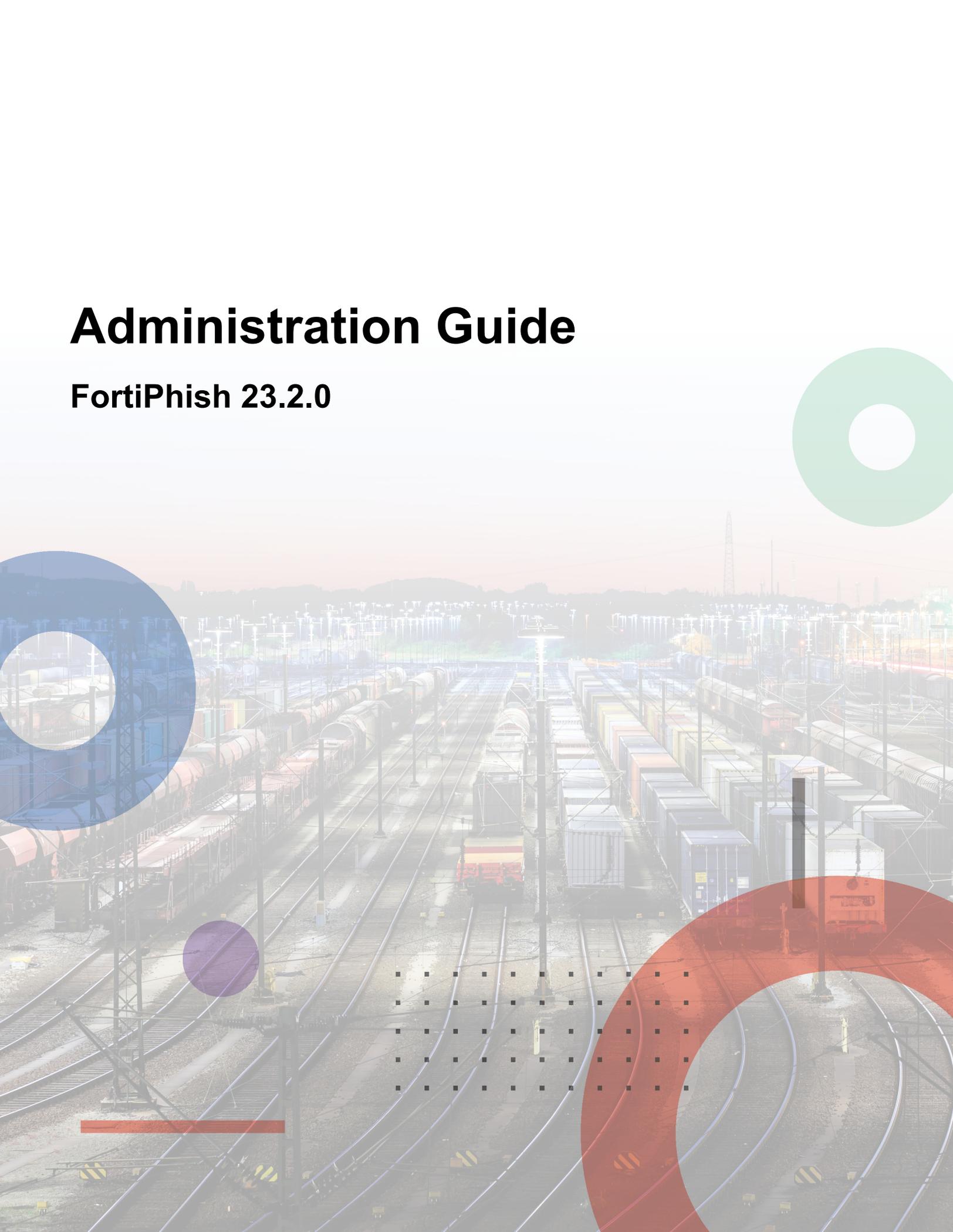


# Administration Guide

FortiPhish 23.2.0



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)

June 12, 2023

FortiPhish 23.2.0 Administration Guide

60-232-920288-20230612

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
What's new in FortiPhish 23.2.0 .....	6
<b>FortiPhish portal</b> .....	<b>7</b>
Accessing the FortiPhish portal .....	7
Notifications .....	8
User Management .....	8
IAM User Roles .....	8
API User Roles .....	8
<b>Getting started</b> .....	<b>10</b>
<b>Dashboard</b> .....	<b>11</b>
<b>Monitoring</b> .....	<b>13</b>
Campaign Analysis .....	13
Overall Responses .....	14
Group Analysis .....	15
User Profile .....	16
Campaigns List .....	16
Executive Report .....	17
<b>Recipients</b> .....	<b>21</b>
Group List .....	21
LDAP server .....	28
Azure AD Server .....	29
Configuring Azure AD for FortiPhish .....	30
Adding an Azure AD server .....	30
Syncing the Azure AD server .....	31
Deleting an Azure AD server .....	32
Risk Grade History .....	33
<b>Domains</b> .....	<b>34</b>
Adding domains .....	34
<b>Campaigns</b> .....	<b>38</b>
Subscription Limit .....	38
Global templates .....	38
Custom campaigns .....	39
Creating campaigns .....	39
Template variables .....	42
Viewing campaign statistics .....	44
Campaign Summary .....	44
Campaign Timeline .....	45
Campaign Preview .....	45
User Pass Rate .....	46
Campaign Status .....	46
Campaign Stats .....	47

---

Campaign Training Stats .....	47
User Profile .....	48
Recipient Stats .....	49
Usergroup Stats .....	50
Retrying a campaign .....	50
Completing a campaign .....	51
Exporting campaign statistics .....	53
Deleting archived campaigns .....	54
<b>Custom .....</b>	<b>55</b>
Templates .....	55
Creating custom templates .....	56
Landing page .....	57
Creating custom landing pages with the editor .....	58
Creating a custom landing page with a Zip file .....	59
Landing page variables .....	60
<b>Settings .....</b>	<b>61</b>
Enable Auto Delete .....	61
FortiPhish alert buttons .....	61
Creating a FortiPhish alert button .....	62
Adding alert buttons in Outlook .....	64
Adding alert buttons in Thunderbird .....	68
FortiPhish alert button compatibility matrix .....	71
SMTP .....	72

# Change Log

Date	Change Description
2023-06-12	Initial release.

# Introduction

FortiPhish is a phishing simulation service to analyze how internal users interact with phishing emails. Use FortiPhish to create custom phishing email campaigns and monitor how users respond to them. The FortiPhish portal contains dashboards with easy-to-read data analysis monitors to view responses across campaigns, and monitor improvements over time.

## What's new in FortiPhish 23.2.0

### Azure AD

- Connect FortiPhish to your organization's Azure AD tenant to import users and groups to create new recipients. For information, see [Azure AD Server](#).

### Group List

- You can hide, unhide, and filter group list. For information, see [Group List](#).

# FortiPhish portal

Use the FortiPhish portal to generate DNS tokens, create users and groups, and launch and monitor email campaigns.

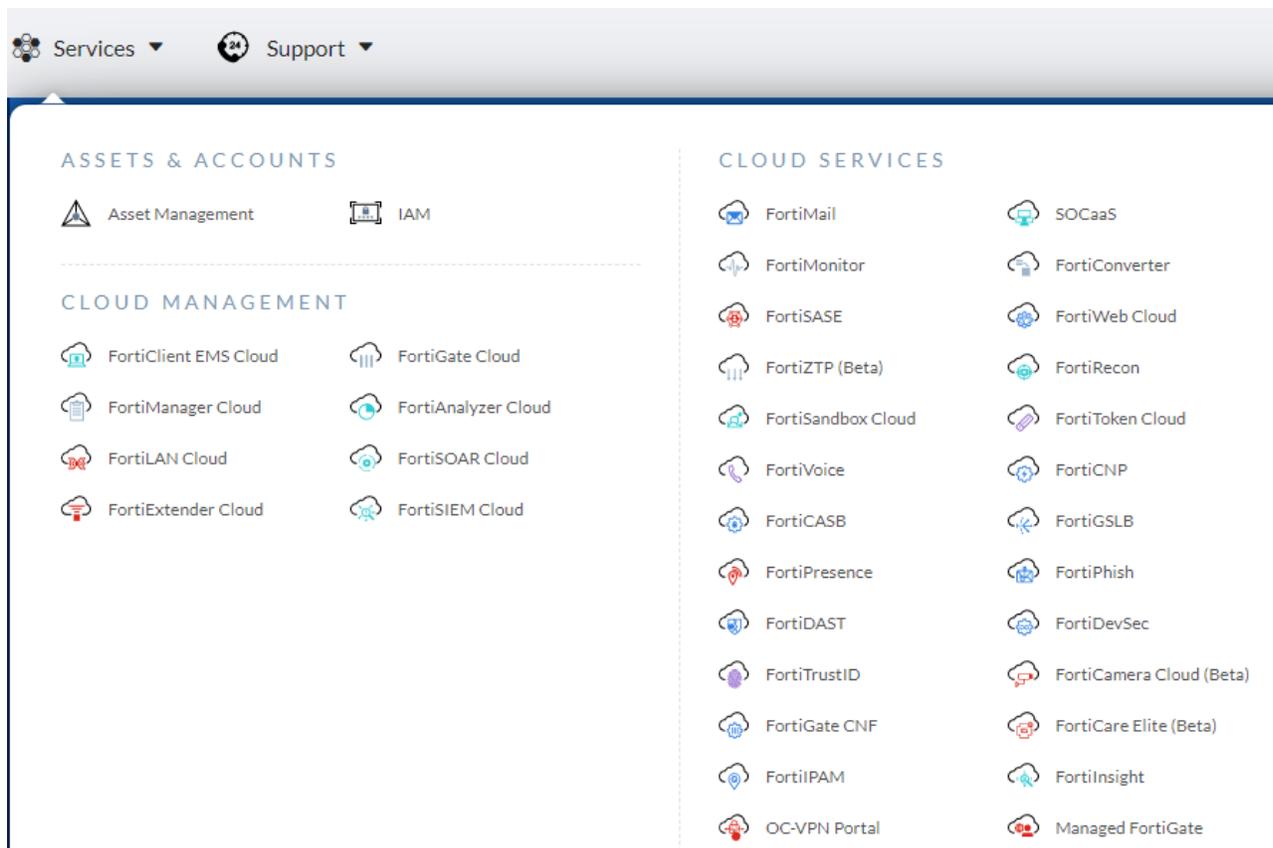


For an optimal user experience, use a desktop computer to view the FortiPhish portal.

## Accessing the FortiPhish portal

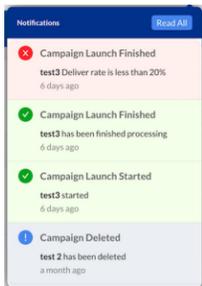
To access the FortiPhish portal:

1. Log in to [FortiCloud](#).
2. Go to *Services > Cloud Services* and click *FortiPhish*.



## Notifications

The *Notifications* icon  in the banner alerts you when there is activity in your account. The message background color indicates the importance of the message. The background color changes to gray when a message is viewed or acknowledged. Scroll down to view the notification history. Click *Read All* to acknowledge all the messages.



## User Management

The FortiPhish portal supports both the Sub User and IAM User management models. For more information, see [Identity & Access Management \(IAM\) > User management models](#).

### IAM User Roles

Identity & Access Management (IAM) User roles can create and manage campaigns depending on their permissions. For information about creating IAM users, go to [Identity & Access Management \(IAM\) > Adding IAM users](#).

IAM User Role	Permissions
<b>Admin</b>	Read/Write access to all user records under the same account, excluding domain records.
<b>Read/Write</b>	Read /Write access to user's own records.
<b>Read Only</b>	Read access to master user records under the same account, excluding Domain records.

### API User Roles

API User roles can access the FortiPhish portal via API requests. API users can view records as a Master user or IAM user with admin privileges.

#### To access the FortiPhish portal as an API user:

1. Create the API user role in the IAM portal. For more information, go to [Identity & Access Management \(IAM\) > Adding an API user](#).

2. Obtain an Access Token. For more information, go to [Identity & Access Management \(IAM\) > Accessing FortiAPIs > Authorization](#).
3. Use the Access Token to make API requests to FortiPhish portal.

# Getting started

Before launching a campaign, ensure FortiPhish's mailer server address is added to your email server's safelist. To launch a new campaign, create a DNS token in FortiPhish, and then add it to the DNS settings of your domain. After your domain is configured, use FortiPhish to verify the authorization is valid. Create a user group in FortiPhish, and then select a campaign template to send to users.

## To configure FortiPhish and deploy a campaign:

1. [Verify you own the domain.](#)
2. Configure the application settings:
  - [Create a schedule to automatically delete archived campaigns.](#)
  - [Create phishing alert buttons.](#)
  - [Connect FortiPhish to a SMTP server.](#)
3. Create group lists and add servers to distribute campaign emails:
  - [Create a group list.](#)
  - [Add an LDAP server.](#)
  - [Add an Azure AD server.](#)
4. (Optional) Configure custom campaigns:
  - [Create custom landing page.](#)
  - [Create a custom template.](#)
5. [Create and launch the campaign.](#)
6. [Monitor campaign statistics.](#)

To send phishing simulation emails, you must disable the DMARC/DKIM policy, as it will cause an error while attempting to send them. Alternatively, you can make slight modifications to the domain name, such as changing a letter, for example, use *apple.con* or *amazon.com* instead of *apple.com* or *amazon.com*, to send the mails. Another option is to bypass this restriction by using a custom SMTP server.

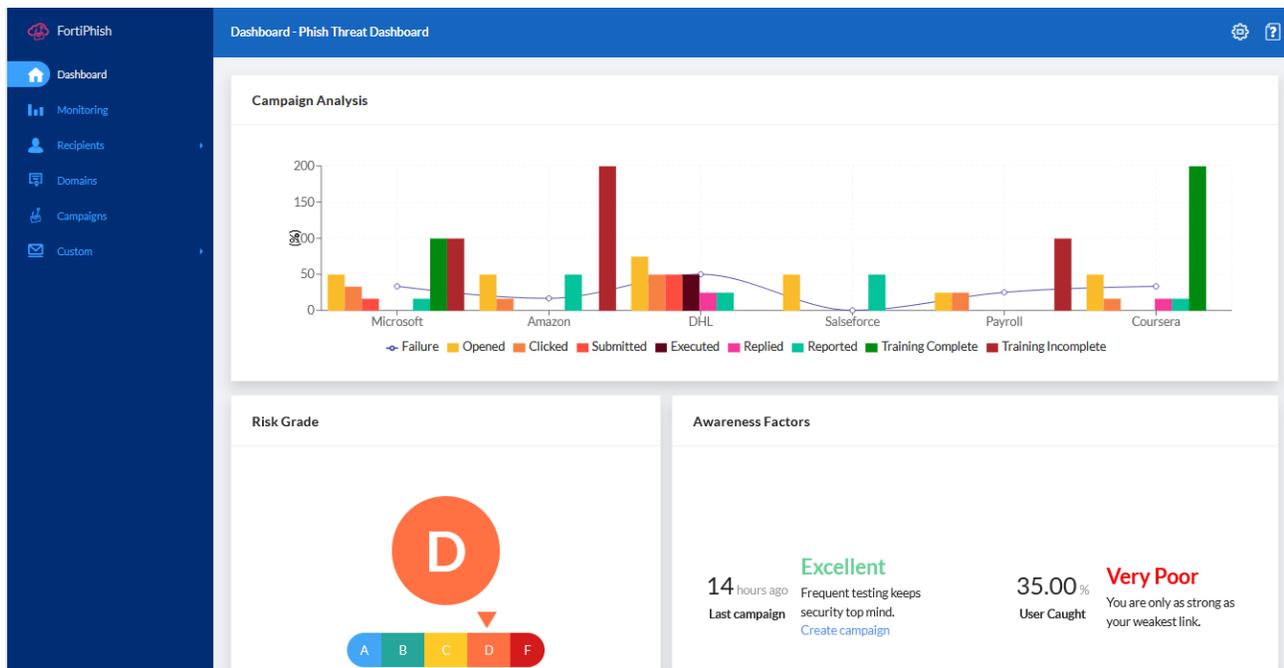


### The test email has the following error :

```
⊗ send failed: closing SMTP DATA writer: 550 5.7.509 Access denied, sending domain [ID.APPLE.COM] does not pass DMARC verification and has a DMARC policy of reject.
[DM4PR11MB6310.namprd11.prod.outlook.com 2023-06-01T07:39:47.549Z 08DB609614E1133F]
[DB9PR06CA0023.eurprd06.prod.outlook.com 2023-06-01T07:39:47.595Z 08DB621DAFFEA003]
[DB8EURO6FT006.eop-eur06.prod.protection.outlook.com 2023-06-01T07:39:47.599Z 08DB61B244003239]
```

# Dashboard

The *Dashboard* provides an overview of responses across campaigns, as well as scores for risk and awareness factors.



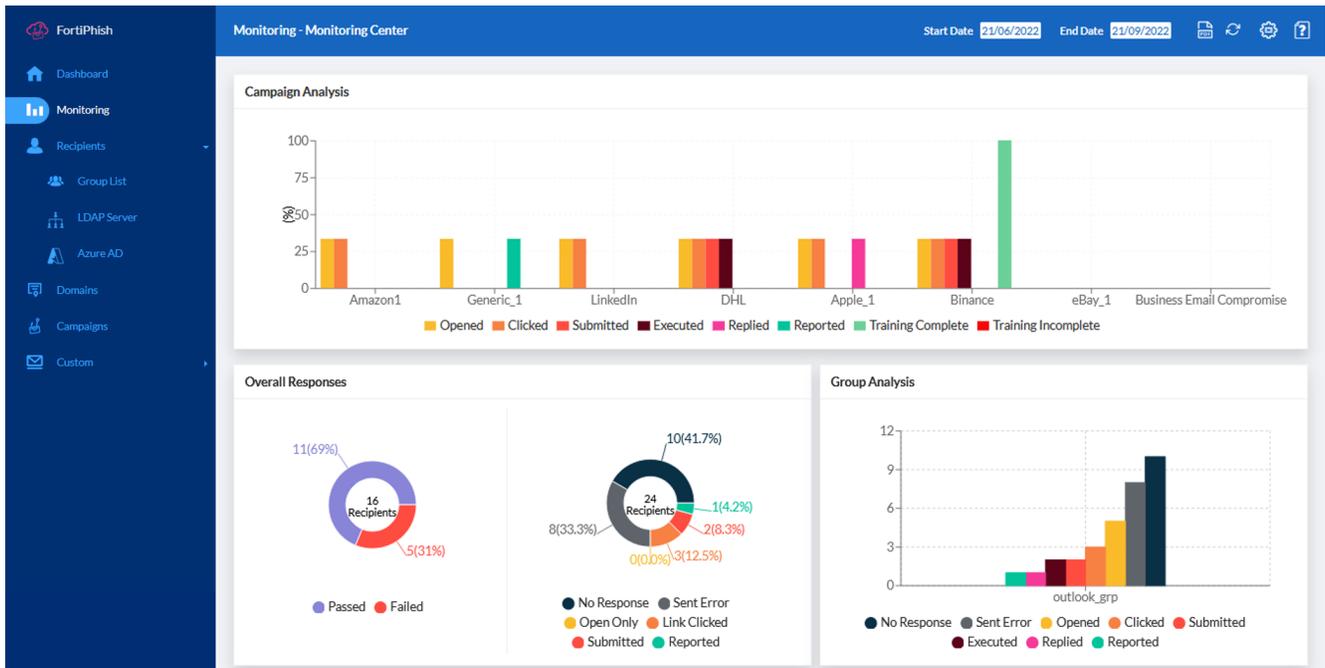
The *Dashboard* displays the following monitors:

Monitor	Description												
<b>Campaign Analysis</b>	Displays the campaign statistics over time. The bar chart shows the following information: <table border="1"> <tr> <td><b>Total</b></td> <td>Total number of recipients in the campaign.</td> </tr> <tr> <td><b>Risk Grade</b></td> <td>The Risk Grade of the campaign. Value is <i>NA</i> if the campaign is in the processing state.</td> </tr> <tr> <td><b>Opened</b></td> <td>The number of recipients who opened the email.</td> </tr> <tr> <td><b>Clicked</b></td> <td>The number of recipients who clicked the redirect link.</td> </tr> <tr> <td><b>Submitted</b></td> <td>The number of recipients who entered information on the landing page.</td> </tr> <tr> <td><b>Executed</b></td> <td>The number of recipients who opened or executed the file attached in the phishing email.</td> </tr> </table>	<b>Total</b>	Total number of recipients in the campaign.	<b>Risk Grade</b>	The Risk Grade of the campaign. Value is <i>NA</i> if the campaign is in the processing state.	<b>Opened</b>	The number of recipients who opened the email.	<b>Clicked</b>	The number of recipients who clicked the redirect link.	<b>Submitted</b>	The number of recipients who entered information on the landing page.	<b>Executed</b>	The number of recipients who opened or executed the file attached in the phishing email.
<b>Total</b>	Total number of recipients in the campaign.												
<b>Risk Grade</b>	The Risk Grade of the campaign. Value is <i>NA</i> if the campaign is in the processing state.												
<b>Opened</b>	The number of recipients who opened the email.												
<b>Clicked</b>	The number of recipients who clicked the redirect link.												
<b>Submitted</b>	The number of recipients who entered information on the landing page.												
<b>Executed</b>	The number of recipients who opened or executed the file attached in the phishing email.												

