Veeva CRM 18 Approved Email Administration Guide

June 2013

Contents

Figures

Tables

Approved Email

Approved Email (AE) enables reps to send approved, compliant emails to Accounts from iRep and CRM Online enabling marketing and sales teams to control the branding of emails and related content, track the activity of email recipients, and automatically removing expired content to ensure the latest approved content always displays.

Certain content used and distributed as a part of the Approved Email solution is kept in the Vault Content Management System. The content is divided into three categories:

- Email Template
  - Email Templates are selected by Reps and emailed to Accounts and represent the basic document a rep sends to one or more recipients. This document contains the rich email content that may link to Vault documents and/or other external resources. Approved Email requires Email Templates to be created and managed in Vault PromoMats.
- Email Fragment
  - An Email Fragment is a small snippet of HTML that contains a specific message and hyperlinks to content stored in Vault, or on your own sites. The HTML snippet provides a visual representation to one or more documents that are shared within an Email Template. These are always managed in Vault PromoMats.
- Shared Documents
  - Links to documents (typically PDFs or web pages) can be shared within Email Templates or Fragments. The system of record for these documents can be Vault PromoMats or other websites that a customer controls.

Approved Email Architecture

The architecture of the Approved Email solution is built as an extension of the existing Veeva CRM application and includes three major entities:

- The integration to Vault PromoMats content management solution
- The Veeva Multichannel engine
- The enterprise email engine

The basic architecture of the full Veeva CRM and Approved Email solution is shown below.

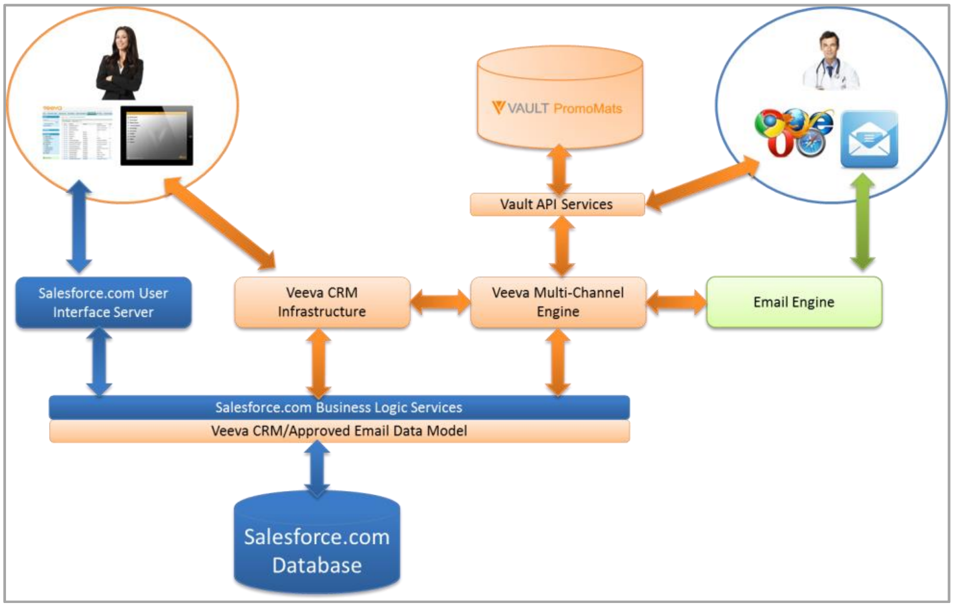

VAULT PromoMats
Vault API Services
Salesforce.com User Interface Server
Veeva CRM Infrastructure
Veeva Multi-Channel Engine
Email Engine
Salesforce.com Business Logic Services
Veeva CRM/Approved Email Data Model
Salesforce.com Database

Figure 1: Architecture

Note: The actual content sent or linked to in the solution is contained in the Vault PromoMats document management solution. Content metadata, email metadata, and email activity/feedback data are all stored in the Salesforce.com data center.

Approved Email Content Validation Flow

To ensure content distributed to end users and customers is the latest approved version of the content, the validity of the content is checked at four stages during the content lifecycle in the Approved Email solution:

- Only content that is approved or is pulled from the Vault PromoMats repository into the Approved Email solution
- Only content that is approved and specifically aligned to the end user is synced to the user's mobile device and available to the user in the online client
- When an end user sends an email, the validation checks are performed again to ensure content is approved
- After a customer receives the email and views the content, only the latest version of the approved content is available for viewing, or suppressed if an approved version is no longer available

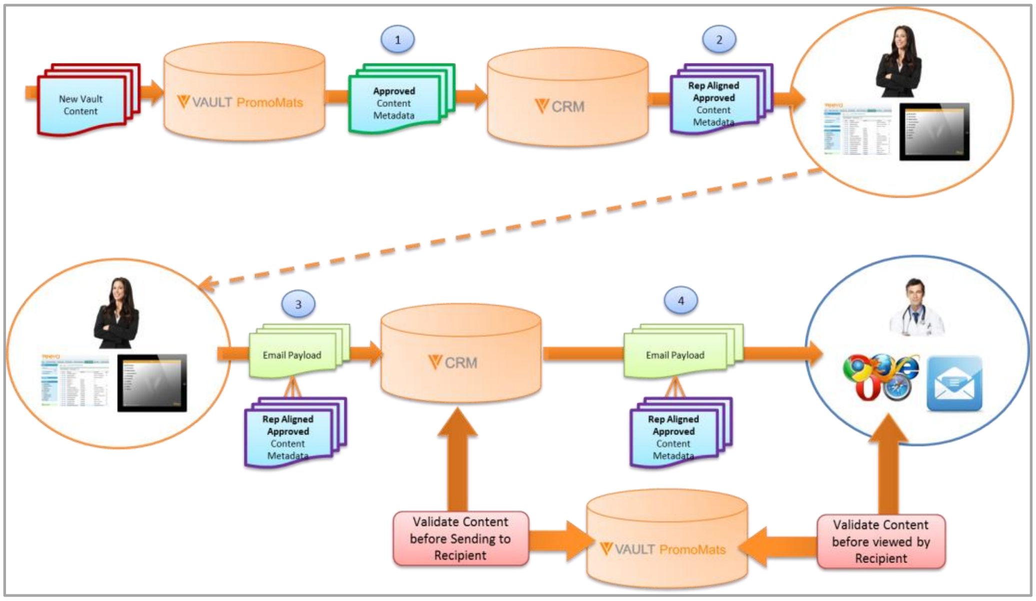

New Vault Content
VAULT PromoMats
1
Approved Content Metadata
CRM
2
Rep Aligned Approved Content Metadata
3
Email Payload
Rep Aligned Approved Content Metadata
CRM
4
Email Payload
Rep Aligned Approved Content Metadata
Validate Content before Sending to Recipient
VAULT PromoMats
Validate Content before viewed by Recipient

Figure 2: Validation Flow

Note: Staged content from Vault PromoMats is also pulled to the Approved Email solution, synced to mobile devices, and available in the online solution for those users who are designated as Approved Email Admins. This allows Approved Email Admins to test content that is not generally available to other users in either sandbox or production environments.

Approved Email Validation -Building and Sending Approved Email

In addition to validating the content available for distribution, Approved Email also performs various types of validation against the email metadata that is built by the end user. The diagram below outlines the validation performed on an email record that a user is preparing to send to one or more customers (recipients).

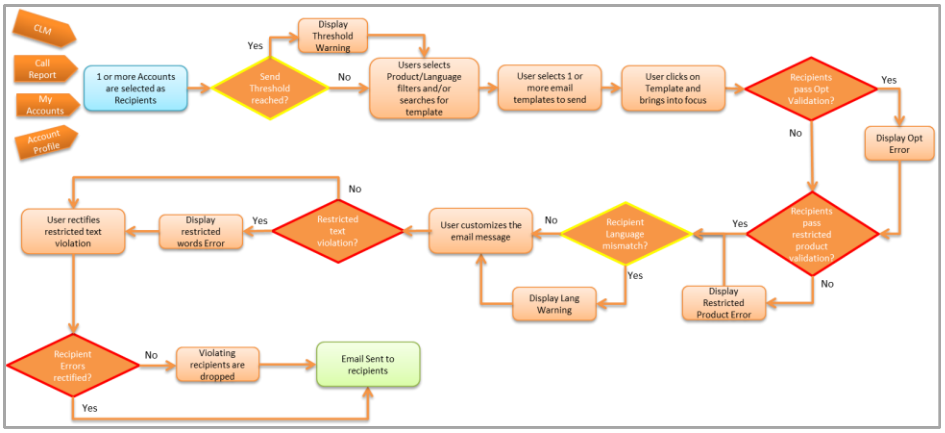

CLM
Call Report
My Accounts
Account Profile
1 or more Accounts are selected as Recipients
Send Threshold reached?
Yes
Display Threshold Warning
No
Users selects Product/Language filters and/or searches for template
User selects 1 or more email templates to send
User clicks on Template and brings into focus
Recipients pass Opt Validation?
Yes
Display Opt Error
No
Recipients pass restricted product validation?
Yes
No
Display Restricted Product Error
Recipient Language mismatch?
Yes
Display Lang Warning
No
User customizes the email message
Restricted text violation?
Yes
Display restricted words Error
No
User rectifies restricted text violation
Recipient Errors rectified?
No
Violating recipients are dropped
Email Sent to recipients
Yes

Figure 3: Email record validation process

Note: Some validation checks result in warnings, while others result in errors. Those validation checks resulting in errors, outlined in red, restrict a user from sending the email to the intended recipient(s). Those validation checks resulting in warnings, outlined in yellow, do not prevent the user from sending the email to the intended recipient(s).

VEEVA CRM APPROVED EMAIL CONFIGURATION INTRODUCTION

Configuring Approved Email is done in several steps.

- Veeva CRM configuration - this activates Approved Email and makes it available to end users. It primarily involves object and page level security and configuration.
- Setup CRM and Vault PromoMats integration - The technical configuration to ensure content metadata from Vault is pulled into CRM.
- Setup sending email domains in the enterprise email engine - This requires the customer to make DNS entries in the domain the own.
- Define the Approved Email processes for opt-in/opt-out consent.
- Load content into Vault and test in CRM - This assumes Email Templates and Fragments HTML content is authored outside of Veeva using the Approved Email Content Creation Guidelines and then loaded into Vault.

There are two types of users who will use Approved Email, End Users and Administrators. Configuring Approved Email for these types of users is mostly the same; however, there are some important differences.

