Administration Guide

FortiSAT 26.2.0

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

April 13, 2026
FortiSAT 26.2.0 Administration Guide
76-262-1249708-20260413

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-04-13	Initial release.
2026-05-08	Updated LDAP Server topic.

Introduction

FortiSAT is a security awareness and phishing simulation platform designed to reduce the risk of successful social engineering attacks. By combining realistic phishing simulations with targeted educational content, the platform helps your organization build a resilient security culture.

FortiSAT helps your organization identify high-risk individuals and train them to protect the corporate network. The platform includes the following core capabilities.

- **Phishing Simulations**: Launch simulated phishing email campaigns to test your employees and analyze how they interact with them. These simulations identify specific behavioral weaknesses and vulnerabilities within your organization.
- **Security Training**: Launch training campaigns featuring targeted modules and quizzes to strengthen user knowledge. These campaigns can be assigned as proactive organizational training or as standalone educational initiatives, with users consuming content through a dedicated *Learner Experience* portal.
- **Remedial Training**: Configure training campaigns to automatically enroll users in specific modules the moment they fail a phishing simulation. Enrollment is based on triggers such as opening the email or clicking a link.
- **Smart Groups**: Organize users dynamically using rule-based logic. Smart Groups automatically update based on user attributes or campaign performance (such as users with failed phishing attempts), ensuring targeted delivery of content.
- **Monitoring and Analytics**: Track the progress of active campaigns through centralized dashboards. These dashboards provide real-time visibility into user behavior, campaign engagement, and training completion rates.
- **Generating Reports**: Generate and export audit-ready detailed reports in *PDF* format to meet compliance requirements.

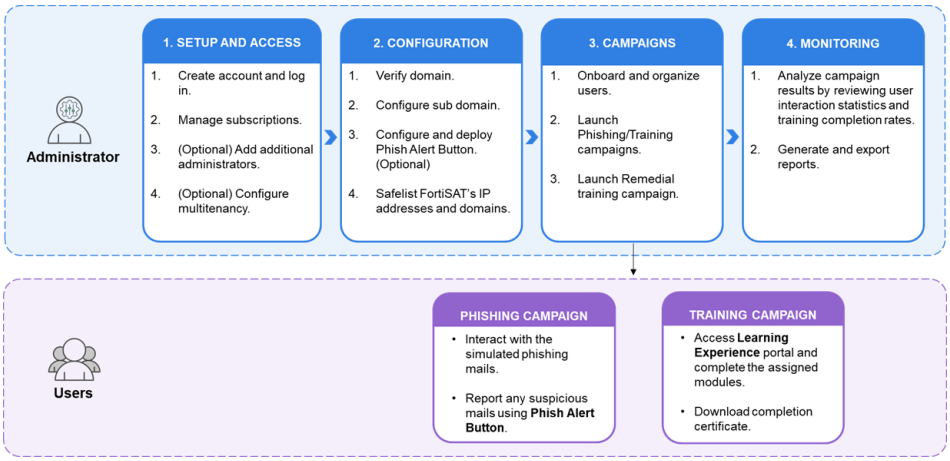
Existing FortiPhish Users

To ensure your existing configurations continue to function correctly during the transition to FortiSAT, please perform the following:

- **Update Safelisting**: Add the following IP addresses and domains to your safelist. This is mandatory for LDAP synchronization and ForitSAT Phish Alert Button (PAB) functionality. See Product and IP Safelist.
  - **LDAP Server**: Add IP *52.49.221.140* and domain *fortisat.forticloud.com*
  - **FortiSAT Phish Alert Button**: Add IP *99.81.86.32* and domain *api.fphplugin.net*
- **Update SCIM Base URL**: If you have configured SCIM provisioning in Entra ID, you must update the *Tenant/Base URL* to: `https://api.fortisat.forticloud.com/scim/v2`

Operational Workflow

The following diagram illustrates the operational workflow of FortiSAT.



Administrator Actions

Administrators manage the platform through four key phases.

1. **Setup and Access**: Initialize the environment by creating an account and managing subscriptions. Administrators can also optionally add additional administrators or configure multitenancy for larger organizations.
2. **Configuration**: Prepare the technical environment by verifying domain ownership, setting up the custom portal domain, configuring the FortiSAT Phish Alert Button (PAB), and safelisting system IPs to ensure delivery.
3. **Campaigns**: Onboard your users and organize them into groups. Launch *Phishing Campaigns* to test behavior or *Training Campaigns* to build knowledge. Enable *Remedial Enrollment* to automate education for users who fail simulations or based on their actions.
4. **Monitoring**: Analyze campaign results by reviewing user interaction statistics and training completion rates. Finally, generate and export audit-ready reports to track progress and compliance.

User Interaction

While the administrator governs the platform, users interact with it in two primary ways.

- **Phishing Campaign** users receive and interact with simulated phishing emails. They practice positive security habits by reporting suspicious messages using the PAB.
- **Training Campaign** users access the *Learning Experience* portal to complete their assigned educational modules and quizzes. Once finished, they can download their completion certificates.

Types of Training

There are two distinct methods for delivering educational content to users:

- **On Click Training**: This is a just-in-time learning experience assigned during the creation of a *Phishing Campaign*. It is triggered immediately when a user interacts with a simulation (e.g., clicking a link or

submitting data), directing them to a landing page with an embedded educational video.

- **Training Campaigns**: These are comprehensive educational modules and quizzes managed independently through the *Training Campaigns* section.

Getting Started

Setting up FortiSAT involves a sequence of steps to establish your identity, activate your subscription, and prepare your network for campaign delivery.

Complete the following configuration steps to prepare your environment for launching security awareness and phishing simulation campaigns.

1. Create and log in to your FortiSAT account. See Accessing FortiSAT.
2. Use DNS tokens to verify domain ownership and authorize the platform to send emails. See Domains .
3. Configure a subdomain for users to access *Learner Experience* portal. See Custom Portal Domains.
4. Configure the *FortiSAT Phish Alert Button* to allow your users to report suspicious emails, and download the required installation files for your email client. See FortiSAT Phish Alert Button.
5. Safelist FortiSAT's IP addresses, API endpoints, domains, and SMTP servers to ensure the successful delivery of phishing simulations and training notifications. See Product and IP Safelist.
6. Explore the administrative tools and workflows available to import and organize users, and to deploy and monitor campaigns. See Managing Your Security Awareness Program

Accessing FortiSAT

To begin using FortiSAT, you must have a FortiCloud account. This account serves as your single set of credentials to access the administration portal and manage your security awareness program.

Perform the following steps to access FortiSAT.

1. **Create a FortiCloud account**: If you do not have a FortiCloud account, go to the FortiSAT or FortiCloud landing page and click **Create Account**. For more information, see Creating a FortiCloud account.

   If you already have a FortiCloud account, you can use those credentials to log in directly
2. **Log in to FortiSAT**: Navigate to fortisat.forticloud.com.

   If you are logging in with an IAM user account or an OU account, select the required account after the system verifies your login credentials.
3. **Register your License**: Upon your first login, your account is automatically assigned a Free license. This allows you to manage up to **3** mailboxes and save up to **3** reports.

   If you have purchased the license, register it in FortiCloud, see FortiCloud Services > Asset Management > Registering assets.

> For information on managing subscriptions, assigning additional administrators, multitenancy, and customization, see Administering FortiSAT.

Managing Your Security Awareness Program

After completing the initial setup, follow the sections below to manage your administrative environment, organize users, and deploy campaigns.

Administering FortiSAT

Manage your subscriptions, multi-tenancy, and portal notifications. This section also covers assigning additional administrators through *IAM* or *External IdPs* and personalizing the portal interface with language and display settings.

For more information, see Administering FortiSAT.

Configuring System Settings

Configure system settings, including data retention periods for completed campaigns, *FortiSAT Phish Alert Button (PAB)* configurations, and the management of *SMTP* and *Azure AD* mail servers. This section also provides the IP addresses and domains that must be safelisted. Additionally, you can manage user settings for the *Learner Experience* portal, such as enforcing 2FA, managing third-party cookie requirements, and setting language options.

For more information, see System Settings.

Onboarding and Organizing Users

Onboard your employees and organize them into targeted audiences for your campaigns. You can add users manually, perform bulk imports using *CSV* files, or automatically synchronize users and groups using *LDAP*, *Azure AD*, or *SCIM*. Once onboarded, use Groups to create static lists of specific individuals, or use *Smart Groups* to dynamically categorize users based on rule-based logic, such as their department or previous campaign performance.

For more information, see User Management.

Creating and Managing Campaigns

Launch simulated phishing campaigns, training campaigns, and campaigns targeting remedial users who require additional intervention. Use the *Manage Campaigns* page to monitor active sessions, retry failed campaigns, or manage completed data through bulk deletion. Additionally, you can use the *Custom Templates* page to create tailored phishing email templates and landing pages to match your organization's specific needs.

For more information, see Campaigns.

Monitoring and Reviewing Campaign Results

Track the effectiveness of your security program through data visualization and detailed behavioral analytics. Use the *Dashboard* page to view your organization's phishing risk score, active campaign counts, and identified

high-risk users or groups. For deeper insights, the *Monitoring* section includes *Phishing* and *Training* dashboard pages to analyze specific user interactions such as link clicks, QR scans, and credential submissions, as well as training metrics to track completion rates and overdue assignments.

For more information, see Dashboard and Monitoring.

Generating Reports

Generate and export audit-ready reports to communicate program success and meet compliance requirements. The *Reports* page allows you to access organization-wide reporting for executive summaries, granular campaign details to analyze specific performance trends, and individual user profiles to track historical risk levels. You can also access and manage your saved reports for quick retrieval of frequently used data.

For more information, see Reports.

Exploring the Learner Experience

Review the interface where your employees engage with educational content and manage their training profiles. This section covers how users access assigned modules, complete quizzes, and track their progress through a dedicated portal.

For more information, see Learner Experience.

Administering FortiSAT

Administer your FortiSAT environment using the following options.

- Review available license options and your license status. See Managing Subscriptions.
- Add additional administrators and manage permissions using IAM, internal IdP, or External IdP. See Managing Administrator Access.
- Organize your environment into multiple tenants to manage distinct business units or sub-organizations independently. See Configuring Multitenancy.
- View and manage notifications of recent activity and alerts. See Managing Notifications.
- Personalize the administrator experience by adjusting the display language or mode. See Customizing FortiSAT Portal.

Managing Subscriptions

FortiSAT offers two tiers of service: *Free* and *Subscription*. Your tier determines your user capacity, reporting limits, and access to advanced management features.

The mailbox count will reset at the beginning of each month.

Feature	Free Tier	Subscription Tier
Usage	For initial evaluation of the platform.	Full access to platform capabilities scaled to your needs.
Mailbox capacity	Up to **3** mailboxes (Phishing and Training).	Additional mailbox capacity based on your specific purchase.
Saved reports	Up to **3** reports.	Up to **10** reports.

Supported Subscription Types

You can choose from three licensing models based on your organizational goals.

- **Phishing**: Dedicated license for phishing simulations.
- **Training**: Dedicated license for training campaigns.
- **Unified**: A combined license that includes both *Phishing* and *Training* capabilities.

Refer to the FortiSAT Datasheet for a complete list of available SKUs.

Licensed Features

The following features require an active subscription:

Feature	Description	License Requirement
Smart Groups	Access to dynamic, rule-based user organization.	Any one license (Phishing or Training).
SCIM Provisioning	Support for SCIM user provisioning.	
QR Code	Include QR codes in phishing emails to test user awareness of mobile-based threats.	Phishing license required.
Multiple Custom Domains	Select up to 4 verified domains per campaign; users will see different domains for campaign links.	
Skip Email Scanner Actions	Prevents mail scanners from triggering false positives to ensure accurate simulation results.	
Enforce 2FA	Require all users to use Two-Factor Authentication when accessing the *Learning Experience* portal.	Training license required.
Remedial Campaigns	Automatically enroll users in training based on their specific actions during a phishing simulation.	Both licenses (Phishing and Training)required.

Managing Your License

To purchase a new license or modify your current subscription, please contact Fortinet Support. The following update scenarios are supported.

- **Adding Services**: If you have a Phishing-only or Training-only license and need to add the other service, you can update your subscription. The original validity period of your license will remain the same.
- **Adding Mailboxes**: If you need to increase your user seat count, you can add additional mailboxes to your existing plan. In this scenario, the validity period of your subscription will be extended.

Navigate to the **Subscriptions** page in the FortiSAT portal to view your active subscription details. See Subscriptions.

Managing Administrator Access

You can assign additional administrators to help manage your FortiSAT environment, including tasks such as system configuration, user onboarding, campaign deployment, and reporting. The FortiSAT 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 FortiSAT portal based on the permissions set by the master user for the IAM portal. Sub users cannot access the IAM Portal.

IAM user types

FortiSAT supports the following IAM user types.

- **IAM Users**: IAM users can access FortiSAT, 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 FortiSAT, 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

FortiSAT 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.

IAM User Role	Permissions
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.

Configuring Multitenancy

FortiSAT leverages FortiCloud Organization to provide multitenancy, enabling Managed Security Service Providers (MSSPs) and large enterprises 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.

Managing Notifications

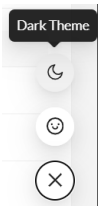
The *Notifications* icon in the portal banner provides real-time alerts regarding activity in your FortiSAT account, such as campaign milestones or system updates. Use the following features to manage your account alerts:

- Messages are color-coded to indicate their priority, and the background color changes to gray once a notification has been viewed or acknowledged.
- You can scroll through the notification history within the dropdown menu to review a chronological log of past account activity.
- Click **Read All** to clear and acknowledge all active messages at once.

