Administration Guide

FortiPhish 24.1.0

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

March 14, 2024
FortiPhish 24.1.0 Administration Guide
60-241-1009217-20240314

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-03-14	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 24.1.0

This release includes the following new features and enhancements.

Campaigns

- You can now set the time delay to skip email scanner events in *Settings* > *Campaigns* page.
- You can now include phishing link as *QR Code* in campaign emails.
- You can now select multiple verified domains to be used for campaign links.

Recipients

- A new *Users* allows you to manage all the recipients of FortiPhish.
- A new *Users Profile* page provides detailed user statistics.
- Added functionality to bulk delete users in a group.

Phish Alert Button (PAB)

- Outlook and Thunder bird plugins have been updated. Download the latest version of PABs and re-deploy them.

UI Enhancements

- Added support for pagination, filters, and sorters in multiple pages.

FortiPhish portal

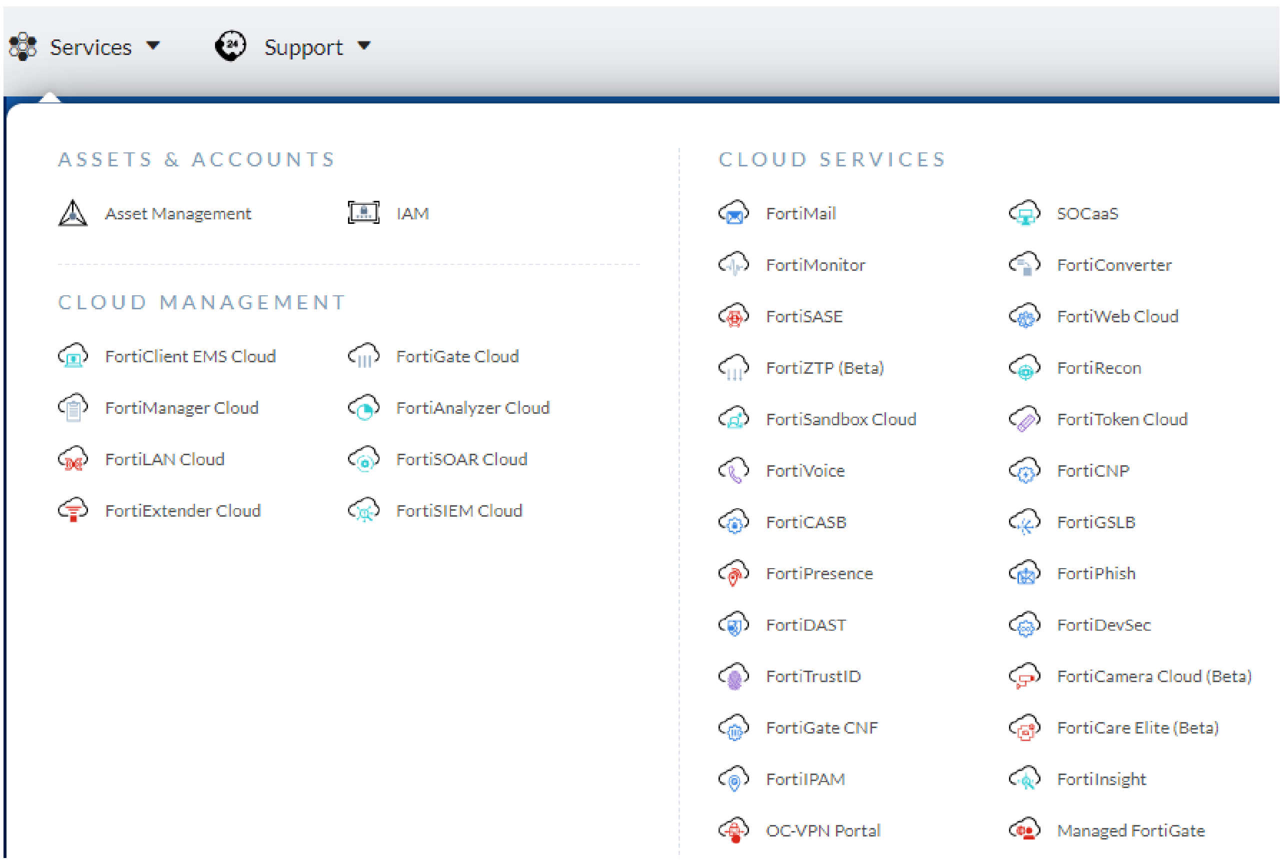
Use the FortiPhish portal to generate DNS tokens, create users and groups, and launch and monitor email campaigns.

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

Accessing the FortiPhish portal

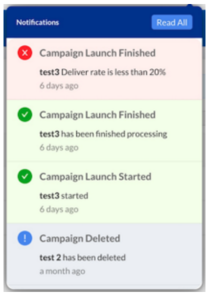
To access the FortiPhish portal:

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
Admin	Read/Write access to all user records under the same account, excluding domain records.
Read/Write	Read /Write access to user's own records.
Read Only	Read access to master user records under the same account.

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.

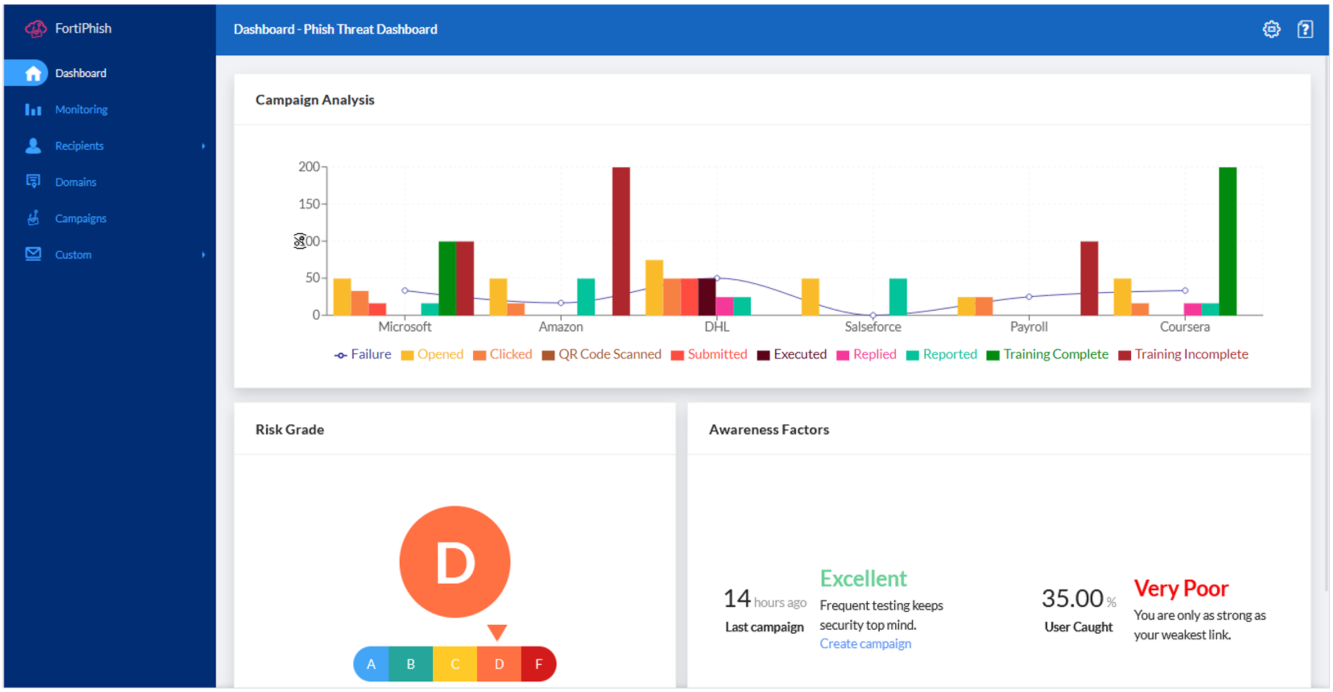
To send phishing simulation emails, you must disable the DMARC/DKIM policy, as it will cause an error while attempting to send them. Alternatively, you can make slight modifications to the domain name, such as changing a letter, for example, use *apple.con* or *amaz0n.com* instead of *apple.com* or *amazon.com*, 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] [DB8EUR06FT006.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.



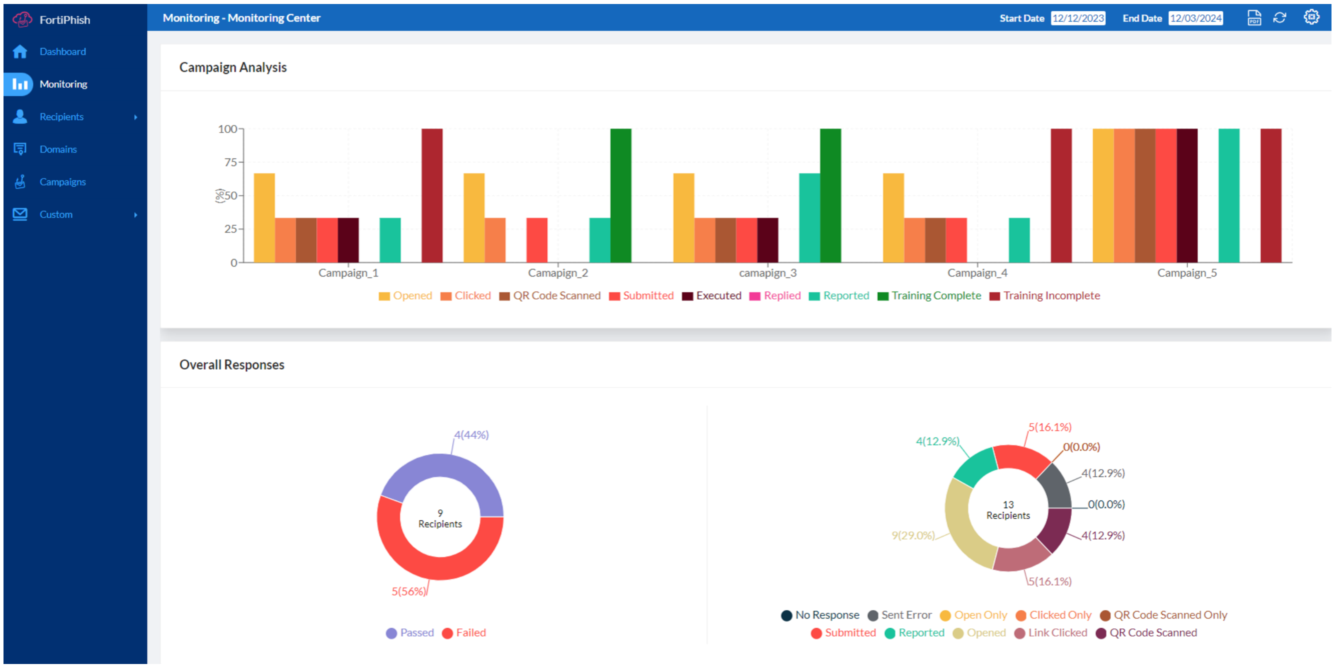
The *Dashboard* displays the following monitors:

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

<table>
<tr><th>Monitor</th><th>Description</th></tr>
<tr><td></td><td><table>
<tr><td></td><td>FortiPhish will not be able to collect the Executed metric when the attached PDF is previewed in a reader that disables links for security purposes.</td></tr>
<tr><td>Replied</td><td>The number of recipients who replied to the email.</td></tr>
<tr><td>Reported</td><td>The number of recipients who reported the phishing email as suspicious.</td></tr>
<tr><td>Training Complete</td><td>The number of recipients who have finished the training.</td></tr>
<tr><td>Training Incomplete</td><td>The number of recipients who have been enrolled but did not finish the training.</td></tr>
</table></td></tr>
<tr><td>Risk Grade</td><td>The letter grade between A and F assigned to the organization. An A indicates the user poses minimal risk and a F grade indicates the user poses the maximum risk to the organization.
If the campaign is active, then the Risk Grade will be NA on the Dashboard and Monitoring pages.</td></tr>
<tr><td>Awareness Factors</td><td>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 Create a Campaign link. See Creating campaigns on page 45.</td></tr>
</table>

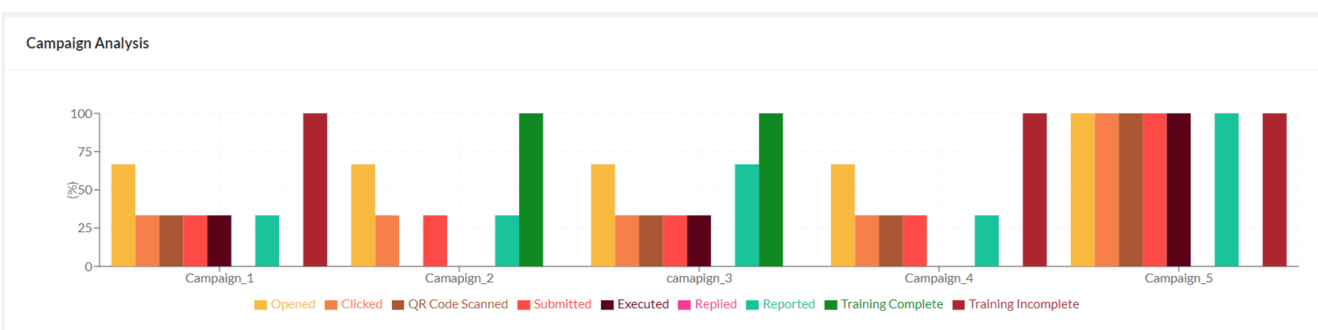
Monitoring

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.

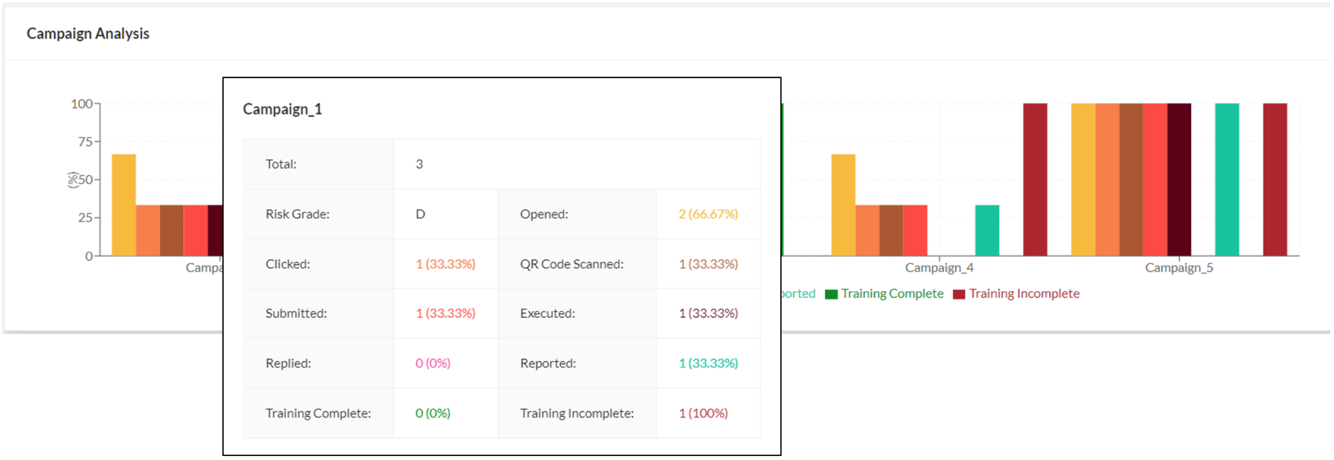


Campaign Analysis

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.

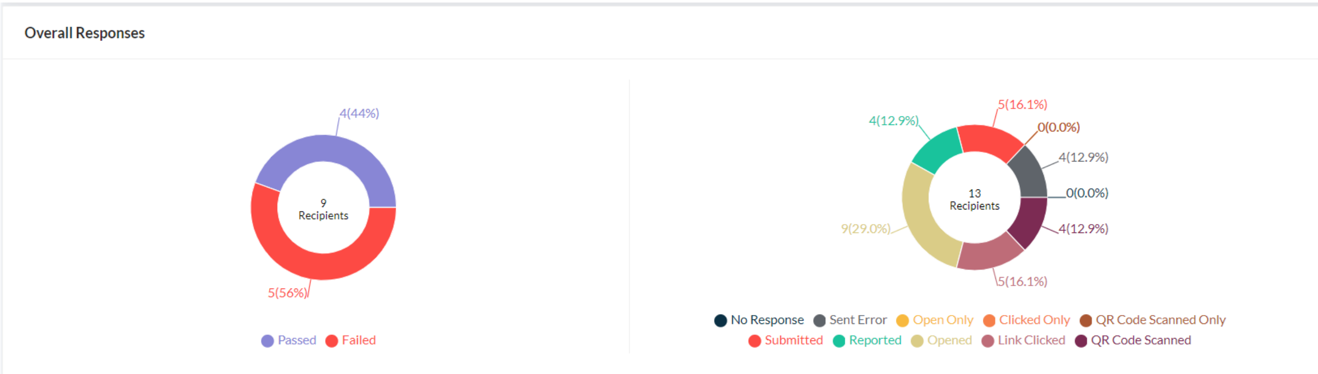


The chart displays the following information:

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

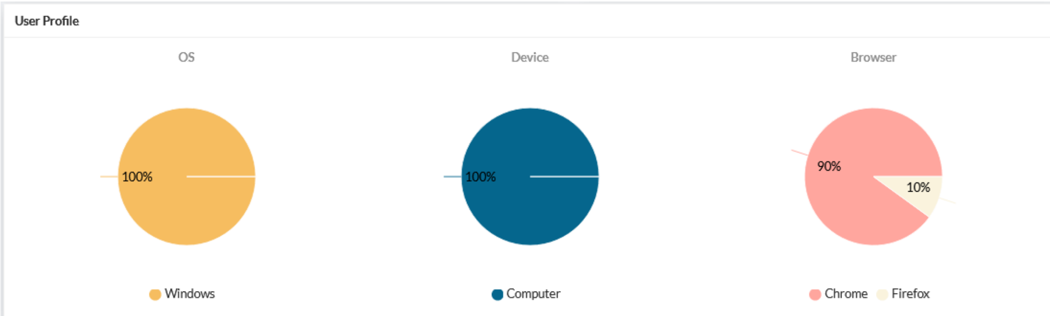


The *Overall Responses* monitor displays the following information:

Passed	The percentage of recipients that did not click or respond to campaign emails. This includes emails that were opened or opened and reported.
Failed	The percentage of recipients that clicked or responded to campaign emails.
No Response	The number of emails that were not opened.
Sent Error	The number of emails that bounced.
Open Only	The number of recipients who opened the mail, but did not perform any other action.
Opened	The number of recipients who opened the mail.
Clicked Only	The number of recipients who clicked the redirect link, but did not perform any other action.
QR Code Scanned	The number of recipients who scanned the QR code.
QR Code Scanned Only	The number of recipients who scanned the QR code, but did not perform any other action.
Link Clicked	The number of recipients who clicked the redirect link.
Submitted	The number of recipients who entered information on the landing page.
Reported	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.

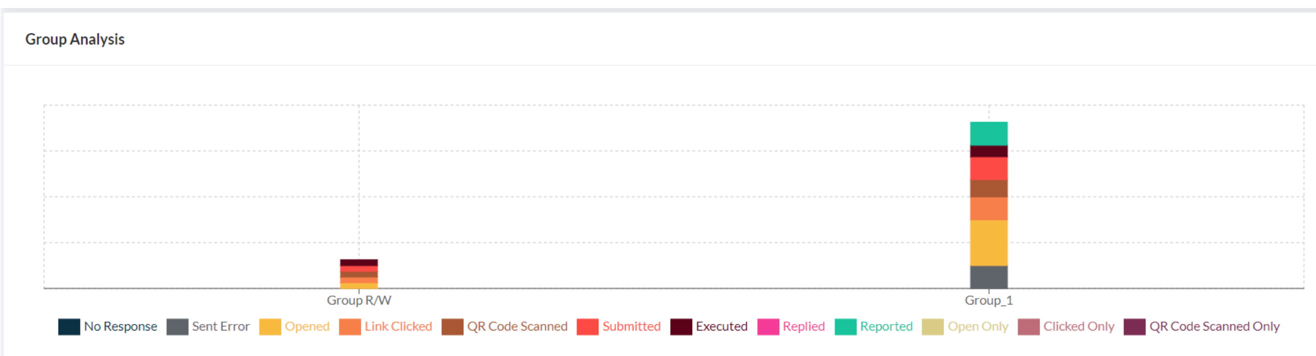


The *User Profile* monitor displays the followling information:

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

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.



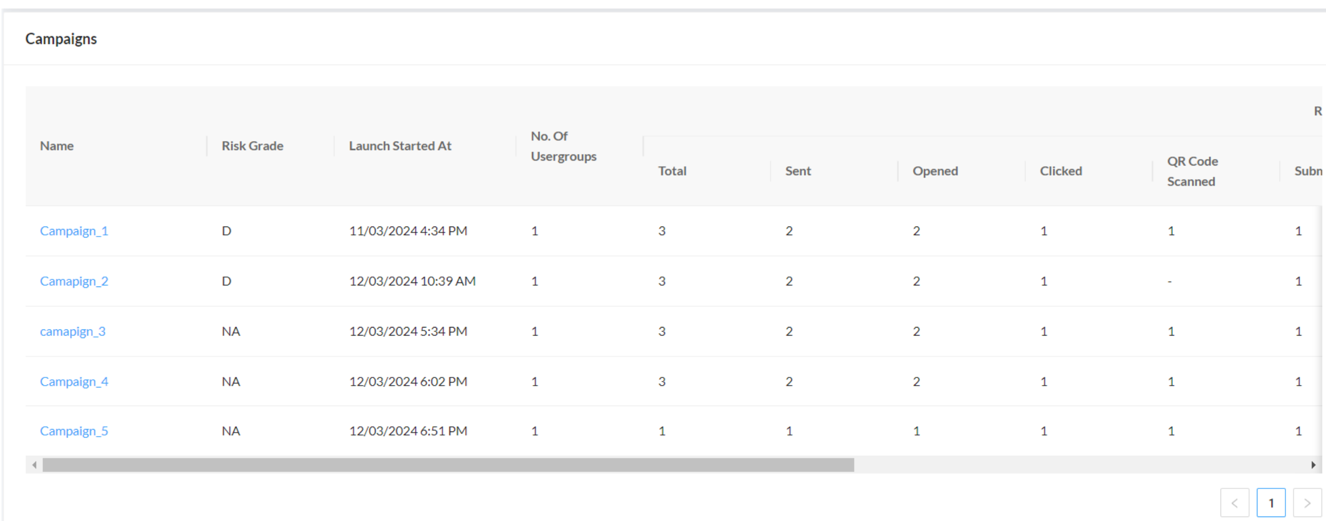
The *Group Analysis* monitor displays the following information:

No Response	The number of emails that were not opened.
Sent Error	The number of emails that bounced.
Opened	The number of recipients who opened the email.
Link Clicked	The number of recipients who clicked the redirect link.
QR Code Scanned	The number of recipients who scanned the QR code.
Submitted	The number of recipients who entered information on the landing page.
Executed	The number of recipients who opened or executed the file attached in the phishing email.

	FortiPhish will not be able to collect the *Executed* metric when the attached PDF is previewed in a reader that disables links for security purposes.
Replied	The number of recipients who replied to the email.
Reported	The number of recipients who reported the phishing email as suspicious.
Open Only	The number of recipients who opened the mail, but did not perform any other action.
Clicked Only	The number of recipients who clicked the redirect link, but did not perform any other action.
QR Code Scanned Only	The number of recipients who scanned the QR code, but did not perform any other action.

Campaigns

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



The *Campaigns List* monitor displays the following information:

Risk Grade	The letter grade between *A and F* assigned to the campaign. An *A* indicates the user poses minimal risk and a *F* grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be *NA* on the *Dashboard* and *Monitoring* pages.
Launch Started At	The timestamp when the campaign started.
No. Of Usergroups	The total number of user groups added to the campaign.

