Red Herring

User Guide

san diego county office of EDUCATION

FUTURE WITHOUT BOUNDARIES℠

Red Herring

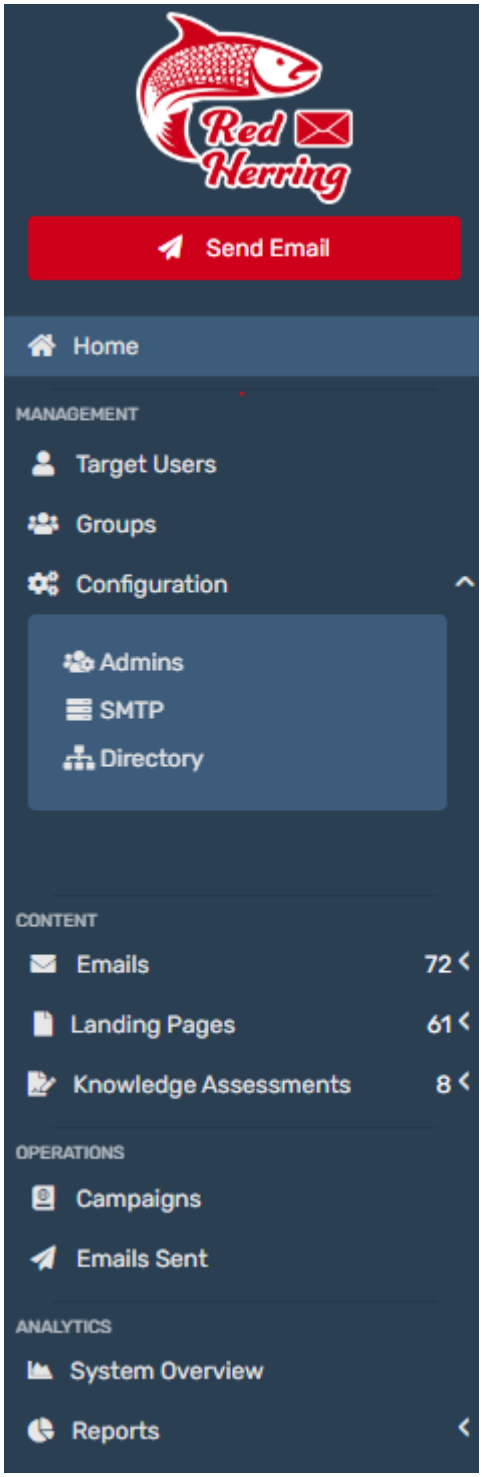
Overview

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.34.*

- **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.50.*

- **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.52.*

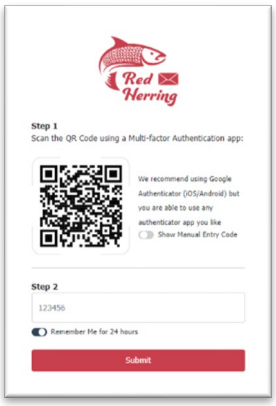
- **LEA Branded:** Any Landing Page or Email template that is tagged as LEA Branded will automatically display the custom information and images that you have configured in **Configuration > Settings**

- **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.58.*

- **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.65.*

MFA

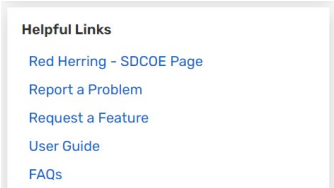
MFA via an authenticator app is now required to access the Red Herring admin portal. Users will be shown an MFA setup page on their next login. The MFA prompt can be bypassed for 24 hours after a verified login. Please contact cyberguardians@sdcoe.net if an MFA reset is needed.



Helpful Resources

The public SDCOE Cybersecurity webpage has multiple helpful resources that can be found at https://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.



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

These IP addresses and domains may need to be allowlisted on your email protection service to prevent them from being flagged as phishing or moved to the target user's quarantine inbox. Some domains may be temporarily unavailable if a threat database has flagged them as malicious.

192.40.172.4, 192.40.172.139, 20.118.176.15, 20.150.176.58

Generic Domains	Generic Domains	Regional Domains

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

Administrator Accounts

COE Administrator

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

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

1. Navigate to Agencies (LEAs)
2. Click **+Create Agency**
3. Fill in the LEA information
    a. Only assign the necessary amount of licenses to the LEA
    b. Expiration date can't be set passed your COE's expiration date
4. Click **Create**
5. Click the Agency (LEA) name to open the Agency details page and assign admins to it (see LEA Administrator). You may also add Notes for each Agency.

LEA Administrator

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

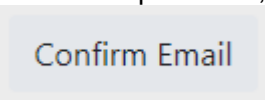
We currently have three LEA admin levels

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

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

- Create Admin - This will assign an admin to the Agency (LEA)

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



Settings

The Settings page has four sections; Profile, Notifications, Campaign Excluded Times and Impersonation.

Profile

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

The available text fields are:

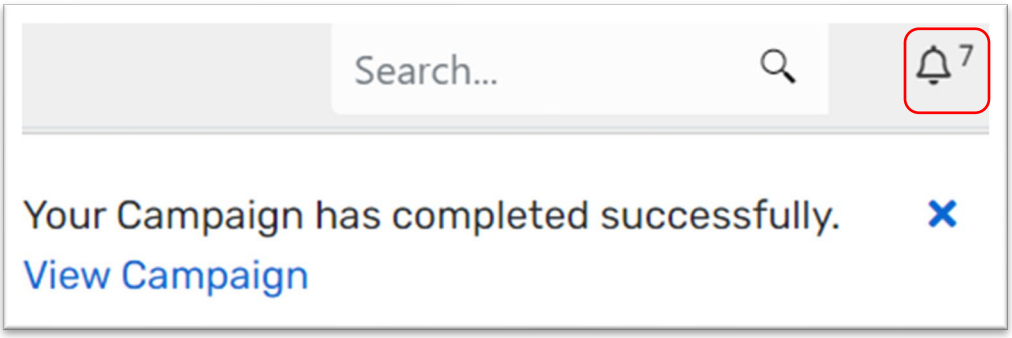
Name	Attribute	Notes
Organization Name	{orgname}	
Organization Website	{orgwebsite}	
Organization Acronym	{orgacronym}	
Help Desk Name	{helpdeskname}	
Help Desk Website	{helpdeskwebsite}	
Help Desk Phone Number	{helpdeskphone}	Only numbers are allowed
Help Desk Email	{helpdeskemail}	

The available logo/images are:

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

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

Notify me 2 months before my LEA's Account Expiration (COE only)

Content Notifications

Notify me when new Email Templates are made publicly available

Notify me when new Landing Page Templates are made publicly available

Notify me when new Knowledge Assessments are made publicly available

Campaign 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

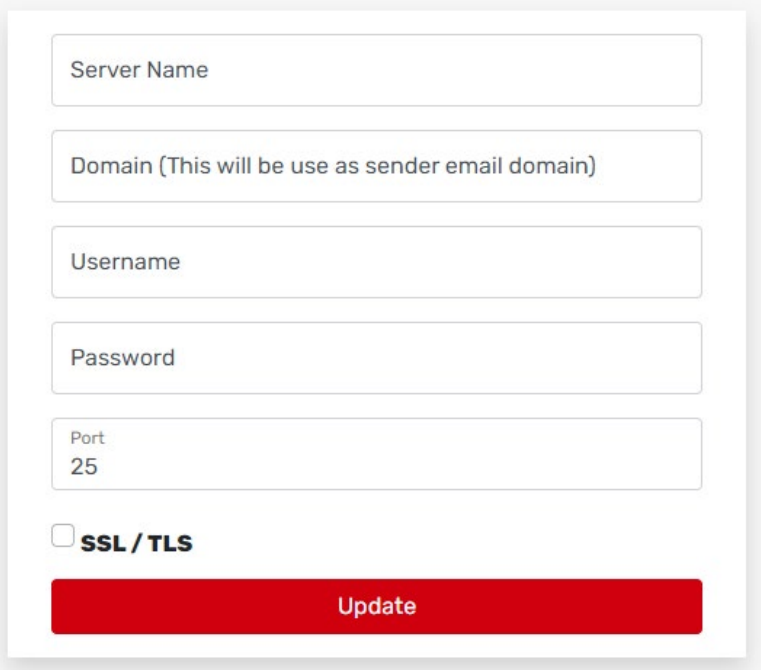
Impersonation (SDCOE Preview)

LEAs may allow their parent COE or SDCOE to impersonate their LEA admin account so that the COE may configure settings, view errors, create/modify templates, and manage campaigns on behalf of the LEA.

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.



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.68.

Sender Policy Framework (SPF)

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

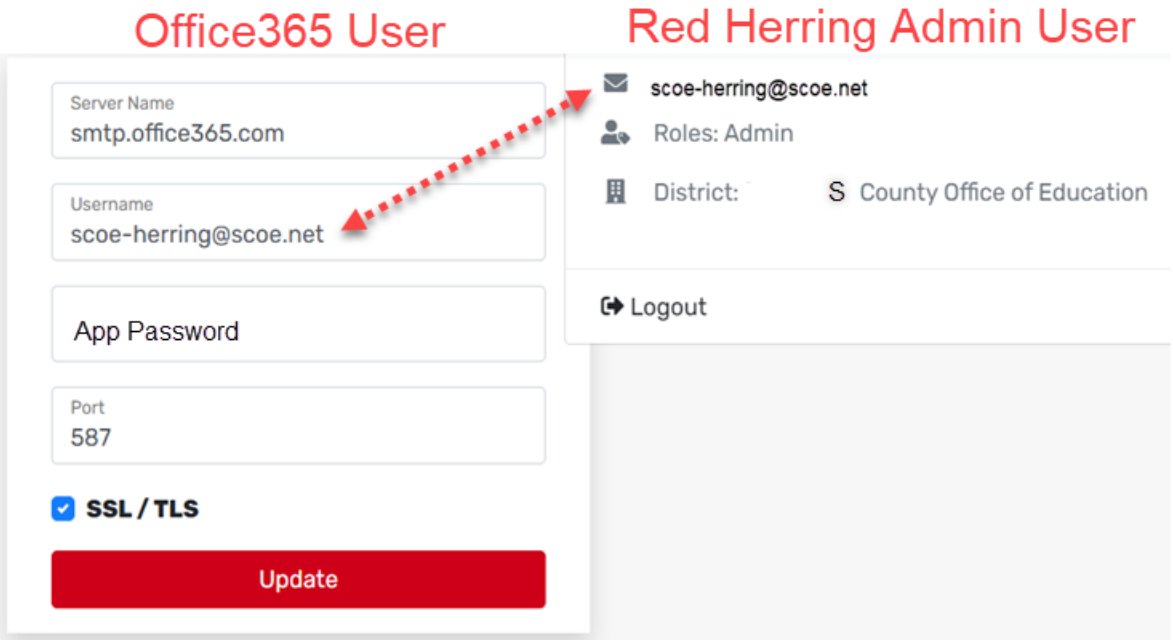
After you update your SPF records, we recommend that you send yourself a test phishing email that spoofs your email domain. If you have successfully added Red Herring to your SPF record, the email should not go to your spam folder or be flagged as malicious.

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.



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.68.

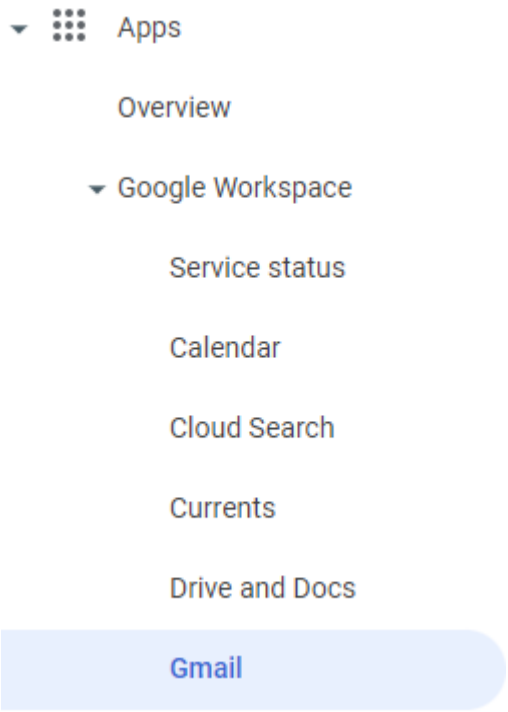
Google Gmail Allowlist & Gateway

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

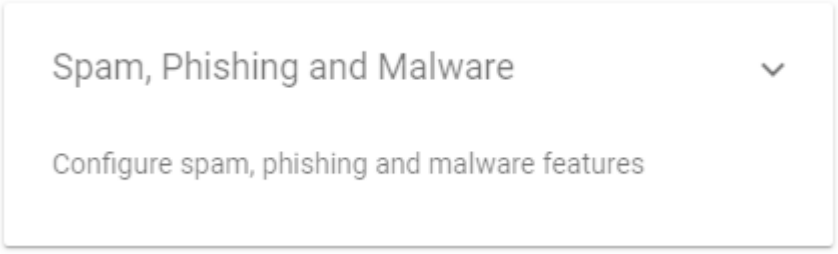
In Google Admin go to Apps > G-Suite > Settings for Gmail > Spam, phishing, and malware

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**

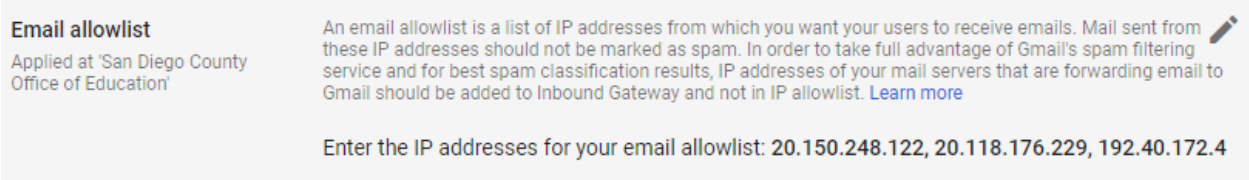


3. Scroll to the bottom of **Settings for Gmail** and select **Spam, Phishing, and Malware**



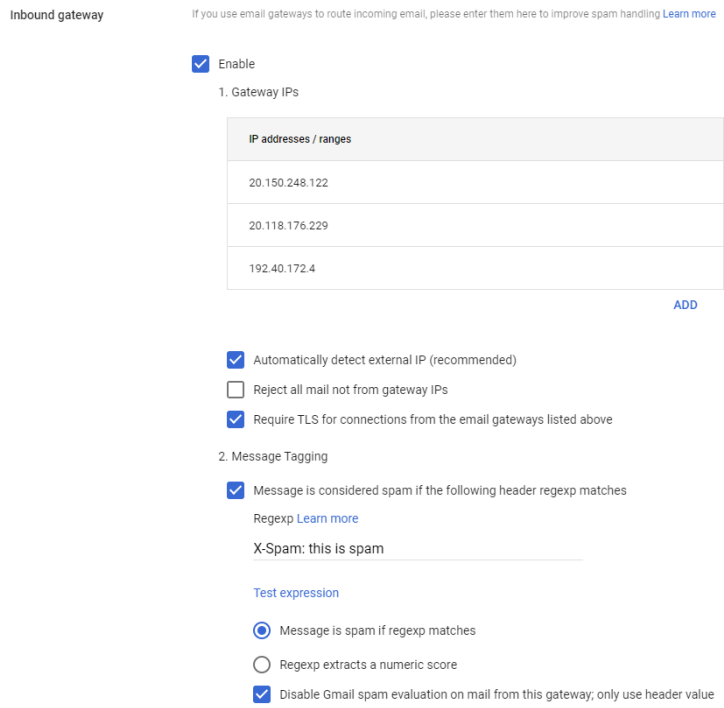
4. Under **Email allowlist** enter the following IP addresses separated by commas:

   192.40.172.4, 192.40.172.139, 20.118.176.15, 20.118.176.58



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

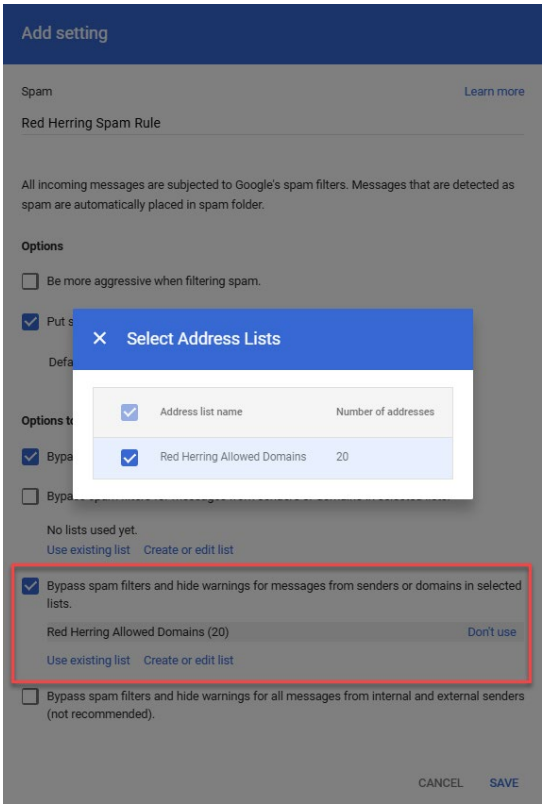
6. In the Inbound gateway settings
   a. Enter a short description: Red Herring email gateway
   b. Add the following gateway IPs
      192.40.172.4, 192.40.172.139, 20.118.176.15, 20.118.176.58
      Check **Automatically detect external IP**
   c. Check **Require TLS for connections from the email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



7. Lastly, find the Spam section and you can either edit your existing rule or click **CONFIGURE** to add your first spam rule.
   a. Name the rule: "LEA's Spam rule"
   b. Select the options based on how your organization wishes to handle spam.

Best practice is to check **Put spam in administrative quarantine** and to **Bypass spam for internal senders**. (Ignore this step if you're adding a dedicated spam rule for just Red Herring in addition to your existing organizational spam rule.)

c. Under **Options to bypass filters and warning banners**, check the box for **Bypass spam filters and hide warnings for messages from senders or domains in selected lists**.
d. Select **Create or edit list**
    i. On the new browser tab that opens, select **ADD ADDRESS LIST**
    ii. Name it "Red Herring Allowed Domains"
    iii. Click **BULK ADD ADDRESSES**
    iv. Add the domains that you plan to use in your Red Herring simulated phishing campaigns from:
    aditisecurity.com, edufinancial.org, countyofsd.net, ctateachers.net, edupointonline.com, sandiegocoe.net, highunion.net, glooglonline.com, sdc0e.net, schoolunified.net, gmailonline.us, sdcoes.net, servicecounty.net, infinite-campus.org, sdcounty.net, uniondistrict.net, microsoftsupport.us, sfcoe.org, peoplesoftsdcoe.com, sfusds.net, sdcoe.net
    v. Check **Require sender authentication**
    vi. Click **ADD**
    vii. Click **SAVE**
e. Return to the previous browser tab
f. Select **Use existing list** and check the box for "Red Herring Allowed Domains"
g. Select **SAVE**



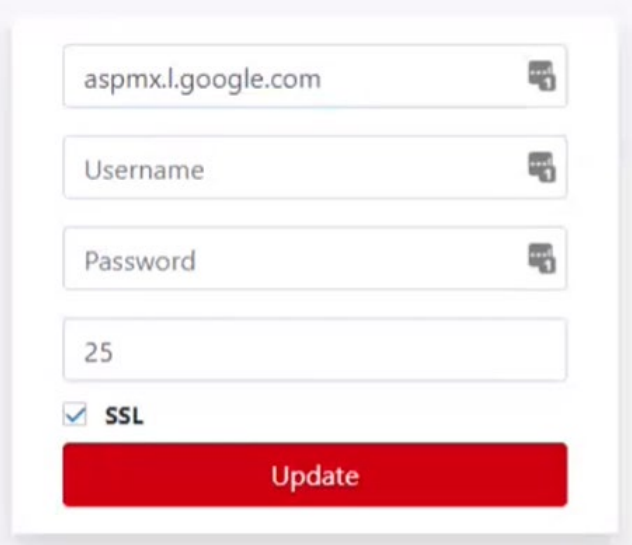
8. Return to Red Herring > Configuration > SMTP and enter aspmx.l.google.com for server name, 25 for port number, check SSL box, and leave username and password blank. Then click update and check your Gmail Inbox for an email from noreply@sdcoe.net.

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 Allowlisting** 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.



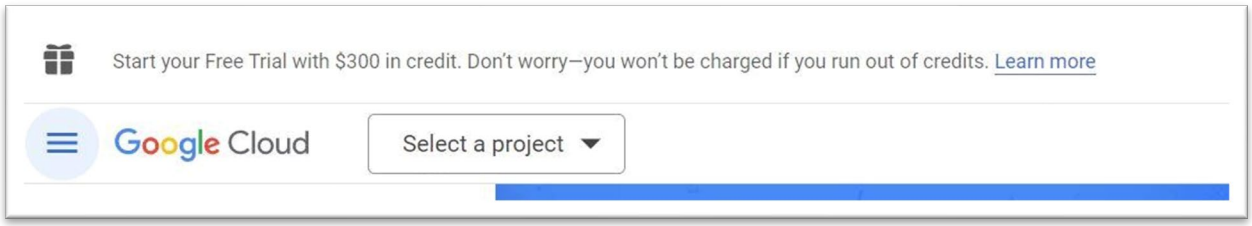
3. Click **Update**.
4. Check your Gmail Inbox for an email from noreply@sdcoe.net.
5. Click the confirm link with-in email.
6. Now test the connection. Refer to *Send a Phishing Email (Ad Hoc)* on p.68.

Google Service Account

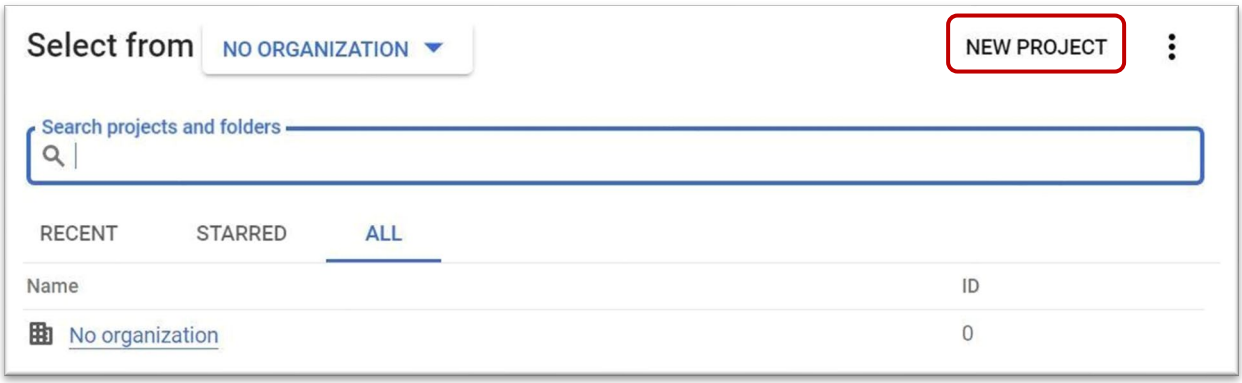
These directions will set up a Service Account in Google Cloud and Google Admin to allow you to import target users into Red Herring.

