For Eloqua users, contacts that share an email address can be a bit of a headache. Each stored contact in Eloqua is identified by their email address, and with out-of-the-box functionality, Eloqua does not allow multiple contacts to be connected to the same email.

The CO Date Calculator Cloud App from 4Thought Marketing lets you perform date calculations within custom object programs. Users can add or subtract days, weeks, months, or even years from any date value and store the results in a CO record.

CO Regex Cloud App Documentation

Table of Contents

Purpose of the CO Regex Cloud App

There are situations where the values of certain fields need to be validated against specific Regular Expressions. This is where this Cloud App comes into play. With CO Regex Cloud App, It takes the value from a field in a Custom Object and applies a Regex expression, and then the result(s) goes to another selected Custom Object field(s). This Cloud App can validate a Regular expression, can split a field value into multiple fields based on Regular expression and also this can transform the value of a field based on Regular transform expression.

- **Validation**: The app can validate If a particular field has to meet certain format, in that case you have to select the “Validate” option in the “Regular Expression Type” and select one field, which will be updated the True or False values when a record is processed. For example the following regular expression validates that a text has the format of an email address: /^([^@s]+)@((?:[-a-z0-9]+.)+[a-z]{2,})$/i
- **Split**: The app can take the value from a field and split it into multiple fields using a Regular Expression. For example, for a field value like “10 VPs, 20 Directors, 40 SMEs.” If we need to split based on the digits with the following expression D+: The result will be:
    - 10 VPs
    - 20 Directors
    - 40 SMEs
- **Transform**: The app allows you to transform the value of a field and executes a Regex

transformation. For example with the following regular expression: .*(snot).* if the field value is “My network does not work.” The result will be ” not”

Regex examples
- https://medium.com/factory-mind/regex-tutorial-a-simple-cheatsheet-by-examples-649dc1c3f285

This document will show how this Cloud action can be used inside CO Based Program Canvas.

Set-up in Oracle Eloqua

Please follow these instructions to set-up this cloud action in your Oracle Eloqua instance.

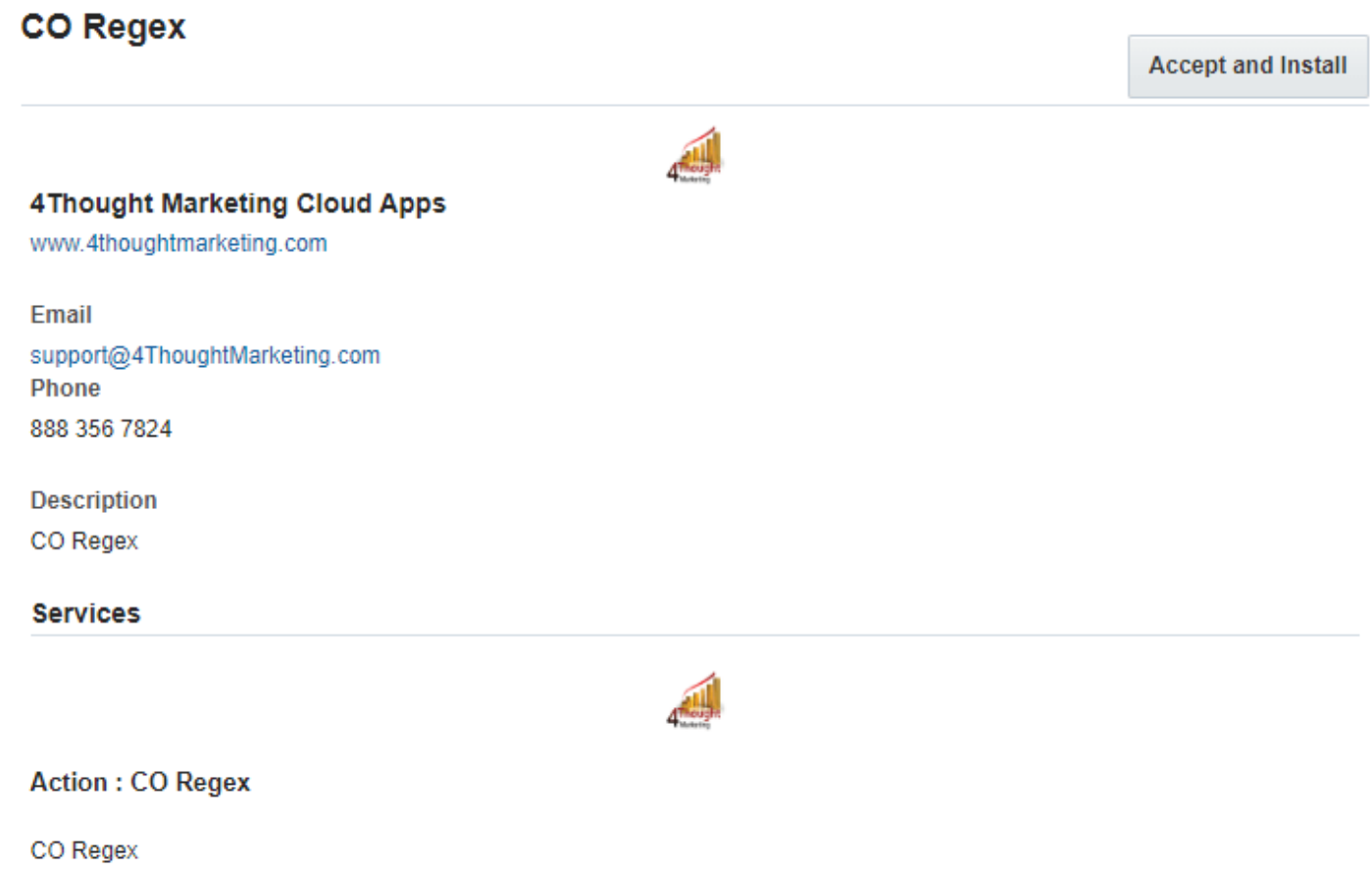
Please follow these instructions to set up this cloud app in your Oracle Eloqua instance.