Customizing FortiSAT Portal

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

- You can select the language for FortiSAT portal from **Settings > User Settings** page. See User Settings.
- Click the floating menu in the lower-right corner and select **Dark Theme** to switch the portal to a dark theme.



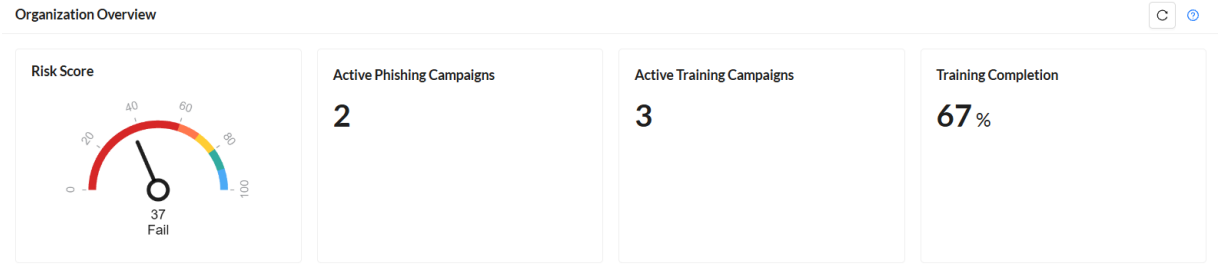
Dashboard

The *Dashboard* provides an overview of risk and awareness factor scores, active campaigns count, training completion rate, high risk users and high risk groups. You can use these metrics to identify high-risk individuals and groups that require immediate attention or additional training.

Organization Overview

This section displays key performance indicators averaged across all time periods.

- **Risk Score**: Your organization's overall risk score and grade. The risk score reflects the average of all previous campaign risk scores.
- **Active Phishing Campaigns**: The total number of phishing simulations currently in progress.
- **Active Training Campaigns**: The total number of educational initiatives currently in progress.
- **Training Completion**: The percentage of users who have finished their assigned training modules.



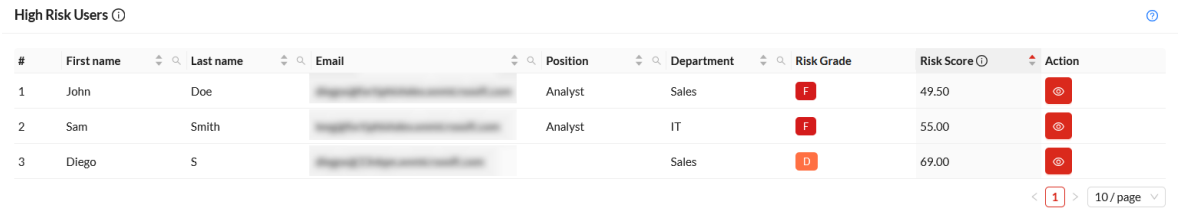
High Risk Users

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.
Position	The user's role if available.
Department	The user's department if available.
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.

Risk grades are determined by the user's risk score as follows:

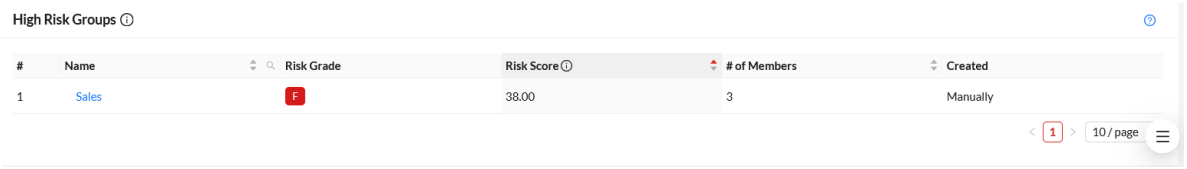
- **A**: Score > 89
- **B**: 80 – 89 (Default grade for users with no recorded actions)
- **C**: 70 – 79
- **D**: 60 – 69
- **F**: 0 – 59
- **NA**: Risk score does not exist or cannot be mapped.



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 group'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*, *SCIM*, *LDAP*, or *Smart Group*).



Monitoring

The Monitoring section includes detailed information for *Phishing* and *Training* campaigns.

- Evaluate how users interact with Phishing campaigns by tracking metrics such as email opens, link clicks, and information submitted on landing pages. See Phishing.
- Monitor the progress of your Training campaigns by tracking user completion rates, in-progress modules, and overdue assignments. See Training.

Phishing

The *Monitoring* > *Phishing* page provides an overview of your phishing simulation campaigns. Use this dashboard to analyze engagement metrics, evaluate user group performance, and compare response trends over time.

Filtering data

You can customize the information displayed on the dashboard using the controls in the top-right corner.

- 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.

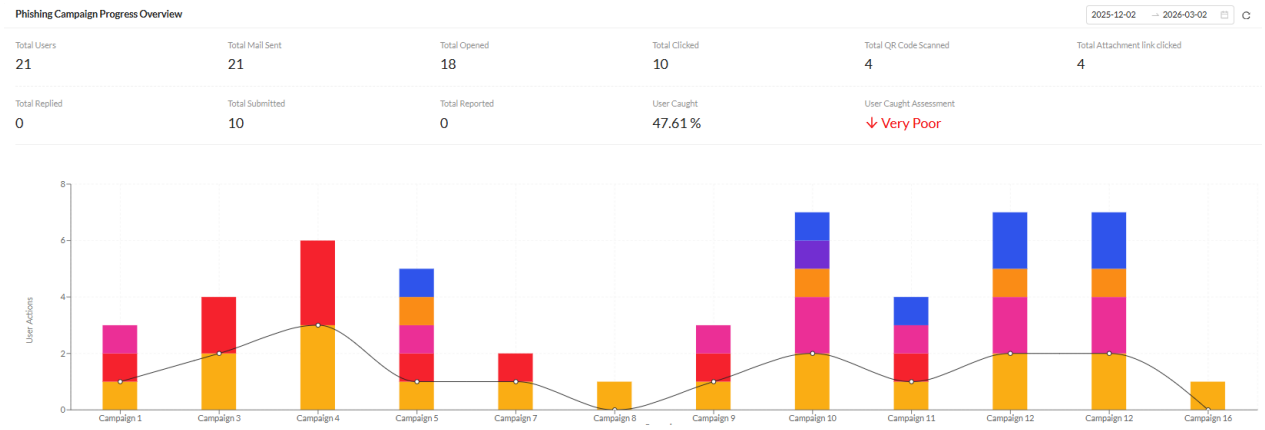
Overview

The *Overview* section displays the following metrics.

Total Users	The total number of users included in your phishing campaigns.
Total Mail Sent	The number of simulation emails successfully delivered to users.
Total Opened	The number of unique users who opened the simulation email.
Total Clicked	The number of users who clicked a link within the phishing email.
Total QR Code Scanned	The number of users who scanned a QR code included in the simulation.
Total Attachment Link Clicked	The number of users who clicked a link found inside an email attachment.
Total Replied	The number of users who responded directly to the phishing email.
Total Submitted	The number of users who entered data into a landing page or form.

Total Reported	The number of users who successfully reported the email using the FortiSAT Phish Alert Button.
User Caught	The percentage of the total user base that performed a risky action.
User Caught Assessment	A qualitative rating of your organization's performance based on the current *User Caught* percentage.

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



Hover a campaign in the chart to view how users interacted with the email for that campaign. The tooltip displays the following information:

Total Users	The total number of users included in the selected phishing campaign.
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 users who opened the email.
Clicked	The number of users who clicked the redirect link.
QR Code Scanned	The number of users who scanned the QR code.
Submitted	The number of users who entered information on the landing page.
Executed	The number of users who opened or executed the file attached in the phishing email. FortiSAT 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 users who replied to the email.
Reported	The number of users reported the email as suspicious.
Training Complete	The number of users who have finished the on click training.

Training Incomplete	The number of users who have been enrolled but did not finish the on click training.

Overall Responses

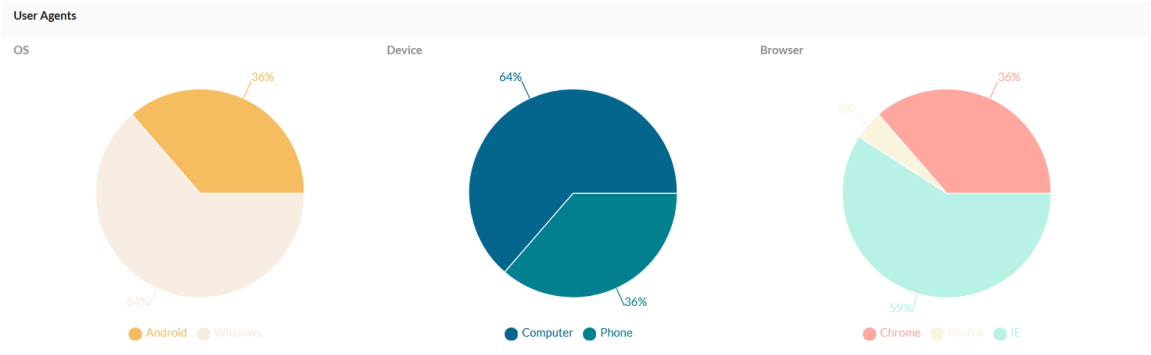
The *Overall Responses* monitor displays the ratio of users who passed or failed your organization's security training. The monitor also includes detailed information about the email distribution and click-rate across all campaigns. Hover over a piece of the chart to view the total number of emails for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

The *Overall Responses* monitor displays the following information:

Passed	The percentage of users that did not click or respond to campaign emails. This includes emails that were opened or opened and reported.
Failed	The percentage of users 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 users who opened the mail, but did not perform any other action.
Opened	The number of users who opened the mail.
Clicked Only	The number of users who clicked the redirect link, but did not perform any other action.
QR Code Scanned	The number of users who scanned the QR code.
QR Code Scanned Only	The number of users who scanned the QR code, but did not perform any other action.
Link Clicked	The number of users who clicked the redirect link.
Submitted	The number of users who entered information on the landing page.
Reported	The number of users who reported the phishing email as suspicious.

User Agents

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

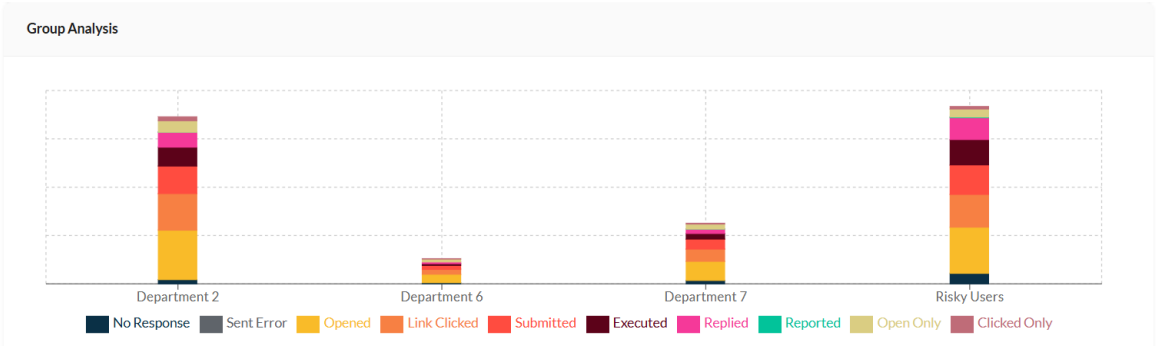


The *User Agents* monitor displays the following information:

OS	The operating system of the device.
Device	The device hardware.
Browser	The browser the user 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.



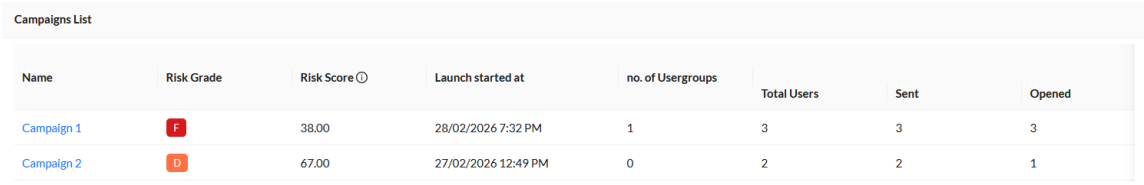
The *Group Analysis* monitor displays the following information:

No Response	The number of emails that were not opened.
Sent Error	The number of emails that bounced.
Opened	The number of users who opened the email.
Link Clicked	The number of users who clicked the redirect link.

QR Code Scanned	The number of users who scanned the QR code.
Submitted	The number of users who entered information on the landing page.
Executed	The number of users who opened or executed the file attached in the phishing email. FortiSAT 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 users who replied to the email.
Reported	The number of users who reported the phishing email as suspicious.
Open Only	The number of users who opened the mail, but did not perform any other action.
Clicked Only	The number of users who clicked the redirect link, but did not perform any other action.
QR Code Scanned Only	The number of users 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. Click Campaign name to view detailed information, see Viewing Phishing Campaign Statistics.



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 users	The total number of users in the campaign.

Sent	The number of emails sent to the user group.
Opened	The number of users who opened the email.
Clicked	The number of users who clicked the redirect link.
QR Code Scanned	The number of users who scanned the QR code.
Submitted	The number of users who entered information on the landing page. FortiSAT does not save the data entered by the user in the landing page.
Executed	The number of users who opened or executed the file attached in the phishing email.
Reported	The number of users who reported the phishing email as suspicious.
Replied	The number of users who replied to the email.
Training Complete	The number of users who have finished the on click training.
Training Incomplete	The number of users who have been enrolled but did not finish the on click training.