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

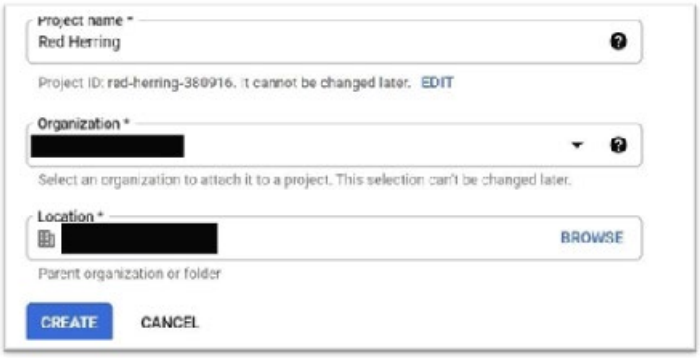
3. Select APIs and Services
4. On the top panel click **Select a project**



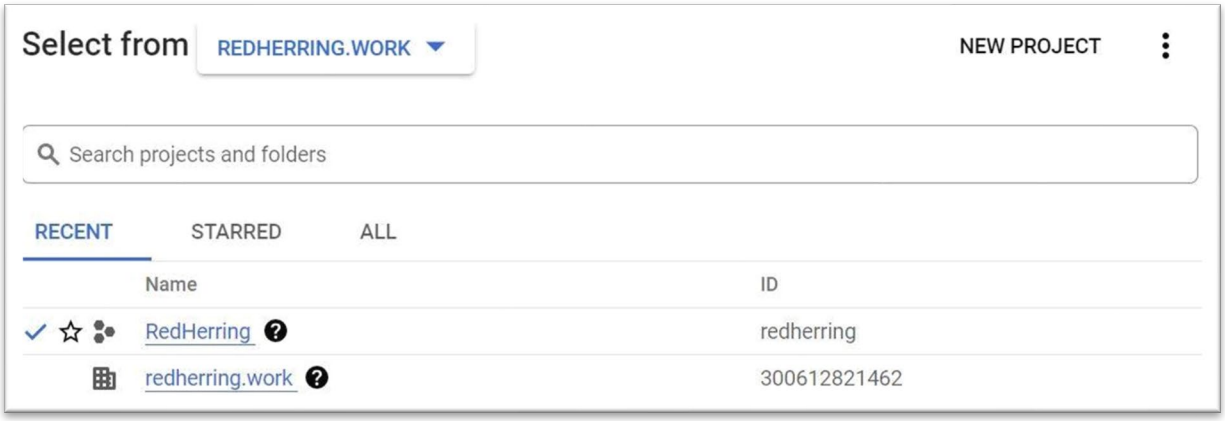
5. Create a **New Project**



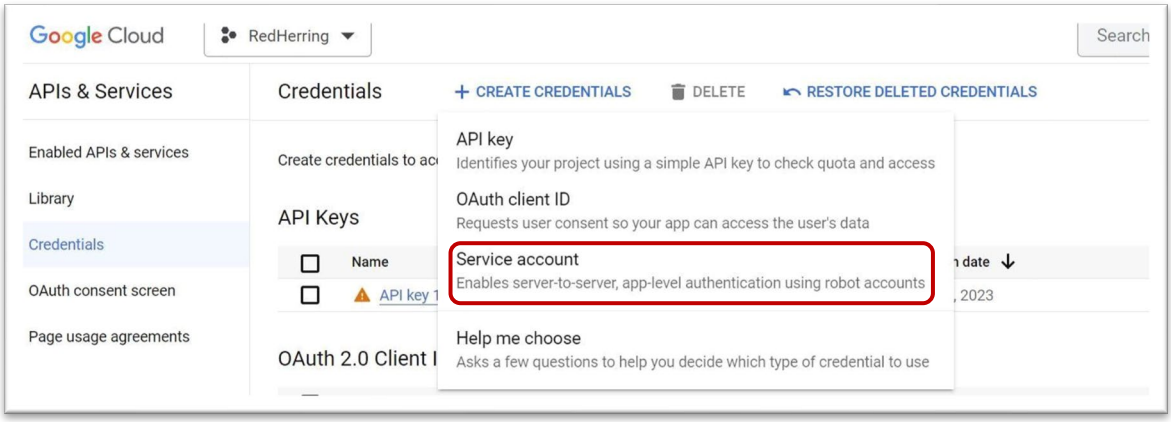
6. Choose your Organization and Location



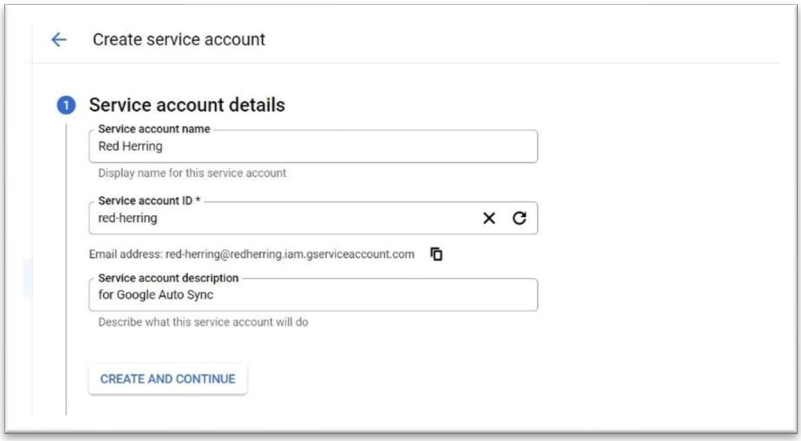
The project could take a while to complete. When the project is ready, it should be listed under your organization.



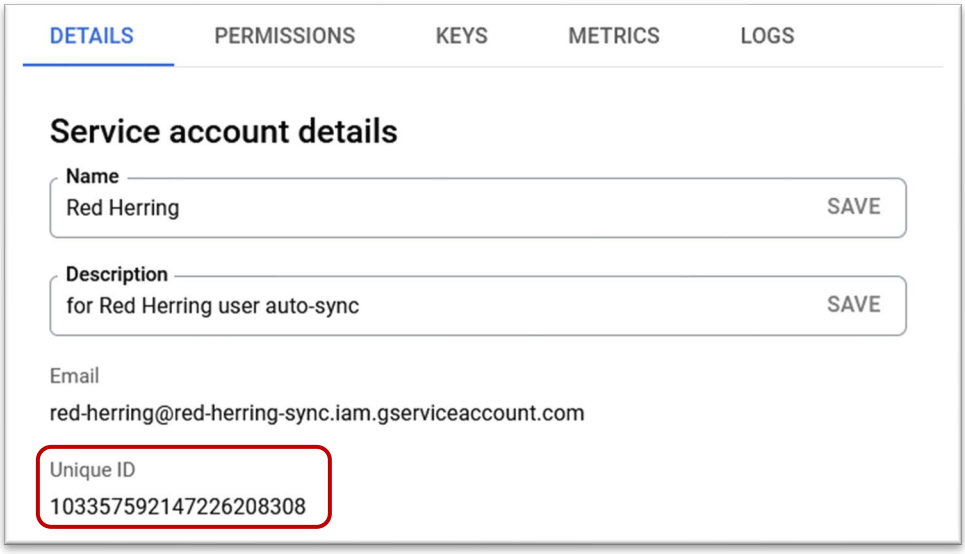
7. Select the project then click the Credentials menu on the left
8. In the Credentials page, click “Create Credential” and select **Service account**



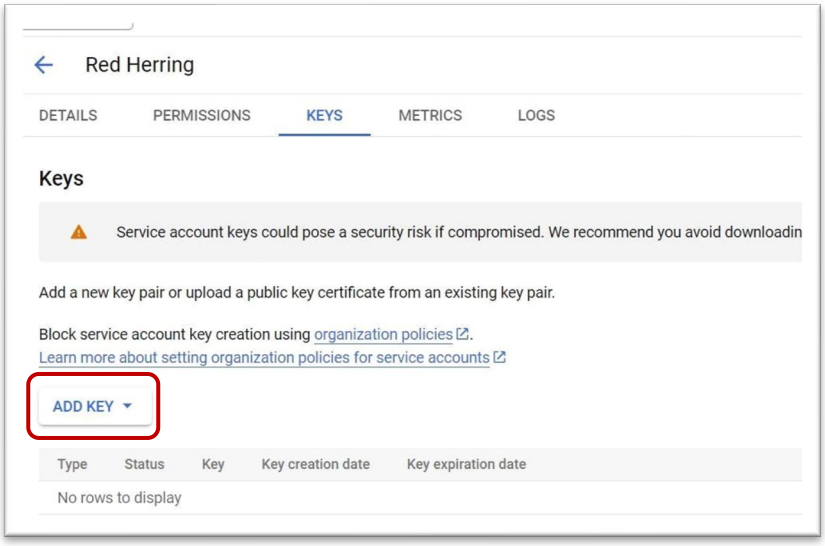
9. Input Service Account Information and click **Create and Continue** then accept the defaults and select **Done**



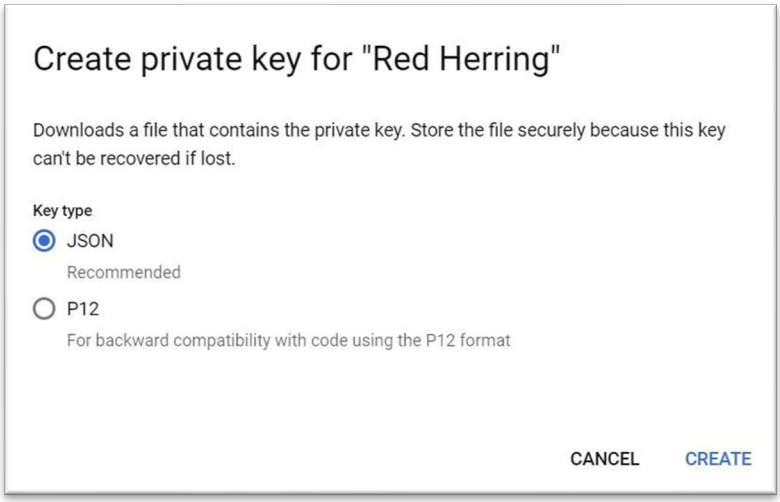
10. After creating the service account, copy the Unique ID from Details tab of the Service Account page Google Cloud > Service Accounts > IAM &Admin > Service Accounts > {Red Herring Service Account}



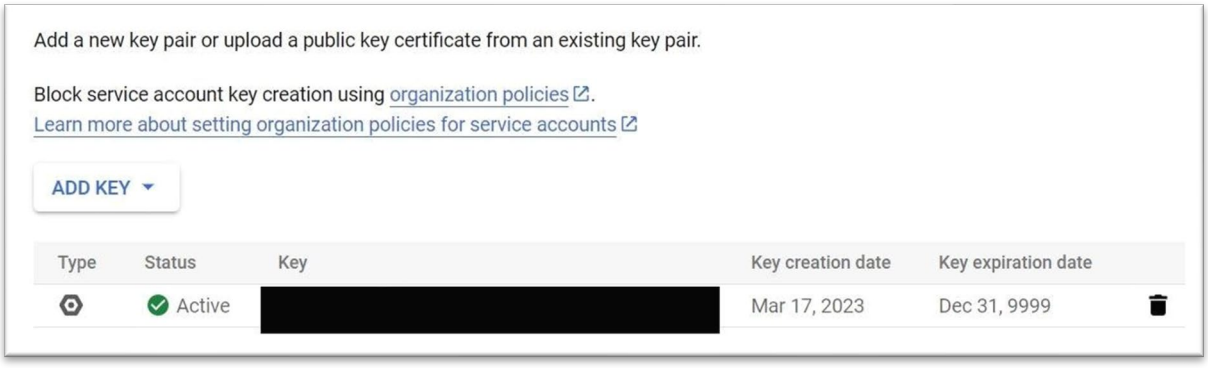
11. Go to the Keys tab of Service Account page and select **Add Key**



12. For key type choose “JSON”

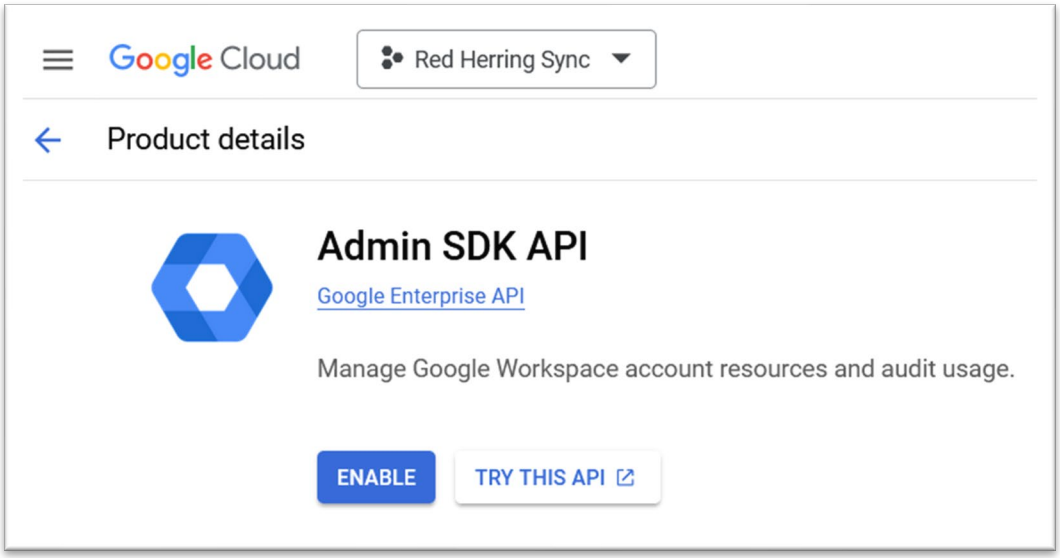


13. After successfully creating, the JSON key will automatically download to your computer (Please keep the JSON safe because you won't be able to download it again)



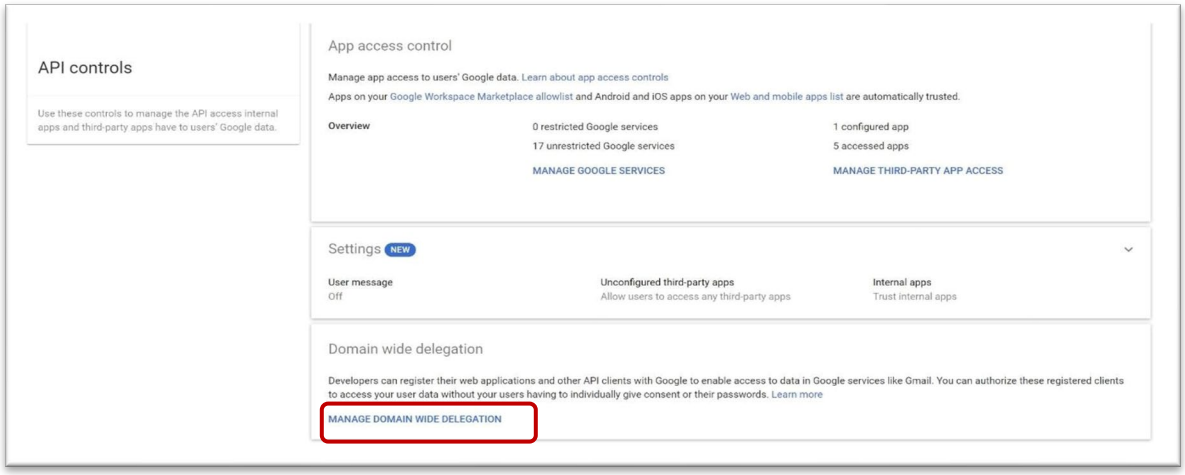
Enable Admin SDK for Service Account in Google Cloud Console

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

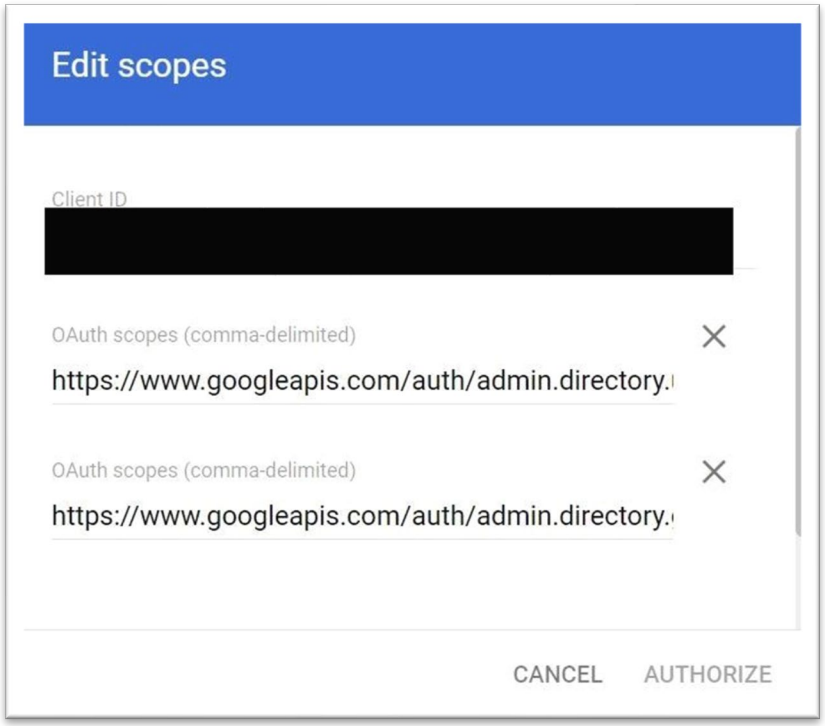


Grant Access for Service Account in Google Admin

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**

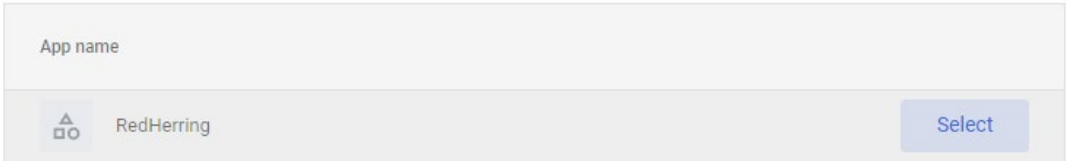


4. Click **Add new** to add new scope for your service account key
5. Input the service account Unique ID (In Service Account Detail page) and the 4 scopes would be:
   https://www.googleapis.com/auth/admin.directory.user
   https://www.googleapis.com/auth/admin.directory.group
   https://www.googleapis.com/auth/admin.reports.audit.readonly
   https://www.googleapis.com/auth/admin.reports.usage.readonly
6. Then click **Authorize**



Trust Red Herring as an OAuth App

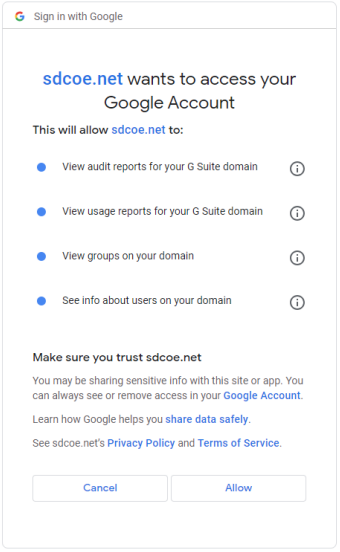
1. Go to Google Admin (https://admin.google.com) and login with Google Admin Account
2. Go to Security > Access and data control > API controls
3. Click **Manage Third-Party App Access**
4. Open the **Add app** drop-down menu
5. Select **OAuth App Name Or Client ID**
6. Search for: 918725752096-bsbsa9v8kl50op3525s5bl21v2aj8061.apps.googleusercontent.com
7. Hover over RedHerring and press **Select**



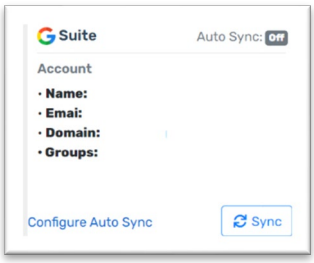
8. Check the box next to OAuth Client ID and press the **Select** button
9. Select All Users and press **Continue**
10. Select the **Trusted** radio button and press **Continue**
11. Review the settings and press **Finish**
12. Wait 5-10 minutes for the changes to propagate and proceed with the next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

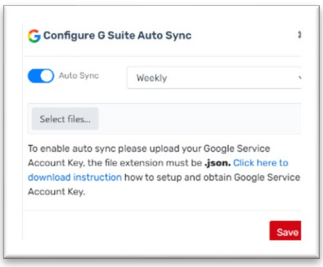
Upload JSON and Sync Target Users into Red Herring

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

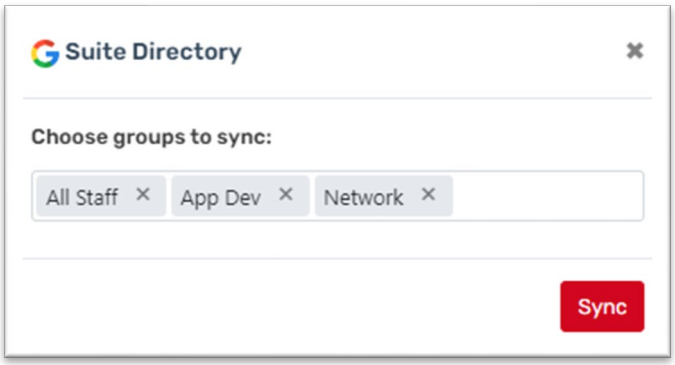


5. On the G-Suite sync tile select **Configure Auto Sync**
6. Slide the toggle switch for Auto Sync and choose your sync frequency
7. Upload the .json file and **Save**





8. On the G-Suite sync tile select **Sync**
9. 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 in Microsoft 365 Admin center
2. Enable SMTP Auth for user in Microsoft 365 Admin Center
3. Enabling Multifactor Authentication for that new user
4. Adding an App Password for that new user
5. Creating an Admin account in Red Herring for that new user
6. Logging into Red Herring as that new user account
7. Configuring SMTP in Red Herring with the new email address and app password.
8. Allowlisting the Red Herring servers

Creating 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**

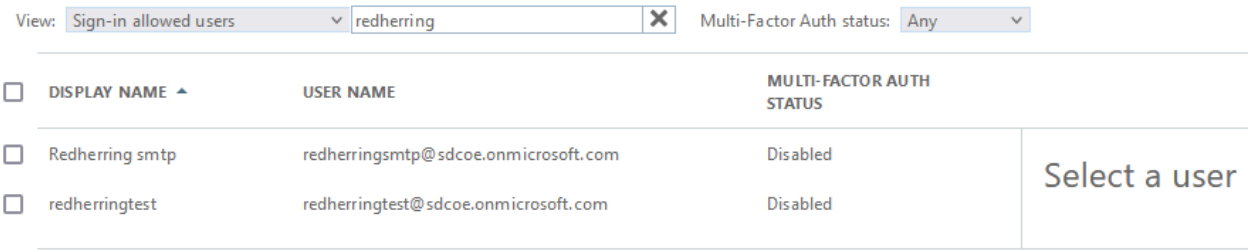
Enable SMTP Auth for user in Microsoft 365 Admin Center

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

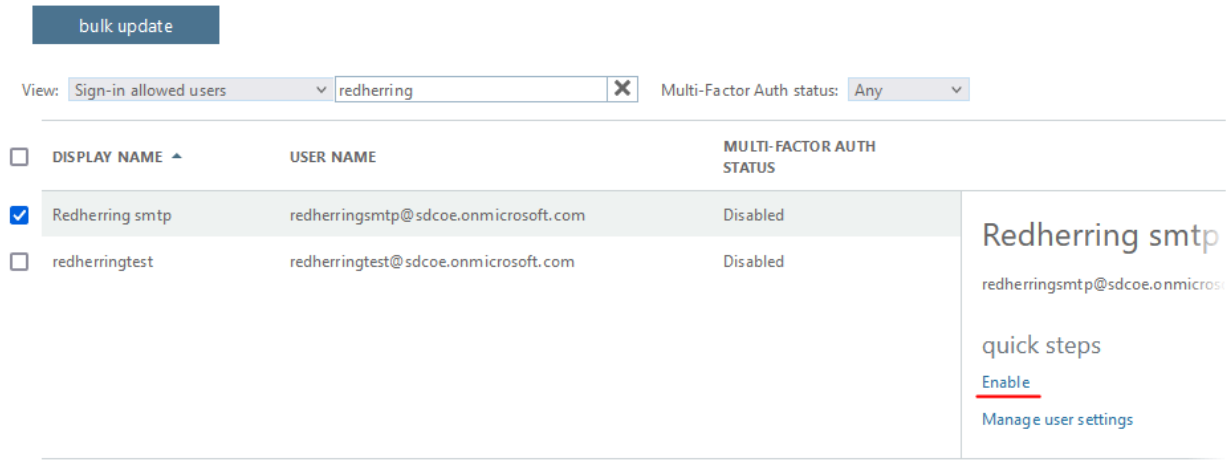
1. Sign into https://admin.microsoft.com
2. Navigate to **Users** > **Active users**
3. Select the user, and in the flyout that appears, click **Mail** tab
4. In the **Email apps** section, click **Manage email apps**
5. Verify the **Authenticated SMTP** setting: unchecked = disabled, **checked = enabled**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



