Administration Guide

FortiPhish 25.4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 22, 2025
FortiPhish 25.4.0 Administration Guide
67-254-1214662-20251022

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-10-22	Initial release.
2025-11-12	Updated FortiPhish portal topic.

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.

FortiPhish portal

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

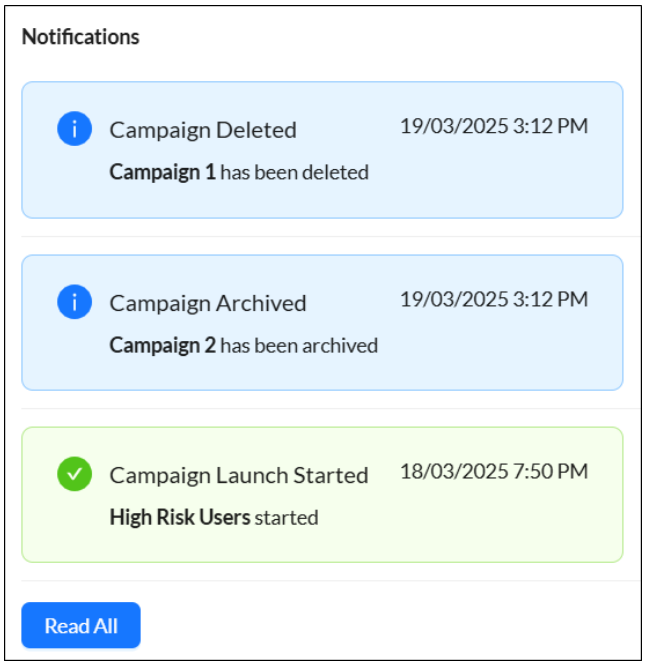
For an optimal user experience, use a desktop computer to view the FortiPhish portal.

Accessing the FortiPhish portal

To access the FortiPhish portal, use the URL: https://fortiphish.com.

Notifications

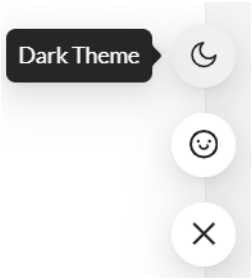
The *Notifications* icon in the banner alerts you when there is activity in your account. The message background color indicates the importance of the message. The background color changes to gray when a message is viewed or acknowledged. Scroll down to view the notification history. Click *Read All*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



Customizing FortiPhish portal

You can customize the language and theme of the FortiPhish portal.

- To customize the language, click the *Language* icon and select the desired language.
- To change the portal's theme to dark mode, click the floating menu in the lower-right corner and select *Dark theme*.



User Management

The FortiPhish portal supports the following user management models.

- IAM User Model
- Sub User Model

For more information, see Identity & Access Management (IAM) > User management models.

IAM User Model

The IAM User Model uses portal-based permission profiles to manage user access and asset permissions.

A master user (Account Owner) who creates the FortiCloud account, can access the IAM portal. IAM Users have access to the FortiPhish portal based on the permissions set by the master user for the IAM portal. Sub users cannot access the IAM Portal.

IAM user types

FortiPhish supports the following IAM user types.

- **IAM Users**: IAM users can access FortiPhish, with a FortiCloud account. Each IAM account requires an *Account ID/Alias*, *User Name*, and *password* to log in to a portal. Administrators can assign permission profiles to an IAM user or to an IAM user group.

  For information on creating and managing IAM users, see IAM Users.
- **API Users**: API users can access FortiPhish, through the API. API users can only use OAuth 2.0 for authentication to access web service APIs. API user IDs and passwords are generated by the IAM service portal. One FortiCloud account can have multiple API users. The IAM service administrator can define the user's permissions.

  For information on creating and managing API users, see API Users.
- **External IdP roles**: External IdP roles allow external users to log in to a cloud portal using their organization's ID provider. External IdP roles are authenticated with a custom login page. After the user is authenticated, they are redirected to a jump page where they can select the cloud portal(s) assigned to their account.

  For information on enrolling for and configuring external IdP, see External IdP. For information on creating and managing, external IdP roles, see External IdP roles.

IAM user roles

FortiPhish supports the following IAM user roles.

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.

Sub User Model

The Sub User model, includes two user types.

- The **Master User**, who creates the FortiCloud account, has full administrative permissions, including the ability to create users and assign their permissions and assets.
- A **Sub User** is assigned access permissions by the Master User, with either full (with limitations) or limited access.

The Sub User model allows only one Master User per account. See Identity & Access Management (IAM) > User management models.

This model will be deprecated in the near future. It is strongly recommended that you use the IAM User Model to take full advantage of the new features.

Multitenancy

FortiPhish leverages FortiCloud Organization to provide multi-tenancy, enabling Managed Security Service Providers (MSSPs) and customers to manage multiple accounts.

FortiCloud Organizations facilitate account management. However, data within each Organization and Organizational Unit (OU) remains separate.

For example, consider an Organization with OUs named *Region A* and *Region B*. If a user has access to Member Accounts within both Region A and Region B, they can view campaign details specific to each region (for example, Campaign 1 in Region A and Campaign 2 in Region B). However, a combined view of all campaigns across Region A and Region B is not available.

- For more information on Organization concepts, see Key concepts.
- For more information on creating and managing Organizations, see Overview of creating and managing Organizations.
- For more information on managing Organization users, see Organization user management.

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.

Dashboard

The *Dashboard* provides an overview of responses across campaigns, high risk users, high risk groups, and risk and awareness factor scores.

The *Dashboard* displays the following monitors.

- Campaign Analysis
- Risk Grade
- High Risk Users
- High Risk Groups

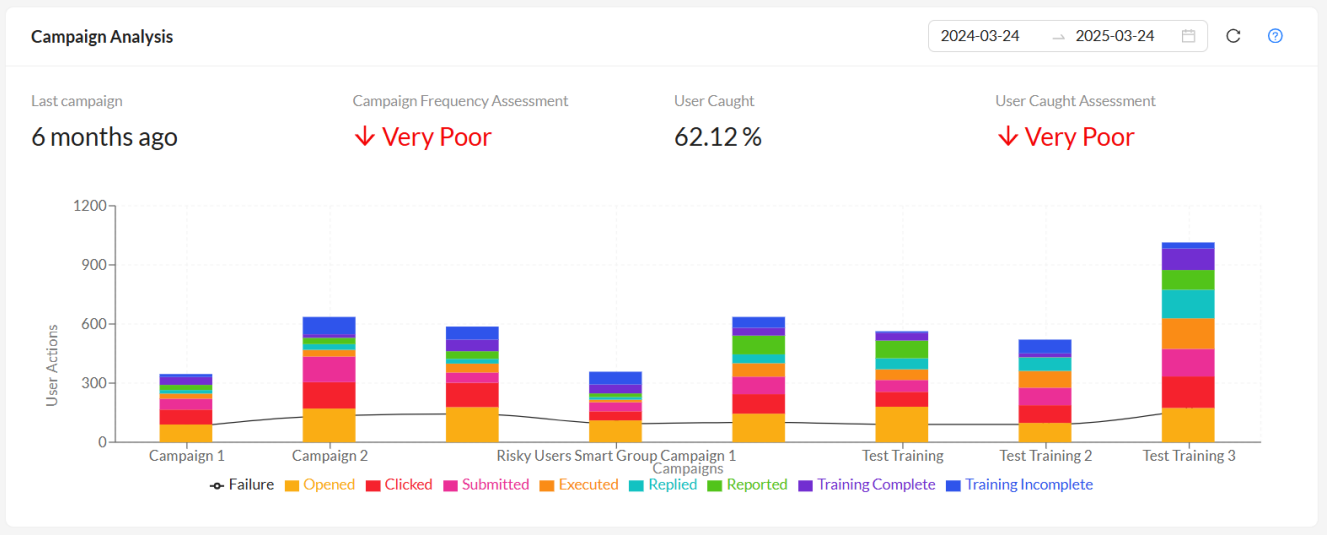
To filter the dashboard data, see Filtering Dashboard.

Campaign Analysis

Displays the campaign statistics over time including, the duration since the last campaign, the campaign frequency assessment, the number and the percentage of users caught. To launch a new campaign, click the *Create a Campaign* link. See Creating campaigns on page 47.

Hover over the stacked bar chart to view the following information:

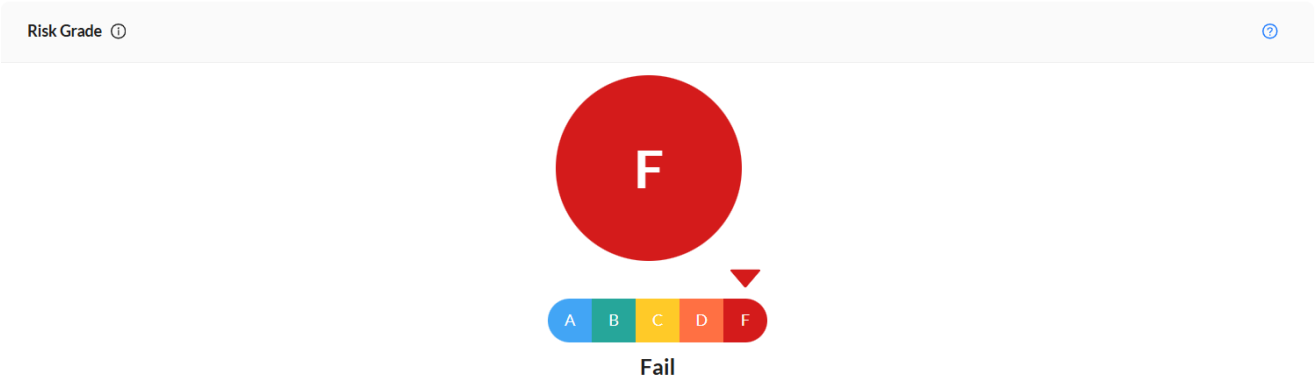
Total	Total number of recipients in the campaign.
Risk Grade	The Risk Grade of the campaign. Value is *NA* if the campaign is in the processing state.
Opened	The number of recipients who opened the email.
Clicked	The number of recipients who clicked the redirect link.
QR Code Scanned	The number of recipients 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 who reported the phishing 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.



Risk Grade

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.



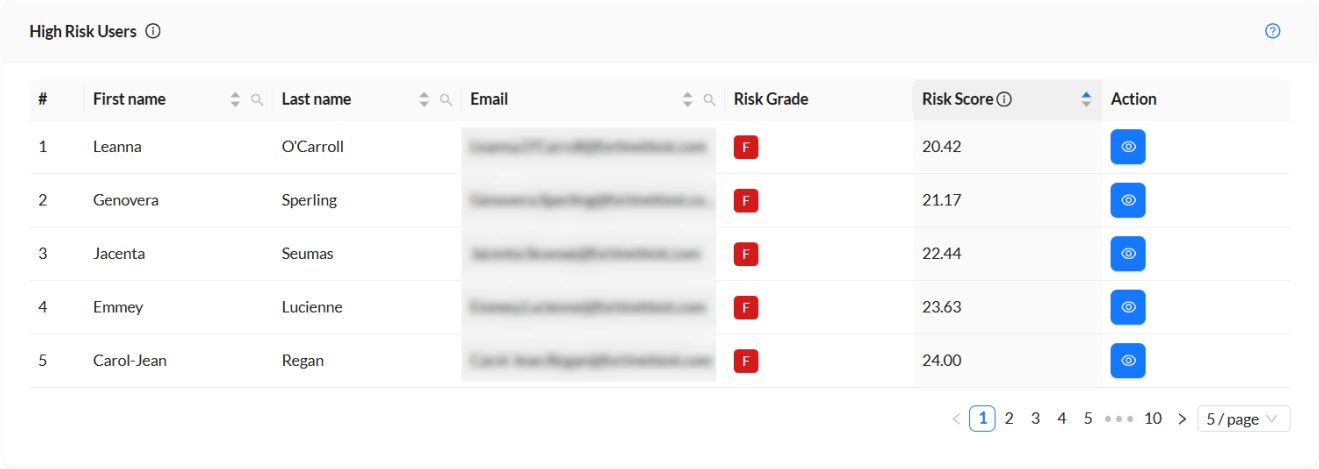
High Risk Users

Displays a list of users who have consistently exhibited high-risk behavior across all time periods. The following information is displayed.

First Name	The user's first name.
Last Name	The user's last name.
Email	The user's email address.
Risk Grade	Risk grade assigned to the user.
Risk Score	A numerical value indicating the user's risk level. A lower risk score signifies a higher risk.

Action	Click *View* icon to view the detailed information of the user. See User Profile.

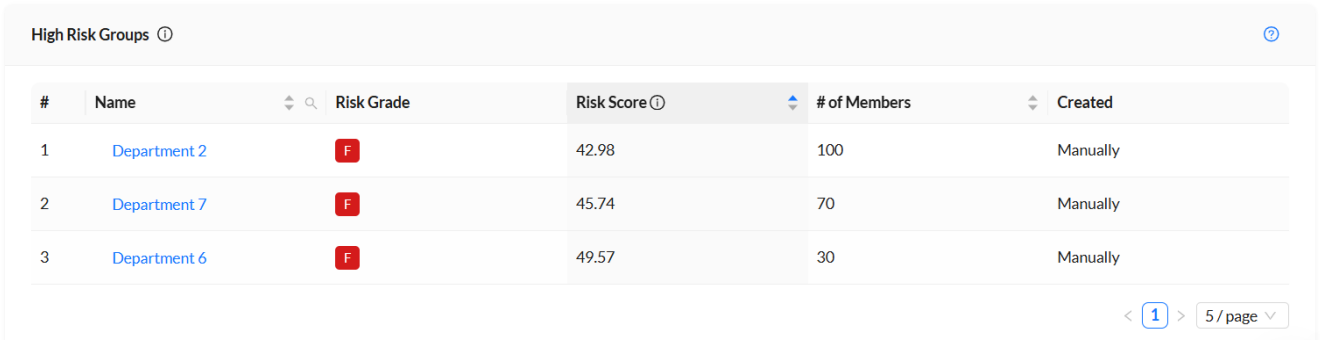
The default risk grade for users not performing any action has been changed from *F* to *B*. Previous campaign ratings remain unaffected.



High Risk Groups

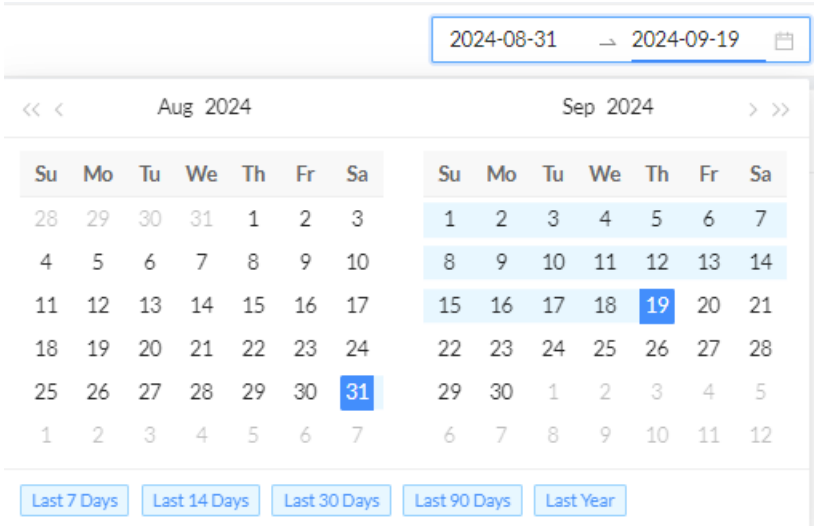
Displays a list of user groups who have consistently exhibited high-risk behavior across all time periods. The following information is displayed.

Name	The name of the group. Clicking the name will take you to the group's detailed information page.
Risk Grade	Risk grade assigned to the group.
Risk Score	A numerical value indicating the user's risk level. A lower risk score signifies a higher risk.
# of Members	The total number of users in the group.
Created	The method used to create the group (*Manually*, *Azure AD*, or *Smart Group*).



Filtering Dashboard

Use date picker on top right corner to filter the *Campaign Analysis* and *Awareness Factors* data by selected time period. You can either select *Start Date* and *End Date* or a quick filter (Last 7, 14, 30, 90 days, or one year).



