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

Version: 3.0

Publication Date: 08/12/2026

Table of Contents

Introduction

Thank you for participating in the security awareness training program 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 and educational content. Then, 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 the Service Provider, 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 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, to complete the steps below.

Onboarding

Step 1: Completing the Onboarding Form

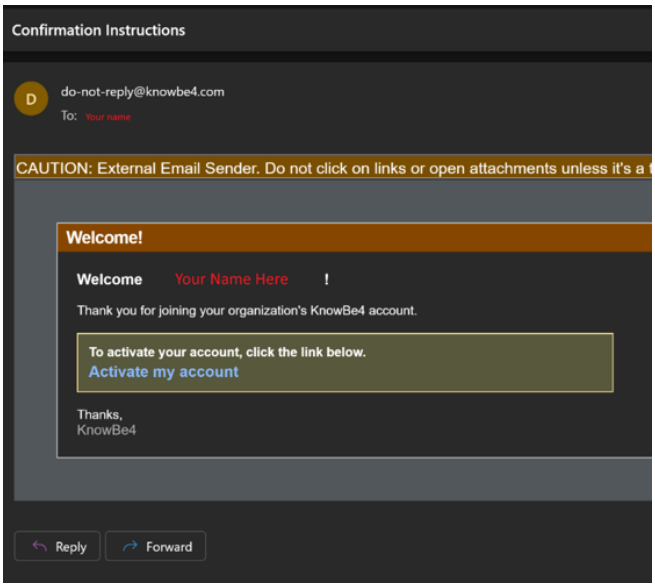
The first step of the process requires you to complete the Onboarding Form. By now, your organization should have received an email from securitytraining@nuharborsecurity.com with the subject "Getting Started with KnowBe4 through SLCGP" Within this email, the Onboarding Form link was provided, with supplemental program guidance.

Please Note: You cannot proceed with configuration until you have completed the Onboarding Form. If you have not completed the Onboarding Form, contact securitytraining@nuharborsecurity.com and please provide your Organization Name.

The Onboarding Form collects all necessary information for creating your console (account), setting up 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

The second step of this process covers signing into your KnowBe4 account. 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 information to your address book.



Please see the 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. Please make sure to enter your work email address.

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

Step 3: Adding Staff to the platform

The next step of onboarding is to add all your staff to the platform. 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 follow 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. This guide outlines how to add staff to your account and where to download one of KnowBe4's sample CSV files: Import Users with a CSV File – Knowledge Base.

Download Our Example CSV Files

If you don't have a CSV file, you can download one of our sample CSV files from your KnowBe4 console. To download one of our CSV files, follow the steps below:

1. Log in to your KnowBe4 console and navigate to **Users** > **Import Users** > **CSV Import**.
2. In the blue box on the right side of the page, select the link for the CSV file that you'd like to use.
3. In the window that opens, select the **Download Example CSV** button.

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

After you initially add accounts to the platform, 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 only requires periodic verification to ensure no deviations. If you upload staff names 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 be unable to receive them.

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. They 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

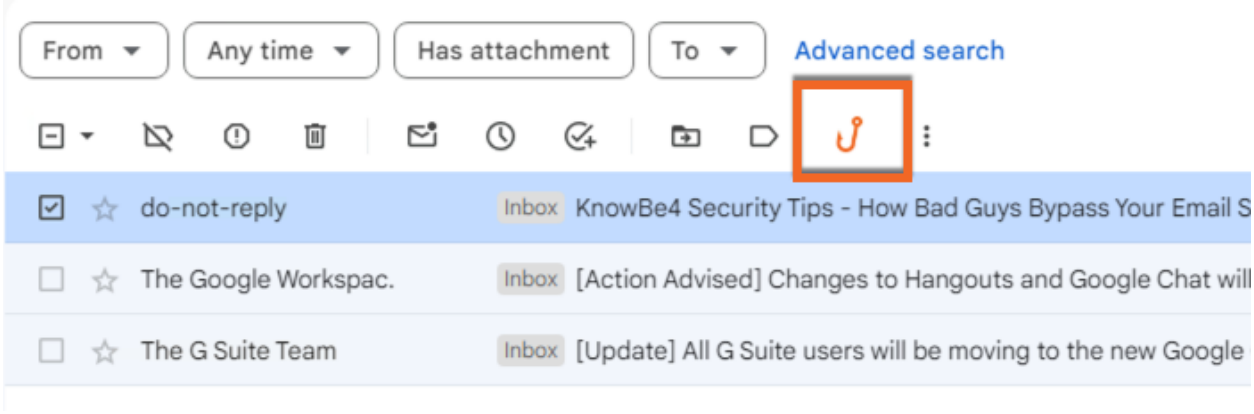
Additional Resource: Whitelisting Guide | KnowBe4 Knowledge Base

Step 5: Enabling the Phish Alert Button

For organizations who will run simulated phishing campaigns, you will need to install the Phish Alert Button (PAB). The 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.