3. Click **Enable**

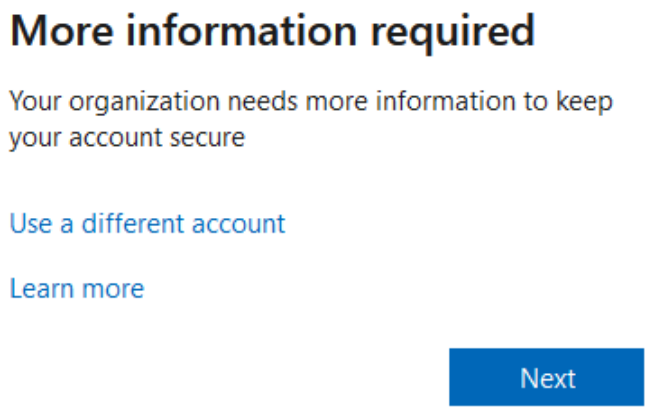


4. Click enable **multi-factor auth**.
5. Click **close**.

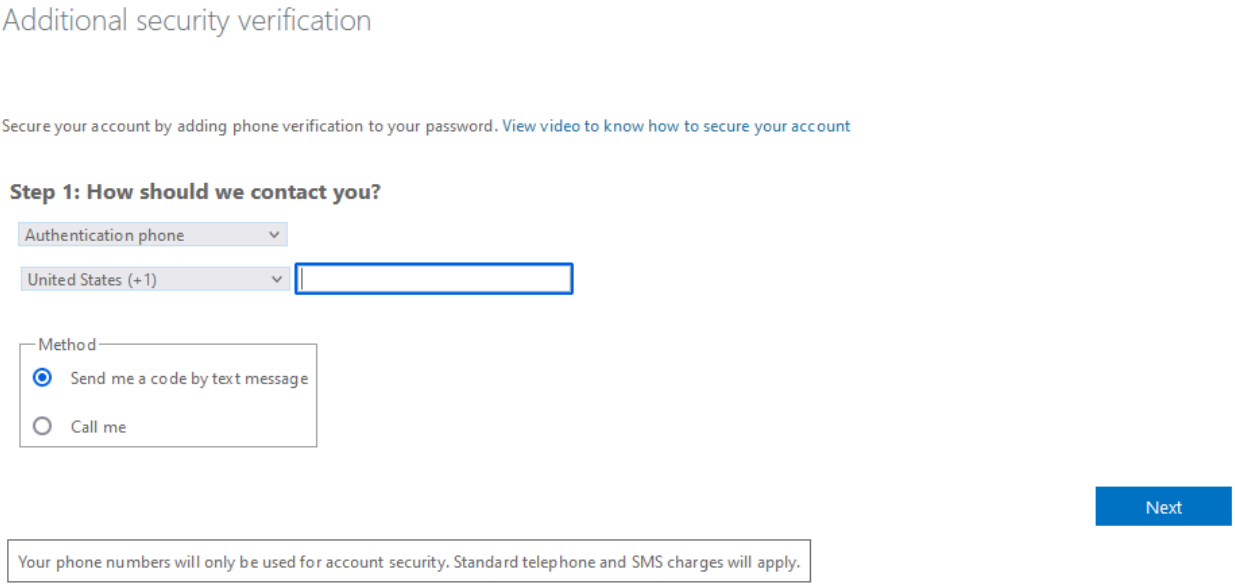
Adding an App Password

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:

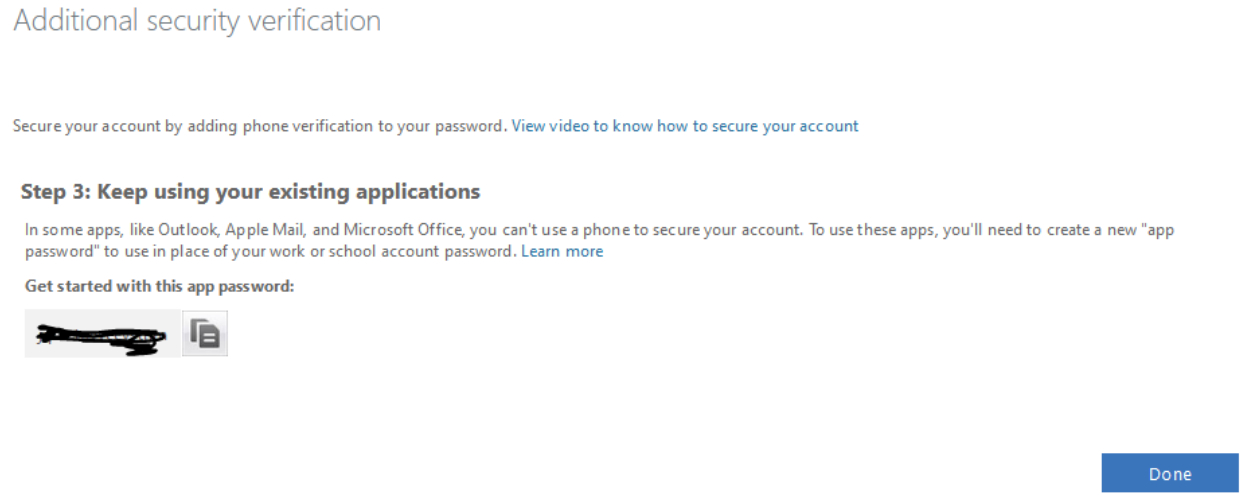


4. Type in your cell phone number for the account.

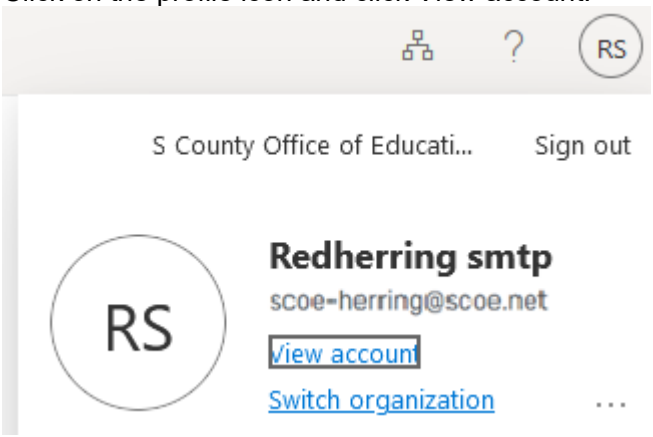


5. Type in the verification code from your cell phone and click verify.

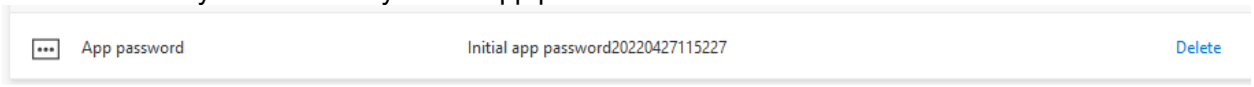
6. Copy the app password (save this password, it will be used to configure the SMTP Server in Red Herring) and click Done.



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

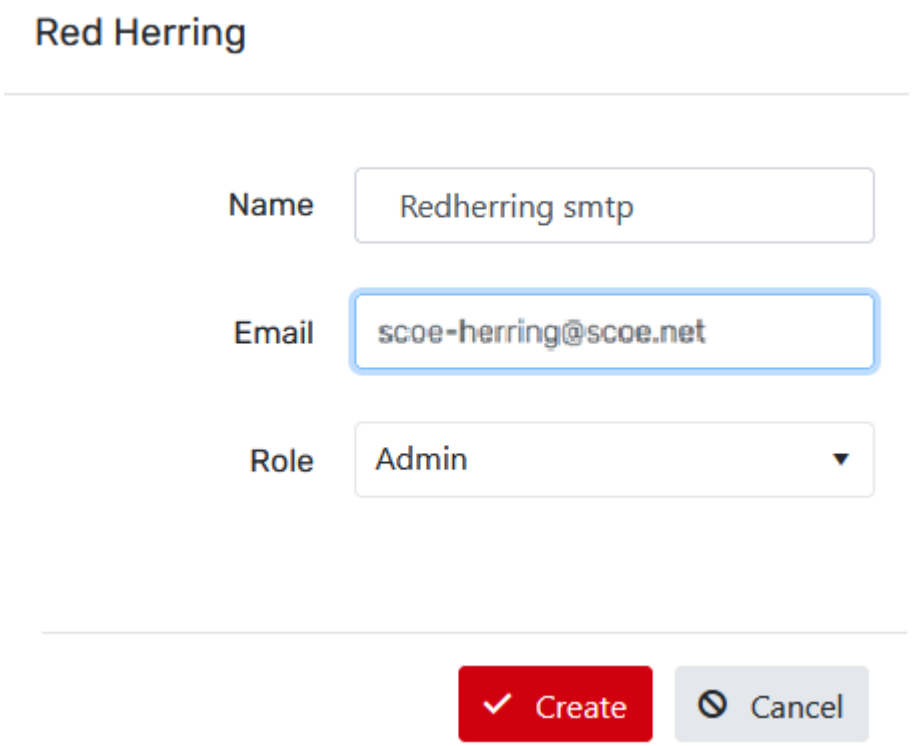


8. Click on Security Info and verify that a App password was created.



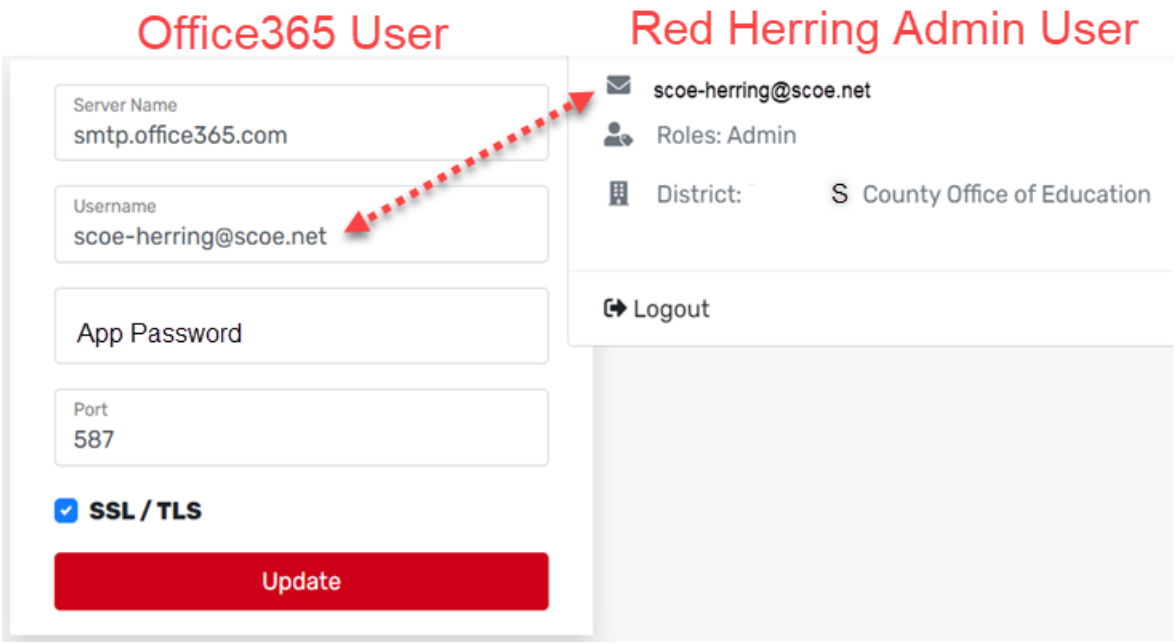
Adding new user as Admin in Red Herring

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

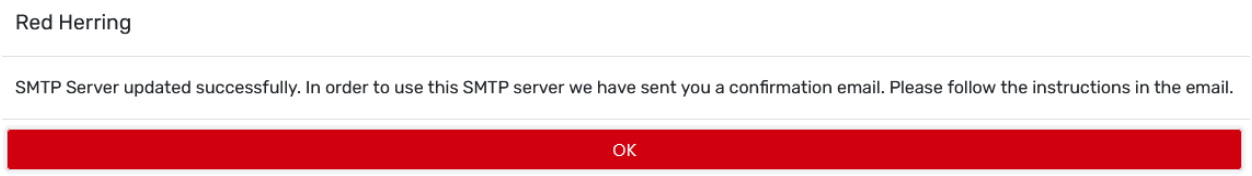


4. A confirmation email will be sent to your “redherring” mailbox. Confirm the email and change the account password.
5. Logout of your current Red Herring Admin account.

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.



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**.



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

Microsoft 365 Allowlisting

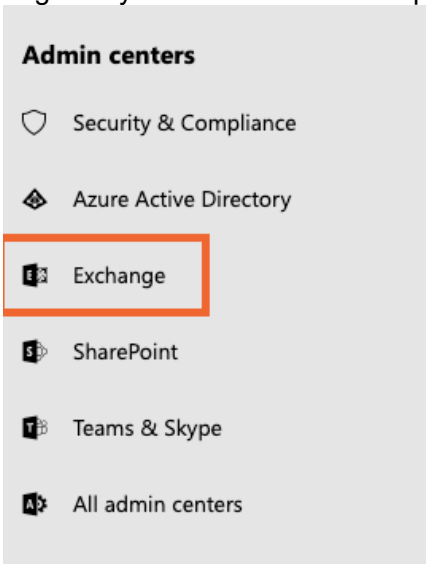
To use Microsoft's Advanced Delivery to categorize your Red Herring emails as simulated phishing emails in your Microsoft 365 environment, follow the steps below:

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 Sending IP 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

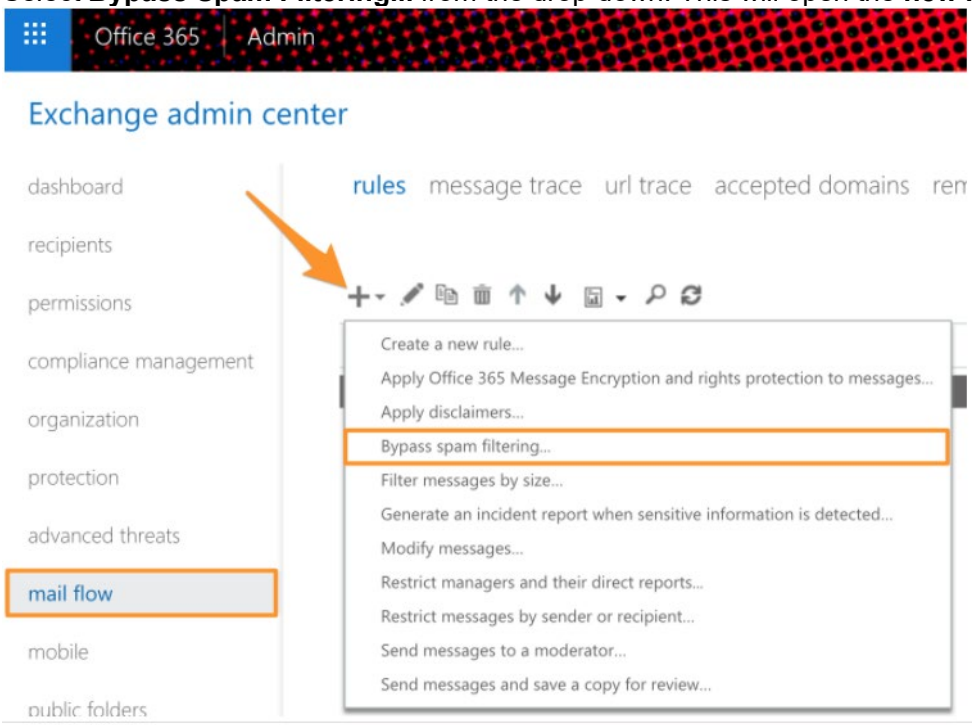
To allowlist simulated phishing emails sent from Red Herring in your Microsoft 365 environment, follow the steps below:

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

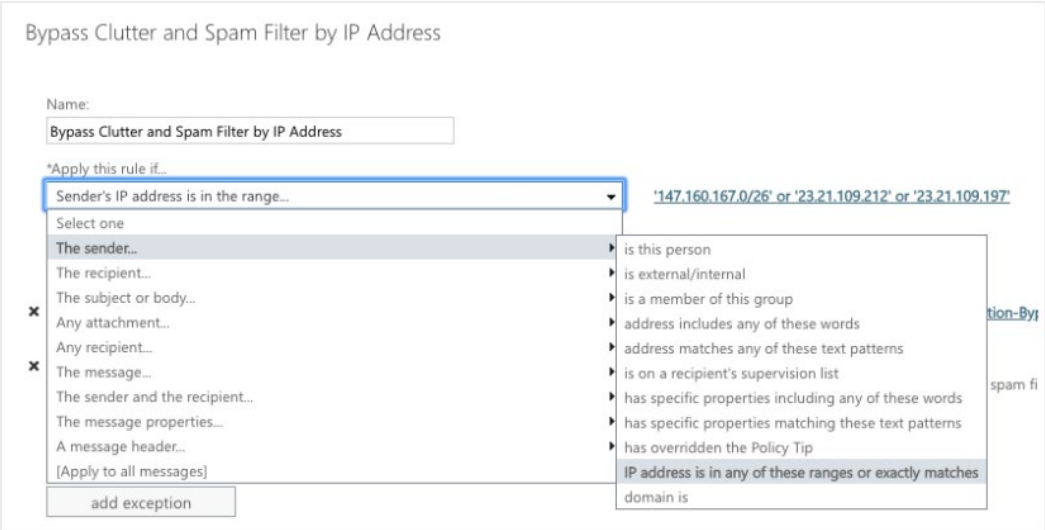


2. Select **Mail Flow > Rules** and click on the **+** sign located in the top-left

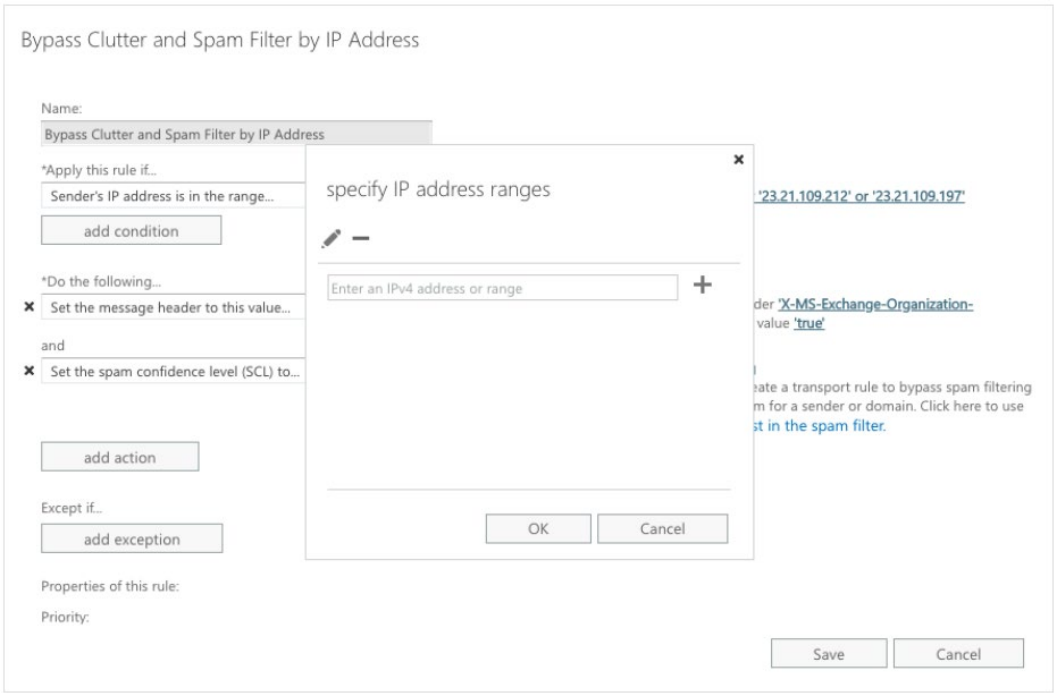
3. Select **Bypass Spam Filtering...** from the drop-down. This will open the **new rule** screen



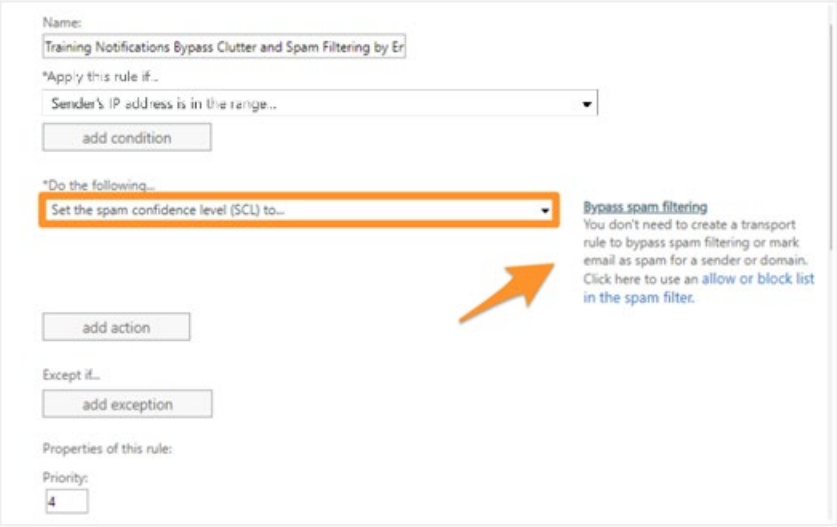
4. Give the rule a name, such as **Training Notifications Bypass Clutter** or **Spam Filtering by Email Header**
5. Select **Apply this rule if…** and then choose **The sender...** > **IP address…** from the drop-down. This will open the **IP address** screen



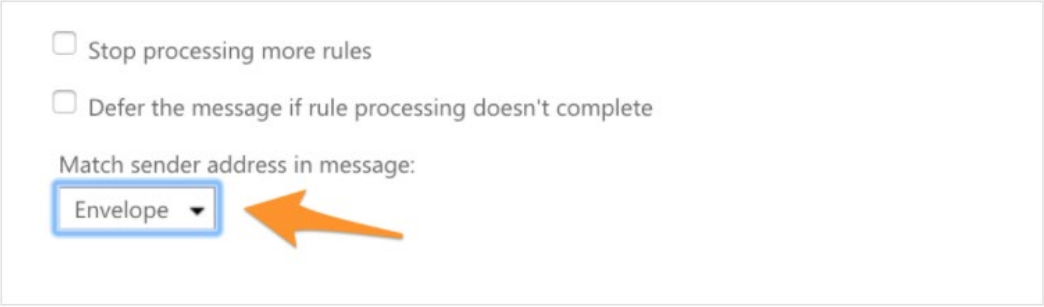
6. Enter our IP addresses “192.40.172.4, 192.40.172.139, 20.118.176.15, 20.118.176.58” on the **specify IP address** screen and click the **+** sign. Then, click the **OK** button.



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.



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

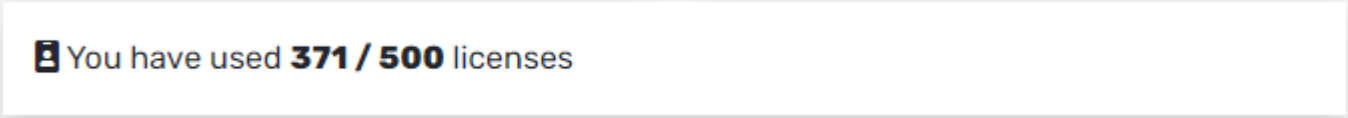


9. Click the **Save** button.

Target Users

The recipients of 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**.

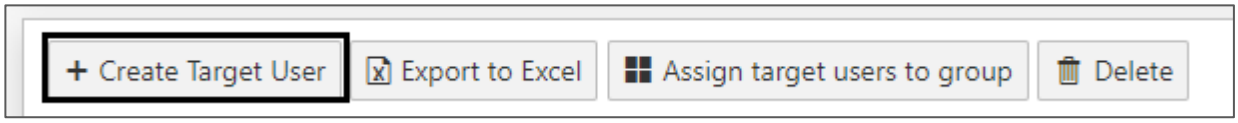
Depending on your subscription, you will be allowed to add a certain amount of target users into Red Herring. The amount of licenses (target users) can be viewed on your Target Users page or the District Report page.



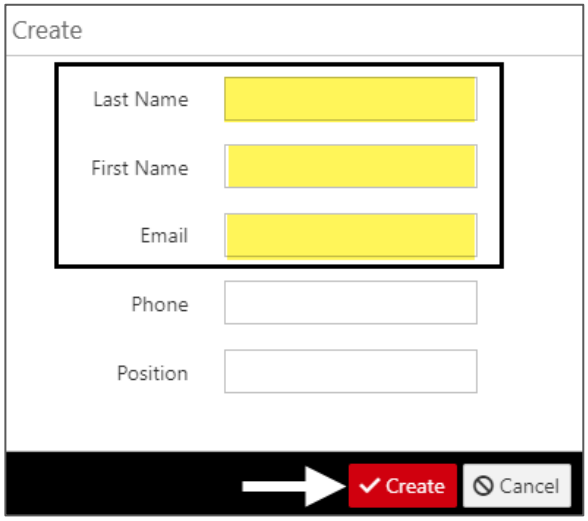
Add Target Users Individually

Follow these steps to add a user manually.

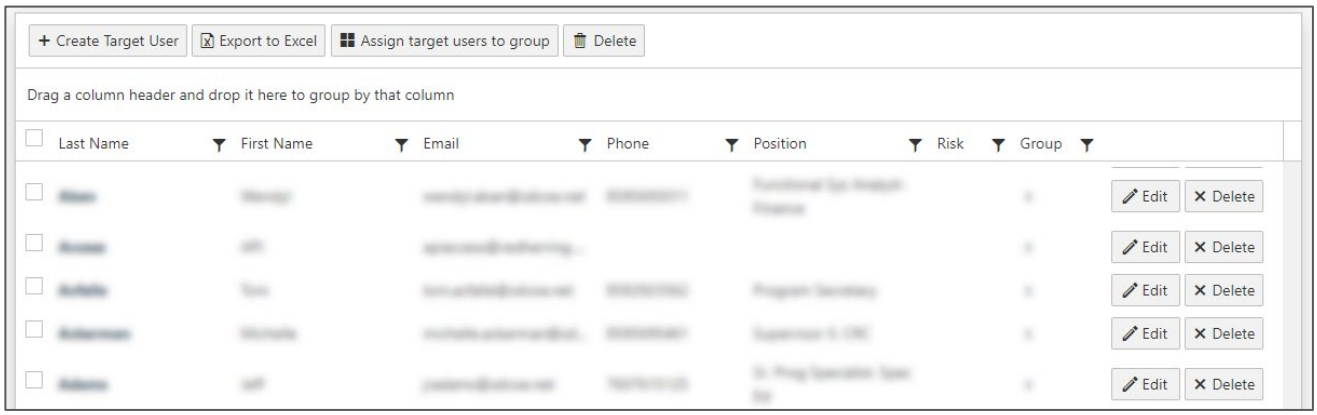
1. In the navbar, click **Target Users**.
2. Click **Create Target User**.



