

Red Herring User Guide

Version 7.1.1 | Updated January 29, 2024

| | |
|---|-----------|
| Overview | 3 |
| What is Red Herring? | 3 |
| Navbar Functions | 4 |
| Concepts and Terminology | 5 |
| Helpful Resources | 6 |
| Configuration | 6 |
| List of IPs and custom domains used with Red Herring | 6 |
| Admin Accounts | 7 |
| Settings | 8 |
| SMTP | 10 |
| Sender Policy Framework (SPF) - Optional | 10 |
| SMTP for Office365 | 11 |
| SMTP for Gmail | 12 |
| Google Gmail Allowlist & Gateway | 13 |
| Google Service Account | 15 |
| Microsoft 365 App Access | 22 |
| Microsoft 365 Allowlisting | 28 |
| Target Users | 32 |
| Add Target Users Individually | 32 |
| CSV Upload | 34 |
| On Premise Active Directory Sync | 35 |
| Azure User Sync | 37 |
| Google Sync | 46 |
| Groups | 48 |
| Create a Group | 48 |
| Assign Target Users to the Group from the Groups page | 49 |
| Assign Target Users to a Group from the Target Users page | 50 |
| View Group Analytics | 51 |
| Landing Pages | 52 |
| Create a New Category | 52 |
| Rename/Delete a Category | 52 |
| Create/Edit a Landing Page Template | 53 |
| Edit the Landing Page Body | 53 |
| Special Buttons: Landing Page Template Editor | 54 |
| Shared Landing Pages (Public) | 55 |
| Clone a Shared Landing Page | 55 |
| Email Templates | 56 |
| Create a New Email Templates Category | 56 |
| Rename/Delete a Category | 56 |
| Create/Edit an Email Template | 57 |
| Edit the Email Body | 58 |
| Special Buttons – Email Template Editor | 58 |
| Test an Email Template | 59 |
| Shared Email Templates (Public) | 60 |
| Clone an Email Template | 60 |
| Knowledge Assessments (Quizzes) | 61 |
| Create/Modify a Quiz | 61 |
| Designing a Quiz | 62 |
| Phishing Campaigns (Scheduled) | 63 |
| View Your Campaigns | 63 |
| Create a New Phishing Campaign | 64 |
| Excluded Time | 65 |
| Send a Phishing Email (Ad Hoc) | 66 |
| View your Emails Sent | 67 |
| Reports and Analytics | 68 |
| Campaign Results Report | 68 |
| District Report | 69 |
| Support | 70 |
| Report a Problem | 71 |
| Request Something | 72 |
| Sending a Test Campaign | 73 |
| Enable Google Less Secure Apps | 76 |

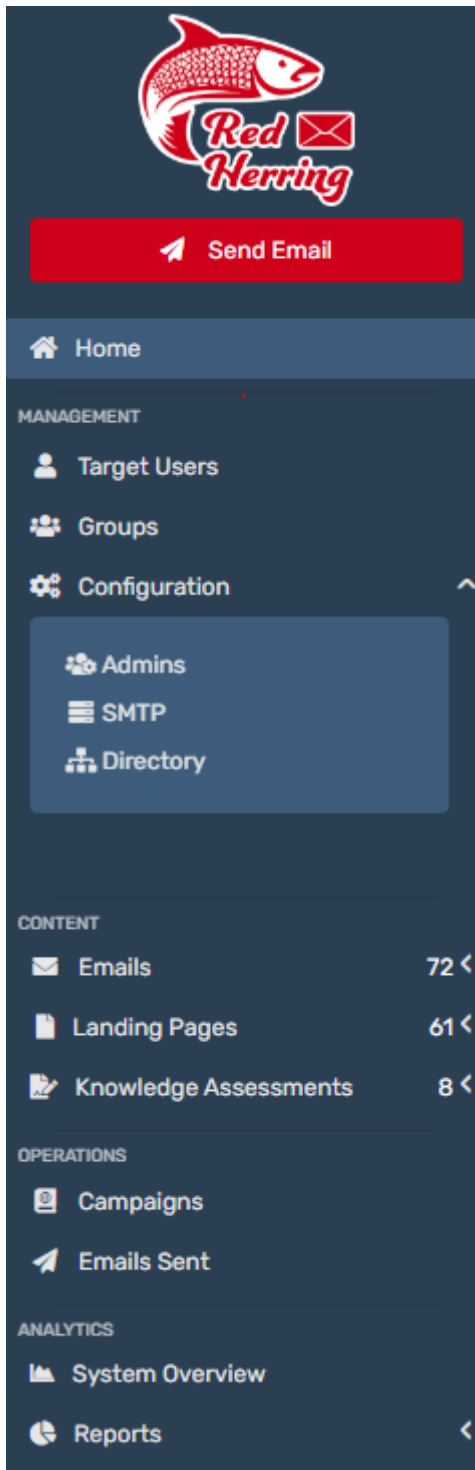
Overview

What is Red Herring?

Red Herring is a system developed by the San Diego County Office of Education (SDCOE) to promote cybersecurity awareness. It also enables an organization to identify employees who need additional cybersecurity awareness training related to identifying phishing emails.

Computer users are often cited in the cybersecurity industry as the weakest link to an organization's information security posture. An organization can easily increase its users' awareness through randomly conducted Red Herring simulated phishing campaigns along with the implementation of an annual cybersecurity-awareness training program.

Navbar Functions



Please see the next page for explanations of the key functions.

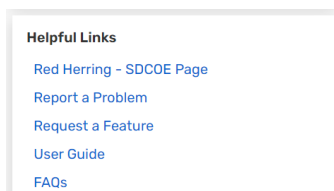
Concepts and Terminology

- **SMTP:** In order to send mail using your domain name, Red Herring will need access to your SMTP mail server. Otherwise, you may send mail using our custom domains without having to configure SMTP.
Details start on p.6.
- **Target Users:** The recipients to your phishing emails are defined in the Target Users section. There are five ways you can add target users to Red Herring: adding individually, CSV upload, on-premise Active Directory sync, Azure sync, and Google G-Suite sync. *Details start on p.32.*
- **Groups:** Red Herring is designed to only send emails to groups and not individual users, although a group can have just one person. *Details are on p.48.*
- **Landing Pages:** When a user clicks on a link in one of your phishing messages, they are sent to a landing page. The URL to the landing page includes identifiers that enable Red Herring to track which users click on phishing messages. You can create Landing Page Categories, which act like folders to help you organize similar landing page templates. *Details start on p.50.*
- **LEA Branded:** Any Landing Page or Email template that is tagged as LEA Branded will automatically display the custom information and images that you have configured in **Configuration > Settings**
- **Email Templates:** Email templates are the phishing emails that will be sent to your users. You can create Email Templates Categories, which act like folders to help you organize similar email templates. *Details start on p.56.*
- **Phishing Campaigns:** A phishing campaign sends the Email Template to a group of users at a scheduled time. When you set up the campaign, you can add one or more user groups, one or more email template categories, and one or more email templates. NOTE: If you add multiple email templates to a campaign, Red Herring will send each user a randomly selected email template from the ones you selected. *Details start on p.63.*

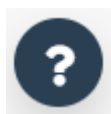
Helpful Resources

The public SDCOE Cybersecurity webpage has multiple helpful resources that can be found at [HTTP://cybersecurity.sdcoe.net](http://cybersecurity.sdcoe.net)

The Red Herring Dashboard has links to the Cybersecurity page, Red Herring User Guide, FAQs, and the Service Now help desk system. <https://redherring.sdcoe.net/Home/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 for further reference.



Configuration

List of IPs and custom domains used with Red Herring

These IP addresses and domains may need to be allow-listed on your email protection service to prevent them from being flagged as phishing or moved to the target user's quarantine inbox.

192.40.172.4, 192.40.172.139, 20.118.176.15, 20.150.176.58

| Generic Domains | Regional Domains |
|-------------------|------------------|
| aditisecurity.com | countyofsd.net |
| ctateachers.net | sandiegocoe.net |
| highunion.net | sdcoe.net |
| schoolunified.net | sdcoes.net |
| servicecounty.net | sdcounty.net |
| uniondistrict.net | |

Admin Accounts

COE Admins

COE or super 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 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 amount of licenses to the LEA
 - b. Expiration date can't be set pass your COE's expiration date
4. Click **Create**
5. Click the Admins button next to agency and assign admins to it (see LEA Admins)

LEA Admins

Agency admins are able to access the Red Herring portal and perform actions according to their admin level. An 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:

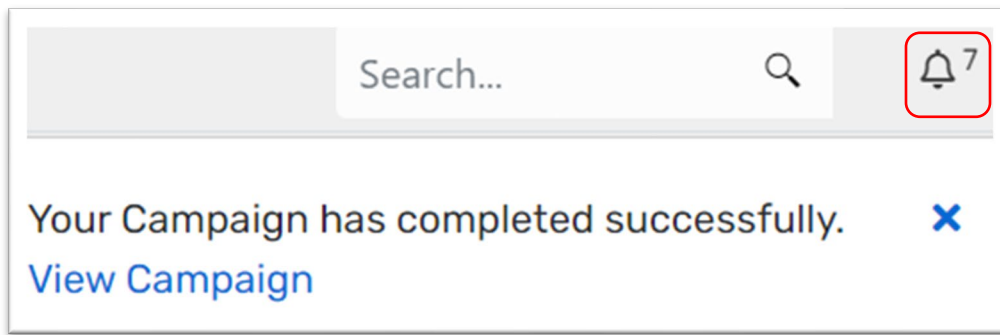
| Name | Attribute | Notes |
|------------------------|-------------------|--------------------------|
| Organization Name | {orgname} | |
| Organization Website | {orgwebsite} | |
| Organization Acronym | {orgacronym} | |
| Help Desk Name | {helpdeskname} | |
| Help Desk Website | {helpdeskwebsite} | |
| 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 | {rectangularlogo} | |
| Text logo | {textlogo} | |
| Preferred Background Image | {backgroundimage} | Will not display as background image in emails |

Notifications

Opt-in or opt-out of receiving certain notifications from Red Herring. There are two types of notifications, Email and System (Bell); the system notifications are accessible by clicking on the bell icon in the top right corner after logging in. Notification frequency can be set for Weekly, Bi-weekly, Monthly, or Quarterly.



Campaign Notifications

Email

Notify me when a Campaign has run Successfully

Notify me when a Campaign has Failed

Account Notifications

Notify me 2 months before my Account Expiration

Content Notifications

Notify me when when new Email Templates are made publicly available

Notify me when when new Landing Page Templates are made publicly available

Notify me when when new Knowledge Assessments are made publicly available

Excluded Times

Excluded Times can be used to pause any campaign that is in progress during a chosen time-frame. This can be used when sending a campaign to a large number of users to prevent emails from being sent after work hours. Or you may set an excluded time for a planned system outage or maintenance window.

The option to add an excluded time is also available from the Campaigns Page:

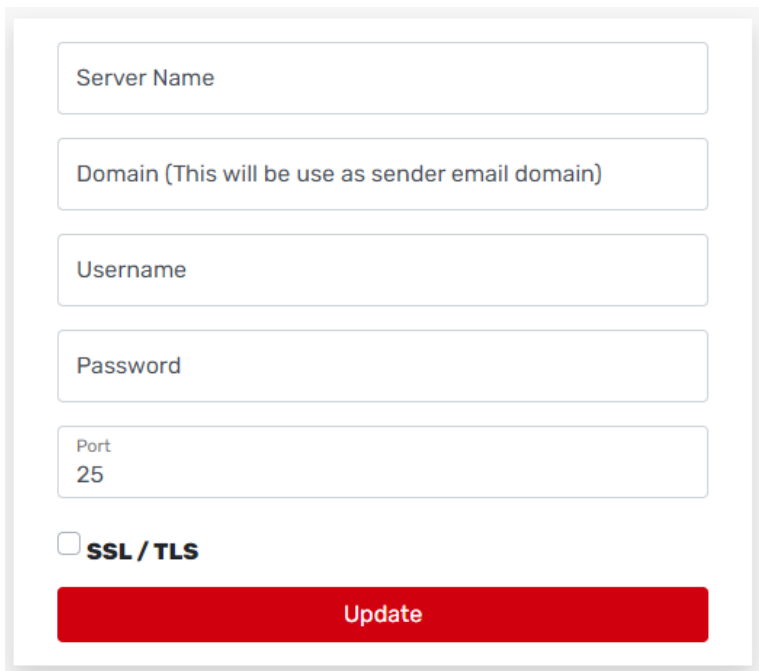
Campaigns > Excluded Time

1. Click the +Add Exclusion Time to create a new exclusion period.
2. Give it a name, Start Date and End Date
3. Select whether the whole day will be excluded or just part of the day.
 - a. For Partial Day choose the timeframe to be excluded.
4. Select whether you would like to exclude the selected timeframe daily or weekly.
 - a. For Weekly, select the day of week to the selected timeframe.
5. Use the dropdown to exclude All campaigns from running during the Excluded Time or a specified campaign.
6. Click Create

SMTP

In order to send mail using your domain name, Red Herring will need access to your SMTP mail server. Otherwise, you may send mail using our custom domains without having to configure SMTP.

1. Navigate to **Configuration > SMTP**.
2. Enter the **Server Name** (fully qualified domain name of your SMTP server), Domain, **Username**, **Password**, **SMTP port number**, and whether you use **SSL** encryption.

A screenshot of a web form for SMTP configuration. The form is enclosed in a light gray border. It contains five input fields: 'Server Name', 'Domain (This will be use as sender email domain)', 'Username', 'Password', and 'Port' (with '25' entered). Below the 'Port' field is a checkbox labeled 'SSL / TLS'. At the bottom of the form is a red button labeled 'Update'.

3. Click **Update**.
4. Check your Inbox for an email from noreply@sdcoe.net.
5. Click the confirm link with-in email.
6. Now test the connection. Refer to *Send a Phishing Email (Ad Hoc)* on p.66.

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

After you update your SPF records, we recommend that you send yourself a test phishing email that spoofs your email 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.

SMTP for Office365

OPTIONAL: Configuration of SMTP is optional and is not necessary in Red Herring. Phishing emails will be sent using our custom domains selectable from the Send Email or Create a Campaign menu items. Configuration of SMTP is only needed in order to send a simulated phishing campaign using your organization's email domain name in the sender's address.

First complete the steps in the **Office365 App Access** section and return here once complete.

1. Login to Red Herring with an admin account that has the same email address that you will be using to connect to Office365.

The image shows two side-by-side panels. The left panel, titled 'Office365 User', contains a form with the following fields: 'Server Name' (smtp.office365.com), 'Username' (scoe-herring@scoe.net), 'App Password', and 'Port' (587). There is a checkbox for 'SSL / TLS' which is checked, and a red 'Update' button at the bottom. The right panel, titled 'Red Herring Admin User', shows a user profile for 'scoe-herring@scoe.net' with the role 'Admin' and district 'County Office of Education'. A 'Logout' button is also visible. A red dotted arrow points from the 'Username' field in the Office365 User form to the email address in the Red Herring Admin User profile.

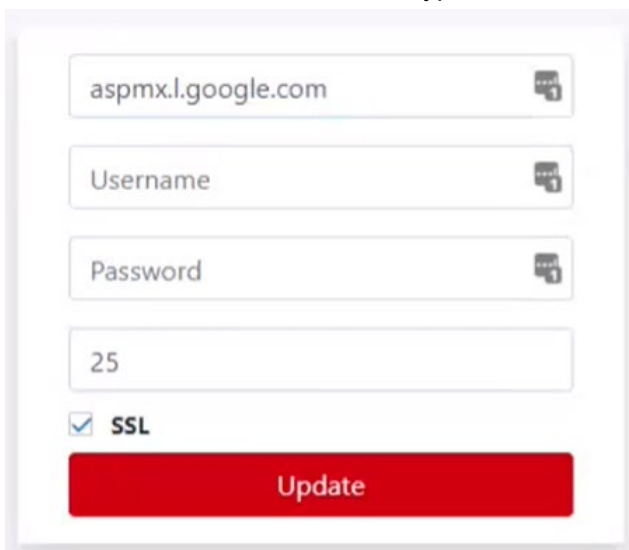
2. Navigate to **Configuration > SMTP**.
3. Enter the **Server Name** (smtp.office365.com), **Username**, **App Password**, **587** for **SMTP port number**, and check the **SSL** encryption box.
4. Click **Update**.
5. Check your Inbox for an email from noreply@sdcoe.net.
6. Click the confirm link with-in email.
7. Now test the connection. Refer to *Send a Phishing Email (Ad Hoc)* on p.66.

SMTP for Gmail

OPTIONAL: Configuration of SMTP is optional and is not necessary in Red Herring. Phishing emails will be sent using our custom domains selectable from the Send Email or Create a Campaign menu items. Configuration of SMTP is only needed in order to send a simulated phishing campaign using your organization's email domain name in the sender's address.

First complete the steps in the **Google Gmail Allow-Listing** section and return here once complete.

1. Navigate to **Configuration > SMTP**.
2. Enter the **Server Name** (aspmx.l.google.com), **No Username, No Password, 25** for **SMTP port number**, and check the **SSL** encryption box.

A screenshot of the SMTP configuration interface. It features four input fields: the first contains 'aspmx.l.google.com', the second is labeled 'Username', the third is labeled 'Password', and the fourth contains '25'. Below these fields is a checkbox labeled 'SSL' which is checked. At the bottom is a red button with the text 'Update'.

3. Click **Update**.
4. Check your Gmail Inbox for an email from noreply@sdcoe.net.
5. Click the confirm link with-in email.
6. Now test the connection. Refer to *Send a Phishing Email (Ad Hoc)* on p.66.

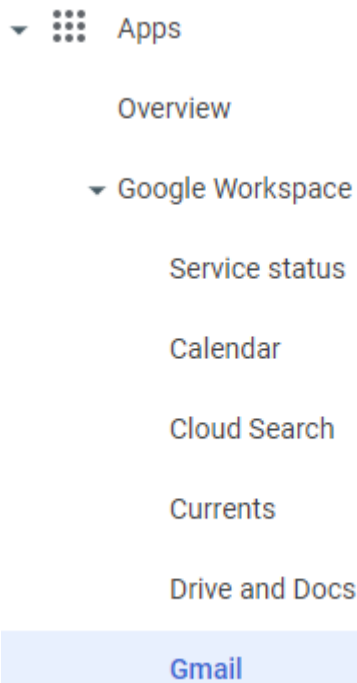
Google Gmail Allowlist & Gateway

These directions will set up an allowlist and Email Gateway for Gmail to ignore simulated phishing emails from Red Herring.

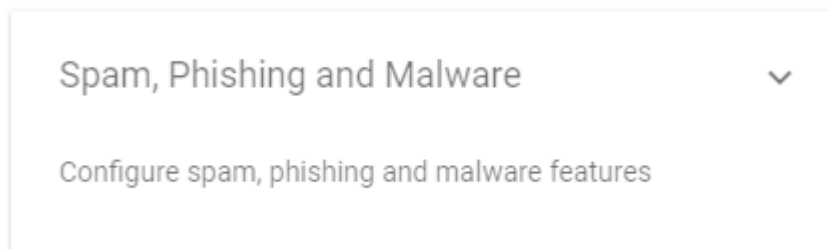
In Google Admin go to Apps > G-Suite > Settings for Gmail > Spam, phishing, and malware

<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, 20.118.176.15, 20.118.176.58

Email allowlist
Applied at 'San Diego County Office of Education'

An email allowlist is a list of IP addresses from which you want your users to receive emails. Mail sent from these IP addresses should not be marked as spam. In order to take full advantage of Gmail's spam filtering service and for best spam classification results, IP addresses of your mail servers that are forwarding email to Gmail should be added to Inbound Gateway and not in IP allowlist. [Learn more](#)

Enter the IP addresses for your email allowlist: 20.150.248.122, 20.118.176.229, 192.40.172.4

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

Inbound gateway
Locally applied

Unfiltered Inbound

EDIT DISABLE DELETE

Gateway IP(s): 204.238.213.227, 198.133.204.0/24, 66.244.5.217, 66.244.2.75, 66.244.2.125, 66.244.2.202, 66.244.2.201

Require Inbound Gateway IP: No

Require Secure (TLS) Connections: Yes

Spam Header Tag: X-Spam: this is spam

Disable Gmail Spam Filtering: Yes

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

Click **Save** or **Add Setting**

Inbound gateway

If you use email gateways to route incoming email, please enter them here to improve spam handling [Learn more](#)

☒ Enable

1. Gateway IPs

| IP addresses / ranges |
|-----------------------|
| 20.150.248.122 |
| 20.118.176.229 |
| 192.40.172.4 |

[ADD](#)

☒ Automatically detect external IP (recommended)

☐ Reject all mail not from gateway IPs

☒ Require TLS for connections from the email gateways listed above

2. Message Tagging

☒ Message is considered spam if the following header regexp matches

Regexp [Learn more](#)

X-Spam: this is spam

[Test expression](#)

☒ Message is spam if regexp matches

☐ Regexp extracts a numeric score

☒ Disable Gmail spam evaluation on mail from this gateway; only use header value

7. 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.