Approved Email Content Administrator Role

There should be one or more designated Approved Email Content Administrators. These are functional users who own the following actions:

- Load content into Vault PromoMats. This includes Email Templates, Email Fragments and Email Template Fragments document types, as well as other documents that are linked within these document types. See details in the Vault documentation. This includes:
  - Loading HTML and (optionally) email images into the correct vault document types
  - Setting the correct Vault properties pulled into Veeva CRM, including Product, (optionally) Language, and the various Email Properties
  - Managing the Vault document workflows to ensure that Vault content is in valid workflow states that Approved Email will understand
- Manually run the refresh process to load content from Vault into Veeva CRM (into the Approved_Document_vod object). The refresh processes are initiated from the Approved Email Administration page.
- Test that Email Templates and Fragments are viewed and sent from within Approved Email, both online and from iRep. This includes:
  - Validate Templates and Fragments render and merge as expected. Note that HTML rendering on different email clients is a separate process that must be done outside of Veeva CRM by content authors. See the Approved Email Content Guidelines for details.
  - Validate all content linked via Vault is in an approved state so that emails can be validated and sent
  - Validate Vault content renders in the Vault Document Viewer when links are clicked from within recipient emails, either in standalone or embedded viewers, depending on what is deployed

SFDC users that act as Approved Email Content Administrators should have User.Approved_Email_Admin_vod Boolean field set to active. This allows the following behavior:

- All emails from the User to all Accounts are sent to the email address in the User.Email field. This ensures the user can test in both staging and production environments without accidentally sending emails to live Account email addresses. A warning message confirms emails are sent to the User's email address.
- Approved Email Content Admins can see Email Fragments and Email Templates where Approved_Document_vod.Status_vod = Staged_vod. This ensures only admins can see content that is not yet Approved so that it can be tested and aligned in sandbox or production environments. Templates and Fragments that are in a Staged status are only visible to Approved Email Content Admins.

Note: Approved Email is designed to support testing of new content in both production and non-production environments. This is facilitated, in part, by two features:

- The Administrator's access to staged content as discussed in this section
- The Approved Email Setting, Approved Email Test Email Address (APPROVED_EMAIL_TEST_ADDRESS_vod). The Test Email Address setting provides an optional safety layer on pre-production environments. When populated, all Approved Emails are sent to the test address to prevent emails from being sent to live Account email addresses.

Veeva CRM Approved Email Technical Setup

The following steps enable basic CRM permissions for users (Reps and Admins). It also covers the technical aspects of integration setup between CRM and Vault PromoMats.

Note: Vault PromoMats must first have Approved Email enabled by Veeva Support.

Object Level Security

There are several new objects included in the Approved Email solution. Use the charts below to configure access according to the type of user.

End Users:

Object/Permission	***Read***	***Create***	***Edit***	***Delete***
Approved Document	✓	x	x	x
Email Activity	✓	x	x	x
Sent Email	✓	✓	✓	x
Multichannel Consent	✓	✓	✓	x

Table 1: End User Object Permissions

Approved Email Admins:

Object/Permission	***Read***	***Create***	***Edit***	***Delete***
Approved Document	✓	✓	✓	✓
Email Activity	✓	✓	✓	x
Sent Email	✓	✓	✓	x
Multichannel Consent	✓	✓	✓	x

Table 2: Admin Object Permissions

Field Level Security

There are several new fields introduced on existing objects that need to be visible to specific types of users using the Approved Email solution.

End Users:

- Account object
    - Approved Email Consent (Approved_Email_Opt_type_vod)
        - Holds the consent type for the Account. Used in Approved Email to drive the opt-in consent model.
    - Language (Language_vod)
        - Holds the preferred language of the Account
    - [Optional] Restricted Products (Restricted_Products_vod__c)
        - Holds the list of Detail level products restricted for detailing/sampling at the Account. Approved Email will respect these restrictions
- Territory Fields Object (TSF)
    - [Optional] Allowed Products (Allowed_Products_vod)
        - Holds the list of Detail level products allowed for detailing/sampling at the Account-Territory combination

Approved Email Admins:

- User object
    - Approved Email Admin (Approved_Email_Admin_vod)
        - Flag used to determine if user can access Approved_Document_vod records where Status_vod = Staged_vod. This flag, if enabled, will also direct all email sent by this user to the User.Email field.
- Product catalog
    - VExternal Id (Vexternal_Id_vod)
        - External Id used by Veeva CRM and Vault to integrate product catalog entries when refreshing Approved_Document_vod object

Record Types

Ensure those users who are using the Approved Email solution (End Users and Approved Email Admins) have access to all of the record types associated to each of the objects below.

- Approved Document Object (Approved_Document_vod)
    - The Approved_Document_vod object is the core object used to persist metadata (with one exception) related to the Approved Email solution
- Sent Email Object (Sent_Email_vod)
    - This object contains a record of outbound emails sent via the Approved Email service. This is the primary object that is synced from a client to the server to build and send email.
- Multichannel Consent Object (Multichannel_Consent_vod)
    - This object stores the consent records associated to an Account. Opt-In and Opt-Out consent records will both be stored in this object. These consent records

may correspond to the Approved Email channel or other customer defined channels.

- Email Activity (Email_Activity_vod)
  - This object holds all of the activity history related to an outbound email event (Sent_Email_vod) such as Opens, Clicks, and Unsubscribes and the details corresponding to each activity

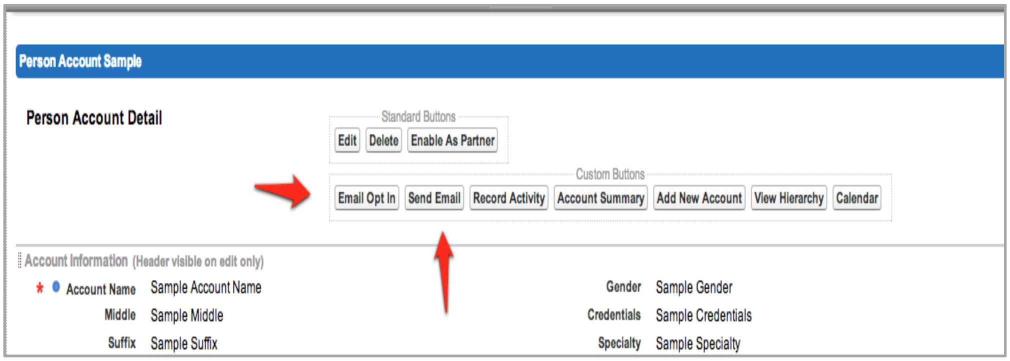
Approved Email Entry Point Configuration

There are additional configuration steps required to enable all entry points. Send Email and Email Opt In actions are available from the following entry points once the configuration is complete:

- Account Detail
- Account List (My Accounts)
- Call Report
- CLM Slides

The following configuration is for all in-use Account page layouts for both End Users and Approved Email Admins:

1. Navigate to the Account page layouts in use by your organization.
2. Add the following buttons to the layouts:
   - Send Email – button to launch the Send Email process at the Account profile level
   - Email Opt In – button to launch the Opt-in process at the Account profile level
3. Ensure that the **Approved_Email_Opt_Type_vod__c** field is on the appropriate Account page layouts if exposing the Opt-In Consent model value at the Account level:
   - If users will be inputting Approved_Email_Opt_Type_vod values directly, ensure the picklist values are accessible for your Account record types
4. Ensure that the **Language_vod** field is on the appropriate Account page layouts if exposing the Account's preferred language.
5. Add the **Sent_Email_vod** related list to the appropriate page layouts.
6. Add the **MultiChannel_Consent_vod** related list to the page layout if exposing Multi-Channel consent capture records at the Account level.



Account Name: Sample Account Name
Middle: Sample Middle
Suffix: Sample Suffix
Gender: Sample Gender
Credentials: Sample Credentials
Specialty: Sample Specialty

Figure 4: Send Email and Email Opt-In Buttons on Account page

Additional steps for Approved Email Admins only:

1. Navigate to the Approved Email Admin page layout on the user object and place the Approved_Email_Admin_vod field in the appropriate section.

Note: Consider removing the Salesforce.com Email Opt Out field from the Account page layouts as this may cause confusion because it is not used by Approved Email.

Tab Visibility

Approved Email Admins need access to two specific tabs in order to perform administrative functions.

- Approved Email Administration – custom Veeva tab used to manage the Veeva-Vault integration
- Approved Documents - standard Salesforce.com tab for the Approved Document object. The system administrator should create a tab and a page layout for this object.

Note: Data in the Approved_Document_vod object should never be updated by users, it should only be updated by the CRM-Vault Integration process.

Note: End users should not have visibility to either of these tabs.

VisualForce Page Access

Access must be granted to specific Visual Force pages for all Approved Email users (End Users and Approved Email Admins). These pages are used to facilitate certain features of the Approved Email solution.

Grant access to the following pages for your user profiles:

- Email_Opt_in_vod
- Send_Approved_Email_vod

Activate/Modify Veeva Mobile Object Configuration Records

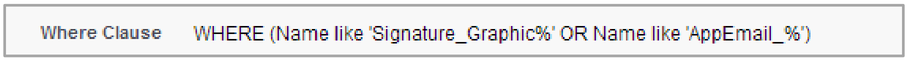
To support Approved Email on iRep, ensure the following VMobile Object Configuration (VMOC) Settings are active.

- Approved_Email_Settings_vod__c
- Approved_Document_vod
- Sent_Email_vod
- MultiChannel_Consent_vod

Email Templates reference images stored on public web servers. To view images in Email Templates while offline in Approved Email, adjust the Attachment VMOC so that Approved Document attachments are synced to iRep. Approved Documents attachments include a copy of the Email Template with embedded images. When synced, the Email Templates and images can be previewed from within Approved Email while offline ensuring that complex emails with many images render properly offline. The disadvantage is initial sync times may increase depending on the volume of Email Templates and embedded images.

To adjust the existing Attachment VMOC to include Email Template Attachments:

1. Navigate to the Attachment VMOC.
2. Click **Edit**.
3. Add the following condition to the WHERE clause:
    a. Name like AppEmail_%



Where Clause WHERE (Name like 'Signature_Graphic%' OR Name like 'AppEmail_%')

Figure 5: Example: WHERE clause in Attachment VMOC to support offline images

Note: Changes made to the Attachment VMOC should be done in addition to any other modifications that may be necessary. The above is just an example of how the VMOC should be configured for Approved Email.

