

# Red Herring

## Google Quick Start





## Table of Contents

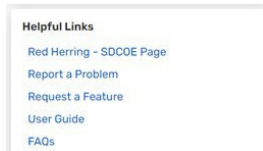
Helpful Resources .....	2
List of IPs and Custom Domains used with Red Herring .....	2
Configuration.....	2
County Office of Education (COE) Admins .....	3
Local Education Agency (LEA) Admins .....	3
Settings .....	4
Google Gmail Allowlist, Gateway & Spam Rule.....	4
Sender Policy Framework (SFP) - Optional.....	7
Google Service Account .....	8
Enable Admin SDK for Service Account in Google Cloud Console .....	11
Grant Access for Service Account in Google Admin .....	12
Trust Red Herring as an OAuth App.....	13
Upload JSON and Sync Target Users into Red Herring.....	13
Create Red Herring User Group.....	14
Configure LEA Branded Settings .....	14
Clone a Red Herring User Email Template.....	15
Send a Test Phishing Campaign.....	15




## Helpful Resources

For comprehensive cybersecurity information, the San Diego County Office of Education (SDCOE) Cybersecurity webpage offers multiple valuable resources. Visit the page at [SDCOE Cybersecurity](#).

The Red Herring Dashboard provides convenient links to essential resources, including the Cybersecurity page, the Service Now help desk system, the Red Herring User Guide, and FAQs. Access the dashboard at [Red Herring Dashboard](#).



In-page help is also provided and can be accessed by navigating to the page where you need help and clicking the question mark icon at the bottom right of page. 

The inline help page will close when you browse away from the current page. The inline window can be expanded to its own browser tab to keep it open for further reference.

## List of IPs and Custom Domains used with Red Herring

To ensure smooth operation and prevent emails from being flagged as phishing or moved to the target user's quarantine inbox, the following IP addresses and domains may need to be allow-listed on your email protection service:

192.40.172.4, 192.40.172.139, 20.118.176.15, 20.118.176.58, 20.118.176.59

Generic Domains	Generic Domains	Regional Domains
aditisecurity.com	edufinancial.org	countyofsd.net
ctateachers.net	edupointonline.com	sandiegocoe.net
highunion.net	glooglonline.com	sdcoe.net
schoolunified.net	gmailonline.us	sdcoes.net
servicecounty.net	infinite-campus.org	sdcounty.net
uniondistrict.net	microsoftsupport.us	sfcoe.org
	peoplesoftsdcoe.com	sfusds.net

## Configuration

The configuration section of the Red Herring platform provides comprehensive instructions for setting up and customizing the system to align with your organization's needs. This section covers configurations for both county offices of education and local education agencies (LEAs). It details how to input organization information and upload logos to create branded templates specific to your LEA. By following the steps outlined, administrators can ensure that the Red Herring platform is effectively tailored to their educational environment, enhancing both usability and security.



## County Office of Education (COE) Admins

COE admins are able to access the Red Herring portal and perform admin activities at the COE level, such as creating and editing Agency (LEAs), adding and editing COE/LEA admins, and viewing COE reports. An admin's email address is only allowed to be assigned to one COE and additionally to one LEA.

COE admins will first have to create an LEA for their organization so that they can send phishing campaigns to their staff. After adding a COE admin to an LEA they'll have to re-login to see the change.

1. Navigate to Agencies (LEAs)
2. Click +Create Agency
3. Fill in the LEA information
  - a. Only assign the necessary number of licenses to the LEA
  - b. Expiration date can't be set passed your COE's expiration date
4. Click Create
5. Click the Admins button next to agency and assign admins to it (see LEA Admins)

## Local Education Agency (LEA) Admins

Agency admins are able to access the Red Herring portal and perform actions according to their admin level. An admin's email address is only allowed to be assigned to one LEA. After adding a COE admin to an LEA they'll have to re-login to see the change.

We currently have three LEA admin levels

- Admin - full admin and can add/modify other admins
- Template Admin - can create and edit templates for Emails, Landing Pages, and Knowledge Assessments
- Campaign Admin - can schedule and modify simulated phishing campaigns, as well as view the campaign results

**Note:** When you create an admin, they are sent a welcome email along with a link to set their password. If they do not set their password within 24 hours, you will have to click the Confirm Email button to send them another email request to set their password.

- Create Admin - This will assign an admin to the Agency (LEA)
- Reset Password - This will send the admin an email requesting that they reset their password
- Confirm Email - This button shows if the admin has not yet clicked on the link in their Welcome Email to set their password; clicking it will send them a new welcome email

Confirm Email



## Settings

The Settings page has three sections; Profile, Notifications and Excluded Times.