Training

The *Monitoring* > *Training* page provides an overview of your security training campaigns. Use this dashboard to monitor the progress of your training campaigns by tracking user completion rates, in-progress modules, and overdue assignments

The progress overview displays a list of all active and completed training campaigns. You can view the status (such as *Active* or *Completed*), scheduled *End Date*, and the total number of *users* assigned to each campaign.

Hover over a campaign's progress bar to view the number of users in each status category (*Completed*, *In Progress*, *Overdue*, and *Not Started*) and the total users count.

- **Completed**: The percentage of users who have finished all modules and passed any associated quizzes with a score of 80% or higher.
- **In Progress**: The percentage of users who have started at least one module but have not yet finished all content within the campaign.
- **Not Started**: The percentage of users who have not yet accessed any assigned training materials.
- **Overdue**: The percentage of users who failed to complete all modules and quizzes between their assigned due date and the campaign's end date.

Click the name of any campaign to open the *Campaign Summary* page for detailed campaign information. See Viewing Training Campaign Statistics.

User Management

The *User Management* section allows you to onboard your employees and organize them into targeted audiences for your security campaigns. Use these tools to manage individual profiles, synchronize data with external directories, and establish the domains authorized for your simulations.

- Add individual employees manually or through bulk CSV imports to track their personal risk scores and training progress. See Users.
- Organize users into static lists or rule-based Smart Groups to launch targeted campaigns. See Groups.
- Automate the onboarding process by synchronizing your users directly from LDAP, Azure AD, or SCIM. See User Sync.
- Manage the corporate domains used for your simulations and monitor their verification status. See Domains .

Users

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

- Importing users via CSV
- Editing user details
- Deleting a user
- Viewing user information

Importing users via CSV

You can perform a bulk import of users into FortiSAT using a CSV file.

1. Click *CSV* and select *Download CSV template*. The user template file is downloaded to your computer.
2. Enter the required user information in the template.

Field Name	Description
First name	The user's first name.
Last name	The user's last name.
Email	The user's primary email address.
Position	The user's job title or position.
Department	The user's organizational department.
Manager	The email address of the user's manager.
Department Lead	Set as *1* (for Yes) or *0* (for No). The *Department* field must be configured for a user to be set as a department lead.

3. Click *CSV* and select *Import CSV*. The *Upload CSV* dialog opens.
4. Upload the prepared CSV file. The new user users are automatically added to FortiSAT.

> A maximum of 10,000 users can be imported per CSV file.

Editing user details

To update the details of an existing user:

1. Navigate to *User Management* > *Users*.
2. Click the *Edit* icon next to the user whose details you wish to modify.
3. Update the necessary user information including in the dialog that opens.
4. Click *Submit* to save the changes.

> For users imported via *Azure AD*, *LDAP*, or *SCIM*, only the *Is department lead?* field is editable. To make changes to other fields, you must modify the user information in the respective client (*Azure AD*, *LDAP*, or *SCIM*) and then perform a synchronization.

Deleting a user

To delete a user:

1. Navigate to *User Management* > *Users*.
2. Click *Delete* icon next to the user you want to delete. Only users with *Others* or *Manually* in the *Created* field can be deleted directly from FortiSAT.
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.

> - Users imported via *Azure AD*, *SCIM*, or *LDAP* cannot be deleted directly within FortiSAT. To remove these users, you must delete them in the source client (*Azure AD*, *SCIM*, or *LDAP*) and then perform a synchronization after a few minutes.
> - If the Azure AD, SCIM, or LDAP client is removed from FortiSAT, the imported users will remain but their *Created* field will be updated to display *Others*. Once marked as *Others*, these users can be deleted in FortiSAT.
>
> If you edit the details of a user marked as *Others* (after the client was deleted), the *Created* field on the *User Management* > *Users* page will change from *Others* to *Manually*.
> - Changes made to a user will also be reflected in any groups they belong to.

Viewing user information

To view detailed user information:

1. Navigate to *User Management* > *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

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.
Department	The user's department.
Is department lead?	Displays *Yes* if user is set as a department lead; else, *No* is displayed.
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, available for users imported via *Azure AD*, *SCIM*, or *LDAP*.
User Created	Displays the method of user creation.
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.

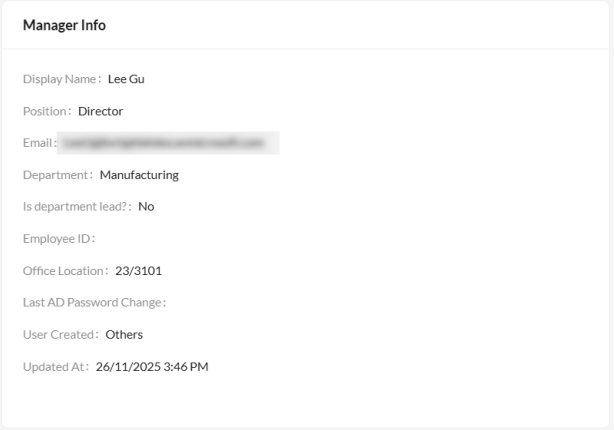
Click *Edit* to update the user details. Click *Delete* to delete the user. See Users.

Campaign counts exclude deleted campaigns.

Manager Information

The **Manager Info** card is displayed if the manager's information is available. The following information is displayed.

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.
Is department lead?	Displays *Yes* if user is set as a department lead; else, *No* is displayed.
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, available for users imported via *Azure AD*, *SCIM*, or *LDAP*.
User Created	Displays the method of user creation.
Updated At	The timestamp of the last modification to the manager's data.



Phishing Campaign Stats

The following user campaign information is displayed.

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.

The following user time of click training information is displayed.

Total Trainings Assigned	The total count of trainings assigned to the user.
Completed Trainings	The count of trainings the user has completed.

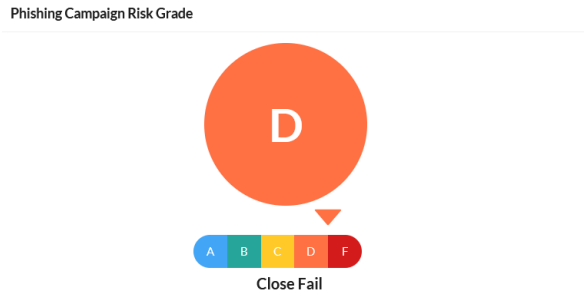
Training Campaign Stats

The following user training campaign progress information is displayed.

Not Started	The count of trainings not yet started.
In Progress	The count of trainings in progress.
Overdue	The count of trainings not completed past due date.
Completed	The count of completed trainings.

Phishing Campaign Risk Grade

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



Phishing Campaign 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.

Phishing Campaigns

Displays a list of active and completed phishing campaigns the user is or was part of. Click a campaign name to navigate to the corresponding campaign details page. See Viewing Phishing Campaign Statistics.

Training Campaigns

Displays a list of active and completed training campaigns the user is or was part of. Click a campaign name to navigate to the corresponding campaign details page. See Viewing Training Campaign Statistics.

Groups

Groups are distribution lists for your campaigns. 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.

> FortiSAT allows manual user imports of up to *15,000* users per group. For larger groups, we recommend using Identity Provider (IDP) groups instead.

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

Use the *Groups* page to:

- Creating a group list
- Adding imported user to a group
- Viewing user details
- Updating user details
- Filtering group list
- Hiding and Unhiding a group
- Exporting group details
- Deleting a group

Creating a group

To create a group:

1. Go to *User Management* > *Groups* and click *Create* > *Group*. The *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.

Adding imported users to a group:

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 FortiSAT, 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.

Updating a user's details:

To update a user's details:

1. Go to *User Management* > *Groups*, and select a group in the list.
2. In *Users 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 FortiSAT.

Filtering groups

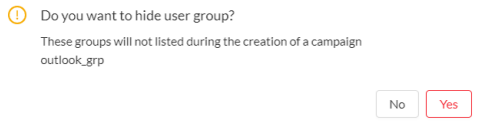
To filter the group, utilize the search option in the Name column to search for specific groups. Additionally, you can apply the risk grade filter in the Risk Grade column. All columns can be sorted by clicking on the arrow icons next to the column title.

Hiding and Unhiding 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:

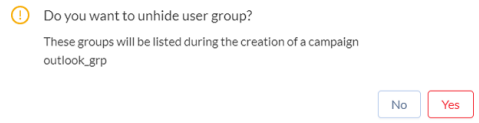
1. Go to *User Management* > *Groups*.
2. Click *Actions* menu and select *Hide groups*.
3. Select the desired groups and click *Hide*.
4. A confirmation message is displayed. Click *Yes*.



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 *User Management* > *Groups*.
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 *User Management* > *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.

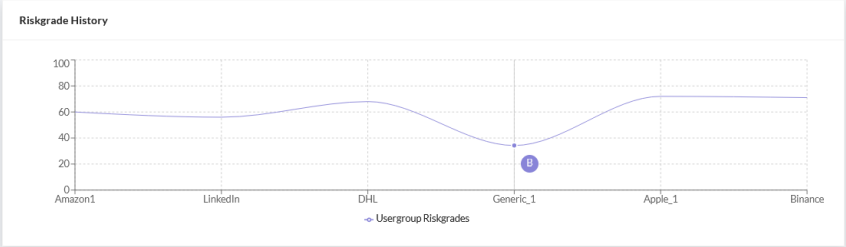
To delete a group:

1. Go to *User Management* > *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*.

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* and *User* 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 *User Management* > *Groups*.
2. Click a group in the list, then scroll down to view the chart.

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

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.

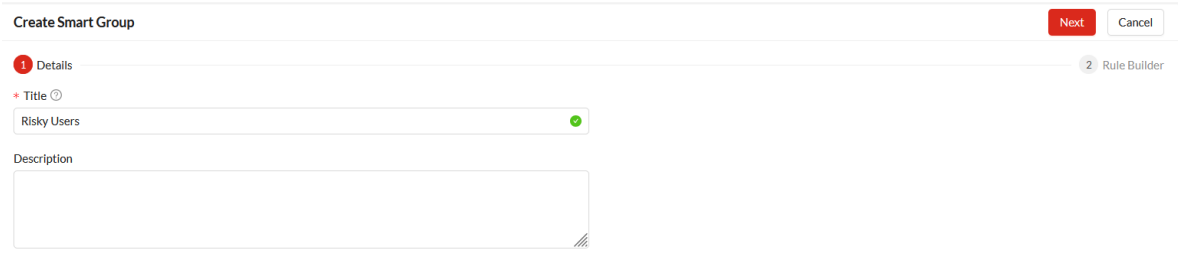
- A maximum of *five* Smart Groups can be created.
- For a user to be added to a Smart Group, they must be part of at least one phishing campaign. This ensures that the necessary parameters (risk grade, actions, campaign interactions, training history) are available for comparison with the defined rules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

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

Creating a Smart Group

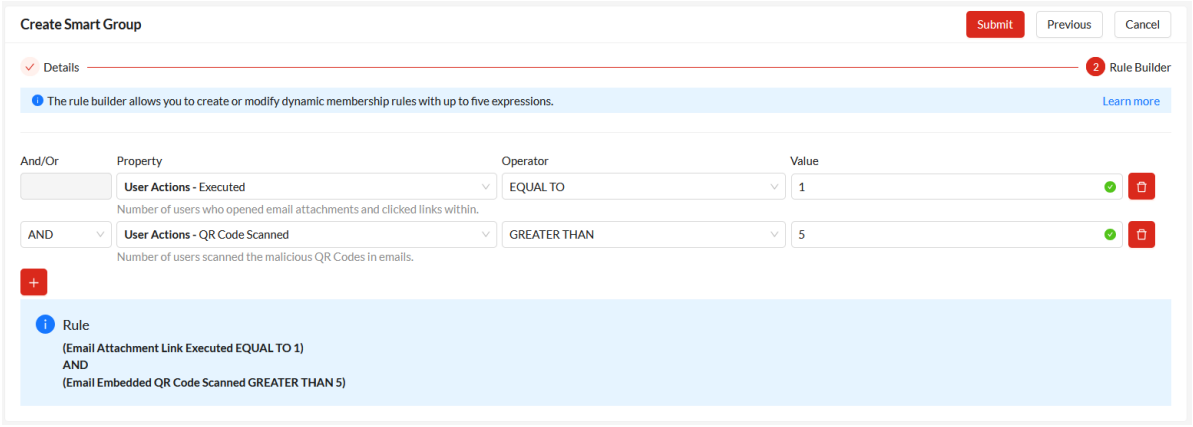
To create a Smart Group:

1. Navigate to *User Management* > *Groups*.
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*.

Viewing Smart Group details

To view Smart Group details:

1. Navigate to *User Management* > *Groups*.
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.
Users 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.
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.

Editing a Smart Group

To edit a Smart Group:

1. Navigate to *User Management* > *Groups*.
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

To delete a Smart Group:

1. Navigate to *User Management* > *Groups*.
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 FortiSAT for Smart Group rules.

Category	Property	Description
User	Risk Grade (Numeric)	The numeric grade between 1 and 100 assigned to the user . 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.

Category	Property	Description
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 On Click Training	Incomplete	Number of users who were assigned on click training but didn't complete.

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

User Sync

The *User Sync* page allows you to automate the onboarding and management of your user base by synchronizing data from external directories. The following methods are supported.