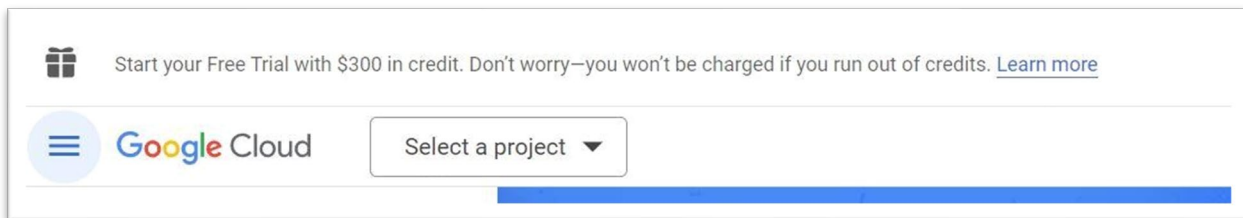
Google Service Account

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

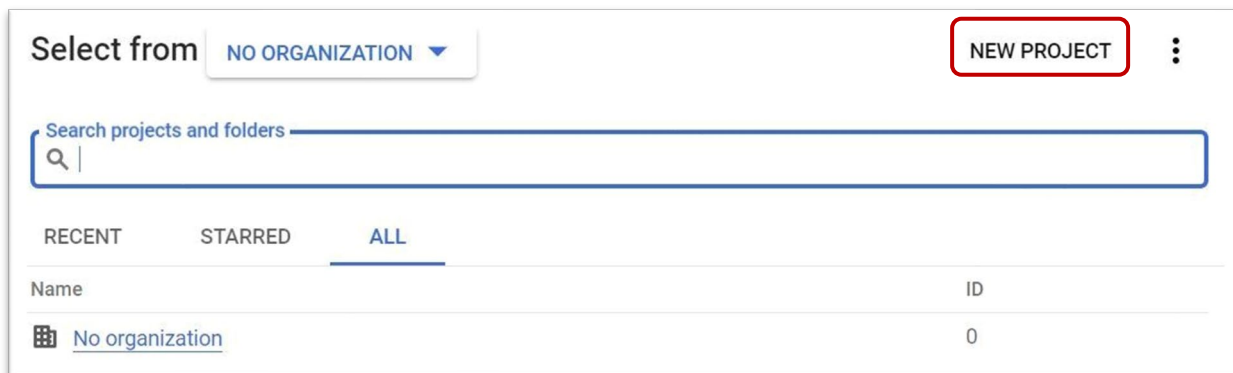
1. Go to <https://cloud.google.com/> and login with your Google Admin Account
2. Click Console to go to the Console Page



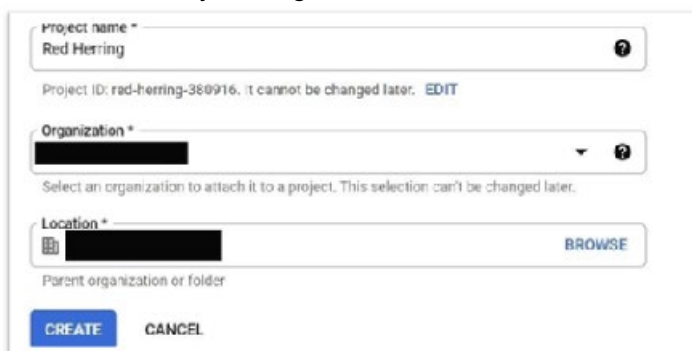
3. Select APIs and Services
4. On the top panel click **Select a project**



5. Create a **New Project**



6. Choose your Organization and Location



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

Select from REDHERRING.WORK NEW PROJECT

Search projects and folders

RECENT STARRED ALL

| Name | ID |
|-------------------|--------------|
| ✓ ☆ RedHerring ? | redherring |
| redherring.work ? | 300612821462 |

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

Google Cloud RedHerring

APIs & Services Credentials + CREATE CREDENTIALS DELETE RESTORE DELETED CREDENTIALS

Create credentials to access Google APIs

API Keys

Service account

Help me choose

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

Create service account

1 Service account details

Service account name
Red Herring

Display name for this service account

Service account ID *
red-herring

Email address: red-herring@redherring.iam.gserviceaccount.com

Service account description
for Google Auto Sync

Describe what this service account will do

CREATE AND CONTINUE

3. After creating the service account, copy the Unique ID from Details tab of the Service Account page
 - a. Google Cloud > Service Accounts > IAM & Admin > Service Accounts > {Red Herring Service Account}

Service account details

Name: Red Herring [SAVE]

Description: for Red Herring user auto-sync [SAVE]

Email: red-herring@red-herring-sync.iam.gserviceaccount.com

Unique ID: 103357592147226208308

4. Go to the Keys tab of Service Account page and select **Add Key**

Red Herring

DETAILS PERMISSIONS **KEYS** METRICS LOGS

Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading keys to your local machine.

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 |
|--------------------|--------|-----|-------------------|---------------------|
| No rows to display | | | | |

5. For key type choose "JSON"

Create private key for "Red Herring"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

☒ JSON
Recommended

☐ P12
For backward compatibility with code using the P12 format

CANCEL CREATE



6. After successfully creating, the JSON key will automatically download to your computer
7. (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](#).

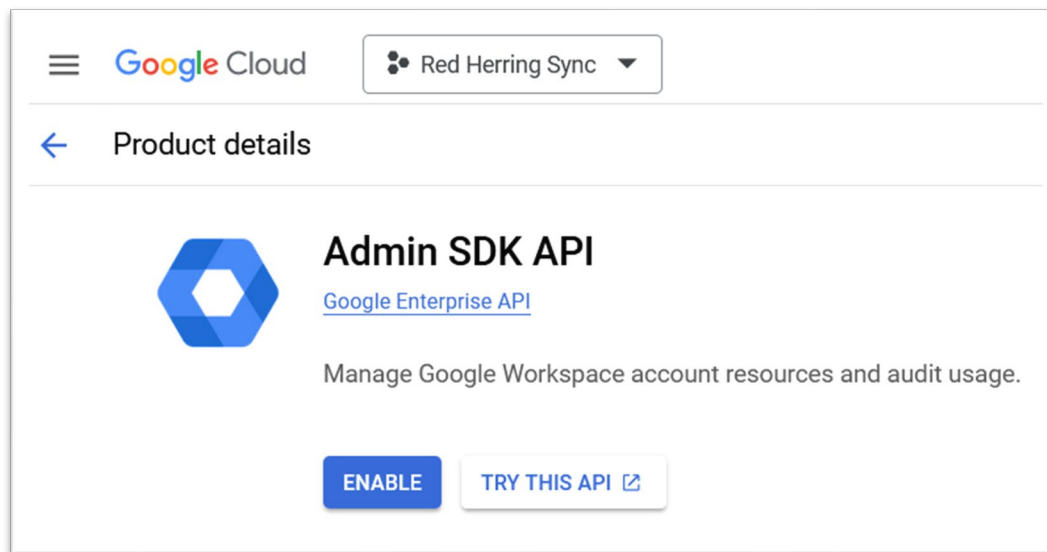
[Learn more about setting organization policies for service accounts](#)

ADD KEY ▾

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

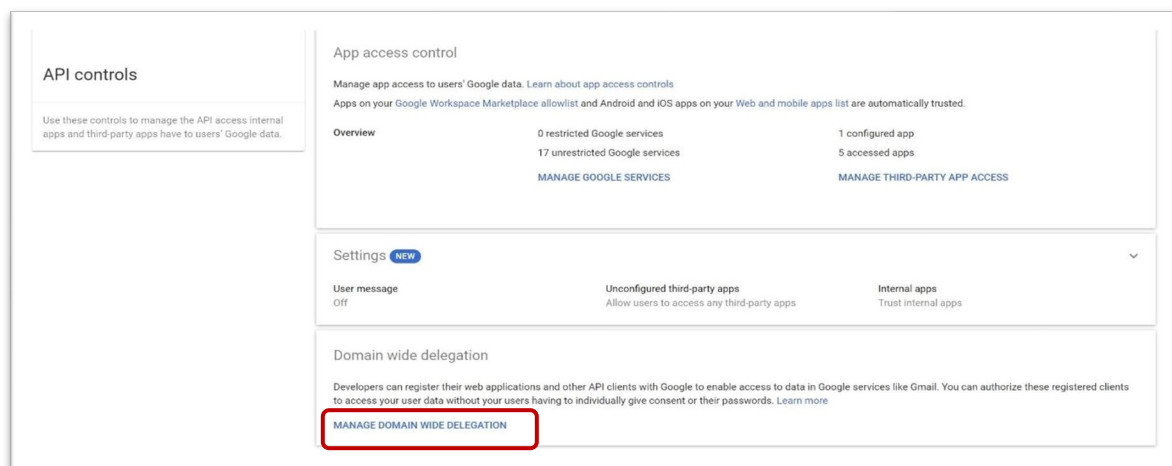
Enable Admin SDK for Service Account in Google Cloud Console

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



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**

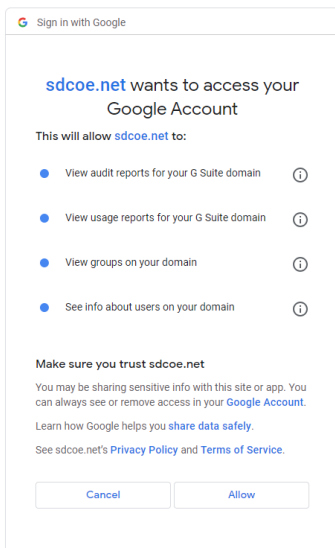
Trust Red Herring as an OAuth App

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 Third-Party App Access**
4. Open the **Add app** drop-down menu
5. Select **OAuth App Name Or Client ID**
6. Search for: 918725752096-bsbsa9v8kl50op3525s5bl21v2aj8061.apps.googleusercontent.com
7. Hover over RedHerring and press **Select**

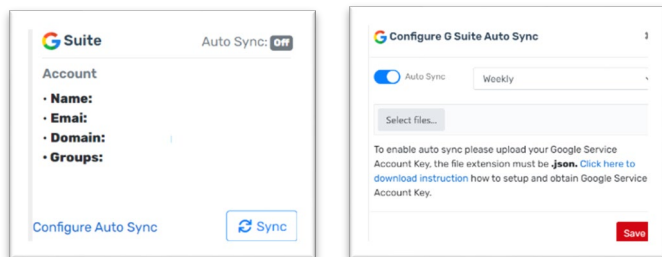
8. Check the box next to OAuth Client ID and press the **Select** button
9. Select All Users and press **Continue**
10. Select the **Trusted** radial button and press **Continue**
11. Review the settings and press **Finish**
12. Wait 5-10 minutes for the changes to propagate and proceed with next step
(Log out of the Red Herring console)

Upload JSON and Sync Target Users into Red Herring

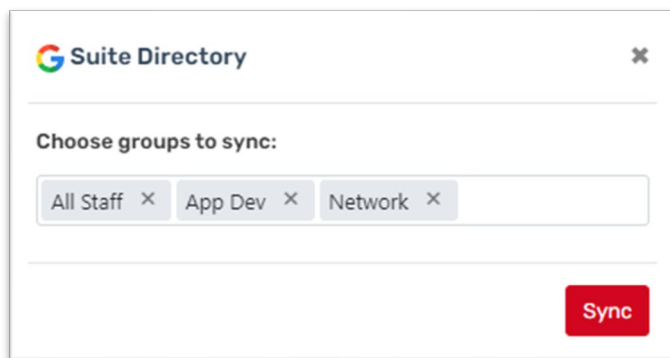
1. Navigate to Red Herring > Configuration > Directory
2. Select **+Add new** and login to G-Suite with an Admin account
3. **Allow** sdcoe.net access to sync your users



4. On the G-Suite sync tile select **Configure Auto Sync**
5. Slide the toggle switch for Auto Sync and choose your sync frequency
6. Upload the .json file and **Save**



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



Microsoft 365 App Access

OPTIONAL: Configuration of SMTP is optional and is not necessary in Red Herring. Phishing emails will be sent using our custom domains selectable from the Send Email or Create a Campaign menu items. Configuration of SMTP is only needed in order to send a simulated phishing campaign using your organization's email domain name in the sender's address.

Depending on your Microsoft 365 license level and configuration, these instructions may not work for you.

This documentation is a step-by-step guide to setup Red Herring SMTP server settings to use an Office 365 mailbox and send mail using SMTP AUTH client submission.

Overview of steps needed:

1. Creating a new user via Microsoft 365 Admin center
2. Enabling Multifactor Authentication for that new user
3. Adding an App Password for that new user
4. Creating an Admin account in Red Herring for that new user
5. Logging into Red Herring as that new user account
6. Configuring SMTP in Red Herring with the new email address and app password.
7. Allow-listing the Red Herring servers

Adding a new user in Microsoft 365 Admin Center

Skip this section if you plan to allow SMTP access through an existing user, you will have to ensure SMTP Auth is enabled and create an App Password for the existing user in the next sections.

1. Sign into <https://admin.microsoft.com>
2. Click on **Users > Active users > Add a user**
Suggested properties:
First name: Red
Last name: Herring
Display name: Red Herring
Username: redherring
3. Click **Next**
4. Select **Assign user a product license** and choose **Office 365 <license plan> for faculty**
5. Under Roles (User: no administration access) select **User (no admin center access)** and click **next**
6. Click **Finish adding**

Enable SMTP Auth for user in Microsoft 365 Admin Center

The user account that you will use to connect in **Red Herring > Configuration > SMTP** will need access to use **Authenticated SMTP** (enabled).

1. Sign into <https://admin.microsoft.com>
2. Navigate to **Users > Active users**
3. Select the user, and in the flyout that appears, click **Mail** tab
4. In the **Email apps** section, click **Manage email apps**
5. Verify the **Authenticated SMTP** setting: unchecked = disabled, **checked = enabled**
6. When you're finished, click **Save changes**

Enabling multifactor authentication for new user

1. Sign into <https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx?BrandContextID=O365>
2. Click on the **Redherring** user.

View: Sign-in allowed users redherring × Multi-Factor Auth status: Any ▼

| <input type="checkbox"/> | DISPLAY NAME ▲ | USER NAME | MULTI-FACTOR AUTH STATUS |
|--------------------------|-----------------|--------------------------------------|--------------------------|
| <input type="checkbox"/> | Redherring smtp | redherringsmtp@sdcoe.onmicrosoft.com | Disabled |
| <input type="checkbox"/> | redherringtest | redherringtest@sdcoe.onmicrosoft.com | Disabled |

Select a user

3. Click **Enable**

bulk update

View: Sign-in allowed users redherring × Multi-Factor Auth status: Any ▼

| <input type="checkbox"/> | DISPLAY NAME ▲ | USER NAME | MULTI-FACTOR AUTH STATUS |
|-------------------------------------|-----------------|--------------------------------------|--------------------------|
| <input checked="" type="checkbox"/> | Redherring smtp | redherringsmtp@sdcoe.onmicrosoft.com | Disabled |
| <input type="checkbox"/> | redherringtest | redherringtest@sdcoe.onmicrosoft.com | Disabled |

Redherring smtp

redherringsmtp@sdcoe.onmicrosoft.com

quick steps

[Enable](#)

[Manage user settings](#)

4. Click enable **multi-factor auth**.
5. Click **close**.

Adding an App Password

This step will require a cell phone number to authenticate via SMS with the “redherring” account.

1. Sign in with the “redherring” account
2. <https://account.activedirectory.windowsazure.com/>
3. Click Next on the page:

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

4. Type in your cell phone number for the account.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone

United States (+1)

Method

☒ Send me a code by text message

☐ Call me

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

5. Type in the verification code from your cell phone and click verify.

When you receive the verification code, enter it here

Cancel

Verify

6. Copy the app password (save this password, it will be used to configure the SMTP Server in Red Herring) and click Done.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 3: Keep using your existing applications

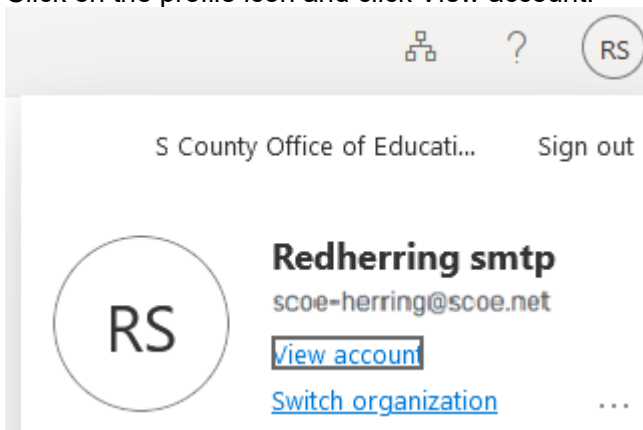
In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. [Learn more](#)

Get started with this app password:

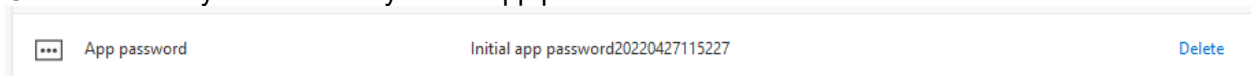


Done

7. Click on the profile icon and click View account.



8. Click on Security Info and verify that a App password was created.



Adding new user as Admin in Red Herring

1. Sign into Red Herring with an Admin account:
<https://redherring.sdcoe.net/>
2. Click on **Configurations > Admins** and click Create Admin.
3. Type your preferred username and click create:
Name: Redherring
Email: redherring@<your domain>
Role: Admin

Red Herring

Name

Redherring smtp

Email

scoe-herring@scoe.net

Role

Admin ▼

✓ Create

⊘ Cancel

4. A confirmation email will be sent to you “redherring” mailbox. Confirm the email and change the account password.
5. Logout of your current Red Herring Admin account.

6. Login to Red Herring with the admin account that you created the App Password for. It has to have the same email address that you will be using to connect to Office365.

Office365 User

Server Name
smtp.office365.com

Username
scoe-herring@scoe.net

App Password

Port
587

☒ **SSL / TLS**

Update

Red Herring Admin User

scoe-herring@scoe.net

Roles: Admin

District: S County Office of Education

Logout

7. Navigate to **Configuration > SMTP**.
8. Enter the Server Name (**smtp.office365.com**), Username, App Password, **587** for SMTP port number, and check the **SSL** encryption box.
9. Click **Update**.

Red Herring

SMTP Server updated successfully. In order to use this SMTP server we have sent you a confirmation email. Please follow the instructions in the email.