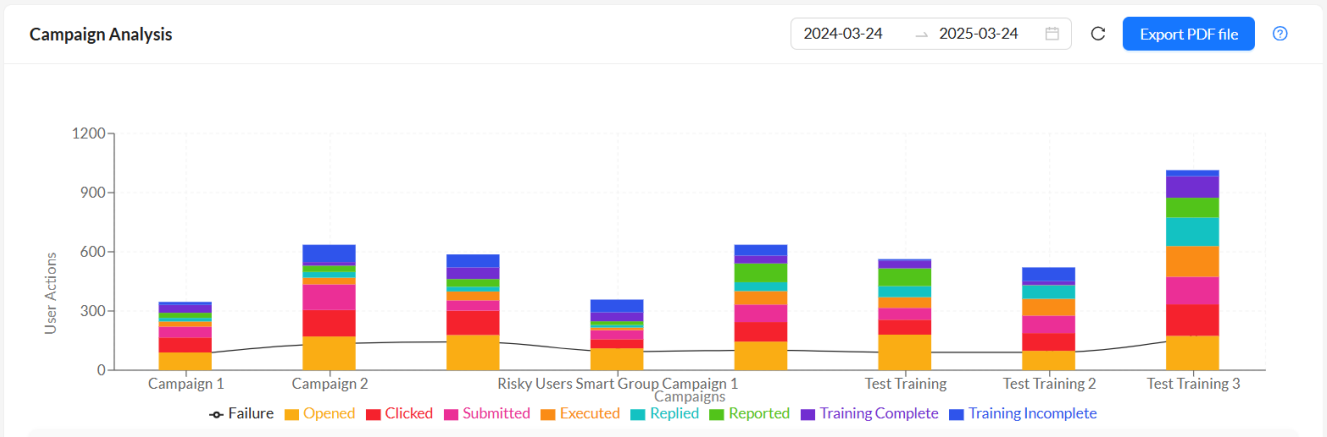
Click *Refresh* icon to manually refresh the dashboard data.

Monitoring

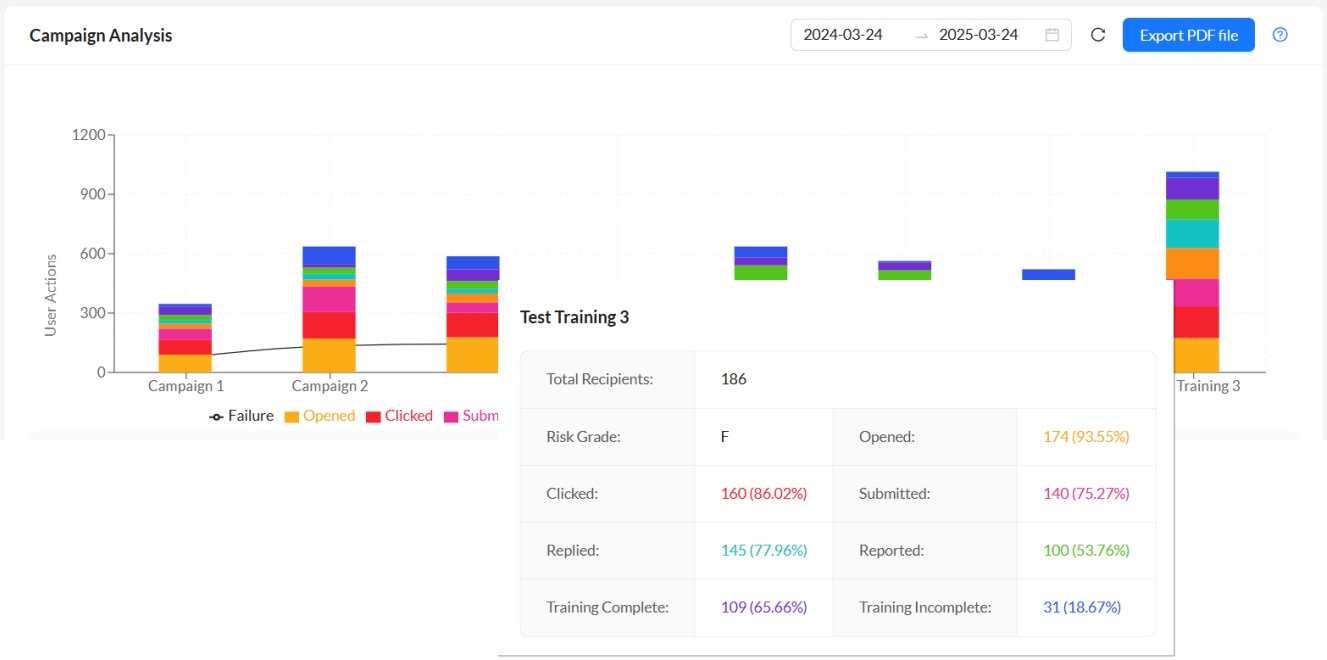
The *Monitoring* page provides an overview of campaign activity. Use this page to view click-rates, user group analysis, user profiles, and campaign response comparison charts.

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.

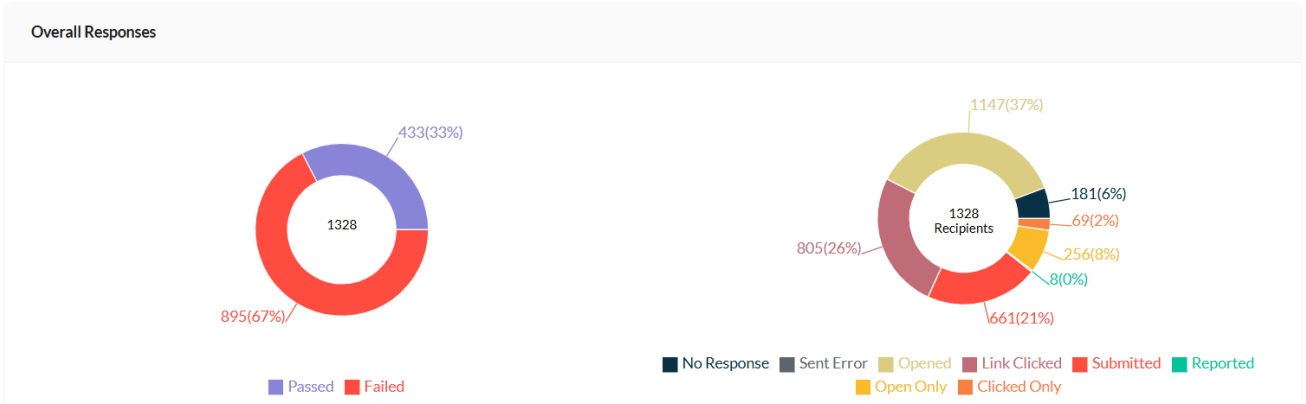


The chart displays the following information:

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.

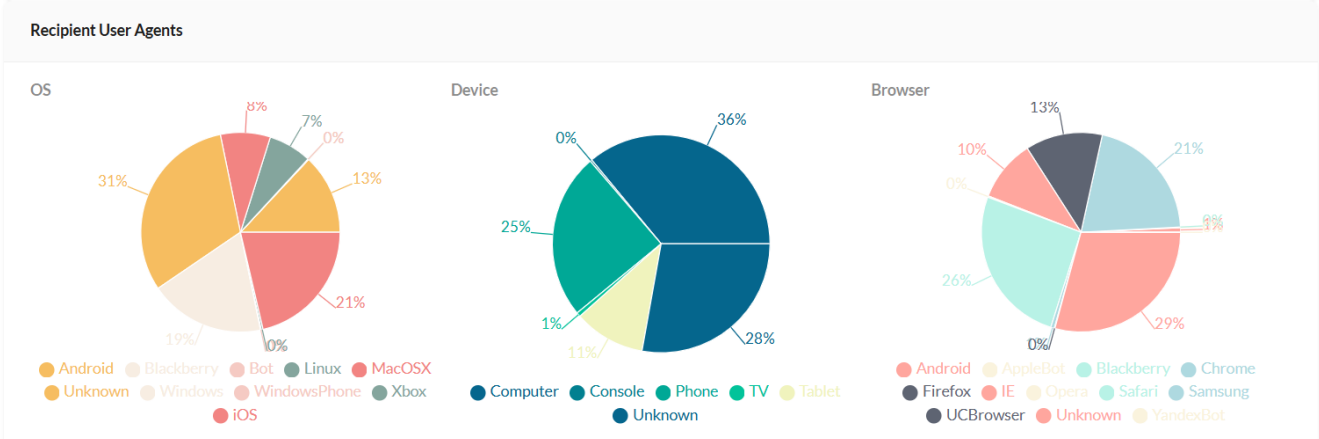


The *Overall Responses* monitor displays the following information:

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.

Recipient User Agents

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

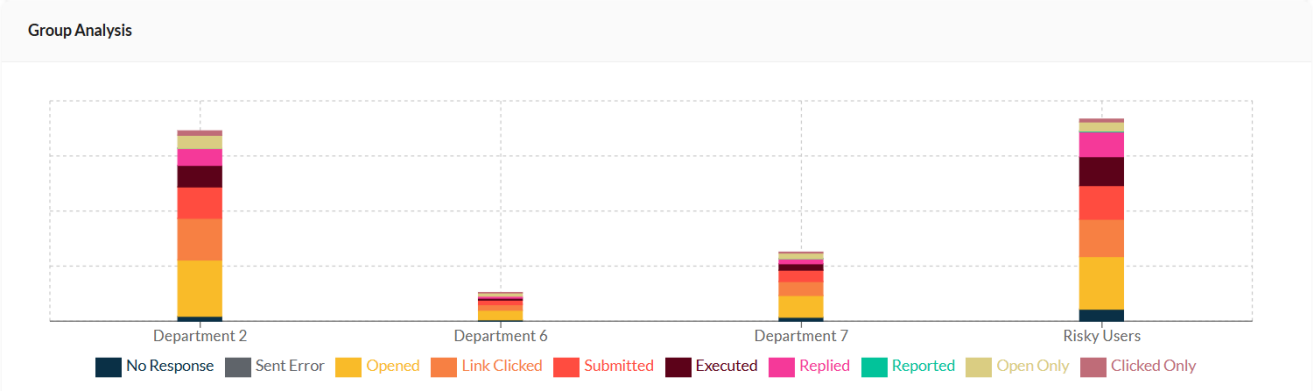


The *Recipient User Agents* monitor displays the following information:

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.

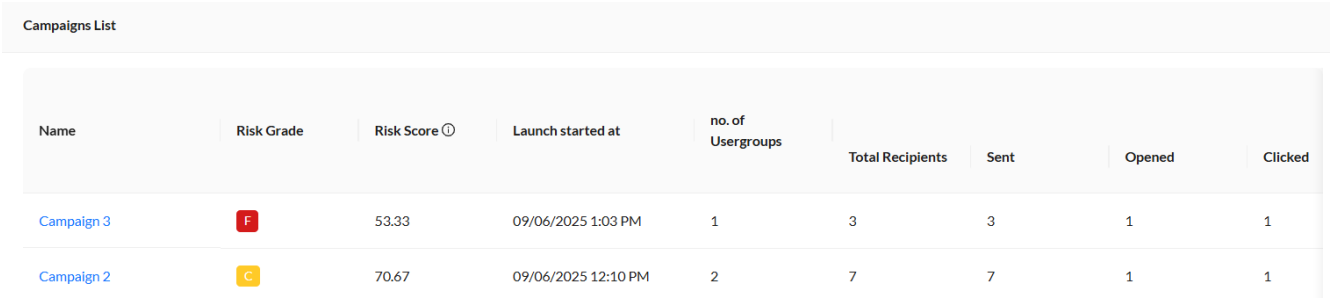


The *Group Analysis* monitor displays the following information:

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 List

The *Campaigns List* 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:

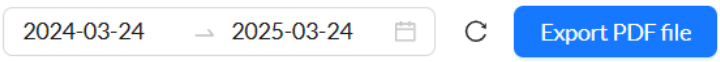
Risk Grade	The letter grade between *A and F* assigned to the campaign. An *A* indicates the user poses minimal risk and a *F* grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be *NA*on the *Dashboard* and *Monitoring* pages.
Risk Score	A numerical value indicating the user's risk level. A lower risk score signifies a higher risk.
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*.
2. Select the *Start Date* and *End Date*, and click *Export PDF File*.



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
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

Name	Description	Example
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. This number should be the same as the *# of Total recipients* in the *Overall*section.	5 Recipients
# 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%)

Name	Description	Example
# 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%)
# 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%)

Name	Description	Example
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*.	
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

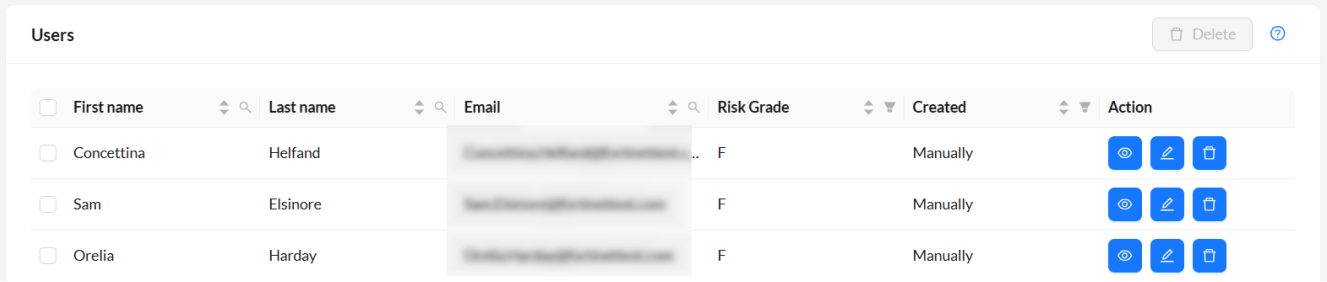
Recipients

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 left.

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

To view detailed user information:

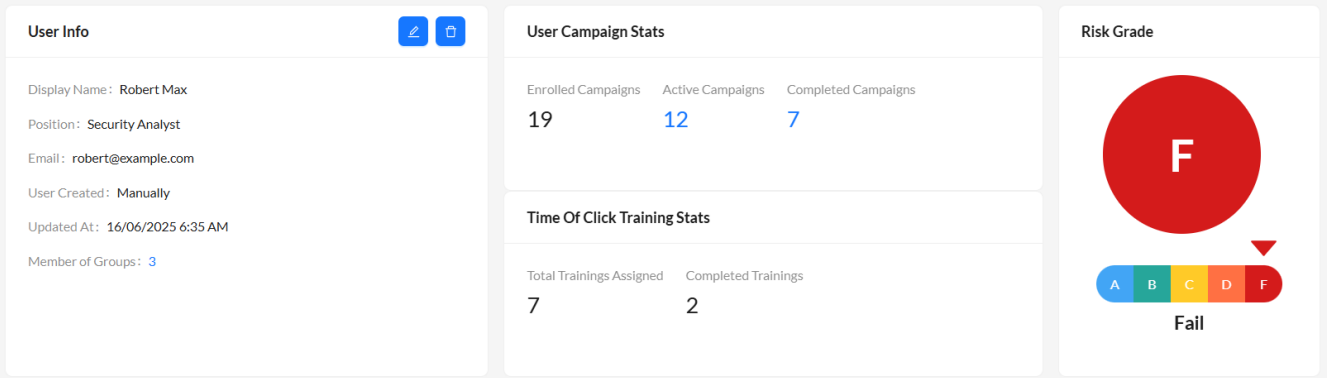
1. Navigate to *Recipients* > *Users*.
2. Click *View User* icon next to the user you want to view.
3. *User Profile* page is displayed. See User Profile.

User Profile

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

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

User Information



The user information section displays the following information.

Display Name	The name of the user.
Position	The job title or role of the user.
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.

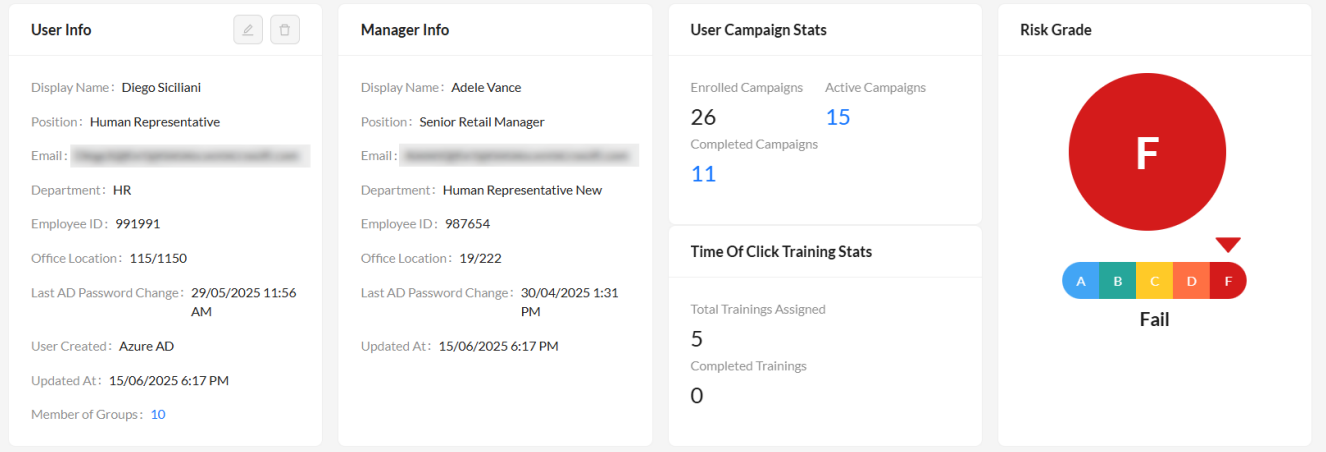
Completed Campaigns	The count of completed campaigns the user was part of. Click count to navigate to *Completed Campaigns* section.
Total Trainings Assigned	The total count of trainings assigned to the user.
Completed Trainings	The count of trainings the user has completed.
Risk Rating	The letter grade 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.