Monitor	Description
	<div data-bbox="857 289 943 401" style="text-align: center;">  </div> <p data-bbox="963 285 1409 415">FortiPhish will not be able to collect the <i>Executed</i> metric when the attached PDF is previewed in a reader that disables links for security purposes.</p> <hr/> <p data-bbox="573 457 1393 485"><b>Replied</b> The number of recipients who replied to the email.</p> <p data-bbox="573 510 1409 569"><b>Reported</b> The number of recipients who reported the phishing email as suspicious.</p> <p data-bbox="573 594 1425 653"><b>Training Complete</b> The number of recipients who have finished the training.</p> <p data-bbox="573 678 1430 737"><b>Training Incomplete</b> The number of recipients who have been enrolled but did not finish the training.</p>
<b>Risk Grade</b>	<p data-bbox="561 772 1453 869">The letter grade between <i>A</i> and <i>F</i> assigned to the recipient . An <i>A</i> indicates the user poses minimal risk and a <i>F</i> grade indicates the user poses the maximum risk to the organization.</p> <p data-bbox="561 884 1422 942">If the campaign is active, then the Risk Grade will be <i>NA</i> on the <i>Dashboard</i> and <i>Monitoring</i> pages.</p>
<b>Awareness Factors</b>	<p data-bbox="561 972 1433 1094">Displays the launch date of the last campaign, the campaign frequency assessment, and the percentage of users caught. The monitor also includes an awareness grade. To launch a new campaign, click the <i>Create a Campaign</i> link. See <a href="#">Creating campaigns on page 39</a>.</p>

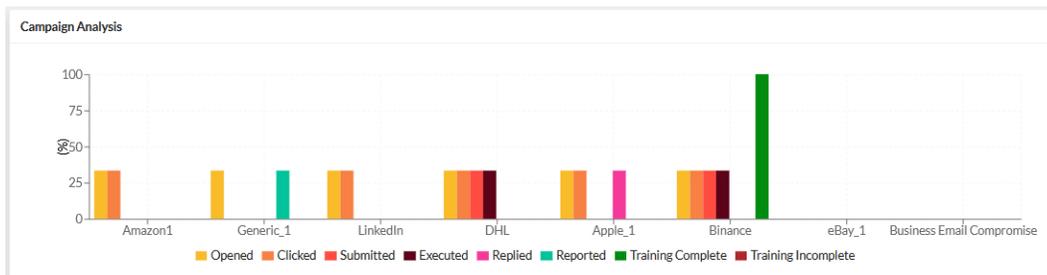
# Monitoring

The *Monitoring* page provides an overview of campaign activity. Use this page to view click-rates, user group analysis, user profiles, and campaign response comparison charts.

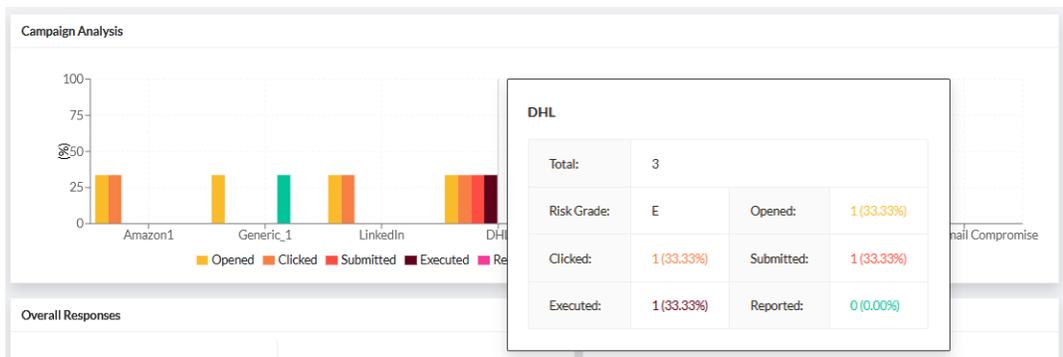


## Campaign Analysis

The *Campaign Analysis* monitor displays click-rate information across all of your campaigns as a bar chart.



Hover a campaign in the chart to view how recipients interacted with the email for that campaign.

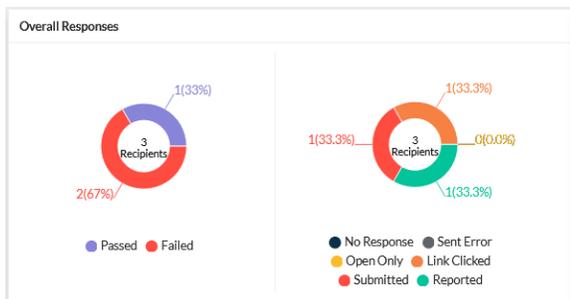


The chart displays the following information:

<b>Risk Grade</b>	The letter grade between <i>A</i> and <i>F</i> assigned to the recipient . An <i>A</i> indicates the user poses minimal risk and a <i>F</i> grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be <i>NA</i> on the <i>Dashboard</i> and <i>Monitoring</i> pages.
<b>Opened</b>	The number of recipients who opened the email.
<b>Clicked</b>	The number of recipients who clicked the redirect link.
<b>Submitted</b>	The number of recipients who entered information on the landing page.
<b>Executed</b>	The number of recipients who opened or executed the file attached in the phishing email.
 FortiPhish will not be able to collect the <i>Executed</i> metric when the attached PDF is previewed in a reader that disables links for security purposes.	
<b>Replied</b>	The number of recipients who replied to the email.
<b>Reported</b>	The number of recipients reported the email as suspicious.
<b>Training Complete</b>	The number of recipients who have finished the training.
<b>Training Incomplete</b>	The number of recipients who have been enrolled but did not finish the training.

## Overall Responses

The *Overall Responses* monitor displays the ratio of recipients who passed or failed your organization's security training. The monitor also includes detailed information about the email distribution and click-rate across all campaigns. Hover over a piece of the chart to view the total number of emails for the category.

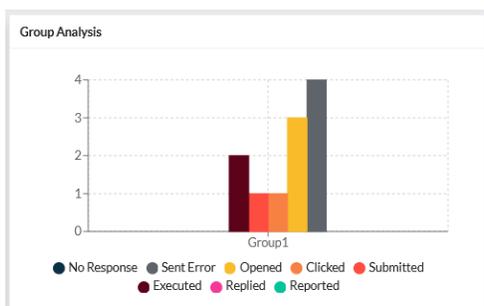


The *Overall Responses* monitor displays the following information:

<b>Passed</b>	The percentage of recipients that did not click or respond to campaign emails. This includes emails that were opened or opened and reported.
<b>Failed</b>	The percentage of recipients that clicked or responded to campaign emails.
<b>No Response</b>	The number of emails that were not opened.
<b>Sent Error</b>	The number of emails that bounced.
<b>Open Only</b>	The number of emails that were opened but not clicked.
<b>Link Clicked</b>	The number of recipients who clicked the redirect link.
<b>Submitted</b>	The number of recipients who entered information on the landing page.
<b>Reported</b>	The number of recipients who reported the phishing email as suspicious.

## Group Analysis

The *Group Analysis* monitor displays the response rates for user groups as a chart. To view the response statistics for a group, hover over the group name in the chart.



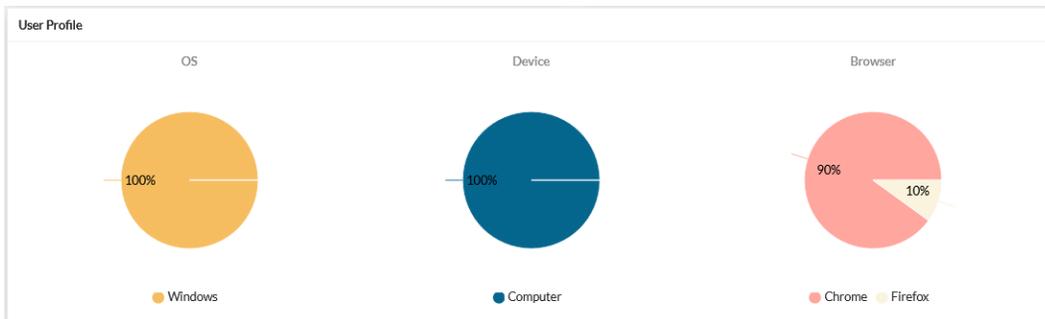
The *Group Analysis* monitor displays the following information:

<b>No Response</b>	The number of emails that were not opened.
<b>Sent Error</b>	The number of emails that bounced.
<b>Opened</b>	The number of recipients who opened the email.

<b>Clicked</b>	The number of recipients who clicked the redirect link.
<b>Submitted</b>	The number of recipients who entered information on the landing page.
<b>Executed</b>	The number of recipients who opened or executed the file attached in the phishing email.
 <p>FortiPhish will not be able to collect the <i>Executed</i> metric when the attached PDF is previewed in a reader that disables links for security purposes.</p>	
<b>Replied</b>	The number of recipients who replied to the email.
<b>Reported</b>	The number of recipients who reported the phishing email as suspicious.

## User Profile

The *User Profile* monitor displays information about the device the recipient used to view the email. Hover over the cart to see the value for each category.



The *User Profile* monitor displays the following information:

<b>OS</b>	The operating system of the device.
<b>Device</b>	The device hardware.
<b>Browser</b>	The browser the recipient used to view the email.

## Campaigns List

The *Campaigns List* monitor displays a list of active and archived campaigns as well as distribution and click-rate statistics for each campaign.

Campaigns List			
<b>DHL</b>	Total: 2	Sent: 1	Risk Grade: A
Launched: 08/03/2023 1:54 AM	Opened: 1	Clicked: 0	Submitted: 0
no. of Usergroups: 1	Executed: 0	Reported: 1	Replied: 0
	Training Complete: 0	Training Incomplete: 0	

The *Campaigns List* monitor displays the following information:

<b>Total</b>	The total number of emails sent to recipients.
<b>Sent</b>	The number of emails sent to the user group.
<b>Risk Grade</b>	The letter grade between <i>A</i> and <i>F</i> assigned to the recipient . An <i>A</i> indicates the user poses minimal risk and a <i>F</i> grade indicates the user poses the maximum risk to the organization. If the campaign is active, then the Risk Grade will be <i>NA</i> on the <i>Dashboard</i> and <i>Monitoring</i> pages.
<b>Opened</b>	The number of recipients who opened the email.
<b>Clicked</b>	The number of recipients who clicked the redirect link.
<b>Submitted</b>	The number of recipients who entered information on the landing page.
 <p>FortiPhish does not save the data entered by the user in the landing page.</p>	
<b>Executed</b>	The number of recipients who opened or executed the file attached in the phishing email.
<b>Reported</b>	The number of recipients who reported the phishing email as suspicious.
<b>Replied</b>	The number of recipients who replied to the email.
<b>Training Complete</b>	The number of recipients who have finished the training.
<b>Training Incomplete</b>	The number of recipients who have been enrolled but did not finish the training.

## Executive Report

The *Executive Report* provides a high level analysis of how your security awareness training is doing across your organization. The report pulls data from the *Dashboard* and *Monitoring* pages, as well as results from multiple campaigns, then exports the data as a PDF.

### To export the Executive Report:

1. Go to *Monitoring* and click the PDF button  in the toolbar.



2. Select the *Start Date* and *End Date*, and click *Export*.

The *Executive Report* contains the following information:

## Account Information

Name	Description	Example
<b>Account Company</b>	Name of the company.	Fortinet Singapore
<b>Account Email</b>	Email of the account owner.	fortiphish@fortinet.com
<b>Date Range</b>	<i>Start Date</i> and <i>End Date</i> in DD-MM-YYYY format.	12-08-2021 - 12-11-2021
<b>Date of Report</b>	Date of the report with Location.	Fri, 12 Nov 2021 04:45:38 am +0800

## Overview

Name	Description	Example
<b>Date of First Campaign</b>	Date of first campaign with Location.	15/06/2022 04:07 AM
<b>Date of Last Campaign</b>	Date of last campaign with Location.	15/06/2022 04:38 AM
<b># of Campaigns</b>	The total number of campaigns.	5
<b># of Total Recipients targeted for Phishing</b>	The number of unique email addresses (recipients or targets) that were sent during the provided period.	10
<b># of Emails (phishing attempts) sent overall:</b>	The number of emails that were successfully sent during the provided period. This value excludes emails marked <i>Sent Error</i> .	30
<b>Most successful phishing campaign</b>	The name of the campaign with the highest phishing rate.	Name of the Campaign
<b>Most successful phishing template</b>	The name of the template for the most successful campaign.	Name of the Template
<b>Risk Grade</b>	The letter grade between <i>A</i> and <i>F</i> assigned to the recipient . An <i>A</i> indicates the user poses minimal risk and a <i>F</i> grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be <i>NA</i> on the <i>Dashboard</i> and <i>Monitoring</i> pages.	A

## Target User Measurements

### Recipient Analysis

Name	Description	Example
<b>Total Recipients targeted for phishing</b>	The number of unique emails (recipients or targets) that were sent during the provided period. This number should be the same as the # of <i>Total recipients</i> in the <i>Overall</i> section.	5 Recipients
<b># of passed recipients overall</b>	The number of <i>Passed</i> recipients divided by the number of <i>Sent</i> emails. This value excludes emails marked <i>Sent Error</i> , <i>Clicked</i> or <i>Submitted</i> .	2 Recipients(40%)
<b># of failed recipients overall</b>	The number of <i>Failed</i> emails divided by the number of <i>Sent</i> emails.	2 Recipients(40%)

### Email Analysis

Name	Description	Example
<b># of emails (phishing attempts) sent overall</b>	The number of <i>Passed</i> recipients divided by the number of emails <i>Sent</i> .	2 Emails (50.0%)
<b># of emails passed overall</b>	The number of <i>Passed</i> recipients divided by the number of emails <i>Sent</i> .	
<b># of emails failed overall</b>	The number of <i>Failed</i> emails divided by the number of emails <i>Sent</i> .	2 Emails (50.0%)
<b># of emails "Open Only"</b>	The number of emails <i>Opened</i> divided by the number of emails <i>Sent</i> .	2 Emails (50.0%)
<b># of emails "Link Clicked"</b>	The number of emails <i>Clicked</i> divided by the number of emails <i>Sent</i> .	2 Emails (50.0%)
<b># of emails "Submitted"</b>	The number of emails <i>Submitted</i> divided by the number of emails <i>Sent</i> .	2 Emails (50.0%)
<b># of emails "Reported"</b>	The number of emails <i>Reported</i> divided by the number of emails <i>Sent</i> .	2 Emails (50.0%)
<b># of recipients training "Completed"</b>	The number of recipients who completed the phishing training.	3
<b># of recipients training "Incomplete"</b>	The number of recipients who did not complete the phishing training.	1
<b># total training "Completed"</b>	The total number of trainings completed within the organization, including repeat trainings.	5

## Overall Phish Percentage by Campaign

Name	Description	Example
<b>Campaign</b>	Name of the campaign.	
<b>Start Date</b>	Start Date.	
<b>Failed Rate</b>	<i>Failed Rate</i> with the difference between previous campaign.	100.0% (50%)
<b>Reported Rate</b>	<i>Reported Rate</i> with the difference between previous campaign.	0.0% (-50%)
<b>Risk Grade</b>	The letter grade between <i>A</i> and <i>F</i> assigned to the recipient . An <i>A</i> indicates the user poses minimal risk and a <i>F</i> grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be <i>NA</i> on the <i>Dashboard</i> and <i>Monitoring</i> pages.	A

## Overall Phish Percentage by Usergroup

Name	Description	Example
<b>Name</b>	Name of the user group.	
<b>Failed Rate</b>	<i>Failed Rate</i> with the difference between previous campaign.	100.0% (50%)
<b>Reported Rate</b>	<i>Reported Rate</i> with the difference between previous campaign.	0.0% (-50%)
<b>Score</b>	The <i>Reported Rate</i> minus the <i>Failed Rate</i> .	
<b>Risk Grade</b>	The letter grade between <i>A</i> and <i>F</i> assigned to the recipient . An <i>A</i> indicates the user poses minimal risk and a <i>F</i> grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be <i>NA</i> on the <i>Dashboard</i> and <i>Monitoring</i> pages.	A

# Recipients

Use the *Recipients* page to create group lists to distribute your campaigns. You can add recipients to a group one at a time or with a bulk user import. You also have the option of importing users from an LDAP server.

Name	Risk Grade	# Of Members	Created	Application	Modified Date
outlook_grp	D	11	Manually	NA	06/06/2023 7:59 AM
Dev	B	3	Azure AD Sync	Phish_AD	06/06/2023 7:24 AM

## Group List

*Group Lists* are distribution lists for your campaigns. A Group List is required even if you are sending an email to only one user. Group Lists allow you to compare responses across segments within your organization. Users can be added to a group one at a time, or using the CSV template to perform a bulk user import. Each user in the group must have a unique email address.

Use the *Group List* page to:

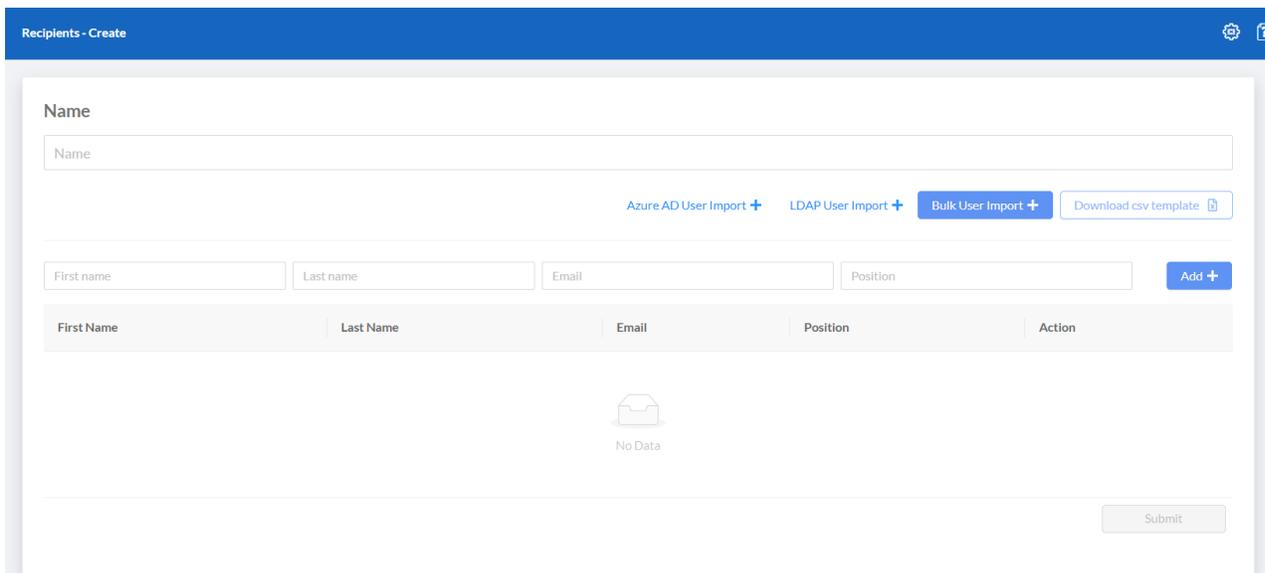
- [Create a group list](#)
- [Perform a bulk user import](#)
- [Import an LDAP user group](#)
- [Import an Azure AD user group](#)
- [Update user details](#)
- [Filtering group list](#)
- [Hide/Unhide a group](#)
- [Deleting a group](#)

### To create a group list:

1. Go to *Recipients* and click *Add Group*. The *Recipients- Create* page opens.

Name	Risk Grade	# Of Members	Created	Application	Modified Date
outlook_grp	D	11	Manually	NA	06/06/2023 7:59 AM
Dev	B	3	Azure AD Sync	Phish_AD	06/06/2023 7:24 AM

2. In the *Group name* field, enter a name for the group.



3. Enter the user's *First name*, *Last name*, *Email*, and *Position*.
4. Click *Add*. The user is added to the group. A warning appears if there is a duplicate email.
5. (Optional) Click the trash button to remove a user.
6. Click *Submit*, and then click *OK*. The group is added to the *Users & Groups* page.