Total	The total number of users in the campaign.
Sent	The number of emails sent to the user group.
Opened	The number of recipients who opened the email.
Clicked	The number of recipients who clicked the redirect link.
QR Code Scanned	The number of recipients who scanned the QR code.
Submitted	The number of recipients who entered information on the landing page. FortiPhish does not save the data entered by the user in the landing page.
Executed	The number of recipients who opened or executed the file attached in the phishing email.
Reported	The number of recipients who reported the phishing email as suspicious.
Replied	The number of recipients who replied to the email.
Training Complete	The number of recipients who have finished the training.
Training Incomplete	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
Account Company	Name of the company.	Fortinet Singapore
Account Email	Email of the account owner.	fortiphish@fortinet.com

Name	Description	Example
Date Range	*Start Date* and *End Date* in `DD-MM-YYYY` format.	12-08-2021 - 12-11-2021
Date of Report	Date of the report with Location.	Fri, 12 Nov 2021 04:45:38 am +0800

Overview

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

Target User Measurements

Recipient Analysis

Name	Description	Example
Total Recipients targeted for phishing	The number of unique emails (recipients or targets) that were sent during the provided period.	5 Recipients

Name	Description	Example
	This number should be the same as the *# of Total recipients* in the *Overall* section.	
# of passed recipients overall	The number of *Passed* recipients divided by the number of *Sent* emails. This value excludes emails marked *Sent Error*, *Clicked* or *Submitted*.	2 Recipients(40%)
# of failed recipients overall	The number of *Failed* emails divided by the number of *Sent* emails.	2 Recipients(40%)

Email Analysis

Name	Description	Example
# of emails (phishing attempts) sent overall	The number of *Passed* recipients divided by the number of emails *Sent*.	2 Emails (50.0%)
# of emails passed overall	The number of *Passed* recipients divided by the number of emails *Sent*.	
# of emails failed overall	The number of *Failed* emails divided by the number of emails *Sent*.	2 Emails (50.0%)
# of emails "Opened"	The number of emails *Opened* divided by the number of emails *Sent*.	2 Emails (50.0%)
# of emails "Link Clicked"	The number of recipients who *Clicked* the redirect link divided by the number of emails *Sent*.	2 Emails (50.0%)
# of emails "QR Code Scanned"	The number of recipients who *scanned the QR code* divided by the number of emails *Sent*.	2 Emails (50.0%)
# of emails "Opened Only"	The number of recipients who *Opened* the mail but performed no other action, divided by the number of emails *Sent*.	2 Emails (50.0%)
# of emails "Link Clicked Only"	The number of recipients who *Clicked* the redirect link but performed no other action, divided by the number of emails *Sent*.	2 Emails (50.0%)
# of emails "QR Code Scanned Only"	The number of recipients who *scanned the QR code* but performed no other action, divided by the number of emails *Sent*.	2 Emails (50.0%)
# of emails "Submitted"	The number of emails *Submitted* divided by the number of emails *Sent*.	2 Emails (50.0%)
# of emails "Reported"	The number of emails *Reported* divided by the number of emails *Sent*.	2 Emails (50.0%)

Name	Description	Example
# of recipients training "Completed"	The number of recipients who completed the phishing training.	3
# of recipients training "Incomplete"	The number of recipients who did not complete the phishing training.	1
# total training "Completed"	The total number of trainings completed within the organization, including repeat trainings.	5

Overall Phish Percentage by Campaign

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

Overall Phish Percentage by Usergroup

Name	Description	Example
Name	Name of the user group.	
Failed Rate	*Failed Rate* with the difference between previous campaign.	100.0% (50%)
Reported Rate	*Reported Rate* with the difference between previous campaign.	0.0% (-50%)
Score	The *Reported Rate* minus the *Failed Rate*.	

Name	Description	Example
Risk Grade	The letter grade between *A and F* assigned to the group. An *A* indicates the user poses minimal risk and a *F* grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be *NA* on the *Dashboard* and *Monitoring* pages.	A

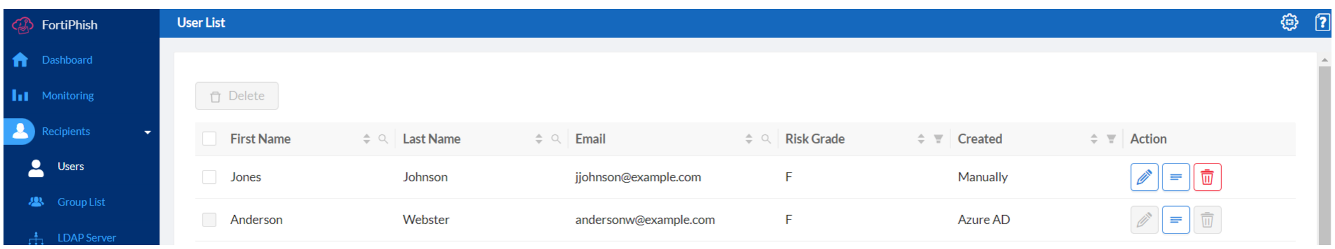
Recipients

Use the *Recipients* page to create group lists to distribute your campaigns and manage recipients. 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 and Azure AD server.

Users

The *Users* page displays all users added as recipients to FortiPhish. You can *edit, delete*, or *view* detailed information for each user.

- Users imported from Azure AD cannot be edited or deleted unless the Azure AD client is removed.
- When you edit the user details after Azure AD client is deleted, the *Created* field in *Recipients* > *Users* page will change from *Azure AD* to *Manually*.



To edit user details:

1. Navigate to *Recipients* > *Users*.
2. Click *Edit* icon next to the user you want to edit.
3. Update the user information and click *Submit*.

To delete a user:

1. Navigate to *Recipients* > *Users*.
2. Click *Delete* icon next to the user you want to delete.
3. In the confirmation pop up, click *Yes*.
4. To bulk delete users, select the users you want to delete and click *Delete* button on top.

Changes made to a user will also be reflected in any groups they belong to.

To view detailed user information:

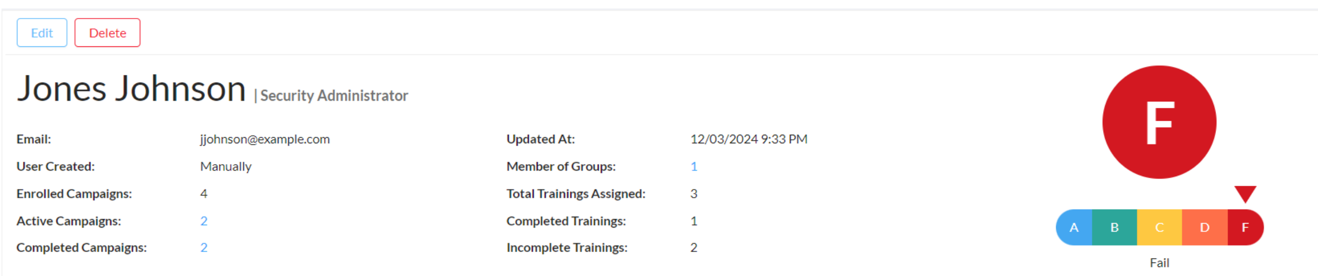
1. Navigate to *Recipients* > *Users*.
2. Click *View User* icon next to the user you want to view.
3. *User Profile* page is displayed. See User Profile.

User Profile

The *User Profile* page displays the detailed information of a user.

- User Information
- User Risk Grades
- Member of Groups
- Active Campaigns
- Completed Campaigns

User Information



The user information section displays the following information.

Email	The email address of the user.
User Created	Displays the method of user creation, *Manually* or *Azure AD*.
Updated At	Displays the timestamp of the last modification to the user's data.
Member of Groups	The count of the groups the user belongs to. Click count to navigate to *Member of Groups* section.
Enrolled Campaigns	The total count of campaigns the user is part of.
Active Campaigns	The count of active campaigns the user is part of. Click count to navigate to *Active Campaigns* section.
Completed Campaigns	The count of completed campaigns the user was part of. Click count to navigate to *Completed Campaigns* section.
Total Trainings Assigned	The total count of trainings assigned to the user.
Completed Trainings	The count of trainings the user has completed.
Incomplete Trainings	The count of trainings the user has enrolled for, but not completed.

Risk Rating	The letter grade between *A and F* assigned to the recipient . An *A* indicates the user poses minimal risk and a *F* grade indicates the user poses the maximum risk to the organization.

Click *Edit* to update the user details. Click *Delete* to delete the user.

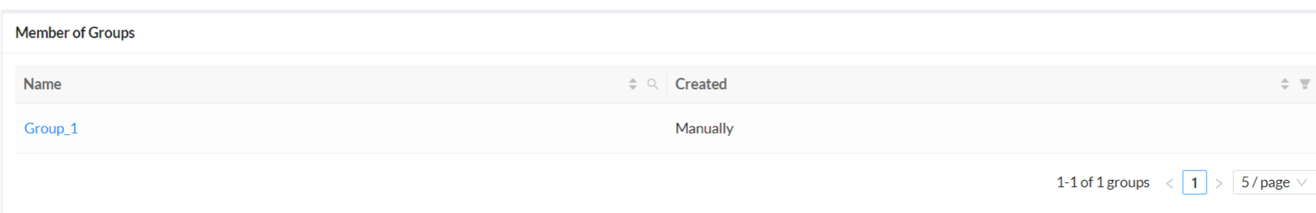
Campaign counts exclude deleted campaigns.

User Risk Grades

Provides a graphical representation of the user's risk score across campaigns. Hover over the graph to view the risk grade.

Member of Groups

Displays a list of groups the user belongs to. Click a group name to navigate to the corresponding group page. See Group List.

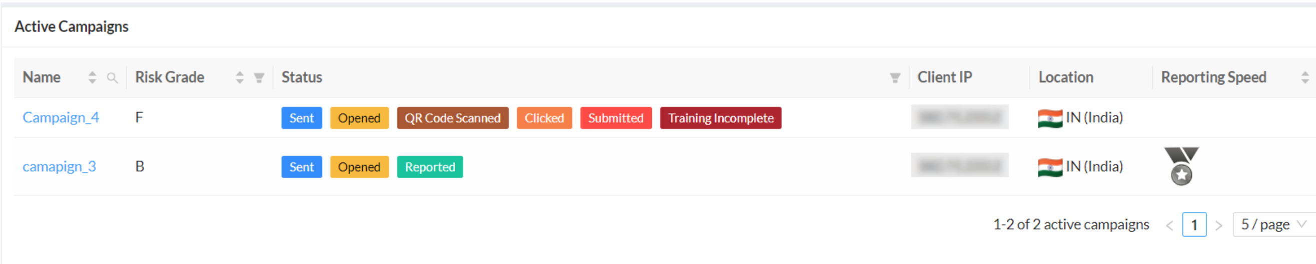

Member of Groups

Name	Created
Group_1	Manually

1-1 of 1 groups 1 5 / page

Active Campaigns

Displays a list of active campaigns the user is currently part of. Click a campaign name to navigate to the corresponding campaign details page. See Viewing campaign statistics.

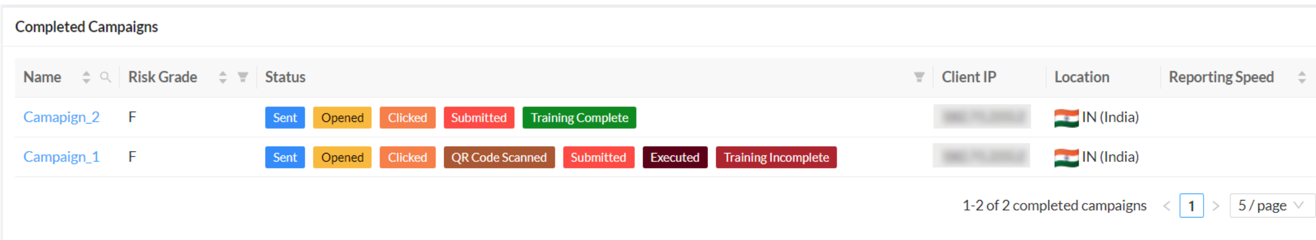

Active Campaigns

Name	Risk Grade	Status	Client IP	Location	Reporting Speed
Campaign_4	F	Sent Opened QR Code Scanned Clicked Submitted Training Incomplete	[illegible]	IN (India)	
camapign_3	B	Sent Opened Reported	[illegible]	IN (India)	

1-2 of 2 active campaigns < 1 > 5 / page

Completed Campaigns

Displays a list of completed campaigns the user was part of. Click a campaign name to navigate to the corresponding campaign details page. See Viewing campaign statistics.


Completed Campaigns

Name	Risk Grade	Status	Client IP	Location	Reporting Speed
Camapign_2	F	Sent Opened Clicked Submitted Training Complete	[illegible]	IN (India)	
Campaign_1	F	Sent Opened Clicked QR Code Scanned Submitted Executed Training Incomplete	[illegible]	IN (India)	

1-2 of 2 completed campaigns < 1 > 5 / page

Group List

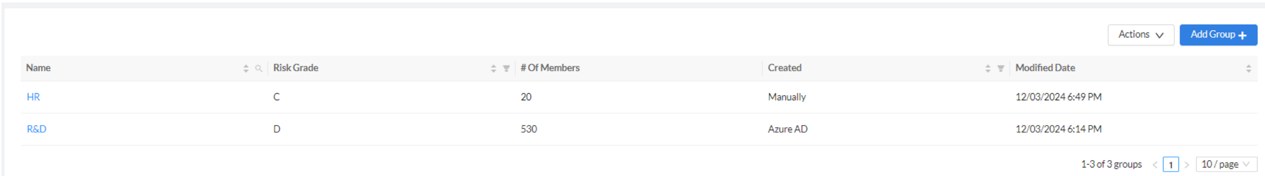
Group Lists are distribution lists for your campaigns. A Group List is required even if you are sending an email to only one user. Group Lists allow you to compare responses across segments within your organization. Users can be added to a group one at a time, or using the CSV template to perform a bulk 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
- View user details
- Update user details
- Filtering group list
- Hide/Unhide a group
- Deleting a group

To create a group list:

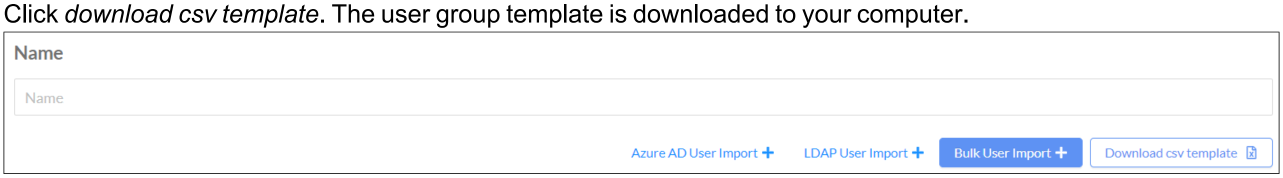
1. Go to *Recipients* and click *Add Group*. The *Recipients- Create* page opens.



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:

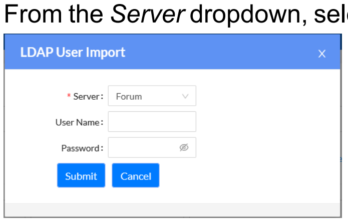
1. Click *Add Group*.
2. Click *download csv template*. The user group template is downloaded to your computer.



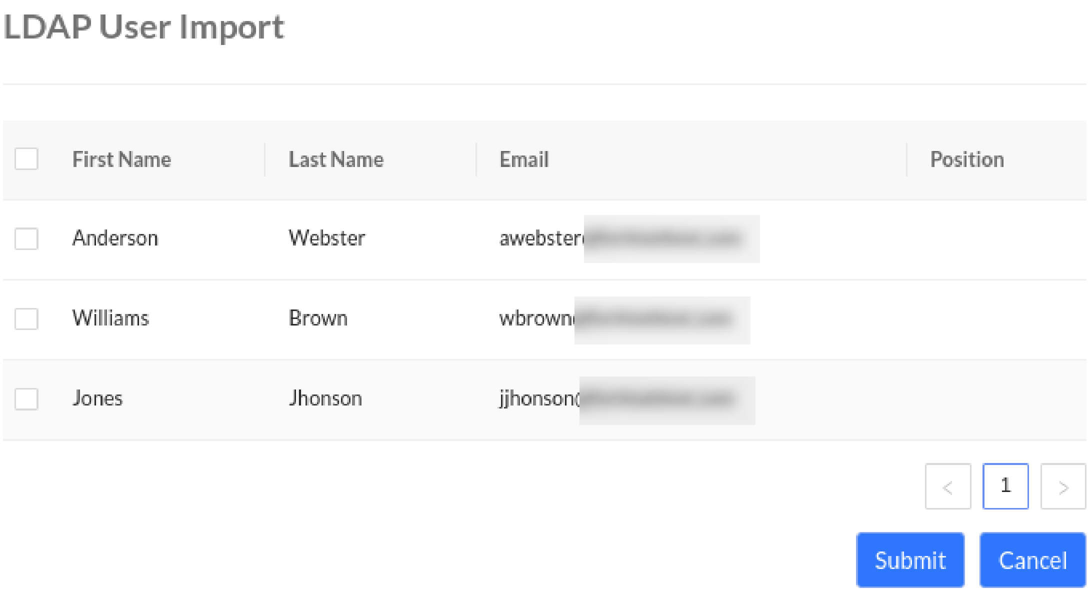
1. Enter the user's *First name*, *Last name*, *Email*, and *Position* in the template, and save the file.
2. In the *Recipients- Create* page, click *Bulk User Import*. The *Upload csv* dialog opens.
3. Upload the csv file. The users are added to the group.
4. In the *Group name* field, enter the name of the group.
5. Click *Submit*.

To import an LDAP user group:

1. Configure the LDAP server. See LDAP server on page 33
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*.



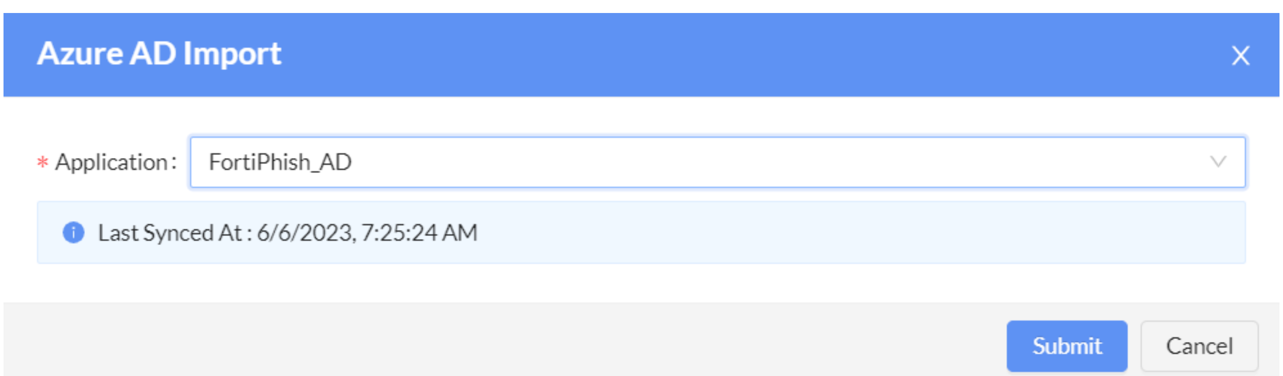
6. Select the users you want to import and click *Submit*. The LDAP users are added to the group.



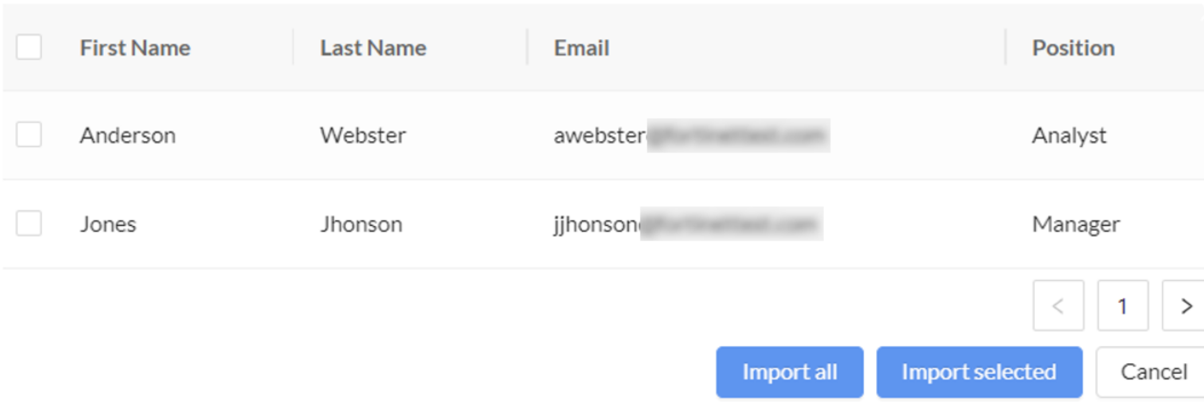
7. In the *Group name* field, enter the name of the group.
8. Click *Submit*.

To import an Azure AD user group:

1. Configure the Azure AD server. See Azure AD Server on page 35
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.



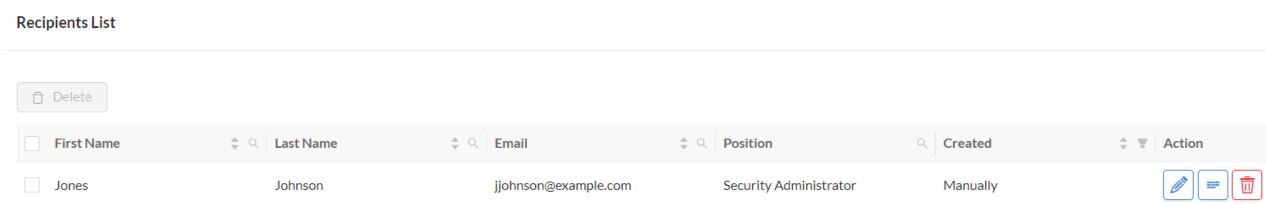
6. Select the users you want to import and click *Import selected*, or click *Import all* to import all users.



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

To view a user's details:

1. Go to *Recipients* > *Group List*, and select a group in the list.
2. In *Recipients List* section, click the *View User* button in *Actions* column for the user you want to view detailed information.



3. The corresponding user profile page is displayed. See User Profile.

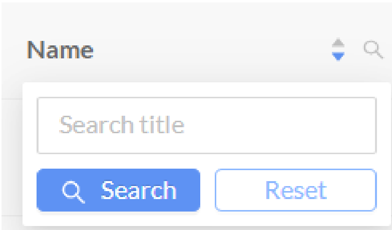
To update a user's details:

1. Go to *Recipients* > *Group List*, and select a group in the list.
2. In *Recipients List* section, click the *Edit* button in *Actions* column for the user you want to edit.
3. Update the details, and click *Submit*.
4. (Optional) Click the Delete button to remove the user from the group.

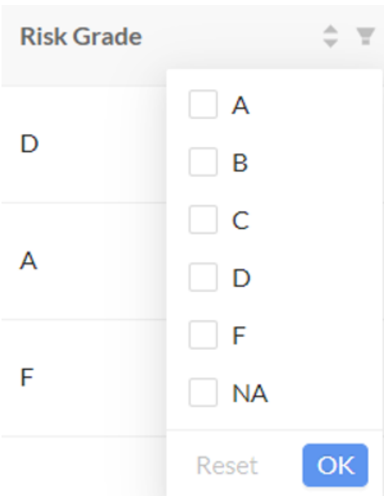
To update details of a user imported from Azure AD, the changes must be made within Azure AD server and then synced back to FortiPhish.

Filtering group list

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



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.