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



4. The screen will display your target users.

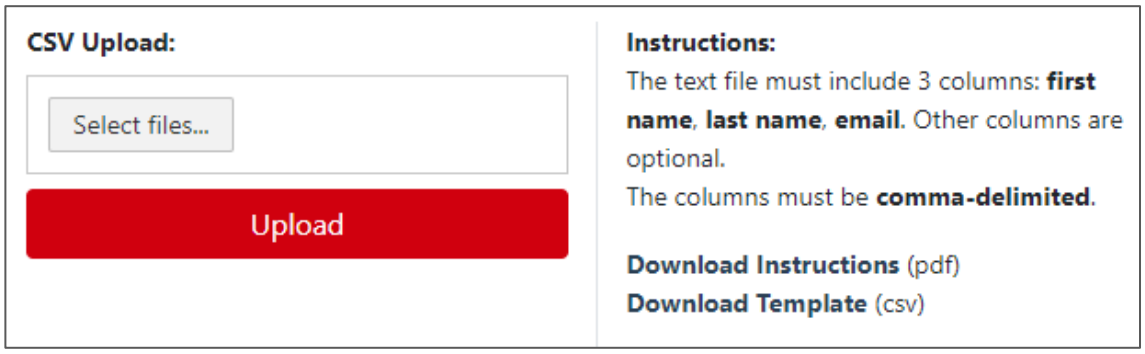


NOTES:

- 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.
- All the columns have a filter icon, allowing you to organize the displayed data as needed.

CSV Upload

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



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

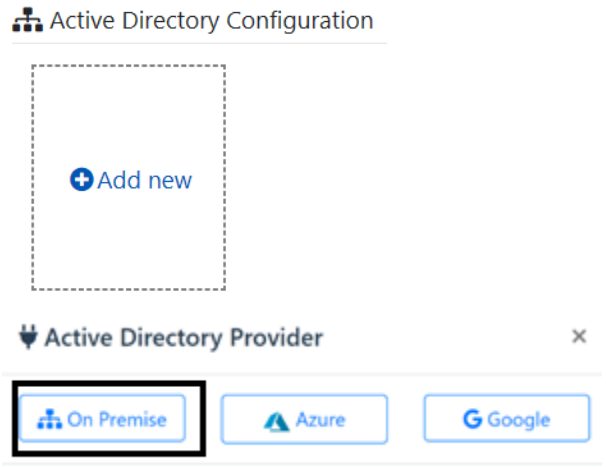
For more detailed instructions, click **Download Instructions (pdf)** on the Target Users page.

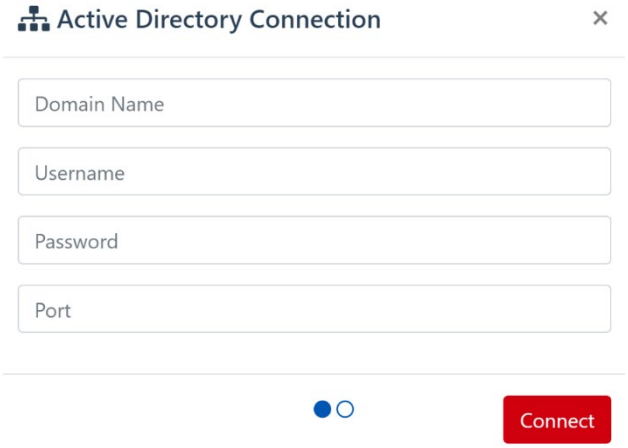
On Premise Active Directory Sync

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

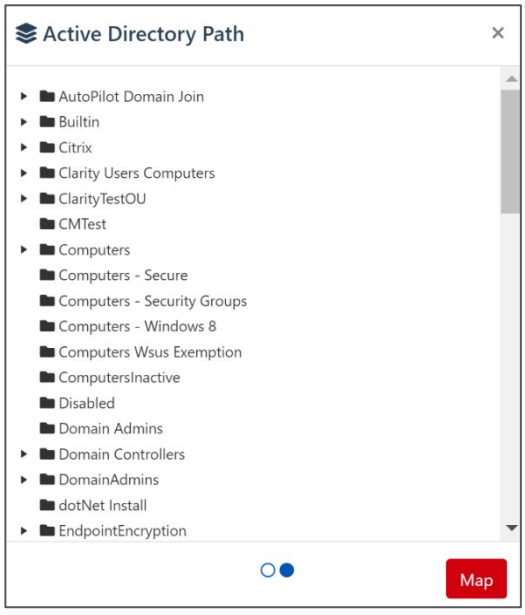
20.118.176.15, 20.150.248.122, 20.118.176.229

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**.

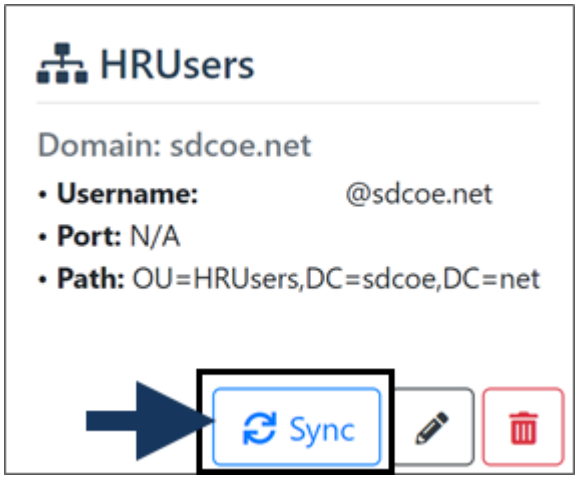




3. Next, you'll select which Active Directory group to pull users from.



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.68. Subsequent syncs will be used to update any new users.



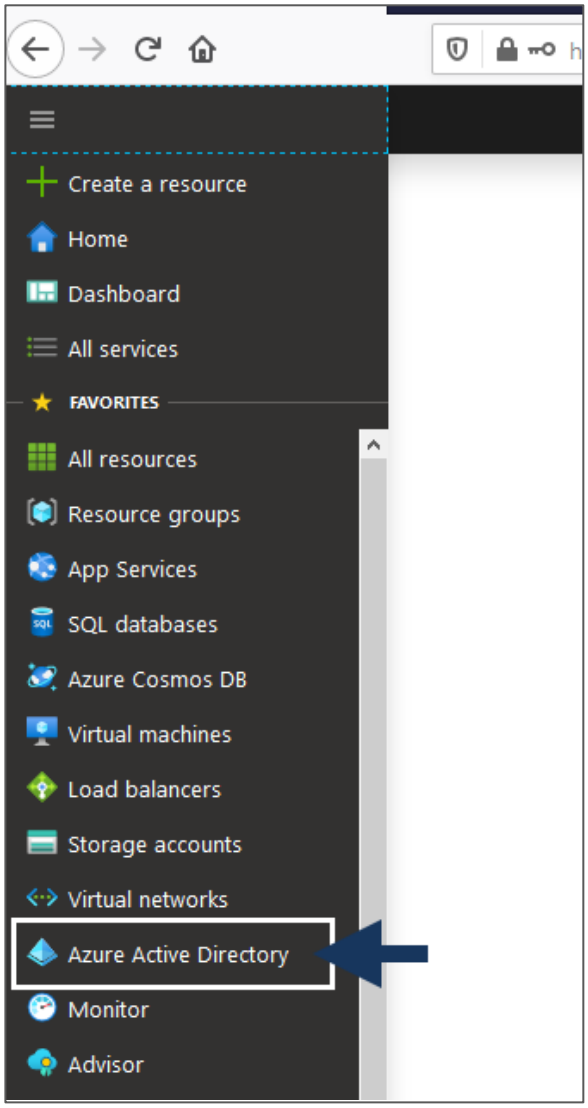
Azure User Sync

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.

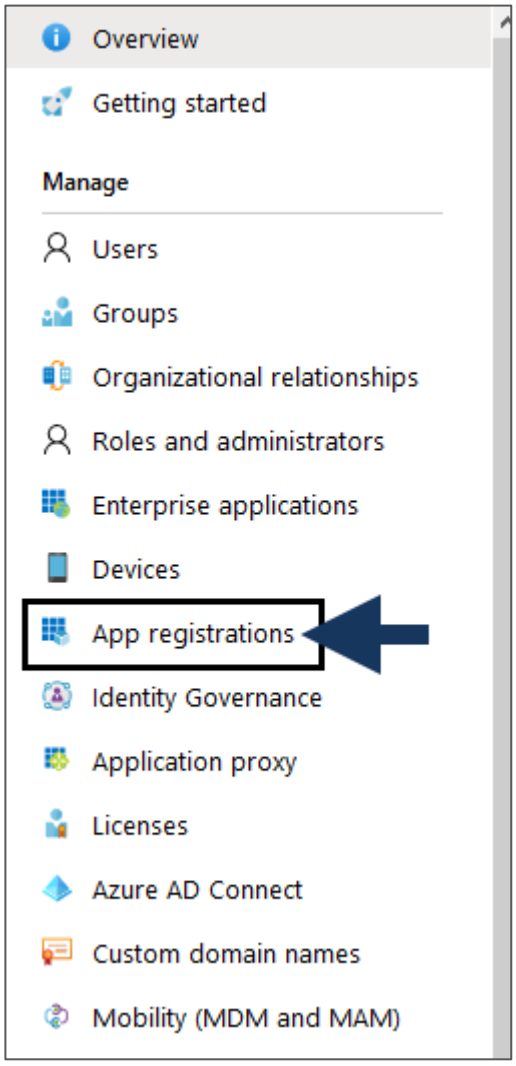
Follow the steps in this section to collect from Azure the **Client ID**, **Tenant ID**, **Client Secret**, and **Group ID**, which you will then enter in Red Herring.

Client ID: Obtained at Step 6 → **Tenant ID:** Obtained at Step 6 → **Client Secret:** Obtained at Step 9 → **Group ID:** Obtained at Step 19 → **ENTER IN RED HERRING:** Step 22

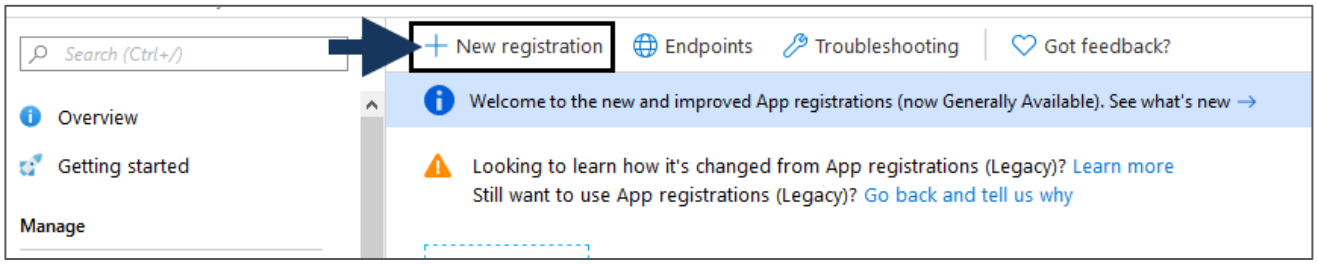
1. Log in to https://portal.azure.com using your Azure administrative account.
2. In the navigation on the left, select **Azure Active Directory**.



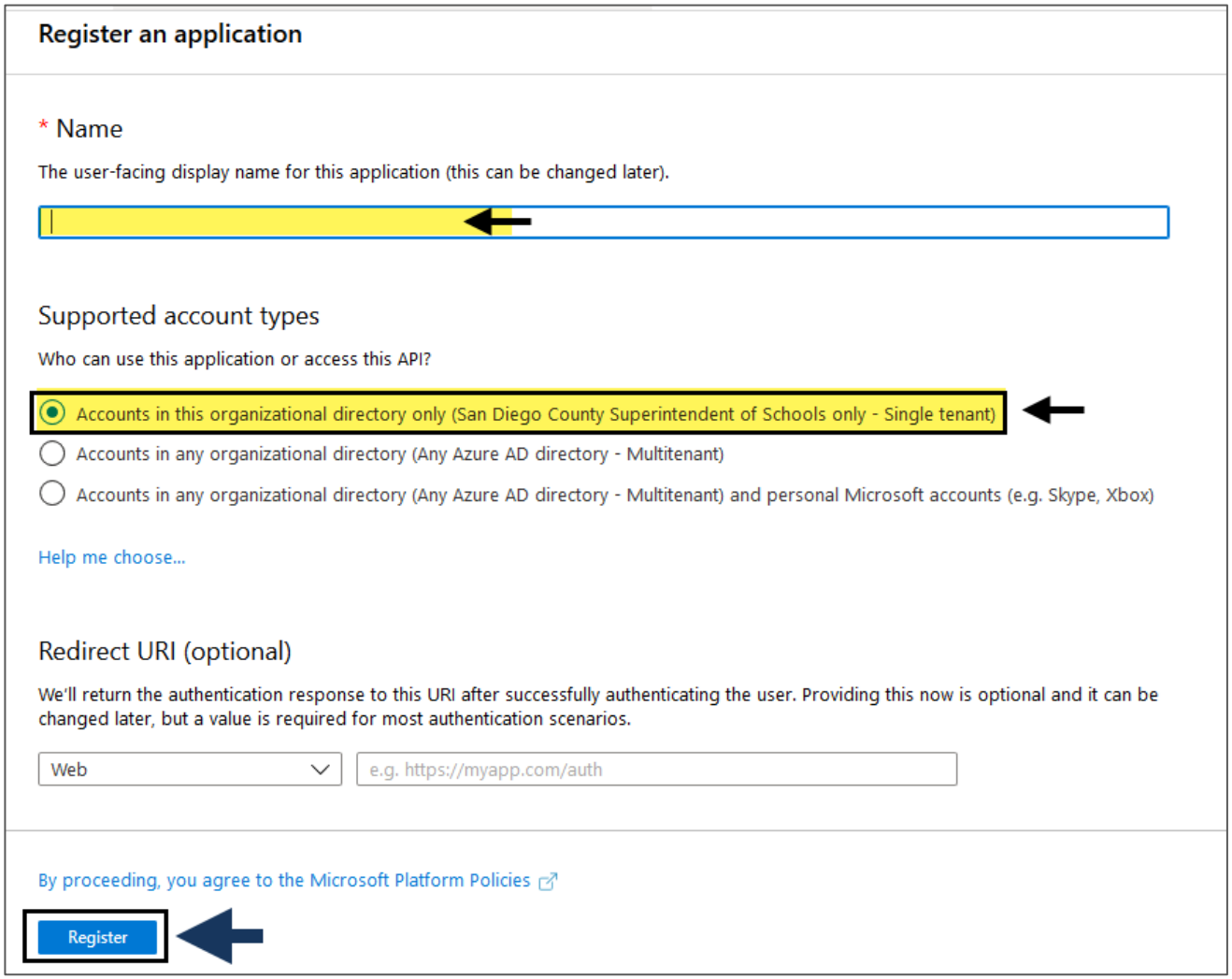
3. Select **App registrations**.



4. Click **New registration**.

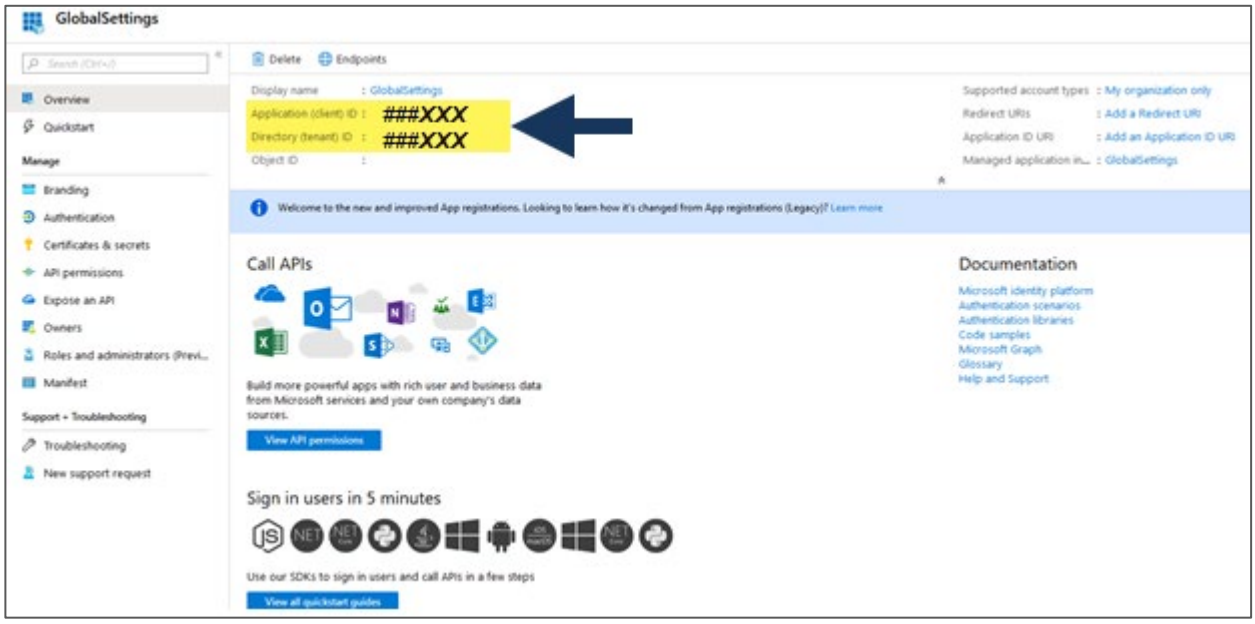


5. On the *Register an application* page, enter the following, then click **Register**.

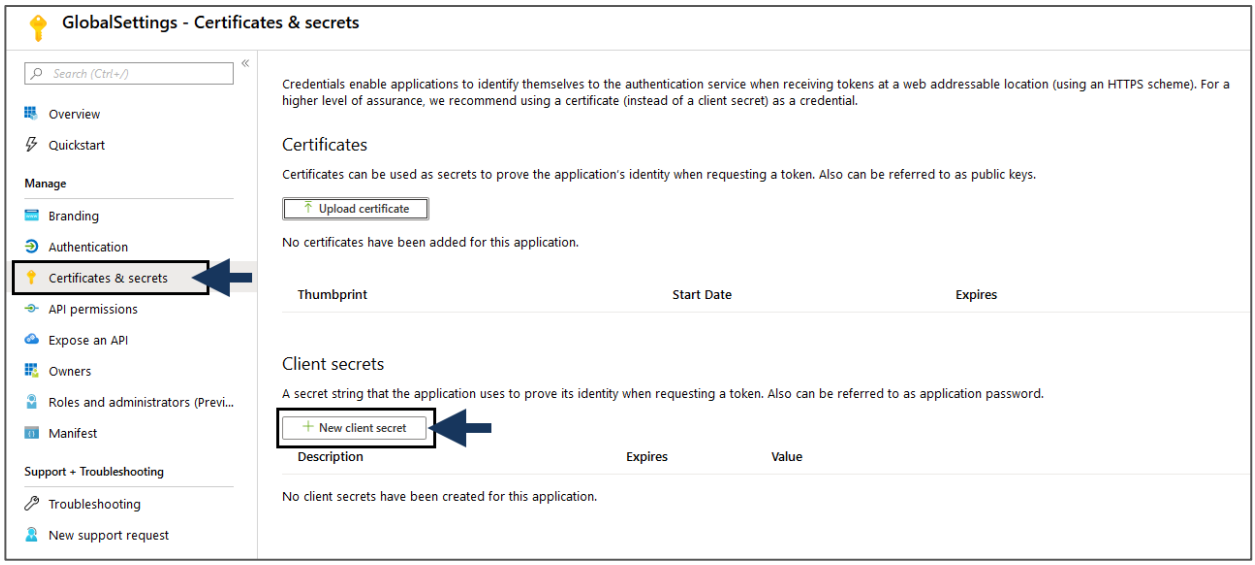


- **Name:** Enter a name for the application. *Example: Red Herring*
- **Supported account types:** Select *Accounts in this organizational directory only*

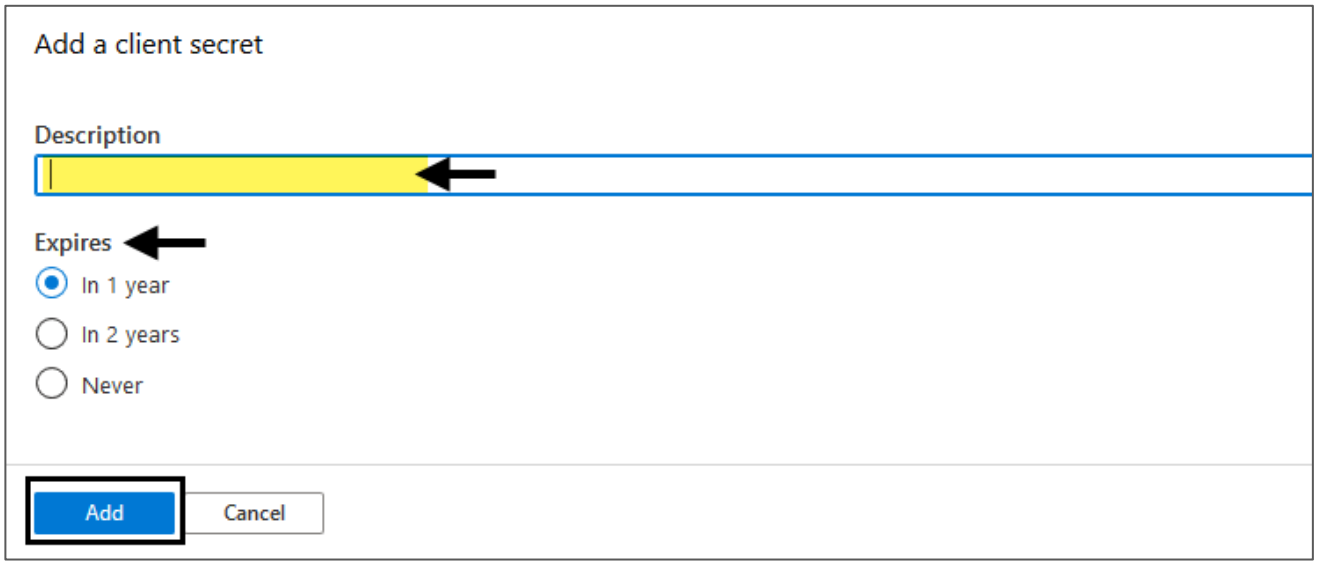
6. Copy the **Application (client) ID** and **Directory (tenant) ID**. ***IMPORTANT: You will later input this information in Red Herring at Step 22.***



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



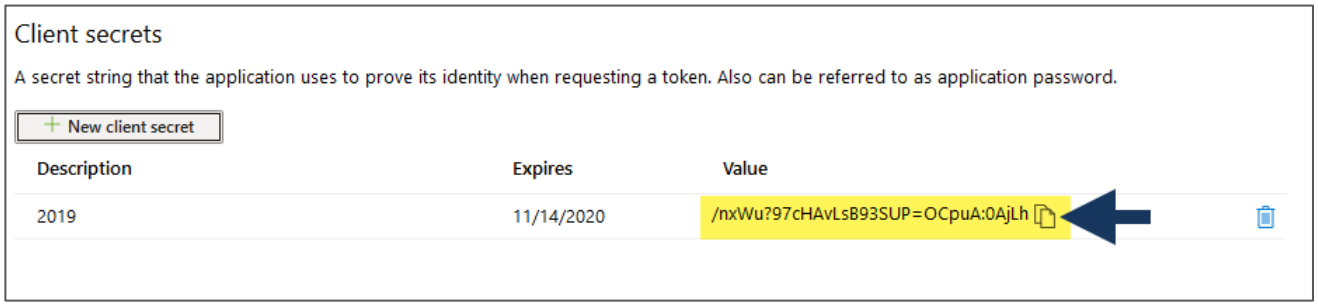
8. Enter the description in the client secret form and select how long you want the secret key to be valid. Click **Add**.