- Log in to Oracle Eloqua.
- Click on Get App below to install.

Get app

NOTE: If prompted to log again, please do so.

- In the next screen, click “Sign In” and then “Accept”



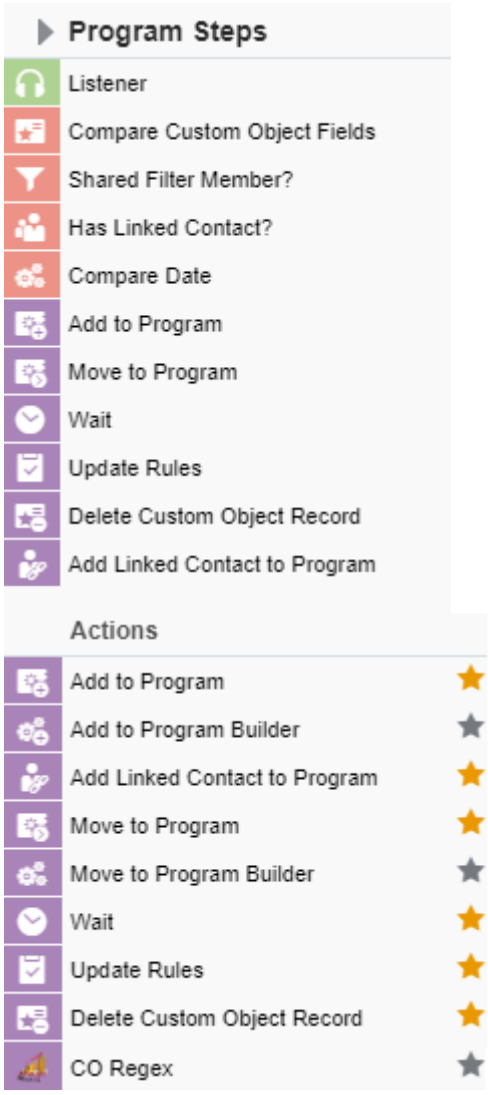
- In the next screen, click “Sign In” and then “Accept”

- You’re all set. The cloud action is ready to be used.

How to use

The following instructions show a basic/simple usage. You can incorporate this Cloud Action to any existing CO based Program Canvas.

- Create/Open a CO Program Canvas
- On “Program Steps” on the top left side then click arrowhead and then locate the “CO Regex” Cloud Action under the Actions options (colored in purple).



