`.

If the target OAS or OBIEE repository already contains customer-configured Marketing metadata, prepare the XML from that active repository so that the segmentation migration utility can use the deployed metadata during migration.

After the RPD file is available, convert it to XML with Oracle's `biserverxmlgen` utility:

```
biserverxmlgen -M -R <rpd_path> -O <output_xml_path>
```

> **Note:** Oracle recommends prompting for repository and user passwords instead of placing passwords directly in scripts or command-line history.

The parent directory for the generated XML file must be writable. During preprocessing, the segmentation migration utility generates a sibling YAML file beside the XML file and uses that generated file during migration.

References

Topic	Oracle Reference
Download deployed RPD	*Download Repository Command*
Generate XML from RPD	*About the Oracle BI Server XML API*

Prepare to Run the Siebel Segmentation Migration Utility

Before running the Siebel Segmentation Migration Utility, you need to do some work to prepare for it:

Here are the preparation steps:

- *Locate the .zip File*
- *Extract the .zip Package*
- *Review the Package Contents*
- *Configure the Wrapper Script*
- *Configure the Properties File*
- *Review the Campaign State Before Migration*

Locate the .zip File

Locate the delivered `mktg-seg-migration.zip` package in the Siebel Server `bin` directory. For example, `<Siebel_Server_Root>/siebsrvr/bin`.

Extract the .zip Package

Extract the migration utility .zip file:

1. Extract the mktg-seg-migration.zip file into the working location for the migration run.
   - Linux/macOS:

     ```
     unzip <migration_application_zip> -d <target_directory>
     ```
   - Windows PowerShell:

     ```
     Expand-Archive -Path <migration_application_zip> -DestinationPath <target_directory>
     ```
2. Confirm that the package folder has been created successfully. The extracted folder is used in the subsequent configuration and execution steps.

Review the Package Contents

Review the package contents to ensure the correct files are present:

1. Open the extracted migration utility folder and verify that the expected runtime files are present.
2. Use these details:

File	Description
`run-mktg-seg-migration.sh`	Linux, Unix, or macOS wrapper script
`run-mktg-seg-migration.bat`	Windows wrapper script
`lib/mktg-seg-migration.jar`	Migration utility executable
`config/application.properties`	Main configuration file
`config/logback.xml`	Logging configuration
`README.md`	Package usage guide

3. Verify that the wrapper script, configuration file, executable JAR, and logging configuration are present before running the migration utility.

> **Note:** The wrapper script, configuration file, executable JAR, and logging configuration are required before running the migration utility.

Configure the Wrapper Script

Configure the wrapper script by updating the environment-specific parameters in the wrapper script:

1. Open the wrapper script for the operating system where the migration utility will run.
   - Linux, Unix, or macOS:

     `run-mktg-seg-migration.sh`
   - Windows:

     `run-mktg-seg-migration.bat`
2. Use these settings:

Setting	Description
`JAVA_HOME_PATH`	Java 21 JRE or JDK home directory
`TRUSTSTORE_PATH`	Path to the truststore prepared in the Certificate Truststore section
`TRUSTSTORE_PASSWORD`	Truststore password
`TRUSTSTORE_TYPE`	Truststore type, such as `JKS`
`LOG_DIR`	Directory where application and audit logs are written
`APP_LOG_LEVEL`	migration utility log verbosity
`ROOT_LOG_LEVEL`	Fallback log level for dependency and framework logging
`MAX_FILE_SIZE`	Log rollover threshold
`EXTRA_JAVA_OPTS`	Optional JVM options, such as heap settings

Note: Don't add Siebel or OAS passwords to the wrapper script. The migration utility prompts for those passwords at runtime.

Configure the Properties File

Configure `config/application.properties` before running the migration utility:

Open `config/application.properties` and enter the required Siebel, OAS, and RPD XML values.

Here are the properties:

Property	Required	Description
`siebel.api.url`	Yes	Siebel API endpoint
`siebel.api.username`	Yes	Siebel user
`oas.api.url`	Yes	OAS endpoint

Property	Required	Description
`oas.api.username`	Yes	OAS user
`rpd.xml.path`	Yes	Path to the RPD XML prepared in the Prerequisites section
`oas.session.timeout`	No	OAS session timeout in seconds
`migration.threads.count`	No	Worker thread count
`siebel.campaign.searchspec`	No	Optional Siebel campaign filter

Note: Don't store Siebel or OAS passwords in this file. The migration utility prompts for both passwords at runtime.

Review the Campaign State Before Migration

Before running the migration utility, open the campaign in Siebel Marketing and confirm the source segmentation artifact is still associated with the campaign.

- In the **Segments/Lists** view, the campaign should show the existing Segment or List artifact that will be migrated.
- In the **Allocation** view, confirm that the campaign allocation is still associated with the Segment or List artifact.
- The **Analyses/Lists** view in the L4 menu should not contain any records before migration.

Next step: *Run the Segmentation Migration Utility and Review the Results*

Run the Segmentation Migration Utility and Review the Results

Use these steps in this topic to run the Siebel Segmentation Migration Utility and then review the results:

Here are the steps:

- *Run the Migration Utility*
- *Enter Runtime Passwords*
- *Review the Terminal Command-line Summary*
- *Review the Audit Log*
- *Review the Campaign State after Migration*
- *Review Migrated Artifact in the OAS/OBIEE Catalog*

Run the Migration Utility

Run the wrapper script from the extracted migration utility folder.

- Linux, Unix, or macOS:

```
./run-mktg-seg-migration.sh
```

Windows:

```
run-mktg-seg-migration.bat
```

- To add a log tag for easier log identification, use `--tag`:

```
./run-mktg-seg-migration.sh --tag MIGR
```

```
run-mktg-seg-migration.bat --tag MIGR
```

- If the configuration file is stored outside the default `config/application.properties` location, pass it explicitly:

```
./run-mktg-seg-migration.sh --config/path/to/application.properties --tag MIGR
```

```
run-mktg-seg-migration.bat --config C:\path\to\application.properties --tag MIGR
```

Note: The wrapper prompts for Siebel and OAS passwords at runtime. Don't pass those passwords in the command.

Enter Runtime Passwords

After the wrapper starts the migration utility, the command line prompts for the Siebel password and the OAS password. Enter the passwords when prompted.

Note: The password characters aren't visible while typing. This is expected terminal behavior.

The passwords are used only for the current migration run. They're not stored in `application.properties` or in the wrapper script.

Review the Terminal Command-line Summary

After the migration utility completes, review the terminal command-line summary.

The command-line summary includes this information:

Field	Description
Total campaigns	Number of campaigns evaluated in the run
Successful campaigns	Number of campaigns migrated successfully
Failed campaigns	Number of campaigns that did not complete successfully
Duration	Total runtime for the migration command

If any campaigns fail, review the application log and audit log in the next steps.

Review the Audit Log

Review the audit log to see migration activity at the campaign and artifact levels:

1. After the run completes, open the generated audit log from the `logs` folder.

   The audit log file uses this naming pattern: `migration-audit-<timestamp>-<log-tag>.log`.
2. Use the audit log to review migration activity at the campaign and artifact levels, including preprocessing, campaign discovery, transformation, campaign linking, and final migration status.
3. For detailed troubleshooting information, review the application log generated in the same `logs` folder: `migration-<timestamp>-<log-tag>.log`.

Review the Campaign State after Migration

After migration, open the campaign in Siebel Marketing and confirm the campaign now references the migrated Analysis-based artifact.

1. In the Analyses/Lists view, the campaign should show the migrated Analysis or Analysis Collection.
2. In the Allocation view, confirm that campaign allocation now points to the migrated Analysis or Analysis Collection.
3. After migration, the Segments/Lists view in the L4 menu should no longer display the previously associated Segment or List artifact.

Review Migrated Artifact in the OAS/OBIEE Catalog

Finally, review the migrated artifact.

1. Open the OAS/OBIEE Catalog and navigate to the source artifact folder.
2. Confirm that the migrated artifact is created with the `M_` prefix, where `M_` indicates a migrated artifact.

