

# Red Herring

## Microsoft Quick Start





## Table of Contents

Helpful Resources .....	2
List of IPs and Custom Domains used with Red Herring .....	2
Configuration.....	2
County Office of Education (COE) Admins .....	3
Local Education Agency (LEA) Admins .....	3
Settings .....	4
Microsoft Allowlist (Advanced Delivery) .....	4
Inbound Anti-spam Policy & Connection Filter .....	6
Exchange Mailflow Rule .....	7
Sender Policy Framework (SPF).....	9
Microsoft Azure (Entra) User Sync.....	10
Sync Target Users (On-Premise AD).....	17
Create Red Herring User Group .....	18
Configure LEA Branded Settings .....	18
Clone a Red Herring User Email Template .....	18
Send a Test Phishing Campaign.....	19




## Helpful Resources

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

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



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

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

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

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

192.40.172.4, 192.40.172.139, 20.118.176.15, 20.118.176.58, 20.118.176.59

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

## Configuration

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



## County Office of Education (COE) Admins

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

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

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

## Local Education Agency (LEA) Admins

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

We currently have three LEA admin levels

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

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

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

Confirm Email



## Settings

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

### Profile

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

The available text fields are:

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

The available logo/images are:

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

## Microsoft Allowlist (Advanced Delivery)

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

**Note:** An A5/E5 license may be needed. Please refer to the **Exchange Mailflow Rule** section if further allowlisting is needed.

1. Open the Microsoft 365 Defender portal at [security.microsoft.com](https://security.microsoft.com)



2. Under the **Email & collaboration** section, navigate to:  
Policies & Rules > Threat Policies > Advanced Delivery  
<https://security.microsoft.com/advanceddelivery>
3. Select the **Phishing Simulation** tab
4. Select Edit/Add/Configure
5. For **Sending IP** addresses enter:  
192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.59, 20.118.176.15
6. For **Domain** enter the domains that you would like to use in your campaigns:  
aditisecurity.com  
countyofsd.net  
ctateachers.net  
edufinancial.org  
edupointonline.com  
glooglonline.com  
gmailonline.us  
highunion.net  
infinite-campus.org  
peoplesoftsdcoe.com  
sandiegocoe.net  
schoolunified.net  
servicecounty.net  
sdc0e.net  
sdcoes.net  
sdcounty.net  
sfcoe.org  
sfusds.net  
uniondistrict.net
7. For **Simulation URL** enter the domains that you would like to use in your campaigns:  
\*.aditisecurity.com/\*  
\*.countyofsd.net/\*  
\*.ctateachers.net/\*  
\*.edufinancial.org/\*  
\*.edupointonline.com/\*  
\*.glooglonline.com/\*  
\*.gmailonline.us/\*  
\*.highunion.net/\*  
\*.infinite-campus.org/\*  
\*.peoplesoftsdcoe.com/\*  
\*.sandiegocoe.net/\*  
\*.schoolunified.net/\*  
\*.servicecounty.net/\*  
\*.sdc0e.net/\*  
\*.sdcoes.net/\*  
\*.sdcounty.net/\*  
\*.sfcoe.org/\*  
\*.sfusds.net/\*  
\*.uniondistrict.net/\*



This most likely will be all that is needed to allow Red Herring emails through your Anti-Spam filter. Please try sending a test email (page 19) through Red Herring and continue with the directions on the next section if you still experience anti-spam filtering of emails from Red Herring.

## Inbound Anti-spam Policy & Connection Filter

The following directions will guide you through the process of setting up an allowlist on your Inbound Anti-spam policy. Adding domains to this list ensures messages are always delivered.

**Note:** An A5/E5 license may be needed. Please refer to the **Exchange Mailflow Rule** section if further allowlisting is needed.

1. Open the Microsoft 365 Defender portal at [security.microsoft.com](https://security.microsoft.com)
2. Under the **Email & collaboration** section, navigate to:  
Policies & Rules > Threat Policies > Anti-spam policies  
<https://security.microsoft.com/antispam>
3. Select **Anti-spam inbound policy (Default)**
4. Scroll down to the section: **Allowed and blocked senders and domains**
5. Click **Edit allowed and blocked senders and domains**
6. Under the Allowed > Domains section, click **Allow domains**
7. Click **+Add Domains**, enter the domains that you would like to use in your campaigns:  
aditisecurity.com  
countyofsd.net  
ctateachers.net  
edufinancial.org  
edupointonline.com  
glooglonline.com  
gmailonline.us  
highunion.net  
infinite-campus.org  
peoplesoftsdcoe.com  
sandiegocoe.net  
schoolunified.net  
servicecounty.net  
sdc0e.net  
sdcoes.net  
sdcounty.net  
sfcoe.org  
sfusds.net  
uniondistrict.net
8. Click **Save** then **Close**

You may optionally add Red Herring IPs as “trusted” in your connection filter policy.

