STATE & LOCAL CYBERSECURITY GRANT PROGRAM (SLGCP) KNOWBE4 CONFIGURATION GUIDE

Version: 2.0

Publication Date: 07/27/2026

Table of Contents

Introduction

Thank you for participating in security awareness training provided by the State of Maine's State and Local Cybersecurity Grant Program! The goal of this project is to equip interested counties, towns, and K-12 schools across Maine with the knowledge and confidence to help prevent, recognize, and report cybersecurity threats. For this program, the KnowBe4 platform will be used to provide staff with centralized access to security awareness training modules, educational content, and regular security newsletters. To test effectiveness of training content, simulated phishing campaigns will be coordinated.

If you require any support going through this process or have any technical issues, please reach out to securitytraining@nuharborsecurity.com. If you have questions or concerns regarding program eligibility, licenses, or removal from the program, please reach out to SLCyberSecurity.Grant@maine.gov.

This reference guide provides the information needed to configure and maintain your organization's KnowBe4 console. It is intended for the organization's KnowBe4 Console Administrator, who oversees security awareness training, regardless of whether console management tasks are performed internally or with vendor support. This guide lays out the steps necessary to complete the configuration portion of setting up your organization's KnowBe4 console.

Onboarding

Step 1: Completing the Onboarding Form

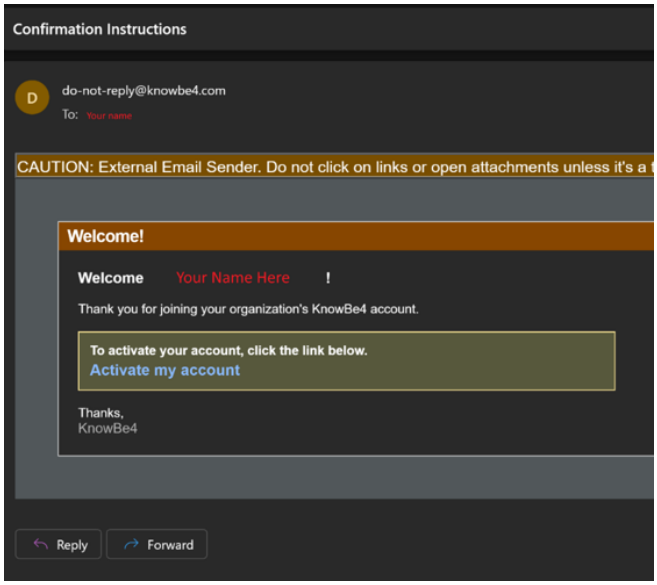
Please Note: You cannot proceed with configuration if you have not completed the Microsoft Onboarding Form distributed at the start of the program. If you have not completed the Microsoft Onboarding Form, please provide your Organization Name when contacting securitytraining@nuharborsecurity.com.

The Onboarding Form collects all necessary information for creating your console (account), setting your security awareness training, and testing preferences. Once you submit your onboarding form, your organization's KnowBe4 console will be created on your behalf. During this time, we may email you if there are any questions. The console creation process can take a maximum of two weeks following onboarding form submission.

Step 2: Signing into Your KnowBe4 Console

Once your console is created, you will receive a confirmation email from do-not-reply@knowbe4.com with your KnowBe4 login link. To ensure you receive this email, save the contact to your address book.

Please see image to the right of what the confirmation email will look like.



Can't find the confirmation email?
Use this link to resend the confirmation. This will lead you to login screen to resend confirmation instructions.

Logging into the console:
You can log in to the KnowBe4 platform through this link. Your username is your organization email address.

Step 3: Uploading Your Users (Staff)

Once you have signed into your KnowBe4 console, you must upload your organization's users into the platform. If you do not upload your users, staff cannot receive any training or phishing testing activities. Please select one of the three methods outlined below based on your organization's environment and level of IT support.

1. **CSV file**

If you are a smaller organization with limited IT support, we recommend you manually import staff using CSV files. Refer to this guide on how to add staff accounts: Import Users with a CSV File – Knowledge Base.

2. **Google Environments**

If you are a larger organization with IT support and use Google Workspace, we recommend you set up Google User Provisioning (GUP) to automatically sync staff accounts with the KnowBe4 platform. Refer to this guide on how to add staff accounts: Google User Provisioning (GUP) Guide | KnowBe4 Knowledge Base.

3. **Microsoft Environments**

If you are a larger organization with IT support and use Microsoft, we recommend you set up Active Directory (AD) to automatically sync staff accounts with the KnowBe4 platform. Refer to this guide on how to add staff accounts: Active Directory Integration (ADI) Configuration Guide – Knowledge Base.

Ongoing Account Maintenance: User Lists

As the administrator for your organization's KnowBe4 training console, you are responsible for maintaining an accurate staff user list within the KnowBe4 platform. If you uploaded your staff via GUP or AD, KnowBe4 will

automatically add or remove users, and would only require periodic verification to ensure no deviations. If you uploaded staff via CSV file, you will be required to manually add and remove staff accounts as needed.

KnowBe4 licenses may be used only by staff within your organization. Use of KnowBe4 Licenses for students or any external individuals (residents, etc.) is prohibited. Your organization is only allowed to use the amount of KnowBe4 Licenses that are allocated to your organization.

Please Note: any additional KnowBe4 Licenses that your organization may require must be requested and approved through proper channels. Please contact SLCyberSecurity.Grant@maine.gov.