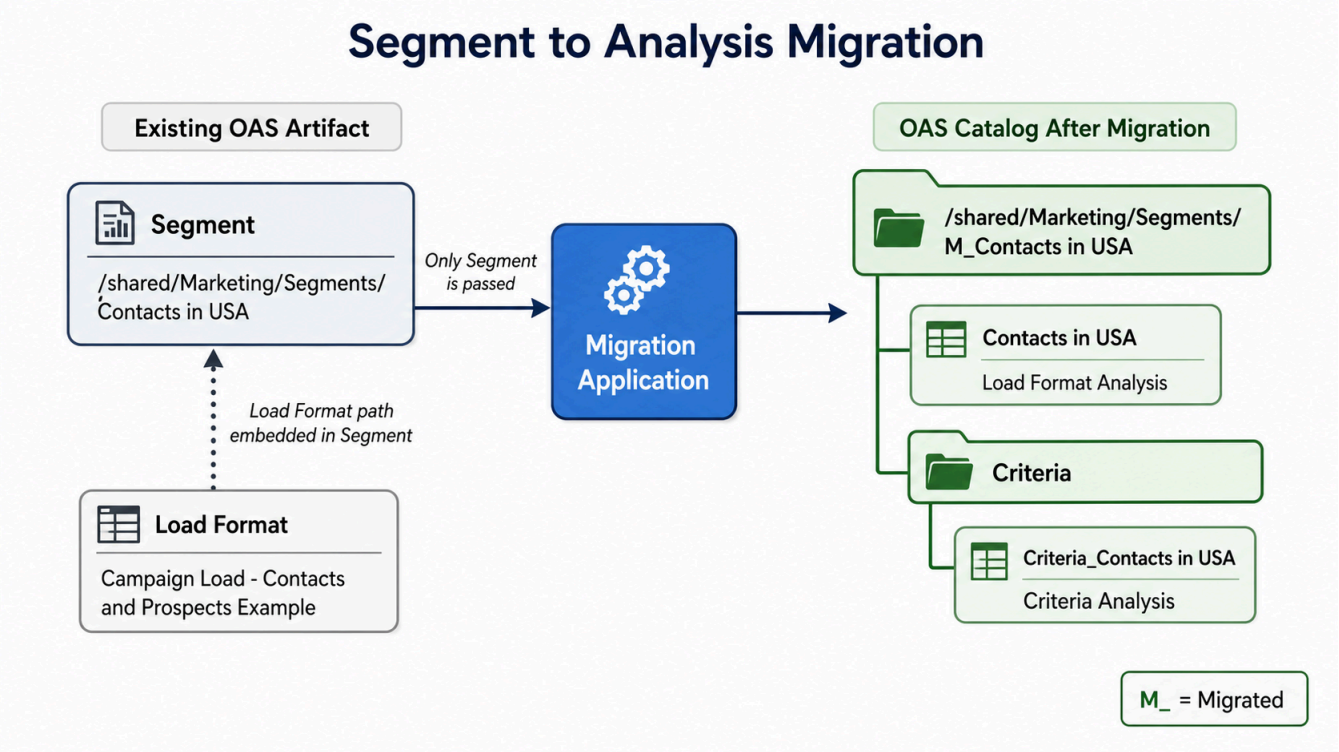
Architecture of the Migration

The Siebel Segmentation Migration Utility converts existing Oracle Analytics Server (OAS) segmentation artifacts into Analysis-based artifacts. This allows migrated Siebel Marketing campaigns to continue using equivalent targeting definitions after the campaign reference is moved from the legacy segmentation artifact to the migrated Analysis or Analysis Collection artifact.

By default, migrated OAS objects are created in the source artifact folder. The generated artifact name starts with `M_`, where `M_` means Migrated. For example, a Segment named `Contacts in USA` is migrated in the same source folder but named `M_Contacts in USA`.

Segment to Analysis Migration

For a Segment migration, the migration utility receives the Segment as the input artifact. The Segment already contains a path reference to its Load Format. Thus, the Load Format isn't passed separately to the migration utility.



During migration, the application reads the Segment definition and the referenced Load Format and then creates the migrated Analysis artifacts in OAS. This table shows source artifacts and migrated artifact naming:

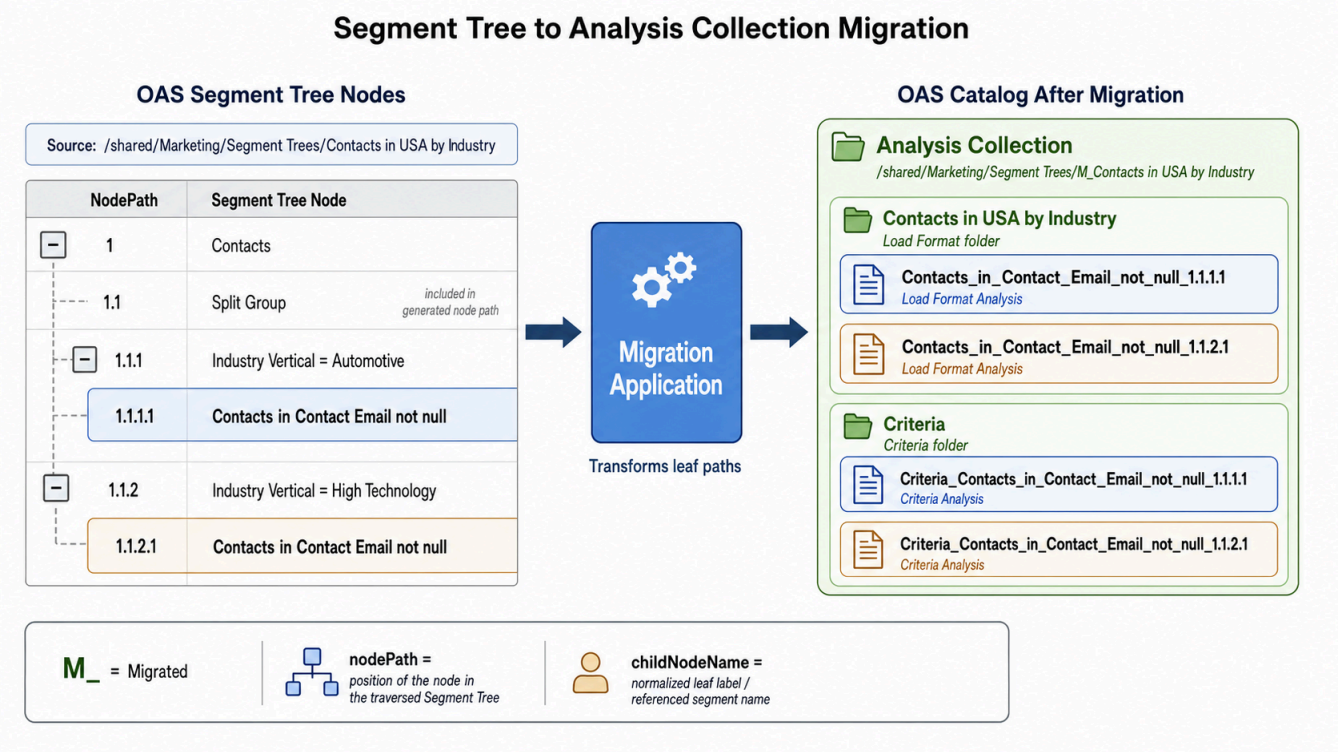
Source Artifact	Migrated OAS Artifact
Segment	Migrated Analysis container named **M_<SegmentName>**
Segment criteria	Criteria Analysis named **Criteria_<SegmentName>**. Provides qualifying-key results
Load Format referenced by the Segment	Load Format Analysis named **<SegmentName>** Associated back to the Siebel Campaign

The Load Format Analysis references the Criteria Analysis through its filter definition. The filter uses the target-level column, such as **Contact Id**, with the operator **is based on results of another analysis**. The saved analysis points to the generated Criteria Analysis, and the filter uses values from the qualifying-key column, such as **ROW_ID**, returned by that Criteria Analysis.

After migration, the Siebel Marketing campaign is associated with the generated Load Format Analysis named **<SegmentName>**. The Criteria Analysis named **Criteria_<SegmentName>** is created under the **Criteria** folder and supplies the qualifying-key result set used by the Load Format Analysis.

Segment Tree to Analysis Collection Migration

For a Segment Tree migration, the Segment Tree is converted into an Analysis Collection. The migration utility traverses the Segment Tree from the root to each leaf node. Each leaf path becomes a generated set of Analysis artifacts in the migrated OAS catalog structure.



The migrated output is grouped under `M_<SegmentTreeName>`. Inside that migrated collection, the original Segment Tree name is used as the Load Format folder, and a separate `Criteria` folder stores the generated Criteria Analysis artifacts.

Source Artifact	Migrated OAS Artifact
Segment Tree	Analysis Collection named `M_<SegmentTreeName>` Associated back to the Siebel Campaign
Leaf path in the Segment Tree	Load Format Analysis named `<childNodeName>_<nodePath>`
Leaf path criteria	Criteria Analysis named `Criteria_<childNodeName>_<nodePath>` Provides qualifying-key results
Original Segment Tree name	Folder that groups generated Load Format Analysis artifacts
`Criteria` folder	Folder that groups generated Criteria Analysis artifacts

For Segment Tree migration, Siebel Marketing is associated with the generated Analysis Collection under `M_<SegmentTreeName>`. Each leaf path contributes a Load Format Analysis and a Criteria Analysis inside that collection structure. The Load Format Analysis for each leaf uses the corresponding Criteria Analysis as its saved-analysis filter source, using the qualifying-key column, such as `ROW_ID`.

The `nodePath` value identifies the position of a node in the traversed Segment Tree. This makes it easier to trace a generated Analysis artifact back to the source leaf node. The `childNodeName` value is derived from the normalized leaf label or referenced Segment name.

Naming and Mapping Notes

Name	Description
`M_`	Migrated artifact prefix
`nodePath`	Position of the node in the traversed Segment Tree
`childNodeName`	Normalized leaf label or referenced Segment name

These names are used so that support teams can map migrated OAS catalog objects back to the original Segment or Segment Tree definition during validation or troubleshooting.

Limitations of the Migration

Be aware that Selection Rules in OBIEE/OAS Marketing Segments and Segment Trees aren't migrated by the Siebel Segmentation Migration Utility.

Oracle Marketing Segmentation uses Selection Rules to control related qualified items included in campaign load and list export processing, including inclusion or exclusion criteria, ranking rules, and record count selectors.

OAS Analysis doesn't provide an equivalent Selection Rules feature. OAS Analysis supports filters, selection steps, groups, and calculated items for limiting or shaping analysis results, but these features don't provide the same qualified-item selection, ranking, and per-target-member record count behavior used by Marketing Selection Rules.

If a source Segment or Segment Tree uses Selection Rules, review and redesign that targeting logic manually after migration.

Incremental Migration for Large Campaign Sets

For large campaign sets, run the Migration Application in smaller, non-overlapping batches by changing `siebel.campaign.searchspec` for each run. This reduces the size of each run and makes validation and rerun handling easier.

Batch Option	Example	When to Use
Name prefix	`Name LIKE 'Customer Demo*'`	Demo or planned migration waves that use a shared campaign naming prefix.
Name sub-prefix	`Name LIKE 'Customer Demo - A*'`	Split a large named set into smaller alphabetical batches.
Created date window	`Created >= '05/01/2026' AND Created <= '05/31/2026'`	Partition campaigns by creation period.
Created-by owner	`Created By Name = 'SADMIN'`	Migrate campaigns owned or created by a specific user.