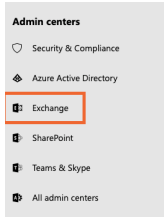
1. In the same **Anti-spam policies** section (<https://security.microsoft.com/antispam>)
2. Select **Connection filter policy (Default)**
3. Click **Edit connection filter policy**
4. Add: 192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.59, 20.118.176.15
5. Click **Save**



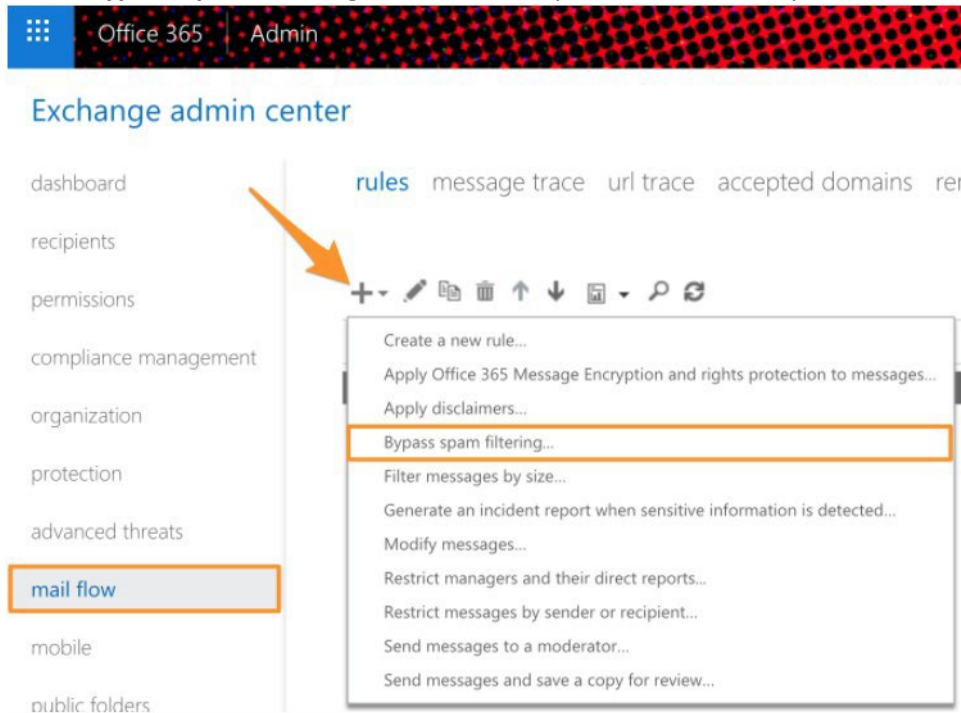
## Exchange Mailflow Rule

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

1. Log in to your mail server Admin portal. Then, navigate to Admin centers > Exchange <https://admin.exchange.microsoft.com>



2. Select **Mail Flow > Rules** and click on the + sign located in the top-left
3. Select **Bypass Spam Filtering...** from the drop-down. This will open the **new rule** screen





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

Bypass Clutter and Spam Filter by IP Address

Name:  
Bypass Clutter and Spam Filter by IP Address

\*Apply this rule if...  
Sender's IP address is in the range... '147.160.167.0/26' or '23.21.109.212' or '23.21.109.197'

Select one

- The sender... (selected)
- The recipient...
- The subject or body...
- Any attachment...
- Any recipient...
- The message...
- The sender and the recipient...
- The message properties...
- A message header...
- [Apply to all messages]

add exception

is this person  
is external/internal  
is a member of this group  
address includes any of these words  
address matches any of these text patterns  
is on a recipient's supervision list  
has specific properties including any of these words  
has specific properties matching these text patterns  
has overridden the Policy Tip  
IP address is in any of these ranges or exactly matches domain is

6. Enter our IP addresses “192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.59, 20.118.176.15” on separate lines of the **specify IP address** screen and click the + sign. Then, click the **OK** button.

Bypass Clutter and Spam Filter by IP Address

Name:  
Bypass Clutter and Spam Filter by IP Address

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

\*Do the following...  
Set the message header to this value...  
and  
Set the spam confidence level (SCL) to...  
add action

Except if...  
add exception

Properties of this rule:  
Priority:

specify IP address ranges

Enter an IPv4 address or range +

OK Cancel

Sender's IP address is in the range... '23.21.109.212' or '23.21.109.197'

Save Cancel



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

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.