### Profile

This is where you can input your organization’s information and logos so that they will automatically appear on any of Red Herring’s LEA Branded templates. Simply enter your agency’s details and click save. You may use the attribute variable on any template that you create or modify.

The available text fields are:

Name	Attribute	Notes
Organization Name	{orgname}	
Organization Website	{orgwebsite}	
Organization Acronym	{orgacronym}	
Help Desk Name	{helpdeskname}	
Help Desk Website	{helpdeskwebsite}	
Help Desk Phone Number	{helpdeskphone}	Only numbers are allowed
Help Desk Email	{helpdeskemail}	

The available logo/images are:

Name	Attribute	Notes
Rectangular Logo	{rectangularlogo}	
Square Logo	{squarelogo}	
Text logo	{textlogo}	
Preferred Background Image	{backgroundimage}	Will only work for Landing Page templates

## Google Gmail Allowlist, Gateway & Spam Rule

The following directions will guide you through the process of setting up an allowlist and configuring the Email Gateway in Gmail. This ensures that simulated phishing emails from Red Herring are not flagged as phishing or moved to the user’s quarantine inbox. By completing these steps, you will ensure that your phishing training emails are successfully delivered and recognized by your Gmail system.

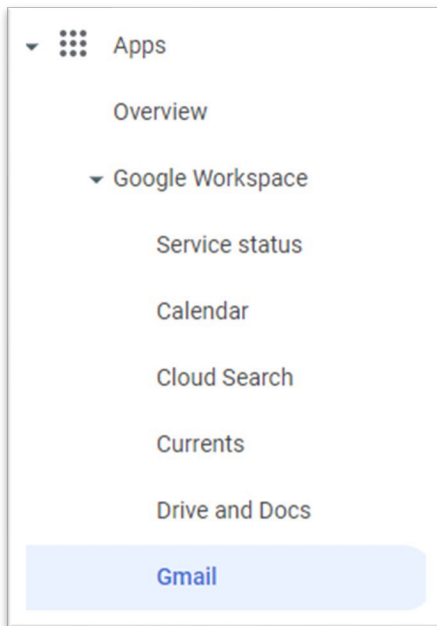
In Google Admin go to Apps > Google Workspace > Settings for Gmail > Spam, phishing, and malware

<https://admin.google.com/ac/apps/gmail/spam>

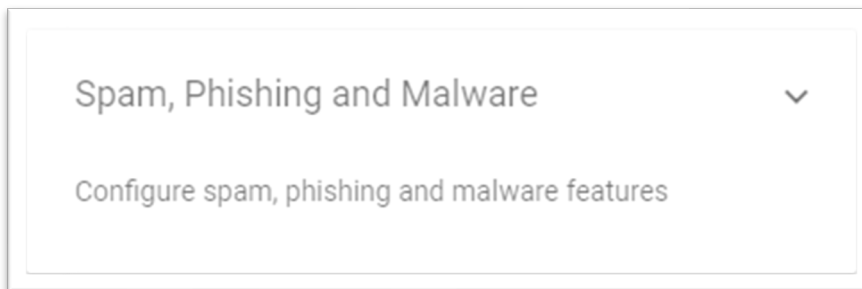
1. From the main menu first expand the **Apps** menu