Batch Option	Example	When to Use
Explicit small subset	`(Name = 'Customer Demo - Spring Loyalty Outreach' OR Name = 'Customer Demo - Winback Engagement')`	Retry or validate a small known group.
Combined scope	`Created By Name = 'SADMIN' AND Name LIKE 'Customer Demo*'`	Narrow a large prefix or owner set.
Status-based scope	`Status = 'Planned'`, `Status = 'Active'`, or `Status = 'Completed'`	Use only if those campaign status values are present in the target environment.

Keep explicit OR lists short. For large campaign sets, use campaign name prefixes, creation date ranges, campaign owners, or verified status values to partition the migration into smaller batches. Because each migration run is stateless, each subsequent run evaluates the current Siebel and OAS state for the campaigns returned by the configured search specification.

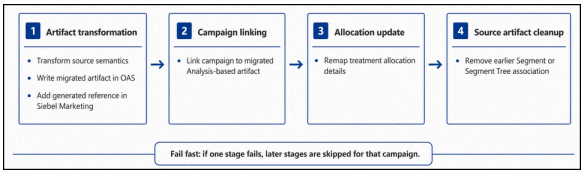
Troubleshooting the Migration Results

Review the command-line summary first. If any campaign fails, review the audit log and application log in the configured logs directory.

Campaign Migration Stages

Campaign migration consists of the following stages:

1. **Artifact transformation:** Transforms the source artifact semantics, creates the migrated artifact in OAS, and adds the generated reference in Siebel Marketing.
2. **Campaign linking:** Updates the Siebel Marketing campaign to reference the migrated Analysis-based artifact.
3. **Allocation update:** Re-maps treatment allocation details to the migrated artifact.
4. **Source artifact cleanup:** Removes the earlier Segment or Segment Tree association from the campaign after the migrated artifact is linked successfully.



List Export and Analysis Export

List Export to Analysis Export migration is exempted from adding the generated artifact into the Siebel Marketing Segment screen. Analysis Export artifacts are referenced directly within the campaign.

The Migration Application follows a fail-fast sequence for each campaign. If any stage fails, later stages aren't executed for that campaign and the campaign migration is marked as failed. Use the audit log to identify which campaign and stage failed, and use the application log for detailed exception information.

Headless and Stateless Run Behavior

The Migration Application runs as a headless CLI process and does not persist run state between executions. Each run discovers campaign and artifact state from the configured Siebel and OAS endpoints. The application uses in-memory

state only within the current run; audit and application logs are for review and are not used as checkpoint data for later runs. If a rerun must target only specific campaigns, use `siebel.campaign.searchspec` to scope the run.

Common Issues and Corrective Actions

Thes table lists common migration issues, their typical symptoms, and the recommended corrective actions:

Run Phase/Area	Issue	Typical Signal	Where to Verify	Corrective Action
Startup - Authentication	Invalid password	Siebel REST API or OAS authentication fails.	Command-line summary and application log.	Rerun the Migration Application and enter the correct runtime password. Verify the Siebel and OAS users have the required access.
Startup - Configuration	Invalid RPD XML path	The configured RPD XML path does not exist or cannot be read.	Application log and `application.properties`	Correct `rpd.xml.path` and confirm the file is accessible from the migration host.
Startup - Configuration	Insufficient write access or disk space	Log files are not created, RPD XML cannot be read, or OAS artifact write fails.	Migration host file system, logs directory, and OAS catalog location.	Use a writable local directory for the RPD XML and logs. Confirm the OAS catalog target location allows artifact creation.
Preflight - Siebel REST	Dynamic IO access not enabled	GET request fails with status 500 and SBL-EAI-50297. The response says the Business Object is not enabled for REST access.	Application log and Siebel Inbound REST API Access view.	Enable Dynamic IO REST access and grant access for Marketing Segment and Mktg List Format. *Enable Dynamic IO Access*
Preflight - Connectivity	Siebel or OAS server not reachable	REST or SOAP preflight fails with host resolution, connection, timeout, or routing errors.	Command-line summary, application log, VPN/ network status, DNS, host, and port.	Verify `siebel.api.url`, `oas.api.url`, VPN or network access, DNS resolution, firewall rules, host and port reachability, and service availability.
Preflight - SSL	SSL or truststore misconfiguration	PKIX path building failed. SunCertPathBuilderExceptio says unable to find valid certification path to requested target.	Application log and truststore configuration.	Import the missing Siebel or OAS certificate chain into the configured truststore. Verify `TRUSTSTORE_PATH`, `TRUSTSTORE_PASSWORD`, and `TRUSTSTORE_TYPE`.
Artifact transformation	Missing qualifying-key metadata	Target level not found, or no qualifying keys matched.	Application log and generated RPD XML.	Regenerate the RPD XML from the active OAS repository and confirm the target level and qualifying-key columns exist.
Artifact transformation	Unsupported or invalid source artifact	Unsupported criteria in Segment, unsupported List Export criteria, or failed artifact transformation.	Audit log for artifact status and application log for detailed exception.	Review the source Segment, Segment Tree, or List Export definition. Correct unsupported criteria before rerunning.

Run Phase/Area	Issue	Typical Signal	Where to Verify	Corrective Action
Artifact transformation	Campaign has no supported artifacts	Campaign has no artifacts to transform.	Audit log and Siebel campaign artifact association.	Review the campaign in Siebel Marketing and confirm a supported Segment, Segment Tree, or List Export artifact is associated before migration.
Artifact transformation - OAS write	Catalog path too long	Campaign linking or Siebel update fails for a generated OAS catalog path.	Application log, generated artifact path, and source folder or artifact names.	Shorten source folder or artifact names before rerunning. Siebel might not accommodate catalog paths beyond about 250 characters.
Artifact transformation - OAS write	Migrated artifact creation fails	Audit log shows artifact transformation failed.	Audit log for campaign and artifact status; application log for the OAS write exception.	Correct the artifact, metadata, OAS catalog path, or OAS access issue and rerun.
Campaign linking	Campaign update fails	Failed updating campaign with migrated artifact reference.	Audit log stage status and application log.	Verify Siebel campaign state, campaign permissions, Dynamic IO access, and the generated artifact reference, then rerun the migration.
Allocation update	Treatment allocation update fails	Treatment allocation update failed.	Audit log stage status and application log.	Review the campaign allocation records in Siebel Marketing, confirm the source allocations still exist, and rerun after correcting allocation data.
Source artifact cleanup	Source artifact deletion fails	Failed deleting existing source artifact from campaign.	Audit log stage status, application log, and campaign artifact association in Siebel Marketing.	Verify the campaign still contains the source Segment or Segment Tree association and that the Siebel user has permission to delete it from the campaign.
Rerun - Recovery	Interrupted migration session	The run stops before completing all campaigns.	Audit log for last completed campaign and application log for final exception.	Correct the interruption cause. Rerun with an appropriate `siebel.campaign.searchspec` if only a subset needs to be retried.

Log Files

The migration utililty writes two log files for each run:

- Application log: `migration-<timestamp>-<log-tag>.log`
- Audit log: `migration-audit-<timestamp>-<log-tag>.log`

Use the audit log for campaign-level migration status and the application log for detailed exception information.

8 Siebel CRM Integration with Oracle Unity

Siebel CRM Integration with Oracle Unity

This chapter describes the Siebel CRM integration with Oracle Unity Customer Data Platform, which is also referred to here as Oracle Unity. This integration is available as of Siebel CRM 21.10 Update. It includes the following topics:

- *Overview of Integration*
- *Data Loading Process*
- *Initial Setup and Configuration*
- *Driver Parameters for the Siebel Unity Data Export Engine*
- *Defining Search Categories and Adding Categories to the Engine*
- *About the CSV File Format*
- *Troubleshooting the Siebel CRM Integration with Oracle Unity*

Overview of Integration

Oracle Unity is a cloud-based offering that combines customer data from online, offline, and third-party sources to create a single, dynamic, real-time view of each customer. The integration between Siebel CRM and Oracle Unity supports the transfer of Siebel CRM data to Oracle Unity, including both the initial bulk loading and subsequent incremental loading.

This integration can help you reduce the effort of integrating the two applications, for bulk and incremental data synchronization. A new screen, Administration - Data Export, provides views that support administrator activities for this integration. You can also leverage features of this integration for other data extraction use cases, for both bulk and incremental loading.

The Siebel CRM integration with Oracle Unity functions as follows:

- Using the Search Data Exporter and Search Data Processor components to identify the objects to export, data is exported from Siebel CRM (in initial bulk loads or in subsequent incremental loads) into a CSV file.
- The CSV file is pushed to Oracle Object Storage (OOS) on Oracle Cloud Infrastructure (OCI).
- Oracle Unity reads this CSV file to import Siebel CRM data into the applicable schema, according to your configured mapping of tables and columns or fields.

Data Loading Process

The Siebel CRM integration with Oracle Unity supports data loading as follows:

- Bulk loading
- Incremental loading

Bulk Loading

The following summarizes the bulk loading process for a configured deployment:

1. In the Data Export Settings view, the administrator clicks the Export or Export All button to send the request to the Search Index Manager Service.

   Where multiple administrators might be working with the data in this view, the administrator can also click Refresh to refresh the displayed data prior to exporting.
2. The result set from the business component query is split into multiple batches, based on the configuration.
3. Jobs are submitted to the Search Data Exporter component.
4. Data is sent to the CSV Export Adapter Service to write into a CSV file.
5. The OOS File Upload Service is invoked to upload the CSV file into OCI Object Storage.

Incremental Loading

The following summarizes the incremental loading process, where the initial bulk loading has been done:

1. The Transaction Processor component reads the data from the S_DOCK_TXN_LOG table and creates the DX file.
2. A recurring job processes the DX file, fetches the data from the respective business component based on the row ID, and sends it to the configured engine.
3. Data is sent to the CSV Export Adapter Service to write into a CSV file.
4. The OOS File Upload Service is invoked to upload the CSV file into OCI Object Storage.