Return to Red Herring > Configuration > SMTP and enter your organization specific SMTP connection information. Then click update and check your Inbox for an email from [noreply@sdcoe.net](mailto:noreply@sdcoe.net).

## 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 ip4:20.118.176.59

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



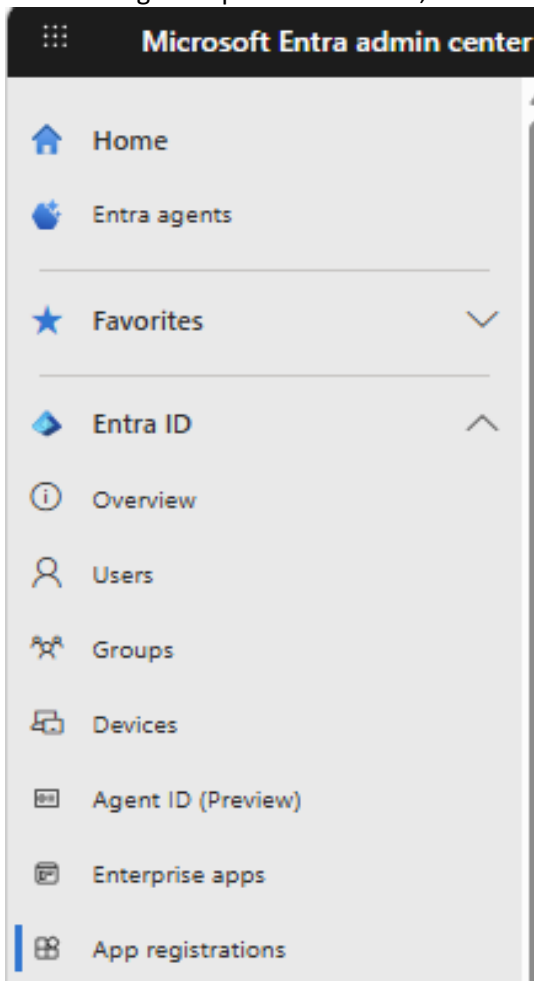
## Microsoft Azure (Entra) User Sync

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**; which you will then enter in Red Herring.

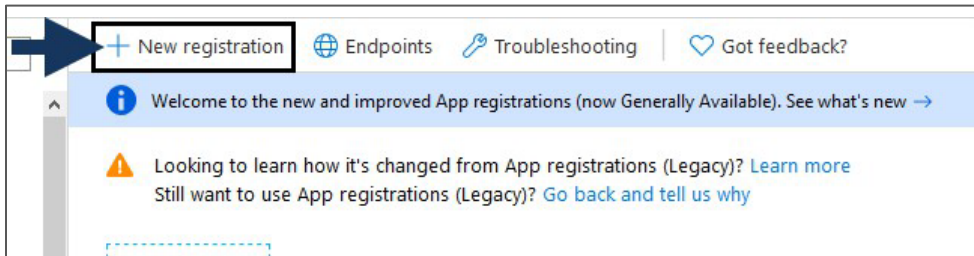


1. Log in to <https://entra.microsoft.com> using your Azure administrative account.
2. In the navigation pane on the left, select **Entra ID > App registrations**.





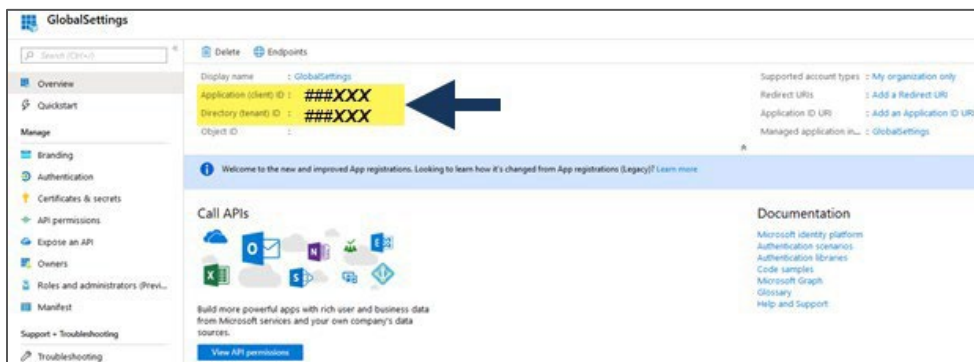
### 3. Click **New registration**.