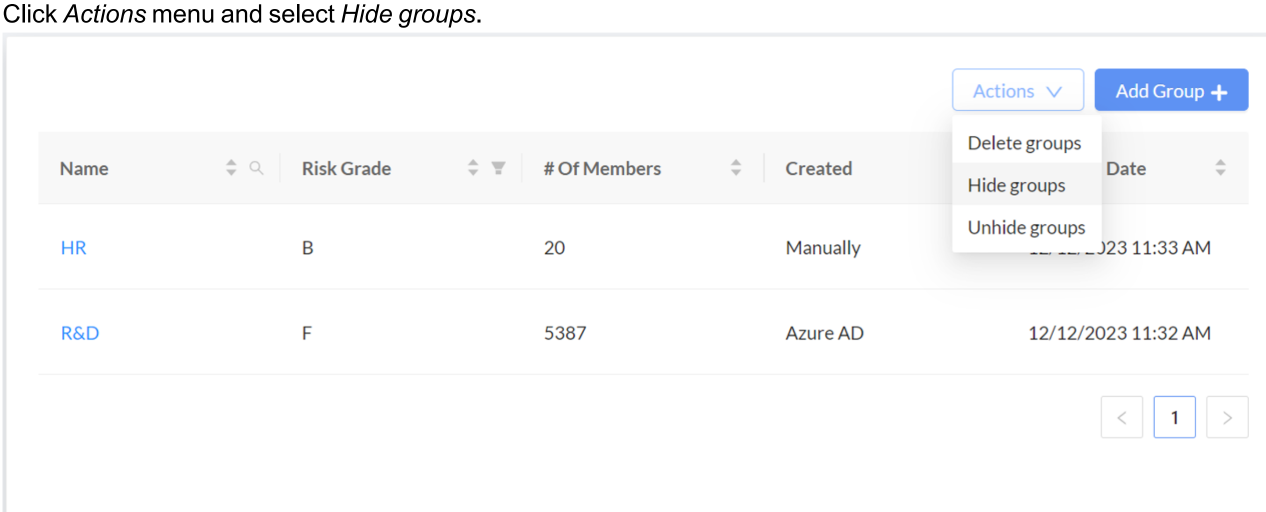


Hide/Unhide a group

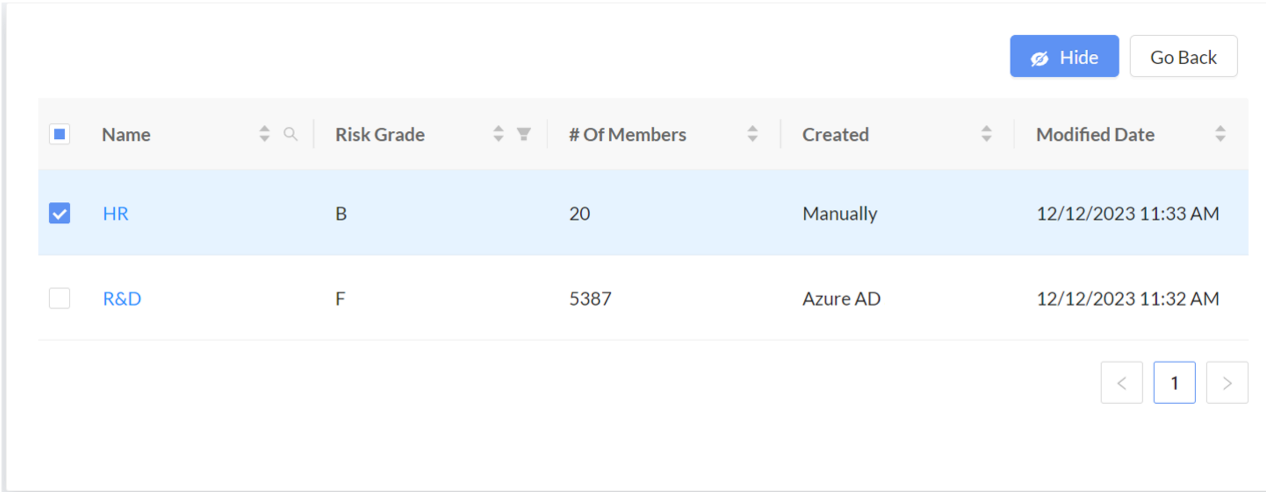
By **hiding** a group, it will no longer appear in the group list page or when creating a campaign. This applies to both manually created groups and groups imported from Azure AD.

To hide a group:

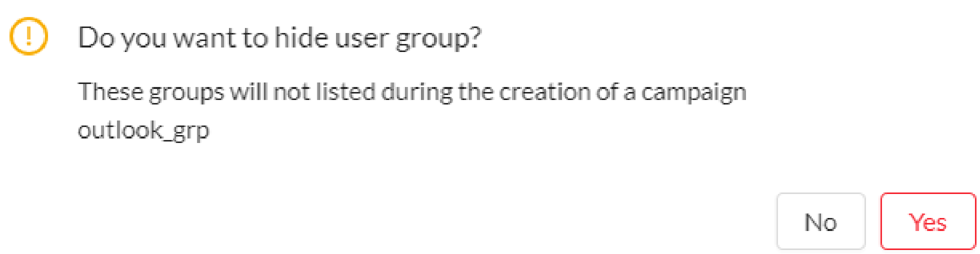
1. Go to *Recipients* > *Group List*.
2. Click *Actions* menu and select *Hide groups*.



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



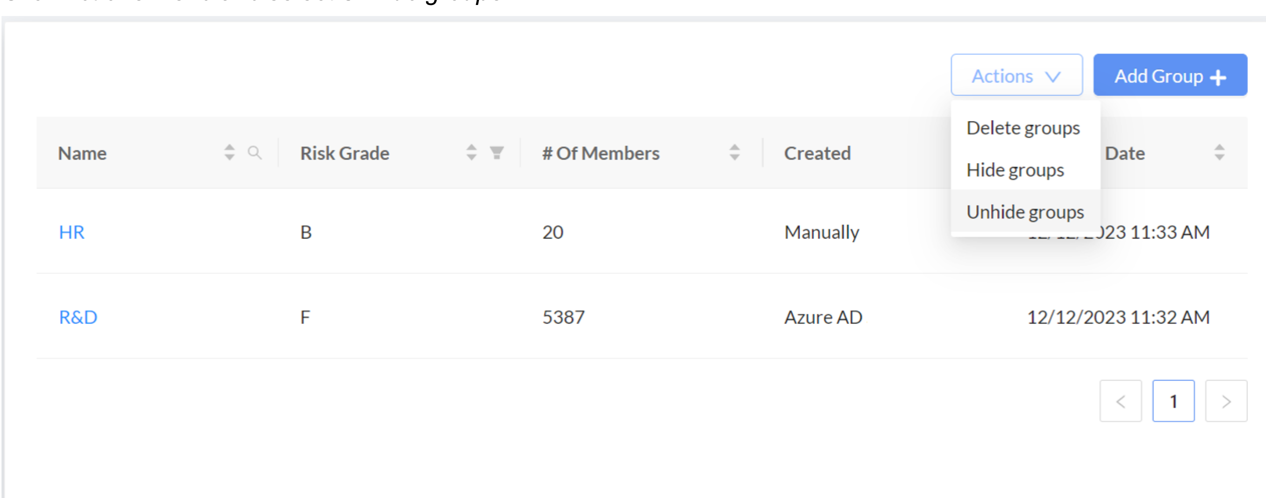
4. A confirmation message is displayed. Click *Yes*.



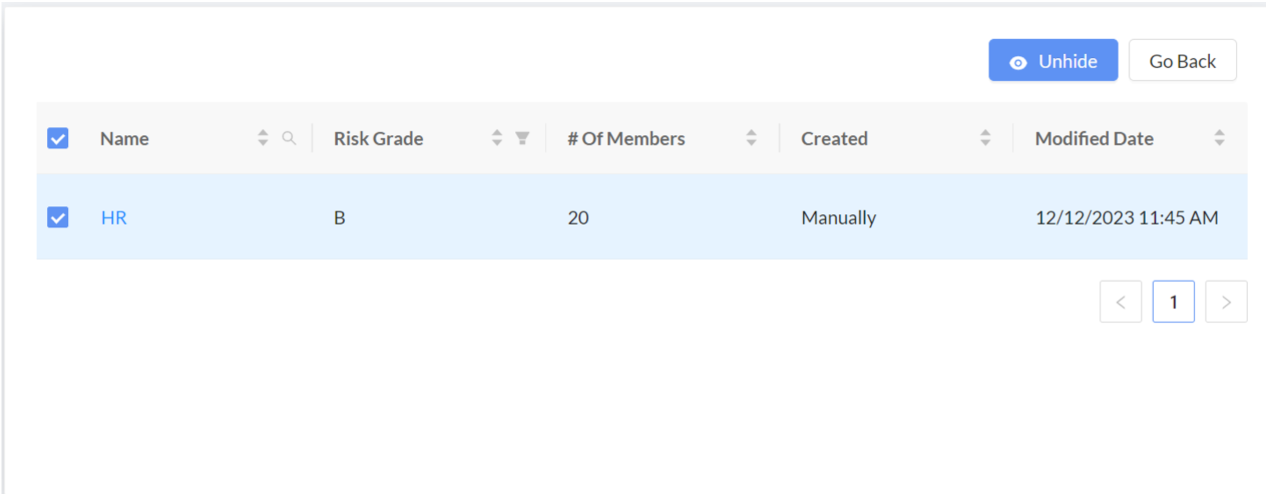
When the unhide option is selected, the list of hidden groups will be displayed. You can unhide the groups, allowing them to appear in the group list page and when creating a campaign.

To unhide a group:

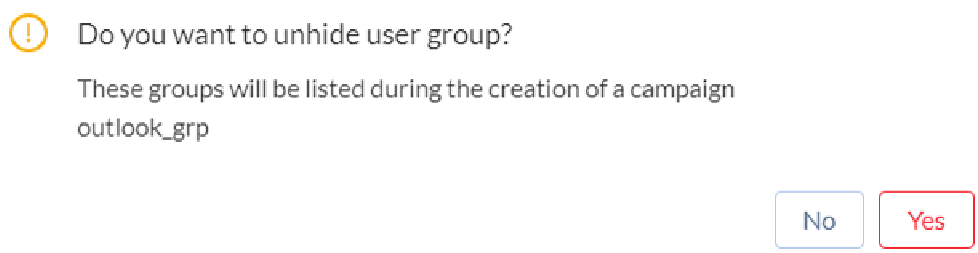
1. Go to *Recipients* > *Group List*.
2. Click *Actions* menu and select *Unhide groups*.



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



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



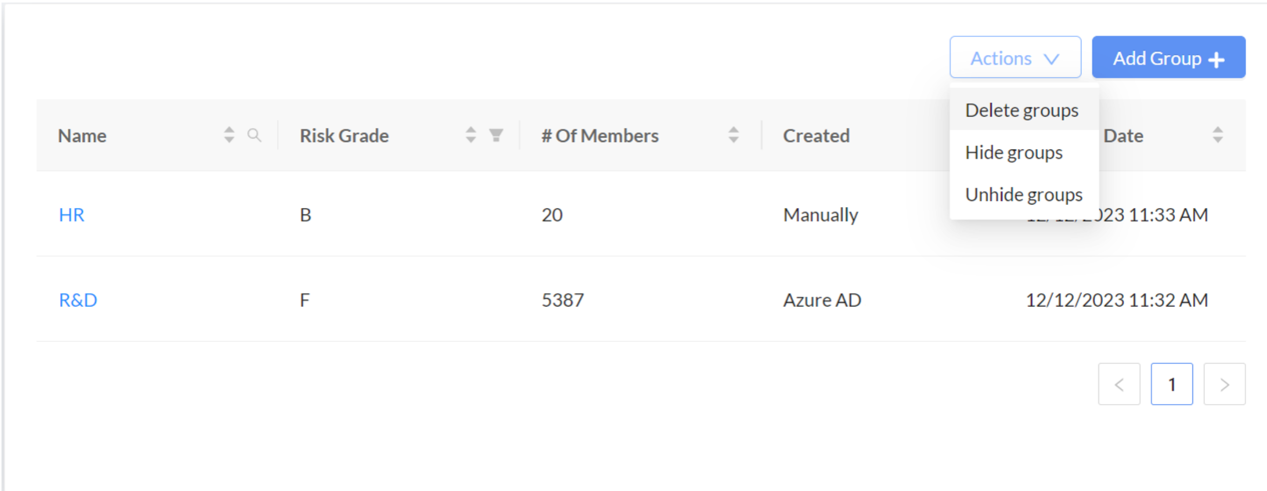
You cannot delete, edit, or modify groups imported from an Azure AD client. You can only modify or manage them from the Azure AD server.

Deleting a group

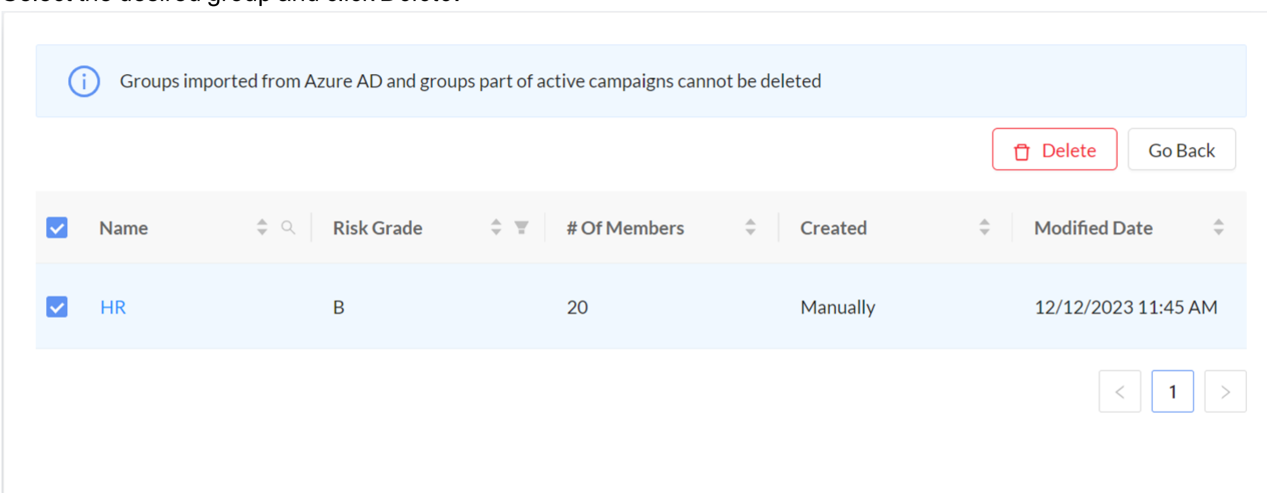
Groups imported from Azure AD can only be deleted once the Azure AD client is removed.

To delete a group:

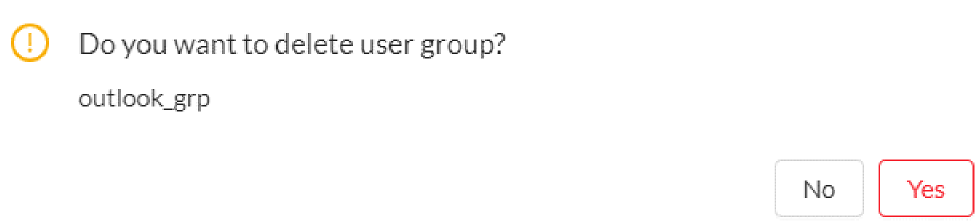
1. Go to *Recipients* > *Group List*.
2. Click *Actions* menu and select *Delete groups*.



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



4. A confirmation is displayed. Click *Yes*.

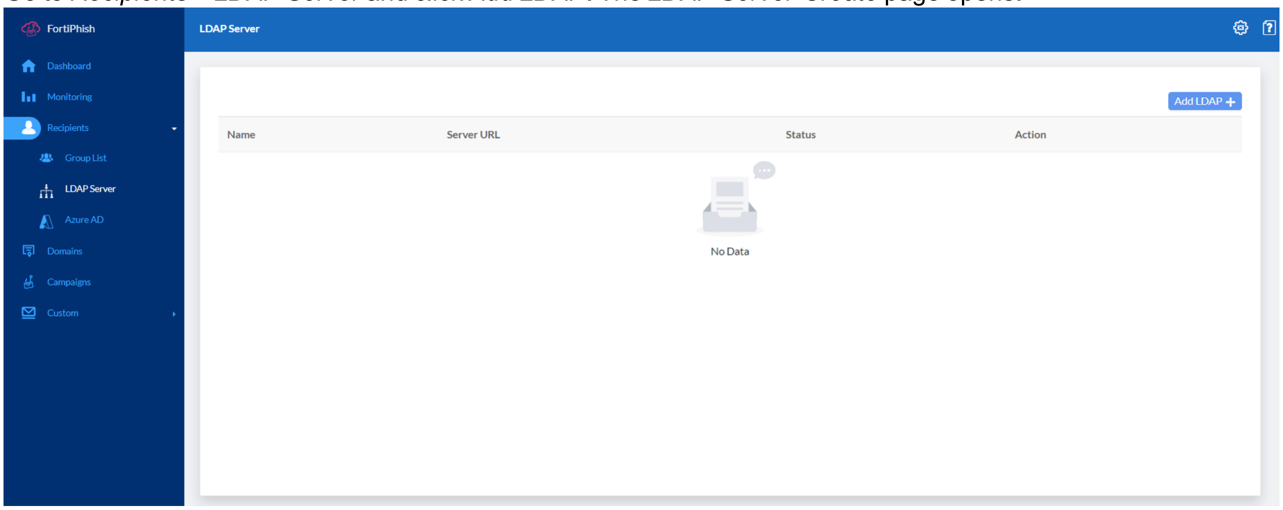


LDAP server

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

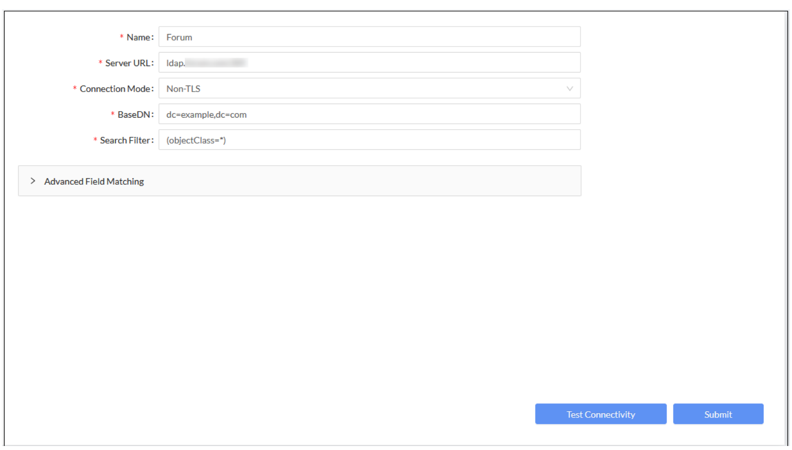
To add an LDAP server:

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

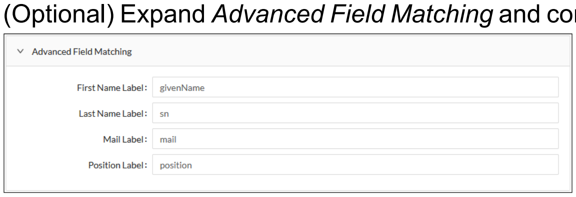


2. Configure the LDAP server settings.

Name	The LDAP server name.
Server URL	The LDAP server URL.
Connection Mode	Select *Non-TLS*, *TLS*, or *STARTTLS*.
BaseDN	The point where the server will search for users.
Search Filter	The search filter syntax.

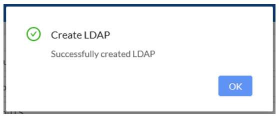


3. (Optional) Expand *Advanced Field Matching* and configure the settings.



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:

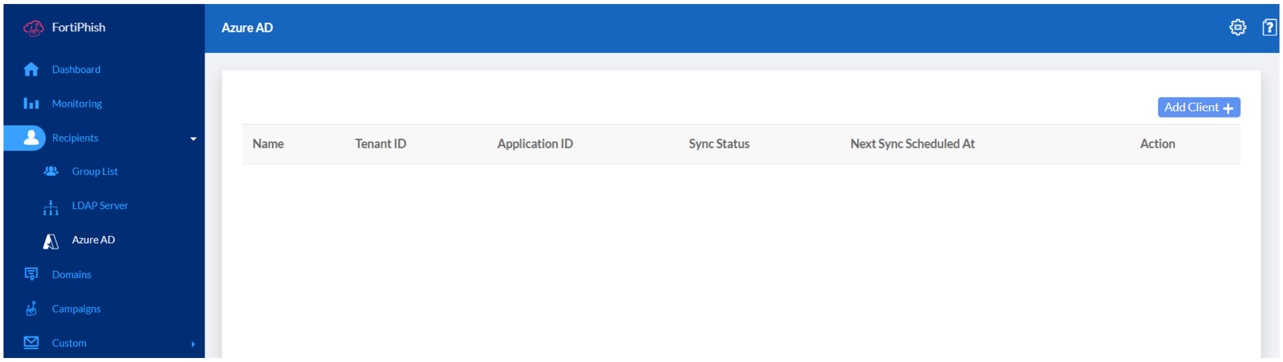
1. In Azure or O365 portal, switch to *Azure Active Directory* page.
2. Create a new application that can be associated with FortiPhish. In azure portal:
   a. Go to *App Registrations* > *New Registration*.
      i. Provide a name for *App. Ex. FortiPhish-AD-Proxy*.
      ii. Select the tenant.
      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

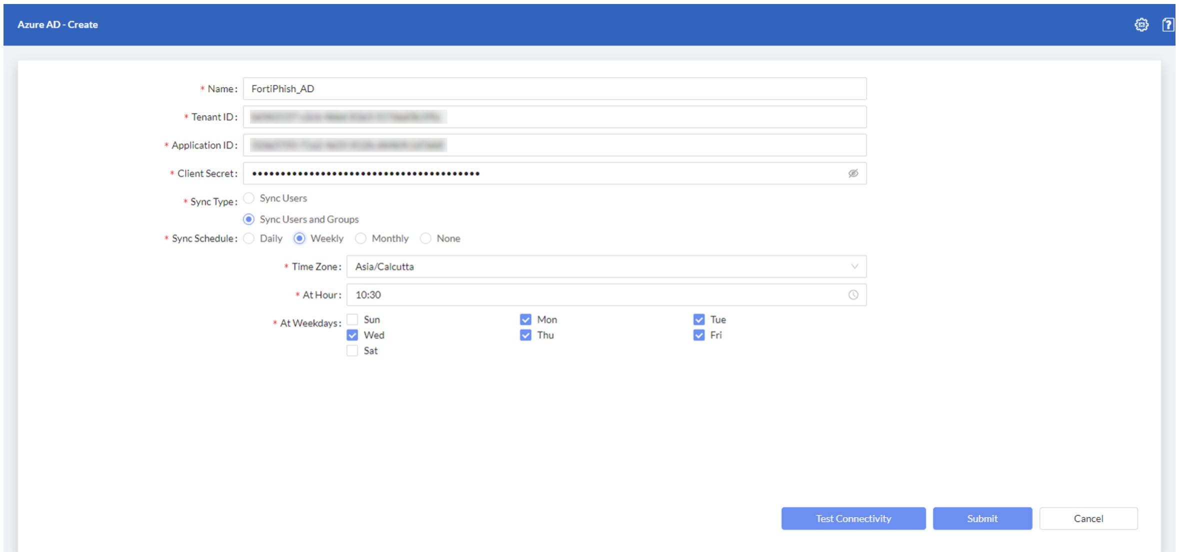
To add an Azure AD server:

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

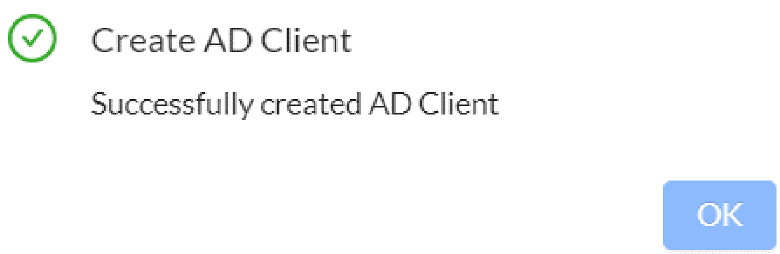


2. Configure the Azure AD server settings.
   a. Enter a *Name* for Azure AD.
   b. - Enter the *Tenant ID, Application AD, and Client Secret* information gathered during Configuring Azure AD for FortiPhish.
   c. Select *Sync Users* to import only the users or select *Sync Users and Groups* to import both users and groups from Azure AD.
   d. Set synchronization schedule to automatically sync users or users and groups.
      i. Select the frequency of the synchronization, *Daily* , *Weekly*, or *Monthly*. Select None to disable automatic syncing.
      ii. Select the desired time zone from the drop down menu.
      iii. Set the time of synchronization by selecting hours and minutes.
      iv. If *Weekly* or *Monthly* is set as the frequency, select the days on which the synchronization must be performed. When configuring the synchronization frequency to *Monthly*, select *31* from *At day* drop down to schedule synchronization on the last day of each month.

> If both the *Sync Schedule* and *Campaign Schedule* which includes Azure AD users as recipients, are configured for the same time, the schedule that is executed first will delay the execution of the other until it is completed.