OK

10. Check your Inbox for an email from noreply@sdcoe.net.
11. Click the confirm link with-in email.

Microsoft 365 Allowlisting

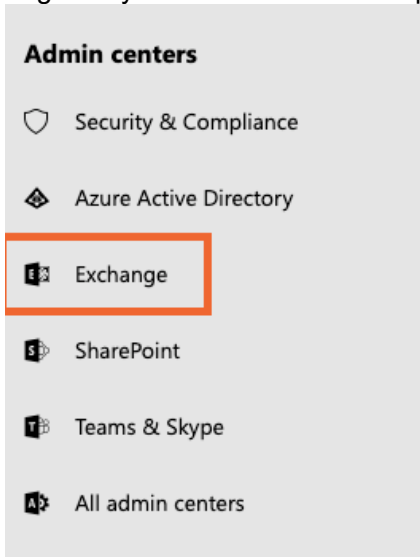
To use Microsoft's Advanced Delivery to categorize your Red Herring emails as simulated phishing emails in your Microsoft 365 environment, follow the steps below:

Note: An A5/E5 license may be needed.

1. Open the Microsoft 365 Defender portal at security.microsoft.com
2. Navigate to Policies & Rules under Email & Collaboration
3. Navigate to Threat Policies > Advanced Delivery
<https://security.microsoft.com/advanceddelivery>
4. Select the Phishing Simulation tab
5. Select Edit/Add/Configure
6. For IP address enter:
192.40.172.4, 192.40.172.139, 20.118.176.15, 20.118.176.58
7. For Domain and Simulation URL enter the domains that you would like to use in your campaigns:
aditisecurity.com
servicecounty.net
schoolunified.net
uniondistrict.net
ctateachers.net
highunion.net
sandiegocoe.net
countyofsd.net
sdcounty.net
sdcoes.net
sdc0e.net

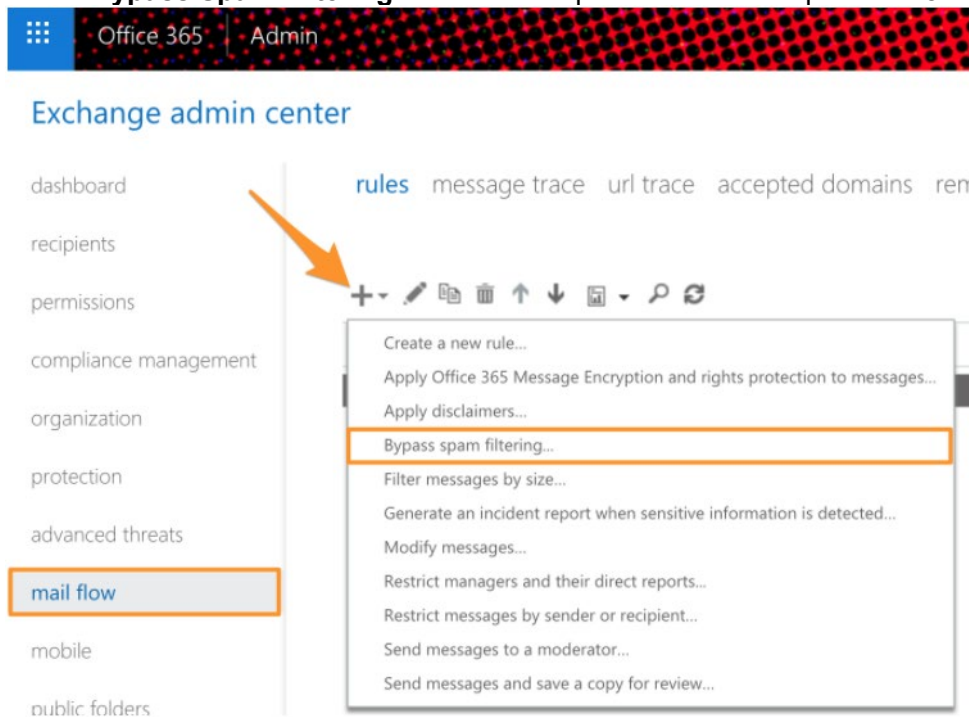
To allowlist simulated phishing emails sent from Red Herring in your Microsoft 365 environment, follow the steps below:

1. Log in to your mail server Admin portal. Then, navigate to Admin centers > Exchange



2. Select **Mail Flow > Rules** and click on the + sign located in the top-left

3. Select **Bypass Spam Filtering...** from the drop-down. This will open the **new rule** screen



4. Give the rule a name, such as **Training Notifications Bypass Clutter** or **Spam Filtering by Email Header**
5. Select **Apply this rule if...** and then choose **The sender... > IP address...** from the drop-down. This will open the **IP address** screen

Bypass Clutter and Spam Filter by IP Address

Name:
Bypass Clutter and Spam Filter by IP Address

*Apply this rule if...
Sender's IP address is in the range...
Select one

- The sender...
 - is this person
 - is external/internal
 - is a member of this group
 - address includes any of these words
 - address matches any of these text patterns
 - is on a recipient's supervision list
 - has specific properties including any of these words
 - has specific properties matching these text patterns
 - has overridden the Policy Tip
 - IP address is in any of these ranges or exactly matches domain is**
- The recipient...
- The subject or body...
- Any attachment...
- Any recipient...
- The message...
- The sender and the recipient...
- The message properties...
- A message header...
- [Apply to all messages]

add exception

'147.160.167.0/26' or '23.21.109.212' or '23.21.109.197'

6. Enter our IP addresses “192.40.172.4, 192.40.172.139, 20.118.176.15, 20.118.176.58” on the **specify IP address** screen and click the + sign. Then, click the **OK** button.

Bypass Clutter and Spam Filter by IP Address

Name:
Bypass Clutter and Spam Filter by IP Address

*Apply this rule if...
Sender's IP address is in the range...
add condition

*Do the following...

- Set the message header to this value...
- and
- Set the spam confidence level (SCL) to...

add action

Except if...
add exception

Properties of this rule:
Priority:

specify IP address ranges

Enter an IPv4 address or range +

OK Cancel

'23.21.109.212' or '23.21.109.197'

Save Cancel

7. Verify the **Do the following...** field is set to **Set the spam confidence level (SCL) to...** and **Bypass spam filtering** is set on the right.

Name: Training Notifications Bypass Clutter and Spam Filtering by Er

*Apply this rule if...

Sender's IP address is in the range...

add condition

*Do the following...

Set the spam confidence level (SCL) to...

add action

Except if...

add exception

Properties of this rule:

Priority: 4

Bypass spam filtering

You don't need to create a transport rule to bypass spam filtering or mark email as spam for a sender or domain. Click here to use an [allow](#) or [block list](#) in the spam filter.

8. Scroll down the screen to the **Match sender address in message** option. Here, select **Envelope** from the drop-down.

☐ Stop processing more rules

☐ Defer the message if rule processing doesn't complete

Match sender address in message:

Envelope

9. Click the **Save** button.

Target Users

The recipients to your phishing emails are defined on the Target Users screen. There are five ways you can add target users to Red Herring: **Add users individually**, **CSV upload**, **On Premise AD sync**, **Azure sync**, and **Google sync**.

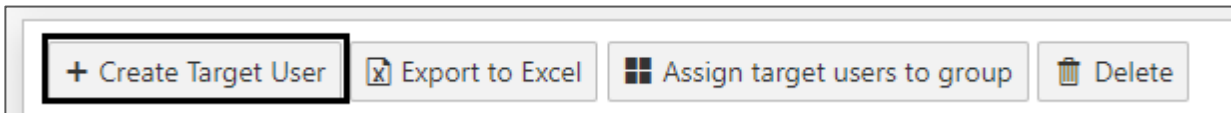
Depending on your license you will be allowed to add a certain amount of users into Red Herring. This amount can be viewed on your Target Users page or the District Report page.

 You have used **1259 / Unlimited** licenses

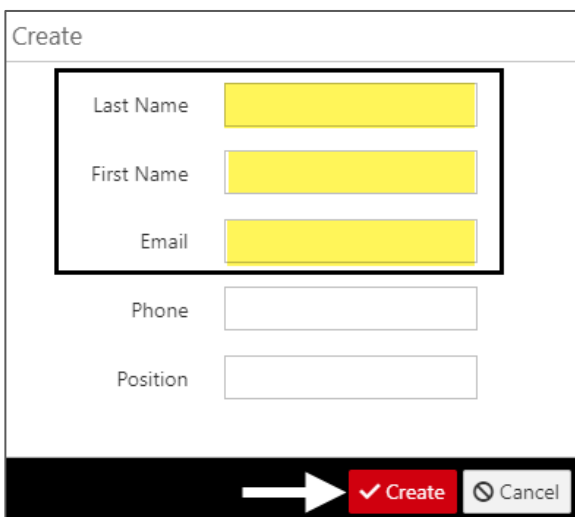
Add Target Users Individually

Follow these steps to add a user manually.

1. In the navbar, click **Target Users**.
2. Click **Create Target User**.



3. Enter the user's **Last Name**, **First Name**, and **Email Address** (required fields). The **Phone** and **Position** fields are optional. Click **Create**.

A screenshot of the 'Create' form. It has a title 'Create' at the top. Below it are five input fields: 'Last Name', 'First Name', 'Email', 'Phone', and 'Position'. The first three fields are highlighted with a black box. At the bottom, there is a black bar with a white arrow pointing right, a red 'Create' button with a white checkmark, and a grey 'Cancel' button with a white circle and slash.

4. The screen will display your target users.

Create Target User

Export to Excel

Assign target users to group

Delete

Drag a column header and drop it here to group by that column

Last Name

First Name

Email

Phone

Position

Risk

Group

| | | | | | | | |
|--------------------------|------|-------|---------------------------|--------------|---------------------------|-----|-----------------------------------|
| <input type="checkbox"/> | John | Smith | john.smith@redherring.com | 555-555-5555 | Technical Support Analyst | Low | <div>Edit</div> <div>Delete</div> |
| <input type="checkbox"/> | Jane | Smith | jane.smith@redherring.com | 555-555-5555 | Technical Support Analyst | Low | <div>Edit</div> <div>Delete</div> |
| <input type="checkbox"/> | John | Smith | john.smith@redherring.com | 555-555-5555 | Program Manager | Low | <div>Edit</div> <div>Delete</div> |
| <input type="checkbox"/> | John | Smith | john.smith@redherring.com | 555-555-5555 | Supervisor in Charge | Low | <div>Edit</div> <div>Delete</div> |
| <input type="checkbox"/> | John | Smith | john.smith@redherring.com | 555-555-5555 | IT Project Specialist | Low | <div>Edit</div> <div>Delete</div> |

NOTES:

- Click **Export to Excel** to export all users (.xlsx).
- To edit a user, click the **Edit** button to the right of the user's record.
- To delete a user, click the **Delete** button to the right of the user's record. A prompt will appear asking if you are sure you would like to delete.
- To delete multiple users, click the checkbox to the left of the record(s), then click the **Delete** button at the top of the list. A prompt will appear asking if you are sure you would like to delete.
- You can filter any column that has a filter icon.

CSV Upload

1. In the navbar, click **Target Users**.
2. In the *CSV Upload* area, select your CSV file and click **Upload**.

CSV Upload:

Select files...

Upload

Instructions:

The text file must include 3 columns: **first name, last name, email**. Other columns are optional.

The columns must be **comma-delimited**.

[Download Instructions \(pdf\)](#)

[Download Template \(csv\)](#)

NOTE: Your file must include nine columns: ***First Name, *Last Name, *Email, Group, Phone, Position, Building, Location, and Supervisor**. Those marked with an asterisk (*) denote that they are required.

| Required | Column Name | Column Number | Length | Format |
|----------|-------------|---------------|--------|---------|
| Yes | First Name | 1 | 255 | Alpha |
| Yes | Last Name | 2 | 255 | Alpha |
| Yes | Email | 3 | 255 | Alpha |
| No | Group | 4 | 255 | Alpha |
| No | Phone | 5 | 10 | Numeric |
| No | Position | 6 | 255 | Alpha |
| No | Building | 7 | 255 | Alpha |
| No | Location | 8 | 255 | Alpha |
| No | Supervisor | 9 | 255 | Alpha |

For more detailed instructions, click **Download Instructions (pdf)** on the Target Users page.

On Premise Active Directory Sync

You may have to allow one of the following IP addresses through your firewall on port 389 (LDAP).

20.118.176.15, 20.150.248.122, 20.118.176.229

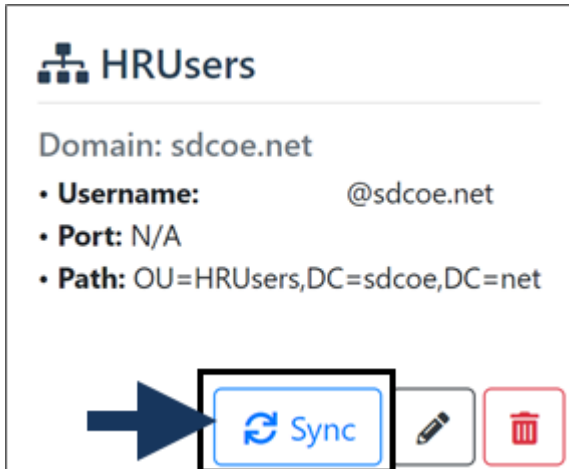
1. Go to **Configuration > Directory**.
2. Click on the **+ Add new** tile. Select **On Premise**. Enter your Active Directory Connection information: **Domain Name**, **Username** (with appropriate permissions), and **Password**. The **Port** field is optional if you use the standard port. Click **Connect**.

The screenshot shows two side-by-side panels. The left panel, titled 'Active Directory Configuration', contains a dashed box with a blue plus icon and the text '+ Add new'. Below this is a section titled 'Active Directory Provider' with three buttons: 'On Premise' (highlighted with a black border), 'Azure', and 'Google'. The right panel, titled 'Active Directory Connection', has a close button (X) in the top right. It contains four input fields: 'Domain Name', 'Username', 'Password', and 'Port'. At the bottom of this panel are two radio buttons (the first is selected) and a red 'Connect' button.

3. Next, you'll select which Active Directory group to pull users from.

The screenshot shows a dialog box titled 'Active Directory Path' with a close button (X) in the top right. It features a list of Active Directory groups with expandable arrows to the left. The groups listed are: AutoPilot Domain Join, Builtin, Citrix, Clarity Users Computers, ClarityTestOU, CMTest, Computers, Computers - Secure, Computers - Security Groups, Computers - Windows 8, Computers Wsus Exemption, ComputersInactive, Disabled, Domain Admins, Domain Controllers, DomainAdmins, dotNet Install, and EndpointEncryption. At the bottom of the dialog are two radio buttons (the second is selected) and a red 'Map' button.

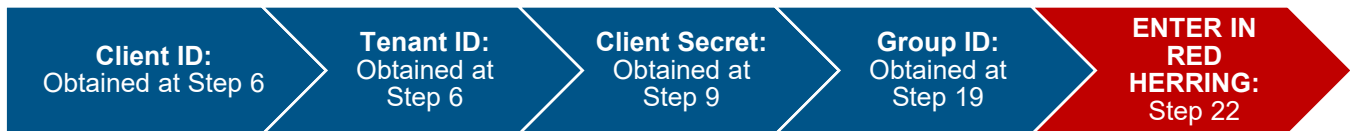
4. Once connected, you'll need to perform an initial **Sync** to import users from AD. Refer to *Send a Phishing Email (Ad Hoc)* on p.66. Subsequential syncs will be used to update any new users.



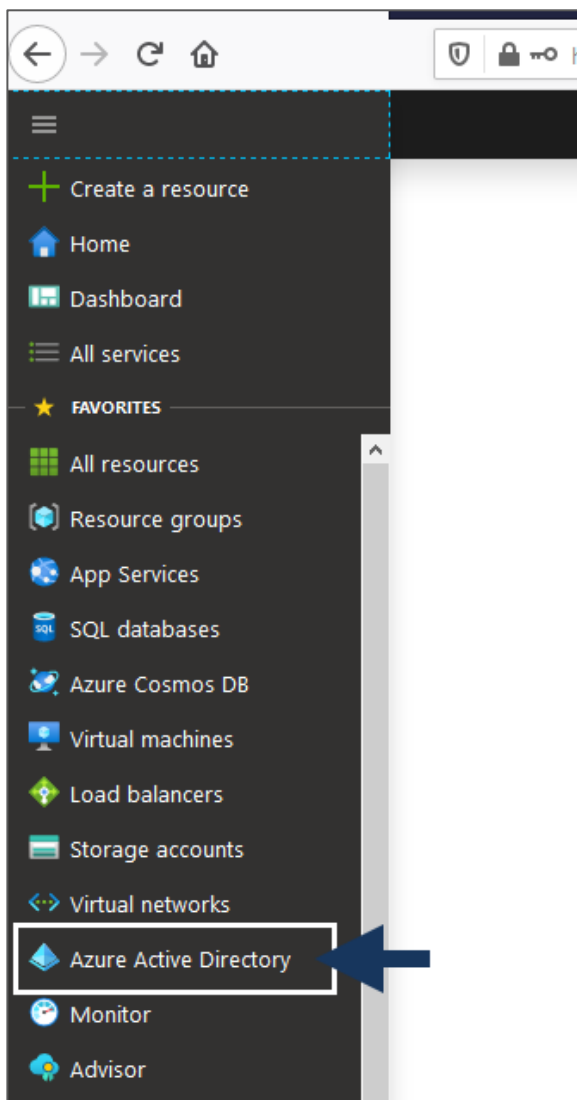
Azure User Sync

To import users from Azure, you'll need to create an App Registration ID in Azure. For additional information about creating an application registration in Azure, please refer to this Microsoft support article: <https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>.

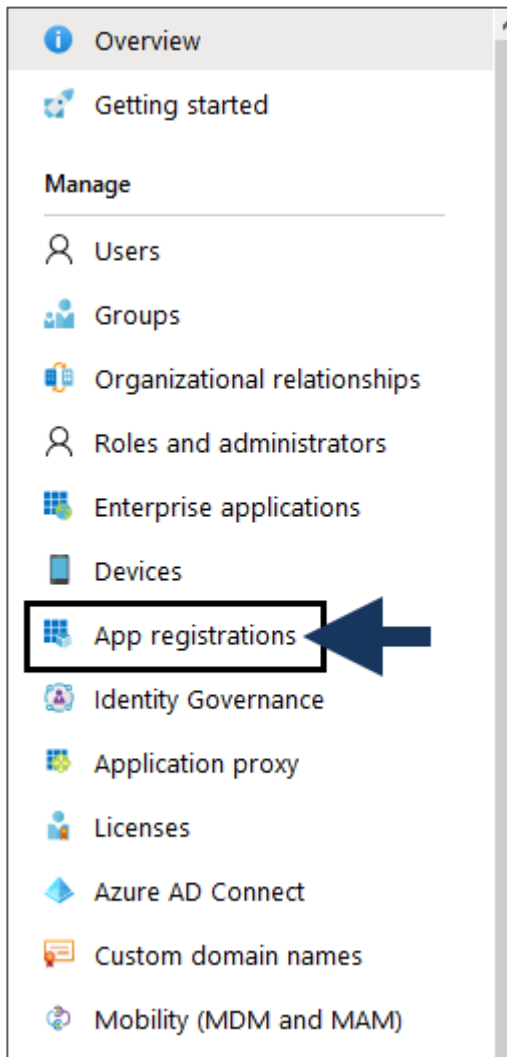
Follow the steps in this section to collect from Azure the **Client ID**, **Tenant ID**, **Client Secret**, and **Group ID**, which you will then enter in Red Herring.