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

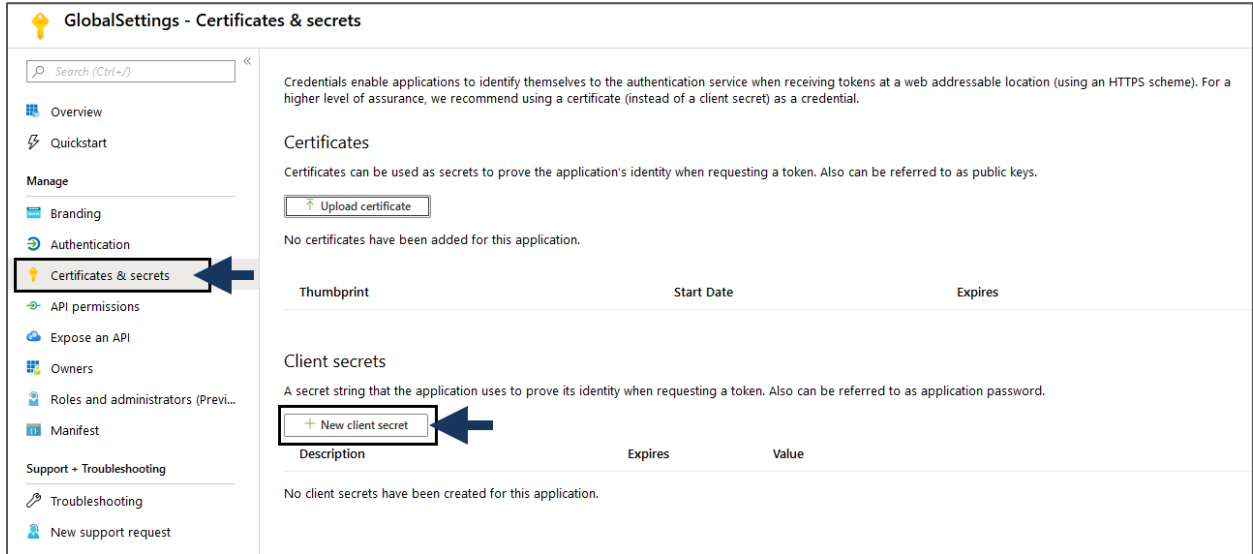
- Name:** Enter a name for the application. *Example: Red Herring*
- Supported account types:** Select *Accounts in this organizational directory only*

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

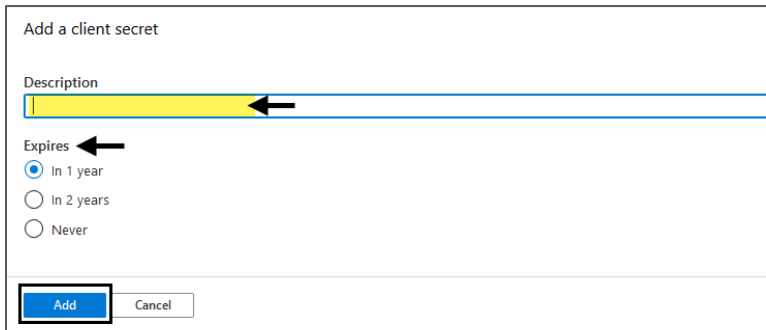




6. In the navigation on the left, select **Certificates & secrets**. Then select **New client secret**.



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



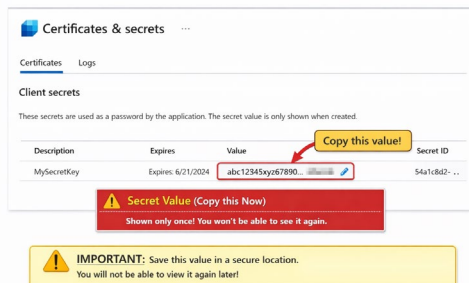
### NOTES ABOUT AN EXPIRED SECRET KEY:

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

8. **Copy the "value" of 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.**

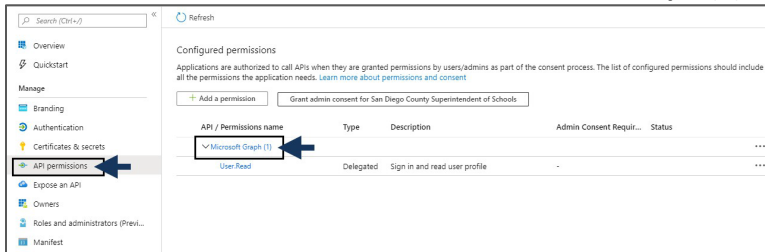
### Copy the Client Secret Value

Make sure to copy the secret value immediately!