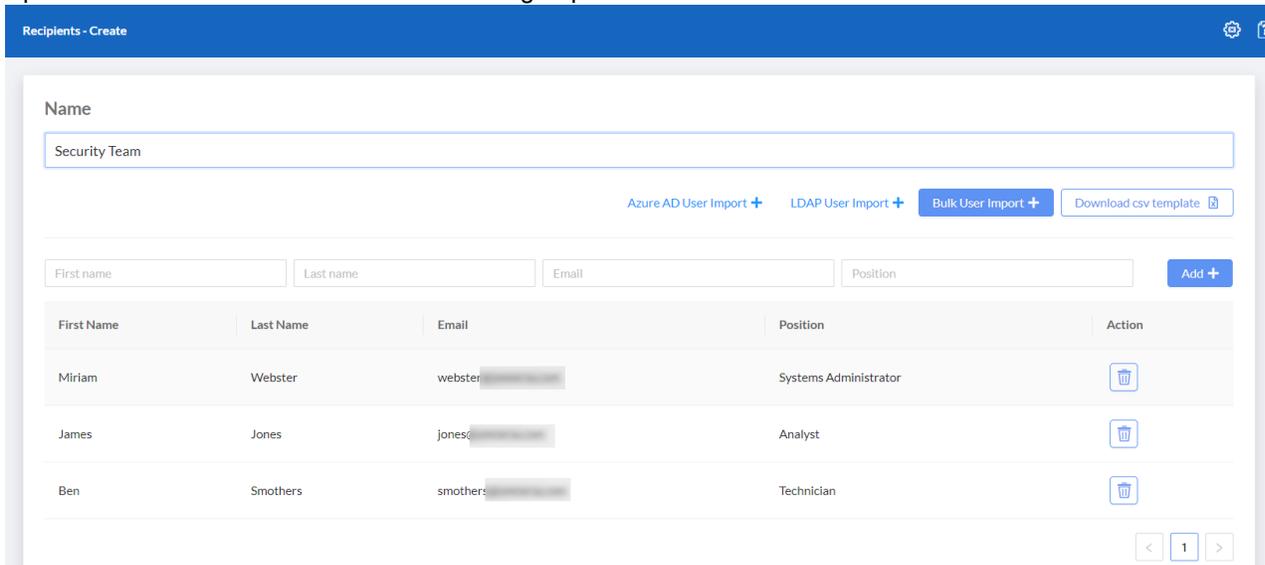
**To perform a bulk user import:**

1. Click *Add Group*.
2. Click *download csv template*. The user group template is downloaded to your computer.



1. Enter the user's *First name*, *Last name*, *Email*, and *Position* in the template, and save the file.
2. In the *Recipients- Create* page, click *Bulk User Import*. The *Upload csv* dialog opens.

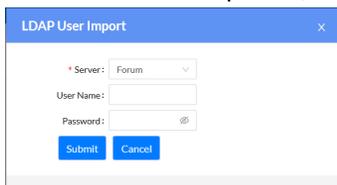
- 3. Upload the csv file. The users are added to the group.



- 4. In the *Group name* field, enter the name of the group.
- 5. Click *Submit*.

**To import an LDAP user group:**

- 1. Configure the LDAP server. See [LDAP server on page 28](#)
- 2. Go to *Recipients > Group List*.
- 3. Click *Add Group*. The *Recipients- Create* page opens.
- 4. Click *LDAP User Import*. The *LDAP User Import* dialog opens.
- 5. From the *Server* dropdown, select a server, and then enter the *User Name* and *Password*.



6. Select the users you want to import and click *Submit*. The LDAP users are added to the group.

### LDAP User Import

<input type="checkbox"/>	First Name	Last Name	Email	Position
<input type="checkbox"/>	Anderson	Webster	awebster@domain.com	
<input type="checkbox"/>	Williams	Brown	wbrown@domain.com	
<input type="checkbox"/>	Jones	Jhonson	jjhonson@domain.com	

7. In the *Group name* field, enter the name of the group.
8. Click *Submit*.

#### To import an Azure AD user group:

1. Configure the Azure AD server. See [Azure AD Server on page 29](#)
2. Go to *Recipients > Group List*.
3. Click *Add Group*.
4. Click *Azure AD User Import*. The *Azure AD User Import* dialog opens.
5. From the *Application* dropdown list, select an application and click *Submit*.
  - If the sync complete, a list of users is displayed.
  - If the sync is in progress, a progress window displays the number of users fetched.
  - An error message is displayed if the sync failed.

Azure AD Import
✕

\* Application: FortiPhish\_AD ▼

Last Synced At : 6/6/2023, 7:25:24 AM

6. Select the users you want to import and click *Import selected*, or click *Import all* to import all users.

<input type="checkbox"/>	First Name	Last Name	Email	Position
<input type="checkbox"/>	Anderson	Webster	awebster@xxxxxxxxxx.com	Analyst
<input type="checkbox"/>	Jones	Jhonson	jjhonson@xxxxxxxxxx.com	Manager

7. In the *Group name* field, enter the name of the group and click *Submit*.

**To update a user's details:**

1. Go to *Recipients > Group List*, and select a group in the list.
2. Click the Edit button next to the username.

[Azure AD User Import +](#)
[LDAP User Import +](#)
[Bulk User Import +](#)
[Download csv template](#)

<input type="text" value="First name"/>	<input type="text" value="Last name"/>	<input type="text" value="Email"/>	<input type="text" value="Position"/>	<input type="button" value="Add +"/>
---	--	------------------------------------	---------------------------------------	--------------------------------------

First Name	Last Name	Email	Position	Action
James	Jones	jones@xxxxxxxxxx.com	Analyst	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

3. Update the details, and click *Submit*.
4. (Optional) Click the Delete button to remove the user from the group.

**Filtering group list**

To filter the group list, utilize the search option in the Name column to search for specific groups.

Name ▲ ▼ 🔍

Additionally, you can apply the risk grade filter in the Risk Grade column. All columns can be sorted by clicking on the arrow icons next to the column title.

**Risk Grade** ⌵

D	<input type="checkbox"/> A
	<input type="checkbox"/> B
A	<input type="checkbox"/> C
	<input type="checkbox"/> D
	<input type="checkbox"/> F
F	<input type="checkbox"/> NA

### Hide/Unhide a group

By **hiding** a group, it will no longer appear in the group list page or when creating a campaign. This applies to both manually created groups and groups imported from Azure AD.

#### To hide a group:

1. Go to *Recipients > Group List*.
2. Click *Actions* menu and select *Hide groups*.

Name	Risk Grade	# Of Members	Created	Application	
outlook_grp	D	11	Manually	NA	9 AM
Dev	A	3	Azure AD Sync	Phish_AD	06/06/2023 7:24 AM

Add Group +

- ▾
- 
- 
-

3. Select the desired groups and click *Hide*.

Name	Risk Grade	# Of Members	Created	Application	Modified Date
<input checked="" type="checkbox"/> outlook_grp	D	11	Manually	NA	06/06/2023 7:59 AM
<input type="checkbox"/> Dev	A	3	Azure AD Sync	Phish_AD	06/06/2023 7:24 AM

- 4.
5. A confirmation message is displayed. Click *Yes*.

! Do you want to hide user group?

These groups will not listed during the creation of a campaign  
outlook\_grp

- 6.

When the unhide option is selected, the list of hidden groups will be displayed. You can unhide the groups, allowing them to appear in the group list page and when creating a campaign.

**To unhide a group:**

1. Go to *Recipients > Group List*.
2. Click *Actions* menu and select *Unhide groups*.

Name	Risk Grade	# Of Members	Created	Application
Dev	A	3	Azure AD Sync	Phish_AD

- 3.
4. Select the desired groups and click *Unhide*.

Name	Risk Grade	# Of Members	Created	Application	Modified Date
<input checked="" type="checkbox"/> outlook_grp	D	11	Manually	NA	06/06/2023 7:59 AM

- 5.
6. A confirmation message is displayed. Click *Yes*.

Do you want to unhide user group?  
These groups will be listed during the creation of a campaign  
outlook\_grp

No Yes

- 7.



You cannot delete, edit, or modify groups imported from an Azure AD client. You can only modify or manage them from the Azure AD server.

**Deleting a group**

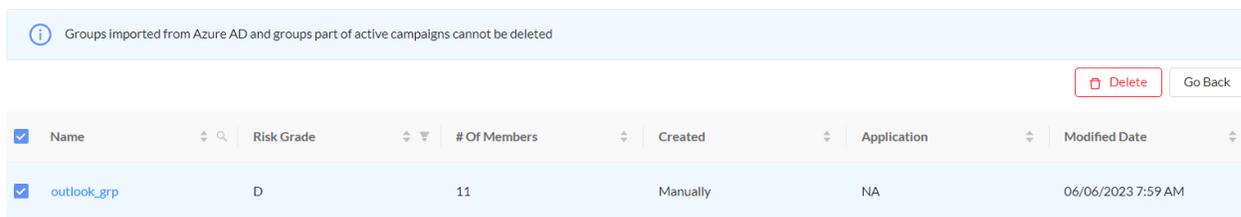
Groups imported from Azure AD and groups part of active campaigns cannot be deleted.

To delete a group:

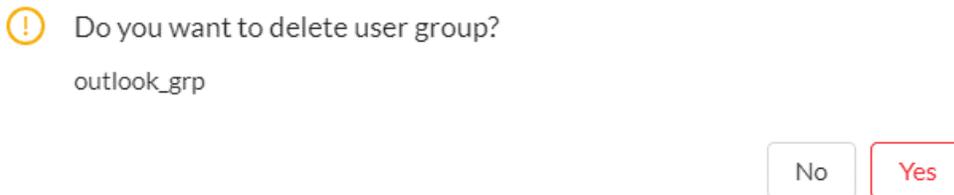
1. Go to *Recipients > Group List*.
2. Click *Actions* menu and select *Delete groups*.

Name	Risk Grade	# Of Members	Created	Application
outlook_grp	D	11	Manually	NA

3. Select the desired group and click *Delete*.



4. A confirmation is displayed. Click Yes.

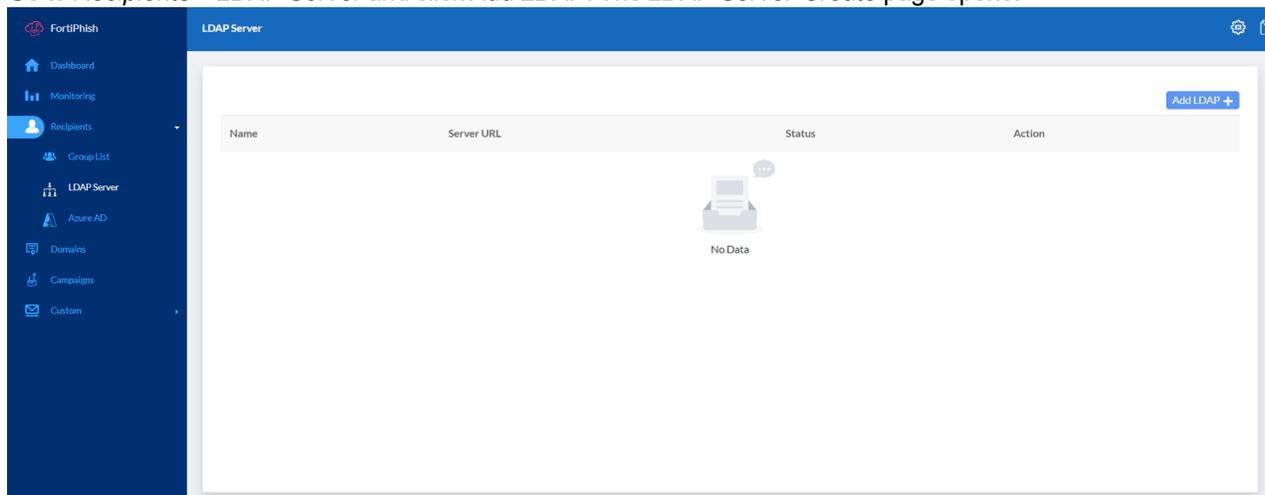


## LDAP server

Perform a bulk user import using an enterprise LDAP/AD. After the server is added, you can import the recipients.

**To add an LDAP server:**

1. Go to *Recipients > LDAP Server* and click *Add LDAP*. The *LDAP Server-Create* page opens.



2. Configure the LDAP server settings.

<b>Name</b>	The LDAP server name.
<b>Server URL</b>	The LDAP server URL.

<b>Connection Mode</b>	Select <i>Non-TLS</i> , <i>TLS</i> , or <i>STARTTLS</i> .
<b>BaseDN</b>	The point where the server will search for users.
<b>Search Filter</b>	The search filter syntax.

3. (Optional) Expand *Advanced Field Matching* and configure the settings.

4. Test the connection.
  - a. Click *Test Connectivity*. The *Test Connectivity* dialog opens.
  - b. Enter the *LDAP User Name* and *Password*.
  - c. Click *Submit*.
5. Click *Submit*. A confirmation message is displayed.

## Azure AD Server

Connect FortiPhish to your organization's Azure AD tenant to import users and groups to create new recipients.

- [Configuring Azure AD for FortiPhish](#)
- [Adding an Azure AD server](#)
- [Syncing the Azure AD server](#)
- [Deleting an Azure AD server](#)

## Configuring Azure AD for FortiPhish

Generate a Application ID and Secret in Azure AD to allow access for FortiPhish service.

### To generate a Application ID and Secret in Azure AD:

1. In Azure or O365 portal, switch to *Azure Active Directory* page.
2. Create a new application that can be associated with FortiPhish. In azure portal:
  - a. Go to *App Registrations > New Registration*.
    - i. Provide a name for App. Ex. *FortiPhish-AD-Proxy*.
    - ii. Select the tenant.
    - iii. Leave *Redirect URI* blank.
  - b. Record the *Application ID* and *Tenant ID*.
3. Create an Access key.
  - a. Under *App Registrations* select the created application.
  - b. Go to *Certificates & Secrets > New Client Secret*.
  - c. Record the Client Secret (named *value* in the GUI).
4. Provide permissions to Graph API.
  - a. Under *App Registrations* select the created application.
  - b. Go to *API Permissions > Add permission*.
  - c. Select *Microsoft Graph* and then *Application Permissions*.
  - d. Provide Permissions to the list of users and groups such as *Directory ReadAll* and *Group ReadAll*.

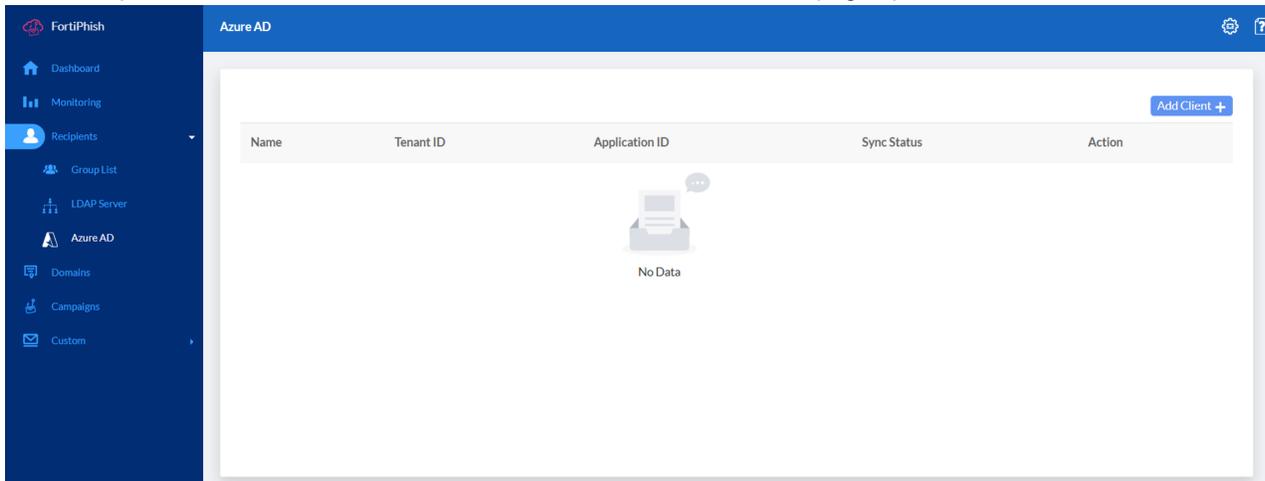


After permissions are added, you should *grant* them using *Grant admin consent to xxx* in permission overview page.

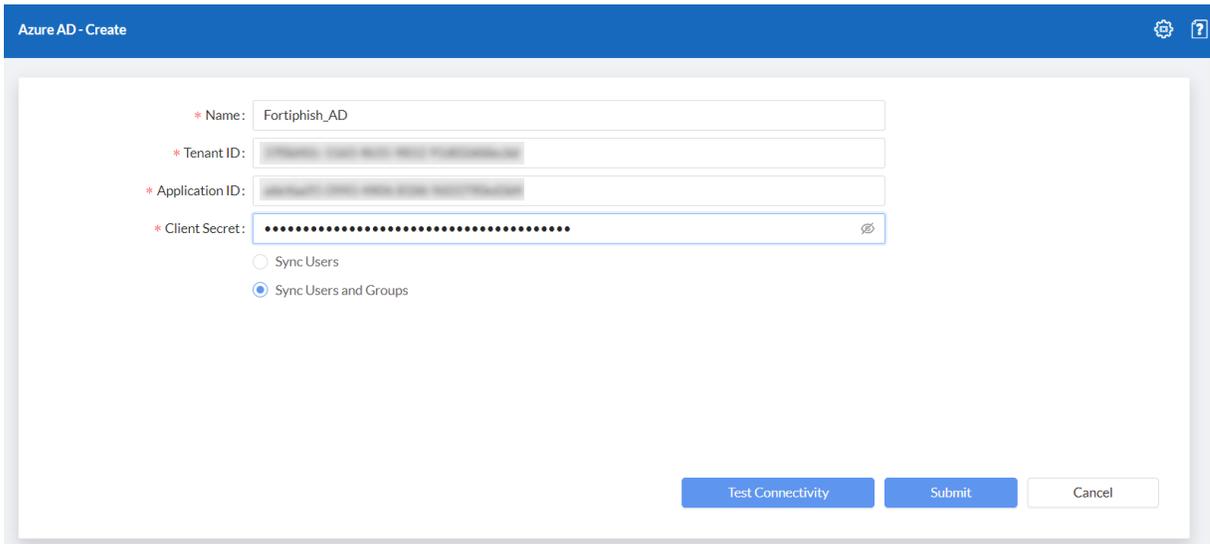
## Adding an Azure AD server

To add an Azure AD server:

1. Go to *Recipients > Azure AD* and click *Add Client+*. The *Azure AD-Create* page opens.



- 2. Configure the Azure AD server settings.
  - a. Enter a *Name* for Azure AD.
  - b. - Enter the *Tenant ID*, *Application AD*, and *Client Secret* information gathered during [Configuring Azure AD for FortiPhish](#).
  - c. Select *Sync Users* to import only the users or select *Sync Users and Groups* to import both users and groups from Azure AD.



- 3. To test the connectivity, click *Test Connectivity*.
- 4. Click *Submit*. A confirmation message is displayed.

 **Create AD Client**  
Successfully created AD Client





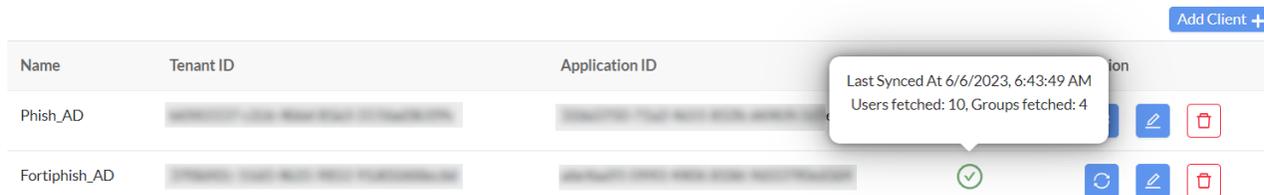
Groups imported from Azure AD are automatically added under [Recipients > Group List](#). If only users are imported, they must be added to a group manually. See [Creating Azure AD user groups](#).

## Syncing the Azure AD server

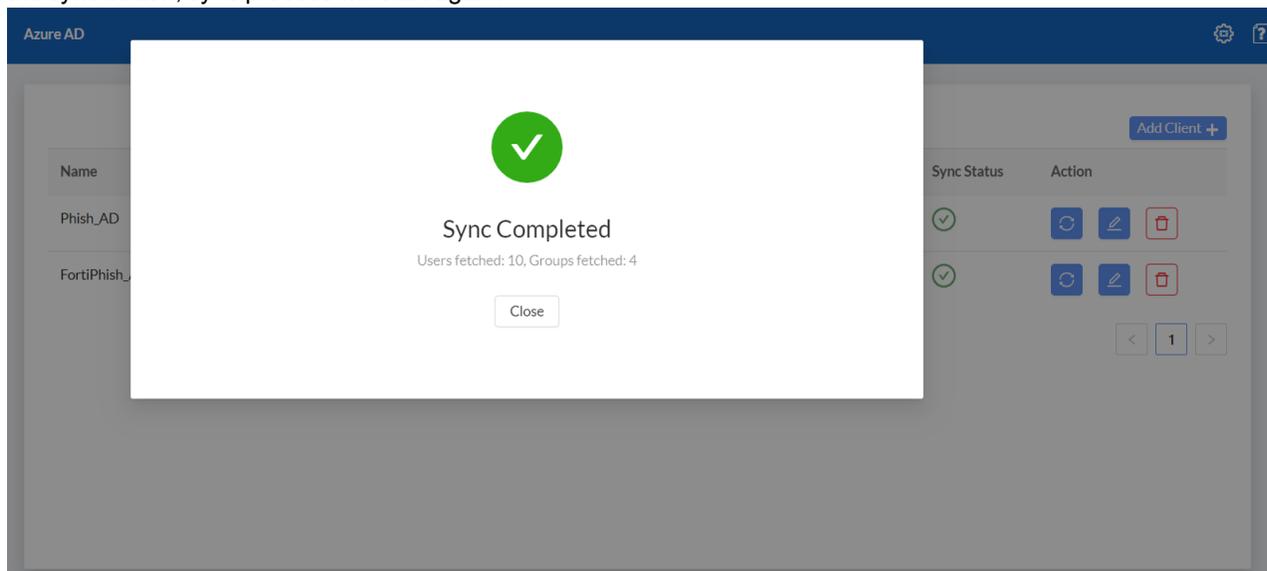
You can sync the Azure AD server when members join or leave your organization.