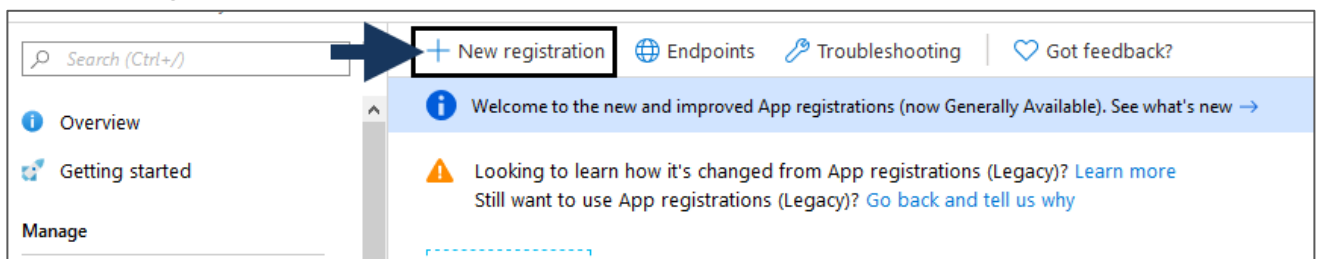
1. Log in to <https://portal.azure.com> using your Azure administrative account.
2. In the navigation on the left, select **Azure Active Directory**.



3. Select **App registrations**.



4. Click **New registration**.




5. On the *Register an application* page, enter the following, then click **Register**.

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (San Diego County Superintendent of Schools only - Single tenant) 

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)


☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)


Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

e.g. https://myapp.com/auth

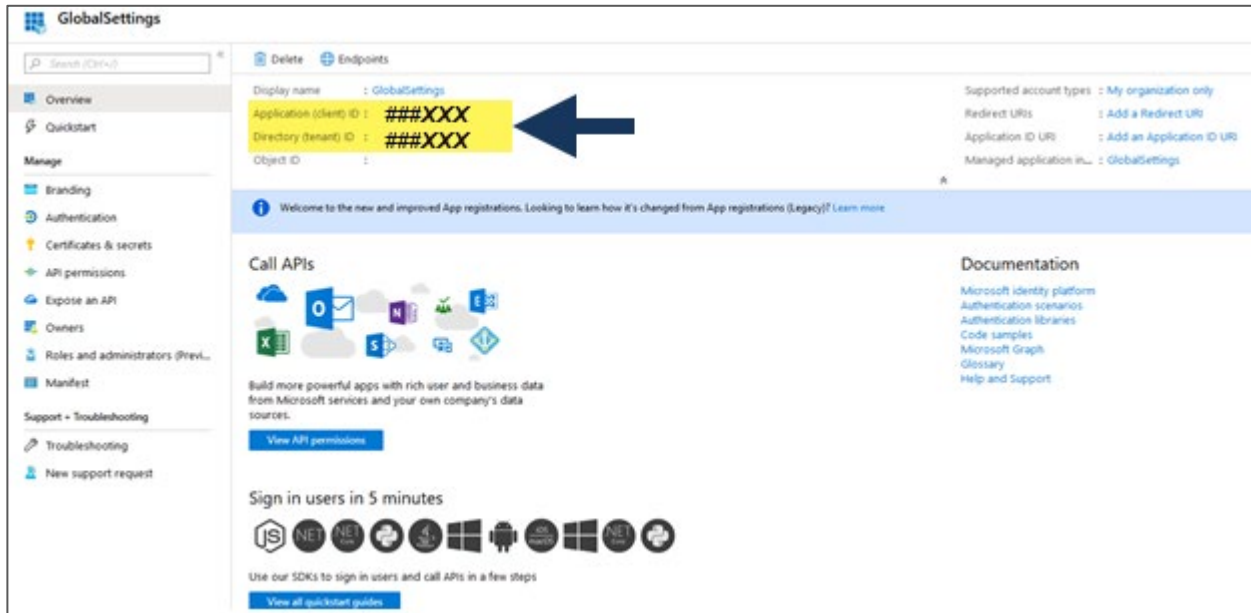
By proceeding, you agree to the [Microsoft Platform Policies](#) 

Register

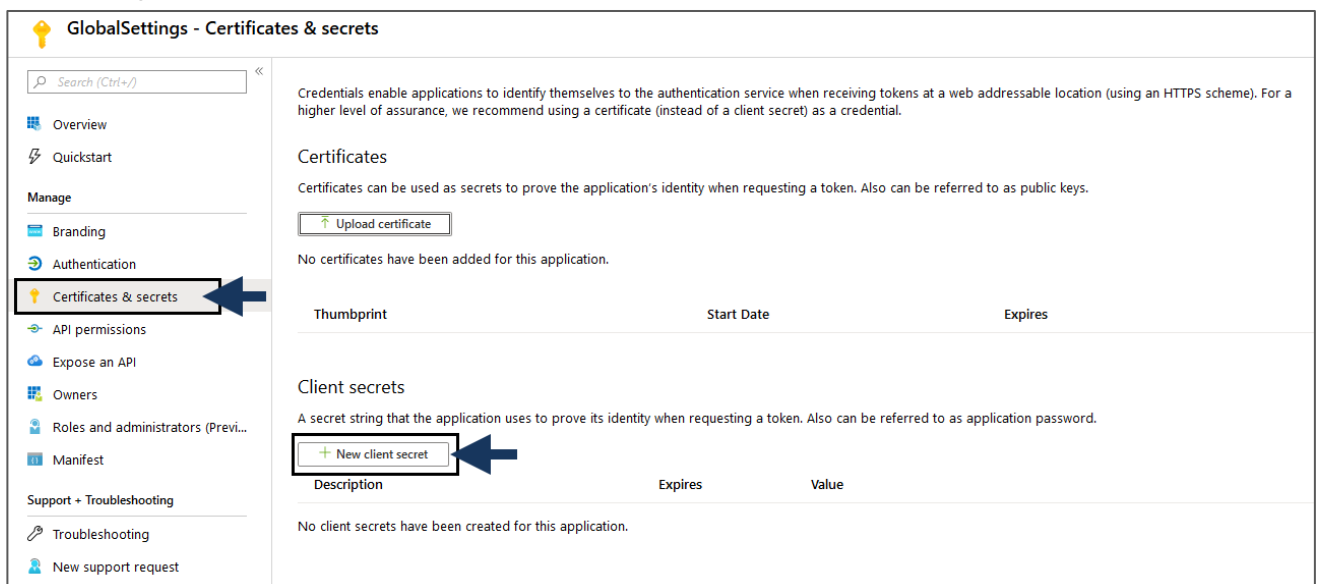


- **Name:** Enter a name for the application. *Example: Red Herring*
- **Supported account types:** Select *Accounts in this organizational directory only*

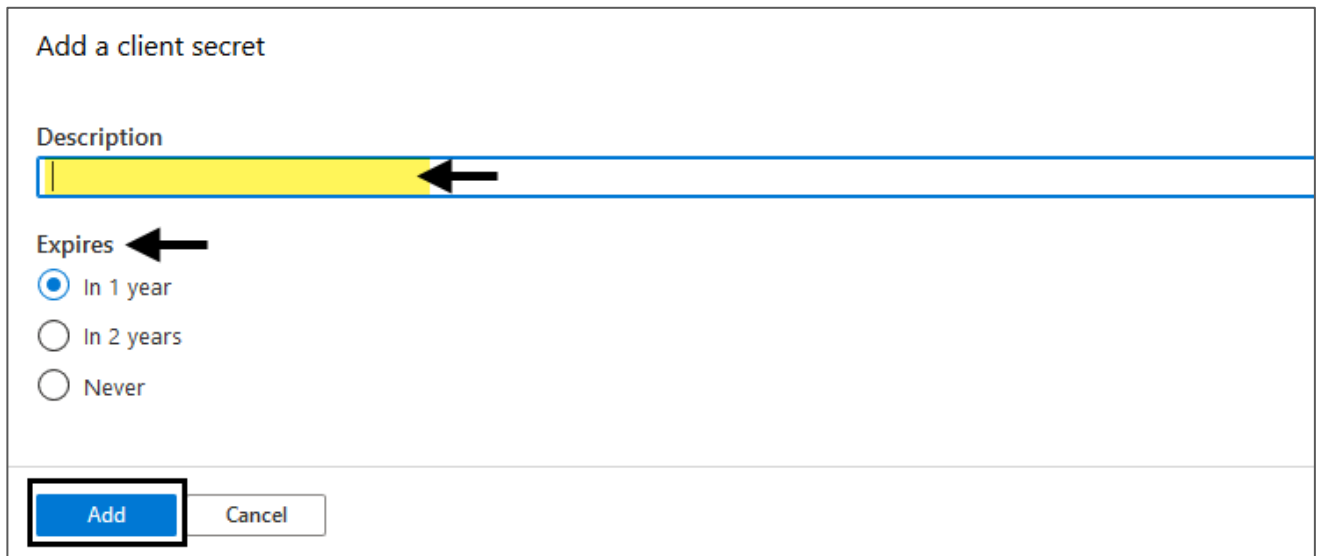
6. Copy the **Application (client) ID** and **Directory (tenant) ID**. **IMPORTANT: You will later input this information in Red Herring at Step 22.**



7. In the navigation on the left, select **Certificates & secrets**. Then select **New client secret**.



8. Enter the description in the client secret form and select how long you want the secret key to be valid. Click **Add**.



Add a client secret

Description

Expires

☒ In 1 year

☐ In 2 years

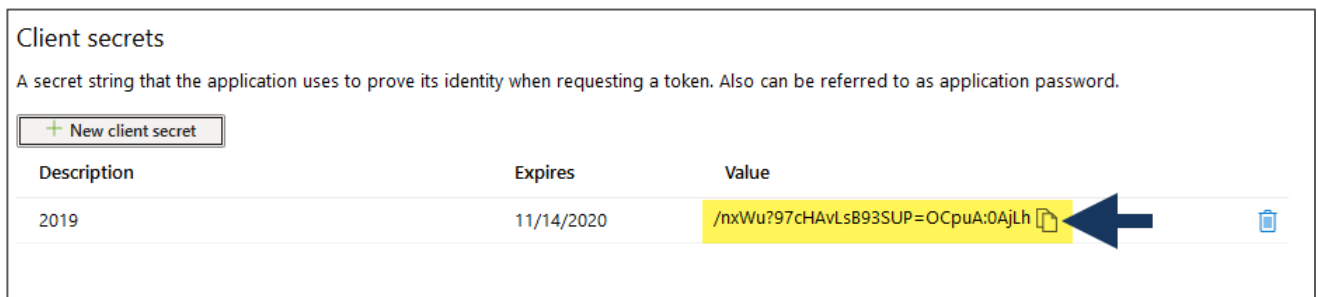
☐ Never

Add Cancel

NOTES ABOUT AN EXPIRED SECRET KEY:

- When the secret key is expired, the application will fail.
- When it expires, use the same steps as creating a new secret key.

9. **Copy the secret key.** If you move away from this page, the key will be hidden when you return to the page. **IMPORTANT: You will later input this information in Red Herring at Step 22.**



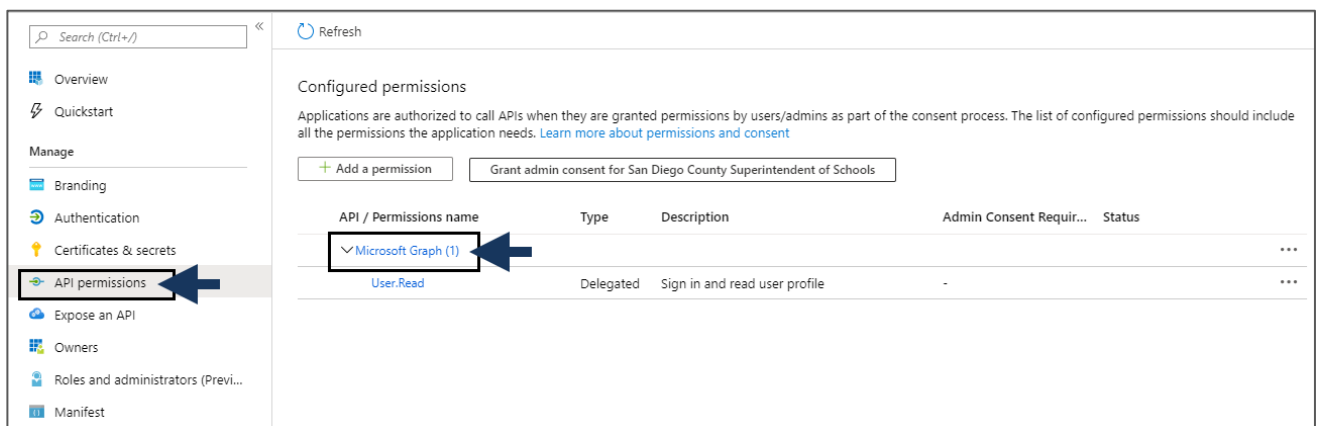
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

| Description | Expires | Value |
|-------------|------------|----------------------------------|
| 2019 | 11/14/2020 | /nxWu?97cHAvLsB93SUP=OCpuA:0AjLh |

10. Click **API Permissions**. Then select the **Microsoft Graph (1)** link.



Search (Ctrl+/) Refresh

Overview Quickstart Manage Branding Authentication Certificates & secrets API permissions Expose an API Owners Roles and administrators (Previous) Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for San Diego County Superintendent of Schools

| API / Permissions name | Type | Description | Admin Consent Requir... | Status |
|------------------------|-----------|-------------------------------|-------------------------|--------|
| Microsoft Graph (1) | | | | ... |
| User.Read | Delegated | Sign in and read user profile | - | ... |

11. On the *Request API permissions* page, under **Delegated Permissions...**

Request API permissions

Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permission does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Type to search

| Permission | Admin Consent Required |
|--|------------------------|
| <input type="checkbox"/> email View users' email address ⓘ | - |
| <input type="checkbox"/> offline_access Maintain access to data you have given it access to ⓘ | - |
| <input type="checkbox"/> openid Sign users in ⓘ | - |
| <input type="checkbox"/> profile View users' basic profile ⓘ | - |
| > AccessReview | |
| > AdministrativeUnit | |
| > AgreementAcceptance | |
| > Agreement | |
| > Analytics | |
| > AppCatalog | |

...scroll down to *User (1)* section and uncheck the **User.Read** checkbox.

▼ **User (1)**

| | |
|--|-----|
| <input type="checkbox"/> User.Export.All Export user's data ⓘ | Yes |
| <input type="checkbox"/> User.Invite.All Invite guest users to the organization ⓘ | Yes |
| <input type="checkbox"/> User.Read Sign in and read user profile ⓘ | - |
| <input type="checkbox"/> User.Read.All Read all users' full profiles ⓘ | Yes |
| <input type="checkbox"/> User.ReadBasic.All Read all users' basic profiles ⓘ | - |
| <input type="checkbox"/> User.ReadWrite Read and write access to user profile ⓘ | - |
| <input type="checkbox"/> User.ReadWrite.All Read and write all users' full profiles ⓘ | Yes |

12. Select **Application permissions**.

Request API permissions

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

13. Scroll down to the *Directory (1)* section, expand the Directory, and check **Directory.Read.All**.

▼ **Directory (1)**

| | |
|--|-----|
| <input checked="" type="checkbox"/> Directory.Read.All Read directory data ⓘ | Yes |
| <input type="checkbox"/> Directory.ReadWrite.All Read and write directory data ⓘ | Yes |

14. Scroll down to the *Group* section, expand the Directory, and check **Group.Read.All**.

15. Scroll down to the *User* section, expand the Directory, and check **User.Read.All**.

16. Click **Update permissions**.

Update permissions Discard

17. Select **Grant admin consent for [your organization]**.

Permissions have changed, please wait a few minutes and then grant admin consent. Users and/or admins will have to consent even if they have already done so previously.

Configured permissions

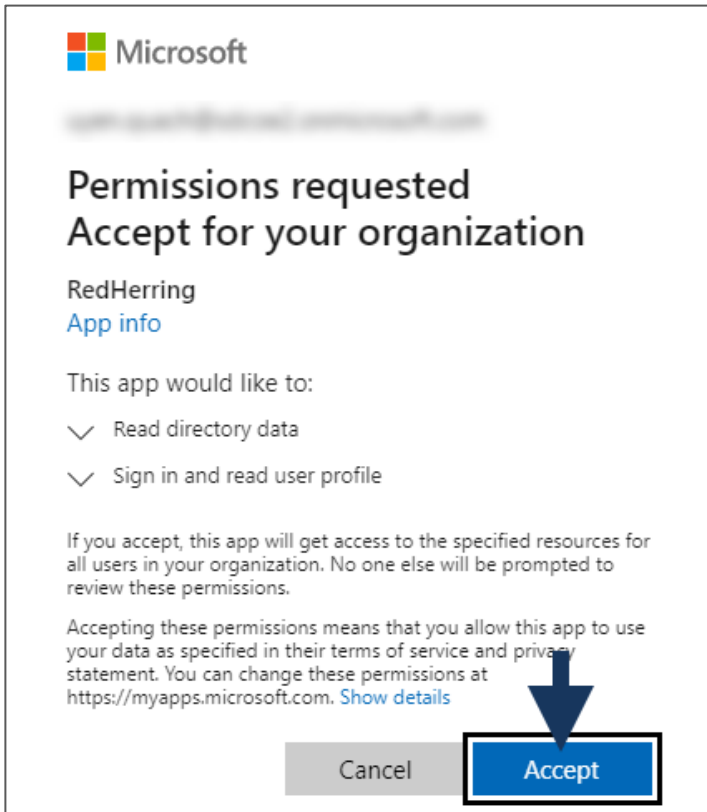
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) **Grant admin consent for San Diego County Superintendent of Schools**

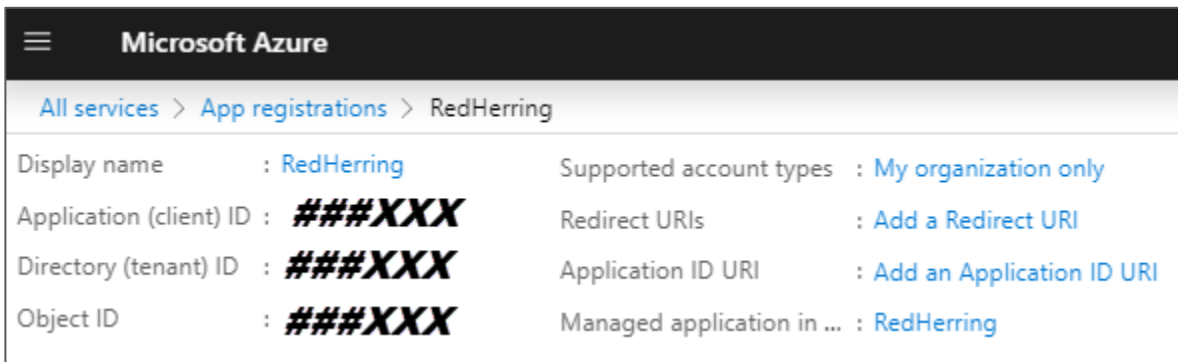
| API / Permissions name | Type | Description | Admin Consent Required | Status |
|----------------------------------|-------------|---------------------|------------------------|--|
| ▼ Microsoft Graph (1) ... | | | | |
| Directory.Read.All | Application | Read directory data | Yes | ⚠ Not granted for San Diego County Superintendent of Schools ... |

18. Azure will ask you to select the admin login account.

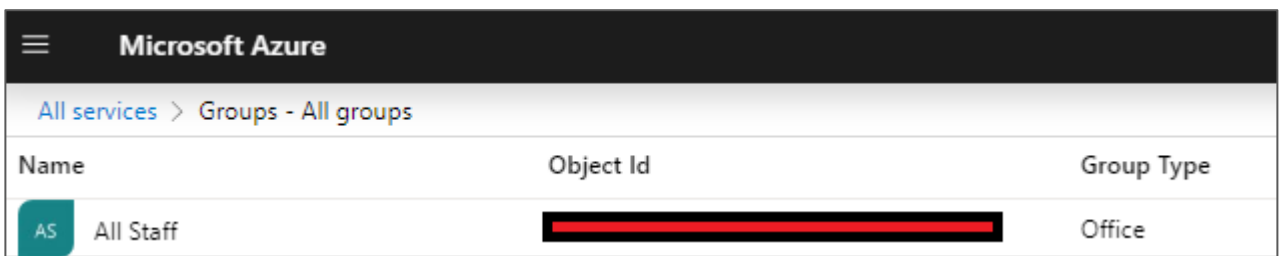
19. Then, select **Accept** on this prompt.