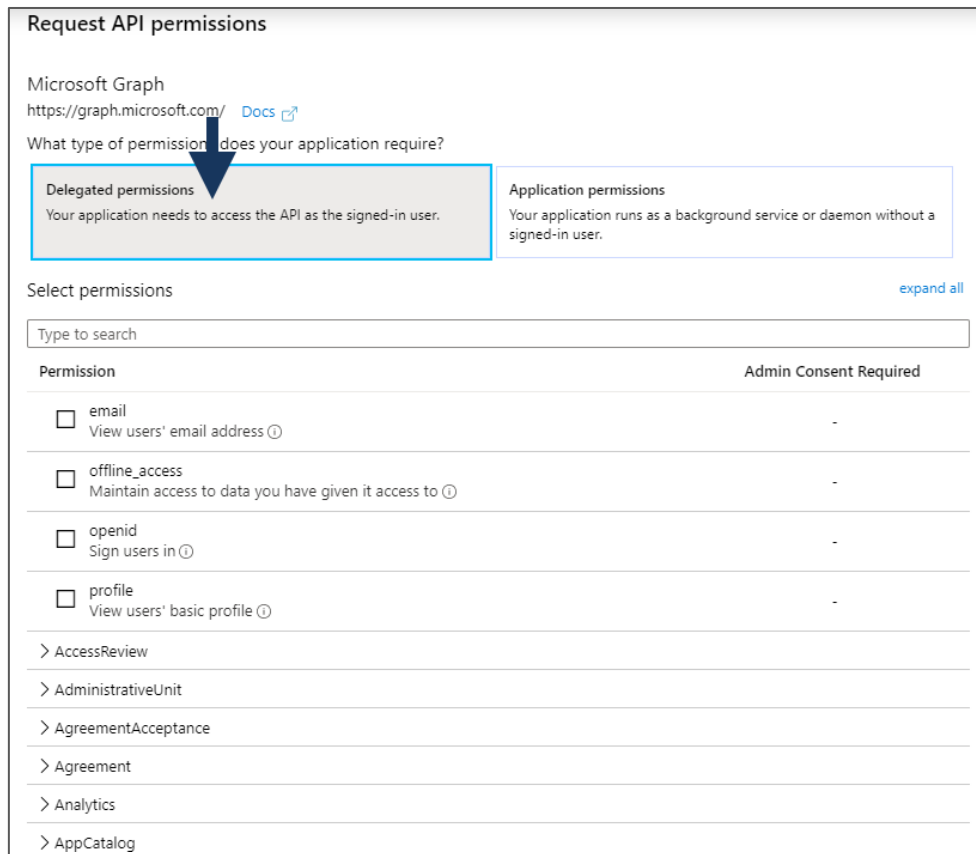




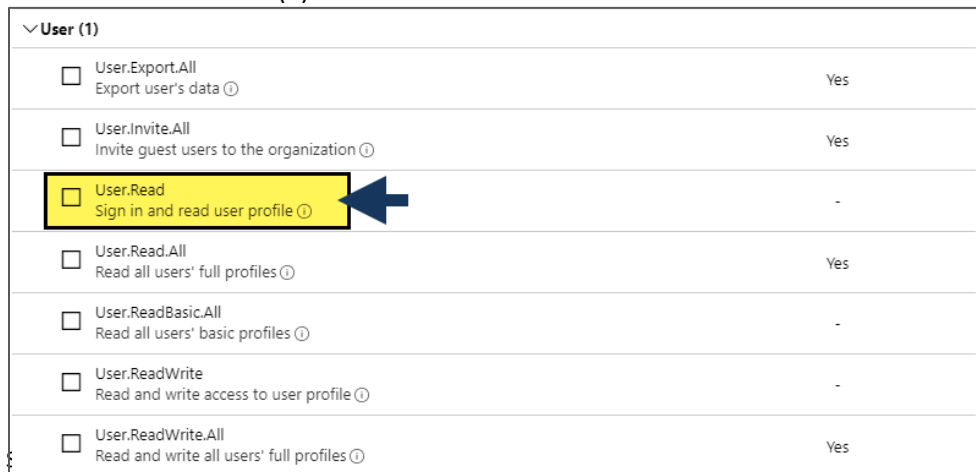
9. Click **API Permissions**. Then select the **Microsoft Graph (1)** link.



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



...scroll down to **User.(7)** section and uncheck the **User.Read** checkbox.





## 11. Select **Application permissions**.

Request API permissions

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

What type of permissions does your application require?