**To sync the server:**

1. In FortiPhish, go to *Recipients > Azure AD*.
2. (Optional) In the *Sync Status* column, hover over the status column to view the latest sync date and time. If *Sync Users and Groups* option is selected while adding Azure AD, number of users and groups fetched is displayed else if *Sync Users* is selected, only the number of users fetched is displayed.



3. In the *Action* column, click the sync button. During the sync process, clicking the sync button will display the number of users or users and groups fetched information.
4. When the sync is complete, a confirmation message is displayed. Once the sync process is completed, if you click the sync button, sync process will start again.



**Deleting an Azure AD server**

To delete an Azure AD server:

1. Go to *Recipients > Azure AD Server*.
2. In the *Actions* column of the desired Azure AD client click the delete button. A confirmation window is displayed.

 Do you want to delete Azure AD Client?

Note: This will delete all existing Azure Active Directory imported data

3. Click Yes.

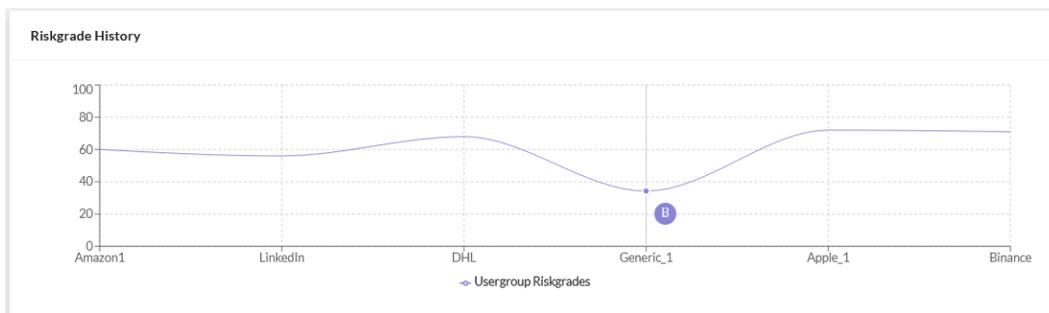


When an Azure AD client is deleted, the associated groups that have been imported will also be deleted, along with the client details.

## Risk Grade History

Each group is assigned a letter grade between A and F based on the responses across multiple campaigns. An A indicates the group poses minimal risk and an F grade indicates the group poses the maximum risk to the organization. The group *Risk Grade* is displayed in both the *Group List* and *Usergroup* pages.

The *Riskgrade History* chart shows the group's performance across campaigns from the oldest to newest. Hover over the chart to view the group's grade.



### To view the Riskgrade History:

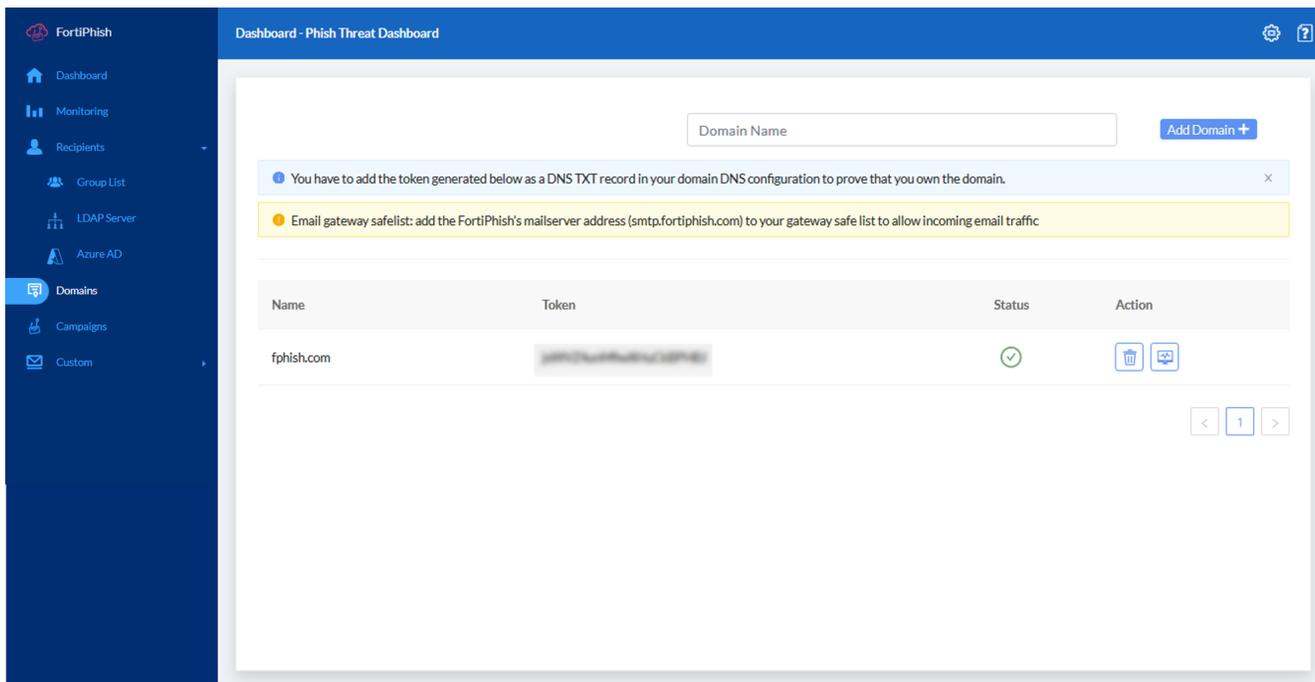
1. Go to *Recipients > Group List*.
2. Click a group in the list, then scroll down to view the chart.



The *Risk Grade* is not displayed in active campaigns.

# Domains

The *Domains* view displays a list of DNS tokens used to verify you own the domain. Use this page to create DNS tokens and monitor their status. See [Adding domains on page 34](#).

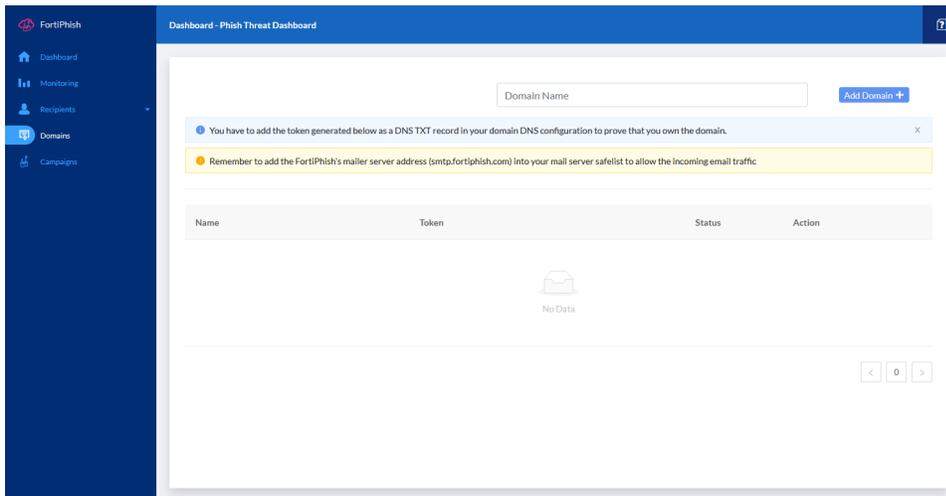


## Adding domains

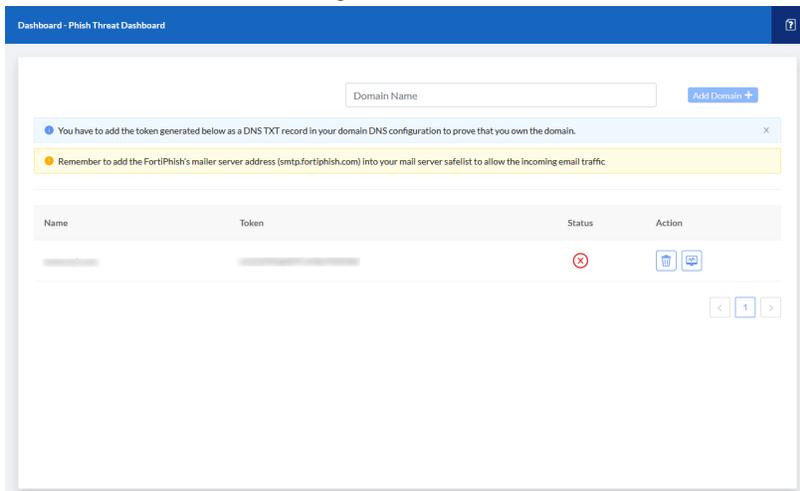
FortiPhish uses DNS tokens to verify you are the domain owner. Create the token in FortiPhish, and then add it to your domain's DNS settings. After the DNS settings are configured, verify the token in FortiPhish.

**To add a domain:**

1. Go to *Domains*.



2. In the *Domain Name* field, enter the domain address. For example, *domain.com*.
3. Click *Add Domain*. FortiPhish generates a DNS token.



**To add the token to your domain:**

1. Log in to your domain.
2. Go to the domain settings, and navigate to the DNS management area.
3. Change the text record setting to *TXT*.
4. Enter the token you created in FortiPhish.
5. Test the token with `nslookup`.



DNS settings will vary depending on your domain provider. For information, refer to the product documentation.

The following images shows the DNS settings in AWS.

**Define simple record** ✕

**Record name**  
To route traffic to a subdomain, enter the subdomain name. For example, to route traffic to blog.example.com, enter blog. If you leave this field blank, the default record name is the name of the domain.

blog

Valid characters: a-z, 0-9, ! \* # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~ -

**Value/Route traffic to**  
The option that you choose determines how Route 53 responds to DNS queries. For most options, you specify where you want to route Internet traffic.

IP address or another value depending on the record type

SMK2dVvonKZc3bXoajjPk

Enter multiple values on separate lines.

**Record type**  
The DNS type of the record determines the format of the value that Route 53 returns in response to DNS queries.

TXT – Used to verify email senders and for application-specific values

Choose instead of SPF, or when you want Route 53 to return application-specific values.

**TTL (seconds)**  
The amount of time, in seconds, that DNS resolvers and web browsers cache the settings in this record. ("TTL" means "time to live.")

300

Recommended values: 60 to 172800 (two days)

**To test the token with the command prompt:**

```
nslookup
  set type=text
  <domain.com>
```

**Example:**

```
C:\Users\Admin_>nslookup
Default Server: dns.google
Address 8.8.8.8
```

```
>set type=txt
>yourdomain.com
Server: dns.google
Address 8.8.8.8
```

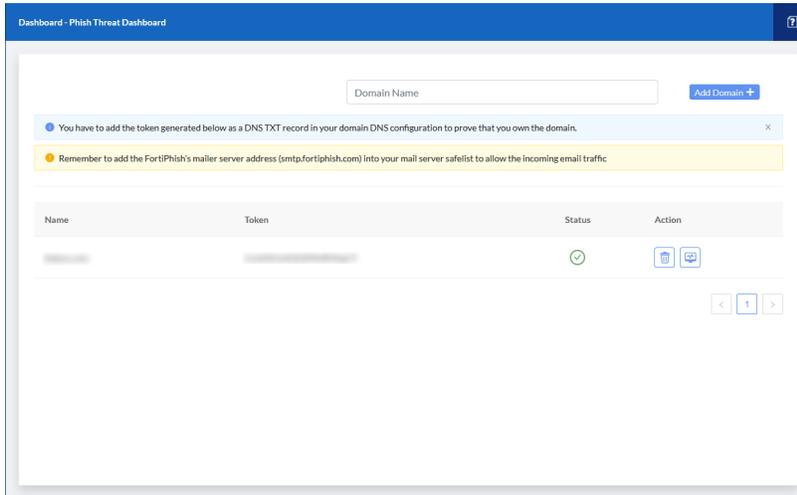
```
Non-authoritative answer:
yourdomain.com text
  <token>
```



DNS propagation delay can take up to 48 hours. Please allow some time for the DNS token to be reflected in the DNS cache.

**To verify the token in FortiPhish:**

1. Go to *Domains*.
2. Under *Actions*, click the *Verify* button. The domain *Status* changes to a green check mark.

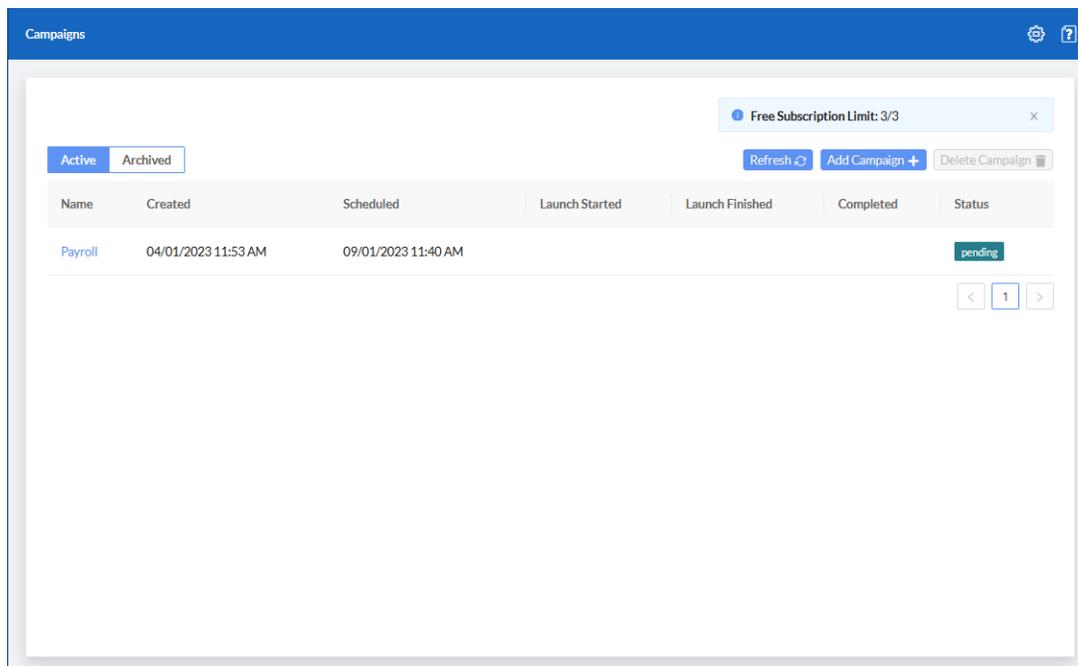


# Campaigns

The *Campaigns* page contains phishing templates to launch a campaign. You can view the status of active campaigns or click the *Archived* tab to view data for completed campaigns. See [Creating campaigns on page 39](#).

## Subscription Limit

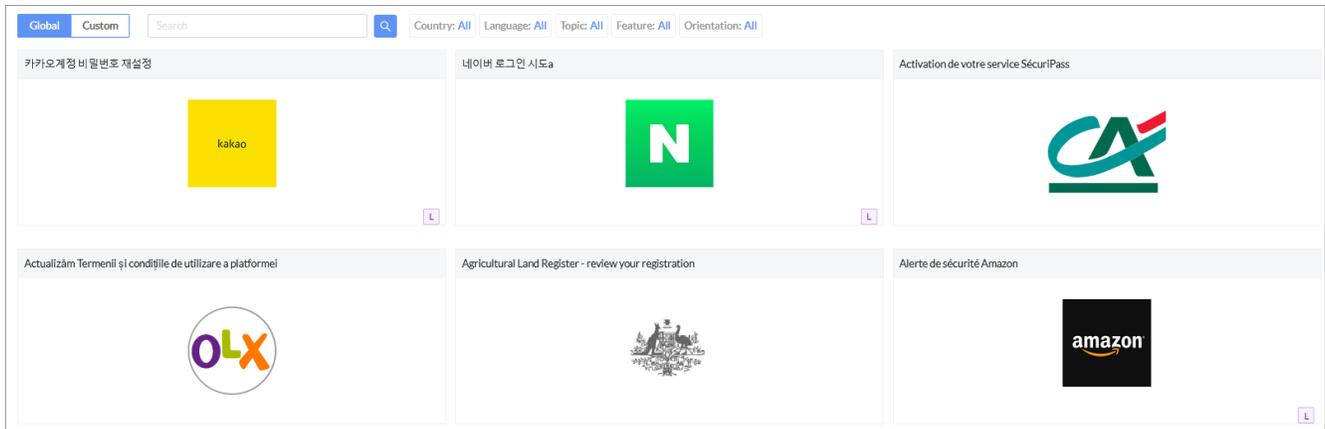
The *Subscription Limit* is directly linked to license entitlement(s). You can run an unlimited number of campaigns, however you are limited by the number of mailboxes. The *Used* count is reset at the beginning of each month.



## Global templates

FortiPhish includes 96 global templates and 70 landing pages allowing you to quickly create and launch campaigns. Global templates are based on popular brands such as Amazon, Apple, and Netflix as well other international brands. You can use the template settings to add a landing page, set the level of difficulty, add attachments and more.

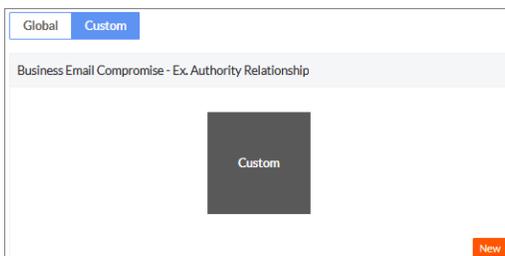
Enter key words in the *Search* field to find a template by name, or use the sort buttons to filter the templates by *Country*, *Language*, *Topic*, *Feature*, or *Orientation*. Templates that contain the letter *L* indicate the template includes a landing page.



## Custom campaigns

FortiPhish allows you to create campaigns based on custom templates and landing pages you created. After the campaign is created, it is added to the templates menu under the *Custom* tab. You can distribute a custom campaign as you would a Global template. For more information, see:

- [Creating custom templates](#)
- [Creating custom landing pages](#)



Custom templates are the property of Fortinet. Fortinet reserves the right to adapt any updates or revisions made to an existing email template and make them available to all users in the *Global Templates* tab.

## Creating campaigns

To create a campaign, select a *Global* or *Custom* template and then configure the clicking behavior, targets and email schedule.

**To create a campaign from a global or custom template:**

1. Go to *Campaigns* and click *Add Campaign*. The *Select a Template* page opens.



To create a campaign from a custom template, click the *Custom* tab. For information, see [Templates on page 55](#).

2. Select a template and configure the campaign settings, then click *Next*. The *Select a Sender* page opens.

<b>Subject</b>	Edit the email subject	
<b>Click Behavior</b>	<b>Only Redirect URL</b>	Enter the URL in the <i>Redirect URL</i> field.
	<b>Landing Page</b>	<ul style="list-style-type: none"> <li>• Select <i>Preset</i> to use the landing page that comes with the template.</li> <li>• Select <i>Custom</i> to use a custom landing page you created. See, <a href="#">Landing page on page 57</a>.</li> </ul> <hr/>  FortiPhish does not save the data entered by the user in the landing page.
<b>Level of Difficulty</b> (This option is only available in <i>Global</i> templates.)	<b>Simple</b>	<p>The email is poorly written and contains spelling and grammar errors in the body text and domain. The link text and URL do not match.</p> <p>The email branding does not match the branding in the landing page.</p>
	<b>Moderate</b>	<p>The email body is well written but contains two or three phishing email indicators such as spelling errors in the domain and mismatched link / URL text.</p> <p>The landing page looks authentic.</p>
	<b>Challenging</b>	<p>The email body is well written and does not contain spelling errors. The email branding and tone mimics authentic corporate communications.</p> <p>The landing page looks very authentic.</p>
<b>Use Attachment</b>	To attach a PDF to the email, Select <i>Yes, Using Filename</i> and enter the filename in the text field.	
		<hr/>  FortiPhish will not be able to collect the <i>Executed</i> metric when the attached PDF is previewed in a reader that disables links for security purposes.

**Track User Reply**

Click **Yes** to create targeted emails that have no click or attachments but will simulate an actual spear-phish and allow you to see which users respond and/or attach compromising information.

**Activate On Click Training**

Click **Yes** to alert recipients they are the victim of a phishing attack. When the recipient clicks a link in the email or submits data using the phishing landing page, they are directed to a page that contains an embedded training video.

There are four types of training pages:

- *Phishing*
- *Avoid Phishing Attack*
- *Identify Phishing Attack*
- *What is Phishing?*

For information, see [Campaign Training Stats](#).

**Preview**

In the text editor, compose the email body.



You can use variables in the email body to generate dynamic data while the campaign is running. See, [Template variables on page 42](#).

**Save as Custom Template**

Save a Global template as a Custom template.

Click to view a preview of the template and then click *Submit*. The template is saved to *Custom > Templates*.



- The *Level of Difficulty* settings are not saved in custom templates.
- Custom templates are the property of Fortinet. Fortinet reserves the right to adapt any updates or revisions made to an existing email template and make them available to all users in the *Global Templates* tab.