Azure AD User Information

For users imported from Azure AD, FortiPhish displays additional attributes when available, supplementing the general user information.



Department	The user's department.
Employee ID	The user's employee identification number.
Office Location	The user's primary office location.
Last AD Password Change	The timestamp of the user's last password change in Azure AD.
User Created	Displays the method of user creation, *Azure AD*.

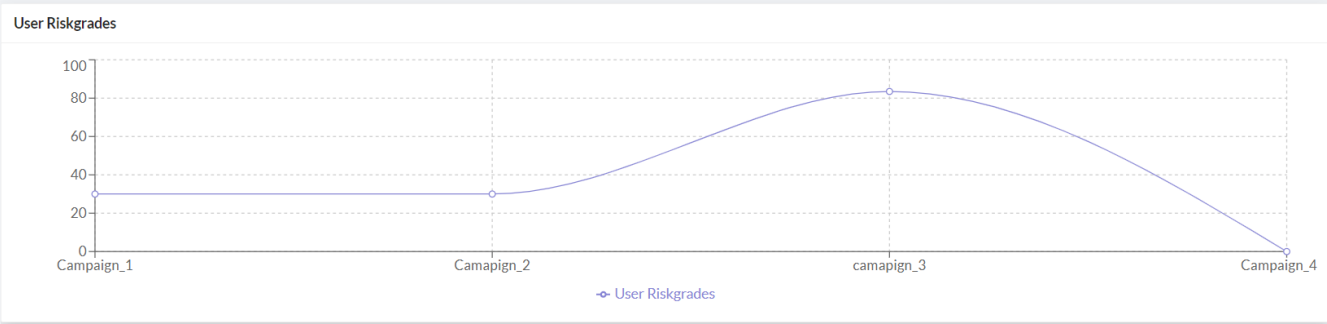
Additionally, a separate **Manager Info** card appears if the manager's information is available from Azure AD.

Display Name	The manager's name.
Position	The manager's job title or role.

Email	The manager's email address.
Department	The manager's department.
Employee ID	The manager's employee identification number.
Office Location	The manager's office location.
Last AD Password Change	The timestamp of the manager's last password change in Azure AD.
Updated At	The timestamp of the last modification to the manager's data.

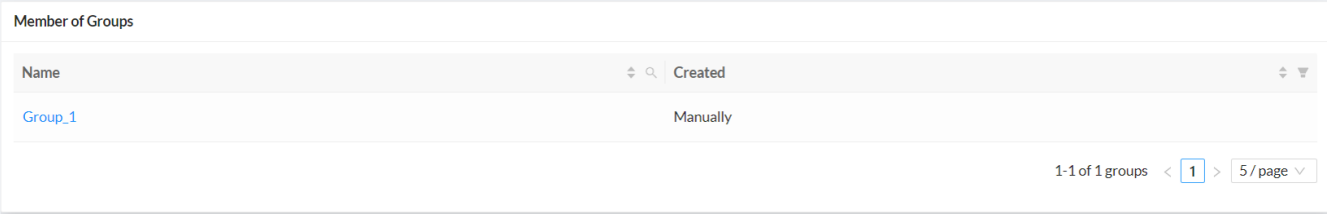
User Risk Grades

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



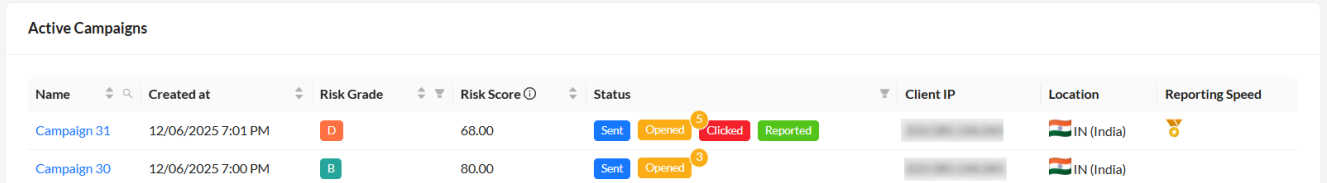
Member of Groups

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



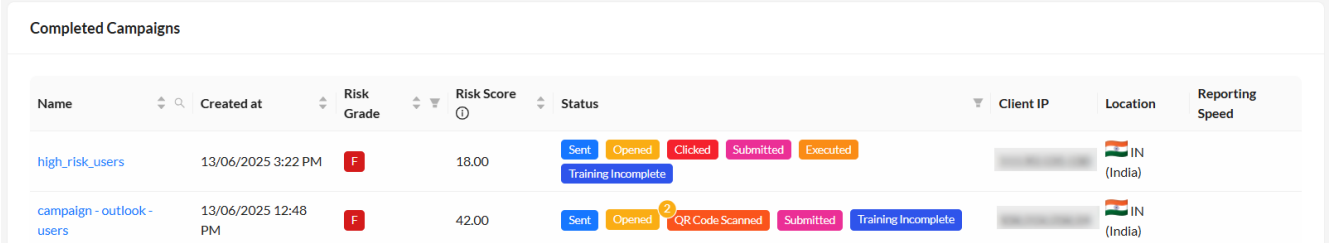
Active Campaigns

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.



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.



Groups

Groups are distribution lists for your campaigns. A Group is required even if you are sending an email to only one user. Groups 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.

Additionally, you can create *Smart Groups* to dynamically assign users based on defined rules. See, Smart Group

Use the *Groups* page to:

- Create a group list
- Perform a bulk user import
- Add imported user to a group
- View user details
- Update user details
- Filtering group list
- Hide/Unhide a group
- Exporting group details
- Deleting a group

To create a group:

1. Go to *Recipients* > *Groups* and click *Create* > *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 *Create* > *Group*.
2. Click *CSV* > *Download csv template*. The user group template is downloaded to your computer.

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

To add imported users to a group:

1. Click *Create* > *Group*.
2. On the Group creation page, click *View imported users*. The *Users* window opens, listing all users currently added to FortiPhish, including users imported from *LDAP*, *Azure AD*, *SCIM*, or manually created users.
3. Optionally, use the filter in *Created* field to view the users based on their import source.
4. Select the check box next to the desired users, and click *Import selected*. Alternatively, click *Import all* to add every user currently displayed in the list.

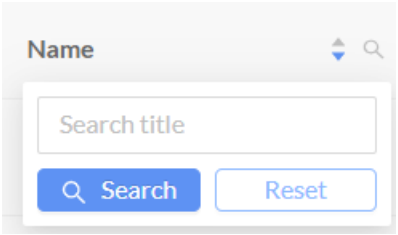
To update a user's details:

1. Go to *Recipients* > *Groups*, 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.

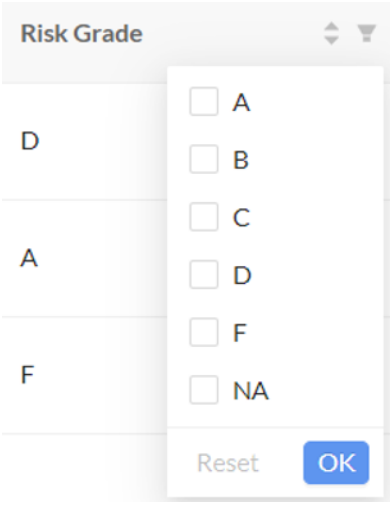
To update details of a user imported from Azure AD, the changes must be made within Azure AD server and then synced back to FortiPhish.

Filtering groups

To filter the group, 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.

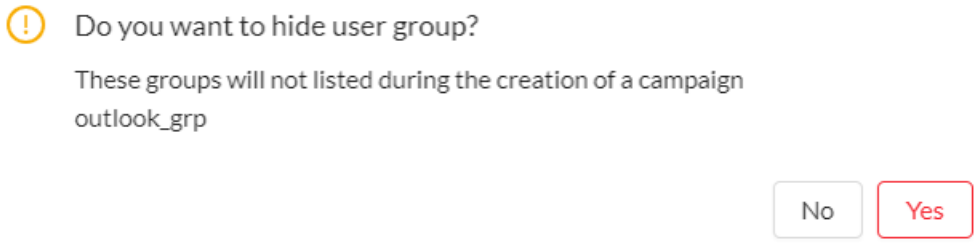


Hide/Unhide a group

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*.

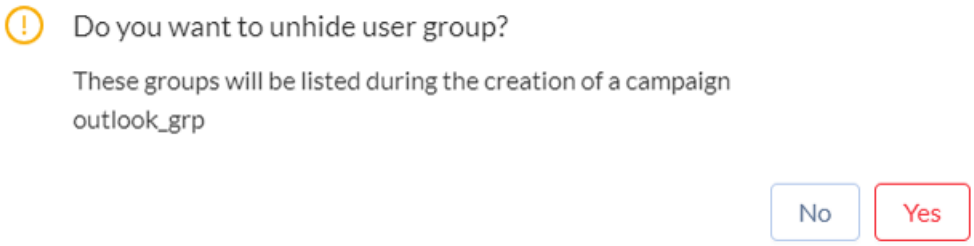


When the unhide option is selected, the list of hidden groups will be displayed. You can unhide the groups, allowing them to appear in the group list page and when creating a campaign.

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.

Exporting group details

You can now export group and smart group members information to a CSV file. This export includes member information, risk grade, risk score, and any synced Azure AD attributes.

To export group details:

1. Go to *Recipients* > *Groups*, and select a group in the list.
2. Click *Export CSV* file.

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*.

Smart Group

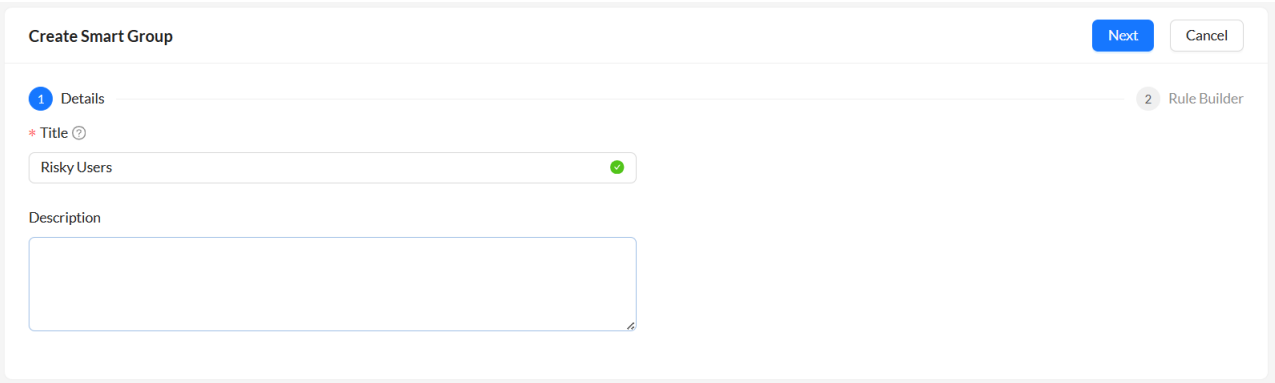
Smart Group allows you to dynamically add users to groups based on predefined rules. These rules can be defined using user properties such as risk grade, actions, campaign interactions, and training history. Once created, Smart Groups can be used to target specific user segments with tailored phishing campaigns.

- A maximum of *five* Smart Groups can be created.
- For a user to be added to a Smart Group, they must be part of at least one phishing campaign. This ensures that the necessary parameters (risk grade, actions, campaign interactions, training history) are available for comparison with the defined rules during Smart Group creation.

- Creating a Smart Group
- Viewing Smart Group details
- Editing a Smart Group
- Deleting a Smart Group

To create a Smart Group:

1. Navigate to *Recipients* > *Group List*.
2. Click *Create* > *Smart Group*.
3. Enter a *Name* and *Description* for the Smart Group. Click *Next*.

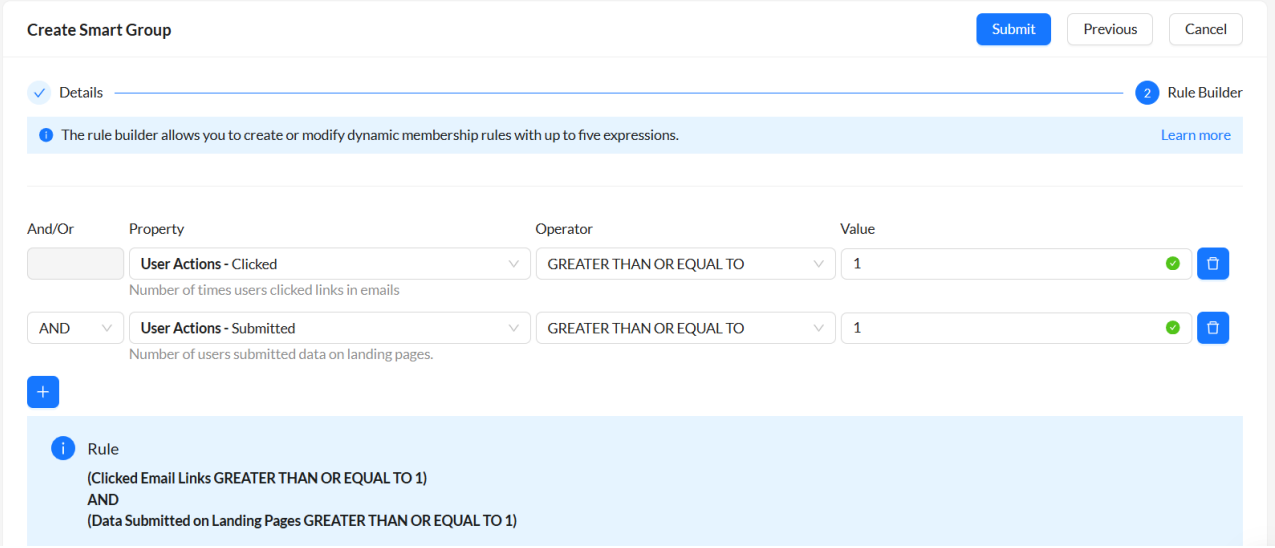


4. In the *Rule Builder* page, define rules.
   a. *Property*: Select the user property you want to use for the rule.
   b. *Operator*: Choose an appropriate operator based on the selected property.

c. *Value*: Enter the desired value for the rule.

d. Click add **+** to add additional rules. Select *And* or *Or* to combine multiple rules.

- A maximum of *five* rules can be added.
- For a list of all supported properties, see Supported properties for Smart Group rules.



5. Review the rules. The added rules will be displayed in a readable format in the *Rule* section.
6. Click *Submit*.

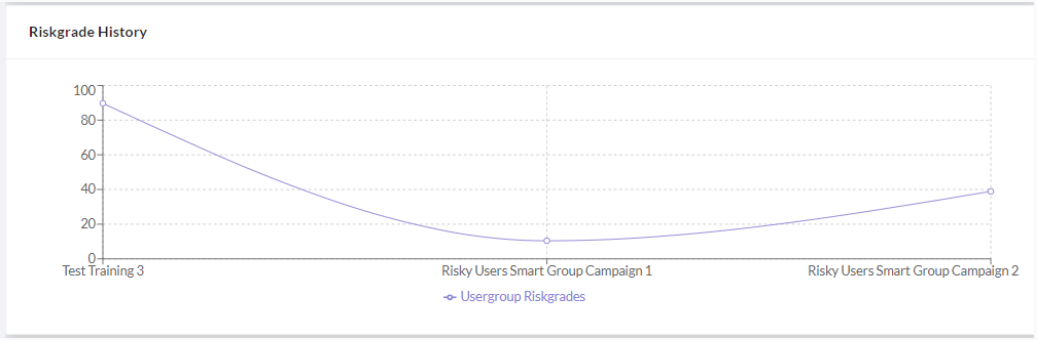
To view Smart Group details:

1. Navigate to *Recipients* > *Group List*.
2. Click the Smart Group name. Smart Groups are indicated by the *Smart Group* value in the *Created* field.
3. The Smart Group details page includes the following information.

Overview	The Overview section displays the following information. • *Name* - The name given to the Smart Group. • *Description* - Provided description of the Smart Group. • *Member Count* - The total number of users currently assigned to the Smart Group. • *Created at* - The date and time the Smart Group was created. • *Updated at* - The date and time the Smart Group was last modified. Smart Groups are refreshed every 24 hours. • *Sync Status* - The current synchronization status. • *Last Synced At* - The date and time the Smart Group was last synchronized. It may take up to 24 hours for initial population or after rule changes. • *Rule* - The rule or set of rules used to determine membership in the Smart Group.

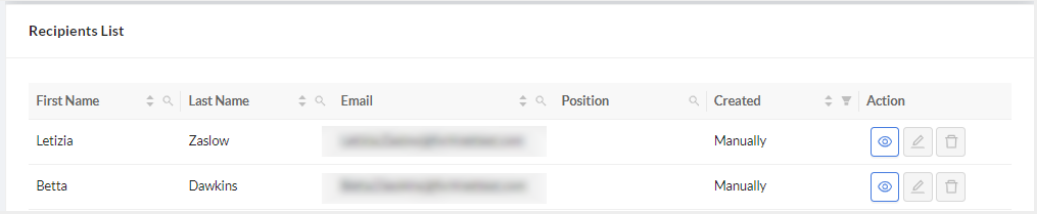
Risk Grade

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. See Risk Grade History.