2. In the Apps section expand **Google Workspace** and then select **Gmail**

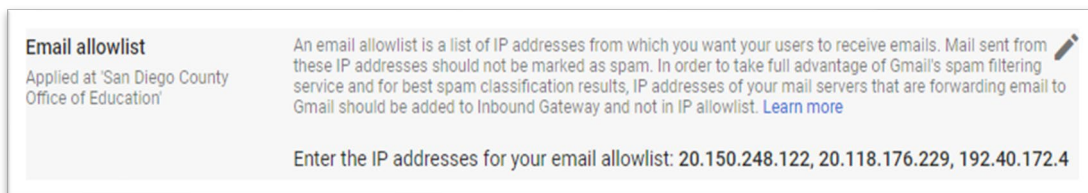


3. Scroll to the bottom of **Settings for Gmail** and select **Spam, phishing, and malware**



4. Under **Email allowlist** enter the following IP addresses separated by commas:

192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.59, 20.118.176.15

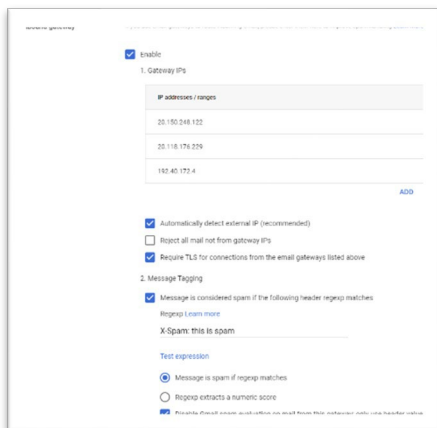


5. Next find **Inbound gateway** and select **Configure** or **EDIT**





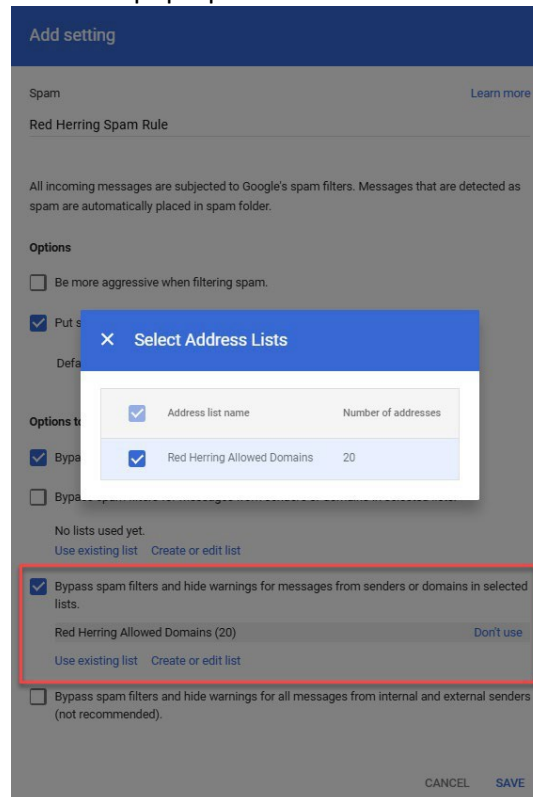
6. In the Inbound gateway settings
  - a. Enter a short description: Red Herring email gateway
  - b. Add the following gateway IPs  
192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.59, 20.118.176.15
  - c. Check **Automatically detect external IP**
  - d. Check **Require TLS for connections from the email gateways listed above**
  - e. Check **Message is considered spam if the following header regexp matches**
    - i. Enter a false statement that won't trigger: **X-Spam: this is spam**
    - ii. Choose the radio for **Message is spam if regexp matches**
    - iii. Check **Disable Gmail spam evaluation...**
  - f. Click **Save** or **Add Setting**



7. Lastly, find the **Spam** section and you can either edit your existing rule or click **CONFIGURE** to add your first spam rule.
  - a. Name the rule: "LEA's Spam rule"
  - b. Select the options based on how your organization wishes to handle spam.  
Best practice is to check **Put spam in administrative quarantine** and to **Bypass spam for internal senders**. (Ignore this step if you're adding a dedicated spam rule for just Red Herring in addition to your existing organizational spam rule.)
  - c. Under **Options to bypass filters and warning banners**, check the box for **Bypass spam filters and hide warnings for messages from senders or domains in selected lists**.
    - i. Select **Create or edit list**
    - ii. On the new browser tab that opens, select **ADD ADDRESS LIST**
    - iii. Name it "Red Herring Allowed Domains"
    - iv. Click **BULK ADD ADDRESSES**
    - v. Add the domains that you plan to use in your Red Herring simulated phishing campaigns:  
aditisecurity.com, edufinancial.org, countyofsd.net, ctateachers.net, edupointonline.com, sandiegocoe.net, highunion.net, glooglonline.com, sdc0e.net, schoolunified.net, gmailonline.us, sdcoes.net, servicecounty.net, infinite-campus.org, sdcounty.net, uniondistrict.net, microsoftsupport.us, sfcoe.org, peoplesoftsdcoe.com, sfusds.net, sdcoe.net
    - vi. Check **Require sender authentication**



- vii. Click **ADD**
- viii. Click **SAVE**
- ix. Return to the previous browser tab
- x. Select **Use existing list** and check the box for “Red Herring allowed Domains”
- xi. Close the pop-up window then select **SAVE**



8. Return to Red Herring > Configuration > SMTP and enter `aspmx.l.google.com` for server name, 25 for port number, check SSL box, and leave username and password blank. Then click update and check your Gmail Inbox for an email from [noreply@sdcoe.net](mailto:noreply@sdcoe.net).