20. This is what is shown after you have created the Red Herring app registration.



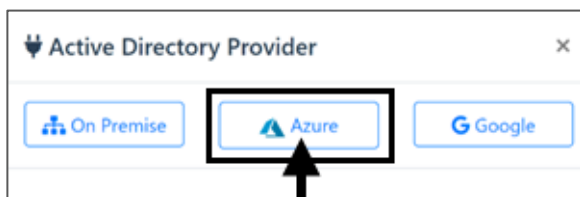
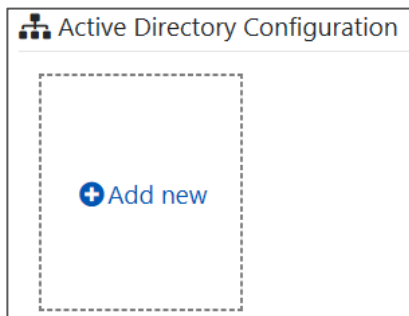
21. Navigate to Groups in Azure and record the Object ID for the user group you would like to import.
IMPORTANT: You will later input this information in Red Herring at Step 22.



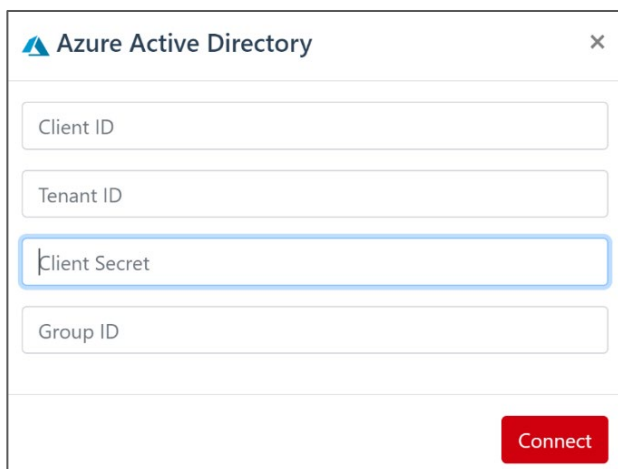
Now go to Red Herring.

22. In Red Herring, navigate to **Configuration > Directory**.

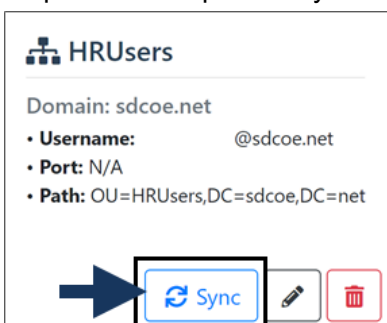
23. Click on the **+ Add new** tile and then select **Azure**.



24. Enter your Azure Connection information: **Client ID**, **Tenant ID**, **Client Secret**, and **Group ID** for the Active Directory Group. Click **Connect**.

A screenshot of the 'Azure Active Directory' configuration form. It has four input fields: 'Client ID', 'Tenant ID', 'Client Secret' (which is currently selected with a blue border), and 'Group ID'. At the bottom right of the form is a red 'Connect' button.

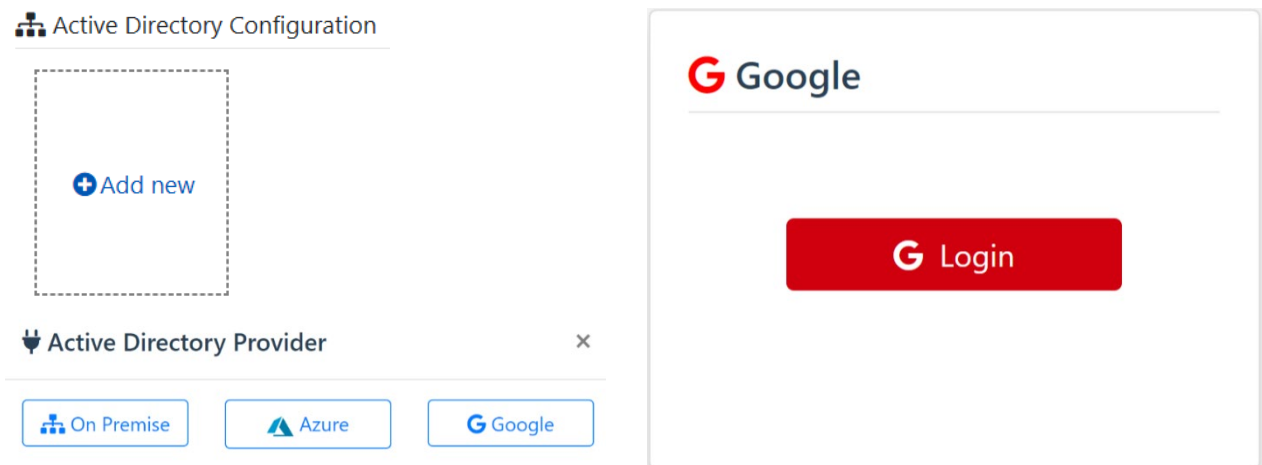
25. Perform an initial sync to import your AD users at any time. Refer to *Send a Phishing Email (Ad Hoc)* on p.66. Subsequent syncs will be used to update any new users.



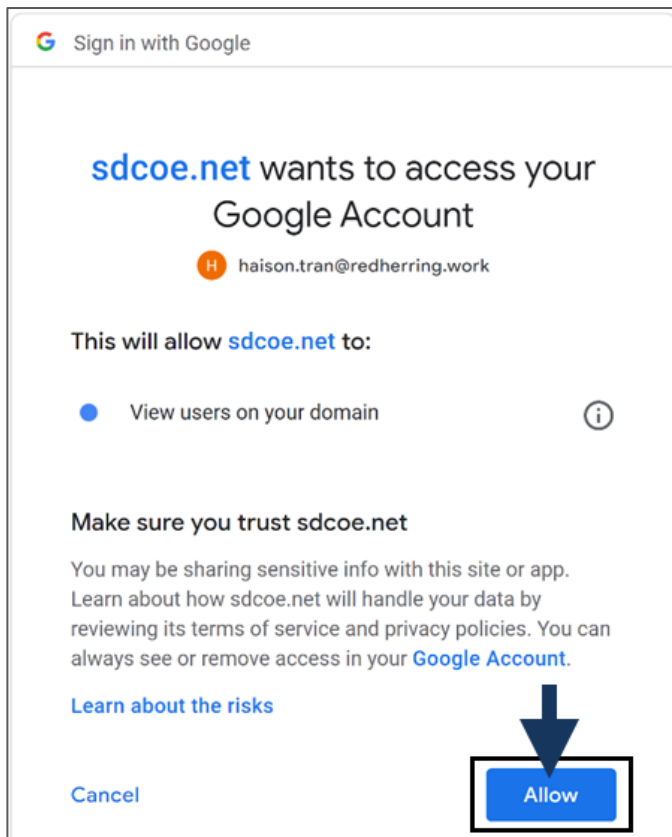
Google Sync

To import the users that you have in Google G-Suite, you'll have to log-in Google through Red Herring using you're G-Suite administrative credentials and allowing Red Herring access to your Google account.


1. Go to **Red Herring > Configuration > Directory > + Add new** and add your Google users by logging into Google through Red Herring.



2. Confirm that you would like to allow Red Herring access to your Google account.




- Once you're logged into Google through Red Herring, perform an initial **Sync** to import your Google users. Refer to *Send a Phishing Email (Ad Hoc)* on p.66. Subsequential syncs will be used to update any new users.



Account

- **Name:** redherring
- **Email:** redherring@redherring.work
- **Domain:** redherring.work

 Sync

- Red Herring does not store your Google Credentials.
- Once you log out of Red Herring, you'll have to sign in to Google again whenever you want to sync your G-Suite users.

NOTE: In your Google Admin settings page, you can confirm that Red Herring was granted access to your Google account or remove that access if needed. <https://admin.google.com/ac/owl/domainwidedelegation>

Admin
☒ Enable
☐ Disable

7 apps, 7 users

| Filters | App Name | App Id | App Type | Permissions | Users ▼ |
|--------------------------------|----------------------|--------|-----------------|-----------------------|---------|
| API Permission Admin ▼ | Securly | | Web Application | Admin | 3 ⋮ |
| App Name Enter App Name | Quickstart | | Web Application | Admin | 2 ⋮ |
| User Count Greater than ▼ 0 | Quickstart | | Web Application | Admin | 1 ⋮ |
| | GoGuardian | | Web Application | Admin | 1 ⋮ |
| | Google APIs Explorer | | Web Application | Admin, Cloud Platform | 1 ⋮ |
| | RedHerring | | Web Application | Admin | 1 ⋮ |
| | RedHerring | | Web Application | Admin | 1 ⋮ |

RESET
SEARCH

Groups

Red Herring is designed to only send emails to groups and not individual users, although a group can have just one person. From the Groups page, you can quickly see how many members are in each group and quickly edit a group’s name or delete it.

Groups

+ Create Group

Search...

Drag a column header and drop it here to group by that column

| Name | Description | Risk Score | Members | |
|-------------------------------|--------------------------|---------------------------------|-------------|---|
| High Risk Score | System Group | High [Risk Score: 91.08] | 15 | |
| Medium High Risk Score | System Group | Medium High [Risk Score: 50.43] | 47 | |
| Medium Low Risk Score | System Group | Medium Low [Risk Score: 27.54] | 340 | |
| Low Risk Score | System Group | Low [Risk Score: 4.47] | 945 | |
| No Risk Score | System Group | Low [Risk Score: 0] | 1266 | |
| All COE Members | All active COE Employees | Low [Risk Score: 12.84] | 1392 | <div><div>Edit</div><div>Delete</div></div> |
| Testing | testing group | Low [Risk Score: 4.65] | 1 | <div><div>Edit</div><div>Delete</div></div> |

There are 5 system groups that are automatically populated with your target users as their risk score increases or decreases.

Create a Group

Click **Create Group**. Enter the **Name** and **Description** to create a group.

Create

Name

Description

Create



Cancel

Assign Target Users to the Group from the Groups page


Follow these steps to add a target user to a group or remove existing users from a group.


Assign (Add)


1. Click **Groups**.
2. Click **Detail** for the group that you would like to add a target user.

| Name ↑ | Description | Members | | |
|------------|----------------------|---------|---------------|---|
| Ali's Test | A test group for Ali | 12 | Detail |  Edit  Delete |


3. In the middle of the screen, click **Assign target users to group**.



 **Target Users in Groups**



 **Assign target users to group**

 **Remove target users from group**

4. Select the user(s) to add from the dropdown menu. Then click **Assign**.

Assign target users to group 

Assign

Remove

Check the box next to a user(s) and then click the **Remove target users from group** button to remove users from it.

Assign Target Users to a Group from the Target Users page

From the Target Users page you can assign individual or multiple users to one or more pre-existing groups.

Method 1: Manually select users (checkboxes)

Click the checkbox to the left of a user's name, then click **Assign target users to group**. Select one or more groups to assign the user to. **TIP:** To find a user who is not listed on Page 1, set the page view to **All** (at the bottom of the screen). Once all records are showing, use the **Last Name** or **First Name** filter to easily find the user. Note that the filters are to the right of the field name.

The screenshot shows the Target Users page interface. At the top, there are four buttons: '+ Create Target User', 'Export to Excel', 'Assign target users to group' (highlighted with a black box and an arrow pointing to it), and 'Delete'. Below the buttons is a text prompt: 'Drag a column header and drop it here to group by that column'. The main table has four columns: 'Last Name' (with an upward arrow), 'First Name' (with a downward arrow), 'Email' (with a downward arrow), and 'Phone' (with a downward arrow). The first row of the table is highlighted in blue, and its first checkbox is checked (highlighted with a black box and an arrow pointing to it). At the bottom of the page, there is a pagination control showing '1' in a box, and a dropdown menu set to 'All' (highlighted with a black box) with the text 'items per page'.

Method 2: Assign ALL users to a group

Set the page view to **All** (at the bottom of the screen). Once all records are showing, click the checkbox at the top of the screen, directly to the left of Last Name. This will select all records – you will see checkboxes next to all names. Click **Assign target users to group**. Select one or more groups to assign the users to.

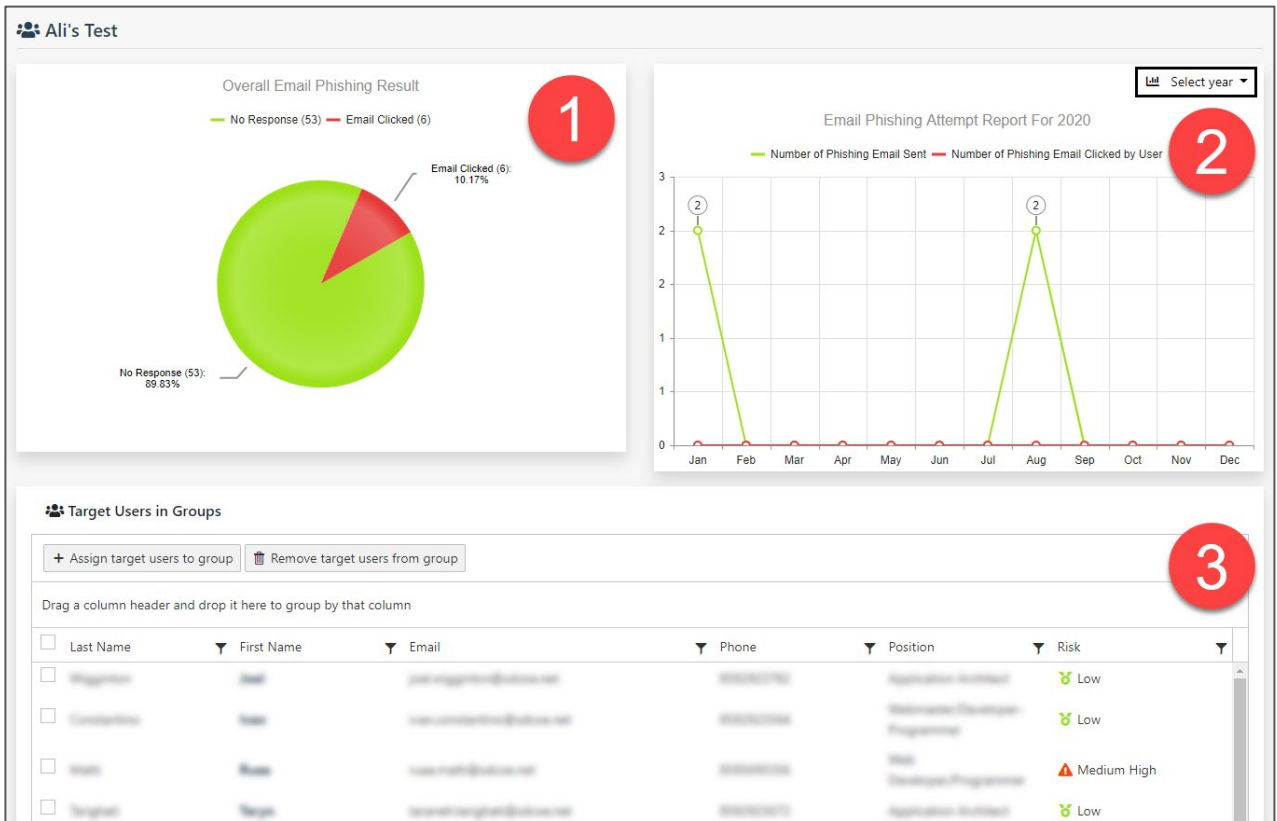
The screenshot shows the Target Users page interface with all records displayed. At the top, there are four buttons: '+ Create Target User', 'Export to Excel', 'Assign target users to group' (highlighted with a black box and an arrow pointing to it), and 'Delete'. Below the buttons is a text prompt: 'Drag a column header and drop it here to group by that column'. The main table has four columns: 'Last Name' (with an upward arrow), 'First Name' (with a downward arrow), 'Email' (with a downward arrow), and 'Phone' (with a downward arrow). The first row of the table is highlighted in blue, and its first checkbox is checked (highlighted with a black box and an arrow pointing to it). Above this checkbox, the text 'SELECT ALL' is written in large, bold, black letters. Below the first row, there are several more rows, each with a checked checkbox in the first column. At the bottom of the page, there is a pagination control showing '1' in a box, and a dropdown menu set to 'All' (highlighted with a black box) with the text 'items per page'.

View Group Analytics

1. Click **Groups**.
2. Click **Detail** for the group that you would like see group analytics.

| Name ↑ | Description | Members | | |
|------------|----------------------|---------|---------------|--------------|
| Ali's Test | A test group for Ali | 12 | Detail | Edit Delete |

3. View the analytics.



- 1 Pie Chart:** Shows the overall results for how many users in the group received the email and opened the phishing link. Shows the number of emails and the percentage. In this example 10.17% of the group clicked the email (shown in red in the pie chart).

- 2 Line Graph:** Shows the total click-thrus by date. Notice you can set the year at the top-right of this graph.

Target Users in Group: Shows a list of the target users in this group.

- 3**
 - **Sort:** Click any column header to sort the column (ascending/descending sort).
 - **Filter:** Click a column filter to the right of a field name to filter the column. Example: To see all High and Medium High risk, filter the Risk column by entering Contains = High.
 - **Drill Down:** Click a user's first name to drill down and view results for just that user. NOTE: You can also drill down on a user's details from the Target Users page by clicking their last name.

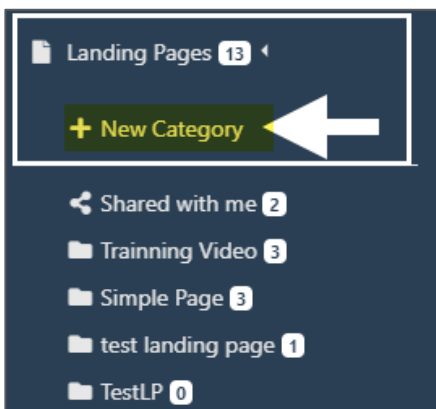
Landing Pages

When a user clicks on a link in one of your phishing messages, they are sent to a landing page. The URL to the landing page includes identifiers that enable Red Herring to track which users click on phishing messages.

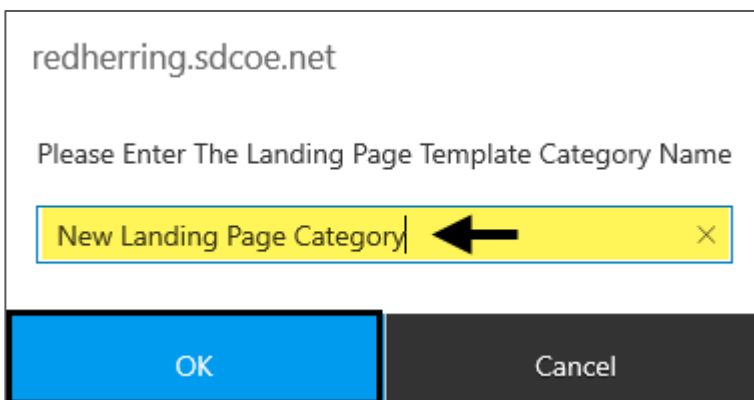
Create a New Category

Categories act like folders to help you organize similar landing page templates.

1. Expand the **Landing Page Templates** menu. Click **New Category**.



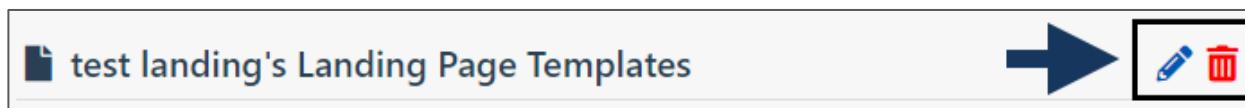
2. Name the category. *Examples: Alert Pages, Cybersecurity Awareness Pages, HR Pages*

A screenshot of a dialog box for naming a category. The top part shows the domain 'redherring.sdcoe.net'. Below that is the instruction 'Please Enter The Landing Page Template Category Name'. A text input field contains 'New Landing Page Category' and is highlighted with a yellow background, with a black arrow pointing to it. At the bottom, there are two buttons: 'OK' (blue) and 'Cancel' (dark grey).