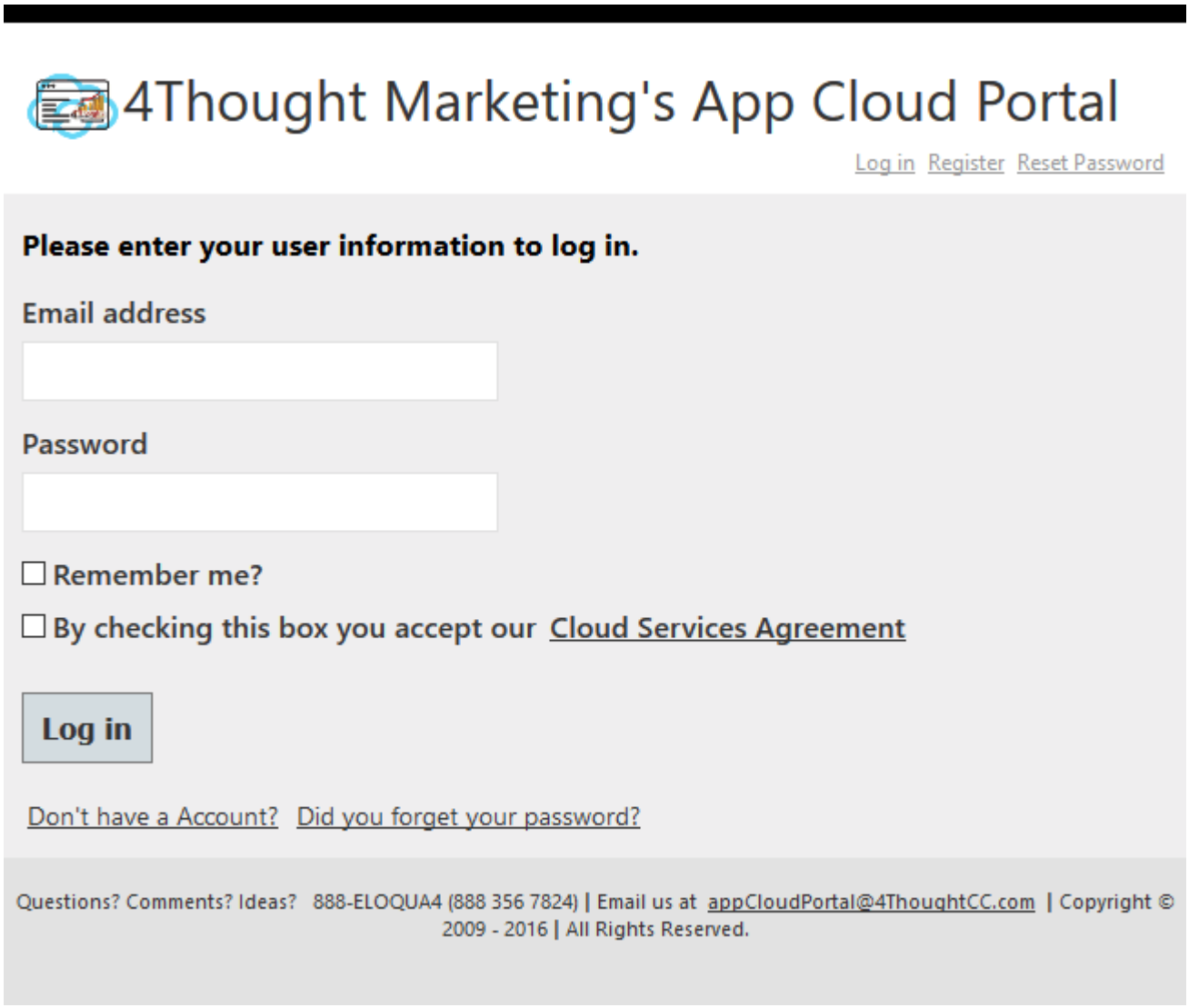
- Drag and drop the cloud action to the canvas area. Connect the corresponding elements to the dropped cloud action

- Double click the CO Regex step; you will see the configuration options for this element.
    - Rename the step if needed

- Click the pencil icon to open the settings for this step.

You will need a user to log in and configure this Cloud Action. If you don’t have one, you can create one.