Additional Notes

The following notes provide more detailed information about how the bulk load and incremental load processes work. Refer to other topics in this chapter for related information.

- In the Data Export Administration view, the Active flag is for incremental data load only. If you set the Active flag to N, the incremental load job creates no CSV file. The Active flag has no relevance to the initial (bulk) data load.
- If you set the Active flag to N for all Data Export engines, including the Search engines, and the incremental load job is running, then the DX file is created continuously and the incremental load job also runs on the scheduled interval. The incremental load job processes the DX file, but because there is no active engine to send the data, it then deletes the DX file.
- When multiple engines are configured, if one of the engines fails to send the data successfully, then it does not delete the DX file. It continues to send the data to all of the engines until it sends to all of the engines successfully.
- You might choose to increase the JVM memory size of the Tomcat container that executes the JBS.
- If you have included an MVG field in your category, then the export writes only the primary record's value in the CSV file and does not write the values of nonprimary records.
- When the user exports a category and no record is returned, the status is updated to Completed. No records are created in the Export Status applet and no CSV file is created.
- When a filter specification is configured for a category, all of the data that match this filter specification are exported. In this case, if you change the value of a field that is part of the filter specification but that that does not meet the filter specification, then the modified data is not exported. This data becomes out of sync in the third-party system.
- Import the OCI root certificate to the internal Tomcat that runs the OOS File Upload Service JBS.

Initial Setup and Configuration

The initial setup and configuration tasks for the Siebel CRM integration with Oracle Unity are as follows:

1. Install Siebel CRM (Siebel CRM 21.10 Update or later).
   For more information, see *Siebel Installation Guide* .
2. Perform the tasks described for configuring incremental indexing for third-party search engines, as described in *Siebel Search Administration Guide* . These tasks include the following:
   a. Enable the Search Processing (alias Search) and Disconnected Mobile Synchronization (alias MobileSync) component groups. See also the note about the Transaction Processor component later in this topic.
   b. Set the Enable Incremental Indexing system preference to True. If the system preference is not already defined, then add it.
   c. Add a job template, add a job, and submit the job.
      Use the settings described in *Siebel Search Administration Guide* .
3. Set the Enable Transaction Logging system preference to True, as described in *Siebel Remote and Replication Manager Administration Guide* . This setting is required to support incremental data loading.
4. Set up the driver parameters for the Siebel - Unity Data Export engine, as follows:
   a. Navigate to the Administration - Data Export screen, then the Data Export Administration view.
   b. In the Export Engine list, select the Siebel Unity - Data Export engine.
   c. In the Driver Parameters list, confirm the default value for each parameter or modify the value, as appropriate for your deployment.
      The driver parameters are listed in *Driver Parameters for the Siebel Unity Data Export Engine*.

CAUTION: When the Enable Incremental Indexing system preference is set to True, the Transaction Processor component (alias TxnProc) runs automatically. In this case, for Siebel Remote deployments, you must stop TxnProc before you run the Database Extract component (alias DbXtract) for the first time. After DbXtract has completed, then you can restart TxnProc. If you do not follow these steps, then some transactions might not be routed to remote clients. For more information about running DbXtract, see *Siebel Remote and Replication Manager Administration Guide* .

Driver Parameters for the Siebel - Unity Data Export Engine

The following table provides the definitions and default values for several driver parameters for the Siebel Unity Data Export engine.

Parameter Name	Default Value	Required	Purpose or Definition
Batch Split Size	1000	Y	The number of records representing the batch size threshold for each batch during

Parameter Name	Default Value	Required	Purpose or Definition
			initial data export. If the batch size exceeds this number of records, then this batch is split into multiple batches, with a separate job for each batch.
Batch Submit Size	100	Y	The value must be lower than the value of Batch Split Size. Each job fetches this many records and invokes the adapter service to write the data into a CSV file. A new job repeats this process until all records in all batches have been processed.
Charset	UTF-8	Y	The character set of the data. Supported values are UTF-8 or UTF-16.
Delete File After Upload	Y	N	Deletes the CSV file after import if the value is Y or the parameter does not exist. Otherwise, the file is not deleted.
ExportOnly	N	Y	If the value is N, then CSV files are uploaded in OOS. Otherwise, the CSV files are generated in the path specified in the filepath parameter.
bucketname	Not applicable	N	The name of the OOS bucket where the CSV file is to be uploaded. This parameter is required only where ExportOnly is set to N.
directory	Not applicable	N	The name of the directory under the OOS bucket. If this parameter is left empty, the file is uploaded into the OOS bucket at the top level.
filepath	Not applicable	Y	The file path where the CSV files are created. This path must be accessible to the Siebel Server where the Search component group is enabled. Also, it must be accessible to the Configuration Agent that runs the JBS.
namespace	Not applicable	N	The name space of the OOS.

Note: For security hardening, the following parameters are deprecated in the Data Export Administration:

- `fingerprint`
- `key_file`
- `region`
- `tenancy`
- `UserId`

This improves the security by moving sensitive authentication data (especially private key metadata) out of UI-maintained driver parameters and into a server-side configuration file.

For more details, see *OCI Authentication Parameters*.

OCI Authentication Parameters

For security reasons, OCI authentication parameters are no longer configured in the Data Export Administration under the Driver Parameters applet.

- `fingerprint`
- `key_file`
- `region`
- `tenancy`
- `UserId`

These values are now sourced from the file:`<Siebel_Build>/ses/applicationcontainer_internal/webapps/ociconfig.properties` under the `[AUTH]` section.

Property key	Description	Notes
`user`	OCI user OCID (replaces `userId`)	Required
`fingerprint`	OCI API key fingerprint	Required
`tenancy`	OCI tenancy OCID	Required
`region`	OCI region identifier	Required
`key_file`	Absolute path to OCI private key file (`.pem`)	Required; sensitive
`compartmentid`	OCI compartment OCID	Optional; may be left blank

Sample:

```
[AUTH]
user=<OCI_USER_OCID>
fingerprint=<OCI_FINGERPRINT>
tenancy=<OCI_TENANCY_OCID>
```

```
region=<OCI_REGION>
key_file=<ABSOLUTE_PATH_TO_PEM>
compartmentid=
```

Defining Search Categories and Adding Categories to the Engine

After you have performed initial setup and configuration tasks, perform the following tasks to define search categories and to add categories to the Siebel - Unity Data Export engine.

1. Create a search category and add the fields to this category. To do so:
   a. Navigate to the Administration - Data Export screen, then the Data Export Category Definition view.
   b. Create records for the data categories that you want to export and specify the BC Name (business component name) that they map to.
2. Define filter specifications for the category.

   You define filter specifications for a category in order to restrict the data to be extracted in bulk and incremental loads. When the data is extracted, this filter specification is added while querying the data from the business component. For more information about the operators you can use in filter specifications, see *Siebel Developer's Reference* . Filter specifications are not applied for delete operations in incremental loads.
3. Define Category Fields in the grandchild applet.

   These are the fields that you want to export for this category.
4. Use the Data Export Settings view to add the categories to the engine.

   If any of the categories fails, select and resubmit it by clicking the Resubmit button.

About the CSV File Format

Note the following characteristics of the CSV files that are created for this integration:

- The name of each CSV file is as follows:
  - For bulk load, the CSV file name is the category name followed by the batch ID.
  - For incremental load, the CSV file name is the Category Name followed by INCREMENTAL and a timestamp (in the format YYYYMMDDHHMISS, including the year, month, day, hour, minute, and second).
- The first row in the CSV file contains the field names. All the data records are written to the file starting from the second row onwards.
- The fields in the CSV file are the same as the fields added in the Category Fields applet in the Data Export Category Definition view, along with system fields, visibility fields, and the isDeleted field (which denotes Delete operations). The system fields and visibility fields, which are identified later in this list, do not need to be added explicitly.
- If the record is deleted from the Siebel application, then isDeleted has the value Y. Otherwise, it is set to N. The deleted record has data only for the fields Row Id and isDeleted (set to Y). All other fields are blank.

- If any of the field data in the CSV file contains a carriage return, line feed, or double-quote character, then the data is enclosed with double-quotes, as per the RFC 4180 standard.
- The system fields are as follows: RowID, Created, Created By, Updated, and Updated By.
- The visibility fields are as follows: PersonalId, PositionId, OrganizationId, Group_Hier_Search, Group_Hier_Org_Member_Search, Group_Private_Field, Catalog_Hier_Search, Catalog_Hier_Org_Member_Search, and Catalog_Private_Search.

Troubleshooting the Siebel CRM Integration with Oracle Unity

The following table provides troubleshooting information for various error conditions you might encounter in your Siebel CRM integration with Oracle Unity:

Troubleshooting the Siebel CRM Integration with Oracle Unity

Error	Symptom	Explanation	Solution
Incremental CSV file is not generated when data is updated.	The end user creates a new record or modifies an existing record. However, the incremental CSV file is not generated.	For incremental loading to work, the Transaction Processor (TxnProc) component is required, and also a recurring Search Incremental Indexer job.	Try the following: • Make sure that the TxnProc component is running. • Make sure that the Search Incremental Indexer job is created and in Active status. • Make sure an Export Engine is configured and its status is Active. • The category for this business component that is associated to the Export Engine must have the status Completed.
Insufficient inputs to perform this operation (SBL-SRH-60007).	When trying to Export or Export All from the Export Engine Settings view, the administrator gets this error.	One or more driver parameters are configured incorrectly.	Try the following: • Refer to the log file of the Application Object Manager. The log file shows the parameter that is configured incorrectly. • Provide the correct value for this parameter and proceed with Export or Export All.
GC overhead limit exceeded in the OOS File Upload Service JBS log.	The CSV file is created in the local File System and is not uploaded to Oracle Object Storage.	When the JVM runs out of memory, this error is encountered.	Try the following: • Verify the RAM size in the system where the OOS File Upload JBS is running. • Verify the max JVM size specified on the Tomcat

Error	Symptom	Explanation	Solution
			where the OOS File Upload JBS is deployed. • If your max JVM size is less, you can increase it, based on the available RAM size. Restart the Tomcat where the OOS File Upload JBS is deployed.
Unable to upload the CSV file to Object Storage.	Certificate error is seen while uploading the CSV file to Object Storage.	The Tomcat that runs the OOS File Upload Service does not have the Root Certificate of the OCI cloud where you are trying to upload.	Try the following: • Download the Root Certificate of the OCI cloud where you are uploading the file. • Import the certificate into the trust store of the Tomcat where the OOS File Upload Service JBS is running. Restart the Tomcat.
Unable to open or find the private key file.	Private key not found error is seen while uploading the CSV file to Object Storage.	The Tomcat is not able to find the private key file that is specified in the driver parameter key_file.	Try the following: • Make sure that the private key file is present in the path specified in the driver parameter key_file. • Make sure that the private key file is accessible to the Tomcat where the OOS File Upload Service JBS is running.