Recipients List

A list of users that match the defined rule. Click the *View User* button next to the user you want to view detailed information. The corresponding user profile page is displayed. See User Profile.



To edit a Smart Group:

1. Navigate to *Recipients* > *Group List*.
2. Click the Smart Group name that you want to edit.
3. In the details page, Click *Edit*.
4. Make necessary changes and click *Save*.

Deleting a Smart Group

1. Navigate to Recipients > Group List.
2. Click the Smart Group name that you want to delete.
3. In the details page, Click *Delete*.
4. Click *Yes* to confirm.

Supported properties for Smart Group rules

The following properties are supported by FortiPhish for Smart Group rules.

Category	Property	Description
User	Risk Grade (Numeric)	The numeric grade between 1 and 100 assigned to the recipient . An 100 indicates the user poses minimal risk and a 1 grade indicates the user poses the maximum risk to the organization.
	User Department	The case-sensitive department name of the user.
User Actions	Clicked	Number of times users clicked links in emails
	Executed	Number of users who opened email attachments and clicked links within.
	Opened	Number of users opened phishing emails.
	QR Code Scanned	Number of users scanned the malicious QR Codes in emails.
	Replied	Number of users replied to emails. Note. Reply is tracked only when campaign is configured to do so.
	Reported	Number of users who reported email.
	Submitted	Number of users submitted data on landing pages.
User Campaigns	Failed In Last Consecutive Campaigns	Users with a history of 'N' consecutive campaign failures.
User Training	Incomplete	Number of users who were assigned training but didn't complete.

User Actions category refers to user actions performed to date or up to the point of data availability.

LDAP Server

Use the *LDAP Server* page to configure and manage connections to your enterprise LDAP or Active Directory (AD) for bulk user and group import into FortiPhish.

- Add an LDAP Server
- Synchronize the LDAP Server
- Delete an LDAP Server

Add an LDAP Server

Perform the following steps to configure the connection details for your LDAP server.

1. Go to *Recipients* > *LDAP Server* and click *Add Client*. The *Create LDAP Client* window opens.
2. Configure the LDAP server settings.

Name	The LDAP server name.
Server URL	The LDAP server URL.
Connection Mode	Select the desired connection security mode: *Non-TLS*, *TLS*, or *STARTTLS*.
BaseDN	The starting point in the directory tree where the server will search for users.
Search Filter	The LDAP search filter syntax used to query the users

3. Set synchronization schedule to automatically sync users or users and groups.
   a. Select the frequency of the synchronization, *Weekly*, or *Monthly*. Select None to disable automatic syncing.
   b. Select the desired time zone from the drop down menu.
   c. Set the time of synchronization by selecting hour and minute.
   d. 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.

4. (Optional) Expand *Advanced Field Matching* and configure the settings to map specific LDAP attributes to FortiPhish user fields..
5. Test the connection.
   a. Click *Test Connectivity*. The *Test Connectivity* dialog opens.
   b. Enter the LDAP *User Name* and *Password*.
   c. Click *Submit*.
6. Click *Submit* to save the new LDAP server configuration. A confirmation message is displayed.

Synchronize the LDAP Server

The LDAP Server page allows you to monitor the status of scheduled synchronizations and manually trigger an update.

1. Go to *Recipients* > *LDAP Server* .
   The *Sync Status* column displays the current status of the last synchronization. Hover over the status to view the total number of users or users and groups fetched during that sync.
   The *Next Sync Scheduled At* column, displays date and time of the next synchronization schedule. If sync schedule is not configured, *NA* is displayed.
2. Click the *Sync* icon in the Action column. During the sync process, the *Sync Status* window displays the number of users (and groups) being fetched.

Delete an LDAP Server

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

When you delete an *LDAP* client from FortiPhish, the existing imported groups and users lose their association with that client but remain in FortiPhish, and their *Created* field changes from *LDAP* to *Others*. Once an entity is marked as *Others*, you can modify or delete it directly within the FortiPhish portal.

Azure AD

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

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:

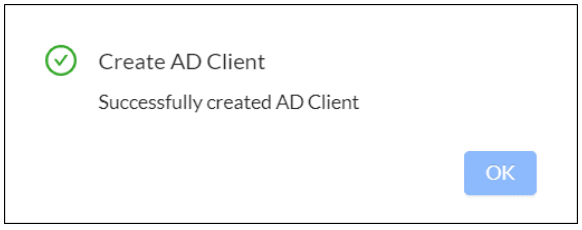
1. Go to *Recipients* > *Azure AD* and click *Add Client+*. The *Create Azure AD* window opens.
2. Configure the Azure AD server settings.
   a. Enter a *Name* for Azure AD.
   b. Enter the *Tenant ID, Application AD, and Client Secret* information gathered during Configuring Azure AD for FortiPhish.
   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, *Weekly*, or *Monthly*. Select None to disable automatic syncing.

      Azure AD sync now only supports *Weekly* or *Monthly* sync schedules. *Daily* sync is no longer supported and existing daily schedules will be automatically migrated to *Weekly*.

      ii. Select the desired time zone from the drop down menu.
      iii. Set the time of synchronization by selecting hours and minutes.
      iv. 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.



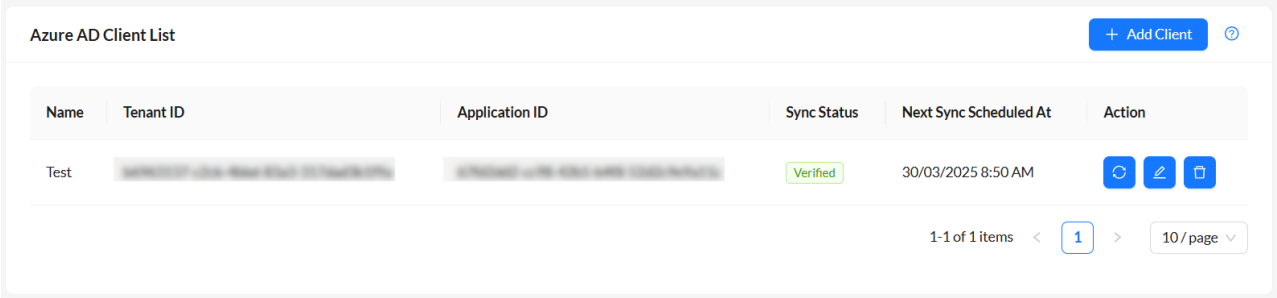
- Groups imported from Azure AD are automatically added under Recipients > Group List. If only users are imported, they must be added to a group manually. See Creating Azure AD user groups.
- To update user information, the changes must be made within Azure AD server and then synced back to FortiPhish.
- 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

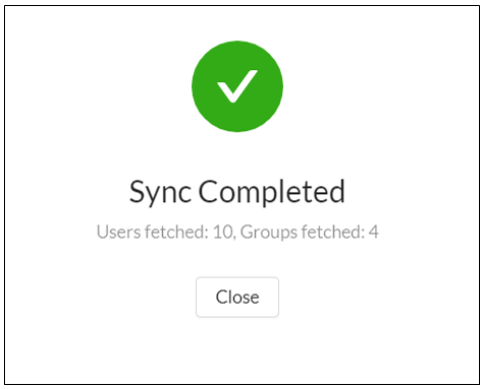
You can sync the Azure AD server when members join or leave your organization.

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.



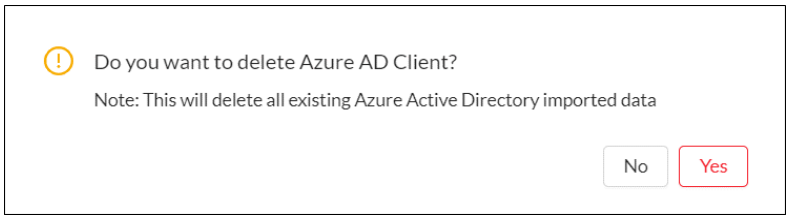
   The *Next Sync Scheduled At* column, displays date and time of the next synchronization schedule. If sync schedule is not configured, *NA* is displayed.
3. In the *Action* column, click the sync button. During the sync process, clicking the sync button will display the number of users or users and groups 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.



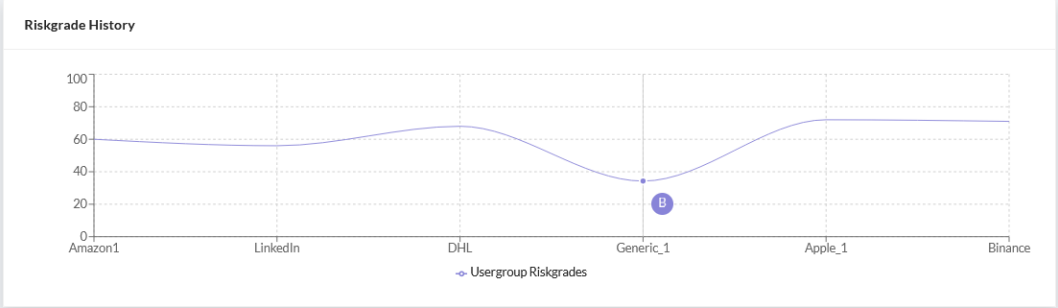
3. Click *Yes*.

When you delete an *Azure AD* client from FortiPhish, the existing imported groups and users lose their association with that client but remain in FortiPhish, and their *Created* field changes from *Azure AD* to *Others*. Once an entity is marked as *Others*, you can modify or delete it directly within the FortiPhish portal.

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.



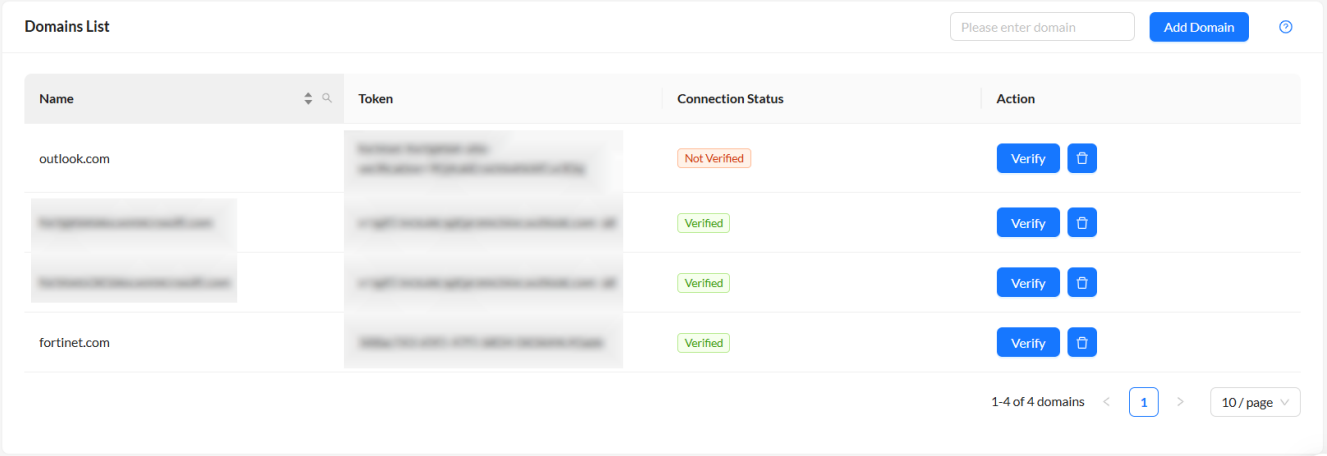
To view the Riskgrade History:

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

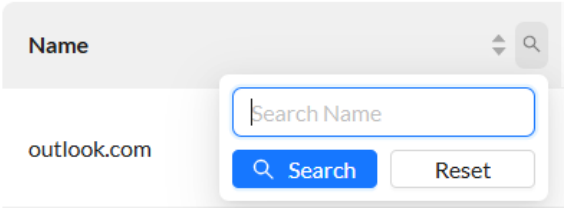
The *Risk Grade* is not displayed in active campaigns.

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 43.



To search for a specific domain, select the search icon in the Name column header.



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.

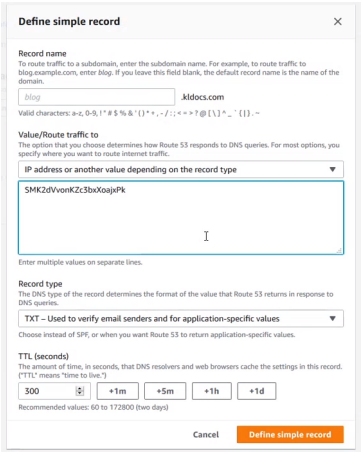
To add the token to your domain:

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.
- To ensure successful domain verification, confirm that both your MX records and TXT records are valid and configured correctly in your DNS settings.

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.

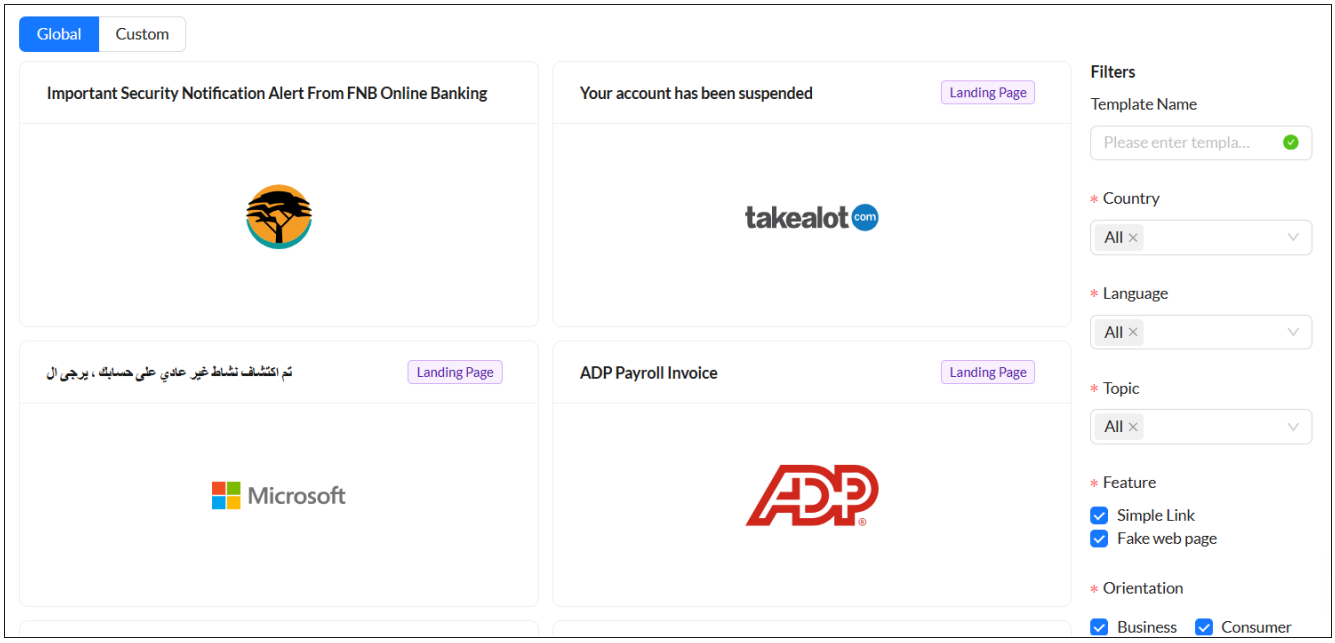
Campaigns

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 47.

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 *Create 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 62.

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 63. 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 50. • 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 Target Group* page opens.

Campaign Name	Enter the campaign name.
Sender Name	Edit the sender's name.
Sender Email	Edit the sender's email address.
URL and Landing Page Domain	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 75.
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. In *Select Target Group* page, select the recipients.
   - To select individual users, go to the *Users* tab. Click *Select All Users* to add all users, and then deselect any you don't need.
   - To select groups, go to the *Groups* tab. Click *Select All Groups* to add all groups, and then deselect any you don't need.

   After you make your selections, click *Next*. The *Select Launch 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 *Select 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
`{{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

Standard	Format
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	2006-01-02T15:04:05.999999999207:00

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 Overview
   - Campaign Summary
   - Risk Grade
   - Campaign Timeline

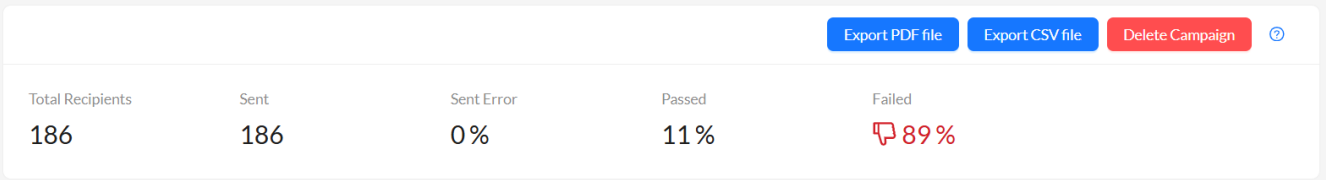
- Campaign Preview
- Campaign Stats
- Recipient User Agents
- Recipient Stats
- Usergroup Stats

Campaign Overview

The Campaign Overview widget displays the following information.