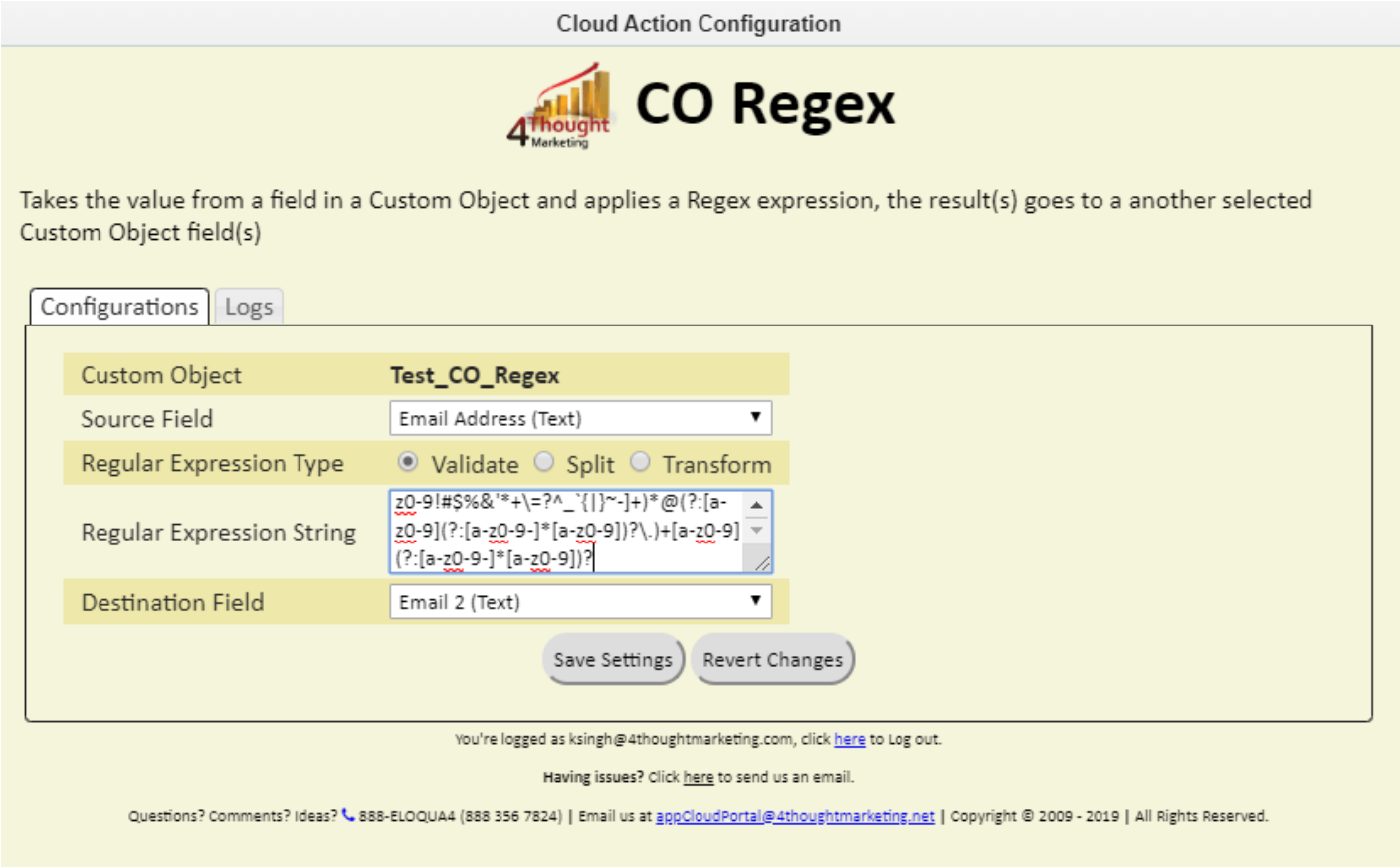
If you do, use your user to Log In in the page shown in the following screenshot:



- For this cloud action, you can perform 3 different actions (anyone at a time) on the CO set fields.

Validate

- Select CO set field as a source field, on which you want to perform action.
- Select **Validate** if you want that source field value meets certain format. in that case you have to select the “Validate” option in the “Regular Expression Type” and select one field, which will be updated the True or False values when a record is processed. For example the following regular expression validates that a text has the format of an email address: /^([^@s]+)@((?:[-a-z0-9]+.)+[a-z]{2,})$/i