Approved Email Custom Settings

Approved Email includes custom settings that govern configuration. These settings are found in the Approved Email Settings object.

- Approved Email Domain (APPROVED_EMAIL_DOMAIN_vod) – this is required. This is the sending domain of emails generated by AE. This domain must be setup in the Veeva enterprise email engine, and SPF, DKIM, and CNAME records created in the customer's DNS for it to be fully functional and pass email authentication tests. This is a string of a domain name, for example, customer.com or email.customer.com. See the Administration Guide for more setup details.
- Approved Email Opt-in Required (MULTICHANNEL_EXPLICIT_OPT_IN) - Determines NULL behavior of Account.Multi_Channel_Opt_Type_vod attribute. If not enabled, Approved Email Opt-In is not required for Accounts. When enabled, Approved Email Opt-In is required for Accounts, and an opt-in record must be present in MultiChannel_Consent_vod before email is sent to an Account.
- Approved Email Test Email Address (APPROVED_EMAIL_TEST_ADDRESS_vod) - This is an org-level override to support sandbox testing. When an email address value is present, all Approved Emails generated are sent to this address. This overrides the value set in Sent_Email_vod.Account_Email_vod.
- Approved Email Volume - Count Threshold (APPROVED_EMAIL_COUNT_LIMIT_vod). This holds the count component of a frequency threshold that when breached will display a recipient warning.
- Approved Email Volume - Duration Threshold (APPROVED_EMAIL_DURATION_LIMIT_vod) – This holds the time component of a frequency threshold that when breached will display a recipient warning when creating Approved Email.
- Example of Frequency Threshold Calculation

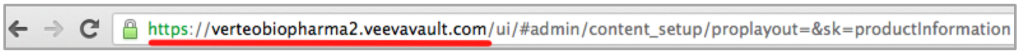
- Approved Email Volume - Count Threshold = 5
- Approved Email Volume - Duration Threshold = 30
- Frequency Threshold is 5 emails per every 30 days. If this threshold is exceeded, a warning displays.

Note: Some of the settings are not listed. These settings link to Veeva Messages described in the following section.

Approved Email Veeva Messages

Below are the Veeva Messages used in certain Approved Email settings. Configuration values should be defined in the Veeva Message not in the setting.

- APPROVED_EMAIL_VAULT_ENDPOINTS (required) - This is a delimited list of Vault endpoints to be used by the Approved Email process to pull documents into the Approved Documents object. Each endpoint is visible after a user logs in to Vault and can be copied from the browser URL bar. The delimiter is double semi-colon, for example https://verteobiopharma1.veevavault.com;; https://verteobiopharma2.veevavault.com. The endpoints are authenticated from within the Approved Email Administration page.



https://verteobiopharma2.veevavault.com/ui/#admin/content_setup/proplayout=&sk=productInformation

Figure 6: Example Vault endpoint in browser

- APPROVED_EMAIL_RESTRICTED_WORDS (not required) - Filters on words or phrases entered in a free text field on an email template. When there is a match, a visible error displays and the email cannot be sent. Double semi-colon is the delimiter, for example, test;;test2;;this is a phrase. Approved Email also supports the {{detailproduct}} markup token; when used will automatically include all the names of products of type Detail in the restricted word validation in the Veeva Message text.
- APPROVED_EMAIL_VAULT_QUERY (not required) - This is a delimited list of Vault query WHERE clauses to add additional filters to limit the data pulled into the Approved_Document_vod object. The order of the clauses maps to the order of the endpoints and must start with the keyword WHERE. This is typically used to filter on other Vault properties. A typical use case would be to filter on the Country (country__v) Vault property. The delimiter is double semi-colon, for example:

  WHERE country__v = 1234567;;WHERE country__v = 8901234 is an example of two filters applied to two separate Vault endpoints.

  This message is used in exceptional cases and is typically NULL. The message value populates the Vault WHERE clause on the Approved Email Administration page.

  Note: It is not possible to create a full Vault query to expand the list of Vault document types that are stored in Approved_Document_vod. This is intended to additionally filter the pre-defined Vault integration query that CRM delivers. The message syntax requires technical knowledge of the Vault API.

- APPROVED_EMAIL_FIELD_EXCLUSIONS (not required) - By default, the Approved Email UI displays all email addresses from fields of type EmailAddress on the Account and Address objects. It is possible to suppress email addresses from specific fields on a global org basis. Enter a list of object.field references, delimited by double semi-colon, for fields of type EmailAddress to suppress values from the Approved Email UI. For example, email address values from a custom field on Account named Home_Email_Address, and a custom field on Address named integration_email can be suppressed by entering Account.Home_Email_Address;;Address.integration_email.
- APPROVED_EMAIL_DISCLAIMER_TEXT (not required) - Holds the disclaimer message to be shown on the opt-in screen. Different messages are displayed for different security Profiles assigned to Reps.
- APPROVED_EMAIL_CONSENT_TEXT (not required) - Holds the consent message adjacent to the confirmation check box displayed on the opt-in screen. Different messages are displayed for different security Profiles assigned to Reps.

Veeva CRM – Vault Integration Setup

After configuring object/field level visibility, page layout configurations, and VMobile Object Configuration, and required settings, you need to configure the Veeva CRM and Vault integration.

Vault documents (Email Templates and Email Fragments) are synchronized via a pre-defined integration with Veeva CRM. Advance configuration is required to ensure this process executes correctly.

Populate External IDs in both Vault and Veeva CRM for Product

In order to match the appropriate Product references from Vault to the Product records in Veeva CRM, the external IDs must be specified for both Vault Products (Product__v) and Veeva CRM Products (Product_vod).

CRM Setup

1. Navigate to the Product_vod (Product Catalog) object and ensure the VExternal_Id_vod field is visible to the Administrator.
2. Place the VExternal_Id_vod field on the Product Catalog page layout for the Administrator.
3. Populate the field for the Products you are using in Approved Email demos. This field is unique and case insensitive, i.e. Restolar's VExternalId could be **Restolar_ExternalId.**

Vault Setup

1. Navigate to the Product Catalog in Vault.

2. Populate an External Id for each product in the Vault Product Catalog that corresponds to what you populated in the CRM app for that specific product. This is used to map the Product references on the Approved Documents refreshed from Vault.

Note: When connecting multiple SFDC orgs to one Vault instance, it is required that each org contain a complete list of external IDs defined in the Vault product catalog. To work around this limitation, populate unique query strings in each org that limit the documents retrieved from Vault based on a product filter. This is set in the Veeva Message APPROVED_EMAIL_VAULT_QUERY. For example this limits the retrieved documents to only two products (note IN is not a supported operator):

WHERE (product__v = 1364863150687 or product__v = 1364850017947)

Populate External IDs for Detail Groups using Vault Public Key

Follow these configuration steps only if you are using the Detail Group functionality. See the Veeva CRM Administration Guide for more information on Detail Groups. The process to define the external ID values is different than with products.

This process involves accessing the name attribute for the Detail Group value assigned to Email Templates and Email Fragments in Vault. The REST query for retrieving the name values is below, where [yourVaultDNS] is the URL endpoint displayed in your browser bar after logging in to Vault PromoMats.

https://[yourVaultDNS]/api/v6.0/objects/picklists/detail_group__v?loc=true

Note: The Vault DNS is the unique Vault instance you are using for the integration.

Configuration

To use Postman to retrieve external IDs from Vault:

1. Download an HTTP Dev tool. Postman (for the Chrome browser) is the tool of choice and is used in these instructions.

Figure 7: HTTP Dev tool options

2. Run the plugin.
3. Click **Environment**.
4. Select **Manage Environments**.

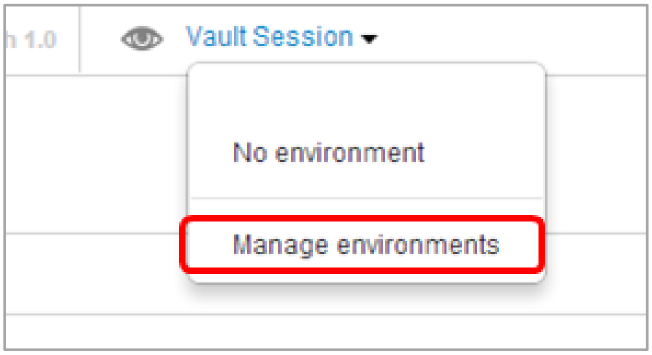
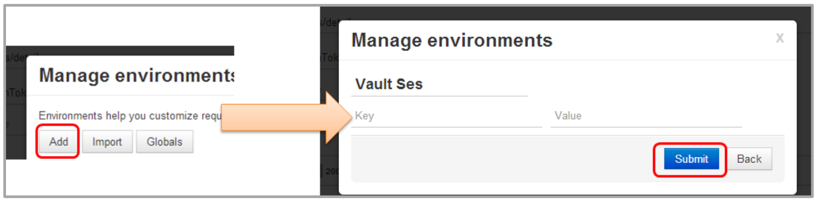


Figure 8: Manage Environments using Postman

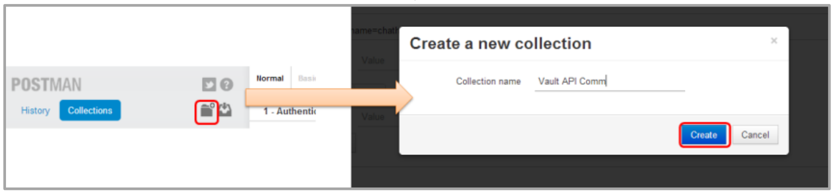
5. Add a new Environment by typing in a name. For example, Vault Sec.
6. Add the key name **authToken**.
7. Click **Submit** to save the environment.