- Configure a connection to your LDAP server to import users and groups directly into the platform. See LDAP Server.
- Use the Microsoft Graph API to synchronize users and groups from your Azure Active Directory (Microsoft Entra ID) environment. See Azure AD.
- Enable System for Cross-domain Identity Management (SCIM) to allow external identity providers to push user updates to the portal in real time. See SCIM Provisioning.

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 FortiSAT.

- Adding a LDAP Server
- Synchronizing the LDAP Server

- Deleting a LDAP Server

Adding a LDAP Server

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

1. Go to *User Management* > *User Sync* > *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 users, are configured for the same time, the schedule that is executed first will delay the execution of the other until it is completed.

4. Expand *Advanced Field Matching* and configure the settings to map specific LDAP attributes to FortiSAT user fields.
   a. In the Object UUID Label field, enter the unique identifier attribute for your LDAP server type. The following table lists the recommended attribute for each supported server type.

LDAP server	Unique ID attribute
OpenLDAP	entryUUID
Active Directory	objectGUID
389 DS	entryUUID
Apache DS	entryUUID
Oracle DS	nsUniqueId
IBM DS	ibm-entryuuid

> The *Object UUID Label* field is mandatory. If you submit the configuration without entering a value, synchronization fails and the *Sync Status* field displays the error **Invalid Object UUID from server**.

b. (Optional) Configure the remaining Advanced Field Matching settings to map additional LDAP attributes to FortiSAT 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.

Synchronizing the LDAP Server

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

1. Go to *User Management* > *User Sync* > *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.

Deleting a LDAP Server

Perform the following steps to delete a LDAP server.

1. Go to *User Management* > *User Sync* > *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 FortiSAT, the existing imported groups and users lose their association with that client but remain in FortiSAT, 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 FortiSAT portal.

Azure AD

Connect FortiSAT to your organization's Azure AD tenant to import users and groups.

- Configuring Azure AD for FortiSAT
- Adding an Azure AD server
- Syncing the Azure AD server

- Deleting an Azure AD server

Configuring Azure AD for FortiSAT

Generate a Application ID and Secret in Azure AD to allow access for FortiSAT 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 FortiSAT. In azure portal:
   a. Go to *App Registrations* > *New Registration*.
      i. Provide a name for *App. Ex. FortiSAT-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 *User Management* > *User Sync* > *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 FortiSAT.
   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, 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 *User Management* > *Groups*. If only users are imported, they must be added to a group manually.
> - To update user information, the changes must be made within Azure AD server and then synced back to FortiSAT.
> - When you remove a user in Azure AD, FortiSAT 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 FortiSAT, go to *User Management* > *User Sync* > *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 *User Management* > *User Sync* > *Azure AD*.
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 FortiSAT, the existing imported groups and users lose their association with that client but remain in FortiSAT, 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 FortiSAT portal.

SCIM Provisioning

The *User Management* > *User Sync* > *SCIM Provisioning* 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 FortiSAT 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 FortiSAT. See SCIM Attribute Mapping.

- Creating a SCIM Token
- Managing SCIM Tokens

For step-by-step instructions on how to configure SCIM to your specific environment, refer to the following cookbooks.

- FortiSAT SCIM Provisioning for Microsoft Entra ID
- FortiSAT SCIM Provisioning for Google Workspace
- FortiSAT SCIM Provisioning for Okta

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.

Creating 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 FortiSAT.

1. Go to *User Management* > *User Sync* > *SCIM Provisioning* 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.

Managing 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 FortiSAT, the existing imported groups and users lose their association with the Identity Provider but remain in FortiSAT, 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 FortiSAT portal.

SCIM Attribute Mapping

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

User attributes

The following user attributes are required for successful user provisioning.

FortiSAT Attribute	Matching Precedence	Description
userName	1	Primary Identifier (Matching Key).
active		Required for user lifecycle management (enabling/disabling).
displayName		The user's full

FortiSAT Attribute	Matching Precedence	Description
		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.

FortiSAT 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.

Domains

Before you can launch campaigns, you must establish ownership of your corporate email domains. FortiSAT uses DNS tokens to verify that you are the authorized owner of a domain, ensuring deliverability and preventing unauthorized use. The *Domains* page displays a list of DNS tokens used to verify you own the domain. Use this page to create DNS tokens and monitor their status.

To verify a domain, you must generate a token in the FortiSAT portal, add it to your domain's DNS settings as a **TXT** record, and then confirm the verification.

Adding a Domain

Perform the following steps to initiate the verification process.

1. Log in to FortiSAT portal
2. Go to **User Management > Domains**.
3. In the **Enter Domain** text field, enter the domain address (for example, domain.com) and click **Add Domain**.
4. The platform will automatically generate a unique DNS token. Copy this token for use in your DNS settings.

Adding the Token to Your DNS Settings

The process for adding a TXT record varies depending on your domain provider (e.g., AWS, GoDaddy, or Cloudflare).

1. Log in to your domain provider's management console.
2. Navigate to the **DNS Management** area for your specific domain.
3. Create a new record and set the record type to **TXT**.
4. Enter the token generated by FortiSAT into the value field and save your changes.

> To ensure successful verification, confirm that both your **MX records** and **TXT records** are valid and configured correctly within your DNS settings.

Testing the Token (Optional)

You can confirm the record is live using the `nslookup` command in your terminal:

1. Type `nslookup` and press **Enter**.
2. Type `set type=txt` and press **Enter**.
3. Enter your domain (e.g., yourdomain.com).
   The output should display the FortiSAT token in the **text** section of the answer.

Example output:

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

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

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

Verifying the added Domain

Once the DNS record has been added, return to the FortiSAT portal to complete the process.

1. Go to **User Management > Domains**.
2. Locate your domain and, under **Actions**, click **Verify**. To search for a specific domain, select the search icon in the Name column header.
3. Once successful, the domain **Status** will change to a green check mark.

DNS propagation can take up to 48 hours. If the verification fails initially, please allow time for the DNS token to reflect in the global DNS cache before trying again.

Campaigns

The *Campaigns* section allows you to create, deploy, and manage campaigns.

- Launch new phishing or training campaigns, monitor progress, and analyze performance statistics. See Manage Campaigns
- Design and manage personalized phishing emails and landing pages. See Custom Templates.

Manage Campaigns

The *Manage Campaigns* page allows you to launch and monitor all phishing and training campaigns. You can track active progress, analyze completed results, and manage the lifecycle of each campaign.

- Create, manage, and monitor the performance statistics of your phishing simulations. See Phishing Campaigns.
- Create and manage training campaigns, including campaigns specifically assigned to Remedial Users. See Training Campaigns.
- Re-send emails that were not delivered or were blocked by the mail server during the initial rollout. See Retrying a Campaign.
- Manually end an active campaign to stop further user interaction and finalize results. See Completing a Campaign.
- Remove old campaign data to keep your dashboard organized and manageable. See Deleting Completed Campaigns.

Phishing Campaigns

Phishing campaigns allow you to strengthen your organization's resilience against phishing attacks by testing user awareness with simulated threats. You can launch campaigns using pre-configured global templates or design personalized content with custom templates.

Global templates

FortiSAT 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.

- Creating a Phishing Campaign
- Viewing Phishing Campaign Statistics

Custom templates

FortiSAT 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:

- Phish Email Templates
- Phish 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 a Phishing Campaign

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

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

1. Go to *Campaigns* > *Manage Campaigns* and click *Create Campaign*. The *Select Campaign Type* page opens.
2. Select *Phishing Campaign* and click *Next*.
3. The *Select a Template* page opens.

   To create a campaign from a custom template, click the *Custom Templates* tab. For information, see Phish Landing Pages.

4. 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, Phish Landing Pages.

		FortiSAT 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. FortiSAT 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 users they are the victim of a phishing attack. When the user 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 on click training modules: • *Phishing* • *Avoid Phishing Attack* • *Identify Phishing Attack* • *What is Phishing?* On click training is triggered immediately by user interaction with a phishing simulation mail and is different from the training modules assigned through a *Training Campaign*.	

Preview	In the text editor, compose the email body.You can insert *links*, *images*, *HTML source code* and *QR code*. Click *Preview* to preview the content. • You can use variables in the email body to generate dynamic data while the campaign is running. See, Template Variables. • QR code option is available only for *FortiSAT Phishing License* 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.

5. Configure the campaign details and click *Next*. The *Select Target Group* page opens.

6.

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 user will see a different selected domain when clicking a campaign link. This feature is available only for *FortiSAT Phishing License* users. Contact Fortinet Support team to upgrade.
SMTP Gateway Server	(Optional) Select an SMTP server from the dropdown. For information, see SMTP.
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.

7. In *Select Target Group* page, select the users.
   - 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.

8. 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.	

9. 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 user 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.

10. Click *Start campaign*. A confirmation message appears.
11. 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}}`	User's email domain	fortisat.com
`{{email_username}}`	User's username	johndoe
`{{num|min|max}}`	Generate a random number	`{{num|0|10000}}`4470 `{{num|0.0|10000.0}}` 4470.4
`{{recipient_email}}`	User's email	johndoe@fortisat.com
`{{recipient_firstname}}`	User's first name	John

Variable	Description	Output
{{recipient_lastname}}	User's last name	Doe
{{recipient_position}}	User's position	Manager
{{time}}	Time	3:04 PM
{{tracking_click_link}}	Link for tracking	https://smtp.fortisat.com/trackings/{{recipient}}
{{qr_code_link}}	QR code for tracking	QR code image will be inserted

Date with Layout or Offset

{{date|layout}}

Standard	Format
ANSIC	Mon Jan _2 15:04:05 2006
UnixDate	Mon Jan _2 15:04:05 MST 2006
RubyDate	Mon Jan 02 15:04:05 -0700 2006
RFC822	02 Jan 06 15:04 MST
RFC822Z	02 Jan 06 15:04 -0700
RFC850	Monday, 02-Jan-06 15:04:05 MST
RFC1123	Mon, 02 Jan 2006 15:04:05 MST
RFC1123Z	Mon, 02 Jan 2006 15:04:05 -0700
RFC3339	2006-01-02T15:04:05Z07:00
RFC3339Nano	2006-01-02T15:04:05.999999999207:00

Example:

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

Output:

09-0ct-20213:04 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 Phishing Campaign Statistics

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

To view the campaign statistics:

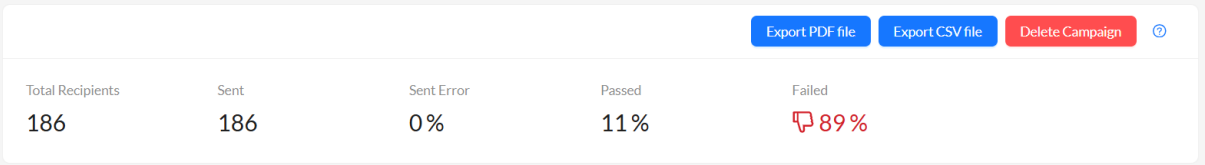
1. Go to *Campaigns*. The campaign list is displayed.
2. (Optional) Click the *Completed* tab. Campaigns are saved to the *Completed* tab after the campaign is completed.
3. Click the campaign name. The *Campaign - Details* page is displayed.
   - Campaign Overview
   - Campaign Summary
   - Risk Grade
   - Campaign Timeline
   - Campaign Preview
   - Campaign Stats
   - User Agents
   - User Stats
   - Usergroup Stats

Campaign Overview

The Campaign Overview widget displays the following information.

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

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



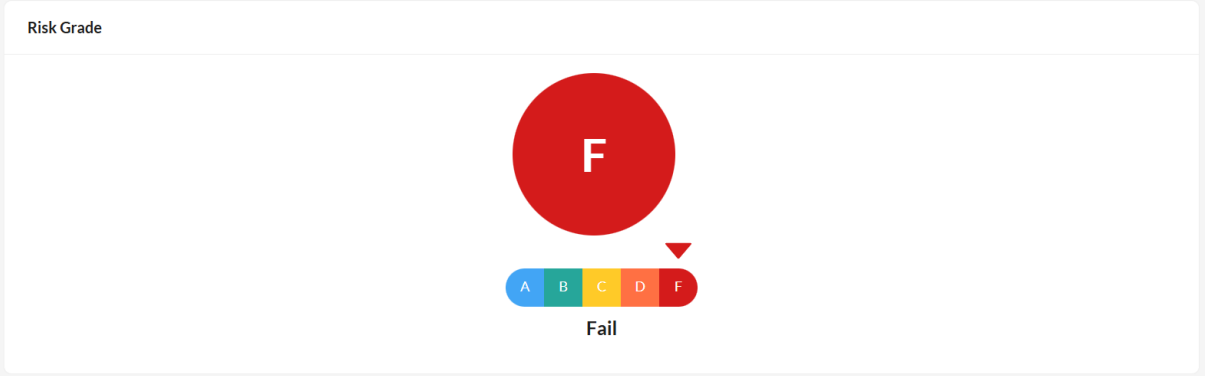
Campaign Summary

The *Campaign Summary* monitor displays the following information.

Campaign Name	The name you entered when you created the campaign.
Campaign Type	Training or Phishing Campaign.
Campaign Status	*Active* when campaign is in progress, *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*.
Sender Email	The email *From* address.
SMTP Gateway Server	The name and domain of the SMTP Gateway Server if one was used.
URL and Landing Page Domain	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 on click training topic assigned.