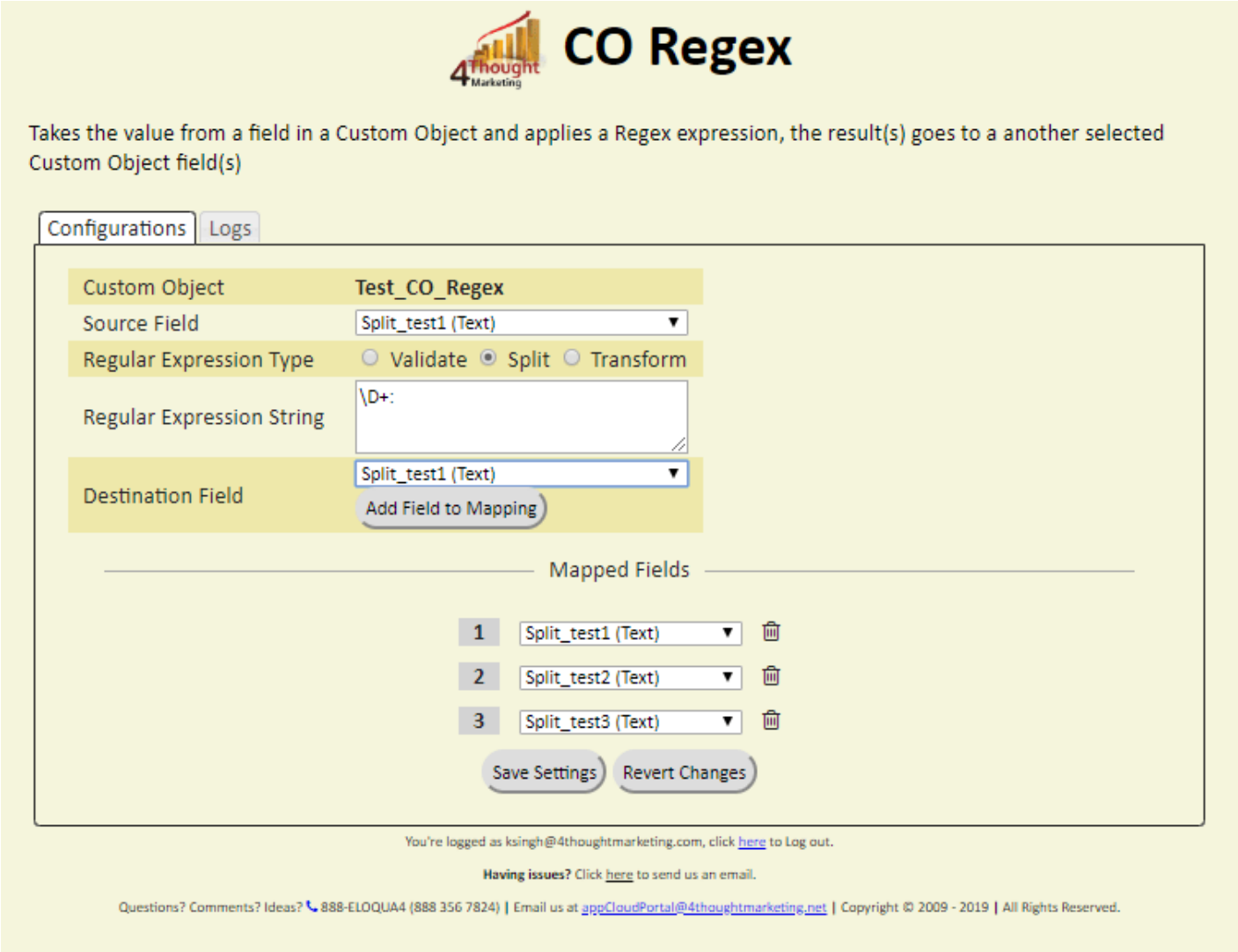


a. Select Source field Email address if you want to Validate Email address.
b. Check option Validate from the Regular Expression Type.
c. Write the Email validation Regular expression in the Regular Expression String.
d. Select destination field to store results and click on the Save Settings.

Split

a. Select **Split** if you want to split a specific field value in to different fields. This option can take the value from a field and split it into multiple fields using a Regular Expression. For example, for a field value like “10 VPs, 20 Directors, 40 SMEs.” If we need to split based on the digits with the following expression D+: The result will be:

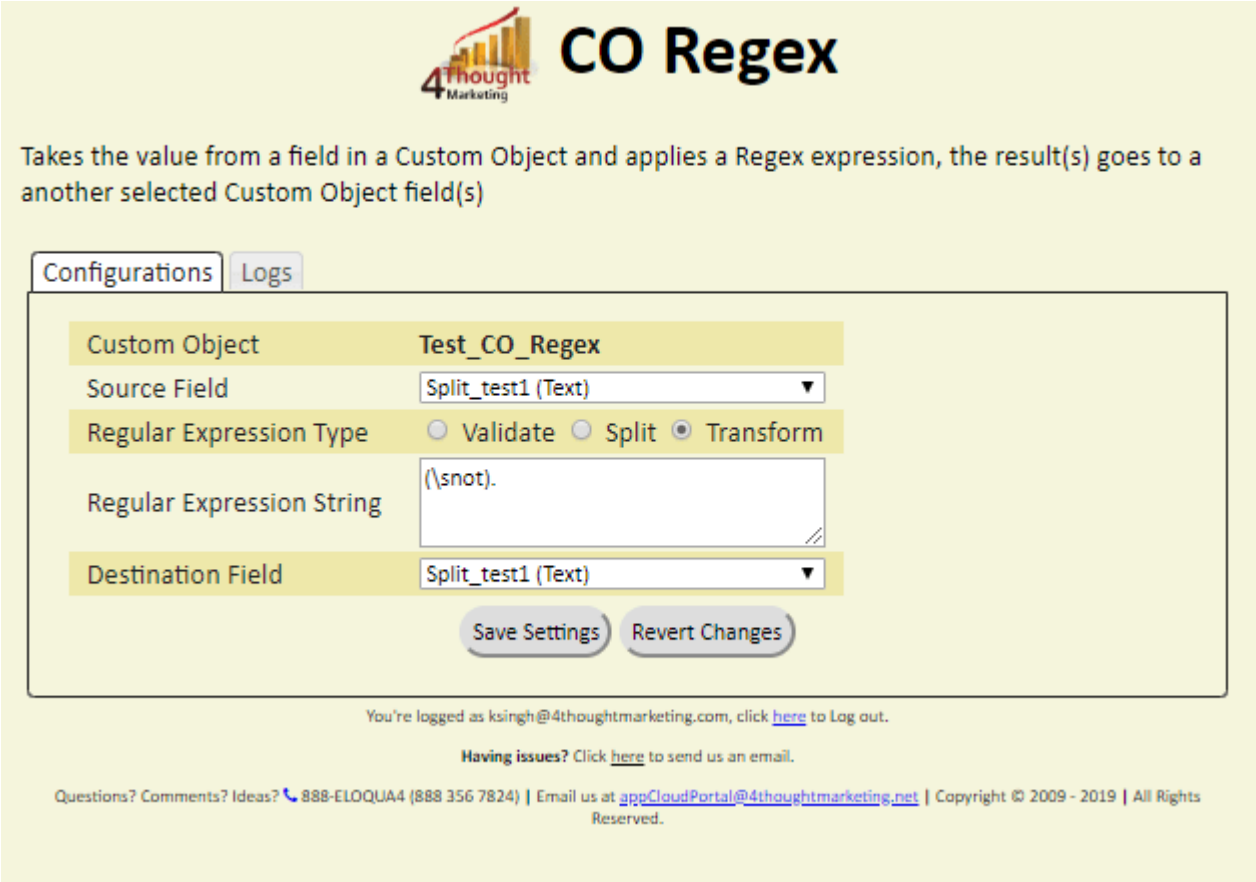
    - 10 VPs
    - 20 Directors
    - 40 SMEs