3. Configure the campaign details and click *Next*. The *Select a Target* page opens.

**Campaign Name**

Enter the campaign name.

**Sender Name**

Edit the sender's name.

**Sender Email**

Edit the sender's email address.

**SMTP Gateway Server**

(Optional) Select an SMTP server from the dropdown. For information, see [SMTP on page 72](#).

**Test Email**

Enter an email address and click *Test*.

Sending a test email is recommended when using a custom SMTP gateway server. The selected SMTP server cannot deliver any campaign emails if error occurs while sending a test mail.

4. Select one or more target groups from the *Recipients* dropdown and click *Next*. The *Set a Schedule* page opens.

- Configure the date, time, and duration of the campaign and click *Next*. The *Set Email Schedule* page opens.

<b>Campaign Schedule</b>	<b>Scheduled</b>	Select the Launch date and time.
	<b>Start it Now</b>	Launch the campaign today.
<b>Time Zone</b>	Select the time zone from the dropdown.	
<b>Campaign Duration</b>	Set the campaign duration from 1 to 4 weeks.	

- On the *Set Email Schedule* page, choose how the emails are to be sent.

<b>All At Once</b>	Start sending emails right away and finish within one hour.	
<b>Randomly</b>	<b>Within</b>	Select the duration in which the emails are to be sent. When <i>1 Week</i> is selected the last day of the week is disabled because it does not provide the recipient enough time to perform any meaningful actions.
	<b>Weekday</b>	Select the days of the week the emails are to be sent.
	<b>Time Range</b>	Select the hours of the day within which the emails are to be sent. The default value is <i>09:00</i> to <i>17:00</i> hours.

- Click *Start campaign*. A confirmation message appears.
- Click *OK*.

## Template variables

You can add template variables to the email subject and body to generate dynamic data when the campaign is running. Template variables are only supported in custom templates.

### Supported Variables for custom template

Variable	Description	Output
{{date layout}}	Date with layout	See <a href="#">Date with Layout or Offset</a>
{{date offset}}	Date with offset	See <a href="#">Date with Layout or Offset</a>
{{date}}	Date	02-Jan-2006
{{email_domain}}	Recipient's email domain	fortiphish.com
{{email_username}}	Recipient's username	johndoe
{{num min max}}	Generate a random number	{{num 0 10000}} 4470 {{num 0.0 10000.0}} 4470.4
{{recipient_email}}	Recipient's email	johndoe@fortiphish.com
{{recipient_firstname}}	Recipient's first name	John
{{recipient_lastname}}	Recipient's last name	Doe
{{recipient_position}}	Recipient's position	Manager

Variable	Description	Output
{{time}}	Time	3:04 PM
{{tracking_click_link}}	Link for tracking	https://smtp.fortiphish.com/trackings/ {{recipient}}

## Date with Layout or Offset

### {{datelayout}}

Standard	Format
ANSIC	Mon Jan _2 15:04:05 2006
UnixDate	Mon Jan _2 15:04:05 MST 2006
RubyDate	Mon Jan 02 15:04:05 -0700 2006
RFC822	02 Jan 06 15:04 MST
RFC822Z	02 Jan 06 15:04 -0700
RFC850	Monday, 02-Jan-06 15:04:05 MST
RFC1123	Mon, 02 Jan 2006 15:04:05 MST
RFC1123Z	Mon, 02 Jan 2006 15:04:05 -0700
RFC3339	2006-01-02T15:04:05Z07:00
RFC3339Nano	2006-01-02T15:04:05.999999999Z07:00

### Example:

```
{{date|02-Jan-2006 3:04 PM}}
```

### Output:

09-Oct-2021 3:04 PM

### {{date/offset}}

**date:** 01 Jan 2021

Type	Symbol	Example	Result
Day	d	{{date +1d}}	02-Jan-2021
Week	w	{{date +2w}}	15-Jan-2021
Month	m	{{date +3m}}	01-Apr-2021
Year	y	{{date -3y}}	01-Jan-2018

## Viewing campaign statistics

View a summary of the campaign details, as well as detailed response statistics. You can view the campaign statistics for active and archived campaigns.

### To view the campaign statistics:

1. Go to *Campaigns*. The campaign list is displayed.
2. (Optional) Click the *Archived* tab. Campaigns are saved to the *Archived* tab after the campaign is completed.
3. Click the campaign name. The *Campaign - Details* page is displayed.
  - [Campaign Summary](#)
  - [Campaign Timeline](#)
  - [Campaign Preview](#)
  - [User Pass Rate](#)
  - [Campaign Status](#)
  - [Campaign Stats](#)
  - [Campaign Training Stats](#)
  - [User Profile](#)
  - [Recipient Stats](#)
  - [Usergroup Stats](#)

## Campaign Summary

The *Campaign Summary* monitor displays the *Campaign Name*, *Campaign Mail Title*, *Email Schedule*, *Campaign Mail Sender*, *Track User Reply*, *Use Attachment* and *Clicking Behavior*. If an attachment was used, the monitor displays *Filename*.

Campaign Summary	
Campaign Name:	Generic_1
Campaign Mail Title:	Request for partnership
Emails Schedule:	All At Once
Campaign Mail Sender:	William Forson 0u9gyx8pub6wz@gmail.com
SMTP Gateway Server:	Default Server
Track User Reply:	Yes
Use Attachment:	No
Clicking Behavior:	Landing Page
Landing Page Type:	System
Landing Page Name:	Generic
Training Topic Name:	Avoid Phishing Attack

Risk Grade

Close Fail

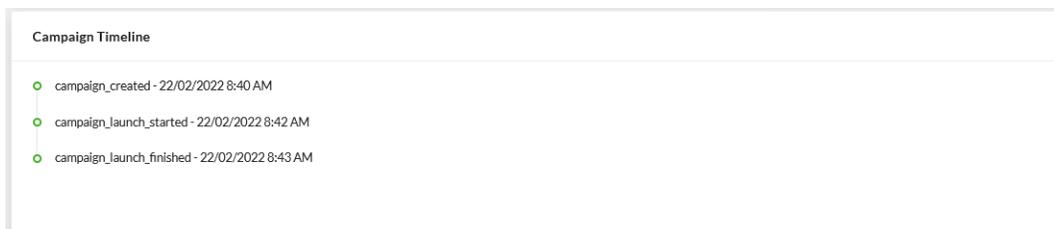
### Campaign Name

The name you entered when you created the campaign.

<b>Campaign Mail Title</b>	The subject line of the email.
<b>Email Schedule</b>	Either <i>All At Once</i> or <i>Random</i> .
<b>Campaign Mail Sender</b>	The email <i>From</i> address.
<b>SMTP Gateway Server</b>	The name and domain of the SMTP Gateway Server if one was used.
<b>Track User Reply</b>	Yes if email has no click or attachments but simulates an actual spear-phish to see which users respond and/or attach compromising information.
<b>Use Attachment</b>	A PDF is attached to the email.
<b>Clicking Behavior</b>	One of <i>Landing Page</i> , <i>Preset</i> or <i>Only Redirect URL</i> .
<b>Landing Page Type</b>	<i>System</i> or <i>Custom</i> .
<b>Landing Page Name</b>	The name entered in the <i>Title</i> field of the landing page.
<b>Filename</b>	The name used for the attachment.
<b>Training Topic Name</b>	The training page name.
<b>Risk Grade</b>	The letter grade between <i>A</i> and <i>F</i> assigned to the campaign.

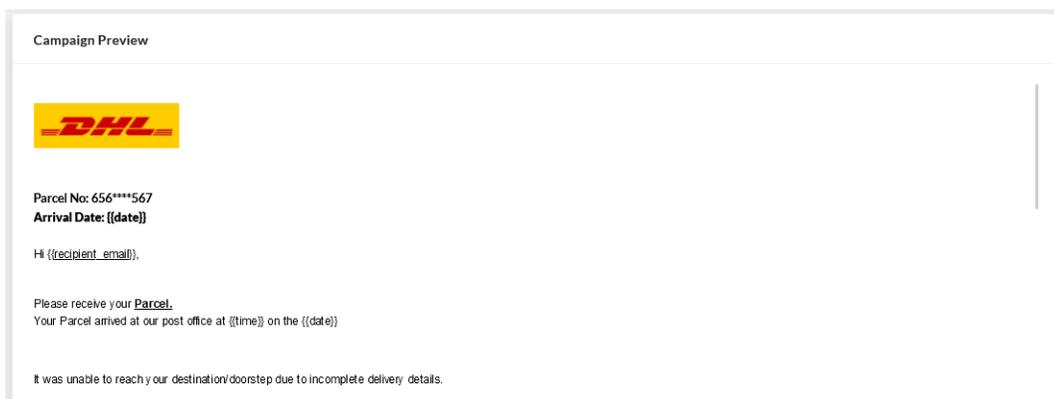
## Campaign Timeline

The Campaign Timeline widget displays when the campaign was created, started and finished as well as the recipient's actions in UTC format.



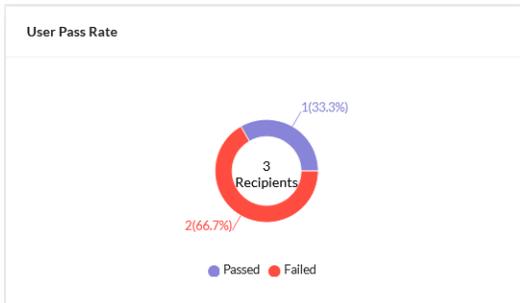
## Campaign Preview

The *Campaign Preview* monitor displays a preview of the email that was distributed to users.



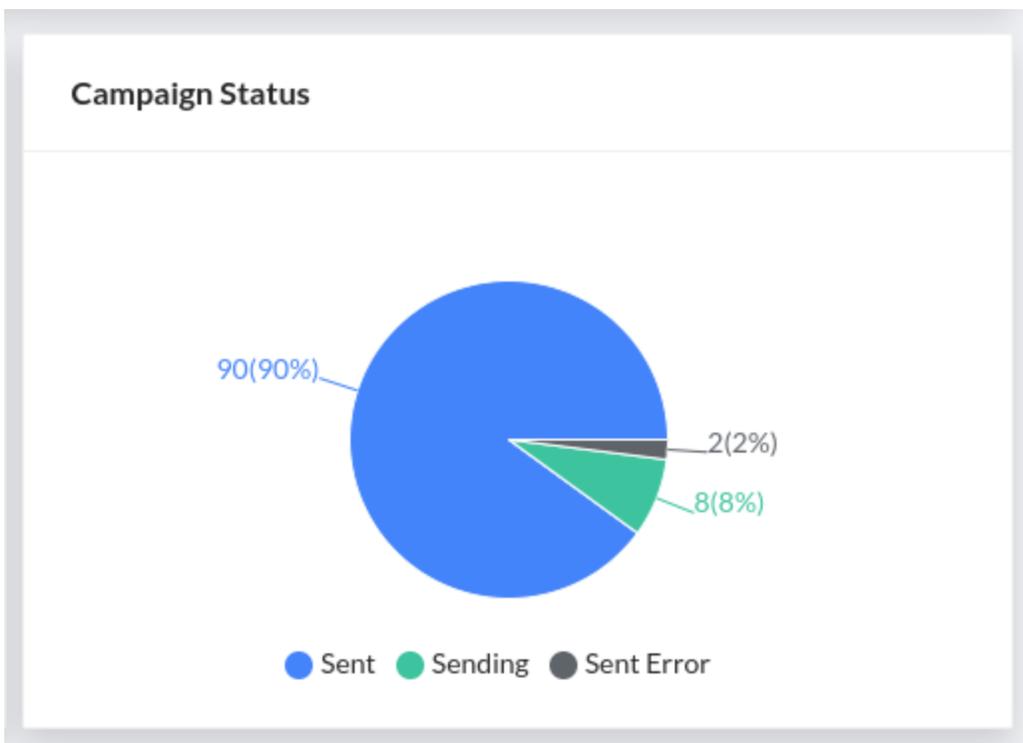
## User Pass Rate

The *User Pass Rate* chart displays the pass rate as a pie chart. Hover over the chart to view the number of recipients who passed or failed.



## Campaign Status

The *Campaign Status* monitor displays the number of emails that were delivered and bounced.

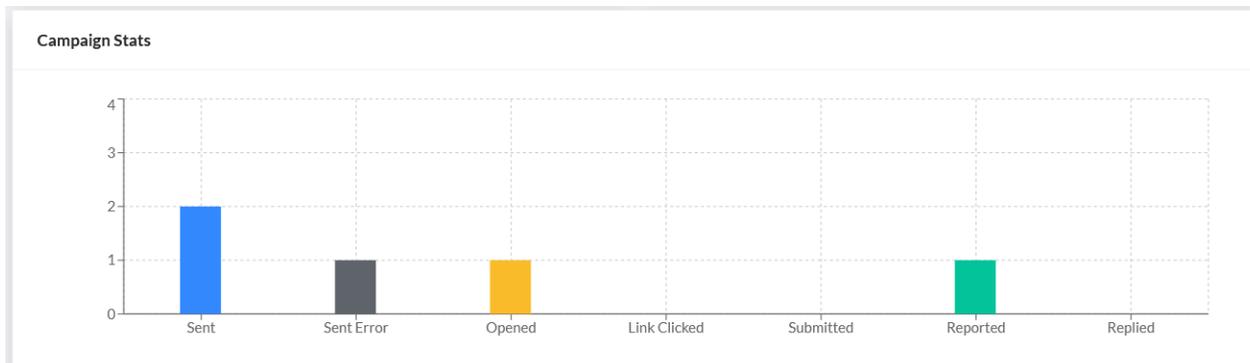


The *Campaign Status* monitor displays the following information:

<b>Sent</b>	The number of emails sent to the user group.
<b>Sending</b>	The number of emails waiting to be sent.
<b>Sent Error</b>	The number of emails that bounced.

## Campaign Stats

The *Campaign Stats* monitor displays information about how the recipient interacted with the email. Hover over the chart to view the number of emails for each category.



<b>Sent</b>	The number of emails sent to the user group.
<b>Sent Error</b>	The number of emails that bounced.
<b>Opened</b>	The number of recipients who opened the email.
<b>Link Clicked</b>	The number of recipients who clicked the redirect link.
<b>Submitted</b>	The number of recipients who entered information on the landing page.
	 <p>FortiPhish does not save the data entered by the user in the landing page.</p>
<b>Reported</b>	The number of recipients who reported the phishing email as suspicious.
<b>Executed</b>	The number of recipients who opened or executed the file attached in the phishing email.
	 <p>FortiPhish will not be able to collect the <i>Executed</i> metric when the attached PDF is previewed in a reader that disables links for security purposes.</p>
<b>Replied</b>	The number of recipients who replied to the email.

## Campaign Training Stats

The *Campaign Training Stats* chart displays the number of recipients who completed and did not complete training for the campaign.



A recipient is counted as *Training Complete* after they acknowledge they have reviewed the information in the training web page. For information about *On Click Training*, see [Creating campaigns](#).

## Woah, You Got Phished!

But Don't worry, this was just a test

You've just participated in a campaign designed to access your organization's risk susceptibility to phishing attacks. Because you have interacted with phishing email, which could be a potential threat for your organization if it was a real phishing attack.

Taking the following mandatory training now will improve your phishing detection skills and prevent you from getting hooked again, ever.

## Avoid Phishing Attack

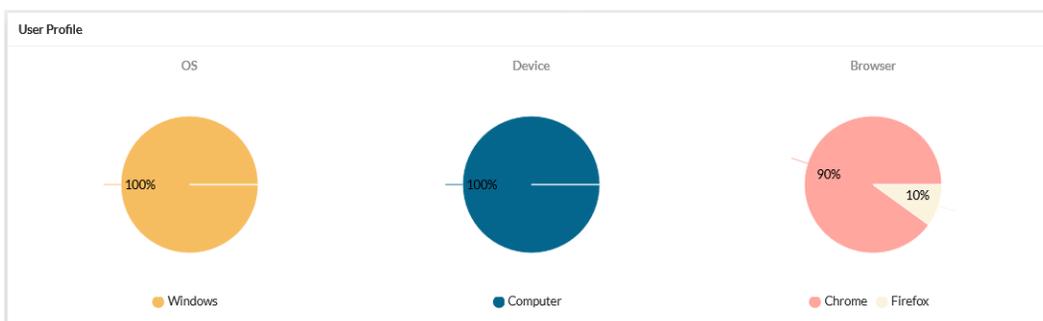
▶

I acknowledge that I have completed this training, and now aware about phishing emails

Completed

## User Profile

The *User Profile* monitor displays information about the device the recipient used to view the email. Hover over the cart to see the value for each category.



The *User Profile* monitor displays the following information:

<b>OS</b>	The operating system of the device.
<b>Device</b>	The device hardware.
<b>Browser</b>	The browser the recipient used to view the email.

## Recipient Stats

The *Recipient Stats* monitor displays the recipient statistics.

Email	Risk Grade	User Group	Status	Client IP	Location	Reporting Speed	Action
[Redacted]	NA	outlook	Error				<a href="#">View Timelines</a>
[Redacted]	F	outlook	<span>Sent</span> <span>Opened</span> <span>Clicked</span> <span>Reported</span> <span>Replied</span> <span>Executed</span> <span>Training Incomplete</span>	182.71.233.2	IN (India)		<a href="#">View Timelines</a>

The *Recipient Stats* monitor displays the following information:

<b>Email</b>	The user email address.
<b>Risk Grade</b>	The letter grade between <i>A</i> and <i>F</i> assigned to the recipient . An <i>A</i> indicates the user poses minimal risk and a <i>F</i> grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be <i>NA</i> on the <i>Dashboard</i> and <i>Monitoring</i> pages.
<b>User Group</b>	The user group the recipient belongs to.
<b>Status</b>	Displays the recipient's response <i>Sent</i> , <i>Pending</i> , <i>Opened</i> , <i>Clicked</i> , <i>Submitted</i> , <i>Reported</i> , <i>Executed</i> and <i>Training Complete/Training Incomplete</i> .
<b>Client IP</b>	The recipient's IP address.
<b>Location</b>	The recipient's country.
<b>Report Speed</b>	<p>The recipient's response time.</p> <ul style="list-style-type: none"> <li><i>Platinum</i>: Under 30 seconds</li> <li><i>Gold</i>: Under 5 minutes</li> <li><i>Silver</i>: Under 30 minutes</li> <li><i>Bronze</i>: Under 59 minutes</li> </ul> <p>An empty field indicates the recipient did not report the phish attempt. To view the actual response time, hover over the medallion.</p>
<b>Action</b>	Click the <i>View Timeline</i> link to view the date and times of the recipient's actions.

## Usergroup Stats

The Usergroup Stats displays group statics.

Usergroup Stats										
User Group	Risk Grade	Sent	Sent Error	Opened	Link Clicked	Submitted	Reported	Replied	Training Complete	Training Incomplete
outlook_grp	D	2	1	1	0	0	1	0	0	0

< 1 >

The *Usergroup Stats* displays the following information:

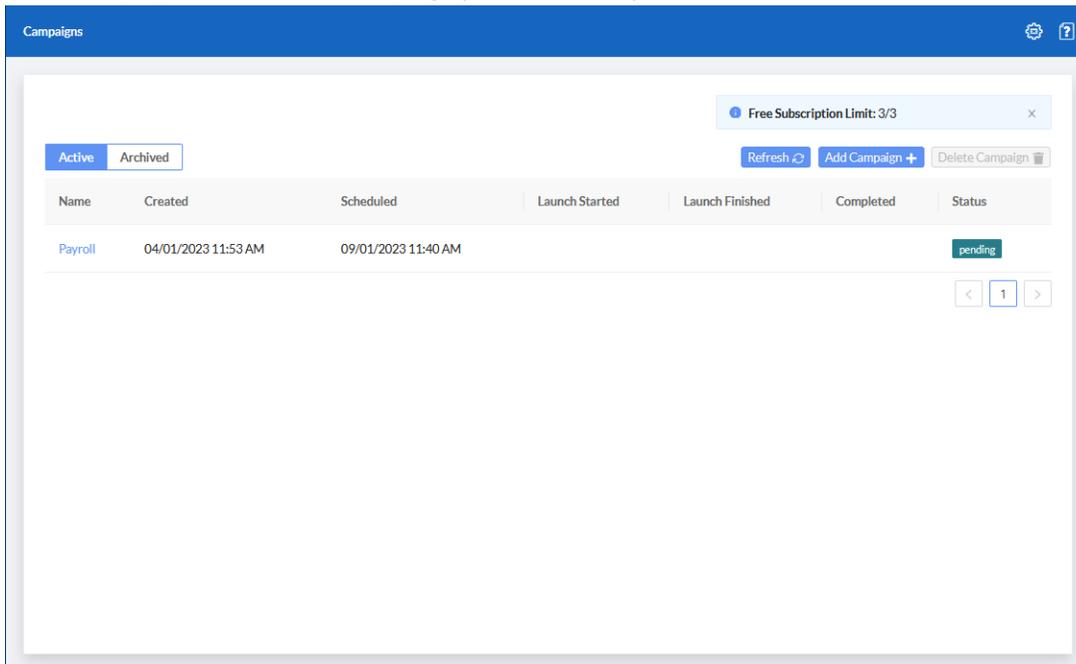
<b>User Group</b>	The user group name.
<b>Risk Grade</b>	The letter grade between <i>A</i> and <i>F</i> assigned to the group. An <i>A</i> indicates the group poses minimal risk and a <i>F</i> grade indicates the group poses the maximum risk to the organization.
<b>Sent</b>	The number of emails sent to the user group.
<b>Sent Error</b>	The number of emails that bounced.
<b>Opened</b>	The number of recipients who opened the email.
<b>Link Clicked</b>	The number of recipients who clicked the redirect link.
<b>Submitted</b>	The number of recipients who entered information on the landing page.
<b>Reported</b>	The number of recipients who reported the phishing email as suspicious.
<b>Replied</b>	The number of recipients who replied to the email.
<b>Training Complete</b>	The number of recipients who have finished the training.
<b>Training Incomplete</b>	The number of recipients who have been enrolled but did not finish the training.