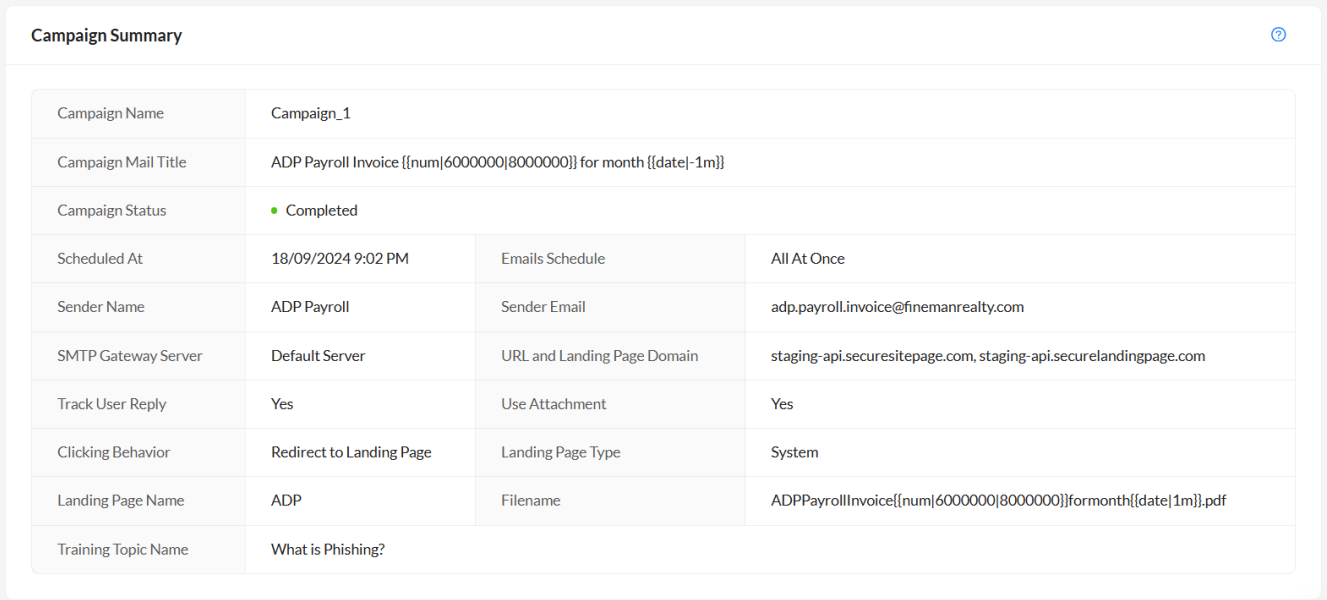
Total Recipients	The total number of recipients in the campaign.
Sent	The number of emails sent to the user group.
Sent Error	The number of emails that bounced.
Passed	Percentage of recipients who passed the campaign.
Failed	Percentage of recipients who failed the campaign.

You can export campaign details by clicking **Export PDF file** to download a *PDF* report or **Export CSV file** to download a *CSV* report. To delete a campaign, click **Delete**.



Campaign Summary

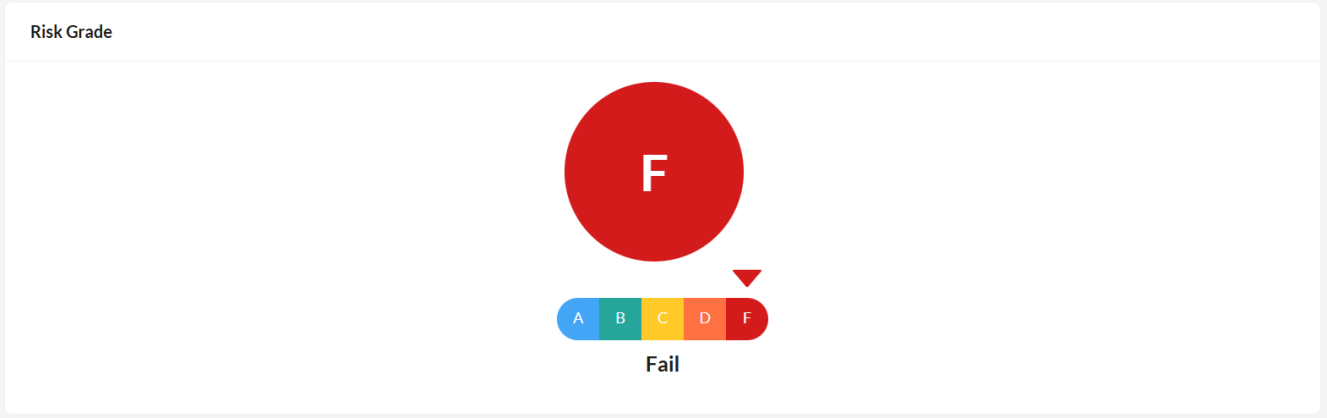
The *Campaign Summary* monitor displays the *Campaign Name*, *Campaign Mail Title*, *Email Schedule*, *Campaign Mail Sender*, *Track User Reply*, *Use Attachment* and *Clicking Behavior*. If an attachment was used, the monitor displays *Filename*.



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.

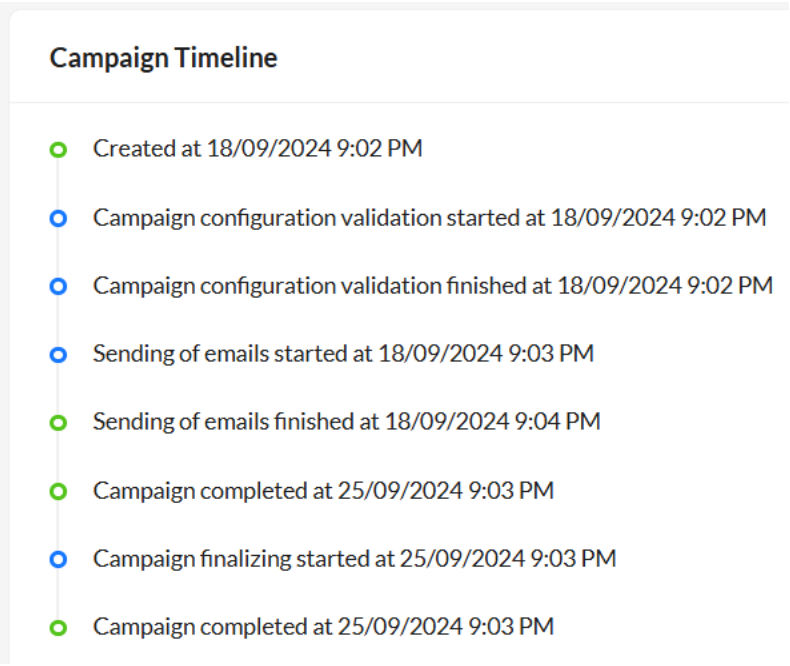
Risk Grade

The Risk Grade widget displays the letter grade between *A and F* assigned to the campaign.



Campaign Timeline

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

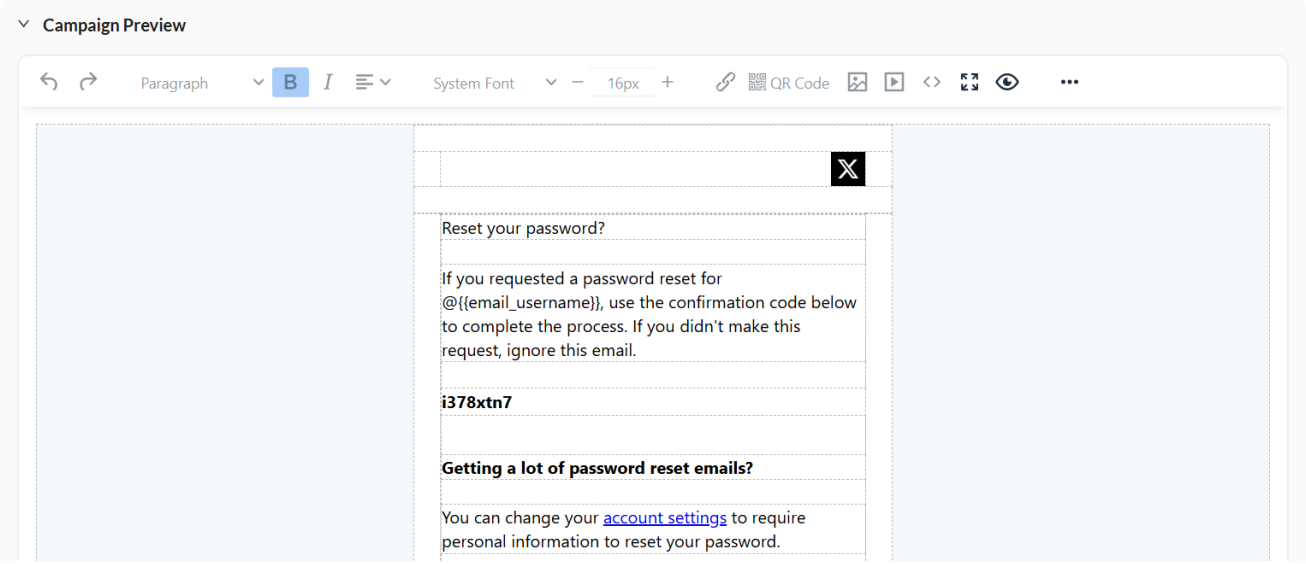


The *Email Status* monitor displays the following information:

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.

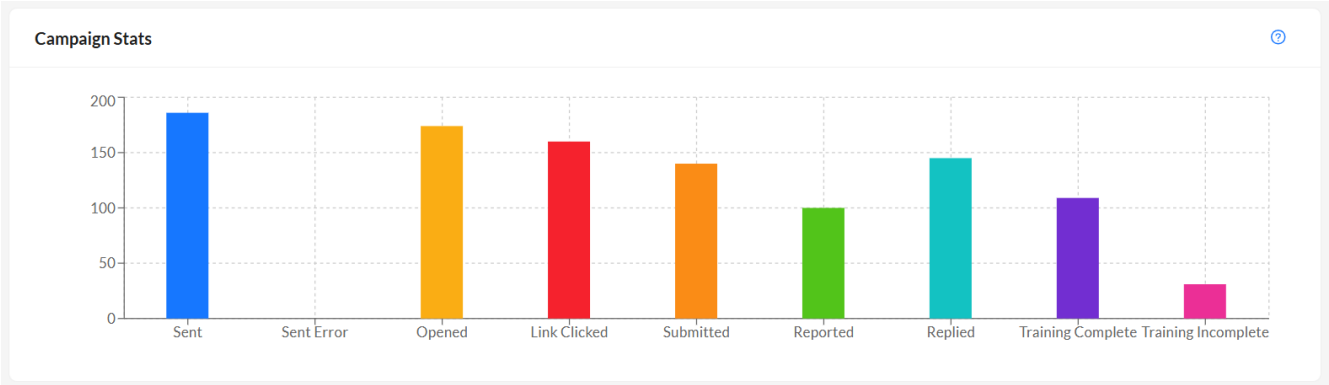
Campaign Preview

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

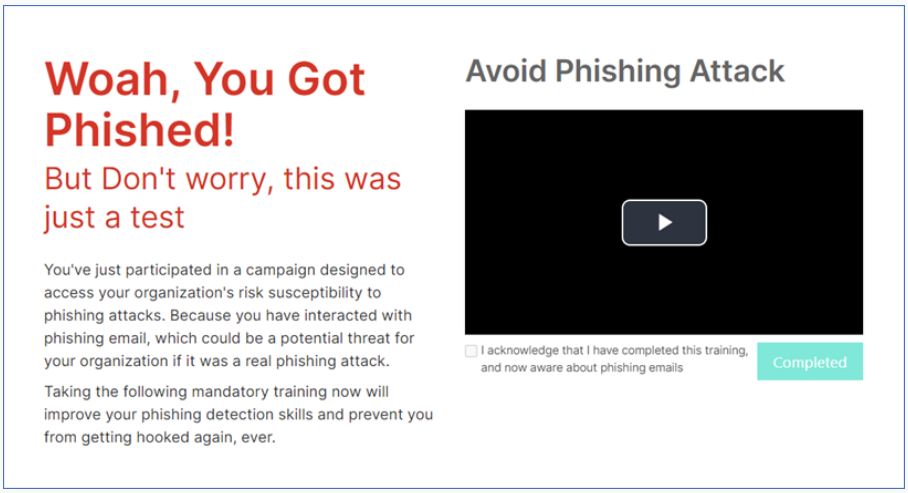


Campaign Stats

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.

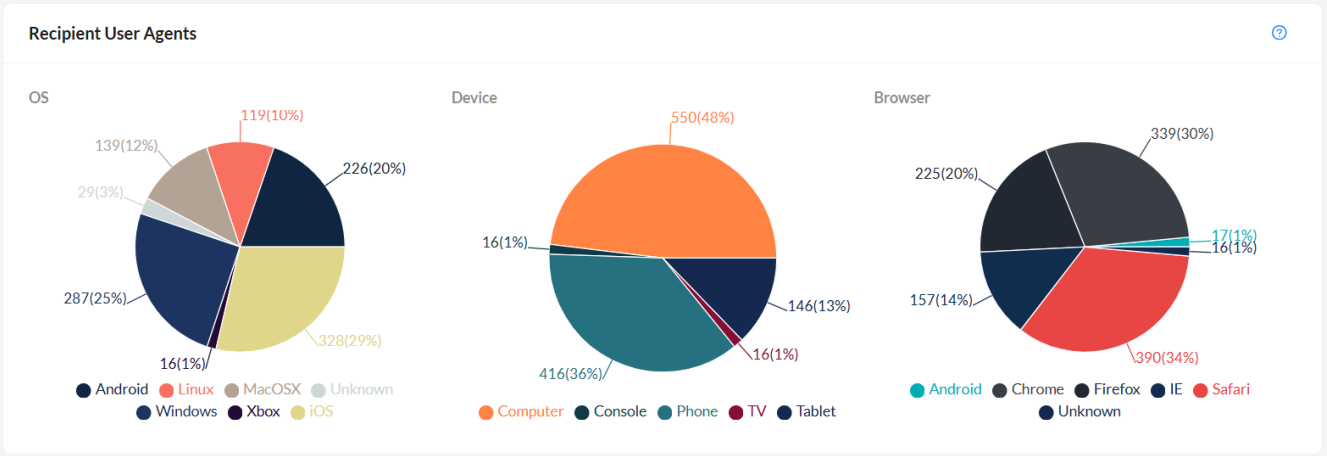


Sent	The number of emails sent to the user group.
Sent Error	The number of emails that bounced.
Opened	The number of recipients who opened the email.
Link Clicked	The number of recipients who clicked the redirect link.
QR Code Scanned	The number of recipients who scanned the QR code.
Submitted	The number 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.
Training Complete	The number of recipients who completed the training. 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. 
Training Incomplete	The number of recipients who have been enrolled but did not finish the training.

Recipient User Agents

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

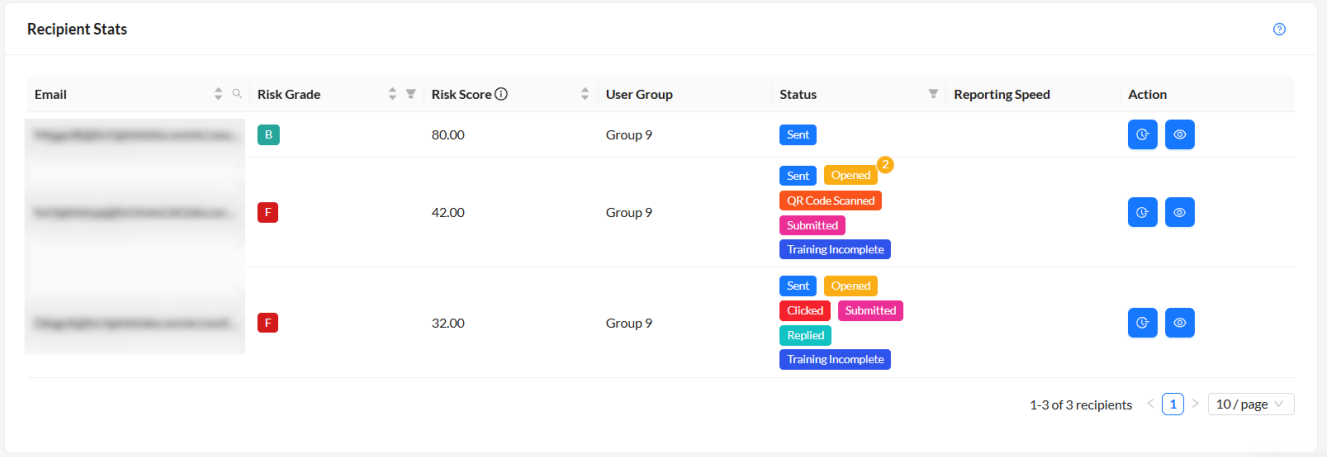


The *Recipient User Agents* monitor displays the following information:

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

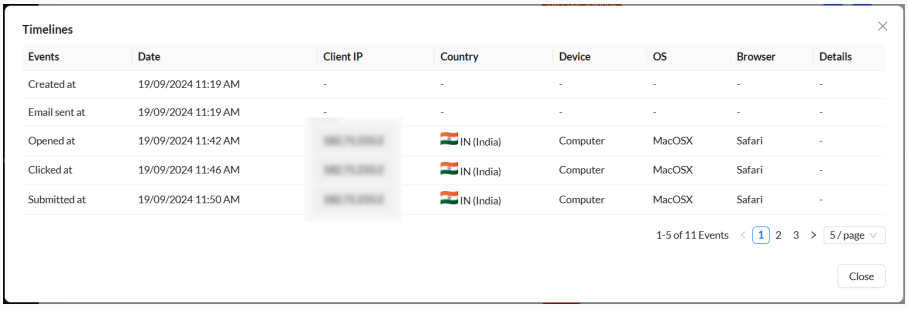
Recipient Stats

The *Recipient Stats* monitor displays the recipient statistics.