a. Select Source field for which you want to Split the values.
b. Check option Split from the Regular Expression Type.
c. Write the Split Regular expression in the Regular Expression String.
d. Select destination field to store results.
e. Click on the “Add Field to Mapping”. If there are more than 1 fields which will store the Split values then select destination field and click “Add Field to Mapping”. Finally click on the Save Settings to save the changes.

Transform

Checked the option **Transform** if you want to transform the value of a field and execute a Regex transformation.



a. Select Source field which needs to be transformed.
b. Check option Transform from the Regular Expression Type.
c. Write the Transform Regular expression in the Regular Expression String.

- When using the Transform expression type the Expression string must contain two lines:

The first line defines the matching elements.
The second line defines the output format.
This is an example of a phone formatter: (d{3})(d{3})(d{4})

($1) $2-$3

There is no need to use a delimiter.

a. Select destination field to store results and click on the Save Settings.

- Make sure you click on ‘Save Settings’ to save your configuration. If you make any changes you

can click on ‘Revert Changes’ to go back to the last saved configuration.

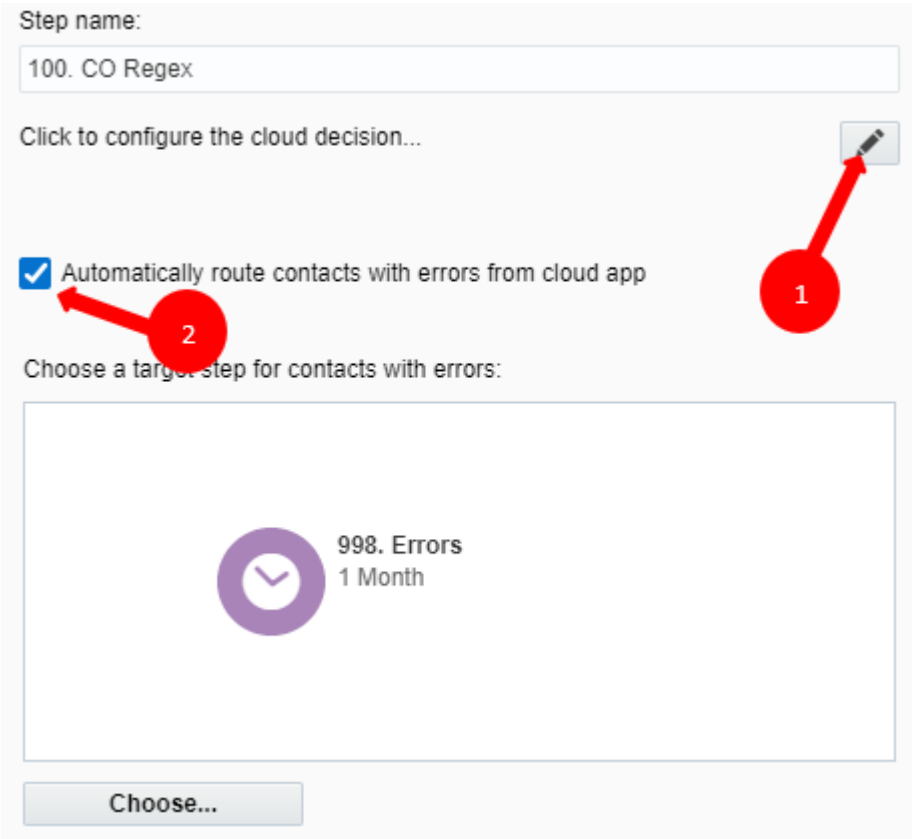
- **Logs Tab:** This section shows the execution logs for the cloud app

- **Show**: Here you can select what type of log you want to see. You have an option to select “All logs”, “Successful logs only”, “Failed logs only”
- **Within the following timeframe:** This field allows you to select the timeframe to view the execution logs.

Note: You can view up to 2 months of logs

- **Recommended**: Create an element in the campaign in case an error happens, in this example it’s a Wait Step. Check the box to “Automatically route records with errors from cloud app”, select the step where you want the records to be routed.