9 Advanced Marketing Information for Administrators

Advanced Marketing Information for Administrators

This appendix contains advanced information for administrators. It includes the following topics:

- *Field Names for Marketing Integration Components*
- *Extending Column Data to Promote Prospects to Contacts*

Field Names for Marketing Integration Components

The followning tbale contains a list of Marketing integration objects, their components, and field names.

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
Business Intelligence Account	Account	Attribute 66	DTYPE_TEXT	100
		Attribute 67	DTYPE_TEXT	100
		Attribute 68	DTYPE_TEXT	100
		Attribute 69	DTYPE_TEXT	100
		Attribute 70	DTYPE_TEXT	100
		Attribute 71	DTYPE_TEXT	100
		Attribute 72	DTYPE_TEXT	100
		Attribute 73	DTYPE_NUMBER	Not applicable
		Attribute 74	DTYPE_NUMBER	Not applicable
		Attribute 75	DTYPE_NUMBER	Not applicable
		Attribute 76	DTYPE_NUMBER	Not applicable

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Attribute 77	DTYPE_NUMBER	Not applicable
		Attribute 78	DTYPE_NUMBER	Not applicable
		Attribute 79	DTYPE_NUMBER	Not applicable
		Attribute 80	DTYPE_NUMBER	Not applicable
		Attribute 81	DTYPE_NUMBER	Not applicable
		Id	DTYPE_ID	30
		Integration Id	DTYPE_TEXT	30
		Location	DTYPE_TEXT	50
		Name	DTYPE_TEXT	100
Business Intelligence Contact	Contact	Attribute 49	DTYPE_TEXT	100
		Attribute 50	DTYPE_TEXT	100
		Attribute 51	DTYPE_TEXT	100
		Attribute 52	DTYPE_TEXT	100
		Attribute 53	DTYPE_TEXT	100
		Attribute 54	DTYPE_TEXT	100
		Attribute 55	DTYPE_TEXT	100
		Attribute 56	DTYPE_NUMBER	Not applicable
		Attribute 57	DTYPE_NUMBER	Not applicable
		Attribute 58	DTYPE_NUMBER	Not applicable
		Attribute 59	DTYPE_NUMBER	Not applicable

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Attribute 60	DTYPE_NUMBER	Not applicable
		Attribute 61	DTYPE_NUMBER	Not applicable
		Attribute 62	DTYPE_NUMBER	Not applicable
		Attribute 63	DTYPE_NUMBER	Not applicable
		Attribute 64	DTYPE_NUMBER	Not applicable
		First Name	DTYPE_TEXT	50
		Id	DTYPE_ID	30
		Integration Id	DTYPE_TEXT	30
		Last Name	DTYPE_TEXT	50
		Person Uid	DTYPE_TEXT	100
Business Intelligence Household	Household	Attribute 48	DTYPE_TEXT	100
		Attribute 49	DTYPE_TEXT	100
		Attribute 50	DTYPE_TEXT	100
		Attribute 51	DTYPE_TEXT	100
		Attribute 52	DTYPE_TEXT	100
		Attribute 53	DTYPE_TEXT	100
		Attribute 54	DTYPE_TEXT	100
		Attribute 55	DTYPE_NUMBER	Not applicable
		Attribute 56	DTYPE_NUMBER	Not applicable
		Attribute 57	DTYPE_NUMBER	Not applicable

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Attribute 58	DTYPE_NUMBER	Not applicable
		Attribute 59	DTYPE_NUMBER	Not applicable
		Attribute 60	DTYPE_NUMBER	Not applicable
		Attribute 61	DTYPE_NUMBER	Not applicable
		Attribute 62	DTYPE_NUMBER	Not applicable
		Attribute 63	DTYPE_NUMBER	Not applicable
		Household Name	DTYPE_TEXT	50
		Household Number	DTYPE_TEXT	100
		Id	DTYPE_ID	30
		Integration Id	DTYPE_TEXT	30
Marketing Contact	Account	Account Location	DTYPE_TEXT	50
		Account Name	DTYPE_TEXT	100
		Home Page	DTYPE_TEXT	100
		Id	DTYPE_TEXT	30
		Integration Id	DTYPE_TEXT	30
		Main Fax Number	DTYPE_TEXT	Not applicable
		Main Phone Number	DTYPE_TEXT	Not applicable
		Region	DTYPE_TEXT	25
Marketing Contact (continued)	Account Address	Address Name	DTYPE_TEXT	100
		City	DTYPE_TEXT	50

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Country	DTYPE_TEXT	50
		Id	DTYPE_TEXT	30
		Integration Id	DTYPE_TEXT	30
		Postal Code	DTYPE_TEXT	30
		State	DTYPE_TEXT	10
		Street Address	DTYPE_TEXT	200
		Street Address 2	DTYPE_TEXT	100
	Account Organization	Organization	DTYPE_TEXT	50
	Campaign Contact	Campaign Id	DTYPE_ID	Not applicable
		Completion Date	DTYPE_TEXT	Not applicable
		Distribution Id	DTYPE_ID	Not applicable
		Key 1	DTYPE_TEXT	30
		Key 2	DTYPE_TEXT	30
		Key 3	DTYPE_TEXT	30
		Key 4	DTYPE_TEXT	30
		Key 5	DTYPE_TEXT	30
		Key 6	DTYPE_TEXT	30
		Key 7	DTYPE_TEXT	30
		Load Number	DTYPE_NUMBER	Not applicable
		Load Wave Id	DTYPE_ID	Not applicable

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Scalability Batch Number	DTYPE_NUMBER	Not applicable
		Segment Id	DTYPE_ID	Not applicable
		Source Code	DTYPE_TEXT	75
		Token Number	DTYPE_NUMBER	Not applicable
		Treatment Id	DTYPE_ID	Not applicable
Marketing Contact (continued)	Contact	Cellular Phone #	DTYPE_TEXT	Not applicable
		Email Address	DTYPE_TEXT	50
		Fax Phone #	DTYPE_TEXT	Not applicable
		First Name	DTYPE_TEXT	50
		Gender	DTYPE_TEXT	30
		Home Phone #	DTYPE_TEXT	Not applicable
		Id	DTYPE_ID	30
		Integration Id	DTYPE_TEXT	30
		Job Title	DTYPE_TEXT	75
		Last Name	DTYPE_TEXT	50
		Middle Name	DTYPE_TEXT	50
		Person Uld	DTYPE_TEXT	100
		Preferred Communications	DTYPE_TEXT	30
		Salutation	DTYPE_TEXT	15
		Status	DTYPE_TEXT	30

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Work Phone #	DTYPE_TEXT	Not applicable
	Contact Address	Id	DTYPE_TEXT	30
		Integration Id	DTYPE_TEXT	30
		Personal Address Name	DTYPE_TEXT	100
		Personal City	DTYPE_TEXT	50
		Personal Country	DTYPE_TEXT	50
		Personal Postal Code	DTYPE_TEXT	30
		Personal State	DTYPE_TEXT	10
		Personal Street Address	DTYPE_TEXT	200
		Personal Street Address 2	DTYPE_TEXT	100
	Contact Organization	Organization	DTYPE_TEXT	50
Marketing Contact (continued)	Household	Fax Number	DTYPE_TEXT	Not applicable
		Household Name	DTYPE_TEXT	50
		Household Number	DTYPE_TEXT	100
		Household Size	DTYPE_NUMBER	Not applicable
		Household Wealth	DTYPE_TEXT	Not applicable
		Id	DTYPE_ID	30
		Income	DTYPE_TEXT	Not applicable
		Integration Id	DTYPE_TEXT	30
		Phone Number	DTYPE_TEXT	Not applicable

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Revenue	DTYPE_TEXT	Not applicable
	Household Organization	Organization	DTYPE_TEXT	50
Marketing Person	Campaign Contact	Account Id	DTYPE_ID	Not applicable
		Campaign Id	DTYPE_ID	Not applicable
		Completion Date	DTYPE_TEXT	Not applicable
		Contact Id	DTYPE_ID	Not applicable
		Distribution Id	DTYPE_ID	Not applicable
		Household Id	DTYPE_ID	Not applicable
		Key 1	DTYPE_TEXT	30
		Key 2	DTYPE_TEXT	30
		Key 3	DTYPE_TEXT	30
		Key 4	DTYPE_TEXT	30
		Key 5	DTYPE_TEXT	30
		Key 6	DTYPE_TEXT	30
		Key 7	DTYPE_TEXT	30
		Load Number	DTYPE_NUMBER	Not applicable
		Load Wave Id	DTYPE_ID	Not applicable
		Prospect Id	DTYPE_ID	Not applicable
		Scalability Batch Number	DTYPE_NUMBER	Not applicable
		Segment Id	DTYPE_ID	Not applicable

