Administration Guide

Security Awareness and Training Service 24.4

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

August 28, 2025
Security Awareness and Training Service 24.4 Administration Guide
76-244-1104332-20250828

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-12-10	Initial release.
2025-08-28	Added Training module reference guide on page 13.

Overview

The Fortinet Security Awareness and Training Service is a SaaS subscription offering. It provides customers with the ability to deploy and maintain a cybersecurity awareness training program within their company. Using the Service, customers can educate and train employees on current cyber threat, such as phishing, social engineering, and ransomware attacks, and provides tips on how to protect themselves and their organization.

The Service also provides the customer with the ability to manage and track employee training progress through a central dashboard. Using the dashboard, they can monitor the training progress of their employees, as each employee progresses through the Security Awareness modules. The customer can view a full list of their employees or focus on specific individuals.

The Fortinet Training Department uses the National Institute of Standards and Technology (NIST): Building an Information Technology Security Awareness and Training Program resource as a benchmark for development and compliance.

Optionally, the Fortinet Security Awareness and Training Service can be integrated with the FortiPhish service. This allows customers to assign training to users based on events that occur in the FortiPhish service. For more information about the FortiPhish service, visit: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiphish.pdf.

For customers who wish to use their own, existing Learning Management System (LMS), the base modules with quizzes and the micro modules can be provided through SCORM files, accessed from a content management server. If you require the content through SCORM files, see Technical support on page 8.

Supported browsers

To make sure the customers’ have the best experience possible, we recommend using the most up-to-date version of one of the following officially supported browsers:

- Google Chrome
- Mozilla Firefox
- Safari
- Microsoft Edge

Supported languages

The Fortinet Security Awareness and Training Service interface supports the languages listed below.

Not all content is supported in all languages supported by the interface. If there is an additional language you would like support for in the interface or for any of the content, please open a feature request by sending an email to: infosec_awareness@fortinet.com

Users can change their preferred language after they log in. When a user changes their preferred language, it is reflected in:

- The Learner’s App
- Reports (Executive Report Current Year (Canned) and the canned report included in the Campaign Setup Wizard Reports Setup section)

The Fortinet Security Awareness and Training Service currently supports the following Languages:

Admin Role

The admin role is currently available in:

- English
- German
- Español (MX)
- French
- Japanese
- Italian
- Portugués (Brasil)
- Portugués

Learner Experience

The learner experience is currently available in:

- Deutsch (German)
- English (Australia)
- English (UK)
- English US
- Español (MX)
- Francais (French (France))
- Italiano
- Portugués (Brasil)
- Portugués
- Japanese

Administrators can set the default language for users when configuring the system.

Learners and sub-admins can change the default language to the language of their choice after logging in to the learner experience.

Technical support

For FortiPhish technical support, you can open a ticket by following these instructions: How to open a helpdesk ticket for the FortiPhish service.

For any of the following Security Awareness and Training requests, including:

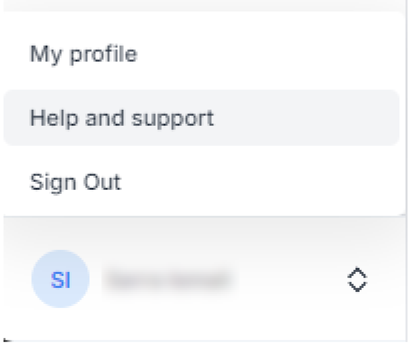
- Updating of licenses (increase / decrease of licensed users)
- Moving from Customer to Partner or Partner to Customer status
- Assistance configuring the Admin Portal tenant
- Upload of users
- Issues
- Feature Requests
- Other questions or queries

There are two ways Administrators can open technical support tickets for the Fortinet Security and Awareness Training Service. Tickets can be opened through the support link in the service, or by submitting through email.

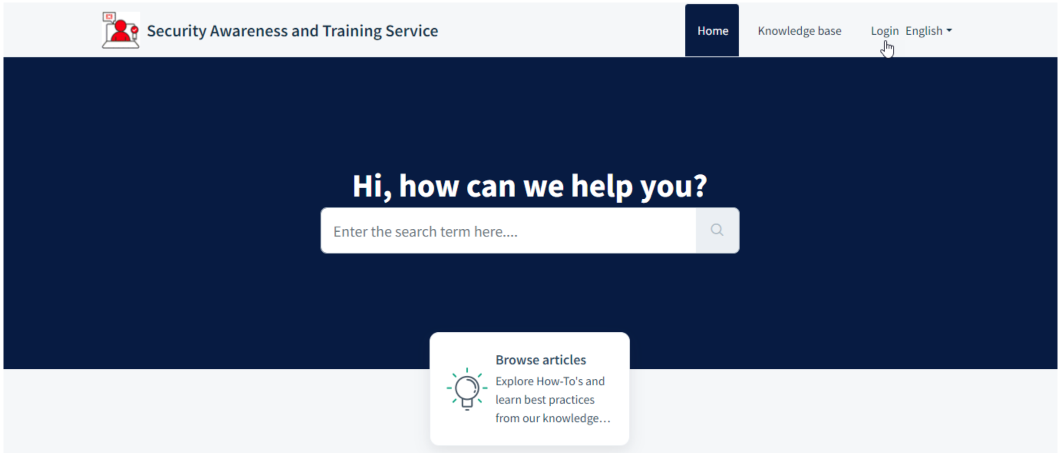
Only Tenant Administrators or people logged in with the Tenant Administrator (FortiCloud account) or people who have been assigned the administrative role can open cases using this method. Learners should report any issues or raise any questions or feature requests to their local Administrator.

To open a ticket from the support link in the service:

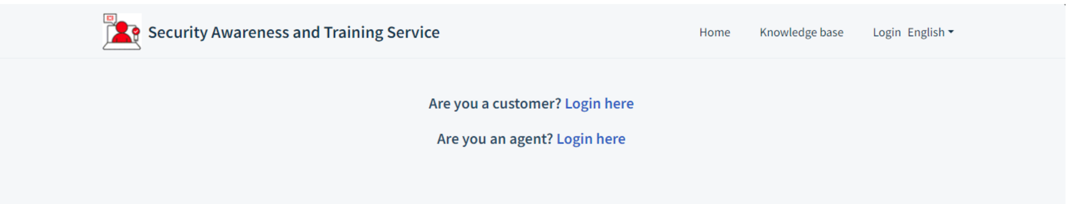
1. From your user name in the lower left-hand corner of the screen, select the *Help and support* menu item to be directed to the Security Awareness and Training Service support site.



2. Once the support site has been loaded, select *Login*.


Security Awareness and Training Service
Home
Knowledge base
Login English
Hi, how can we help you?
Enter the search term here....
Browse articles
Explore How-To's and learn best practices from our knowledge…

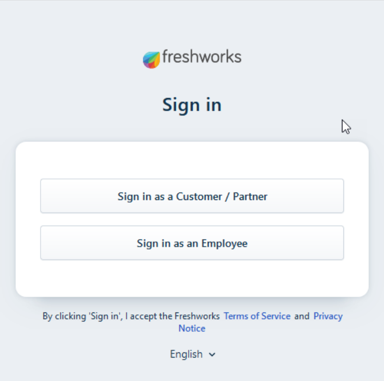
3. Select *Are you a customer? Login here*.



Are you a customer? Login here

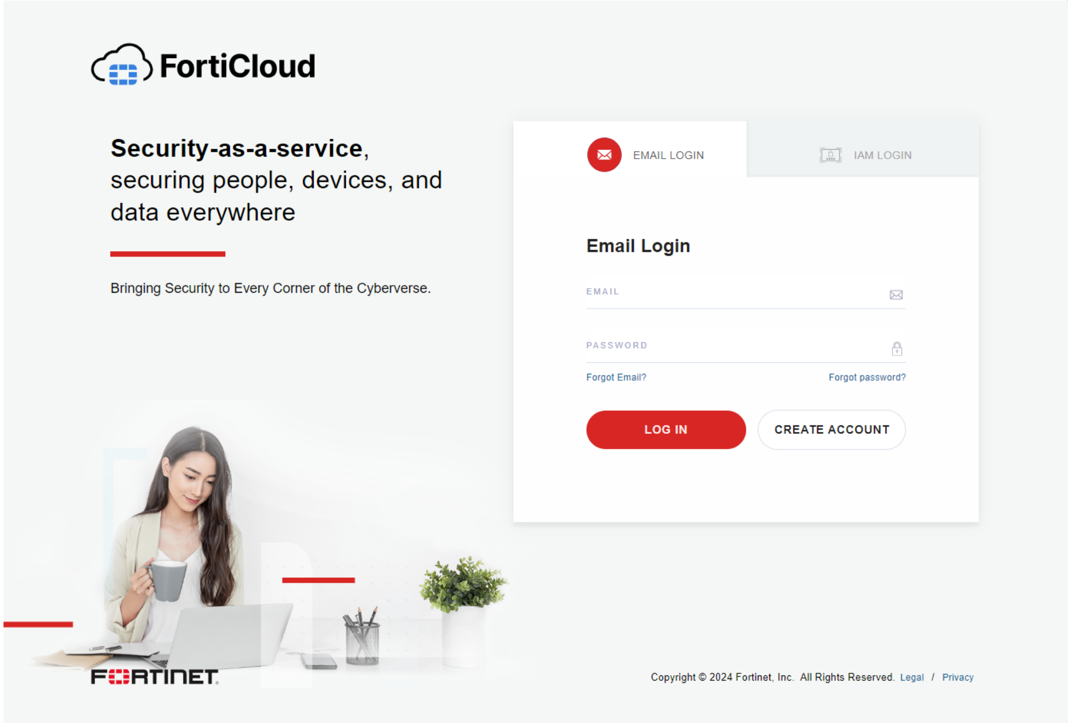
Are you an agent? Login here

4. Select *Sign in as a Customer / Partner*.



By clicking 'Sign in', I accept the Freshworks Terms of Service and Privacy Notice

5. If prompted, log in as your Tenant Administrator - FortiCloud Support credentials.



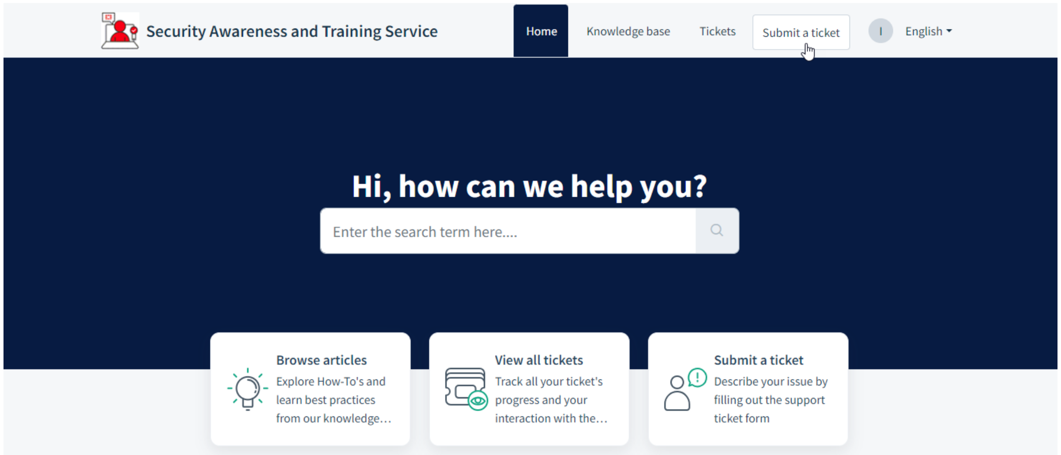
Security-as-a-service, securing people, devices, and data everywhere

Bringing Security to Every Corner of the Cyberverse.

Email Login

Copyright © 2024 Fortinet, Inc. All Rights Reserved.

6. Select *Submit a ticket*.



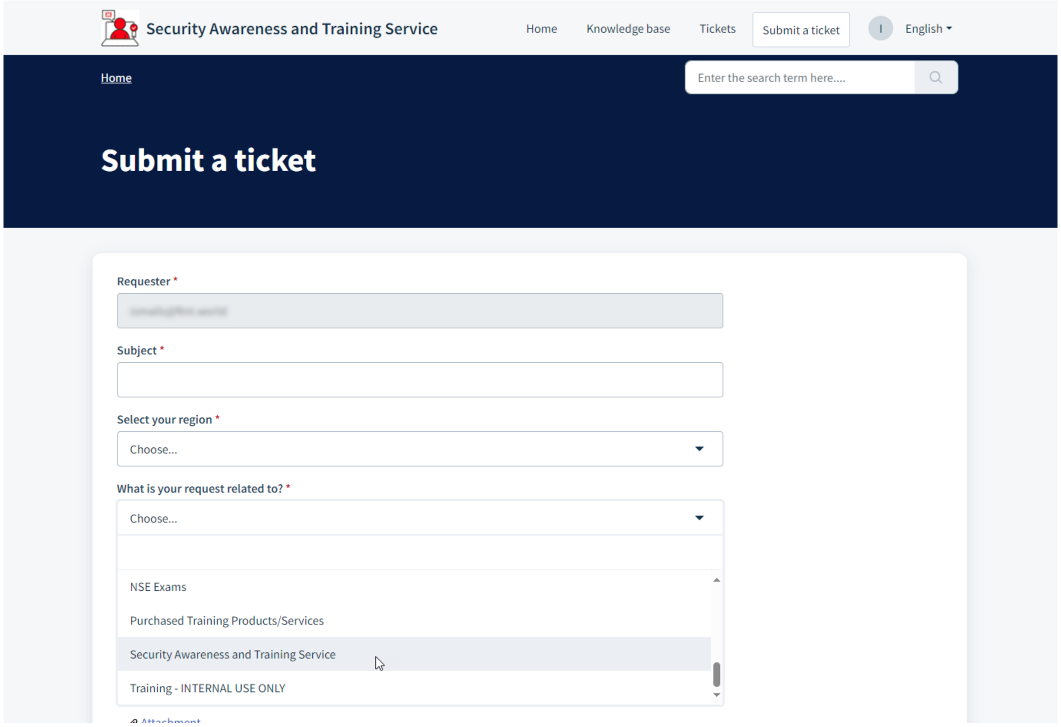
Hi, how can we help you?

Explore How-To's and learn best practices from our knowledge…

Track all your ticket's progress and your interaction with the…

Describe your issue by filling out the support ticket form

7. Complete the fields in the form:
   - *Subject*: A brief description of the question or issue being faced.
   - *Select your region*: The region of the Administrator opening the ticket.
   - *What is your request related to?*: Select *Security Awareness and Training Service*. This ensures your ticket is routed directly to the correct support team.
   - *Description*: Provide a detailed description of the question or issue, including steps to reproduce, screen shots, browser build, and so on.
   - *+ Attach a file* – Include any files you wish to submit with the ticket.


Security Awareness and Training Service
Home
Knowledge base
Tickets
Submit a ticket
English
Enter the search term here....
Home

Submit a ticket

Requester *
[redacted]

Subject *

Select your region *
Choose...

What is your request related to? *
Choose...

NSE Exams
Purchased Training Products/Services
Security Awareness and Training Service
Training - INTERNAL USE ONLY

8. Click *Submit*

   You will receive an automated response that your ticket has been opened. Keep all correspondence for this issue or question in response to this notification email so that it gets added to your ticket.

To create a ticket through email submission

1. Open a support case by sending an email to infosec_awareness@fortinet.com.

> Only Administrators of the service should open cases with support. Learners should report any issues or raise any questions or feature requests to their local Administrators.

Once a case has been opened you will receive a confirmation email of the submission and a Deployment Specialist will follow up on the newly created ticket thread.

Support Ticket Best Practices

The following is a list of best practices:

- Raise one question, issue, feature request per ticket.
- Do not raise new queries on existing or older (closed/resolved) tickets.
- When opening a support ticket through email, insure to include:
  - A high-level description in the subject
  - Details of the request in the body of the message
  - Section (Learning Application, Reporting, Campaigns, Configuration, and so on) if applicable

- Usernames and emails (if applicable)
- Any error messages encountered.
- Screen shots
- Steps to reproduce the issue.
- Operating System and version (if applicable)
- Browser and version (if applicable)

User types

Each customer or partner has a tenant. The tenant is the unique instance of the Admin Portal. The Tenant Administrator / Super Admin is the first account created in the system. It is tied to the FortiCloud account used to initialize the service. The Super Admin also inputs the licenses for Fortinet products and services from the FortiCloud portal.

The Tenant Administrator user is the super admin of the Security Awareness and Training Service and is responsible for setting up the customer account (users, authentication method, branding) as well as training campaigns, reporting and remediation. They can also assign the admin role to other users of the system. These additional administrators have full access to perform the same functions as the Super User account, except they cannot access the FortiCloud portal.

User Admin role

These additional Administrators have full access to perform the same functions as the Super User account, except they cannot access the FortiCloud portal.

If the sub administrators require access to the Assets and FortiPhish configuration, they can create a FortiCloud account and the Tenant Administrator FortiCloud account owner can add them as a sub account with administrative permissions in order to access these additional features.

Partner Permissions

Partner permissions set is not currently available in version 3 of this service.

Standard Users (Learners)

This user (usually employees) is the intended audience for the Security Awareness and Training Service. The learners receive the training campaigns set up by the administrator. Learners can authenticate by entering their login credentials from the URL provided by their tenant Admin or through the Training enrollment confirmation email.

Training module reference guide

The following reference guide lists the training modules that are available for Security Awareness and Training Service for the following editions:

- Enterprise Training Modules on page 13
- Education Training Modules on page 15

Enterprise Training Modules

The following are modules included in the Enterprise Edition of Fortinet's Security Awareness and Training Service platform:

Enterprise Edition Modules

The following Enterprise edition modules are available:

- Access Control
- AI-Powered Threats
- Bad Actors
- BEC
- Clean Desk
- Cloud Risks
- Data Privacy
- Data Security
- Email Security
- Generative AI
- Insider Threat
- Intellectual Property
- Introduction to Information Security
- Malware
- MFA
- Mobile Security
- Password Protection
- Phishing
- Secure Travel Tips
- Social Engineering
- Social Media
- Web Conference Security
- Working Remotely
- Manager Awareness
- Manager Frameworks

- Manager Deployment

Micro Learning Modules

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

Fortinet Security Awareness and Training Service includes 12 micro learning modules available in both Standard and Premium service tiers:

Topic	Description/Reinforces Base Module
Social Engineering	Reinforces tactics used in social attacks
Phishing Attacks	Quick guide to spotting phishing emails
Email Security	Reinforces email-based threat awareness
Malware and Ransomware	Covers malware/Ransomware behavioral risks
Password Protection	Tips for creating strong passwords
Data Security	Highlights secure handling of sensitive data
Data Privacy	Reinforces privacy-related handling protocols
Business Email Compromise (BEC)	Short version on BEC attack prevention
Insider Threat	Brief on recognizing internal threats
Clean Desk Policy	Desk security best practices
Access Control	Authentication and authorization basics
Bad Actors	Summary of threat actors and motivations

Nano Learning Modules

Nano learning modules are lessons under 1 minute each. They are designed for reinforcement and awareness assets.

There are 20 nano learning videos, each reinforcing one security topic:

- Shoulder Surfing
- Tailgating
- See Something, Hear Something...
- Follow Company Policy
- Avoid Unknown Wi Fi Networks
- Good Password Hygiene
- Think Before You Click
- Web Conference Tips
- Travel Tips

- Backup Your Data
- Data Disposal
- Disable Automatic Wi Fi
- Encrypt Sensitive Data
- Enable Screen Locks
- Update Your Software
- Protect Your Devices
- Non-discoverable Bluetooth
- Use Multi-factor Authentication

Education Training Modules

The following are modules included in the Education Edition of Fortinet’s Security Awareness and Training Service platform.

Education Edition Modules

The following Education edition modules are available:

- Access Control
- AI-Powered Threats
- Bad Actors
- BEC
- Clean Desk
- Cyberbullying
- Cyberbullying Strategies
- Data Privacy
- Data Security
- Educational Technologies
- Email Security
- Generative AI
- Insider Threat
- Intellectual Property
- Introduction to Information Security
- Malware
- MFA
- Mobile Security
- Online Learning
- Online Scams and Identity Theft
- Password Protection
- Phishing
- Safer Online Gaming

- Secure Travel Tips
- Social Engineering
- Social Media
- Web Conference Security
- Working Remotely

K-12 Curriculum Modules

K-12 curriculum modules are designed for specific age groups.

The following curriculum modules are available:

- Level 03 (Ages 12-14)
  - Securing Data and Keeping it Private
  - Cyberbullying
  - Understanding Cybersecurity
  - Computing and Culture
  - Respecting Intellectual Property
  - Social Media Influence
  - Identity in the Digital World
- Level 02 (Ages 8-11)
  - Respecting Work Online
  - Making Sense of Social Media
  - Online Identity
  - History of Computing Innovations
  - Introducing Cybersecurity
  - Building Password Essentials
  - Recognizing Cybersecurity

Micro Learning Modules

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

Fortinet Security Awareness and Training Service includes 12 micro learning modules available in both Standard and Premium service tiers:

Topic	Description/Reinforces Base Module
Social Engineering	Reinforces tactics used in social attacks
Phishing Attacks	Quick guide to spotting phishing emails
Email Security	Reinforces email-based threat awareness
Malware and Ransomware	Covers malware/Ransomware behavioral risks

Topic	Description/Reinforces Base Module
Password Protection	Tips for creating strong passwords
Data Security	Highlights secure handling of sensitive data
Data Privacy	Reinforces privacy-related handling protocols
Business Email Compromise (BEC)	Short version on BEC attack prevention
Insider Threat	Brief on recognizing internal threats
Clean Desk Policy	Desk security best practices
Access Control	Authentication and authorization basics
Bad Actors	Summary of threat actors and motivations

Nano Learning Modules

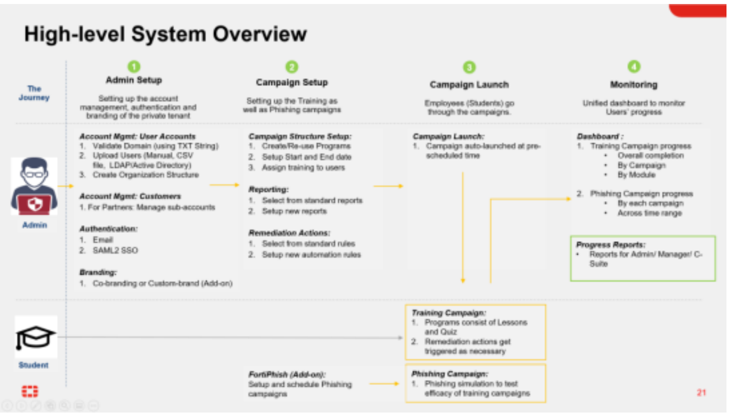
Nano learning modules are lessons under 1 minute each. They are designed for reinforcement and awareness assets. Nano modules are available to both Standard and Premium subscriber.

There are 20 nano learning videos, each reinforcing one security topic:

- Shoulder Surfing
- Tailgating
- See Something, Hear Something...
- Follow Company Policy
- Avoid Unknown Wi Fi Networks
- Good Password Hygiene
- Think Before You Click
- Web Conference Tips
- Travel Tips
- Backup Your Data
- Data Disposal
- Disable Automatic Wi Fi
- Encrypt Sensitive Data
- Enable Screen Locks
- Update Your Software
- Protect Your Devices
- Non-discoverable Bluetooth
- Use Multi-factor Authentication
- Good Mobile Habits (Education only)
- (Plus educational variants of above)

System overview

The following image present a high-level overview of all the key features organized in a logical sequence that represents the interaction points of Admin and Learner with the Security Awareness and Training Service:



High-level System Overview

1 **Admin Setup**

Setting up the account management, authentication and branding of the private tenant

2 **Campaign Setup**

Setting up the Training as well as Phishing campaigns

3 **Campaign Launch**

Employees (Students) go through the campaigns.

4 **Monitoring**

Unified dashboard to monitor Users' progress

Account Mgmt: User Accounts

1. Validate Domain (using TXT String)
2. Upload Users (Manual, CSV file, LDAP/Active Directory)
3. Create Organization Structure

Account Mgmt: Customers

1. For Partners: Manage sub-accounts

Authentication:

1. Email
2. SAML2 SSO

Branding:

1. Co-branding or Custom-brand (Add-on)

Campaign Structure Setup:

1. Create/Re-use Programs
2. Setup Start and End date
3. Assign training to users

Reporting:

1. Select from standard reports
2. Setup new reports

Remediation Actions:

1. Select from standard rules
2. Setup new automation rules

Campaign Launch:

1. Campaign auto-launched at pre-scheduled time

Dashboard :

1. Training Campaign progress
   - Overall completion
   - By Campaign
   - By Module
2. Phishing Campaign progress
   - By each campaign
   - Across time range

Progress Reports:

- Reports for Admin/ Manager/ C-Suite

Training Campaign:

1. Programs consist of Lessons and Quiz
2. Remediation actions get triggered as necessary

FortiPhish (Add-on):
Setup and schedule Phishing campaigns

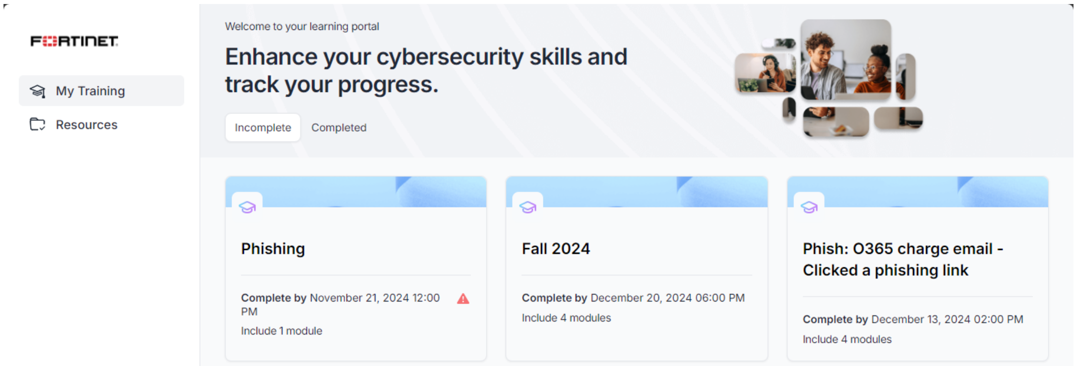
Phishing Campaign:

1. Phishing simulation to test efficacy of training campaigns

Learner Experience

The learner experience is the interface learners use to:

- Complete new training assignments through the *Incomplete* tab selector.
- Review completed training assignments and associated quizzes through the *Completed* tab selector.
- Download the certificate of completion for each completed campaign assignment.
- Access the assets in the *My assets* navigation menu item. The administrator must allow access to these assets. If you do not see a *My assets* navigation menu item, then you have not been granted access.
- Change learner interface and training module or quiz language.
- Change their time zone.
- Configure two-factor Authentication (2FA) settings: This option is only available if the administrator has not configured the system to use an existing 2FA solution for their users.
- Reset or change their password: This option is only available for customers who do not configure their own SAML2 (SSO) authentication solution. When a third party SSO solution is configured, learners will change their password through that solution (such as Google Workspace, RapidID, Azure/Entra, ADFS on premises domain validation, and so on).



Welcome to your learning portal

Enhance your cybersecurity skills and track your progress.

Phishing

Complete by November 21, 2024 12:00 PM

Include 1 module

Fall 2024

Complete by December 20, 2024 06:00 PM

Include 4 modules

Phish: O365 charge email - Clicked a phishing link

Complete by December 13, 2024 02:00 PM

Include 4 modules

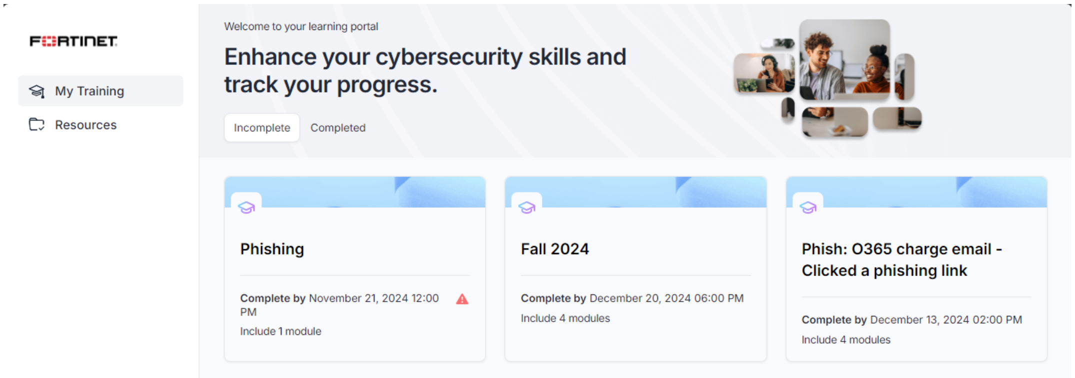
My Training

The *My Training* navigation menu item allows learners 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.



FORTINET

My Training

Resources

Welcome to your learning portal

Enhance your cybersecurity skills and track your progress.

Incomplete Completed

Phishing

Complete by November 21, 2024 12:00 PM

Include 1 module

Fall 2024

Complete by December 20, 2024 06:00 PM

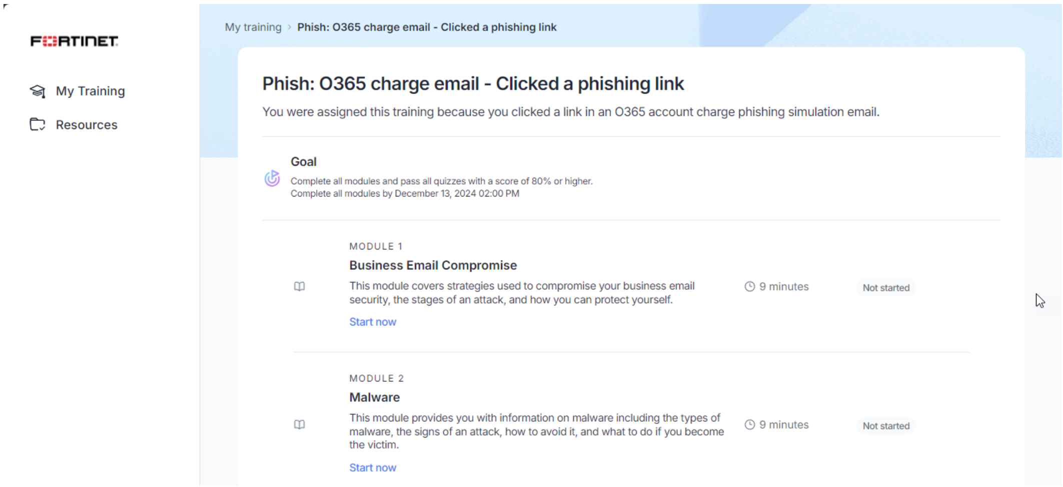
Include 4 modules

Phish: O365 charge email - Clicked a phishing link

Complete by December 13, 2024 02:00 PM

Include 4 modules

2. Click on one of the assignments. The assignment appears in the right-hand pane.



FORTINET

My Training

Resources

My training › Phish: O365 charge email - Clicked a phishing link

Phish: O365 charge email - Clicked a phishing link

You were assigned this training because you clicked a link in an O365 account charge phishing simulation email.

Goal

Complete all modules and pass all quizzes with a score of 80% or higher.
Complete all modules by December 13, 2024 02:00 PM

MODULE 1

Business Email Compromise

This module covers strategies used to compromise your business email security, the stages of an attack, and how you can protect yourself.

9 minutes Not started

Start now

MODULE 2

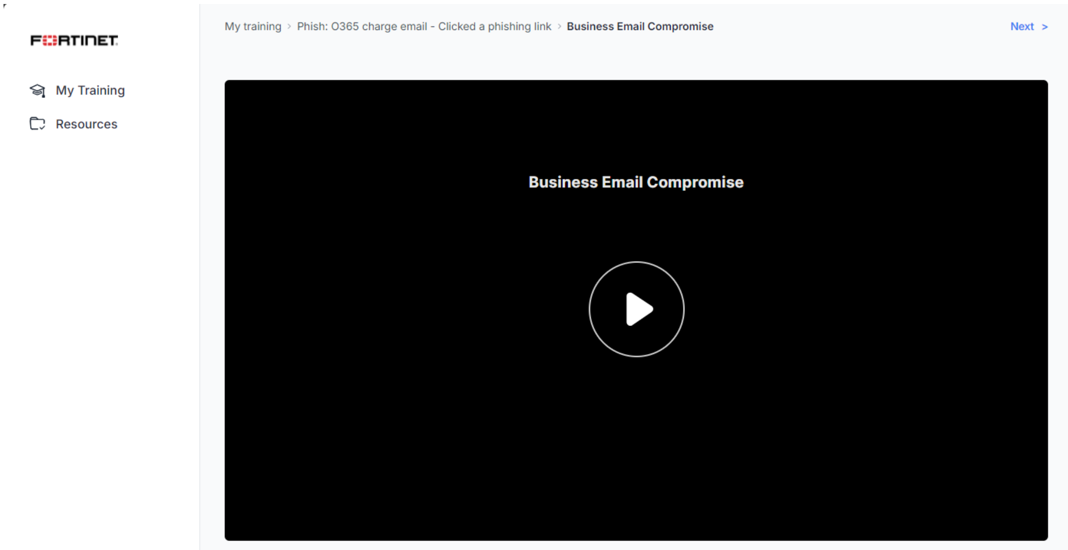
Malware

This module provides you with information on malware including the types of malware, the signs of an attack, how to avoid it, and what to do if you become the victim.

9 minutes Not started

Start now

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.



FORTINET

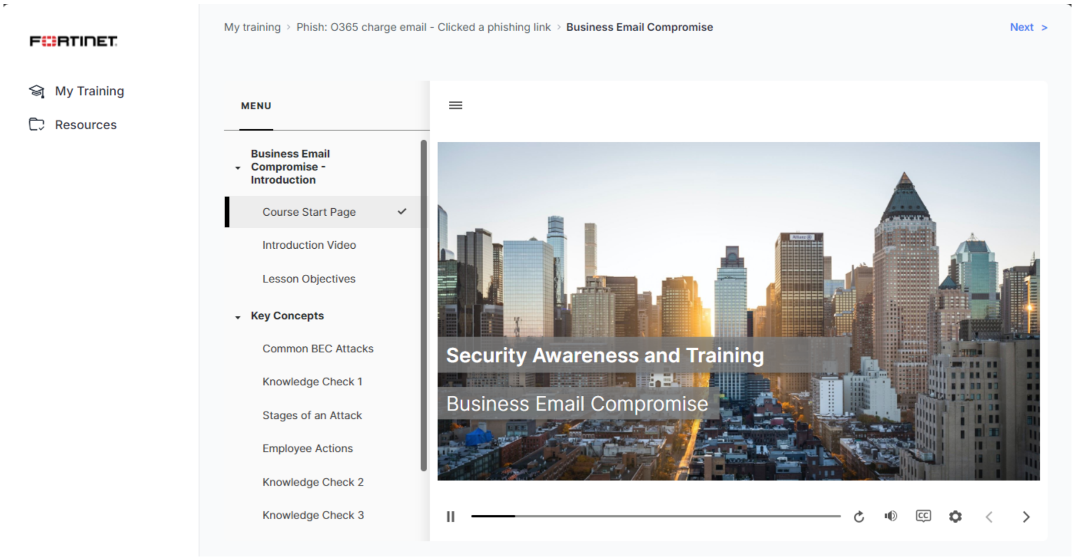
My Training

Resources

My training › Phish: O365 charge email - Clicked a phishing link › Business Email Compromise Next >

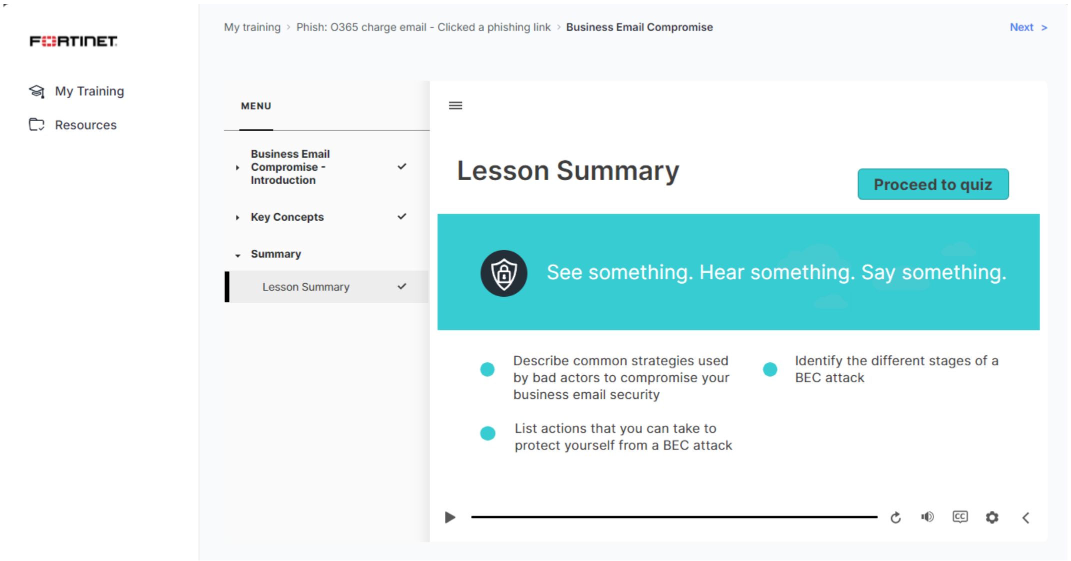
Business Email Compromise

4. Click the play icon to load the training module.

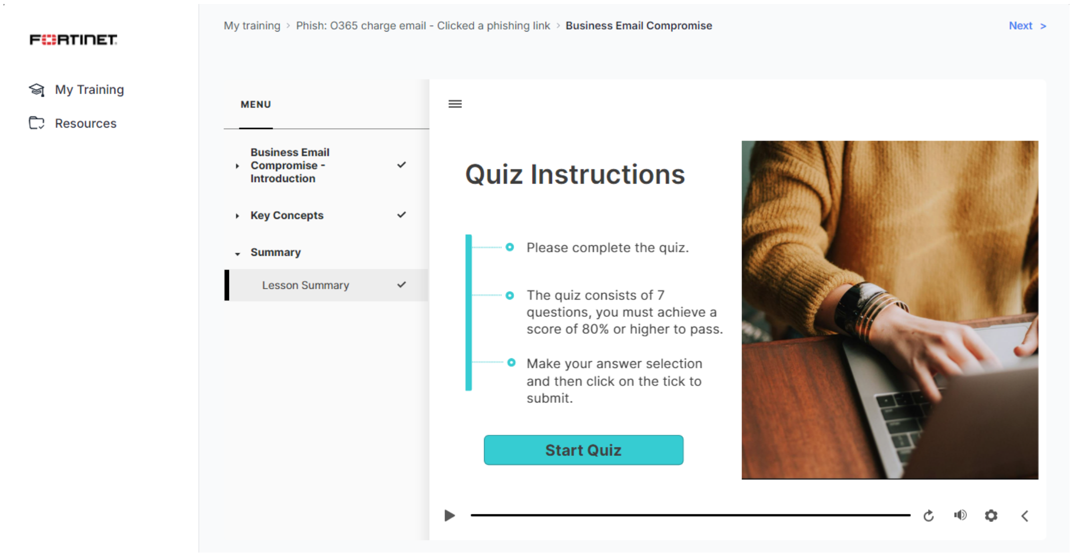


- Learners can hide the menu by clicking the three horizontal bars above the video to increase the size of the video and any text displayed in the window.
- Learners can move from topic to topic in the menu system.
- Once all videos have been clicked and watched, the learners can access the quiz (if 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 learner.

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.


FORTINET
My Training
Resources
My training › Phish: O365 charge email - Clicked a phishing link › Business Email Compromise
Next >
MENU
Business Email Compromise - Introduction ✓
Key Concepts ✓
Summary
Lesson Summary ✓
Lesson Summary
Proceed to quiz
See something. Hear something. Say something.
Describe common strategies used by bad actors to compromise your business email security
Identify the different stages of a BEC attack
List actions that you can take to protect yourself from a BEC attack

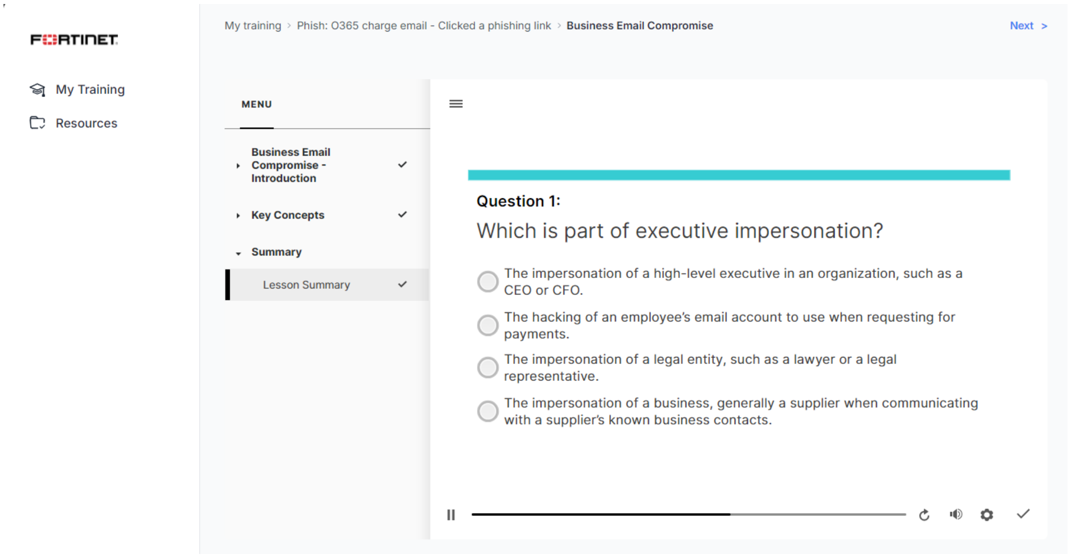
The *Quiz Instructions* page is displayed.


FORTINET
My Training
Resources
My training › Phish: O365 charge email - Clicked a phishing link › Business Email Compromise
Next >
MENU
Business Email Compromise - Introduction ✓
Key Concepts ✓
Summary
Lesson Summary ✓

Quiz Instructions

- Please complete the quiz.
- The quiz consists of 7 questions, you must achieve a score of 80% or higher to pass.
- Make your answer selection and then click on the tick to submit.

6. Click the *Start Quiz* button to proceed to the quiz. The quiz is displayed.


FORTINET
My Training
Resources
My training › Phish: O365 charge email - Clicked a phishing link › Business Email Compromise
Next >
MENU
Business Email Compromise - Introduction ✓
Key Concepts ✓
Summary
Lesson Summary ✓

Question 1:

Which is part of executive impersonation?

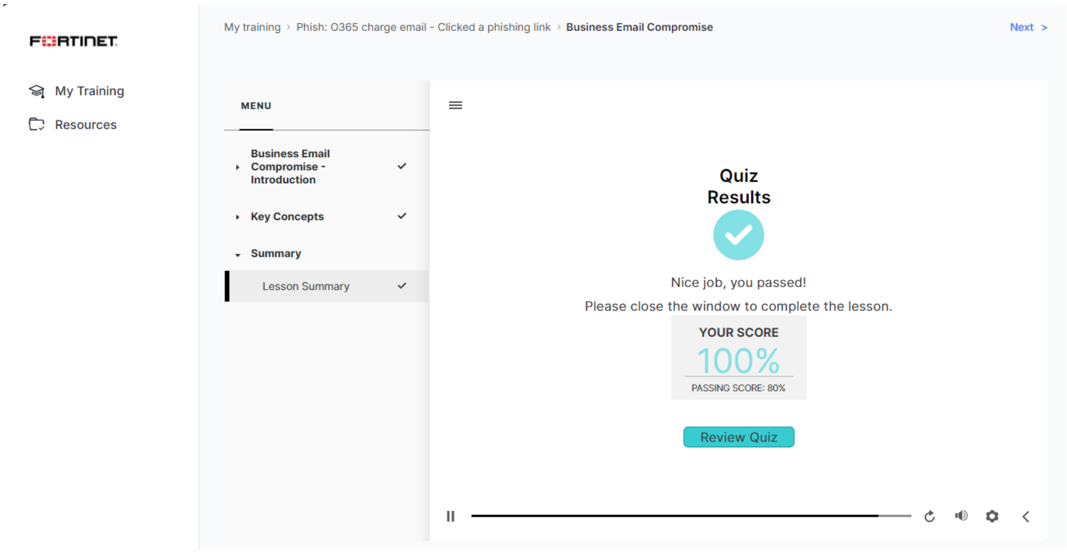
○ The impersonation of a high-level executive in an organization, such as a CEO or CFO.

○ The hacking of an employee's email account to use when requesting for payments.

○ The impersonation of a legal entity, such as a lawyer or a legal representative.

○ The impersonation of a business, generally a supplier when communicating with a supplier's known business contacts.

7. Select the correct answer for each question. Once you have answered all of the questions, your score will be presented.


FORTINET
My Training
Resources
My training › Phish: O365 charge email - Clicked a phishing link › Business Email Compromise
Next >
MENU
Business Email Compromise - Introduction ✓
Key Concepts ✓
Summary
Lesson Summary ✓
Review Quiz

Quiz Results

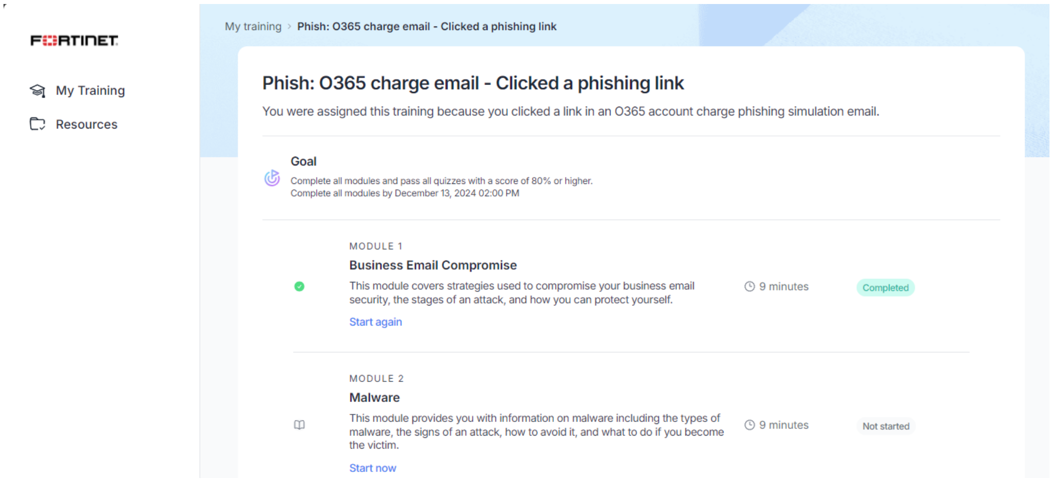
Nice job, you passed!

Please close the window to complete the lesson.

YOUR SCORE 100%

PASSING SCORE: 80%

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.


FORTINET
My Training
Resources
My training › Phish: O365 charge email - Clicked a phishing link

Phish: O365 charge email - Clicked a phishing link

You were assigned this training because you clicked a link in an O365 account charge phishing simulation email.

Goal

Complete all modules and pass all quizzes with a score of 80% or higher.
Complete all modules by December 13, 2024 02:00 PM

MODULE 1

Business Email Compromise

This module covers strategies used to compromise your business email security, the stages of an attack, and how you can protect yourself.