3. Click **OK**.

Rename/Delete a Category

You can rename or delete a category by using the icons to the far right of the category name.



Create/Edit a Landing Page Template

4. Click the **Create a New Landing Page Template** button for a new template. Or click **Edit** to edit one of your existing landing page templates.

test landing's Landing Page Templates

+ Create New Landing Page Template

| Name | Shared | Created Date | | | |
|-------------------|-------------------------------------|--------------|---------|------|--------|
| test Landing Page | <input checked="" type="checkbox"/> | 07/24/2019 | Preview | Edit | Delete |
| Test L page | <input type="checkbox"/> | 06/01/2020 | Preview | Edit | Delete |

1 - 2 of 2 items

5. Enter a **Name** for the Landing Page Template. This name is just for your reference and will be displayed on the Category page.

Landing Page Template

Name

Test Landing Page

Category

Demo

☐ Share

Tags

#Help Desk × #Informational ×

B I U abc

Format ▾

(inherited font) ▾

(inherited size) ▾

A ▾

T

B

Insert landing page body here.

Cancel

Save

6. **OPTIONAL:** Click the **Share** checkbox if you would like to make this landing page template public (shared) to all Red Herring users across all organizations.

Edit the Landing Page Body

To enter or modify the landing page body, use the included text editor. Hover over the text editor buttons to get a pop-up description of what each button does.

B I U abc

Format
 (inherited font)
 (inherited size)

NOTES:

- Click the **View HTML </>** button to view HTML code or copy in from another source.
- Many of our shared templates have commented out notes to help you customize them after cloning. You may use a free WYSIWYG HTML editor to help customize these landing pages.

<https://www.freeformatter.com/html-formatter.html> - will auto indent to make the code easier to read


<https://www.tiny.cloud/> - free account needed

<https://www.html5-editor.com/> - free account needed
<https://htmlg.com/html-editor/> - free and ready to use

- You cannot upload files or images. You would have to host them on an external site and link to them using the **Insert Image** or **Insert File** buttons.
 - Or convert an image to Base64 code: <https://codebeautify.org/image-to-base64-converter>

Special Buttons: Landing Page Template Editor

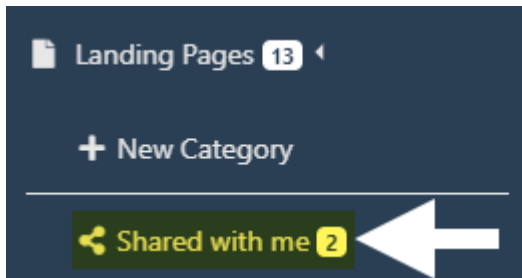
There are a few special buttons in the editor ribbon:

- 1 **Insert Video:** Displays a pop-up that will let you insert a video URL and specify the size of video. Video has a tracking mechanism that will know if a user started video and completed it.
 - 2 **Link to Landing Page:** Inserts a weblink with tracking mechanism that will know if a user navigated to a webpage.
 - 3 **Text Box:** Inserts a text box with tracking mechanism that will know if a user inputted any data inside text box. (user input is not recorded)
 - 4 **Button:** Inserts a button with tracking mechanism that will know if user clicked it.
 - 5 **Knowledge Assessment:** Opens a pop-up with a drop-down list that allows you to insert a quiz. A static box with a non-gradable preview of quiz questions will then appear in the editor. The full quiz is best viewed by clicking on the landing page link in a test email.
 - 6 **Organization Assets:** Inserts a code that will automatically populate the page with your organizational info that was saved to the **Configuration > Settings** page.
- 

Clone URL: Opens a pop-up where you can enter the URL of a webpage that you would like to copy. This function may or may not work based on the security protections of the webpage being cloned.

Shared Landing Pages (Public)

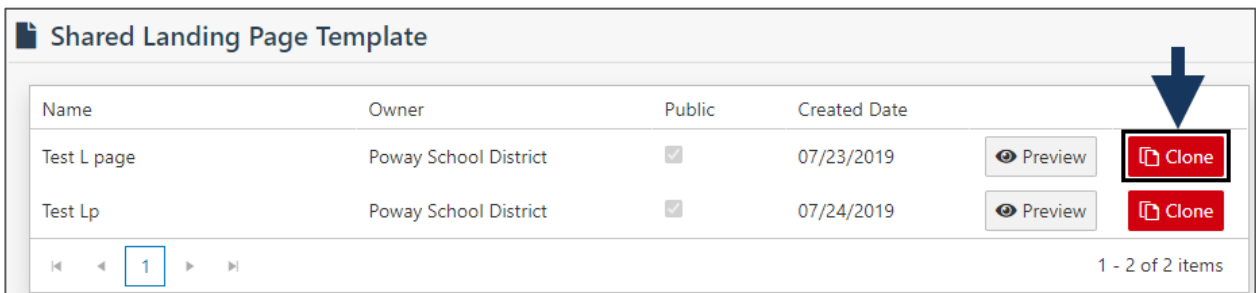
Expand the Landing Pages section and click **Shared with me** to access public landing pages. Public means another user clicked the “Share” checkbox. You will be able to see the organization owner of the shared landing template.



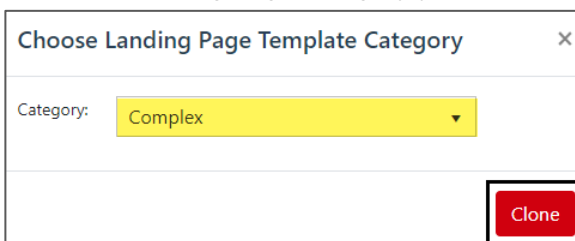
Clone a Shared Landing Page

You can clone a shared (public) landing page to modify for your own purposes.

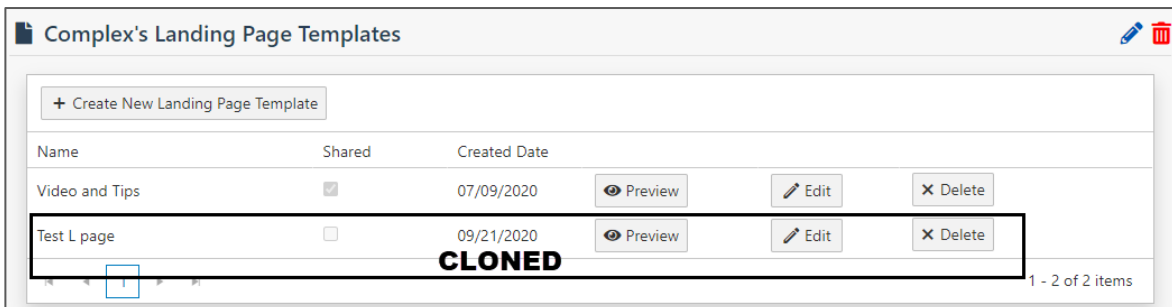
1. Navigate to **Landing Pages > Shared with me**.
2. Find the landing page you would like to clone. Click **Clone**.



3. Select the landing page category you would like to clone to. Click **Clone**.



4. The cloned landing page will appear in your specified category. Edit as desired.



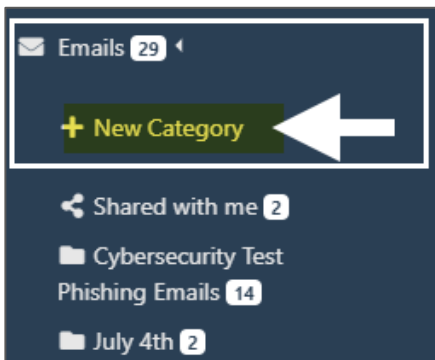
Email Templates

Email templates are the phishing emails that will be sent to your users.

Create a New Email Templates Category

Categories act like folders to help you organize similar templates. By clicking on a category, you can see what email templates are available, their complexity ratings, and creation dates, as well as preview and edit them.

1. Expand the **Email Templates** menu. Click **New Category**.



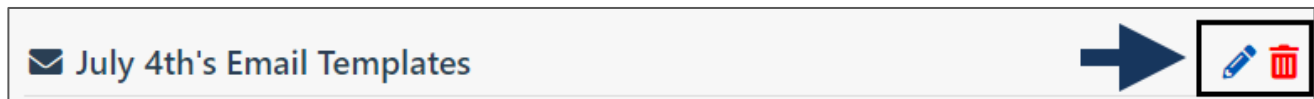
2. Name the category. *Examples: Vendor Emails, Industry Emails, Impersonation Emails*

A screenshot of a dialog box titled 'redherring.sdcoe.net'. It contains the text 'Please Enter The Email Template Category Name'. Below this text is a yellow input field containing the text 'New Email Category' with a black arrow pointing to it. At the bottom of the dialog are two buttons: 'OK' (blue) and 'Cancel' (grey).

3. Click **OK**.

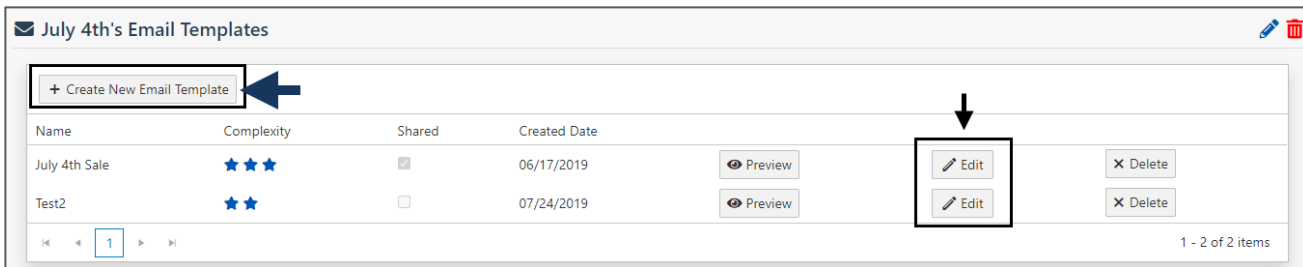
Rename/Delete a Category

You can rename or delete a category by using the icons to the far right of the category name.



Create/Edit an Email Template

1. Click the **Create a New Email Template** button for a new template. Or click **Edit** to edit one of your existing email templates.

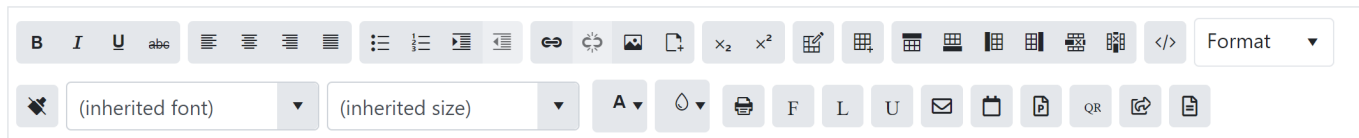


2. Enter the details for the template.

- **Name:** Enter the name of the Email Template. This name is just for your reference and will be displayed on the Category page.
- The rest of the information you enter will be the fictional information needed for the phishing message.
- **Sender Email Prefix:** Add the prefix of the email address that you would like to use, the domain portion will be selected by either using the Send Email feature or when you create a new campaign from the Campaigns page. For example: by setting the email prefix to accounts and choosing aditisecurity.com when you create a campaign, the email that the target user receives will then show the sender as accounts@aditisecurity.com.
- **Share (OPTIONAL):** Click the **Share** checkbox if you would like to make this email template public (shared) to all Red Herring users across all organizations.

Edit the Email Body

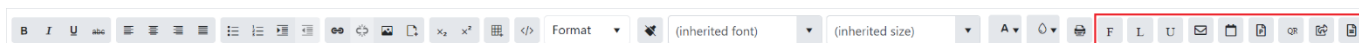
To enter or modify the email body, use the included text editor. Hover over the text editor buttons to get a pop-up description of what each button's purpose.



NOTES:

- Click the **View HTML </>** button to copy in HTML code from another source or customize the HTML.
- You cannot upload files or images to the system. You would have to host file or images on an external site and link to them using the **Insert Image** or **Insert File** buttons.

Special Buttons – Email Template Editor



First and Last

The email editor has two special buttons – **First** and **Last** – that allow you to enter a variable code that will automatically enter the first and/or last name of the recipient you are sending the email to. This allows Red Herring to send multiple emails to different recipients from one email template while having the target user's individual name in the body of each email.

| Email Template | Phishing Email Sent to Recipient |
|-------------------------------|----------------------------------|
| Hello {firstname} {lastname}, | Hello Jane Doe, |
| Hello {firstname} {lastname}, | Hello Joe Public, |

Insert target user's username and email address

This will insert a variable code that will automatically enter the username (prefix of email address) or the full email address of the recipient you are sending the email to. This allows Red Herring to send multiple emails to different recipients from one email template while having the target user's email address in the body of each email.

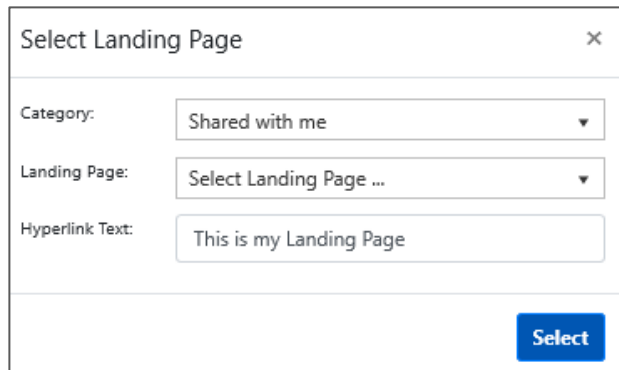
| Email Template | Phishing Email Sent to Recipient |
|------------------------------------|---------------------------------------|
| Hello {username} of {emailaddress} | Hello jdoe of jdoe@my.org |
| Hello {username} of {emailaddress} | Hello joe.public of joe.public@my.org |

Insert current date

This will insert a variable code that will automatically enter the current date. This allows Red Herring to send multiple emails to different recipients from one email template while having the current date in the body of each email without having to update the email template each day you send the campaign out.

Coded Hyperlink and QR Code

These special buttons that the email editor has enters a specially coded hyperlink to the landing page or a QR Code that points to a landing page. The token in each link is changed for each recipient when Red Herring sends each email. If a recipient forwards the email to other people and those persons click on the link, Red Herring will see multiple clicks by the same user. If you would like to attach the landing page hyperlink to an image, you would first have to click the button to create a text hyperlink, then copy the code over to the image via the HTML </> editor.



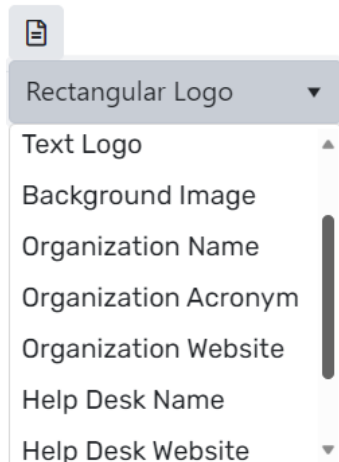
A dialog box titled "Select Landing Page" with a close button (X) in the top right corner. It contains three input fields: "Category:" with a dropdown menu showing "Shared with me", "Landing Page:" with a dropdown menu showing "Select Landing Page ...", and "Hyperlink Text:" with a text input field containing "This is my Landing Page". A blue "Select" button is located at the bottom right.

Insert a Forward Header to Email Template

This will make the email look like it is being forwarded from another user. This is useful in training your employees to inspect the entire email for suspicious indicators and not to just trust the sender of the forwarded email.

Organization Assets

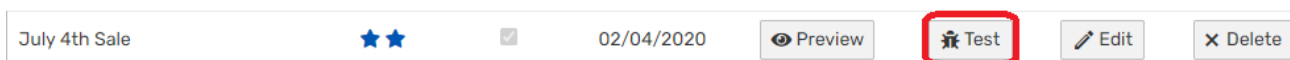
This will insert a variable code that will automatically enter your organizational info found under **Configuration > Settings** menu. This allows Red Herring to send multiple emails to different recipients from one email template while having organizational branding in the body of each email.



A dropdown menu with a document icon at the top. The menu is currently open, showing a list of organization assets: "Rectangular Logo", "Text Logo", "Background Image", "Organization Name", "Organization Acronym", "Organization Website", "Help Desk Name", and "Help Desk Website".

Test an Email Template

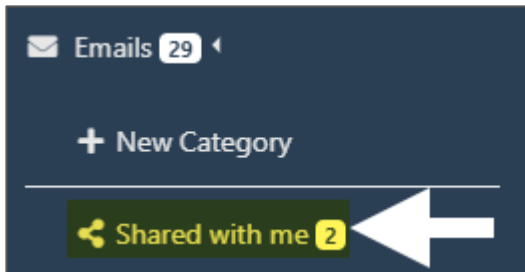
While in the Email Category view you may click the **Test** button next to an Email to automatically get sent the email to the email address associated with your Red Herring account so that you may ensure the Email can pass your mail filtering and that the Email, Landing Page with quiz or video is all working.



A horizontal action bar for an email template. It contains the following elements from left to right: the text "July 4th Sale", two blue stars, a checked checkbox, the date "02/04/2020", a "Preview" button with an eye icon, a "Test" button with a mail icon (highlighted with a red rectangle), an "Edit" button with a pencil icon, and a "Delete" button with an X icon.

Shared Email Templates (Public)

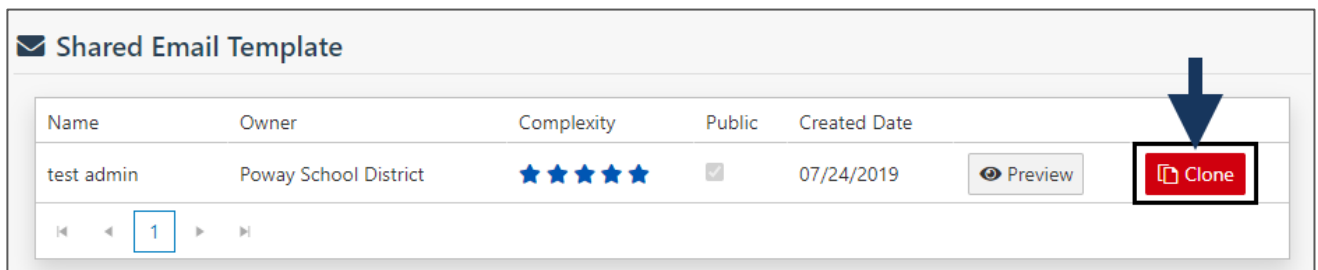
Expand the Emails section and click **Shared with me** to access public email templates. Public means another user clicked the “Share” checkbox. You will be able to see the organization owner of the shared template.



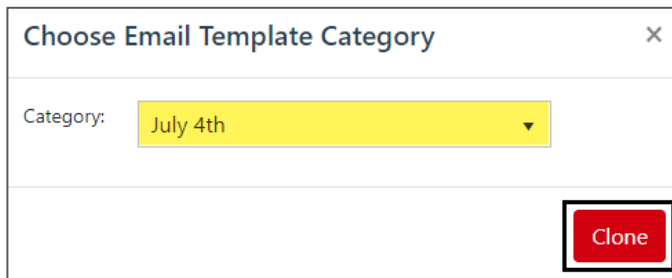
Clone an Email Template

You can clone a shared (public) email template to modify for your own purposes.