Vault Ses

Figure 9: Add new Postman Environment

8. Create a collection bucket to hold your Vault API commands so that they can be re-used.



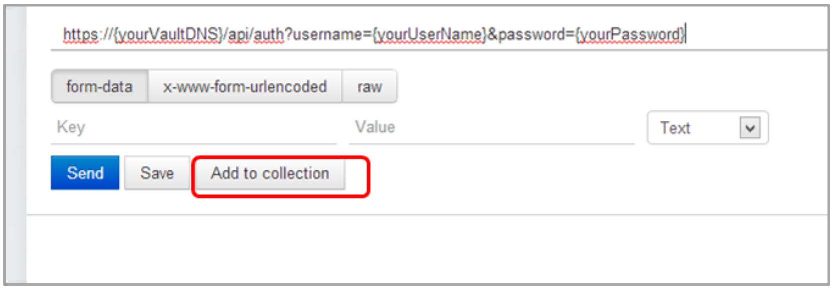
Collection name Vault API Comm

Figure 10: Create HTTP Request Collection in Postman

9. Create an authentication POST request and store it in the collection. The below request is how you authenticate to the Vault API. Replace the bracketed text with your corresponding information.

   https://[yourVaultDNS]/api/auth?username=[yourUsername]
   &password=[yourPassword]

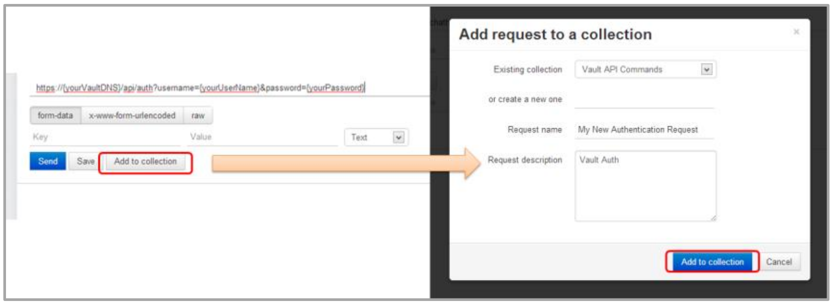
10. Click **Add to Collection**.



https://{yourVaultDNS}/api/auth?username={yourUserName}&password={yourPassword}

Figure 11: Add to Collection in Postman

11. Add HTTP authentication request to the collection created in Step 8.



https://{yourVaultDNS}/api/auth?username={yourUserName}&password={yourPassword}

Add request to a collection

Existing collection: Vault API Commands

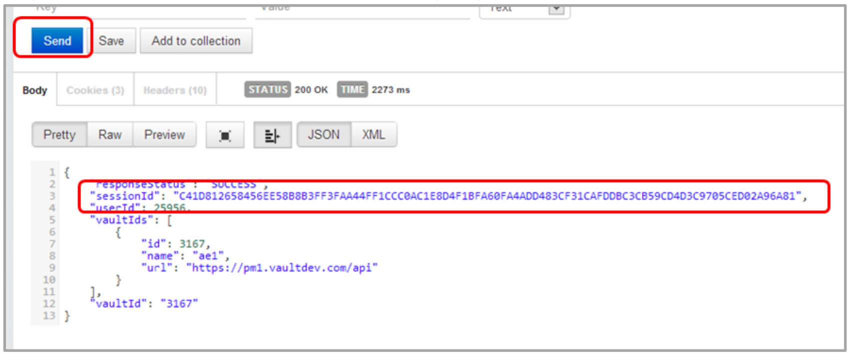
or create a new one:

Request name: My New Authentication Request

Request description: Vault Auth

Figure 12: Select Existing Collection

12. Send the authentication request to Vault. The default response from Vault is a JSON object that contains the sesionId. Highlight and copy this sessionId to the clipboard.



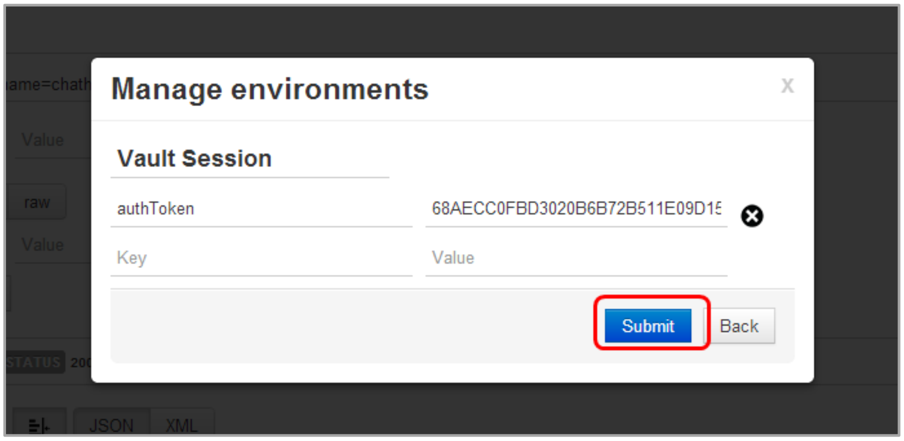
STATUS 200 OK TIME 2273 ms

```
{
    "responseStatus": "SUCCESS",
    "sessionId": "C41D812658456EE58B8B3FF3FAA44FF1CCC0AC1E8D4F1BFA60FA4ADD483CF31CAFDDBC3CB59CD4D3C9705CED02A96A81",
    "userId": 25956,
    "vaultIds": [
        {
            "id": 3167,
            "name": "ae1",
            "url": "https://pm1.vaultdev.com/api"
        }
    ],
    "vaultId": "3167"
}
```

Figure 13: Send Authentication request to Vault

13. Navigate back to the environment manager.

14. Click the environment created in step 5 and paste this sessionId into the Value field (screenshot assumes the parameter key is named authToken).



Manage environments

Vault Session

authToken	68AECC0FBD3020B6B72B511E09D15
Key	Value

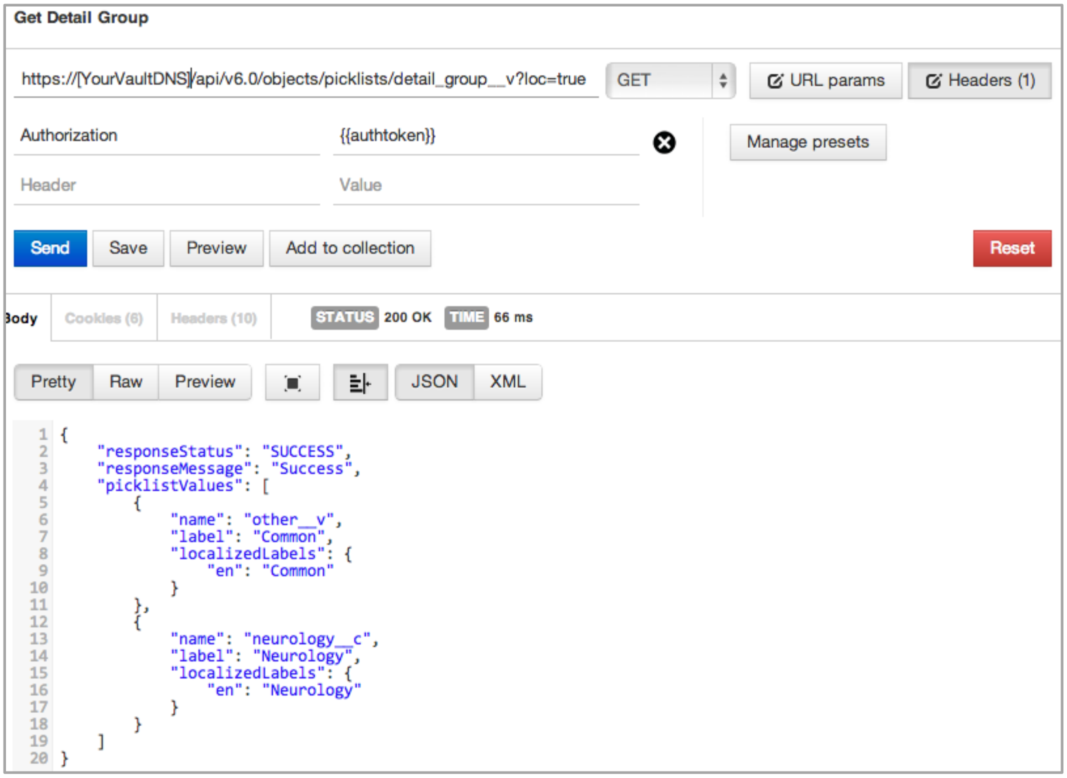
Figure 14: Update sessionID in Postman environment

15. Create an API GET request to retrieve the Detail Group picklist keys. Construct your request as shown below. Be sure to include the authorization token in this request. The string {{authToken}} must be entered literally as the value corresponding to the

authorization header. Postman will replace {{authToken}} with the sessionId saved as an environment variable in step 5 when sending the request to the Vault API.

Example

GET request to retrieve Detail Group values
https://[yourVaultDNS]/api/v6.0/objects/picklists/detail_group__v?loc=true



https://[YourVaultDNS]/api/v6.0/objects/picklists/detail_group__v?loc=true

Authorization {{authtoken}}

STATUS 200 OK TIME 66 ms

```
{
    "responseStatus": "SUCCESS",
    "responseMessage": "Success",
    "picklistValues": [
        {
            "name": "other__v",
            "label": "Common",
            "localizedLabels": {
                "en": "Common"
            }
        },
        {
            "name": "neurology__c",
            "label": "Neurology",
            "localizedLabels": {
                "en": "Neurology"
            }
        }
    ]
}
```

Figure 15: Values for Detail Groups from GET request

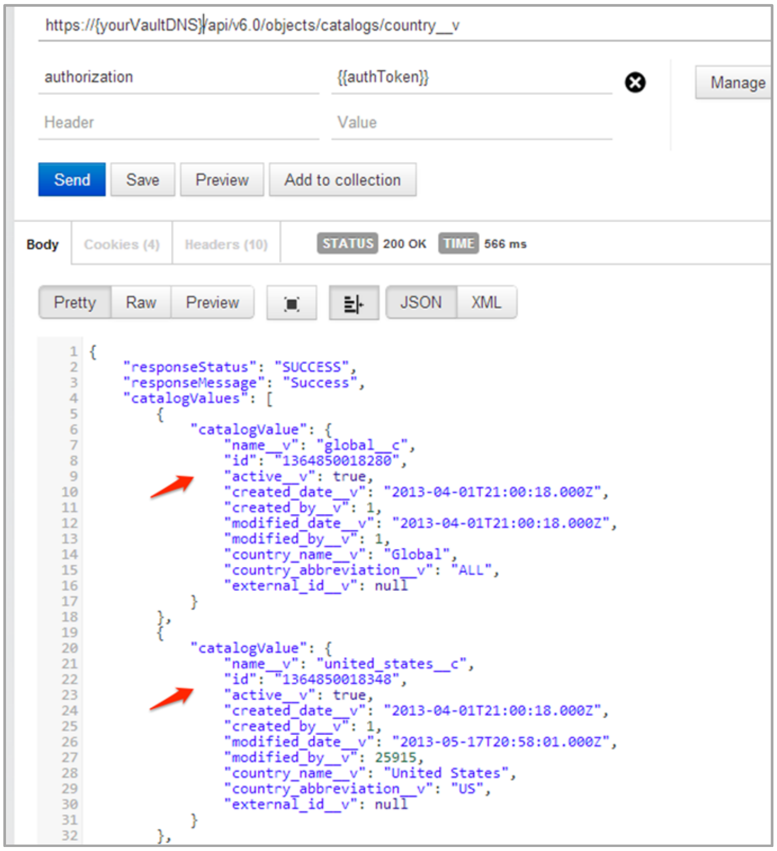
The JSON response contains names and labels of the Detail Groups. Store the “name” values in the VExternal_Id_vod field for the corresponding Detail Group records in the Veeva CRM Product Catalog (Product_vod).