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Source Code	DTYPE_TEXT	75
		Treatment Id	DTYPE_ID	Not applicable
		Token Number	DTYPE_NUMBER	Not applicable
Marketing Prospect	Campaign Contact	Call Completed	DTYPE_TEXT	Not applicable
		Campaign Id	DTYPE_ID	Not applicable
		Completion Date	DTYPE_TEXT	Not applicable
		Distribution Id	DTYPE_ID	Not applicable
		Key 1	DTYPE_TEXT	30
		Key 2	DTYPE_TEXT	30
		Key 3	DTYPE_TEXT	30
		Key 4	DTYPE_TEXT	30
		Key 5	DTYPE_TEXT	30
		Key 6	DTYPE_TEXT	30
		Key 7	DTYPE_TEXT	30
		Load Number	DTYPE_NUMBER	Not applicable
		Load Wave Id	DTYPE_ID	Not applicable
		Prospect Id	DTYPE_ID	Not applicable
		Scalability Batch Number	DTYPE_NUMBER	Not applicable
		Segment Id	DTYPE_ID	Not applicable
		Treatment Id	DTYPE_ID	Not applicable

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Token Number	DTYPE_NUMBER	Not applicable
	Prospect	Account	DTYPE_TEXT	Not applicable
		Account Id	DTYPE_ID	Not applicable
		Alias	DTYPE_TEXT	Not applicable
		Alternate Phone #	DTYPE_TEXT	Not applicable
		Annual Revenue	DTYPE_NUMBER	Not applicable
		Assistant	DTYPE_TEXT	Not applicable
		Assistant Phone #	DTYPE_TEXT	Not applicable
		Birth Date	DTYPE_DATETIME	Not applicable
		Cellular Phone #	DTYPE_TEXT	Not applicable
		City	DTYPE_TEXT	Not applicable
		Comment	DTYPE_TEXT	Not applicable
		Country	DTYPE_TEXT	Not applicable
Marketing Prospect (continued)	Prospect (continued)	County	DTYPE_TEXT	Not applicable
		Disable DataCleansing	DTYPE_TEXT	Not applicable
		DUNS Number	DTYPE_ID	Not applicable
		Email Address	DTYPE_TEXT	Not applicable
		Employee At Site	DTYPE_NUMBER	Not applicable
		Employee Total	DTYPE_NUMBER	Not applicable
		Expiration Date	DTYPE_TEXT	Not applicable

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
		Fax Phone #	DTYPE_TEXT	Not applicable
		First Name	DTYPE_TEXT	Not applicable
		Gender	DTYPE_TEXT	30
		Hide DUNS Number Flag	DTYPE_TEXT	Not applicable
		Home Page	DTYPE_TEXT	100
		Home Phone #	DTYPE_TEXT	Not applicable
		Id	DTYPE_ID	30
		Job Title	DTYPE_TEXT	Not applicable
		Last Name	DTYPE_TEXT	Not applicable
		Line of Business	DTYPE_TEXT	50
		Maiden Name	DTYPE_TEXT	Not applicable
		Manager Name	DTYPE_TEXT	Not applicable
		Marital Status Code	DTYPE_TEXT	Not applicable
		Middle Name	DTYPE_TEXT	Not applicable
		Nationality	DTYPE_TEXT	Not applicable
		Postal Code	DTYPE_TEXT	Not applicable
		Preferred Communications	DTYPE_TEXT	30
		Preferred Language Name	DTYPE_TEXT	Not applicable
		Primary Account Location	DTYPE_TEXT	Not applicable
		Primary SIC Code	DTYPE_TEXT	30

Parent Integration Object	Parent Integration Component	Name	Data Type	Length
Marketing Prospect (continued)	Prospect (continued)	Primary SIC Id	DTYPE_ID	Not applicable
		Product Interest	DTYPE_TEXT	100
		Prospective Contact UId	DTYPE_TEXT	100
		Province	DTYPE_TEXT	Not applicable
		Public	DTYPE_TEXT	1
		Race	DTYPE_TEXT	Not applicable
		Salutation	DTYPE_TEXT	Not applicable
		Social Security Number	DTYPE_TEXT	Not applicable
		Source Name	DTYPE_TEXT	100
		State	DTYPE_TEXT	Not applicable
		Street Address	DTYPE_TEXT	Not applicable
		Street Address 2	DTYPE_TEXT	Not applicable
		Suppress Call Flag	DTYPE_TEXT	Not applicable
		Suppress Email Flag	DTYPE_TEXT	Not applicable
		Suppress Fax Flag	DTYPE_TEXT	Not applicable
		Suppress Mail Flag	DTYPE_TEXT	Not applicable
		Time Zone	DTYPE_TEXT	Not applicable
		Work Phone #	DTYPE_TEXT	Not applicable
		Year Started	DTYPE_NUMBER	Not applicable

Extending Column Data to Promote Prospects to Contacts

When promoting prospects to contacts, use this example as a guide for promoting data stored in extension columns in the S_PRSP_CONTACT table to the S_CONTACT table.

To promote data stored in extension columns in the S_PRSP_CONTACT table to the S_CONTACT table

1. Add a new extension column called X_ACADEMIC_TITLE to S_PRSP_CONTACT.
2. Add a new extension column called X_ACADEMIC_TITLE to S_CONTACT.
3. Add a field called Academic Title to the List Management Prospective Contact business component.
4. Add user properties to the List Management Prospective Contact business component with the following values:
    - Name: Promotion Map:Contact.Academic Title
    - Value: Academic Title
5. Add a field called Academic Title to the Contact business component.
6. Add a field called Academic Title to the List Management Prospective Contact List applet and Contact List applet.
7. Add a field called Academic Title to the Promote To Contact or Promote To Contact (SIA) integration object.

10 Assigning Character Sets for the Email Marketing Server

Assigning Character Sets for the Email Marketing Server

This appendix describes how to assign character sets for the Email Marketing Server. It includes the following topic:

- *Working with Character Sets for Email Marketing Servers*

Working with Character Sets for Email Marketing Servers

To change the character set used for outbound emails, add a parameter to the Email Marketing Server profile that is used for the outbound email campaign. The parameter you must add or change is Character Set, using a value from the far column of the following table.

When the Communications Server processes an email request for a campaign, it identifies the character set and locale of the first offer, changes to that offer's character set and locale, and processes that offer and associated offers using that character set and locale.

To assign the character set for the Email Marketing Server configuration

1. Navigate to the Administration - Marketing screen and then the Servers view.
2. Query for records of type Email Marketing Server.
3. Select an email server and add a new parameter type with the name Charset.
4. Set the parameter value to the value of the character set with which to send the email offer.

The following table identifies the name of the character set used in an email campaign.

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
CP10004	Arabic	Macintosh Arabic	Microsoft or IBM	CP10004
CP1256	Arabic	Not applicable	Microsoft or IBM	CP1256
CP20420	Arabic	(With full-width Latin and punctuation)	Microsoft or IBM	CP20420
CP28596	Arabic	Arabic Alphabet (ISO)	Microsoft or IBM	CP28596
CP720	Arabic	Transparent ASMO	Microsoft or IBM	CP720

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
CP864	Arabic	Not applicable	Microsoft or IBM	CP864
ISO 8859-6	Arabic	ISOLatinArabic	International or National Standard	Arabic
CP708	Arabic	ASMO708	Microsoft or IBM	CP708
CP1257	Baltic	Not applicable	Microsoft or IBM	CP1257
CP28594	Baltic	Baltic Alphabet (ISO)	Microsoft or IBM	CP28594
CP775	Baltic	Not applicable	Microsoft or IBM	CP775
ISO 8859-4	Baltic	Latin4	International or National Standard	Latin4, ISO-8859-4
ISO 8859-13	Baltic	Latin7	International or National Standard	Latin7, ISO-8859-13
ISO 8859-14	Celtic	Latin8	International or National Standard	ISO-8859-14
CCSID 935	Chinese, Simplified	Not applicable	IBM	CCSID-935, CCSID935
EUC-CN	Chinese, Simplified	GB2312, EUC-SC	UNIX	GB2312
GB2312	Chinese, Simplified	EUC-CN, EUC-SC	International or National Standard	GB2312
HZ-GB-2312	Chinese, Simplified	HZ-GB-2312	International or National Standard	HZ, HZ-GB-2312
CP936	Chinese, Simplified	GBK	Microsoft or IBM	CP936, GBK
MacChinese Simplified	Chinese, Simplified	Not applicable	Macintosh	MacChinese Simplified
CCSID 937	Chinese, Traditional	Not applicable	IBM	CCSID-937, CCSID937

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
CNS-11643-1986	Chinese, Traditional	EUC-TW	International or National Standard	CNS-11643-1986
CNS-11643-1992	Chinese, Traditional	EUC-TW	International or National Standard	CNS-11643, CNS-11643-1992
EUC-TW	Chinese, Traditional	CNS-11643-1986, CNS-11643-1992	UNIX	CNS-11643, CNS-11643-1992
GB12345	Chinese, Traditional	Not applicable	International or National Standard	GB12345
Big5	Chinese, Traditional	Not applicable	International or National Standard	Big5
CP10002	Chinese, Traditional	Macintosh Traditional Chinese	Microsoft or IBM	CP10002
CP950	Chinese, Traditional	Not applicable	Microsoft or IBM	CP950
MacChinese Traditional	Chinese, Traditional	Not applicable	Macintosh	MacChinese Traditional
MacCroatian	Croatian	Not applicable	Macintosh	MacCroatian
CP10007	Cyrillic	Macintosh Cyrillic	Microsoft or IBM	CP10007
CP1251	Cyrillic	MS Windows Cyrillic (Slavic)	Microsoft or IBM	CP1251
CP20866	Cyrillic	Cyrillic Alphabet, KOI8-R	Microsoft or IBM	CP20866
CP20880	Cyrillic	(With full-width Latin and punctuation)	Microsoft or IBM	CP20880
CP21025	Cyrillic	(With full-width Latin and punctuation)	Microsoft or IBM	CP21025
CP21866	Cyrillic	Ukranian KOI8-RU	Microsoft or IBM	CP21866
CP28595	Cyrillic	Cyrillic Alphabet (ISO)	Microsoft or IBM	CP28595
CP855	Cyrillic	IBM Cyrillic	Microsoft or IBM	CP855