9 minutes — Completed — Start again

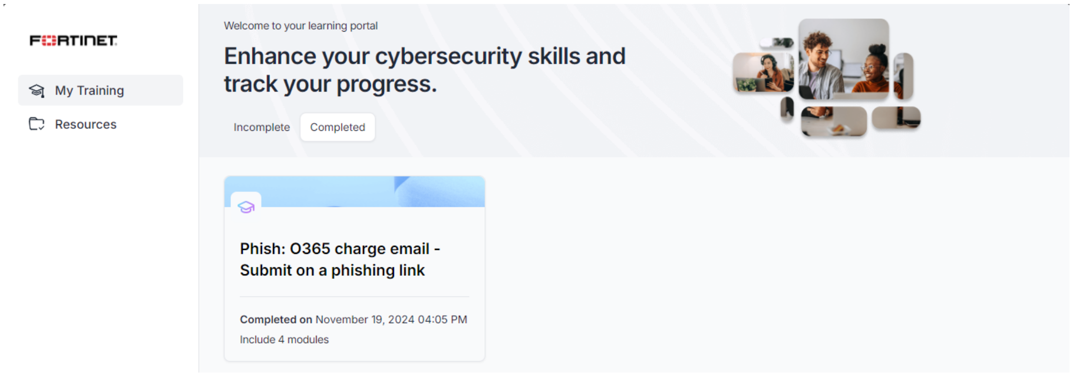
MODULE 2

Malware

This module provides you with information on malware including the types of malware, the signs of an attack, how to avoid it, and what to do if you become the victim.

9 minutes — Not started — Start now

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.



Welcome to your learning portal

Enhance your cybersecurity skills and track your progress.

Phish: O365 charge email - Submit on a phishing link

Completed on November 19, 2024 04:05 PM

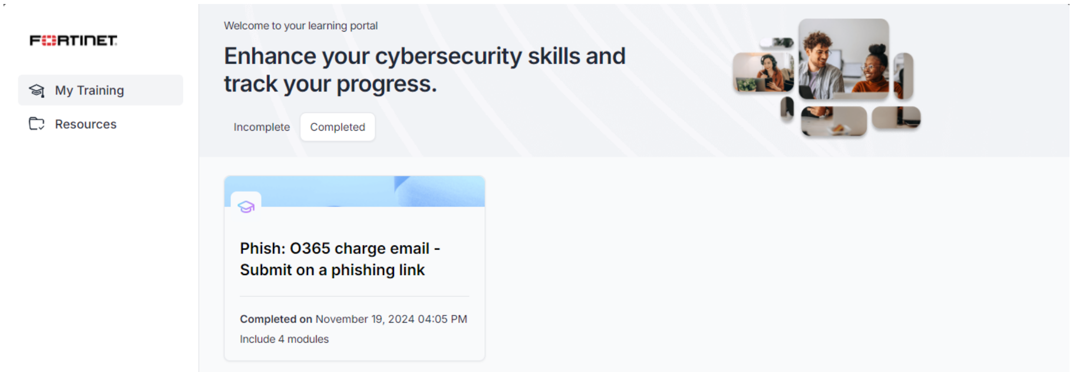
Include 4 modules

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:



FORTINET

My Training

Resources

Welcome to your learning portal

Enhance your cybersecurity skills and track your progress.

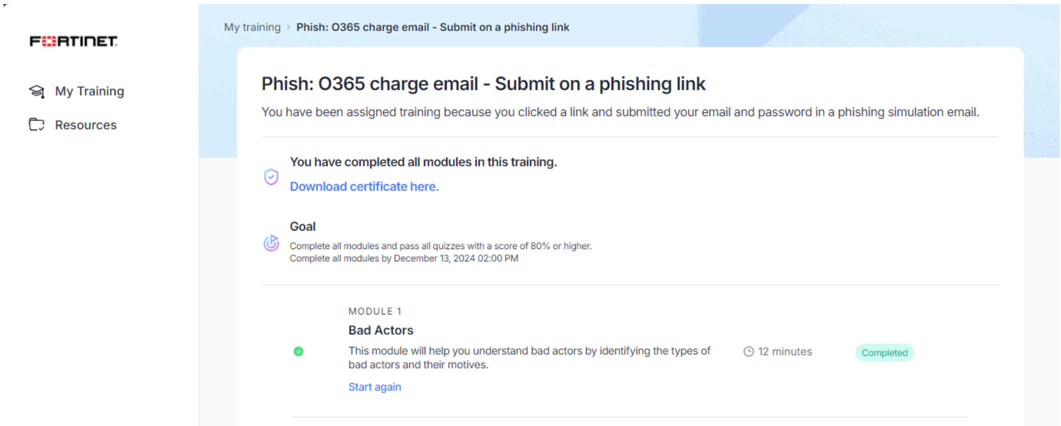
Incomplete Completed

Phish: O365 charge email - Submit on a phishing link

Completed on November 19, 2024 04:05 PM

Include 4 modules

2. Click the desired completed assignment to display the campaign details. The campaign page is displayed:



FORTINET

My Training

Resources

My training › Phish: O365 charge email - Submit on a phishing link

Phish: O365 charge email - Submit on a phishing link

You have been assigned training because you clicked a link and submitted your email and password in a phishing simulation email.

You have completed all modules in this training.

Download certificate here.

Goal

Complete all modules and pass all quizzes with a score of 80% or higher.

Complete all modules by December 13, 2024 02:00 PM

MODULE 1

Bad Actors

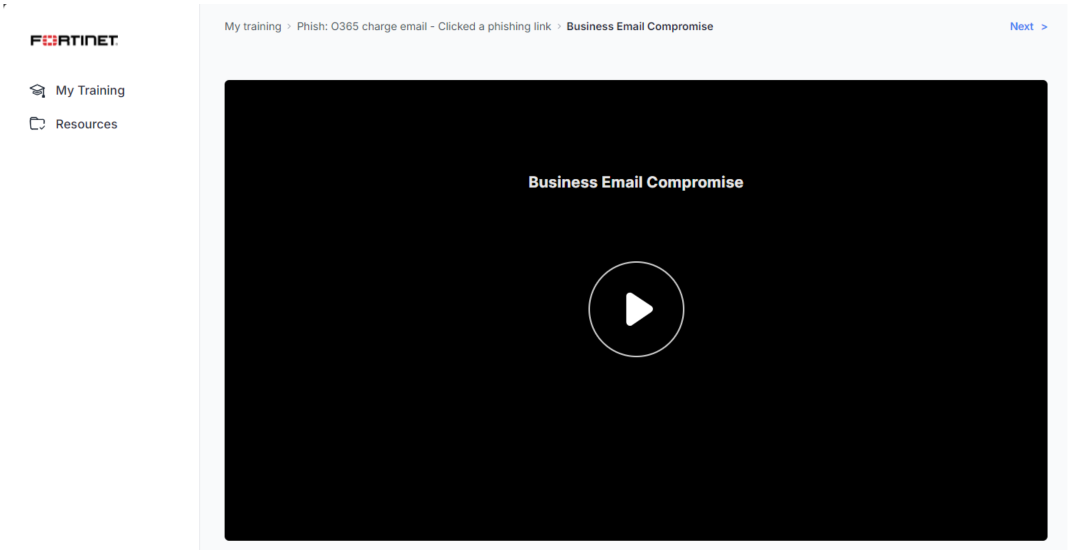
This module will help you understand bad actors by identifying the types of bad actors and their motives.

12 minutes

Completed

Start again

3. Click the *Start again* link for the module you wish to review. The module is relaunched.

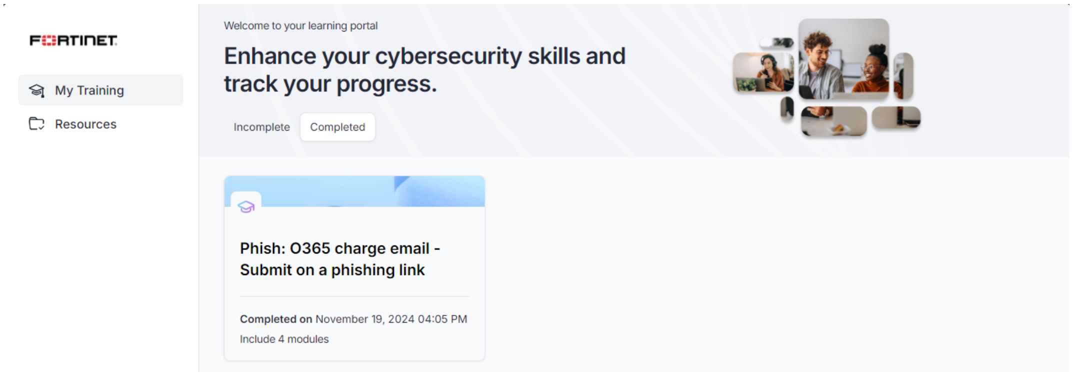

FORTINET
My Training
Resources
My training › Phish: O365 charge email - Clicked a phishing link › Business Email Compromise
Next >
Business Email Compromise

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. Learners 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:

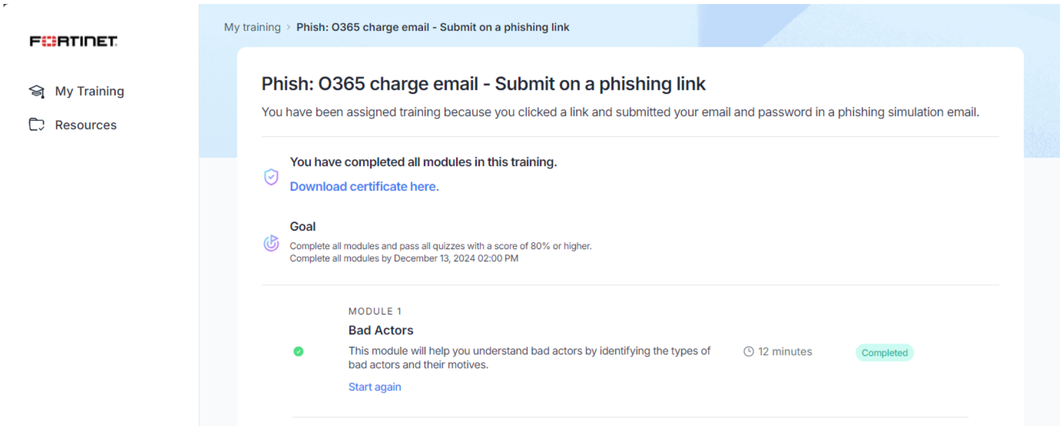

FORTINET
My Training
Resources
Welcome to your learning portal
Enhance your cybersecurity skills and track your progress.
Incomplete
Completed

Phish: O365 charge email - Submit on a phishing link

Completed on November 19, 2024 04:05 PM

Include 4 modules

2. Click the desired completed assignment to display the campaign details. The campaign page is displayed.


FURTINET
My Training
Resources
My training › Phish: O365 charge email - Submit on a phishing link

Phish: O365 charge email - Submit on a phishing link

You have been assigned training because you clicked a link and submitted your email and password in a phishing simulation email.

You have completed all modules in this training.

Download certificate here.

Goal

Complete all modules and pass all quizzes with a score of 80% or higher.
Complete all modules by December 13, 2024 02:00 PM

MODULE 1

Bad Actors

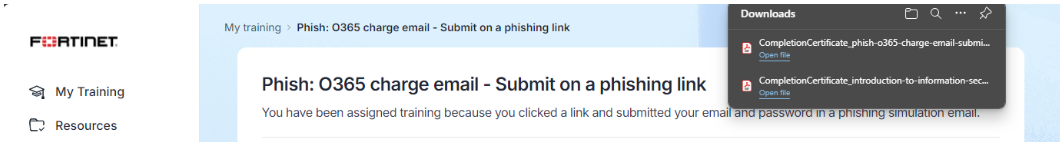
This module will help you understand bad actors by identifying the types of bad actors and their motives.

12 minutes

Completed

Start again

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.


FURTINET
My Training
Resources
My training › Phish: O365 charge email - Submit on a phishing link
Downloads

Phish: O365 charge email - Submit on a phishing link

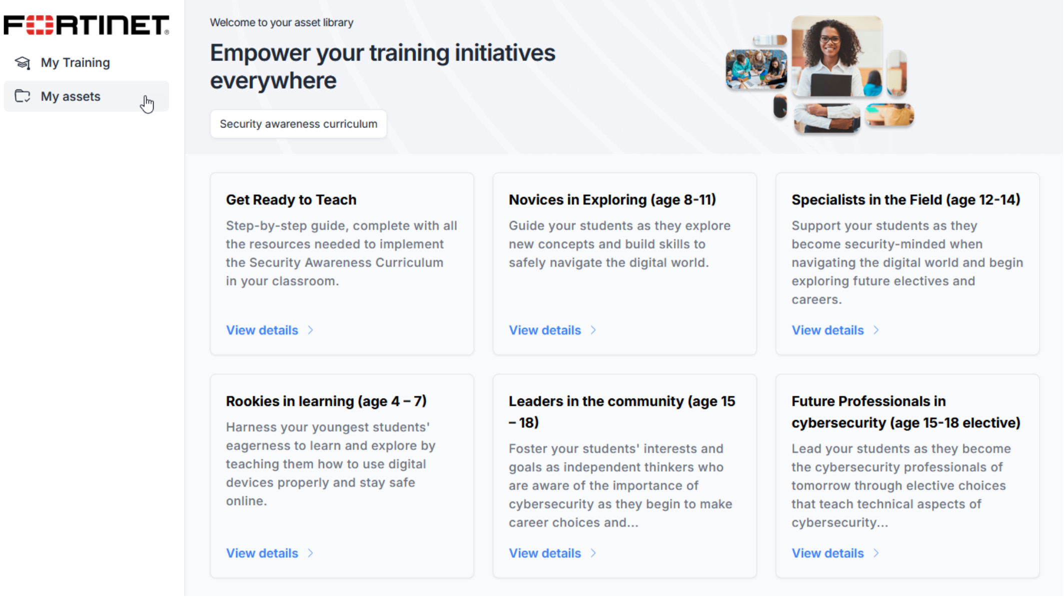
You have been assigned training because you clicked a link and submitted your email and password in a phishing simulation email.

CompletionCertificate_phish-o365-charge-email-submi...
Open file

CompletionCertificate_introduction-to-information-sec...
Open file

My assets

The *My assets* navigation item (if configured by the administrator) allows learners to access additional security awareness curriculum assets. These assets are provided to allow teachers or other professionals to download the materials necessary to deliver different security awareness topics to younger audiences in a classroom environment. These younger learners do not require accounts to access the Fortinet Security Awareness and Training Service as their content is delivered in classroom.



Empower your training initiatives everywhere

Get Ready to Teach

Step-by-step guide, complete with all the resources needed to implement the Security Awareness Curriculum in your classroom.

View details ›

Novices in Exploring (age 8-11)

Guide your students as they explore new concepts and build skills to safely navigate the digital world.

View details ›

Specialists in the Field (age 12-14)

Support your students as they become security-minded when navigating the digital world and begin exploring future electives and careers.

View details ›

Rookies in learning (age 4 – 7)

Harness your youngest students' eagerness to learn and explore by teaching them how to use digital devices properly and stay safe online.

View details ›

Leaders in the community (age 15 – 18)

Foster your students' interests and goals as independent thinkers who are aware of the importance of cybersecurity as they begin to make career choices and...

View details ›

Future Professionals in cybersecurity (age 15-18 elective)

Lead your students as they become the cybersecurity professionals of tomorrow through elective choices that teach technical aspects of cybersecurity...

View details ›

For more information on the assets provided and a description of each, see Security Awareness Curriculum.

My profile

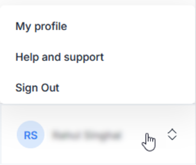
When learners log in to the service, they can make changes to their account by accessing the *My profile* section of the user menu.

From this menu, learners can:

- Change the default time zone assigned by the administrator.
- Change the default language assigned by the administrator.
- Configure two factor authentication (if the administrator has not configured the service to use an existing solution for the users).
- Change the leaner password (if the administrator has not configured the service to use an existing solution for the users).

Accessing the My profile Menu

To access the *My profile* menu, select the user name from the bottom left corner of the learner experience screen.



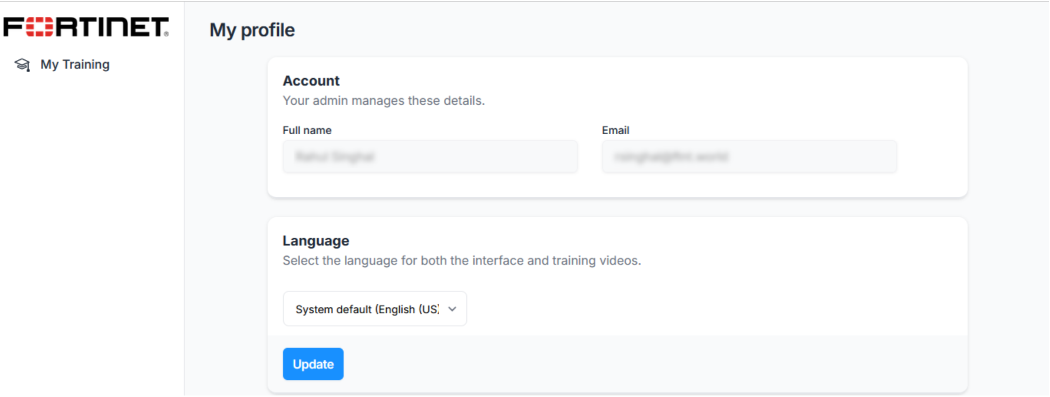
Service Default Language and Time zone

Administrators of the system can set the default language and time zone of the service. Initially, all users who are added will be set to the currently configured default language and time zone. When learners log in to the learner experience, this is the language that the interface and any assigned training will be presented in. The time zone will also match the administrator assigned default.

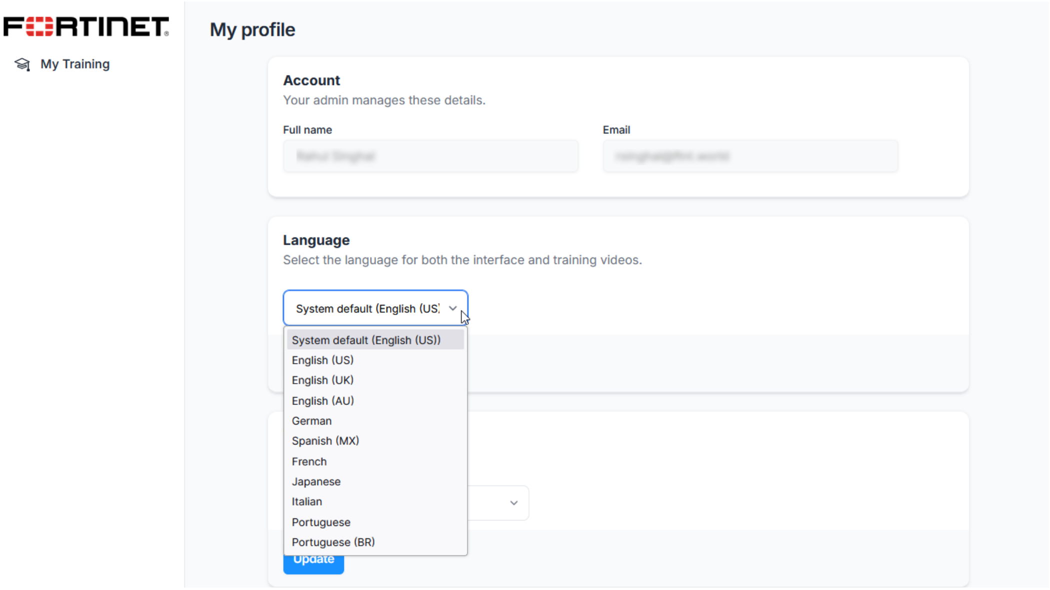
Regardless of the learner experience time zone setting, campaign start times and associated time zone are dictated by the administrator at campaign creation time. For example, if the administrator schedules the campaign for 6 a.m. Eastern time, learners will receive the invites at 6 a.m. Eastern time regardless of the time zone setting they select.

To modify the learner experience language setting:

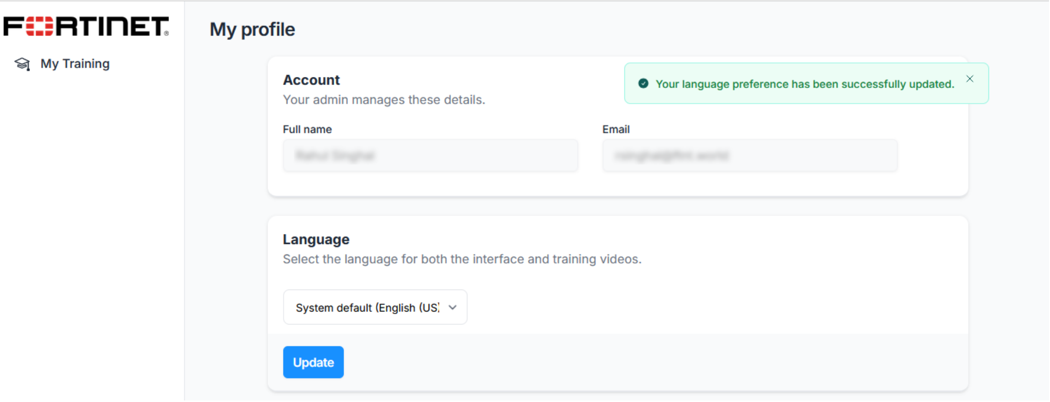
1. Select *My profile* from the user menu system. The *My profile* setting page is presented.


FORTINET
My Training
My profile
Account
Your admin manages these details.
Full name
Email
Language
Select the language for both the interface and training videos.
System default (English (US)
Update

2. In the *Language* section, click on the language selection drop-down box and select the desired language.



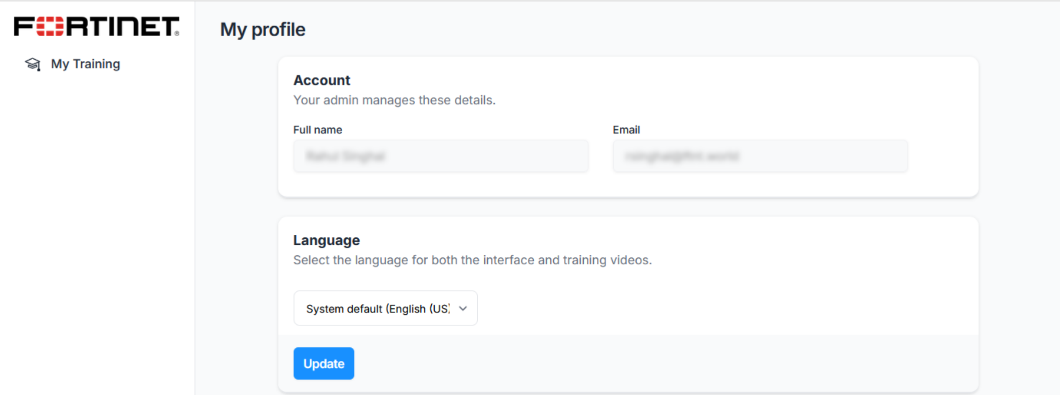
3. Select the desired language from the list of currently supported languages.
4. Click *Update*.


Your language preference has been successfully updated.
FORTINET
My Training
My profile
Account
Your admin manages these details.
Full name
Email
Language
Select the language for both the interface and training videos.
System default (English (US)
Update

5. A confirmation message is displayed. Your interface and training should now appear in the desired language.

To modify the learner experience time zone setting:

1. Select *My profile* from the user menu system. The *My profile* setting page is presented.



My profile

Account

Your admin manages these details.

Full name: [redacted]

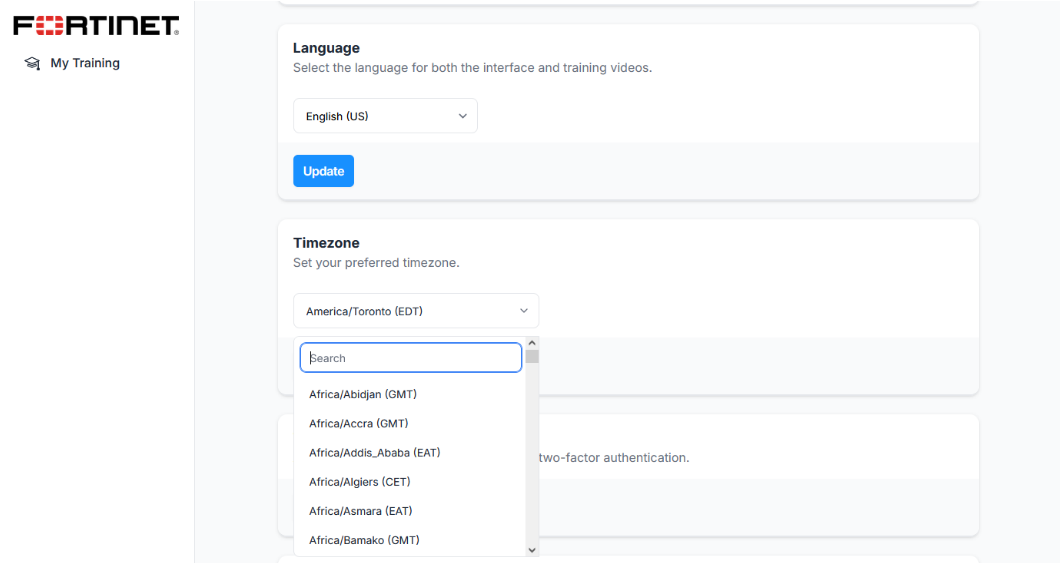
Email: [redacted]

Language

Select the language for both the interface and training videos.

System default (English (US)

2. In the *Timezone* section, click on the time zone selection drop-down box, search and select the desired time zone.



Language

Select the language for both the interface and training videos.

English (US)

Timezone

Set your preferred timezone.

America/Toronto (EDT)

Search

Africa/Abidjan (GMT)

Africa/Accra (GMT)

Africa/Addis_Ababa (EAT)

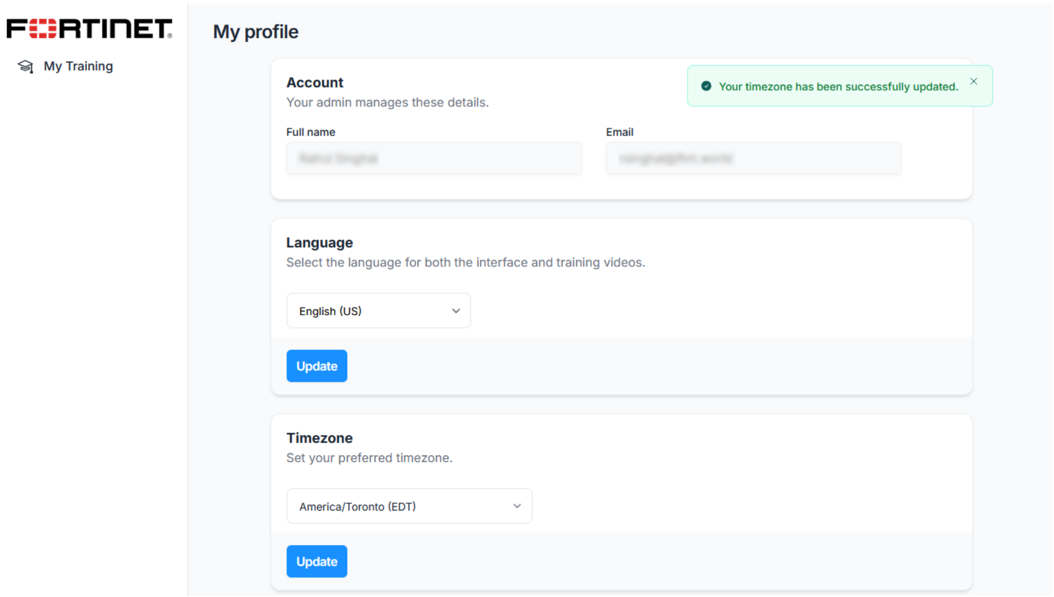
Africa/Algiers (CET)

Africa/Asmara (EAT)

Africa/Bamako (GMT)

two-factor authentication.

3. Search and select the desired time zone from the list provided.
4. Click *Update*. A confirmation message is displayed. Your interface and training should now appear in the desired language.



My profile

Your timezone has been successfully updated. ×

Account

Your admin manages these details.

Full name: [redacted]

Email: [redacted]

Language

Select the language for both the interface and training videos.

English (US)

Timezone

Set your preferred timezone.

America/Toronto (EDT)

Two-Factor Authentication (2FA)

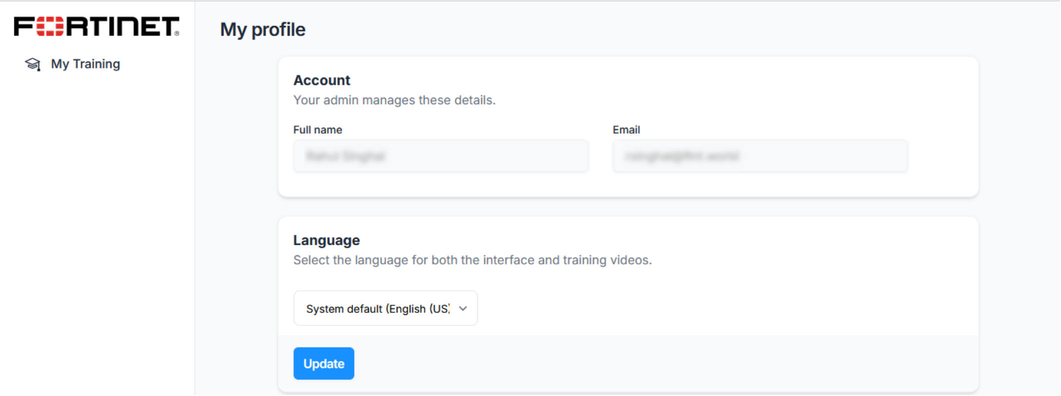
This option is only available if the administrator has not configured the service to use an existing Single Sign-On (SSO) solution for the service. If the administrator of the service configures the service to use an existing SSO solution, this option will not appear in the Learner Experience interface.

Two-factor authentication adds an extra layer of security. When users log in, they will need to verify the login using an authenticator application after they enter their username (email) and password. This ensures that two factors are enforced when accessing the learner experience: something you know and something you have (your phone). Only a person who possesses knowledge of the username and password and has physical access to the mobile device will be able to log in to the service. This setting is highly recommended for the administrators of the service.

Configuring Two-Factor Authentication (2FA)

To configure 2FA:

1. Select *My profile* from the user menu system. The *My profile* setting page is presented.



My profile

Account

Your admin manages these details.

Full name: [redacted]

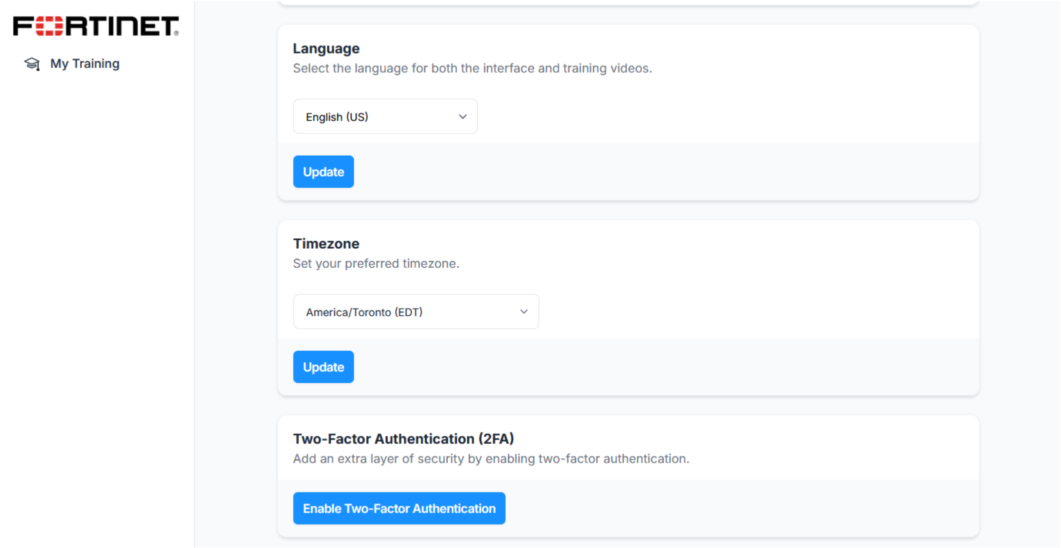
Email: [redacted]

Language

Select the language for both the interface and training videos.

System default (English (US)

2. In the *Two-Factor Authentication (2FA)* section, click *Enable Two-Factor Authentication*.



Language

Select the language for both the interface and training videos.

English (US)

Timezone

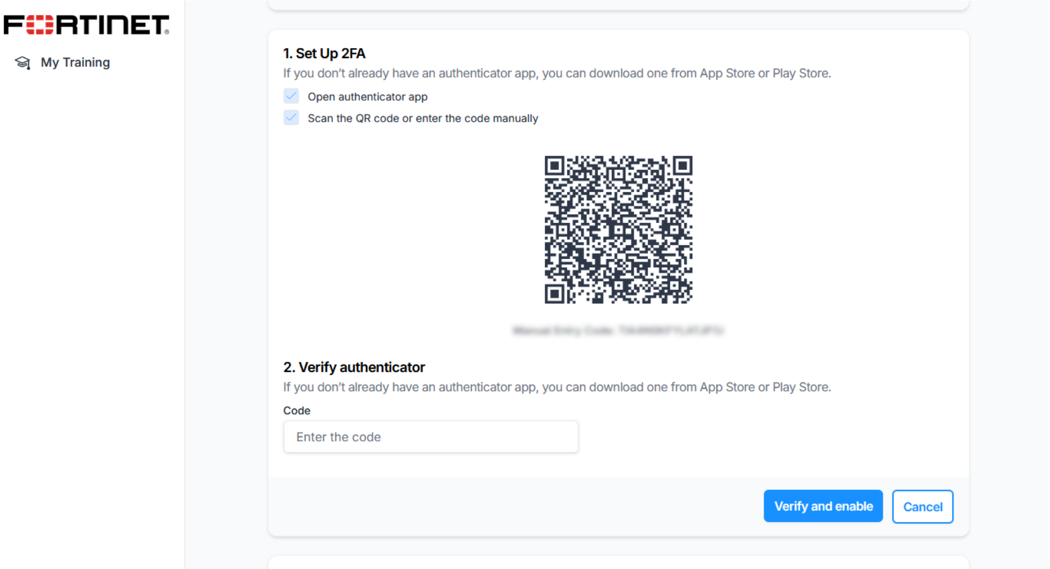
Set your preferred timezone.

America/Toronto (EDT)

Two-Factor Authentication (2FA)

Add an extra layer of security by enabling two-factor authentication.

3. The configuration section is presented.



1. Set Up 2FA

If you don't already have an authenticator app, you can download one from App Store or Play Store.

☑ Open authenticator app

☑ Scan the QR code or enter the code manually

[redacted]

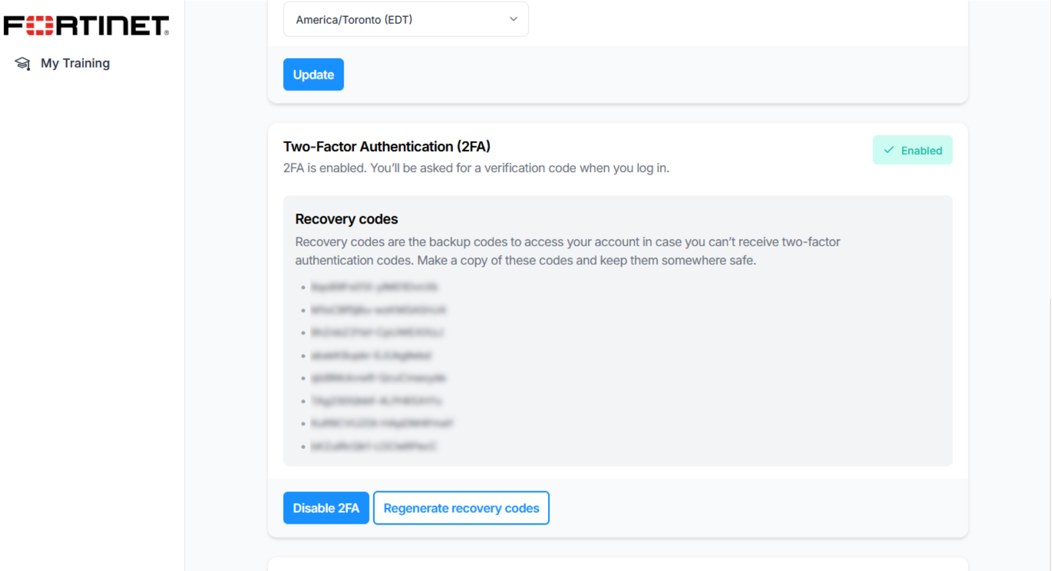
2. Verify authenticator

If you don't already have an authenticator app, you can download one from App Store or Play Store.

Code: Enter the code

4. Download a new or open an existing authenticator application and scan the QR code (instructions very by application), then enter the code the application provides and click on the *Verify and enable* button.

   A confirmation message confirms that two-factor authentication has been enabled.



Two-Factor Authentication (2FA) ✓ Enabled

2FA is enabled. You'll be asked for a verification code when you log in.

Recovery codes

Recovery codes are the backup codes to access your account in case you can't receive two-factor authentication codes. Make a copy of these codes and keep them somewhere safe.

[redacted]

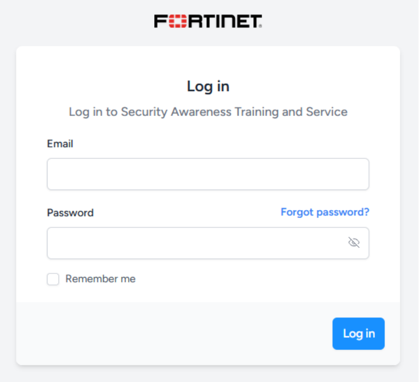
Recovery codes are the backup codes to access your account in case you can't receive two-factor authentication codes. Make a copy of these codes and keep them somewhere safe.

You also have the option to disable 2FA. You will be required to log in using the currently configured method (username and password or two-factor authentication) when accessing this section to change the configuration).

Reset password

For learners whose organizations have not configured a third-party SAML2 single sign-on solution for the service (such as Google Workspace, Azure, RapidID, and so on), it is important to regularly change your password in order to keep your account secure.

The learner experience allows you to change your password. This requires that you know your current password and that you can successfully log in to the service. Learners who have forgotten their password can perform a password reset from the login screen:



Log in

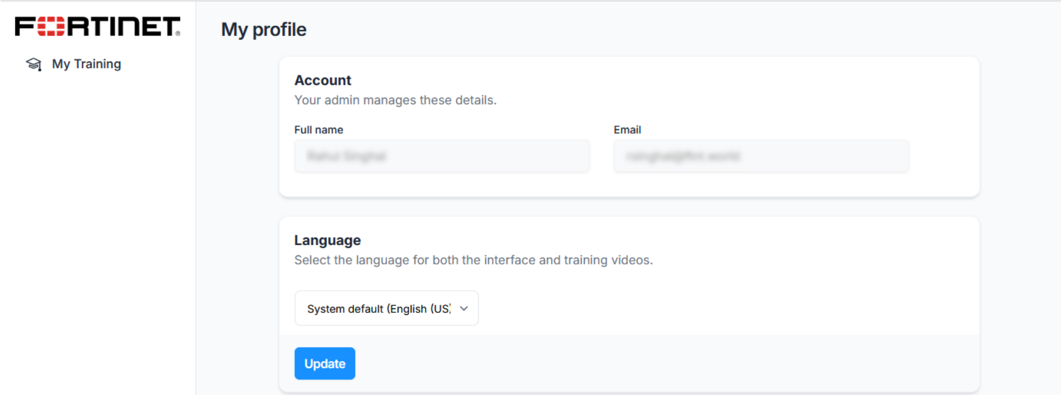
Log in to Security Awareness Training and Service

If you do not remember your password and you are attempting to regain access to the service, you must select the *Forgot password* link from the respective landing page presented when you click on the training link provided by your administrator.

Changing your password

To change the password:

1. Select *My profile* from the user menu system. The *My profile* setting page is presented.



My profile

Account

Your admin manages these details.

Full name: [redacted]

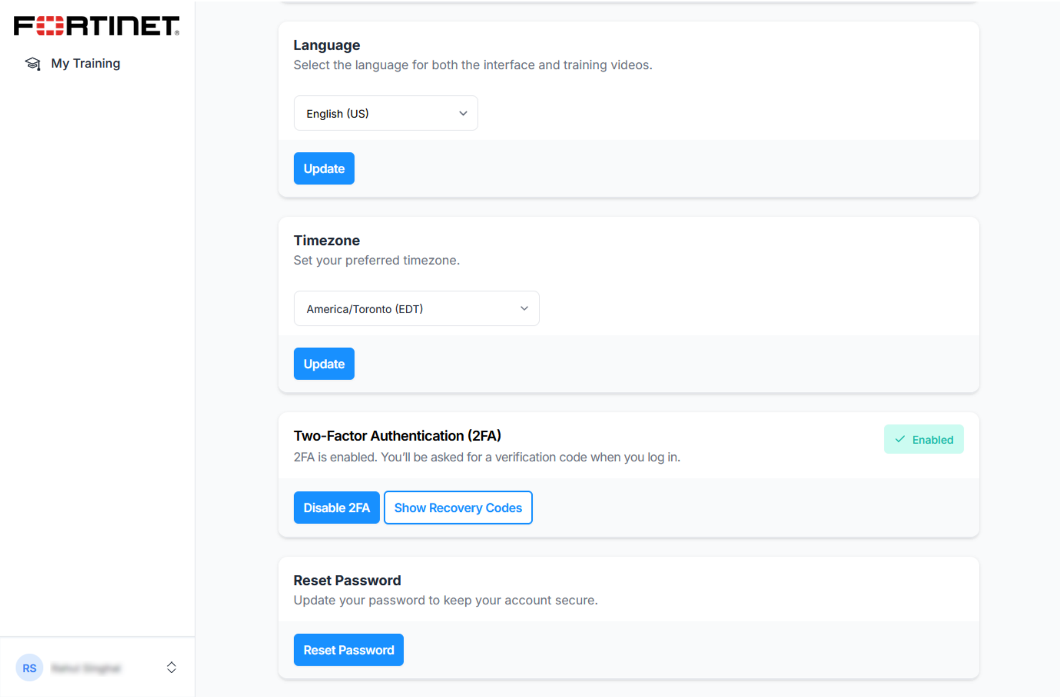
Email: [redacted]

Language

Select the language for both the interface and training videos.

System default (English (US)

2. Scroll down to the *Reset Password* section at the bottom of the screen and select *Reset Password*.



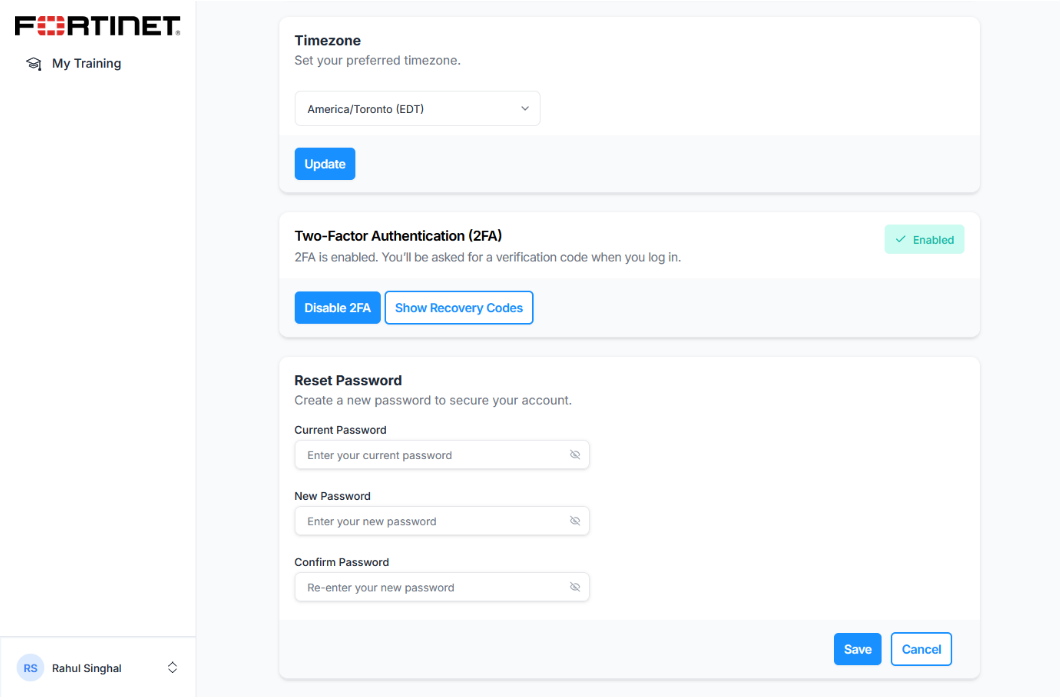
Language
Select the language for both the interface and training videos.
English (US)

Timezone
Set your preferred timezone.
America/Toronto (EDT)

Two-Factor Authentication (2FA)
2FA is enabled. You'll be asked for a verification code when you log in.

Reset Password
Update your password to keep your account secure.

The *Reset Password* section is displayed.



Timezone
Set your preferred timezone.
America/Toronto (EDT)

Two-Factor Authentication (2FA)
2FA is enabled. You'll be asked for a verification code when you log in.

Reset Password
Create a new password to secure your account.

Current Password
Enter your current password

New Password
Enter your new password

Confirm Password
Re-enter your new password

3. Enter your current password in the *Current Password* field.
4. Enter your new password in the *New Password* field.
5. Re-enter your new password in the *Confirm Password* field.
6. Click on the *Save* button.

Initializing the service

Creating a FortiCloud master support account

Before you can initialize and configure the service, you must first create a FortiCloud master support account. Some customers may wish to use an existing FortiCloud master support account. They do not need to complete this step.

To create an account, see FortiCloud Account guide.

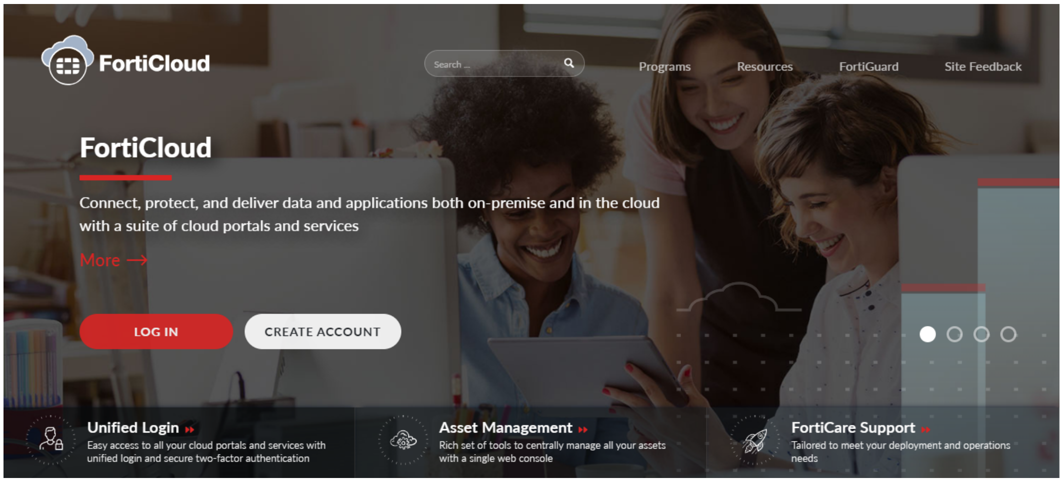
You can only initialize the Fortinet Security Awareness and Training Service using a master support account. If you attempt to initialize using a FortiCloud sub account, the operation will fail.

Registering the service using the service contract:

Once you have access to a FortiCloud account you can initialize the service. Initializing the service without a license (contract number), will set up the free 25 user, standard level service. A license can be entered at a later date.