The *Recipient Stats* monitor displays the following information:

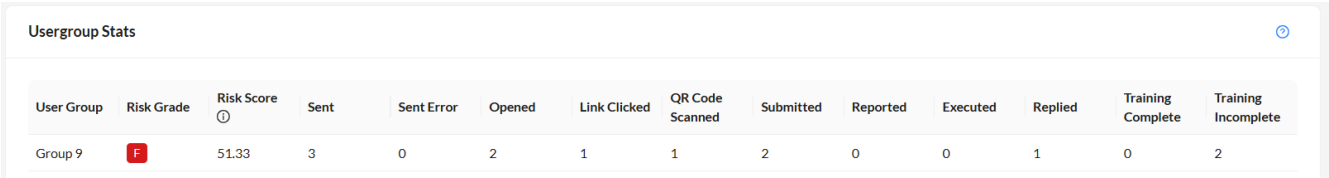
Email	The user email address.
Risk Grade	The letter grade between *A and F* assigned to the recipient . An *A* indicates the user poses minimal risk and a *F* grade indicates the user poses the maximum risk to the organization.If the campaign is active, then the Risk Grade will be *NA*on the *Dashboard* 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*. The count badge displays the number of times that specific action has been performed and is only displayed when the recipient has performed the action more than once.
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 timeline of the recipient's actions including *Event*, *Date*, *Client IP*, *Country*, *Device*, *OS*, *Browser*, and *Details*.  Click the *View User* icon to view the detailed user information. See User Profile.

Usergroup Stats

The Usergroup Stats displays group statics.

The *Usergroup Stats* section appears only when you select one or more groups during campaign creation.



The *Usergroup Stats* displays the following information:

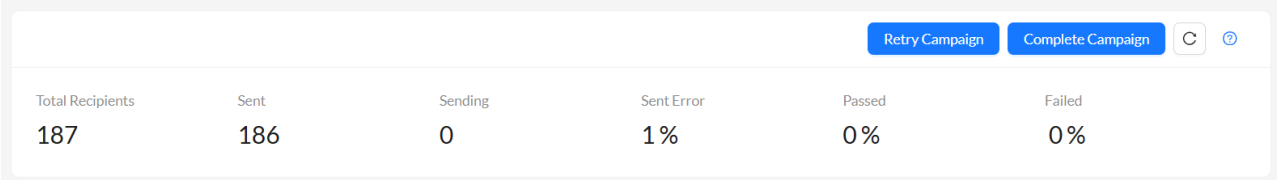
User Group	The user group name.
Risk Grade	The letter grade between *A and F* assigned to the group. An *A* indicates the group poses minimal risk and a *F* grade indicates the group poses the maximum risk to the organization.
Sent	The number of emails sent to the user group.
Sent Error	The number of 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

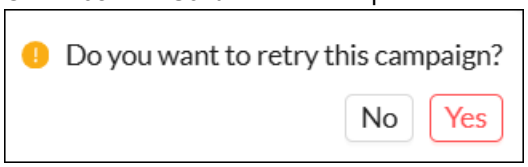
Resend emails that were not delivered or blocked by the mail server.

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 *Yes*. The *Sent* metrics are updated.

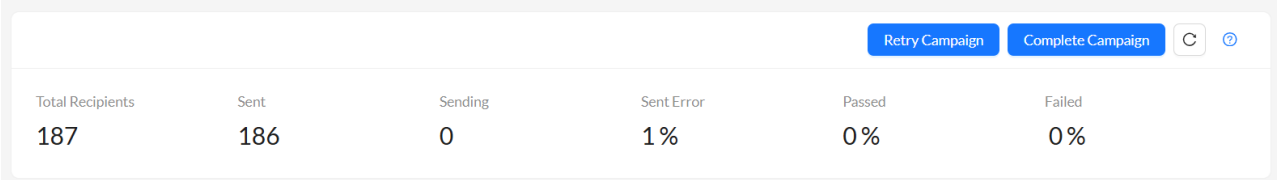


Completing a campaign

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 *Yes* 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	• Click *Download Summary CSV*to save summary of the campaign to your device. The file shows the recipients' *email*, as well the statistics for *delivered*, *opened*, *clicked*, *submitted*, *QR code scanned*, *executed*, *replied*, *Risk Grade*, and *reported* emails as yes or no (*Y*/*N*) values. • Click *Download Detailed CSV*to save detailed report of the campaign to your device. The file shows the recipients' *email*, as well the detailed statistics for *Risk Grade*, *Risk Score*, *Events*, *Date*, *Client IP*, *Country*, *Device*, *OS*, *Browser* and a link to user profile.

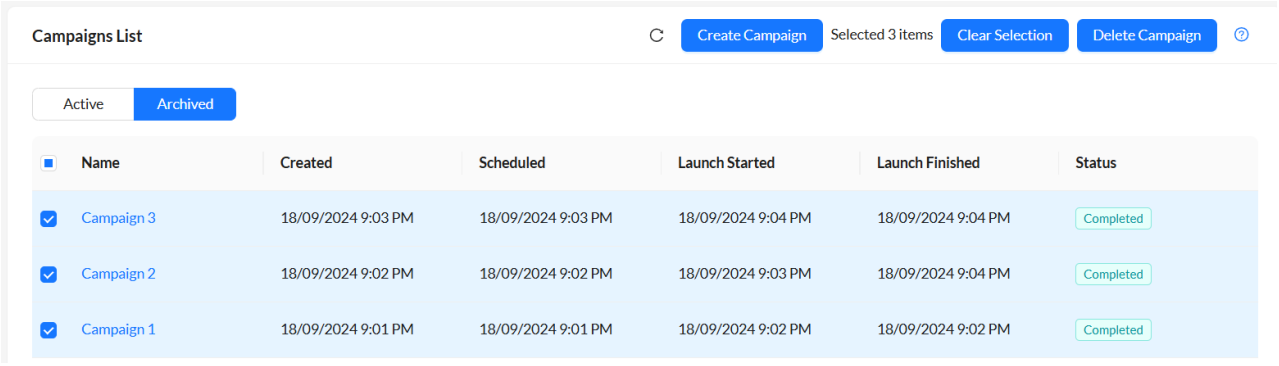
Deleting archived campaigns

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

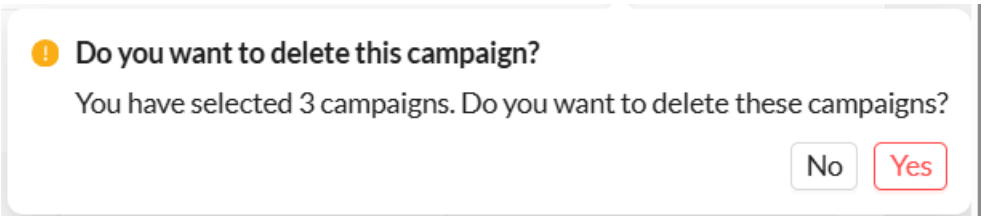
You can schedule archived campaigns to be automatically deleted at monthly intervals in the application settings page. See, Enable Auto Delete on page 67.

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.



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 *Edit* 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 template* page 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 63.
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*.

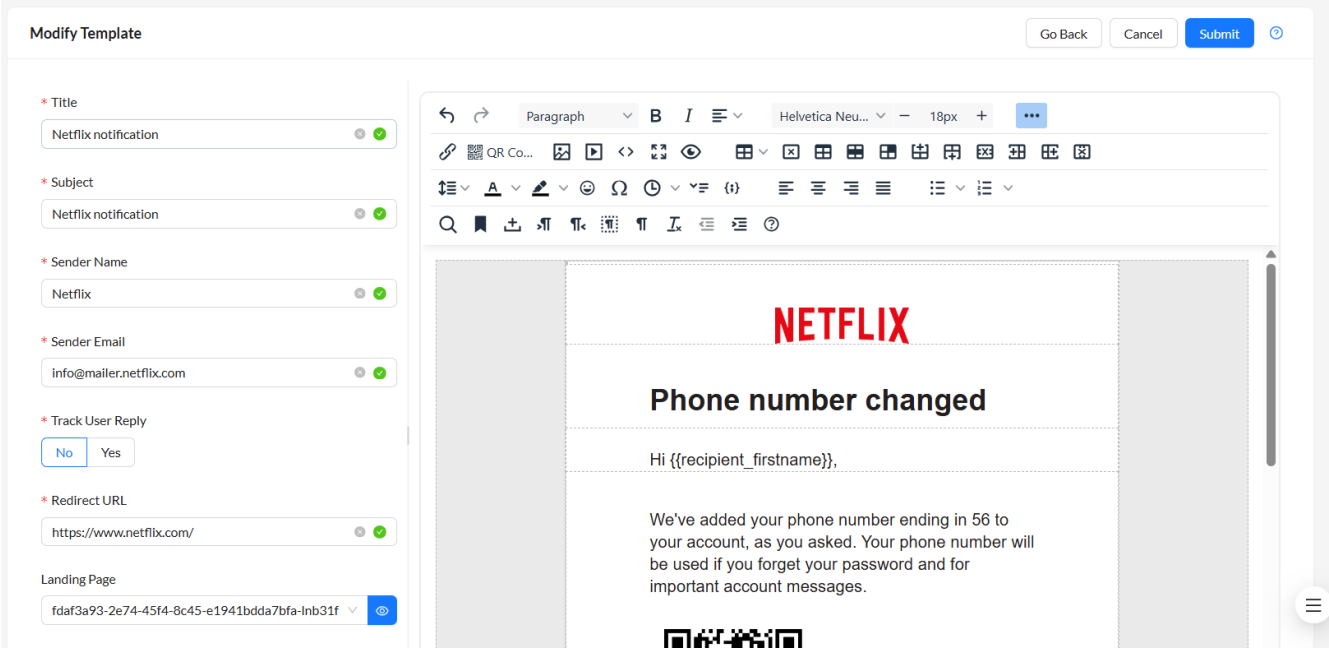
- You can use variables in the email body to generate dynamic data while the campaign is running. See, Template variables on page 50.
- QR code option is available only for *FortiPhish Premium* users. Contact Fortinet Support team to upgrade.

5. Click *Submit*. The template is added to the *Custom* tab in the *Campaigns* module. See, Creating campaigns on page 47.

Click *Reset* to clear all the entered information.

To edit a template:

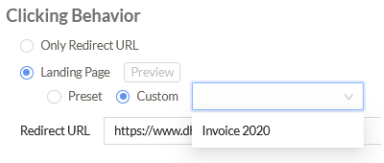
1. Click the *Edit* icon. The *Modify Template* page opens.
2. Update the template and click *Submit*.



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 47.

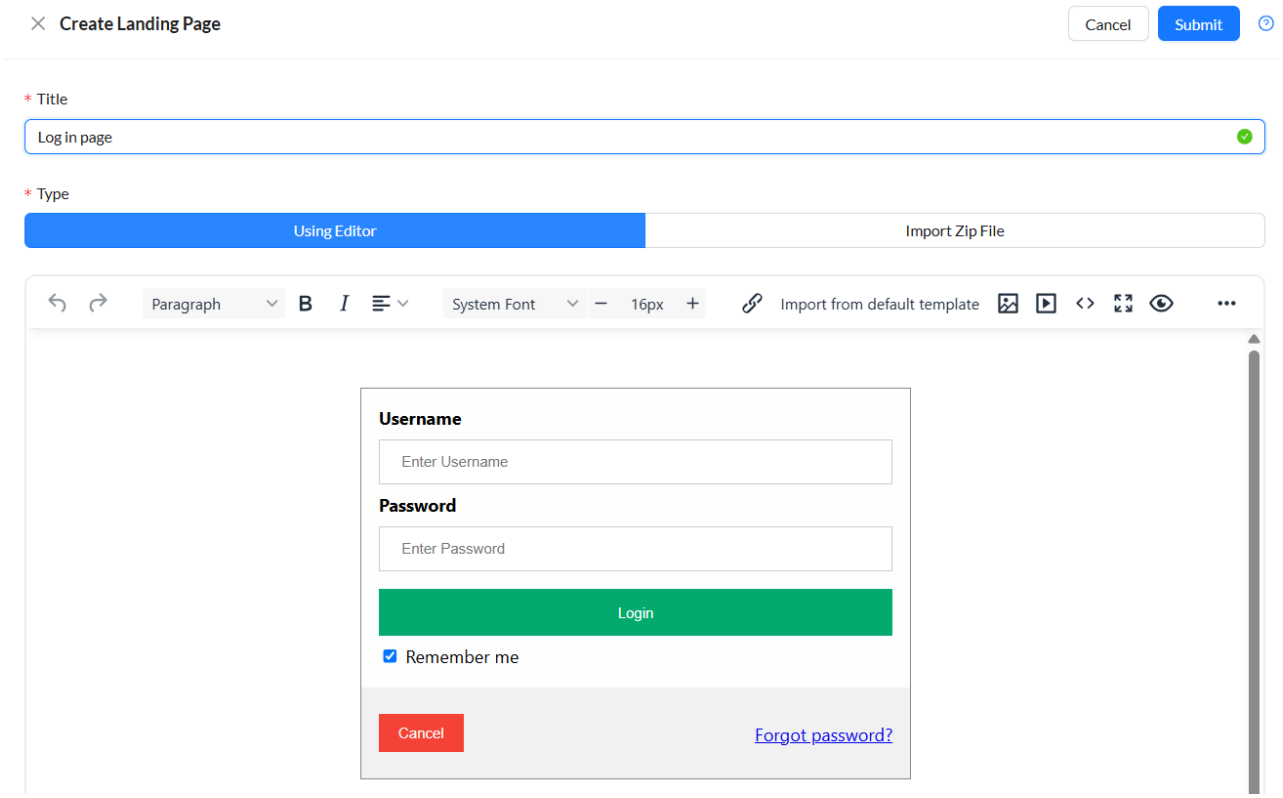


FortiPhish does not save the data entered by the user in the landing page.

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 65.
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:

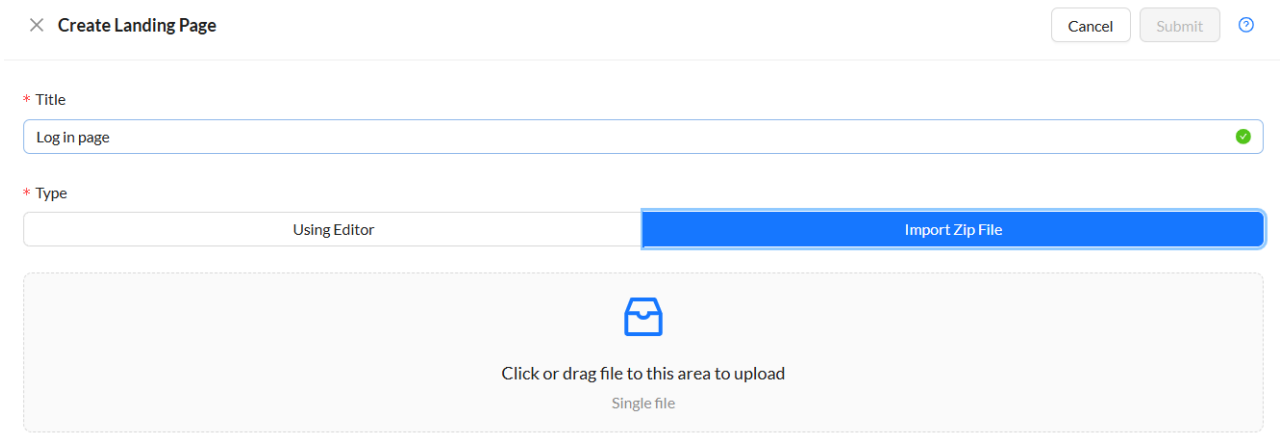
The Zip file should contain an `index.html` file that must include the following:

- 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}}

Variable	Syntax
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, add SMTP server accounts, and view IP addresses, API endpoints, and SMTP servers that must be safelisted.