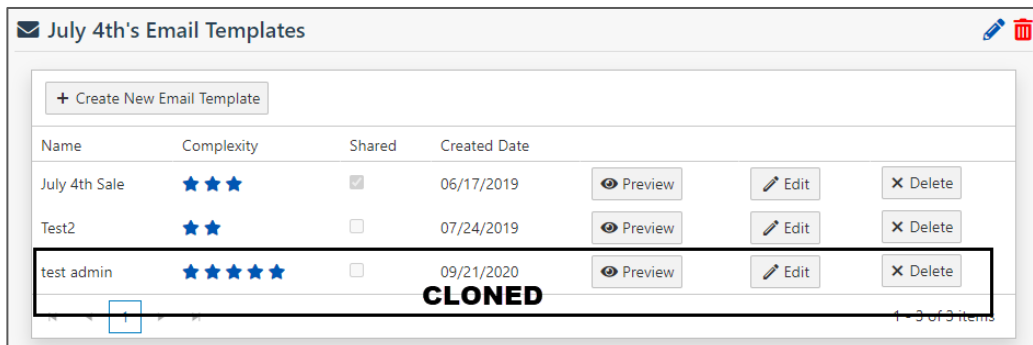
1. Navigate to **Emails > Shared with me**.
2. Find the email template you would like to clone. Click **Clone**.



3. Select the email category you would like to clone to. Click **Clone**.



4. The cloned email template will appear in your specified category. Edit as desired.

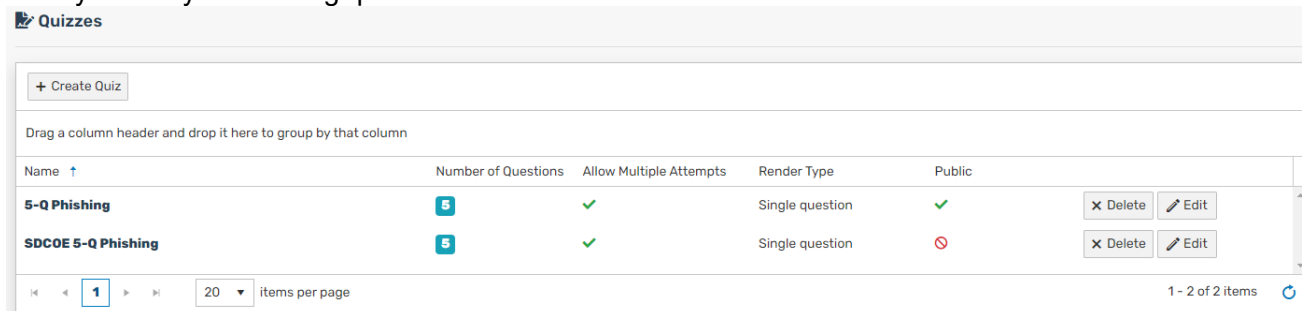


Knowledge Assessments (Quizzes)

Knowledge assessments are the quizzes that may be provided to your target users via a Landing Page. Refer to the **Edit the Landing Page Body** section under Landing Pages to find out how to insert a Quiz on a Landing Page..

Create/Modify a Quiz

1. Click the **Create Quiz** button for a new knowledge assessment. Or click on the **Edit** button to modify one of your existing quizzes.



2. Enter a **Name** for the Knowledge Assessment. This name is just for your reference.
 - Check **Allow Multiple Attempts** if the target user will be allowed to take the quiz multiple times or just once.
 - **Render Type**: This feature is currently unavailable.

Red Herring Notification

Name

Allow Multiple Attempts ☐

Render Type

Public ☐

- **OPTIONAL**: Click the **Public** checkbox if you would like to make this knowledge assessment public (shared) to all Red Herring users across all organizations (please ensure there are no quiz questions that are specific to your site).

Designing a Quiz

1. Click on the **title** of the quiz to create/delete questions and/or modify the existing quiz questions and answers for that selected quiz.
 - One or more answers can be marked with the green check mark to indicate that they are the correct answer.
 - Click on the three ellipses box to provide a training note (explanation) to the user that they will see after submitting their answer.
 - Click **+Add option** to provide another option to the target user for a correct or wrong answer, this can be deleted by selecting the trash icon next to the **Option** title.
 - Click the **+Add Question** box to add another question to the current quiz, this can be deleted by selecting the trash icon next to the **Question** title.
 - Click **Cancel** at the top right to exit without saving your changes.
 - Click **Save** at the top right to save your changes and exit.

The screenshot displays the '5-Q Phishing' quiz design interface. At the top, there is a header bar with the title '5-Q Phishing' and buttons for 'Cancel' and 'Save'. The main content area contains two question cards. Each card has a title, a list of options, and controls for marking correct answers, adding options, and deleting the question.

Question 1: Is SPAM the same as phishing?

- Yes
- No

Question 2: What should I check in an email to ensure that it is valid?

- Cookies
- Sender's email address and display name
- Misspellings or grammatical errors in message body and subject line
- Fishes
- Hover over links to see if it goes to a suspicious sounding website

At the bottom of the interface, there is a red button labeled '+ Add Question'.

Phishing Campaigns (Scheduled)

The Campaign section sends the Email Template to a group of users at a scheduled time.

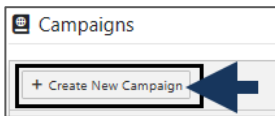
View Your Campaigns

You may view the scheduled and completed campaigns from the Campaigns page along with scheduled and completion dates, current status, and the option to view the full report for each completed campaign.

| Campaigns | | | | | | | |
|---|-------------------------|-------------------------|-------------|-------|----------------|-------------|--------|
| + Create New Campaign | | | | | | | |
| Drag a column header and drop it here to group by that column | | | | | | | |
| Name ↓ | Scheduled Date | Completed Date | Delay (sec) | Group | Email Template | Status ↓ | |
| Test | 10/22/2019: 10:00:00 PM | 10/22/2019: 10:00:32 PM | 1 | 1 | 1 | ✓ Completed | Report |
| October 31 2019 | 10/31/2019: 12:00:00 AM | 10/31/2019: 12:05:16 AM | 1 | 1 | 3 | ✓ Completed | Report |
| October 27 2019 | 10/27/2019: 10:00:00 PM | 10/22/2019: 10:28:16 AM | 1 | 2 | 1 | ✓ Completed | Report |
| October 27-2 2019 | 10/27/2019: 12:00:00 AM | 10/27/2019: 12:05:25 AM | 1 | 1 | 1 | ✓ Completed | Report |
| October 2019 Frequent flyers | 10/17/2019: 12:30:00 PM | 10/17/2019: 12:31:58 PM | 2 | 1 | 1 | ✓ Completed | Report |
| Trial Run | 10/08/2019: 07:30:00 AM | 10/08/2019: 04:28:50 PM | 1 | 1 | 1 | ✓ Completed | Report |

Create a New Phishing Campaign

1. At the top of the Campaigns page, click the **Create New Campaign** button.



2. Enter the details for this campaign.

Campaign Detail

Campaign Name



User Groups

Domain for email and landing page URL



Email Template Category

Email Template

Frequency

Start date
  

Delay (Seconds)

 Save  Back To Campaign List

- **Campaign Name:** Give the campaign a title for your reference only
- **User Groups:** Add one or more user groups
- **Domain for email and landing page URL:** Choose a domain to be used in the Landing Page's URL and added to the Sender's Email Prefix that was chosen for that specific email template. For example; if you choose aditisecurity.com from dropdown, the sender's spoofed email address will show {prefix}@aditisecurity.com and the link in message body will show www.aditisecurity.com/LandingPage/... when a target user hovers over the landing page link.
 - i. Each custom domain is hosted with our cloud provider and has a SPF and DKIM record.
(List of IP address and domains to allowlist is in SMTP section p.6.)
- **Email Template Category:** Add one or more email template categories
- **Email Template:** Add one or more email templates. NOTE: If you add multiple email templates to a campaign, Red Herring will send each user a randomly selected email template from the ones you selected.
- **Frequency:** Choose Once for a one-off campaign or select any of the other options for a recurring campaign.
- **Start Date:** Choose a scheduled date for the campaign to automatically run
- **End Date:** Choose an end date for the last campaign to run (recurring campaigns only)
- **Delay (Seconds):** Please have at least a 1-second delay in the sending of emails to the recipients in the campaign settings

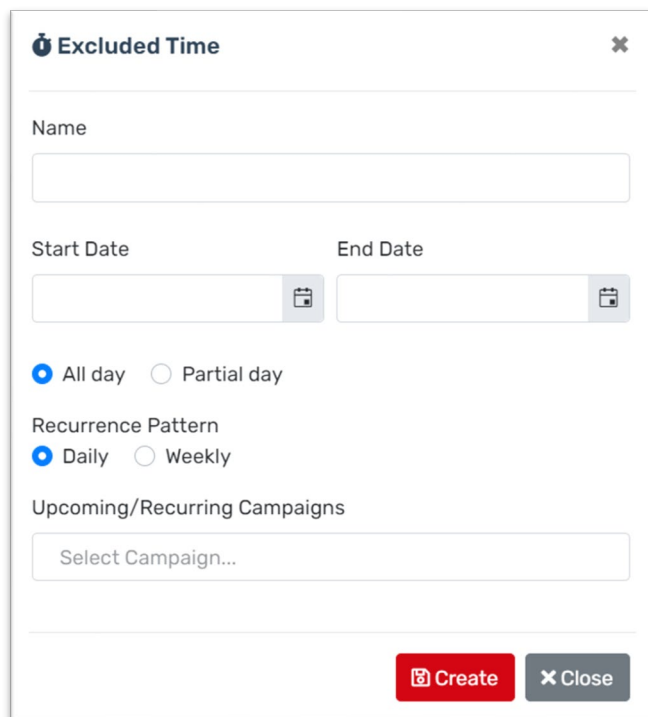
3. Click **Save**.

Excluded Time

Excluded Times can be used to pause any campaign that is in progress during certain hours. This can be used when sending a campaign to a large number of users to prevent emails from being sent after work hours. Or you may set an excluded time for a planned system outage or maintenance window.

The option to add an excluded time is available from either the Settings or Campaigns pages:
Configuration > Settings > Excluded Time or Campaigns > Excluded Time

1. Click the **+Add Exclusion Time** to create a new exclusion period.
2. Give it a name, Start Date and End Date
3. Select whether the whole day will be excluded or just part of the day.
 - a. For Partial Day choose the timeframe to be excluded.
4. Select whether you would like to exclude the selected timeframe daily or weekly.
 - a. For Weekly, select the day of week to the selected timeframe.
5. Use the dropdown to exclude All campaigns from running during the Excluded Time or a specified campaign.
6. Click **Create**



The screenshot shows a modal window titled "Excluded Time" with a close button (X) in the top right corner. The form contains the following fields and options:

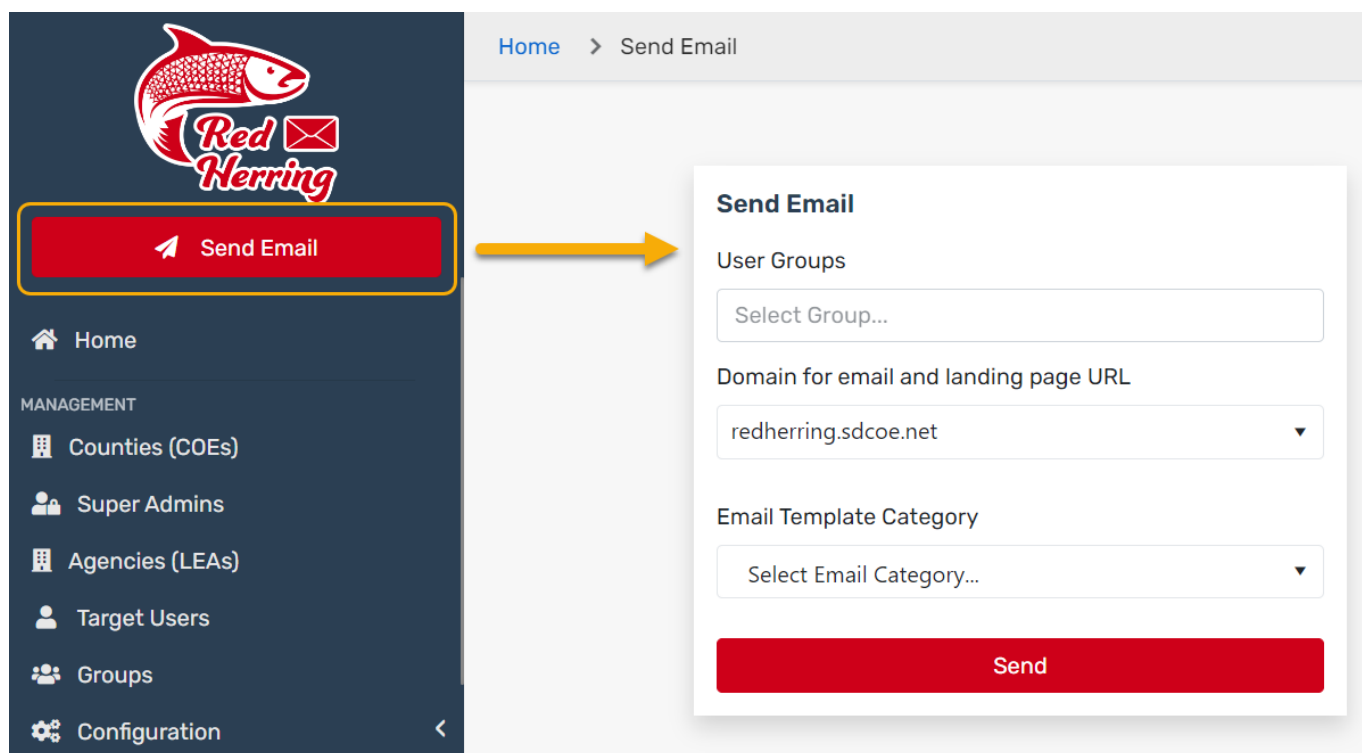
- Name:** A text input field.
- Start Date:** A date picker field with a calendar icon.
- End Date:** A date picker field with a calendar icon.
- Day Selection:** Two radio buttons: "All day" (selected) and "Partial day".
- Recurrence Pattern:** Two radio buttons: "Daily" (selected) and "Weekly".
- Upcoming/Recurring Campaigns:** A dropdown menu with the placeholder text "Select Campaign...".
- Buttons:** A red "Create" button and a grey "Close" button at the bottom right.

Send a Phishing Email (Ad Hoc)

You can easily send an email from the main page by clicking the **Send Email** button under the Red Herring logo. This function is especially helpful in testing or verifying that you set up an email as desired.

NOTE: You will not be able to view the stats of these phishing emails like the Results in the Campaign page. You'll instead have to find the user in the Target Users page to see if they clicked on a phishing link or view the details page for the group that the user belongs to.

- **Domain for email and landing page URL:** Choose a domain to be used in the Landing Page's URL and added to the Sender's Email Prefix chosen for that email template. For example; if you choose aditisecurity.com from dropdown, the sender's spoofed email address will show {prefix}@aditisecurity.com and the link in message body will show www.aditisecurity.com/LandingPage/... when a target user hovers over the landing page link.
 - Each custom domain is hosted with our cloud provider and has a SPF and DKIM record. (List of IP address and domains to allowlist is in SMTP section p.6.)



View your Emails Sent

You may view the sent emails from the Emails Sent page along with the completion dates, current status, and the option to view the full report for each sent email.

To send an email, click the Send New Email button at the top left of the Emails Sent page.

To prevent emails from running during a certain time, click the Excluded Time button at the top of the Campaigns page.

- Click the number in the Group or Email Template column to quickly view the Group(s) that the email was sent to or the Email Template(s) that was used.
- Click the bar graph symbol to view the results and metrics gathered from the sent email.
- To delete a Sent Email, click the Delete button to the right of the Sent Email's record. A prompt will appear asking if you are sure you would like to delete.
NOTE: Deleting a Sent Email will also delete any Target User actions (telemetry)/score associated with that Campaign.
- You can filter any column that has a filter icon.

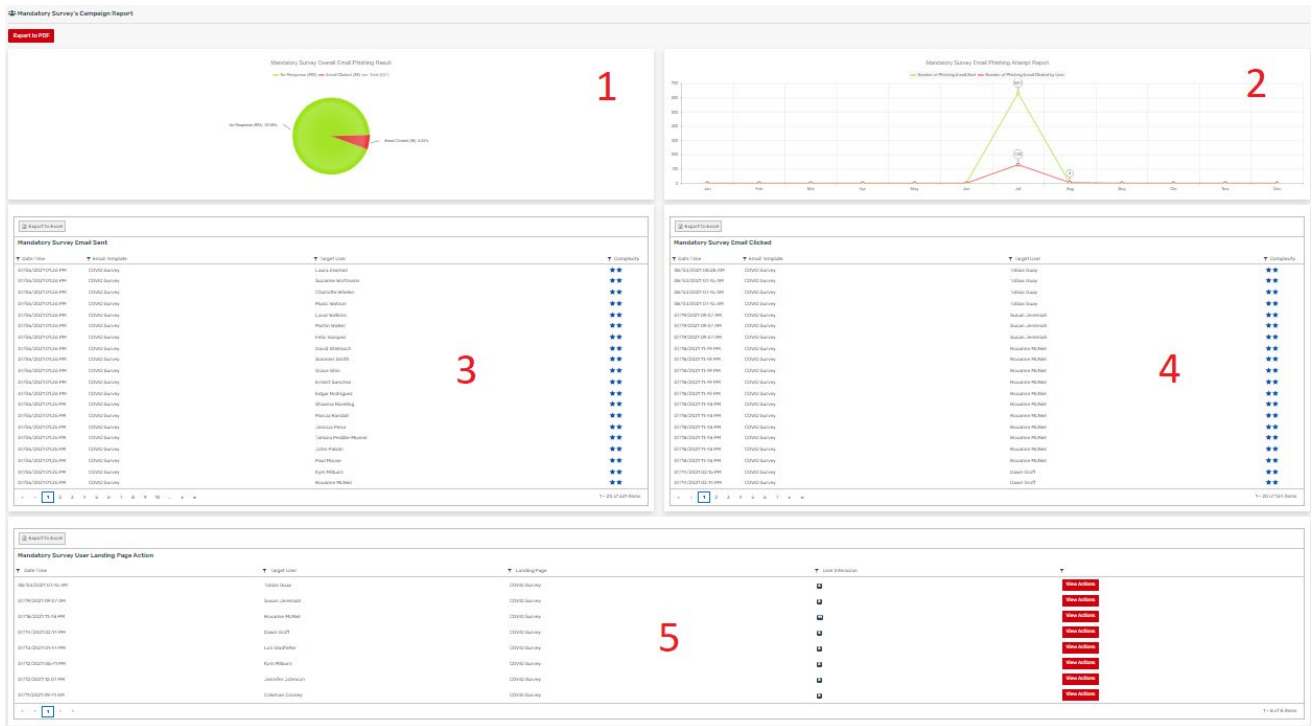
Reports and Analytics

Campaign Results Report

- From the Campaign page, select the **Report** button to view the results of a completed phishing campaign.

Mandatory Survey 07/06/2021: 01:11:00 PM 07/06/2021: 01:26:16 PM 1 2 1 Completed 630/630 Report Delete

- View the results.



- 1 Pie Chart:** Shows the overall results for how many users received the email and opened the phishing link. Shows the number of emails and the percentage. In this example 6.02% clicked the email (shown in red in the pie chart).

- 2 Line Graph:** Shows the total click-thrus by date.

- 3 Email Sent:** Shows a list of users to whom the phishing email was sent, and which email template was sent, if applicable. You can export this list to Excel.