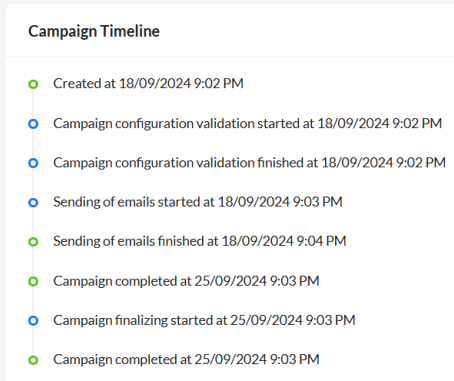
Risk Grade

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



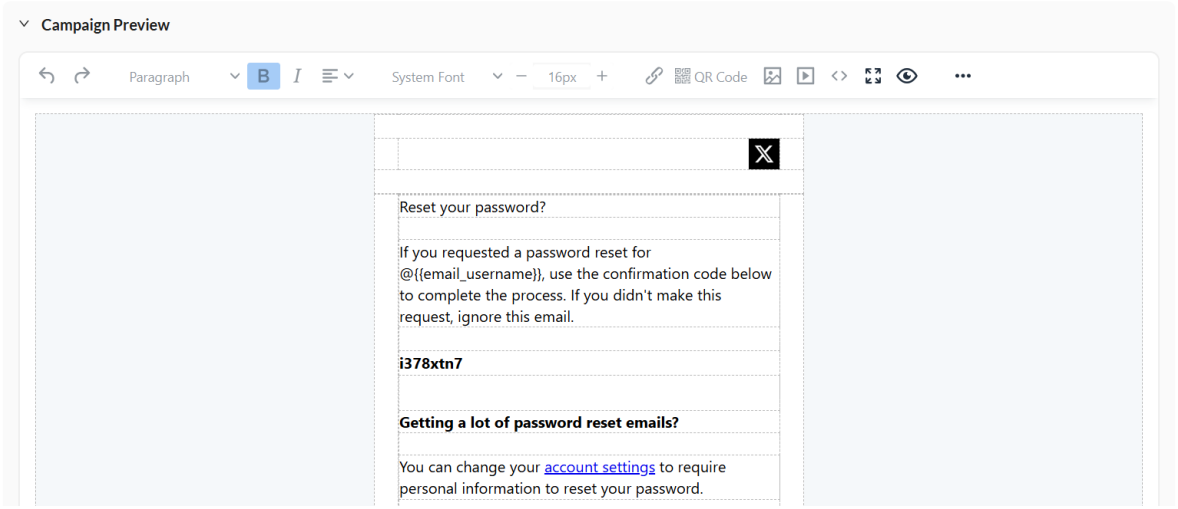
Campaign Timeline

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



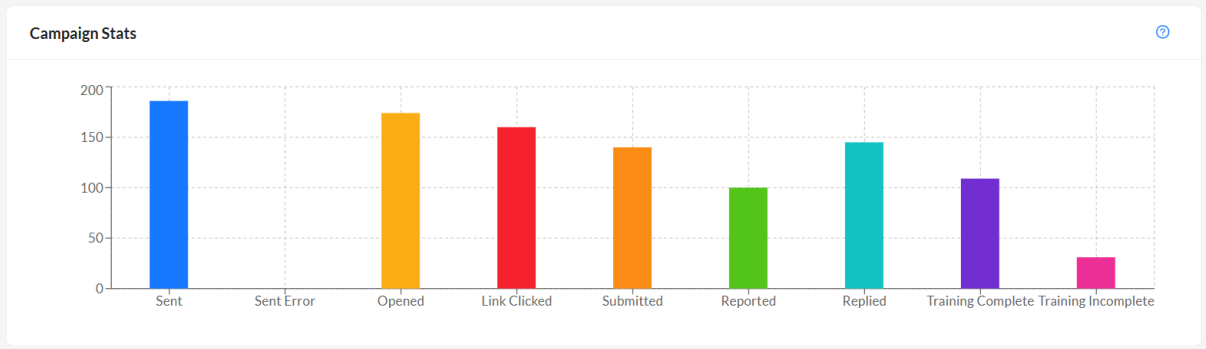
Campaign Preview

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 user interacted with the email. Hover over the chart to view the number of emails for each category.

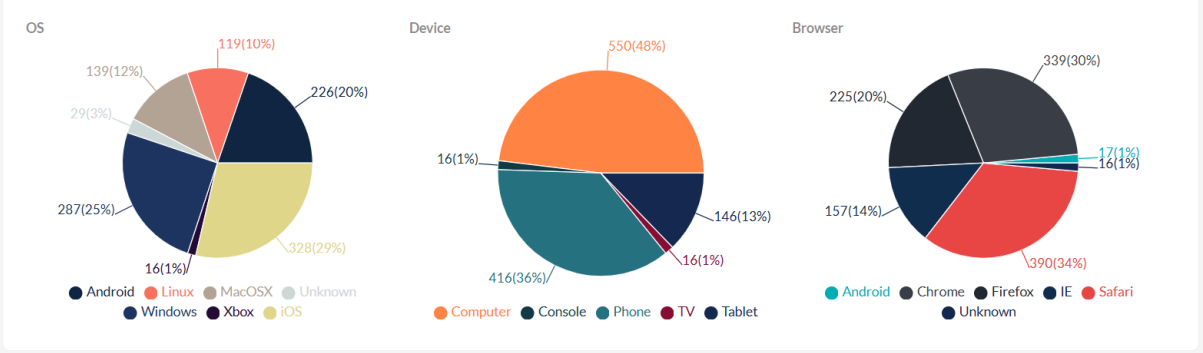


Sent	The number of emails sent to the user group.
Sent Error	The number of emails that bounced.
Opened	The number of users who opened the email.
Link Clicked	The number of users who clicked the redirect link.
QR Code Scanned	The number of users who scanned the QR code.
Submitted	The number of users who entered information on the landing page. FortiSAT does not save the data entered by the user in the landing page.
Reported	The number of users who reported the phishing email as suspicious.
Executed	The number of users who opened or executed the file attached in the phishing email. FortiSAT 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 users who replied to the email.
Training Complete	The number of users who completed the training. A user 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 users who have been enrolled but did not finish the training.

User Agents

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

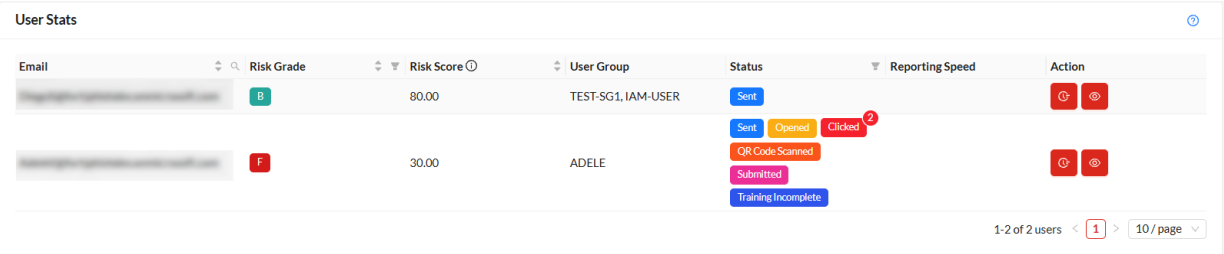


The *User Agents* monitor displays the following information:

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

User Stats

The *User Stats* monitor displays the user statistics.



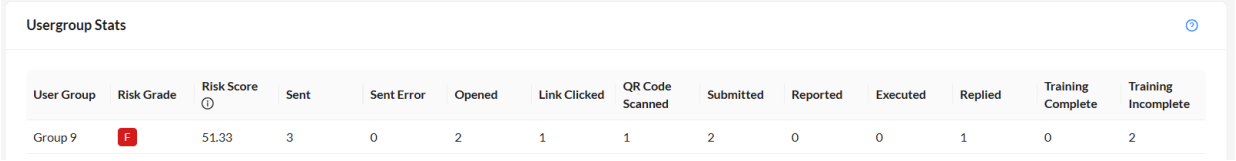
The *User Stats* monitor displays the following information:

Email	The user email address.
Risk Grade	The letter grade between *A and F* assigned to the user . 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 user belongs to.
Status	Displays the user'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 user has performed the action more than once.
Reporting Speed	The user's response time. • *Platinum*: Under 30 seconds • *Gold*: Under 5 minutes • *Silver*: Under 30 minutes • *Bronze*: Under 59 minutes An empty field indicates the user 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 user'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 users who opened the email.
Link Clicked	The number of users who clicked the redirect link.
QR Code Scanned	The number of users who scanned the QR code.
Submitted	The number of users who entered information on the landing page.
Reported	The number of users who reported the phishing email as suspicious.
Replied	The number of users who replied to the email.
Training Complete	The number of users who have finished the training.
Training Incomplete	The number of users who have been enrolled but did not finish the training.

Training Campaigns

Training campaigns are comprised of one or more modules. Users must complete all modules (and any associated quizzes, with a minimum score of 80%) in order to complete a campaign.

There are two types of modules that can be included within a campaign:

- **Micro modules** – Micro modules are 2-3 minutes in length. There is no quiz included for micro modules. However, users must access the quiz page at the end of each module to confirm they have viewed the associated module and videos. Micro modules can be used to introduce new topics, or as a review of previously completed training.
- **Base Modules** – Base modules are typically 8-15 minutes in length. There are knowledge check exercises throughout the module. Base modules also include a quiz (typically 7 questions) which users must achieve at least an 80% in order to pass. Once an 80% score is obtained by the user, the module is marked as complete.

Administrators can combine micro modules and base modules within a single campaign assignment.

The Fortinet FortiSAT supports running multiple campaigns across your organization at once. Training campaigns can be created and assigned to the entire organization, to specific groups or based on an event trigger from the phishing campaigns.

- Creating a Training Campaign
- Configuring Training Campaign with Remedial Users
- Viewing Training Campaign Statistics

Creating a Training Campaign

To create a training campaign:

1. Go to *Campaigns* > *Manage Campaigns* and click *Create Campaign*. The *Select Campaign Type* page opens.
2. Select *Training Campaign* and click *Next*.
3. Provide the following information and click *Next*.

Field Name	Details
Campaign name	This name should be meaningful to the users. It can reflect the frequency or a high level description of the content. It can be an assignment due to clicking a link in a phishing simulation email or submitting a username and password in a phishing simulation email. It should be descriptive enough that administrators will recognize when to use it and users will understand the purpose of the assignment.
Campaign start date	This is the date and time that users will begin to receive their training assignment emails. If you are assigning this campaign on a phishing event (User clicked, User replied, User submitted), this should match the scheduled date and start time of the associated phishing campaign.
Due date for users	This is the date and time that users who have not completed the entire campaign will begin to receive the overdue reminder email. This reminder email is sent only once. If you are assigning this campaign on a phishing event (User clicked, User replied, User submitted), this should match the scheduled date and end time of the associated phishing campaign.
Campaign end date	This is the date and time that the campaign will end. When this date has been reached, users can no longer complete training. If you are assigning this campaign on a phishing event (User clicked, User replied, User submitted), this date and time should allow any user who may have triggered a phishing event late in the phishing campaign enough time to complete the training. such as If your training campaign is 4 weeks long, you should give users 4 weeks after the training due date to complete the training.
Time zone	Set the appropriate time zone for the above dates.
Campaign welcome message (optional)	You can include any information that may be helpful to the users. This may include the type of training, support phone and email should users have questions or issues, and so on If you are assigning this campaign on a phishing event (User clicked, User replied, User submitted), you may want to include information on why they were assigned the training.
SMTP Gateway Server	(Optional) Select an SMTP server from the dropdown. For information, see SMTP.

4. Click *Start with a template* and select the template you would like to use:
   a. Select the *Training template* to select a pre-configured training campaign and click *Next*.

      The following templates are available. These templates are logical groupings of topics. You can neither modify nor delete these templates from the system.

Templates	Modules
Common Attacks	Social Engineering, Phishing, Malware,Business Email Compromise
Authentication	Introduction to Information Security, Password Protection, Multi-Factor Authentication, Access Control
Data Privacy and Security	Email Security, Data Privacy, Data Security, Mobile Security, Intellectual Property
Online Safety	Bad Actors, Working Remotely, Web Conference Security, Social Media

   a. Or click *Select your own modules*, then select the module grouping button, then select the individual modules. When you are finished selecting modules, click *Next*. Also, you can search for a specific module.

      - You can preview modules and get more information about the contents and languages supported by clicking on the *View details* link for each module.
      - If the language selected in User Settings is not available for a specific module, the *English (US)* version of the module will be used by default.
      - For the complete list of modules, see Training Module Reference Guide.

5. Reorder the content (if desired) by selecting the name and dragging the module to the correct position.
6. Click *Next*.
7. Choose if this campaign will be assigned to *Users*, *Groups* or *Remedial* users from phishing campaigns.

   You may select *Users/Groups* together, but selecting *Remedial Users* will override any prior user or group selections.

   a. If you select *Remedial Users*, you will be able to choose the applicable phishing campaign and user action. See Configuring Training Campaign with Remedial Users.
   b. If you select *All Users,* every user will receive the training assignment.
   c. If you select *Specific Groups*, you will be able to assign to users based on your imported department and title unique values.
8. Review and enable required *Email Notification* toggles to ensure your users receive the automated messages. Click *View Template* to preview the email content that will be sent to your users.
9. Click *Start campaign* to begin the campaign.

Configuring Training Campaign with Remedial Users

You can configure a training campaign to automatically enroll users who interact with a phishing campaign. This ensures that users who demonstrate risky behavior receive immediate, relevant education.

Adding Remedial Users

Perform the following steps during training campaign creation to add remedial users. See Creating a Training Campaign.