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



- 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.
- To update user information, the changes must be made within Azure AD server and then synced back to FortiPhish.
- When you remove a user in Azure AD, FortiPhish removes them from all the groups they belong to, including manually created groups. This change takes effect after the next synchronization

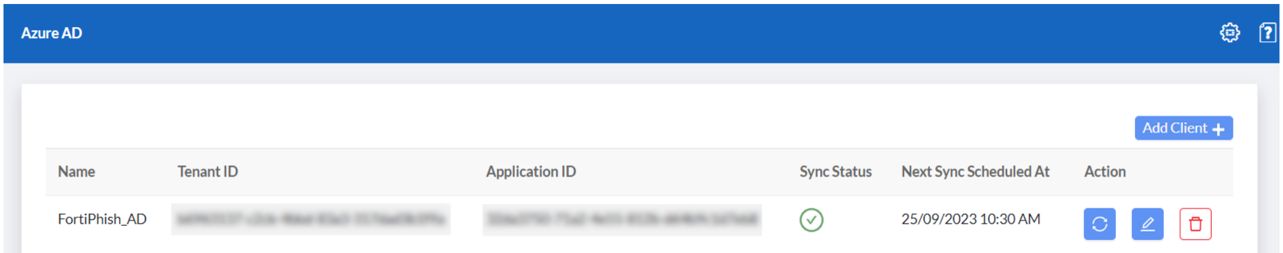
Syncing the Azure AD server

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

To sync the server:

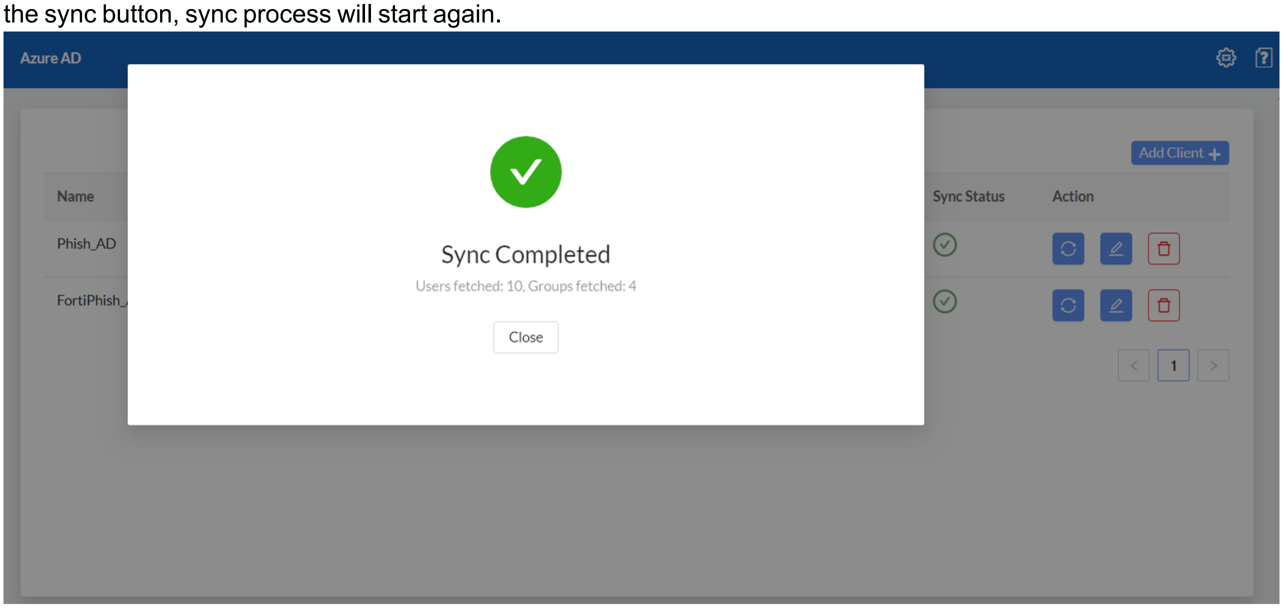
1. In FortiPhish, go to *Recipients > Azure AD* .
2. (Optional) In the *Sync Status* column, hover over the status column to view the latest sync date and time. If *Sync Users and Groups* option is selected while adding Azure AD, number of users and groups fetched is displayed else

if *Sync Users* is selected, only the number of users fetched is displayed.



The *Next Sync Scheduled At* column, displays date and time of the next synchronization schedule. If sync schedule is not configured, *NA* is displayed.

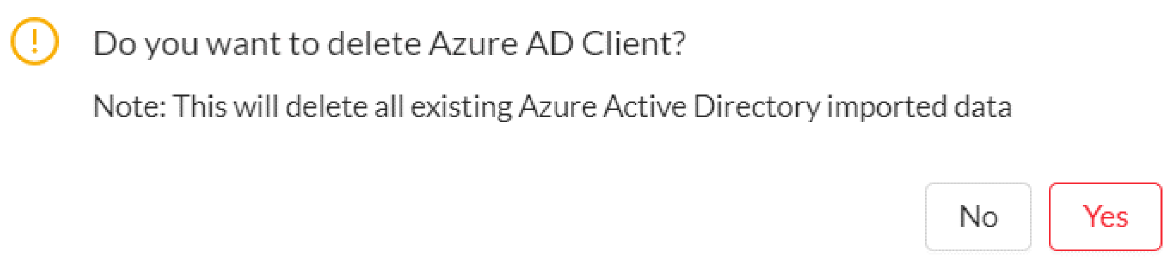
3. In the *Action* column, click the sync button. During the sync process, clicking the sync button will display the number of users or users and groups fetched information.
4. When the sync is complete, a confirmation message is displayed. Once the sync process is completed, if you click the sync button,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



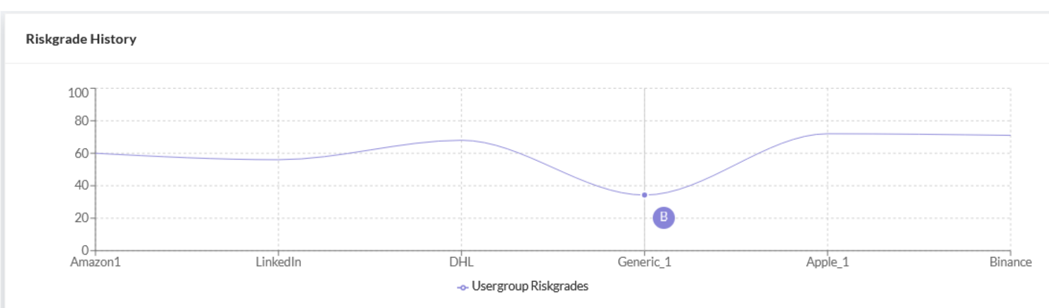
3. Click *Yes*.

- Deleting an Azure AD client from FortiPhish won't affect existing Azure AD imported groups. However, you can manually delete them if no longer needed.
- Adding or removing recipients from these AD groups automatically will change the *Created* field in *Recipients* > *Group List* page from *Azure AD* to *Manually*.

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.



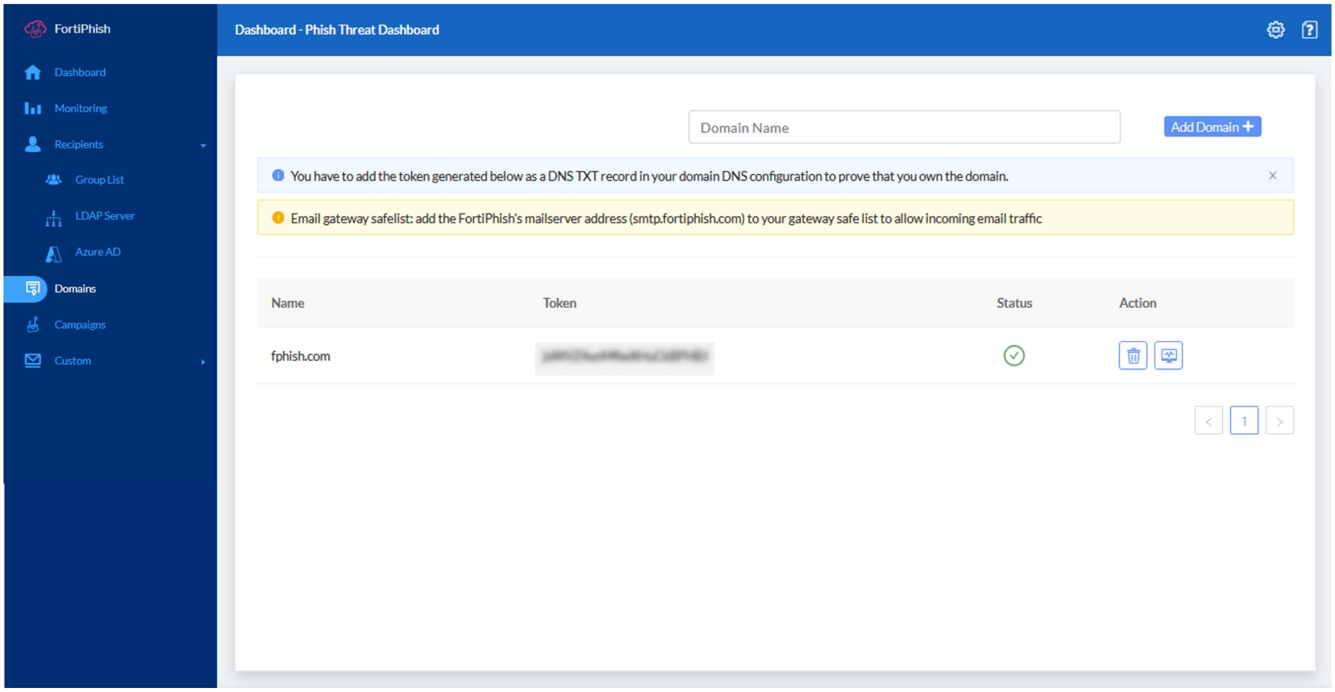
To view the Riskgrade History:

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 40.

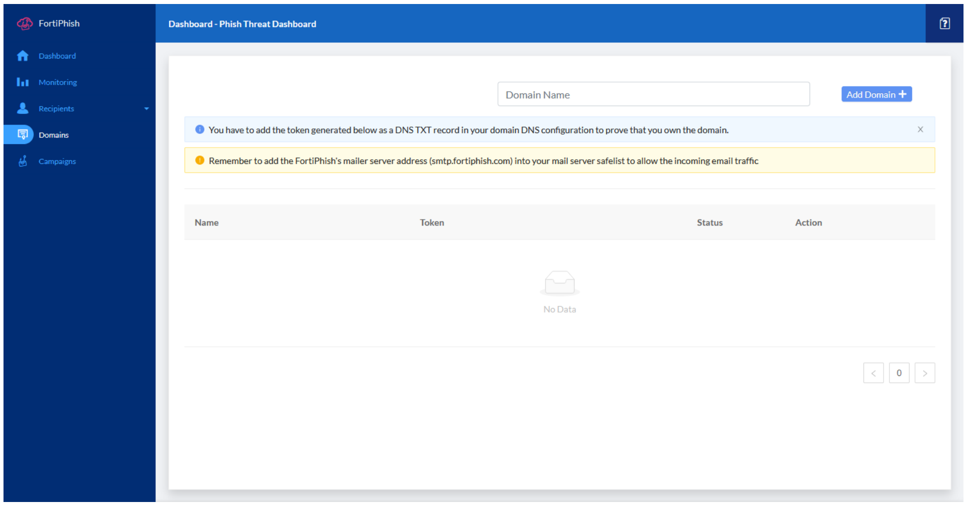


Adding domains

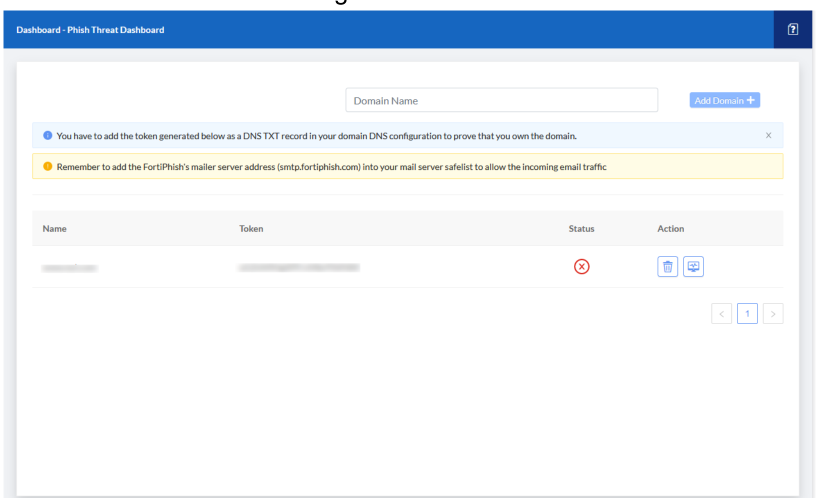
FortiPhish uses DNS tokens to verify you are the domain owner. Create the token in FortiPhish, and then add it to your domain's DNS settings. After the DNS settings are configured, verify the token in FortiPhish.

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.

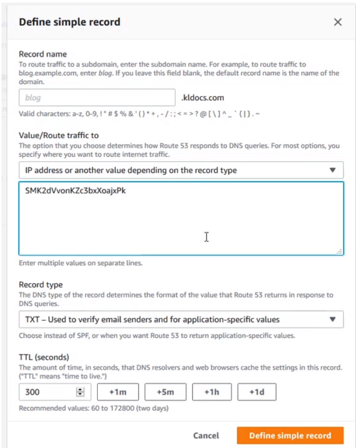


To add the token to your domain:

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.



To test the token with the command prompt:

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

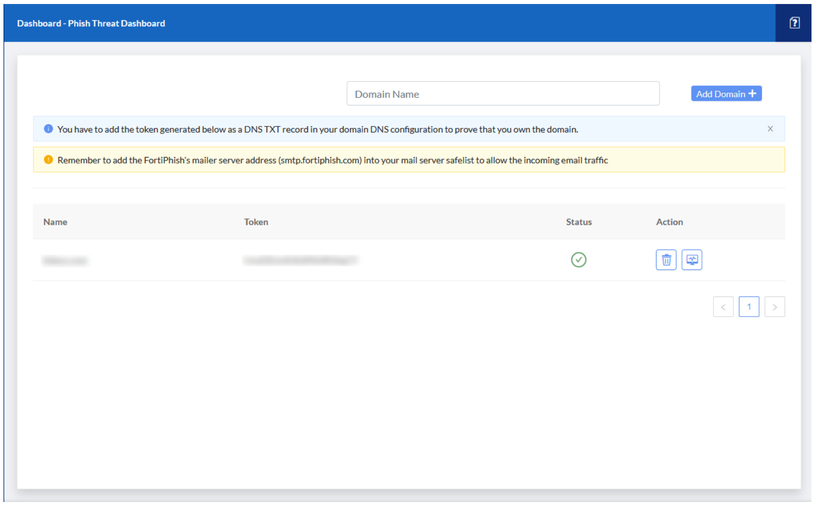
Example:

```
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-authorititative 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.

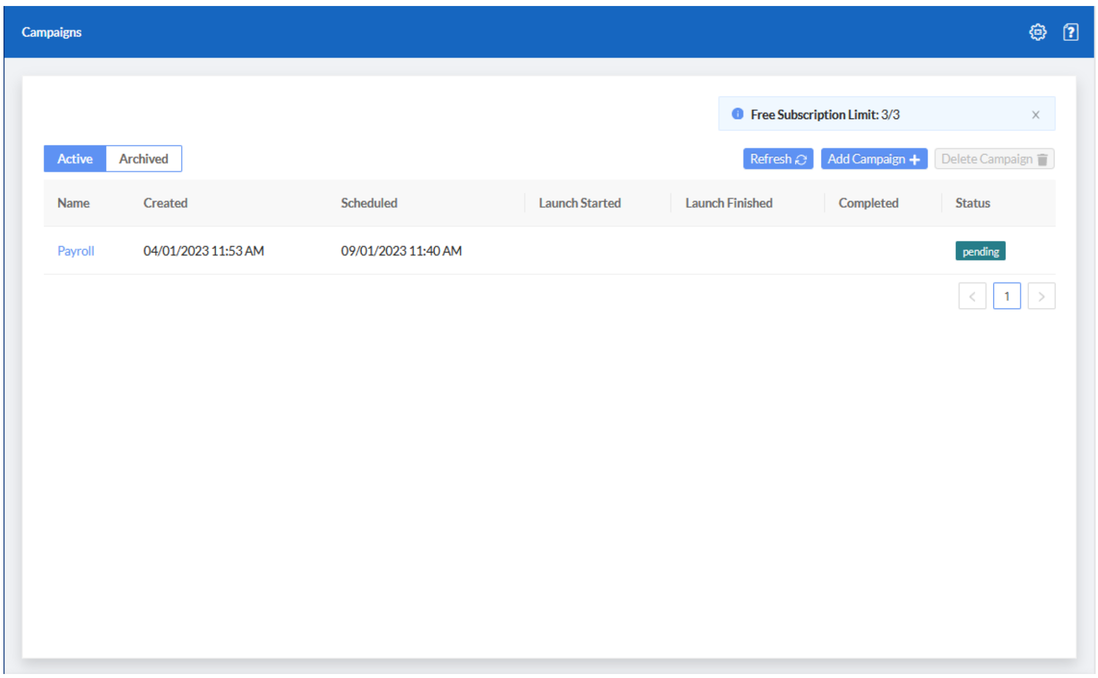


Campaigns

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 45.

Subscription Limit

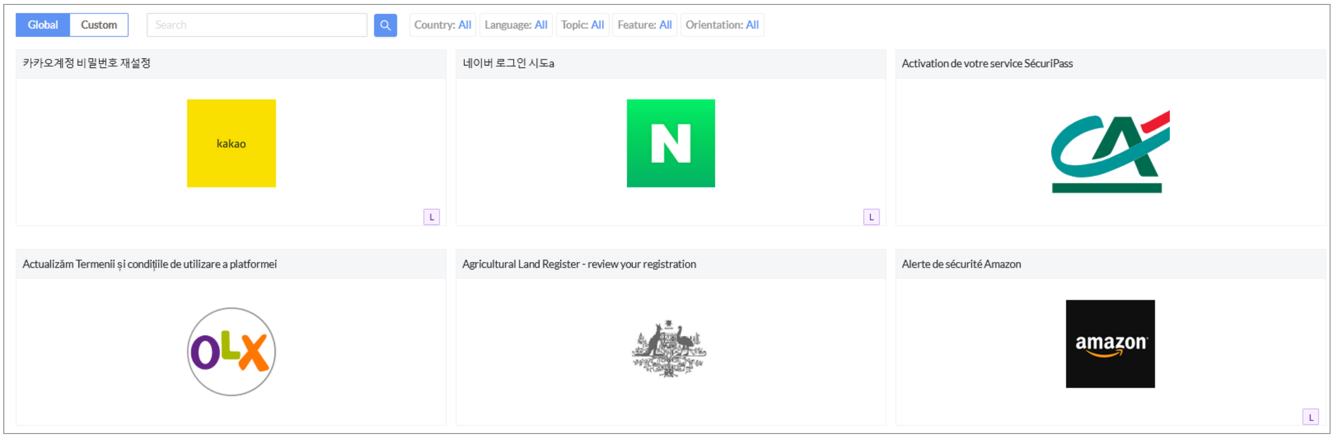
The *Subscription Limit* is directly linked to license entitlement(s). You can run an unlimited number of campaigns, however you are limited by the number of mailboxes. The *Used* count is reset at the beginning of each month.



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.

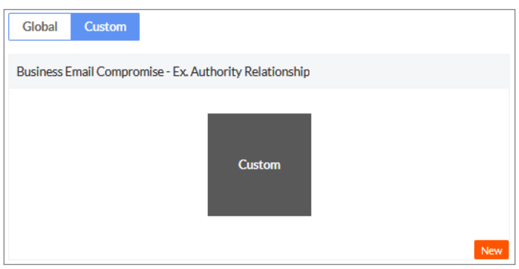
Enter key words in the *Search* field to find a template by name, or use the sort buttons to filter the templates by *Country*, *Language*, *Topic*, *Feature*, or *Orientation*. Templates that contain the letter *L* indicate the template includes a landing page.



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 63.

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

Subject		Edit the email subject
Click Behavior	**Only Redirect URL**	Enter the URL in the *Redirect URL* field.
	Landing Page	• Select *Preset* to use the landing page that comes with the template. • Select *Custom* to use a custom landing page you created. See, Landing page on page 65. FortiPhish does not save the data entered by the user in the landing page.
Level of Difficulty (This option is only available in *Global* templates.)	**Simple**	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. The email branding does not match the branding in the landing page.
	Moderate	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. The landing page looks authentic.
	Challenging	The email body is well written and does not contain spelling errors. The email branding and tone mimics authentic corporate communications. The landing page looks very authentic.
Use Attachment	To attach a PDF to the email, Select *Yes, Using Filename* and enter the filename in the text field. FortiPhish will not be able to collect the *Executed* 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 insert *links*, *images*, *QR code*, and *media*. • You can use variables in the email body to generate dynamic data while the campaign is running. See, Template variables on page 48. • QR code option is available only for *FortiPhish Premium* users. Contact Fortinet Support team to upgrade.
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.
Custom Domains	Select the custom domains you want from the dropdown. You can select up to 4 domains from a list of verified and approved domains for each campaign. Each recipient will see a different selected domain when clicking a campaign link.

	This feature is available only for *FortiPhish Premium* users. Contact Fortinet Support team to upgrade.
SMTP Gateway Server	(Optional) Select an SMTP server from the dropdown. For information, see SMTP on page 82.
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* list and click *Next*. The *Set a Schedule* page opens.
5. Configure the date, time, and duration of the campaign and click *Next*. The *Set Email Schedule* page opens.

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

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

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

7. Click *Start campaign*. A confirmation message appears.
8. 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 Date with Layout or Offset
`{{date|offset}}`	Date with offset	See Date with Layout or Offset

Variable	Description	Output
`{{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
`{{time}}`	Time	3:04 PM
`{{tracking_click_link}}`	Link for tracking	https://smtp.fortiphish.com/trackings/ {{recipient}}
`{{qr_code_link}}`	QR code for tracking	QR code image will be inserted

Date with Layout or Offset

{{date|layout}}

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:

09-0ct-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

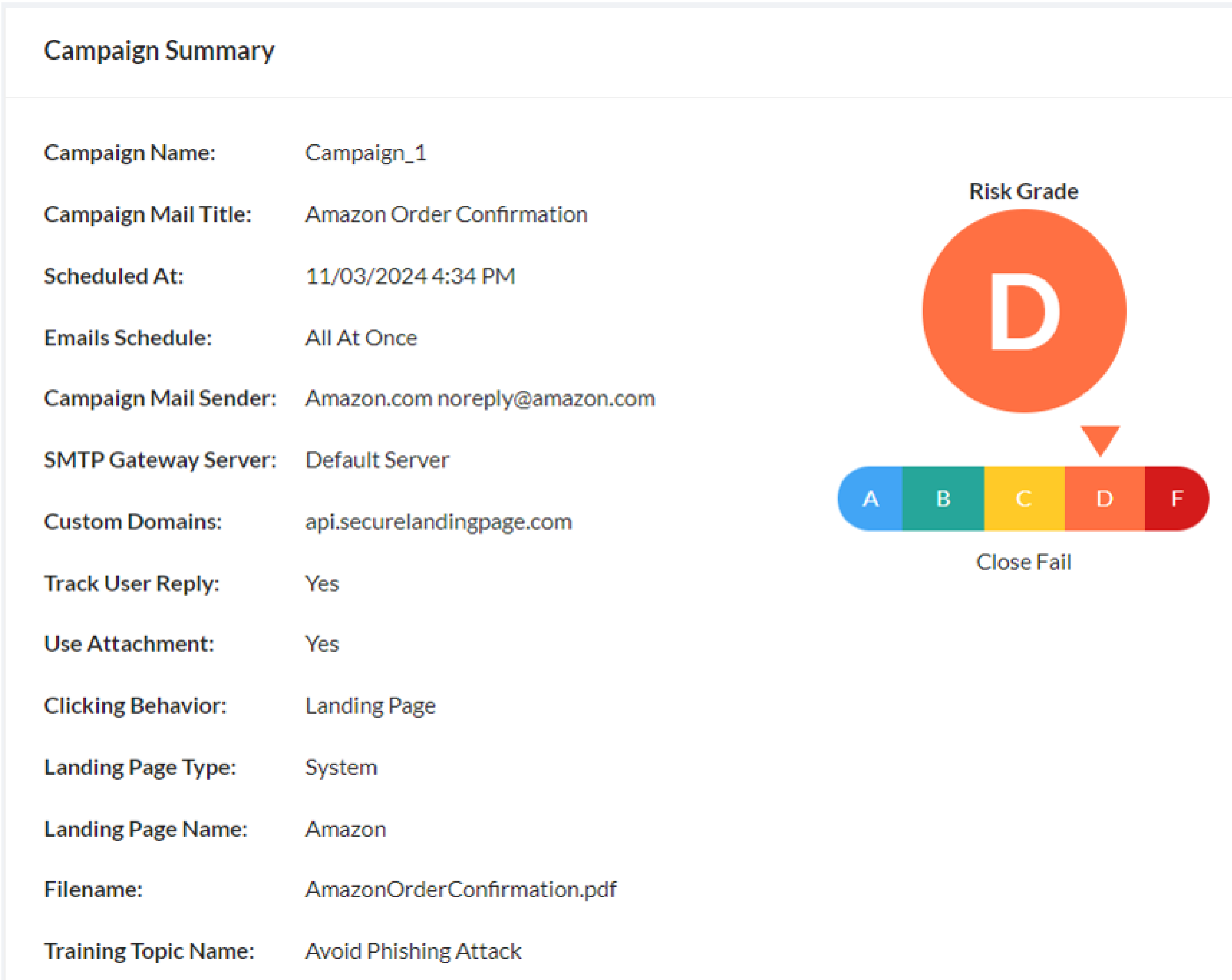
View a summary of the campaign details, as well as detailed response statistics. You can view the campaign statistics for active and archived campaigns.

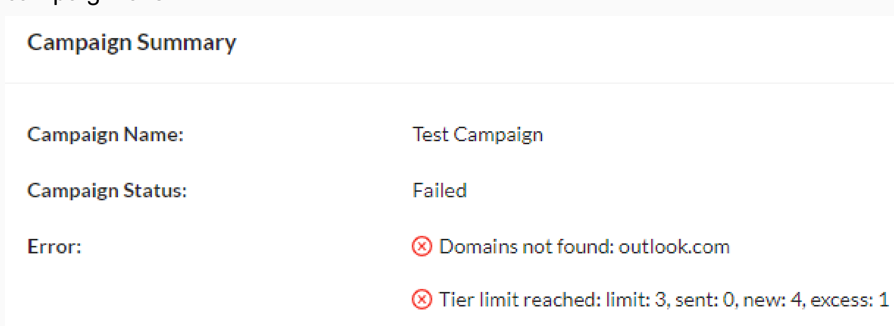
To view the campaign statistics:

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 Status
   - Campaign Preview
   - User Pass Rate
   - 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*.

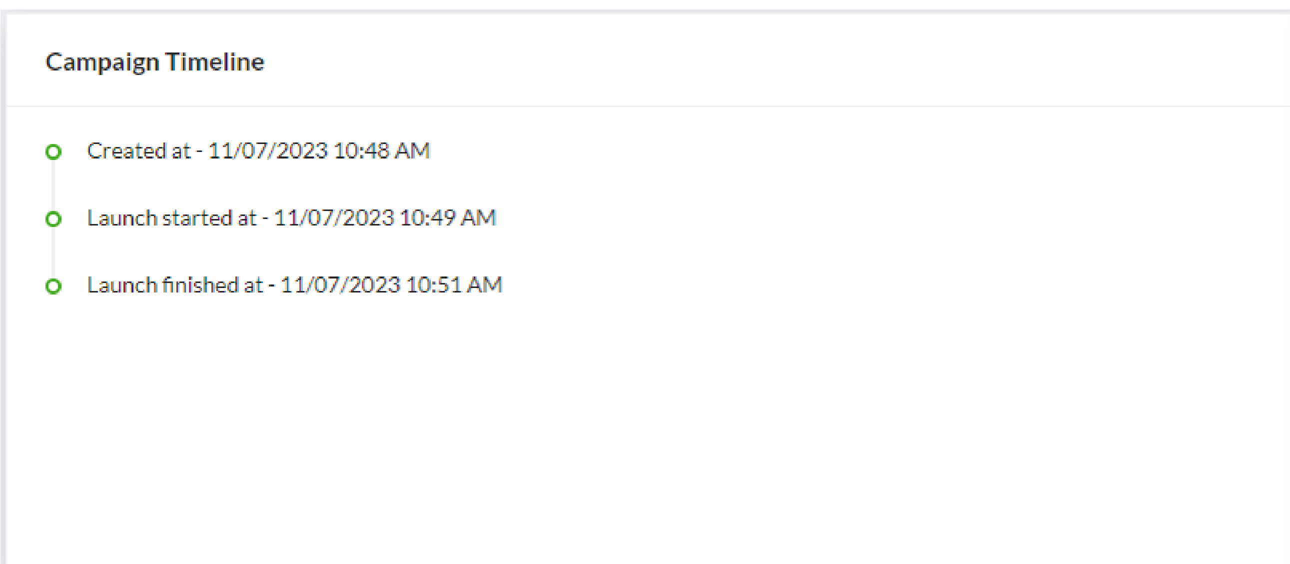


Campaign Name	The name you entered when you created the campaign.
Campaign Status	*Pending* when a new campaign is created and is yet to be started or *Failed* if the campaign fails. 
Error	Displays the error due to which the campaign failed. You can use this information for troubleshooting purposes.

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

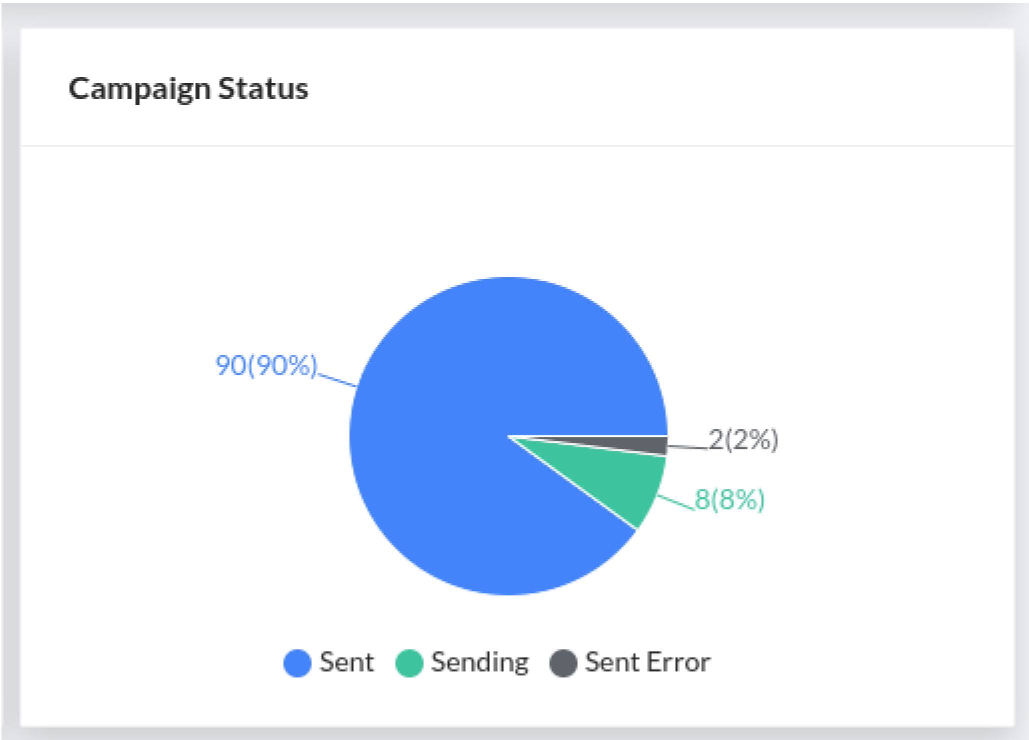
Campaign Timeline

The Campaign Timeline widget displays when the campaign was created, started and finished.



Campaign Status

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

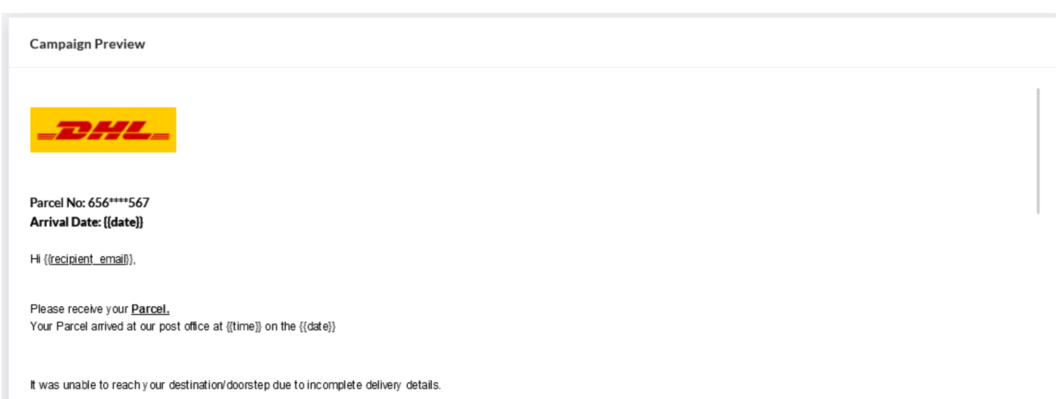


The *Campaign Status* monitor displays the following information:

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

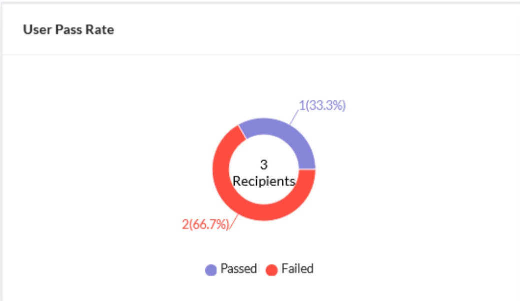
Campaign Preview

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