Note: The name value “other__v” automatically maps to the Detail Group Common that displays in My Setup and in the Approved Email filters. It is not required to populate this value in Product_vod.VExternal_Id_vod because there is no corresponding value in the CRM Product Catalog.

Note: Do not delete the Detail Group Common picklist value in Vault because this will break the Vault-CRM integration. If deleted by accident, a Veeva Support ticket is required to fix the problem.

In some cases, retrieving the Country or Product attributes for Vault documents is useful, especially when creating custom Vault Queries for the integration service. When specifying a query for the integration process, Vault Query Language (VQL) syntax must be used. VQL utilizes a SQL-like syntax when passing query requests to the Vault API. When querying Vault documents based on the Country attribute, VQL syntax requires the use of the Vault Primary Key for the Country record in the VQL WHERE clause. A similar approach to what is outlined above must be used to retrieve the Country Primary Keys from the Vault API. Steps 1-13 are the same; however, a different request is made to retrieve the Vault Primary Keys for the Country records:

- ○ Create an API GET request to retrieve the private keys. Unlike the request in step 14 that was used to retrieve picklist metadata, this request will be for catalog data. Configure your request as shown below. Be sure to include the authorization token in this request. The {{authToken}} needs to be entered literally as the value corresponding to the authorization header. Postman will replace the sessionId saved as an environment variable in the previous step when sending the request to the Vault API.
- ○ GET request to retrieve Country key id values
    - ○ https:// [yourVaultDNS]/api/v6.0/objects/catalogs/country__v
- ○ GET request to retrieve Product key id values
    - ○ https:// [yourVaultDNS]/api/v6.0/objects/catalogs/product__v



https://{yourVaultDNS}/api/v6.0/objects/catalogs/country__v

authorization {{authToken}}

```
{
    "responseStatus": "SUCCESS",
    "responseMessage": "Success",
    "catalogValues": [
        {
            "catalogValue": {
                "name__v": "global__c",
                "id": "1364850018280",
                "active__v": true,
                "created_date__v": "2013-04-01T21:00:18.000Z",
                "created_by__v": 1,
                "modified_date__v": "2013-04-01T21:00:18.000Z",
                "modified_by__v": 1,
                "country_name__v": "Global",
                "country_abbreviation__v": "ALL",
                "external_id__v": null
            }
        },
        {
            "catalogValue": {
                "name__v": "united_states__c",
                "id": "1364850018348",
                "active__v": true,
                "created_date__v": "2013-04-01T21:00:18.000Z",
                "created_by__v": 1,
                "modified_date__v": "2013-05-17T20:58:01.000Z",
                "modified_by__v": 25915,
                "country_name__v": "United States",
                "country_abbreviation__v": "US",
                "external_id__v": null
            }
        },
```

Figure 16: The ID values for the Country catalog entries can be used in the VQL WHERE clause

Example scenario for filtering Vault Documents by Country:

- 1 Veeva CRM Org connects to 2 different Veeva Vaults (VaultA and VaultB)
- 2 Vault Endpoints are setup in the Approved Email Administration Tab

- The Veeva CRM Org should only pull Approved Documents from VaultA where the country attribute is set to United States (id= 1364850018348); therefore the Vault query for VaultA should look like the example:

  WHERE country__v = '1364850018348'

- The Veeva CRM Org should only pull Approved Documents from VaultB where the country attribute is set to Global (id= 1364850018280); therefore the Vault query for VaultA should look like the example:

  WHERE country__v = '1364850018348'

Language

Approved Email supports language attributes on the Approved Document and Account Objects. This attribute drives the preferred language functionality for the recipient list and filtering in the Approved Email document selector.

Approved Document - Language_vod
This field holds the language attribute of the Vault document. Language values for Approved Document records are populated directly from Vault by the Veeva CRM - Vault integration. This is a picklist which should hold the ISO codes for all of the languages in use by the Vault application. Out of the box, this field is populated with the ISO code for English, en_US. This is the only delivered value and is the default. Customers can modify this picklist field by adding the necessary ISO codes for the languages in use by Vault. Different default values can also be set.

Note: Approved Email users must have visibility to this field.

Approved Email users will have the ability to filter content based on language.

Account - Language_vod
This field holds the preferred language for the Account record. The Language value for an Account record displays in the Approved Email solution when viewing selected recipients. This is a picklist which should hold the ISO codes for the Account’s preferred language. This field is delivered with a single value, en_US, and can be expanded to hold the complete set of ISO language codes in use by the organization.

The Approved Email solution will alert the end users when recipients with different languages are selected to receive a single email. This warning message comes from the LANGUAGE_CONFLICT_WARNING Veeva Message.

Note: Approved Email users must have visibility to this field.

Using Detail Groups in Vault PromoMats

When using Detail Groups in a CRM org, they must be enabled in Vault. Detail Groups are disabled by default in Vault.

To enable Detail Groups, follow these steps:

1. Populate the **Detail Group** values in Vault (Admin->Promomats Setup->Picklists->DetailGroup).
2. Click **Edit** to add new Detail Groups. Do not delete the Common entry. This is required to map to the default Common group delivered in Veeva CRM.

To enable Detail Groups, add the picklist to the Email Template, Email Fragment, and Template Fragment document types.

1. Navigate to the **Document Properties**. (Admin->Content Setup).
2. Select each of the above document types.
3. Select **Add**, **Existing Shared Property**, **Detail Group**. You should only be able to select one value
4. Navigate to **Property Layout** (Admin->Content Setup->Property Layout) to order the Product Properties.
5. Select **Product Information** from the list
6. Click **Edit** and order so Detail Group is first, Product is second.

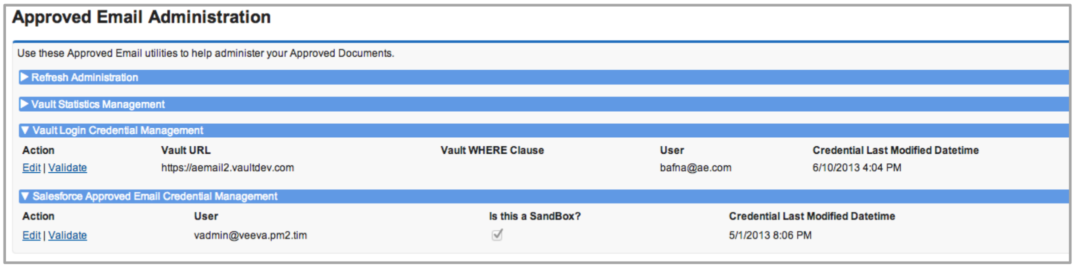
A Vault content administrator may not be familiar with the dependency between Detail Groups and Products. This is typically defined within CRM. In Vault, it is possible to setup dependent picklists where specific Products are grouped beneath specific Detail Groups to represent the CRM Detail Group + Product relationships. While not required, this will help guarantee valid Detail Group + Product attributes are selected.

To setup Property Dependencies:

1. Navigate to **Property Dependencies**.
2. Click **Add a New Property Dependency**.
3. Select **Controlled by Document Property**.
4. Select the **Type**.
5. Repeat for Email Template, Email Fragment, Template Fragment.
6. Select **Detail Group** from the Property picklist.
7. Click **OK**.
8. Select the desired Detail Group from the picklist in the Condition section if property equals Detail Group.
9. Select **Picklist** from the first picklist under the Dependency Rules section.
10. Select **Product** from the next picklist.
11. Choose the list of products to associate with the selected Detail Group.

Managing Vault Integration using Approved Email Administration Tab

The Approved Email Administration Tab is used for administering Vault content in Veeva CRM. There are several sections on this page representing a different administrative task.



Approved Email Administration

Use these Approved Email utilities to help administer your Approved Documents.

▶ Refresh Administration
▶ Vault Statistics Management
▼ Vault Login Credential Management

Action	Vault URL	Vault WHERE Clause	User	Credential Last Modified Datetime
Edit | Validate	https://aemail2.vaultdev.com		bafna@ae.com	6/10/2013 4:04 PM

▼ Salesforce Approved Email Credential Management

Action	User	Is this a SandBox?	Credential Last Modified Datetime
Edit | Validate	vadmin@veeva.pm2.tim	☑	5/1/2013 8:06 PM

Figure 17: Administration Tab

Refresh Administration

Use this section for pulling content from Vault into Veeva CRM. There are three major functions:

- Allow the admin to initiate an Incremental Refresh - This will pull documents from Vault into Veeva CRM that have been modified since the last refresh. This is the same process that is executed by the scheduled task, and is used when in a steady-state.
- Allow the admin to initiate a Force Full Refresh - This will pull all documents from Vault into Veeva CRM. This is normally used in the early stages of implementation or to troubleshoot.
- Give the admin visibility into the success and failure of the last 10 refresh processes

Vault Statistics Management

Vault Statistics Management provides an option to manually trigger the scheduled task that pulls Vault statistics into Email_Activity_vod (see Scheduling the Veeva CRM-Vault Integration Process for details). *To run the process, c*lick the **Pull Vault Statistics** button.

Vault is the system of record for document views and downloads for all Vault documents referenced within Email Templates and Email Fragments. When an email recipient clicks a link to view a document, Vault captures the view activity. When *a recipient clicks the* Download button on the Vault viewer, the download activity is captured. These activity statistics are inserted into Email_Activity_vod when this process is run.

Links that point to documents hosted outside of Vault will not have activity records in Email_Activity_vod. However, the click event, and the target URL of the click, *are* captured in Email_Activity_vod

Vault Credential Management for Approved Email

This manages the Vault credentials for integration with CRM. In this section, you must populate all of the credentials corresponding to one or more Vaults that support Approved Email. Each line in this section represents a single Vault instance from which Veeva will pull Vault Document metadata into the Approved_Document_vod object.

