These directions will assist with setting up an Allowlist and Inbound Email Gateway for Gmail to ignore spoofed emails from Red Herring, as well as configuring Red Herring as a trusted app to synchronize target users. Finally, you’ll clone a Google email template and send it through Red Herring to verify functionality.”

Contents

Helpful Resources ............................................................................................................................................. 2
List of IPs and custom domains used with Red Herring .................................................................................... 2
Configuration ........................................................................................................................................................ 3
COE Admins....................................................................................................................................................... 3
LEA Admins ....................................................................................................................................................... 3
Settings ............................................................................................................................................................. 4
Profile............................................................................................................................................................. 4
Microsoft Allowlist (Advanced Delivery) ........................................................................................................... 4
Microsoft Azure User Sync ................................................................................................................................ 9
Sync Target Users ........................................................................................................................................ 17
Sending a Test Campaign .................................................................................................................................... 19
Create Red Herring User Group ................................................................. 19
Configure LEA Branded Settings ................................................................................................................... 19
Create Red Herring Template Categories ................................................................................................... 19
Clone a Red Herring User Email Template .................................................................................................. 19
Send a Test Phishing Campaign .................................................................................................................... 20
Helpful Resources

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


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.

List of IPs and custom domains used with Red Herring

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

192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.15

<table>
<thead>
<tr>
<th>Generic Domains</th>
<th>Regional Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>aditisecurity.com</td>
<td>countyofsd.net</td>
</tr>
<tr>
<td>cstateachers.net</td>
<td>sandiegocoe.net</td>
</tr>
<tr>
<td>highunion.net</td>
<td>sdc0e.net</td>
</tr>
<tr>
<td>schoolunified.net</td>
<td>sdcoes.net</td>
</tr>
<tr>
<td>servicecounty.net</td>
<td>sdcounty.net</td>
</tr>
<tr>
<td>uniondistrict.net</td>
<td></td>
</tr>
</tbody>
</table>
Configuration

**COE Admins**

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

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

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

**LEA Admins**

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

We currently have three LEA admin levels

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

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Name</td>
<td>{orgname}</td>
<td></td>
</tr>
<tr>
<td>Organization Website</td>
<td>{orgwebsite}</td>
<td></td>
</tr>
<tr>
<td>Organization Acronym</td>
<td>{orgacronym}</td>
<td></td>
</tr>
<tr>
<td>Help Desk Name</td>
<td>{helpdeskname}</td>
<td></td>
</tr>
<tr>
<td>Help Desk Website</td>
<td>{helpdeskwebsite}</td>
<td></td>
</tr>
<tr>
<td>Help Desk Phone Number</td>
<td>{helpdeskphone}</td>
<td>Only numbers are allowed</td>
</tr>
<tr>
<td>Help Desk Email</td>
<td>{helpdeskemail}</td>
<td></td>
</tr>
</tbody>
</table>

The available logo/images are:

<table>
<thead>
<tr>
<th>Name</th>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rectangular Logo</td>
<td>{rectangularlogo}</td>
<td></td>
</tr>
<tr>
<td>Square Logo</td>
<td>{rectangularlogo}</td>
<td></td>
</tr>
<tr>
<td>Text logo</td>
<td>{textlogo}</td>
<td></td>
</tr>
<tr>
<td>Preferred Background Image</td>
<td>{backgroundimage}</td>
<td>Will not display as background image in emails</td>
</tr>
</tbody>
</table>

**Microsoft Allowlist (Advanced Delivery)**

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

Note: An A5/E5 license may be needed.

1. Open the Microsoft 365 Defender portal at security.microsoft.com
2. Navigate to Policies & Rules under Email & Collaboration
3. Navigate to Threat Policies > Advanced Delivery
   https://security.microsoft.com/advanceddelivery

4. Select the Phishing Simulation tab

5. Select Edit/Add/Configure

6. For IP addresses enter:
   192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.15

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
   - cstateachers.net
   - highunion.net
   - sandiegocoe.net
   - countyofsd.net
   - sdc0e.net
   - saniegocoe.net
   - countyofsd.net
   - sdc0e.net
   - sdc0e.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 page if you still experience Spam filtering with Red Herring emails. Otherwise continue on page 9.
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.