## Sender Policy Framework (SPF) - Optional

Sender Policy Framework (SPF) is a crucial email authentication protocol that helps prevent email spoofing and enhances email deliverability. These directions are only needed if you plan to use Red Herring to impersonate your organization’s email domain.

Add the following IP statements before the ~all statement of your SPF record on your DNS nameserver.

`ip4:20.118.176.15 ip4:20.118.176.58, ip4:20.118.176.59`

After you update your SPF records, we recommend that you send yourself a test phishing email that spoofs your domain. If you have successfully added Red Herring to your SPF record, the email should not go to your Spam folder or be flagged as malicious.



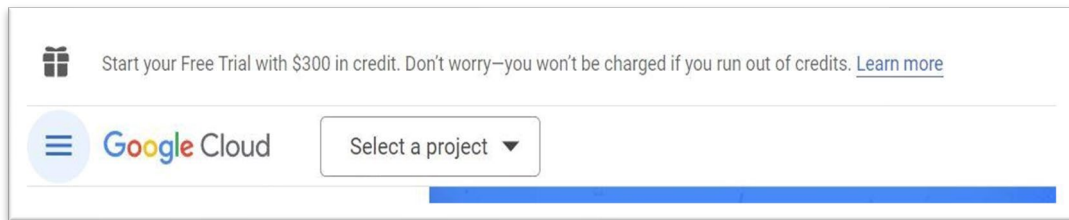
## Google Service Account

These directions will set up a Service Account in Google Cloud and Google Admin to allow you to import target users into Red Herring.

1. Go to <https://cloud.google.com/> and login with your Google Admin Account
2. Click Console to go to the Console Page



3. Select APIs and Services
4. On the top panel click **Select a project**



5. Create a **New Project**



6. Choose your Organization and Location

Project name \*  
Red Herring

Project ID: red-herring-380916. It cannot be changed later. [EDIT](#)

Organization \*  
[Redacted]

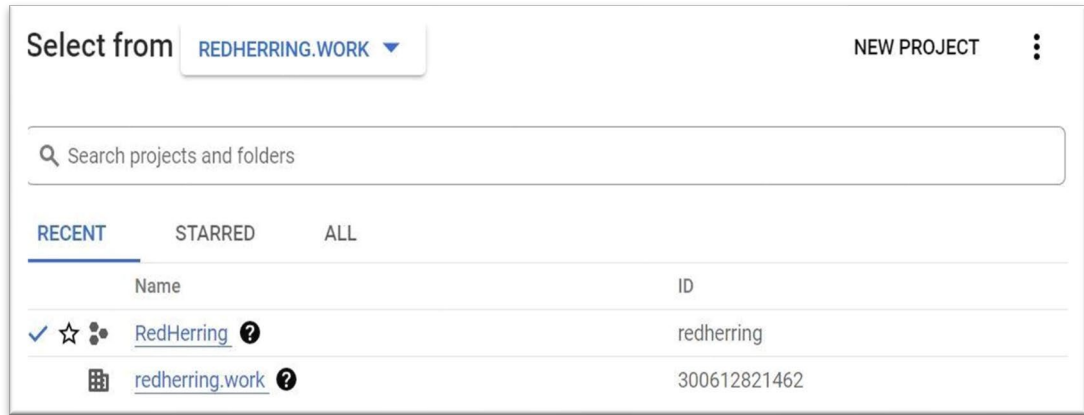
Select an organization to attach it to a project. This selection can't be changed later.

Location \*  
[Redacted] [BROWSE](#)

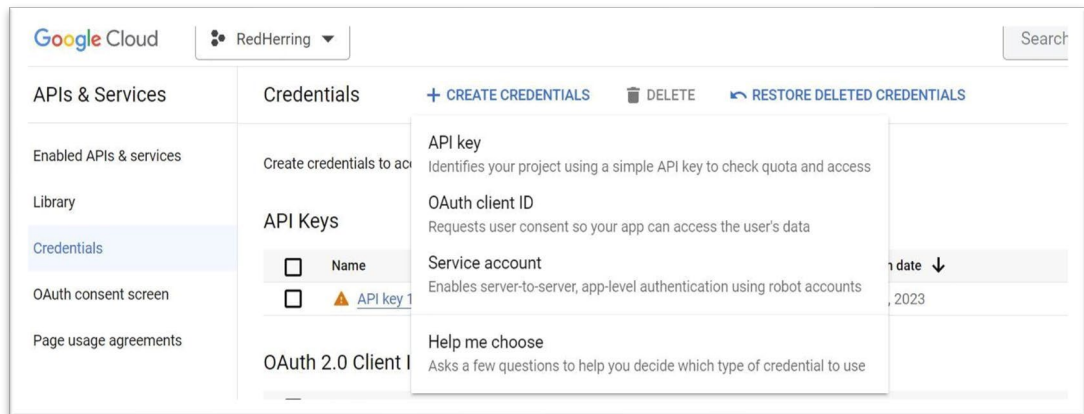
Parent organization or folder

[CREATE](#) [CANCEL](#)