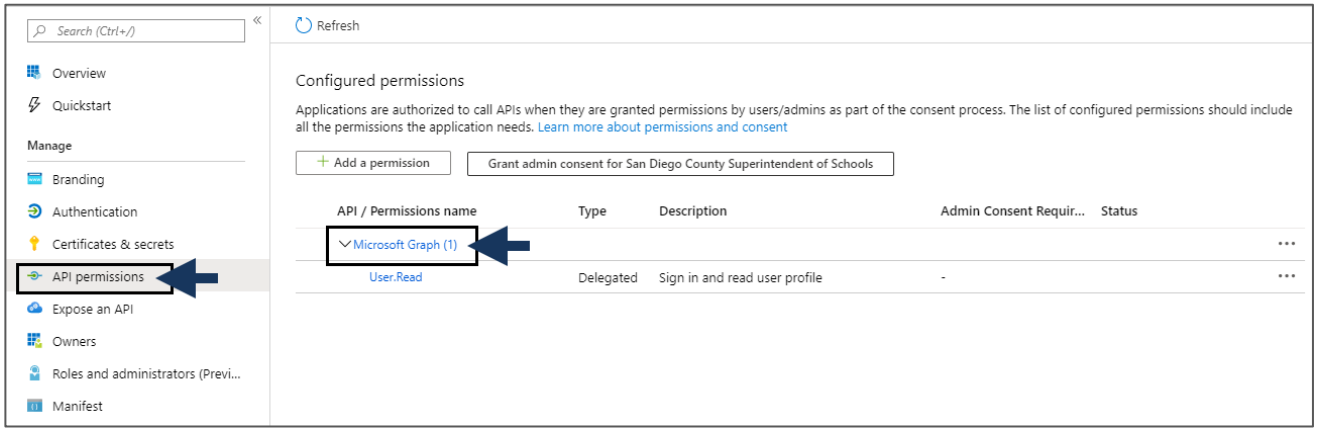
NOTES ABOUT AN EXPIRED SECRET KEY:

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

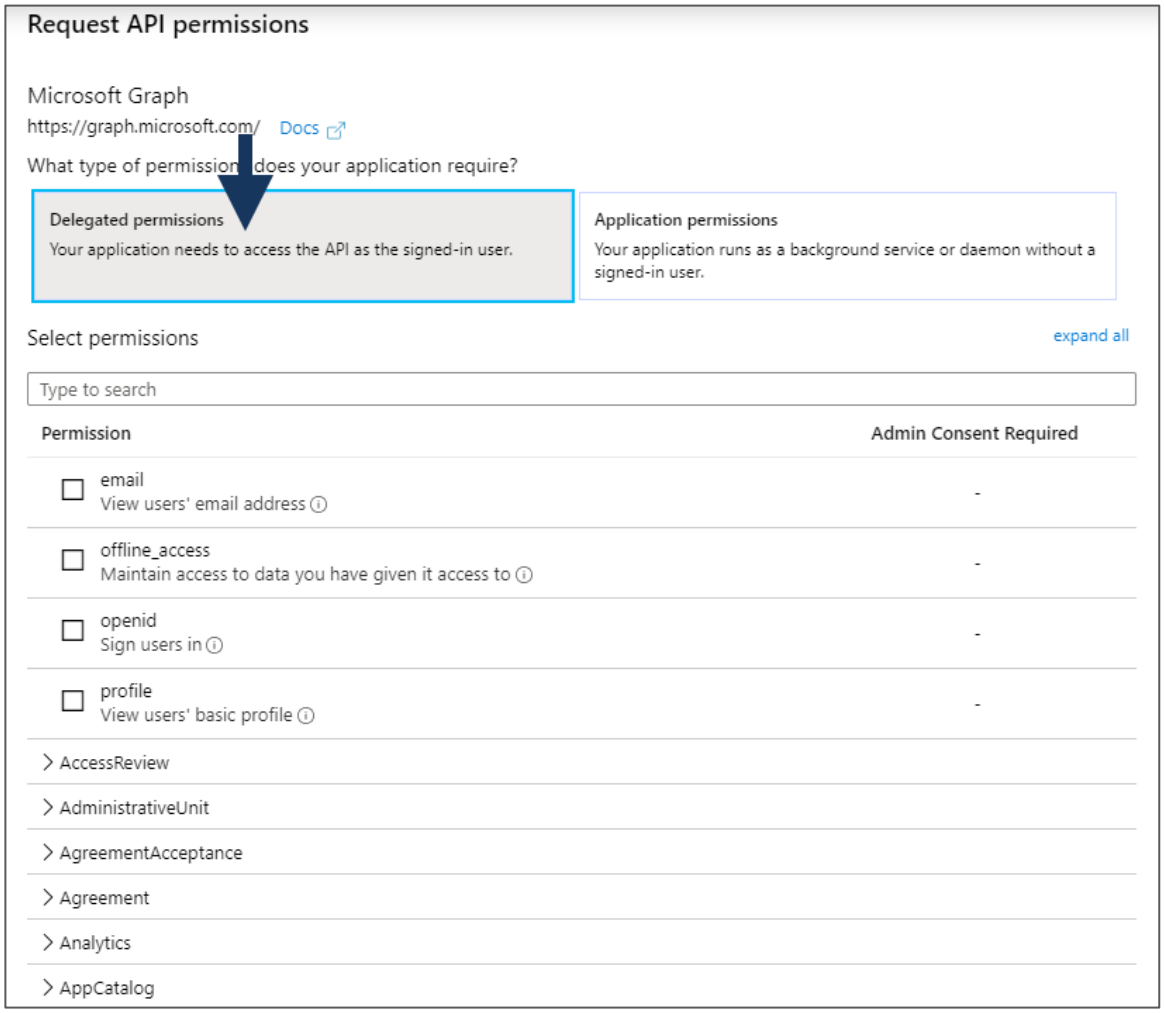
9. **Copy the secret key.** If you move away from this page, the key will be hidden when you return to the page. ***IMPORTANT: You will later input this information in Red Herring at Step 22.***



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

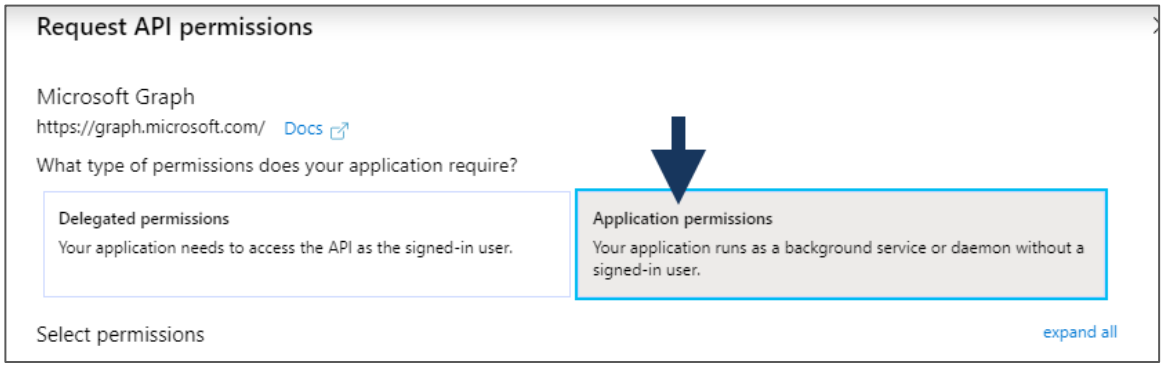


11. On the *Request API permissions* page, under **Delegated Permissions**…

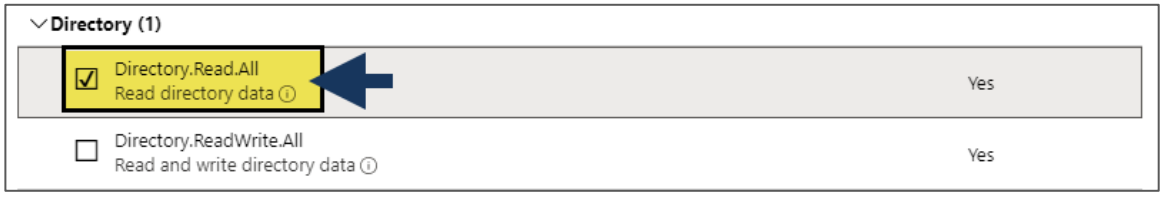


…scroll down to *User (1)* section and uncheck the **User.Read** checkbox.

12. Select **Application permissions**.

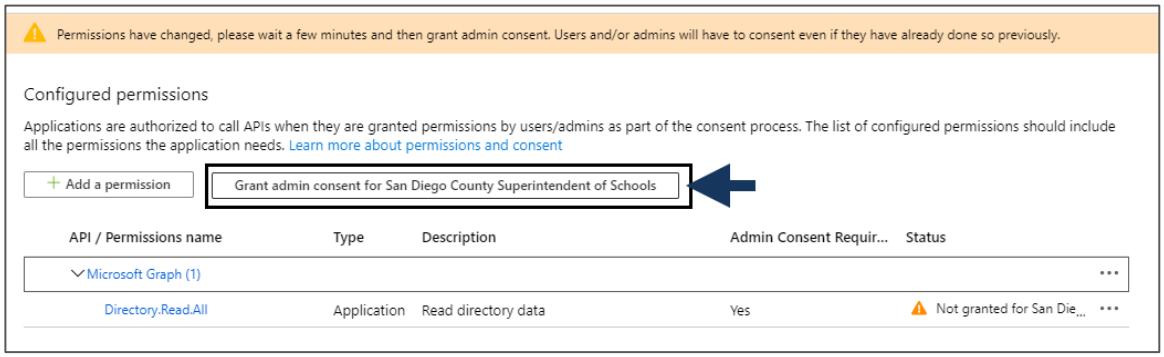


13. Scroll down to the *Directory (1)* section, expand the Directory, and check **Directory.Read.All**.



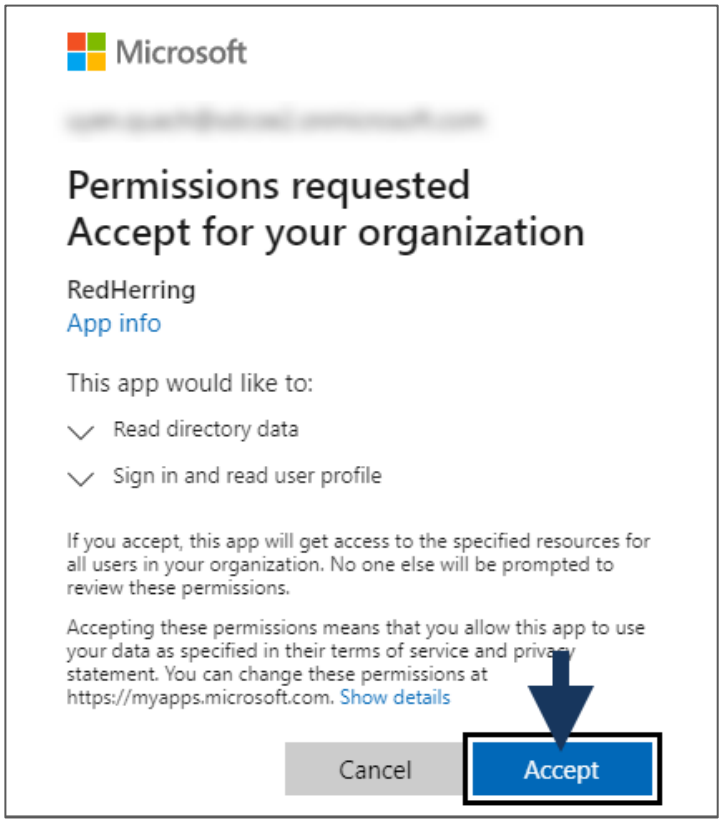
14. Scroll down to the *Group* section, expand the Directory, and check **Group.Read.All**.
15. Scroll down to the *User* section, expand the Directory, and check **User.Read.All**.
16. Click **Update permissions**.

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

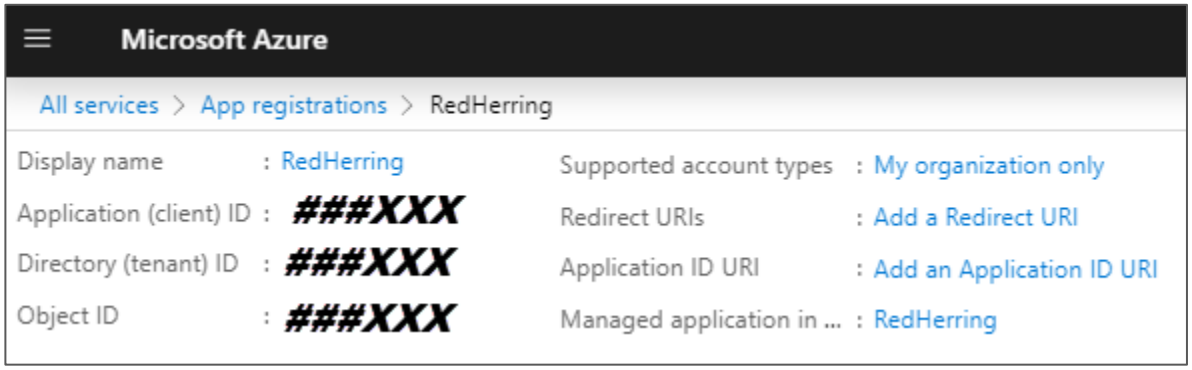


18. Azure will ask you to select the admin login account.

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



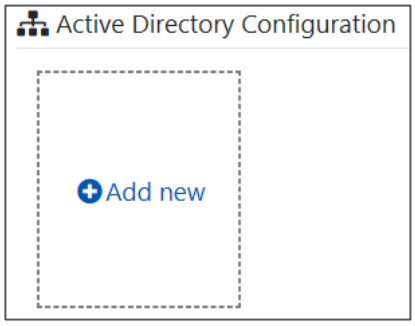
20. This is what is shown after you have created the Red Herring app registration.

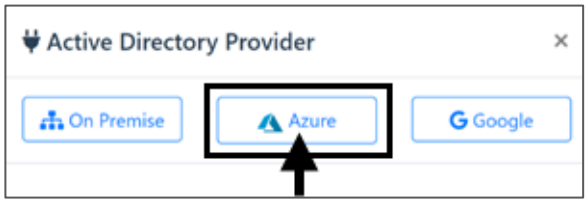


IMPORTANT: You will later input this information in Red Herring at Step 22.

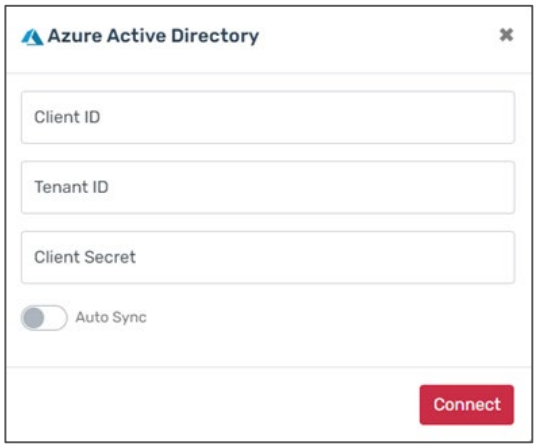
Now go to Red Herring.

21. In Red Herring, navigate to **Configuration > Directory**.
22. Click on the **+ Add new** tile and then select **Azure**.

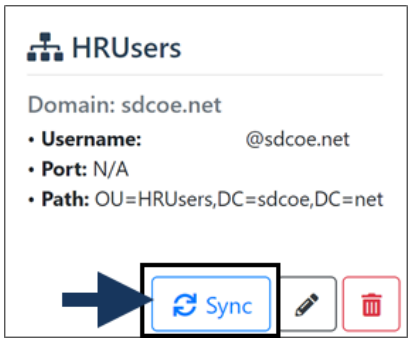




23. Enter your Azure Connection information: **Client ID**, **Tenant ID**, and **Client Secret**. Click **Connect**.



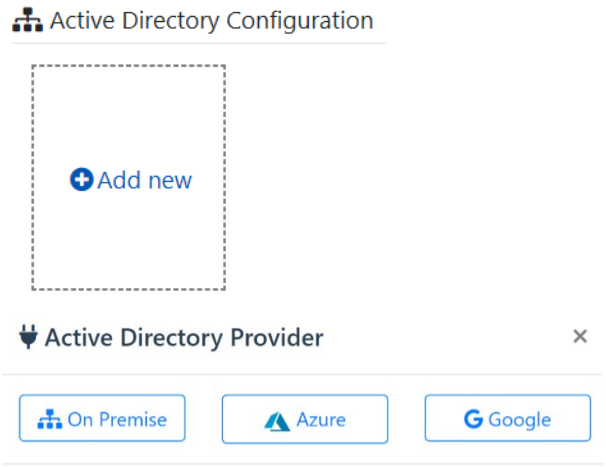
24. Perform an initial sync to import your AD users at any time. Refer to *Send a Phishing Email (Ad Hoc)* on p.68. Subsequential syncs will be used to update any new users.

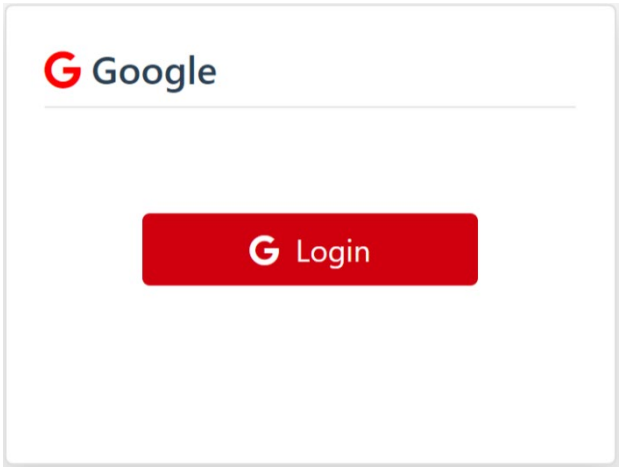


Google Sync

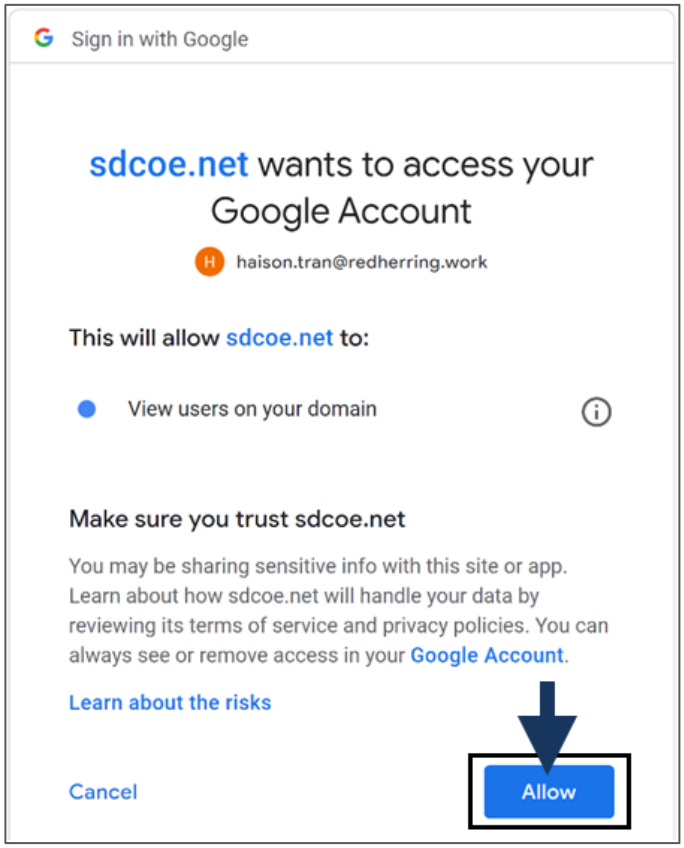
To import the users that you have in Google G-Suite, you'll have to log-in Google through Red Herring using your G-Suite administrative credentials to allow Red Herring access to your Google account.

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

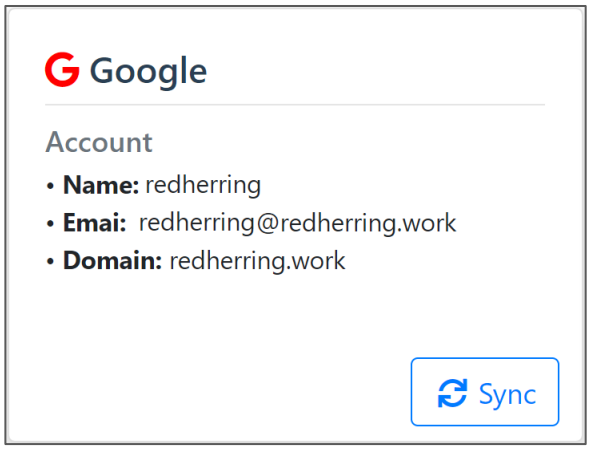




2. Confirm that you would like to allow Red Herring access to your Google account.

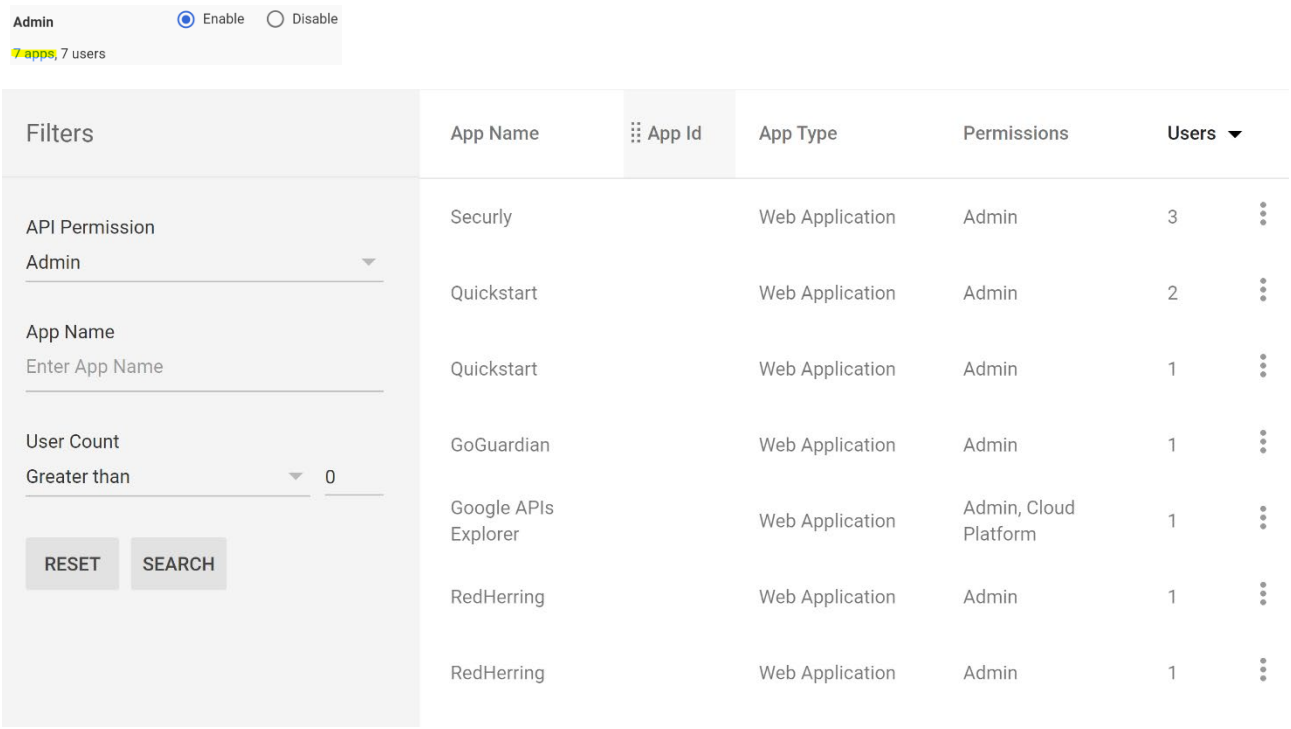


3. Once you're logged into Google through Red Herring, perform an initial **Sync** to import your Google users. Refer to *Send a Phishing Email (Ad Hoc)* on p.68. Subsequential syncs will be used to update any new users.



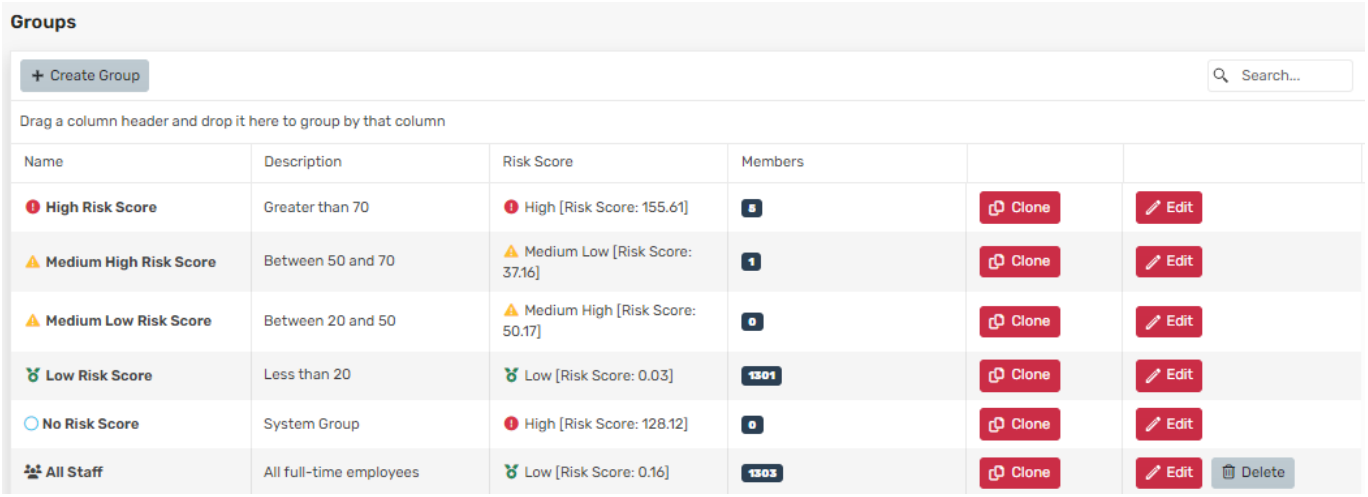
- Red Herring does not store your Google Credentials.
- Once you log out of Red Herring, you'll have to sign in to Google again whenever you want to sync your G-Suite users.