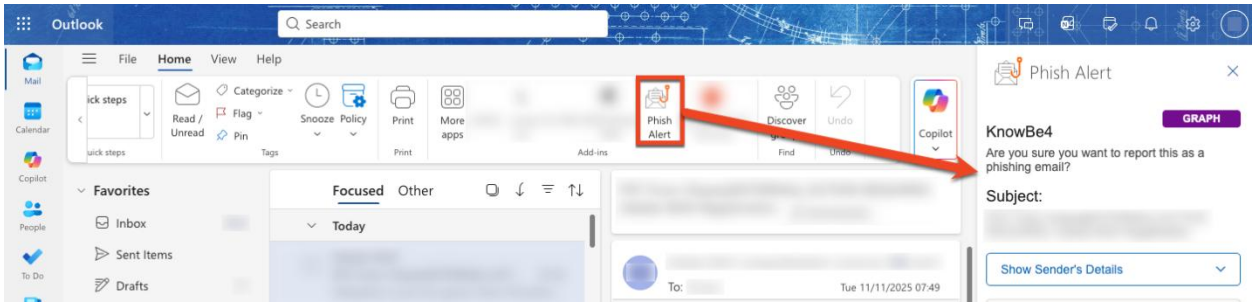
Please follow one of the three methods outlined below based on which email client your organization uses.

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, we recommend notifying and training staff on how to use it. While practices for educating staff may vary based on your individual organization, here are some recommended steps to follow.

1. Inform staff that the PAB has been installed and the tool's purpose.
2. Enroll staff in a PAB training module to teach staff about the feature.
3. Send a test email so staff can practice reporting emails with the PAB.

For detailed guidance on how to approach informing and teaching staff about the PAB, follow this guide.

Resources

Onboarding

KnowBe4 Resend Confirmation Email	This link is used for resending confirmation emails to allow you to log into the KnowBe4 platform.
KnowBe4 login link	This link is used for logging into the KnowB4 platform.

Adding Staff

Import Users with a CSV File – Knowledge Base	This article walks through the steps required for adding staff accounts via (Comma Separated Value (CSV) file upload.
Google User Provisioning (GUP) Guide | KnowBe4 Knowledge Base	This article walks through the steps required for adding staff accounts via Google User Provisioning.
Active Directory Integration (ADI) Configuration Guide – Knowledge Base	This article walks through the steps required for adding staff accounts via Active Directory Integration.

Whitelisting

Whitelisting Guide – KnowBe4 Knowledge Base	This article covers all the steps and best practices to consider when whitelisting KnowBe4 for your organization.
Direct Message Injection (DMI) Configuration Guide – KnowBe4 Knowledge Base	This article walks though how to configure Direct Message Injection (DMI) for Google Workspace environments.

Smart Hosting Guide – KnowBe4 Knowledge Base	This article covers how to configure smart hosting for Microsoft 365 environments to allow delivery of KnowBe4 emails.
Advanced Delivery Policies in Microsoft Defender – KnowBe4 Knowledge Base	This article covers how to configure advanced delivery policy in Microsoft Defender to allow delivery of KnowBe4 emails.
Whitelist by Email Headers in Microsoft 365 and Exchange SE – KnowBe4 Knowledge Base	This article covers how to configure whitelisting via email headers for Microsoft 365 environments to allow delivery of KnowBe4 emails.
Whitelist by IP Address in Exchange SE – KnowBe4 Knowledge Base	This article covers how to configure IP whitelisting in Microsoft Exchange to allow delivery of KnowBe4 emails.

Phishing and Phish Alert Button (PAB)

Phishing Campaigns Overview – KnowBe4 Knowledge Base	This article provides an overview of what phishing campaigns are.
Phish Alert Button (PAB) Compatibility Matrix – KnowBe4 Knowledge Base	This article provides a matrix on which version PAB is compatible for which email clients.
Best Practices: Phish Alert Button (PAB) Implementation – KnowBe4 Knowledge Base	This article covers best practices on how to integrate the PAB within your environment
Gmail Phish Alert Button (PAB) Add-on Product Manual – KnowBe4 Knowledge Base	This article walks through how to install the PAB within Gmail.
Microsoft Outlook (EXE Version) Phish Alert Button (PAB) Product Manual – KnowBe4 Knowledge Base	This article walks through how to install the PAB within Outlook **Classic**.
Microsoft Ribbon Phish Alert Button (PAB) Product Manual – KnowBe4 Knowledge Base	This article walks through how to install the PAB within **New** Outlook.

Change Control

Version No.	Date	Description of changes	Owner
1.0	06/24/2026	Document Created	nuHarbor
2.0	07/27/2026	Document updated and finalized	nuHarbor
3.0	08/12/2026	Resources section added	nuHarbor