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
CP866	Cyrillic	MS DOS Russian	Microsoft or IBM	CP866
ISO 8859-5	Cyrillic	ISOLatinCyrillic	International or National Standard	ISOLatinCyrillic
MacCyrillic	Cyrillic	Not applicable	Macintosh	MacCyrillic
Mac Devanagari	Devanagari	Not applicable	Macintosh	MacDevanagari
CP10006	Greek	Macintosh Greek 1	Microsoft or IBM	CP10006
CP1253	Greek	Not applicable	Microsoft or IBM	CP1253
CP20423	Greek	(With full-width Latin and punctuation)	Microsoft or IBM	CP20423
CP28597	Greek	Greek Alphabet (ISO)	Microsoft or IBM	CP28597
CP737	Greek	Not applicable	Microsoft or IBM	CP737
CP869	Greek	IBM Modern Greek	Microsoft or IBM	CP869
ISO 8859-7	Greek	ISOLatinGreek	International or National Standard	Greek
MacGreek	Greek	Not applicable	Macintosh	MacGreek
MacGujarati	Gujarati	Not applicable	Macintosh	MacGujarati
CP10010	Gurmukhi	Macintosh Gurmukhi	Microsoft or IBM	CP10010
MacGurmukhi	Gurmukhi	Not applicable	Macintosh	MacGurmukhi
CP10005	Hebrew	Macintosh Hebrew	Microsoft or IBM	CP10005
CP1255	Hebrew	Not applicable	Microsoft or IBM	CP1255
CP28598	Hebrew	Hebrew Alphabet (ISO)	Microsoft or IBM	CP28598
CP38598	Hebrew	ASCII and Hebrew and private use characters	Microsoft or IBM	CP38598

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
CP862	Hebrew	Not applicable	Microsoft or IBM	CP862
ISO 8859-8	Hebrew	ISOLatinHebrew	International or National Standard	Hebrew
CP10079	Icelandic	Macintosh Icelandic	Microsoft or IBM	CP10079
CP861	Icelandic	MS DOS Icelandic	Microsoft or IBM	CP861
MacIcelandic	Icelandic	Not applicable	Macintosh	MacIcelandic
CCSID 1027	Japanese	EBCDIK	Microsoft or IBM	CCSID-1027, CCSID1027
CCSID 290	Japanese	EBCDIK	Microsoft or IBM	CCSID-290, CCSID290
CCSID 930	Japanese	Not applicable	IBM	CCSID-930, CCSID930
CCSID 939	Japanese	Not applicable	IBM	CCSID-939, CCSID939
CCSID 942	Japanese	Not applicable	Microsoft or IBM	CCSID-942, CCSID942
CP10001	Japanese	Macintosh Japanese	Microsoft or IBM	CP10001
CP20290	Japanese	(full and half width Latin and halfwidth katakana)	Microsoft or IBM	CP20290
CP21027	Japanese	(half-width Latin, half-width katakana and private use)	Microsoft or IBM	CP21027
EUC-JP	Japanese	Not applicable	UNIX	EUC-JP, EUC-J
ISO-2022-JP	Japanese	Not applicable	International or National Standard	ISO-2022-JP
JIS_X_0201	Japanese	Half-WidthKatakana	International or National Standard	JIS_X_0201
JIS_X_0208	Japanese	Not applicable	International or National Standard	JIS_X_0208
MacJapanese	Japanese	Not applicable	Macintosh	MacJapanese

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
Shift-JISMS	Japanese	MS_Kanji, CP932	Microsoft or IBM	Shift-JIS, SJIS
Shift-JIS78	Japanese	Shift-JIS without MS or IBM extensions	UNIX or Macintosh	Shift-JIS78, SJIS78
CP10003	Korean	Macintosh Korean	Microsoft or IBM	CP10003
CP1361	Korean	Korean Johab (based on KSC 5861-1992)	Microsoft or IBM	CP1361
CP949	Korean	Not applicable	Microsoft or IBM	CP949
EUC-KR	Korean	KS_C_5861-1992	UNIX	EUC-KR, EUC-K
ISO-2022-KR	Korean	KS_C_5601-1987	International or National Standard	ISO-2022-KR
Johab	Korean	Not applicable	International or National Standard	Johab
KS_C_5601-1987	Korean	ISO-2022-KR	International or National Standard	ISO-2022-KR
KS_C_5861-1992	Korean	EUC-KR	International or National Standard	KS_C_5861-1992
MacKorean	Korean	Not applicable	Macintosh	MacKorean
CP10000	Latin	Macintosh Roman	Microsoft or IBM	CP10000
CP10029	Latin	Macintosh Latin2	Microsoft or IBM	CP10029
CP10082	Latin	(With mathematical symbols)	Microsoft or IBM	CP10082
CCSID 1047	Latin	EBCDIC (for IBM Open Systems platform)	Microsoft or IBM	CCSID1047
CP20261	Latin	(With private use characters)	Microsoft or IBM	CP20261
CP20269	Latin	Not applicable	Microsoft or IBM	CP20269
CP20273	Latin	(With full-width Latin and punctuation)	Microsoft or IBM	CP20273

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
CP20277	Latin	(With full-width Latin and punctuation)	Microsoft or IBM	CP20277
CP20278	Latin	(With full-width Latin and punctuation)	Microsoft or IBM	CP20278
CP20280	Latin	(With full-width Latin and punctuation)	Microsoft or IBM	CP20280
CP20284	Latin	(With full-width Latin and punctuation)	Microsoft or IBM	CP20284
CP20285	Latin	(With full-width Latin and punctuation)	Microsoft or IBM	CP20285
CP20297	Latin	(With full-width Latin and punctuation)	Microsoft or IBM	CP20297
CP20833	Latin	(With full-width Latin and punctuation)	Microsoft or IBM	CP20833
CP20871	Latin	(With full-width Latin and punctuation)	Microsoft or IBM	CP20871
CP28591	Latin	ASCII and Latin accented vowels	Microsoft or IBM	CP28591
CP28593	Latin	Latin 3 Alphabet (ISO)	Microsoft or IBM	CP28593
CP850	Latin	MS DOS Multilingual, MS-DOS Latin1	Microsoft or IBM	CP850
CP870	Latin	(With fullwidth punctuation)	Microsoft or IBM	CP870
ISO 8859-1	Latin	Latin1	International or National Standard	Latin1, ISO-8859-1
ISO 8859-15	Latin	Latin1 plus Euro symbol and accented characters	International or National Standard	ISO-8859-15
ISO 8859-2	Latin	Latin2	International or National Standard	Latin2, ISO-8859-2
MacRoman	Latin	Not applicable	Macintosh	MacRoman

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
NextStep	Latin	Not applicable	Apple or Next	NextStep
Adobe-Standard-Encoding	Latin	(used in PS printers)	Other Corporate	Adobe-Standard-Encoding
CP863	Latin, Canadian French	MS DOS Canadian French	Microsoft or IBM	CP863
CP28592	Latin, Central European	Central European Alphabet (ISO)	Microsoft or IBM	CP28592
MacCentral European	Latin, Central European	Not applicable	Macintosh	MacCentral European
CP1250	Latin, Eastern Europe	Not applicable	Microsoft or IBM	CP1250
CP20905	Latin, Esperanto	(With full-width Latin and punctuation)	Microsoft or IBM	CP20905
CP860	Latin, Portuguese	MS DOS Portuguese	Microsoft or IBM	CP860
ISO 8859-3	Latin, Southeast European	Latin3	International or National Standard	Latin3, ISO-8859-3
ASCII	Latin, US English	US-ASCII, CP367	International or National Standard	ASCII
CP037	Latin, US English	EBCDIC	Microsoft or IBM	CP037
CP1026	Latin, US English	EBCDIC	Microsoft or IBM	CP1026
CP1252	Latin, US English	MS Windows Latin1 (ANSI)	Microsoft or IBM	CP1252
CP20105	Latin, US English	US ASCII	Microsoft or IBM	CP20105
CP437	Latin, US English	MS-DOS Latin US	Microsoft or IBM	CP437
CP500	Latin, US English	EBCDIC	Microsoft or IBM	CP500
CP875	Latin, US English	EBCDIC	Microsoft or IBM	CP875
CP10017	Malayalam	Macintosh Malayalam	Microsoft or IBM	CP10017

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
CP865	Nordic	MS DOS Nordic	Microsoft or IBM	CP865
ISO 8859-10	Nordic	Latin6	International or National Standard	Latin6, ISO-8859-10
Mac Romanian	Romanian	Not applicable	Macintosh	MacRomanian
CP852	Slavic	MS DOS Slavic	Microsoft or IBM	CP852
Adobe-Symbol-Encoding	Symbol	(used in PS printers)	Adobe	Adobe-Symbol-Encoding
Adobe-Zapf-Dingbats-Encoding	Symbol	(used in PS printers)	Adobe	Adobe-Zapf-Dingbats-Encoding
CP10008	Symbol	Macintosh RSymbol (Right-left symbol)	Microsoft or IBM	CP10008
MacDingbats	Symbol	Not applicable	Macintosh	MacDingbats
MacSymbol	Symbol	Not applicable	Macintosh	MacSymbol
CP20838	Thai	(With full-width Latin and punctuation)	Microsoft or IBM	CP20838
CP874	Thai	IBMThai	Microsoft or IBM	CP874
ISO 8859-11 (draft)	Thai	ISOLatinThai	International or National Standard	Thai
MacThai	Thai	Not applicable	Macintosh	MacThai
CP10081	Turkish	Macintosh Turkish	Microsoft or IBM	CP10081
CP1254	Turkish	Not applicable	Microsoft or IBM	CP1254
CP28599	Turkish	Turkish (ISO)	Microsoft or IBM	CP28599
CP857	Turkish	IBM Turkish	Microsoft or IBM	CP857
ISO 8859-9	Turkish	Latin5	International or National Standard	Latin5, ISO-8859-9