To enter your license (contract number) to access a larger number of seats or the premium service level:

1. Navigate to https://support.fortinet.com and select *Login Now*.



FortiCloud

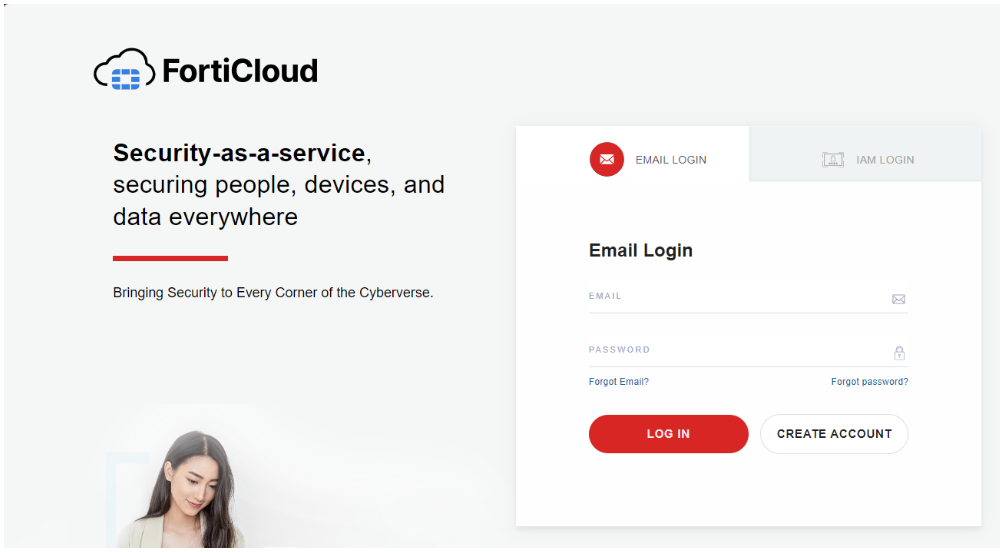
Connect, protect, and deliver data and applications both on-premise and in the cloud with a suite of cloud portals and services

Unified Login: Easy access to all your cloud portals and services with unified login and secure two-factor authentication

Asset Management: Rich set of tools to centrally manage all your assets with a single web console

FortiCare Support: Tailored to meet your deployment and operations needs

2. Log in using your email and password.



FortiCloud

Security-as-a-service, securing people, devices, and data everywhere

Bringing Security to Every Corner of the Cyberverse.

3. Click *Register Now*.
4. Enter the license (contract number) provided by your distributor in the *Registration Code* input field, select your *End User Type* and select *Next*.
5. You will be asked to agree to the End User License Agreements. Once registered, you can access your Security Awareness and Training Service (and optionally FortiPhish) license information from the *Account Services* option in the Asset Management portal.

If you click on the Serial Number of the Security Awareness and Training entry, you will see more information about your issued licenses.

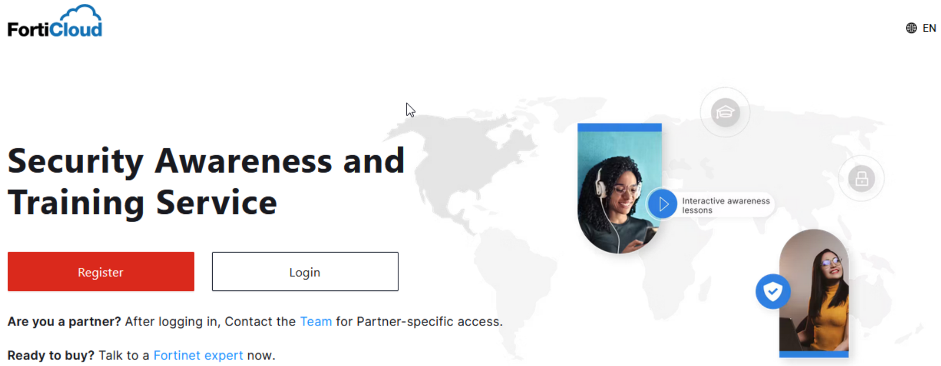
If you have purchased a FortiPhish license, you will also need to enter this product code using the steps above. This license must be registered using the same account that was used to enter the Security Awareness and Training Service product code.

Initializing the service or tenant

Before you can configure the service, you must first initialize the service. This is done by logging to one of the links provided below, using a FortiCloud master support account. This must be a master account. Logging in to the links provided below with a non master support account will not initialize a tenant.

To initialize the service or tenant:

1. Navigate to https://ftnt.info.



FortiCloud

EN

Security Awareness and Training Service

Register Login

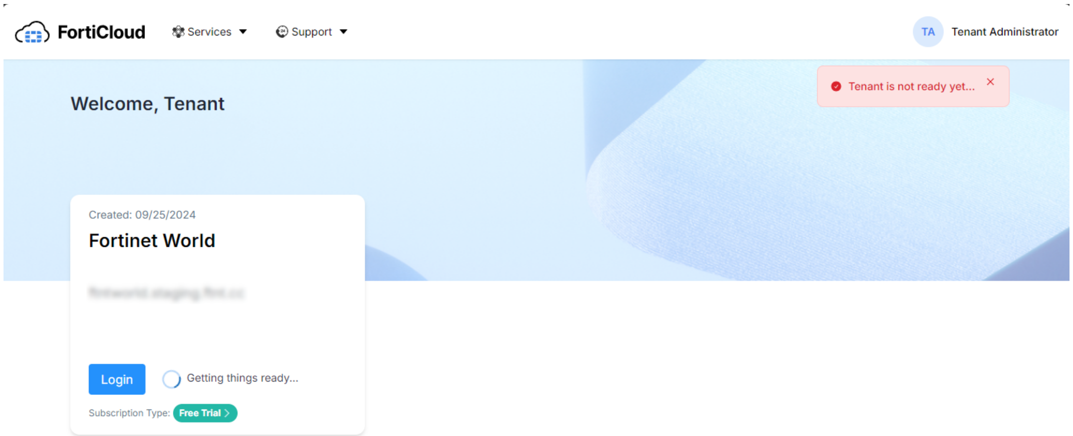
Are you a partner? After logging in, Contact the Team for Partner-specific access.

Ready to buy? Talk to a Fortinet expert now.

2. Select *Login* and enter the username and password for your FortiCloud account. The service will initialize after a few seconds and you will be presented with the Let's set up your site screen:
3. Enter the official name of the organization in the *Organization Name* field. This information is used in the site title.
4. Select the region you would like to store your learner data in from the *Region* dropdown.
5. Fortinet may add additional selections in this field as required in the future. If you would like to request an additional region, you can open a support ticket and a feature request will be raised for future consideration. See Technical support on page 8.
6. Currently, you can select to store your learner data in: Americas (data is stored in the United States (Washington) or Europe, Middle East and Africa (data is stored in Frankfurt, Germany).
7. Enter the desired domain name in the *Domain Name* field. You can use a different domain when verifying your domain. This is a unique identify to differentiate your tenant from others.

The domain name can only contain letters and numbers. If the name is already in use, you will need to choose a different domain.

8. You may wish to enter the first section of your domain name. For example, for Fortinet, we might enter fortinet.us.ftnt.info or fortinet.de.ftnt.info (depending on your learner data storage location selection).
9. Select *Set up*.
10. Your service will be initialized. You will need to wait until the process completes.



Tenant is not ready yet...

Welcome, Tenant

Created: 09/25/2024

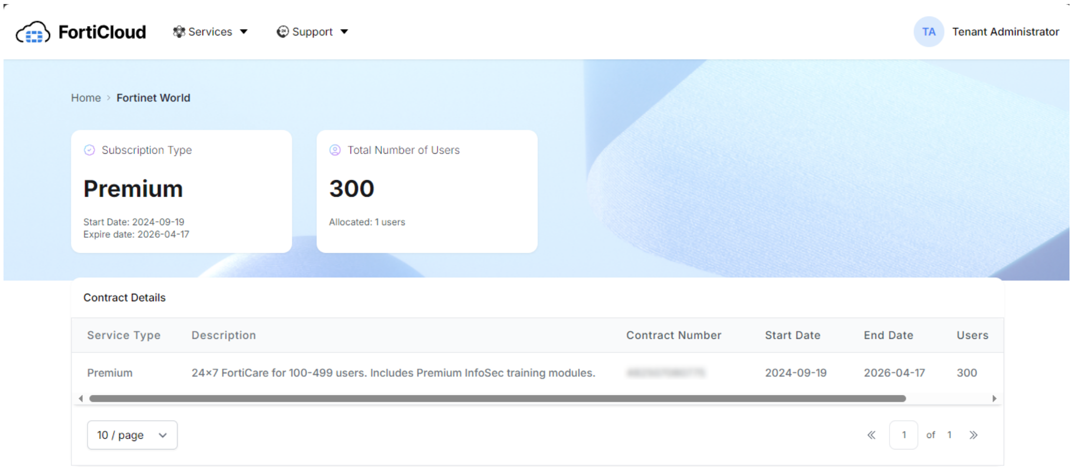
Fortinet World

[redacted]

Getting things ready...

Subscription Type: Free Trial

11. You can verify your subscription level by clicking on the *Subscription Type* (green) button.
12. The current subscription information is presented:



Subscription Type

Premium

Start Date: 2024-09-19
Expire date: 2026-04-17

Total Number of Users

300

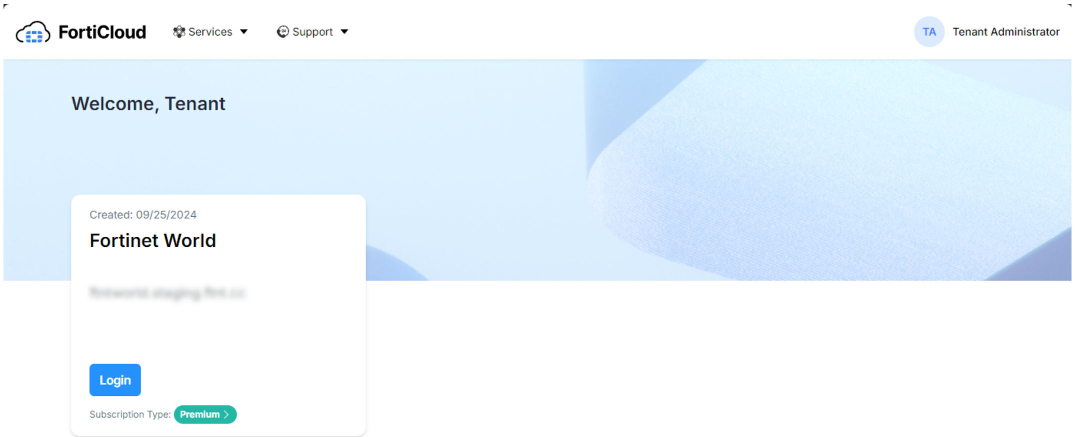
Allocated: 1 users

Contract Details

Service Type	Description	Contract Number	Start Date	End Date	Users
Premium	24×7 FortiCare for 100-499 users. Includes Premium InfoSec training modules.	[redacted]	2024-09-19	2026-04-17	300

It will take some time for the license info to update. If it does not show up immediately, you can check again later. If the license info has been input into the associated FortiCloud account and it is not updating after 24 hours, please open a support ticket.

13. You can return to the log in screen by selecting Home from the path near the top left corner of the screen. The log in screen is presented.



Welcome, Tenant

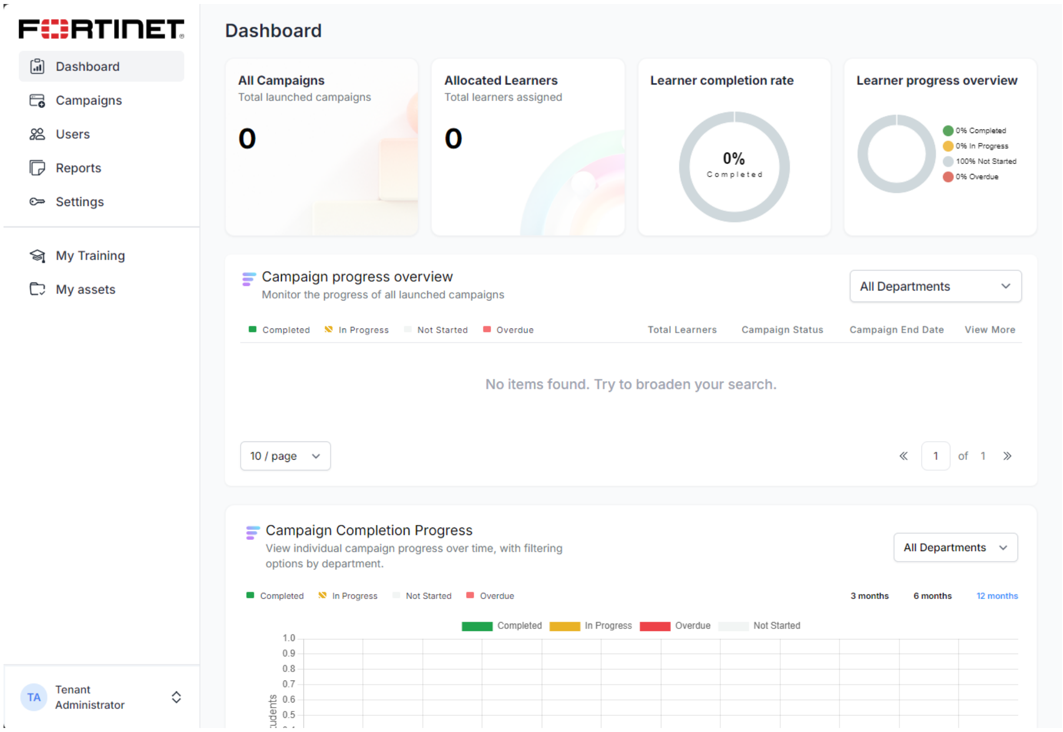
Created: 09/25/2024

Fortinet World

[redacted]

Subscription Type: Premium

14. Select *Login*to access the Fortinet Security Awareness and Training Service admin role. The admin role *Dashboard* page is displayed.



Dashboard

All Campaigns
Total launched campaigns
0

Allocated Learners
Total learners assigned
0

Learner completion rate
0% Completed

Learner progress overview
0% Completed
0% In Progress
100% Not Started
0% Overdue

Campaign progress overview
Monitor the progress of all launched campaigns

🟩 Completed ▨ In Progress Not Started 🟥 Overdue	Total Learners	Campaign Status	Campaign End Date	View More

No items found. Try to broaden your search.

Campaign Completion Progress
View individual campaign progress over time, with filtering options by department.

Configuring and customizing the service or tenant

Configuring the Security Awareness and Training Service has some mandatory and some optional steps. Some configurations are only available to premium service level customers:

- Domain verification on page 41
- Single Sign-On (SSO) SAML2 Configuration (premium service level only)
- Settings – Admin Settings – SMTP settings
- URL Domain Customization (standard service level / free 25 user service)
- URL Domain Customization (premium level service only)
- Appearance and Email Template Customization (premium service level only)
- Creating and importing users on page 70

Settings

Domain verification

The first configuration step is to verify your domain in the Admin Portal tenant. You need to add DNS TXT records for each email domain you wish to send training campaign email notifications to. This is required to prove ownership of the domains you wish to send emails to. You can only add users with email addresses that use a verified domains.

This task must be completed before customizing your URL domain or importing users into the system.

If you do not have access to change your DNS records, you may need to reach out to another resource within your organization.

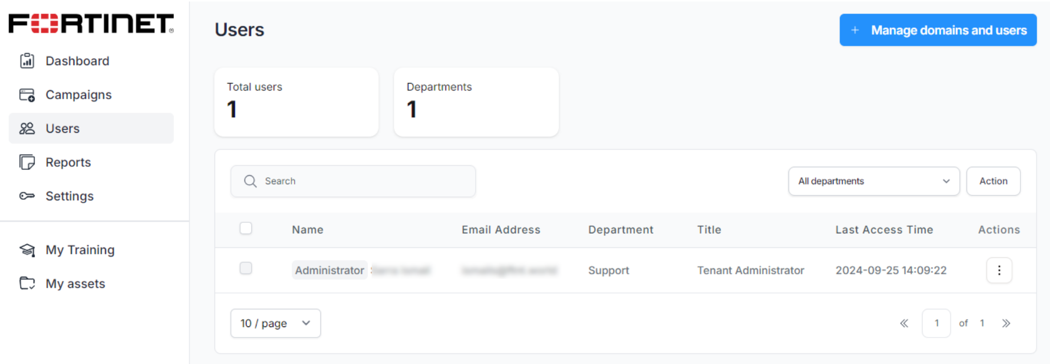
Customers can verify up to 40 email domains.

Domain names must contain:

- Lowercase only
- At least one letter
- At least three characters
- No more than 64 characters
- Only characters supported in domain names (such as hyphen)

To verify domain ownership:

1. Select *Users* from the Navigation Menu.
2. Click + *Manage domains and users*.



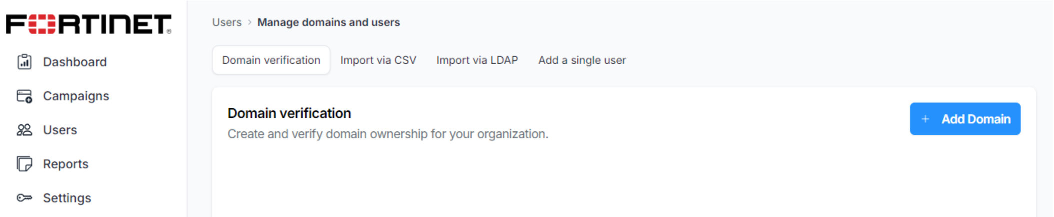
Users

Total users 1

Departments 1

□	Name	Email Address	Department	Title	Last Access Time	Actions
□	Administrator [redacted]	[redacted]	Support	Tenant Administrator	2024-09-25 14:09:22	⋮

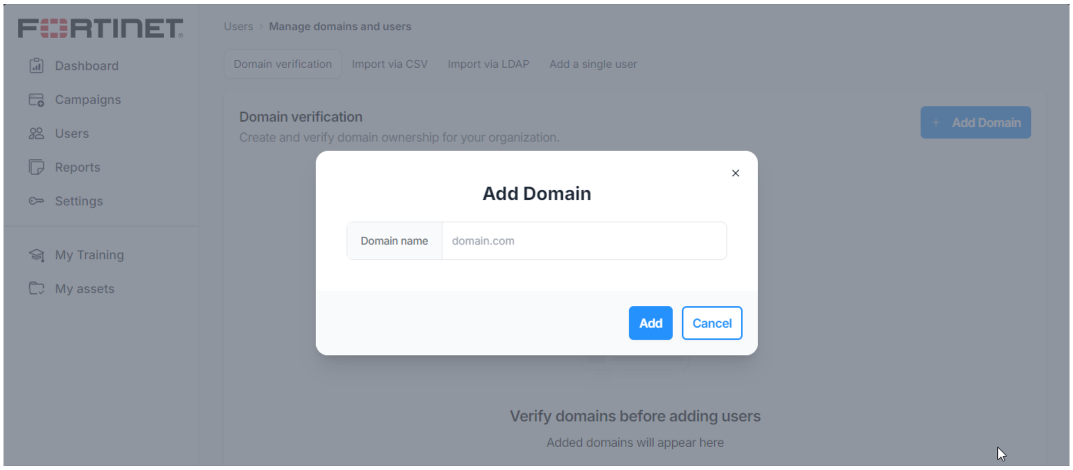
3. Click + *Add Domain*.



Domain verification

Create and verify domain ownership for your organization.

4. Enter the email domains (one at a time) that you would like to be able to send training emails to in the *Domain name* field and select *Add*.



Domain verification

Create and verify domain ownership for your organization.

Add Domain

Domain name: domain.com

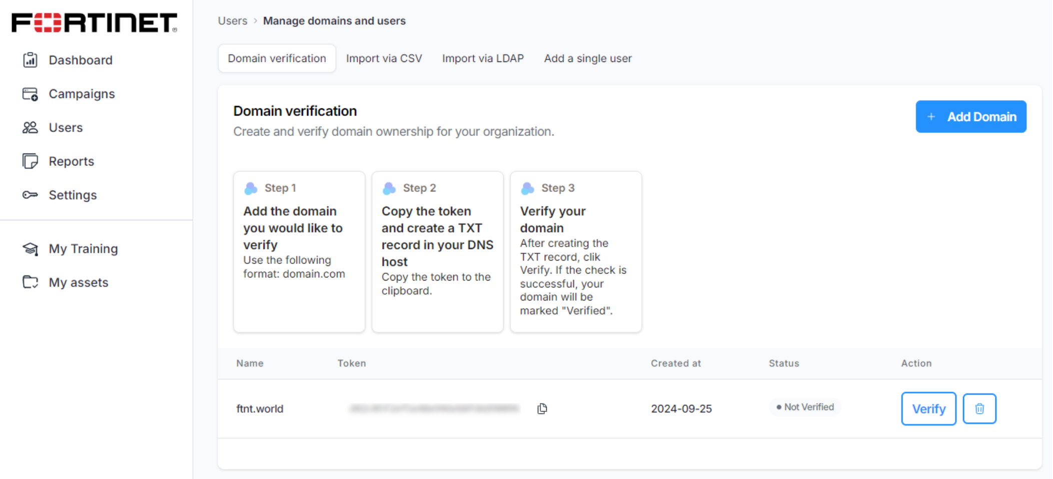
Verify domains before adding users

Added domains will appear here

5. A token will be produced. Follow the three steps on the screen to complete verification of the domain.

Propagation of the DNS TXT record may take up to 72 hours depending on your DNS System and Service Provider.

6. Once these steps have been completed, click *Verify*.



Domain verification

Create and verify domain ownership for your organization.

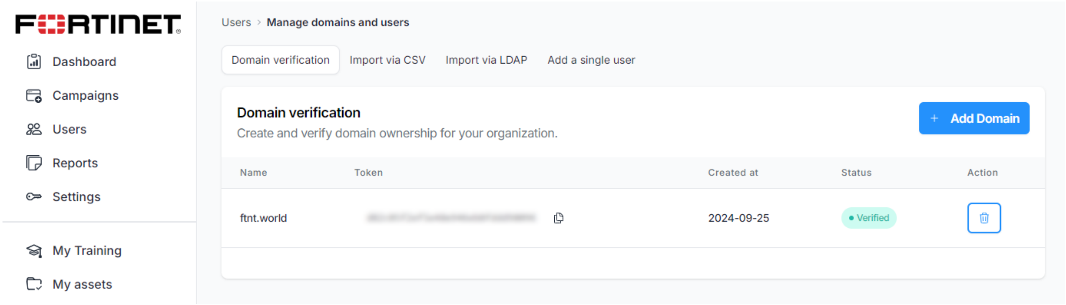
Step 1
Add the domain you would like to verify
Use the following format: domain.com

Step 2
Copy the token and create a TXT record in your DNS host
Copy the token to the clipboard.

Step 3
Verify your domain
After creating the TXT record, clik Verify. If the check is successful, your domain will be marked "Verified".

Name	Token	Created at	Status	Action
ftnt.world	[redacted]	2024-09-25	● Not Verified	Verify

7. If the DNS TXT record was created successfully and the record has propagated, the *Status* should change to a green *Verified*.



Domain verification

Create and verify domain ownership for your organization.

Name	Token	Created at	Status	Action
ftnt.world	[redacted]	2024-09-25	● Verified	🗑

If your domain does not verify after 72 hours, please verify if your DNS TXT record is available using Google Dig. See How to verify your DNS TXT and 'A' records have been added correctly and have been successfully propagated.

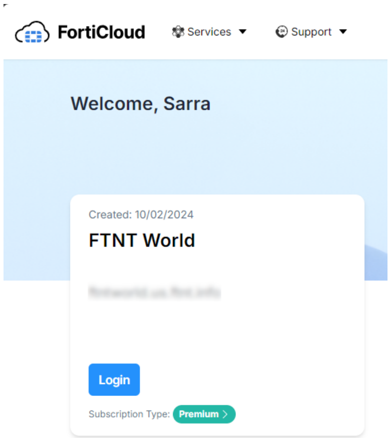
If the DNS TXT record is not available using Google Dig, you will need to verify your DNS TXT record exists. You may also have issues if the DNS TXT token is missing characters or contains leading or trailing spaces. The token must match exactly and is case sensitive.

If you make a mistake, you can delete the registered domain by selecting the trash can icon to the right of the entry.

Admin Settings

Domain setup (Standard level service / Free 25 user service)

You may configure up to one learner domain. The default is set when you initialized your tenant. You can view this by selecting the log in screen tab.



Welcome, Sarra

Created: 10/02/2024

FTNT World

[redacted]

Subscription Type: Premium

In this example, the default domain name is ftntworld.us.ftnt.info. *ftntworld* is the custom domain input during the initialization. *us* refers to the location you chose to store your user data when you initialized your tenant.

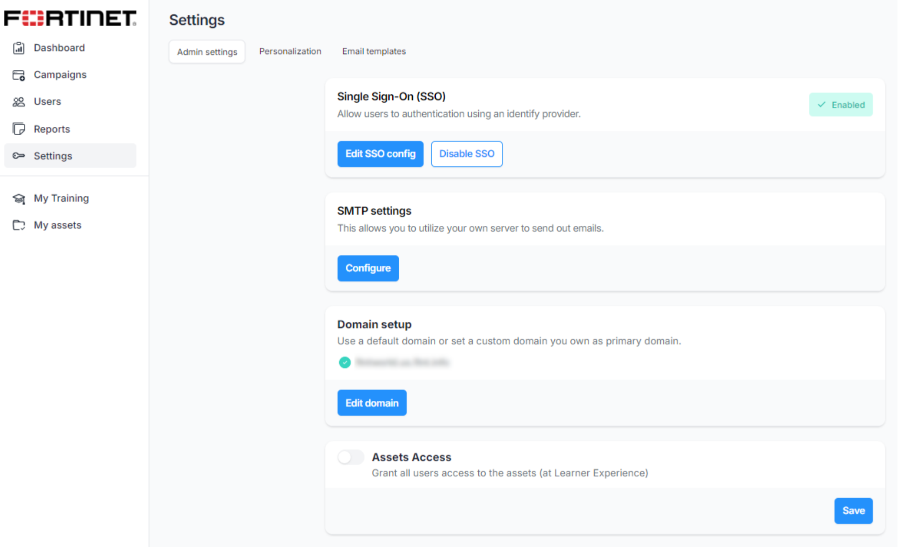
You may edit this custom domain after initialization. This domain will be the URL sent to and used by your learners when they are sent training invitations. It is the URL they will use when logging in to the system in order to complete training campaigns.

Sub domain names may contain:

- Lowercase only
- At least one letter
- At least three characters
- No more than 64 characters
- Only characters supported in domain names (such as hyphen)

To edit the default learner domain after initialization:

1. Select *Settings* from the navigation menu.
2. Click *Edit domain* in the *Domain setup* section.



FORTINET

Dashboard
Campaigns
Users
Reports
Settings
My Training
My assets

Settings

Admin settings | Personalization | Email templates

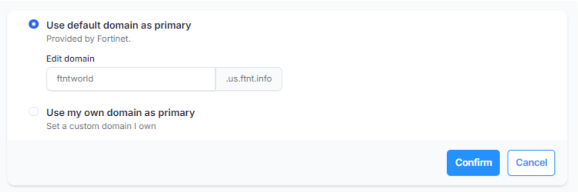
Single Sign-On (SSO)
Allow users to authentication using an identify provider.
✓ Enabled
Edit SSO config | Disable SSO

SMTP settings
This allows you to utilize your own server to send out emails.
Configure

Domain setup
Use a default domain or set a custom domain you own as primary domain.
✓ [redacted]
Edit domain

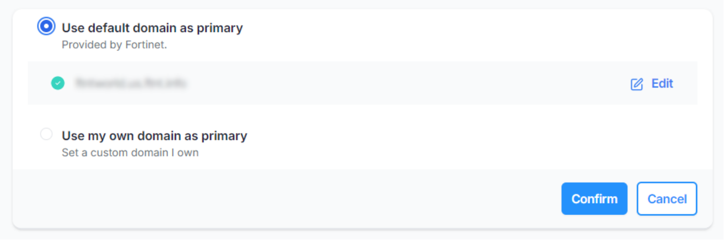
Assets Access
Grant all users access to the assets (at Learner Experience)
Save

3. For standard subscription licenses, you may edit the domain you provided when initializing your tenant by typing a new sub domain in the *Edit domain* field and select *Confirm*.



● Use default domain as primary
Provided by Fortinet.
Edit domain
ftntworld | .us.ftnt.info
○ Use my own domain as primary
Set a custom domain I own
Confirm | Cancel

You should see a green check mark next to the domain entry.



● Use default domain as primary
Provided by Fortinet.
✓ [redacted] Edit
○ Use my own domain as primary
Set a custom domain I own
Confirm | Cancel

Domain setup (Premium level service)

This option is not available with the standard level service or the free 25 user service. Users of the standard level or free service will only be able to create a custom sub domain to our ftnt.info domain, such as ourdomain.ftnt.info.

If you wish to create a custom domain subordinate to one of your verified domains, you should contact your distributor and request an upgrade to the premium level service.

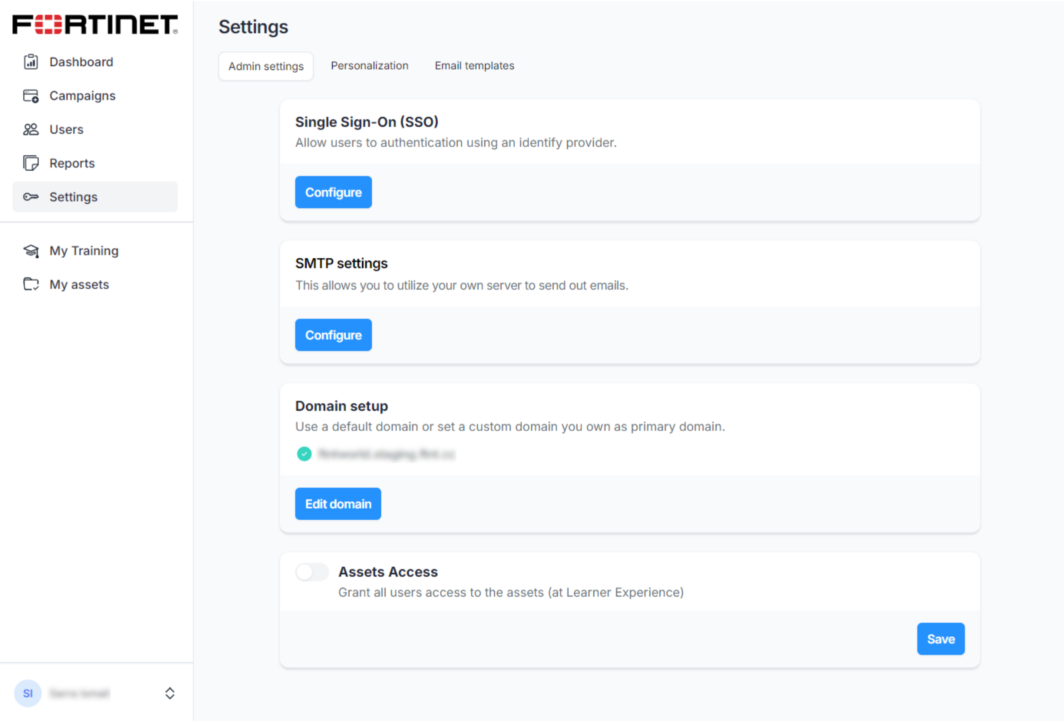
For premium license subscriptions, you can create a custom sub domain of your choice. This domain will be the URL sent to and used by your learners when they are sent training invitations. It is the URL they will use when logging in to the system to complete training campaigns.

Sub domain names may contain:

- Lowercase only
- At least one letter
- At least three characters
- No more than 64 characters
- Only characters supported in domain names (such as hyphen)

To configure the domain of your choice as the primary domain:

1. Select *Settings* from the navigation menu, then select *Edit domain* in the *Domain setup* section:



Single Sign-On (SSO)

Allow users to authentication using an identify provider.

SMTP settings

This allows you to utilize your own server to send out emails.

Domain setup

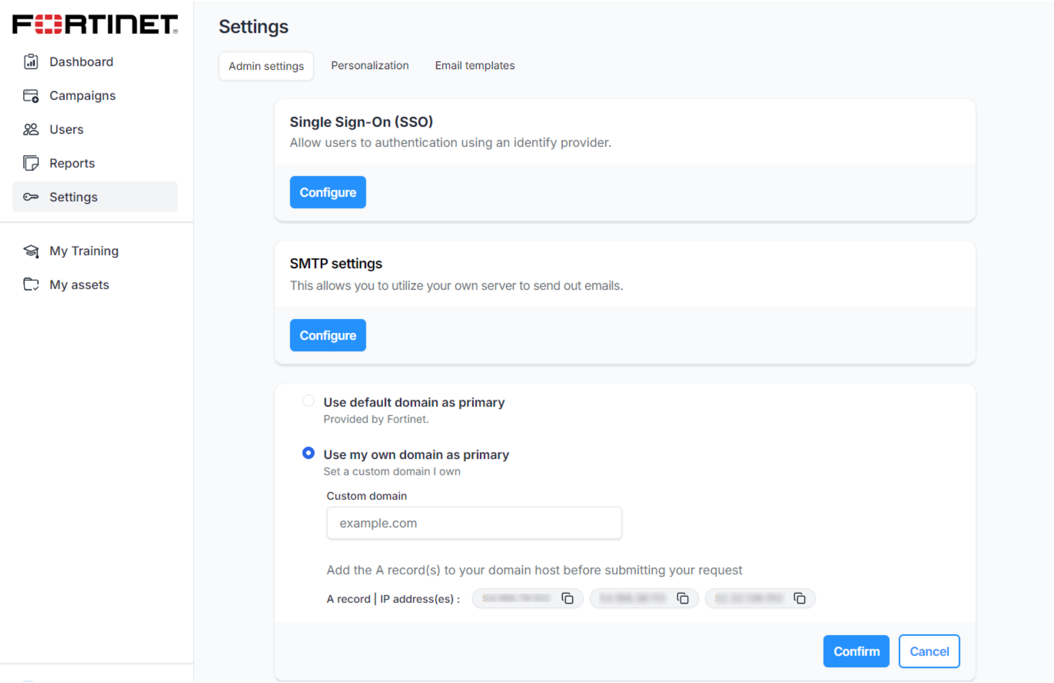
Use a default domain or set a custom domain you own as primary domain.

[redacted]

Assets Access

Grant all users access to the assets (at Learner Experience)

2. Select the *Use my own domain as primary* option.



Single Sign-On (SSO)
Allow users to authentication using an identify provider.

SMTP settings
This allows you to utilize your own server to send out emails.

○ Use default domain as primary
Provided by Fortinet.

● Use my own domain as primary
Set a custom domain I own

Custom domain: example.com

Add the A record(s) to your domain host before submitting your request

A record | IP address(es) : [redacted] [redacted] [redacted]

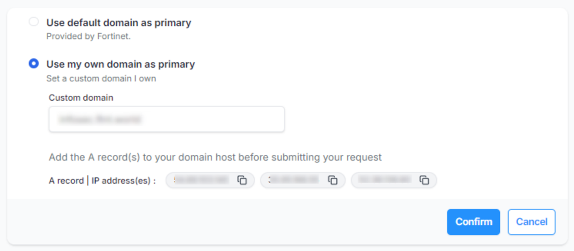
3. Create the ‘A’ records for the desired name using each of the IP addresses listed on the screen (these will vary based on your learner data storage country).

For example, if we wanted a custom domain of ‘infosec.ftnt.world’, we would create three ‘A’ records each containing infosec.ftnt.world and the listed IP addresses:

- infosec.ftnt.world using IP: 54.69.103.145
- infosec.ftnt.world using IP: 35.95.166.55
- infosec.ftnt.world using IP: 52.38.136.80

Always use the IP addresses presented in the service and not the ones listed in this document as they may differ depending on where your learner data is stored.

4. After the A records have been created and propagated, you can enter the new domain (such as infosec.ftnt.world) into the Custom domain field and select the Confirm button.



○ Use default domain as primary
Provided by Fortinet.

● Use my own domain as primary
Set a custom domain I own

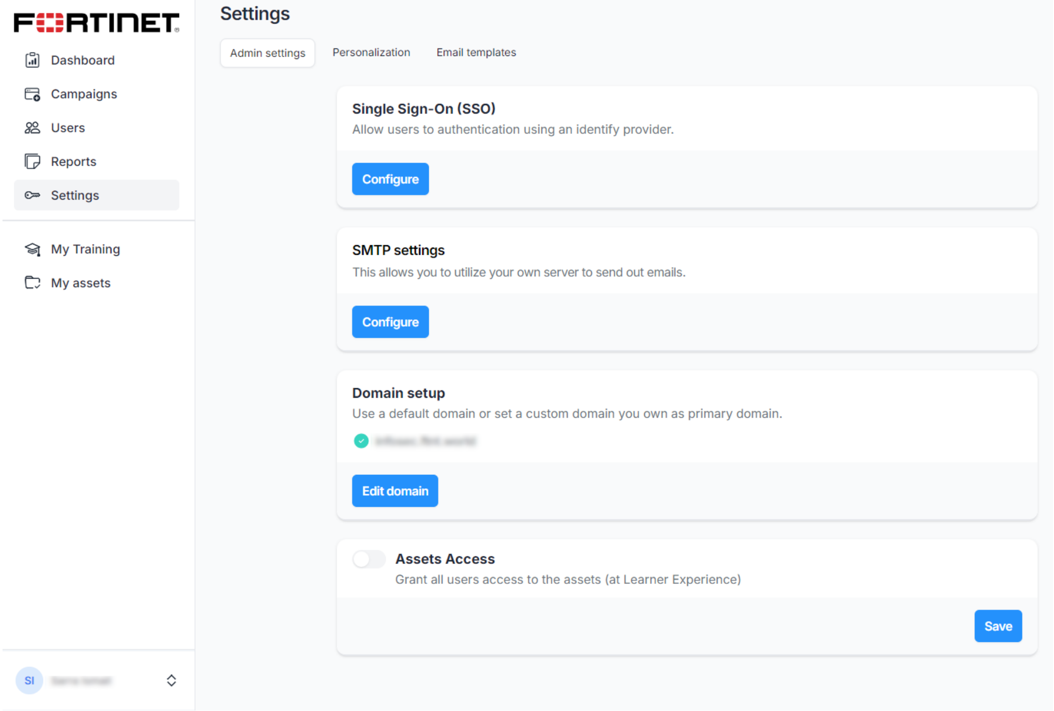
Custom domain: [redacted]

Add the A record(s) to your domain host before submitting your request

A record | IP address(es) : [redacted] [redacted] [redacted]

Propagation of the DNS TXT record may take up to 24 hours depending on your DNS System / Service Provider.

5. If the ‘A’ records have been created correctly and the information has propagated, you should bet a green check mark beside the name of your custom domain.



Settings

Single Sign-On (SSO)
Allow users to authentication using an identify provider.

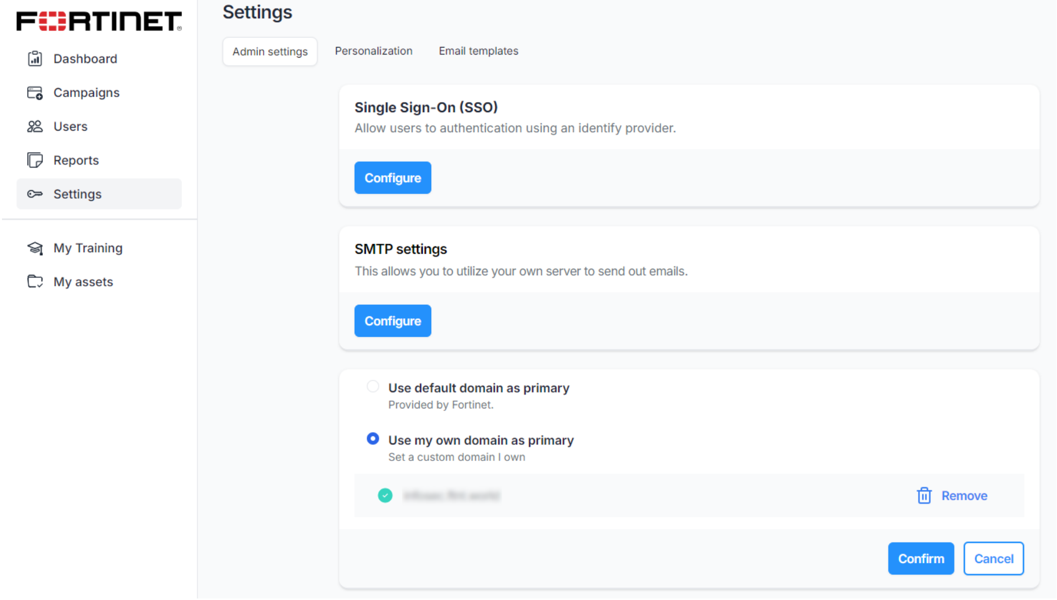
SMTP settings
This allows you to utilize your own server to send out emails.

Domain setup
Use a default domain or set a custom domain you own as primary domain.
✓ [redacted]

Assets Access
Grant all users access to the assets (at Learner Experience)

If your A Record does not verify after 24 hours, please use the following instructions to verify if you’re a record is available using Google Dig. See How to verify your DNS TXT and 'A' records have been added correctly and have been successfully propagated.

You can delete this mapping and create a new one should you decide to change your custom domain in the future.



Settings

Single Sign-On (SSO)
Allow users to authentication using an identify provider.

SMTP settings
This allows you to utilize your own server to send out emails.

○ Use default domain as primary
Provided by Fortinet.

● Use my own domain as primary
Set a custom domain I own

✓ [redacted]

Single sign-on (SSO)

You should complete the Domain verification and Domain setup steps before completing this configuration. The links generated for the SSO configuration are built based on the Domain setup configuration. This will also allow you to manually add one of your users to test the SSO (SAML2) configuration after completing the configuration steps.

These features are only available for premium service level licenses: Free 25 user Premium (for Partners only) and Premium (purchased by customer). It is not available for free and standard service level licenses.

The Security Awareness and Training Service allows customers and partners to share meta data to establish a baseline of trust and interoperability using the XML based Security Assertion Markup Language (SAML) standard.

Using one of your existing SAML2 single sign-on solutions to authenticate users when they log in to the system allows users to use an existing credential set, such as email, password, and MFA (optional), when logging in to the system. Users will not have to use a Fortinet assigned credential set when logging in to the service.

Configuring a single sign-on solution allows users to authenticate to the Fortinet Security Awareness and Training Service. Before users can log in, they must first be imported into the service. See Creating and importing users on page 70.

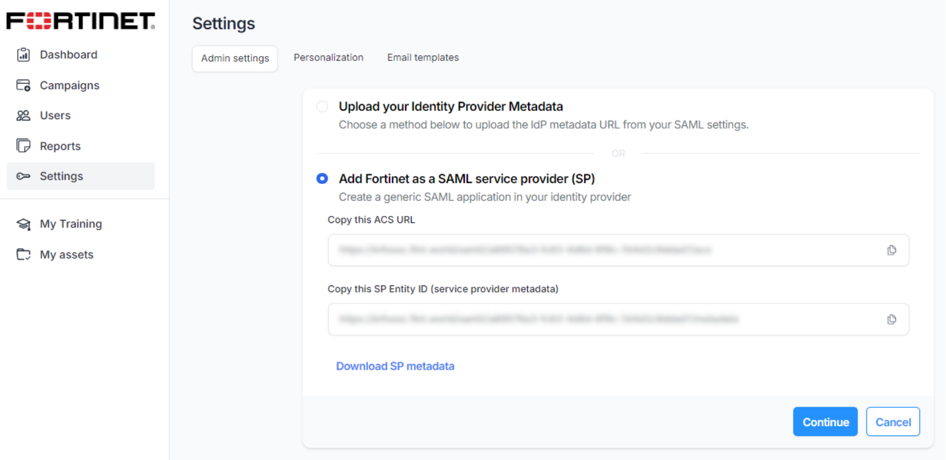
Currently, the service does not support account creation during the single sign-on log in process.

Different solution providers have different configuration steps for configuring a SAML2 app for authentication with third-party services. Customers will need to work with their internal IT department or service provider to configure the SAML2 application for the Fortinet Security Awareness and Training Service.

If you require assistance configuring the authentication component, send an email to infosec_awareness@fortinet.com. A Deployment Specialist will reach out to request times that work and will schedule a meeting with our team, and, if necessary, the support team from your SSO vendor.

To configure SSO by adding Fortinet as a SAML service provider:

1. Select *Add Fortinet as a SAML service provider (SP)*.



Settings

Admin settings | Personalization | Email templates

○ Upload your Identity Provider Metadata
Choose a method below to upload the IdP metadata URL from your SAML settings.

OR

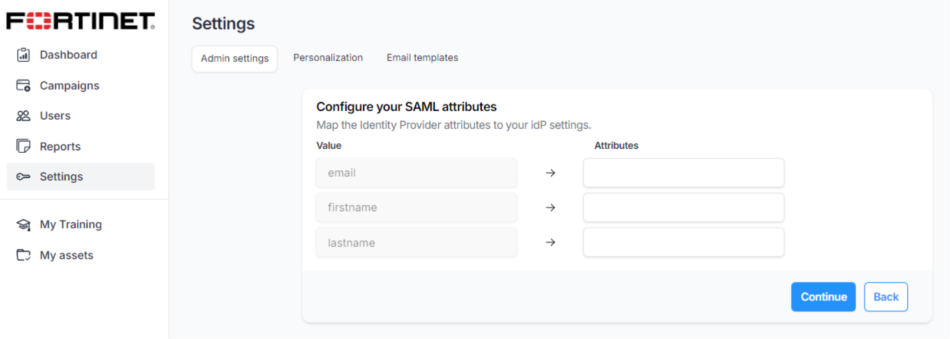
● Add Fortinet as a SAML service provider (SP)
Create a generic SAML application in your identity provider

Copy this ACS URL
[redacted]

Copy this SP Entity ID (service provider metadata)
[redacted]

Download SP metadata

2. In your SSO/SAML2 application configuration, enter the *Assertion Consumer service (ACS) URL* and the *Service Provider metadata (SP Entity ID)* in the appropriate fields.
3. Select *Continue*. The *Configure your SAML attributes* screen is presented.



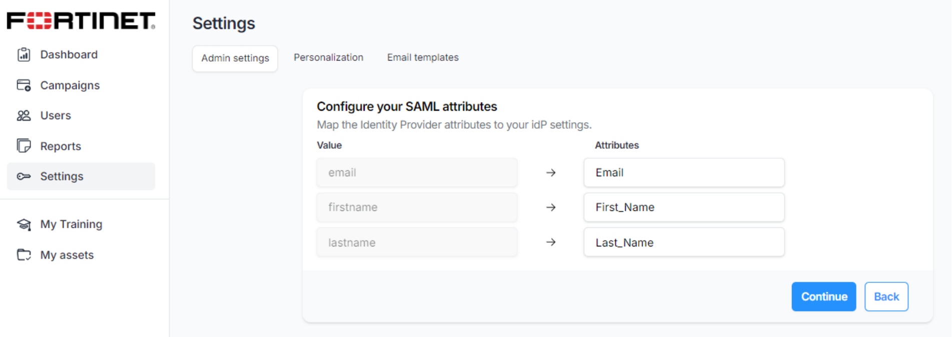
Settings

Admin settings | Personalization | Email templates

Configure your SAML attributes
Map the Identity Provider attributes to your idP settings.

Value		Attributes
email	→	
firstname	→	
lastname	→	

4. Enter the SAML attributes you will configure in the third-party application. You can choose whatever name you desire, however, you must map the same attributes in your SAML application.



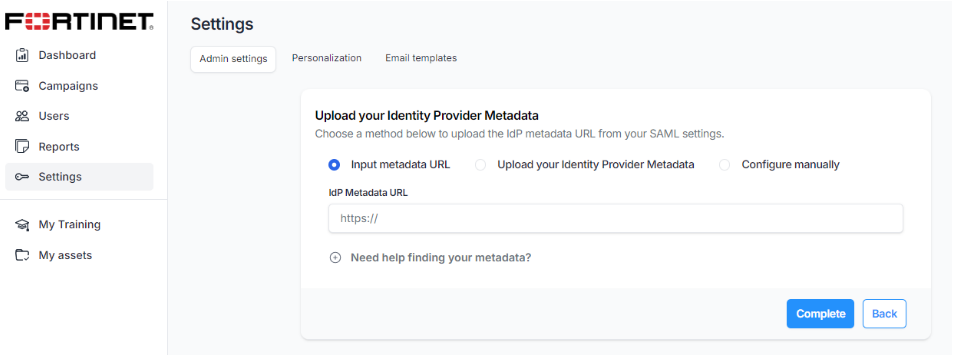
Settings

Admin settings | Personalization | Email templates

Configure your SAML attributes
Map the Identity Provider attributes to your idP settings.

Value		Attributes
email	→	Email
firstname	→	First_Name
lastname	→	Last_Name

5. Select *Continue*. The *Upload your Identity Provider Metadata* page is displayed.



Upload your Identity Provider Metadata

Choose a method below to upload the IdP metadata URL from your SAML settings.

● Input metadata URL ○ Upload your Identity Provider Metadata ○ Configure manually

IdP Metadata URL: https://

Need help finding your metadata?