For each Vault instance listed in this section, you must supply a Vault username and password, and this user must have the Vault User Type of System Admin. Clicking the Validate link next to the credentials confirms they authenticate and creates a Vault session.

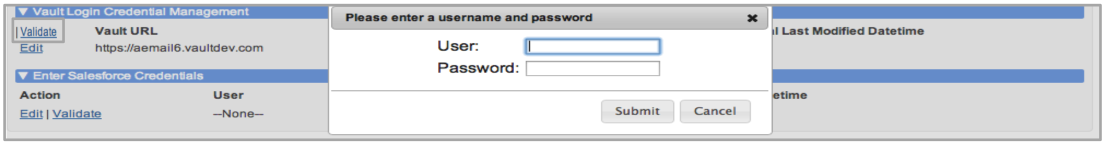
Note: The Vault integration user must be assigned to a Vault Security Policy (Users->Settings->Security Policy) that has a Password Expiration value of No Expiration. If the password ever expires, the integration will fail.

The Vault URL endpoints and optional Vault WHERE Clause automatically populate from the following Veeva Messages under the category Approved Email (see Approved Email Veeva Messages for details).

- APPROVED_EMAIL_VAULT_ENDPOINTS
- APPROVED_EMAIL_VAULT_QUERY

The Vault authentication credentials are used for several Approved Email integration processes. All actions are fully audited in the Vault activity logs.

- Query Vault during the 'Incremental Refresh' of Vault metadata into Approved_Document_vod
- Query Vault during the 'Full Refresh' of Vault metadata into Approved_Document_vod
- Query Vault to validate outbound Email Templates, Email Fragments and all referenced Vault documents are approved or in a steady state for distribution prior to sending an email.
- Query Vault to pull Vault document events (views and downloads by email recipients) into CRM object Email_Activity_vod
- Write back to the Vault activity log events related to the Incremental Refresh and Full Refresh processes. This provides an audit trail within Vault that lists all SFDC orgs that reference each Email Template or Email Fragment.



https://aemail6.vaultdev.com

--None--

Figure 18: Vault Log in

Salesforce Credential Management for Approved Email

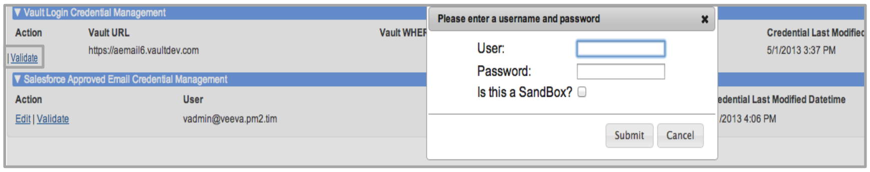
Approved Email admins need to specify a separate integration user that the Approved Email process will run under. There is no limitation on the type of user that can be used for this process as long as the basic CRM and Approved Email Administrator permissions are set and the user has access to the force.com API.

Note: The SFDC integration user Profile must have the Password Never Expires field selected (set to true). If not, the Veeva Multichannel engine integration will fail.

To setup your Approved Email integration user:

1. Click on the **Approved Email Administration** tab.
2. Click Edit under the Salesforce Approved Email Credential Management section.
3. Enter the SFDC credentials for your SFDC account.

4. Select if this is a Sandbox, if you are using a sandbox (SFDC login URL is https://test.salesforce.com).
5. Click Submit.
6. Click Validate to confirm you can authenticate against SFDC with these credentials.



▼ Vault Login Credential Management

Action	Vault URL	Vault WHEF	Credential Last Modifiec
| Validate	https://aemail6.vaultdev.com		5/1/2013 3:37 PM

▼ Salesforce Approved Email Credential Management

Action	User	edential Last Modified Datetime
Edit | Validate	vadmin@veeva.pm2.tim	/2013 4:06 PM

Please enter a username and password

User:

Password:

Is this a SandBox? □

Figure 19: Approved Email Integration

Scheduling the Veeva CRM-Vault Integration Processes

The refresh document process, as well as other important Approved Email processes, should be scheduled to execute once a day during non-office hours.

This scheduled process has these four main functions:

- Pull Vault Statistics - View and Download activities of Vault documents referenced in Approved Emails are collected by Vault. This process inserts the activity records into the Veeva CRM Email_Activity_vod object.
- Retry Email Send – Retries sending email that is not sent. This is typically because of a failed connection to the email engine. Unsent emails in Sent_Email_vod have a status of Saved.
- Retry Inserting Email Engine Activities - Any Email activity, for example, clicks and opens, that were not inserted to Veeva CRM Email_Activity_vod for any reason will be retried
- Fetch Approved Document Changes - Any changes to Vault Document metadata that have not been synced to Veeva CRM will be sent to Veeva CRM via the incremental refresh process

Ensure the Approved Email Admin's Profile has security access to the following class: VEEVA_MULTICHANNEL_SCHEDULED_TASKS

You will need to schedule this job to run at a recurring interval.

To setup the schedule for this process:

1. On the **Apex Classes** page.
2. Click **Schedule Apex**.
3. Give a name to the Job.
4. Select the class mentioned above via the lookup.
5. Set your run frequency for your job – it is recommended to run the process during off-peak hours, once a day.

Managing the Approved Email Configuration across Environments

The configuration driving the functionality of the Approved Email solution is managed across environments in the same manner as it is in Veeva CRM with one exception. When refreshing/creating sandboxes, be sure to enter the correct credentials corresponding to the testing environment in the Approved Email Administration Tab. This is important to understand for full sandboxes because this data is not within the scope of the Salesforce.com full sandbox refresh process.

Understanding Approved_Document_vod and the Vault Refresh Processes

Users are aligned to Approved Email content stored in Approved_Document_vod. This object is populated from Vault PromoMats using the refresh processes described above. Administrators should never manually update or insert content into this object. Users should generally never have access to a native SFDC tab for this object unless they are Approved Email Administrators who want to validate content synced from Vault.

Approved Email Setup – Email Engine, Email Headers, Activities, And Consent

Implementing and administering Approved Email requires decision making and technical setup related to several functional areas.

Email Engine Introduction

The email engine requires at least one sending domain be configured and properly authenticated. This requires customers to create a DNS record to authorize Veeva to send email on behalf of customer domain(s).

Email authentication is a broad topic. To learn more, review this document published by Return Path, a widely respected email monitoring service. It is standard practice for email marketing solutions to send email on behalf of a customer.

To be in compliance with USA CAN-SPAM and EU Directive laws regarding domain spoofing, and to be in compliance with industry standard email authentication technologies, it is required for customers to grant permission for Veeva Approved Email to send email on behalf of a registered internet domain that a customer owns. To do this, a customer creates DNS entries for the domains that authorize Veeva's Enterprise Email Engine to send email.

The configuration process accomplishes three things:

- Technically segregates a customer's outbound corporate email from promotional email. This protects the sending IP addresses that the customer uses for their internal email servers
- Ensures that outbound Approved Emails are properly authenticated, and have a valid <return-path> header that is not spoofed
- Ensures that Approved Emails pass industry standard email authentication protocols that are widely used by MS Exchange and public webmail providers. These standards include:
    - SPF (Sender Policy Framework)
    - DKIM (a Google standard widely adopted by many email providers and Exchange servers)
    - SenderID (derived from SPF and pioneered by Microsoft. Used by all MSFT webmail services)

- Legitimately preserves the outbound branding and appearance of Approved Emails so recipient email clients do not display messages, for example, ***on behalf of*** (MS Outlook and Hotmail) or ***via*** Gmail that indicate to recipients that emails are sent from third party systems.

Email Engine Configuration

While email authentication standards vary their implementations, the validation mechanisms are identical and all rely on domain owners to publish DNS TXT records that are publicly accessible. The TXT records are referenced by receiving email servers to validate that Veeva's Email Engine is authorized to send email from customer domains.

A customer can setup one or more sending domains, but is required to setup at least one. It is the customer's choice to use a domain or subdomain, for example, @company.com vs. @subdomain.company.com. Using a domain offers more flexibility if the customer wants emails to be from the Rep's email address (assuming the format *rep@company.com* is used). Using one or more subdomains is also acceptable, but uses slightly more administration to effectively use the domains across different email templates. An example of a subdomain could be @promotions.company.com.

Another alternative is to use brand.com domains. This reinforces the product branding, but may also limit the ability to use rep email addresses in the from header. An example of a sending domain could be @cholecap.com, with a from header of promo@cholecap.com.

Setting up sending domains for customers requires several steps. It can take time to update customer DNS records so this should be coordinated with customer IT departments early in the implementation.

To setup a sending domain:

1. Define the sending domain(s) or subdomain(s), for example, company.com or subdomain.company.com.
2. Create a CRM Support Ticket to create the domains in the email engine. After creating the domains CRM Support will respond with the specific DNS entries the customer must create to authorize the domain. Three DNS records are required per domain:
   a. One TXT record for SPF & SenderID authentication
   b. One TXT record for DKIM and DomainKeys authentication
   c. One CNAME record used for URL re-directs. For example, URLs contained within emails will be wrapped by the re-direct URL to track when a recipient clicks a link. The CNAME will be used to create a re-direct URL in the form of http://email.company-domain.com/long-tracking-string

The customer must work with internal IT stakeholders to gain permission to update DNS records. This may take time, but is a standard practice when sending promotional or transactional email from most CRM or Marketing Automation solutions, including Salesforce.com, ExtractTarget, Eloqua, and many others.

CRM Support must validate that the supplied DNS entries are properly setup by the Customer. A standard dig (on Unix) or ns lookup (on Windows) can validate this. For example (replace the italics with the customer domain):

- dig CNAME email.*customer-domain.com*
- dig TXT *customer-domain.com*

The customer can use the configured sending domains in Approved Email:

- APPROVED_EMAIL_DOMAIN_vod. This is the default. Required Approved Email setting
- In the Vault Email Template, Email Domain property that is pulled into Approved_Document_vod.Email_Domain_vod. This is optional. It defines the domain only for this email template and overrides the value in APPROVED_EMAIL_DOMAIN_vod.

Email Headers – From, Replies, Sending Domains

For each email template, you can configure unique from, (optionally) reply-to, and (optionally) sending domain headers. You may want specific emails to be from the Rep (User.Email), and others from a fixed email address, for example always from brand@customer.com. Details on how these values are set by Approved Email Content Admins is in the Approved Email Content Guidelines.