Select the Step where you want the records to be routed.



That’s all. Activate the campaign or program, put some records in it and see the CO Regex in action!

Note: *Most 4Thought Marketing apps use the Eloqua BULK API to export/import records, therefore when an app is used in a campaign or program the user that activates the campaign should have the following permissions:*

- *API*
  - *Consume API*
- *Contacts*
  - *Upload Contacts/Prospects/Companies*
  - *Manage Data Export*
  - *Manage Contacts*

License Information

You need a license to configure and execute this Cloud App. If you don’t have a license, an error message will appear on the configuration page.

If you don’t see CO Records being processed by the app, it may be because your license is missing or expired. To obtain a license, contact your account manager or contact us.

- Each Eloqua instance requires a separate cloud app license.
- Each cloud app license includes a reasonable usage limitation of 250k records processed daily and up to 5 app instantiations per Eloqua instance. Higher usage tiers are available at extra cost.
- For additional license details, please review the Cloud Services User License Agreement.

Oracle Eloqua Upload Wizard Demo Video

Oracle Eloqua Upload Wizard

The Oracle Eloqua Upload Wizard allows you to let more people perform Eloqua uploads, without compromising or being concerned about data quality.

With this app, your data will be verified as clean, before it enters your Oracle Marketing Cloud database. Plus, you can tie the uploaded contacts to shared lists, campaigns, external activities and even CDOs!

Call us at 888-ELOQUA4 (888-356-7824) or email us at info@4ThoughtMarketing.com

https://www.youtube.com/embed/JUuAKq144P0

First Name *

Last Name
*

Email Address
*

Company
*

Title

country

Please select country*

stateProv

Please select state/region

☐
I give consent for 4Thought Marketing to Process my data

Submit

Social Media Campaign Attribution in Eloqua

Learn how to ascribe leads, opportunities, and revenue to specific social media campaigns using Eloqua.

In this video, we explain how to track social media campaign engagement of unknown visitors so that once they become known, you can accurately:

- Understand which platforms work best
- Measure their ROI
- Take corrective measures

https://www.youtube.com/embed/d_T71J4nBvg

We fed 400 real form submissions to AI and let it sort the spam, vendors, and leads. The results were not what we expected.

Is your marketing tech stack actually earning its keep? Learn how to scrutinize marketing tech stack ROI, identify underperforming tools, and recover hidden value with a structured Martech audit approach.

AI marketing data hygiene is the foundation that determines whether your AI pilots deliver results or amplify chaos. Most teams skip data cleanup, chase new tools, and wonder why ROI never materializes.

We’re diving into Eloqua Signature Rules and how to remove Bulk Export dependencies with n8n. See real-world examples and leave with ideas you can implement right away.

4Thought Marketing Incident Response Plan

Table of Contents

Security Policy Home

Last Update:

November 17, 2025

Introduction

Following industry ‘best practices’ and to comply with numerous compliance regulations, 4Thought Marketing has implemented various procedures, policies, and guidelines to protect the confidentiality, integrity, and availability (CIA) of its critical client data and computing resources. This Incident Response Plan is a procedural document to prepare our team to address such security incidents. Regular testing and refinement of this plan will help 4Thought Marketing prepare for adverse security incidents and ultimately help us to manage and minimize risk.

It may be appropriate to use this plan in conjunction with 4Thought Marketing's Disaster Recovery Plan, which can be found at <Path Redacted for Public> for internal use or as a link at www.4ThoughtMarketing.com/Trust.

It is anticipated that as new technologies and requirements are introduced, this document will need to be modified and should be reviewed at least annually. Members of the security team will perform this function at the direction of the Chief Security Officer.

Note that at 4Thought Marketing, our "DPO" or Data Privacy Officer (a requirement of GDPR) is the same role/person as our Security Officer.

Plan Overview

Many security incidents can occur with assorted severity levels, and not all incidents require focus on each step. However, it is essential to be prepared and understand that typically different phases exist in responding to an incident, as well as the goals and objectives of each phase. The various phases of a security incident response plan at 4Thought Marketing are as follows:

- Prepare
- Identify
- Contain
- Eradicate

- Recover
- Review
- Notification

Prepare

In preparing for security incidents, several items need to be addressed.

- The incident handling team should include our security officer, system analysts from our TMAS team, and, depending on the type of data lost, human resources personnel.
- End users and analysts should be trained at an appropriate level. Login banner and warning messages should be posted.
- Contact information is included as an appendix to this document and should be available in hard copy for:
    - Personnel who might assist in handling an incident
    - Key partners who may need to be notified
    - Business owners to make key business decisions

    - Outside support analysts with security expertise

- Backups should be taken and tested!

- Supplies to assist the team in the event of an incident (sometimes referred to a jump bag)
    - An empty notebook (Thorough documentation should be done throughout an incident to include hand written notes in a fresh notebook.)