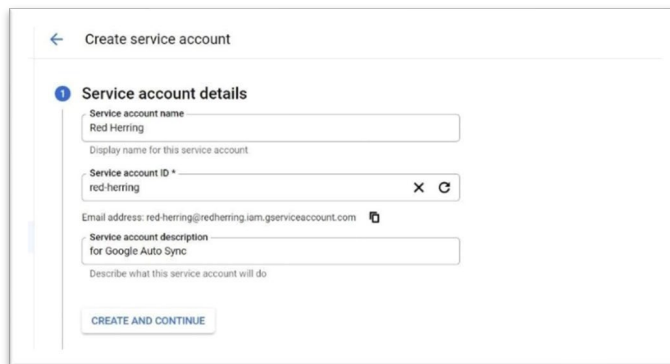
The project could take a while to complete. When the project is ready, it should be listed under your organization.



7. Select the project then click the Credentials menu on the left
8. In the Credentials page, click “+Create Credentials” and select **Service account**



9. Input Service Account Information and click **Create and Continue** then accept the defaults and select **Done**



10. After creating the service account, take note of the Unique ID from Details tab of the Service Account page  
Google Cloud > Service Accounts > IAM &Admin > Service Accounts > {Red Herring Service Account}



The screenshot shows the 'Service account details' page for 'Red Herring'. The 'Unique ID' field is highlighted with a red box and contains the value '103357592147226208308'. Other fields include 'Name' (Red Herring), 'Description' (for Red Herring user auto-sync), and 'Email' (red-herring@red-herring-sync.iam.gserviceaccount.com).

11. Go to the **Keys** tab of Service Account page and select **Add Key > Create new key**

The screenshot shows the 'Keys' tab of the 'Red Herring' service account page. The 'ADD KEY' button is highlighted with a red box. Below the button is a table with columns: Type, Status, Key, Key creation date, and Key expiration date. The table currently shows 'No rows to display'.

12. For key type choose "JSON"

The screenshot shows the 'Create private key for "Red Herring"' dialog. The 'JSON' radio button is selected under 'Key type'. The 'CREATE' button is highlighted with a red box.



13. After successfully creating, the JSON key will automatically download to your computer (Please keep the JSON safe because you won't be able to download it again)

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).  
[Learn more about setting organization policies for service accounts](#)

ADD KEY ▾

Type	Status	Key	Key creation date	Key expiration date
	Active	[REDACTED]	Mar 17, 2023	Dec 31, 9999

## Enable Admin SDK for Service Account in Google Cloud Console

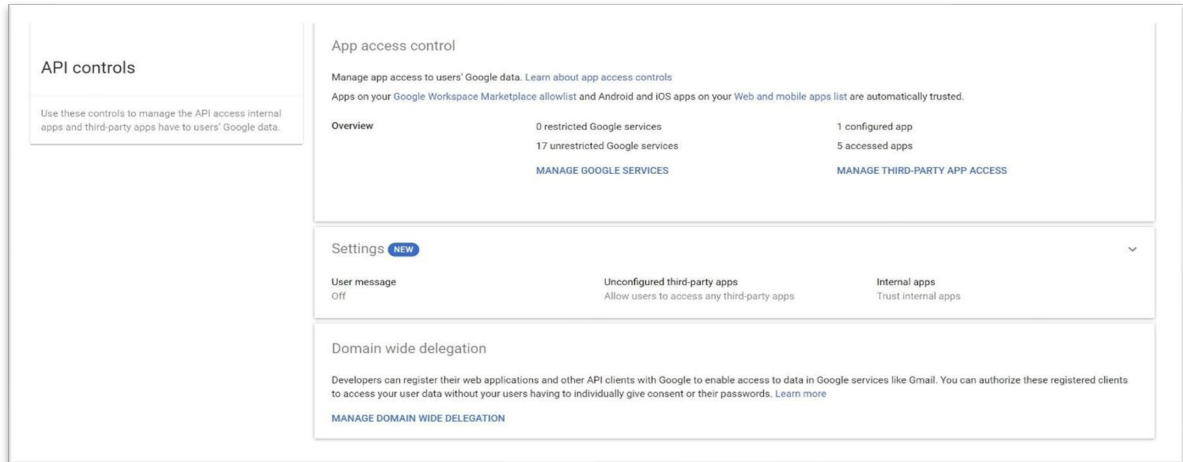
1. Go to <https://console.cloud.google.com/> and login with your Google Admin Account
2. Select APIs and Services > Library
3. On the top panel make sure your sync project is selected from top-left dropdown.
4. Search for Admin SDK API and click on its tile
5. **Enable** the Admin SDK API