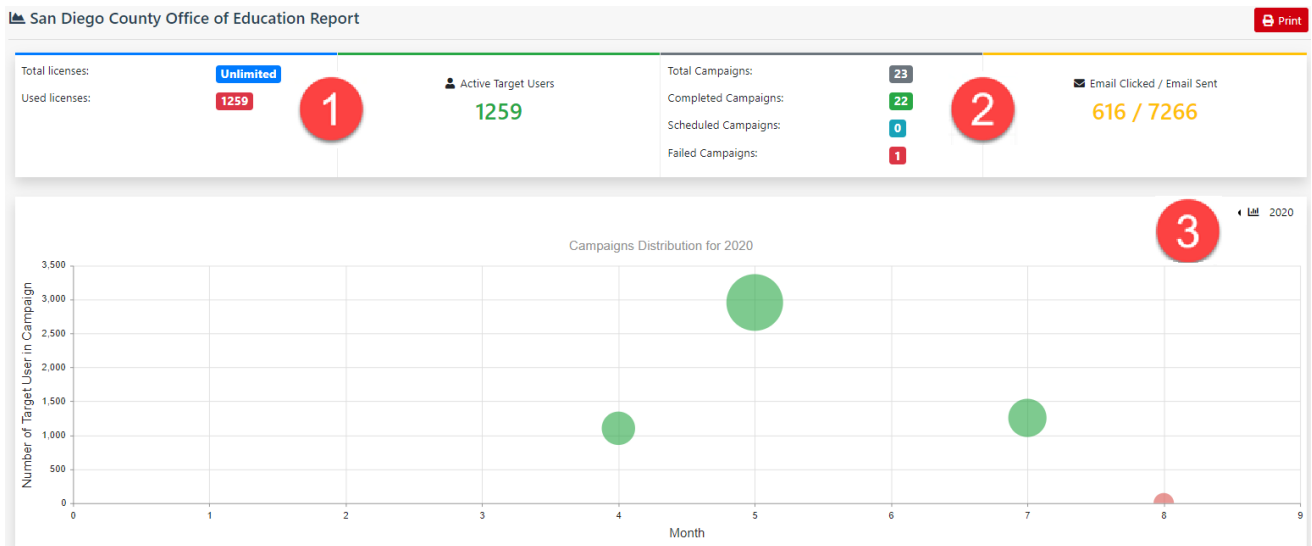
- 4 Email Clicked:** Shows a list of users who clicked the phishing email link. You can export this list to Excel.

- 5 User Landing Page Action:** Click the **View Actions** button next to user for more details on user activity such as if they viewed a training video or completed a quiz.

NOTE: Click Export to PDF for a multi-page report. Or press Ctrl+P to print the page.

District Report

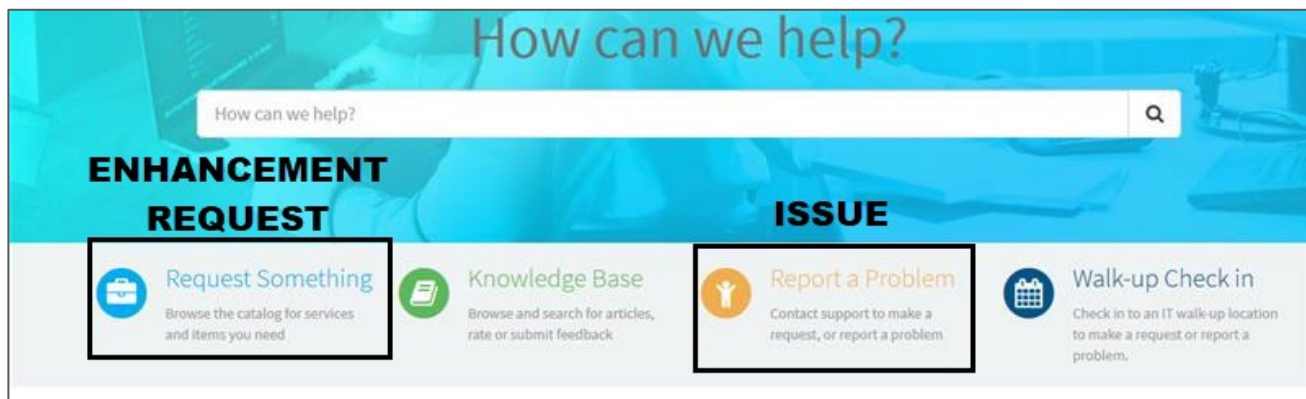
- From the left navbar, select **Report** then the **District Report** button to view the overall and annual report on your district's Red Herring usage.



- Upper Left:** Shows your **Total Licenses** and **Used Licenses**. If your Used Licenses exceed your Total Licenses, then SDCOE will be in contact with you to help remedy the overage. You may need to delete some users or delete all users then resync your users to get rid of any expired users or only load the user groups that you would like to concentrate on.
Note: Deleted users will stay in the system for a year and their history will be shown if they're deleted and added back again.
- Upper Right:** Shows your overall totals since the time you started using Red Herring.
- Lower Section:** Selecting the dropdown for the year will display the Red Herring usage for a certain year.

Support

Many support resources can be found at: cybersecurity.sdcoe.net > Red Herring



As part of your Red Herring on-boarding process you will be given an account on SDCOE's ServiceNow customer support platform. There will only be one authorized user per agency (district or COE) that will be able to submit ServiceNow requests to SDCOE. Districts that are on Red Herring through their COE will have to report the issue directly to their COE's Red Herring representative.

1. Go to ServiceNow at <https://sdcoe.service-now.com>.
2. If you are a new user and are awaiting a ServiceNow account or forgot your password, you may click on the **Forgot Password** link and enter your email to get a password sent to you if you are in the system.
3. After logging in, click **Report a Problem** if you need assistance with an issue or something is not working properly. Or click **Request Something** to submit a feature request.

Report a Problem

Report a Problem is for help with resolving a problem that you are experiencing in Red Herring.

1. Enter your incident.

Create Incident

Request assistance or report an issue you are having

Submit

Request assistance with an issue you are having. An Incident will be created and managed through to successful resolution. You will also be notified of progress. To add attachments now or after submission, simply drag and drop them onto the form, or press the paper clip in the upper right.

I am having trouble with

*Short description ?

*Please provide your location ?

*Please provide your work phone number ?

Additional comments & information ?

Add attachments

PICK ONE:

- Red Herring - User sync issues
- Red Herring - Administration issues
- Red Herring - Configuration issues

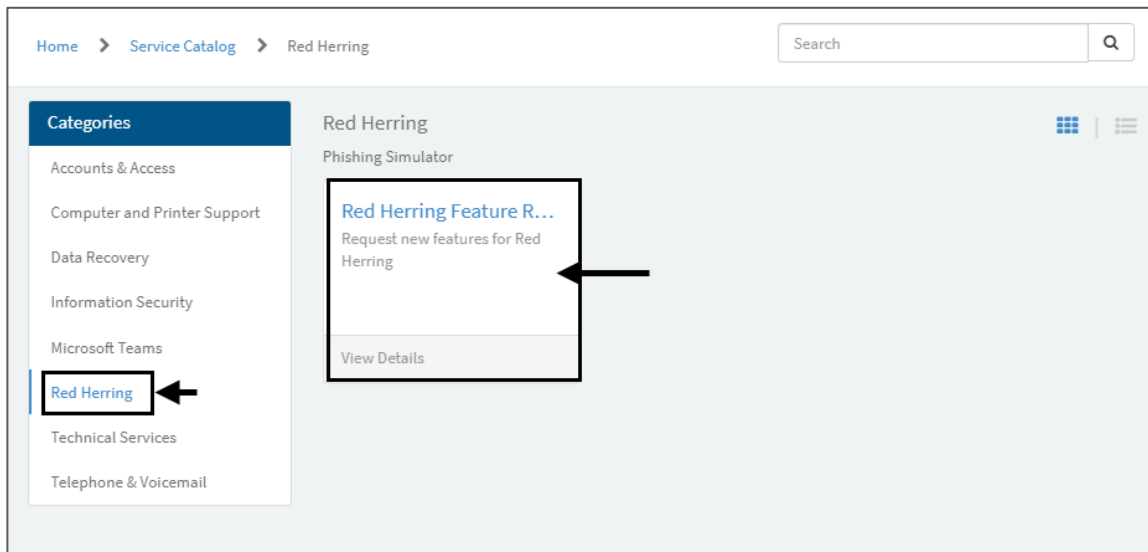
- **I am having trouble with:** Select one of the Red Herring options.
 - **Red Herring - Administration issues:** User Log-In, Email or Landing Page Templates, Reports
 - **Red Herring - Configuration issues:** SMTP Configuration, Email problems, Campaign, Groups, Video Playback
 - **Red Herring - User Sync issues:** Problems with importing users from CSV, G-Suite, On Premises AD, and Azure
- **Short description:** Enter a short description, like a title
- **Location:** Typically your location is pre-populated. If not, please enter your district or COE.
- **Phone number:** Please enter a phone number where we can reach you.
- **Additional comments & information:** IMPORTANT: Please be descriptive and attach a screenshot of problem.
- **Add attachments:** Click here to upload a screenshot.

2. Click **Submit**.

Request Something

Request Something is for adding a new capability or feature that you think would make Red Herring better or easier to use.

1. Click **Red Herring** on the left (Categories).
2. Click **Red Herring Feature Request**.



3. Enter your request:

A screenshot of the 'Red Herring Feature Request' form. The form title is 'Red Herring Feature Request' with the subtitle 'Request new features for Red Herring'. It includes a 'Submit' button on the right. The form fields are: '* Requested for' (a dropdown menu), '* Short Description' (a text input field), '* Description of desired feature' (a larger text input field), and 'Additional comments' (a text input field). There is an 'Add attachments' button at the bottom right. On the right side of the form, there is a 'Required information' section with two tabs: 'Short Description' and 'Description of desired feature'.

- **Requested for:** Typically your name is pre-populated. If not, please enter it.
- **Short Description:** Enter a short description, like a title
- **Description of desired feature:** IMPORTANT: Please be descriptive and attach a screenshot of where you would like to see the change. If you can create a mockup, please include that.

4. Click **Submit**.

Sending a Test Campaign

Create Red Herring User Group

Red Herring has 5 groups that are automatically populated with your target users based on their Risk Score. 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.

1. Navigate to Red Herring > Groups
2. Select **+Create Group**
3. Name the group **Testing**
4. 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 our templates that have the **#LEA Branded** tag.

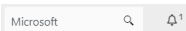
1. Navigate to Red Herring > Configuration > Settings
<https://redherring.sdcoe.net/Admin/settings>
2. Enter your organizational information under Agency Details
3. Upload your organizational logos under Agency Images
4. Click Save Profile

Create Red Herring Template Categories

Next we will create a folder to house the templates that we clone, modify or create. For the purposes of this guide we will name them Testing, you may choose a different name or rename them at any time. You may skip this step if you have already created a category for each content type.

1. Navigate to Red Herring > Emails > **+New Category**
2. Name it **Testing** and click **Ok**
3. Navigate to Red Herring > Landing Pages > **+New Category**
4. Name it **Testing** and click **Ok**
5. Navigate to Red Herring > Knowledge Assessments > **+New Category**
6. Name it **Testing** and click **Ok**

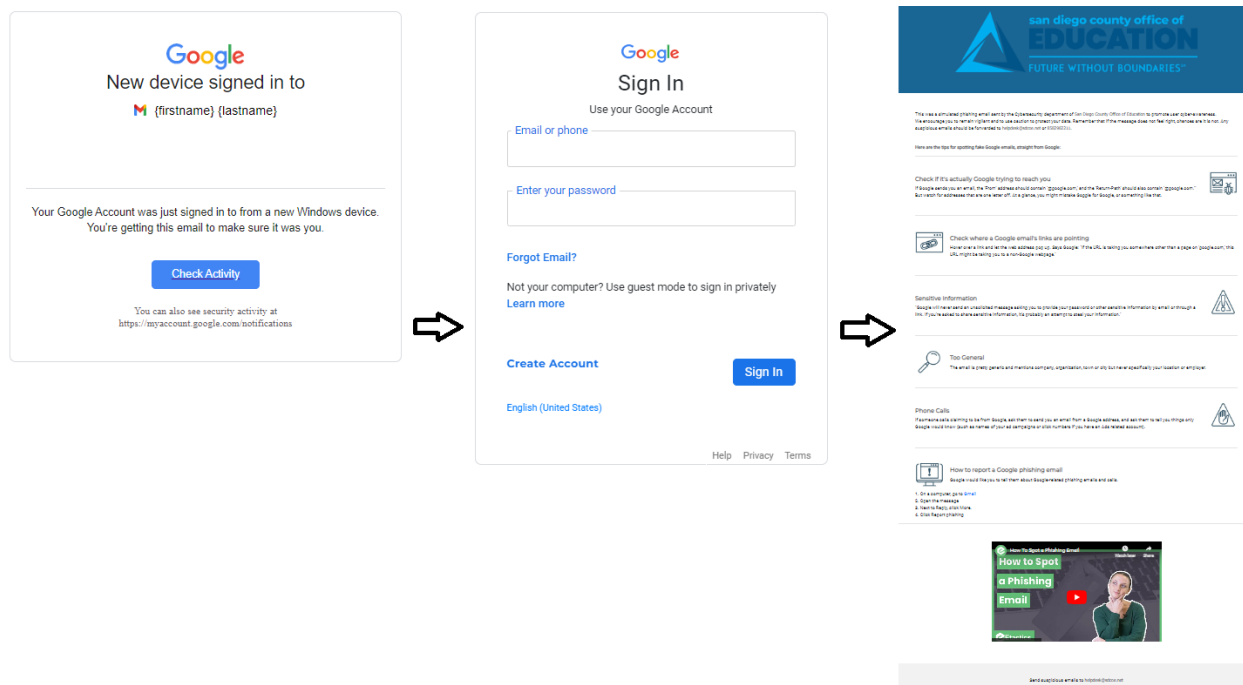
Clone a Red Herring User Email Template

1. Navigate to Red Herring
2. Search for Microsoft 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 Testing folder (an example of email to landing page click-path is on next page)
6. Optionally you check the box for Landing Page Templates and clone them so that you may customize them.
 - a. You will have to edit the link to the email template if you decide to clone and customize a landing page.

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 your negative Risk Score for clicking on that email campaign.

We suggest that you use the Campaigns menu when sending simulated phishing campaigns to your staff. All the Google/Microsoft email templates are configured to point to a shared Google/Microsoft Login page, if they enter their login credentials and click 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 Configuration > Settings page.

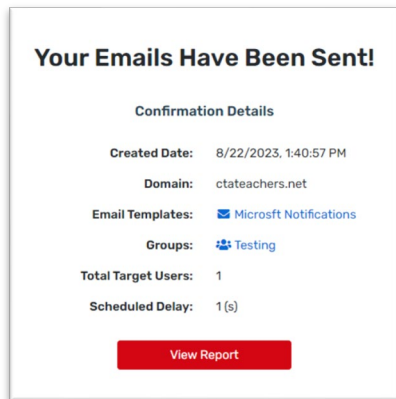


1. Navigate to Red Herring > Send Email
 - a. For User Groups select your Testing group
 - b. Choose one of the custom domains such as cteachers.net
 - c. For Email Template Category select your Testing category
 - d. Finally select the email to send and click Send

The 'Send Email' form includes the following fields and controls:

- User Groups:** A dropdown menu with 'Testing' selected.
- Domain for email and landing page URL:** A dropdown menu with 'cteachers.net' selected.
- Email Template Category:** A dropdown menu with 'Test' selected.
- Email Templates:** A dropdown menu with 'Microsoft Notifications' selected.
- Delay time for each email in second(s):** A numeric input field with the value '1'.
- Send:** A red button at the bottom of the form.

2. Find the email in your inbox
 - a. Click on any links in 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

| | |
|----------------|-----------------------------------|
| Email Sent | Microsoft - Shared File (OneNote) |
| Email Clicked | Microsoft - Shared File (OneNote) |
| Access Page | Microsoft Login |
| Button Clicked | Microsoft Login |

5. Delete the Email once 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

Campaign Detail

Campaign Name
Quarterly All-staff

User Groups
All Staff

Domain for email and landing page URL
ctateachers.net

Email Template Category
Credential Harvesting

Email Template
Microsoft Password Reset Microsoft - Shared File (Word)
MS Teams Activity Microsoft Security Alert

Frequency
Every 3 months

Start date
01/01/2024 12:00:00 AM

End date
12/31/2024 12:00:00 AM

Delay (Seconds)
1

Campaign will run every 3 months starting on 01/01/2024 12:00:00 AM until 12/31/2024 12:00:00 AM

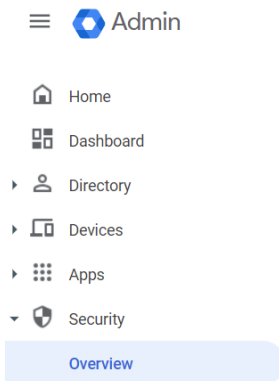
[Save](#) [Back To Campaign List](#)

Enable Google Less Secure Apps

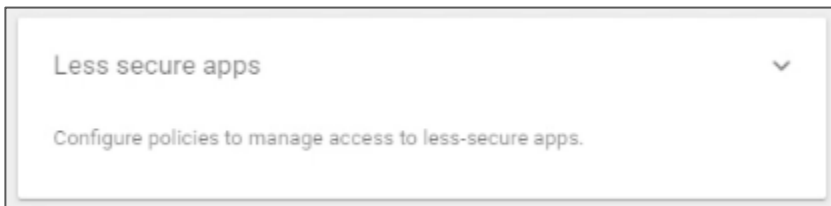
Follow these steps to allow Red Herring access to use Gmail as SMTP server. MFA will have to be turned off for the Google User Account or an App Password will have to be configured for Red Herring.

NOTE: Google may be phasing out this feature.

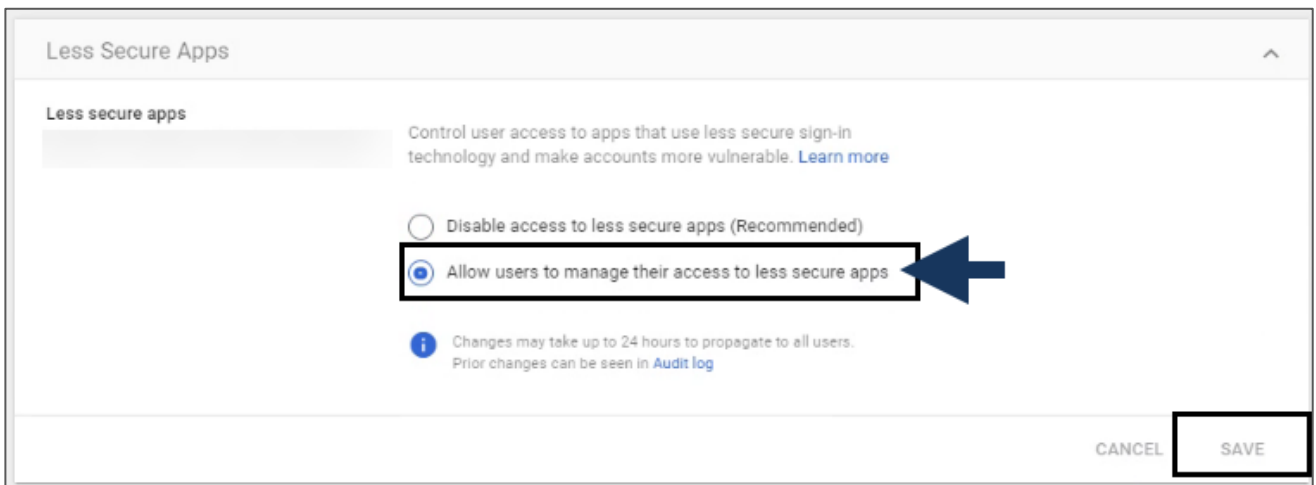
1. Log in to the Google Admin G-Suite account at admin.google.com.
2. On the Admin Console, expand the **Security** menu and then select **Overview**.



3. Expand the *Less secure apps* section. The direct link is <https://admin.google.com/ac/security/lsa>.



4. Select **Allow users to manage their access to less secure apps**.



5. Click **Save**
6. Next, enable Less Secure Apps for the account that will be used to send mail from Red Herring by navigating to the link below and changing the setting to “**Allow less secure apps: ON**”
<https://myaccount.google.com/lesssecureapps>
7. If an App Password is needed, that may be setup by navigating to:
<https://myaccount.google.com/signinoptions/two-step-verification>