You can cut and paste the *Input metadata URL* (such as Microsoft), *Upload your Identity Provider Metadata* (such as Google Workspace), or *Configure manually* using the matching values provided by your third-party application configuration.

For Microsoft Entra/Azure/O365 implementations you must replace the IDP Logout URL under the *Configure Manually* tab with: https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0

---

6. Select *Complete*.

You should now test that your custom URL redirects to the configured provider login screen.

Manually create a test user (you cannot use the Tenant Administrator account since it must use the FortiCloud SSO login) and verify that the user can log in through the third-party identity provider.

If you require assistance configuring the Authentication component, send an email to infosec_awareness@fortinet.com. A Deployment Specialist will reach out to request times that work and will schedule a meeting with our team, and, if necessary, the support team from your SSO vendor.

See the following articles for configuration of SSO/SAML2 for Microsoft Azure/Entra and Google Workspace:

- Microsoft:
  - (V3.x) How do I Configure SAML2 Single Sign-on (Authentication) to use Azure AD SSO? : Security Awareness and Training Service
- Google:
  - (V3.x) How do I Configure SAML2 Single Sign-on (Authentication) to use Google Workspace SSO? : Security Awareness and Training Service

Name of User Profile Field	Mapped SAML Attributes	Examples
Name ID Format	N/A	*Google:* Email
Unique User Identifier (Microsoft only)	N/A	*Microsoft:* user.mail
Email	The name of the attribute varies depending on SSO/SAML2 solution (should be mapped to the primary email attribute).	Google: Email or Primary Email *Microsoft:* user.mail

Name of User Profile Field	Mapped SAML Attributes	Examples
First_name	The name of the attribute varies depending on SSO/SAML2 solution (should be mapped to the primary First Name attribute).	*Google:* First Name *Microsoft:* user.givenName
Last_name	The name of the attribute varies depending on SSO/SAML2 solution (should be mapped to the Last Name attribute).	*Google:* Last Name *Microsoft:* user.surname (or sn)

For Google configurations, see How do I Configure SAML2 Single Sign-on (Authentication) to use Google Workspace SSO?

For Microsoft configurations, you will need to first delete the existing entries and create new entries using the table above. You can also refer to your Microsoft documentation (Federated Services / Azure (Entra)).

If you wish to configure access to the service through the user apps (Microsoft and Google), sometimes called the Start URL, see How do I configure Google Workspace so that learners can access the Security Awareness and Training Service from the Google Apps Icon?

You will need to open a ticket in order to get your tenant name. Email infosec_awareness@fortinet.com asking for your tenant name. The URL will be: https://app.training.fortinet.com/local/bridge/launch.php?name=<tenant_name

Ensure that you add the users you wish to access the app through your SSO/SAML2 configuration interface.

If you are getting errors when accessing the link, then your SAML2 configuration on the SSO solution is incorrect.

If you are able to access the log in page for your configured SAML2 SSO solution, but get errors when attempting to log in, then your attributes are likely not configured properly. To troubleshoot this issue, you can use Chrome and the SAML-tracer plug in to verify the correct attributes and attribute values are being passed. See Authentication: SAML2 (SSO) Troubleshooting Guide.

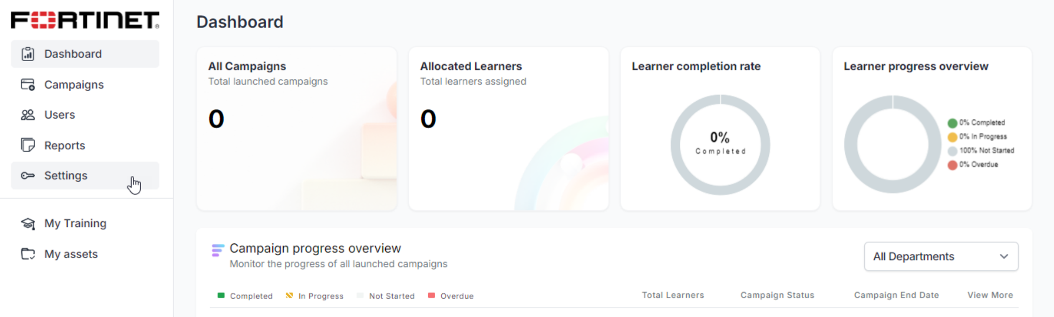
SMTP settings

The SMTP settings allow you to use an email account from your organization to send all emails from the service.

If you do not configure SMTP settings, all emails will be sent from noreply@ftnt.info. In order to ensure these emails are not blocked as spam or sent to the learners spam or junk folder, ensure you allowlist the noreply@ftnt.info email address.

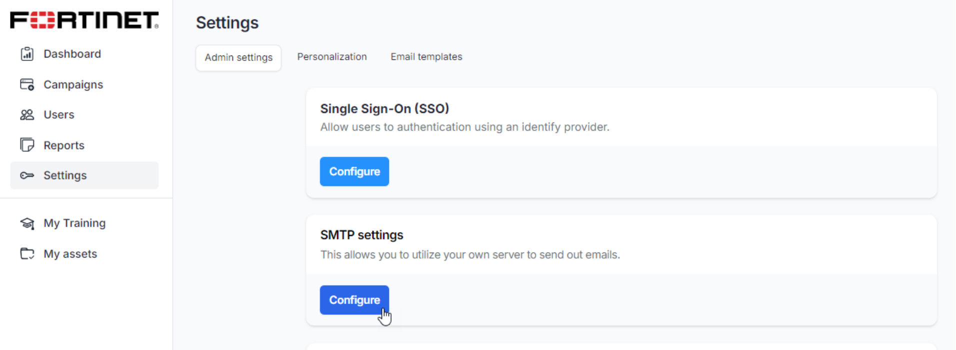
To configure SMTP settings:

1. Select *Settings* from the navigation menu:

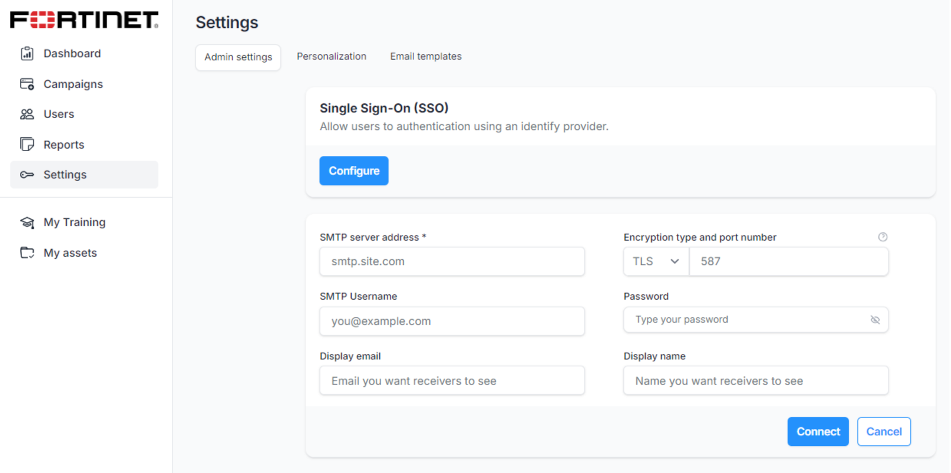


The *Settings* page is displayed.

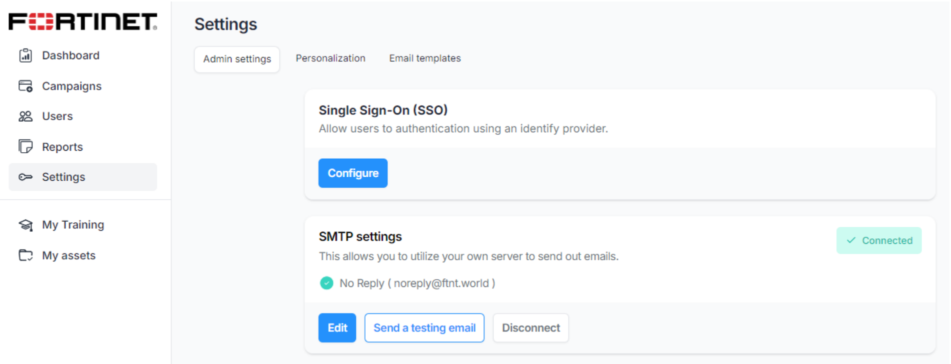
2. Click *Configure* in the *SMTP settings* section.



The SMTP settings page is displayed.



3. Complete the form and click *Connect*.
   If the settings are correct, you should see a green *Connected* status.



Single Sign-On (SSO)
Allow users to authentication using an identify provider.

SMTP settings
This allows you to utilize your own server to send out emails.
No Reply (noreply@ftnt.world)

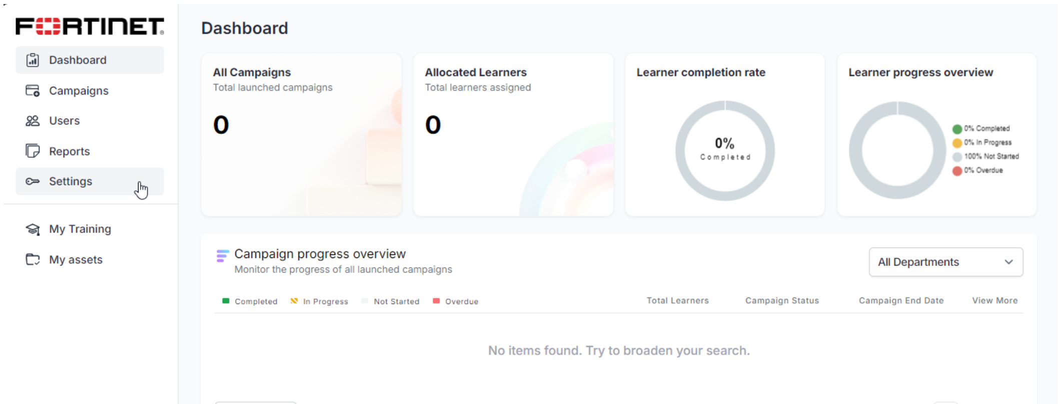
4. To verify the settings, click *Send a testing email*. You should see a *Test email has been sent* confirmation and verify the email is received.

Assets Access

This setting grants all users access to the available assets in the learner experience.

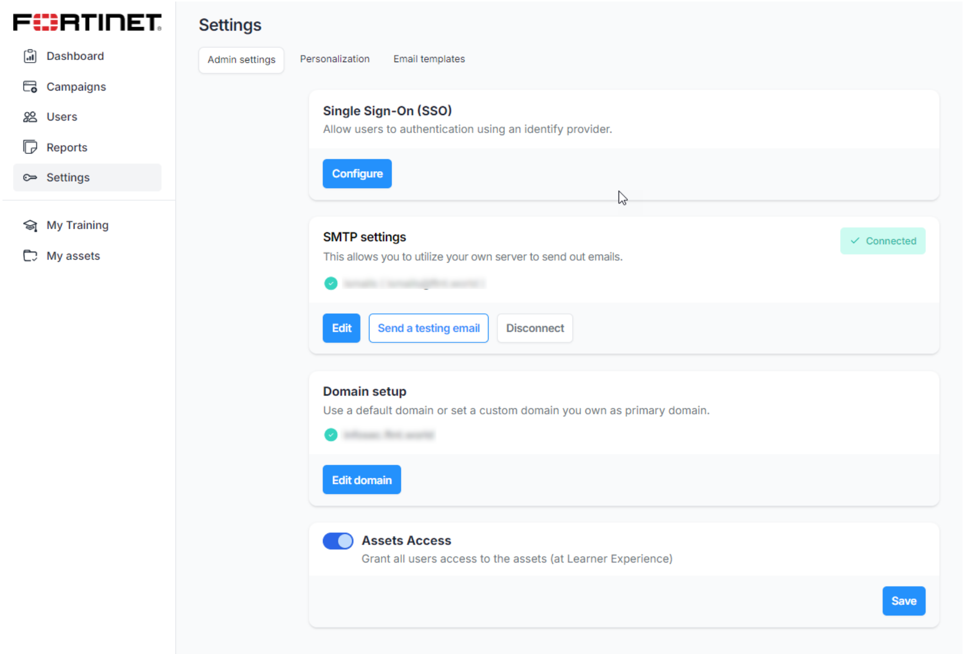
To grant access to assets:

1. Select *Settings* from the navigation menu.



No items found. Try to broaden your search.

The *Settings* page is displayed.



Settings

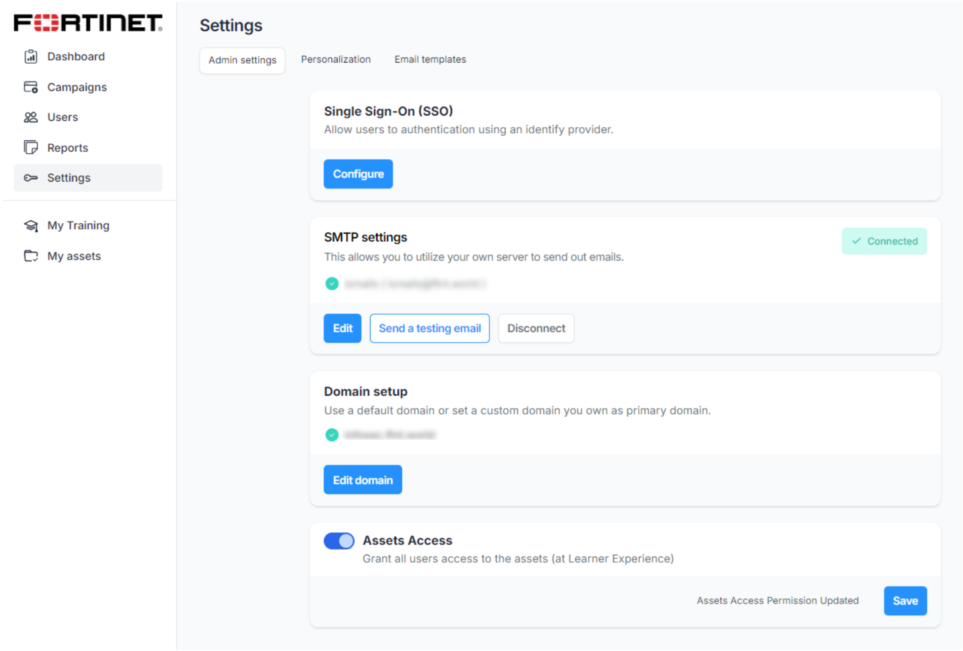
Single Sign-On (SSO)
Allow users to authentication using an identify provider.

SMTP settings
This allows you to utilize your own server to send out emails.
[redacted]

Domain setup
Use a default domain or set a custom domain you own as primary domain.
[redacted]

Assets Access
Grant all users access to the assets (at Learner Experience)

2. Enable the *Assets Access* toggle, then click *Save*.
   An assets access permission updated message is displayed.



Settings

Single Sign-On (SSO)
Allow users to authentication using an identify provider.

SMTP settings
This allows you to utilize your own server to send out emails.
[redacted]

Domain setup
Use a default domain or set a custom domain you own as primary domain.
[redacted]

Assets Access
Grant all users access to the assets (at Learner Experience)

Assets Access Permission Updated

Refer to My Assets on page 84 to learn more about *My assets* content.

Personalization

Default language for learners

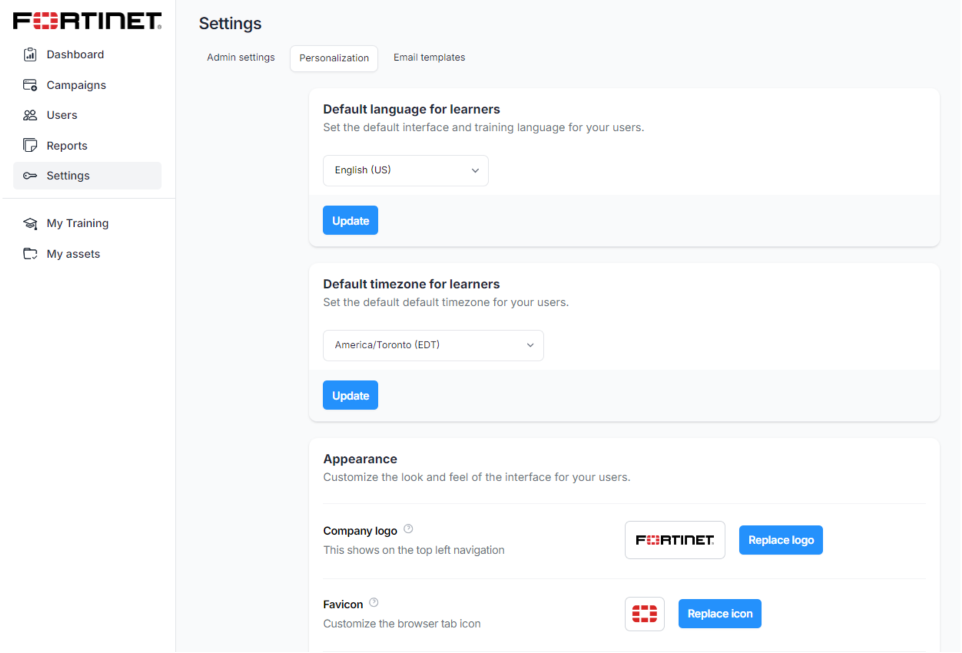
These features are only available for premium service level licenses: Free 25 user Premium (for Partners only) and Premium (purchased by customer). It is not available for free and standard service level licenses.

Administrators can set a default language for learners that are added to the system. This setting applies to the Learner interface as well as the training module content.

Learners can change this setting after they log in if they prefer to take the training in a different language.

To change the default language for learners:

1. Select *Settings* from the navigation menu.
2. Select the *Personalization* tab. The *Personalization* page is displayed.



Settings

Default language for learners
Set the default interface and training language for your users.
English (US)

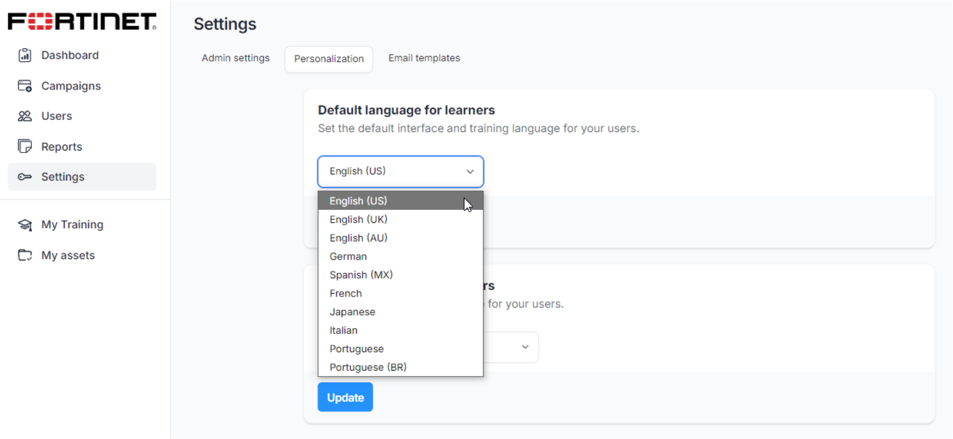
Default timezone for learners
Set the default default timezone for your users.
America/Toronto (EDT)

Appearance
Customize the look and feel of the interface for your users.

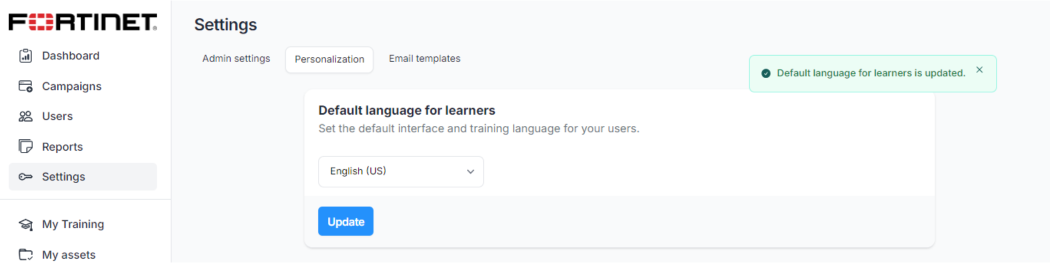
Company logo
This shows on the top left navigation

Favicon
Customize the browser tab icon

3. Set the desired default language for learners by selecting the language drop down in the *Default language for learners* section.



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



Default language for learners is updated.

Default language for learners

Set the default interface and training language for your users.

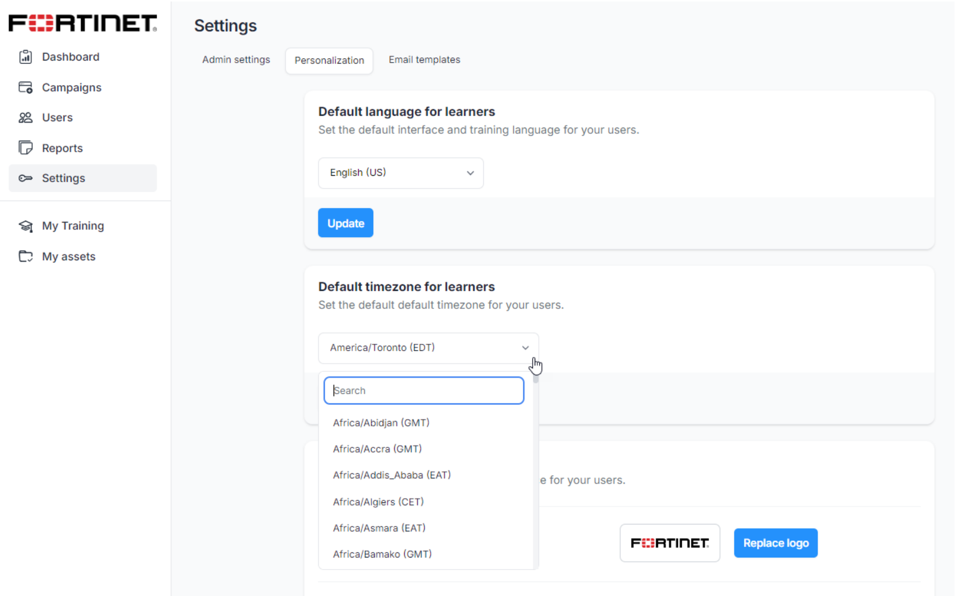
English (US)

Default time zone for learners

These features are only available for premium service level licenses: Free 25 user Premium (for Partners only) and Premium (purchased by customer). It is not available for free and standard service level licenses.

To define the time zone:

1. Select *Settings* from the navigation menu.
2. Select the *Personalization* tab.
3. Set the desired default time zone for learners by searching and selecting the language drop down in the *Default time zone for learners* section.



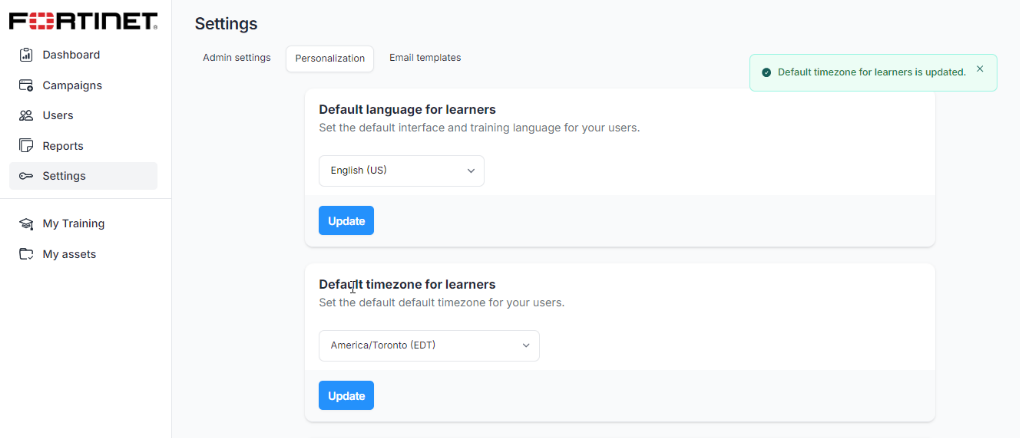
Default language for learners
Set the default interface and training language for your users.
English (US)
Update

Default timezone for learners
Set the default default timezone for your users.
America/Toronto (EDT)
Search
Africa/Abidjan (GMT)
Africa/Accra (GMT)
Africa/Addis_Ababa (EAT)
Africa/Algiers (CET)
Africa/Asmara (EAT)
Africa/Bamako (GMT)

e for your users.

4.

5. Click *Update* to commit the changes. A confirmation message is displayed.



Default timezone for learners is updated.

Default language for learners
Set the default interface and training language for your users.
English (US)
Update

Default timezone for learners
Set the default default timezone for your users.
America/Toronto (EDT)
Update

Appearance

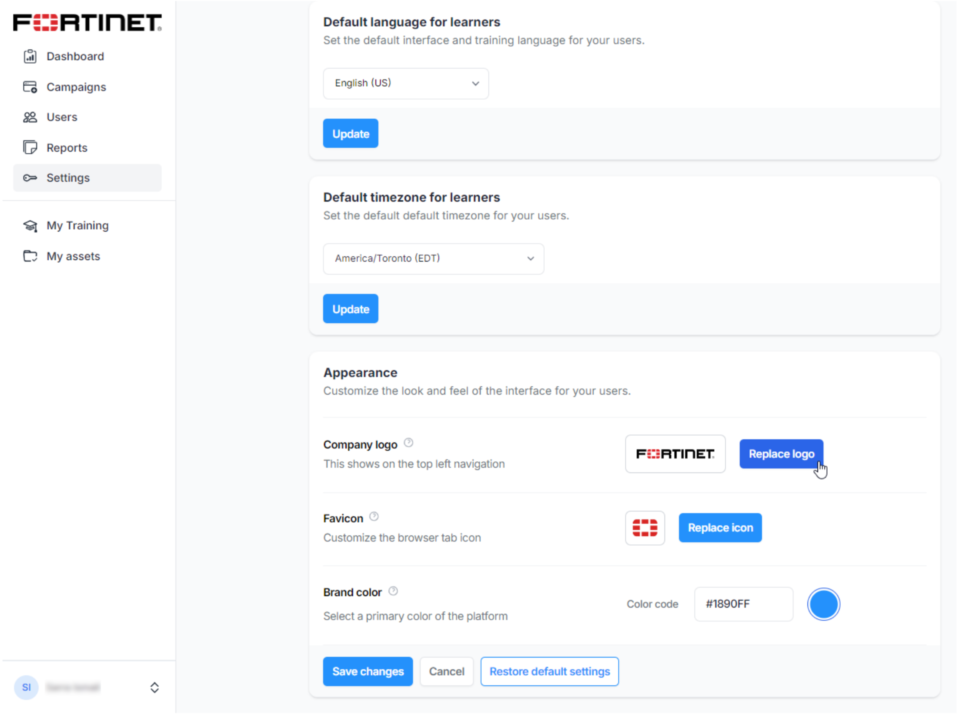
These features are only available for premium service level licenses: Free 25 user Premium (for Partners only) and Premium (purchased by customer). It is not available for free and standard service level licenses.

Changing the Company logo

The company logo is displayed in the upper left hand corner of the learner experience and the admin interface. It is also the logo that will be used on the certificates of completion.

To change the company logo:

1. Select *Settings* from the navigation menu.
2. Select the *Personalization* tab.
3. Scroll down to the *Appearance* section and click *Replace logo*.



[redacted]

Default language for learners
Set the default interface and training language for your users.
English (US)

Default timezone for learners
Set the default default timezone for your users.
America/Toronto (EDT)

Appearance
Customize the look and feel of the interface for your users.

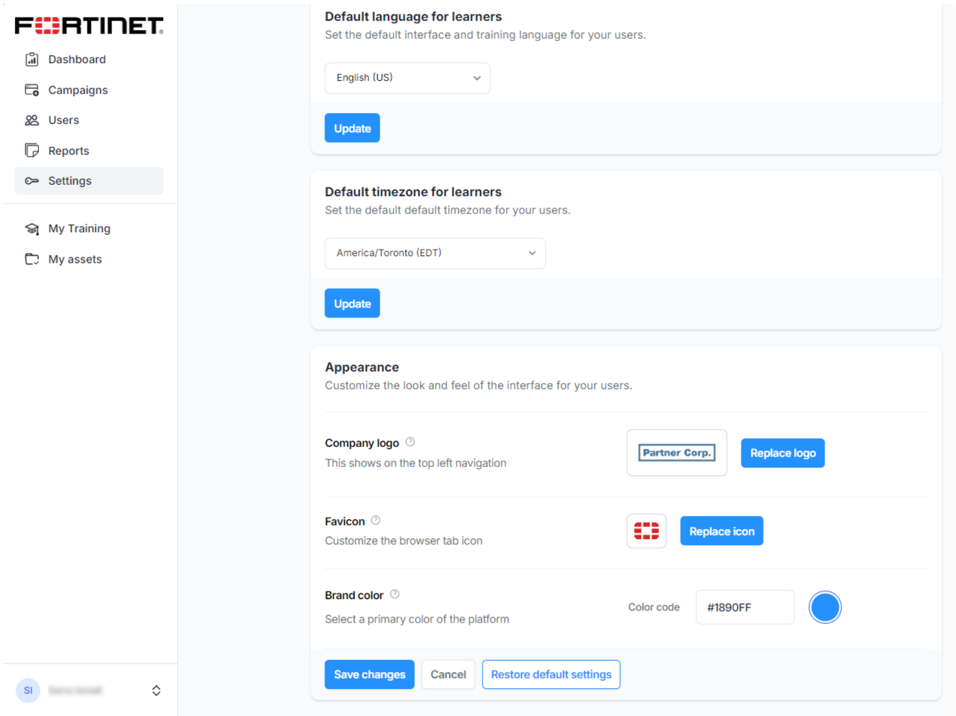
Company logo
This shows on the top left navigation

Favicon
Customize the browser tab icon

Brand color
Select a primary color of the platform
Color code #1890FF

A Windows Open file dialogue will appear for you to select your logo file.

4. Browse and select the file you would like to use as your logo.
   The new logo appears in the *Company logo* window.



Default language for learners
Set the default interface and training language for your users.

English (US)

Default timezone for learners
Set the default default timezone for your users.

America/Toronto (EDT)

Appearance
Customize the look and feel of the interface for your users.

Company logo
This shows on the top left navigation

Favicon
Customize the browser tab icon

Brand color
Select a primary color of the platform

Color code: #1890FF

[redacted]

5. Select *Save changes*.

Changing the Favicon (favorite icon)

The favicon dictates the icon that will be presented in each of the Fortinet Security Awareness and Training Service browser tabs.

To change the favicon:

1. Select *Settings* from the navigation menu.
2. Select the *Personalization* tab.
3. Scroll down to the *Appearance* section and click *Replace icon*.
4. Browse and select the file you would like to use as your favicon.
5. Select *Save changes*.

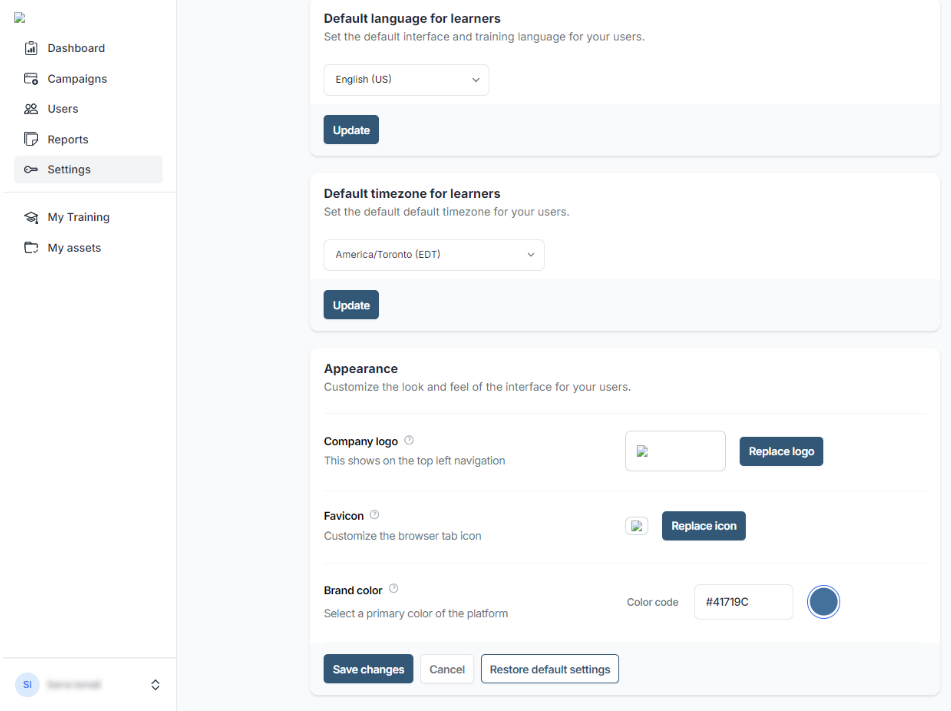
Changing the Brand color

The brand color is used to match the button color throughout the service to a color of your choice. Typically, customers use one of the hex codes from their logo. These can be obtained by using an eyedropper application, or, by getting the official color hex codes from your marketing department.

To change the color:

1. Select *Settings* from the navigation menu.
2. Select the *Personalization* tab.

3. Enter the desired color hex code in the *Color code* field in the *Brand color* section.



Default language for learners
Set the default interface and training language for your users.

English (US)

Update

Default timezone for learners
Set the default default timezone for your users.

America/Toronto (EDT)

Update

Appearance
Customize the look and feel of the interface for your users.

Company logo
This shows on the top left navigation

Replace logo

Favicon
Customize the browser tab icon

Replace icon

Brand color
Select a primary color of the platform

Color code: #41719C

Save changes | Cancel | Restore default settings

4. Select *Save changes*.

If you wish to reset the color and branding to default, select the *Restore default settings* button.

Email templates

These features are only available for premium service level licenses: Free 25 user Premium (for Partners only) and Premium (purchased by customer). It is not available for free and standard service level licenses.

The email templates section allows you to choose default subject, body and action button text. The system provides variables for each email template. These can be used to refer information in the system (such as campaign name, campaign due date, and so on). These email templates are used by the campaign. You do have the option to turn off any of these emails. This allows you to send the email of your choice from your native email client instead of the using the service email templates. There is also a preview button you can use to see the default content that will be sent should you choose not to customize the templates.

Notification Type	Description	Time frame
First-time login email notification	Enable or disable email notifications for users logging in for the first time.	There are two options to choose from: • When user is added to the system

Notification Type	Description	Time frame
		• When user is assigned the first training
Training enrollment confirmation email	This email notifies users of their enrollment.	Sent when the training campaign starts, including late enrollees.
Reminder before due date	This email notifies users who have incomplete campaign assignments.	Sent on the due date.
Campaign completion	This email notifies a user when they have completed their campaign assignments. There is a link in the email that allows learners to download a copy of their certificate of completion.	Sent upon user completion of the training.
Scheduled Reports	This email informs recipients that a specific report is now available and accessible.	Sent according to the report schedule.

Each email template contains a list of available placeholders you can insert in that template when accessing campaign information to include in the template.

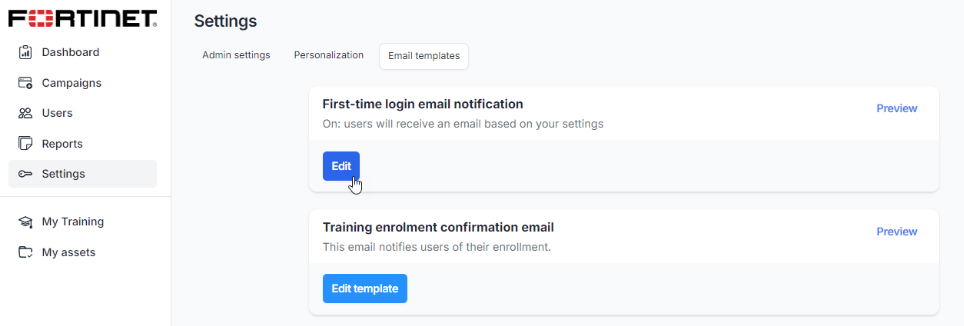
You can only use the placeholders listed under the body in the template you are modifying. You cannot copy placeholders from one template and use them in another template.

Customizing the First-time login email notification template

Sending this notification is optional. For customers using their own single-sign on (SSO) authentication application, this step is not required since they already have an existing username and password to authenticate with.

To customize the first-time login email template:

1. Select *Settings* from the navigation menu.
2. Select the *Email templates* tab.
3. In the *First-time login email notification* section, select *Edit*.



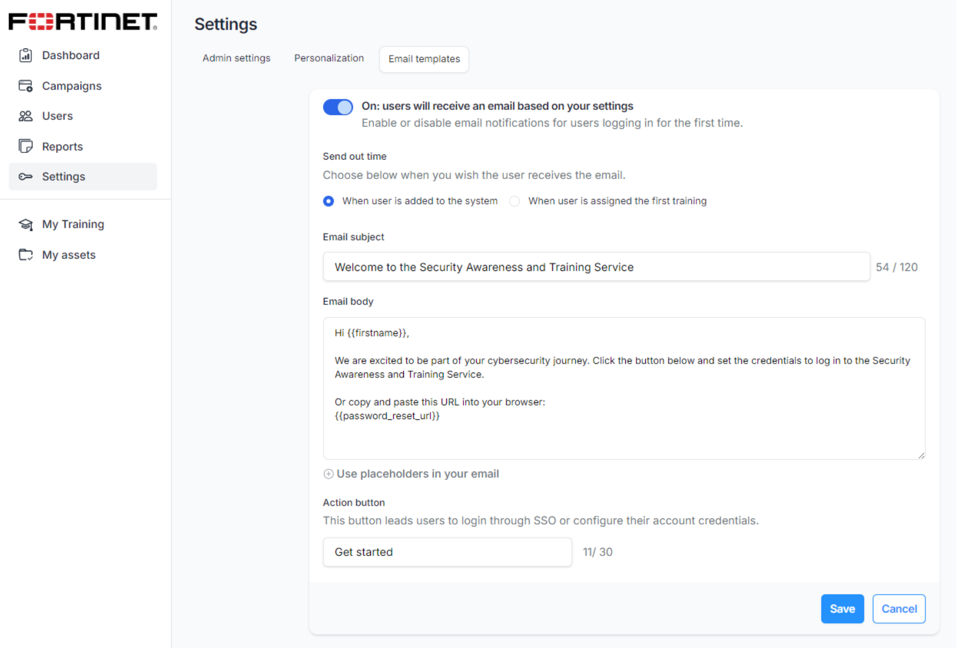
First-time login email notification

On: users will receive an email based on your settings

Training enrolment confirmation email

This email notifies users of their enrollment.

4. Enable the notification. The configuration page is displayed.



On: users will receive an email based on your settings
Enable or disable email notifications for users logging in for the first time.

Send out time
Choose below when you wish the user receives the email.
● When user is added to the system ○ When user is assigned the first training

Email subject
Welcome to the Security Awareness and Training Service 54 / 120

Email body
Hi {{firstname}},

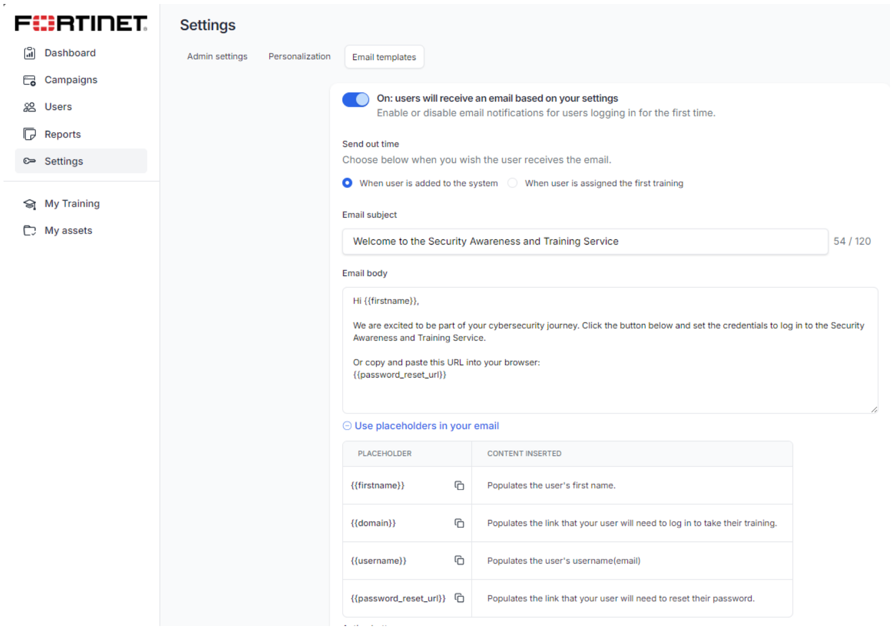
We are excited to be part of your cybersecurity journey. Click the button below and set the credentials to log in to the Security Awareness and Training Service.

Or copy and paste this URL into your browser:
{{password_reset_url}}

⊕ Use placeholders in your email

Action button
This button leads users to login through SSO or configure their account credentials.
Get started 11/ 30

5. From the *Send out time* section, select the option button to either send the email *When the user is added to the system* or *When the user is assigned the first training*.
6. Customize the *Email subject* field if you wish to include a different email subject.
7. Customize the content of the *Email body* as desired. You may wish to include a support number and email, additional information on why the training is being assigned and so on You an also use any of the provided placeholders in the email body. To view the placeholder values, click *+ Use placeholders in your email* below the body to expand the list of available placeholders.



On: users will receive an email based on your settings
Enable or disable email notifications for users logging in for the first time.

Send out time
Choose below when you wish the user receives the email.
● When user is added to the system ○ When user is assigned the first training

Email subject
Welcome to the Security Awareness and Training Service 54 / 120

Email body
Hi {{firstname}},

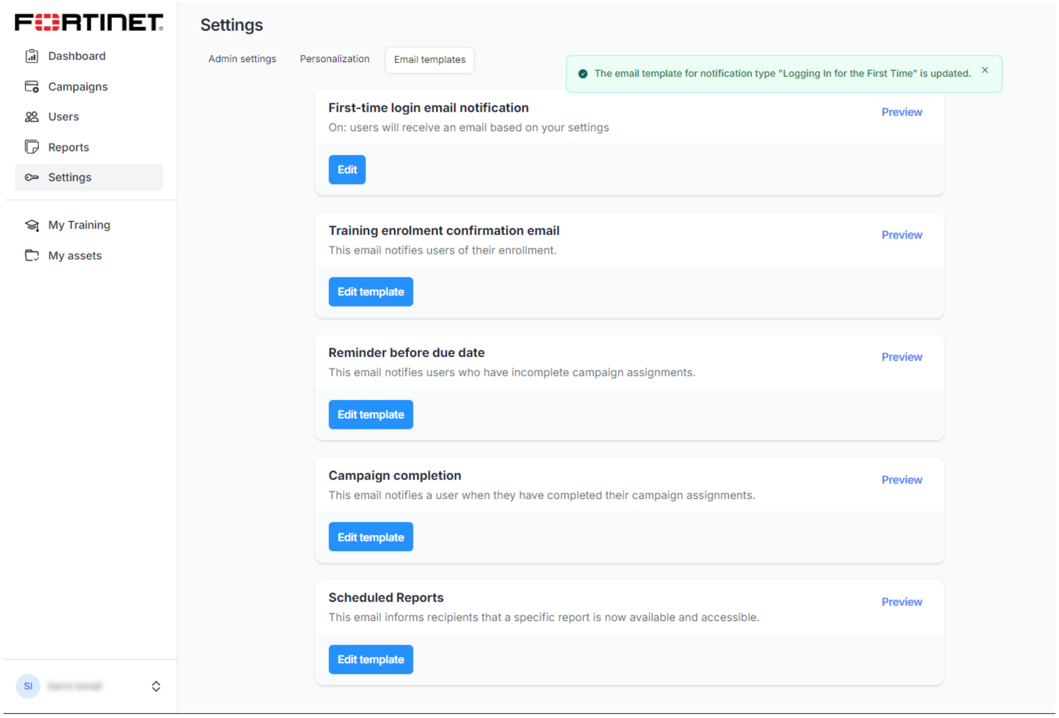
We are excited to be part of your cybersecurity journey. Click the button below and set the credentials to log in to the Security Awareness and Training Service.

Or copy and paste this URL into your browser:
{{password_reset_url}}

⊖ Use placeholders in your email

PLACEHOLDER	CONTENT INSERTED
{{firstname}}	Populates the user's first name.
{{domain}}	Populates the link that your user will need to log in to take their training.
{{username}}	Populates the user's username(email)
{{password_reset_url}}	Populates the link that your user will need to reset their password.

8. Customize the *Action button* text as desired. This is the text that will appear on the button within the email that redirects the learner to set their initial password.
9. Click *Save*. A confirmation message is displayed.



The email template for notification type "Logging In for the First Time" is updated.

First-time login email notification
On: users will receive an email based on your settings

Training enrolment confirmation email
This email notifies users of their enrollment.

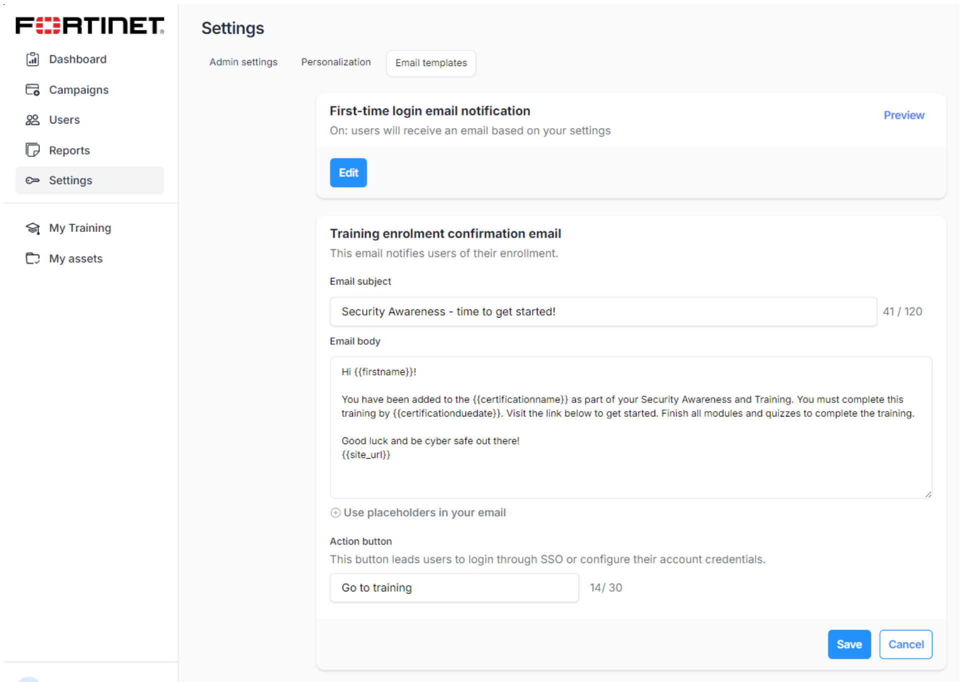
Reminder before due date
This email notifies users who have incomplete campaign assignments.

Campaign completion
This email notifies a user when they have completed their campaign assignments.

Scheduled Reports
This email informs recipients that a specific report is now available and accessible.

To customize the training enrollment confirmation email template:

1. Select *Settings* from the navigation menu.
2. Select the *Email templates* tab.
3. In the *Training enrollment confirmation email* section, select *Edit template*. The *Training enrollment confirmation email* settings are displayed.



First-time login email notification
On: users will receive an email based on your settings

Training enrolment confirmation email
This email notifies users of their enrollment.

Email subject: Security Awareness - time to get started! 41 / 120

Email body:

Hi {{firstname}}!

You have been added to the {{certificationname}} as part of your Security Awareness and Training. You must complete this training by {{certificationduedate}}. Visit the link below to get started. Finish all modules and quizzes to complete the training.