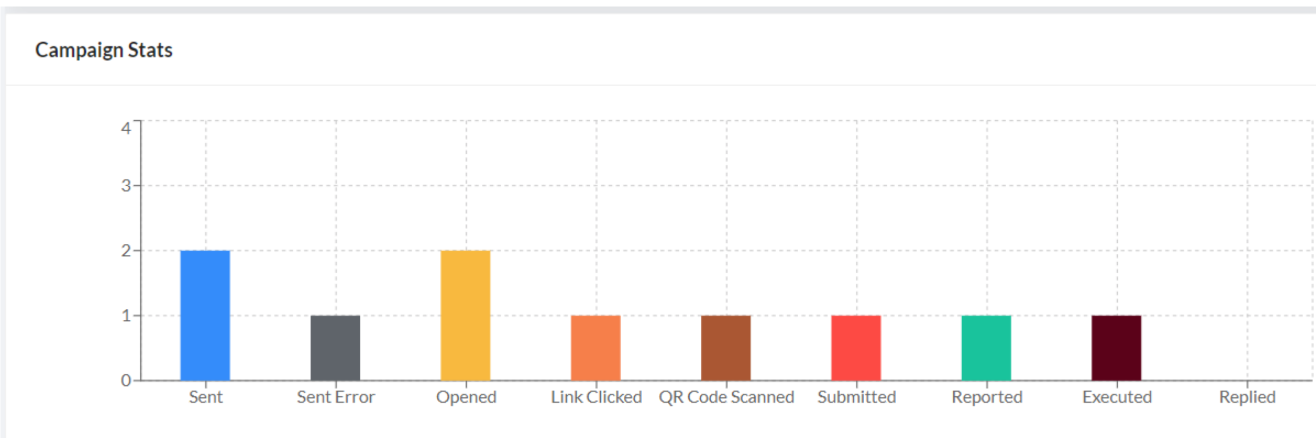
User Pass Rate

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 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.

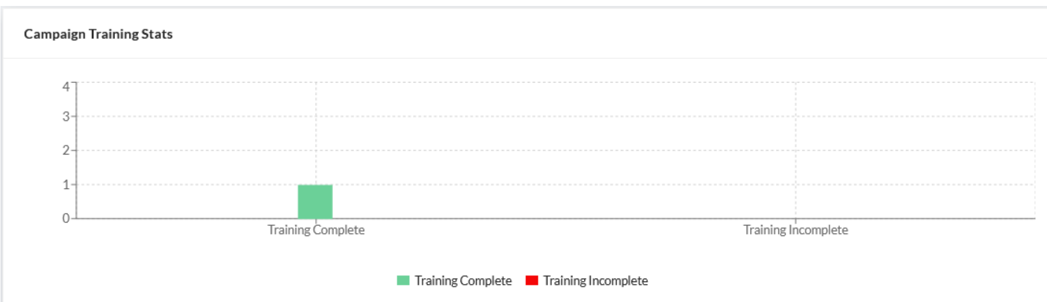


Sent	The number of emails sent to the user group.
Sent Error	The number of emails that bounced.
Opened	The number of recipients who opened the email.
Link Clicked	The number of recipients who clicked the redirect link.
QR Code Scanned	The number of recipients who scanned the QR code.
Submitted	The number of recipients who entered information on the landing page. FortiPhish does not save the data entered by the user in the landing page.

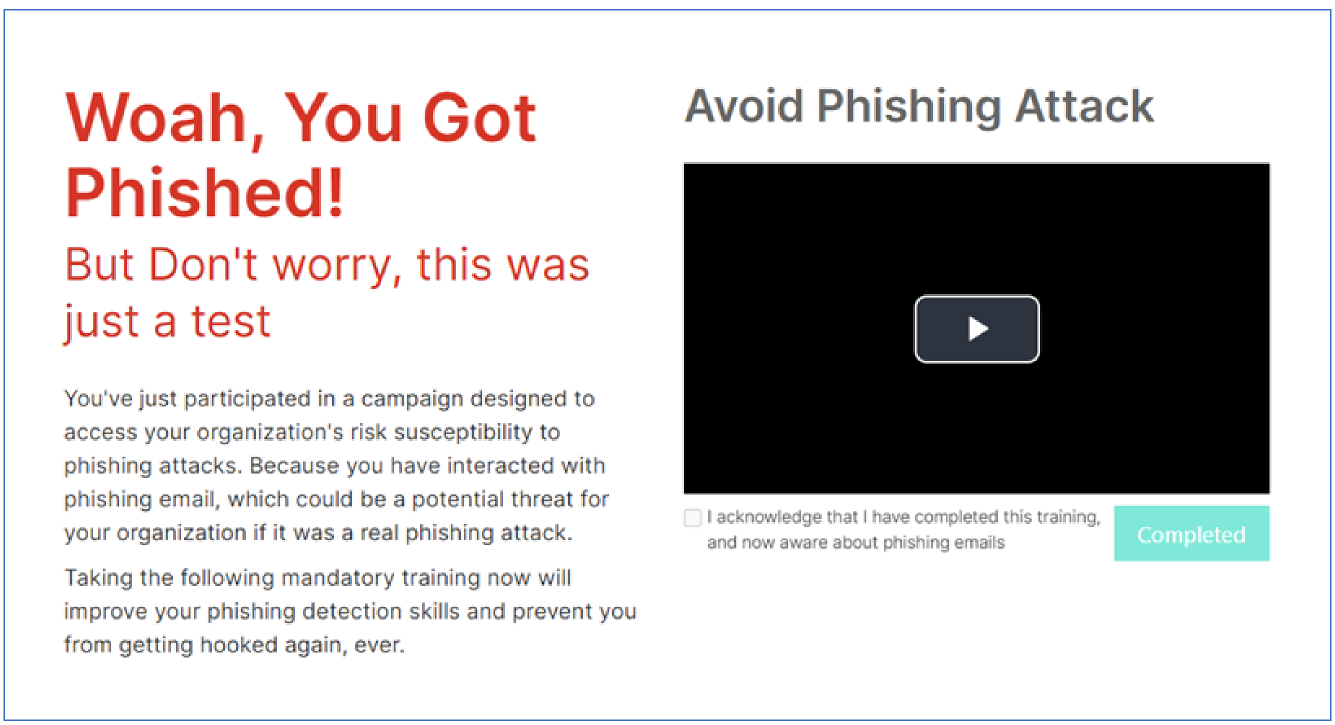
Reported	The number of recipients who reported the phishing email as suspicious.
Executed	The number of recipients who opened or executed the file attached in the phishing email. FortiPhish will not be able to collect the *Executed* metric when the attached PDF is previewed in a reader that disables links for security purposes.
Replied	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.

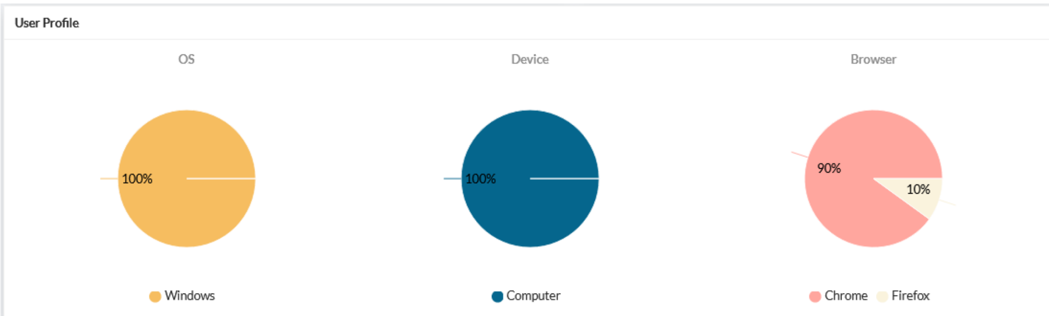


A recipient is counted as *Training Complete* after they acknowledge they have reviewed the information in the training web page. For information about *On Click Training*, see Creating campaigns.



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.

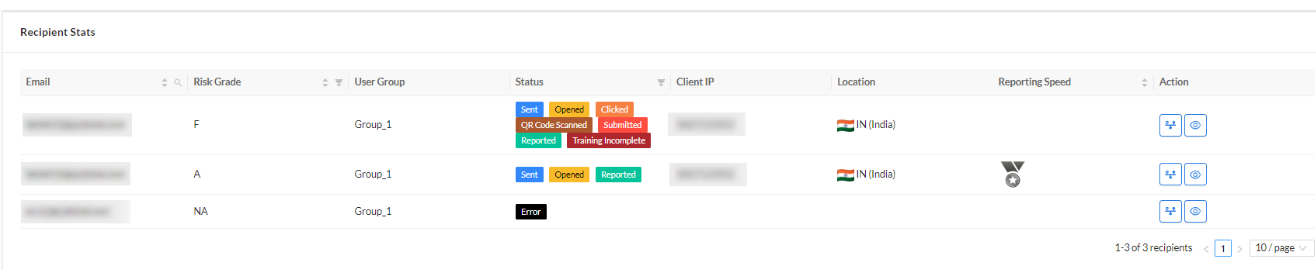


The *User Profile* monitor displays the followling information:

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

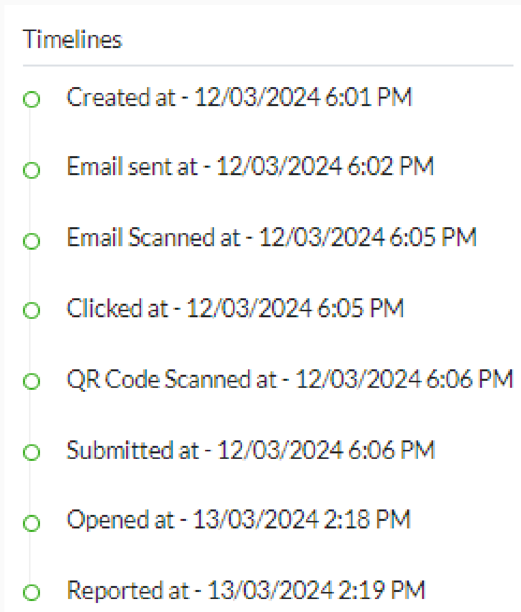
Recipient Stats

The *Recipient Stats* monitor displays the recipient statistics.



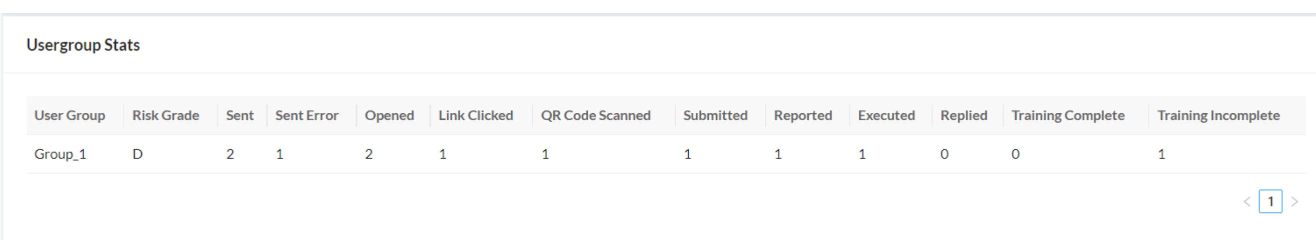
The *Recipient Stats* monitor displays the following information:

Email	The user email address.
Risk Grade	The letter grade between *A and F* assigned to the recipient . An *A* indicates the user poses minimal risk and a *F* grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be *NA* on the *Dashboard* and *Monitoring* pages.
User Group	The user group the recipient belongs to.
Status	Displays the recipient's response *Sent*, *Pending*, *Opened*, *Clicked*, *Submitted*, *QR Code Scanned*, *Reported*, *Executed* and *Training Complete/Training Incomplete*.

Client IP	The recipient's IP address.
Location	The recipient's country.
Reporting Speed	The recipient's response time. • *Platinum*: Under 30 seconds • *Gold*: Under 5 minutes • *Silver*: Under 30 minutes • *Bronze*: Under 59 minutes An empty field indicates the recipient did not report the phish attempt. To view the actual response time, hover over the medallion.
Action	Click the *View Timelines* icon to view the date and times of the recipient's actions.  Click the *View User* icon to view the detailed user information. See User Profile.

Usergroup Stats

The Usergroup Stats displays group statics.



Usergroup Stats

User Group	Risk Grade	Sent	Sent Error	Opened	Link Clicked	QR Code Scanned	Submitted	Reported	Executed	Replied	Training Complete	Training Incomplete
Group_1	D	2	1	2	1	1	1	1	1	0	0	1

The *Usergroup Stats* displays the following information:

User Group	The user group name.

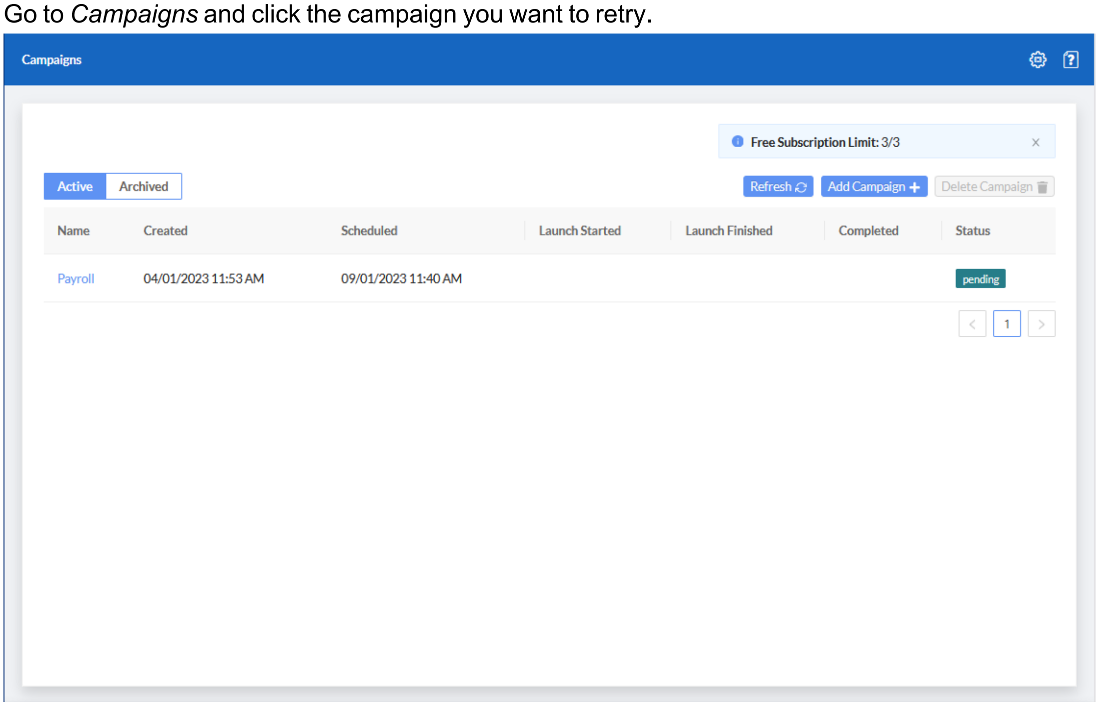
Risk Grade	The letter grade between *A and F* assigned to the group. An *A* indicates the group poses minimal risk and a *F* grade indicates the group poses the maximum risk to the organization.
Sent	The number of emails sent to the user group.
Sent Error	The number of emails that bounced.
Opened	The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

Retrying a campaign

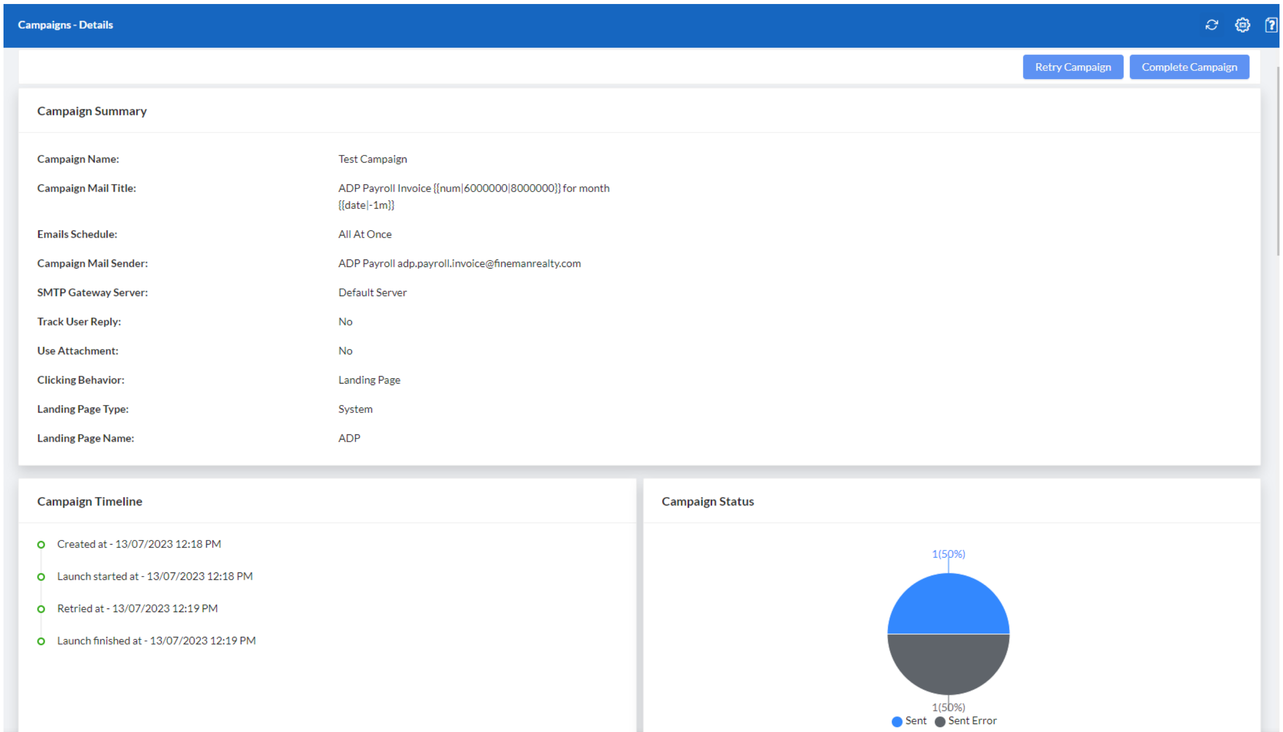
Resend emails that were not delivered or blocked by the mail server.

To retry a campaign:

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



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



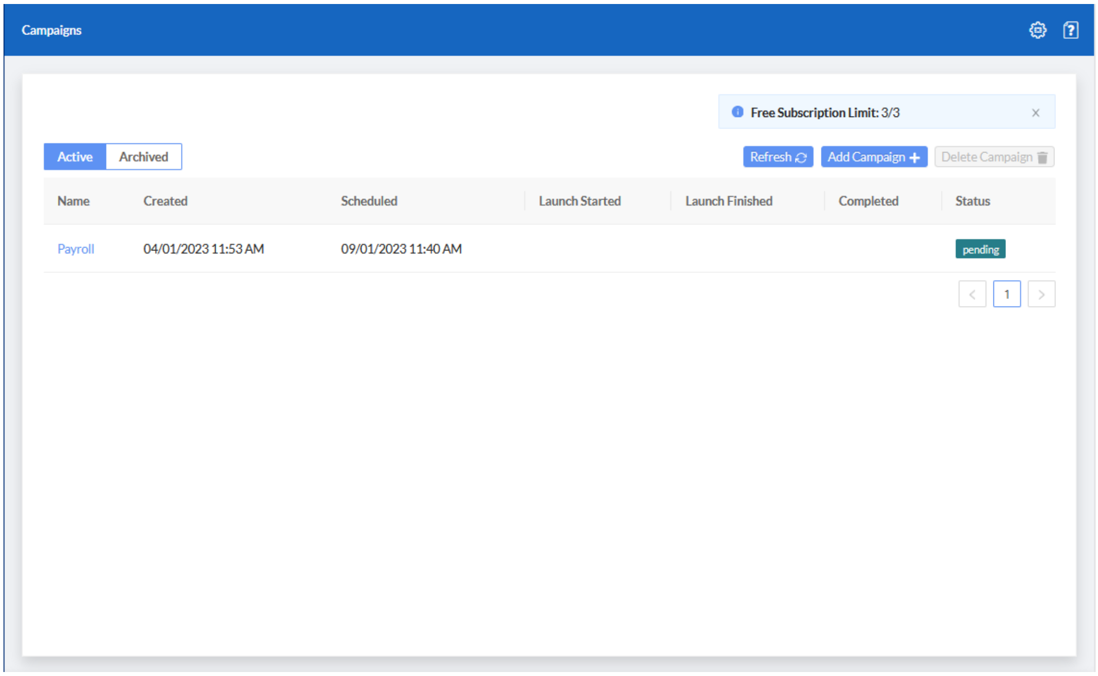
3. Click *OK*. The *Sent* metrics are updated.

Completing a campaign

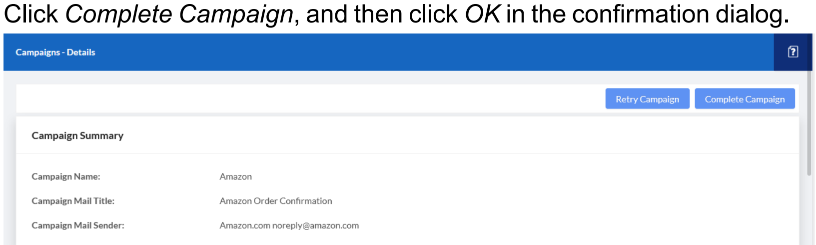
Campaigns are completed after the close date. You can complete a campaign before the campaign close date. After the campaign is completed, it is saved to the *Archived* tab.

To complete a campaign:

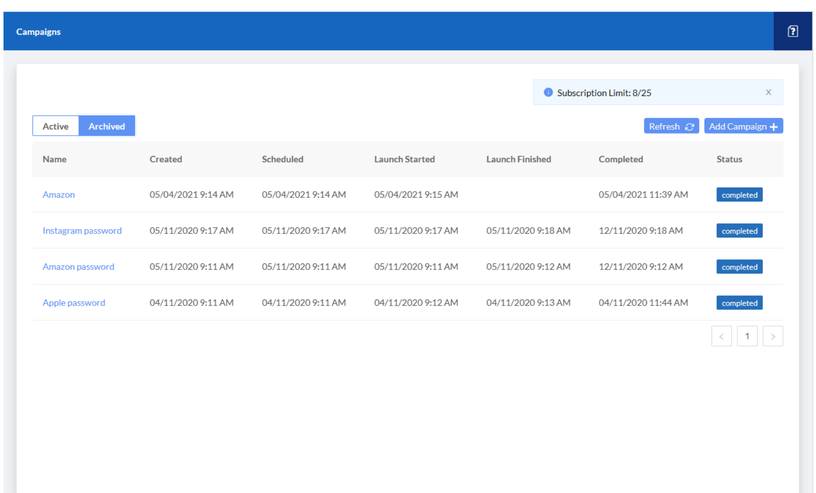
1. Go to *Campaigns* and click the name of the campaign you want to complete. The *Campaigns - Details* page opens.



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



The campaign is moved to the *Archived* tab.

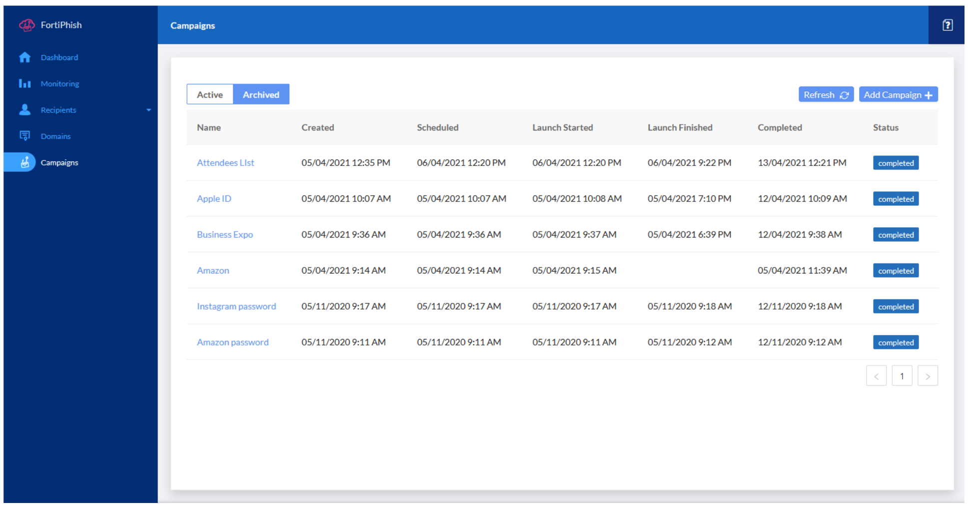


Exporting campaign statistics

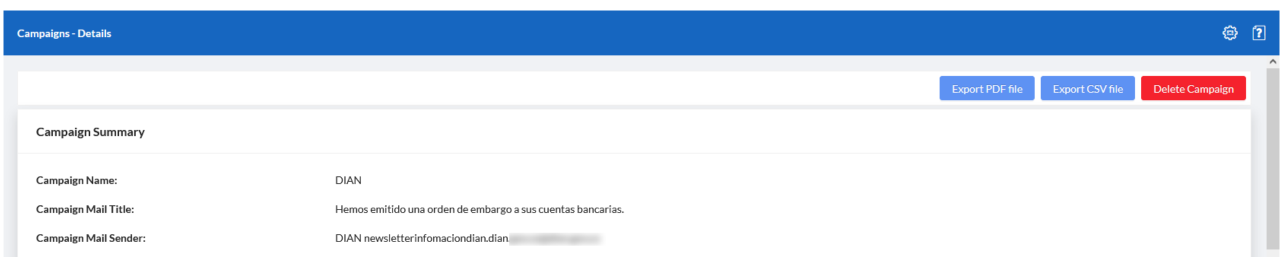
After a campaign is completed, you can export campaign data as a CSV to view the user list and behaviors. You can also generate a *FortiPhish Campaign Report* to view details about the campaign.

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	Click *Export PDF* file to generate the *FortiPhish Campaign Report* in PDF format. Once the report is ready click *Download Report PDF*. The PDF file is saved to your device. **Note**: Usually it takes a few minutes to generate the report. 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 as the statistics for *delivered*, *opened*, *clicked*, *submitted*, *QR code scanned*, *executed*, *replied*, *Risk Grade*, and *reported* emails as yes or no (*Y*/*N*) values.

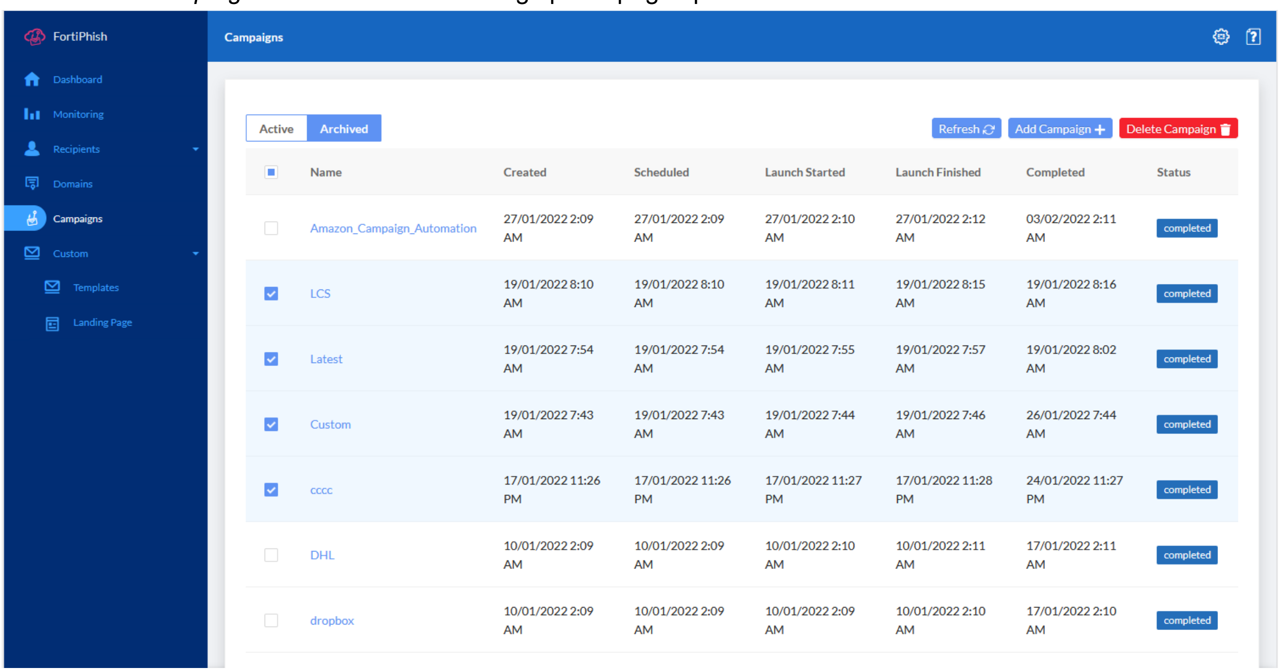
Deleting archived campaigns