Campaigns

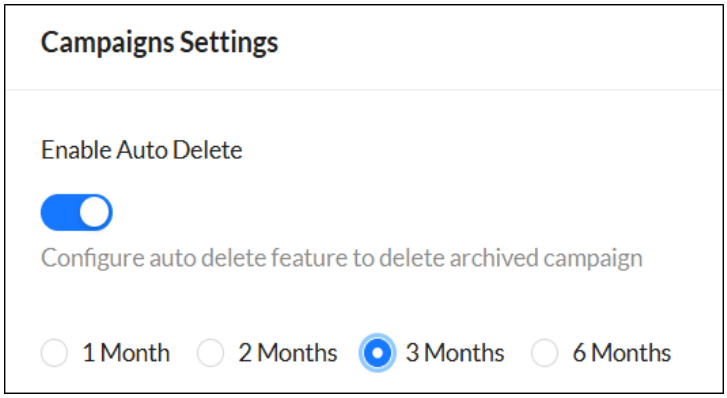
The *Settings* > *Campaigns* page allows you to automatically delete archived campaigns, and set time period to skip email scanner actions.

Enable Auto Delete

Schedule archived campaigns to be automatically deleted at monthly intervals.

To enable auto delete:

1. Navigate to *Settings* > *Campaigns* page.
2. Enable the *Enable Auto Delete* toggle.
3. From the dropdown menu, select *1 Month*, *2 Months*, *3 Months*, or *6 Months*.



4. Click *Submit*.

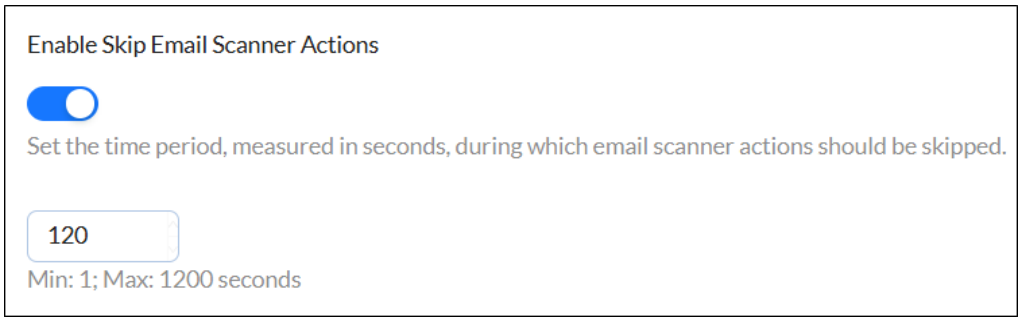
Enable Skip Email Scanner Actions

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. Navigate to *Settings* > *Campaigns* page.
2. Enable 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. After a user reports a suspicious email, the response is recorded in the *Monitoring* and *Campaigns* statistics.

To enable FortiPhish alert buttons:

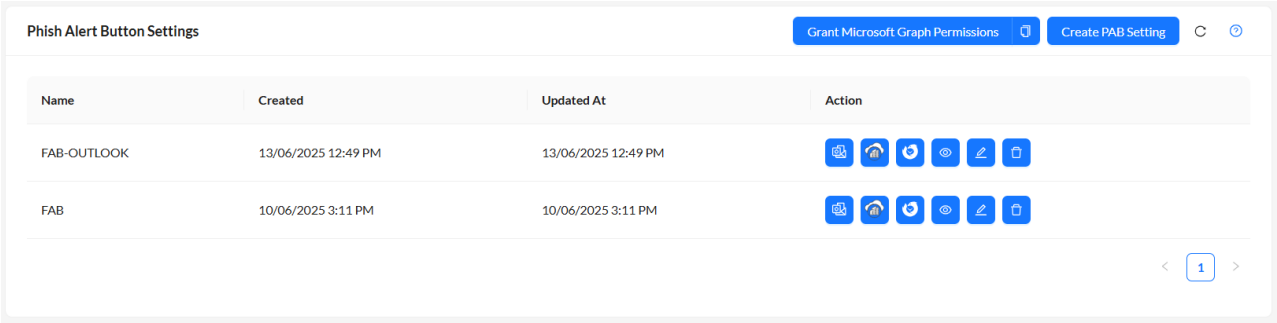
1. Create a FortiPhish alert button.
2. Install the button on Microsoft Exchange or Thunderbird.
   - Adding alert buttons in Microsoft Exchange Environments
   - Adding alert buttons in Thunderbird

Creating a FortiPhish alert button

The FortiPhish Alert Button (PAB) template is located in the *Settings* section. 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 button in Microsoft Exchange or Thunderbird.

To create a FortiPhish alert button:

1. Navigate to *Settings* > *Phish Alert Button* page.



2. 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. Navigate to *Settings* > *Phish Alert Button* page.
2. In Actions column, next to the alert button name, select one of the following file formats based on the environment you want to deploy the alert button.
   - *Download Outlook Add-In Manifest - Exchange Online / Microsoft 365 (FAB_Online.xml)*
   - *Download Outlook Add-In Manifest - Exchange On-Premises (FAB_OnPrem.xml)*
   - *Download Thunderbird PAB Installer Configuration(.xpi)*
3. Save the file to your device.

To edit an alert button:

1. Navigate to *Settings* > *Phish Alert Button* page.
2. Click the *Edit* icon next to the alert button name.
3. Update the message and click *Save*.

To delete an alert button:

1. Navigate to *Settings* > *Phish Alert Button* page.
2. Click the *Delete* icon next to the alert button name.
3. A confirmation dialog opens. Click *Yes*.

Adding alert buttons in Microsoft Exchange Environments

The FortiPhish Alert Button (FAB) enables users to report suspicious or phishing emails directly from their mailbox. As an administrator, deploy this add-in to your users' Outlook clients from your Exchange environment:

- Exchange Server
- Exchange Online (Microsoft 365)
- Hybrid environments

After installation, users can report phishing by clicking the **Report Phishing** button on the Outlook ribbon for Windows and Mac or by selecting **Report Phishing** from the message menu on Outlook Web and mobile devices.

Existing Exchange Online/Microsoft 365 and Hybrid environment customers who installed the FortiPhish Alert Button prior to the 25.2 release must update their FortiPhish Alert Button due to Microsoft phasing out legacy authentication tokens by **October 2025**.

Complete the following steps to install the new Phish Alert Button:

1. Remove the existing FAB add-in.
2. Grant Microsoft Graph Permissions.
3. Deploy the new *FAB_Online.xml* manifest for Exchange Online mailboxes.

- Compatibility and Prerequisites
- Adding FAB in Exchange Online / Microsoft 365
- Adding FAB to Exchange Server On-premises

Compatibility and Prerequisites

Following are the compatibility and prerequisites for deploying the FortiPhish Alert Button in Microsoft Exchange environments.

Feature	Environment		
	Exchange On-Premises (Exchange 2016 or later)	Exchange Online / Microsoft 365	Hybrid Environment
Required XML File	FAB_OnPrem.xml	FAB_Online.xml	• FAB_Online.xml (for Online mailboxes) • FAB_OnPrem.xml (for On-premises

Feature	Environment		
	Exchange On-Premises (Exchange 2016 or later)	Exchange Online / Microsoft 365	Hybrid Environment
			mailboxes)
Supported Outlook Clients	• Outlook 2016 or later (Windows/Mac) • Outlook Web App (OWA) or Outlook on the web	• Outlook 2016 or later (Windows/Mac) • Outlook Web App (OWA) or Outlook on the web • Outlook Mobile (iOS/Android)	Varies by mailbox environment type
Microsoft Graph Permissions	No	Yes	Yes (for Exchange Online mailboxes)

General Limitations Across All Environments:

- Only Azure AD (Microsoft Entra ID) work or school accounts can fully use FAB's reporting features. Personal Microsoft accounts can install the add-in but cannot authenticate to report.
- Guest users cannot use centrally deployed FAB add-ins across tenants. They must install FAB within their own tenant to report phishing.
- For assistance with FortiPhish Alert Button (FAB) in sovereign/government cloud environments (GCC, GCCH, DoD), contact Fortinet Support.
- Outlook accounts configured with POP/IMAP do not support add-ins, making FAB incompatible.
- Mobile Outlook (iOS/Android) and modern web clients are unsupported for on-premises Exchange Servers.

Adding FAB in Exchange Online / Microsoft 365

Existing Exchange Online/Microsoft 365 and Hybrid environment customers who installed the FortiPhish Alert Button prior to the 25.2 release must update their FortiPhish Alert Button due to Microsoft phasing out legacy authentication tokens by **October 2025**.

Complete the following steps to install the new Phish Alert Button:

1. Remove the existing FAB add-in.
2. Grant Microsoft Graph Permissions.
3. Deploy the new *FAB_Online.xml* manifest for Exchange Online mailboxes.

Centralized Deployment is an Office 365 feature that enables Global or Exchange administrators to deploy Office add-ins tenant-wide without requiring user action. This method is available through the Integrated Apps pane in the Microsoft 365 admin center.

- You must hold a *Global Administrator*, *Exchange Administrator*, or *Application Administrator* role.
- Your tenant must have an active Microsoft 365 subscription with Exchange Online.

Perform the following steps to deploy FAB.

1. Download the *FAB_Online.xml* file from the FortiPhish portal.
2. Sign in to the Microsoft 365 admin center for your environment: https://admin.microsoft.com
3. Navigate to **Settings > Integrated Apps > Add-ins**.
4. Click **Deploy Add-in**, then choose **Upload Custom Apps > From file**, and upload *FAB_Online.xml*.
5. Assign the add-in to everyone, specific users, or mail-enabled groups, and choose **Fixed** or **Optional** deployment.

Save your changes. The add-in appears for new users within 24 hours and fully propagates within 72 hours.

Granting Microsoft Graph Permissions

This step applies only to Exchange Online and hybrid deployments because the updated add-in utilizes Microsoft Graph API calls (*Mail.ReadWrite*, *Mail.Send*, *User.Read*). Pure on-premises environments do not require admin consent.

1. In FortiPhish portal, go to **Settings > Phish Alert Button**.
2. Click **Grant Microsoft Graph Permissions**.
3. Sign in with a global administrator account when prompted.

Adding FAB to Exchange Server On-premises

On-premises Exchange servers require deployment through the Exchange Admin Center (EAC).

Your installer account must have Organization Management permissions.

Perform the following steps to deploy FAB.

1. Download the *FAB_OnPrem.xml* file from the FortiPhish portal. See Creating a FortiPhish alert button.
2. Sign in to your on-premises Exchange Admin Center (EAC).
3. Navigate to **Organization > Add-ins**. Click **+ New > Add from file**, and upload *FAB_OnPrem.xml*.
4. Click **Save**. Propagation can take up to 72 hours.

To view or remove installed Outlook add-ins on an on-premises Exchange server, navigate to Organization > Add-ins in the EAC, select FAB, and click Delete.

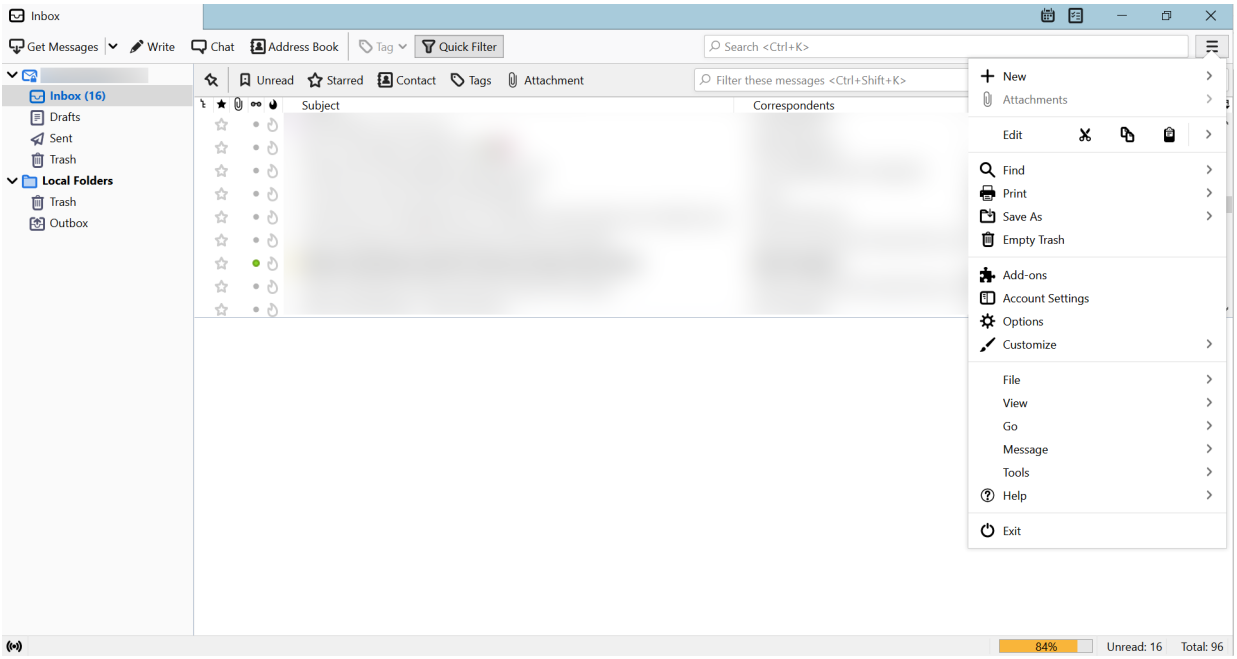
Adding alert buttons in Thunderbird

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.

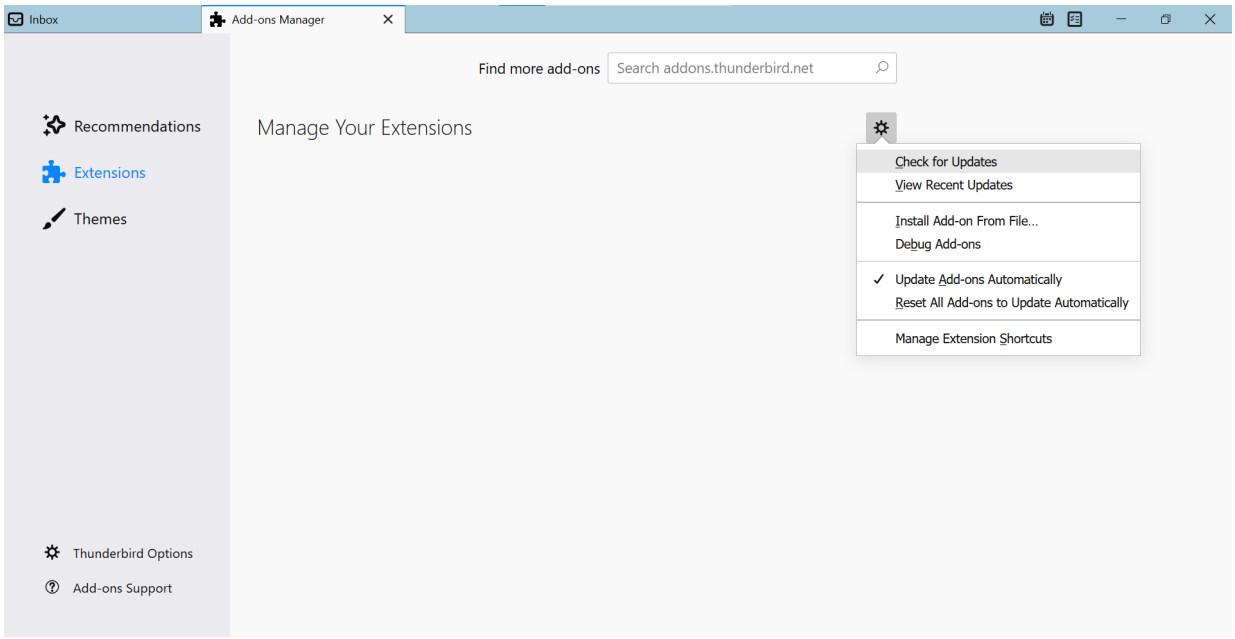
- This process requires Read/Write Mailbox permissions for your email client.
- The images in the following task are based on Thunderbird for desktop v 78.12.0. The user interface may look different than the one you are using. For more information, please refer to the product documentation.
- Thunderbird Client (version >=78) are compatible. For Thunderbird release, see https://www.thunderbird.net/en-US/thunderbird/releases

To install the FortiPhish alert button:

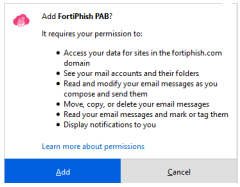
1. In Thunderbird, click the Thunderbird menu and select *Add-Ons*.



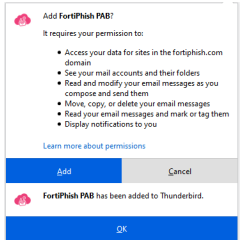
2. In the *Extensions* tab, click the gear icon, and click *Install Add-on From File...*.