Good luck and be cyber safe out there!
{{site_url}}

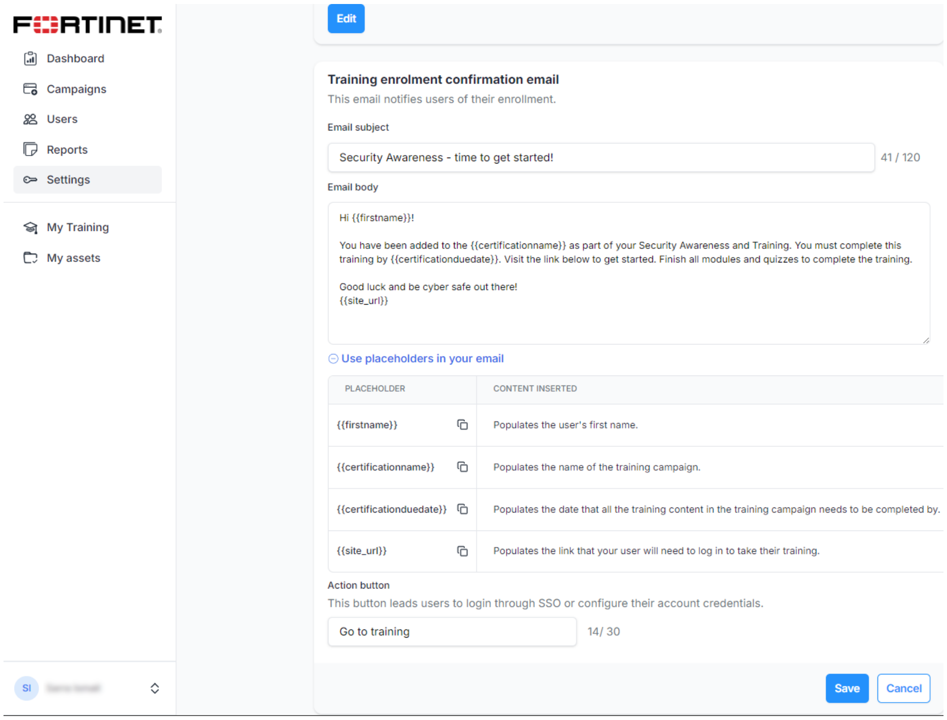
Use placeholders in your email

Action button
This button leads users to login through SSO or configure their account credentials.

Go to training 14/ 30

4. Customize the *Email subject* field if you wish to include a different email subject.

5. Customize the content of the *Email body* as desired. You may wish to include a support number and email, additional information on why the training is being assigned and so on You an also use any of the provided placeholders in the email body. To view the placeholder values, click *+ Use placeholders in your email* below the body to expand the list of available placeholders.



Training enrolment confirmation email

This email notifies users of their enrollment.

Email subject

Security Awareness - time to get started! 41 / 120

Email body

Hi {{firstname}}!

You have been added to the {{certificationname}} as part of your Security Awareness and Training. You must complete this training by {{certificationduedate}}. Visit the link below to get started. Finish all modules and quizzes to complete the training.

Good luck and be cyber safe out there!
{{site_url}}

⊖ Use placeholders in your email

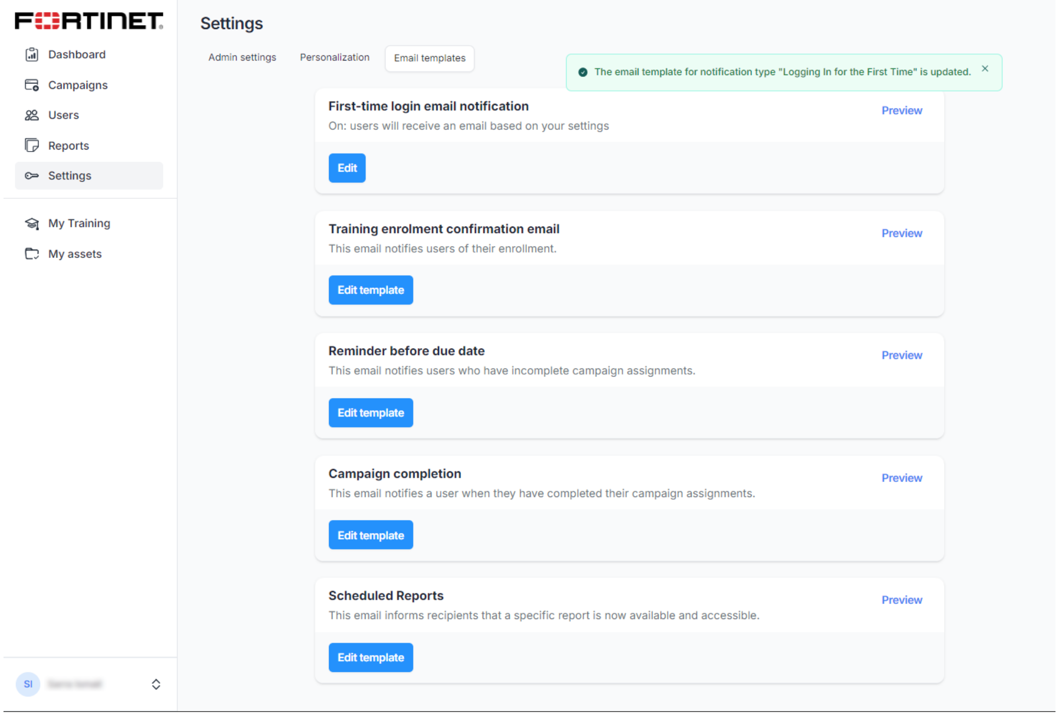
PLACEHOLDER	CONTENT INSERTED
{{firstname}}	Populates the user's first name.
{{certificationname}}	Populates the name of the training campaign.
{{certificationduedate}}	Populates the date that all the training content in the training campaign needs to be completed by.
{{site_url}}	Populates the link that your user will need to log in to take their training.

Action button

This button leads users to login through SSO or configure their account credentials.

Go to training 14/ 30

6. Customize the *Action button* text as desired. This is the text that will appear on the button within the email that redirects the learner to set their initial password.
7. Click *Save*. A confirmation message is displayed.



✓ The email template for notification type "Logging In for the First Time" is updated. ×

First-time login email notification

On: users will receive an email based on your settings

Training enrolment confirmation email

This email notifies users of their enrollment.

Reminder before due date

This email notifies users who have incomplete campaign assignments.

Campaign completion

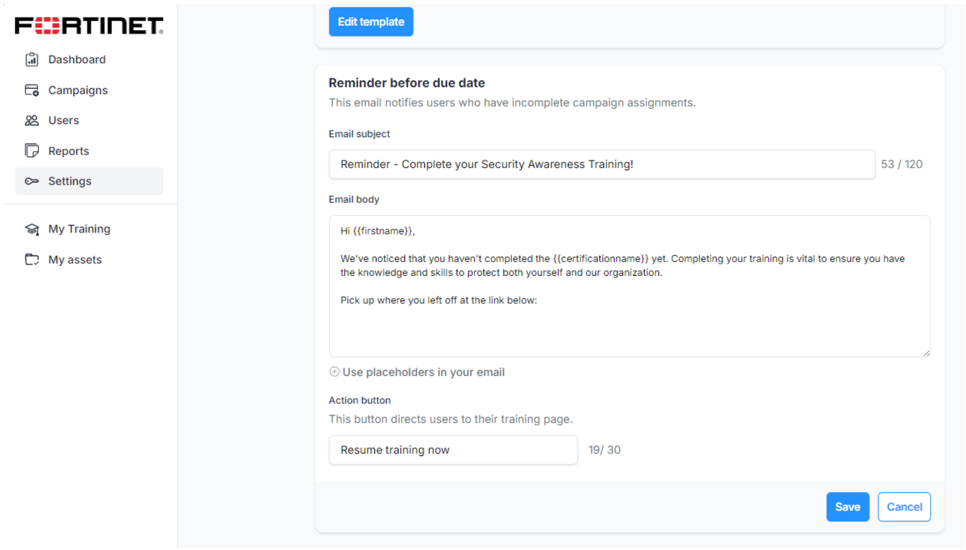
This email notifies a user when they have completed their campaign assignments.

Scheduled Reports

This email informs recipients that a specific report is now available and accessible.

To customize the reminder before due date email template:

1. Select *Settings* from the navigation menu.
2. Select the *Email templates* tab.
3. In the *Reminder before due date* section, click *Edit template*. The *Reminder before due date* settings page is displayed.



Reminder before due date

This email notifies users who have incomplete campaign assignments.

Email subject

Reminder - Complete your Security Awareness Training! 53 / 120

Email body

Hi {{firstname}},

We've noticed that you haven't completed the {{certificationname}} yet. Completing your training is vital to ensure you have the knowledge and skills to protect both yourself and our organization.

Pick up where you left off at the link below:

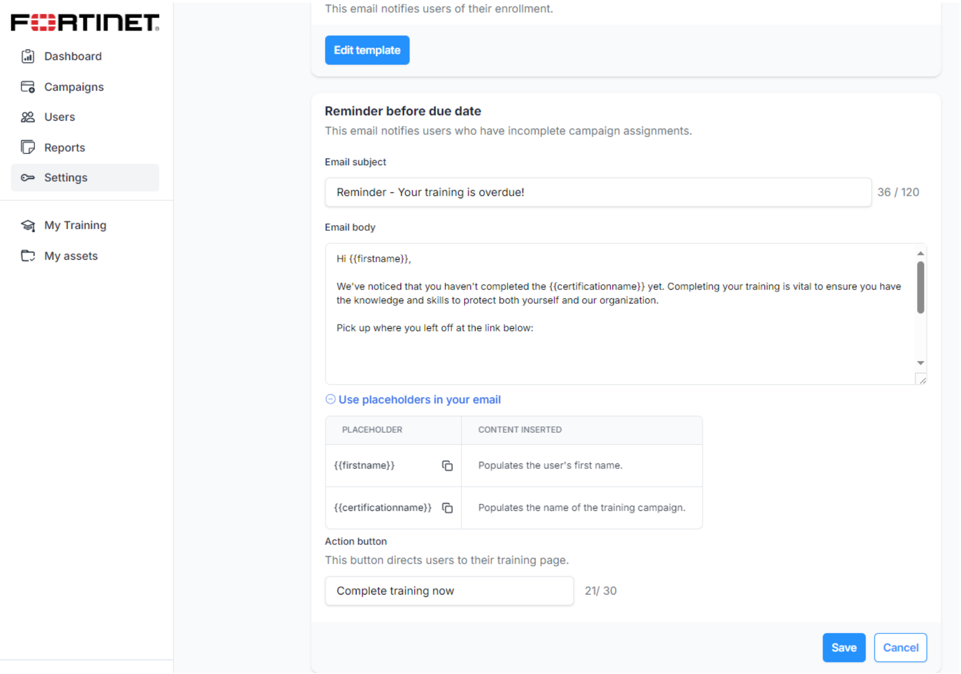
⊕ Use placeholders in your email

Action button

This button directs users to their training page.

Resume training now 19/ 30

4. Customize the *Email subject* field if you wish to include a different email subject.
5. Customize the content of the *Email body* as desired. You may wish to include a support number and email, additional information on why the training is being assigned and so on You an also use any of the provided placeholders in the email body. To view the placeholder values, click *+ Use placeholders in your email* below the body to expand the list of available placeholders.



This email notifies users of their enrollment.

Reminder before due date

This email notifies users who have incomplete campaign assignments.

Email subject

Reminder - Your training is overdue! 36 / 120

Email body

Hi {{firstname}},

We've noticed that you haven't completed the {{certificationname}} yet. Completing your training is vital to ensure you have the knowledge and skills to protect both yourself and our organization.

Pick up where you left off at the link below:

⊖ Use placeholders in your email

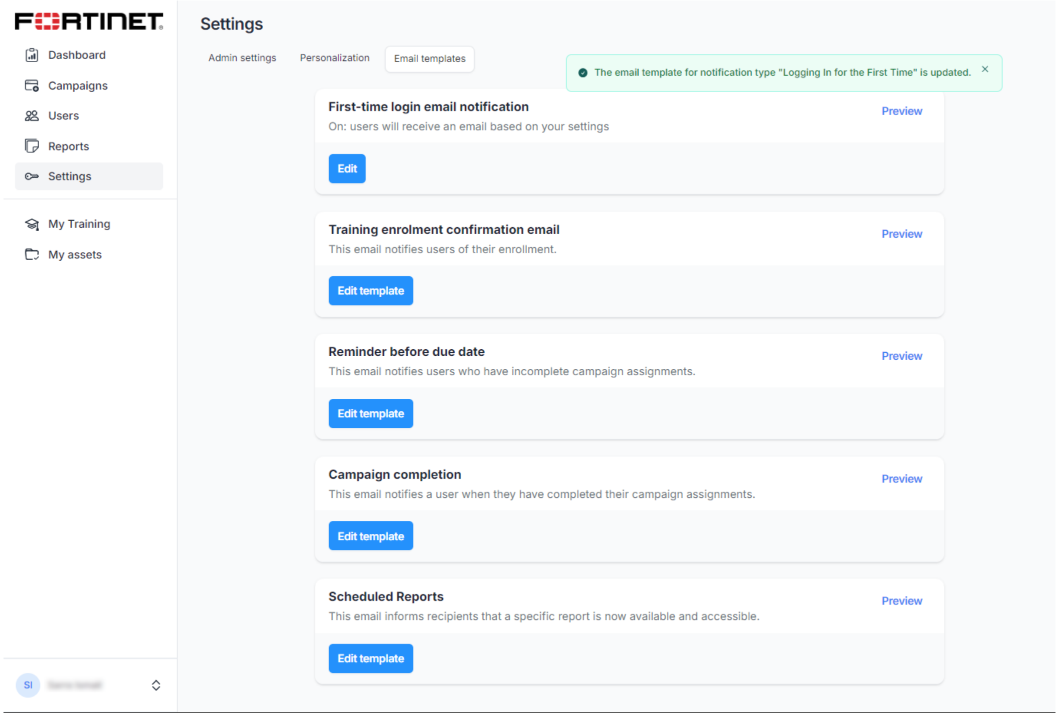
PLACEHOLDER	CONTENT INSERTED
{{firstname}}	Populates the user's first name.
{{certificationname}}	Populates the name of the training campaign.

Action button

This button directs users to their training page.

Complete training now 21/ 30

6. Customize the *Action button* text as desired. This is the text that will appear on the button within the email that redirects the learner to set their initial password.
7. Click *Save*. A confirmation message is displayed.



The email template for notification type "Logging In for the First Time" is updated.

First-time login email notification
On: users will receive an email based on your settings

Training enrolment confirmation email
This email notifies users of their enrollment.

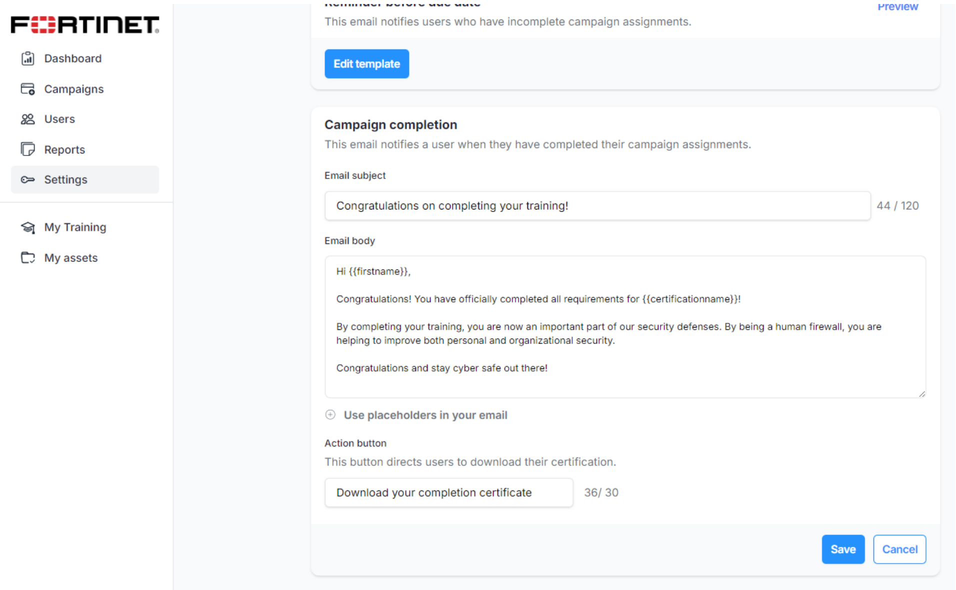
Reminder before due date
This email notifies users who have incomplete campaign assignments.

Campaign completion
This email notifies a user when they have completed their campaign assignments.

Scheduled Reports
This email informs recipients that a specific report is now available and accessible.

To customize the campaign completion email template:

1. Select *Settings* from the navigation menu:
2. Select the *Email templates* tab.
3. In the *Campaign completion* section, select *Edit Template*. The *Campaign Completion* email template settings page is displayed.



This email notifies users who have incomplete campaign assignments.

Campaign completion
This email notifies a user when they have completed their campaign assignments.

Email subject: Congratulations on completing your training! 44 / 120

Email body:

Hi {{firstname}},

Congratulations! You have officially completed all requirements for {{certificationname}}!

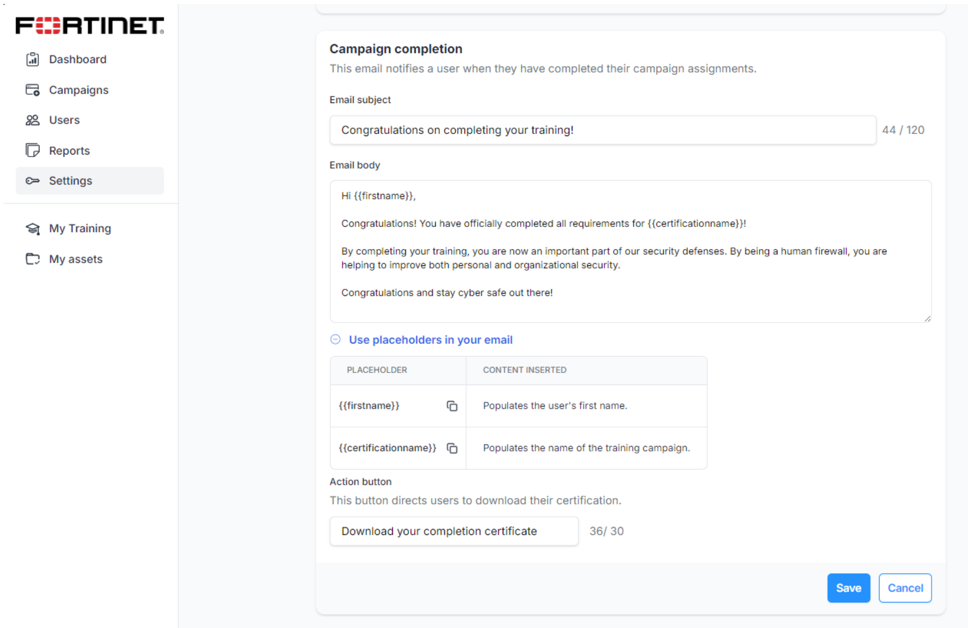
By completing your training, you are now an important part of our security defenses. By being a human firewall, you are helping to improve both personal and organizational security.

Congratulations and stay cyber safe out there!

Action button
This button directs users to download their certification.

Download your completion certificate 36/ 30

4. Customize the *Email subject* field if you wish to include a different email subject.
5. Customize the content of the *Email body* as desired. You may wish to include a support number and email. You an also use any of the provided placeholders in the email body. To view the placeholder values, click *+ Use placeholders in your email* below the body to expand the list of available placeholders.



Campaign completion

This email notifies a user when they have completed their campaign assignments.

Email subject

Congratulations on completing your training! 44 / 120

Email body

Hi {{firstname}},

Congratulations! You have officially completed all requirements for {{certificationname}}!

By completing your training, you are now an important part of our security defenses. By being a human firewall, you are helping to improve both personal and organizational security.

Congratulations and stay cyber safe out there!

⊖ Use placeholders in your email

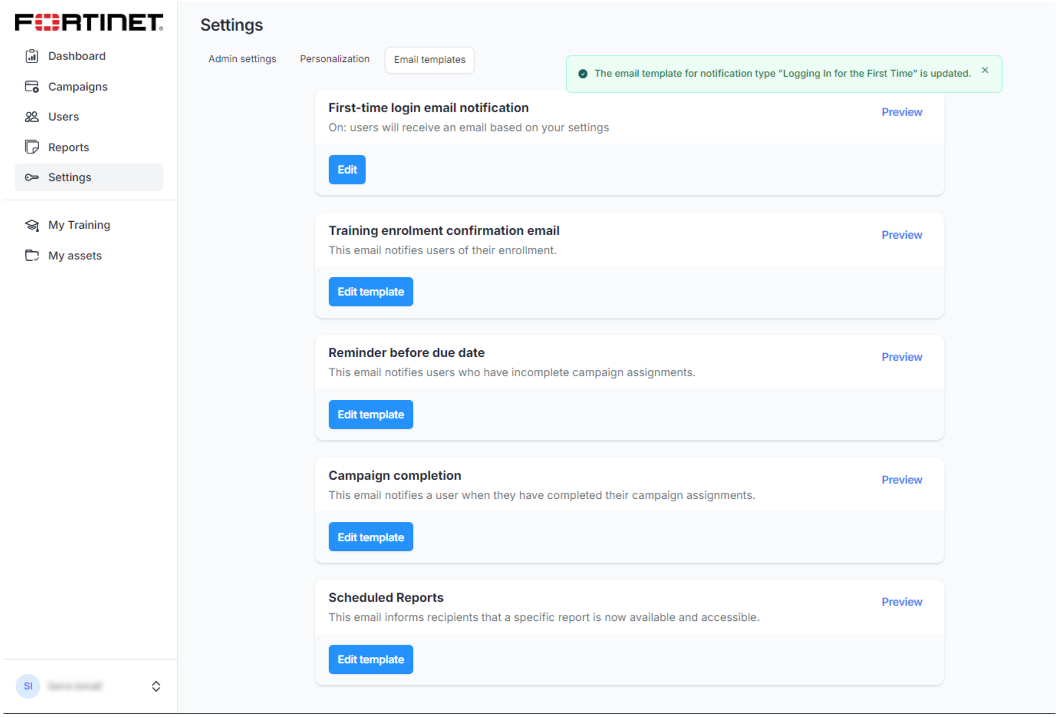
PLACEHOLDER	CONTENT INSERTED
{{firstname}}	Populates the user's first name.
{{certificationname}}	Populates the name of the training campaign.

Action button

This button directs users to download their certification.

Download your completion certificate 36/ 30

6. Customize the *Action button* text as desired. This is the text that will appear on the button within the email that redirects the learner to set their initial password.
7. Click *Save*. A confirmation message is displayed.



[redacted]

Settings

The email template for notification type "Logging In for the First Time" is updated. ×

First-time login email notification Preview

On: users will receive an email based on your settings

Training enrolment confirmation email Preview

This email notifies users of their enrollment.

Reminder before due date Preview

This email notifies users who have incomplete campaign assignments.

Campaign completion Preview

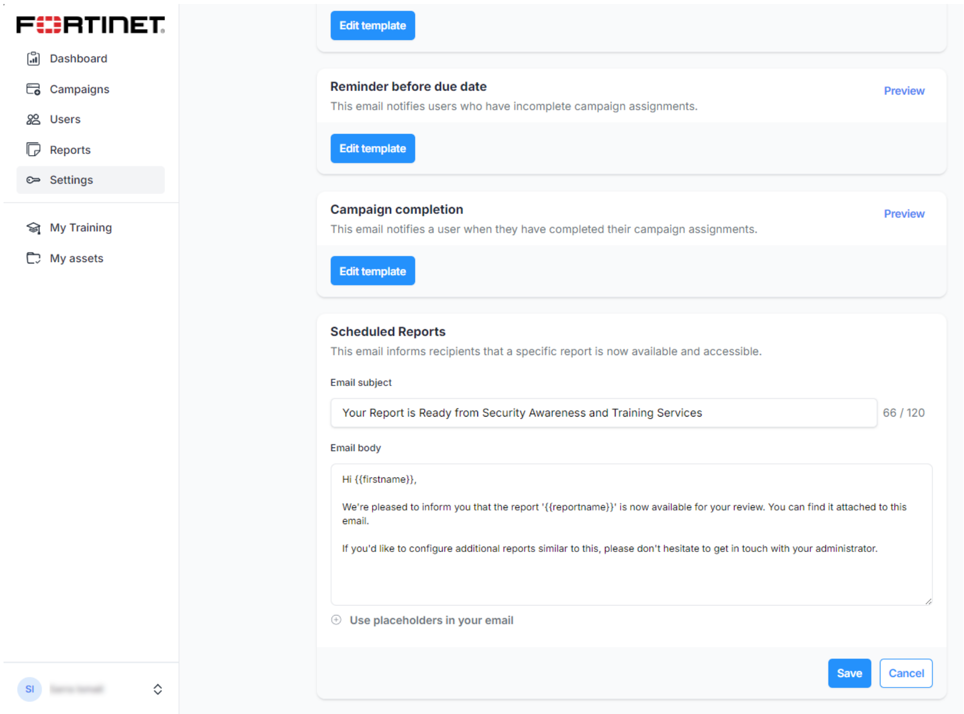
This email notifies a user when they have completed their campaign assignments.

Scheduled Reports Preview

This email informs recipients that a specific report is now available and accessible.

To customize the Scheduled Reports Email Template:

1. Select *Settings* from the navigation menu.
2. Select the *Email templates* tab.
3. In the *Scheduled Reports* section, select *Edit template*. The *Scheduled Reports* email template settings page is displayed.



Reminder before due date

This email notifies users who have incomplete campaign assignments.

Campaign completion

This email notifies a user when they have completed their campaign assignments.

Scheduled Reports

This email informs recipients that a specific report is now available and accessible.

Email subject

Your Report is Ready from Security Awareness and Training Services 66 / 120

Email body

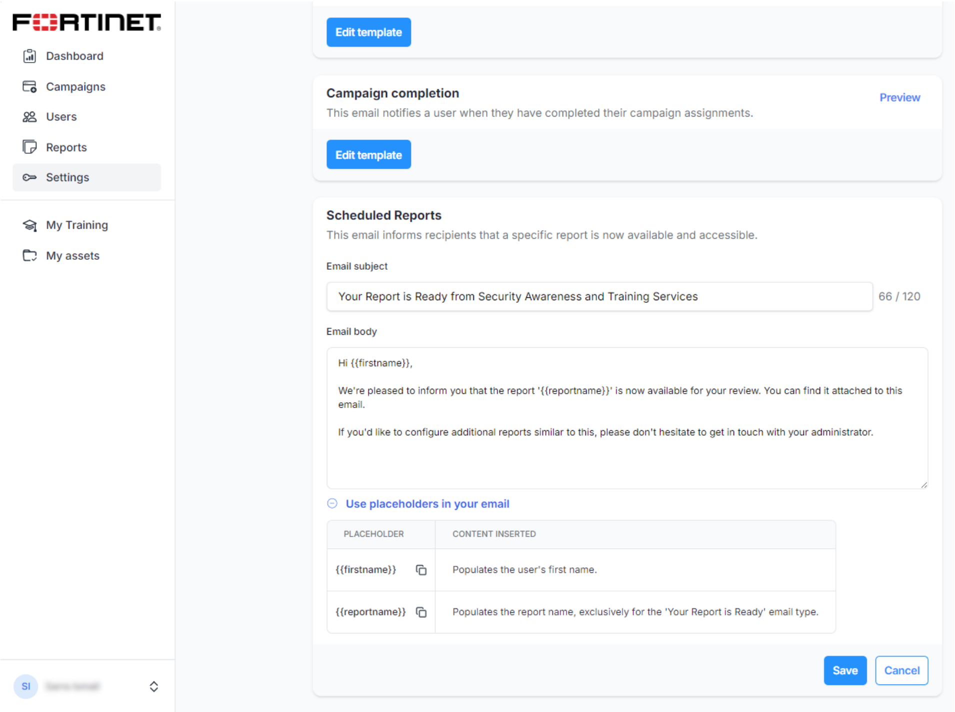
Hi {{firstname}},

We're pleased to inform you that the report '{{reportname}}' is now available for your review. You can find it attached to this email.

If you'd like to configure additional reports similar to this, please don't hesitate to get in touch with your administrator.

⊕ Use placeholders in your email

4. Customize the *Email subject* field if you wish to include a different email subject.
5. Customize the content of the *Email body* as desired. You may wish to include a support number and email. You an also use any of the provided placeholders in the email body. To view the placeholder values, click *+ Use placeholders in your email* below the body to expand the list of available placeholders.



Campaign completion

This email notifies a user when they have completed their campaign assignments.

Scheduled Reports

This email informs recipients that a specific report is now available and accessible.

Email subject

Your Report is Ready from Security Awareness and Training Services 66 / 120

Email body

Hi {{firstname}},

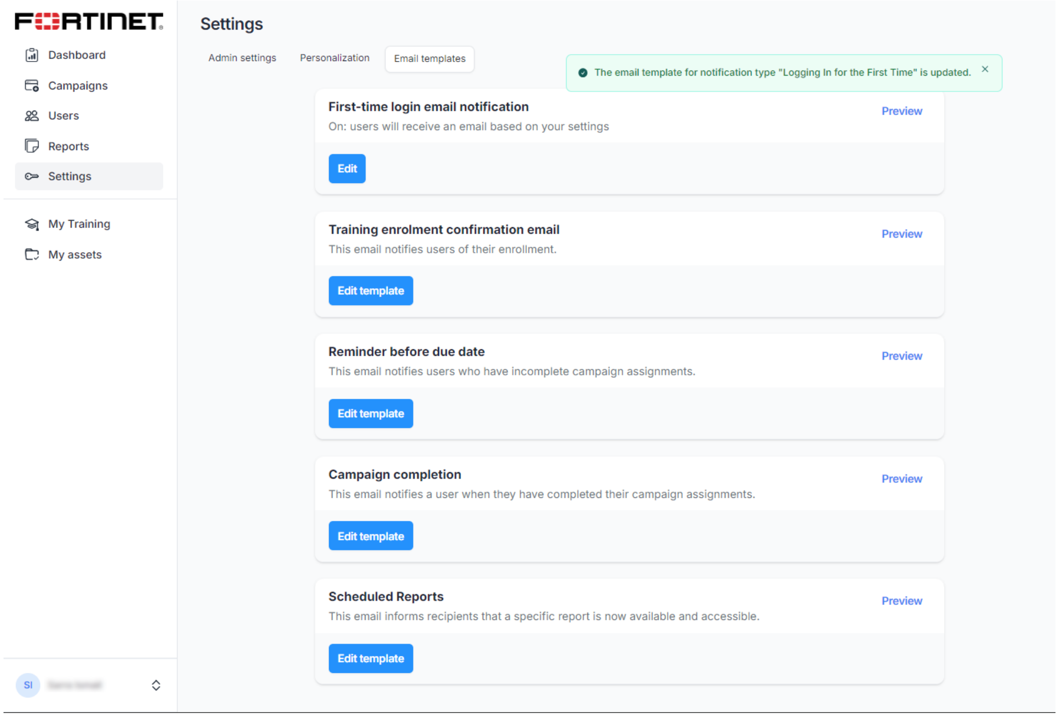
We're pleased to inform you that the report '{{reportname}}' is now available for your review. You can find it attached to this email.

If you'd like to configure additional reports similar to this, please don't hesitate to get in touch with your administrator.

Use placeholders in your email

PLACEHOLDER	CONTENT INSERTED
{{firstname}}	Populates the user's first name.
{{reportname}}	Populates the report name, exclusively for the 'Your Report is Ready' email type.

6. Click *Save*. A confirmation message is displayed.



The email template for notification type "Logging In for the First Time" is updated.

First-time login email notification

On: users will receive an email based on your settings

Training enrolment confirmation email

This email notifies users of their enrollment.

Reminder before due date

This email notifies users who have incomplete campaign assignments.

Campaign completion

This email notifies a user when they have completed their campaign assignments.

Scheduled Reports

This email informs recipients that a specific report is now available and accessible.

Users

Creating and importing users

Before you create and launch your campaign, you must create or import your learners. There are three ways to import your learners. Typically, the option to add a single user is used in the preliminary stages. You can create single users to test your SSO/SAML2 configuration, or, to add a small number of users to allow them to review the system and content. Before going to production, you will import the balance of your user communities information. This is done by either populating the example .csv and importing them, or by configuring a connection to your LDAP (Active Directory).

There are three ways to import your learners (single, through CSV, through LDAP synch).

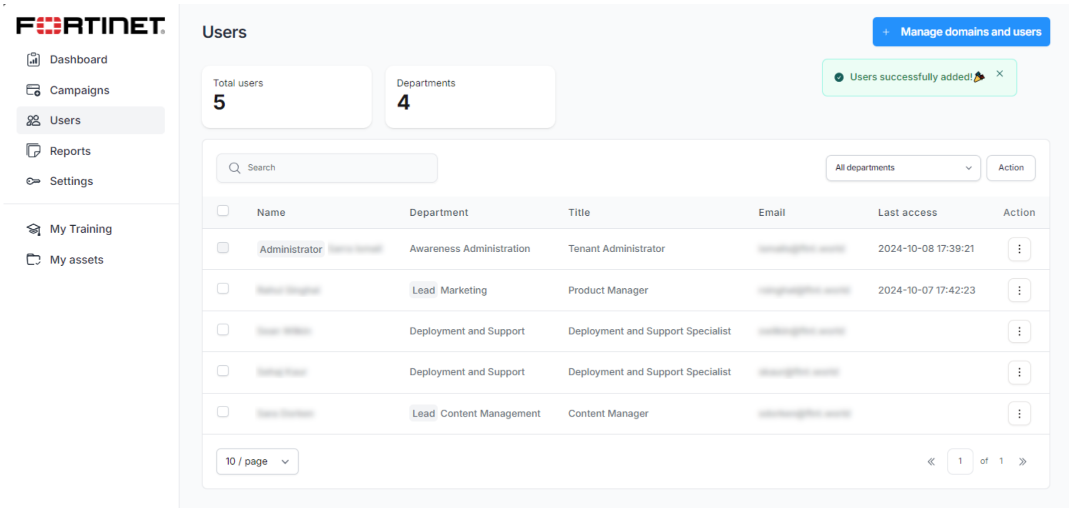
To add a single user:

1. Select *Users* from the navigation menu.
2. Click *+ Manage domains users*.
3. Select the *Add a single user* tab.
4. Complete the form with the desired values:

Field	Description
First Name* **(required)**	Denotes the first name of the user. This should be represented in title case as this is how the user name will appear in the system, reports and completion certificates.
Last Name* **(required)**	Denotes the last name of the user. This should be represented in title case as this is how the user name will appear in the system, reports and completion certificates.
Email Address* **(required)**	Denotes the email of the user. This should match the email for the user. When configuring SSO/SAML2 authentication, this email MUST match the value being passed from the authentication solution. If it does not match, the user will not be recognized by the system and the user will be presented with an error.
Title* **(required)**	While this field is labeled Title, it need not contain a title. However, whatever unique values appear in this field will be used when assigning training campaigns and outputting report data.
Department* **(required)**	While this field is labeled Department, it need not contain a department name. However, whatever unique values appear in this field will be used when assigning training campaigns and outputting report data.

Field	Description
Manager Email	The manager email is the email of the person the user reports to. These manager emails must also be users included in the system. I.e. you cannot refer to any email that is not part of the imported user community. This field is used for advanced notifications (copy manager). If you do not populate this field, or, the mapped attribute in LDAP is a null value, you will not be able to use this functionality.
Role	Default: No Role, options: No Role or Administrator
Is this user a department lead?	Default: No. If yes, user will be selectable when scheduling management level campaign reports. They will receive statistics for any users who match their assigned department value. These reports provide the overall progress of the campaign (Completed, In Progress, Not Started, Overdue statistics) for the campaign. It does not provide learner information (names or emails).

5. Once completed, click *Add*. A confirmation message will be presented:



Total users 5

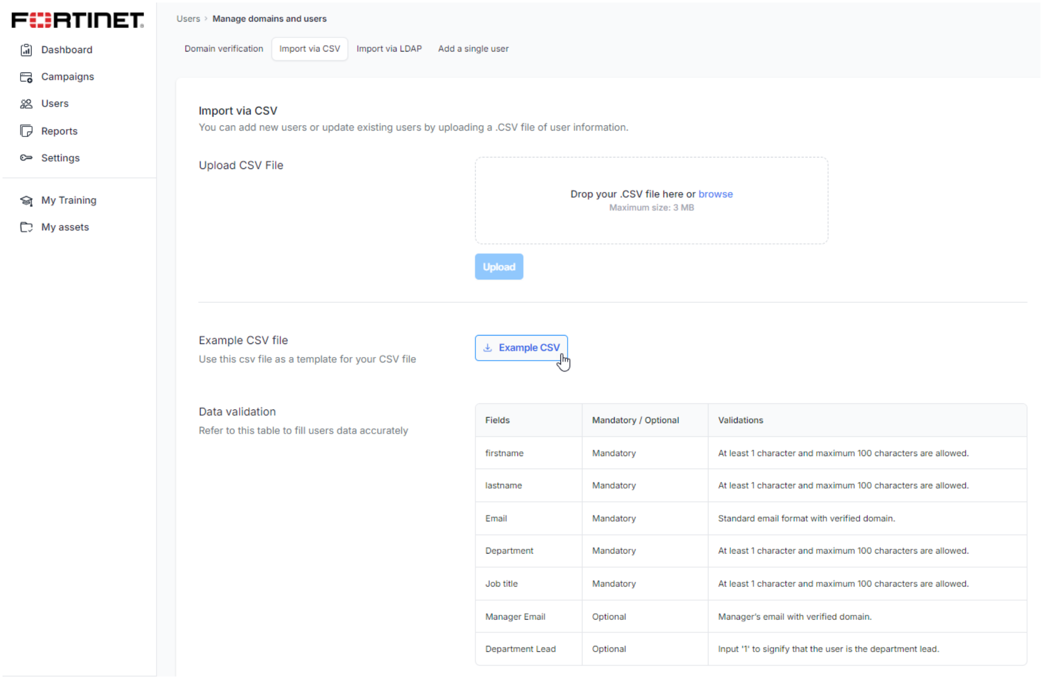
Departments 4

Users successfully added!

Name	Department	Title	Email	Last access	Action
Administrator [redacted]	Awareness Administration	Tenant Administrator	[redacted]	2024-10-08 17:39:21	⋮
[redacted]	Lead Marketing	Product Manager	[redacted]	2024-10-07 17:42:23	⋮
[redacted]	Deployment and Support	Deployment and Support Specialist	[redacted]		⋮
[redacted]	Deployment and Support	Deployment and Support Specialist	[redacted]		⋮
[redacted]	Lead Content Management	Content Manager	[redacted]		⋮

To import users through a CSV file:

1. Select *Users* from the navigation menu, then.
2. Select + *Manage domains users*.
3. Select *Import via CSV* tab.
4. Download the *ExampleCsvFile.csv*.



Import via CSV

You can add new users or update existing users by uploading a .CSV file of user information.

Upload CSV File

Example CSV file

Use this csv file as a template for your CSV file

Data validation

Refer to this table to fill users data accurately

Fields	Mandatory / Optional	Validations
firstname	Mandatory	At least 1 character and maximum 100 characters are allowed.
lastname	Mandatory	At least 1 character and maximum 100 characters are allowed.
Email	Mandatory	Standard email format with verified domain.
Department	Mandatory	At least 1 character and maximum 100 characters are allowed.
Job title	Mandatory	At least 1 character and maximum 100 characters are allowed.
Manager Email	Optional	Manager's email with verified domain.
Department Lead	Optional	Input '1' to signify that the user is the department lead.

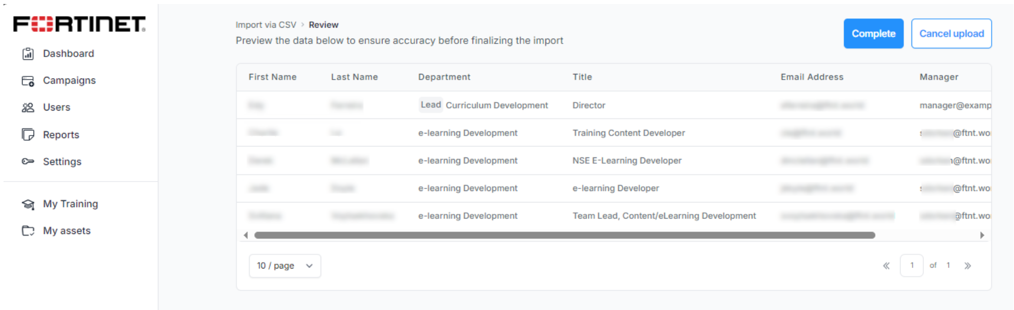
5. Open the *ExampleCsvFile.csv* and delete the sample data but do not delete the first row or change the values in the first row.

> If the *department_lead* column value is set to '1' (true), then this user will receive reports for all users who match their *Department* field value if the corresponding *Department Leads* option button is selected in the *Report Setup* tab of the Campaign configuration wizard.

6. Populate the file with your user data.

> While the columns department and job_title are labled as such, you need not specify departments or titles in these columns. The unique values you include in these two columns will be used to assign learners to training as well as to group users in reports. For example, you may wish to populate company names in department and city names in title if this is how you wish to group your users for campaign assignments.

7. Save the .csv as a CSV UTF-8 file type.
8. Drag and drop your populated .csv file on the *Drop your .CSV file here or browse* area or select *browse* to navigate to the file.
9. Select *Upload*. You will receive a review of your upload with any warnings or errors.



Import via CSV › Review

Preview the data below to ensure accuracy before finalizing the import

First Name	Last Name	Department	Title	Email Address	Manager
[redacted]	[redacted]	Lead Curriculum Development	Director	[redacted]	manager@examp
[redacted]	[redacted]	e-learning Development	Training Content Developer	[redacted]	[redacted]@ftnt.wo
[redacted]	[redacted]	e-learning Development	NSE E-Learning Developer	[redacted]	[redacted]@ftnt.wo
[redacted]	[redacted]	e-learning Development	e-learning Developer	[redacted]	[redacted]@ftnt.wo
[redacted]	[redacted]	e-learning Development	Team Lead, Content/eLearning Development	[redacted]	[redacted]@ftnt.wo

10. Select *Complete*. A *User upload is in progress* notification will be presented.

    When the upload is complete, a notification will be presented.

If you need to add more users, or, if changes need to be made to the user last name, title, department, manager or lead flag, you should update the .csv file you used initially. Then, re-upload the .csv.

Existing entries that have not changed will be ignored. Entries that have changed will get updated.

How to import through LDAP

For premium level service customers, administrators may import users from a Microsoft Active Directory instance. If this method is used, you must map the appropriate attributes from the LDAP Directory to the correct attributes in the service.

Once configured, any changes to user entries in the LDAP / Microsoft Active Directory will be periodically synchronized to the Security Awareness and Training Service. This includes user deletion and changes to attributes such as surname, title, department, and manager mappings.

A firewall rule may be required to allow the service to connect to the Directory in order to synchronize user data.

Do not add users until you have fully verified the LDAP configuration and filter is returning the expected results.

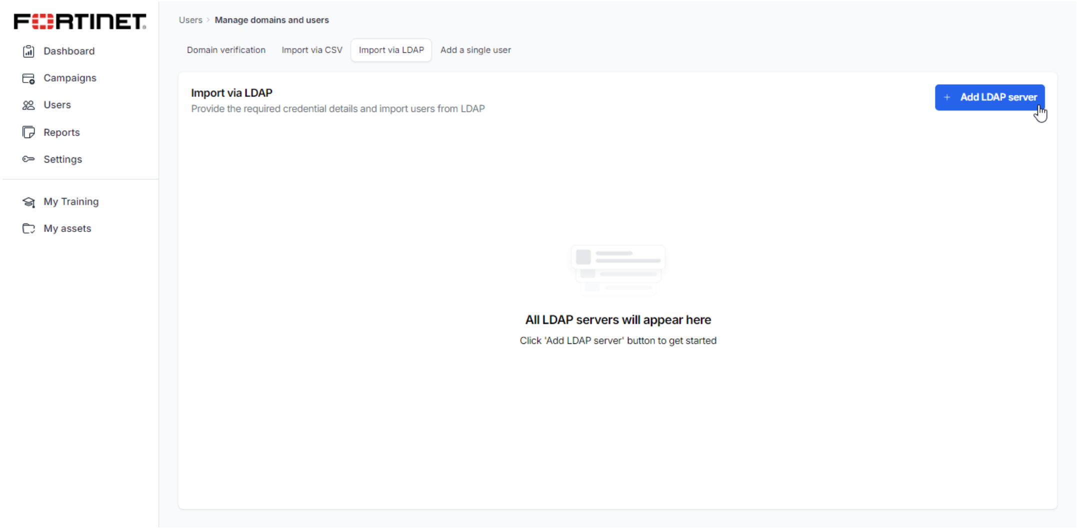
You can use a third party ldap browser to do this (such as Softerra LDAP Browser).

Before configuring the LDAP user import, we recommend testing your firewall rule and developing a good LDAP filter that returns only the users that will be taking the training. See Verifying and Testing LDAP settings using Softerra LDAP Browser.

If you would like assistance configuring and testing your LDAP configuration and LDAP filter, you can open a ticket by sending an email to: infosec_awareness@fortinet.com

To create an LDAP configuration:

1. Select *Users* from the navigation menu.
2. Select + *Manage domains users*.
3. Select the *Import via LDAP* tab.
4. Click + *Add LDAP server*.



Import via LDAP

Provide the required credential details and import users from LDAP

All LDAP servers will appear here

Click 'Add LDAP server' button to get started

5. Complete the *Configuration* section of the page to access your Active Directory.

Field	Description	Notes
Name	Give your connection a meaningful name.	For example, you can have multiple configurations each pointing to different OU levels within your Directory. The name should reflect the type of connection and location of the data that will be imported in this configuration.
LDAP Server URL	Provide the IP address or FQDN of the LDAP server you are configuring for user import.	This must be the externally accessible IP or FQDN for the server. Do not enter a URL.
Port Number	Enter the port number that your Directory listens on.	Default registered ports are: 389 (ldap) and 636 (ldaps). Ensure that you set the correct port corresponding to the Connect Mode (below): LDAP or LDAPS which dictates the protocol used to bind to the Directory.
Base DN	Enter the top-level OU that you would like to import users from.	You can specify all users from the top of the Directory or a single OU within the Directory Information Tree (DIT) structure. If you wish to specify multiple OUs from different locations in the Directory, you can create multiple configurations or use the Search Filter field to specify more specific data locations.

Field	Description	Notes
Search Filter	Enter the search filter you wish to identify users from within the DIT structure. The default (all users) should be set to: (objectClass=*)	The default (all users with any objectClass) is: (objectClass=*). A deployment specialist can help with a well-formed LDAP filter. Currently the length limit for the LDAP search filter is 255 characters. If your value is larger than 255, will get an error message similar to: *“Data too long for column ‘search_filter`” in debuginfo server response was shown. This column is in the database table mdl_local_users_ldap_servers.”*
User DN	Enter the Directory username that will be used to allow the service to bind to your Directory.	This should be the full DN of the user.
Password	Enter the corresponding password for the User DN Directory username that will be used to allow the service to bind to your Directory.	
Connect Mode	Select the protocol you will use that corresponds to the Port Number above (i.e. LDAP or LDAPS).	The service currently does not support Azure Active directory (Entra).

Before configuring this section, contact your Directory administrator to obtain the Directory attributes being used to store the following information. Default Directory attributes for Active Directory have been provided. All data points mentioned below should be present and populated either in the default attribute, or a different attribute.

Attribute names are case sensitive.

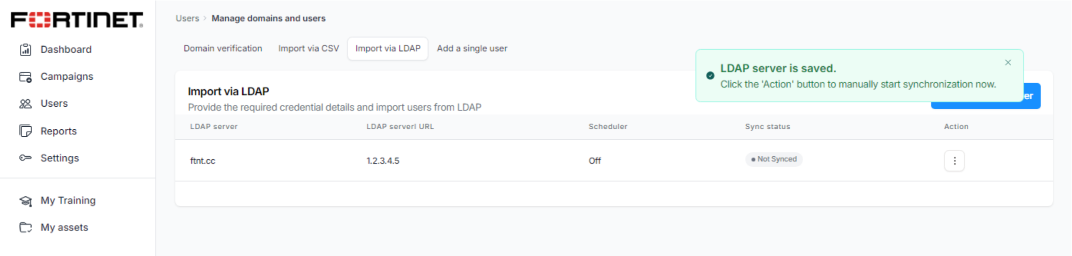
6. Complete the *Attribute Mapping* section.