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

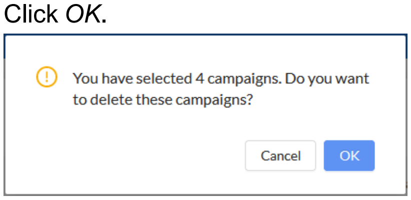
You can schedule archived campaigns to be automatically deleted at monthly intervals in the application settings page. See, Enable Auto Delete on page 69.

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.

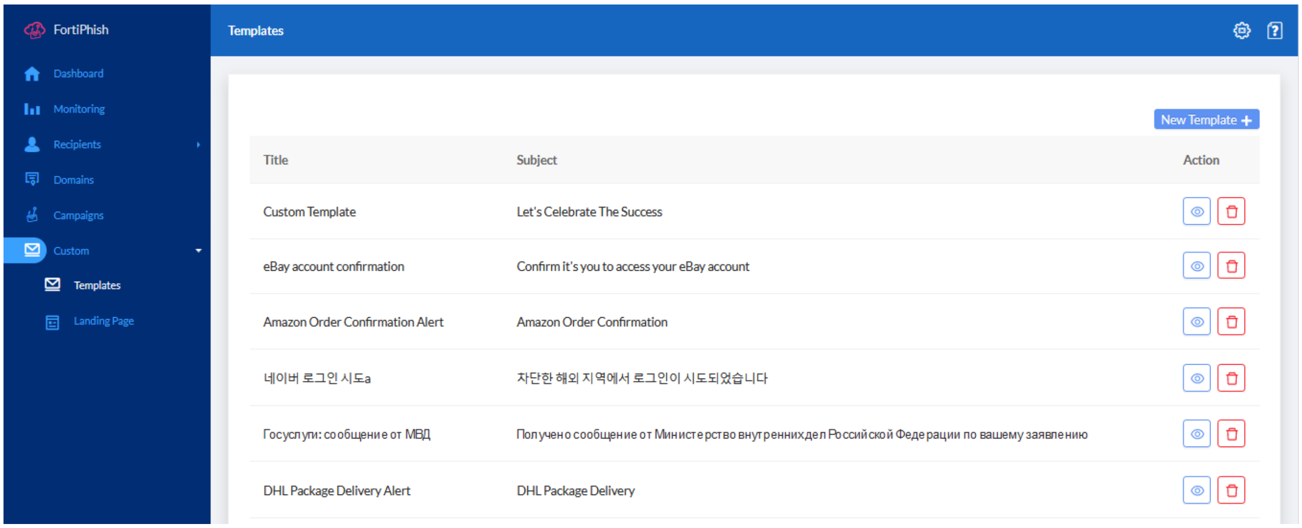


4. Click *OK*.



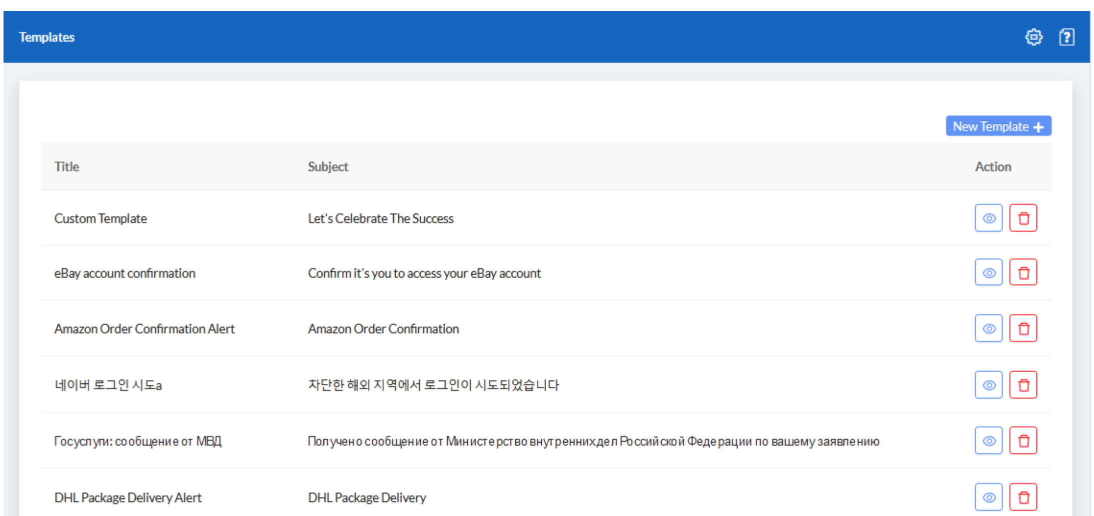
Custom

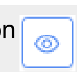
Use the pages in *Custom* view to create custom landing pages and templates for your account.



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.

Title	Enter a title for the template.
Subject	Enter the email subject.
Sender Name	Enter the sender's name.
Sender Email	Enter the sender's email address.
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.
Redirect URL	Enter the redirect URL.
Landing Page	*Landing Page* > *Custom* is selected by default. Select the landing page from the dropdown. For information about custom landing pages, see Landing page on page 65.
Attachment Filename	Click *Yes, Using Filename* and enter the filename in the text field.

4. In the text editor, compose the email body. You can insert *links*, *images*, *QR code*, and *media*.

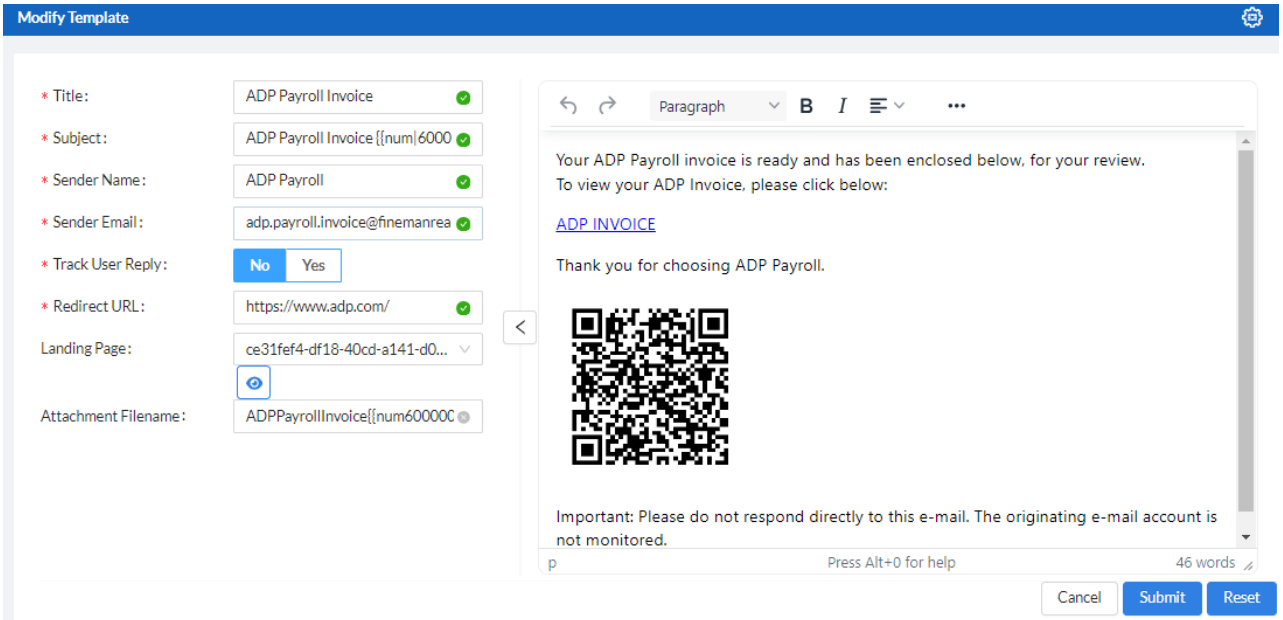
- You can use variables in the email body to generate dynamic data while the campaign is running. See, Template variables on page 48.
- QR code option is available only for *FortiPhish Premium* users. Contact Fortinet Support team to upgrade.

5. Click *Submit*. The template is added to the *Custom* tab in the *Campaigns* module. See, Creating campaigns on page 45.

Click *Reset* to clear all the entered information.

To edit a template:

1. Click the *View* icon . The *Modify Template* page opens.

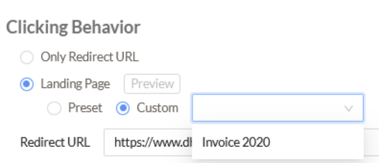


2. Update the template and click *Submit*.

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 45.

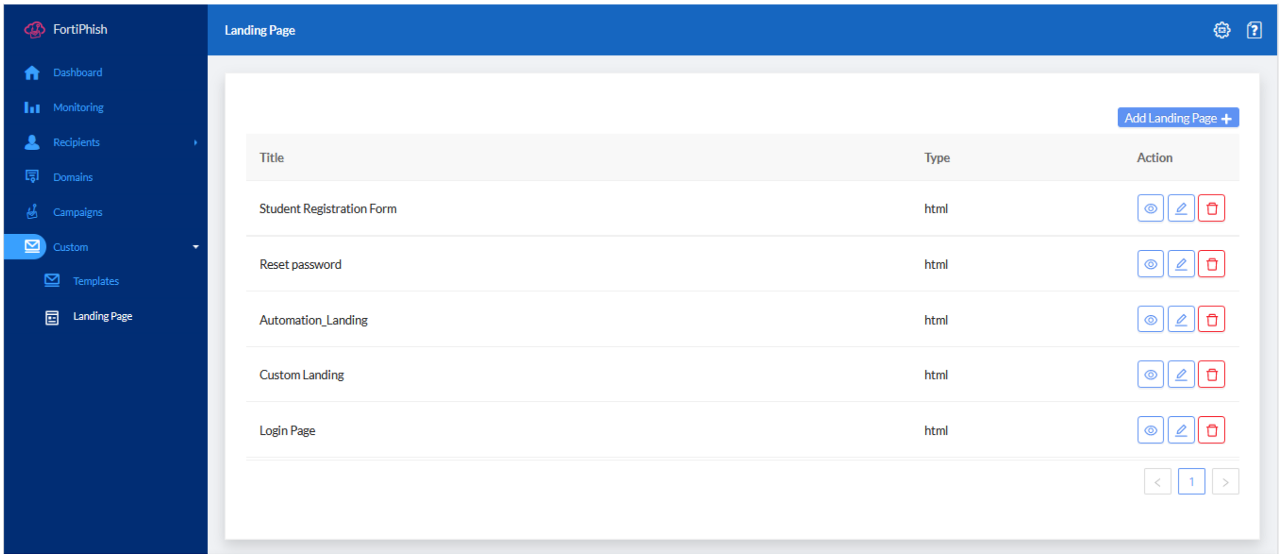


FortiPhish does not save the data entered by the user in the landing page.

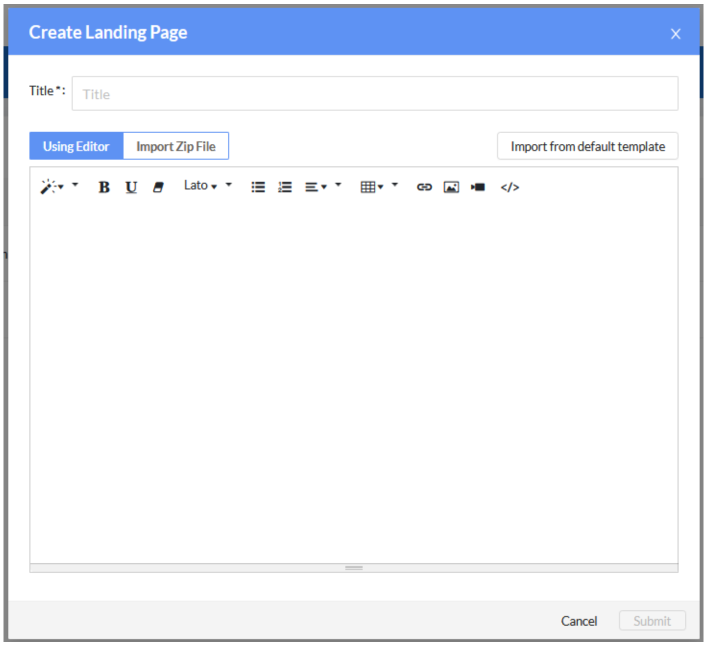
Creating custom landing pages with the editor

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 68.
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:

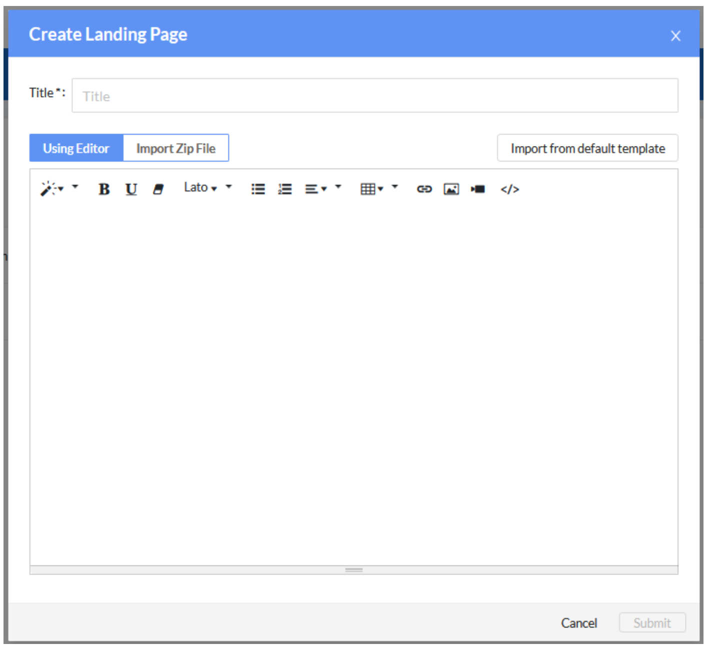
The Zip file should contain an `index.html` file that must include the following:

- 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}}"`

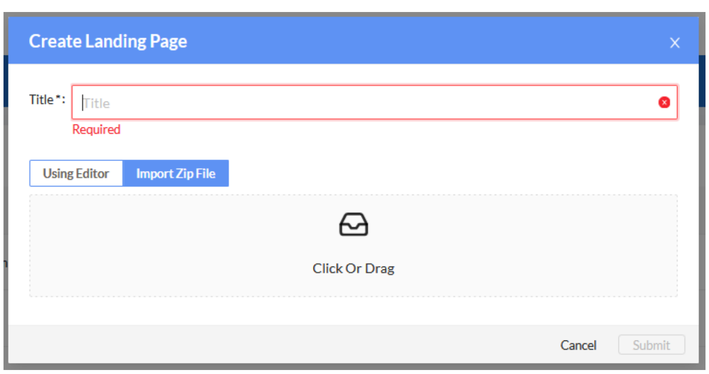
This is required for redirection of the recipient from landing page to configured redirect URL.

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 you 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 configure campaigns settings, create alert buttons, and add SMTP server accounts.

Campaigns

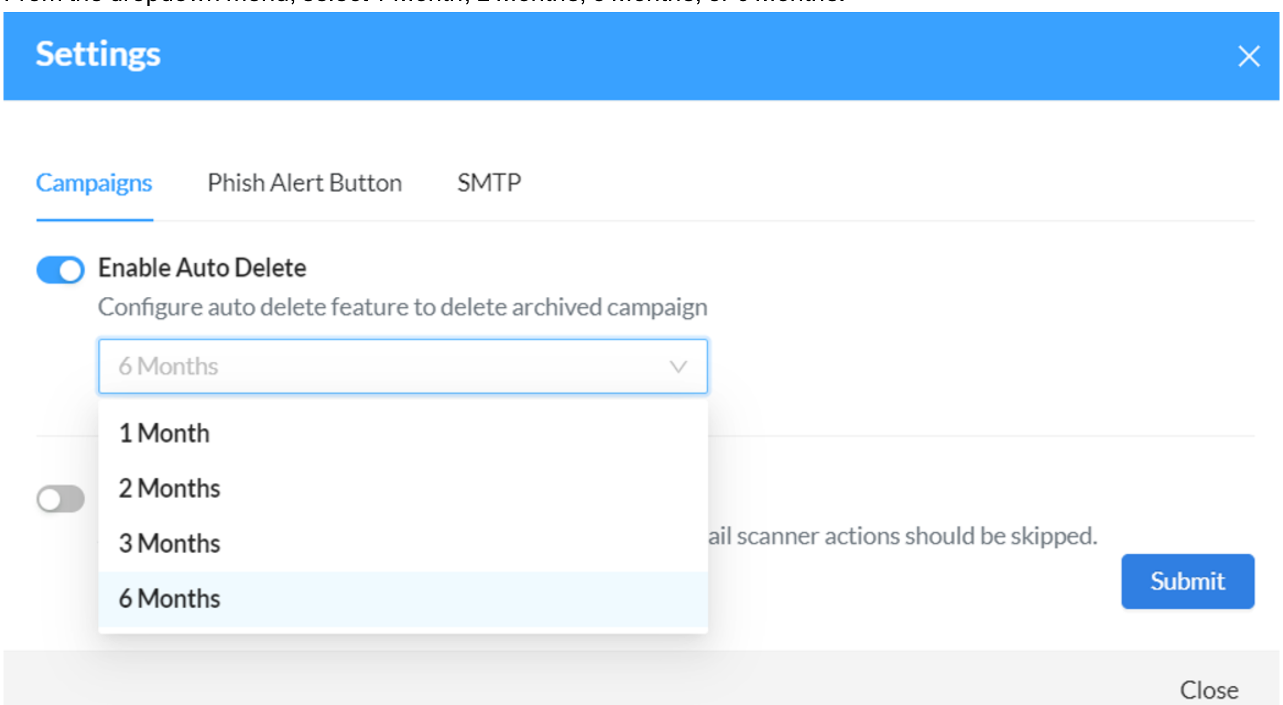
The *Settings* > *Campaigns* page allows you to automatically delete archived campaigns, and set time period to skip email scanner actions.

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. In the *Campaigns* tab, click the *Enable Auto Delete* toggle.
3. From the dropdown menu, select *1 Month*, *2 Months*, *3 Months*, or *6 Months*.



4. Click *Submit*.

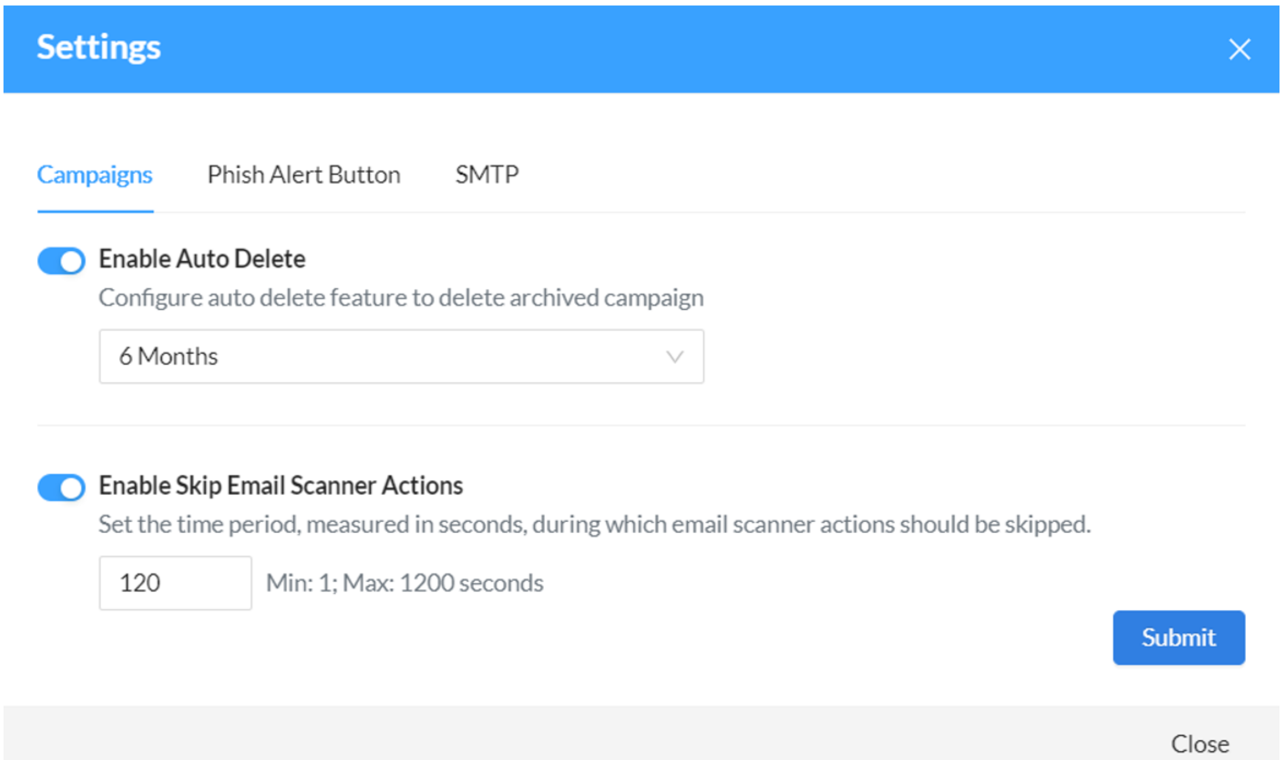
Enable Skip Email Scanner Actions

The third-party scans can sometimes trigger the FortiPhish system to incorrectly register an email as clicked, even if the user has not interacted with it. To avoid this, you can set a delay (in seconds) during which email scanner activities such as opening email, clicking links, and opening attachments are skipped. This setting reduces the false positives caused by third-party applications that scan emails for malicious content.

During the delay, emails are labeled as Email Scanned at [timestamp] in the user timeline details in FortiPhish GUI. After the delay, normal email activity display resumes, allowing you to focus on genuine user behavior.

To enable skip email scanner actions:

1. In the banner, click the gear icon.
2. In the *Campaigns* tab, click the *Enable Skip Email Scanner Actions* toggle.
3. Enter the delay time (in seconds).



4. Click *Submit*.

- The *Enable Skip Email Scanner Actions* setting is global and applies to all campaigns.
- This feature is available only for *FortiPhish Premium* users. Contact Fortinet Support team to upgrade.

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:

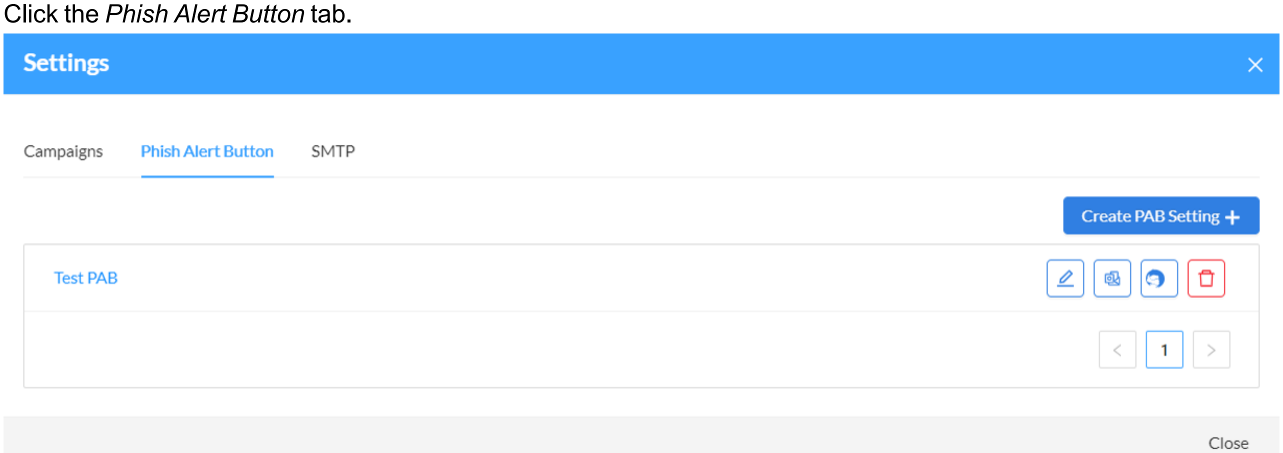
1. Create a FortiPhish alert button.
2. Manually install the button on Outlook or Thunderbird. See FortiPhish alert button compatibility matrix on page 81.
   - Adding alert buttons in Outlook on page 74
   - Adding alert buttons in Thunderbird on page 78

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 n compose alert messages. After button is created, download the PAB installation file to your device and upload the button in Outlook or Thunderbird.

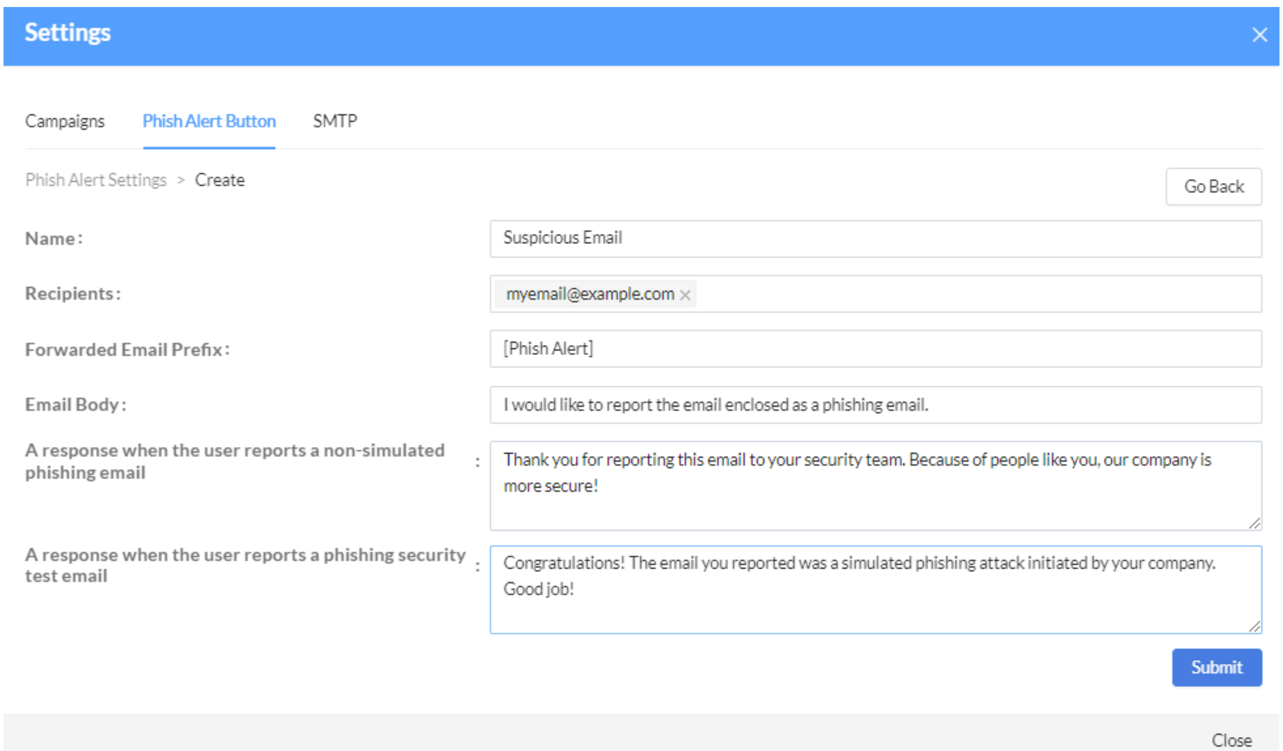
To create a FortiPhish alert button:

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



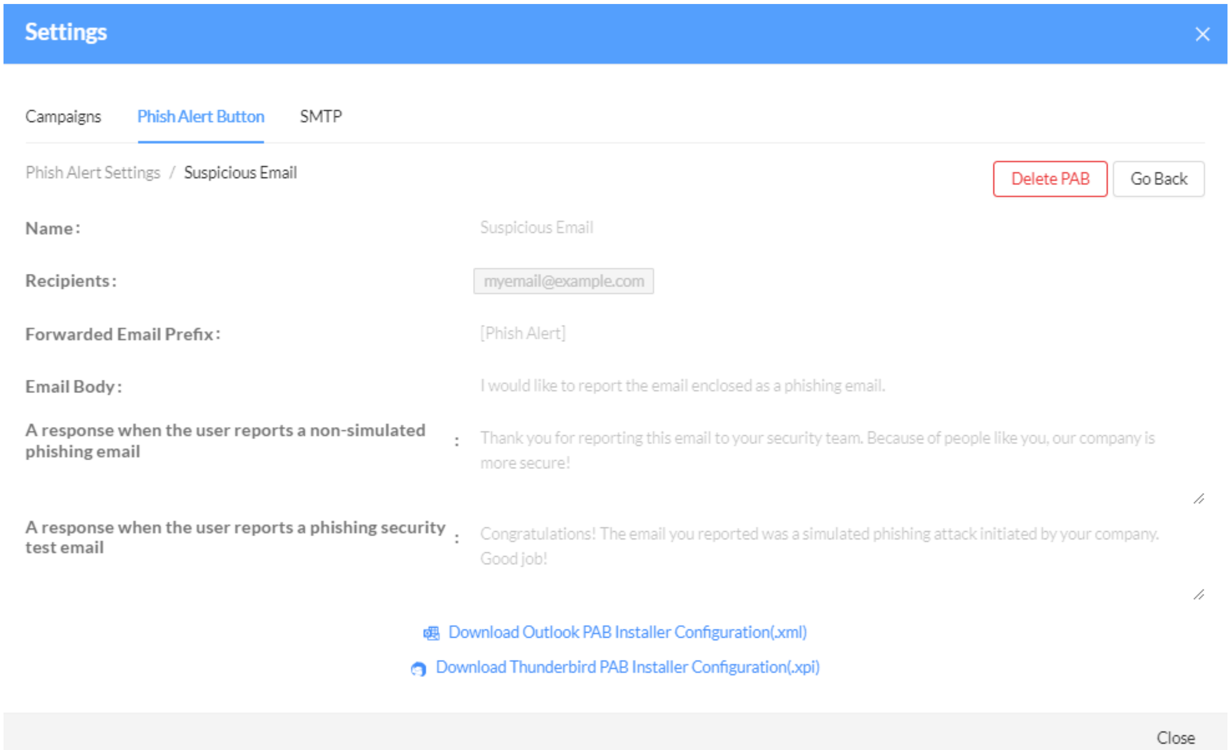
3. Click *Create PAB Setting* + to configure the alert button settings, and then click *Submit*.

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



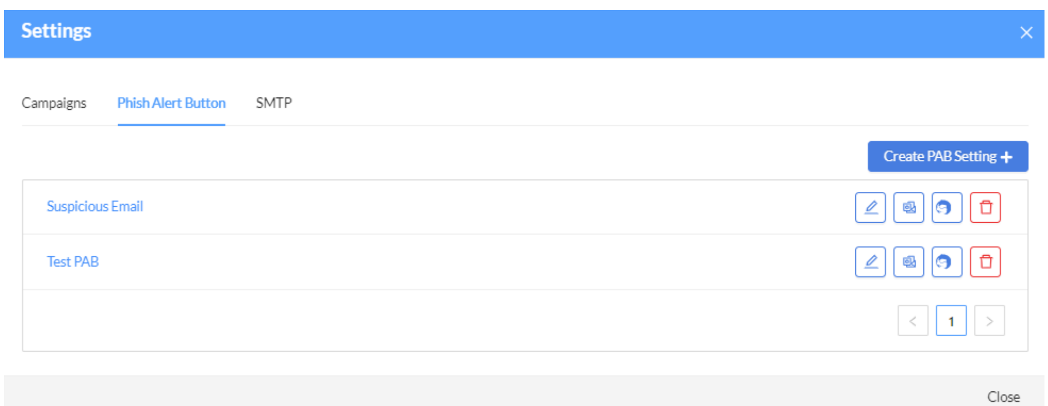
To download the PAB installation file:

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.