1. In the *Select Target Group* step, select the *Remedial Users* option.
2. Choose the active phishing campaign you want to monitor from the dropdown menu. The associated phishing campaign must be *Active*.
3. Choose one or more phishing events that will trigger the training enrollment. The following actions are supported:
   - **Opened**: The user opened the phishing email.
   - **Clicked**: The user clicked a link within the phishing email.
   - **Submitted**: The user entered credentials or information into a landing page.
   - **Replied**: The user responded to the phishing email.
   - **Executed**: The user opened or ran an attachment.
   - **Reported**: The user reported the email using the FortiSAT Phish Alert Button.
4. Complete the remaining email notification settings and click *Start Campaign*.

Once the campaign is started, any user who performs the selected action in the specified phishing campaign is automatically enrolled in the training. They will receive an enrollment email and the training will appear in their *Learning Experience* portal.

Viewing Training Campaign Statistics

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

To view the campaign statistics:

1. Go to *Campaigns*. The campaign list is displayed.
2. (Optional) Click the *Completed* tab. Campaigns are saved to the *Completed* tab after the campaign is completed.
3. Click the campaign name. The *Campaign - Details* page is displayed.
   - Campaign Overview
   - Campaign Summary
   - Campaign Timeline
   - User Stats
   - Usergroup Stats

Campaign Overview

The *Campaign Overview* widget displays the following information.

Total Users	The total number of users enrolled in this training campaign.

Not Started	The number of users who have not yet begun the training.
In Progress	The number of users who have started at least one module but have not yet finished all content.
Completed	The number of users who have successfully finished all modules and associated quizzes.
Overdue	The number of users who did not finish the training by the assigned due date.
Completed Percentage	The percentage of total enrolled users who have successfully finished the training.

Campaign Summary

The *Campaign Summary* monitor displays the following information.

Campaign Name	The name you entered when you created the campaign.
Campaign Type	Training or Phishing Campaign.
Campaign Status	*Active* when campaign is in progress, *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 Welcome Message	The custom message displayed to users.
Campaign Start Date	The date and time when the training becomes available and enrollment emails are sent.
Training Enrollment Confirmation	Indicates if an automated email is sent to notify users of their enrollment on the start date
Due Date For Users	The deadline for users to complete all assigned modules.
Due Date Alert	Indicates if an automated reminder email is sent to users with incomplete assignments on the due date.
Campaign End Date	The date and time when the campaign ends.
Campaign Completion Email	Indicates if an automated email (including a certificate) is sent to users upon finishing the training.
SMTP Gateway Server	The name and domain of the SMTP Gateway Server if one was used.
Modules	The list of specific training topics or micro-modules assigned to the users.

Campaign Timeline

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

User Stats

The *User Stats* monitor displays the following information:

Field	Description
Email	The email address of the enrolled user.
Name	The full name of the user.
User Group	The specific department or group the user belongs to within the organization.
Module Completion	Displays the number of modules completed out of the total modules assigned.
Enrollment Date	The date and time the user was officially added to the training campaign.
Completion Date	The date and time the user successfully finished all assigned modules and quizzes.
Training Status	The user's current progress, such as Not Started, In Progress, Completed, or Overdue.
Email Status	Indicates whether the enrollment or notification emails were successfully delivered to the user.
Action	Contains a link to the User Profile page.

Usergroup Stats

The Usergroup Stats displays group statics.

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

Training Module Reference Guide

The following training modules are available in FortiSAT.

Enterprise Modules

The following Enterprise modules are available:

- Access Control (12 minutes)
- Bad Actors (12 minutes)
- Business Email Compromise (9 minutes)
- Data Privacy (10 minutes)
- Data Security (12 minutes)
- Email Security (12 minutes)
- Generative AI (17 minutes)
- Insider Threat (10 minutes)

- Intellectual Property (9 minutes)
- Introduction to Information Security (10 minutes)
- Malware (9 minutes)
- Multi-Factor Authentication (11 minutes)
- Mobile Security (13 minutes)
- Password Protection (12 minutes)
- Phishing (10 minutes)
- Secure Travel (13 minutes)
- Social Media (10 minutes)
- Social Engineering (8 minutes)
- Web Conference Security (7 minutes)
- Working Remotely (10 minutes)
- AI-Powered Threats (15 minutes)

Education Modules

The following Education modules are available.

- Access Control (12 minutes)
- Bad Actors (12 minutes)
- Business Email Compromise (9 minutes)
- Data Privacy (14 minutes)
- Data Security (14 minutes)
- Email Security (13 minutes)
- Insider Threat (12 minutes)
- Intellectual Property (8 minutes)
- Introduction to Information Security (11 minutes)
- Clean Desk (8 minutes)
- Multi-Factor Authentication (13 minutes)
- Malware (11 minutes)
- Mobile Security (14 minutes)
- Password Protection (12 minutes)
- Phishing (13 minutes)
- Secure Travel (13 minutes)
- Social Engineering (12 minutes)
- Social Media (14 minutes)
- Web Conference Security (13 minutes)
- Working Remotely (13 minutes)
- Safer Online Gaming (14 minutes)
- Online Scams and Identity Theft (16 minutes)
- Online Learning (21 minutes)
- Educational Technologies (16 minutes)
- Cyberbullying Strategies (12 minutes)

- Cyberbullying (17 minutes)
- Generative AI (15 minutes)
- AI-Powered Threats (15 minutes)

Micro Learning Modules

Micro learning modules are approximately 2–3 minutes long each. They act as summary versions of longer base modules. The following modules are available.

- Business Email Compromise (3 minutes)
- Clean Desk (3 minutes)
- Data Privacy (3 minutes)
- Data Security (3 minutes)
- Email Security (3 minutes)
- Insider Threat (3 minutes)
- Malware (3 minutes)
- Password Protection (3 minutes)
- Phishing (3 minutes)
- Social Engineering (3 minutes)

Manager Modules

The following Manager modules are available.

- Cyber Security Frameworks for Managers (12 minutes)
- Deploying and Managing the Fortinet Security Awareness and Training Service (10 minutes)
- Security Awareness for Managers (14 minutes)

Retrying a Campaign

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

To retry a campaign:

1. Go to *Campaigns* > *Manage Campaigns* and click the campaign you want to retry.
2. Click *Retry Campaign*. The confirmation dialog opens.
3. Click *Yes*. The metrics are updated.

Completing a Campaign

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

Once a phishing campaign is completed, user actions are no longer captured. Consequently, no additional users will be automatically enrolled in any associated *Remedial Training* campaigns.

To complete a campaign:

1. Go to *Campaigns* > *Manage 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 *Completed* tab.

Deleting Completed Campaigns

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

- You can schedule completed campaigns to be automatically deleted at monthly intervals in the application settings page. See Campaigns.
- Once a phishing campaign is deleted, user actions are no longer captured. Consequently, no additional users will be automatically enrolled in any associated *Remedial Training* campaigns.

To delete a campaign:

1. Go to *Campaigns* > *Manage Campaigns* > *Completed*.
2. Select the campaign(s) you want to delete.
3. Click *Delete Campaign*. The confirmation dialog opens.
4. Click *Yes*.

Custom Templates

The Custom Templates page allows you to create custom landing pages and templates for your account.

- Create and customize the emails sent to users during a phishing campaign. See Phish Email Templates.
- Create custom web pages that appear when a user interacts with a simulated threat. See Phish Landing Pages.

Phish Email Templates

The *Custom Templates* > *Phish Email Templates* tab 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 phishing email 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:

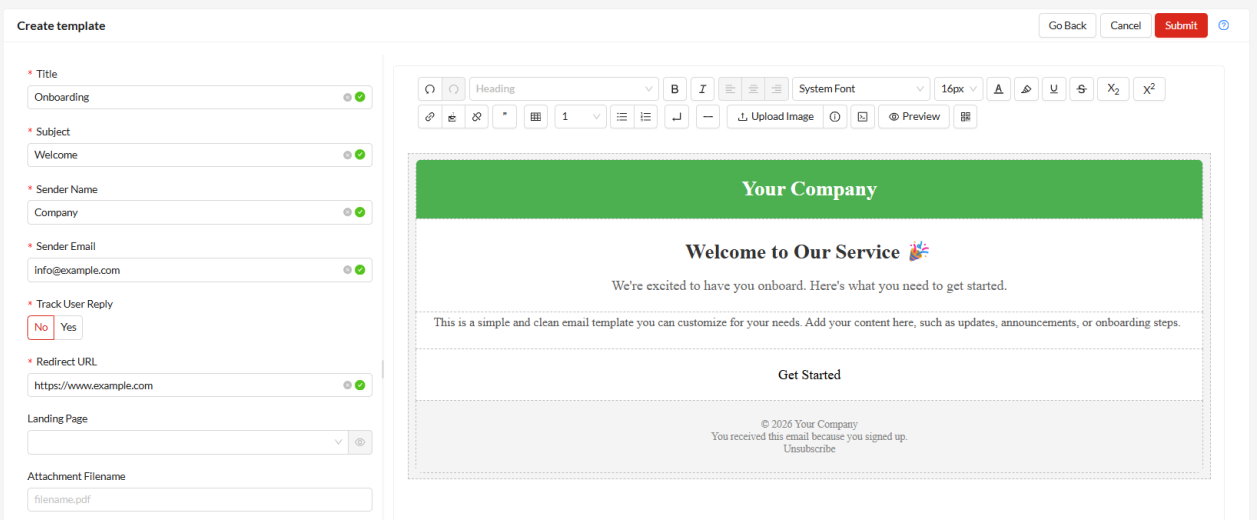
1. Go to *Custom Templates* > *Phish Email Templates*.
2. Click *New Template*. The *Create template* page opens.
3. Configure the template settings.

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 Phish Landing Pages.
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*, *HTML source code* and *QR code*. Click *Preview* to preview the content.

- You can use variables in the email body to generate dynamic data while the campaign is running. See, Template Variables.
- QR code option is available only for *FortiSAT 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 a Phishing Campaign.



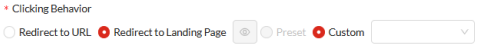
To edit a template:

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

Phish Landing Pages

You can create a custom phish 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 a Phishing Campaign.

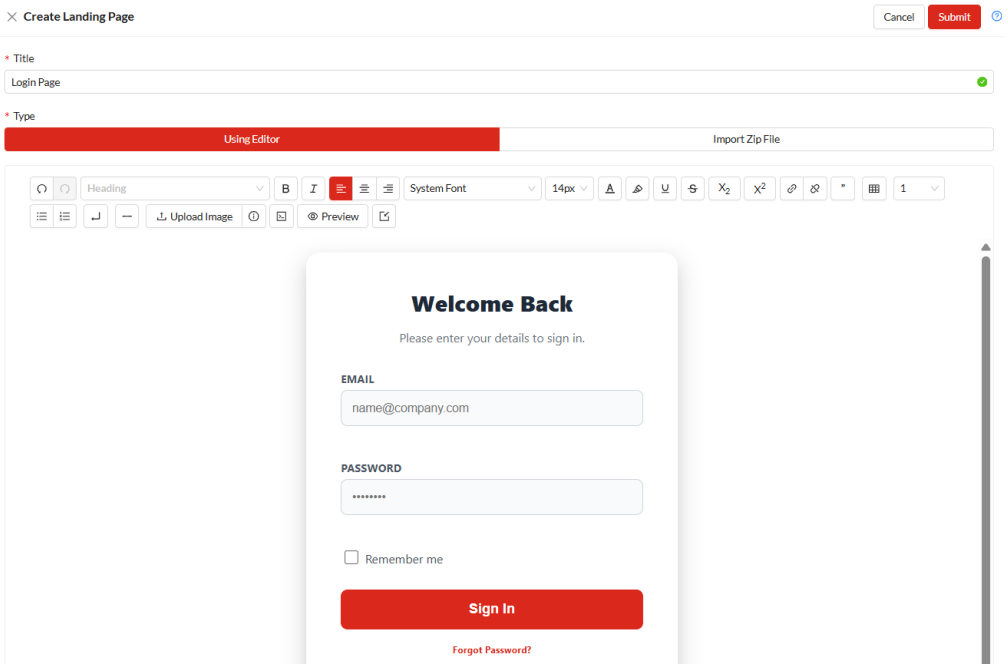


FortiSAT does not save the data entered by the user in the landing page.

Creating custom landing pages with the editor

To create a custom landing page with the editor:

1. Go to *Custom Templates> Phish Landing Pages*.
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 .
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:

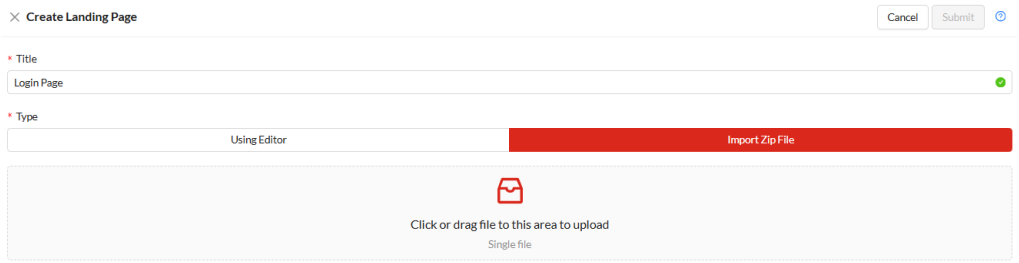
- A hidden tag with dynamic value used to track the user: `<input name="recp_uuid" type="hidden" value="{{.recp_uuid}}">`
- A submit form action with dynamic value set to `"{{.submit_url}}"`

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

To create a custom landing page with a Zip file:

1. Go to *Custom* > *Landing page*.
2. Click *Add Landing Page*. The Landing Page editor opens.
3. In the *Title* field, enter a name for the landing page.
4. Click *Import Zip File*.