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

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

Select permissions expand all

## 12. Scroll down to the Directory.(7) section, expand the Directory, and check **Directory.Read.All**.

▼ Directory (1)

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

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

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

## 15. Click **Update permissions**.

## 16. Select **Grant admin consent for [your.organization]**.

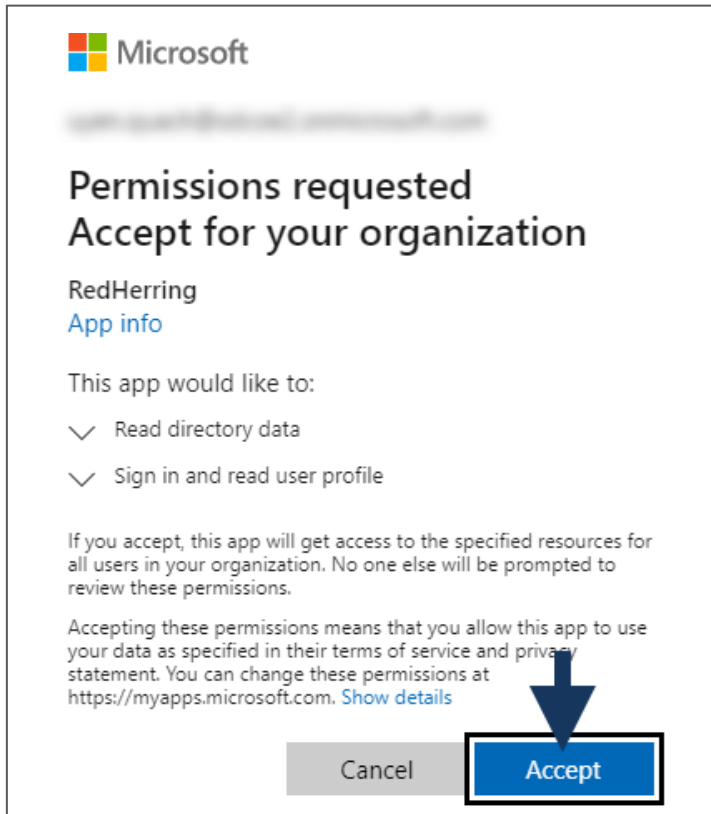
⚠ Permissions have changed, please wait a few minutes and then grant admin consent. Users and/or admins will have to consent even if they have already done so previously.

Configured permissions

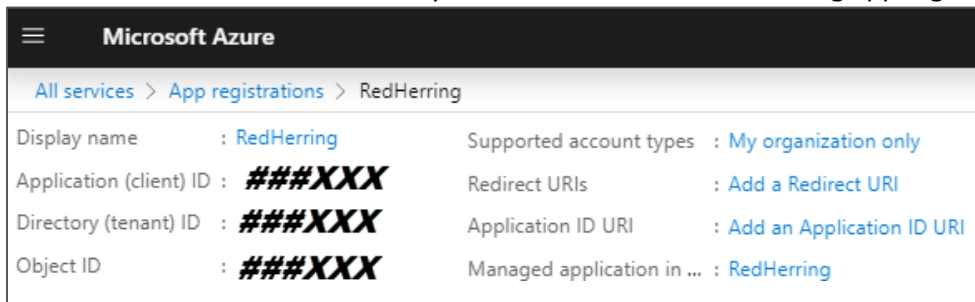
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

API / Permissions name	Type	Description	Admin Consent Requir...	Status
▼ Microsoft Graph (1)				
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for San Die... <span>...</span>

## 17. Azure will ask you to select the admin login account.



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



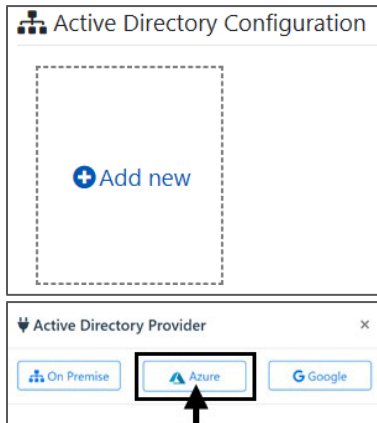
**IMPORTANT:** You will later input this information in Red Herring at Step 22.



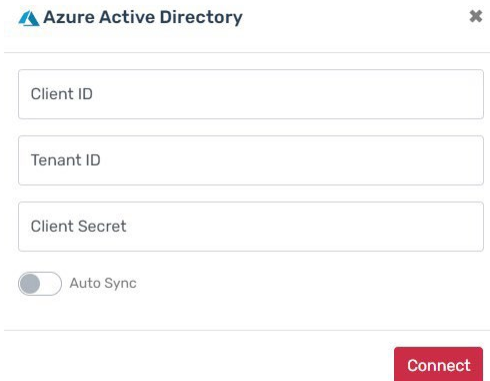
## Now go to Red Herring.