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



Groups

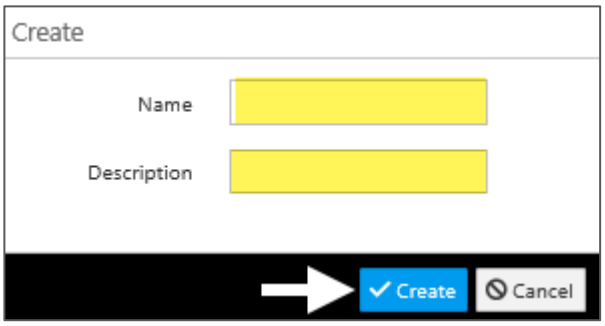
Red Herring is designed to only send emails to groups and not individual users, although a group can have just one person. From the Groups page, you can quickly see how many members are in each group and quickly create a group, clone a group, edit a group's name or delete it.



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

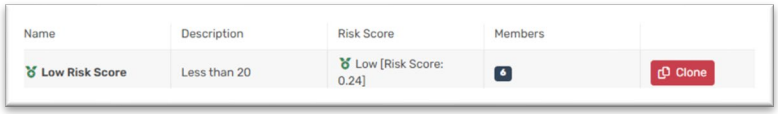
Create a User Group

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



Clone a User Group

Find the User Group that you would like to clone. Click **Clone**.

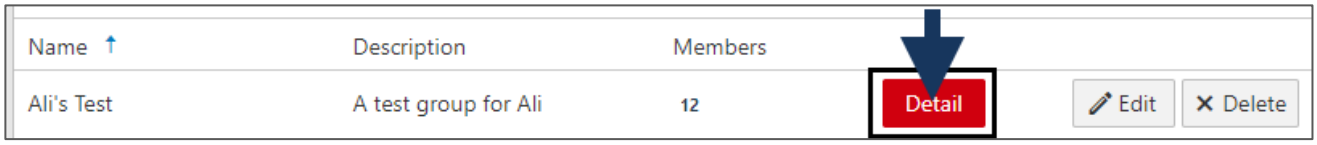


Assign Target Users to the Group

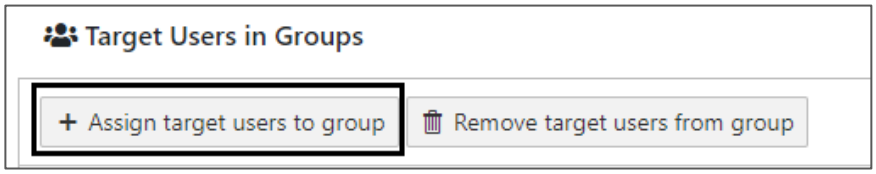
Follow these steps to add a target user to a group or remove existing users from a group via the Groups page.

Assign (Add)

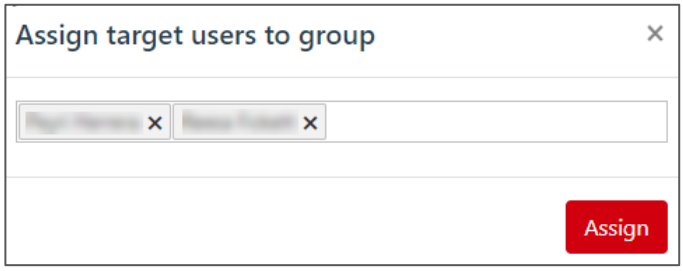
1. Click **Groups**.
2. Click **Detail** for the group that you would like to add a target user.



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



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



Remove

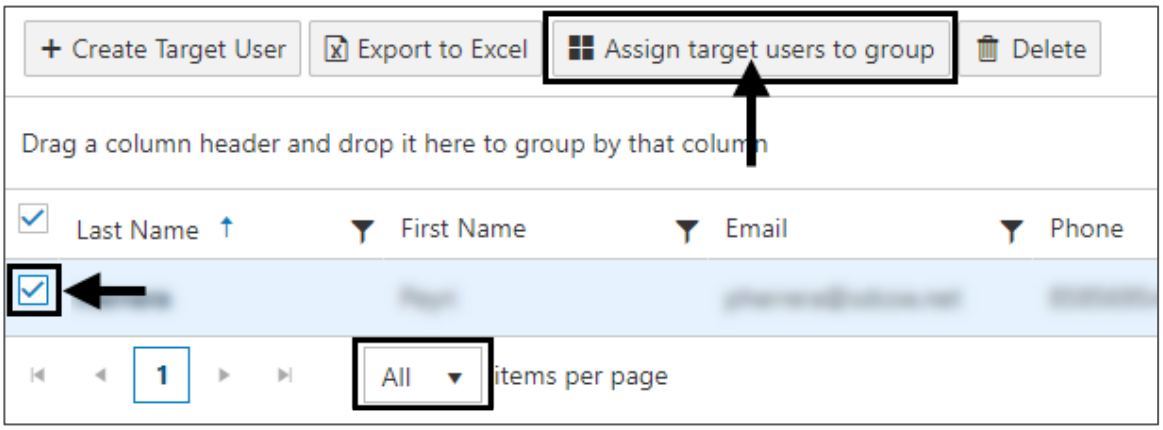
Check the box next to a user(s) and then click the **Remove target users from group** button to remove users from it.

Assign Target Users to a Group

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

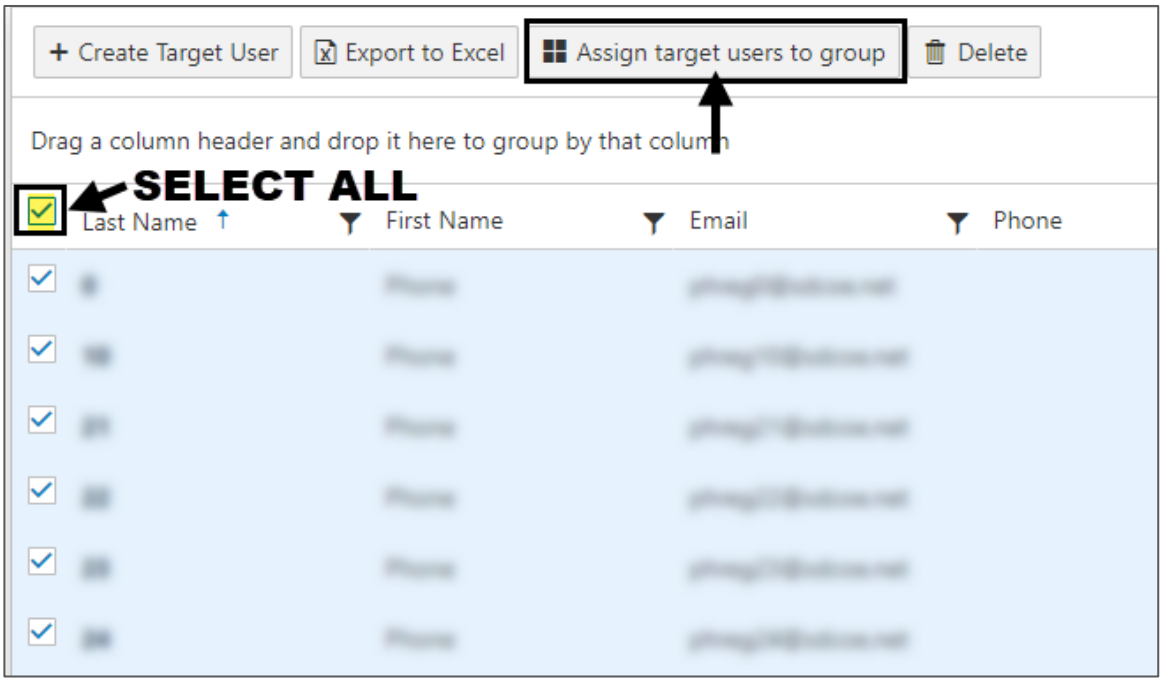
Method 1: Manually select users (checkboxes)

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.



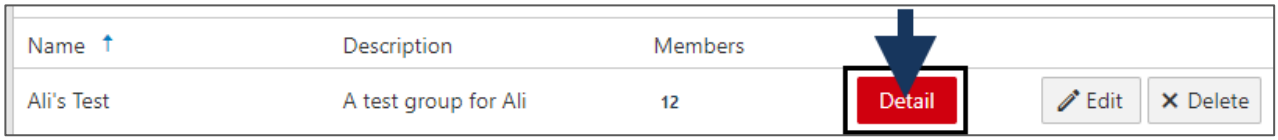
Method 2: Assign ALL users to a group

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.

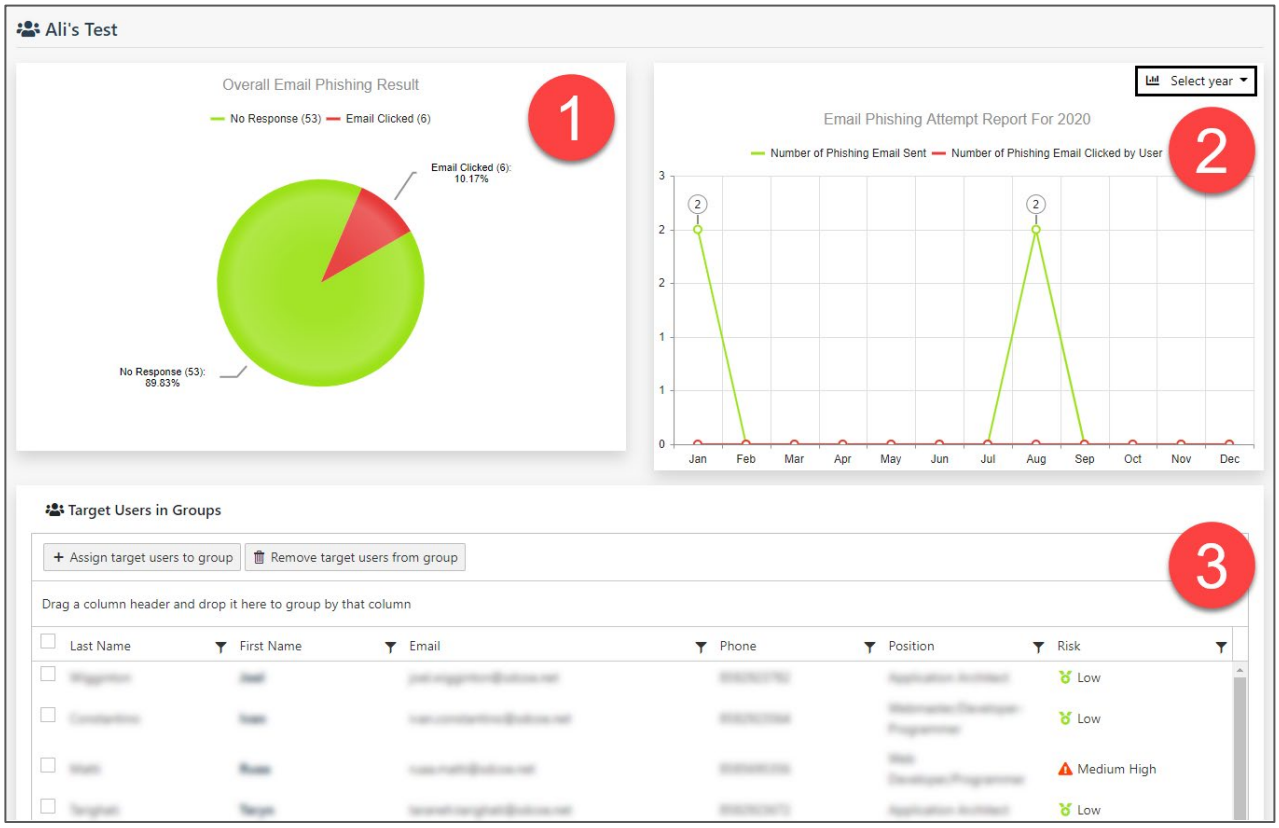


View Group Analytics

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



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-throughs by date. Notice you can set the year at the top-right of this graph.
3	**Target Users in Group:** Shows a list of the target users in this group. • **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 last 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.

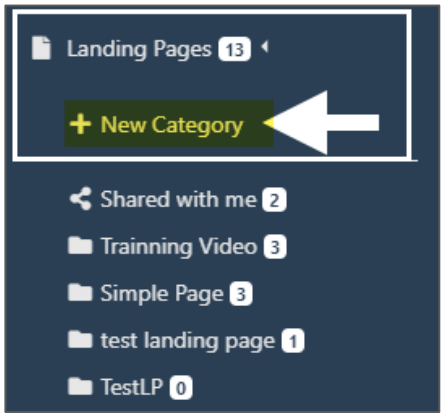
Landing Pages

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.

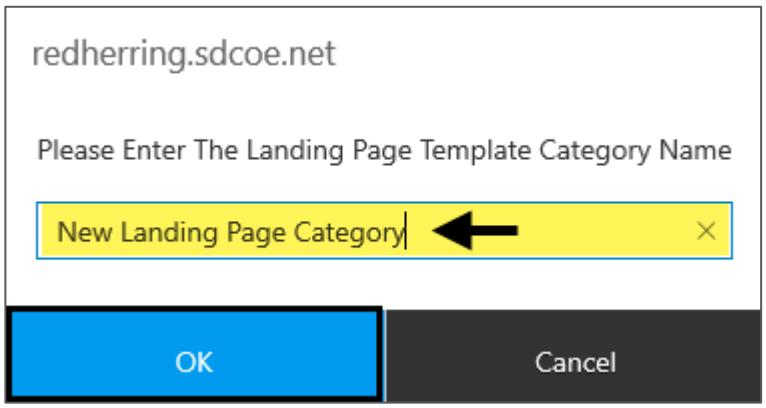
Create a New Category

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

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



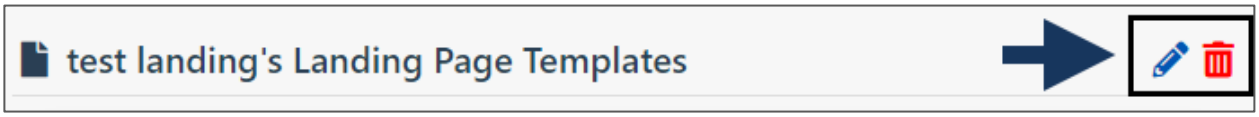
2. Name the category. *Examples: Alert Pages, Cybersecurity Awareness Pages, HR Pages*



3. Click **OK**.

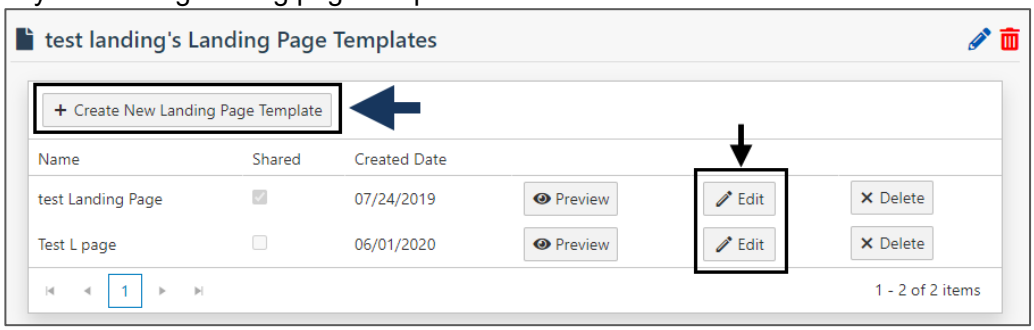
Rename/Delete a Category

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

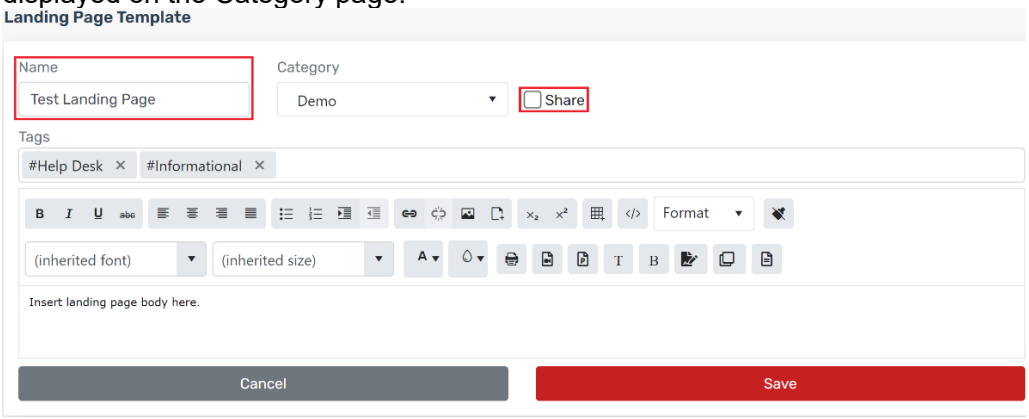


Create/Edit a Landing Page

1. 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.



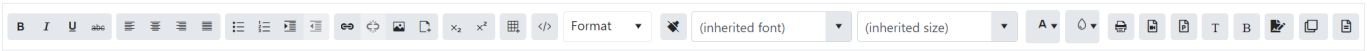
2. Enter a **Name** for the Landing Page Template. This name is just for your reference and will be displayed on the Category page.



3. **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.



NOTES:

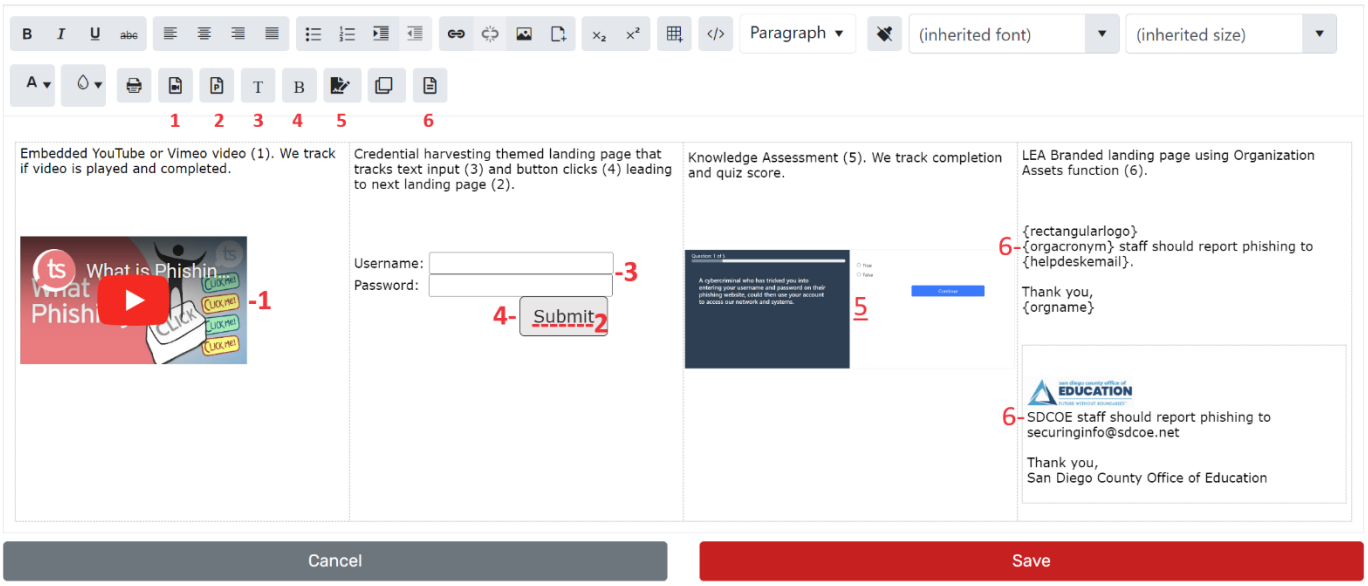
- Click the **View HTML </>** button to view HTML code or copy in from another source.
- Many of our shared templates have commented out notes to help you customize them after cloning. You may use a free WYSIWYG HTML editor to help customize these landing pages.

  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://htmlg.com/html-editor/ - free and ready to use

- You cannot upload files or images. Red Herring has a repository of several images that can be attached to a Landing Page. Contact cyberguardians@sdcoe.net to request an image be uploaded.
  - Or convert an image to Base64 code: https://codebeautify.org/image-to-base64-converter

Special Buttons: Landing Page

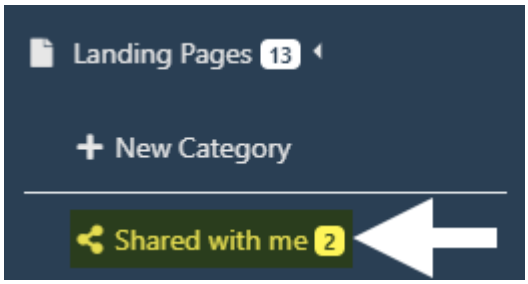
There are a few special buttons in the editor ribbon:



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 the text box. (user input is not recorded)
4	**Button:** Inserts a button with link to a Landing Page and a 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)

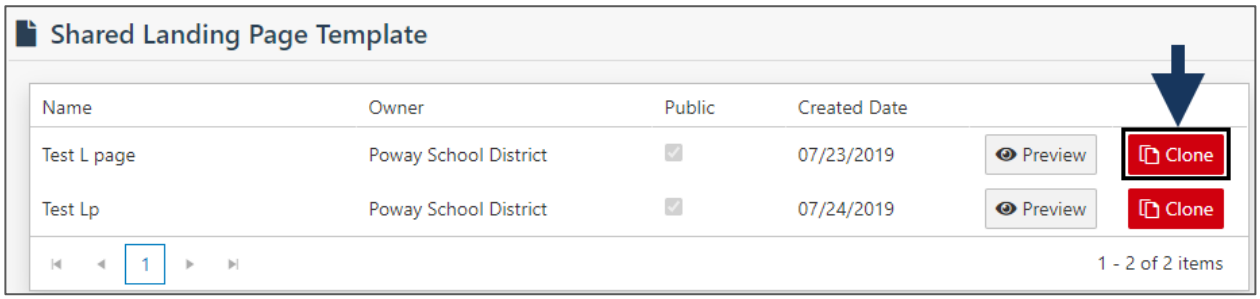
Expand the Landing Pages section and click **Shared with me** to access public landing pages. Public means another user clicked the “Share” checkbox. You will be able to see the organization owner of the shared template.



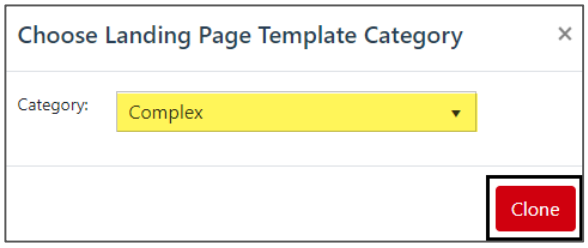
Clone a Shared Landing Page

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 save the cloned template in. Click **Clone**.



4. The cloned email template will appear in your specified category and a pop-up window will display. Click the link to navigate to the Category specified in the previous step or click **Ok** to stay in the **Shared with me window**.

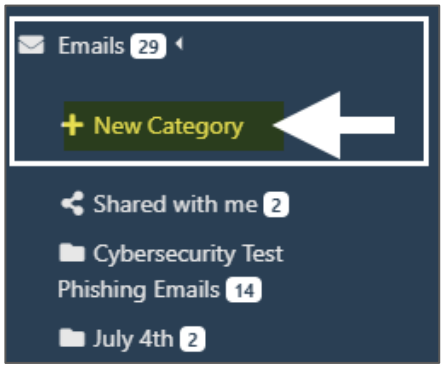
Email Templates

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

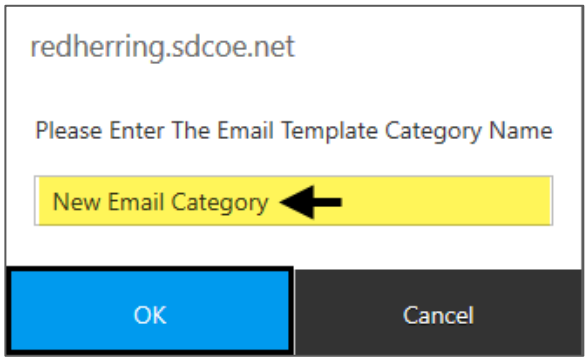
Create a New Email Templates

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*



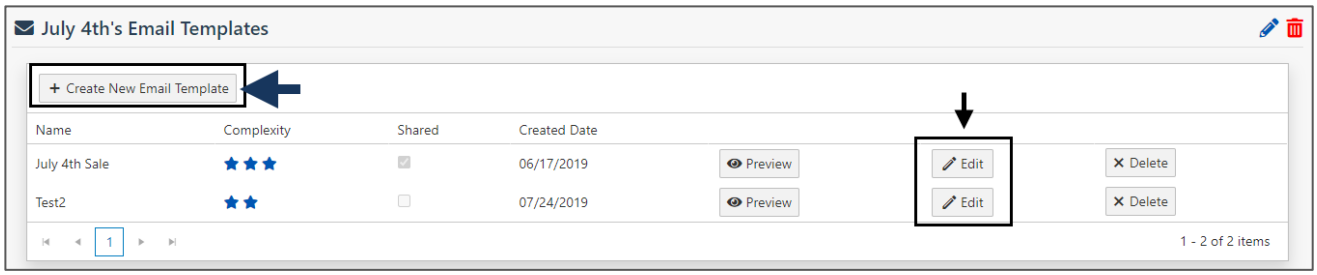
3. Click **OK**.