Email headers are defined by internet standards, and Veeva complies with these and the email authentication standards such as SPF, DKIM, DomainKeys and SenderID.

The following are functional descriptions of email header values and how they impact the Approved Email experience:

- From Address – this is the email address that displays in the From field in all email clients. This is a required field and is set in Vault on the Email Template document type.
- From Name – this is the descriptive name (for example, first name and last name) that email clients display. Set in Vault on the Email Template and is optional.
- Reply To Address – this is the email address that replies are sent to. This can be different from the From Address. (If not set, replies go to the From Address.) Set in Vault on the Email Template and is optional.
- Reply To Name – this is the descriptive name that email clients will display. This is optional.
- Subject – this is the subject that displays in all email clients. Set in Vault on the Email Template and is required.
- Sending Email Domain – This is the authenticated domain that emails are sent from and is set by the email engine in the <return-path> email header. This is required and can be configured in two ways:
  - Sending Email Domain field on Approved_Document_vod. Set in Vault on the Email Template and is optional. When set in Vault, this value overrides the value set in the Approved Email Setting Approved Email Domain (APPROVED_EMAIL_DOMAIN_vod). This allows a product branded email template to be sent from a brand.com authenticated domain. When NULL, we default to (see below).
  - Approved Email Setting Approved Email Domain (APPROVED_EMAIL_DOMAIN_vod). This is the default when a value is not set

on the Email Template. A unique domain can optionally be defined for each security Profile. The common example is for multi-country orgs where the sending domain is different for each country.

In general, you will want your sending domains to be the same as the domains used in the from address header. For example, if the from address is user@company1.com, the sending domain should be configured as company.com. This offers two advantages:

- Email clients will not display a message that indicates a mismatch between these domains. For example, Outlook typically displays this message in the format From user@company1.com on behalf of company2.com. Gmail typically displays it as From user@company1.com via company2.com.
- Slightly higher ability to deliver email directly to the recipient's inbox

The following are examples of how the From and Reply-to headers can be configured on Email Templates in Vault. For reference, User.Email will use the email address from the User (Rep's) record, User.Name will use Rep's name. This assumes the user's name is Sarah Jones, and her email address is sjones@company.com.

Example 1

From displays as: Sarah Jones <sjones@company.com>
Replies go to: Sarah Jones <sjones@company.com>

	From Address	*From Name*	*Reply-to Address*	*Reply-to Name*
Example Values	User.Email	User.Name	n/a	n/a

Table 3: Email Headers – Example 1

Example 2

From displays as: Sarah Jones <sjones@company.com>
Replies go to: Customer Service <replies@brand.com>

	From Address	*From Name*	*Reply-to Address*	*Reply-to Name*
Example Values	User.Email	User.Name	replies@brand.com	Customer Service

Table 4: Email Headers – Example 2

Example 3

From displays as: Sarah Jones <name@company.com>
Replies go to: Sarah Jones <name@company.com>

	From Address	*From Name*	*Reply-to Address*	*Reply-to Name*
Example Values	name@company.com	User.Name	n/a	n/a

Table 5: Email Headers – Example 3

Example 4

From displays as: Company Mailbox <name@company.com>
Replies go to: Sarah Jones inbox@salesforce.com
Note: The following example requires that a force.com inbox be setup in your org. It requires custom Apex code to manage and route the inbound email replies. But it allows customers to manages replies within salesforce and maintain a conversation thread.

	From Address	*From Name*	*Reply-to Address*	*Reply-to Name*
Example Values	name@company.com	Company Mailbox	inbox@salesforce.com	User.Name

Table 6: Email Headers – Example 4

Approved Email Activity Tracking

The Enterprise Email Engine and Vault track different types of activities and related information. This section describes the events and data attributes collected.

Email Activity is captured at a granular level in the Email_Activity_vod object that is a child of the Sent_Email_vod object. The Event_Type_vod field on Email_Activity_vod indicates the type of activity.

The following actions are tracked and posted back to Veeva by the Enterprise Email Engine:

- Opens (Event_Type_vod = Opened_vod) - Indicates an email has been opened by the recipient
- Clicks (Event_Type_vod = Clicked_vod) - Indicates a link within the email has been clicked
- Unsubscribes (Eevent_Type_vod = Unsubscribe_vod) - Indicates the recipient has successfully completed the unsubscribe process. When an unsubscribe is received, an Opt-Out Multichannel_Consent_vod record is also created.
- Bounces (Event_Type_vod = Bounced_vod) - Indicates a delivery failure. This type of response comes from the recipients inbound mail server and can indicate various issues with the delivery attempt.
    - When the initial Bounce response is generated by the recipient, a Dropped response will also be posted back to Veeva to indicate further messages to this recipient from the sending domain will also be dropped
    - An Opt-Out type Multichannel_Consent_vod record will also be generated
- Mark as Spam Messages (Event_Type_vod = Marked_Spam_vod) - Indicates the message was marked as spam by the recipient
    - When the initial Spam response is generated by the recipient, a Dropped response will also be posted back to Veeva to indicate further messages to this recipient from the sending domain will also be dropped
    - An Opt-Out type Multichannel_Consent_vod record will also be generated
- Drops (Event_Type_vod = Dropped_vod) - Indicates a delivery failure. This type of response comes from the Enterprise Email Engine when an email is sent to a recipient that has previously 1) marked communications from the sending domain as spam or 2) the email address has previously bounced.

The following activities are tracked by Vault when documents are viewed by email recipients. Activities are written into CRM manually from the Approved Email Administration page, or the Vault-CRM scheduled task:

- Views (Event_Type_vod = Viewed_vod) - Indicates a document included in the email message was viewed on Vault PromoMats
- Downloads (Event_Type_vod = Downloaded_vod) - Indicates a document included in the email message was downloaded from Vault PromoMats

Aligning Approved Email Content to Reps

Throughout the Approved Email solution, access to content is handled by four fundamental controls:

- Approved Document Status field (Approved_Document_vod.Status_vod) - An End User can only access Approved Documents which have Status_vod = Approved_vod
    - An Admin User (as defined by configuration) can only access Approved Documents which have Status_vod = Approved_vod or Status_vod = Staged_vod
- My Setup Products object (My_Setup_Products_vod) - An End/Admin user can only access content that is aligned to a Detail Product/Detail Topic that is aligned to the user via My Setup Products
    - Approved Email content access also adheres to the Veeva Detail Group functionality meaning a user will need to be aligned to the appropriate Detail Group – Detail Product/Topic data via My Setup Products to gain access to the content
- Standard Salesforce.com Security Model (Sharing rules) - Custom sharing rules can also be setup on the Approved_Document_vod object as an additional layer of restricted access. A special Territory field (Territory_vod) is delivered in the Approved Email solution which can be sourced from Vault specifically for usage in sharing rules defined in Veeva CRM.
- Restricted Products and Allowed Products functionality - Approved Email will respect the Restricted Products field on Account, and will not allow email to be sent for a Restricted product
    - Approved Email will respect the Allowed Products field on TSF
- VMobile Object Configuration - The VMobile Object Configuration record for Approved_Document_vod can be configured to filter Approved_Document_vod data sync to iRep

Managing Approved Email Consent for Accounts

Each account has some control over email being sent to them. Veeva CRM has a flexible consent model that supports both opt-in required and opt-in not required modes. The ability to designate existing Accounts as never being allowed to receive emails is also possible.

All emails generated by Approved Email include unsubscribe links that allow recipients to opt-out of future emails. Pre-existing content preferences can be loaded from external systems into Multichannel_Consent_vod.

Every Account can have a unique consent type. This allows a single org to apply different consent types to different Accounts. The common example is in multi-country orgs where countries have diverse consent requirements. In single-country orgs, there will typically only be one consent type that can be pre-defined using an Approved Email Setting (see below).

It's important to understand the difference between a consent type and a consent record.

Consent Types

The consent type determines if opt-in is required or if opt-in is not required to send email. It also determines if email should never be sent to an Account. Consent types include the following:

- Opt-in Required – An opt-in record is required prior to sending email
- Opt-in Not Required – An opt-in record is not required to send email
- Never Email – It is not possible to send email nor to opt-in (this option is only available when set on an existing Account)

Configure consent types in two ways:

- Account.Approved_Email_Opt_Type_vod – This picklist contains the consent type values listed above (the actual values are Explicit_Opt_in_vod,='Opt-in Required', Implicit_Opt_In_vod='Opt-in Not Required', Never_vod='Never Email'). When a value is set, this provides the most granular level of control for existing Accounts. This determines if an opt-in record is required or not. If your consent model is simple and straightforward, a NULL value is valid. When the value is NULL, the consent type is determined by the following Approved Email Setting.
- Approved Email Settings – The boolean setting Approved Email Opt-in Required (MULTICHANNEL_EXPLICIT_OPT_IN) determines the consent type. One value can be applied org-wide, for example Opt-In Not Required, or unique values can be applied to different security Profiles. The latter option allows users in one Profile to require an opt-in record, and users in another Profile to not require an opt-in record. The value of this setting is overridden by a non-NULL value in Account.Approved_Email_Opt_Type_vod.

Consent Records

The consent record is a specific instance of an opt choice, either opt-in or opt-out, stored within Multichannel_Consent_vod. A consent record has a create datetime and is valid for a unique Account and email address pair. Consent records can be loaded from external systems.

The Opt_Type_vod picklist contains two values that determine the consent record type:

- Opt_In_vod – An opt-in record exists for a unique Account plus email address. Emails (for all Products) can be sent to this Account and email address associated to the opt-in record. There will be one opt-in record for each opt-in action from the Approved Email Opt In user interface (or from external integration).
- Opt_Out_vod – An opt-out record exists for a specific Account, email address, and product triplet. Email cannot be sent to this Account, email address, and product associated to the opt-out record. There will be one opt-out record for each opt-out

event type. (There is a related Opt_Out_Event_type_vod picklist that determines the source of the opt-out:

- Clicking on an unsubscribe link
- The email address bounced
- The email recipient clicked the mark as spam button in their email client.)

Multichannel_Consent_vod records are a child of the Account. It is important to understand that consent records are associated to an Account and to a specific email address on the Account. The email address is stored in Multichannel_Consent_vod.Channel_Value_vod.