Service Field Name	Directory Attribute	Notes
First Name	givenName	Enter the Directory attribute where the user’s first name information is stored. By default, in Active Directory, this is the givenName attribute.

Service Field Name	Directory Attribute	Notes
Last Name	sn	Enter the Directory attribute where the user’s first name information is stored. By default, in Active Directory, this is the sn (surname) attribute.
Email	mail	Enter the Directory attribute where the user’s email is stored. By default, in Active Directory, this is the mail attribute.
Title	title	Enter the Directory attribute where the user’s first name information is stored. By default, in Active Directory, this is the title attribute.
Department	department	Enter the Directory attribute where the user’s department information is stored. By default, in Active Directory, this is the department attribute.
Manager	manager	Enter the Directory attribute where the user’s first name information is stored. By default, in Active Directory, this is the manager attribute. If this attribute is not populated, the advanced ‘copy manager’ on email communications will not function.

In the above table, the Title and Department fields can be mapped to other attributes. The unique values harvested by these two attributes will dictate how you assign training campaigns to users and report on campaigns. I.e. If you map the title field to city, then you will be able to assign and report on training by city names. If the department field is mapped to company, then you will be able to assign training campaigns and report by the unique company values that are harvested.

7. Select your preferred weekly synchronization schedule.
8. Click *Save Configuration*. You should get a confirmation message that your LDAP server configuration is saved:



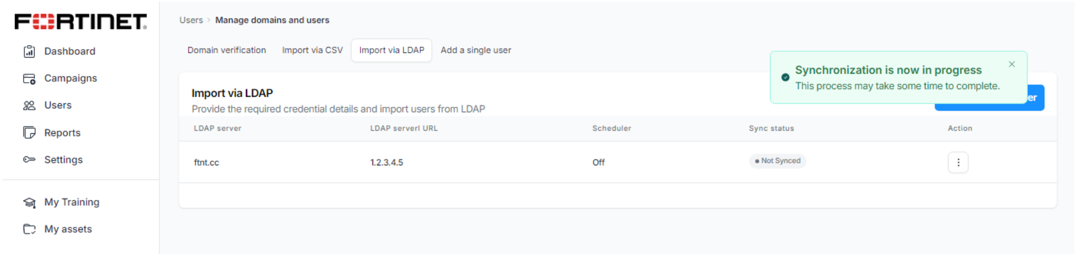
LDAP server is saved.
Click the 'Action' button to manually start synchronization now.

Import via LDAP
Provide the required credential details and import users from LDAP

LDAP server	LDAP serverl URL	Scheduler	Sync status	Action
ftnt.cc	1.2.3.4.5	Off	● Not Synced	⋮

To manually force the LDAP synchronization:

1. Select *Action* on the right of the *Import via LDAP* configuration you would like to force synchronization on, and then select *Sync Now*.

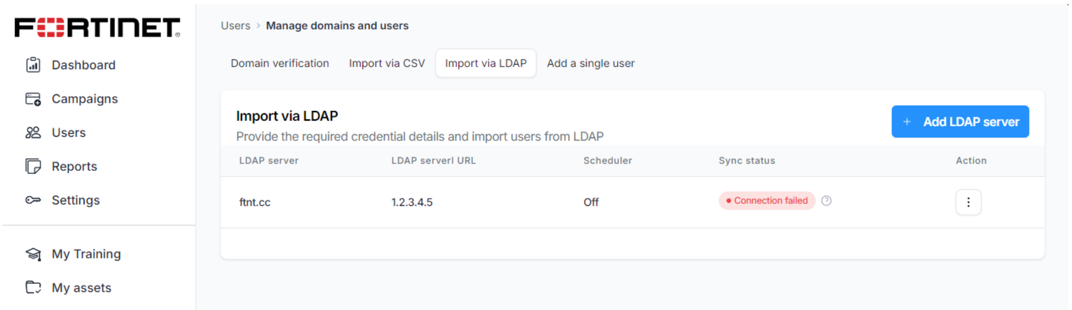


Synchronization is now in progress
This process may take some time to complete.

Import via LDAP
Provide the required credential details and import users from LDAP

LDAP server	LDAP serverl URL	Scheduler	Sync status	Action
ftnt.cc	1.2.3.4.5	Off	● Not Synced	⋮

2. After the sync attempt, if any of your LDAP Configuration settings are incorrect, you will receive the following error:

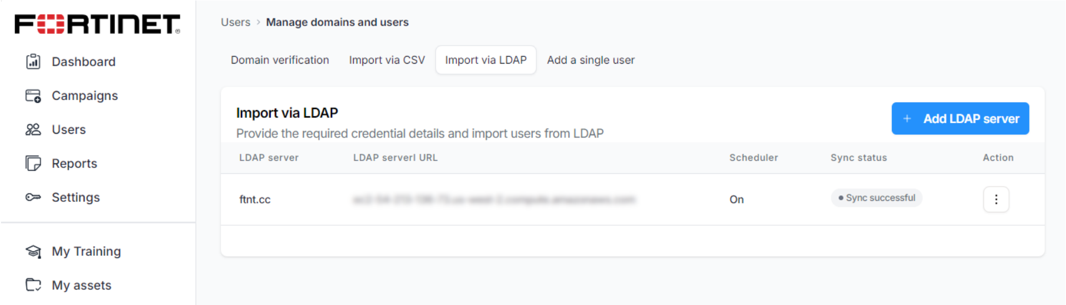


Import via LDAP
Provide the required credential details and import users from LDAP

LDAP server	LDAP serverl URL	Scheduler	Sync status	Action
ftnt.cc	1.2.3.4.5	Off	● Connection failed	⋮

3. Check your settings and try again. You can get assistance by sending an email to infosec_awareness@fortinet.com

4. If successful, you should now be redirected and see your configuration saved on the *Import via LDAP* page.

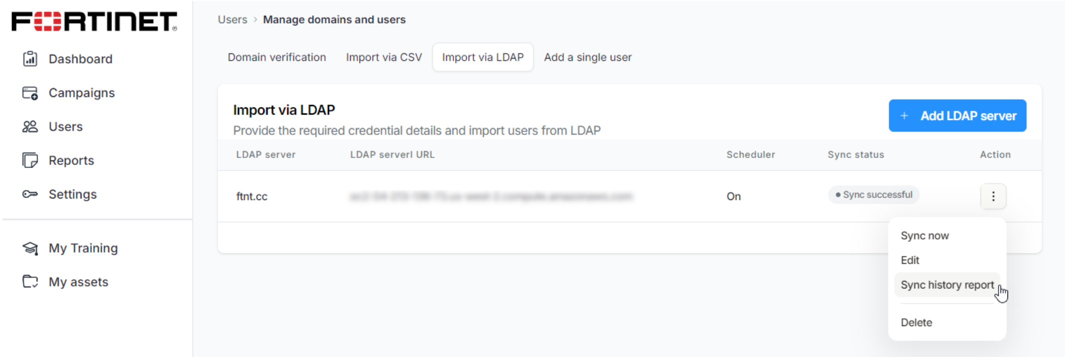


Import via LDAP
Provide the required credential details and import users from LDAP

LDAP server	LDAP serverl URL	Scheduler	Sync status	Action
ftnt.cc	[redacted]	On	● Sync successful	⋮

To check the LDAP synchronization history:

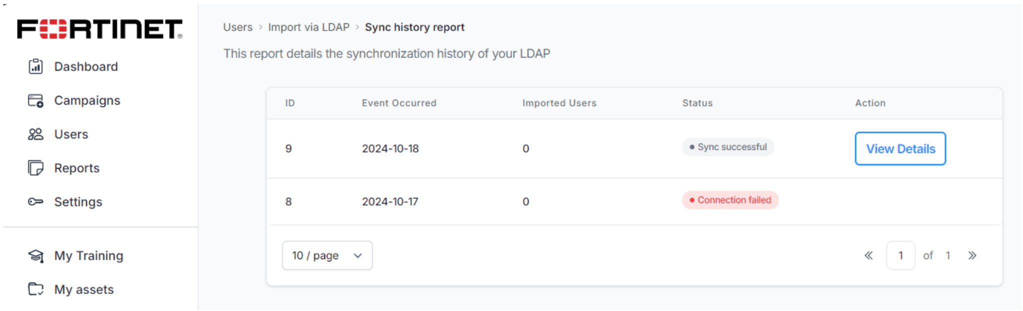
1. Click *Action* > *Sync history report*.



Import via LDAP
Provide the required credential details and import users from LDAP

LDAP server	LDAP serverl URL	Scheduler	Sync status	Action
ftnt.cc	[redacted]	On	● Sync successful	⋮

The *Sync history report* is displayed.



Users > Import via LDAP > Sync history report

This report details the synchronization history of your LDAP

ID	Event Occurred	Imported Users	Status	Action
9	2024-10-18	0	● Sync successful	View Details
8	2024-10-17	0	● Connection failed	

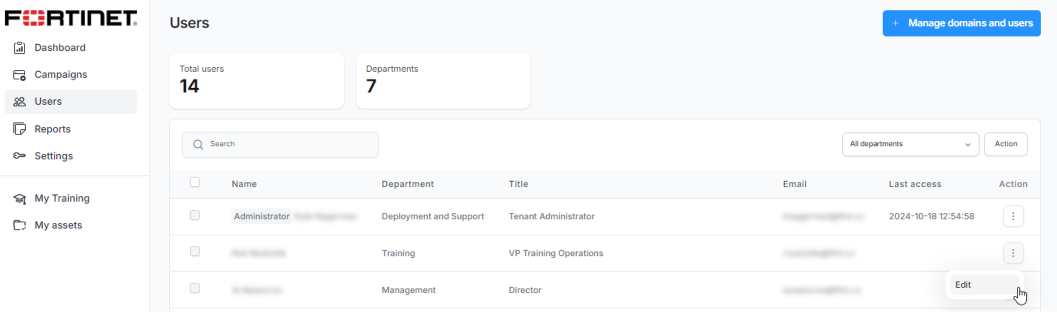
The synchronization of users can take some time, depending on the number of users. Weekly LDAP synchronization is run according to the settings above. If users do not synch within 24 hours, open a ticket by sending an email to infosec_awareness@fortinet.com

Setting the Department Lead flag for users

After the LDAP synchronization has completed you may wish to set the department_lead flag for specific users.

To set the department lead flag:

1. Select *Users* from the navigation menu, then select the *Action* > *Edit*.



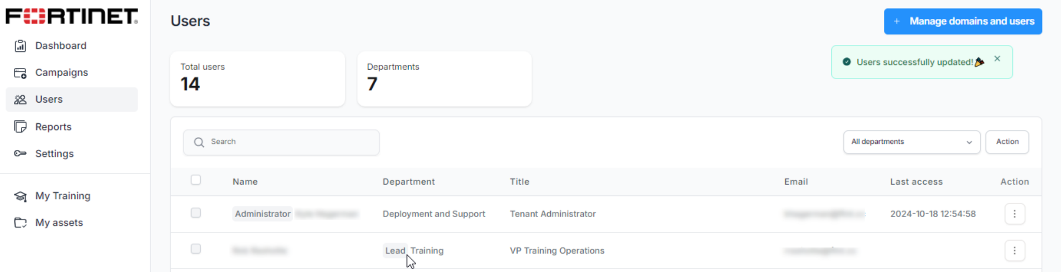
Users

Total users 14

Departments 7

□	Name	Department	Title	Email	Last access	Action
□	Administrator [redacted]	Deployment and Support	Tenant Administrator	[redacted]	2024-10-18 12:54:58	⋮
□	[redacted]	Training	VP Training Operations	[redacted]		⋮
□	[redacted]	Management	Director	[redacted]		

2. Select *Yes* in the *Is this user a department lead?* section.
3. Click *Save*.
   You will see the *Lead* indicator icon added to the *Department* column to indicate this user has been assigned the department lead entitlement.



Users

Total users 14

Departments 7

Users successfully updated!

□	Name	Department	Title	Email	Last access	Action
□	Administrator [redacted]	Deployment and Support	Tenant Administrator	[redacted]	2024-10-18 12:54:58	⋮
□	[redacted]	Lead Training	VP Training Operations	[redacted]		⋮

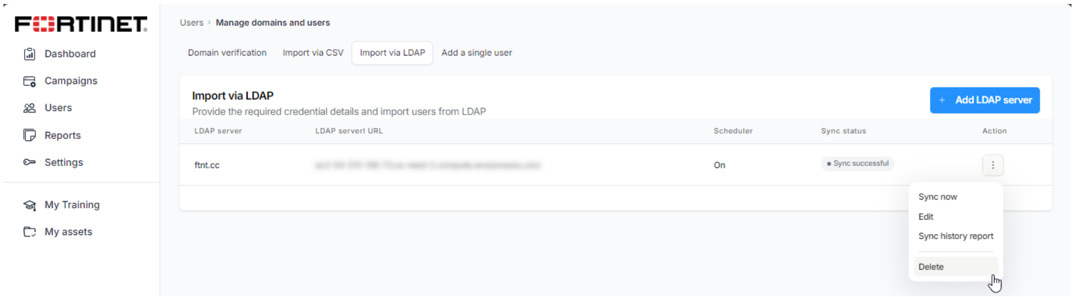
If the Department Lead check box is selected, then this user will receive reports for all users who match their *Department* field value if the corresponding *Department Leads* option button is selected in the *Report Setup* tab of the Campaign configuration wizard.

Deleting Import via LDAP configuration entries

Users assigned the Administrator role can also delete *Import via LDAP* configurations.

To delete an Import via LDAP configuration:

1. Select *Users* from the navigation menu.
2. Select *+ Manage domains and users*.
3. Select the *Import via LDAP* tab.
4. To the right of the entry, select *Action > Delete*.



Import via LDAP

Provide the required credential details and import users from LDAP

LDAP server	LDAP serverl URL	Scheduler	Sync status	Action
ftnt.cc	[redacted]	On	● Sync successful	⋮

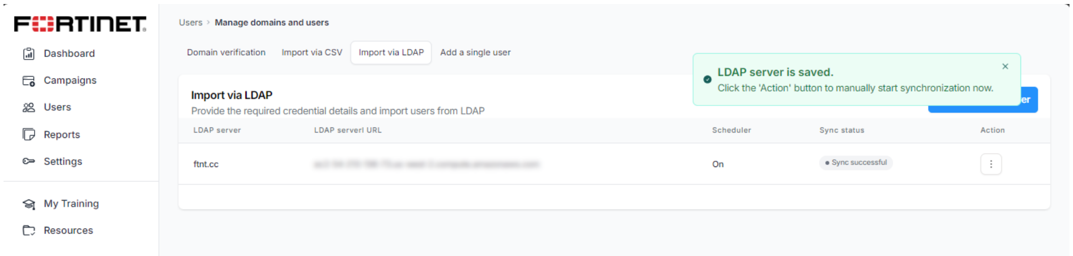
5. Click *Delete*.

Editing an Import via LDAP configuration entry

Users assigned the Administrator role can also edit *Import via LDAP* configurations.

To edit a configuration entry:

1. Select *Users* from the navigation menu.
2. Select *+ Manage domains and users*.
3. Select the *Import via LDAP* tab.
4. To the right of the entry, click *Action > Edit*.
5. Modify any settings you wish to change, then select *Save*.
6. Modify any settings you wish to change, then select Save.
   A confirmation message is displayed.

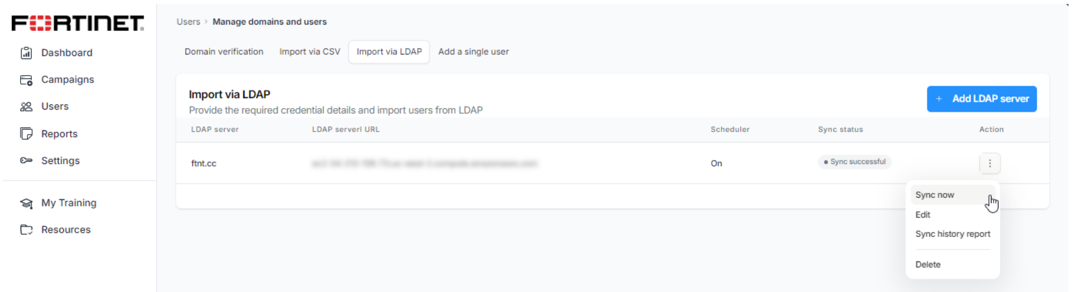


LDAP server is saved.
Click the 'Action' button to manually start synchronization now.

Import via LDAP
Provide the required credential details and import users from LDAP

LDAP server	LDAP serverl URL	Scheduler	Sync status	Action
ftnt.cc	[illegible]	On	● Sync successful	⋮

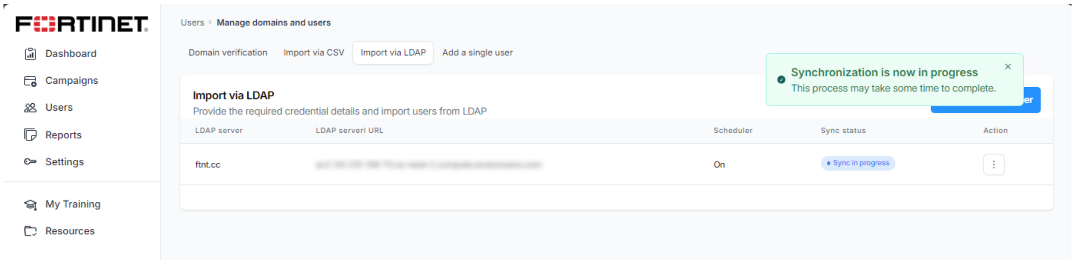
7. When ready, start the synchronization by selecting *Action* > *Sync now*.



Import via LDAP
Provide the required credential details and import users from LDAP

LDAP server	LDAP serverl URL	Scheduler	Sync status	Action
ftnt.cc	[illegible]	On	● Sync successful	⋮

A confirmation message is displayed.



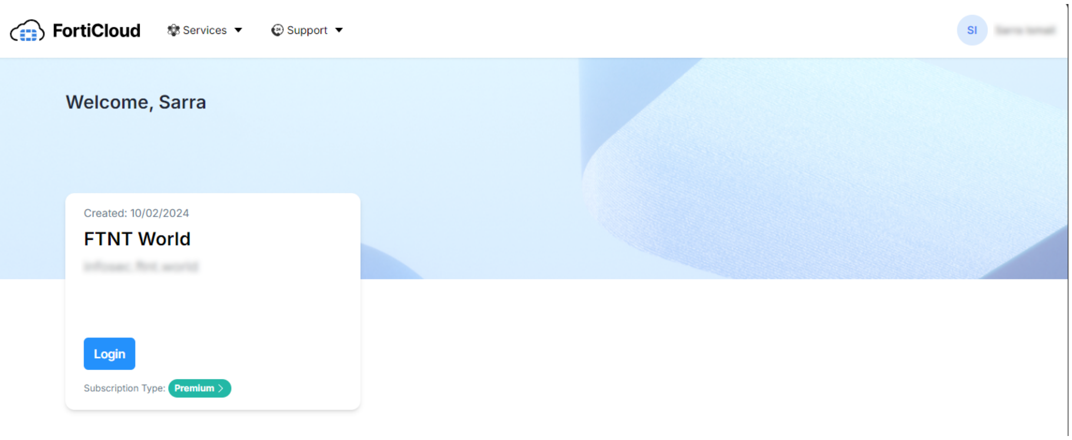
Synchronization is now in progress
This process may take some time to complete.

Import via LDAP
Provide the required credential details and import users from LDAP

LDAP server	LDAP serverl URL	Scheduler	Sync status	Action
ftnt.cc	[illegible]	On	● Sync in progress	⋮

Subscription Type

If you log in to the https://ftnt.info as the Tenant Administrator (the initial FortiCloud account used to initialize the service and input the licenses), you will land on the home page.



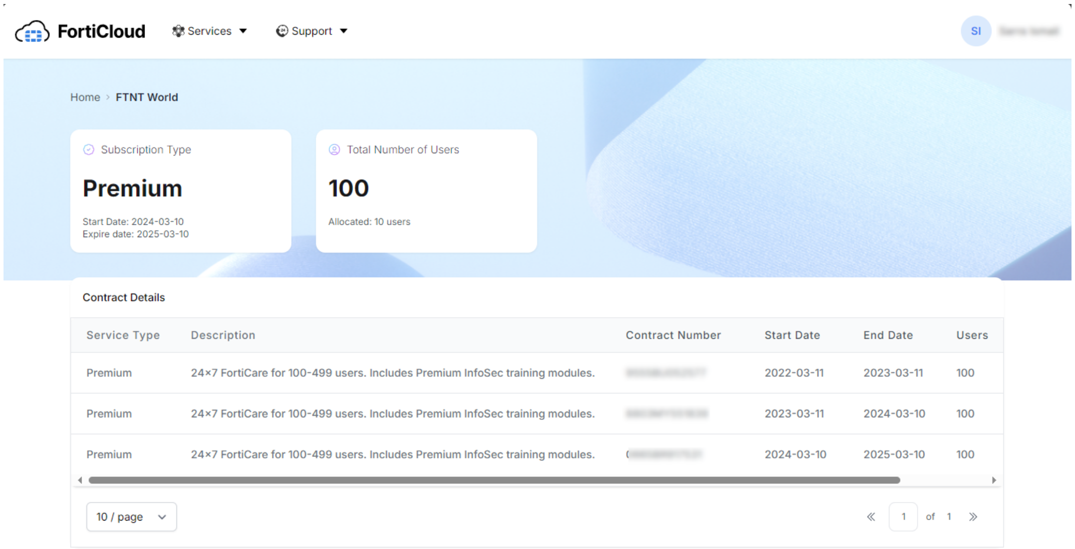
Welcome, Sarra

Created: 10/02/2024
FTNT World

Subscription Type: Premium

From this page, you can access FortiCloud Services and Support menu options from the FortiCloud banner at the top of the page.

You can also access your license information by clicking on the *Subscription Type* indicator.



[redacted]

Home › FTNT World

Subscription Type

Premium

Start Date: 2024-03-10
Expire date: 2025-03-10

Total Number of Users

100

Allocated: 10 users

Contract Details

Service Type	Description	Contract Number	Start Date	End Date	Users
Premium	24×7 FortiCare for 100-499 users. Includes Premium InfoSec training modules.	[redacted]	2022-03-11	2023-03-11	100
Premium	24×7 FortiCare for 100-499 users. Includes Premium InfoSec training modules.	[redacted]	2023-03-11	2024-03-10	100
Premium	24×7 FortiCare for 100-499 users. Includes Premium InfoSec training modules.	[redacted]	2024-03-10	2025-03-10	100

Here you can view your history of contracts as well as the current contract start and end dates, the number of purchased seats as well as the seats currently in use and the subscription type.

Assigning Additional Administrators

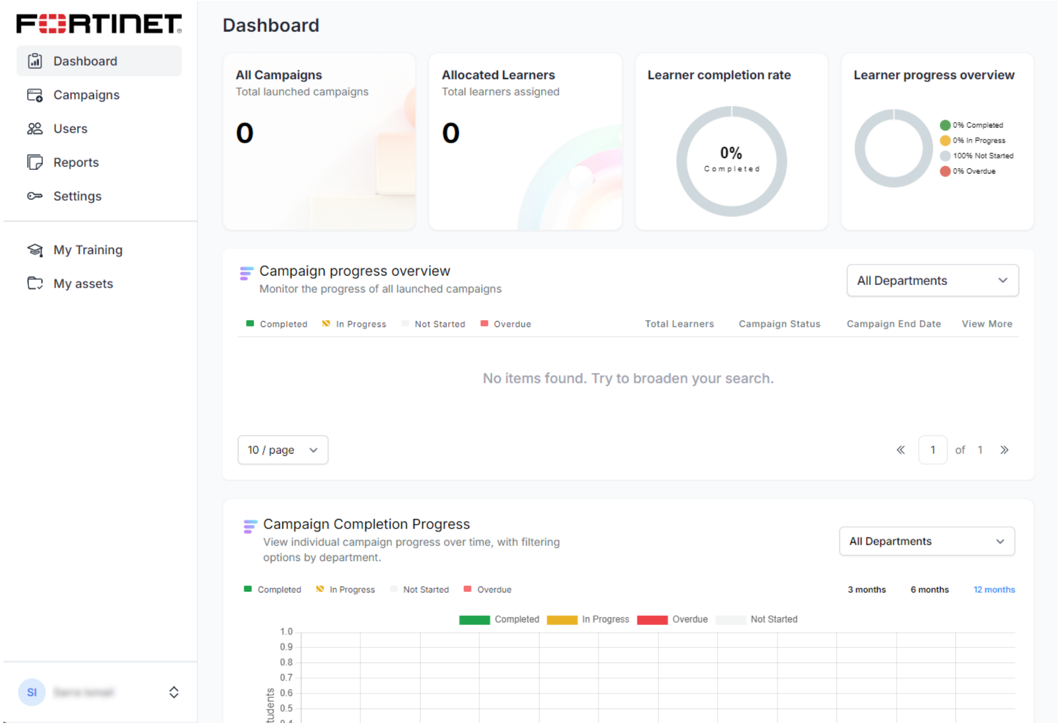
Only users that have been assigned administrative roles will have access to the administrative functionality of the service.

Additional administrators can assist with configuration, user management, campaign management and reporting.

Currently, these sub-admins have full access to the administrative functionality of the service with two exceptions:

- It does not allow them access to the FortiPhish service pages or configuration from the Dashboard page. This information can only be accessed if the sub-admin creates their own FortiCloud account and the Tenant Administrator FortiCloud grants them access through the Manager User functionality in FortiCloud.
- It does not allow them access to download assets from the *Assets* navigation menu item. This information can only be accessed if the sub-admin creates their own FortiCloud account AND the Tenant Administrator FortiCloud grants them access through the Manager User functionality in FortiCloud.

Once a user is assigned administrative rights, they will see the administrative function menu in the app.



No items found. Try to broaden your search.

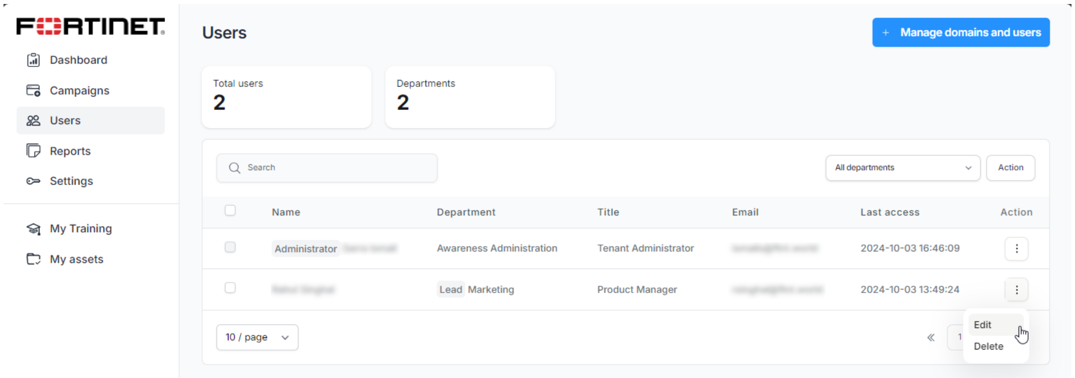
Administrative users can still access their training and assets from the lower menu.

Administrative roles can be assigned through the *Users* navigation menu.

Assigning Administrative Roles

To assign administrative roles:

1. After logging in as the tenant administrator, select *Users* from the navigation menu.
2. Select the options button to the right of the user that you want to assign an administrative role to and select *Edit*.

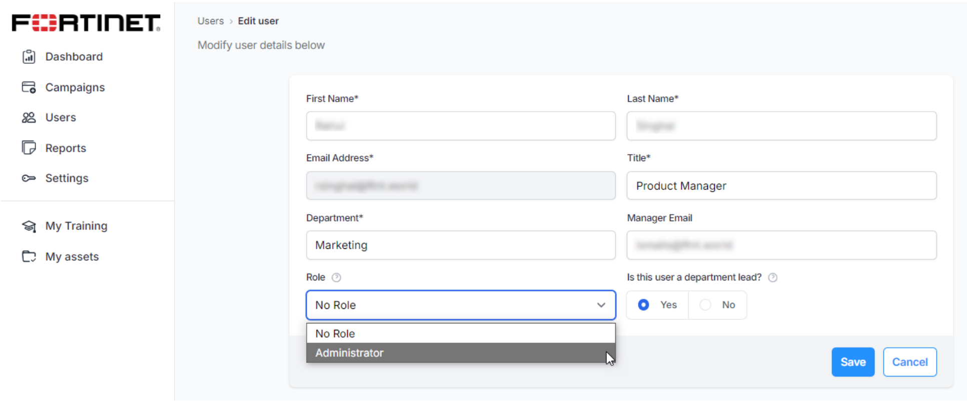


Users

Total users	Departments
2	2

	Name	Department	Title	Email	Last access	Action
□	Administrator [redacted]	Awareness Administration	Tenant Administrator	[redacted]	2024-10-03 16:46:09	⋮
□	[redacted]	Lead Marketing	Product Manager	[redacted]	2024-10-03 13:49:24	⋮

3. Select the desired *Role*.



Modify user details below

First Name*: [redacted]

Last Name*: [redacted]

Email Address*: [redacted]

Title*: Product Manager

Department*: Marketing

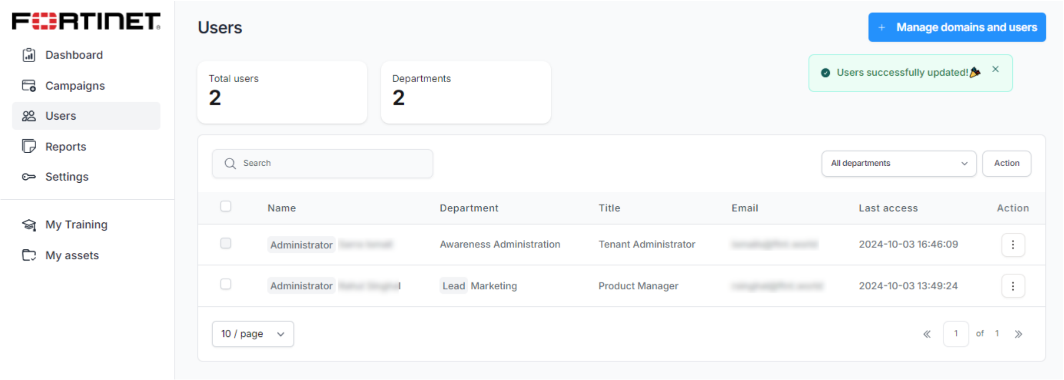
Manager Email: [redacted]

Role: No Role

Is this user a department lead? ● Yes ○ No

4. Click *Save*.

   A confirmation message is presented and the user role is indicated in the *Name* column.



Users

Users successfully updated!

Total users	Departments
2	2

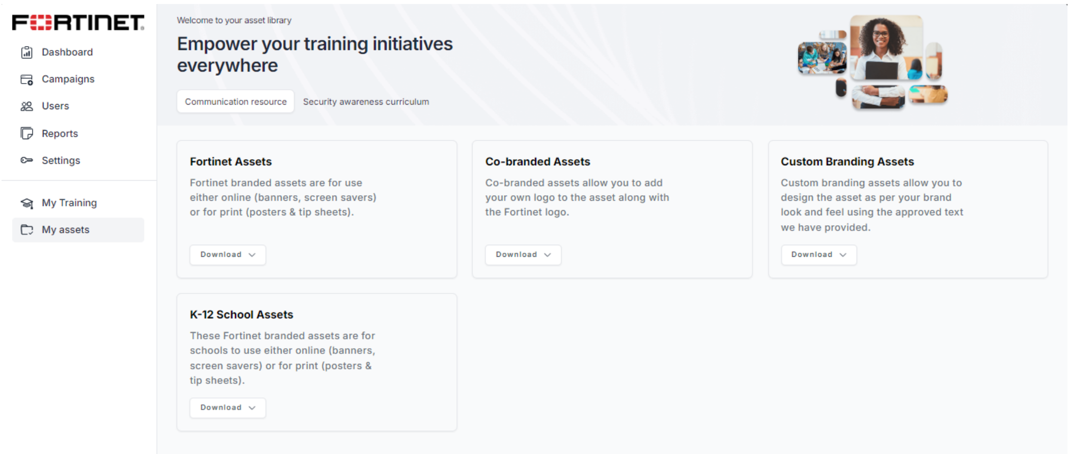
	Name	Department	Title	Email	Last access	Action
□	Administrator [redacted]	Awareness Administration	Tenant Administrator	[redacted]	2024-10-03 16:46:09	⋮
□	Administrator [redacted]	Lead Marketing	Product Manager	[redacted]	2024-10-03 13:49:24	⋮

You can remove or change administrative permissions by following the same steps and selecting the new role.

My Assets

The Assets available in this section are made available depending on what service level and Add-on packages you have purchased.

There are two tabs on the *Assets* navigation menu item: *Communication resource* and *Security awareness curriculum*.



Welcome to your asset library

Empower your training initiatives everywhere

Fortinet Assets

Fortinet branded assets are for use either online (banners, screen savers) or for print (posters & tip sheets).

Co-branded Assets

Co-branded assets allow you to add your own logo to the asset along with the Fortinet logo.

Custom Branding Assets

Custom branding assets allow you to design the asset as per your brand look and feel using the approved text we have provided.

K-12 School Assets

These Fortinet branded assets are for schools to use either online (banners, screen savers) or for print (posters & tip sheets).

Communication Resources

Fortinet Assets

Fortinet branded assets are for use either online (banners, screen savers) or for print (posters & tip sheets).

All license levels get access to the Fortinet branded assets (Free 25 / Standard Level Service / Premium Service).

Assets included:

- Banners (JPEGs)
- Emails (.docx)
- Posters (JPEGs/PDFs)
- Screen Savers (JPEGs)
- Tips Sheets (PDFs)

Co-branded Assets

Co-branded assets allow you to add your own logo to the asset along with the Fortinet logo.

Premium level service subscribers get access to the Fortinet branded assets.

Assets included:

- Banners (JPEGs/PDFs)
- Emails (.docx)
- Posters (PDFs)
- Screen Savers (PDFs)
- Tips Sheets (PDFs)

Custom Branding Assets

Custom branding assets allow you to design the asset as per your brand look and feel using the approved text we have provided.

Custom branding assets are available to those who purchase a license for the Custom Branding Add-on only.

Custom Assets are all contained in a .docx (Microsoft Office – Word) format file.

K-12 School Assets

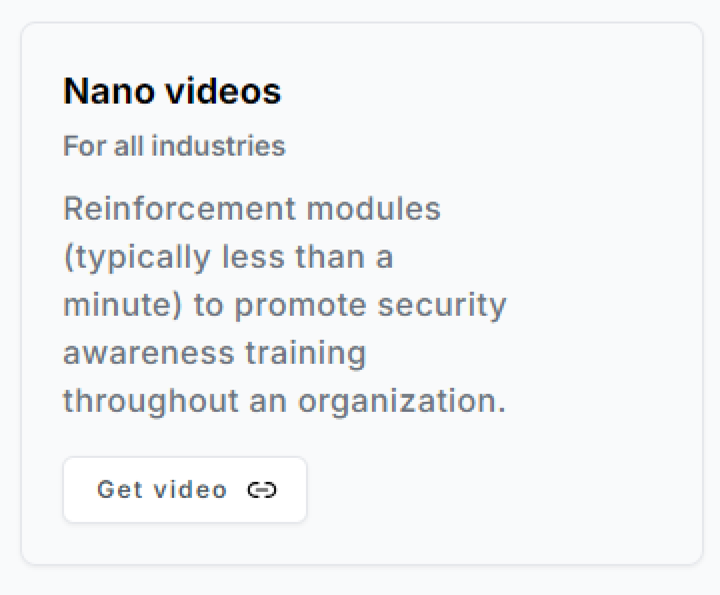
These Fortinet branded assets are for schools to use either online (banners, screen savers) or for print (posters & tip sheets). They use education vertical language and images instead of the corporate or enterprise style that the other assets use.

- Banners (JPEGs/PDFs)
- Posters (PDFs)
- Screen Savers (JPGs)
- Tips Sheets (PDFs)

Nano Videos

Reinforcement modules (typically less than a minute) to promote security awareness training throughout an organization. These videos are provided through a URL and can be cycling on kiosks or terminals in common areas to spread awareness of your campaigns and provide security tips. They are available in all supported languages. There are also videos specifically designed for the K-12 school space.

To access the Nano Videos, click *Get video*.

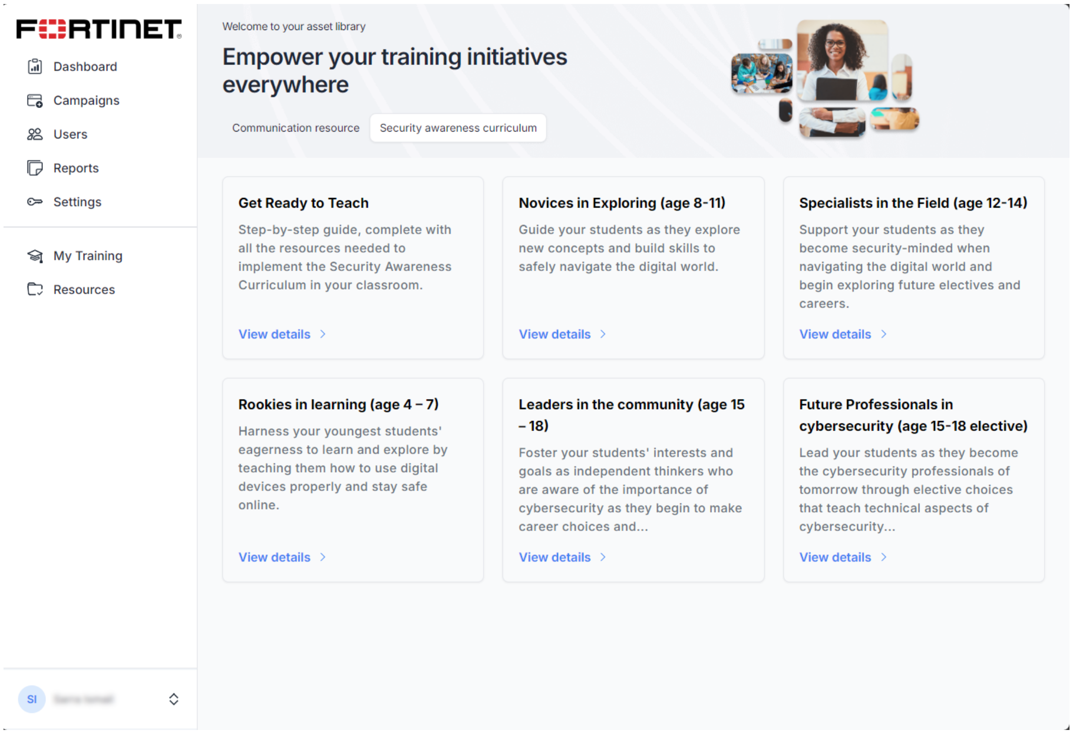


Nano videos

For all industries

Reinforcement modules (typically less than a minute) to promote security awareness training throughout an organization.

Security Awareness Curriculum



Welcome to your asset library

Empower your training initiatives everywhere

Get Ready to Teach

Step-by-step guide, complete with all the resources needed to implement the Security Awareness Curriculum in your classroom.

View details >

Novices in Exploring (age 8-11)

Guide your students as they explore new concepts and build skills to safely navigate the digital world.

View details >

Specialists in the Field (age 12-14)

Support your students as they become security-minded when navigating the digital world and begin exploring future electives and careers.

View details >

Rookies in learning (age 4 – 7)

Harness your youngest students' eagerness to learn and explore by teaching them how to use digital devices properly and stay safe online.

View details >

Leaders in the community (age 15 – 18)

Foster your students' interests and goals as independent thinkers who are aware of the importance of cybersecurity as they begin to make career choices and...

View details >

Future Professionals in cybersecurity (age 15-18 elective)

Lead your students as they become the cybersecurity professionals of tomorrow through elective choices that teach technical aspects of cybersecurity...

View details >

This section includes security awareness curriculum for classrooms. The curriculum helps students learn how to apply cybersecurity skills to their digital interactions at school, at home and everywhere they go.

Get Ready to Teach

A step-by-step guide, complete with all the resources needed to implement the Security Awareness Curriculum in your classroom.

This section contains the following elements:

Teacher Resources

- Ready-to-Teach Lesson Plan with step-by-step explanations of how to teach this lesson including all classroom instructions, learning objectives, lesson pacing adjustment, vocabulary and talking points.
- Teacher Guide with background information teachers can reference before teaching the lesson. This is an optional resource to equip teachers with in-depth knowledge to support student learning.
- Teacher Answer Guide with possible answers and key points to assess and guide classroom learning and discussions.

Classroom Materials

- Lesson Slides that teachers can use during classroom instruction in both PowerPoint and Google Slides format including embedded videos.
- Student Handouts to be used with the lesson.
- Multimedia Assets should teachers wish to access the videos separately from the lesson plan presentations.

The suggested order is:

1. Review the lesson plan and key points for teaching this lesson. If you are not familiar with some concepts or terms, you can refer to the teacher guide with background information.
2. If needed, view the teacher guide background information and supplement your knowledge on the topic.
3. Choose the slide deck in your preferred format.
4. Print off or access the fillable PDF student handouts.
5. Print off or access the fillable PDF rubrics and teacher answer guides.
6. Incorporate the lesson into your day.

The package contents are:

- Lesson plans
- Teacher guides
- Answer guides
- PowerPoint slideshows
- Videos
- Student handouts

Security Awareness Curriculum Content:

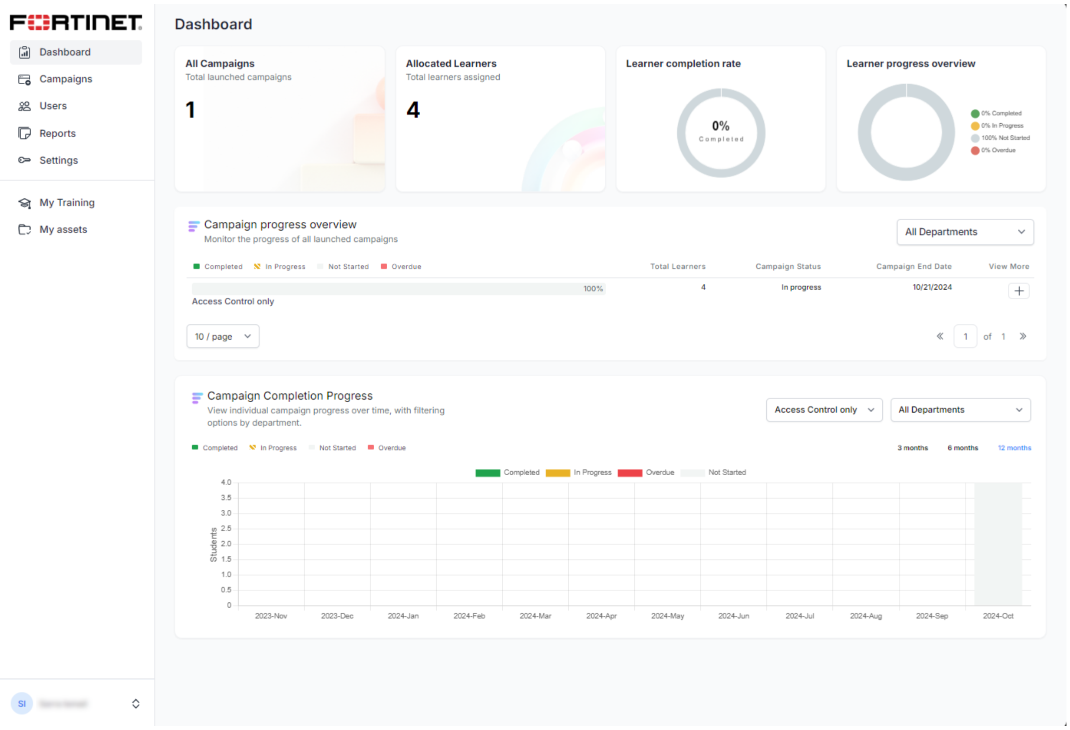
Specialists in the Field (age 12-14)

Securing Data and Keeping it Private	Students learn the impact of cybersecurity on their personal safety and how they can protect, recognise and respond to cyberattacks now and as future professionals.
Understanding Cybersecurity	Students learn the impact of cybersecurity on their personal safety and how they can protect, recognize, and respond to cyberattacks now, and as future professionals.
Identity in the Digital World	Students will learn to create a positive and safe online presence and make mindful choices about sharing content, identity, and information online.
Cyberbullying	Digital Safety Strand: Students will learn how to protect themselves from dangerous or unfamiliar people and places online and understand what to do if they get uncomfortable online.
Social Media Influence	Students will become advocates for their knowledge as they seek reliable information and share appropriate sources of information online.
Respecting Intellectual Property	Students will make informed decisions about actions and choices when using technology by understanding the rights, responsibilities, and consequences of online behaviors.

Campaign management

Dashboard

The *Dashboard* page is available by selecting the *Dashboard* navigation menu item.



The *Dashboard* is designed to give a high-level overview of the currently active campaigns. It does not show information for scheduled campaigns or campaigns that are in a draft state. It does not present learner specific information.

Administrators can view the total number of launched campaigns (In progress / Ended) from the *All Campaigns* widget.

The *Allocated learners* widget displays the total number of learners assigned across all launched campaigns.

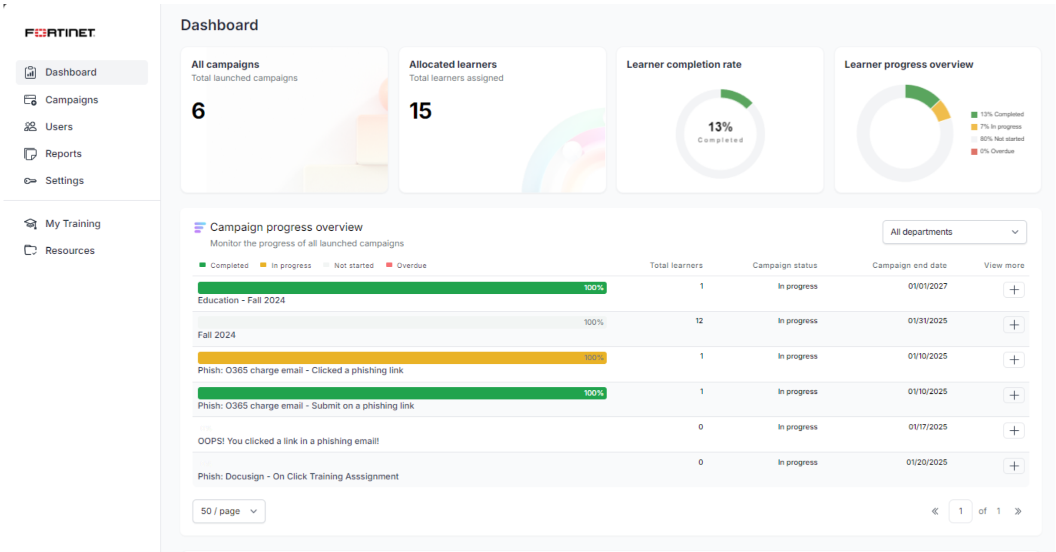
The *Learner completion rate* widget displays the total percentage of learners who have completed all modules and any associated quizzes (with a passing score of 80% or higher) across all launched campaigns.

The *Learner progress overview* widget displays the percentage of users in each state:

- *Completed*: The percentage of users who have completed all modules (and any associated quizzes with a passing score of 80% or higher).
- *In progress*: The percentage of users who have completed one or more modules (and any associated quizzes with a passing score of 80% or higher), but not completed all modules and associated quizzes within a campaign.

- *Not started*: The percentage of users who have not started viewing any training.
- *Overdue*: The percentage of users who have not completed all modules (and any associated quizzes with a passing score of 80% or higher) between the learner due date and the campaign end date.