You can also download the PAB installation files from the *Settings* > *Phish Alert Button* tab. Click the *Download Outlook PAB Install Installer Configuration(.xml)* or *Download Thunderbird PAB Installer Configuration(.xpi)* icon next to the required alert button.



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. Click *Delete PAB*. A confirmation dialog opens.
4. Click *Yes*.

Adding alert buttons in Outlook

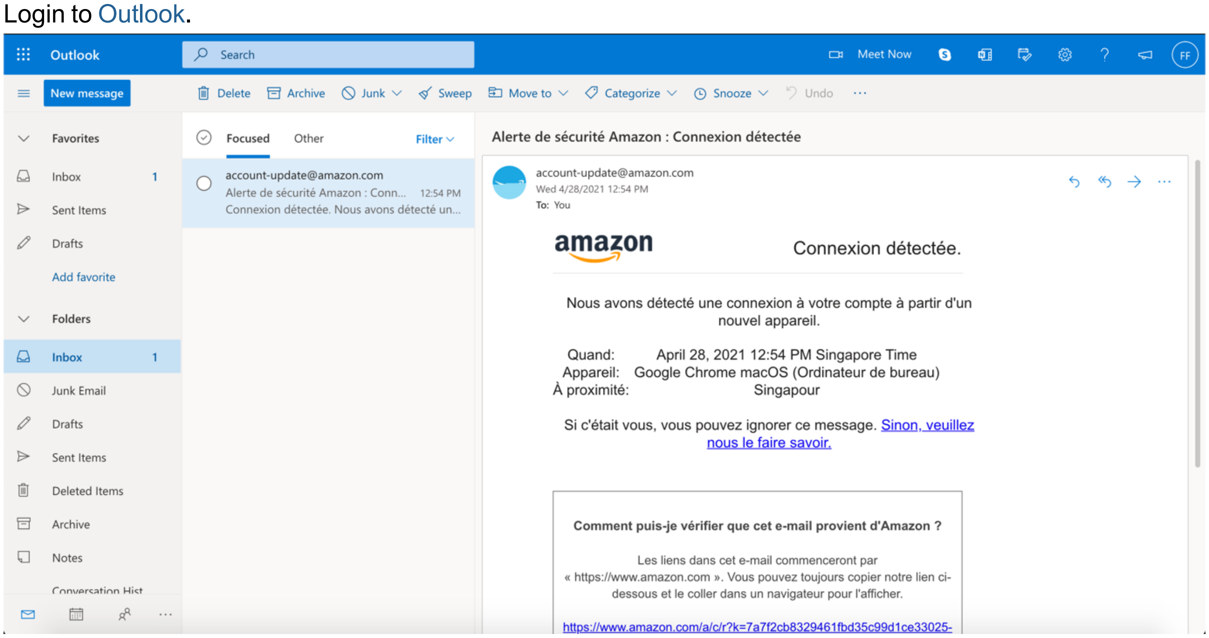
After the alert button is created, download the installation file to your device. To add the button to Outlook, open the *Add-ins* menu and upload the installation file as a custom add-in.

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

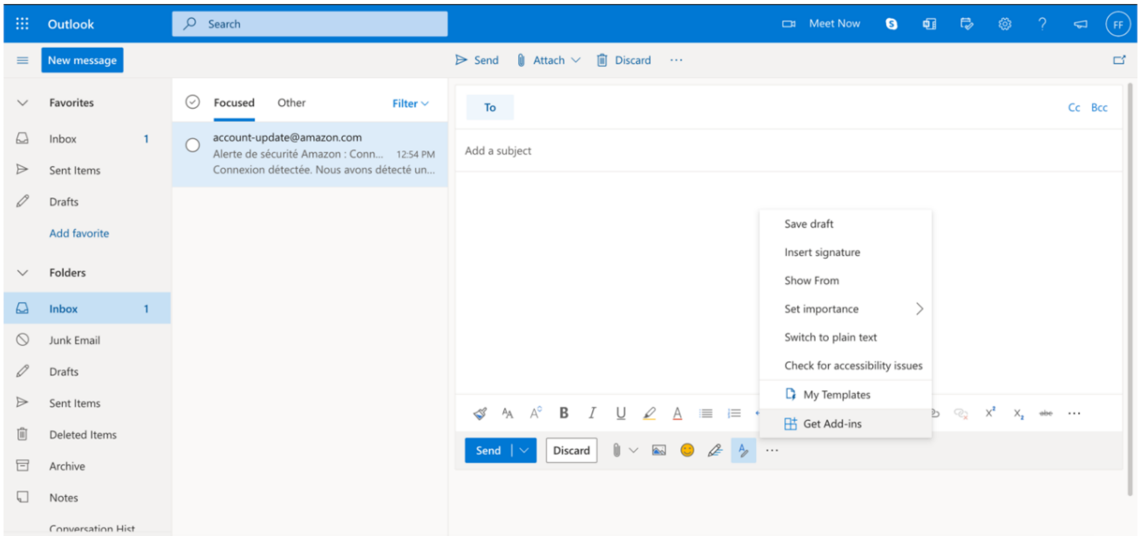
The images for the following task are based on Outlook for Office 365 online. The user interface may look different than the one you are using. For more information, please refer to the product documentation.

To install the Outlook add-in:

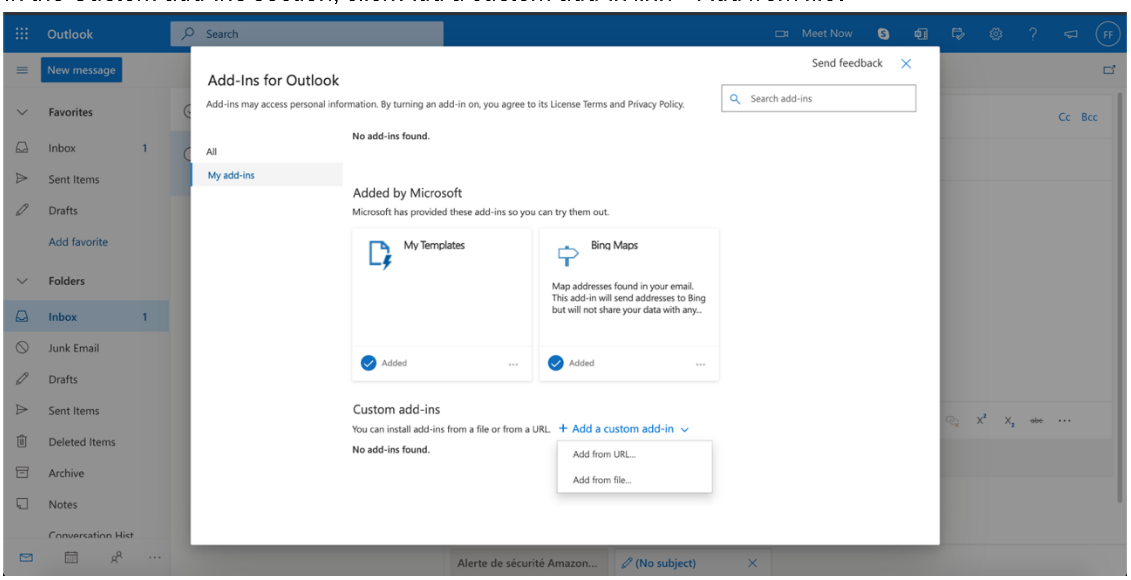
1. Login to Outlook.



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.

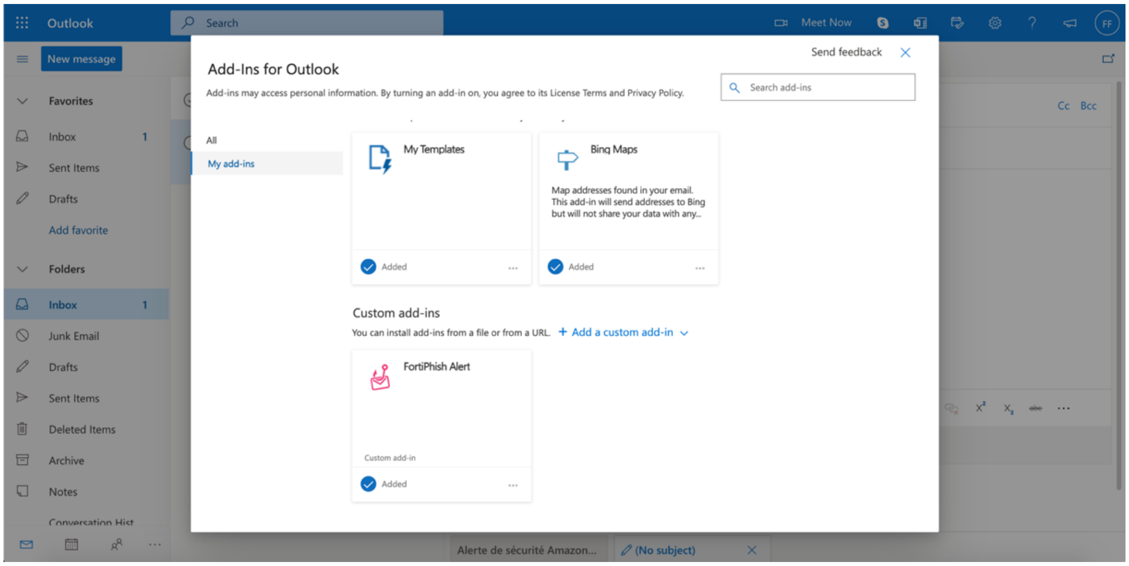


4. Install the FortiPhish alert button.
   a. Click *My add-ins*.
   b. In the *Custom add-ins* section, click *Add a custom add-in link* > *Add from file*.



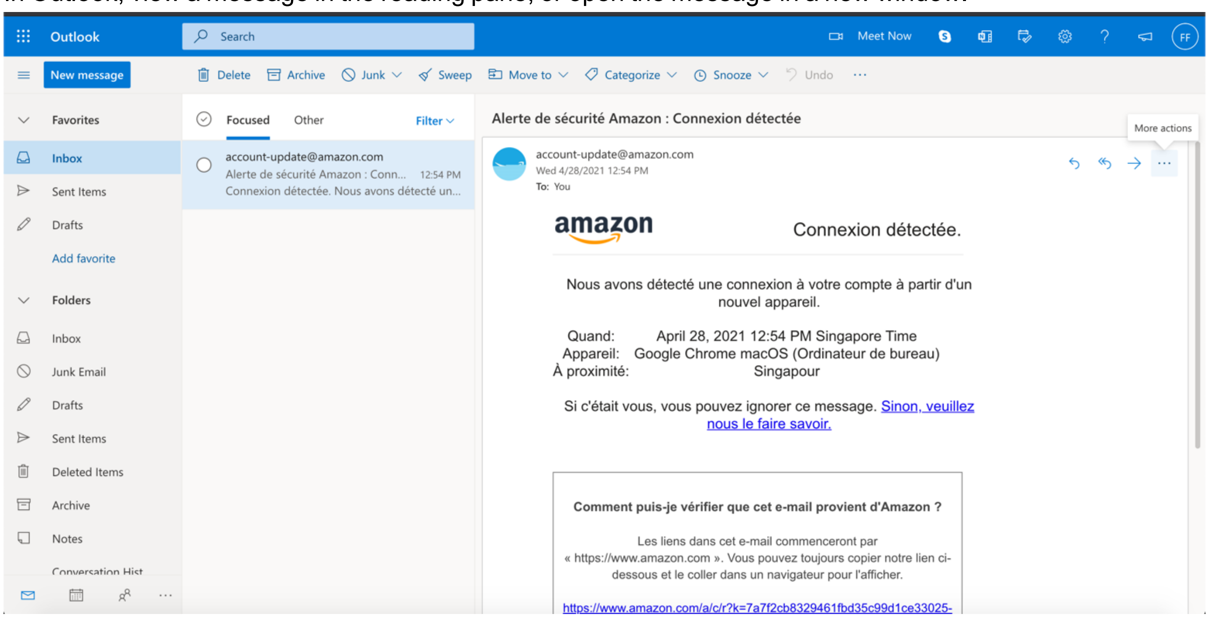
   c. Locate the installation file you downloaded and click *Open*. A *Warning* message appears.

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

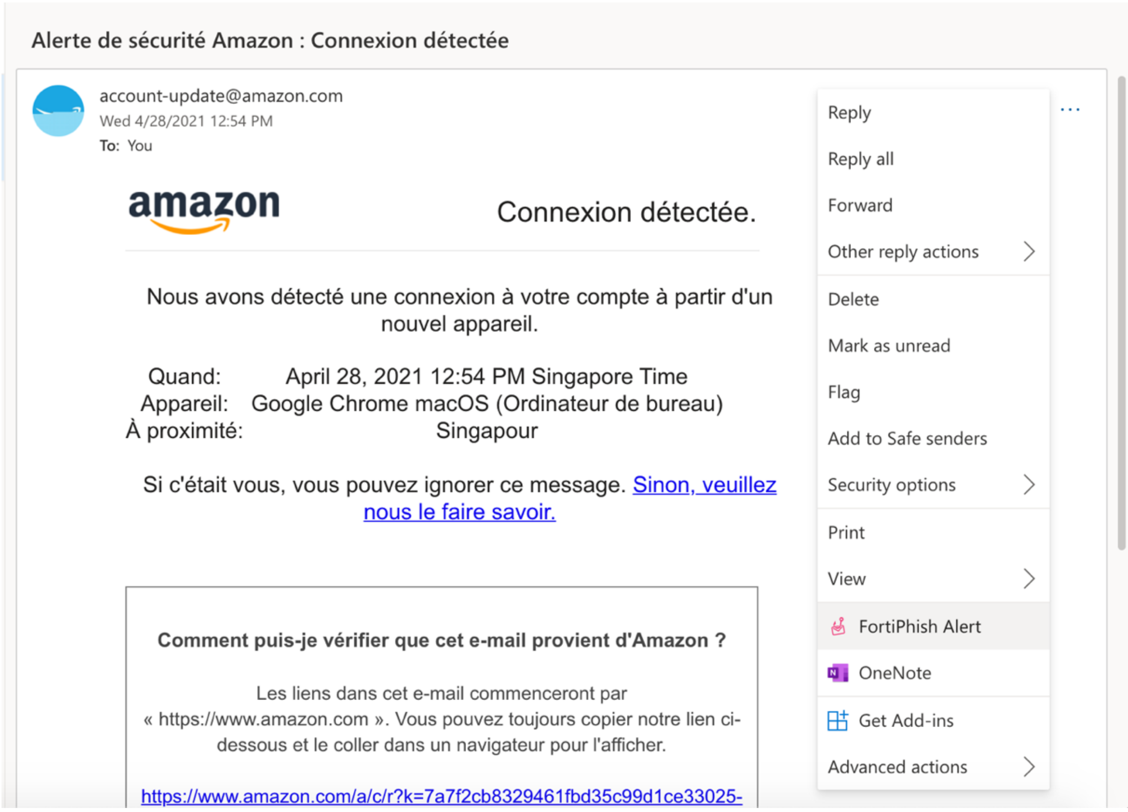


To test the FortiPhish alert button:

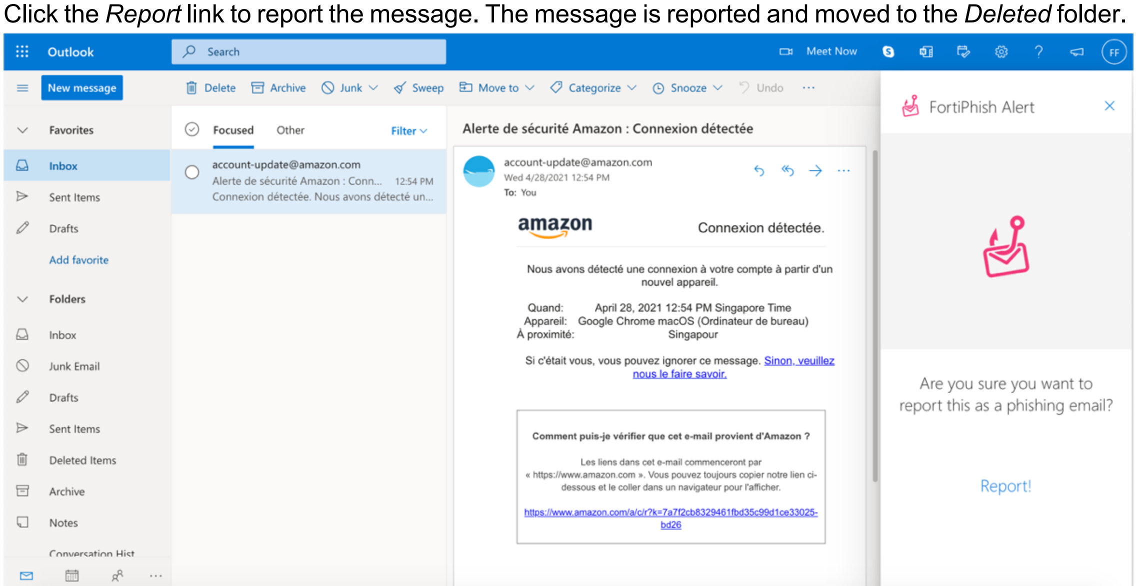
1. In Outlook, view a message in the reading pane, or open the message in a new window.



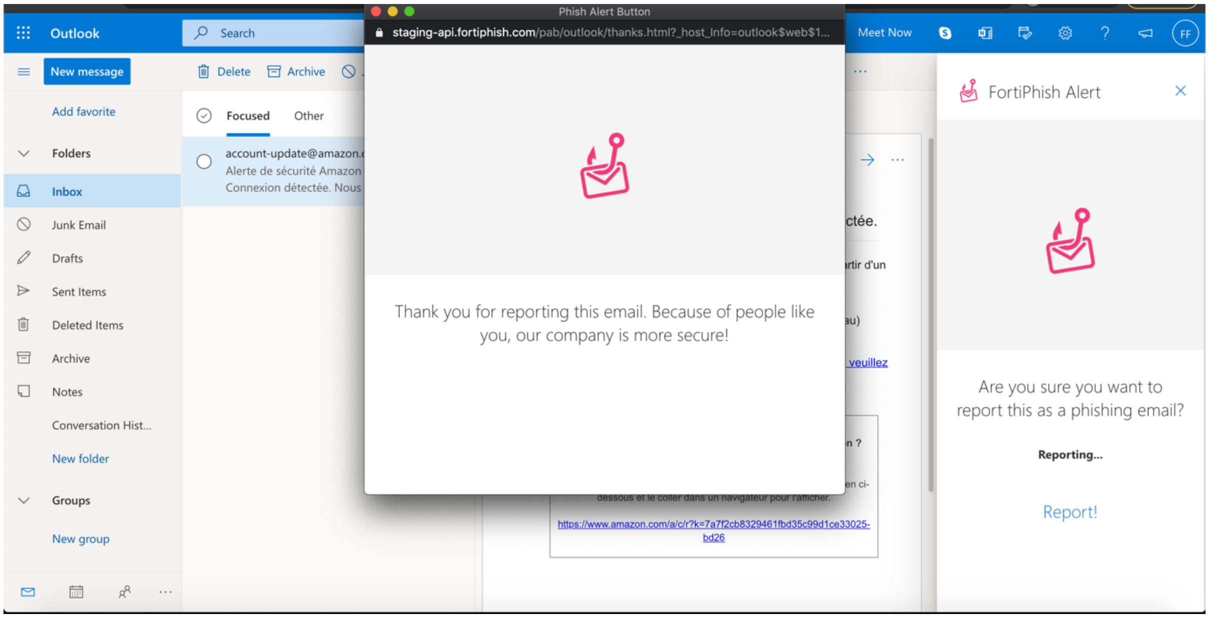
2. Click the ellipses (...) at the top-right corner of the message, and click the *FortiPhish Alert* . The *PAB add-in* task pane opens.



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

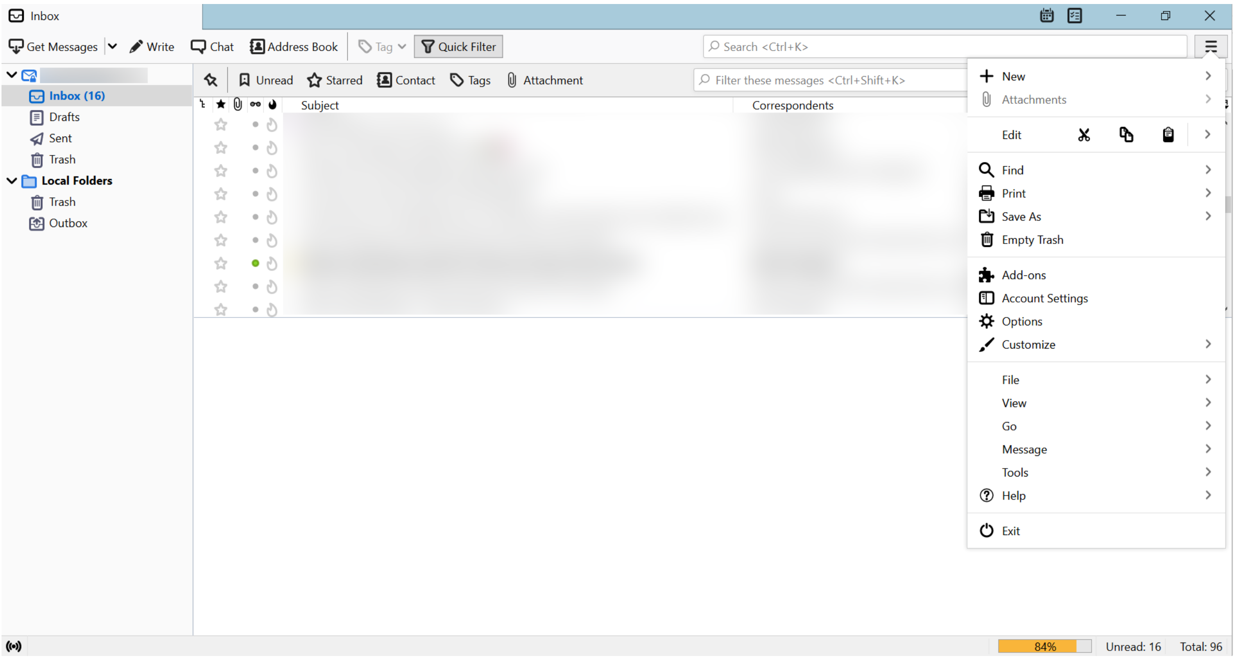
After the alert button is created, download the installation file to your device. To add the button to Thunderbird, open the *Extensions and Themes* settings and upload the installation file as a custom plug-in.

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

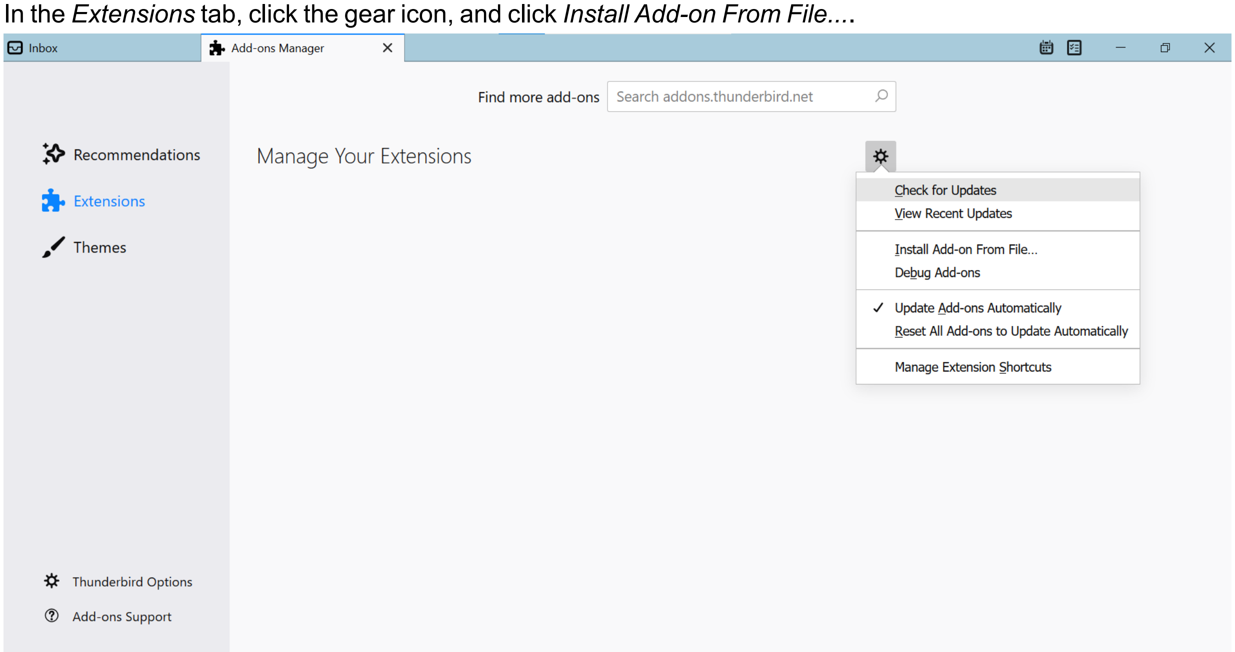
The images in the following task are based on Thunderbird for desktop v 78.12.0. The user interface may look different than the one you are using. For more information, please refer to the product documentation.

To install the FortiPhish alert button:

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

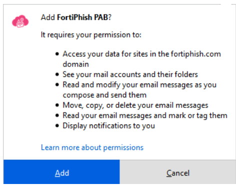


2. In the *Extensions* tab, click the gear icon, and click *Install Add-on From File...*.

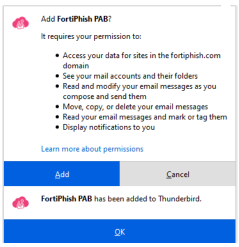


3. Navigate to the location of the *xpi* file on your device and click *Open*. The *Add FortiPhish PAB* confirmation dialog opens.

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

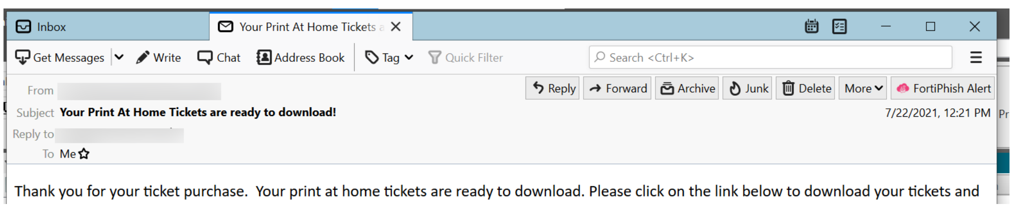


5. Click *OK* and click *Add* to close the dialog.

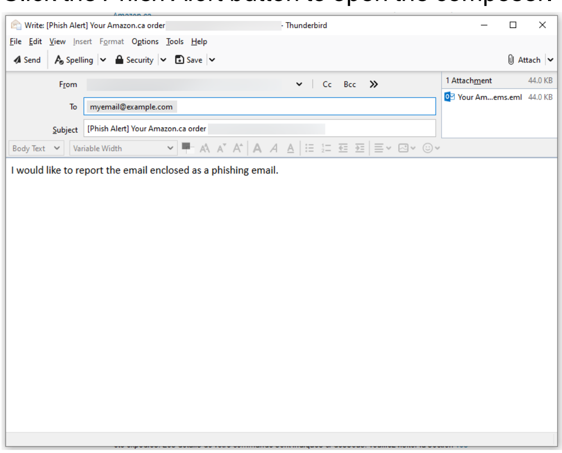


To test the alert button:

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

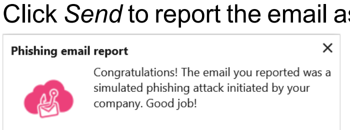


2. Click the *Phish Alert* button to open the composer. The suspicious email is attached as an EML file.



Thunderbird email recipients can edit the email message body.

3. 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		
Microsoft Windows	Outlook 2016	Compatible
	Outlook 2019	Compatible
	OWA/Outlook Online	Compatible
Apple OSX	Outlook 2016	Compatible
	Outlook 2019	Compatible
	OWA/Outlook Online	Compatible
Android	Outlook mobile app	
IOS	Outlook mobile app	

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

Outlook (Client based)		
Microsoft Windows	Outlook 2010	Compatible
	Outlook 2013	Compatible
	Outlook 2016	Compatible
	Outlook 2019	Compatible

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

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.

Name	Enter the mail server name.
Username	Enter the username to be used to authenticate with SMTP server.
Password	Enter the password to be used to authenticate with SMTP server.
Domain Name	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
Port	Enter the port number used by SMTP server to send emails.
Security	Select the method to encrypt the email traffic between the email client and the SMTP server: *SSL*,*TLS* or *STARTTLS (Opportunistic)*.
Protocol	Select the method to authenticate the user with the SMTP server: *LOGIN*, *PLAIN* and *CRAM-MD5*.

4. Slick *Save*.

Frequently Asked Questions (FAQs)

I have reached the subscription limit, what should I do next?

You have two options:

1. Purchase additional FortiPhish license to increase the subscription limit.
2. Alternatively, you can choose to wait until the beginning of the next month when the subscription limit is automatically reset to *zero.*

My campaign has failed. What are the scenarios in which campaign might fail?

Campaign may fail in the following scenarios:

- The domain of the recipients is not verified.
- A recipient group or Azure Active Directory (AD) groups used in the campaign are deleted while the campaign is in *Pending* state.
- The subscription limit is exceeded.

Can I import nested groups (group containing groups) from Azure AD?

Currently, we do not support importing nested groups from Azure AD.

www.fortinet.com