5. Click the upload icon to navigate to the Zip file on you computer. Alternatively, you can drag the file onto the field.



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

Landing page variables

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

Supported variables for custom landing pages:

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

Settings

The *Settings* section allows you to configure campaigns settings, create alert buttons, add SMTP server accounts, and view IP addresses, API endpoints, and SMTP servers that must be safelisted, configure user settings, and set subdomain for *Learner Experience* portal.

- Set the period to automatically delete the completed campaign data and configure delays to prevent email scanners from triggering false positives. See Campaigns.
- Configure and deploy the FortiSAT Phish Alert Button (PAB) that allows users to notify suspicious emails. See FortiSAT Phish Alert Button.
- Connect your organization's mail servers, such as a SMTP server or Azure AD, to distribute simulation emails. See SMTP.
- View the necessary IP addresses and domains that must be safelisted to ensure successful email delivery. See Product and IP Safelist.
- Configure security requirements like two-factor authentication, third party cookies for users and set the default language for the *Learning Experience* portal. See User Settings.
- Configure a subdomain for Learner Experience portal. See Custom Portal Domains.

Campaigns

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

Enable Auto-delete

Schedule completed 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 options, 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 FortiSAT 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 FortiSAT 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 Phishing License users. Contact Fortinet Support team to upgrade.

FortiSAT Phish Alert Button

FortiSAT Phish Alert Buttons (PAB) allow email users 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.

Configuring PAB is required for *Phishing Simulation* campaign and is not required for *Training* campaigns.

To enable FortiSATPhish Alert Buttons (PAB):

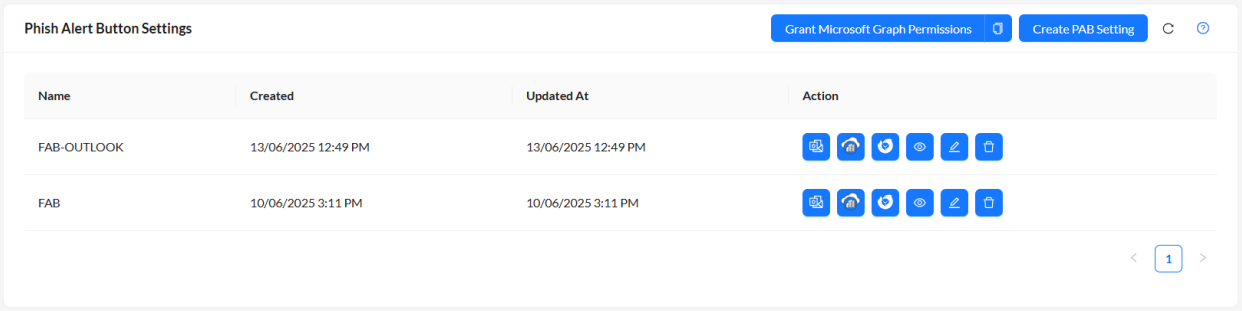
1. Create a FortiSAT phish alert button.
2. Install the button on Microsoft Exchange or Thunderbird.
   - Adding FortiSAT Phish Alert Button (PAB) in Microsoft Exchange Environments
   - Adding FortiSAT Phish Alert Button (PAB) in Thunderbird

Creating a FortiSAT Phish Alert Button

The FortiSAT 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 FortiSAT Phish 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.
Users	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 users send to report a suspicious email.
A response when the user reports a non-simulated phishing email	The email message body users see when they report a non-simulated email.
A response when the user reports a phishing security test email	The email message body users 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 FortiSAT Phish Alert Button (PAB) in Microsoft Exchange Environments

The FortiSAT Phish Alert Button (PAB) 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 FortiSAT Phish Alert Button prior to the 25.2 release must update their FortiSAT Phish Alert Button due to Microsoft phasing out legacy authentication tokens by **October 2025**.

Complete the following steps to install the new PAB:

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

Following are the compatibility and prerequisites for deploying the FortiSAT Phish Alert Button (PAB) 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)

Feature	Environment		
	Exchange On-Premises (Exchange 2016 or later)	Exchange Online / Microsoft 365	Hybrid Environment
			• FAB_OnPrem.xml (for On-premises 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 FortiSAT Phish Alert Button (PAB) 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 PAB 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 FortiSAT portal. See Creating a FortiSAT Phish 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 PAB in Exchange Online / Microsoft 365

Existing Exchange Online/Microsoft 365 and Hybrid environment customers who installed the FortiSAT Phish Alert Button prior to the 25.2 release must update their FortiSAT Phish 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 FortiSAT 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 FortiSAT portal, go to **Settings > Phish Alert Button**.
2. Click **Grant Microsoft Graph Permissions**.
3. Sign in with a global administrator account when prompted.

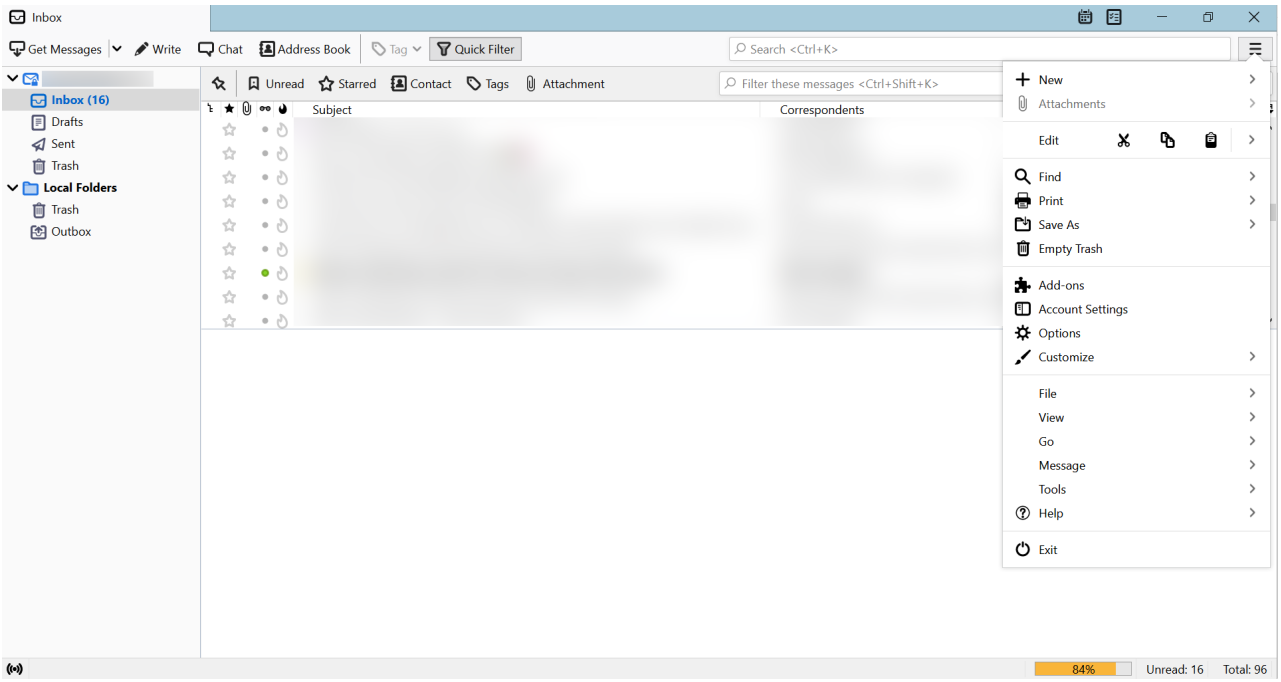
Adding FortiSAT Phish Alert Button (PAB) in Thunderbird

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.

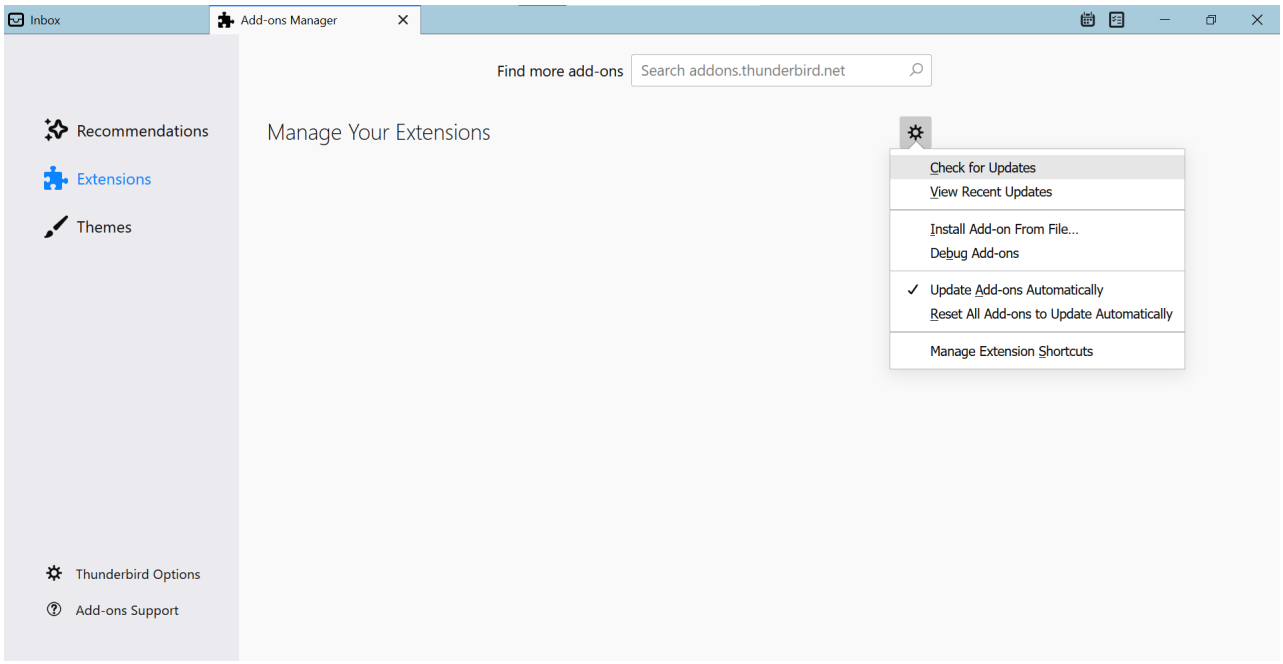
- This process requires Read/Write Mailbox permissions for your email client.
- The images in the following task are based on Thunderbird for desktop v 78.12.0. The user interface may look different than the one you are using. For more information, please refer to the product documentation.
- Thunderbird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

To install the PAB:

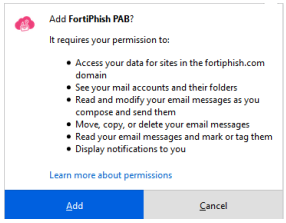
1. In Thunderbird, click the Thunderbird menu and select *Add-Ons*.



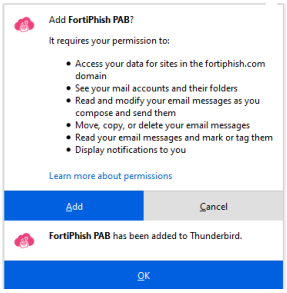
2. In the *Extensions* tab, click the gear icon, and click *Install Add-on From File...*.



3. Navigate to the location of the *xpi* file on your device and click *Open*. The *Add FortiSAT PAB* confirmation dialog opens.
4. Click *Add*. A confirmation message appears.

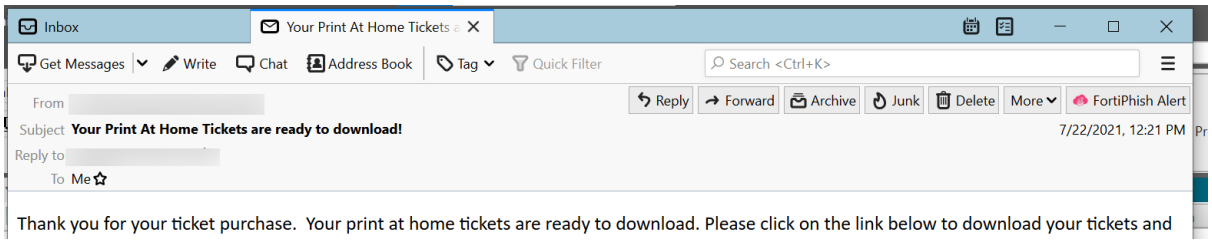


5. Click *OK* and click *Add* to close the dialog.

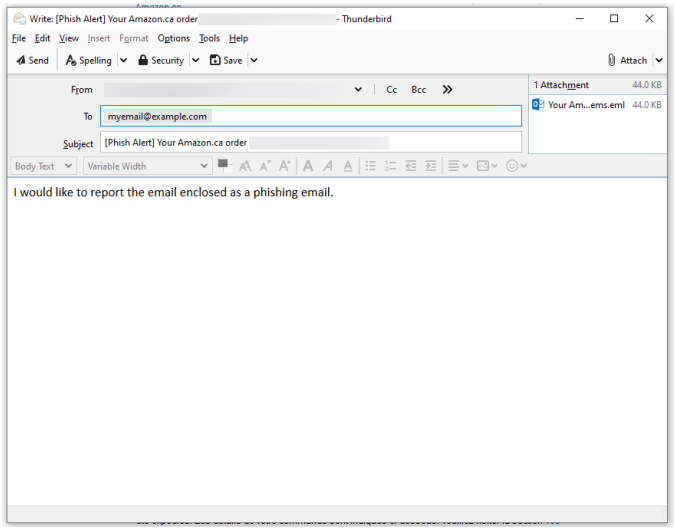


To test thePAB:

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

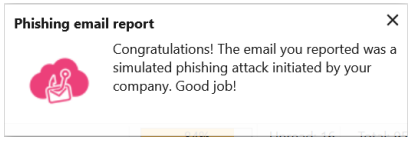


2. Click the *Phish Alert* button to open the composer. The suspicious email is attached as an EML file.



Thunderbird email users 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

The *Settings* > *SMTP* page allows you to use your organization's own mail servers to distribute emails. FortiSAT uses the *FortiSAT Mail Server* by default for all communications unless a specific custom SMTP server is configured and selected.