The screenshot shows the Google Cloud Console interface. At the top, there is a navigation bar with the Google Cloud logo and a dropdown menu for the project 'Red Herring Sync'. Below this, a breadcrumb trail shows 'Product details'. The main content area displays the 'Admin SDK API' with its logo, the text 'Google Enterprise API', and a description: 'Manage Google Workspace account resources and audit usage.' At the bottom of the card, there are two buttons: 'ENABLE' and 'TRY THIS API'.



## Grant Access for Service Account in Google Admin

1. Go to Google Admin (<https://admin.google.com>) and login with Google Admin Account
2. Go to Security > Access and data control > API controls
3. Click **Manage Domain Wide Delegation**



4. Click **Add new** to add new scope for your service account key
5. Input the service account Unique ID (In Service Account Detail page) and the 4 scopes would be:

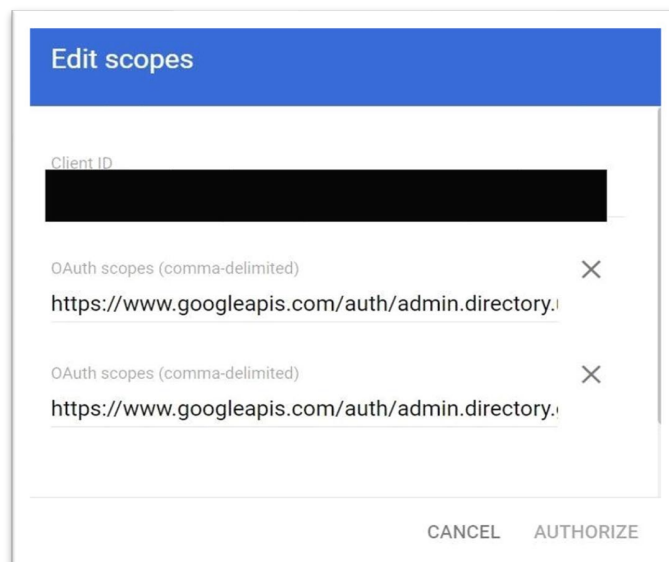
<https://www.googleapis.com/auth/admin.directory.user>

<https://www.googleapis.com/auth/admin.directory.group>

<https://www.googleapis.com/auth/admin.reports.audit.readonly>

<https://www.googleapis.com/auth/admin.reports.usage.readonly>

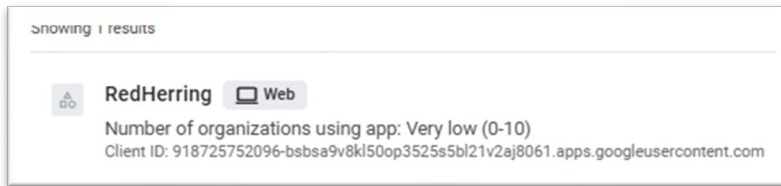
6. Then click **Authorize**





## Trust Red Herring as an OAuth App

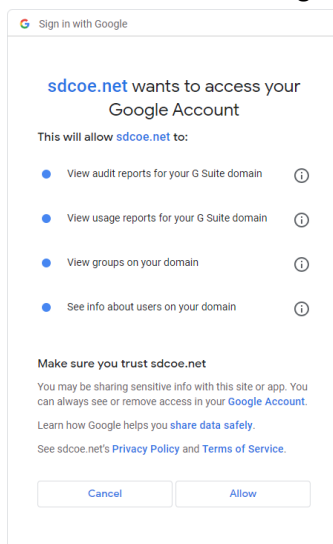
1. Go to Google Admin (<https://admin.google.com>) and login with Google Admin Account
2. Go to Security > Access and data control > API controls
3. Click **Manage App Access**
4. Click **Configure new app**
5. Select **OAuth App Name or Client ID** if prompted
6. Search for:  
918725752096-bsbsa9v8kl50op3525s5bl21v2aj8061.apps.googleusercontent.com
7. Click **RedHerring**