Campaign progress overview



Dashboard

All campaigns
Total launched campaigns
6

Allocated learners
Total learners assigned
15

Learner completion rate
13%
Completed

Learner progress overview
🟩 13% Completed
🟨 7% In progress
80% Not started
🟥 0% Overdue

Campaign progress overview
Monitor the progress of all launched campaigns

All departments

🟩 Completed 🟨 In progress Not started 🟥 Overdue

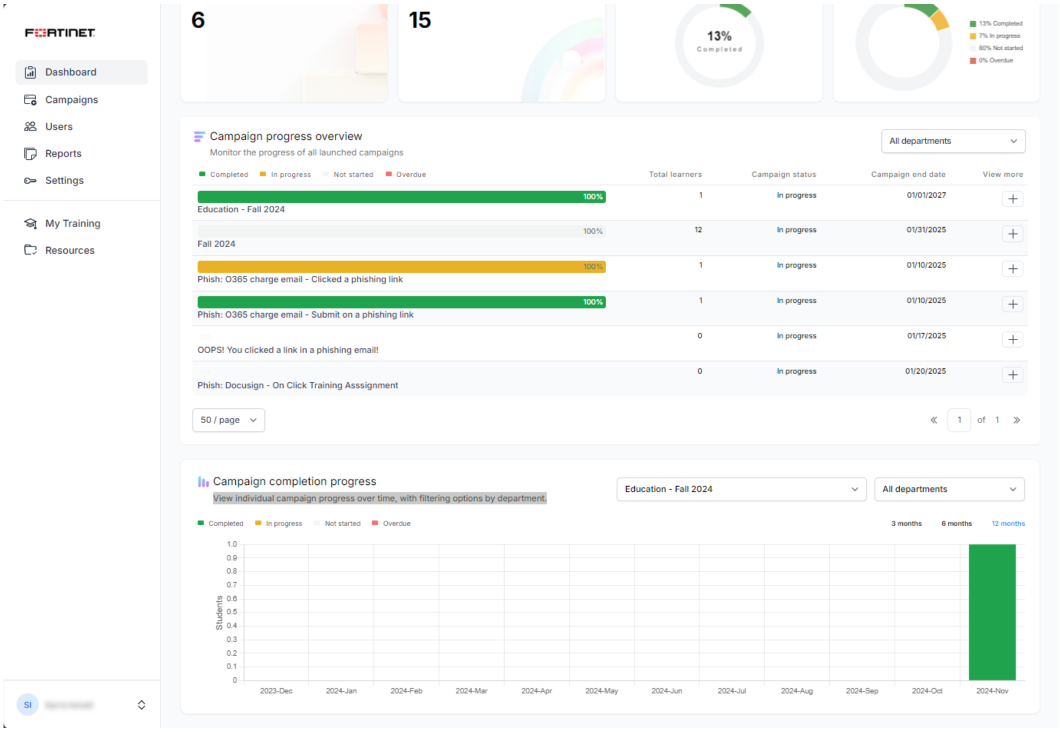
	Total learners	Campaign status	Campaign end date	View more
100% Education - Fall 2024	1	In progress	01/01/2027	+
100% Fall 2024	12	In progress	01/31/2025	+
100% Phish: O365 charge email - Clicked a phishing link	1	In progress	01/10/2025	+
100% Phish: O365 charge email - Submit on a phishing link	1	In progress	01/10/2025	+
0% OOPS! You clicked a link in a phishing email!	0	In progress	01/17/2025	+
0% Phish: Docusign - On Click Training Asssignment	0	In progress	01/20/2025	+

50 / page « 1 of 1 »

This section allows administrators to monitor the progress of all launched campaigns. Administrators can use the *Department* drop down to select *All departments*, or a specific department.

Campaign completion progress

This section allows administrators to monitor individual campaign progress over time, with filtering options by department.



Campaign progress overview

Monitor the progress of all launched campaigns

	Total learners	Campaign status	Campaign end date	View more
100% Education - Fall 2024	1	In progress	01/01/2027	+
100% Fall 2024	12	In progress	01/31/2025	+
100% Phish: O365 charge email - Clicked a phishing link	1	In progress	01/10/2025	+
100% Phish: O365 charge email - Submit on a phishing link	1	In progress	01/10/2025	+
OOPS! You clicked a link in a phishing email!	0	In progress	01/17/2025	+
Phish: Docusign - On Click Training Asssignment	0	In progress	01/20/2025	+

Campaign completion progress

View individual campaign progress over time, with filtering options by department.

Administrators can use the *Campaign* dropdown box to select a specific campaign. They can also use the *Department* dropdown to select all departments, or a specific department.

Administrators can also choose to view data for the last 3 months, the last 6 months or the last 12 months (default view).

Campaigns

Campaigns are assignments assigned to learners. Campaigns are comprised of one or more modules. Learners 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, learners 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 learner’s must achieve at least an 80% in order to pass. Once an 80% score is obtained by the learner, the module is marked as complete.

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

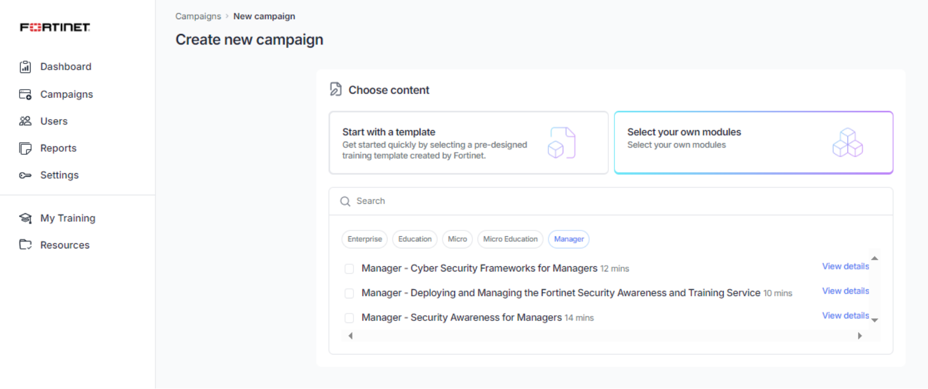
The Fortinet Security Awareness and Training Service supports running multiple campaigns across your organization at once. Campaigns can be created and assigned to the entire organization, to specific groups (depending on how you populate your user import data) or based on an event trigger from the FortiPhish automated phishing service. For example, you can design a campaign and assign it when people click a link in a phishing simulation email.

Before launching your initial campaign, Fortinet recommends reading the following documents and taking the Manager Modules training available in the service:

- Setting Goals and Planning Your Security Awareness and Training Program
- Planning Your Security Awareness and Training Calendar

Online Training

The online training is available when creating a new campaign from within the service.



Create new campaign

Choose content

Start with a template
Get started quickly by selecting a pre-designed training template created by Fortinet.

Select your own modules
Select your own modules

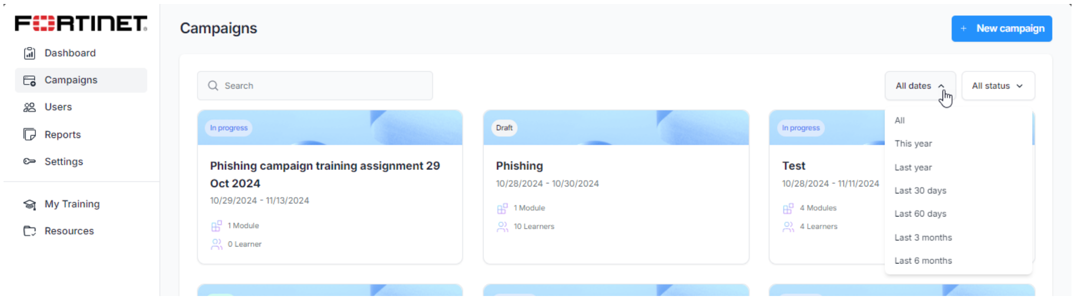
□ Manager - Cyber Security Frameworks for Managers 12 mins — View details
□ Manager - Deploying and Managing the Fortinet Security Awareness and Training Service 10 mins — View details
□ Manager - Security Awareness for Managers 14 mins — View details

Campaigns page

You can access the *Campaigns* page by selecting the *Campaigns* navigation menu item.

By default, this page will list all campaigns by default. You can filter the views by:

- Dates

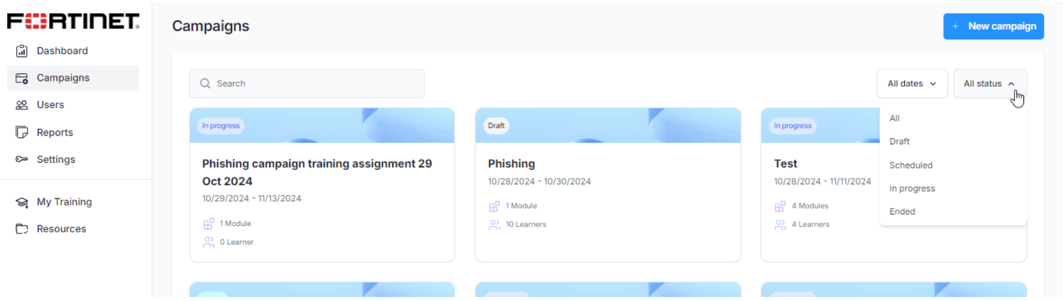


In progress
Phishing campaign training assignment 29 Oct 2024
10/29/2024 - 11/13/2024
1 Module
0 Learner

Draft
Phishing
10/28/2024 - 10/30/2024
1 Module
10 Learners

In progress
Test
10/28/2024 - 11/11/2024
4 Modules
4 Learners

- Status



In progress
Phishing campaign training assignment 29 Oct 2024
10/29/2024 - 11/13/2024
1 Module
0 Learner

Draft
Phishing
10/28/2024 - 10/30/2024
1 Module
10 Learners

In progress
Test
10/28/2024 - 11/11/2024
4 Modules
4 Learners

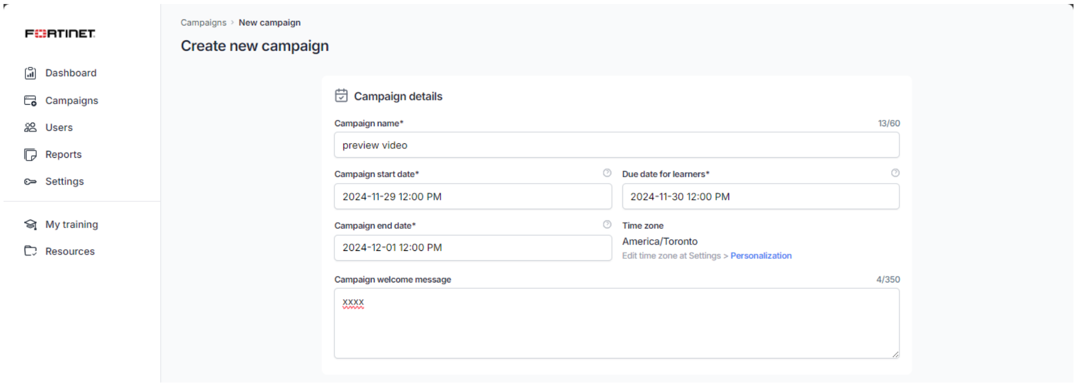
- A combination of using both filters.

Previewing individual module videos

Customers can preview video content. These previews only display the video content and not knowledge checks or quiz questions and answers.

To preview video content:

1. From the *Campaigns* navigation menu, select *+ New Campaign* button.
2. Enter something in the *Campaign details* fields, select some dates and enter any value in the *Campaign welcome message* field and select *Next*.



Campaign name* 13/60
preview video

Campaign start date*
2024-11-29 12:00 PM

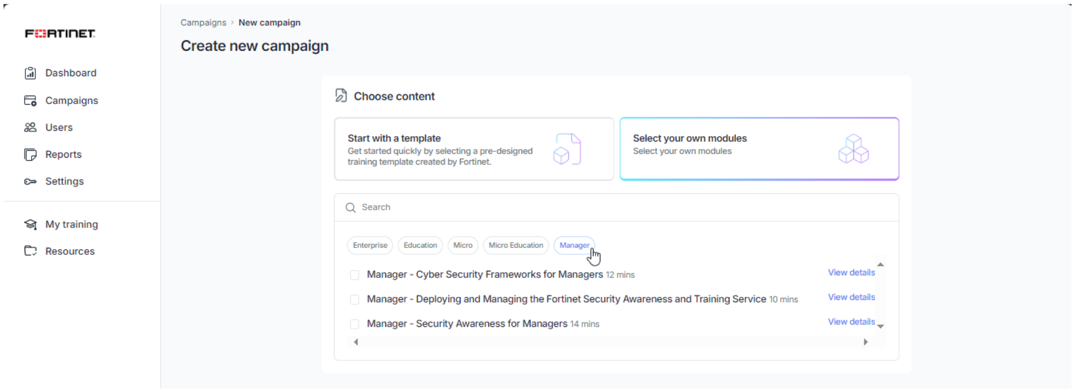
Due date for learners*
2024-11-30 12:00 PM

Campaign end date*
2024-12-01 12:00 PM

Time zone
America/Toronto
Edit time zone at Settings > Personalization

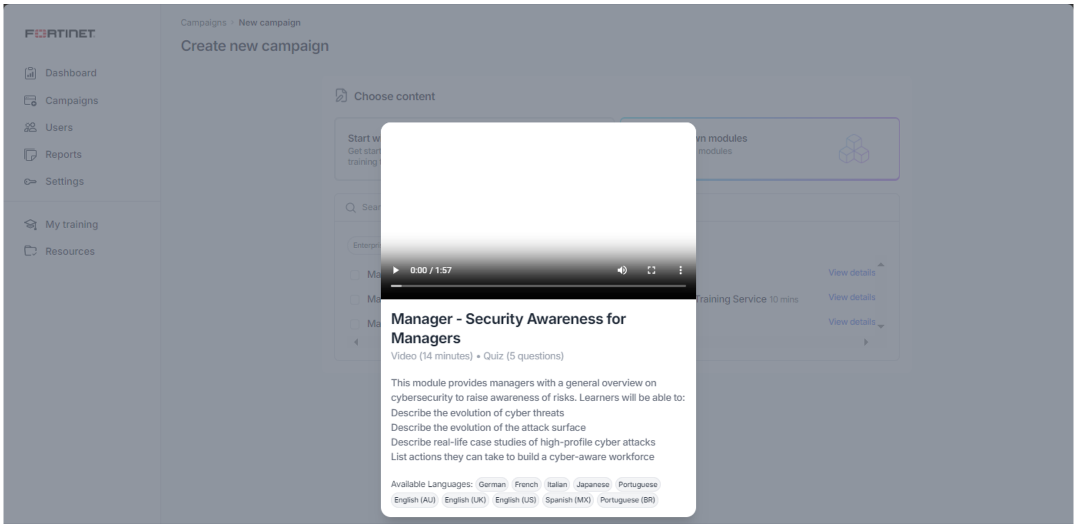
Campaign welcome message 4/350
xxxx

3. Select the *Select your own modules* button, then choose the appropriate content grouping that contains the video you would like to preview:



□ Manager - Cyber Security Frameworks for Managers 12 mins View details
□ Manager - Deploying and Managing the Fortinet Security Awareness and Training Service 10 mins View details
□ Manager - Security Awareness for Managers 14 mins View details

4. Mouse over the module you would like to preview and select the *View details* button for the module you would like to preview. The video player loads.



Manager - Security Awareness for Managers

Video (14 minutes) • Quiz (5 questions)

This module provides managers with a general overview on cybersecurity to raise awareness of risks. Learners will be able to:
Describe the evolution of cyber threats
Describe the evolution of the attack surface
Describe real-life case studies of high-profile cyber attacks
List actions they can take to build a cyber-aware workforce

Available Languages: German French Italian Japanese Portuguese English (AU) English (UK) English (US) Spanish (MX) Portuguese (BR)

You can press the play icon to preview a few minutes of the content.

You can also see additional information about the video, including the approximate length of the video, quiz information, the learning objectives, and the languages the video is currently available in.

You cannot preview the entire video or the quizzes.

When you are done viewing the window, you can click anywhere on the screen away from the player to return to the Create new campaign page.

You can now click any item in the navigation menu. The campaign will not be saved.

Campaign templates

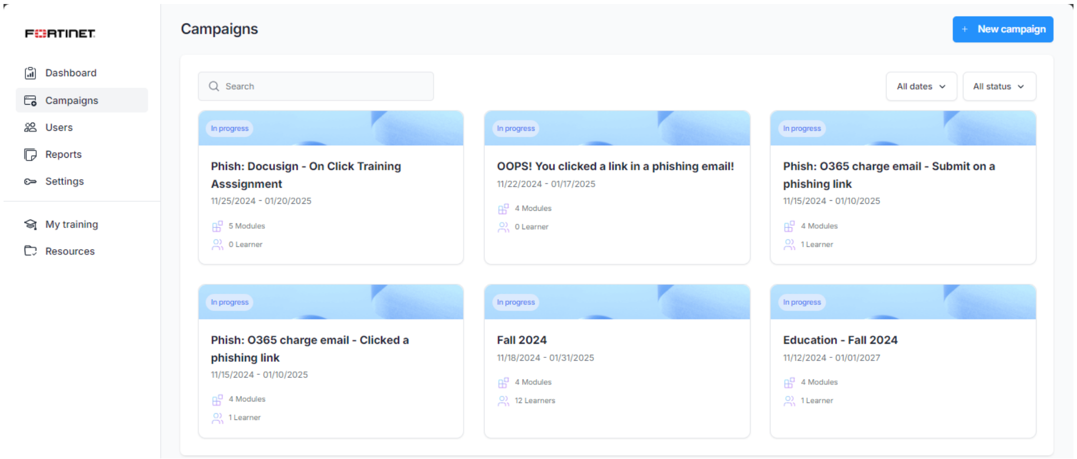
Included campaign templates (Premium level service only)

For customers that have purchased the premium level service, the Fortinet Security Awareness and Training Service comes pre-loaded with several campaign templates. These templates are logical groupings of topics customers may or may not wish to deploy. You can neither modify nor delete these templates from the system. These templates and their continent include:

Templates for Base Training	
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

Managing campaigns

All campaigns are managed from the *Campaigns* navigation menu page.



In progress
Phish: Docusign - On Click Training Asssignment
11/25/2024 - 01/20/2025
5 Modules
0 Learner

In progress
OOPS! You clicked a link in a phishing email!
11/22/2024 - 01/17/2025
4 Modules
0 Learner

In progress
Phish: O365 charge email - Submit on a phishing link
11/15/2024 - 01/10/2025
4 Modules
1 Learner

In progress
Phish: O365 charge email - Clicked a phishing link
11/15/2024 - 01/10/2025
4 Modules
1 Learner

In progress
Fall 2024
11/18/2024 - 01/31/2025
4 Modules
12 Learners

In progress
Education - Fall 2024
11/12/2024 - 01/01/2027
4 Modules
1 Learner

Campaigns should never be deleted if you wish to retain the training data. Always use the filters to access the relevant campaign data.

It is ok to delete test campaigns, pilot campaigns, campaigns created while training administrators, or any campaign that you do not wish to retain the data for.

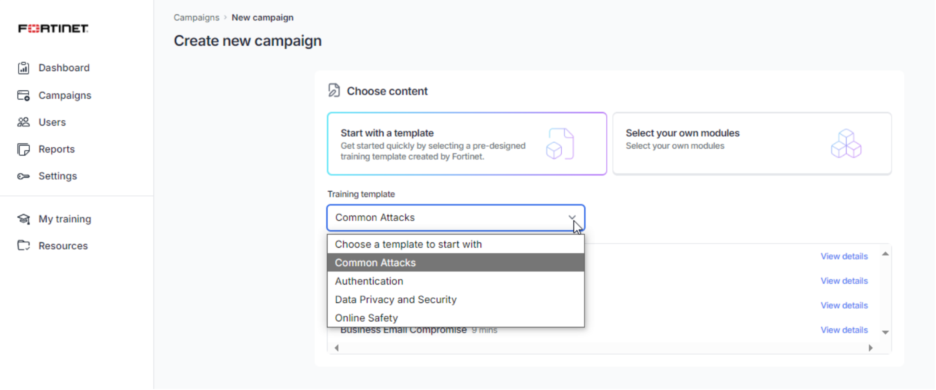
To create a campaign:

1. Select *Campaigns* from the navigation menu, then select *+ New campaign*.
2. Complete the form fields and select *Next*.

Field Name	Details
Campaign name* (mandatory)	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 learners will understand the purpose of the assignment.
Campaign start date* (mandatory)	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 learners* (mandatory)	This is the date and time that users who have not completed the entire campaign will begin to receive the overdue reminder email. 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.

Field Name	Details
Campaign end date* (mandatory)	This is the date and time that the campaign will end. When this date has been reached, users can no longer complete training. Any users who did not complete the training in time will need to be added to a supplementary campaign. 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 (verify)	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 learners 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.

3. Select the template you would like to use:
4. Click *Start with a template*, then select the *Training template*.



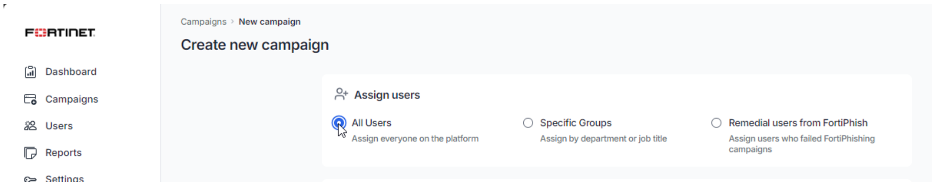
Training template: Common Attacks

5. Click *Select your own modules*, then select the module grouping button, then select the individual modules. When you are finished selecting modules, click *Next*.

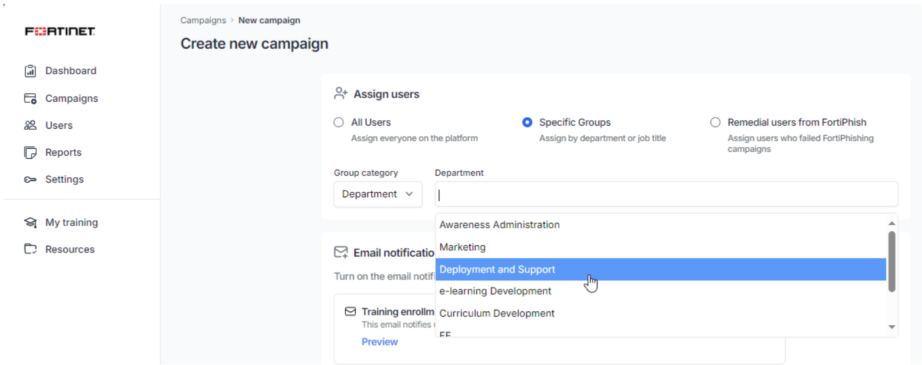
You can preview modules and get more information about the contents and languages supported by clicking on the *View details* link for each module.

6. Reorder the content (if desired) by selecting the dots next to the name and dragging the module to the correct position.
7. Click *Next*.
8. Choose if this campaign will be assigned to All Users, Specific Groups or Remedial users from FortiPhish:

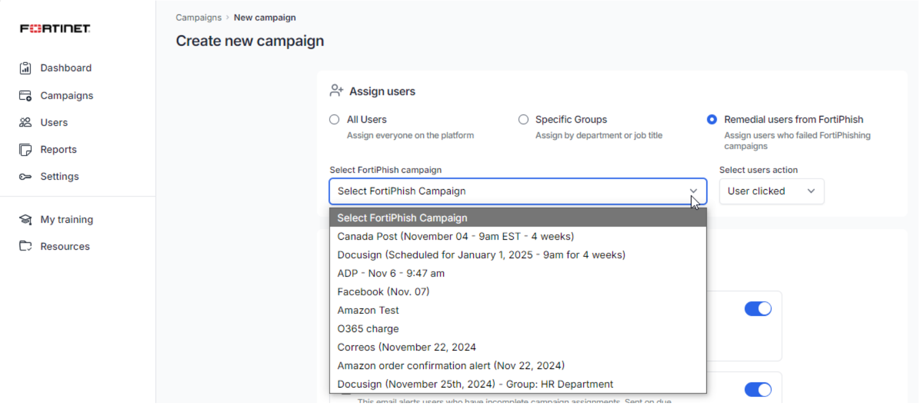
- If you select *All Users*, every user will receive the training assignment.


FORTINET
Dashboard
Campaigns
Users
Reports
Settings
Campaigns › New campaign
Create new campaign
Assign users
● All Users
Assign everyone on the platform
○ Specific Groups
Assign by department or job title
○ Remedial users from FortiPhish
Assign users who failed FortiPhishing campaigns

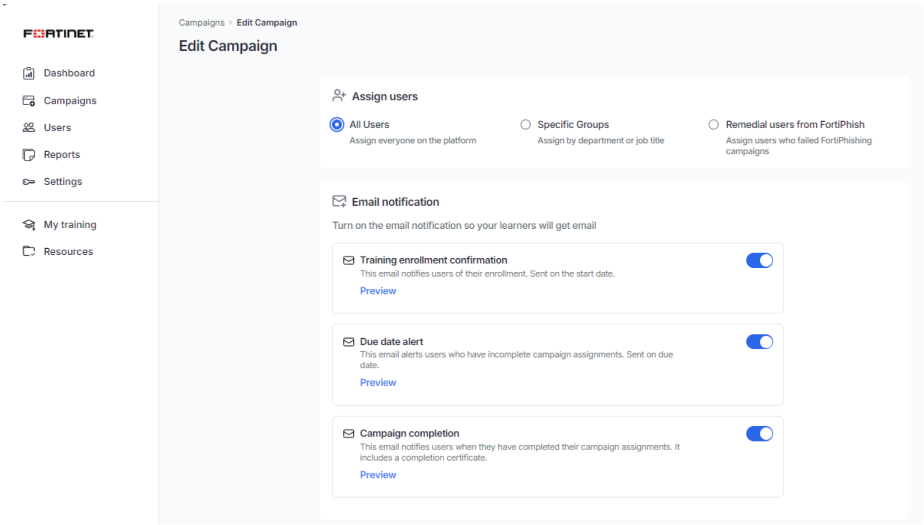
- If you select *Specific Groups*, you will be able to assign to users based on your imported department and title unique values.



- If you select *Remedial users from FortiPhish*, you will be able to choose the applicable FortiPhish campaign and user action.


FORTINET
Dashboard
Campaigns
Users
Reports
Settings
My training
Resources
Campaigns › New campaign
Create new campaign
Assign users
○ All Users
Assign everyone on the platform
○ Specific Groups
Assign by department or job title
● Remedial users from FortiPhish
Assign users who failed FortiPhishing campaigns
Select FortiPhish campaign
Select FortiPhish Campaign
Select users action
User clicked
Select FortiPhish Campaign
Canada Post (November 04 - 9am EST - 4 weeks)
Docusign (Scheduled for January 1, 2025 - 9am for 4 weeks)
ADP - Nov 6 - 9:47 am
Facebook (Nov. 07)
Amazon Test
O365 charge
Correos (November 22, 2024
Amazon order confirmation alert (Nov 22, 2024)
Docusign (November 25th, 2024) - Group: HR Department

9. You may choose to turn off the email notifications:



Edit Campaign

Assign users

● All Users
Assign everyone on the platform

○ Specific Groups
Assign by department or job title

○ Remedial users from FortiPhish
Assign users who failed FortiPhishing campaigns

Email notification

Turn on the email notification so your learners will get email

Training enrollment confirmation
This email notifies users of their enrollment. Sent on the start date.

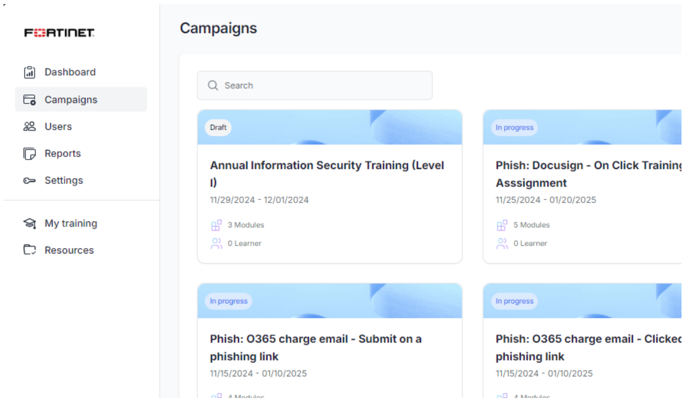
Due date alert
This email alerts users who have incomplete campaign assignments. Sent on due date.

Campaign completion
This email notifies users when they have completed their campaign assignments. It includes a completion certificate.

Reasons you may wish to disable one or more notifications:

- You plan to send the invitation emails from a different email client.
- You plan to send the reminders from a different email client.
- The campaign assignment is tied to a phishing campaign and you do not want to send a certificate and completion email for phishing assignments.

10. Now you can launch the campaign by selecting the *Launch campaign* button. The campaign will remain in a *Scheduled* state until the configured start date and time are reached at which point its status will change to *In progress*. If you want to save the campaign as a draft, select the *Cancel* button and an option to *Save as draft* or *Cancel* will be presented.
11. If you save as draft, the campaign will appear as a *Draft* on the *Campaigns* page.



Campaigns

Draft
Annual Information Security Training (Level I)
11/29/2024 - 12/01/2024
3 Modules
0 Learner

In progress
Phish: Docusign - On Click Training Asssignment
11/25/2024 - 01/20/2025
5 Modules
0 Learner

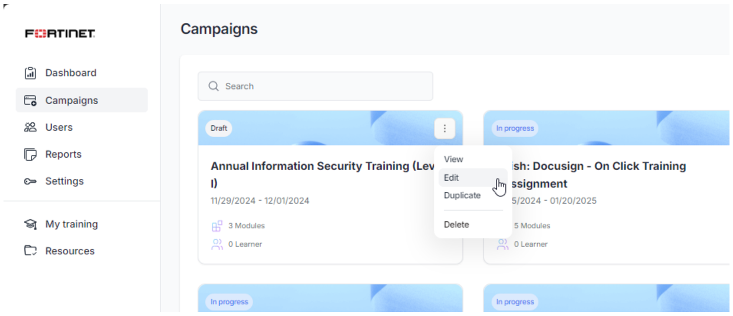
In progress
Phish: O365 charge email - Submit on a phishing link
11/15/2024 - 01/10/2025
4 Modules

In progress
Phish: O365 charge email - Clicked phishing link
11/15/2024 - 01/10/2025
4 Modules

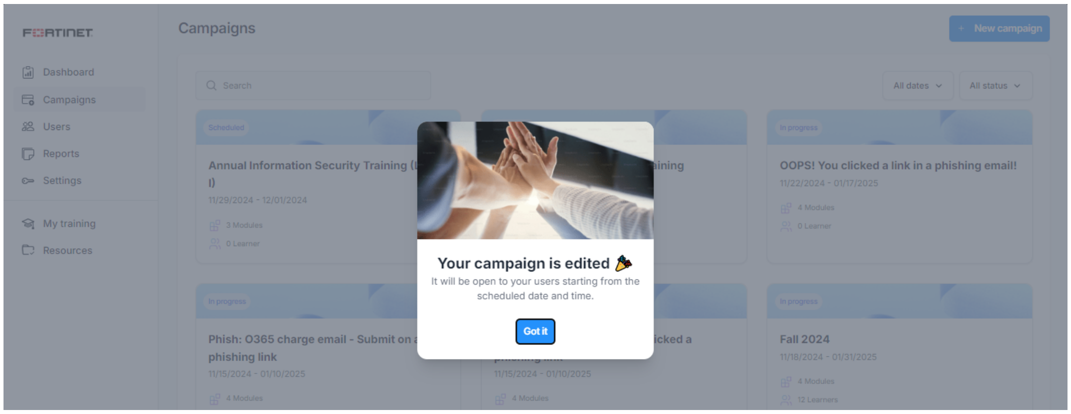
Administrators can edit campaigns from the *Campaigns* page. The status of the campaign will dictate what can be edited.

To edit a campaign:

1. Select *Campaigns* from the navigation menu, filter the campaigns to access the desirable campaign, then mouse over the campaign and select the three dots in the upper right hand corner and select *Edit*.



2. Move through the wizard and make any necessary modifications to the campaign.
3. When you get to the final page, select *Launch Campaign*. A confirmation message is displayed.

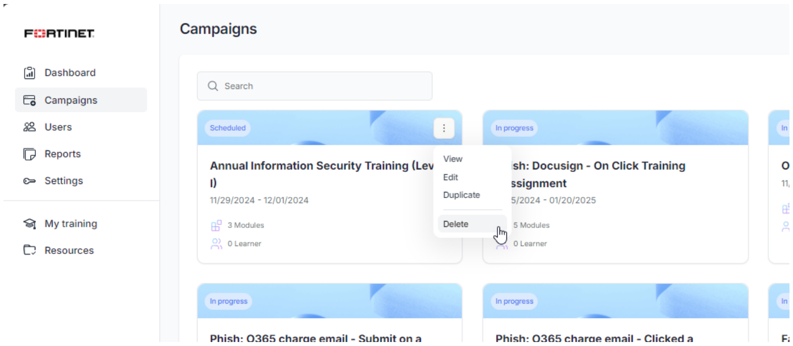

Campaigns
New campaign
All dates
All status
Your campaign is edited
It will be open to your users starting from the scheduled date and time.
Got it
OOPS! You clicked a link in a phishing email!
Fall 2024
Phish: O365 charge email - Submit on a phishing link

To delete a campaign:

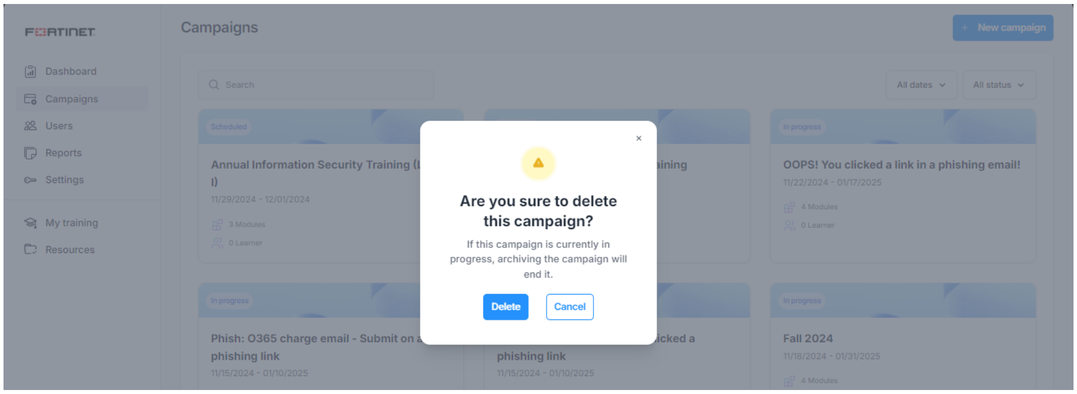
Campaigns should never be deleted if you wish to retain the training data. Always use the filters to access the relevant campaign data.

It is ok to delete test campaigns, pilot campaigns, campaigns created while training administrators, or any campaign that you do not wish to retain the data for.

1. Select *Campaigns* from the navigation menu.
2. Filter the campaigns to access the desirable campaign.
3. Mouse over the campaign and select the three dots in the upper right hand corner and select *Delete*.


FURTINET
Dashboard
Campaigns
Users
Reports
Settings
My training
Resources
Campaigns
Search
Scheduled
Annual Information Security Training (Lev l)
11/29/2024 - 12/01/2024
View
Edit
Duplicate
Delete
In progress
sh: Docusign - On Click Training ssignment
Phish: O365 charge email - Submit on a
Phish: O365 charge email - Clicked a

A confirmation dialogue is presented.



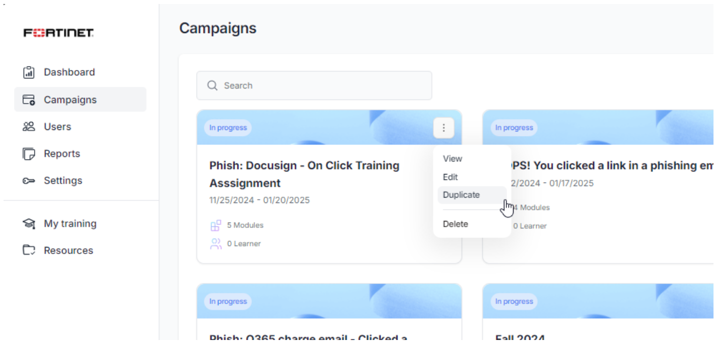
Are you sure to delete this campaign?

If this campaign is currently in progress, archiving the campaign will end it.

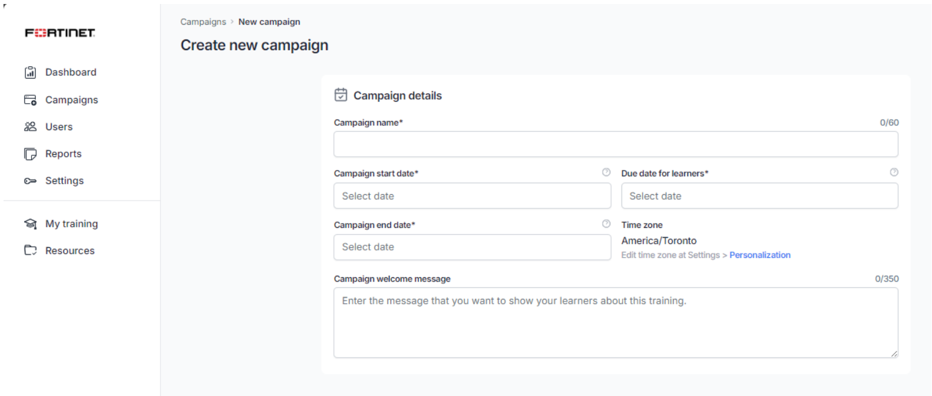
Organizations may wish to re-use campaigns. For example, some campaigns are used to meet annual or more frequent training requirements. Organizations may also reuse campaigns when assigning training during regular phishing campaigns. Administrators can duplicate any existing campaign in the system. Only the content is retained from the previous campaign. Administrators must fill out all other fields (Campaign name, dates, comments, and so on).

To duplicate a campaign:

1. Select *Campaigns* from the navigation menu.
2. Filter the campaigns to access the desirable campaign.
3. Mouse over the campaign and select the three dots in the upper right hand corner and select *Duplicate*.



The campaign wizard is presented.



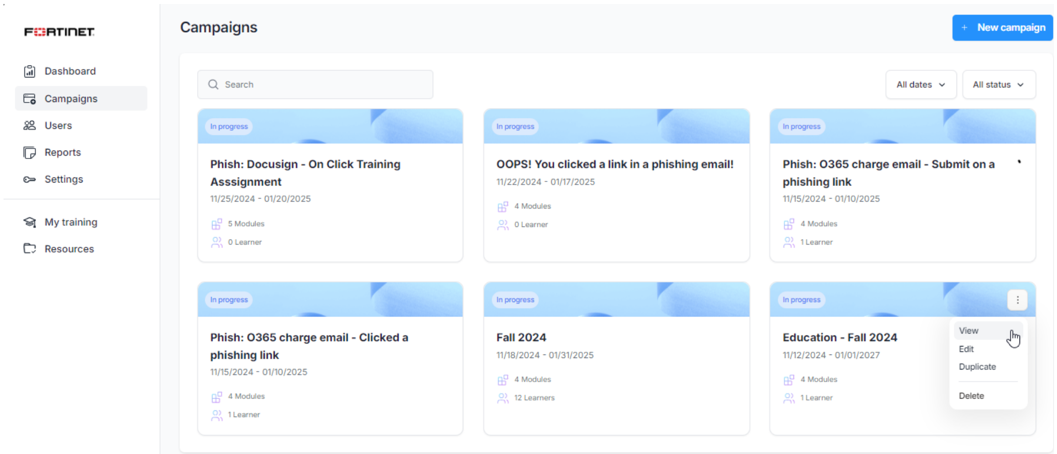
4. Complete the wizard and save or launch the campaign.

Scheduling training progress reports

Administrators have the option to create and schedule training progress reports. These reports are high level and do not contain learner status, however, they do give a high level overview of the progress of a campaign.

To schedule training progress reports:

1. Select *Campaigns* from the navigation menu.
2. Filter the campaigns to access the desirable campaign.
3. Mouse over the campaign and select the three dots in the upper right hand corner and select *View*.



In progress
Phish: Docusign - On Click Training Asssignment
11/25/2024 - 01/20/2025
5 Modules
0 Learner

In progress
OOPS! You clicked a link in a phishing email!
11/22/2024 - 01/17/2025
4 Modules
0 Learner

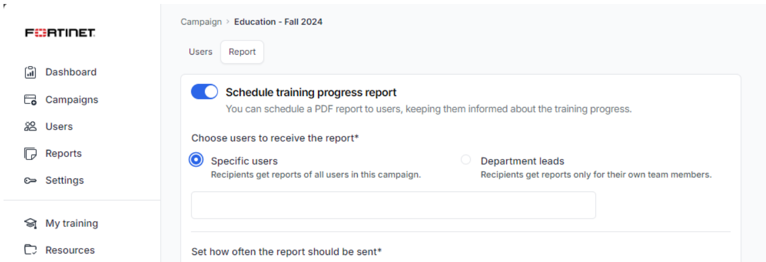
In progress
Phish: O365 charge email - Submit on a phishing link
11/15/2024 - 01/10/2025
4 Modules
1 Learner

In progress
Phish: O365 charge email - Clicked a phishing link
11/15/2024 - 01/10/2025
4 Modules
1 Learner

In progress
Fall 2024
11/18/2024 - 01/31/2025
4 Modules
12 Learners

In progress
Education - Fall 2024
11/12/2024 - 01/01/2027
4 Modules
1 Learner

4. Select the *Report* tab, then enable *Schedule training progress report*.
5. Choose whether to send to *Specific Users* or *Department Leads* by selecting the appropriate *Send To* option button selection.



Schedule training progress report
You can schedule a PDF report to users, keeping them informed about the training progress.

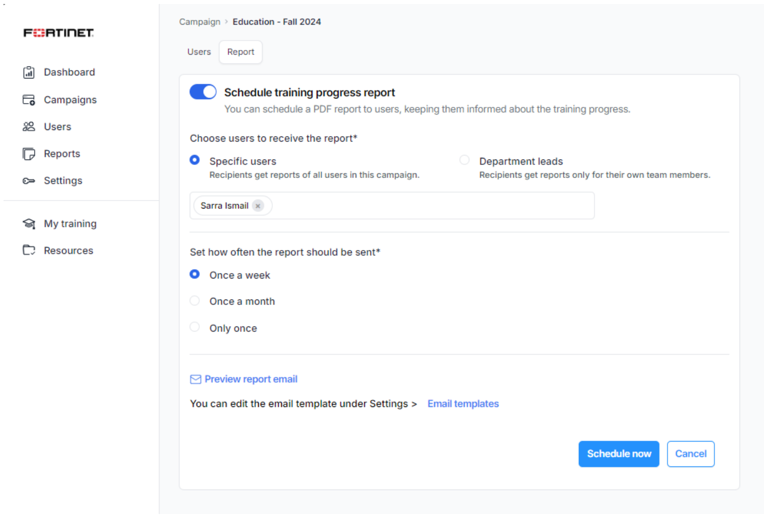
Choose users to receive the report*

● Specific users
Recipients get reports of all users in this campaign.

○ Department leads
Recipients get reports only for their own team members.

Set how often the report should be sent*

6. Select the appropriate option button under *Set how often the report should be sent*.



Schedule training progress report

You can schedule a PDF report to users, keeping them informed about the training progress.

Choose users to receive the report*

● Specific users
Recipients get reports of all users in this campaign.

○ Department leads
Recipients get reports only for their own team members.

Sarra Ismail ×

Set how often the report should be sent*

● Once a week

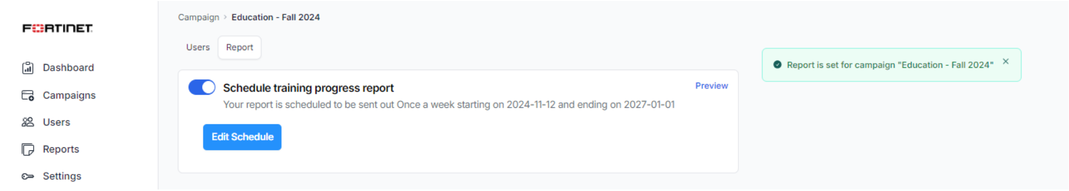
○ Once a month

○ Only once

Preview report email

You can edit the email template under Settings > Email templates

7. Click *Schedule now*. A confirmation message is displayed:



Report is set for campaign "Education - Fall 2024" ×

Schedule training progress report

Your report is scheduled to be sent out Once a week starting on 2024-11-12 and ending on 2027-01-01

Managing learners after a campaign has been launched

When creating a campaign, learners are assigned by the values mapped to the Title and Department data provided through a .csv upload or mapped attributes in the LDAP Directory.

After launching a campaign, admins may be required to add new users or remove existing users assigned to a campaign. They may also want to see more detail about which users have not yet started, have partially completed, have fully completed or are overdue on their training assignments.

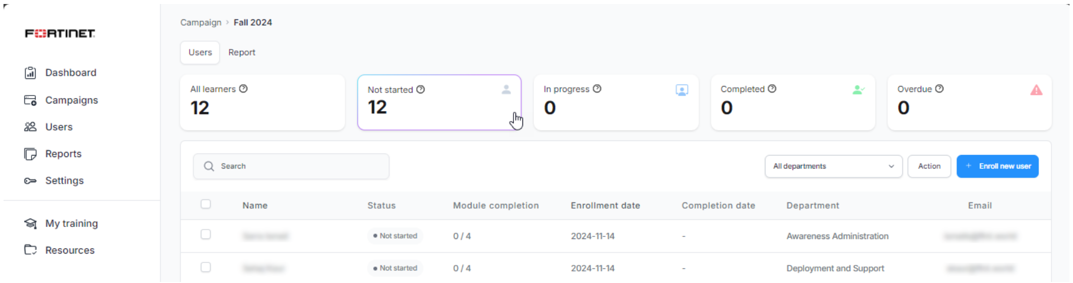
You can use the *Manage Learners* page to achieve these goals and export current user statistics without having to configure and run a report.

To access the Manage Learners Console:

1. Select *Campaigns* from the navigation menu.
2. Filter the campaigns to access the desirable campaign.
3. Mouse over the campaign and select the three dots in the upper right hand corner and select *View*.

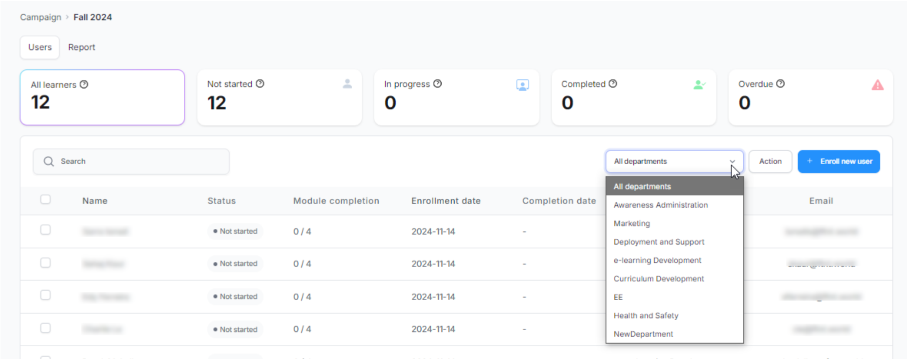
From this page, admins can:

- Sort users by selecting one of the sort buttons at the top (*All learners*, *Not started*, *In progress*, *Completed* and *Overdue*).



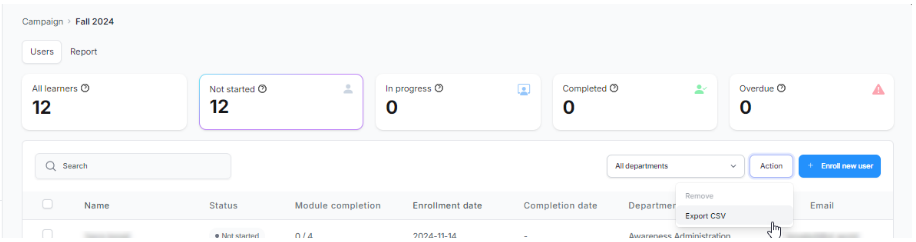
☐	Name	Status	Module completion	Enrollment date	Completion date	Department	Email
☐	[redacted]	● Not started	0 / 4	2024-11-14	-	Awareness Administration	[redacted]
☐	[redacted]	● Not started	0 / 4	2024-11-14	-	Deployment and Support	[redacted]

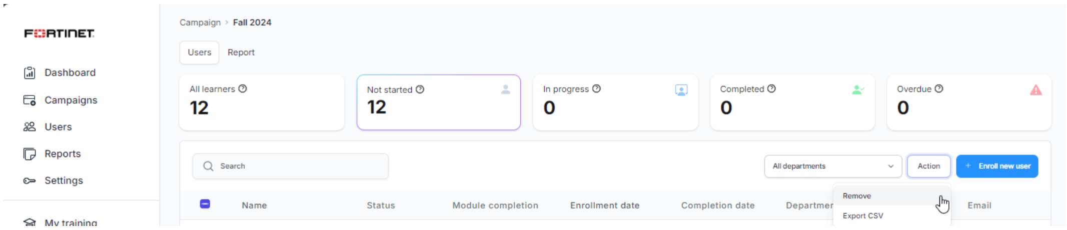
- Filter data for *All departments* or a single department.