- If you enable the **Default Server** toggle for a SMTP server, the platform will use your selected server instead of the default *FortiSAT Mail Server* to send reports, *Learning Experience Portal* onboarding notifications, and *Learning Experience Portal* password reset emails.
- Only one server can be selected as the default at any time.
- During the creation of individual campaigns, you can manually select the SMTP server. If no custom server is selected, the system defaults to the *FortiSAT Mail Server*.
  - **Phishing Campaigns**: The selected server sends simulated phishing emails.
  - **Training Campaigns**: The selected server sends *Training Assigned*, *Due Date Reminders*, and *Training Completed* notifications.

Adding a SMTP server

Perform the following steps to add a SMTP server.

1. Navigate to **Settings > SMTP** tab.
2. Click **Add Account**.
3. Enter the following required details, and click **Submit**.

Field	Description
Name	A unique name for the mail server.
User Name	The username used to authenticate with the SMTP server.
Password	The password used to authenticate with the SMTP server.
SMTP Name	The IP address or domain name of the outgoing SMTP server.
Port	The port number used by the server to send emails.
Security	The encryption method used: *SSL*, *TLS*, or *STARTTLS*.
Protocol	The authentication method: *LOGIN*, *PLAIN*, or *CRAM-MD5*.
Max Connections	The maximum number of simultaneous connections allowed.
Max Mails Per Hour	The maximum number of emails the server can receive every hour.
Default Server	A toggle to use this server instead of the FortiSAT default SMTP server.

Product and IP Safelist

To ensure that simulated phishing emails and training notifications are delivered successfully, you must safelist FortiSAT's IP addresses and domains.

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

For step-by-step instructions on how to apply these settings to your specific environment, refer to the following cookbooks.

- Safelisting FortiSAT in Office 365
- Safelisting FortiSAT in FortiMail
- Safelisting FortiSAT in Gmail

User Settings

The *Settings* > *User Settings* page allows you to configure the environment and security requirements for users accessing the *Learning Experience* portal.

Use the following settings to manage the user experience:

- **Enforce 2FA for All Users**: Enable this toggle to require all users to set up and use two-factor authentication during login. If this is enforced, users cannot disable 2FA from their individual accounts.
- **Enable Third-Party Cookies**: Enable this toggle to improve video playback performance and loading speeds within the portal. When this setting is enabled, users have the option to modify this setting within *Learning Experience* portal. By default the third-party cookies is enabled. If the setting is disabled, the toggle on the *Settings* page in *Learning Experience* portal becomes greyed out and users cannot modify it.
- **Select Language**: Choose a default language for both the FortiSAT portal and the *Learning Experience* portal. If available, training content will also display in the selected language. Users can later change their individual language preference within the *Learning Experience* portal.

Custom Portal Domains

You can personalize the URL your employees use to access the *Learner Experience* portal by setting a custom subdomain. Configuring a custom portal domain is a requirement for launching *Training Campaigns*, as it provides the primary access point for the *Learning Experience* portal; however, this setting is not required for *Phishing Simulation* campaigns.

Perform the following steps to configure your subdomain.

1. Navigate to **Settings > Custom Portal Domain** in the FortiSAT portal.
2. Enter your desired name in the subdomain field. The entry must be between 1 and 63 characters using only letters (a-z, A-Z), numbers (0-9), or hyphens.
3. Ensure your entry does not start or end with a hyphen; the system will automatically convert all characters to lowercase.
4. Click **Save Subdomain**. The confirmation popup appears.
5. Review and click **Submit** to acknowledge and finalize the setting.

Your full portal URL will follow the format: `<yoursubdomain>.fortisat.forticloud.com`.

The custom portal domain can only be set once. Ensure the spelling and naming convention are correct before submitting, as this value cannot be changed later.

If you are using a **Free Tier** subscription, FortiSAT automatically appends an **-eval** suffix to your configured subdomain.

Example: If you configure your subdomain as **<companyname>**.fortisat.forticloud.com, it will be provisioned as **<companyname-eval>**.fortisat.forticloud.com.

The **-eval** suffix is not automatically removed upon upgrading to a paid subscription. To remove the suffix, please contact Fortinet Support.

Reports

The *Reports* page allows you to generate and manage detailed information about your security awareness program. The page is organized into two tabs.

- **Reports Type**: Contains templates that you can select to generate a new report. See Creating a New Report.
- **Saved Reports**: Displays a list of your generated reports. You can download reports once they are ready, or edit and delete them as needed. See Saved Reports.

Creating a New Report

Perform the following steps to generate a new report.

1. Navigate to **Reports > Reports Type** tab.
2. Choose from the available Report Templates based on your reporting needs and click **Create**.
3. Provide the following information and click **Submit**.

Field	Description
Report Name	Enter a unique title for your report.
Data Scope	Select the time period for your report.
Report Format	Select PDF as the output format.
Schedule Recurring Delivery	Enable this toggle to automatically generate and send the report at set intervals.

4. If **Schedule Recurring Delivery** is enabled, provide the following additional information.

Field	Description
Report Users	Search for and select users by email address to receive the report.
Report Frequency	Choose how often the report should be generated and sent.
Time Zone	Set the time zone for the scheduled delivery.
Start and End Date	Select the active date range for the recurring schedule.

Once the report is ready, you can download it from the *Saved Reports* tab. See Saved Reports.

Report Templates

The following report templates are available.

- **Organization-Wide Reporting for Executives**- Provides high-level visual summaries of completion status and security performance for all phishing and training campaigns across the organization.
- **Individual Campaign Detail: Phishing and Training Performance**- Provides a granular analysis of a specific campaign, detailing engagement metrics, pass/fail rates, and completion trends for all assigned users.
- **Individual User Detail: Phishing and Training Performance**- Provides comprehensive profiles of individual users, tracking their historical performance across all simulations and assignments to identify personal risk levels.

Saved Reports

The *Saved Reports* tab provides a list of all reports you have created. You can track the generation status, manage schedules, and access your data from this tab.

The *Reports Usage* indicator shows how many reports you have saved out of your total limit. The **Saved Reports** tab displays the following information for each generated report:

Field	Description
Report Name	The unique title assigned to the report.
Created at / Updated At	The timestamps for when the report was first generated and most recently modified.
Schedule Status	Indicates if the report is set for recurring delivery.
Status	Displays the current state of the report file.
Next Run / Last Run	The scheduled time for the next delivery and the timestamp of the most recent delivery.
Frequency	The type of recurring schedule assigned to the report.

Use the options under the *Actions* column to manage your reports.

Action	Description
Edit	Modify the report name, data scope, or delivery schedule.
Download	Save the completed PDF report to your local device.
Delete	Permanently remove the report from the saved list to free up usage space.

The following statuses and notifications provide updates on the progress and availability of your reports.

Status / Notification	Description
Pending	Request received and queued for processing.
Queued	System is preparing to compile your report data.

Status / Notification	Description
Processing	Fetching campaign statistics and calculating metrics from the database.
Data Ready	Data has been compiled. We are now preparing the final report file.
Building File	The report file is being generated and formatted for delivery.
File Prepared	Report ready. You can download the file now or wait for email delivery.
Sending Email	The report is available for download while we dispatch it to your email.
Sent	Report successfully emailed. A copy remains available here for download.
Download Only	The report exceeds email attachment limits. Automatic delivery was aborted, but you can download it directly from this list.
Mail Delivery Failed	Email delivery failed, but you can still download your report directly from this list.
No Activity	No active or completed campaigns were found for this period.
Failed	Something went wrong. Please try again.
Access Denied	Your license has expired. Reports cannot be processed, though you may still download previously completed files.
HTML Format Only	The dataset is too large to be stabilized as a PDF. The report has been generated in HTML for better compatibility.

Subscriptions

The *Subscription* page displays your current FortiSAT 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.

Learner Experience

The *Learner Experience* portal is the primary interface for training campaign users to complete their security awareness training.

- Access and complete your assigned training modules and quizzes. See My Training.
- Manage your language preferences and security settings. See Settings

> New users will receive an onboarding email to set their initial password. If you miss the onboarding email, you can use the link in your training enrollment email, and click **Forgot Password** on the login page to reset your credentials.

My Training

The *My Training* page allows users to:

- Complete new training assignments through the *Incomplete* tab selector.
- Review completed training assignments and associated quizzes through the *Completed* tab selector.

To complete a training assignment

1. Select *My Training* from the navigation menu. A list of assignments appears in the right-hand pane.
2. Click on one of the assignments. The assignment appears in the right-hand pane.
3. Begin your training by clicking on any of the *Start now* links presented for each assignment. You do not have to take the training in any specific order. The training module will load in the right-hand pane.
4. Click the play icon to load the training module.
   - Users can hide the menu by clicking the three horizontal bars above the video to increase the size of the video and any text displayed in the window.
   - Users can move from topic to topic in the menu system.
   - Once all videos have been clicked and watched, the users can access the quiz (if applicable) or sign off on having watched the video. No module is complete until. Micro modules only require you sign off on having watched the video. For base modules, a quiz of 7 questions must be completed with a passing score of 80%. Modules are not considered complete until the 80% score is obtained by the user.
5. Once all videos have been clicked and watched, the *Proceed to quiz* button will appear after watching the *Lesson Summary* video of each module.

   The *Quiz Instructions* page is displayed.
6. Click the *Start Quiz* button to proceed to the quiz. The quiz is displayed.
7. Select the correct answer for each question. Once you have answered all of the questions, your score will be presented.
8. You may select the *Review Quiz* button to check which answers you got correct or incorrect.

9. You can return to the module by selecting the module name from the path above the video window (in this example, *Cicked a phishing link*. If you scored 80% or higher on the quiz, the module is marked as complete.
10. Once all modules have been completed and any associated quizzes have been completed with an 80% or higher, the campaign will be marked as complete and appear on the *My Training* > *Completed* tab.

Reviewing completed training modules

After completing a training assignment, you may wish to review the material or your quiz answers and score.

To review your completed campaigns and quizzes:

1. Select *My Training* from the navigation menu, then select the *Completed* tab to display the campaigns you have completed:
2. Click the desired completed assignment to display the campaign details. The campaign page is displayed:
3. Click the *Start again* link for the module you wish to review. The module is relaunched.

Accessing your certificate of completion

Administrators can configure campaigns to email you a link to download a certificate of completion after you have completed the assigned material and obtained an 80% on any associated quizzes. Users can also access certificates of completion from the *Learner Experience* interface.

To access your certificate of completion for a completed course:

1. Select *My Training* from the navigation menu, then select the *Completed* tab to display the campaigns you have completed:
2. Click the desired completed assignment to display the campaign details. The campaign page is displayed.
3. Click the *Download certificate here* link near the top of the page. It will take some time for the certificate to be generated and downloaded. Once downloaded you will be notified by your browser.

Settings

The *Settings* page allows the user to manage the following security and language settings.

Two-Factor Authentication (2FA)

Two-factor authentication adds an extra layer of security to your account. When enabled, you must provide something you know (your password) and something you have (a code from an authenticator app on your phone) to log in. This ensures that only you can access your account, even if someone else knows your password.

To configure 2FA:

1. Navigate to **Settings**.
2. In the Two-Factor Authentication (2FA) section, enable the **Enable 2FA** toggle.
3. Use an authenticator app on your mobile device to scan the displayed QR code.
4. Enter the 6-digit code provided by the app and click **Verify** and enable.

> If your administrator has enforced 2FA globally, the toggle will be locked, and you will not be able to disable this setting.

Language Settings

Use the **Select Language** dropdown menu to change your interface language. This updates the portal text and training module content (where available) to your preferred language.

Third-Party Cookies

Enable the **Allow Third-Party Cookies** toggle to optimize your learning experience. Enabling this setting improves video playback performance and ensures training modules load quickly. By default, this is enabled and allows users to modify the setting within their own portal view. If disabled by an administrator, users cannot enable it from their individual accounts.

> A greyed-out user toggle reflects the last state configured before the admin disabled the option. If the toggle remains in the enabled position while greyed out, third-party cookies are not applied or enforced, as the configuration is inactive due to admin restrictions.

Frequently Asked Questions (FAQs)

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

You have two options:

1. Purchase additional FortiSAT 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 users is not verified.
- A user 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 user 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 FortiSAT, even though the intended user hasn't viewed the email. To resolve this, safelist FortiSAT traffic within your email scanners.

Why are FortiSAT 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 FortiSAT in Office 365. Ensure you add the sender email domain configured in your FortiSAT 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 FortiSAT Phish Alert Button in Outlook.

The FortiSAT Phish 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 PAB in Exchange Online / Microsoft 365.

www.fortinet.com