8. Select All Users and press **Continue**
9. Select the **Trusted** radio button and press **Continue**
10. Review the settings and press **Finish**
11. Wait 5-10 minutes for the changes to propagate and proceed with next page  
(Ensure you're logged out of the Red Herring console before proceeding)

## Upload JSON and Sync Target Users into Red Herring

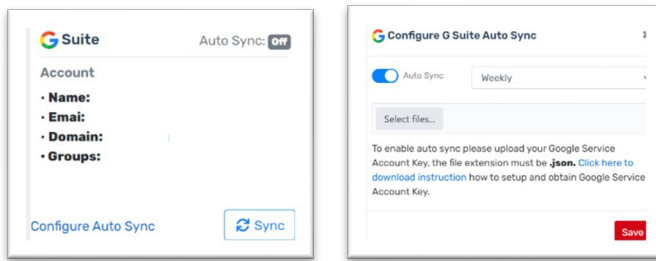
1. Log into a fresh web browser instance of Red Herring
2. Navigate to Red Herring > Configuration > Directory
3. Select **+Add new** and login to G-Suite with an Admin account



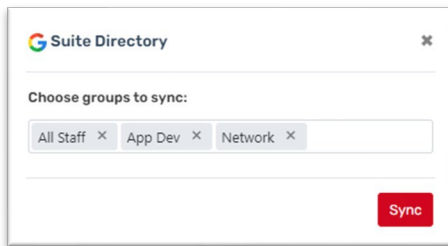
4. **Allow** sdcoe.net access to sync your users
5. On the G-Suite sync tile select **Configure Auto Sync**



- Slide the toggle switch for Auto Sync and choose your sync frequency
- Upload the .json file and **Save**



- On the G-Suite sync tile select **Sync**
- Choose the groups that you want to synchronize and press **Sync**



## Create Red Herring User Group

Red Herring has 5 Risk Score (High risk, Medium High Risk, Medium Low Risk, Low Risk, and No Risk Score) groups that are automatically populated with your target users, based on their interactions with Red Herring campaigns. You may use any or all of these groups in your simulated phishing campaigns. We recommend that you create a group for testing purposes to ensure the templates are formatted correctly and that spam prevention is bypassed.

- Navigate to Red Herring > Groups
- Select **+Create Group**
- Name the group **Testing**
- Optionally create another group for **All Staff**

## Configure LEA Branded Settings

Once you enter your agency's details here, the information will automatically appear on any of the templates that have the **#LEA Branded** tag.

- Navigate to Red Herring > Configuration > Settings  
<https://redherring.sdcoe.net/Admin/settings>
- Enter your organizational information under Agency Details
- Upload your organizational logos under Agency Images
- Click Save Profile



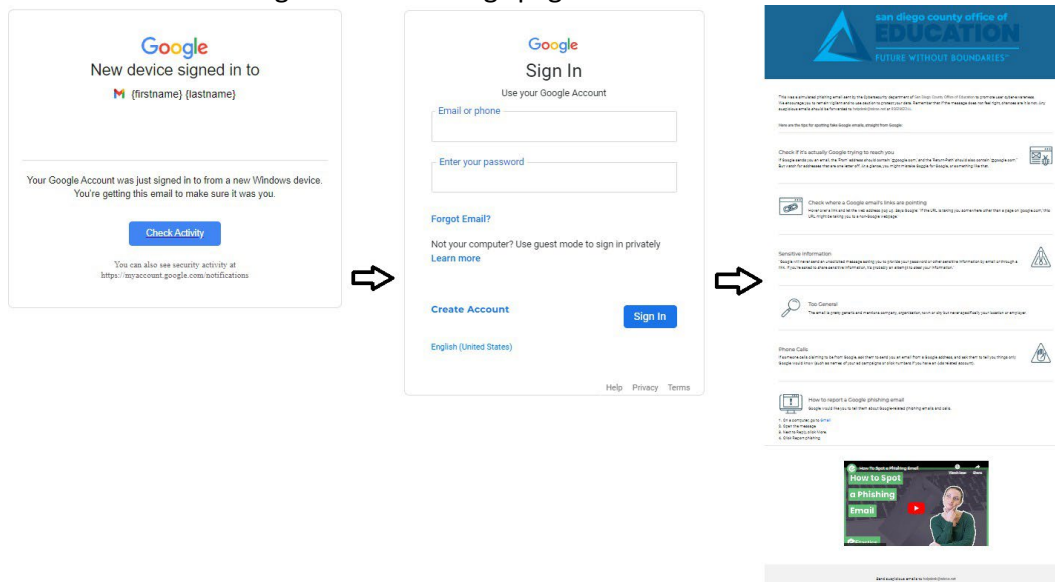
## Clone a Red Herring User Email Template

1. Navigate to Red Herring
  2. Search for Google or any keyword in the top-right search bar
  3. Navigate to Red Herring > Emails > **+Shared with Me**
  4. In the Filters box, click **Deselect all** and then check the box for **Email Templates**
  5. Find a template that you like and clone it to your Default folder  
(a visual example of email to landing page click-path is viewable on the next page)
  6. Optionally, you may check the box for Landing Page Templates and clone them if you would like to customize them.
- NOTE: You will have to edit the link in the email template and point it to the Landing Page that you customized.