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

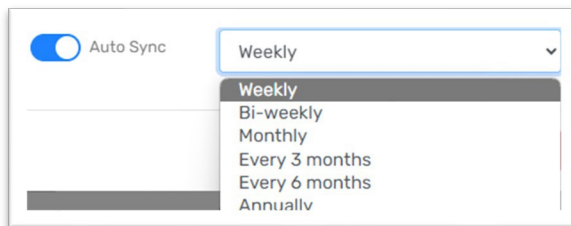
21. Click on the **+ Add new** tile and then select **Azure**.



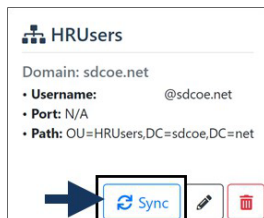
22. Enter your Azure Connection information: **Client ID**, **Tenant ID** and **Client Secret**. Click **Connect**.



23. Enable Auto Sync to automatically sync your directory to Red Herring on a scheduled basis. The sync process will add any new users and remove inactive/suspended accounts.



24. Perform an initial sync to import your AD users at any time. Subsequent syncs will be used to update any new users.

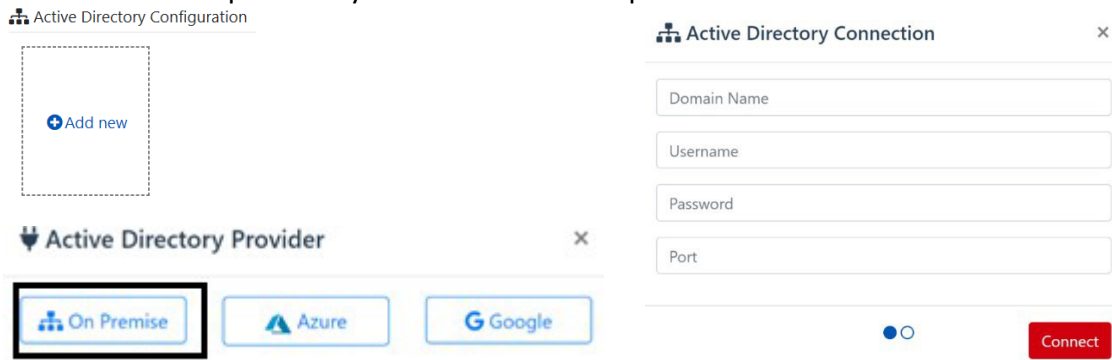




## Sync Target Users (On-Premise AD)

These directions will import users from Azure as Target Users in Red Herring.

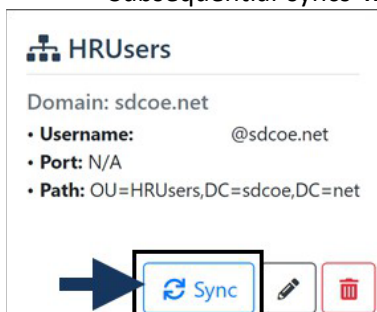
1. In Red Herring go to **Configuration > Directory**.
2. Click on the **+ Add new** tile. Select **On Premise**. Enter your Active Directory Connection information: **Domain Name**, **Username** (with appropriate permissions), and **Password**. The **Port** field is optional if you use the standard 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. Subsequent syncs will be used to update any new users.





## Create Red Herring User Group

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

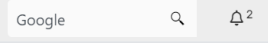
1. Navigate to Red Herring > Groups
2. Select **+Create Group**
3. Name the group **Testing**
4. Optionally create another group for **All Staff**

## Configure LEA Branded Settings

Once you enter your agency's details here, the information will automatically appear on any of the 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