Step 4: Allowing KnowBe4 Emails (Whitelisting)

To prepare your organization for simulated phishing campaigns, steps must be taken to allow staff to receive the messages from KnowBe4. This process is called "whitelisting." If this step is not completed correctly, the phishing simulations may be blocked by your email security system, and your organization's staff may not receive them at all.

Please use the table below to determine your setup path based on which email client your organization utilizes.

Your Email Client	If you use a Spam Filter:	If you do not use a Spam Filter
Google Workspace	1.Set up Direct Message Injection to bypass email filtering rules. 2. Reach out to the Service Provider with the name of the Spam filter used. We will provide additional information on configuring the spam filter.	Set up Direct Message Injection only
Microsoft 365	1.Setup Smart Hosts 2.Setup Advanced Delivery Policies (ADP)	Setup Advanced Delivery Policies (ADP)
Microsoft Exchange	1. Whitelist Email Headers 2. Contact the Service Provider with your spam filter name for additional instructions.	Set up whitelisting by IP address

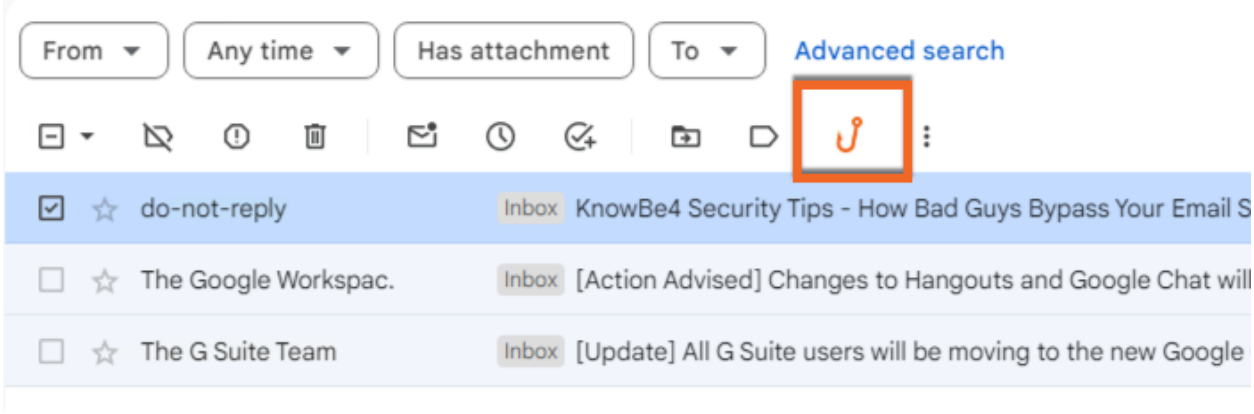
Additional Resource: Whitelisting Guide | KnowBe4 Knowledge Base

Step 5: Enabling the Phish Alert Button

The Phish Alert Button (PAB) allows staff to report suspicious emails directly from their inbox. Enabling the PAB helps track when staff report phishing simulations and reinforce safe reporting behavior. If you do not enable the PAB, your staff will not be able to properly report simulated phishing emails or be enrolled into remedial training or testing activities.

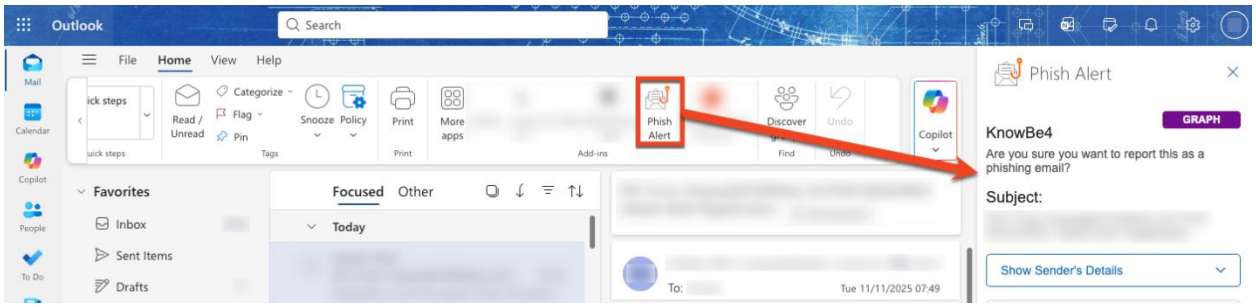
Please select one of the three methods outlined below based on which email client your organization uses.

1. **Google Workspace**
   Gmail Phish Alert Button (PAB) Add-on Product Manual | KnowBe4 Knowledge Base



2. **Outlook Classic**
   Microsoft Outlook (EXE Version) Phish Alert Button (PAB) Product Manual | KnowBe4 Knowledge Base

3. **New Outlook**
   Microsoft Ribbon Phish Alert Button (PAB) Product Manual | KnowBe4 Knowledge Base



Additional Resource: Phish Alert Button (PAB) Compatibility Matrix | KnowBe4 Knowledge Base

Educating Staff on Phish Alert Button

Once the Phish Alert Button is installed, staff will need to be trained on how and when to use it. While practices for educating staff may vary based on your individual organization, here are some recommended steps:

1. Inform staff that the PAB is available and explain when to use it.
2. Enroll staff in a PAB training module.
3. Send a test email so staff can practice reporting.

Additional Resource: Best Practices: Phish Alert Button (PAB) Implementation | KnowBe4 Knowledge Base

Change Control

Version No.	Date	Description of changes	Owner
1.0	06/24/2026	Document Created	nuHarbor
2.0	07/27/20226	Document updated and finalized	nuHarbor