## Retrying a campaign

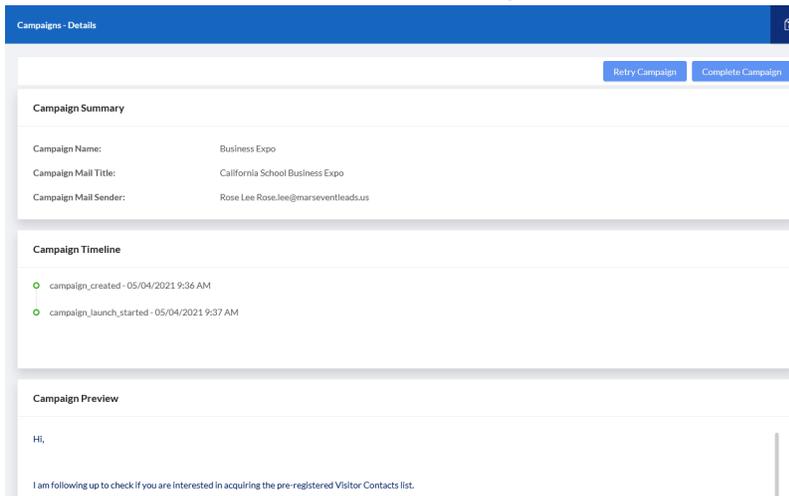
Resend emails that were not delivered or blocked by the mail server.

**To retry a campaign:**

1. Go to *Campaigns* and click the campaign you want to retry.



2. Click *Retry Campaign*. The confirmation dialog opens.



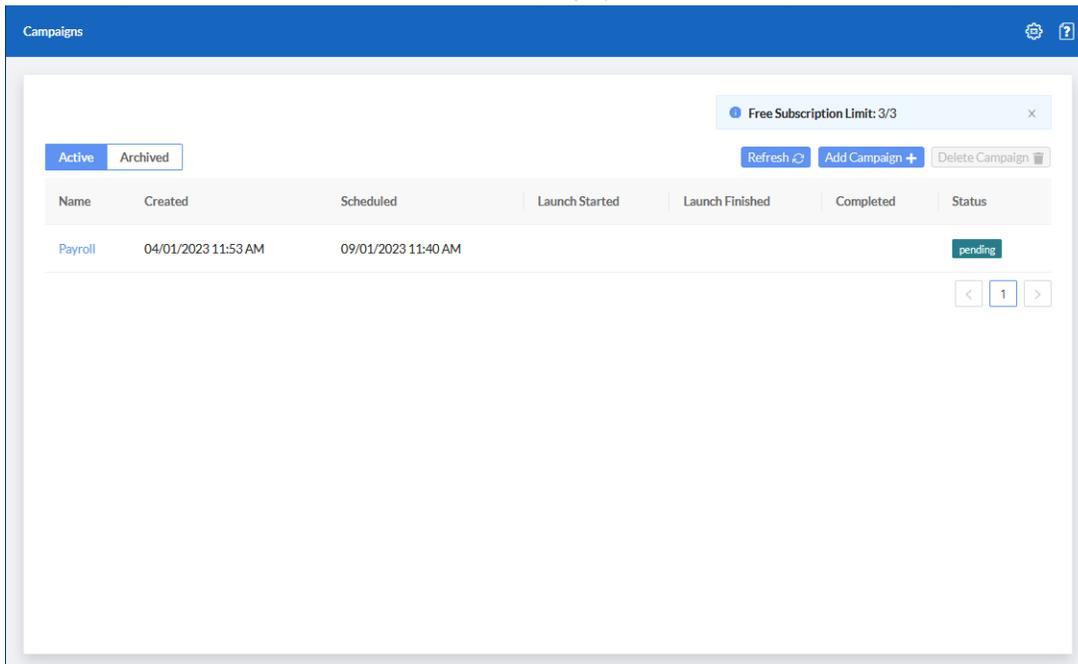
3. Click *OK*. The *Sent* metrics are updated.

## Completing a campaign

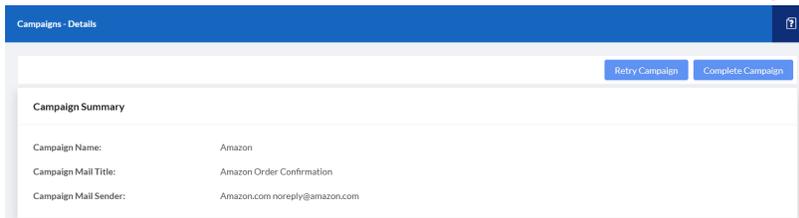
Campaigns are completed after the close date. You can complete a campaign before the campaign close date. After the campaign is completed, it is saved to the *Archived* tab.

**To complete a campaign:**

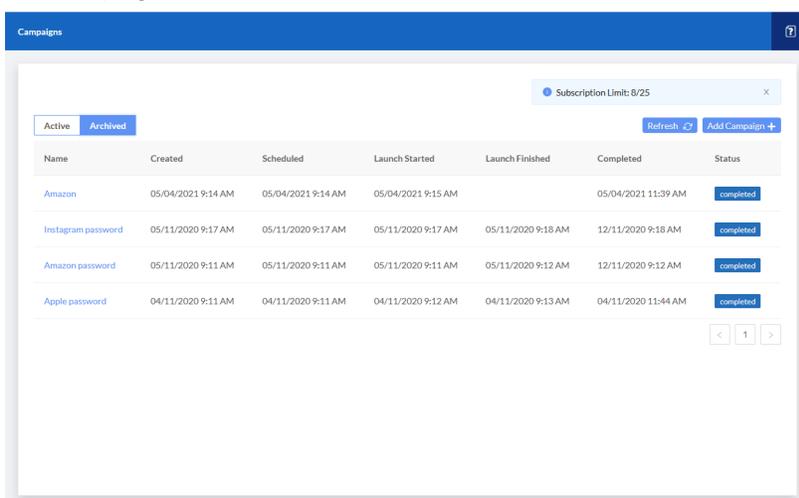
1. Go to *Campaigns* and click the name of the campaign you want to complete. The *Campaigns - Details* page opens.



2. Click *Complete Campaign*, and then click *OK* in the confirmation dialog.



The campaign is moved to the *Archived* tab.

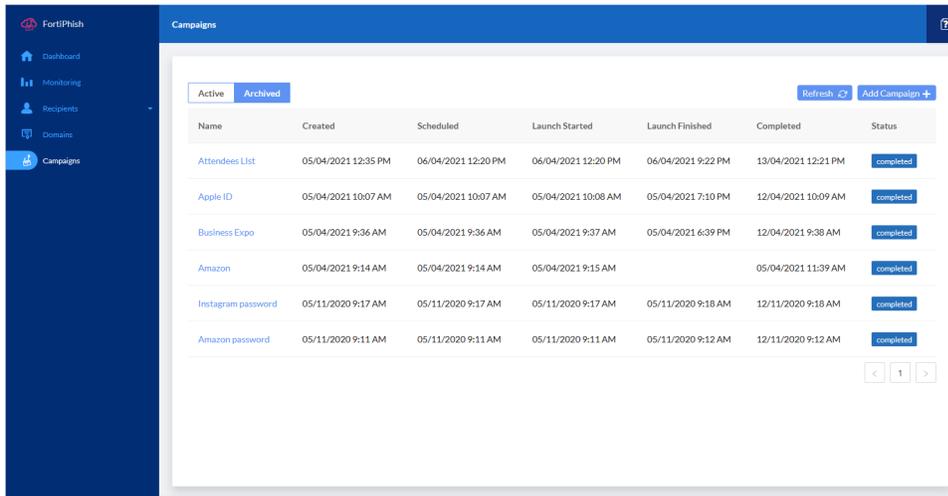


## Exporting campaign statistics

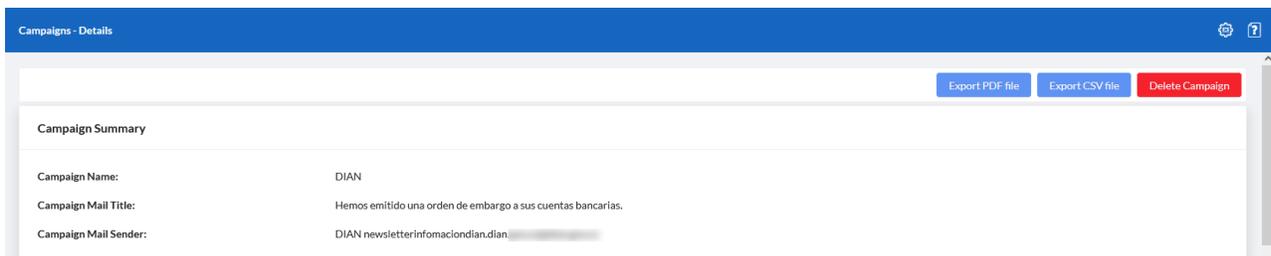
After a campaign is completed, you can export campaign data as a CSV to view the user list and behaviors. You can also generate a *FortiPhish Campaign Report* to view details about the campaign.

### To export campaign data:

1. Go to *Campaigns* and click the *Archived* tab.



2. Click the name of a completed campaign. The *Campaign - Details* page opens.
3. Export the campaign data:



#### Export PDF File

The *FortiPhish Campaign Report* opens in a new browser tab.

The report contains the following sections: *Risk Grade*, *Click To Open Rate*, *Campaign Summary*, *Click To Open Rate*, *Campaign Preview*, *Campaign Timelines*, *Campaign Metric*, and *User Group Report*.

#### Export CSV file

The CSV file is saved to your device.

The file shows the recipients' *email*, as well the statistics for *delivered*, *opened*, *clicked*, *submitted*, *executed*, *replied*, *Risk Grade*, and *reported* emails as yes or no (Y/N) values.

## Deleting archived campaigns

You can manually delete archived campaigns. After a campaign is deleted from the campaign, all the data related to the campaign is removed.



You can schedule archived campaigns to be automatically deleted at monthly intervals in the application settings page. See, [Enable Auto Delete on page 61](#).

### To delete a campaign:

1. Go to *Campaigns > Archived*.
2. Select the campaign(s) you want to delete or click the *Select All* checkbox at the top page .
3. Click *Delete Campaign*. The confirmation dialog opens. page opens.

The screenshot shows the FortiPhish interface with the 'Campaigns' section selected in the sidebar. The main area displays a table of archived campaigns. The table has columns for Name, Created, Scheduled, Launch Started, Launch Finished, Completed, and Status. There are buttons for 'Refresh', 'Add Campaign', and 'Delete Campaign' at the top right of the table. The 'Delete Campaign' button is highlighted in red. The table contains the following data:

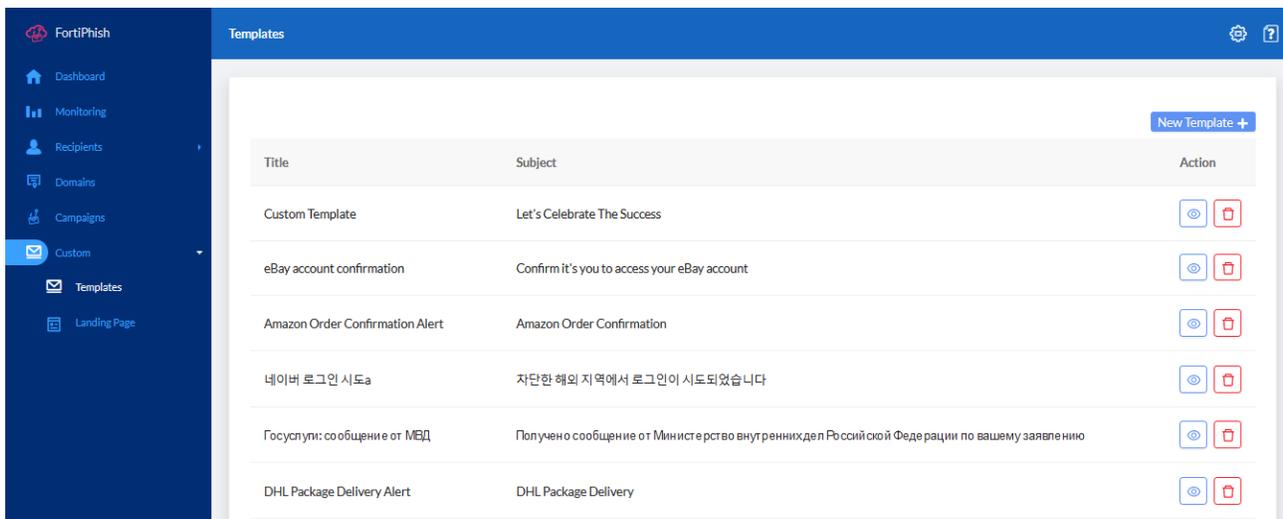
<input type="checkbox"/>	Name	Created	Scheduled	Launch Started	Launch Finished	Completed	Status
<input type="checkbox"/>	Amazon_Campaign_Automation	27/01/2022 2:09 AM	27/01/2022 2:09 AM	27/01/2022 2:10 AM	27/01/2022 2:12 AM	03/02/2022 2:11 AM	completed
<input checked="" type="checkbox"/>	LCS	19/01/2022 8:10 AM	19/01/2022 8:10 AM	19/01/2022 8:11 AM	19/01/2022 8:15 AM	19/01/2022 8:16 AM	completed
<input checked="" type="checkbox"/>	Latest	19/01/2022 7:54 AM	19/01/2022 7:54 AM	19/01/2022 7:55 AM	19/01/2022 7:57 AM	19/01/2022 8:02 AM	completed
<input checked="" type="checkbox"/>	Custom	19/01/2022 7:43 AM	19/01/2022 7:43 AM	19/01/2022 7:44 AM	19/01/2022 7:46 AM	26/01/2022 7:44 AM	completed
<input checked="" type="checkbox"/>	cccc	17/01/2022 11:26 PM	17/01/2022 11:26 PM	17/01/2022 11:27 PM	17/01/2022 11:28 PM	24/01/2022 11:27 PM	completed
<input type="checkbox"/>	DHL	10/01/2022 2:09 AM	10/01/2022 2:09 AM	10/01/2022 2:10 AM	10/01/2022 2:11 AM	17/01/2022 2:11 AM	completed
<input type="checkbox"/>	dropbox	10/01/2022 2:09 AM	10/01/2022 2:09 AM	10/01/2022 2:09 AM	10/01/2022 2:10 AM	17/01/2022 2:10 AM	completed

4. Click *OK*.

The confirmation dialog box contains the following text: "You have selected 4 campaigns. Do you want to delete these campaigns?" Below the text are two buttons: "Cancel" and "OK".

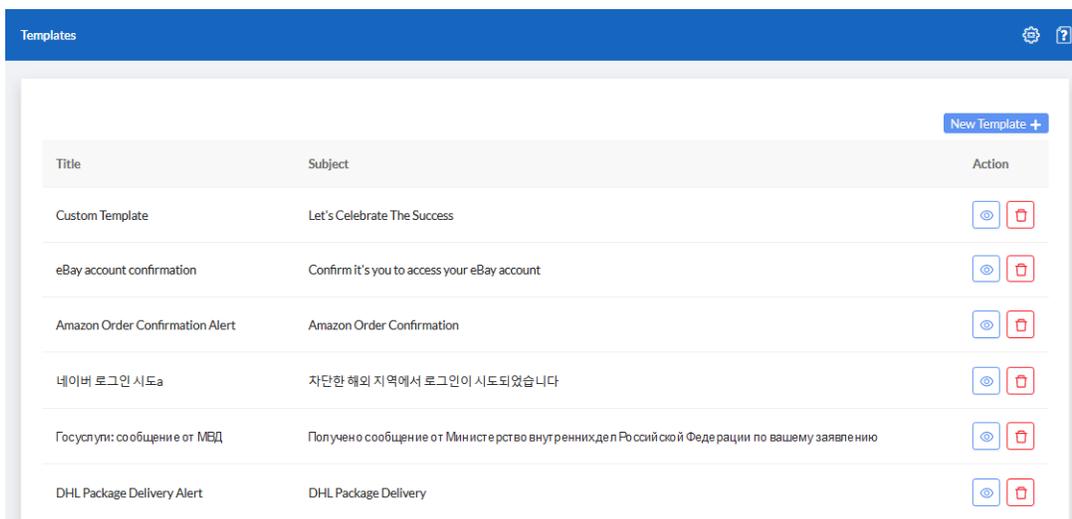
# Custom

Use the pages in *Custom* view to create custom landing pages and templates for your account.



# Templates

The *Templates* page displays the custom templates created for your account. After the template is created it will be available from the *Custom* tab when you launch a new campaign.



**To view a template** Click the **View icon** .

**To delete a template**Click the *Delete* icon .

## Creating custom templates



Custom templates are the property of Fortinet. Fortinet reserves the right to adapt any updates or revisions made to an existing email template and make them available to all users in the *Global Templates* tab.

**To create a new campaign template:**

1. Go to *Custom > Templates*.
2. Click *New Template*. The *Create Custom Template* dialog opens.
3. Configure the template settings.

<b>Title</b>	Enter a title for the template.
<b>Subject</b>	Enter the email subject.
<b>Sender Name</b>	Enter the sender's name.
<b>Sender Email</b>	Enter the sender's email address.
<b>Clicking Behavior</b>	<i>Landing Page &gt; Custom</i> is selected by default. Select the landing page from the dropdown. For information about custom landing pages, see <a href="#">Landing page on page 57</a> .
<b>Redirect URL</b>	Enter the redirect URL.
<b>Use Attachment</b>	Click <i>Yes, Using Filename</i> and enter the filename in the text field.
<b>Track User Reply</b>	Click <i>Yes</i> to create targeted emails that have no click or attachments but will simulate an actual spear-phish and allow you to see which users respond and/or attach compromising information.

4. In the text editor, compose the email body.

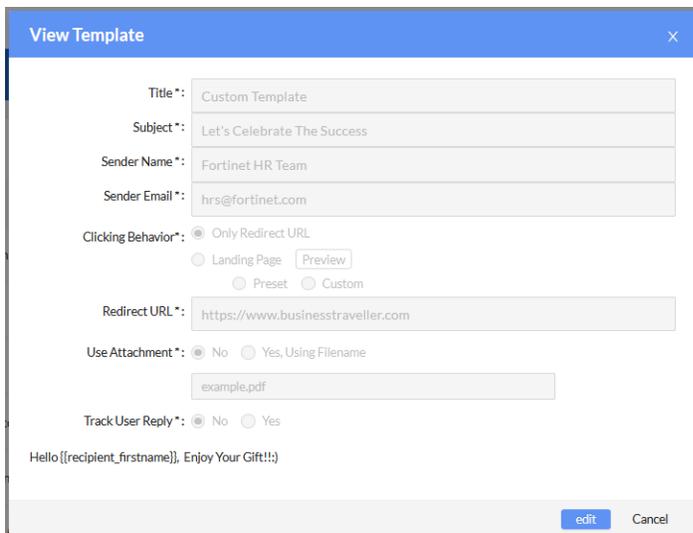


You can use variables in the email body to generate dynamic data while the campaign is running. See, [Template variables on page 42](#).

5. Click *Submit*. The template is added to the *Custom* tab in the *Campaigns* module. See, [Creating campaigns on page 39](#).

**To edit a template:**

1. Click the *View* icon . The *View Template* dialog opens.
2. Scroll to the bottom of the dialog and click *Edit*.



3. Update the template and click *Submit*.

## Landing page

You can create a custom landing page with the text editor or by uploading a Zip file. Custom landing pages support variables to create more convincing campaigns.

Custom landing pages appear in the *Clicking Behavior* section of the campaign wizard for both global and custom templates. See [Creating campaigns on page 39](#).