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
MacTurkish	Turkish	Not applicable	Macintosh	MacTurkish
MacUkrainian	Ukranian	Not applicable	Macintosh	MacUkrainian
BMP	Unicode	Not applicable	Unicode	BMP, Unicode20:big-endian
Java	Unicode	Way of representing Unicode characters in ASCII	Oracle	Java, Unicode20:BOM:Java, Unicode11:Java, Unicode11:BOM:Java
UCS2	Unicode	ISO-10646-UCS2, UTF16	Unicode	UCS2, Unicode, Unicode20:UCS2
Unicode Big-endian	Unicode	Not applicable	Unicode	big-endian, Unicode20:big-endian, Unicode11:big-endian, Unicode11:BOM:big-endian
Unicode Little-endian	Unicode	Not applicable	Unicode	little-endian, Unicode20:little-endian, Unicode11:little-endian, Unicode11:BOM:little-endian
Unicode11-UCS2	Unicode	Not applicable	Unicode	Unicode11-UCS2, Unicode11: UCS2, Unicode11:BOM:UCS2
Unicode11-UTF7	Unicode	Not applicable	Unicode	Unicode11-UTF7, Unicode11: UTF7, Unicode11:BOM:UTF7
Unicode11-UTF8	Unicode	Not applicable	Unicode	Unicode11-UTF8, Unicode11: UTF8, Unicode11:BOM:UTF8
UTF7	Unicode	Not applicable	Unicode	UTF7, Unicode20:BOM:UTF7
UTF8	Unicode	Not applicable	Unicode	UTF8, Unicode20:BOM:UTF8

Encoding	Character Set Name	Also Known As	Vendor or Standard Body	Character Set Value (Unicode)
UTF-EBCDIC	Unicode	Not applicable	Unicode	UTF8-EBCDIC, UTF-8-EBCDIC
CP1258	Vietnamese	Not applicable	Microsoft or IBM	CP1258

11 Logical Entity Relationships

Logical Entity Relationships

This appendix lists the logical entity relationships between marketing objects, business components, and specific columns in the S_SRC table. It includes the following topic:

- *Logical Entity Relationships for Marketing Objects*

Logical Entity Relationships for Marketing Objects

The following table shows the logical entity relationships between marketing objects, business components, and specific columns in the S_SRC table.

Object	Business Component Name	Columns in S_SRC					
		CAMP_TYPE_ CD	PAR_SRC_ID	SUB_TYPE	TEMPLATE _ ID	TMPL_ID	ULT_ PAR_SRC_ ID
Campaign	Campaign	Campaign	Parent Campaign Id	MARKETING_ CAMPAIGN	Campaign Template Id	Stage Id	Program Id
Campaign Template	Campaign Template	Campaign	NULL	MARKETING_ CAMPAIGN	NULL	Stage Id	Program Tmpl Id
Marketing Plans	Marketing Plans	Marketing Plan	Parent Mktg Plan Id	MARKETING_ CAMPAIGN	NULL	NULL	NULL
Program	Program Container	PROGRAM CONTAINER	NULL	MARKETING_ CAMPAIGN	Program Template Id	NULL	Program Id
Program Template	Program Template	PROGRAM CONTAINER	NULL	MARKETING_ CAMPAIGN	NULL	NULL	Program Tmpl Id
Stage	Program (DBM)	STAGE	NULL	MARKETING_ CAMPAIGN	NULL	Program Id	Program Id

12 Email Marketing Configuration Properties

Email Marketing Configuration Properties

This appendix describes the new and changed properties in the email marketing configuration files in Siebel CRM Release 8.1 and later. It includes the following topics:

- *New and Changed Properties in the esd.properties Configuration File*
- *New and Changed Properties in the ctd.properties Configuration File*
- *New and Changed Properties in the bhd.properties Configuration File*

New and Changed Properties in the esd.properties Configuration File

The following information lists the new properties in the esd.properties file.

Property and Seeded Value	Description
esd.moduleName = ESD	Module name.
esd.handlerClass=com.siebel.sem.esd.integrated.OnPremiseMailingEventHandler	Handler class available for custom code.
esd.smtp.throttleVal=-1	Determines the number of emails sent out per second.
esd.priorityThreshold=5001	Determines whether a mailing has enough recipients to have its priority level observed.
esd.mailing.deliveryFlushThreshold=100	Determines the number of recipients that will be recorded from memory and flushed.
esd.callbackQueue.queueLength=100	Determines the maximum number of entries to the queue before the queue is flushed.
esd.smtp.starttls=false	Determines whether Transport Layer Security (TLS) is enabled for communications between the Email Sending Daemon (ESD) and the Simple Mail Transfer Protocol (SMTP) server.

The following table lists the changed properties in the esd.properties file.

Siebel CRM Version 8.0	Siebel CRM Version 8.1 and Later
siebel.user.language=enu	esd.userLocale = enu

Siebel CRM Version 8.0	Siebel CRM Version 8.1 and Later
siebel.connection.string=CHANGE_ME	esd.handler.webservice.url=CHANGE_ME
siebel.user.name=CHANGE_ME	esd.handler.webservice.username=CHANGE_ME
siebel.password=CHANGE_ME	esd.handler.webservice.password=CHANGE_ME

New and Changed Properties in the ctd.properties Configuration File

The following information lists the new properties in the ctd.properties file.

Property and Seeded Value	Description
ctd.moduleName = CTD	Module name.
ctd.handlerClass = com.siebel.sem.ctd.integrated.OnPremiseCl	Handler class available for custom code.
ctd.queue.clickQSubDir.name = clickQ	ctd subdirectory for click Queue.
ctd.queue.ftfQSubDir.name = ftfQ	ctd subdirectory for forward-to-friend Queue.
ctd.queue.msgOpenQSubDir.name = msgOpenQ	ctd subdirectory for message open Queue.
ctd.queue.listUnsubQSubDir.name = unsubQ	ctd subdirectory for unsubscribe Queue.
ctd.queue.listQSubDir.name = listsubQ	ctd subdirectory for unsubscribe from list Queue.
ctd.validateParameters = true	Determines whether to validate the destination URL against the Trackable URL in the email.

The following table lists the changed properties in the ctd.properties file.

Siebel CRM Version 8.0	Siebel CRM Version 8.1 and Later
siebel.user.language=enu	ctd.user.language=ENU

Siebel CRM Version 8.0	Siebel CRM Version 8.1 and Later
siebel.connection.string=CHANGE_ME	ctd.webservice.url = CHANGE_ME
siebel.user.name=CHANGE_ME	ctd.webservice.username = CHANGE_ME
siebel.user.password=CHANGE_ME	ctd.webservice.password = CHANGE_ME

New and Changed Properties in the bhd.properties Configuration File

The following table lists the new properties in the bhd.properties file.

Property and Seeded Value	Description
Bhd.moduleName = BSD	Module name.
BhdModule.handlerClass = com.siebel.sem.bhd.integrated.OnPremiseB	Handler class available for custom code.
BhdModule.handler.webservice.url = CHANGE_ME	URL for the Web Service connection to the Marketing computer.
BhdModule.handler.webservice.username= ME	Username for the Web Service connection to the Marketing computer.
BhdModule.handler.webservice.password = CHANGE_ME	Password for the Web Service connection to the Marketing computer.

The following table lists the changed properties in the bhd.properties file.

Siebel CRM Version 8.0	Siebel CRM Version 8.1 and Later
BhdModule.bounce_reason.lic.BAD_ ADDRESS_REASON=Bad Address	BhdModule.handler.bounceReason.BadAddress=Bad Address
BhdModule.bounce_reason.lic.ADDRESS_ MOVED_ REASON=Address Moved	BhdModule.handler.bounceReason.AddressMoved= Address Moved
BhdModule.bounce_reason.lic.BAD_ SENDER_REASON=Bad Sender	BhdModule.handler.bounceReason.BadSender=Bad Sender

Siebel CRM Version 8.0	Siebel CRM Version 8.1 and Later
BhdModule.bounce_reason.lic.MAILBOX_ PROBLEM_REASON=Mailbox Problem	BhdModule.handler.bounceReason.MailboxProblem=Mailbox Problem
BhdModule.bounce_reason.lic.SYSTEM_ PROBLEM_REASON=System Problem	BhdModule.handler.bounceReason.SystemProblem=System Problem
BhdModule.bounce_reason.lic.NETWORK_ PROBLEM_ REASON=Network Problem	BhdModule.handler.bounceReason.NetworkProblem=Network Problem
BhdModule.bounce_ reason.lic.PROTOCOL_PROBLEM_ REASON=Protocol Problem	BhdModule.handler.bounceReason.ProtocolProblem=Protocol Problem
BhdModule.bounce_reason.lic.SECURITY_ PROBLEM_ REASON=Security Problem	BhdModule.handler.bounceReason.SecurityProblem=Security Problem
BhdModule.bounce_reason.lic.MESSAGE_ TOO_ LARGE_REASON=Message Too Large	BhdModule.handler.bounceReason.MessageTooLarge=Message Too Large
BhdModule.bounce_reason.lic.LAST_ RESORT_REASON=Last Resort	BhdModule.handler.bounceReason.LastResort=Last Resort
BhdModule.bounce_reason.lic.VACATION_ REASON =Vacation	BhdModule.handler.bounceReason.Vacation= Vacation
BhdModule.bounce_reason.lic. UNPARSABLE_REASON=Unparsable	BhdModule.handler.bounceReason.Unparsable= Unparsable