## Send a Test Phishing Campaign

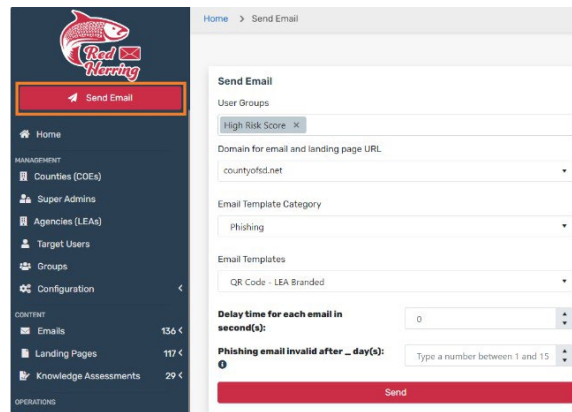
We suggest that you use the Send Email menu item for testing your email templates to ensure that spam prevention measures are bypassed, email and landing pages display nicely, and that telemetry works. For telemetry we track email clicks, landing page views, data entered in login fields, video views, and knowledge assessment results. Deleting the email campaign from the Emails Sent menu item will remove any negative Risk Score for clicking on links in that email campaign.

We suggest that you use the Campaigns menu when sending simulated phishing campaigns to your staff. All the Google email templates are configured to point to a cloned Google Login page, if the target user enters their login credentials and clicks the Login button, they will be redirected to an LEA Branded user awareness page to help them better identify phishing emails and websites. Your logo and organization will automatically appear on the user awareness page if you have configured the items in the Configuration > Settings page.

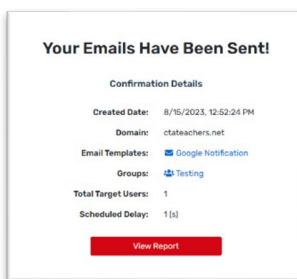




1. Navigate to Red Herring > Send Email
  - a. For User Groups select your Testing group
  - b. Choose one of the custom domains such as cteachers.net
  - c. For Email Template Category select your Default category
  - d. Select the email to send
  - e. Phishing Email Invalid After \_ day(s): This setting determines how long the simulated phishing link in email will be valid for. Once link has expired, link clicks will no longer be tracked, and the target user will be redirected to a static Red Herring page
  - f. Delay time for each email in second(s): This setting will insert a # second delay between each email as they are sent from our email server
  - g. Click the red Send button



2. Find the email in your inbox
  - a. Click on any links in the email and landing page
  - b. Fill out any form fields
  - c. View video if present
  - d. Complete Knowledge Assessment if present
3. Click on View Report or Emails Sent and then view the Campaign Report for the email you just sent





4. Verify telemetry shows in the email campaign report
5. Delete the Email once the test is completed
6. Schedule a department/division/all-staff campaign by navigating to Campaigns > **+Create New Campaign**
  - a. Here is an example of a quarterly campaign that will randomly send a different email once every quarter with the simulated phishing link valid for 3 days for each quarterly campaign

**Campaign Detail**

Campaign Name\*  
Quarterly All-Staff

User Groups\*  
High Risk Score × Medium High Risk Score × Medium Low Risk Score ×  
Low Risk Score × No Risk Score ×

Domain for email and landing page URL\*  
ctateachers.net

Email Template Category\*  
Credential Harvesting ×

Email Template\*  
Google Password Reset × Google Security Alert ×  
Google - Shared File (Google Docs) × Google Meet Invitation ×

Frequency\*  
Every 3 months

Start date\*  
05/06/2024 09:07:15 AM

End date\*  
05/06/2025 10:00:00 AM

Phishing Email Invalid After \_ day(s)\* 3      Delay (Seconds) 1

[Save](#)      [Back To Campaign List](#)

7. Contact [cyberguardians@sdcoe.net](mailto:cyberguardians@sdcoe.net) if assistance is needed.