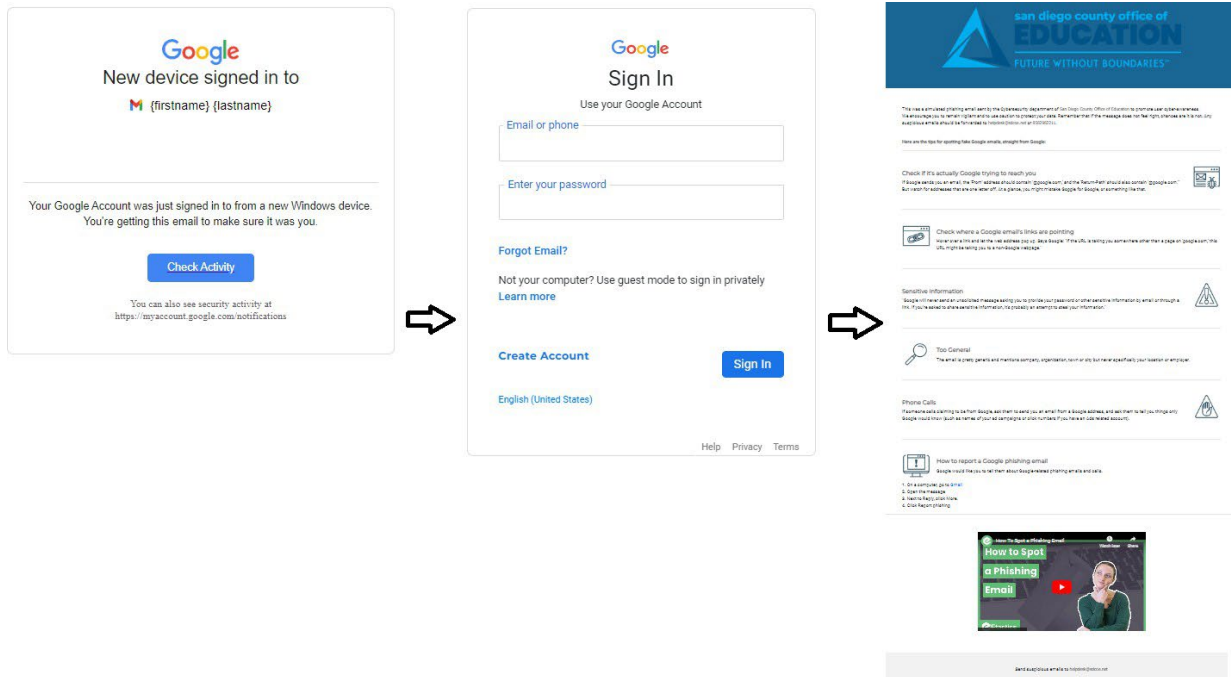
1. Navigate to Red Herring
2. Search for Google or any keyword in the top-right search bar  

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 Default folder  
(a visual example of email to landing page click-path is viewable on the next page)
6. Optionally, you may check the box for Landing Page Templates and clone them if you would like to customize them.  
NOTE: You will have to edit the link in the email template and point it to the Landing Page that you customized.



## Send a Test Phishing Campaign

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

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

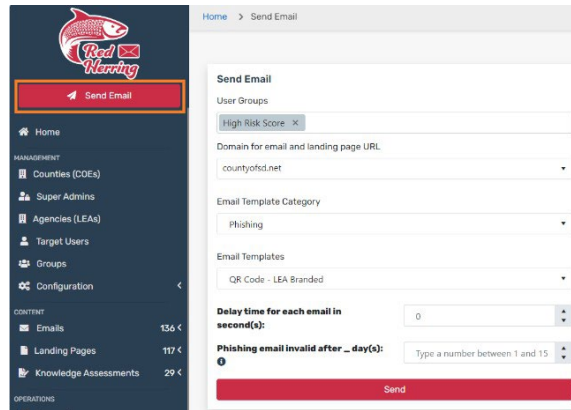


1. Navigate to Red Herring > Send Email

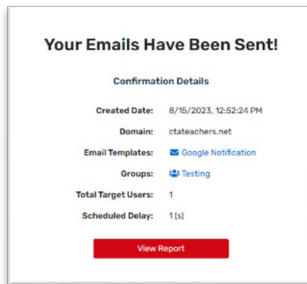
- a. For User Groups select your Testing group
- b. Choose one of the custom domains such as ctateachers.net
- c. For Email Template Category select your Default category
- d. Select the email to send
- e. Phishing Email Invalid After \_ day(s): This setting determines how long the simulated phishing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



- g. Click the red Send button



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



4. Verify telemetry shows in the email campaign report

Email Sent	Google Security Alert
Text Input	Google Login
Video Started	Google User Awareness
Video Completed	Google User Awareness

5. Delete the Email once the test is completed
6. Schedule a department/division/all-staff campaign by navigating to Campaigns > **+Create New Campaign**



- a. Here is an example of a quarterly campaign that will randomly send a different email once every quarter with the simulated phishing link valid for 3 days for each quarterly campaign

**Campaign Detail**

Campaign Name\*  
Quarterly All-Staff

User Groups\*  
High Risk Score X Medium-High Risk Score X Medium Low Risk Score X  
Low Risk Score X No Risk Score X

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

Email Template Category\*  
Credential Harvesting X

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

Frequency\*  
Every 3 months

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

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

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

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

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