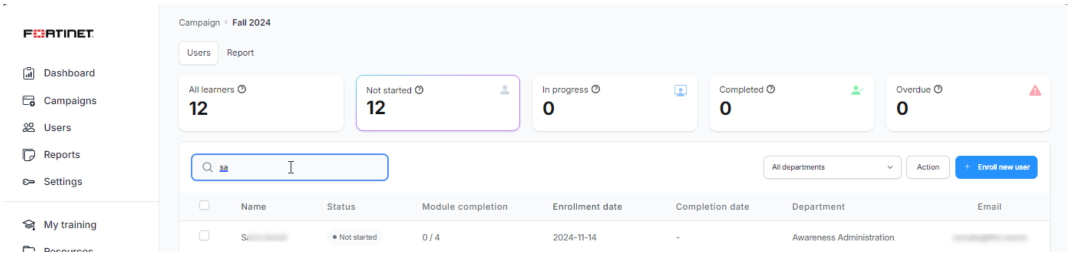
☐	Name	Status	Module completion	Enrollment date	Completion date	Email
☐	[redacted]	● Not started	0 / 4	2024-11-14	-	[redacted]
☐	[redacted]	● Not started	0 / 4	2024-11-14	-	[redacted]
☐	[redacted]	● Not started	0 / 4	2024-11-14	-	[redacted]
☐	[redacted]	● Not started	0 / 4	2024-11-14	-	[redacted]

- Export the user list from the sorted users by clicking *Export CSV* option after clicking *Action*.



- Enroll new users into the campaign after it has been launched. To perform this action, you must select the *+Enroll new user* button in the upper right corner.
- Remove users from the campaign by selecting the check box(es) next to users, then selecting the *Remove* option after clicking *Action*.
- 

- Search for learners enrolled in the campaign by department, name, email or title.



Search: sa

☐	Name	Status	Module completion	Enrollment date	Completion date	Department	Email
☐	S[redacted]	● Not started	0 / 4	2024-11-14	-	Awareness Administration	[redacted]

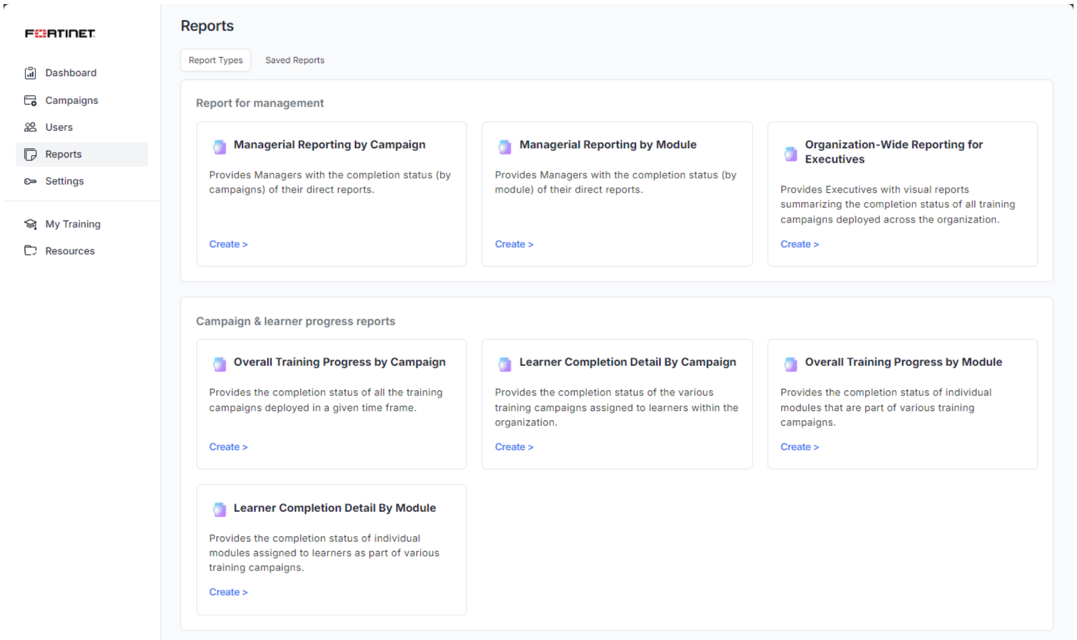
- Sort user information by selecting the sort buttons in the *Name* (sorts by first name) and *Enrollment* date column headers.

Reports

Reports allow Administrators to take a snapshot of Users progress in the learning Campaign. To create a report, Administrators need should understand:

- What type of information they would like to report on.
- The audience that will be sent and view the report data as well as the format it will be presented in.
- The frequency (schedules) of the report distribution.
- Who should be able to access the report data in the Admin portal.

The system comes with “canned” reports already pre-loaded. These are the most common types of reports customers and partners may run to manage the user learning campaigns.



Reports

Report for management

Managerial Reporting by Campaign
Provides Managers with the completion status (by campaigns) of their direct reports.
Create >

Managerial Reporting by Module
Provides Managers with the completion status (by module) of their direct reports.
Create >

Organization-Wide Reporting for Executives
Provides Executives with visual reports summarizing the completion status of all training campaigns deployed across the organization.
Create >

Campaign & learner progress reports

Overall Training Progress by Campaign
Provides the completion status of all the training campaigns deployed in a given time frame.
Create >

Learner Completion Detail By Campaign
Provides the completion status of the various training campaigns assigned to learners within the organization.
Create >

Overall Training Progress by Module
Provides the completion status of individual modules that are part of various training campaigns.
Create >

Learner Completion Detail By Module
Provides the completion status of individual modules assigned to learners as part of various training campaigns.
Create >

Included reports

Reports for management

- Managerial Reporting by Campaign
  - Provides Managers with the completion status (by campaigns) of their direct reports.
- Managerial Reporting by Module
  - Provides Managers with the completion status (by module) of their direct reports.
- Organization-Wide Reporting for Executives

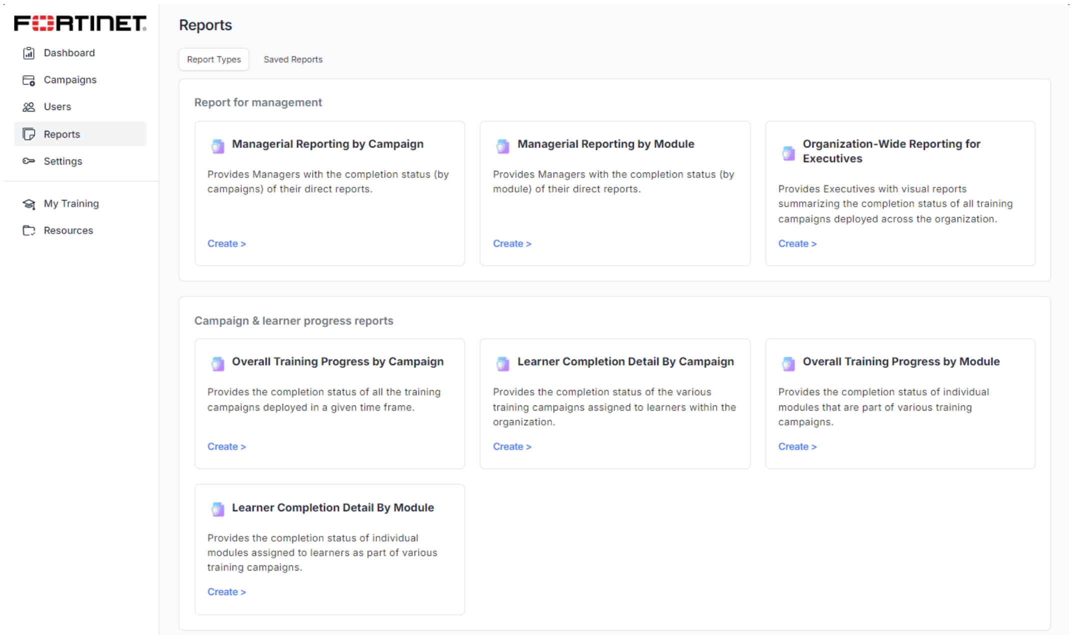
- Provides Executives with visual reports summarizing the completion status of all training campaigns deployed across the organization.

Campaign & learner progress reports

- Overall Training Progress by Campaign
  - Provides the completion status of all the training campaigns deployed in a given time frame.
- Learner Completion Detail By Campaign
  - Provides the completion status of the various training campaigns assigned to learners within the organization.
- Overall Training Progress by Module
  - Provides the completion status of individual modules that are part of various training campaigns.
- Learner Completion Detail By Module
  - Provides the completion status of individual modules assigned to learners as part of various training campaigns.

To create a new custom report:

1. Select *Reports* from the navigation menu.
2. Click *Create* for the type of report you wish to create.



Report for management

Managerial Reporting by Campaign
Provides Managers with the completion status (by campaigns) of their direct reports.
Create >

Managerial Reporting by Module
Provides Managers with the completion status (by module) of their direct reports.
Create >

Organization-Wide Reporting for Executives
Provides Executives with visual reports summarizing the completion status of all training campaigns deployed across the organization.
Create >

Campaign & learner progress reports

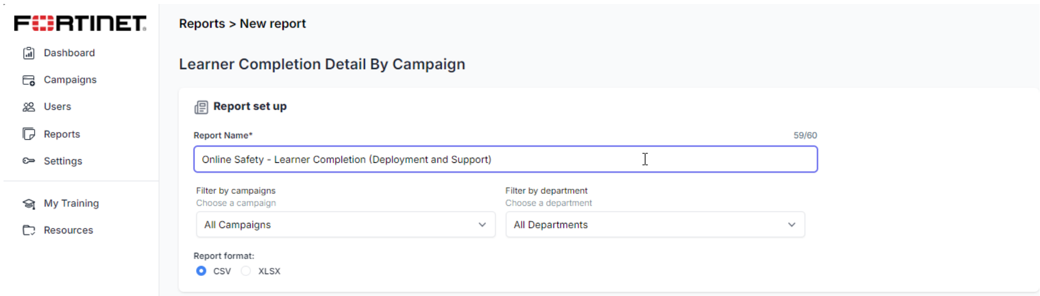
Overall Training Progress by Campaign
Provides the completion status of all the training campaigns deployed in a given time frame.
Create >

Learner Completion Detail By Campaign
Provides the completion status of the various training campaigns assigned to learners within the organization.
Create >

Overall Training Progress by Module
Provides the completion status of individual modules that are part of various training campaigns.
Create >

Learner Completion Detail By Module
Provides the completion status of individual modules assigned to learners as part of various training campaigns.
Create >

3. Give your report a meaningful name.



Reports > New report

Learner Completion Detail By Campaign

Report set up

Report Name* 59/60

Online Safety - Learner Completion (Deployment and Support)

Filter by campaigns
Choose a campaign
All Campaigns

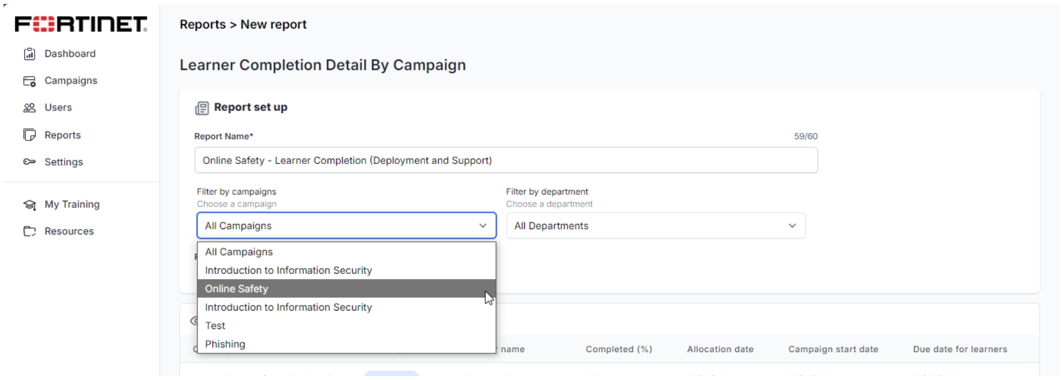
Filter by department
Choose a department
All Departments

Report format:
● CSV ○ XLSX

In the above example, the name contains: <campaign name> - <report type> (<department>)

It is important that you use good naming conventions so that when you create a report, you can recognize what the report is for (reporting on). You should include the type of report you selected, the campaign it is tied to and the department (if you wish to create a separate report to be emailed to a specific person for their staff). You can also report on all data, export as an xlsx and then extract the data department by department to manually send the report to the appropriate department manager.

4. From the *Filter by campaigns* dropdown, select the Campaign you would like to create the report for.



Reports > New report

Learner Completion Detail By Campaign

Report set up

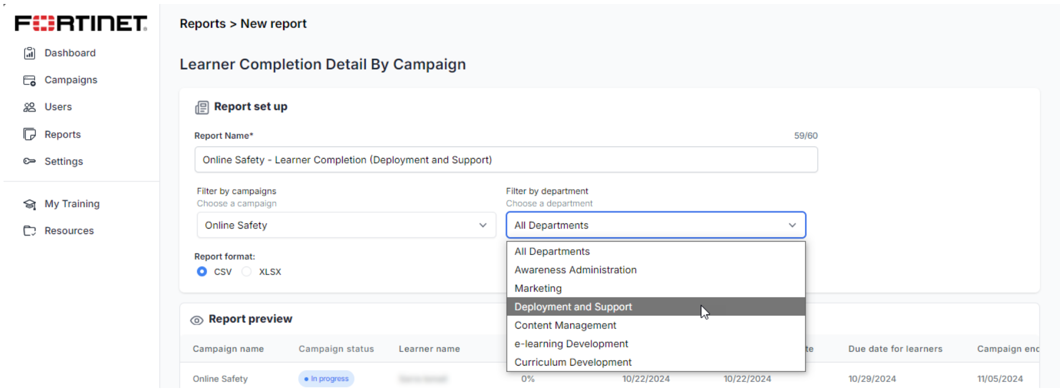
Report Name* 59/60

Online Safety - Learner Completion (Deployment and Support)

Filter by campaigns
Choose a campaign
All Campaigns

Filter by department
Choose a department
All Departments

5. If you wish to create a report department by department, from the *Filter by department* dropdown, select the department you wish to create the report for, or report for all departments:



Reports > New report

Learner Completion Detail By Campaign

Report set up

Report Name* 59/60

Online Safety - Learner Completion (Deployment and Support)

Filter by campaigns
Choose a campaign
Online Safety

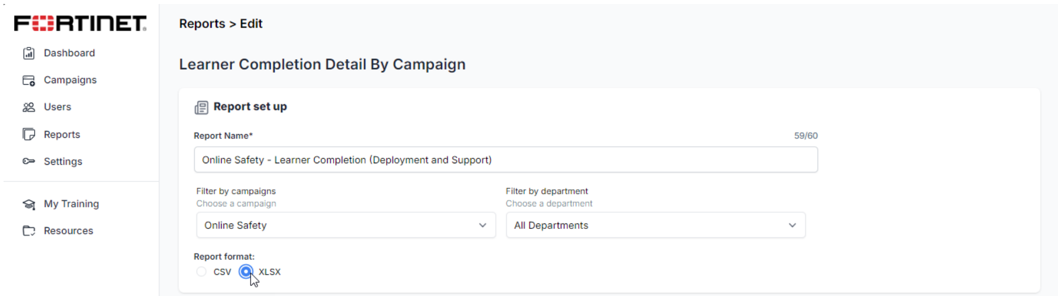
Filter by department
Choose a department
All Departments

Report format:
● CSV ○ XLSX

Report preview

Campaign name	Campaign status	Learner name				te	Due date for learners	Campaign enc
Online Safety	● In progress	[redacted]	0%	10/22/2024	10/22/2024		10/29/2024	11/05/2024

6. Choose the format you would like the report to be sent in.



Reports > Edit

Learner Completion Detail By Campaign

Report set up

Report Name* 59/60

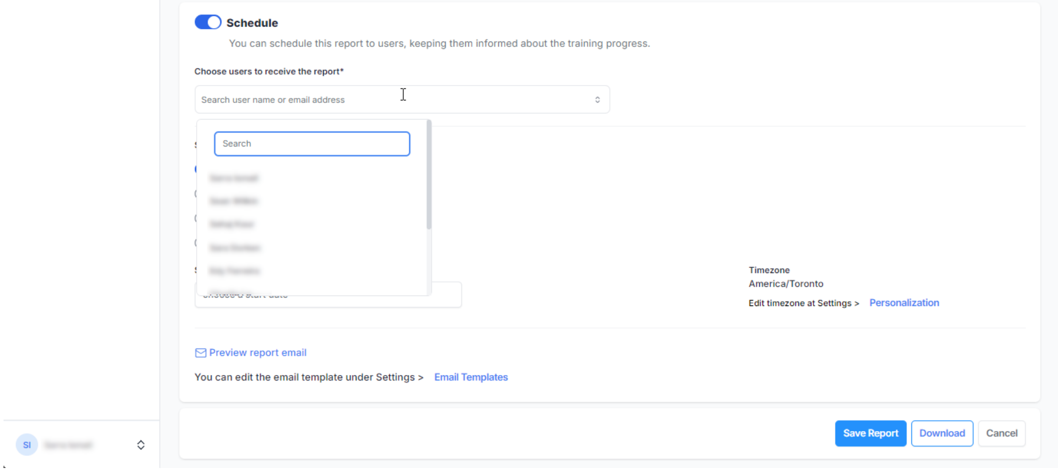
Online Safety - Learner Completion (Deployment and Support)

Filter by campaigns
Choose a campaign
Online Safety

Filter by department
Choose a department
All Departments

Report format:
○ CSV ● XLSX

7. If you wish to just save the report and not schedule it, then click *Save Report*, otherwise select *Schedule* to set a schedule.
8. If you selected the *Save* button, a confirmation message is displayed and the new report appears under the *Saved Reports* tab.
9. If scheduling the report, after enabling *Schedule*, complete the *Schedule* form.
10. Search and add users who should receive the report using the *Send to* search field.



Schedule

You can schedule this report to users, keeping them informed about the training progress.

Choose users to receive the report*

Search user name or email address

Search

[redacted]

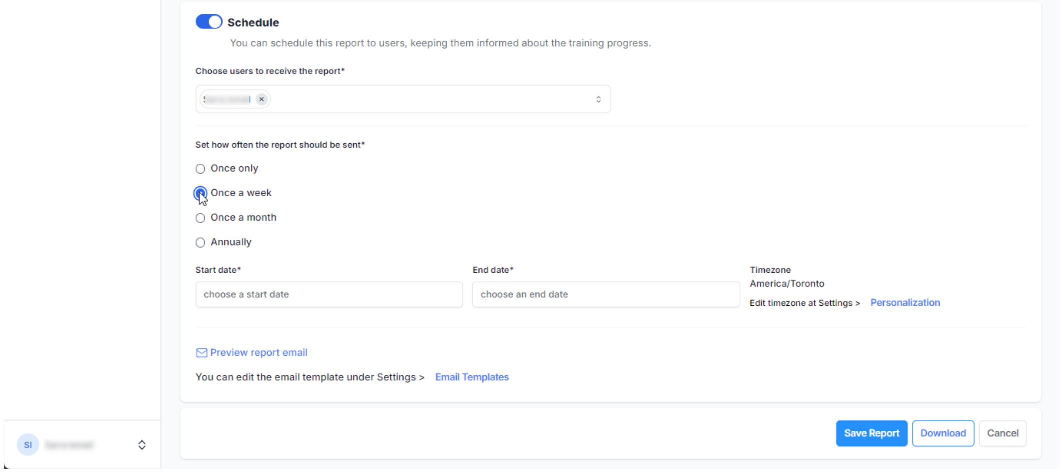
Timezone
America/Toronto

Edit timezone at Settings > Personalization

Preview report email

You can edit the email template under Settings > Email Templates

11. Select the frequency the report should be sent from the *Set how often the report should be sent* option.



Schedule

You can schedule this report to users, keeping them informed about the training progress.

Choose users to receive the report*

[redacted]

Set how often the report should be sent*

○ Once only
● Once a week
○ Once a month
○ Annually

Start date*
choose a start date

End date*
choose an end date

Timezone
America/Toronto

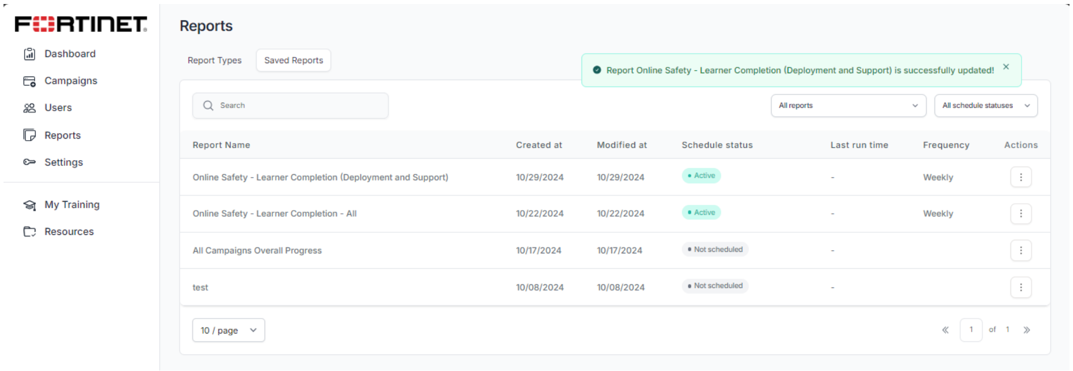
Edit timezone at Settings > Personalization

Preview report email

You can edit the email template under Settings > Email Templates

12. Enter the start and end dates for sending the report. The start date is typically the start date (end of day hour, such as 6 p.m.) and the end date should be the last day of the campaign (i.e. the campaign end date, not the learner due date).

13. Verify your time zone is correctly set. The report will be sent at the times specified in the configured time zone.
14. Click *Save Report*.
    You should receive a confirmation message and see the new report listed under the *Saved Reports* tab.



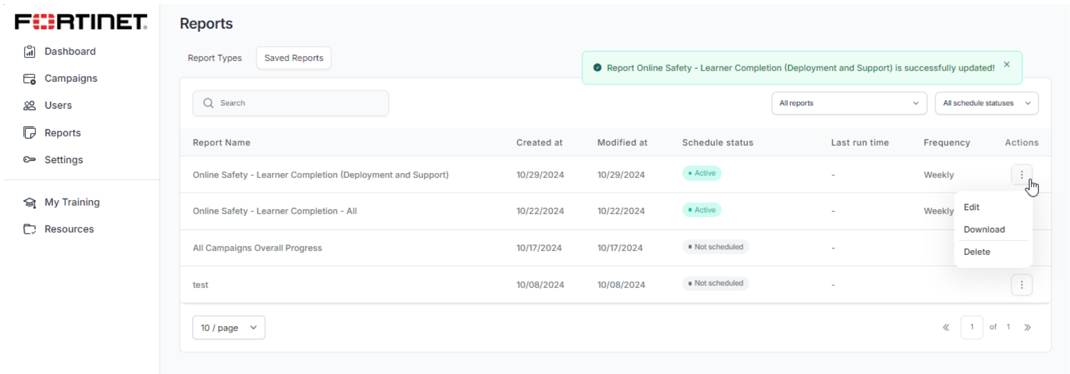
Report Online Safety - Learner Completion (Deployment and Support) is successfully updated! ×

Report Name	Created at	Modified at	Schedule status	Last run time	Frequency	Actions
Online Safety - Learner Completion (Deployment and Support)	10/29/2024	10/29/2024	● Active	-	Weekly	⋮
Online Safety - Learner Completion - All	10/22/2024	10/22/2024	● Active	-	Weekly	⋮
All Campaigns Overall Progress	10/17/2024	10/17/2024	● Not scheduled	-		⋮
test	10/08/2024	10/08/2024	● Not scheduled	-		⋮

You can edit, download or delete a report at any time by visiting the *Saved Reports* tab under the *Reports* navigation menu item.

To manage a saved report:

1. Click the *Actions* button to the right of the report, then select the *Edit*, *Download* or *Delete* option from the list.



Report Online Safety - Learner Completion (Deployment and Support) is successfully updated! ×

Report Name	Created at	Modified at	Schedule status	Last run time	Frequency	Actions
Online Safety - Learner Completion (Deployment and Support)	10/29/2024	10/29/2024	● Active	-	Weekly	⋮
Online Safety - Learner Completion - All	10/22/2024	10/22/2024	● Active	-	Weekly	
All Campaigns Overall Progress	10/17/2024	10/17/2024	● Not scheduled	-		
test	10/08/2024	10/08/2024	● Not scheduled	-		⋮

You can also delete the report by selecting the *Delete* link.

Different reports have different configuration options than the example provided above. Best practice is to always give the report a meaningful name so that it is clear what data the report includes. Never use the default name which is just the report type with a sequential number at the end as this will make it difficult to determine what data is included in the report.

Integrating with FortiPhish

Customers who purchase both FortiPhish Service and the Fortinet Security Awareness and Training Service can integrate the two services.

For more information about FortiPhish, see Phishing Simulation Service.

Customers can create training campaigns that can be assigned to users who trigger a phishing event. For example, they may wish to assign one or more training modules when someone clicks a link in a phishing email, replies to a phishing email, or, submits their username and password to a site after clicking a link in a phishing email. Customers can assign different, additional training for each event the user performs.

To do this, there are a few steps:

- Create and schedule a FortiPhish campaign.
- Create and schedule a Security Awareness and Training Campaign for each phishing event (User clicked, User replied, User submitted) you wish to assign training to.
- Create a report for the campaign

Before completing the following steps, customers must first complete the configuration of the FortiPhish service:

- Verify each email domain the customer wishes to send phishing emails to by creating a DNS TXT record for each. This is a separate configuration than the DNS TXT records created in the Security Awareness and Training Service. See Adding domains.
- Import the users that customers wish to send phishing emails to. This is a separate user import than the DNS user import performed in the Security Awareness and Training Service. You can import users into FortiPhish using the example.csv provided in the FortiPhish service. You cannot use the .csv file used to import users in Fortinet Security Awareness and Training Service, although the data may be cut and paste between the two .csv files. You may also import and sync users through LDAP/LDAPS or Azure Active Directory for the FortiPhish service. Security Awareness and Training Service currently does not support Azure Active Directory user imports/syncs. See Recipients.

For help configuring FortiPhish and creating phishing campaigns, see the FortiPhish Administration Guide.

If you need more technical assistance configuring FortiPhish or creating campaigns, open a ticket with the FortiPhish service team. See How to open a helpdesk ticket for the FortiPhish service.

You can also request assistance configuring the service and setting up campaigns by opening a support ticket from within the Security Awareness and Training Service *Get Support* link under the avatar menu or by sending an email to infosec_awareness@fortinet.com.

Creating a FortiPhish Campaign:

FortiPhish provides online help for creating phishing campaigns. See Creating campaigns.

If you wish to tie a Security Awareness and Training Service campaign to phishing user email events, ensure you mark down the following:

- The name you give to the phishing campaign.
- The start date and time (hour) and time zone.
- The end date and time (hour) and time zone. You can determine this from the number of weeks you configure the phishing campaign for. It will be 1-4 weeks after the start date and time, and time zone offset.

To create a FortiPhish campaign:

1. Log in to the FortiPhish service from the FortiCloud header (if logged in as the Tenant Administrator), or, log in from support.fortinet.com. You must have a registered support account and it must be added to the master support account that owns the license.
2. From the navigation menu, select *Campaigns*, then click *Create Campaign*.
3. Use the headers to find the appropriate template, or, select *Custom* in the navigation menu to create your own.
4. Make any modifications to the template that you require and click *Next*.

   Activate On Click Training must be set to *No* to assign training in the Security Awareness and Training Service platform. If set to *Yes*, you can choose from pre-defined training videos available in the system. The *Yes* setting is typically used by customers who do not use the Security Awareness and Training Service.

   For information on what each of the settings mean when creating a campaign, see Creating Campaigns.

5. Give your phishing campaign a meaningful name. You may also wish to date stamp or add other information about the campaign and make any desired changes to the *Campaign Name*, *Sender Name*, *Sender Email*, and *SMTP Gateway Server* fields and click *Next*.

   Sending a test email is recommended before launching a campaign.

   Add the FortiPhish's mailserver address (smtp.fortiphish.com) to your gateway safe list to allow incoming email traffic.

   Add noreply@ftnt.info or ftnt.info to your safe sender list to allow incoming Security Awareness and Training Service email traffic (campaign related emails).

   Add FortiPhish's website URLs (smtp.fortiphish.com, fortiphish.com, api.fortiphish.com) to the browser allowlist.

6. Select the desired *Recipients* by selecting one of the groups you created during user import, then click *Next*.
7. Select *Scheduled* from the *Campaign Schedule* drop down and configure the other fields.
8. Click *Next*.

   Give yourself enough time so that you can create the associated training campaigns. Typically, phishing campaigns are scheduled days or weeks in advance.

   Take note of the start date and time as well as the timezone as you will need to enter these values later, when you configure the training campaign assignment.

   You will also need to mark down the duration so that you can match the Learner Due Date for the training campaign assignment.

9. Choose the frequency of emails and then click *Start campaign*.

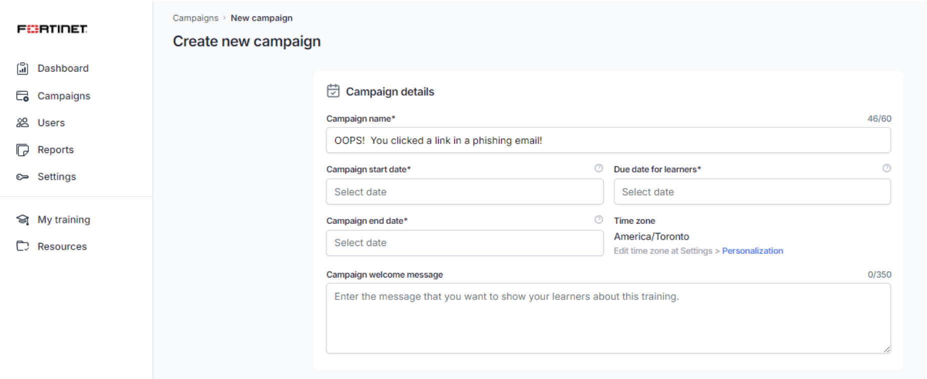
   You have successfully scheduled your phishing campaign.

It can take up to 30 minutes for the phishing campaign to be available on the *Remediation* page of the Fortinet Security Awareness and Training Service.

All campaigns should be scheduled for future launching to allow for this delay (at least 2 hours before hand). This will give you time to complete configuration on the Fortinet Security Awareness and Training Service.

To schedule the event training campaign in Security Awareness and Training Service:

1. Select *Campaigns* from the navigation menu, then select *New campaign*.
2. Enter a meaningful name in the Campaign name field. This name will be used in the invitation email. You may include things like the event triggered and they campaign email name.



Create new campaign

Campaign details

Campaign name* 46/60
OOPS! You clicked a link in a phishing email!

Campaign start date*
Select date

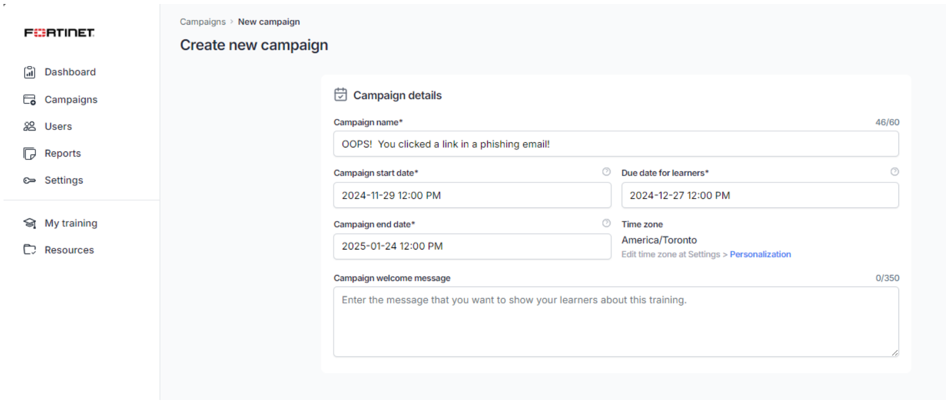
Due date for learners*
Select date

Campaign end date*
Select date

Time zone
America/Toronto
Edit time zone at Settings > Personalization

Campaign welcome message 0/350
Enter the message that you want to show your learners about this training.

3. Configure:
   - The *Campaign start date* and time. This should match your FortiPhish start date and time and timezone.
   - The *Training due date for learners* and time. This should match your FortiPhish end date and time (start time plus 1-4 weeks.
   - The *Campaign End Date* and time. You should enter enough time for any users that may have triggered the event on the last day (such as one to four weeks).



Create new campaign

Campaign details

Campaign name* 46/60
OOPS! You clicked a link in a phishing email!

Campaign start date*
2024-11-29 12:00 PM

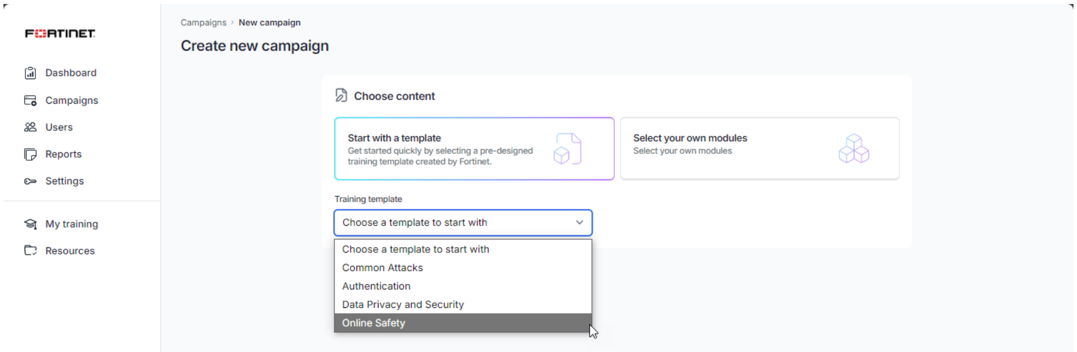
Due date for learners*
2024-12-27 12:00 PM

Campaign end date*
2025-01-24 12:00 PM

Time zone
America/Toronto
Edit time zone at Settings > Personalization

Campaign welcome message 0/350
Enter the message that you want to show your learners about this training.

4. Add a *Campaign welcome message* that will appear with the training assignment in the learner experience.
5. Click *Next*.
6. Select the content you would like to assign the user if they trigger an event (User clicked, User replied, User submitted). In this example, we are triggering on the *User clicked* event.
7. Click *Next*.



Create new campaign

Choose content

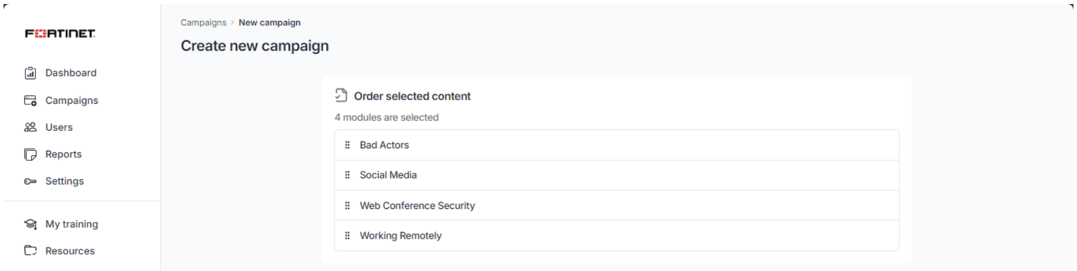
Start with a template
Get started quickly by selecting a pre-designed training template created by Fortinet.

Select your own modules
Select your own modules

Training template: Choose a template to start with

- Choose a template to start with
- Common Attacks
- Authentication
- Data Privacy and Security
- Online Safety

8. You may re-order the content if you wish. Then click *Next*.



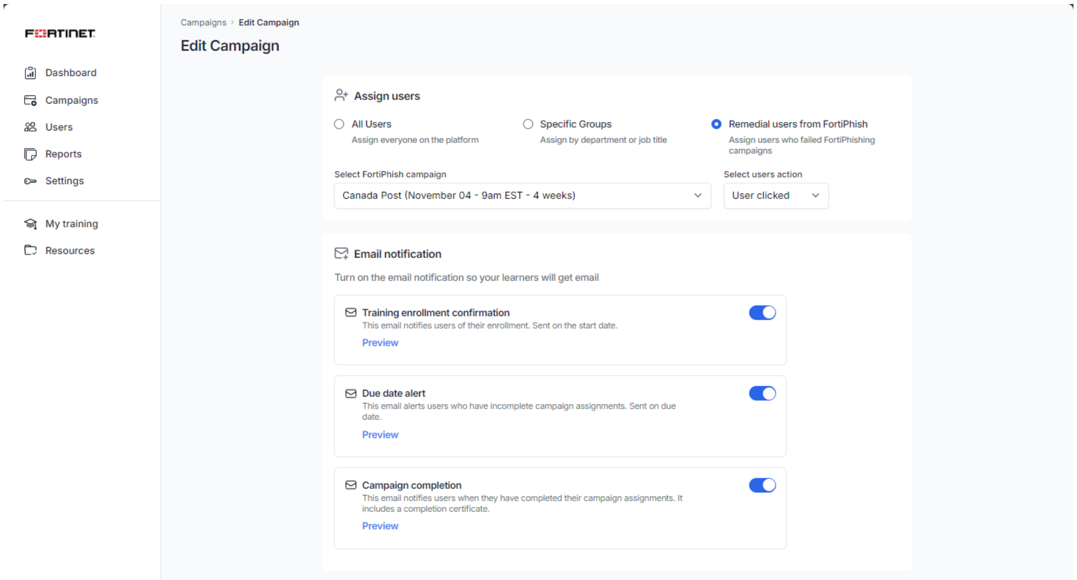
Create new campaign

Order selected content

4 modules are selected

- Bad Actors
- Social Media
- Web Conference Security
- Working Remotely

9. Select the *Remedial users from FortiPhish* option, choose the FortiPhish campaign you just created from the *Select FortiPhish campaign* dropdown, and choose the action the assignment will trigger on from the *Select users action* dropdown.



Edit Campaign

Assign users

○ All Users
Assign everyone on the platform

○ Specific Groups
Assign by department or job title

● Remedial users from FortiPhish
Assign users who failed FortiPhishing campaigns

Select FortiPhish campaign: Canada Post (November 04 - 9am EST - 4 weeks)

Select users action: User clicked

Email notification

Turn on the email notification so your learners will get email

Training enrollment confirmation
This email notifies users of their enrollment. Sent on the start date.
Preview

Due date alert
This email alerts users who have incomplete campaign assignments. Sent on due date.
Preview

Campaign completion
This email notifies users when they have completed their campaign assignments. It includes a completion certificate.
Preview

The FortiPhish campaigns are updated through a scheduled API call. If your campaign does not yet appear in the list, you can select a different campaign and update this later after selecting *Cancel*, then selecting *Save as draft* when the confirmation dialogue pops up.

10. Choose whether you will send the *Training enrollment confirmation*, *Due date alert* and *Campaign completion* emails.
11. Select *Launch campaign*.

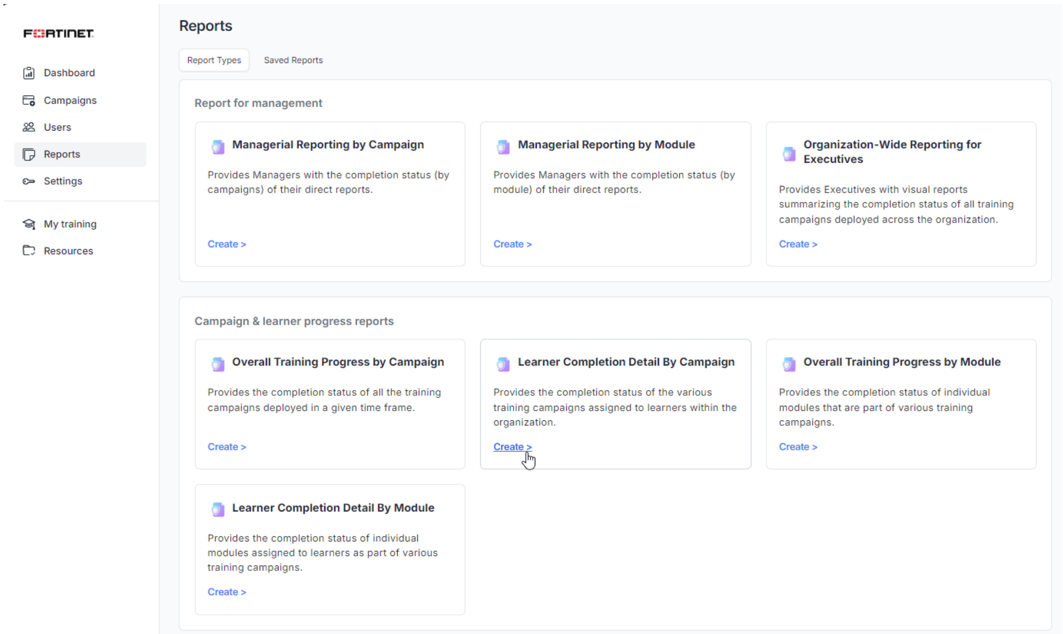
12. You will receive a confirmation message stating that the campaign has been launched. The Campaign should show a status of *Scheduled*.

Creating reports

FortiPhish provides detailed reporting for FortiPhish campaigns. However, for the purposes of tracking the users who have opened, clicked, submitted, or reported phishing emails, you can create a report in the Security Awareness and Training Service.

To schedule a report for your phishing campaign:

1. Select *Reports* from the navigation menu.
2. Select *Create* for the *Learner Completion Detail By Campaign* report from the *Campaign & learner progress reports* section.



Reports

Report for management

Managerial Reporting by Campaign
Provides Managers with the completion status (by campaigns) of their direct reports.

Managerial Reporting by Module
Provides Managers with the completion status (by module) of their direct reports.

Organization-Wide Reporting for Executives
Provides Executives with visual reports summarizing the completion status of all training campaigns deployed across the organization.

Campaign & learner progress reports

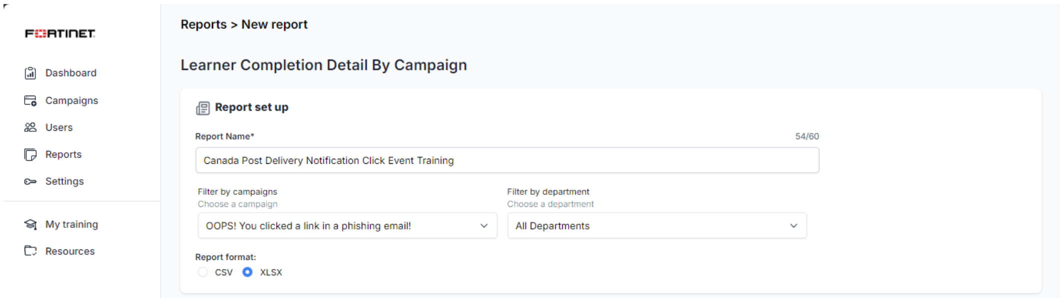
Overall Training Progress by Campaign
Provides the completion status of all the training campaigns deployed in a given time frame.

Learner Completion Detail By Campaign
Provides the completion status of the various training campaigns assigned to learners within the organization.

Overall Training Progress by Module
Provides the completion status of individual modules that are part of various training campaigns.

Learner Completion Detail By Module
Provides the completion status of individual modules assigned to learners as part of various training campaigns.

3. Complete the form:
   - Give your report a meaningful name (such as the phishing campaign name and the trigger event) in the *Report name* field.
   - Select the phishing campaign from the *Choose a campaign* drop down.
   - Select *All Departments* from the *Choose a department* drop down.
   - Choose the *Report format* by selecting one of the option buttons.



Learner Completion Detail By Campaign

Report set up

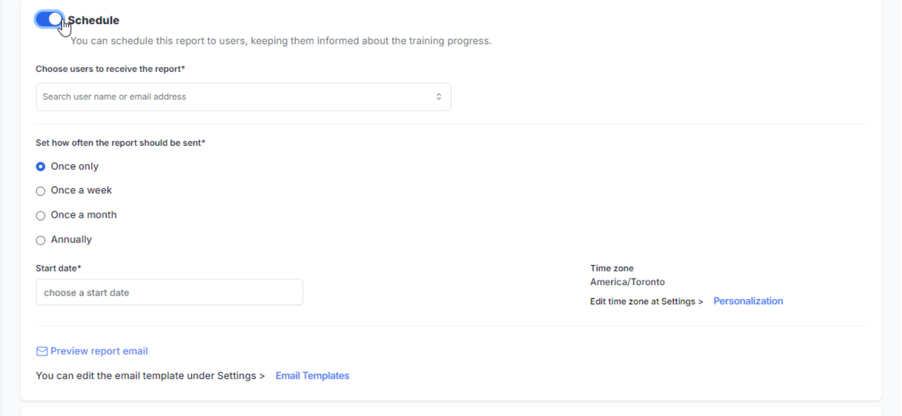
Report Name* 54/60
Canada Post Delivery Notification Click Event Training

Filter by campaigns: OOPS! You clicked a link in a phishing email!

Filter by department: All Departments

Report format: ○ CSV ● XLSX

4. If you wish to schedule the send of the report, scroll down and select *Schedule*. Otherwise, you can just select *Save Report* if you do not wish to send the report to users on a schedule.



Schedule

You can schedule this report to users, keeping them informed about the training progress.

Choose users to receive the report*

Set how often the report should be sent*

● Once only
○ Once a week
○ Once a month
○ Annually

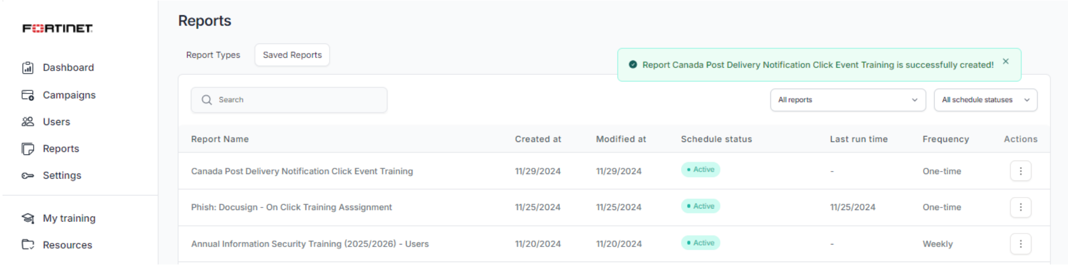
Start date*

Time zone
America/Toronto
Edit time zone at Settings > Personalization

You can edit the email template under Settings > Email Templates

5. Search and select the users that will receive the report from the *Choose users to receive the report* field.
6. Set the frequency by selecting the desired frequency of your choice in the *Set how often users receive the report* section.
7. Set the *Start date* to match or be after the campaign start date and time.
8. Verify and set the correct *Time zone* setting.
9. Click *Save Report*.

   A confirmation message is displayed.



Report Canada Post Delivery Notification Click Event Training is successfully created!

Report Name	Created at	Modified at	Schedule status	Last run time	Frequency	Actions
Canada Post Delivery Notification Click Event Training	11/29/2024	11/29/2024	Active	-	One-time	⋮
Phish: Docusign - On Click Training Asssignment	11/25/2024	11/25/2024	Active	11/25/2024	One-time	⋮
Annual Information Security Training (2025/2026) - Users	11/20/2024	11/20/2024	Active	-	Weekly	⋮

You can *Edit*, *Download* or *Delete* reports by selecting *Reports* from the navigation menu, then selecting the *Saved Reports* tab.

www.fortinet.com