Clicking Behavior

Only Redirect URL  
 Landing Page Preview  
 Preset  Custom ▼  
 Redirect URL

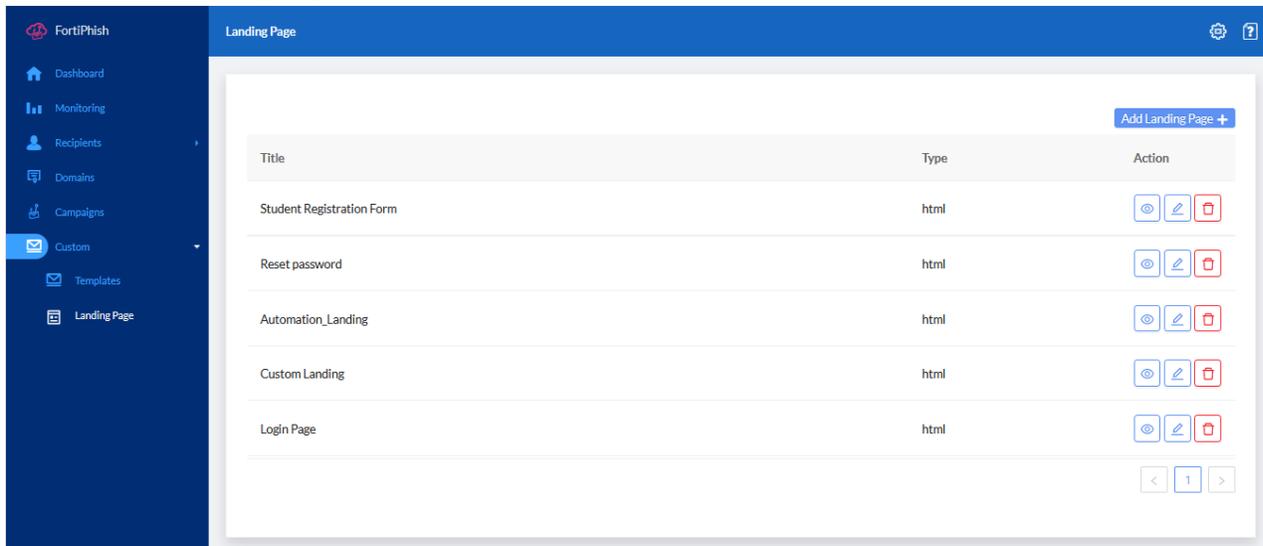


FortiPhish does not save the data entered by the user in the landing page.

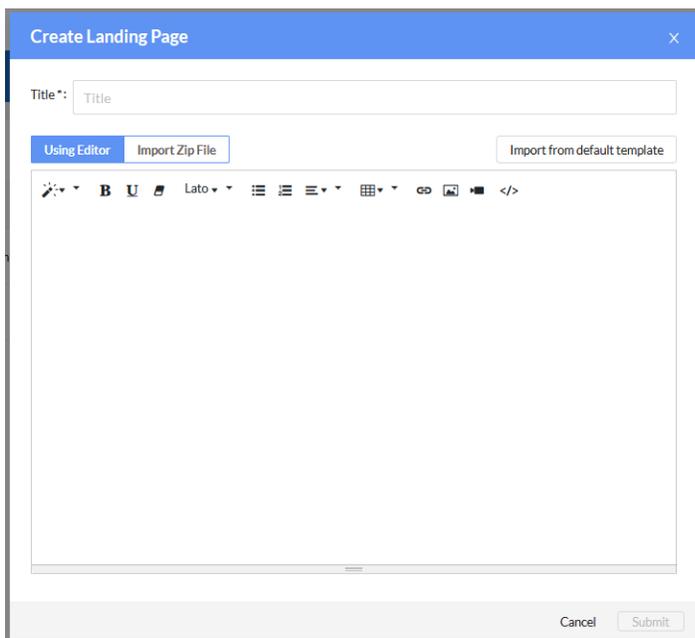
## Creating custom landing pages with the editor

To create a custom landing page with the editor:

1. Go to *Custom > Landing Page*.



2. Click *Add Landing Page*. The Landing Page editor opens.



3. In the *Title* field, enter a name for the landing page.
4. In the text editor, compose the body of the landing page. See [Landing page variables on page 60](#).
5. Click *Submit*. The new page is added to the *Landing Page* view in the navigation menu.

## Creating a custom landing page with a Zip file

### Requirements:

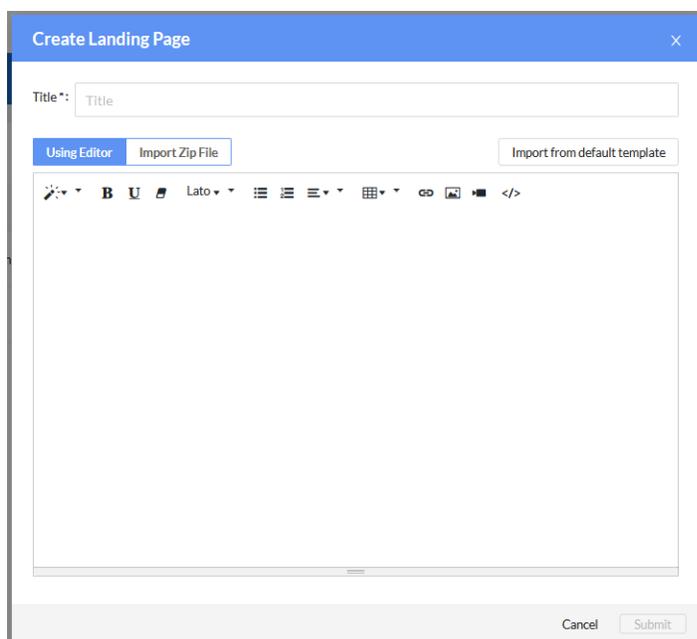
The Zip file should contain an `index.html` file that must include the following:

- A hidden tag with dynamic value used to track the recipient: `<input name="recp_uuid" type="hidden" value="{{.recp_uuid}}">`
- A submit form action with dynamic value set to `"{{.submit_url}}"`

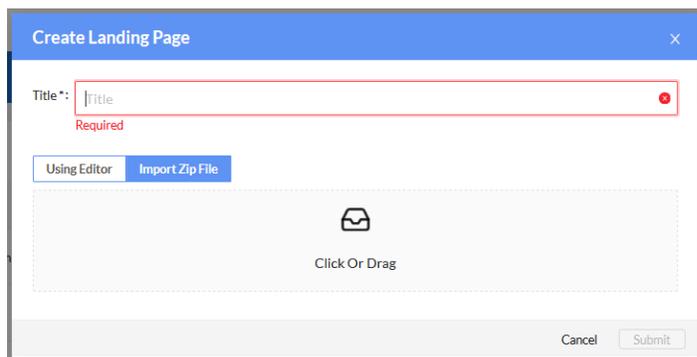
This is required for redirection of the recipient from landing page to configured redirect URL.

### To create a custom landing page with a Zip file:

1. Go to *Custom > Landing page*.
2. Click *Add Landing Page*. The Landing Page editor opens.



3. In the *Title* field, enter a name for the landing page.
4. Click *Import Zip File*.
5. Click the upload icon to navigate to the Zip file on your computer. Alternatively, you can drag the file onto the field.



6. Click *Submit*. The landing page is imported and added to the Landing Page list.

## Landing page variables

You can add variables to the landing page to generate dynamic data when the campaign is running.

### Supported variables for custom landing pages:

Variable	Syntax
submit url	{{.submit_url}}
email	{{.recipient_email}}
username	{{.email_username}}
domain	{{.email_domain}}
fname	{{.recipient_firstname}}
lname	{{.recipient_lastname}}
position	{{.recipient_position}}
date	{{.date}}
time	{{.time}}

# Settings

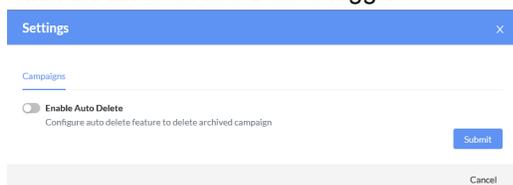
Use the Settings page to automatically delete archived campaigns, create alert buttons, and add SMTP server accounts.

## Enable Auto Delete

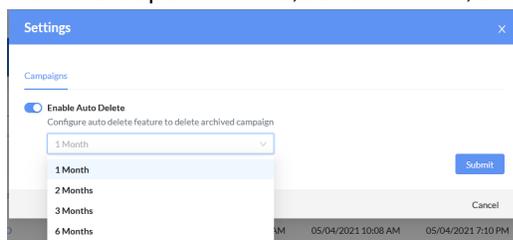
Schedule archived campaigns to be automatically deleted at monthly intervals.

### To enable auto delete:

1. In the banner, click the gear icon.
2. Click the *Enable Auto Delete* toggle.



3. From the dropdown menu, select *1 Month*, *2 Months*, *3 Months*, or *6 Months*.



4. Click *Submit*.

## FortiPhish alert buttons

FortiPhish Alert Buttons (PAB) allow email recipients to report suspicious email, regardless of whether the email is simulated. Use alert buttons to engage users in your security strategy and to be alerted of legitimate phishing threats.

Alert buttons can be manually installed as add-ons in Outlook and Thunderbird email clients. After a user reports a suspicious email, the response is recorded in the *Monitoring* and *Campaigns* statistics.

### To enable FortiPhish alert buttons:

1. [Create a FortiPhish alert button.](#)
2. Manually install the button on Outlook or Thunderbird. See [FortiPhish alert button compatibility matrix on page 71](#).
  - [Adding alert buttons in Outlook on page 64](#)
  - [Adding alert buttons in Thunderbird on page 68](#)

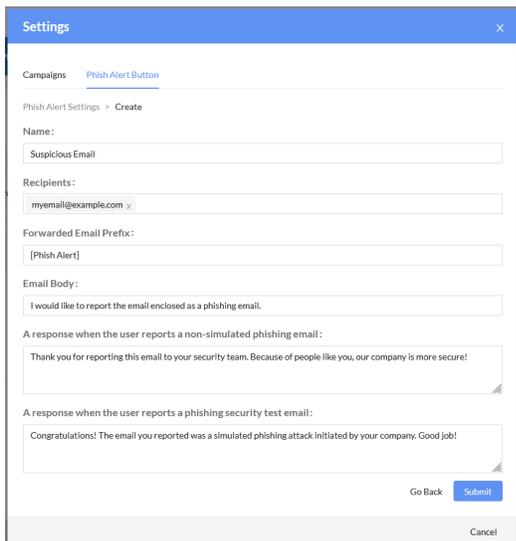
## Creating a FortiPhish alert button

The FortiPhish Alert Button (PAB) template is located in the *Settings* menu. To create a button, determine who will receive alert notification, and compose alert messages. After button is created, download the PAB installation file to your device and upload the the button in Outlook or Thunderbird.

### To create a FortiPhish alert button:

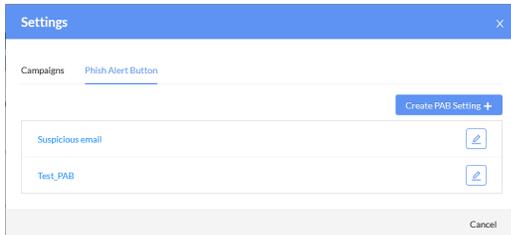
1. In the menu bar, click the *Settings* icon . The *Settings* window opens.
2. Click the *Phish Alert Button* tab.
3. Click *Create PAB Setting +* to configure the alert button settings, and then click *Submit*.

Setting	Description
<b>Name</b>	The alert button name.
<b>Recipients</b>	Enter the email address of the admins to be notified when an email is reported.
<b>Forwarded Email Prefix</b>	The prefix that appears before the subject of the suspicious email.
<b>Email Body</b>	The email message body recipients send to report a suspicious email.
<b>A response when the user reports a non-simulated phishing email</b>	The email message body recipients see when they report a non-simulated email.
<b>A response when the user reports a phishing security test email</b>	The email message body recipients see when they report a simulated email.

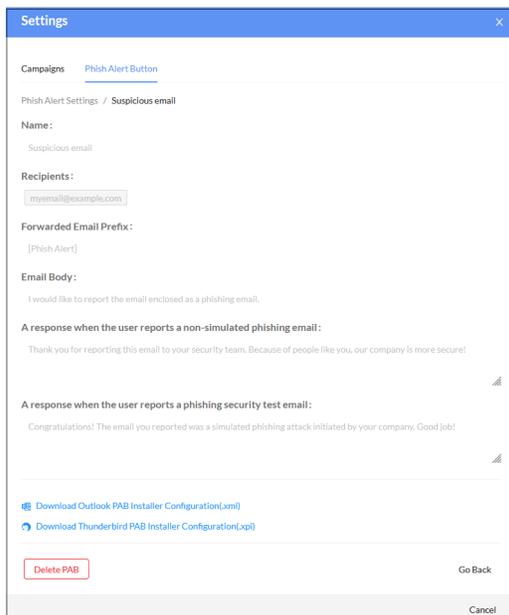


### To download the PAB installation file:

1. In the menu bar, click the *Settings* icon . The *Settings* window opens.
2. Click the *Phish Alert Button* tab.
3. Click the alert button name. The *Settings* window opens.



4. Scroll down to the bottom of the page and select one of the following file formats.
  - *Download Outlook PAB Install Installer Configuration(.xml)*
  - *Download Thunderbird PAB Installer Configuration(.xpi)*



5. Save the file to your device.

### To edit an alert button:

1. In the menu bar, click the *Settings* icon . The *Settings* window opens.
2. Click the *Phish Alert Button* tab.
3. Click the Edit icon  next to the alert button name .
4. Update the message and click *Save*.

### To delete an alert button:

1. Click the *Phish Alert Button* tab.
2. Click alert button name. The *Settings* window opens.

3. Scroll to the bottom of the page and click *Delete PAB*. A confirmation dialog opens.
4. Click Yes.

## Adding alert buttons in Outlook

After the alert button is created, download the installation file to your device. To add the button to Outlook, open the *Add-ins* menu and upload the installation file as a custom add-in.

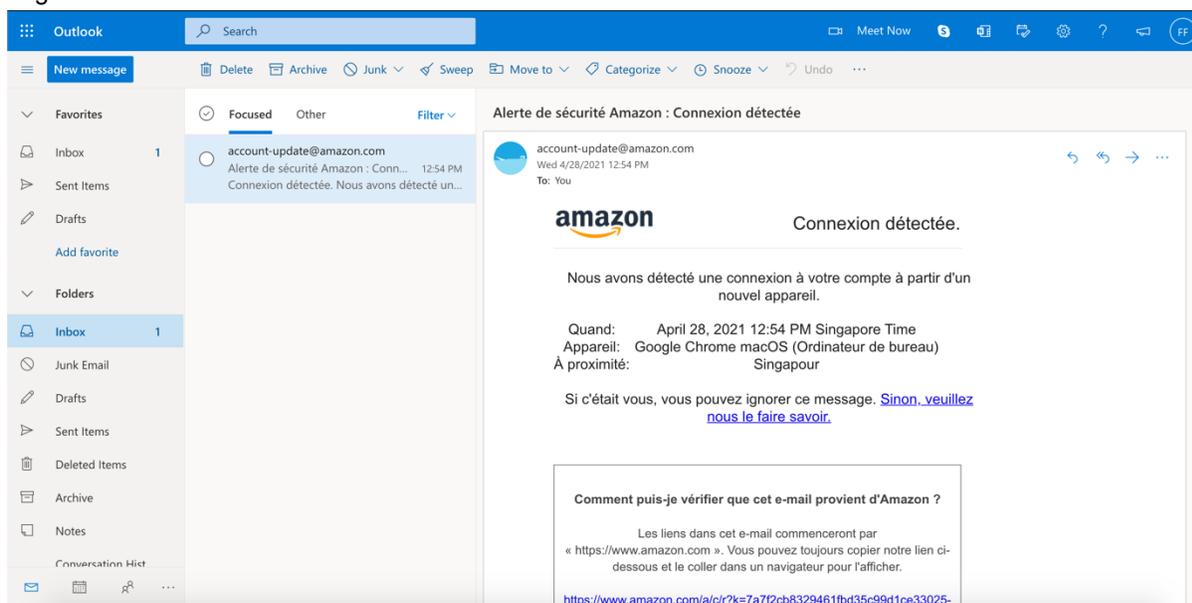


This process requires Read/Write Mailbox permissions for your email client.

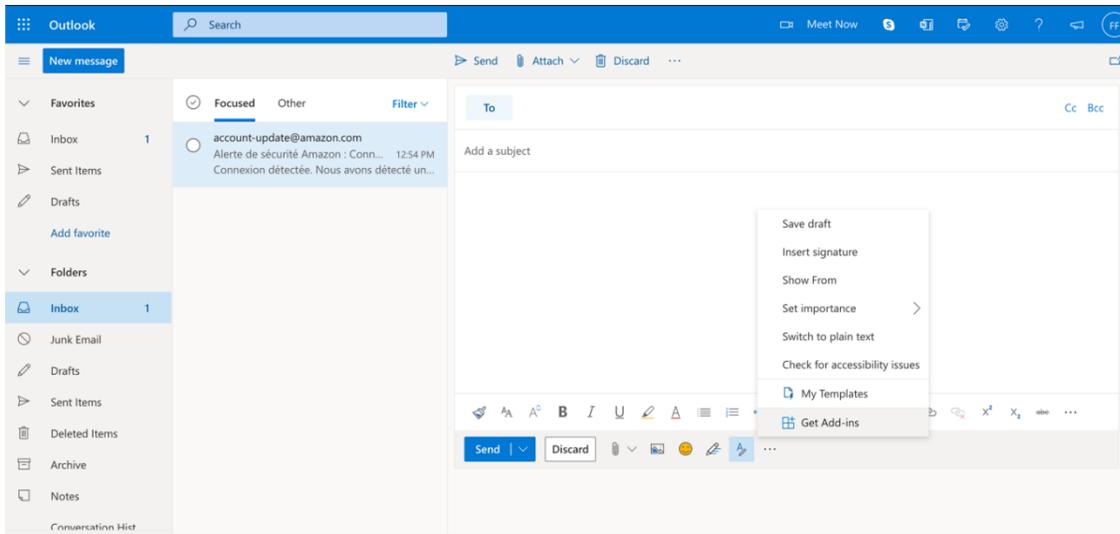
The images for the following task are based on Outlook for Office 365 online. The user interface may look different than the one you are using. For more information, please refer to the product documentation.

### To install the Outlook add-in:

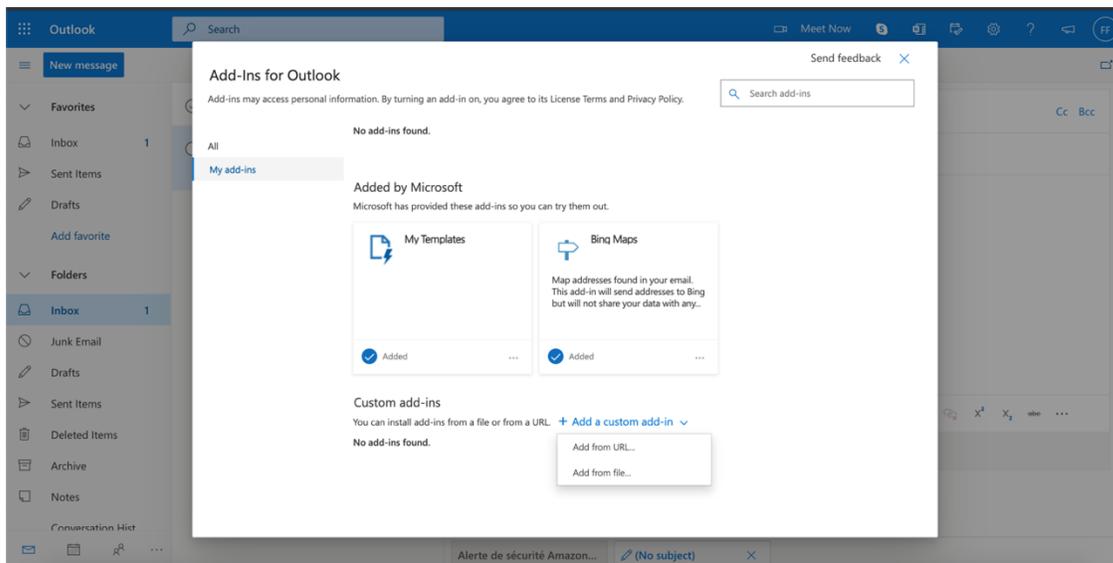
1. Login to Outlook.



2. Create a new Outlook message.
3. Click the ellipses (...) at the bottom of the message, and select *Get Add-ins* from the menu. The *Add-Ins for Outlook* dialog opens.

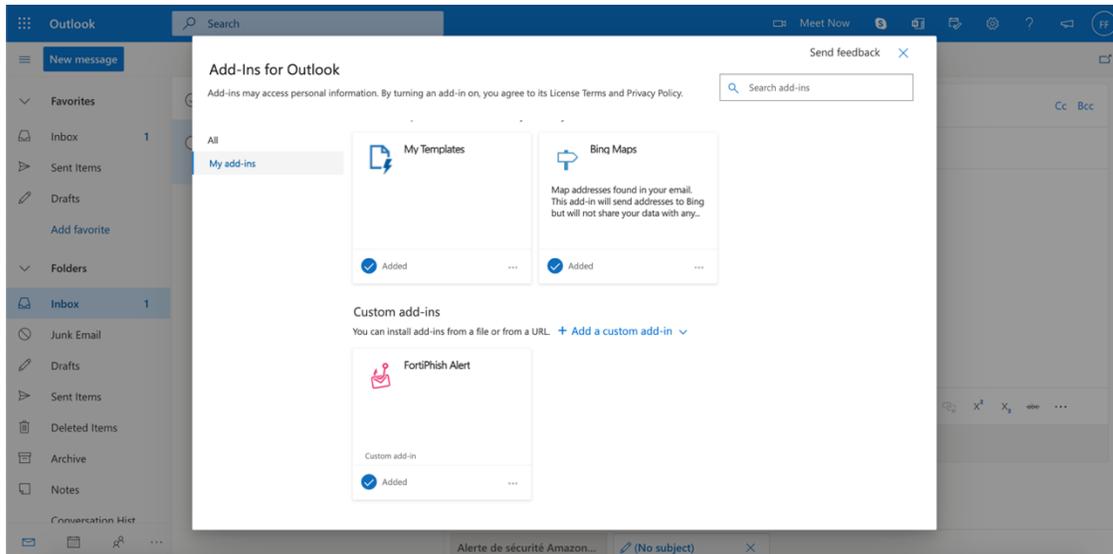


4. Install the FortiPhish alert button.
  - a. Click *My add-ins*.
  - b. In the *Custom add-ins* section, click *Add a custom add-in link > Add from file*.