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.

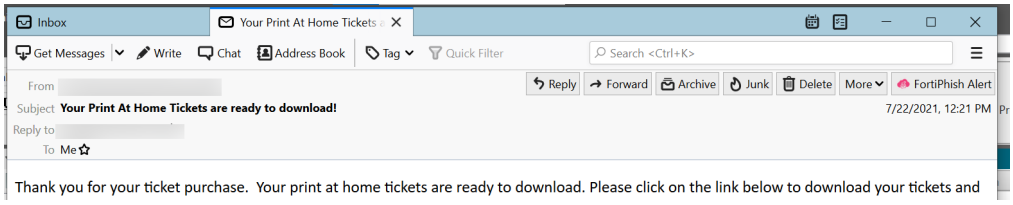


5. Click *OK* and click *Add* to close the dialog.

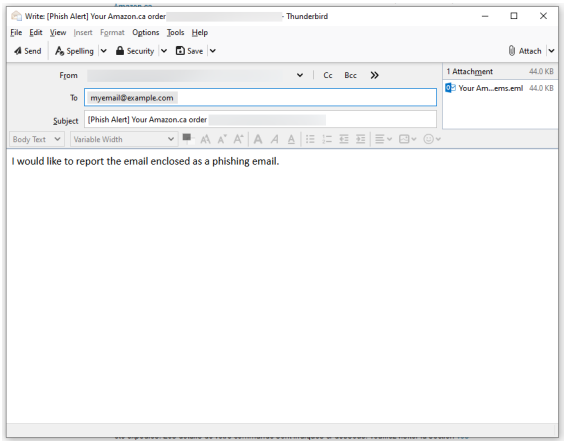


To test the alert button:

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

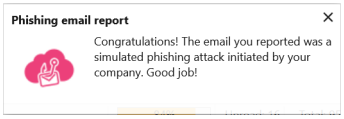


2. Click the *Phish Alert* button to open the composer. The suspicious email is attached as an EML file.



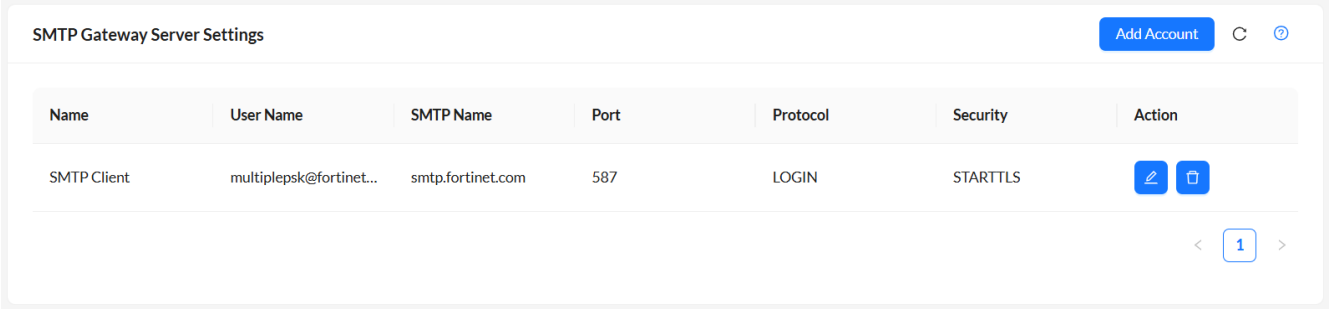
Thunderbird email recipients can edit the email message body.

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



SMTP

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



To add a SMTP server to FortiPhish:

1. Navigate to *Settings* > *SMTP*.
2. Click *Add Account*.

3. Configure the SMTP settings. All settings are required.

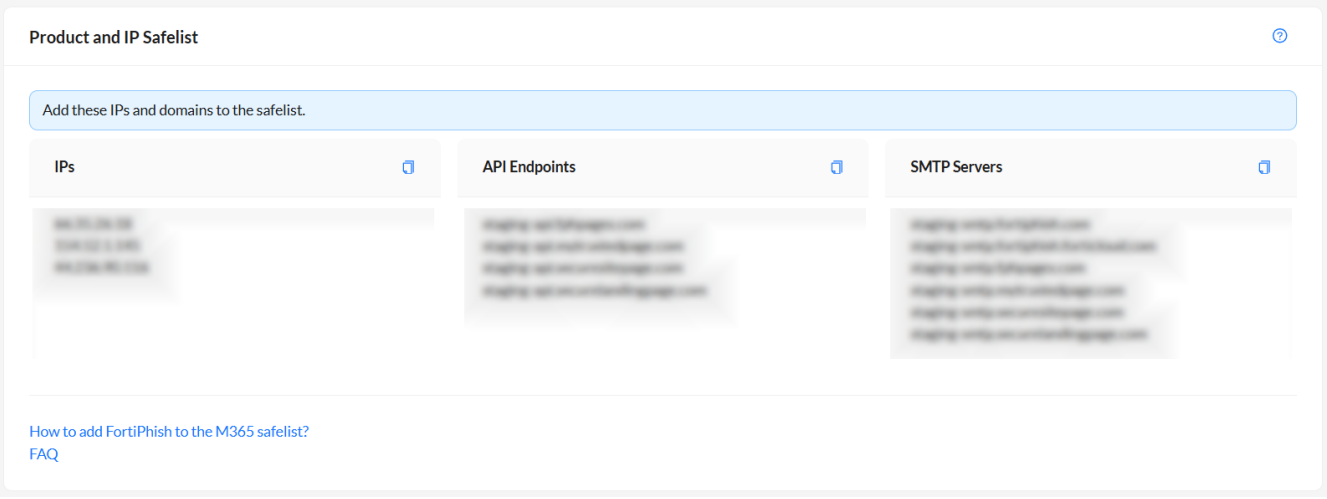
Name	Enter the mail server name.
Username	Enter the username to be used to authenticate with SMTP server.
Password	Enter the password to be used to authenticate with SMTP server.
Domain Name	Enter the address of the SMTP server to be used to send outgoing emails. The address can be in the form of IP 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*.

Product and IP Safelist

The *Settings* > *Product & IP Safelist* page lists IP addresses, API endpoints, and SMTP servers that must be safelisted for optimal FortiPhish functionality.

- For more information on safelisting FortiPhish in Office 365, see Safelisting FortiPhish in Office 365.
- For more information on safelisting FortiPhish in FortiMail, see Safelisting FortiPhish in FortiMail.



SCIM Token Management

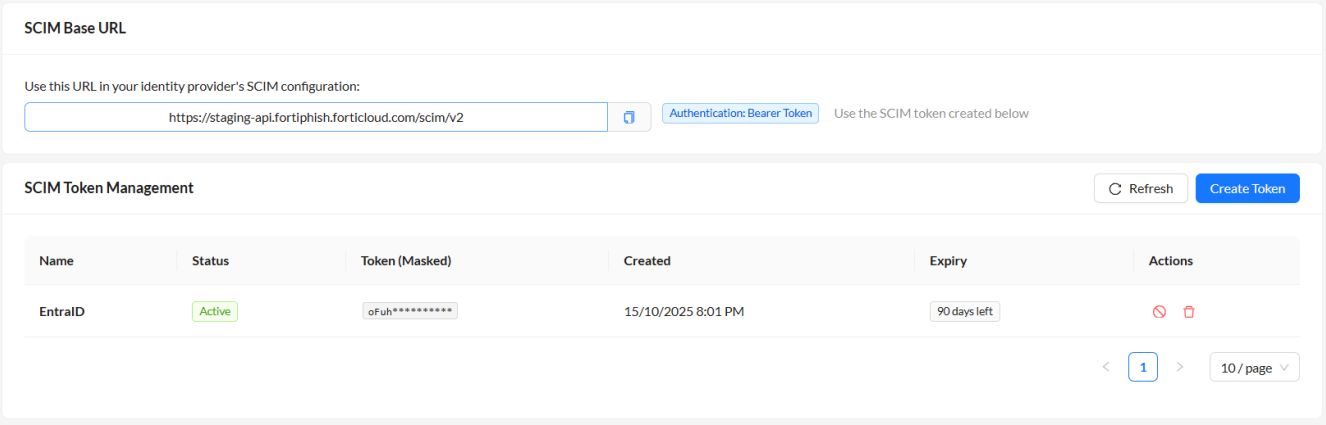
The *Settings* > *SCIM Token Management* page allows you to create and manage the bearer tokens required to authenticate and secure user provisioning with your Identity Provider (IdP) via SCIM 2.0 (System for Cross-domain Identity Management). SCIM automatically manages user accounts in FortiPhish based on changes in your IdP.

You will use the SCIM Base URL and one of the generated tokens to configure SCIM provisioning in your IdP. During this setup, you must configure attribute mapping to define which user and group fields are synchronized from your IdP to FortiPhish. See SCIM Attribute Mapping.

- Create a SCIM Token
- Manage SCIM Tokens

For detailed information on SCIM provisioning for Microsoft Entra ID, see FortiPhish SCIM Provisioning for Microsoft Entra ID.

The *SCIM Token Management* table lists all tokens you have created, displaying the *Name*, *Status*, *Token (Masked)*, *Created date*, *Expiry date*, and available *Actions (Revoke and Delete)*



Currently, *Microsoft Entra ID* is the only supported Identity Provider for SCIM provisioning.

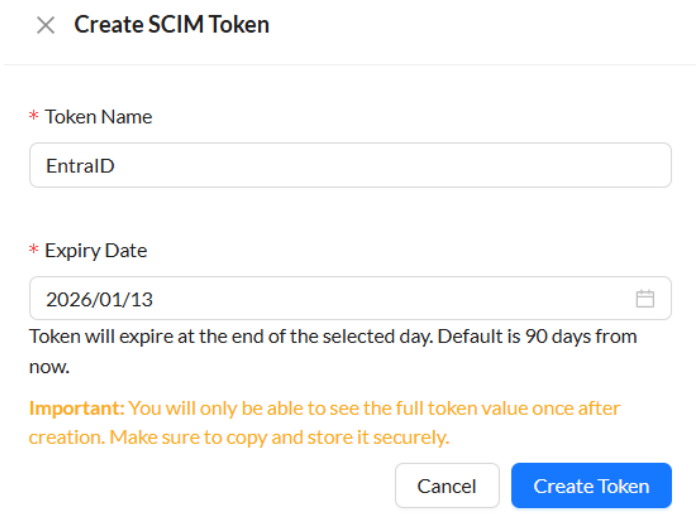
Create a SCIM Token

You must generate a SCIM token and use it as a Bearer Token to enable secure communication between your Identity Provider and FortiPhish.

1. Go to *Settings* > *SCIM Token Management* page, click *Create Token*. The *Create SCIM Token* window opens.
2. In the *Token Name* field, enter a name for the token.
3. In the *Expiry Date* field, select an expiration date for the token.

The token will expire at the end of the selected day. The default expiration is 90 days from the current date.

4. Click *Create Token*.



5. The unmasked token is displayed. Copy this token immediately and store it in a secure location.

You can only view the full token value once, immediately after creation. You cannot retrieve the full token value after you close this window.

6. Click *Close*. The new token appears in the *SCIM Token Management* table.

Manage SCIM Tokens

You can manage existing tokens from the SCIM Token Management table.

- *Revoke a Token*: To immediately invalidate a token and prevent any further SCIM synchronization using that token, select the *Revoke* icon under the Actions column for the token you want to revoke.
- *Delete a Token*: To delete a token, select the *Delete* icon under the Actions column for the token you want to delete.

When you delete a SCIM token from FortiPhish, the existing imported groups and users lose their association with the Identity Provider but remain in FortiPhish, and their *Created* field changes from *SCIM* to *Others*. Once an entity is marked as *Others*, you can modify or delete it directly within the FortiPhish portal.

SCIM Attribute Mapping

Attribute mapping defines how user and group data are synchronized between your Identity Provider (IdP) and FortiPhish via SCIM 2.0.

User attributes

The following user attributes are required for successful user provisioning.

FortiPhish Attribute	Matching Precedence	Description
userName	1	Primary Identifier (Matching Key).
active		Required for user lifecycle management (enabling/disabling).
displayName		The user's full display name.
title		The user's job title or role.
emails[type eq "work"].value		User's email address.
name.givenName		User's first name.
name.familyName		User's last name.
addresses[type eq "work"].formatted		User's office location.
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNumber		The user's organizational employee ID.
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department		The user's department or organizational unit.
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:manager		The user's manager.

Group Attributes

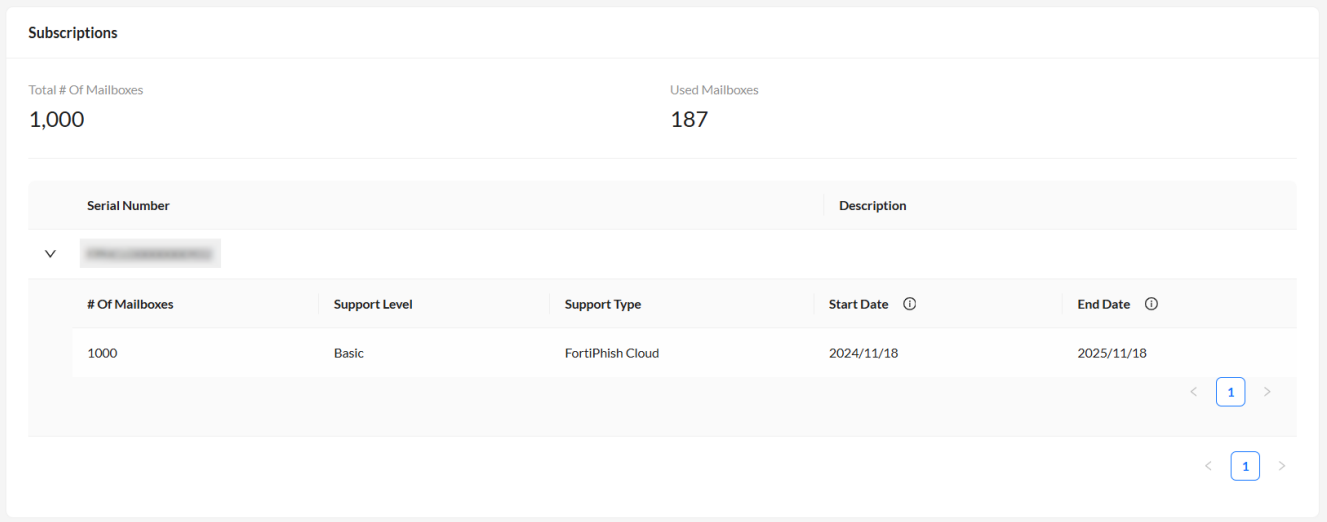
The following group attributes are required for successful group provisioning.

FortiPhish Attribute	Matching Precedence	Description
externalId	1	Primary Identifier (Matching Key).
displayName		The name of the group.
members		The list of user accounts belonging to this group.

Subscriptions

The Subscription page displays your current FortiPhish subscription details. You can view the total and used number of mailboxes, as well as license information, including the serial number.

Expand the serial number to see detailed license specifications, such as the total mailbox count, support level and type, and subscription start and end dates.



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.

Sending a test email failed with an error "550.5.7.509 Access Denied", what should I do next?

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 ensure the domain does not match any verified domains.

I am receiving a "421 4.7.0 Not allowed" error while sending an email campaign. What does it mean?

This error occurs when SMTP server tries to open more connections than allowed in a given period. There are two solutions.

1. *Increase the sending limit*: You can adjust your mail server settings to allow more connections. Following are the recommended settings.
   - Number of connections in 30 minutes: *100*
   - Number of emails per connection: *200*
2. *Retry the campaign* : If you don't want to change server settings, retry sending your email campaign until all emails are delivered.

Why are images not displayed in phishing simulation emails?

Using *.svg* image format can cause images to not display correctly in phishing simulation emails. To resolve this issue, please use *.png* images instead.

Why do emails show as opened in campaign recipient statistics, even if I haven't opened them?

Email scanners, such as Trend Micro and similar tools, often cause this behavior. These scanners proactively open emails to check for malicious content. This action registers as an *Open* in FortiPhish, even though the intended recipient hasn't viewed the email. To resolve this, safelist FortiPhish traffic within your email scanners.

Why are FortiPhish emails going to quarantine in Microsoft 365 instead of the inbox?

This typically occurs because Microsoft 365's security filters are flagging the emails. To resolve this, follow the steps in Safelisting FortiPhish in Office 365. Ensure you add the sender email domain configured in your FortiPhish campaign to your Microsoft 365 safelist.

Microsoft Exchange Online / Microsoft 365 users receive a "Need admin approval" error when attempting to report phishing emails using the FortiPhish Alert Button in Outlook.

The FortiPhish Alert Button requires Microsoft Graph API permissions (*Mail.ReadWrite*, *Mail.Send*, *User.Read*) to function correctly. Ensure your administrator grants these permissions. For detailed steps, see Adding FAB in Exchange Online / Microsoft 365.

www.fortinet.com