Rename/Delete a Category

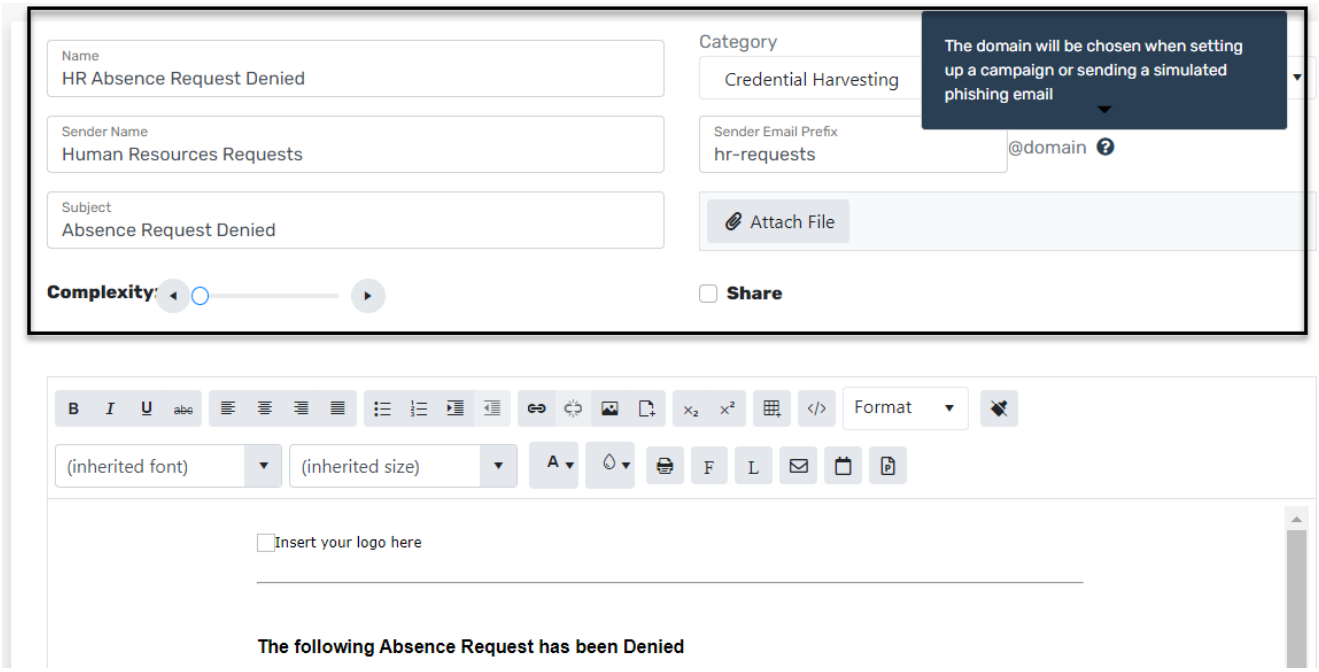
You can rename or delete a category by using the icons to the far right of the category name.

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.



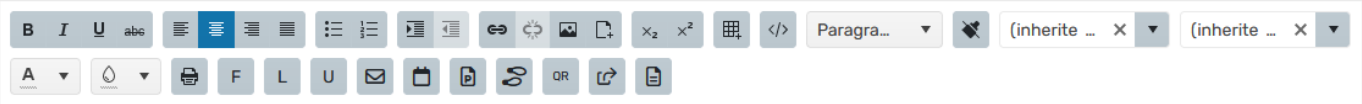
2. Enter the details for the template.



- **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 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

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.

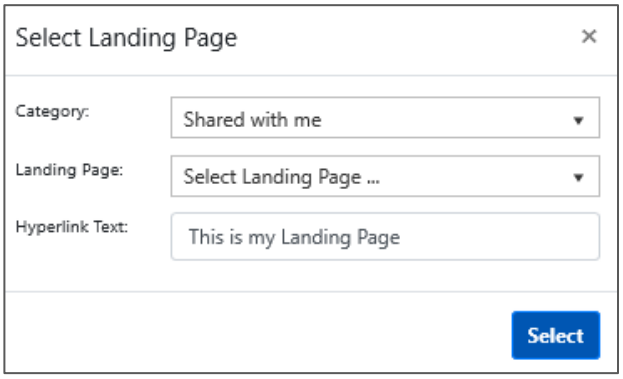
Email Template	Phishing Email Sent to Recipient
Hello {username} of {emailaddress}	Hello jdoe of jdoe@my.org
Hello {username} of {emailaddress}	Hello joe.public of joe.public@my.org

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

This will enter 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.



Insert Footer

This will insert a footer at bottom of email with an Unsubscribe link. If the Target User clicks on the Unsubscribe link will not affect their Risk Score and they will be directed to a page explaining:

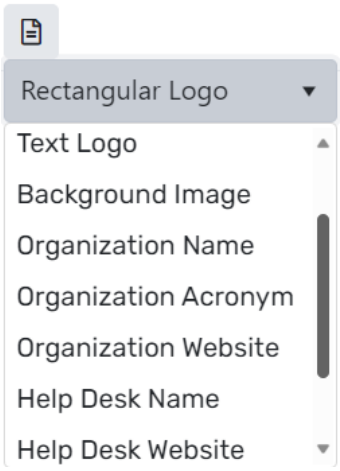
“As part of our ongoing efforts to enhance cybersecurity awareness among SDCOE employees, your organization has conducted a simulated email phishing exercise. If you receive any suspicious emails, please promptly forward them to our Help Desk at {organization email}”

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 information 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.

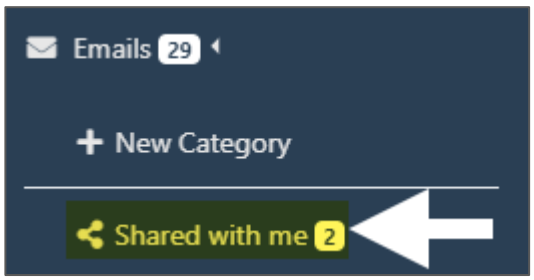


Test an Email Template

While in the Email Category view, you may click the **Test** button next to an Email to automatically send the email to the email address associated with your Red Herring admin account so that you may ensure the email displays correctly.

Shared Email Templates (Public)

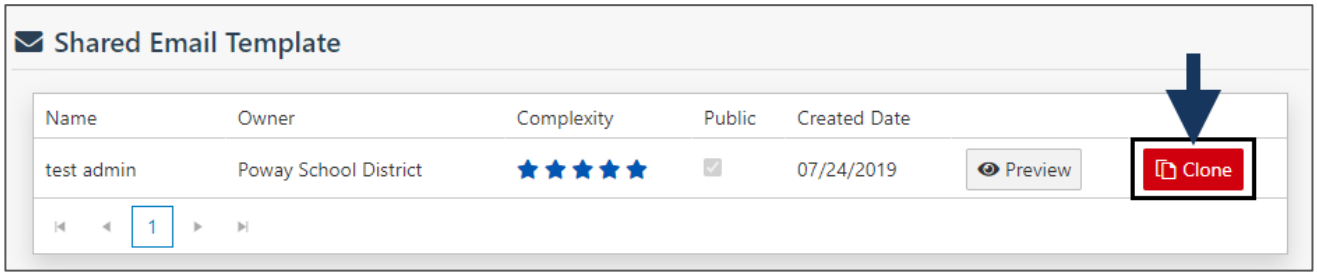
Expand the Emails section and click **Shared with me** to access public email templates. Public means another user clicked the “Share” checkbox. You will be able to see the organization owner of the shared template.



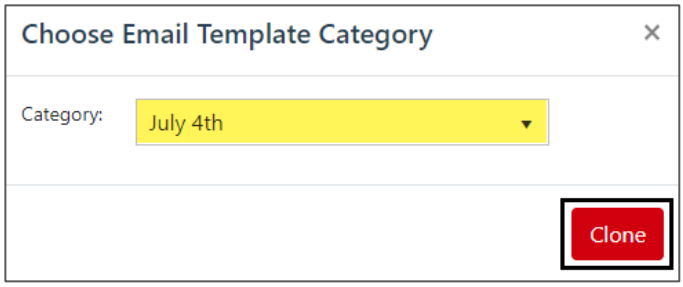
Clone an Email Template

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 that you would like to save the cloned template in. Click **Clone**.



4. The cloned email template will appear in your specified category and a pop-up window will display. Click the link to navigate to the Category specified in the previous step or click **Ok** to stay in the **Shared with me** window.

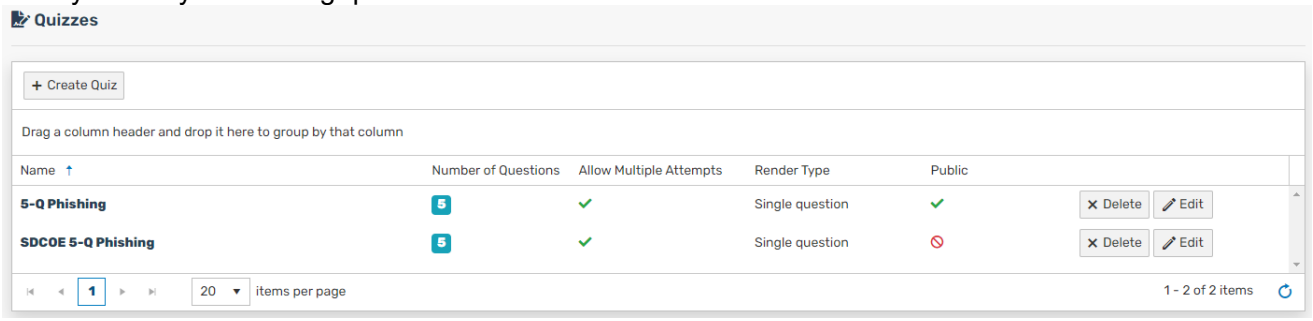
Knowledge Assessments (Quizzes)

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.

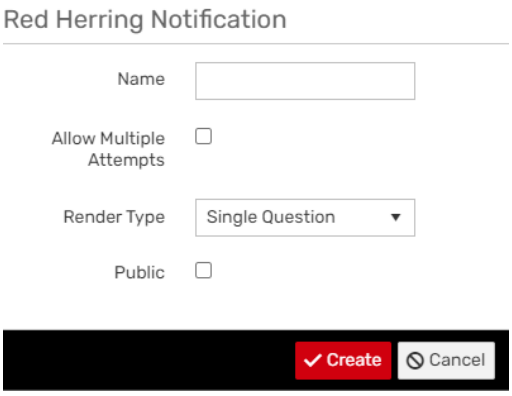
You may revies a summary of quiz activity in the **Campaign Report** or view detailed quiz results on a Target User's report page.

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.



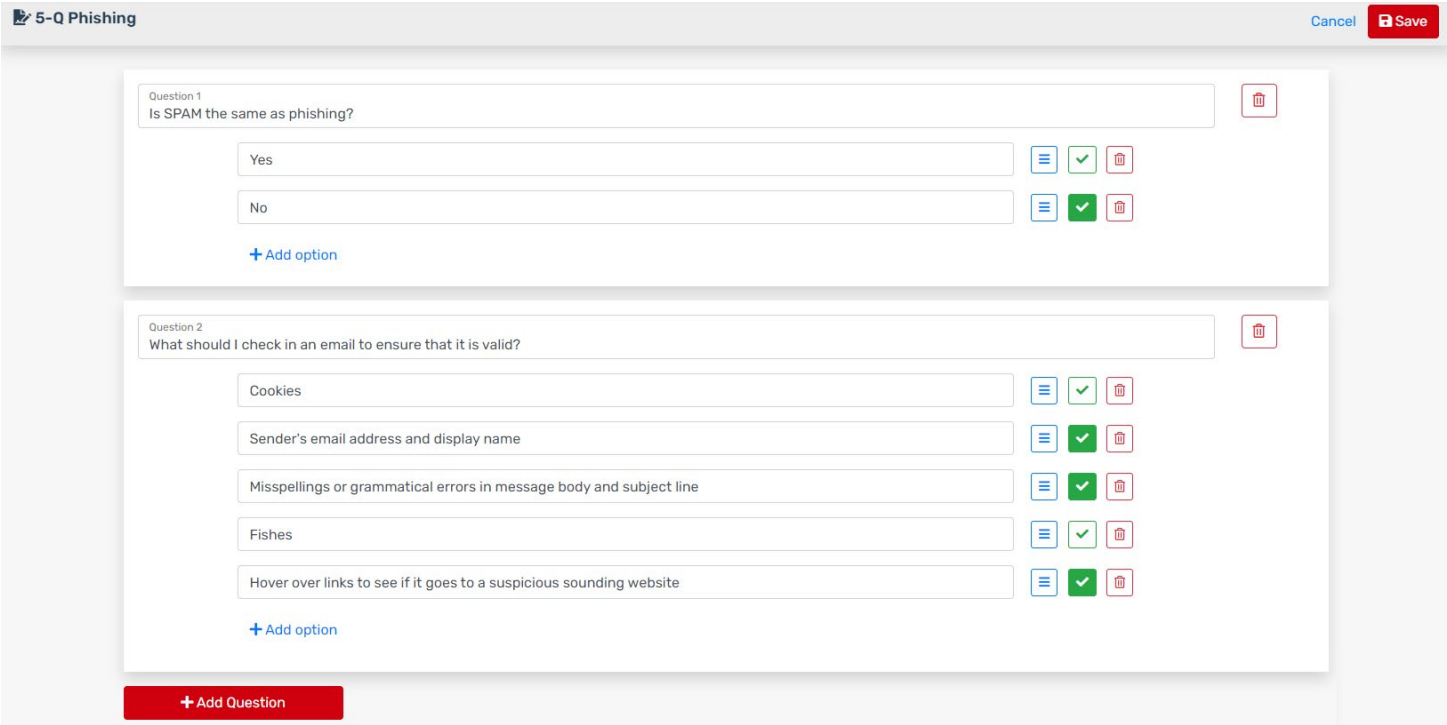
2. Enter a **Name** for the Knowledge Assessment. This name is just for your reference.
    - Check **Allow Multiple Attempts** if the target user will be allowed to take the quiz multiple times or just once.
    - **Render Type**: This feature is currently unavailable.



    - **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 (hamburger) 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** button 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.

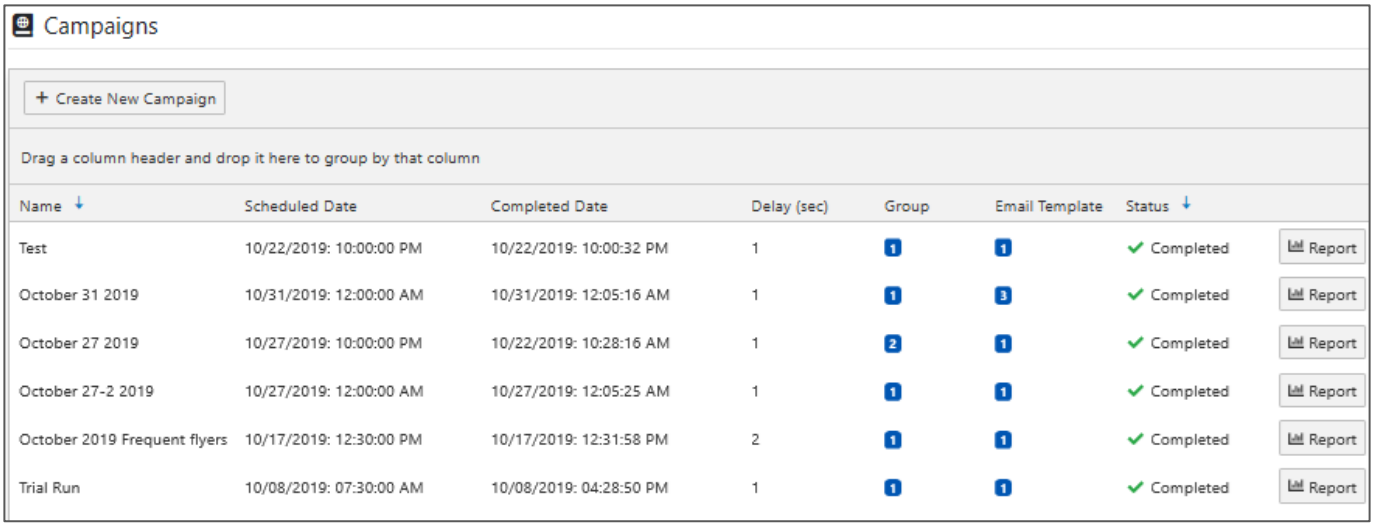


Phishing Campaigns (Scheduled)

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

View Your Campaigns

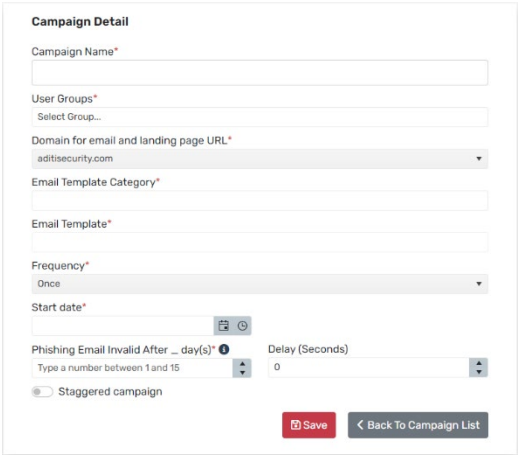
You may view the scheduled and completed campaigns from the Campaigns page along with scheduled and completion dates, current status, and the option to view the full report for each completed campaign.



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 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.
    - 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.
- **Phishing Email Invalid After _ day(s)**: This setting determines how long the simulated phishing link in email will be valid for. Once link has expired, link clicks will no longer be tracked and the target user will be redirected to a static Red Herring page.
- **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
- **Staggered campaign:** Sends emails to your target users in stages. You can choose to send to 10%, 25%, or 50% of the selected user group(s) every 1-12 hours, until all recipients have received the email.

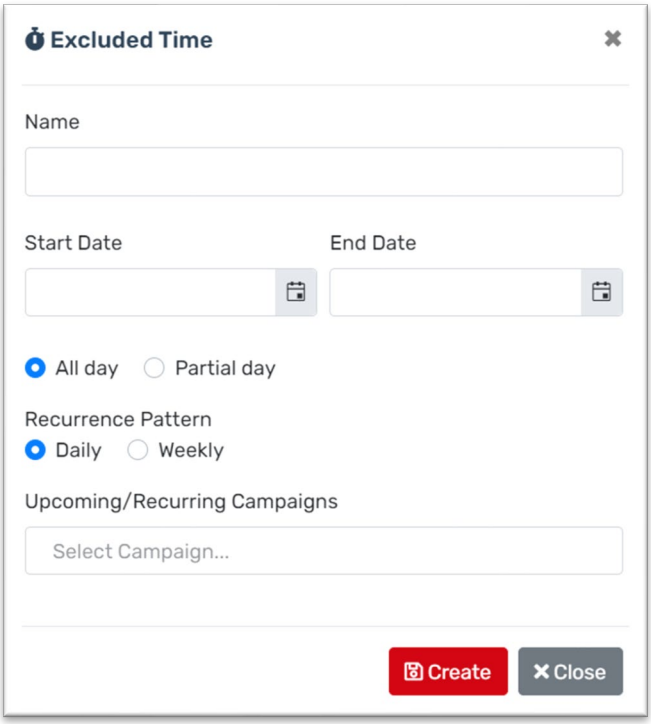
3. Click **Save**.

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**

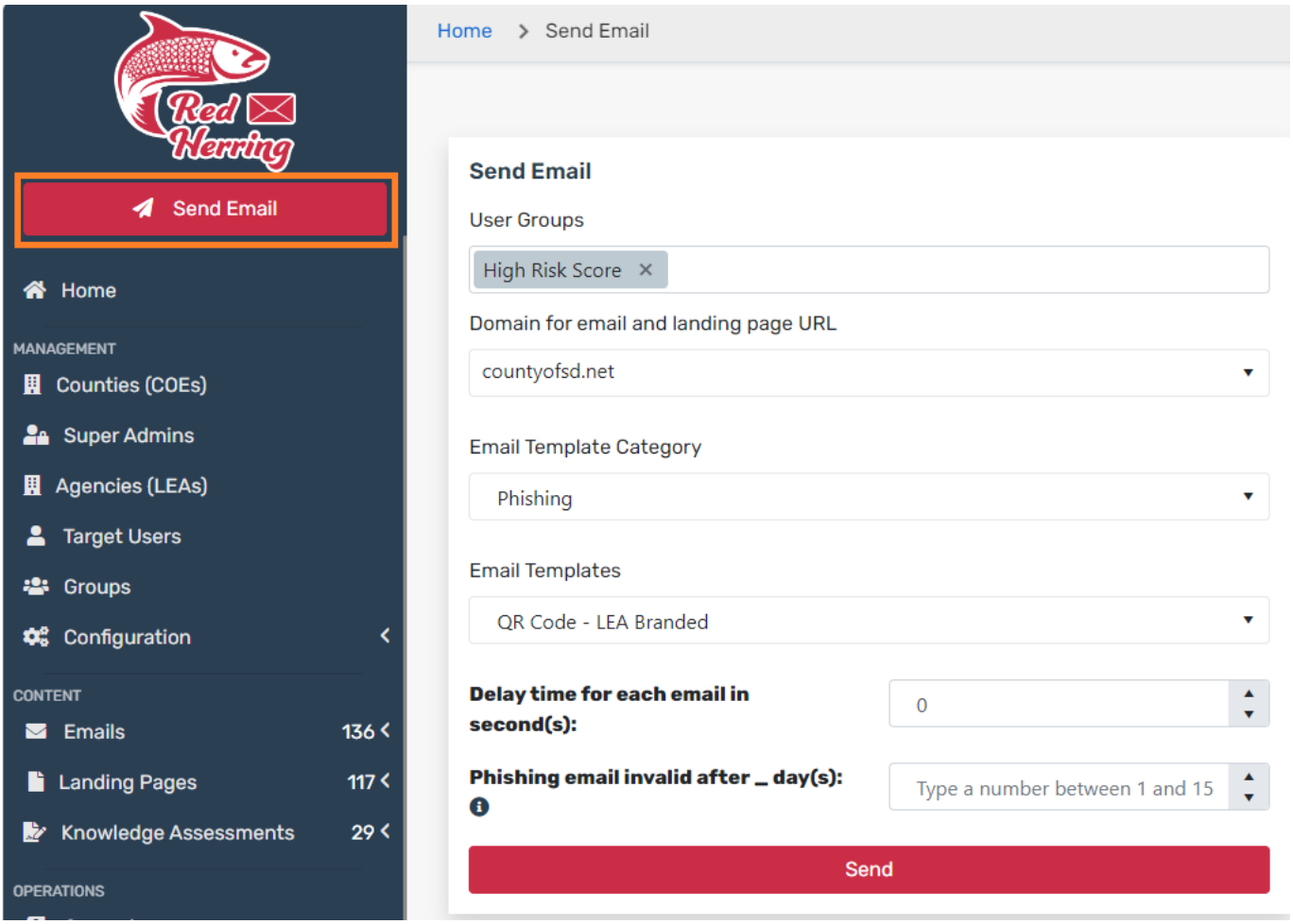


Send a Phishing Email (Ad Hoc)

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.)
- **Phishing Email Invalid After _ day(s)**: This setting determines how long the simulated phishing link in email will be valid for. Once link has expired, link clicks will no longer be tracked and the target user will be redirected to a static Red Herring page.



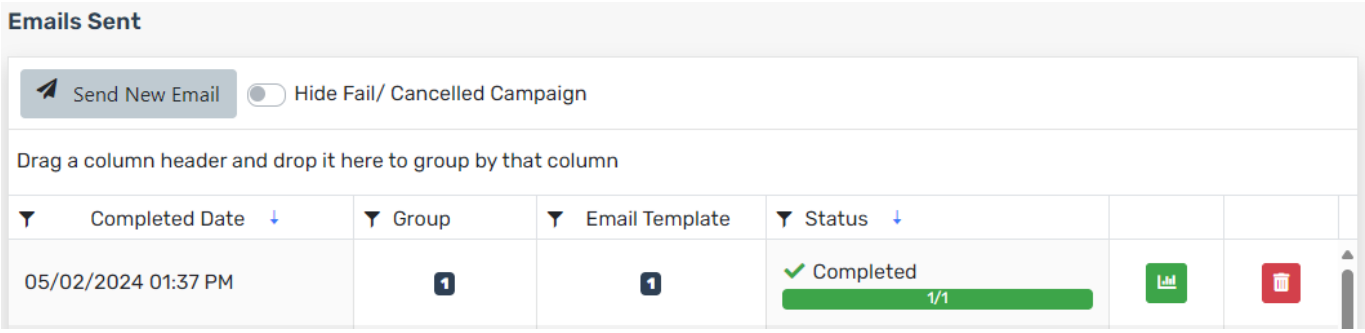
View your Emails Sent

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.