6. Enter our IP addresses “192.40.172.4, 192.40.172.139, 20.118.176.58, 20.118.176.15” on separate lines of 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.
Microsoft 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](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.

2. In the navigation on the left, select *Azure Active Directory*. 

   ![Azure Active Directory navigation](image-url)
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*...

![Request API permissions](image)

...scroll down to *User (1)* section and uncheck the *User.Read* checkbox.
12. Select **Application permissions**.

![Request API permissions](image)

- **Microsoft Graph**
  - https://graph.microsoft.com/   **[docs](https://graph.microsoft.com/)**

**What type of permissions does your application require?**

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

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

Select permissions **[expand all]**

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

![Directory (1)](image)

- **Directory.Read.All**
  - Read directory data
  - Yes

- **Directory.ReadWrite.All**
  - Read and write directory data
  - Yes

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

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

16. Click **Update permissions**.

![Update permissions](image)

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

![Permissions have changed](image)

**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](https://docs.microsoft.com/en-us/graph/permission-settings).

**API / Permissions name**

- **Grant admin consent for San Diego County Superintendent of Schools**

<table>
<thead>
<tr>
<th>API / Permissions name</th>
<th>Type</th>
<th>Description</th>
<th>Admin Consent Required</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="https://graph.microsoft.com/" alt="Microsoft Graph" /></td>
<td>Application</td>
<td>Read directory data</td>
<td>Yes</td>
<td>□ Not granted for San Diego County Superintendent of Schools</td>
</tr>
</tbody>
</table>

18. Azure will ask you to select the admin login account.
19. Then, select **Accept** on this prompt.

![Permission Request](image)

- **Permissions requested**
- **Accept for your organization**

**RedHerring**

**App info**

- This app would like to:
  - Read directory data
  - Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. **Show details**

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

![Microsoft Azure](image)

**Microsoft Azure**

**All services** > **App registrations** > **RedHerring**

- **Display name**: RedHerring
- **Application (client) ID**: ###XXX
- **Directory (tenant) ID**: ###XXX
- **Object ID**: ###XXX

- **Supported account types**: My organization only
- **Redirect URIs**: Add a Redirect URI
- **Application ID URI**: Add an Application ID URI
- **Managed application in**: RedHerring

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

![Azure Groups](image)

**Microsoft Azure**

**All services** > **Groups - All groups**

<table>
<thead>
<tr>
<th>Name</th>
<th>Object Id</th>
<th>Group Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Staff</td>
<td></td>
<td>Office</td>
</tr>
</tbody>
</table>
Sync Target Users
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. Refer to *Send a Phishing Email (Ad Hoc)* on p. Error! Bookmark not defined.. Subsequent syncs will be used to update any new users.

Now go to Red Herring.

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

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

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

25. Perform an initial sync to import your AD users at any time. Refer to *Send a Phishing Email (Ad Hoc)* on p. Error! Bookmark not defined.. Subsequent syncs will be used to update any new users.
Sending a Test Campaign

Create Red Herring User Group
Red Herring has 5 groups that are automatically populated with your target users based on their Risk Score. You may use any or all of these groups in your simulated phishing campaigns. We recommend that you create a group for testing purposes to ensure the templates are formatted correctly and that spam prevention is bypassed.

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

Configure LEA Branded Settings
Once you enter your agency’s details here the information will automatically appear on any of our templates that have the #LEA Branded tag.

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

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

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

Clone a Red Herring User Email Template

1. Navigate to Red Herring
2. Search for Microsoft in the top-right search bar
3. Navigate to Red Herring > Emails > +Shared with Me
4. In the Filters box click Deselect all and then check the box for Email Templates
5. Find a template that you like and clone it to your Testing folder (an example of email to landing page click-path is on next page)
6. Optionally you check the box for Landing Page Templates and clone them so that you may customize them.
   a. You will have to edit the link to the email template if you decide to clone and customize a landing page.
Send a Test Phishing Campaign

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

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

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

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

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

4. Verify telemetry shows in the email campaign report

5. Delete the Email once test is completed

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

7. Contact securinginfo@sdcoe.net if assistance is needed.