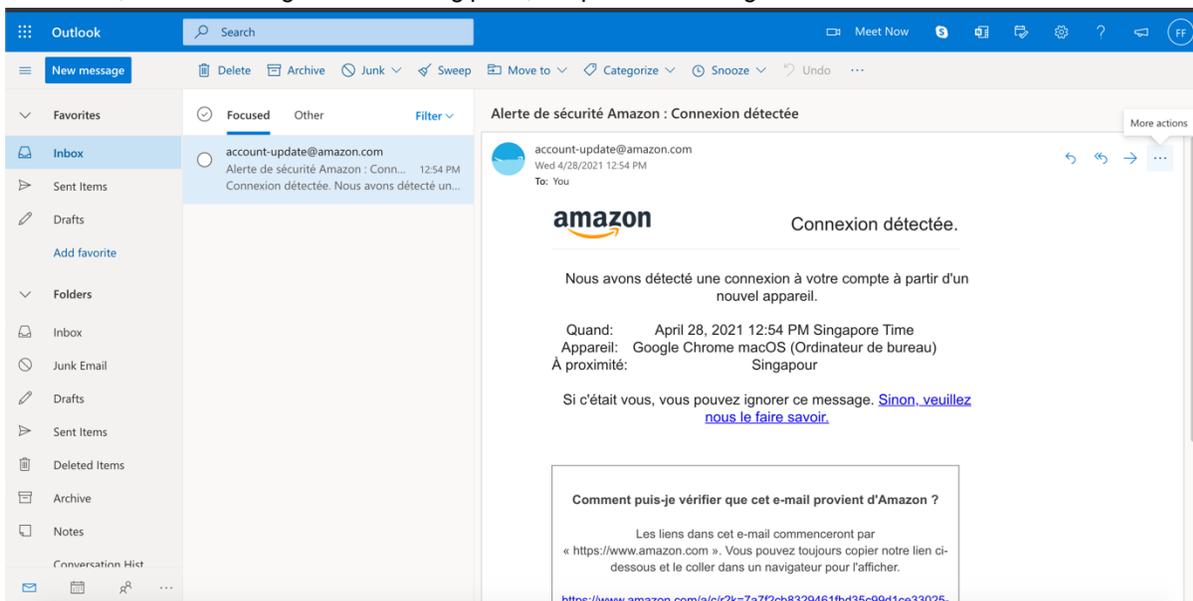
- c. Locate the installation file you downloaded and click *Open*. A *Warning* message appears.

- d. Click *Install*. The *FortiPhish Alert* tile is added to the *Custom add-ins* menu. Close the window.

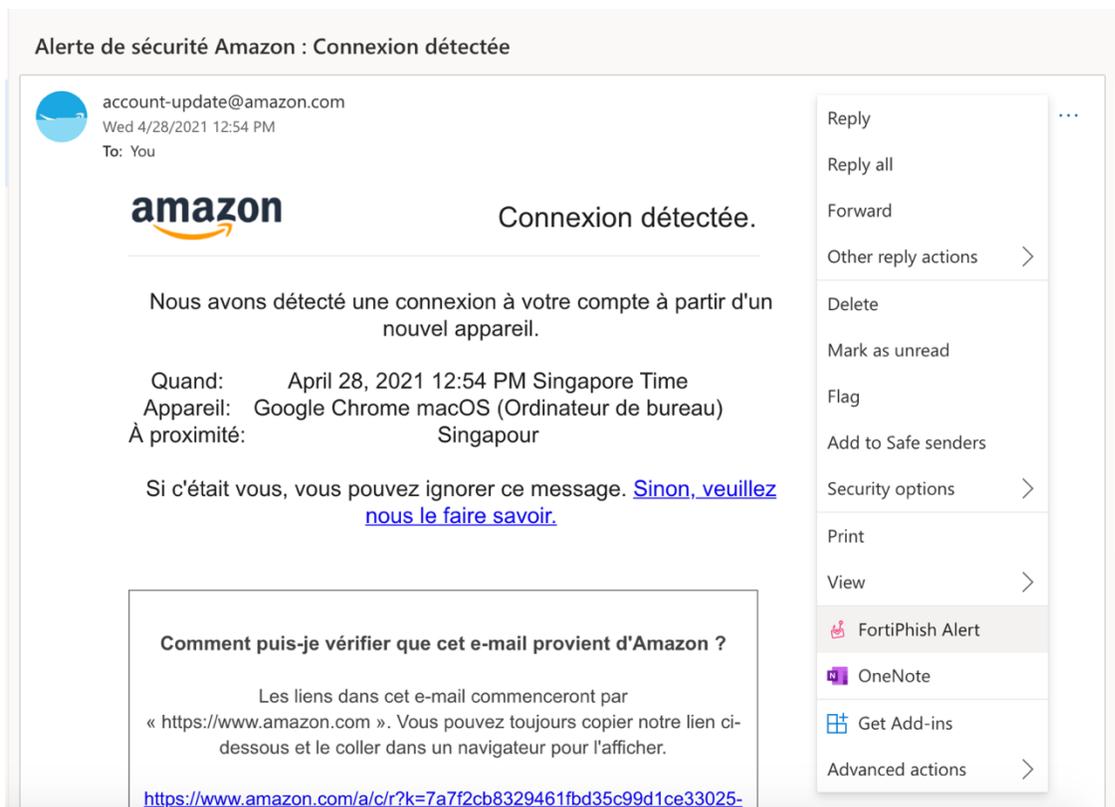


### To test the FortiPhish alert button:

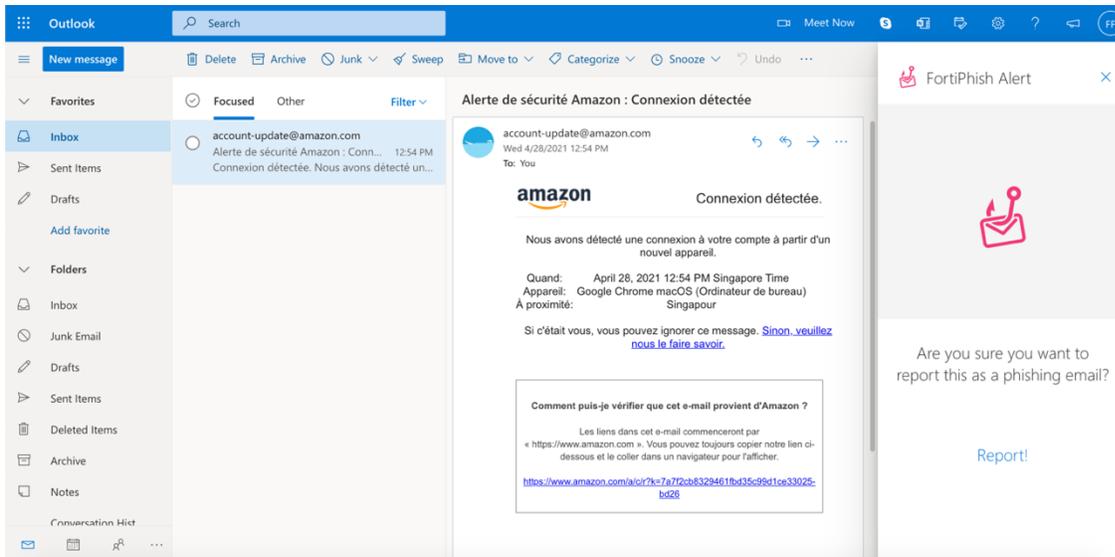
1. In Outlook, view a message in the reading pane, or open the message in a new window.



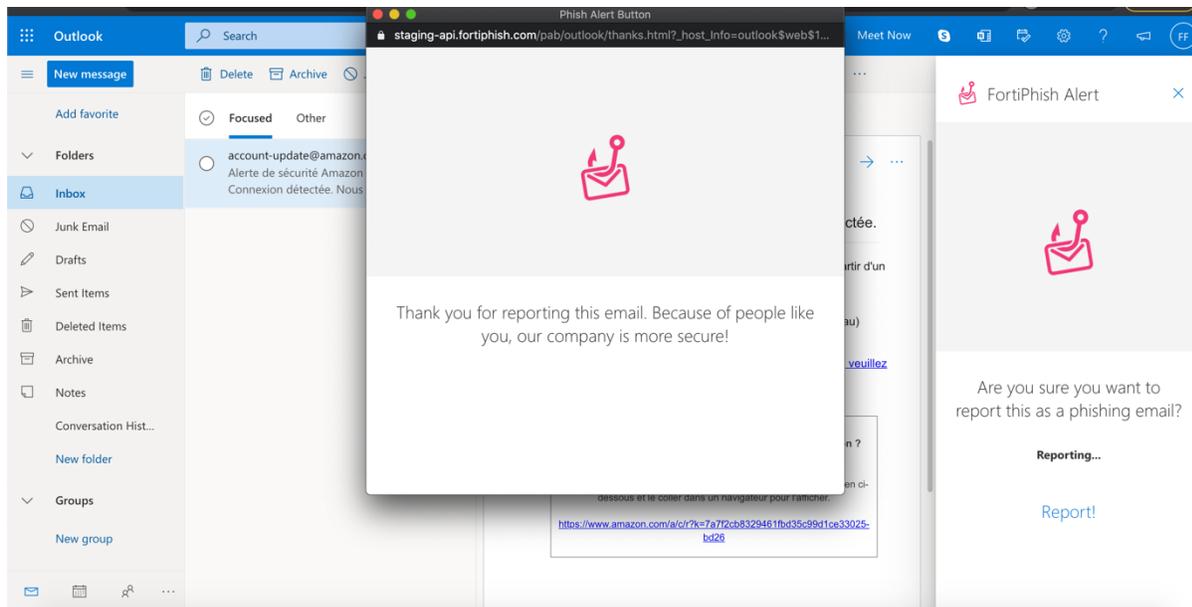
2. Click the ellipses (...) at the top-right corner of the message, and click the *FortiPhish Alert*. The *PAB add-in* task pane opens.



3. Click the *Report* link to report the message. The message is reported and moved to the *Deleted* folder.



A custom message is displayed.



## Adding alert buttons in Thunderbird

After the alert button is created, download the installation file to your device. To add the button to Thunderbird, open the *Extensions and Themes* settings and upload the installation file as a custom plug-in.

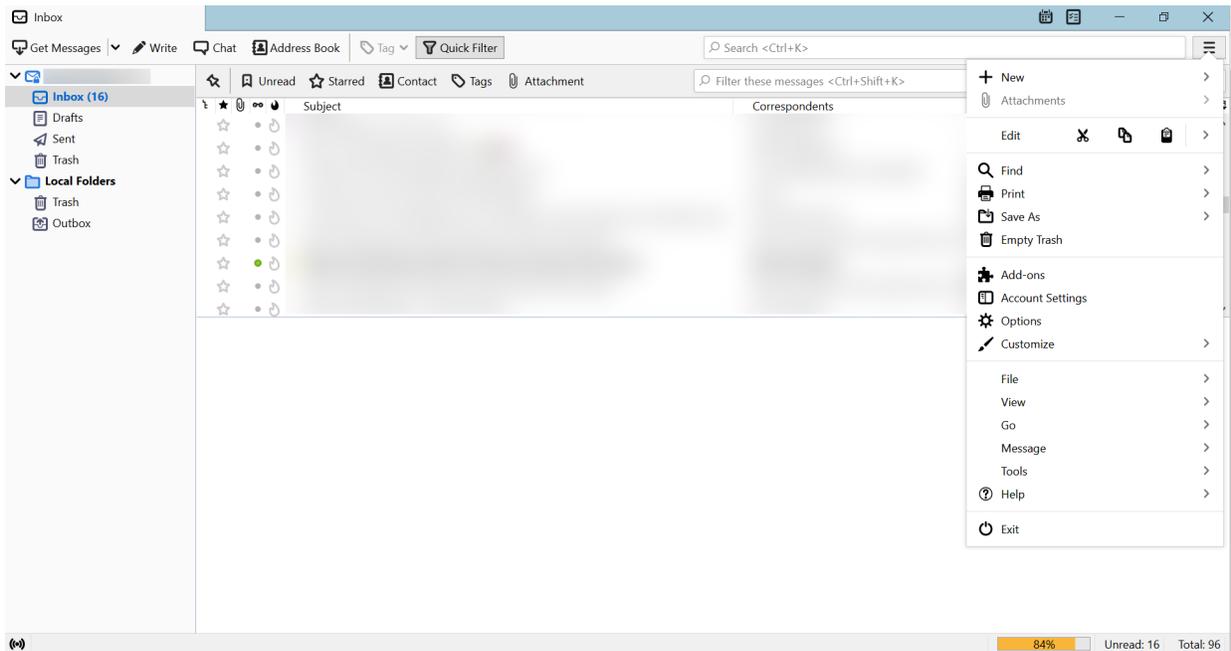


This process requires Read/Write Mailbox permissions for your email client.

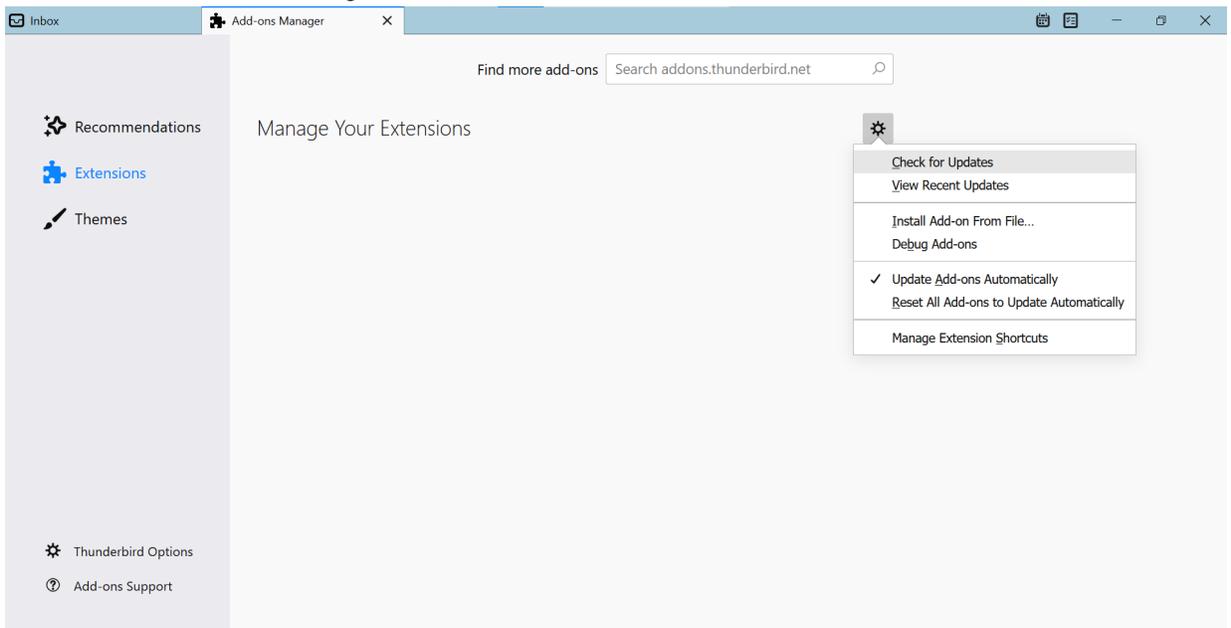
The images in the following task are based on Thunderbird for desktop v 78.12.0. The user interface may look different than the one you are using. For more information, please refer to the product documentation.

## To install the FortiPhish alert button:

1. In Thunderbird, click the Thunderbird menu and select *Add-Ons*.

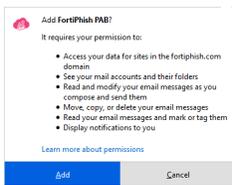


2. In the *Extensions* tab, click the gear icon, and click *Install Add-on From File....*

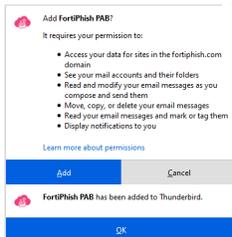


3. Navigate to the location of the *xpi* file on your device and click *Open*. The *Add FortiPhish PAB* confirmation dialog opens.

- Click **Add**. A confirmation message appears.

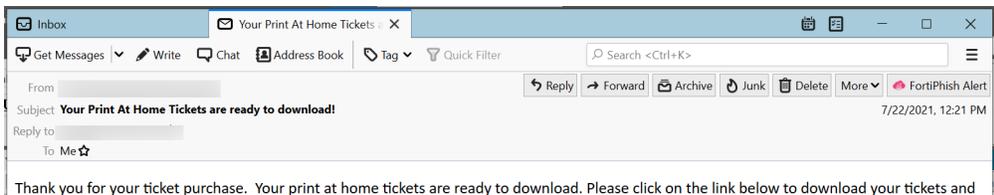


- Click **OK** and click **Add** to close the dialog.

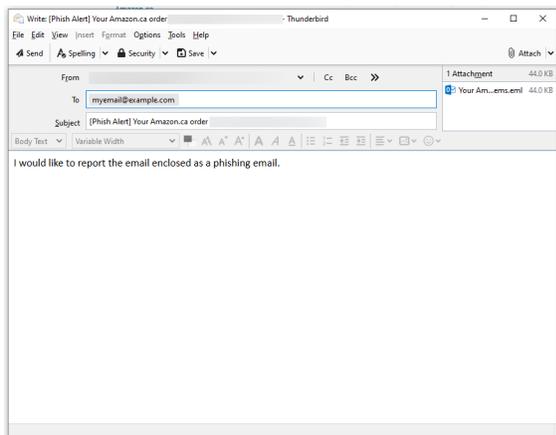


**To test the alert button:**

- In Thunderbird, go to your *Inbox* and open a message. The *Phish Alert* action button appears next to the existing buttons.



- Click the *Phish Alert* button to open the composer. The suspicious email is attached as an EML file.



Thunderbird email recipients can edit the email message body.

- Click **Send** to report the email as a phishing email. The original email is automatically moved to the *Trash* folder.



## FortiPhish alert button compatibility matrix

FortiPhish Alert Buttons are compatible with Outlook and Thunderbird email clients.

Microsoft 365					
<b>Microsoft Windows</b>	Outlook 2016	Compatible			
	Outlook 2019	Compatible			
	OWA/Outlook Online	Compatible			
<b>Apple OSX</b>	Outlook 2016	Compatible			
	Outlook 2019	Compatible			
	OWA/Outlook Online	Compatible			
<b>Android</b>	Outlook mobile app	Compatible			
<b>IOS</b>	Outlook mobile app	Compatible			

Exchange (Server based)					
		Exchange Version			
		2013	2016	2019	Microsoft 365
<b>Microsoft Windows</b>	Outlook 2013	Compatible	Compatible	Compatible	Compatible
	Outlook 2016	Compatible	Compatible	Compatible	Compatible
	Outlook 2019			Compatible	Compatible
<b>Apple OSX</b>		Compatible	Compatible		Compatible (until version 16.23)

Outlook (Client based)		
<b>Microsoft Windows</b>	Outlook 2010	Compatible
	Outlook 2013	Compatible
	Outlook 2016	Compatible
	Outlook 2019	Compatible

Thunderbird	
Thunderbird Client (version >=78)	Compatible
For Thunderbird release, see <a href="https://www.thunderbird.net/en-US/thunderbird/releases">https://www.thunderbird.net/en-US/thunderbird/releases</a>	

## SMTP

Use your organization's SMTP servers to distribute campaign phishing emails to your employees.

### To add a SMTP server to FortiPhish:

1. In the banner, click the gear icon.
2. Click *Add Account*.
3. Configure the SMTP settings. All settings are required.

<b>Name</b>	Enter the mail server name.
<b>Username</b>	Enter the username to be used to authenticate with SMTP server.
<b>Password</b>	Enter the password to be used to authenticate with SMTP server.
<b>Domain Name</b>	Enter the address of the SMTP server to be used to send outgoing emails. The address can be in the form of IP address or domain name
<b>Port</b>	Enter the port number used by SMTP server to send emails.
<b>Security</b>	Select the method to encrypt the email traffic between the email client and the SMTP server: <i>SSL, TLS</i> or <i>STARTTLS (Opportunistic)</i> .
<b>Protocol</b>	Select the method to authenticate the user with the SMTP server: <i>LOGIN, PLAIN</i> and <i>CRAM-MD5</i> .

4. Click *Save*.