    - Boot CDs to analyze hard drives and recover passwords

    - Petty cash (food, cabs, batteries as needed)

Identify

Awareness of a security incident can originate from different sources, such as technical people, end users, or even clients.

Best practices suggest declaring an incident has occurred when security officers sense an adverse risk to the company and then assembling the team and implementing the plan. It is also suggested that multiple people be involved early on, that all key system files or records, such as log files, be saved, and that detailed documentation be started as soon as possible.

Ultimately, business owners need to be involved in many security incidents to decide what the goals of handling a particular incident are, such as immediate business recovery or forensic examination.

Contain

Following basic procedures can prevent many incidents. Specific guidelines will frequently depend on the nature of the incident, as well as the direction of the business owner. Remember that a compromised machine might not present valid data! Basic steps to consider include:

- Obtain and analyze as much system information as possible including key files and possibly a backup of the compromised machine for later forensic analysis.

- Powering off a machine might lose data and evidence. Preferably disconnecting the LAN cable facilitates containment and forensic activity. (Putting the computer on a separate network with a network analyzer might help analyzing network activity)

- If one machine has been exploited others might be vulnerable. Actions that might need to be taken on a large scale might include:
    - Download security patches from vendors
    - Update antivirus signatures
    - Close firewall ports
    - Disable compromised accounts

    - Run vulnerability analyzers to see where other vulnerable hosts are ■ Change passwords as appropriate

Eradicate

To eradicate the problem specific procedures will frequently depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

- Boot CDs should be used to access data on compromised machines. (Rootkits installed on compromised machines might affect basic system level utilities and discourage use of a compromised host)
- If machines OS has been compromised it needs to be rebuilt using hardened machines on appropriate platforms
- Test any backups prior to restore and monitor for a new incident.
- Document everything.

Recover

The recovery phase's goal is to return safely to production. Once again specific actions might depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

- Retest the system preferably with a variety of end users.

- Consider timing of the return to production.
- Discuss customer notification and their concerns
- Discuss media handling issues
- Continue to monitor for security incidents

Review

This phase allows 4Thought Marketing to better handle future security incidents. A final report should describe the incident and how it was handled using the Incident reporting form. This report should also include suggestions for handling future incidents and reworking this document.

Notification

Notification of breaches is limited to violations of PII (Personally Identifiable Information) unless such information is encrypted with a reasonable expectation that such encryption will not be breached. A breach of PII shall be treated as “discovered” as of the first day on which such breach is known to the organization.

Notification does not necessarily occur at the end of the above processes but will typically occur in parallel with them and at many stages, depending on who is being notified and the geographical impact.

- **Internal Notification** o This occurs typically as soon as breach awareness or even possible breach awareness occurs.

- **Impacted Customer & Partner Notification** o Within 4 business hours of discovery or sooner if possible, upon confirmation of impact to a customer or partner

o If Individuals of customers are impacted, it is the sole responsibility of the customer to notify those individuals

- **EU DPO Notification** of Announcement to Data Privacy Authorities of GDPR Countries required within 72 hours of discovery to comply with GDPR Article 33

- **Notification of Individuals**
    - Notification to EU Citizens shall comply with Article 34 of GDPR

    - Announcements to other individuals based on geographical legal requirements

    - (As previously mentioned) If customers are impacted, it is the sole responsibility of the customer to notify those individuals

- **General / Public Announcement** as and when determined appropriate by marketing, customers, and ETeam.

Notification Content:

The notice shall be written in plain language and must contain the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the PII fields that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known;
- Any steps the Customer should take to protect Customer data from potential harm resulting from the breach.
- A brief description of what 4Thought is doing to investigate the breach, to mitigate harm to individuals and Customers, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which may include our 800 number, an e-mail address, a web site, or postal address.

Notification Methods:

4Thought Customers will be notified via email or phone or both within the timeframe for reporting breaches, as outlined above.

Incident Logging

Incident logging shall occur within the standard applicable security logs and the standards applicable and documented for those logs shall apply.

Roles and Responsibilities

Task/Responsibility	Assigned To:	Notes
Identify & Contain Breach	Head of TMAS	
Communicate Breach	CSO & CEO	For EU as per GDPR (Within 72 Hours to DPO as per Article 33, and to Data Subjects as per Article 34)
Eradicate Breach	Head of TMAS	
Recover & Restore	Resources assigned by Head of TMAS	
Review	Security Team (CEO, CSO, Head of TMAS)	
Document Post Mortem	CSO	
Notification -Internal	CSO	
Notification -External	Head of Mktg	

Contact Information for Incident Response Roles

Role	Contact Information
CEO	<Redacted for Public Version>
CSO*	<Redacted for Public Version>
Head of TMAS	<Redacted for Public Version>
Head of Marketing	<Redacted for Public Version>

*Includes GDPR mandated role of DPO

<End Incident Response Plan of 4Thought Marketing>