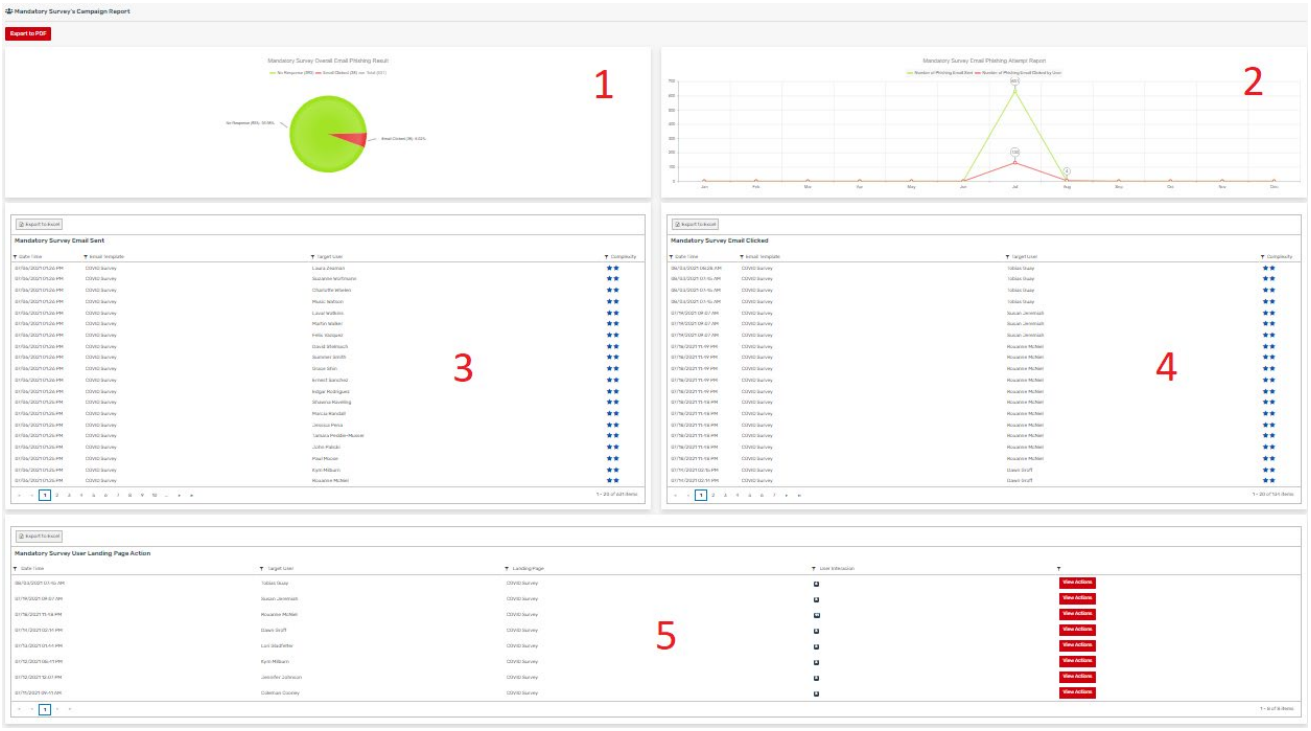
- Click the number in the Group or Email Template column to quickly view the Group(s) that the email was sent to or the Email Template(s) that was used.
- Click the bar graph symbol to view the results and metrics gathered from the sent email.
- To delete a Sent Email, click the Delete button to the 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.
- The columns have a filter icon, allowing you to organize the displayed data as needed.



Campaign Results Report

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

2. View the results.

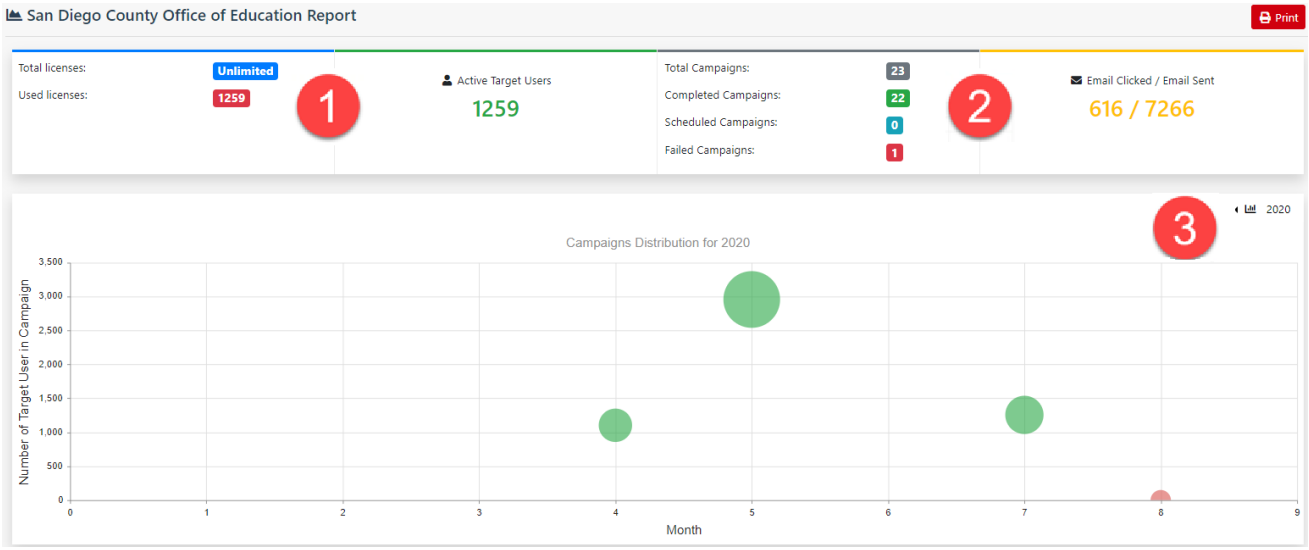


1	**Pie Chart:** Shows the overall results for how many users received the email and opened the phishing link. Shows the number of emails and the percentage. In this example 6.02% clicked the email (shown in red in the pie chart).
2	**Line Graph:** Shows the total click-thrus by date.
3	**Email Sent:** 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 the user for more details on user activity such as if they viewed a training video or completed a quiz.

NOTE: Click Export Options to export the report to a PDF or to directly email the report to a third party.

District Report

1. 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.



1	**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.
2	**Upper Right:** Shows your overall totals since the time you started using Red Herring.
3	**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

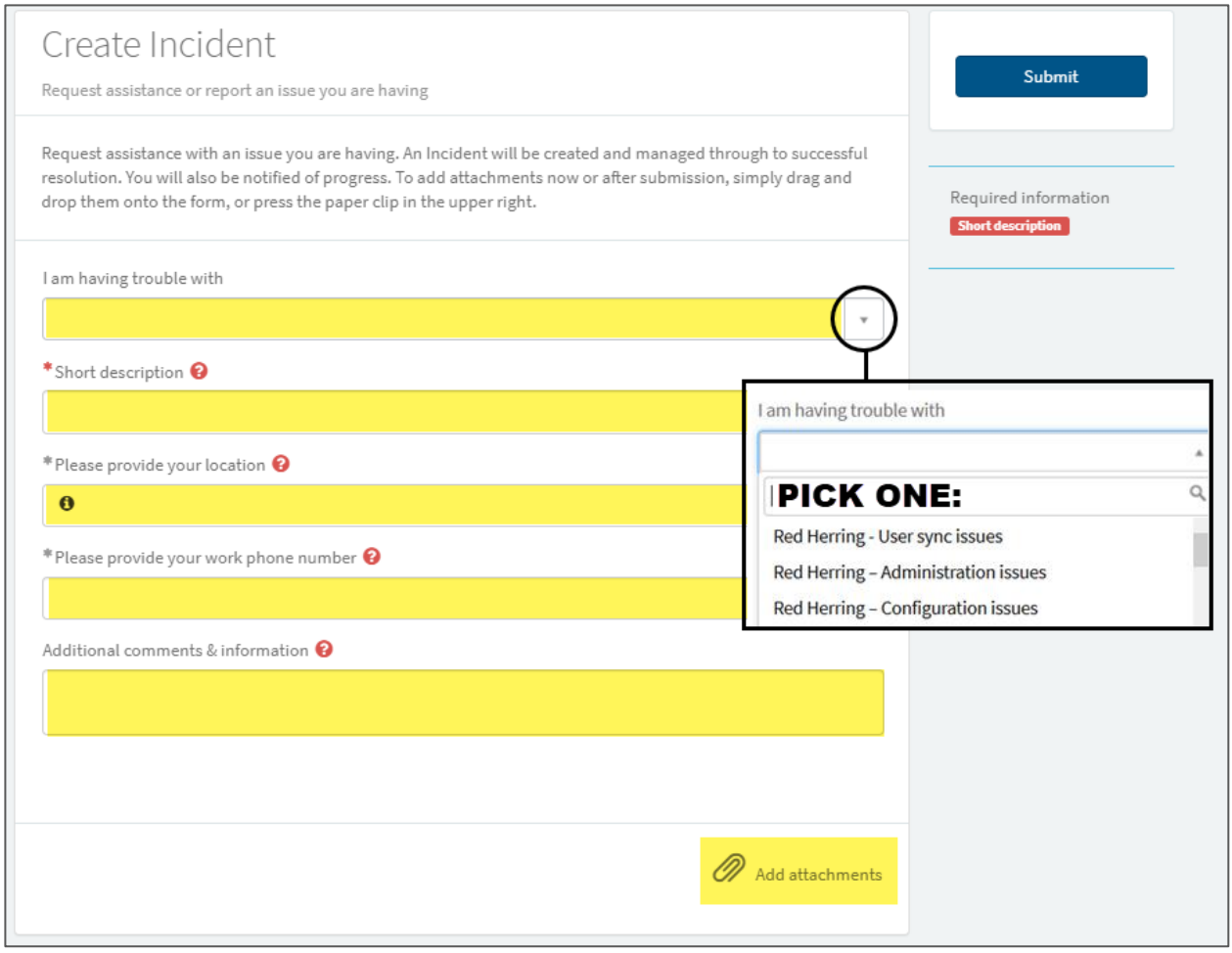
As part of your Red Herring on-boarding process you will be given an account on SDCOE's ServiceNow customer support platform. There will only be one authorized user per agency (district or COE) that will be able to submit ServiceNow requests to SDCOE. Districts that are on Red Herring through their COE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



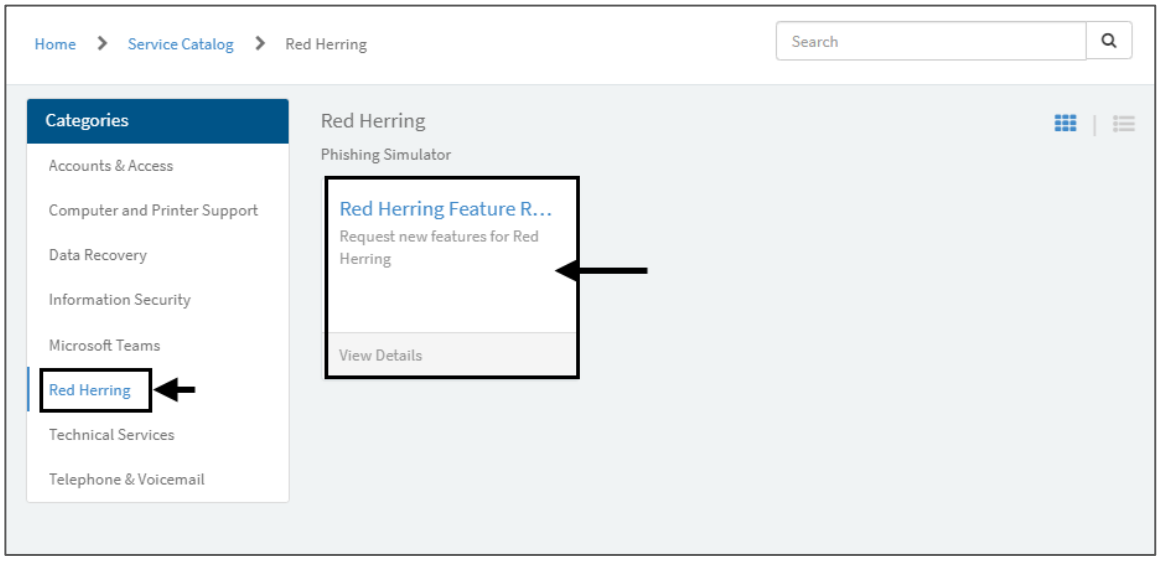
- **I am having trouble with:** Select one of the Red Herring options.
  - **Red Herring - Administration issues:** User Log-In, Email or Landing Page Templates, Reports
  - **Red Herring - Configuration issues:** SMTP Configuration, Email problems, Campaign, Groups, Video Playback
  - **Red Herring - 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 the problem.
- **Add attachments:** Click here to upload a screenshot.

2. Click **Submit**.

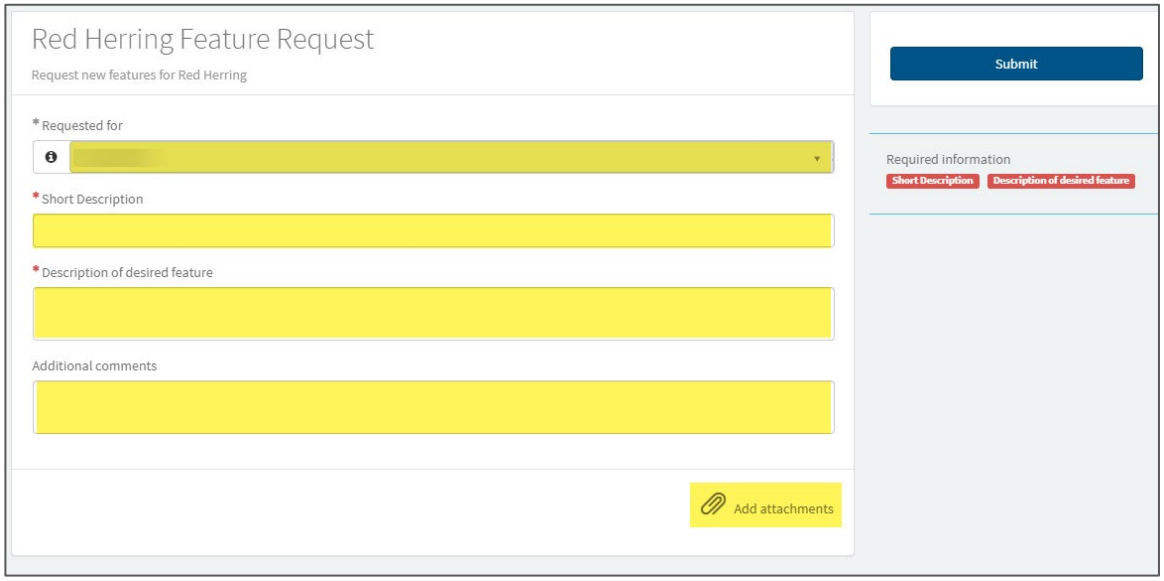
Request Something

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:



- **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.
- **Additional comments:** IMPORTANT: Please be descriptive and attach a screenshot of the problem.
- **Add attachments:** Click here to upload a screenshot.

4. Click **Submit**.

Sending a Test Campaign

Create Red Herring User Group

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

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

Clone a Red Herring User Email Template

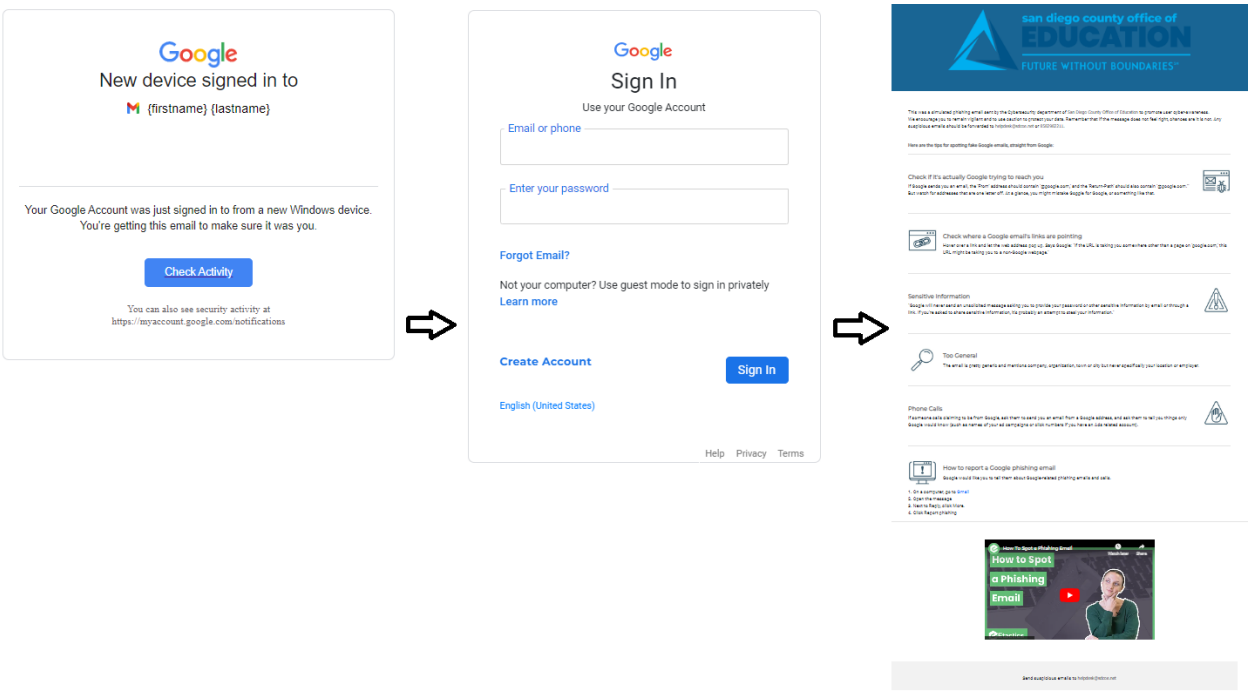
1. Navigate to Red Herring
2. Search for Google or any keyword in the top-right search bar

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

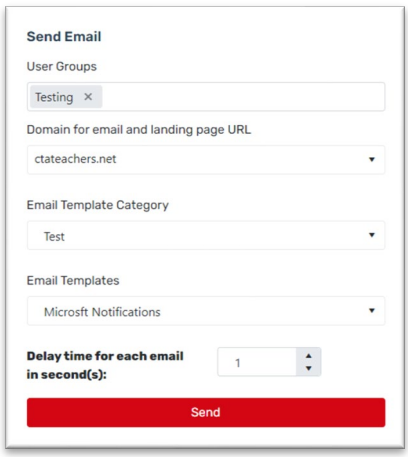
Send a Test Phishing Campaign

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

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

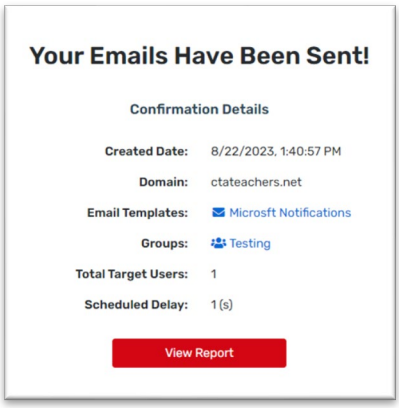


1. Navigate to Red Herring > Send Email
    a. For User Groups select your Testing group
    b. Choose one of the custom domains such as ctateachers.net
    c. For Email Template Category select your Default category
    d. Finally select the email to send and click Send

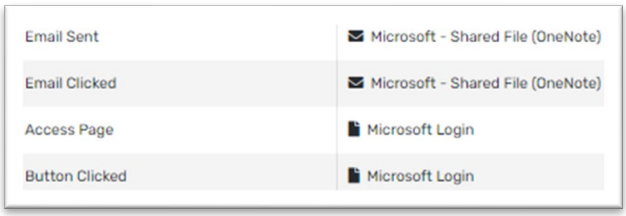


2. Find the email in your inbox
    a. Click on any links in the email and landing page
    b. Fill out any form fields
    c. View video if present
    d. Complete Knowledge Assessment if present

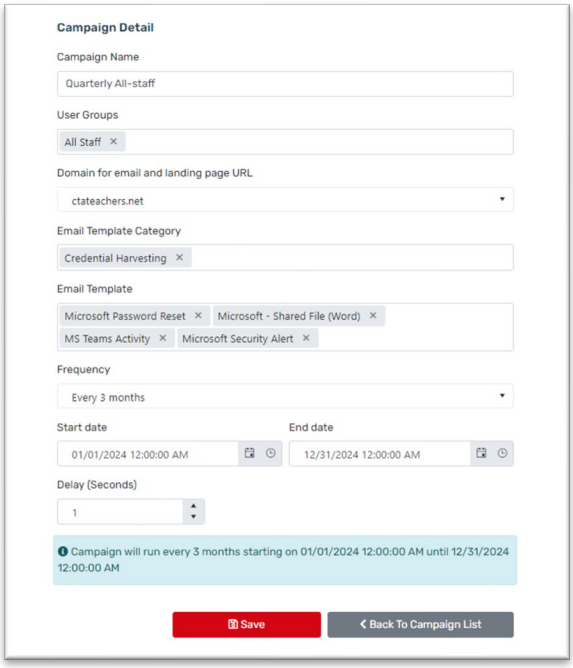
3. Click on View Report or Emails Sent and then view the Campaign Report for the email you just sent



4. Verify telemetry shows in the email campaign report



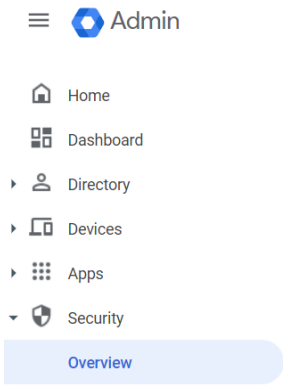
5. Delete the Email once the test is completed
6. Schedule a department/division/all-staff campaign by navigating to Campaigns > **+Create New Campaign**
    a. Here is an example of a quarterly campaign that will randomly send a different email once every quarter



Enable Google Less Secure Apps

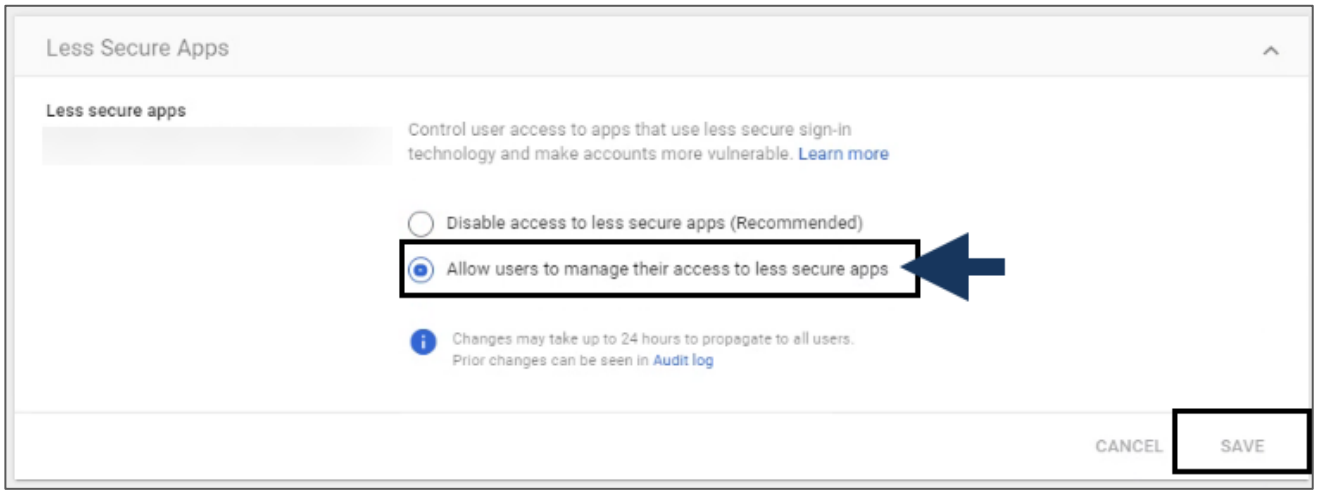
Follow these steps to allow Red Herring access to use Gmail as SMTP server. MFA will have to be turned off for the Google User Account or an App Password will have to be configured for Red Herring.
NOTE: Google may be phasing out this feature.

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