The following is an example of what happens when Opt-In is enabled:

1. Account Clinton Ackerman opts in to receive email.
2. An opt-in record is created in MultiChannel_Consent_vod with an opt-type of Opt-in.
3. Clinton Ackerman's email address that was opted-in is drclint@gmail.com. The Channel_Value_vod value is drclint@gmail.com.
4. The Rep is now able to use Approved Email to send email to Clinton Ackerman using drclint@gmail.com.

Note: If Clinton Ackerman has more than one email address, one opt-in record per email address is required prior to sending email for each address.

Consent Validation

When sending email, Approved Email consent validation works as follows:

1. Check the consent type for the Account:
   a. First evaluate Account.Approved_Email_Opt_Type_vod. When not NULL, determine the consent type picklist value (Opt-in Required, Opt-in Not Required or Never Email). When NULL, default to:
   b. Approved Email Settings – **Approved Email Opt-in Required** (MULTICHANNEL_EXPLICIT_OPT_IN). When selected, opt-in is required. When not selected, opt-in is not required.
2. When consent type = Opt-in Required :
   a. Look for opt-in records in Multichannel_Consent_vod.
   b. Look for opt-out records in Multichannel_Consent_vod that match the Product associated to the selected Email Template.
      - Opt-out records for an Account, email address, and Product are always respected, even when an opt-in record is found.
   c. When an opt-out exists, prompt the Rep that opt-in is required to send email to the Account, email address, and Product.
   d. When an opt-out does not exist (and an opt-in does exist) allow the rep to send email.
3. When consent type = Opt-in Not Required:
   a. Look for opt-out records in Multichannel_Consent_vod that match the Product associated to the selected Email Template.
      - When an opt-out exists, prompt the Rep that opt-in is required to send email to the Account, email address and Product triplet.

        - Emails are suppressed until a subsequent opt-in expires the existing opt-out record.
    b. If no opt-out record exists that match the Product associated to the selected Email Template, allow the rep to send email.

4. When a valid (un-expired) opt-out record is found, email cannot be sent. The user is alerted in the Approved Email UI, and is presented with the option to opt-in the Account and email address.

Configuring Email Opt-in User Experience

When configured to require opt-in, Approved Email will only send email to Accounts when a consent record of type opt-in is present in the Multichannel_Consent_vod object. When opt-in is not required, an opt-in record is not required (this also assumes an opt-out record does not exist).

There are two use cases where the end user will want to collect an Email Opt In from an Account:

- Opt-in is required for the Account, or for the security Profile assigned to the User
- An opt-out record exists for the Account and the goal is to expire the opt-out record so that the Account is now validated to receive email

Approved Email provides a user experience to allow end users to collect Approved Email opt-in records from Accounts. The user experience and data capture requirements for opt-in are configurable in two ways;

- Disclaimers and messaging displayed on the opt-in screen
- Validation behavior of the opt-in screen

There are two Veeva Messages displayed on the opt-in screens. The messages can be different for each security Profile, but the messages are identical for iRep and Online. Companies can edit these messages, provided they fit within the constraints of the message field.

- APPROVED_EMAIL_CONSENT_TEXT - Holds the message next to the check box to be shown on the opt in/out screen
- APPROVED_EMAIL_DISCLAIMER_REQUIRED – Holds the message on the screen about reading and understanding the consent disclaimer

Validation behavior is slightly different on iRep vs Online – iRep allows signature capture and Online does not. The tables below describe the configuration options and behavior. It is not possible to configure beyond what is described below. The fields in the tables are on the Multichannel_Consent_vod object.

To provide more granularity to the opt-in process types, different page layouts can be configured for different user Profiles. This controls how validations are processed.

Option 1:

iRep Behavior – Signature or Paper Consent ID are required (either one)
Online Behavior – Paper Consent ID is required

Page Layout Properties	*Signature_Datetime_vod*	*Signature_ID_vod*
Included on Page Layout	Yes	Yes
Required on Page Layout	Yes	No

Table 7: Option 1 – Opt-In

Option 2:

iRep Behavior – Signature capture possible but not required
Online Behavior – No data capture during opt-in

Page Layout Properties	*Signature_Datetime_vod*	*Signature_ID_vod*
Included on Page Layout	Yes	No
Required on Page Layout	No (note: changing to Y does not require signature)	n/a

Table 8: Option 2– Opt-In

Option 3:

iRep Behavior – Signature capture not possible. Paper Consent ID capture possible but not required.
Online Behavior – Paper Consent ID capture possible but not required

Page Layout Properties	*Signature_Datetime_vod*	*Signature_ID_vod*
Included on Page Layout	No	Yes
Required on Page Layout	n/a	No

Table 9: Option 3– Opt-In

Option 4:
iRep Behavior – Signature capture not possible. Paper Consent ID required.
Online Behavior – Paper Consent ID required

Page Layout Properties	*Signature_Datetime_vod*	*Signature_ID_vod*
Included on Page Layout	No	Yes
Required on Page Layout	n/a	Yes

Table 10: Option 4– Opt-In

Opt-in Processing in Multichannel_Consent_vod

When reps capture opt-ins using the Approved Email Opt-in user interface, Multichannel_Consent_vod processing is identical regardless of the consent type (Opt-in Required or Opt-in Not Required.)

- An opt-in record is created for the Account and email address pair, with a NULL expiration date
- All opt-out records for the Account and email address pair are expired
    - Opt-in allows reps to send email for all Products and content they are aligned to
- Prior opt-in records are expired. There is only zero or one active opt-in record

Opt-out Processing in Multichannel_Consent_vod

Approved Email always respects opt-out records that are not expired, for example Opt_Expiration_Date_vod is NULL. It is important to understand that an opt-out record validation applies in the following way:

- Account_vod - For a specific Account. Required.
- Channel_Value_vod - For a specific email address of the Account. Required.
- Product_vod – For a specific Product of type Detail. Required.
- Detail_Group_vod – For a specific Detail Group (optional, only relevant when using Detail Groups with Products)

For example, if Account Clinton Ackerman using drclint@gmail.com clicks the Unsubscribe link in an Approved Email that is aligned to the Product Cholecap, an opt-out record is created. All future Cholecap emails to Clinton Ackerman using drclint@gmail.com are suppressed (until the opt-out record is expired). Emails for other products, for example Restolar, are still sent.

Opt-out records are created in three ways. Optout_Event_Type_vod picklist describes the event that generates the opt-out.

- Recipient (Account) clicks the unsubscribe link in an Approved Email
- Email Engine generates an event that Approved Email interprets to be an opt-out
    - Email address ‘hard’ bounces (the receiving MX server responds with a hard bounce, typically after many retries, or the MX server does not accept for delivery)
    - Email is flagged as spam. The recipient must make a conscious action to press the ‘Spam’ button in their email client
- Custom data integration directly with Multichannel_Consent_vod

An opt-out record exists for a specific Account, email address and product. Email cannot be sent to this Account, email address, or product associated to the opt-out record. There will be one opt-out record for each opt-out event type. (There is a related Opt_Out_Event_type_vod picklist that determines the source of the opt-out:

- Clicking on an unsubscribe link
- The email address bounced
- The email recipient clicked the mark as spam button in their email client

Integrating External Consent Records into Multichannel_Consent_vod

It is possible to populate Multichannel_Consent_vod using dataloader or other integrations.

Each Multichannel_Consent_vod record requires the following values:

- Account ID
- Channel Value (the email address value)
- Record Type value must be set to Approved_Email_vod
- Opt_Type_vod (opt-in or opt-out)
    - When type = opt-out, the Product lookup must be populated and, optionally, Detail Group lookup

- When type = opt-out, optionally set an Event_Type_vod picklist value
- When type = opt-in, the Product lookup must be NULL. Product-level opt-in records are not supported.
- When type = opt-in, in order to be consistent with Approved Email consent logic, all existing opt-out records for the Account and Channel value must be expired by setting an expiration date

Approved Email Reports and Dashboards

A set of Approved Email reports and dashboards are delivered as examples. These are intended to be used as starting points for creating reports relevant to your organization.

Reports	***Description***
Bounced Email by Account	This report shows a list of all the emails that have bounced, corresponding email address and the account details are displayed as well. A filter is added in the report customization - Where status equals "Bounced". The list is further categorized by the Accounts.
Document Views By Product	This report summarizes the number of times a document was viewed. A filter is added in the report customization where Activity: Record Type equals "Document Activity". The documents are grouped by the product they are associated with.
Document Views By Product and ET	This report summarizes the number of times a document was viewed. A filter is added in the report customization where Activity: Record Type equals "Document Activity". The documents are grouped by the product they are associated with. It is further grouped by the email templates associated with those sent emails.
Email by Template	This report shows the various metrics on the email activities for the sent emails. Formula fields are added that perform various functions on the fields in Sent Email and Email Activity objects. This report is grouped by the product and further grouped by the approved document.
Send vs. Open Rate by Product	This report compares the open rate vs. the send rate for the emails sent for each of the products.
Open/ Click Rate by Product	This report summarizes the open and click rate for each product. This report is mainly used for the corresponding dashboard.
Sent Email by Account	This report summarizes the number of emails sent to each account. This report is grouped by Account Name and further grouped by the Account's Email address.
Sent Email by Month	This report summarizes the number of emails sent each month. It is grouped by Sent Date, which in turn is grouped by "Calendar Month".
Sent Email by Sender by Product and ET	This report summarizes the number of emails sent by each user. A filter is added Sent Email: Owner Name does not contain "Admin". This report is grouped by the sender's name, then grouped by the products and further grouped by the email templates.
Spam Reports by Product and ET	This report lists all the emails that were "Marked as Spam" by the recipients. It is further grouped by the products and the email templates associated with those emails
Unsubscribes by Template	This report lists all the emails that were unsubscribed to by the recipients. A filter is added in the report customization - Where status equals "Unsubscribed". It is further categorized by the product and the email templates associated with those emails
Vault Domain Views by Product	This report list the number of times a document associated by a product was viewed. A filter is added in the report customization where Activity: Record Type equals "Document Activity". This is further categorized by the different Vault IDs.
Dashboard Name	**Description**
Dashboard for Products	This dashboard is used for graphically representing the different activities associated with the sent emails. The three components of this dashboards are - Sent Email by Products, Document Views by Product and Open Click rate for Products. These components use the corresponding reports as their data source.
Sent Email by Month	This dashboard is used to graphically representing the number of emails sent

Reports	Description
	by all the users in any given calendar month. The data source for this dashboard is the report labeled 'Sent Email by Month'

Table 11: Reports and Dashboards